B6FY-4911-01 Z0

FUJITSU Desktop ESPRIMO

導入ガイド

ESPRIMO Edge Computing Edition Z0110/E

FUJITSU

目次

本書をお読みになる前に

このマニュアルの目的

本製品の機能紹介、システム運用開始までの流れ、本製品の設置方法、アプリのインストールや設定方法など本製品をお使いいただくまでに必要なセットアップ情報を説明しています。また、BIOS 設定などの技術情報のほか、導入時のトラブルが発生したときの対処を説明しています。このマニュアルは、本製品のシステム設計担当者とシステム導入担当者を対象としており、コンピューター、OS、およびネットワークについて基本的な知識を有している方がご覧になることを前提としています。

安全にお使いいただくために

本製品を安全に正しくお使いいただくための重要な情報が『取扱説明書』に記載されています。
特に、「安全上のご注意」をよくお読みになり、理解されたうえで本製品をお使いください。

本書の表記

本書の記号

本書に記載されている記号には、次のような意味があります。

重要	お使いになるときの注意点や、してはいけないことを記述しています。必ずお読みください。
POINT	操作に関連することを記述しています。必要に応じてお読みください。
→	参照ページを示しています。

キーの表記と操作方法

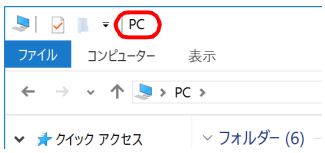
本書中のキーの表記は、キーボードに書かれているマークを記述するのではなく、説明に必要な文字を使い、次のように記述しています。
　例：【Ctrl】キー、【Enter】キー、【→】キーなど
また、複数のキーを同時に押す場合には、次のように「+」でつないで表記しています。
　例：【Ctrl】＋【F3】キー、【Shift】＋【↑】キーなど

連続する操作の表記方法

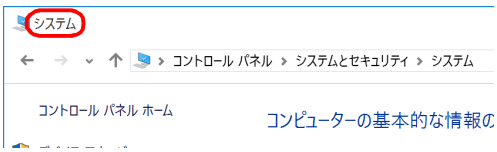
本書中の操作手順において、連続する操作手順を、「→」でつなげて記述しています。
　例：コントロールパネルの「システムとセキュリティ」をクリックし、「システム」をクリックし、「デバイスマネージャー」をクリックする操作
　　↓
　「システムとセキュリティ」→「システム」→「デバイスマネージャー」の順にクリックします。

■ウィンドウ名の表記
本文中のウィンドウ名は、アドレスバーの最後に表示されている名称を表記しています。

例：



↓
「PC」ウィンドウ



↓
「システム」ウィンドウ

画面例およびイラストについて

本文中の画面およびイラストは一例です。お使いの機種やモデルによって、実際に表示される画面やイラスト、およびファイル名などが異なることがあります。また、イラストは説明の都合上、本来接続されているケーブル類を省略したり形状を簡略化したりしていることがあります。

製品の呼び方

本書では、製品名称を次のように略して表記します。

製品名称	本書の表記		
ESPRIMO Edge Computing Edition Z0110/E	エッジコンピューティングデバイス		本製品
Windows 10 IoT Enterprise 2016 LTSB	Windows 10 IoT Enterprise	Windows 10	Windows
Open Java Development Kit	OpenJDK		
Intel Unite®	Intel Unite		

Windows の操作

アクションセンター（Windows 10）

アプリからの通知を表示するほか、クリックすることで画面の明るさ設定や通信機能の状態などを設定できるアイコンが表示されます。

1 画面右下の通知領域にある をクリックします。
画面右側に「アクションセンター」が表示されます。

「コントロールパネル」ウィンドウ

次の手順で「コントロールパネル」ウィンドウを表示させてください。

1「スタート」ボタン→「Windows システム ツール」→「コントロールパネル」の順にクリックします。

「コマンドプロンプト」ウィンドウ

次の手順で「コマンドプロンプト」ウィンドウを表示させてください。

1「スタート」ボタン→「Windows システム ツール」の順にクリックします。

2「コマンドプロンプト」を右クリックし、「その他」→「管理者として実行」をクリックします。

ユーザーアカウント制御

本書で説明している Windows の操作の途中で、「ユーザーアカウント制御」ウィンドウが表示される場合があります。これは、重要な操作や管理者の権限が必要な操作の前に Windows が表示しているものです。表示されるメッセージに従って操作してください。

通知領域のアイコン

デスクトップ画面右下の通知領域にすべてのアイコンが表示されていない場合があります。
表示されていないアイコンを一時的に表示するには、通知領域の をクリックします。

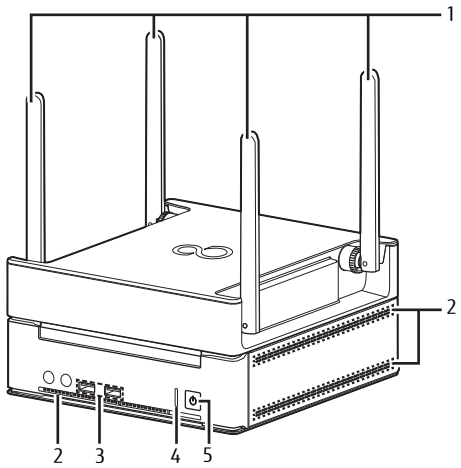
商標および著作権

1

第 1 章
各部名称

各部の名称と働きについて説明します。

1. エッジコンピューティングデバイス前面



1　外部アンテナ

無線電波を受信／送信します。

2　吸気孔

冷却用の空気を取り込むための穴です。

3　USB3.0 コネクタ（•<）

USB 対応周辺機器を接続します。本製品の電源を入れたまま接続、取り外しできます。

4　ステータスランプ

本製品の状態を表示します。

モード	本製品の状態	ステータスランプ
ステータス表示	状態監視機能が異常を検出したとき	点灯
	正常動作時	消灯

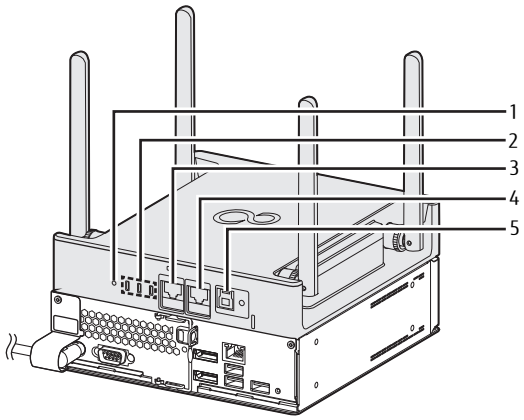
5　電源ボタン／電源ランプ（⏻）

製品本体の電源を入れます。また、本製品の状態を表示します。

LED ランプ	本製品の状態
点灯	動作状態
点滅	スリープ状態
消灯	電源オフまたは休止状態

2. エッジコンピューティングデバイス背面

アクセスポイント部分



（イラストは、電源ケーブル以外のすべてのケーブルを省略した状態です。）

1　RESET ボタン

アクセスポイントを再起動したり、アクセスポイントの設定をご購入時の状態に戻したりします。

・5 秒未満ボタンを押す
　アクセスポイントが再起動します。
・5 秒以上ボタンを押す
　アクセスポイント状態ランプが全部消え、アクセスポイントの設定がご購入時の状態に戻ります。

2　アクセスポイント状態表示ランプ

アクセスポイントの状態を表示します。

アクセスポイントの状態		LED ランプ		
		Ready	2.4G	5G
起動中		点滅 注 1	消灯	消灯
正常稼働	2.4GHz 帯のみ有効	点灯	点灯 注 2	消灯
	5GHz 帯のみ有効		消灯	点灯 注 2
	2.4GHz 帯 /5GHz 帯有効		点灯 注 2	点灯 注 2
緊急モード 有効	2.4GHz 帯のみ有効	点滅 注 3	点灯 注 2	消灯
	5GHz 帯のみ有効		消灯	点灯 注 2
	2.4GHz 帯 /5GHz 帯有効		点灯 注 2	点灯 注 2
エラー発生	2.4GHz 帯のみ有効	点滅 注 4	点灯 注 2	消灯
	5GHz 帯のみ有効		消灯	点灯 注 2
	2.4GHz 帯 /5GHz 帯有効		点灯 注 2	点灯 注 2
電源オフ	2.4GHz 帯のみ有効	消灯	消灯	消灯
	5GHz 帯のみ有効			
	2.4GHz 帯 /5GHz 帯有効			

注 1：1 秒間隔で点滅します。
注 2：データを送受信中の場合は点滅します。
注 3：3 秒間隔で点滅します。
注 4：0.5 秒間隔で点滅します。

3　WAN コネクタ

LAN ケーブルで接続します。
LED の状態は次のとおりです。

	左 LED（Link/Act）	右 LED（Speed）
1000Mbps で Link を確立	緑色点灯注	オレンジ色点灯
100Mbps で Link を確立	緑色点灯注	緑色点灯
10Mbps で Link を確立	緑色点灯注	消灯

注 ： データ転送中は緑色点滅

4　LAN コネクタ

コンピューター部分と LAN ケーブルで接続します。なお、ご購入時に LAN ケーブルは接続されています。ご使用時に必要ですのでケーブルは取り外さないでください。
LED の状態は次のとおりです。

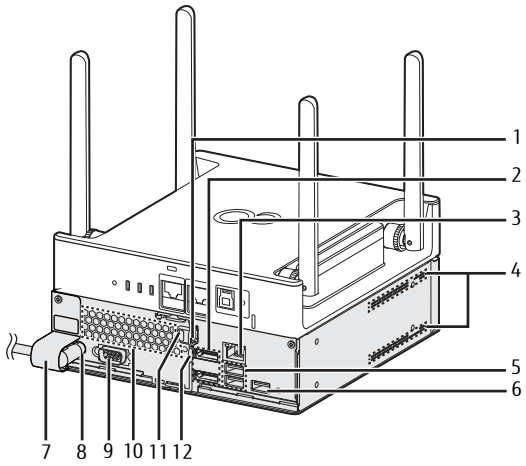
	左 LED（Link/Act）	右 LED（Speed）
1000Mbps で Link を確立	緑色点灯[注]	オレンジ色点灯
100Mbps で Link を確立	緑色点灯[注]	緑色点灯
10Mbps で Link を確立	緑色点灯[注]	消灯

注 ： データ転送中は緑色点滅

5　電源供給用 USB コネクタ

コンピューター部分の電源供給用 USB コネクタに専用ケーブルで接続します。なお、ご購入時に専用ケーブルは接続されています。ご使用時に必要ですのでケーブルは取り外さないでください。

コンピューター部分



（イラストは、電源ケーブル以外のすべてのケーブルを省略した状態です。）

1　セキュリティ施錠金具

市販の鍵を取り付けます。セキュリティ施錠金具の穴径は φ6mm です。

2　DisplayPort コネクタ

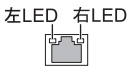
ディスプレイなどの画面表示機器の DisplayPort 信号ケーブルを接続します。

HDMI 形式の画面表示機器を接続する場合は、添付の DP-HDMI 変換アダプタが必要です。

3　LAN コネクタ

コンピューター部分とアクセスポイント部分を LAN ケーブルで接続します。なお、ご購入時に専用ケーブルは接続されています。ご使用時に必要ですのでケーブルは取り外さないでください。

LED の状態は次のとおりです。



状態		左 LED（Link/Act）	右 LED（Speed）
起動時	1000Mbps で Link を確立	緑色点灯[注 1]	オレンジ色点灯
	100Mbps で Link を確立	緑色点灯[注 1]	緑色点灯
	10Mbps で Link を確立	緑色点灯[注 1]	消灯
スリープ 休止状態 電源 OFF	Wake on LAN 有効	緑色点灯[注 1]	消灯[注 2]
		緑色点灯[注 1]	緑色点灯[注 3]
		緑色点灯[注 1]	オレンジ色点灯[注 4]
	Wake on LAN 無効	消灯	消灯

注1：データ転送中は緑色点滅

注2：10Mbps 優先

注3：100Mbps 優先

注4：速度最低ではない

4　吸気孔

冷却用の空気を取り込むための穴です。

5　USB3.0 コネクタ

USB 対応周辺機器を接続します。本製品の電源を入れたまま接続、取り外しできます。

6　電源供給用 USB コネクタ

アクセスポイント部分の電源供給用 USB コネクタに専用ケーブルで接続します。なお、ご購入時に専用ケーブルはネジ止めされています。他の USB 機器を接続すると、故障の原因となります。ご使用時に必要ですので、ケーブルは取り外さないでください。

7　電源ケーブルカバー

電源ケーブルの抜き差しを防止するカバーです。なお、電源ケーブルカバーや電源ケーブルを取り外さないでください。

8　インレット

電源ケーブルを接続します。なお、ご購入時に電源ケーブルは接続されています。電源ケーブルカバーや電源ケーブルを取り外さないでください。

9　シリアルコネクタ

10　排気孔

製品内部の熱を外部に逃がします。

11　盗難防止用ロック取り付け穴

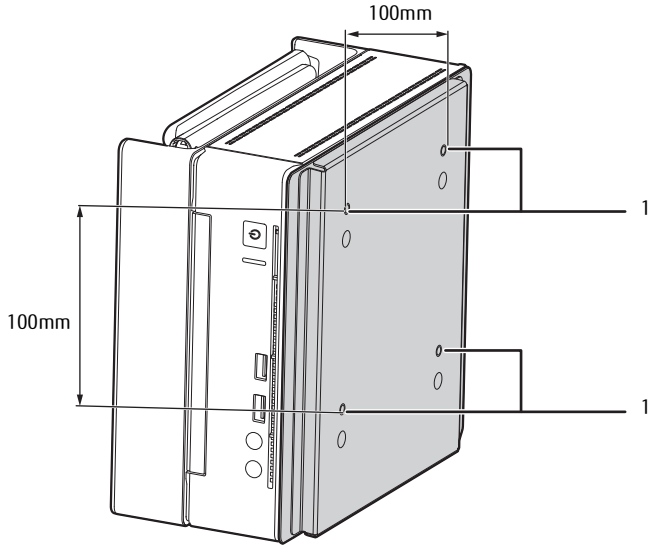
盗難防止用ケーブルを取り付けます。

12　ロック金具

コンピューター部分本体と底面のカバーを留めます。

3. VESA マウント

カスタムメイドオプションで VESA マウントを選択した場合、本製品の底面に VESA 対応のアタッチメントが取り付けてあります。



1　壁掛け金具固定用ネジ穴（4ヶ所）

VESA FDMI 規格対応の壁掛け金具を取り付けるための穴です。

重要

▶必ずお守りください

・取り付け方法および壁掛けキットの設置に際しては、壁掛けキットの取扱説明書に従ってください。
・壁掛け設置には特別な技術が必要です。必ず専門の取付工事業者へご依頼ください。
・本製品の修理依頼時は、保守員に修理作業を依頼する前に、あらかじめお客様で専門の取付業者にご依頼のうえ、壁から本製品を取り外した状態にしておいてください。

POINT

▶VESAマウントを取り外して使用する場合は、添付の底面カバーを取り付けてください。詳しくは、「VESAマウントの取り付け／取り外し」（→P.255）をご覧ください。

壁掛けキットの取り付け方法

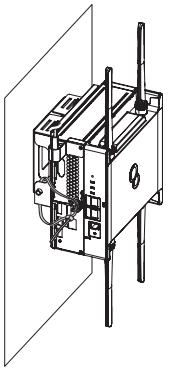
本製品の VESA マウントは、VESA FDMI 規格対応の壁掛け金具に取り付けることができます。

重要

▶本製品に取り付ける壁掛け金具は、VESA FDMI規格に適合したものをお選びください。
▶本製品に取り付けられる壁掛け金具は、次の条件を満たしている必要があります。

・取り付け部分のネジ穴の間隔が 100mm×100mm である
・M4×10mm のネジで、取り付けができる
・8kg の重さに耐えられる

▶ネジは、M4×10mmを必ず使用してください。
▶ネジは最後までしっかりと締めてください。取り付け方が不充分な場合、外れて落ちたり倒れたりして、けがや故障の原因となります。
▶壁掛け金具を取り付けおよび設置するときは、壁掛け金具のマニュアルをご覧ください。
▶壁掛け金具と本体を固定する固定バンドを2本添付しています。壁掛け金具を取り付けおよび設置するときは、固定バンドを取り付けてください。固定バンドの取り付けについては、「壁掛け金具への取り付け」（→P.258）をご覧ください。
▶生徒の手の届かない場所に設置してください。
▶壁掛け金具および壁への取り付け、取り外しは、アンテナを折りたたんだ状態で行ってください。
▶エッジコンピューティングデバイスの向きが下図のようになるように（本製品の銘版ラベルが下から見えるように）取り付けてください。



▶壁に取り付けた後は、上図のようにアンテナを広げてください。折りたたんだままですとアンテナの性能に影響が出る可能性があります。
▶電源ケーブルが突っ張るなど、本製品に負荷がかかる設置状態でのご使用はお控えください。
▶天井からのつり下げには対応しておりません。

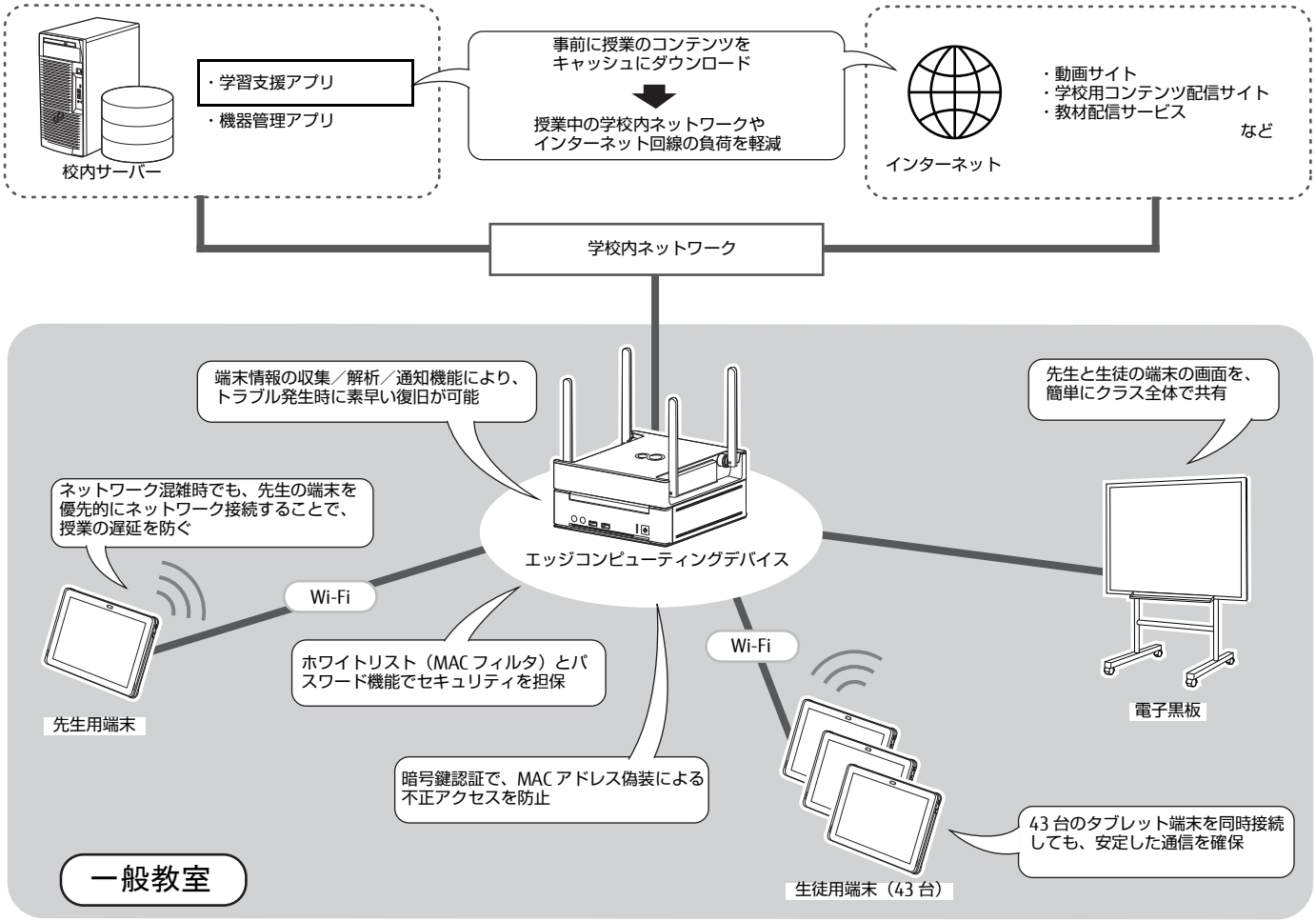
2

第 2 章
概要

本製品の概要について説明します。

1. 本製品について

教室内で発生しているさまざまな困りごとを各教室に本製品が配置されることで解決するソリューションです。



2. 本製品でできること

アプリについて

本製品に搭載されているアプリは、大きく分けて 2 種類があります。

●授業をする先生を支援するアプリ

●タブレット端末を管理 / メンテナンスする管理者を支援するアプリ

各アプリの機能詳細については「本製品の機能について」（→ P.17）をご覧ください。

重要

- 基本機能は本製品を使用するうえで、必要な機能です。基本機能を使用しない場合でも、必ずインストールと設定をしてください。
- 本製品には、コンピューターウイルスを検出・駆除するセキュリティアプリ添付されていません。別途ご用意ください。

先生向けアプリ

種別		アプリ名称	機能概要	機能詳細
授業支援	基本機能	管理画面	本製品に付属するアプリの操作をするための UI 機能	→ P.17
		インターネットキャッシュ機能	インターネット上コンテンツ（動画、静止画を含む）のデータキャッシュ機能	→ P.18
		サーバファイルキャッシュ機能	教材 / 生徒のアップロードした成果物のデータキャッシュ機能	→ P.18
	拡張機能	優先接続設定	本製品に接続するタブレット端末のネットワーク帯域の優先順位を設定する機能	→ P.22
		無線 LAN 接続台数表示	本製品に接続しているタブレット端末の台数表示機能	→ P.21
		Intel Unite	画面共有機能	→ P.22

管理者向けアプリ

種別		アプリ名称	機能概要	機能詳細
アプリの管理 / 操作	基本機能	管理画面	本製品に付属するアプリの操作をするための UI 機能	→ P.17
セキュリティ	拡張機能	端末認証	アクセス制限機能	→ P.19
情報収集		端末情報収集ツール	本製品およびタブレット端末の稼働時間の収集機能	→ P.20
メンテナンス（タブレット端末）		端末情報収集ツール	バッテリー劣化診断機能	→ P.20
		無線 LAN 診断	無線 LAN 接続トラブル診断機能	→ P.20
メンテナンス（本製品自身）	基本機能	動作状態監視ツール	トラブル発生時の自動修復機能と通知機能	→ P.19
		インターネットキャッシュ機能	インターネット上コンテンツ（動画、静止画含む）のデータキャッシュ機能	→ P.18
		お手入れナビ	通風孔のお手入れの時期と装置内部が高温状態であることを通知する機能	→ P.19
通知		メール通知設定	無線 LAN 診断、稼働時間、バッテリー劣化診断の結果を指定したメールアドレスに自動送信する機能	→ P.22

ハードウェアについて

アクセスポイント

本製品は、エッジコンピューティングデバイス本体にアクセスポイント機能を基本機能として搭載しています。本製品のアクセスポイント機能を使用することで、安定した通信と安心のセキュリティを提供します。

●無線規格　IEEE802.11a/b/g/n/ac 4x4 MIMO の搭載

●44 台無線 LAN 端末の安定稼働保証

●インターネットキャッシュ機能の同時接続は、無線 LAN ／有線 LAN 合わせて最大 100 台まで可能

●当社独自のセキュリティ機能搭載

●960 台の MAC アドレスフィルタ対応（15 マルチ SSID ×1 SSID につき 64 台の設定）

●WDS 機能により有線 LAN バックボーンが少ない環境でも無線ネットワークの拡張が可能

アクセスポイント機能について詳しくは、『アクセスポイント操作ガイド』をご覧ください。

3. 本製品の機能について

基本機能 - 管理画面

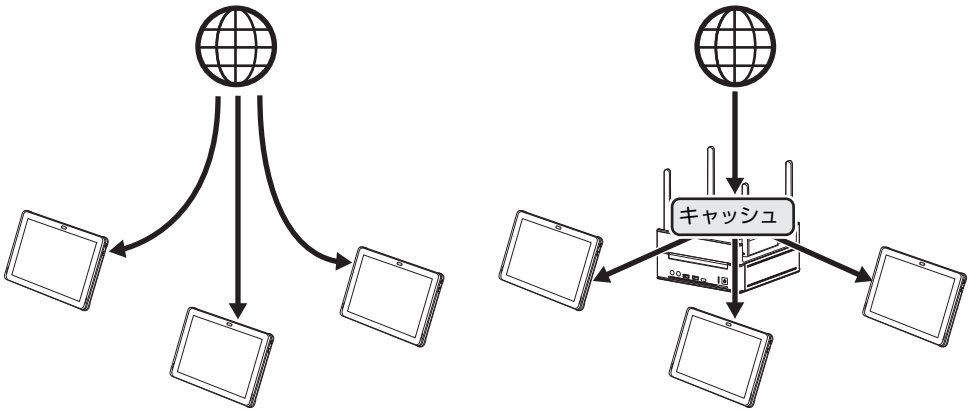
本製品に付属するアプリの設定を管理画面に集約して管理／操作できます管理画面では、本製品を運用するうえで必要な各種設定をブラウザーで行います。
本製品にアクセス可能な端末で設定してください。

管理画面の項目			説明
インターネットキャッシュ管理	キャッシュデータ	キャッシュデーター覧	本製品のキャッシュに保存されているファイルの一覧を閲覧とキャッシュ済みデータを削除できます。
		キャッシュデータ事前登録	授業で使うコンテンツをあらかじめキャッシュすることができます。
		認証情報登録	認証サイトのログイン ID とパスワードを登録します。
	キャッシュエンジン	キャッシュエンジン制御	キャッシュエンジンの起動、停止、再起動、初期化を行うことができます。
		使用状況	キャッシュの使用状況（ヒット率や使用率など）を確認できます。
		ログ取得	インターネットキャッシュ管理機能のログファイルをダウンロードできます。
	キャッシュ設定		キャッシュに関するネットワーク設定とキャッシュデータ制御に関する項目を設定します。
サーバファイルキャッシュ管理	実況状況	簡易情報取得・手動制御	各装置のサーバーキャッシュの同期状態の確認と手動で同期の割込実行ができます。
		詳細情報取得	サーバファイルキャッシュによる同期状況を記載したファイルをダウンロードすることができます。
	キャッシュエンジン	キャッシュエンジン制御	キャッシュエンジンの起動、停止、再起動を行うことができます。
		グループ共通設定	グループ設定したエッジコンピューティングデバイス間で共通の設定項目を変更することができます。
		個別設定	各エッジコンピューティングデバイスのキャッシュエンジンの個別の設定項目の変更やキャッシュエンジンの初期化をすることができます。
		ログ取得	サーバファイルキャッシュ管理機能のログファイルをダウンロードできます。
端末情報管理	解析結果	バッテリー状況一覧	バッテリーの状態を確認できます。
		無線 LAN 診断状況一覧	無線 LAN 診断の状況を確認できます。
		端末稼働時間一覧	本製品に接続した端末の稼働状況を確認できます。
	収集・通知設定	稼働時間	無線 LAN 診断のメール通知に関する設定を変更できます。
		バッテリー	稼働時間のメール通知に関する設定を変更できます。
		メール通知設定	バッテリーのメール通知に関する設定を変更できます。
		情報収集設定（コンピュータ）	エッジコンピューティングデバイスの情報収集の設定を変更したい場合に使用します。
		情報収集設定（端末）	タブレット端末の情報収集の設定を変更したい場合に使用します。
		SMTP 設定	メール通知の SMTP サーバの設定の変更ができます。
管理画面設定	ユーザー管理	パスワード更新	現在ログインしているユーザー ID のパスワードを変更できます。
		ユーザー一覧	登録されているユーザーの情報を確認できます。
	コンピュータ設定	エクスポート / インポート	管理画面の設定と端末から本製品に収集したデータをバックアップと再設定することができます。
	本アプリケーションについて	バージョン情報	管理画面のバージョンを確認できます。

基本機能 - データキャッシュ機能

インターネットキャッシュ機能

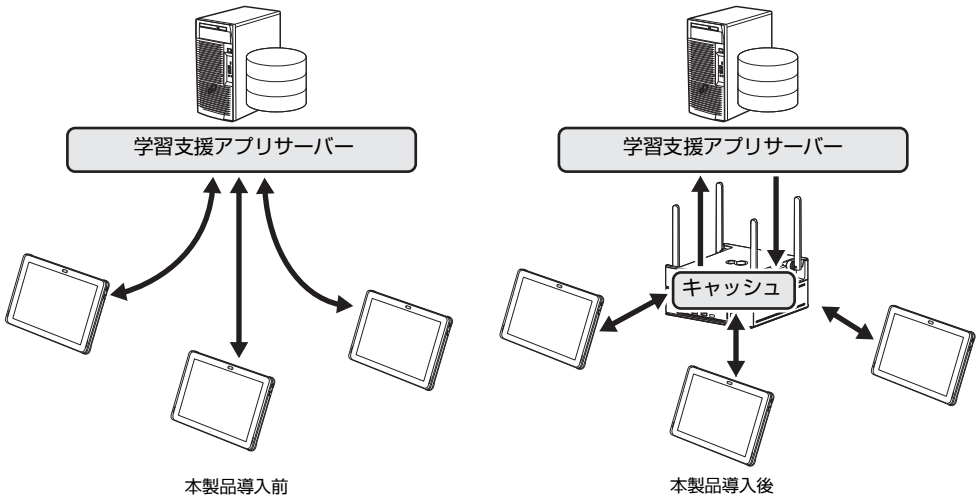
インターネットキャッシュ機能は、本製品に利用コンテンツを保存する機能です。本製品を導入したネットワーク上の最初のタブレット端末がインターネット上のコンテンツをダウンロードするときに、本製品のキャッシュにコンテンツが保存されます。以降のタブレット端末は本製品のキャッシュに保存されたコンテンツをダウンロードすることでインターネット回線の速度の影響を受けることなく、安定して利用することができます。



授業が始まる前に、授業で使うコンテンツをあらかじめキャッシュしておくと、授業をスムーズに進められます。
コンテンツの事前キャッシュは、必ず必要なものではなく、インターネット上の教材を使った授業をスムーズに進めるためのものです。

サーバファイルキャッシュ機能

学習支援アプリとファイル連携する機能です。
先生や生徒が、授業中にそれぞれのタブレット端末で学習支援アプリを使って教材のダウンロードや成果物の提出（アップロード）を行うと、校内ネットワーク回線速度の低下を招きます。その結果、ファイル転送に時間がかかり、先生や生徒はタブレット操作で待ち時間が生じ、円滑な授業の妨げとなります。
サーバファイルキャッシュ機能には、学習支援アプリサーバーに保存された教材などのファイルを本製品にキャッシュする機能と、各生徒（タブレット端末）からの提出物を本製品にキャッシュする機能を持ちます。
本製品にキャッシュされた教材などのファイルをタブレット端末にダウンロードし、本製品に提出物をキャッシュして授業以外の時間帯にサーバーにアップロードすることで、授業中でも安定した校内ネットワーク回線を利用することができます。



基本機能 - 状態監視

動作状態監視ツール

インターネットキャッシュ機能、サーバファイルキャッシュ機能、メンテナンス機能、Intel Unite の動作を監視します。これらの機能が停止した場合、トラブル解決のための機能が発動します。

●インターネットキャッシュ機能、Intel Unite のプロセスがなんらかのトラブルにより機能停止した場合、それらのプロセスを自動復旧します。
自動復旧しても問題が解決しない場合は、MailSetting.ini 設定ファイル（C:¥Program Files¥FCCL¥ProcessAliveWatcher¥Ini¥MailSetting.ini）で指定したメールアドレスに異常が発生したことを通知します。詳しくは、「MailSetting.ini 設定ファイルの変更」（→ P.139）をご覧ください。

●ステータスランプを点灯させ、トラブルが起きていることを通知して復旧をうながします。

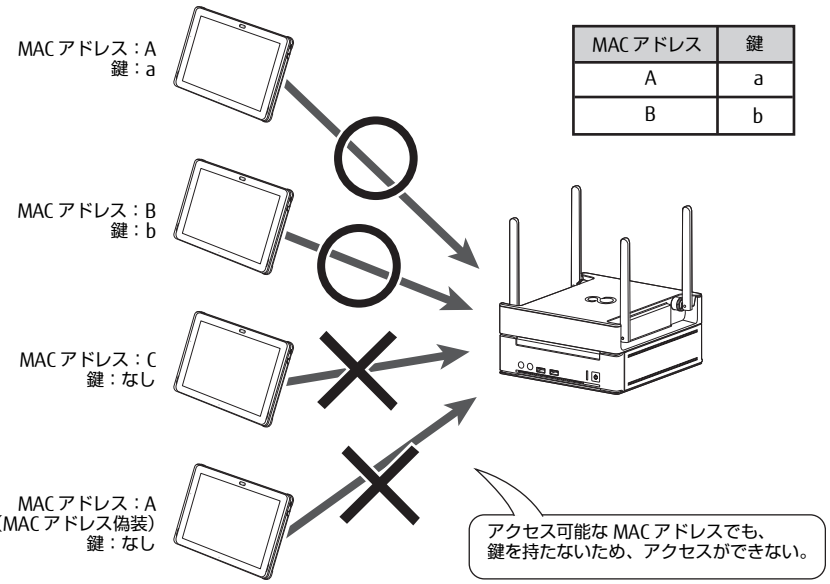
お手入れナビ

本製品の通風孔（空冷用通風路）のお手入れ時期や、ほこりが詰まっていることなどを自動的にお知らせするアプリです。製品本体内部の温度や、本製品の総利用時間をチェックし、本製品のお手入れのを定期的にうながします。

拡張機能 - セキュリティ

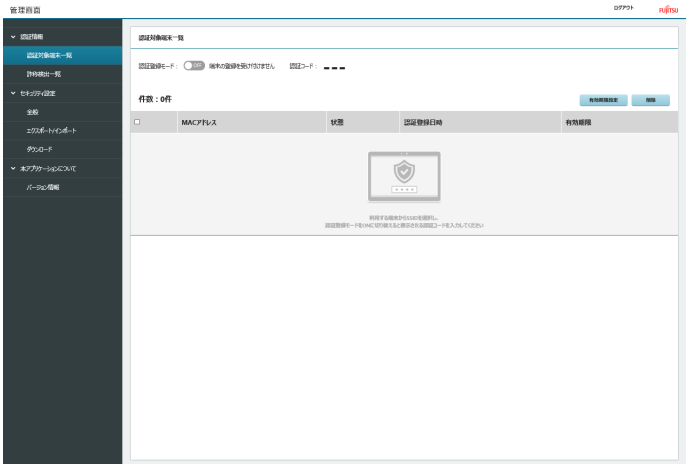
端末認証

端末認証は、MAC アドレス偽装などネットワークへの不正接続を防止することを目的としています。端末認証用の管理画面で端末を認証登録すると、登録した端末だけに暗号鍵が付与されて暗号鍵認証が可能になります。MAC アドレスのフィルタリング機能と暗号鍵認証を組み合わせることで強固なセキュリティを構築でき、悪意のある不正なアクセスから校内ネットワークを守ります。



POINT

▶「端末認証」は、認証端末機能専用の管理画面で設定します。



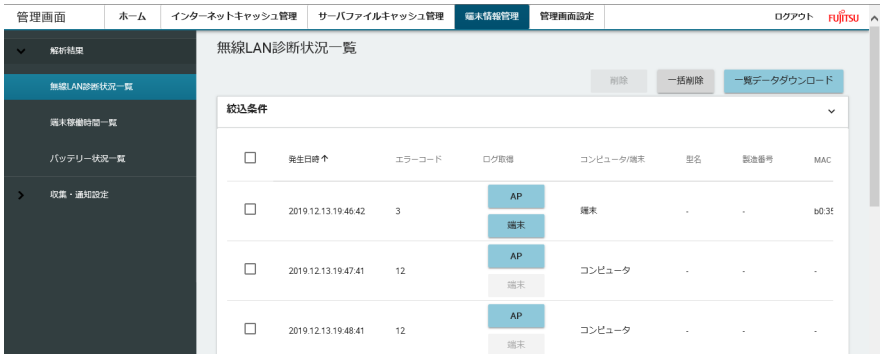
拡張機能 - 端末情報収集

バッテリー劣化診断

タブレット端末のバッテリー劣化を自動判定しバッテリーの交換時期が近づいた端末やバッテリー交換が必要な端末を把握することができます。診断結果は、管理画面で指定したメールアドレスに通知できます。本機能を使うことで授業中にバッテリーが切れるなどのバッテリーに関するトラブルを未然に防ぐことができます。

無線 LAN 診断

本製品の無線 LAN アクセスポイントへの接続に対して、ログイン失敗や接続失敗などのトラブル情報を診断します。診断結果は、管理画面で指定したメールアドレスに通知できます。本機能により、現在発生しているネットワーク接続のトラブルをリアルタイムで把握でき、トラブルの原因を切り分けるための情報として利用することができます。



稼働時間

本製品と本製品に接続したタブレット端末の 1 日当たりの稼働時間と接続台数を集計できます。集計結果は、管理画面で指定したメールアドレスに通知できます。この集計結果は、IT 機器を使った授業の分析 / 提案などに活用いただけます。

無線 LAN 接続台数表示

本製品のアクセスポイント部分に接続されているパソコンやタブレット端末の台数を確認できます。本機能を使用することで、ネットワークに未接続の生徒に対して接続をうながすことができ、クラス全員のタブレット端末が接続している状態で授業を開始できます。

例：先生用端末 1 台、生徒用端末 40 台の場合

先生と生徒全員接続している場合

1 名の生徒が接続できていない場合

拡張機能 - ネットワーク

優先接続設定

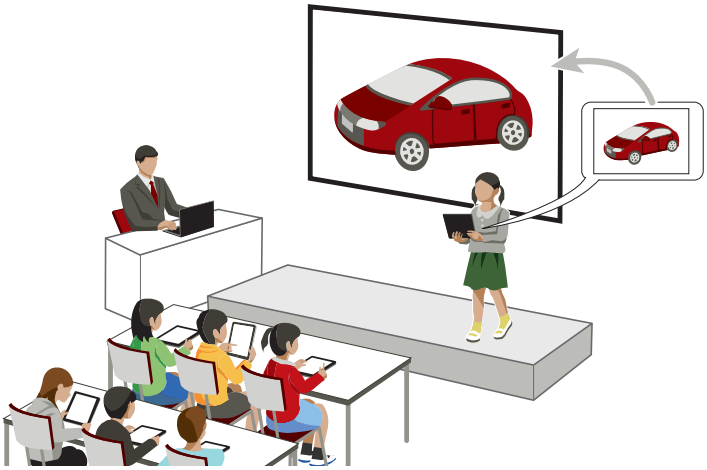
先生の端末を優先的にネットワークに接続することができます。授業で使用するコンテンツのダウンロードに時間がかかるなど、ネットワークの混雑が原因で授業の進行が遅れている場合は、本機能を使用してください。優先接続設定は、複数の先生用端末で設定することが可能ですが、優先接続できる端末は 1 台のみです。2 台以上で同時に優先接続設定を使うことはできません。

拡張機能 - 画面共有

Intel Unite

複数のタブレット端末やパソコンの画面を本製品に接続した画面表示機器（電子黒板、プロジェクター、デジタルテレビなど）の画面に表示して、先生と生徒で画面を共有できます。また、無線 LAN を使うためケーブルをつなぎ替える必要がなく、授業を円滑に進めることができます。

先生が授業で画面共有する場合



生徒が発表などで画面共有する場合

基本機能 - 通知

メール通知設定

次の機能で診断もしくは情報収集した結果を、管理画面で指定したメールアドレスに自動送信します。本製品の管理画面にアクセスできないサポート担当者が状況を把握して、トラブルを未然に防いだり解決したりするのに役立ちます。

- ●バッテリー劣化診断（→ P.20）
- ●無線 LAN 診断（→ P.20）
- ●稼働時間（→ P.20）

4. ストレージ内のアプリについて

本製品には、必要となる各種アプリがストレージ内に格納されています。
フォルダー構成は次のとおりです。

C:¥Fujitsu¥Software¥

- SmartMaintenance　メンテナンス機能用フォルダー
  - ・端末情報収集ツール
  - ・無線 LAN 接続台数表示
  - ・動作状態監視ツール
  - ・管理画面
- InternetCache　インターネットキャッシュ機能用フォルダー
- aplCache　サーバキャッシュ機能用フォルダー
- PriorityBand　優先接続設定用フォルダー
- WirelesslanAnalysis　無線 LAN 診断用フォルダー
- IntelUnite　Intel Unite 用フォルダー
- Oteire　お手入れナビ用フォルダー
- CA_100　端末認証用フォルダー
- Java　OpenJDK 用フォルダー

重要

- 「C:¥Fujitsu¥Software¥SmartMaintenance」フォルダー全体をDVDなどの媒体に書き込んだり、USBメモリにコピーしたりしようとすると失敗する場合があります。その場合は、「SmartMaintenance」フォルダー内の必要なフォルダーをコピーするようにしてください。

5. インストール補助ツール

一部のアプリのインストールと設定は、インストール補助ツールを使ってインストールすることができます。本製品のセットアップは、インストール補助ツールを使用することを推奨いたします。

インストール補助ツールは、下記サイトからダウンロードしてください。

「ドライバダウンロード」（http://www.fmworld.net/biz/fmv/index_down.html）

各バッチファイルは、必ず、管理者権限のアカウントで行ってください。その他の操作方法などについては、インストール補助ツールに添付の Readme.txt をご覧ください。

アプリ名称	対応バッチ名	バッチファイルがインストール／設定する項目	参照先
基本機能			
基本アプリ	01_BasicFunction_BaseAPP_Install.cmd 02_BasicFunction_BaseAPP_Install.cmd	「エクスプローラーの設定」（→ P.62） ～「メンテナンス機能各種サービスの追加」（→ P.83）	「インストール補助ツールを使用する（初期設定）」（→ P.62）
インターネットキャッシュ	BasicFunction_InternetCache_Install.cmd	「インターネットキャッシュ機能のインストールと設定」（→ P.100） ～「シャットダウンの設定」（→ P.114）	「インストール補助ツールを使用する（インターネットキャッシュ機能）」（→ P.100）
動作状態監視ツール	BasicFunction_WatchProcessApp_Install.cmd	「動作状態監視ツールのインストール」（→ P.138） ～「SmtpSetting.txt 設定ファイルの変更」（→ P.140）	「インストール補助ツールを使用する（動作状態監視ツール）」（→ P.138）
拡張機能			
端末認証	01_ExtensionFunction_Auth_Install.cmd 02_ExtensionFunction_Auth_Install.cmd	「Node.js のインストール」（→ P.145） ～「管理アプリケーション（UI 部）の起動」（→ P.167）	「インストール補助ツールを使用する（端末認証）」（→ P.142）
無線 LAN 診断	ExtensionFunction_WirelesslanAnalysis_Install.cmd	「無線 LAN 診断のインストールと設定」（→ P.181） ～「MibAPConfig.xml 設定ファイルの変更」（→ P.183）	「インストール補助ツールを使用する（無線 LAN 診断）」（→ P.181）

6. インターネットキャッシュ機能 V3.1.0

本製品に添付されているインターネットキャッシュ機能は V3.0.0 です。機能の追加や修正のためインターネットキャッシュ機能を V3.1.0 にアップデートする必要があります。

下記サイトから「インターネットキャッシュ機能 V3.0.0 用アップデートモジュール」をダウンロードしてください。

「ドライバダウンロード」（http://www.fmworld.net/biz/fmv/index_down.html）

インターネットキャッシュ機能 V3.0.0 をインストールおよび設定した後、「インターネットキャッシュ機能 V3.0.0 用アップデートモジュール」をインストールしてください。

3

第 3 章
セットアップフロー

本製品をご利用いただくために必要なセットアップのフローを説明しています。

1. セットアップフロー

1. システム設計

「本製品でできること」（→ P.16）をご覧になり、使用する機能の選択や運用パターンなどを設計します。
本製品のアクセスポイント部分の動作モードは、AccessPoint（ブリッジ）に設定した運用を想定しています。
必要に応じて DHCP サーバーや固定 IP アドレスの準備をお願いします。

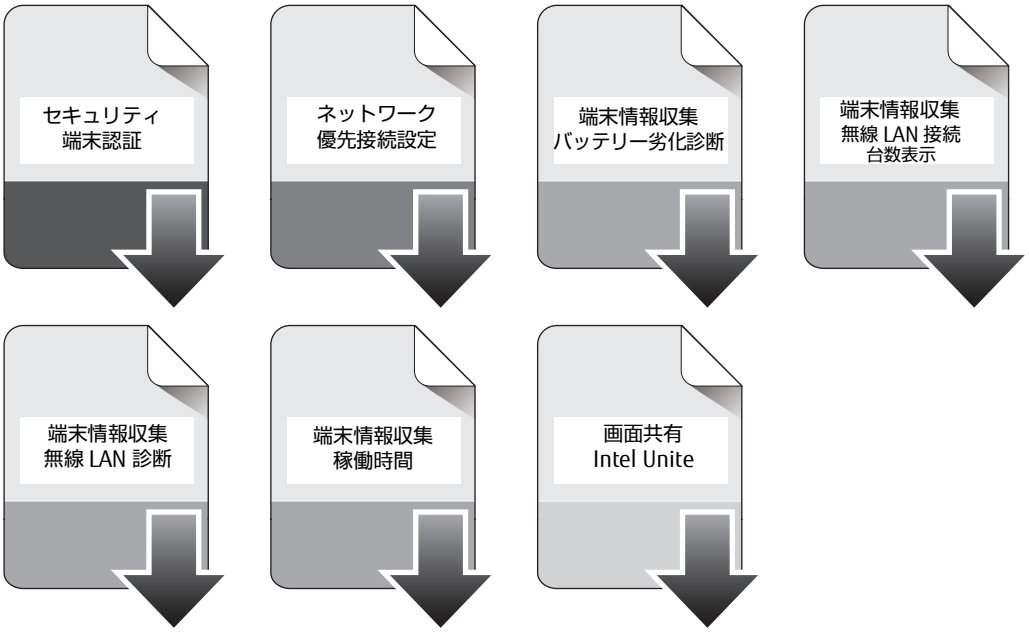
2. 基本機能の設定

基本機能の設定を実施します。
本製品とタブレット端末の基本設定を実施します。
・本製品の設定（設置、電源投入、Windows のセットアップ、基本のアプリのインストールと設定など）
「基本機能 - 初期設定（製品本体）」（→ P.28）
・タブレット端末の設定（基本のアプリのインストールと設定）
「基本機能 - 初期設定（タブレット端末）」（→ P.91）

3. 拡張機能の設定

拡張機能の設定を実施します。
本製品とタブレット端末に拡張機能アプリのインストールと設定を実施します。

システム設計に基づいてインストールする機能を選択してインストール



4. アプリのインストール確認

「セットアップの確認とバックアップ」（→ P.201）をご覧になり、本製品とタブレット端末のセットアップが完了していることを確認します。

5. バックアップ

すべてのセットアップが完了したら、システムイメージ、アクセスポイントの設定、管理画面の設定、端末認証機能の設定のバックアップを作成します（→ P.206）。

6. 運用開始

4

第 4 章
セットアップ

本製品のセットアップについて説明します。

重要

- 本製品のセットアップには、画面表示機器、USBキーボード、USBマウス、USBメモリーなどの機器が必要です。これらの機器は、本製品には添付されておりません。セットアップの前にあらかじめご用意ください。

1. 基本機能 - 初期設定 （製品本体）

インストール補助ツールとインターネットキャッシュ機能 V3.0.0 用アップデートモジュールのダウンロード

一部のアプリのインストールと設定は、「インストール補助ツール」を使ってインストールすることができます。
本製品のセットアップは、「インストール補助ツール」を使用することを推奨します。

「インストール補助ツール」および「インターネットキャッシュ機能 V3.0.0 用アップデートモジュール」は、下記サイトからダウンロードしてください。

「ドライバダウンロード」（http://www.fmworld.net/biz/fmv/index_down.html）

各バッチファイルは、必ず、管理者権限のアカウントで行ってください。その他の操作方法などについては、「インストール補助ツール」および「インターネットキャッシュ機能 V3.0.0 用アップデートモジュール」の README.txt をご覧ください。

製品を設置する

設置に適さない場所

●極端に高温または低温になる場所

●直射日光のあたる場所

●振動の激しい場所や傾いた場所など、不安定な場所

●車、飛行機、船など、輸送機器への設置

●湿気やほこり、油煙の多い場所
CPU ファンなどの機能を低下させる可能性があります。

●風呂場、シャワー室などの水のかかる場所

●腐食性ガス（温泉から出る硫黄ガスなど）が出る場所

●通気性の悪い場所

●火気のある場所

●台所などの油を使用する場所の近く

●テレビやスピーカーの近くなど、強い磁界が発生する場所

●電源ケーブルなどのケーブルが足にひっかかる場所

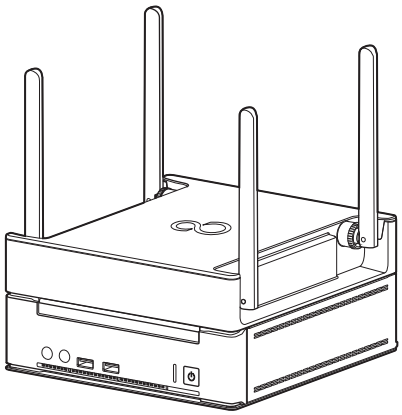
●次の温湿度条件の範囲を超える場所
・ 動作時：温度 10 ～ 35 ℃／湿度 20 ～ 80%RH
・ 非動作時：温度 -10 ～ 60 ℃／湿度 20 ～ 80%RH
ただし、動作時、非動作時とも結露していないこと。

●結露する場所
結露は、空気中の水分が水滴になる現象です。本製品を温度の低い場所から温度の高い場所、または温度の高い場所から温度の低い場所へ移動すると、本製品の装置内部に結露が発生する場合があります。結露が発生したまま本製品を使用すると故障の原因となります。
本製品を移動したときは、室温と同じくらいになるのを待ってから電源を入れてください。

設置する

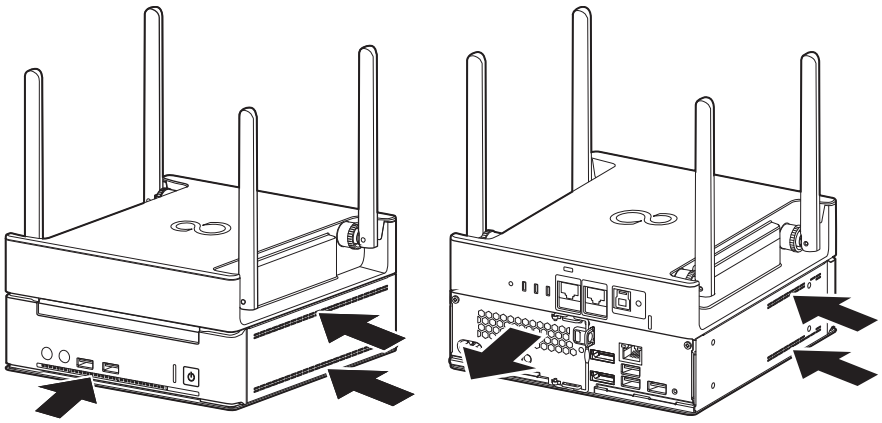
本製品は、アクセスポイント部分が上になるように設置してください。また、本製品の上には、物を置かないでください。

■ 設置例



空気の流れ

本製品の空気の流れは次の図のとおりです。排気孔や吸気孔をふさがないように注意してください。



（イラストは、すべてのケーブルを省略した状態です。）

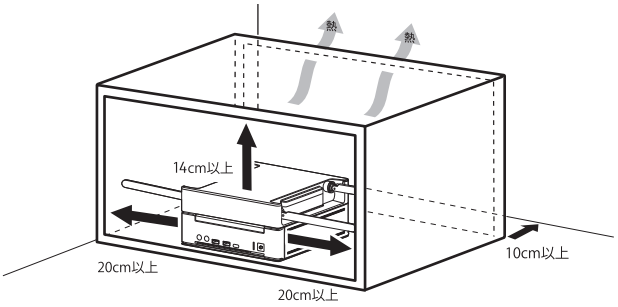
設置時の注意

本製品から排気した熱が周辺にこもらないように次の点に注意してください。

●本製品と壁の間に図で示すようなすき間を空けてください。

●本製品の排気孔や吸気孔をふさがないでください。

●ラックに収納する場合は、次の点にご注意ください。
- 金属のように電波が通りにくくなる素材でできたラックは避けてください。
- ラック収納時は、本製品前面および背面をふさがないでください。

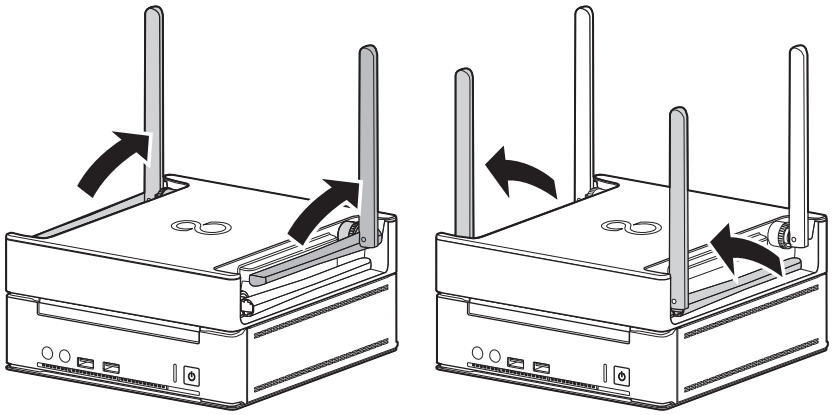


外部アンテナを立てる

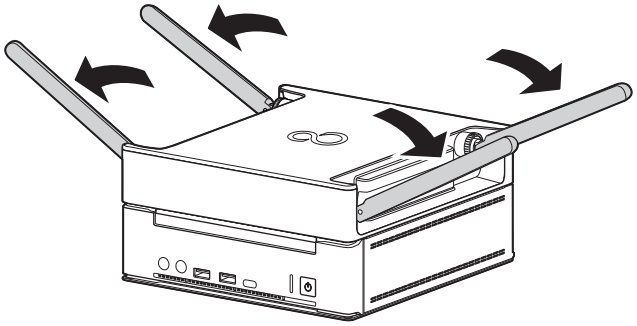
重要

▸外部アンテナに過度な力を加えないでください。

1　本製品の背面側の外部アンテナ（2 本）を垂直に立てた後、前面側の外部アンテナ（2 本）を立てます。



2 本製品上部にスペースがない場合や電波状況が悪い場合など、状況に応じて外部アンテナを横に倒します。



ケーブルを接続する

重要

- 本製品には、画面表示機器、USBキーボード、USBマウスが必要です。これらの機器は、本製品には添付されておりません。セットアップの前にあらかじめご用意ください。
- DisplayPort接続以外の画面表示機器を使用する場合は、変換アダプタが必要になります。HDMI接続の画面表示機器を使用する場合は、添付のDP-HDMI変換アダプタをご使用ください。その他の画面表示機器を接続する場合は、ご使用の画面表示機器にあった変換アダプタをご用意ください。

画面表示機器を接続する

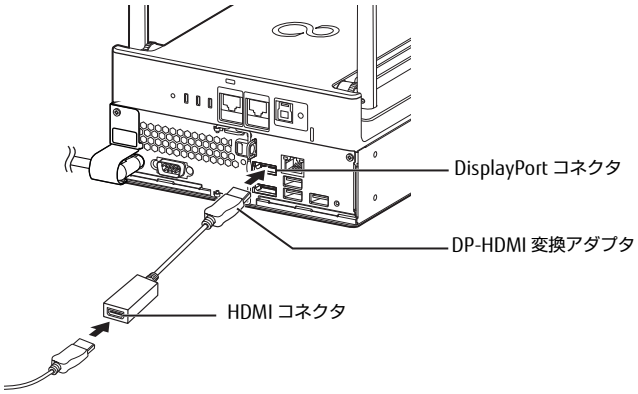
重要

- セットアップが完了するまで、接続する画面表示機器は1台のみにしてください。
- 画面表示機器は1台につき、1本のケーブルで接続してご利用ください。

■HDMI 接続の画面表示機器をお使いの場合

1　画面表示機器の HDMI ケーブルを DP-HDMI 変換アダプタの HDMI コネクタに接続します。

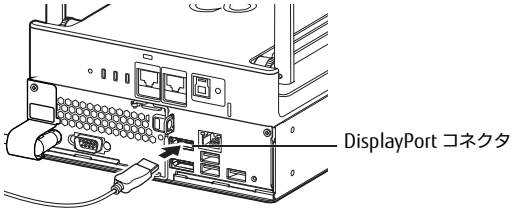
2　本製品背面の DisplayPort コネクタに DP-HDMI 変換アダプタを接続します。



（イラストは、電源ケーブル以外のすべてのケーブルを省略した状態です。）

■DisplayPort 接続の画面表示機器をお使いの場合

1　画面表示機器の DisplayPort 信号ケーブルを本製品背面の DisplayPort コネクタに接続します。



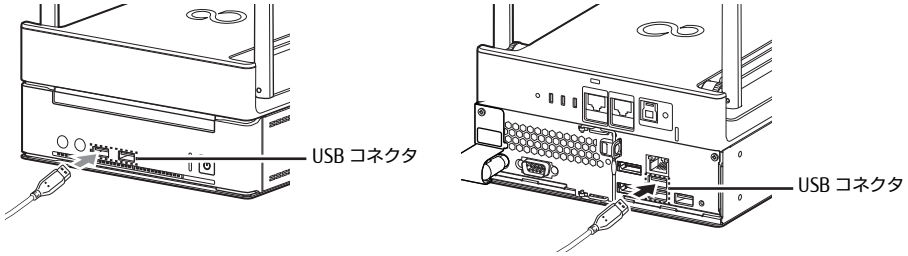
（イラストは、電源ケーブル以外のすべてのケーブルを省略した状態です。）

USB キーボード、USB マウスを接続する

重要

- USBキーボード、USB マウスは、本製品には添付されておりません。あらかじめご用意ください。

1　USB マウスと USB キーボードを本製品の前面、または背面の USB コネクタに接続します。



（イラストは、電源ケーブル以外のすべてのケーブルを省略した状態です。）

電源ケーブルを接続する

重要

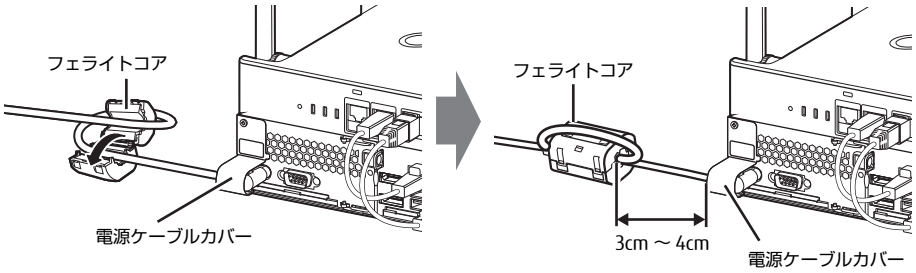
▶本製品を移動する場合や長時間使用しない場合などで、電源ケーブルを取り付けや取り外しを行うときは電源プラグ側を抜き差ししてください。

1　フェライトコアを開きます。

ストッパー（2ヶ所）を外して開いてください。

2　電源ケーブルをフェライトコアに 1 回巻きつけて閉じます。

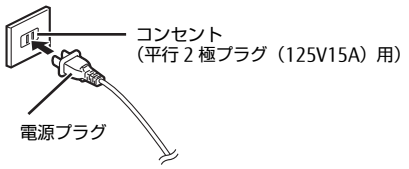
電源ケーブルカバーから約 3cm ～ 4cm の位置に取り付けてください。



3　電源プラグをコンセントに接続します。

重要

▶電源プラグを持ってまっすぐに差し込んでください。ケーブルを差し込んだ状態で上下左右に無理な力を加えないでください。
▶コンセント近くに本製品を設置し、電源プラグに手が容易に届くようにしてください。
▶本製品と電源ケーブルの接続部を押し込んだり引き出したりしないでください。



Windows のセットアップ

注意事項

●Windows のセットアップが完全に行われなかったり、エラーメッセージが表示されたりする場合があります。Windows のセットアップが完了するまでは、次のものを接続または変更しないでください。
・ 周辺機器・拡張カード・2 台目の画面表示機器・BIOS の設定
・ LAN ケーブル（セットアップ時にインターネット接続する場合を除く）

●Windows のセットアップ中は、トラブルを解決する場合を除き、電源を切らないでください。

●Windows のセットアップの各ウィンドウが完全に表示されないうちに、キーを押したりすると、Windows のセットアップが完全に行われない場合があります。ウィンドウが完全に表示されてから操作してください。

■ セットアップで困ったときは

●Windows のセットアップが進められなくなった
電源ボタンを 4 秒以上押して電源を切り、電源ケーブルを抜いてください。30 秒以上待ってから再度電源ケーブルを接続し、電源を入れてセットアップをやり直してください。

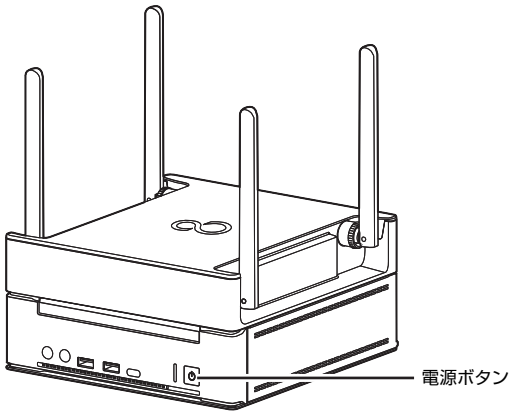
セットアップを実行する

ここで説明するセットアップ手順は一例（インターネットに接続しない方法）です。画面の説明を読み、ご使用になる環境にあわせてセットアップをしてください。
ネットワーク管理者がいる場合は、その指示に従ってください。

■ 電源を入れる

1　画面表示機器に電源を入れます。
画面表示機器の電源の入れ方は、お使いの画面表示機器のマニュアルをご覧ください。

2　電源ボタンを押します。



（イラストは、すべてのケーブルを省略した状態です。）

画面に「FUJITSU」ロゴが表示され、自己診断（POST）が始まります。
画面が表示されるまで、一時的に画面が真っ暗になることや変化がないことがありますが、故障ではありません。絶対に電源を切らずにそのままお待ちください。
自己診断（POST）が終わると「Windows のセットアップ」画面が表示されます。

この後は、Windows のセットアップを行ってください。

■ Windows のセットアップ

次の手順で Windows のセットアップを実行してください。

1「こんにちは」画面が表示されたら、画面の各項目について設定し「次へ」をクリックします。

2「法的文書をお読みください」を読み、「承諾する」をクリックします。

3「簡単設定を使う」をクリックします。

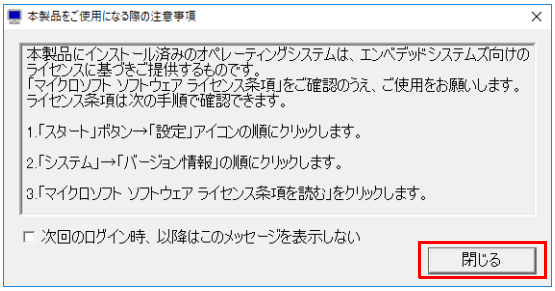
4「この PC のアカウントの作成」の画面で、次の項目を入力し、「次へ」をクリックします。

重要
▸パスワードは必ず設定してください。パスワードが設定されていない場合、一部のアプリでセットアップが失敗します。

・ ユーザー名：12 文字以内の半角英数字（a ～ z、A ～ Z、0 ～ 9）で入力してください。
・ パスワードを入力してください：12 文字以内の半角英数字（a ～ z、A ～ Z、0 ～ 9）で入力してください。
・ もう一度パスワードを入力してください：パスワードを再入力してください。
・ パスワードのヒント：半角英数字のほか、かな、漢字も使用できます。

Windows のセットアップが完了すると、Windows 10 のデスクトップが表示された後、「本製品をご使用になる際の注意事項」が表示されるので、必ず内容をご確認ください。

5「閉じる」をクリックします。

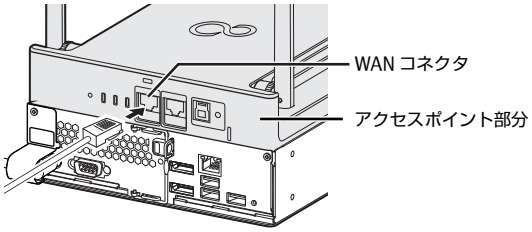


POINT

- 以降、アプリのインストール／設定、ネットワークなどの初期設定を行います。初期設定でトラブルが発生した場合に備え、Windowsセットアップが完了した状態のシステムイメージのバックアップを取得することをお勧めします。システムバックアップについては、『管理ガイド』の「バックアップと復元」をご覧ください。
- BIOSパスワードを設定することで、第三者によるWindowsの起動やBIOS設定を防ぐことができます。必要に応じて、設定してください。BIOSパスワードについては、「BIOSのパスワード機能を使う」（→P.211）をご覧ください。

LAN ケーブルを接続する

アクセスポイント部分の WAN コネクタに LAN ケーブルを接続します。



（イラストは、電源ケーブル以外のすべてのケーブルを省略した状態です。）

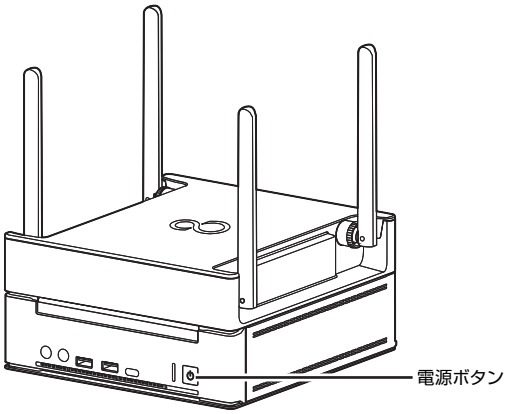
電源の入れ方／切り方

電源を入れる

POINT

▸電源を入れた後、2分程度で無線の電波状態が安定します。

1 電源ボタンを押します。



電源を切る

■注意事項

●電源を切る前に、すべての作業を終了し必要なデータを保存してください。
●電源を切った後、すぐに電源を入れないでください。必ず 30 秒以上たってから電源を入れるようにしてください。
●長期間使用しない場合、または電源を完全に切断する場合は、本製品の電源を切り電源プラグをコンセントから抜いてください。

■Windows を終了する

1 電源ボタンを押します。

重要

▸電源ボタンを長押ししないでください。長押して強制終了するとストレージ内のデータが消失する場合があります。

Windows が終了すると、電源が切れます。

Windows サインイン

次の手順で Windows にサインインします。

1 本製品に画面表示機器を接続します。
「ケーブルを接続する」（→ P.31）

2 BIOS パスワードや Windows パスワードを設定している場合は、本製品に USB キーボード、USB マウスを接続します。
「USB キーボード、USB マウスを接続する」（→ P.31）

3 本製品の電源ボタンを押します。
「電源を入れる」（→ P.35）

4 BIOS のパスワード入力画面が表示された場合は、パスワードを入力します。

5 Windows のパスワード入力画面が表示された場合は、パスワードを入力し、Windows にサインインします。

BIOS パスワードの設定

BIOS パスワードを設定することで、第三者による Windows の起動や BIOS 設定を防ぐことができます。必要に応じて、設定してください。詳しくは、「BIOS のパスワード機能を使う」（→ P.211）をご覧ください。

ME 機能の有効化

ME 機能を BIOS メニューから有効化します。

1 BIOS メニュー 「詳細」ー「AMT 設定」ー「Intel AMT BIOS Extension」を「使用しない」から「使用する」に変更します。
BIOS メニューの使い方、設定の保存方法は「BIOS セットアップの操作のしかた」（→ P.209）をご覧ください。

ME セットアップ初期パスワードの変更

ここでは、ME BIOS Extension の設定を行う ME セットアップ初期パスワードの変更方法について説明します。

パスワードは、必ず変更してください。
本製品ご購入時のパスワードのままですと、第三者に AMT 機能などを使用されるおそれがあります。
本製品を含むすべての AMT 機能搭載製品の初期パスワードは同じパスワードです。
そのため、AMT 機能に第三者がログインすることを防ぐために、必ずパスワードを変更してください。
AMT 機能を使用するとリモート接続で本製品の制御（電源 ON/OFF、設定変更など）が可能となります。

・パスワードは第三者に推測されないように工夫してください。
・パスワードの変更は、本書に記載している設定手順のほか、USB プロビジョニング、リモートプロビジョニングでも行えます。
　詳しくは、Intel® Setup and Configuration Software (Intel® SCS) の User Guide でご確認ください。
　URL：https://www.intel.com/content/www/us/en/software/setup-configuration-software.html

重要

- 修理などによりメインボードを交換された場合は、パスワードを含むMEセットアップの設定値が出荷時の状態に戻る場合があります。その場合は、MEセットアップを設定し直してください。

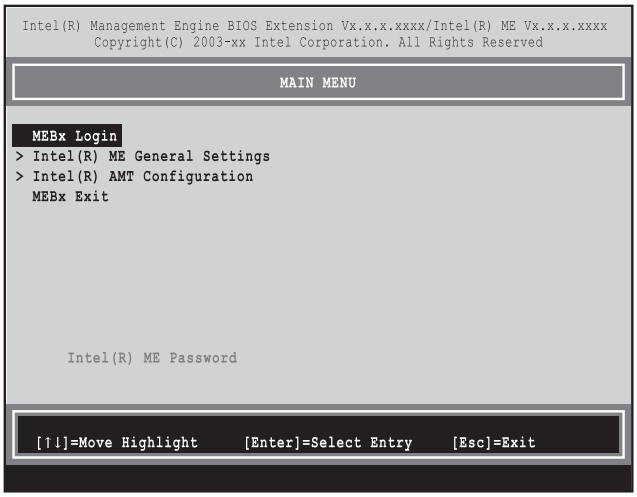
初期パスワードを変更する

ME セットアップの初期パスワードを変更します。ご利用にあたり、パスワードは必ず変更してください。なお、変更したパスワードは、忘れないように大切に保管しておいてください。

1　本製品の電源を入れる、または再起動します。

2　「FUJITSU」ロゴが表示されている間に、【Ctrl】＋【P】キーを押します。
ME セットアップログイン画面が表示されます。

3　「MEBx Login」を選択し、【Enter】キーを押します。



パスワード入力画面が表示されます。

4　「admin」と入力し、【Enter】キーを押します。
出荷時のパスワードは「admin」に設定されています。

POINT

- 「Invalid Password - Try Again」と表示された場合、入力したパスワードが間違っています。【Enter】キーを押してメッセージを消去し、Caps Lockがオフになっていることを確認して、手順3からやり直してください。
- パスワードを3回間違えると「Max password attempts exceeded, system will reboot」と表示され、【Enter】キーを押すと本パソコンが再起動します。手順2からやり直してください。

5　「Intel(R) ME New Password」と表示されたら、新しいパスワードを入力し、【Enter】キーを押します。
パスワードは、次の条件をすべて満たすもので設定してください。
・8 文字以上 32 文字以下
・1 文字以上の数字を含む
・「”」、「,」を除く 1 文字以上の特殊文字（例：@、$、&）を含む。
　ただし、「_」はアルファベットとみなされるため対象外。
・1 文字以上の小文字のアルファベットを含む
・1 文字以上の大文字のアルファベットを含む

6「Verify password」と表示されたら、手順 5 で入力したパスワードを再度入力し、【Enter】キーを押します。

POINT

- 「Error applying new password」と表示された場合、新しいパスワードが手順5の条件を満たしていません。【Enter】キーを押してエラーメッセージを消去し、文字数と使用している文字を確認して、手順3からやり直してください。
- 「Password Mismatch - Abort Change」と表示された場合、手順5と手順6で入力したパスワードが一致していません。【Enter】キーを押してエラーメッセージを消去し、Caps Lockがオフになっていることを確認して、手順3からやり直してください。

7 カーソルキーで「MEBx Exit」を選択し、【Enter】キーを押します。

8「Are you sure you want to exit? (Y/N)」と表示されたら、【Y】キーを押します。
ME セットアップが終了し、Windows が起動します。

ネットワークの設定

ここでは、ネットワークの利用環境を構築するためのコンピューター部分とアクセスポイント部分の最低限の設定方法を説明しています。その他のアクセスポイントの設定方法については、別マニュアルの『アクセスポイント操作ガイド』をご覧ください。

IP アドレスについて

本製品は、固定 IP アドレスによる運用を想定しております。お使いの環境が DHCP により動的に IP アドレスを割り振られた場合でも、使用することは可能ですが、DHCP に対応していないアプリは、IP アドレスが変更になるたびに設定ファイルに記載した IP アドレスの変更が必要なため実用的ではありません。DHCP 対応アプリは下記表をご確認ください。

○：使用可能　×：利用非推奨

アプリ名称	固定 IP アドレス	DHCP サーバー IP アドレス割り当て
管理画面	○	×
インターネットキャッシュ機能	○	×
サーバファイルキャッシュ機能	○	×
端末認証	○	×
端末情報収集ツール（稼働時間）	○	×
端末情報収集ツール（バッテリー劣化診断）	○	×
無線 LAN 診断	○	×
無線 LAN 接続台数表示	○	×
優先接続設定	○	×
Intel Unite	○	○
メール通知設定	○	×

IP アドレスの取得・設定について

コンピューター部分の IP アドレスとアクセスポイント部分の IP アドレスのクラスが異なると、アクセスポイントの Web 設定画面にアクセスできなくなります。どちらかの IP アドレスを変更する場合は、同一セグメント内で IP アドレスを取得して設定する必要があります。
IP アドレスの設定の順番は、設定の順番は次のとおりです。

1　アクセスポイント部分の IP アドレスの設定（→ P.41）

2　コンピューター部分の IP アドレスの設定（→ P.43）

コンピューター部分の IP アドレスから設定すると、アクセスポイントの Web 設定画面にアクセスできなくなりますのでご注意ください。

POINT

▶ アクセスポイント部分のRESETボタンを押してご購入時の設定に戻した後、アクセスポイント部分のIPアドレスを設定する場合は、コンピューター部分のIPアドレスの次の設定を行ってください。

1. 「インターネット プロトコル バージョン 4（TCP/IPv4）のプロパティ」で、コンピューター部分の IP アドレスの設定を、いったん「IP アドレスを自動的に取得する」に設定します。
   設定後、IP アドレス、サブネットマスク、デフォルトゲートウェイの設定は消えてしまいます。設定変更前にテキストファイルなどに記録してください。
   なお、プロパティの表示方法については、「コンピューター部分の固定 IP アドレスの設定」（→ P.43）の手順 1 ～手順 5 をご覧ください。
2. アクセスポイント部分の IP アドレスを設定します（→ P.41）。
3. コンピューター部分の IP アドレスの設定を元に戻します（→ P.43）。

ping コマンドについて

本製品のコンピューター部分から ping コマンドを実行する場合、本製品および ping コマンド送付先の端末で次の設定を行う必要があります。
設定しない場合は、ping コマンド送信先からの応答はありません。

POINT

- 市販のセキュリティ対策ソフトをインストールしている場合は、セキュリティ対策ソフトのマニュアルをご覧になり、ファイアウォールの設定を行ってください。
- セキュリティの関係上、アクセスポイント部分は ping コマンドに応答しません。

1 「コントロールパネル」を表示します（→ P.7）。
「コントロールパネル」が表示されます。

2 「システムとファイアウォール」→「Windows Defender ファイアウォール」の順にクリックします。
「Windows Defender ファイアウォールによる PC の保護」が表示されます。

3 画面右側の「詳細設定」をクリックします。
「セキュリティが強化された Windows Defender ファイアウォール」が表示されます。

4 画面右側の「受信の規則」をクリックします。
「受信の規則」が表示されます。

5 「ファイルとプリンターの共有 （エコー要求 - ICMPv4 受信）」をダブルクリックします。
「ファイルとプリンターの共有 （エコー要求 - ICMPv4 受信）」プロパティが表示されます。

6 「有効」にチェックを入れて、「OK」をクリックします。

7 すべての「ファイルとプリンターの共有 （エコー要求 - ICMPv4 受信）」について、手順 5 ～ 6 を繰り返し実行します。

Web 設定画面へのログイン

アクセスポイント部分の設定を行う場合、本製品から Web 設定画面にログインします。

1 ブラウザーを起動します。

2 アドレスバーに URL（http:// IP アドレス ）を入力し、Web 設定画面にアクセスします。

POINT

- IPアドレスには、本製品のアクセスポイント部分のIPアドレスをお使いください。
  アクセスポイント部分のIPアドレスが「192.168.1.1」の場合は、次のようになります。
  http://192.168.1.1
- ご購入時のIPアドレスは、「192.168.1.1」です。

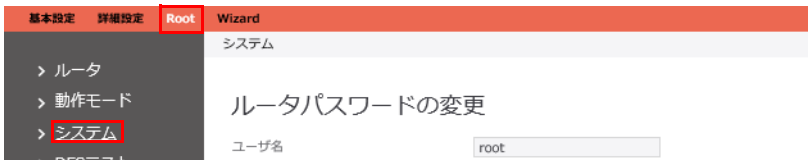
ログイン画面が表示されます。

3 ユーザ名とパスワードを入力し、「ログイン」をクリックします。
ユーザ名の初期値は「root」、パスワードの初期値は「root」です。

パスワードの変更

アクセスポイント部分の初期パスワードを変更します。ご利用にあたり、パスワードは必ず変更してください。なお、変更したパスワードは、忘れないように大切に保管しておいてください。

1 「Root」→「システム」の順にクリックします。



2 ユーザ名「root」と「admin」の「新しいパスワード」と「パスワードの確認入力」にパスワードを入力し、「適用」をクリックします。

重要

▸安全性を高めるため、8文字以上15文字以下で、半角英数字（a～z、A～Z、0～9）および半角記号を組み合わせて作成してください。

パスワード変更後はログイン画面に戻ります。新しいパスワードを入力して、再度、ログインしてください。

動作モードと固定 IP アドレスの設定

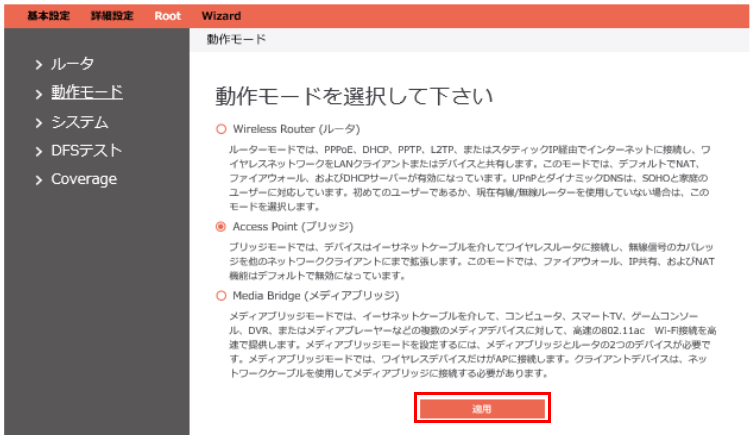
本製品のアクセスポイント部分の固定 IP アドレスや SSID を設定します。

POINT

- アクセスポイント部分の固定IPアドレスが変更されるとブラウザーからはアクセスできなくなり、エラーの表示になります。コンピューター部分の固定IP アドレスの設定をすると正常にアクセスできるようになります。

1「Root」→「動作モード」の順にクリックします。

2「Access Point（ブリッジ）」を選択し、「適用」をクリックします。



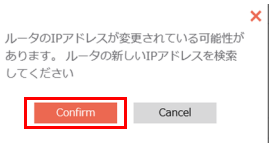
3「LAN IP アドレスの自動取得」で「いいえ」を選択した後、LAN IP 設定の各項目に、取得した固定 IP アドレス、サブネットマスク、デフォルトゲートウェイを入力します。

4 LAN IP 設定の「DNS サーバ 1」と「DNS サーバ 2」に DNS サーバーの IP アドレスを入力し、「次へ」をクリックします。

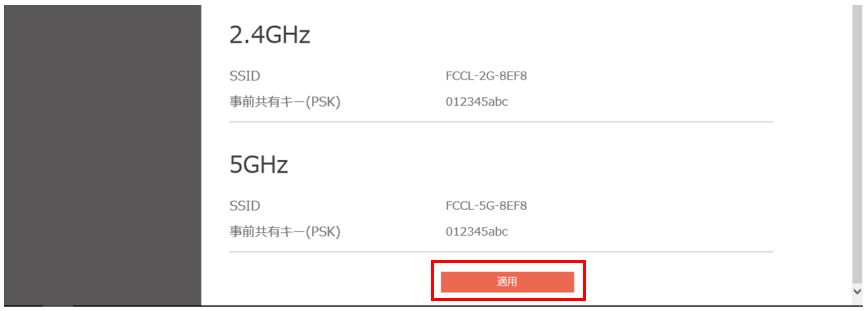
5「2.4GHz」および「5GHz」無線接続の SSID と事前共有キー（PSK）を設定し、「次へ」をクリックします。

「ルータの IP アドレスが変更されている可能性があります。」というメッセージが表示されます。

6「Confirm」をクリックします。



7 画面を下にスクロールしてから「適用」をクリックします。

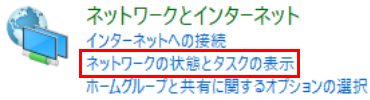


コンピューター部分の固定 IP アドレスの設定

次の手順で、コンピューター部分の固定 IP アドレスを設定します。なお、固定 IP アドレスの設定は、必ず、管理者権限のアカウントで行ってください。

1 「コントロールパネル」を表示します（→ P.7）。
「コントロールパネル」が表示されます。

2 「ネットワークとインターネット」の「ネットワークの状態とタスクの表示」をクリックします。

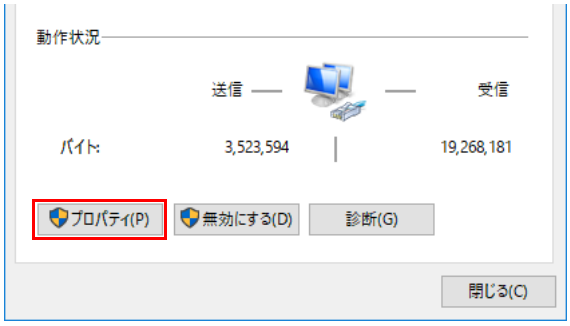


「基本ネットワーク情報の表示と接続のセットアップ」が表示されます。

3 「イーサネット」をクリックします。
「イーサネット 2」と表示される場合は、「イーサネット 2」をクリックしてください。

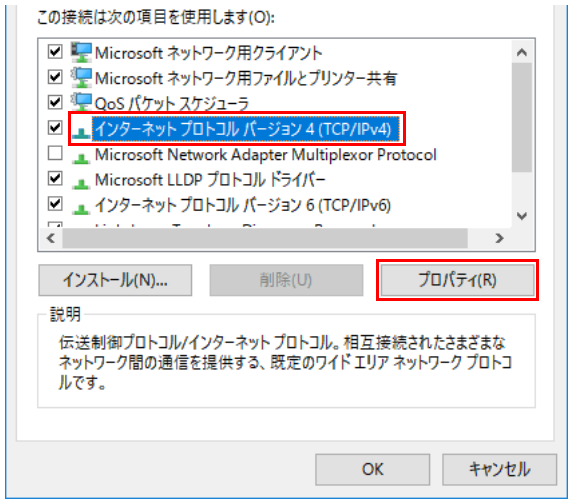
「イーサネットの状態」が表示されます。

4 「プロパティ」をクリックします。



「イーサネットのプロパティ」が表示されます。

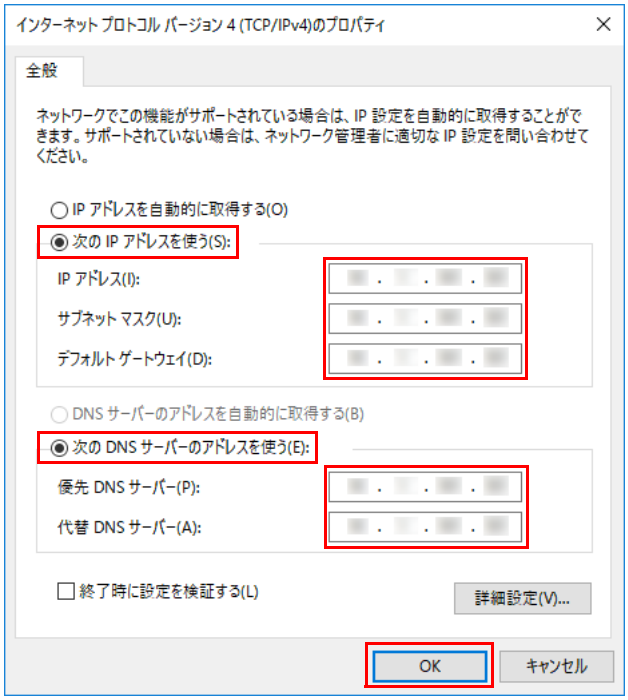
5 「インターネット プロトコル バージョン 4（TCP/IPv4）」を選択し、「プロパティ」クリックします。



