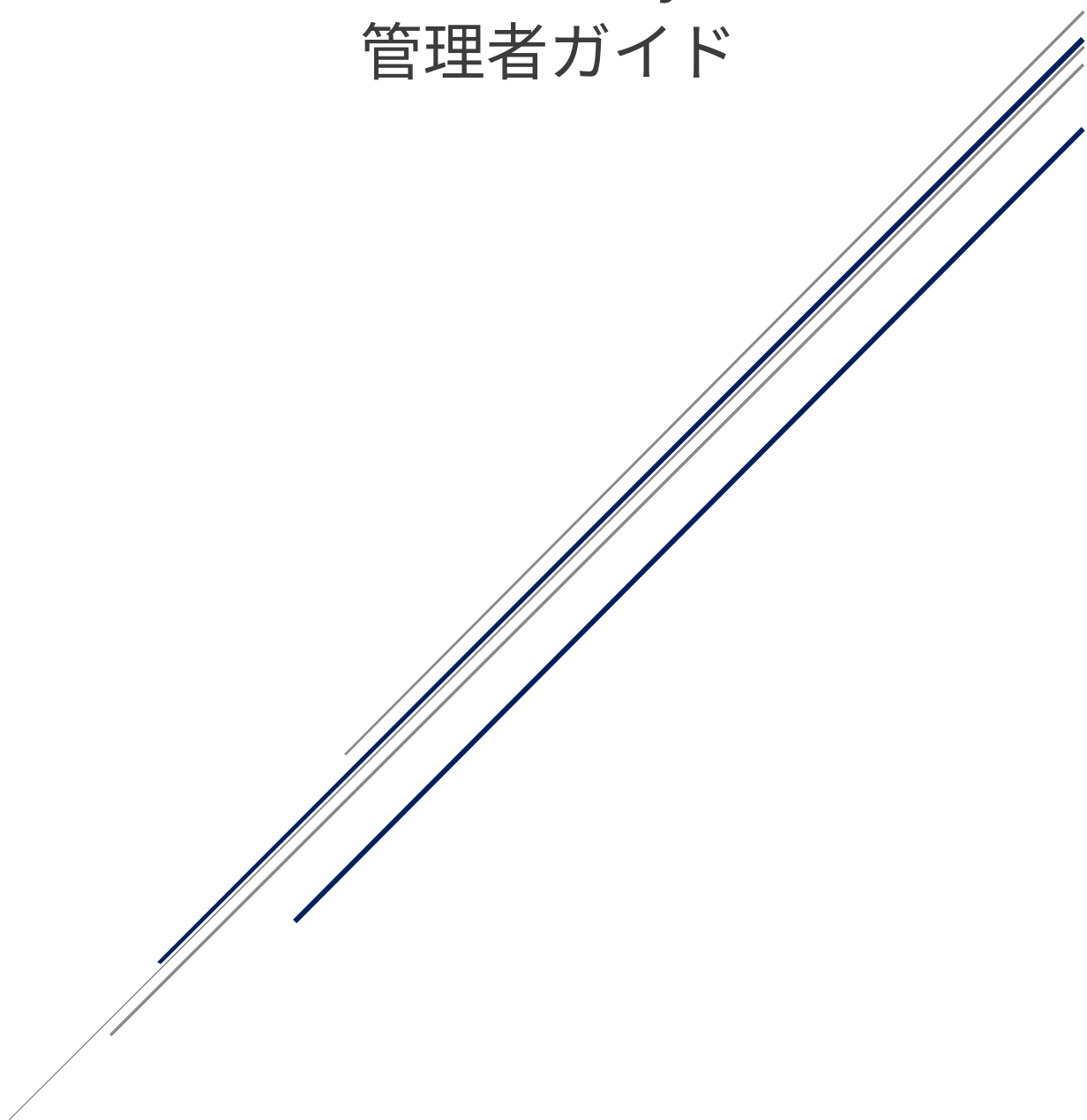


WithSecure™

Elements Security Center

管理者ガイド



W / T H®
secure

ウィズセキュア株式会社

改版履歴

履歴	リビジョン	リリース日
初版	1.0	2022/09/30

●免責事項

本書は、本書記述時点の情報を基に記述されており、特に断りのない限り、本書内の記述は、本書記載時の製品のバージョンを基にしております。例の中で使用されている会社、名前およびデータは、別途記載のない限り架空のものとなります。

ウィズセキュア株式会社（以下、弊社）は、本書の情報の正確さに万全を期していますが、本書に記載されている情報の誤り、脱落、または、本書の情報に基づいた運用の結果について、弊社は、如何なる責任も負わないものとします。本書に記載されている仕様は、予告なく変更される場合があります。

本書は 2022 年 9 月現在の情報を基に記述されております

●商標

WithSecure™および四角形の記号はウィズセキュア株式会社の登録商標です。また、弊社の製品名および記号／ロゴは、いずれも弊社の商標です。本書に記載されている全ての製品名は、該当各社の商標または登録商標です。弊社では、自社に属さない商標および商標名に関する、いかなる所有上の利益も放棄します。

●複製の禁止

本書の著作権は弊社が保有しており、弊社による許諾無く、本書の一部であっても複製することはできません。また、譲渡もできません。

●お問い合わせ

弊社は常に資料の改善に取り組んでいます。そのため、本書に関するご質問、ご意見、ご要望等ございましたら、是非 japan@withsecure.com までご連絡ください。

目次

1.	はじめに	9
2.	Elements Security Center 概要	10
2.1.	対応ブラウザ	10
2.2.	Elements EPP の構成要素.....	10
2.3.	Elements Security Center のアカウントの概念	11
2.4.	ライセンスキーの概念	12
2.5.	使用開始までの流れ.....	12
3.	Elements Security Center への接続とログイン	13
4.	Elements Security Center の操作メニュー	14
4.1.	Elements Security Center の操作メニュー概要	14
5.	Elements EPP の操作メニュー	17
5.1.	Elements EPP の操作メニュー概要	17
5.2.	サイドメニュー [ダッシュボード].....	18
5.3.	新規デバイスを追加	19
6.	デバイス	21
6.1.	[デバイス] の操作メニュー概要	21
6.2.	“コンピュータ” タブ アクションメニュー	22
6.2.1.	デバイスの招待状を管理する	23
6.2.2.	自動削除を管理する.....	24
6.2.3.	運用の管理.....	25
6.3.	“モバイルデバイス” タブ アクションメニュー	26
6.4.	“Connector” タブ アクションメニュー	27
6.5.	コンピュータ[表示]の切り替え	28
6.6.	モバイルデバイス[表示]の切り替え	30
6.7.	Connector [表示]の切り替え	31
7.	コンピュータへの操作	32
7.1.	処理項目	32
7.2.	処理内容	34
7.2.1.	ステータスアップデートを送る.....	34
7.2.2.	ソフトウェアアップデートをインストール.....	35
7.2.3.	スキャン.....	36
7.2.4.	プロファイルを指定する	37
7.2.5.	ラベルを管理する	38

7.2.6.	ライセンスを変更する	39
7.2.7.	デバイスを削除する	40
7.2.8.	ネットワークの隔離	42
7.2.9.	システムを再起動する	43
7.2.10.	診断ファイルを要求する	44
7.2.11.	デバイスにメッセージを送信する	45
7.2.12.	アンインストール	46
8.	モバイルデバイスへの操作	47
8.1.	処理項目	47
8.2.	処理内容	48
8.2.1.	プロファイルを指定する	48
8.2.2.	ラベルを管理する	49
8.2.3.	デバイスを削除する	51
9.	ソフトウェアのアップデート	52
9.1.	[ソフトウェアのアップデート] 操作メニュー概要	52
9.1.1.	アクションメニュー	52
9.2.	タブメニュー	53
9.2.1.	適応されていないアップデート	53
9.2.2.	インスールの概要	55
9.2.3.	インストール履歴	57
9.3.	すべてのコンピュータで更新	59
9.4.	すべてのサーバで更新	60
9.5.	アップデートするデバイスの選択	61
10.	レポート	62
10.1.	[レポート] の操作メニュー概要	62
10.2.	アクションメニュー	62
10.3.	レポートのサマリ送信	63
10.4.	タブメニュー	64
10.5.	保護ステータス	64
10.5.1.	Computer Protection のステータス	64
10.5.2.	コンピュータに適用されている最新のマルウェア定義ファイル	65
10.6.	セキュリティイベント	66
10.6.1.	ブロックした脅威- コンピュータ (上位)	66
10.6.2.	感染	67
10.6.3.	処理した脅威	67
10.7.	脅威	68
10.7.1.	脅威レポートのエクスポート	68

10.7.2.	脅威の警告を設定する	69
10.8.	ライセンスの使用状況	71
10.9.	ソフトウェア アップデート	72
10.10.	監査ログ	73
10.11.	デバイス	74
10.11.1.	クライアントバージョン別の Windows デバイス	74
10.11.2.	クライアントバージョン別の Mac デバイス	74
10.11.3.	クライアントバージョン別のモバイルデバイス	75
10.11.4.	クライアントバージョン別の Connector デバイス	75
10.11.5.	メーカー別の人気コンピュータ	76
10.11.6.	コンピュータ (OS 別)	76
10.11.7.	モバイルデバイス (OS 別)	77
10.11.8.	パスワードポリシー：最小の長さ	77
10.11.9.	ドライブの暗号化状況別のコンピュータ	78
10.11.10.	デフォルトブラウザ別のコンピュータ	78
11.	ライセンス	79
12.	プロファイル	80
12.1.	プロファイルとは?	80
12.2.	[プロファイル] の基本操作	81
12.2.1.	タブメニュー	81
12.2.2.	アクションメニュー	81
12.2.3.	設定アイコンの意味と操作	83
12.3.	基本のプロファイル	84
12.4.	設定値のロックとは?	85
12.5.	プロファイルの作成	86
12.5.1.	アクションメニュー	87
12.6.	コンピュータプロファイル (Windows)	88
12.6.1.	一般設定	88
12.6.2.	ウイルスのリアルタイム スキャン	91
12.6.3.	マニュアルスキャン	95
12.6.4.	ブラウザ保護	98
12.6.5.	ファイアウォール	101
12.6.6.	ソフトウェアアップデート	104
12.6.7.	デバイス制御	107
12.6.8.	自動化されたタスク	109
12.6.9.	ネットワーク場所の設定	110
12.6.10.	データガード (Premium)	111

12.6.11.	アプリケーション制御 (Premium)	113
12.7.	コンピュータプロファイル (Windows Servers)	114
12.7.1.	一般設定.....	114
12.7.2.	ウイルスのリアルタイム スキャン.....	117
12.7.3.	マニュアルスキャン.....	121
12.7.4.	ブラウザ保護.....	124
12.7.5.	ファイアウォール	127
12.7.6.	ソフトウェアアップデート	130
12.7.7.	デバイス制御.....	133
12.7.8.	自動化されたタスク.....	135
12.7.9.	ネットワーク場所の設定.....	136
12.7.10.	データガード (Premium)	137
12.7.11.	アプリケーション制御 (Premium)	139
12.8.	コンピュータプロファイル (Mac)	140
12.8.1.	一般設定.....	140
12.8.2.	ウイルスのリアルタイム スキャン.....	141
12.8.3.	マニュアルスキャン.....	142
12.8.4.	ブラウザ保護.....	143
12.8.5.	ファイアウォール	145
12.9.	Linux プロファイル	147
12.9.1.	一般設定.....	148
12.9.2.	ウイルスのリアルタイム スキャン.....	148
12.9.3.	マニュアル スキャン.....	151
12.9.4.	完全性検査.....	152
12.10.	モバイルデバイス プロファイル.....	153
12.10.1.	ネットワーク保護	153
12.10.2.	マルウェア保護.....	154
12.11.	Connector プロファイル.....	155
12.11.1.	一般設定.....	155
12.11.2.	イベント転送.....	156
13.	ダウンロード	157
14.	サポート.....	159
15.	アカウント.....	160
15.1.	企業アカウントとユーザアカウントの概念.....	160
15.2.	アカウント管理 [管理者] タブメニュー.....	161
15.2.1.	管理者を作成.....	161
15.2.2.	管理者を編集する	163

15.2.3.	管理者を削除.....	165
16.	セキュリティイベントの PILOT	166
16.1.	[セキュリティイベント] の操作メニュー概要	166
16.2.	アクションメニュー	167
17.	Appendix	168
17.1.	Elements EPP が利用する URL	168

1. はじめに

本書は WithSecure™ Elements EPP for Computers (以下、「Elements EPP」) の契約ユーザ、または評価ユーザとしてお使いくださるお客様を対象とした、WithSecure™ Elements Security Center (以降「Elements Security Center」と呼称します) のガイドです。

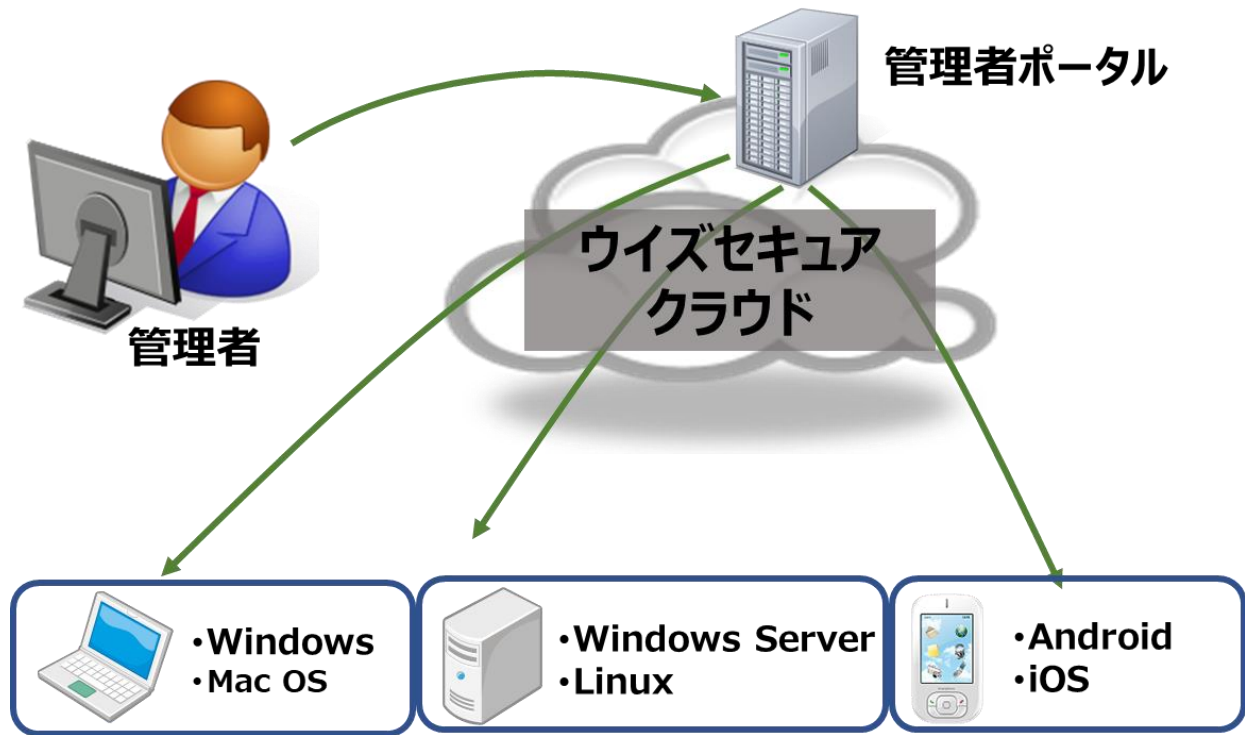
まず、「[2. Elements Security Center 概要](#)」において、Elements Security Center の概要と、独自の概念と技術について説明します。

この章の内容は、「3.」以降の内容をご理解いただくための準備に位置づけられています。

※本書は 2022 年 9 月現在の情報を基に記述されており、今後、予告なく内容が変更される可能性があります。

2. Elements Security Center 概要

ここでは、下図の Elements Security Center の構成概念図に従って、Elements Security Center の概要について説明します。



2.1. 対応ブラウザ

Elements Security Center は、以下のブラウザに対応しています。

- Edge の最新のバージョン
- Chrome の最新のバージョン
- Firefox の最新のバージョン
- Safari の最新のバージョン

2.2. Elements EPP の構成要素

Elements EPP は、各コンピュータにインストールされる Elements EPP クライアントと、それらを集中管理するための Elements Security Center によって構成されています。

- Elements EPP クライアント

Elements EPP のクライアントには3つの種類があります。

- ワークステーション用クライアント

クライアント OS 向けのソフトウェアです。Windows 用と Mac 用があります。

- サーバ用クライアント

サーバ OS 向けのソフトウェアです。Windows Server 用、Linux 用、の2つがあります。

- ・モバイル用クライアント

モバイル OS 向けのソフトウェアです。Android 用と iOS 用があります。

- ・Elements Security Center

クラウド上にあるポータルサイトです。WEB ブラウザを使ってアクセスします。

Elements Security Center から Elements EPP クライアントを集中管理することができます。

※Elements EPP クライアントのインストールプログラムは、Elements Security Center からダウンロードしてください。

CD-R/DVD-R 等の媒体での提供方法はございません。

2.3. Elements Security Center のアカウントの概念

Elements Security Center には以下 2 種類のアカウントがあります。

- ・企業アカウント

お客様の所属する企業(または組織)を表すアカウントです。

Elements EPP をご契約いただいたお客様は、通常 1 つの会社アカウントを保持します。

会社アカウントの中に、Elements EPP クライアントをインストールした自社のコンピュータが登録されます。

- ・ユーザアカウント

Elements Security Center へログインするためのユーザアカウントです。

企業アカウント作成時に、その企業の管理者としてユーザアカウントを作成します。

企業アカウント及び所属する Elements EPP クライアントを管理するには、ユーザアカウントを使用して Elements Security Center へログインし、各種の集中管理機能を使用します。

ユーザアカウントは、追加作成・削除が可能です。

ユーザアカウントには以下 2 つの権限があります。

- ①管理者

すべての Elements Security Center 機能を使用できます。

- ②読み取り専用

情報の読み取りだけで変更はできません。

※ユーザアカウントは、自動作成されません。お客様ご自身でユーザアカウントを作成していただきます。

2.4. ライセンスキーの概念

Elements EPP で扱われるライセンスキーは、英数字 20 桁からなるコードです。

エンドユーザはこのライセンスキーを使用し、企業アカウントの作成、Elements EPP クライアントのインストールを行うことができます。

ライセンスキーには以下の仕様と特徴があります。

- ・ライセンスキーは、Elements EPP クライアントのインストール時に必要で、ライセンスキーが無い場合、Elements EPP クライアントを使用することはできません。

- ・1つのライセンスキーを複数の端末で利用できますが、利用可能な台数が決められています。

- ・企業アカウントの作成時にライセンスキーコードが必要です。

- ・ライセンスキーには有効期限日があります。

有効期限日を過ぎるとそのライセンスキーを使用している Elements EPP クライアントは使用できなくなります。

- ・ライセンスキーは弊社全製品を通して一意であり固有(ユニーク)です。

- ・20 桁の英数字から成り、4 桁ずつハイフンを挟んで表記されます（但し、モバイル端末用のキーは、この限りではありません）。

例：1234-ABCD-5678-EFGH-90JK

※ライセンスキーのご購入、評価用ライセンスキーの入手については、ウィズセキュア営業本部までお問い合わせください。

2.5. 使用開始までの流れ

Elements EPP を利用するための準備として、以下の手順が必要になります。

- ・Elements Security Center へアクセスする為のユーザアカウントを作成します

- ・Elements Security Center からインストールプログラムを配布し、Elements EPP クライアントをインストールします。

- ・インストールが完了すると、各コンピュータが Elements Security Center へ自動登録され、集中管理ができるようになります。

※ライセンスキーのご購入、評価用ライセンスキーの入手については、WithSecure 営業本部までお問い合わせください。

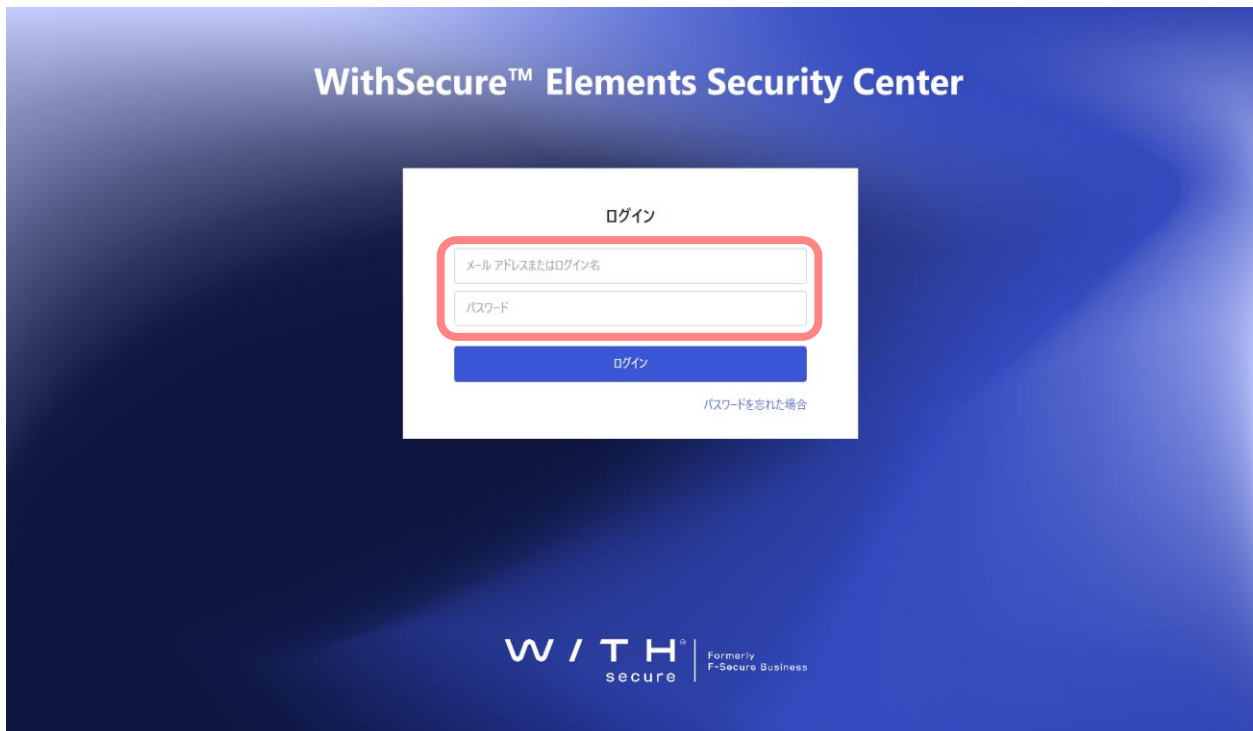
次の章からは、上記の手順の具体的な解説を行います。

3. Elements Security Center への接続とログイン

Elements Security Center サイトへの接続は、WEB ブラウザにて以下の URL を入力します。

<https://elements.f-secure.com/>

すると、以下の様な画面が開きますので、ここから「ユーザ名」と「パスワード」を入力し、Login ボタンをクリックします。



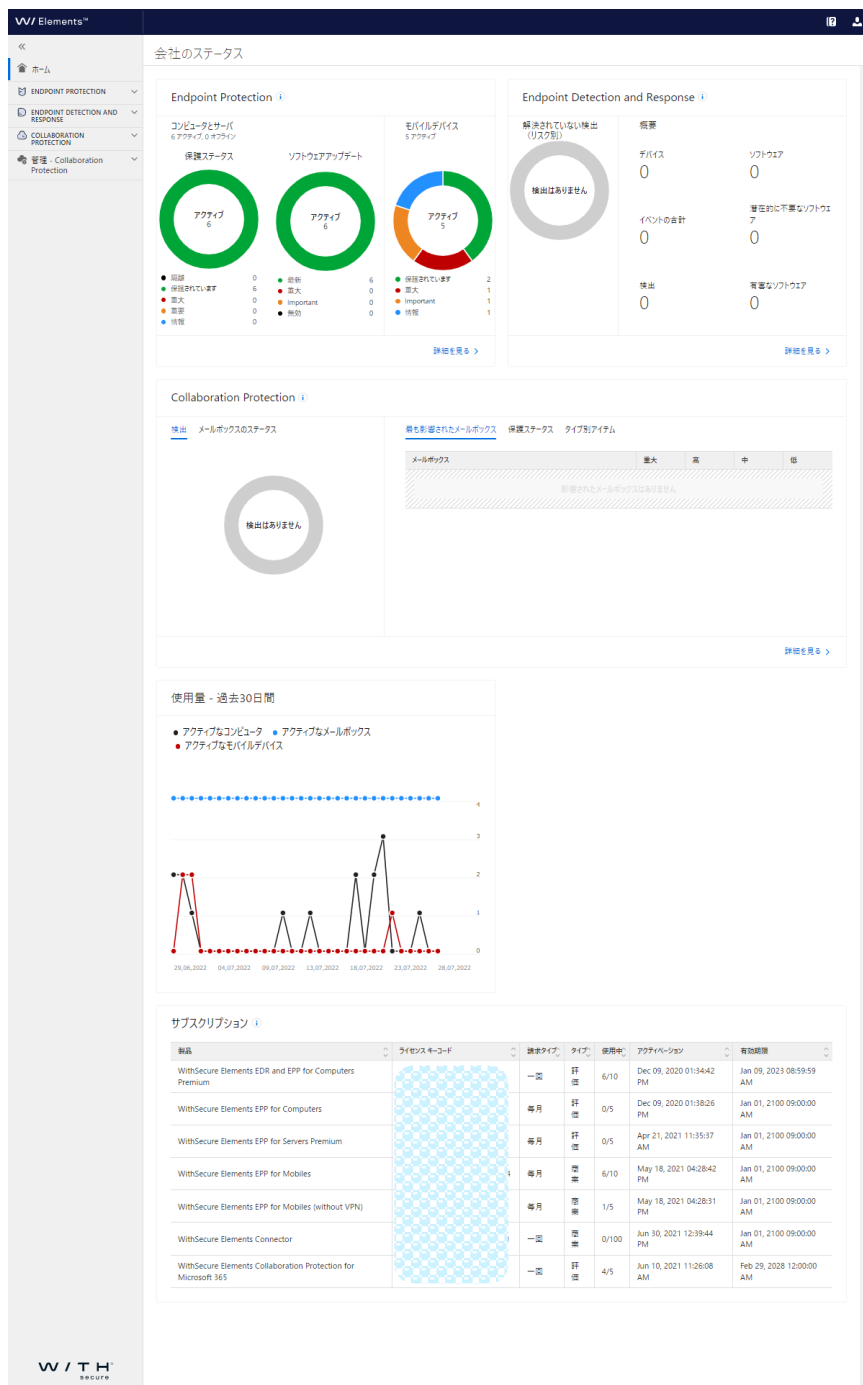
4. Elements Security Center の操作メニュー

ここでは、Elements Security Centerにある操作用のメニューについて説明します。

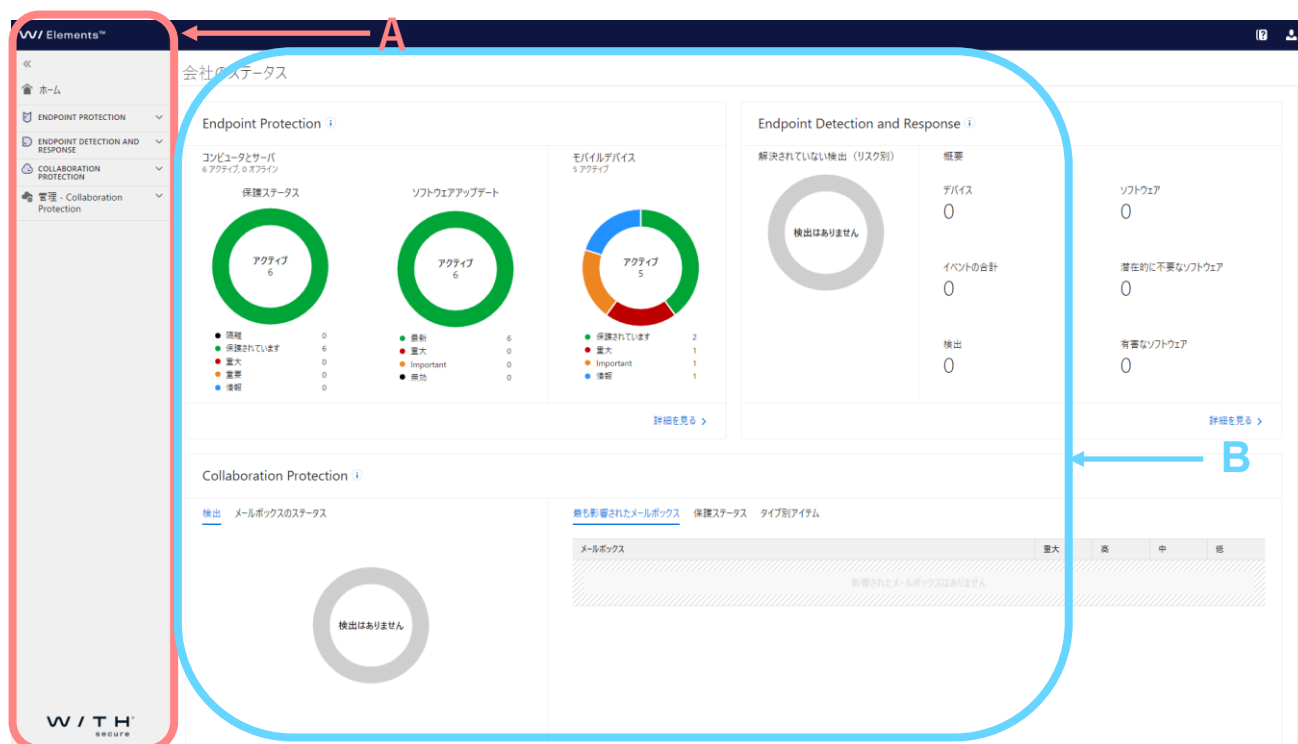
4.1. Elements Security Center の操作メニュー概要

Elements Security Center へログインをすると、以下の画面が表示されます。

①画面全体図



②画面上部



A. サイドメニュー

Elements Security Center から操作可能なアプリケーション毎にボタンが分けられています。

* 所用している、ライセンスにより表示させる製品は異なります。

B. ダッシュボードメニュー

各アプリケーションの情報を表示しています。

③画面下部



C. 使用量メニュー

Elements Security Center に接続した端末数を確認できます。

* 所用している、ライセンスにより表示させる製品は異なります。

D. サブスクリプションメニュー

所用している、ライセンス情報とインストールされている端末台数を確認できます。

5. Elements EPP の操作メニュー

ここでは、Elements Security Centerにある Elements EPP の操作のメニューについて説明します。

5.1. Elements EPP の操作メニュー概要

Elements EPP のメニューを選択すると、以下の画面が表示されます。

The screenshot shows the Elements EPP dashboard. On the left is a sidebar menu (A) with options: ホーム, ENDPOINT PROTECTION, ダッシュボード, デバイス, ソフトウェアのアップデート, レポート, ライセンス, プロファイル, ダウンロード, サポート, アカウント, セキュリティイベントのPILOT, and ENDPOINT DETECTION AND RESPONSE. At the top right is a user account menu (B) with options: 新着情報 and 新規デバイスを追加. The main content area displays protection status cards for Workstations (50% protected), Servers (0 servers), Software Updates (0 computers), and Mobile (0 mobile devices). Below these is a '問題' (Issues) table.

アイテムタイプ	深刻度	影響されているデバイス
リアルタイムスキャンが無効です プロファイルでリアルタイムスキャンが有効になっていることを確認します。有効になっていない場合は、設定を有効にします。ユーザが無効にできないように、設定をロックしてください。1台のデバイスを確認する	重大	1
リアルタイムスキャンの異常 クライアントのバージョンを確認する。デバイスのシステムドライブに十分な空き容量 (5GB以上) があることを確認してください。デバイスを強制します。1台のデバイスを確認する	重大	1
グループポリシーによってファイアウォールが無効 グループポリシーが本当にファイアウォールを無効するためのものであることを確認してください。その場合、何もする必要はありません。2台のデバイスを確認する	重要	2

A. サイドメニュー

Elements EPP から操作可能な主要な機能がボタン毎に分けられています。

Elements EPP クライアントを集中管理するためのメニューです。

B. ユーザーアカウントメニュー

ユーザの[アカウント管理]と[ログアウト]をするためのメニューです。

注意：以前、ご利用されていた古いダッシュボードとデバイスビューは2022年10月4日までにサポート終了します。

5.2. サイドメニュー [ダッシュボード]

Elements Security Center にログイン直後は [ダッシュボード] 画面が表示されます。[ダッシュボード] 画面では、自社内のコンピュータの保護ステータスと、修正する必要があるセキュリティ上の問題が表示されます。その他に、ログインユーザの管理や設定を行えます。

The screenshot shows the Elements Security Center dashboard. The left sidebar contains navigation options: Home, Endpoint Protection, Dashboard (highlighted with a red box), Devices, Software Updates, Reports, Licenses, Profiles, Downloads, Support, Account, and Security Events. The main content area is titled 'ダッシュボード' and features four status cards: 'ワークステーションの保護ステータス' (50% protected), 'サーバの保護ステータス' (0 servers), 'ソフトウェアアップデートのステータス' (0 computers), and 'モバイルの保護ステータス' (0 mobile devices). A '新規デバイスを追加' button is in the top right. Below the cards is a '問題' (Issues) table.

アイテムタイプ	深刻度	影響されているデバイス
リアルタイムスキャンが無効です プロファイルでリアルタイムスキャンが有効になっていることを確認します。有効になっていない場合は、設定を有効にします。ユーザが無効にできないように、設定をロックしてください。1台のデバイスを確認する	重大	1
リアルタイムスキャンの異常 クライアントのバージョンを確認する。デバイスのシステムドライブに十分な空き容量 (5GB以上) があることを確認してください。デバイスを再起動します。1台のデバイスを確認する	重大	1
グループポリシーによってファイアウォールが無効 グループポリシーが本当にファイアウォールを無効するためのものであることを確認してください。その場合、何もする必要はありません。2台のデバイスを確認する	重要	2

A.保護ステータスの表示エリア

青色アイコンは、問題がないことを示しています。橙色または赤色は、処置が必要な問題が生じていることを示しています。

B.[新規デバイスの追加] ボタン

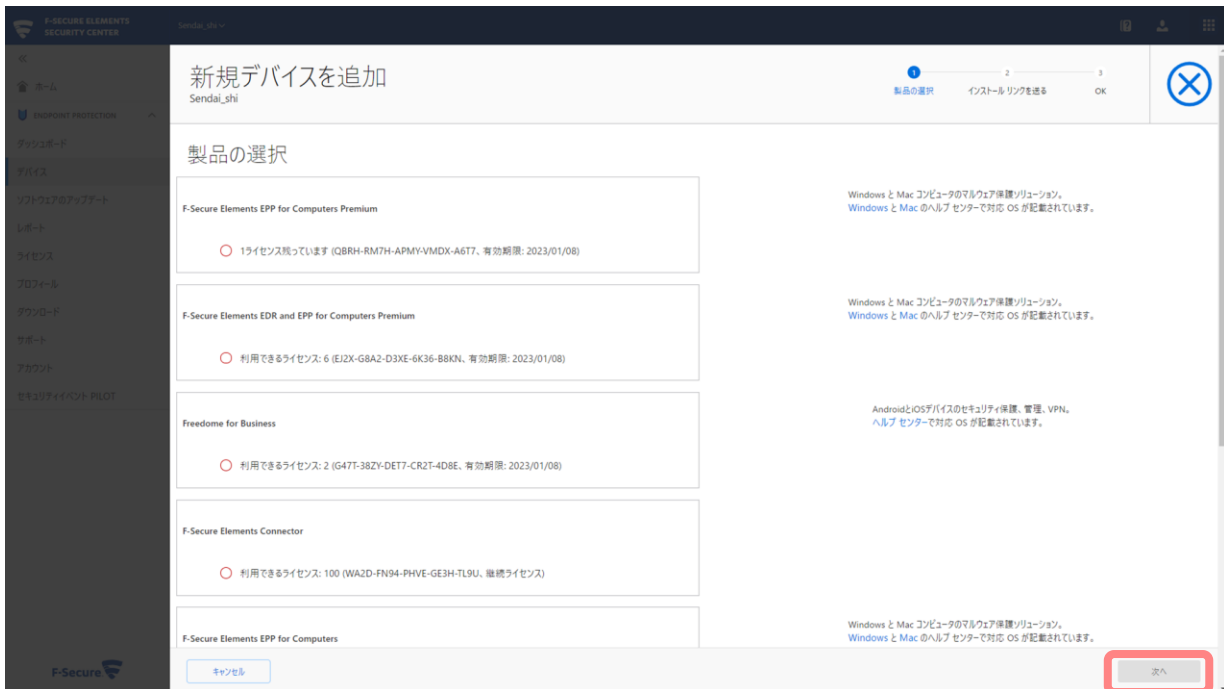
クリックするとデバイスを追加する[製品の選択]画面に移動します。

注意: 以前、ご利用されていた古いダッシュボードとデバイスビューは 2022 年 10 月 4 日までにサポート終了します。

5.3. 新規デバイスを追加

管理するコンピュータを追加する処理です。対象のコンピュータを保持しているユーザのメールアドレスに、ライセンスキーとインストールモジュールがダウンロードできる URL を送信することで、メールを受信したユーザが自身でコンピュータにモジュールをインストールできるようにします。

- ・[製品の選択]画面にて、追加するコンピュータに適用する製品とライセンスキーを選択し[次へ]をクリック



クします。

- ・[インストールリンクを送る] 画面にて、追加したいコンピュータのユーザのメールアドレスを入力します。

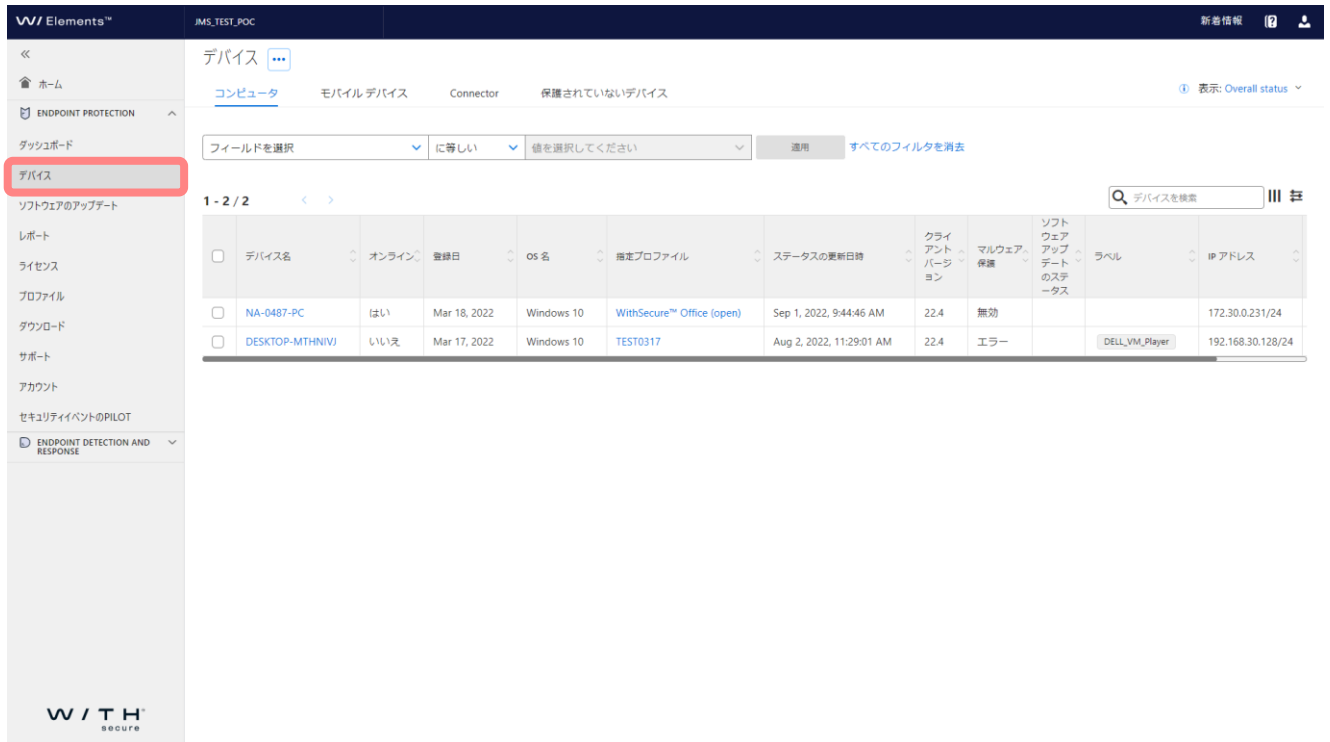


- 複数のメールアドレスに送る際は複数のメールアドレスをカンマ、セミコロン、新しい行で区切りことができます。これにより、複数のメールアドレスへ一度に送信できます。
- 送信先を CSV ファイルからインポートすることも可能です。
- [送信]ボタンを押すことで、対象のメールアドレスにメールが送信されます。

6. デバイス

6.1. [デバイス] の操作メニュー概要

[デバイス] ボタンをクリックすると、以下の画面が表示されます。



注意：以前、ご利用されていた古いダッシュボードとデバイスビューは2022年10月4日までにサポート終了します。

デバイス ⋮

コンピュータ

モバイルデバイス

Connector

保護されていないデバイス

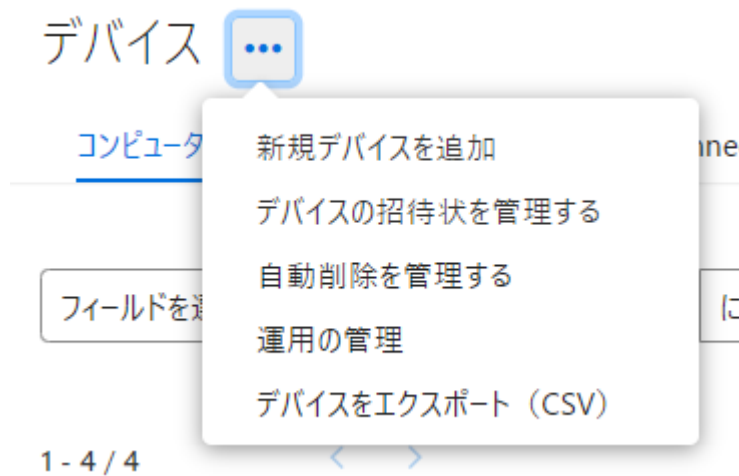
コンピュータ/モバイルデバイス/レガシーモバイルデバイス/Connector/保護されていないデバイスのタブを選択して、各デバイスの情報を表示します。

