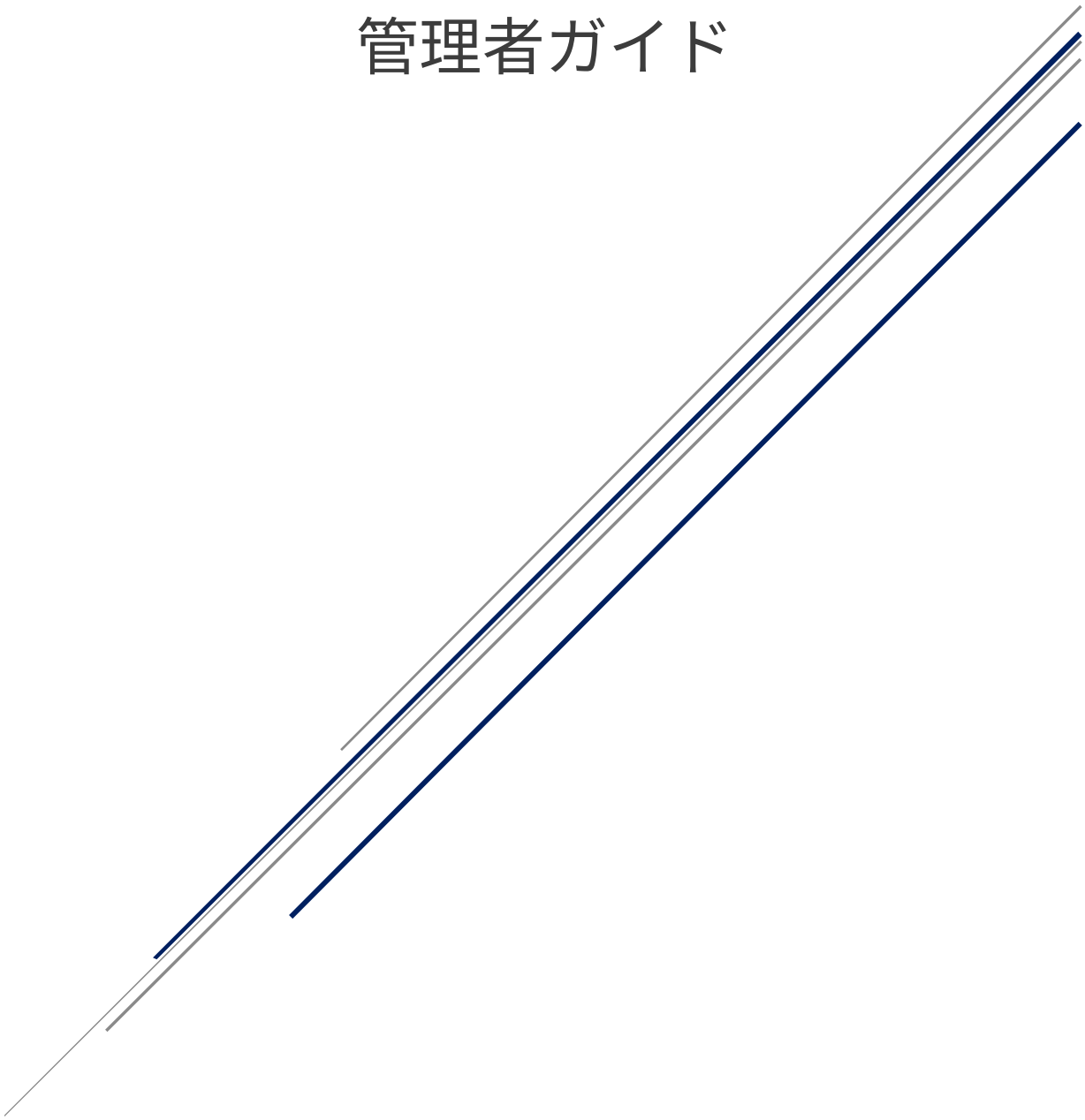
WithSecure™ Elements Security Center 管理者ガイド



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

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。

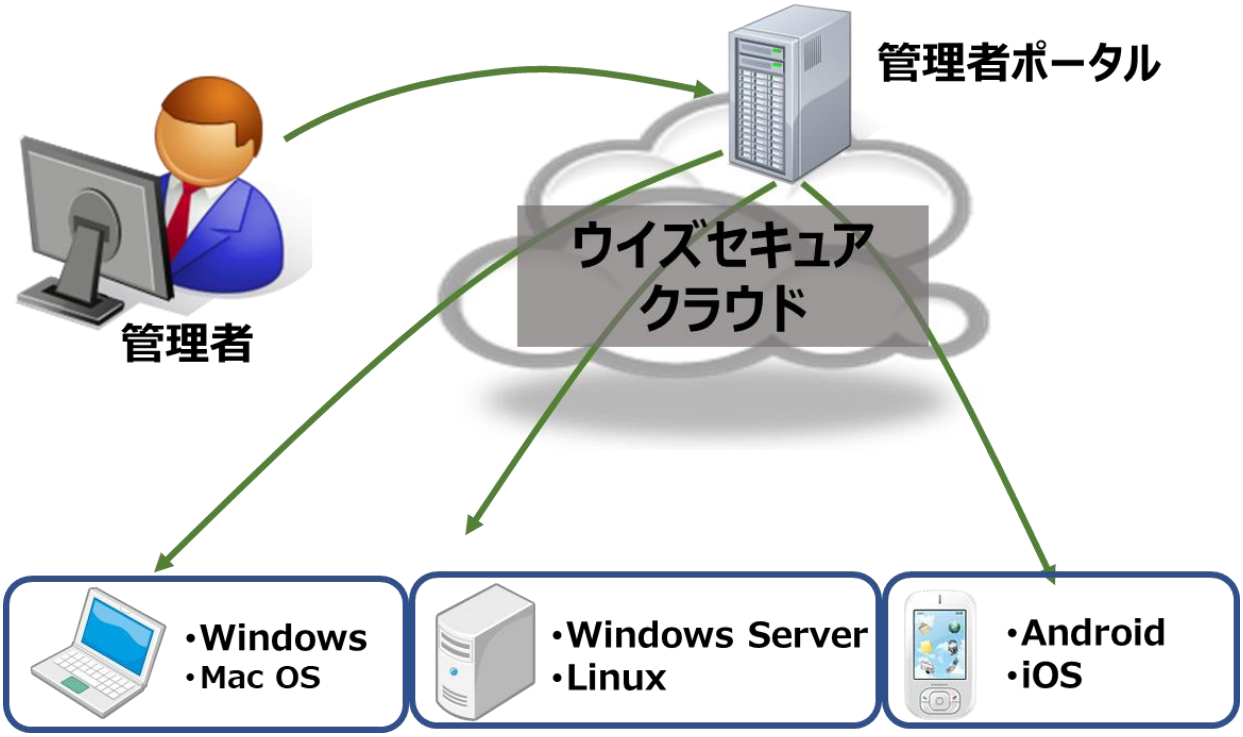
まず、「2.Elements Security Center 概要」において、Elements Security Center の概要と、独自の概念と技術について説明します。

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 向けのソフトウエアです。Windows 用と Mac 用があります。

・サーバ用クライアント

サーバ OS 向けのソフトウエアです。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 向けのソフトウエアです。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。

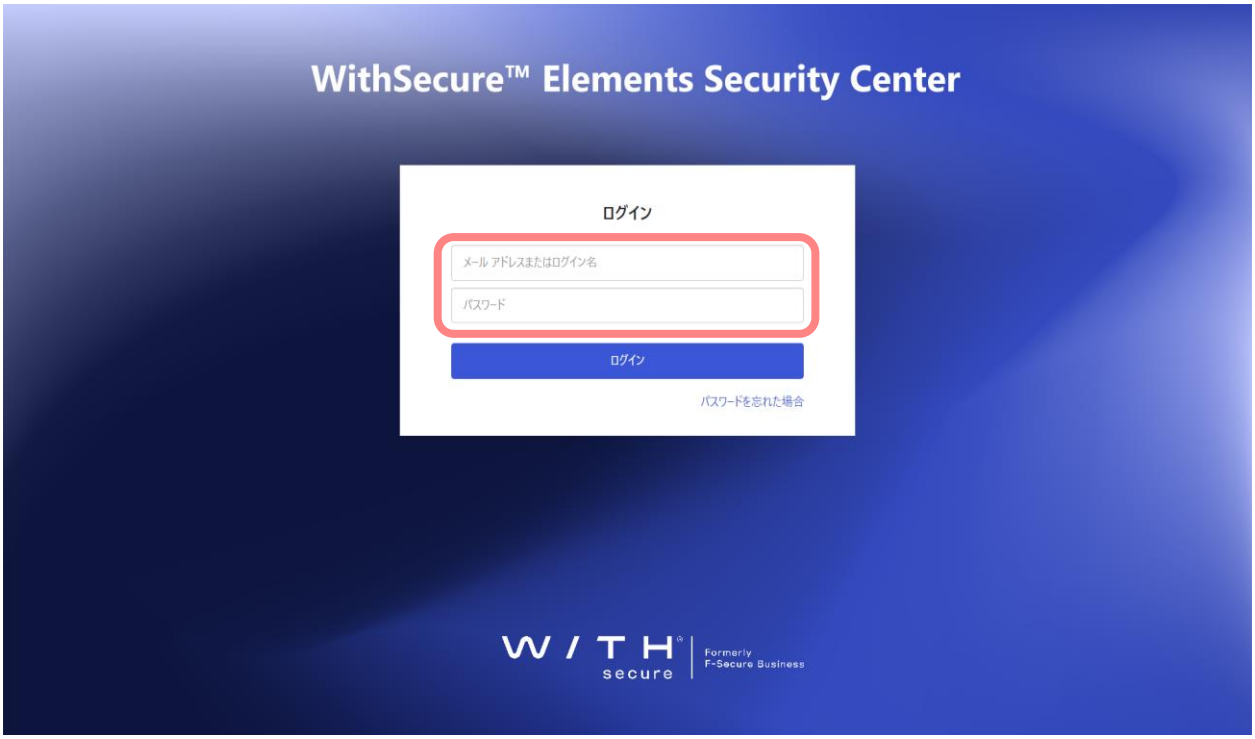
次の章からは、上記の手順の具体的な解説を行います。

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。



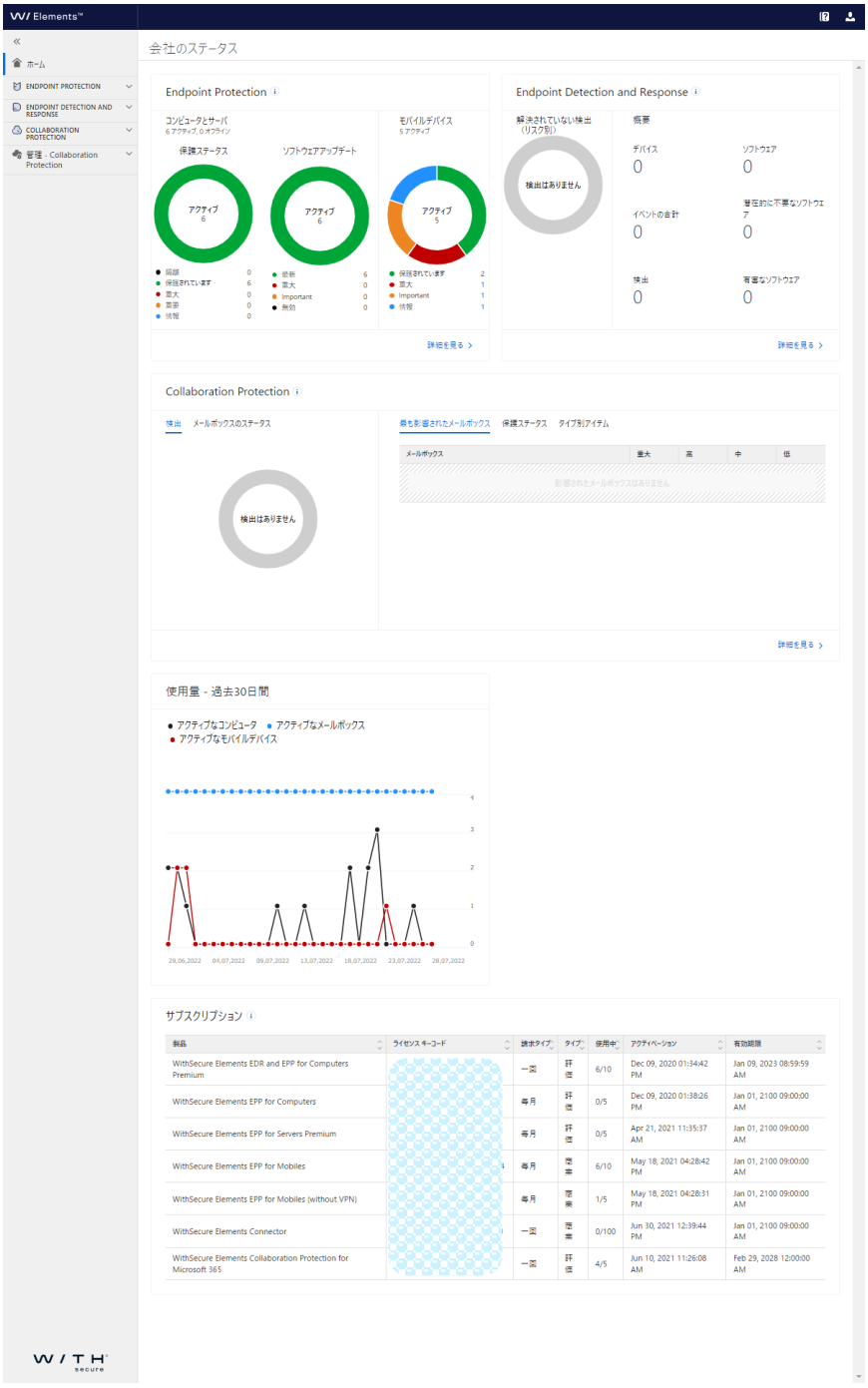
4. Elements Security Center の操作メニュー

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。

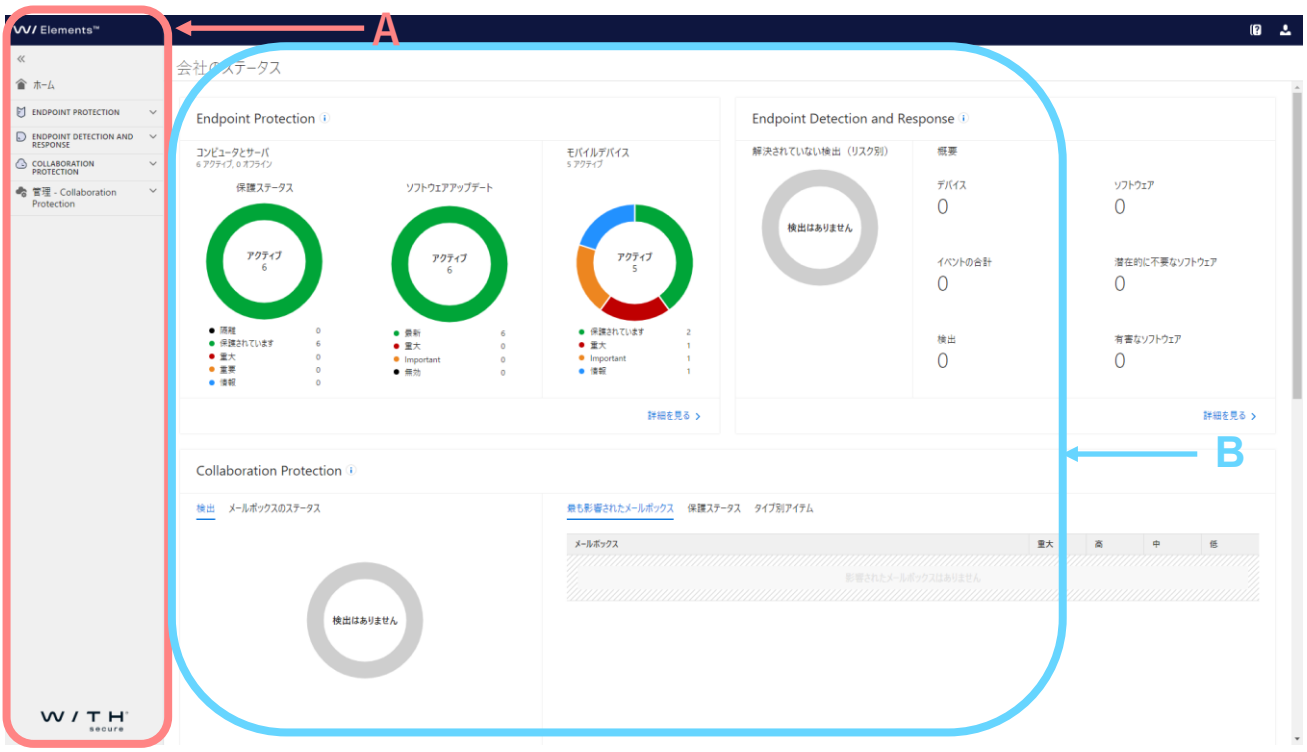
4.1. Elements Security Center の操作メニュー概要

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

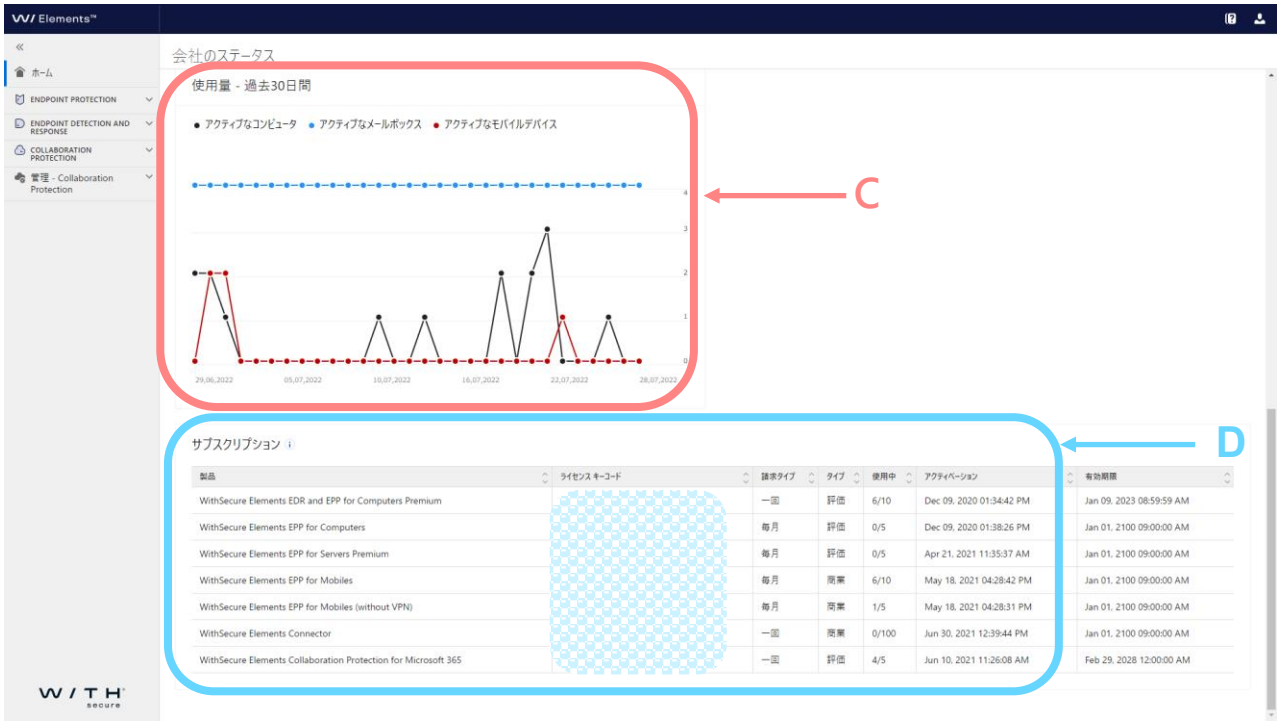
Elements Security Center から操作可能なアプリケーション毎にボタンが分けられています。

＊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

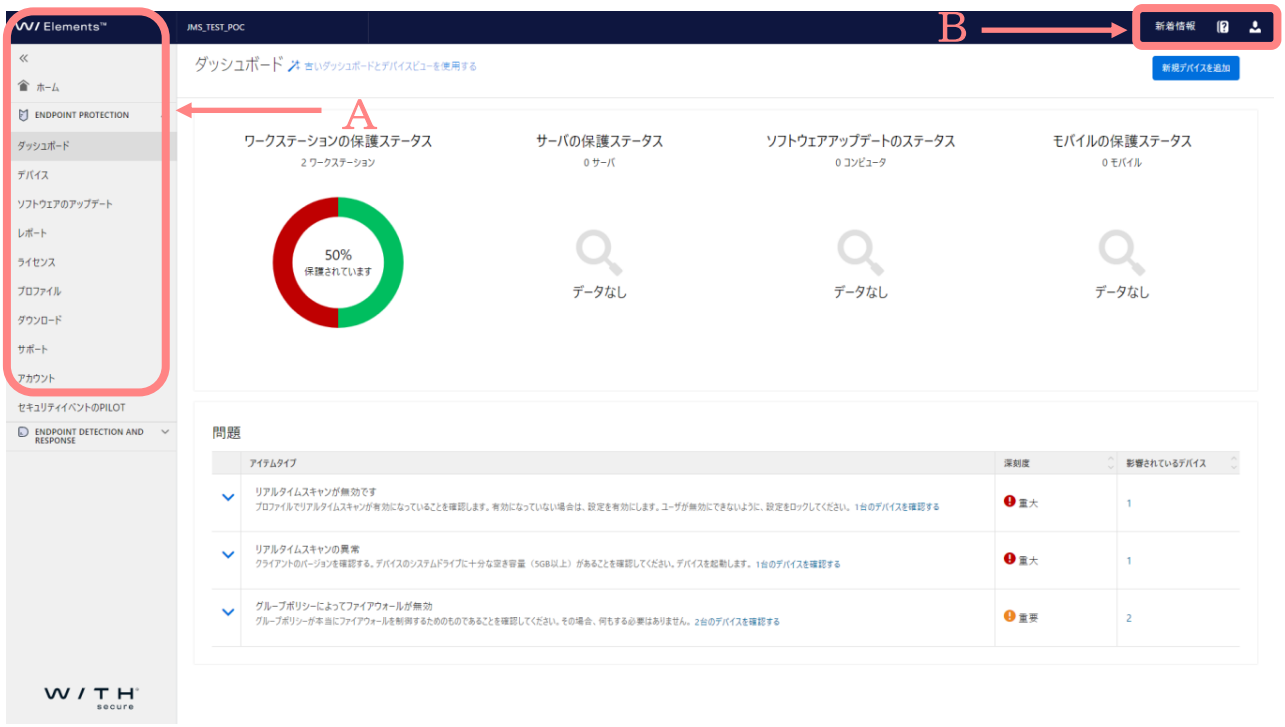
所用している、ライセンス情報とインスト－ルされている端末台数を確認できます。

5. Elements EPP の操作メニュー

ここでは、Elements Security Center にある Elements EPP の操作用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。



