B6FY-4771-02 Z0

FUJITSU Desktop ESPRIMO

管理ガイド

ESPRIMO Edge Computing Edition Z0110/E

FUJITSU

目次

本書をお読みになる前に 5
このマニュアルの目的 5
安全にお使いいただくために 5
本書の表記 5
Windows の操作 6
商標および著作権 6

第 1 章　各部名称

1 エッジコンピューティングデバイス前面 8
2 エッジコンピューティングデバイス背面 9
アクセスポイント部分 9
コンピューター部分 11
3 VESA マウント 12

第 2 章　概要

1 本製品について 14
2 本製品でできること 15
アプリについて 15
ハードウェアについて 15
3 本製品の機能について 16
基本機能 - 管理画面 16
基本機能 - データキャッシュ機能 17
基本機能 - 状態監視 18
拡張機能 - セキュリティ 18
拡張機能 - 端末情報収集 19
拡張機能 - ネットワーク 21
拡張機能 - 画面共有 21
基本機能 - 通知 21

第 3 章　設置／接続する

1 外部アンテナを立てる 23
2 ケーブル類を接続する 24
画面表示機器を接続する 24
LAN ケーブルを接続する 25
電源プラグをコンセントに接続する 25
3 電源の入れ方／切り方 26
電源を入れる 26
電源を切る 26

第 4 章　各種機能の操作方法

1 基本機能 - アクセスポイント 28
2 基本機能 - 管理画面 28
管理画面へのログイン 29
管理画面設定 30
3 基本機能 - インターネットキャッシュ機能 34
[キャッシュデータ] − [キャッシュデーター覧] 34
[キャッシュデータ] − [キャッシュデータ事前登録] 35
[キャッシュエンジン] − [キャッシュエンジン制御] 36
[キャッシュエンジン] − [使用状況] 37
[キャッシュエンジン] − [ログ取得] 37
[キャッシュ設定] 38
キャッシュに登録されたことを確認する 44
[設定項目の追加] 45
キャッシュを削除する 46

証明書の作成とインストール 48
キャッシュログ集計ツール 54
4 基本機能 - サーバファイルキャッシュ管理 55
[実況状況] − [簡易情報取得・手動制御] 55
[実況状況] − [詳細情報取得] 55
[キャッシュエンジン] − [キャッシュエンジン制御] 56
[キャッシュエンジン] − [グループ共通設定] 56
[キャッシュエンジン] − [個別設定] 57
[キャッシュエンジン] − [ログ取得] 57
5 基本機能 - 状態監視 58
動作状態監視ツール 58
お手入れナビ 58
6 拡張機能 - セキュリティ（端末認証） 59
管理画面へログイン 59
認証情報 59
7 拡張機能 - ネットワーク 64
優先接続設定 64
8 拡張機能 - 端末情報収集 65
端末情報管理 65
バッテリー劣化診断 65
無線 LAN 診断 66
稼働時間 67
無線 LAN 接続台数表示 67
9 拡張機能 - 画面共有 67
Intel Unite 67

第 5 章　バックアップと復元

1 本製品のバックアップと復元 69
システムイメージバックアップについて 69
システムイメージをバックアップする 70
システムイメージを復元する 73
回復ドライブ（USB）を作成する 78
システム修復ディスクを作成する 78
2 リカバリ USB メモリを使ったリカバリ 79
内蔵ディスク構成 79
内蔵ディスク全体をリカバリする 79
内蔵ディスク全体をリカバリする前の準備 81
内蔵ディスク全体のリカバリを実行する 82
リカバリ後のセットアップ 83
3 内蔵ディスク内のデータを使った回復方法 84
「この PC を初期状態に戻す」機能の注意事項 84
「この PC を初期状態に戻す」の種類 84
「この PC を初期状態に戻す」手順 85
4 アクセスポイントの設定のバックアップと再設定 86
設定ファイルの保存 86
設定ファイルからの再設定 87
5 管理画面の設定と収集データのバックアップと再設定 88
管理画面設定と端末から収集したデータのエクスポート 88
管理画面設定と端末から収集したデータのインポート 89
6 証明書ファイルのバックアップと再設定 90
証明書ファイルのバックアップ 90
証明書ファイルの再設定 90
7 端末認証機能の設定のバックアップと再設定 94
登録済み端末データファイルの保存 94
登録済み端末データファイルのインポート 95

第 6 章　お手入れ

1 日常のお手入れ 97
2 定期的なお手入れ 97

第 7 章　トラブルシューティング

1 トラブル発生時の基本操作 99
状況を確認する 99
以前の状態に戻す 99
トラブルシューティングで調べる 99
診断プログラムを使用する 100
2 トラブルシューティング 101
起動・終了時のトラブル 101
Windows・ソフトウェア関連のトラブル 101
メンテナンス機能のトラブル 102
インターネットキャッシュ機能のトラブル 105
サーバファイルキャッシュ機能のトラブル 107
優先接続設定のトラブル 107
無線 LAN 接続台数表示のトラブル 108
Intel Unite のトラブル 108
端末認証機能のトラブル 108
ハードウェアのトラブル 113
エラーメッセージ一覧 115
Intel Unite のファイアウォールの設定 117
3 それでも解決できないときは 118
ファームウェアと BIOS のアップデート 118
問い合わせ先 118

第 8 章　付録

1 仕様 120
ESPRIMO Edge Computing Edition Z0110/E 120
CPU 122
アプリの動作環境 123
2 VESA マウントの取り付け／取り外し 125
VESA マウントの取り外し 125
底面カバーの取り付け 126
VESA マウントの取り付け 127

本書をお読みになる前に

このマニュアルの目的

添付アプリの操作方法、本製品のバックアップと復元方法、本製品のお手入れに関する情報を説明しています。また、システム運用・管理で発生したトラブルの対処を説明しています。このマニュアルは、システム管理者を対象としており、コンピューター、OS、およびネットワークについて基本的な知識を有している方がご覧になることを前提としています。

安全にお使いいただくために

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

本書の表記

本書の記号

本書に記載されている記号には、次のような意味があります。

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

キーの表記と操作方法

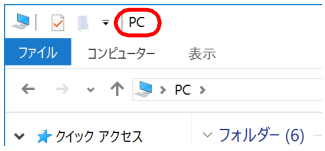
本書中のキーの表記は、キーボードに書かれているマークを記述するのではなく、説明に必要な文字を使い、次のように記述しています。
　例：【Ctrl】キー、【Enter】キー、【→】キーなど
また、複数のキーを同時に押す場合には、次のように「+」でつないで表記しています。
　例：【Ctrl】＋【F3】キー、【Shift】＋【↑】キーなど

連続する操作の表記方法

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

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

例：



↓
「PC」ウィンドウ

↓
「システム」ウィンドウ

画面例およびイラストについて

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

製品の呼び方

本書では、製品名称を次のように略して表記します。

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

Windows の操作

アクションセンター（Windows 10）

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

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

「コントロールパネル」ウィンドウ

次の手順で「コントロールパネル」ウィンドウを表示させてください。

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

「コマンドプロンプト」ウィンドウ

次の手順で「コマンドプロンプト」ウィンドウを表示させてください。

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

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

ユーザーアカウント制御

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

通知領域のアイコン

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

商標および著作権

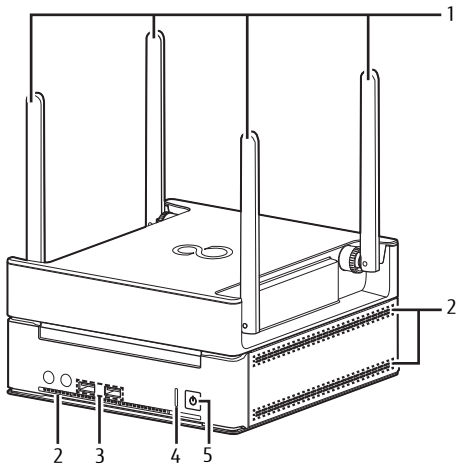
1

第 1 章
各部名称

各部の名称と働きについて説明します。

1. エッジコンピューティングデバイス前面 8
2. エッジコンピューティングデバイス背面 9
3. VESA マウント 12

1. エッジコンピューティングデバイス前面



1　外部アンテナ

無線電波を受信／送信します。

2　吸気孔

冷却用の空気を取り込むための穴です。

3　USB3.0 コネクタ（•<）

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

4　ステータスランプ

本製品の状態を表示します。

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

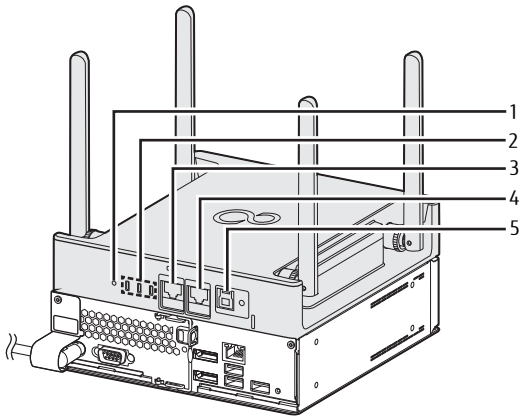
5　電源ボタン／電源ランプ（⏻）

製品本体の電源を入れます。また、本製品の状態を表示します。

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

2. エッジコンピューティングデバイス背面

アクセスポイント部分



（イラストは、電源ケーブル以外のすべてのケーブルを省略した状態です。）

1　RESET ボタン

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

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

2　アクセスポイント状態表示ランプ

アクセスポイントの状態を表示します。

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

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

3　WAN コネクタ

LAN ケーブルで接続します。
LED の状態は次のとおりです。

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

注 ： データ転送中は緑色点滅

4　LAN コネクタ

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

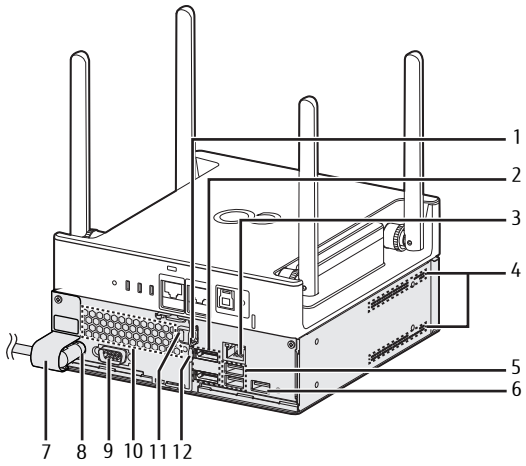
	左 LED（Link/Act）	右 LED（Speed）
1000Mbps で Link を確立	緑色点灯[注]	オレンジ色点灯
100Mbps で Link を確立	緑色点灯[注]	緑色点灯
10Mbps で Link を確立	緑色点灯[注]	消灯

注 ： データ転送中は緑色点滅

5　電源供給用 USB コネクタ

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

コンピューター部分



（イラストは、電源ケーブル以外のすべてのケーブルを省略した状態です。）

1　セキュリティ施錠金具

市販の鍵を取り付けます。セキュリティ施錠金具の穴径は φ6mm です。

2　DisplayPort コネクタ

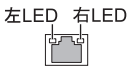
ディスプレイなどの画面表示機器の DisplayPort 信号ケーブルを接続します。

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

3　LAN コネクタ

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

LED の状態は次のとおりです。



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

注1：データ転送中は緑色点滅

注2：10Mbps 優先

注3：100Mbps 優先

注4：速度最低ではない

4　吸気孔

冷却用の空気を取り込むための穴です。

5　USB3.0 コネクタ

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

6　電源供給用 USB コネクタ

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

7　電源ケーブルカバー

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

8　インレット

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

9　シリアルコネクタ

10　排気孔

製品内部の熱を外部に逃がします。

11　盗難防止用ロック取り付け穴

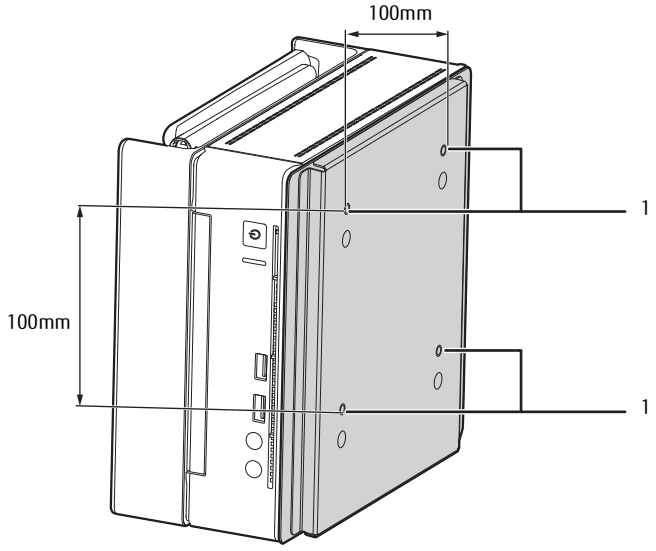
盗難防止用ケーブルを取り付けます。

12　ロック金具

コンピューター部分本体と底面のカバーを留めます。

3. VESA マウント

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



1　壁掛け金具固定用ネジ穴（4ヶ所）

VESA FDMI 規格対応の壁掛け金具を取り付けるための穴です。

重要

▸必ずお守りください

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

POINT

▸VESAマウントを取り外して使用する場合は、添付の底面カバーを取り付けてください。詳しくは、「VESAマウントの取り付け／取り外し」（→P.125）をご覧ください。

壁掛けキットの取り付け方法

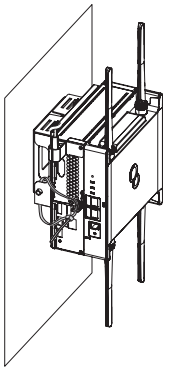
本製品の VESA マウントは、VESA FDMI 規格対応の壁掛け金具に取り付けることができます。

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.128）をご覧ください。
▸生徒の手の届かない場所に設置してください。
▸壁掛け金具および壁への取り付け、取り外しは、アンテナを折りたたんだ状態で行ってください。
▸エッジコンピューティングデバイスの向きが下図のようになるように（本製品の銘版ラベルが下から見えるように）取り付けてください。



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

2

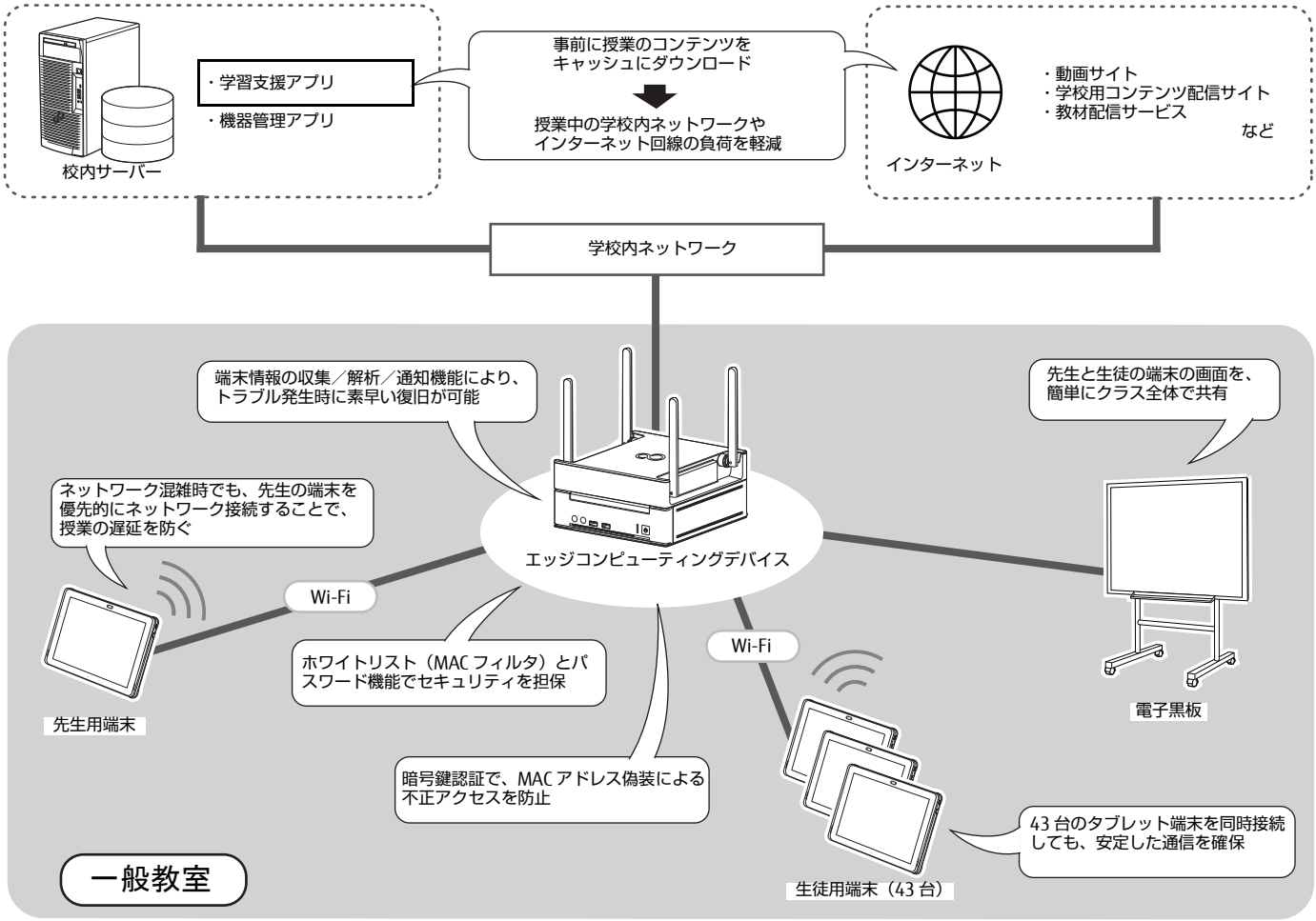
第 2 章
概要

本製品の概要について説明します。

1. 本製品について 14
2. 本製品でできること 15
3. 本製品の機能について 16

1. 本製品について

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



2. 本製品でできること

アプリについて

本製品に搭載されているアプリは、大きく分けて 2 種類があります。

●授業をする先生を支援するアプリ

●タブレット端末を管理 / メンテナンスする管理者を支援するアプリ

先生向けアプリ

種別		アプリ名称	機能概要	機能詳細
授業支援	基本機能	管理画面	本製品に付属するアプリの操作をするための UI 機能	→ P.16
		インターネットキャッシュ機能	インターネット上コンテンツ（動画、静止画を含む）のデータキャッシュ機能	→ P.17
		サーバファイルキャッシュ機能	教材 / 生徒のアップロードした成果物のデータキャッシュ機能	→ P.17
	拡張機能	優先接続設定	本製品に接続するタブレット端末のネットワーク帯域の優先順位を設定する機能	→ P.21
		無線 LAN 接続台数表示	本製品に接続しているタブレット端末の台数表示機能	→ P.20
		Intel Unite	画面共有機能	→ P.21

管理者向けアプリ

種別		アプリ名称	機能概要	機能詳細
アプリの管理 / 操作	基本機能	管理画面	本製品に付属するアプリの操作をするための UI 機能	→ P.16
セキュリティ	拡張機能	端末認証	アクセス制限機能	→ P.18
情報収集		端末情報収集ツール	本製品およびタブレット端末の稼働時間の収集機能	→ P.19
メンテナンス（タブレット端末）		端末情報収集ツール	バッテリー劣化診断機能	→ P.19
		無線 LAN 診断	無線 LAN 接続トラブル診断機能	→ P.19
メンテナンス（本製品自身）	基本機能	動作状態監視ツール	トラブル発生時の自動修復機能と通知機能	→ P.18
		インターネットキャッシュ機能	インターネット上コンテンツ（動画、静止画含む）のデータキャッシュ機能	→ P.17
		お手入れナビ	通風孔のお手入れの時期と装置内部が高温状態であることを通知する機能	→ P.18
通知		メール通知設定	無線 LAN 診断、稼働時間、バッテリー劣化診断の結果を指定したメールアドレスに自動送信する機能	→ P.21

ハードウェアについて

アクセスポイント

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

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

●44 台無線 LAN 端末の安定稼働保証

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

●当社独自のセキュリティ機能搭載

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

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

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

3. 本製品の機能について

基本機能 - 管理画面

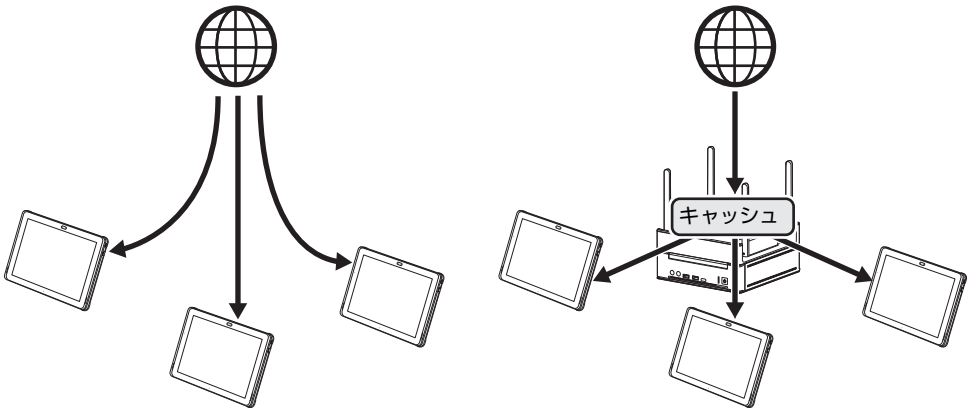
本製品に付属するアプリの設定を管理画面に集約して管理／操作できます管理画面では、本製品を運用するうえで必要な各種設定をブラウザーで行います。
本製品にアクセス可能な端末で設定してください。

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

基本機能 - データキャッシュ機能

インターネットキャッシュ機能

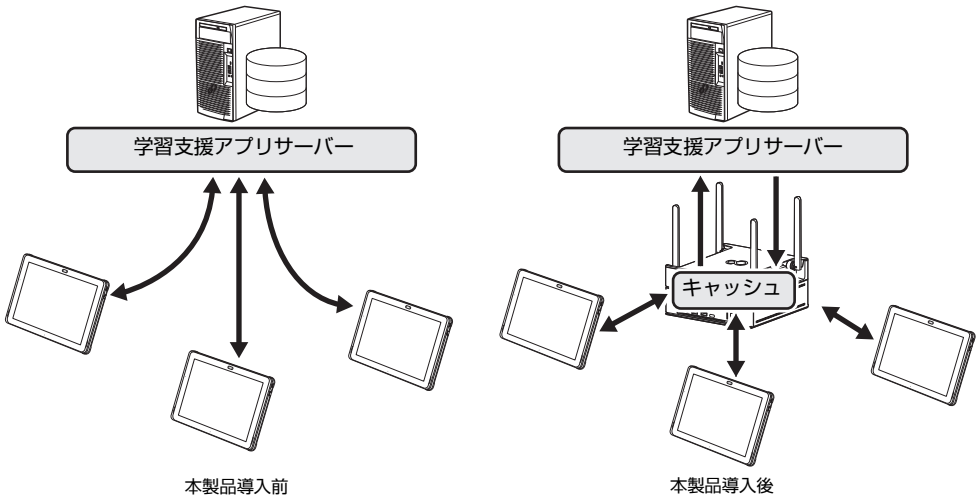
インターネットキャッシュ機能は、本製品に利用コンテンツを保存する機能です。本製品を導入したネットワーク上の最初のタブレット端末がインターネット上のコンテンツをダウンロードするときに、本製品のキャッシュにコンテンツが保存されます。以降のタブレット端末は本製品のキャッシュに保存されたコンテンツをダウンロードすることでインターネット回線の速度の影響を受けることなく、安定して利用することができます。



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

サーバファイルキャッシュ機能

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



基本機能 - 状態監視

動作状態監視ツール

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

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

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

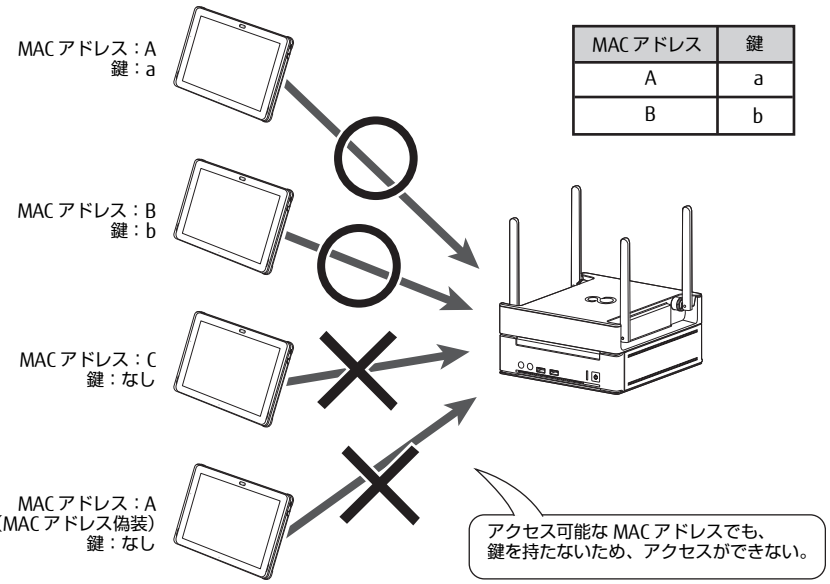
お手入れナビ

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

拡張機能 - セキュリティ

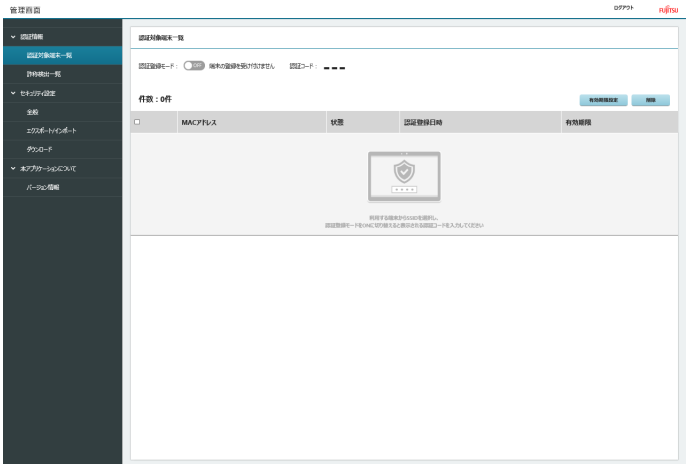
端末認証

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



POINT

▶「端末認証」は、認証端末機能専用の管理画面で設定します。



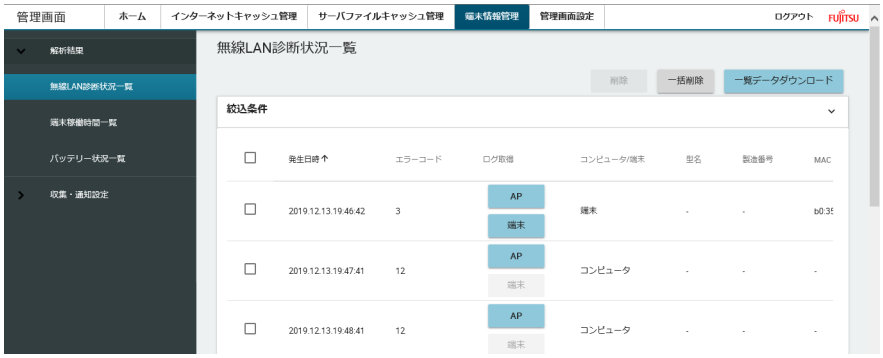
拡張機能 - 端末情報収集

バッテリー劣化診断

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

無線 LAN 診断

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



稼働時間

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

無線 LAN 接続台数表示

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

例：先生用端末 1 台、生徒用端末 40 台の場合

先生と生徒全員接続している場合

1 名の生徒が接続できていない場合

拡張機能 - ネットワーク

優先接続設定

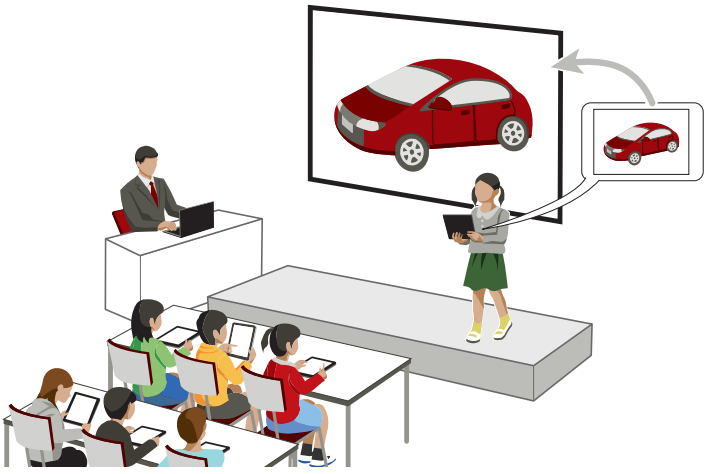
先生の端末を優先的にネットワークに接続することができます。授業で使用するコンテンツのダウンロードに時間がかかるなど、ネットワークの混雑が原因で授業の進行が遅れている場合は、本機能を使用してください。優先接続設定は、複数の先生用端末で設定することが可能ですが、優先接続できる端末は 1 台のみです。2 台以上で同時に優先接続設定を使うことはできません。

拡張機能 - 画面共有

Intel Unite

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

先生が授業で画面共有する場合



生徒が発表などで画面共有する場合

基本機能 - 通知

メール通知設定

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

●バッテリー劣化診断（→ P.19）
●無線 LAN 診断（→ P.19）
●稼働時間（→ P.19）

3

第 3 章
設置／接続する

本製品を設置／接続する方法や、注意点について説明します。

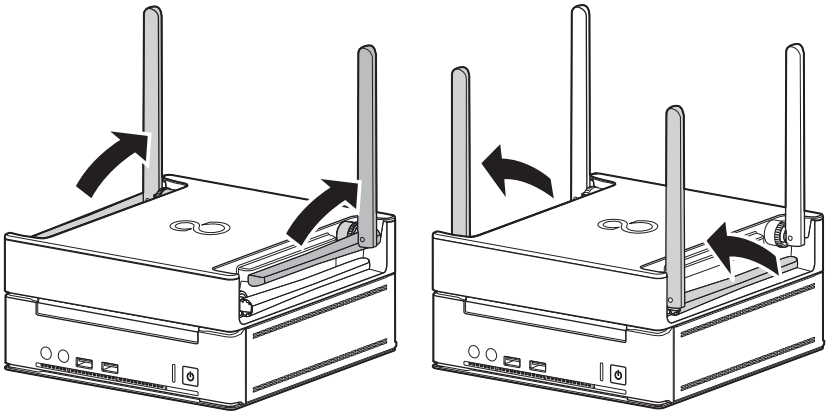
1. 外部アンテナを立てる 23
2. ケーブル類を接続する 24
3. 電源の入れ方／切り方 26