「インターネット プロトコル バージョン 4（TCP/IPv4）のプロパティ」が表示されます。

6 次の設定を行い、「OK」をクリックします。

1. 「次の IP アドレスを使う」を選択し、IP アドレス、サブネットマスク、デフォルトゲートウェイを入力します。
2. 「次の DNS サーバーのアドレスを使う」を選択した後、優先 DNS サーバーと代替 DNS サーバーを入力し、「OK」をクリックします。



「イーサネットのプロパティ」が表示されます。

7 「閉じる」をクリックします。

重要

- ネットワーク設定が完了したら、インターネットに接続してWindowsを最新の状態に更新してください。

時刻設定

NTP サーバを追加します。NTP サーバと日付および時刻を同期することで、アクセスポイント部分の日付や時刻の設定を行います。

重要

- 本製品の電源を切ると、アクセスポイントの日付や時刻の設定がクリアされます。
- NTPサーバにアクセスできない場合に備え、複数のNTPサーバを登録してください。

1　ブラウザーのアドレスバーに URL（http:// 新しい IP アドレス）を入力し、Web 設定画面のログイン画面を表示します。

2　「基本設定」→「システム」の順にクリックします。

3　ネットワーク環境に即した NTP サーバ名を入力し、⊕ をクリックします。
学校内に NTP サーバを設置している場合は、学校内の NTP サーバ名を入力してください。

4　「適用」をクリックします。

POINT

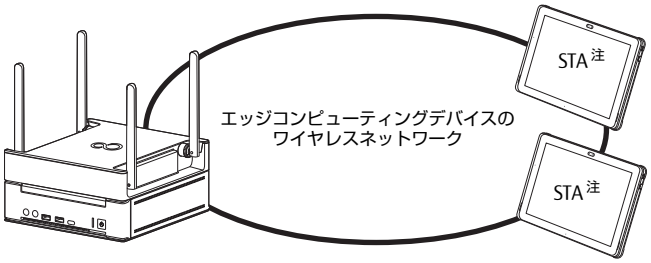
- 登録したNTPサーバを削除する場合は、⊖ をクリックしてください。

無線 LAN 環境を構築する

ここでは、教室内でタブレット端末などを接続するための無線 LAN 環境を構築する手順を説明します。

POINT

▸無線LANの周波数帯で、2.4GHzを使用する場合は、Wi-Fiチャネルを5チャネル以上間隔を空けて、電波干渉がない状態で使用してください。2.4GHzに電波干渉があると、多数のタブレット端末を接続するときに、無線LANに接続できない場合があるため、無線LANの周波数帯は、5GHzを使用することを推奨します。



注：ワイヤレス網内のタブレットなどの端末

本書では以下の設定条件を例に、設定手順を説明します。実際に利用する環境にあわせて設定してください。

- 周波数帯　：5GHz
- SSID　：SSID-sample
- 通信モード　：IEEE 802.11 ac/n/a
- チャネルボンディング　：20/40/80 MHz
- 認証モード　：WPA2Personal
- 事前共有キー（PSK）　：012345abc

1 「詳細設定」→「ネットワーク」→「無線」の順にクリックします。

基本設定が表示されます。

2 「周波数帯」を「5GHz」に設定し、「無線機能」を「有効」に設定します。

3 「SSID」に「SSID-sample」を入力し、「ステルス（隠蔽）SSID」を「無効」に設定します。

4 「通信モード」で、「ac/n/a」を選択します。

5 「チャネルボンディング」で、「20/40/80 MHz」を選択します。

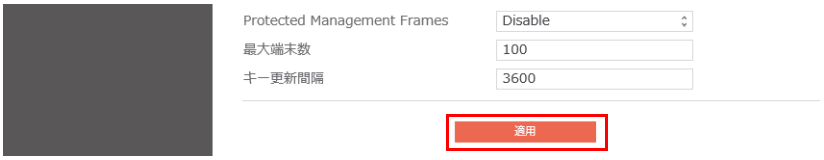
6 「認証モード」で「WPA2 Personal」を選択します。

7 「事前共通キー（PSK）」に「012345abc」を入力します。

POINT

▸「事前共通キー（PSK）」の設定は、ご購入時の設定から変更することをお勧めします。

8 「適用」をクリックします。



優先接続設定

「優先接続設定」がインストール済みのパソコンやタブレット端末で、通信を優先するために必要な設定です。次の手順で設定を行ってください。

1 「詳細設定」→「セキュリティ」→「ACL」→「ユーザ DB」の順にクリックします。

2 「ユーザ DB リスト」の「追加」をクリックします。

ユーザ DB が表示されます。

3 次の項目を設定し、「確認」をクリックします。

1. 「ユーザ DB 名」に「smart」と入力します。
2. 優先接続する複数の端末間でお互いの端末が識別できるような文字列を「ユーザ名」に入力します。
   例）先生の名前で識別する場合
   「富士通太郎先生端末」
   「富士通花子先生端末」
3. 「MAC Address」に優先接続する端末の MAC アドレスを入力します。

4 「ユーザ DB を選択して下さい」に「smart」が登録されていることを確認します。

ネットワーク分離について

ネットワーク分離機能には、3 つのモードがあります。お使いのネットワーク環境と状況によって設定してください。

●Model1
MAC アドレスと IP アドレスで、パケットの転送または破棄を判定します（→ P.51）。

●Model2
MAC アドレスと IP アドレスで送信元を識別して、VLAN ID を決定します。設定したアクセスルールに従って VLAN TAG を付与します（→ P.54）。

●Model3
SSID で VLAN ID を決定します。設定したアクセスルールに従って VLAN TAG を付与します（→ P.56）。

■ VLAN 環境がない場合

Model1（→ P.51）を設定してください。
設定は任意ですが、設定することによってセキュリティがより強化されます。

■ VLAN 環境がある場合で、 かつ VLAN 設定が必要な場合

設定する状況にあわせて必ず Model2（→ P.54）か Model3（→ P.56）を設定してください。

ネットワーク分離の設定ファイルについて

ネットワーク分離は、次の CSV ファイルをインポートして設定します。

●サーバ DB 設定ファイル（SERVER.csv）
サーバの名称とサーバの IP アドレスを記載します。

●アクセスルール DB 設定ファイル（ACL.csv）
アクセスルールを記載します。

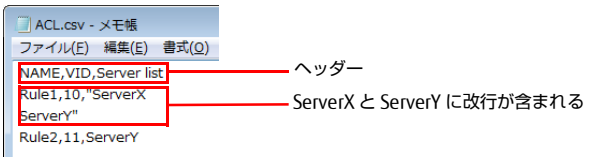
●ユーザ DB 設定ファイル（USER1.csv）
タブレット端末の情報（ユーザー名や MAC アドレス）、ネットワークアクセスの優先度、どのアクセスルールを適用するかを記載します。

●SSID DB 設定ファイル（SSID.csv）
ワイヤレス網の SSID を記載します。

CSV ファイルの作成には、CSV ファイルに対応した表計算ソフトウェアを利用することをお勧めします。表計算ソフトウェアがない場合は、テキストエディターで作成してください。

POINT

▸ CSV ファイルを作成する場合、次の点にご注意ください。
下の図は、CSV ファイルの記載例です。



・必ずヘッダーを記載してください。
・各設定値に改行が含まれる場合は、必ず、ダブルクォート「"」で囲ってください。なお、設定値内に改行がない場合は、ダブルクォートを省略できます。
・各設定値の間にカンマ「,」を記入してください。
・各設定の間は、改行してください。

詳しくは、次の項目をご覧ください。
・「Model1 のネットワーク分離を設定する」（→ P.51）
・「Model2 のネットワーク分離を設定する」（→ P.54）
・「Model3 のネットワーク分離を設定する」（→ P.56）

ネットワーク分離の設定方法

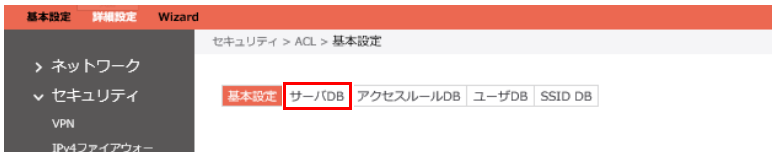
■アクセスコントロールを有効にする

1「詳細設定」→「セキュリティ」→「ACL」の順にクリックします。

2「アクセスコントロール」を「有効」にして、「適用」をクリックします。

■サーバ DB 設定ファイル （SERVER.csv） をインポートする

1「サーバ DB」をクリックします。

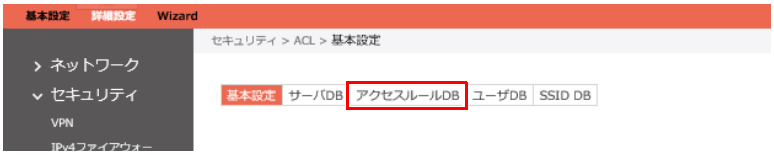


2「サーバ DB のインポート」で をクリックした後、表示されたウィンドウから SERVER.csv ファイルを選択し、「実行」をクリックします。

インポートが完了すると SERVER.csv で記載した設定が「サーバ DB リスト」に表示されます。

■アクセスルール DB 設定ファイル （ACL.csv） をインポートする

1「アクセスルール DB」をクリックします。

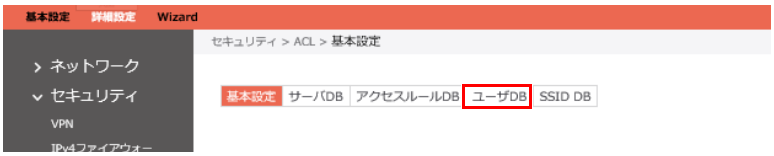


2「アクセスルール DB のインポート」で をクリックした後、表示されたウィンドウから ACL.csv ファイルを選択し、「実行」をクリックします。

インポートが完了すると ACL.csv で記載した設定が「アクセスルールリスト」に表示されます。

■ユーザ DB 設定ファイル （USER1.csv） をインポートする

1「ユーザ DB」をクリックします。

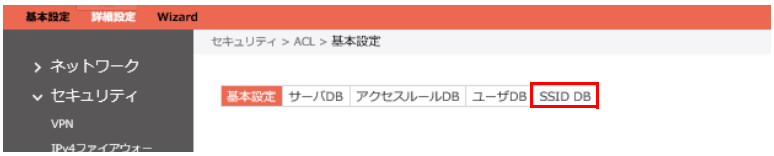


2「新しい DB 名」に「USER1」を入力し、「ユーザ DB のインポート」で をクリックした後、表示されたウィンドウから USER1.csv ファイルを選択し、「実行」をクリックします。
このユーザ DB 名は、SSID.csv で必要となります。

インポートが完了した後、「ユーザ DB を選択して下さい」で「USER1」を選択すると、USER1.csv に記載した設定が「ユーザ DB リスト」に表示されます。

■SSID DB 設定ファイル （SSID.csv） をインポートする

1「SSID DB」をクリックします。

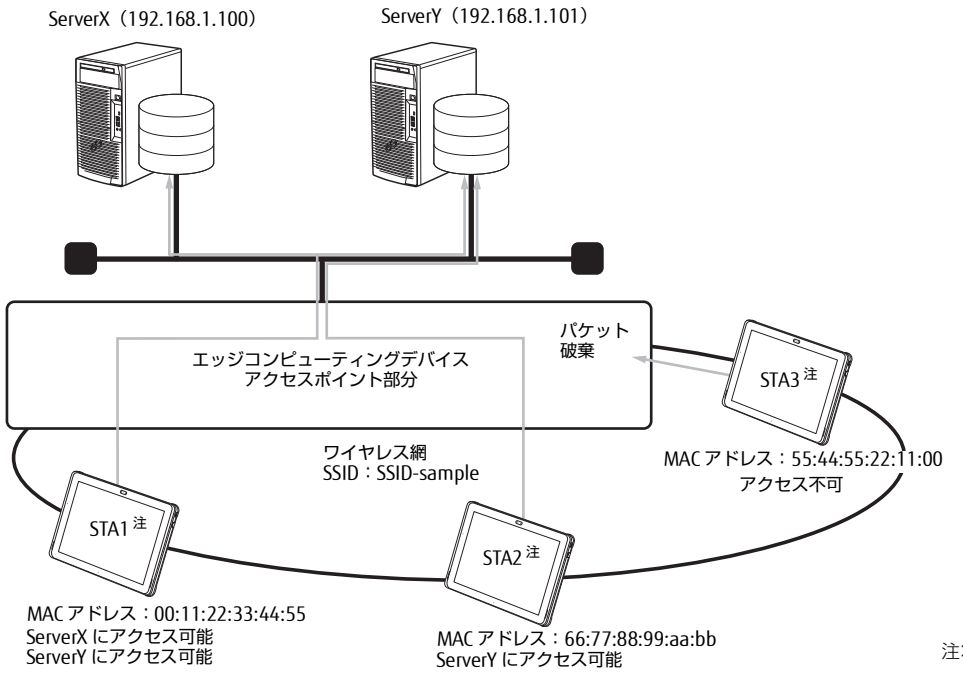


2「SSID DB のインポート」で をクリックした後、表示されたウィンドウから SSID.csv ファイルを選択し、「実行」をクリックします。

インポートが完了すると SSID.csv で記載した設定が「SSID DB リスト」に表示されます。

Model1 のネットワーク分離を設定する

Model1 は、MAC アドレスと IP アドレスでパケットの転送または破棄を判定します。
次の図のような条件を例に、Model1 のネットワーク分離を設定する手順を説明します。



注: ワイヤレス網内のタブレットなどの端末

■設定ファイルを作成する

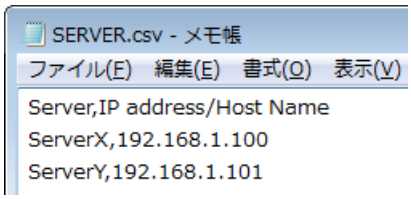
Model1 の設定に必要な CSV ファイルは SERVER、ACL、USER1、SSID です。これらのファイルを事前に、作成してください。なお、各 CSV ファイルの記載内容は、次のとおりです。

●SERVER.csv

Server 注 1	IP address/Host Name 注 2
ServerX	192.168.1.100
ServerY	192.168.1.101

注1：サーバの名称を記載します。
注2：サーバの IP アドレスを記載します。

上の表を CSV ファイルで作成すると、下の図のようになります。

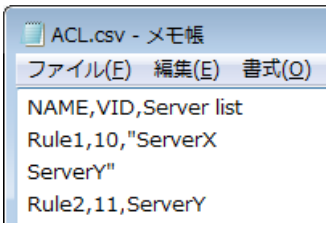


●ACL.csv

NAME	VID 注 1	Server list 注 2
Rule1	10	ServerX ServerY
Rule2	11	ServerY

注1：Model1 では、使用しません。任意の数値を記載してください。
注2：アクセス可能なサーバ名を記載します。

上の表を CSV ファイルで作成すると、下の図のようになります。



●USER1.csv

User Name	MAC address	Access Class 注 1	Access rule 注 2
STA1	00:11:22:33:44:55	AC_VO	Rule1
STA2	66:77:88:99:aa:bb	AC_VO	Rule2

注1：ネットワークアクセスの優先度を記載します。設定値は次のとおりです。
　　Voice：「AC_VO」
　　Video：「AC_VI」
　　Best Effort：「AC_BE」
　　Background：「AC_BK」
注2：ACL.csv で設定したアクセスルールに沿った NAME を記載します。

上の表を CSV ファイルで作成すると、下の図のようになります。

●SSID.csv

SSID Name	Action mode 注 1	VID 注 2	User DB 注 3
SSID-sample	1	12	USER1

注1：ACL モード「1」を記載します。
注2：Model1 では、使用しません。任意の数値を記載してください。
注3：USER1.csv をインポートするときに設定する User DB 名を記載します。

上の表を CSV ファイルで作成すると、下の図のようになります。

■設定ファイルをインポートする

1 SERVER.csv ファイルをインポートします（→ P.49）。

2「サーバ DB リスト」に SERVER.csv ファイルの設定が読み込まれたことを確認します。

サーバDBリスト (最大数: 64)

サーバ名	IPアドレス / ホスト名	編集	削除
ServerX	192.168.1.100		
ServerY	192.168.1.101		

3 ACL.csv ファイルをインポートします（→ P.50）。

4「アクセスルールリスト」に ACL.csv ファイルの設定が読み込まれたことを確認します。

アクセスルールリスト (最大数: 64)

アクセスルール名	VLAN ID	編集	削除
Rule1	10		
Rule2	11		

5 USER1.csv ファイルをインポートします（→ P.50）。

6「ユーザ DB を選択して下さい」で「USER1」を選択します。

ユーザDBを選択して下さい　USER1

7「ユーザ DB リスト」に USER1.csv ファイルの設定が読み込まれたことを確認します。

ユーザDBリスト (最大数: 128)

ユーザ名	MAC Address	Access Class	アクセスルール	編集	削除
STA1	00:11:22:33:44:55	Voice	Rule1		
STA2	66:77:88:99:aa:bb	Voice	Rule2		

8 SSID.csv ファイルをインポートします（→ P.51）。

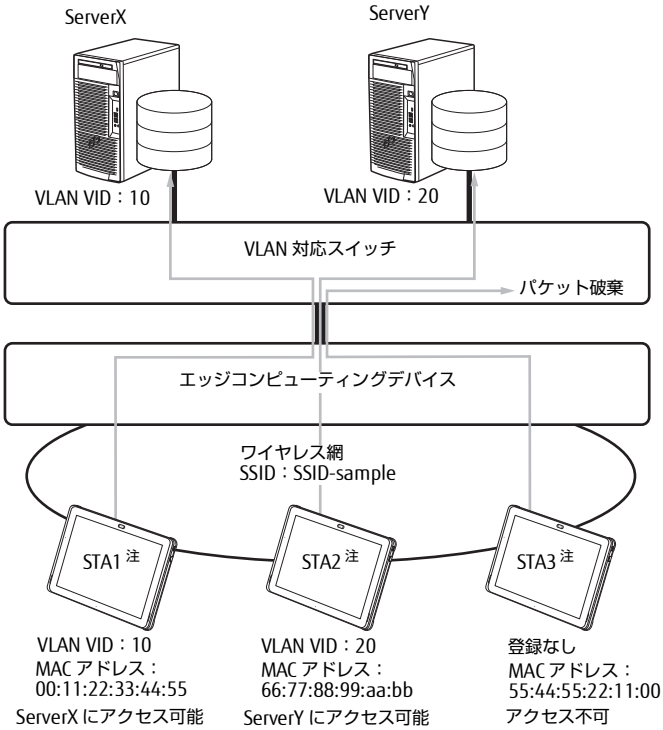
9「SSID DB リスト」に SSID.csv ファイルの設定が読み込まれたことを確認します。

SSID DBリスト (最大数: 32)

SSID名	ACL モード	VLAN ID	ユーザDB	編集	削除
SSID-Sample	1	12	USER1		

Model2 のネットワーク分離を設定する

Model2 は、MAC アドレスと IP アドレスで送信元を識別して、VLAN ID を決定します。
設定したアクセスルールに従って VLAN TAG を付与します。



注： ワイヤレス網内のタブレットなどの端末

■設定ファイルを作成する

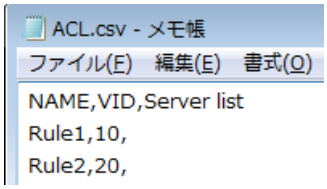
Model2 の設定に必要な CSV ファイルは ACL、USER1、SSID です。これらのファイルを事前に、作成してください。なお、各 CSV ファイルの記載内容は、次のとおりです。

●ACL.csv

NAME	VID 注 1	Server list 注 2
Rule1	10	
Rule2	20	

注1：使用する VID を記載します。
注2：Model2 では、使用しません。CSV ファイルへの記載は不要です。

上の表を CSV ファイルで作成すると、下の図のようになります。



●USER1.csv

User Name	MAC address	Access Class 注 1	Access rule 注 2
STA1	00:11:22:33:44:55	AC_VO	Rule1
STA2	66:77:88:99:aa:bb	AC_VO	Rule2

注1：ネットワークアクセスの優先度を記載します。設定値は次のとおりです。
　　Voice：「AC_VO」
　　Video：「AC_VI」
　　Best Effort：「AC_BE」
　　Background：「AC_BK」
注2：ACL.csv で設定したアクセスルールに沿った NAME を記載します。

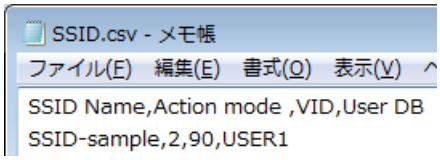
上の表を CSV ファイルで作成すると、下の図のようになります。

●SSID.csv

SSID Name	Action mode 注 1	VID 注 2	User DB 注 3
SSID-sample	2	90	USER1

注1：ACL モード「2」を記載します。
注2：Model2 では、使用しません。任意の数値を記載してください。
注3：USER1.csv をインポートするときに設定する User DB 名を記載します。

上の表を CSV ファイルで作成すると、下の図のようになります。



■設定ファイルをインポートする

1 ACL.csv ファイルをインポートします（→ P.50）。

2 「アクセスルールリスト」に ACL.csv ファイルの設定が読み込まれたことを確認します。

3 USER1.csv ファイルをインポートします（→ P.50）。

4 「ユーザ DB を選択して下さい」で「USER1」を選択します。

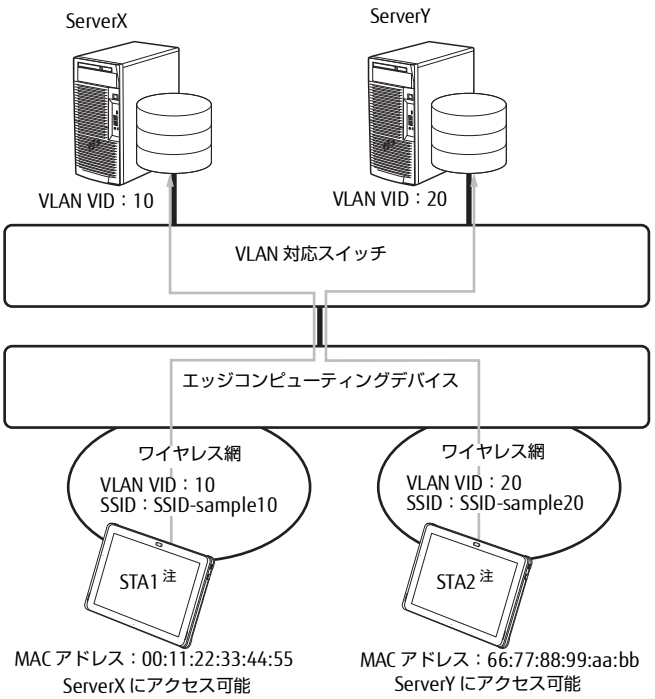
5 「ユーザ DB リスト」に USER1.csv ファイルの設定が読み込まれたことを確認します。

6 SSID.csv ファイルをインポートします（→ P.51）。

7 「SSID DB リスト」に SSID.csv ファイルの設定が読み込まれたことを確認します。

Model3 のネットワーク分離を設定する

SSID で VLAN ID を決定します。
設定したアクセスルールに従って VLAN TAG を付与します。



注 ： ワイヤレス網内のタブレットなどの端末

■設定ファイルを作成する

Model3 の設定に必要な CSV ファイルは ACL、USER1、SSID です。これらのファイルを事前に、作成してください。なお、各 CSV ファイルの記載内容は、次のとおりです。

●ACL.csv

NAME	VID 注 1	Server list 注 2
Rule1	90	

注1：Model3 では、使用しません。任意の数値を記載してください。
注2：Model3 では、使用しません。CSV ファイルへの記載は不要です。

上の表を CSV ファイルで作成すると、下の図のようになります。

●USER1.csv

User Name	MAC address	Access Class 注 1	Access rule 注 2
STA1	00:11:22:33:44:55	AC_VO	Rule1
STA2	66:77:88:99:aa:bb	AC_VO	Rule1

注1：ネットワークアクセスの優先度を記載します。設定値は次のとおりです。
　　Voice：「AC_VO」
　　Video：「AC_VI」
　　Best Effort：「AC_BE」
　　Background：「AC_BK」
注2：ACL.csv で設定したアクセスルールに沿った NAME を記載します。

上の表を CSV ファイルで作成すると、下の図のようになります。

●SSID.csv

SSID Name	Action mode 注 1	VID 注 2	User DB 注 3
SSID-sample10	3	10	USER1
SSID-sample20	3	20	USER1

注1：ACL モード「3」を記載します。
注2：VID の値を記載します。
注3：USER1.csv をインポートするときに設定するユーザ DB 名を記載します。

上の表を CSV ファイルで作成すると、下の図のようになります。

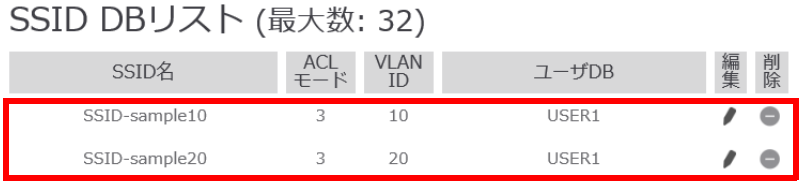
■設定ファイルをインポートする

1 ACL.csv ファイルをインポートします（→ P.50）。
2 「アクセスルールリスト」に ACL.csv ファイルの設定が読み込まれたことを確認します。

3 USER1.csv ファイルをインポートします（→ P.50）。
4 「ユーザ DB を選択して下さい」で「USER1」を選択します。

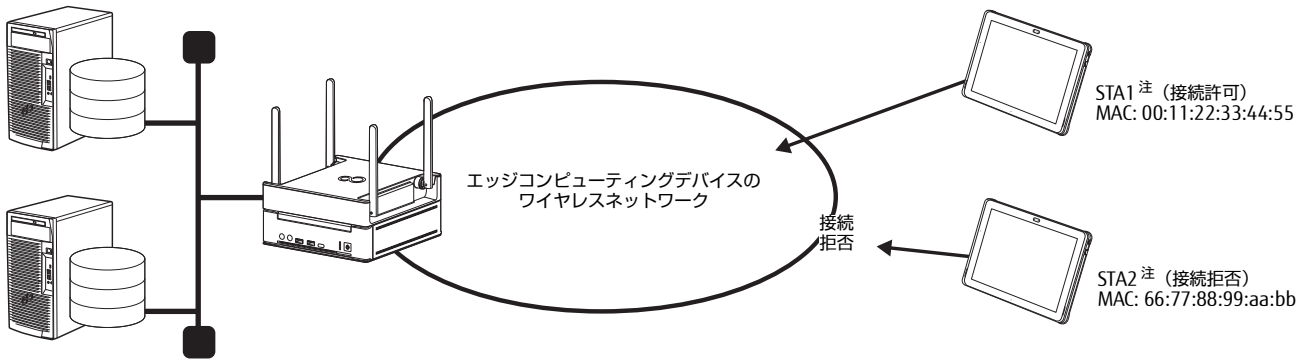
5 「ユーザ DB リスト」に USER1.csv ファイルの設定が読み込まれたことを確認します。

6 SSID.csv ファイルをインポートします（→ P.51）。
7 「SSID DB リスト」に SSID.csv ファイルの設定が読み込まれたことを確認します。



MAC フィルタ

MAC フィルタは STA の MAC アドレスを使用して、ワイヤレス網への接続を許可または拒否する機能です。
ここでは、特定の STA のみワイヤレス網への接続を許可する場合を例に説明します。



注： ワイヤレス網内のタブレットなどの端末

次の設定条件を例に MAC フィルタを構築します。

・ 周波数帯　　：5GHz
・ SSID　　：SSID-sample
・ MAC フィルタモード　：許可

■設定ファイルを作成する

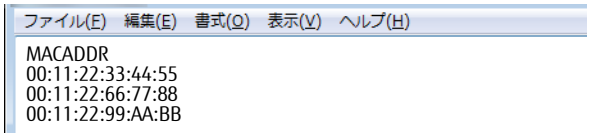
CSV ファイルを事前に作成してください。なお、CSV ファイルの記載内容は、次のとおりです。

●mac_filter.csv

MACADDR 注
00:11:22:33:44:55
00:11:22:66:77:88
00:11:22:99:AA:BB

注：接続許可する MAC アドレスを記載します。

上の表を CSV ファイルで作成すると、下の図のようになります。

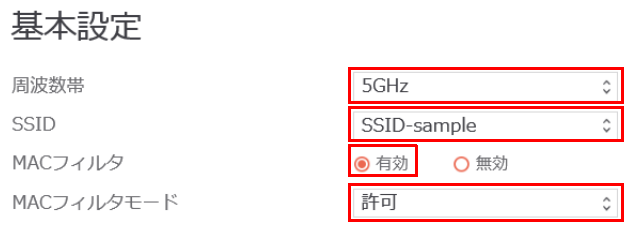


■設定ファイルをインポートする

1「詳細設定」→「ネットワーク」→「無線」→「MAC フィルタ」の順にクリックします。

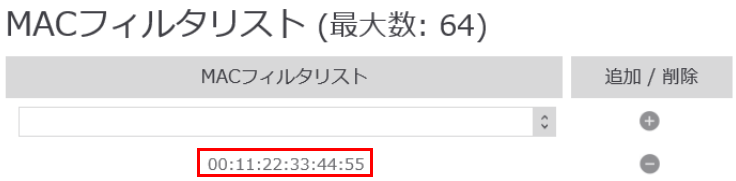
2 基本設定の各項目を次のように設定します。

・ 周波数帯　　：5GHz
・ SSID　　：SSID-sample
・ MAC フィルタ　　：有効
・ MAC フィルタモード　　：許可



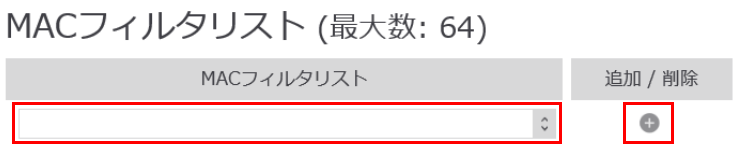
3 「MAC アドレスリスト」をインポートで、作成した CSV ファイルを選択し、「実行」をクリックします。

4 「MAC フィルタリスト」に CSV ファイルの設定が読み込まれたことを確認します。



POINT

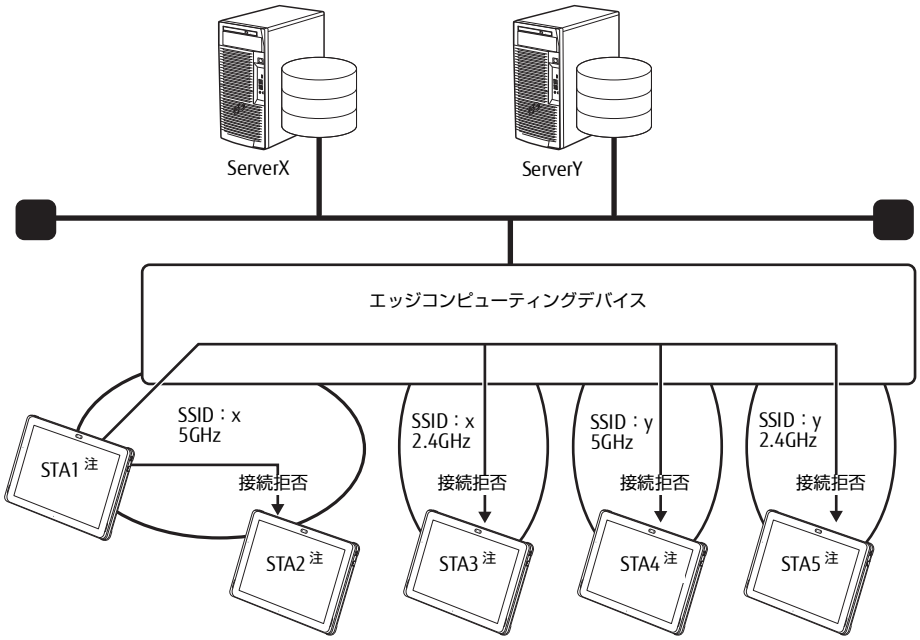
▸MACアドレスを手動で設定する場合は、次の操作を行ってください。



1.「MAC フィルタリスト」に MAC アドレスを入力します。
2.「追加／削除」で、⊕（追加）をクリックします。

プライバシープロテクション

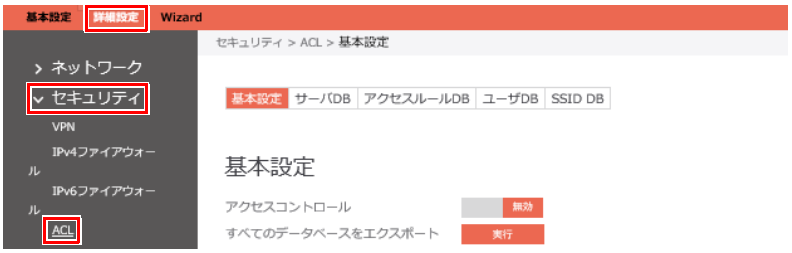
プライバシープロテクションは STA のセキュリティを確保するため、STA 間の通信を制限する機能です。
ここでは、STA 間の通信をすべて制限する場合の設定について説明します。



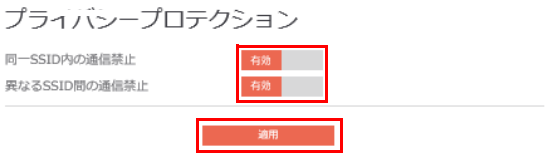
注： ワイヤレス網内のタブレットなどの端末

■ プライバシープロテクションを有効にする

1「詳細設定」→「セキュリティ」→「ACL」の順にクリックします。

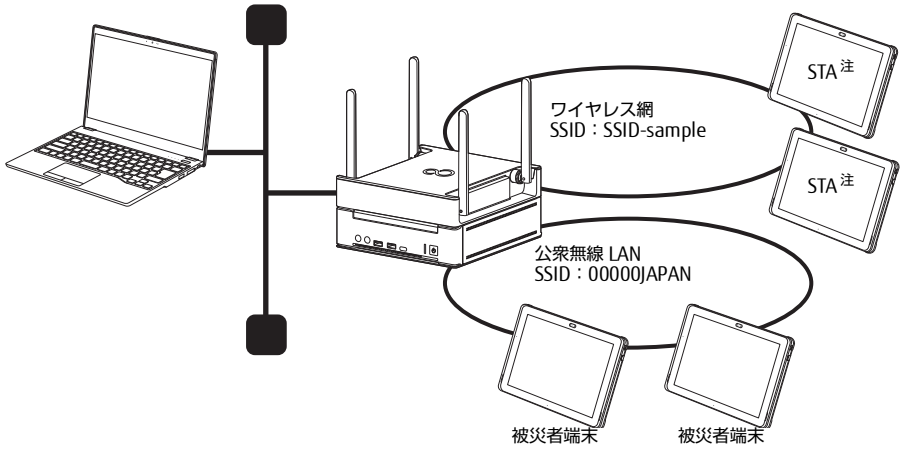


2「同一 SSID 内の通信禁止」と「異なる SSID 間の通信禁止」を「有効」に設定して、「適用」をクリックします。



緊急モード

大規模災害発生時に公衆無線 LAN を無料開放することができます。
「公衆無線 LAN の無料開放に関するガイドライン」に基づき SSID などの初期設定は完了しています。
必要に応じて SSID 名の変更が可能です。



注： ワイヤレス網内のタブレットなどの端末

■緊急モードを起動する

1「詳細設定」→「ネットワーク」→「無線」→「緊急モード」の順にクリックします。

2「緊急モード」で「有効」にチェックを付け、「周波数帯」を「2.4GHz/5GHz」「2.4GHz」「5GHz」の中から選択し、「適用」をクリックします。

重要

▸緊急モードにてMACフィルタを有効にした場合、接続を希望する端末のMACフィルタリストを別途登録する必要があります。

インストール補助ツールを使用する （初期設定）

「インストール補助ツール」（→ P.23）は、本製品に添付されておりません。「インストール補助ツール」を使用する場合は、「インストール補助ツールとインターネットキャッシュ機能 V3.0.0 用アップデートモジュールのダウンロード」（→ P.28）をご覧になり、ダウンロードしてください。

ダウンロード後、「01_BasicFunction_BaseAPP_Install.cmd」を実行して本製品を再起動した後、「02_BasicFunction_BaseAPP_Install.cmd」を実行してください。なお、バッチファイルは、必ず、管理者権限のアカウントで実行してください。次のインストールと設定が自動で行われます。

「エクスプローラーの設定」（→ P.62）～「メンテナンス機能各種サービスの追加」（→ P.83）

バッチファイルの実行が完了したら、本製品を再起動して、「管理画面の初期パスワード変更」（→ P.84）からインストールと設定を進めてください。
なお、「インストール補助ツール」を使用しない場合は、本マニュアルに沿ってインストールと設定を行ってください。

基本アプリのインストールと設定

基本アプリについて

次のアプリは、本製品ですべての機能が動作するために必要な基本となるアプリです。本製品を使用するためには、このアプリを必ずインストールして設定する必要があります。

- cygwin
- Open Java Development Kit

基本アプリは、本製品のストレージに添付されています（→ P.23）。アプリのインストールや設定は、必ず、管理者権限のアカウントで行ってください。

エクスプローラーの設定

エクスプローラーで、隠しファイルやフォルダー、拡張子を表示します。

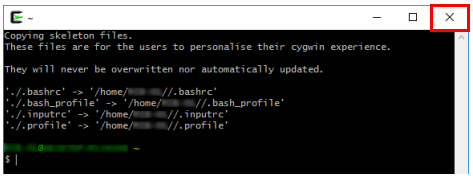
1. **「スタート」→「Windows システムツール」→「エクスプローラー」の順にクリックします。**
   エクスプローラーが起動します。
2. **「表示」をクリックし、「隠しファイル」と「ファイル名拡張子」にチェックを付けます。**

cygwin64 フォルダーの配置

1. **「C:¥cygwin64」を作成します。**
2. **「C:¥Fujitsu¥Software¥InternetCache¥cygwin64」内のすべてのファイルとフォルダーを「C:¥cygwin64」にコピーします。**
3. **フォルダーとファイルの構成が次のようになっていることを確認します。**

フォルダーとファイルの構成	
C:¥cygwin64¥	bin
	cacheUI
	dev
	etc
	home
	lib
	opt
	sbin
	squid
	squidcontroller
	tmp
	usr
	var
	Cygwin.bat
	Cygwin.ico
	Cygwin64 Terminal
	Cygwin-Terminal.ico

4. **「C:¥cygwin64¥Cygwin64 Terminal」を実行します。**
   Terminal が起動した後、コマンドラインが入力可能な状態になります。
5. **閉じるボタン（ × ）をクリックし、画面を閉じます。**



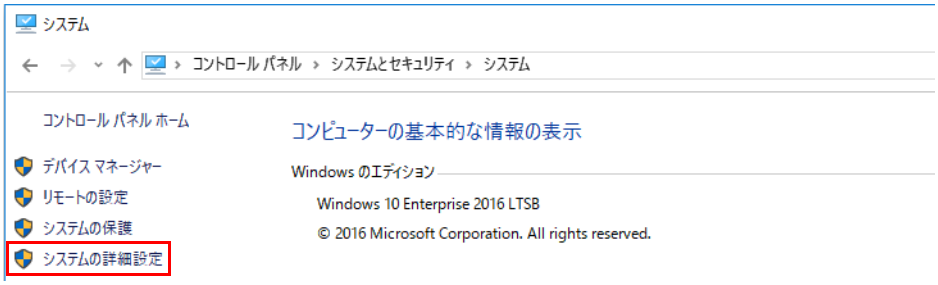
6. **「C:¥cygwin64¥home」に、Windows にログインしたときのユーザーフォルダーが作成されていることを確認します。**

cygwin64 フォルダーの環境変数設定

1「コントロールパネル」を表示します（→ P.7）。
「コントロールパネル」が表示されます。

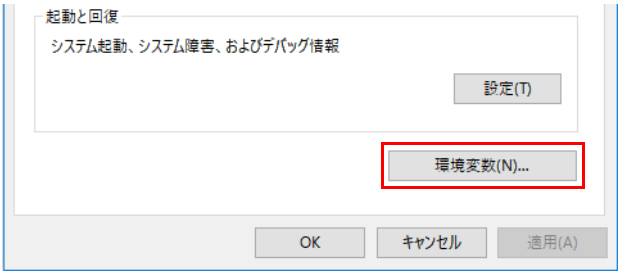
2「システムとセキュリティ」→「システム」の順にクリックします。

3「システムの詳細設定」をクリックします。



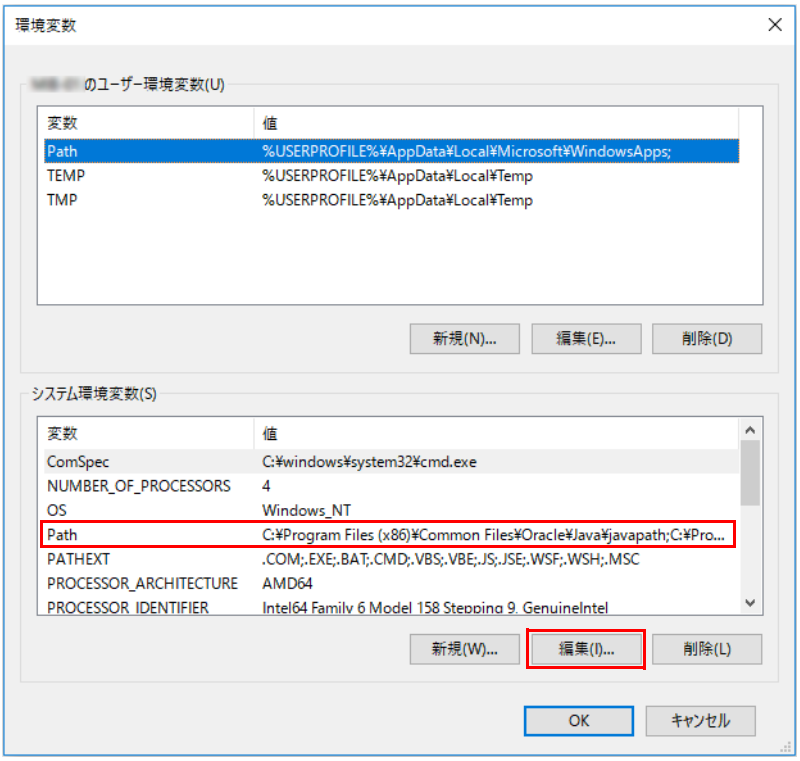
「システムのプロパティ」が表示されます。

4「環境変数」をクリックします。



「環境変数」が表示されます。

5「システム環境変数」の「Path」をクリックし、「編集」をクリックします。

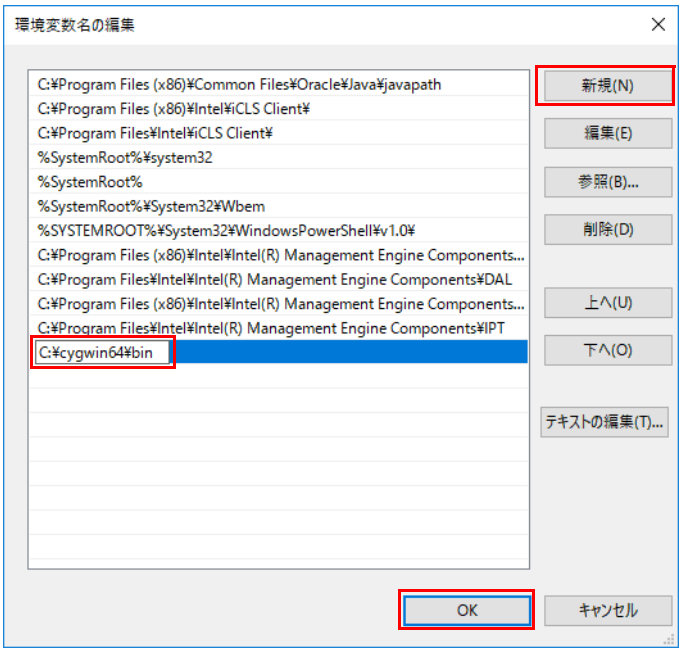


「環境変数名の編集」が表示されます。

6 「新規」をクリックし、最終行に表示されたテキストボックスに「C:¥cygwin64¥bin」を入力し、「OK」をクリックします。

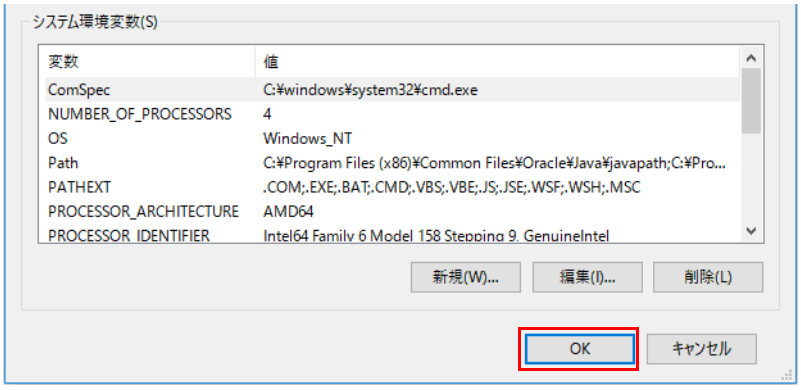
POINT

▸「C:¥cygwin64¥bin」の優先順位を「%SystemRoot%¥System32」より上にしないでください。アプリのインストールが失敗します。



「環境変数」が表示されます。

7 「OK」をクリックします。



Open Java Development Kit のインストール

本製品に OpenJDK をインストールします。

1 次のフォルダーを作成します。

C:¥Program Files¥Java¥jdk8u-jre

2 「C:¥Fujitsu¥Software¥Java」フォルダー内のすべてのフォルダーとファイルを手順 1 で作成した「jdk8u-jre」フォルダーに格納します。

POINT

▸「このフォルダーへコピーするには管理者権限が必要です」と表示された場合は、「続行」をクリックします。

3 フォルダーとファイルの構成が次のようになっていることを確認します。

フォルダーとファイルの構成	
C:¥Program Files¥Java¥jdk8u-jre¥	bin
	lib
	ASSEMBLY_EXCEPTION
	LICENSE
	openj9-notices.html
	openj9-openjdk-notices
	release
	THIRD_PARTY_README

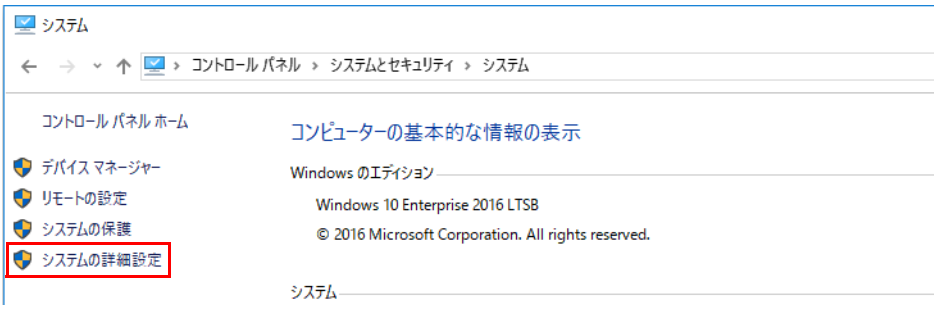
Open Java Development Kit の環境変数設定

OpenJDK の環境変数を設定します。

1 「コントロールパネル」を表示します（→ P.7）。
「コントロールパネル」が表示されます。

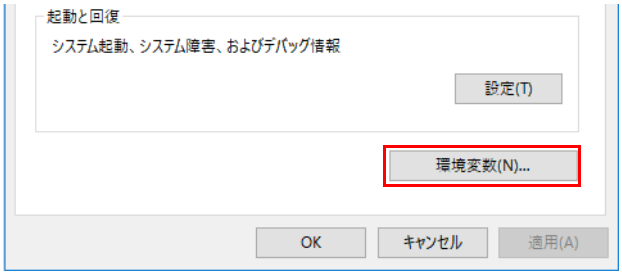
2 「システムとセキュリティ」→「システム」の順にクリックします。

3 「システムの詳細設定」をクリックします。



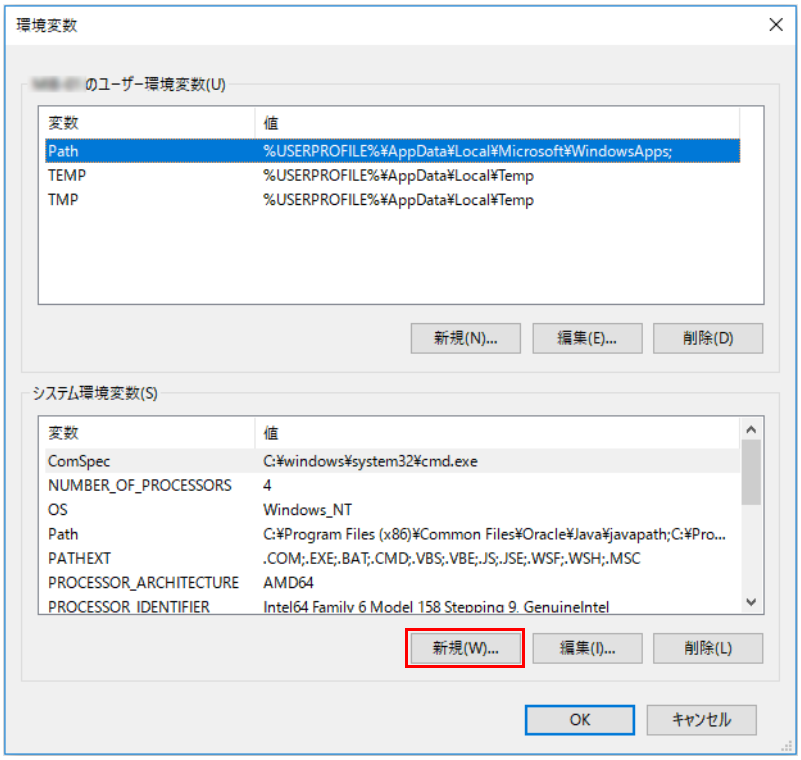
「システムのプロパティ」が表示されます。

4 「環境変数」をクリックします。



「環境変数」が表示されます。

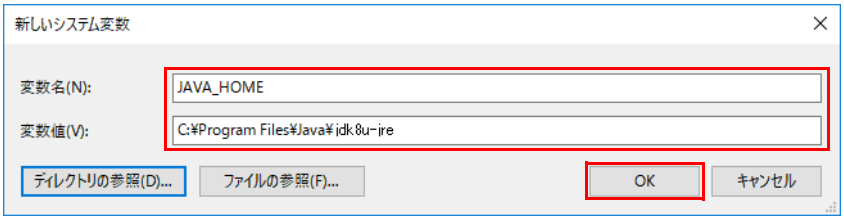
5 「システム環境変数」の「新規」をクリックします。



「新しいシステム変数」が表示されます。

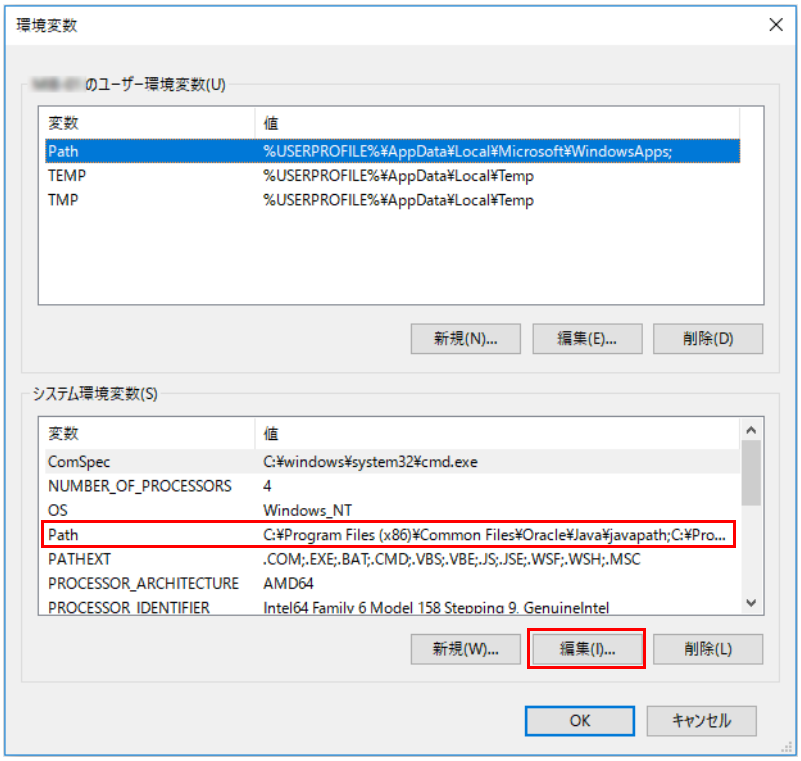
6 変数名と変数値に次の値を入力し、「OK」をクリックします。

変数名：「JAVA_HOME」
変数値：「C:¥Program Files¥Java¥jdk8u-jre」



「環境変数」が表示されます。

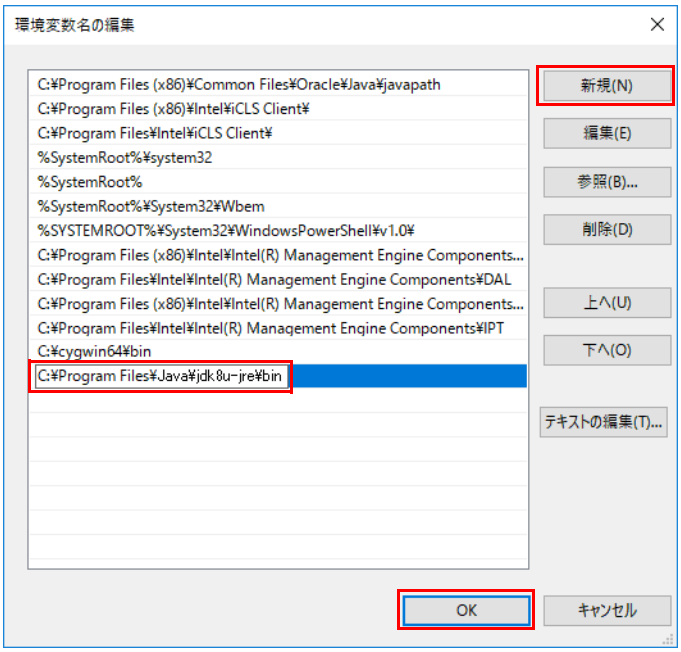
7 「システム環境変数」の「Path」をクリックし、「編集」をクリックします。



「環境変数名の編集」が表示されます。

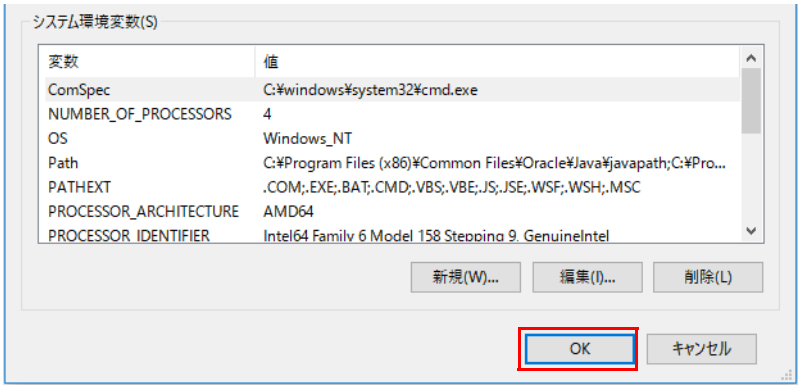
8「新規」をクリックし、最後行に表示されたテキストボックスに次のフォルダーのパスを入力し、「OK」をクリックします。

「C:¥Program Files¥Java¥jdk8u-jre¥bin」



「環境変数」が表示されます。

9「OK」をクリックします。



10「OK」をクリックします。

メンテナンス機能のフォルダーの配置

1「C:¥SmartMaintenance」フォルダーを作成します。

2「C:¥Fujitsu¥Software¥SmartMaintenance」内のすべてのファイルとフォルダーを「C:¥SmartMaintenance」にコピーします。

3 フォルダーとファイルの構成が次のようになっていることを確認します。

フォルダーとファイルの構成	
C:¥SmartMaintenance¥	bat
	Batch
	ElasticSearch
	Java
	Logstash
	Management
	nginx
	OSS
	Other
	mib.ini

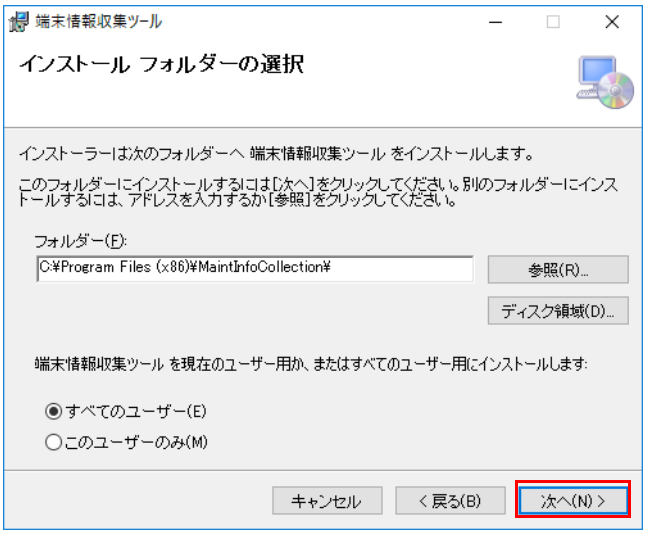
端末情報収集ツールのインストール

本製品に端末情報収集ツールのインストールと設定を行います。

1 **「C:¥SmartMaintenance¥Other¥ 端末情報収集ツール ¥TerminalInfoAppSetup.msi」を起動します。**
「セットアップ ウィザード」が表示されます。

2 **「次へ」をクリックします。**
「インストール フォルダーの選択」が表示されます。

3 **「すべてのユーザー」を選択し、「次へ」をクリックします。**



「インストールの確認」が表示されます。

4 **「次へ」をクリックします。**
インストールが開始します。

POINT
▸「ユーザーアカウント制御」が表示された場合は、「はい」をクリックします。

5 **「閉じる」をクリックします。**

端末情報収集ツールの設定ファイルのコピー

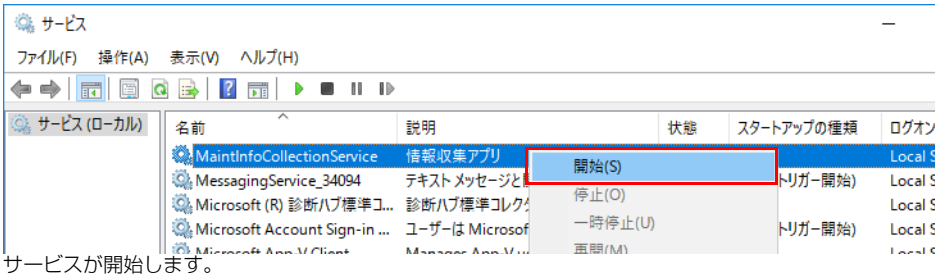
1 **「C:¥SmartMaintenance¥Other¥ 端末情報収集ツール ¥Server¥TerminalInfoAppSetting.ini」を「C:¥ProgramData¥FCCL¥MaintInfoCollection¥Ini」に上書きコピーします。**

POINT
▸「対象のフォルダーへのアクセスは拒否されました」というメッセージが表示される場合は、「続行」をクリックします。

端末情報収集ツールのサービスの起動

1 **「スタート」→「Windows 管理ツール」→「サービス」の順にクリックします。**
サービスが起動します。

2 **一覧から「MaintInfoCollectionService」の状態を確認し、実行中になっていない場合は、右クリックし「開始」をクリックします。**



サービスが開始します。

セキュリティ除外設定

セキュリティ対策ソフトをインストールしている場合は、お使いのセキュリティ対策ソフトによって本製品が正常に動作しない場合があります。セキュリティ対策ソフトのマニュアルをご覧になり、次のファイルをチェック対象から除外してください。

C:¥cygwin64¥squid¥sbin¥squid.exe
C:¥cygwin64¥squid¥bin¥squidclient.exe

ファイアウォールの設定

メンテナンス機能で使用するアプリやポートについて、ファイアウォール経由の通信を許可する設定を行います。ここでは、本製品に Windows ファイアウォールを設定する方法を説明します。

POINT

- 市販のセキュリティ対策ソフトをインストールしている場合は、セキュリティ対策ソフトのマニュアルをご覧になり、ファイアウォールの設定を行ってください。

●設定が必要なプログラム

通信許可設定が必要なアプリは、次のとおりです。「ドメイン」、「プライベート」、「パブリック」すべての接続で通信を許可してください。

プログラム	プログラムのパス	受信／送信
nginx.exe	C:¥SmartMaintenance¥nginx¥nginx.exe	受信
Open Java Development Kit	C:¥Program Files¥Java¥jdk8u-jre¥bin¥java.exe	受信

●設定が必要なポート

通信許可設定が必要なポートは、次のとおりです。「ドメイン」、「プライベート」、「パブリック」すべての接続で通信を許可してください。

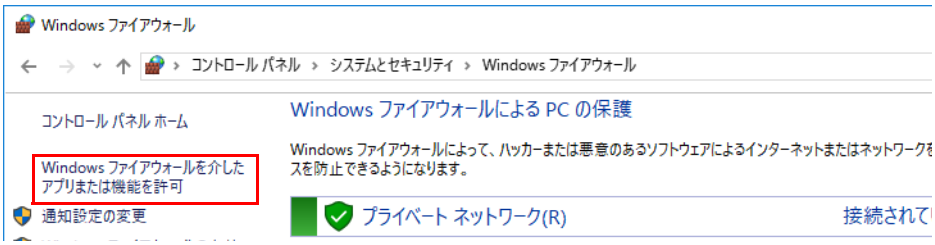
用途	プロトコル	ポート	設定対象のプログラムのパス	受信／送信
管理画面	TCP	10080	-	受信
Squid Cache Server	TCP	8080	C:¥cygwin64¥squid¥sbin¥squid.exe	受信
Squid ICP	TCP	3130	C:¥cygwin64¥squid¥sbin¥squid.exe	受信

nginx.exe の許可設定

1 「コントロールパネル」を表示します（→ P.7）。

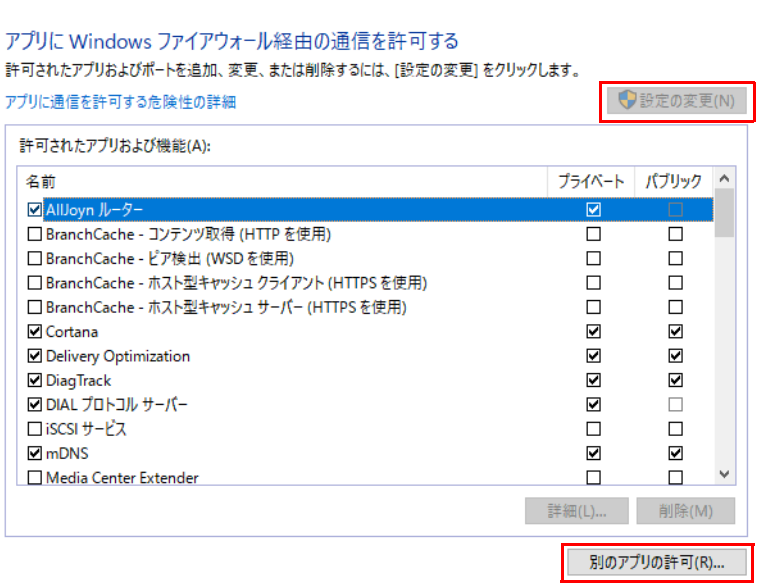
「コントロールパネル」が表示されます。

2 「システムとセキュリティ」→「Windows　ファイアウォール」→「Windows　ファイアウォールを介したアプリまたは機能を許可」の順にクリックします。



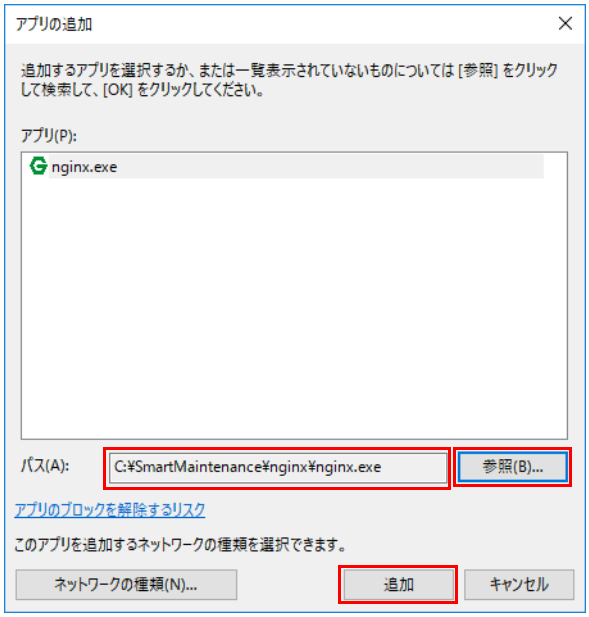
「アプリに Windows ファイアウォール経由の通信を許可する」が表示されます。

3 「設定の変更」をクリックし、「別のアプリの許可」をクリックします。



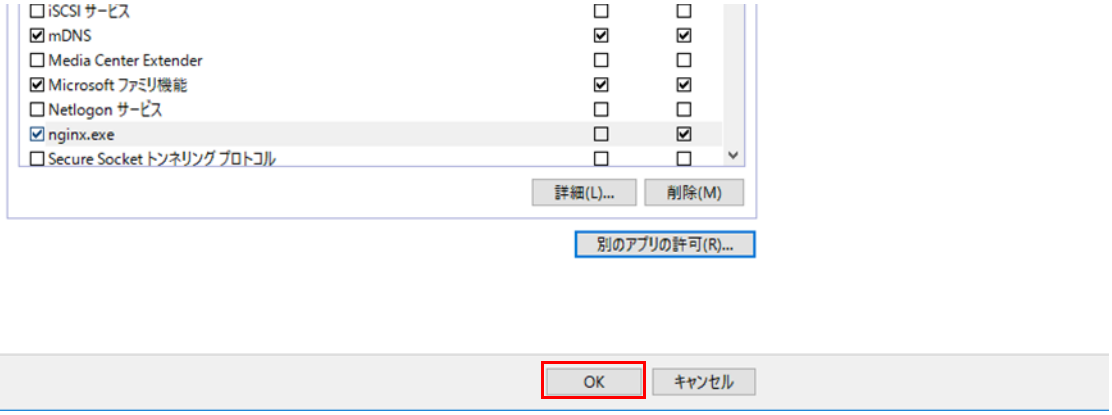
「アプリの追加」が表示されます。

4「参照」をクリックした後、「C:¥SmartMaintenance¥nginx¥nginx.exe」を指定し、「追加」をクリックします。



「アプリに Windows ファイアウォール経由の通信を許可する」が表示されます。

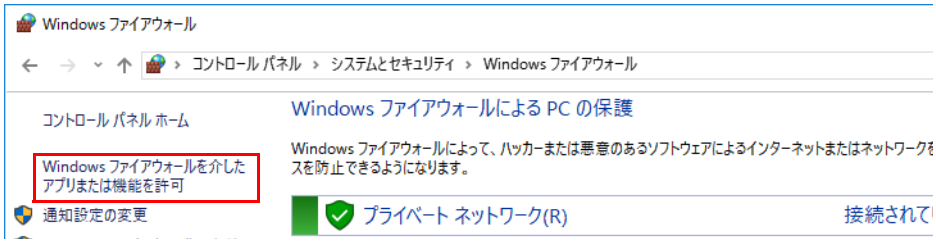
5「OK」をクリックします。



管理画面の許可設定

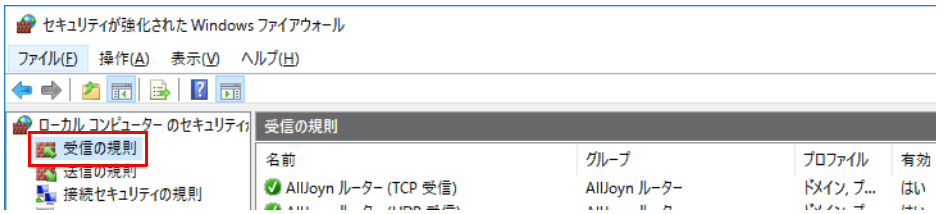
1「コントロールパネル」を表示します（→ P.7）。
「コントロールパネル」が表示されます。

2「システムとセキュリティ」→「Windows ファイアウォール」→「詳細設定」の順にクリックします。

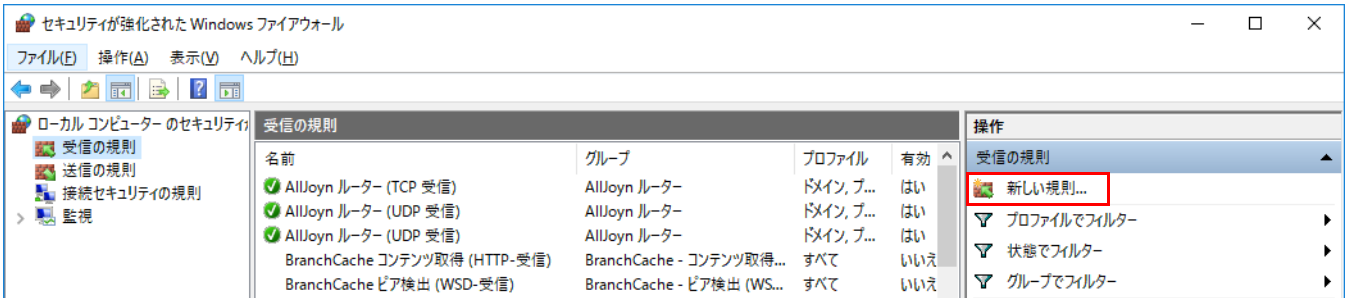


「アプリに Windows ファイアウォール経由の通信を許可する」が表示されます。

3「受信の規則」をクリックします。

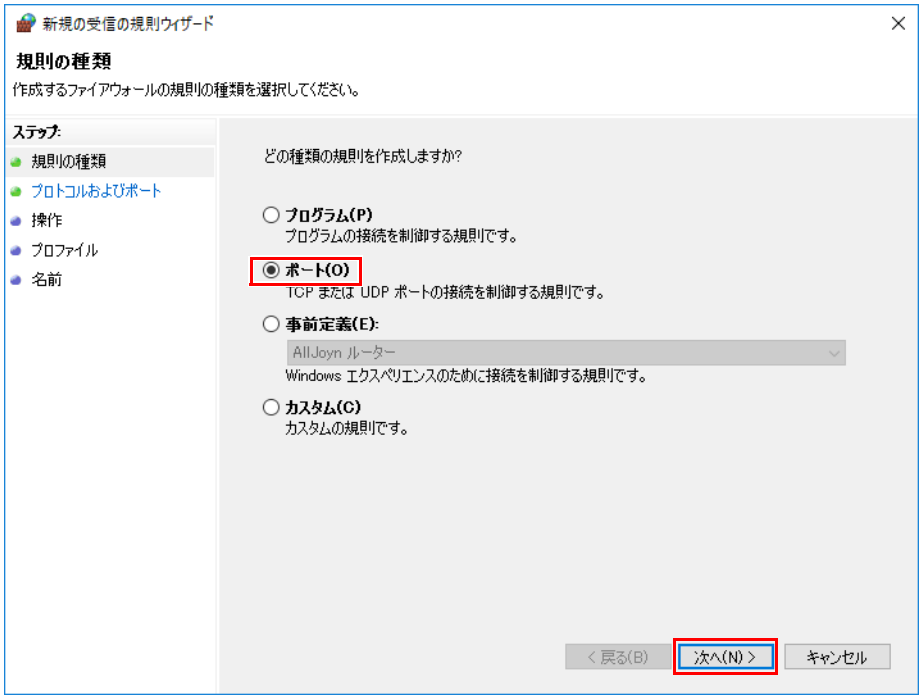


4 画面右側の「新しい規則 ...」をクリックします。



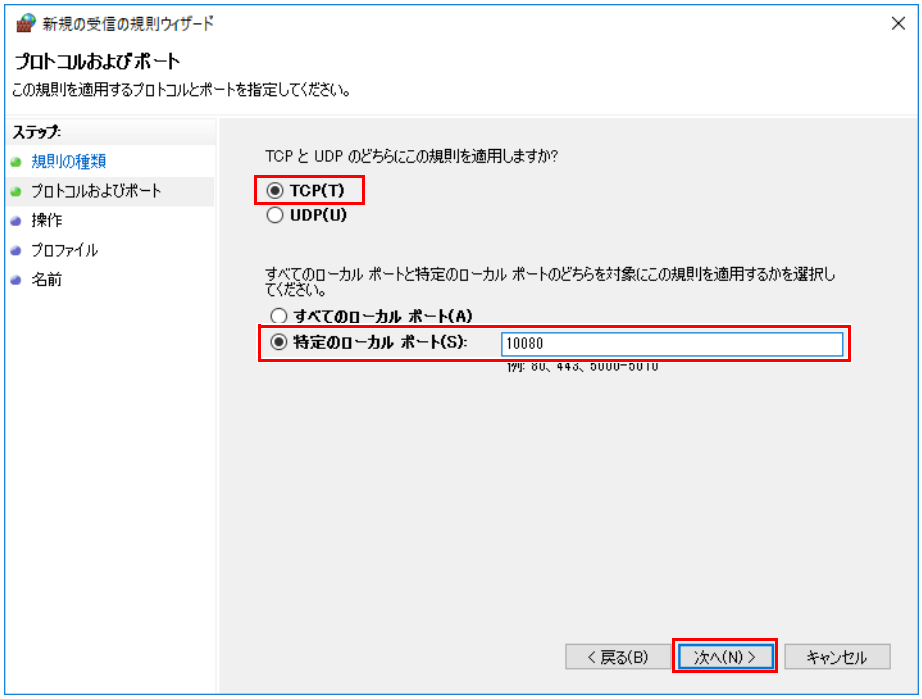
「規則の種類」が表示されます。

5「ポート」を選択し、「次へ」をクリックします。



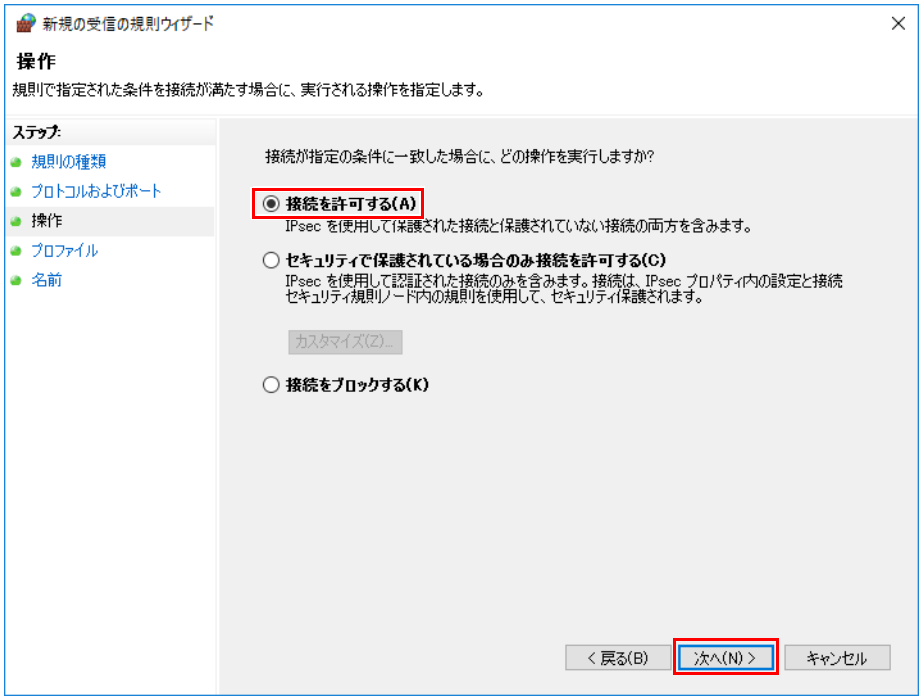
「プロトコルおよびポート」が表示されます。

6　プロトコルを「TCP」に設定し、ポートを「特定のローカルポート」に設定して「10080」を入力した後、「次へ」をクリックします。



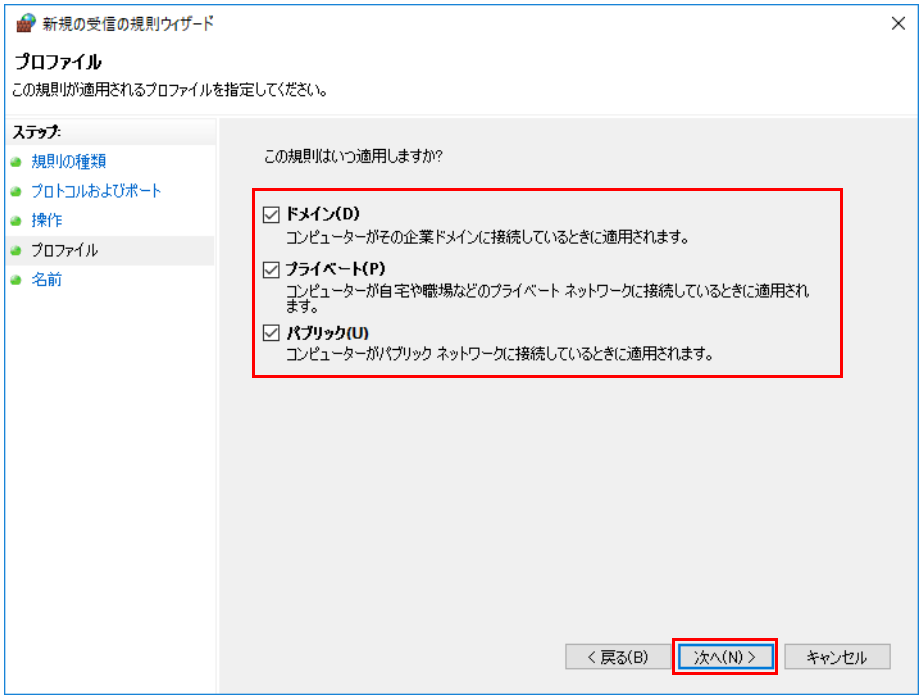
「操作」が表示されます。

7「接続を許可する」を選択し、「次へ」をクリックします。



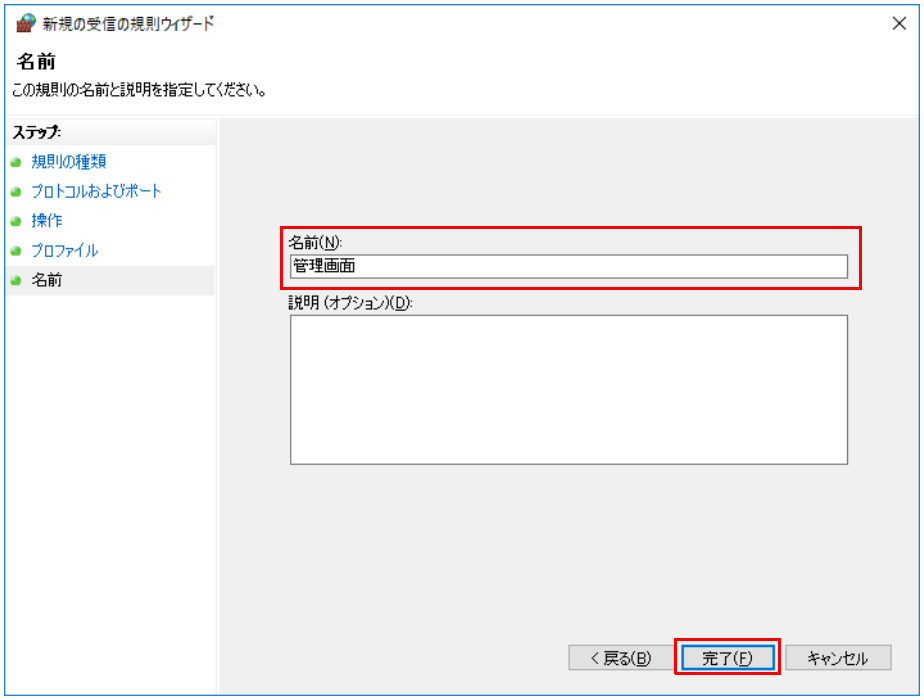
「プロファイル」画面が表示されます。

8「ドメイン」、「プライベート」、「パブリック」すべてにチェックを付け、「次へ」をクリックします。



「名前」が表示されます。

9「名前」に「管理画面」を入力し、「完了」をクリックします。



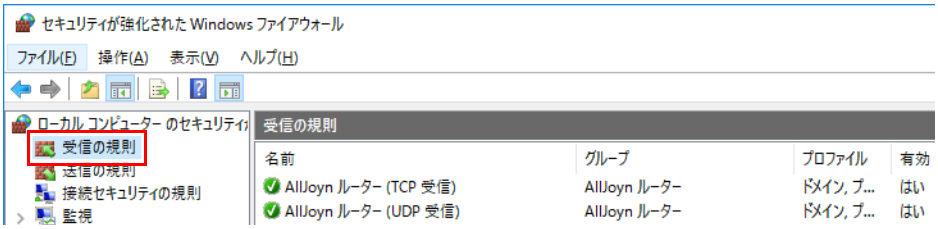
「セキュリティが強化された Windows ファイアウォール」が表示されます。

Squid Cache Server の許可設定

1「コントロールパネル」を表示します（→ P.7）。
「コントロールパネル」が表示されます。

2「システムとセキュリティ」→「Windows ファイアウォール」→「詳細設定」の順にクリックします。
「セキュリティが強化された Windows ファイアウォール」が表示されます。

