Fujitsu Desktop ESPRIMO

B6FK-5781-01 Z0

導入ガイド

ESPRIMO Edge Computing Edition Z0111/W

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

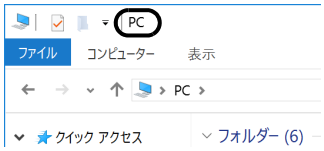
本書中のキーの表記は、キーボードに書かれているマークを記述するのではなく、説明に必要な文字を使い、次のように記述しています。
　例：【Ctrl】キー、【Enter】キー、【→】キーなど
また、複数のキーを同時に押す場合には、次のように「＋」でつないで表記しています。
　例：【Ctrl】＋【F3】キー、【Shift】＋【↑】キーなど

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。本文中のアプリの画面例は、Windows 10 の場合の設定例です。Windows 8.1 の場合と異なることがあります。また、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

本書で使用する用語を次に説明します。

用語	意味
管理者端末	運用管理ツールを操作するための端末
マスター端末	Windows Update を最初に適用する端末

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 Z0111/W	Z0111/W	エッジコンピューティングデバイス	本製品
Windows 10 IoT Enterprise 2019 LTSC	Windows 10 IoT Enterprise	Windows 10	Windows
Open Java Development Kit	OpenJDK		

Windows の操作

クイック設定（Windows 11）／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 または をクリックします。
画面右側に「クイック設定」または「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。

■ Windows 10 の場合

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。

■ Windows 11 の場合

1「スタート」ボタン→画面右上の「すべてのアプリ」→「Windows ツール」の順にクリックし、「コントロールパネル」をダブルクリックします。

「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。

■ Windows 10 の場合

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。

■ Windows 11 の場合

1「スタート」ボタン→画面右上の「すべてのアプリ」→「Windows 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 または をクリックします。

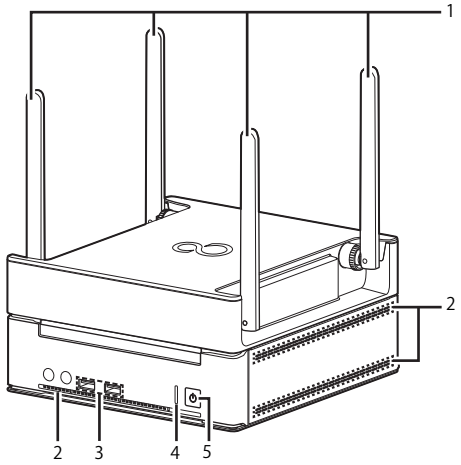
商標および著作権

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。

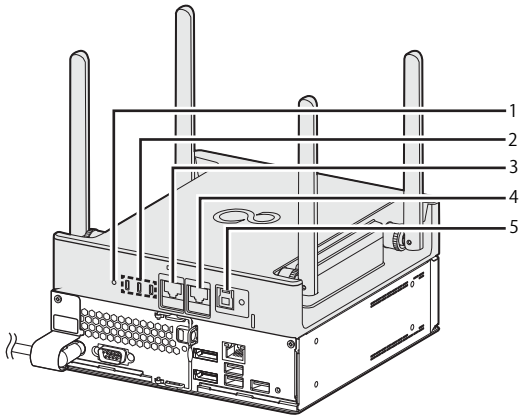
モード	本製品の状態	ステータスランプ
ステータス表示	状態監視機能が異常を検出したとき	点灯
	正常動作時	消灯

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。

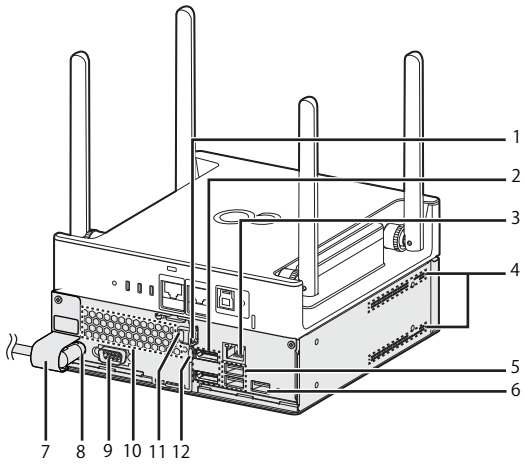
	左 LED（Link/Act）	右 LED（Speed）
1000Mbps で Link を確立	緑色点灯[注]	オレンジ色点灯
100Mbps で Link を確立	緑色点灯[注]	緑色点灯
10Mbps で Link を確立	緑色点灯[注]	消灯

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

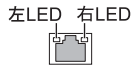


（イラストは、電源ケーブル以外のすべてのケーブルを省略した状態です。）

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
ディスプレイの DisplayPort 信号ケーブルを接続します。
HDMI 形式のディスプレイを接続する場合は、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

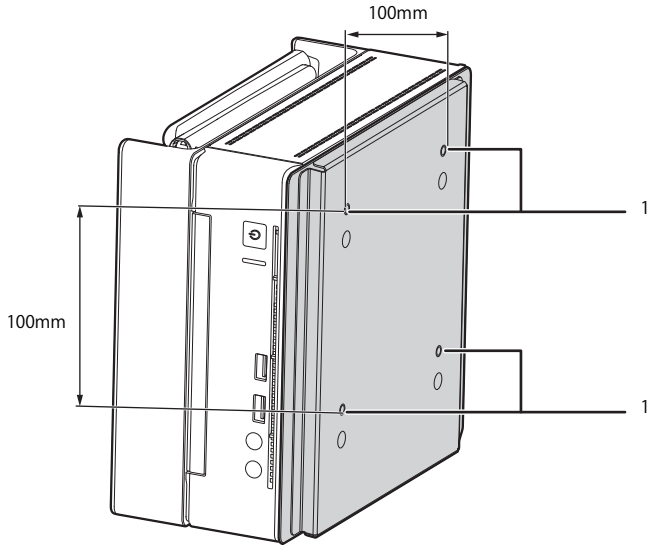
10 排気孔
製品内部の熱を外部に逃がします。

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

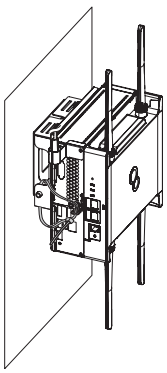
- VESA マウントを取り外して使用する場合は、添付の底面カバーを取り付けてください。詳しくは、「VESA マウントの取り付け／取り外し」（→P.148）をご覧ください。

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.151）をご覧ください。
- 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。

●Windows の更新プログラムをキャッシュするアプリ

●エッジコンピューティングデバイス・マスター端末を管理 / メンテナンスする管理者を支援するアプリ

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.15
メンテナンス（本製品自身）		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.17
		お手入れナビ / RAS Utility	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.17
データキャッシュ		インターネットキャッシュ機能	WSUS サーバーの Windows Update ファイルをキャッシュする機能	→ P.16
		アップデート情報取得モジュール	管理画面のキャッシュ一覧上で WindowsUpdate の更新プログラムのタイトル欄に表示する KB（Microsoft Knowledge Base）番号を取得する機能	→ P.16
管理ツール		運用管理ツール	本製品の運用管理（稼働の監視、保守作業）する機能	→ P.17
			Windows Update のキャッシュを自動で作成する機能	
通知		動作状態監視ツール（メール通知設定）	動作状態監視ツールの診断結果を送信指定したメールアドレスに自動送信する機能	→ P.17
		運用管理ツール（メール通知設定）	運用管理ツールが、システム異常時にアラートを検知した場合にアラートメールを 送信したり、スケジュール機能でスケジュールが完了した場合に結果メールを送信したりする機能	→ P.17

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

●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。

2. 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。

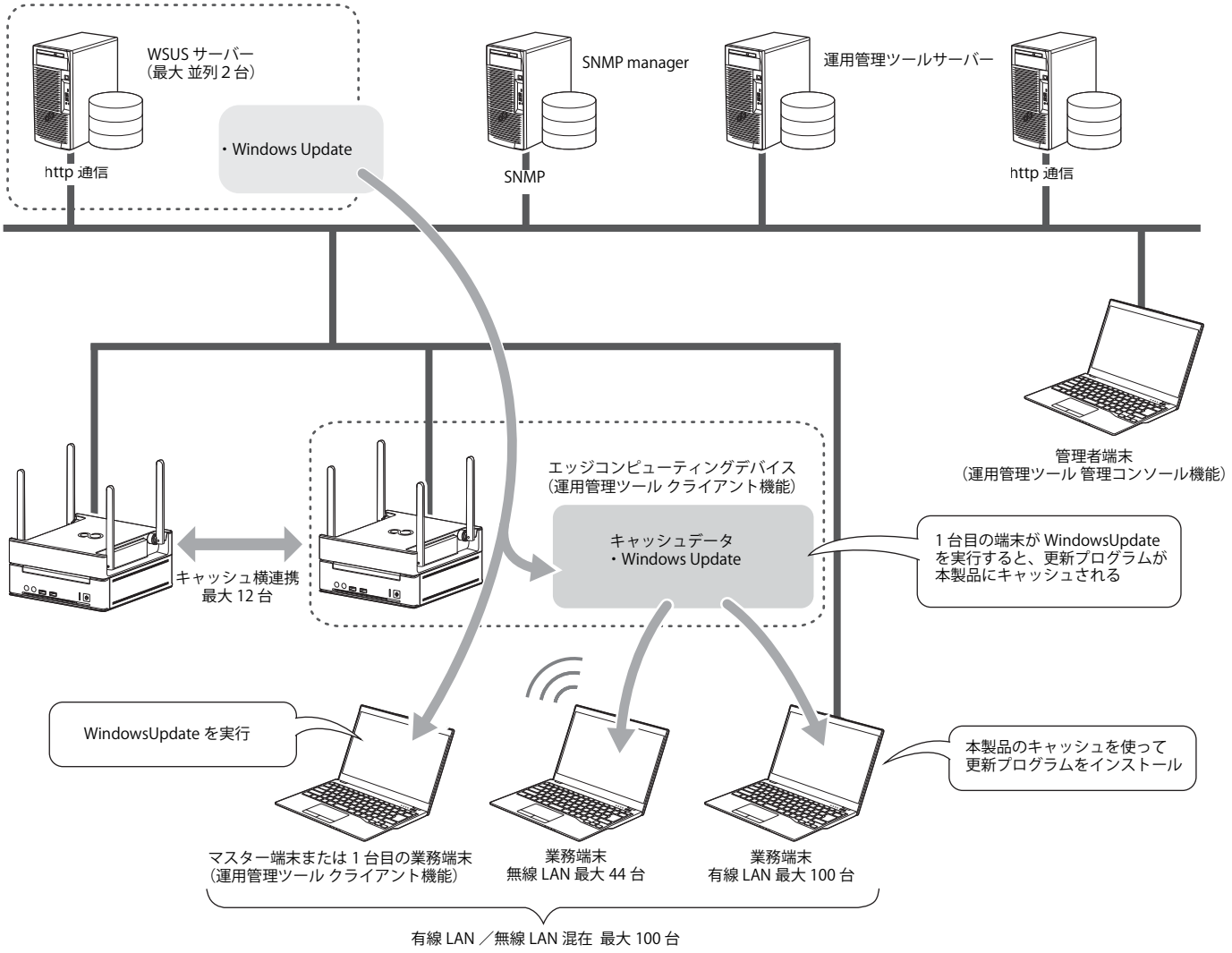
管理画面の項目			説明
インターネットキャッシュ管理	キャッシュデータ	キャッシュデーター一覧	本製品のキャッシュに保存されているファイルの一覧を閲覧とキャッシュ済みデータを削除できます。
		キャッシュデータ事前登録	Windows の更新プログラムをあらかじめキャッシュすることができます。
	キャッシュエンジン	キャッシュエンジン制御	キャッシュエンジンの起動、停止、再起動を行うことができます。
		使用状況	キャッシュの使用状況（ヒット率や使用率など）を確認できます。
		ログ取得	インターネットキャッシュ管理機能のログファイルをダウンロードできます。
	キャッシュ設定		キャッシュに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。
	設定項目の追加		キャッシュエンジンの機能変更時に利用します。通常はご使用にならないでください。
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

■ WSUS サーバーから Windows Update 情報を取得する機能

WindowsUpdate の更新プログラムを効率的に適用する機能です。
1 台目の端末が WSUS サーバーからダウンロードした更新プログラムを本製品にキャッシュすることで、2 台目以降は本製品のキャッシュからの配布が可能となります。キャッシュ作成後は、ネットワーク回線の速度に影響を受けることなく、端末の更新プログラムをインストールできます。なお、本製品にキャッシュされた更新プログラムの状況は、管理者端末で管理画面を表示して確認できます。
詳しくは、「管理ガイド」-「Windows Update 実行の運用イメージ」をご覧ください。



■ アップデート情報取得モジュール

機能更新プログラム（Feature Updates）や品質更新プログラム（Quality Updates）など、WindowsUpdate のキャッシュの状況を KB（Microsoft Knowledge Base）番号で表示できるようになります。

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、メンテナンス機能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。

●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 / RAS Utility

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。

基本機能 - 運用管理ツール

本製品を運用管理（稼働の監視、保守作業）することや、Windows Update のキャッシュを作成することができます。
詳しくは、『Windows Update 運用最適化モデル 運用管理ツール ユーザーガイド』をご覧ください。

●運用管理ツール サーバ機能
端末を管理するアプリです。管理者が運用管理ツール 管理コンソール機能で登録したスケジュールに沿って、各端末に処理を開始するよう指示を出します。

●運用管理ツール 管理コンソール機能
運用管理ツールを操作するためのアプリです。管理者が端末（マスター端末、エッジコンピューティングデバイス）の機器管理、グループ管理、ユーザー管理等のシステム管理操作を行います。

●運用管理ツール クライアント機能
端末用のエージェントアプリです。運用管理サーバーから指示を受けると処理を開始し、処理結果をサーバーに通知します。

基本機能 - 通知

動作状態監視ツール（メール通知設定）

動作状態管理ツールによりプロセスを自動復旧しても問題が解決しない場合に、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。

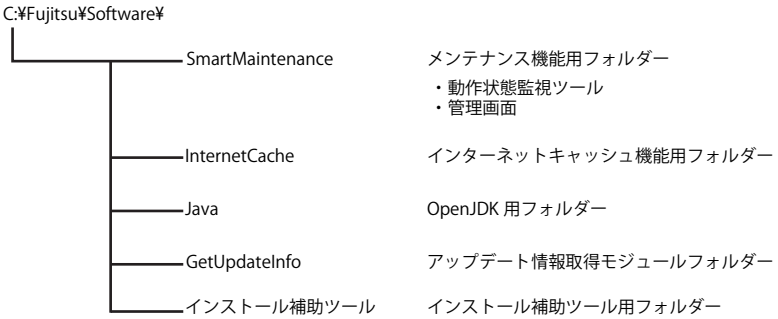
運用管理ツール（メール通知設定）

運用管理ツールがシステム異常等のアラートを検知した場合に、システム管理者に対してアラートメールを送信したり、スケジュール機能で作成したスケジュールが完了した場合に結果メールを送信したりできます。
詳しくは、『Windows Update 運用最適化モデル 運用管理ツール ユーザーガイド』をご覧ください。

3. 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。



このほか、「Windows Update 運用最適化モデル 運用管理ツール ソフトウェアディスク」が添付されます。
セットアップについては、『Windows Update 運用最適化モデル 運用管理ツール セットアップガイド』をご覧ください。

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。

4. アプリアップデートパック

本製品添付のアプリ以外にアプリアップデートパックをダウンロードしてインストールする必要があります。

POINT

- 本製品添付のアプリのインストールが完了している場合は、『アプリアップデートガイド』をご覧ください。

アプリアップデートパック V1.0.2

「アプリアップデートパック V1.0.2」には、インターネットキャッシュ機能やアップデート情報取得モジュールの更新プログラムが含まれます。
「アプリアップデートパック V1.0.2」は、「アプリアップデートパック V1.0.4」に含まれるため、インストールする必要はありません。

アプリアップデートパック V1.0.3

「アプリアップデートパック V1.0.3」には、インターネットキャッシュ機能、アップデート情報取得モジュール、メンテナンス機能を修正する更新プログラムが含まれます。
「アプリアップデートパック V1.0.3」は、「アプリアップデートパック V1.0.4」に含まれるため、インストールする必要はありません。

アプリアップデートパック V1.0.4

「アプリアップデートパック V1.0.4」には、インターネットキャッシュ機能を修正する更新プログラムのほか、「アプリアップデートパック V1.0.2」、「アプリアップデートパック V1.0.3」が含まれます。
インストール補助ツールを実行した後、「アプリアップデートパック V1.0.4」をインストールしてください。

アプリアップデートパックのダウンロード

アプリアップデートパックは、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」（https://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、アプリアップデートパック内の Readme.txt をご覧ください。

5. インストール補助ツール

本製品のセットアップは、インストール補助ツール（バッチファイル）を使用してください。

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。

次の表は、セットアップで使用するインストール補助ツールの一覧です。

アプリ名称	対応バッチファイル名	参照先
基本機能		
基本アプリ	01_BasicFunction_BaseAPP_Install.cmd 02_BasicFunction_BaseAPP_Install.cmd	「インストール補助ツールの実行（初期設定）」（→ P.56）
インターネットキャッシュ	BasicFunction_InternetCache_Install.cmd	「インストール補助ツールの実行（インターネットキャッシュ機能）」（→ P.74）
アップデート情報取得モジュール	BasicFunction_UpdateCache_Install.cmd	「インストール補助ツールの実行（アップデート情報取得モジュール）」（→ P.89）
動作状態監視ツール	BasicFunction_WatchProcessApp_Install.cmd	「インストール補助ツールの実行（動作状態監視ツール）」（→ P.95）

6. ポート番号変更ツール

本製品ご購入時、ブラウザーで管理画面を表示するときにポート番号「10080」を使用するように設定していますが、最新のブラウザーでは、ポート番号「10080」がブロックされるようになり管理画面が表示できなくなりました。この問題を解決するために、「ポート番号変更ツール」を提供いたします。次の弊社サイトからポート番号変更ツールをダウンロードして、エッジコンピューティングデバイスで実行してください。

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

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

『管理ガイド』の「第 2 章 Windows Update 実行の運用イメージ」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。
・すでに WSUS サーバーを導入されている環境に対して本製品をセットアップすることを想定しています。

2. 基本機能の設定

基本機能の設定を実施します。
本製品とマスター端末、業務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.23）
・マスター端末、業務端末の設定（基本のアプリのインストールと設定）
　「基本機能 - 初期設定（業務端末／マスター端末）」（→ P.58）

運用管理ツールの設定を実施します。
・インストール
　『Windows Update 運用最適化モデル 運用管理ツール セットアップガイド』
・設定、操作
　『Windows Update 運用最適化モデル 運用管理ツール ユーザーガイド』

3. 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.102）をご覧になり、必要なアプリのセットアップが完了していることを確認します。

4. 設定の確認

「設定項目確認一覧表」（→ P.152）をご覧になり、運用に当たって必要な設定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、本製品のシステムイメージ、アクセスポイントの設定、管理画面の設定、の設定のバックアップを作成します（→ P.104）。

6. 運用開始

運用に当たっては、次のマニュアルを参照ください。

●管理ガイド
　・ インターネットキャッシュ機能での、キャッシュの確認・管理などの操作方法

●Windows Update 運用最適化モデル 運用管理ツール ユーザーガイド
　・ WindowsUpdate 連携（機能更新プログラム / 品質更新プログラム）のスケジューラ機能の操作
　・ WindowsUpdate 連携の実行結果確認
　・ 本製品、マスター端末の稼働状況確認

●Windows Update 運用最適化モデル 運用管理ツール リモート操作ガイド
　・ 本製品、マスター端末の遠隔操作（更新プログラムの適用確認の際に利用）

※ ここでの設定項目は、Windows Update 実行の運用で必要な主項目を上げています。

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、ディスプレイ、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）

アプリアップデートパックとポート番号変更ツールのダウンロード

「アプリアップデートパック V1.0.4」と「ポート番号変更ツール」は、本製品には含まれていません。本製品をセットアップする前に、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」（https://www.fmworld.net/biz/fmv/index_down.html）

本製品を設置する

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

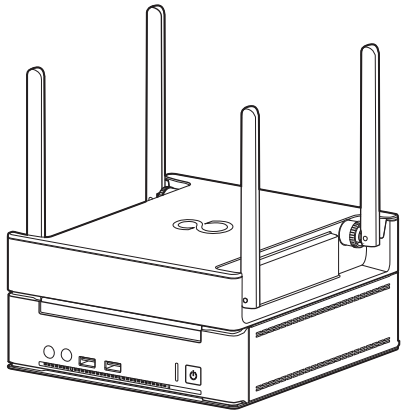
●次の温湿度条件の範囲を超える場所
・ 動作時：温度 10 ～ 35 ℃／湿度 20 ～ 80%RH
・ 非動作時：温度 -10 ～ 60 ℃／湿度 20 ～ 80%RH
ただし、動作時、非動作時とも結露していないこと。

●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

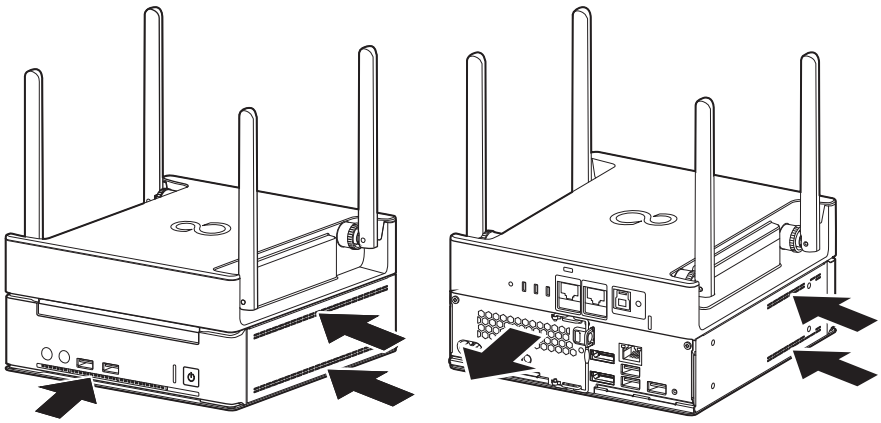
本製品は、アクセスポイント部分が上になるように設置してください。また、本製品の上には、物を置かないでください。

■ 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。）

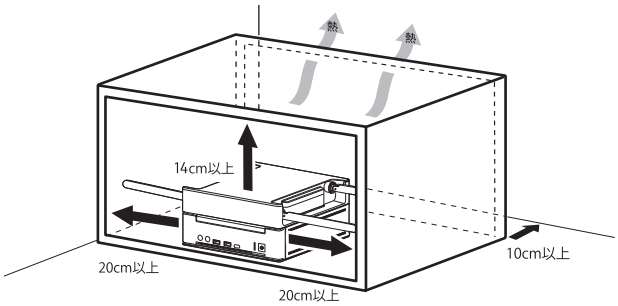
設置時の注意

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。

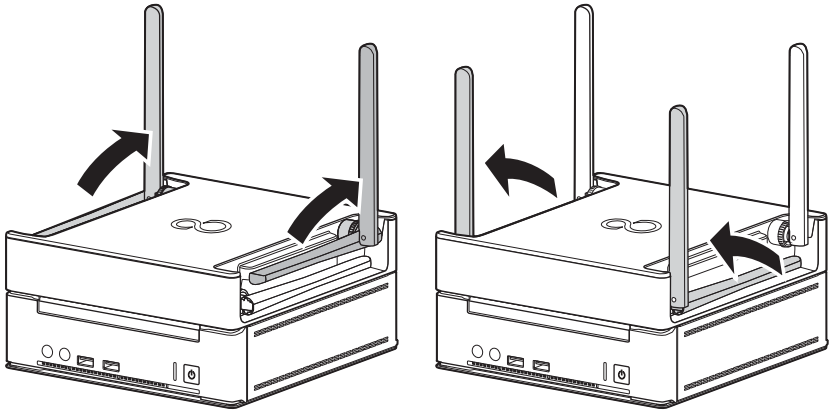


外部アンテナを立てる

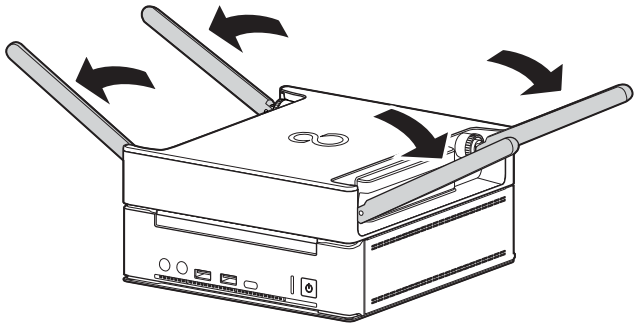
重要

▸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、ディスプレイ、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接続以外のディスプレイを使用する場合は、変換アダプタが必要になります。HDMI接続のディスプレイを使用する場合は、添付のDP-HDMI変換アダプタをご使用ください。その他のディスプレイを接続する場合は、ご使用のディスプレイにあった変換アダプタをご用意ください。

ディスプレイを接続する

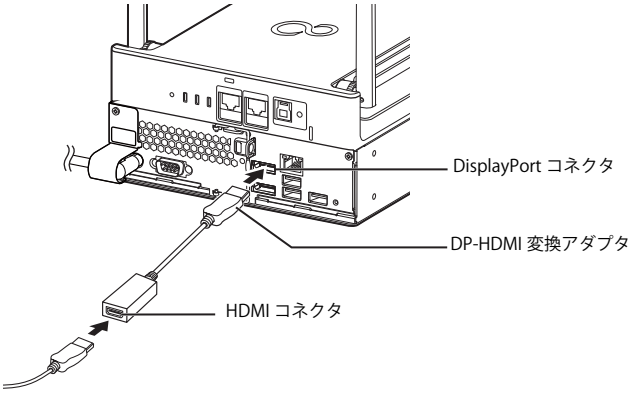
重要

- セットアップが完了するまで、接続するディスプレイは1台のみにしてください。
- ディスプレイは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 接続のディスプレイをお使いの場合

1　ディスプレイの 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。

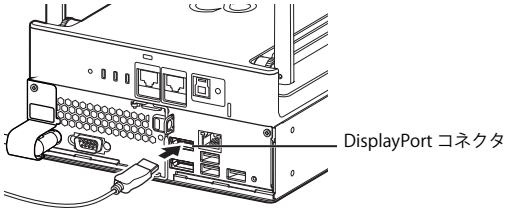
2　本製品背面の DisplayPort コネクタに DP-HDMI 変換アダプタを接続します。