タブメニューではそのアカウント内の全てのコンピュータとモバイル等一覧で表示されます。

項目名	内容
コンピュータ	そのアカウント内の全てのコンピュータが一覧で表示
モバイルデバイス	そのアカウント内の全てのモバイルが一覧で表示
Connector	コネクタを使用した全てのコンピュータが一覧で表示
保護されていないデバイス	Active Directoryを使用した際の、クライアントの未インストール端末を一覧で表示

6.2. “コンピュータ” タブ アクションメニュー

デバイス数の右側にある[アクションメニュー]をクリックすると、デバイスの追加やエクスポートに関するメニューが表示されます。



アクションメニュー

項目名	内容
新規デバイスを追加	[新規デバイスを追加]の画面に移動します。 5.3. 新規デバイスを追加 参照
デバイスの招待状を管理する	[デバイスの招待を管理する]の画面に移動します
自動削除を管理する	[自動削除を管理する]の画面に移動します。
運用の管理	[運用の管理]の画面に移動します。
デバイスをエクスポート (CSV)	コンピュータのレポートが CSV 形式でダウンロードされます。

6.2.1. デバイスの招待状を管理する

新規デバイスを追加した際の招待メールのステータスを管理します

WithSecure Elements

Sendai_shi

デバイスの招待状を管理する

Sendai_shi

保留中 (1) 期限切れ

これらのデバイスには、保護アプリケーションがまだインストールされていません。インストールリンクがまだ有効である間、30日以内にリマインダーを送信できます。その後、招待状は期限切れの招待状に移動され、[新しいデバイスの追加] から再度招待する必要があります

<input type="checkbox"/>	メールアドレス	サブスクリプション名	名	姓	エイリアス	メールを送信しました	有効期限
<input type="checkbox"/>	nagasaki@hotmail.com	WithSecure Elements EDR and EPP for Computers Premium	カズシ	ナガサワ		2022/09/01 14:29	2022/10/01 14:29

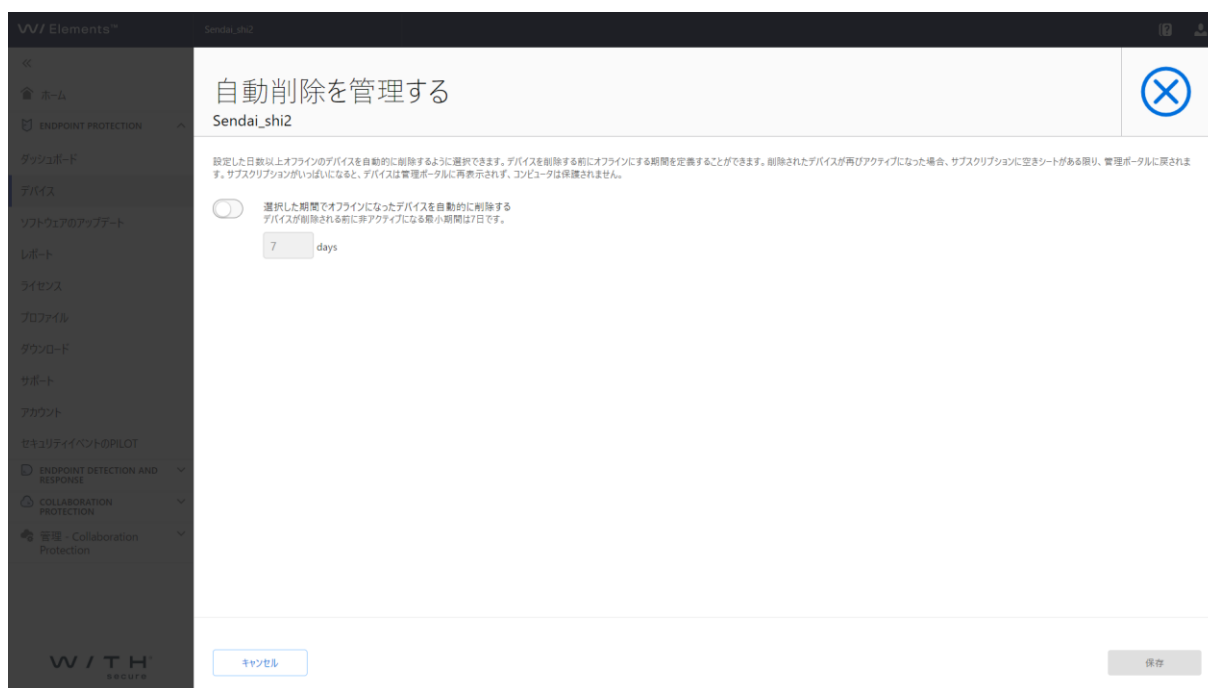
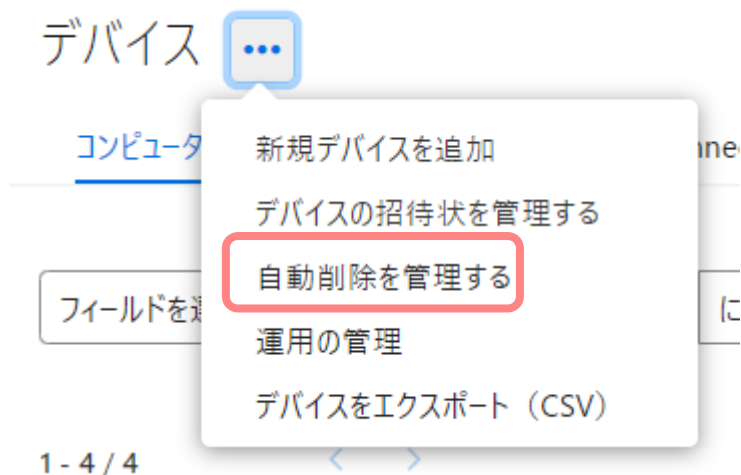
閉じる

保留事項を削除する

リマインダーを送信

6.2.2. 自動削除を管理する

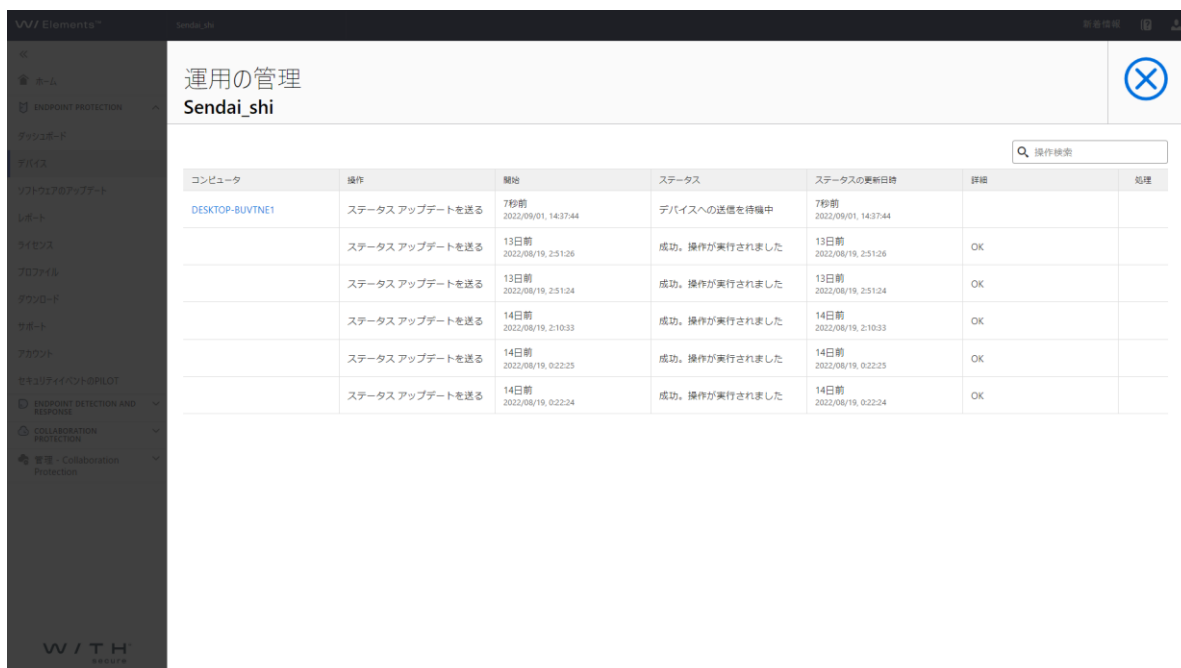
オフラインになってから時間が経過したデバイスを自動的に削除することができます。また、デバイスが削除されるまでのオフラインの期間を定義することもできます。



選択した期間でオフラインになったデバイスを自動的に削除することができます。

6.2.3. 運用の管理

端末への操作の履歴を確認できます

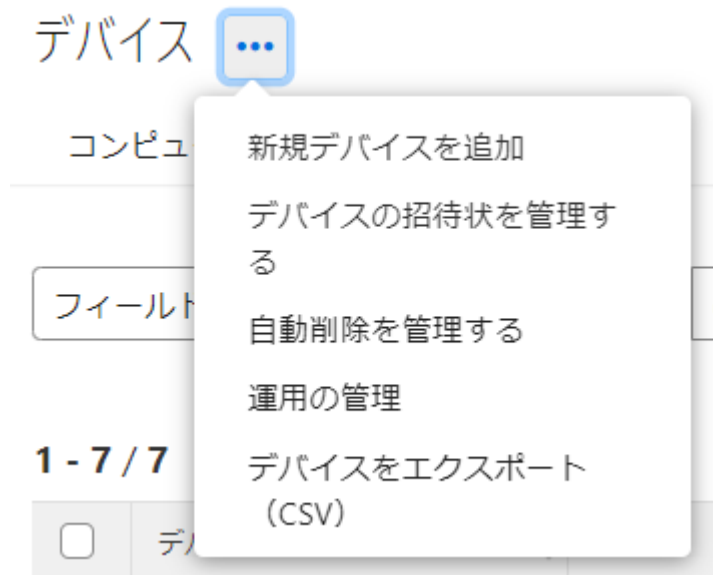


The screenshot shows the '運用の管理' (Operational Management) page for 'Sendai_shi'. The page features a search bar for '操作検索' (Operation Search) and a table with the following columns: コンピュータ (Computer), 操作 (Operation), 開始 (Start), ステータス (Status), ステータスの更新日時 (Status Update Time), 詳細 (Details), and 処理 (Action). The table lists several status update operations for the computer 'DESKTOP-BUVTNE1'.

コンピュータ	操作	開始	ステータス	ステータスの更新日時	詳細	処理
DESKTOP-BUVTNE1	ステータス アップデートを送る	7秒前 2022/09/01, 14:37:44	デバイスへの送信を待機中	7秒前 2022/09/01, 14:37:44		
	ステータス アップデートを送る	13日前 2022/08/19, 2:51:26	成功。操作が実行されました	13日前 2022/08/19, 2:51:26	OK	
	ステータス アップデートを送る	13日前 2022/08/19, 2:51:24	成功。操作が実行されました	13日前 2022/08/19, 2:51:24	OK	
	ステータス アップデートを送る	14日前 2022/08/19, 2:10:33	成功。操作が実行されました	14日前 2022/08/19, 2:10:33	OK	
	ステータス アップデートを送る	14日前 2022/08/19, 0:22:25	成功。操作が実行されました	14日前 2022/08/19, 0:22:25	OK	
	ステータス アップデートを送る	14日前 2022/08/19, 0:22:24	成功。操作が実行されました	14日前 2022/08/19, 0:22:24	OK	

6.3. “モバイルデバイス” タブ アクションメニュー

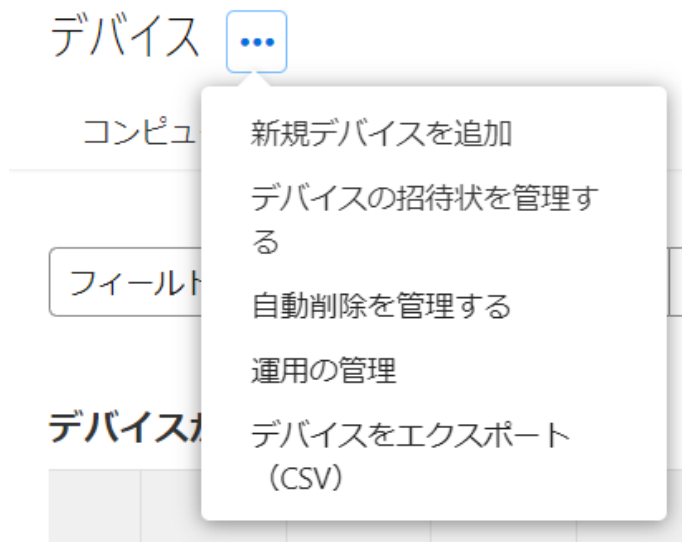
デバイスの右側にある[アクションメニュー]をクリックすると、デバイスの追加やインポート、エクスポートに関するメニューが表示されます。



項目名	内容
新規デバイスを追加	[新規デバイスを追加]の画面に移動します。 5.3. 新規デバイスを追加 参照
デバイスの招待状を管理する	[デバイスの招待状を管理する]の画面に移動します。 6.2.1. デバイスの招待状を管理する 参照
自動削除を管理する	[自動削除を管理する]の画面に移動します。 6.2.2. 自動削除を管理する 参照
運用の管理	端末への操作の履歴を確認できます 6.2.3. 運用の管理 参照
デバイスをエクスポート(CSV)	モバイルデバイスのレポートが CSV 形式でダウンロードされます。

6.4. “Connector” タブ アクションメニュー

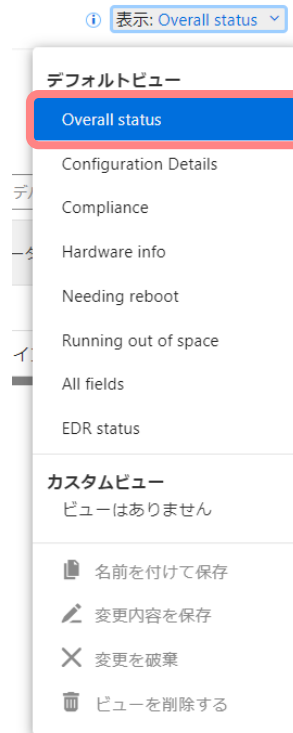
デバイスの右側にある[アクションメニュー]をクリックすると、デバイスの追加やインポート、エクスポートに関するメニューが表示されます。



項目名	内容
新規デバイスを追加	[新規デバイスを追加]の画面に移動します。 5.3. 新規デバイスを追加 参照
デバイスの招待を管理する	[デバイスの招待状を管理する]の画面に移動します。 6.2.1. デバイスの招待状を管理する 参照
自動削除を管理する	[自動削除を管理する]の画面に移動します。 6.2.2. 自動削除を管理する 参照
運用の管理	端末への操作の履歴を確認できます 6.2.3. 運用の管理 参照
デバイスをエクスポート(CSV)	Connector のレポートが CSV 形式でダウンロードされます。

6.5. コンピュータ[表示]の切り替え

[表示]では、製品種別によりステータスの内容を切り替えることができます。必要に応じて切り替えてください。



任意の項目を選択して「カスタムビュー」を作成する事も可能です

デバイス名	オンライン	登録日	OS名	指定プロファイル	ステータスの更新日時	クラウドエージェントバージョン	マルウェア保護	ソフトウェアアップデートのステータス	ラベル	IPアドレス
NA-0487-PC	はい	Mar 18, 2022	Windows 10	WithSecure™ Office (open)	Sep 1, 2022, 9:44:46 AM	22.4	無効			172.30.0.231/24
DESKTOP-MTHNIV	いいえ	Mar 17, 2022	Windows 10	TEST0317	Aug 2, 2022, 11:29:01 AM	22.4	エラー		DELL_VM_Player	192.168.30.128/24

表示メニュー

[Overall status]

全体の状態に関する項目の情報を表示します

[Configuration Details]

構成の詳細に関する項目の情報を表示します

[Compliance]

コンプライアンスに関する項目の情報を表示します

[Hardware info]

ハードウェア情報に関する項目を表示します

[Needing reboot]

再起動の必要がある端末に関する項目の情報を表示します

[Running out of space]

システムドライブの空き容量 が 5.0 GB より少ない端末に関する項目の情報を表示します

[All fields]

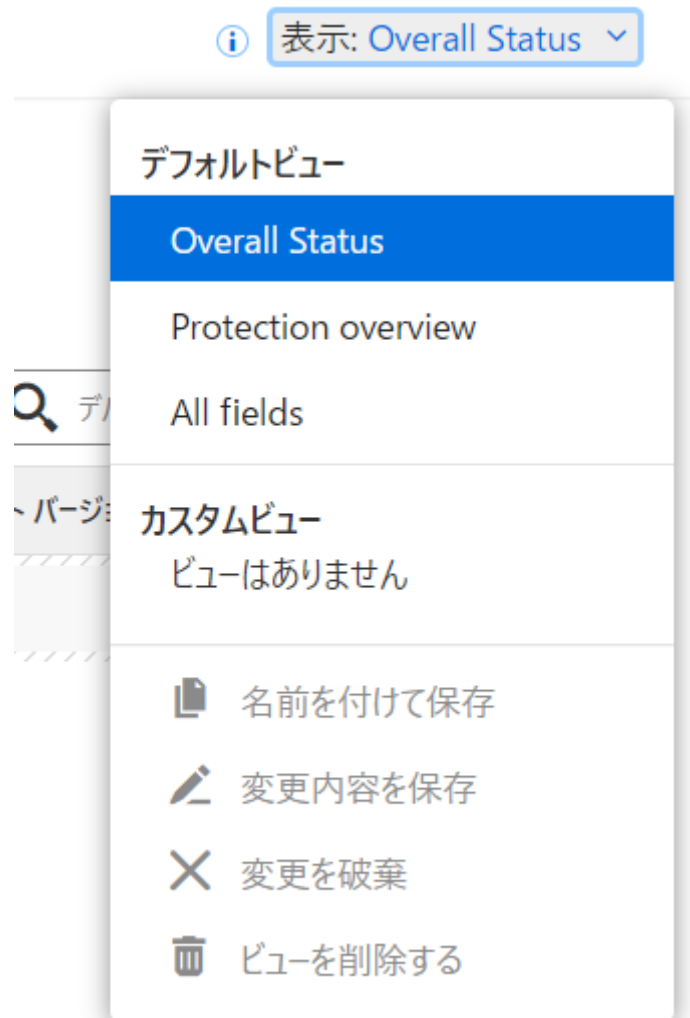
すべての項目を表示します

[EDR status]

EDR のサブスクリプションを所有している端末に関する項目の情報を表示します

6.6. モバイルデバイス[表示]の切り替え

[表示]では、製品種別によりステータスの内容を切り替えることができます。必要に応じて切り替えてください。



任意の項目を選択して「カスタムビュー」を作成する事も可能です。

表示メニュー

[Overall status]

全体の状態に関する項目の情報を表示します。

[Protection overview]

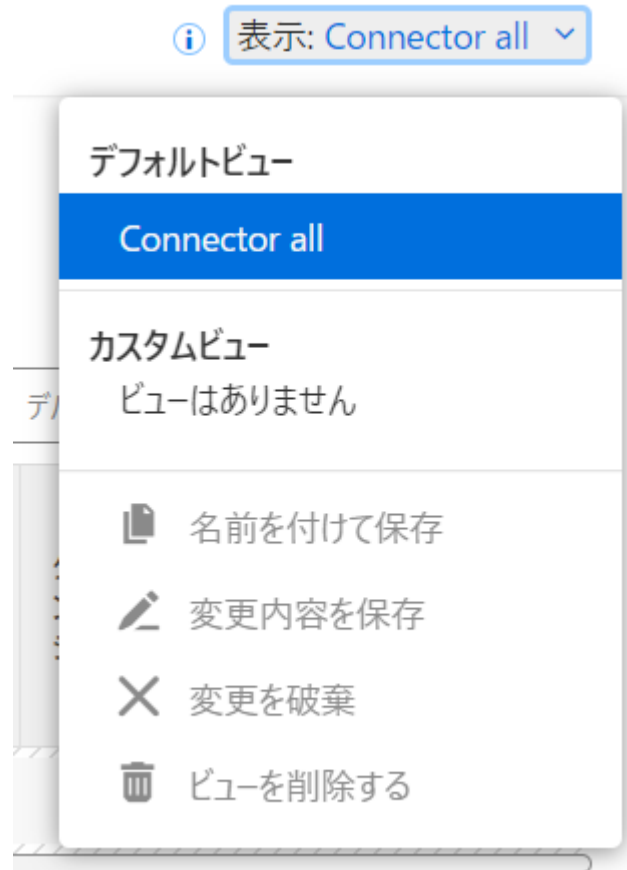
保護した概要に関する項目の情報を表示します。

[All fields]

すべての項目を表示します。

6.7. Connector [表示]の切り替え

[表示]では、製品種別によりステータスの内容を切り替えることができます。必要に応じて切り替えてください。



任意の項目を選択して「カスタムビュー」を作成する事も可能です。

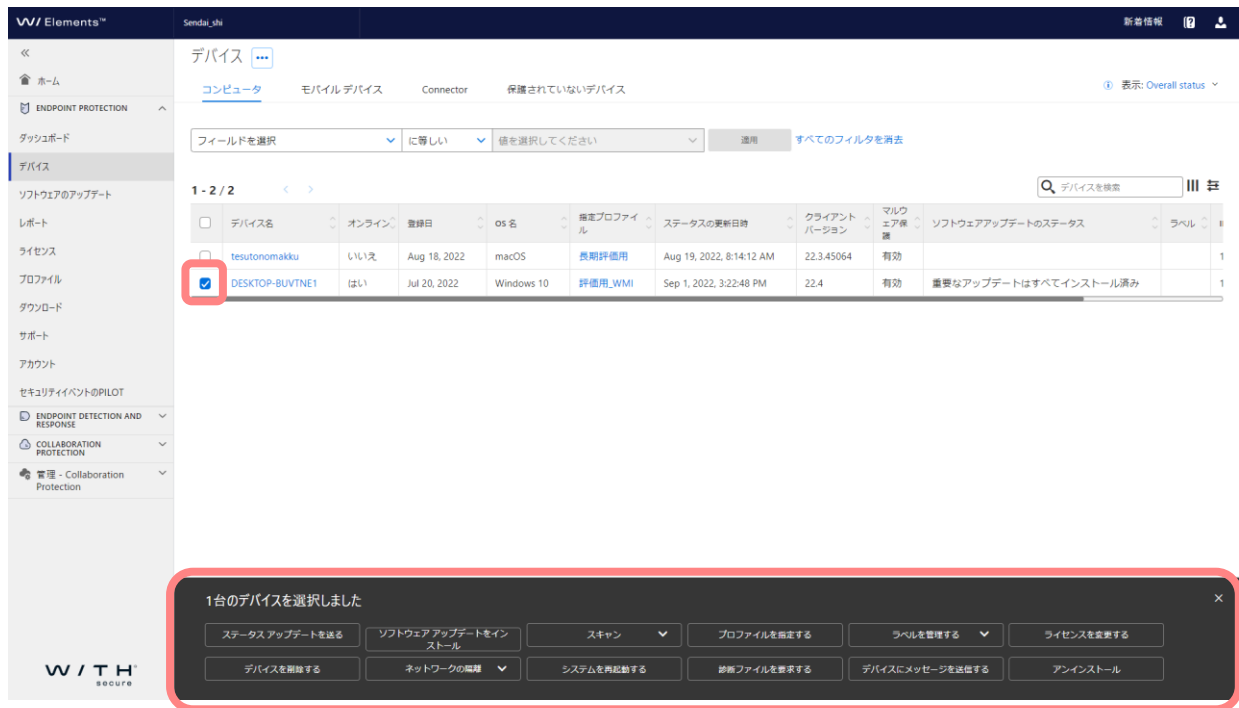
表示メニュー

[Connector all]すべての項目を表示します。

7. コンピュータへの操作

7.1. 処理項目

選択したコンピュータに対して、Elements Security Center 側から処理させたい項目を選択して実行させることができます。



- ① デバイス名欄のチェックを入れ処理を実行させる対象のコンピュータを選択します。
- ② 画面下部に「処理ボタン」が表示されます。
- ③ 「処理ボタン」を押すと選択対象のコンピュータに対して、処理が実行されます。設定や確認を行った後に処理を実行する項目も存在します。

処理ボタン

項目名	内容
ステータスアップデートを送る	ステータスの更新情報をアップデートするコマンドを送信します。
ソフトウェアアップデートをインストール	ソフトウェアのアップデートを行うコマンドを送信します。
スキャン	マルウェアのスキャンまたはソフトウェアの状態が最新であるかどうかをスキャンさせるコマンドを送信します。
プロファイルを指定する	デバイスにプロファイルを指定します。
ラベルを管理する	デバイスにラベルの追加/交換/削除ができます
ライセンスを変更する	デバイスに適用されているキーコードを変更します。
デバイスを削除する	デバイスを完全に削除します
ネットワークの隔離	デバイスをネットワークから隔離または隔離から解放します。
システムを再起動する	MAC 端末では表示されません
診断ファイルを要求する	デバイスに診断ファイルの取得を行うコマンドを送信します
デバイスにメッセージを送信する	デバイスにメッセージを送信します。ログインしているすべてのユーザにメッセージが表示されます。 MAC 端末では表示されません
アンインストール	MAC 端末では表示されません

7.2. 処理内容

7.2.1. ステータスアップデートを送る

任意のコンピュータに対してステータスアップデートの指示を送信します。

The screenshot shows the W/ Elements management interface. On the left is a navigation menu with options like 'デバイス', 'レポート', 'ライセンス', etc. The main area displays a table of devices. The second row, 'DESKTOP-BUVTNE1', has its checkbox selected. Below the table, a modal dialog titled '1台のデバイスを選択しました' is shown, with the 'ステータスアップデートを送る' button highlighted.

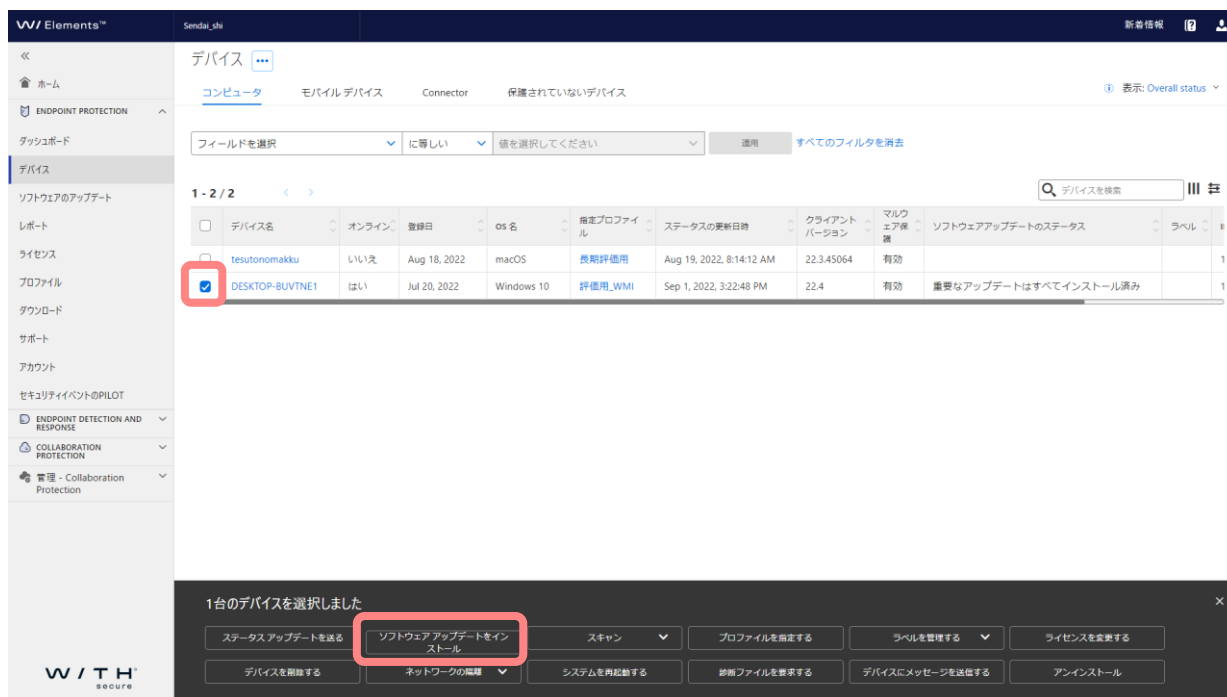
デバイス名	オンライン	登録日	OS名	指定プロファイル	ステータスの更新日時	クライアントバージョン	マルウェア保護	ソフトウェアアップデートのステータス	ラベル
tesutonomakku	いいえ	Aug 18, 2022	macOS	長期評価用	Aug 19, 2022, 8:14:12 AM	22.3.45064	有効		
DESKTOP-BUVTNE1	はい	Jul 20, 2022	Windows 10	評価用_WMI	Sep 1, 2022, 3:22:48 PM	22.4	有効	重要なアップデートはすべてインストール済み	

①対象となるコンピュータをチェックボックスで指定します。

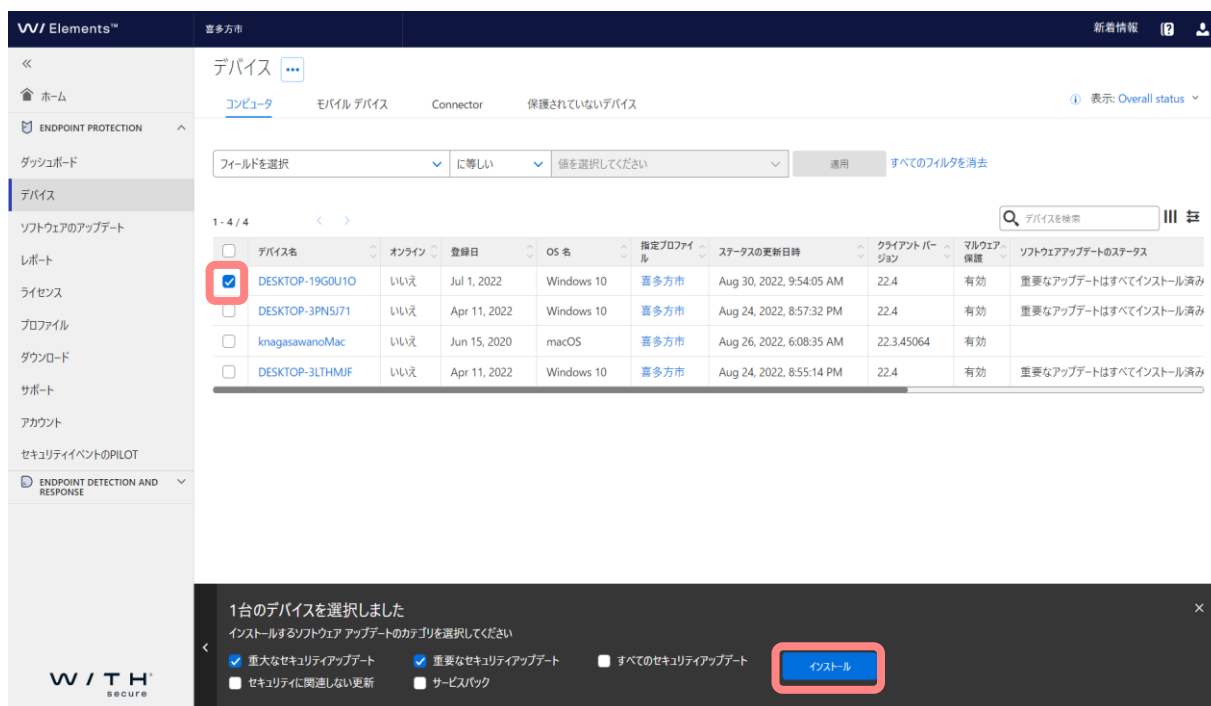
②[ステータス アップデートを送る] ボタンを押すことで、対象のコンピュータにステータスアップデートをさせます。

7.2.2. ソフトウェアアップデートをインストール

任意のコンピュータに対してソフトウェアアップデートのインストールを実行させることが出来ます。



- ①対象となるコンピュータをチェックボックスで指定します。
- ②[ソフトウェア アップデートをインストール] ボタンを押します。
- ③メニューが表示されるので、インストールするソフトウェアアップデートのカテゴリを選択します。
- ④[インストール]ボタンをクリックします。



7.2.3. スキャン

任意のコンピュータに対してマルウェアのスキャンまたは適用されていないソフトウェアのアップデートのスキャンを実行させることができます。

The screenshot shows the W/TH Elements interface. On the left, there is a navigation menu with options like 'ホーム', 'ENDPOINT PROTECTION', 'ダッシュボード', 'デバイス', 'ソフトウェアのアップデート', 'レポート', 'ライセンス', 'プロフィール', 'ダウンロード', 'サポート', 'アカウント', and 'セキュリティイベントのPILOT'. The main area is titled 'デバイス' and shows a table of devices. The first device, 'DESKTOP-19G0U1Q', has its checkbox selected. A modal dialog box is open at the bottom, with the 'スキャン' button highlighted.

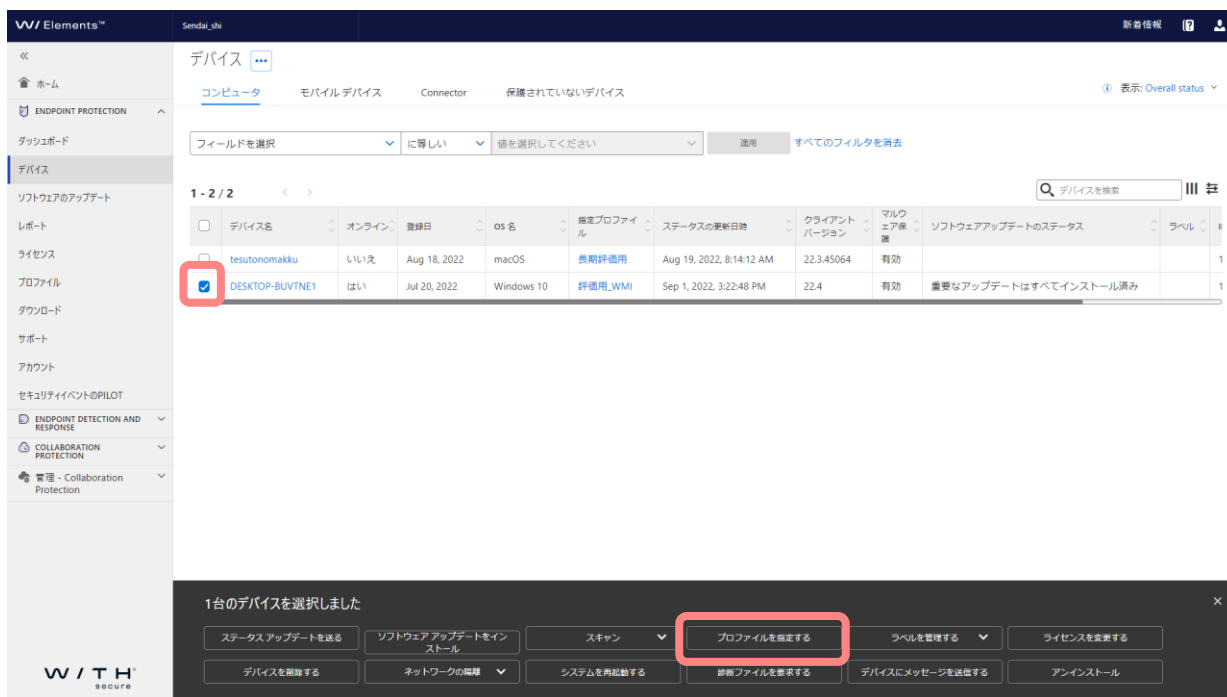
デバイス名	オンライン	登録日	os名	指定プロファイル	ステータスの更新日時	クライアントバージョン	マルウェア保護	ソフトウェアアップデートのステータス	ラベル
<input checked="" type="checkbox"/> DESKTOP-19G0U1Q	いいえ	Jul 1, 2022	Windows 10	豊多門市	Aug 30, 2022, 9:54:05 AM	22.4	有効	重要なアップデートはすべてインストール済み	
<input type="checkbox"/> DESKTOP-3PNSJ71	いいえ	Apr 11, 2022	Windows 10	豊多門市	Aug 24, 2022, 8:57:32 PM	22.4	有効	重要なアップデートはすべてインストール済み	
<input type="checkbox"/> knagasawanoMac	いいえ	Jun 15, 2020	macOS	豊多門市	Aug 26, 2022, 6:08:35 AM	22.3.45064	有効		MacBook_Parallels_MacOS10
<input type="checkbox"/> DESKTOP-3LTHMJF	いいえ	Apr 11, 2022	Windows 10	豊多門市	Aug 24, 2022, 8:55:14 PM	22.4	有効	重要なアップデートはすべてインストール済み	

①対象となるコンピュータをチェックボックスで指定します。

②[スキャン] ボタンを押すことで、対象のコンピュータにマルウェアのスキャンまたは適用されていないソフトウェアのアップデートのスキャンを実行します。

7.2.4. プロファイルを指定する

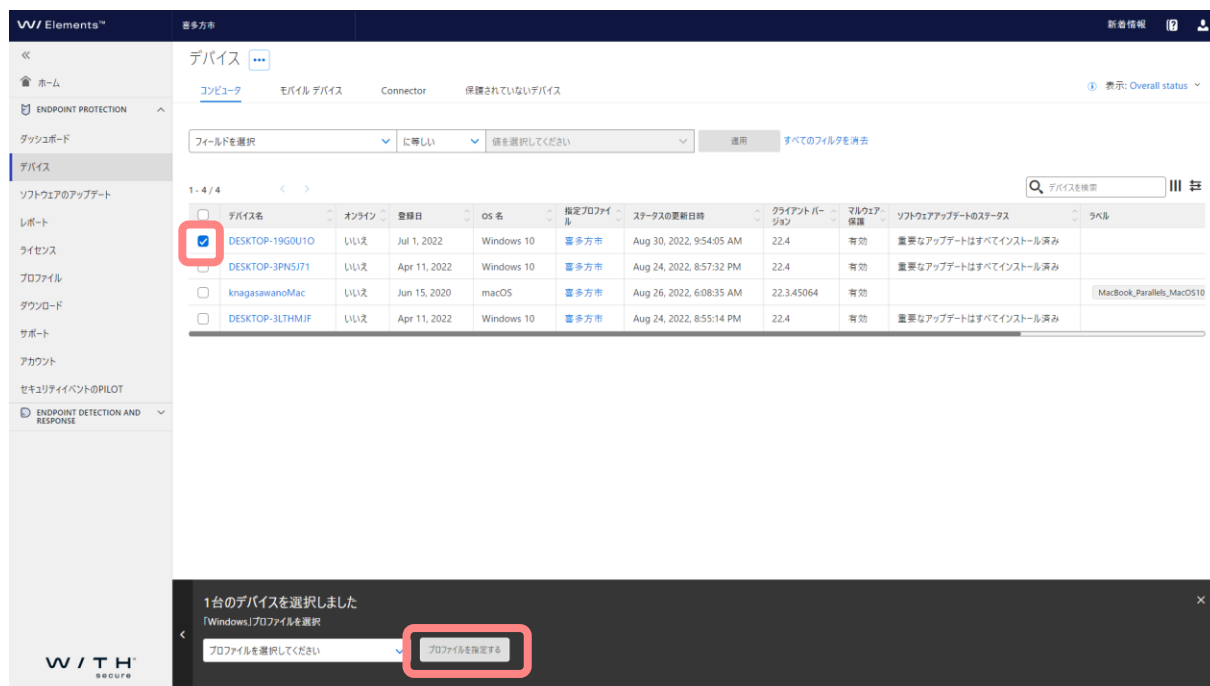
任意のコンピュータに対して、プロファイルを指定します。



①対象となるコンピュータをチェックボックスで指定します。

②[プロファイルを指定する]を選択します。

③以下の画面が表示されるので、適用するプロファイルをプルダウンメニューから選択します。



7.2.5. ラベルを管理する

任意のコンピュータに対して、プロファイルまたはラベルを指定します。

The screenshot shows the WTH Elements management console interface. The main area displays a table of devices under the 'デバイス' (Devices) section. The first device, 'DESKTOP-19G0U10', is selected with a red checkmark. A red box highlights the 'ラベルを管理する' (Manage Labels) button in the bottom right corner of the interface. A modal dialog box is open, showing options to 'ラベルを追加する' (Add Label), 'ラベルを交換する' (Exchange Label), and 'ラベルを削除する' (Delete Label). The dialog also includes a 'ラベルを管理する' (Manage Labels) button with a dropdown arrow.

デバイス名	オンライン	登録日	os名	指定プロファイル	ステータスの更新日時	クライアントバージョン	マルウェア保護	ソフトウェアアップデートのステータス	ラベル
DESKTOP-19G0U10	いいえ	Jul 1, 2022	Windows 10	喜多方市	Aug 30, 2022, 9:54:05 AM	22.4	有効	重要なアップデートはすべてインストール済み	
DESKTOP-3PNSJ71	いいえ	Apr 11, 2022	Windows 10	喜多方市	Aug 24, 2022, 8:57:32 PM	22.4	有効	重要なアップデートはすべてインストール済み	
knagasawanoMac	いいえ	Jun 15, 2020	macOS	喜多方市	Aug 26, 2022, 6:08:35 AM	22.3.45064	有効		MacBook_Parallels_MacOS10
DESKTOP-3LTHMJF	いいえ	Apr 11, 2022	Windows 10	喜多方市	Aug 24, 2022, 8:55:14 PM	22.4	有効	重要なアップデートはすべてインストール済み	

①対象となるコンピュータをチェックボックスで指定します。

②[ラベルを管理する] ボタンをクリックし、ラベルを追加/交換/削除を選択します。

7.2.6. ライセンスを変更する

デバイスを指定し、適用されているキーコードを変更できます。

The screenshot shows the W/ Elements console interface. The left sidebar contains navigation options like 'ホーム', 'ENDPOINT PROTECTION', 'デバイス', and 'ソフトウェアのアップデート'. The main area displays a table of devices under the 'デバイス' tab. The table has columns for 'デバイス名', 'オンライン', '登録日', 'os 名', '指定プロファイル', 'ステータスの更新日時', 'クライアントバージョン', 'マルウェア保護', and 'ソフトウェアアップデートのステータス'. Two devices are listed: 'tesutonomakku' and 'DESKTOP-BUVTNE1'. The 'DESKTOP-BUVTNE1' row has a red checkmark in the selection column. Below the table, a modal window titled '1台のデバイスを選択しました' is open, showing several action buttons. The 'ライセンスを変更する' button is highlighted with a red rectangle.