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。

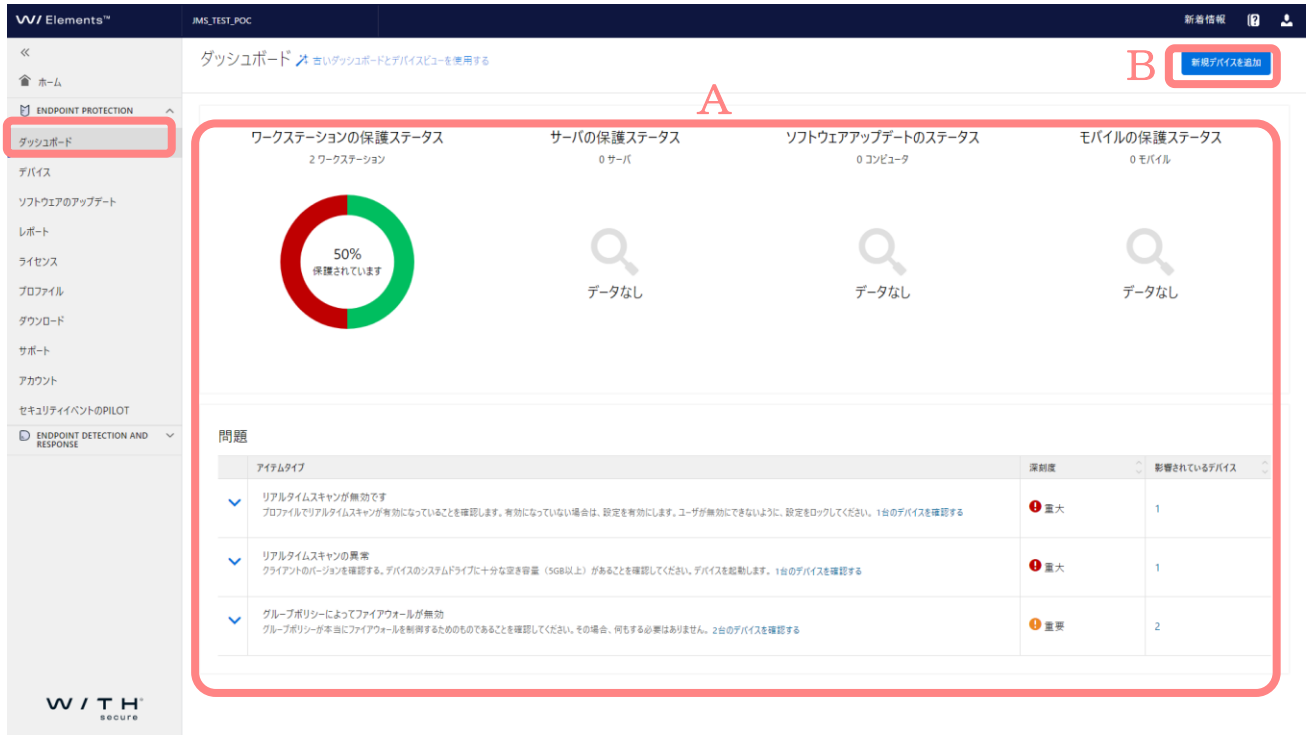
B.ユーザーアカウントメニュー

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、修正する必要の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。



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**

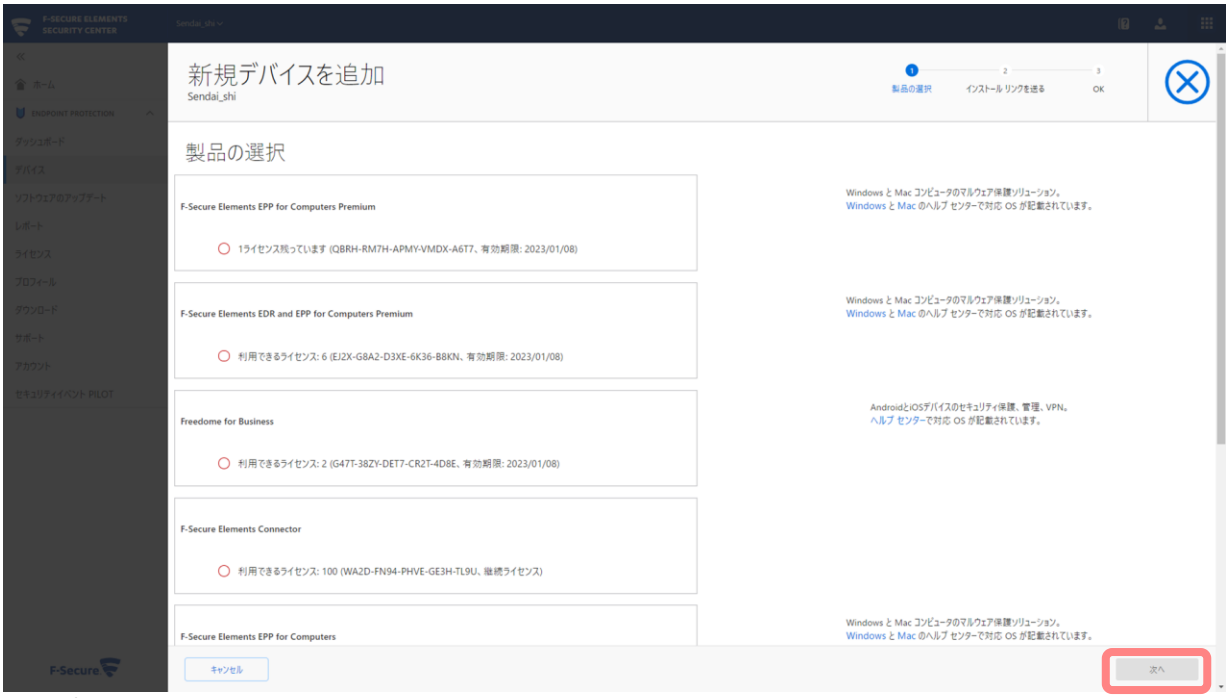
クリックするとデバイスを追加する[製品の選択]画面に移動します。

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。

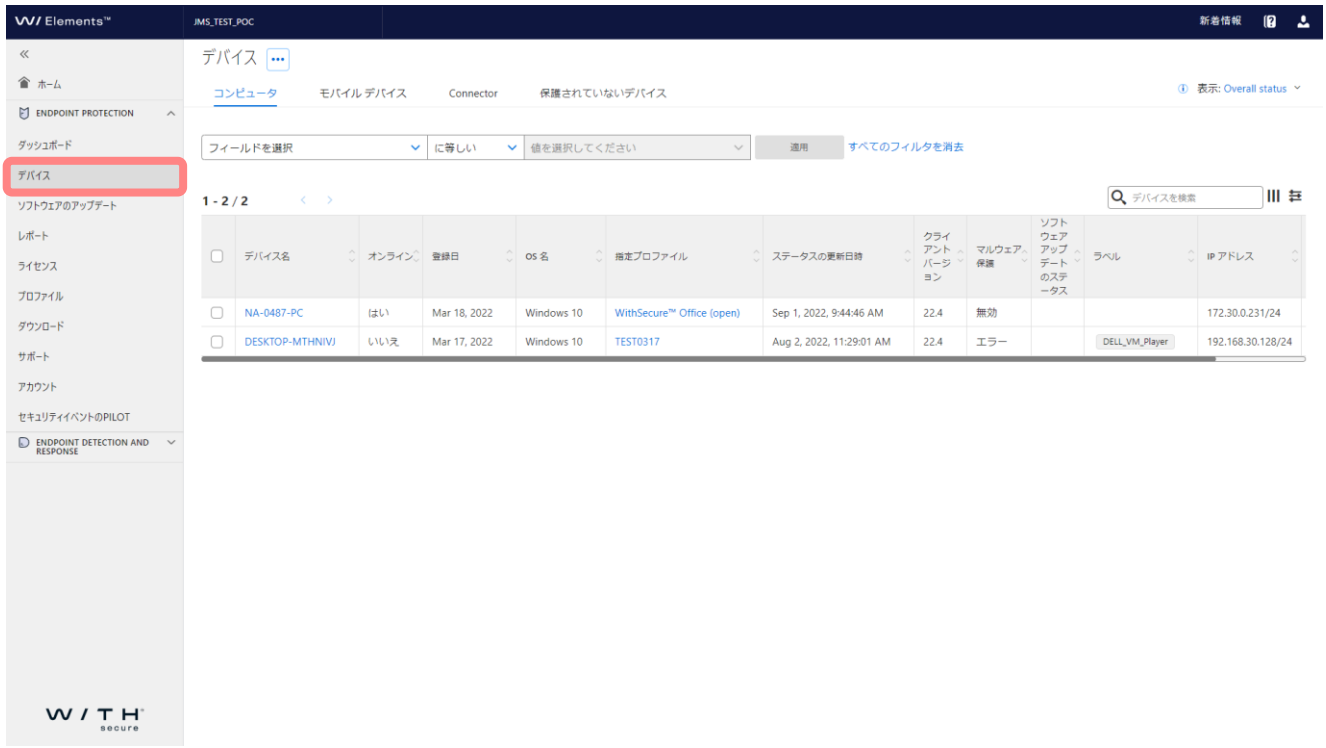
・送信先を CSV ファイルからインポートすることも可能です。

・[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。

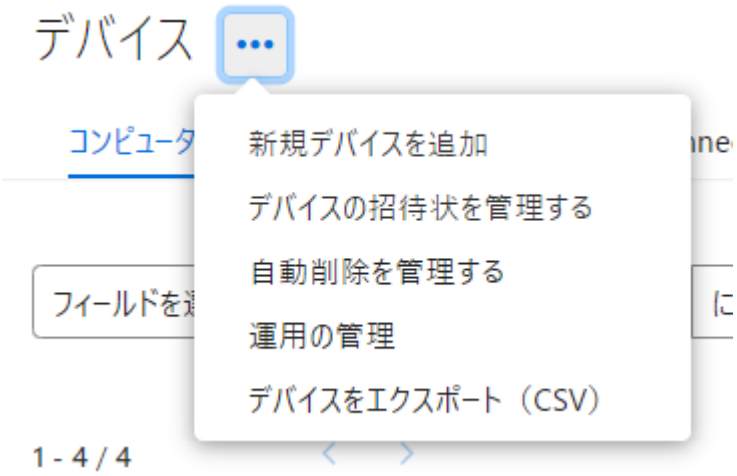
コンピュータ/モバイルデバイス/レガシーモバイルデバイス/Connector/保護されていないデバイスのタブを選択して、各デバイスの情報を表示します。

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

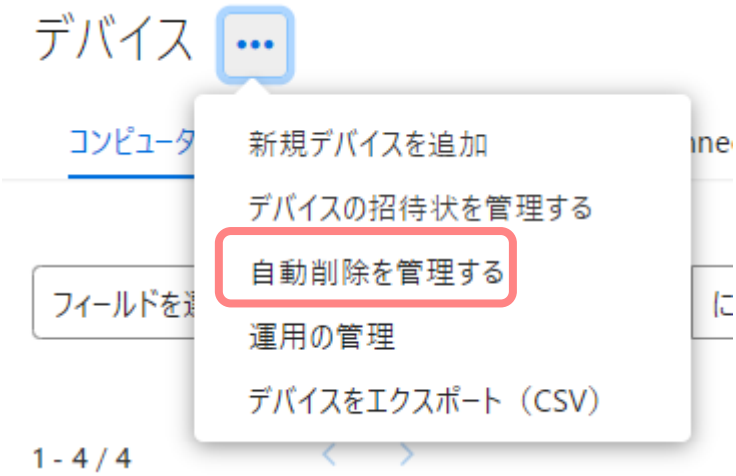
項目名	内容
新規デバイスを追加	[新規デバイスを追加]の画面に移動します。 5.3. 新規デバイスを追加 参照
デバイスの招待状を管理する	[デバイスの招待を管理する]の画面に移動します
自動削除を管理する	[自動削除を管理する]の画面に移動します。
運用の管理	[運用の管理]の画面に移動します。
デバイスをエクスポート（CSV）	コンピュータのレポートが CSV 形式でダウンロードされます。

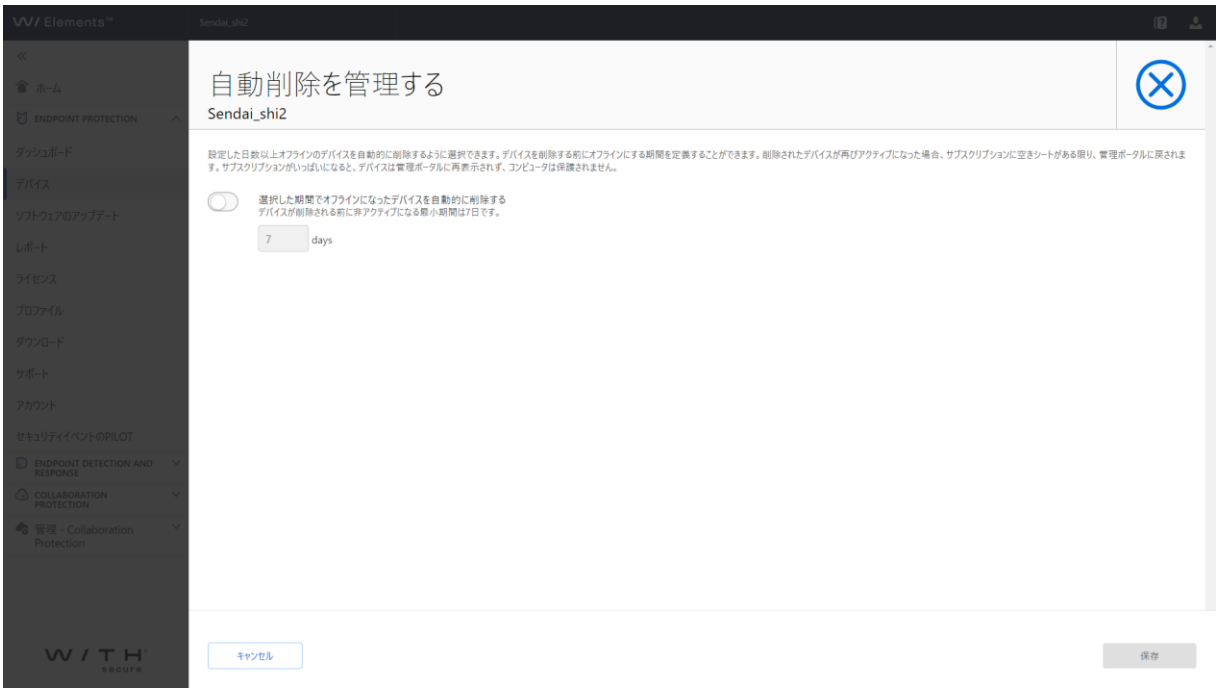
6.2.1. デバイスの招待状を管理する

新規デバイスを追加したに際の招待メールのステータスを管理します

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。

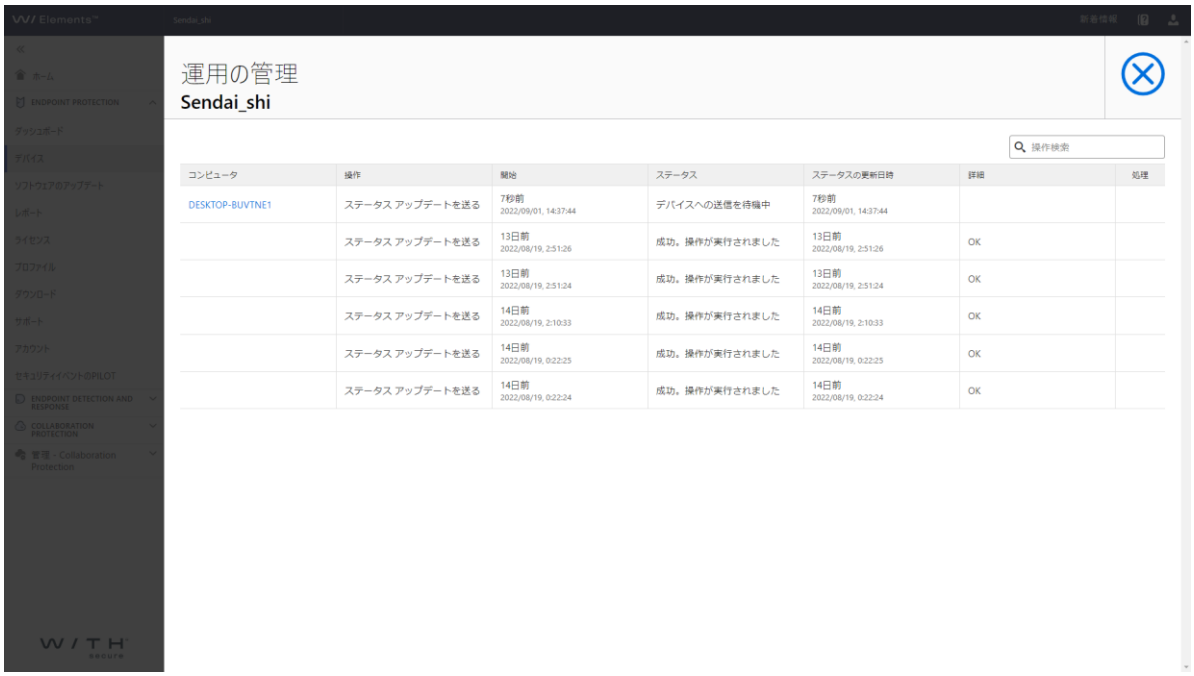




選択した期間でオフラインになったデバイスを自動的に削除することができます。

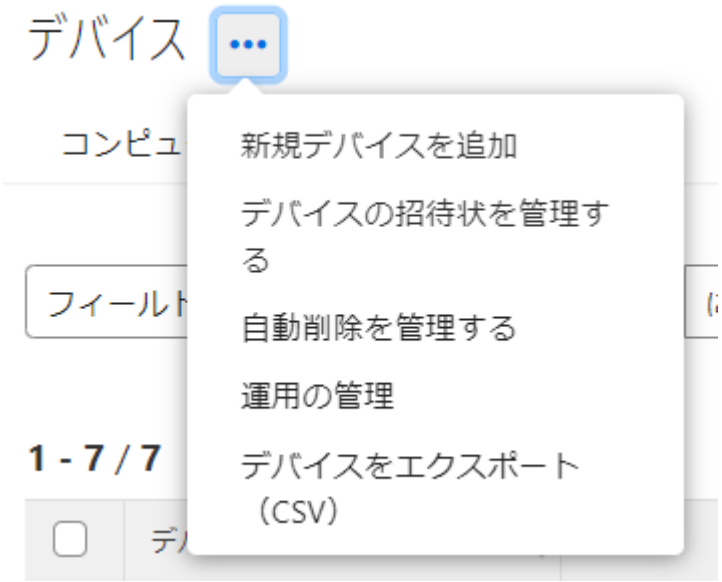
6.2.3. 運用の管理

端末への操作の履歴を確認できます



6.3. “モバイルデバイス” タブ アクションメニュー

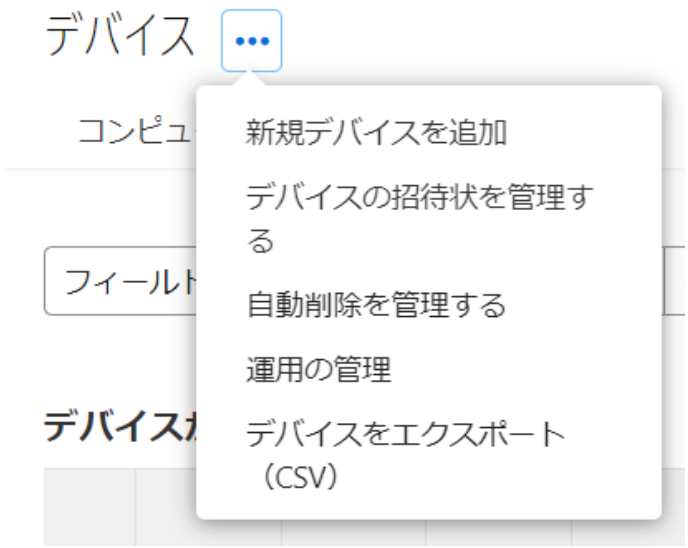
デバイスの右側にある[アクションメニュー]をクリックすると、デバイスの追加やインポート、エクスポートに関するメニューが表示されます。



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

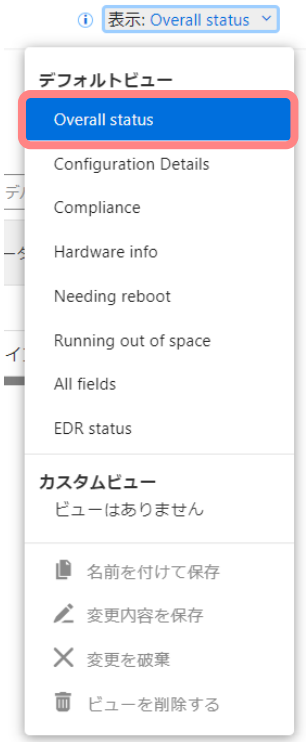
デバイスの右側にある[アクションメニュー]をクリックすると、デバイスの追加やインポート、エクスポートに関するメニューが表示されます。