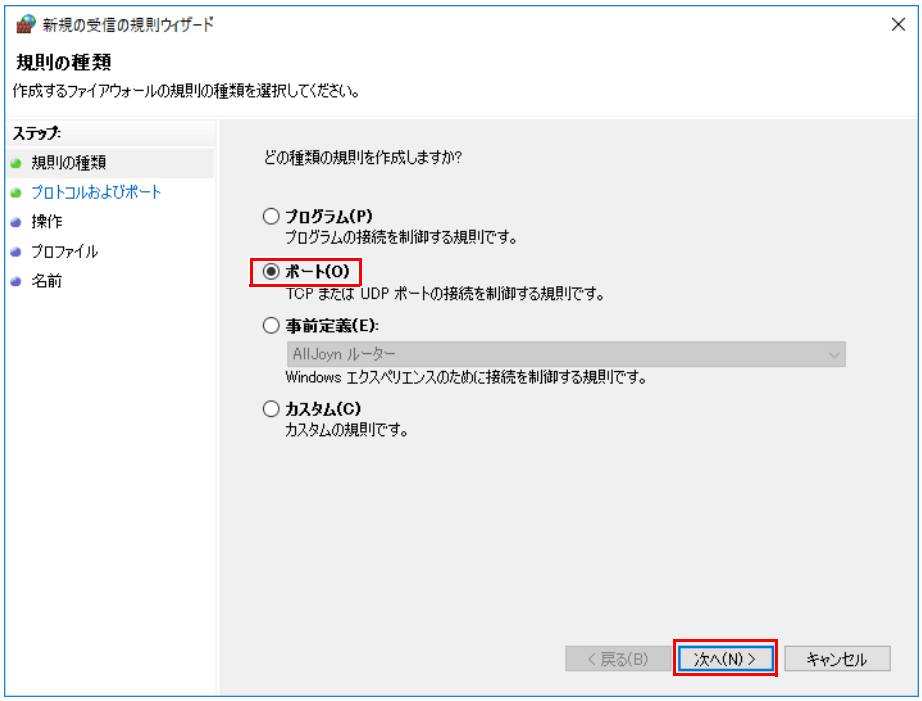
3「受信の規則」をクリックします。



4 画面右側の「新しい規則 ...」をクリックします。

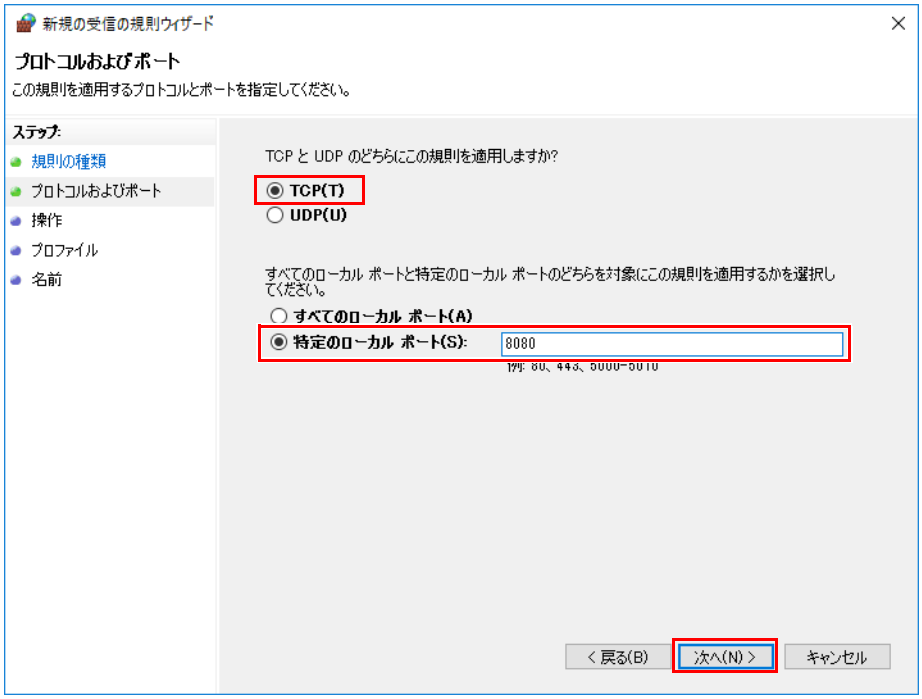
「規則の種類」が表示されます。

5「ポート」を選択し、「次へ」をクリックします。



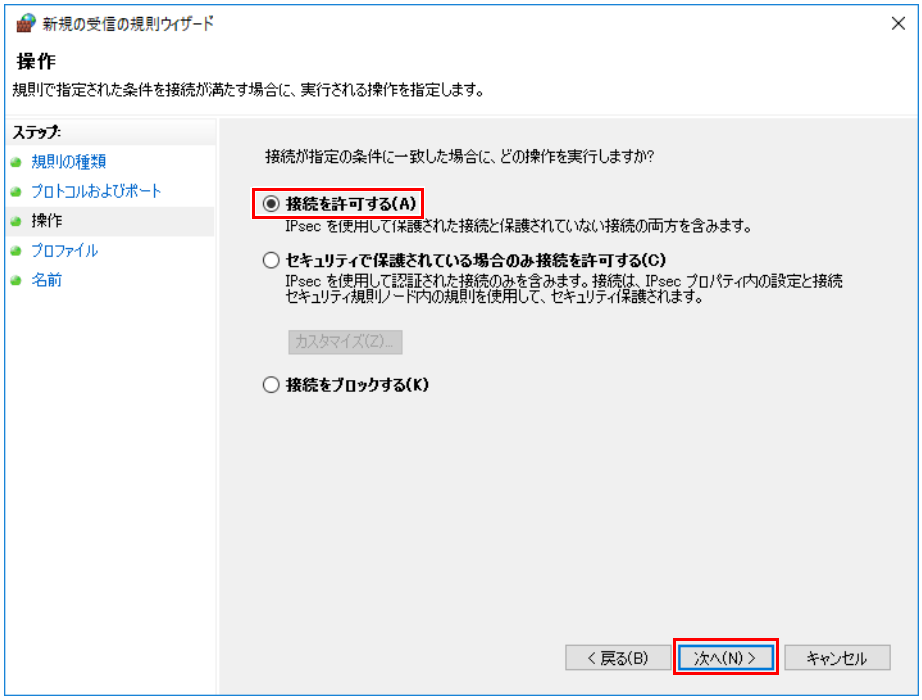
「プロトコルおよびポート」が表示されます。

6 プロトコルを「TCP」に設定し、ポートを「特定のローカルポート」に設定して「8080」を入力した後、「次へ」をクリックします。



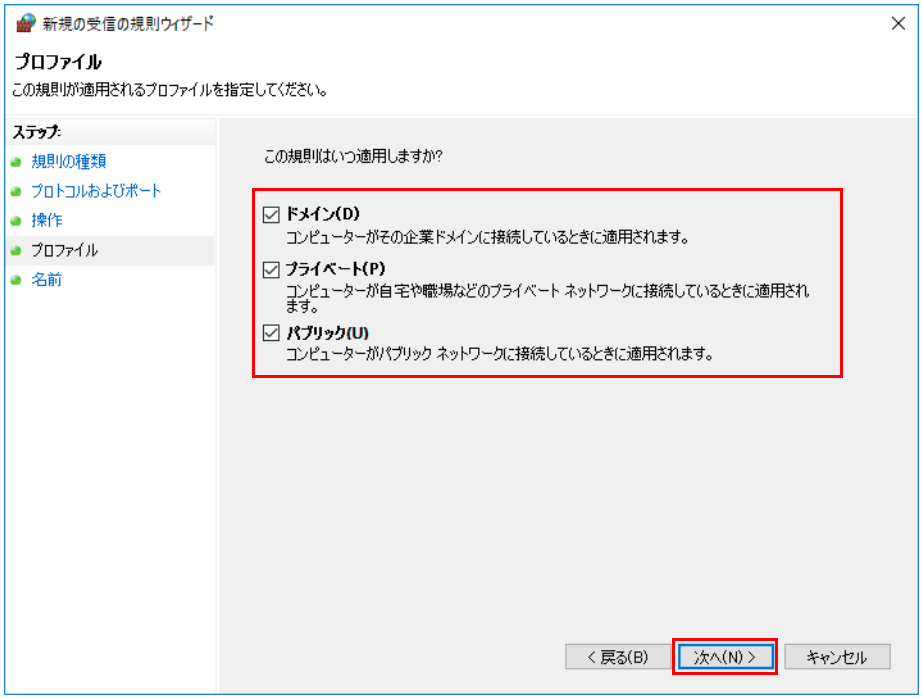
「操作」が表示されます。

7「接続を許可する」を選択し、「次へ」をクリックします。



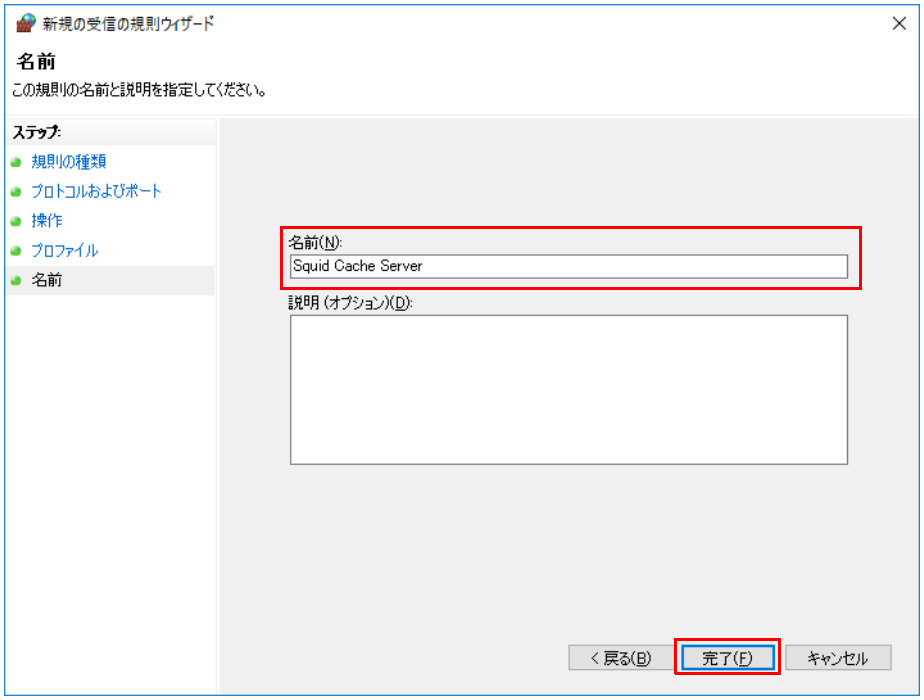
「プロファイル」画面が表示されます。

8「ドメイン」、「プライベート」、「パブリック」すべてにチェックを付け、「次へ」をクリックします。



「名前」が表示されます。

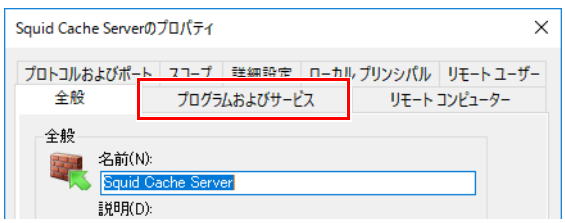
9「名前」に「Squid Cache Server」を入力し、「完了」をクリックします。



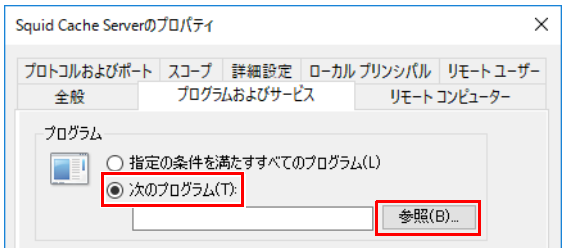
「セキュリティが強化された Windows ファイアウォール」が表示されます。

10「Squid Cache Server」を右クリックし、「プロパティ」をクリックします。
「Squid Cache Server のプロパティ」が表示されます。

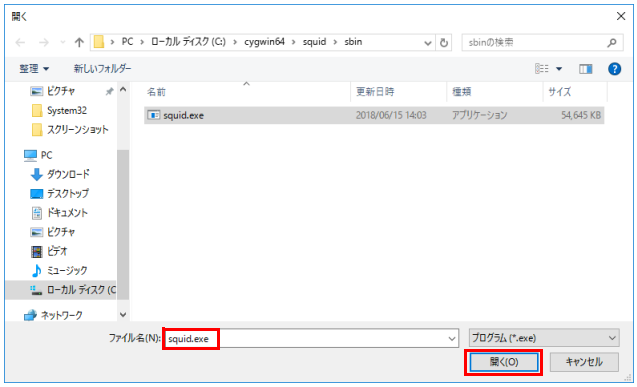
11「プログラムおよびサービス」タブをクリックします。



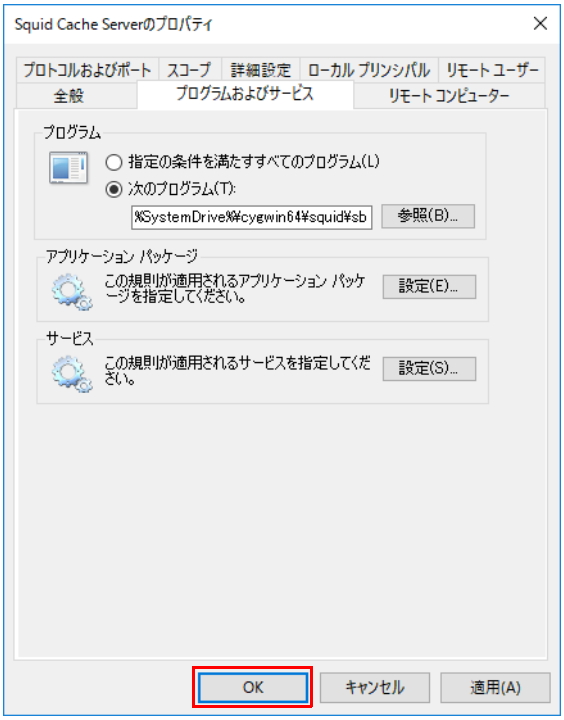
12「次のプログラム」を選択し、「参照」をクリックします。



13「C:¥cygwin64¥squid¥sbin¥squid.exe」を選択し、「開く」をクリックします。



14「OK」をクリックします。

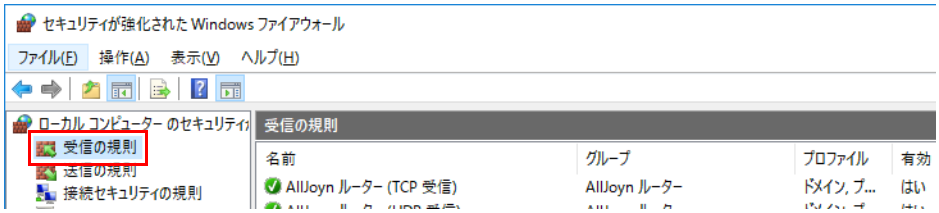


Squid ICP の許可設定

1「コントロールパネル」を表示します（→ P.7）。
「コントロールパネル」が表示されます。

2「システムとセキュリティ」→「Windows ファイアウォール」→「詳細設定」の順にクリックします。
「セキュリティが強化された Windows ファイアウォール」が表示されます。

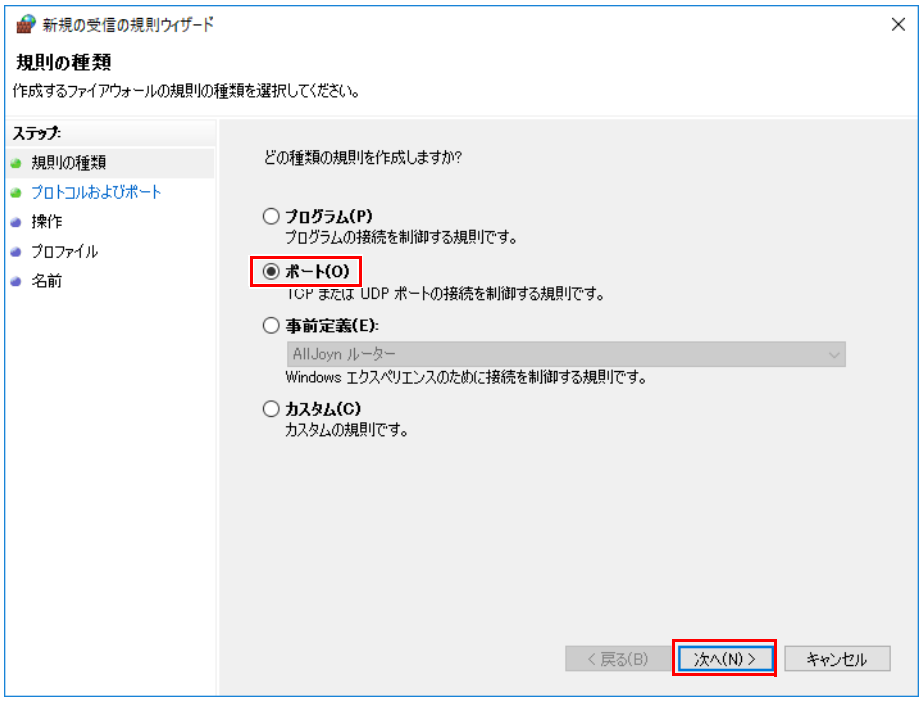
3「受信の規則」をクリックします。



4 画面右側の「新しい規則 ...」をクリックします。

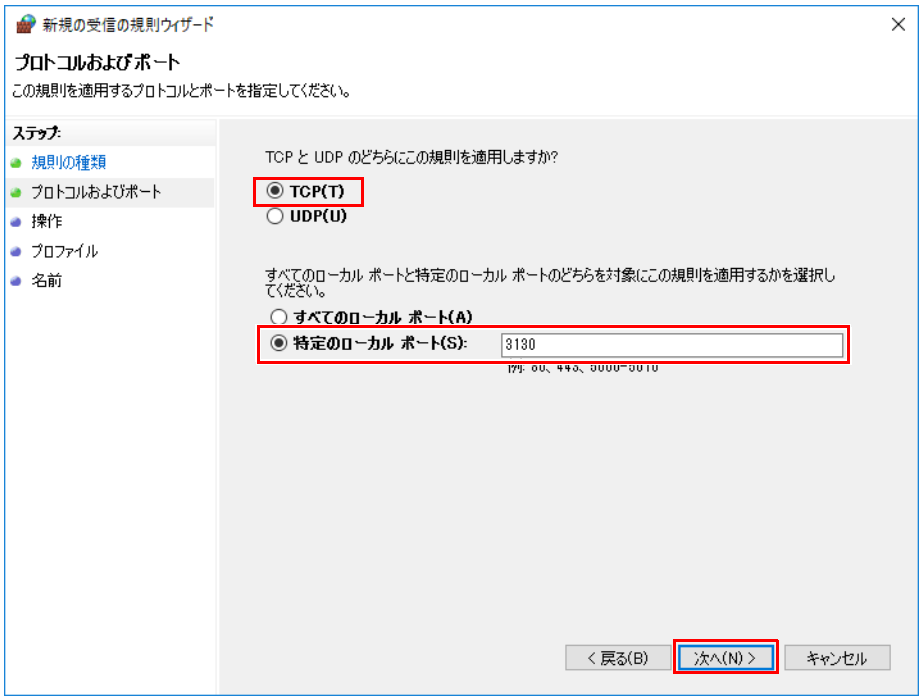
「規則の種類」が表示されます。

5「ポート」を選択し、「次へ」をクリックします。



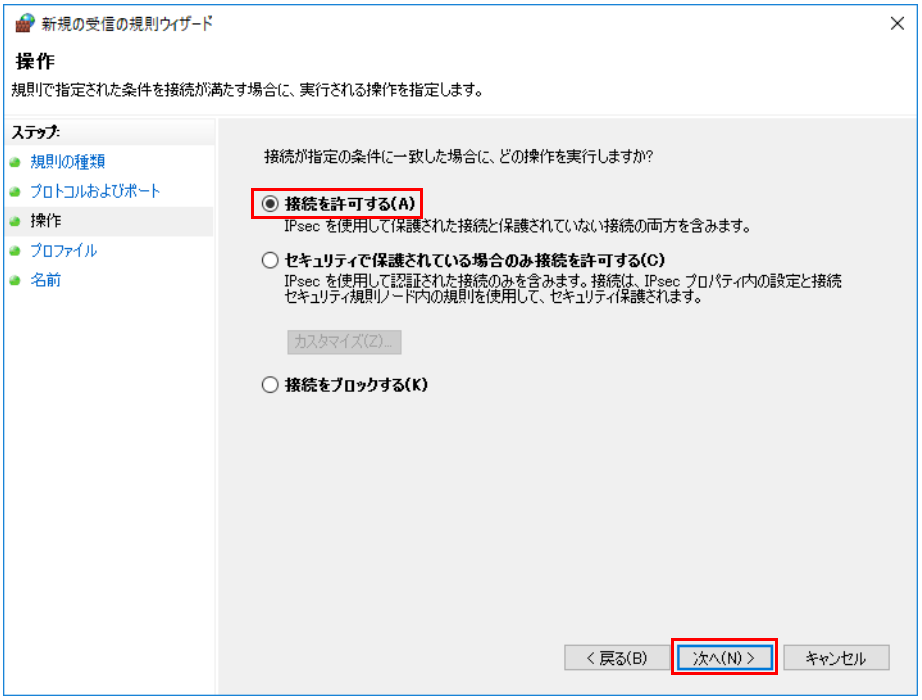
「プロトコルおよびポート」が表示されます。

6 プロトコルを「TCP」に設定し、ポートを「特定のローカルポート」に設定して「3130」を入力した後、「次へ」をクリックします。



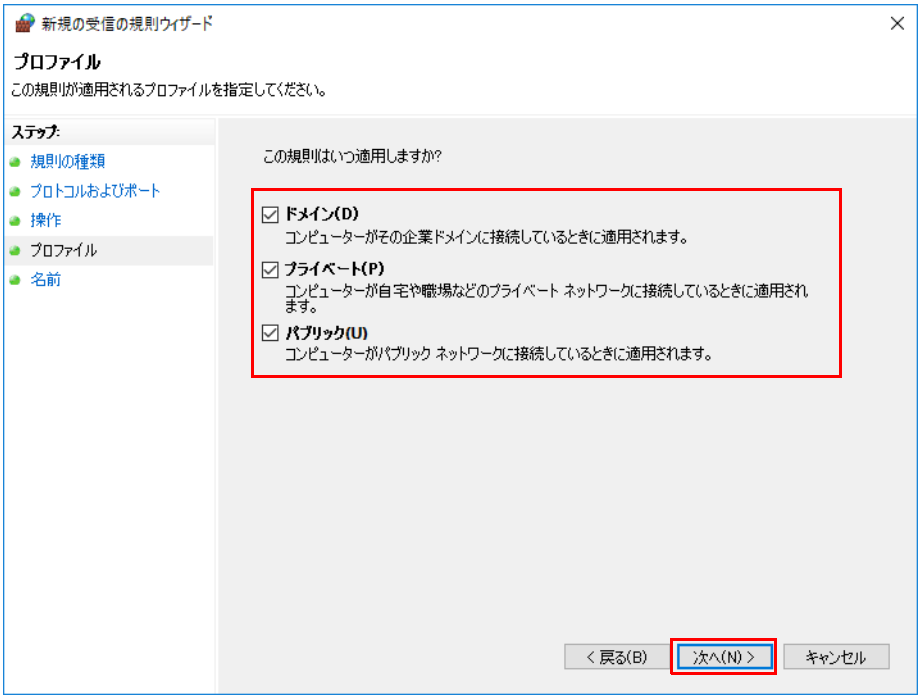
「操作」が表示されます。

7「接続を許可する」を選択し、「次へ」をクリックします。



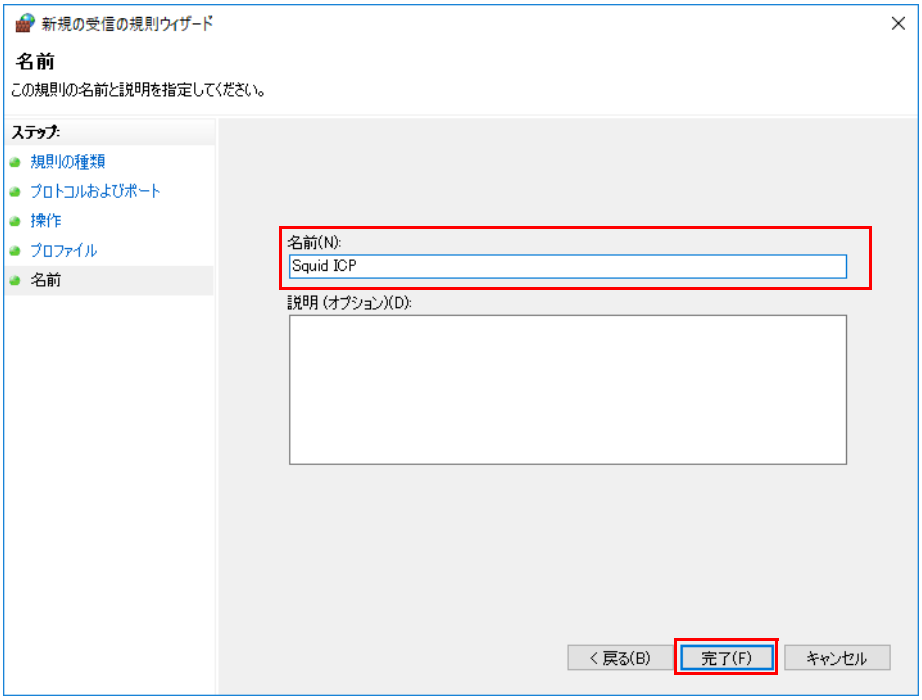
「プロファイル」画面が表示されます。

8「ドメイン」、「プライベート」、「パブリック」すべてにチェックを付け、「次へ」をクリックします。



「名前」が表示されます。

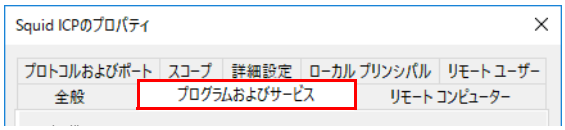
9「名前」に「Squid ICP」を入力し、「完了」をクリックします。



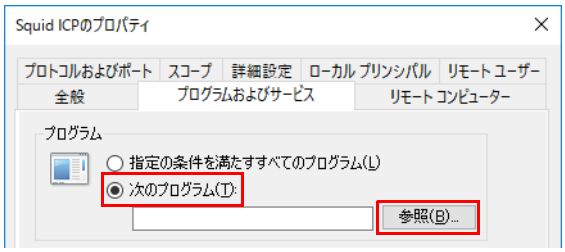
「セキュリティが強化された Windows ファイアウォール」が表示されます。

10「Squid ICP」を右クリックし、「プロパティ」をクリックします。
「Squid ICP のプロパティ」が表示されます。

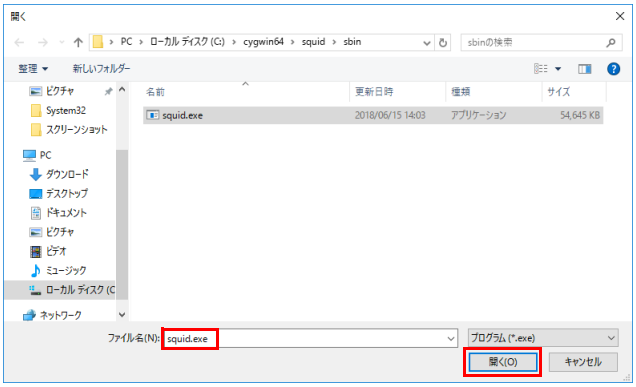
11「プログラムおよびサービス」タブをクリックします。



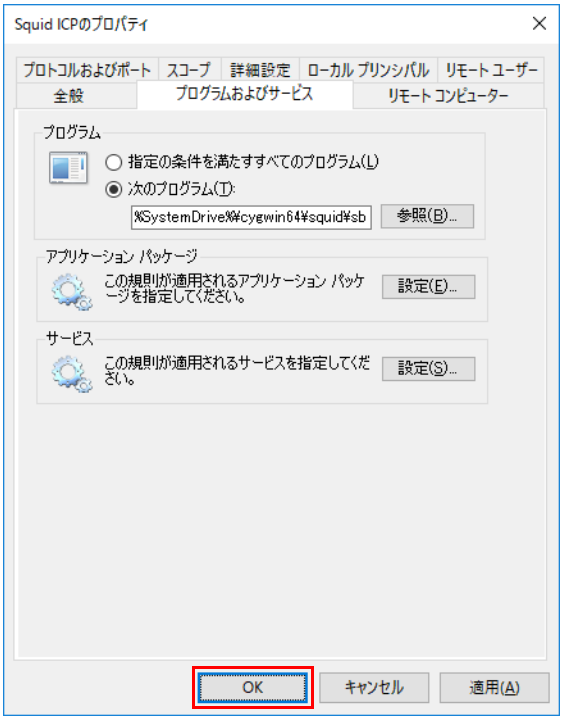
12「次のプログラム」を選択し、「参照」をクリックします。



13「C:¥cygwin64¥squid¥sbin¥squid.exe」を選択し、「開く」をクリックします。



14「OK」をクリックします。



メンテナンス機能の設定ファイル変更

config.ini 設定ファイルの変更

1　テキストエディターで「C:¥SmartMaintenance¥Batch¥config.ini」を開き、設定ファイルを変更します。
※IP アドレスには、本製品のコンピューター部分の固定 IP アドレスを入力します。

hostAddress = IPアドレス

```
[common]
; ### API のポート番号 (Server 用 )
serverPortNumber = 10080
; ### この PC の IP アドレス
hostAddress = x.x.x.x
```

コンピューター部分の固定 IP アドレスを入力してください。

2　ファイルを保存して閉じます。

POINT
▸「対象のフォルダーへのアクセスは拒否されました」というメッセージが表示される場合は、「続行」をクリックします。

mib.ini 設定ファイルの変更

1　テキストエディターで「C:¥SmartMaintenance¥mib.ini」を開き、[cacheService] セクションの url の記載を次のように変更します。
※「x.x.x.x」には、本製品のコンピューター部分の固定 IP アドレスを入力します。

url = http://IPアドレス:10080/squid/

```
[cacheService]
url = http://x.x.x.x:10080/squid/
backupPath = cache
restorePath = cache
sleepSecond = 1
```

コンピューター部分の固定 IP アドレスを入力してください。

2　ファイルを保存して閉じます。

3　「C:¥tmp¥mib.ini」がある場合は、「C:¥SmartMaintenance¥mib.ini」を上書きコピーします。

nginx 設定ファイル変更

nginx 設定ファイルを変更します。設定ファイルを変更するときは、テキストエディターを使用してください。

1　テキストエディターで「C:¥SmartMaintenance¥nginx¥conf¥nginx.conf」を開き、設定ファイルを変更します。

重要
▸下図のIPアドレスの設定箇所をすべて変更してください。変更しない場合、セットアップ中にエラーが発生します。

※「x.x.x.x」には、本製品のコンピューター部分の固定 IP アドレスを入力します。

```
#*****IP アドレス設定箇所 *****
location / {
   proxy_pass  http://x.x.x.x:18081/;
}

location /maintenance/ {
   proxy_pass  http://x.x.x.x:18080/;
}

location /squid/ {
   proxy_pass  http://x.x.x.x:3000/;
}

location /aplcache/ {
   proxy_pass  http://x.x.x.x:3002/;
}

location /aplcacheui/ {
   proxy_pass  http://x.x.x.x:3003/;
}

location /security/ {
   proxy_pass  http://x.x.x.x:3010/;
}

location /nodejs/ {
   proxy_pass  http://x.x.x.x:3001/;
}

#error_page  404          /404.html;
```

コンピューター部分の固定 IP アドレスを入力してください。
コンピューター部分の固定 IP アドレスを入力してください。
コンピューター部分の固定 IP アドレスを入力してください。
コンピューター部分の固定 IP アドレスを入力してください。
コンピューター部分の固定 IP アドレスを入力してください。
コンピューター部分の固定 IP アドレスを入力してください。
コンピューター部分の固定 IP アドレスを入力してください。

2　ファイルを保存して閉じます。

POINT
▸「対象のフォルダーへのアクセスは拒否されました」というメッセージが表示される場合は、「続行」をクリックします。

メンテナンス機能各種サービスの追加

1 **管理者権限でコマンドプロンプトを起動します（→ P.7）。**

2 **次のコマンドを入力し、【Enter】キーを押します。**
cd C:¥SmartMaintenance¥Other
「C:¥SmartMaintenance¥Other」フォルダーへ移動します。

3 **「setup.bat」を入力し、【Enter】キーを押します。**
「セットアップ処理を終了します」メッセージが表示されたら、サービスの設定は完了です。

4 **「スタート」→「Windows 管理ツール」→「サービス」の順にクリックします。**
サービスが起動します。

5 **サービスの一覧に次のサービスが存在することを確認します。**

サービス名
Elasticsearch 5.5.0（elasticsearch-service-x64）
LogstashService
PortalAppService
SmartMaintBatteryBatService
SmartMaintDeleteBatService
SmartMaintMailBatService
SmartMaintSystemuptimeBatService
SmartMaintWebAppService
SmartMaintWirelesslanBatService
NginxService

POINT

▸サービスをいったん削除したい場合は、「C:¥SmartMaintenance¥Other¥servicedelete.bat」を実行してください。

管理画面の初期パスワード変更

管理画面へのログイン

本製品上で「管理画面」にログインします。

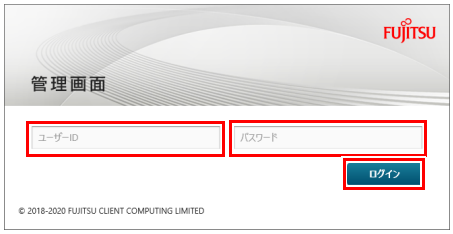
1　ブラウザーを起動し、管理画面の URL（http://IP アドレス :10080/）に接続します。

POINT

- IPアドレスにはコンピューター部分のIPアドレスをお使いください。
  コンピューター部分のIPアドレスが「192.168.1.3」の場合は次のようになります。
  http://192.168.1.3:10080/
- Internet Explorer で管理画面を表示したときに入力フォームが表示されない場合は、次の設定をご確認ください。
  1.Internet Explorer を起動します。
  2.画面右上のツールアイコン（設定）→「互換表示設定」の順にクリックします。
  「互換性設定の変更」が表示されます。
  3.「イントラネットサイトを互換表示で表示する」のチェックを外します。

ログイン画面が表示されます。

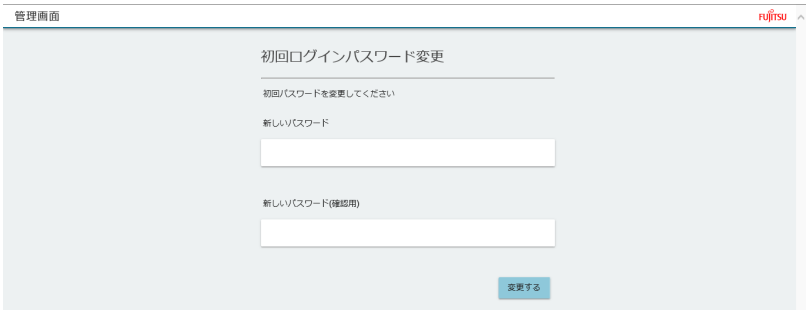
2　ユーザー ID およびパスワードを入力し、「ログイン」をクリックします。
ユーザー ID の初期値は「administrator」、パスワードの初期値は「administrator」です。



「初回ログインパスワード変更」が表示されます。

パスワードの変更

1　ユーザー ID「administrator」の「新しいパスワード」と「新しいパスワード（確認用）」にパスワードを入力し、変更をクリックします。
パスワードは、8 文字以上 16 文字以下で設定してください。なお、変更したパスワードは、忘れないように大切に保管しておいてください。



POINT

- 初期ログインパスワードを変更後に、パスワードを変更したい場合は、次の操作を行ってください。なお、変更したパスワードは、忘れないように大切に保管しておいてください。
  1. 「管理画面設定」→「パスワード更新」の順にクリックします。
  2. パスワード更新に関する項目を入力し、「更新」をクリックします。

各項目については、次の表をご覧ください。

項目	説明
ユーザー名	現在ログインしているユーザーの名前が表示されます。
現在のパスワード	現在使っているパスワードを入力します。
新しいパスワード	新しいパスワードを、8 ～ 16 文字で入力します。
パスワード再入力	確認のため、「新しいパスワード」欄に入力したパスワードを入力します。

メンテナンス機能の設定

管理画面へのログイン

メンテナンス機能の設定を行う場合、本製品上で「管理画面」にログインします。

1　ブラウザーを起動し、管理画面の URL（http://IP アドレス :10080/）に接続します。

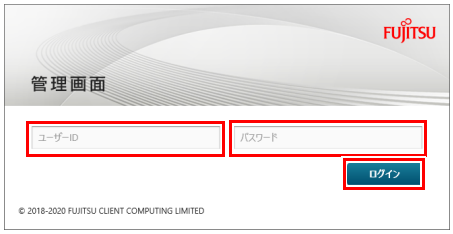
POINT

▸IPアドレスにはコンピューター部分のIPアドレスをお使いください。
コンピューター部分のIPアドレスが「192.168.1.3」の場合は次のようになります。
http://192.168.1.3:10080/

▸Internet Explorer で管理画面を表示したときに入力フォームが表示されない場合は、次の設定をご確認ください。
1.Internet Explorer を起動します。
2.画面右上のツールアイコン（設定）→「互換表示設定」の順にクリックします。
「互換性設定の変更」が表示されます。
3.「イントラネットサイトを互換表示で表示する」のチェックを外します。

ログイン画面が表示されます。

2　ユーザー ID およびパスワードを入力し、「ログイン」をクリックします。
ユーザー ID「administrator」と「パスワードの変更」（→ P.84）で変更したパスワードを入力してください。

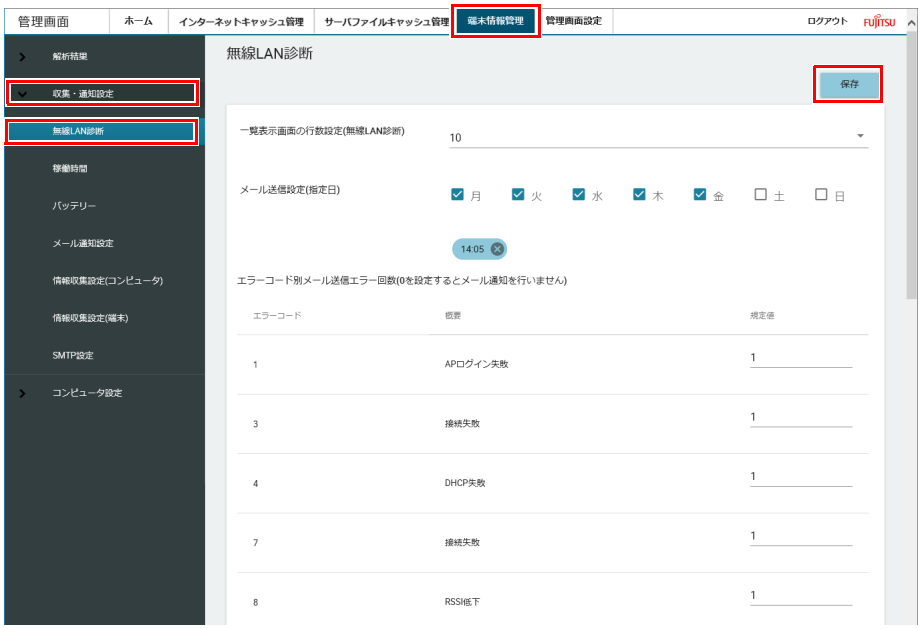


「収集・通知」に関する設定

メンテナンス機能に関する項目は、「収集・通知設定」メニューにあります。
上から順に必要な情報を設定していきます。

●「収集・通知」設定が可能な機種：ARROWS Tab Q508/SE 以降の 10 インチタブレット「Q シリーズ」

1　「端末情報管理」→「収集・通知設定」→「無線 LAN 診断」の順にクリックして設定画面を表示し、無線 LAN 診断に関する項目を設定して「保存」をクリックします。



各項目については、次の表をご覧ください。

項目	説明
一覧表示画面の桁数設定(無線LAN診断)	「解析結果」の「無線 LAN 診断状況一覧」に表示する診断結果の表示桁数を設定します。5 桁、10 桁（初期設定値）、25 桁に設定できます。
メール送信設定（毎月の指定日）	収集した無線 LAN 診断情報を送信する曜日と時間を指定します。
エラーコード別メール送信エラー回数	無線 LAN に関する各種エラーについて設定します。診断は一定間隔で行われます。なお、規定値は「1」を指定してください。 「0」を指定すると、そのエラーに関するメール送信が行われません。

POINT

▸無線LAN診断のエラーコードの意味、対処方法については、「無線LAN診断で表示されるエラーメッセージ」（→P.246）をご覧ください。

2 「稼働時間」をクリックして設定画面を表示し、稼働時間に関する項目を設定して「保存」をクリックします。

各項目については、次の表をご覧ください。

項目	説明
メール送信設定（毎月の指定日）	稼働時間の情報に関するメール送信日（毎月 1 日 ~28 日）と時間を指定します。

3 「バッテリー」をクリックして設定画面を表示し、バッテリーに関する項目を設定して「保存」をクリックします。

各項目については、次の表をご覧ください。

項目	説明
バッテリー劣化と判定される タブレット端末の台数	利用しているタブレット端末のうち、何台がバッテリー劣化と判定されたらメールを送信するかを設定します。
メール送信設定（毎月の指定日）	収集したバッテリー診断に関する情報を送信する曜日と時間を指定します。なお、指定の時間に本製品がネットワークに接続していない、電源が入ってない場合は、次回ネットワークに接続したタイミングでメールが送信されます。

4「メール通知設定」をクリックして設定画面を表示し、メールの通知に関する項目を設定して「保存」をクリックします。

各項目については、次の表をご覧ください。

項目		説明
メール共通設定	送信元メールアドレス	各種情報をメールで送信するときの、差出人となるメールアドレスを入力します。 なお、送信元メールアドレスは、事前に準備しておく必要があります。
	メール送信先登録と送信項目設定	送信先と、送信する情報を設定します。 「送信先メールアドレス」の欄にメールアドレスを入力し、「登録」をクリックすると、送信先のメールアドレスが追加されます。その後、送信する情報を選択します。 なお、送信先のメールアドレスは、事前に準備しておく必要があります。
無線 LAN 診断	定型文	メールを送信するときの定型文を入力します。 定型文の中に、「●●小学校の X 組のエッジコンピューティングデバイスです。」など、送信元がわかるような文章を入れてください。
	送信エラー時のリトライ回数	メール送信に失敗した場合の、リトライ回数を指定します。
バッテリー	定型文	メールを送信するときの定型文を入力します。 定型文の中に、「●●小学校の X 組のエッジコンピューティングデバイスです。」など、送信元がわかるような文章を入れてください。
	送信エラー時のリトライ回数	メール送信に失敗した場合の、リトライ回数を指定します。
稼働時間	定型文	メールを送信するときの定型文を入力します。 定型文の中に、「●●小学校の X 組のエッジコンピューティングデバイスです。」など、送信元がわかるような文章を入れてください。
	送信エラー時のリトライ回数	メール送信に失敗した場合の、リトライ回数を指定します。

5 本製品の情報収集に関する項目について設定変更が必要な場合は、「情報収集設定（コンピュータ）」をクリックして設定画面を表示した後、設定を変更して「保存」をクリックします。設定変更が不要な場合は、手順 9 に進んでください。

各項目については、次の表をご覧ください。

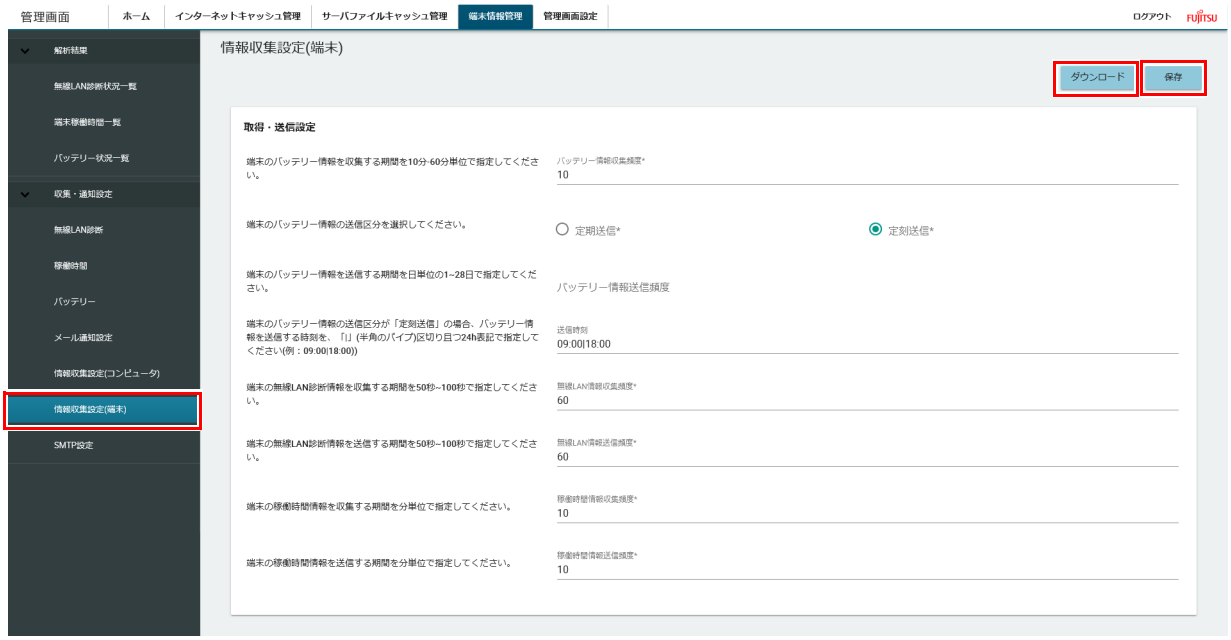
項目	説明
無線 LAN 情報収集頻度	本製品の無線 LAN アクセスポイントの診断情報を収集する頻度を、50 秒～ 100 秒の間で指定します。 この項目は初期値「60」で設定することを推奨いたします。
無線 LAN 情報送信頻度	収集した無線 LAN 診断情報を送信する頻度を、50 秒～ 100 秒の間で指定します。 この項目は初期値「60」で設定することを推奨いたします。
稼働時間情報収集頻度	本製品の稼働時間情報を収集する頻度を、分単位で指定します。
稼働時間情報送信頻度	収集した稼働時間情報を送信する頻度を、分単位で指定します。

6「ダウンロード」をクリックして、ファイルをダウンロードします。

7 ダウンロードしたファイルを次のフォルダーに移動して、既存のファイルと置換します。
C:¥ProgramData¥FCCL¥MaintInfoCollection¥Ini
なお、「対象のフォルダーへのアクセスは拒否されました」というメッセージが表示される場合は、「続行」をクリックします。

8 本製品を再起動します。

9 端末の情報収集に関する項目について設定変更が必要な場合は、「情報収集設定（端末）」をクリックして設定画面を表示した後、タブレット端末の情報収集に関する項目を設定し、「保存」をクリックします。設定変更が不要な場合は、手順 13 に進んでください。



各項目については、次の表をご覧ください。

項目	説明
バッテリー情報収集頻度	タブレット端末のバッテリー情報を収集する頻度を、10分～60分の間で指定します。この項目は、変更しないでください。 この項目は初期値「10」で設定することを推奨いたします。
定期送信	バッテリー情報を指定した周期で送信します。
定刻送信	バッテリー情報を指定した時刻に毎日送信します。
バッテリー情報送信頻度	収集したバッテリー情報を送信する頻度を、1 日～ 28 日の間で指定します。定期送信を選択した場合に設定できます。
送信時刻	収集したバッテリー情報を送信する時刻を、24h 表記（00:00 ～ 24:00）かつ複数回送信する場合は、「|」（半角のパイプ）区切って指定します。定刻送信を選択した場合に設定できます。 例：9 時と 18 時に送信する場合　「09:00|18:00」
無線 LAN 情報収集頻度	タブレット端末の無線 LAN 診断情報を収集する頻度を、50 秒～ 100 秒の間で指定します。 この項目は初期値「60」で設定することを推奨いたします。
無線 LAN 情報送信頻度	収集した無線 LAN 診断情報を送信する頻度を、50 秒～ 100 秒の間で指定します。 この項目は初期値「60」で設定することを推奨いたします。
稼働時間情報収集頻度	タブレット端末の稼働時間情報を収集する頻度を、分単位で指定します。
稼働時間情報送信頻度	収集した稼働時間情報を送信する頻度を、分単位で指定します。

10「ダウンロード」をクリックして、設定ファイル（TerminalInfoAppSetting.ini）をダウンロードします。

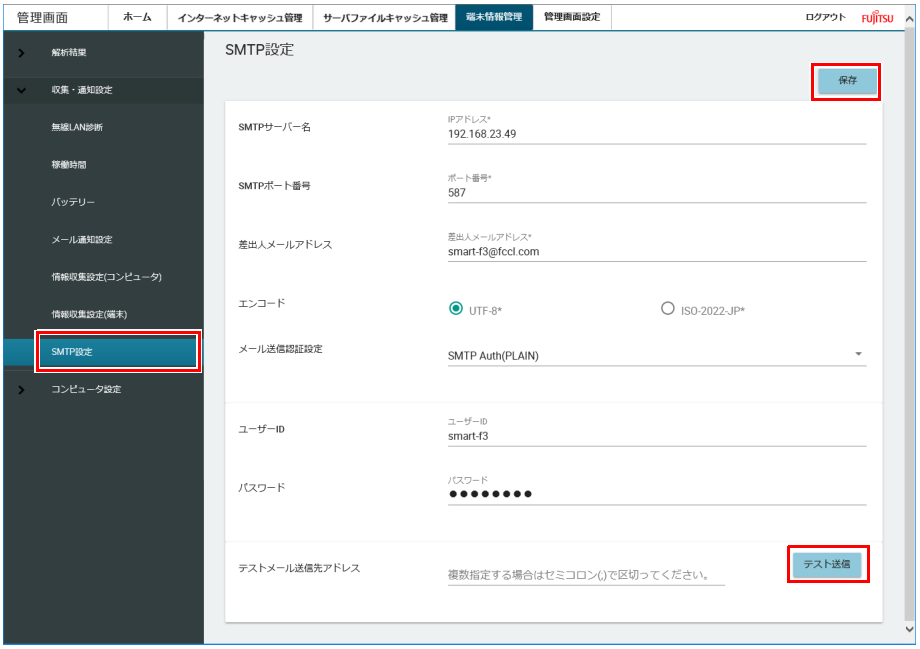
11 USB メモリーなどに設定ファイルをコピーします。

重要

▸本製品には、USB メモリーなどの媒体は添付されておりません。セットアップの前にあらかじめご用意ください。

12 ダウンロードした設定ファイルは、「基本機能 - 初期設定（タブレット端末）」（→ P.91）で使用します。詳しくは、「TerminalInfoAppSetting.ini のコピー」（→ P.99）をご覧ください。

13「SMTP 設定」をクリックして設定画面を表示し、SMTP サーバー（メールの配信サーバー）に関する項目を設定して「保存」をクリックします。



各項目については、次の表をご覧ください。

項目	説明
SMTP サーバー名	SMTP サーバーの IP アドレスを指定します。
SMTP ポート番号	SMTP サーバーで利用するポート番号を指定します。
差出人メールアドレス	通知メールの差出人のメールアドレスを指定します。
エンコード	文字のエンコードの種類を指定します。 「UTF-8」と「ISO-2022-JP」のどちらかを指定します。
メール送信認証設定	SMTP サーバーの認証が必要なときに、認証方法とユーザー ID、パスワードなどを指定します。 認証方法は、「認証なし」「SMTP Auth(PLAIN)」「SMTP Auth(LOGIN)」から指定します。
ユーザー ID	SMTP サーバーにログオンするためのアカウント名を指定します。
パスワード	SMTP サーバーにログオンするためのパスワードを指定します。
テストメール送信先アドレス	テストメールの送信先を指定します。 複数のメールを送信する場合は、メールとメールの間をセミコロン「;」を入力してください。テストメールを送信する場合は、「テスト送信」をクリックしてください。

POINT

▸SMTPの各設定は、事前に用意した送信元メールアドレスの設定を確認して入力する必要があります。

以上で、メンテナンス機能に関する設定は終了です。

システム時刻の設定

本製品とタブレット端末のシステム時刻が 30 秒以上ずれていると、無線 LAN 診断のログに不具合が出ます。本製品、タブレット端末共に時刻を合わせてください。

2. 基本機能 - 初期設定 （タブレット端末）

タブレット端末のセットアップ

タブレット端末本体のマニュアルをご覧になり、セットアップを実行してください。

エクスプローラーの設定

エクスプローラーで、隠しファイルやフォルダー、拡張子を表示します。

1「スタート」→「Windows システムツール」→「エクスプローラー」の順にタップします。
エクスプローラーが起動します。

2「表示」をタップし、「隠しファイル」と「ファイル名拡張子」にチェックを付けます。

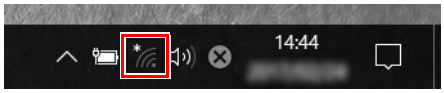
プロキシの設定

本製品のデータキャッシュ機能を使用するにはタブレット端末にプロキシを設定する必要があります。無線 LAN の設定をする前にプロキシの設定を行ってください。

手動プロキシ設定

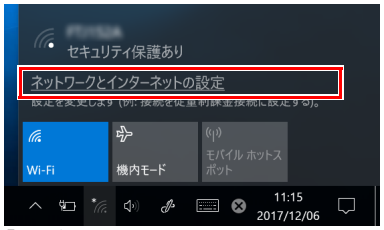
手動プロキシを設定します。自動構成スクリプト（PAC）を使用する場合は、「自動プロキシ設定」（→ P.93）をご覧ください。

1 画面右下の通知領域の をタップします。



（これ以降の画面は機種や状況により異なります）

2「ネットワークとインターネットの設定」をタップします。

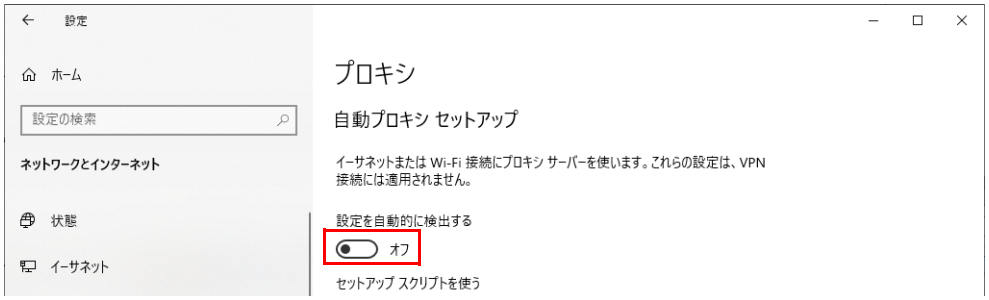


「設定」ウィンドウが表示されます。

3「プロキシ」をタップします。

「プロキシ」が表示されます。

4「自動プロキシセットアップ」の「設定を自動的に検出する」をタップして（オフ）にします。

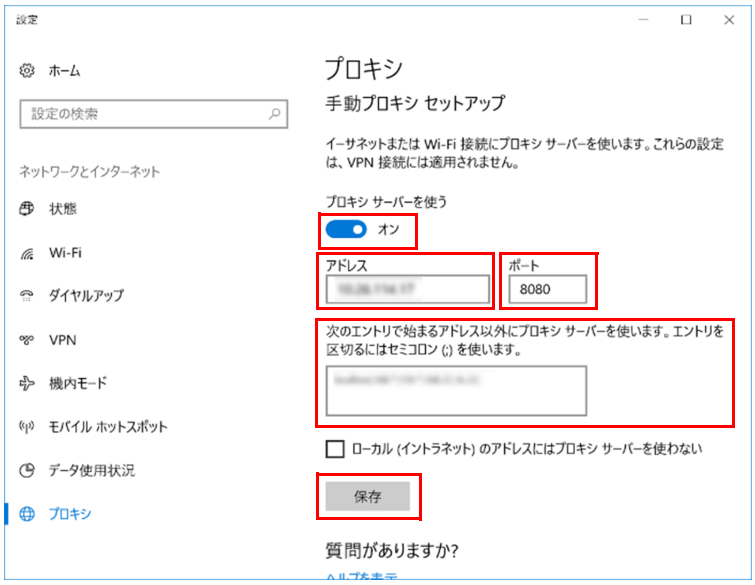


5「手動プロキシセットアップ」の「プロキシサーバーを使う」をタップして（オン）にし、次のように入力し、「保存」をタップします。

・アドレス：本製品のコンピューター部分の IP アドレス
・ポート：8080
・次のエントリで始まるアドレス以外にプロキシサーバーを使います。：本製品のコンピューター部分の IP アドレス

POINT

▸管理画面にアクセスする端末については、本製品へのアクセス時に本製品のコンピューター部分をプロキシとして使用しないように除外設定をしてください。
「次のエントリで始まるアドレス以外にプロキシサーバーを使います。」に本製品のコンピューター部分の IP アドレスを入力してください。



6　をタップして「設定」ウィンドウを閉じます。

7 管理者権限でコマンドプロンプトを起動します（→ P.7）。

8 次のコマンドを入力して【Enter】キーを押します。

netsh winhttp set proxy proxy-server="IPアドレス:8080"

※IP アドレスには、本製品のコンピューター部分の IP アドレスを入力します。

9 コマンドプロンプトを終了します。

自動プロキシ設定

プロキシの自動設定には、次の 2 つの方法があります。

●自動構成スクリプト（PAC）ファイル（→ P.93）

●プロキシ自動設定機能（→ P.97）

POINT

- プロキシ自動設定機能は、自動構成スクリプト（PAC）ファイルが使用できない場合に使用してください。
- サーバファイルキャッシュ機能を使用する場合は、プロキシ自動設定機能を使用せず、必ず、自動構成スクリプト（PAC）ファイルを使用してください。

■ 自動構成スクリプト （PAC） ファイル

□ サブネットマスク一覧

次の表は、A から C のアドレスクラスで使用する、サブネットマスクと IP アドレスの総数の一覧です。実際に利用する環境の IP アドレスの総数に適したサブネットマスクを使用します。

アドレスクラス	サブネットマスク		IP アドレスの総数
A クラス （大規模ネットワーク向け）	255.0.0.0	/8	16,777,216
	255.128.0.0	/9	8,388,608
	255.192.0.0	/10	4,194,304
	255.224.0.0	/11	2,097,152
	255.240.0.0	/12	1,048,576
	255.248.0.0	/13	524,288
	255.252.0.0	/14	262,144
	255.254.0.0	/15	131,072
B クラス （中規模ネットワーク向け）	255.255.0.0	/16	65,536
	255.255.128.0	/17	32,768
	255.255.192.0	/18	16,384
	255.255.224.0	/19	8,192
	255.255.240.0	/20	4,096
	255.255.248.0	/21	2,048
	255.255.252.0	/22	1,024
	255.255.254.0	/23	512
C クラス （小規模ネットワーク向け）	255.255.255.0	/24	256
	255.255.255.128	/25	128
	255.255.255.192	/26	64
	255.255.255.224	/27	32
	255.255.255.240	/28	16
	255.255.255.248	/29	8
	255.255.255.252	/30	4
	255.255.255.254	/31	2
	255.255.255.255	/32	1

□ 自動構成スクリプト （PAC） ファイルの作成

本書では次の条件を例に、ファイルの作成方法を説明します。実際に利用する環境にあわせて設定してください。

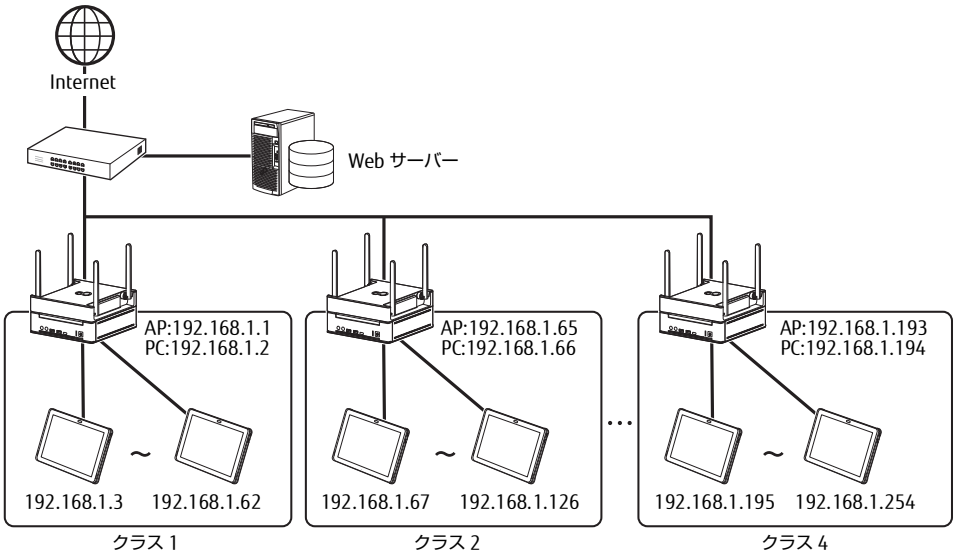
・ クラス（学級）の数　　：4
・ エッジコンピューティングデバイス　：各学級で 1 台設置
・ 接続する端末の台数　　：各学級で 62 台接続

※ 本製品で接続できる端末の台数は次のとおりです。
無線 LAN 接続：44 台まで
無線 LAN/ 有線 LAN 合わせて：100 台まで

ここでは、IP アドレスの第 4 オクテッドを 4 つに分割します。サブネットマスク（→ P.93）は、「255.255.255.192/26」を使用します。

各クラスへの割り当て可能な IP アドレス、PAC に用いるネットワークアドレス、サブネットマスクは次の表のようになります。

クラス	IP （ネットワーク）	IP （ホスト）	割り当て可能な IP 範囲	ネットワーク アドレス	サブネットマスク
1	192.168.1	0 ～ 63	1 ～ 62	192.168.1.0	255.255.255.192/26
2	192.168.1	64 ～ 127	65 ～ 126	192.168.1.64	255.255.255.192/26
3	192.168.1	128～191	129 ～ 190	192.168.1.128	255.255.255.192/26
4	192.168.1	192～255	193 ～ 254	192.168.1.192	255.255.255.192/26



注 AP：アクセスポイント部分
PC：コンピューター部分

PAC ファイルには、ネットワークアドレスとサブネットマスクより次のように記述します。

```
function FindProxyForURL(url, host) {
    // URL のホストがローカルの場合
    if (isInNet(host, "192.168.1.0", "255.255.255.0")) {
        return "DIRECT"; // プロキシを経由しない
    } else {
        // 自分の IP アドレスを取得
        myip = myIpAddress();
        // クラス 1
        if (isInNet(myip, "192.168.1.0", "255.255.255.192")) {
            return "PROXY 192.168.1.2:8080";
        // クラス 2
        } else if (isInNet(myip, "192.168.1.64", "255.255.255.192")) {
            return "PROXY 192.168.1.66:8080";
        // クラス 3
        } else if (isInNet(myip, "192.168.1.128", "255.255.255.192")) {
            return "PROXY 192.168.1.130:8080";
        // クラス 4
        } else if (isInNet(myip, "192.168.1.192", "255.255.255.192")) {
            return "PROXY 192.168.1.194:8080";
        // 上記以外のクラス
        } else {
            return "DIRECT";
        }
    }
}
```

□ PAC ファイルの記載方法

●FindProxyForURL 関数

PAC ファイルが実行時に、FindProxyForURL 関数が実行されます。

```
function FindProxyForURL(url, host) {
```

・引数
　url：アクセス先の URL。http:// から始まる URL のパスとクエリ要素は取り除かれます。
　host：URL から抜き出したホスト名
・戻り値
　プロキシサーバー名＋ポート番号

●myIpAddress 関数

タブレット端末（自分）の IP アドレスを取得します。

```
myip = myIpAddress();
```

●isInNet 関数

どのネットワークに属しているかを判定します。

```
isInNet(IP アドレス , ネットワークアドレス , サブネットマスク )
```

IP アドレスをサブネットマスクでマスクし、ネットワークアドレスと一致すれば OK（True）、一致しなければ NG（False）
（例）isInNet(172.16.1.3, 172.16.1.0, 255.255.255.0) → OK(True)
　　isInNet(172.16.2.3, 172.16.1.0, 255.255.255.0) → NG(False)

●PAC ファイル内の例外設定

外部にアクセスする場合はプロキシサーバーを経由したいが、ローカルアドレスについては経由しない方が良いという場合、ローカルアドレスを例外設定することができます。
方法としては、isInNet 関数を用い、入力 URL のホスト名がローカルの場合はプロキシを経由しないように記述します。

```
// URL のホストがローカルの場合
if (isInNet(host, "192.168.1.0", "255.255.255.0")) {
    return "DIRECT"; // プロキシを経由しない
}
```

また、管理画面にアクセスする端末に関しては、本製品を例外設定する必要があります。

```
if (isInNet(host, "IP アドレス", "255.255.255.0")){
    return "DIRECT";
}
```

※IP アドレスには本製品のコンピューター部分の IP アドレスを記入してください。

また、サーバファイルキャッシュ機能を使用する場合は、以下の例のように学習支援アプリサーバを例外設定する必要があります。

```
if (isInNet(host, "IP アドレス", "255.255.255.0")){
    return "DIRECT";
}
```

※IP アドレスには学習支援アプリサーバの IP アドレスを記入してください。

●ファイル名

「proxy.pac」という名前で、テキスト形式で保存します。

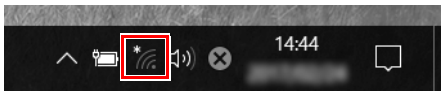
□ PAC ファイルを WEB サーバーに配置する

作成した「proxy.pac」を学校のイントラネット内にある WEB サーバー内に配置します。

□ 自動構成スクリプト （PAC） の設定

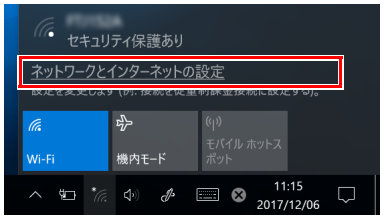
自動構成スクリプト（PAC）を使った自動プロキシを設定します。

1 画面右下の通知領域の をタップします。



（これ以降の画面は機種や状況により異なります）

2「ネットワークとインターネットの設定」をタップします。



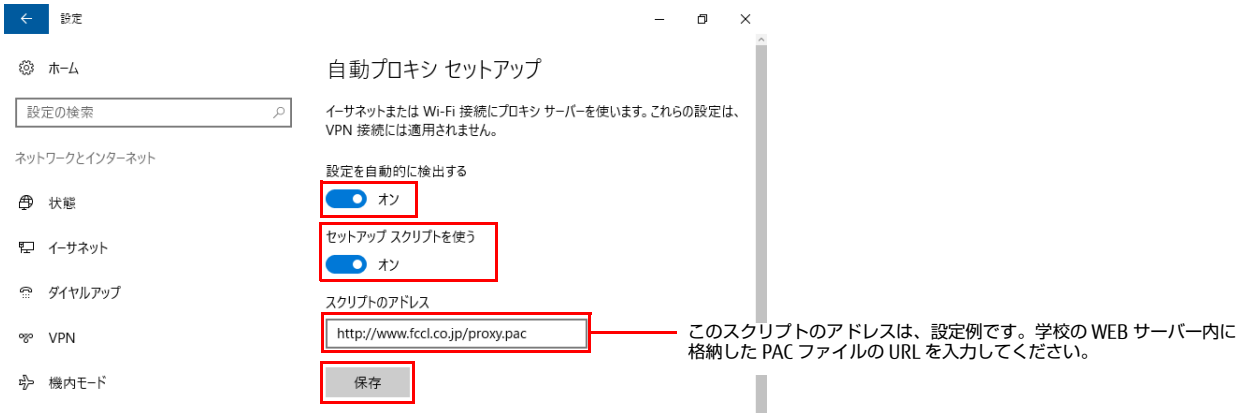
「設定」ウィンドウが表示されます。

3「プロキシ」をタップします。

「設定」ウィンドウが表示されます。

4「自動プロキシセットアップ」の「設定を自動的に検出する」と「セットアップスクリプトを使う」をタップして （オン）にし、次のように入力し、「保存」をタップします。

・スクリプトのアドレス：PAC ファイルの URL



5 ✕ をタップして「設定」ウィンドウを閉じます。

6 管理者権限でコマンドプロンプトを起動します（→ P.7）。

7 次のコマンドを入力して【Enter】キーを押します。

netsh winhttp set proxy proxy-server="IPアドレス:8080"

※IP アドレスには、本製品のコンピューター部分の IP アドレスを入力します。

8 コマンドプロンプトを終了します。

■ プロキシ自動設定機能

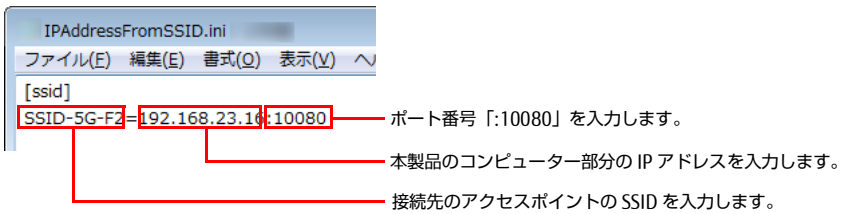
本製品のアクセスポイントを AP モード（ブリッジモード）で利用している場合は、次の方法でプロキシの自動設定を設定します。

□ インストール

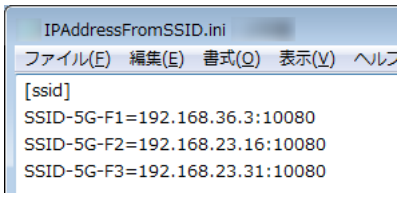
1. エッジコンピューティングデバイスの「C:¥Fujitsu¥Software¥InternetCache¥ProxyController」フォルダーをタブレット端末の「C:¥」にコピーします。
2. 次のファイルを長押しタップし、「管理者として実行」を選択します。

   C:¥ProxyController¥inst.bat
3. 次のファイルをデスクトップにコピーします。

   C:¥ProgramData¥FCCL¥ProxyController¥Ini¥IPAddressFromSSID.ini
4. コピーした「IPAddressFromSSID.ini」設定ファイルをテキストエディターで開きます。
5. 次の部分を変更します。
   接続先のアクセスポイントの SSID と本製品のコンピューター部分の IP アドレスを次のように設定します。



   複数登録する場合は、次のように設定します。



6. 変更後、保存してファイルを閉じます。
7. デスクトップの「IPAddressFromSSID.ini」設定ファイルを次のフォルダーに移動して、既存のファイルと置換します。

   C:¥ProgramData¥FCCL¥ProxyController¥Ini¥IPAddressFromSSID.ini

   POINT
   ▸「対象のフォルダーへのアクセスは拒否されました」というメッセージが表示される場合は、「続行」をタップします。
8. 管理者権限でコマンドプロンプトを起動します（→ P.7）。
9. 次のコマンドを入力して【Enter】キーを押します。

   netsh winhttp set proxy proxy-server="IPアドレス:8080"

   ※IP アドレスには、本製品のコンピューター部分の IP アドレスを入力します。
10. コマンドプロンプトを終了します。

端末情報収集ツールのインストール

1 エッジコンピューティングデバイスの「C:¥Fujitsu¥Software¥SmartMaintenance¥Other¥ 端末情報収集ツール」フォルダーをタブレット端末にコピーします。

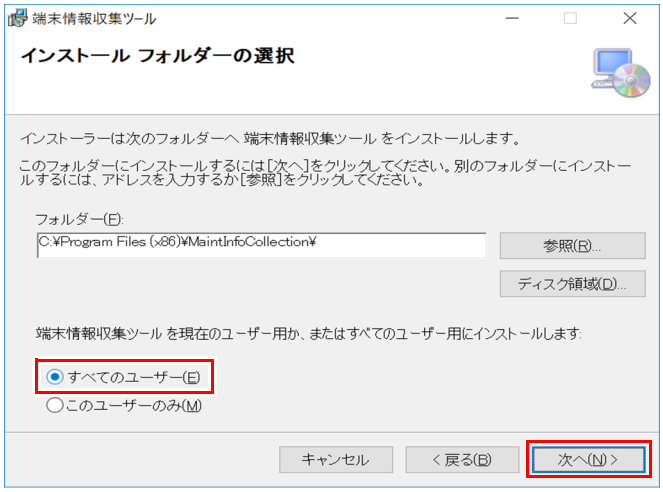
2 次のフォルダーの「TerminalInfoAppSetup.msi」をダブルタップします。
次のフォルダーは、C:¥ にコピーした場合の例です。

C:¥端末情報収集ツール¥TerminalInfoAppSetup.msi

セットアップ・ウィザードが表示されます。

3「次へ」をタップします。
インストール先フォルダーの入力画面が表示されます。

4「すべてのユーザー」を選択し、「次へ」をタップします。



「インストールの確認」が表示されます。

5「次へ」をタップします。

POINT
▸ユーザーアカウント制御の画面が表示される場合は、「はい」タップします。

インストールが開始されます。しばらくすると、「インストールが完了しました。」と表示されます。

6「閉じる」をタップします。
以上で端末情報収集ツールのインストールは終了です。

端末情報収集ツール設定ファイルの変更

TerminalInfoAppSetting.ini のコピー

「「収集・通知」に関する設定」の手順 9 で設定を変更した場合は、次の手順を実行します。設定を変更していない場合は、「TerminalInfoAppSetting.ini」設定ファイルのコピーは不要です。

1 「「収集・通知」に関する設定」の手順 12 で USB メモリーに保存した「TerminalInfoAppSetting.ini」設定ファイルを、次のフォルダーに上書きコピーします。

C:¥ProgramData¥FCCL¥MaintInfoCollection¥Ini

POINT

▸「対象のフォルダーへのアクセスは拒否されました」というメッセージが表示される場合は、「続行」をタップします。

2 タブレット端末を再起動します。

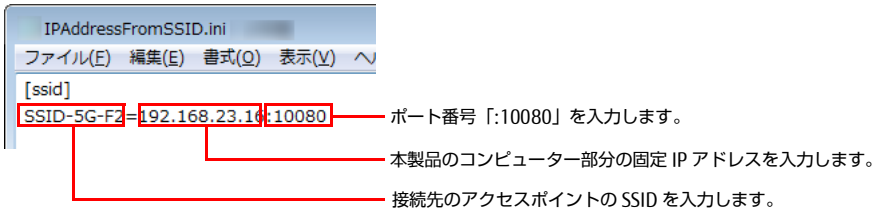
IPAddressFromSSID.ini の変更

1 次のファイルを USB メモリーにコピーします。

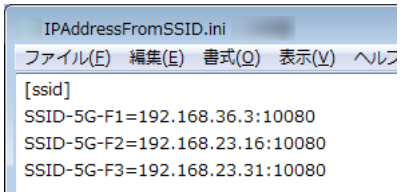
C:¥ProgramData¥FCCL¥MaintInfoCollection¥Ini¥IPAddressFromSSID.ini

2 USB メモリーにコピーした「IPAddressFromSSID.ini」設定ファイルをエッジコンピューティングデバイスのテキストエディターで開きます。

3 次の部分を変更します。
接続先のアクセスポイントの SSID と本製品のコンピューター部分の固定 IP アドレスを次のように設定します。



複数登録する場合は、次のように設定します。



4 変更後、保存してファイルを閉じます。

5 USB メモリーの「IPAddressFromSSID.ini」設定ファイルをタブレット端末の次のフォルダーに移動して、既存のファイルと置換します。

C:¥ProgramData¥FCCL¥MaintInfoCollection¥Ini

POINT

▸「対象のフォルダーへのアクセスは拒否されました」というメッセージが表示される場合は、「続行」をタップします。

サービスの起動

次の手順でサービス「MaintInfoCollectionService」を開始します。

1 → 「Windows 管理ツール」→「サービス」の順にタップします。

2 一覧から「MaintInfoCollectionService」の状態を確認し、実行中になっていない場合は、長押しタップし「開始」をタップします。
サービスが開始します。

3. 基本機能 - データキャッシュ機能 （製品本体）

インストール補助ツールを使用する （インターネットキャッシュ機能）

「インストール補助ツール」（→ P.23）は、本製品に添付されておりません。「インストール補助ツール」を使用する場合は、「インストール補助ツールとインターネットキャッシュ機能 V3.0.0 用アップデートモジュールのダウンロード」（→ P.28）をご覧になり、ダウンロードしてください。

ダウンロード後、「BasicFunction_InternetCache_Install.cmd」を実行してください。なお、バッチファイルは、必ず、管理者権限のアカウントで実行してください。次のインストールと設定が、自動で行われます。

「インターネットキャッシュ機能のインストールと設定」（→ P.100）～「シャットダウンの設定」（→ P.114）

バッチファイルの実行が完了したら、本製品を再起動した後、「インターネットキャッシュ機能 V3.0.0 用アップデートモジュールのインストール」（→ P.115）からインストールと設定を進めてください。
なお、「インストール補助ツール」（→ P.23）を使用しない場合は、本マニュアルに沿ってインストールと設定を行ってください。

インターネットキャッシュ機能のインストールと設定

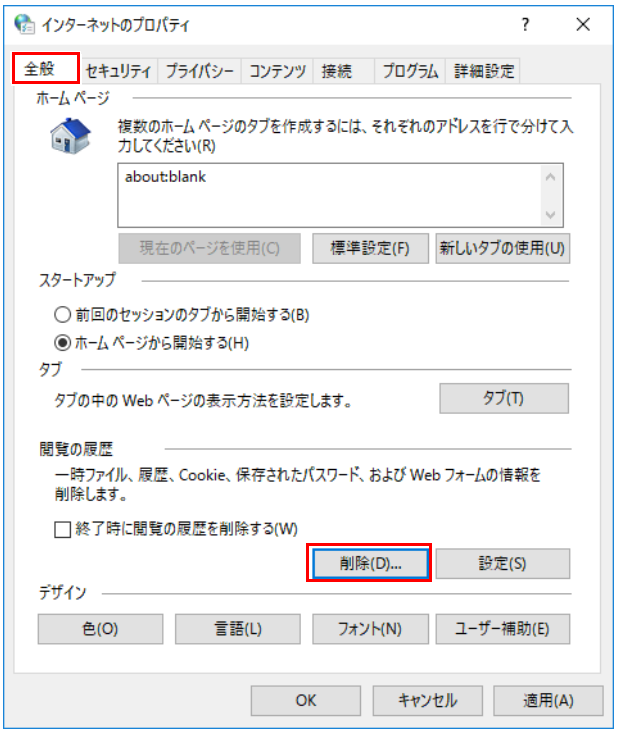
Internet Explorer のキャッシュの初期化

Internet Explorer ネットキャッシュ、ユーザーキャッシュを初期化します。

1 「コントロールパネル」を表示します（→ P.7）。
「コントロールパネル」が表示されます。

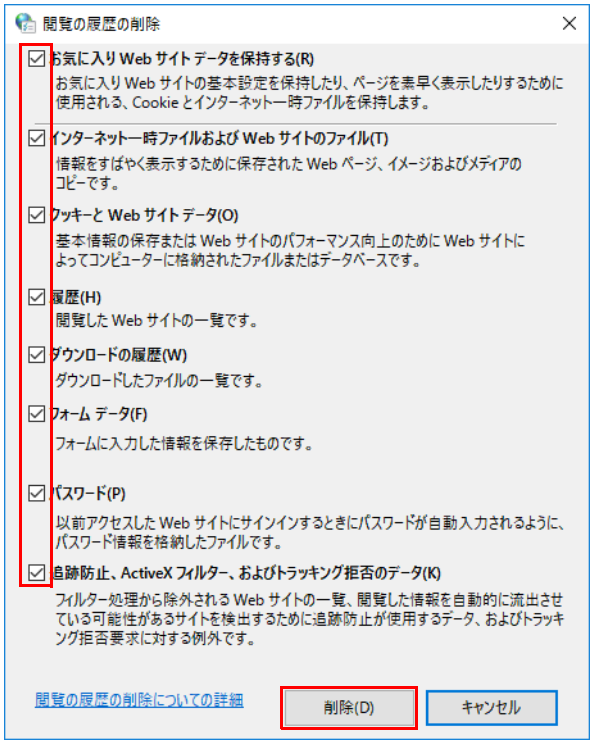
2 「ネットワークとインターネット」→「インターネット オプション」の順にクリックします。
「インターネットのプロパティ」が表示されます。

3 「全般」タブを選択し、「削除」をクリックします。



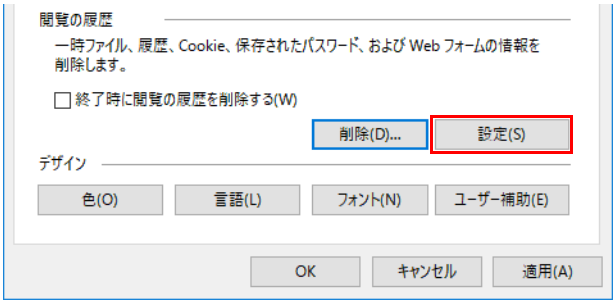
「閲覧の履歴の削除」が表示されます。

4 すべての項目にチェックを付けて、「削除」をクリックします。



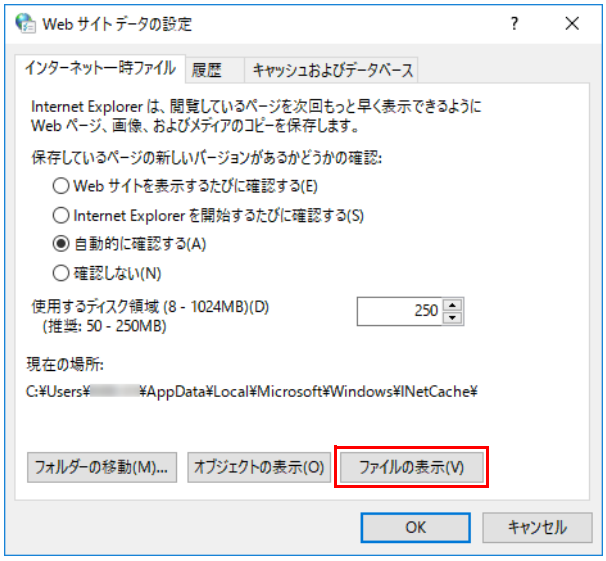
「インターネットオプション」が表示されます。

5「設定」をクリックします。



「Web サイトの データ設定」が表示されます。

6「ファイルの表示」をクリックします。

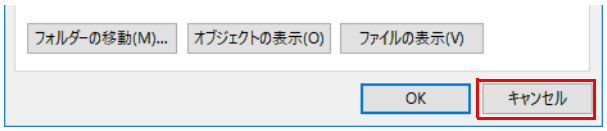


「INetCache」フォルダーが表示されます。

7 次の JavaScript のファイルがある場合は、ファイルを削除してフォルダーを閉じます。

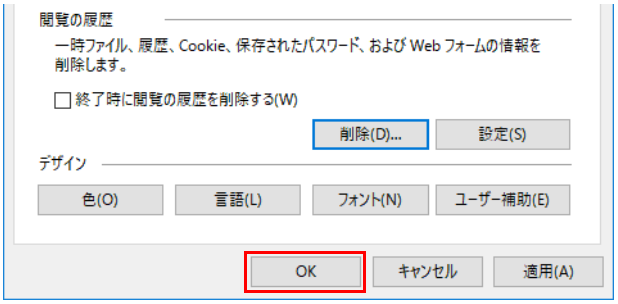
cache-data.js
squid.js

8「Web サイト のデータ設定」の「キャンセル」をクリックします。



「インターネットオプション」が表示されます。

9「OK」をクリックします。



キャッシュフォルダーの生成

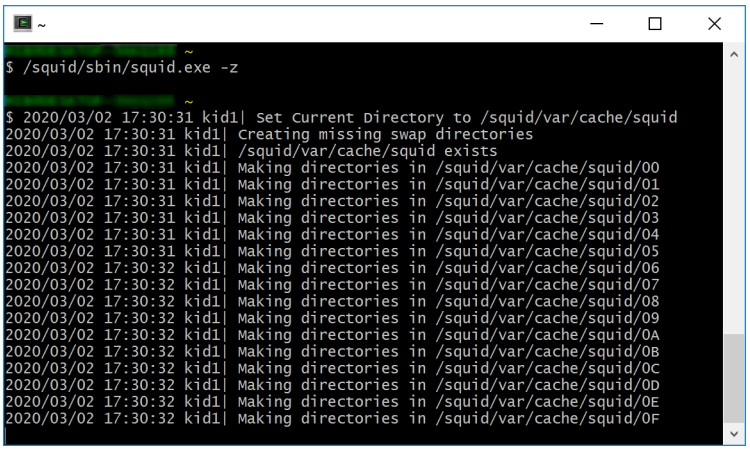
1「C:¥cygwin64¥Cygwin64 Terminal」を右クリックし「管理者として実行」をクリックします。
コンソールが起動します。

POINT
▸「ユーザーアカウント制御」が表示された場合は、「はい」をクリックします。

2 次のコマンドを入力し、【Enter】キーを押します。
rm -rf /squid/var/cache/squid/*

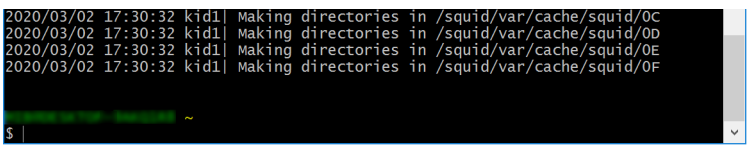
キャッシュフォルダーが削除されます。

3 次のコマンドを入力し、【Enter】キーを押します。
/squid/sbin/squid.exe -z



コマンド実行結果が表示されます。

4【Enter】キーを押します。



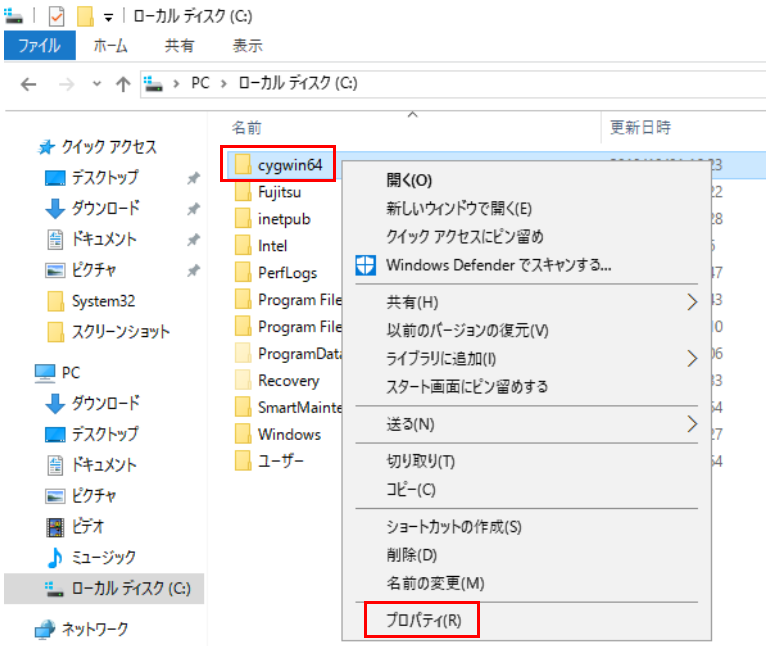
キャッシュフォルダーの生成が完了します。

5 閉じるボタン（ × ）をクリックします。

管理者権限の設定

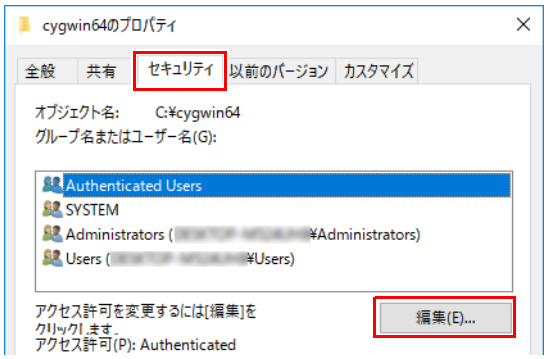
C:¥cygwin64 フォルダーに Administrators とユーザーアカウントのフルコントロールの権限を設定します。