デバイス名	オンライン	登録日	os 名	指定プロファイル	ステータスの更新日時	クライアントバージョン	マルウェア保護	ソフトウェアアップデートのステータス	ラベル
tesutonomakku	いいえ	Aug 18, 2022	macOS	長期評価用	Aug 19, 2022, 8:14:12 AM	22.3.45064	有効		
DESKTOP-BUVTNE1	はい	Jul 20, 2022	Windows 10	評価用_WMI	Sep 1, 2022, 3:22:48 PM	22.4	有効	重要なアップデートはすべてインストール済み	

①対象となるコンピュータをチェックボックスで指定します。

②[ライセンスを変更する] ボタンをクリックします。

The screenshot shows the W/ Elements console interface. The left sidebar contains navigation options like 'ホーム', 'ENDPOINT PROTECTION', 'デバイス', and 'ソフトウェアのアップデート'. The main area displays a table of devices under the 'デバイス' tab. The table has columns for 'デバイス名', 'オンライン', '登録日', 'os 名', '指定プロファイル', 'ステータスの更新日時', 'クライアントバージョン', 'マルウェア保護', and 'ソフトウェアアップデートのステータス'. Four devices are listed: 'DESKTOP-19G0U1O', 'DESKTOP-3PNS171', 'knagasawanoMac', and 'DESKTOP-3LTHMJF'. The 'DESKTOP-19G0U1O' row has a red checkmark in the selection column. Below the table, a modal window titled '1台のデバイスを選択しました' is open, showing a dropdown menu for 'サブスクリプションの選択' and a 'ライセンスを変更する' button highlighted with a red rectangle.

デバイス名	オンライン	登録日	os 名	指定プロファイル	ステータスの更新日時	クライアントバージョン	マルウェア保護	ソフトウェアアップデートのステータス	ラベル
DESKTOP-19G0U1O	いいえ	Jul 1, 2022	Windows 10	喜多市	Aug 30, 2022, 9:54:05 AM	22.4	有効	重要なアップデートはすべてインストール済み	
DESKTOP-3PNS171	いいえ	Apr 11, 2022	Windows 10	喜多市	Aug 24, 2022, 8:57:32 PM	22.4	有効	重要なアップデートはすべてインストール済み	
knagasawanoMac	いいえ	Jun 15, 2020	macOS	喜多市	Aug 26, 2022, 6:08:35 AM	22.3.45064	有効		MacBook_Parallels_MacOS10
DESKTOP-3LTHMJF	いいえ	Apr 11, 2022	Windows 10	喜多市	Aug 24, 2022, 8:55:14 PM	22.4	有効	重要なアップデートはすべてインストール済み	

③新しいキーコードを入力または、別のキーコードを選択します。

④[ライセンスを変更する] ボタンをクリックします。

7.2.7. デバイスを削除する

Elements Security Center 上から、コンピュータを削除することができます。コンピュータを削除すると、そのコンピュータが使用していたライセンスの使用可能数は解放され、その使用可能数を使用して別なコンピュータへ Elements EPP クライアントをインストールすることができます。通常は、コンピュータを廃棄した場合、OS を再インストールした場合などに、コンピュータの削除を行います。

The screenshot shows the 'Devices' page in the W/ Elements Security Center. The table below is a representation of the data shown in the interface:

デバイス名	オンライン	登録日	OS 名	指定プロファイル	ステータスの更新日時	クライアントバージョン	マルウェア保護	ソフトウェアアップデートのステータス	ラベル
tesutonomakku	いいえ	Aug 18, 2022	macOS	長期評価用	Aug 19, 2022, 8:14:12 AM	22.3.45064	有効		
DESKTOP-BUYTNE1	はい	Jul 20, 2022	Windows 10	評価用_WMI	Sep 1, 2022, 3:22:48 PM	22.4	有効	重要なアップデートはすべてインストール済み	

The modal dialog at the bottom contains the following buttons:

- ステータス アップデートを送る
- ソフトウェア アップデートをインストール
- スキャン
- プロファイルを設定する
- ラベルを管理する
- ライセンスを查看する
- デバイスを削除する** (highlighted)
- ネットワークを開閉
- システムを再起動する
- 診断ファイルを取得する
- デバイスにメッセージを送信する
- アンインストール

①対象となるコンピュータをチェックボックスで指定します。

②[デバイスを削除する] ボタンをクリックします。

The screenshot shows the 'Devices' page in the W/ Elements Security Center. The table below is a representation of the data shown in the interface:

デバイス名	オンライン	登録日	OS 名	指定プロファイル	ステータスの更新日時	クライアントバージョン	マルウェア保護	ソフトウェアアップデートのステータス	ラベル
DESKTOP-19G0U10	いいえ	Jul 1, 2022	Windows 10	喜多山市	Aug 30, 2022, 9:54:05 AM	22.4	有効	重要なアップデートはすべてインストール済み	
DESKTOP-3PN5J71	いいえ	Apr 11, 2022	Windows 10	喜多山市	Aug 24, 2022, 8:57:32 PM	22.4	有効	重要なアップデートはすべてインストール済み	
knagasawanoMac	いいえ	Jun 15, 2020	macOS	喜多山市	Aug 26, 2022, 6:08:35 AM	22.3.45064	有効		MacBook_Parallels_MacOS10
DESKTOP-3LTHM1F	いいえ	Apr 11, 2022	Windows 10	喜多山市	Aug 24, 2022, 8:55:14 PM	22.4	有効	重要なアップデートはすべてインストール済み	

The modal dialog at the bottom contains the following buttons:

- デバイスの再追加をブロックする
- デバイスを削除する** (highlighted)



Elements Security Center よりコンピュータを削除後も、その削除されたコンピュータにインストールされている Elements EPP クライアントは、暫くの間（最大8時間）稼働した後、ライセンスエラーとなり動きは止まります。

7.2.8. ネットワークの隔離

デバイスを指定し、ネットワークから隔離及び隔離からの解放を行います

The screenshot shows the W/ Elements management interface. On the left is a navigation menu with options like 'ホーム', 'ENDPOINT PROTECTION', 'デバイス', etc. The main area displays a table of 8 devices. The first device, 'DESKTOP-11TTHRP', is selected with a red checkmark. Below the table, a dark overlay contains several action buttons. A red box highlights the 'ネットワークから隔離する' button, which has a dropdown menu open showing 'ネットワークの隔離' as the selected option.

デバイス名	全体保護	Endpoint Detection and Response	マルウェア保護	ファイアウォール	自動更新	ソフトウェアのアップデート	指定プロファイル	操作	ラベル
<input checked="" type="checkbox"/> DESKTOP-11TTHRP	保護されています	高リスク	有効	有効	最新	重要なアップデートはインストール済み	nagasawa_1214	0	トレーニング用
<input type="checkbox"/> knagasawanoMac	重大	有効	無効	有効	非常に古い	未インストール	WithSecure™ Office for Mac (locked)	1	MacBook_Parallels_MacOS_11_23_作業用PSB
<input type="checkbox"/> nagasawakatsushino MacBook-Air	保護されています	非アクティブ	有効	Apple	最新	未インストール	YD_TEST	0	

ネットワークから隔離する

- ①対象となるコンピュータをチェックボックスで指定します。
- ②[ネットワークからの隔離] ボタンをクリックします。

ネットワークから隔離から解放する

- ①対象となるコンピュータをチェックボックスで指定します。
- ②[ネットワークの隔離からの解放する] ボタンをクリックします。

7.2.9. システムを再起動する

Windows の端末に限り、デバイスの再起動を実行させることが可能です。

デバイスを自動的に再起動させますので、ユーザはすべてのデータを5分以内に保存する必要があります。また、デバイスの再起動を停止することはできません。

The screenshot shows the WTI Elements console interface. On the left, a sidebar contains navigation options like 'デバイス' (Devices) and 'ソフトウェアのアップデート' (Software Updates). The main area displays a table of devices. The device 'DESKTOP-BUVTNET' is selected with a red checkmark. Below the table, a modal window titled '1台のデバイスを選択しました' (Selected 1 device) is open, showing various action buttons. The 'システムを再起動する' (Restart System) button is highlighted with a red box.

デバイス名	オンライン	登録日	OS名	指定プロファイル	ステータスの更新日時	クライアントバージョン	マルウェア保護	ソフトウェアアップデートのステータス	ラベル
tesutonomakku	はい	Aug 18, 2022	macOS	長期評価用	Aug 19, 2022, 8:14:12 AM	22.3.45064	有効		
DESKTOP-BUVTNET	はい	Jul 20, 2022	Windows 10	評価用_WMI	Sep 1, 2022, 3:22:48 PM	22.4	有効	重要なアップデートはすべてインストール済み	

①対象となるコンピュータをチェックボックスで指定します。

②[システムを再起動する] ボタンをクリックします。

The screenshot shows the WTI Elements console interface for a specific device, 'DESKTOP-11TTHRP'. The left sidebar is the same as in the previous screenshot. The main area displays the device's status and configuration. The 'OS' field is highlighted with a red box. Below the device details, a modal window titled 'デバイスが自動的に再起動します' (Device will restart automatically) is open, showing a warning message and a '再起動' (Restart) button.

DESKTOP-11TTHRP エイリアスを追加
ステータスの更新日時 2022/08/02 10:40:47 | 前回のユーザ USER0531 | 登録日 2022/07/22 | ラベル トレーニング用 | セキュリティイベントを表示

保護ステータス	操作	接続されているデバイス: (54)	アプリケーション: (0)	スキャンレポート
✓	ネットワーク接続が有効になっています			
⚠	ライセンス			評価
✓	Endpoint Protection			保護されています
✓	マルウェア保護			有効
✓	ファイアウォール			有効
✓	自動更新			最新
✓	ソフトウェアのアップデート			重要なアップデートはすべてインストール済み
✓	デバイス制御			有効

7.2.10. 診断ファイルを要求する

The screenshot shows the W/ Elements console interface. On the left, a sidebar contains navigation options like 'ホーム', 'ENDPOINT PROTECTION', and 'デバイス'. The main area displays a table of devices under the 'デバイス' tab. Two devices are listed: 'tesutonomakku' (macOS) and 'DESKTOP-BUVTNE1' (Windows 10). The checkbox for 'DESKTOP-BUVTNE1' is checked and highlighted with a red box. Below the table, a modal window titled '1台のデバイスを選択しました' (Selected 1 device) is displayed. In this modal, the '診断ファイルを要求する' (Request diagnostic file) button is highlighted with a red box.

デバイス名	オンライン	登録日	OS名	指定プロファイル	ステータスの更新日時	クライアントバージョン	マルウェア保護	ソフトウェアアップデートのステータス	ラベル
tesutonomakku	いいえ	Aug 18, 2022	macOS	長期評価用	Aug 19, 2022, 8:14:12 AM	22.3.45064	有効		
DESKTOP-BUVTNE1	はい	Jul 20, 2022	Windows 10	評価用_WMI	Sep 1, 2022, 3:22:48 PM	22.4	有効	重要なアップデートはすべてインストール済み	

- ①対象となるコンピュータをチェックボックスで指定します。
- ②[診断ファイルを要求する] ボタンをクリックします。
- ③確認画面が表示されるので、内容を確認し[要求]ボタンをクリックします。

The screenshot shows the W/ Elements console with a modal dialog open. The dialog title is '1台のデバイスを選択しました' (Selected 1 device). The main text explains that diagnostic data will be uploaded to WithSecure and that user consent is required. A reference note states that diagnostic data (fsdiag files) is large and handled according to privacy policy. At the bottom, there is a text input field for a message to the user and a blue '要求' (Request) button, which is highlighted with a red box.

診断データをWithSecure™にアップロードすることを許可するようにユーザーに要求を送信してください。ファイブサーの理由から、ユーザーは承認を求められます。(サーバー製品には該当しません。サーバー製品では、診断ファイルはユーザーの承認を必要とせずに要求されます。)

① 参考: 診断データ (fsdiag ファイル) は非常に大きく、プライバシーポリシーに従って処理されます。

ユーザーへのオプションのメッセージ: 収集を許可するリクエストでユーザーに表示されるメッセージをここに入力できます

7.2.11. デバイスにメッセージを送信する

The screenshot shows the W/ Elements console interface. On the left, there is a navigation menu with options like 'ダッシュボード', 'デバイス', 'ソフトウェアのアップデート', etc. The main area displays a table of devices under the 'デバイス' section. The table has columns for 'デバイス名', 'オンライン', '登録日', 'os名', '指定プロファイル', 'ステータスの更新日時', 'クライアントバージョン', 'マルウェア保護', and 'ソフトウェアアップデートのステータス'. One device, 'DESKTOP-BUVTNE1', is selected, indicated by a red checkmark in the first column. Below the table, a modal window titled '1台のデバイスを選択しました' (1 device selected) is visible. It contains several buttons: 'ステータスアップデートを送る', 'ソフトウェアアップデートをインストール', 'スキャン', 'プロファイルを指定する', 'ラベルを管理する', 'ライセンスを変更する', 'デバイスを削除する', 'ネットワークの編集', 'システムを再起動する', '診断ファイルを表示する', and 'デバイスにメッセージを送信する'. The 'デバイスにメッセージを送信する' button is highlighted with a red box.

- ①対象となるコンピュータをチェックボックスで指定します。
- ②[デバイスにメッセージを送信する] ボタンをクリックします。
- ③デバイスに送信したいメッセージを記入し、[送信]ボタンをクリックします。

The screenshot shows the W/ Elements console interface. The main area displays a table of 8 devices. The first device, 'DESKTOP-11TTHRP', is selected with a blue checkmark. The table has columns for 'デバイス名', '全体保護', 'Endpoint Detection and Response', 'マルウェア保護', 'ファイアウォール', '自動更新', 'ソフトウェアのアップデート', '指定プロファイル', '操作', and 'ラベル'. Below the table, a modal window titled '1台のデバイスを選択しました' (1 device selected) is visible. It contains a text input field with the placeholder text 'ここにメッセージを入力します。' (Enter message here) and a '送信' (Send) button.

7.2.12. アンインストール

The screenshot shows the W/TH Elements console interface. The main content area displays a table of devices under the 'デバイス' (Devices) section. The table has columns for 'デバイス名' (Device Name), 'オンライン' (Online), '登録日' (Registration Date), 'os 名' (OS Name), '指定プロファイル' (Assigned Profile), 'ステータスの更新日時' (Status Update Date), 'クライアントバージョン' (Client Version), 'マルウェア保護' (Malware Protection), 'ソフトウェアアップデートのステータス' (Software Update Status), and 'ラベル' (Label). The device 'DESKTOP-BUVTNE1' is selected with a red checkmark. Below the table, a modal window titled '1台のデバイスを選択しました' (Selected 1 device) is displayed, with the 'アンインストール' (Uninstall) button highlighted in red.

デバイス名	オンライン	登録日	os 名	指定プロファイル	ステータスの更新日時	クライアントバージョン	マルウェア保護	ソフトウェアアップデートのステータス	ラベル
tesutonomakku	いいえ	Aug 18, 2022	macOS	長期評価用	Aug 19, 2022, 8:14:12 AM	22.3.45064	有効		
DESKTOP-BUVTNE1	はい	Jul 20, 2022	Windows 10	評価用_WMI	Sep 1, 2022, 3:22:48 PM	22.4	有効	重要なアップデートはすべてインストール済み	

①対象となるコンピュータをチェックボックスで指定します。

②[アンインストール] ボタンをクリックします。

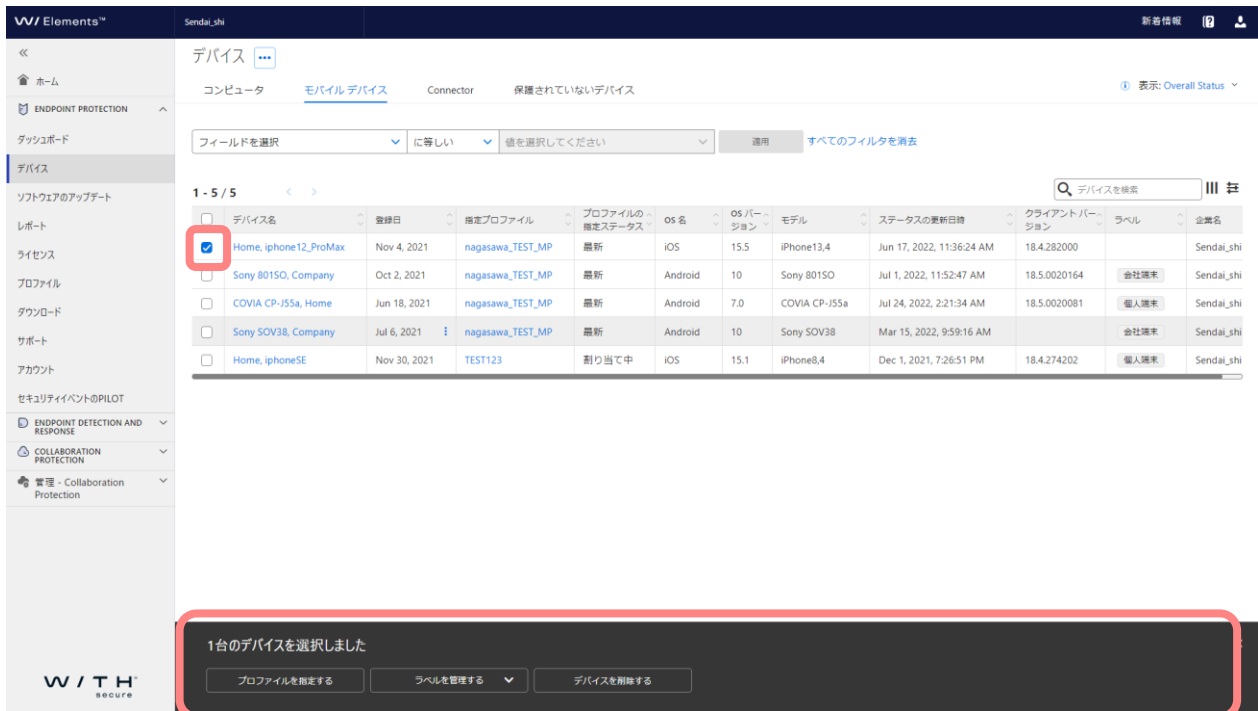
The screenshot shows the W/TH Elements console interface. The main content area displays a table of devices under the 'デバイス' (Devices) section. The table has columns for 'デバイス名' (Device Name), 'オンライン' (Online), '登録日' (Registration Date), 'os 名' (OS Name), '指定プロファイル' (Assigned Profile), 'ステータスの更新日時' (Status Update Date), 'クライアントバージョン' (Client Version), 'マルウェア保護' (Malware Protection), 'ソフトウェアアップデートのステータス' (Software Update Status), and 'ラベル' (Label). The device 'DESKTOP-19G0U1O' is selected with a red checkmark. Below the table, a modal window titled '1台のデバイスを選択しました' (Selected 1 device) is displayed, with the 'アンインストール' (Uninstall) button highlighted in red. The modal also contains the text: 'デバイス上でクライアントのアンインストールが行われます。これにより、サブスクリプションが解放され、デバイスに関するすべての情報がシステムから削除されます。' (Client uninstallation will be performed on the device. This will release the subscription and delete all information about the device from the system.)

デバイス名	オンライン	登録日	os 名	指定プロファイル	ステータスの更新日時	クライアントバージョン	マルウェア保護	ソフトウェアアップデートのステータス	ラベル
DESKTOP-19G0U1O	いいえ	Jul 1, 2022	Windows 10	喜多山市	Aug 30, 2022, 9:54:05 AM	22.4	有効	重要なアップデートはすべてインストール済み	
DESKTOP-3PNS171	いいえ	Apr 11, 2022	Windows 10	喜多山市	Aug 24, 2022, 8:57:32 PM	22.4	有効	重要なアップデートはすべてインストール済み	
knagasawanoMac	いいえ	Jun 15, 2020	macOS	喜多山市	Aug 26, 2022, 6:08:35 AM	22.3.45064	有効		MacBook_Parallels_MacOS10
DESKTOP-3LTHM1F	いいえ	Apr 11, 2022	Windows 10	喜多山市	Aug 24, 2022, 8:55:14 PM	22.4	有効	重要なアップデートはすべてインストール済み	

8. モバイルデバイスへの操作

8.1. 処理項目

選択したモバイルデバイスに対して、Elements Security Center 側から処理させたい項目を選択して実行させることができます。



- ①デバイス名欄のチェックを入れ処理を実行させる対象のモバイルデバイスを選択します。
- ②画面下部に「処理ボタン」が表示されます。
- ③「処理ボタン」を押すと選択対象のコンピュータに対して、処理が実行されます。設定や確認を行った後に処理を実行する項目も存在します

処理ボタン

項目名	内容
プロファイルを指定する	デバイスにプロファイルまたはラベルを指定します。
完全に削除	デバイスをブロックリストに移動または完全に削除します。
ラベルを管理する	デバイスにラベルを指定します。

8.2. 処理内容

8.2.1. プロファイルを指定する

任意のモバイルデバイスに対して、プロファイルまたはラベルを指定します。

The screenshot shows the 'Devices' page in the W/ Elements console. The table below lists the devices, with the 'Sony 80150, Company' row selected (checkbox checked).

デバイス名	登録日	指定プロファイル	プロファイルの指定ステータス	OS 名	OS バージョン	モデル	ステータスの更新日時	クライアントバージョン
<input type="checkbox"/> null, null	Nov 4, 2021	nagasawa_TEST_MP	最新	iPadOS	15.5	iPad5,2	Jun 25, 2022, 3:43:07 AM	18.4.282000
<input type="checkbox"/> nagasawk@gmail.com	Mar 15, 2022	nagasawa_TEST_MP	最新	Android	10	Sony SOV38	Jul 1, 2022, 12:27:42 PM	18.5.0020164
<input type="checkbox"/> Home, iphone12_ProMax	Nov 4, 2021	nagasawa_TEST_MP	最新	iOS	15.5	iPhone13,4	Jun 17, 2022, 11:36:24 AM	18.4.282000
<input checked="" type="checkbox"/> Sony 80150, Company	Oct 2, 2021	nagasawa_TEST_MP	最新	Android	10	Sony 80150	Jul 1, 2022, 11:52:42 AM	18.5.0020164
<input type="checkbox"/> COVIA CP-J55a, Home	Jun 18, 2021	nagasawa_TEST_MP	最新	Android	7.0	COVIA CP-J55a	Jul 24, 2022, 2:21:34 AM	18.5.0020081
<input type="checkbox"/> Sony SOV38, Company	Jul 6, 2021	nagasawa_TEST_MP	最新	Android	10	Sony SOV38	Mar 15, 2022, 9:59:16 AM	
<input type="checkbox"/> Home, iphoneSE	Nov 30, 2021	TEST123	割り当て中	iOS	15.1	iPhone8,4	Dec 1, 2021, 7:26:51 PM	18.4.274202

A modal dialog titled '1台のデバイスを選択しました' (Selected 1 device) is displayed at the bottom. It contains a button 'プロファイル指定する' (Specify profile) which is highlighted with a red box.

The screenshot shows the 'Devices' page in the W/ Elements console. The table below lists the devices, with the 'Sony 80150, Company' row selected (checkbox checked).

デバイス名	登録日	指定プロファイル	プロファイルの指定ステータス	OS 名	OS バージョン	モデル	ステータスの更新日時	クライアントバージョン
<input type="checkbox"/> null, null	Nov 4, 2021	nagasawa_TEST_MP	最新	iPadOS	15.5	iPad5,2	Jun 25, 2022, 3:43:07 AM	18.4.282000
<input type="checkbox"/> nagasawk@gmail.com	Mar 15, 2022	nagasawa_TEST_MP	最新	Android	10	Sony SOV38	Jul 1, 2022, 12:27:42 PM	18.5.0020164
<input type="checkbox"/> Home, iphone12_ProMax	Nov 4, 2021	nagasawa_TEST_MP	最新	iOS	15.5	iPhone13,4	Jun 17, 2022, 11:36:24 AM	18.4.282000
<input checked="" type="checkbox"/> Sony 80150, Company	Oct 2, 2021	nagasawa_TEST_MP	最新	Android	10	Sony 80150	Jul 1, 2022, 11:52:42 AM	18.5.0020164
<input type="checkbox"/> COVIA CP-J55a, Home	Jun 18, 2021	nagasawa_TEST_MP	最新	Android	7.0	COVIA CP-J55a	Jul 24, 2022, 2:21:34 AM	18.5.0020081
<input type="checkbox"/> Sony SOV38, Company	Jul 6, 2021	nagasawa_TEST_MP	最新	Android	10	Sony SOV38	Mar 15, 2022, 9:59:16 AM	
<input type="checkbox"/> Home, iphoneSE	Nov 30, 2021	TEST123	割り当て中	iOS	15.1	iPhone8,4	Dec 1, 2021, 7:26:51 PM	18.4.274202

A modal dialog titled '1台のデバイスを選択しました' (Selected 1 device) is displayed at the bottom. It contains a dropdown menu 'プロファイルを選択してください' (Select profile) and a button 'プロファイル指定する' (Specify profile), both highlighted with red boxes.

8.2.2. ラベルを管理する

任意のモバイルデバイスに対して、ラベルを追加/交換/削除します。

The screenshot shows the W/ Elements console interface. The 'デバイス' (Devices) section is active, displaying a table of devices. The device 'Sony 801SO, Company' is selected. A modal window at the bottom shows the following options:

- プロフィールを指定する
- ラベルを管理する (highlighted with a red box)
- デバイスを削除する

デバイス名	登録日	指定プロファイル	プロファイルの指定ステータス	OS名	OSバージョン	モデル	ステータスの更新日時	クライアントバージョン
null, null	Nov 4, 2021	nagasawa_TEST_MP	最新	iPadOS	15.5	iPad5,2	Jun 25, 2022, 3:43:07 AM	18.4.282000
nagasaw@gmail.com	Mar 15, 2022	nagasawa_TEST_MP	最新	Android	10	Sony SOV38	Jul 1, 2022, 12:27:42 PM	18.5.0020164
Home, iphone12_ProMax	Nov 4, 2021	nagasawa_TEST_MP	最新	iOS	15.5	iPhone13,4	Jun 17, 2022, 11:36:24 AM	18.4.282000
<input checked="" type="checkbox"/> Sony 801SO, Company	Oct 2, 2021	nagasawa_TEST_MP	最新	Android	10	Sony 801SO	Jul 1, 2022, 11:52:42 AM	18.5.0020164
COVIA CP-J55a, Home	Jun 18, 2021	nagasawa_TEST_MP	最新	Android	7.0	COVIA CP-J55a	Jul 24, 2022, 2:21:34 AM	18.5.0020081
Sony SOV38, Company	Jul 6, 2021	nagasawa_TEST_MP	最新	Android	10	Sony SOV38	Mar 15, 2022, 9:59:16 AM	
Home, iphoneSE	Nov 30, 2021	TEST123	割り当て中	iOS	15.1	iPhone8,4	Dec 1, 2021, 7:26:51 PM	18.4.274202

The screenshot shows the same W/ Elements console interface. The 'ラベルを管理する' dropdown menu is open, showing the following options:

- ラベルを追加する
- ラベルを交換する
- ラベルを削除する
- ラベルを管理する (highlighted with a red box)

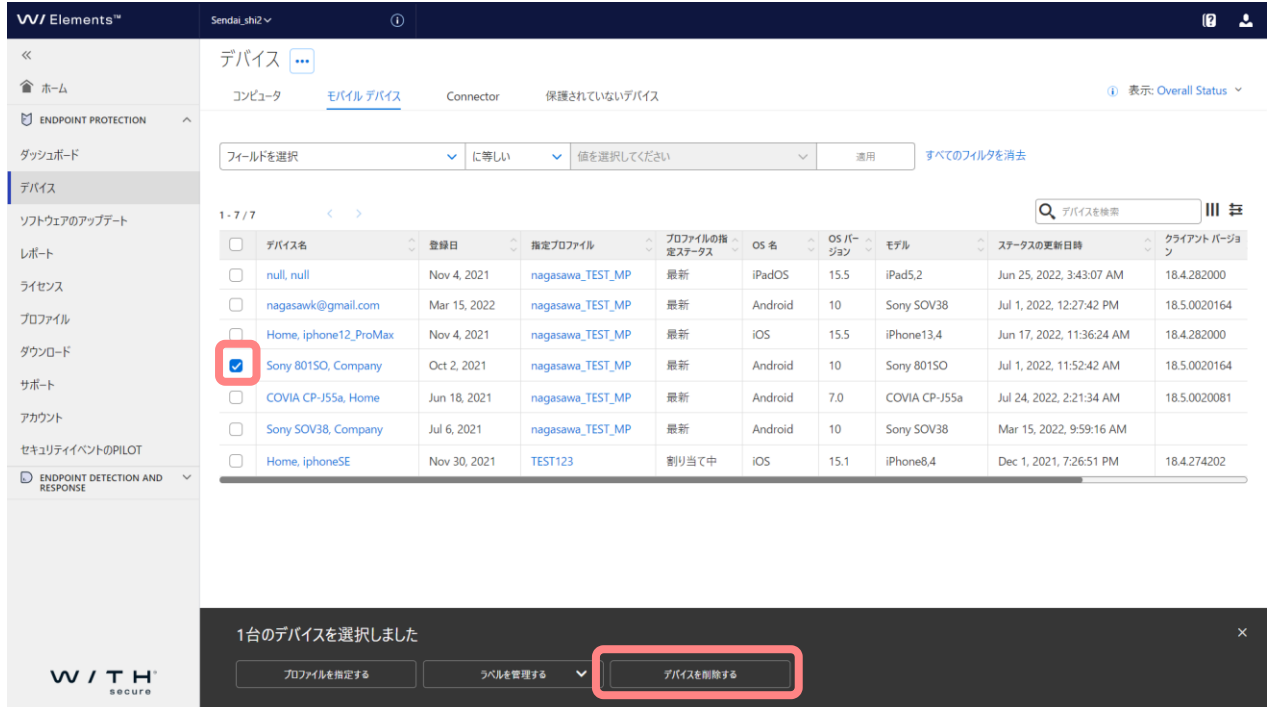
デバイス名	登録日	指定プロファイル	プロファイルの指定ステータス	OS名	OSバージョン	モデル	ステータスの更新日時	クライアントバージョン
null, null	Nov 4, 2021	nagasawa_TEST_MP	最新	iPadOS	15.5	iPad5,2	Jun 25, 2022, 3:43:07 AM	18.4.282000
nagasaw@gmail.com	Mar 15, 2022	nagasawa_TEST_MP	最新	Android	10	Sony SOV38	Jul 1, 2022, 12:27:42 PM	18.5.0020164
Home, iphone12_ProMax	Nov 4, 2021	nagasawa_TEST_MP	最新	iOS	15.5	iPhone13,4	Jun 17, 2022, 11:36:24 AM	18.4.282000
<input checked="" type="checkbox"/> Sony 801SO, Company	Oct 2, 2021	nagasawa_TEST_MP	最新	Android	10	Sony 801SO	Jul 1, 2022, 11:52:42 AM	18.5.0020164
COVIA CP-J55a, Home	Jun 18, 2021	nagasawa_TEST_MP	最新	Android	7.0	COVIA CP-J55a	Jul 24, 2022, 2:21:34 AM	18.5.0020081
Sony SOV38, Company	Jul 6, 2021	nagasawa_TEST_MP	最新	Android	10	Sony SOV38	Mar 15, 2022, 9:59:16 AM	
Home, iphoneSE	Nov 30, 2021	TEST123	割り当て中	iOS	15.1	iPhone8,4	Dec 1, 2021, 7:26:51 PM	18.4.274202

ラベルを管理する

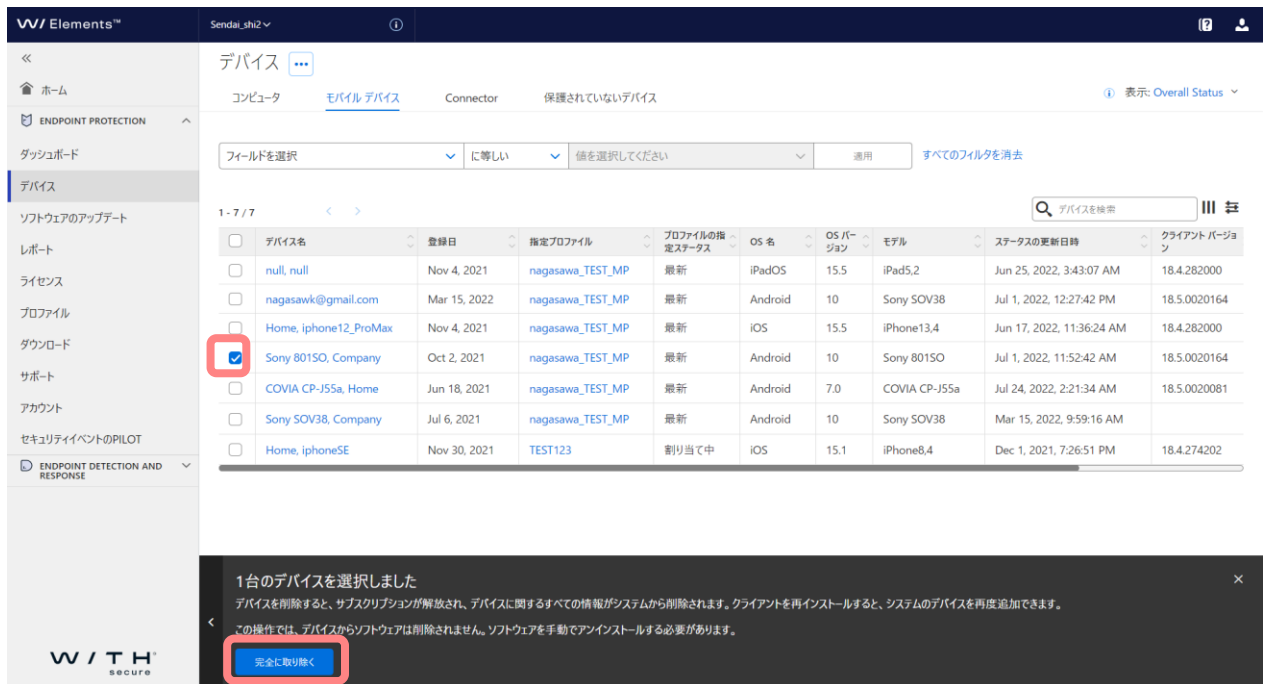
項目名	内容
ラベルを追加する	デバイスに追加するラベルを作成または選択します
ラベルを交換する	デバイスに交換するラベルを選択します 既に他のデバイスで使用しているラベルに交換できます
ラベルを削除する	デバイスから削除するラベルを選択します

8.2.3. デバイスを削除する

Elements Security Center 上から、モバイルデバイスを削除することができます。モバイルデバイスを削除すると、そのモバイルデバイスが使用していたライセンスの使用可能数は解放され、その使用可能数を使用して別なモバイルデバイスへインストールすることができます。



①対象となるコンピュータをチェックボックスで指定します。



②[完全に取り除く] ボタンをクリックします。

③確認画面が表示されるので、内容を確認し[完全に取り除く]ボタンをクリックします

9. ソフトウェアのアップデート

セキュリティパッチやアップデートを適用させます。

9.1. [ソフトウェアのアップデート] 操作メニュー概要

[ソフトウェアのアップデート] ボタンをクリックすると、以下の画面が表示されます。

ベンダー	ソフトウェア	現在のバージョン	ターゲットバージョン	カテゴリ	CVE ID	セキュリティ情報番号	コンピュータ	サーバ
Microsoft Corporation	Microsoft OneDrive	21.220.1024.0005	22.131.0619.0001	セキュリティに関連しない		FSPM-842-62029-113	1	0

9.1.1. アクションメニュー

ソフトウェアのアップデート



適用されていないアップデート インストール

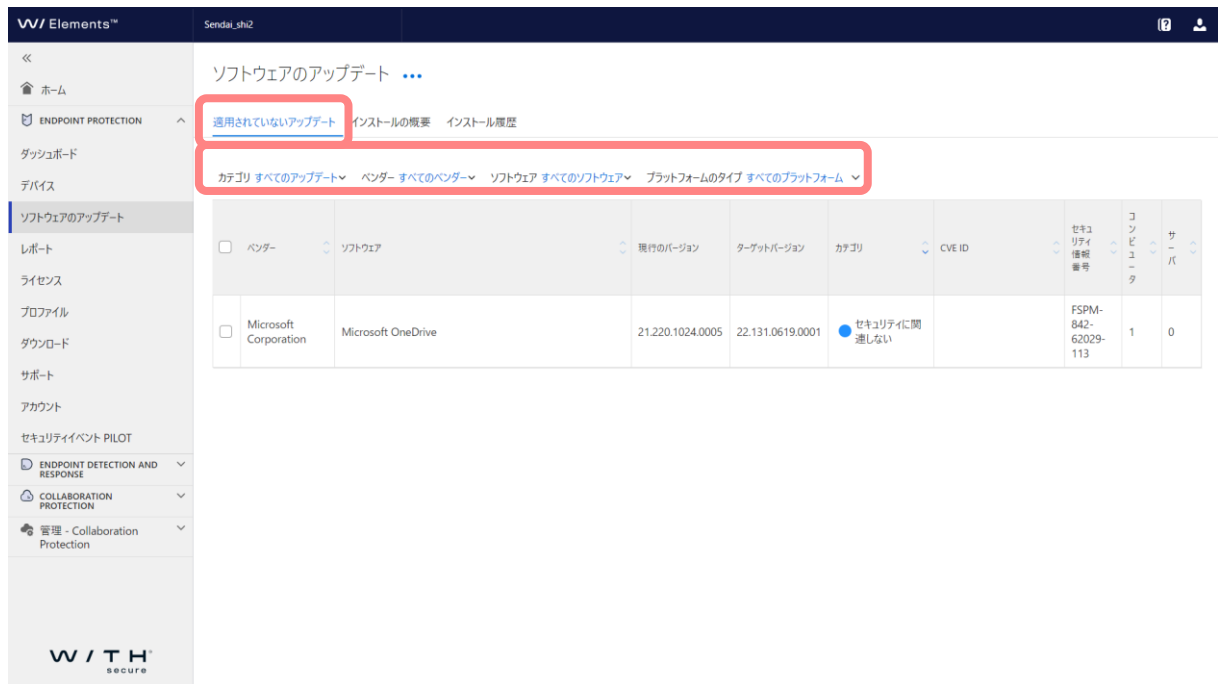
すべてのソフトウェア アップデート操作をエクスポート (CSV)

項目名	内容
すべてのソフトウェアアップデート操作をエクスポート (CSV)	ソフトウェアアップデートの操作のレポートが、CSV形式でダウンロードされます。

9.2. タブメニュー

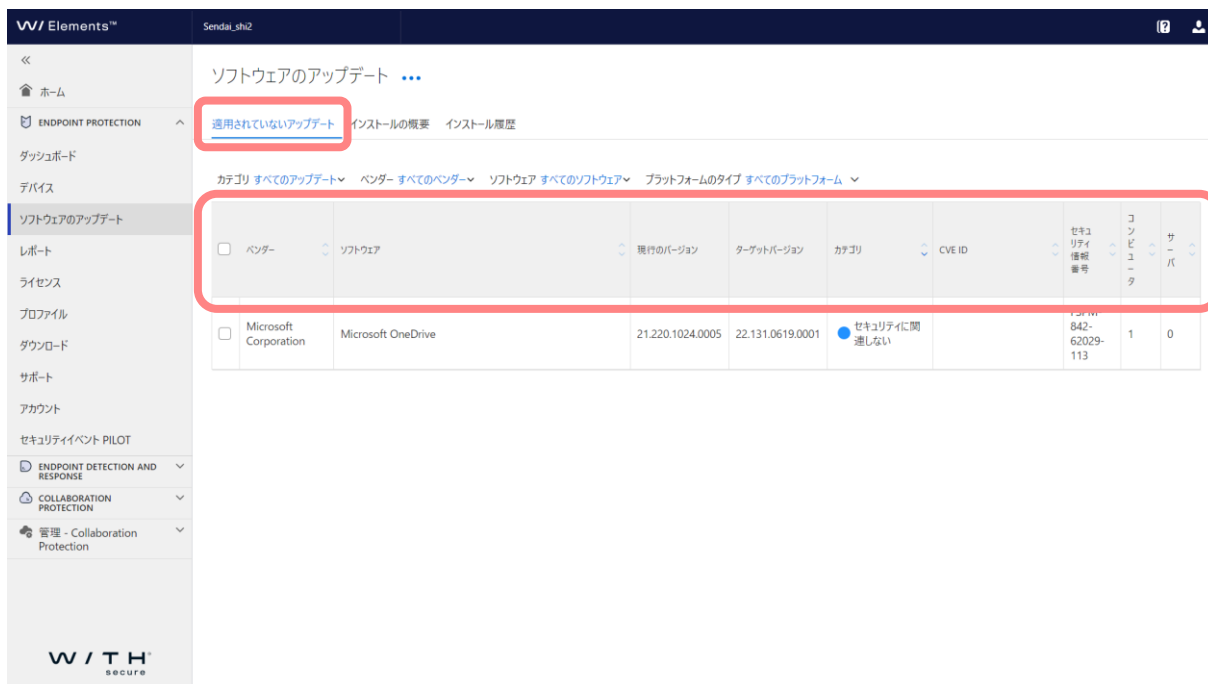
[適応されていないアップデート] / [インストールの概要] / [インストール履歴] ボタンで表示方法の切り替えができます。

9.2.1. 適応されていないアップデート



・適応されていないアップデート タブ

項目名	内容
カテゴリ	重要/重大などセキュリティアップデートの種類別に表示
ベンダー	ソフトウェアベンダー別に表示
ソフトウェア	ソフトウェア種類別に表示
プラットフォーム	サーバまたはワークステーション別に表示



・適応されていないアップデート タブ

項目名	内容
ベンダー	ソフトウェアベンダー
ソフトウェア	ソフトウェア種類
現在のバージョン	インストール済 バージョン
ターゲットバージョン	アップデート予定 バージョン
カテゴリ	重要/重大などセキュリティアップデートの種類別に表示
CVE ID	CVE ID の表示
セキュリティ情報番号	マイクロソフトのセキュリティ情報番号の表示
コンピュータ	対象コンピュータ端末
サーバ	対象サーバ端末

9.2.2. インスールの概要

ソフトウェアのアップデート ...