1. 外部アンテナを立てる

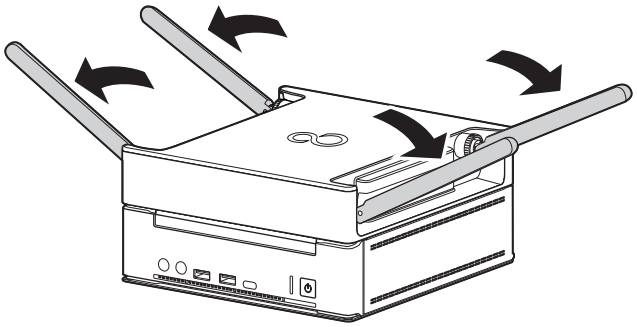
重要

▸外部アンテナに過度な力を加えないでください。

1 本製品背面側の外部アンテナ（2 本）を立てた後、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。



2. ケーブル類を接続する

画面表示機器を接続する

ディスプレイや電子黒板、プロジェクター、テレビなどの画面表示機器を接続する方法を説明します。

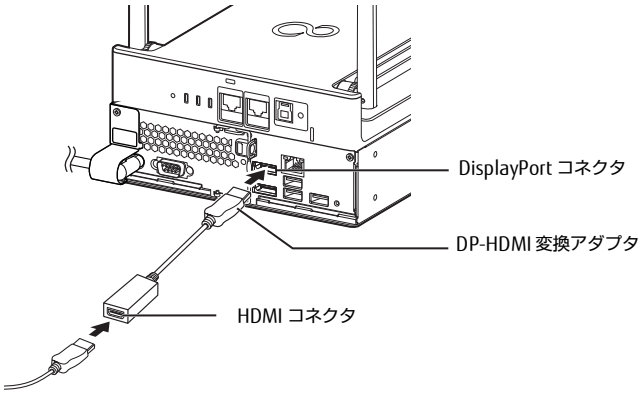
重要

- セットアップが完了するまで、接続する画面表示機器は 1 台のみにしてください。
- 画面表示機器 1 台につき、1 本のケーブルで接続してご利用ください。
- 画面表示機器については、フル HD の解像度（1920×1080）または、16 対 9 のアスペクト比が推奨の画面表示機器をご使用ください。それ以外の画面表示機器を使用される場合は、「グラフィックス・コントロール・パネル」または、「ディスプレイの設定」にて解像度を 1920×1080 または 16 対 9 のアスペクト比に変更してご使用ください。

HDMI 接続の画面表示機器をお使いの場合

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

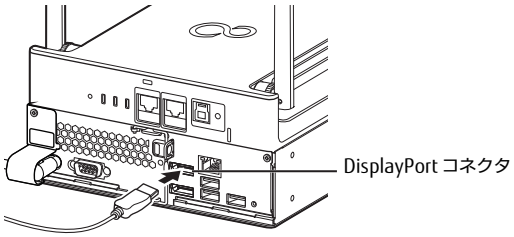
2 本製品背面の DisplayPort コネクタに DP-HDMI 変換アダプタを接続します。



（イラストは、電源ケーブル以外のすべてのケーブルを省略した状態です。）

DisplayPort 接続の画面表示機器をお使いの場合

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



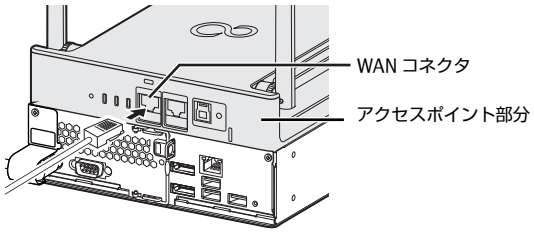
（イラストは、電源ケーブル以外のすべてのケーブルを省略した状態です。）

LAN ケーブルを接続する

重要

- 必ず、電源プラグをコンセントに接続する前に、LAN ケーブルを接続してください。

1　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。）

電源プラグをコンセントに接続する

重要

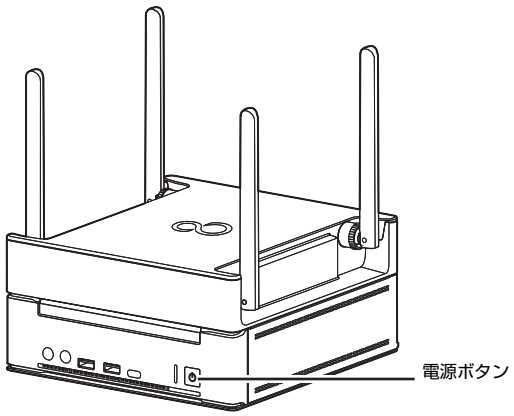
- 電源プラグをコンセントに接続する前に、LAN ケーブルが接続されていることを確認してください。LAN ケーブルが接続されていない場合は、「LAN ケーブルを接続する」（→P.25）をご覧になり、LAN ケーブルを接続してください。
- アクセスポイント部分は、電源プラグをコンセントから抜くと電源が切れます。
- コンセント近くに本製品を設置し、電源プラグに手が容易に届くようにしてください。
- 本製品と電源ケーブルの接続部を押し込んだり引き出したりしないでください。

1　電源プラグをコンセントに接続します。

3. 電源の入れ方／切り方

電源を入れる

1 電源ボタンを押します。



POINT

- アクセスポイント部分は、電源プラグをコンセントに接続すると電源が入ります。
- 電源プラグをコンセントに接続した後、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。
- 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。

電源を切る

POINT

- アクセスポイント部分は、電源プラグをコンセントから抜くと電源が切れます。

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。

4

第 4 章
各種機能の操作方法

ここでは、各種機能の操作方法を説明します。

1. 基本機能 - アクセスポイント 28
2. 基本機能 - 管理画面 28
3. 基本機能 - インターネットキャッシュ機能. 34
4. 基本機能 - サーバファイルキャッシュ管理. 55
5. 基本機能 - 状態監視 58
6. 拡張機能 - セキュリティ （端末認証） 59
7. 拡張機能 - ネットワーク 64
8. 拡張機能 - 端末情報収集 65
9. 拡張機能 - 画面共有 67

1. 基本機能 - アクセスポイント

本製品のアクセスポイントの設定については、『アクセスポイント操作ガイド』をご覧ください。

2. 基本機能 - 管理画面

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。
管理画面に表示される項目は、ログインしているユーザーの管理者権限の有無で異なります。
管理者権限の有無は、「ユーザー管理」でユーザーを作成するときに決めます。後から変更することもできます。

管理画面の項目			管理者権限		説明
			あり	なし	
インターネットキャッシュ管理	キャッシュデータ	キャッシュデーター覧	○	○	本製品のキャッシュに保存されているファイルの一覧を閲覧とキャッシュ済みデータを削除できます（→ P.34）。
		キャッシュデータ事前登録	○	○	授業で使うコンテンツをあらかじめキャッシュすることができます（→ P.35）。
	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。（→ P.36）。
		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（→ P.37）。
		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（→ P.37）。
	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（→ P.38）。
	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。（→ P.45）
サーバファイルキャッシュ管理	実況状況	簡易情報取得・手動制御	○	−	各装置のサーバーキャッシュの同期状態の確認と手動で同期の割込実行ができます（→ P.55）。
		詳細情報取得	○	○	サーバファイルキャッシュによる同期状況を記載したファイルをダウンロードすることができます（→ P.55）。
	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（→ P.56）。
		グループ共通設定	○	−	グループ設定したエッジコンピューティングデバイス間で共通の設定項目を変更することができます（→ P.56）。
		個別設定	○	○	各エッジコンピューティングデバイスのキャッシュエンジンの個別の設定項目の変更やキャッシュエンジンの初期化をすることができます（→ P.57）。
		ログ取得	○	○	サーバファイルキャッシュ管理機能のログファイルをダウンロードできます（→ P.57）。
端末情報管理	解析結果	バッテリー状況一覧	○	○	バッテリーの状態を確認できます（→ P.65）。
		無線 LAN 診断状況一覧	○	○	無線 LAN 診断の状況を確認できます（→ P.66）。
		端末稼働時間一覧	○	○	本製品に接続した端末の稼働状況を確認できます（→ P.67）。
	収集・通知設定	稼働時間	○	○	設定変更はお勧めしません。
		バッテリー	○	○	
		メール通知設定	○	−	
		情報収集設定（コンピュータ）	○	−	
		情報収集設定（端末）	○	−	
		SMTP 設定	○	−	
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（→ P.30）。
		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（→ P.30）。
	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（→ P.33）。
	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（→ P.33）。

管理画面へのログイン

次の手順で「管理画面」にログインします。

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

POINT

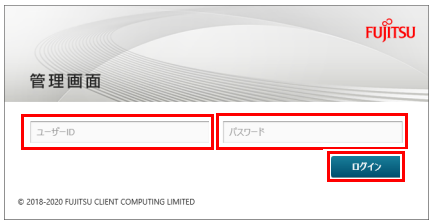
- IPアドレスにはコンピューター部分のIPアドレスをお使いください。
  コンピューター部分のIPアドレスが「192.168.1.3」の場合は次のようになります。
  http://192.168.1.3:10080/
- Internet Explorer で管理画面を表示したときに入力フォームが表示されない場合は、次の設定をご確認ください。
  1.Internet Explorer を起動します。
  2.画面右上のツールアイコン ⚙（設定）→「互換表示設定」の順にクリックします。
  「互換性設定の変更」が表示されます。
  3.「イントラネットサイトを互換表示で表示する」のチェック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

ログイン画面が表示されます。

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

POINT

- 本製品導入時に設定したユーザー IDとパスワードを入力してください。ユーザー ID名やパスワードを変更した場合やユーザー IDを新規作成した場合は、そのユーザー IDとパスワードを入力してください。



「管理画面」が表示されます。

それぞれのタブをクリックすると、各機能の管理画面に切り替わります。

管理画面設定

管理画面を利用するユーザーに関する設定ができます。

[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。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。

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。

[ユーザー管理] – [ユーザー一覧]

登録されているユーザーの一覧が表示されます。ユーザー一覧では、次のことができます。

POINT

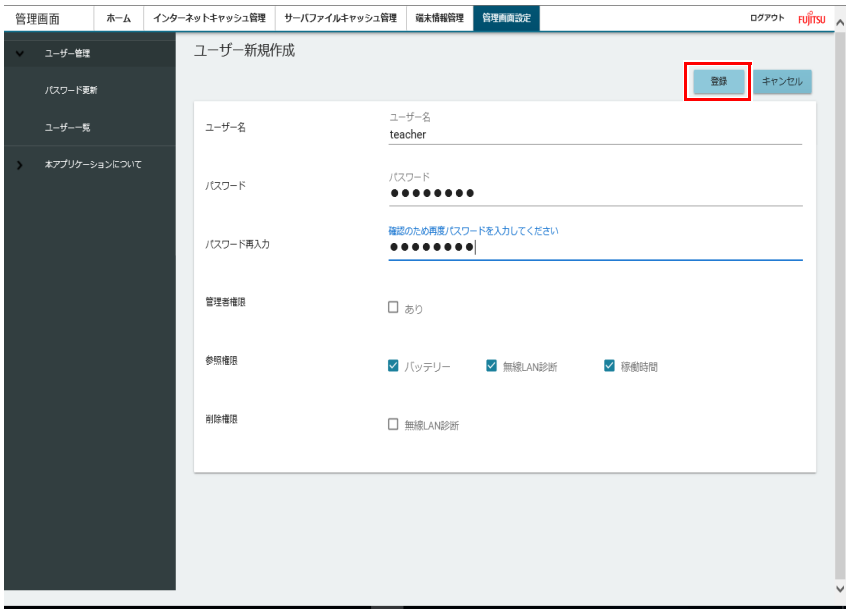
- 管理者権限のないユーザー ID でログインした場合は、この項目は表示されません。管理者権限のユーザー ID でログインする必要があります。管理者権限については、「新しいユーザーを登録する」（→P.31）の表をご覧ください。

●新しいユーザーを登録する（→ P.31）
●ユーザーの情報を更新する（→ P.32）
●ユーザーを削除する（→ P.32）

■新しいユーザーを登録する

1「新規登録」をクリックします。

2 必要な情報を入力し、「登録」をクリックします。



項目	説明
ユーザー名	1 ～ 64 文字で入力します。 ※ 次の記号は使用できません。< ⇒ % * + = [ ] \ / | ; : " < > ? , @
パスワード	8 ～ 16 文字で入力します。
パスワード再入力	確認のため、「パスワード」欄に入力したパスワードを入力します。
管理者権限	管理者権限を有効にしたい場合は、「あり」に設定します。 管理者権限を有効にすると、管理画面のすべての項目を設定できるようになります。 学校の先生向けにユーザーを作成する場合は、無効にすることをお勧めします。管理者権限が無効でも、キャッシュの事前登録など、先生が使う機能は利用できます。
参照権限	「バッテリー」「無線 LAN 診断」「稼働時間」を参照させるか設定します。
削除権限	「無線 LAN 診断」の結果を、削除できるようにするか設定します。

■ユーザーの情報を更新する

ユーザー名、パスワード、権限などを修正できます。

1 ユーザー名をクリックします。

2 必要に応じて情報を変更し、「更新」をクリックします。

■ユーザーを削除する

不要になったユーザーを、ユーザー一覧から削除できます。

1 削除したいユーザー名の後ろにある をクリックします。

2 削除確認の画面が表示されたら「はい」をクリックします。
ユーザーが削除され、ユーザー一覧に戻ります。

[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することができます。詳しくは、「管理画面の設定と収集データのバックアップと再設定」（→ P.88）をご覧ください。

POINT

- インポートを行うと、管理画面のキャッシュデーター覧のデータがすべて削除されます。

[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。

3. 基本機能 - インターネットキャッシュ機能

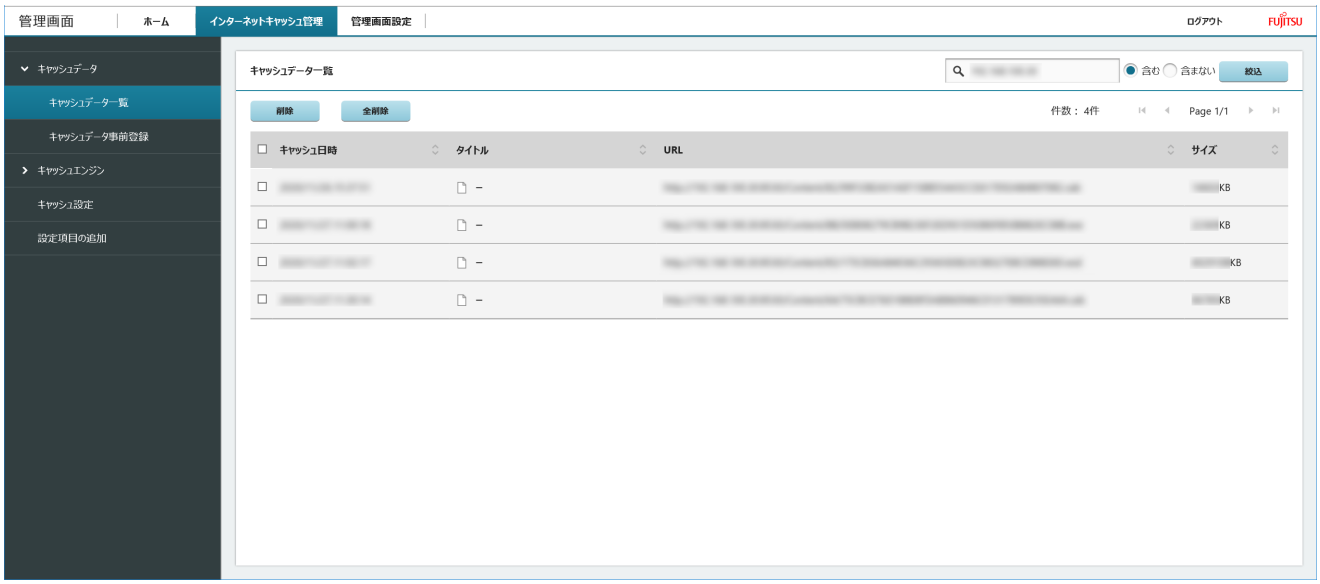
本製品内のインターネットキャッシュ機能の制御、設定、使用状況の確認などができます。
また、キャッシュデータの確認、削除、事前登録ができます。

[キャッシュデータ] – [キャッシュデーター覧]

本製品のキャッシュに保存されているファイルの一覧を閲覧できます。
また、不要になったファイルは、選択して「削除」をクリックすることで削除できます。
「キャッシュ日時」「URL」「サイズ」の部分をクリックすると、日時順（新しい日時、古い日時）、URL アルファベット順（昇順、降順）、サイズ順（大きい順、小さい順）に並べ替えることができます。

POINT

- 端末のブラウザーがバックグラウンドでインターネット上のコンテンツにアクセスしている場合があり、このときキャッシュされるとキャッシュデーター覧に表示されるデータの件数が変動します。



キャッシュの有効期限は、「キャッシュ制御」-「コンテンツの有効期限」で設定されます。

[キャッシュデータ] – [キャッシュデータ事前登録]

授業が始まる前に、授業で使うコンテンツ（動画、静止画、音声など）を、あらかじめキャッシュしておきます。
キャッシュしたいコンテンツのリストを、テキストファイルで作成し、アップロードすることで、キャッシュに登録できます。

■キャッシュできるプロトコルとコンテンツ

キャッシュできるプロトコル・コンテンツファイルは次のとおりです。

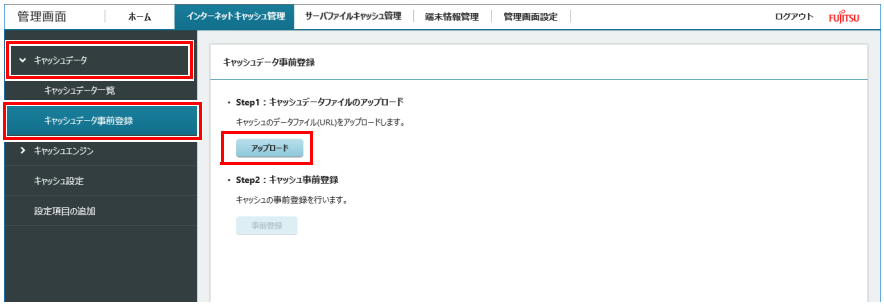
プロトコル	http、 https（キャッシュ対象プロトコルで「http/https」に設定している場合）
コンテンツファイル拡張子	gif、png、jpg、jpeg、ico、iso、avi、wav、mp3、mp4、wmv、mpeg、swf、flv、x-flv、deb、rpm、exe、zip、tar、tgz、ram、rar、bin、ppt、doc、tiff、html、htm、css、js、pdf など

すべてのコンテンツを保証するものではありません。また、使用するブラウザー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。

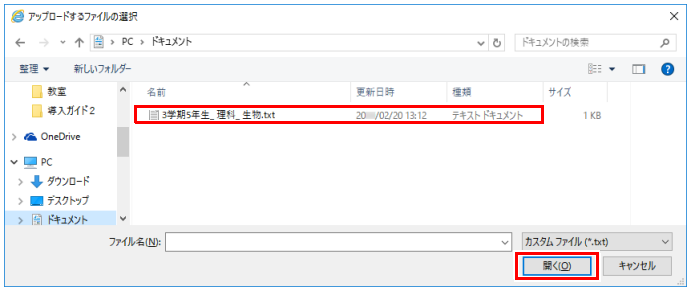
■リストを登録する

キャッシュしたいコンテンツのリストを作成したら、次の手順で本製品に登録します。なお、リストの作成方法については、『ユーザーガイド』の「インターネットキャッシュ機能を使用する」をご覧ください。

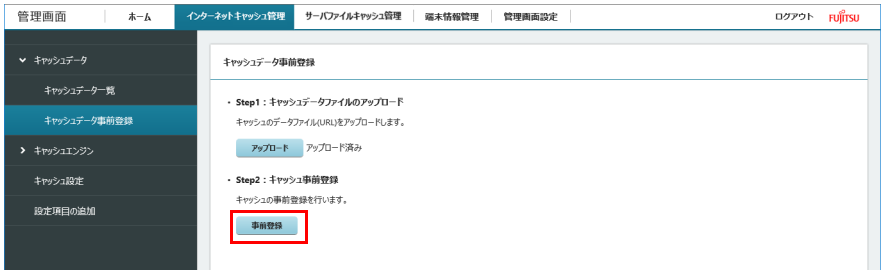
1 「キャッシュデータ」→「キャッシュデータ事前登録」→「アップロード」の順にクリックします。



2 あらかじめ作成したリストのファイルを指定し、「開く」をクリックします。

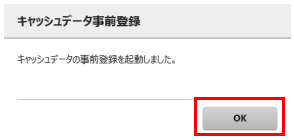


3 「事前登録」をクリックします。



「処理中」と表示されます。

4 「OK」をクリックします。



これで事前登録は完了です。

[キャッシュエンジン] ー [キャッシュエンジン制御]

POINT

▶Pキャッシュエンジンの初期化を実行すると、管理画面上で設定した値が初期化されます。初期化実行後は、再度設定しなおしてください（→P.38）。

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。

項目	説明
キャッシュエンジンの起動	キャッシュエンジンを起動します。
キャッシュエンジンの停止	キャッシュエンジンを停止します。
キャッシュエンジンの再起動	キャッシュエンジンを停止した後、再起動します。
初期化	キャッシュエンジンの設定を、ご購入時の状態に戻します（設定した管理画面上の値が全て初期化されます）。 キャッシュエンジンが動作している場合は、キャッシュエンジンの停止をしてから初期化してください。そのあと、キャッシュエンジンの起動をしてください。

[キャッシュエンジン] – [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。

[キャッシュエンジン] – [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]

POINT

▸キャッシュ設定を行う前に、ブラウザーのキャッシュをクリアしてください。ブラウザー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。

※OSやブラウザーのアップデートにより、手順が変更になる可能性があります。

・Internet Explorer の場合

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

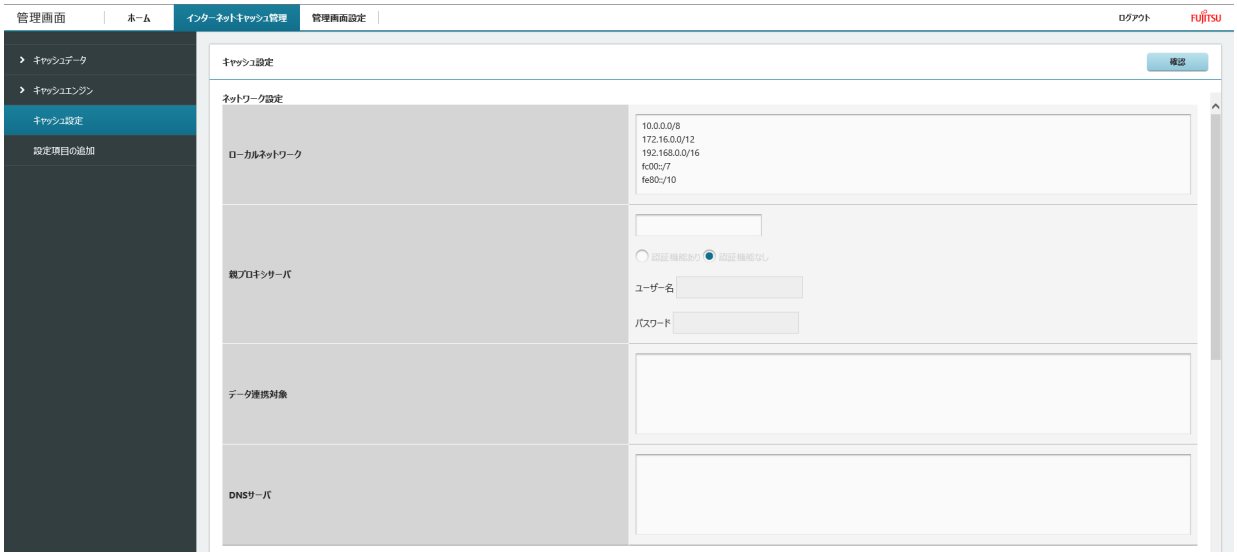
・Microsoft Edge（Chromium 版）の場合

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

・Google Chrome の場合

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

1 ネットワーク設定に関する項目を設定します。



各項目については、次の表をご覧ください。

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

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

2 キャッシュ制御に関する項目を設定します。

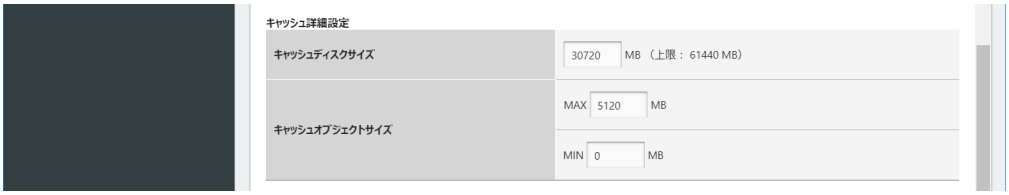
各項目については、次の表をご覧ください。

項目		説明
キャッシュ制御		
キャッシュ対象プロトコル[注 1]	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[注 1]	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。
X-Forwarded-For[注 1]	使用する	親プロキシサーバにリクエストを転送する際に X-Forwarded-For ヘッダにクライアントの IP アドレスの情報が追加されます。
	使用しない	親プロキシサーバにリクエストを転送する際に X-Forwarded-For ヘッダにクライアントの IP アドレスの情報が追加されません。
ホワイトリスト / ブラックリスト	ホワイトリスト[注 2]	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。
	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：ご購入時のインターネットキャッシュ機能では、設定できません。インターネットキャッシュ機能 V3.1.0 またはそれ以降のバージョンにアップデートすると項目が表示されて設定することができるようになります。

注 2：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。

3 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。

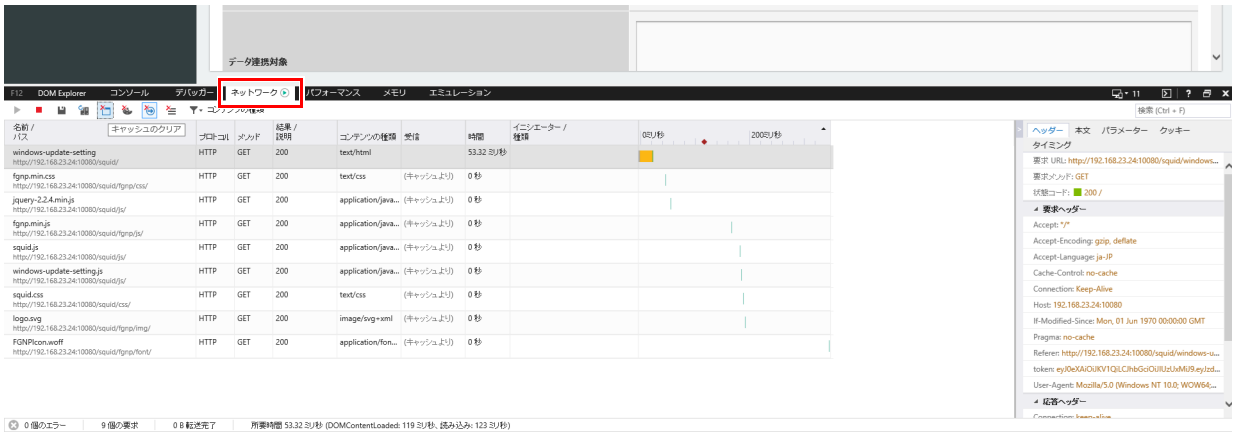
項目	説明	
キャッシュ詳細設定		
キャッシュディスクサイズ	キャッシュエンジンがキャッシュするデータ合計の最大サイズをMB単位で指定します。設定サイズを超過する場合は、キャッシュする領域が確保できるまで最古のデータから順に削除されます。	
	上限値	122880
	下限値	30720
	デフォルト設定	30720
キャッシュオブジェクトサイズ	MAX	キャッシュエンジンがキャッシュする 1 データの最大サイズを MB 単位で指定できます。 設定サイズを超過したデータはキャッシュされません。 キャッシュディスクサイズより大きいサイズは指定できません。
	上限値	2048
	下限値	1024
	デフォルト設定	1024
	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	2048
	下限値	0
	デフォルト設定	0

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

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

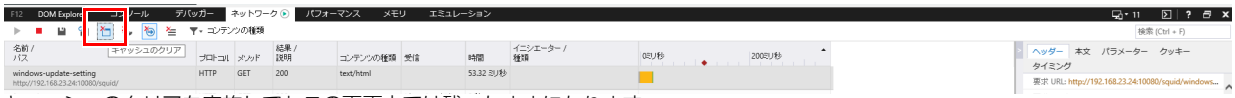
Internet Explorer にて親プロキシサーバで IP アドレスとポート番号を設定し、「確認」ボタンをクリックしたときに「プロキシサーバの入力が正しくありません。」と表示された場合は、次の手順を実施してください。

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



4. 下図に表示された項目の 1 番上の項目を選択します。

5. （キャッシュクリアアイコン）をクリックします。

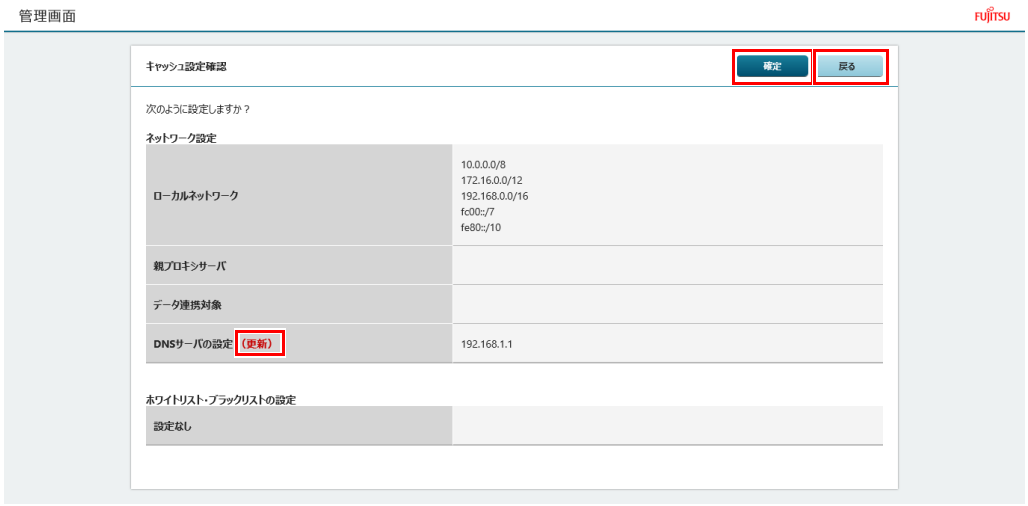


キャッシュのクリアを実施してもこの画面上では残ったままになります。

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

7. 画面右上にある ツールアイコン（設定）→「インターネット オプション」の順にクリックします。
8. 「全般」タブを選択し、「削除」をクリックします。
9. すべての項目にチェックを付けて、「削除」をクリックします。
10. 「OK」をクリックします。
11. 【F12】キーを押して開発者ツールを閉じます。

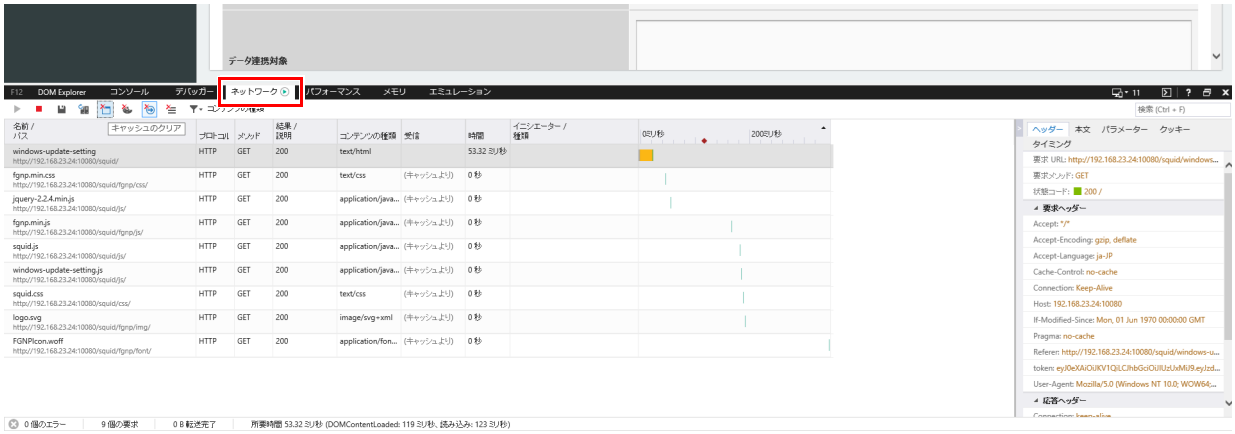
5　変更が問題ない場合は、「確定」をクリックします。
修正が必要な場合は、「戻る」をクリックして設定画面に戻ってください。