（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 接続のディスプレイをお使いの場合

1　ディスプレイの 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。



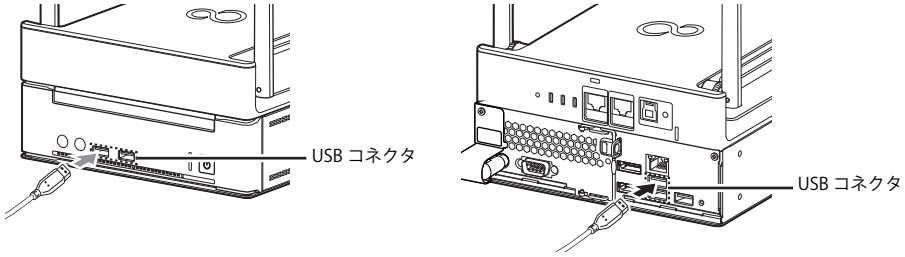
（イラストは、電源ケーブル以外のすべてのケーブルを省略した状態です。）

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

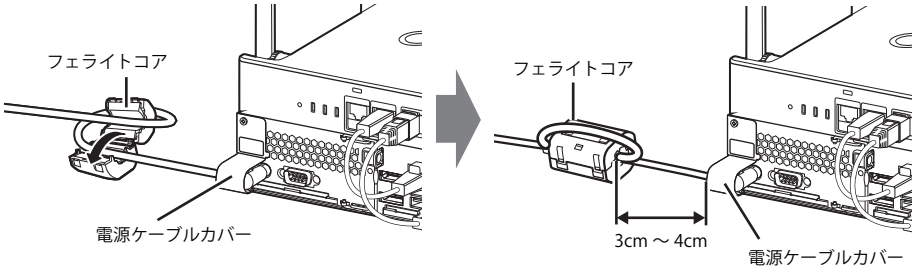
▶本製品を移動する場合や長時間使用しない場合などで、電源ケーブルを取り付けや取り外しを行うときは電源プラグ側を抜き差ししてください。

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。

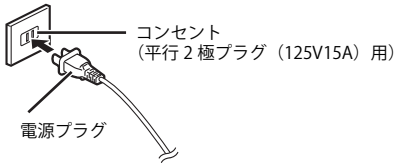
電源ケーブルカバーから約 3cm ～ 4cm の位置に取り付けてください。



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 台目のディスプレイ・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。

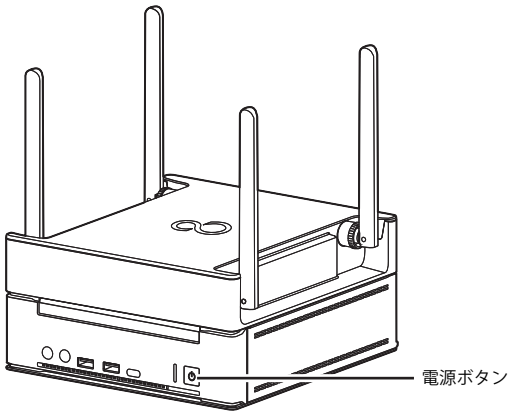
セットアップを実行する

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　ディスプレイに電源を入れます。
ディスプレイの電源の入れ方は、お使いのディスプレイ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 お住まいの地域を確認する画面では、「はい」をクリックします。

2 キーボードレイアウトを確認する画面では、「はい」をクリックします。

3 2 つ目のキーボードレイアウトを追加する画面では、「スキップ」をクリックします。

4 ネットワークに接続する画面では、「今はスキップ」をクリックします。

5「後で時間を節約するために今すぐ接続」の画面では、「いいえ」をクリックします。

6 ライセンス契約の画面では、内容をよく読み、同意いただける場合は「同意」をクリックします。

7「この PC を使うのはだれですか？」画面では、次の項目を入力し、「次へ」をクリックします。

ユーザー名：ローカルアカウントを作成します。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。

8「確実に覚えやすいパスワードを作成します」画面では、パスワードを入力し「次へ」をクリックします。

パスワード：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。

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。

9「パスワードの確認」の画面が表示されたら、前の手順と同じパスワードを入力し、「次へ」をクリックします。

10「このアカウントのセキュリティの質問を作成します」画面が表示されたら、画面の指示に従って操作します。

11「アクティビティの履歴を利用してデバイス間でより多くのことを行う」画面が表示されたら、「はい」を選択します。

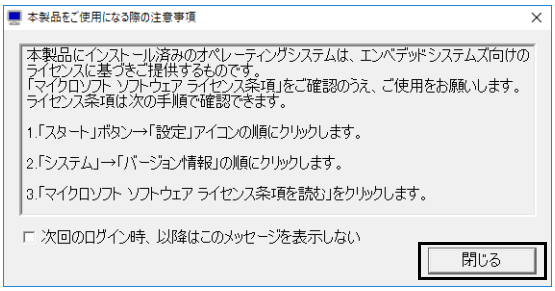
12「デバイスのプライバシー設定の選択」画面では、同意いただける場合は「同意」をクリックします。

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ます。

13「本製品をご使用になる際の注意事項」画面が表示されたら、内容を確認した後、「閉じる」をクリックします。

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。

14「閉じる」をクリックします。

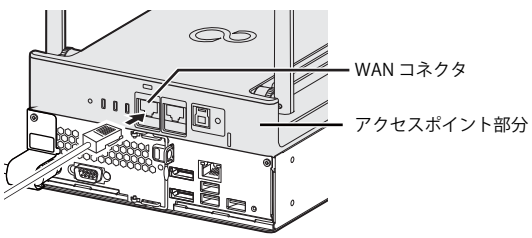


POINT

- 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.109）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。）

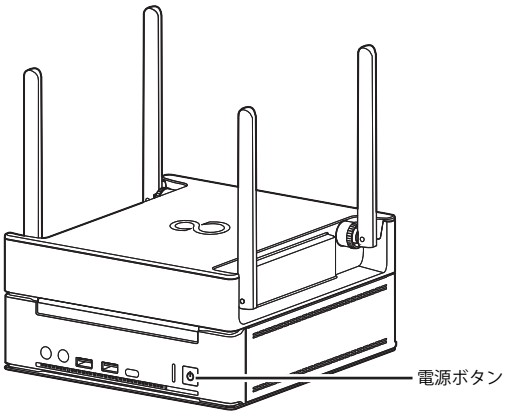
電源の入れ方／切り方

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 本製品にディスプレイを接続します。
「ケーブルを接続する」（→ P.26）

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.26）

3 本製品の電源ボタンを押します。

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.109）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.106）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

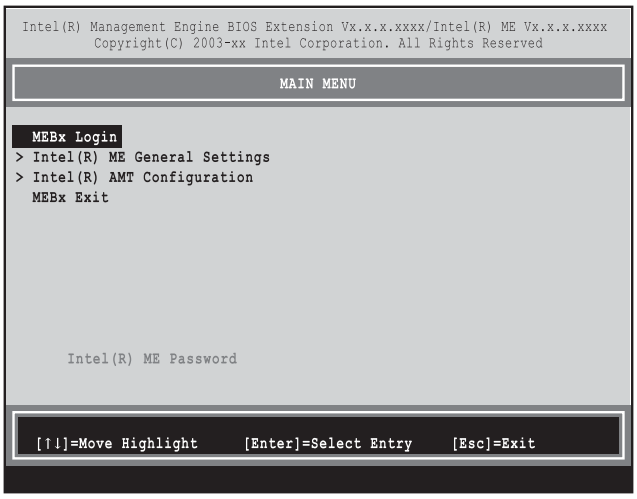
ME セットアップの初期パスワードを変更します。ご利用にあたり、パスワードは必ず変更してください。なお、変更したパスワードは、忘れないように大切に保管しておいてください。

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、本製品の 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本製品の IP アドレスの変更が必要なため実用的ではありません。固定 IP アドレスは必ずご準備ください。

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.35）

2　コンピューター部分の IP アドレスの設定（→ P.37）

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.37）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.35）。
  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.37）。

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.6）。
「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 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　画面左側の「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　画面左側の「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 〜手順 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。

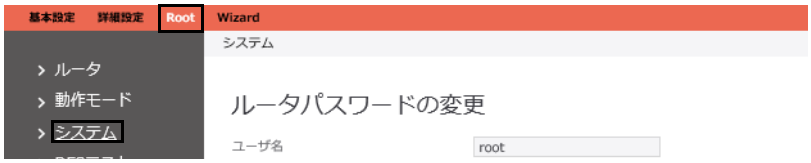
3 ユーザ名とパスワードを入力し、「ログイン」をクリックします。

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。

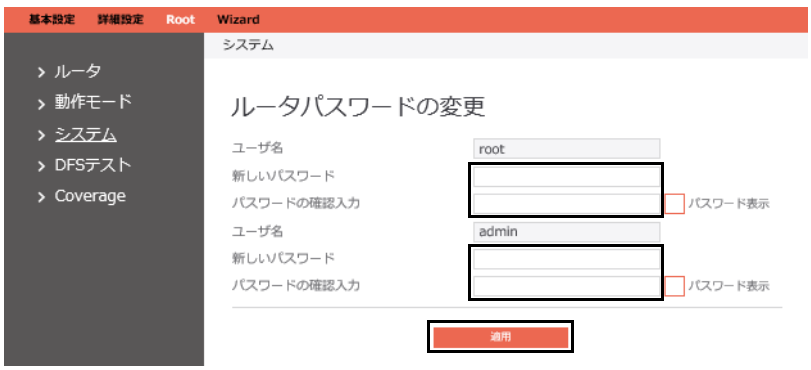
1 「Root」→「システム」の順にクリックします。



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。
- 運用管理ツールを利用して運用する場合は、エッジコンピューティングデバイスに運用管理ツールクライアント機能をインストール後、必ず「運用管理ツール/AP部 連携用パスワード設定ツール」を実行してください。「運用管理ツール/AP部 連携用パスワード設定ツール」ではadminのパスワードを入力する必要があります。



パスワード変更後はログイン画面に戻ります。ユーザー名「root」で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

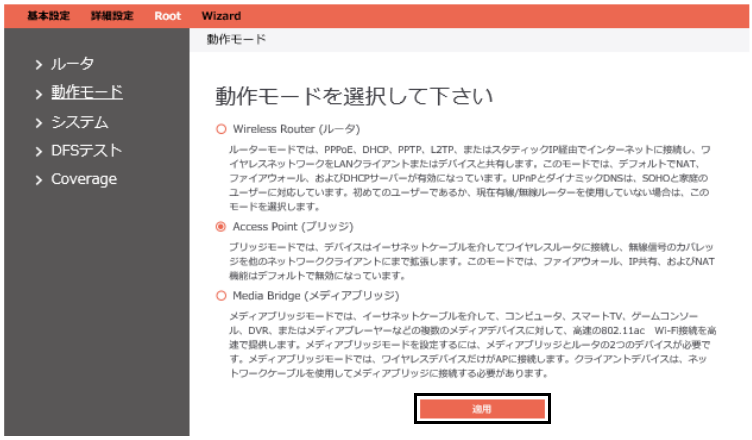
本製品のアクセスポイント部分の固定 IP アドレスや SSID を設定します。

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。



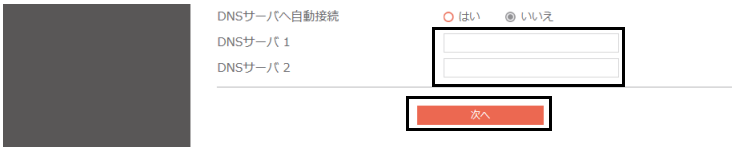
3 「LAN IP アドレスの自動取得」で「いいえ」を選択した後、LAN IP 設定の各項目に、取得した固定 IP アドレス、サブネットマスク、デフォルトゲートウェイを入力します。

POINT

- グローバルIPアドレスには対応していません。入力すると「マスクエラー」が表示されます。IPアドレスには、プライベートIPアドレスを入力してください。プライベートIPアドレスとは、組織内のネットワーク（プライベートネットワーク）でのみ使用できるIPアドレスです。プライベートIPアドレスの範囲は次のとおりです。

クラス	範囲	サブネットマスク	アドレス数
クラス A	10.0.0.0 ～ 10.255.255.255	255.0.0.0	16,777,216（16,777,216×1 サブネット）
クラス B×16	172.16.0.0 ～ 172.31.255.255	255.240.0.0	1,048,576（65,536×16 サブネット）
クラス C×256	192.168.0.0 ～ 192.168.255.255	255.255.0.0	65,536（256×256 サブネット）

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。

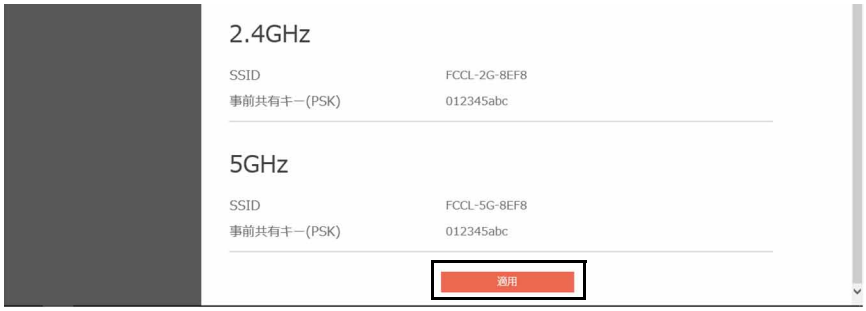


5「2.4GHz」および「5GHz」無線接続の SSID と事前共有キー（PSK）を設定し、「次へ」をクリックします。

「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。

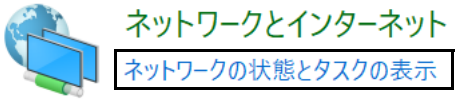


コンピューター部分の固定 IP アドレスの設定

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.6）。
「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。

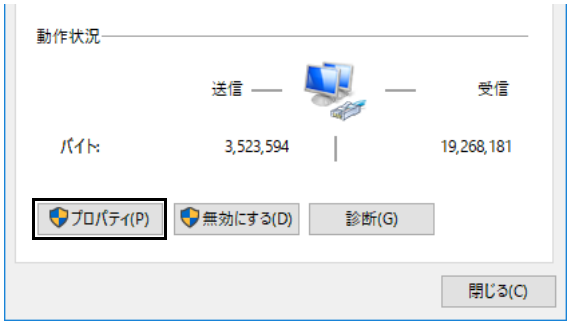


「基本ネットワーク情報の表示と接続のセットアップ」が表示されます。

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。

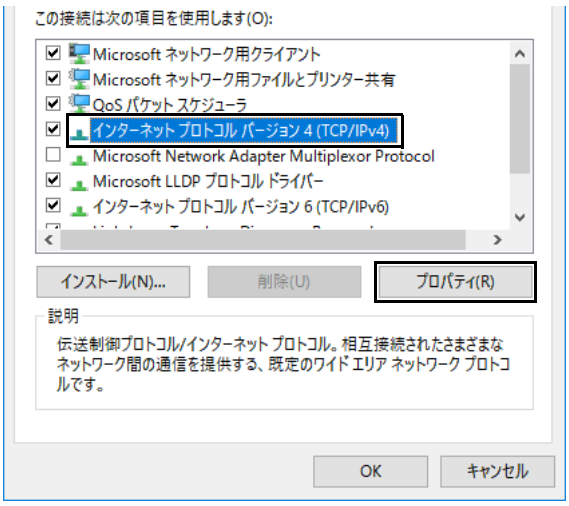
「イーサネットの状態」が表示されます。

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。

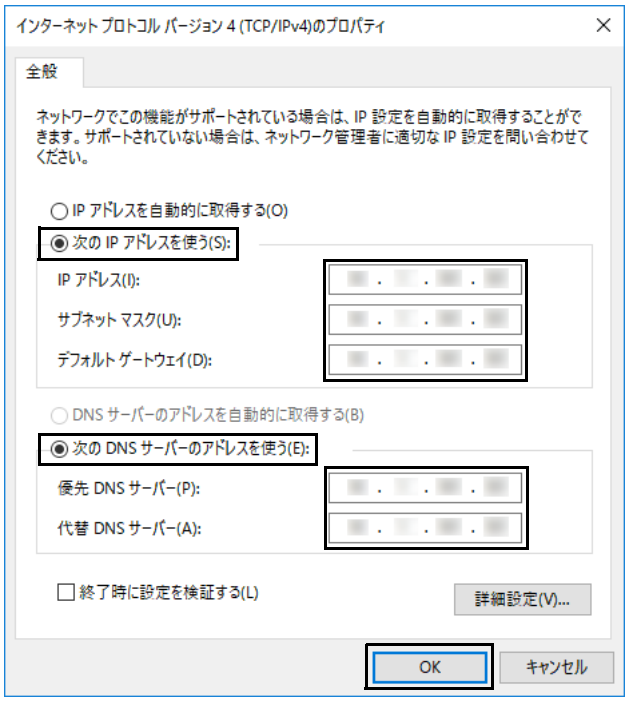
5「インターネット プロトコル バージョン 4（TCP/IPv4）」を選択し、「プロパティ」クリックします。



「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 サーバーを追加します。NTP サーバー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サーバーにアクセスできない場合に備え、複数のNTPサーバー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。

POINT

- NTPサーバーの設定はユーザー名「root」でも、「admin」でも変更可能です。

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。

NTP サーバーを設置している場合は、NTP サーバー名を入力してください。

4　「適用」をクリックします。

POINT

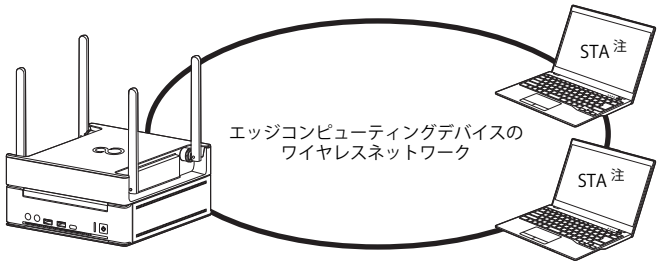
- 登録したNTPサーバーを削除する場合は、⊖ をクリックしてください。

無線 LAN 環境を構築する

ここでは、社内で端末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：ワイヤレス網内のノートパソコンなどの端末

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。

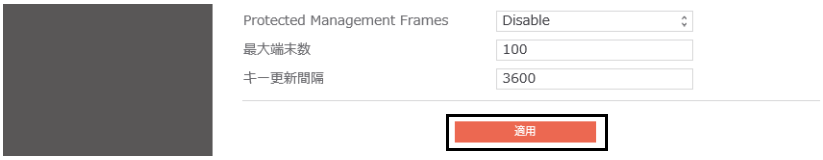
6「認証モード」で「WPA2 Personal」を選択します。

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。



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.45）。

●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.48）。

●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.50）。

■ VLAN 環境がない場合

Model1（→ P.45）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.48）か Model3（→ P.50）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。

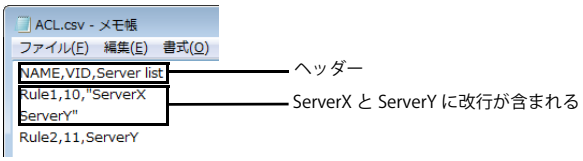
●ユーザ DB 設定ファイル（USER1.csv）
端末の情報（ユーザー名や MAC アドレス）、ネットワークアクセスの優先度、どのアクセスルールを適用するかを記載します。

●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。

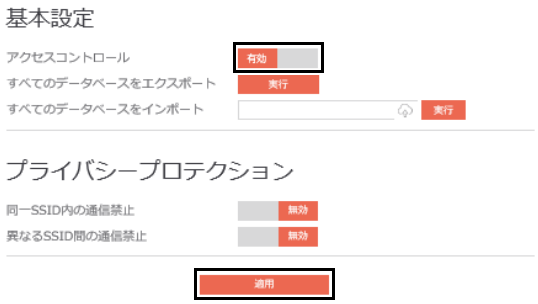
詳しくは、次の項目をご覧ください。
・「Model1 のネットワーク分離を設定する」（→ P.45）
・「Model2 のネットワーク分離を設定する」（→ P.48）
・「Model3 のネットワーク分離を設定する」（→ P.50）

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

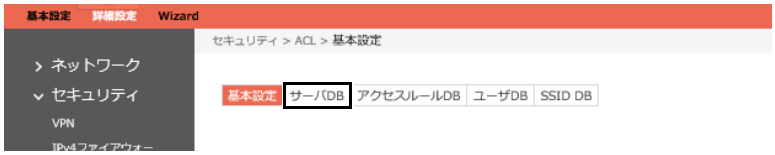
1「詳細設定」→「セキュリティ」→「ACL」の順にクリックします。

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。

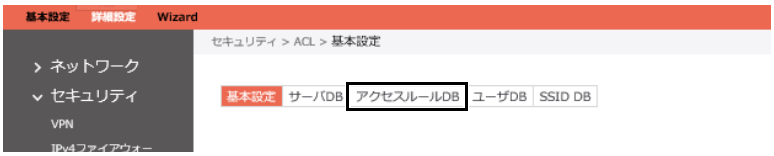


2「サーバ DB のインポート」で をクリックした後、表示されたウィンドウから SERVER.csv ファイルを選択し、「実行」をクリックします。

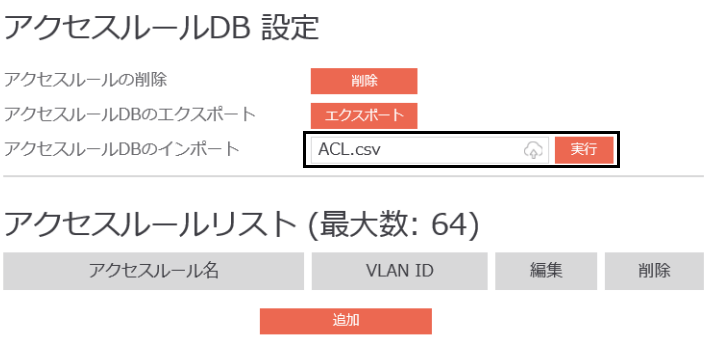
インポートが完了すると SERVER.csv で記載した設定が「サーバ DB リスト」に表示されます。

■ 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。



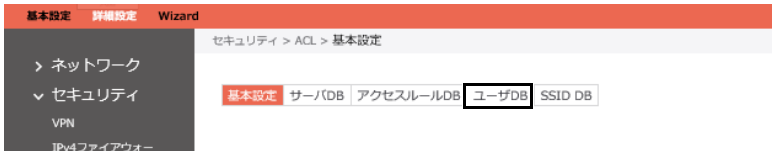
2「アクセスルール DB のインポート」で をクリックした後、表示されたウィンドウから ACL.csv ファイルを選択し、「実行」をクリックします。



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。

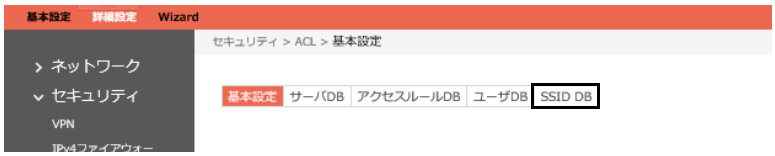


2「新しい DB 名」に「USER1」を入力し、「ユーザ DB のインポート」で をクリックした後、表示されたウィンドウから USER1.csv ファイルを選択し、「実行」をクリックします。
このユーザ DB 名は、SSID.csv で必要となります。

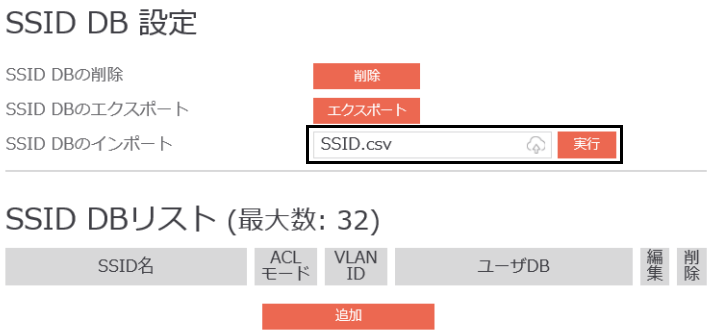
インポートが完了した後、「ユーザ DB を選択して下さい」で「USER1」を選択すると、USER1.csv に記載した設定が「ユーザ DB リスト」に表示されます。

■ 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。



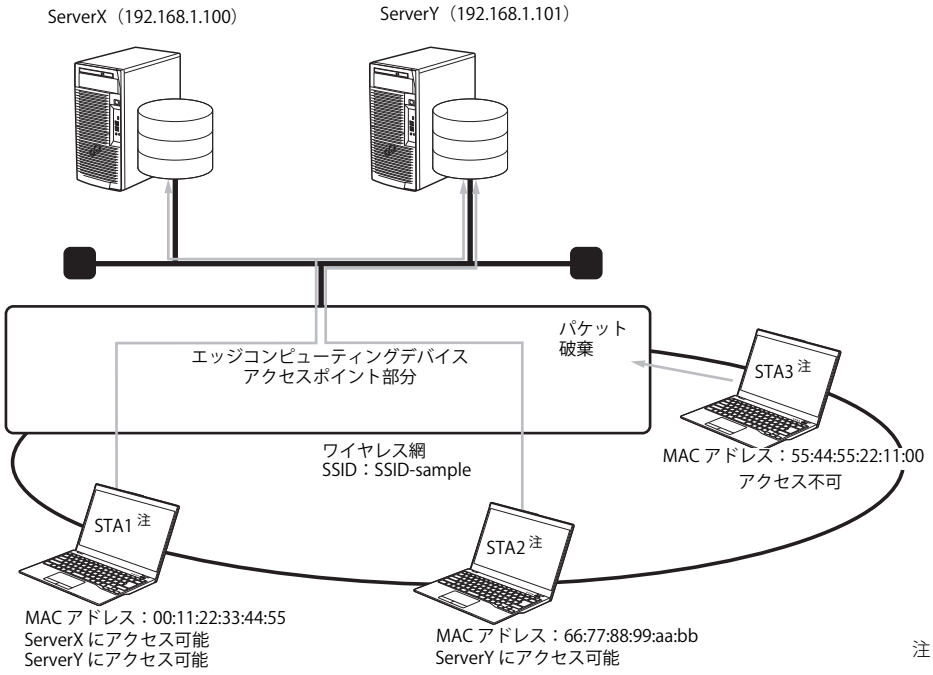
2「SSID DB のインポート」で をクリックした後、表示されたウィンドウから SSID.csv ファイルを選択し、「実行」をクリックします。



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：ワイヤレス網内のノートパソコンなどの端末

■設定ファイルを作成する

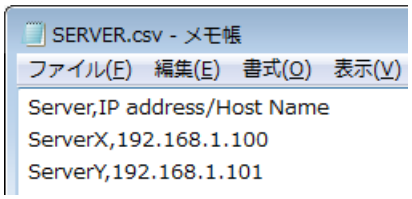
Model1 の設定に必要な CSV ファイルは SERVER、ACL、USER1、SSID です。これらのファイルを事前に、作成してください。なお、各 CSV ファイルの記載内容は、次のとおりです。