適用されていないアップデート **インストールの概要** インストール履歴

2022年7月27日 - 2022年8月2日

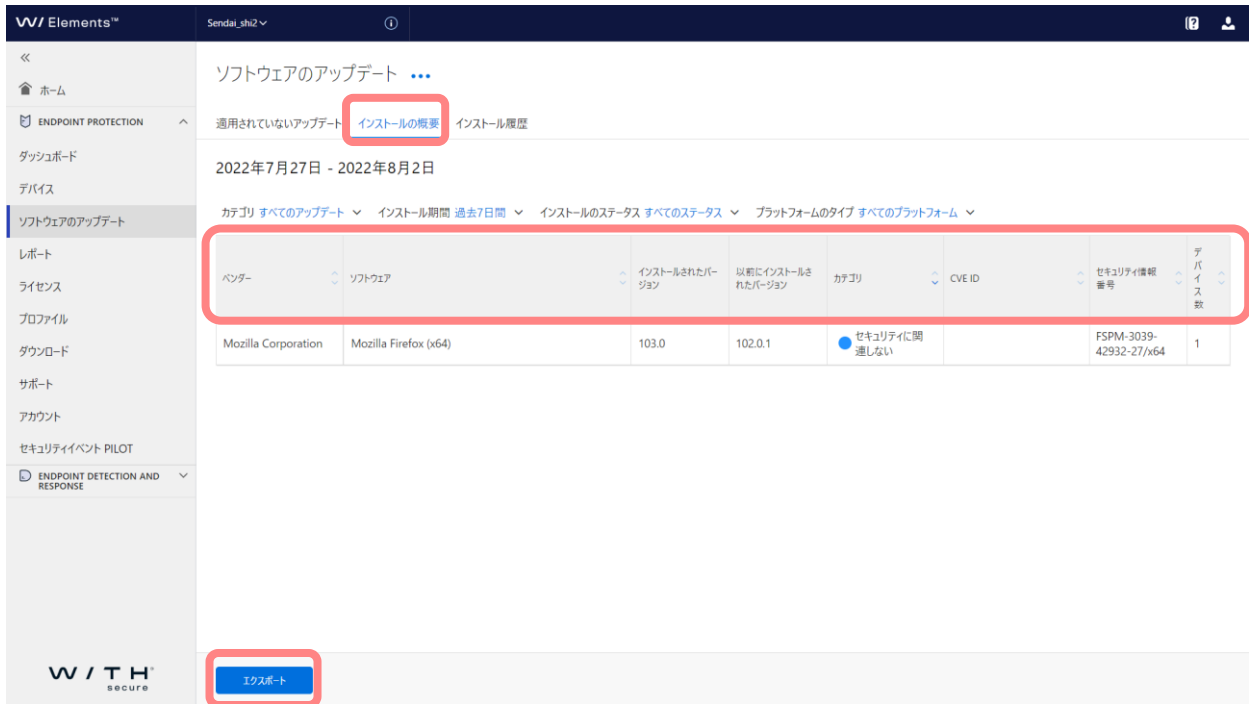
カテゴリ すべてのアップデート インストール期間 過去7日間 インストールのステータス すべてのステータス プラットフォームのタイプ すべてのプラットフォーム

ベンダー	ソフトウェア	インストールされたバージョン	以前にインストールされたバージョン	カテゴリ	CVE ID	セキュリティ情報番号	デバイス数
Mozilla Corporation	Mozilla Firefox (x64)	103.0	102.0.1	● セキュリティに関連しない		FSPM-3039-42932-27/x64	1

W / T H secure エクスポート

・インストールの概要 タブ

項目名	内容
カテゴリ	重要/重大などセキュリティアップデートの種類別に表示
インストール期間	日数別に表示
インストールのステータス	インストールのステータス状況の表示
プラットフォーム	サーバまたはワークステーション別に表示

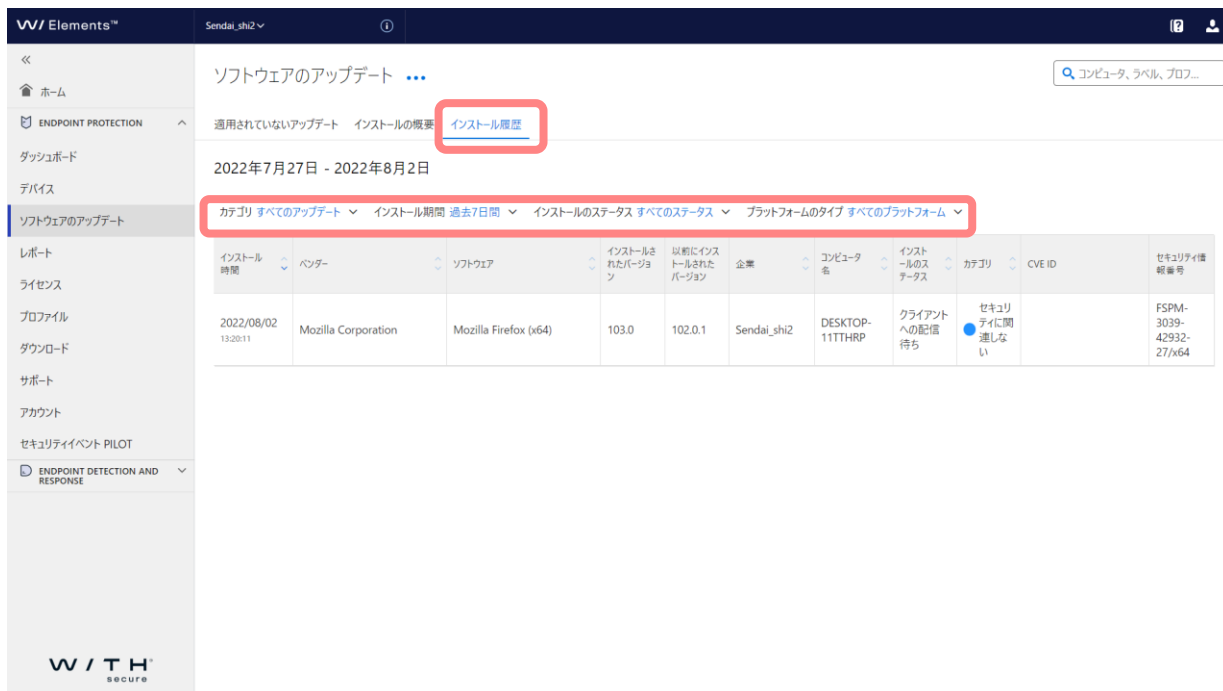


インストールの概要 タブ

項目名	内容
ベンダー	ソフトウェアベンダー
ソフトウェア	ソフトウェア種類
インストールされたバージョン	インストールされた バージョン
以前にインストールされたバージョン	以前にインストールされていた バージョン
カテゴリ	重要/重大などセキュリティアップデートの種類別に表示
CVE ID	CVE ID の表示
セキュリティ情報番号	マイクロソフトのセキュリティ情報番号の表示
デバイス数	対象の端末数

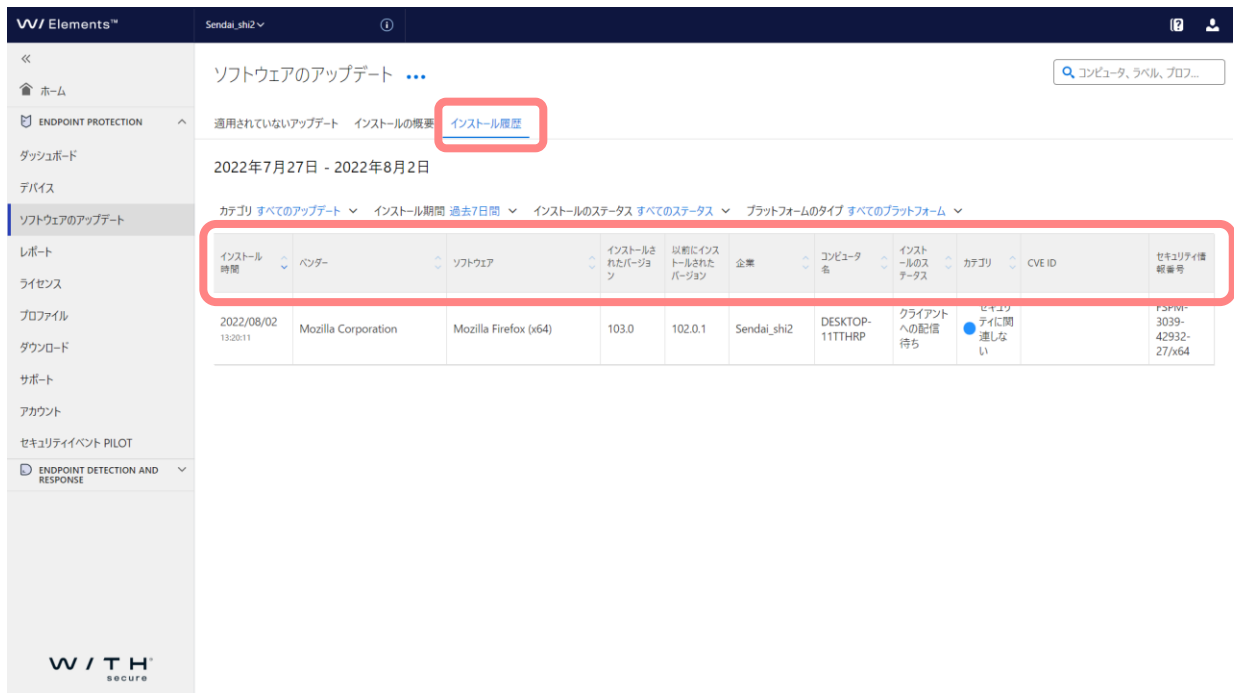
- ・ [エクスポート] ボタンで CSV 形式のリストのダウンロードが可能

9.2.3. インストール履歴



・インストール履歴 タブ

項目名	内容
カテゴリ	重要/重大などセキュリティアップデートの種類別に表示
インストール期間	日数別に表示
インストールのステータス	インストールのステータス状況の表示
プラットフォーム	サーバまたはワークステーション別に表示



インストールの概要 タブ

項目名	内容
インストール時間	インストール日時
ベンダー	ソフトウェアベンダー
ソフトウェア	ソフトウェア種類
インストールされたバージョン	インストールされた バージョン
以前にインストールされたバージョン	以前にインストールされていた バージョン
企業	インストールを実行した企業名
コンピュータ名	インストールを実行したコンピュータ名
カテゴリ	重要/重大などセキュリティアップデートの種類別に表示
CVE ID	CVE ID の表示
セキュリティ情報番号	マイクロソフトのセキュリティ情報番号の表示

9.3. すべてのコンピュータで更新

任意のセキュリティパッチやアップデートをコンピュータに対して適用させます。

ソフトウェアのアップデート ...

適用されていないアップデート インストールの概要 インストール履歴

カテゴリ すべてのアップデート ベンダー すべてのベンダー ソフトウェア すべてのソフトウェア プラットフォームのタイプ すべてのプラットフォーム

<input checked="" type="checkbox"/>	ベンダー	ソフトウェア	現在のバージョン	ターゲットバージョン	カテゴリ	CVE ID	セキュリティ情報番号	コンピュータ	サーバ
<input checked="" type="checkbox"/>	Microsoft Corporation	Microsoft OneDrive	21.220.1024.0005	22.131.0619.0001	セキュリティに関連しない		FSPM-842-62029-113	1	0

1件のアップデートを選択しました

すべてのコンピュータで更新 すべてのサーバで更新 アップデートするデバイスの選択

[すべてのコンピュータで更新]ボタンをクリックします。

9.4. すべてのサーバで更新

任意のセキュリティパッチやアップデートをサーバに対して適用させます。

ソフトウェアのアップデート ...

適用されていないアップデート インストールの概要 インストール履歴

カテゴリ すべてのアップデート ベンダー すべてのベンダー ソフトウェア すべてのソフトウェア プラットフォームのタイプ すべてのプラットフォーム

ベンダー	ソフトウェア	現在のバージョン	ターゲットバージョン	カテゴリ	CVE ID	セキュリティ情報番号	コンピュータ	サーバ
<input checked="" type="checkbox"/> Microsoft Corporation	Microsoft OneDrive	21.220.1024.0005	22.131.0619.0001	セキュリティに関連しない		ESPM-842-62029-113	1	0

1件のアップデートを選択しました

すべてのコンピュータで更新 **すべてのサーバで更新** アップデートするデバイスの選択

[すべてのサーバで更新]ボタンをクリックします。

9.5. アップデートするデバイスの選択

任意のセキュリティパッチやアップデートを任意のコンピュータに対して適用させます。

The screenshot shows the 'ソフトウェアのアップデート' (Software Updates) page in the W/ Elements interface. The table below lists available updates:

ベンダー	ソフトウェア	現在のバージョン	ターゲットバージョン	カテゴリ	CVE ID	セキュリティ情報番号	コンピュータ	サーバ
<input checked="" type="checkbox"/>	Microsoft Corporation	Microsoft OneDrive	21.220.1024.0005	22.131.0619.0001	セキュリティに関連しない	FSPM-842-62029-113	1	0

At the bottom of the interface, a dark bar contains three buttons: 'すべてのコンピュータで更新' (Update all computers), 'すべてのサーバで更新' (Update all servers), and 'アップデートするデバイスの選択' (Select devices to update), which is highlighted with a red box.

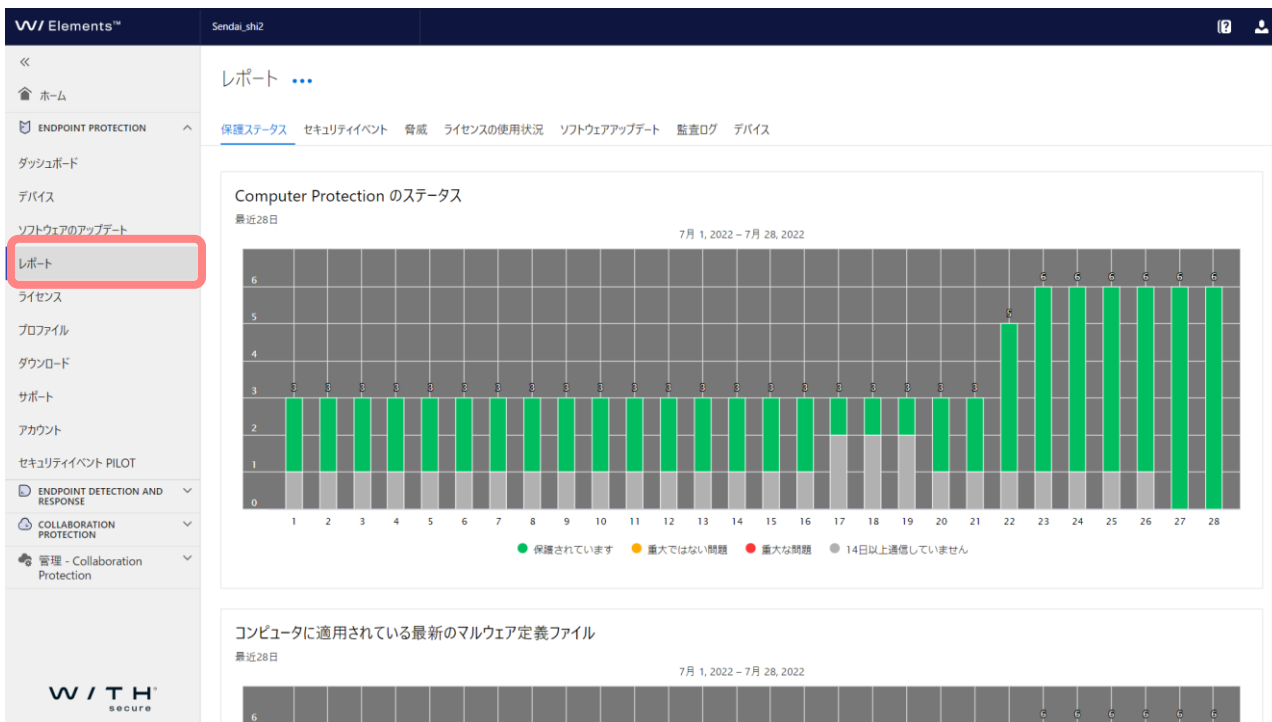
- ①アップデートさせたいセキュリティパッチやアップデートを一覧から選択します。
- ②[アップデートするデバイスの選択] ボタンをクリックします。
- ③すると、選択されたセキュリティパッチやアップデートが適用されていない端末の一覧が表示されます。
- ④表示された一覧から、適用する [コンピュータ] を選択します。
- ⑤[更新] ボタンをクリックします。

10. レポート

レポートの概要をグラフで確認できます。

10.1. [レポート] の操作メニュー概要

[レポート]ボタンをクリックすると、以下のような画面が表示されます。



10.2. アクションメニュー

レポート ⋮

保護ステータス

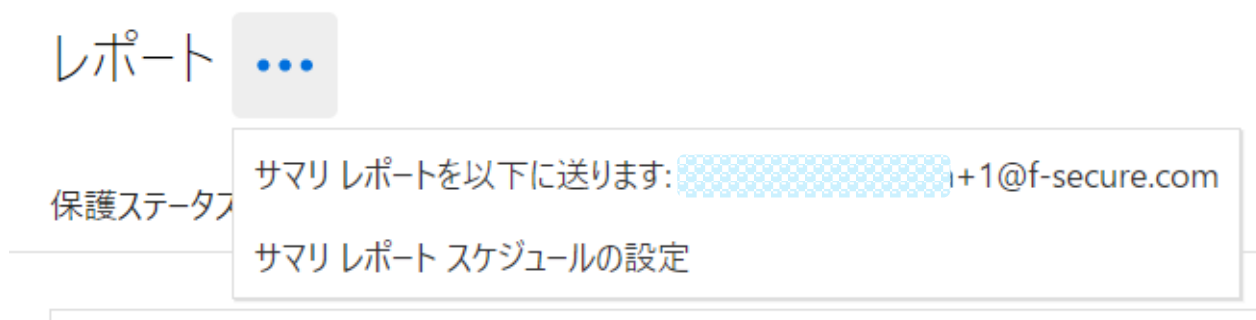
サマリレポートを以下に送ります: [メールアドレス]@f-secure.com

サマリレポート スケジュールの設定

項目名	内容
サマリレポートを以下に送ります：メールアドレス	指定のメールアドレスにサマリレポートを送付

10.3. レポートのサマリ送信

「レポート」見出し横のアクションメニューボタンをクリックし、「サマリレポートを以下に送ります:」をクリックすることで、その時点でのサマリをログインユーザに送付します。



また、「サマリレポートのスケジュール設定」を選択することで、任意のメールアドレスに、週次または月次でのサマリレポートを送付する設定を行えます。



10.4. タブメニュー

タブメニューをクリックするとレポート概要を切り替えることができます。

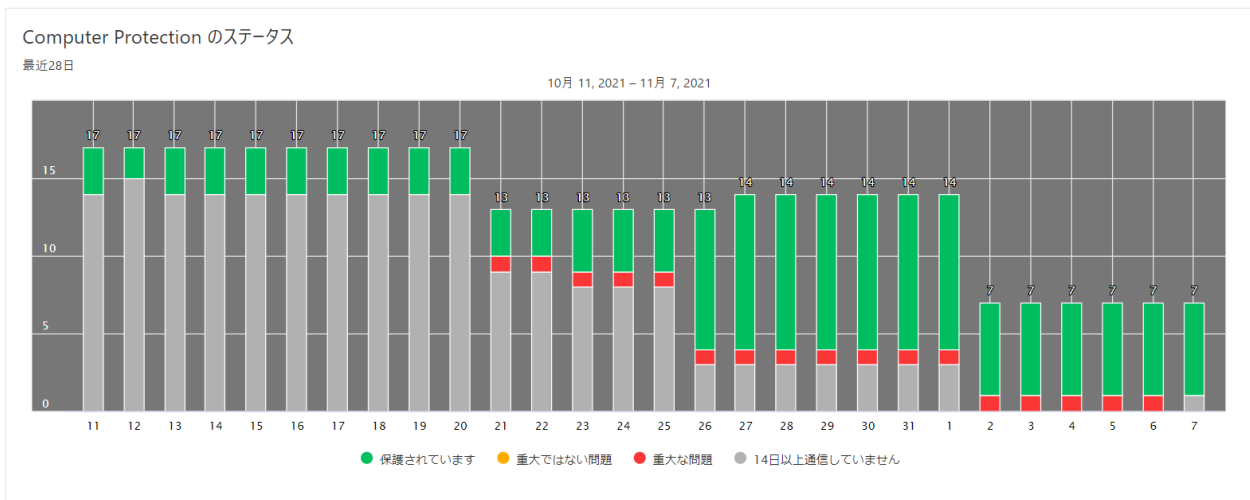
レポート ...

保護ステータス セキュリティイベント 脅威 ライセンスの使用状況 ソフトウェアアップデート 監査ログ デバイス

10.5. 保護ステータス

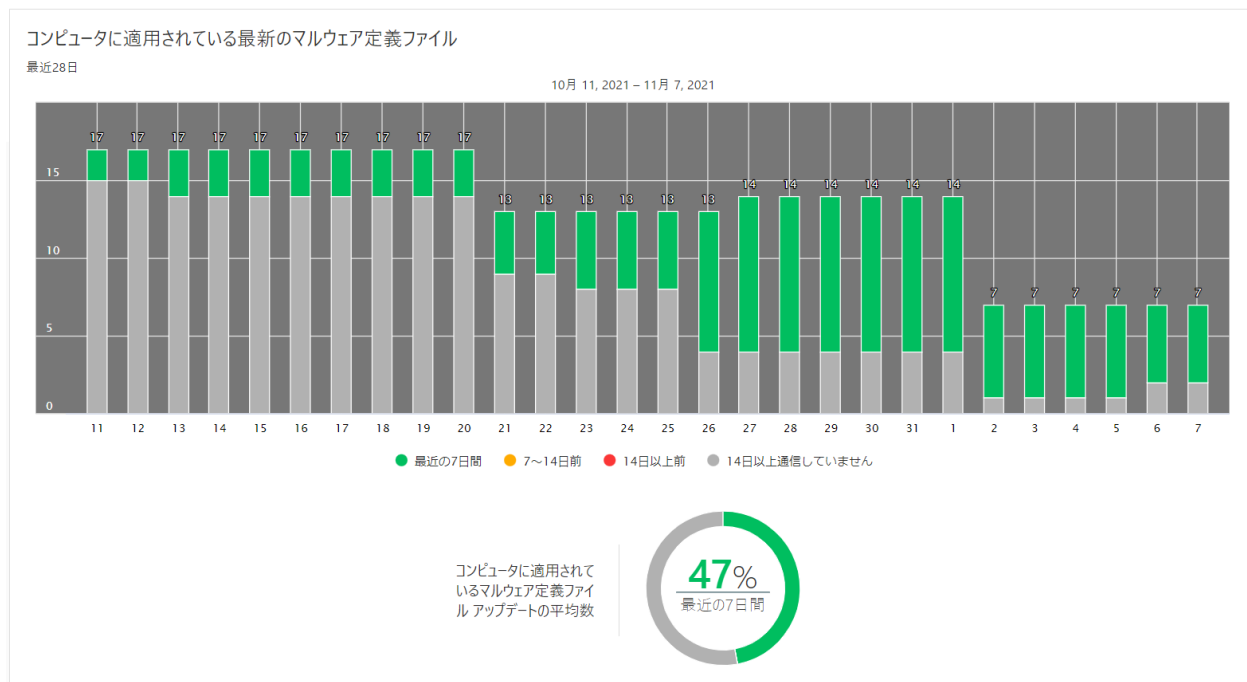
10.5.1. Computer Protection のステータス

コンピュータの保護状況が日毎に棒グラフで表示されます。



10.5.2. コンピュータに適用されている最新のマルウェア定義ファイル

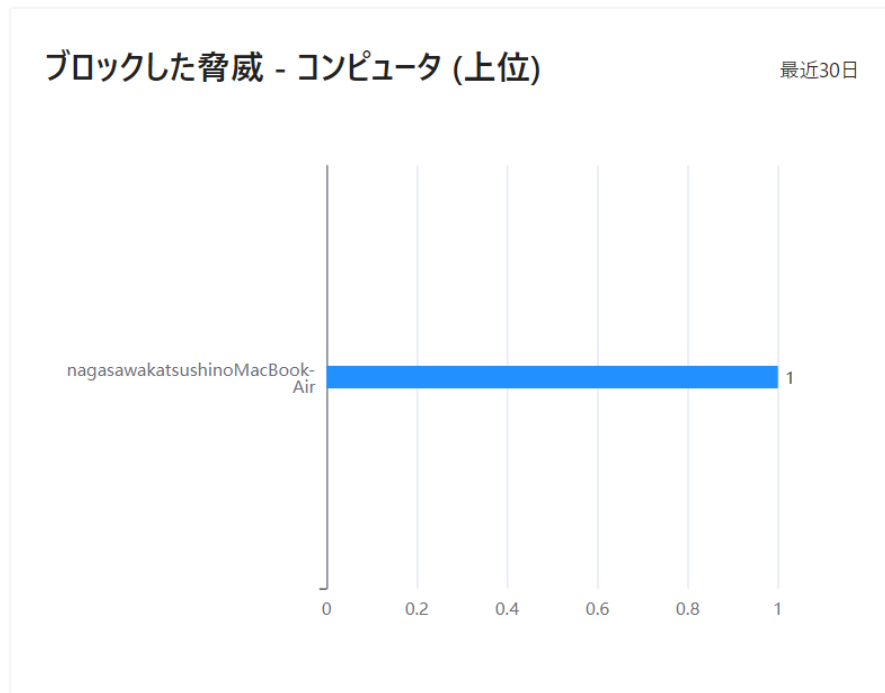
コンピュータに適用されているパターンファイルの更新状況を毎日に棒グラフで表示します。



10.6. セキュリティイベント

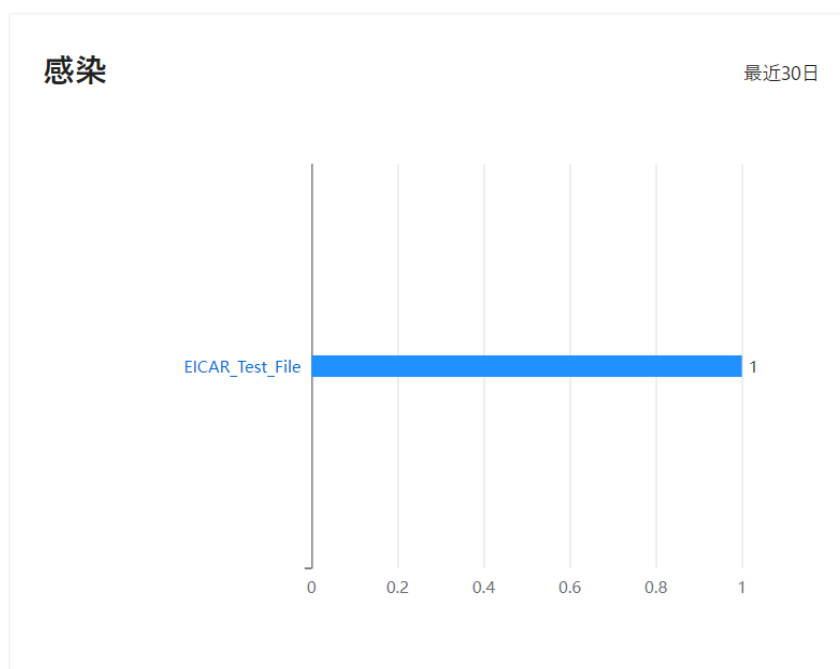
10.6.1. ブロックした脅威- コンピュータ（上位）

直近の 30 日の間にウイルスを検知したコンピュータの上位トップ 10 までを表示します。数字は、検知した数です。



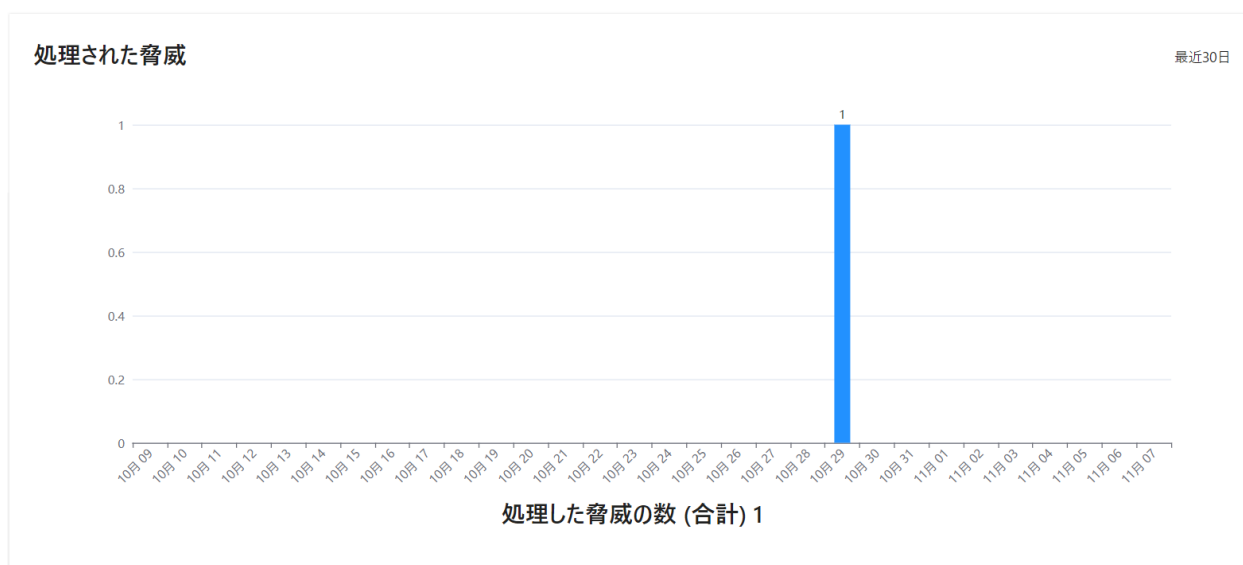
10.6.2. 感染

直近の 30 日の間に検知されたマルウェアの上位トップ 10 までを表示します。数字は、検知した数です。



10.6.3. 処理した脅威

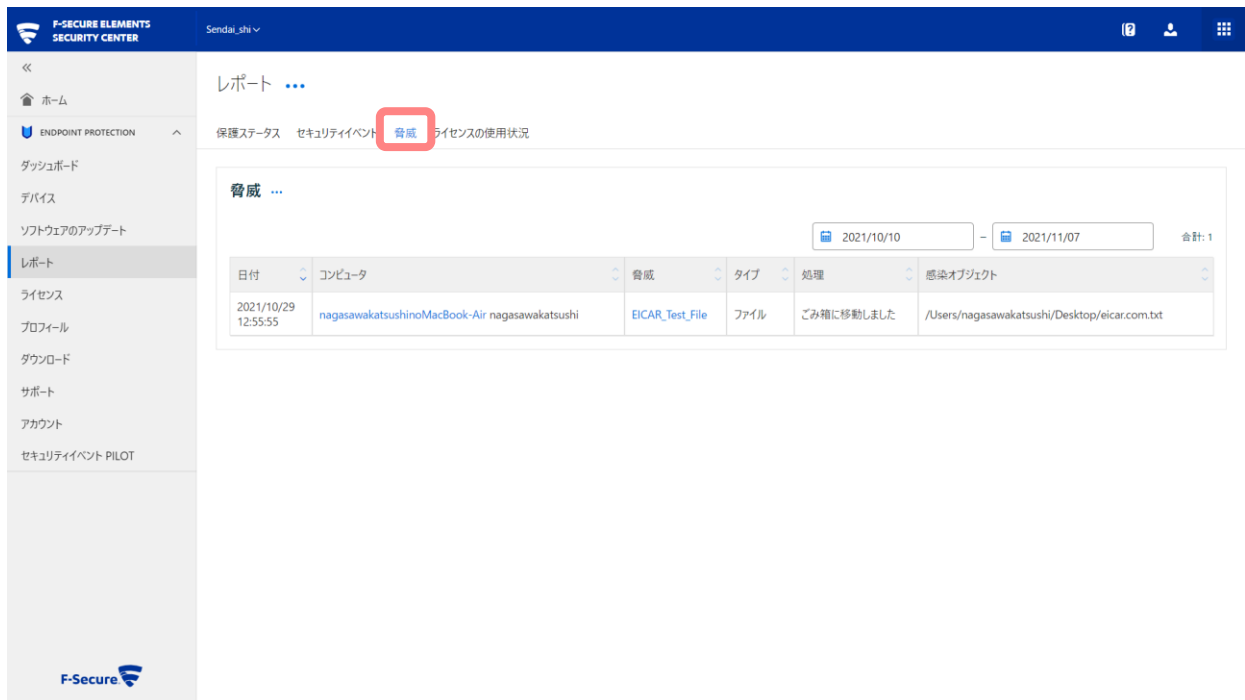
直近の 30 日の間に検知されたマルウェアの上位トップ 10 までを表示します。数字は、検知された数です。



10.7. 脅威

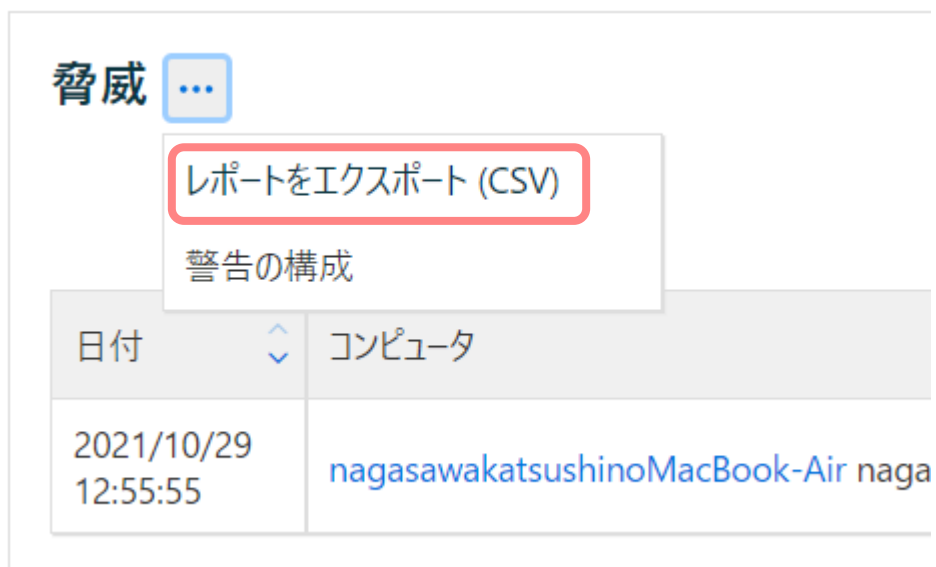
[脅威] タブをクリックするとマルウェアの検知した履歴が一覧で表示されます。

注意：「脅威」タブは、「セキュリティイベント PILOT」ビューに置き換えられ、2022年10月4日までにサポート終了します。



10.7.1. 脅威レポートのエクスポート

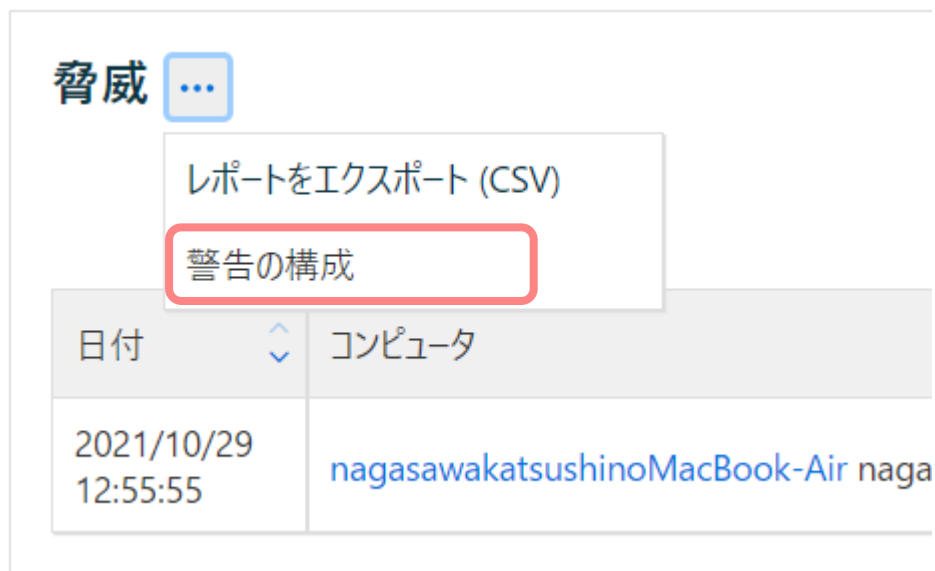
「脅威」見出し横のアクションメニューボタンをクリックし、[レポートをエクスポート (CSV)] をクリックすると CSV 形式でのレポートがダウンロードされます。