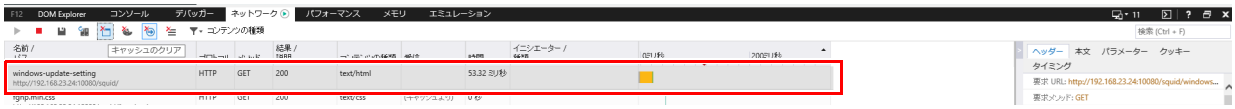
「設定の変更が完了しました。」というメッセージが表示されます。

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。

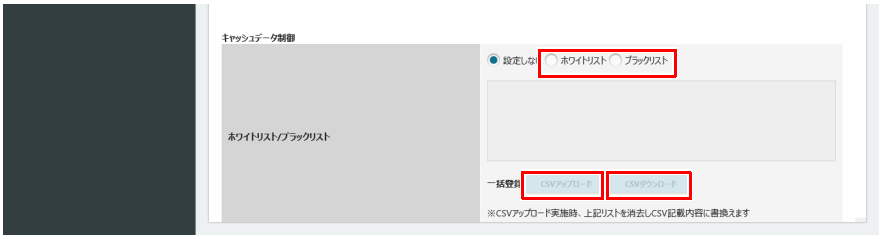
キャッシュのクリアを実施してもこの画面上では残ったままになります。

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。

csv ダウンロード／アップロード

「キャッシュデータ制御」のデータは、CSV ファイルとしてダウンロードすることもできます。



■ 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。「ホワイトリスト／ブラックリスト」が未設定の場合はダウンロードできません。

1 「csv ダウンロード」をクリックすると、「ホワイトリスト」または、「ブラックリスト」を CSV ファイルとして保存できます。

■ 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。

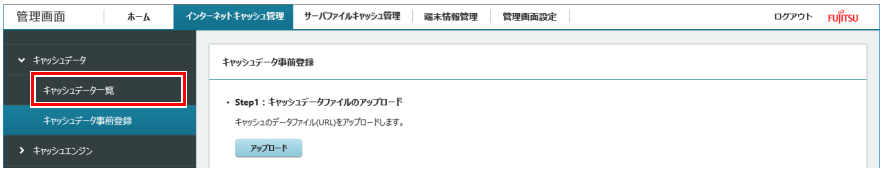
1 「ホワイトリスト」または、「ブラックリスト」をクリックします。

2 「csv アップロード」をクリックすると、「ホワイトリスト」または、「ブラックリスト」を CSV ファイルとして保存できます。

キャッシュに登録されたことを確認する

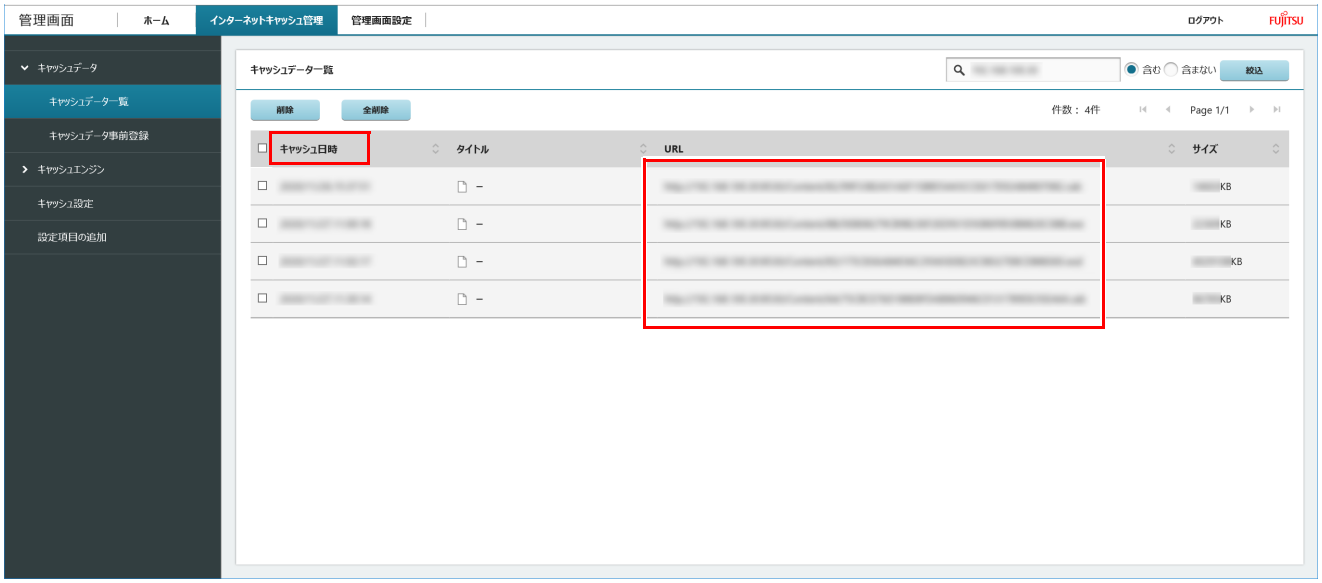
登録が終わったら、正常にキャッシュされているか確認します。

1 「キャッシュデーター覧」をタップします。



2 登録した URL が、正しく表示されているか確認します。

登録したキャッシュデータは、200 件ごとにページを切り替えて表示されます。
「キャッシュ日時」をタップすると、日時が新しい順、古い順に並べ替えることができます。
日時が新しい順にすると、登録した URL を確認しやすくなります。



[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。

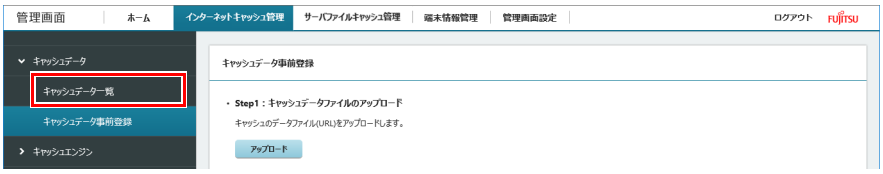
重要

- 「リカバリUSBメモリを使ったリカバリ」（→P.79）や「内蔵ディスク内のデータを使った回復方法」（→P.84）でシステムイメージを復元した場合は、この設定は再度必要です。

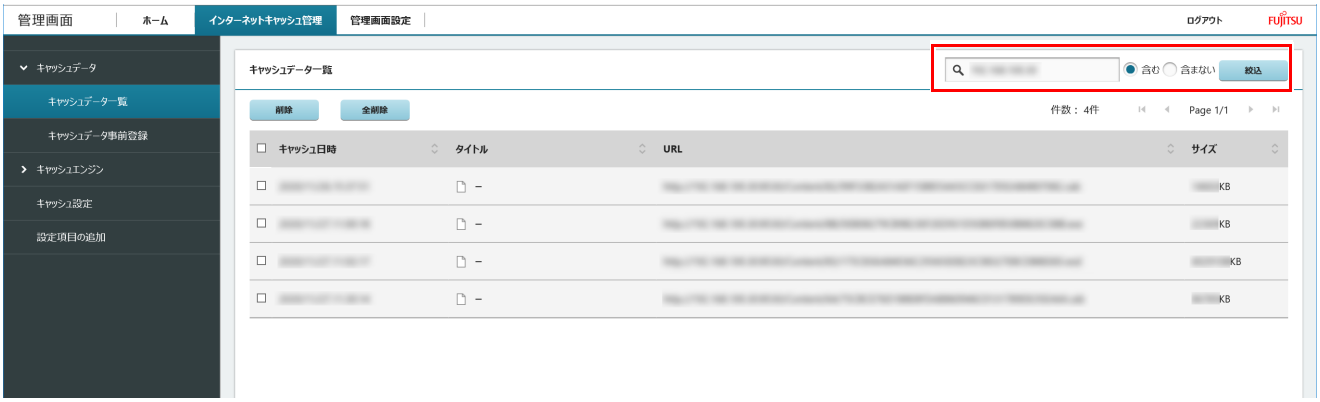
キャッシュを削除する

キャッシュに登録したデータのうち、不要になったものは「キャッシュデーター覧」（→ P.34）で削除できます。

1「キャッシュデーター覧」をします。



2 **削除したいデータを絞り込みます。**
キーワード入力域にキーワードを入力し、「含む」「含まない」を選択して「絞込」をタップすると、該当するデータだけが表示されます。



3 削除したいキャッシュデータのチェックボックスを選択し、「削除」をタップします。すべてのキャッシュを削除する場合は、「全削除」をタップします。

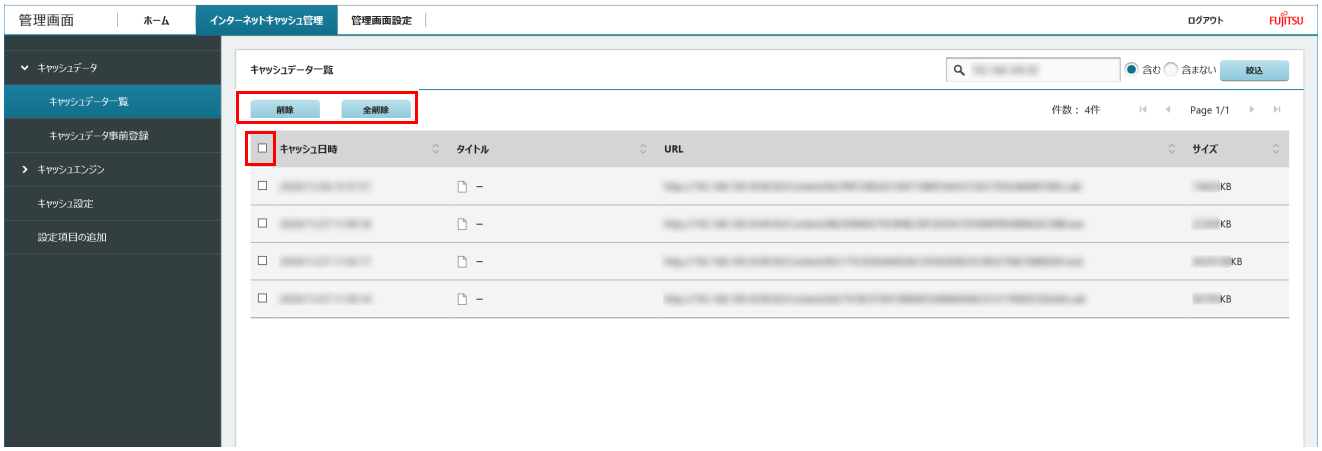
タイトル行の□を選択すると、ページ内で表示されているデータを一度に選択できます。

重要

- 「全削除」ボタンでデータの削除を行うと、「キャッシュログ集計ツール」（→P.54）で出力されるデータについて、過去のアクセスログは削除されます。
- 「全削除」ボタンでデータの削除を行うと、キャッシュ全削除処理中にキャッシュエンジンが再起動します。キャッシュエンジンの再起動が完了するまで、でインターネット接続ができなくなります。

POINT

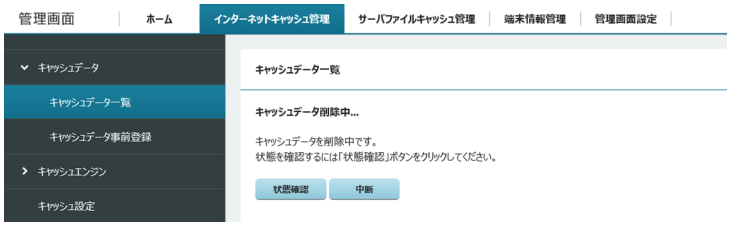
- URLの最後に（vary）がついているファイルは、一覧から削除できない場合があります。削除する場合は、「全削除」ボタンでデータを削除してください。



「キャッシュデータ削除中」と表示されます。しばらくすると、選択したデータがキャッシュから削除されます。

POINT

- キャッシュデータの削除中に、状況確認とキャッシュデータ削除の中断ができます。



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.38）。

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タブレット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 。
- タブレット端末用の証明書は、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.50）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（タブレット端末用）」（→ P.51）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）。

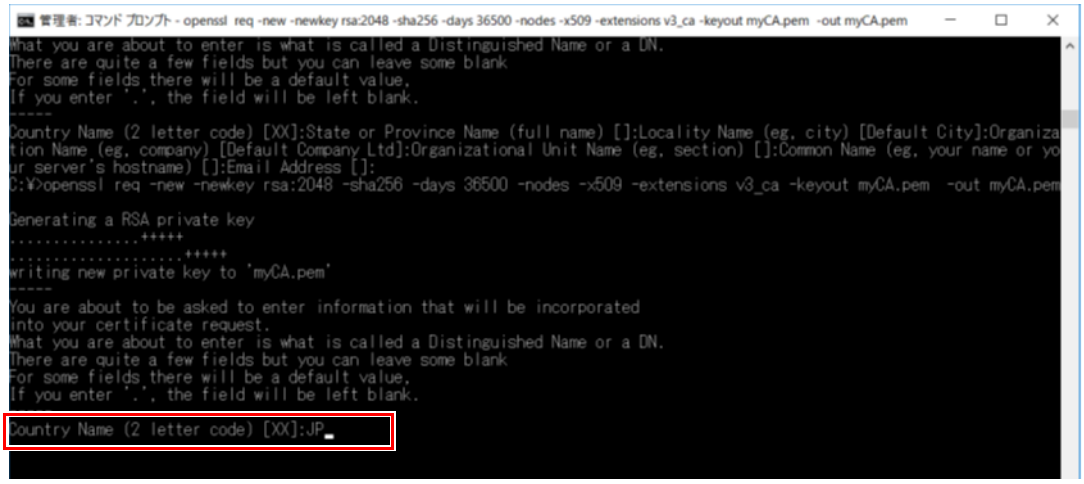
2 次のコマンドを入力して【Enter】キーを押します。
cd C:¥cygwin64¥bin

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。

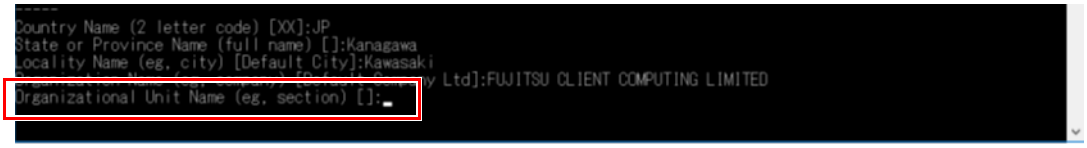


5 次の入力画面で「Kanagawa」を入力して【Enter】キーを押します。

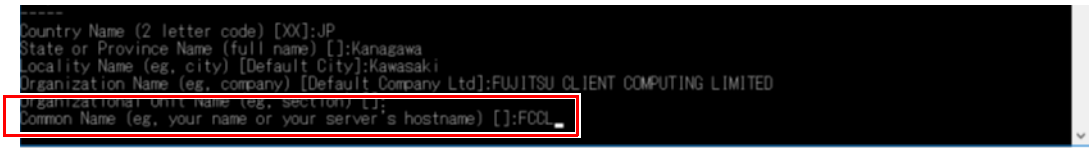
6 次の入力画面で「Kawasaki」を入力して【Enter】キーを押します。

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（タブレット端末用）

重要

- タブレット端末用の証明書は、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。
- 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タブレット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.48）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。

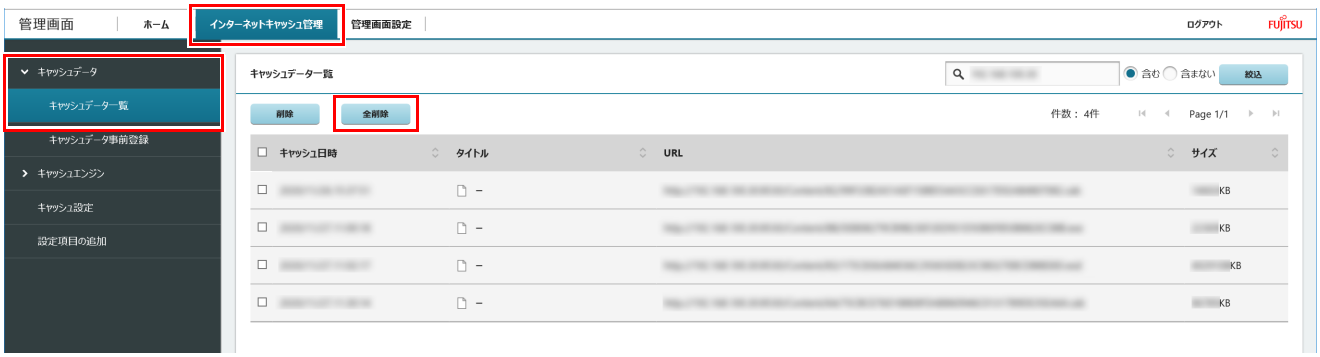
3 次のコマンドを入力して【Enter】キーを押します。
openssl x509 -in myCA.pem -outform DER -out myCA.der

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。
以上でタブレット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　管理画面でキャッシュ一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。



2　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制御」-「 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。

3　次のフォルダに「証明書の作成（エッジコンピューティングデバイス用）」（→ P.48）、「証明書の作成（タブレット端末用）」（→ P.49）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（タブレット用証明書）

4　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。

5　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制御」-「 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。

6　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。

証明書のインストール（タブレット端末用）

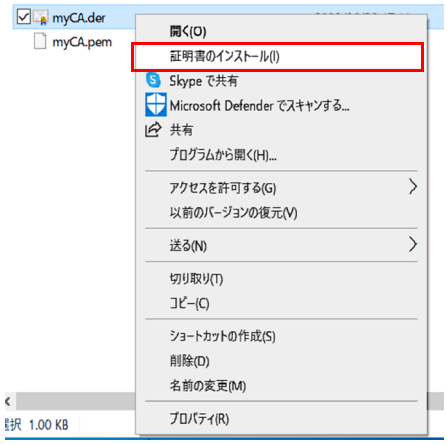
管理画面で「キャッシュ設定」の「キャッシュ対象プロトコル」を「http」に設定する場合は、証明書のインストールは不要です（→ P.38）。

重要

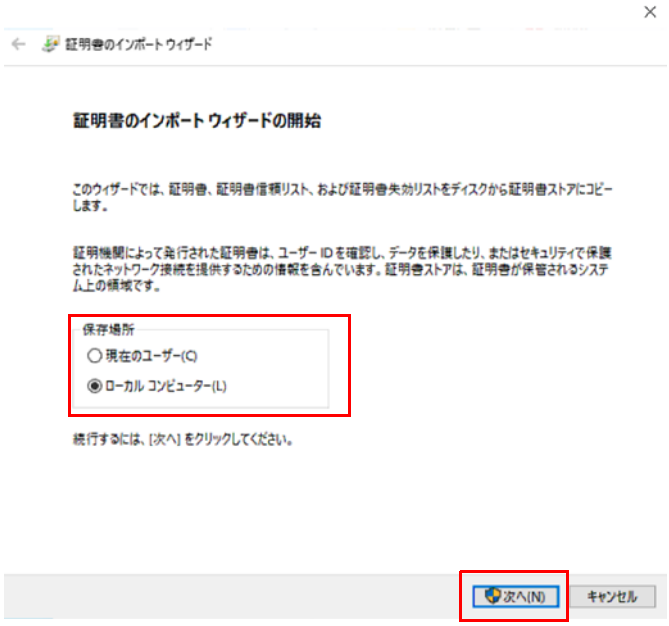
- Windows以外の端末への証明書のインストール方法は、ご使用の端末のマニュアルをご参照ください。

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。

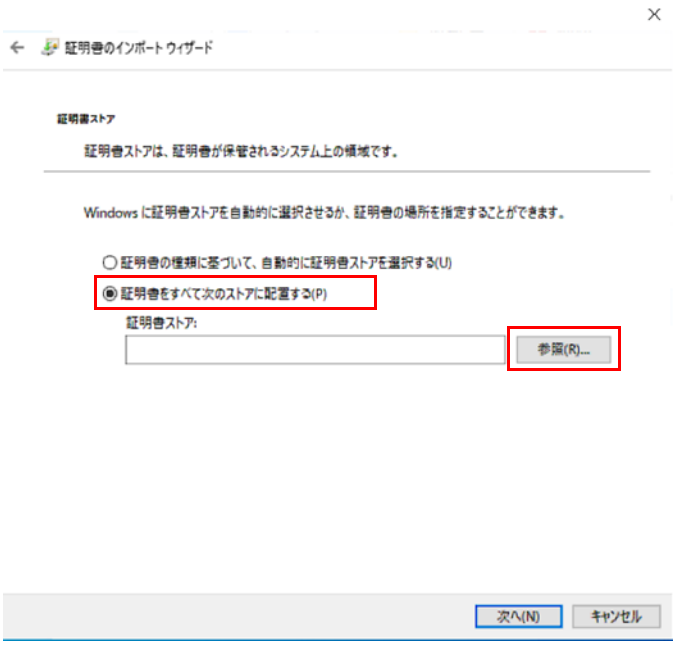
2 コピーした証明書ファイル「myCA.der」を右クリックし、「証明書のインストール」を選択します。



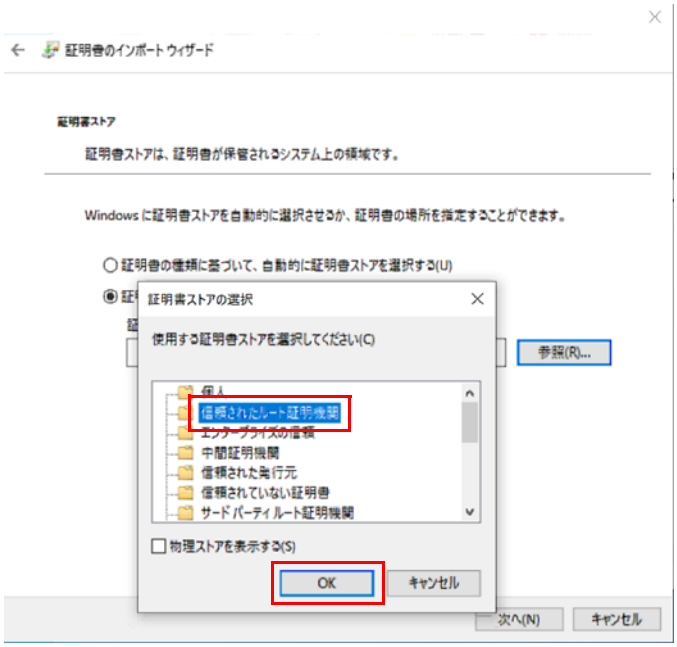
3 保存場所を「現在のユーザー」か「ローカルコンピュータ」を選択し、「次へ」をクリックします。



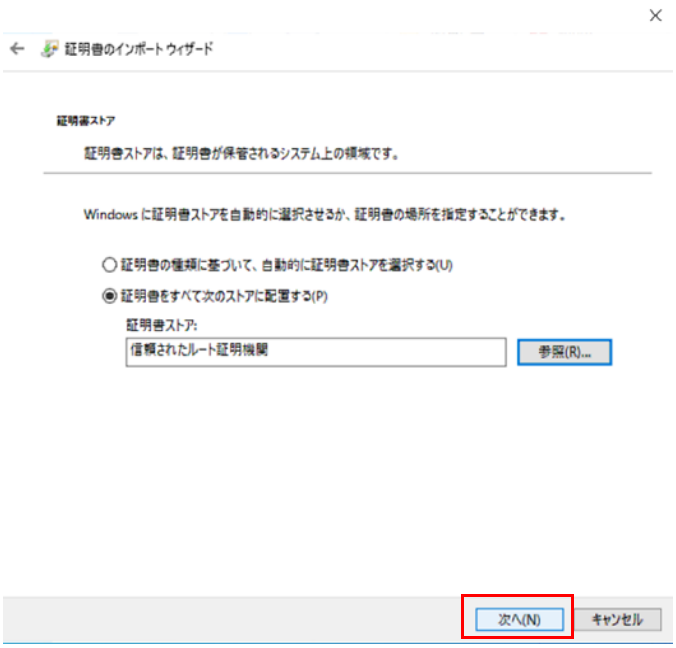
4「証明書をすべての次のストアに配置する」にチェックをして「参照」をクリックします。



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。

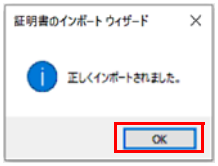


6「次へ」をクリックします。



7「完了」をクリックします。

8「OK」をクリックします。



キャッシュログ集計ツール

キャッシュログ収集ツールについて

キャッシュログ集計ツールは、インターネットキャッシュ機能のキャッシュエンジンのアクセスログを集計し、キャッシュ効果（キャッシュによる上位ネットワーク帯域の使用量削減分）の把握ができるデータを出力します。

●キャッシュログ集計ツールはインターネットキャッシュ機能 V4.1.0 またはそれ以降のバージョンをインストールするとエッジコンピューティングデバイス内に格納されます。

●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。
そのため、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。
この場合、キャッシュログ収集ツールでの解析はできません。

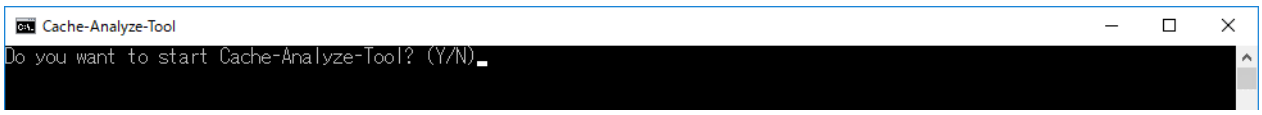
キャッシュログ集計ツールの使用方法

■キャッシュログ集計ツールの実行

1　エッジコンピューティングデバイス上でコマンドプロンプトを管理者権限で起動します（→ P.6）。

C:¥cygwin64¥cacheanalyze¥start-cacheanalyze.bat

2　コマンドプロンプトで【Y】キーを入力します。



実行結果が出力されます。

3　「継続するには何かキーを押してください ...」と表示されたら、任意のキーを押します。
コマンドプロンプトが終了します。

■キャッシュログ集計ツールの実行結果

キャッシュログ集計ツールを実行すると、次の結果ファイルが出力されます。

C:¥cygwin64¥cacheanalyze¥result¥cacheanalyzeresult_yyyymmddhhmmss.csv

※yyyymmddhhmmss は実行した日時
例）2020/12/1/12:00:00 に実行した場合
　cacheanalyzeresult_20201201120000.csv

□出力ファイル (csv) の見方

出力例 :

```
2020120811,http://domain1.com,8689,4726548,1,117
2020120818,https://domain2.com,512295,166918,42,151
2020120818,https://domain3.com,463977,1195366,58,223
```

①　②　③　④　⑤　⑥

出力された値は「,」で区切られいます。各値の内容については、次の① ~ ⑥をご覧ください。
①時間帯情報 (YYYYMMDDHH)※1 時間単位です
②対象のドメイン
③日時の時間帯でこのドメインから取得したデータのうち、キャッシュから取得したデータサイズ [byte]
④日時の時間帯でこのドメインから取得したデータのうち、配信元サーバから取得したデータサイズの合計値 [byte]
⑤日時の時間帯でこのドメインに対するリクエストのうち、キャッシュから取得したリクエストの合計数
⑥日時の時間帯でこのドメインに対するリクエストのうち、配信元サーバから取得したリクエストの合計数

4. 基本機能 - サーバファイルキャッシュ管理

サーバファイルキャッシュ機能の制御、設定、状況の確認などができます。

[実況状況] ー [簡易情報取得 ・ 手動制御]

各装置のサーバーキャッシュの同期状態が確認できます。なお、同期状態には以下の種類があります。

●計画同期
　大きいサイズの同期は、授業に影響しない時間帯（同期計画対象時間帯）に計画し、自動実行されます。急いでいる場合は、手動で同期できます。

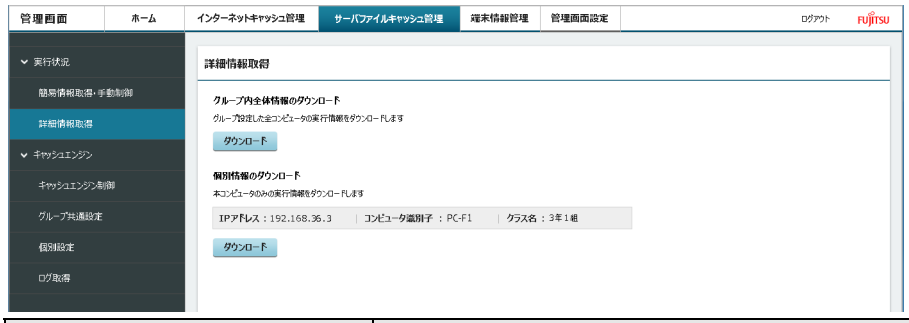
●調停同期
　各クラスの本装置が一度に重複して同期しない様計画し、自動実行されます。基本的に自動で実施されますが、急いでいる場合は、手動で同期できます。

割込実行

手動で同期の割込実行ができます。優先してキャッシュしたい装置がある場合は、「割込実行」をクリックしてください。

[実況状況] ー [詳細情報取得]

サーバファイルキャッシュ機能による同期状況を記載したファイルをダウンロードできます。



項目	説明
グループ内全体情報のダウンロード	グループ設定したすべてのコンピューターのサーバーキャッシュ実行情報（同期スケジュール管理ファイル）をダウンロードします。
個別情報のダウンロード	「個別情報のダウンロード」に表示されたコンピューターの実行情報（個別同期スケジュール管理ファイル）をダウンロードします。

[キャッシュエンジン] – [キャッシュエンジン制御]

キャッシュエンジンの起動、停止、再起動を行うことができます。

[キャッシュエンジン] – [グループ共通設定]

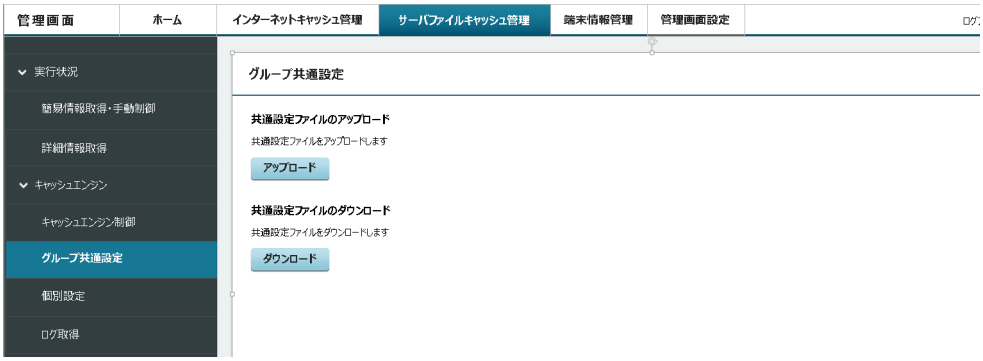
エッジコンピューティングデバイスを複数台使用する場合に、グループ設定したエッジコンピューティングデバイス間で共通の設定項目を設定できます。
設定の変更が必要な場合は、現在の設定ファイルをダウンロードしてファイルを編集した後、アップロードしてください。