●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。

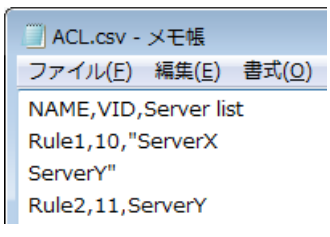


●ACL.csv

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。



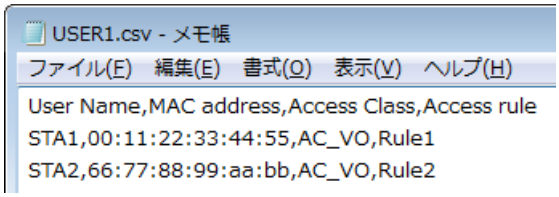
●USER1.csv

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。

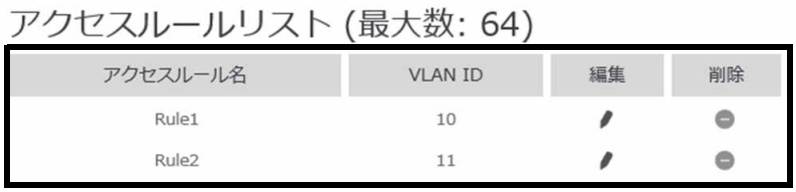
■設定ファイルをインポートする

1 SERVER.csv ファイルをインポートします（→ P.42）。

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。

3 ACL.csv ファイルをインポートします（→ P.43）。

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。



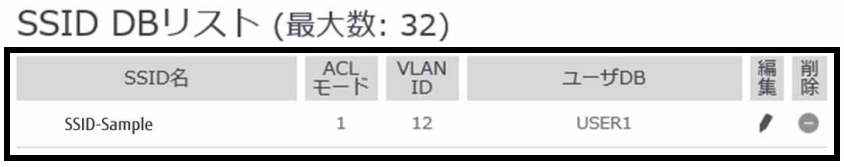
5 USER1.csv ファイルをインポートします（→ P.43）。

6「ユーザ DB を選択して下さい」で「USER1」を選択します。

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。

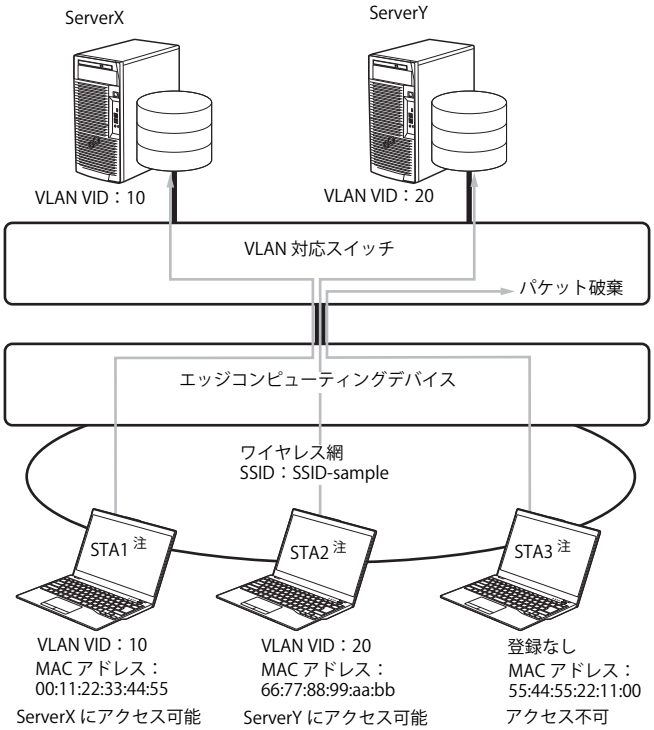
8 SSID.csv ファイルをインポートします（→ P.44）。

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。



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： ワイヤレス網内のノートパソコンなどの端末

■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。

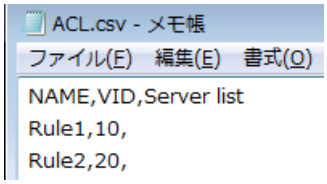
●ACL.csv

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。

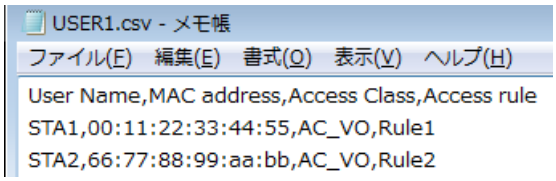


●USER1.csv

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。

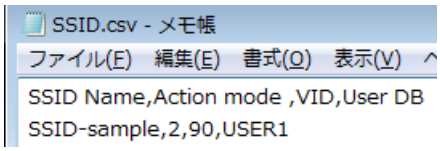


●SSID.csv

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。

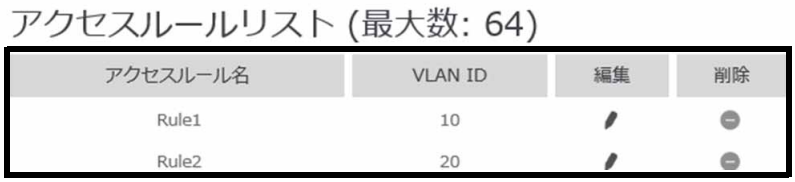
上の表を CSV ファイルで作成すると、下の図のようになります。



■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.43）。

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。



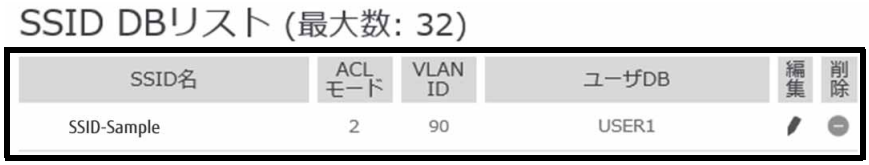
3 USER1.csv ファイルをインポートします（→ P.43）。

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。

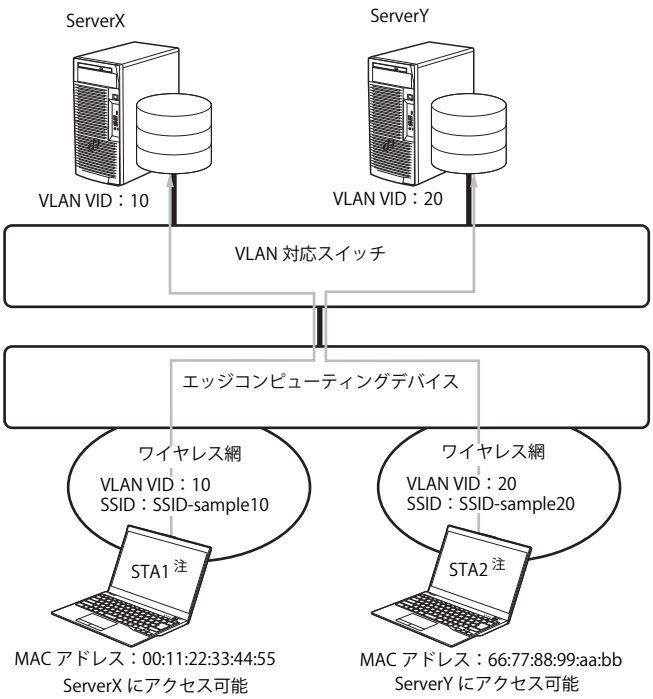
6 SSID.csv ファイルをインポートします（→ P.44）。

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 ： ワイヤレス網内のノートパソコンなどの端末

■設定ファイルを作成する

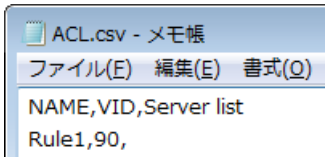
Model3 の設定に必要な CSV ファイルは ACL、USER1、SSID です。これらのファイルを事前に、作成してください。なお、各 CSV ファイルの記載内容は、次のとおりです。

●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.43）。

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。

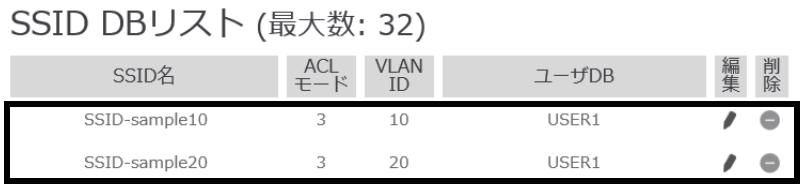
3 USER1.csv ファイルをインポートします（→ P.43）。

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。

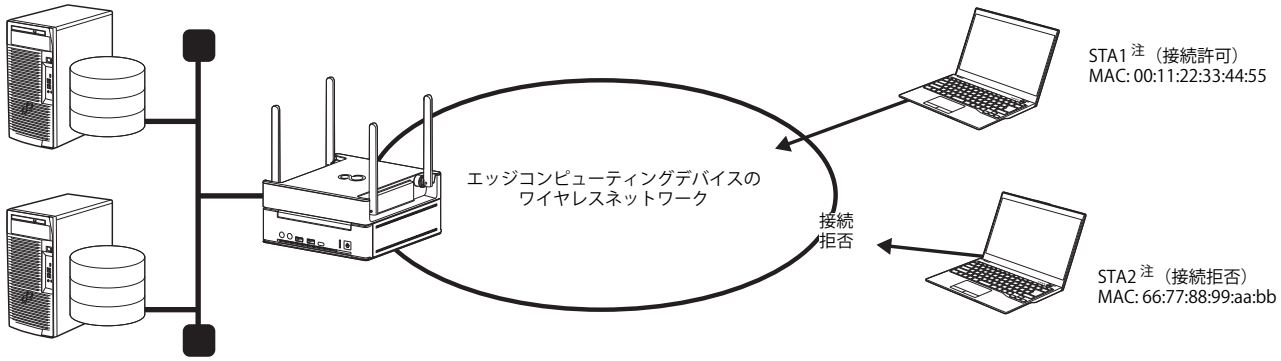
6 SSID.csv ファイルをインポートします（→ P.44）。

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： ワイヤレス網内のノートパソコンなどの端末

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

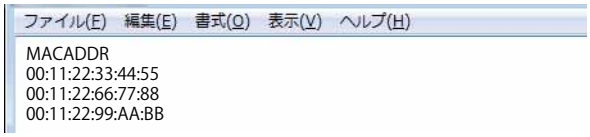
CSV ファイルを事前に作成してください。なお、CSV ファイルの記載内容は、次のとおりです。

●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

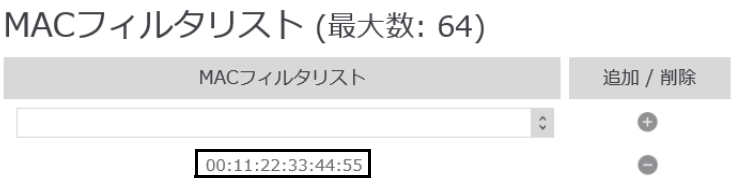
1「詳細設定」→「ネットワーク」→「無線」→「MAC フィルタ」の順にクリックします。

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

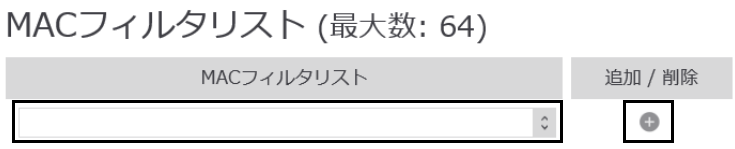
3「MAC アドレスリスト」をインポートで、作成した CSV ファイルを選択し、「実行」をクリックします。

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

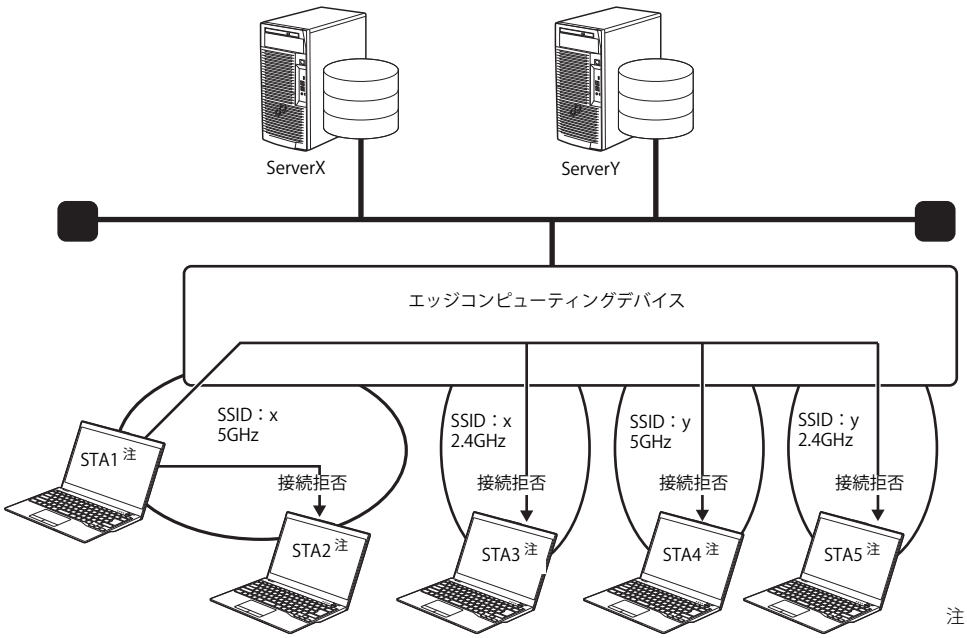
▸MACアドレスを手動で設定する場合は、次の操作を行ってください。



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

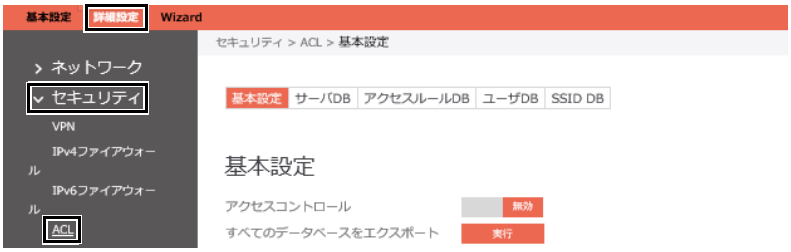
プライバシープロテクションは STA のセキュリティを確保するため、STA 間の通信を制限する機能です。
ここでは、STA 間の通信をすべて制限する場合の設定について説明します。



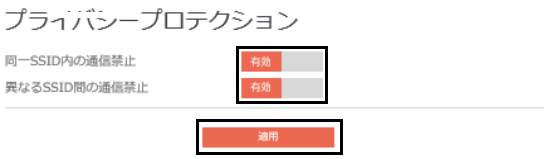
注： ワイヤレス網内のノートパソコンなどの端末

■ 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。

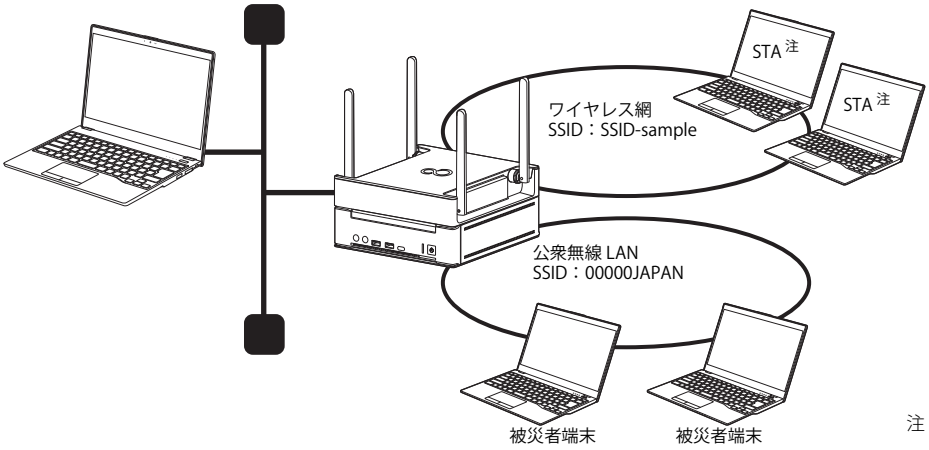


2「同一 SSID 内の通信禁止」と「異なる SSID 間の通信禁止」を「有効」に設定して、「適用」をクリックします。



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： ワイヤレス網内のノートパソコンなどの端末

■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。

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、「インストール補助ツールの実行（初期設定）」（→ P.56）を実行することでインストールされます。

インストール補助ツールの実行 （初期設定）

重要

▸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。

1 「C:¥fujitsu¥Software¥ インストール補助ツール ¥01. 基本機能（基本アプリ）¥01_BasicFunction_BaseAPP_Install.cmd」を実行します。
以降は表示された画面に従ってください。バッチファイルが完了したら、本製品を再起動してください。

2 「C:¥fujitsu¥Software¥ インストール補助ツール ¥01. 基本機能（基本アプリ）¥02_BasicFunction_BaseAPP_Install.cmd」を実行します。
以降は表示された画面に従ってください。バッチファイルが完了したら、本製品を再起動してください。

バッチファイルの実行後の再起動が完了したら、「セキュリティ除外設定」（→ P.56）からインストールと設定を進めてください。

セキュリティ除外設定

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、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
C:¥cygwin64¥squid¥libexec¥security_file_certgen.exe

ファイアウォールの設定

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ってください。なお、OS 標準の機能「Windows Defender ファイアウォール」を使用する場合は、インストール補助ツールとポート番号変更ツールを実行することで設定されるので、ここでの設定は不要です。

■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 注	-	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
Squid ICP2	UDP	3130	C:¥cygwin64¥squid¥sbin¥squid.exe	受信

注　：ポート番号変更ツール実行後に再設定する必要があります（→ P.98）。

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。

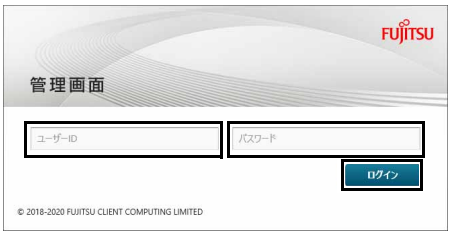
POINT

- 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/
- ポート番号変更ツールを実行した場合は、URLのポート番号「10080」を「10090」または変更したポート番号に置き換えてアクセスしてください。
- 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。

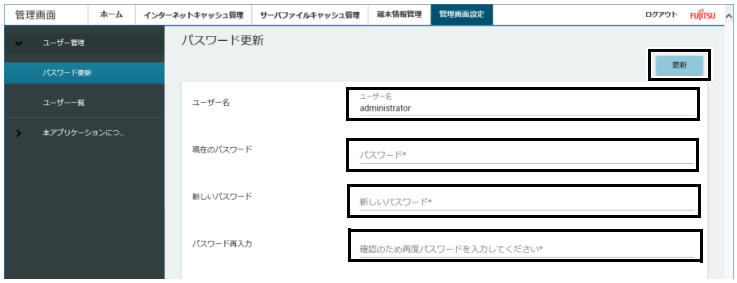
パスワードの変更

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。

2. 基本機能 - 初期設定　（業務端末／マスター端末）

業務端末とマスター端末の初期設定を行います。

重要

- マスター端末／業務端末を設定する場合、次の点に注意してください。
  - 複数のアカウントが作成されている端末に設定する場合は、すべてのアカウントに対して設定が必要となります。

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。

■ Windows10 の場合

1 「スタート」ボタン→「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。

■ Windows11 の場合

1 「スタート」ボタン→画面右上の「すべてのアプリ」→「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。

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業務端末／マスター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。

重要

- プロキシの設定は、エッジコンピューティングデバイス本体には設定しないでください。不具合が発生することがあります。
- Windows以外の端末へのプロキシ設定の方法は、ご使用の端末のマニュアルをご参照ください。
- インターネットキャッシュ機能の設定が完了するまで、インターネット接続できません。

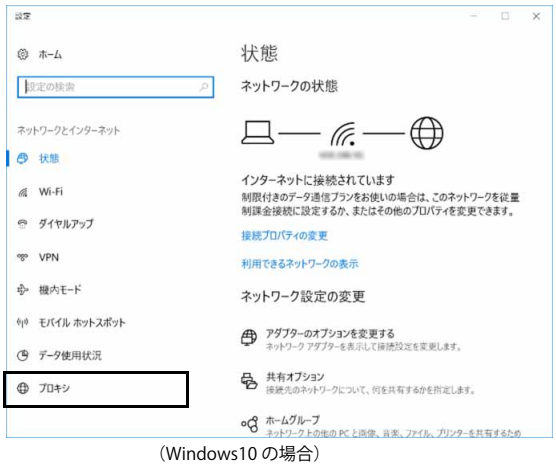
手動プロキシ設定

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.61）をご覧ください。

1 「スタート」ボタン→ または （設定）の順にクリックします。
「設定」ウィンドウが表示されます。

2 「ネットワークとインターネット」をクリックします。

3 「プロキシ」をクリックします。



（Windows10 の場合）

（Windows11 の場合）

「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」をクリックして（オフ）にします。

（Windows10 の場合）

（Windows11 の場合）

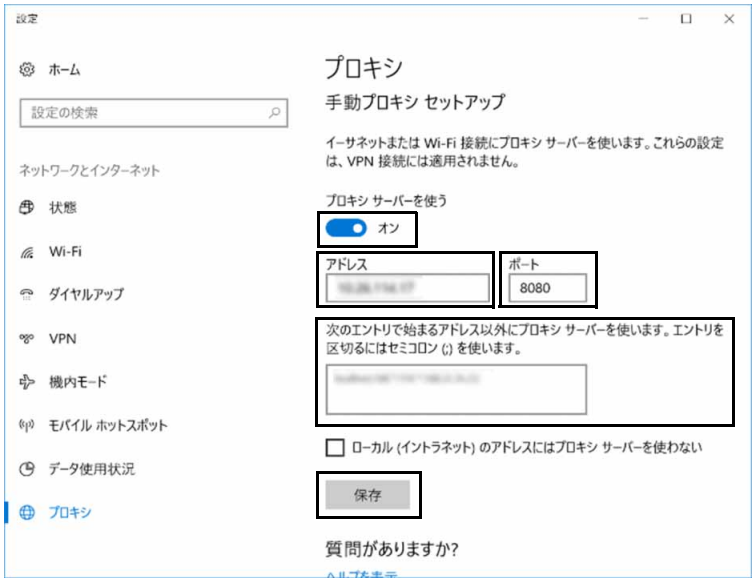
5 次の手順を実行し、手動プロキシの設定を行います。

● Windows10 の場合

1.「手動プロキシセットアップ」の「プロキシサーバーを使う」をクリックして（オン）にし、次のように入力し、「保存」をクリックします。
   - 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。
   - Windows 端末に関しては「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。
   - Windows 以外の端末へのプロキシの対象外の設定の方法については、ご使用の端末のマニュアルをご覧になり、本製品のコンピュータ部分の IP アドレスをプロキシの対象外にしてください。ただし iPad に関しては、プロキシ除外の設定項目が有りませんので、pac ファイルにて本製品のコンピュータ部分の IP アドレスをプロキシの対象外に設定してください。



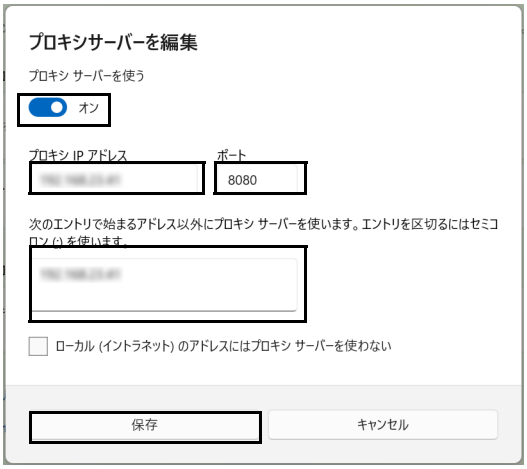
● Windows11 の場合

1. 「手動プロキシセットアップ」の「セットアップ」をクリックします。

2. 「プロキシサーバーを使う」をクリックして（オン）にし、次のように入力し、「保存」をクリックします。
   - 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。
  - Windows 端末に関しては「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。
  - Windows 以外の端末へのプロキシの対象外の設定の方法については、ご使用の端末のマニュアルをご覧になり、本製品のコンピュータ部分の IP アドレスをプロキシの対象外にしてください。ただし iPad に関しては、プロキシ除外の設定項目が有りませんので、pac ファイルにて本製品のコンピュータ部分の IP アドレスをプロキシの対象外に設定してください。



6　×をクリックして「設定」ウィンドウを閉じます。

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.61）

●プロキシ自動設定機能（→ P.67）

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。

■ 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） ファイルの作成例 1

この PAC ファイルのサンプルは、次の条件を想定しています。PAC ファイルを作成する場合は、実際に利用する環境にあわせて設定してください。

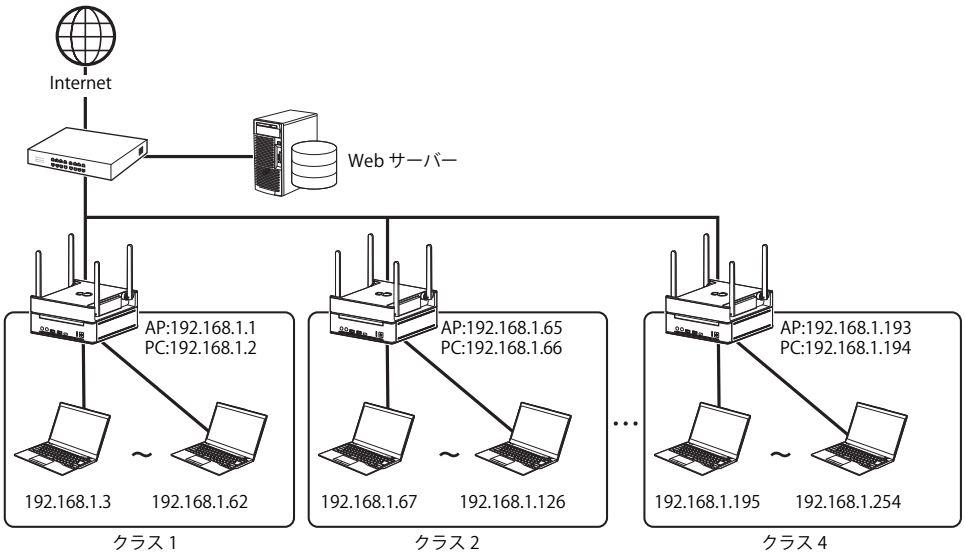
- 部署の数　：4
- エッジコンピューティングデバイス　：部署で 1 台設置
- 接続する端末の台数　：部署で 62 台接続

※ 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.61）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。