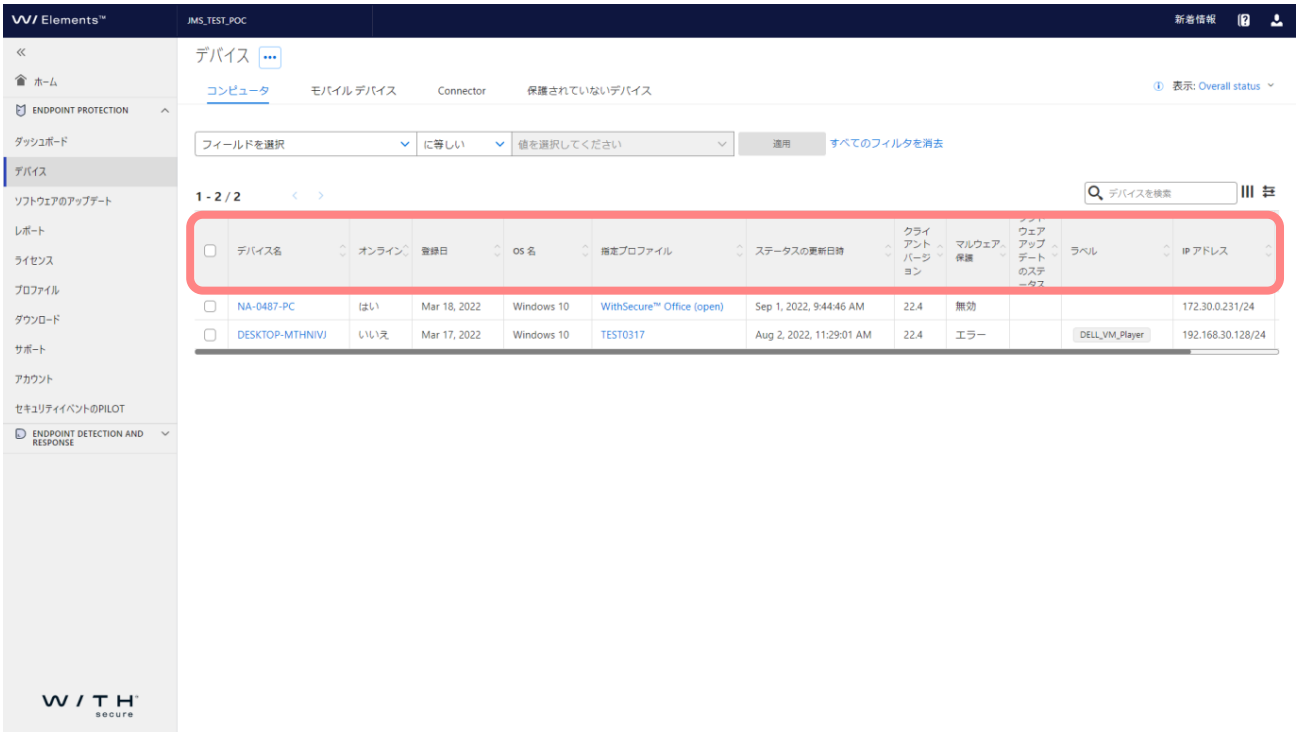
項目名	内容
新規デバイスを追加	[新規デバイスを追加]の画面に移動します。 5.3.　新規デバイスを追加　参照
デバイスの招待を管理する	[デバイスの招待状を管理する]の画面に移動します。 6.2.1.　デバイスの招待状を管理する　参照
自動削除を管理する	[自動削除を管理する]の画面に移動します。 6.2.2.　自動削除を管理する　参照
運用の管理	端末への操作の履歴を確認できます 6.2.3.　運用の管理　参照
デバイスをエクスポート(CSV)	Connector のレポートが CSV 形式でダウンロードされます。

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



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]

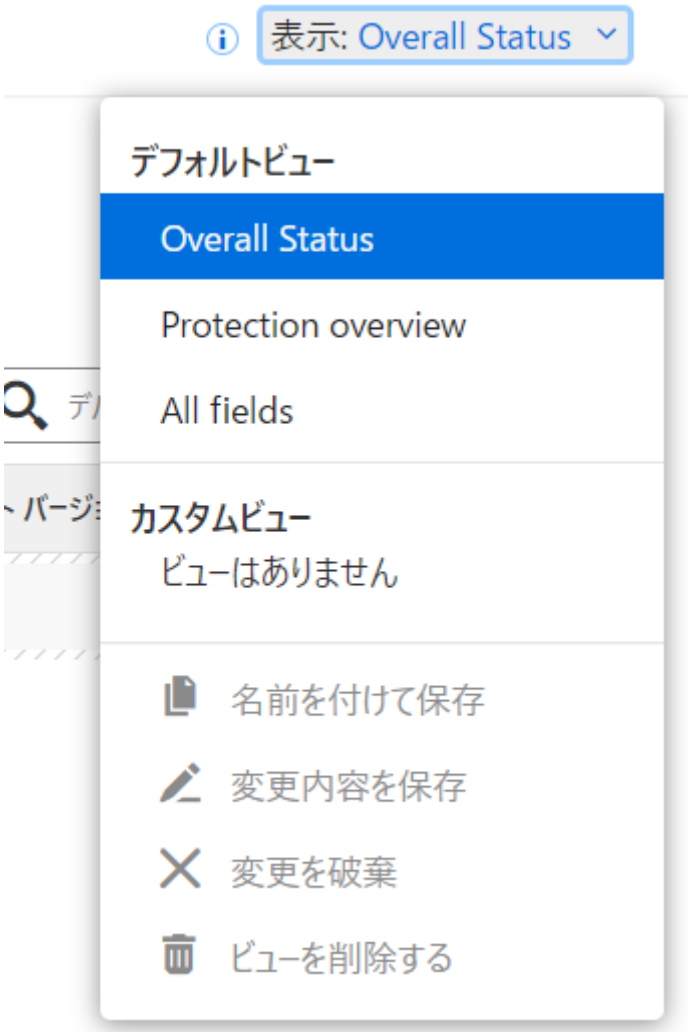
すべての項目を表示します

[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]

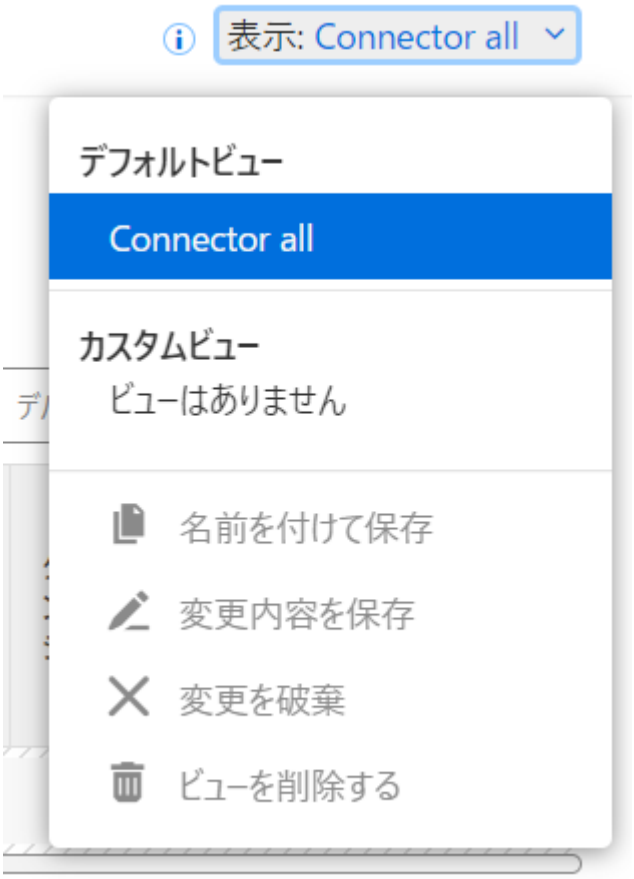
保護した概要に関する項目の情報を表示します。

[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。

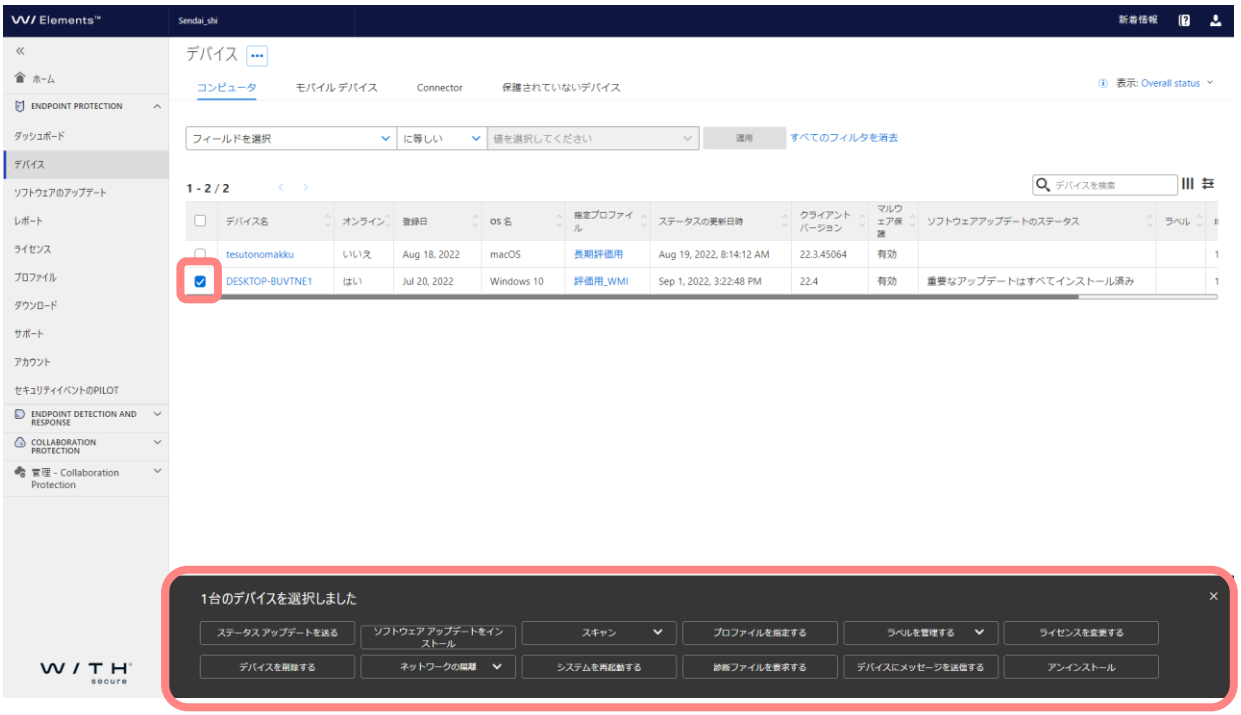
表示メニュー

[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出来ます。



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。

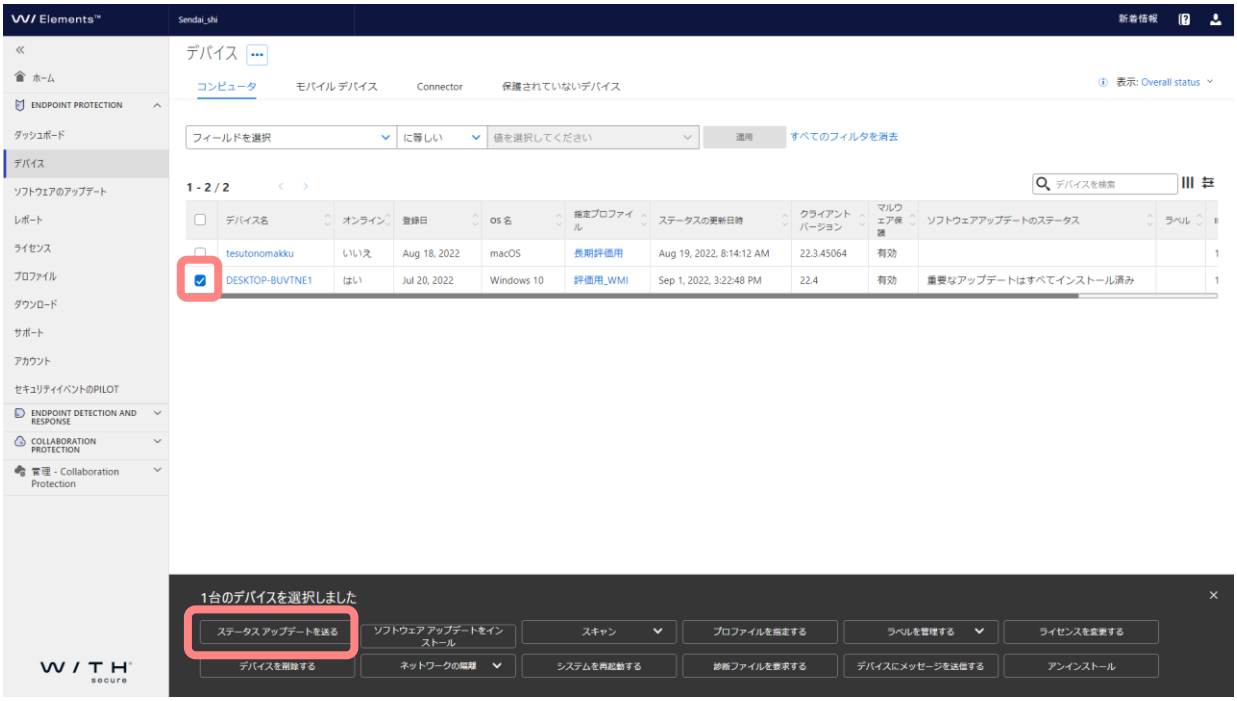
処理ボタン

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	ソフトウエ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エ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。

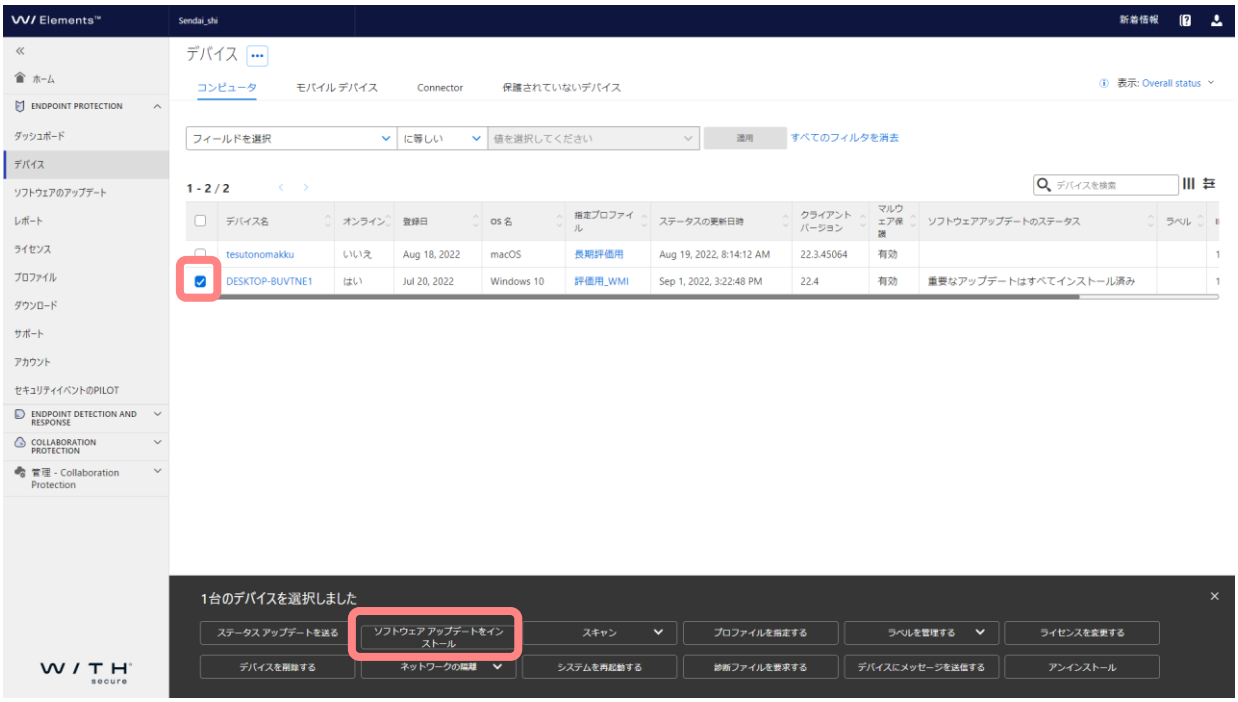


①対象となるコンピュータをチェックボックスで指定します。

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。

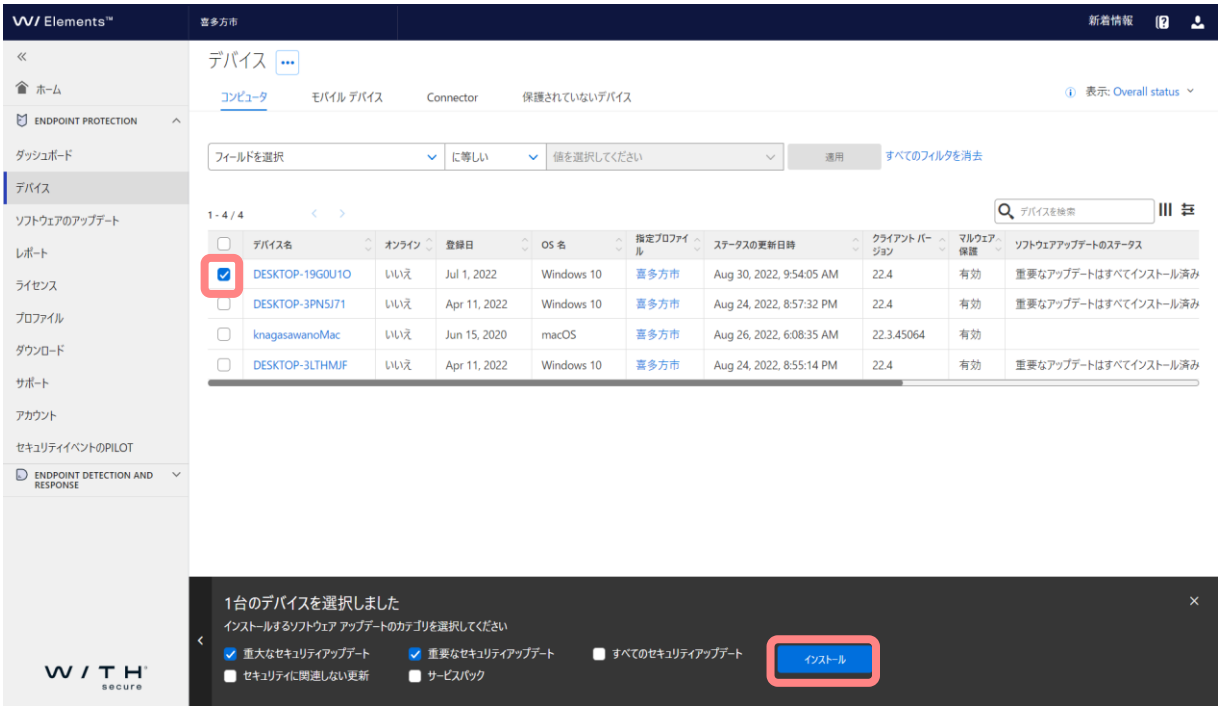


①対象となるコンピュータをチェックボックスで指定します。

②[ソフトウエア アップデートをインストール] ボタンを押します。

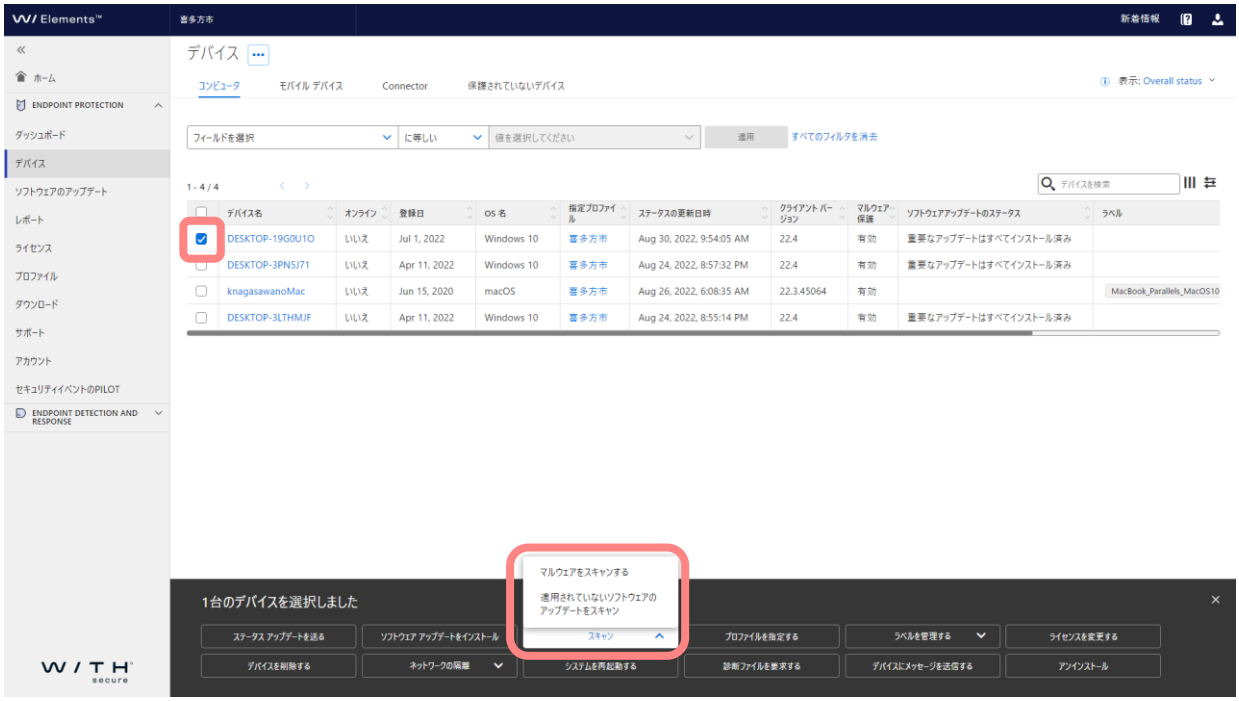
③メニューが表示されるので、インストールするソフトウェアアップデートのカテゴリを選択します。