10.7.2. 脅威の警告を設定する

***アラートは現在無効にすることしかできません。**

「脅威」見出し横のアクションメニューボタンをクリックし、[警告の構成]をクリックすると、マルウェア検知時のメールによる警告転送の設定が行えます。

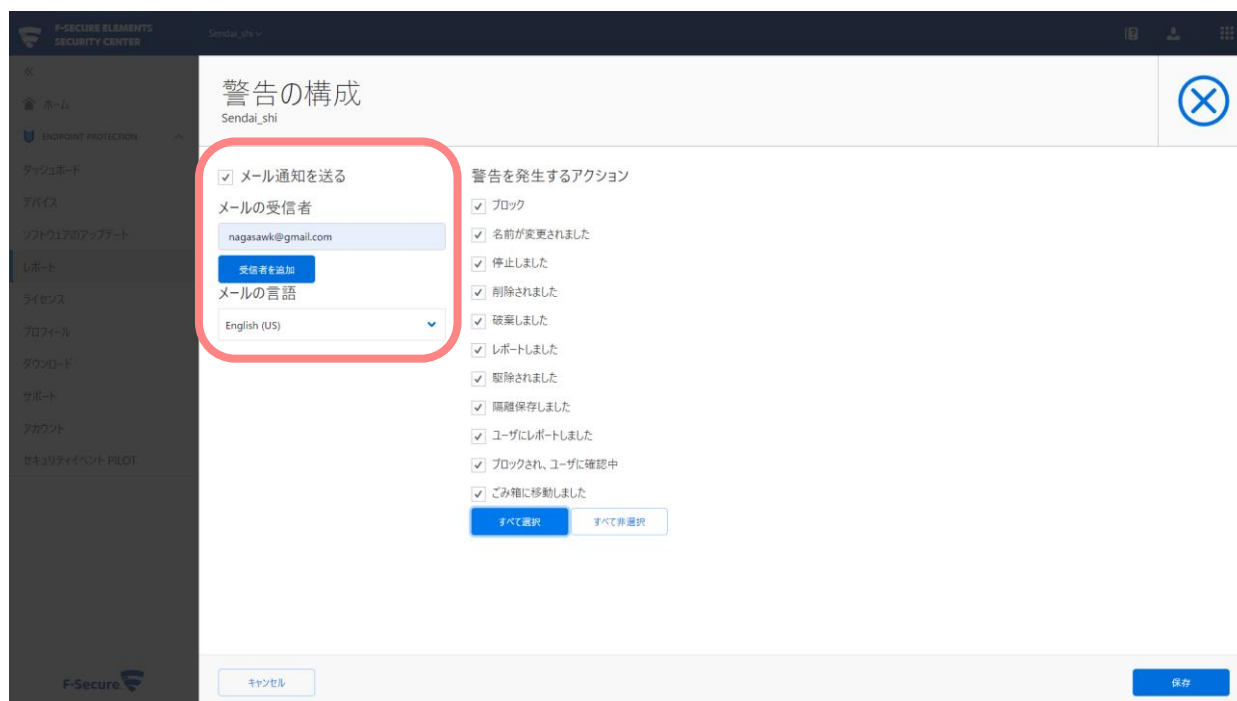


「メール通知を送る」にチェックを入れると、メールによる警告転送機能が有効になります。

「メールの受信者」のテキストボックスに警告を送信するメールアドレスを入力し「保存」をクリックします。

「メールの言語」を日本語に設定する場合は、[日本語] を選択します。

「警告の設定」の各設定の定義は以下のとおりです。



- ・ブロック

検知されたマルウェアが保存/展開されるのをブロックしました。

- ・名前を変更されました

検知されたマルウェアに対し、名前の変更（拡張子の一文字目を数字に変更）を行いました。

- ・停止しました

すでに感染して動作していて検知したマルウェアの動作を停止しました。

- ・削除されました

検知されたマルウェアに対し、削除を行いました。

- ・破棄しました

検知されたマルウェアの一部悪意のある活動に対し、ブロックを行いました。（ディープガードでの検知）

- ・レポートしました

検知されたマルウェアに対し、活動のブロックを行い、レポートを記録しました。

- ・駆除されました

検知されたマルウェアに対し、駆除処理を行いました。

- ・隔離保存しました

検知されたマルウェアに対し、隔離保存を行いました。

- ・ブロックされ、ユーザに確認中

検知されたマルウェアに対し、活動のブロックを行いましたが、ユーザが処理を選択しませんでした。

- ・ゴミ箱に移動しました

検知されたマルウェアに対し、ごみ箱に移動しました

10.8. ライセンスの使用状況

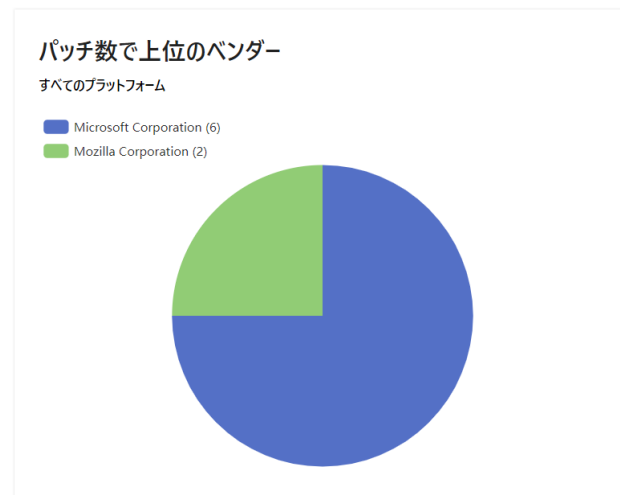
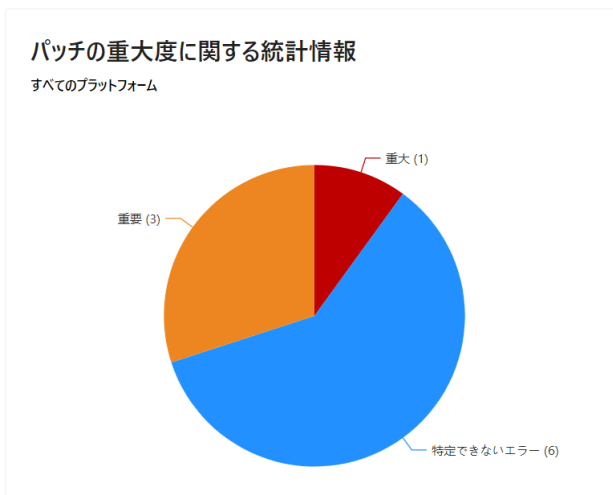
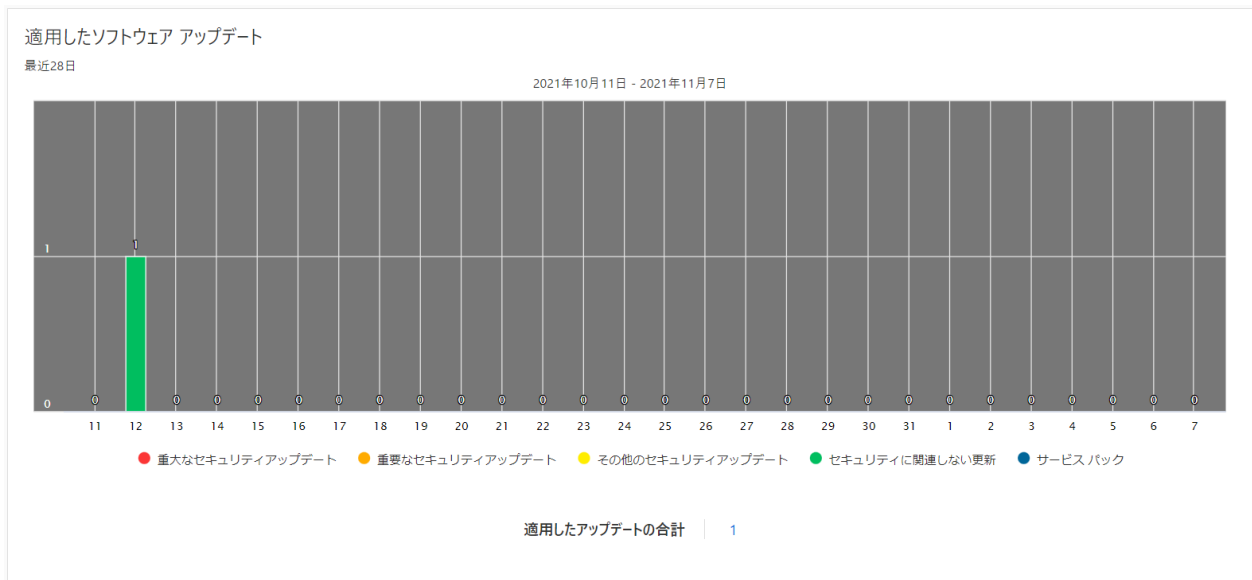
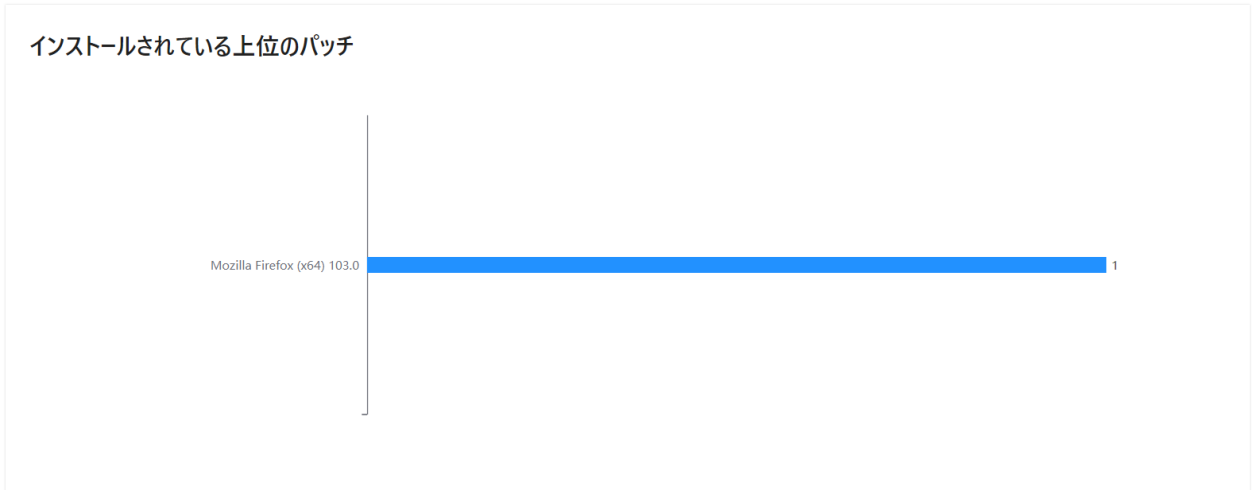
[ライセンスの使用状況] タブをクリックし、[エクスポート] ボタンをクリックすると、CSV ファイルがダウンロードできます。



*お客様の設定状況においては表示されない場合がございます。

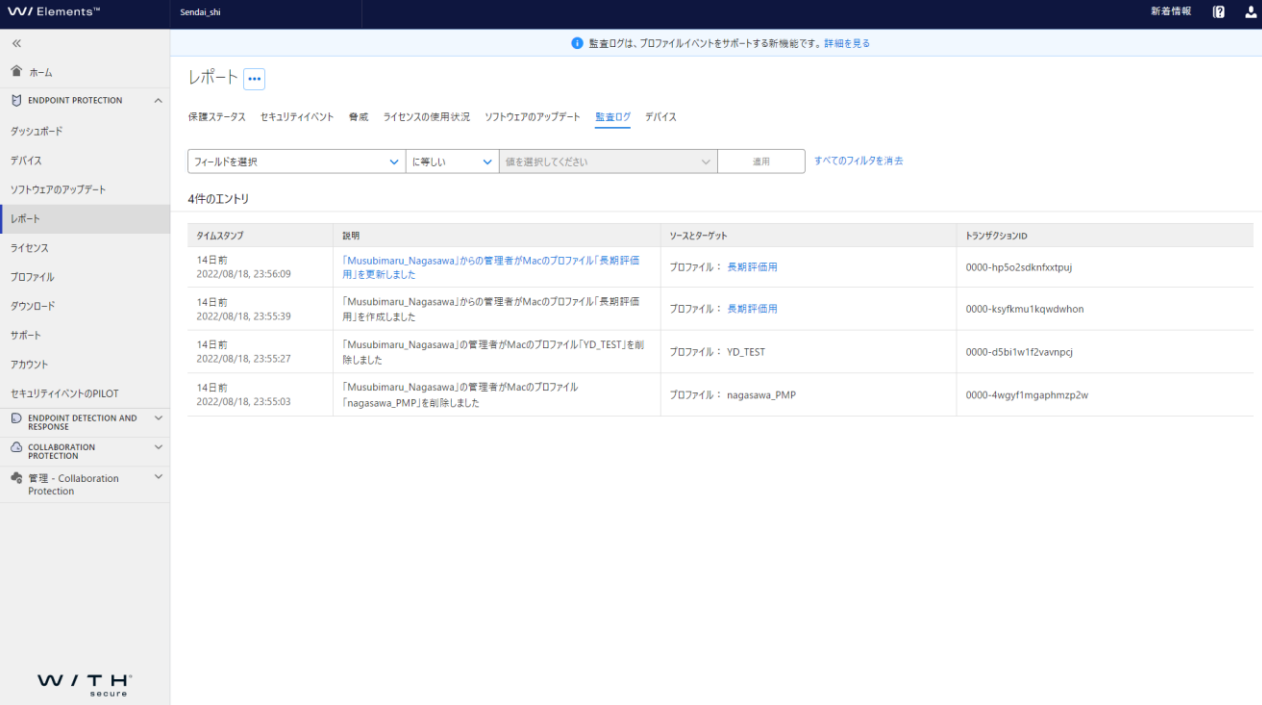
10.9. ソフトウェア アップデート

ソフトウェアアップデートにより、コンピュータに適用されたアップデートの状況を表示します。



10.10. 監査ログ

監査ログは、プロファイルの作成/削除/更新などのイベントをサポートする機能です。



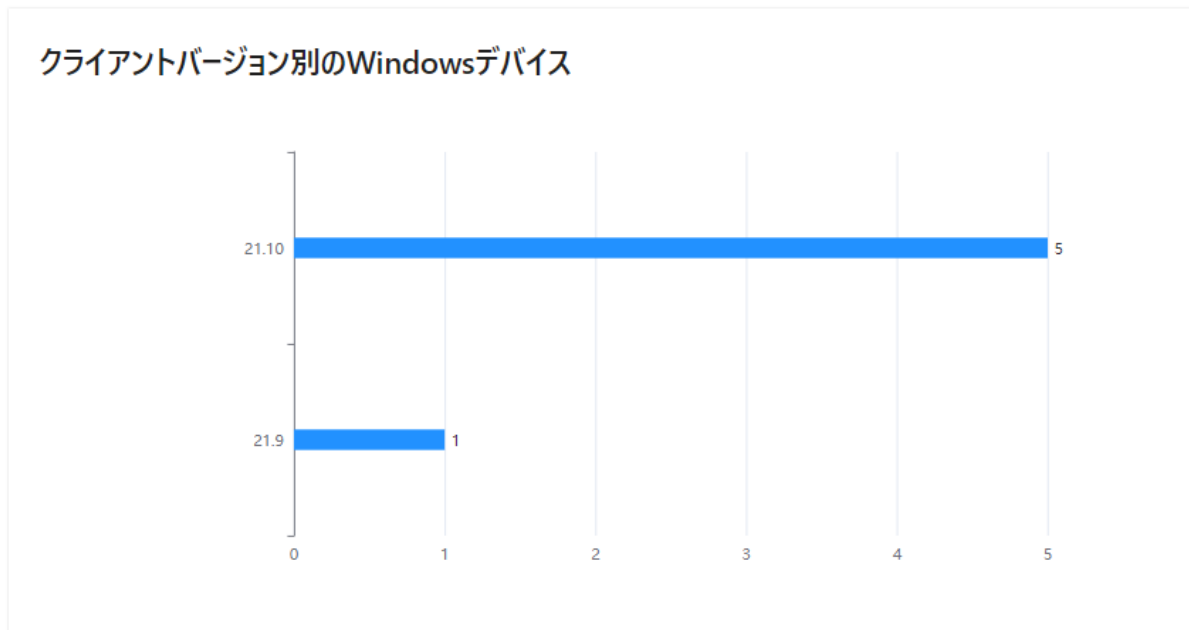
The screenshot shows the W/TH Elements management interface. The left sidebar contains navigation options like Home, Endpoint Protection, Dashboard, Devices, Software Updates, Reports, Licenses, Profiles, Downloads, Support, Accounts, and Security Events. The main content area is titled '監査ログ' (Audit Log) and shows a list of 4 events. A filter bar at the top allows selecting fields, sorting, and filtering. A notification at the top states: '監査ログは、プロファイルイベントをサポートする新機能です。詳細を見る' (Audit Log is a new feature that supports profile events. See details).

タイムスタンプ	説明	ソースとターゲット	トランザクションID
14日前 2022/08/18, 23:56:09	「Musubimaru_Nagasawa」からの管理者がMacのプロファイル「長期評価用」を更新しました	プロファイル: 長期評価用	0000-hp5o2sdknfxtpuj
14日前 2022/08/18, 23:55:39	「Musubimaru_Nagasawa」からの管理者がMacのプロファイル「長期評価用」を作成しました	プロファイル: 長期評価用	0000-ksyfkmu1kqwdwhon
14日前 2022/08/18, 23:55:27	「Musubimaru_Nagasawa」の管理者がMacのプロファイル「YD_TEST」を削除しました	プロファイル: YD_TEST	0000-d5bi1w1f2vavmpcj
14日前 2022/08/18, 23:55:03	「Musubimaru_Nagasawa」の管理者がMacのプロファイル「nagasawa_PMP」を削除しました	プロファイル: nagasawa_PMP	0000-4wgyl1mgaphmzp2w

10.11. デバイス

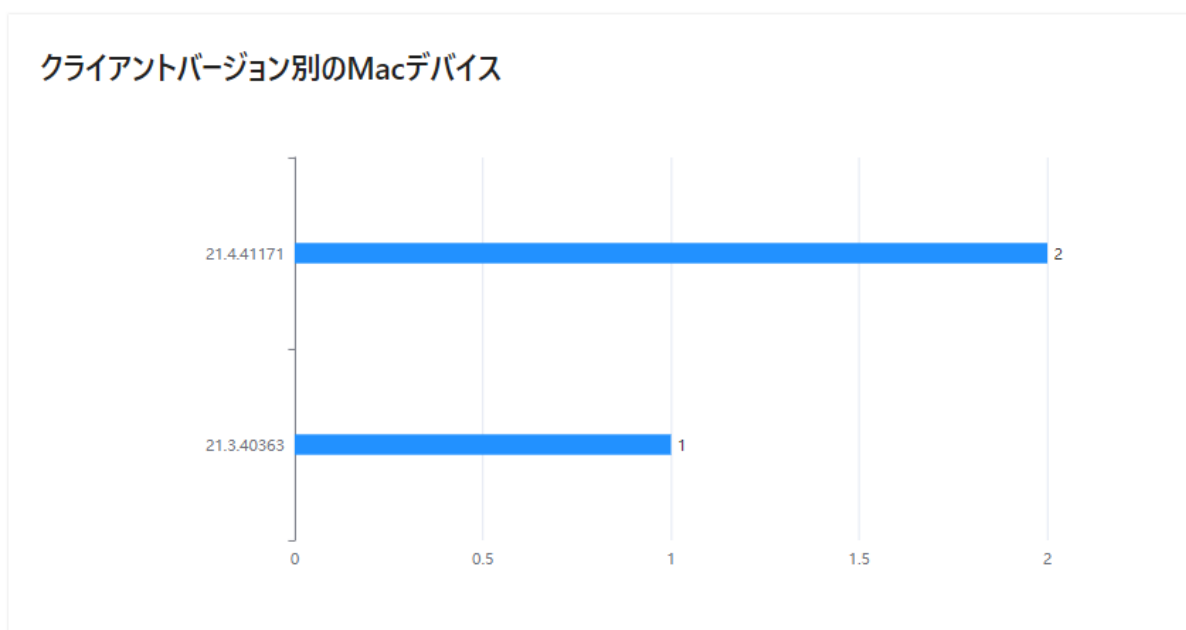
10.11.1. クライアントバージョン別の Windows デバイス

Windows デバイスにインストールしているクライアントモジュールのバージョンを確認できます。



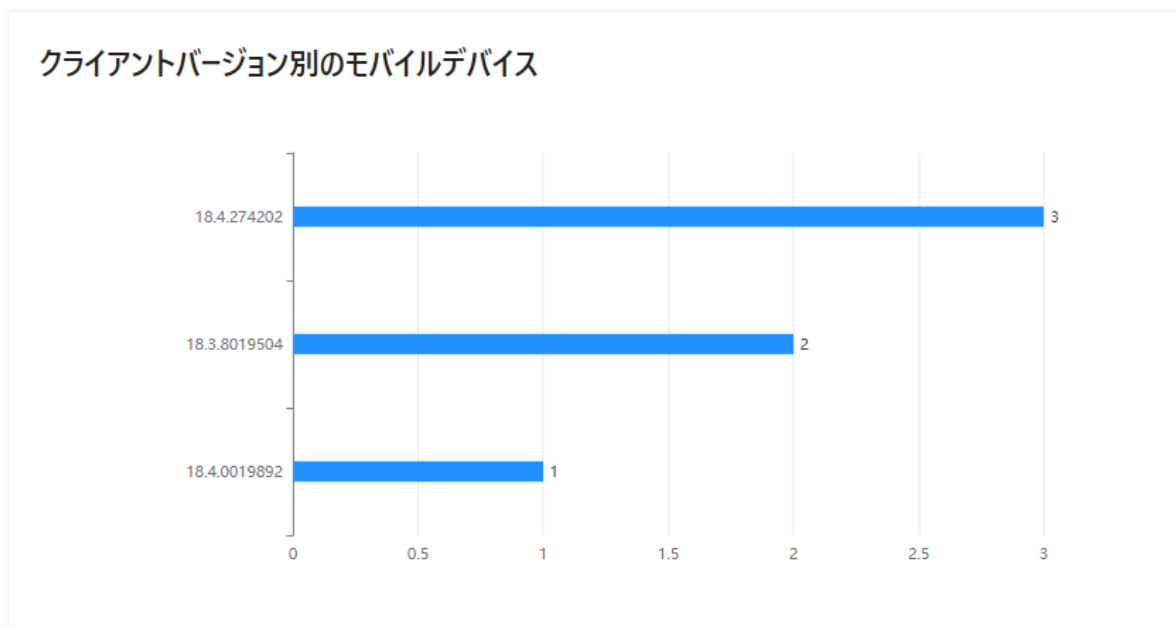
10.11.2. クライアントバージョン別の Mac デバイス

Mac デバイスにインストールしているクライアントモジュールのバージョンを確認できます。

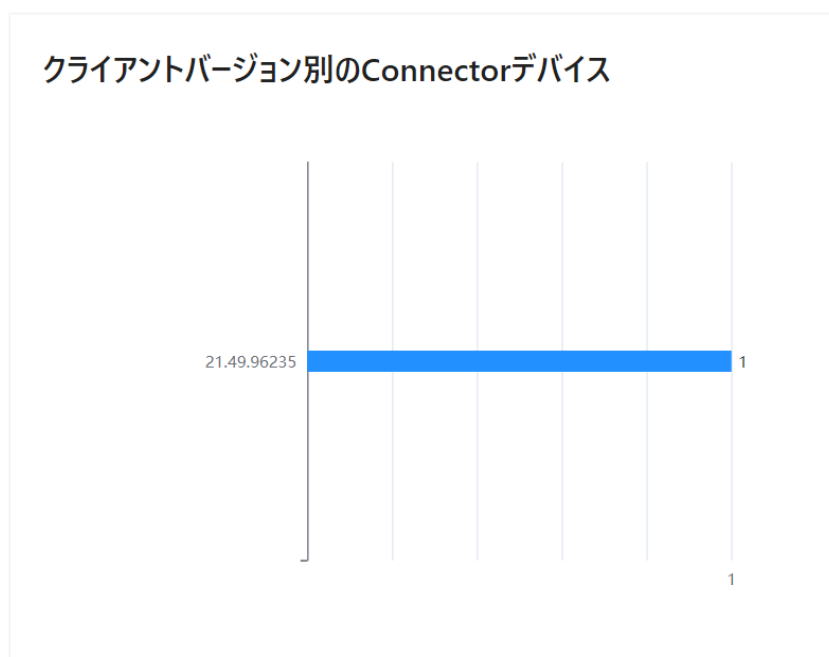


10.11.3. クライアントバージョン別のモバイルデバイス

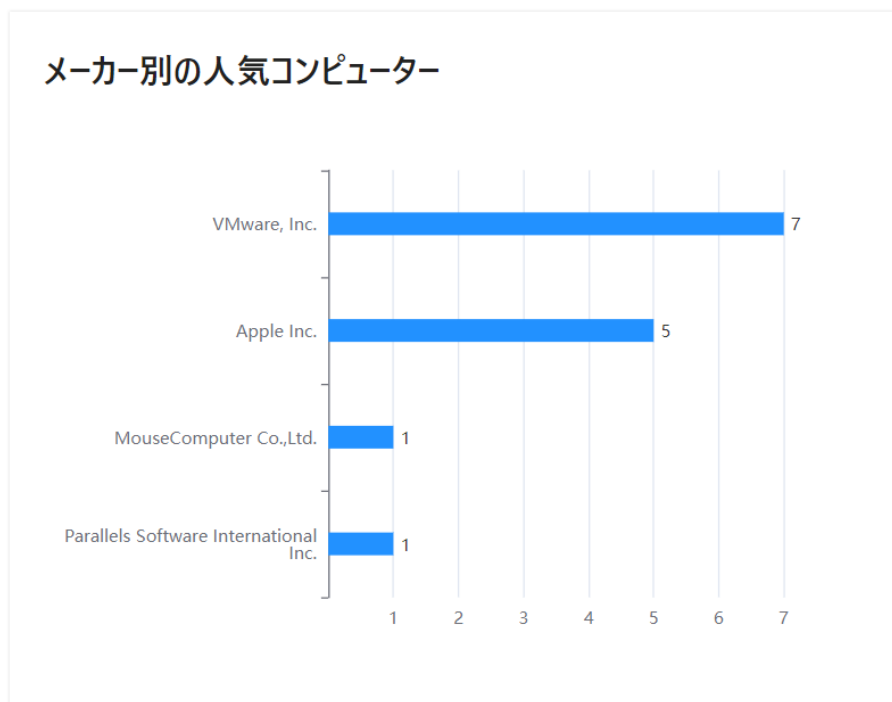
モバイルデバイスにインストールしているクライアントモジュールのバージョンを確認できます。



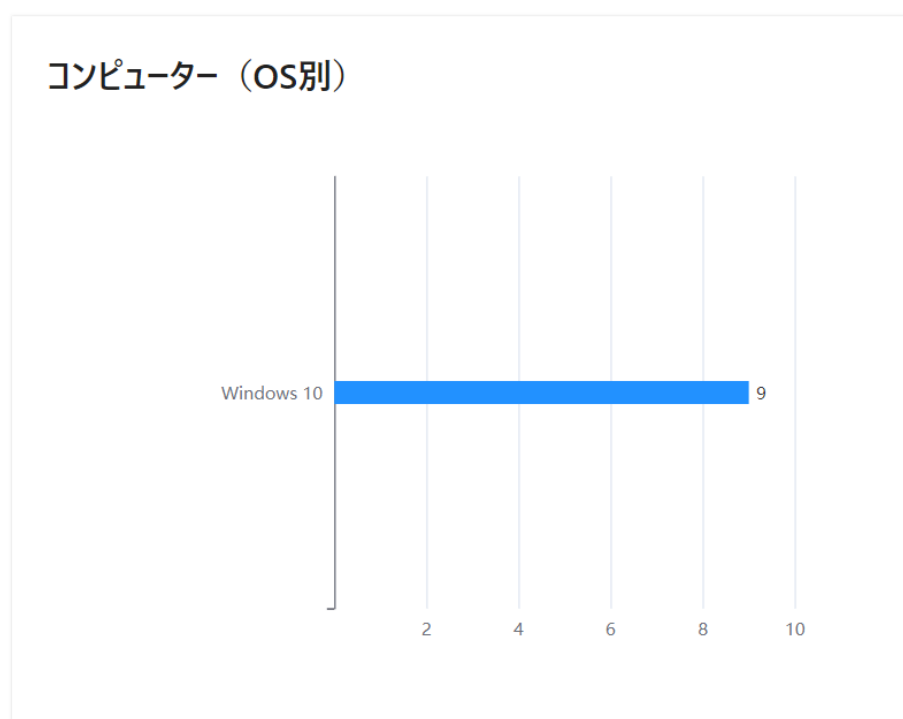
10.11.4. クライアントバージョン別の Connector デバイス



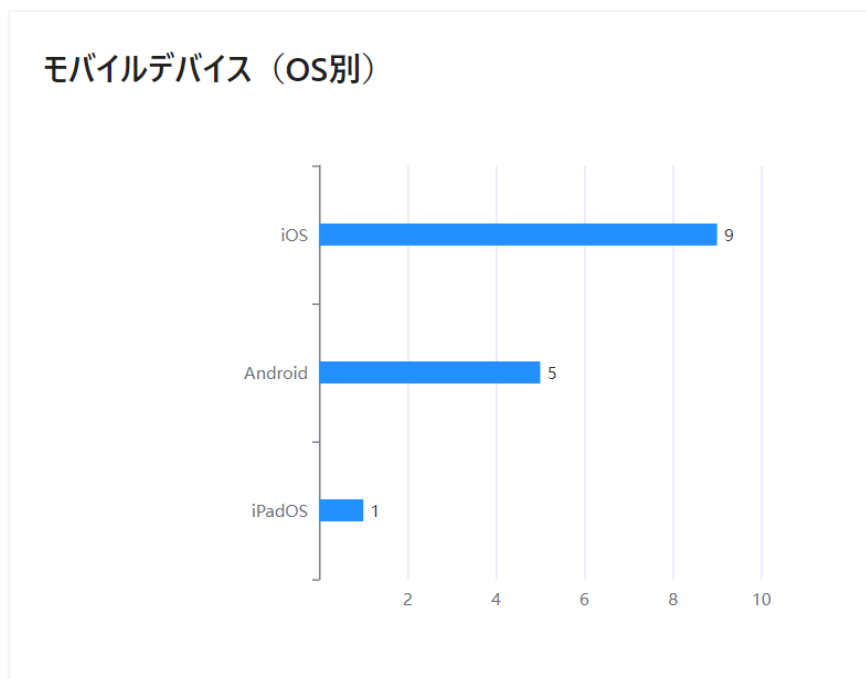
10.11.5. メーカー別の人気コンピュータ



10.11.6. コンピュータ (OS 別)

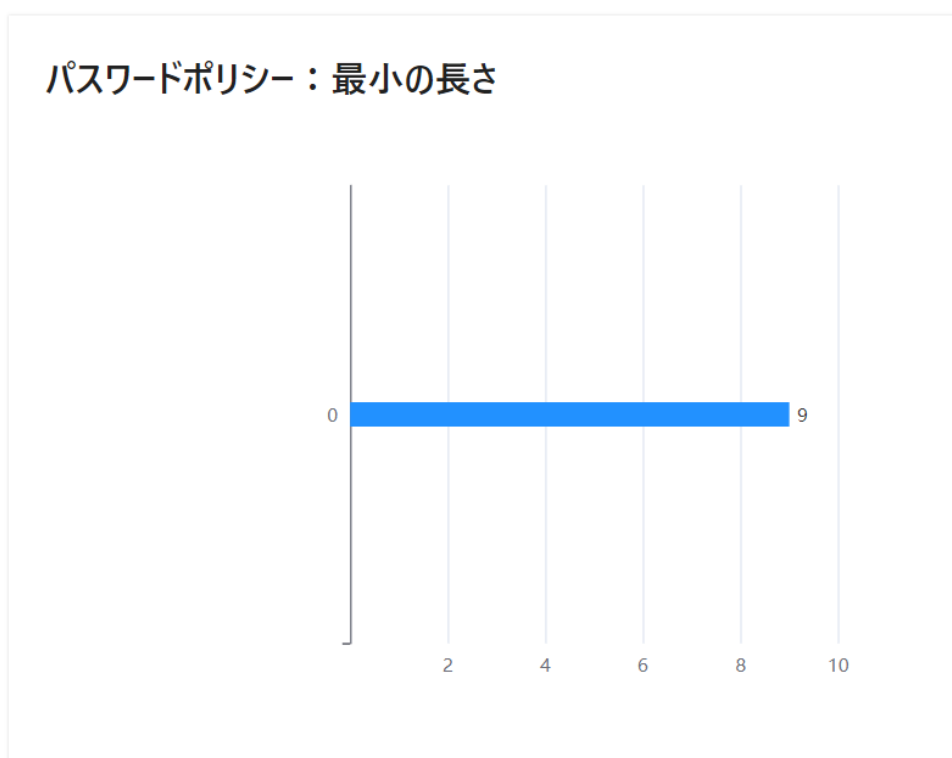


10.11.7. モバイルデバイス（OS 別）

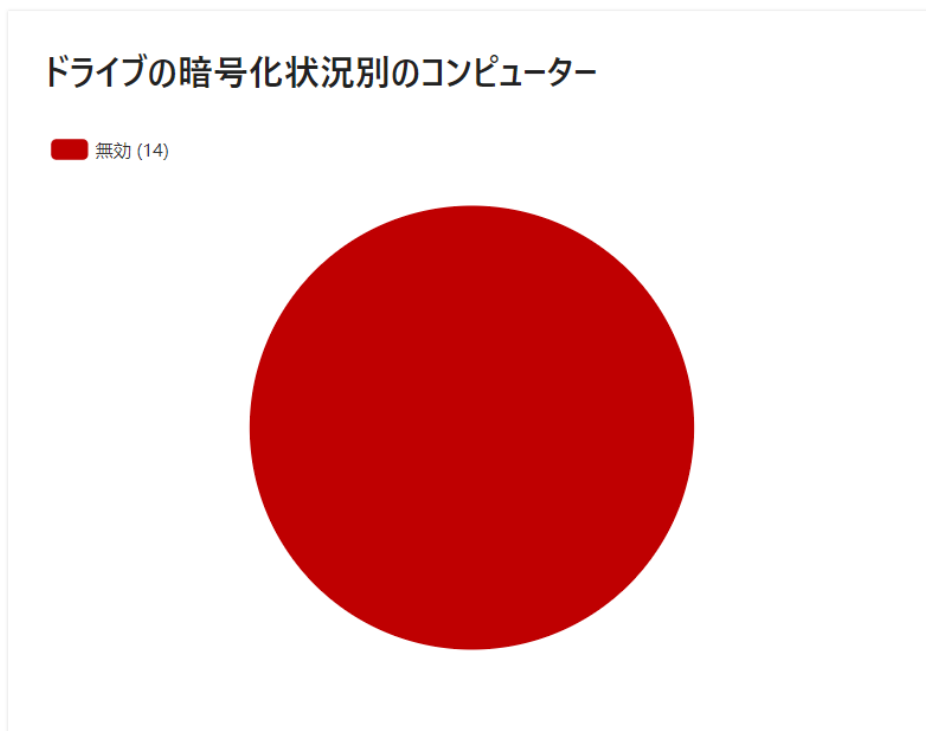


10.11.8. パスワードポリシー：最小の長さ

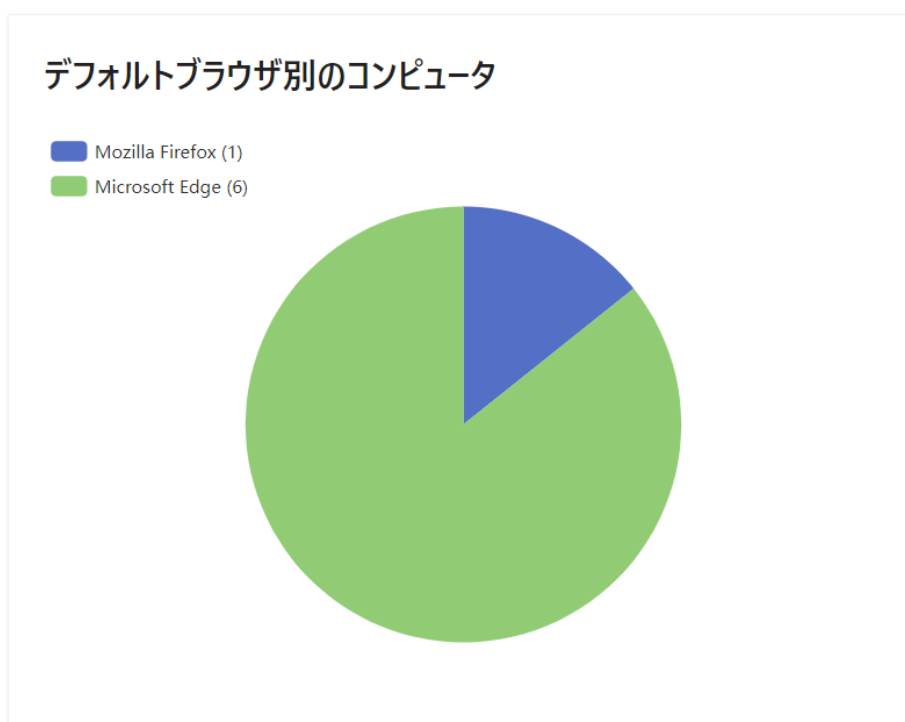
設定されているパスワードの字数と端末の台数



10.11.9. ドライブの暗号化状況別のコンピュータ

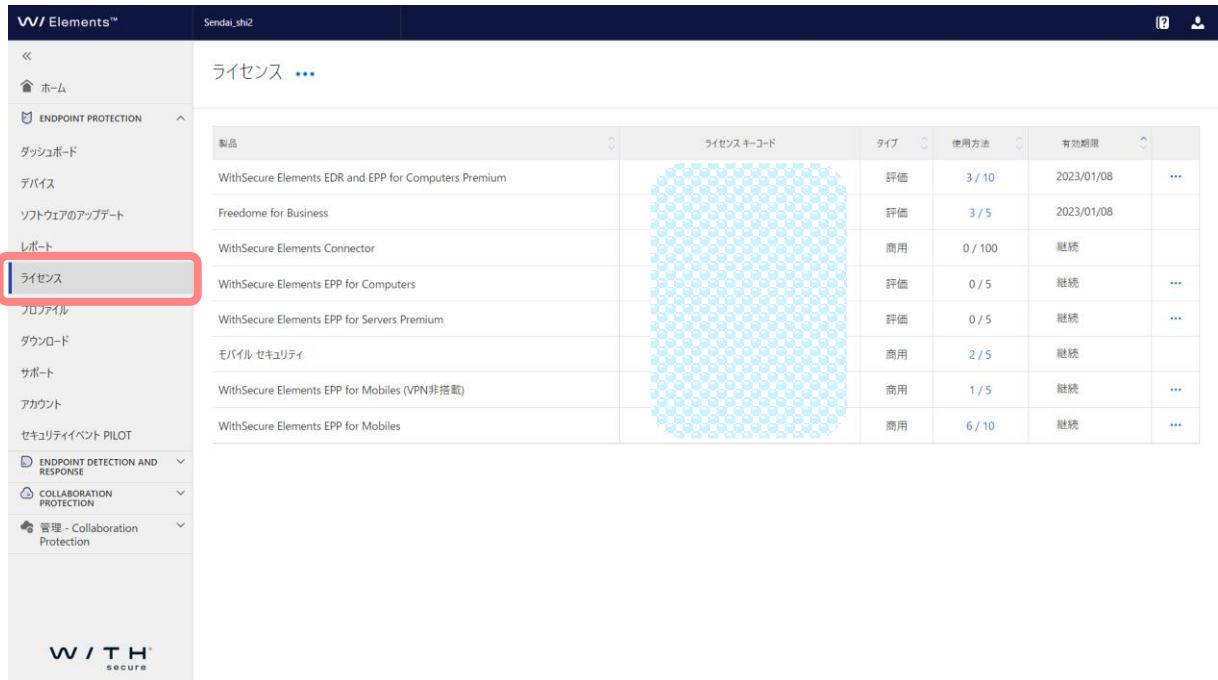


10.11.10. デフォルトブラウザ別のコンピュータ



11. ライセンス

[ライセンス] ボタンをクリックすると、以下の画面が表示されます。



アクションメニュー

項目名	内容
ライセンスキーコードを追加	キーコードを入力することで追加できます

12. プロファイル

画面の左に表示されるメニューから[プロファイル] ボタンをクリックすると、以下の画面が表示されます。

12.1. プロファイルとは？

プロファイルとは、Elements EPP クライアント用のセキュリティ設定のセットです。Elements Security Center から各 Elements EPP クライアントへプロファイルを適用することにより、設定を一元管理できます。

The screenshot shows the 'Profiles' page in the Elements Security Center. The left sidebar contains a menu with 'プロファイル' (Profiles) highlighted. The main content area shows a table of profiles. The 'Actions' column in the table is highlighted with a red box, and the label '詳細メニュー' (Detailed Menu) is placed below it. The 'Profiles' menu item in the sidebar is also highlighted with a red box, and the label 'タブメニュー' (Tab Menu) is placed next to it.

プロファイル名	ステータス	タイプ	説明	所有者	指定されているコンピュータ	アクション
nagasawa_TEST				Nakadori	0	...
WithSecure™ Laptop (locked) (読み取り専用)			A laptop profile that is locked to prevent users from changing any settings.	システム	0	...
WithSecure™ Laptop (open) (読み取り専用)			A laptop profile that is open for users to change any settings.	システム	0	...
WithSecure™ Office (locked) (読み取り専用)			Office locked for accessing the Internet from a fixed location such as office premises. End users are not allowed to change security settings.	システム	0	...
WithSecure™ Office (open) (読み取り専用)			Office open for accessing the Internet from a fixed location such as office premises. End users are allowed to change security settings.	システム	0	...