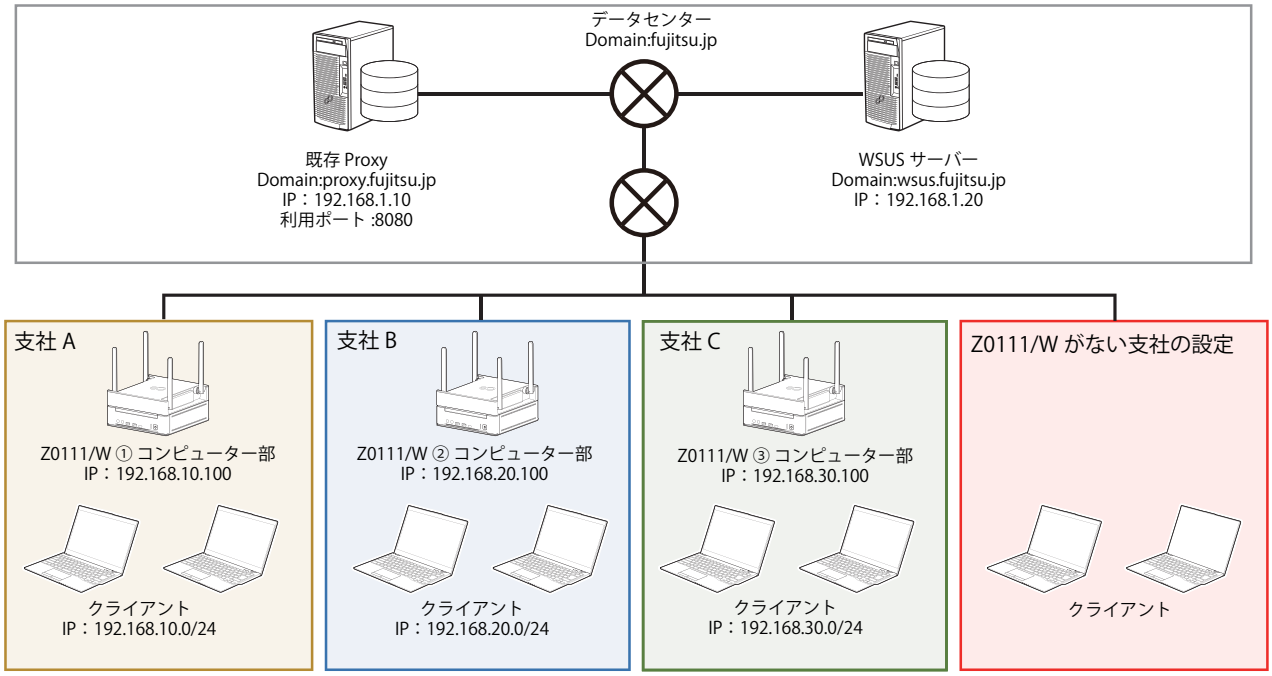
```
function FindProxyForURL(url, host) {
    // URL のホストがローカルの場合
    if (isInNet(host, "192.168.1.0", "255.255.255.0")) {
        return "DIRECT"; // プロキシを経由しない
    } else {
        // 自分の IP アドレスを取得
        myip = myIpAddress();
        // クラス 1
        if (isInNet(myip, "192.168.1.0", "255.255.255.192")) {
            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";
        }
    }
}
```

□ 自動構成スクリプト （PAC） ファイルの作成例 2

この PAC ファイルのサンプルは、次の条件を想定しています。

- 1 つの PAC ファイルに各支店の Proxy 設定を記述して運用
- WSUS サーバーへのアクセスは Z0111/W をそれ以外は既存 Proxy を経由

・下図の環境を想定しています。



●PACファイル記述サンプル

```
function FindProxyForURL(url, host) {
        myip = myIpAddress();

  if (isInNet(myip, "192.168.10.0", "255.255.255.0")) {     /*支社Ａの設定*/
        if (dnsDomainIs(host, "wsus.fujitsu.jp")) {     /*WSUSのみZ0111/Wにそれ以外は既存プロキシに*/
            return "PROXY 192.168.10.100:8080; DIRECT";
            /*Z0111/Wが応答しない場合のセカンダリに直接WSUSサーバーへのアクセスを指定*/
   }

     /* WSUSアクセス以外は既存プロキシへ*/
     return "PROXY 192.168.1.10:8080";

  } else if(isInNet(myip, "192.168.20.0", "255.255.255.0")){ /*支社Ｂの設定*/
        if (dnsDomainIs(host, "wsus.fujitsu.jp")) {     /*WSUSのみZ0111/Wにそれ以外は既存プロキシに*/
            return "PROXY 192.168.20.100:8080; DIRECT";
            /*Z0111/Wが応答しない場合のセカンダリに直接WSUSサーバーへのアクセスを指定*/
        }

     /* WSUSアクセス以外は既存プロキシへ*/
     return "PROXY 192.168.1.10:8080";

  } else if(isInNet(myip, "192.168.30.0", "255.255.255.0")){ /*支社Ｃの設定*/
        /*WSUSサーバーがIPアドレスのみでの運用の場合*/
        if (shExpMatch(host, "192.168.1.20")) {
            return "PROXY 192.168.30.100:8080; DIRECT";
            /*Z0111/Wが応答しない場合のセカンダリに直接WSUSサーバーへのアクセスを指定*/
        }

     /* WSUSアクセス以外は既存プロキシへ*/
     return "PROXY 192.168.1.10:8080";

  } else {   /*Z0111/Wがない支社の設定*/
        if (dnsDomainIs(host, "wsus.fujitsu.jp" )) {    /*WSUSのみ直接アクセスそれ以外は既存プロキシに*/
            return "DIRECT" ;
            /*直接WSUSサーバーへのアクセスを指定*/
        }

     /* WSUSアクセス以外は既存プロキシへ*/
     return "PROXY 192.168.1.10:8080";
  }

}
```

支社Aの設定

支社Bの設定

支社Cの設定

Z0111/Wがない支社の設定

□ PAC ファイルの作成例で使用している関数について

●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

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)

●dnsDomainIs 関数

ホスト名が、指定された ドメインに属しているかどうかを検出します。

```
dnsDomainIs(host, domain)
```

・引数
　host：URL から抜き出したホスト名
　domain: ドメイン名
・戻り値
　true または false

（例）dnsDomainIs("www.fujitsu.com",".fujitsu.com") → OK（True）
　　dnsDomainIs("www",".fujitsu.com")　　→ NG（False）

●shExpMatch 関数

ホスト名または URL をマッチングすることができます。

```
shExpMatch(str, shexp)
```

・引数
　str：比較対象の文字列（通常は URL またはホスト名を指定）
　shexp：比較するシェル表現（IP アドレス、URL 等）
・戻り値
　true または false

（例）shExpMatch("http://www.fujitsu.com/test/index.html",".*/test/.*") → OK（True）
　　shExpMatch("http://www.fujitsu.com/test/index.html","/test/.*")　→ NG（False）　※「/test」の前に「＊」がないため NG となります。

●例外設定について

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。

●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

重要

▶Windows以外の端末への自動構成スクリプト（PAC）の設定方法については、ご使用の端末のマニュアルをご覧ください。

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 「スタート」ボタン→ または （設定）の順にクリックします。
「設定」ウィンドウが表示されます。

2 「ネットワークとインターネット」をクリックします。

3 「プロキシ」をクリックします。

（Windows10 の場合）

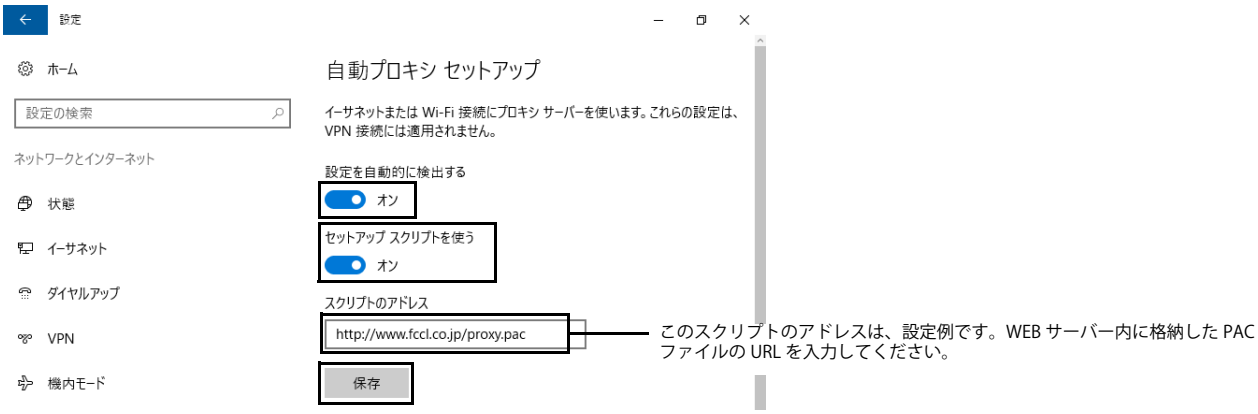
（Windows11 の場合）

「プロキシ」が表示されます。

4 次の手順を実行し、自動プロキシの設定を行います。

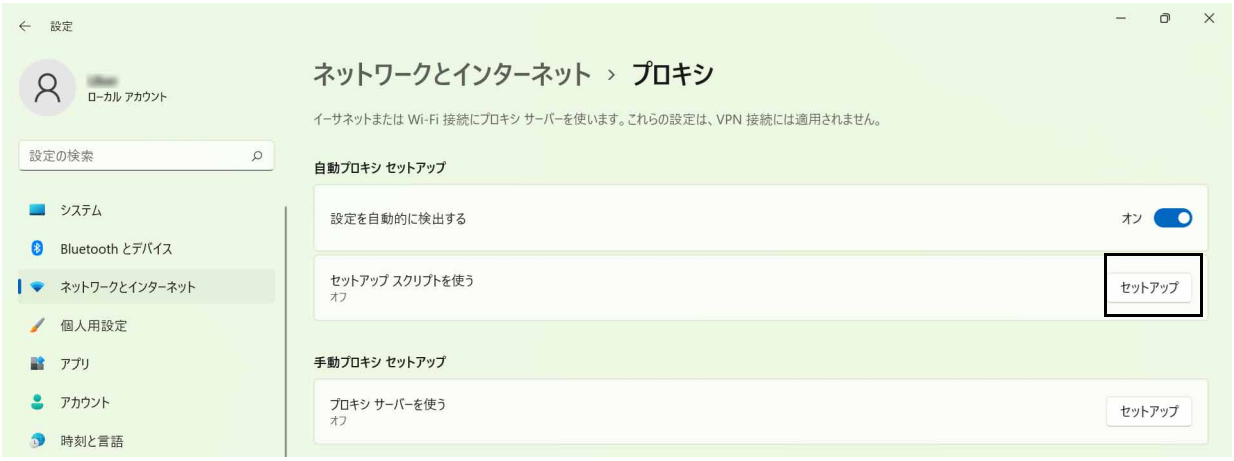
● Windows10 の場合

1. 「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」をクリックして （オン）にし、次のように入力し、「保存」をクリックします。
   ・スクリプトのアドレス：PAC ファイルの URL

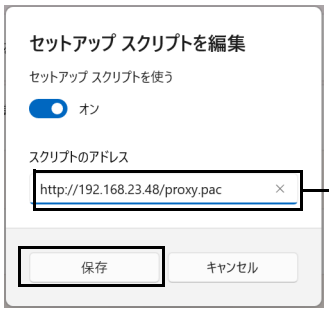


● Windows11 の場合

1. 「自動プロキシセットアップ」の「設定を自動的に検出する」をクリックして（オン）にし、「セットアップ」をクリックします。



2. 次のように入力し、「保存」をクリックします。
   ・スクリプトのアドレス：PAC ファイルの URL



このスクリプトのアドレスは、設定例です。WEB サーバー内に格納した PAC ファイルの URL を入力してください。

5　✕をクリックして「設定」ウィンドウを閉じます。

■ 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。

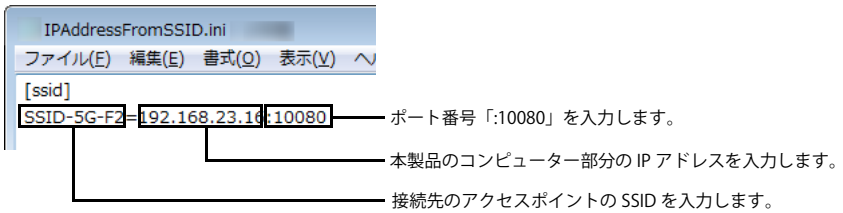
□ インストール

1. エッジコンピューティングデバイスの「C:¥Fujitsu¥Software¥InternetCache¥ProxyController」フォルダーを端末の「C:¥」にコピーします。
2. 次のファイルを右クリックし、「管理者として実行」を選択します。

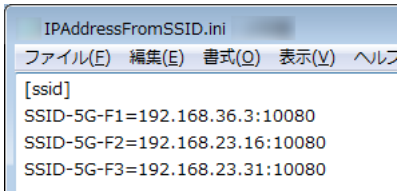
   C:¥ProxyController¥inst.bat
3. 次のファイルをデスクトップにコピーします。

   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」をクリックします。

WindowsUpdate の通信がプロキシサーバーを使用する設定　（マスター端末の場合）

マスター端末の場合、次の設定を行います。

1　管理者権限でコマンドプロンプトを起動します（→ P.6）。

2　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。

3　コマンドプロンプトを終了します。

WindowsUpdate の通信がプロキシサーバーを使用する設定　（業務用端末の場合）

業務用端末で、ユーザーがアカウントにログインしていない状態で WindowsUpdate を実行する運用の場合、業務用端末に対して次の設定を行います。

POINT

▸ユーザーがアカウントにログインしている状態でWindowsUpdateを実行する運用の場合はこの設定をする必要はありません。ただし、マスター端末を使用した運用の場合は、マスター端末に対してこの設定は必須となります。[END]

1　管理者権限でコマンドプロンプトを起動します（→ P.6）。

2　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。

3　コマンドプロンプトを終了します。

イントラネットの Microsoft 更新サービスの場所を指定する設定

マスター端末／業務端末で、ローカルグループポリシーに「イントラネットの Microsoft 更新サービスの場所を指定する」を設定します。

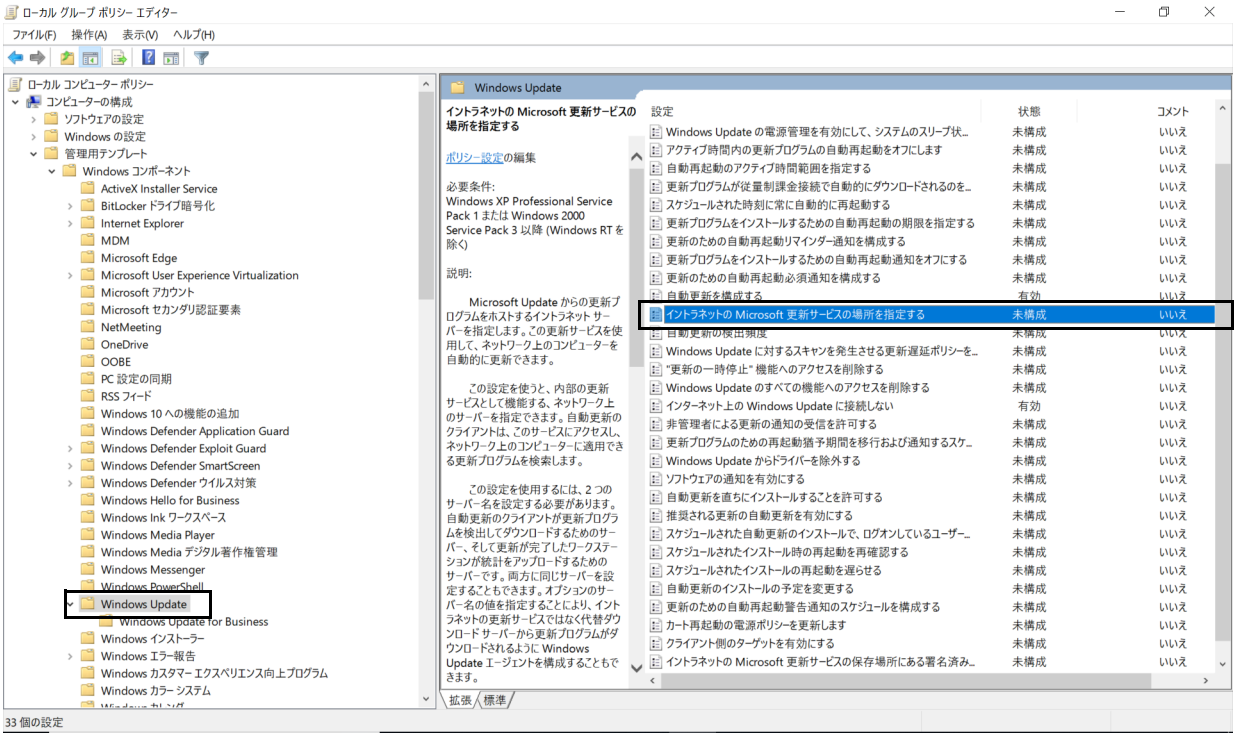
1 **管理者権限でコマンドプロンプトを起動します（→ P.6）。**

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 **次の手順を実行し、「イントラネットの Microsoft 更新サービスの場所を指定する」の設定画面を表示します。**

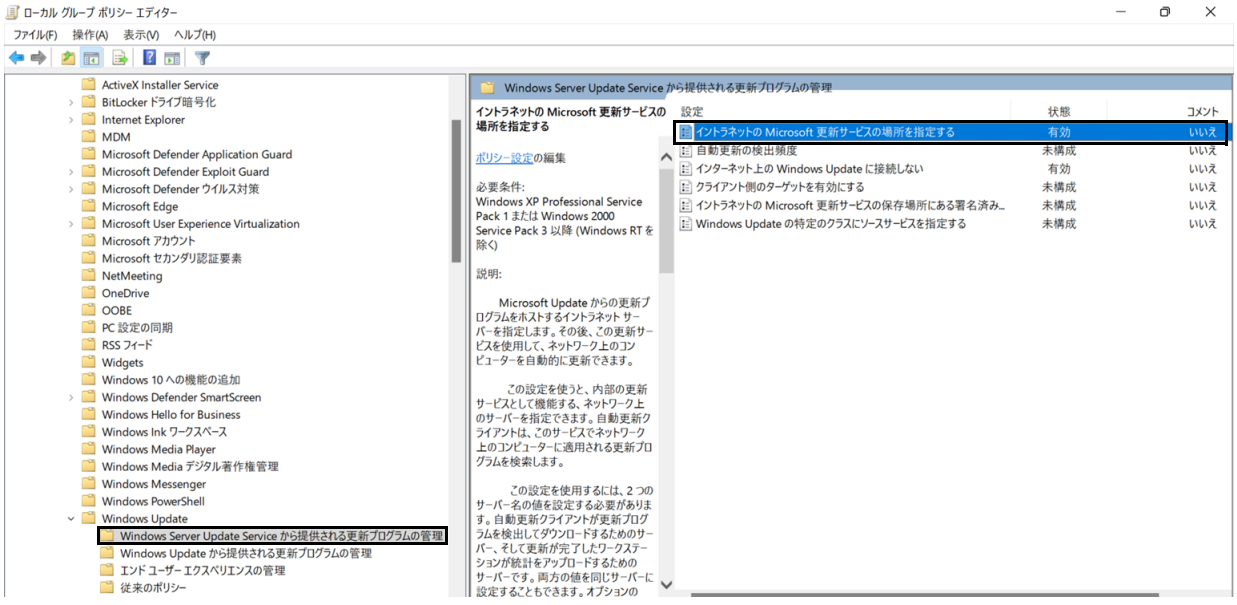
● Windows10 の場合

1. 「コンピューターの構成」の「管理者用テンプレート」-「Windows コンポーネント」-「Windows Update」を選択し、「イントラネットの Microsoft 更新サービスの場所を指定する」をダブルクリックします。



● Windows11 の場合

1. 「コンピューターの構成」の「管理者用テンプレート」-「Windows コンポーネント」-「Windows Update」-「Widows Server Update Service から提供される更新プログラムの管理」を選択し、「イントラネットの Microsoft 更新サービスの場所を指定する」をダブルクリックします。

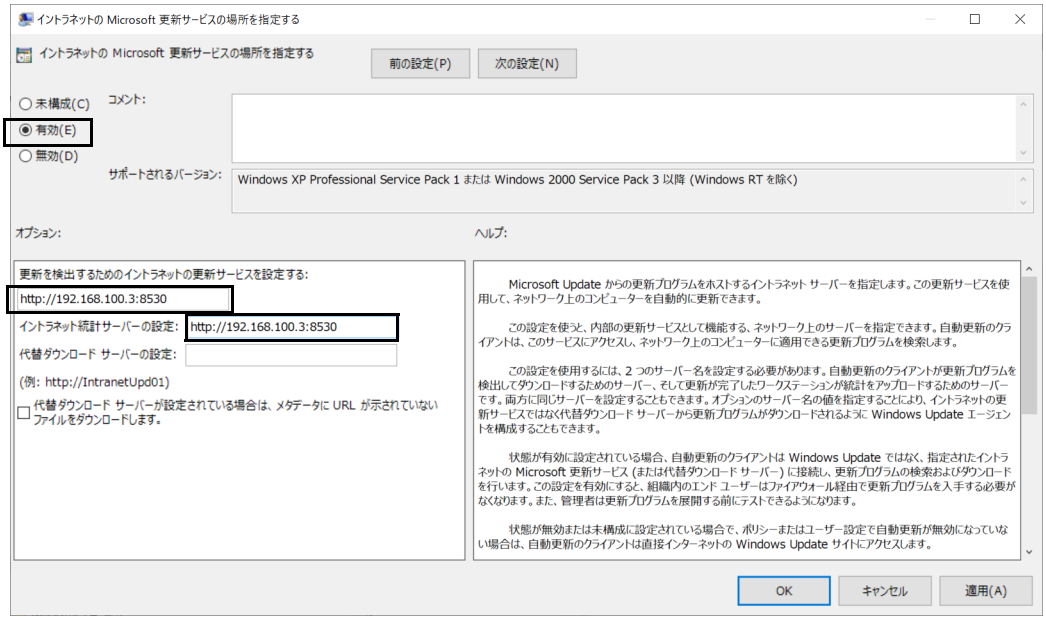


4「有効」を選択し、「更新を検出するためのイントラネットの更新サービスを更新する」と「イントラネット統計サーバーの設定」に「http://WSUS サーバー名 : ポート番号」を入力します。

POINT

- WSUSサーバー名には、WSUSサーバーのIPアドレス、完全修飾ドメイン名 （FQDN）、または、ホスト名を入力してください。
- WSUSサーバー名を完全修飾ドメイン名（FQDN）で設定する場合、本製品をドメイン参加させるなど、本製品の名前解決ができるように本製品をネットワーク上に配置してください。
  WSUSサーバーのホスト名が「wsus-server」、ドメイン名が「fujitsu.co.jp」、WSUS のポート番号が「8530」の場合、完全修飾ドメイン名（FQDN）は次のようになります。
  http://wsus-server.fujitsu.co.jp:8530
- WSUSサーバーを完全修飾ドメイン名（FQDN）で設定する場合やホスト名で設定する場合は、「WUServer.conf」を設定する必要があります。詳しくは、「設定ファイルの変更」（→P.89）をご覧ください。
- WSUSサーバーをホスト名で設定する場合は、「hosts」ファイルを設定する必要があります。詳しくは、「hostsファイルの変更」（→P.90）をご覧ください。

次の画面の例は、WSUS サーバーの IP アドレスが「192.168.100.3」、WSUS のポート番号が「8530」の場合です。



5「適用」をクリックして「OK」をクリックします。

インターネット上の Windows Update に接続しない設定

マスター端末／業務端末で、ローカルグループポリシーに「インターネット上の Windows Update に接続しない」を設定します。

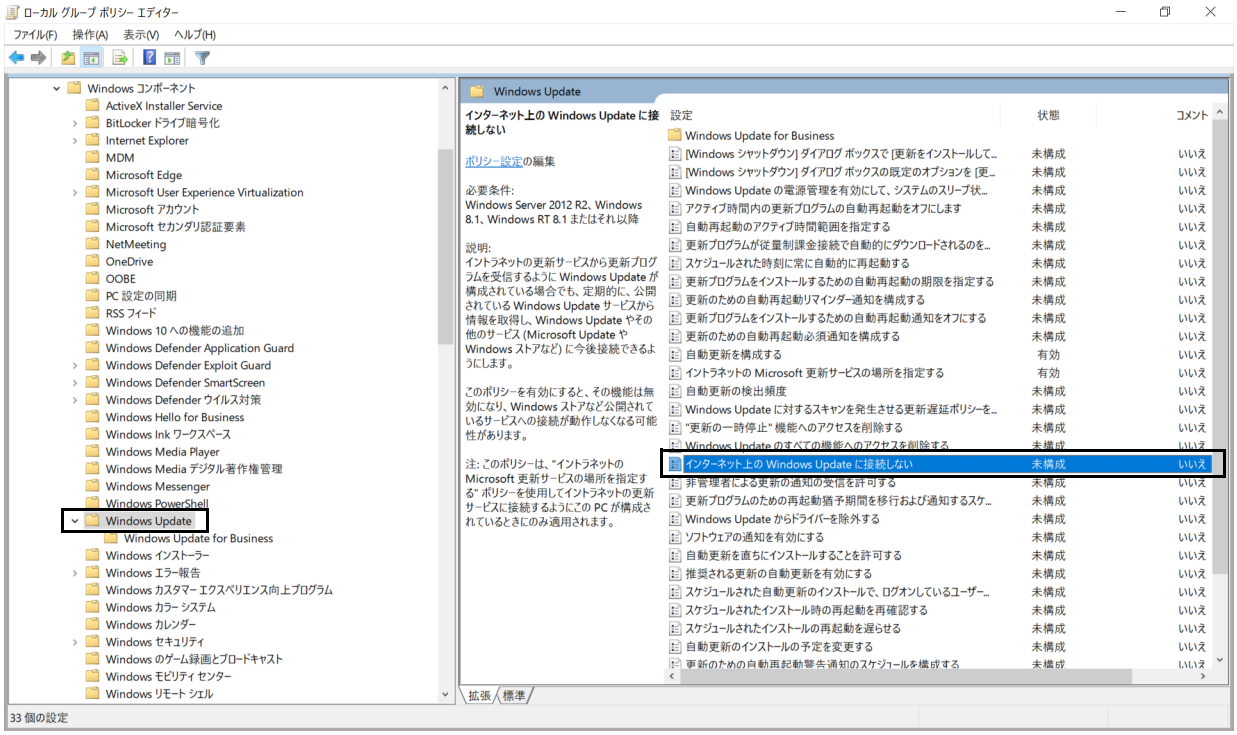
1 **管理者権限でコマンドプロンプトを起動します（→ P.6）。**

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 **次の手順を実行し、「インターネット上の Windows Update に接続しない」の設定画面を表示します。**

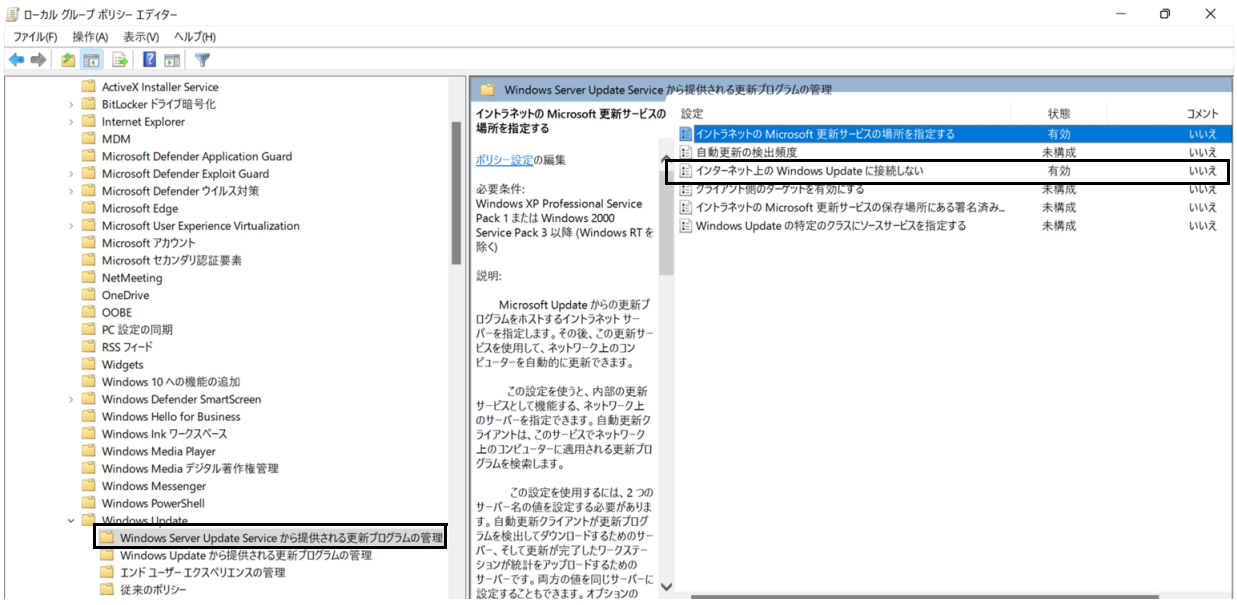
● Windows10 の場合

1. 「コンピューターの構成」の「管理者用テンプレート」-「Windows コンポーネント」-「Windows Update」を選択し、「インターネット上の Windows Update に接続しない」をダブルクリックします。