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エアのアップデートのスキャンを実行させることが出来ます。

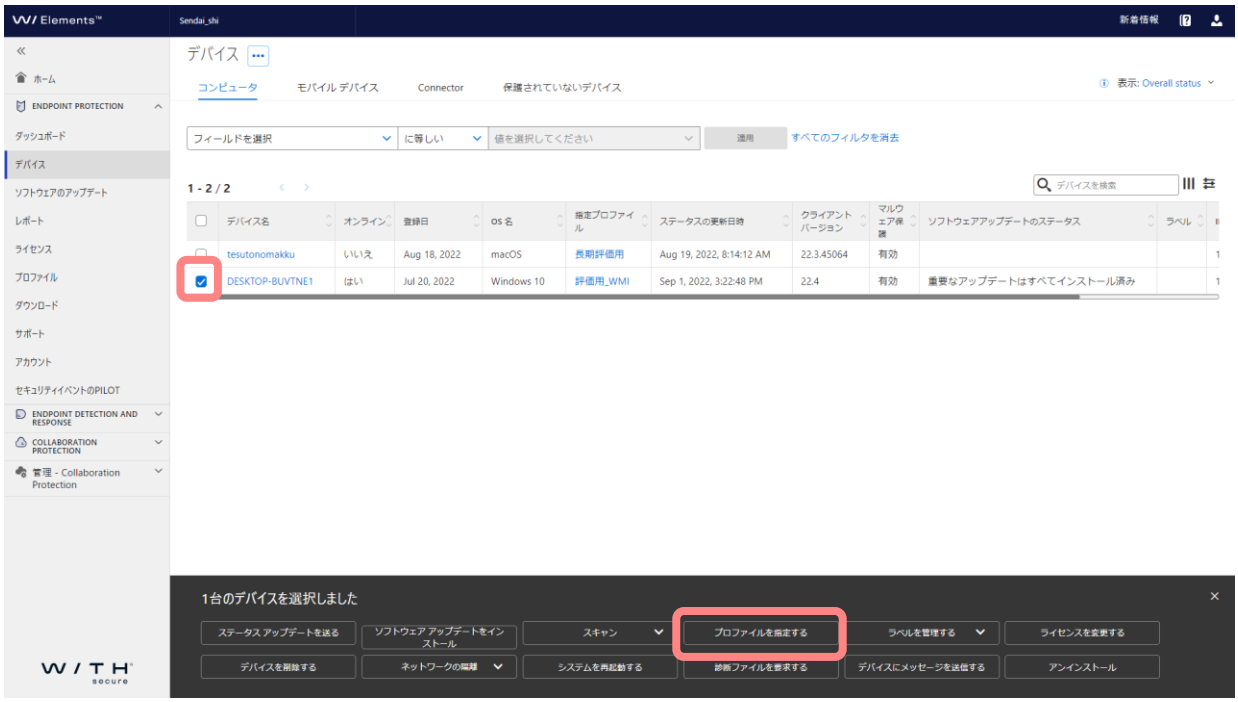


①対象となるコンピュータをチェックボックスで指定します。

②[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エ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