1 「C:¥cygwin64」フォルダーを右クリックし「プロパティ」をクリックします。



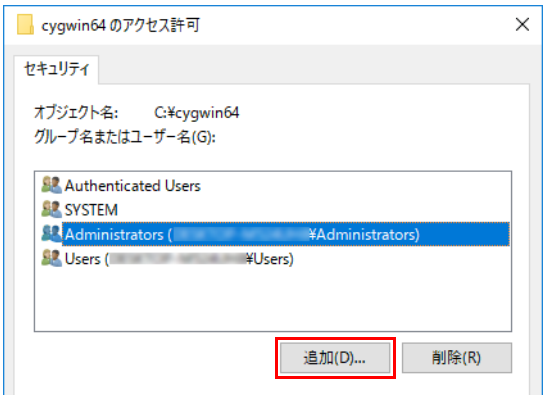
「cygwin64 のプロパティ」が表示されます。

2 「セキュリティ」タブをクリックし、「編集」をクリックします。



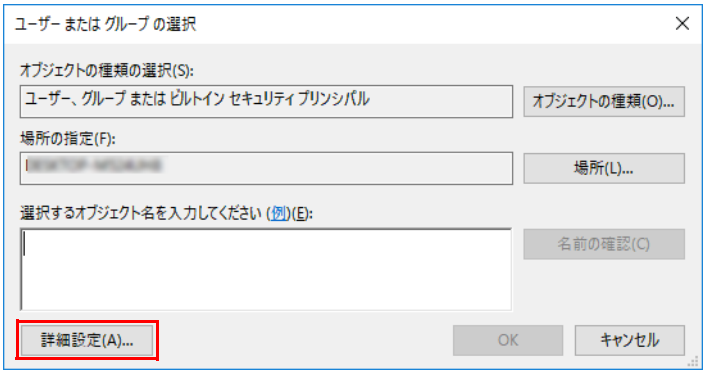
「cygwin64 のアクセス許可」が表示されます。

3 「追加」をクリックします。

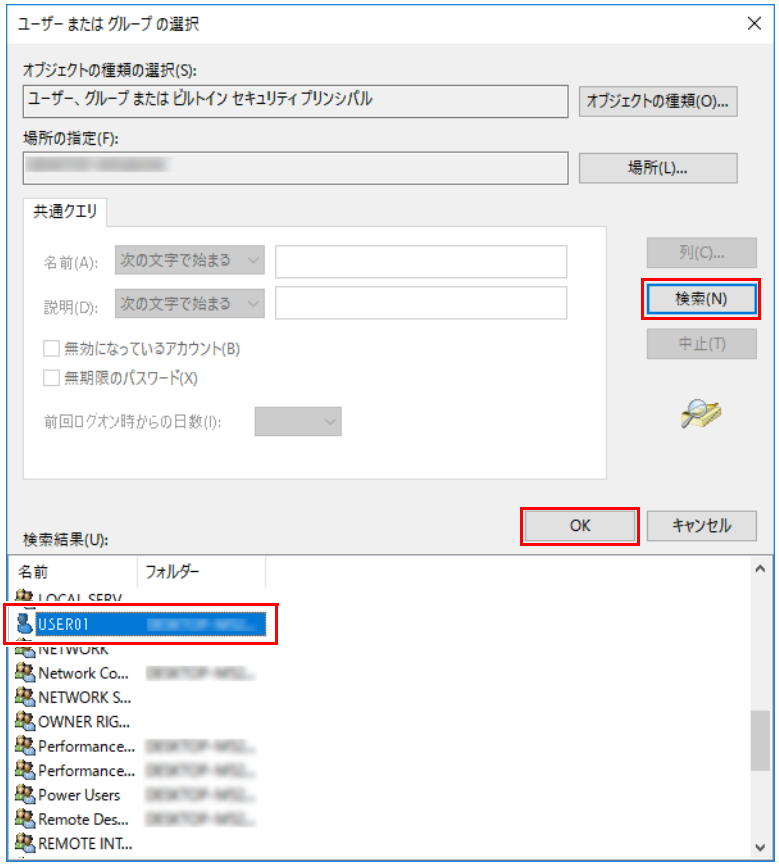


「ユーザーまたはグループの選択」が表示されます。

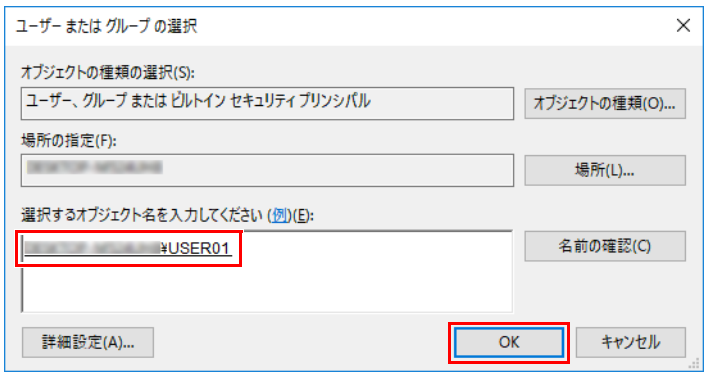
4「詳細設定」をクリックします。



5「検索」をクリックし、検索結果から現在サインインしているユーザーアカウントを選択し、「OK」をクリックします。

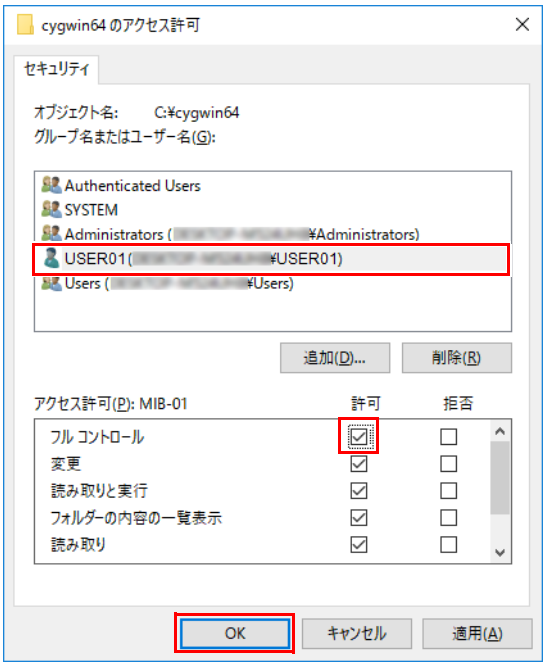


6「選択するオブジェクト名を入力してください」にユーザーアカウントが入力されていることを確認し、「OK」をクリックします。



「cygwin64 のアクセス許可」が表示されます。

7 追加したユーザーアカウントをクリックし、「アクセス許可」の「フルコントロール」にチェックを付け、「OK」をクリックします。



8 「はい」をクリックします。
しばらくすると、「cygwin64 のプロパティ」が表示されます。

9 「OK」をクリックします。

キャッシュ UI のサービス登録用バッチの実行

1 管理者権限でコマンドプロンプトを起動します（→ P.7）。

2 次のコマンドを入力し、【Enter】キーを押します。
cd C:¥cygwin64¥cacheUI¥setup
「C:¥cygwin64¥cacheUI¥setup」フォルダーへ移動します。

3 「CacheUI_setup.bat」を入力し、【Enter】キーを押します。
「セットアップ処理を終了します」と表示されたらサービスの登録は完了しました。

4 コマンドプロンプトを終了します。

5 「スタート」→「Windows 管理ツール」→「サービス」の順にクリックします。
サービスが起動します。

6 サービスの一覧に「CacheUIService」が存在することを確認します。

キャッシュ制御のサービス登録用バッチの実行

1 管理者権限でコマンドプロンプトを起動します（→ P.7）。

2 次のコマンドを入力し、【Enter】キーを押します。
cd C:¥cygwin64¥cacheUI¥setup
「C:¥cygwin64¥cacheUI¥setup」フォルダーへ移動します。

3 「CacheCtl_setup.bat」を入力し、【Enter】キーを押します。
「セットアップ処理を終了します」と表示されたらサービスの登録は完了しました。

4 コマンドプロンプトを終了します。

5 「スタート」→「Windows 管理ツール」→「サービス」の順にクリックします。
サービスが起動します。

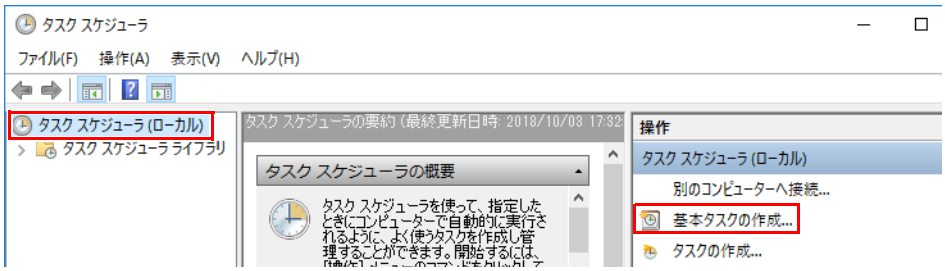
6 サービスの一覧に「cacheCtl」が存在することを確認します。

ログローテーションの設定

■ タスクスケジューラへのログローテートの登録

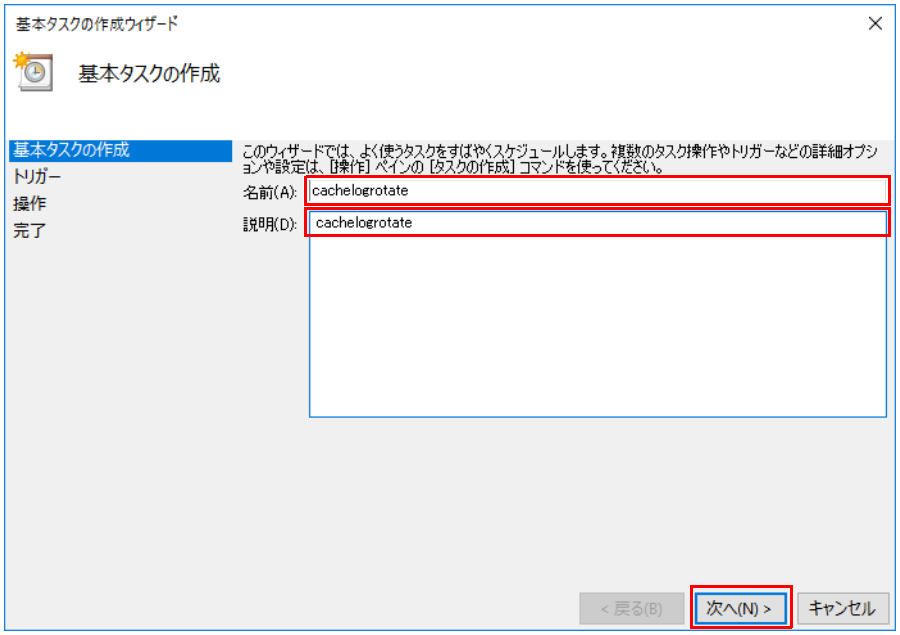
1 **「スタート」→「Windows 管理ツール」→「タスクスケジューラ」の順にクリックします。**
「タスクスケジューラ」が起動します。

2 **「タスクスケジューラ（ローカル）」を選択し、「操作」の「基本タスクの作成」をクリックします。**



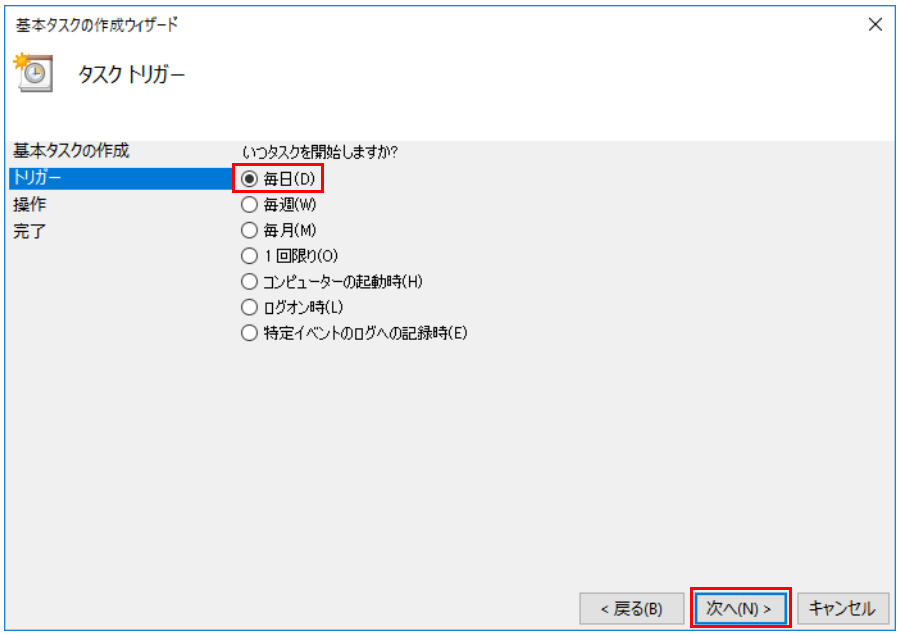
「基本タスクの作成」が表示されます。

3 **次の値を入力して、「次へ」をクリックします。**
名前：「cachelogrotate」
説明：「cachelogrotate」



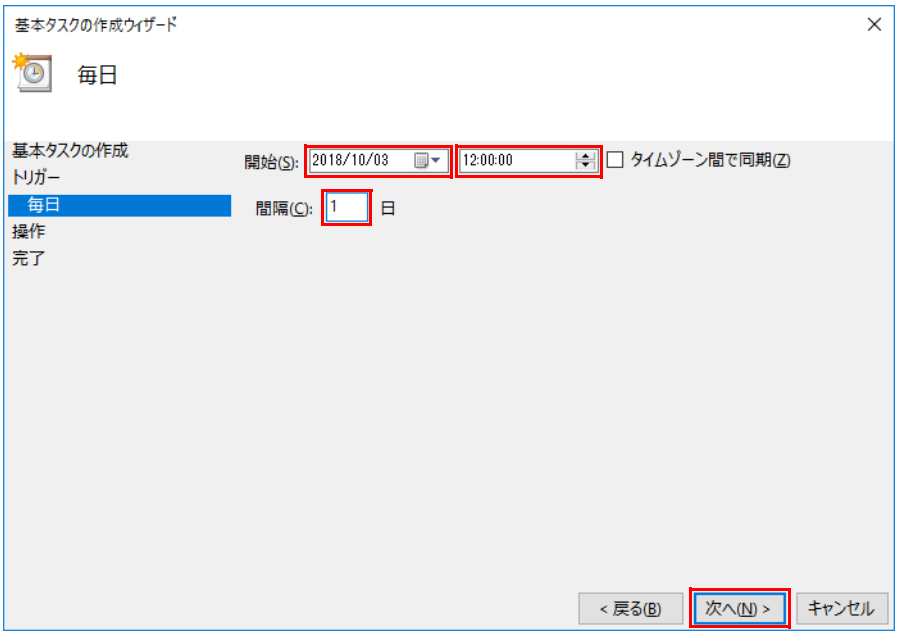
「タスク トリガー」が表示されます。

4「毎日」を選択し、「次へ」をクリックします。



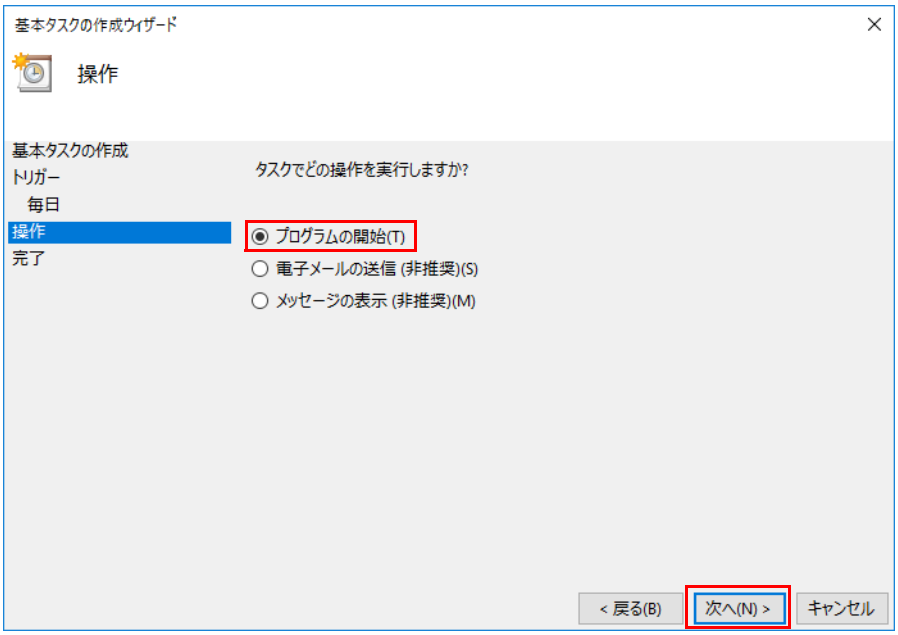
「毎日」が表示されます。

5「開始」に本日の日付と「12:00:00」を、「間隔」に「1 日」を設定し、「次へ」をクリックします。



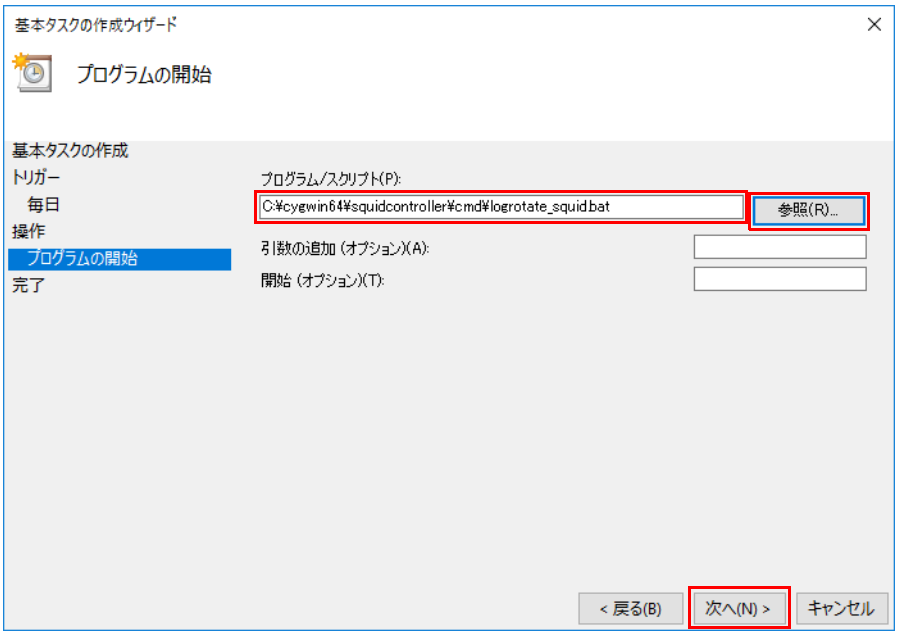
「操作」が表示されます。

6「プログラムの開始」を選択し、「次へ」をクリックします。



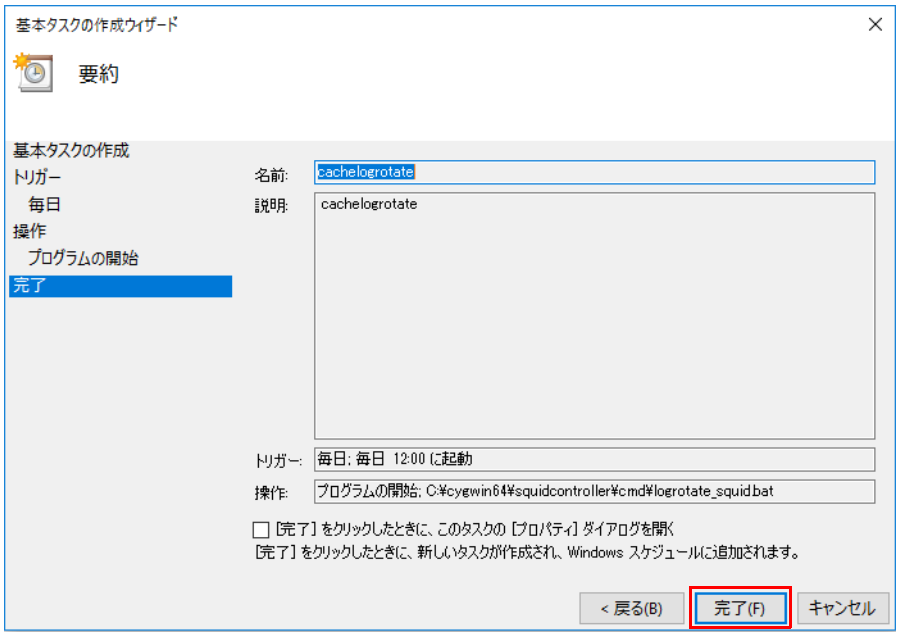
「プログラムの開始」が表示されます。

7「プログラム / スクリプト」の「参照」をクリックし、表示されたウィンドウから次のファイルを選択し、「次へ」をクリックします。
C:¥cygwin64¥squidcontroller¥cmd¥logrotate_squid.bat

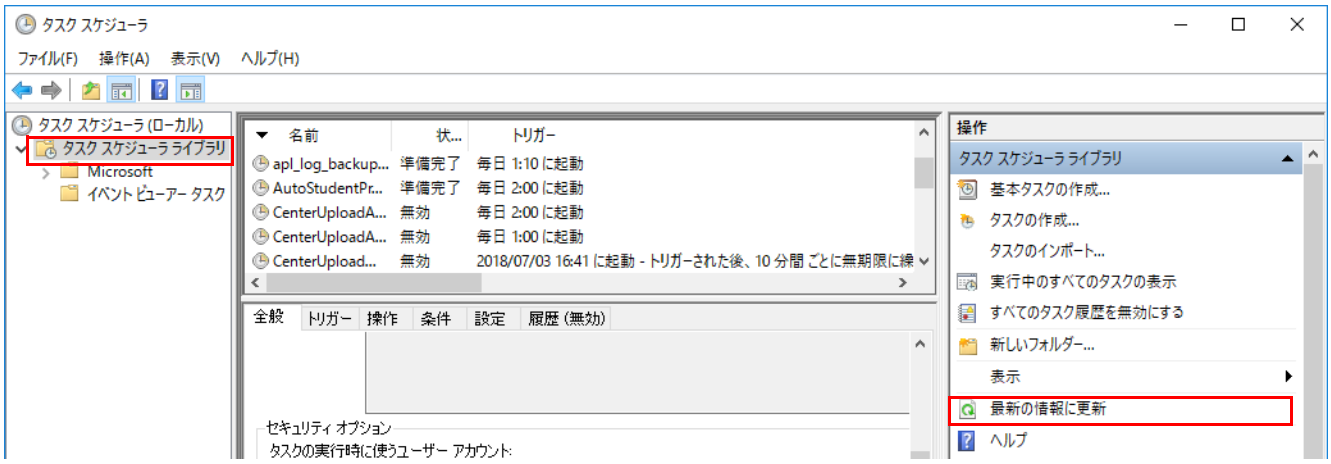


「要約」が表示されます。

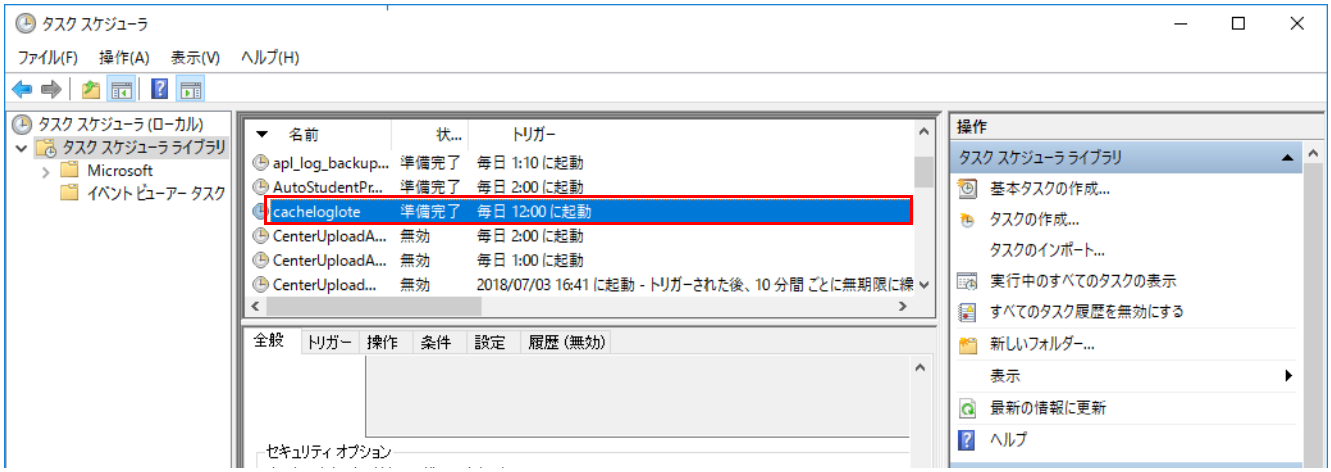
8「完了」をクリックします。



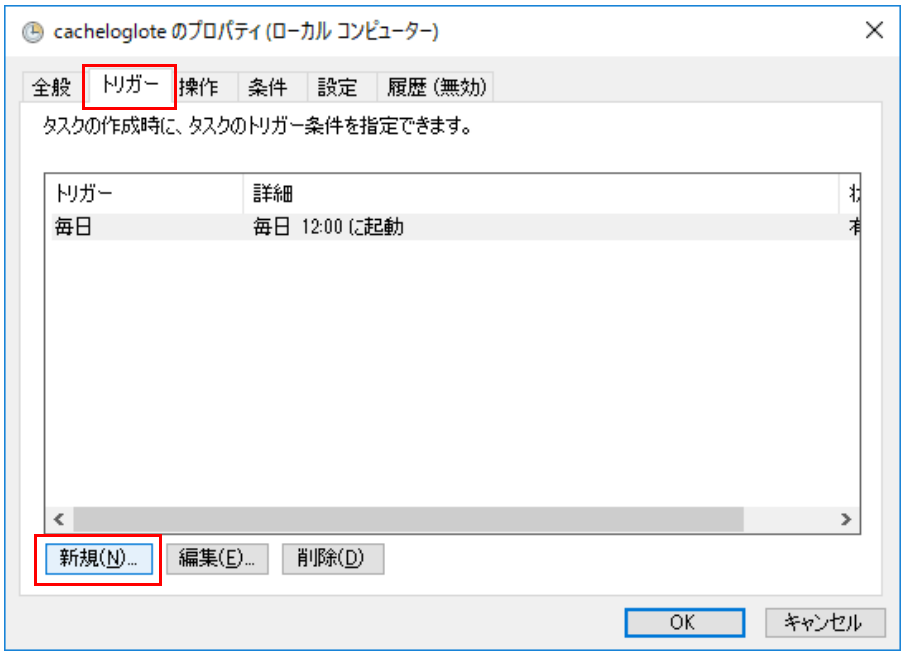
9「タスクスケジューラライブラリ」をクリックし、「最新の情報に更新」をクリックします。



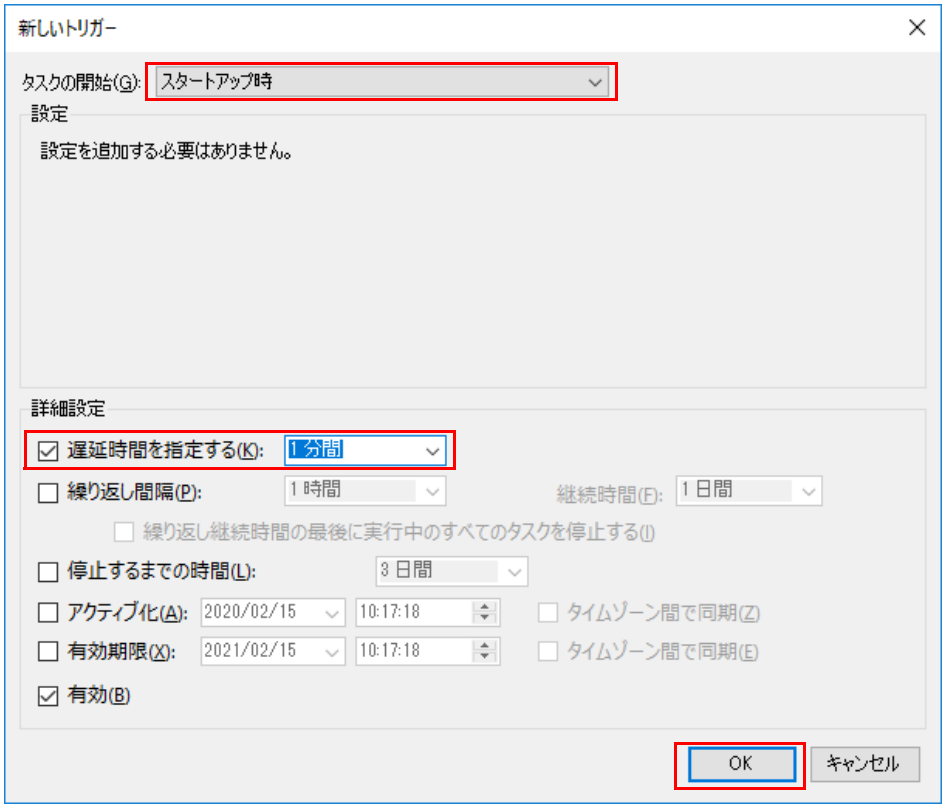
10「cachelogrotate」をダブルクリックします。



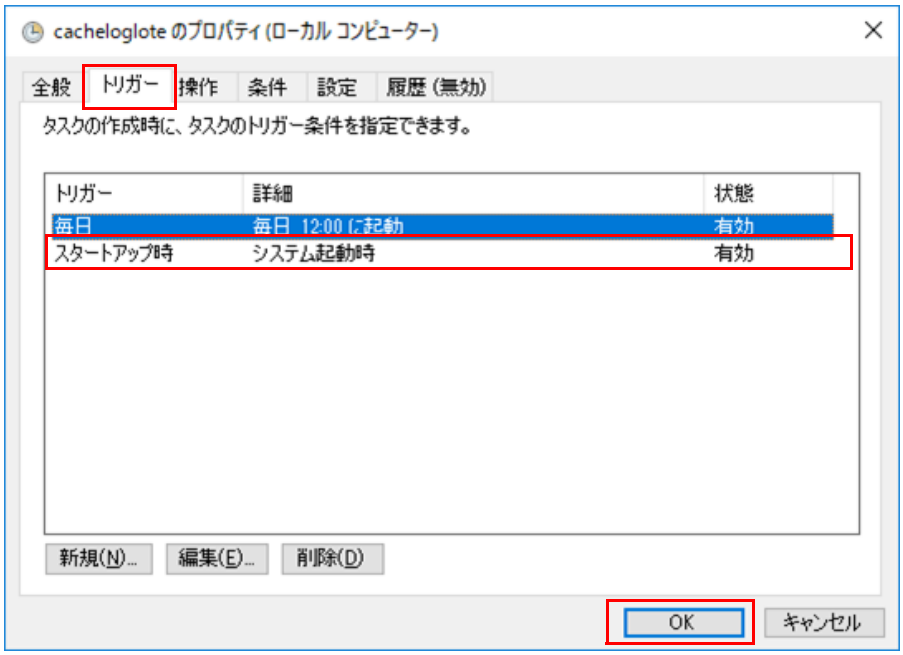
11 「トリガー」タブをクリックし、「新規」をクリックします。



12 タスクの開始に「スタートアップ時」を選択した後、詳細設定の 「遅延時間を指定する」にチェックを入れ「1 分間」を選択して、「OK」をクリックます。



13「スタートアップ時」が登録されていることを確認して「OK」をクリックします。



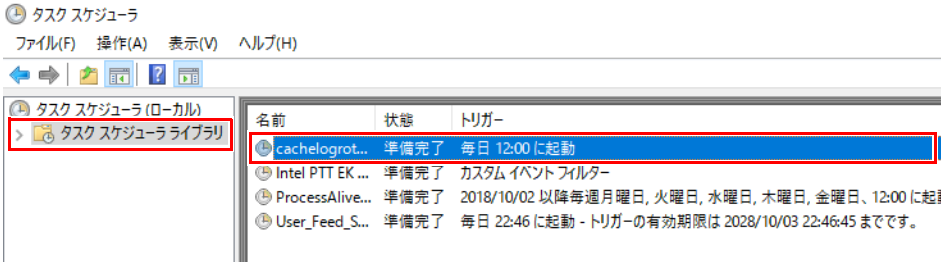
14「タスクスケジューラ」を閉じます。

■ログローテーション への SYSTEM アカウント登録

ログローテーション は管理者権限でないと動作しないため、管理権限を持っている SYSTEM アカウントを登録します。

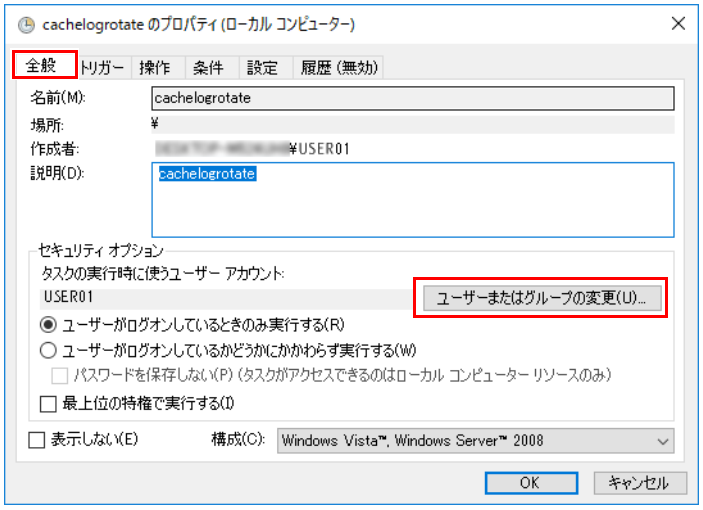
1 「スタート」→「Windows 管理ツール」→「タスクスケジューラ」の順にクリックします。
「タスクスケジューラ」が起動します。

2 「タスクスケジューラライブラリ」をクリックし、「cachelogrotate」をダブルクリックします。



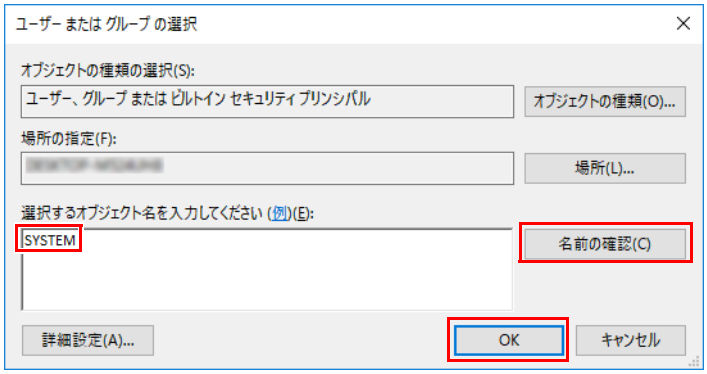
「cachelogrotate のプロパティ（ローカル コンピューター）」が表示されます。

3 「全般」タブをクリックし、「ユーザーまたはグループの変更」をクリックします。



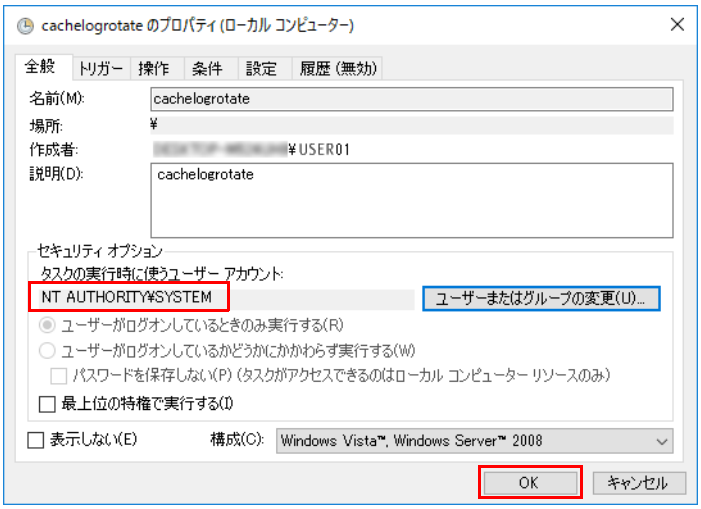
「ユーザーまたはグループの選択」が表示されます。

4 「選択するオブジェクト名を入力してください」に「SYSTEM」を入力した後、「名前の確認」をクリックし、「OK」をクリックします。



「cachelogrotate のプロパティ（ローカル コンピューター）」が表示されます。

5 セキュリティオプションの「タスクの実行時に使うユーザー アカウント」が「NT AUTHORITY¥SYSTEM」であることを確認し「OK」をクリックします。



6「タスクスケジューラ」を閉じます。

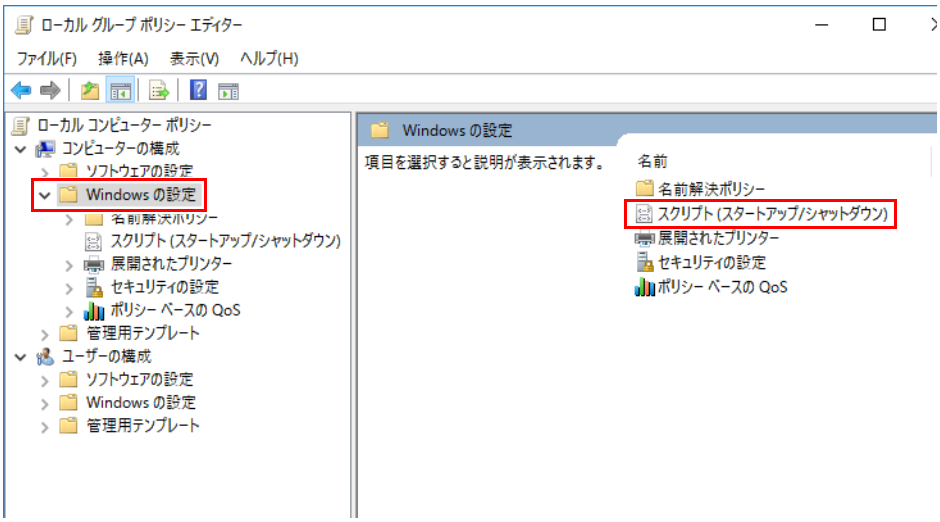
■シャットダウンの設定

ローカルグループポリシーにシャットダウンスクリプトを設定します。

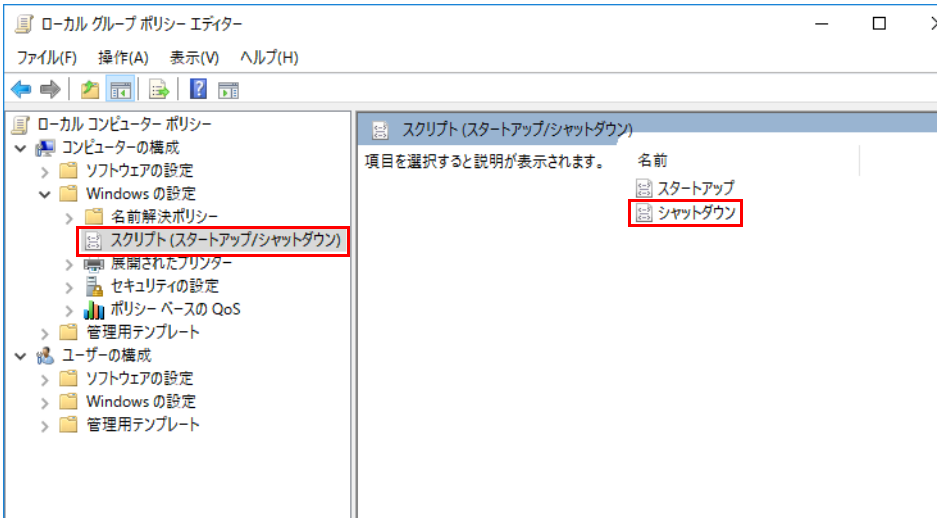
1 管理者権限でコマンドプロンプトを起動します（→ P.7）。

2 「gpedit.msc」を入力し、【Enter】キーを押します。
「ローカルグループポリシーエディター」が起動します。

3 「コンピューターの構成」の「Windows の設定」を選択し、「スクリプト（スタートアップ / シャットダウン）」をダブルクリックします。

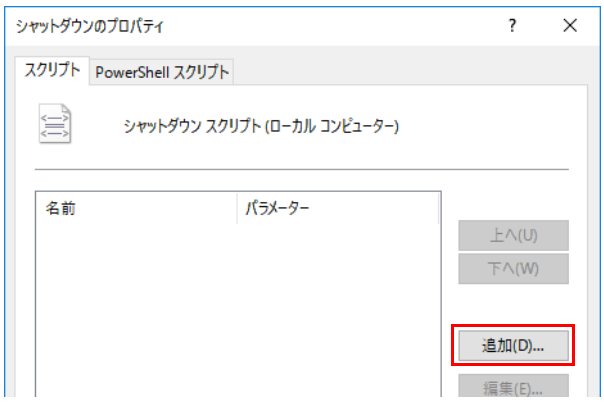


4 「シャットダウン」をダブルクリックします。



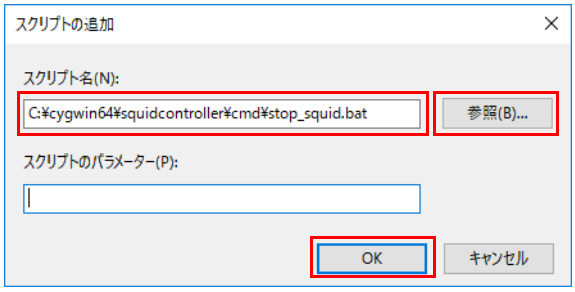
「シャットダウンのプロパティ」が表示されます。

5 「追加」をクリックします。



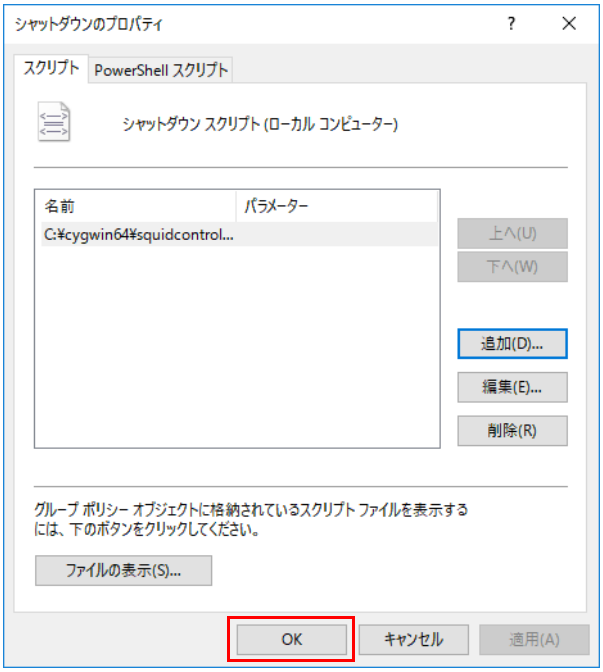
「スクリプトの追加」が表示されます。

6「参照」をクリックし、表示されたウィンドウで、「C:¥cygwin64¥squidcontroller¥cmd¥stop_squid.bat」を選択し、「OK」をクリックします。



「シャットダウンのプロパティ」が表示されます。

7「OK」をクリックします。



8「ローカルグループポリシーエディター」を閉じます。

インターネットキャッシュ機能 V3.0.0 用アップデートモジュールのインストール

「インターネットキャッシュ機能 V3.1.0」（→ P.24）は、本製品に添付されておりません。「インストール補助ツールとインターネットキャッシュ機能 V3.0.0 用アップデートモジュールのダウンロード」（→ P.28）をご覧になり、ダウンロードしてください。

1「インターネットキャッシュ機能 V3.0.0 用アップデートモジュール」をインストールします。
「インターネットキャッシュ機能 V3.0.0 用アップデートモジュール」添付の README.txt に従ってインストールしてください。

親プロキシサーバーの設定

親プロキシサーバーを使用する場合は、本製品に共通のプロキシ設定を行います。親プロキシサーバーを設定しない場合は、この設定は不要です。

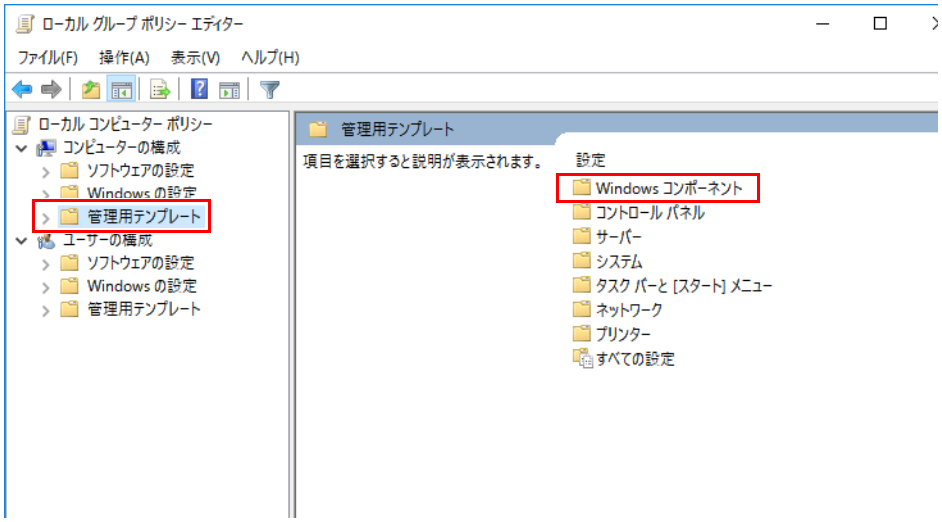
POINT

- お使いのネットワーク環境にプロキシサーバーが設置／設定されている場合は、親プロキシサーバーの設定をしてください。

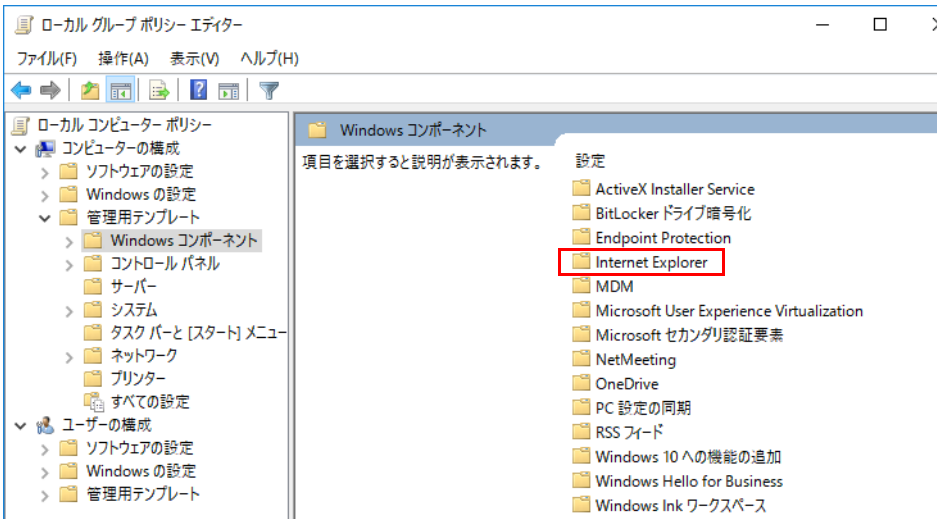
1 **管理者権限でコマンドプロンプトを起動します（→ P.7）。**

2 **「gpedit.msc」を入力し、【Enter】キーを押します。**
「ローカルグループポリシーエディター」が起動します。

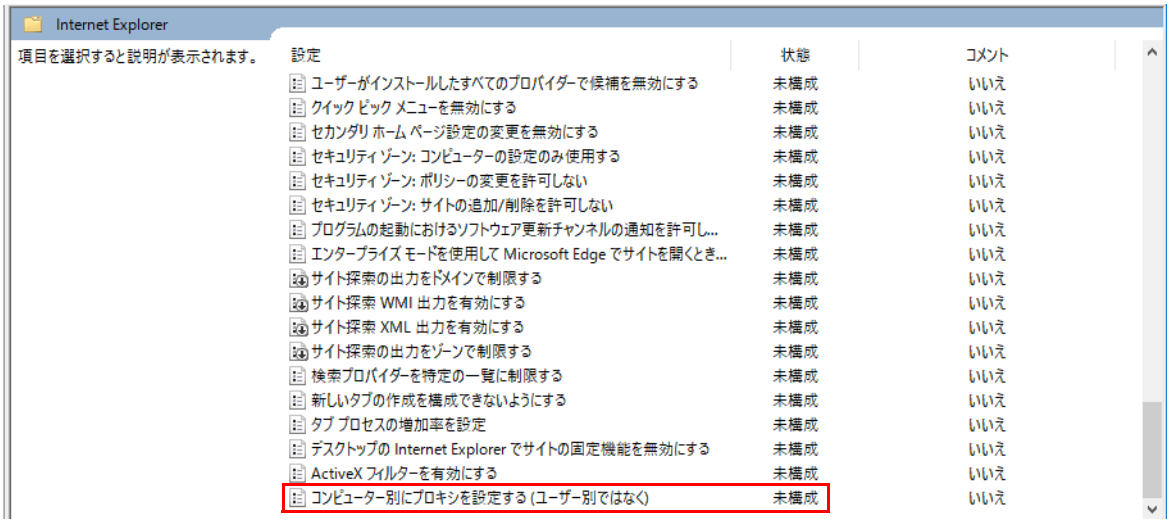
3 **「コンピューターの構成」の「管理用テンプレート」を選択し、「Windows コンポーネント」をダブルクリックします。**



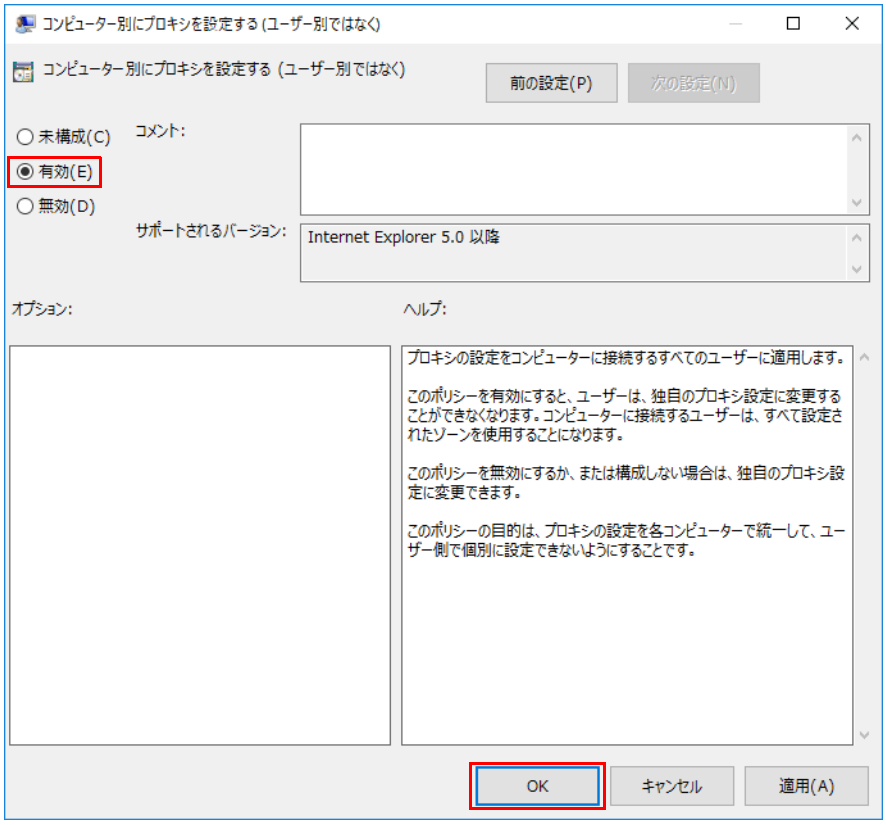
4 **「Internet Explorer」をダブルクリックします。**



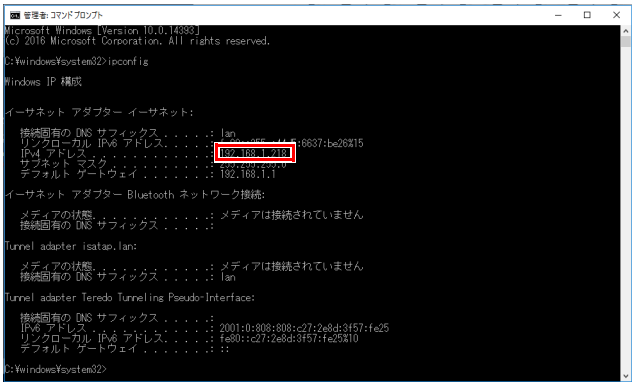
5「コンピューター別にプロキシを設定する（ユーザー別ではなく）」をダブルクリックします。



6「有効」を選択して、「OK」をクリックします。



7 コマンドプロンプトで、「ipconfig」を入力し、【Enter】キーを押します。



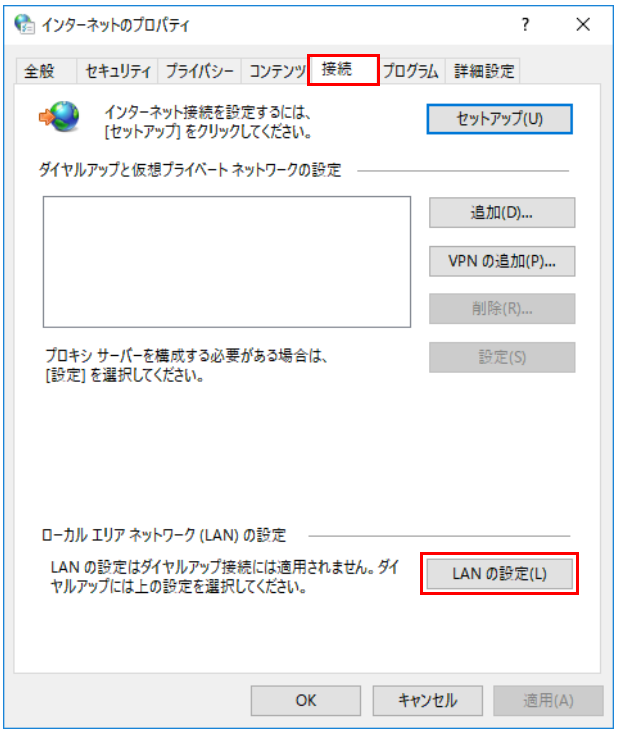
表示された IP アドレスを確認し、メモに控えておいてください。

8「スタート」ボタン→「Windows アクセサリ」の順にクリックします。

9「Internet Explorer」を右クリックし、「その他」→「管理者として実行」の順にクリックします。

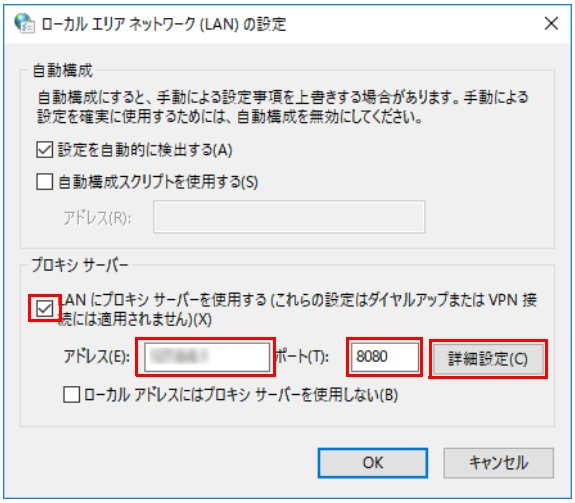
10 Internet Explorer の画面の右上隅の（ツール）→「インターネット オプション」の順にクリックします。
「インターネットのプロパティ」が表示されます。

11「接続」タブをクリックし、「LAN の設定」をクリックします。



「ローカルエリアネットワーク（LAN）の設定」が表示されます。

12 プロキシ サーバーの「LAN にプロキシ サーバーを使用する」にチェックを付け、「アドレス」に親プロキシサーバーの IP アドレス、「ポート」に親プロキシサーバーのポート番号を入力して、「詳細設定」をクリックします。

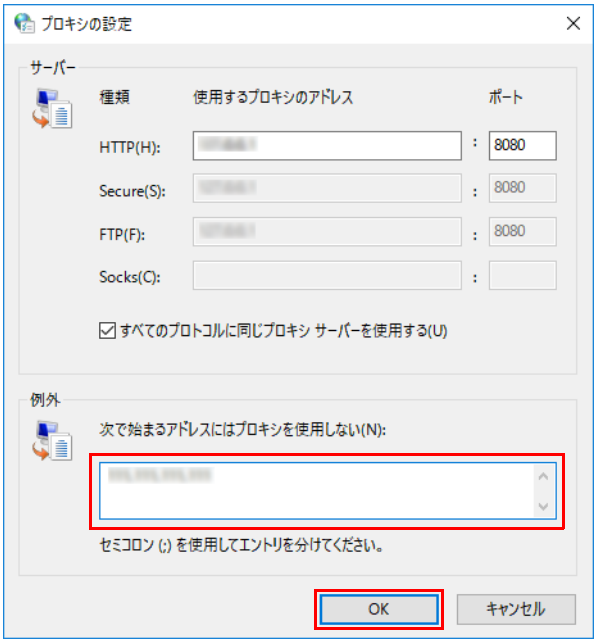


「プロキシ設定」が表示されます。

13「例外」に手順 7 で確認した IP アドレスを入力し、「OK」をクリックします。

POINT

▸ユーザーのネットワーク環境によって、例外の設定が反映されない場合は、手順7で確認したIPアドレスとポートを入力してください。
例:手順7で、IPアドレスが192.168.1.1だった場合、「192.168.1.1:10080」と入力します。



「ローカルエリアネットワーク（LAN）の設定」が表示されます。

14「OK」をクリックします。

インターネットキャッシュ機能の設定

管理画面でインターネットキャッシュ機能の設定を行います。

1　ブラウザーを起動し、管理画面の URL（http://IP アドレス :10080/）に接続します。

POINT

▸IPアドレスにはコンピューター部分のIPアドレスをお使いください。
コンピューター部分のIPアドレスが「192.168.1.3」の場合は次のようになります。
http://192.168.1.3:10080/

▸Internet Explorer で管理画面を表示したときに入力フォームが表示されない場合は、次の設定をご確認ください。
1.Internet Explorer を起動します。
2.画面右上のツールアイコン（設定）→「互換表示設定」の順にクリックします。
「互換性設定の変更」が表示されます。
3.「イントラネットサイトを互換表示で表示する」のチェックを外します。

ログイン画面が表示されます。

2　ブラウザーのキャッシュを削除します。

ブラウザのキャッシュが残っていると管理画面の設定項目が表示されない場合や設定が反映されない場合があります。閲覧履歴のすべての項目にチェックを入れ削除してください。
※OS やブラウザーのアップデートにより、手順が変更になる可能性があります。

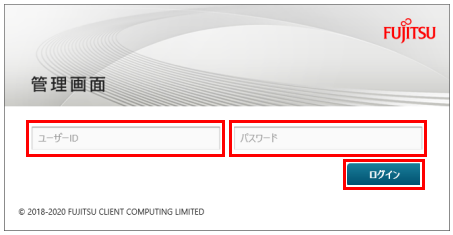
・ Internet Explorer の場合
1. Internet Explorer 11 を起動します。
2. 画面右上にある ツールアイコン（設定）→「インターネット オプション」の順にクリックします。
3. 「全般」タブを選択し、「削除」をクリックします。
4. すべての項目にチェックを付けて、「削除」をクリックします。
5. 「OK」をクリックします。

・ Microsoft Edge（Chromium 版）の場合
1. Microsoft Edge を起動し、…（設定など）→「履歴」→「閲覧データをクリア」の順にクリックします。
2. 「時間の範囲」で「すべての期間」を選択した後、すべての項目にチェックを付けて「今すぐクリア」をクリックします。

・ Google Chrome の場合
1. Google Chrome を起動し、⋮（Google Chrome の設定）→「その他のツール」→「閲覧履歴の削除」の順にクリックします。
「閲覧履歴データの削除」が表示されます。
2. 「詳細設定」の「期間」で「全区間」を選択した後、すべての項目にチェックを付けて「データ消去」をクリックします。

3　ユーザー ID およびパスワードを入力し、「ログイン」をクリックします。

ユーザー ID の初期値は「administrator」です。パスワードは、「パスワードの変更」（→ P.84）で変更した値を入力してください。



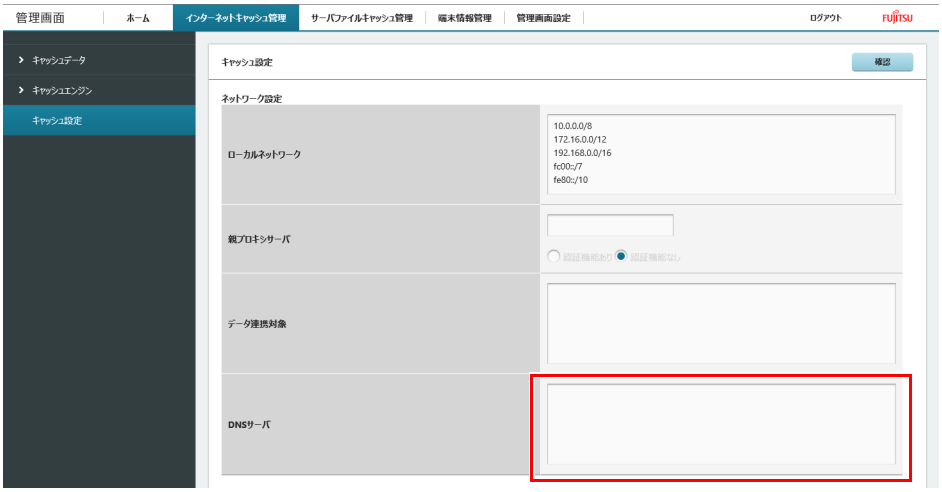
管理画面が表示されます。

4「インターネットキャッシュ管理」の「キャッシュ設定」をクリックします。

データキャッシュ機能を設定する画面が表示されます。

5　ネットワーク設定の「DNS サーバ」を設定します。

DNS サーバーを設定しないと、インターネットの閲覧ができません。必ず連携する DNS サーバーを設定してください。



各項目については、次の表をご覧ください。

項目	説明	
ネットワーク設定		
DNS サーバ	連携する DNS サーバーを指定することができます。	
	最大設定数	4 個
	入力形式	IP アドレス 使用可能文字：半角英数字と「.:-」 例）168.192.10.1 　　168.192.10.2
	デフォルト設定	未設定

6「DNS サーバ」以外のネットワーク設定に関する項目を設定します。

各項目については、次の表をご覧ください。

項目	説明	
ネットワーク設定		
ローカルネットワーク	キャッシュデータを使用するタブレット端末のネットワークの範囲を指定します。指定範囲外のネットワークからのアクセスは拒否されます。設定なしの場合は入力 NG となります。	
	最大設定数	5 個
	入力形式	IP アドレス 使用可能文字：半角英数字と「./:-」 例）10.0.0.0/8 　　fe80::/10
	デフォルト設定	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16 fc00::/7 fe80::/10
親プロキシサーバ	連携するプロキシサーバーを指定することができます。 キャッシュエンジンが受信したリクエストはすべて親プロキシサーバーに転送されます。	
	最大設定数	1 個
	入力形式	IP アドレス : ポート番号 注 ※ ポート番号を指定しない場合、「8080」が設定されます。 使用可能文字：半角英数字と「.:-」 例）168.192.10.1:8080（親プロキシサーバーのポート番号が 8080 の場合）
	デフォルト設定	未設定
	認証機能あり	親プロキシサーバーに認証機能がある場合、認証機能ありに設定してください。親プロキシサーバーの認証 ID とパスワードの入力が求められます。
	認証機能なし	親プロキシサーバに認証機能がない場合、認証機能なしに設定してください。親プロキシサーバーの認証は行いません。
データ連携対象	学校内ネットワークに本製品が複数存在する場合に連携対象のエッジコンピューティングデバイスのIPアドレスを指定します。 連携先エッジコンピューティングデバイスのキャッシュエンジンにデータの有無を問い合わせ、データがある場合は、連携先のキャッシュエンジンからデータを取得します。	
	最大設定数	11 個
	入力形式	IP アドレス 使用可能文字：半角英数字と「.:-」 例）168.192.10.1 　　168.192.10.2
	デフォルト設定	未設定

注　：ご購入時のインターネットキャッシュ機能では、ポートは設定できません。インターネットキャッシュ機能 V3.1.0 またはそれ以降のバージョンにアップデートすると設定することができるようになります。ご購入時のインターネットキャッシュ機能を使用する場合は、IP アドレスのみ記入してください。

7 キャッシュ詳細設定に関する項目を設定します。

各項目については、次の表をご覧ください。

項目	説明	
X-Forwarded-For 注	使用する	親プロキシサーバにリクエストを転送する際に X-Forwarded-For ヘッダにクライアントの IP アドレスの情報が追加されます。
	使用しない	親プロキシサーバにリクエストを転送する際に X-Forwarded-For ヘッダにクライアントの IP アドレスの情報が追加されません。

注　：ご購入時のインターネットキャッシュ機能では、設定できません。インターネットキャッシュ機能 V3.1.0 またはそれ以降のバージョンにアップデートすると項目が表示されて設定することができるようになります。

8 キャッシュデータ制御に関する項目を設定します。

各項目については、次の表をご覧ください。

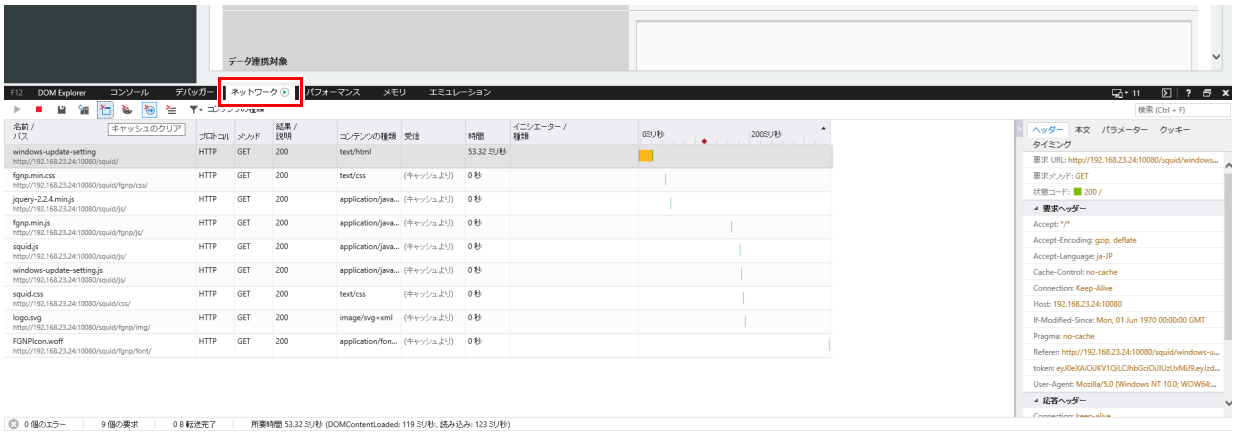
項目	説明	
キャッシュデータ制御		
ホワイトリスト / ブラックリスト	ホワイトリスト	指定された URL のデータがキャッシュ対象となります。URL は正規表現の記述が可能です。
	ブラックリスト	指定された URL のデータがキャッシュ非対象となります。URL は正規表現の記述が可能です。
	設定しない	すべてのデータがキャッシュ対象となります。
	最大設定数	10 個
	入力形式	URL 使用可能文字：半角英数字と「.*+?[]-|()/^$\:」 次の例は正規表現を使ったものとなります。 例）^http://.*\sample\.com/
	デフォルト設定	未設定
	csv アップロード	URL の設定を csv ファイルから入力欄に読み込みます。 アップロード前にホワイトリストまたはブラックリストの選択が必要です。
	csv ダウンロード	設定済みのリストを csv ファイルに出力します。未設定の場合はダウンロードできません。

9「キャッシュ設定」のすべての設定が完了したら、右上にある「確認」をクリックします。

「キャッシュ設定確認」が表示され、変更した設定に「(更新)」と表示されます。

Internet Explorer にて親プロキシサーバで IP アドレスとポート番号を設定し、「確認」ボタンをクリックしたときに「プロキシサーバの入力が正しくありません。」と表示された場合は、次の手順を実施してください。

1. 【F12】キーを押して開発者ツールを表示します。
2. 「キャッシュ設定」を表示します。
3. 「ネットワーク」タブをクリックします。



4. 下図に表示された項目の 1 番上の項目を選択します。

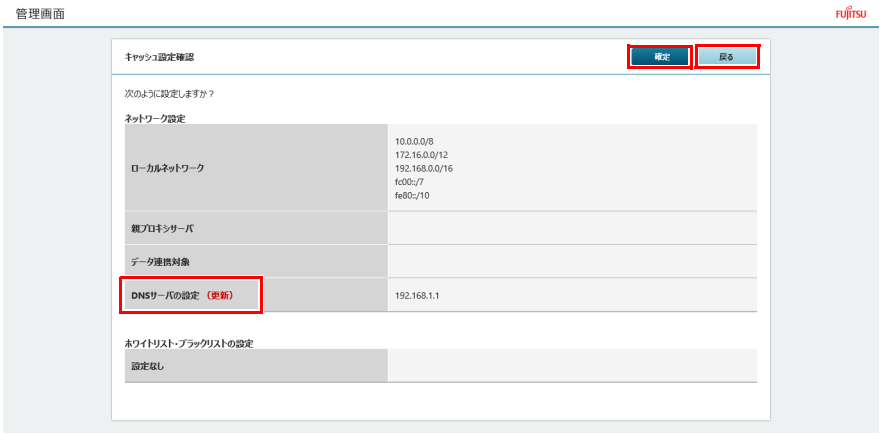
5. （キャッシュクリアアイコン）をクリックします。

キャッシュのクリアを実施してもこの画面上では残ったままになります。

6. 表示されている全ての項目について 1 つずつ手順 4 ～手順 5 を繰り返します。

7. 画面右上にある ツールアイコン（設定）→「インターネット オプション」の順にクリックします。
8. 「全般」タブを選択し、「削除」をクリックします。
9. すべての項目にチェックを付けて、「削除」をクリックします。

10 「OK」をクリックします。**変更が問題ない場合は、「確定」をクリックします。**
修正が必要な場合は、「戻る」をクリックして設定画面に戻ってください。

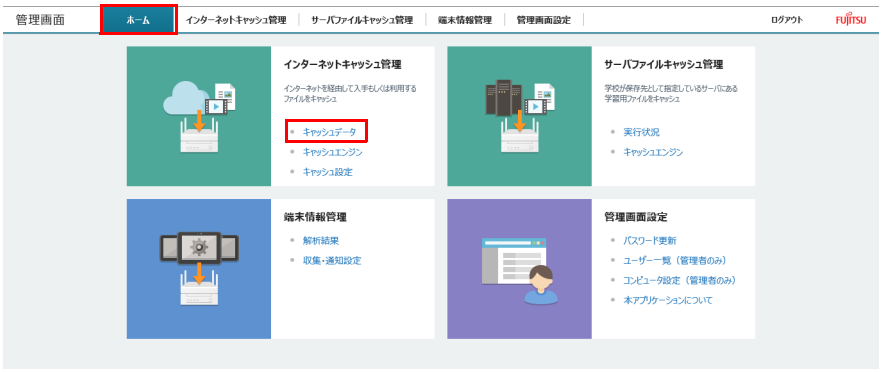


「設定の変更が完了しました。」というメッセージが表示されます。

認証情報を登録する

認証が必要なサイトのキャッシュデータを登録する場合、管理画面で認証情報を登録する必要があります。

1「ホーム」→「キャッシュデータ」の順にクリックします。

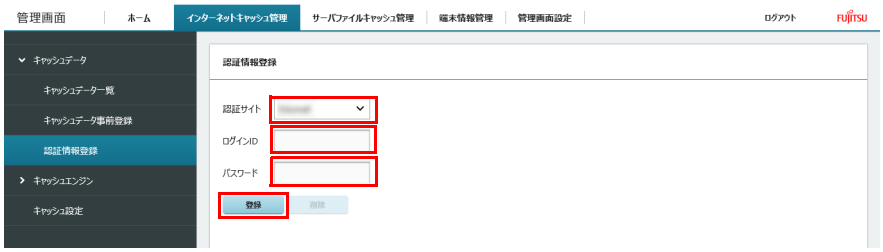


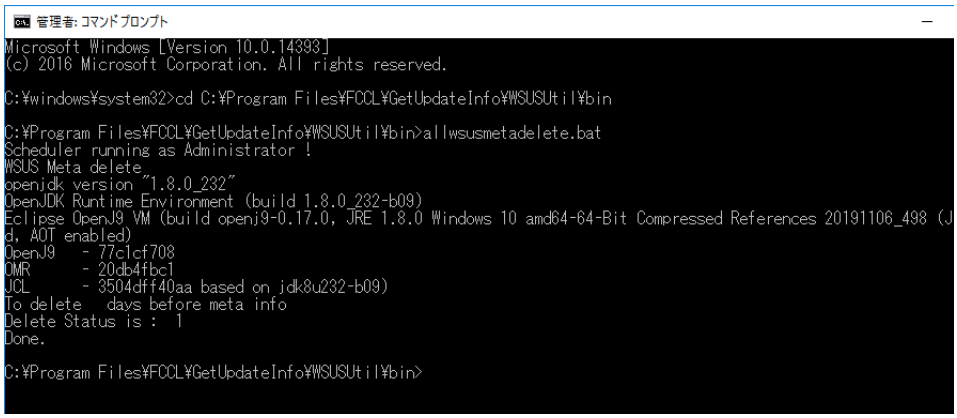
2「認証情報登録」をクリックします。

3「認証サイト」で対象の認証サイトを選択した後、ログイン ID とパスワードを入力し、「登録」をクリックします。

POINT

▸設定可能な認証サイトは EduMall のみです。





サーバファイルキャッシュ機能のインストールと設定

ここでは、サーバファイルキャッシュ機能のインストールと設定について、以下の設定条件を例にインストールおよび設定手順を説明します。実際に利用する環境にあわせて設定してください。

・ 学習支援アプリサーバの IP アドレス　：192.168.0.100
・ 学習支援アプリサーバ内のフルコントロール可能な共有フォルダー　：chietama
・ 管理ファイル格納フォルダー　：conf

事前準備

■学習支援アプリのインストール

サーバファイルキャッシュ機能を使用するためには、本製品に学習支援アプリをインストールする必要があります。インストール手順については、学習支援アプリのマニュアルをご覧ください。

サーバファイルキャッシュ機能のインストール

■フォルダーとファイルの配置

1 「C:¥Fujitsu¥Software¥aplCache」フォルダーを「C:¥」にフォルダーごとコピーします。

2 フォルダーの構成が次のようになっていることを確認します。

フォルダーの構成	
C:¥aplCache¥	aplCacheEngine
	aplCacheUI

サーバファイルキャッシュ機能設定ファイルの変更

■ CommonList.conf 設定ファイルの変更

1　テキストエディターで「C:¥aplCache¥aplCacheEngine¥conf_server¥CommonList.conf」を開き、設定ファイルを変更します。
学校内ネットワークで使用する本製品の台数に応じて、それぞれのコンピューター部分の IP アドレス、コンピューター識別子、クラス名を設定します。
ここでは、学校内ネットワークに本製品を 3 台使用する場合を例に説明します。

```
192.168.0.107,PC1,職員室
192.168.0.111,PC2,3 年 1 組
192.168.0.109,PC3,2 年 1 組
```

クラス名
コンピューター識別子
コンピューター部分の固定 IP アドレス

2　変更後、ファイルを保存して閉じます。

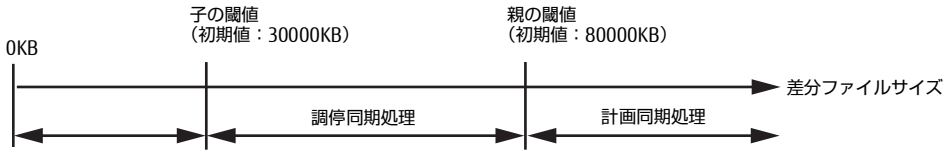
■ CommonSyncParam.conf の変更

同期関連のパラメータを設定します。子の閾値、親の閾値の設定を、システムの構成などに合わせ変更します。

□ 子の閾値、 親の閾値

子の閾値、親の閾値とは、サーバーと本製品と差分が発生した場合、差分ファイルサイズの大きさにより、どのような同期処理を行うのかの指標となる値です。

子の閾値 =30000KB、親の閾値 =80000KB とした場合、次のような同期処理を行います。
- 子の閾値（30000KB）未満の場合、タブレット端末から本製品へのアップロードと同時にサーバーとの同期処理を行います。
- 子の閾値（30000KB）以上～親の閾値（80000KB）未満の場合、タブレット端末から本製品へのアップロードした後、学校内ネットワークの他の本製品と調整しながらサーバーとの同期処理を行います。
- 親の閾値（80000KB）以上の場合、タブレット端末から本製品へのアップロードした後、同期計画対象時間帯にサーバーとの同期処理を行います。



□ 設定ファイルの変更

1　テキストエディターで「C:¥aplCache¥aplCacheEngine¥conf_server¥CommonSyncParam.conf」を開き、設定ファイルを変更します。
- 閾値の設定

```
#-------------------------------------------------------------------------------
# ■子の閾値（同期サイズ）(KB)
#-------------------------------------------------------------------------------
child.SyncSize=30000

#-------------------------------------------------------------------------------
# ■親の閾値（予測時間）( 秒 )
#-------------------------------------------------------------------------------
parent.SyncTime=1800

#-------------------------------------------------------------------------------
# ■親の閾値（同期サイズ）(KB)
#-------------------------------------------------------------------------------
parent.SyncSize=80000
```

子の閾値を入力します。
親の閾値を入力します。

- 同期計画対象時間帯の設定
同期計画を実行する時間帯（例：昼休み、放課後）を設定します。親の閾値以上の同期要件は同期計画対象時間帯に行われます。

```
#-------------------------------------------------------------------
# ■同期計画対象時間帯 (HH:MM)
#-------------------------------------------------------------------
planSync.TimeZone1.Start=12:15
planSync.TimeZone1.End=13:15
planSync.TimeZone2.Start=17:00
planSync.TimeZone2.End=21:00
planSync.TimeZone3.Start=
planSync.TimeZone3.End=
```

12:15 から 13:15 までの時間を同期対象時間帯に設定します。
17:00 から 21:00 までの時間を同期対象時間帯に設定します。

- 日付切替時刻 の設定
日付切替時刻を 1 日の境とし、同期スケジュール管理ファイル、本製品個別同期スケジュール管理ファイルのローテートの基準時間とします。

```
#-------------------------------------------------------------------------------
# ■日付切替時刻 (HH:MM)
#   ※ 同期計画対象時間帯で指定した時間帯に含まれない時刻を設定する
#      (planSync.TimeZone1.Start よりも前、かつ planSync.TimeZone3.End よりも後の時
刻 )
#-------------------------------------------------------------------------------
date.Switching.Time=5:00
```

日付切替時刻を入力します。

2　変更後、ファイルを保存して閉じます。

■ EachSyncParam.conf 設定ファイルの変更

1　テキストエディターで「C:¥aplCache¥aplCacheEngine¥conf¥EachSyncParam.conf」を開き、設定ファイルを変更します。

・学習支援アプリサーバの IP アドレスの設定

```
svrIpAddress=192.168.0.100
```
ここに学習支援アプリサーバの IP アドレスを入力してください。

・一律 DownLink ／ UpLink 優先時間帯
ダウンロードとアップロードの優先同期を実行する時間帯の指定します。
ダウンロード優先時間帯はアップロード同期は 5 回に 1 回の実行頻度となります。
アップロード優先時間帯はダウンロード同期は 5 回に 1 回の実行頻度となる。

```
#-------------------------------------------------------------------------------------------
# ■一律 DownLink/UpLink 優先時間帯 (HH:MM)
#-------------------------------------------------------------------------------------------
priority.DownTimeZone1.Start=07:00
priority.DownTimeZone1.End=17:00
priority.DownTimeZone2.Start=21:00
priority.DownTimeZone2.End=22:00
priority.UpTimeZone1.Start=05:00
priority.UpTimeZone1.End=07:00
priority.UpTimeZone2.Start=22:00
priority.UpTimeZone2.End=05:00
```
7:00 から 17:00 までの時間をダウンロード優先時間帯に設定します。
21:00 から 22:00 までの時間をダウンロード優先時間帯に設定します。
5:00（日付切替時刻）から 7:00 までの時間をアップロード優先時間帯に設定します。
22:00 から 5:00（日付切替時刻）までの時間をアップロード優先時間帯に設定します。

2　変更後、ファイルを保存して閉じます。

□ AplCacheDefault.properties 設定ファイルの変更

1　テキストエディターで「C:¥aplCache¥aplCacheEngine¥jar¥AplCacheDefault.properties」を開き、設定ファイルを変更します。

1. 学習支援アプリサーバの管理ファイル格納フォルダーのパスを入力します。

```
/** 設定ファイル保存場所 ( サーバ ) */
config.file.dir.server = //${SRV_IP_ADDR}/chietama/conf/
```
ここに学習支援アプリサーバの管理ファイル格納フォルダーのパスを入力します。

2. 学習支援アプリサーバの同期対象フォルダーのパスを入力します。
ここでは、学習支援アプリの所属 ID=2 を使用している場合を例に説明します。

```
/** 同期対象ディレクトリ 1 ( サーバ ) */
sync.target.dir.1.server = //${SRV_IP_ADDR}/chietama/files/2/

/** 同期対象ディレクトリ 2 ( サーバ ) */
sync.target.dir.2.server = //${SRV_IP_ADDR}/chietama/files/mybox/2/
```
同期対象フォルダーのパスを入力します。
同期対象フォルダーのパスを入力します。

3. エッジコンピューティングデバイスの同期対象フォルダーパスの設定 (同期元フォルダー設定)
ここでは、学習支援アプリの所属 ID= 2 を使用している場合を例に説明します。

```
/** 同期対象ディレクトリ 1 (MIB) */
sync.target.dir.1.mib = C:/chietama/files/2/

/** 同期対象ディレクトリ 2 (MIB) */
sync.target.dir.2.mib = C:/chietama/files/mybox/2/
```
同期対象フォルダーのパスを入力します。
同期対象フォルダーのパスを入力します。

2　変更後、ファイルを保存して閉じます。

ファイルの配置

1　C:¥aplCache¥aplCacheEngine¥conf_server 配下のファイルを管理ファイル格納フォルダー「conf」（→ P.127）にコピーします。

2　ファイルの構成が次のようになっていることを確認します。

ファイルの構成	
¥¥192.168.0.100¥chietama¥conf¥	CommonList.conf
	CommonMaster.conf
	CommonStatus.csv
	CommonSyncParam.conf
	CommonSyncScheduleList.csv
	CommonSyncScheduleList.csv_org