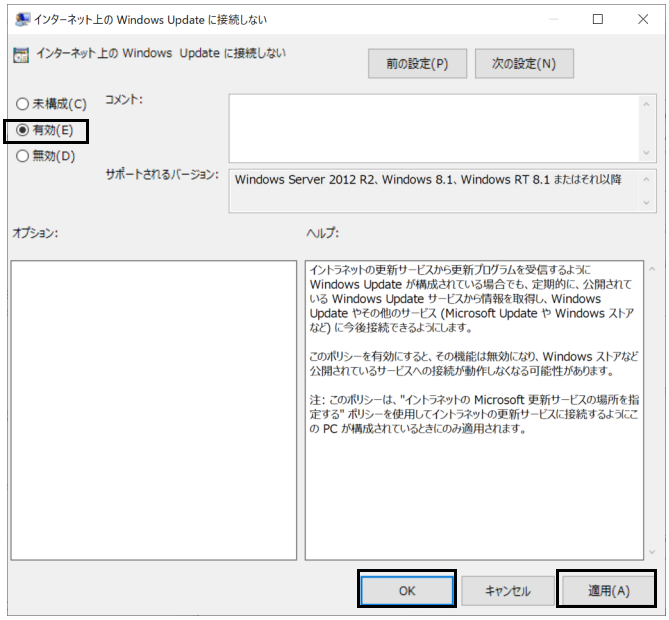


● Windows11 の場合

1. 「コンピューターの構成」の「管理者用テンプレート」-「Windows コンポーネント」-「Windows Update」-「Widows Server Update Service から提供される更新プログラムの管理」を選択し、「インターネット上の Windows Update に接続しない」をダブルクリックします。



4「有効」を選択した後、「適用」をクリックして「OK」をクリックします。



配信の最適化を OFF にする設定

マスター端末／業務端末で、配信の最適化を OFF に設定します。

1 次の手順を実行し、「Windows Update」の「詳細オプション」を表示します。

● Windows10 の場合

1.「スタート」ボタン→ または （設定）→「更新とセキュリティ」→「Windows Update」→「詳細オプション」の順にクリックします。

● Windows11 の場合

1.「スタート」ボタン→ または （設定）→「Windows Update」→「詳細オプション」の順にクリックします。

2「配信の最適化」をクリックします。

（Windows10 の場合）

（Windows11 の場合）

3「他の PC からダウンロードを許可する」を「オフ」にします。

（Windows10 の場合）

（Windows11 の場合）

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の実行　（インターネットキャッシュ機能）

重要

▸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。

1「C:¥Fujitsu¥Software¥ インストール補助ツール ¥02. 基本機能（インターネットキャッシュ）¥BasicFunction_InternetCache_Install.cmd」を実行します。
以降は表示された画面に従ってください。バッチファイルが完了したら、本製品を再起動してください。

バッチファイルの実行が完了したら、「親プロキシサーバーの設定」（→ P.74）からインストールと設定を進めてください。

インターネットキャッシュ機能の設定

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。

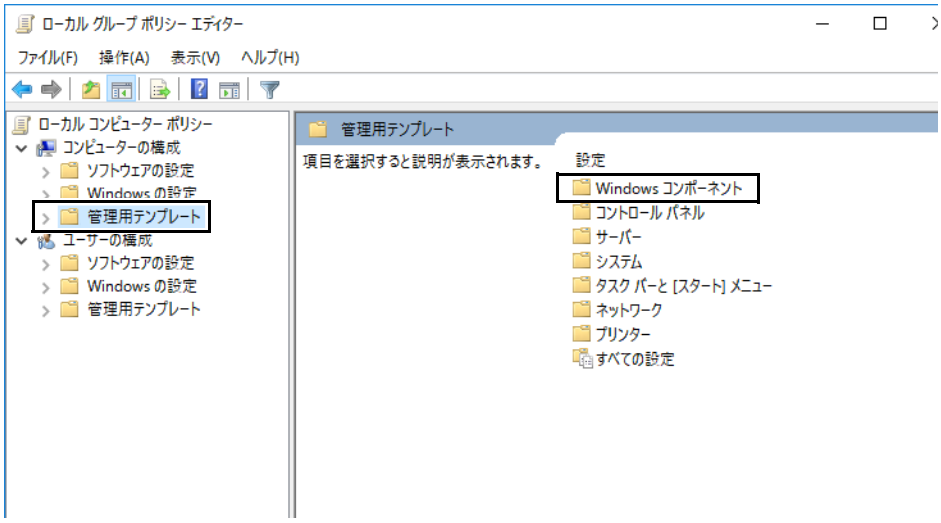
POINT

▸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。

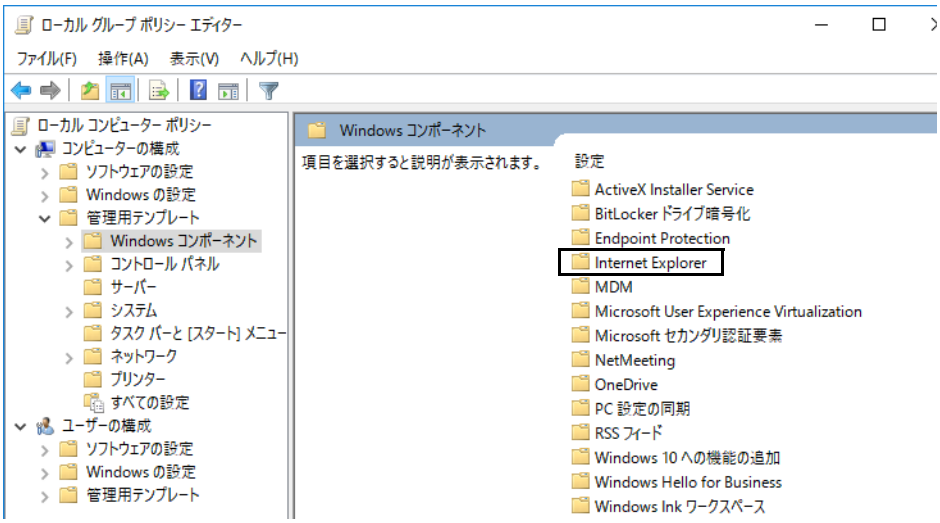
1 管理者権限でコマンドプロンプトを起動します（→ P.6）。

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。

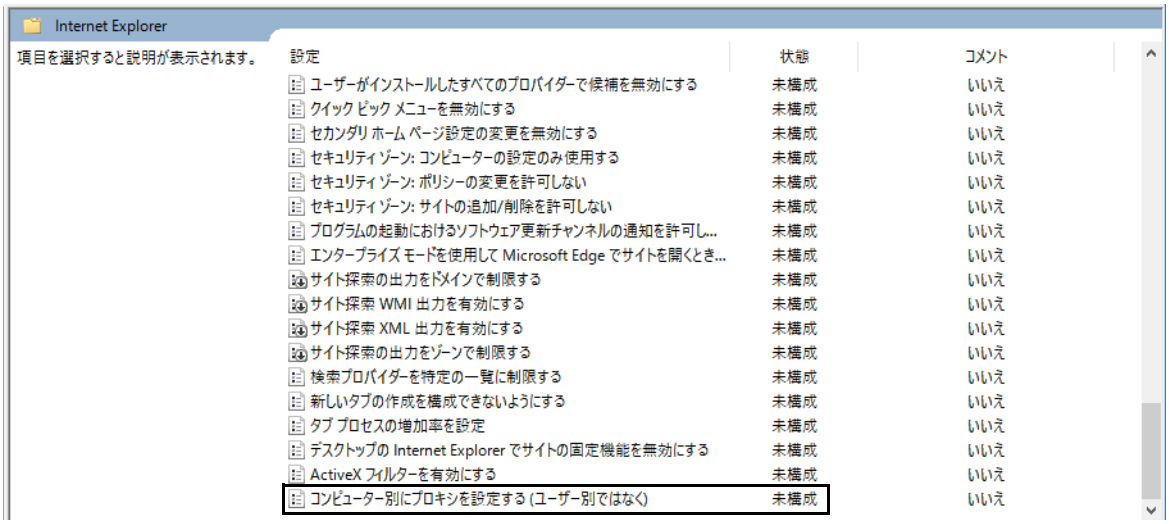
3「コンピューターの構成」の「管理用テンプレート」を選択し、「Windows コンポーネント」をダブルクリックします。



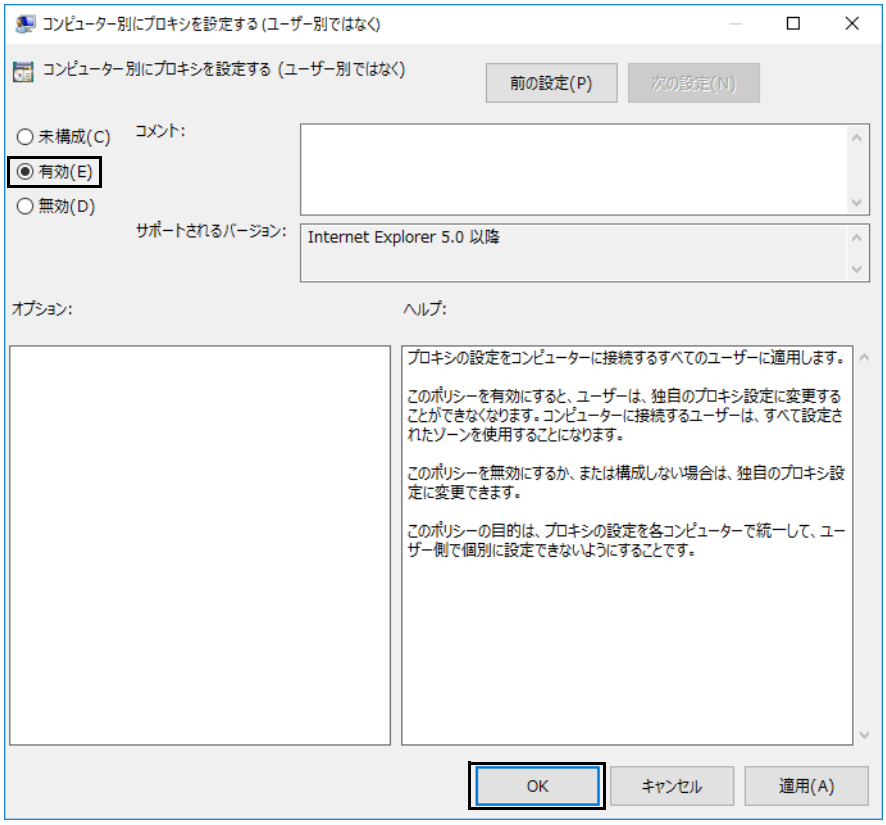
4「Internet Explorer」をダブルクリックします。



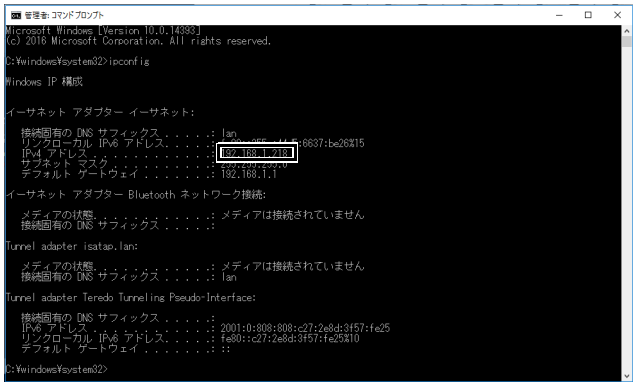
5「コンピューター別にプロキシを設定する（ユーザー別ではなく）」をダブルクリックします。



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。



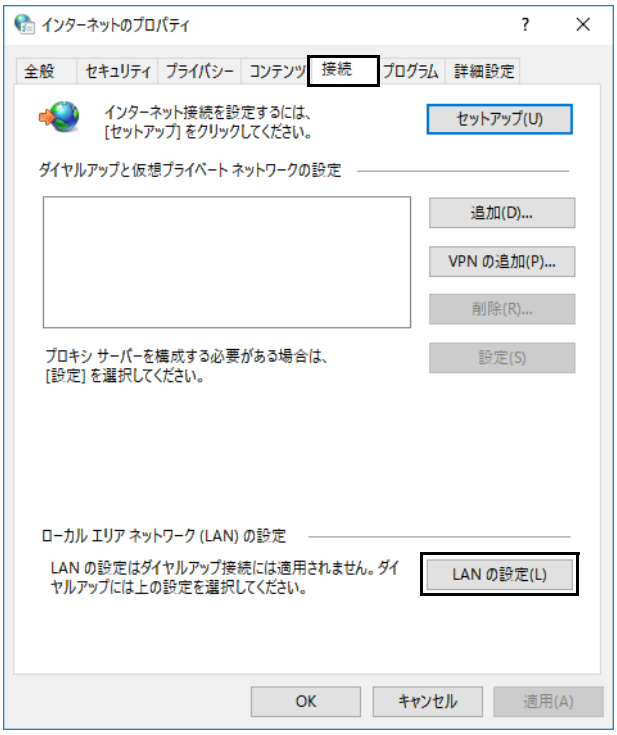
表示された IP アドレスを確認し、メモに控えておいてください。

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。

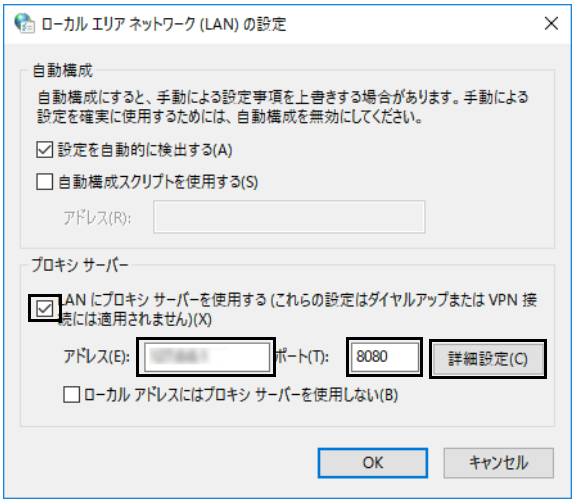
10 Internet Explorer の画面の右上隅の（ツール）→「インターネット オプション」の順にクリックします。
「インターネットのプロパティ」が表示されます。

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。

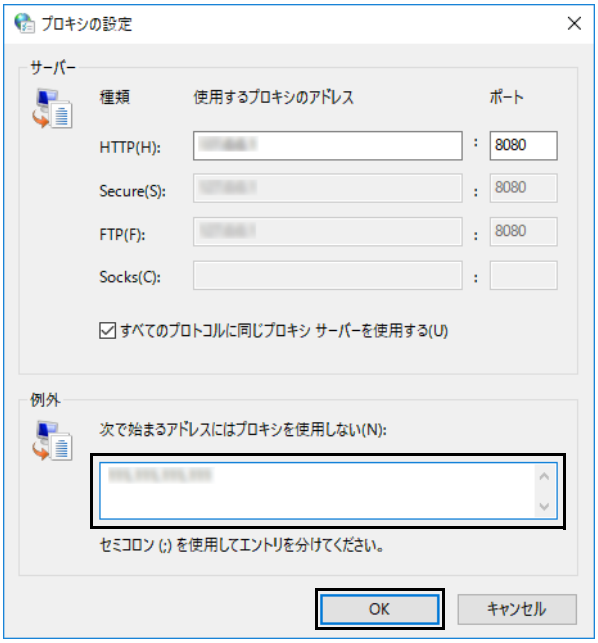


「プロキシ設定」が表示されます。

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。
ポート番号は、ポート番号変更ツール実行後に再設定する必要があります（→ P.98）。ここでは、「10080」を入力してください。



「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。**

証明書の作成とインストール

ここでは、証明書の作成方法と作成した証明書をエッジコンピューティングデバイス本体にインストールする方法を説明します。
なお、管理画面で「キャッシュ設定」の「キャッシュ対象プロトコル」を「http」に設定する場合は、証明書の作成およびインストールは不要です（→ P.83）。

重要

- インターネットキャッシュ機能をお使いになるには、エッジコンピューティングデバイス本体と業務端末/マスター端末に証明書をインストールする必要があります。証明書は作成する必要があります。
- 業務端末/マスター端末用の証明書は、エッジコンピューティングデバイスの証明書から作成します。エッジコンピューティングデバイスの証明書を必ず先に作成してください。
- 証明書の有効期間が切れた場合、証明書を新しく作成してインストールし直す必要がります。
- エッジコンピューティングデバイスを複数台導入してhttpsプロトコルをキャッシュする場合は、すべてのエッジコンピューティングデバイス共通の証明書ファイル（myCA.pem、myCA.der）をご利用ください。共通の証明書ファイルをご利用するには、最初に作成した証明書ファイル（myCA.pem、myCA.der）を他のエッジコンピューティングデバイスにコピーして、「証明書のインストール（エッジコンピューティングデバイス用）」（→P.79）の手順に従ってインストールしてください。
端末についても共通の証明書ファイル（myCA.der）を「証明書のインストール（業務端末／マスター端末用）」（→P.92）に従ってインストールしてください。共通の証明書を利用しない場合、正しくキャッシュデータが作成/利用できません。

■ 証明書の作成　（エッジコンピューティングデバイス用）

1 **管理者権限でコマンドプロンプトを起動します（→ P.6）。**

2 **次のコマンドを入力して【Enter】キーを押します。**
cd C:¥cygwin64¥bin

POINT

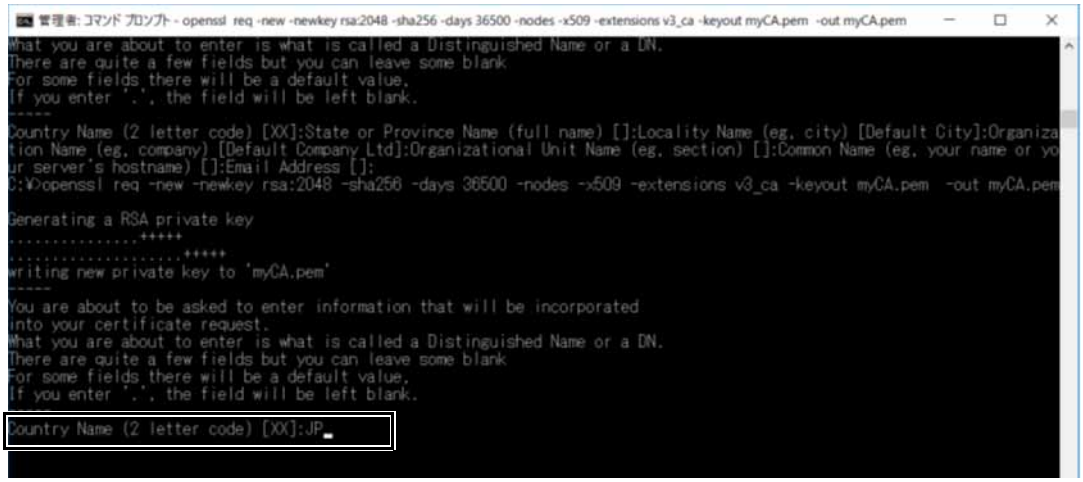
▸次の手順でコマンド（openssl.exe）を実行するためには、カレントディレクトリを「C:¥cygwin64¥bin」にしておく必要があります。

3 **次のコマンドを入力して【Enter】キーを押します。**
openssl req -new -newkey rsa:2048 -sha256 -days [証明書の有効期間(日)] -nodes -x509 -extensions v3_ca -keyout myCA.pem -out myCA.pem

POINT

▸証明書の推奨有効期間は825日です。
▸証明書の名称は「myCA.pem」で固定です。それ以外の名前にするとインターネットキャッシュ機能が動作しない可能性が有ります。

4 次の入力画面で「JP」を入力して【Enter】キーを押します。

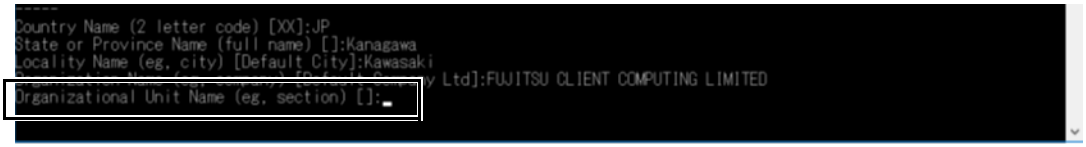


5 次の入力画面で「Kanagawa」を入力して【Enter】キーを押します。

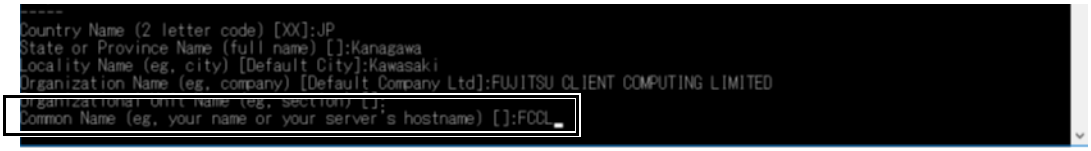
6 次の入力画面で「Kawasaki」を入力して【Enter】キーを押します。

7 次の入力画面で「FUJITSU CLIENT COMPUTING LIMITED」を入力して【Enter】キーを押します。

8 次の入力画面では、何も入力しないで【Enter】キーを押します。



9 次の入力画面では、「FCCL」を入力して【Enter】キーを押します。



10 次の入力画面では、何も入力しないで【Enter】キーを押します。

11 「C:¥cygwin64¥bin¥myCA.pem」が作成されていることを確認します。

以上でエッジコンピューティングデバイスの証明書の作成は終了です。

■証明書の作成　（業務端末 / マスター端末用）

重要

- 業務端末/マスター端末の証明書は、エッジコンピューティングデバイスの証明書から作成します。エッジコンピューティングデバイスの証明書を必ず先に作成してください。
- エッジコンピューティングデバイスに次のファイルがあることを確認してから業務端末/マスター端末の証明書の作成を行ってください。
  C:¥cygwin64¥bin¥myCA.pem
  ファイルがない場合は、「証明書の作成（エッジコンピューティングデバイス用）」（→P.77）から実施してください。

1　管理者権限でコマンドプロンプトを起動します（→ P.6）。

2　次のコマンドを入力して【Enter】キーを押します。
cd C:¥cygwin64¥bin

POINT

- 次の手順でコマンド（openssl.exe）を実行するためには、カレントディレクトリを「C:¥cygwin64¥bin」にしておく必要があります。

3　次のコマンドを入力して【Enter】キーを押します。
openssl x509 -in myCA.pem -outform DER -out myCA.der

POINT

- 証明書の名称は「myCA.der」で固定です。それ以外の名前にするとインターネットキャッシュ機能が動作しない可能性が有ります。

4　「C:¥cygwin64¥bin¥myCA.der」が作成されていることを確認します。
以上で業務端末 / マスター端末の証明書の作成は終了です。

■証明書のインストール　（エッジコンピューティングデバイス用）

1　ブラウザーを起動します。

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、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。

・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。

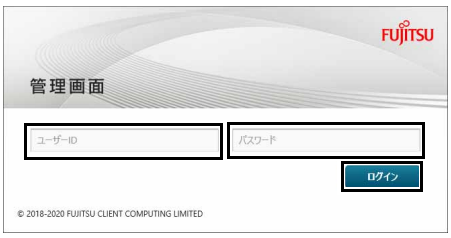
3　管理画面の URL（http://IP アドレス :10080/）に接続します。

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/
- ポート番号変更ツールを実行した場合は、URLのポート番号「10080」を「10090」または変更したポート番号に置き換えてアクセスしてください。
- 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。

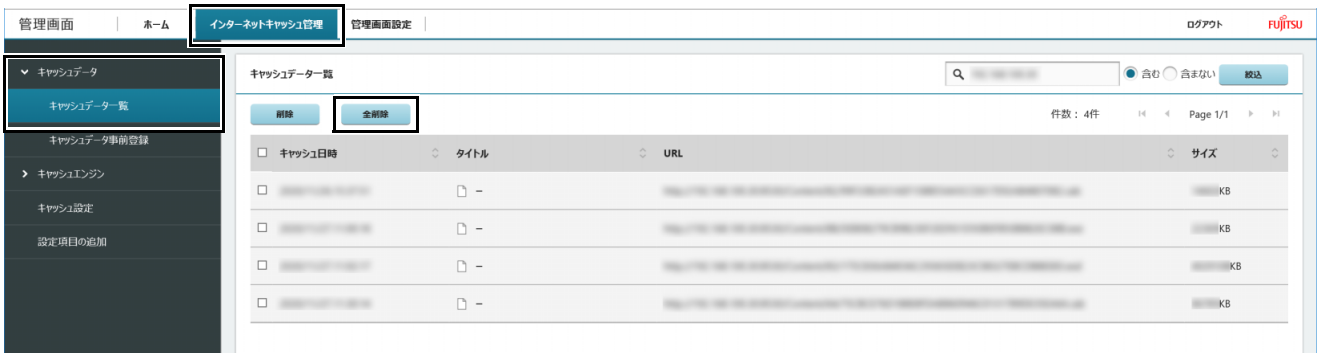
4　ユーザー ID およびパスワードを入力し、「ログイン」をクリックします。
ユーザー ID の初期値は「administrator」です。パスワードは、「パスワードの変更」（→ P.57）で変更した値を入力してください。



管理画面が表示されます。

5　管理画面でキャッシュー覧のデータをすべて削除します。

「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」-「全削除」をクリックします。



6　管理画面を表示し、キャッシュエンジンを停止します。

「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停止」-「停止」をクリックします。

7　次のフォルダーに「証明書の作成（エッジコンピューティングデバイス用）」（→ P.77）、「証明書の作成（業務端末 / マスター端末用）」（→ P.79）で作成した証明書を上書きコピーします。

C:¥cygwin64¥squid¥etc¥ssl_cert

POINT

- 新規インストールの場合でも、上記フォルダーにmyCA.pem、myCA.derがあります。作成した証明書を上書きをコピーしてください。
- 作成した証明書は次のフォルダーにあります。
  C:¥cygwin64¥bin¥myCA.pem（エッジコンピューティングデバイス用証明書）
  C:¥cygwin64¥bin¥myCA.der（業務端末/マスター端末用証明書）