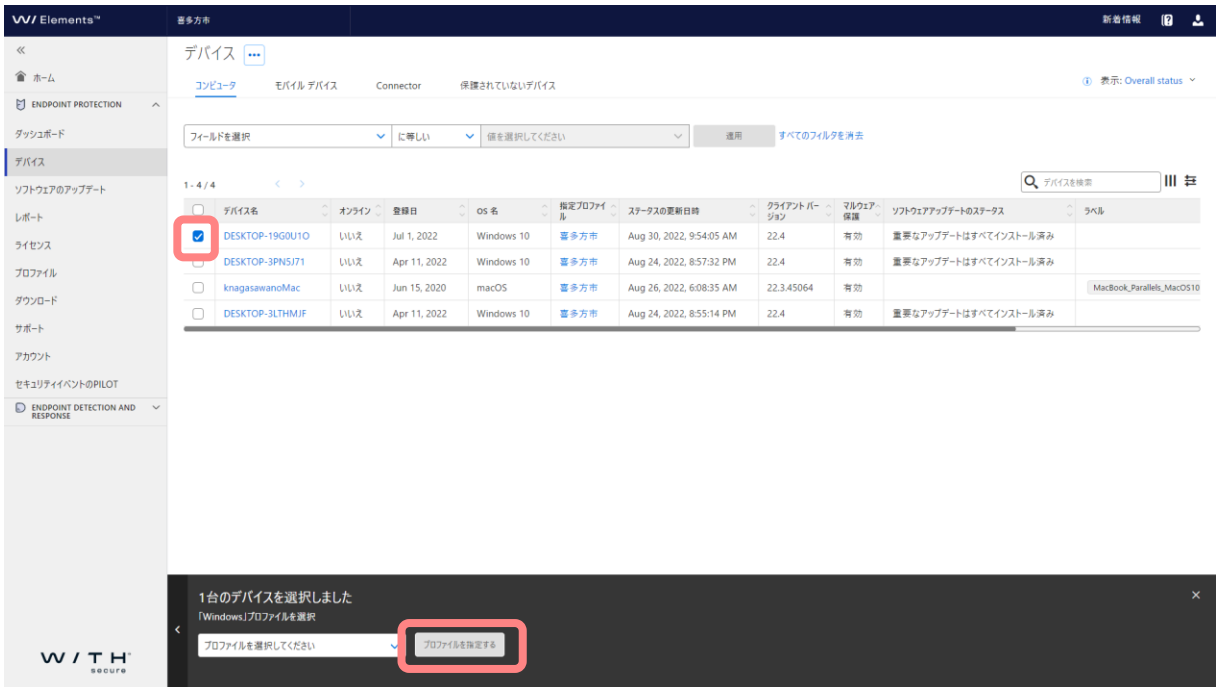
任意のコンピュータに対して、プロファイルを指定します。



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。

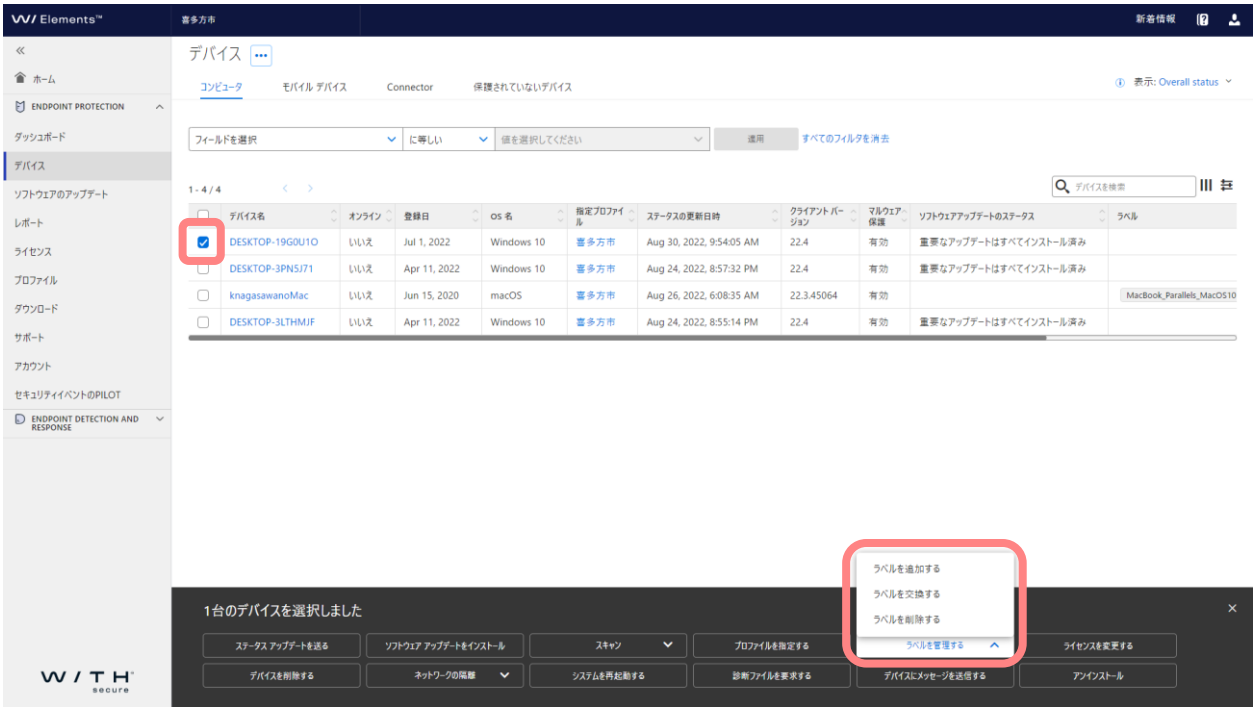
②[プロファイルを指定する]を選択します。

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。

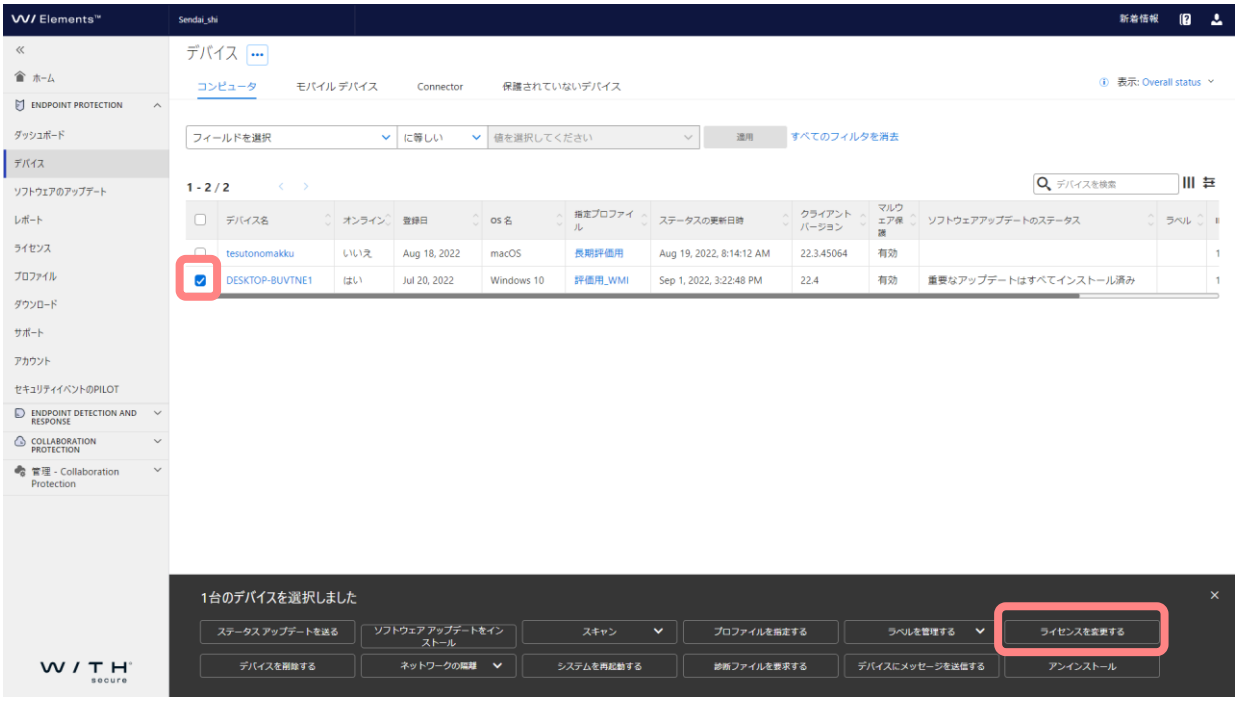


①対象となるコンピュータをチェックボックスで指定します。

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。

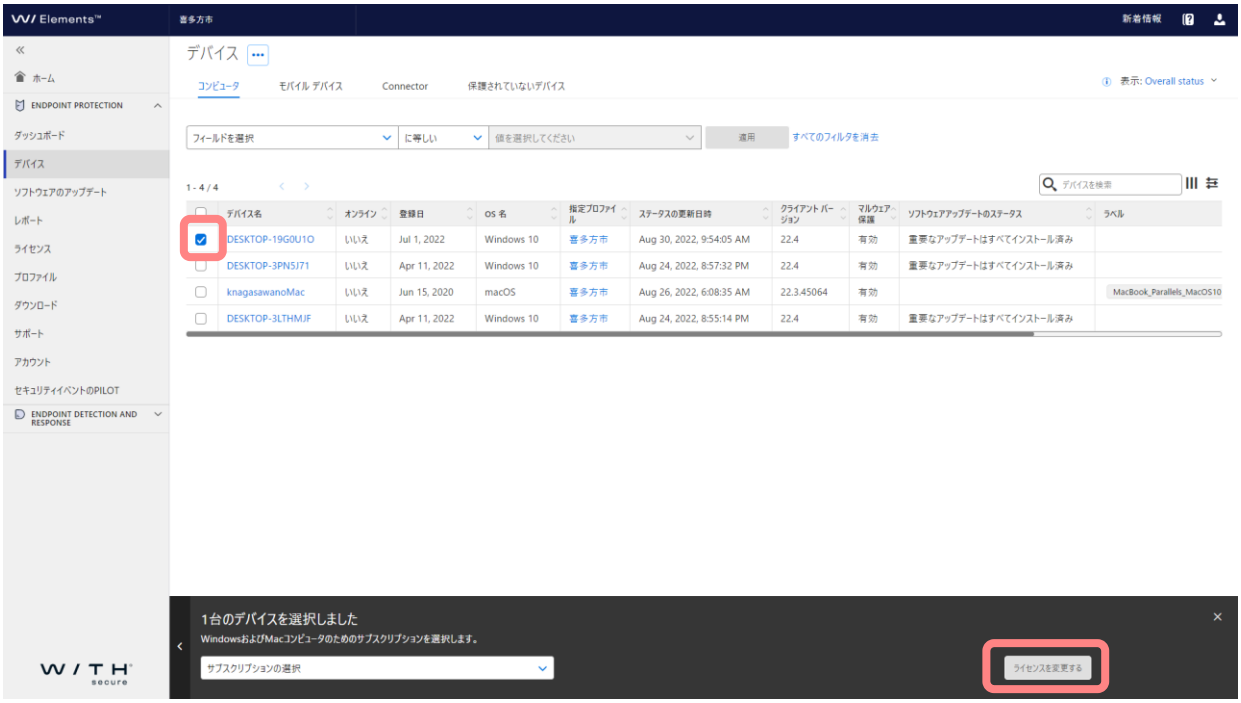
7.2.6. ライセンスを変更する

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。



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。

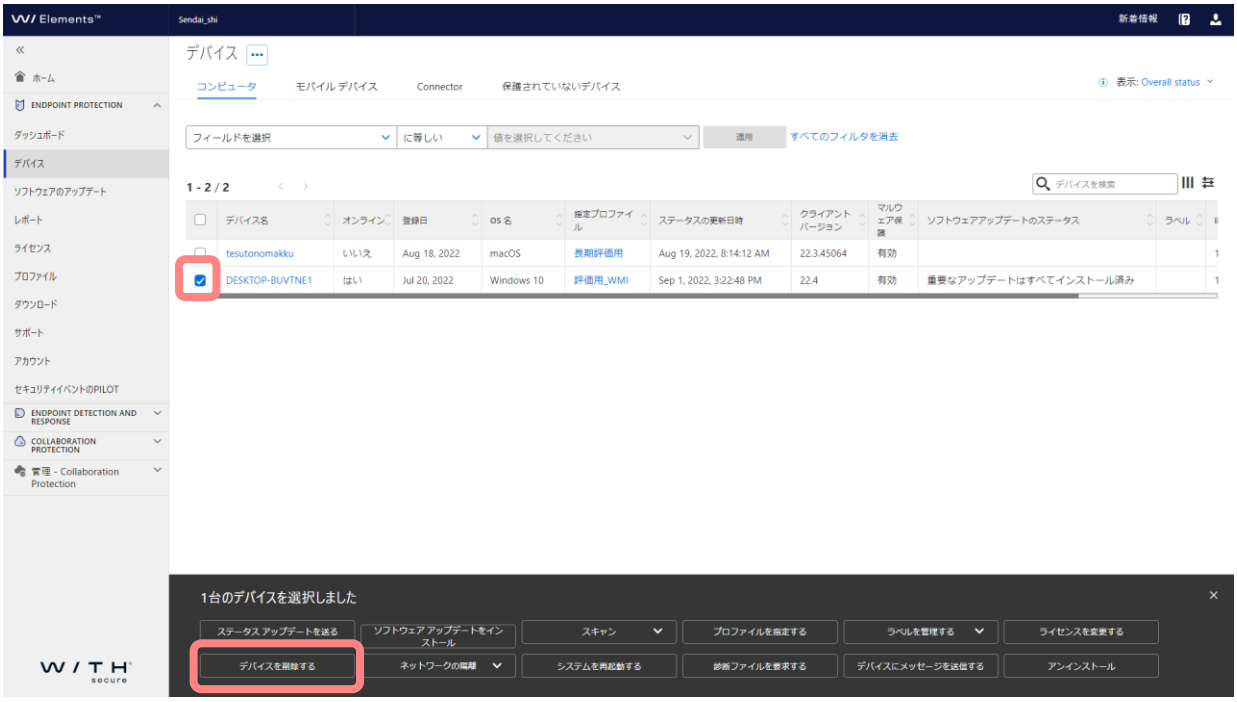


③新しいキーコードを入力または、別のキーコードを選択します。

④[ライセンスを変更する] ボタンをクリックします。

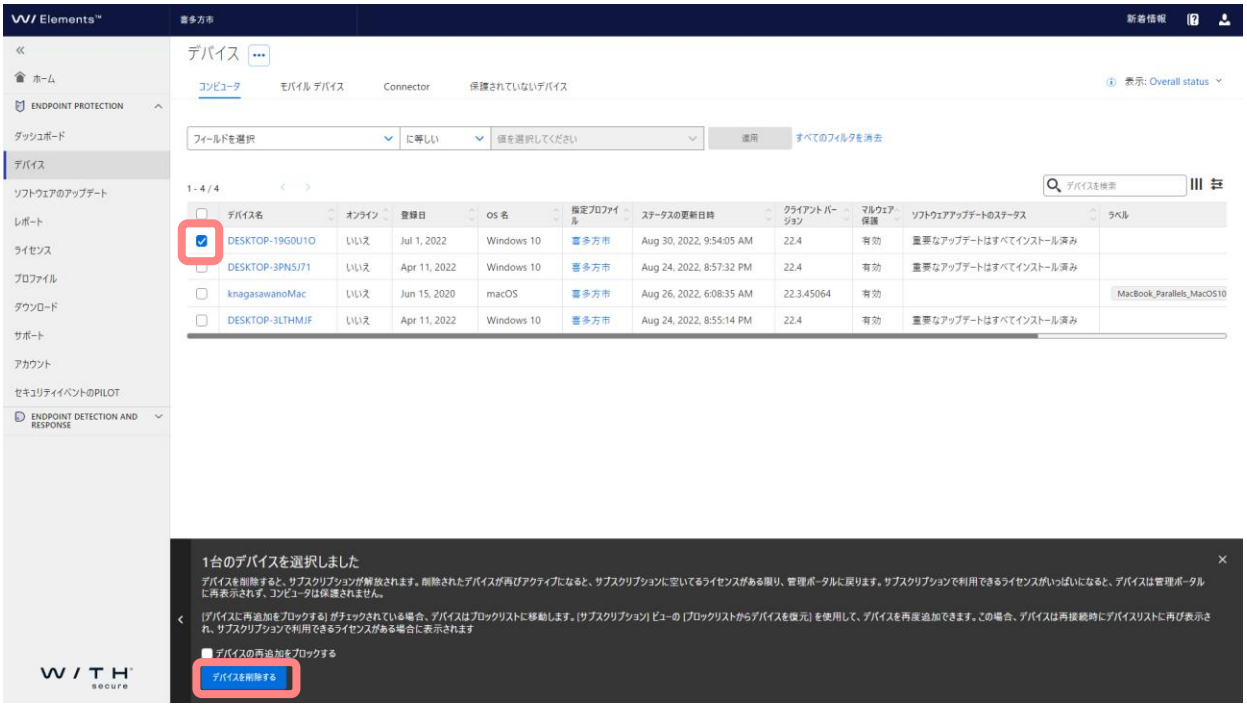
7.2.7. デバイスを削除する

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。



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。

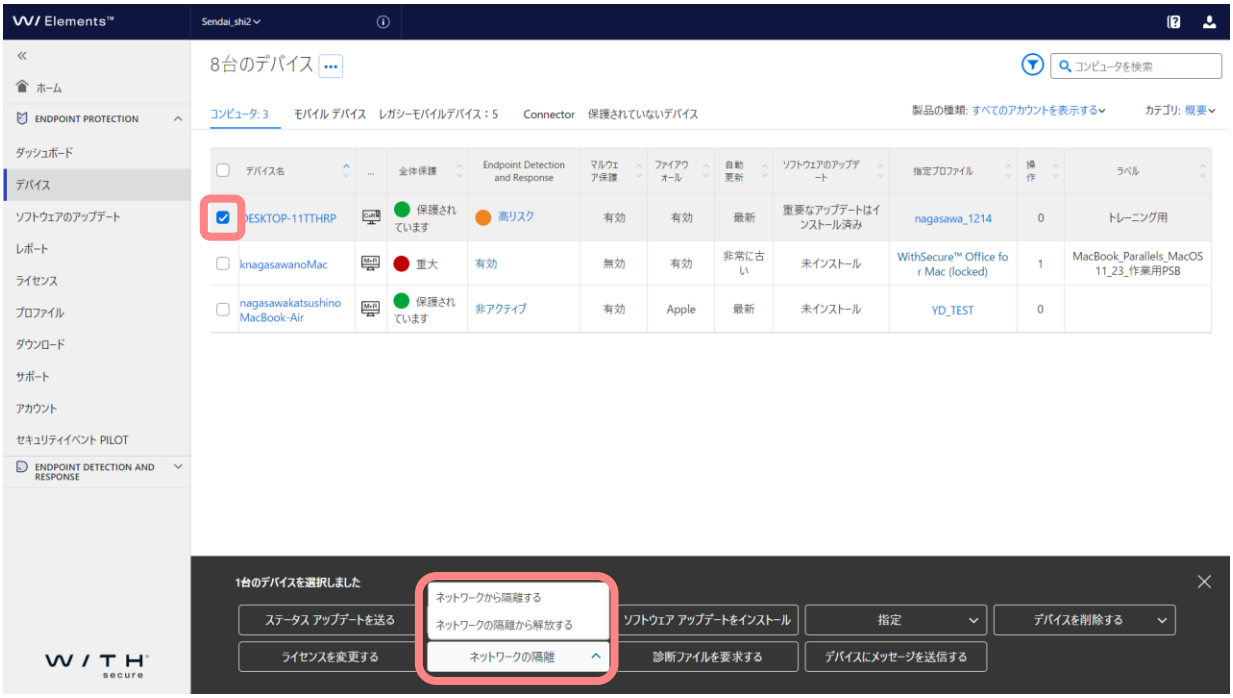
②[デバイスを削除する] ボタンをクリックします。



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



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

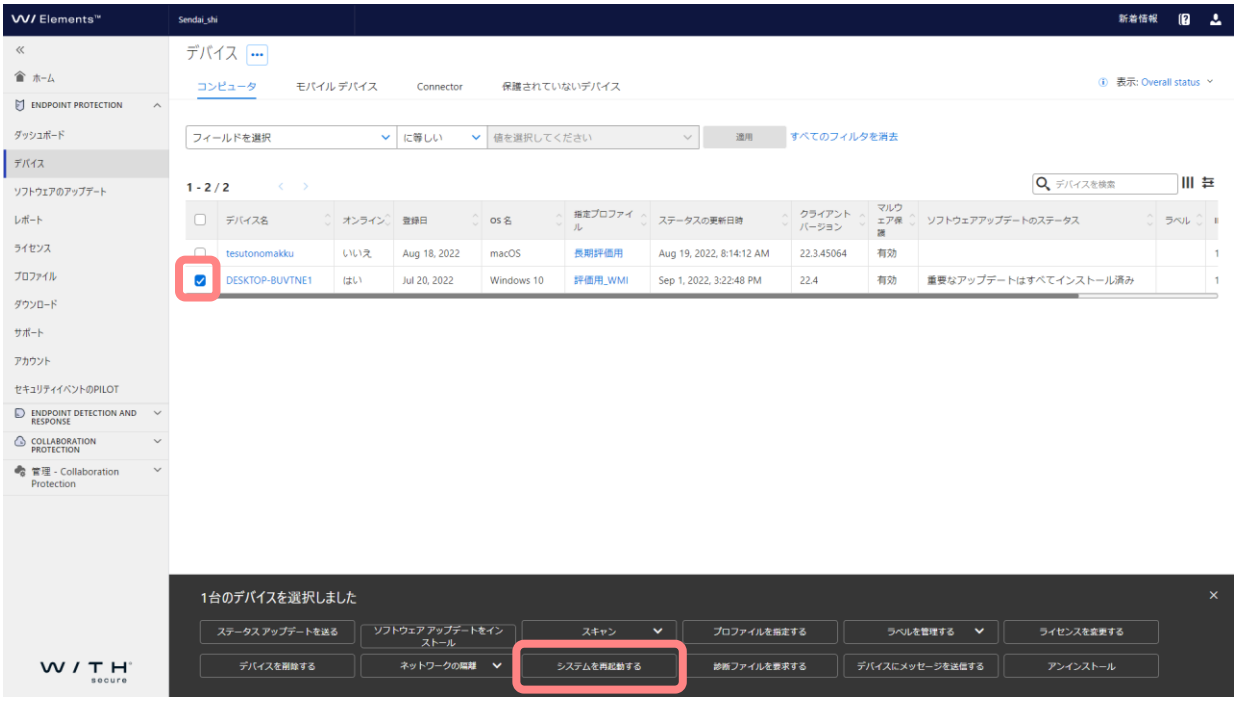
①対象となるコンピュータをチェックボックスで指定します。

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

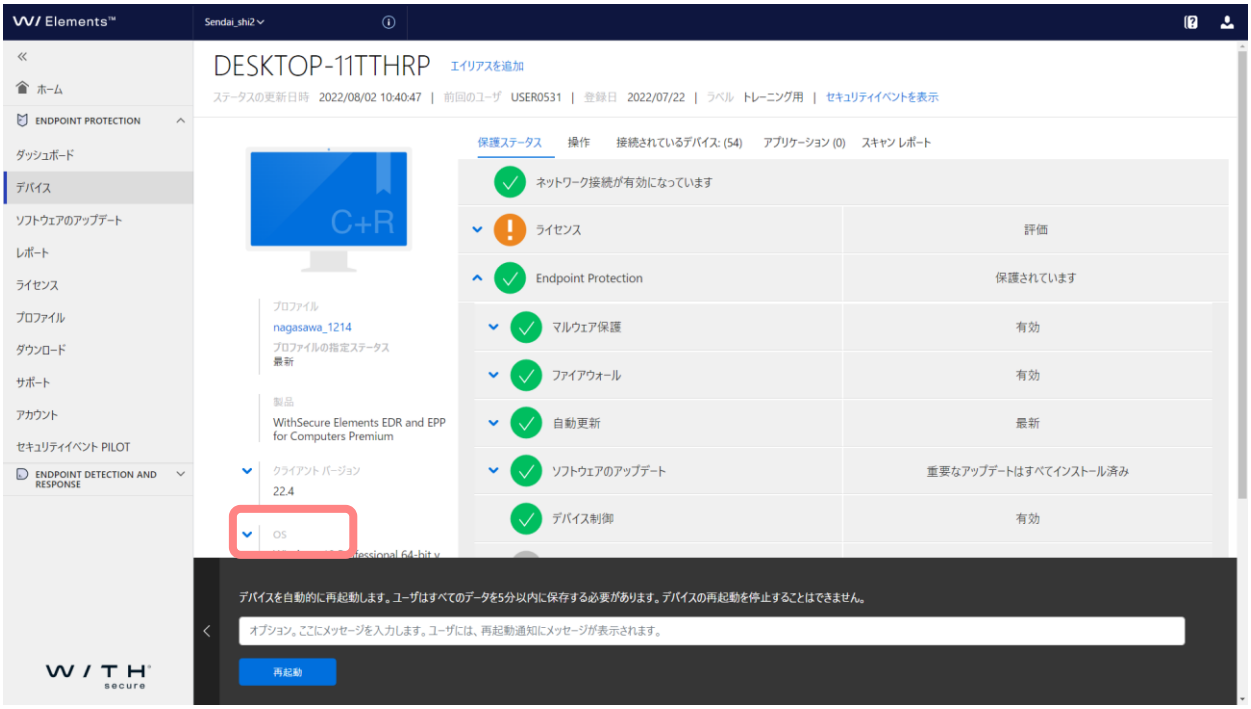
Windows の端末に限り、デバイスの再起動を実行させることが可能です。

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。

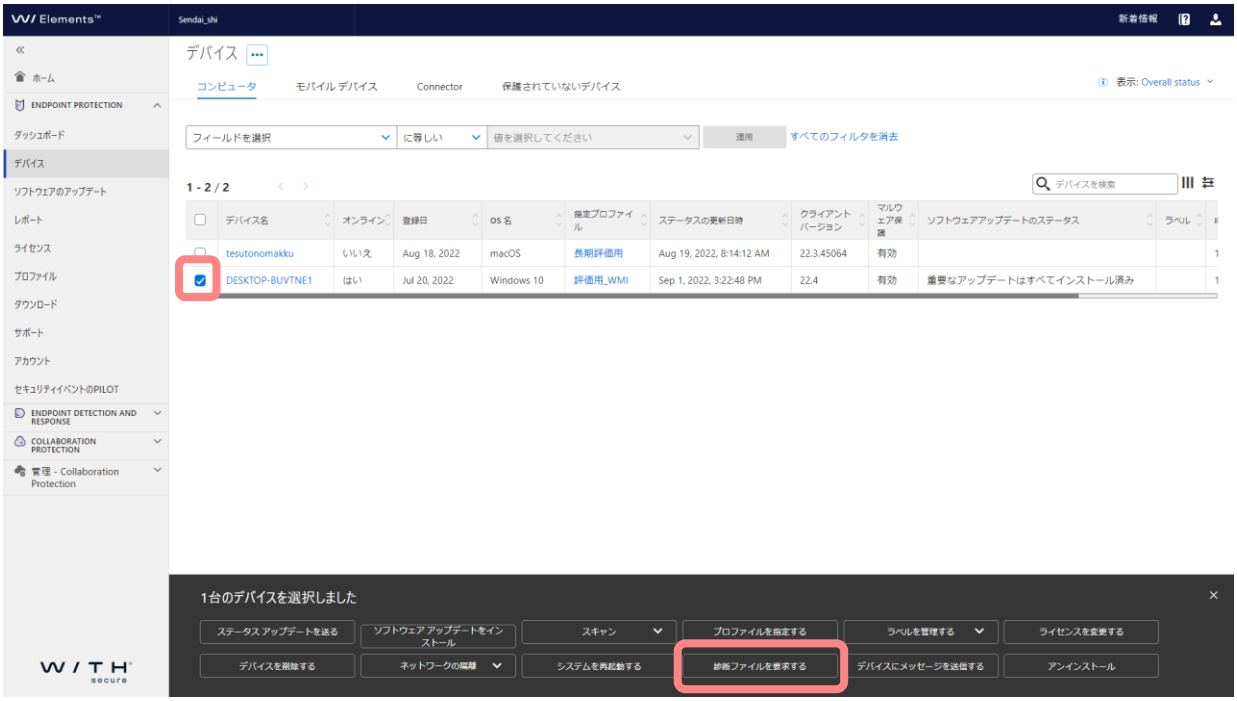


①対象となるコンピュータをチェックボックスで指定します。