●CommonList.conf
エッジコンピューティングデバイスを識別するための設定ファイルです。学校内ネットワークで使用する本製品の台数に応じて、それぞれのコンピューター部分の IP アドレス , コンピューター識別子 , クラス名を設定します。

●CommonMaster.conf
ダウンロードされますが設定変更は不要です。

●CommonSyncParam.conf
同期計画対象時間帯、日付切替時刻、どの同期処理（即時同期、調停同期、計画同期）を行うのかの指標となる値 など、本製品と学習支援アプリサーバとの同期関連のパラメータを設定します。

ファイルの変更方法については、『導入ガイド』の「サーバファイルキャッシュ機能のインストールと設定」をご覧ください。



項目	説明
共有設定ファイルのアップロード	作成した共通設定ファイルを読み込み、キャッシュエンジンの設定を変更します。
共有設定ファイルのダウンロード	キャッシュエンジンの現時点の共通設定をファイルとして保存します。

[キャッシュエンジン] – [個別設定]

キャッシュエンジンの個別設定ができます。また、キャッシュエンジンを初期化できます。設定の変更が必要な場合は、現在の設定ファイルをダウンロードしてファイルを編集した後、アップロードしてください。

●EachSyncParam.conf
学習支援アプリサーバのファイルと本製品のキャッシュとの同期を優先する時間帯を設定できます。

●AplCacheDefault.properties
学習支援アプリサーバの管理ファイル格納フォルダーと同期対象フォルダー、本製品の同期対象フォルダーを設定します。

●AplCacheUiDefault.properties
ダウンロードされますが設定変更は不要です。

ファイルの変更方法については、『導入ガイド』の「基本機能 - データキャッシュ機能（製品本体）」-「サーバファイルキャッシュ機能のインストールと設定」をご覧ください。

項目	説明
個別設定ファイルのアップロード	作成した個別設定ファイルを読み込み、キャッシュエンジンの設定を変更します。
個別設定ファイルのダウンロード	キャッシュエンジンの現時点の個別設定をファイルとして保存します。
キャッシュエンジンの初期化	キャッシュエンジンの設定を、ご購入時の状態に戻します。

[キャッシュエンジン] – [ログ取得]

サーバファイルキャッシュ管理機能のログファイルをダウンロードできます。

5. 基本機能 - 状態監視

動作状態監視ツール

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

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

●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

長期間製品を使用していると、通風孔にほこりがたまります。ほこりがたまった状態で使用し続けると、故障の原因となりますので、定期的にお手入れをしてください（→ P.96）。

お手入れナビとは

吸気孔、排気孔のお手入れ時期や、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、お手入れの時期をお知らせします。

表示されるメッセージ

「お手入れナビ」の表示するメッセージには、次のものがあります。

メッセージ	原因と対処
パソコンの空冷用通風路のお手入れ時期が来ました。	定期的なお手入れの時期が来ると表示されます。なお、定期的な通知は無効になっています。
	吸気孔と排気孔のほこりを取ってください。 吸気孔と排気口の場所については、「各部名称」（→ P.7）をご覧ください。
パソコン内部の空気の流れがさえぎられ、高温になっています。	ファンが高速で回転しているのに、製品本体内部の温度が低くならない場合に表示されます。
	・製品本体の周囲に 10cm 以上のすき間を空け、吸気孔や排気孔をふさがないようにしてください。 ・吸気口と排気口のほこりを取ってください。
パソコンの CPU ファンが正しく動作していません。	製品本体内部の温度が高いのに、ファンが高速で回転していない場合に表示されます。
	空冷用ファンの故障が考えられますので、電源を切った後、「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。

設定を変更する

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します。
通知時期を変更する方法については、「お手入れナビ」のヘルプをご覧ください。

POINT

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

6. 拡張機能 - セキュリティ （端末認証）

端末認証用の管理画面で設定を行います。エッジコンピューティングデバイスにアクセス可能なパソコンで設定してください。また、認証対象端末を登録するときに認証対象の端末が必要です。あらかじめご用意ください。

POINT

- 認証対象端末を登録する場合、登録対象の端末に「端末認証設定」をインストールする必要があります。詳しくは、『導入ガイド』の「拡張機能 - セキュリティ（タブレット端末）」をご覧ください。
- マニュアル内で記載されているアイコンには、次のような意味があります。

：エッジコンピューティングデバイスの設定や操作です。

：タブレット（パソコン）端末の設定や操作です。

管理画面へログイン

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

POINT

- IPアドレスにはコンピューター部分のIPアドレスをお使いください。
  コンピューター部分のIPアドレスが「192.168.1.3」の場合は次のようになります。
  http://192.168.1.3:10080/security/
- 端末認証を使用するために必要なアプリが起動するのに時間がかかるため、端末認証の管理画面へのログインは、OSが起動後充分待ってから実施してください。

ログイン画面が表示されます。

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

端末認証機能の管理画面が表示されます。

認証情報

認証情報には本製品に接続した端末の情報が記録されます。この情報を元に端末に対して、認証登録を行ったり、不正アクセスの確認を行ったりします。

認証対象端末一覧

認証情報には本製品に接続した端末の情報が記録されます。この情報を元に端末に対して、認証登録を行います。

項目	説明
認証登録モード	ON または、OFF をクリックして設定を変更します。 端末を認証登録するとき ON に設定します。通常は、OFF に設定します。
認証コード	未登録の端末が本製品に接続したときに、認証コードの入力が必要になります。なお、登録後、暗号鍵認証による接続になるため、本製品接続時の入力は不要になります。
登録端末一覧	登録端末の MAC アドレス、状況、認証登録日時、有効期限に関する情報が表示されます。
MAC アドレス詐称警告	MAC アドレス詐称の疑いがある接続があった場合、件数の横に「MAC アドレスの詐称を検出しました」と表示されます。この場合、「詐称検出一覧」（→ P.62）で、詐称された MAC アドレスを確認できます。

■認証端末の登録

重要

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

1 管理画面にログインし、「認証登録モード」を ON にします

POINT

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

しばらくすると、認証コードが表示されます。

2 登録対象の端末で次の操作を行います。

1. 画面右下の通知領域の をタップします。

（これ以降の画面は機種や状況により異なります）

現在利用できる無線 LAN の SSID の一覧が表示されます。

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

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

POINT

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

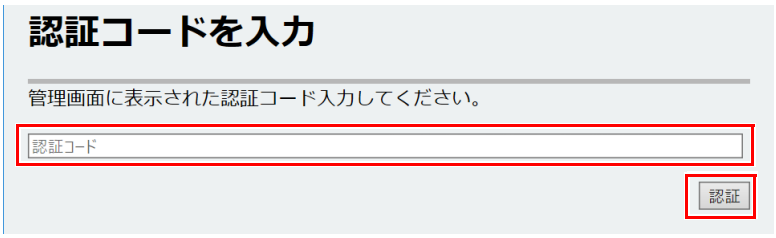
3. 「接続」をタップします。

認証コード入力画面が表示されます。

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

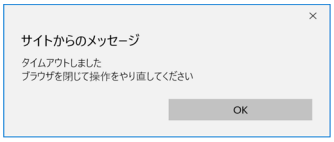
POINT

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



POINT

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



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

認証対象端末一覧に、無線 LAN 接続した端末が追加されます。

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

4 管理画面で「認証登録モード」を OFF にします。

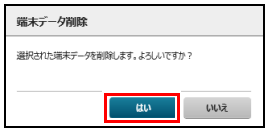
■認証端末の削除

次の手順で登録済みの認証端末を削除できます。

1 削除対象の端末にチェックを付け、「削除」をクリックします。

「端末データ削除」が表示されます。

2 「はい」をクリックします。



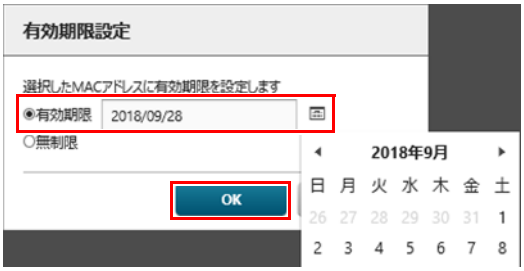
登録済み認証端末のデータが削除されます。

■ 有効期限の設定

登録した認証端末に有効期限を設定できます。有効期限をすぎると状態が「有効期限オーバー」と表示され、本製品に接続できなくなります。長期間同じ鍵を使い続けると、ミスや事故、第三者からの不正アクセスなど鍵の漏えいの可能性が高まります。有効期限を設定して定期的な鍵の更新をお勧めします。

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

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



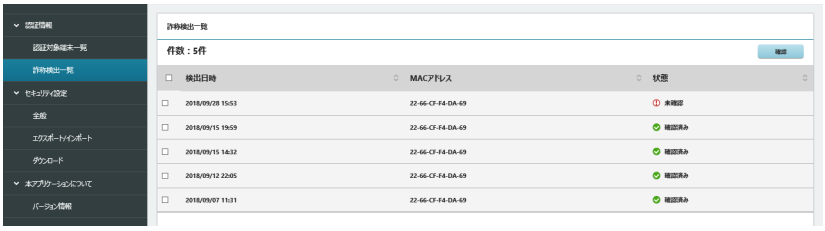
有効期限が設定されます。

■ 詐称の検出

MAC アドレスの詐称が検出されると下図のようにメッセージが表示されます。詳細をクリックすると「詐称検出一覧」（→ P.62）へ画面遷移します。

詐称検出一覧

詐称検出一覧には、登録済み端末と同じ MAC アドレスを持つ端末が、本製品との暗号鍵認証に失敗した場合に記録されます。この一覧では、詐称された MAC アドレスを確認できます。



■ MAC アドレス詐称の状態変更

次の手順で「未確認」を「確認済み」の状態に変更できます。

1 チェックボックスにチェックを付け、「確認」をクリックします。

POINT

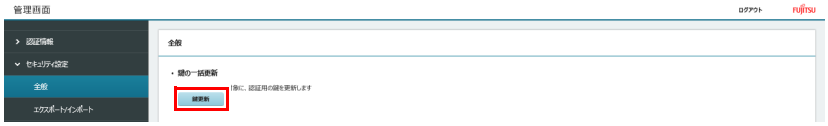
▸「詐称検出一覧」の状態がすべて「確認済み」になるまで、「認証対象端末一覧」に詐称検出のメッセージが表示されます。

セキュリティ設定 - 全般

■鍵の一括更新

鍵が漏えいした場合は、早急に鍵の更新を実施してください。登録済みの全端末に対して、認証用の鍵を更新することができます。

1 **「鍵更新」をクリックします。**

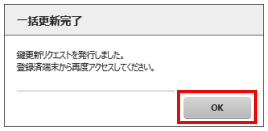


「鍵の一括更新」が表示されます。

2 **「OK」をクリックします。**

「一括更新完了」が表示されます。

3 **「OK」をクリックします。**



登録済み端末の認証用の鍵が更新され、「認証対象端末一覧」（→ P.59）の状態が「鍵更新待ち」になります。登録済み端末を本製品に接続すると端末の鍵更新が実行されます。更新が完了すると、状態が「登録完了」になります。

セキュリティ設定 - エクスポート／インポート

登録済み端末データをエクスポートしたり、インポートしたりすることができます。詳しくは、「端末認証機能の設定のバックアップと再設定」（→ P.94）をご覧ください。

セキュリティ設定 - ダウンロード

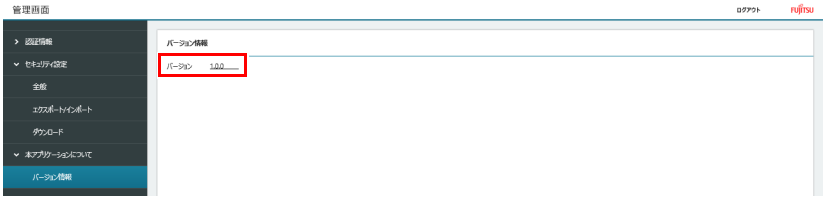
登録済み端末の接続ログ（connect.log）と MAC アドレス詐称端末ログ（sasyo.log）をダウンロードできます。

1 **「ダウンロード」をクリックします。**

「ダウンロード」フォルダーに「seclog.zip」がダウンロードされます。

本アプリケーションについて - バージョン情報

端末認証機能のバージョンを確認できます。



7. 拡張機能 - ネットワーク

優先接続設定

優先接続設定を「ON」にすると、優先的にネットワークを使用することが出来ます。

POINT

▸無線LAN接続台数表示のインストール方法については、『導入ガイド』の「優先接続設定のインストールと設定」をご覧ください。

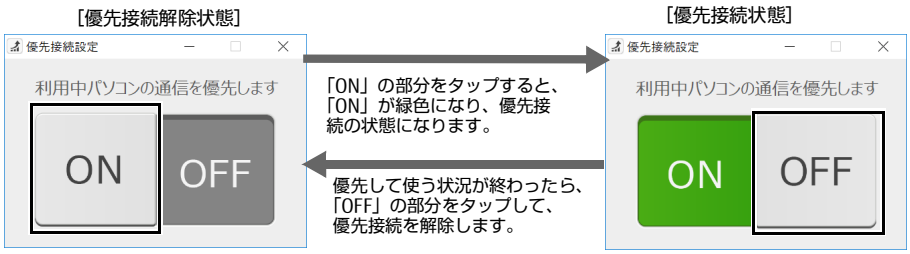
優先接続設定の起動

この機能は、「優先接続設定」をインストールしたパソコン、タブレット端末のみで使用できます。次の手順で「優先接続設定」を起動します。

1　ネットワークへ接続します。（設定済みの SSID：SSID-5G-F2 など）

2　 →「優先接続設定」の順にタップします。
「優先接続設定」が起動します。

3「優先接続設定」ウィンドウが表示されたら、「ON」または「OFF」を押して切り替えます。



POINT

▸優先接続設定で優先されるのは本製品1台につき、端末1台のみです。
▸本製品1台に対して複数の端末が優先接続を設定した場合、最後に設定した端末が優先されます。

8. 拡張機能 - 端末情報収集

端末情報管理

管理画面で本製品の診断情報の確認、収集した情報のメール送信に関する設定などができます。無線 LAN 診断は、本製品に無線接続したタブレット端末に対して実行されます。

POINT

- 本機能を使用する場合、タブレット端末に端末情報収集ツールをインストールしておく必要があります。詳しくは、『導入ガイド』のをご覧ください。
- 次の設定項目について、設定の変更はお勧めしません。変更が必要な場合は、『導入ガイド』の「セットアップ」をご覧ください。
  - [収集・通知] － [稼働時間]
  - [収集・通知] － [メール通知設定]
  - [収集・通知] － [情報収集設定（コンピュータ）]
  - [収集・通知] － [情報収集設定（端末）]
  - [収集・通知] － [SMTP 設定]

バッテリー劣化診断

管理画面で、バッテリーの状態を確認できます。

[解析結果] － [バッテリー状況一覧]

タブレット端末のバッテリー状況の情報を収集し、交換が必要な端末の台数を表示します。また、「一覧データダウンロード」をクリックすると、交換対象のタブレット端末について型名や製造番号などバッテリー状況一覧の情報を CSV ファイルとしてダウンロードできます。

無線 LAN 診断

管理画面で、無線 LAN 診断の状況を確認できます。

[解析結果] – [無線 LAN 診断状況一覧]

無線 LAN に関する診断情報が表示されます。

各エラーコードが示す無線 LAN の状況は次のとおりです。診断状況の詳細や対処方法については、「無線 LAN 診断で表示されるエラーメッセージ」(→ P.116)をご覧ください。

エラーコード	無線 LAN 診断状況
1	AP ログイン失敗
3	IP なし
4	DHCP 失敗
7	接続の失敗
8	RSSI 低下
9	干渉
10	認証またはその他端末問題
12	AP 設定異常
13	AP 異常

CSV ファイルとしてダウンロードすることもできます。

1 「絞込条件」をクリックすると、本体型名、シリアル番号、エラーコード、発生日などで絞り込むことができます。

2 「一覧データダウンロード」をクリックすると、無線 LAN 診断状況一覧を CSV ファイルとして保存できます。

3 「AP」「端末」をクリックすると、そのエラーに関する情報だけを、CSV ファイルとして保存できます。

稼働時間

管理画面で本製品に接続した端末の稼働状況を確認できます。

[解析結果] – [端末稼働時間一覧]

タブレット端末の接続台数の情報を収集し、CSV ファイルとしてダウンロードできます。

POINT

- 端末稼働台数データは無線LAN診断状況一覧のデータを使用しています。そのため、無線LAN診断状況一覧のデータを削除すると端末稼働台数データも削除されます。

項目	説明
ICT 授業日数	ICT 授業を行った回数（エッジコンピューティングデバイスの無線 LAN に端末から接続があった日の総数）
接続時間	エッジコンピューティングデバイスの無線 LAN に 1 台以上の端末が接続を行った時間の累計
平均接続時間	接続時間の一日平均 (接続時間を ICT 授業日数で割った値)
接続台数	端末の最大接続台数の累計
平均接続台数	接続台数の一日平均 (接続台数を ICT 授業日数で割った値)
コンピュータ稼働時間	エッジコンピューティングデバイスの累計稼働時間

無線 LAN 接続台数表示

この表示は、「無線 LAN 接続台数表示」をインストールしたパソコン、タブレット端末のみで使用できます。本製品に接続している端末の台数を表示できます。

POINT

- 無線LAN接続台数表示のインストール方法については、『導入ガイド』の「無線LAN接続台数表示」をご覧ください。

無線 LAN 接続台数表示の起動

次の手順で無線 LAN 接続台数表示を起動します。

1. **ネットワークへ接続します。（設定済みの SSID：SSID-5G-F2 など）**
2. **→「無線 LAN 接続台数表示」の順にタップします。**
   画面の右下に、現在の接続台数が表示されます。表示される接続台数には、先生が利用しているパソコン、タブレット端末の台数も含まれます。
   例：先生用端末 1 台、生徒用端末 40 台の場合、41 台と表示されます。

表示は、定期的に更新されます。

9. 拡張機能 - 画面共有

Intel Unite

Intel Unite については、『ユーザーガイド』をご覧ください。

5

第 5 章
バックアップと復元

システムイメージやアクセスポイントの設定のバックアップ、復元について説明します。

1. 本製品のバックアップと復元 69
2. リカバリ USB メモリを使ったリカバリ 79
3. 内蔵ディスク内のデータを使った回復方法 84
4. アクセスポイントの設定のバックアップと再設定 86
5. 管理画面の設定と収集データのバックアップと再設定 88
6. 証明書ファイルのバックアップと再設定 90
7. 端末認証機能の設定のバックアップと再設定 94

1. 本製品のバックアップと復元

Windows が起動しなくなった場合や、データを誤って紛失してしまった場合に備え、大切なデータのバックアップを行うようにしてください。

重要

▶バックアップと復元の操作をするためには、本製品に画面表示機器、USBキーボード、USBマウスを接続してください。

システムイメージバックアップについて

システムイメージバックアップとは、C ドライブ全体をシステムイメージとしてバックアップできる機能です。
現在の本製品の状態をそのままバックアップするので、インターネットの設定やインストールしたアプリなどの情報を保存できます。復元するとシステムイメージを作成した時点の状態に復元されます。
トラブルに備えて、本製品のセットアップが完了した後、本製品が快適に使用できている状態のときにバックアップすることをお勧めします。

システムイメージバックアップの注意事項

●すべてのデータのバックアップ／復元を保証するものではありません
すべてのデータのバックアップ／復元を保証するものではありません。また、著作権保護された映像（デジタル放送の録画番組など）や音楽などはバックアップ／復元できない場合があります。

●万が一、システムイメージで復元できないときのために、大事なファイルは個別にバックアップしてください

●本製品に不具合が起こっているときは、システムイメージをバックアップしないでください
システムイメージバックアップは、本製品の C ドライブをそのままの状態で保存するため、不具合も保存されてしまい、復元時に不具合も復元してしまいます。

●システムイメージから復元をする場合は、復元する項目を個別に選択できません
現在のアプリ、システム設定、およびファイルやフォルダーは、システムイメージバックアップをとった時点の内容ですべて上書きされます。

●システムイメージバックアップは 1 つの保存先に 1 つしかとれません
保存先ドライブにすでにシステムイメージがある場合、「このコンピューターに関する既存のシステムイメージは、上書きされる場合があります。」と警告が表示され、上書きされます。以前にとったシステムイメージバックアップを消したくない場合は別の保存先を用意してください。

●管理者アカウントで Windows にサインインしていることを確認してください
セットアップ時に作成したアカウントは管理者アカウントです。標準アカウントでサインインしている場合は、「ユーザーアカウント制御」ウィンドウで管理者アカウントのパスワードを入力してバックアップしてください。

●システム修復ディスクを作成する場合は、外付けの光学ドライブが必要です。
外付け光学ドライブは USB 接続のものを用意してください。USB 接続以外の接続方式では正常動作しない場合があります。

●回復ドライブを作成する場合は、USB メモリが必要です。32GB 以上の空き容量がある USB メモリの利用をお勧めします（→ P.78）。

●Windows が起動しなくなった場合、システムイメージのデータだけでは復元を実行できません。
システムイメージのほかに、回復ドライブ（→ P.78）やシステム修復ディスク（→ P.78）などが必要です。
・ システム修復ディスクの場合、CD-R で作成できます。
・ 回復ドライブの場合、システムファイルに問題が発生している場合や SSD 内のデータがすべて削除されている場合でも Windows が起動する状態に戻せます。
このため、万が一の場合に備え、システムイメージとあわせて、回復ドライブの作成をお勧めします。

システムイメージをバックアップする場所

POINT

▶すべての周辺機器の動作を保証するものではありません。

●外付けハードディスク
直接システムイメージをバックアップできます。外付けハードディスクは USB 接続のものを用意してください。USB 接続以外の接続方式では正常に動作しない場合があります。
バックアップの方法については、「外付けハードディスクにバックアップする方法」（→ P.70）をご覧ください。

システムイメージをバックアップする

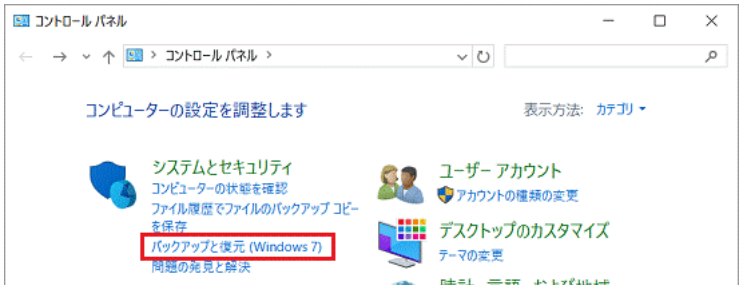
外付けハードディスクにバックアップする方法

1 外付けハードディスクを本製品に接続します。

2 「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。

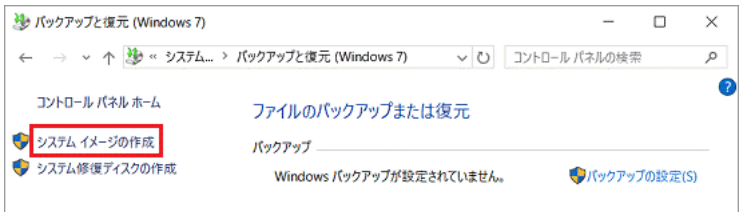
3 「バックアップと復元（Windows 7）」をクリックします。

POINT
▸名称は「Windows 7」ですが、Windows 10で利用できる機能です。



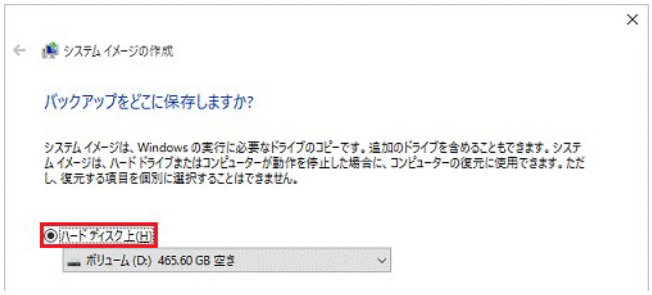
「バックアップと復元（Windows 7）」が表示されます。

4 「システムイメージの作成」をクリックします。



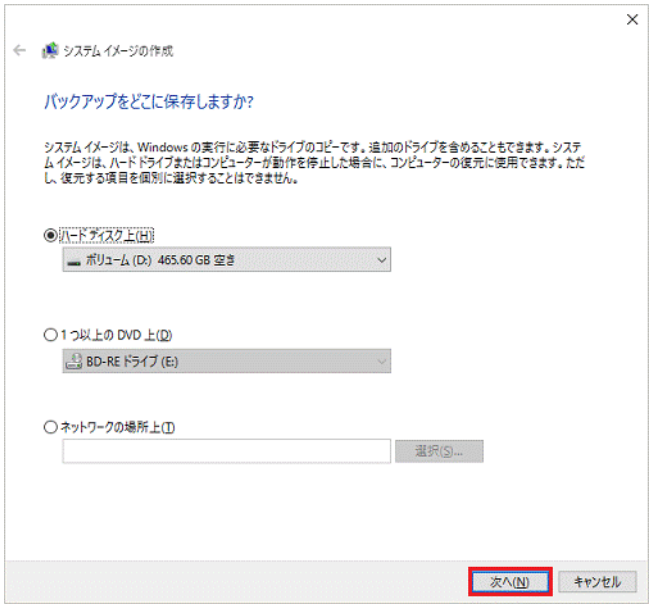
「バックアップをどこに保存しますか？」と表示されます。

5 「ハードディスク上」をクリックし、接続した外付けハードディスクが表示されていることを確認します。
下の図は、外付けハードディスクが D ドライブの場合です。



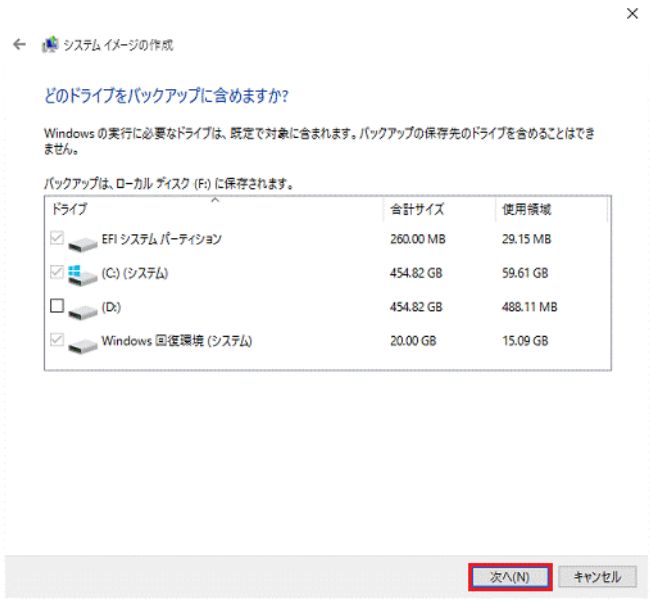
POINT
▸バックアップ先の外付けハードディスクが表示されていない場合は「下向きの三角」をクリックし、表示される一覧から選択します。
▸「ハードディスク上」に「このドライブはNTFSでフォーマットされていないため、システムイメージを保存することはできません。」と表示されている場合は、外付けハードディスクをNTFSでフォーマットする必要があります。

6「次へ」をクリックします。



バックアップ元と、バックアップ先以外にもドライブが存在する場合、「どのドライブをバックアップに含めますか？」と表示されます。

7 システムイメージと一緒にバックアップしたいドライブがある場合は、クリックしてチェックを付け、「次へ」をクリックします。
表示されない場合は、手順 8 に進みます。



「バックアップの設定を確認します」と表示されます。

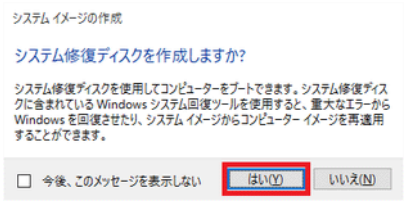
8「バックアップの開始」をクリックします。

バックアップが開始されます。バックアップが終了すると、「システム修復ディスクを作成しますか？」と表示されます。

9 状況に応じて、次の操作を行います。

・システム修復ディスクを作成する場合

1. 外付け光学ドライブを接続します。
2. 「はい」をクリックし、画面の指示に従いシステム修復ディスクを作成したら、手順 10 に進みます。

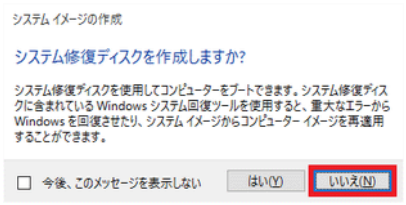


POINT

▸システム修復ディスクとは、Windowsが起動できない状態になったときに、システムイメージを読み込んで復元するために使用するディスクです。ここで「いいえ」を選択しても、後から作成できます（→P.78）。

・システム修復ディスクを作成しない場合

「いいえ」をクリックし、手順 10 に進みます。



「バックアップは正常に完了しました。」と表示されます。

10「閉じる」をクリックします。

システムイメージを復元する

POINT

▶回復ドライブまたはシステム修復ディスクが必要です。作成方法については、次の項目をご覧ください。
・回復ドライブを使用する場合
「回復ドライブ（USB）を作成する」（→ P.78）
・システム修復ディスクを使用する場合
「システム修復ディスクを作成する」（→ P.78）

1　本製品の電源を切ります（→ P.26）。

2　データが保存されている外付けハードディスクを接続します。

重要

▶システムイメージの復元に使用しない外付けハードディスクやUSBメモリなどの各種ストレージ機器は、すべて取り外してください。

3　次の手順で回復ドライブまたはシステム修復ディスクを起動します。

・回復ドライブを使用する場合

1. 回復ドライブとして作成した USB メモリを USB コネクタに接続します。
2. 【F12】キーを押したまま、本製品の電源を入れます。
3. 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.26）をご覧ください。
   起動メニューが表示されます。
4. キーボードの【↓】キーを押して、使用する項目を選択します。
5. 接続している USB メモリの項目を選択し、【Enter】キーを押します。

POINT

▶起動方法（起動モード）を選択する画面が表示された場合は、「UEFI」から始まる項目を【↑】キーまたは【↓】キーで選択して、【Enter】キーを押します。
▶「UEFI」から始まる項目にUSBメモリの表示がない場合は、USBメモリが正しく接続されていることを確認して、【Ctrl】＋【Alt】＋【Delete】キーを押して本製品の再起動を行い、続けて【F12】キーを押して、起動メニューを表示してください。
▶「Press any key to boot from CD or DVD...」と表示された場合は、【スペース】キーなどを押します。
起動メニューに戻ってしまう場合は、はじめからやり直します。

・システム修復ディスクを使用する場合

1. 外付け光学ドライブを USB コネクタに接続します。
2. 【F12】キーを押したまま、本製品の電源を入れます。
3. 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.26）をご覧ください。
   起動メニューが表示されます。
4. システム修復ディスクを外付け光学ドライブにセットします。
   ディスクをセットしたまま、【Ctrl】＋【Alt】＋【Delete】キーを押して、本製品の再起動を行い、続けて【F12】キーを押します。
   起動メニューが表示されます。
5. データの読み込みが終了し光学ドライブが停止してから、ディスクをセットした外付け光学ドライブ（例：GENERIC DVD-ROM）を選択し、【Enter】キーを押します。