サービス登録と権限付与

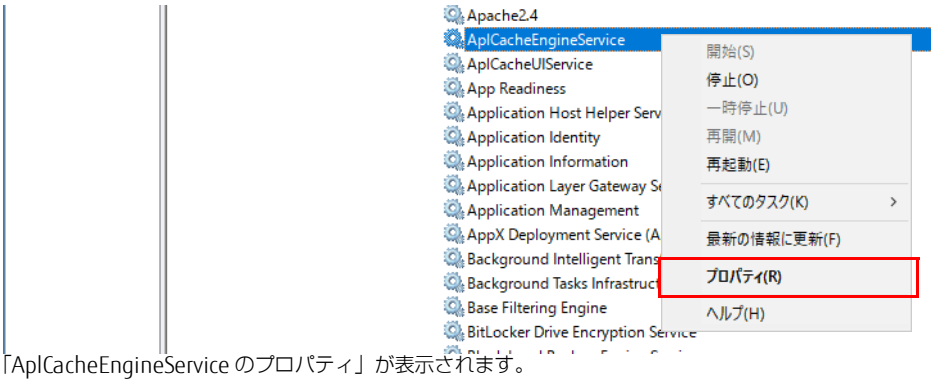
■サーバファイルキャッシュエンジン

1 次のファイルを右クリックし、「管理者として実行」をクリックします。

C:¥aplCache¥aplCacheEngine¥setup¥AplCache_setup.bat

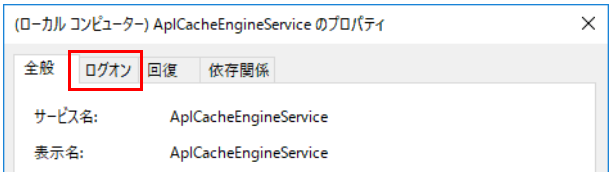
2 「スタート」→「Windows 管理ツール」→「サービス」の順にクリックします。
サービスが起動します。

3 「AplCacheEngineService」を右クリックし、「プロパティ」をクリックします。



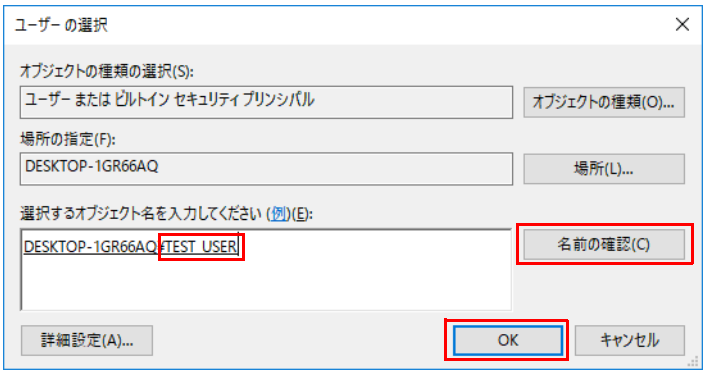
「AplCacheEngineService のプロパティ」が表示されます。

4 「ログオン」タブをクリックします。

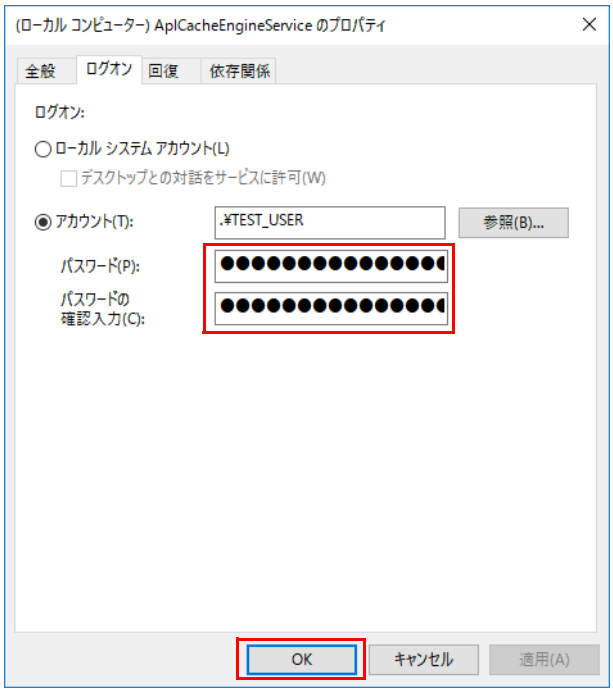


5 「アカウント」を選択し、「参照」をクリックします。

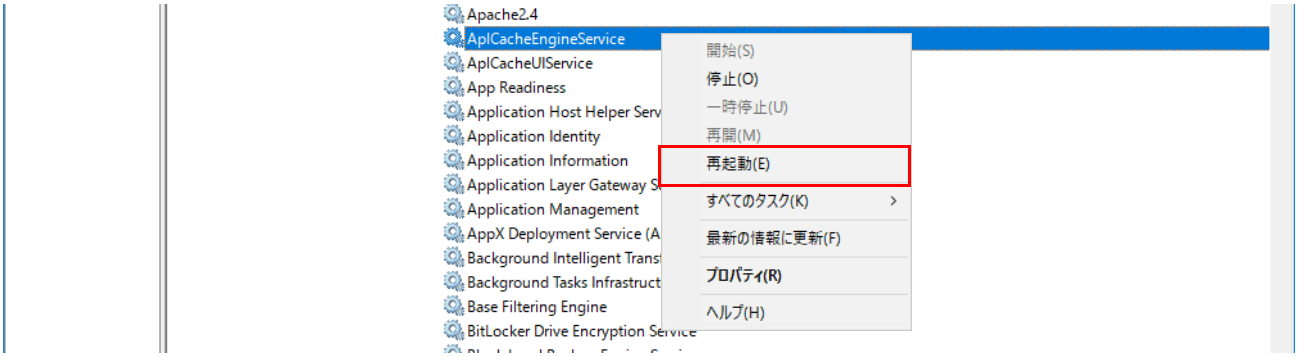
6 「選択するオブジェクト名を入力してください」に、本製品にサインインしているユーザーのアカウント（例：TEST_USER）を入力した後、「名前の確認」をクリックし、「OK」をクリックします。



7 「パスワード」と「パスワードの確認入力」にユーザーアカウントのパスワードを入力し、「OK」をクリックします。



8 サービスの一覧にある「AplCacheEngineService」を右クリックし、「再起動」をクリックします。



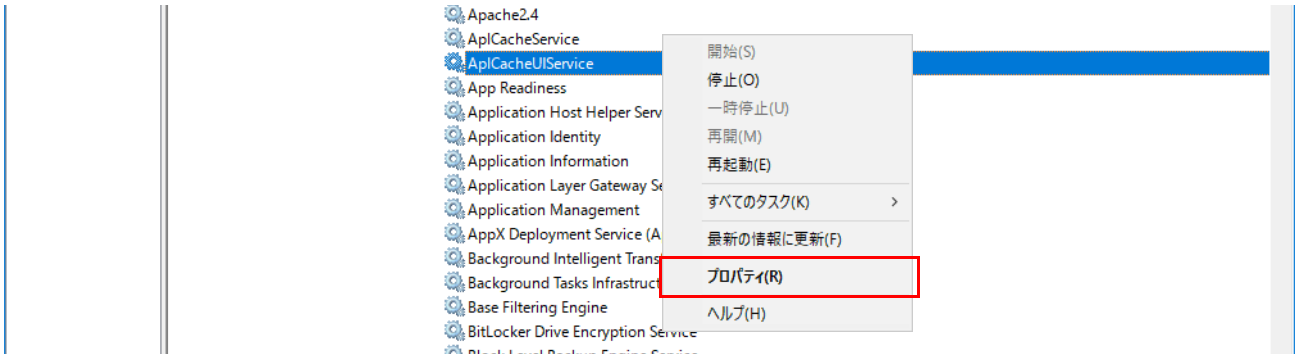
■ サーバファイルキャッシュ UI

1 次のファイルを右クリックし、「管理者として実行」をクリックします。

C:¥aplCache¥aplCacheUI¥setup¥AplCacheUi_setup.bat

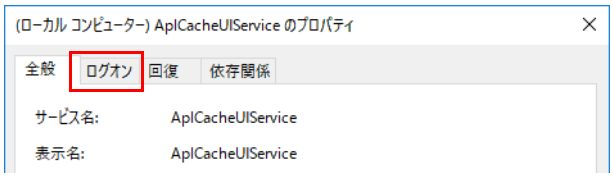
2 「スタート」→「Windows 管理ツール」→「サービス」の順にクリックします。
サービスが起動します。

3 「AplCacheUIService」を右クリックし、「プロパティ」をクリックします。



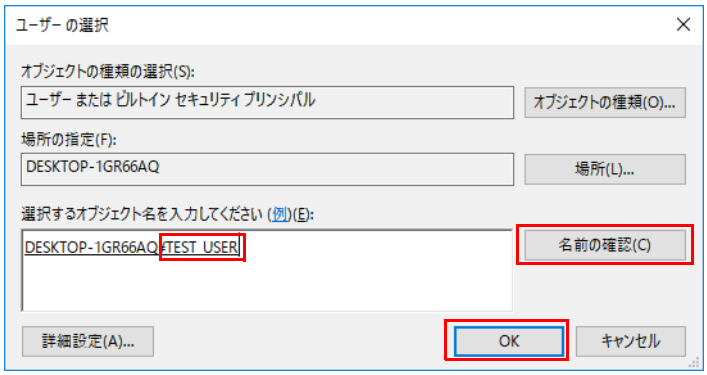
「AplCacheUIService のプロパティ」が表示されます。

4 「ログオン」タブをクリックします。

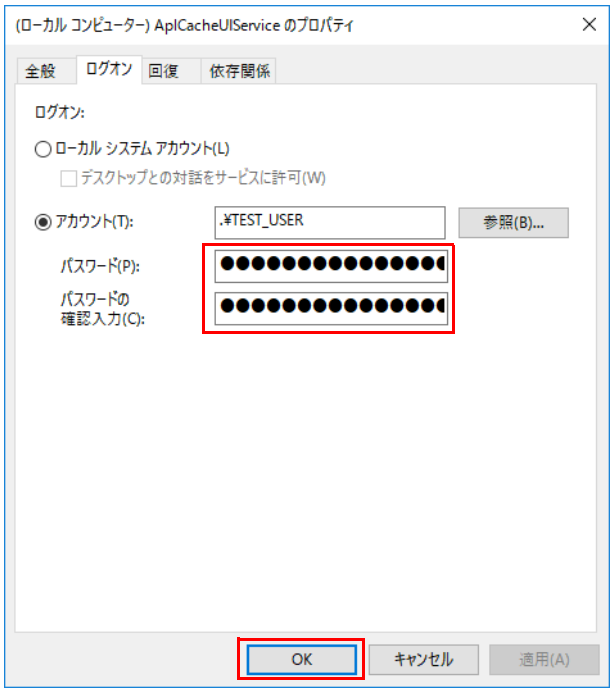


5 「アカウント」を選択し、「参照」をクリックします。

6 「選択するオブジェクト名を入力してください」に、本製品にサインインしているユーザーのアカウント（例：TEST_USER）を入力した後、「名前の確認」をクリックし、「OK」をクリックします。



7「パスワード」と「パスワードの確認入力」にユーザーアカウントのパスワードを入力し、「OK」をクリックします。

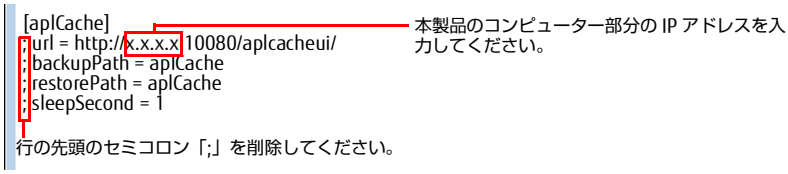


8 サービスの一覧にある「AplCacheUIService」を右クリックし、「再起動」をクリックします。

サーバファイルキャッシュ機能のエクスポート／インポートの設定

■ mib.ini 設定ファイルの変更

1　テキストエディターで「C:¥SmartMaintenance¥mib.ini」を開き、設定ファイルを変更します。
※「x.x.x.x」には、本製品のコンピューター部分の固定 IP アドレスを入力します。



2　ファイルを保存して閉じます。

POINT
▸「対象のフォルダーへのアクセスは拒否されました」というメッセージが表示される場合は、「続行」をクリックします。

3　「C:¥tmp¥mib.ini」がある場合は、「C:¥SmartMaintenance¥mib.ini」を上書きコピーします。

■ 本製品の再起動

1　設定ファイル変更後、本製品を再起動します。

キャッシュエンジンを初期化する

サーバファイルキャッシュ機能のキャッシュエンジンを初期化して再起動します。

1　ブラウザーを起動し、管理画面の URL（http://IP アドレス :10080/）に接続します。

POINT

▸IPアドレスにはコンピューター部分のIPアドレスをお使いください。
コンピューター部分のIPアドレスが「192.168.1.3」の場合は次のようになります。
http://192.168.1.3:10080/

ログイン画面が表示されます。

2　ユーザー ID およびパスワードを入力し、「ログイン」をクリックします。
ユーザー ID「administrator」と「パスワードの変更」（→ P.84）で変更したパスワードを入力してください。

3「ホーム」→「キャッシュエンジン」の順にクリックします。

4「キャッシュエンジン制御」をクリックし、「停止」をクリックします。

「エンジンキャッシュを停止しました。」というメッセージが表示されます。

5「OK」をクリックします。

6「個別設定」をクリックし、「初期化」をクリックします。

「エンジンキャッシュを初期化します。よろしいですか？」というメッセージが表示されます。

7「はい」をクリックします。
しばらくすると、「キャッシュエンジンを初期化しました。」というメッセージが表示されます。

8「OK」をクリックします。

9「キャッシュエンジン制御」をクリックし、「起動」をクリックします。

「エンジンキャッシュを起動しました。」というメッセージが表示されます。

10「OK」をクリックします。

4. 基本機能 - データキャッシュ機能 （タブレット端末）

インターネットキャッシュ機能設定

プロキシの設定

プロキシの設定は、「プロキシの設定」（→ P.91）で完了しています。

サーバキャッシュ機能設定

学習支援アプリの設定を行ってください。必要な手順については学習支援アプリのマニュアルをご覧ください。

5. 基本機能 - 状態監視 （製品本体）

インストール補助ツールを使用する （動作状態監視ツール）

「インストール補助ツール」（→ P.23）は、本製品に添付されておりません。「インストール補助ツール」を使用する場合は、「インストール補助ツールとインターネットキャッシュ機能 V3.0.0 用アップデートモジュールのダウンロード」（→ P.28）をご覧になり、ダウンロードしてください。

ダウンロード後、「BasicFunction_WatchProcessApp_Install.cmd」を実行してください。なお、バッチファイルは、必ず、管理者権限のアカウントで実行してください。次のインストールと設定が自動で行われます。

「動作状態監視ツールのインストール」（→ P.138）～「SmtpSetting.txt 設定ファイルの変更」（→ P.140）

バッチファイルの実行が完了したら、動作状態監視ツールのインストールと設定は、すべて完了します。
なお、「インストール補助ツール」（→ P.23）を使用しない場合は、本マニュアルに沿ってインストールと設定を行ってください。

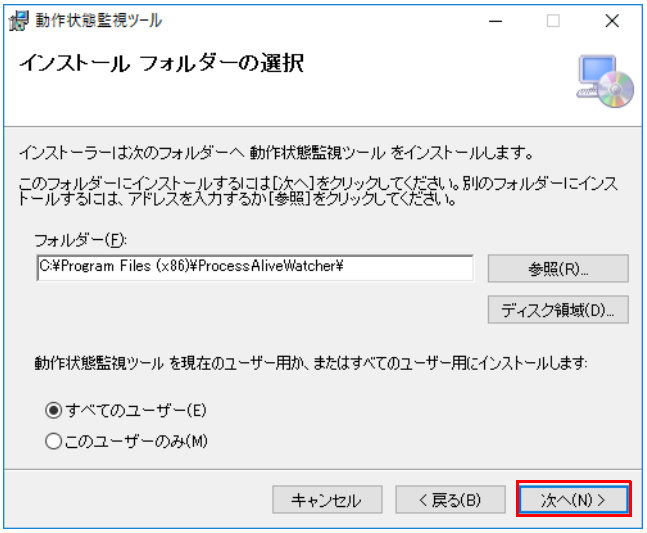
動作状態監視ツールのインストール

製品本体に、動作状態監視ツールをインストールします。

1 「C:¥SmartMaintenance¥Other¥ 動作状態監視ツール ¥WatchProcessAppSetup.msi」を実行します。
「セットアップ ウィザード」が表示されます。

2 「次へ」をクリックします。
「インストール フォルダーの選択」が表示されます。

3 「すべてのユーザー」を選択し、「次へ」をクリックします。



「インストールの確認」が表示されます。

4 「次へ」をクリックします。
インストールが開始します。

POINT
▸「ユーザーアカウント制御」が表示された場合は、「はい」をクリックします。

5 「閉じる」をクリックします。

動作状態監視ツールの設定

動作状態監視ツールの設定を行います。

WatchProcessApp.ini 設定ファイルの変更

動作状態監視ツールをインストール後、次の設定を行ってください。

1 次のファイルをデスクトップにコピーします。

C:¥Program Files¥FCCL¥ProcessAliveWatcher¥Ini¥WatchProcessApp.ini

2 コピーした「WatchProcessApp.ini」をテキストエディターで開き、設定ファイルを変更します。

・[WlanDiagnosis] セクション

```
[WlanDiagnosis]
ProcessEnable=True
ProcessKind=service
RebootFilePath=C:\SmartMaintenance\bat\start_WlanDiagnosi
```

「False」に変更します。

・[Intel Unite] セクション

```
[[Intel Unite]
ProcessEnable=True
ProcessKind=exe
RebootFilePath=C:\SmartMaintenance\bat\start_unite.bat;
```

「False」に変更します。

3 変更後、ファイルを保存して閉じます。

4 デスクトップの「WatchProcessApp.ini」設定ファイルを次のフォルダーに移動して、既存のファイルと置換します。

C:¥Program Files¥FCCL¥ProcessAliveWatcher¥Ini¥WatchProcessApp.ini

POINT

▸「対象のフォルダーへのアクセスは拒否されました」というメッセージが表示される場合は、「続行」をクリックします。

監視結果の送付先の設定

本製品の動作状態監視ツールが、診断結果／ログファイルを送信する先のメールアドレスを設定します。

■ MailSetting.ini 設定ファイルの変更

1 次のファイルをデスクトップにコピーします。

C:¥Program Files¥FCCL¥ProcessAliveWatcher¥Ini¥MailSetting.ini

2 コピーした「MailSetting.ini」をテキストエディターで開き、設定ファイルを変更します。

```
[setting]
; メールタイトルのテンプレート（最大 255 文字）
Title=【 [PC 名 ] 通知】([ メールアカウント名 ])([ 対象 ] 診断通
知）[ 発生日時 ]
; メール本文のテンプレート
Text=[ 発生日時 ][ 対象 ][ 検知した内容 ]
; メール出力先アドレス（'|」( 半角のパイプ ) で複数のメールア
ドレスを区切る）
ToMailAddress=xxx@example.com
```

送信先のメールアドレスを入力してください。

送付先のメールアドレスを複数設定する場合は、メールアドレスの間に「|」を入力してください。
例：test_user1@fccl.com|test_user2@fccl.com

3 変更後、保存してファイルを閉じます。

4 デスクトップの「MailSetting.ini」設定ファイルを次のフォルダーに移動して、既存のファイルと置換します。

C:¥Program Files¥FCCL¥ProcessAliveWatcher¥Ini¥MailSetting.ini

POINT

▸「対象のフォルダーへのアクセスは拒否されました」というメッセージが表示される場合は、「続行」をクリックします。

■ SmtpSetting.txt 設定ファイルの変更

SMTP サーバーの情報について設定します。

1 次のファイルをデスクトップにコピーします。

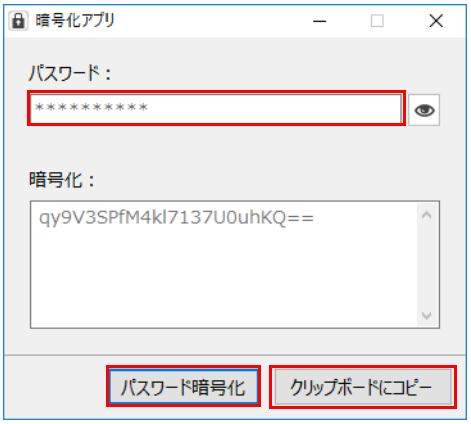
C:¥Program Files¥FCCL¥ProcessAliveWatcher¥Ini¥SmtpSetting.txt

2 コピーした「SmtpSetting.txt」をテキストエディターで開き、設定ファイルを変更します。

;SMTP サーバー名（ホスト名、または IP アドレス）
Server=xxx.xxx.xxx.xxx　→ SMTP サーバーの IP アドレスを指定します。
;SMTP ポート番号
Port=xxx　→ SMTP サーバーで利用するポート番号を指定します。
; 差出人メールアドレス
FromAddress=xxx@example.com　→ 通知メールの差出人のメールアドレスを指定します。
; エンコード（UTF-8,ISO-2022-JP）
Encode=UTF-8　→ 文字のエンコードの種類を指定します。「UTF-8」と「ISO-2022-JP」のどちらかを指定します。
; メール送信認証設定（NONE,PLAIN,LOGIN）
Auth=LOGIN　→ SMTP サーバーの認証が必要なときに、認証方法とユーザー ID、パスワードなどを指定します。認証方法は、「認証なし」「SMTP Auth(PLAIN)」「SMTP Auth(LOGIN)」から指定します。それぞれの指定方法は次のとおりです。
「認証なし」：「NONE」
「SMTP Auth(PLAIN)」：「PLAIN」
「SMTP Auth(LOGIN)」：「LOGIN」
; ユーザー ID（暗号化なし）
; メール送信認証設定に「NONE」が指定された場合、本値は無視する
UserID=xxx　→ SMTP サーバーにログオンするためのアカウント名を指定します。
; パスワード（別途提供するツールにて暗号化）
; メール送信認証設定に「NONE」が指定された場合、本値は無視する
Pass=xxx　→ SMTP サーバーにログオンするためのパスワードを暗号化して指定します。

重要

パスワードは、暗号化アプリで暗号化した文字列を指定してください。



1. 「C:¥SmartMaintenance¥Other¥ 暗号化アプリ ¥PasswordEncoder.exe」を実行します。
2. 「パスワード」にパスワードを入力します。
3. 「パスワード暗号化」をクリックします。
4. 「クリップボードにコピー」をクリックします。

3 変更後、保存してファイルを閉じます。

4 デスクトップの「SmtpSetting.txt」設定ファイルを次のフォルダーに移動して、既存のファイルと置換します。

C:¥Program Files¥FCCL¥ProcessAliveWatcher¥Ini¥SmtpSetting.txt

POINT

▸「対象のフォルダーへのアクセスは拒否されました」というメッセージが表示される場合は、「続行」をクリックします。

お手入れナビのインストール

製品本体に、お手入れナビをインストールします。インストールは、必ず、管理者権限のアカウントで行ってください。

1 「C:¥Fujitsu¥Software¥Oteire¥setup.exe」を実行します。
以降の操作は、表示された画面に従って、設定を変えずに行ってください。

お手入れナビの設定

本アプリの設定を変更することにより、空冷用通風路のお手入れの通知時期の変更や、メッセージを表示させないようにできます。
通知時期を変更する方法については、「お手入れナビ」のヘルプをご覧ください。

POINT

- **「お手入れナビ」のヘルプは、次の操作で表示されます。**
  1. 「スタート」ボタン→「FUJITSU - お手入れナビ」→「ヘルプ」の順にクリックします。

6. 拡張機能 - セキュリティ （製品本体）

インストール補助ツールを使用する （端末認証）

「インストール補助ツール」（→ P.23）は、本製品に添付されておりません。「インストール補助ツール」を使用する場合は、「インストール補助ツールとインターネットキャッシュ機能 V3.0.0 用アップデートモジュールのダウンロード」（→ P.28）をご覧になり、ダウンロードしてください。

ダウンロード後、バッチファイルを実行する前に、次の設定を行ってください。なお、バッチファイルは、必ず、管理者権限のアカウントで実行してください。

●「アクセスポイントの設定」（→ P.143）

●「Docker for Windows のインストール」（→ P.144）

●「Docker for Windows の設定」（→ P.145）

設定が完了したら、「01_ExtensionFunction_Auth_Install.cmd」を実行した後、「02_ExtensionFunction_Auth_Install.cmd」を実行してください。
次のインストールと設定が自動で行われます。

「Node.js のインストール」（→ P.145）～「管理アプリケーション（UI 部）の起動」（→ P.167）

バッチファイルの実行が完了したら、「拡張機能 - セキュリティ（タブレット端末）」（→ P.168）からインストールと設定を進めてください。
なお、「インストール補助ツール」（→ P.23）を使用しない場合は、本マニュアルに沿ってインストールと設定を行ってください。

端末認証機能

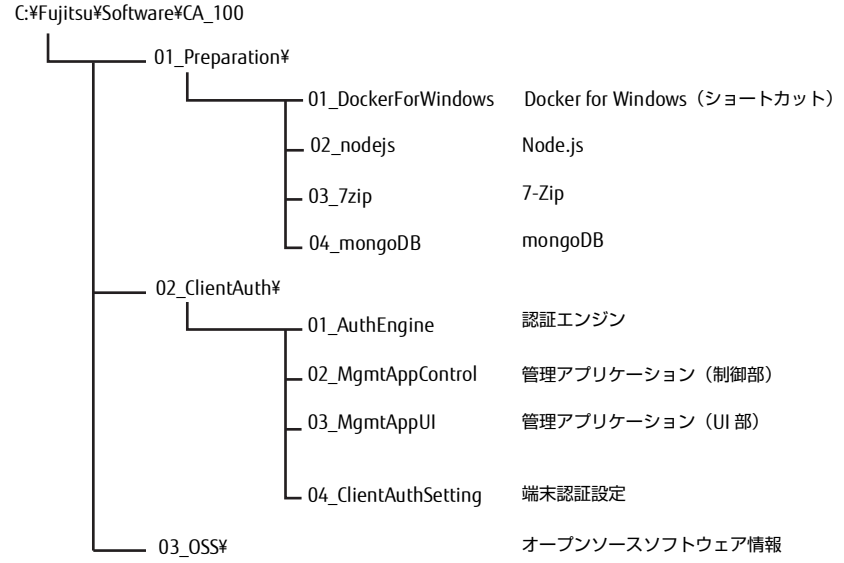
ここでは、「端末認証」に必要な設定を記載します。

POINT

- Intel Uniteをインストールしていた場合、本製品を起動すると、Intel Uniteが自動起動します。「端末認証」のインストールや各種設定を行う場合は、「仮想デスクトップを使用する」（→P.194）をご覧になり、仮想ディスプレイを使用してインストールや設定を行ってください。
- 「端末認証」のインストール、各種設定、および操作は、必ず、管理者権限のアカウントで行ってください。

端末認証用フォルダーについて

端末認証用フォルダーには、端末認証で必要なアプリが格納されています。フォルダー構成は次のとおりです。



アクセスポイントの設定

SSID の認証モードを「WPA2 Enterprise」に設定します。ここでは、基本設定の設定方法について説明します。

重要

▶複数のSSIDを使用する場合は、端末認証機能を適用するすべてのSSIDについて、認証モードを「WPA2 Enterprise」に設定してください。

1 アクセスポイントの Web 設定画面にログインします（→ P.39）。
「パスワードの変更」（→ P.40）で変更したパスワードを入力してください。

2「詳細設定」→「ネットワーク」→「無線」の順にクリックします。

3「周波数帯」を「5GHz」を選択した後、「認証モード」で「WPA2 Enterprise」を選択し、「適用」をクリックします。

Docker for Windows のインストール

POINT

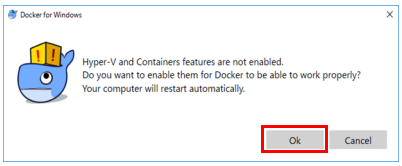
- Docker for Windowsをインストールすると、Intel Uniteの画面に表示されるクライアントのダウンロード元のURLが変わりますが、「メトリックの設定」（→ P.159）を実行後に、元のURLに戻ります。

1 次のインターネットリンクファイルを実行します。
C:¥Fujitsu¥Software¥CA_100¥01_Preparation¥01_DockerForWindows¥DockerForWindows

ブラウザーが起動し、「Docker for Windows」のダウンロードサイトにアクセスします。

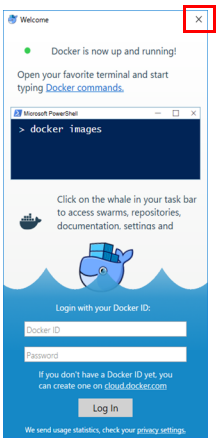
2 ダウンロードしたインストーラーを本製品で実行し、画面の指示に従ってインストールします。

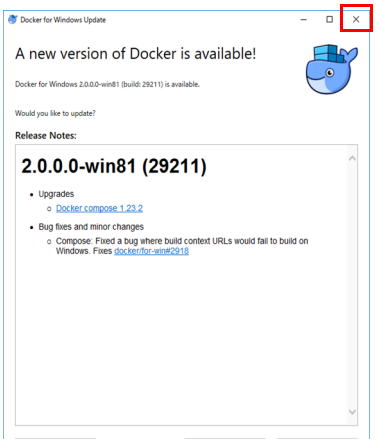
3 インストール後に Windows にログインし、以下の Hyper-V の有効化を選択する画面が表示された場合は、「OK」をクリックします。



POINT

- Hyper-Vが有効になった後、本製品は、再起動します。
- コミュニティへの参加をうながす画面やバージョンアップをうながす画面が表示された場合は、× をクリックしてください。





■ Hyper-V 有効化の確認

1 「コントロールパネル」を表示します（→ P.7）。
「コントロールパネル」が表示されます。

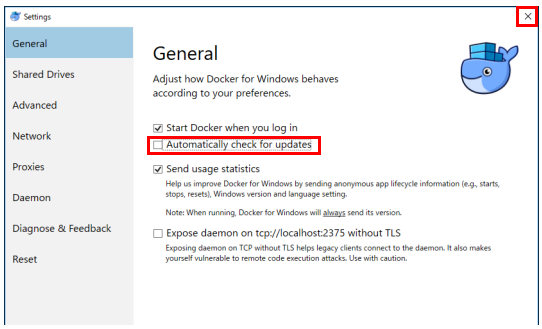
2 「プログラム」→「Windows の機能の有効化または無効化」をクリックします。
「Windows の機能」が表示されます。

3 次の項目にチェックが付いていることを確認します。
Hyper-V
Hyper-V プラットフォーム
Hyper-V Hypervisor
Hyper-V サービス
Hyper-V 管理ツール
Hyper-V GUI 管理ツール
Windows PowerShell 用 Hyper-V モジュール

Docker for Windows の設定

1 **画面右下の通知領域の  を右クリックし、表示されたメニューから「Setting...」を選択します。**
「General」が表示されます。

2 **「Automatically check for updates」のチェックを外し、画面右上の × をクリックします。**



Node.js のインストール

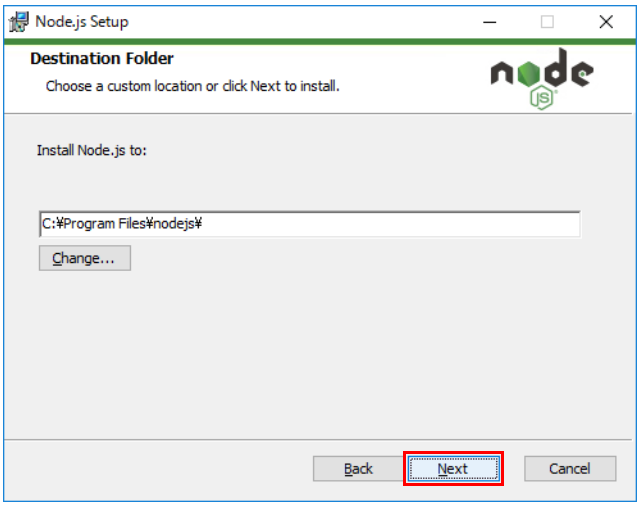
1 **「C:¥Fujitsu¥Software¥CA_100¥01_Preparation¥02_nodejs¥node-v12.14.1-x64.msi」を実行します。**
Setup Wizard が表示されます。

2 **「Next」をクリックします。**
「End-User License agreement」が表示されます。

3 **License Agreement を確認したら、「I accept the terms in the License Agreement」にチェックを付け、「Next」をクリックします。**

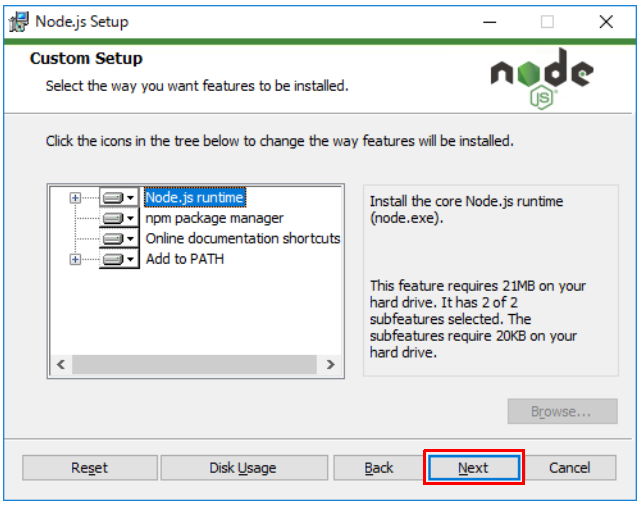
「Destination Folder」が表示されます。

4 **「Next」をクリックします。**



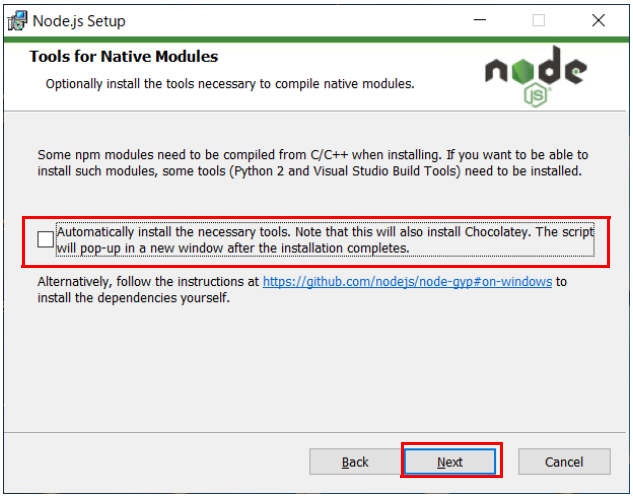
「Custom Setup」が表示されます。

5 「Next」をクリックします。



「Tools for Native Modules」が表示されます。

6 チェックボックスのチェックを外し、「Next」をクリックします。



「Ready to Install Node.js」が表示されます。

7 「Next」をクリックします。

8 「Install」をクリックします。

POINT

▸「ユーザーアカウント制御」が表示された場合は、「はい」をクリックします。

インストールが開始します。しばらくすると、インストールが完了します。

9 「Finish」をクリックします。

10 本製品を再起動します。

11 管理者権限でコマンドプロンプトを起動します（→ P.7）。

12 次のコマンドを入力して【Enter】キーを押し、「v12.14.1」が表示されることを確認します。

```
node -v
```

13 次のコマンドを入力して【Enter】キーを押し、「6.13.4」が表示されることを確認します。

```
npm -v
```

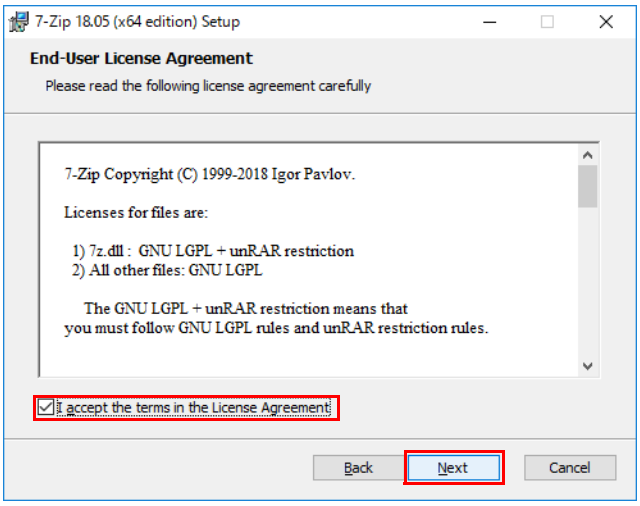
14 コマンドプロンプトを終了します。

7-Zip のインストール

1 「C:¥Fujitsu¥Software¥CA_100¥01_Preparation¥03_7zip¥7z1805-x64.msi」を実行します。
Setup Wizard が表示されます。

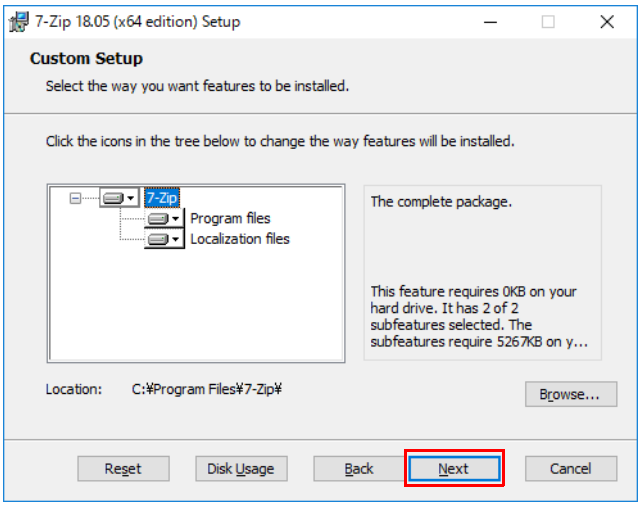
2 「Next」をクリックします。
「End-User License agreement」が表示されます。

3 License Agreement を確認したら、「I accept the terms in the License Agreement」にチェックを付け、「Next」をクリックします。



「Custom Setup」が表示されます。

4 「Next」をクリックします。



「Ready to Install」が表示されます。

5 「Install」をクリックします。

POINT

▸「ユーザーアカウント制御」が表示された場合は、「はい」をクリックします。

インストールが開始します。しばらくすると、インストールが完了します。

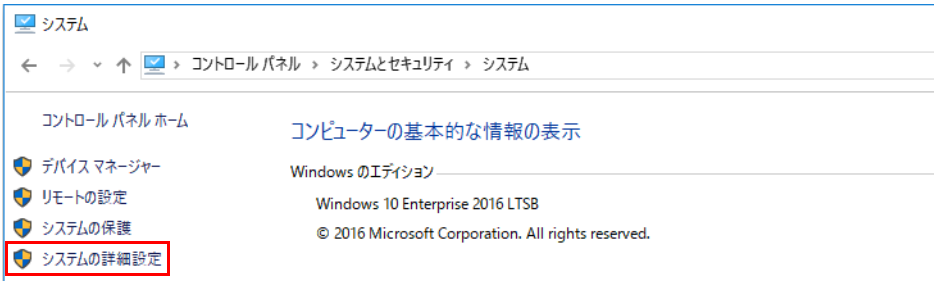
6 「Finish」をクリックします。

7-zip の設定

1「コントロールパネル」を表示します（→ P.7）。
「コントロールパネル」が表示されます。

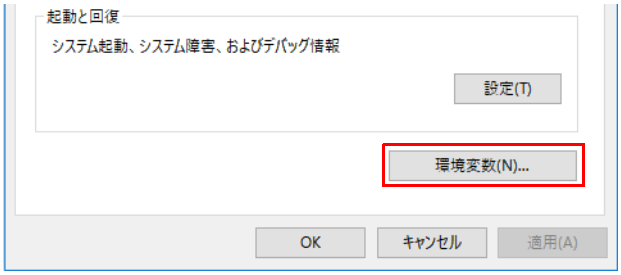
2「システムとセキュリティ」→「システム」の順にクリックします。

3「システムの詳細設定」をクリックします。



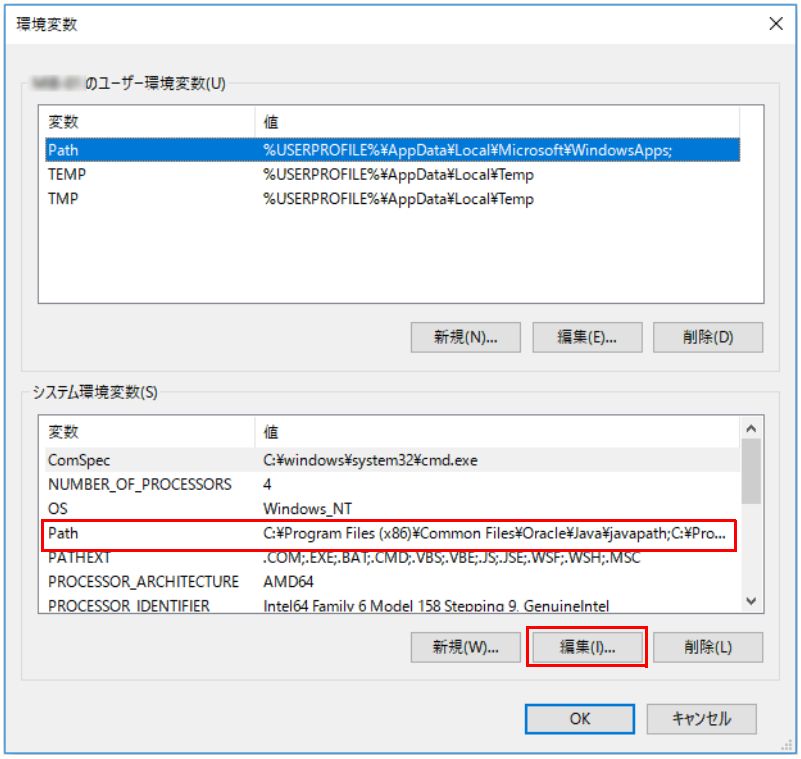
「システムのプロパティ」が表示されます。

4「環境変数」をクリックします。



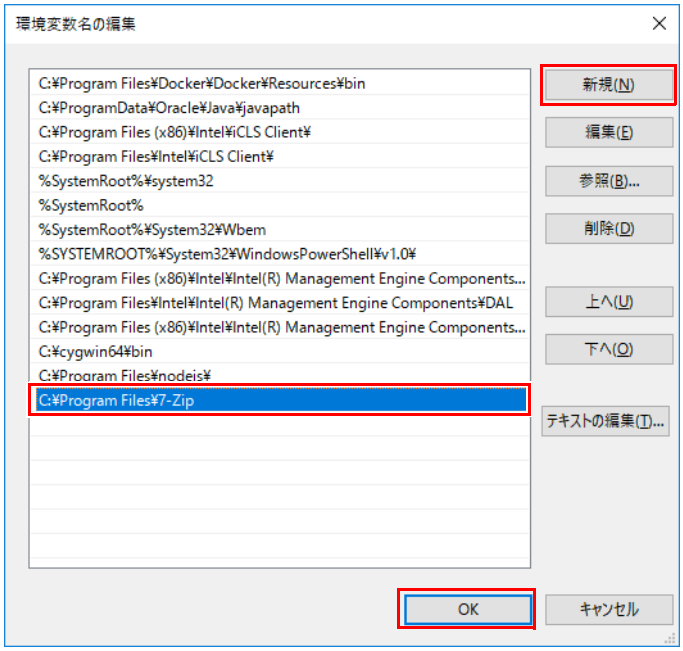
「環境変数」が表示されます。

5「システム環境変数」の「Path」をクリックし、「編集」をクリックします。



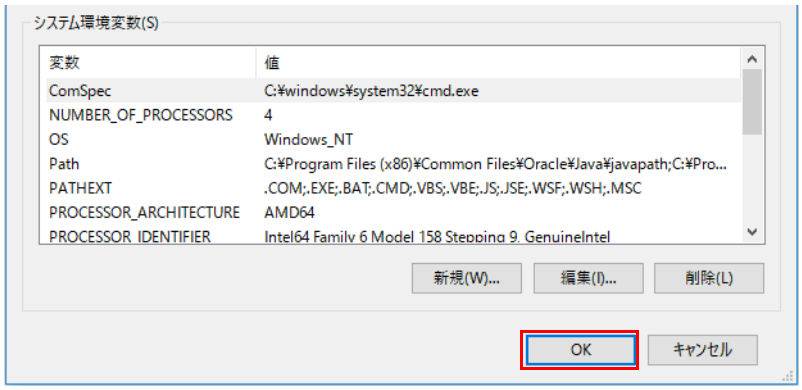
「環境変数名の編集」が表示されます。

6「新規」をクリックし、最後行に表示されたテキストボックスに「C:¥Program Files¥7-Zip」を入力し、「OK」をクリックします。



「環境変数」が表示されます。

7「OK」をクリックします。

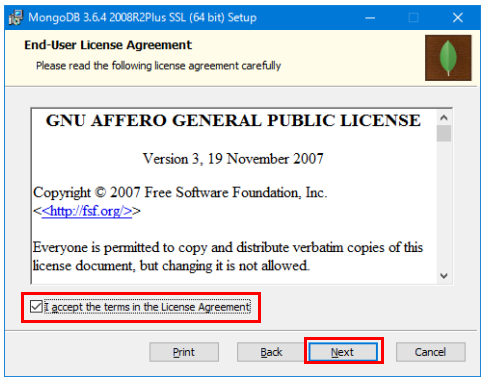


mongoDB のインストール

1 **「C:¥Fujitsu¥Software¥CA_100¥01_Preparation¥04_mongoDB¥mongodb-win32-x86_64-2008plus-ssl-3.6.4-signed.msi」を実行します。**
Setup Wizard が表示されます。

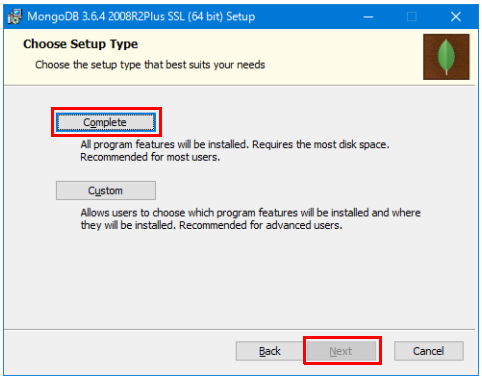
2 **「Next」をクリックします。**
「End-User License agreement」が表示されます。

3 **License Agreement を確認したら、「I accept the terms in the License Agreement」にチェックを付け、「Next」をクリックします。**



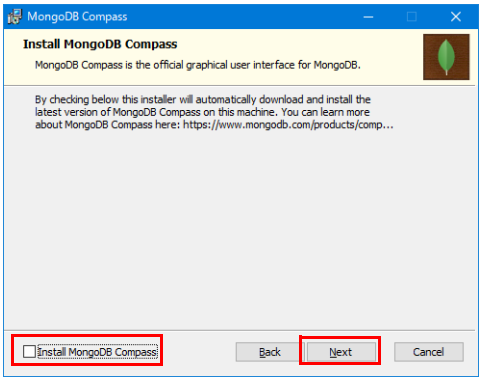
「Choose Setup Type」が表示されます。

4 **「Complete」をクリックし、「Next」をクリックします。**



「Install MongoDB Compass」が表示されます。

5 **「Install MongoDB Compass」のチェックを外し、「Next」をクリックします。**



「Ready to Install」が表示されます。

6 **「Install」をクリックします。**

POINT
▸「ユーザーアカウント制御」が表示された場合は、「はい」をクリックします。

インストールが開始します。しばらくすると、インストールが完了します。

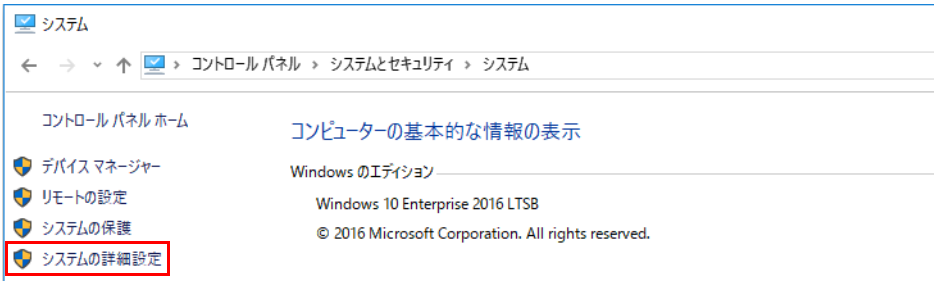
7 **「Finish」をクリックします。**

mongoDB の設定

1「コントロールパネル」を表示します（→ P.7）。
「コントロールパネル」が表示されます。

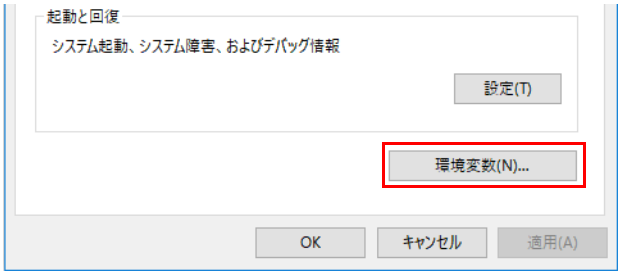
2「システムとセキュリティ」→「システム」の順にクリックします。

3「システムの詳細設定」をクリックします。



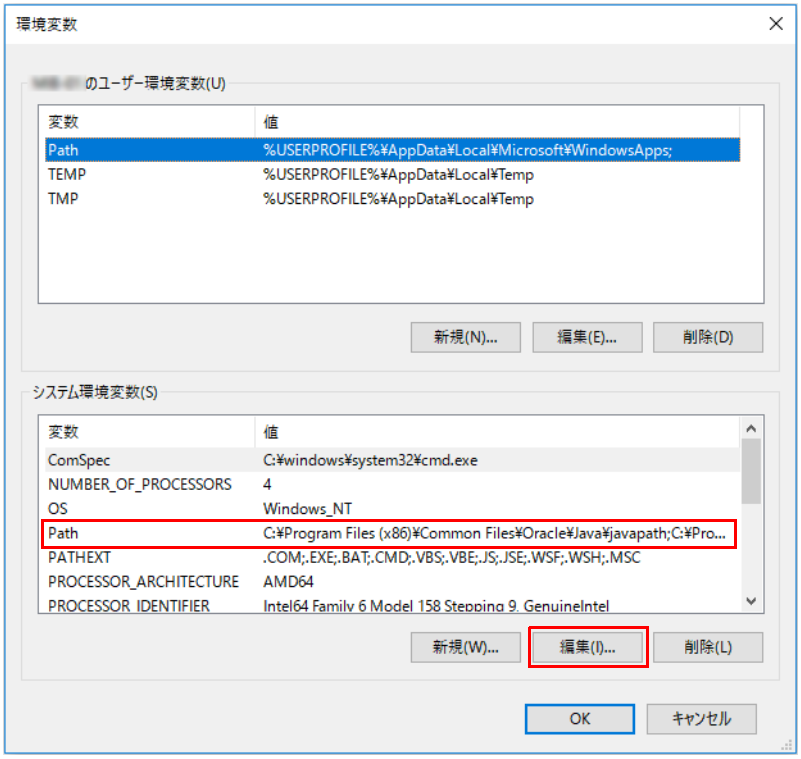
「システムのプロパティ」が表示されます。

4「環境変数」をクリックします。



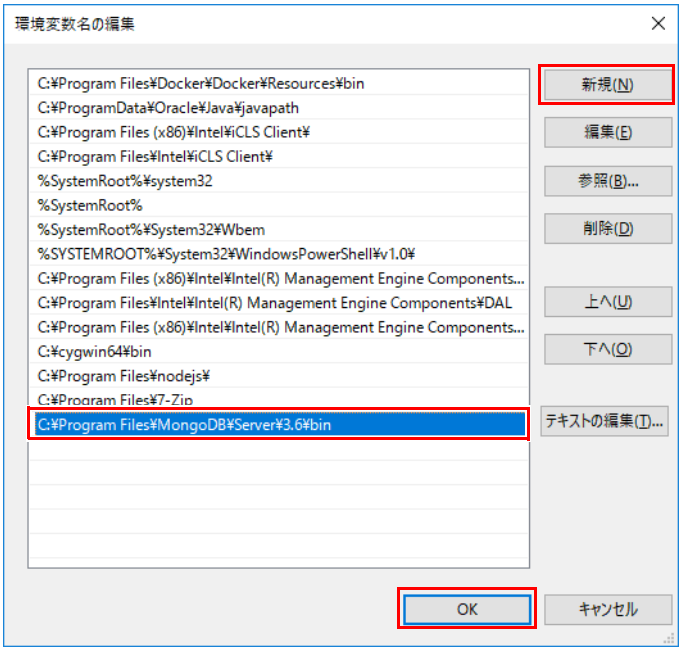
「環境変数」が表示されます。

5「システム環境変数」の「Path」をクリックし、「編集」をクリックします。



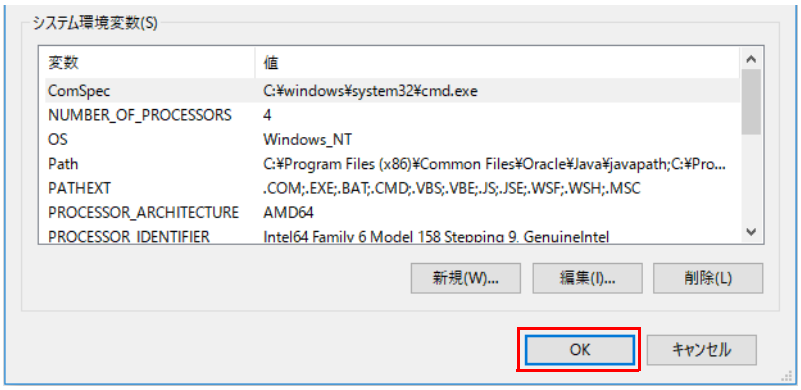
「環境変数名の編集」が表示されます。

6 「新規」をクリックし、最後行に表示されたテキストボックスに「C:¥Program Files¥mongoDB¥Server¥3.6¥bin」を入力し、「OK」をクリックします。



「環境変数」が表示されます。

7 「OK」をクリックします。



8 次のデータ格納用のフォルダー「C:¥mongoDB¥data」を作成します。

9 「C:¥Fujitsu¥Software¥CA_100¥01_Preparation¥04_mongoDB¥mongodb.config」を「C:¥Program Files¥mongoDB¥Server¥3.6¥bin」にコピーします。

POINT
▸「対象のフォルダーへのアクセスは拒否されました」というメッセージが表示される場合は、「続行」をクリックします。

10 管理者権限でコマンドプロンプトを起動します（→ P.7）。

11 次のコマンドを入力して【Enter】キーを押し、mongoDB を実行します。
mongod --config "C:¥Program Files¥mongoDB¥Server¥3.6¥bin¥mongodb.config"

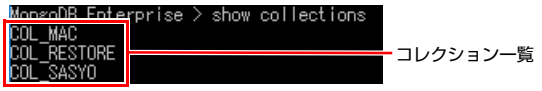
POINT
▸手順15を実行するまでコマンドプロンプトを終了しないでください。コマンドプロンプトを終了すると、手順13以降の設定ができなくなります。

12 管理者権限で別のコマンドプロンプトを起動します（→ P.7）。

13 次のコマンドを入力して【Enter】キーを押し、セキュリティ用の DB を作成します。
mongo MIB_SEC

14 「mongoDB Enterprize>」、または「>」と表示されたら、次のコマンドを入力し、【Enter】キーを押します。
db.createCollection('COL_MAC')
db.createCollection('COL_SASYO')
db.createCollection('COL_RESTORE')

15 次のコマンドを入力して【Enter】キーを押し、作成したコレクション「COL_MAC」「COL_RESTORE」「COL_SASYO」が表示されることを確認します。
show collections



16 手順 12 で起動したコマンドプロンプトを終了します。

17 手順 10 で起動したコマンドプロンプトを終了します。

認証エンジンのインストール

1 管理者権限でコマンドプロンプトを起動します（→ P.7）。

2 次のコマンドを入力して【Enter】キーを押します。
cd C:¥Fujitsu¥Software¥CA_100¥02_ClientAuth¥01_AuthEngine
「C:¥Fujitsu¥Software¥CA_100¥02_ClientAuth¥01_AuthEngine」フォルダーへ移動します。

3 次のコマンドを入力して【Enter】キーを押し、docker build を実行します。
docker load < clientauth.tar

認証エンジンのインストールが開始します。「Loaded image: clientauth: lastest」というメッセージが表示されたら、インストールは完了です。

4 コマンドプロンプトを終了します。

管理アプリのインストール

1「C:¥Fujitsu¥Software¥CA_100¥02_ClientAuth¥02_MgmtAppControl¥wifi-mgmg-nodejs.zip」を「C:¥wifi-mgmg-nodejs」に展開します。

2「C:¥Fujitsu¥Software¥CA_100¥02_ClientAuth¥03_MgmtAppUI¥wifi-mgmg-ui.zip」を「C:¥wifi-mgmg-ui」に展開します。

管理アプリの設定

■設定ファイルの変更

1 管理者権限でコマンドプロンプトを起動します（→ P.7）。

2 次のコマンドを入力し、【Enter】キーを押し、アクセスポイントの MAC アドレスを確認します。

arp -a

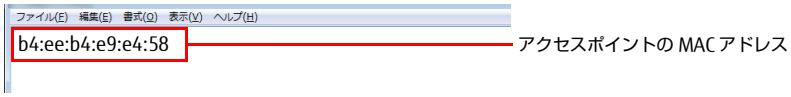
表示されたアクセスポイントの MAC アドレスを確認し、メモに控えておいてください。

POINT

▸arp -a コマンドでアクセスポイントのMACアドレスが表示されない場合は、以下を実行してください。
ping 本製品のアクセスポイント部分の IP アドレス
例）本製品のアクセスポイント部分の IP アドレスが 192.168.1.22 の場合
ping 192.168.1.22 を実行後、arp -a を実行してください。

3 テキストエディターで、「C:¥wifi-mgmg-nodejs¥APaddress」を表示し、手順 2 で確認したアクセスポイントの MAC アドレスを入力し保存します。

※MAC アドレスの後にスペースや改行を入力しないでください。



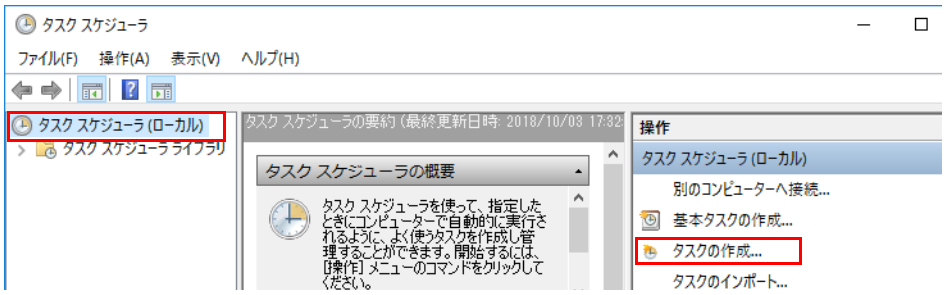
4 コマンドプロンプトを終了します。

■タスクスケジューラの登録

1 「スタート」→「Windows 管理ツール」→「タスクスケジューラ」の順にクリックします。

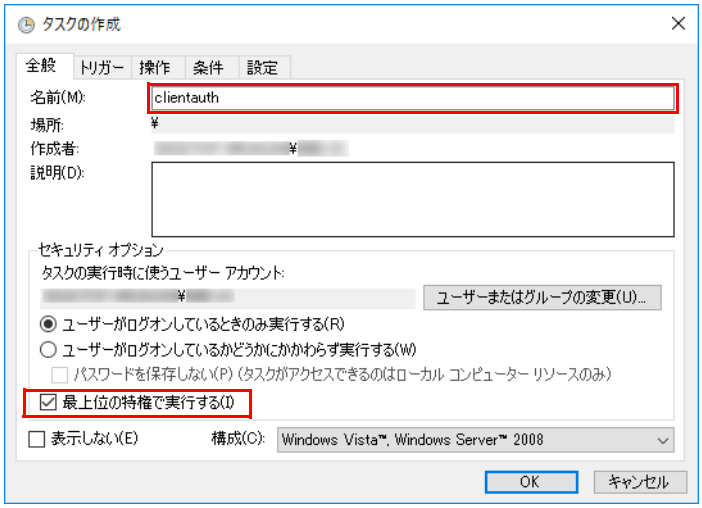
「タスクスケジューラ」が起動します。

2 「タスクスケジュール（ローカル）」を選択し、「操作」の「タスクの作成」をクリックします。

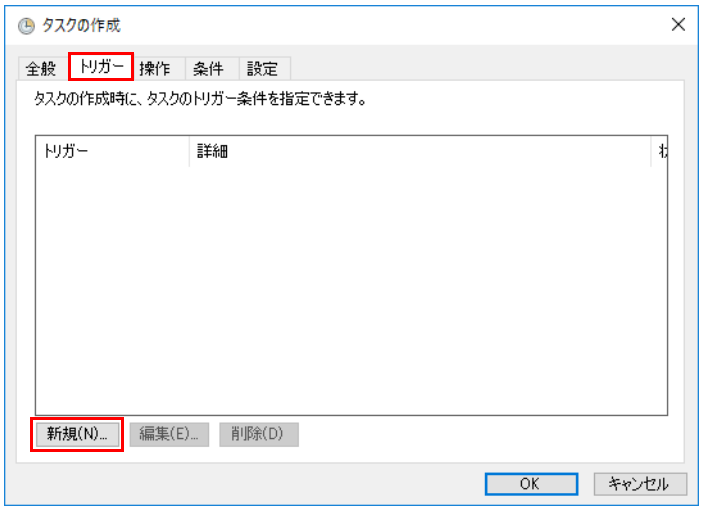


「タスクの作成」が表示されます。

3 名前に「clientauth」を入力し、「最上位の特権で実行する」にチェックを付けます。

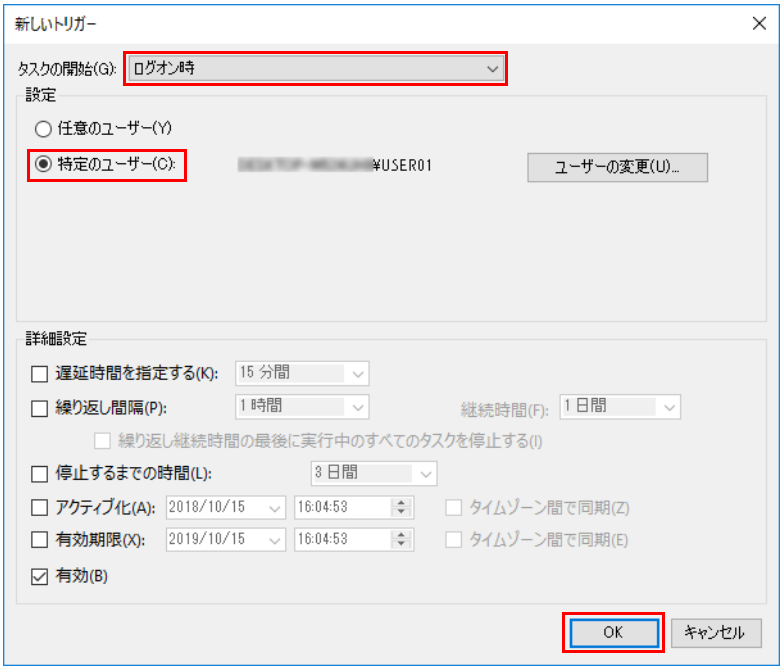


4「トリガー」タブをクリックし「新規」をクリックします。



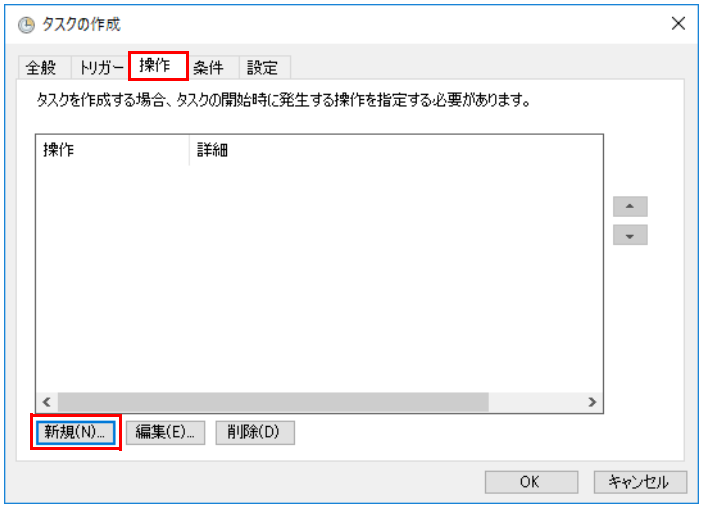
「新しいトリガー」が表示されます。

5 タスクの開始で「ログオン時」を選択し、設定で「特定のユーザー」を選択し、「OK」をクリックします。



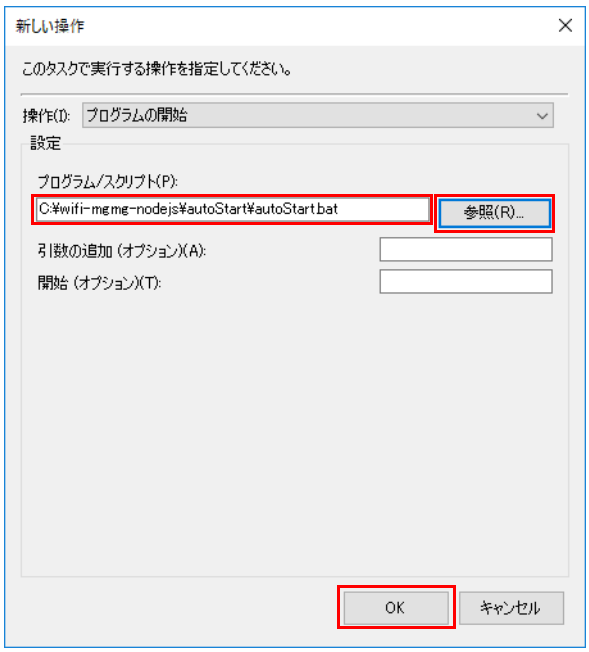
「タスクの作成」が表示されます。

6「操作」タブをクリックし「新規」をクリックします。



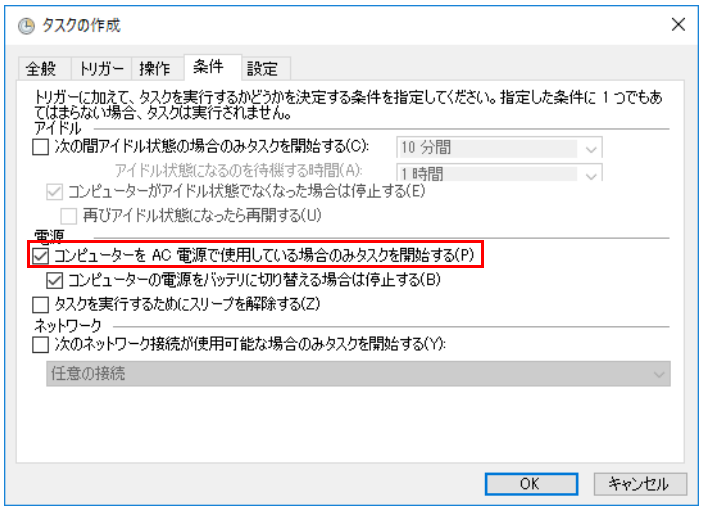
「新しい操作」が表示されます。

7「プログラム / スクリプト」の「参照」をクリックし、表示されたウィンドウから次のファイルを選択し、「OK」をクリックします。
C:¥wifi-mgmg-nodejs¥autoStart¥autoStart.bat

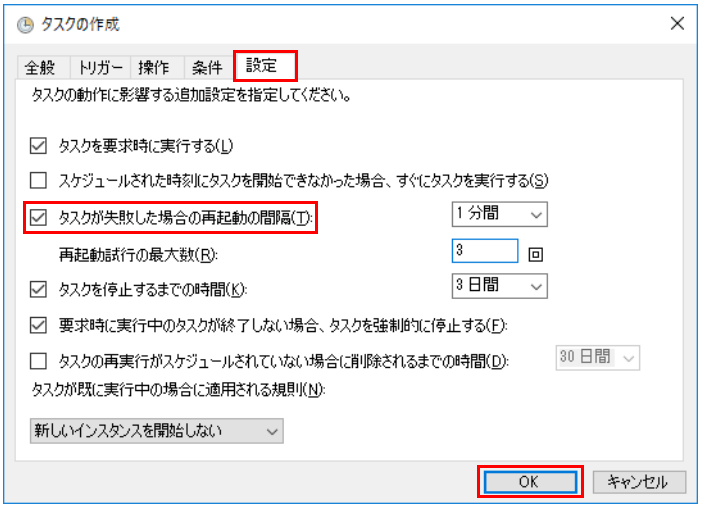


「タスクの作成」が表示されます。

8「条件」タブをクリックし、「コンピューターを AC 電源で使用している場合のみタスクを開始する」にチェックを付けます。



9「設定」タブをクリックし、「タスクが失敗した場合の再起動の間隔」にチェックを付け、「OK」をクリックします。



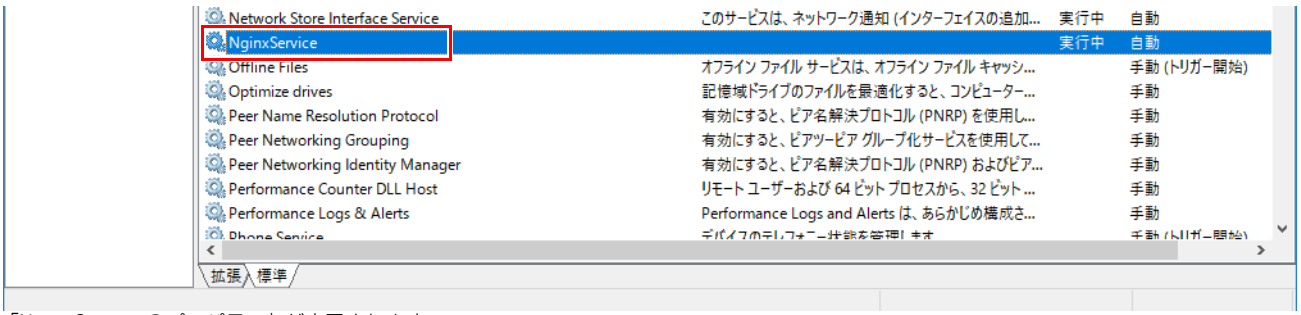
nginx の設定

POINT

- 本製品では、動作状態監視ツールが動作しているため、nginx がプロセス停止状態であると検知され、nginx がプロセスが再起動します。

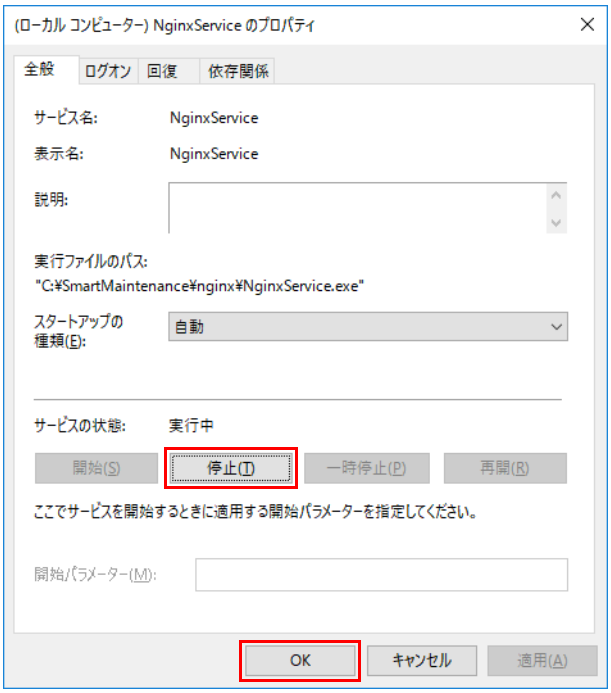
1「スタート」→「Windows 管理ツール」→「サービス」の順にクリックします。
サービスが起動します。

2「NginxService」を選択し右クリックし、「プロパティ」をクリックします。



「NginxService のプロパティ」が表示されます。

3「停止」をクリックし、「OK」をクリックします。



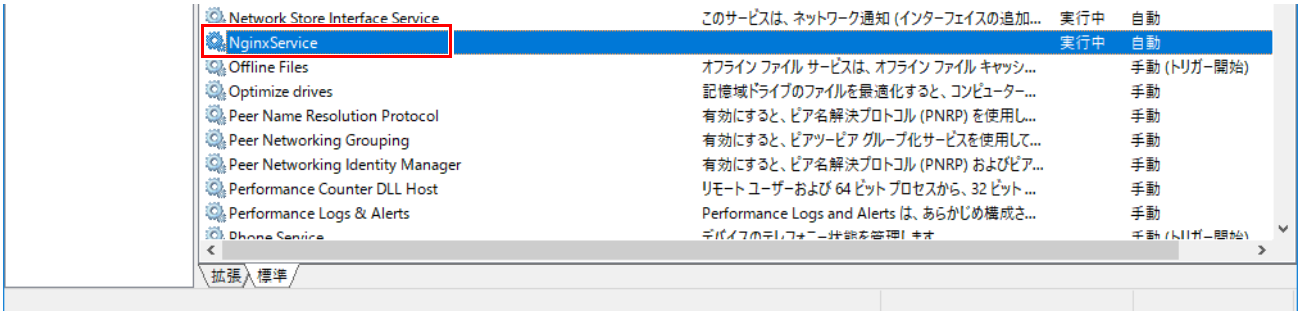
4　テキストエディターで「C:¥SmartMaintenance¥nginx¥conf¥nginx.conf」を開き、表記内容を確認してください。
「x.x.x.x」に、本製品のコンピューター部分の固定 IP アドレスが記載されていることを確認します。

```
location /security/ {
   proxy_pass  http://x.x.x.x:8010/;
}

location /nodejs/ {
   proxy_pass  http://x.x.x.x:8001/;
}

#error_page  404          /404.html;
```

5　ファイルを保存して閉じます。

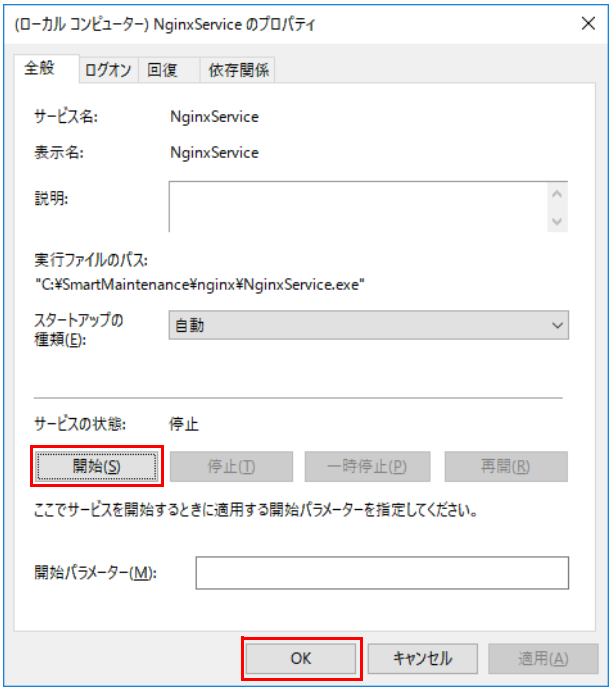
6　「スタート」→「Windows 管理ツール」→「サービス」の順にクリックします。
サービスが起動します。

7　「NginxService」を選択し右クリックし、「プロパティ」をクリックします。



「NginxService のプロパティ」が表示されます。

8　「開始」をクリックし、「OK」をクリックします。

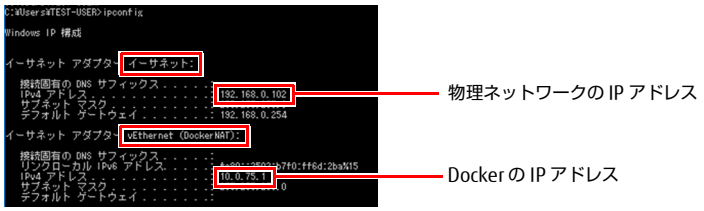


メトリックの設定

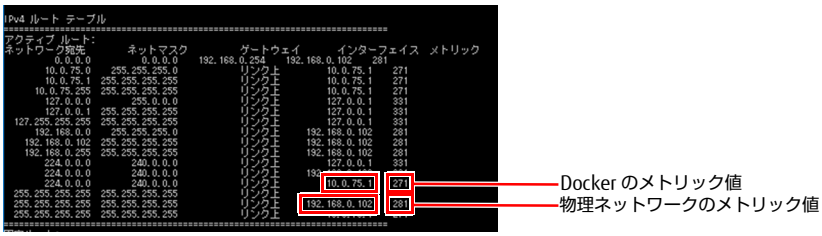
物理ネットワークのメトリック値を Docker のメトリック値より低く設定し、物理ネットワークの優先度を上げます。

1 管理者権限でコマンドプロンプトを起動します（→ P.7）。

2 次のコマンドを入力し、【Enter】キーを押し、IP アドレスを確認します。
ipconfig

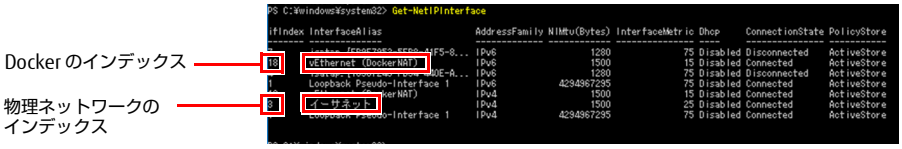


3 次のコマンドを入力し、【Enter】キーを押し、メトリック値を確認します。
route print



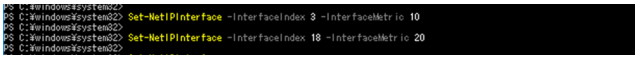
4 次のコマンドを入力し、【Enter】キーを押し、PowerShell のコンソールを立ち上げます。
powershell

5 次のコマンドを入力し、【Enter】キーを押し、インターフェースインデックスを確認します。
Get-NetIPInterface

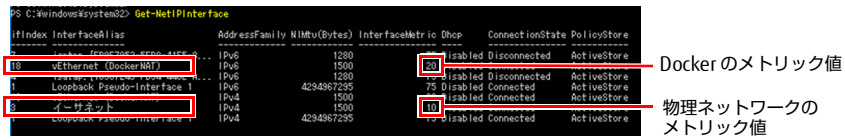


6 次のコマンドを入力し、【Enter】キーを押し、物理ネットワークのメトリック値を Docker より低く設定します。
Set-NetIPInterface -InterfaceIndex ○ -InterfaceMetric 10
Set-NetIPInterface -InterfaceIndex △ -InterfaceMetric 20

○には、物理ネットワークのインデックスを入力します。
△には、Docker のインデックスを入力します。

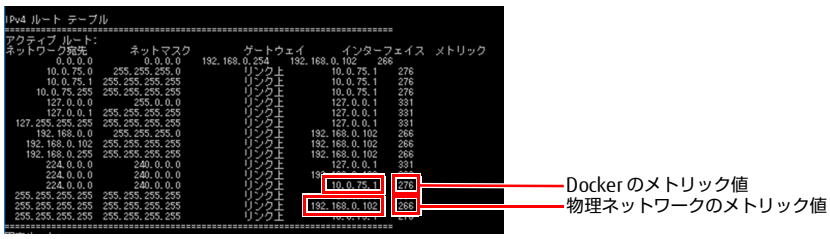


7 次のコマンドを入力し、【Enter】キーを押し、物理ネットワークのメトリック値が Docker より低く設定されていることを確認します。
Get-NetIPInterface



8 次のコマンドを入力し、【Enter】キーを押し、PowerShell のコンソールを終了します。
exit

9 次のコマンドを入力し、【Enter】キーを押してルーティングテーブルを表示します。物理ネットワークのメトリック値が Docker より低く設定されていることを確認します。
route print



10 コマンドプロンプトを終了します。

ファイアウォールの設定

端末認証で使用するポートのファイアウォール経由の通信を許可する設定を行います。ここでは、本製品に Windows ファイアウォールを設定する方法を説明します。

POINT

- 市販のセキュリティ対策ソフトをインストールしている場合は、セキュリティ対策ソフトのマニュアルをご覧になり、ファイアウォールの設定を行ってください。

■使用するポート

設定が必要なポートは、次のとおりです。

用途	プロトコル	ポート
管理アプリケーション（制御部）	TCP	8001
Radius サーバ 注	UDP	1812、1813

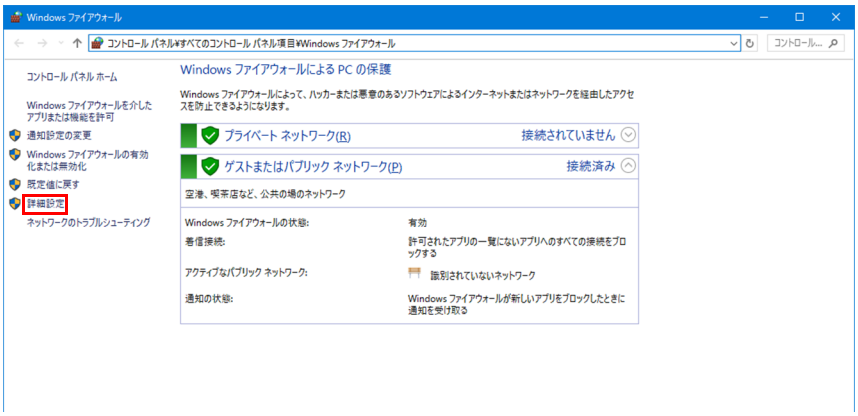
注 ：RADIUS（Remote Authentication Dial In User Service）プロトコルを使って、認証サービスを提供するサーバー

■管理アプリケーション （制御部） の設定

1 「コントロールパネル」を表示します（→ P.7）。

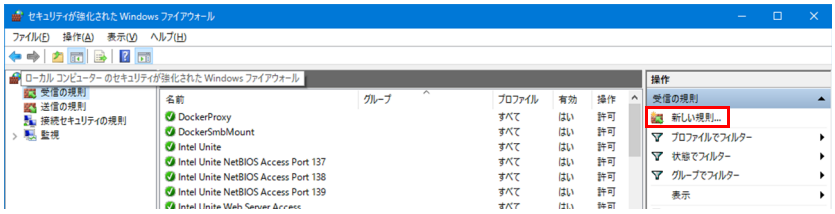
「コントロールパネル」が表示されます。

2 「システムとセキュリティ」→「Windows ファイアウォール」→「詳細設定」の順にクリックします。



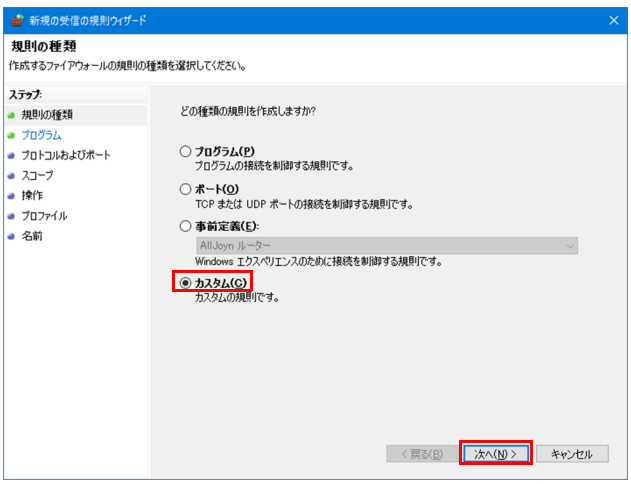
「セキュリティが強化された Windows ファイアウォール」が表示されます。

3 「受信の規則」をクリックし、「新しい規則 ...」をクリックします。



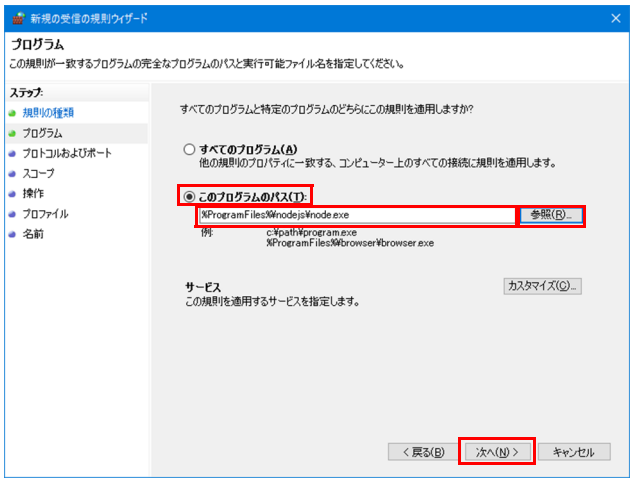
「規則の種類」が表示されます。

4 「カスタム」を選択し、「次へ」をクリックします。



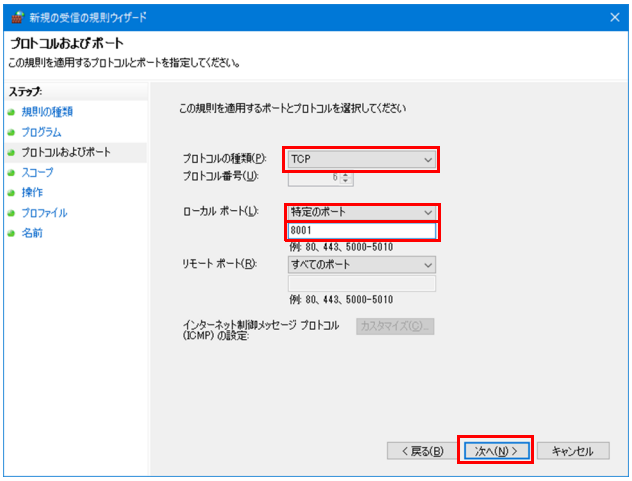
「プログラム」が表示されます。

5「このプログラムのパス」を選択し、「参照」をクリックして、表示されたウィンドウから次のファイルを選択して、「次へ」をクリックします。
C:¥Program Files¥nodejs¥node.exe