②[システムを再起動する] ボタンをクリックします。



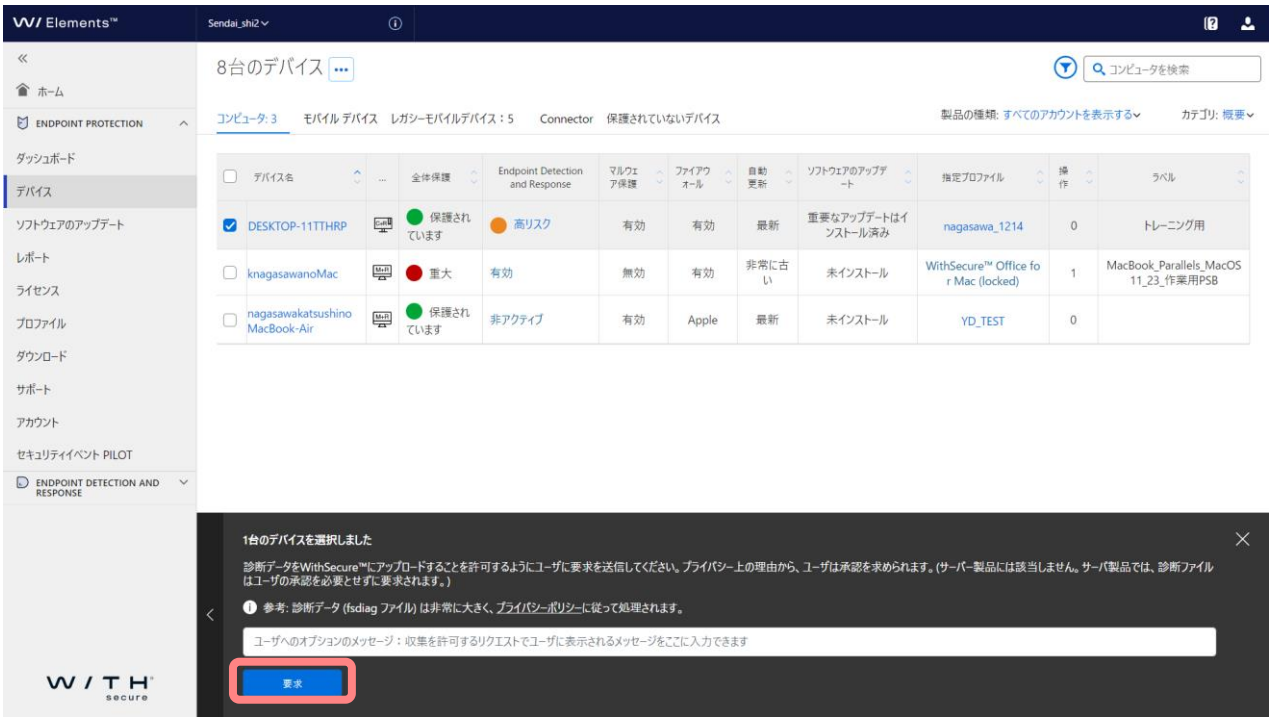
7.2.10. 診断ファイルを要求する



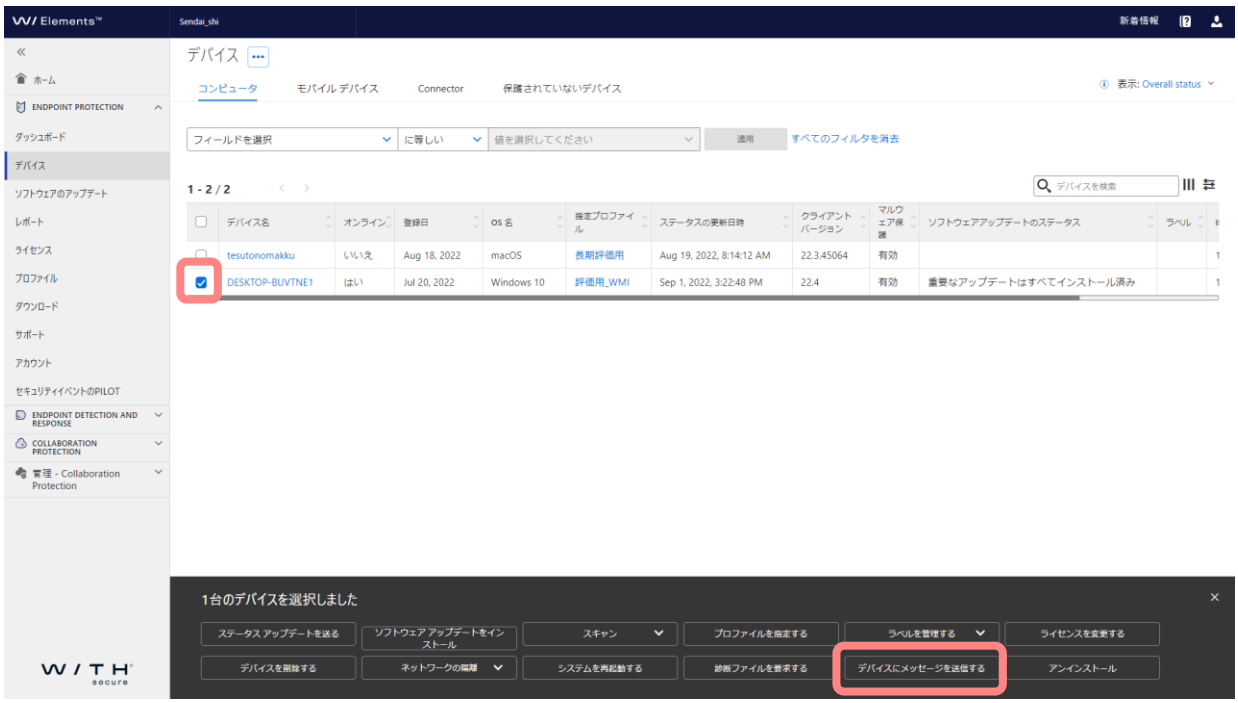
①対象となるコンピュータをチェックボックスで指定します。

②[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。



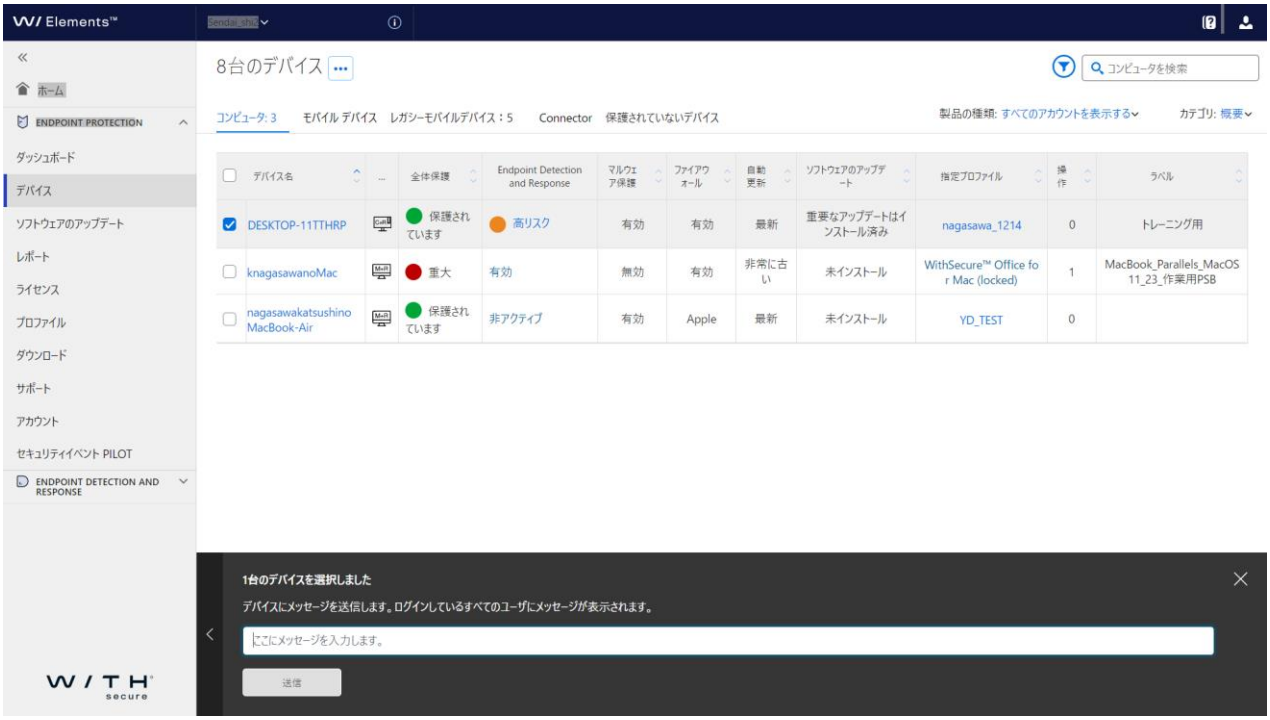
7.2.11. デバイスにメッセージを送信する



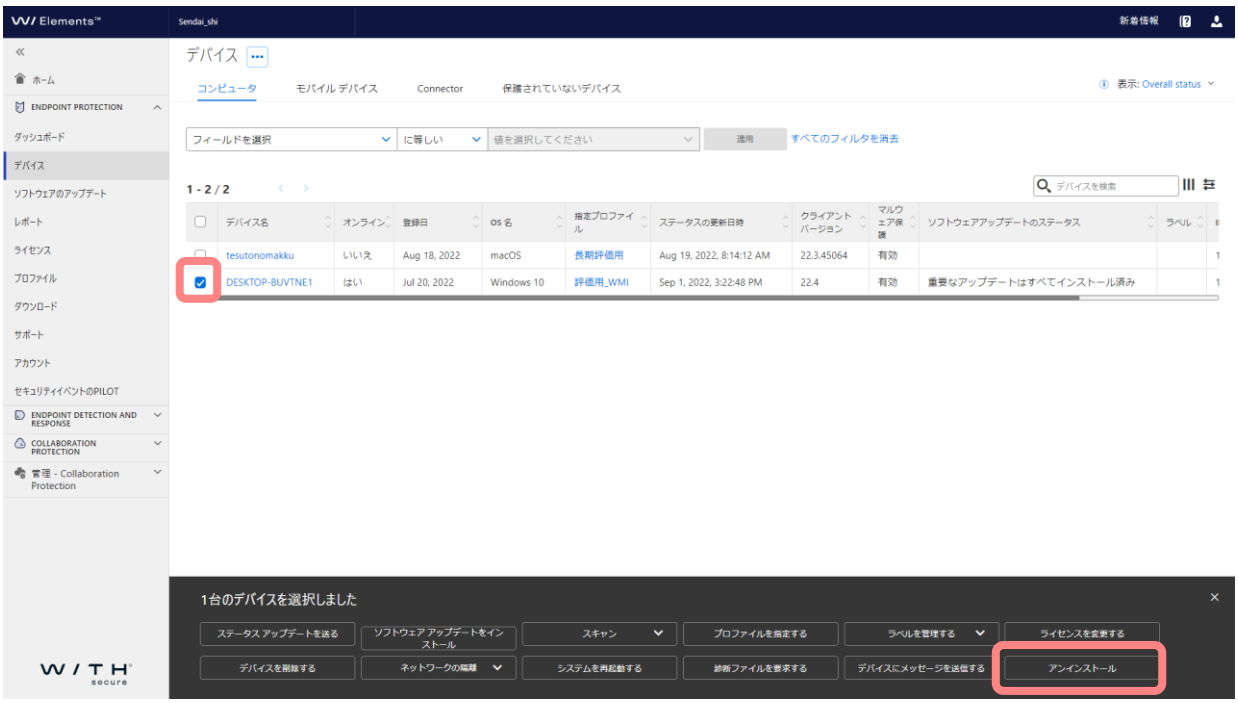
①対象となるコンピュータをチェックボックスで指定します。

②[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。

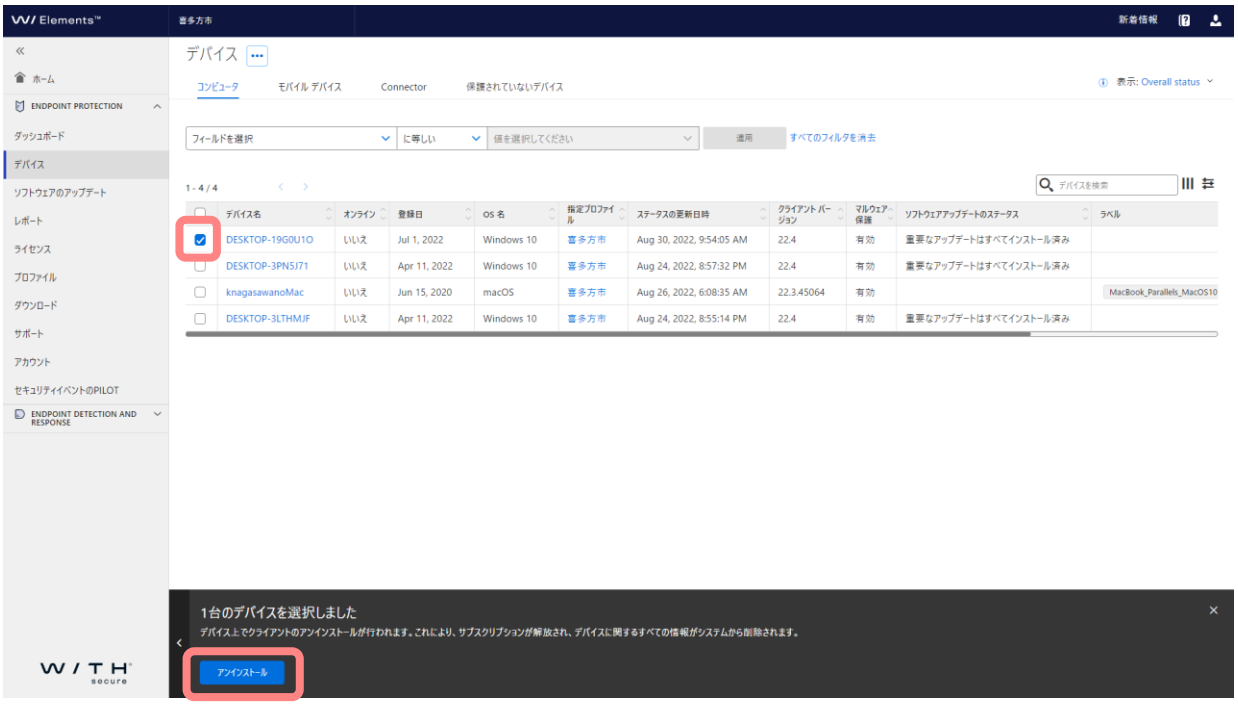


7.2.12.　アンインストール



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。

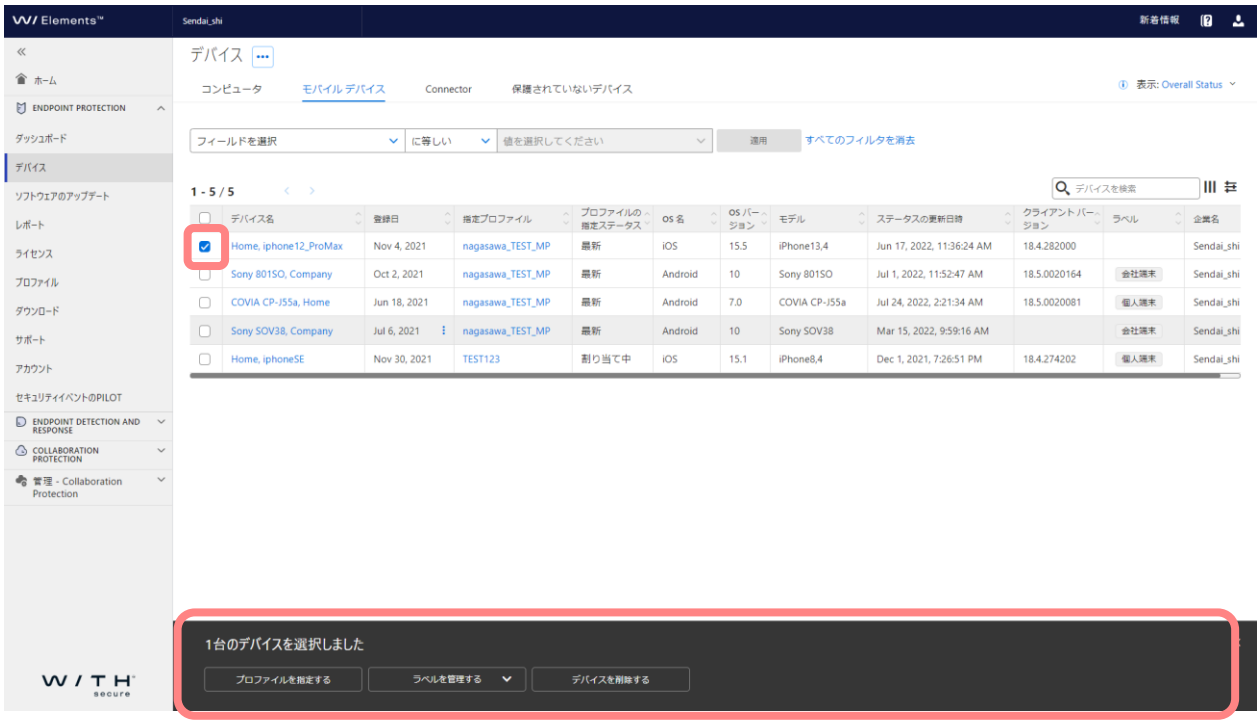
②[アンインストール] ボタンをクリックします。



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出来ます。



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

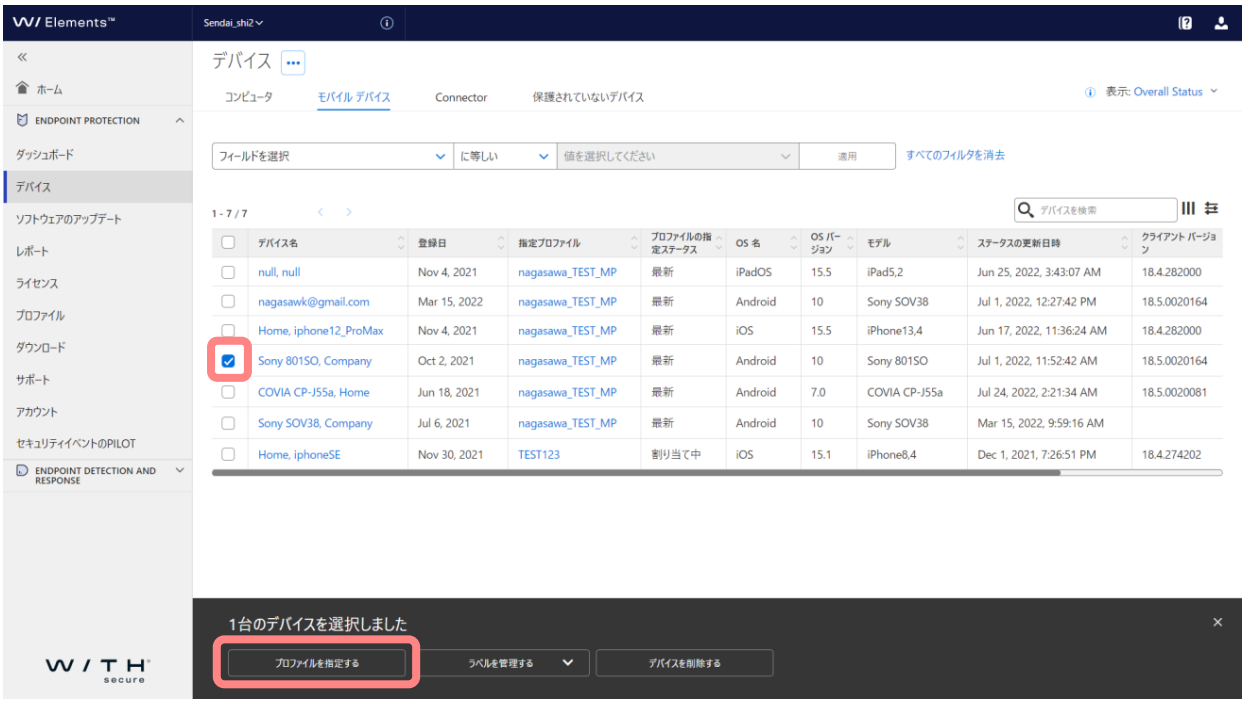
処理ボタン

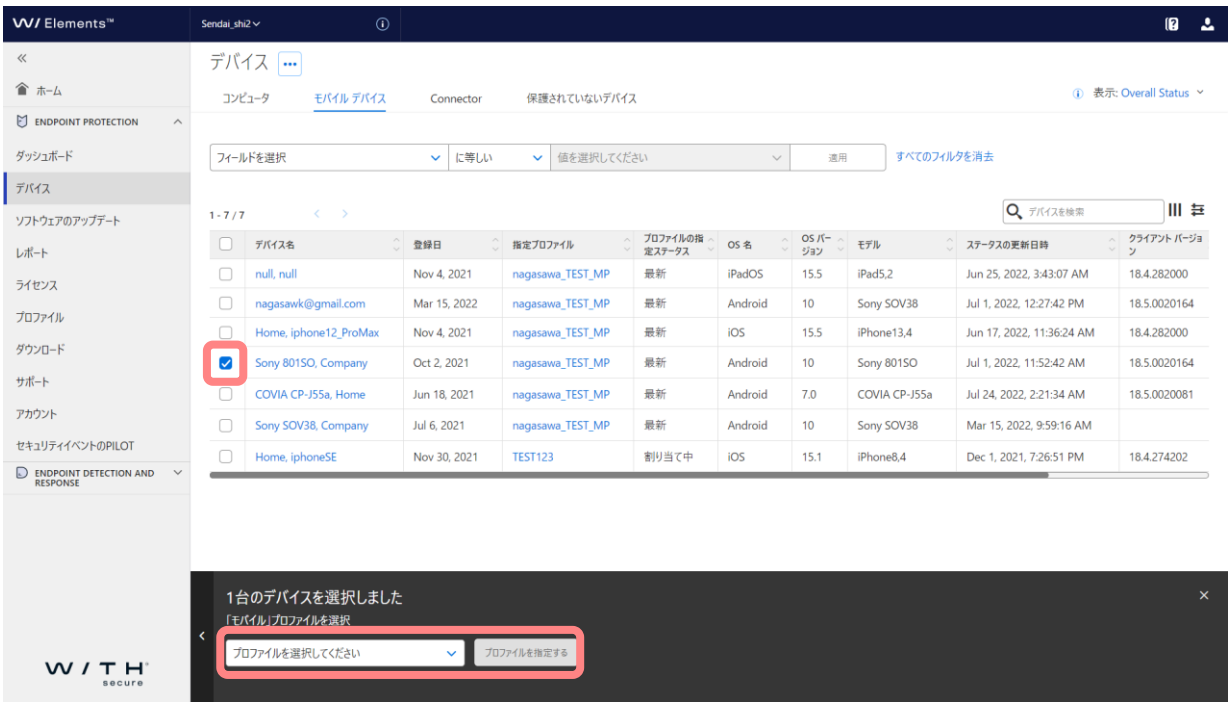
項目名	内容
プロファイルを指定する	デバイスにプロファイルまたはラベルを指定します。
完全に取り除く	デバイスをブロックリストに移動または完全に削除します。
ラベルを管理する	デバイスにラベルを指定します。

8.2. 処理内容

8.2.1. プロファイルを指定する

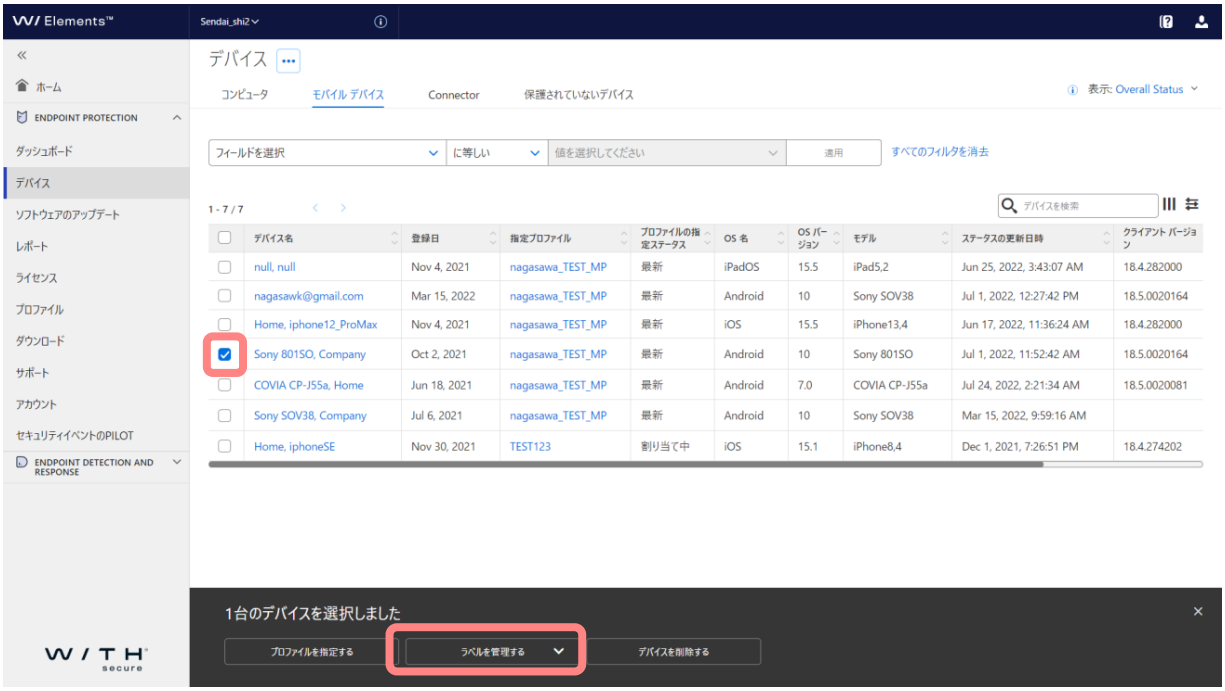
任意のモバイルデバイスに対して、プロファイルまたはラベルを指定します。

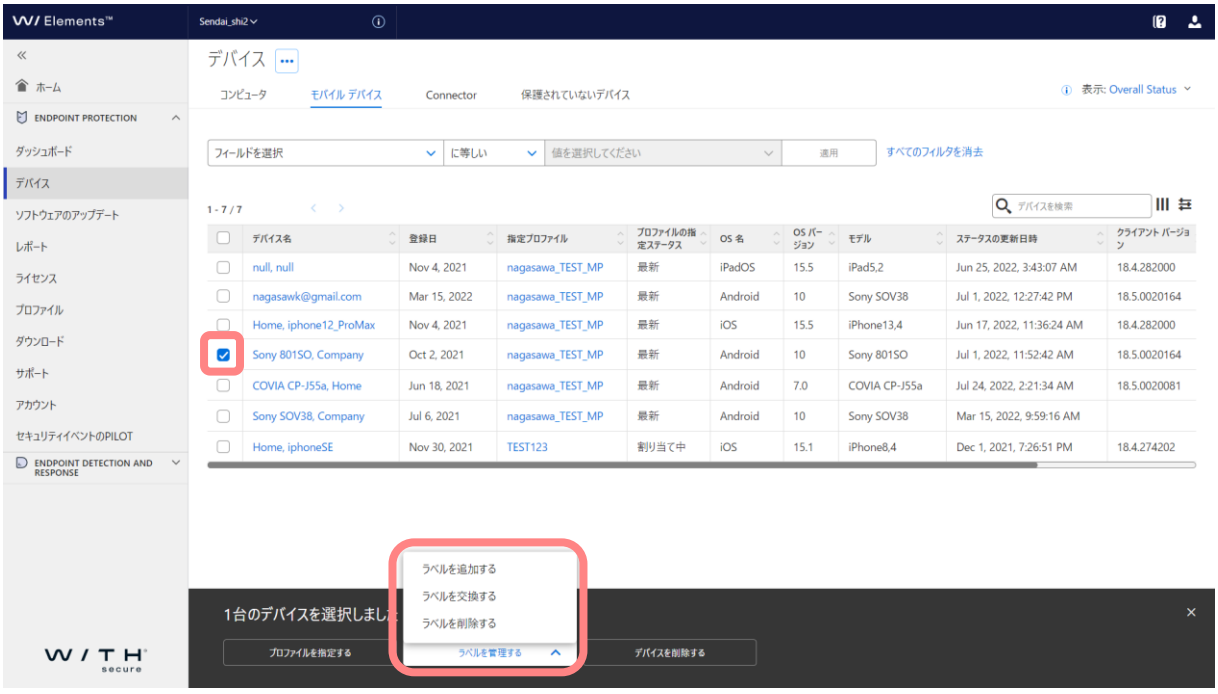




8.2.2. ラベルを管理する

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。



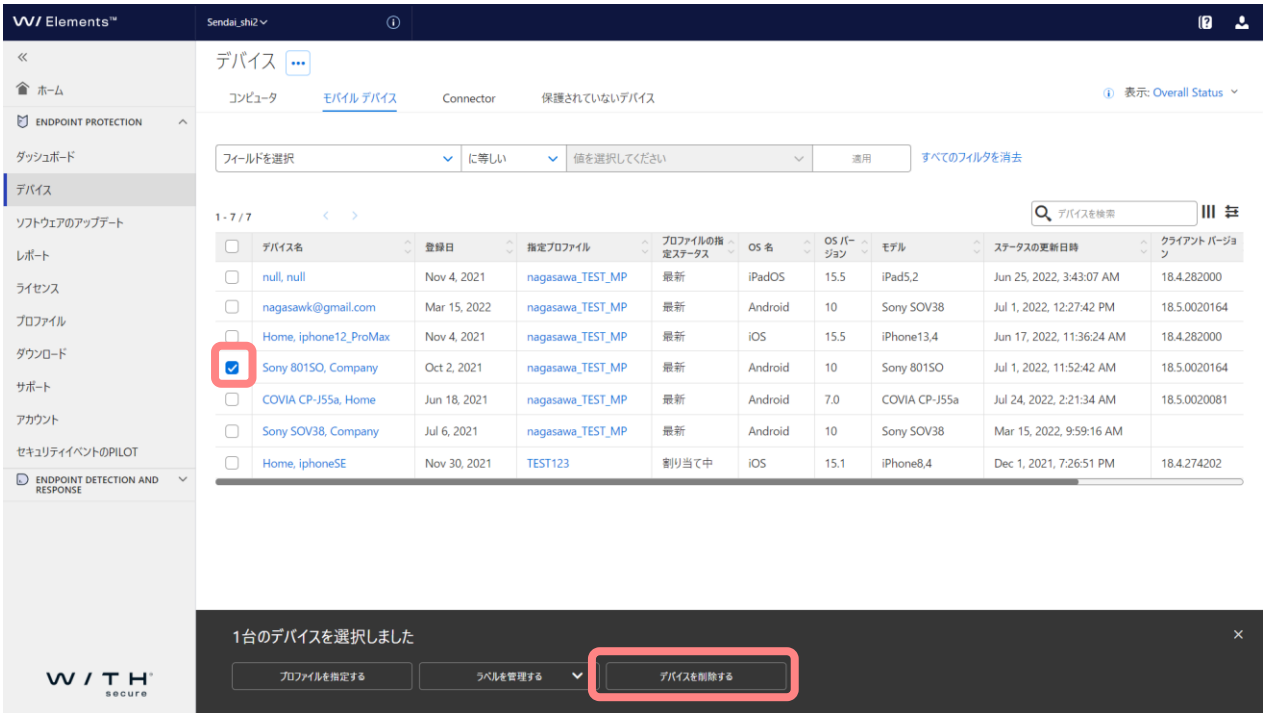


ラベルを管理する

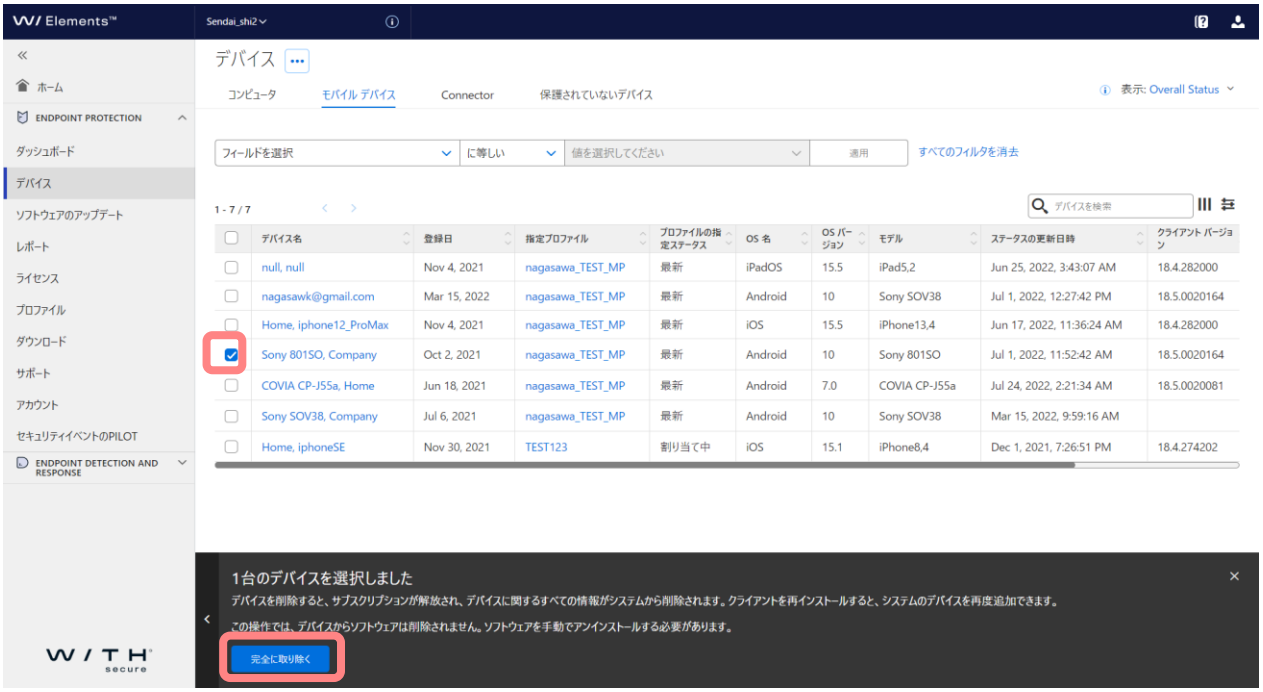
項目名	内容
ラベルを追加する	デバイスに追加するラベルを作成または選択します
ラベルを交換する	デバイスに交換するラベルを選択します 既に他のデバイスで使用しているラベルに交換できます
ラベルを削除する	デバイスから削除するラベルを選択します