12.2.[プロファイル] の基本操作

12.2.1. タブメニュー

タブメニューには、[Windows]、[Windows Server] [Mac]、[Linux] [モバイルデバイス] 「Connector」のタブがあります。それぞれのタブメニューでコンピュータとモバイルデバイスそれぞれのプロファイル設定を確認、設定が行えます。必要に応じてタブを選択してください。

12.2.2. アクションメニュー

[アクションメニュー] をクリックすると、操作メニューが表示されます。



プロフィール アクションメニュー (※ 以下の例は [ワークステーションとサーバ] の場合です)

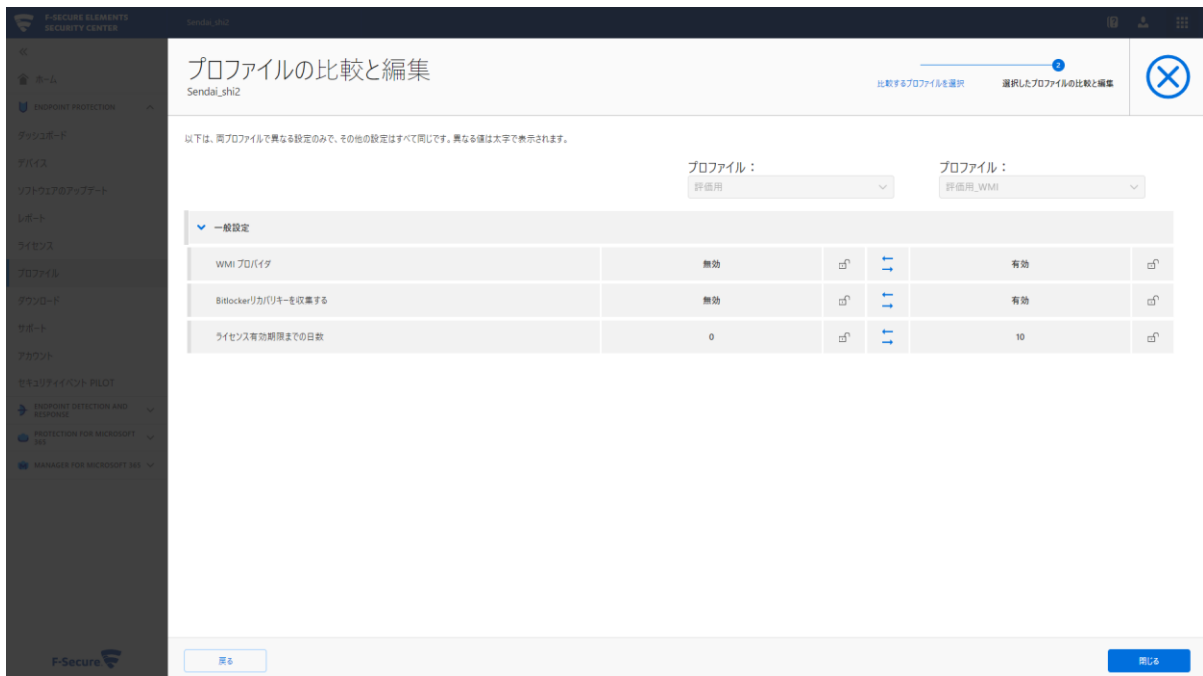
項目名	内容
プロフィールをクローンする	選択中のプロフィールを基に新たなプロフィールを作成します。
プロフィールを削除	選択中のプロフィールを削除します。
プロフィールの比較と編集	選択中のプロフィールと選択可能なプロフィールを比較できます。
「Windows Server」プロフィールにコピーする	選択中のプロフィールをサーバのデフォルトプロフィールにコピーできます。

・プロファイルの比較と編集

1. 比較を行いたいプロファイルの選択



2. 比較を行うプロファイルの異なる設定が表示され、値のコピーを行います。



手順








「←」 右側のプロファイルから左側のプロファイルに値をコピーします

「→」 左側のプロファイルから右側のプロファイルに値をコピーします

12.2.3. 設定アイコンの意味と操作

コンピュータプロファイル画面で表示されるアイコンの意味と操作方法は以下の通りです。

プロファイルアイコン

アイコン	意味
	ヘルプを表示
	設定可能なプロファイルのロック状態、ユーザによる変更を拒否した状態です。
	設定可能なプロファイルのロック解除状態、ユーザによる変更を許可した状態です。
	設定可能なプロファイルの無効状態
	設定可能なプロファイルの有効状態

12.3. 基本のプロファイル

各タブ内には基本となるプロファイルが複数用意されています。これらの基本のプロファイルはグレーアウトして表示されており、この**基本のプロファイルを編集することはできません**。プロファイルを編集してご利用になられる場合には、アクションメニューから「プロファイルをクローンする」を選択して、プロファイル作成する事が可能です。

基本のプロファイル (※ 以下の例は [ワークステーション] の場合です)

項目名	概要	内容
WithSecure™ Laptop (locked)(読み取り専用)	ノート PC (ロック)	モバイル環境での利用が想定されるノート PC 向けのプロファイルです。
WithSecure™ Laptop (open)(読み取り専用)	ノート PC (開放)	モバイル環境での利用が想定されるノート PC 向けのプロファイルです。
WithSecure™ Office (locked)(読み取り専用)	オフィス (ロック)	オフィス内で使用される PC 向けのプロファイルです。
WithSecure™ Office (open) (読み取り専用)	オフィス (開放)	オフィス内で使用される PC 向けのプロファイルです。

※Elements EPP クライアントへのプロファイル適用方法は、「6.5 プロファイルを指定する」を参照してください。

12.4. 設定値のロックとは？

設定値のロックの設定は、設定項目毎に設けられおり、各設定について Elements EPP クライアントによる変更の可否を設定します。

プロファイル上では、錠前マークでロックの設定状態が表現されています。



ロック解除



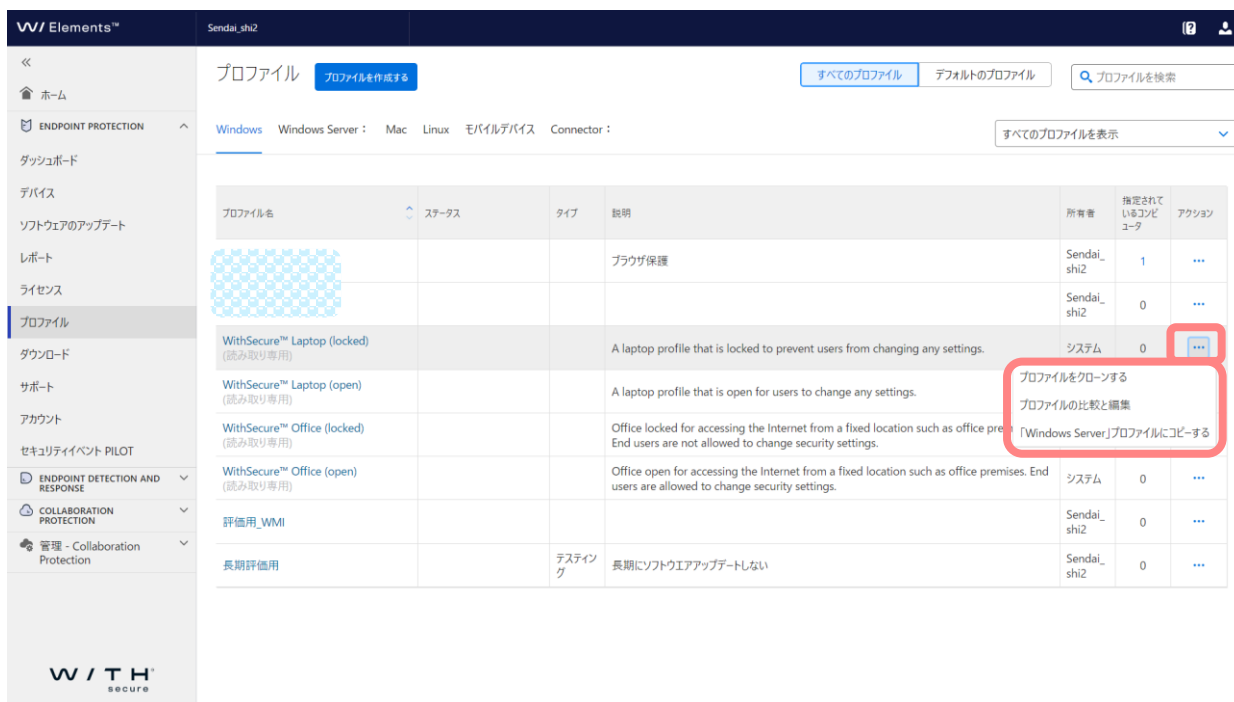
ロック

錠前が閉まっているマークの設定項目は、「ロック」されており、Elements EPP クライアントにて、この設定項目の値を変更することはできません。錠前が開いているマークは「開放（ロック解除）」されており、Elements EPP クライアント側にてこの設定項目の変更が可能です。

※「開放」状態の設定項目は、ローカルで変更されることを想定しているため、ローカルの設定が優先されます。つまり、プロファイルをコンピュータに適用した際に、「開放」状態の設定項目の値はローカルには反映されません。

12.5. プロファイルの作成

独自の設定値からなるカスタムプロファイルを作成することができます。基本のプロファイルでは自社の用途に合わない場合等などに使用します。



- ①プロファイル一覧から基本としたいプロファイルの [アクション] をクリックします。
- ②[プロファイルをクローンする]または [「Windows Server」プロファイルにコピーする] を選択します。
- ③[プロファイル名] と [説明] を入力し、[ラベル] を選択後、[保存して発行] ボタンを押すとプロファイル

Windowsのプロファイル
Sendai_shi

プロフィールID: 12465

...
✕

プロフィール名

説明

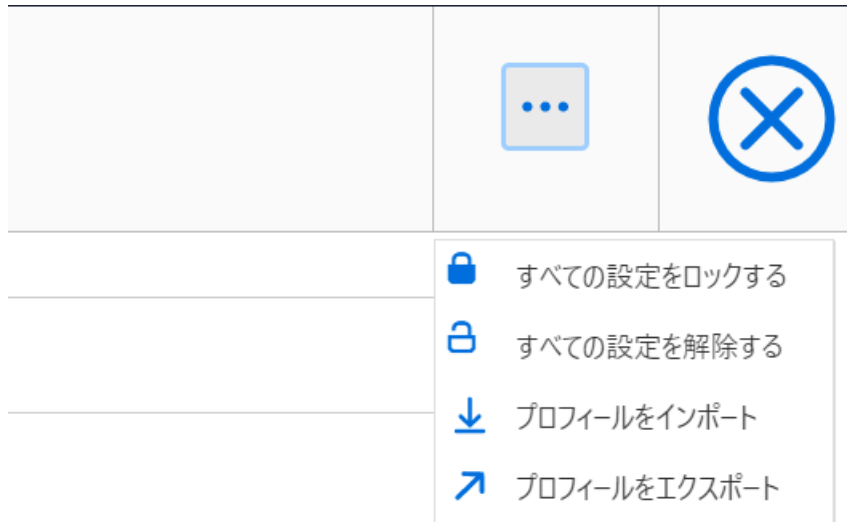
ラベル

ルが作成されます。

このプロファイルに基いて新しいプロファイルを作成する

項目名	内容
プロファイル名	プロファイルの名前を入力します。日本語も入力可能です。必須入力項目です。
説明	プロファイルの説明文です。任意のテキストを入力できます。日本語も入力可

	能です。
ラベル	作成するプロファイルのラベルを選択できます。



12.5.1. アクションメニュー

項目名	内容
すべての設定をロックする	プロファイル内のすべての設定をロックする
すべての設定を解除する	プロファイル内のすべての設定を解除する
プロフィールをインポート	json 形式のプロファイルをインポートする
プロフィールをエクスポート	プロフィールを json 形式にエクスポートする

12.6. コンピュータプロファイル (Windows)

以下の表では、Elements EPP for Computers のプロファイルで設定可能な設定項目について説明します。

12.6.1. 一般設定

The screenshot shows the 'General Settings' (一般設定) section of the Windows security settings. The left sidebar has '一般設定' highlighted. The main area contains various settings with their current states and icons for locking or unlocking them.

設定項目	説明	状態	ロックアイコン
ウイルスのリアルタイムスキャン	クライアント ソフトウェアを誰よりも早く利用する	オフ	なし
マニュアル スキャン	クライアントにユーザーフェースを表示する	オン	なし
ブラウザ保護	自動更新	オン	なし
ファイアウォール	手動で定義されたプロキシアドレス	入力欄	ロック
ソフトウェア アップデート	HTTP プロキシを使用	ユーザーブラウザの設定を検出	ロック
デバイス制御	HTTPSを使用してアップデートをダウンロードする	オフ	ロック
自動化されたタスク	HTTPSを使用してアップデートをダウンロードする	オフ	ロック
ネットワーク場所の設定	直接接続ではなく、プロキシを使用する	オフ	ロック
PREMIUM	プロキシの設定を無視	オフ	ロック
データガード	F-Secure Elements Connector	入力欄	ロック
アプリケーション制御	クライアントに.NETの管理を許可する	オン	ロック
	すべてのセキュリティスキャンからファイル/フォルダを除外する		
	ここで指定したフォルダ、ファイル、SHA-1チェックサムは、すべてのセキュリティスキャンと対策から除外されているため、F-Secure が提供するセキュリティ機能から除外になります。指定したフォルダ内のサブフォルダも含まれます。重要: この設定はスキャンから絶対に除外しなければならないファイルまたはフォルダに対してのみ使用してください。たとえば、C:* をスキャンの対象から除外すると、デフォルトのシステムドライブ全体とその中のすべてのフォルダ、サブフォルダ、およびファイルがすべてのセキュリティ対策から除外されます。 例: C:\Program Files (x86)\Microsoft Office\root\Office16\OUTLOOK.EXE C:\Program Files (x86)\Microsoft Office C:\Program Files\Microsoft 3395856ce812b7382dee72602f798b642f14140		解除
	例外を追加		ロック

項目名	内容
クライアント ソフトウェアを誰よりも早く利用する	クライアント ソフトウェアを一般リリースよりも早く利用できます
クライアントにユーザーインターフェイスを表示する	クライアント端末にアイコンを表示します

自動更新

項目名	内容
HTTP プロキシを使用	すべての製品の接続は、HTTP プロキシを経由します。HTTP プロキシに到達できない場合、コンポーネントは直接接続を行うようになります。これは、Endpoint Detection and Responseのエージェントにも適用します。
手動で定義されたプロキシアドレス	このアドレスは、[HTTP プロキシを使用する] が「リモート管理」に設定されている場合に使用されます。
プロキシを介した強制接続	直接接続の代わりにプロキシ接続を使用します。
プロキシの設定を隠す	ローカル ユーザ設定インターフェイスでプロキシの設定パネルを非表示にします。
HTTPS を使用してアップデートをダウンロードする	HTTPS を使用してアップデートをダウンロードすると、プライバシーが向上し、特定の規定に準拠します。
WithSecure™ Elements Connector	WithSecure™ Elements Connector を使用している場合、そのアドレスを指定します。
クライアントに.NET の管理を許可する	.NET 4.7.2 を使用してユーザインターフェイスを表示します。

すべてのセキュリティスキャンからファイル/フォルダを除外する

項目名	内容
パス	スキャンから除外されるファイル/フォルダを指定します。
クライアントからの除外を非表示にする	クライアントからの除外を非表示にします。
通知を表示する	再起動の要求、検出された脅威に関する情報、エラー通知など、どのユーザがクライアント通知を表示できるかを選択できます。
一時ファイルの最大サイズ	スキャン中にスキンプラットフォームが一時ファイルを保存するために使用できるディスク容量の最大値。

連携

項目名	内容
-----	----

WMI プロバイダ	WMI プロバイダを有効または無効にします。
Bitlocker リカバリキーを収集する	Bitlocker リカバリキーを収集する場合は、この設定をオンにします。
EDR センサーを有効にする	この設定は、EDR センサーを制御するために使用します（EDR のサブスクリプションがあるデバイスのみ使用可能）
アドバンスド・レスポンス	EDRのアドバンスド・レスポンス・モジュールを有効にする場合は、この設定をオンにしてください。

隔離保存

項目名	内容
ユーザがブロックおよび隔離されたアイテムを解放できるようにする	ユーザは隔離されたアイテムを解放し、ブロックされたアイテムを許可できます。
ブロックまたは隔離されたアイテムを開放するためのパスワード（オプション）	コンピュータのユーザへのパスワードを提供
古い隔離アイテムを自動的に削除する	構成された時間が経過した際に隔離したアイテムが削除されます。
アイテムを隔離する日数	値を 1～1095 日で設定

ライセンスの失効

項目名	内容
通知を表示する	ユーザにはライセンスの有効期限に関連する通知が表示されます
ライセンス有効期限までの日数	通知の表示を開始するためのライセンス期限の日数です。
ライセンスの有効期限に関するカスタマイズされたメッセージ	ユーザに表示するメッセージ。

改ざん防止

項目名	内容
リソース保護	有効にすると、WithSecure サービス、プロセス、ファイル、およびレジストリエントリを制御できなくなります。

ユーザがセキュリティ機能を無効にすることを許可

項目名	内容
製品のアンインストールをユーザに許可	ユーザが製品のアンインストールが可能となります
ユーザがセキュリティ機能を無効にすることを許可	ユーザは WithSecure のセキュリティ機能を無効にすることができます。

パスワード	ユーザに設定したパスワードの入力を求めます。
-------	------------------------

改ざん保護イベントを除外する

項目名	内容
イベントタイプ/アプリケーション パス	特定のアプリケーションによる改ざん保護イベントを除外

12.6.2. ウイルスのリアルタイム スキャン

ウイルスのリアルタイム スキャン

項目名	内容	有効/無効	ロック
ウイルスのリアルタイム スキャン	ウイルスのリアルタイム スキャン	<input checked="" type="checkbox"/>	🔓
マニユアル スキャン	マルウェア対策スキャン インターフェース (AMSI)	<input checked="" type="checkbox"/>	🔓
ブランチ保護	▼ ファイル スキャン		
ファイアウォール	スキャンするファイル	指定した拡張子のファイルのみ	🔓
ソフトウェア アップデータ	感染時の処理を自動的に行う	<input type="checkbox"/>	🔓
デバイス制御	感染時の処理	隔離保存	🔓
自動化されたタスク	リスクウェアに対するアクション	ブロック	🔓
ネットワーク場所の設定	スパイクウェアに対するアクション	隔離保存	🔓
PREMIUM	Hosts ファイルの保護	<input checked="" type="checkbox"/>	🔓
データガード	ネットワーク ドライブをスキャンする	<input checked="" type="checkbox"/>	🔓
アプリケーション制御	ネットワーク ドライブのスキャンモード	実行時にスキャン	🔓
	次の拡張子のファイルはスキャンしない	<input type="checkbox"/>	🔓
	除外拡張子		🔓
	F-Secure Security Cloud を使用する	<input checked="" type="checkbox"/>	🔓
	▼ 除外したオブジェクト	<input type="checkbox"/>	🔓

項目名	内容
ウイルスのリアルタイム スキャン	リアルタイム スキャンの有効/無効を設定します。
マルウェア対策スキャン インターフェース (AMSI)	マルウェア対策スキャン インターフェース (AMSI) の統合

ファイル スキャン

項目名	内容	
スキャンするファイル	「すべてのファイル」、「次の拡張子のファイル」のいずれかを選択します。	
	すべてのファイル	すべてのファイルをリアルタイム スキャンします。
	次の拡張子のファイル	「対象拡張子」に登録されている拡張子のファイルを対象にスキャンします。

感染時の処理を自動的に行う	本設定を「有効」にした場合、「感染時の処理」がグレーアウトし無効化され、マルウェア感染時に最適な処理を自動的にを行います。「無効」にした場合は、下の「感染時の処理」がアクティブになり、「感染時の処理」で設定された内容に従って処理されます。	
感染時の処理	リアルタイム保護でウイルス検知が発生した場合の処理方法を指定します。「感染時の処理を自動的に行う」を「有効」にしている場合は無効化されます。	
	名前の変更	検知したファイルに対し、自動的に名前（拡張子）変更処理を行います。
	削除	検知したファイルに対し、自動的に削除処理を行います。削除したファイルは復旧できなくなります。
	駆除	検知したファイルに対し、自動的に駆除処理を行います。駆除できない場合は、名前（拡張子）変更処理を行います。
	隔離保存	検知したファイルに対し、自動的に検疫処理を行います。検疫されたファイルは別のディレクトリに隔離保存されます。
	スキャン後に確認	検知時にユーザが処理を指定します。
	ブロック	検知したファイルをブロックします
リスクウェアに対するアクション	削除/隔離保存/スキャン後に確認/ブロック	
スパイウェアに対するアクション	削除/隔離保存/スキャン後に確認/ブロック	
Hosts ファイルの保護	有効な場合、Hosts ファイルを保護します。	
ネットワークドライブをスキャンする	ネットワークドライブのスキャンの有効/無効を設定します。	
ネットワークドライブのスキャンモード	ネットワークドライブのリアルタイム スキャンモードを選択します。	
次の拡張子のファイルはスキャンしない	特定の拡張子を持つファイルをスキャンの対象から除外します。「除外拡張子」欄に除外したい拡張子を記入します。	
除外拡張子	リアルタイム スキャンから除外するファイル拡張子のリストを登録します。複数の拡張子を記入する場合は、拡張子間に半角スペースを置きます。	
WithSecure™ Security Cloud を使用する	WithSecure™ Security Cloud の使用	

除外したオブジェクト

項目名	内容
-----	----

除外したオブジェクト	特定のファイルまたはディレクトリをリアルタイム スキャンの対象から除外する機能の有効・無効を設定します。	
	オブジェクト	除外対象とするファイルまたはフォルダを指定します。[オブジェクトを追加]をクリックするとオブジェクトの追加が行えます。

除外しているプロセス

項目名	内容	
除外しているプロセス	特定のプロセスをリアルタイム スキャンの対象から除外する機能の有効・無効を設定します。	
	プロセス	除外する対象のプロセスを指定します。除外するプロセスのフルパスを入力する必要があります。
すべてのリスクウェアを除外する	すべてのリスクウェアのスキャンをスキップできます。	
すべてのスパイウェアを除外する	すべてのスパイウェアのスキャンをスキップします。	

除外されたリスクウェア/スパイウェア

項目名	内容
除外されたリスクウェア/スパイウェア	スパイウェアまたはリスクウェアをリアルタイム スキャンから除外します。

Web スキャン

項目名	内容	
Web スキャン	有効な場合、Web からダウンロードするファイルを受信前にスキャンします。	
	Web トラフィックをスキャンして、検出したマルウェアを削除する	スキャンする対象を選択します。

Web スキャンから除外されているアプリケーション

項目名	内容
Web スキャンから除外されているアプリケーション	Web スキャンから特定のアプリケーションを除外する場合、有効に設定します。

	アプリケーションを追加	除外するアプリケーションの SHA-1 ハッシュ値を追加します。
--	-------------	----------------------------------

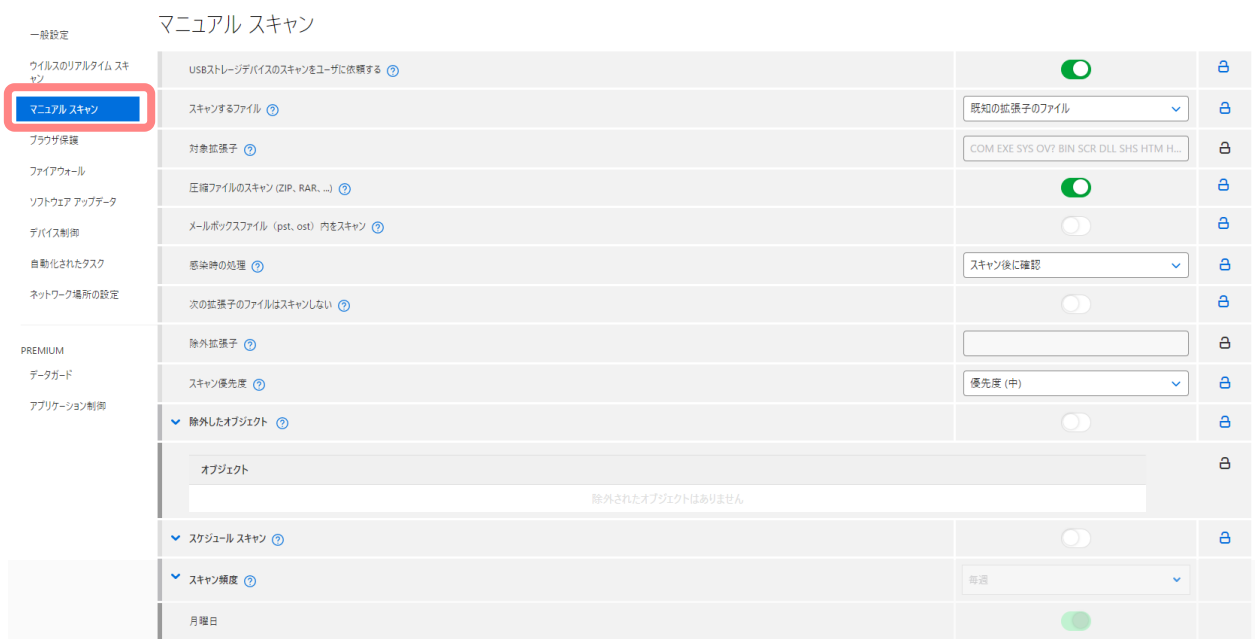
ディープガード

項目名	内容
ディープガード	WithSecure の振る舞い検知機能であるディープガードの有効/無効を設定できます。
まれで疑わしいファイルをブロックする	ディープガードがまれで疑わしいファイルをブロックできるようにします。

ディープガードの保護ルール

項目名	内容	
ディープガードの保護ルール	ディープガードからアプリケーションを除外する場合などに有効にします。	
	ルールを追加	ルールを登録したいアプリケーションの SHA-1 ハッシュを追加します。信頼済みがはいの場合常に実行され、いいえの場合常に実行を拒否されます。

12.6.3. マニュアルスキャン



項目名	内容	
USB ストレージを接続したときの動作	接続する USB ストレージデバイスをスキャンするようにユーザーに確認できます。	
	何もしない	スキャンを実行しません
	USB のスキャンをユーザーに依頼する	スキャンをユーザーに確認します
	USB のサイレントスキャン	スキャンをユーザーに確認せず実行します
	USB をスキャンし、結果をユーザーに表示	スキャン後、結果をユーザーに表示します
スキャンするファイル	「すべてのファイル」、「次の拡張子のファイル」のいずれかを選択します。	
	すべてのファイル	すべてのファイルをマニュアルスキャンしま

		す。
	次の拡張子のファイル	登録されている拡張子のファイルをマニュアルスキャンします。定義されている拡張子は、「対象拡張子」で確認できます。
	既知の拡張子のファイル	一般的に使用される拡張子をスキャンします。
対象拡張子	スキャンするファイルを次の拡張子のファイルに設定した場合に、検査対象となる拡張子を登録します。	
圧縮ファイルのスキャン (zip、rar、...)	「有効」にすると圧縮ファイルもマニュアルスキャンします。	
メールボックスファイル (pst、ost) 内をスキャン	メールボックスファイルの内部にあるファイルをスキャンします。	
感染時の処理	マニュアルスキャンでウイルス検知、およびスパイウェア検知が発生した場合の処理方法を指定します。	
	消去	検知したファイルに対し、自動的に駆除処理を行います。駆除できない場合は、名前（拡張子）変更処理を行います。
	削除	検知したファイルに対し、自動的に削除処理を行います。削除したファイルは復旧できなくなります。
	名前の変更	検知したファイルに対し、自動的に名前（拡張子）変更処理を行います。
	スキャン後に確認	マルウェア検知が発生すると「駆除ウィザード」が表示されます。ユーザは駆除ウィザードに従って処理を選択します。
	隔離保存	検知したファイルに対し、自動的に検疫処理を行います。検疫されたファイルは別のディレクトリに隔離保存されます。
次の拡張子のファイルはスキャンしない	「有効」にすると特定の拡張子を持つファイルをスキャンの対象から除外します。「対象外とする拡張子」欄に除外したい拡張子を記入します。	
除外拡張子	マニュアルスキャンから除外するファイル拡張子のリストを登録します。複数の拡張子を記入する場合は、拡張子間に半角スペースを置きます。	
スキャン優先度	スキャンの優先度を [優先度 (中)] と [バックグラウンド] から選択します。[バックグラウンド] にすることで、スキャンに割り当てられる CPU のリソースの優先度が下げられます。	

除外したオブジェクト

項目名	内容
-----	----

除外したオブジェクト	特定のファイルまたはディレクトリをマニュアルスキャンの対象から除外する機能の有効・無効を設定します。	
	オブジェクト	除外対象とするファイルまたはフォルダを指定します。[オブジェクトを追加]をクリックするとオブジェクトの追加が行えます。

スケジュールスキャン

項目名	内容
スケジュールスキャン	有効な場合、スケジュールスキャンを設定できます。

スキャン頻度

項目名	内容
スキャン頻度	スキャン頻度を、日次か週次か月次で指定します。週次の場合は、スキャンを実施する曜日を指定します。月次の場合は、スキャンを実施する日を三日まで指定します。

スキャンを開始

項目名	内容
スキャンを開始	スキャンの開始時刻を、時間またはアイドル時間で指定します。
次のシステム アイドル時間が経過したらスキャンを開始	コンピュータで指定したアイドル時間が経過した時点で開始されます。

スケジュールスキャンのオプション

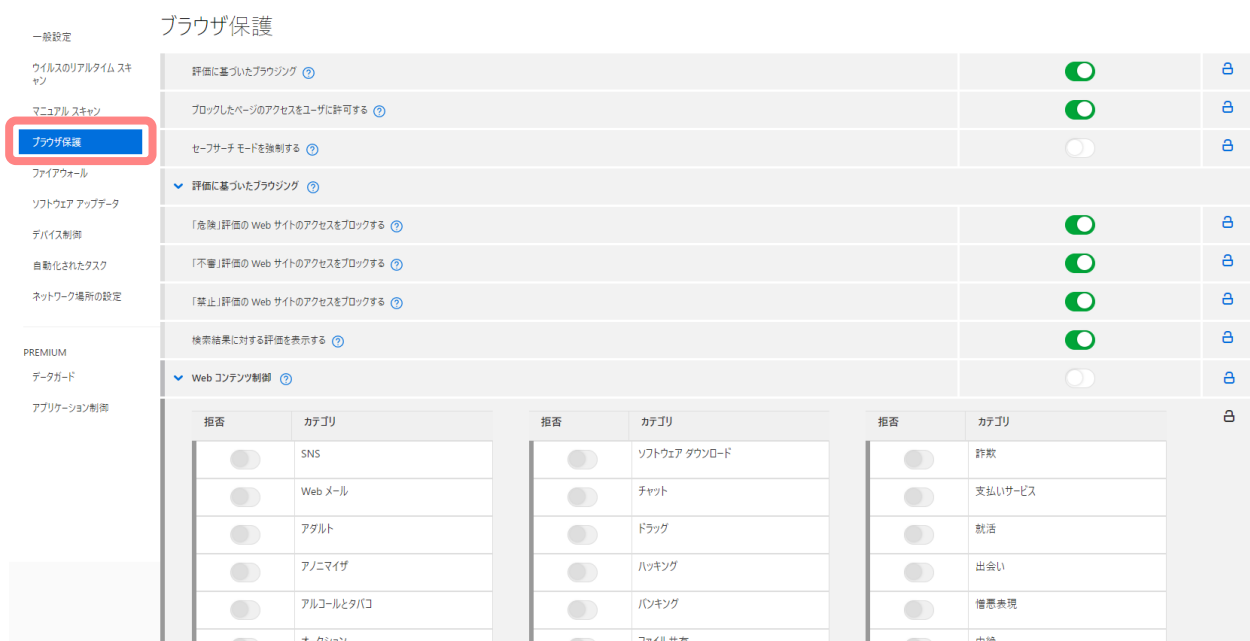
項目名	内容
スキャンを低い優先度で実行する	有効な場合、スケジュールスキャンに割り当てられる CPU のリソースの優先度が下げられます。
指定ファイルのみスキャン(高速)	有効な場合、主要なファイルのみをスキャンし、短時間でスキャンを終了します。
圧縮ファイルをスキャン(低速)	有効な場合、圧縮ファイルのスキャンを行うため、スキャンが要する時間が長くなります。
通知をユーザに表示する	スケジュールスキャンの通知を表示します

除外するオブジェクトの指定では、「?」と「*」の正規表現が利用可能です。正規表現を利用しない場合は、完全一致です。フォルダ単位の指定を行う場合は、最後に「¥ (バックスラッシュ)」の記載をお願いします。

リアルタイム スキャンの除外設定でワイルドカードを使用する場合は、ドライブ名を判断できません。そのため、ワイルドカードを利用した除外設定を行う場合は、ドライブ銘を記載する代わりに、必ず「*¥¥」記載してください。（例：「*¥¥Windows¥system32¥」）

この指定で除外されるスキャンは、振る舞い検知を含まない（パターンマッチングによる）スキャンからの除外設定になります。そのため、振る舞い検知からも除外を行いたい場合には、「ウイルスのリアルタイム スキャン」→「ディープガードの保護ルール」から、除外するアプリケーションを登録する必要があります。

12.6.4. ブラウザ保護



項目名	内容
評価に基づいたブラウジング	レピュテーションベースのブラウジングをオンにします。
ブロックしたページのアクセスをユーザに許可する	警告ページからブロックされたページに進めることを許可します。
セーフサーチ モードを強制する	検索結果フィルタを有効にして、アダルトコンテンツを非表示にすることができます。

評価に基づいたブラウジング

項目名	内容
「危険」評価の Web サイトのアクセスをブロックする	有効な場合、危険と評価された Web サイトへのアクセスがブロックされます。
「不審」評価の Web サイトのアクセスをブロックする	有効な場合、不審と評価された Web サイトへのアクセスがブロックされます。
「禁止」評価の Web サイトのアクセスをブロックする	有効な場合、危険と評価された Web サイトへのアクセスがブロックされます。
検索結果に対する評価を表示する	有効な場合、サーチエンジンの検索結果に評価を表示します。

Web コンテンツ制御

項目名	内容
Web コンテンツ制御	「有効」にすると特定のカテゴリに関するサイトのアクセスを禁止します。禁止するカテゴリを有効に設定してください。
許可されたサイトを除くすべてをブロックする	許可されたサイトのリストにあるサイトを除くすべてのサイトへのアクセスをブロックします。

コンテンツタイプのフィルタリング

項目名	内容
コンテンツタイプのフィルタリング	「有効」にすると、サイトの安全性の評価が「不審」または「不明」なサイトのコンテンツのタイプ別にフィルタリング設定が行えます。 コンテンツタイプまたはファイル名でフィルタリング対象が設定されています。 各フィルタリング項目について、有効/無効を設定することができます。

Web サイトの例外

項目名	内容	
Web サイトの例外	有効な場合、許可したサイトには常に接続が許可され、拒否したサイトには常に接続が拒否されます。	
サイト	許可したサイト	接続を許可するサイトを追加します。
	拒否したサイト	接続を拒否するサイトを追加します。

接続制御

項目名	内容	
接続制御	「有効」にすると、銀行サイトと個人情報保護されているサイトはセキュア ブラウジング モードで処理されます。	
有効なインターネット接続を中断しない	有効な場合、接続制御が動作時に有効だったインターネット接続が維持されます。	
完了したらクリップボードを消去する	セッション終了後にクリップボードを消去します。	
ブロックコマンドラインとスクリプトツール	ネットワーク接続のコマンドラインツールとスクリプトツールをブロックできます。	
リモートアクセスをブロックする	デバイスへのリモートアクセスをブロックすることができます。	
接続制御のサイトを追加	機密データを含み、セキュア ブラウジング モードの有効時にのみアクセスが可能なサイトの一覧が登録できます。[サイトを追加] をクリックすると登録できます。	
	有効	有効・無効を設定します。「有効」にするとセキュアブラウジングモードでのみアクセス可能となります。
	アドレス	サイトの URL を入力します。

「信頼済みのサイト」「拒否したサイト」の登録に正規表現は利用できません。ホスト名による登録となり（パスまで記載された場合、パスは無視されます）、前方一致になります。「http」などのプロトコルの記載は必要ありません。

12.6.5. ファイアウォール

Windows Firewall の設定。Windows ファイアウォールが有効の場合、システムが Windows ファイアウォールのユーザ ルールを使用します。F-Secure ファイアウォール ルールは Windows ファイアウォールのユーザ ルールの上に追加のセキュリティを提供します。

一般設定

ファイアウォール

Windows Firewall の設定。Windows ファイアウォールが有効の場合、システムが Windows ファイアウォールのユーザ ルールを使用します。F-Secure ファイアウォール ルールは Windows ファイアウォールのユーザ ルールの上に追加のセキュリティを提供します。

▼ 一般設定 ⓘ

F-Secure ファイアウォール プロファイル
これらのルールは、Windows ファイアウォールのユーザ ルールの上に追加のセキュリティを提供します。

Windows ファイアウォールを使用
この設定を有効にすると、Windows ファイアウォールのユーザ ルールとネットワーク ルールがデバイスに適用されます。ドメイン ルールはこれらのルールよりも優先されることに注意してください。

プロファイルを編集する
プロファイルの一次および二次設定を行い、プリセットの F-Secure プロファイル ルールを上書きする新しいルールを作成できます。プリセット ルールを使用せずにすべてのルールを作成する場合、カスタム プロファイルを選択してください。

F-Secureファイアウォールモード ⓘ

F-Secureファイアウォールをオンにする

F-Secure ファイアウォール プロファイルの選択 ⓘ

Normal Workstation

注意：自動プロファイル選択ルールを以下の場所に移動しました。ネットワーク場所の設定。

▲ F-Secure ファイアウォール プロファイル ⓘ

ファイアウォール ルールのマッピング
F-Secure プロファイルは Windows ファイアウォールのユーザ ルールと他のドメイン ルールの上に機能します。

1. F-Secure ファイアウォールの一般設定がまず適用されます。
2. 次に、ファイアウォール ルール テーブルのルールが評価されます。
3. プロファイルで他に一致するルールがない場合にはフォールバック設定が適用されます。

ブロック ルールは許可ルールより優先されます。

一般設定

項目名	内容	
WithSecure™ Firewall モード	WithSecure™ファイアウォールの動作を制御するには、次のいずれかのオプションを選択します。	
	何もしない	WithSecure™ファイアウォールがオフになります
	Windows ファイアウォールをオフ	WithSecure™ファイアウォールが Wi

	にする	Windows ファイアウォールをオフにします。
	WithSecure™ファイアウォールをオンにする	WithSecure™ファイアウォールは Windows ファイアウォールをオンにし、構成されたプロファイルから追加のルールと設定を適用します。
WithSecure™ ファイアウォールプロファイルの選択	Windows のファイアウォールのルールに追加する WithSecure™ファイアウォールのルールを選択します。ファイアウォール ルールの内容については、「ファイアウォール ルールテーブル」で確認できます。	

WithSecure™ ファイアウォールプロファイル

項目名	内容
変更するプロファイルを選択してください	プロファイル エディタで変更するファイアウォールプロファイルを選択します。
すべての受信接続をブロック	クライアントに対する全ての受信通信の接続リクエストをブロックします。
ユニキャスト レスポンスをマルチキャストに許可	この設定が有効の場合、マルチキャストまたはブロードキャスト メッセージに対するユニキャストのレスポンスがコンピュータに受信されることを阻止します。

フェイルバックの設定

項目名	内容
不明な受信接続を許可	この設定を有効にすると、コンピュータに対する不明な受信接続のリクエストが許可されます。通常、この設定の無効を推奨します。
不明な送信接続を許可	この設定を有効にすると、コンピュータに対する不明な送信接続のリクエストが許可されます。通常、この設定の無効を推奨します。
ファイアウォールが新しいアプリをブロックしたときに通知	この設定を有効にした場合、新しいアプリの発信接続がブロックされた際にエンドユーザーに通知が送られます。

WithSecure™プロファイルのファイアウォール ルール : Normal Workstation

項目名	内容
WithSecure™プロファイルのファイアウォールルール Normal Workstation	表示されているファイアウォール ルールを変更できます。WithSecure™プロファイル ルールの上にルールを追加できます。ブロック ルールは許可ルールの前に評価されます。ルールの順序は評価に影響しません。 ルールは、通信方向とプロトコルおよびポート番号で構成されます。
他のルールを許可する	他の (WithSecure™によって作成されていない) ファイアウォール ルールを許可します。無効に設定すると、プロファイルの有効時にすべてのルールが無効になり、有効に設定されているときには再び有効になります。

WithSecure™プロファイルのファイアウォール ルール : Network isolation

項目名	内容
WithSecure™プロファイルのファイアウォールルール Network isolation	表示されているファイアウォール ルールを変更できます。WithSecure™プロファイル ルールの上にルールを追加できます。ブロック ルールは許可ルールの前に評価されます。ルールの順序は評価に影響しません。 ルールは、通信方向とプロトコルおよびポート番号で構成されます。
許可されたドメイン	他の (WithSecure™によって作成されていない) ファイアウォール ルールを許可します。無効に設定すると、プロファイルの有効時にすべてのルールが無効になり、有効に設定されているときには再び有効になります。
隔離されたコンピュータに関するカスタマイズされたメッセージ	コンピュータがネットワークから隔離されたときにユーザに表示されるメッセージ。

12.6.6. ソフトウェアアップデート

一般設定	ソフトウェア アップデータ		
ウイルスのリアルタイム スキャン	ソフトウェア アップデータ ?	<input checked="" type="checkbox"/>	?
マニュアル スキャン	ローカル ユーザ インターフェース ?	<input checked="" type="checkbox"/>	?
ブラウザ保護	運用されていないアップデートを自動的にスキャン ?	<input checked="" type="checkbox"/>	?
ファイアウォール	スキャン優先度 ?	標準	?
デバイス制御	<input checked="" type="checkbox"/> 自動インストール ? 注意: 自動インストールの設定を以下の場所に移動しました。 自動化されたタスク 。		
自動化されたタスク	<input checked="" type="checkbox"/> 自動インストールにソフトウェアを含める ? ルールを追加 有効 ルール ... ?		
ネットワーク場所の設定	<input checked="" type="checkbox"/> 自動インストールにソフトウェアを含める ? ルールを追加 有効 ルール ... ?		
PREMIUM			
データガード			
アプリケーション制御			
	システム起動時のスキャン ?	<input type="checkbox"/>	?
	再起動通知ポリシー ?	表示しない	?

項目名	内容
ソフトウェアアップデート	ソフトウェアアップデートの機能の有効/無効を選択できます。「無効」にした場合、Elements EPP の機能によるソフトウェアのアップデートが行われなくなります。

ローカル ユーザ インターフェイス	ソフトウェアアップデートのローカル ユーザ インターフェイスをオンまたはオフにします。
適用されていないアップデートを自動的にスキャン	適用していない更新プログラムの自動スキャンをソフトウェアアップデートをオンにします。
スキャン優先度	スキャンの優先度を設定します。

自動インストール

項目名	内容
自動インストール	「自動化されたタスク」項目を移動されました

自動インストールにソフトウェアを含める

項目名	内容
自動インストールにソフトウェアを含める	ソフトウェアアップデートによって自動的にインストールするソフトウェアの名前を入力します。名前に一致するソフトウェアは、自動的インストールの対象となります。

ソフトウェアを自動インストールから除外

項目名	内容
ソフトウェアを自動インストールから除外	ソフトウェアアップデートによって自動的にインストールさせないソフトウェアの名前を入力します。名前に一致するソフトウェアは、自動インストールの対象外となります。
システム起動時のスキャン	有効な場合、システムの起動時に適用されていないアップデートを常に確認します。
再起動通知ポリシー	再起動通知ポリシーの設定
インストール後に再起動する	アップデートのインストール後に再起動が必要なものについて、「ユーザに確認」と「再起動を強制する」から選べます。
再起動を強制する時間	再起動を強制する場合、何時間後に強制するかを選択します。
アプリケーション実行時のアクション	アプリケーションに適用するアクションを選択します。
インストールをユーザに通知する	有効な場合、アップデートのインストールがユーザに通知されます。
WSUS が使用されている場合、ソフトウェアアップデートと WSUS の両方が Microsoft の更新プログラムをインストールします	有効な場合、WSUS とソフトウェアアップデートの両方で更新がインストールされる場合があります。WSUS を使用している場合、無効に設定することを推奨します。

スキャン結果にアップデートを含める

項目名	内容
スキャン結果にアップデートを含める	ルールに一致するアプリケーションのみをスキャンの結果に追加します。

スキャンからアップデートを除外

項目名	内容
セキュリティに関連しない更新	「有効」にするとセキュリティに関連しない更新をスキャンした結果から除外します。

スキャン結果からアップデートを除外

項目名	内容
スキャン結果からアップデートを除外	ルールに一致するアプリケーションをスキャンの結果に追加しません。

通信

項目名	内容
HTTP プロキシを使用	ソフトウェアのアップデート時に、プロキシを介してアップデートプログラムをダウンロード可能になります。
手動で定義されたプロキシアドレス	ソフトウェアアップデートのリモート管理 HTTP プロキシ アドレスを入力します。
WithSecure™ Elements Connector	WithSecure™ Elements Connector をソフトウェアアップデートで使用するよう設定します。
WithSecure™ Elements Connector	WithSecure™プロキシアドレスを入力します。

12.6.7. デバイス制御

一般設定

ウイルスのリアルタイム スキャン

マニュアル スキャン

ブラウザ保護

ファイアウォール

リモートアクセス

デバイス制御

自動化されたタスク

ネットワーク場所の設定

PREMIUM

データガード

アプリケーション制御

デバイス制御

「デバイス制御」タブでは、ユーザが大容量記憶装置、USB カメラ、プリンタなどの USB デバイスにアクセスする方法に関する制限を設定できます。USB ストレージ デバイスへの書き込みアクセスを禁止したり、実行中の実行ファイルを禁止したり、デバイス グループに基づいて制限を設定することができます。

デバイス制御	<input checked="" type="checkbox"/>	🔒
リムーバブル大容量ストレージデバイス	<input checked="" type="checkbox"/>	🔒
書き込みアクセスを許可	<input checked="" type="checkbox"/>	🔒
実行可能ファイルの実行を許可	<input checked="" type="checkbox"/>	🔒
リムーバブル大容量ストレージデバイスの例外		
ルールを追加		
有効	ハードウェア ID	コメント
例外は定義されていません		
デバイスのフィルタリング ルール		
ルールを追加		
ルール		...
HTREE*ROOT*0		×
ROOT*LEGACY_*		×
SWD*PRINTENUM*		×
STORAGE*VOLUMESNAPSHOT*		×

項目名	内容
デバイス制御	有効な場合、USB デバイスに対するアクセス制御が有効になります。

リムーバブル大容量ストレージデバイス

項目名	内容
書き込みアクセスを許可	有効な場合、USB ストレージデバイスへのファイルの書き込み、変更が許可されます。
実行可能ファイルの実行を許可	有効な場合、USB ストレージデバイス上のファイルの実行が許可されます。

リムーバブル大容量ストレージデバイスの例外

項目名	内容
リムーバブル大容量ストレージデバイスの例外	特定の外部デバイスの実行および書き込み権限を常に許可する

デバイスのフィルタリングルール

項目名	内容
デバイスのフィルタリングルール	デバイスのフィルタリングルールを編集します。

デバイスのアクセスルール

項目名	内容
デバイスのアクセスルール	USB デバイスへのアクセスルールを許可またはブロックで設定します。 USB デバイスは、ハードウェア ID で指定します。USB デバイスのハードウェア ID を確認するには、当該デバイスを接続した Windows PC で、デバイスマネージャでデバイスのプロパティを確認します。

12.6.8. 自動化されたタスク





項目名	内容
自動化されたタスク	自動タスクをオンまたはオフにします
自動化されたタスクのリスト	自動タスクのリストを追加します。


12.6.9. ネットワーク場所の設定

一般設定

ウイルスのリアルタイムスキャン

ネットワーク場所の設定  

マニュアル スキャン

ロケーションとルール 

ブラウザ保護

場所を追加

ファイアウォール

場所は追加されていません

...