POINT

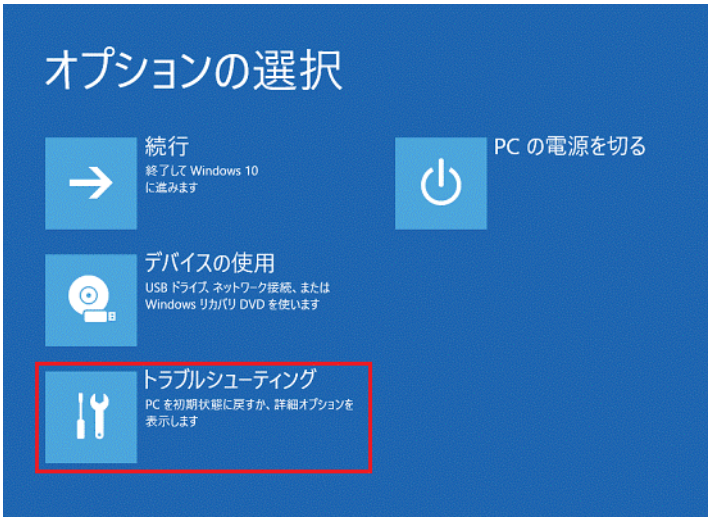
▶起動方法（起動モード）を選択する画面が表示された場合は、「UEFI」から始まる項目を【↑】キーまたは【↓】キーで選択して、【Enter】キーを押します。
▶「UEFI」から始まる項目に外付け光学ドライブの表示がない場合は、USB機器が正しく接続されていることを確認して、【Ctrl】＋【Alt】＋【Delete】キーを押して本製品の再起動を行い、続けて【F12】キーを押して、起動メニューを表示してください。
▶「Press any key to boot from CD or DVD...」と表示された場合は、【スペース】キーなどを押します。

「キーボードレイアウトの選択」と表示されます。

4　「Microsoft IME」をクリックします。

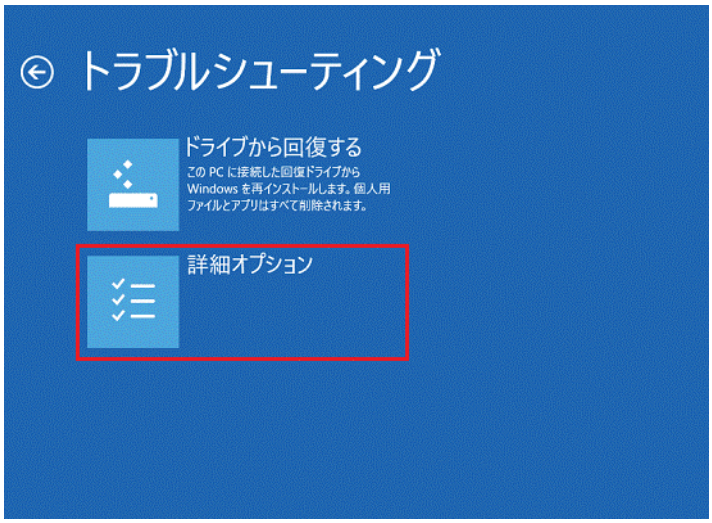
「オプションの選択」と表示されます。

5「トラブルシューティング」をクリックします。



「トラブルシューティング」が表示されます。

6「詳細オプション」をクリックします。



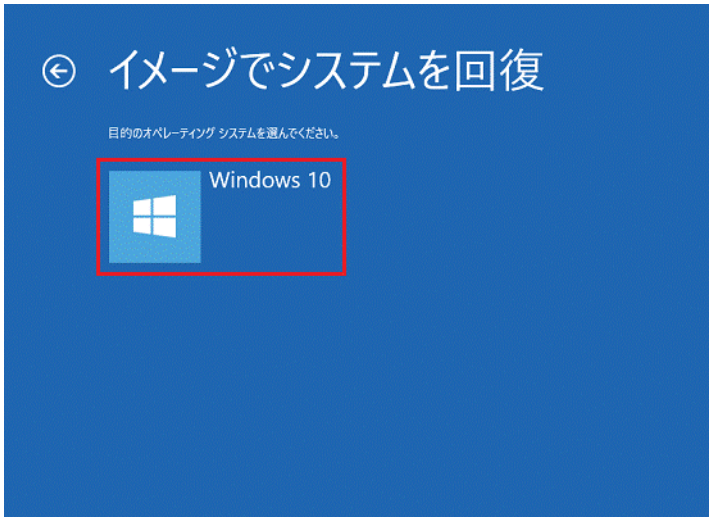
（回復ドライブから起動した場合）

「詳細オプション」と表示されます。

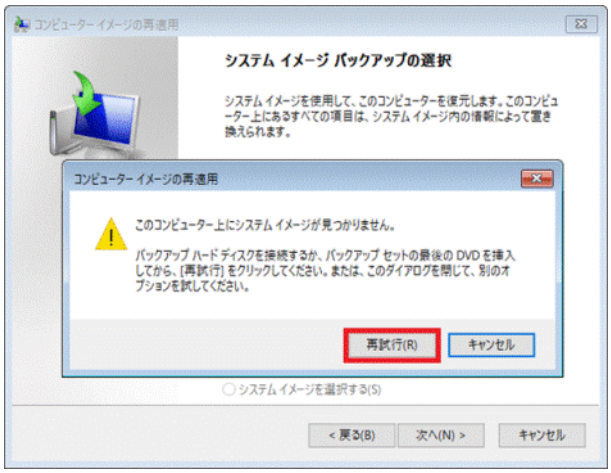
7「イメージでシステムを回復」をクリックします。

しばらくすると「イメージでシステムを回復」と表示されます。

8「Windows 10」をクリックします。



9「このコンピューター上にシステムイメージが見つかりません。」と表示された場合は、「再試行」をクリックします。表示されない場合は、手順 10 に進みます。

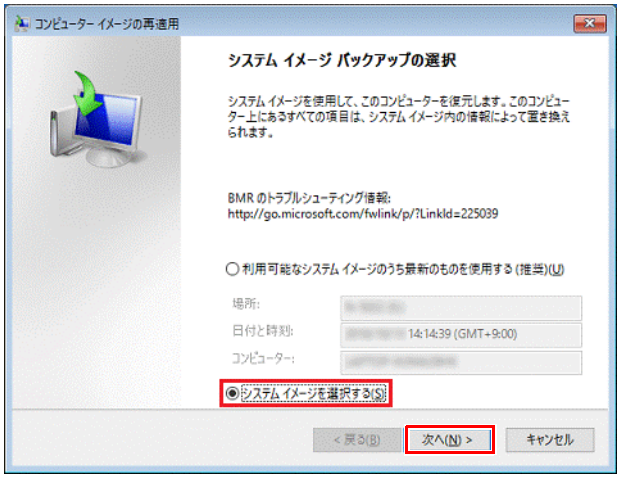


重要

- システムイメージをバックアップしたドライブをセットしているにも関わらず、「このコンピューター上にシステムイメージが見つかりません。」と表示される場合は、システムイメージのファイルにアクセスできていません。
  再接続などを行い、Windows上でシステムイメージをバックアップしたドライブにアクセスできることを確認してから、もう一度、お試しください。

「システムイメージのバックアップの選択」が表示されます。

10「システムイメージを選択する」をクリックし、「次へ」をクリックします。

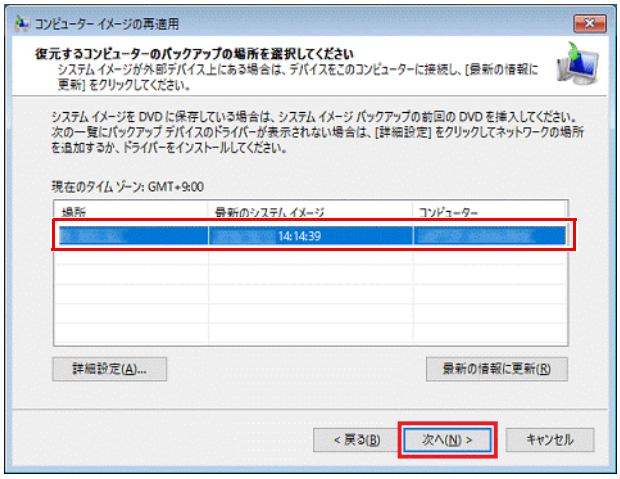


「復元するコンピューターのバックアップの場所を選択してください」と表示されます。

11 復元したいシステムイメージの場所をクリックし、「次へ」をクリックします。

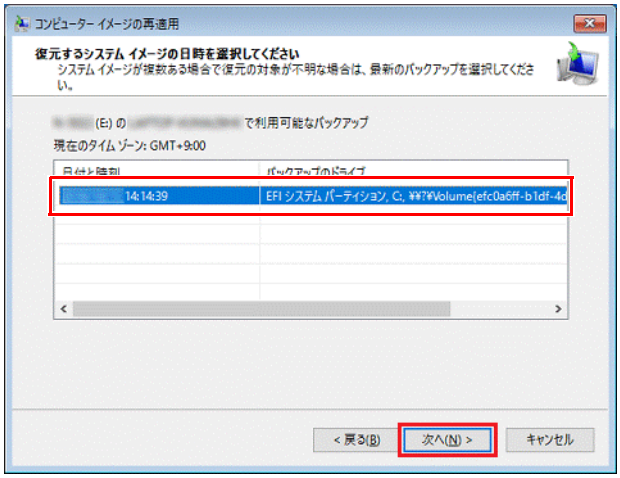
POINT

▸「他の復元方法を選択してください」と表示されたら、「次へ」をクリックします。



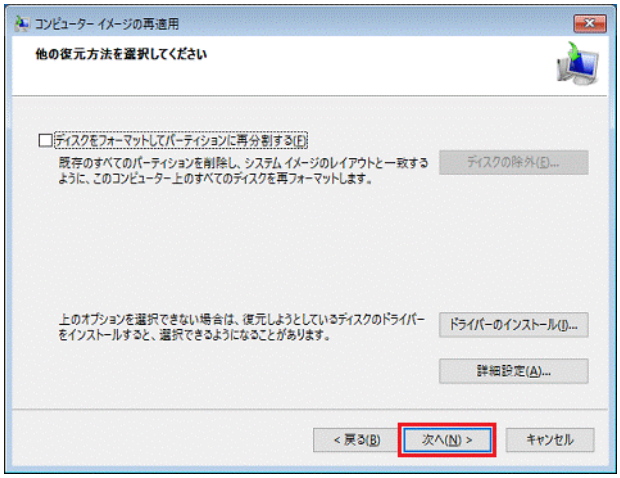
「復元するシステムイメージの日時を選択してください」と表示されます。

12 復元したい日時のシステムイメージをクリックし、「次へ」をクリックします。



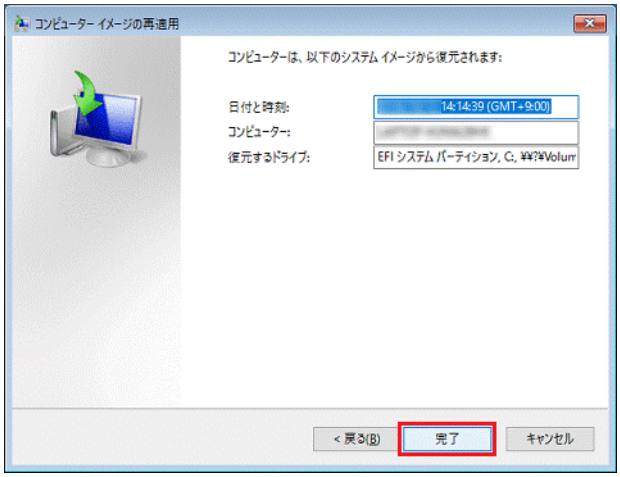
「他の復元方法を選択してください」と表示されます。

13「次へ」をクリックします。



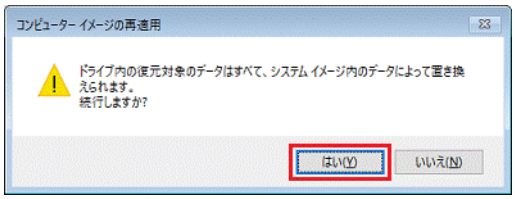
「コンピューターは、以下のシステムイメージから復元されます」と表示されます。

14「完了」をクリックします。



「ドライブ内の復元対象のデータはすべて、システムイメージ内のデータによって置き換えられます。」と表示されます。

15「はい」をクリックします。



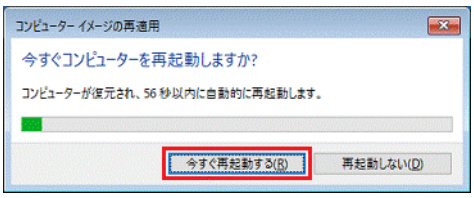
システムイメージからの復元が開始されます。完了するまで、そのまましばらく待ちます。

POINT

▸「以下のディスクを挿入してください」と表示された場合は、メッセージ内に表示されたラベルの媒体をセットして、「OK」ボタンをクリックします。

復元が完了したら、「今すぐコンピューターを再起動しますか？」と表示されます。

16「今すぐ再起動する」をクリックします。



回復ドライブ （USB） を作成する

Windows 10 には、USB メモリを使って、回復ドライブ（USB）を作成する機能があります。

重要

- 万が一に備え、回復ドライブ（USB）をできるだけ早く作成しておくことをお勧めします。
- 回復ドライブ（USB）の作成には、USBメモリが必要です。32GB以上の空き容量があるUSBメモリの利用をお勧めします。
- 管理者アカウントでWindowsにサインインしていることを確認してください。

1 「コントロールパネル」を表示します（→ P.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」の「問題の発見と解決」をクリックします。

3 「コンピューターの問題のトラブルシューティング」ウィンドウ左下の「回復」をクリックします。

4 「高度な回復ツール」の「回復ドライブの作成」をクリックします。

5 「ユーザーアカウント制御」ウィンドウが表示されたら、「はい」をクリックします。

6 「回復ドライブの作成」ウィンドウが表示されたら、「次へ」をクリックします。

POINT

- 「システムファイルを回復ドライブにバックアップします。」は、チェックを付けたままにしてください。

7 「USB フラッシュドライブの接続」と表示されたら、USB メモリを接続します。

8 「USB フラッシュドライブの選択」と表示されたら、「使用可能なドライブ」に保存先として使用するドライブが表示されていることを確認し、「次へ」をクリックします。

POINT

- 「使用可能なドライブ」に複数のドライブが表示されている場合は、使用するドライブをクリックします。

9 「回復ドライブの作成」と表示されたら、「作成」をクリックします。

10 「回復ドライブの準備ができました」と表示されたら、「完了」をクリックします。
作成した回復ドライブ（USB）を大切に保管してください。

11 「閉じる」をクリックします。

システム修復ディスクを作成する

Windows 10 には、光ディスクを使って、システム修復ディスクを作成する機能があります。

POINT

- CD-R、CD-RW、DVD-R、DVD-RW、DVD-R DL、DVD+R、DVD+RW、DVD+R DL、BD-R、BD-R DL、BD-R XL ディスクでシステム修復ディスクを作成できます。
- 外付け光学ドライブは、USB接続のものを用意してください。USB接続以外の接続方式では正常に動作しない場合があります。
- 管理者アカウントでWindowsにサインインしていることを確認してください。
- システム修復ディスクは、空のCD-Rで1枚程度の容量に収まります。

1 起動しているアプリをすべて終了します。

2 「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。

3 「バックアップと復元（Windows7）」をクリックします。
「ファイルのバックアップまたは復元」が表示されます。

4 「システム修復ディスクの作成」をクリックします。
「CD/DVD ドライブを選択し、空のディスクをドライブに挿入してください。」と表示されます。

5 空のディスクを外付け光学ドライブにセットして、「ディスクの作成」をクリックします。
ディスクの作成が開始されます。
完了するまで、しばらく待ちます。

重要

- ディスクへの書き込み中に、強制サインアウトをすると、光学ドライブがロックされ、ディスクを取り出せません。
- ディスクの書き込みも失敗してしまうため、ディスクの書き込み中はサインアウトしないでください。

「システム修復ディスクを使用」と表示されます。

6 ディスクを取り出し、必要に応じて、ディスク名をディスクのレーベル面に記入します。

POINT

- レーベル面に記入するときは、ボールペンや鉛筆などの先の硬いものは使わないでください。ディスクに傷が付くおそれがあります。

7 「閉じる」をクリックします。

8 「OK」をクリックします。

2. リカバリ USB メモリを使ったリカバリ

カスタムメイドオプションで「リカバリ USB メモリ追加」を選択して本製品をご購入された場合は、内蔵ディスクをリカバリすることができます。

重要

- 本製品に、リカバリデータは標準添付されておりません。また、リカバリデータの書き出しはできません。

内蔵ディスク構成

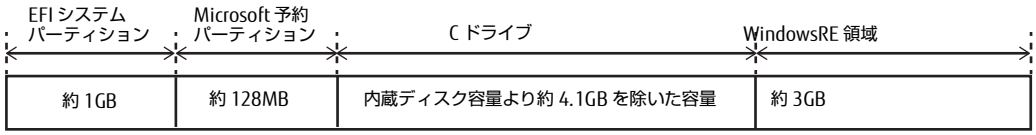
内蔵ディスクは、次の領域から構成されています。

●「OS、アプリ（ソフトウェア）、ドライバーなどの領域と空き領域（C ドライブ）」
（内蔵ディスク容量より約 4.1GB を除いた容量）

●「Windows RE 領域」（約 3GB）

●「EFI システムパーティション」（約 1GB）

●「Microsoft 予約パーティション」（約 128MB）



POINT

- 「EFIシステムパーティション」、「Microsoft予約パーティション」、「Windows RE領域」は、Windowsからは見えない領域です。
- 各パーティションのファイルシステムは、EFIシステムパーティションの区画のみFAT32となります。そのほかのパーティションは、NTFSとなります。

内蔵ディスク全体をリカバリする

内蔵ディスク全体をリカバリします。変更したドライブ構成を元に戻す場合などにも、この作業が必要です。

注意事項

●内蔵ディスク全体をリカバリすると、内蔵ディスクのすべてのデータが削除されます。必要に応じて事前にバックアップしてください。

●内蔵ディスク全体をリカバリするときは、「リカバリ USB メモリ」が必要です。

●本製品から、外付けハードディスク、プリンターなどすべての周辺機器を、必ず取り外してください。

●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。あらかじめご用意ください。

重要

- デバイスドライバーのインストールが必要な機器は、使用しないでください。リカバリに失敗する場合があります（例：指紋認証／手のひら静脈センサー付きキーボード、タッチ機能付きディスプレイなど）。
- DisplayPort接続以外の画面表示機器を使用する場合は、変換アダプタが必要になります。HDMI接続の画面表示機器を使用する場合は、添付のDP-HDMI変換アダプタをご使用ください。その他の画面表示機器を接続する場合は、ご使用の画面表示機器にあった変換アダプタをご用意ください。

●モデルやカスタムメイドオプションの選択によって、内蔵ディスク全体をリカバリした後に、アプリやドライバーのインストールが必要になります。詳しくは「セットアップ後のインストール状態」（→ P.83）をご覧ください。

●セキュリティチップ搭載機種やセキュリティ機能内蔵機種でフォルダーやファイルの暗号化を行っている場合は、内蔵ディスク全体をリカバリする前に復元用のバックアップをしてください。復元用のバックアップデータがないと、データが読み出せないことがあります。これによる損害などの責任は一切負いかねますので、あらかじめご了承ください。

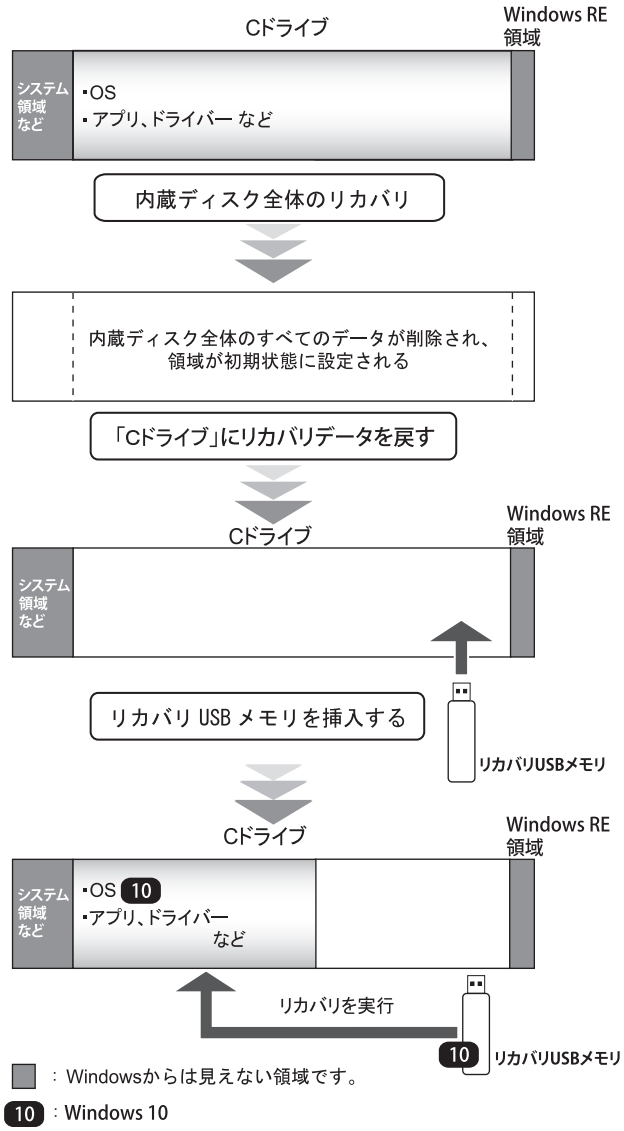
●内蔵ディスク全体をリカバリするには時間がかかります。時間に余裕をもって、操作してください。

●外部メディアを接続したまま、リカバリ作業や内蔵ディスクの領域設定を行うと、外部メディアに保存されているデータが削除される場合があります。

内蔵ディスク全体をリカバリする場合の考え方

いったん内蔵ディスク内のすべてのデータが削除され、領域がご購入時の状態や OS を切り替えた初期状態に設定されます。続いて C ドライブにリカバリデータを戻し、その後リカバリを実行します。

■Windows 10 にリカバリする場合



内蔵ディスク全体をリカバリする前の準備

内蔵ディスク全体をリカバリする前に、次の準備を行ってください。

リカバリ USB メモリを用意する

ディスプレイ、USB キーボード、USB マウスを本製品に接続する。

1 ディスプレイを本製品の DisplayPort コネクタに接続します。

2 USB キーボードと USB マウスを、本製品の USB コネクタに接続します。

BIOS の設定を確認する

BIOS の設定をご購入時から変更している場合は、ご購入時の設定に戻します。
BIOS セットアップの操作方法については、『導入ガイド』をご覧ください。

重要

▸設定が異なると、Windows 10が起動しなかったり、正常にリカバリが完了しなかったりすることがありますので、必ず確認してください。

■Windows 10 の BIOS 設定

POINT

▸「BIOSパスワード」や「管理者用パスワード」を設定されている場合は、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 BIOS セットアップ画面の「終了」メニューから「標準設定値を読み込む」を実行します。

2 次にメニューから設定項目を選択し、次のとおりに設定してください。

メニュー	設定項目	設定値
詳細	ネットワークスタック	
	ネットワークスタック	使用する
	TPM（セキュリティチップ）設定	
	セキュリティチップ	有効にする
セキュリティ	セキュアブート設定	
	セキュアブート機能	使用する

注 : 本製品には、チップセット内蔵のセキュリティ機能として Intel® PTT が搭載されています。Windows 10 は Intel®PTT に対応していますので、セキュリティチップの設定を有効にすることが可能です。

デバイスの暗号化を無効にする

次の手順でデバイス暗号化を無効にしてください。

1 → (設定) →「システム」の順にクリックします。

2「システム」ウィンドウ左の「バージョン情報」をクリックし、画面を下にスクロールします。

3「デバイスの暗号化が有効になっています。」と表示されている下にある「オフにする」をクリックします。

内蔵ディスク全体のリカバリを実行する

重要

- 内蔵ディスク内のすべてのデータが削除されます。あらかじめ、必要なデータをバックアップしてください。

1　製品本体の電源が切れた状態で、リカバリ USB メモリをセットします。

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。

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、『導入ガイド』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.26）をご覧ください。

3　カーソルキーで「USB HDD：[USB メモリ名]」を選択し、【Enter】キーを押します。

そのまましばらくお待ちください。「ディスク全体をご購入時の状態に戻す」が表示されます。

4　「ご使用上の注意」をよく読み、「同意する」をクリックし、「次へ」をクリックします。

5　画面のメッセージに従って操作します。

この後は、ディスクの確認の後、

1. ハードディスクの領域を設定する
2. ソフトウェアを復元する
3. リカバリを実行する
4. 最終処理を実行する

「リカバリが完了しました。」というメッセージが表示されたら手順 6 に進んでください。

6　リカバリ USB メモリを取り外し、「完了」をクリックします。

製品本体の電源が自動的に切れます。

以上で内蔵ディスク全体をリカバリする操作が終了しました。
続けて、「リカバリ後のセットアップ」（→ P.83）をご覧になり、セットアップを行ってください。なお、電源は 30 秒以上待ってから入れてください。

リカバリ後のセットアップ

注意事項

●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。セットアップが正常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。
- 周辺機器（セットアップ作業に必要なディスプレイ、USB キーボード、USB マウスを除く）
- 2 台目のディスプレイ
- BIOS の設定
- LAN ケーブル（アクセスポイント部分とコンピューター部分を接続するケーブルを除く）

●セットアップ中は、ネットワークに接続しないでください。ネットワークに接続してセットアップを行うと、非常に時間がかかり 1 時間以上セットアップが進んでいないように見える場合があります。

●デバイスドライバーのインストールが必要な機器の場合、リカバリ作業に必要な機器であっても、リカバリ作業時に接続しているとリカバリに失敗する場合があります（例：指紋認証／手のひら静脈センサー付きキーボード、タッチ機能付きディスプレイなど）。この場合は、デバイスドライバーのインストールを必要としない機器を別途ご用意いただき、リカバリを実施してください。

●セットアップ中は、電源を切らないでください。

●Windows 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、画面をクリックしたりすると、Windows 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、キーボードまたはマウスで操作してください。

●Windows セットアップが進められなくなった場合は、電源ボタンを 10 秒以上押して、製品本体の電源を一度切り、セットアップをやり直してください。セットアップがやり直せない場合は、リカバリを行ってください。リカバリについては、「内蔵ディスク全体をリカバリする」（→ P.79）をご覧ください。

●Windows セットアップの途中で、「新しいハードウェアの追加ウィザード」ウィンドウが表示された場合は、お使いのディスプレイに合わせたドライバーをインストールしてください。

Windows のセットアップ

製品本体の電源を入れ、表示された画面のメッセージに従って Windows のセットアップを行います。
詳しい手順や注意事項につきましては、『導入ガイド』の「Windows のセットアップ」をご覧ください。

セットアップ後のインストール状態

セットアップ後のアプリが未インストールの状態になります。必要に応じて、アプリをインストールしてください。

■アプリやドライバーのインストール状態

お使いの機種	ドライバー／アプリ	
エッジコンピューティングデバイス	ドライバー	すべてのドライバー類がインストールされます。
	お手入れナビ	インストールされていません。 アプリの再インストールと再設定が必要です。
	基本アプリ	
	・ cygwin	
	・ Open Java Development Kit	
	メンテナンス機能	
	・ 管理画面	
	・ 動作状態監視ツール	
	・ 無線 LAN 診断	
	・ 端末情報収集ツール	
	インターネットキャッシュ機能[注]	
	サーバファイルキャッシュ機能	
	端末認証	
	無線 LAN 接続台数表示	
	優先接続設定	
	Intel Unite	

注　：インターネットキャッシュ機能は V3.0.0 になります。
https プロトコルのコンテンツのキャッシュに対応したインターネットキャッシュ機能（V4.1.0）をご使用の場合は、『アプリアップデートガイド』または、『導入ガイド』（第 2 版以降）をご覧ください。

■アプリの再インストールおよび再設定

1 『導入ガイド』の「セットアップ」をご覧になり再度、インストールおよび設定してください。

2 設定のバックアップを行っている場合は、設定を復元してください。

「管理画面の設定と収集データのバックアップと再設定」（→ P.88）をご覧になり、再設定してください。また、「設定項目の追加」を使用して設定している場合は、「[設定項目の追加]」（→ P.45）をご覧になり、再設定してください。

「端末認証機能の設定のバックアップと再設定」（→ P.94）をご覧になり、再設定してください。

3. 内蔵ディスク内のデータを使った回復方法

Windows 10 には、トラブルに備え、以前の状態に戻す機能が搭載されています。ここでは、内蔵ディスク内のデータから本製品をご購入時に近い状態に回復する方法「この PC を初期状態に戻す」について説明します。

POINT

▶ここで説明する方法は、Windows 10標準の機能です。今後、Windowsの更新により、手順や画面の表示が変更される場合があります。

「この PC を初期状態に戻す」 機能の注意事項

●ご購入時に近い状態に戻るため、削除されるデータもあります。必要に応じて事前にバックアップしてください。

●Windows に適用されたロールアップ（修正プログラム、セキュリティ修正プログラム、重要な更新およびアップデートを配布しやすいように 1 つにまとめた累積的なパッケージ）は、「この PC を初期状態に戻す」を行っても、適用された状態が維持されます。

●本製品から、外付けハードディスク、プリンターなどすべての周辺機器を、必ず取り外してください（画面表示機器、USB キーボード、USB マウスを除く）。

●「この PC を初期状態に戻す」を行うと、本製品をご購入された後にインストールされたアプリは削除されます。

●「この PC を初期状態に戻す」を行うには時間がかかります。時間に余裕をもって、操作してください。

●BitLocker 回復キーを取得してください。
次の手順で BitLocker 回復キーを取得し、大切に保管してください。なお、この操作は他のコンピューターやタブレット端末でも行うことができます。

1. 次の URL にアクセスし、Microsoft アカウントでサインインします。
   http://windows.microsoft.com/recoverykey
   この後は、画面の指示に従って操作してください。
2. 「BitLocker 回復キー」が画面に表示されたら、印刷したりメモをとったりして大切に保管します。

●「この PC を初期状態に戻す」手順を終え、セットアップが完了すると、デバイスの暗号化が無効になります。次の手順でデバイス暗号化を有効にしてください。

1. → 「設定」→「システム」の順にクリックします。
2. 「システム」ウィンドウ左の「バージョン情報」をクリックし、画面を下にスクロールします。
3. 「デバイス暗号化が無効になっています。」と表示されている下にある「オンにする」をクリックします。

POINT

▶個人用ファイルを保持する場合は、デバイス暗号化は無効になりません。上記の操作は不要です。

●「この PC を初期状態に戻す」手順で、「使用できる状態に戻すには回復キーを入力してください」と表示された場合は、BitLocker 回復キーを入力し、「続行」をクリックしてください。

●「この PC を初期状態に戻す」手順で、初期化が開始された後、「オプションの選択」画面が表示された場合は、「続行」をクリックしてください。初期化が再開されます。