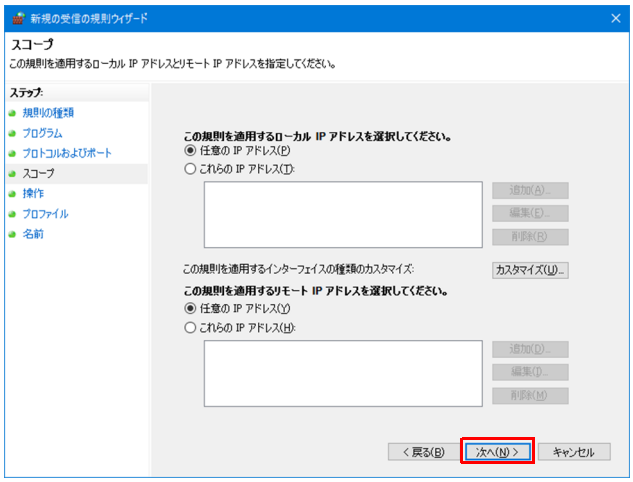
「プロトコルおよびポート」が表示されます。

6 **次の項目を設定し、「次へ」クリックします。**
・「プロトコルの種類」で「TCP」を選択します。
・「ローカルポート」で「特定のポート」を選択して、「8001」を入力します。



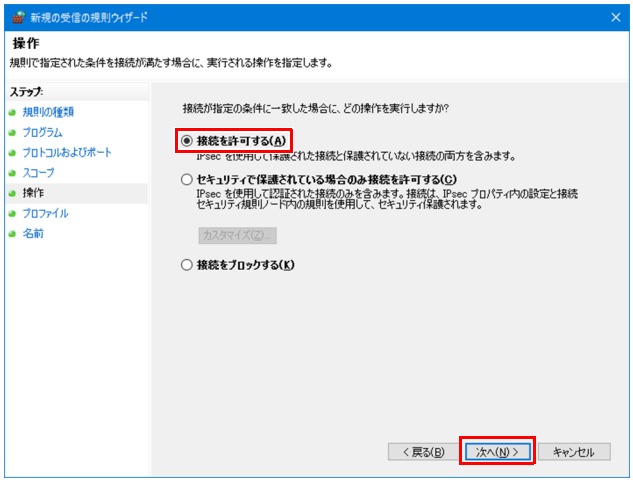
「スコープ」が表示されます。

7「次へ」をクリックします。



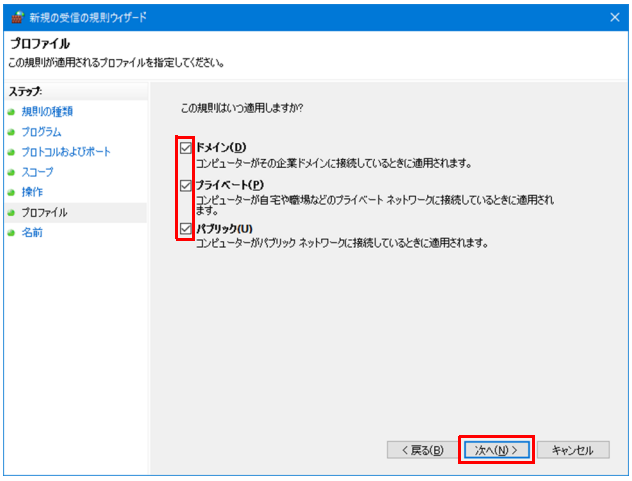
「プロトコルおよびポート」が表示されます。

8「接続を許可する」を選択し、「次へ」をクリックします。



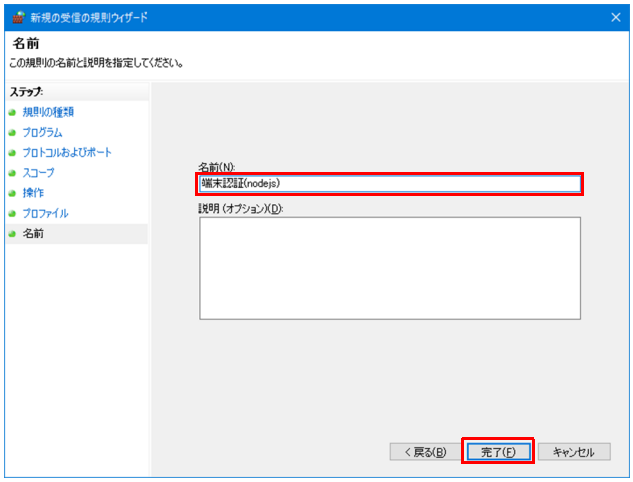
「プロファイル」が表示されます。

9 すべての項目にチェックを付け、「次へ」をクリックします。



「名前」が表示されます。

10「名前」に「端末認証（nodejs）」と入力し、「完了」をクリックします。

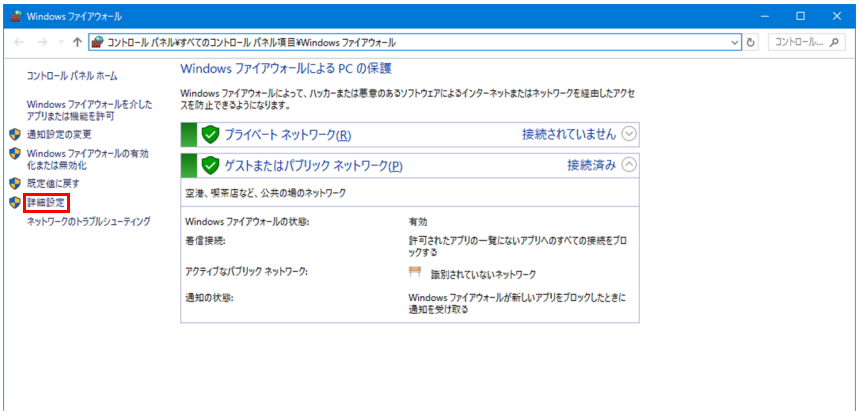


管理アプリケーション（制御部）の設定が完了しました。

■ Radius サーバの設定

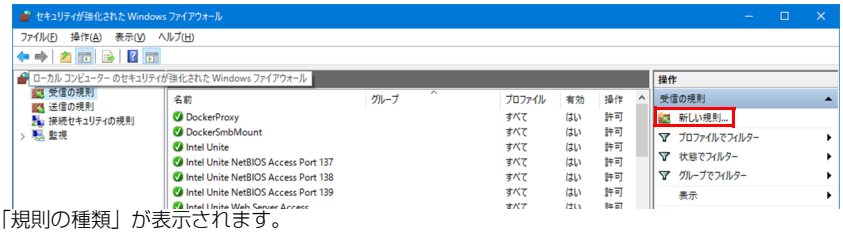
1「コントロールパネル」を表示します（→ P.7）。
「コントロールパネル」が表示されます。

2「システムとセキュリティ」→「Windows ファイアウォール」→「詳細設定」の順にクリックします。



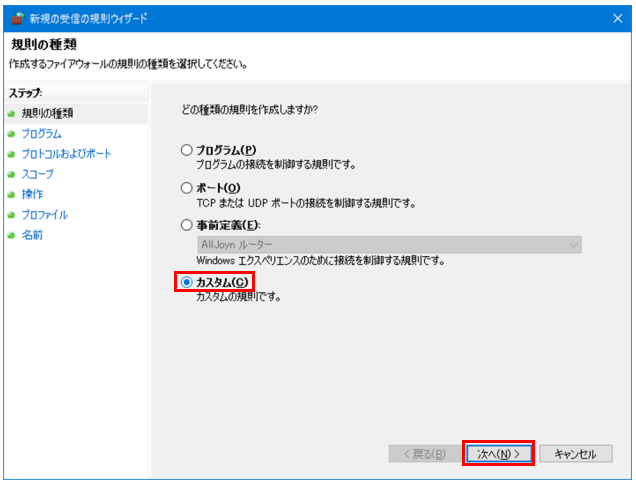
「セキュリティが強化された Windows ファイアウォール」が表示されます。

3「受信の規則」をクリックし、「新しい規則 ...」をクリックします。



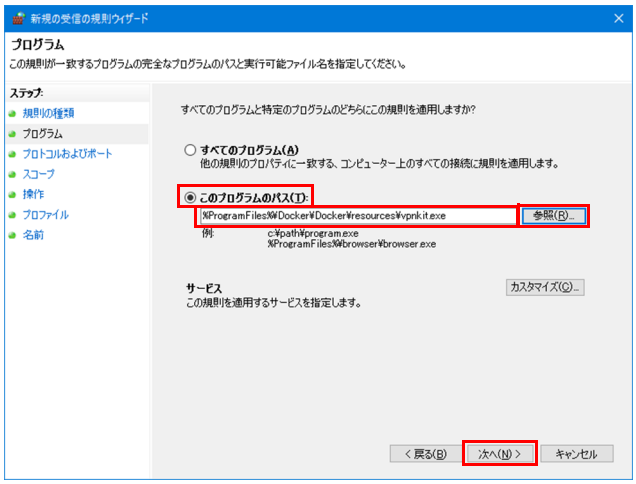
「規則の種類」が表示されます。

4「カスタム」を選択し、「次へ」をクリックします。



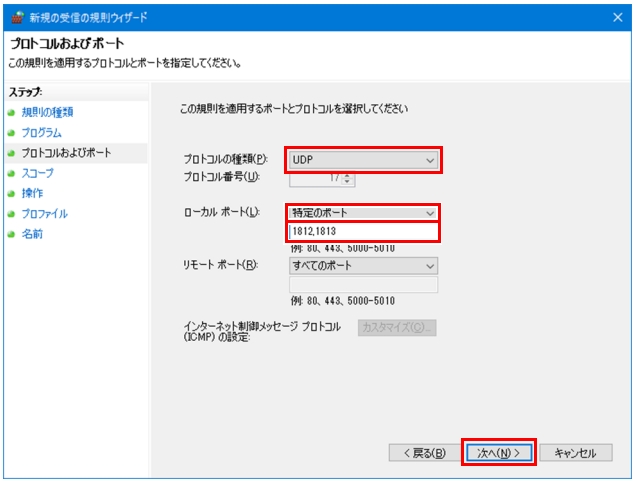
「プログラム」が表示されます。

5「このプログラムのパス」を選択し、「参照」をクリックして、表示されたウィンドウから次のファイルを選択して、「次へ」をクリックします。
C:¥Program Files¥Docker¥Docker¥resources¥vpnkit.exe



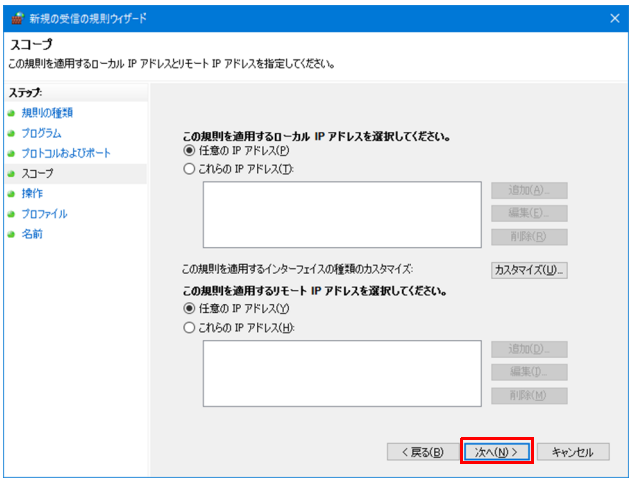
「プロトコルおよびポート」が表示されます。

6 **次の項目を設定し、「次へ」クリックします。**
・「プロトコルの種類」で「UDP」を選択します。
・「ローカルポート」で「特定のポート」を選択して、「1812,1813」を入力します。



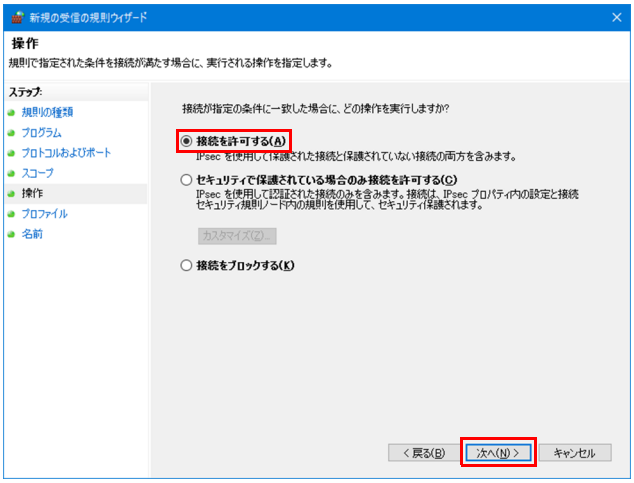
「スコープ」が表示されます。

7「次へ」をクリックします。



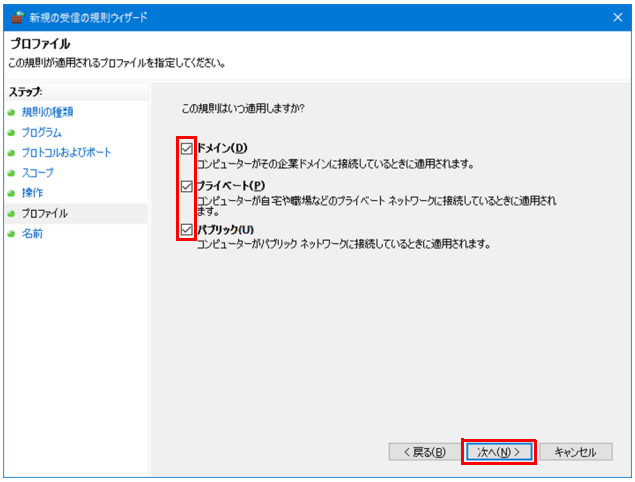
「プロトコルおよびポート」が表示されます。

8「接続を許可する」を選択し、「次へ」をクリックします。



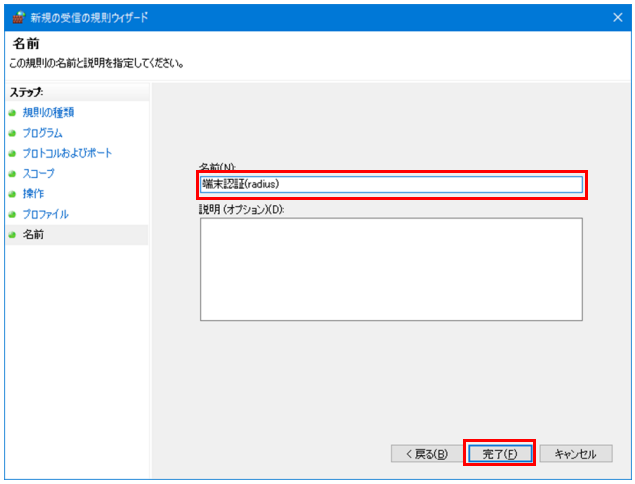
「プロファイル」が表示されます。

9 すべての項目にチェックを付け、「次へ」をクリックします。



「名前」が表示されます。

10「名前」に「端末認証（radius)」と入力し、「完了」をクリックします。

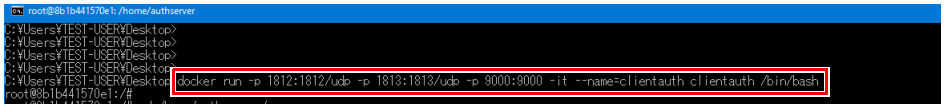


これで、設定が完了しました。

認証エンジンの起動

1 管理者権限でコマンドプロンプトを起動します（→ P.7）。

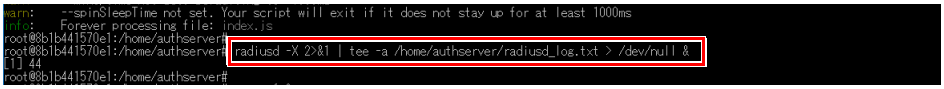
2 次のコマンドを入力して【Enter】キーを押し、コンテナを作成（ログイン）します。
docker run -p 1812:1812/udp -p 1813:1813/udp -p 9000:9000 -it --name=clientauth clientauth /bin/bash



3 次のコマンドを入力して【Enter】キーを押し、「/home/authserver」へ移動します。
cd /home/authserver

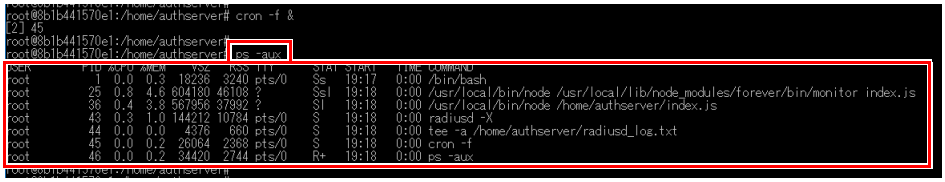
4 次のコマンドを入力して【Enter】キーを押し、認証サーバーを起動します。
forever start -o out.log -e err.log index.js

5 次のコマンドを入力して【Enter】キーを押し、radius を起動します。
radiusd -X 2>&1 | tee -a /home/authserver/radiusd_log.txt > /dev/null &



6 次のコマンドを入力して【Enter】キーを押し、cron を起動します。
cron -f &

7 次のコマンドを入力して【Enter】キーを押して、各プロセスが起動していることを確認します。
ps -aux



8 コマンドプロンプトを終了します。

管理アプリの起動

■ mongoDB の起動

1. 管理者権限でコマンドプロンプトを起動します（→ P.7）。
2. 次のコマンドを入力し、【Enter】キーを押します。
   mongod --config "C:¥Program Files¥mongoDB¥Server¥3.6¥bin¥mongodb.config"

重要
- ここで起動したコマンドプロンプトは、「管理アプリケーション（UI部）」を起動するまで、終了しないでください。

■ 管理アプリケーション （制御部） の起動

1. 管理者権限でコマンドプロンプトを起動します（→ P.7）。
2. 次のコマンドを入力し、【Enter】キーを押します。
   cd C:¥wifi-mgmg-nodejs
   「C:¥wifi-mgmg-nodejs」フォルダーへ移動します。
3. 次のコマンドを入力し、【Enter】キーを押します。
   node index.js

POINT
- コマンド実行後にエラーが発生する場合、システム環境変数を見直してください。Node.jsのインストール後、システム環境変数に「C:¥Program Files¥nodejs」が設定されますが、まれにこの環境変数が消えることがあります。その場合はシステム環境変数（Path）に「C:¥Program Files¥nodejs」を追加してください。

4. コマンドプロンプトに次のメッセージが表示されていることを確認します。
   :INF0:sendInit() end
   以降、本製品を再起動すると、管理アプリケーション（制御部）は自動で起動します。

■ 管理アプリケーション （UI 部） の起動

1. 管理者権限でコマンドプロンプトを起動します（→ P.7）。
2. 次のコマンドを入力し、【Enter】キーを押します。
   cd C:¥wifi-mgmg-ui
   「C:¥wifi-mgmg-ui」フォルダーへ移動します。
3. 次のコマンドを入力し、【Enter】キーを押します。
   wifiMng_start.bat

POINT
- 「このアプリ機能のいくつかがWindowsファイアウォールでブロックされています」というメッセージが表示された場合は、「アクセスを許可する」をクリックしてください。

4. コマンドプロンプトに次のメッセージが表示されていることを確認します。
   [] INF0 - Started MibApplication in seconds(JVM running seconds(JVM running for)
   以降、本製品を再起動すると、管理アプリケーション（UI 部）は自動で起動します。

7. 拡張機能 - セキュリティ （タブレット端末）

端末認証

タブレット端末への端末認証設定のインストール、認証登録およびアンインストールは、必ず、管理者権限のアカウントで行ってください。

POINT

- 端末認証機能動作のためにコマンドプロンプトが起動します。起動したコマンドプロンプトは終了させないでください。コマンドプロンプトが非表示の状態で操作したい場合は、仮想デスクトップをご使用ください（→P.194）。
- マニュアル内で記載されているアイコンには、次のような意味があります。

：エッジコンピューティングデバイスの設定や操作です。

：タブレット（パソコン）端末の設定や操作です。

管理画面へログイン

1 ブラウザーを起動し、管理画面の URL（http://IP アドレス :10080/security/）に接続します。

POINT

- IPアドレスにはコンピューター部分のIPアドレスをお使いください。
  コンピューター部分のIPアドレスが「192.168.1.3」の場合は次のようになります。
  http://192.168.1.3:10080/security/
- 端末認証を使用するために必要なアプリが起動するのに時間がかかります。OS起動直後の場合は、充分に待ってから端末認証の管理画面にアクセスしてください。

ログイン画面が表示されます。

2 アクセスポイント（AP）で利用している「root」アカウントのパスワードを入力し、「ログイン」をクリックします。

「パスワードの変更」（→ P.40）で変更したパスワードを入力してください。

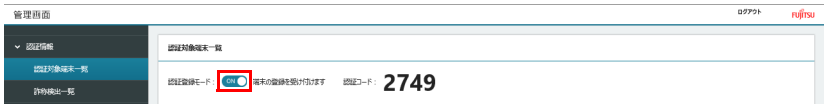
端末認証機能の管理画面が表示されます。

認証登録モードを ON にする

端末認証機能の管理画面で「認証登録モード」を ON にします。

1 「認証情報」の「認証対象端末一覧」をクリックし、OFF をクリックします。

しばらくすると、「認証登録モード」が ON になります。



重要

- 管理画面からログアウトまたは、本製品を再起動しても、認証登録モードは保持されます。「認証登録モード」を「ON」にしている間は、アクセスポイントの設定／パスワード変更は実施しないでください。アクセスポイントの設定／パスワード変更を行う場合は、「認証登録モード」が「OFF」であることを確認してください。

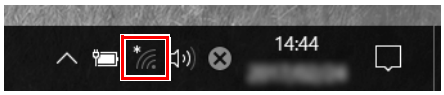
プロキシ設定を無効にする

タブレット端末に端末認証のインストールおよび設定をする前に、「プロキシの設定」（→ P.91）で設定したプロキシ設定を無効にします。端末認証登録が完了した後、プロキシ設定を元の状態に戻してください。

■手動プロキシ設定の場合

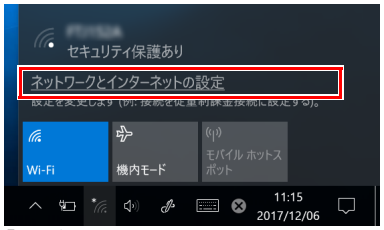
手動プロキシを無効にします。

1 **画面右下の通知領域の をタップします。**



（これ以降の画面は機種や状況により異なります）

2 **「ネットワークとインターネットの設定」をタップします。**

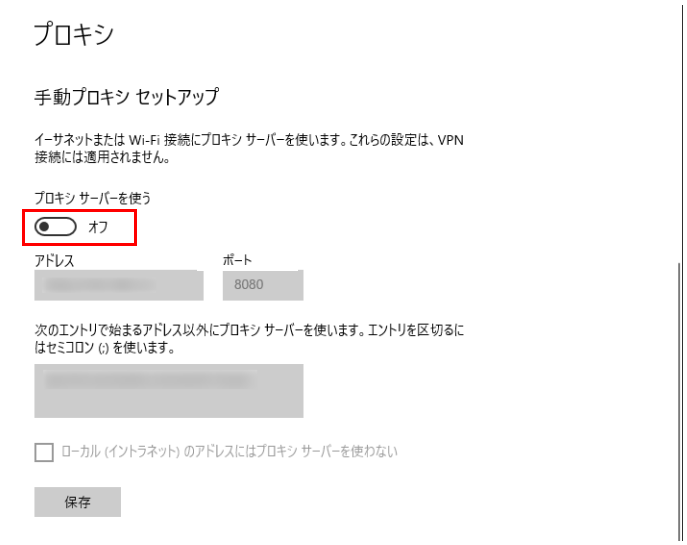


「設定」ウィンドウが表示されます。

3 **「プロキシ」をタップします。**

「設定」ウィンドウが表示されます。

4 **「手動プロキシセットアップ」の「プロキシサーバーを使う」をタップして （オフ）にします。**

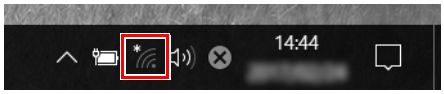


5 **×をタップして「設定」ウィンドウを閉じます。**

■自動構成スクリプト （PAC） の場合

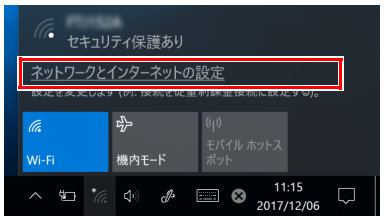
自動プロキシを無効にします。

1 **画面右下の通知領域の をタップします。**



（これ以降の画面は機種や状況により異なります）

2 **「ネットワークとインターネットの設定」をタップします。**

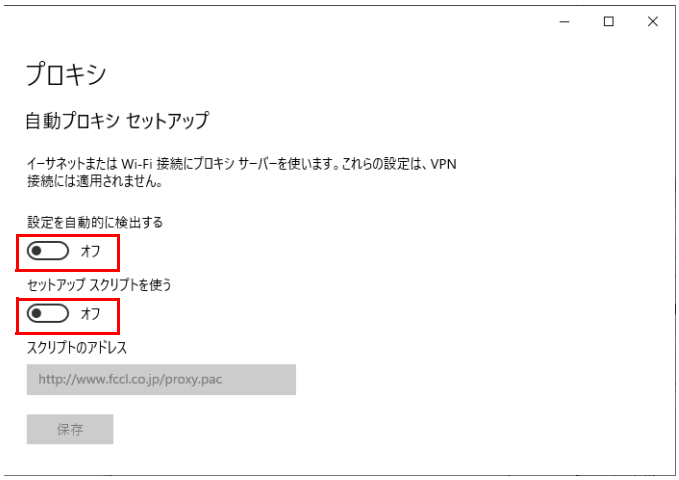


「設定」ウィンドウが表示されます。

3 **「プロキシ」をタップします。**

「設定」ウィンドウが表示されます。

4 **「自動プロキシセットアップ」の「設定を自動的に検出する」と「セットアップスクリプトを使う」をタップして (オフ）にします。**

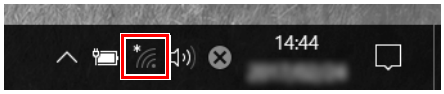


5 **×をタップして「設定」ウィンドウを閉じます。**

■ プロキシ自動設定機能の場合

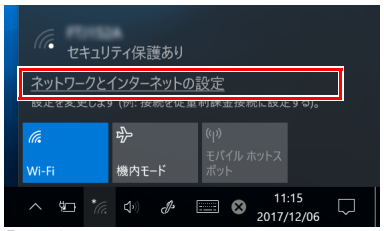
手動プロキシを無効にした後、タスクスケジューラで、「プロキシ自動設定」タスクを「無効」に設定します。

1 **画面右下の通知領域の をタップします。**



（これ以降の画面は機種や状況により異なります）

2 **「ネットワークとインターネットの設定」をタップします。**

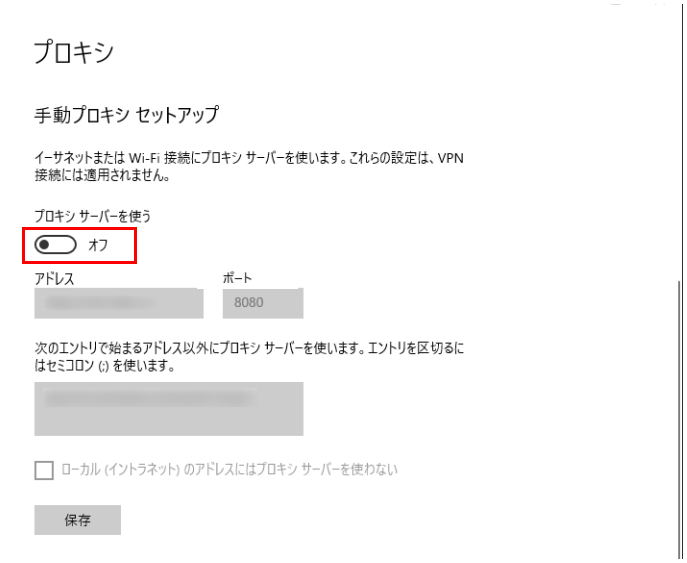


「設定」ウィンドウが表示されます。

3 **「プロキシ」をタップします。**

「設定」ウィンドウが表示されます。

4 **「手動プロキシセットアップ」の「プロキシサーバーを使う」をタップして（オフ）にします。**



5 **×をタップして「設定」ウィンドウを閉じます。**

6 **「スタート」→「Windows 管理ツール」→「タスクスケジューラ」の順にクリックします。**

「タスクスケジューラ」が起動します。

7 「プロキシ自動設定」を右クリックし「無効」をクリックします。

8 「タスクスケジューラ」を閉じます。

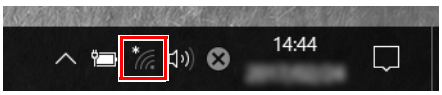
端末認証設定のインストール

タブレット端末を無線 LAN に接続し、端末認証設定のインストーラーをダウンロードしてインストールします。なお、すでに端末認証設定がインストールされている場合は、インストール作業は不要です。「認証端末の登録」へ進んでください（→ P.174）。

1　管理画面の「認証登録モード」を ON にします（→ P.168）。

2　登録対象の端末で次の操作を行います。

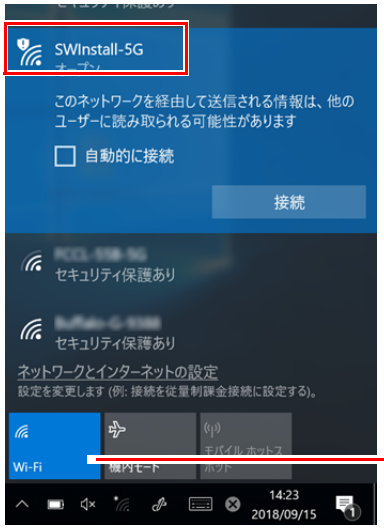
1. 登録対象のタブレット端末で、画面右下の通知領域の をタップします。



（これ以降の画面は機種や状況により異なります）

現在利用できる無線 LAN の SSID の一覧が表示されます。

2. クライアントアプリインストール専用の SSID「SWInstall-5G」をタップします。

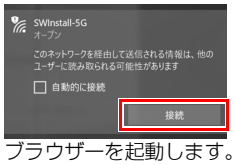


ネットワーク名（SSID）が表示されず「無効」と表示されているときは、「Wi-Fi」をタップして「オン」にしてください。

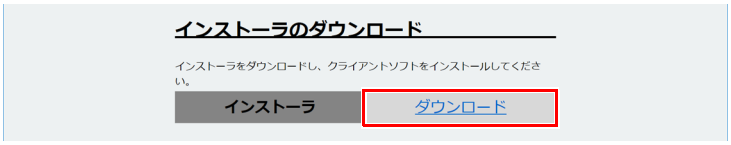
POINT

▸セキュリティのためネットワーク名（SSID）が表示されないようにしている場合は、「非公開のネットワーク」をタップし画面の指示に従って操作してください。「非公開のネットワーク」は画面下に隠れていることがあります。ネットワーク名の一覧を上にスクロールしてください。

3. 「接続」をタップします。



4. ブラウザーを起動します。
5. インストーラーのダウンロードページが表示されます。
6. 「ダウンロード」をタップし、ファイルをダウンロードします。



7. ダウンロードした「Setup.msi」を実行します。

POINT

▸「現在、SmartScreen を使用できません」というメッセージが表示された場合は、「実行」をタップしてください。

「インストールの確認」が表示されます。

8. 「次へ」をタップします。
インストールが開始します。しばらくすると、「インストールが完了しました」と表示されます。

POINT

▸「ユーザーアカウント制御」が表示された場合は、「はい」をクリックします。

9. 「閉じる」をタップします。

3　複数のタブレット端末にインストールする場合は、「認証登録モード」を ON にしたまま、手順 2 の 1 ～ 6 を繰り返します。すべてのタブレット端末のインストールが完了したら、「認証端末の登録」（→ P.174）に進みます。

認証端末の登録

端末認証機能の管理画面でタブレット端末を登録します。まだ、タブレット端末に「端末認証設定」をインストールしていない場合は、先に「プロキシ設定を無効にする」（→ P.169）を実施した後、インストールしてください。

重要

- 複数台のエッジコンピューティングデバイスで認証登録モードを同時に ON にしないでください。

1 管理画面で「認証登録モード」を ON にします（→ P.168）。

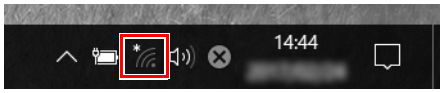
POINT

- 端末認証設定のインストールで「認証登録モード」を ON にしている場合は、手順1は不要です。

しばらくすると、認証コードが表示されます。

2 登録対象のタブレット端末で次の操作を行います。

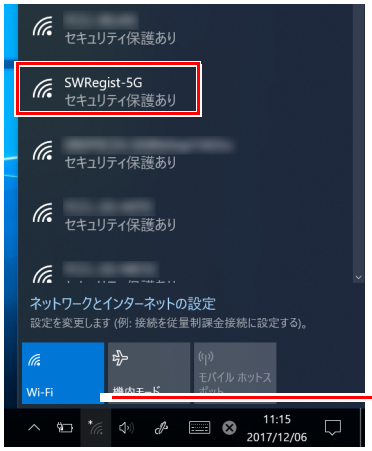
1. 登録対象のタブレット端末で、画面右下の通知領域の をタップします。



（これ以降の画面は機種や状況により異なります）

現在利用できる無線 LAN の SSID の一覧が表示されます。

2. 認証端末登録専用の SSID「SWRegist-5G」をタップします。

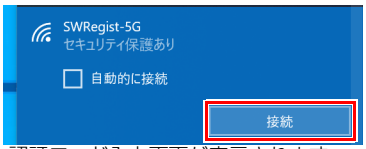


ネットワーク名（SSID）が表示されず「無効」と表示されているときは、「Wi-Fi」をタップして「オン」にしてください。

POINT

- セキュリティのためネットワーク名（SSID）が表示されないようにしている場合は、「非公開のネットワーク」をタップし画面の指示に従って操作してください。「非公開のネットワーク」は画面下に隠れていることがあります。ネットワーク名の一覧を上にスクロールしてください。

3. 「接続」をタップします。

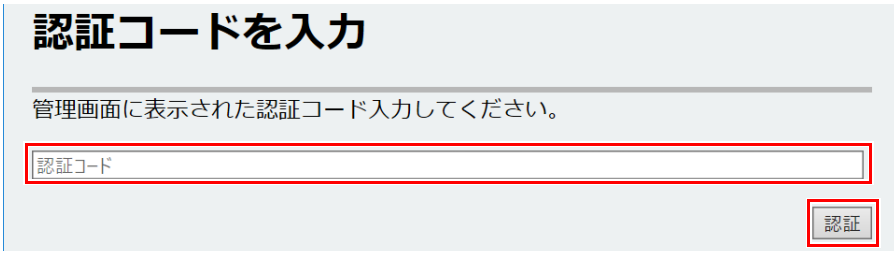


認証コード入力画面が表示されます。

4. 端末認証機能の管理画面に表示された認証コードを入力し、「認証」をクリックします。

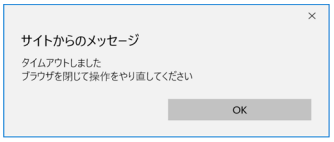
POINT

- ブラウザーで「ポップアップがブロックされました」と表示された場合は、ポップアップのブロックを解除してください。
- ユーザアカウント制御が無効になっている場合、認証コード入力画面が表示されません。



POINT

▸30秒経過するとタイムアウトの画面が表示されます。ブラウザーを閉じてSSIDの接続を中止してやり直してください。



5. 正しく設定できたか確認します。
正しく設定できると、「接続済み」と表示されます。

認証対象端末一覧に、無線 LAN 接続した端末が追加されます。

3 複数のタブレット端末を登録する場合は、「認証登録モード」を ON にしたまま、手順 2 の 1 ～ 5 を繰り返します。すべてのタブレット端末の登録が完了したら、手順 4 に進みます。

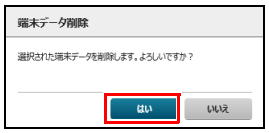
4 すべてのタブレット端末の登録が完了したら、「認証登録モード」を「OFF」にします（→ P.180）。

POINT

▸登録した情報を削除する場合は、次の手順を実行してください。

1. 削除対象の端末にチェックを付け、「削除」をクリックします。

2.「はい」をクリックします。



登録済み認証端末のデータが削除されます。

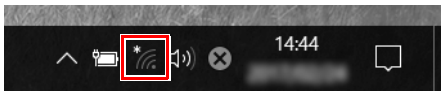
プロキシ設定を有効にする

「プロキシ設定を無効にする」（→ P.169）で設定したプロキシ設定を有効にします。

■手動プロキシ設定の場合

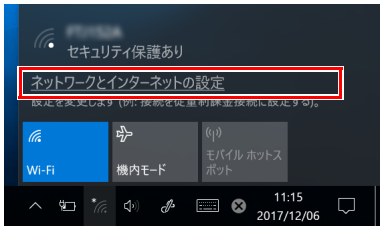
手動プロキシを有効にします。

1 **画面右下の通知領域の をタップします。**



（これ以降の画面は機種や状況により異なります）

2 **「ネットワークとインターネットの設定」をタップします。**

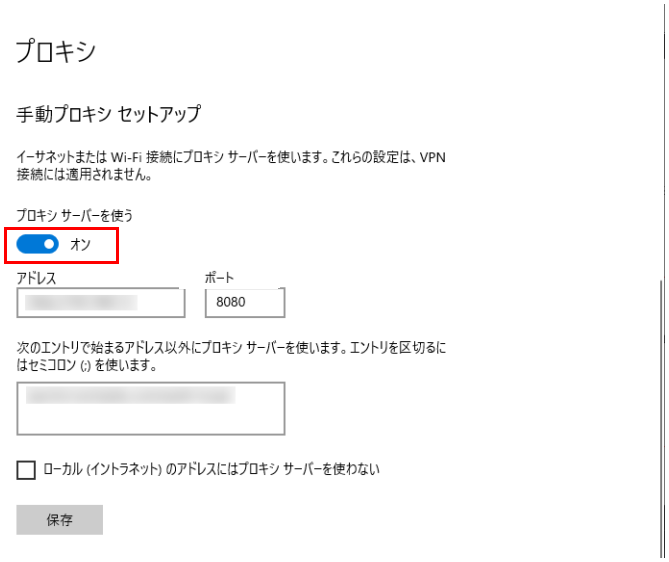


「設定」ウィンドウが表示されます。

3 **「プロキシ」をタップします。**

「設定」ウィンドウが表示されます。

4 **「手動プロキシセットアップ」の「プロキシサーバーを使う」をタップして （オン）にします。**

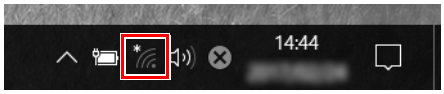


5 **×をタップして「設定」ウィンドウを閉じます。**

■自動構成スクリプト （PAC） の場合

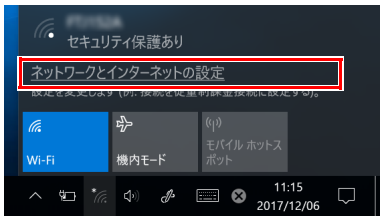
自動プロキシを有効にします。

1 **画面右下の通知領域の をタップします。**



（これ以降の画面は機種や状況により異なります）

2 **「ネットワークとインターネットの設定」をタップします。**

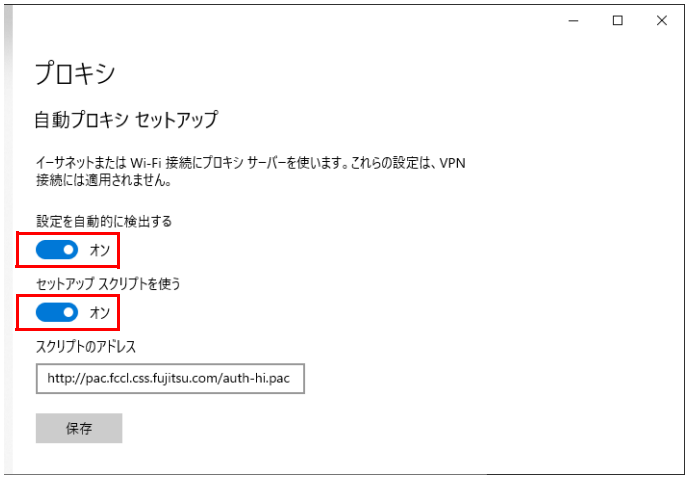


「設定」ウィンドウが表示されます。

3 **「プロキシ」をタップします。**

「設定」ウィンドウが表示されます。

4 **「自動プロキシセットアップ」の「設定を自動的に検出する」と「セットアップスクリプトを使う」をタップして （オン）にします。**

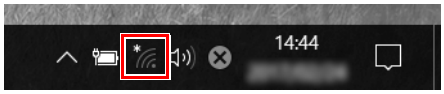


5 **×をタップして「設定」ウィンドウを閉じます。**

■ プロキシ自動設定機能の場合

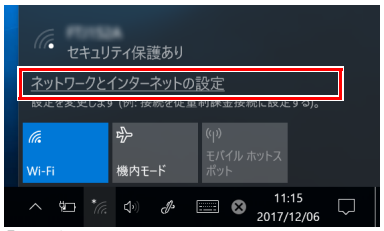
手動プロキシを有効にした後、タスクスケジューラで、「プロキシ自動設定」タスクを「有効」に設定します。

1 **画面右下の通知領域の をタップします。**



（これ以降の画面は機種や状況により異なります）

2 **「ネットワークとインターネットの設定」をタップします。**

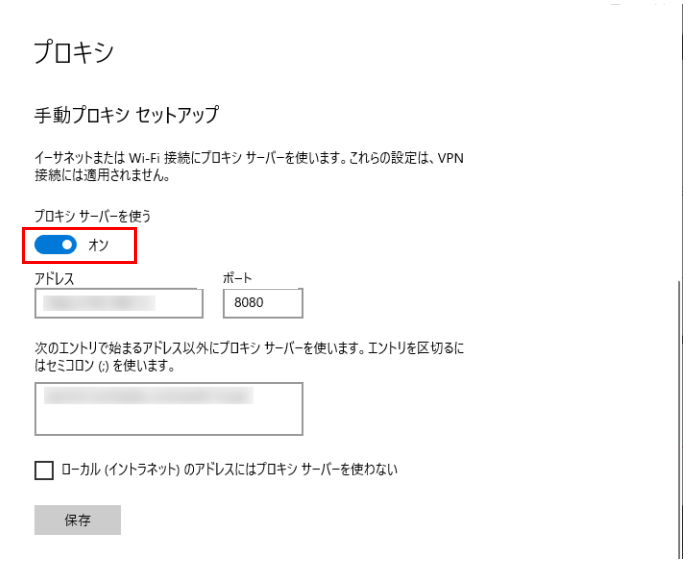


「設定」ウィンドウが表示されます。

3 **「プロキシ」をタップします。**

「設定」ウィンドウが表示されます。

4 **「手動プロキシセットアップ」の「プロキシサーバーを使う」をタップして （オン）にします。**

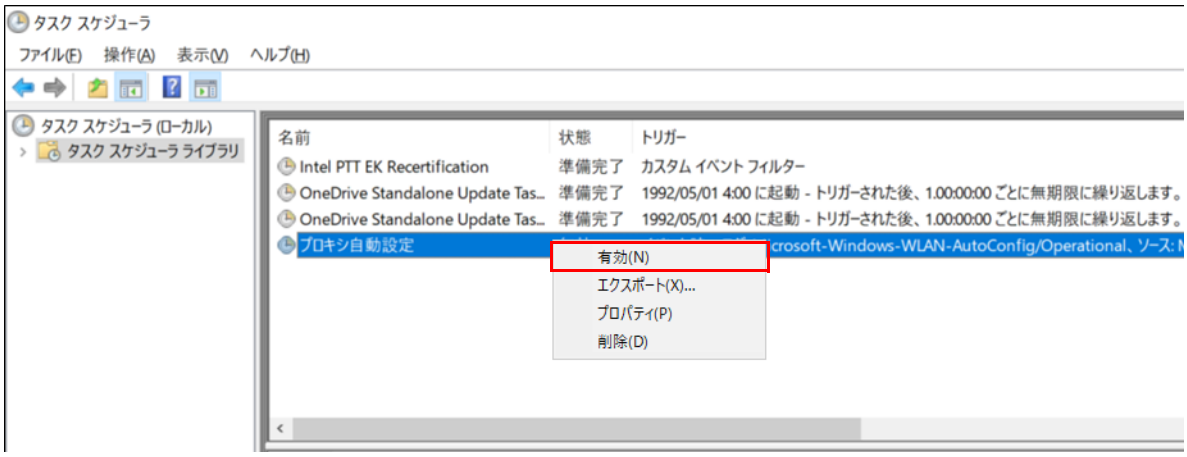


5 **×をタップして「設定」ウィンドウを閉じます。**

6 **「スタート」→「Windows 管理ツール」→「タスクスケジューラ」の順にクリックします。**

「タスクスケジューラ」が起動します。

7 「プロキシ自動設定」を右クリックし「有効」をクリックします。



8 「タスクスケジューラ」を閉じます。

認証登録モードを OFF にする

端末認証機能の管理画面で「認証登録モード」を「OFF」にします。

1 「認証情報」の「認証対象端末一覧」をクリックし、ON をクリックします。

しばらくすると、「認証登録モード」が「OFF」になります。

重要

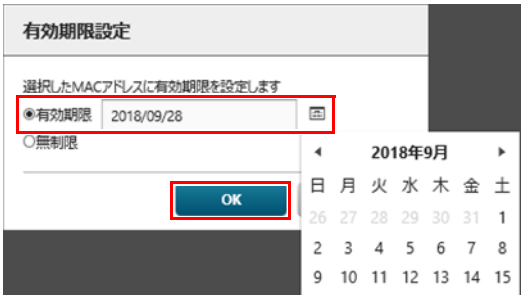
- 管理画面からログアウトしても、本製品を再起動しても、認証登録モードは保持されます。「認証登録モード」を「ON」にしている間は、アクセスポイントの設定／パスワード変更は実施しないでください。アクセスポイントの設定／パスワード変更を行う場合は、「認証登録モード」が「OFF」であることを確認してください。

有効期限の設定

登録した認証端末に有効期限を設定できます。有効期限を過ぎると状態が「有効期限オーバー」と表示され、本製品に接続できなくなります。

1 「認証情報」の「認証対象端末一覧」をクリックし、対象端末にチェックを付け、「有効期限設定」をクリックします。

2 有効期限を選択して をクリックし期限の年月日を選択した後、「OK」をクリックします。



3 有効期限が設定されます。

8. 拡張機能 - 端末情報収集 （製品本体）

バッテリー劣化診断のインストールと設定

「基本アプリのインストールと設定」（→ P.62）でバッテリー劣化診断のインストールと設定は完了しています。

インストール補助ツールを使用する （無線 LAN 診断）

「インストール補助ツール」（→ P.23）は、本製品に添付されておりません。「インストール補助ツール」を使用する場合は、「インストール補助ツールとインターネットキャッシュ機能 V3.0.0 用アップデートモジュールのダウンロード」（→ P.28）をご覧になり、ダウンロードしてください。

ダウンロード後、「ExtensionFunction_WirelesslanAnalysis_Install.cmd」を実行してください。なお、バッチファイルは、必ず、管理者権限のアカウントで実行してください。次のインストールと設定が自動で行われます。

「無線 LAN 診断のインストールと設定」（→ P.181）～「MibAPConfig.xml 設定ファイルの変更」（→ P.183）

バッチファイルの実行が完了したら、本製品を再起動した後、「拡張機能 - 端末情報収集（タブレット端末）」（→ P.185）からインストールと設定を進めてください。
なお、「インストール補助ツール」（→ P.23）を使用しない場合は、本マニュアルに沿ってインストールと設定を行ってください。

無線 LAN 診断のインストールと設定

無線 LAN 診断フォルダーの配置

1. **「C:¥Program Files¥FCCL¥WirelesslanAnalysis」フォルダーを作成します。**
2. **「C:¥ProgramData¥FCCL¥WirelesslanAnalysis」フォルダーを作成します。**

   POINT
   - エクスプローラーに「C:¥ProgramData」が表示されない場合は、「エクスプローラー」→「表示」→「隠しファイル」にチェックを付けてください（→ P.62）。
3. **「C:¥Fujitsu¥Software¥WirelesslanAnalysis¥Drivers」内のすべてのファイルとフォルダーを「C:¥Program Files¥FCCL¥WirelesslanAnalysis」にコピーします。**

   POINT
   - 「このフォルダーへコピーするには管理者権限が必要です」と表示された場合は、「続行」をクリックします。
4. **ファイルとフォルダーの構成が次のようになっていることを確認します。**

フォルダーとファイルの構成	
C:¥Program Files¥FCCL¥WirelesslanAnalysis	App_Data
	XML
	Elasticsearch.Net.dll
	Elasticsearch.Net.xml
	Newtonsoft.Json.dll
	Newtonsoft.Json.xml
	Renci.SshNet.dll
	Renci.SshNet.xml
	System.Reactive.Core.dll
	System.Reactive.Core.xml
	System.Reactive.Interfaces.dll
	System.Reactive.Interfaces.xml
	System.Reactive.Linq.dll
	System.Reactive.Linq.xml
	WlanDiagnosisLib.dll
	WlanDiagnosisLib.pdb
	WlanDiagnosisService.exe
	WlanDiagnosisService.exe.CodeAnalysisLog.xml
	WlanDiagnosisService.exe.config
	WlanDiagnosisService.exe.lastcodeanalysissucceeded
	WlanDiagnosisService.pdb

設定ファイルのコピー

1. **「C:¥Program Files¥FCCL¥WirelesslanAnalysis¥XML¥MibAPConfig.xml」を「C:¥ProgramData¥FCCL¥WirelesslanAnalysis」にコピーします。**

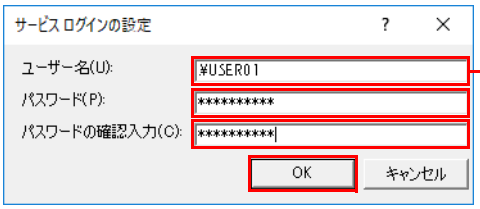
無線 LAN 診断サービスのインストール

1 **管理者権限でコマンドプロンプトを起動します（→ P.7）。**

2 **次のコマンドを入力し、【Enter】キーを押します。**
cd C:¥Windows¥Microsoft.NET¥Framework64¥v4.0.30319
「C:¥Windows¥Microsoft.NET¥Framework64¥v4.0.30319」フォルダーへ移動します。

3 **次のコマンドを入力し、【Enter】キーを押します。**
InstallUtil.exe "C:¥Program Files¥FCCL¥WirelesslanAnalysis¥WlanDiagnosisService.exe"
「サービスログインの設定」が表示されます。

4 **「ユーザー名」、「パスワード」、「パスワードの確認」に管理者権限のユーザーアカウント（現在、ログインしているアカウント）とパスワードを入力し、「OK」をクリックします。**

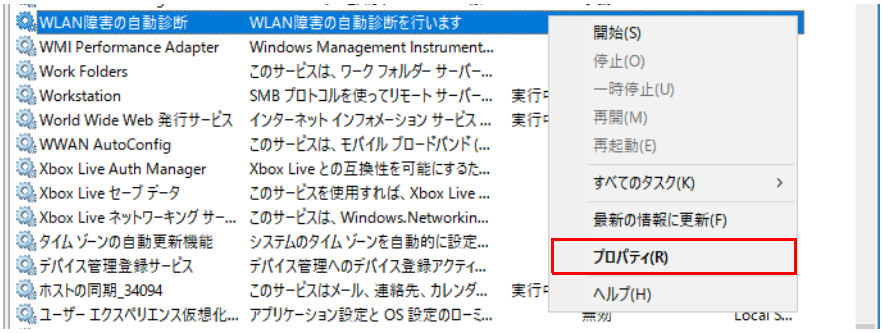


「トランザクション インストールが完了しました」のメッセージが表示されたら、インストールは完了しました。

無線 LAN 診断サービスの自動化

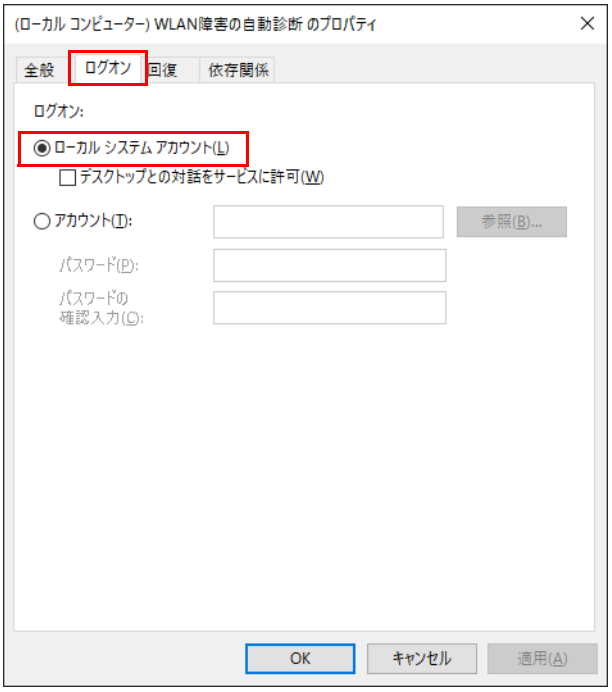
1 **「スタート」→「Windows 管理ツール」→「サービス」の順にクリックします。**
サービスが起動します。

2 **「WLAN 障害の自動診断」を選択し右クリックし、「プロパティ」をクリックします。**

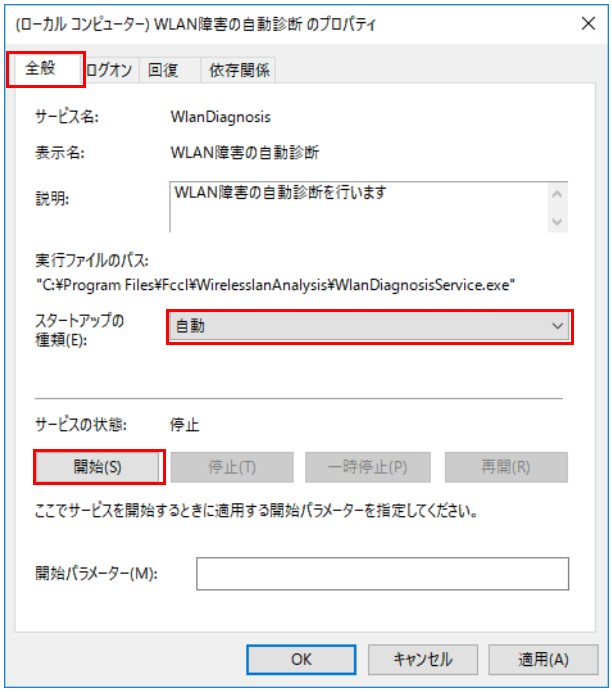


WLAN 障害の自動診断のプロパティが表示されます。

3 **「ログオン」タブをクリックし、「ローカルシステムアカウント」を選択します。**



4 「全般」タブをクリックし、「スタートアップの種類」リストで「自動」を選択し、「開始」をクリックします。



5 「OK」をクリックします。

MibAPConfig.xml 設定ファイルの変更

1 次のファイルをデスクトップにコピーします。

C:¥ProgramData¥FCCL¥WirelesslanAnalysis¥MibAPConfig.xml

2 コピーした「MibAPConfig.xml」をテキストエディターで開き、設定ファイルを変更します。

```
<?xml version="1.0" encoding="UTF-8"?>
<Configuration>
  <Name>MIB-AP</Name>
  <IPAddress>192.168.1.1</IPAddress>
  <Port>22</Port>
  <User>root</User>
 <Password>root</Password>
 <!--Password>MmvGB^RY3#</Password-->
</Configuration>
```

ここにアクセスポイント部分の固定 IP アドレスを入力してください。

ここにアクセスポイントのユーザ名「root」に設定した新しいパスワードを入力してください（→ P.40）。

3 変更後、保存してファイルを閉じます。

4 デスクトップの「MibAPConfig.xml」設定ファイルを次のフォルダーに移動して、既存のファイルと置換します。

C:¥ProgramData¥FCCL¥WirelesslanAnalysis¥MibAPConfig.xml

POINT

▶「対象のフォルダーへのアクセスは拒否されました」というメッセージが表示される場合は、「続行」をクリックします。

WatchProcessApp.ini 設定ファイルの変更

1 次のファイルをデスクトップにコピーします。

C:¥Program Files¥FCCL¥ProcessAliveWatcher¥Ini¥WatchProcessApp.ini

2 コピーした「WatchProcessApp.ini」をテキストエディターで開き、設定ファイルを変更します。

・[WlanDiagnosis] セクション

```
[WlanDiagnosis]
ProcessEnable=False
ProcessKind=service
RebootFilePath=C:\SmartMaintenance\bat\start_WlanDiagnosi
```

「True」に変更します。

3 変更後、ファイルを保存して閉じます。

4 デスクトップの「WatchProcessApp.ini」設定ファイルを次のフォルダーに移動して、既存のファイルと置換します。

C:¥Program Files¥FCCL¥ProcessAliveWatcher¥Ini¥WatchProcessApp.ini

POINT

▸「対象のフォルダーへのアクセスは拒否されました」というメッセージが表示される場合は、「続行」をクリックします。

端末稼働時間のインストールと設定

「基本アプリのインストールと設定」（→ P.62）で端末稼働時間のインストールと設定は完了しています。

無線 LAN 接続台数のインストールと設定

「基本アプリのインストールと設定」（→ P.62）で無線 LAN 接続台数のインストールと設定は完了しています。

9. 拡張機能 - 端末情報収集 （タブレット端末）

バッテリー劣化診断のインストール

「基本機能 - 初期設定（タブレット端末）」（→ P.91）でバッテリー劣化診断のインストールと設定は完了しています。

無線 LAN 診断のインストール

「基本機能 - 初期設定（タブレット端末）」（→ P.91）で無線 LAN 診断のインストールと設定は完了しています。

端末稼働時間のインストール

「基本機能 - 初期設定（タブレット端末）」（→ P.91）で稼働時間のインストールと設定は完了しています。

無線 LAN 接続台数表示

無線 LAN 接続台数表示のインストールと設定を行います。

重要

▸無線LAN接続台数表示は、先生が授業をスムーズに進めるためのツールです。そのため、先生の端末にのみインストールしてください。

.NET Framework 3.5 の有効化

1 「コントロールパネル」を表示します（→ P.7）。
「コントロールパネル」が表示されます。

2 「プログラム」→「Windows の機能の有効化または無効化」をクリックします。
「Windows の機能」が表示されます。

3 「.NET Framework 3.5（.NET2.0 および 3.0 を含む）」にチェックを付け、「OK」をクリックします。
「必要な変更が完了しました。」というメッセージが表示されます。

4 「今すぐ再起動」をクリックします。

無線 LAN 接続台数表示のインストール

先生のタブレット端末に無線 LAN 接続台数表示をインストールします。

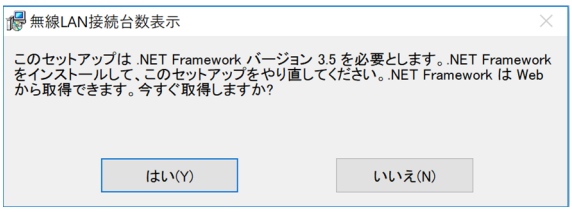
1 エッジコンピューティングデバイスの「C:¥Fujitsu¥Software¥SmartMaintenance¥Other¥ 無線 LAN 接続台数表示」フォルダーをタブレット端末にコピーします。

2 次のフォルダーの「WlanConnStatusAppSetup.msi」をダブルタップします。
次のフォルダーは、C:¥ にコピーした場合の例です。

C:¥無線LAN接続台数表示¥WlanConnStatusAppSetup.msi

POINT

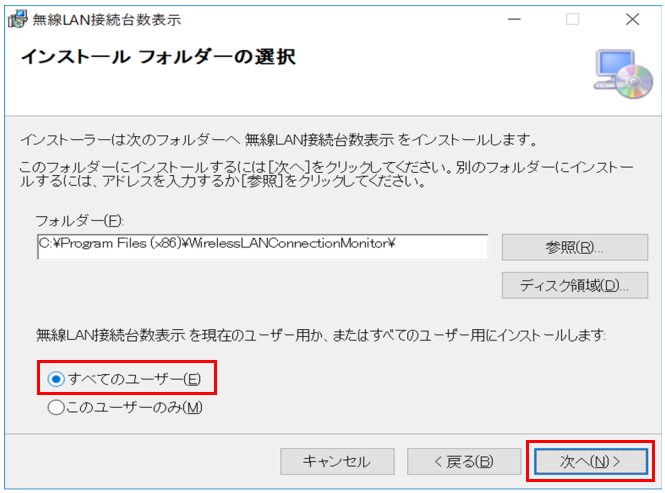
▸「このセットアップは.NET Frameworkバージョン3.5を必要としています。・・・」というメッセージが表示された場合は、「いいえ」をクリックし、「NET Framework 3.5」を有効化してください（→P.185）。有効化が完了したら、再度、「WlanConnStatusAppSetup.msi」を実行してください。



セットアップ・ウィザードが表示されます。

3 「次へ」をタップします。
インストール先フォルダーの入力画面が表示されます。

4「すべてのユーザー」を選択し、「次へ」をタップします。



「インストールの確認」が表示されます。

5「次へ」をタップします。

POINT

▸ユーザーアカウント制御の画面が表示される場合は、「はい」タップします。

インストールが開始されます。しばらくすると、「インストールが完了しました。」と表示されます。

6「閉じる」をタップします。

以上で無線 LAN 接続台数表示のインストールは終了です。

無線 LAN 接続台数表示設定ファイルの変更

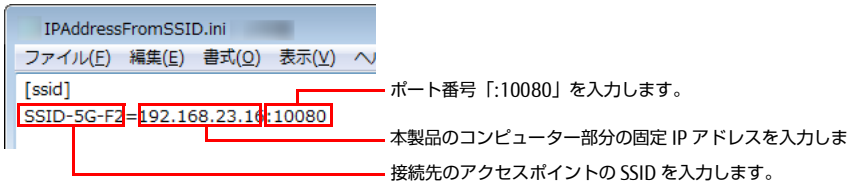
1 次のファイルを USB メモリーにコピーします。

C:¥Program Files (x86)¥FCCL¥WirelessLANConnectionMonitor¥Ini¥IPAddressFromSSID.ini

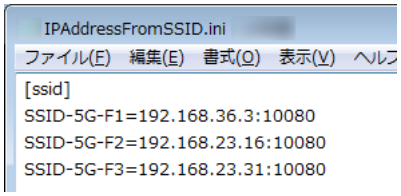
2 USB メモリーにコピーした「IPAddressFromSSID.ini」設定ファイルをエッジコンピューティングデバイスのテキストエディターで開きます。

3 次の部分を変更します。

接続先のアクセスポイントの SSID と本製品のコンピューター部分の固定 IP アドレスを次のように設定します。



複数登録する場合は、次のように設定しています。



4 変更後、保存してファイルを閉じます。

5 USB メモリーの「IPAddressFromSSID.ini」設定ファイルを次のフォルダーに移動して、既存のファイルと置換します。

C:¥Program Files (x86)¥FCCL¥WirelessLANConnectionMonitor¥Ini

POINT

▸「対象のフォルダーへのアクセスは拒否されました」というメッセージが表示される場合は、「続行」をタップします。

無線 LAN 接続台数表示の起動

次の手順で無線 LAN 接続台数表示を起動します。

1 ネットワークへ接続します。（設定済みの SSID：SSID-5G-F2 など）

2 → 「無線 LAN 接続台数表示」の順にタップします。

画面の右下に、現在の接続台数が表示されます。表示される接続台数には、先生が利用しているパソコン、タブレット端末の台数も含まれます。

例：先生用 1 台、生徒 40 台の場合 41 台と表示されます。

無線 LAN 接続台数表示が正しく起動／表示されない原因

●接続台数の画面が表示されずに「初期化に失敗しました」などのメッセージが表示される場合、次の原因が考えられます。
- ネットワークに接続していない。
- プロキシ設定に間違いがある。

●接続台数の画面は表示されるが「×」が表示される場合、次の原因が考えられます。
- ネットワークに接続していない。
- 対象の SSID を選択していない。
- 接続対象以外のエッジコンピューティングデバイスへ接続している。
- 設定ファイル（IPAddressFromSSID.ini）に間違いがある。

10.拡張機能 - ネットワーク （製品本体）

優先接続設定のインストールと設定

アクセスポイントの設定

優先接続設定のための設定は、「優先接続設定」（→ P.47）で完了しています。

設定ファイルの変更

■config.ini 設定ファイルの変更

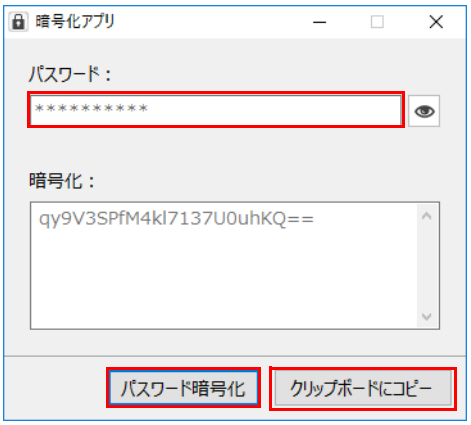
1 テキストエディターで「C:¥SmartMaintenance¥java¥config.ini」を開き、設定ファイルを変更します。

```
; ## 優先帯域
[priority]
; ## 優先帯域ユーザー
userId = admin
; ## 優先帯域パスワード
password = admin
; プロトコル
protocol = http
; 接続ポート
port = 80
```

アクセスポイントのユーザ名「admin」に設定した新しいパスワード（→ P.40）を暗号化アプリで暗号化した文字列を入力してください。

重要

▸パスワードは、暗号化アプリで暗号化した文字列を入力してください。



1. 「C:¥SmartMaintenance¥Other¥ 暗号化アプリ ¥PasswordEncoder.exe」を実行します。
2. 「パスワード」にパスワードを入力します。
3. 「パスワード暗号化」をクリックします。
4. 「クリップボードにコピー」をクリックします。

2 ファイルを保存して閉じます。

11.拡張機能 - ネットワーク （タブレット端末）

優先接続設定のインストールと設定

先生のタブレット端末に優先接続設定をインストールします。

インストール

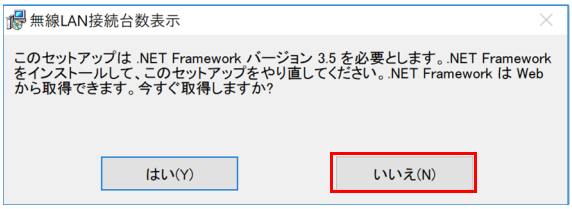
1 エッジコンピューティングデバイスの「C:¥Fujitsu¥Software¥PriorityBand」フォルダーをタブレット端末にコピーします。

2 次のフォルダーの「PriorityBandwidthCtrlSetup.msi」をダブルタップします。
次のフォルダーは、C:¥ にインストーラーがある場合の例です。

C:¥PriorityBand¥PriorityBandwidthCtrlSetup.msi

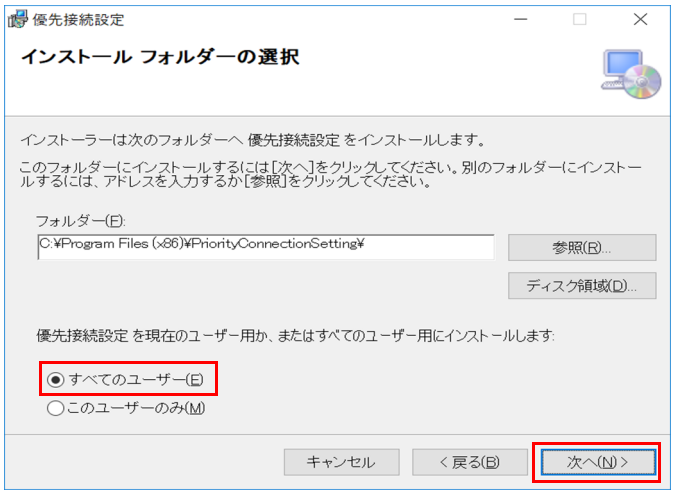
POINT

▸「このセットアップは .NET Framework バージョン 3.5 を必要としています。・・・」というメッセージが表示された場合は、「いいえ」をクリックし、「NET Framework 3.5」を有効化してください（→P.185）。有効化が完了したら、再度、「PriorityBandwidthCtrlSetup.msi」を実行してください。



3 「次へ」をタップします。
インストール先フォルダーの入力画面が表示されます。

4 「すべてのユーザー」を選択し、「次へ」をタップします。



「インストールの確認」が表示されます。

5 「次へ」をタップします。

POINT

▸ユーザーアカウント制御の画面が表示される場合は、「はい」タップします。

インストールが開始されます。しばらくすると、「インストールが完了しました。」と表示されます。

6 「閉じる」をタップします。
以上で優先接続設定のインストールは終了です。

優先接続設定の設定ファイルの変更

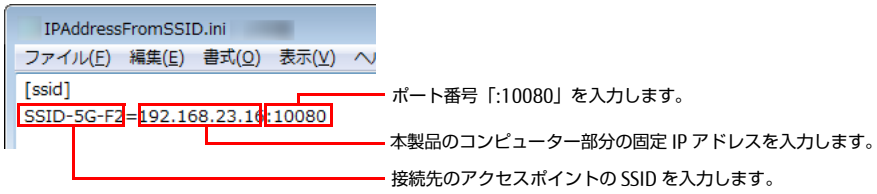
1 次のファイルを USB メモリーにコピーします。

C:¥Program Files (x86)¥FCCL¥PriorityConnectionSetting¥Ini¥IPAddressFromSSID.ini

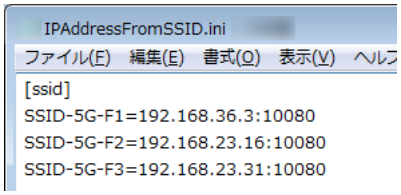
2 USB メモリーにコピーした「IPAddressFromSSID.ini」設定ファイルをエッジコンピューティングデバイスのテキストエディターで開きます。

3 次の部分を変更します。

接続先のアクセスポイントの SSID と本製品のコンピューター部分の固定 IP アドレスを次のように設定します。



複数登録する場合は、次のように設定します。



4 変更後、保存してファイルを閉じます。

5 USB メモリーの「IPAddressFromSSID.ini」設定ファイルを次のフォルダーに移動して、既存のファイルと置換します。

C:¥Program Files (x86)¥FCCL¥PriorityConnectionSetting¥Ini

POINT

▸「対象のフォルダーへのアクセスは拒否されました」というメッセージが表示される場合は、「続行」をタップします。

優先接続設定の起動

次の手順で「優先接続設定」を起動します。

1 ネットワークへ接続します。（設定済みの SSID：SSID-5G-F2 など）

2 → 「優先接続設定」の順にタップします。

「優先接続設定」が起動します。

■ 優先接続設定が正しく起動／表示されない原因

●「優先接続設定の変更処理が失敗しました」のメッセージが表示された場合、次の原因が考えられます。

・ アクセスポイント部分の Web 設定画面で、ユーザ DB に「smart」が設定がされていない（→ P.47）。

●その他

・ ネットワークに接続していない。
・ 対象の SSID を選択していない。
・ 接続対象以外のエッジコンピューティングデバイスへ接続している。
・ プロキシ設定に間違いがある。
・ 設定ファイル（IPAddressFromSSID.ini）に間違いがある。

12.拡張機能 - 画面共有 （製品本体）

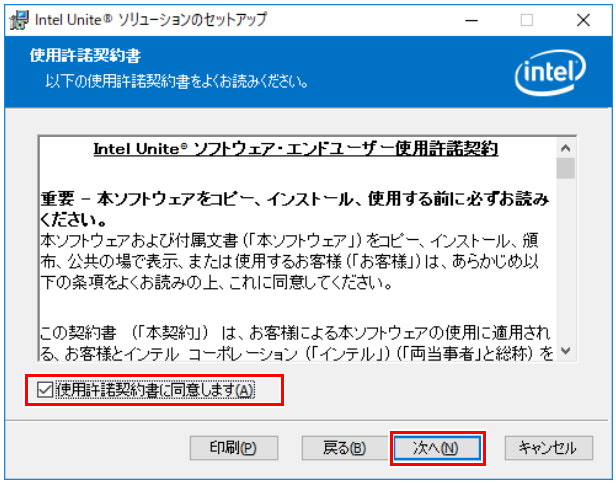
Intel Unite のインストール

本製品に Intel Unite をインストールします。

1 「C:¥Fujitsu¥Software¥IntelUnite¥Intel Unite Hub.mui.msi」を実行します。
セットアップ・ウィザードが表示されます。

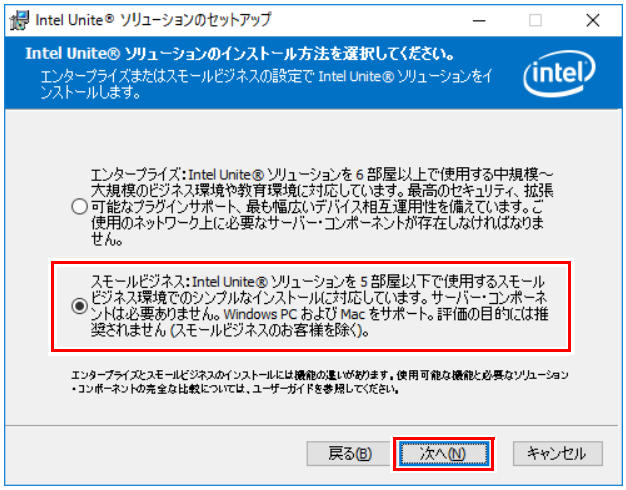
2 「次へ」をクリックします。
「使用許諾契約書」が表示されます。

3 使用許諾契約書を確認したら、「使用許諾契約書に同意します」にチェックを付けて、「次へ」をクリックします。



インストール方法の選択画面が表示されます。

4 「スモールビジネス」を選択して、「次へ」をクリックします。



インストール先フォルダーの入力画面が表示されます。

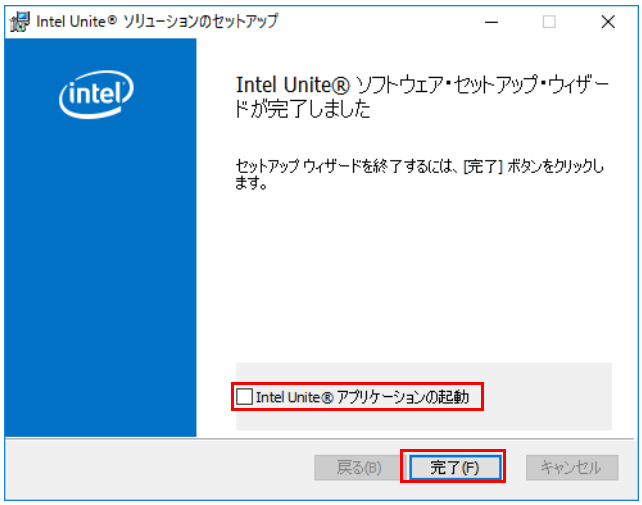
5 「次へ」をクリックします。
「インストール準備完了」が表示されます。

6 「インストール」をクリックします。

POINT
▸「ユーザーアカウント制御」ウィンドウが表示される場合は、「はい」をクリックします。

インストールが開始されます。

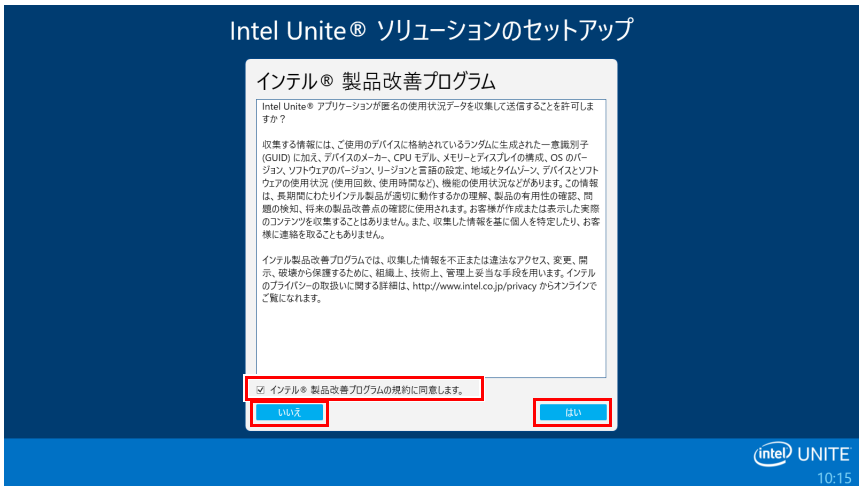
7 セットアップ・ウィザードが完了したら、「Intel Unite アプリケーションの起動」のチェックを外し、「完了」をクリックします。



8 デスクトップ画面の「IntelUniteSettings」をクリックします。
「Intel Unite ソリューションのセットアップ」が表示されます。

POINT
▸「ユーザーアカウント制御」ウィンドウが表示される場合は、「はい」をクリックします。

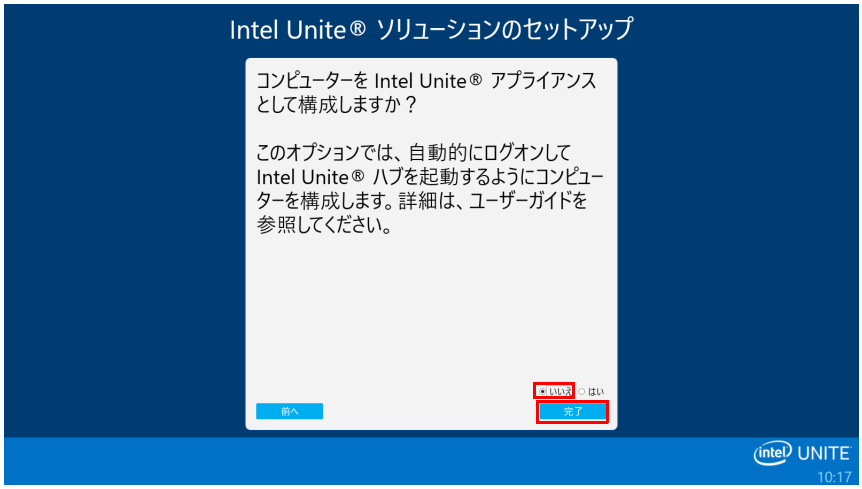
9「インテル製品改善プログラムの規約に同意します。」にチェックを付けて「はい」をクリックするか、「いいえ」をクリックします。



POINT
▸本ステートメントは、インテル社が将来の商品改善に役立てるため、デバイスデータと使用状況を収集することを許可するかどうかの確認となります。許可する場合は「はい」を、許可しない場合は「いいえ」を選択してください。どちらを選択してもIntel Uniteの動作に制限はありません。

「アプライアンスとして構成しますか？」と表示されます。

10「いいえ」を選択して「完了」をクリックします。



「構成が完了しました」と表示されます。

POINT

▸「はい」を選択し、「完了」ボタンを押した場合は、Intel Uniteをアンインストールし、再インストールまたはインストール時のデフォルト値へのリセットを行ってください。インストールのリセットについては、「Intel Uniteの詳細設定」（→P.195）をご覧ください。

11「閉じる」をクリックします。

以上で Intel Unite のインストールは終了です。

動作状態監視ツールの設定

動作状態監視ツールで Intel Unite を監視する場合は、次の設定を行ってください。監視しない場合は、本設定は不要です。

1 次のファイルをデスクトップにコピーします。

C:¥Program Files¥FCCL¥ProcessAliveWatcher¥Ini¥WatchProcessApp.ini

2 コピーした「WatchProcessApp.ini」をテキストエディターで開き、設定ファイルを変更します。

・[Intel Unite] セクション

```
[[Intel Unite]
ProcessEnable=False
ProcessKind=exe
RebootFilePath=C:\SmartMaintenance\bat\start_unite.bat;
```

「True」に変更します。

3 変更後、ファイルを保存して閉じます。

4 デスクトップの「WatchProcessApp.ini」設定ファイルを次のフォルダーに移動して、既存のファイルと置換します。

C:¥Program Files¥FCCL¥ProcessAliveWatcher¥Ini¥WatchProcessApp.ini

POINT

▸「対象のフォルダーへのアクセスは拒否されました」というメッセージが表示される場合は、「続行」をクリックします。

Intel Unite の設定

リモートビューの設定

リモートビューの機能は、動作保証していません。次の設定を必ず行ってください。

1「スタート」ボタン→「Intel」→「Intel Unite Settings」の順にクリックします。

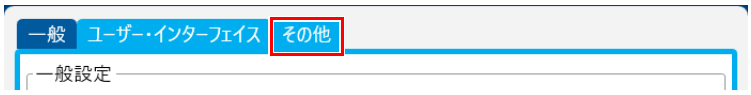
設定アプリが起動します。

POINT

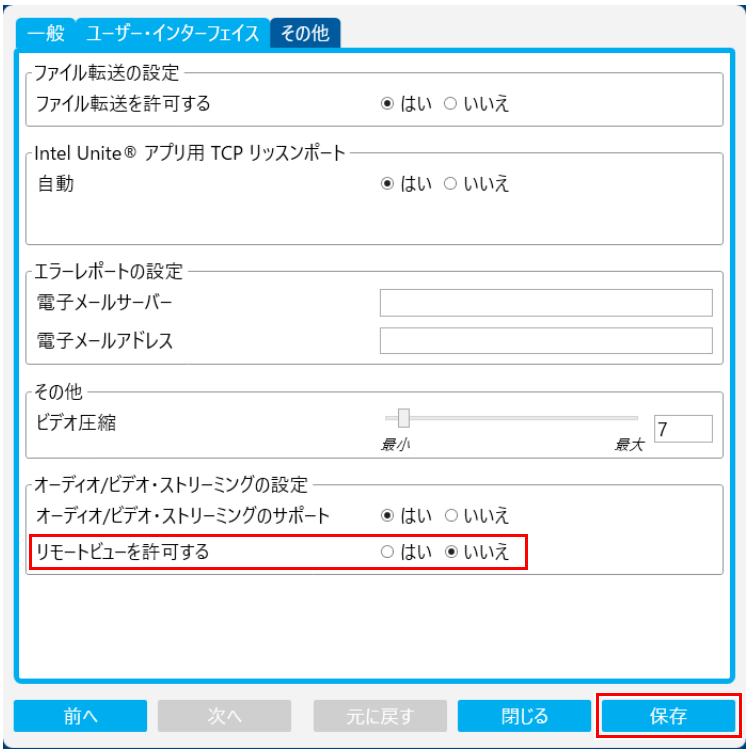
▸OS起動時にIntel Uniteが起動する場合は、次の手順でIntel Uniteを終了してから設定画面を起動してください。

1.USB キーボード、USB マウスを接続します。
2.画面上の任意の場所で 1 回左クリックします。
3.【Alt】+【F4】キーを押します。

2「その他」をクリックします。



3「リモートビューを許可する」を「いいえ」に設定し、「保存」をクリックします。



4「閉じる」をクリックします。

POINT

▸初期化設定、画面の設定、セキュリティ設定などを設定する場合は、「Intel Uniteの詳細設定」（→P.195）をご覧ください。

仮想デスクトップの設定

動作状態監視ツールによって自動的に Intel Unite が全画面で起動します。Intel Unite をインストール後、仮想デスクトップを使用して初期設定を行ってください。