ソフトウェア アップデータ

デバイス制御

自動化されたタスク

ネットワーク場所の設定

項目名	内容
ネットワーク場所の設定	作成されたすべての場所とルールをオンまたはオフにできます。
ロケーションとルール	ルールを適用する場所を追加できます。

12.6.10. データガード (Premium)

Premium 設定は WithSecure™ Elements EPP for Computers Premium を搭載したデバイスのみ適用されます。

一般設定

- ウイルスのリアルタイムスキャン
- マニユアル スキャン
- ブラウザ保護
- ファイアウォール
- ソフトウェア アップデータ
- デバイス制御
- 自動化されたタスク
- ネットワーク場所の設定
- データガード
- アプリケーション制御

データガード

「E-Secure データガード」は、高度な動作ルールを活用して、システムに影響を与えようとするマルウェア (ランサムウェアなど) の試みを取締することでデータガード (リアルタイム スキャンタブを参照) を強化するプレミアム機能です。フォルダは自動的に検出され、例外は手動で追加できます。信頼できるアプリケーションはフォルダにアクセスできます。重要: データガードが機能するには、データガードおよびリアルタイム スキャンを有効にする必要があります。

データガードの高度な動作ブロック	<input checked="" type="checkbox"/>	🔒
許可およびレポートモード	<input type="checkbox"/>	🔒
▼ 監視フォルダ		
監視対象のユーザのデータ フォルダを自動的に検出する	<input checked="" type="checkbox"/>	🔒
手動で含まれるフォルダ		
パスを追加		
パス	...	
パスはありません		
手動で除外されるフォルダ		
パスを追加		
パス	...	
パスはありません		
▼ アクセス制御		
信頼済みのアプリケーションを自動的に検出する	<input checked="" type="checkbox"/>	🔒
手動で追加された信頼済みのアプリケーションとフォルダ	<input checked="" type="checkbox"/>	🔒
パスを追加		

項目名	内容
-----	----

データガードの高度な動作ブロック	データガードの高度な動作ルールを有効にします。
許可およびレポートモード	保護されたフォルダを監視し、ブロックされるアクセスを報告します。

監視フォルダ

項目名	内容
監視対象のユーザのデータフォルダを自動的に検出する	この設定を有効にすると、ドキュメント、画像、またはその他のエンド ユーザー コンテンツを含むフォルダが自動的に保護されます。
保護されているフォルダの上部にアイコンを表示する	この設定を有効にすると、データガードで保護されているファイルやフォルダの上にオーバーレイアイコンが表示され、より快適に使用することができます。
手動で含まれるフォルダ	保護対象のフォルダを追加することができます。
手動で除外されるフォルダ	保護対象外のフォルダを追加することができます。

アクセス制御

項目名	内容
アクセス制御	データガードが保護しているファイルやフォルダを変更できるアクセス権をアプリケーションに指定できます。
信頼済みのアプリケーションを自動的に検出する	信頼できるアプリケーションを自動的に検出することができます。
手動で追加された信頼済みのアプリケーションとフォルダ	信頼できる実行可能ファイルと信頼できる実行可能ファイルを含むフォルダを手動で定義することができます。

リスト

項目名	内容
DataGuard リスト	ディープガード保護にリストを追加することができます。

12.6.11. アプリケーション制御 (Premium)

Premium 設定は WithSecure Elements EPP for Computers Premium を搭載したデバイスのみにも適用されます。

一般設定

ウイルスのリアルタイムスキャン

マニュアルスキャン

ブラウザ保護

ファイアウォール

ソフトウェアアップデート

デバイス制御

自動化されたタスク

ネットワーク場所の設定

PREMIUM

データガード

アプリケーション制御

アプリケーション制御

「アプリケーション制御」タブでは、アプリケーションを実行するための制限を設定できます。

アプリケーション制御

グローバルルール

例外

例外を追加

有効	ルール名	イベント	処理	説明	メニュー
<input type="checkbox"/>	Block malicious files in Temp fol...	アプリケーションの開始	ブロック	Prevents execution of malicious ...	↑ ↓ ×
<input type="checkbox"/>	Block rare and unknown files in T...	アプリケーションの開始	ブロック	Prevents execution of rare files ...	↑ ↓ ×
<input type="checkbox"/>	Block malicious files in Downloa...	アプリケーションの開始	ブロック	Prevents execution of malicious ...	↑ ↓ ×
<input type="checkbox"/>	Block unknown and rare files in ...	アプリケーションの開始	ブロック	Prevents execution of rare files ...	↑ ↓ ×
<input type="checkbox"/>	Block batch scripts started by MI...	アプリケーションの開始	ブロック	Prevents batch scripts execution ...	↑ ↓ ×
<input type="checkbox"/>	Block powershell scripts started ...	アプリケーションの開始	ブロック	Prevents powershell scripts exec...	↑ ↓ ×
<input type="checkbox"/>	Block malicious Dlls in Temp fold...	モジュールの読み込み	ブロック	Prevents loading of malicious DLL...	↑ ↓ ×
<input type="checkbox"/>	Block rare Dlls with unknown rep...	モジュールの読み込み	ブロック	Prevents loading of rare Dlls wit...	↑ ↓ ×
<input type="checkbox"/>	Block malicious Dlls in Downloa...	モジュールの読み込み	ブロック	Prevents loading of malicious DLL...	↑ ↓ ×

項目名	内容
アプリケーション制御	アプリケーション制御を有効/無効にする
アプリケーション制御のルール	アプリケーション制御のルールを作成できます
グローバル ルール	すべてのアプリケーションに適用されるグローバルルールです。

12.7. コンピュータプロファイル (Windows Servers)

以下の表では、Elements EPP for Servers のプロファイルで設定可能な設定項目について説明します。

12.7.1. 一般設定

一般設定

一般設定

このタブには、F-Secure Elements Agentのセキュリティ機能で共有される設定が含まれています。

ウイルスのリアルタイム スキャン	クライアント ソフトウェアを速く利用する ?	<input type="checkbox"/>	
マニュアル スキャン	クライアントにユーザ インタフェースを表示する ?	<input checked="" type="checkbox"/>	
ブラウザ保護	<div style="display: flex; align-items: center;"> 自動更新 ? </div>		
ファイアウォール	手動で定義されたプロキシアドレス ?	<input type="text"/>	🔒
ソフトウェア アップデータ	HTTP プロキシを使用 ?	ユーザブラウザの設定を検出 ▼	🔒
デバイス制御	HTTPSを使用してアップデートをダウンロードする ?	<input type="checkbox"/>	🔒
自動化されたタスク	直接接続ではなく、プロキシを使用する ?	<input type="checkbox"/>	🔒
ネットワーク場所の設定	プロキシの設定を隠す ?	<input type="checkbox"/>	🔒
PREMIUM			
データガード	F-Secure Elements Connector ?	<input type="text"/>	🔒
アプリケーション制御	クライアントに.NETの管理を許可する ?	<input checked="" type="checkbox"/>	🔒
	<div style="display: flex; align-items: center;"> すべてのセキュリティ スキャンからファイル/フォルダを除外する ? </div>		
	ここで指定したフォルダ、ファイル、SHA-1チェックサムは、すべてのセキュリティ スキャンと対策から除外されているため、F-Secure が提供するセキュリティ機能から対象外になります。指定したフォルダ内のサブフォルダも含まれます。重要: この設定はスキャンから絶対に除外しなければならないファイルまたはフォルダに対してのみ使用してください。たとえば、C:\ をスキャンの対象から除外すると、デフォルトのシステム ドライブ全体とその中のすべてのフォルダ、サブフォルダ、およびファイルがすべてのセキュリティ対策から除外されます。 例: C:\Program Files (x86)\Microsoft Office\root\Office16\OUTLOOK.EXE C:\Program Files (x86)\Microsoft Office C:\Program Files\Microsoft 3395856ce812b7382dee726027f98b642f14140		
	例外を追加		🔒

項目名	内容
クライアント ソフトウェアを誰よりも早く利用する	クライアント ソフトウェアを一般リリースよりも早く利用できます
クライアントにユーザ インターフェイスを表示する	クライアント端末にアイコンを表示します

自動更新

項目名	内容
HTTP プロキシを使用	自動更新エージェントから更新サーバへ接続を行う際の、HTTP プロキシを設定することができます。
手動で定義されたプロキシアドレス	このアドレスは、[HTTP プロキシを使用する] が「リモート管理」に設定されている場合に使用されます。
プロキシを介した強制接続	直接接続の代わりにプロキシ接続を使用します。
プロキシの設定を隠す	ローカル ユーザ設定インターフェイスでプロキシの設定パネルを非表示にします。
HTTPS を使用してアップデートをダウンロードする	HTTPS を使用してアップデートをダウンロードします
WithSecure Elements Connector	WithSecure Elements Connector を使用している場合、そのアドレスを指定します。
クライアントに.NET の管理を許可する	.NET 4.7.2 を使用してユーザインターフェイスを表示します。

すべてのセキュリティスキャンからファイル/フォルダを除外する

項目名	内容
パス	スキャンから除外されるファイル/フォルダを指定します。
クライアントからの除外を非表示にする	クライアントからの除外を非表示にする
通知を表示する	再起動の要求、検出された脅威に関する情報、エラー通知など、どのユーザがクライアント通知を表示できるかを選択できます。
一時ファイルの最大サイズ	スキャン中にスキャンプラットフォームが一時ファイルを保存するために使用できるディスク容量の最大値。

連携

項目名	内容
-----	----

WMI プロバイダ	WMI プロバイダを有効または無効にします。
Bitlocker リカバリキーを収集する	Bitlocker リカバリキーを収集する場合は、この設定をオンにします。
EDR センサーを有効にする	この設定は、EDR センサーを制御するために使用します (EDR のサブスクリプションがあるデバイスのみ使用可能)
アドバンスド・レスポンス	EDR のアドバンスド・レスポンス・モジュールを有効にする場合は、この設定をオンにしてください。

隔離保存

項目名	内容
ユーザがブロックおよび隔離されたアイテムを解放できるようにする	ユーザは隔離されたアイテムを解放し、ブロックされたアイテムを許可できます。
ブロックまたは隔離されたアイテムを開放するためのパスワード (オプション)	コンピュータのユーザへのパスワードを提供
古い隔離アイテムを自動的に削除する	構成された時間が経過した際に隔離したアイテムが削除されます。
アイテムを隔離する日数	値を 1~1095 日で設定

ライセンスの失効

項目名	内容
通知を表示する	ユーザにはライセンスの有効期限に関連する通知が表示されます
ライセンス有効期限までの日数	通知の表示を開始するためのライセンス期限の日数です。
ライセンスの有効期限に関するカスタマイズされたメッセージ	ユーザに表示するメッセージ。

改ざん防止

項目名	内容
リソース保護	有効にすると、WithSecure サービス、プロセス、ファイル、およびレジストリエントリを制御できなくなります。

ユーザがセキュリティ機能を無効にすることを許可

項目名	内容
-----	----

製品のアンインストールをユーザに許可	ユーザが製品のアンインストールが可能となります
ユーザがセキュリティ機能を無効にすることを許可	ユーザは WithSecure のセキュリティ機能を無効にすることができます。
パスワード	ユーザに設定したパスワードの入力を求めます。

改ざん保護イベントを除外する

項目名	内容
イベントタイプ/アプリケーション パス	特定のアプリケーションによる改ざん保護イベントを除外

12.7.2. ウイルスのリアルタイム スキャン

一般設定 ウイルスのリアルタイム スキャン

ウイルスのリアルタイム スキャン	ウイルスのリアルタイム スキャン	<input checked="" type="checkbox"/>	⊞
マニュアル スキャン	マルウェア対策スキャン インターフェース (AMSD)	<input checked="" type="checkbox"/>	⊞
フラグ保護	ファイル スキャン		
ファイアウォール	スキャンするファイル	指定した拡張子のファイルのみ	⊞
ソフトウェア アップデータ	感染時の処理を自動的に行う	<input type="checkbox"/>	⊞
デバイス制御	感染時の処理	隔離保存	⊞
自動化されたタスク	リスクウェアに対するアクション	ブロック	⊞
ネットワーク場所の設定	スパイウェアに対するアクション	隔離保存	⊞
PREMIUM	Hosts ファイルの保護	<input checked="" type="checkbox"/>	⊞
データガード	ネットワークドライブをスキャンする	<input checked="" type="checkbox"/>	⊞
アプリケーション制御	ネットワークドライブのスキャンモード	実行時にスキャン	⊞
	次の拡張子のファイルはスキャンしない	<input type="checkbox"/>	⊞
	除外拡張子		⊞
	F-Secure Security Cloud を使用する	<input checked="" type="checkbox"/>	⊞
	除外したオブジェクト	<input type="checkbox"/>	⊞

項目名	内容
ウイルスのリアルタイム スキャン	リアルタイム スキャンの有効/無効を設定します。
マルウェア対策スキャン インターフェイス (AMSI)	マルウェア対策スキャン インターフェース (AMSI) の統合

ファイル スキャン

項目名	内容	
スキャンするファイル	「すべてのファイル」、「次の拡張子のファイル」のいずれかを選択します。	
	すべてのファイル	すべてのファイルをリアルタイム スキャンします。
	次の拡張子のファイル	「対象拡張子」に登録されている拡張子のファイルを対象にスキャンします。
感染時の処理を自動的に行う	本設定を「有効」にした場合、「感染時の処理」がグレーアウトし無効化され、マルウェア感染時に最適な処理を自動的に行います。「無効」にした場合は、下の「感染時の処理」がアクティブになり、「感染時の処理」で設定された内容に従って処理されます。	
感染時の処理	リアルタイム保護でウイルス検知が発生した場合の処理方法を指定します。「感染時の処理を自動的に行う」を「有効」にしている場合は無効化されます。	
	名前の変更	検知したファイルに対し、自動的に名前（拡張子）変更処理を行います。
	削除	検知したファイルに対し、自動的に削除処理を行います。削除したファイルは復旧できなくなります。
	駆除	検知したファイルに対し、自動的に駆除処理を行います。駆除できない場合は、名前（拡張子）変更処理を行います。
	隔離保存	検知したファイルに対し、自動的に検疫処理を行います。検疫されたファイルは別のディレクトリに隔離保存されます。
	スキャン後に確認	検知時にユーザが処理を指定します。
	ブロック	検知したファイルをブロックします
リスクウェアに対するアクション	削除/隔離保存/スキャン後に確認/ブロック	
スパイウェアに対するアクション	削除/隔離保存/スキャン後に確認/ブロック	
Hosts ファイルの保護	有効な場合、Hosts ファイルを保護します。	

ネットワークドライブをスキャンする	ネットワークドライブのスキャンの有効/無効を設定します。
ネットワークドライブのスキャンモード	ネットワークドライブのリアルタイム スキャンモードを選択します。
次の拡張子のファイルはスキャンしない	特定の拡張子を持つファイルをスキャンの対象から除外します。「除外拡張子」欄に除外したい拡張子を記入します。
除外拡張子	リアルタイム スキャンから除外するファイル拡張子のリストを登録します。複数の拡張子を記入する場合は、拡張子間に半角スペースを置きます。
WithSecure™ Security Cloud を使用する	WithSecure™ Security Cloud の使用

除外したオブジェクト

項目名	内容
除外したオブジェクト	特定のファイルまたはディレクトリをリアルタイム スキャンの対象から除外する機能の有効・無効を設定します。
オブジェクト	除外対象とするファイルまたはフォルダを指定します。[オブジェクトを追加]をクリックするとオブジェクトの追加が行えます。

除外しているプロセス

項目名	内容
除外しているプロセス	特定のプロセスをリアルタイム スキャンの対象から除外する機能の有効・無効を設定します。
プロセス	除外する対象のプロセスを指定します。除外するプロセスのフル パスを入力する必要があります。
すべてのリスクウェアを除外する	すべてのリスクウェアのスキャンをスキップできます。
すべてのスパイウェアを除外する	すべてのスパイウェアのスキャンをスキップします。

除外されたリスクウェア/スパイウェア

項目名	内容
除外されたリスクウェア/スパイウェア	スパイウェアまたはリスクウェアをリアルタイム スキャンから除外します。

Web スキャン

項目名	内容	
Web スキャン	有効な場合、Web からダウンロードするファイルを受信前にスキャンします。	
	Web トラフィックをスキャンして、検出したマルウェアを削除する	スキャンする対象を選択します。

Web スキャンから除外されているアプリケーション

項目名	内容	
Web スキャンから除外されているアプリケーション	Web スキャンから特定のアプリケーションを除外する場合、有効に設定します。	
	アプリケーションを追加	除外するアプリケーションの SHA-1 ハッシュ値を追加します。

ディープガード

項目名	内容
ディープガード	WithSecure の振る舞い検知・サンドボックス機能であるディープガードの有効/無効を設定できます。
まれで疑わしいファイルをブロックする	ディープガードがまれで疑わしいファイルをブロックできるようにします。

ディープガードの保護ルール

項目名	内容	
ディープガードの保護ルール	ディープガードからアプリケーションを除外する場合などに有効にします。	
	ルールを追加	ルールを登録したいアプリケーションの SHA-1 ハッシュを追加します。信頼済みが高いの場合常に実行され、いいえの場合常に実行を拒否されます。

12.7.3. マニュアルスキャン

一般設定 マニュアル スキャン

ウイルスのリアルタイムスキャン	USBストレージデバイスのスキャンをユーザに依頼する	<input checked="" type="checkbox"/>	🔒
マニュアル スキャン	スキャンするファイル	既知の拡張子のファイル	🔒
プラグイン保護	対象拡張子	COM EXE SYS OV? BIN SCR DLL SHS HTM H...	🔒
ファイアウォール	圧縮ファイルのスキャン (ZIP, RAR, ...)	<input checked="" type="checkbox"/>	🔒
ソフトウェア アップデータ	メールボックスファイル (.pst, .ost) 内をスキャン	<input type="checkbox"/>	🔒
デバイス制御	感染時の処理	スキャン後に確認	🔒
自動化されたタスク	次の拡張子のファイルはスキャンしない	<input type="checkbox"/>	🔒
ネットワーク場所の設定	除外拡張子		🔒
PREMIUM	スキャン優先度	優先度 (中)	🔒
データガード	除外したオブジェクト	<input type="checkbox"/>	🔒
アプリケーション制御	オブジェクト	除外されたオブジェクトはありません	🔒
	スケジュール スキャン	<input type="checkbox"/>	🔒
	スキャン頻度	毎週	
	月曜日	<input checked="" type="checkbox"/>	

項目名	内容
USB ストレージを接続した	接続する USB ストレージデバイスをスキャンするようにユーザに確認

ときの動作	できます。	
	何もしない	スキャンを実行しません
	USB のスキャンをユーザに依頼する	スキャンをユーザに確認します
	USB のサイレントスキャン	スキャンをユーザに確認せず実行します
	USB をスキャンし、結果をユーザに表示	スキャン後、結果をユーザに表示します
スキャンするファイル	「すべてのファイル」、「次の拡張子のファイル」のいずれかを選択します。	
	すべてのファイル	すべてのファイルをマニュアルスキャンします。
	次の拡張子のファイル	登録されている拡張子のファイルをマニュアルスキャンします。定義されている拡張子は、「対象拡張子」で確認できます。
	既知の拡張子のファイル	一般的に使用される拡張子をスキャンします。
対象拡張子	スキャンするファイルを次の拡張子のファイルに設定した場合に、検査対象となる拡張子を登録します。	
圧縮ファイルのスキャン (zip、rar、...)	「有効」にすると圧縮ファイルもマニュアルスキャンします。	
メールボックスファイル (pst、ost) 内をスキャン	メールボックスファイルの内部にあるファイルをスキャンします。	
感染時の処理	マニュアルスキャンでウイルス検知、およびスパイウェア検知が発生した場合の処理方法を指定します。	
	消去	検知したファイルに対し、自動的に駆除処理を行います。駆除できない場合は、名前 (拡張子) 変更処理を行います。
	削除	検知したファイルに対し、自動的に削除処理を行います。削除したファイルは復旧できなくなります。
	名前の変更	検知したファイルに対し、自動的に名前 (拡張子) 変更処理を行います。
	スキャン後に確認	マルウェア検知が発生すると「駆除ウィザード」が表示されます。ユーザは駆除ウィザードに従って処理を選択します。
	隔離保存	検知したファイルに対し、自動的に検疫処理を行います。検疫されたファイルは別のディレクトリに隔離保存されます。

次の拡張子のファイルはスキャンしない	「有効」にすると特定の拡張子を持つファイルをスキャンの対象から除外します。「対象外とする拡張子」欄に除外したい拡張子を記入します。
除外拡張子	マニュアルスキャンから除外するファイル拡張子のリストを登録します。複数の拡張子を記入する場合は、拡張子間に半角スペースを置きます。
スキャン優先度	スキャンの優先度を [優先度 (中)] と [バックグラウンド] から選択します。[バックグラウンド] にすることで、スキャンに割り当てられる CPU のリソースの優先度が下げられます。

除外したオブジェクト

項目名	内容	
除外したオブジェクト	特定のファイルまたはディレクトリをマニュアルスキャンの対象から除外する機能の有効・無効を設定します。	
	オブジェクト	除外対象とするファイルまたはフォルダを指定します。[オブジェクトを追加]をクリックするとオブジェクトの追加が行えます。

スケジュールスキャン

項目名	内容
スケジュールスキャン	有効な場合、スケジュールスキャンを設定できます。

スキャン頻度

項目名	内容
スキャン頻度	スキャン頻度を、日次か週次か月次で指定します。週次の場合は、スキャンを実施する曜日を指定します。月次の場合は、スキャンを実施する日を三日まで指定します。

スキャンを開始

項目名	内容
スキャンを開始	スキャンの開始時刻を、時間またはアイドル時間で指定します。
次のシステム アイドル時間が経過したらスキャンを開始	コンピュータで指定したアイドル時間が経過した時点で開始されます。

スケジュールスキャンのオプション

項目名	内容
スキャンを低い優先度で実行する	有効な場合、スケジュールスキャンに割り当てられる CPU のリソースの優先度が下げられます。

指定ファイルのみスキャン (高速)	有効な場合、主要なファイルのみをスキャンし、短時間でスキャンを終了します。
圧縮ファイルのスキャン(低速)	有効な場合、圧縮ファイルのスキャンを行うため、スキャンが要する時間が長くなります。
通知をユーザに表示する	スケジュールスキャンの通知を表示します

除外するオブジェクトの指定では、「?」と「*」の正規表現が利用可能です。正規表現を利用しない場合は、完全一致です。フォルダ単位の指定を行う場合は、最後に「¥ (バックスラッシュ)」の記載をお願いします。

リアルタイム スキャンの除外設定でワイルドカードを使用する場合は、ドライブ名を判断できません。そのため、ワイルドカードを利用した除外設定を行う場合は、ドライブ銘を記載する代わりに、必ず「*¥¥」記載してください。(例: 「*¥¥Windows¥system32¥」)

ここの指定で除外されるスキャンは、振る舞い検知を含まない (パターンマッチングによる) スキャンからの除外設定になります。そのため、振る舞い検知からも除外を行いたい場合には、「ウイルスのリアルタイム スキャン」→「ディープガードの保護ルール」から、除外するアプリケーションを登録する必要があります。

12.7.4. ブラウザ保護

ブラウザ保護

一般設定	ウイルスのリアルタイムスキャン	評価に基づいたブラウジング	<input checked="" type="checkbox"/>	ⓘ					
	マニュアル スキャン	ブロックしたページのアクセスをユーザに許可する	<input checked="" type="checkbox"/>	ⓘ					
	ブラウザ保護	セーフサーチ モードを強制する	<input type="checkbox"/>	ⓘ					
	ファイアウォール	評価に基づいたブラウジング	<input checked="" type="checkbox"/>	ⓘ					
	ソフトウェア アップデータ	「危険」評価の Web サイトのアクセスをブロックする	<input checked="" type="checkbox"/>	ⓘ					
	デバイス制御	「不審」評価の Web サイトのアクセスをブロックする	<input checked="" type="checkbox"/>	ⓘ					
	自動化されたタスク	「禁止」評価の Web サイトのアクセスをブロックする	<input checked="" type="checkbox"/>	ⓘ					
	ネットワーク場所の設定	検索結果に対する評価を表示する	<input checked="" type="checkbox"/>	ⓘ					
PREMIUM	データガード	Web コンテンツ制御	<input type="checkbox"/>	ⓘ					
	アプリケーション制御	拒否	カテゴリ	拒否	カテゴリ	拒否	カテゴリ	ⓘ	
		<input type="checkbox"/> SNS		<input type="checkbox"/> ソフトウェア ダウンロード		<input type="checkbox"/> 詐欺		<input type="checkbox"/> 支払いサービス	
		<input type="checkbox"/> Web メール		<input type="checkbox"/> チャット		<input type="checkbox"/> 就活		<input type="checkbox"/> 出会い	
		<input type="checkbox"/> アダルト		<input type="checkbox"/> ドラッグ		<input type="checkbox"/> 権限表現		<input type="checkbox"/> 虫歯	
		<input type="checkbox"/> アニメイザ		<input type="checkbox"/> ハッキング					
		<input type="checkbox"/> アルコールとタバコ		<input type="checkbox"/> ハッキング					
		<input type="checkbox"/> オペレーション		<input type="checkbox"/> ファイル共有					

項目名	内容
評価に基づいたブラウジング	レピュテーションベースのブラウジングをオンにします。
ブロックしたページのアクセスをユーザに許可する	警告ページからブロックされたページに進めることを許可します。
セーフサーチ モードを強制する	検索結果フィルタを有効にして、アダルトコンテンツを非表示にすることができます。

評価に基づいたブラウジング

項目名	内容
「危険」評価の Web サイトのアクセスをブロックする	有効な場合、危険と評価された Web サイトへのアクセスがブロックされます。
「不審」評価の Web サイトのアクセスをブロックする	有効な場合、不審と評価された Web サイトへのアクセスがブロックされます。
「禁止」評価の Web サイトのアクセスをブロックする	有効な場合、危険と評価された Web サイトへのアクセスがブロックされます。
検索結果に対する評価を表示する	有効な場合、サーチエンジンの検索結果に評価を表示します。

Web コンテンツ制御

項目名	内容
Web コンテンツ制御	「有効」にすると特定のカテゴリに関するサイトのアクセスを禁止します。禁止するカテゴリを有効に設定してください。
許可されたサイトを除くすべてをブロックする	許可されたサイトのリストにあるサイトを除くすべてのサイトへのアクセスをブロックします。

コンテンツタイプのフィルタリング

項目名	内容
コンテンツタイプのフィルタリング	「有効」にすると、サイトの安全性の評価が「不審」または「不明」なサイトのコンテンツのタイプ別にフィルタリング設定が行えます。コンテンツタイプまたはファイル名でフィルタリング対象が設定されています。各フィルタリング項目について、有効/無効を設定することができます。

Web サイトの例外

項目名	内容	
Web サイトの例外	有効な場合、許可したサイトには常に接続が許可され、拒否したサイトには常に接続が拒否されます。	
サイト	許可したサイト	接続を許可するサイトを追加します。
	拒否したサイト	接続を拒否するサイトを追加します。

接続制御

項目名	内容
接続制御	「有効」にすると、銀行サイトと個人情報が保護されているサイトはセキュア ブラウジング モードで処理されます。
有効なインターネット接続を中断しない	有効な場合、接続制御が動作時に有効だったインターネット接続が維持されます。
完了したらクリップボードを消去する	セッション終了後にクリップボードを消去します。
ブロックコマンドラインとスクリプトツール	ネットワーク接続のコマンドラインツールとスクリプトツールをブロックできます。
リモートアクセスをブロックする	デバイスへのリモートアクセスをブロックすることができます。
サイトを追加	機密データを含み、セキュア ブラウジング モードの有効時にのみアクセスが可能なサイトの一覧が登録できます。[サイトを追加] をクリックすると登録できます。

	有効	有効・無効を設定します。「有効」にするとセキュアブラウジングモードでのみアクセス可能となります。
	アドレス	サイトの URL を入力します。

「信頼済みのサイト」「拒否したサイト」の登録に正規表現は利用できません。ホスト名による登録となり（パスまで記載された場合、パスは無視されます）、前方一致になります。「http」などのプロトコルの記載は必要ありません。

12.7.5. ファイアウォール

一般設定

ウイルスのリアルタイムスキャン

マニュアル スキャン

ブラウザ保護

ファイアウォール

ソフトウェア アップデータ

デバイス制御

自動化されたタスク

ネットワーク場所の設定

PREMIUM

データガード

アプリケーション制御

ファイアウォール

Windows Firewall の設定。Windows ファイアウォールが有効の場合、システムが Windows ファイアウォールのユーザー ルールを使用します。F-Secure ファイアウォール ルールは Windows ファイアウォールのユーザー ルールの上に追加のセキュリティを提供します。

▼ 一般設定 ⓘ

 F-Secure ファイアウォール プロファイル
これらのルールは、Windows ファイアウォールのユーザー ルールの上に追加のセキュリティレイヤを提供します。

 Windows ファイアウォールを使用
この設定を有効にすると、Windows ファイアウォールのユーザー ルールとネットワーク ルールがデバイスに適用されます。ドメイン ルールはこれらのルールよりも優先されることに注意してください。 ⓘ

 プロファイルを編集する
プロファイルの一次および二次設定を行い、プリセットの F-Secure プロファイル ルールを上書きする新しいルールを作成できます。プリセット ルールを使用せずにすべてのルールを作成する場合、カスタム プロファイルを選択してください。

F-Secureファイアウォールモード ⓘ

F-Secureファイアウォールをオンにする ⓘ

F-Secure ファイアウォール プロファイルの選択 ⓘ

Normal Workstation ⓘ

注意：自動プロファイル選択ルールを以下の場所に移動しました。ネットワーク場所の設定。

▲ F-Secure ファイアウォール プロファイル ⓘ

ファイアウォール ルールのマッピング
F-Secure プロファイルは Windows ファイアウォールのユーザー ルールと他のドメイン ルールの上に機能します。

1. F-Secure ファイアウォールの一般設定がまず適用されます。
2. 次に、ファイアウォール ルール テーブルのルールが評価されます。
3. プロファイルで他に一致するルールがない場合にはフォールバック設定が適用されます。

ブロックルールは許可ルールより優先されます。 ⓘ

一般設定

項目名	内容	
WithSecure™ファイアウォールプロモード	WithSecure™ファイアウォールの動作を制御するには、次のいずれかのオプションを選択します。	
	何もしない	WithSecure™ファイアウォールがオフになります
	Windows ファイアウォールをオフにする	WithSecure™ファイアウォールが Windows ファイアウォールをオフにします。
	WithSecure™ファイアウォールをオンにする	WithSecure™ファイアウォールは Windows ファイアウォールをオンにし、構成されたプロファイルから追加のルールと設定を適用します。
WithSecure™ファイアウォールプロファイルの選択	Windows のファイアウォールのルールに追加する WithSecure™ファイアウォールのルールを選択します。ファイアウォール ルールの内容については、「ファイアウォール ルールテーブル」で確認できます。	

WithSecure™ファイアウォールプロファイル

項目名	内容
変更するプロファイルを選択してください	プロファイル エディタで変更するファイアウォールプロファイルを選択します。
すべての受信接続をブロック	クライアントに対する全ての受信通信の接続リクエストをブロックします。
ユニキャスト レスポンスをマルチキャストに許可	この設定が有効の場合、マルチキャストまたはブロードキャスト メッセージに対するユニキャストのレスポンスがコンピュータに受信されることを阻止します。

フェイルバックの設定

項目名	内容
不明な受信接続を許可	この設定を有効にすると、コンピュータに対する不明な受信接続のリクエストが許可されます。通常、この設定の無効を推奨します。

不明な送信接続を許可	この設定を有効にすると、コンピュータに対する不明な送信接続のリクエストが許可されます。通常、この設定の無効を推奨します。
ファイアウォールが新しいアプリをブロックしたときに通知	この設定を有効にした場合、新しいアプリの発信接続がブロックされた際にエンドユーザに通知が送られます。

WithSecure™プロファイルのファイアウォール ルール : Normal Workstation

項目名	内容
WithSecure™プロファイルのファイアウォールルール	表示されているファイアウォール ルールを変更できます。WithSecure プロファイル ルールの上にルールを追加できます。ブロック ルールは許可ルールの前に評価されます。ルールの順序は評価に影響しません。
Normal Workstation	ルールは、通信方向とプロトコルおよびポート番号で構成されます。
他のルールを許可する	他の (WithSecure によって作成されていない) ファイアウォール ルールを許可します。無効に設定すると、プロファイルの有効時にすべてのルールが無効になり、有効に設定されているときには再び有効になります。

WithSecure™プロファイルのファイアウォール ルール : Network isolation

項目名	内容
WithSecure™プロファイルのファイアウォールルール	表示されているファイアウォール ルールを変更できます。WithSecure プロファイル ルールの上にルールを追加できます。ブロック ルールは許可ルールの前に評価されます。ルールの順序は評価に影響しません。
Network isolation	ルールは、通信方向とプロトコルおよびポート番号で構成されます。
許可されたドメイン	他の (WithSecure™ によって作成されていない) ファイアウォール ルールを許可します。無効に設定すると、プロファイルの有効時にすべてのルールが無効になり、有効に設定されているときには再び有効になります。
隔離されたコンピュータに関するカスタマイズされたメッセージ	コンピュータがネットワークから隔離されたときにユーザに表示されるメッセージ。

12.7.6. ソフトウェアアップデート

一般設定

ソフトウェア アップデータ

ウイルスのリアルタイム スキャン	ソフトウェア アップデータ ⓘ	<input checked="" type="checkbox"/>	🔍
マニュアル スキャン	ローカル ユーザー インターフェイス ⓘ	<input checked="" type="checkbox"/>	🔍
ブラウザ保護	適用されていないアップデートを自動的にスキャン ⓘ	<input checked="" type="checkbox"/>	🔍
ファイアウォール	スキャン優先度 ⓘ	標準	🔍
ソフトウェア アップデータ	▼ 自動インストール ⓘ		
デバイス制御	注意：自動インストールの設定を以下の場所に移動しました。自動化されたタスク。		
自動化されたタスク	▼ 自動インストールにソフトウェアを含める ⓘ		
ネットワーク場所の設定	ルールを追加		
PREMIUM	有効	ルール	… 🔍
データガード	ルールがありません		
アプリケーション制御	▼ ソフトウェアを自動インストールから除外 ⓘ		
	ルールを追加		
	有効	ルール	… 🔍
	ルールがありません		
	システム起動時のスキャン ⓘ	<input type="checkbox"/>	🔍
	再起動通知ポリシー ⓘ	表示しない	🔍

項目名	内容
ソフトウェアアップデート	ソフトウェアアップデートの機能の有効/無効を選択できます。「無効」にした場合、Elements EPP の機能によるソフトウェアのアップデートが行われなくなります。
ローカル ユーザ インターフェイス	ソフトウェア アップデータのローカル ユーザ インターフェイスをオンまたはオフにします。
適用されていないアップデートを自動的にスキャン	適用していない更新プログラムの自動スキャンをソフトウェアアップデートをオンにします。
スキャン優先度	スキャンの優先度を設定します。

自動インストール

項目名	内容
自動インストール	「自動化されたタスク」項目に移動

自動インストールにソフトウェアを含める

項目名	内容
自動インストールにソフトウェアを含める	ソフトウェアアップデートによって自動的にインストールされるソフトウェアの名前を入力します。名前に一致するソフトウェアは、自動インストールの対象となります。

ソフトウェアを自動インストールから除外

項目名	内容
ソフトウェアを自動インストールから除外	ソフトウェアアップデートによって自動的にインストールさせないソフトウェアの名前を入力します。名前に一致するソフトウェアは、自動インストールの対象外となります。
システム起動時のスキャン	有効な場合、システムの起動時に適用されていないアップデートを常に確認します。
アプリケーション実行時のアクション	アプリケーションに適用するアクションを選択します。
インストールをユーザに通知する	有効な場合、アップデートのインストールがユーザに通知されます。
WSUS が使用されている場合、ソフトウェア アップデータと WSUS の両方が Microsoft の更新プログラムをインストールします	有効な場合、WSUS とソフトウェアアップデートの両方で更新がインストールされる場合があります。WSUS を使用している場合、無効に設定することを推奨します。

スキャン結果にアップデートを含める

項目名	内容
スキャン結果にアップデートを含める	ルールに一致するアプリケーションのみをスキャンの結果に追加します。

スキャンからアップデートを除外

項目名	内容
セキュリティに関連しない更新	「有効」にするとセキュリティに関連しない更新をスキャンした結果から除外します。

スキャン結果からアップデートを除外

項目名	内容
スキャン結果からアップデートを除外	ルールに一致するアプリケーションをスキャンの結果に追加しません。

通信

項目名	内容
HTTP プロキシを使用	ソフトウェアのアップデート時に、プロキシを介してアップデートプログラムをダウンロード可能になります。
手動で定義されたプロキシアドレス	ソフトウェア アップデータのリモート管理 HTTP プロキシ アドレスを入力します。
WithSecure™ Elements Connector	WithSecure™ Elements Connector をソフトウェアアップデートで使用するように設定します。
WithSecure™ Elements Connector	WithSecure™ プロキシアドレスを入力します。

12.7.7. デバイス制御

一般設定

ウイルスのリアルタイムスキャン

マニュアルスキャン

ブラウザ保護

ファイアウォール

ソフトウェアアップデート

デバイス制御

自動化されたタスク

ネットワーク場所の設定

PREMIUM

データガード

アプリケーション制御

デバイス制御

(デバイス制御)タブでは、ユーザが大容量記憶装置、USBカメラ、プリンタなどのUSBデバイスにアクセスする方法に関する制限を設定できます。USBストレージデバイスへの書き込みアクセスを禁止したり、実行中の実行ファイルを禁止したり、デバイスグループに基づいて制限を設定することができます。

デバイス制御	<input checked="" type="checkbox"/>	🔒
リムーバブル大容量ストレージデバイス	<input checked="" type="checkbox"/>	🔒
書き込みアクセスを許可	<input checked="" type="checkbox"/>	🔒
実行可能ファイルの実行を許可	<input checked="" type="checkbox"/>	🔒
リムーバブル大容量ストレージデバイスの例外		
ルールを追加		
有効	ハードウェアID	コメント
例外は定義されていません		
デバイスのフィルタリングルール		
ルールを追加		
ルール		...
HTREE\ROOT#0		×
ROOT\LEGACY_*		×
SWD\PRINTENUM*		×
STORAGE\VOLUMESNAPSHOT*		×

項目名	内容
デバイス制御	有効な場合、USB デバイスに対するアクセス制御が有効になります。

リムーバブル大容量ストレージデバイス

項目名	内容
書き込みアクセスを許可	有効な場合、USB ストレージデバイスへのファイルの書き込み、変更が許可されます。
実行可能ファイルの実行を許可	有効な場合、USB ストレージデバイス上のファイルの実行が許可されます。

リムーバブル大容量ストレージデバイスの例外

項目名	内容
リムーバブル大容量ストレージデバイスの例外	特定の外部デバイスの実行および書き込み権限を常に許可する

デバイスのフィルタリングルール

項目名	内容
デバイスのフィルタリングルール	デバイスのフィルタリング ルールを編集します。

デバイスのアクセスルール

項目名	内容
デバイスのアクセスルール	USB デバイスへのアクセスルールを許可またはブロックで設定します。 USB デバイスは、ハードウェア ID で指定します。USB デバイスのハードウェア ID を確認するには、当該デバイスを接続した Windows PC で、デバイスマネージャでデバイスのプロパティを確認します。

12.7.8. 自動化されたタスク

一般設定

自動化されたタスク [自動タスク] タブでは、自動的に実行されるタスクを追加または削除できます。

ウイルスのリアルタイム スキャン

マニユアル スキャン

ブラウザ保護

ファイアウォール

ソフトウェア アップデータ

デバイス制御

自動化されたタスク

ネットワーク場所の設定

PREMIUM

データガード

アプリケーション制御

有効	タイプ	スケジュールを	説明	利用可能なときに開始	...
自動化されたタスクはありません。					

項目名	内容
自動化されたタスク	自動タスクをオンまたはオフにします

自動化されたタスクのリスト	自動タスクのリストを追加します。
---------------	------------------

12.7.9. ネットワーク場所の設定

ネットワーク場所の設定 [ネットワーク場所] タブでは、ネットワークの場所を追加し、現在デバイスが接続されているネットワークに応じて適用されるルールを設定することができます。

一般設定

- ウイルスのリアルタイムスキャン
- マニュアル スキャン
- ブラウザ保護
- ファイアウォール
- ソフトウェア アップデータ
- デバイス制御
- 自動化されたタスク
- ネットワーク場所の設定**

ネットワーク場所の設定 🔒

ロケーションとルール ?