「この PC を初期状態に戻す」 の種類

個人用ファイルを保持する

消去されないデータについても念のためバックアップをとったり、メモしたりすることをお勧めします。
個人用ファイルは次のパス配下のデータです。
C:¥Users
「個人用ファイルを保持する」を選択した場合、個人用ファイルは消去されません。しかし、次のパスの配下のデータは消去されます。この配下にはアプリに固有のアプリ設定、ファイル、データが含まれます。
C:¥Users¥[ユーザー名]¥AppData

すべて削除する

●ファイルの削除のみ行う
ほぼご購入時の状態に戻ります。アカウントも削除されるので、セットアップをやり直す必要があります。

●ドライブを完全にクリーンアップする
消去されるものは「すべて削除する（ファイルの削除のみ行う）」と同じですが、簡単に回復できないように完全に削除されます。そのため操作に数時間かかります。

「この PC を初期状態に戻す」 手順

「オプションの選択」画面を表示する

Windows が起動しない場合でも、「オプションの選択」画面を表示できるときがあります。
そのとき「この PC を初期状態に戻す」を行えば、Windows を起動できるようになることがあります。

■「自動修復」 画面が表示された場合

Windows が起動しないとき、しばらく待っていると「自動修復」画面が表示されることがあります。「再起動」をクリックしても Windows が正常に起動せず、また「自動修復」画面が表示された場合、「詳細オプション」をクリックしてください。
「オプションの選択」画面が表示されます。

■回復ドライブ （USB） を作成していた場合

1 本体の電源が切れた状態で、回復ドライブ（USB）をセットします。

2 起動メニューを表示します。

3 カーソルキーで「USB HDD：[USB メモリ名]」を選択し、【Enter】キーを押します。

4「キーボードレイアウトの選択」と表示されたら、「Microsoft IME」をクリックします。

5「オプションの選択」画面が表示されます。

■Windows が起動する場合

1「スタート」ボタン→「設定」→「更新とセキュリティ」の順にクリックします。

2「更新とセキュリティ」ウィンドウ左の「回復」をクリックします。

3 ウィンドウ右の「今すぐ再起動する」をクリックします。

4「オプションの選択」画面が表示されます。

■「使用できる状態に戻すには回復キーを入力してください」 と表示された場合

BitLocker 回復キーを入力し、「続行」をクリックしてください。

■初期化が開始された後、 「オプションの選択」 画面が表示された場合

「続行」をクリックしてください。初期化が再開されます。

「オプションの選択」画面からの手順

1「オプションの選択」画面で、「トラブルシューティング」をクリックします。

2「トラブルシューティング」画面で、「この PC を初期状態に戻す」をクリックします。

■ 個人用ファイルを保持する場合

POINT

▸初期化した後、デスクトップアプリが消去された場合、デスクトップに「削除されたアプリケーション.html」が作成されます。消去されたデスクトップアプリ一覧が確認できます。

1. 「個人用ファイルを保存する」をクリックします。
2. 「続けるにはアカウントを選んでください。」と表示されたら、お使いのアカウントをクリックします。
3. 「このアカウントのパスワードを入力してください。」と表示されたら、パスワードを入力し、「続行」をクリックします。
4. 「準備が完了しました。」と表示されたら、「初期状態に戻す」をクリックします。
   初期化が開始されます。電源を切らずにお待ちください。Microsoft アカウントのパスワード入力を求められたら入力してください。Windows セットアップはありません。デスクトップが表示されたら初期化は完了です。「セットアップ後のインストール状態」（→ P.83）をご覧になり処理を続けてください。

■ すべて削除する（ファイルの削除のみ行う）場合

1. 「すべて削除する」をクリックします。
2. 「ファイルの削除のみ行う」をクリックします。
3. 「準備が完了しました。」と表示されたら、「初期状態に戻す」をクリックします。
   初期化が開始されます。電源を切らずにお待ちください。「こんにちは」画面が表示されたら、初期化は完了です。「リカバリ後のセットアップ」（→ P.83）をご覧になり処理を続けてください。

■ すべて削除する（ドライブを完全にクリーンアップする）場合

1. 「すべて削除する」をクリックします。
2. 「ドライブを完全にクリーンアップする」をクリックします。
3. 「準備が完了しました。」と表示されたら、「初期状態に戻す」をクリックします。
   初期化が開始されます。電源を切らずにお待ちください。初期化が完了したら、「リカバリ後のセットアップ」（→ P.83）をご覧になり処理を続けてください。

4. アクセスポイントの設定のバックアップと再設定

Web 設定画面で設定したアクセスポイントの設定をバックアップすることができます。

設定ファイルの保存

1 **ブラウザーを起動します。**

2 **アドレスバーに本製品の 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

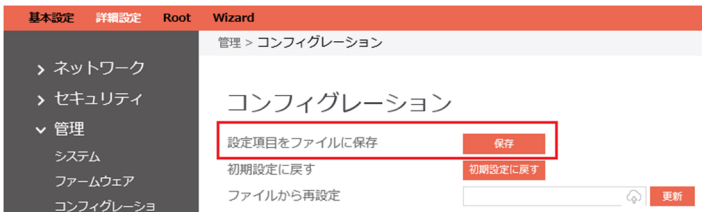
▸IPアドレスには、本製品のアクセスポイント部分のIPアドレスをお使いください。
アクセスポイント部分のIPアドレスが「192.168.1.1」の場合は、次のようになります。
http://192.168.1.1

ログイン画面が表示されます。

3 **ユーザ名「root」とパスワードを入力し、「ログイン」をクリックします。**
本製品導入時に変更したパスワードを入力してください。

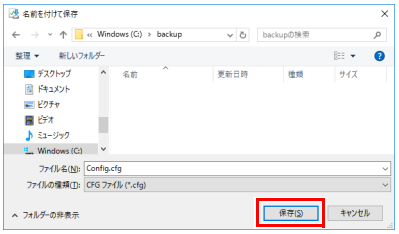
4 **「詳細設定」→「管理」→「コンフィグレーション」の順にクリックします。**
コンフィグレーションが表示されます。

5 **設定項目をファイルに保存の「保存」をクリックします。**



6 **▾をクリックし、「保存」または「名前を付けて保存」をクリックします。**

7 **保存する場所を指定して、「保存」をクリックします。**



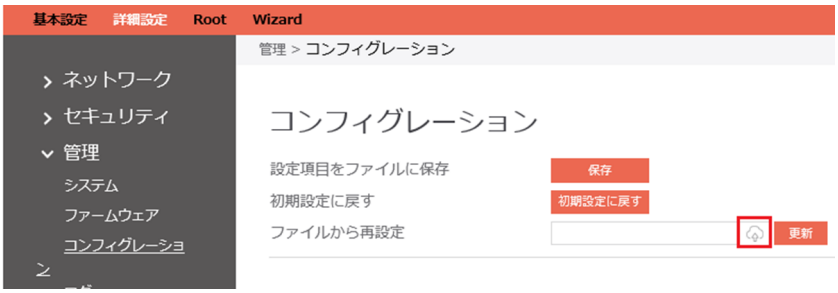
保存したデータはなくさないよう大切に保管してください。

設定ファイルからの再設定

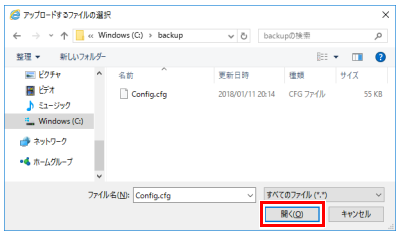
「設定ファイルの保存」（→ P.86）で保存したファイルを使って、再設定できます。

1 「詳細設定」→「管理」→「コンフィグレーション」の順にクリックします。
コンフィグレーションが表示されます。

2 をクリックします。



3 保存したファイルを指定して「開く」をクリックします。



4 「更新」をクリックします。

5 「Confirm」をクリックします。

5. 管理画面の設定と収集データのバックアップと再設定

管理画面の「エクスポート／インポート」機能を使い、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することができます。

POINT

- 「管理画面」の「キャッシュデーター覧」に表示されるコンテンツのデータはバックアップの対象ではありません。
- サーバファイルキャッシュ機能で本製品にキャッシュされた教材などのデータはバックアップの対象ではありません。

管理画面設定と端末から収集したデータのエクスポート

次の手順で、管理画面の設定や端末から収集したデータをバックアップします。

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、ログインします（→ P.29）。

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

2　「管理画面設定」をクリックし、「コンピュータ設定」→「エクスポート／インポート」の順にクリックします。

3　「エクスポート」をクリックします。

エクスポート出力先のフォルダーに設定ファイルが保存されます。

4　「状態をチェック」をクリックします。

「エクスポート結果」に「成功」と表示されればエクスポートは終了です。

管理画面設定と端末から収集したデータのインポート

次の手順で、管理画面の設定や端末から収集したデータを再設定します。

POINT

- インポートを行うと、管理画面のキャッシュデーター覧のデータがすべて削除されます。

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、ログインします（→ P.29）。

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/

2「管理画面設定」をクリックし、「コンピュータ設定」→「エクスポート／インポート」の順にクリックします。

3　エクスポート出力先のフォルダーからインポート読込先のフォルダーに必要なファイルをコピーします。

4「インポート」をクリックします。

5「状態をチェック」をクリックします。

「インポート結果」に「成功」と表示されればインポートは終了です。

6. 証明書ファイルのバックアップと再設定

証明書ファイルのバックアップ

POINT

- 証明書は、期限が切れるまで大切に保管ください。また、本製品を複数台導入している場合は、証明書ファイル（myCA.pem、myCA.der）は,共通になります。そのため、証明書ファイルのバックアップは、複数台で取得する必要はありません。

次の手順で、証明書ファイルのバックアップをします。

1　エッジコンピューティングデバイス上の以下のフォルダにアクセスします。
C:¥cygwin64¥squid¥etc¥ssl_cert

2　ファイルを外付け HDD や DVD、USB フラッシュメモリにコピーします。
myCA.pem（エッジコンピューティングデバイス用証明書）
myCA.der（タブレット端末用証明書）

証明書ファイルの再設定

次の手順で、証明書ファイルを再設定します。

エッジコンピューティングデバイス用証明書

■証明書のインストール

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、ログインします（→ P.29）。

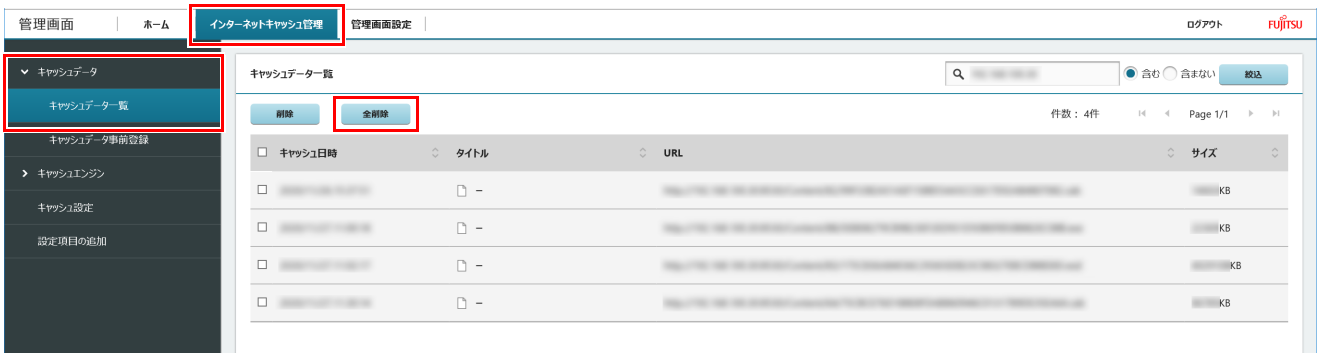
POINT

- 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/

2　キャッシュエンジンを停止します。
「キャッシュエンジン制御」-「 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。

3　「証明書ファイルのバックアップ」（→ P.90）でバックアップした証明書を次のフォルダに上書きコピーします。
C:¥cygwin64¥squid¥etc¥ssl_cert

4　管理画面でキャッシュ一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。



5　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。

6　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制御」-「 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。

7　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。

タブレット端末用証明書

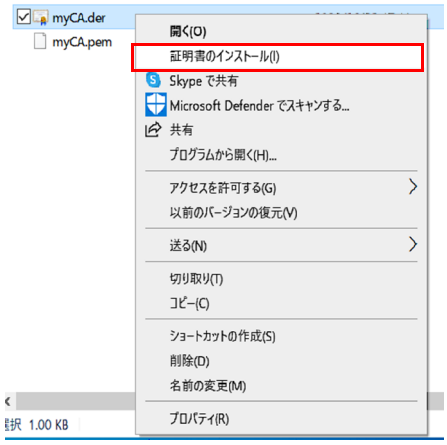
■証明書のインストール

重要

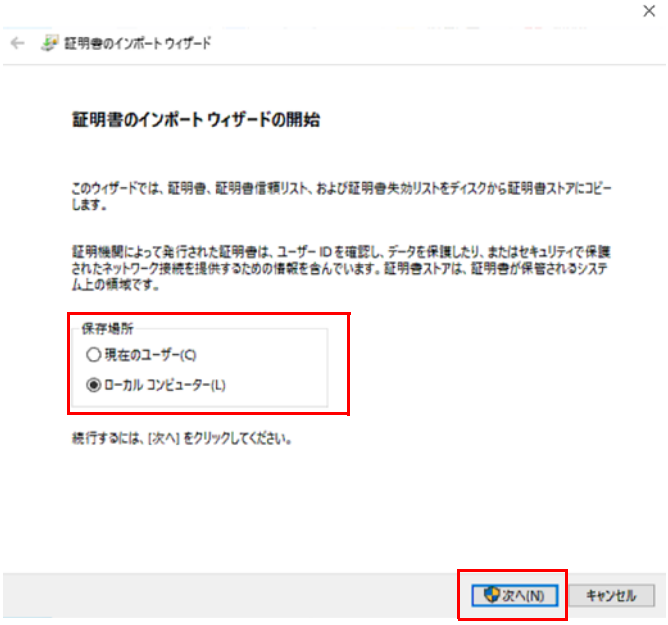
▸※Windows以外の端末への証明書のインストール方法は、ご使用の端末のマニュアルをご参照ください。

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。

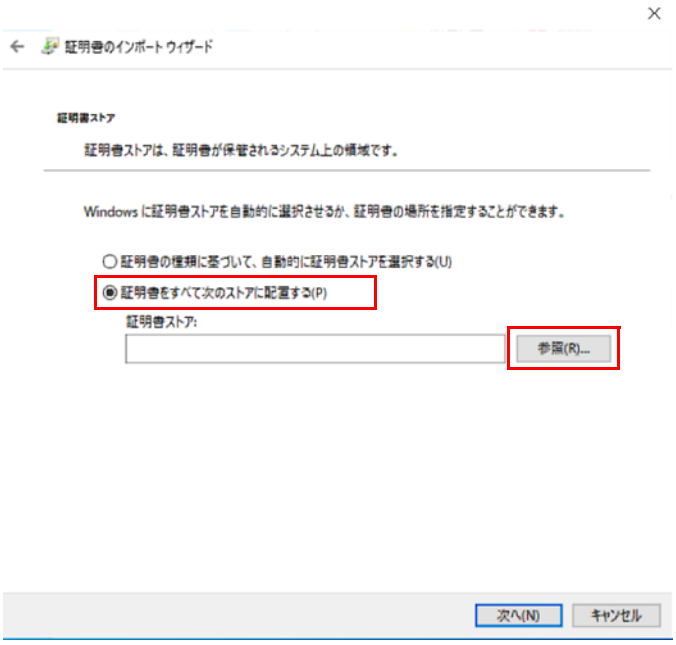
2　「証明書ファイルのバックアップ」（→ P.90）でバックアップした証明書ファイル「myCA.der」を右クリックし、「証明書のインストール」を選択します。



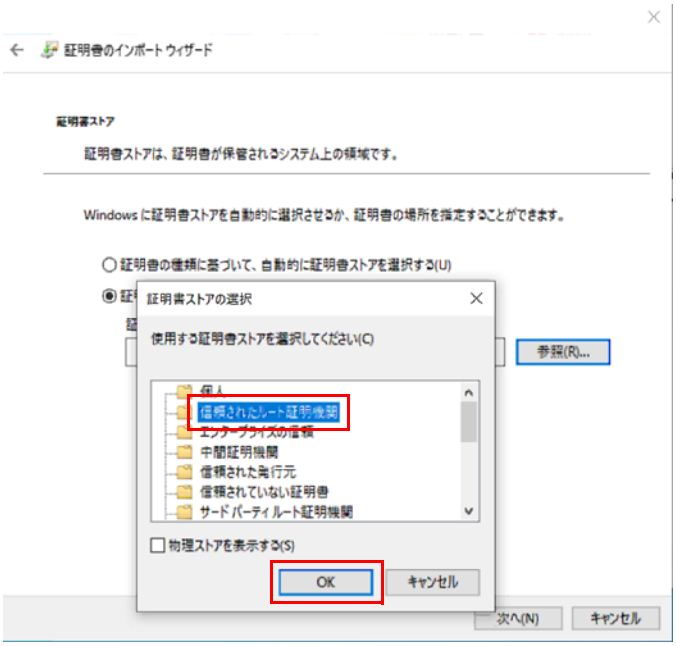
3 保存場所を「現在のユーザー」か「ローカルコンピュータ」を選択し、「次へ」をクリックします。



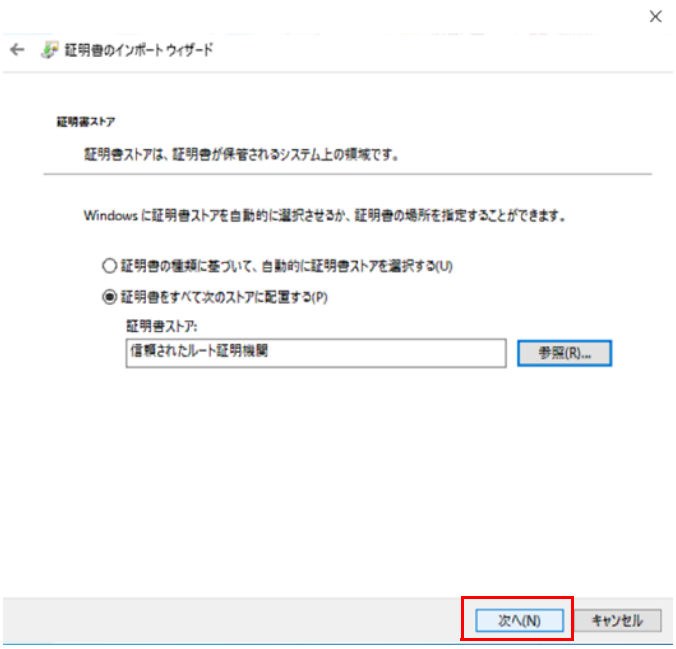
4「証明書をすべての次のストアに配置する」にチェックをして「参照」をクリックします。



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。

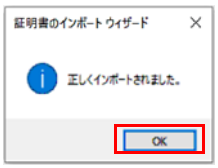


6「次へ」をクリックします。



7「完了」をクリックします。

8「OK」をクリックします。



7. 端末認証機能の設定のバックアップと再設定

端末認証登録のデータをバックアップすることができます。

登録済み端末データファイルの保存

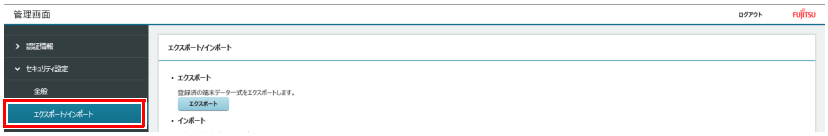
認証端末の登録データを保存します。

1 管理画面にログインします。

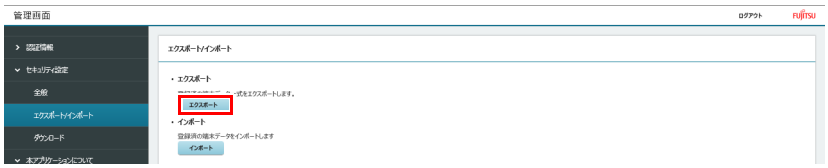
管理画面にログインする方法については、「管理画面へログイン」（→ P.59）をご覧ください。

2「認証情報」の「認証対象端末一覧」をクリックし、「認証登録モード」が「ON」の場合は「OFF」に設定します。

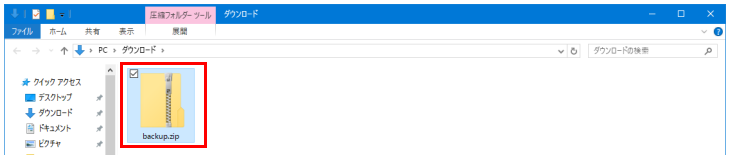
3「セキュリティ」の「エクスポート／インポート」をクリックします。



4「エクスポート」をクリックします。



ファイルがダウンロードされます。



保存したデータはなくさないよう大切に保管してください。

登録済み端末データファイルのインポート

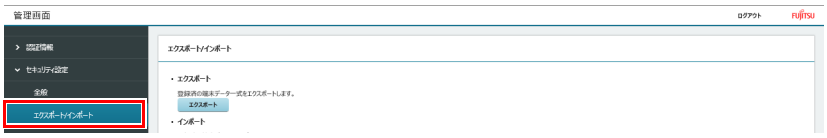
次の手順で、登録済み端末データをインポートします。

1 管理画面にログインします。

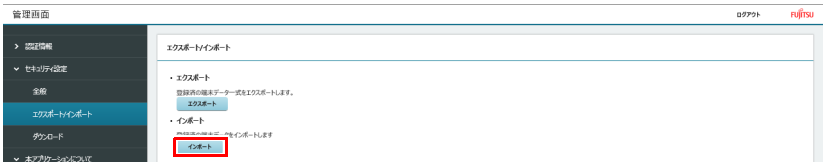
管理画面にログインする方法については、「管理画面へログイン」（→ P.59）をご覧ください。

2 「認証情報」の「認証対象端末一覧」をクリックし、「認証登録モード」が「ON」の場合は「OFF」に設定します。

3 「セキュリティ」の「エクスポート／インポート」をクリックします。

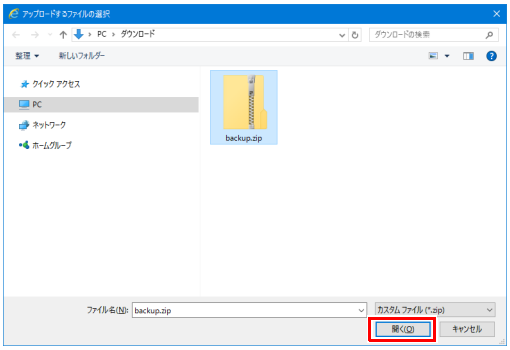


4 「インポート」をクリックします。



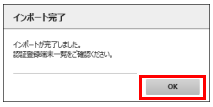
「アップロードするファイルの選択」が表示されます。

5 保存したファイルを指定して、「開く」をクリックします。



「インポート完了」が表示されます。

6 「OK」をクリックします。



6

第 6 章
お手入れ

快適にお使いいただくためのお手入れ方法を説明しています。

1. 日常のお手入れ 97
2. 定期的なお手入れ 97

1. 日常のお手入れ

製品本体や周辺機器を長時間使用していると、汚れが付いたり、ほこりがたまったりします。ここでは、日常のお手入れのしかたを説明しています。

製品本体表面の汚れ

乾いた柔らかい布で拭き取ってください。
汚れがひどい場合は、水または水で薄めた中性洗剤を含ませた布を、固く絞って拭き取ってください。中性洗剤を使用して拭いた場合は、水に浸した布を固く絞って中性洗剤を拭き取ってください。

重要

- 拭き取るときは、内部に水が入らないよう充分に注意してください。
- シンナーやベンジンなど揮発性の強いものや、化学ぞうきんは使わないでください。損傷する原因となります。

2. 定期的なお手入れ

長期間製品を使用していると、通風孔にほこりがたまります。ほこりがたまった状態で使用し続けると、故障の原因となりますので、定期的にお手入れをしてください。

注意事項

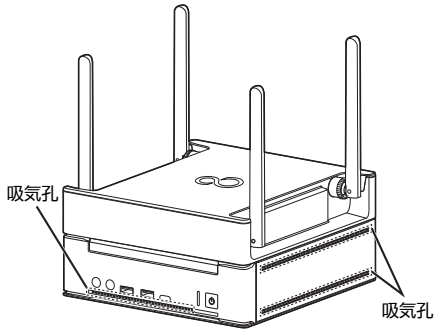
●お手入れをする場合は、製品本体および接続されている機器の電源を切り、電源プラグをコンセントから抜いた後に行うようにしてください。
この手順を守らずに作業を行うと、感電・火災または故障の原因となります。
電源の切り方については、「電源を切る」（→ P.26）をご覧ください。

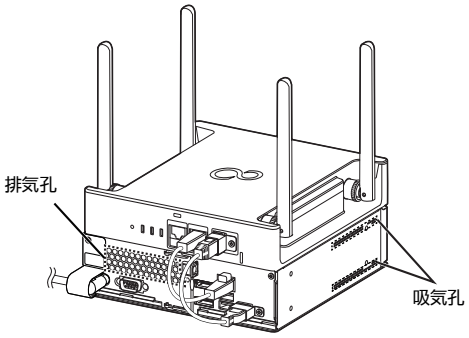
●清掃時には、ほこりなどを口や鼻から吸い込まないように、窓を開けたり、換気扇を回したりするなどして、充分に換気してください。

●清掃時に破損した場合は、保証期間にかかわらず修理は有償となります。取り扱いについては、充分にご注意ください。

製品本体外部のほこりを取る

製品本体の通風孔（吸気や排気）などの開孔部にほこりがたまると、故障の原因となります。
通風孔などに付着したほこりは、掃除機で吸い取ってください。





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 99
2. トラブルシューティング 101
3. それでも解決できないときは 118

1. トラブル発生時の基本操作

トラブルを解決するにはいくつかのポイントがあります。トラブル発生時に対応していただきたい順番に記載しています。なお、画面表示機器、USB キーボード、USB マウスを接続した状態でご確認ください。

状況を確認する

トラブルが発生したときは、直前に行った操作や現在の製品の状況を確認しましょう。

メッセージなどが表示されたら控えておく

画面上にメッセージなどが表示されたら、メモ帳などに控えておいてください。マニュアルで該当するトラブルを検索する場合や、お問い合わせのときに役立ちます。

製品や周辺機器の電源を確認する

電源が入らない、画面に何も表示されない、ネットワークに接続できない、などのトラブルが発生したら、まず製品や周辺機器の電源が入っているか確認してください。

●電源ケーブルや周辺機器との接続ケーブルは正しいコネクタに接続されていますか？また緩んだりしていませんか？

●電源コンセント自体に問題はありませんか？

●他の電器製品を接続して動作するか確認してください。OA タップを使用している場合、OA タップ自体に問題はありませんか？

●他の電気製品を接続して動作するか確認してください。使用する装置の電源はすべて入っていますか？

●ネットワーク接続ができなくなった場合は、ネットワークを構成する機器（サーバー本体やハブなど）の接続や電源も確認してください。

●キーボードの上に物を載せていませんか？
　キーが押され、製品が正常に動作しないことがあります。

このほか、「起動・終了時のトラブル」（→ P.101）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.101）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.26）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、『導入ガイド』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、『導入ガイド』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.26）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.115）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。

●画面表示機器に関して、次の項目を確認してください。

・ ケーブルのコネクタのピンが破損していませんか？
・ 画面表示機器のブライトネス／コントラストボリュームは、正しく調節されていますか？
・ 複数台の画面表示機器を接続している場合、製品本体の電源を入れる前に、画面表示機器の電源を入れていますか？

必ず製品本体の電源を入れる前に画面表示機器の電源を入れてください。製品本体の電源を入れた後に画面表示機器の電源を入れると、画面が表示されないことがあります。そのような場合は、いったん電源を切ってから入れ直してください。

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、システムイメージの復元を行ってください（→ P.69）。

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。
・「お手入れ」（→ P.96）をご覧になり、本製品のお手入れをしてください。
・ 再起動してください。問題が解決する場合があります。

アプリのヘルプを表示しようとすると「この ms-getstarted を開くには新しいアプリが必要です」と表示されヘルプが表示されない

●本製品の仕様です。
本製品では「GetStarted」が含まれていないためです。

「アクションセンター」の「ノート」が使用できない

●OneNote のクイックノートを起動しますが、OneNote は含まれないため使用できません。

メンテナンス機能のトラブル

管理画面を表示したときに、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 :10080（管理画面のポート番号）と記載します。
エッジコンピューティングデバイスの IP アドレスが 192.168.1.1 だった場合
192.168.1.1:10080
と入力します。

●「ステータスランプ」（→ P.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」→「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
『導入ガイド』の「手動プロキシ設定」をご覧になり、プロキシの例外設定を行ってください。
・ 自動構成スクリプト（PAC ファイル）を使用している場合
PAC ファイルで本製品のコンピューター部分の IP アドレスをプロキシの例外に設定してください。

診断が行われない

●「Elasticsearch」サービスが起動していない可能性があります。
「スタート」→「Windows 管理ツール」→「サービス」の順にクリックして、サービスが起動していることを確認してください。

●アクセスポイント部分の IP アドレスとパスワードが変更されている可能性があります。
ネットワーク管理者にご確認ください。

●セキュリティ対策アプリの影響で、接続できない場合があります。
セキュリティ対策アプリのログと設定を確認してください。

●アクセスポイントの SSH でのアクセス可否設定が「拒否」に設定されている可能性があります。
アクセスポイントの Web 設定画面にて、SSH でのアクセス可否設定が「許可」に設定されているかご確認ください。

●次のフォルダーに診断結果のログファイルが作成されていることを確認してください。
「C:¥ProgramData¥FCCL¥WirelesslanAnalysis¥Log」

●本製品と端末で時間がずれている場合、正しく診断できない場合があります。
ファイルを最新にするか、本製品と端末との時間を合わせてください。

「AP ログイン失敗」と診断された

●アクセスポイント部分の IP アドレスとパスワードが変更されている可能性があります。
ネットワーク管理者にご確認ください。

●アクセスポイントの SSH でのアクセス可否設定が「拒否」に設定されている可能性があります。
アクセスポイントの Web 設定画面にて、SSH でのアクセス可否設定が「許可」に設定されているかご確認ください。

●セキュリティ対策アプリに影響で、接続できない場合があります。
セキュリティ対策アプリのログと設定を確認してください。

●LAN ケーブルは外れていませんか？
アクセスポイント部分に接続する LAN ケーブル、および、アクセスポイント部分とコンピューター部分を接続する LAN ケーブルの接続を確認してください。

「IP なし」と診断された

●アクセスポイント部分の設定で DHCP 機能が OFF になっている可能性があります。
アクセスポイントの Web 設定画面で、DHCP の設定をご確認ください。

「DHCP 失敗」と診断された

●アクセスポイント部分の Web 設定画面で、「動作モード」が「ルータ」になっていることを確認してください。また、IP アドレスの割り振り可能範囲の設定が適切かをご確認ください。

「切断の可能性あり」と診断された

●端末の「MaintInfoCollectionService」サービスが起動していない可能性があります。
「スタート」→「Windows 管理ツール」→「サービス」の順にクリックして、サービスが起動していることを確認してください。
サービスが起動していない場合は、一覧から「MaintInfoCollectionService」を右クリックして「開始」をクリックしてください。