■仮想デスクトップを設定する

1 タスクバーのタスクビューアイコン（ ）をクリックします。
デスクトップの右下に「新しいデスクトップ」が表示されます。

2 画面右下の「新しいデスクトップ」をクリックします。

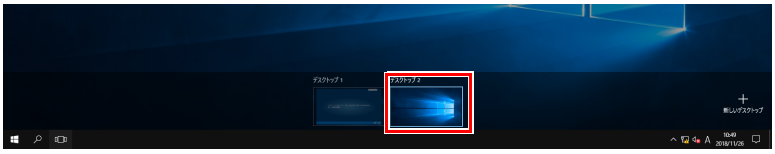
「デスクトップ 2」が作成されます。

■仮想デスクトップを使用する

Intel Unite が起動した場合は、次の手順で仮想デスクトップを使用してください。

1【 】キーを押します。
タスクバーが表示されます。

2 タスクバーのタスクビューアイコン（ ）をクリックします。
仮想デスクトップの一覧が表示されます。

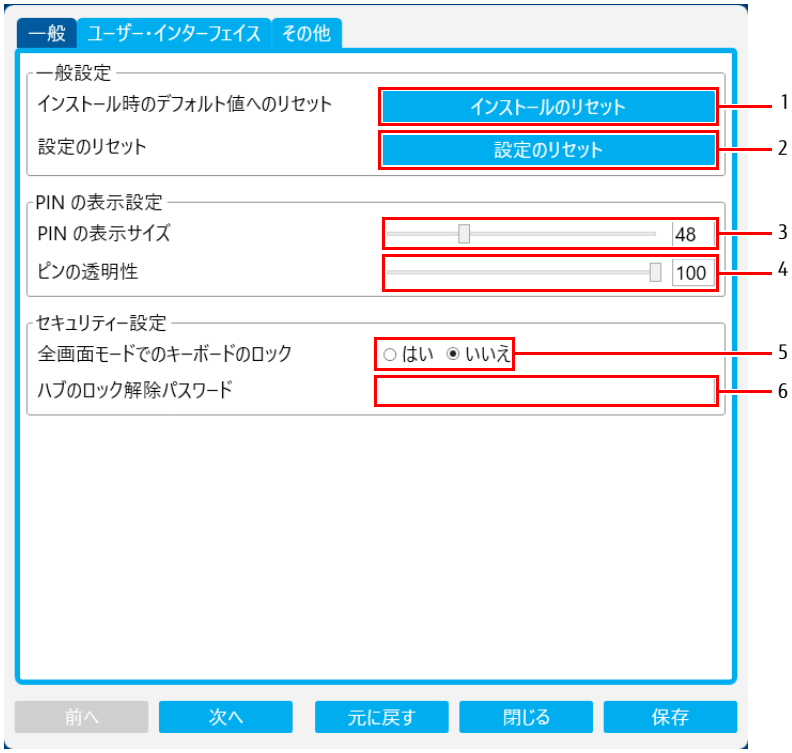


3「デスクトップ 2」をクリックします。
仮想デスクトップが表示されます。

Intel Unite の詳細設定

設定のリセットや画面表示の設定などをカスタマイズできます。なお、カスタマイズしなくても、そのまま Intel Unite をお使いいただけます。

■一般設定



1　**インストール時のデフォルト値へのリセット**
インストール中に行われたすべてのシステム変更を削除し、すべての設定を初期値に戻します。Intel Unite はシステムに残りますが、次回アプリを起動したときに「Intel Unite ソリューションのセットアップ」ウィザードが起動します。このオプションは、インストール時に選択したアプライアンス・モードを変更する場合に便利です。アプライアンス・モードを選択すると、OS 起動時に Intel Unite が起動します。

2　**設定のリセット**
すべての設定を初期値に戻します。インストール中に行われたシステム変更は削除されません。

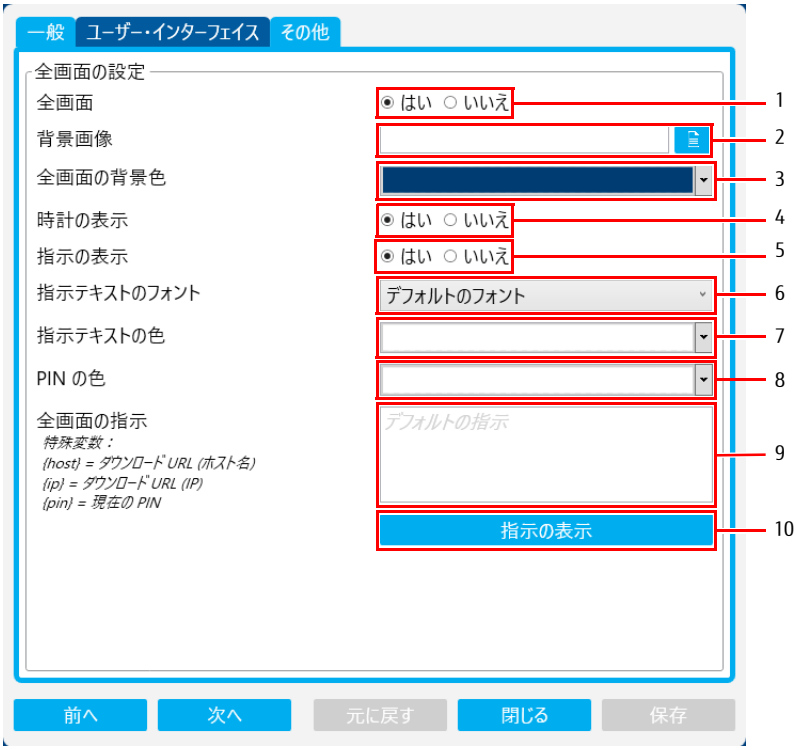
3　**PIN の表示サイズ**
画面の右上隅に表示される PIN のテキストサイズをカスタマイズすることができます。値の変更中は、例として 0000-0000 という PIN でプレビューが表示されます。

4　**ピンの透明性**
PIN の透明性を変更することができます。0 は透明で 100 は初期値の色モードです。0 ～ 100 の値で透明度を指定できます。

5　**全画面モードでのキーボードのロック**
「はい」に設定されている場合、「ハブのロック解除パスワード」が表示されます。
Intel Unite はキオスクモードで実行されます。キオスクモードでは、ユーザーがアプリを終了するために使用するキーの組み合わせがブロックされます。終了するには、本製品のロック解除パスワードを入力する必要があります。なお、初期値は「いいえ」に設定されています。

6　**ハブのロック解除パスワード**
「全画面モードでのキーボードのロック」が「はい」に設定されている場合にのみ表示されます。オプションの本製品のロック解除パスワードは、Intel Unite がキオスクモードで実行されている場合に使用されます。入力すると、Intel Unite が終了します。キオスクモードではパスワードを入力しているときは表示されませんので、注意してください。

■ユーザー ・ インターフェイス



1　**全画面**
「はい」に設定されている場合、Intel Unite は画面全体に表示されます。
「いいえ」に設定した場合、他の設定はすべて非表示になります。

2　**背景画像**
背景画像を選択できます。ファイル名を入力するか、または「参照」を使用してローカルの画像を指定します。

3　**全画面の背景色**
全画面モードで使用される背景色を設定します。テキストボックスをクリックすると、カラーピッカーが表示されます。カラーピッカーで色をクリックするか、16 進数値を指定したい場合は RGB カラースライダーを使用して、色を選択します。

4　**時計の表示**
「はい」に設定されている場合、現在のシステム時刻が画面の右下隅に表示されます。

5　**指示の表示**
「はい」に設定されている場合、テキスト指示が画面の中央に表示されます。初期値の指示を使用するか、または任意で指定することができます。

6　**指示テキストのフォント**
指示に使用されるフォントを設定します。

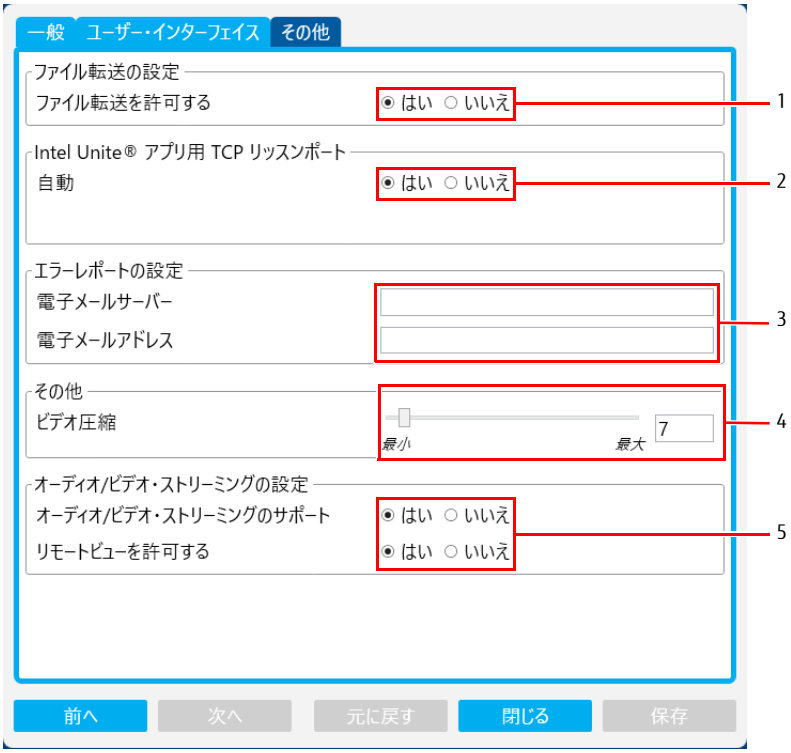
7　**指示テキストの色**
指示に表示されるテキストの色を設定します。テキストボックスをクリックすると、カラーピッカーが表示されます。カラーピッカーで色をクリックするか、16 進数値を指定したい場合は RGB カラースライダーを使用して、色を選択します。

8　**PIN の色**
指示には PIN を表示させることもできます。このオプションでは、強調するために PIN を別の色に設定することができます。テキストボックスをクリックすると、カラーピッカーが表示されます。カラーピッカーで色をクリックするか、16 進数値を指定したい場合は RGB カラースライダーを使用して、色を選択します。

9　**全画面の指示**
本製品に表示されているテキスト指示をカスタマイズすることができます。空白の場合、初期値の指示が表示されます。次の 3 つの特殊変数を使用できます。
・{host} 本製品のホスト名を表示します。
・{ip} 本製品のコンピューター部分の IP アドレスを表示します。
・{pin} 現在の PIN を表示します。

10　**指示の表示**
このボタンをクリックすると、現在の設定をプレビューできます。プレビューを終了するには、「指示の非表示」をクリックします。

■ その他



1　**ファイル転送を許可する**
「はい」に設定すると、接続されているタブレット端末は、本製品に接続されている他のユーザーにファイルを送信できるようになります。

2　**Intel Unite アプリ用 TCP リッスンポート**
Intel Unite がリッスンする TCP ポートを指定する、ネットワークの詳細設定です。
「自動」が「はい」に設定されたままにすることをお勧めします。
「自動」を「いいえ」に設定すると、Intel Unite が着信接続をリッスンする TCP ポートを選択できます。

3　**エラーレポートの設定**
電子メールサーバーの設定であり、エラーが発生した場合に通知を取得できるようにする詳細オプションです。次のオプションを指定する必要があります。
・電子メールサーバー
有効な SMTP サーバーを入力します。
・電子メールアドレス
電子メールを受信する有効な電子メールアドレスを入力します。

4　**ビデオ圧縮**
この詳細設定では、画面共有時に適用する圧縮率を指定します。値を大きくすると、必要な帯域幅は低減しますが、高い圧縮率が適用されるため画像が劣化する可能性があります。値を小さくすると、品質は向上しますが、より多くの帯域幅が必要になる場合があります。
推奨設定値は「7」です。

5　**オーディオ / ビデオ・ストリーミングの設定**
室内の参加者のみにオーディオ付きのビデオコンテンツを最大 1080p、20 ～ 30fps で表示および共有します。タブレット端末が Windows 10/Windows 8.1/Windows 7 の場合で、第 3 世代インテル® Core プロセッサー以上とインテル・グラフィックスが必要です。

重要
▸次の機能は動作保証していません。次の設定について「いいえ」を選択してください。
・リモートビューを許可する
別の部屋からリモートで表示できてしまうため、「いいえ」を選択して機能を無効にしてください。

■ 設定の保存と終了

すべての設定が終了したら、設定を保存するため次の操作を行ってください。

1 「保存」→「閉じる」の順にクリックしてください。

Intel Unite Settings が終了します。

13.拡張機能 - 画面共有 （タブレット端末）

Intel Unite のインストール

1 インストールするタブレット端末でブラウザーを起動し、本製品に接続している画面表示機器に表示されている URL を入力します。
本製品に接続するタブレット端末でブラウザーを起動し、本製品に表示される URL を入力します。

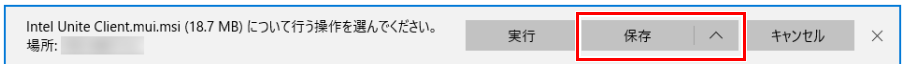
POINT

▸「Intel Unite Settings」の「ユーザー・インターフェイス」で「全画面の指示」の設定を行った場合、URLが表示されない場合があります。この場合は、「全画面の指示」の記載を削除するか、特殊変数を使ってダウンロードのURLを記載してください（→P.196）。

「Welcome to the Intel Unite app download」が表示されます。

2 「Intel Unite 3.3 for Microsoft Windows」をタップします。

3 「保存」をタップします。

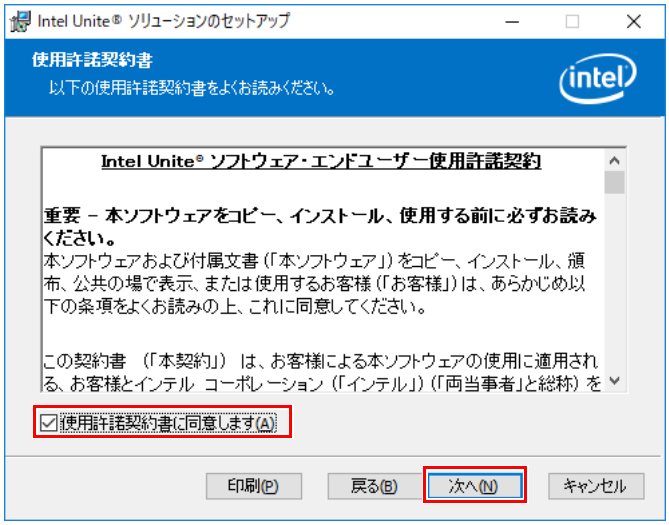


4 保存する場所を指定して、「保存」または「名前を付けて保存」をタップします。

5 ダウンロードした「Intel Unite Client.mui.msi」を実行します。
セットアップ・ウィザードが表示されます。

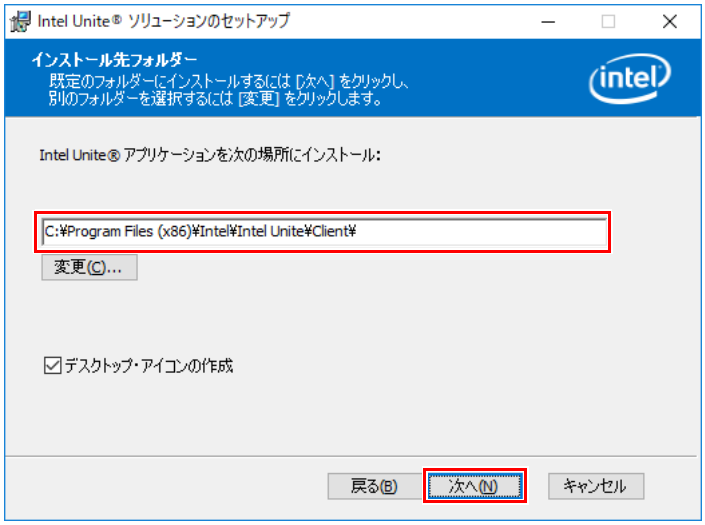
6 「次へ」をタップします。
「使用許諾契約書」が表示されます。

7　使用許諾契約書を確認したら、「使用許諾契約書に同意します」にチェックを付けて、「次へ」をタップします。



インストール先フォルダーの入力画面が表示されます。

8　インストール先を初期値のままにして、「次へ」をタップします。



「インストール準備完了」が表示されます。

9　「インストール」をタップします。

POINT

▸「ユーザーアカウント制御」ウィンドウが表示される場合は、「はい」をタップします。

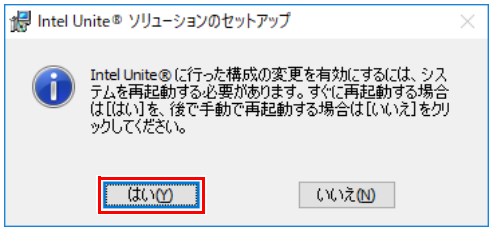
インストールが開始されます。

10　セットアップ・ウィザードが完了したら、「完了」をタップします。

POINT

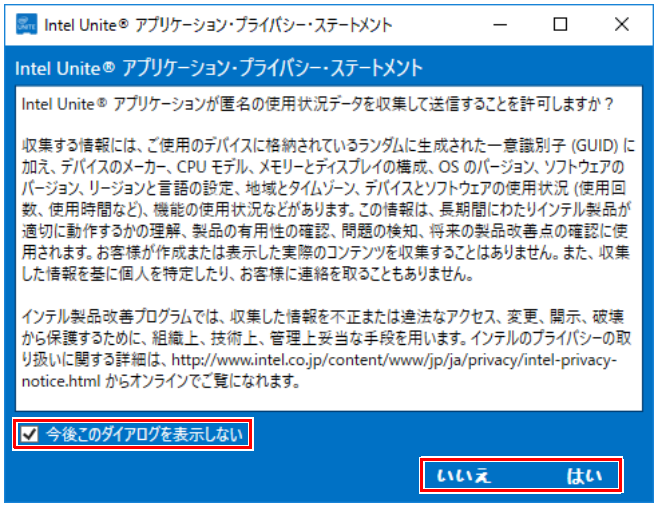
▸「Windows セキュリティの重要な警告」が表示された場合は、「アクセスを許可する」をクリックしてください。

11 再起動を要求されたら、「はい」をタップします。



12 再起動が完了したら、「スタート」ボタン→「Intel」→「Intel Unite」の順にタップします。
Intel Unite が起動します。
「Intel Unite アプリケーション・プライバシー・ステートメント」ウィンドウが表示されます。

13 「今後このダイアログを表示しない」にチェックを付けて、「はい」または「いいえ」をタップします。



POINT

- 本ステートメントは、インテル社が将来の商品改善に役立てるため、デバイスデータと使用状況を収集することを許可するかどうかの確認となります。許可する場合は「はい」を、許可しない場合は「いいえ」を選択してください。どちらを選択してもIntel Uniteの動作に制限はありません。

14 Intel Unite をインストールしたタブレット端末に「C:¥Intel¥Unitelog」フォルダーを作成します。

15 管理者権限でコマンドプロンプトを起動します（→ P.7）。

16 次のコマンドを入力し、【Enter】キーを押します。

```
reg add "HKEY_LOCAL_MACHINE¥Software¥Intel¥Unite" /v LogFile /t REG_SZ /d "C:¥Intel¥UniteLog¥UniteLogs.txt" /f
```

以上で Intel Unite のインストールは終了です。

5

第 5 章
セットアップの確認とバックアップ

インストールや設定の確認方法を説明しています。

1. 基本機能 - データキャッシュ機能

インターネットキャッシュ機能

『ユーザーガイド』の「インターネットキャッシュ機能を使用する」をご覧になり、事前キャッシュできることを確認してください。また、確認後、キャッシュを削除してください。

サーバファイルキャッシュ機能

サーバファイルキャッシュ機能に必要なサービスが開始されていることを確認します。

1 **「スタート」→「Windows 管理ツール」→「サービス」の順にクリックします。**
サービスが起動します。

2 **次のサービスが開始されていることを確認します。**

サービス名
AplCacheEngineService
AplCacheUIService

3 **サービスを閉じます。**

2. 基本機能 - 状態監視

動作状態監視ツール

状態監視に必要なサービスが開始されていることを確認します。

1 **「スタート」→「Windows 管理ツール」→「サービス」の順にクリックします。**
サービスが起動します。

2 **次のサービスが開始されていることを確認します。**

サービス名
ProcessAliveWatcher

3 **サービスを閉じます。**

お手入れナビ

1 **「コントロールパネル」を表示します（→ P.7）。**
「コントロールパネル」が表示されます。

2 **「プログラム」の「プログラムのアンインストール」をクリックします。**
「プログラムのアンインストールまたは変更」が表示されます。

3 **「お手入れナビ」が表示され、バージョンが「6.10.00.000」であることを確認します。**

3. 拡張機能 - 端末情報収集

バッテリー劣化診断

バッテリー劣化診断に必要なサービスが開始されていることを確認します。

エッジコンピューティングデバイスの確認

エッジコンピューティングデバイスで、バッテリー劣化診断に必要なサービスが開始されていることを確認します。

1 **「スタート」→「Windows 管理ツール」→「サービス」の順にクリックします。**
サービスが起動します。

2 **次のサービスが開始されていることを確認します。**

サービス名
Elasticsearch 5.5.0（elasticsearch-service-x64）
LogstashService
PortalAppService
SmartMaintBatteryBatService
SmartMaintDeleteBatService
SmartMaintMailBatService
SmartMaintSystemuptimeBatService
SmartMaintWebAppService
SmartMaintWirelesslanBatService
NginxService

3 **サービスを閉じます。**

タブレット端末の確認

タブレット端末で、バッテリー劣化診断に必要なサービスが開始されていることを確認します。

1 **「スタート」→「Windows 管理ツール」→「サービス」の順にタップします。**
サービスが起動します。

2 **次のサービスが開始されていることを確認します。**

サービス名
MaintInfoCollectionService

3 **サービスを閉じます。**

無線 LAN 診断

無線 LAN 診断に必要なサービスが開始されていることを確認します。

エッジコンピューティングデバイスの確認

エッジコンピューティングデバイスで、無線 LAN 診断に必要なサービスが開始されていることを確認します。

1 **「スタート」→「Windows 管理ツール」→「サービス」の順にクリックします。**
サービスが起動します。

2 **次のサービスが開始されていることを確認します。**

サービス名
Elasticsearch 5.5.0（elasticsearch-service-x64）
LogstashService
PortalAppService
SmartMaintBatteryBatService
SmartMaintDeleteBatService
SmartMaintMailBatService
SmartMaintSystemuptimeBatService
SmartMaintWebAppService
SmartMaintWirelesslanBatService
NginxService
WLAN 障害の自動診断

3 **サービスを閉じます。**

タブレット端末の確認

タブレット端末で、無線 LAN 診断に必要なサービスが開始されていることを確認します。

1 **「スタート」→「Windows 管理ツール」→「サービス」の順にタップします。**
サービスが起動します。

2 **次のサービスが開始されていることを確認します。**

サービス名
MaintInfoCollectionService

3 **サービスを閉じます。**

稼働時間

稼働時間に必要なサービスが開始されていることを確認します。

エッジコンピューティングデバイスの確認

エッジコンピューティングデバイスで、バッテリー劣化診断に必要なサービスが開始されていることを確認します。

1 **「スタート」→「Windows 管理ツール」→「サービス」の順にクリックします。**
サービスが起動します。

2 **次のサービスが開始されていることを確認します。**

サービス名
Elasticsearch 5.5.0（elasticsearch-service-x64）
LogstashService
MaintInfoCollectionService
PortalAppService
SmartMaintBatteryBatService
SmartMaintDeleteBatService
SmartMaintMailBatService
SmartMaintSystemuptimeBatService
SmartMaintWebAppService
SmartMaintWirelesslanBatService
NginxService

3 **サービスを閉じます。**

無線 LAN 接続台数表示

「無線 LAN 接続台数表示」をインストールしたパソコン／タブレット端末で、「無線 LAN 接続台数表示」が正常動作することを確認します。

1 **ネットワークへ接続します。（設定済みの SSID：SSID-5G-F2 など）**

2 **→「無線 LAN 接続台数表示」の順にタップします。**
画面の右下に、現在の接続台数が表示されます。

3 **現在、エッジコンピューティングデバイスのアクセスポイント部分に接続している端末の台数と同じ台数が表示されることを確認します。**
例：先生用端末 1 台、生徒用端末 1 台の場合、2 台と表示されます。

4. 拡張機能 - セキュリティ

端末認証

管理画面へログイン

1 ブラウザーを起動し、管理画面の URL（http://IP アドレス :10080/security/）に接続します。

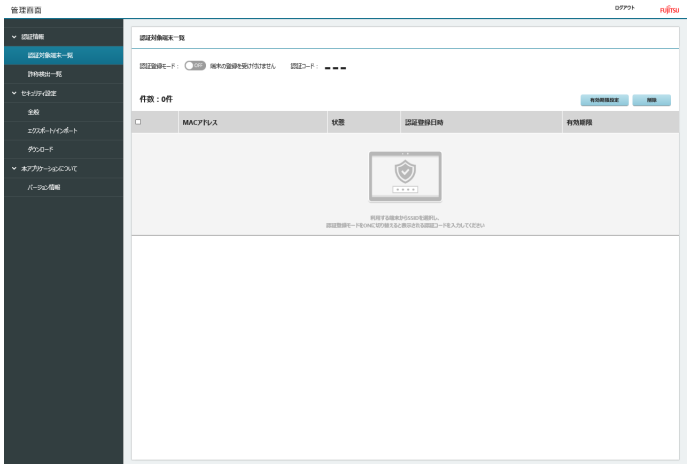
POINT

▸IPアドレスにはコンピューター部分のIPアドレスをお使いください。
コンピューター部分のIPアドレスが「192.168.1.3」の場合は次のようになります。
http://192.168.1.3:10080/security/

ログイン画面が表示されます。

2 アクセスポイント（AP）で利用している「root」アカウントのパスワードを入力し、「ログイン」をクリックします。
「パスワードの変更」（→ P.40）で変更したパスワードを入力してください。

3 ログインした後、次のような管理画面が表示されることを確認します。



5. 拡張機能 - ネットワーク

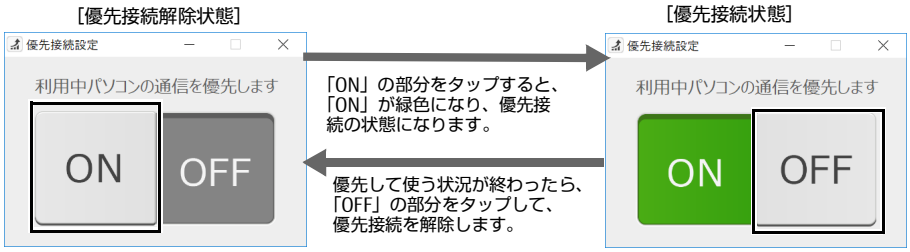
優先接続設定

「優先接続設定」をインストールしたパソコン／タブレット端末で、「優先接続設定」が正常動作することを確認します。

1 ネットワークへ接続します。（設定済みの SSID：SSID-5G-F2 など）

2 → 「優先接続設定」の順にタップします。
「優先接続設定」が起動します。

3 「OFF」→「ON」→「OFF」を押して、切り替えが正常に行われることを確認します。



POINT

- 優先接続設定で優先されるのは本製品1台につき、端末1台のみです。
- 本製品1台に対して複数の端末が優先接続を設定した場合、最後に設定した端末が優先されます。

6. 拡張機能 - 画面共有

Intel Unite

画面表示確認

エッジコンピューティングデバイスとタブレット端末で次の操作を行います。

1 『ユーザーガイド』をご覧になり、エッジコンピューティングデバイスに接続した画面表示機器の画面にタブレット端末の画面が表示できることを確認します。

バージョンの確認

エッジコンピューティングデバイスとタブレット端末で次の操作を行います。

1 「コントロールパネル」を表示します（→ P.7）。
「コントロールパネル」が表示されます。

2 「プログラム」の「プログラムのアンインストール」をクリックします。
「プログラムのアンインストールまたは変更」が表示されます。

3 「Intel Unite」が表示され、バージョンが「3.3.176.13」であることを確認します。

7. バックアップ

Windows や本製品のアプリが起動しなくなった場合に備え、システムイメージやアクセスポイントの設定をバックアップすることをお勧めします。
詳しくは、『管理ガイド』の「バックアップと復元」をご覧ください。

6

第 6 章
BIOS

BIOS セットアップについて説明しています。

1. BIOS セットアップ

BIOS セットアップは、メモリやフラッシュメモリディスクなどのハードウェアの環境を設定するためのプログラムです。

本製品ご購入時には、すでに最適なハードウェア環境に設定されています。次のような場合に BIOS セットアップの設定を変更します。

●特定の人だけが利用できるように、本製品の BIOS にパスワードを設定するとき

●起動デバイスを変更するとき

●セキュリティチップの設定を変更するとき

●Wake On LAN の設定を変更するとき

●起動時の自己診断（POST）に BIOS セットアップをうながすメッセージが表示されたとき

重要

- BIOSセットアップは、リモートデスクトップ接続で設定することはできません。必ず、本製品に、画面表示機器、USBキーボード、USBマウスを接続して設定してください。
- BIOSセットアップの設定は、必ず電源を切ってから行ってください。電源の切り方は、「電源を切る」（→P.35）をご覧ください。
- BIOSセットアップは正確に設定してください。
  設定を間違えると、本製品が起動できなくなったり、正常に動作しなくなったりすることがあります。
  このような場合には、変更した設定値を元に戻すか、ご購入時の設定に戻して本製品を再起動してください。
- 起動時の自己診断中は、電源を切らないでください。

2. BIOS セットアップの操作のしかた

ここでは、BIOS セットアップの起動と終了、および基本的な操作方法について説明しています。

BIOS セットアップを起動する

1 **【F2】キーまたは【Delete】キーを押したまま、本製品の電源を入れます。**

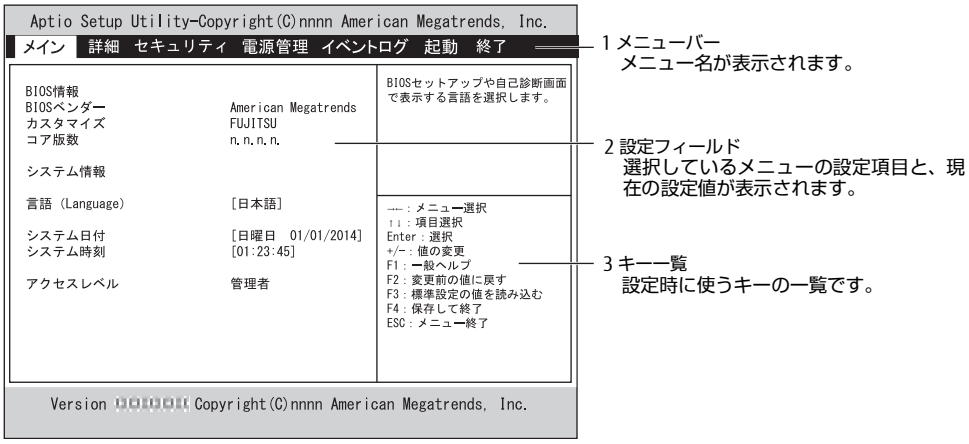
2 **BIOS セットアップ画面が表示されたら、【F2】キーまたは【Delete】キーを離します。**

POINT

▸Windowsが起動してしまった場合は、本製品の電源を完全に切ってからもう一度操作してください。電源の切り方は、「電源を切る」（→P.35）をご覧ください。

BIOS セットアップ画面

BIOS セットアップ画面の各部の名称と役割は、次のとおりです。
各項目についての説明は「項目ヘルプ」を、操作方法は「各キーの役割」（→ P.209）をご覧ください。



各キーの役割

BIOS セットアップで使う、主なキーの役割は次のとおりです。

キー	役割
【F1】キー	BIOS セットアップで使用するキーについて説明しているヘルプ画面が表示されます。 閉じる場合は、【Esc】キーまたは【Enter】キーを押します。
【←】【→】キー	メニューを切り替えます。
【↑】【↓】キー	設定する項目にカーソルを移動します。 【Page Up】【Page Down】キーを押すと、ページの先頭または最後にカーソルを移動できます。
【−】【+】キー	各項目の設定値を変更します。
【Shift】＋ 【↑】【↓】キー	項目の説明が表示されている部分をスクロールします。
【Esc】キー	「終了」メニューが表示されます。サブメニューが表示されている場合は、1 つ前の画面が表示されます。
【Enter】キー	・▶が付いている項目にカーソルを合わせて【Enter】キーを押すと、サブメニューが表示されます。 ・設定値にカーソルを合わせて【Enter】キーを押すと、設定値の一覧が表示され、設定値を選択できます。 ・時刻や日付の設定時に時、分、秒または年、月、日の間でカーソルを移動します。
【F2】キー	変更前の値を読み込みます。
【F3】キー	標準設定値を読み込みます。
【F4】キー	変更した設定値を保存して BIOS セットアップを終了します。

BIOS セットアップを終了する

変更を保存して終了する

1 「終了」メニューを選択します。
サブメニューが表示されている場合は、メニューバーに「終了」メニューが表示されるまで【Esc】キーを数回押してから、「終了」メニューを選択してください。

POINT
- 【Esc】キーを押し続けると、「変更を保存せずに終了しますか？」と表示されます。
  表示されたときは、もう一度【Esc】キーをして画面を消してから、「終了」メニューを選択してください。

2 「変更を保存して終了する（再起動）」または「変更を保存して終了する（電源 OFF）」を選択し、【Enter】キーを押します。
確認メッセージが表示されます。

3 「はい」を選択し、【Enter】キーを押します。
BIOS セットアップが終了します。「変更を保存して終了する（再起動）」を選択した場合は Windows が起動し、「変更を保存して終了する（電源 OFF）」を選択した場合は製品の電源が切れます。

変更を保存せずに終了する

1 「終了」メニューを選択します。
サブメニューが表示されている場合は、メニューバーに「終了」メニューが表示されるまで【Esc】キーを数回押してから、「終了」メニューを選択してください。

2 「変更を保存せずに終了する（再起動）」を選択し、【Enter】キーを押します。
確認メッセージが表示されます。

3 「はい」を選択し、【Enter】キーを押します。
BIOS セットアップが終了し、Windows が起動します。

起動メニューを使用する

起動するデバイスを選択して本製品を起動します。「システム修復ディスク」から本製品を起動する場合などに使用します。

1 【F12】キーを押したまま、本製品の電源を入れます。

2 起動メニューが表示されたら、【F12】キーを離します。
Windows が起動してしまった場合は、本製品の電源を完全に切ってからもう一度操作してください。電源の切り方は、「電源を切る」（→ P.35）をご覧ください。

3 カーソルキーで起動するデバイスを選択し、【Enter】キーを押します。
選択したデバイスから本製品が起動します。

POINT
- 光学ドライブから起動する場合、光学ドライブにディスクをセットしてから操作してください。
- UEFI起動メディアから起動する場合は、「UEFI：(光学ドライブ名)」を選択してください。
- 「UEFI：(光学ドライブ名)」が表示されていないときは、次の操作を行い、本製品を再起動してください。

1. ディスクをセットしたまま【Ctrl】＋【Alt】＋【Delete】キーを押し、続けて【F12】キーを押したままにします。
2. 起動メニューが表示されたら【F12】キーを離します。

POINT
- 光学ドライブから起動する場合、光学ドライブのデータの読み出しが停止していることを確認してから【Enter】キーを押してください。
  光学ドライブのデータの読み出し中に【Enter】キーを押すと、光学ドライブから正常に起動できない場合があります。
- 起動メニューを終了して通常の方法で起動する場合は、【Esc】キーを押してください。

3. 設定事例集

ここでは、よく使われる設定について、その設定方法を記載しています。お使いの状況にあわせてご覧ください。

その他の BIOS 設定については、「BIOS セットアップメニュー詳細」（→ P.216）をご覧ください。

BIOS のパスワード機能を使う

パスワードの種類

本製品で設定できるパスワードは次のとおりです。

■管理者用パスワード

システム管理者用のパスワードです。パスワード機能を使う場合は、必ず設定してください。

■ユーザー用パスワード

一般利用者用のパスワードです。管理者用パスワードが設定されている場合のみ設定できます。
ユーザー用パスワードで BIOS セットアップを起動した場合は、設定変更のできる項目が制限されます。制限された設定項目はグレー表示になり、変更できません。

POINT

▸管理者用パスワードが削除された場合、ユーザー用パスワードも削除されます。

■ハードディスクパスワード

本製品のハードディスクを、他のユーザーが使用したり、他のコンピューターで使用したりできないようにするためのパスワードです。管理者用パスワードを設定してからハードディスクパスワードを設定することをお勧めします。

パスワード入力が必要となる場合

管理者用パスワードを設定することにより、次の場合に入力が必要となります。
・BIOS セットアップを起動するとき
ユーザー用パスワードを設定することにより、次の場合に入力が必要となります。
・本製品を起動するとき
・休止状態からレジュームするとき
必要に応じて、管理者用またはユーザー用パスワードを入力してください。

パスワードを設定／変更／削除する

重要

▸ハードディスクパスワードを設定する場合は、電源オフ状態から作業を開始してください。本製品を再起動してBIOSセットアップを起動した場合、ハードディスクパスワードを設定することはできません。
▸「管理者用パスワード」を変更するには、BIOSセットアップを「管理者用パスワード」で起動する必要があります。

1 ハードディスクパスワードを設定する場合は、次の操作を行います。

1. 本製品の電源が入っている場合は、電源を切ります。
   電源の切り方は、「電源を切る」（→ P.35）をご覧ください。
2. BIOS セットアップを起動します（→ P.209）。

2「セキュリティ」メニューで次の項目を選択し、【Enter】キーを押します。

■ 管理者用パスワード／ユーザー用パスワードを設定する場合
・「管理者用パスワード設定」
・「ユーザー用パスワード設定」
■ ハードディスクパスワードを設定する場合
・「ハードディスクセキュリティ設定」→「Pn：(ハードディスクドライブ名)」の「ユーザーパスワード設定」

3 すでにパスワードが設定されている場合は、現在のパスワードを入力します。

「新しいパスワードを入力してください」にカーソルが移ります。

4 新しいパスワードを入力します。

管理者用パスワード／ユーザー用パスワードは 3 ～ 32 桁、ハードディスクパスワードは 1 ～ 32 桁まで入力できます。
パスワードを削除する場合は、何も入力せずに【Enter】キーを押します。
「新しいパスワードを確認してください」にカーソルが移ります。

重要

- パスワードには次の文字を使用できます。
  - ・半角英数字（a-z、A-Z、0-9）
  - ・半角スペース
  - ・半角記号（"|、「|」、「\（バックスラッシュ）」は除く）
  - 複数の種類のキーボードを接続する場合は、アルファベットと数字を使用することをお勧めします。また、接続するキーボードの種類にあわせ、事前に BIOS セットアップの「メイン」メニューの「キーボードレイアウト」を設定する必要があります。設定後は、「終了」メニューの「変更を保存して終了する（再起動）」または「変更を保存して終了する（電源 OFF）」を実行してください。
- 入力した文字は表示されず、代わりに「＊」が表示されます。
- 数字だけでなく英字を入れたり、定期的に変更したりするなど、第三者に推測されないように工夫してください。
- 本製品の修理が必要な場合は、必ずパスワードを解除してください。パスワードがかかった状態では、保証期間にかかわらず、修理は有償となります。

5 手順 4 で入力したパスワードをもう一度入力します。

「変更が保存されました。」と表示され、パスワードが変更されます。

POINT

- 再入力したパスワードが間違っていた場合は、警告メッセージが表示されます。【Enter】キーを押してウィンドウを消去し、手順4からやり直してください。

6 変更を保存して、BIOS セットアップを終了します。

「BIOS セットアップを終了する」（→ P.210）

パスワードを使用する

設定したパスワードは、BIOS セットアップの設定により、次の場合に入力が必要になります。

POINT

- 誤ったパスワードを3回入力すると、エラーメッセージが表示されます。この場合は、電源ボタンを4秒以上押して本製品の電源を切ってください。その後、10秒以上待ってからもう一度電源を入れて、正しいパスワードを入力してください。

●管理者用パスワード／ユーザー用パスワード

- BIOS セットアップを起動するとき
- 本製品を起動するとき
- 休止状態からレジュームするとき

次の入力画面が表示されたら、管理者用パスワードまたはユーザー用パスワードを入力してください。

```
パスワードを入力してください
_
```

●ハードディスクパスワード

- 本製品を起動するとき

次の入力画面が表示されたら、対応するドライブのハードディスクパスワードを入力してください。

```
P0:（ハードディスク名）
ハードディスクのパスワードを入力してください:
_
```

パスワードを忘れてしまったら

重要

- ハードディスクパスワードは、盗難などによる不正使用を防止することを目的とした強固なセキュリティです。ハードディスクパスワードを忘れてしまった場合、修理をしてもハードディスク内のデータやプログラムは復元できず、消失してしまいます。パスワードの管理には充分ご注意ください。

■対処が可能な場合

●ユーザー用パスワードを忘れてしまった

管理者用パスワードを削除すると、ユーザー用パスワードも削除されます。

■対処が不可能な場合

次の場合は、修理が必要です。「富士通ハードウェア修理相談センター」、またはご購入元にご連絡ください。修理は保証期間にかかわらず、有償になります。

●管理者用パスワードを忘れてしまった

●ハードディスクパスワードを忘れてしまった

起動デバイスを変更する

本パソコンの起動時に OS を読み込むデバイスの順序は、「起動」メニューの「起動デバイスの優先順位」で設定します。
「起動デバイス」に設定されている順に OS を検索します。
変更したデバイスの順序は、再起動後に反映されます。

1. **「起動」メニューを選択します。**
2. **「起動デバイスの優先順位」を選択し、【Enter】キーを押します。**
3. **設定を変更したい順位を選択し、【Enter】キーを押します。**
4. **設定したいデバイスを選択し、【Enter】キーを押します。**
   選択したデバイスの順位が入れ替わります。
5. **希望する順番になるまで手順 3 ～ 4 を繰り返します。**
6. **変更を保存して、BIOS セットアップを終了します。**
   「BIOS セットアップを終了する」（→ P.210）

セキュリティチップの設定を変更する

セキュリティチップを有効／無効にする

1. **「詳細」メニューを選択します。**
2. **「TPM（セキュリティチップ）設定」を選択し、【Enter】キーを押します。**
3. **「セキュリティチップ」を選択し、【Enter】キーを押します。**
4. **「有効にする」または「無効にする」を選択し、【Enter】キーを押します。**
5. **「終了」メニューの「変更を保存して終了する（再起動）」を選択し、【Enter】キーを押します。**
   確認メッセージが表示されます。
6. **「はい」を選択し、【Enter】キーを押します。**
   起動時の自己診断が実行された後、セキュリティチップの設定が変更されます。

セキュリティチップをクリアする

重要

- セキュリティチップをクリアすると、セキュリティチップで保護されたデータなどは利用できなくなります。
- セキュリティチップをクリアする前に保護を解除してください。

1. **「詳細」メニューを選択します。**
2. **「TPM（セキュリティチップ）設定」を選択し、【Enter】キーを押します。**
3. **「TPM 状態の変更内容」を選択し、【Enter】キーを押します。**

   POINT
   - 「TPM 状態の変更内容」を選択するためには、「セキュリティチップ」が「有効にする」に設定されている必要があります。
4. **「クリアする」を選択し、【Enter】キーを押します。**
5. **「終了」メニューの「変更を保存して終了する（再起動）」を選択し、【Enter】キーを押します。**
   確認メッセージが表示されます。
6. **「はい」を選択し、【Enter】キーを押します。**
   起動時の自己診断が実行された後、セキュリティチップの状態が変更されます。

ソフトウェアからの変更を反映する

Windows 上のソフトウェアを使ってセキュリティチップの状態を変更する場合、本製品の再起動後に、変更が有効になっていることがあります。
再起動を要求するメッセージが表示されたら、本製品を再起動してください。起動時の自己診断が実行された後、セキュリティチップの状態が変更されます。

Wake On LAN を有効にする

Wake on LAN 機能とは、他のコンピューターから有線 LAN 経由で本製品を起動・レジュームする機能です。ここでは、電源オフ状態から起動するための設定について説明します。電源を切る方法については、「電源を切る」（→ P.35）をご覧ください。

1 「電源管理」メニューを選択します。

2 「AC 通電再開時の動作」を選択し、【Enter】キーを押します。

3 「使用しない」以外を選択し、【Enter】キーを押します。

4 「LAN」を選択し、【Enter】キーを押します。

5 「使用する」を選択し、【Enter】キーを押します。

6 変更を保存して、BIOS セットアップを終了します。
「BIOS セットアップを終了する」（→ P.210）
Windows が起動します。続けて次の操作を行います。

7 「電源オプション」を表示します。
1. 「スタート」ボタン→ ⚙(設定）→「システム」の順にクリックします。
2. 画面左側のメニューで「電源とスリープ」をクリックします。
3. 画面右側の関連設定の「電源の追加設定」をクリックします。

8 ウィンドウ左の「スリープ解除のパスワード保護」、または「電源ボタンの動作を選択する」をクリックします。

9 「現在利用可能ではない設定を変更します」をクリックします。

10 「スタート」ボタン→ ⚙(設定）→「システム」の順にクリックします。

11 画面左側のメニューで「バージョン情報」をクリックします。

12 画面右側の関連設定の「デバイスマネージャー」をクリックします。
「デバイスマネージャー」が表示されます。

13 「ネットワーク アダプター」→「Intel（R）Ethernet Controller I219-LM」の順にダブルクリックします。
Intel LAN のプロパティが表示されます。

14 「詳細設定」タブで次の設定を変更します。
「PME をオンにする」を選択し、値を「有効」にします。

15 「OK」をクリックします。

POINT

- 本製品で、Wake On LAN機能を使用する場合、アクセスポイントで「Wake on LAN」の設定が必要です。詳しくは、『アクセスポイント操作ガイド』の「Wake on LAN」をご覧ください。
- 省電力状態からのレジューム設定には、デバイスマネージャーでの設定も必要になります。
  1. 「スタート」ボタン→ ⚙(設定）→「システム」の順にクリックします。
  2. 画面左側のメニューで「バージョン情報」をクリックします。
  3. 画面右側の関連設定の「デバイスマネージャー」をクリックします。
  「デバイスマネージャー」が表示されます。
  4. 「ネットワーク アダプター」→「Intel（R）Ethernet Controller I219-LM」の順にダブルクリックします。
  Intel LAN のプロパティが表示されます。
  5. 「電源の管理」タブをクリックします。
  6. Wake on LAN 機能を有効にするには次の項目にチェックを付け、無効にするにはチェックを外します。
  電力の節約のために、コンピューターでこのデバイスの電源をオフにできるようにする
  このデバイスで、コンピューターのスタンバイ状態を解除できるようにする
  （マジックパケットを受信したときのみ省電力状態からレジュームさせるようにするには、「Magic Packet でのみ、コンピューターのスタンバイ状態を解除できるようにする」にもチェックを付けます。）
  7. 「OK」をクリックします。

イベントログを確認する

1. **「イベントログ」メニューを選択します。**
2. **「イベントログの表示」を選択し、【Enter】キーを押します。**
   記録されているイベントログが表示されます。

イベントログに記録されるメッセージについては、「起動時に表示されるエラーメッセージ」（→ P.245）をご覧ください。

イベントログを消去する

1. **「イベントログ」メニューを選択します。**
2. **「イベントログ設定」を選択し、【Enter】キーを押します。**
3. **「イベントログの消去」を選択し、【Enter】キーを押します。**
4. **次回起動時に消去する場合は「次回起動時に消去します」を、毎回起動時に消去する場合は「毎回起動時に消去します」をそれぞれ選択し、【Enter】キーを押します。**
5. **変更を保存して、BIOS セットアップを終了します。**
   「BIOS セットアップを終了する」（→ P.210）

POINT

▸「イベントログの消去」に「次回起動時に消去します」を選択した場合、再起動すると設定値は「いいえ」になります。

ご購入時の設定に戻す

1. **「終了」メニューを選択します。**
2. **「標準設定値を読み込む」を選択し、【Enter】キーを押します。**
   確認メッセージが表示されます。
3. **「はい」を選択して【Enter】キーを押します。**
   次の項目を除くすべての設定が、ご購入時の設定値に戻ります。

   ■「標準設定値を読み込む」で変更されない項目
   - 日時の設定
   - 言語設定
   - キーボードレイアウト
   - 管理者用パスワード
   - ユーザー用パスワード
   - ハードディスクパスワード
   - 起動デバイスの優先順位
4. **変更を保存して、BIOS セットアップを終了します。**
5. **「電源を切る」（→ P.35）をご覧になり、本製品の電源を切ります。**

4. BIOS セットアップメニュー詳細

BIOS セットアップのメニューについて説明しています。
BIOS セットアップのメニューは次のとおりです。

メニュー	説明
メイン（→ P.216）	BIOS やパソコン本体についての情報が表示されます。 また、日時や言語を設定します。
詳細（→ P.217）	CPU や内蔵デバイス、周辺機器などを設定します。
セキュリティ（→ P.217）	パスワードなどのセキュリティ機能を設定します。
電源管理（→ P.217）	停電復旧時の動作や、Wake On LAN 機能などを設定します。
イベントログ（→ P.223）	イベントログに関する設定を行います。
起動（→ P.223）	起動時の動作について設定します。
終了（→ P.224）	設定値の保存や読み込み、BIOS セットアップの終了などを行います。

重要

- BIOSセットアップの仕様は、改善のために予告なく変更することがあります。あらかじめご了承ください。

POINT

- ユーザー用パスワードでBIOSセットアップを起動すると、設定変更のできる項目が制限されます。制限された項目はグレーに表示されます。ユーザー用パスワードでBIOSセットアップを起動した場合に変更できる項目は次のとおりです。

メニュー	設定項目
メイン	言語（Language）
	システム日付
	システム時刻
セキュリティ	ユーザー用パスワード設定
起動	起動時の NumLock 設定
	起動時のロゴ表示
終了	変更を保存して終了する（再起動）
	変更を保存せずに終了する（再起動）
	変更を保存して終了する（電源 OFF）

メインメニュー

□選択肢　■初期値

設定項目	備考
BIOS 情報	
BIOS ベンダー	
カスタマイズ	
コア版数	
コンプライアンス	
システム情報	
システムボードおよびファームウェア	
BIOS 版数	
BIOS 日付	
Board	
型名	
製造番号	
カスタムメイド番号	
UUID	
LAN デバイス	
LAN 1 MAC Address	
CPU 詳細	
CPU 名	
メモリ詳細	
メモリ容量／周波数	1MB=1024^2 バイト換算
DIMM CHA 1	1MB=1024^2 バイト換算
DIMM CHB 2	1MB=1024^2 バイト換算

□選択肢　■初期値

設定項目	備考
Open Source Software Licence Information	
言語（Language） □ English　■日本語	
システム日付 01/01/1998 ～ 12/31/2100	【Tab】キー／【Enter】キー … 右の項目に移動 数字キーで入力 OS が自動的に変更する場合あり
システム時刻 00：00：00 ～ 23：59：59	【Tab】キー／【Enter】キー … 右の項目に移動 数字キーで入力
キーボードレイアウト □ English(US) □ Spanish □ French □ Brazilian □ Dutch □ German □ Italian □ Swedish □ Danish □ Finnish □ Norwegian □ Russian ■日本語 □ Korean □ Chinese	BIOS パスワードを設定している場合は設定不可
アクセスレベル	BIOS セットアップを管理者用パスワードで起動した場合は「管理者」、ユーザー用パスワードで起動した場合は「ユーザー」と表示される

詳細メニュー

□選択肢　■初期値

設定項目	備考
オンボードデバイス設定	
内蔵 LAN デバイス ■使用する　□使用しない	
Status LED ■使用する　□使用しない	
CPU 設定	
アクティブコア ■全て／□ 1　□ 2　□ 3	
Intel Virtualization Technology □使用しない　■使用する	
VT-d ■使用しない　□使用する	
TXT 設定 ■使用しない　□使用する	下記の項目が次のように設定されているときに設定可能 「VT-d」が「使用する」 「セキュリティチップ」が「有効にする」
SW Guard Extentions (SGX) □使用しない　□使用する ■ソフトウェア制御	
Enhanced SpeedStep □使用しない　■使用する	※ 注
Turbo Mode □使用しない　■使用する	下記の項目が次のように設定されているときに設定可能 「Enhanced SpeedStep」が「使用する」 ※ 注
Package C State limit □ C0　□ C2　□ C3　□ C6 □ C7　□ C7s state　■自動	※ 注
ドライブ設定	
OnBorad SATA 設定	
SATA Mode ■ AHCI Mode □ Intel RST Premium With Untel Option System Acceleration	

□選択肢　■初期値

設定項目	備考
M.2 SATA Port 0	
Port 0 □使用しない　■使用する	
SATA Port 2	
Port 2 □使用しない　■使用する	
SATA Port 3	
Port 3 □使用しない　■使用する	
SMART 設定	
SMART 診断 ■使用しない　□使用する	
Acoustic Management 設定	※ 注
互換性サポートモジュール設定	
互換性サポートモジュール □使用しない　■使用する	下記の項目が次のように設定されているときに設定可能 「セキュアブート機能」が「使用しない」
ネットワークからの起動 □使用しない　□ UEFI のみ起動 ■ Legacy のみ起動	下記の項目が次のように設定されているときに設定可能 「互換性サポートモジュール」が「使用しない」 または「セキュアブート機能」が「使用しない」
TPM（セキュリティチップ）設定	
TPM（セキュリティチップ）設定	
セキュリティチップ □無効にする ■有効にする	
TPM 状態の変更内容 ■変更しない □クリアする	下記の項目が次のように設定されているときに設定可能 「セキュリティチップ」が「有効にする」 「セキュリティチップを有効／無効にする」（→ P.213）を参照
USB 設定	
USB 設定	接続されている USB デバイスを表示
USB レガシーサポート ■使用する　□使用しない □自動	
PS/2 デバイスエミュレーション ■使用しない　□使用する	
USB ポートセキュリティ	
USB ポート設定 ■全て有効　□全て無効 □前面と内部のみ有効 □背面と内部のみ有効 □内部のみ有効 □使用中ポートのみ有効	
USB デバイス設定 ■全てのデバイス □キーボード / マウスのみ □ストレージと Hub 以外	下記の項目が次のように設定されているときに設定可能 「USB ポート設定」が「前面と内部のみ有効」 または「背面と内部のみ有効」 または「使用中ポートのみ有効」
System Management	
FAN 制御 ■ Enhanced　□自動　□ Full	※ 注
温度	
CPU	温度センサー（CPU 内蔵）の現在の状態
M.2	温度センサー（M.2）の現在の状態
PSU	温度センサー（電源ユニットに搭載）の現在の状態
Core	温度センサー（Core）の現在の状態
Memory	温度センサー（Memory）の現在の状態
PCH	温度センサー（チップセット内部）の現在の状態
FAN	
SYS	システムファンの現在の状態

□選択肢　■初期値

設定項目	備考
シリアル設定	
シリアルポート 1 設定	
シリアルポート □使用しない　■使用する	
デバイス設定	下記の項目が次のように設定されているときに表示 「シリアルポート」が「使用する」
I/O アドレスと割り込み ■自動 □ IO=3F8h; IRQ4; □ IO=3F8h;IRQ3,4,5,6,7,9,10,11,12; □ IO=2F8h; IRQ3,4,5,6,7,9,10,11,12; □ IO=3E8h; IRQ3,4,5,6,7,9,10,11,12; □ IO=2E8h; IRQ3,4,5,6,7,9,10,11,12;	下記の項目が次のように設定されているときに設定可能 「シリアルポート」が「使用する」
シリアルポートコンソールリダイレクション設定	
コンソールリダイレクション ■使用しない　□使用する	
AMT 設定	
ME 版数	
Intel AMT BIOS Extension ■使用しない　□使用する	
AMT USB プロビジョニング ■使用しない　□使用する	
AMT/ME 設定のクリア ■使用しない　□使用する	
ME セットアップ ■Normal　□Enter MEBx Setup	
ネットワークスタック	
ネットワークスタック □使用しない　■使用する	
IPV4 環境での起動 □使用しない　■使用する	下記の項目が次のように設定されているときに設定可能 「ネットワークスタック」が「使用する」
IPV6 環境での起動 □使用しない　■使用する	下記の項目が次のように設定されているときに設定可能 「ネットワークスタック」が「使用する」
内蔵ビデオ設定	
内蔵ビデオ設定	
プライマリディスプレイ ■自動　□内蔵ビデオ	
内蔵ビデオ ■自動　□使用しない □使用する	
内蔵ビデオメモリサイズ □ 32MB　■ 64MB □ 128MB　□ 256MB □ 512MB　□ 1024MB □ 1536MB	下記の項目が次のように設定されているときに設定可能 「内蔵ビデオ」が「自動」または「使用する」 ※ 注
DVMT メモリサイズ □ 128MB　■ 256MB □ MAX	下記の項目が次のように設定されているときに設定可能 「内蔵ビデオ」が「自動」または「使用する」 ※ 注
Intel（R）Ethernet Controller	オンボード LAN デバイスのオプション ROM に関するサブメニュー ※ 注

注　：本設定は初期値のまま変更せずにお使いください。

セキュリティメニュー

□選択肢　■初期値

設定項目	備考
管理者用パスワード設定	「BIOS のパスワード機能を使う」（→ P.211）を参照
ユーザー用パスワード設定	「BIOS のパスワード機能を使う」（→ P.211）を参照
起動時のパスワード入力 □毎回　□最初のみ ■使用しない	管理者用パスワード設定時に設定可能 毎回 … 本製品の起動時ごとに、パスワード入力を要求 最初のみ … 本製品の電源を入れたときにのみ、パスワード入力を要求 使用しない … 本製品の起動時に、パスワード入力の要求なし 「BIOS のパスワード機能を使う」（→ P.211）を参照
自動ウェイクアップ時の パスワードスキップ ■使用しない　□使用する	管理者用パスワード設定時に設定可能 使用しない … 自動ウェイクアップ時での起動時に、パスワード入力を要求 使用する … 自動ウェイクアップ時での起動時に、パスワード入力の要求なし ハードディスクパスワードの入力スキップは不可
システムファームウェア更新機能 □使用しない ■使用する（制限付き） □使用する	
起動時の HDD パスワード入力 ■使用する　□使用しない	ハードディスクパスワード設定時に設定可能 使用する … 本製品起動時に、ハードディスクパスワード入力を要求 使用しない … 本製品起動時に、ハードディスクパスワード入力の要求なし 「BIOS のパスワード機能を使う」（→ P.211）を参照
〔ハードディスクドライブ名〕	
ハードディスクセキュリティ設定	
Security Supported	設定状況を表示
Security Enabled	設定状況を表示
Security Locked	設定状況を表示
Security Frozen	設定状況を表示
ユーザーパスワードの状態	設定状況を表示
マスターパスワードの状態	設定状況を表示
ユーザーパスワード設定	電源投入直後に BIOS セットアップを起動した場合に設定可能。再起動後は表示されない。
セキュアブート設定	
署名情報の保護	設定状態を表示 「無効（セットアップモード）」または「有効（ユーザーモード）」と表示される
セキュアブート	設定状態を表示 「セキュアブート機能」が「使用する」時は「使用する」、「使用しない」時は「使用しない」と表示される
Vendor Keys	セキュアブート機能が「使用する」時の設定状態を表示
セキュアブート機能 □使用しない　■使用する	※ 注 1 ※ 注 2
署名情報設定 ■標準　□カスタム	
署名情報の管理	
署名情報の初期化 □使用しない　■使用する	下記の項目が次のように設定されているときに設定可能 「署名情報設定」が「カスタム」
署名情報の初期化	下記の項目が次のように設定されているときに表示／設定可能 「署名情報設定」が「カスタム」 「署名情報の初期化」が「使用する」
署名情報の削除	下記の項目が次のように設定されているときに表示／設定可能 「署名情報設定」が「カスタム」 「署名情報の初期化」が「使用しない」
キーの保存	下記の項目が次のように設定されているときに設定可能 「署名情報設定」が「カスタム」
Platform Key(PK)	
Save To File	下記の項目が次のように設定されているときに設定可能 「署名情報設定」が「カスタム」
Set New Key	下記の項目が次のように設定されているときに設定可能 「署名情報設定」が「カスタム」
Delete Key	下記の項目が次のように設定されているときに設定可能 「署名情報設定」が「カスタム」

□選択肢　■初期値

設定項目	備考
Key Exchange Key	
Save To File	下記の項目が次のように設定されているときに設定可能 「署名情報設定」が「カスタム」
Set New Key	下記の項目が次のように設定されているときに設定可能 「署名情報設定」が「カスタム」
Append Key	下記の項目が次のように設定されているときに設定可能 「署名情報設定」が「カスタム」
Delete Key	下記の項目が次のように設定されているときに設定可能 「署名情報設定」が「カスタム」
Authorized Signatures	
Save To File	下記の項目が次のように設定されているときに設定可能 「署名情報設定」が「カスタム」
Set New Key	下記の項目が次のように設定されているときに設定可能 「署名情報設定」が「カスタム」
Append Key	下記の項目が次のように設定されているときに設定可能 「署名情報設定」が「カスタム」
Delete Key	下記の項目が次のように設定されているときに設定可能 「署名情報設定」が「カスタム」
Forbidden Signatures	
Save To File	下記の項目が次のように設定されているときに設定可能 「署名情報設定」が「カスタム」
Set New Key	下記の項目が次のように設定されているときに設定可能 「署名情報設定」が「カスタム」
Append Key	下記の項目が次のように設定されているときに設定可能 「署名情報設定」が「カスタム」
Delete Key	下記の項目が次のように設定されているときに設定可能 「署名情報設定」が「カスタム」
Authorized TimeStamps	
Set New Key	下記の項目が次のように設定されているときに設定可能 「署名情報設定」が「カスタム」
Append Key	下記の項目が次のように設定されているときに設定可能 「署名情報設定」が「カスタム」
OSRecivery Signatures	
Set New Key	下記の項目が次のように設定されているときに設定可能 「署名情報設定」が「カスタム」
Append Key	下記の項目が次のように設定されているときに設定可能 「署名情報設定」が「カスタム」
Easy PC Protection	
Easy PC Protection □使用する　■使用しない	

注 1：「セキュアブート機能」が「使用する」で、Windows 10（UEFI モード）以外の OS から起動した場合、「起動可能なデバイスがみつかりませんでした」などのメッセージが表示されます。

注 2：Windows 10 のモード（UEFI ／レガシー）は、次の手順で確認できます。
Windows 10 を起動します。
タスクバーの「検索」ボックスに、「msinfo32」と入力して【Enter】キーを押します。
「システム情報」が表示され、「BIOS モード」の項目に「UEFI」または「レガシー」が表示されています。

電源管理メニュー

□選択肢　■初期値

設定項目	備考
電源管理設定	
AC 通電再開時の動作 □使用しない　■電源 OFF □電源 ON　□自動	設定変更は再起動後に有効 電源 OFF… 通電再開時に一瞬電源が入り、WoL などを初期化。その後電源 OFF。 自動 … 電源断発生時の状態による。 起動中、スリープは「電源 ON」 シャットダウン、休止状態は「電源 OFF」 ※ 注 1
電力制限 ■使用しない　□使用する	※ 注 7
電源オフ時の USB 電源供給 □電源 OFF　■電源 ON	※ 注 7

□選択肢　■初期値

設定項目	備考
ウェイクアップ設定	
LAN □使用しない　■使用する	設定変更は再起動後に有効 ※ 注 2 ※ 注 3 ※ 注 4 ※ 注 5 「Wake On LAN を有効にする」（→ P.214）を参照
LAN によるウェイクアップ後の起動 ■起動順位に従う □ネットワークから起動する	下記の項目が次のように設定されているときに設定可能 「LAN」が「使用する」
USB キーボード ■使用しない　□使用する	下記の項目が次のように設定されているときに設定可能 「電源オフ時の USB 電源供給」が「電源 ON」 ※ 注 7
時刻 ■使用しない　□使用する	設定変更は再起動後に有効 ※ 注 2 ※ 注 3 ※ 注 6
時 0 ～ 23	下記の項目が次のように設定されているときに設定可能 「時刻」が「使用する」
分 0 ～ 59	下記の項目が次のように設定されているときに設定可能 「時刻」が「使用する」
秒 0 ～ 59	下記の項目が次のように設定されているときに設定可能 「時刻」が「使用する」
モード □毎週　■毎日　□毎月	下記の項目が次のように設定されているときに設定可能 「時刻」が「使用する」
日曜日 □使用する　■使用しない	下記の項目が次のように設定されているときに設定可能 「時刻」が「使用する」 「モード」が「毎週」
月曜日 □使用する　■使用しない	下記の項目が次のように設定されているときに設定可能 「時刻」が「使用する」 「モード」が「毎週」
火曜日 □使用する　■使用しない	下記の項目が次のように設定されているときに設定可能 「時刻」が「使用する」 「モード」が「毎週」
水曜日 □使用する　■使用しない	下記の項目が次のように設定されているときに設定可能 「時刻」が「使用する」 「モード」が「毎週」
木曜日 □使用する　■使用しない	下記の項目が次のように設定されているときに設定可能 「時刻」が「使用する」 「モード」が「毎週」
金曜日 □使用する　■使用しない	下記の項目が次のように設定されているときに設定可能 「時刻」が「使用する」 「モード」が「毎週」
土曜日 □使用する　■使用しない	下記の項目が次のように設定されているときに設定可能 「時刻」が「使用する」 「モード」が「毎週」
日 1 ～ 31	下記の項目が次のように設定されているときに設定可能 「時刻」が「使用する」 「モード」が「毎月」

注 1： UPS などを使って通電再開時に電源を投入させたい場合は、「電源 ON」に設定してください。ただし、「電源 ON」設定時に、本製品の電源切断状態から AC 入力に瞬断が発生すると、本製品の電源が投入されることがあります。
注 2： Windows 10 および Windows 8.1 の場合、Windows の高速スタートアップを無効にしてください。
注 3： 「AC 通電再開時の動作」を「使用しない」に設定した場合、停電などの AC 電源切断が発生すると、次に本製品の電源を入れるまで本機能は使用できなくなります。
注 4： 省電力状態（スリープ状態）からレジューム（復帰）させることはできません。デバイスマネージャーでの設定が必要です。
注 5： 省電力状態（休止状態）からレジューム（復帰）させるには、デバイスマネージャーでの設定も必要です。
注 6： 省電力状態（スリープ状態）からレジューム（復帰）させることはできません。タスクスケジューラまたはタスクでの設定が必要です。
注 7： 本設定は初期値のまま変更せずにお使いください。

イベントログメニュー

□選択肢　■初期値

設定項目	備考
イベントログ設定	
イベントログ設定	
イベントログ □使用しない　■使用する	
イベントログ消去設定	
イベントログの消去 ■いいえ □次回起動時に消去します □毎回起動時に消去します	下記の項目が次のように設定されているときに設定可能 「イベントログ」が「使用する」 「イベントログを消去する」（→ P.215）を参照
イベントログフル ■何もしない □すぐに消去する	下記の項目が次のように設定されているときに設定可能 「イベントログ」が「使用する」
イベントログの表示	「イベントログを確認する」（→ P.215）を参照

起動メニュー

□選択肢　■初期値

設定項目	備考
起動設定	
起動時の NumLock 設定 ■ On　□ Off	Windows サインイン後は前回終了時の状態になる
起動時のロゴ表示 □使用しない　■使用する	
起動エラー時の動作 □起動を続ける ■キー押下まで待つ	※ 注 1
キーボードエラー検出 ■使用しない　□使用する	
UEFI 起動デバイス追加時の 優先順位 □標準　■最上位　□最下位	
起動メニュー □使用しない　■使用する	
リムーバブルメディアからの起動 ■使用しない　□使用する	
起動デバイスの優先順位	OS を読み込むデバイスの優先順位を設定 ※ 注 2 「起動デバイスを変更する」（→ P.213）を参照
Boot Option #n	n は起動の順位を示す ご購入時は次のように設定 #1: P2: [HDD デバイス名]: Windows Boot Manager #2: UEFI: IPv4 [LAN デバイス名] #3: UEFI: IPv6 [LAN デバイス名] ・ カスタムメイドオプションおよびお使いの状況により、起動順位は異なる ・「UEFI: [CD/DVD デバイス名]」は、UEFI 起動可能なディスクをセットしている場合に表示 ・ UEFI 起動デバイスから起動する場合は、BIOS 起動デバイスより上位に設定すること ・ 起動ドライブまたはディスクを交換すると、その順位が初期化され、最下位に追加される ・ UEFI アプリが、優先順位を変更することがある

注 1：本設定を「使用しない」に設定しても、エラーメッセージは表示され、イベントログにも記録されます。
注 2：ネットワークサーバーから起動するためには、「Wired for Management Baseline Version 2.0」に準拠したインストレーションサーバーシステムが必要となります。

終了メニュー

項目を選んで【Enter】キーを押すと、確認画面が表示されます。

設定項目	備考
変更を保存して終了する（再起動）	
変更を保存せずに終了する（再起動）	
変更を保存して終了する（電源 OFF）	
標準設定値を読み込む	次の項目は対象外 言語（Language） システム日付 システム時刻 キーボードレイアウト 管理者用パスワード ユーザー用パスワード ハードディスクパスワード 起動デバイスの優先順位 「ご購入時の設定に戻す」（→ P.215）を参照
強制起動	
起動デバイス名	

5. ME BIOS Extension セットアップメニュー詳細

ここでは、ME セットアップの主なメニュー項目について説明します。

「Intel(R) ME General Settings」メニュー

メニュー	備考
Change ME Password	ME セットアップのパスワードを変更します。 パスワード入力画面でパスワードを入力後、「ME セットアップ初期パスワードの変更」（→ P.36）の手順 5 以降をご覧になり、パスワードを変更してください。

「Intel(R) AMT Configuration」メニュー

□選択肢　■初期値

設定項目	備考
Manageability Feature Selection ■ Enabled　□ Disabled	AMT 機能の有効／無効を設定する。
SOL/IDER/KVM	「SOL/IDER/KVM」メニューを表示する。
Username and Password ■ Enabled　□ Disabled	SOL/IDE-R 使用時にユーザー認証を行うかどうかを設定する。
SOL ■ Enabled　□ Disabled	Serial Over LAN 機能の有効／無効を設定する。 本機能を有効に設定した場合、COM ポートを占有する。
IDER ■ Enabled　□ Disabled	IDE Redirection 機能の有効／無効を設定する。
KVM Feature Selection ■ Enabled　□ Disabled	KVM 機能の有効／無効を設定する。
User Consent	「User Consent」メニューを表示する。
Username and Password ■ None　□ KVM　□ All	SOL/IDE-R 使用時にユーザー認証を行うかどうかを設定する。
Opt-in Configurable from Remote IT □ Disable Remote Control of KVM Opt-In Policy ■ Enable Remote Control of KVM Opt-In Policy	リモートユーザーが KVM Opt-in ポリシーを変更できるかを設定する。
Password Policy □ Default Password Only □ During Setup And Configuration ■ Anytime	パスワードポリシーを設定する。
Network Setup	「Network Setup」メニューを表示する。
Intel(R) ME Network Name Settings	「INTEL(R) ME NETWORK NAME SETTINGS」メニューを表示する。
Host Name	本製品の AMT のコンピューターネームを設定する。
Domain Name	本製品の AMT のドメインネームを設定する。
Shared/Dedicated FQDN □ Dedicated　■ Shared	Intel ME の FQDN（完全修飾ドメイン名）を OS で認識されるドメイン名と共有するか、ME でのみ使用するかを設定する。
Dynamic DNS Update ■ Enabled　□ Disabled	DDNS プロトコルを使用し、IP アドレスと FQDN を DNS に登録するかを設定する。
Periodic Update Interval	初期値：1440（変更しない）
TTL	初期値：990（変更しない）
TCP/IP Settings	「TCP/IP SETTINGS」メニューを表示する。
Wired LAN IPV4 Configuration	「WIRED LAN IPV4 CONFIGURATION」メニューを表示する。
DHCP Mode ■ Enabled　□ Disabled	ネットワークの DHCP 機能で IP を自動取得するかどうかを設定する。 ペーパーレス会議システムは、固定 IP アドレスを使用するため、「Disabled」に設定する。
IPV4 Address	IP アドレスを設定する。
Subnet Mask Address	サブネットマスクを設定する。
Default Gateway Address	デフォルトゲートウェイの IP アドレスを設定する。
Preferred DNS Address	DNS サーバーの IP アドレスを設定する。
Alternate DNS Address	代替 DNS サーバーの IP アドレスを設定する。
Activate Network Access	ME セットアップで設定した値を反映させ、Intel ME をサービス提供状態にする。 ME セットアップで必要な設定を行った後でこの項目を選択すると、メッセージが表示されるので【Y】を押す。一度実行するとこの項目は非表示となる。 再表示させる場合は、「Unconfigure Network Access」を選択し、「Full Unprovision」を実行する。
Unconfigure Network Access	Intel ME サービスを提供前の状態に戻し、ME セットアップの設定をご購入時の状態に戻す。

□選択肢　■初期値

設定項目	備考
Remote Setup And Configuration	「AUTOMATED SETUP AND CONFIGURATION」メニューを表示する。
Current Provisioning Mode	現在のプロビジョニング TLS モードを表示する。
Provisioning Record	PKI/PSK プロビジョニング記録データを表示する。

7

第 7 章
トラブルシューティング

おかしいなと思ったときや、わからないことがあったときの対処方法について説明しています。

1. トラブル発生時の基本操作

トラブルを解決するにはいくつかのポイントがあります。トラブル発生時に対応していただきたい順番に記載しています。なお、画面表示機器、USB キーボード、USB マウスを接続した状態でご確認ください。

状況を確認する

トラブルが発生したときは、直前に行った操作や現在の製品の状況を確認しましょう。

メッセージなどが表示されたら控えておく

画面上にメッセージなどが表示されたら、メモ帳などに控えておいてください。マニュアルで該当するトラブルを検索する場合や、お問い合わせのときに役立ちます。

製品や周辺機器の電源を確認する

電源が入らない、画面に何も表示されない、ネットワークに接続できない、などのトラブルが発生したら、まず製品や周辺機器の電源が入っているか確認してください。

●電源ケーブルや周辺機器との接続ケーブルは正しいコネクタに接続されていますか？また緩んだりしていませんか？

●電源コンセント自体に問題はありませんか？

●他の電器製品を接続して動作するか確認してください。OA タップを使用している場合、OA タップ自体に問題はありませんか？

●他の電気製品を接続して動作するか確認してください。使用する装置の電源はすべて入っていますか？

●ネットワーク接続ができなくなった場合は、ネットワークを構成する機器（サーバー本体やハブなど）の接続や電源も確認してください。

●キーボードの上に物を載せていませんか？
　キーが押され、製品が正常に動作しないことがあります。

このほか、「起動・終了時のトラブル」（→ P.230）の「画面に何も表示されない」もあわせてご覧ください。

以前の状態に戻す

周辺機器の取り付けやソフトウェアのインストールの直後にトラブルが発生した場合は、いったん以前の状態に戻してください。

●周辺機器を取り付けた場合は、取り外します。

●ソフトウェアをインストールした場合は、アンインストールします。

その後、製品に添付されているマニュアル、「Readme.txt」などの補足説明書、インターネット上の情報を確認し、取り付けやインストールに関して何か問題がなかったか確認してください。
発生したトラブルに該当する記述があれば、指示に従ってください。

トラブルシューティングで調べる

「トラブルシューティング」（→ P.230）は、トラブルシューティングが記載されています。発生したトラブルの解決方法がないかご覧ください。

診断プログラムを使用する

診断プログラムを使用して、ハードウェアに障害が発生していないか診断してください。
まず BIOS の起動メニューにある診断プログラムで簡単に診断し、異常が発見されなければ続けて「富士通ハードウェア診断ツール」でデバイスを選んで詳しく診断します。
診断後にエラーコードが表示された場合は控えておき、「富士通ハードウェア修理相談センター」にご連絡ください。
診断時間は 5 ～ 10 分程度ですが、診断する内容や製品の環境によっては長時間かかる場合があります。

重要

- 診断プログラムを使用する場合は、完全に電源を切った状態から操作してください。
- 電源の切り方は、「電源を切る」（→P.35）をご覧ください。
- BIOSの設定をご購入時の状態に戻してください。
  診断プログラムを使用する前に、必ず、BIOSをご購入時の状態に戻してください。詳しくは、「ご購入時の設定に戻す」（→P.215）をご覧ください。
- 診断プログラムを使用する前に周辺機器を取り外してください。
  USBメモリや外付けハードディスクなど、ハードディスクやリムーバブルディスクと認識される周辺機器は、診断を行う前に取り外してください。
- 診断プログラムは、Bluetoothのキーボードおよびマウスでの操作ができません。USBキーボード／USBマウスを用意してください。

1 【F12】キーを押したまま、本製品の電源を入れます。

2 起動メニューが表示されたら、【F12】キーを離します。

POINT

- BIOSセットアップの「起動」メニューの「起動メニュー」が「使用しない」の場合は、起動メニューを使用できません。その場合は、「使用する」に設定し直してください。
  BIOSセットアップについては、「BIOSセットアップ」（→P.208）をご覧ください。
- 起動時のパスワードを設定している場合は、パスワードを入力し、すぐに【F12】キーを押してください。
- 起動メニューが表示されずWindowsが起動してしまった場合は、本製品の電源を切ってからもう一度操作してください。カーソルキーで「診断プログラム」を選択し、【Enter】キーを押します。

「診断プログラムを実行しますか？」と表示されます。

3 【Y】キーを押します。
ハードウェア診断が始まります。
ハードウェア診断が終了したら、診断結果が表示されます。診断結果が表示される前に、自動的に製品が再起動する場合があります。

4 次の操作を行います。
■ トラブルが検出されなかった場合
【Enter】キーを押してください。続けて「富士通ハードウェア診断ツール」が起動します。
「富士通ハードウェア診断ツール」ウィンドウと「注意事項」ウィンドウが表示されます。手順 5 へ進んでください。
■ トラブルが検出された場合
手順 5 以降の「富士通ハードウェア診断ツール」での診断は不要です。画面に表示された内容を控え、お問い合わせのときにお伝えください。その後、【Y】キーを押して製品の電源を切ってください。
電源が自動で切れない場合は、電源ボタンを押して電源を切ってください。

5 「注意事項」ウィンドウの内容を確認し、「OK」をクリックします。

6 診断したいアイコンにチェックが付いていることを確認し、「実行」をクリックします。
ハードウェア診断が始まります。

7 「診断結果」ウィンドウに表示された内容を確認します。
表示された内容に従って操作してください。エラーコードが表示された場合には控えておき、お問い合わせのときにお伝えください。

8 「診断結果」ウィンドウで「閉じる」をクリックします。
「富士通ハードウェア診断ツール」ウィンドウに戻ります。

9 「終了」をクリックします。
「終了」ウィンドウが表示されます。

10 「はい」をクリックします。
電源が切れ、診断プログラムが終了します。

2. トラブルシューティング

トラブルシューティングの対処を実施しても改善されない場合は、「富士通ハードウェア修理相談センター」、またはご購入元にご連絡ください。

起動 ・ 終了時のトラブル

Q ビープ音が鳴った

●電源を入れた後の自己診断（POST）時に、ビープ音が鳴る場合があります。
ビープ音によるエラー通知は、「ピーッ」「ピッ」「ピッピッ」「ピッピッピッ」のように、1 回または連続したビープ音の組み合わせにより行われます。
ビープ音が鳴る原因と対処方法は、次のとおりです。
・ メモリのテストエラー
　メモリが正しく取り付けられていないか、本製品でサポートしていないメモリを取り付けている可能性があります。
　メモリテストエラーの場合、画面には何も表示されません。
　メモリが正しく取り付けられているか確認してください。

上記のことを確認してもビープ音が鳴る場合は、「富士通ハードウェア修理相談センター」、またはご購入元にご連絡ください。

Q メッセージが表示された

●電源を入れた後の自己診断（POST）時に、画面にメッセージが表示される場合があります。「エラーメッセージ一覧」（→ P.245）の「■ 起動時に表示されるエラーメッセージ」で該当するメッセージを確認し、記載されている処置に従ってください。
上記の処置をしてもまだエラーメッセージが発生する場合は、本製品が故障している可能性があります。「富士通ハードウェア修理相談センター」、またはご購入元にご連絡ください。

Q 画面に何も表示されない

●電源ランプが点灯していますか？
電源ボタンを押して動作状態にしてください。

●画面表示機器に関して、次の項目を確認してください。
・ ケーブルのコネクタのピンが破損していませんか？
・ 画面表示機器のブライトネス／コントラストボリュームは、正しく調節されていますか？
・ 複数台の画面表示機器を接続している場合、製品本体の電源を入れる前に、画面表示機器の電源を入れていますか？
　必ず製品本体の電源を入れる前に画面表示機器の電源を入れてください。製品本体の電源を入れた後に画面表示機器の電源を入れると、画面が表示されないことがあります。そのような場合は、いったん電源を切ってから入れ直してください。

Q Windows が動かなくなってしまい、電源が切れない

● 次の手順で Windows を終了させてください。

1.【Ctrl】＋【Alt】＋【Delete】キーを押し、画面右下の「シャットダウン」アイコンをクリックします。
この操作で強制終了できないときは、電源ボタンを 4 秒以上押して電源を切り、電源ケーブルを抜いてください。30 秒以上待ってから再度電源ケーブルを接続し、電源を入れてください。

重要

▸強制終了した場合、プログラムでの作業内容を保存することはできません。
▸強制終了した場合は、フラッシュメモリディスクのチェックをお勧めします。

Windows ・ ソフトウェア関連のトラブル

ここでは、Windows、ソフトウェアに関連するトラブルを説明しています。トラブルにあわせてご覧ください。

Q ソフトウェアが動かなくなってしまった

●「タスクマネージャー」から、動かなくなったソフトウェアを強制終了してください。

重要

▸ソフトウェアを強制終了した場合、ソフトウェアでの作業内容を保存することはできません。
▸ソフトウェアを強制終了した場合は、フラッシュメモリディスクのチェックをお勧めします。

頻繁にフリーズするなど動作が不安定になる

●次の項目を確認してください。
・ ウイルス対策ソフトウェアでフラッシュメモリディスクをスキャンする
定期的にフラッシュメモリディスクをスキャンすることをお勧めします。
・C ドライブの空き容量が充分か確認する
Windows のシステムファイルが格納されている C ドライブの空き容量が少ないと、Windows の動作が不安定になることがあります。
C ドライブの空き容量が少ない場合は、空き容量を増やしてください。空き容量を増やすには次の方法があります。
・ごみ箱を空にする
・不要なファイルやソフトウェアを削除する
・ディスクのクリーンアップを行う
・ フラッシュメモリディスクのエラーチェックを行う
それでもトラブルが頻繁に発生する場合は、『管理ガイド』の「バックアップと復元」をご覧になり、システムイメージの復元を行ってください。

Windows やソフトウェアの動作が遅くなった

●通風孔などにほこりが付着し、本製品の内部が高温になっている可能性があります。
・『管理ガイド』の「お手入れ」をご覧になり、本製品のお手入れをしてください。
・ 再起動してください。問題が解決する場合があります。

アプリのヘルプを表示しようとすると「この ms-getstarted を開くには新しいアプリが必要です」と表示されヘルプが表示されない

●本製品の仕様です。
本製品では「GetStarted」が含まれていないためです。

「アクションセンター」の「ノート」が使用できない

●OneNote のクイックノートを起動しますが、OneNote は含まれないため使用できません。

メンテナンス機能のトラブル

管理画面を表示したたきに、入力フォームが表示されない（画面が真っ白になる）

●Internet Explorer でイントラネットサイトを互換モードで表示している場合、管理画面が正常に表示できないことがあります。
次の手順で設定を変更してください。
1.Internet Explorer 11 を起動します。
2.画面右上にある ツールアイコン ⚙（設定）→「互換表示設定」の順にクリックします。
「互換性設定の変更」が表示されます。
3.「イントラネットサイトを互換表示で表示する」のチェックを外します。

●本製品に親プロキシサーバーを設定している場合、管理画面が正常に表示できないことがあります。
1.Internet Explorer の画面の右上隅の（ツール）→「インターネット オプション」の順にクリックします。「インターネットのプロパティ」が表示されます。
2.「接続」タブをクリックし、「LAN の設定」をクリックします。
3.プロキシ サーバーの「LAN にプロキシ サーバーを使用する」にチェックが入っていることを確認し、「アドレス」にプロキシサーバーの IP アドレス、プロキシサーバーのポート番号が入っていることを確認します。
4.「例外」にエッジコンピューティングデバイスの IP アドレス :10080（管理画面のポート番号）と記載します。
エッジコンピューティングデバイスの IP アドレスが 192.168.1.1 だった場合
192.168.1.1:10080
と入力します。

●「ステータスランプ」（→ P.9）が点灯していますか？
ステータスランプが点灯している場合は、メンテナンス機能が停止している可能性があります。
次の手順で、本製品を再起動してください。
1.電源ボタンを押します。
しばらくすると、本製品の電源が切れます。
2.電源プラグをコンセントから抜きます。
3.30 秒以上待ってから電源プラグをコンセントに付けます。
4.電源ボタンを押します。