8　データベースの初期化をします。

1. 「C:¥cygwin64¥squid¥var¥lib¥ssl_db」フォルダーを削除します。
2. 「C:¥cygwin64¥squidcontroller¥initdb¥ssl_db」フォルダーを「C:¥cygwin64¥squid¥var¥lib」フォルダーにコピーします。

9　管理画面を表示し、キャッシュエンジンを起動します。

「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」-「起動」をクリックします。

10　本製品を再起動します。

以上で、エッジコンピューティングデバイスへの証明書のインストールは終了です。

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、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。

・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 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/

▶ポート番号変更ツールを実行した場合は、URLのポート番号「10080」を「10090」または変更したポート番号に置き換えてアクセスしてください。

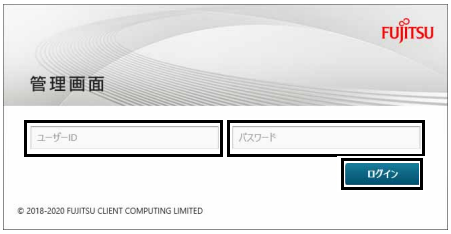
▶Internet Explorer で管理画面を表示したときに入力フォームが表示されない場合は、次の設定をご確認ください。

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。

4 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.57）で変更した値を入力してください。



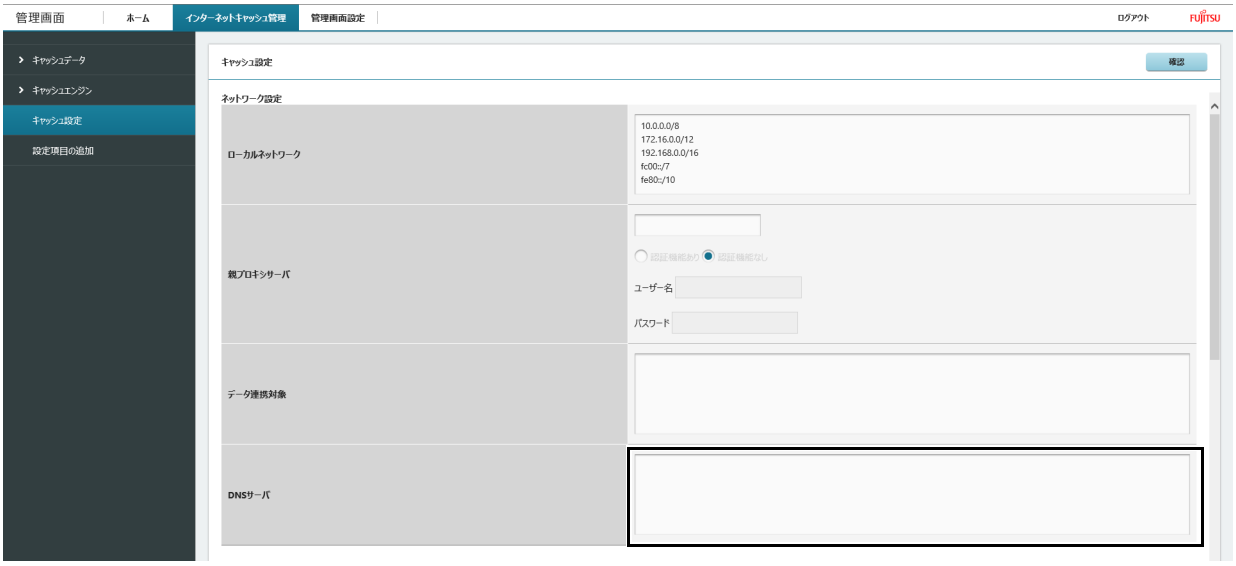
管理画面が表示されます。

5「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。

6 ネットワーク設定の「DNS サーバ」を設定します。

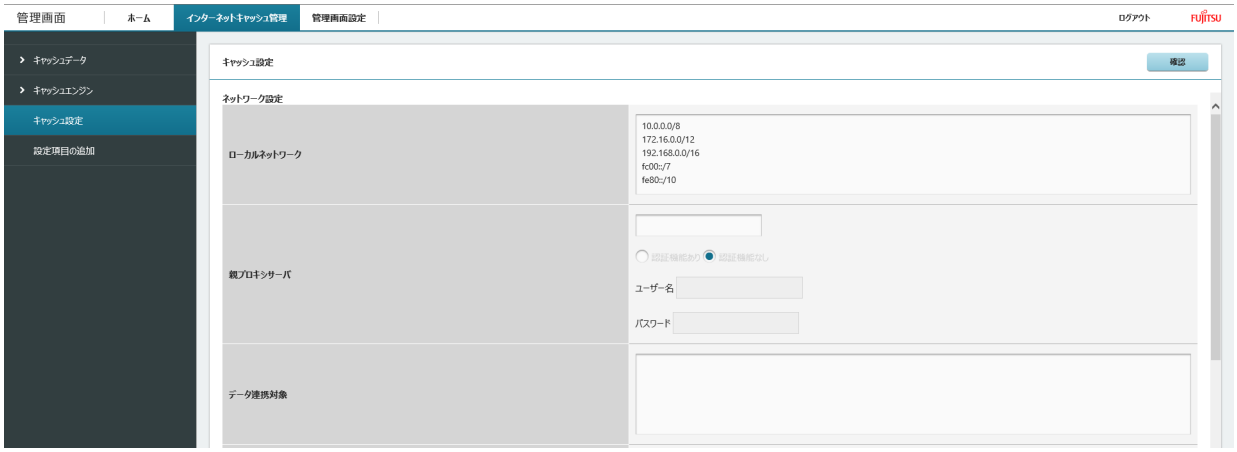
DNS サーバーを設定しないと、インターネットの閲覧ができません。必ず連携する DNS サーバーを設定してください。



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

7「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 ※ 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
	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。
	認証機能なし	親プロキシサーバー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。
	ユーザー名	「認証機能あり」の場合、ユーザー名を入力してください。
	パスワード	「認証機能あり」の場合、パスワードを入力してください。
データ連携対象	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

8 キャッシュ制御に関する項目を設定します。

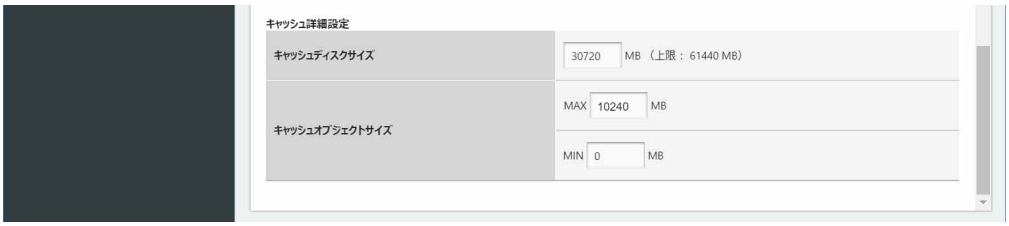
各項目については、次の表をご覧ください。

項目		説明
キャッシュ制御		
キャッシュ対象プロトコル	http/https	http/https プロトコルをキャッシュ対象にします。
	http	http プロトコルをキャッシュ対象にします。https プロトコルはキャッシュしません。
コンテンツの有効期限	サーバの設定に従う	本製品にキャッシュされたコンテンツの配信元サーバーによってコンテンツの有効期限が設定されている場合、その有効期限にしたがってキャッシュコンテンツを使用します。 しかし、配信元サーバーによってコンテンツの有効期限が設定されていない場合は、「7 ～ 30 日間」を選択した場合と同じ動きをします。 ※ 初期値は「サーバの設定に従う」が選択されています。通常はこちらの設定で問題ありません。
	7~30 日間	キャッシュコンテンツの配信元サーバーによって設定された有効期限は無効となり、キャッシュ期間に応じて使用されるコンテンツが異なります。 キャッシュコンテンツの配信元サーバーの有効期限が短いことがわかっている場合は、「7 ～ 30 日間」を選択してください。 ・ キャッシュ後 7 日経過前 本製品にキャッシュされたコンテンツを使用します。 ・ キャッシュ後 7 日経過後～キャッシュ後 30 日経過前 「キャッシュしてからの経過時間」÷「配信元サーバーでのコンテンツ作成または変更からの経過時間」が 90% より小さい場合、本製品にキャッシュしたコンテンツを使用します。 90% より大きい場合、配信元サーバーにコンテンツの更新を確認して更新されていれば、コンテンツをキャッシュしなおします。 ・ キャッシュ後 30 日経過後 配信元サーバーにコンテンツの更新を確認します。更新されている場合は、コンテンツをキャッシュしなおします。
キャッシュ保存期間	WindowsUpdate 関連データのキャッシュ有効期限を日単位で指定できます。この設定の対象となるのは、拡張子が cab、esd、exe、dat のファイルです。 アクセスの対象が有効期限内のファイルの場合、キャッシュしたファイルを使用します。 アクセスの対象が有効期限を超過したファイルの場合、配信元サーバーにファイルの更新を確認して更新されていればキャッシュしなおします。 キャッシュ保存期間に「0」を指定した場合は、常に配信元サーバーからファイルを取得します。	
	上限値	90
	下限値	0
	デフォルト設定	90
X-Forwarded-For	使用する	親プロキシサーバー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	親プロキシサーバー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。

項目		説明
ホワイトリスト / ブラックリスト	ホワイトリスト[注 1]	・ WSUS サーバーを指定します。 ホワイトリストに WSUS サーバーの URL を設定すると WindowsUpdate に特化した運用をすることができます。 ・ 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。

注 1：ホワイトリストに指定した URL が配信元サーバーでキャッシュできない設定になっている場合はキャッシュできません。

9 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
キャッシュ詳細設定		
キャッシュディスクサイズ		キャッシュエンジンがキャッシュするデータ合計の最大サイズを MB 単位で指定します。設定サイズを超過する場合は、キャッシュする領域が確保できるまで最古のデータから順に削除されます。
	上限値	122880
	下限値	30720
	デフォルト設定	30720
キャッシュオブジェクトサイズ	MAX [注 1]	キャッシュエンジンがキャッシュする 1 データの最大サイズを MB 単位で指定できます。 設定サイズを超過したデータはキャッシュされません。 キャッシュディスクサイズより大きいサイズは指定できません。
	上限値	10240
	下限値	1024
	デフォルト設定	10240
	MIN	キャッシュエンジンがキャッシュする 1 データの最小サイズを MB 単位で指定できます。 設定サイズ未満のデータはキャッシュされません。 キャッシュオブジェクトサイズ（MAX）より大きいサイズは指定できません。
	上限値	5120
	下限値	0
	デフォルト設定	0

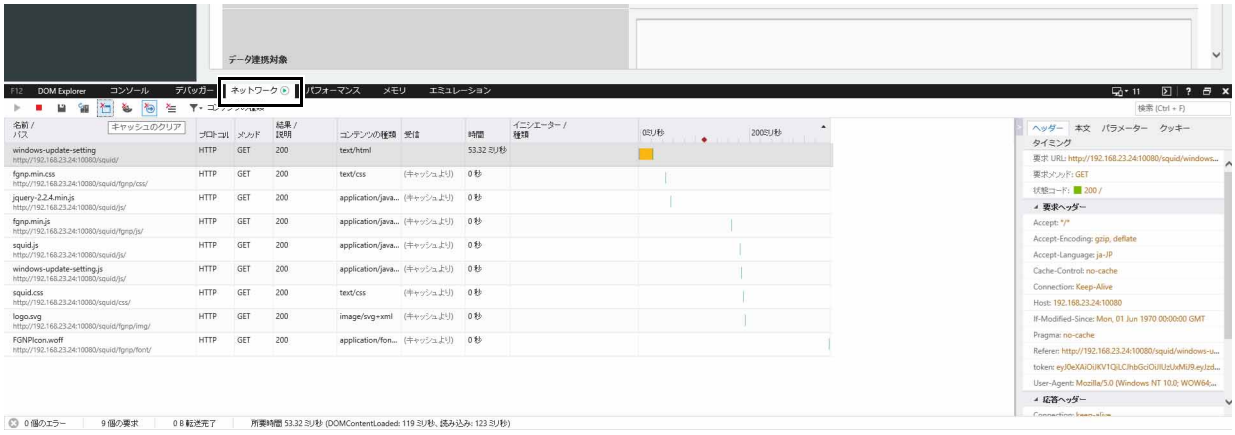
注 1：インターネットキャッシュ機能 V4.2.2 以前のバージョンでは、キャッシュオブジェクトサイズの MAX の上限値が「5120」です。
アプリアップデートパック V1.0.4 以降を適用することで MAX の上限 値、デフォルト値、および設定値が「10240」になります。

10 「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。

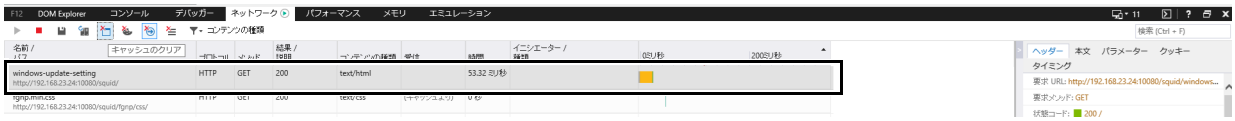
「キャッシュ設定確認」が表示され、変更した設定に「(更新)」と表示されます。

Internet Explorer にて親プロキシサーバーで 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。

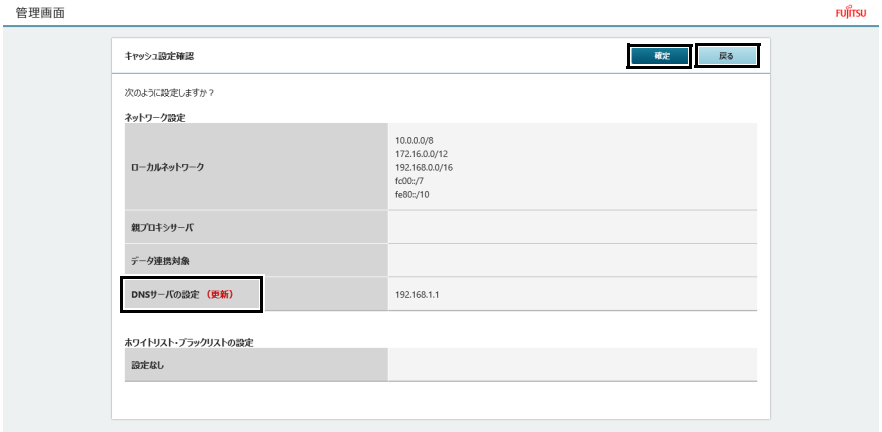
キャッシュのクリアを実施してもこの画面上では残ったままになります。

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。
11. 【F12】キーを押して開発者ツールを閉じます。

11　変更が問題ない場合は、「確定」をクリックします。

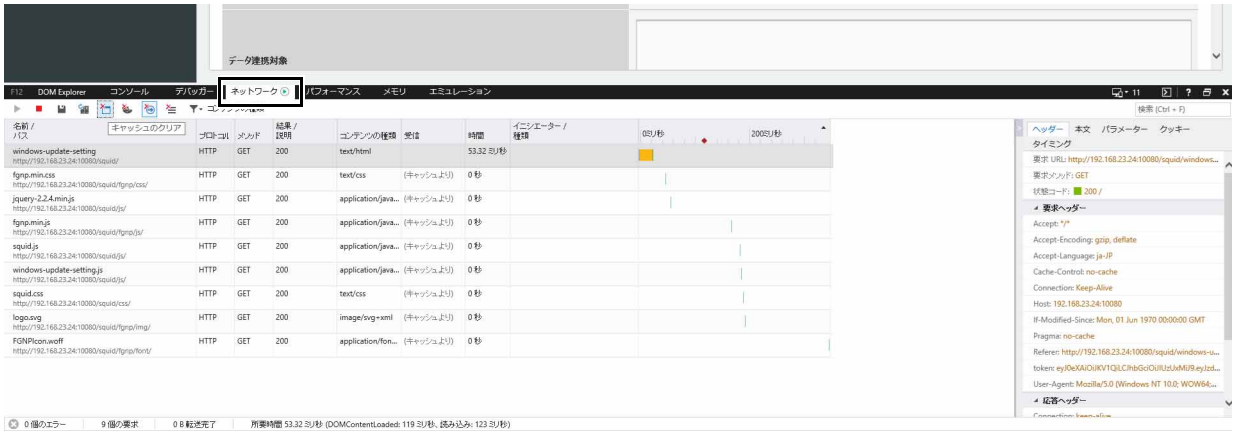
修正が必要な場合は、「戻る」をクリックして設定画面に戻ってください。



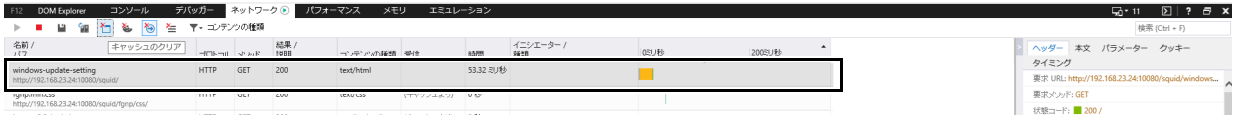
「設定の変更が完了しました。」というメッセージが表示されます。

Internet Explorer にて「設定の変更が完了しました。」と表示された後、「キャッシュ設定」の設定が変更されない場合は、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。
11. 【F12】キーを押して開発者ツールを閉じます。

インストール補助ツールの実行 （アップデート情報取得モジュール）

重要

▸ 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。

1 「C:¥Fujitsu¥Software¥ インストール補助ツール ¥03. 基本機能（アップデート情報取得モジュール）¥BasicFunction_UpdateCache_Install.cmd」を実行します。

以降は表示された画面に従ってください。バッチファイルが完了したら、本製品を再起動してください。

バッチファイル実行後の再起動が完了したら、「アップデート情報取得モジュールのインストールと設定」（→ P.89）からインストールと設定を進めてください。

アップデート情報取得モジュールのインストールと設定

設定ファイルの変更

マスター端末／業務端末に対し、「イントラネットの Microsoft 更新サービスの場所を指定する設定」（→ P.69）で、「更新を検出するためのイントラネットの更新サービスを更新する」と「イントラネット統計サーバーの設定」の設定で WSUS サーバーを完全修飾ドメイン名 （FQDN）で指定する場合や WSUS サーバーをホスト名で指定する場合、製品本体で次の設定ファイルを変更してください。

●WSUS サーバーを完全修飾ドメイン名 （FQDN）で指定する場合（→ P.89）
- WUServer.conf

●WSUS サーバーをホスト名で指定する場合（→ P.90）
- WUServer.conf
- hosts ファイル

●IP アドレスで指定する場合
設定ファイルを変更する必要はありません。

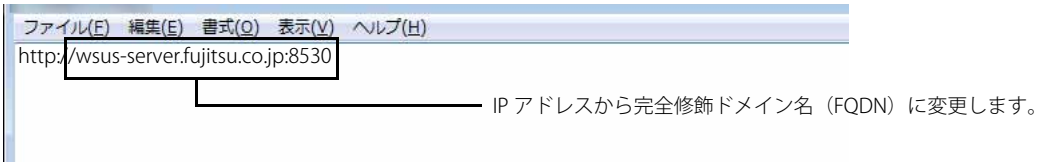
■ WSUS サーバーを完全修飾ドメイン名 （FQDN） で指定する場合

□ **WUServer.conf**

1 次のファイルを設定ファイルをテキストエティターで開きます。
C:¥cygwin64¥cacheUI¥setup¥WUServer.conf」

2 IP アドレスの記載を完全修飾ドメイン名 （FQDN）に変更します。

例：WSUS サーバーのポート番号が「8530」、
　　WSUS サーバーの完全修飾ドメイン名 （FQDN）が「wsus-server.fujitsu.co.jp」の場合、次のように変更します。



3　変更後、保存してファイルを閉じます。

□ **本製品の再起動**

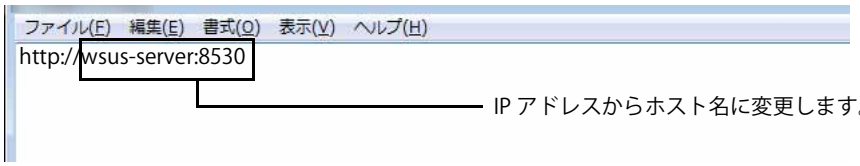
1 設定ファイルを変更後、本製品を再起動します。

■ WSUS サーバーをホスト名で指定する場合

□ WUServer.conf

1 次のファイルを設定ファイルをテキストエディターで開きます。
C:¥cygwin64¥cacheUI¥setup¥WUServer.conf

2 IP アドレスの記載をホスト名に変更します。
例：WSUS サーバーのポート番号が「8530」、
WSUS サーバーのホスト名が「wsus-server」の場合、次のように変更します。



3 変更後、保存してファイルを閉じます。

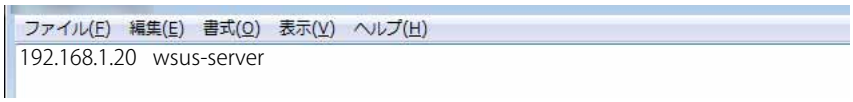
□ hosts ファイルの変更

本製品の hosts ファイルを変更し、IP アドレスと WSUS サーバーのホスト名を記入します。

POINT
▸「C:¥cygwin64¥etc」にあるhostsファイルを直接開いて編集するとWSUSサーバーにアクセスできない場合があります。hostsファイルを編集する場合は、テキストエディターで新しいファイルを作成して、名前を付けて上書き保存してください。

1 テキストエディターを起動して、新しいファイルを作成します。

2 ホスト名と IP アドレスを記入します。
例：WSUS サーバーの IP アドレスが「192.168.1.20」
WSUS サーバーのホスト名が「wsus-server」の場合、次のように記入します。
※IP アドレスとホスト名の間に 1 文字分のスペース（空白）を記入してください。また、必ず改行してください。



3「C:¥cygwin64¥etc」フォルダーにある「hosts」ファイルを上書き保存します。

POINT
▸メモ帳でファイルを編集する場合は、「ファイル」→「名前を付けて保存」を選択し、文字コードを「ANSI」に設定して保存してください。

□ 本製品の再起動

1 設定ファイルを変更後、本製品を再起動します。

WSUS の設定

■ 本製品導入後に WSUS サーバーを変更した場合の設定

本製品導入後に使用する WSUS サーバーを変更した場合、次の手順でバッチファイルを実行する必要があります。
※WSUS サーバーの IP アドレスに変更しない場合でも、WSUS サーバーを変更して再構成を実施したときは、バッチファイルを実行する必要があります。
なお、本製品導入時にこのバッチファイルを実行するを行う必要はありません。

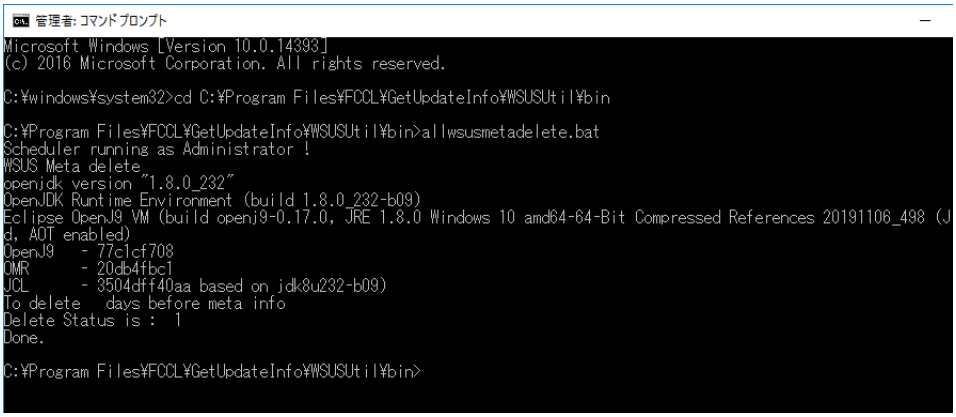
POINT

- WSUSサーバー変更時は、別マニュアル『設定項目確認一覧表』の「アップデート情報取得モジュール」-「WSUSサーバー変更時」の項目で「○」になっているファイルの変更が必要です。

1 **管理者権限でコマンドプロンプトを起動します（→ P.6）。**

2 **次のコマンドを入力して【Enter】キーを押します。**
cd C:¥Fujitsu¥Software¥GetUpdateInfo¥WSUSUtil¥bin

3 **次のコマンドを入力して【Enter】キーを押します。**
allwsusmetadelete.bat



4 **コマンドプロンプトを終了します。**

4. 基本機能 - データキャッシュ機能　（業務端末／マスター端末）

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.58）で完了しています。

証明書のインストール（業務端末／マスター端末用）

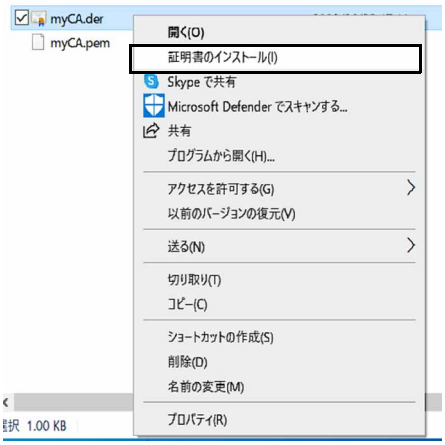
管理画面で「キャッシュ設定」の「キャッシュ対象プロトコル」を「http」に設定する場合は、証明書のインストールは不要です（→ P.84）。

重要

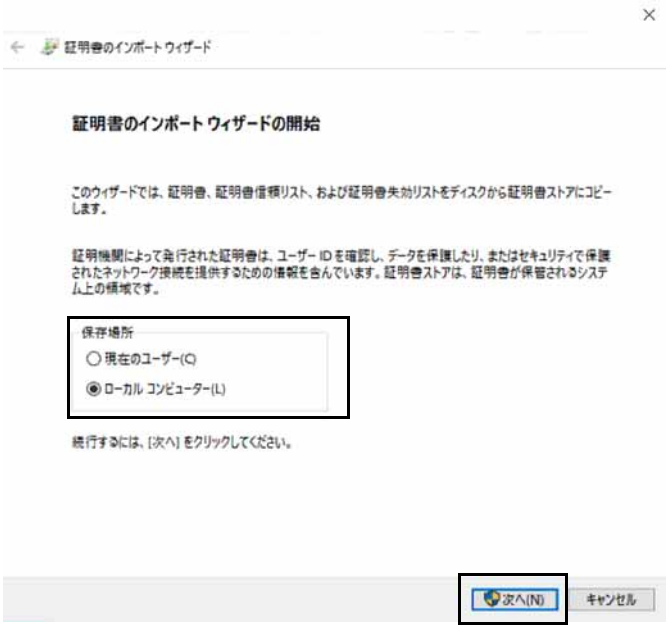
- Windows以外の端末への証明書のインストール方法は、ご使用の端末のマニュアルをご参照ください。
- エッジコンピューティングデバイスを複数台導入してhttpsプロトコルをキャッシュする場合は、すべてのエッジコンピューティングデバイス共通の証明書ファイル（myCA.pem、myCA.der）をご利用ください。共通の証明書ファイルをご利用するには、最初に作成した証明書ファイル（myCA.pem、myCA.der）を他のエッジコンピューティングデバイスにコピーして、「証明書のインストール（エッジコンピューティングデバイス用）」（→P.79）の手順に従ってインストールしてください。
  端末についても共通の証明書ファイル（myCA.der）を「証明書のインストール（業務端末／マスター端末用）」（→P.92）に従ってインストールしてください。共通の証明書を利用しない場合、正しくキャッシュデータが作成/利用できません。