「接続失敗」と診断された

●端末接続時の設定が間違っている可能性があります。
アクセスポイントに接続したときに入力したネットワークセキュリティキーが間違っていないかご確認ください。

「RSSI 低下 / 干渉」と診断された

●端末の使用環境に問題ないかご確認ください。
端末がアクセスポイントから離れすぎてないかや、端末とアクセスポイントの間に遮へい物がないかなど、端末の使用環境に問題がないかをご確認ください。

●端末において接続したい SSID の電波が弱い可能性があります。
アクセスポイントの Web 設定画面で、アクセスポイントの送信出力を大きくするように設定を変更してください。

●ご使用のチャネルがすでに使用されている可能性があります。
アクセスポイントの Web 設定画面で、使用するチャネル番号を変更してください。

「認証またはその他端末問題」と診断された

●ご使用の端末がなんらかの要因で接続できない状態になっている可能性があります。
端末を再起動してください。また、端末の使用環境に問題ないかご確認ください。

「AP 異常」と診断された

●アクセスポイント部分になんらかの問題が発生し、端末が接続できなくなっています。
次の手順で本製品を再起動してください。

1.電源ボタンを押します。
2.シャットダウンしたら、電源プラグをコンセントから抜きます。
3.30 秒以上待ってから電源プラグをコンセントに付けます。
4.電源ボタンを押します。

診断結果やログを通知するメールが送信先に届かない

●次の手順でテストメールを送信して送信先にメールが届くかご確認ください。

1.ブラウザーで「管理画面」を表示します（→ P.29）。
2.「情報端末管理」→「収集・通知設定」→「SMTP 設定」の順にクリックします。
3.「テストメール送信先アドレス」に送信先のメールアドレスを入力し、「テスト送信」をクリックします。詳しくは、『導入ガイド』の「「収集・通知」に関する設定」の SMTP 設定に関する記載をご覧ください。

メールが届かない場合は、「SMTP 設定」をご確認ください。

●メール送信の指定日時に、本製品が起動していなかった可能性があります。

●『導入ガイド』をご覧になり、「収集・通知」の各設定項目について、メールの配信設定をご確認ください。「ステータスランプ」（→ P.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。

端末稼働時間一覧にデータが表示されない

●端末稼働時間一覧には、当月のデータは表示されません。前月分のデータが表示されます。
月が替わるのをお待ちください。

端末稼働台数のデータが少ない

●端末稼働台数に表示されるデータは過去 1ヶ月分のデータです。それ以前のデータは表示されません。

管理画面に解析結果の一覧が表示されない

●「管理画面設定」の「インポート / エクスポート」で、インポートを実行している可能性があります。
インポート中は、「端末情報管理」の「無線 LAN 診断状況一覧」、「端末稼働時間一覧」、「バッテリー状況一覧」に解析結果の一覧が表示されず、次のメッセージが表示されます。

「インポート中です。インポート終了後に画面を表示します。」

インポート処理中は管理画面の表示が制限されます。インポートが終わるまでお待ちください。

エクスポートできない

●「管理画面設定」の「インポート / エクスポート」で、エクスポートできない場合は、ストレージの空き容量が少なくなっている可能性があります。
空き容量が 15GB より少ない場合は、不要なファイルを削除してください。

インポートできない

●エクスポートしたデータを他のフォルダーに移動していませんか？
インポート読み込み先フォルダーに、エクスポートしたすべてのデータが格納されていることを、確認してください。

●インターネットキャッシュ機能 V3.0.0 でエクスポートしたデータを、インターネットキャッシュ機能 V4.1.0 をインストールした環境にインポートすることはできません。

インターネットキャッシュ機能のトラブル

動画の再生が遅い

●本製品のストレージの空き容量が少なくなっている可能性があります。
不要なファイルや使用しなくなったキャッシュのコンテンツデータを削除してください。

●「ステータスランプ」（→ P.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、データキャッシュ機能が停止している可能性があります。
次の手順で、本製品を再起動してください。

1.電源ボタンを押します。
しばらくすると、本製品の電源が切れます。
2.電源プラグをコンセントから抜きます。
3.30 秒以上待ってから電源プラグをコンセントに付けます。
4.電源ボタンを押します。

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。

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.38）。

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.48）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.48）をご覧ください。

サーバファイルキャッシュ機能のトラブル

Q 学習支援アプリサーバにファイルをアップロードできない

●アップロードしようとしているファイルのサイズの合計が、サーバファイルキャッシュの閾値（初期値：80MB）を超えている可能性があります。
この場合、計画同期となり、同期計画対象時間帯にアップロードされます。すぐに学習支援アプリサーバにファイルをアップロードしたい場合は、管理画面の「簡易情報取得・手動制御」で、タブレット端末でファイルをアップロードしたときに接続していたエッジコンピューティングデバイスの「割込実行」を実行してください（→ P.55）。

優先接続設定のトラブル

Q 優先接続設定が正しく起動しない

● 優先接続設定を起動すると、次のメッセージが表示される場合があります。

起動に失敗しました。以下をご確認ください。
タブレットのネットワーク状態
コンピューターのネットワーク状態
本アプリの設定

・タブレット端末が本製品に接続されていない可能性があります。
『ユーザーガイド』の「タブレット端末を無線 LAN に接続する」をご覧になり、お使いのタブレット端末の無線 LAN 接続を確認してください。

・アクセスポイント部分になんらかの問題が発生し、端末が接続できなくなっています。
タブレット端末で利用できる SSID の一覧に本製品の SSID が表示されない場合は、アクセスポイント部分から無線電波が出ていない可能性があります。
本製品の SSID が表示されない場合は、次の手順で本製品を再起動してください。
1.電源ボタンを押します。
2.シャットダウンしたら、電源プラグをコンセントから抜きます。
3.30 秒以上待ってから電源プラグをコンセントに付けます。
4.電源ボタンを押します。

● 「優先接続設定の変更処理が失敗しました」のメッセージが表示された場合、次の原因が考えられます。
・アクセスポイント部分の Web 設定画面で、ユーザ DB に「smart」が設定がされていない。
詳しくは、『導入ガイド』をご覧ください。

●ネットワークに接続していない。
タブレット端末をネットワークに接続してください。

●対象の SSID を選択していない。
タブレット端末をエッジコンピューティングデバイスの SSID に接続してください。

●接続対象以外のエッジコンピューティングデバイスに接続している。
タブレット端末を接続対象のエッジコンピューティングデバイスに接続し直してください。

●プロキシ設定に間違いがある。
『導入ガイド』をご覧になり、タブレット端末のプロキシ設定を確認してください。

●設定ファイル（IPAddressFromSSID.ini）に間違いがある。
『導入ガイド』をご覧になり、設定ファイルが正しいことを確認してください。

無線 LAN 接続台数表示のトラブル

無線 LAN 接続台数表示が正しく起動しない

●「×」が表示され、台数が表示されない場合は、設定ファイルが間違えている可能性があります。
『導入ガイド』をご覧になり、設定ファイルを確認してください。

●接続台数の画面が表示されずに「初期化に失敗しました」などのメッセージが表示される場合、次の原因が考えられます。

・ネットワークに接続していない。
　タブレット端末をネットワークに接続してください。
・プロキシ設定に間違いがある。
　『導入ガイド』をご覧になり、タブレット端末のプロキシ設定を確認してください。
・対象の SSID を選択していない。
　タブレット端末をエッジコンピューティングデバイスの SSID に接続してください。
・接続対象以外のエッジコンピューティングデバイスに接続している。
　タブレット端末を接続対象のエッジコンピューティングデバイスに接続し直してください。
・設定ファイル（IPAddressFromSSID.ini）に間違いがある。
　『導入ガイド』をご覧になり、設定ファイルが正しいことを確認してください。

Intel Unite のトラブル

PIN を入力したが、タブレット端末側で接続中と表示されたままになる

●PIN コードを 2 回連続で間違えて入力している可能性があります。
タブレット端末の Intel Unite を再起動してください。
1.タスクバーの Intel Unite アイコンを長押しタップして、「ウィンドウを閉じる」を選択します。
2.Intel Unite を起動します。
3.本製品の画面に表示されている PIN を確認して、再度、入力してください。

●本製品のファイアウォールの設定で Intel Unite の通信がブロックされている可能性があります。
ファイアウォールの設定で、Intel Unite の通信を許可してください。詳細は、「Intel Unite のファイアウォールの設定」（→ P.117）をご覧ください。

●タブレット端末のプロキシ設定に間違いがある可能性があります。
タブレット端末のプロキシ設定で、アドレスと例外に記載されている IP アドレスを本製品と同じ IP アドレスに設定してください。
タブレット端末のプロキシ設定の方法については、『導入ガイド』の「プロキシの設定」をご覧ください。

端末認証機能のトラブル

認証エンジンが起動しない

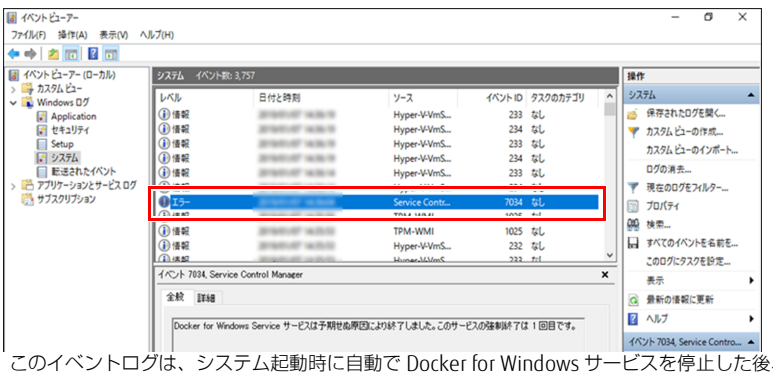
●「Docker for Windows」サービスが起動していない可能性があります。
サービスが起動していない場合は、サービスを起動するか、
「C:¥Program Fiels¥Docker¥Docker¥Docker for Windows.exe」を実行してください。

●Docker が、前回起動時のポートを開放していない場合あります。
サービスを再起動してください。

イベントビューアーでエラーログが発生する

●端末認証システム起動時、「イベントビューアー」→「Windows ログ」→「システム」に以下のイベントログが登録されます。

ソース：Service Control Manager
イベント ID：7034
内容：Docker for Windows サービスは予期せぬ原因により終了しました。このサービスの強制終了は、〇回目です。
※ 〇には数字が入ります。



このイベントログは、システム起動時に自動で Docker for Windows サービスを停止した後、再起動しているため登録されます。動作に問題はありません。

管理画面のログイン画面が表示されない

●「NginxService」サービスが起動していない可能性があります。
「スタート」→「Windows 管理ツール」→「サービス」の順にクリックして、サービスが起動していることを確認してください。

管理画面にログインできない

●アクセスポイントが正常に起動していない可能性があります。
次の手順で、本製品を再起動してください。
1.電源ボタンを押します。
2.シャットダウンしたら、電源プラグをコンセントから抜きます。
3.30 秒以上待ってから電源プラグをコンセントに付けます。
4.電源ボタンを押します。

●管理アプリケーション（制御部）が停止している可能性があります。
本製品を再起動してください。

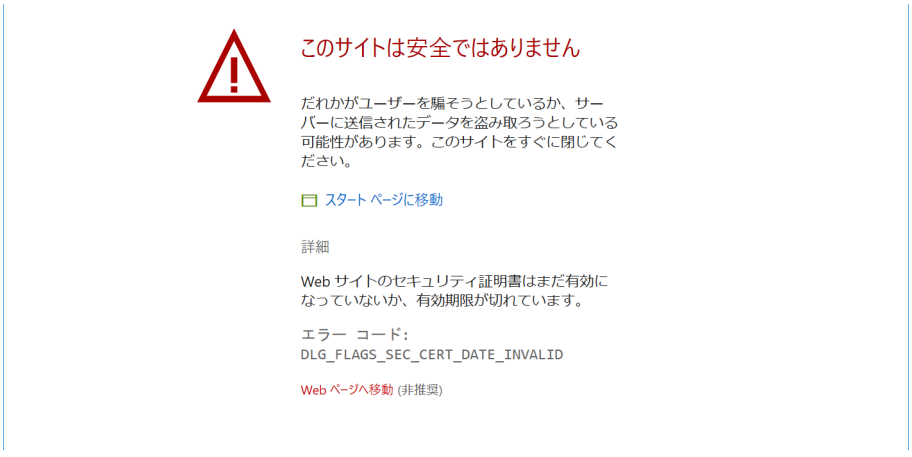
認証コード入力画面が表示されない

●認証登録モードが「OFF」になっていませんか？
端末認証機能の管理画面で、「認証登録モード」を「ON」に設定してください。

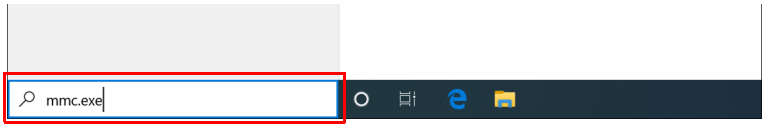
●アクセスポイントの設定が間違っている可能性があります。
SSID の設定について、次の点を確認してください。
・radius の参照 IP アドレス、ID/Pass が正しいこと。
・暗号化方式が「WPA2-Enterprose」になっていること。

●ファイアウォールの設定が間違っている可能性があります。
・「Node.js」と「vpnkit」の操作がブロックされている場合は、規則を無効化します

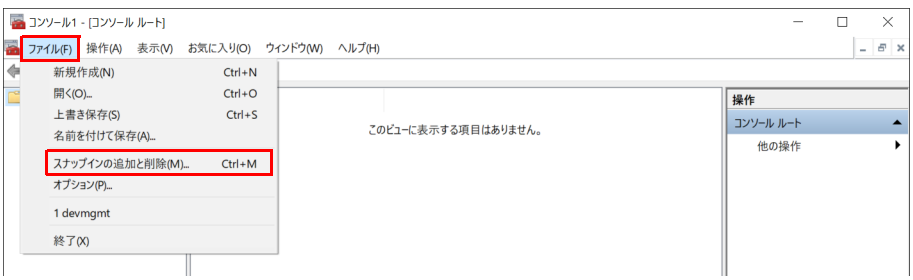
●証明書の有効期限が切れている可能性があります。
下図のような証明書エラーが表示された場合は、証明書の有効期限が切れています。次の手順に従い証明書を削除した後、端末認証登録用の SSID（SWRegist-5G）を再度タップしてください。



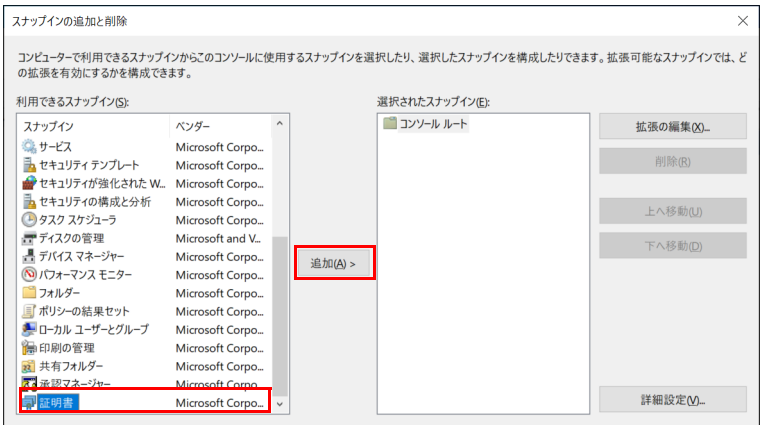
1.検索ボックスに「mmc.exe」を入力して、「Enter」キーを押します。



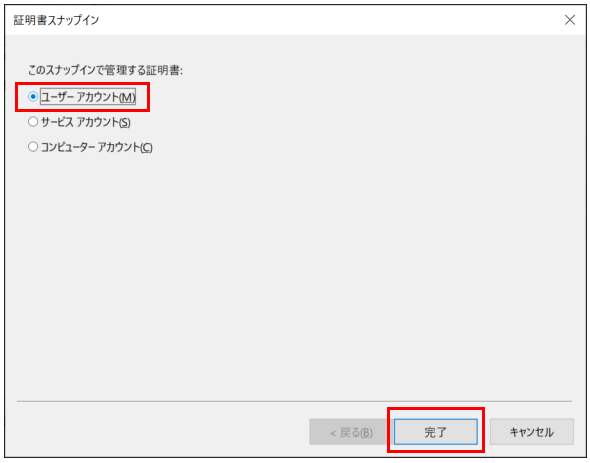
2.「ファイル」→「スナップインの追加と削除」の順にタップします。



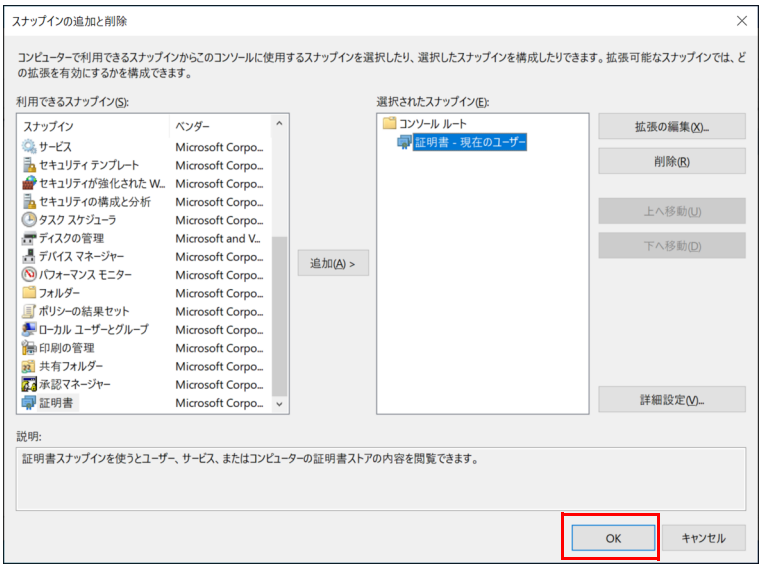
3.「証明書」を選択して「追加」をタップします。



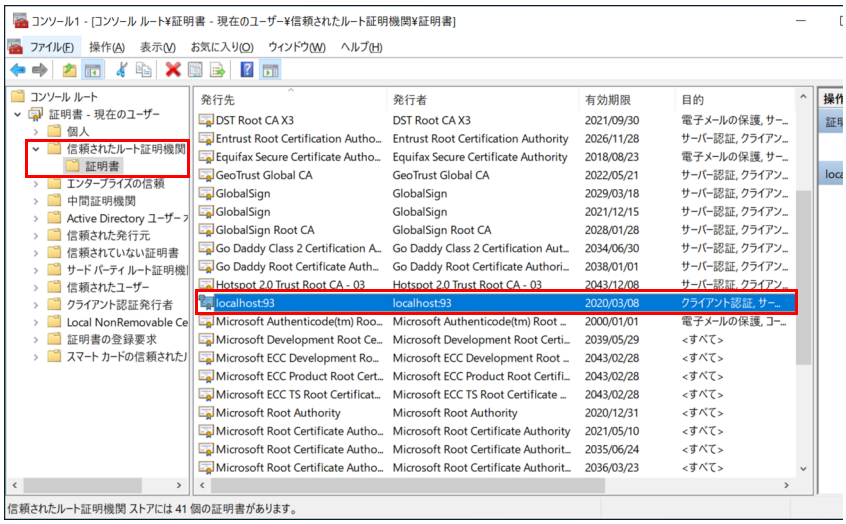
4.「ユーザーアカウント」を選択し「完了」をタップします。



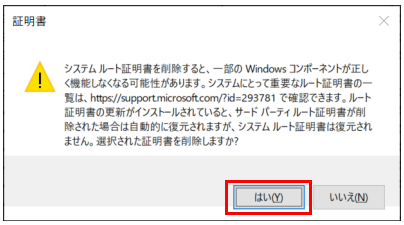
5.「OK」をタップします。



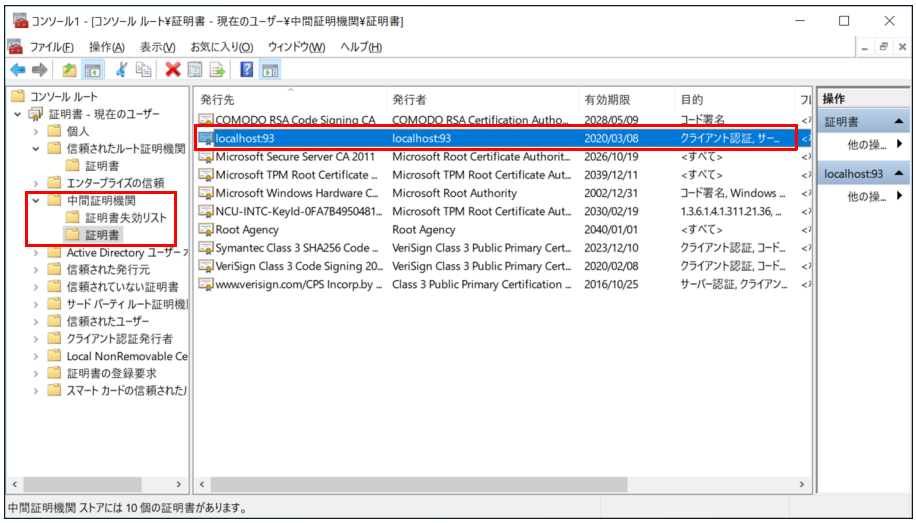
6.「信頼されたルート証明機関」→「証明書」の順にタップし、「localhost:93」を選択、右タップします。表示されたメニューから、「削除」をタップします。



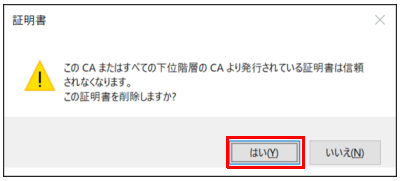
7.「はい」をタップします。



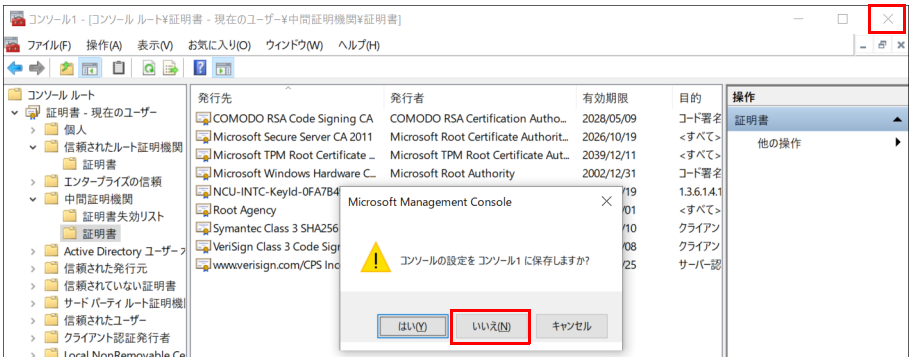
8.「中間証明機関」→「証明書」の順にタップし、「localhost:93」を選択、右タップします。表示されたメニューから、「削除」をタップします。



9.「はい」をタップします。



10.コンソール画面右上の × をタップし、「いいえ」をタップします。



クライアントアプリのインストーラーがダウンロードできない

●プロキシ設定が有効になっている可能性があります。
プロキシ設定を無効にして再度実施してください。
1.プロキシ設定を無効にします。
2.端末を再起動します。
3.端末認証設定をインストールします。
4.認証端末を登録します。
5.プロキシ設定を無効にします。
詳しくは、『導入ガイド』の「拡張機能 - セキュリティ（タブレット端末）」をご覧ください。

●ブラウザーのキャッシュデータを削除してください。
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）→「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。

●アクセスポイント部分の SSID を削除してください。
1.画面右下の通知領域の Wifi マークをタップします。
2.利用する本製品の SSID（この例では、「2nen_3kumi_5G」）を長押しタップして「削除」を選択します。
3.端末認証のクライアントアプリインストール専用の SSID「SWInstall-5G」を長押しタップして「削除」を選択します。

●IP アドレスをリリースしてください。
1.管理者権限でコマンドプロンプトを起動します（→ P.6）。
2. 次のコマンドを入力し、【Enter】キーを押します。
ipconfig /release

端末登録できない

●端末のセキュリティチップが無効になっている可能性があります。
端末認証ではセキュリティチップを使用します。セキュリティチップを有効にする方法は、端末のマニュアルをご覧ください。

エクスポートできない

●管理アプリケーション（制御部）のフォルダーにアクセス権がない可能性があります。
C:¥wifi-mgmg-nodejs¥work のアクセス権限を書き込み可能に設定してください。

端末登録済みだが、接続できない

●有効期限を過ぎていませんか？
有効期限を設定し直してください（→ P.62）。
有効期限を現在以降に設定しても接続できない場合、一度、端末情報を削除してください（→ P.61）。その後、登録し直してください（→ P.60）。

SSID に「SWInstall-5G」または、「SWRegist-5G」が表示される

●認証登録モードが「ON」になっている可能性があります。
端末の登録が完了している場合は、端末認証機能の管理画面で「認証登録モード」を「OFF」にしてください（→ P.59）。

ハードウェアのトラブル

ステータスランプ

ステータスランプが点灯している

●ステータスランプが点灯している場合は、次の手順で本製品を再起動してください。
1.電源ボタンを押します。
しばらくすると、本製品の電源が切れます。
2.電源プラグをコンセントから抜きます。
3.30 秒以上待ってから電源プラグをコンセントに付けます。
4.電源ボタンを押します。

アクセスポイント

端末が無線接続できない

●タブレット端末の無線 LAN 設定で、利用できる SSID の一覧に本製品の SSID が表示されない場合は、アクセスポイント部分から無線電波が出ていない可能性があります。
アクセスポイント部分の無線設定が正しく行われていることを確認してください。
●タブレット端末の無線 LAN 設定で、利用できる SSID の一覧に本製品の SSID が表示されている場合は、次の確認を行ってください。

- アクセスポイント部分の設定で、MAC アドレスフィルタリングが有効な場合、当該のタブレット端末が接続可能な設定になっていること。
- アクセスポイント部分の設定で接続端末数を指定した場合、設定した接続端末数より実際に接続している端末の台数がオーバーしていないこと。
- タブレット端末の認証キーなどのセキュリティ設定がアクセスポイント部分の設定と合っていること。
- タブレット端末の設定で、自動接続のチェックが付いていること。

AP Management の設定項目が変更できない

●AP Management の設定項目は、通常は変更の必要はありません。
AP Management の設定項目を変更する場合は、次の手順を実施してください。
1.WEB 設定画面にログインします。
2.「詳細設定」→「管理」→「AP Management」の順にクリックします。
3.ログファイルパスを「/tmp/syslog/messages」に変更します。
4.ログファイルパス以外の項目を設定します。
5.「適用」をクリックします。
アクセスポイント部分の RESET で設定を初期化した場合、再度、本手順を実行して設定してください。

WAN

ネットワークに接続できない

●ネットワークケーブルは正しく接続されていますか？
●ネットワークケーブルに関して、次の項目を確認してください。

- ケーブルのコネクタやケーブルは損傷していませんか？
- 使用するネットワーク環境に合ったケーブルを使っていますか？

ネットワークの設定については、ネットワーク管理者に確認してください。

通信速度が遅い

●ネットワーク機器の電源を入れてから本製品に電源ケーブルを接続して電源を入れてください。また、本製品の使用中に LAN ケーブルを抜いたり、ネットワーク機器の電源をオフにしたりしないでください。
ネットワーク機器との接続ができなくなったり、通信速度が極端に低下したりする場合があります。
例：1000Mbps で通信していたのに 10Mbps の速度になる
ネットワーク機器との接続ができない場合は、ネットワーク機器の電源が入っていること、および LAN ケーブルで本製品とネットワーク機器が接続されていることを確認後、製品本体を再起動してください。

その他

「ジー」「キーン」という音がする

●静かな場所では、「ジー」「キーン」という製品本体内部の電子回路の動作音が聞こえる場合があります。
故障ではありませんので、そのままお使いください。

エラーメッセージ一覧

ここでは、本製品が表示するメッセージと、その対処方法を説明しています。
エラーメッセージ一覧には、お使いの製品に搭載されているハードウェアによっては、表示されないメッセージも含まれています。
本書に記載されていないエラーメッセージが表示された場合は、「富士通ハードウェア修理相談センター」、またはご購入元にご連絡ください。

起動時に表示されるエラーメッセージ

起動時の自己診断（POST）で異常が見つかった場合に表示されるメッセージは、次のとおりです。

重要

- エラーメッセージが表示された場合は、ご購入元に確認してください。対処を行った後にBIOSセットアップを起動し、「終了」メニューの「変更を保存して終了する（再起動）」または「変更を保存して終了する（電源OFF）」を実行してください。

BIOS セットアップメニューについては、『BIOS 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。

無線 LAN 診断で表示されるエラーメッセージ

無線 LAN 診断で異常が見つかった場合に表示されるメッセージは、次のとおりです。

エラーコード		状態	対処方法	備考
	詳細			
1	アクセスポイント Login Fail（アクセスポイントログイン失敗）	診断サーバー PC がアクセスポイントにログインできない	・アクセスポイント状態表示ランプが正常に点灯していることを確認してください（→ P.9）。 ・コンピューター部分とアクセスポイント部分を接続している 2 本のケーブルが、正しく接続していることを確認してください。特に LAN ケーブルが半抜けになっていないことを確認してください。 ・本製品の電源を切って、電源ランプ（→ P.8）が消灯したことを確認した後、コンセントから電源プラグを抜き、30 秒程度待ってから再度、コンセントに接続してください。 ・アクセスポイント部分の RESET ボタンを 5 秒未満押してリセットを実行してください（→ P.9）。	本製品が自身にログインする行為のため 物理的な問題が想定されます。
3	Node No IP Address（IP なし）	該当端末のIPをアクセスポイントが取得できていない	・端末の SSID を切断して再度、接続してください。 ・端末の DHCP 設定を確認してください。 ・端末を再起動してください。 ・端末の無線 IP アドレスを確認してください。 ・端末の無線 LAN のパスワードに間違いがないことを確認してください。	アクセスポイントの機能として端末の IP アドレスの更新に 2 分程度かかります。 このため無線切断した状態から接続した最初のタイミングによっては本診断となる可能性があります。
4	Node DHCP Fail（DHCP 失敗）	該当端末に IP アドレスが DHCP サーバーから割り振られていない状態	・端末の SSID を切断して再度、接続してください。 ・端末の DHCP 設定を確認してください。 ・端末を再起動してください。 ・端末の無線 IP アドレスを確認してください。 ・端末の無線 LAN のパスワードに間違いがないことを確認してください。	ブリッジモードで動作している場合は、DHCP の確認は行いません。 「IP アドレスなし」と診断されます。
7	Node Connection Fail（接続失敗）	該当端末がアクセスポイントとの接続に失敗した状態	・端末の SSID を切断して再度、接続してください。 ・端末の設定（無線 LAN のパスワード、認証設定）を確認してください。	端末が本製品から離れることでも、発生します。
8	Node RSSI low（RSSI 低下）	該当端末からの RSSI が低下して通信が切断された状態	・本製品の近くで、端末の SSID を再度、接続してください。 ・周囲に障害物がある場合は、取り除いてください。	端末が本製品から離れることでも、発生します。
9	Node Interference（干渉）	該当端末が干渉によって通信が切断された状態	・本製品の電源を切って、電源ランプ（→ P.8）が消灯したことを確認した後、コンセントから電源プラグを抜き、30 秒程度待ってから再度、コンセントに接続してください。 ・端末の SSID を切断して再度、接続してください。 ・すべての端末で切断する症状が出ている場合は、無線チャネルの設定を見直す必要があります。	頻発する場合は、アクセスポイント部分の無線チャネルの設定を自動にする必要があります。 端末が本製品から離れることでも、発生します。
10	Node Authentication or Other Error（認証または他の端末問題）	上記以外の理由で該当端末が切断された状態	・端末の SSID を切断して再度、接続してください。 ・端末の DHCP 設定を確認してください。 ・端末を再起動してください。 ・端末の無線 IP アドレスを確認してください。 ・端末の無線 LAN のパスワードに間違いがないことを確認してください。	端末が本製品から離れることでも、発生します。
12	アクセスポイント Setting Fail（アクセスポイント設定異常）	アクセスポイントの設定が基準値から変化している	・アクセスポイント部分の設定変更がなかったか確認してください。 ・本製品の電源を切って、電源ランプ（→ P.8）が消灯したことを確認した後、コンセントから電源プラグを抜き、30 秒程度待ってから再度、コンセントに接続してください。	
13	アクセスポイント Fail（アクセスポイント異常）	アクセスポイントがハングアップや認証処理の不具合などで正常に動作していない状態	・本製品の電源を切って、電源ランプ（→ P.8）が消灯したことを確認した後、コンセントから電源プラグを抜き、30 秒程度待ってから再度、コンセントに接続してください。 ・周辺に遮へいするような障害物がないことを確認してください。	