管理画面にログインできない、または、ログイン画面が表示されない

●nginx の設定ファイルについて、IP アドレス設定が間違っている可能性があります。
「nginx 設定ファイル変更」（→ P.82）をご覧になり、設定ファイルを確認してください。

●「NginxService」サービスが起動していない可能性があります。
「スタート」→「Windows 管理ツール」→「サービス」の順にクリックして、サービスが起動していることを確認してください。
サービスが登録されていない場合は、「メンテナンス機能各種サービスの追加」（→ P.83）をご覧になり、サービスを再設定してください。

管理画面の表示が更新されない、表示がおかしい

●管理画面を表示している端末、またはエッジコンピューティングデバイスのネットワークが切断されていないかご確認ください。
正しく接続されている場合は、ブラウザーの画面を更新（再読み込み）して管理画面を再表示してください。

管理画面で処理中のダイアログが消えない

●プロキシに本製品のコンピューター部分の IP アドレスを指定し、本製品のコンピューター部分の IP アドレスをプロキシの例外に設定していない場合、管理画面が正しく表示されないことがあります。
本製品のコンピューター部分の IP アドレスをプロキシの例外に設定してください。
・ 手動でプロキシを設定している場合
「手動プロキシ設定」（→ P.91）をご覧になり、プロキシの例外設定を行ってください。
・ 自動構成スクリプト（PAC ファイル）を使用している場合
PAC ファイルで本製品のコンピューター部分の IP アドレスをプロキシの例外に設定してください。

診断が行われない

●nginx の設定ファイルについて、IP アドレス設定が間違っている可能性があります。
「nginx 設定ファイル変更」（→ P.82）をご覧になり、設定ファイルを確認してください。

●「Elasticsearch」サービスが起動していない可能性があります。
「スタート」→「Windows 管理ツール」→「サービス」の順にクリックして、サービスが起動していることを確認してください。
サービスが登録されていない場合は、「無線 LAN 診断のインストールと設定」（→ P.181）をご覧になり、サービスを再設定してください。

●アクセスポイント部分の IP アドレスとパスワードが変更されている可能性があります。
ネットワーク管理者にご確認ください。

●「MibAPConfig.xml」設定ファイルが「C:¥ProgramData¥FCCL¥WirelesslanAnalysis」フォルダーに格納されていることを確認してください。また、記載されている IP アドレス、パスワードが正しいかご確認ください。
詳しくは、「MibAPConfig.xml 設定ファイルの変更」（→ P.183）をご覧ください。

●セキュリティ対策アプリの影響で、接続できない場合があります。
セキュリティ対策アプリのログと設定を確認してください。

●アクセスポイントの SSH でのアクセス可否設定が「拒否」に設定されている可能性があります。
アクセスポイントの Web 設定画面にて、SSH でのアクセス可否設定が「許可」に設定されているかご確認ください。

●フォルダー構成が間違っている可能性があります。次の項目をご覧になり、フォルダー構成を確認してください。
「cygwin64 フォルダーの配置」（→ P.62）
「メンテナンス機能のフォルダーの配置」（→ P.67）
「無線 LAN 診断のインストールと設定」（→ P.181）

●次のフォルダーに診断結果のログファイルが作成されていることを確認してください。
「C:¥ProgramData¥FCCL¥WirelesslanAnalysis¥Log」

●本製品と端末で時間がずれている場合、正しく診断できない場合があります。
ファイルを最新にするか、本製品と端末との時間を合わせてください。

「AP ログイン失敗」と診断された

●アクセスポイント部分の IP アドレスとパスワードが変更されている可能性があります。
ネットワーク管理者にご確認ください。

●アクセスポイントの SSH でのアクセス可否設定が「拒否」に設定されている可能性があります。
アクセスポイントの Web 設定画面にて、SSH でのアクセス可否設定が「許可」に設定されているかご確認ください。

●セキュリティ対策アプリに影響で、接続できない場合があります。
セキュリティ対策アプリのログと設定を確認してください。

●LAN ケーブルは外れていませんか？
アクセスポイント部分に接続する LAN ケーブル、および、アクセスポイント部分とコンピューター部分を接続する LAN ケーブルの接続を確認してください。

「IP なし」と診断された

●アクセスポイント部分の設定で DHCP 機能が OFF になっている可能性があります。
アクセスポイントの Web 設定画面で、DHCP の設定をご確認ください。

「DHCP 失敗」と診断された

●アクセスポイント部分の Web 設定画面で、「動作モード」が「ルータ」になっていることを確認してください。また、IP アドレスの割り振り可能範囲の設定が適切かをご確認ください。

「切断の可能性あり」と診断された

●端末の「MaintInfoCollectionService」サービスが起動していない可能性があります。
「スタート」→「Windows 管理ツール」→「サービス」の順にクリックして、サービスが起動していることを確認してください。
サービスが起動していない場合は、一覧から「MaintInfoCollectionService」を右クリックして「開始」をクリックしてください。

「接続失敗」と診断された

●端末接続時の設定が間違っている可能性があります。
アクセスポイントに接続したときに入力したネットワークセキュリティキーが間違っていないかご確認ください。

「RSSI 低下 / 干渉」と診断された

●端末の使用環境に問題ないかご確認ください。
端末がアクセスポイントから離れすぎてないかや、端末とアクセスポイントの間に遮へい物がないかなど、端末の使用環境に問題がないかをご確認ください。
●端末において接続したい SSID の電波が弱い可能性があります。
アクセスポイントの Web 設定画面で、アクセスポイントの送信出力を大きくするように設定を変更してください。
●ご使用のチャネルがすでに使用されている可能性があります。
アクセスポイントの Web 設定画面で、使用するチャネル番号を変更してください。

「認証またはその他端末問題」と診断された

●ご使用の端末がなんらかの要因で接続できない状態になっている可能性があります。
端末を再起動してください。また、端末の使用環境に問題ないかご確認ください。

「AP 異常」と診断された

●アクセスポイント部分になんらかの問題が発生し、端末が接続できなくなっています。
次の手順で本製品を再起動してください。
1.電源ボタンを押します。
2.シャットダウンしたら、電源プラグをコンセントから抜きます。
3.30 秒以上待ってから電源プラグをコンセントに付けます。
4.電源ボタンを押します。

診断結果やログを通知するメールが送信先に届かない

●次の手順でテストメールを送信して送信先にメールが届くかご確認ください。
1.ブラウザーで「管理画面」を表示します（→ P.84）。
2.「情報端末管理」→「収集・通知設定」→「SMTP 設定」の順にクリックします。
3.「テストメール送信先アドレス」に送信先のメールアドレスを入力し、「テスト送信」をクリックします。詳しくは、「メンテナンス機能の設定」（→ P.85）をご覧ください。
メールが届かない場合は、「SMTP 設定」をご確認ください。

●メール送信の指定日時に、本製品が起動していなかった可能性があります。

●「メンテナンス機能の設定」（→ P.85）をご覧になり、各設定項目について、メールの配信設定をご確認ください。「ステータスランプ」（→ P.9）が点灯していますか？
ステータスランプが点灯している場合は、メンテナンス機能が停止している可能性があります。
次の手順で、本製品を再起動してください。
1.電源ボタンを押します。
しばらくすると、本製品の電源が切れます。
2.電源プラグをコンセントから抜きます。
3.30 秒以上待ってから電源プラグをコンセントに付けます。
4.電源ボタンを押します。

端末稼働時間一覧にデータが表示されない

●端末稼働時間一覧には、当月のデータは表示されません。前月分のデータが表示されます。
月が替わるのをお待ちください。

端末稼働台数のデータが少ない

●端末稼働台数に表示されるデータは過去 1ヶ月分のデータです。それ以前のデータは表示されません。

管理画面に解析結果の一覧が表示されない

●「管理画面設定」の「インポート / エクスポート」で、インポートを実行している可能性があります。
インポート中は、「端末情報管理」の「無線 LAN 診断状況一覧」、「端末稼働時間一覧」、「バッテリー状況一覧」に解析結果の一覧が表示されず、次のメッセージが表示されます。

「インポート中です。インポート終了後に画面を表示します。」

インポート処理中は管理画面の表示が制限されます。インポートが終わるまでお待ちください。

エクスポートできない

●「管理画面設定」の「インポート / エクスポート」で、エクスポートできない場合は、ストレージの空き容量が少なくなっている可能性があります。
空き容量が 15GB より少ない場合は、不要なファイルを削除してください。

インポートできない

●エクスポートしたデータを他のフォルダーに移動していませんか？
インポート読み込み先フォルダーに、エクスポートしたすべてのデータが格納されていることを、確認してください。

インターネットキャッシュ機能のトラブル

Q 動画の再生が遅い

●本製品のストレージの空き容量が少なくなっている可能性があります。
不要なファイルや使用しなくなったキャッシュのコンテンツデータを削除してください。

●「ステータスランプ」（→ P.9）が点灯していますか？
ステータスランプが点灯している場合は、データキャッシュ機能が停止している可能性があります。
次の手順で、本製品を再起動してください。
1.電源ボタンを押します。
しばらくすると、本製品の電源が切れます。
2.電源プラグをコンセントから抜きます。
3.30 秒以上待ってから電源プラグをコンセントに付けます。
4.電源ボタンを押します。

Q ブラウザーでページが表示できない

●お使いのセキュリティ対策ソフトによってインターネットキャッシュ機能が正常に動作しない場合があります。この場合は、次のファイルをセキュリティ対策ソフトのチェックから除外してください。
C:¥cygwin64¥squid¥sbin¥squid.exe
C:¥cygwin64¥squid¥bin¥squidclient.exe

Q 管理画面のキャッシュ一覧が正しく表示されない

● 管理画面のキャッシュ一覧にキャッシュしたデータが正しく表示されない場合は、ブラウザーのキャッシュデータを削除してください。
※OS やブラウザーのアップデートにより、手順が変更になる可能性があります。
・ Internet Explorer の場合
1.Internet Explorer 11 を起動します。
2.画面右上にある ツールアイコン ⚙（設定）→「インターネット オプション」の順にクリックします。
3.「全般」タブを選択し、「削除」をクリックします。
4.すべての項目にチェックを付けて、「削除」をクリックします。
5.「OK」をクリックします。

・ Microsoft Edge（Chromium 版）の場合
1.Microsoft Edge を起動し、…（設定など）→「履歴」→「閲覧データをクリア」の順にクリックします。
2.「時間の範囲」で「すべての期間」を選択した後、すべての項目にチェックを付けて「今すぐクリア」をクリックします。

・ Google Chrome の場合
1.Google Chrome を起動し、⋮（Google Chrome の設定）→「その他のツール」→「閲覧履歴の削除」の順にクリックします。
「閲覧履歴データの削除」が表示されます。
2.「「詳細設定」の「期間」で「全区間」を選択した後、すべての項目にチェックを付けて「データ消去」をクリックします。

Q 管理画面のキャッシュ一覧のデータが削除される

●全キャッシュデータのサイズの合計がキャッシュディスクサイズの上限を超えるとキャッシュした日付の古いデータから順番に削除されていきます。
削除された場合は、再度、キャッシュしてください。

Q キャッシュエンジンの初期化後、キャッシュできない

●キャッシュエンジンの初期化を実行すると、管理画面で設定した値が全て削除されます。再度、設定してください（→ P.120）。

サーバファイルキャッシュ機能のトラブル

Q 学習支援アプリサーバにファイルをアップロードできない

●アップロードしようとしているファイルのサイズの合計が、サーバファイルキャッシュの閾値（初期値：80MB）を超えている可能性があります。
この場合、計画同期となり、同期計画対象時間帯にアップロードされます。すぐに学習支援アプリサーバにファイルをアップロードしたい場合は、管理画面の「簡易情報取得・手動制御」で、タブレット端末でファイルをアップロードしたときに接続していたエッジコンピューティングデバイスの「割込実行」を実行してください。

優先接続設定のトラブル

優先接続設定が正しく起動しない

● 優先接続設定を起動すると、次のメッセージが表示される場合があります。

起動に失敗しました。以下をご確認ください。
タブレットのネットワーク状態
コンピューターのネットワーク状態
本アプリの設定

・ タブレット端末が本製品に接続されていない可能性があります。
『ユーザーガイド』の「タブレット端末を無線 LAN に接続する」をご覧になり、お使いのタブレット端末の無線 LAN 接続を確認してください。

・ アクセスポイント部分になんらかの問題が発生し、端末が接続できなくなっています。
タブレット端末で利用できる SSID の一覧に本製品の SSID が表示されない場合は、アクセスポイント部分から無線電波が出ていない可能性があります。
本製品の SSID が表示されない場合は、次の手順で本製品を再起動してください。
1.電源ボタンを押します。
2.シャットダウンしたら、電源プラグをコンセントから抜きます。
3.30 秒以上待ってから電源プラグをコンセントに付けます。
4.電源ボタンを押します。

● 「優先接続設定の変更処理が失敗しました」のメッセージが表示された場合、次の原因が考えられます。
・ アクセスポイント部分の Web 設定画面で、ユーザ DB に「smart」が設定がされていない（→ P.47）。

●ネットワークに接続していない。
タブレット端末をネットワークに接続してください。

●対象の SSID を選択していない。
タブレット端末をエッジコンピューティングデバイスの SSID に接続してください。

●接続対象以外のエッジコンピューティングデバイスに接続している。
タブレット端末を接続対象のエッジコンピューティングデバイスに接続し直してください。

●プロキシ設定に間違いがある。
「プロキシの設定」（→ P.91）をご覧になり、タブレット端末のプロキシ設定を確認してください。

●設定ファイル（IPAddressFromSSID.ini）に間違いがある。
「プロキシ自動設定機能」（→ P.97）または「IPAddressFromSSID.ini の変更」（→ P.99）をご覧になり、設定ファイルが正しいことを確認してください。

無線 LAN 接続台数表示のトラブル

無線 LAN 接続台数表示が正しく起動しない

●「×」が表示され、台数が表示されない場合は、設定ファイルが間違えている可能性があります。
「無線 LAN 接続台数表示設定ファイルの変更」（→ P.186）をご覧になり、設定ファイルを確認してください。

●接続台数の画面が表示されずに「初期化に失敗しました」などのメッセージが表示される場合、次の原因が考えられます。
・ ネットワークに接続していない。
タブレット端末をネットワークに接続してください。
・ プロキシ設定に間違いがある。
「プロキシの設定」（→ P.91）をご覧になり、タブレット端末のプロキシ設定を確認してください。
・ 対象の SSID を選択していない。
タブレット端末をエッジコンピューティングデバイスの SSID に接続してください。
・ 接続対象以外のエッジコンピューティングデバイスに接続している。
タブレット端末を接続対象のエッジコンピューティングデバイスに接続し直してください。

●接続台数の画面が表示されずに「初期化に失敗しました」などのメッセージが表示される場合、次の原因が考えられます。
・ ネットワークに接続していない。
タブレット端末をネットワークに接続してください。
・ 設定ファイル（IPAddressFromSSID.ini）に間違いがある。
「プロキシ自動設定機能」（→ P.97）または「IPAddressFromSSID.ini の変更」（→ P.99）をご覧になり、設定ファイルが正しいことを確認してください。

Intel Unite のトラブル

PIN を入力したが、タブレット端末側で接続中と表示されたままになる

●PIN コードを 2 回連続で間違えて入力している可能性があります。
タブレット端末の Intel Unite を再起動してください。
1.タスクバーの Intel Unite アイコンを長押しタップして、「ウィンドウを閉じる」を選択します。
2.Intel Unite を起動します。
3.本製品の画面に表示されている PIN を確認して、再度、入力してください。

●本製品のファイアウォールの設定で Intel Unite の通信がブロックされている可能性があります。
ファイアウォールの設定で、Intel Unite の通信を許可してください。詳細は、「Intel Unite のファイアウォールの設定」（→ P.247）をご覧ください。

●タブレット端末のプロキシ設定に間違いがある可能性があります。
タブレット端末のプロキシ設定で、アドレスと例外に記載されている IP アドレスを本製品と同じ IP アドレスに設定してください。
タブレット端末のプロキシ設定の方法については、「プロキシの設定」（→ P.91）をご覧ください。

●本製品のメトリックの設定が導入時に変更されていない可能性があります。
「端末認証」を導入する場合、メトリックの設定を変更しないと接続できません。
メトリックの設定の変更方法については、「メトリックの設定」（→ P.159）をご覧ください。

端末認証機能のトラブル

認証エンジンが起動しない

●「Docker for Windows」サービスが起動していない可能性があります。
サービスが起動していない場合は、サービスを起動するか、
「C:¥Program Fiels¥Docker¥Docker¥Docker for Windows.exe」を実行してください。

●Docker が、前回起動時のポートを開放していない場合あります。
サービスを再起動してください。

管理アプリケーション（制御部）が起動しない

●mongoDB が起動していない可能性があります。
mongoDB が起動していない場合は、再起動してください詳しくは、「mongoDB の起動」（→ P.167）をご覧ください。

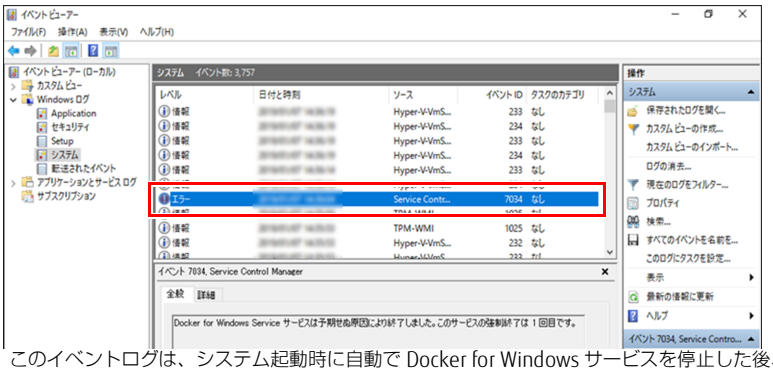
管理アプリケーション（UI 部）が起動しない

●格納ディレクトリのパスが間違っている可能性があります。
間違っている場合は、格納ディレクトリのパスを修正確認してください。詳しくは、「管理アプリのインストール」（→ P.153）をご覧ください。

イベントビューアーでエラーログが発生する

●端末認証システム起動時、「イベントビューアー」→「Windows ログ」→「システム」に以下のイベントログが登録されます。

ソース：Service Control Manager
イベント ID：7034
内容：Docker for Windows サービスは予期せぬ原因により終了しました。このサービスの強制終了は、○回目です。
※ ○には数字が入ります。



このイベントログは、システム起動時に自動で Docker for Windows サービスを停止した後、再起動しているため登録されます。動作に問題はありません。

管理画面のログイン画面が表示されない

●nginx が起動していない、もしくは設定が反映されていない可能性があります。
起動状態と設定を確認してください（→ P.157）。

管理画面にログインできない

●アクセスポイントが正常に起動していない可能性があります。
次の手順で、本製品を再起動してください。
1.電源ボタンを押します。
2.シャットダウンしたら、電源プラグをコンセントから抜きます。
3.30 秒以上待ってから電源プラグをコンセントに付けます。
4.電源ボタンを押します。

●管理アプリケーション（制御部）が停止している可能性があります。
本製品を再起動してください。

認証コード入力画面が表示されない

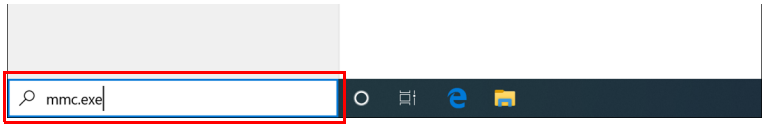
●認証登録モードが「OFF」になっていませんか？
端末認証機能の管理画面で、「認証登録モード」を「ON」に設定してください。

●アクセスポイントの設定が間違っている可能性があります。
SSID の設定について、次の点を確認してください。
・radius の参照 IP アドレス、ID/Pass が正しいこと。
・暗号化方式が「WPA2-Enterprose」になっていること。

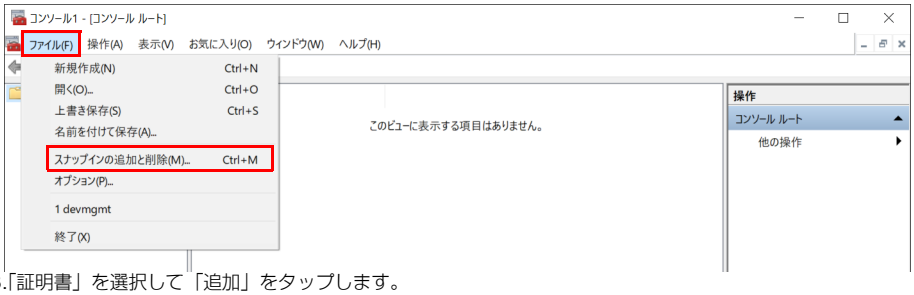
●ファイアウォールの設定が間違っている可能性があります。
・ セキュリティ設定が正しく設定されているか確認してください（→ P.160）。
・「Node.js」と「vpnkit」の操作がブロックされている場合は、規則を無効化します（→ P.168）。

●証明書の有効期限が切れている可能性があります。
下図のような証明書エラーが表示された場合は、証明書の有効期限が切れています。次の手順に従い証明書を削除した後、端末認証登録用の SSID（SWRegist-5G）を再度タップしてください。

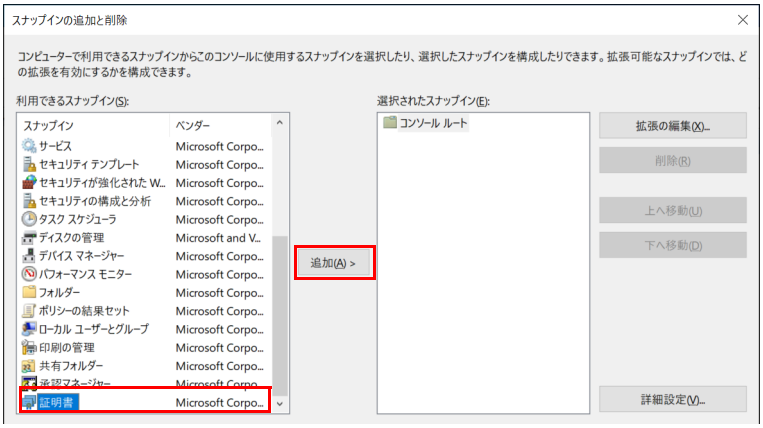
1.検索ボックスに「mmc.exe」を入力して、「Enter」キーを押します。



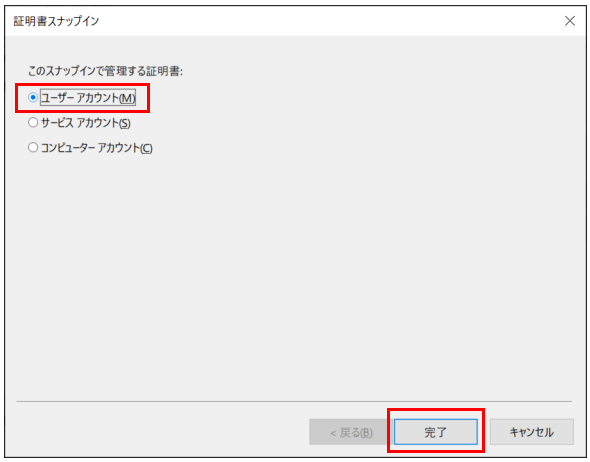
2.「ファイル」→「スナップインの追加と削除」の順にタップします。



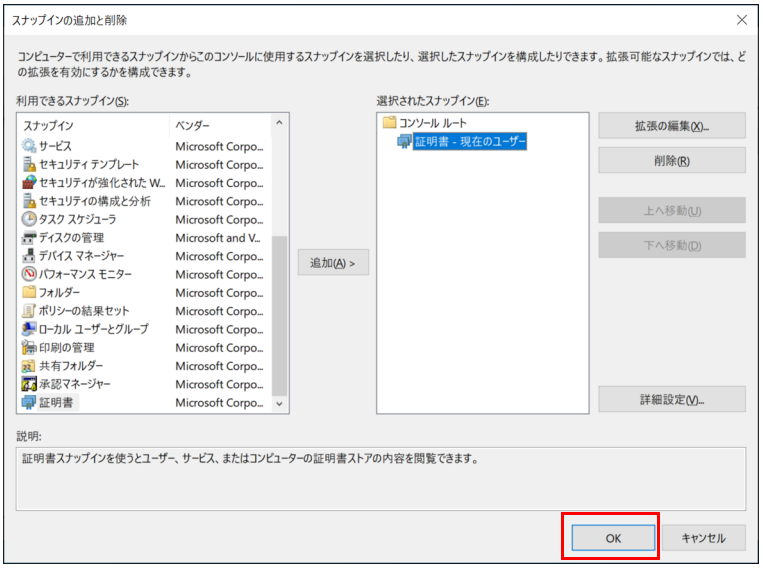
3.「証明書」を選択して「追加」をタップします。



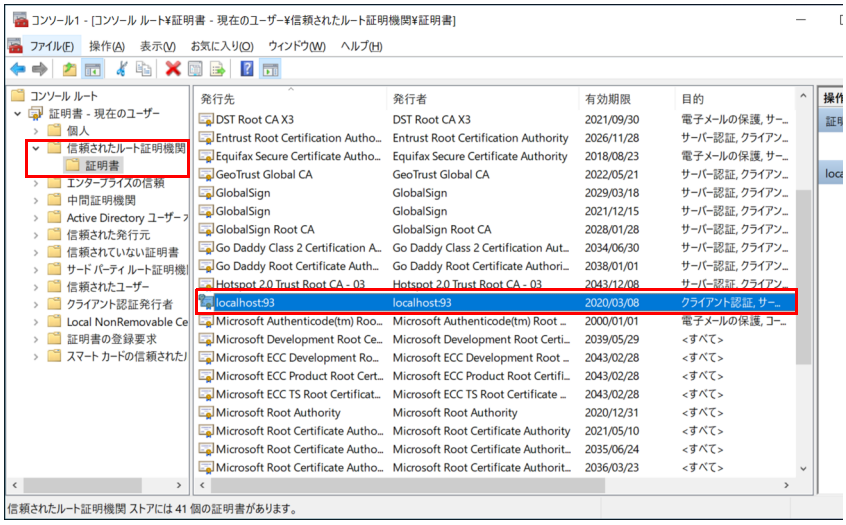
4.「ユーザーアカウント」を選択し「完了」をタップします。



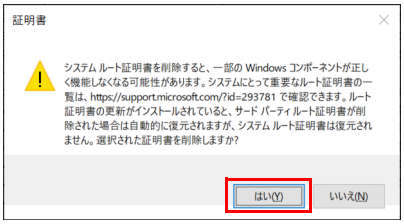
5.「OK」をタップします。



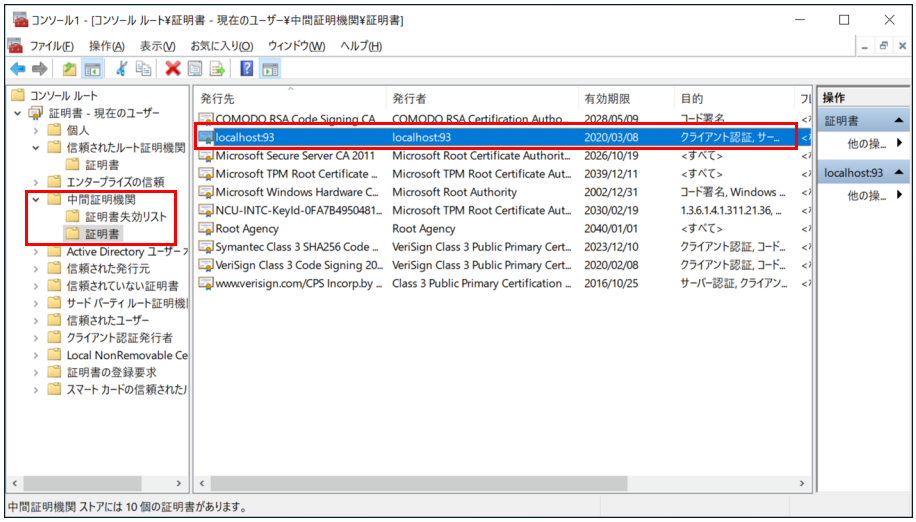
6.「信頼されたルート証明機関」→「証明書」の順にタップし、「localhost:93」を選択、右タップします。表示されたメニューから、「削除」をタップします。



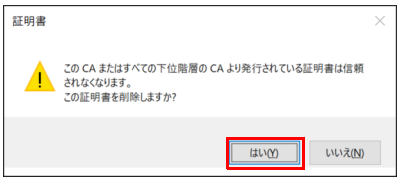
7.「はい」をタップします。



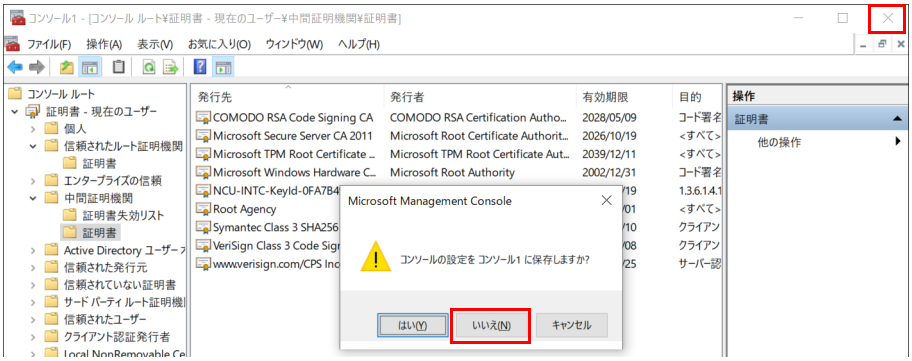
8.「中間証明機関」→「証明書」の順にタップし、「localhost:93」を選択、右タップします。表示されたメニューから、「削除」をタップします。



9.「はい」をタップします。



10.コンソール画面右上の × をタップし、「いいえ」をタップします。



クライアントアプリのインストーラーがダウンロードできない

●プロキシ設定が有効になっている可能性があります。
プロキシ設定を無効にして再度実施してください。
1.プロキシ設定を無効にします（→ P.169）。
2.端末を再起動します。
3.端末認証設定をインストールします（→ P.173）。
4.認証端末を登録します（→ P.174）。
5.プロキシ設定を無効にします（→ P.176）。

●ブラウザーのキャッシュデータを削除してください。
・ Internet Explorer の場合
1.「コントロールパネル」を表示します（→ P.7）。
2.「ネットワークとインターネット」→「インターネット オプション」の順にクリックします。
3.「全般」タブを選択し、「削除」をクリックします。
4.すべての項目にチェックを付けて、「削除」をクリックします。
5.「OK」をクリックします。
・ Microsoft Edge の場合
1.Microsoft Edge を起動し、…（設定など）→「設定」→「プライバシーとサービス」の順にクリックします。
2.「閲覧データのクリア」の「クリアするデータの選択」をクリックします。
3.すべての項目にチェックを付けて、「クリア」をクリックします。
4.「OK」をクリックします。

●アクセスポイント部分の SSID を削除してください。
1.画面右下の通知領域の Wifi マークをタップします。
2.利用する本製品の SSID（この例では、「2nen_3kumi_5G」）を長押しタップして「削除」を選択します。
3.端末認証のクライアントアプリインストール専用の SSID「SWInstall-5G」を長押しタップして「削除」を選択します。

●IP アドレスをリリースしてください。
1.管理者権限でコマンドプロンプトを起動します（→ P.7）。
2. 次のコマンドを入力し、【Enter】キーを押します。
ipconfig /release

端末登録できない

●端末のセキュリティチップが無効になっている可能性があります。
端末認証ではセキュリティチップを使用します。セキュリティチップを有効にする方法は、端末のマニュアルをご覧ください。

エクスポートできない

●管理アプリケーション（制御部）のフォルダーにアクセス権がない可能性があります。
C:¥wifi-mgmg-nodejs¥work のアクセス権限を書き込み可能に設定してください。

端末登録済みだが、接続できない

●有効期限を過ぎていませんか？
有効期限を設定し直してください（→ P.180）。
有効期限を現在以降に設定しても接続できない場合、一度、端末情報を削除してください（→ P.180）。その後、登録し直してください（→ P.174）。

SSID に「SWInstall-5G」または、「SWRegist-5G」が表示される

●認証登録モードが「ON」になっている可能性があります。
端末の登録が完了している場合は、端末認証機能の管理画面で「認証登録モード」を「OFF」にしてください（→ P.180）。

ハードウェアのトラブル

ステータスランプ

ステータスランプが点灯している

●ステータスランプが点灯している場合は、次の手順で本製品を再起動してください。
1.電源ボタンを押します。
しばらくすると、本製品の電源が切れます。
2.電源プラグをコンセントから抜きます。
3.30 秒以上待ってから電源プラグをコンセントに付けます。
4.電源ボタンを押します。

アクセスポイント

端末が無線接続できない

●タブレット端末の無線 LAN 設定で、利用できる SSID の一覧に本製品の SSID が表示されない場合は、アクセスポイント部分から無線電波が出ていない可能性があります。
アクセスポイント部分の無線設定が正しく行われていることを確認してください。

●タブレット端末の無線 LAN 設定で、利用できる SSID の一覧に本製品の SSID が表示されている場合は、次の確認を行ってください。

・ アクセスポイント部分の設定で、MAC アドレスフィルタリングが有効な場合、当該のタブレット端末が接続可能な設定になっていること。
・ アクセスポイント部分の設定で接続端末数を指定した場合、設定した接続端末数より実際に接続している端末の台数がオーバーしていないこと。
・ タブレット端末の認証キーなどのセキュリティ設定がアクセスポイント部分の設定と合っていること。
・ タブレット端末の設定で、自動接続のチェックが付いていること。

AP Management の設定項目が変更できない

●AP Management の設定項目は、通常は変更の必要はありません。
AP Management の設定項目を変更する場合は、次の手順を実施してください。
1.WEB 設定画面にログインします。
2.「詳細設定」→「管理」→「AP Management」の順にクリックします。
3.ログファイルパスを「/tmp/syslog/messages」に変更します。
4.ログファイルパス以外の項目を設定します。
5.「適用」をクリックします。
アクセスポイント部分の RESET で設定を初期化した場合、再度、本手順を実行して設定してください。

WAN

ネットワークに接続できない

●ネットワークケーブルは正しく接続されていますか？

●ネットワークケーブルに関して、次の項目を確認してください。

・ケーブルのコネクタやケーブルは損傷していませんか？
・使用するネットワーク環境に合ったケーブルを使っていますか？

ネットワークの設定については、ネットワーク管理者に確認してください。

通信速度が遅い

●ネットワーク機器の電源を入れてから本製品に電源ケーブルを接続して電源を入れてください。また、本製品の使用中に LAN ケーブルを抜いたり、ネットワーク機器の電源をオフにしたりしないでください。

ネットワーク機器との接続ができなくなったり、通信速度が極端に低下したりする場合があります。
例：1000Mbps で通信していたのに 10Mbps の速度になる
ネットワーク機器との接続ができない場合は、ネットワーク機器の電源が入っていること、および LAN ケーブルで本製品とネットワーク機器が接続されていることを確認後、製品本体を再起動してください。

その他

「ジー」「キーン」という音がする

●静かな場所では、「ジー」「キーン」という製品本体内部の電子回路の動作音が聞こえる場合があります。

故障ではありませんので、そのままお使いください。

エラーメッセージ一覧

ここでは、本製品が表示するメッセージと、その対処方法を説明しています。
エラーメッセージ一覧には、お使いの製品に搭載されているハードウェアによっては、表示されないメッセージも含まれています。
本書に記載されていないエラーメッセージが表示された場合は、「富士通ハードウェア修理相談センター」、またはご購入元にご連絡ください。

起動時に表示されるエラーメッセージ

起動時の自己診断（POST）で異常が見つかった場合に表示されるメッセージは、次のとおりです。

重要

- エラーメッセージが表示された場合は、ご購入元に確認してください。対処を行った後にBIOSセットアップを起動し、「終了」メニューの「変更を保存して終了する（再起動）」または「変更を保存して終了する（電源OFF）」を実行してください。

BIOS セットアップメニューについては、「BIOS」をご覧ください。

キー	役割
B	
Bad RTC Battery 内蔵リチウム電池の電圧低下	内蔵リチウム電池が取り外されました。
BIOS Settings defaults loaded. BIOS設定が標準設定値へ読み込まれました。	すべての BIOS 設定項目が標準設定値に変更されました。BIOS セットアップの各設定を確認し、正しい値に設定し直してください。 起動するたびに本エラーメッセージが表示される場合は、「富士通ハードウェア修理相談センター」、またはご購入元にご連絡ください。
F	
FAN fault: SYS FAN absent: SYS FAN エラー : SYS FAN 未接続 : SYS	SYS ファン動作確認時にファンでエラーが発生しました。 接続されているファンが壊れていないか、ファンの電源ケーブルが正しく接続されているかを確認してください。また、ファンの回転部分にケーブルや異物がはさまっていないか確認してください。 確認後、BIOS セットアップを起動し、「終了」メニューの「変更を保存して終了する（再起動）」または「変更を保存して終了する（電源 OFF）」を実行してください。 それでも本メッセージが表示されるときは、「富士通ハードウェア修理相談センター」、またはご購入元にご連絡ください。
I	
Invalid date / time 日付と時刻の設定を確認してください。	日付／時刻がリセットされました。 BIOS セットアップを起動して、正しい日付／時刻を設定してください。
Invalid Password パスワードが正しくありません	誤ったパスワードが入力されました。
K	
Keyboard/Interface Error. キーボードエラーまたはキーボードが接続されていません。	キーボードテストでエラーが発生しました。電源を切って、キーボードが正しく接続されているか確認し、30 秒以上待ってから電源を入れ直してください。 また、キーボードを接続せずにお使いになる場合は、エラーが表示されないように BIOS セットアップの「起動」メニューの「キーボードエラー検出」を「使用しない」に設定してください。
P	
Press <F2> to enter setup or any other key to continue. <ESC> キーまたは <F2> キーを押すと BIOS セットアップを起動します。その他のキーを押すと継続します。	POST 中にエラーが発生すると OS を起動する前に本メッセージが表示されます。 【F2】キーを押すと BIOS セットアップを起動して設定を変更できます。他のキーを押すと OS の起動を開始します。
PXE-T01:File not found	Preboot Execution Environment 実行時のエラーです。ブートサーバー上のブートイメージファイルが取得できませんでした。ブートサーバーを正しく設定するか、BIOS セットアップの「詳細」メニューの「互換性サポートモジュール設定」→「ネットワークからの起動」を「使用しない」に設定してください。
PXE-E32:TFTP open timeout	Preboot Execution Environment 実行時のエラーです。ネットワークブートに失敗しました。ブートサーバーを正しく設定するか、BIOS セットアップの「詳細」メニューの「互換性サポートモジュール設定」→「ネットワークからの起動」を「使用しない」に設定してください。
PXE-E51: No DHCP or proxyDHCP offers were received	Preboot Execution Environment 実行時のエラーです。ブートサーバーがクライアントから認識されていない場合に発生するエラーです。ブートサーバーを正しく設定するか、BIOS セットアップの「詳細」メニューの「互換性サポートモジュール設定」→「ネットワークからの起動」を「使用しない」に設定してください。
PXE-E53:No boot filename received	Preboot Execution Environment 実行時のエラーです。ブートサーバーがクライアントから認識されていない場合に発生するエラーです。ブートサーバーを正しく設定するか、BIOS セットアップの「詳細」メニューの「互換性サポートモジュール設定」→「ネットワークからの起動」を「使用しない」に設定してください。
PXE-E61:Media test failure, Check cable	Preboot Execution Environment 実行時のエラーです。LAN ケーブルが正しく接続されていません。LAN ケーブルを正しく接続してください。それでも本メッセージが表示されるときは、「富士通ハードウェア修理相談センター」、またはご購入元にご連絡ください。
PXE-E78:Could not locate boot server	Preboot Execution Environment 実行時のエラーです。ブートサーバーがクライアントから認識されていない場合に発生するエラーです。ブートサーバーを正しく設定するか、BIOS セットアップの「詳細」メニューの「互換性サポートモジュール設定」→「ネットワークからの起動」を「使用しない」に設定してください。
PXE-E89:Could not download boot image	Preboot Execution Environment 実行時のエラーです。ブートサーバー上のブートイメージファイルが取得できませんでした。ブートサーバーを正しく設定するか、BIOS セットアップの「詳細」メニューの「互換性サポートモジュール設定」→「ネットワークからの起動」を「使用しない」に設定してください。それでも本メッセージが表示されるときは、「富士通ハードウェア修理相談センター」、またはご購入元にご連絡ください。

キー	役割
S	
System Disabled. システムは使用できません。	誤ったパスワードが 3 回入力されました。

無線 LAN 診断で表示されるエラーメッセージ

無線 LAN 診断で異常が見つかった場合に表示されるメッセージは、次のとおりです。

エラーコード	詳細	状態	対処方法	備考
1	アクセスポイント Login Fail（アクセスポイントログイン失敗）	診断サーバー PC がアクセスポイントにログインできない	・ アクセスポイント状態表示ランプが正常に点灯していることを確認してください（→ P.10）。 ・ コンピューター部分とアクセスポイント部分を接続している 2 本のケーブルが、正しく接続していることを確認してください。特に LAN ケーブルが半抜けになっていないことを確認してください。 ・ 本製品の電源を切って、電源ランプ（→ P.9）が消灯したことを確認した後、コンセントから電源プラグを抜き、30 秒程度待ってから再度、コンセントに接続してください。 ・ アクセスポイント部分の RESET ボタンを 5 秒未満押してリセットを実行してください（→ P.10）。	本製品が自身にログインする行為のため 物理的な問題が想定されます。
3	Node No IP Address（IP なし）	該当端末のIPをアクセスポイントが取得できていない	・ 端末の SSID を切断して再度、接続してください。 ・ 端末の DHCP 設定を確認してください。 ・ 端末を再起動してください。 ・ 端末の無線 IP アドレスを確認してください。 ・ 端末の無線 LAN のパスワードに間違いがないことを確認してください。	アクセスポイントの機能として端末の IP アドレスの更新に 2 分程度かかります。 このため無線切断した状態から接続した最初のタイミングによっては本診断となる可能性があります。
4	Node DHCP Fail（DHCP 失敗）	該当端末に IP アドレスが DHCP サーバーから割り振られていない状態	・ 端末の SSID を切断して再度、接続してください。 ・ 端末の DHCP 設定を確認してください。 ・ 端末を再起動してください。 ・ 端末の無線 IP アドレスを確認してください。 ・ 端末の無線 LAN のパスワードに間違いがないことを確認してください。	ブリッジモードで動作している場合は、DHCP の確認は行いません。 「IP アドレスなし」と診断されます。
7	Node Connection Fail（接続失敗）	該当端末がアクセスポイントとの接続に失敗した状態	・ 端末の SSID を切断して再度、接続してください。 ・ 端末の設定（無線 LAN のパスワード、認証設定）を確認してください。	端末が本製品から離れることでも、発生します。
8	Node RSSI low（RSSI 低下）	該当端末からの RSSI が低下して通信が切断された状態	・ 本製品の近くで、端末の SSID を再度、接続してください。 ・ 周囲に障害物がある場合は、取り除いてください。	端末が本製品から離れることでも、発生します。
9	Node Interference（干渉）	該当端末が干渉によって通信が切断された状態	・ 本製品の電源を切って、電源ランプ（→ P.9）が消灯したことを確認した後、コンセントから電源プラグを抜き、30 秒程度待ってから再度、コンセントに接続してください。 ・ 端末の SSID を切断して再度、接続してください。 ・ すべての端末で切断する症状が出ている場合は、無線チャネルの設定を見直す必要があります。	頻発する場合は、アクセスポイント部分の無線チャネルの設定を自動にする必要があります。 端末が本製品から離れることでも、発生します。
10	Node Authentication or Other Error（認証または他の端末問題）	上記以外の理由で該当端末が切断された状態	・ 端末の SSID を切断して再度、接続してください。 ・ 端末の DHCP 設定を確認してください。 ・ 端末を再起動してください。 ・ 端末の無線 IP アドレスを確認してください。 ・ 端末の無線 LAN のパスワードに間違いがないことを確認してください。	端末が本製品から離れることでも、発生します。
12	アクセスポイント Setting Fail（アクセスポイント設定異常）	アクセスポイントの設定が基準値から変化している	・ アクセスポイント部分の設定変更がなかったか確認してください。 ・ 本製品の電源を切って、電源ランプ（→ P.9）が消灯したことを確認した後、コンセントから電源プラグを抜き、30 秒程度待ってから再度、コンセントに接続してください。	
13	アクセスポイント Fail（アクセスポイント異常）	アクセスポイントがハングアップや認証処理の不具合などで正常に動作していない状態	・ 本製品の電源を切って、電源ランプ（→ P.9）が消灯したことを確認した後、コンセントから電源プラグを抜き、30 秒程度待ってから再度、コンセントに接続してください。 ・ 周辺に遮へいするような障害物がないことを確認してください。	

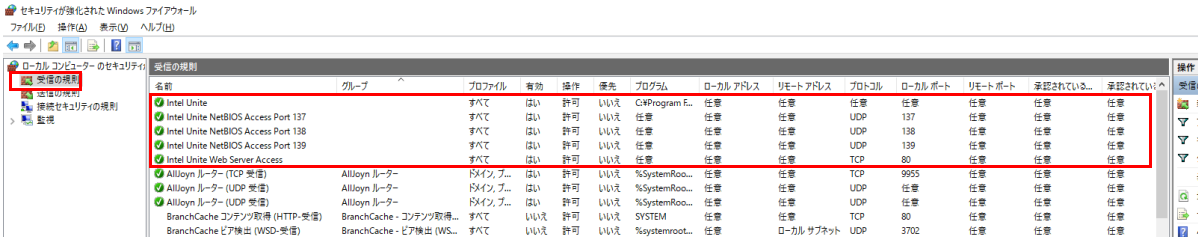
Intel Unite のファイアウォールの設定

本製品のファイアウォールの設定で Intel Unite の通信を許可する必要があります。なお、これらの設定は、ご購入時に設定されています。
なお、市販のセキュリティ対策ソフトをインストールしている場合は、セキュリティ対策ソフトのマニュアルをご覧になり、設定を確認してください。

1 **「コントロールパネル」を表示します（→ P.7）。**
「コントロールパネル」が表示されます。

2 **「システムとセキュリティ」→「Windows ファイアウォール」→「詳細設定」の順にクリックします。**
「セキュリティが強化された Window ファイアウォール」が表示されます。

3 **「受信の規則」をクリックし、下の図のように設定されていることを確認します。**



設定がない場合は、本製品から Intel Unite をアンインストールして、再インストールしてください。

3. それでも解決できないときは

故障かなと思われたときや、技術的なご質問・ご相談などについては、「問い合わせ先」をご覧になり、弊社までお問い合わせください。

ファームウェアと BIOS のアップデート

本製品のアクセスポイント部分やコンピューター部分を修理した後に、アクセスポイントのファームウェアや BIOS などがアップデート前の版数になることがあります。弊社ホームページの「ドライバダウンロード」（http://www.fmworld.net/biz/fmv/index_down.html）から最新版を入手してアップデートしてください。

問い合わせ先

マニュアルをご覧になっても不明な点がございましたらお問い合わせください。
お問い合わせの前に、製品本体のラベルまたは保証書に記載されている、型名（MODEL）、製造番号（SERIAL）、16 桁の数字（0000-0000-0000-0000）または（0000000-00-0000-000）をご確認ください。

こんなときには	こちらへ
故障かなと思われたとき	富士通ハードウェア修理相談センター https://eservice.fujitsu.com/webrepair/ 「修理ご相談チャット」で 24 時間いつでも、故障診断、修理費用のご案内から、修理のお申し込みまでできます。
	お電話でのご相談が必要な場合は、次におかけください。 通話料無料　0120-422-297 受付時間　　9：00 ～ 17：00（土曜、日曜、祝日および年末年始を除く）
技術的なご質問、ご相談	ご購入元（販売会社または富士通の担当営業、SE）にご相談ください。
	個人のお客様など、ご相談先がご不明の場合は、次の窓口へお問い合わせください。 富士通パーソナル製品に関するお問い合わせ窓口 （運営：富士通クライアントコンピューティング株式会社） 通話料無料　0120-950-222 受付時間　　9：00 ～ 17：00（土曜、日曜、祝日およびシステムメンテナンス日を除く） 受け付け後に専門技術員からのコールバックとなります。

・ おかけ間違いのないよう、ご注意ください。
・ 各窓口ともダイヤル後、音声ガイダンスに従い、ボタン操作を行ってください。お客様の相談内容によって、各窓口へご案内いたします。
・ システムメンテナンスのため、受付時間であっても受け付けを休止させていただく場合があります。

8

第 8 章
付録

1. 仕様

ESPRIMO Edge Computing Edition Z0110/E

コンピューター部分

項目			仕様
CPU 注 1	名称		インテル® Core™i5-7500T プロセッサー
	動作周波数		2.70 GHz （最大 3.30 GHz 注 2）
	コア数／スレッド数		4/4
	キャッシュメモリ		3 次：6MB
チップセット			インテル® Q270
システムバス			8GT/s DMI 注 3
メインメモリ			標準 16GB （PC4-2400 DDR4 SDRAM SO-DIMM CL15 ECC なし）
メモリースロット			×2 注 4
表示機能	グラフィックスアクセラレータ		Intel® HD Graphics 630
	ビデオメモリ		メインメモリと共用
	解像度／発色数	DisplayPort	最大 3840×2160 ドット／最大 1677 万色
	DirectX		12.0
	OpenGL		4.4
ストレージ注 5			フラッシュメモリディスク 標準 128GB/ 最大 256GB 注 6
セキュリティ機能			
	セキュリティチップ（TPM）注 7		あり
	盗難防止用ロック取り付け穴		あり
	筐体施錠		あり
インターフェース			
	外部ディスプレイ	DisplayPort	2 ポート
		HDMI	1 ポート注 8
	シリアル注 9		非同期 RS-232C 準拠 D-SUB 9 ピン ×1（16550A 互換）
	USB 注 10		USB3.0 準拠 ×4（前面 ×2、背面 ×2）注 11
	LAN		RJ-45×2（アクセスポイント部との接続で 1 ポート使用、取り外し不可）
自己診断（POST）時			あり注 12
サポート OS			Windows 10 IoT Enterprise 2016 LTSB

本製品の仕様は、改善のために予告なく変更することがあります。あらかじめご了承ください。

注 1 ：・ソフトウェアによっては、CPU 名表記が異なる場合があります。
・本製品に搭載されている CPU で使用できる主な機能については、「CPU」（→ P.252）をご覧ください。

注 2 ：インテル® ターボ・ブースト・テクノロジー 2.0 動作時。

注 3 ：DMI は Direct Media Interface の略です。

注 4 ：空きメモリスロットは 1 つありますが、メモリの増設は保証していません。

注 5 ：容量は、1GB=1000^3 バイト換算値です。

注 6 ：カスタムメイドオプションの選択により、フラッシュメモリディスク 256GB（M.2NVMe）が搭載されます。

注 7 ：チップセット内蔵のセキュリティ機能（Intel® PTT）を使用することができます。

注 8 ：標準添付品のケーブル（DP-HDMI 変換ケーブル）使用時

注 9 ：すべてのシリアル対応周辺機器の動作を保証するものではありません。

注 10：すべての USB 対応周辺機器の動作を保証するものではありません。

注 11：USB3.0 の場合、外部から電源が供給されない USB 対応周辺機器を接続するときの消費電流の最大容量は、1 ポートにつき 900mA です。
詳しくは、USB 対応周辺機器のマニュアルをご覧ください。

注 12：起動時の自己診断（POST）で異常が見つかった場合に表示されるメッセージについては「起動時に表示されるエラーメッセージ」（→ P.245）を参照してください。

アクセスポイント部分

項目	仕様		
WAN	1000BASE-T ／ 100BASE-TX ／ 10BASE-T 準拠[注 1]		
	インターフェース		RJ-45
	転送レート		1000Mbps / 100Mbps / 10Mbps
無線 LAN インターフェース	IEEE 802.11ac 準拠	周波数 / チャンネル	[W52] 5.2GHz（5150 - 5250）: 36 40 44 48ch [注 2] [W53] 5.3GHz（5250 - 5350）: 52 56 60 64ch [注 2] [W56] 5.6GHz（5470 - 5725）: 100 104 108 112 116 120 124 128 132 136 140ch
		変調方式[注 3]	OFDM / サブキャリアの数 [VHT20]:56 [VHT40]:114 [VTH80]:242, MIMO
		転送レート	5.2GHz （W52） 5.3GHz （W53） 5.6GHz （W56） 最大 1733Mbps （VHT80）
	IEEE 802.11n 準拠	周波数 / チャンネル	2.4GHz（2400 - 2484MHz）: 1- 13ch [W52] 5.2GHz（5150 - 5250）: 36 40 44 48ch [注 2] [W53] 5.3GHz（5250 - 5350）: 52 56 60 64ch [注 2] [W56] 5.6GHz（5470 - 5725）: 100 104 108 112 116 120 124 128 132 136 140ch
		変調方式[注 4]	OFDM / サブキャリアの数 [HT20]:56 [HT40]:114, MIMO
		転送レート	2.4GHz 最大 450Mbps（HT40） 5.2GHz （W52） 5.3GHz （W53） 5.6GHz （W56） 最大 600Mbps（HT4）
	IEEE 802.11a 準拠	周波数 / チャンネル	[W52] 5.2GHz （5150 - 5250）: 36 40 44 48ch [注 2] [W53] 5.3GHz （5250 - 5350）: 52 56 60 64ch [注 2] [W56] 5.6GHz （5470 - 5725）: 100 104 108 112 116 120 124 128 132 136 140ch
		変調方式	OFDM / サブキャリアの数 :52
		転送レート	54/48/36/24/28/12/9/6Mbps
無線 LAN インターフェース	IEEE 802.11g 準拠	周波数 / チャンネル	2.4GHz（2400 - 2484MHz）: 1- 13ch
		変調方式	OFDM / サブキャリアの数 :52
		転送レート	54/48/36/24/28/12/9/6Mbps
	IEEE 802.11b 準拠	周波数 / チャンネル	2.4GHz（2400 - 2484MHz）: 1- 13ch
		変調方式	DS-SS
		転送レート	11 / 5.5 / 2 / 1 Mbps
	アンテナ	5GHz : Tx4 x Rx4 2.4GHz : Tx2 x Rx2	
	セキュリティ[注 5]	SSID（ネットワーク名）、MAC アドレスフィルタリング機能 WEP（セキュリティキー（WEP キー）: 128 ビット）[注 6] WPA2-PSK（AES）, WPA/WPA2-PSK（AES）, WPA/WPA2-PSK（AES/TKIP）, エンタープライズ	
無線 LAN 準処規格	ARIB 標準規格（日本）		
	IEEE 標準規格	IEEE 802.11 a/b/g, 802.11n, 802.11d, 802.11e,802.11h, 802.11i	
		IEEE 802.11 ac（Wi-Fi® 準拠）[注 7]	
		IEEE 802.1D, 802.1Q	
		IEEE 802.3 802.3az, 802.3u	
	マルチメディア	Wi-Fi マルチメディア（WMM）	
USB	USB3.0 Type-B（給電用）		
インジケーター	状態表示ランプ		
RESET ボタン	システムリセット		
使用プロトコル	TCP/IP プロトコル		
ネットワーク管理	SNMP V1/V2/V3 トラップ対応 標準 MIB		
その他	無線 QoS,00000JAPAN 対応、44 台同時接続		

注 1 ： ・ 1000Mbps は 1000BASE-T の理論上の最高速度であり、実際の通信速度はお使いの機器やネットワーク環境により変化します。
・ 1000Mbps の通信を行うためには、1000BASE-T に対応したハブが必要となります。また、LAN ケーブルには、1000BASE-T に対応したエンハンスドカテゴリー 5（カテゴリー 5E）以上の LAN ケーブルを使用してください。

注 2 ： 屋内で使用してください。5.2/5.3GHz 帯の屋外での使用は、電波法により禁じられています（法廷により許可された場合を除く）。

注 3 ： IEEE 802.11ac を使用する際の無線 LAN アクセスポイントの設定で、VHT40/80 の機能を有効にする場合には、周囲の電波状況を確認して他の無線局に電波干渉を与えないことを事前に確認してください。万一、他の無線局において電波干渉が発生した場合には、ただちに VHT40/80 の機能を無効にしてください。

注 4 ： IEEE 802.11n を使用する際の無線 LAN アクセスポイントの設定で、HT40 の機能を有効にする場合には、周囲の電波状況を確認して他の無線局に電波干渉を与えないことを事前に確認してください。万一、他の無線局において電波干渉が発生した場合には、ただちに HT40 の機能を無効にしてください。

注 5 ： IEEE 802.11n、IEEE 802.11ac で接続するためには、パスフレーズ（PSK）を AES に設定する必要があります。

注 6 ： WEP による暗号化は上記ビット数で行いますが、ユーザーが設定可能なビット数は固定長 24 ビットを引いた 40 ビット /104 ビットです。

注 7 ： Wi-Fi® 準拠とは、無線 LAN の相互接続性を保証する団体「Wi-Fi Alliance®」の相互接続性テストに合格していることを示します。

エッジコンピューティングデバイス本体

項目			仕様
質量			約 2.4kg
電源／周波数			AC100V±10%、50/60Hz +2% -4%（入力波形は正弦波のみサポート）
消費電力	電源オフ時[注 1]		約 5.7W
	動作時[注 2]（通常時／最大時[注 3]）		約 17W ／約 48W
	最大消費電力		約 75W
定格電流		動作時	最大 1.5A
外形寸法（突起部含まず）		アンテナをたたんだ状態	W190×D185×H 91.5mm
		アンテナを立てた状態	W 190×D185×H 214.9mm
電波障害対策			VCCI クラス B
国際エネルギースタープログラム[注 4]			なし
温湿度条件			温度 10 ～ 35 ℃／湿度 20 ～ 80%RH（動作時） 温度 -10 ～ 60 ℃／湿度 20 ～ 80%RH（非動作時）

本製品の仕様は、改善のために予告なく変更することがあります。あらかじめご了承ください。

注 1 ： 消費電力を 0 にするには、電源ケーブルをコンセントから抜いてください。

注 2 ： ・ご使用になる機器構成により値は変動します。
・標準構成で OS を起動させた状態での本体のみの測定値です。

注 3 ： 測定プログラムは当社独自の高負荷テストプログラムを使用しています。

注 4 ：「国際エネルギースタープログラム」は、長時間電源を入れた状態になりがちなオフィス機器の消費電力を削減するための制度です。

CPU

本製品に搭載されている CPU で使用できる主な機能は、次のとおりです。

お使いの本製品本体に搭載されている CPU の欄をご覧ください。

機能	インテル® Core™ i5-7500T プロセッサー
インテル® ターボ・ブースト・テクノロジー 2.0	○
インテル® バーチャライゼーション・テクノロジー	○
拡張版 Intel SpeedStep® テクノロジー（EIST）	○
エグゼキュート・ディスエーブル・ビット機能	○

インテル® ターボ・ブースト・テクノロジー 2.0

インテル® ターボ・ブースト・テクノロジー 2.0 は、従来のマルチコアの使用状況にあわせて CPU が処理能力を自動的に向上させる機能に加え、高負荷時にパフォーマンスを引き上げるように最適化された機能です。

POINT

▸ OSおよびソフトウェアの動作状況や設置環境などにより処理能力量は変わります。性能向上量は保証できません。

インテル® バーチャライゼーション・テクノロジー

インテル® バーチャライゼーション・テクノロジーは、本機能をサポートする VMM（仮想マシンモニター）をインストールすることによって、仮想マシンの性能と安全性を向上させるための機能です。
この機能はご購入時には有効に設定されています。設定は BIOS セットアップで変更できます。

拡張版 Intel SpeedStep® テクノロジー（EIST）

拡張版 Intel SpeedStep® テクノロジーは、実行中のソフトウェアの CPU 負荷に合わせて、Windows が CPU の動作周波数および動作電圧を自動的に低下させる機能です。

POINT

▸ この機能により本製品の性能が低下することがあります。お使いの環境で性能の低下が気になる場合は、電源プランを「高パフォーマンス」に切り替えてください。

エグゼキュート・ディスエーブル・ビット機能

エグゼキュート・ディスエーブル・ビット機能は、Windows のデータ実行防止（DEP）機能と連動し、悪意のあるプログラムが不正なメモリ領域を使用すること（バッファー・オーバーフロー脆弱性）を防ぎます。
データ実行防止（DEP）機能がウイルスやその他の脅威を検出した場合、「[ソフトウェア名称] は動作を停止しました」という画面が表示されます。「プログラムの終了」をクリックし、表示される対処方法に従ってください。

アプリの動作環境

ここでは、各アプリの動作環境と注意事項を説明します。

アプリの動作環境と注意事項

●添付のアプリは、本製品と本製品にアクセスする端末でご使用いただけます。

●次の富士通製文教向けタブレットで動作検証を実施しています。

ARROWS Tab Q508/SE、Q509/VE、Q5010/CE、Q739/AE

その他の機種をお使いの場合は、お客様にて事前に検証を実施したうえでお使いください。

●動作検証は次の環境で実施しております。

Windows 10 Pro（64 ビット版）、version 1809 以降で実施しております。

●本製品のすべての機能をタブレット端末にインストールする場合、ハードディスクの空き容量は 130MB 以上必要です。

●各アプリの動作環境と注意事項については、次の表をご覧ください。

名称	動作環境と注意事項
管理画面	・対象 OS は Windows 10 です。 ・対象ブラウザは Internet Explorer 11 および Microsoft Edge になります。 ・画面解像度は 1366 x 768 以上でお使いください。
インターネットキャッシュ機能	・推奨ブラウザは Internet Explorer 11、Microsoft Edge（Chromium 版）、Google Chrome です。 ブラウザによってはキャッシュ機能が利用できない場合がありますので、お客様にて事前に検証を実施した上でお使いください。 ・キャッシュによる効果はご使用になる学校内のネットワーク環境により異なります。 ・キャッシュできるプロトコルは http（https は対象外）になります。 ただし、著作権保護されているコンテンツやキャッシュを禁止しているコンテンツはキャッシュできません。 ・インターネットキャッシュ機能で使用するポートについて、ファイアウォール経由の通信を許可する設定を行う必要があります。 ・1 ファイル 500MB 以下のデータをキャッシュすることができます。
サーバファイルキャッシュ機能	・連携する学習支援アプリケーションのサポート対象環境に準じます。お客様にて事前に検証を実施した上でお使いください。 ・キャッシュによる効果はご使用になる学校内のネットワーク環境により異なります。 ・ご使用になるには連携する学習支援アプリケーション側の対応と、それに応じた設定が必要です。 「FUJITSU 文教ソリューション K-12 学習情報活用 知恵たま」は標準で対応しています。
動作状態監視ツール	・監視対象はご使用される機能に応じて、設定変更する必要があります。
お手入れナビ	―
端末情報収集ツール	・本製品と組み合わせてお使いになるタブレット端末のサポート対象は富士通製文教向けタブレットのみとなります。
無線 LAN 診断	―
優先接続設定	・優先接続設定で優先されるのは本製品 1 台につき、端末 1 台のみです。 ・本製品と組み合わせてお使いになるタブレット端末のサポート対象は Windows 10 Pro（64 ビット版）, version 1809 以降の OS を搭載した機種となります。お客様にて事前に検証を実施したうえでお使いください。
無線 LAN 接続台数表	・無線 LAN 診断は、本製品のアクセスポイント部分に接続された端末の台数が表示されます。 ・この機能は本製品以外のアクセスポイントでは使用できません。 ・本製品と組み合わせてお使いになるタブレット端末のサポート対象は富士通製文教向けタブレットのみとなります。
Intel Unite	・解像度を低くした場合に正しく表示されないことがあります。最大解像度でお使いになることをお勧めします。 フル HD（1920×1080）、またはアスペクト比が 16 対 9 の画面表示機器を接続することを推奨します。 ・Intel Unite のサポート対象端末は以下の OS を搭載した端末となります。 - Windows 10 Pro, version 1809 - Windows 10 Pro, version 1903 - Windows 10 Pro, version 1909 - Windows 8.1 - Mac OS 10.13.5 - OS 11.2.6 ※上記OSを搭載した機種全ての動作を保証するものではありません。お客様にて事前に検証を実施した上でお使いください。 ※ 上記以外のバージョンの対応状況については別途お問い合わせください。
端末認証	・タブレット端末のサポート対象は、Windows 10 Pro（64 ビット版）を搭載し、セキュリティチップ（Intel® PTT）をサポートしている端末環境となります。

使用するポート

アプリ名称	ポート番号
管理画面	10080
インターネットキャッシュ機能	8080、3130、443、8000
サーバファイルキャッシュ機能	8002、8003
メンテナンス機能	9200、9300、18080、18081、18090、18091、18092、18093、18094、9600
端末認証	1812、1813、9000、8001、8010
Intel Unite	80

2. アプリのアンインストール

ここでは、一部のアプリについてアンインストールする方法を記載しています。

重要

- アプリのアンインストールは、推奨していません。トラブルが発生した場合は、作成したバックアップを復元してください。
- 次のアプリは、アンインストールしないでください。
  - 基本アプリ
    - cygwin
    - Open Java Development Kit
  - メンテナンス機能
    - 管理画面
    - 端末情報収集ツール
    - 動作状態監視ツール
    - 無線 LAN 接続台数表示
  - インターネットキャッシュ機能
  - サーバファイルキャッシュ機能
  - 端末認証機能
  - 優先接続設定
  - 無線 LAN 診断
  - Intel Unite

お手入れナビのアンインストール

お手入れナビのアンインストールは、管理者権限のアカウントで行ってください。

1. **「コントロールパネル」を表示します（→ P.7）。**
   「コントロールパネル」が表示されます。
2. **「プログラム」の「プログラムのアンインストール」をクリックします。**
   「プログラムのアンインストールまたは変更」が表示されます。
3. **「プログラムのアンインストール」をクリックしします。**
4. **「お手入れナビ」を選択し、「アンインストール」をクリックします。**
   以降は表示された画面に従って操作してください。
   以上でアンインストールは終了です。

3. VESA マウントの取り付け／取り外し

ここでは、カスタムメイドオプションの VESA マウントを取り外してご使用になる場合に、VESA マウントを取り外す手順を記載しています。

VESA マウントの取り外し

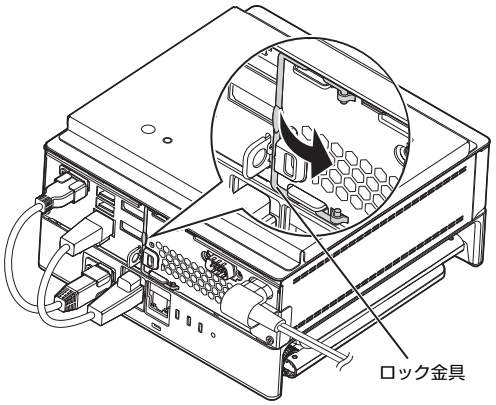
1 本製品の電源を切り、アンテナをたたみます。また、電源プラグをコンセントから取り外した後、専用ケーブルを除く本製品に接続しているすべてのケーブルを取り外します。

2 壁掛け金具と本体を固定している固定バンドをほどいて取り外します。

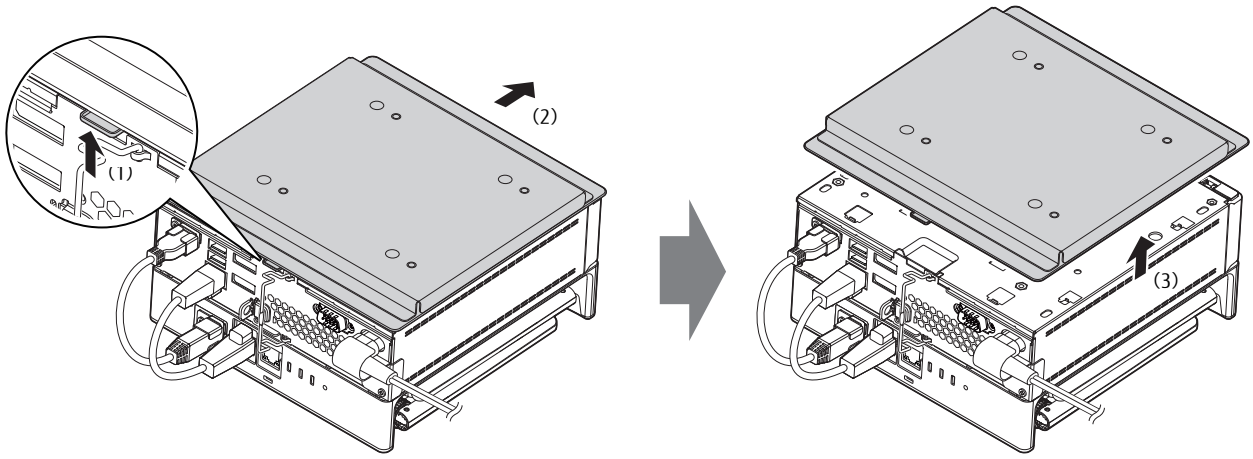
3 壁掛け金具から本製品を取り外します。取り外し方法については、壁掛け金具のマニュアルをご覧ください。

4 VESA マウントが上側になるように、本製品を置きます。

5 本製品背面のロック金具を矢印の向きに動かし、ロックを外します。



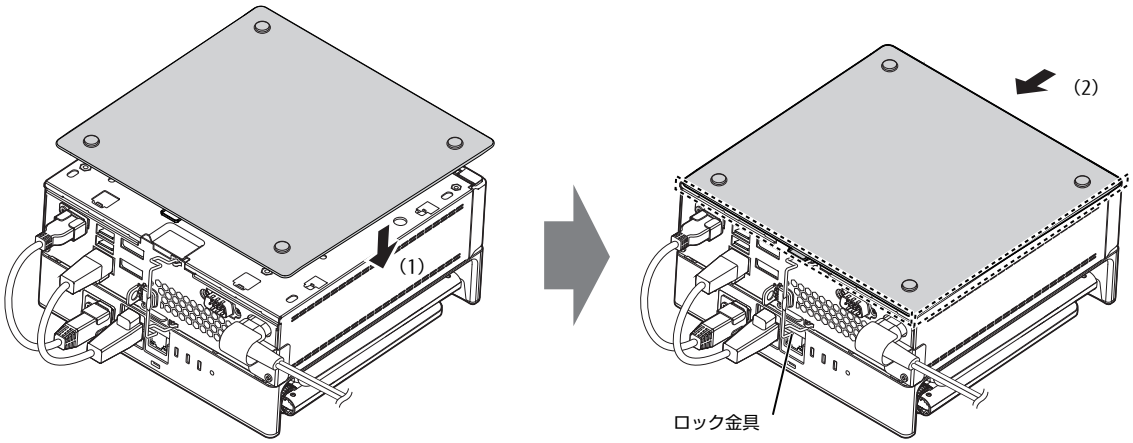
6 （1）本製品背面のツメを上に押し上げながら、（2）VESA マウントを本製品の前面側に（5mm 程度）スライドさせ、（3）そのまま VESA マウントを上に持ち上げます。



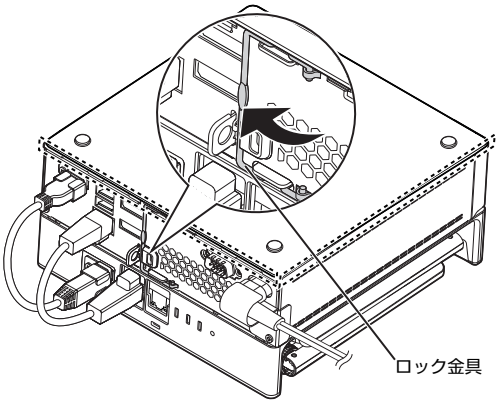
VESA マウントを取り外した後、底面カバーを取り付けてください（→ P.256）。

底面カバーの取り付け

1 （1）本体のツメ穴に底面カバーのツメがはまるようにまっすぐに下ろし、（2）本体背面側にスライドさせた後、本体と底面カバーの間にすき間がないことを確認します。
底面カバーのツメが本体に引っかかっていない場合にすき間ができます。この場合は、底面カバーを取り外してこの手順をやり直してください。



2 本体背面のロック金具を矢印の向きに動かしてロックします。



VESA マウントの取り付け

ここでは、VESA マウントを取り外した後、再度、取り付けて使用する場合の注意事項と取り付け方法を説明しています。

注意事項

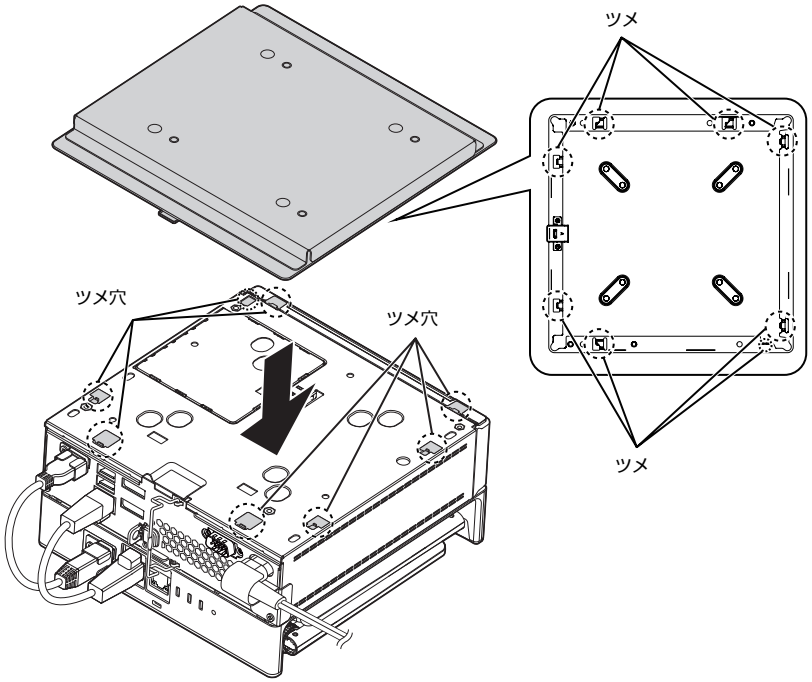
■ 壁掛けの設置は専門の取付工事業者にご依頼すると共に落下防止措置を講じてください。

壁掛け設置には特別な技術が必要です。必ず専門の取付工事業者へご依頼ください。
本製品の設置に不備があると落下事故などの原因となります。
カスタムメイドオプションで VESA マウントを選択した場合は、本製品に固定バンド（2 本）を添付されています。
製品本体のセキュリティ施錠金具に固定バンドを通し、壁掛け金具などしっかりと固定された箇所に結び付けて落下防止措置を必ず講じてください。

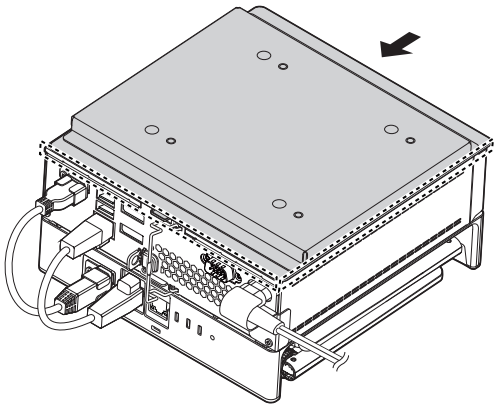
VESA マウント取り付け

1 底面カバーを取り外します。
「VESA マウントの取り外し」（→ P.255）で「VESA マウント」を「底面カバー」に読み替えて底面カバーを取り外してください。

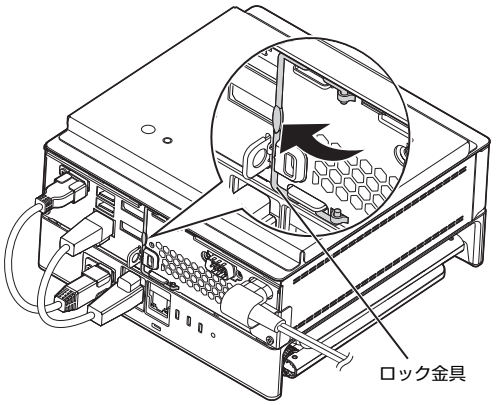
2 本体のツメ穴に VESA マウント内側のツメがはまるようにまっすぐに下ろします。



3 VESA マウントを本体背面側にスライドさせた後、本体と VESA マウントの間にすき間がないことを確認します。
VESA マウントのツメが本体に引っかかっていない場合にすき間ができます。この場合は、VESA マウントを取り外して手順 2 からやり直してください。



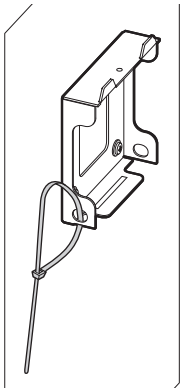
4 本体背面のロック金具を矢印の向きに動かしてロックします。



壁掛け金具への取り付け

壁掛け金具の取り付けおよび設置については、壁掛け金具のマニュアルをご覧ください。

1 壁側の壁掛け金具の穴などに固定バンドを通して輪の状態にします。
固定バンドが外れない場所に固定バンドを通してください。

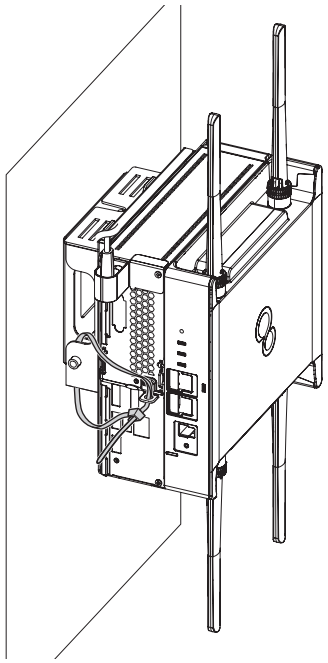


2 壁側の壁掛け金具に本製品を取り付けます。
壁掛け金具を取り付けおよび設置については、壁掛け金具のマニュアルをご覧ください。

3 固定バンドをほどき、製品本体のセキュリティ施錠金具に固定バンドを通して留めます。固定バンドがほどけないことを確認した後、アンテナを広げます。

POINT

- カスタムメイドオプションでVESAマウントを選択した場合、固定バンドが2本添付されています。固定バンドの長さが足りない場合は、壁側の壁掛け金具に通したの固定バンドを輪の状態に戻した後、2本目の固定バンドを製品本体のセキュリティ施錠金具と輪の状態にした1本目の固定バンドに通して固定してください。
- 本製品背面の各コネクタが使用できるように、固定バンドを取り付けてください。



4. 製品本体の廃棄時の注意

ここでは、製品を廃棄するときにデータが流出するのを防ぐための対策について説明しています。

製品廃棄時のフラッシュメモリディスク上のデータ消去に関する注意

製品は、オフィスや家庭などで、いろいろな用途に使われるようになってきています。これらの製品の中のフラッシュメモリディスクという記憶装置に、お客様の重要なデータが記録されています。
従って、その製品を譲渡あるいは廃棄するときには、これらの重要なデータを消去するということが必要です。
ところが、このフラッシュメモリディスク内に書き込まれたデータを消去するというのは、それほど簡単ではありません。
「データを消去する」という場合、一般に
① データを「ごみ箱」に捨てる
②「削除」操作を行う
③「ごみ箱を空にする」コマンドを使って消す
④ ソフトで初期化（フォーマット）する
⑤ ご購入時に近い状態に回復する
などの作業を行うと思います。
まず、「ごみ箱」にデータを捨てても、OS のもとでファイルを復元することができてしまいます。さらに②～⑤の操作をしても、フラッシュメモリディスク内に記録されたデータのファイル管理情報が変更されるだけで、実際はデータが見えなくなっているだけの場合があります。
つまり、一見消去されたように見えますが、Windows などの OS のもとで、それらのデータを呼び出す処理ができなくなっただけで、本来のデータは残っているという状態にあるのです。
従って、特殊なデータ回復のためのソフトウェアを利用すれば、これらのデータを読み取ることが可能な場合があります。このため、悪意のある人により、この製品のフラッシュメモリディスク内の重要なデータが読み取られ、予期しない用途に利用されるおそれがあります。
製品ユーザーが、廃棄を行う際に、フラッシュメモリディスク上の重要なデータが流出するというトラブルを回避するためには、フラッシュメモリディスクに記録された全データを、ユーザーの責任において消去することが非常に重要です。消去するためには、専用ソフトウェアあるいはサービス（共に有償）を利用するか、フラッシュメモリディスク上のデータを物理的・磁気的に破壊して、読めなくすることを推奨します。

専用ソフトウェアによるデータ消去

本製品には、専用ソフトウェア「ハードディスクデータ消去」が添付されています。「ハードディスクデータ消去」は、Windows などの OS によるファイル削除やフォーマットと違い、フラッシュメモリディスクの全領域に固定パターンを上書きするため、データが復元されにくくなります。
ただし、特殊な設備や特殊なソフトウェアの使用によりデータを復元される可能性はあります。あらかじめご了承ください。

注意事項

- ●製品本体に USB メモリ、メモリーカード、外付けハードディスクなど周辺機器を接続している場合は、「ハードディスクデータ消去」を実行する前に必ず取り外してください。
- ●データ消去を実行すると、ディスク内のデータを使用してご購入時に近い状態に回復することはできなくなります。必要があれば「ハードディスクデータ消去」の前に回復ドライブを作成したりシステムイメージバックアップをとったりしてください。作成方法は『管理ガイド』の「バックアップと復元」をご覧ください。
- ●必要なデータはバックアップしてください。
- ●データ消去中に電源を切らないでください。フラッシュメモリディスクが故障する可能性があります。

データ消去方法

1 【F12】キーを押したまま、本製品の電源を入れます。

2 起動メニューが表示されたら、【F12】キーを離します。

POINT

- BIOSセットアップの「起動」メニューの「起動メニュー」が「使用しない」の場合は、起動メニューを使用できません。その場合は、「使用する」に設定し直してください。
  BIOSセットアップについては、「BIOSセットアップ」（→P.208）をご覧ください。
- 起動時のパスワードを設定している場合は、パスワードを入力し、すぐに【F12】キーを押してください。
- 起動メニューが表示されずWindowsが起動してしまった場合は、本製品の電源を切ってからもう一度操作してください。電源の切り方は、「電源を切る」（→P.35）をご覧ください。

3 カーソルキーで「診断プログラム」を選択し、【Enter】キーを押します。
「診断プログラムを実行しますか？」と表示されます。

4 【Y】キーを押します。
ハードウェア診断が始まります。
ハードウェア診断が終了したら、診断結果が表示されます。診断結果が表示される前に、自動的に製品が再起動する場合があります。

5 次の操作を行います。

■ トラブルが検出されなかった場合
【Enter】キーを押してください。続けて「富士通ハードウェア診断ツール」が起動します。
「富士通ハードウェア診断ツール」ウィンドウと「注意事項」ウィンドウが表示されます。手順 6 へ進んでください。

■ トラブルが検出された場合
手順 6 以降の「富士通ハードウェア診断ツール」での診断は不要です。画面に表示された内容を控え、お問い合わせのときにお伝えください。その後、【Y】キーを押して製品の電源を切ってください。
電源が自動で切れない場合は、電源ボタンを押して電源を切ってください。

6 「注意事項」ウィンドウの内容を確認し、「OK」をクリックします。

7 「ツール」タブをクリックます。

8 「データ消去」にチェックを付け「実行」をクリックします。
表示された画面に従って操作してください。
データの消去には数時間かかります。完了すると「消去が完了しました。」と表示されます。

重要

- データを消去する方式は、必ず「SSD対応（フラッシュメモリディスク用）」を選択してください。それ以外の方式を選択すると、完全にデータを消去することができませんのでご注意ください。

9 「終了」をクリックします。
製品本体の電源が切れます。

重要

- 電源が自動で切れない場合は、電源ボタンを4秒以上押して、電源を切ってください。

5. 廃棄／リサイクル

本製品の廃棄について

●フラッシュメモリディスクのデータを消去していますか？
製品本体に搭載されているフラッシュメモリディスクには、お客様の重要なデータ（作成したファイルや送受信したメールなど）が記録されています。製品を廃棄するときは、フラッシュメモリディスク内のデータを完全に消去することをお勧めします。
フラッシュメモリディスク内のデータ消去については、「製品本体の廃棄時の注意」（→ P.259）をご覧ください。

●本製品（付属品を含む）を廃棄する場合は、「廃棄物の処理及び清掃に関する法律」の規制を受けます。
本製品の廃棄については、弊社ホームページ「ICT 製品の処分・リサイクル方法」（http://www.fujitsu.com/jp/about/environment/society/recycleinfo/）をご覧ください。

ESPRIMO Edge Computing Edition Z0110/E
導入ガイド
B6FY-4911-01 Z0-02
発 行 日　　2020 年 4 月
発行責任　　富士通株式会社
〒 105-7123 東京都港区東新橋 1-5-2 汐留シティセンター