場所を追加

場所は追加されていません ⋮

項目名	内容
ネットワーク場所の設定	作成されたすべての場所とルールをオンまたはオフにできます。

ロケーションとルール	ルールを適用する場所を追加できます。
------------	--------------------

12.7.10. データガード (Premium)

Premium 設定は WithSecure Elements EPP for Servers Premium を搭載したデバイスのみ適用されま
す。

一般設定

ウィルスのリアルタイムスキャン

マニュアル スキャン

ブラウザ保護

ファイアウォール

ソフトウェア アップデータ

デバイス制御

自動化されたタスク

ネットワーク場所の設定

データガード

アプリケーション制御

データガード

「F-Secure データガード」は、高度な動作ルールを適用して、システムに影響を与えようとするマルウェア (ランサムウェアなど) の検みを認識することでデータガード (リアルタイム スキャン) を強化するプレミアム機能です。フォルダは自動的に検出され、例外は手動で追加できます。信頼できるアプリケーションはフォルダにアクセスできます。重要: データガードが機能するには、データガードおよびリアルタイム スキャンを有効にする必要があります。

データガードの高度な動作ブロック	<input checked="" type="checkbox"/>	ⓘ
許可およびレポートモード	<input type="checkbox"/>	ⓘ
▼ 監視フォルダ ⓘ		
監視対象のユーザのデータ フォルダを自動的に検出する	<input checked="" type="checkbox"/>	ⓘ
手動で含まれるフォルダ ⓘ	パスを追加	
パス	パスはありません	
手動で除外されるフォルダ ⓘ	パスを追加	
パス	パスはありません	
▼ アクセス制御 ⓘ		
信頼済みのアプリケーションを自動的に検出する ⓘ	<input checked="" type="checkbox"/>	ⓘ
手動で追加された信頼済みのアプリケーションとフォルダ ⓘ	<input checked="" type="checkbox"/>	ⓘ
パスを追加		

項目名	内容
データガードの高度な動作ブロック	データガードの高度な動作ルールを有効にします。
許可およびレポートモード	保護されたフォルダを監視し、ブロックされるアクセスを報告します。

監視フォルダ

項目名	内容
監視対象のユーザのデータフォルダを自動的に検出する	この設定を有効にすると、ドキュメント、画像、またはその他のエンド ユーザー コンテンツを含むフォルダが自動的に保護されます。
手動で含まれるフォルダ	保護対象のフォルダを追加することができます。
手動で除外されるフォルダ	保護対象外のフォルダを追加することができます。

アクセス制御

項目名	内容
アクセス制御	データガードが保護しているファイルやフォルダを変更できるアクセス権をアプリケーションに指定できます。
信頼済みのアプリケーションを自動的に検出する	信頼できるアプリケーションを自動的に検出することができます。
手動で追加された信頼済みのアプリケーションとフォルダ	信頼できる実行可能ファイルと信頼できる実行可能ファイルを含むフォルダを手動で定義することができます。

リスト

項目名	内容
DataGuard リスト	ディープガード保護にリストを追加することができます。

12.7.11. アプリケーション制御 (Premium)

Premium設定はWithSecure Elements EPP for Servers Premiumを搭載したデバイスのみ適用されま
す。

一般設定

ウイルスのリアルタイム スキャン

マニユアル スキャン

ブラウザ保護

ファイアウォール

ソフトウェア アップデータ

デバイス制御

自動化されたタスク

ネットワーク場所の設定

PREMIUM

データガード

アプリケーション制御

アプリケーション制御

「アプリケーション制御」タブでは、アプリケーションを実行するための制限を設定できます。

アプリケーション制御

グローバル ルール すべてのアプリケーションを許可

▼ 例外

例外を追加

有効	ルール名	イベント	処理	説明	メニュー	...
<input type="checkbox"/>	Block malicious files in Temp fol...	アプリケーションの開始	ブロック	Prevents execution of malicious ...	↑ ↓	×
<input type="checkbox"/>	Block rare and unknown files in T...	アプリケーションの開始	ブロック	Prevents execution of rare files ...	↑ ↓	×
<input type="checkbox"/>	Block malicious files in Downloa...	アプリケーションの開始	ブロック	Prevents execution of malicious ...	↑ ↓	×
<input type="checkbox"/>	Block unknown and rare files in ...	アプリケーションの開始	ブロック	Prevents execution of rare files ...	↑ ↓	×
<input type="checkbox"/>	Block batch scripts started by Mi...	アプリケーションの開始	ブロック	Prevents batch scripts execution ...	↑ ↓	×
<input type="checkbox"/>	Block powershell scripts started ...	アプリケーションの開始	ブロック	Prevents powershell scripts exec...	↑ ↓	×
<input type="checkbox"/>	Block malicious DLLs in Temp fold...	モジュールの読み込み	ブロック	Prevents loading of malicious DLL...	↑ ↓	×
<input type="checkbox"/>	Block rare DLLs with known rep...	モジュールの読み込み	ブロック	Prevents loading of rare DLLs wit...	↑ ↓	×
<input type="checkbox"/>	Block malicious DLLs in Downloa...	モジュールの読み込み	ブロック	Prevents loading of malicious DLL...	↑ ↓	×

項目名	内容
アプリケーション制御	アプリケーション制御を有効/無効にする
アプリケーション制御のルール	アプリケーション制御のルールを作成できます
グローバル ルール	すべてのアプリケーションに適用されるグローバルルールです。

12.8. コンピュータプロファイル (Mac)

以下の表では、WithSecure Elements EPP for Computers Mac のプロファイルで設定可能な設定項目について説明します。

12.8.1. 一般設定

一般設定

一般設定

- ウイルスのリアルタイムスキャン
- マニュアル スキャン
- ブラウザ保護
- ファイアウォール

製品のアンインストールをユーザに許可	<input checked="" type="checkbox"/>	🔒
自動更新		
プロキシオプション	システム環境設定の HTTP プロキシを使用する	
リモート管理されているプロキシアドレス	<input type="text"/>	
F-Secure Elements Connector	<input type="text"/>	
グローバルF-Secureアップデートサーバへのフォールバック	<input checked="" type="checkbox"/>	
すべてのセキュリティスキャンからファイル/フォルダを除外する		
<small>ここで指定されたフォルダとファイルは、すべてのセキュリティスキャンと対策から除外されるため、F-Secure のセキュリティ保護の対象にはなりません。これには、指定されたフォルダ内のサブフォルダが含まれます。たとえば、/Users//folder-to-exclude/ は、すべてのユーザの folder-to-exclude フォルダで見つかったすべてのファイルとコンテンツを除外します。 重要: これは、スキャンから絶対に除外する必要があるファイルまたはフォルダにのみ使用してください。たとえば、スキャンから / を除外すると、システムボリューム全体とその中のすべてのフォルダ、サブフォルダ、およびファイルがすべてのセキュリティ対策から除外されます。 参考: 除外されたファイルとフォルダは、クライアントバージョン 17.7 以降にのみ適用されます。</small>		
例外を追加		
パス	...	
例外はありません		

項目名	内容
クライアント ソフトウェアを誰よりも早く利用する	クライアント ソフトウェアを一般リリースよりも早く利用できます
製品のアンインストールをユーザに許可	WithSecure™製品のアンインストールをユーザに許可するかどうかを指定します。

自動更新

項目名	内容
プロキシ オプション	プロキシの設定を行うことができます。
リモート管理されているプロキシ アドレス	HTTP プロキシサーバのアドレスを入力します。
WithSecure™ Elements Connector	WithSecure™ Elements Connector を使用している場合、そのアドレスを指定します。
グローバル WithSecure™アップデートサーバへのフォールバック	Elements Connector にアクセスできない場合、グローバルな WithSecure™更新サーバが使用されます。
すべてのセキュリティスキャンからファイル/フォルダを除外する	ここで指定されたフォルダとファイルは、すべてのセキュリティ スキャンと対策から除外されます。

12.8.2. ウイルスのリアルタイム スキャン

一般設定 ウイルスのリアルタイム スキャン

ウイルスのリアルタイム スキャン	ウイルスのリアルタイム スキャン	<input checked="" type="checkbox"/>	ⓘ
マニュアル スキャン	Security Cloud (ORSP)	<input checked="" type="checkbox"/>	ⓘ
プラグザ保護	XFence	<input type="checkbox"/>	ⓘ
ファイアウォール	この設定は、コンピュータのセキュリティに対する脅威を検出および阻止して、データを安全に保つためのユーティリティである XFence を有効にします。 詳細については、XFenceのヘルプドックを参照してください。		✕

項目名	内容
ウイルスのリアルタイム スキャン	リアルタイム スキャンの有効/無効を設定します。
Security Cloud (ORSP)	リアルタイム スキャン時に、Security Cloud のファイルレピュテーションを使用するかどうかを設定します。
XFence	Mac の振る舞い検知機能である XFence を使用するかどうかを設定します。

12.8.3. マニュアルスキャン

一般設定

ウイルスのリアルタイムスキャン

マニュアルスキャン

ブラウザ保護

ファイアウォール

マニュアルスキャン

▼ スケジュール スキャン ⓘ	<input type="checkbox"/>	
▼ スキャン頻度 ⓘ	再選	▼
月曜日	<input checked="" type="checkbox"/>	
火曜日	<input type="checkbox"/>	
水曜日	<input type="checkbox"/>	
木曜日	<input type="checkbox"/>	
金曜日	<input type="checkbox"/>	
土曜日	<input type="checkbox"/>	
日曜日	<input type="checkbox"/>	
▼ スキャンを開始 ⓘ		
時	10	▼
分	0	▼

項目名	内容
-----	----

スケジュールスキャン	スケジュールスキャンを行うかどうかを設定します。
スキャン頻度	スキャン頻度を、日次か週次か月次で指定します。週次の場合は、スキャンを実施する曜日を指定します。月次の場合は、スキャンを実施する日を三日まで指定します。
スキャンを開始	スキャンの開始時刻を指定します。

12.8.4. ブラウザ保護

一般設定

ウイルスのリアルタイムスキャン

マニファストスキャン

ブラウザ保護

ファイアウォール

ブラウザ保護

ブラウザ保護

Web コンテンツ制御

拒否	カテゴリ	拒否	カテゴリ	拒否	カテゴリ
<input type="checkbox"/>	SNS	<input type="checkbox"/>	ソフトウェア ダウンロード	<input type="checkbox"/>	詐欺
<input type="checkbox"/>	Web メール	<input type="checkbox"/>	チャット	<input type="checkbox"/>	支払いサービス
<input type="checkbox"/>	アダルト	<input type="checkbox"/>	ドラッグ	<input type="checkbox"/>	就活
<input type="checkbox"/>	アニメイザ	<input type="checkbox"/>	ハッキング	<input type="checkbox"/>	出会い
<input type="checkbox"/>	アルコールとタバコ	<input type="checkbox"/>	バンキング	<input type="checkbox"/>	憎悪表現
<input type="checkbox"/>	オークション	<input type="checkbox"/>	ファイル共有	<input type="checkbox"/>	中絶
<input type="checkbox"/>	ギャンブル	<input type="checkbox"/>	ブログ	<input type="checkbox"/>	不埒
<input type="checkbox"/>	ゲーム	<input type="checkbox"/>	違法	<input type="checkbox"/>	武器
<input type="checkbox"/>	ショッピング	<input type="checkbox"/>	海賊版ソフトウェア	<input type="checkbox"/>	暴力
<input type="checkbox"/>	ストリーミング メディア	<input type="checkbox"/>	芸術	<input type="checkbox"/>	不明
<input type="checkbox"/>	スパム	<input type="checkbox"/>	広告の提供		

許可されたサイトを強くすべてをブロックする

項目名	内容
ブラウザ保護	ブラウザ保護の有効/無効を設定できます。

Web コンテンツ制御

項目名	内容
Web コンテンツ制御	「有効」にすると特定のカテゴリに関するサイトのアクセスを禁止します。禁止するカテゴリを有効に設定してください。
許可されたサイトを除くすべてをブロックする	許可されたサイトのリストにあるサイトを除くすべてのサイトへのアクセスをブロックします。
接続制御	有効な場合、正しいオンラインバンキングサイトや機密情報を取り扱うサイトに接続していると、ユーザに通知を表示します。

Web サイトの例外

項目名	内容
Web サイトの例外	これらのサイトは許可またはブロックされています。

サイト

項目名	内容
許可したサイト	これらのサイトは決してブロックされません。
拒否したサイト	これらのサイトは常にブロックされます。

12.8.5. ファイアウォール

一般設定

ファイアウォール

ウイルスのリアルタイム スキャン	Appleファイアウォール ⓘ	On	
マニュアル スキャン	▼ F-Secure ファイアウォール ⓘ	<input type="checkbox"/>	
ブラウザ保護	F-Secure ファイアウォール プロファイルの選択 ⓘ	Default	
ファイアウォール	▼ F-Secure ファイアウォール プロファイル エディタ ⓘ		
	ファイアウォール ルールのマッピング 1. F-Secure ファイアウォール ルールの設定がまず適用されます。 2. プロファイルで他に一致するルールがない場合にはデフォルトのアクションが使用されます。		
	変更するプロファイルを選択してください Default		
	▼ 着信接続のデフォルトアクション	許可	
	組み込みアプリケーションを許可する ⓘ	<input checked="" type="checkbox"/>	
	F-Secureが信頼するアプリケーションを許可する ⓘ	<input type="checkbox"/>	
	匿名済みアプリケーションを許可する ⓘ	<input checked="" type="checkbox"/>	
	▼ 発信接続のデフォルトアクション	許可	
	組み込みアプリケーションを許可する ⓘ	<input checked="" type="checkbox"/>	
	F-Secureが信頼するアプリケーションを許可する ⓘ	<input type="checkbox"/>	

項目名	内容
Apple ファイアウォール	Mac OS のファイアウォールの有効/無効を設定します。

WithSecure™ ファイアウォール

項目名	内容
WithSecure™ ファイアウォール	WithSecure™ ファイアウォールを制御します。
WithSecure™ ファイアウォール プロファイルの選択	WithSecure™ ファイアウォール ルールの設定を選択します

WithSecure™ ファイアウォール プロファイル エディタ

項目名	内容
WithSecure™ ファイアウォール プロファイル エディタ	WithSecure™ ファイアウォール ルールを編集します

着信接続のデフォルトアクション

項目名	内容
着信接続のデフォルトアクション	着信接続のアクションの設定
組み込みアプリケーションを許可する	Apple が提供する組み込みアプリケーションのホワイトリスト。
WithSecure™が信頼するアプリケーションを許可する	WithSecure™の信頼できる開発者が署名したアプリケーションをホワイトリストに登録します。
署名済みアプリケーションを許可する	Apple または特定の開発者が署名したすべてのアプリケーションをホワイトリストに登録します。

発信接続のデフォルトアクション

項目名	内容
発信接続のデフォルトアクション	発信接続のアクションの設定
組み込みアプリケーションを許可する	Apple が提供する組み込みアプリケーションのホワイト

	リスト。
WithSecure™が信頼するアプリケーションを許可する	WithSecure™の信頼できる開発者が署名したアプリケーションをホワイトリストに登録します。
署名済みアプリケーションを許可する	Apple または特定の開発者が署名したすべてのアプリケーションをホワイトリストに登録します。
証明書の認証	証明書の認証ルールを設定します

WithSecure™プロファイルのファイアウォール ルール : Default

項目名	内容
WithSecure™プロファイルのファイアウォール ルール : Default	ファイアウォール ルールを編集

12.9. Linux プロファイル

以下の表では、WithSecure Elements EPP for Servers Linux のプロファイルで設定可能な設定項目について説明します。

12.9.1. 一般設定

一般設定 このタブには、F-Secure Elements Agentのセキュリティ機能で共有される設定が含まれています。

ウイルスのリアルタイムスキャン
 マニュアルスキャン
 完全性検査

項目名	設定	状態
インターネット接続		無効 白
HTTP プロキシを使用		無効 白
HTTP プロキシホスト	localhost	白
HTTP プロキシポート	3128	白
HTTP プロキシユーザ名		白
HTTP プロキシのパスワード		白
自動更新		
自動更新を有効にする		有効 白
アップデートを適用	受信時に	白
アップデート後に警告を送る		有効 白
改ざん防止		
ユーザがセキュリティ機能を無効にすることを許可		無効

項目名	内容
インターネット接続	Linux Protection のアップデート (製品とマルウェアの定義) および Security Cloud (ORSP) のプロキシ設定
HTTP プロキシを使用	使用の設定
HTTP プロキシホスト	更新プログラムのダウンロードや Security Cloud (ORSP)への接続に使用する HTTP プロキシサーバのアドレス
HTTP プロキシポート	更新プログラムのダウンロードや Security Cloud (ORSP)への接続に使用する HTTP プロキシサーバのアドレス
HTTP プロキシユーザ名	HTTP プロキシ Basic 認証のユーザ
HTTP プロキシのパスワード	HTTP プロキシ Basic 認証のパスワード
自動更新を有効にする	製品およびマルウェア定義の自動更新設定
アップデートを適用	製品アップデートのインストールポリシー
アップデート後に警告を送る	警告設定
改ざん防止	エンドユーザやサードパーティによる変更から WithSecure のインストーラを保護し、WithSecure のサービス、プロセス、ファイル、レジストリエントリを制御しようとする試行から保護します。
ユーザがセキュリティ機能を無効にすることを許可	WithSecure のセキュリティ機能の無効設定

12.9.2. ウイルスのリアルタイム スキャン

一般設定		ウイルスのリアルタイム スキャン	
ウイルスのリアルタイム スキャン	ウイルスのリアルタイム スキャン	有効	白
マニュアル スキャン	Security Cloud (ORSP) を使用	有効	白
完全性検査	スキャンするファイル		
	スキャンするファイルとフォルダ:		白
	パス 対象はありません		...
	スキャンから除外されたファイルとフォルダ:		白
	パス 例外はありません		...
	実行可能ファイルのみをスキャン	無効	白
	不要な可能性があるアプリケーションをスキャン	有効	白
	リアルタイムスキャンでのアーカイブの処理		
	アーカイブ内をスキャン	無効	白
	暗号化されたアーカイブを安全でないとして扱う	無効	白
	ネスト レベルまでアーカイブをスキャンします:	5	白

項目名	内容
ウイルスのリアルタイム スキャン	リアルタイム スキャンの有効/無効を設定します。
Security Cloud (ORSP) を使用	WithSecure Security Cloud との未知のファイルに対する評価の確認を有効にします。
スキャンするファイルとフォルダ	フォルダやファイルのスキャン設定
スキャンから除外されたファイルとフォルダ	フォルダやファイルのスキャン除外設定
実行可能ファイルのみをスキャン	実行ファイルのみをスキャン設定
不要な可能性があるアプリケーションをスキャン	不要の可能性のあるアプリケーションに対するスキャン
アーカイブ内をスキャン	アーカイブ内のファイルのスキャンを有効にします。
暗号化されたアーカイブを安全でないとして扱う	暗号化されたアーカイブはマルウェアとして処理されます。
ネスト レベルまでアーカイブをスキャンします	アーカイブに対してスキャンする最大ネスト レベルを設定します。
最大ネスティングレベルを超えたアーカイブを安全でないとして扱う	最大ネストレベルを超えるアーカイブがマルウェアとして処理されます。

リアルタイム スキャンに対するアクション

項目名	内容
マルウェアに対するアクション	マルウェアに対するアクションを選択します。
不要な可能性があるアプリケーションに対するアクション	不要の可能性があるアプリケーションに対するアクションを選択します。
不審なファイルに対するアクション	不審なファイルに対するアクションを選択します。

12.9.3. マニュアル スキャン

一般設定

ウイルスのリアルタイムスキャン

マニュアル スキャン

完全性検査

マニュアル スキャン

スキャンから除外されたファイルとフォルダ。		白
パス	例外はありません	...
不要な可能性のあるアプリケーションをスキャン	有効	白
マニュアルスキャンでのアーカイブの処理		
アーカイブ内をスキャン	無効	白
暗号化されたアーカイブを安全でないとして扱う	無効	白
ネスト レベルまでアーカイブをスキャンします	5	白
最大ネスティングレベルを超えたアーカイブを安全でないとして扱う	無効	白
マニュアルスキャンのアクション		
マルウェアに対するアクション	名前の変更	白
不要な可能性のあるアプリケーションに対するアクション	何もしない	白
不審なファイルに対するアクション	何もしない	白
スケジュール スキャン		
日時	00:00	白

項目名	内容
スキャンから除外されたファイルとフォルダ	ここで指定されたフォルダとファイルは、マニュアルスキャンから除外され、すべてのユーザの指定されたフォルダ内のサブフォルダも含まれます。
不要な可能性のあるアプリケーションをスキャン	この設定により、不要の可能性のあるアプリケーションに対するスキャンがオンになります。
アーカイブ内をスキャン	アーカイブ内のファイルのスキャンを有効にします。
暗号化されたアーカイブを安全でないとして扱う	暗号化されたアーカイブはマルウェアとして処理されません。
ネスト レベルまでアーカイブをスキャンします	アーカイブに対してスキャンする最大ネスト レベルを設定します。
最大ネスティングレベルを超えたアーカイブを安全でないとして扱う	最大ネストレベルを超えるアーカイブがマルウェアとして処理されます。
マルウェアに対するアクション	マルウェアに対するアクションを選択します。
不要な可能性のあるアプリケーションに対するアクション	不要の可能性のあるアプリケーションに対するアクションを選択します。
不審なファイルに対するアクション	不審なファイルに対するアクションを選択します。
スケジュールスキャン	システムをスキャンする日時の設定をします。

12.9.4. 完全性検査



項目名	内容
ファイルの整合性を確認する	指定されたファイルまたは指定されたディレクトリ内のファイルのベースラインを作成します。

12.10. モバイルデバイス プロファイル

以下では、「モバイル デバイス」タブにあるプロファイルの設定を説明します。

12.10.1. ネットワーク保護

ネットワーク保護

マルウェア保護

VPN 閉

VPNプロトコル 閉

ブラウザ保護 閉

ブラウザ保護 (HTTPS) 閉

追跡保護 閉

仮想ロケーションを選択

デフォルト	利用可能	場所	デフォルト	利用可能	場所	デフォルト	利用可能	場所
<input type="checkbox"/>	<input checked="" type="checkbox"/>	エスボー、フィンランド	<input type="checkbox"/>	<input type="checkbox"/>	パリ、フランス	<input type="checkbox"/>	<input type="checkbox"/>	米国東海岸
<input type="checkbox"/>	<input type="checkbox"/>	ストックホルム、スウェーデン	<input type="checkbox"/>	<input type="checkbox"/>	ブリュッセル、ベルギー	<input type="checkbox"/>	<input type="checkbox"/>	米国西海岸
<input type="checkbox"/>	<input type="checkbox"/>	オスロ、ノルウェー	<input type="checkbox"/>	<input type="checkbox"/>	アムステルダム、オランダ	<input type="checkbox"/>	<input type="checkbox"/>	モントリオール、カナダ
<input type="checkbox"/>	<input type="checkbox"/>	コペンハーゲン、デンマーク	<input type="checkbox"/>	<input type="checkbox"/>	ミラノ、イタリア	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	東京、日本
<input type="checkbox"/>	<input type="checkbox"/>	マドリッド、スペイン	<input type="checkbox"/>	<input type="checkbox"/>	ファルケンシュタイン、オーストリア	<input type="checkbox"/>	<input type="checkbox"/>	メルボルン、オーストラリア
<input type="checkbox"/>	<input type="checkbox"/>	ワルシャワ、ポーランド	<input type="checkbox"/>	<input type="checkbox"/>	ロンドン、イギリス			

項目名	内容
VPN	VPN の設定
VPN プロトコル	iOS 専用の VPN プロトコル設定
ブラウザ保護	疑わしい、または悪意のあることがわかっている Web サイトのブロック設定。
ブラウザ保護 (HTTPS)	HTTPS で暗号化された Web サイトのブロック設定。
追跡保護	トラッキング保護の設定
仮想ロケーションを選択	17 地域の中から仮想ロケーションを選択
VPN をバイパスするアプリ	信頼できるアプリケーションは、ネットワーク保護機能を回避して、インターネットに直接接続します。これは Android のみの機能です。Android 専用の機能です。

12.10.2. マルウェア保護



項目名	内容
マルウェア保護	ファイルとアプリケーションスキャンのオン/オフの設定。Android 専用
従量制スキャン	従量制接続でスキャンします。これは Android 専用
スケジュールスキャン	システムをスキャンする日時の設定をします。

12.11. Connector プロファイル

以下では、「Connector」タブにあるプロファイルの設定を説明します。

12.11.1. 一般設定

このタブには、F-Secure Connectorのセキュリティ機能で共有される設定が含まれています。

一般設定	
通信設定	
ポーリング間隔	600
ソフトウェアアップデートの設定	
最大ディスク容量 (MB)	20480
データベースが古くなっている日数	5
インターネット接続	
HTTP プロキシ	システムのデフォルト
手動で定義されたプロキシアドレス	

項目名	内容
通信設定	マルウェア定義の自動更新を処理設定
ポーリング間隔	サーバをポーリングする頻度
最大ディスク容量 (MB)	プロキシがソフトウェアの更新に割り当てることができる最大ディスク容量
データベースが古くなっている日数	最後にインストールされたウイルス署名データベースの更新からの日数がこの値を超えると、ユーザに警告が表示されます。
HTTP プロキシ	HTTP プロキシ設定
手動で定義されたプロキシアドレス	HTTP プロキシの手動設定

12.11.2. イベント転送

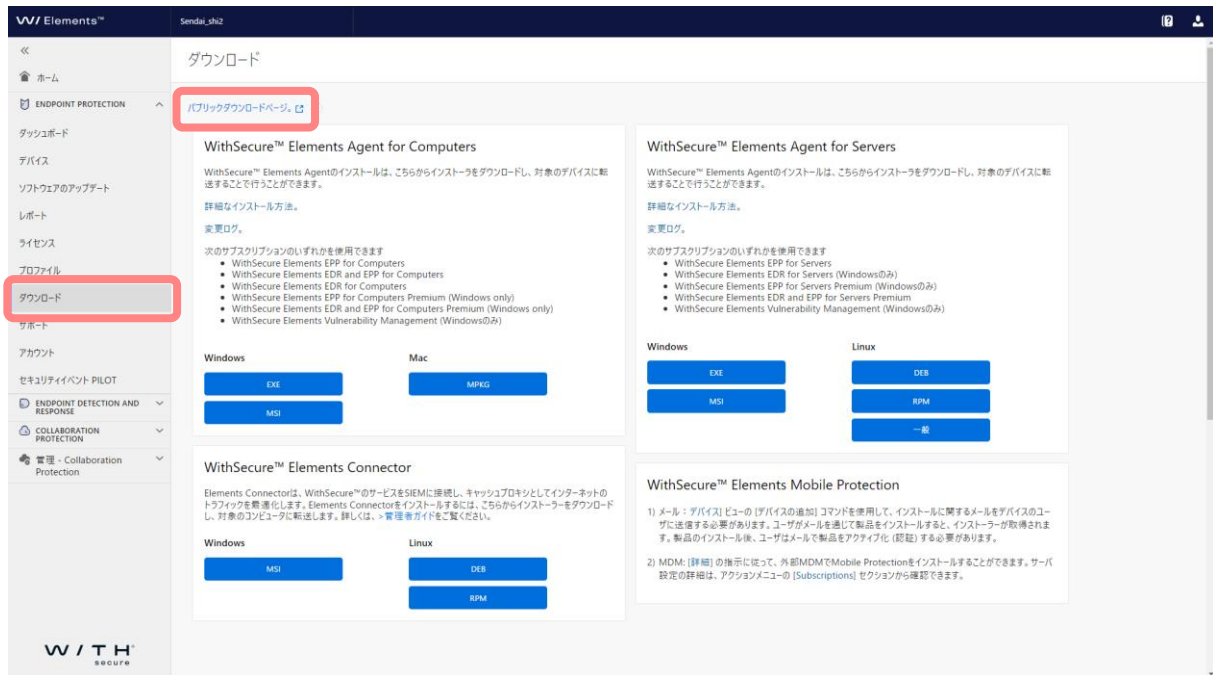
一般設定 **イベント転送** このタブには、F-Secure Connectorでのイベント転送の設定が含まれています。

イベント転送を有効にする ?	無効	🗑
SIEMシステムアドレス ?	<input type="text"/>	🗑
メッセージ形式 ?	Syslog (RFC 3164) ▾	🗑
プロトコル ?	TCP ▾	🗑

項目名	内容
イベント転送を有効にする	SIEM システムへのセキュリティイベントの転送を有効または無効にします。
SIEM システムアドレス	SIEM システムのユーザ定義の HTTP アドレス。
メッセージ形式	メッセージ形式 - Syslog (RFC3164)、共通イベント形式 (Splunk、ArcSight)、ログイベント拡張形式 (QRadar)。
プロトコル	通信プロトコル設定

13. ダウンロード

[ダウンロード] ボタンをクリックすると以下の画面が表示されます。ボタンクリックで各種ソフトウェアのダウンロードができます。ご利用の環境に合ったソフトウェアをお使いください。なお、ライセンスを保持していない製品については、ダウンロードリンクが表示されません。



・パブリックダウンロードページ

パブリックダウンロードは、展開ツールや IT 担当者がサブスクリプションキーを持っているが Elements Security Center にはアクセスできず、常に最新版をダウンロードのようにしたい場合に URL をご案内下さい。

<https://apac.psb.f-secure.com/#/public-downloads>

ソフトウェアをダウンロードできます

WithSecure™ Elements Agent for Computers

WithSecure™ Elements Agentのインストールは、こちらからインストーラをダウンロードし、対象のデバイスに転送することで行うことができます。

詳細なインストール方法。
変更ログ。

次のサブスクリプションのいずれかを使用できます

- WithSecure Elements EPP for Computers
- WithSecure Elements EDR and EPP for Computers
- WithSecure Elements EDR for Computers
- WithSecure Elements EPP for Computers Premium (Windows only)
- WithSecure Elements EDR and EPP for Computers Premium (Windows only)
- WithSecure Elements Vulnerability Management (Windowsのみ)

Windows: EXE, MSI
Mac: MPKG

WithSecure™ Elements Agent for Servers

WithSecure™ Elements Agentのインストールは、こちらからインストーラをダウンロードし、対象のデバイスに転送することで行うことができます。

詳細なインストール方法。
変更ログ。

次のサブスクリプションのいずれかを使用できます

- WithSecure Elements EPP for Servers
- WithSecure Elements EDR for Servers (Windowsのみ)
- WithSecure Elements EPP for Servers Premium (Windowsのみ)
- WithSecure Elements EDR and EPP for Servers Premium
- WithSecure Elements Vulnerability Management (Windowsのみ)

Windows: EXE, MSI
Linux: DEB, RPM, 一般

WithSecure™ Elements Connector

Elements Connectorは、WithSecure™のサービスとSEMIに接続し、キャプチャロギングとしてインターネットのトラフィックを高速化します。Elements Connectorをインストールするには、こちらからインストーラをダウンロードし、対象のコンピュータに転送します。詳しくは、>管理ガイドをご覧ください。

Windows: MSI
Linux: DEB, RPM

WithSecure™ Elements Mobile Protection

- 1) メール、デバイスビュー、(デバイス用途) コマンドを使用して、インストールに関するメールをデバイスのユーザに送信する必要があります。ユーザがメールを通して製品をインストールすると、インストーラが取得されます。製品のインストール後、ユーザはメールで製品をアクティブ化(登録)する必要があります。
- 2) MDM: [詳細] の使用に従って、外部MDMで(Mobile Protection)をインストールすることができます。サーバ設定の詳細は、アクションメニューの [Subscriptions] セクションから確認できます。

W / T H
secure | Formerly F-Secure Business

14. サポート

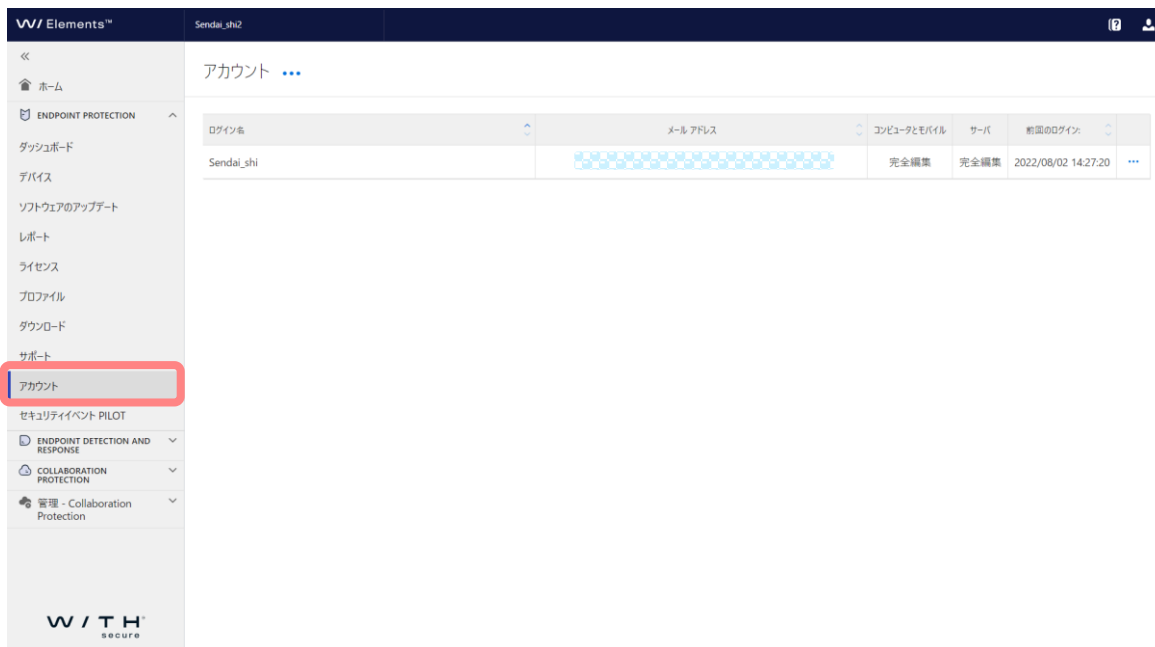
[サポート] ボタンをクリックすると以下の画面が表示されます。リンクをクリックすると各サポートに関する Web サイトが表示されます。



項目名	内容
ヘルプセンター	使い方などをまとめたヘルプセンターページが開きます。
変更ログ	Elements Security Center の更新履歴 (英語) のページが開きます。
WithSecure コミュニティ	Elements EPP のコミュニティページ (英語) が開きます。
サポートサイト	WithSecure のサポートサイトが開きます。
サポートの依頼	サポートリクエストフォームのページが開きます。

15. アカウント

[アカウント] ボタンをクリックすると以下の画面が表示されます。

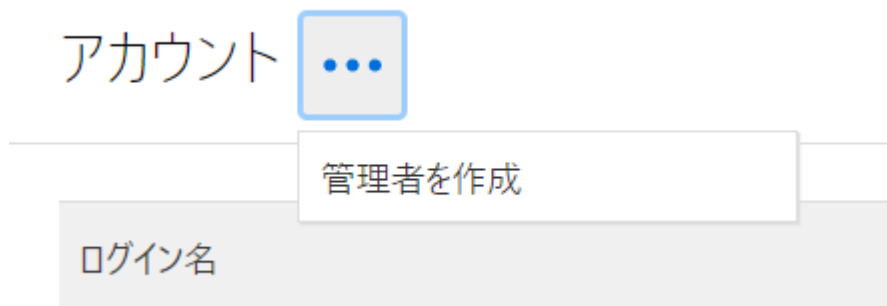


15.1. 企業アカウントとユーザアカウントの概念

アカウントの概念、および権限については、本書「[2.3 Elements Security Center のアカウントの概念](#)」をご参照ください。

15.2. アカウント管理 [管理者] タブメニュー

15.2.1. 管理者を作成



- ①アカウントの [アクションメニュー] をクリックします。
- ②[管理者を作成] をクリックすることで、「アカウントを作成する」画面が表示されます。
- ③入力が完了し [送信] ボタンをクリックすることでユーザが作成されます。

The screenshot shows the '管理者を作成' (Create Administrator) form in the F-Secure Elements Security Center. The form includes the following fields and options:

- メールアドレス* (Email Address): A text input field.
- ユーザ名を追加 (任意) (Add Username (Optional)): A plus icon and text.
- 言語* (Language): A dropdown menu set to '日本語' (Japanese).
- Server-only: サーバには読み取り専用 (Read-only for server).
- Computer and mobile: コンピュータとモバイルには読み取り専用 (Read-only for computer and mobile).

Buttons for 'キャンセル' (Cancel) and '送信' (Send) are at the bottom. A progress indicator at the top right shows '1' and '2' steps, with '管理者を作成' (Create Administrator) and 'OK' labels.

- ④登録したメールアドレスへ、ユーザ作成の通知がメールされます。ここで作成したユーザのパスワードは、この通知メールのリンクから設定します。

・アカウントを作成する

項目名	内容
メールアドレス	Elements Security Center から送信されるメールのあて先アドレスを指定します。
ユーザ名を追加 (任意)	Elements Security Center へのログインユーザ名をしています。通常はユーザのメールアドレスを使用します。
言語	ポータルで使用する言語を指定します。
サーバには読み取り専用	読み取り専用のアカウントかどうか指定します。
コンピュータとモバイルには読み取り専用	読み取り専用のアカウントかどうか指定します。

15.2.2. 管理者を編集する

「アカウント管理」画面にて、編集するユーザの [アクションメニュー] をクリックします。

ログイン名	メール アドレス	コンピュータとモバイル	サーバ	前回のログイン:	
Sendai_shi	[REDACTED]	完全編集	完全編集	2021/11/08 0:19:32	...

管理者を編集
管理者を削除

- ①[管理者を編集] をクリックします。
- ②各入力欄に編集内容を入力します。
- ③[保存] ボタンをクリックします。

管理者を編集
Sendai_shi

ユーザ名
Sendai_shi

メール アドレス
[REDACTED]

電話番号
▼ 番号

アクセス権限
セキュリティの管理権限 ▼

ポータルで匿名化されたデータと統計情報を収集できることを許可する
 サーバには読み取り専用
 コンピュータとモバイルには読み取り専用

[パスワードを変更するか、2段階認証を設定する](#)

キャンセル 保存

アカウントを編集する

項目名	内容
ユーザ名	(変更不可)
メールアドレス	管理者のメールアドレスを指定します。
電話番号	管理者の電話番号を指定します (任意入力項目)。
アクセス権限	セキュリティの管理権限のみ設定可能
ポータルで匿名化されたデータと統計情報を収集できることを許可する	ポータル上の操作を匿名データとして WithSecure が収集することを許可するかどうかを指定します。収集した情報は、ユーザビリティの改善情報などとして使用します。
パスワードを変更するか、2段階認証を設定する	

15.2.3. 管理者を削除

ログイン名	メール アドレス	コンピュータとモバイル	サーバ	前回のログイン:
Sendai_shi		完全編集	完全編集	2021/11/08 0:19:32

管理者を編集
管理者を削除

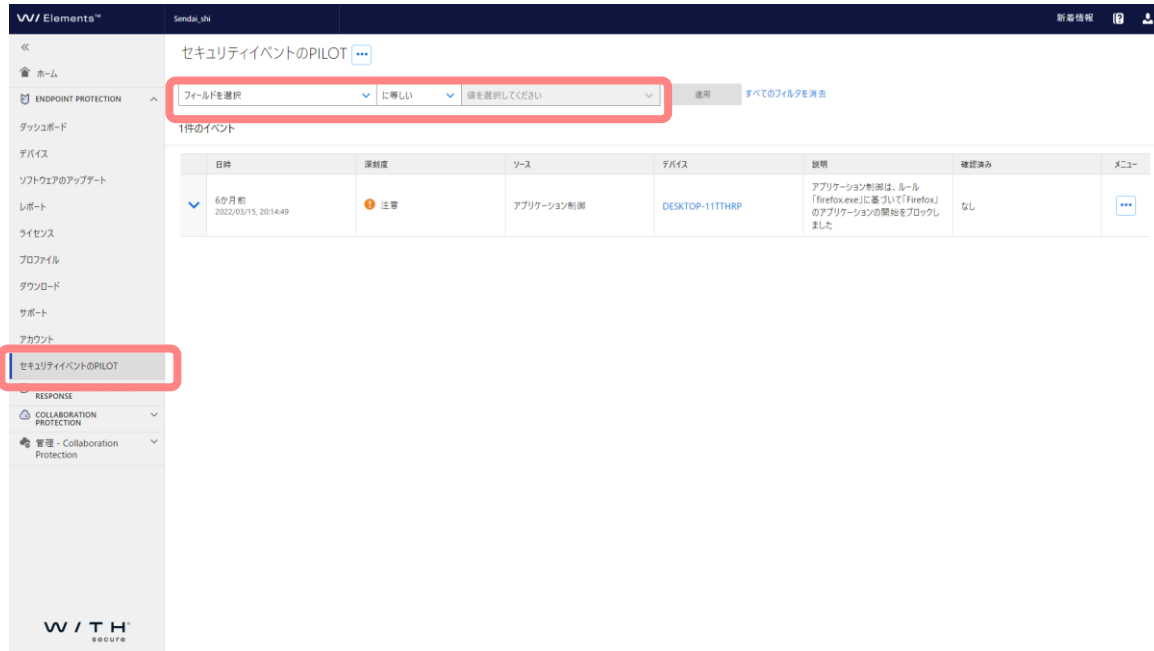
- ① 「アカウント管理」画面にて、削除するユーザの [アクションメニュー] をクリックします。
- ② [管理者を削除] をクリックします。
- ③ メッセージを確認し [OK] をクリックします。

16. セキュリティイベントの PILOT

[セキュリティイベント] の概要を確認できます。

16.1. [セキュリティイベント] の操作メニュー概要

[セキュリティイベント]ボタンをクリックすると、以下のような画面が表示されます。



項目名	内容
日時	発生日時
深刻度	対応が必要です/注意/情報
ソース	提供情報
デバイス	デバイス名
説明	イベントの説明
確認済み	管理者の確認状況
メニュー	項目により表示内容は変わります。 確認/隔離から削除する/元の場所に復元/誤検知の可能性を報告する/ フルパスでファイルを除外する/感染したアーカイブを隔離します/ SHA1 でファイルを除外する

16.2. アクションメニュー



項目名	内容
セキュリティイベントのエクスポート (JSON)	セキュリティイベントが、CSV 形式でダウンロードされます
感染警告の構成	警告送信時のメールアドレスを設定します

17. Appendix

17.1. Elements EPP が利用する URL

LAN からインターネットへの出入口の通信を制御することで、インターネット経由の攻撃に対するセキュリティを向上させることが出来ますが、Elements EPP の通信だけは、開ける必要があります。そこで以下では、Elements EPP が利用する URL を記載します。

[*.f-secure.com](https://community.f-secure.com)

[*.fsapi.com](https://community.f-secure.com)

参照情報 URL

<https://community.f-secure.com/common-business-ja/kb/articles/5529-f-secure-更新サービスの-url-アドレス>

以上