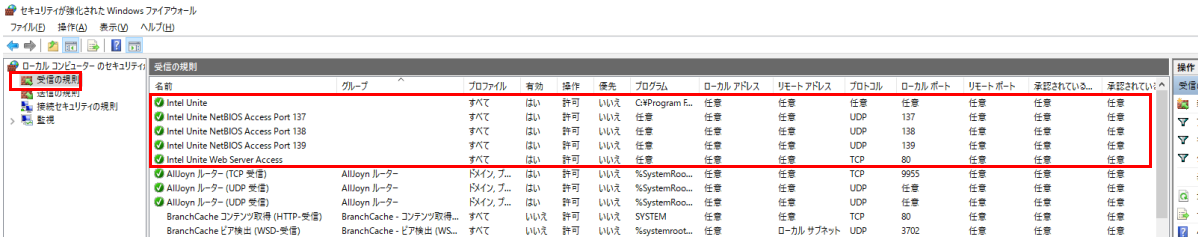
Intel Unite のファイアウォールの設定

本製品のファイアウォールの設定で Intel Unite の通信を許可する必要があります。なお、これらの設定は、ご購入時に設定されています。
なお、市販のセキュリティ対策ソフトをインストールしている場合は、セキュリティ対策ソフトのマニュアルをご覧になり、設定を確認してください。

1 **「コントロールパネル」を表示します（→ P.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 ファイアウォール」→「詳細設定」の順にクリックします。**
「セキュリティが強化された Window ファイアウォール」が表示されます。

3 **「受信の規則」をクリックし、下の図のように設定されていることを確認します。**



設定がない場合は、本製品から Intel Unite をアンインストールして、再インストールしてください。

3. それでも解決できないときは

故障かなと思われたときや、技術的なご質問・ご相談などについては、「問い合わせ先」をご覧になり、弊社までお問い合わせください。

ファームウェアと BIOS のアップデート

本製品のアクセスポイント部分やコンピューター部分を修理した後に、アクセスポイントのファームウェアや BIOS などがアップデート前の版数になることがあります。弊社ホームページの「ドライバダウンロード」（http://www.fmworld.net/biz/fmv/index_down.html）から最新版を入手してアップデートしてください。

問い合わせ先

マニュアルをご覧になっても不明な点がございましたらお問い合わせください。
お問い合わせの前に、製品本体のラベルまたは保証書に記載されている、型名（MODEL）、製造番号（SERIAL）、16 桁の数字（0000-0000-0000-0000）または（0000000-00-0000-000）をご確認ください。

こんなときには	こちらへ
故障かなと思われたとき	富士通ハードウェア修理相談センター https://eservice.fujitsu.com/webrepair/ 「修理ご相談チャット」で 24 時間いつでも、故障診断、修理費用のご案内から、修理のお申し込みまでできます。
	お電話でのご相談が必要な場合は、次におかけください。 通話料無料　0120-422-297 受付時間　　9：00 ～ 17：00（土曜、日曜、祝日および年末年始を除く）
技術的なご質問、ご相談	ご購入元（販売会社または富士通の担当営業、SE）にご相談ください。
	個人のお客様など、ご相談先がご不明の場合は、次の窓口へお問い合わせください。 富士通パーソナル製品に関するお問い合わせ窓口 （運営：富士通クライアントコンピューティング株式会社） 通話料無料　0120-950-222 受付時間　　9：00 ～ 17：00（土曜、日曜、祝日およびシステムメンテナンス日を除く） 受け付け後に専門技術員からのコールバックとなります。

・ おかけ間違いのないよう、ご注意ください。
・ 各窓口ともダイヤル後、音声ガイダンスに従い、ボタン操作を行ってください。お客様の相談内容によって、各窓口へご案内いたします。
・ システムメンテナンスのため、受付時間であっても受け付けを休止させていただく場合があります。

8

第 8 章
付録

1. 仕様 120
2. VESA マウントの取り付け／取り外し 125

1. 仕様

ESPRIMO Edge Computing Edition Z0110/E

コンピューター部分

項目			仕様
CPU 注 1	名称		インテル® Core™i5-7500T プロセッサー
	動作周波数		2.70 GHz （最大 3.30 GHz 注 2）
	コア数／スレッド数		4/4
	キャッシュメモリ		3 次：6MB
チップセット			インテル® Q270
システムバス			8GT/s DMI 注 3
メインメモリ			標準 16GB （PC4-2400 DDR4 SDRAM SO-DIMM CL15 ECC なし）
メモリースロット			×2 注 4
表示機能	グラフィックスアクセラレータ		Intel® HD Graphics 630
	ビデオメモリ		メインメモリと共用
	解像度／発色数	DisplayPort	最大 3840×2160 ドット／最大 1677 万色
	DirectX		12.0
	OpenGL		4.4
ストレージ注 5			フラッシュメモリディスク 標準 128GB/ 最大 256GB 注 6
セキュリティ機能			
	セキュリティチップ（TPM）注 7		あり
	盗難防止用ロック取り付け穴		あり
	筐体施錠		あり
インターフェース			
	外部ディスプレイ	DisplayPort	2 ポート
		HDMI	1 ポート注 8
	シリアル注 9		非同期 RS-232C 準拠 D-SUB 9 ピン ×1（16550A 互換）
	USB 注 10		USB3.0 準拠 ×4（前面 ×2、背面 ×2）注 11
	LAN		RJ-45×2（アクセスポイント部との接続で 1 ポート使用、取り外し不可）
自己診断（POST）時			あり注 12
サポート OS			Windows 10 IoT Enterprise 2016 LTSB

本製品の仕様は、改善のために予告なく変更することがあります。あらかじめご了承ください。

注 1 ：・ソフトウェアによっては、CPU 名表記が異なる場合があります。
・本製品に搭載されている CPU で使用できる主な機能については、「CPU」（→ P.122）をご覧ください。

注 2 ：インテル® ターボ・ブースト・テクノロジー 2.0 動作時。

注 3 ：DMI は Direct Media Interface の略です。

注 4 ：空きメモリスロットは 1 つありますが、メモリの増設は保証していません。

注 5 ：容量は、1GB=1000^3 バイト換算値です。

注 6 ：カスタムメイドオプションの選択により、フラッシュメモリディスク 256GB（M.2NVMe）が搭載されます。

注 7 ：チップセット内蔵のセキュリティ機能（Intel® PTT）を使用することができます。

注 8 ：標準添付品のケーブル（DP-HDMI 変換ケーブル）使用時

注 9 ：すべてのシリアル対応周辺機器の動作を保証するものではありません。

注 10：すべての USB 対応周辺機器の動作を保証するものではありません。

注 11：USB3.0 の場合、外部から電源が供給されない USB 対応周辺機器を接続するときの消費電流の最大容量は、1 ポートにつき 900mA です。
詳しくは、USB 対応周辺機器のマニュアルをご覧ください。

注 12：起動時の自己診断（POST）で異常が見つかった場合に表示されるメッセージについては「起動時に表示されるエラーメッセージ」（→ P.115）を参照してください。

アクセスポイント部分

項目	仕様		
WAN	1000BASE-T ／ 100BASE-TX ／ 10BASE-T 準拠[注 1]		
	インターフェース		RJ-45
	転送レート		1000Mbps / 100Mbps / 10Mbps
無線 LAN インターフェース	IEEE 802.11ac 準拠	周波数 / チャンネル	[W52] 5.2GHz（5150 - 5250）: 36 40 44 48ch [注 2] [W53] 5.3GHz（5250 - 5350）: 52 56 60 64ch [注 2] [W56] 5.6GHz（5470 - 5725）: 100 104 108 112 116 120 124 128 132 136 140ch
		変調方式[注 3]	OFDM / サブキャリアの数 [VHT20]:56 [VHT40]:114 [VTH80]:242, MIMO
		転送レート	5.2GHz （W52） 5.3GHz （W53） 5.6GHz （W56） 最大 1733Mbps （VHT80）
	IEEE 802.11n 準拠	周波数 / チャンネル	2.4GHz（2400 - 2484MHz）: 1- 13ch [W52] 5.2GHz（5150 - 5250）: 36 40 44 48ch [注 2] [W53] 5.3GHz（5250 - 5350）: 52 56 60 64ch [注 2] [W56] 5.6GHz（5470 - 5725）: 100 104 108 112 116 120 124 128 132 136 140ch
		変調方式[注 4]	OFDM / サブキャリアの数 [HT20]:56 [HT40]:114, MIMO
		転送レート	2.4GHz 最大 450Mbps（HT40） 5.2GHz （W52） 5.3GHz （W53） 5.6GHz （W56） 最大 600Mbps（HT4）
	IEEE 802.11a 準拠	周波数 / チャンネル	[W52] 5.2GHz （5150 - 5250）: 36 40 44 48ch [注 2] [W53] 5.3GHz （5250 - 5350）: 52 56 60 64ch [注 2] [W56] 5.6GHz （5470 - 5725）: 100 104 108 112 116 120 124 128 132 136 140ch
		変調方式	OFDM / サブキャリアの数 :52
		転送レート	54/48/36/24/28/12/9/6Mbps
無線 LAN インターフェース	IEEE 802.11g 準拠	周波数 / チャンネル	2.4GHz（2400 - 2484MHz）: 1- 13ch
		変調方式	OFDM / サブキャリアの数 :52
		転送レート	54/48/36/24/28/12/9/6Mbps
	IEEE 802.11b 準拠	周波数 / チャンネル	2.4GHz（2400 - 2484MHz）: 1- 13ch
		変調方式	DS-SS
		転送レート	11 / 5.5 / 2 / 1 Mbps
	アンテナ	5GHz : Tx4 x Rx4 2.4GHz : Tx2 x Rx2	
	セキュリティ[注 5]	SSID（ネットワーク名）、MAC アドレスフィルタリング機能 WEP（セキュリティキー（WEP キー）: 128 ビット）[注 6] WPA2-PSK（AES）, WPA/WPA2-PSK（AES）, WPA/WPA2-PSK（AES/TKIP）, エンタープライズ	
無線 LAN 準処規格	ARIB 標準規格（日本）		
	IEEE 標準規格	IEEE 802.11 a/b/g, 802.11n, 802.11d, 802.11e,802.11h, 802.11i	
		IEEE 802.11 ac（Wi-Fi® 準拠）[注 7]	
		IEEE 802.1D, 802.1Q	
		IEEE 802.3 802.3az, 802.3u	
	マルチメディア	Wi-Fi マルチメディア（WMM）	
USB	USB3.0 Type-B（給電用）		
インジケーター	状態表示ランプ		
RESET ボタン	システムリセット		
使用プロトコル	TCP/IP プロトコル		
ネットワーク管理	SNMP V1/V2/V3 トラップ対応 標準 MIB		
その他	無線 QoS,00000JAPAN 対応、44 台同時接続		

注 1 ： ・ 1000Mbps は 1000BASE-T の理論上の最高速度であり、実際の通信速度はお使いの機器やネットワーク環境により変化します。
・ 1000Mbps の通信を行うためには、1000BASE-T に対応したハブが必要となります。また、LAN ケーブルには、1000BASE-T に対応したエンハンスドカテゴリー 5（カテゴリー 5E）以上の LAN ケーブルを使用してください。

注 2 ： 屋内で使用してください。5.2/5.3GHz 帯の屋外での使用は、電波法により禁じられています（法廷により許可された場合を除く）。

注 3 ： IEEE 802.11ac を使用する際の無線 LAN アクセスポイントの設定で、VHT40/80 の機能を有効にする場合には、周囲の電波状況を確認して他の無線局に電波干渉を与えないことを事前に確認してください。万一、他の無線局において電波干渉が発生した場合には、ただちに VHT40/80 の機能を無効にしてください。

注 4 ： IEEE 802.11n を使用する際の無線 LAN アクセスポイントの設定で、HT40 の機能を有効にする場合には、周囲の電波状況を確認して他の無線局に電波干渉を与えないことを事前に確認してください。万一、他の無線局において電波干渉が発生した場合には、ただちに HT40 の機能を無効にしてください。

注 5 ： IEEE 802.11n、IEEE 802.11ac で接続するためには、パスフレーズ（PSK）を AES に設定する必要があります。

注 6 ： WEP による暗号化は上記ビット数で行いますが、ユーザーが設定可能なビット数は固定長 24 ビットを引いた 40 ビット /104 ビットです。

注 7 ： Wi-Fi® 準拠とは、無線 LAN の相互接続性を保証する団体「Wi-Fi Alliance®」の相互接続性テストに合格していることを示します。

エッジコンピューティングデバイス本体

項目			仕様
質量			約 2.4kg
電源／周波数			AC100V±10%、50/60Hz +2% -4%（入力波形は正弦波のみサポート）
消費電力	電源オフ時 注 1		約 5.7W
	動作時 注 2（通常時／最大時 注 3）		約 17W ／約 48W
	最大消費電力		約 75W
定格電流		動作時	最大 1.5A
外形寸法（突起部含まず）		アンテナをたたんだ状態	W190×D185×H 91.5mm
		アンテナを立てた状態	W 190×D185×H 214.9mm
電波障害対策			VCCI クラス B
国際エネルギースタープログラム 注 4			なし
温湿度条件			温度 10 ～ 35 ℃／湿度 20 ～ 80%RH（動作時） 温度 -10 ～ 60 ℃／湿度 20 ～ 80%RH（非動作時）

本製品の仕様は、改善のために予告なく変更することがあります。あらかじめご了承ください。

注 1 ： 消費電力を 0 にするには、電源ケーブルをコンセントから抜いてください。

注 2 ： ・ご使用になる機器構成により値は変動します。

・標準構成で OS を起動させた状態での本体のみの測定値です。

注 3 ： 測定プログラムは当社独自の高負荷テストプログラムを使用しています。

注 4 ：「国際エネルギースタープログラム」は、長時間電源を入れた状態になりがちなオフィス機器の消費電力を削減するための制度です。

CPU

本製品に搭載されている CPU で使用できる主な機能は、次のとおりです。

お使いの本製品本体に搭載されている CPU の欄をご覧ください。

機能	インテル® Core™ i5-7500T プロセッサー
インテル® ターボ・ブースト・テクノロジー 2.0	○
インテル® バーチャライゼーション・テクノロジー	○
拡張版 Intel SpeedStep® テクノロジー（EIST）	○
エグゼキュート・ディスエーブル・ビット機能	○

インテル® ターボ・ブースト・テクノロジー 2.0

インテル® ターボ・ブースト・テクノロジー 2.0 は、従来のマルチコアの使用状況にあわせて CPU が処理能力を自動的に向上させる機能に加え、高負荷時にパフォーマンスを引き上げるように最適化された機能です。

POINT

- OSおよびソフトウェアの動作状況や設置環境などにより処理能力量は変わります。性能向上量は保証できません。

インテル® バーチャライゼーション・テクノロジー

インテル® バーチャライゼーション・テクノロジーは、本機能をサポートする VMM（仮想マシンモニター）をインストールすることによって、仮想マシンの性能と安全性を向上させるための機能です。
この機能はご購入時には有効に設定されています。設定は BIOS セットアップで変更できます。

拡張版 Intel SpeedStep® テクノロジー（EIST）

拡張版 Intel SpeedStep® テクノロジーは、実行中のソフトウェアの CPU 負荷に合わせて、Windows が CPU の動作周波数および動作電圧を自動的に低下させる機能です。

POINT

- この機能により本製品の性能が低下することがあります。お使いの環境で性能の低下が気になる場合は、電源プランを「高パフォーマンス」に切り替えてください。

エグゼキュート・ディスエーブル・ビット機能

エグゼキュート・ディスエーブル・ビット機能は、Windows のデータ実行防止（DEP）機能と連動し、悪意のあるプログラムが不正なメモリ領域を使用すること（バッファー・オーバーフロー脆弱性）を防ぎます。
データ実行防止（DEP）機能がウイルスやその他の脅威を検出した場合、「[ソフトウェア名称] は動作を停止しました」という画面が表示されます。「プログラムの終了」をクリックし、表示される対処方法に従ってください。

アプリの動作環境

ここでは、各アプリの動作環境と注意事項を説明します。

アプリの動作環境と注意事項

●添付のアプリは、本製品と本製品にアクセスする端末でご使用いただけます。

●次の富士通製文教向けタブレットで動作検証を実施しています。

ARROWS Tab Q508/SE、Q509/VE、Q5010/CE、Q739/AE

その他の機種をお使いの場合は、お客様にて事前に検証を実施したうえでお使いください。

●動作検証は次の環境で実施しております。

Windows 10 Pro（64 ビット版）、version 1903 以降 で実施しております。

●本製品のすべての機能をタブレット端末にインストールする場合、ハードディスクの空き容量は 130MB 以上必要です。

●各アプリの動作環境と注意事項については、次の表をご覧ください。

名称	動作環境と注意事項
管理画面	・対象 OS は Windows 10 、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 - 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。
インターネットキャッシュ機能	・対象 OS は Windows 10 、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 - 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学校内のネットワーク環境により異なります。 ・キャッシュできるプロトコルは http になります。 ご購入時に、https プロトコルはキャッシュできません。最新のアプリにアップデートすることで https プロトコルがキャッシュできるようになります。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。 https プロトコルをキャッシュする場合は、『アプリアップデートガイド』をご覧になり「インターネットキャッシュ機能 V4.1.0」をインストールしてください。 ・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 2GB（デフォルト 1GB）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 V4.1.0 の留意事項については、マニュアル『アプリアップデートガイド』をご覧ください。 ・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。

名称	動作環境と注意事項
サーバファイルキャッシュ機能	・連携する学習支援アプリケーションのサポート対象環境に準じます。お客様にて事前に検証を実施した上でお使いください。 ・キャッシュによる効果はご使用になる学校内のネットワーク環境により異なります。 ・ご使用になるには連携する学習支援アプリケーション側の対応と、それに応じた設定が必要です。 「FUJITSU 文教ソリューション K-12 学習情報活用 知恵たま」は標準で対応しています。
動作状態監視ツール	・監視対象はご使用される機能に応じて、設定変更する必要があります。
お手入れナビ	―
端末情報収集ツール	・本製品と組み合わせてお使いになるタブレット端末のサポート対象は富士通製文教向けタブレットのみとなります。
無線 LAN 診断	―
優先接続設定	・優先接続設定で優先されるのは本製品 1 台につき、端末 1 台のみです。 ・本製品と組み合わせてお使いになるタブレット端末のサポート対象は Windows 10 Pro（64 ビット版）, version 1809 以降の OS を搭載した機種となります。お客様にて事前に検証を実施したうえでお使いください。
無線 LAN 接続台数表	・無線 LAN 診断は、本製品のアクセスポイント部分に接続された端末の台数が表示されます。 ・この機能は本製品以外のアクセスポイントでは使用できません。 ・本製品と組み合わせてお使いになるタブレット端末のサポート対象は富士通製文教向けタブレットのみとなります。
Intel Unite	・解像度を低くした場合に正しく表示されないことがあります。最大解像度でお使いになることをお勧めします。 フル HD（1920×1080）、またはアスペクト比が 16 対 9 の画面表示機器を接続することを推奨します。 ・Intel Unite のサポート対象端末は以下の OS を搭載した端末となります。 - Windows 10 Pro, version 20H2 - Windows 10 Pro, version 20H1 - Windows 10 Pro, version 1809 - Windows 10 Pro, version 1903 - Windows 10 Pro, version 1909 - Windows 8.1 - macOS 10.13.5 ～ 10.15.5 - iOS 11.2.6 ～ 13.3.1 ※上記OSを搭載した機種全ての動作を保証するものではありません。お客様にて事前に検証を実施した上でお使いください。 ※ 上記以外のバージョンの対応状況については別途お問い合わせください。
端末認証	・タブレット端末のサポート対象は、Windows 10 Pro（64 ビット版）を搭載し、セキュリティチップ（Intel® PTT）をサポートしている端末環境となります。 ・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）

使用するポート

アプリ名称	ポート番号
管理画面	10080
インターネットキャッシュ機能	8080、3130、443、8000
サーバファイルキャッシュ機能	8002、8003
メンテナンス機能	9200、9300、18080、18081、18090、18091、18092、18093、18094、9600
端末認証	1812、1813、9000、8001、8010
Intel Unite	80

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。

2. 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

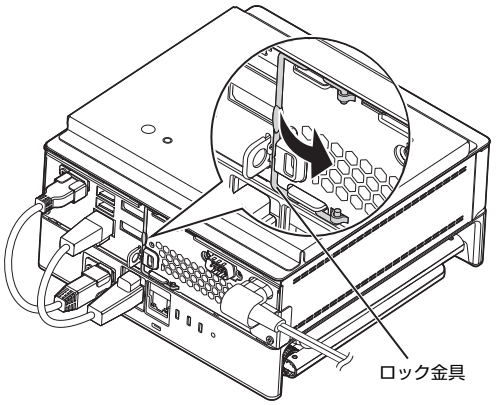
1 本製品の電源を切り、アンテナをたたみます。また、電源プラグをコンセントから取り外した後、専用ケーブルを除く本製品に接続しているすべてのケーブルを取り外します。

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。

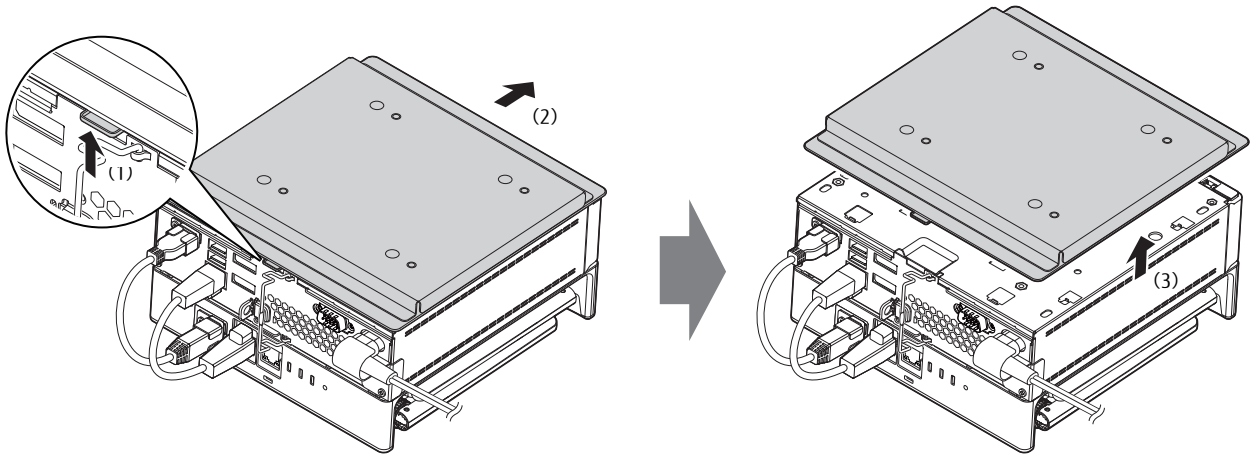
3 壁掛け金具から本製品を取り外します。取り外し方法については、壁掛け金具のマニュアルをご覧ください。

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。



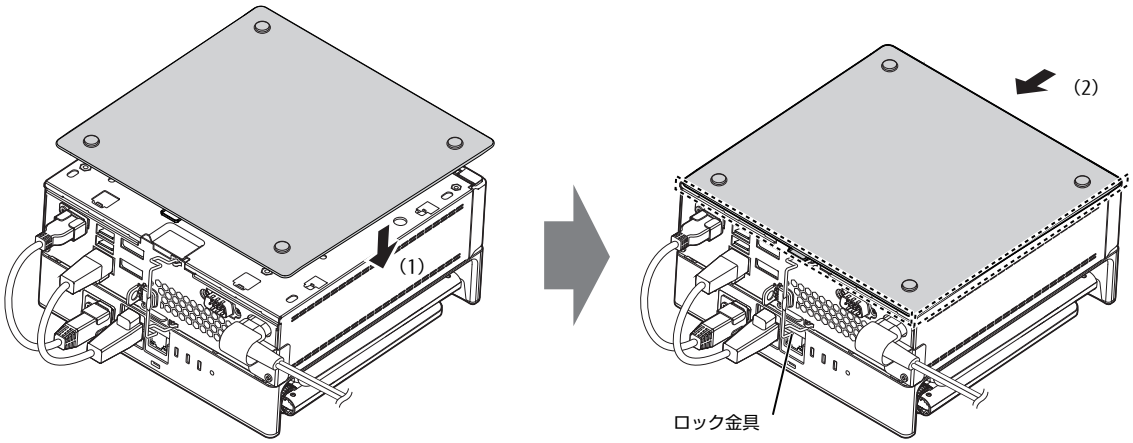
6 （1）本製品背面のツメを上に押し上げながら、（2）VESA マウントを本製品の前面側に（5mm 程度）スライドさせ、（3）そのまま VESA マウントを上に持ち上げます。



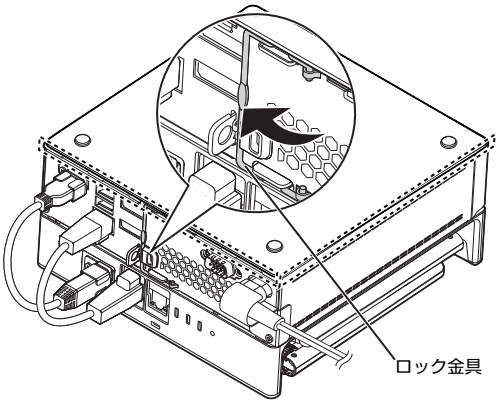
VESA マウントを取り外した後、底面カバーを取り付けてください（→ P.126）。

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

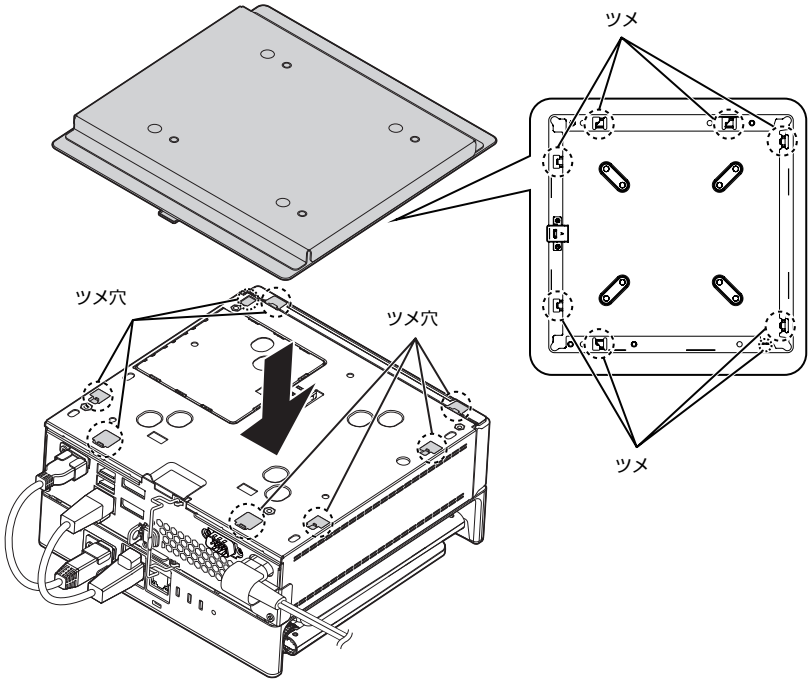
■ 壁掛けの設置は専門の取付工事業者にご依頼すると共に落下防止措置を講じてください。

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。

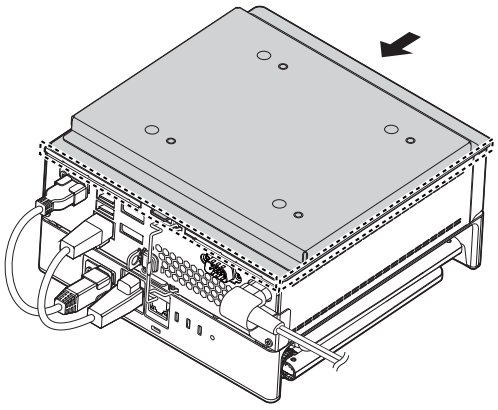
VESA マウント取り付け

1　底面カバーを取り外します。
「VESA マウントの取り外し」（→ P.125）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。

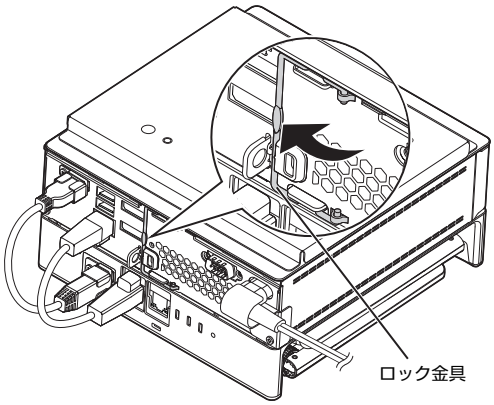
2　本体のツメ穴に VESA マウント内側のツメがはまるようにまっすぐに下ろします。



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。



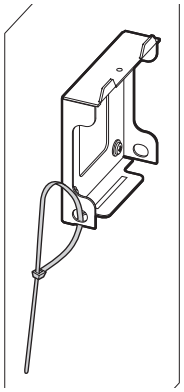
4 本体背面のロック金具を矢印の向きに動かしてロックします。



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。

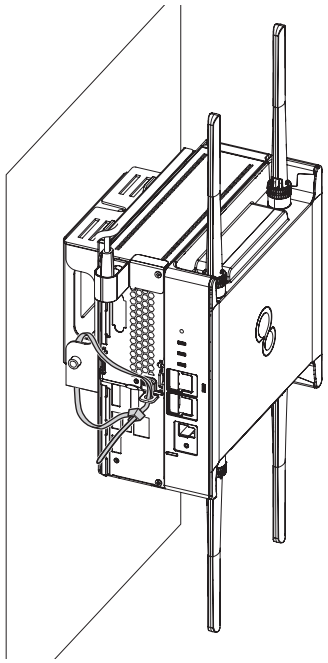


2 壁側の壁掛け金具に本製品を取り付けます。
壁掛け金具を取り付けおよび設置については、壁掛け金具のマニュアルをご覧ください。

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。



ESPRIMO Edge Computing Edition Z0110/E
管理ガイド
B6FY-4771-02 Z0-01
発 行 日　　2021 年 1 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