1 エッジコンピューティングデバイスの「C:¥cygwin64¥squid¥etc¥ssl_cert」フォルダーをタブレット端末の任意のフォルダーにコピーします。

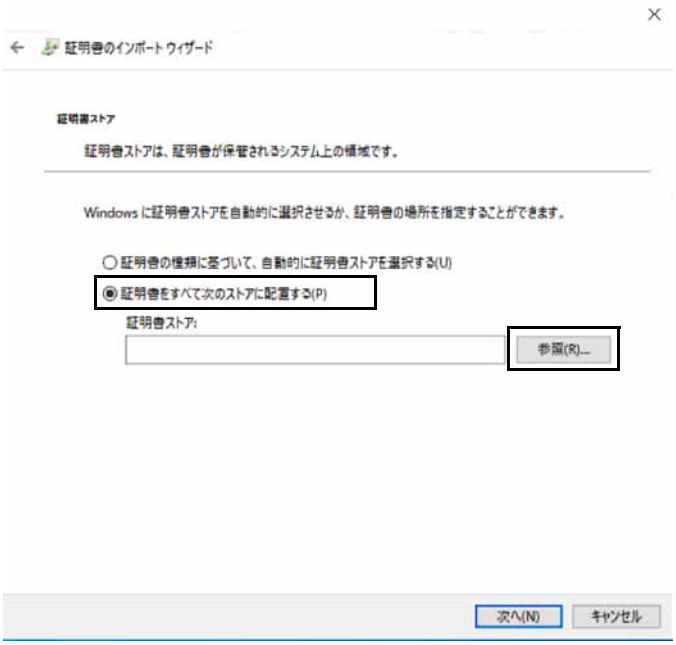
2 コピーした証明書ファイル「myCA.der」を右クリックし、「証明書のインストール」を選択します。



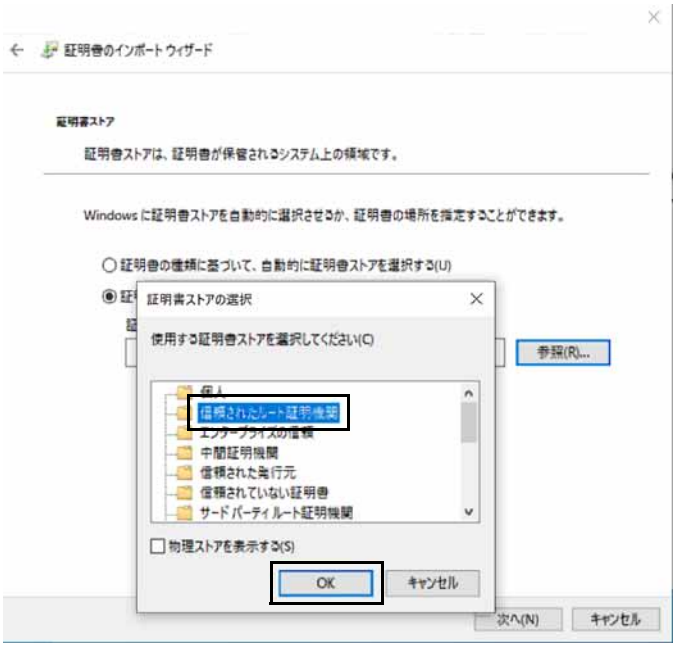
3 保存場所を「現在のユーザー」か「ローカルコンピュータ」を選択し、「次へ」をクリックします。



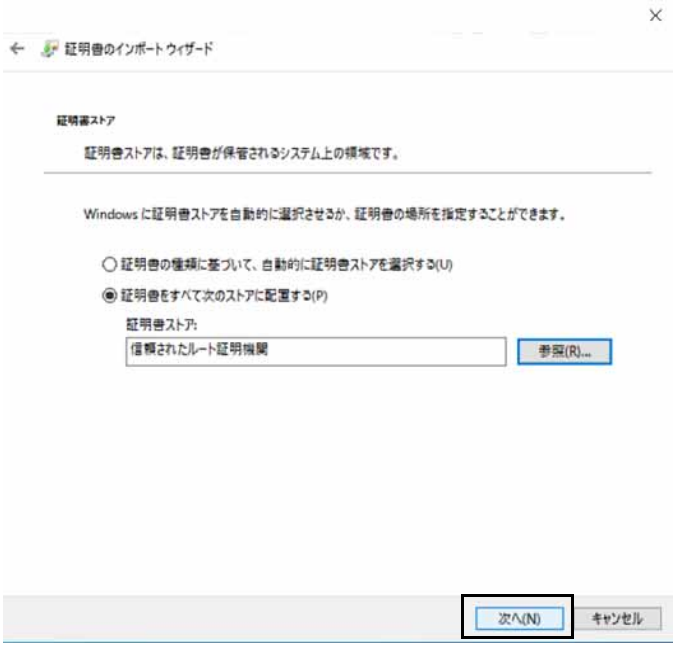
4「証明書をすべての次のストアに配置する」にチェックをして「参照」をクリックします。



5「信頼されたルート証明機関」を選択して「OK」をクリックします。

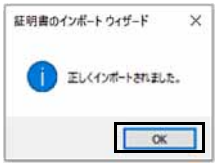


6「次へ」をクリックします。



7「完了」をクリックします。

8「OK」をクリックします。



5. 基本機能 - 状態監視 （製品本体）

動作状態監視ツールのインストールと設定

インストール補助ツールの実行（動作状態監視ツール）

重要

- 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。

1 「C:¥Fujitsu¥Software¥ インストール補助ツール ¥04. 基本機能（動作状態監視ツール）¥BasicFunction_WatchProcessApp_Install.cmd」を実行します。

以降は表示された画面に従ってください。バッチファイルが完了したら、本製品を再起動してください。

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。

お手入れナビ / RAS Utility 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 / RAS Utility」のヘルプをご覧ください。

POINT

- 「お手入れナビ / RAS Utility」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 / RAS Utility」→「ヘルプ」の順にクリックします。

6. 基本機能 - WindowsUpdate 運用最適化モデル 運用管理ツール

重要

▶マスター端末／業務端末を設定する場合、次の点に注意してください。
・複数のアカウントが作成されている端末に設定する場合は、すべてのアカウントに対して設定が必要となります。
・運用管理ツール クライアントをインストールするときは、管理者権限のあるローカルユーザーアカウントが 必要です。
また、管理者権限のあるローカルユーザーアカウントには、必ずパスワードを付けてください。

運用管理ツールのインストールと設定

サーバー、エッジコンピューティングデバイス、マスター端末、管理者端末に WindowsUpdate 運用最適化モデル 運用管理ツールをインストールおよび設定します。詳しくは、『WindowsUpdate 運用最適化モデル 運用管理ツール セットアップガイド』をご覧ください。

7. アプリアップデートパック V1.0.4 （製品本体）

POINT

▶「アプリアップデートパックV1.0.2」と「アプリアップデートパックV1.0.3」は、「アプリアップデートパックV1.0.4」に含まれるため、インストールする必要はありません。

アプリアップデートパック V1.0.4 のコピーと解凍

アプリアップデートパック V1.0.4 は、本製品に添付されておりません。「アプリアップデートパックとポート番号変更ツールのダウンロード」（→ P.23）をご覧になり、ダウンロードしてください。

1 ダウンロードした「アプリアップデートパック V1.0.4」（exe ファイル）を本製品の任意のフォルダーにコピーします。

2 exe ファイルを実行します。

「ApPkV104」フォルダー内にアプリアップデートパック V1.0.4 が解凍されます。

アプリアップデートパック V1.0.4 のインストール

ここでは、アプリアップデートパック V1.0.4 を「C:¥」に解凍した場合を例に説明します。

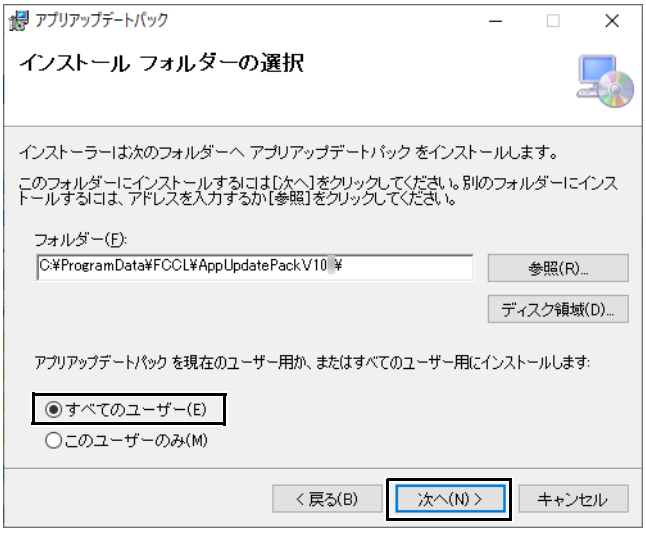
1 「C:¥ApPkV104¥AppUpdatePack.msi」を実行します。

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。

インストール先フォルダーの入力画面が表示されます。

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。

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」クリックします。

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。

5 「閉じる」をクリックします。

6 コマンドプロンプトに次のメッセージが表示されるまで待ちます。

アプリアップデートパックによる以下のアップデートは完了しました。

- インターネットキャッシュ機能
- アップデート情報取得モジュール
- メンテナンス機能

7 次のフォルダにある「version.txt」を開き、「V4.2.3」と表示されることを確認します。

C:¥cygwin64¥cacheUI¥jar

8. ポート番号変更ツールの実行

ポート番号変更ツールの実行　（製品本体）

管理番号で使用するポート番号を変更します。通常は、ポート番号を「10090」に変更してください。

●「ポート番号を 10090 に変更する場合」（→ P.98）
●「ポート番号を 10090 以外に変更する場合」（→ P.99）

ポート番号を 10090 に変更する場合

ここでは、ポート番号変更ツールを「C:¥」に解凍した場合を例に説明します。

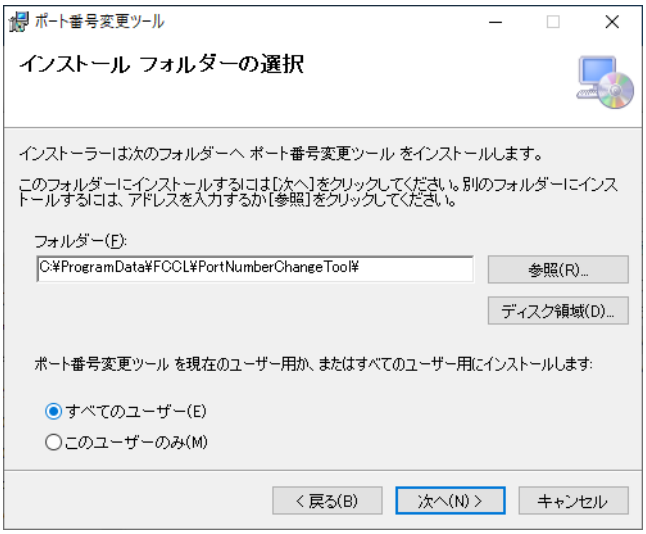
1 「アプリアップデートパックとポート番号変更ツールのダウンロード」（→ P.23）でダウンロードした exe ファイルを本製品の任意のフォルダーにコピーします。

2 exe ファイルを実行します。
「PortNumberChangeTool」フォルダー内にポート番号変更ツールが解凍されます。

3 「C:¥PortNumberChangeTool¥PortNumberChangeToolInstaller.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。

4 「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 「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。

6 「次へ」をクリックします。

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」クリックします。

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。

7 「閉じる」をクリックします。
コマンドプロンプトが消えた後、本製品が再起動されます。

ポート番号を 10090 以外に変更する場合

ここでは、ポート番号変更ツールを「C:¥」に解凍した場合を例に説明します。

1 「アプリアップデートパックとポート番号変更ツールのダウンロード」（→ P.23）でダウンロードした exe ファイルを本製品の任意のフォルダーにコピーします。

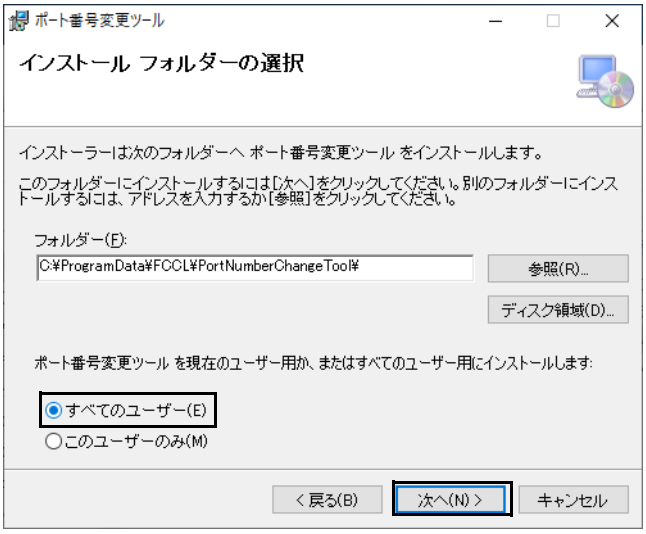
2 exe ファイルを実行します。
「PortNumberChangeTool」フォルダー内にポート番号変更ツールが解凍されます。

3 「C:¥PortNumberChangeTool¥PortNumber.bat」を実行します。
以降、画面の指示に従ってポート番号を入力してください。バッチファイルが完了したら、次の手順に進んでください。

4 「C:¥PortNumberChangeTool¥PortNumberChangeToolInstaller.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。

5 「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。

6 「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。

7 「次へ」をクリックします。

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」クリックします。

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。

8 「閉じる」をクリックします。
コマンドプロンプトが消えた後、本製品が再起動されます。

ポート番号変更ツールで再度ポート番号を変更する場合

ここでは、ポート番号変更ツールを「C:¥」に解凍した場合を例に説明します。

1 「コントロールパネル」を表示します（→ P.6）。
「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。

3 「ポート番号変更ツール」をダブルクリックしてアンインストールします。

4 「ポート番号を 10090 以外に変更する場合」（→ P.99）の手順 3 ～手順 8 を実行します。

ポート番号変更ツールの実行後の設定　（製品本体）

ファイアウォールの設定

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ってください。なお、OS 標準の機能「Windows Defender ファイアウォール」を使用する場合は、ポート番号変更ツールを実行することで設定されるので、ここでの設定は不要です。

■ 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	10090 または、ポート番号変更ツールで指定した番号	-	受信

親プロキシサーバーの設定

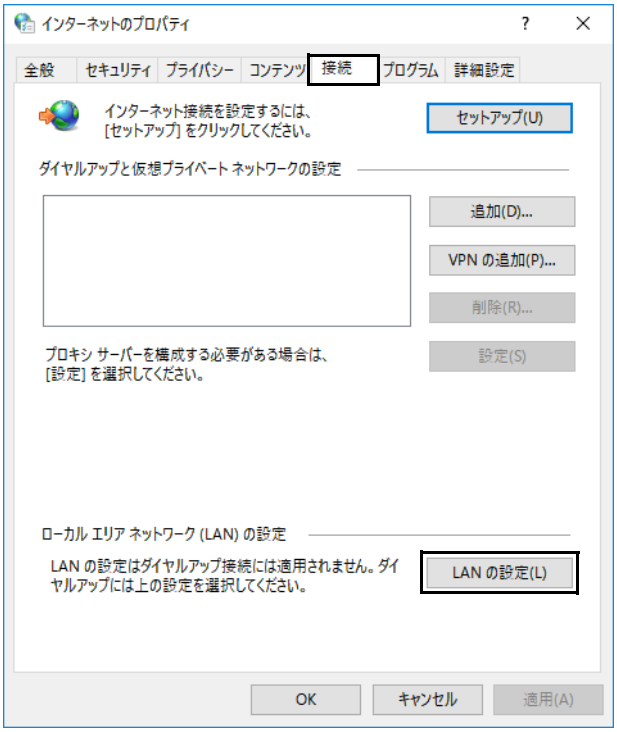
「親プロキシサーバーの設定」（→ P.74）で「例外」を設定した場合は、「例外」の URL のポート番号を変更します。

1「スタート」ボタン→「Windows アクセサリ」の順にクリックします。

2「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。

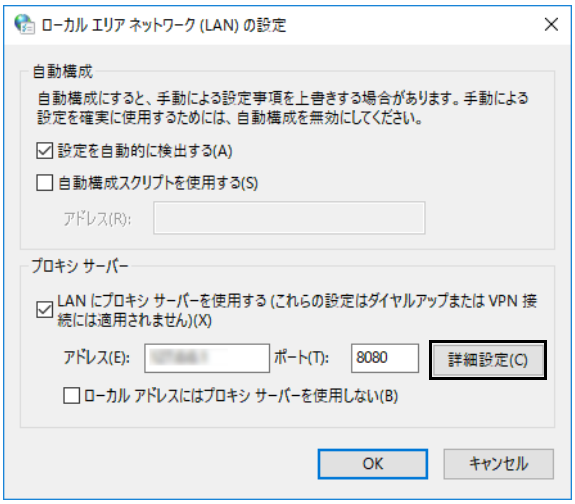
3 Internet Explorer の画面の右上隅の ⚙（ツール）→「インターネット オプション」の順にクリックします。
「インターネットのプロパティ」が表示されます。

4「接続」タブをクリックし、「LAN の設定」をクリックします。



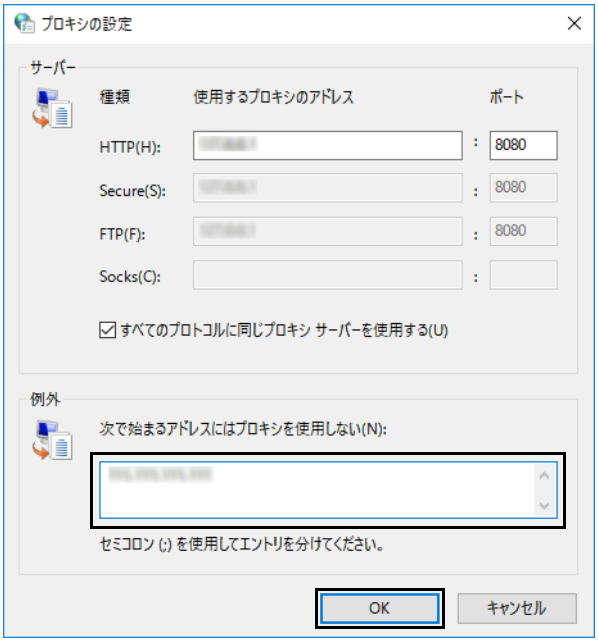
「ローカルエリアネットワーク（LAN）の設定」が表示されます。

5「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。

6「例外」に設定した URL のポート番号「10080」を「10090」またはポート番号変更ツールで指定した番号に変更し、「OK」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。

7「OK」をクリックします。

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

インターネット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」ボタン→「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
cacheCtl
CacheUIService

3 サービスを閉じます。

アップデート情報取得モジュールの確認

1 次のフォルダーが作成されていることを確認します。
C:¥Program Files¥FCCL¥GetUpdateInfo

2 「スタート」ボタン→「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。

3 「タスクスケジューラ ライブラリ」をクリックします。

4 一覧の中に「GetWSUSInfo」があることを確認します。

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」ボタン→「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。

3. 基本機能 - 運用管理ツール

運用管理ツール サーバ

運用管理ツール サーバをインストールしたサーバー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.6）。**
「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 **「運用管理ツール サーバ」が表示され、バージョンが「24.30.10」であることを確認します。**

運用管理ツール 管理コンソール

管理者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.6）。**
「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 **「運用管理ツール 管理コンソール」が表示され、バージョンが「24.30.10」であることを確認します。**

運用管理ツール クライアント

エッジコンピューティングデバイス / マスター端末で次の操作を行います。

1 **タスクトレイの運用管理ツールアイコンを右クリックし、「プロパティを表示する」をクリックします。**

2 **バージョンが「V4 L30」であることを確認します。**

4. アプリアップデートパック

エッジコンピューティングデバイスで次の操作を行います。

インターネットキャッシュ機能更新プログラム

1 **次のフォルダにある「version.txt」を開き、「V4.2.3」と表示されることを確認します。**
C:¥cygwin64¥cacheUI¥jar

5. ポート番号変更ツール

ポート番号変更ツール

エッジコンピューティングデバイス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.6）。**
「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 **「ポート番号変更ツール」が表示され、バージョンが「1.0.0」であることを確認します。**

6. 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、ディスプレイ、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.30）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。**

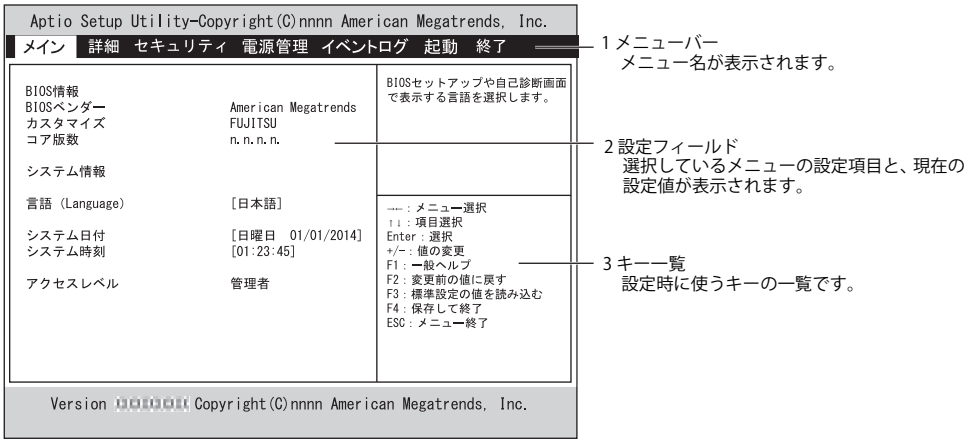
2 **BIOS セットアップ画面が表示されたら、【F2】キーまたは【Delete】キーを離します。**

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.30）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.107）をご覧ください。



1 メニューバー
メニュー名が表示されます。

2 設定フィールド
選択しているメニューの設定項目と、現在の設定値が表示されます。

3 キー一覧
設定時に使うキーの一覧です。

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.30）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。

・BIOS のパスワード機能を使う（→ P.109）
・起動デバイスを変更する（→ P.112）
・セキュリティチップの設定を変更する（→ P.112）
・Wake On LAN を有効にする（→ P.113）
・イベントログを確認する（→ P.114）
・イベントログを消去する（→ P.114）
・ご購入時の設定に戻す（→ P.114）

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.115）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.30）をご覧ください。
2. BIOS セットアップを起動します（→ P.106）。

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.108）

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 〜手順 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.108）

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.30）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.108）
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.136）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.108）

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.30）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.115）	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.116）	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.116）	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.116）	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.122）	イベントログに関する設定を行います。
起動（→ P.122）	起動時の動作について設定します。
終了（→ P.123）	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.112）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.109）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.109）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.109）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.109）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.113）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.114）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.114）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.112）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.114）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.31）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。
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、ディスプレイ、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.129）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.129）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.30）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.114）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.106）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。電源の切り方については、「電源を切る」（→P.30）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 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。

8 「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。

9 「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。

10 「終了」をクリックします。

「終了」ウィンドウが表示されます。

11 「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

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。

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.136）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。

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。

●ディスプレイに関して、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？
・ ディスプレイのブライトネス／コントラストボリュームは、正しく調節されていますか？
・ 複数台のディスプレイを接続している場合、製品本体の電源を入れる前に、ディスプレイ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ディスプレイの電源を入れてください。製品本体の電源を入れた後にディスプレイの電源を入れると、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。

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。

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。

Windows Update 連携のトラブル

マスター端末が「適用中」のまま機能更新プログラムの適用が終わらない

●マスター端末有りの運用で、WindowsUpdate 連携機能を使って機能更新プログラムを実行したときに、マスター端末が「適用中」のまま機能更新プログラムの適用が終わらないことがあります。この場合、
運用管理ツール 管理コンソールからスケジューラ機能の実行ログを確認してください。
確認方法については、『Windows Update 運用最適化モデル 運用管理ツール ユーザーガイド』-「第 4 章 スケジューラ機能の操作」-「実行ログを確認する」をご覧ください。

実行結果が「実行中」の場合は、機能更新プログラムの適用中ですので、お待ちください。
実行結果が「失敗」となっていた場合は、WSUS サーバーで次の設定を確認してください。
・ 機能更新プログラムが承認がされていることを確認してください。
・ 複数の機能更新プログラムを承認していないことを確認してください。
複数の機能更新プログラムを承認していると WindowsUpdate 連携機能が実行されません。

スケジューラ機能でスケジュールを実行したが、設定した時間が来ても実行されない。

●運用管理ツール サーバ機能をインストールしている管理サーバーで、次のサービスが起動してことを確認してください。
・ 運用管理ツール サーバ機能
BzServer2
BzSchServer2
・ SQL サーバー
MSSQL$NEBULA2015DB
SQLBrowser
SQLWriter
SQLAgent$NEBULA2015DB

スケジューラ機能を使って WindowsUpdate 連携を実行後、運用管理ツール 管理コンソールから端末の「MSUpdate 適用状況」-「パッチ一覧」を確認したところ、適用したはずの更新プログラムの一覧が表示されていない

●端末での更新プログラムの適用は成功しているが、運用管理ツールでの更新プログラム適用済みの情報取得に失敗している可能性があります。
端末での更新プログラムの適用状況を確認し、適用されている場合はそのままお使いください。

●端末での更新プログラムの適用に失敗している可能性があります。端末の適用状況を確認し、適用されていない場合は、端末の Windows Update クライアントの情報をクリアして、再度更新プログラムの適用の実行をしてください。
Windows Update クライアントの情報をクリアの詳細情報・手順については Microsoft のホームページをご覧ください。

管理画面のトラブル

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（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 :10090（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
192.168.1.1:10090
と入力します。

●「ステータスランプ」（→ P.8）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。

「An Error occurred.」というエラーメッセージが表示される

●エッジコンピューティングデバイスの起動直後にブラウザーで管理画面を開いてまだソフトウェアの起動処理が完了してない場合に表示されることがあります。
このエラーメッセージが表示された場合は、しばらく待ってから、管理画面を表示し直してください。

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

●「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」ボタン→「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。

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.58）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。

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

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
C:¥cygwin64¥squid¥libexec¥security_file_certgen.exe

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（Chromium 版）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（Windows10、Chrome OS）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。

・ Google Chrome（iPadOS）の場合
1.Google Chrome を起動します。
2.画面下の [...] をタップします。
3.「履歴」→「閲覧履歴データを削除」の順にタップします。
4.「期間」で「全区間」を選択した後、「Cookie、サイトデータ」と「キャッシュされた画像とファイル」にチェックを付けます。
5.「閲覧履歴データを削除」をタップします。

・ Safari（macOS）の場合
1.Safari を起動し、メニューバーの「Safari」→「履歴」メニュー→「履歴を消去」をクリックします。
2.「消去の対象」で「すべて の履歴」選択した後、「履歴を消去」をクリックします。