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。

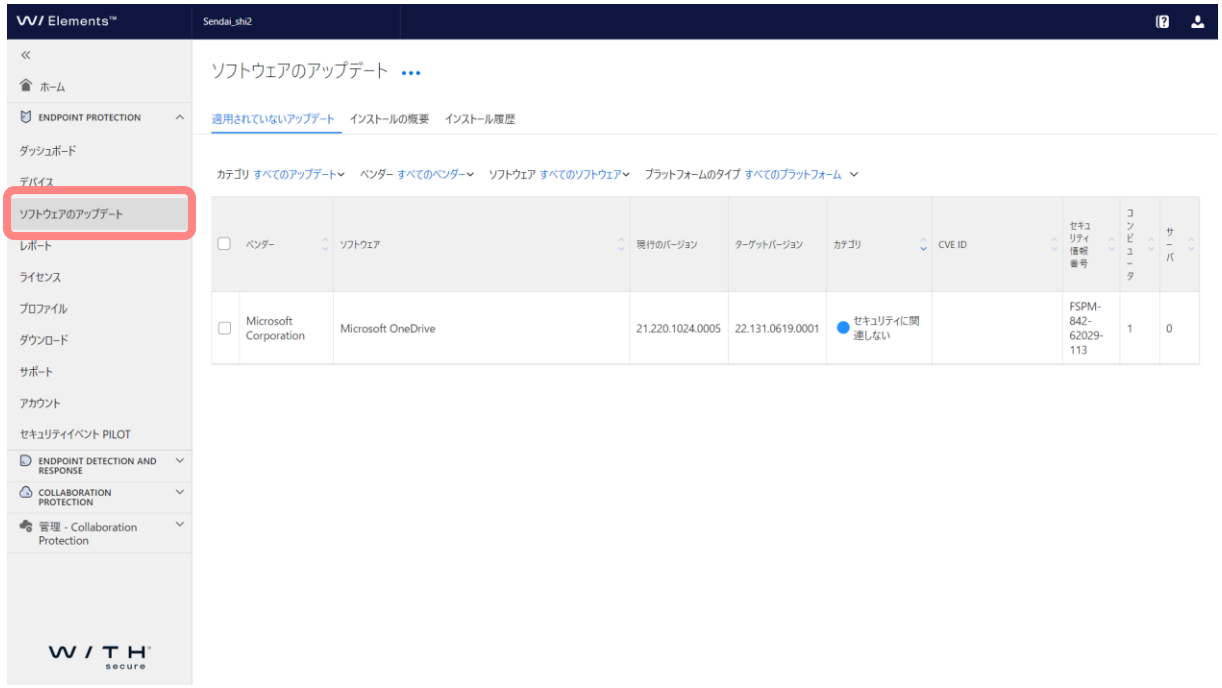
③確認画面が表示されるので、内容を確認し[完全に取り除く]ボタンをクリックします

9. ソフトウエアのアップデート

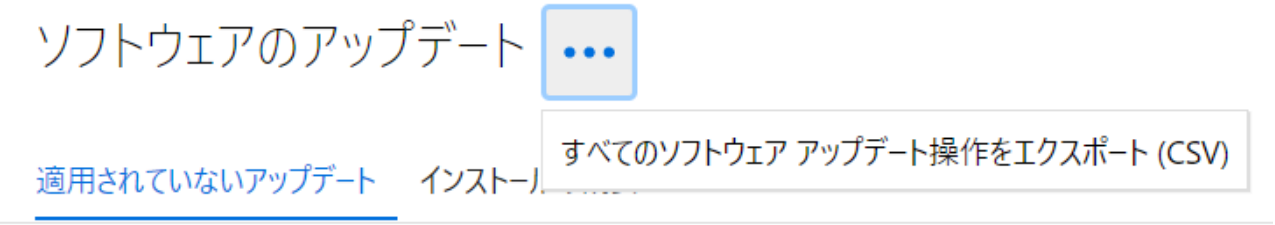
セキュリティパッチやアップデートを適用させます。

9.1. [ソフトウエアのアップデート] 操作メニュー概要

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



9.1.1. アクションメニュー

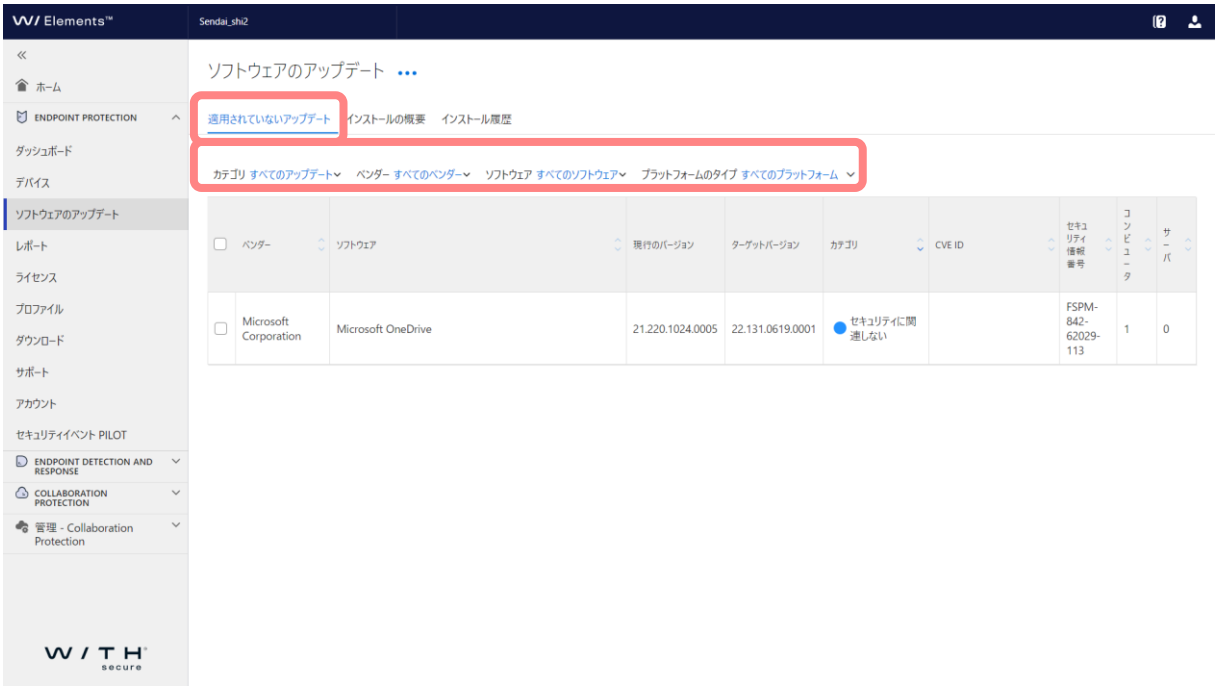


項目名	内容
すべてのソフトエアアップデート操作をエクスポート （CSV）	ソフトウェアアップデートの操作のレポートが、CSV形式でダウンロードされます。

9.2. タブメニュー

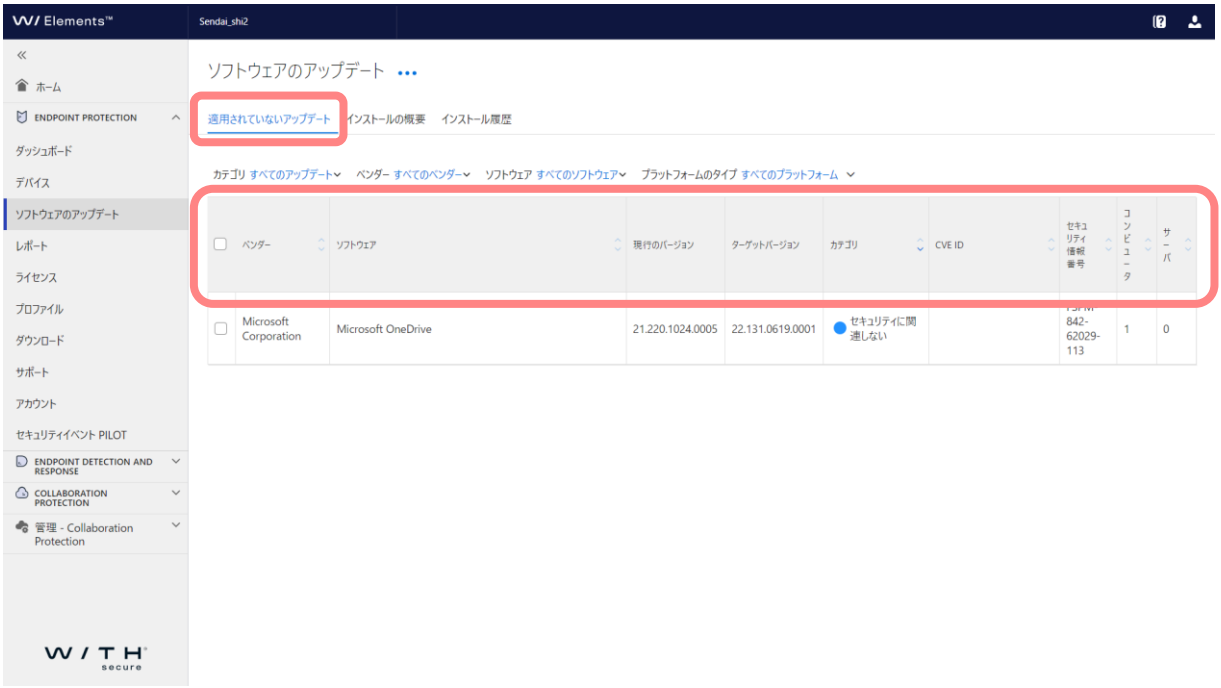
[適応されていないアップデート] / [インスールの概要] / [インスール履歴] ボタンで表示方法の切り替えができます。

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

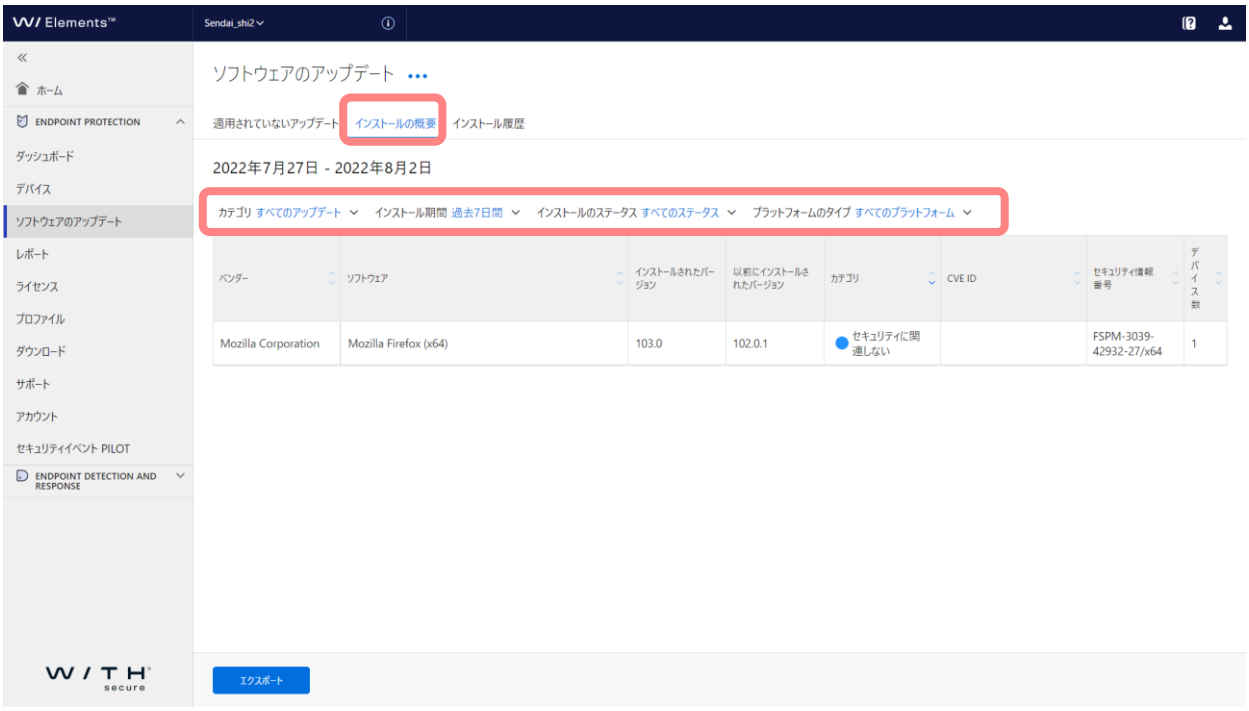
項目名	内容
カテゴリ	重要/重大などセキュリティアップデートの種類別に表示
ベンダー	ソフトウエアベンダー別に表示
ソフトウエア	ソフトウエア種類別に表示
プラットフォーム	サーバまたはワークステーション別に表示



・適応されていないアップデート　タブ

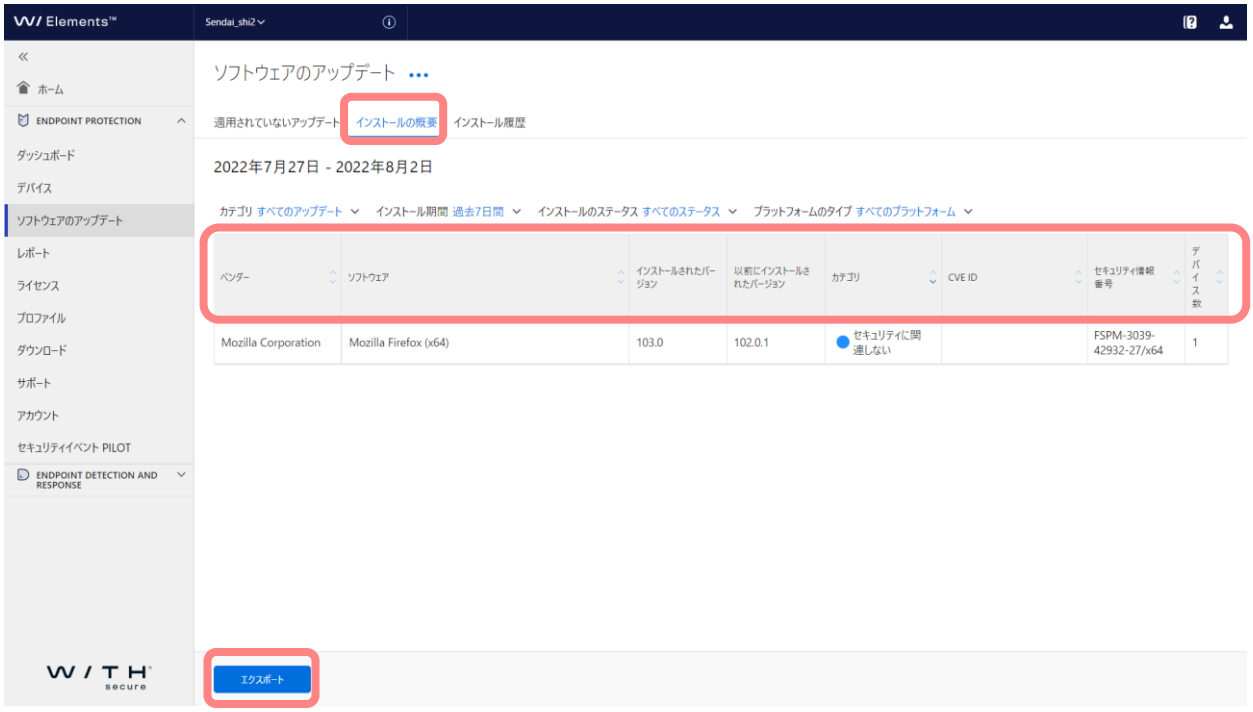
項目名	内容
ベンダー	ソフトウエアベンダー
ソフトウエア	ソフトウエア種類
現行のバージョン	インストール済　バージョン
ターゲットバージョン	アップデート予定　バージョン
カテゴリ	重要/重大などセキュリティアップデートの種類別に表示
CVE ID	CVE ID の表示
セキュリティ情報番号	マイクロソフトのセキュリティ情報番号の表示
コンピュータ	対象コンピュータ端末
サーバ	対象サーバ端末

9.2.2. インスールの概要



・インスールの概要 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

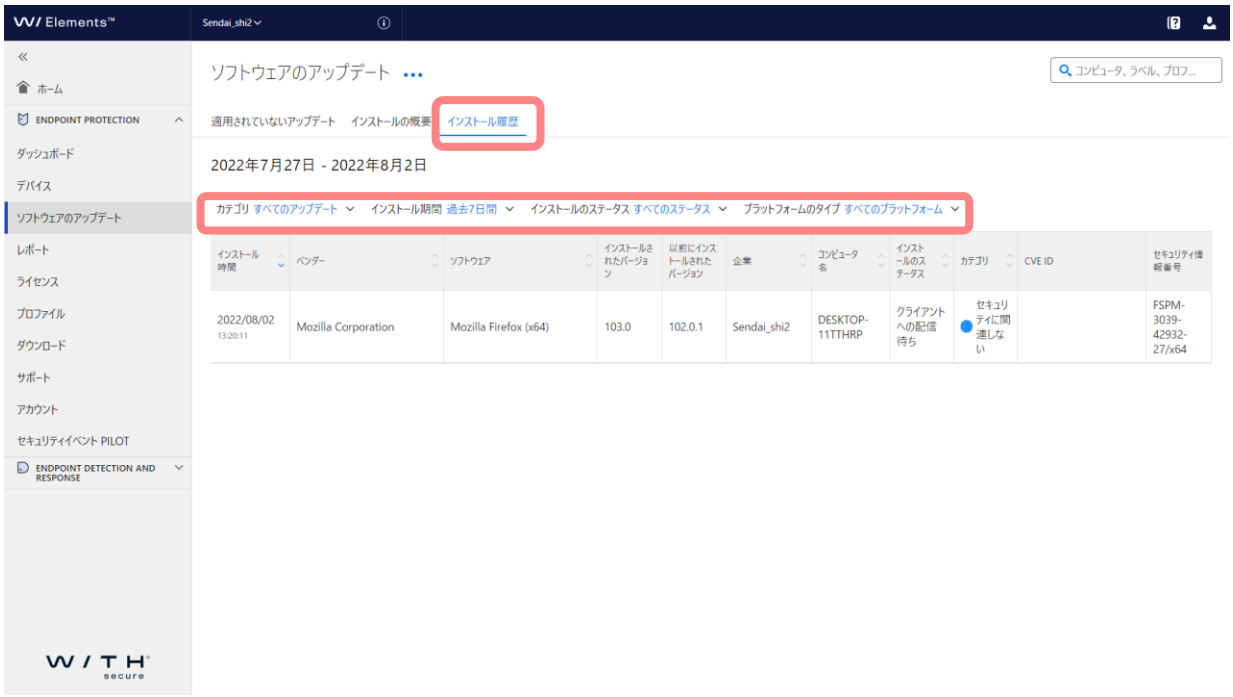


インストールの概要　タブ

項目名	内容
ベンダー	ソフトウエアベンダー
ソフトウエア	ソフトウエア種類
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