・ Safari（iPadOS）の場合
1.「設定」→「Safari」の順に選択し、「履歴と Web サイトデータを消去」をタップします。

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。

管理画面のキャッシュ一覧に KB（Microsoft Knowledge Base）番号が表示されない

●アップデート情報取得モジュールはインストール時に設定した時刻に一日一回 WSUS サーバーから KB 番号の情報を取得します。そのため、その時刻以降に WSUS にダウンロードされた更新プログラムの KB 番号は次の日の取得が行われるまで表示されません。

●Windows Update の更新プログラムの中で KB 番号が存在しないものがあります。この場合は、キャッシュ一覧に KB 番号が表示されません。

●エッジコンピューティングデバイスとマスター端末／業務端末の設定で、WSUS サーバー名の指定方法（IP アドレスまたは WSUS サーバー名を完全修飾ドメイン名（FQDN））に差異がある可能性があります。
次の設定を確認してください。差異がある場合は、「WUServer.conf」の設定を変更してください。
・ エッジコンピューティングデバイス
アップデート情報取得モジュール設定ファイル「C:¥cygwin64¥cacheUI¥setup¥WUServer.conf」の設定。
詳しくは、「設定ファイルの変更」（→ P.89）をご覧ください。
・ マスター端末／業務端末
ローカルグループポリシー「コンピューターの構成」-「管理者用テンプレート」-「Windows コンポーネント」-「Windows Update」-「イントラネットの Microsoft 更新サービスの場所を指定する」の「更新を検出するためのイントラネットの更新サービスを更新する」と「イントラネット統計サーバーの設定」の設定値。
詳しくは、「イントラネットの Microsoft 更新サービスの場所を指定する設定」（→ P.69）をご覧ください。

●本製品導入後に使用する WSUS サーバーを変更した場合、次の手順でバッチファイルを実行する必要があります。
WSUS サーバーの IP アドレスに変更しない場合でも、WSUS サーバーを変更して再構成を実施したときは、バッチファイルを実行する必要があります。
1.管理者権限でコマンドプロンプトを起動します（→ P.6）。
2.次のコマンドを入力して【Enter】キーを押します。
cd C:¥Fujitsu¥Software¥GetUpdateInfo¥WSUSUtil¥bin
3.次のコマンドを入力して【Enter】キーを押します。
allwsusmetadelete.bat

WindowsUpdate のキャッシュが作られない

●マスター端末および、WindowsUpdate を最初に適用する業務端末の配信の最適化が ON になっている可能性が有ります。配信の最適化は OFF にしてください。

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.81）。

ブラウザーで https のサイトを表示すると証明書のエラーメッセージが表示される

●ブラウザで https のページを開くと次のようなページが表示されるされる場合があります。
「接続がプライベートではありません」
「接続はプライベートではありません」
「この接続ではプライバシーが保護されません」
「このサイトは安全ではありません」

・ 証明書がインストールされていない可能性があります。
エッジコンピューティングデバイスと端末に証明書をインストールする必要があります。
証明書の作成とインストール方法については、「証明書の作成とインストール」（→ P.77）をご覧ください。

・ 証明書が期限切れの可能性があります。
証明書の有効期間をご確認してください。有効期間を過ぎている場合、証明書を新しく作り直して、再度、エッジコンピューティングデバイスと端末にインストールする必要があります。
証明書の作成とインストール方法については、「証明書の作成とインストール」（→ P.77）をご覧ください。

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

●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。

●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。
・ 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。
・ 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 セットアップメニュー 一覧』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。

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」（https://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	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	本製品に添付の「添付ソフトウェアサポート書」をご覧ください。

8

第 8 章
付録

1. 仕様

ESPRIMO Edge Computing Edition Z0111/W

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 8GB （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 256GB
セキュリティ機能			
	セキュリティチップ（TPM）注 6		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 7
	シリアル注 8		非同期 RS-232C 準拠 D-SUB 9 ピン ×1（16550A 互換）
	USB 注 9		USB3.0 準拠 ×4（前面 ×2、背面 ×2）注 10
	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 11
サポート OS			Windows 10 IoT Enterprise 2019 LTSC

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.142）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 ：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 7 ：標準添付品のケーブル（DP-HDMI 変換ケーブル）使用時
注 8 ：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 9 ：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 10 ：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 11 ：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.136）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、防災 Wi-Fi 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 5.8W
	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。

●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 2004 以降、および、Windows 11 で実施しております。

●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 、Windows 11、iPadOS、macOS、Chrome OS です。 ・対象ブラウザは次の通りです。 ・- Windows 10 対象ブラウザー：Internet Explorer 11、Microsoft Edge（Chromium 版）、Google Chrome ・- Windows 11 対象ブラウザー：Microsoft Edge（Chromium 版）、Google Chrome - iPadOS 対象ブラウザー：Safari、Google Chrome - macOS 対象ブラウザー：Safari - Chrome OS 対象ブラウザー：Google Chrome ・画面解像度は 1366 x 768 以上でお使いください。

名称	動作環境と注意事項
インターネットキャッシュ機能	・対象 OS は Windows 10 、Windows 11、iPadOS、macOS、Chrome OS です。 インターネットキャッシュ機能 V4.2.2 以前のバージョンの場合、Windows 11 で Windows Update を実行するとキャッシュ時にエラーが発生する可能性があります。Windows 11 をご利用時は、アプリアップデートパック V1.0.4 以降のバージョンを適用してインターネットキャッシュ機能 V4.2.3 以降のバージョンにアップデートしてください。 ・対象ブラウザは次の通りです。 - Windows 10 対象ブラウザー：Internet Explorer 11、Microsoft Edge（Chromium 版）、Google Chrome - Windows 11 対象ブラウザー：Microsoft Edge（Chromium 版）、Google Chrome - iPadOS 対象ブラウザー：Safari、Google Chrome - macOS 対象ブラウザー：Safari - Chrome OS 対象ブラウザー：Google Chrome 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 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。 ・エッジコンピューティングデバイスを複数台導入して https プロトコルをキャッシュしたい場合は、全数共通の証明書ファイル（myCA.pem、myCA.der）をご利用ください。共通の証明書ファイルをご利用するには、最初に作成した証明書ファイル２つ（myCA.pem、myCA.der）を他のエッジコンピューティングデバイスにコピーし、『導入ガイド』の「証明書のインストール（エッジコンピューティングデバイス）」に従ってインストールしてください。端末についても共通の証明書ファイル（myCA.der）を、『導入ガイド』の「証明書のインストール」に従ってインストールしてください。共通の証明書を利用しない場合、正しくキャッシュデータが作成 / 利用できません。 ・インターネットキャッシュ機能で使用する証明書の有効期限が切れたときに本製品およびクライアント端末の証明書を入れ替える必要があります。本製品の証明書を入れ替えの際は、キャッシュしていたコンテンツの全削除と再起動をする必要があります。新しい証明書の本製品へのインストール、キャッシュデータの全削除後、本製品を再起動をしてください。 ・キャッシュログ収集ツールについて インターネットキャッシュ機能のアクセスログは最大過去 10 日分まで保存されます。その場合、キャッシュログ収集ツールで解析できるのは最大 10 日分までとなります。キャッシュデーター覧画面で「全削除」ボタンでデータの削除を行うと過去のアクセスログは削除されます。その場合、キャッシュログ収集ツールでの解析はできません。 ・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 10GB 以下のデータをキャッシュすることができます。 インターネットキャッシュ機能 V4.2.2 以前のバージョンでは、1 ファイル 5GB 以下のデータまでのキャッシュとなります。 ・キャッシュディスクサイズ（キャッシュエンジンがキャッシュするデータ合計の最大サイズ）の上限値は「122880」MB になります。 ・Windows Update の更新プログラムをキャッシュするには、お客様にて Windows Server Update Services（WSUS）サーバーを用意していただく必要があります。 ・Windows Server Update Services（WSUS）サーバーの OS は Windows Server 2012 R2 および Windows Server 2019 で動作確認しています。その他の場合は、お客様にて事前に検証を実施した上でお使いください。 ・Office の更新プログラムでキャッシュできるのは Microsoft インストーラー（MSI）でインストールされた Microsoft Office 2016 です。 ・Microsoft System Center Configuration Manager（SCCM）からの Windows Update の更新プログラムのキャッシュはサポートしていません。 ・マスター端末［注］/ 業務端末においては、配信の最適化は OFF にしてご使用ください。配信の最適化を OFF にしないと、キャッシュデータが作成されない場合があります。 ・管理画面を表示する端末は OS の設定や pac ファイルで本製品のコンピュータ部分の IP アドレスアクセス時に本製品がプロキシにならないよう、対象外の設定をしてください。 ただし、iPadOS では OS の設定でプロキシ対象外の設定ができないため pac ファイル運用を推奨いたします。pac ファイル運用をされない場合は、管理画面を表示する際、プロキシ設定を一時的に OFF にしてください。 ・This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. （http://www.openssl.org/） This product includes cryptographic software written by Eric Young（eay@cryptsoft.com） ・本製品利用の際にもインラインフレーム (<iframe>) を多く使用しているような重たい Web ページ（例. 広告が多いページなど）にアクセスした際、ブラウザ上で Web ページの表示が完了しない（広告表示欄が空白になるなど）ことがあります。その場合は、ブラウザでリロードを行い、読み込みなおしてください。 注　マスター端末：Windows Update を最初に適用する端末
アップデート情報取得モジュール	・一日に一回Windows Server Update Services（WSUS）サーバーからWindows Updateの更新プログラムのMicrosoft Knowledge Base(KB) 番号の情報を取得します。その時刻にエッジコンピューティングデバイスを起動しておく必要があります。取得時刻は変更可能です。 ・Windows Server Update Services（WSUS）サーバーの OS は Windows Server 2012 R2 および Windows Server 2019 で動作確認しています。その他の場合はお客様にて事前に検証を実施した上でお使いください。 ・業務端末 / マスター端末の設定で、「イントラネットの Microsoft 更新サービスの場所を指定する設定」において、WSUS サーバーの指定方法を完全修飾ドメイン名 (FQDN) を指定した場合、本製品が名前解決できるように、本製品をネットワーク上に配置してください（本製品をドメイン参加させる等）。

名称	動作環境と注意事項
Windows Update 運用最適化モデル 運用管理ツール	・本ツールのクライアント機能は 5 台までインストール可能です。但しエッジコンピューティングデバイスへのインストールが必須のため、その他の端末に関しては 4 台までインストール可能です。 ・WindowsUpdate 連携機能実行の際は、マスター端末[注]を用意することを推奨します。ご用意いただけない場合は、WSUS サーバーにて更新プログラムが公開承認されてから、本製品に更新プログラムのキャッシュ作成が完了するまで、他の端末の更新プログラムのダウンロード処理は保留される場合がありますのでご注意ください。 ・キャッシュから更新プログラムをダウンロードするためには、マスター端末[注]と他の端末の OS のバージョンが同じである必要があります。 OS バージョンが異なる場合には、マスター端末[注]で作成されたキャッシュは使われず、新たにキャッシュが作成されます。 ・機種固有の更新プログラム（ドライバ、ツールなど）の場合は、キャッシュが利用されない場合があります。 ・セキュリティの観点から、マスター端末やエッジコンピューティングデバイスに運用管理ツール 管理コンソール機能をインストールしないでください。 ・ エッジコンピューティングデバイスにクライアント機能をインストール後は、「運用管理ツール /AP 部 連携用パスワード設定ツール」を必ず実行してください。 ・クライアント機能をアンインストール、再インストールした場合は、再度「運用管理ツール /AP 部 連携用パスワード設定ツール」を実行してください。 ・「運用管理ツール /AP 部 連携用パスワード設定ツール」にてアクセスポイント部分とパスワード連携後、再びアクセスポイント部の admin ユーザーのパスワードを変更した場合は、再度「運用管理ツール /AP 部 連携用パスワード設定ツール」を実行する必要があります。 ・動作検証は下記環境にて実施しています。 -『運用管理ツール サーバー機能』 Windows Server 2012、Windows Server 2012 R2、Windows Server 2016、Windows Server 2019、Windows Server 2022 -『運用管理ツール 管理コンソール機能』 Windows 8.1、Windows 8.1 with Bing、Windows 8.1 Pro、Windows 8.1 Enterprise、 Windows 10 Pro、Windows 10 Pro Education、Windows 10 Enterprise、Windows 10 Education、 Windows 10 Enterprise LTSB 2016、 Windows 10 Enterprise LTSC 2019、Windows 10 Enterprise LTSC 2021、 Windows 11 Pro、Windows 11 Pro Education、Windows 11 Pro for Workstations、 Windows 11 Enterprise、Windows 11 Education、 Windows Server 2012、Windows Server 2012 R2、Windows Server 2016、Windows Server 2019、Windows Server 2022 -『運用管理ツール クライアント機能』 Windows 8.1、Windows 8.1 with Bing、Windows 8.1 Pro、Windows 8.1 Enterprise、 Windows 10 Pro、Windows 10 Pro Education、Windows 10 Enterprise、Windows 10 Education、 Windows 10 Enterprise LTSB 2016、 Windows 10 IoT Enterprise 2016 LTSB、Windows 10 Enterprise LTSC 2019、 Windows 10 IoT Enterprise 2019 LTSC、Windows 10 Enterprise LTSC 2021、 Windows 11 Pro、Windows 11 Pro Education、Windows 11 Pro for Workstations、 Windows 11 Enterprise、Windows 11 Education ・クライアント機能を使用する際のネットワーク環境条件は、以下のとおりです - 有線 LAN 環境 100Mbps 以上（1Gbps 以上を推奨） - 無線 LAN 環境 11n （300Mbps 以上） 11ac（6.9Gbps）（推奨） - リモート画面操作機能使用時 1 台あたりの実効速度に、1Mbps 以上（推奨 5Mbps 以上）が必要です。 ・詳細動作環境は「Windows Update 運用最適化モデル 運用管理ツール セットアップガイド」-「付録 E 動作環境」をご参照ください。 注　マスター端末：Windows Update を最初に適用する端末
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 / RAS Utility	―

使用するポート

アプリ名称	ポート番号
管理画面	ポート番号変更ツール実行前：10080 ポート番号変更ツール実行後：10090、またはポート番号変更ツールで変更したポート番号
インターネットキャッシュ機能	8080、3130、443、8000
メンテナンス機能	9200、9300、18080、18081、18090、18091、18092、18093、18094、9600
運用管理ツール	運用管理ツールの使用ポート番号については『Windows Update 運用最適化モデル 運用管理ツール セットアップガイド』の「付録 F ご利用に関しての制限事項 / 留意事項について（重要）」-「3.1 ネットワーク環境に関する留意事項」-「(3) 利用するポート番号」をご覧ください。

i-FILTER を導入している場合の留意事項について

市販の i-FILTER を「認証あり」の親プロキシサーバーとして使用する場合、オンプレミス版 i-FILTER にて共通のユーザー名・パスワードを使用する方式のみ連携できます。本製品で「管理画面」-「インターネットキャッシュ管理」-「キャッシュ設定」-「親プロキシサーバ」の設定項目で、「認証機能あり」を選択し、i-FILTER で使用する共通のユーザー名とパスワードを設定してください。
各端末のブラウザでユーザー名・パスワードを入力する方式や、クラウド版の常駐アプリ DigitalArts@Cloud Agent で認証する方式については連携できません。端末のプロキシ設定を自動構成スクリプト（PAC）で設定し、PAC ファイルにて、WSUS サーバーや本製品にキャッシュさせる WEB サイトなどへのアクセスのみ本製品経由、それ以外のアクセスは i-FILTER を経由するよう設定をお願いいたします。

アクセスポイント部分の留意事項について

●グローバル IP アドレスには対応していません。入力すると「マスクエラー」が表示されます。IP アドレスには、プライベート IP アドレスを入力してください。プライベート IP アドレスとは、組織内のネットワーク（プライベートネットワーク）でのみ使用できる IP アドレスです。プライベート IP アドレスの範囲は次のとおりです。

クラス	範囲	サブネットマスク	アドレス数
クラス A	10.0.0.0 ～ 10.255.255.255	255.0.0.0	16,777,216（16,777,216×1 サブネット）
クラス B×16	172.16.0.0 ～ 172.31.255.255	255.240.0.0	1,048,576（65,536×16 サブネット）
クラス C×256	192.168.0.0 ～ 192.168.255.255	255.255.0.0	65,536（256×256 サブネット）

●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。

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。
  - 管理画面
  - インターネットキャッシュ機能
  - お手入れナビ / RAS Utility

WindowsUpdate 運用最適化モデル 運用管理ツール

『WindowsUpdate 運用最適化モデル 運用管理ツール セットアップガイド』をご覧になり、アンインストールを行ってください。

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

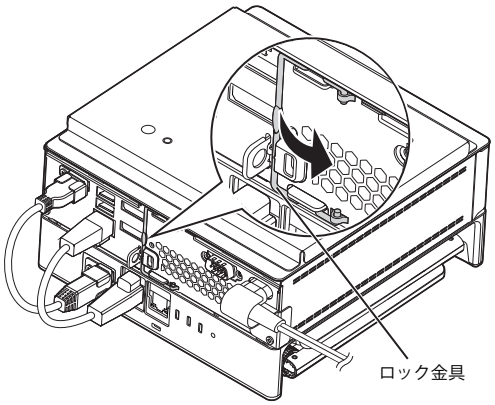
1 本製品の電源を切り、アンテナをたたみます。また、電源プラグをコンセントから取り外した後、専用ケーブルを除く本製品に接続しているすべてのケーブルを取り外します。

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。

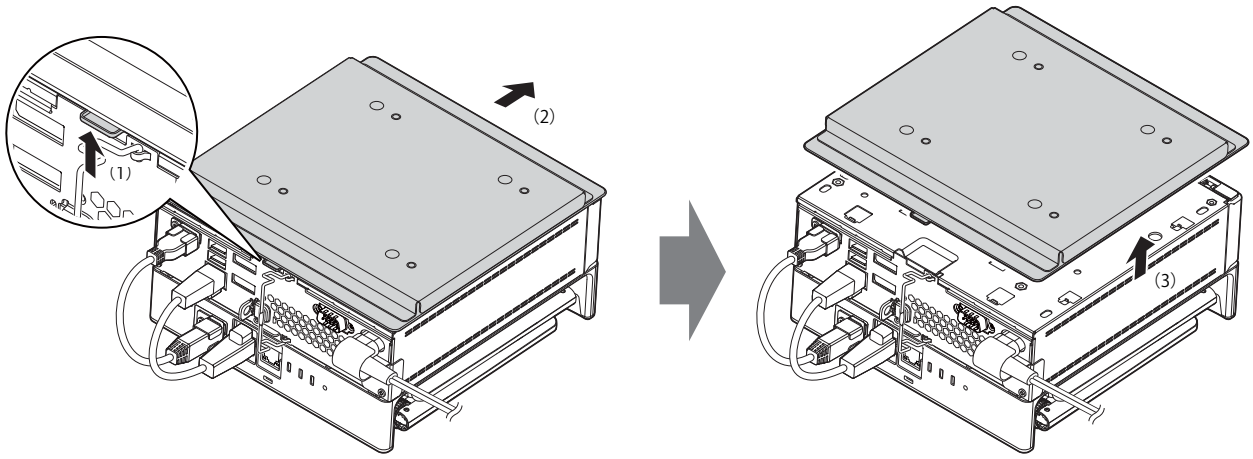
3 壁掛け金具から本製品を取り外します。取り外し方法については、壁掛け金具のマニュアルをご覧ください。

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。

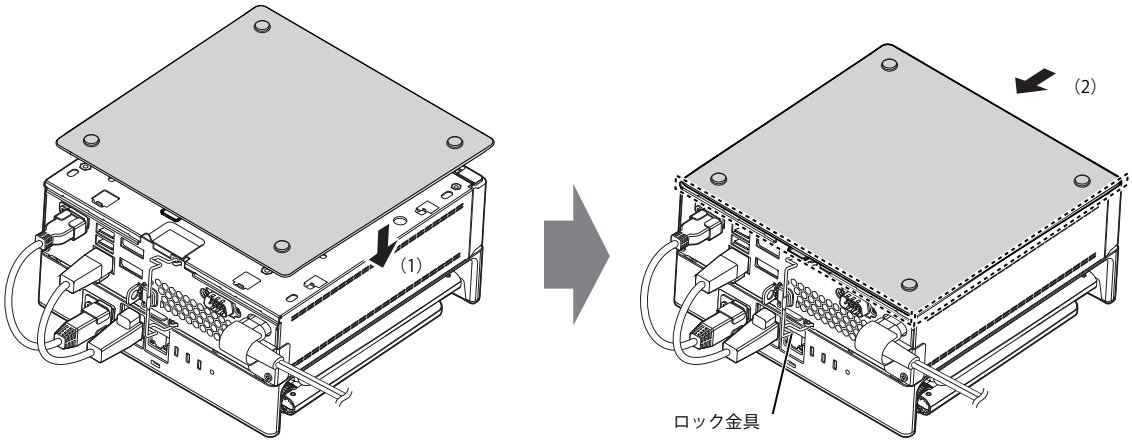


VESA マウントを取り外した後、底面カバーを取り付けてください（→ P.149）。

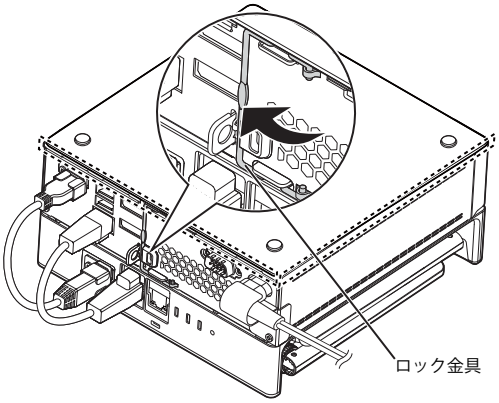
底面カバーの取り付け

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。

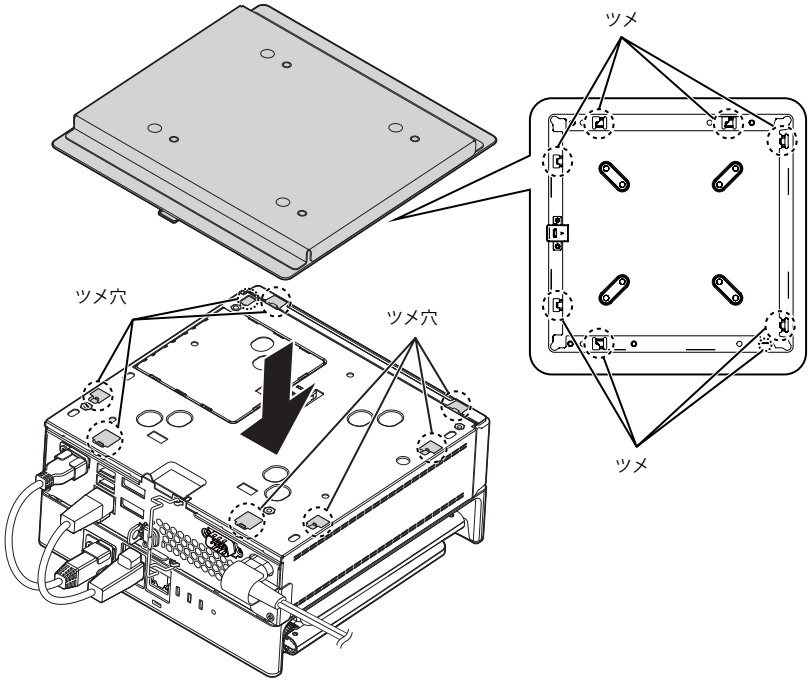
壁掛け設置には特別な技術が必要です。必ず専門の取付工事業者へご依頼ください。
本製品の設置に不備があると落下事故などの原因となります。
カスタムメイドオプションで VESA マウントを選択した場合は、本製品に固定バンド（2 本）を添付されています。
製品本体のセキュリティ施錠金具に固定バンドを通し、壁掛け金具などしっかりと固定された箇所に結び付けて落下防止措置を必ず講じてください。

VESA マウント取り付け

1　底面カバーを取り外します。

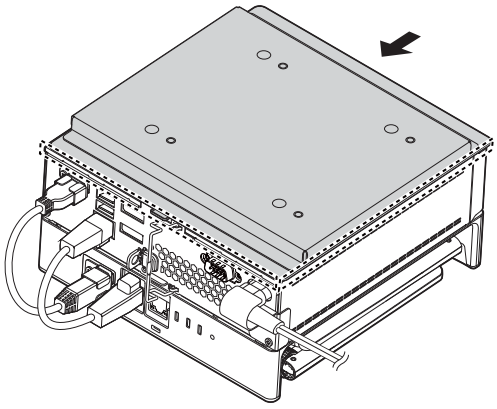
「VESA マウントの取り外し」（→ P.148）で「VESA マウント」を「底面カバー」に読み替えて底面カバーを取り外してください。

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。

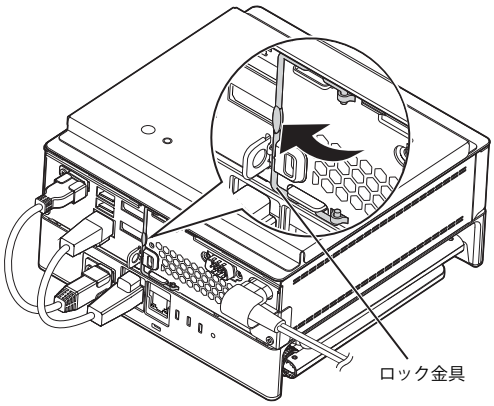


3　VESA マウントを本体背面側にスライドさせた後、本体と VESA マウントの間にすき間がないことを確認します。

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。

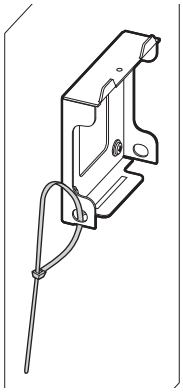


壁掛け金具への取り付け

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。



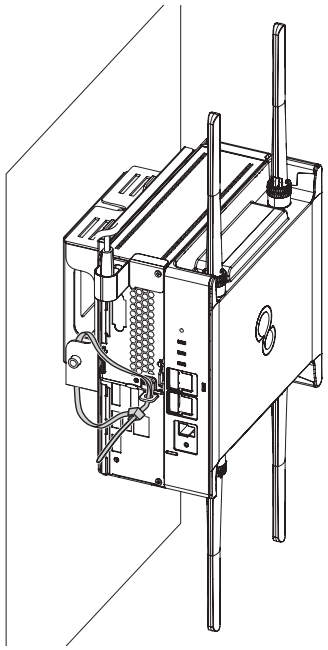
2 壁側の壁掛け金具に本製品を取り付けます。

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. 設定項目確認一覧表

本製品を運用するに当たって必要な設定を説明します。詳しくは、別マニュアルの『設定項目確認一覧表』をご覧ください。

5. 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.106）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.30）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。

6. 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.153）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」（https://www.fujitsu.com/jp/about/environment/recycleinfo/）をご覧ください。

ESPRIMO Edge Computing Edition Z0111/W

導入ガイド

B6FK-5781-01 Z0-06

発 行 日　　2021 年 5 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