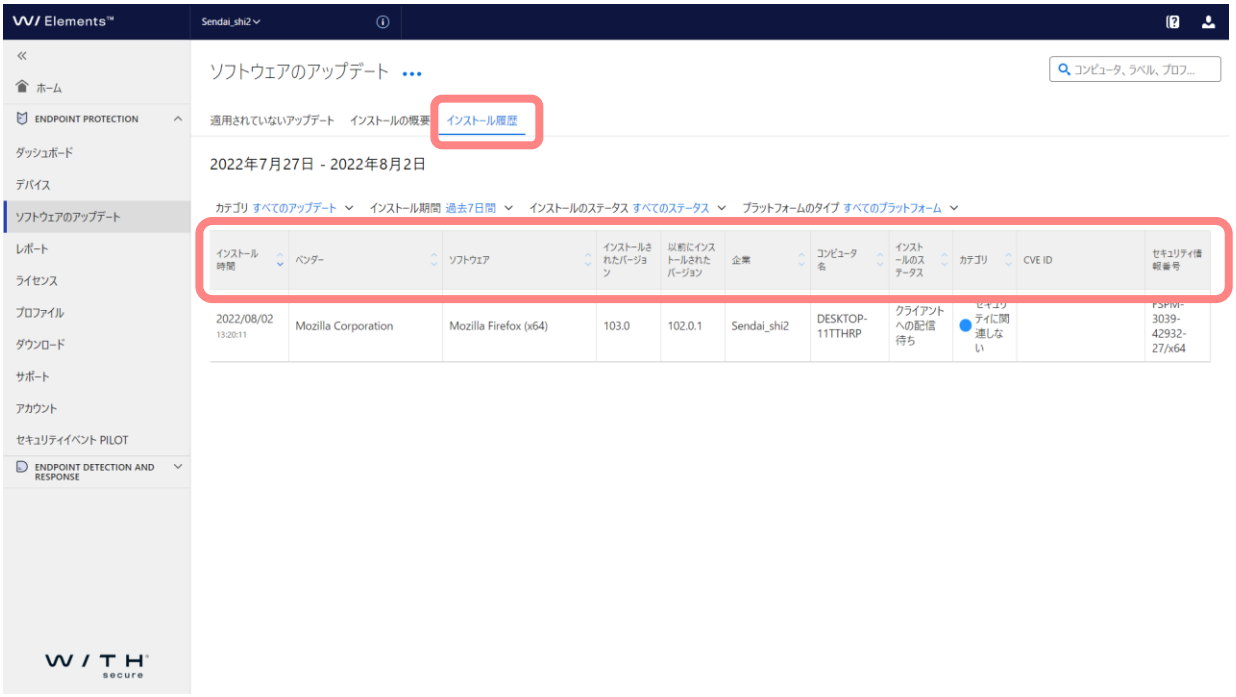
・[エクスポート]　ボタンで CSV 形式のリストのダウンロードが可能

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

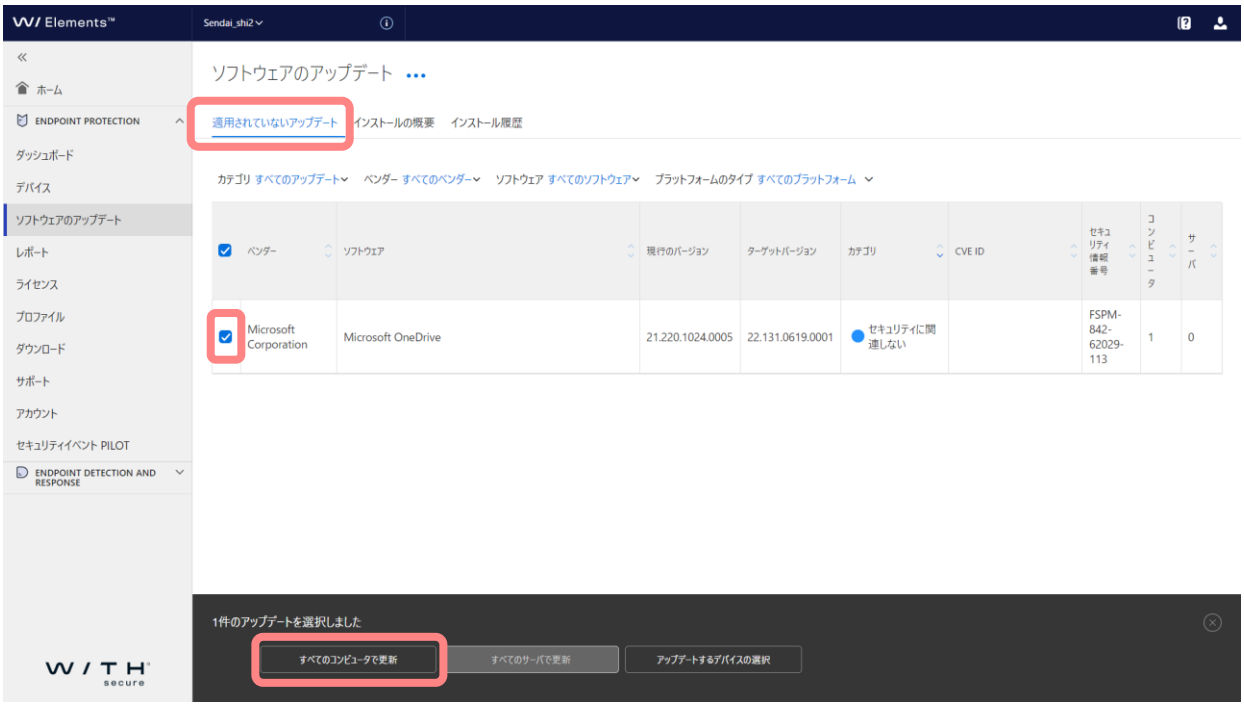


インストールの概要　タブ

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	ソフトウエアベンダー
ソフトウエア	ソフトウエア種類
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

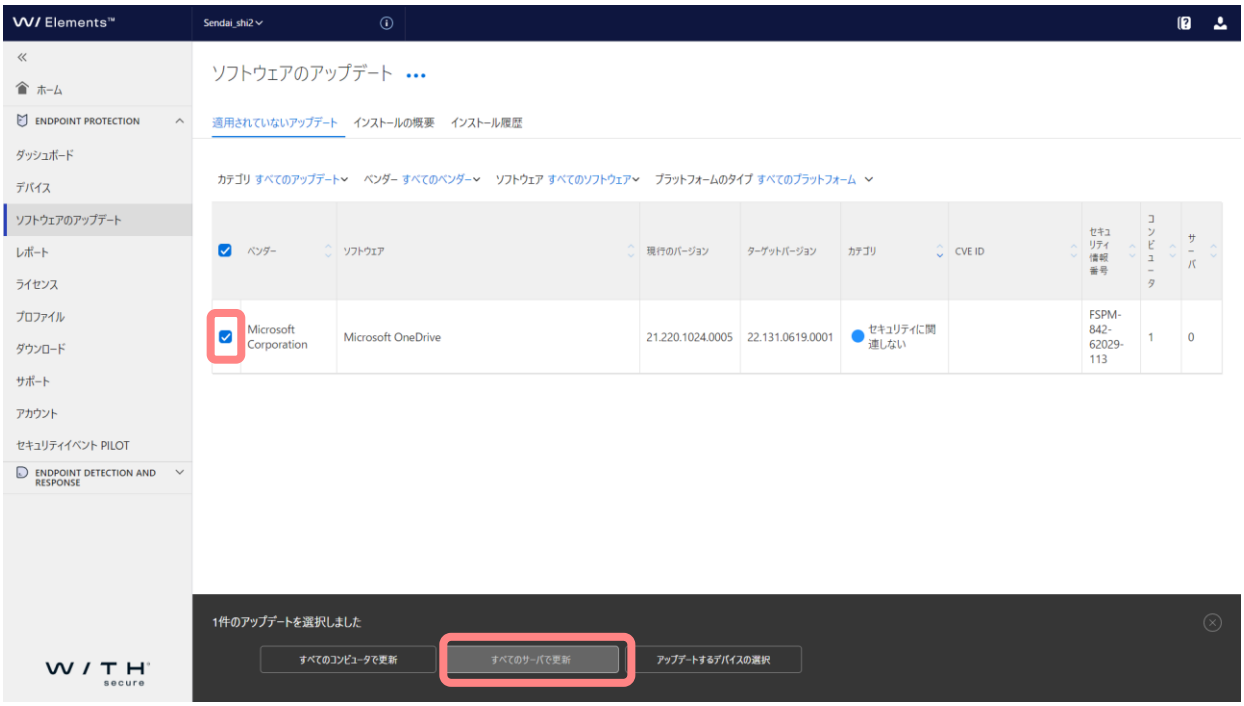
任意のセキュリティパッチやアップデートをコンピュータに対して適用させます。



[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

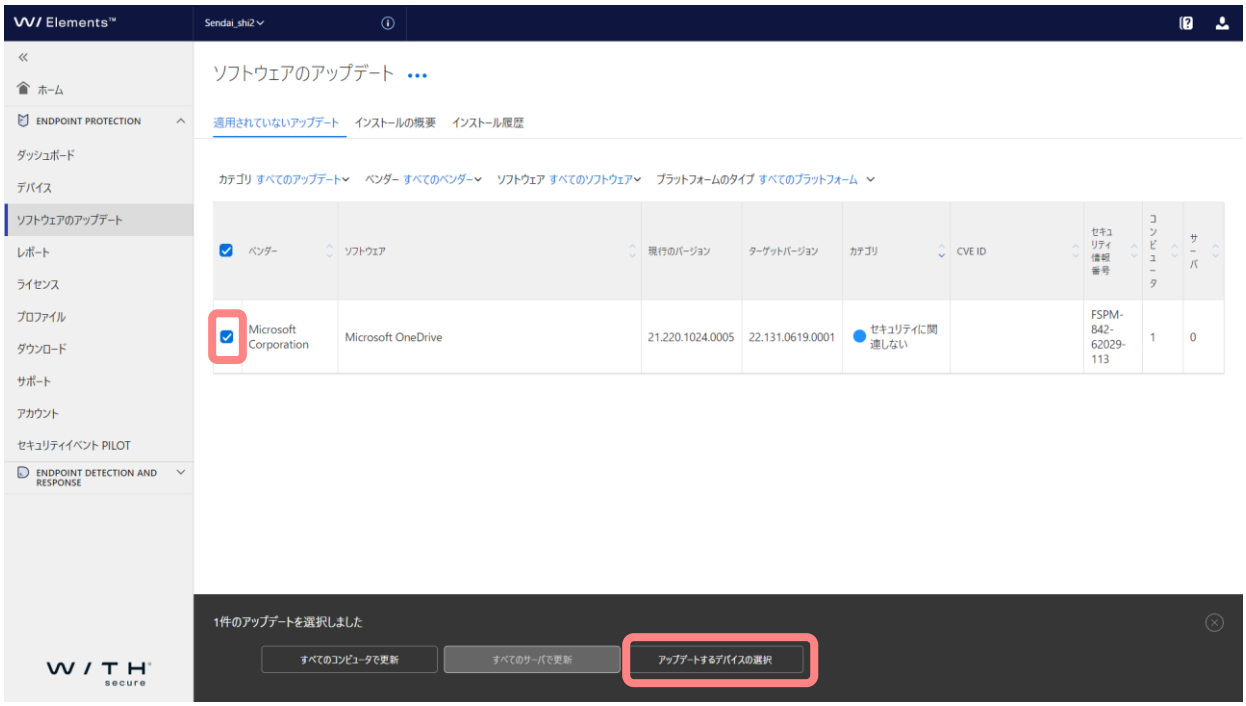
任意のセキュリティパッチやアップデートをサーバに対して適用させます。



[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。



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。

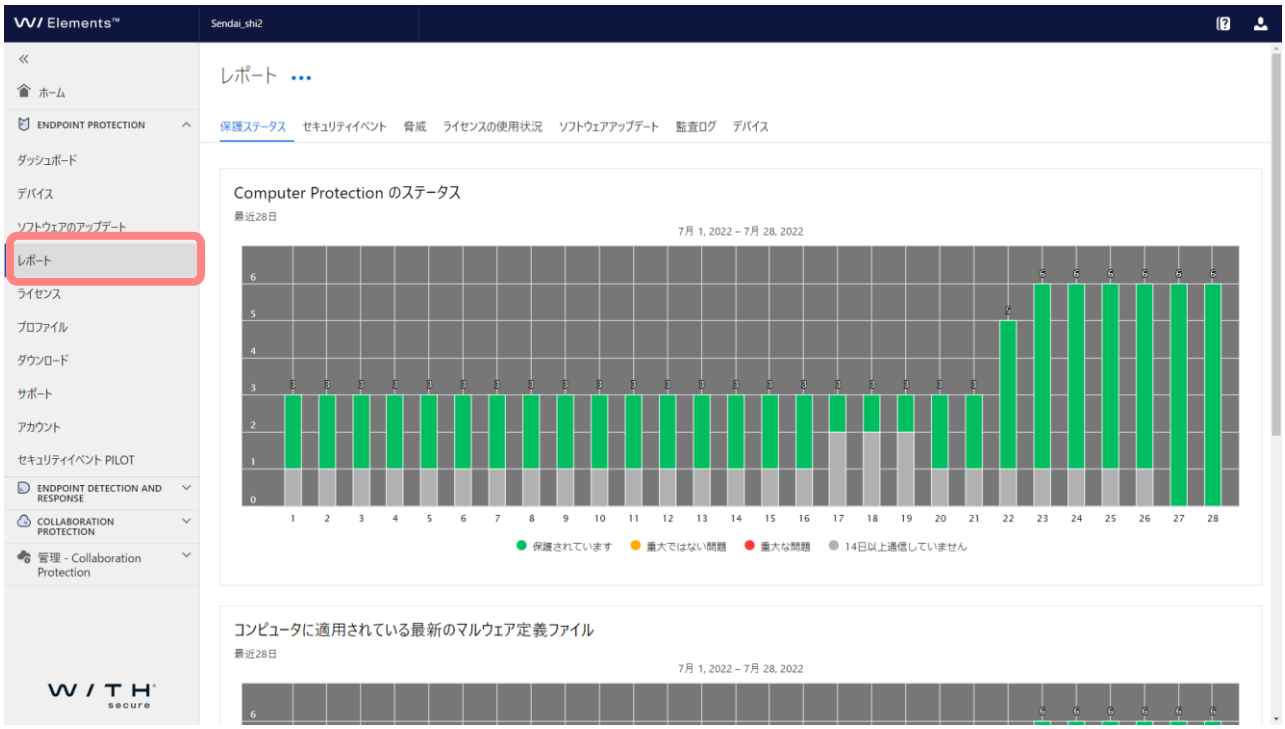
⑤[更新] ボタンをクリックします。

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。



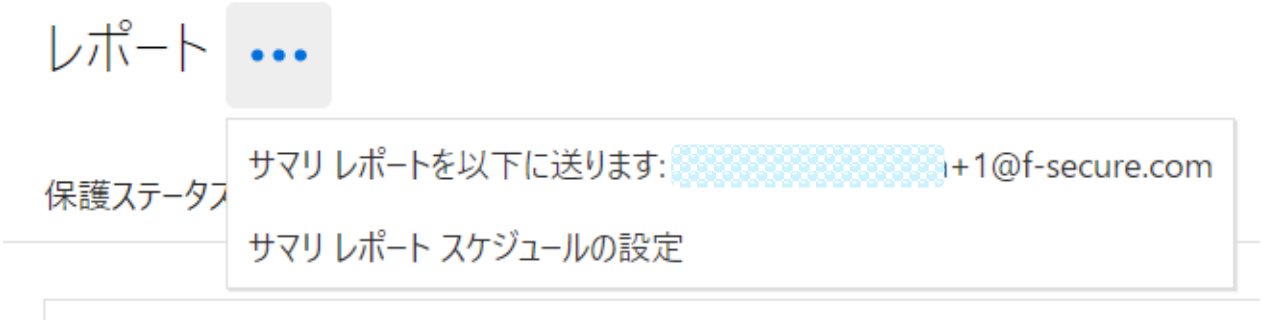
10.2. アクションメニュー

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

サマリ レポート スケジュールの設定	サマリ レポート スケジュールの設定画面に移動

10.3. レポートのサマリ送信

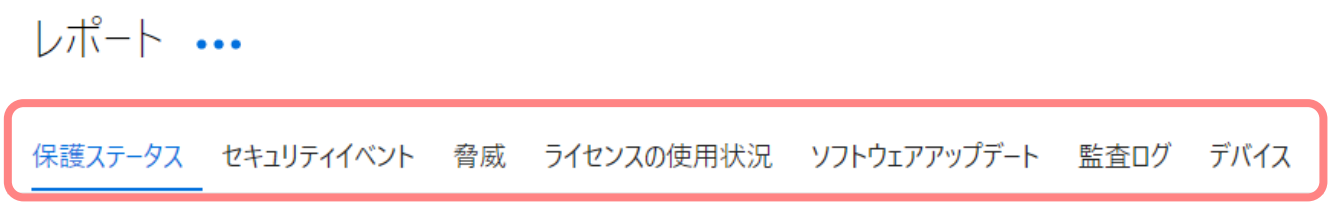
「レポート」見出し横のアクションメニューボタンをクリックし、「サマリレポートを以下に送ります:」をクリックすることで、その時点でのサマリをログインユーザに送付します。



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

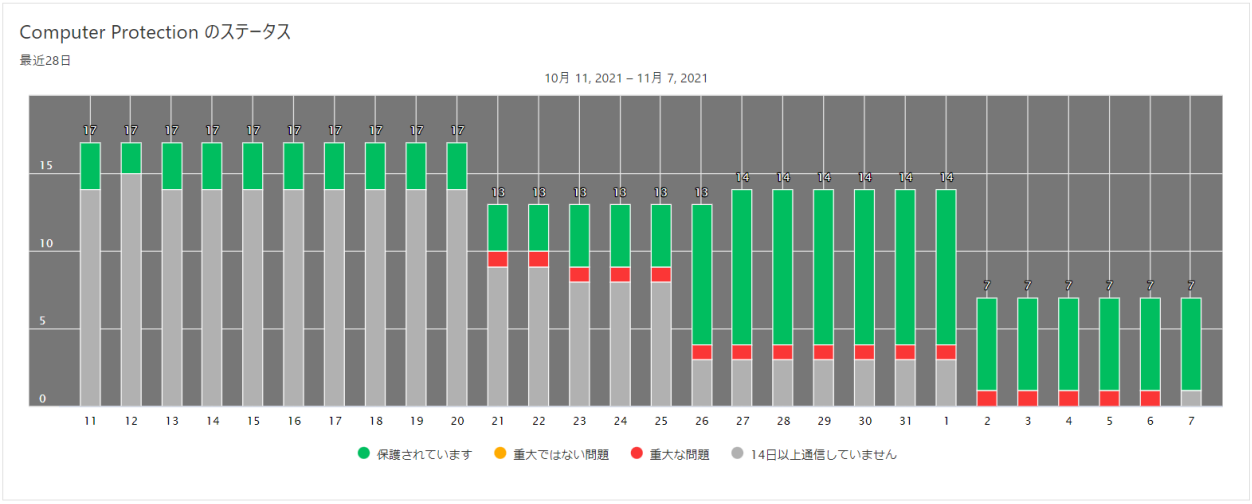
タブメニューをクリックするとレポート概要を切り替えることができます。



10.5. 保護ステータス

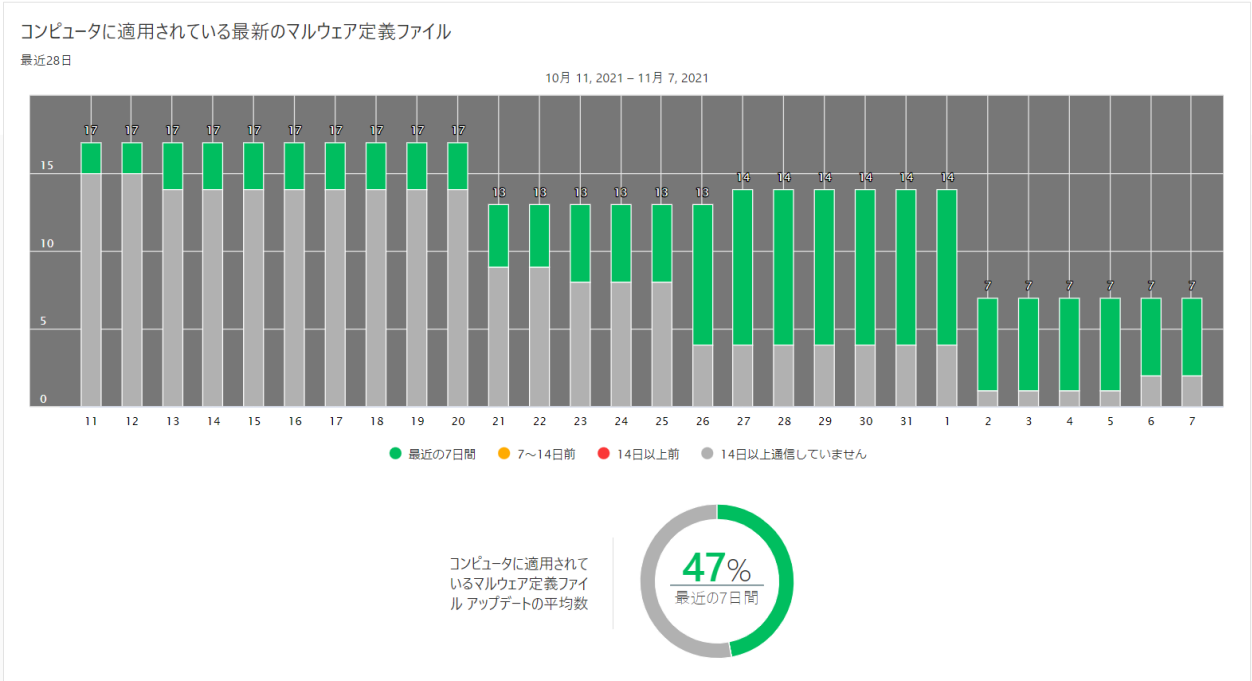
10.5.1. Computer Protection のステータス

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

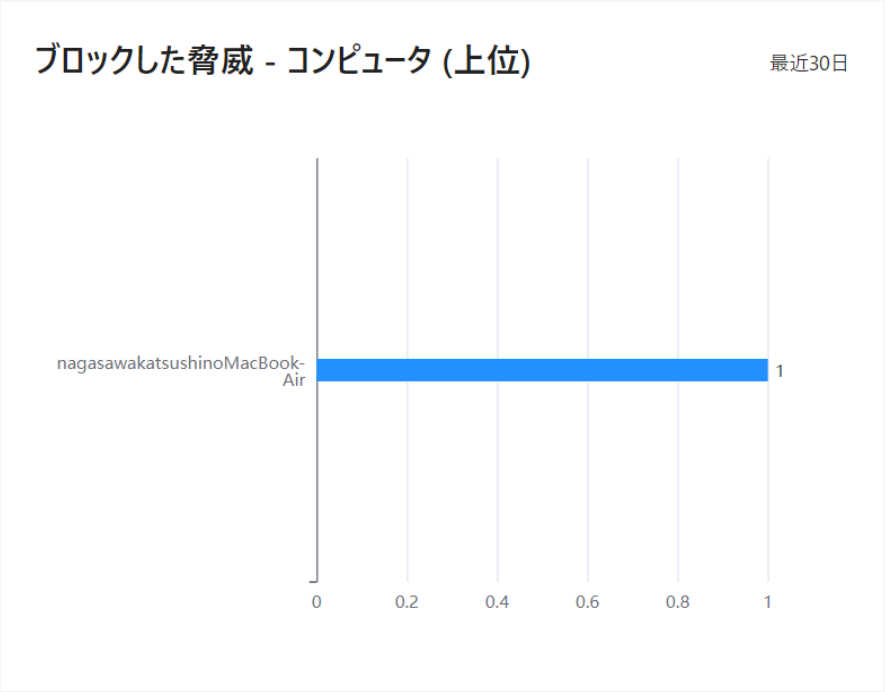
コンピュータに適用されているパターンファイルの更新状況を日毎に棒グラフで表示します。



10.6. セキュリティイベント

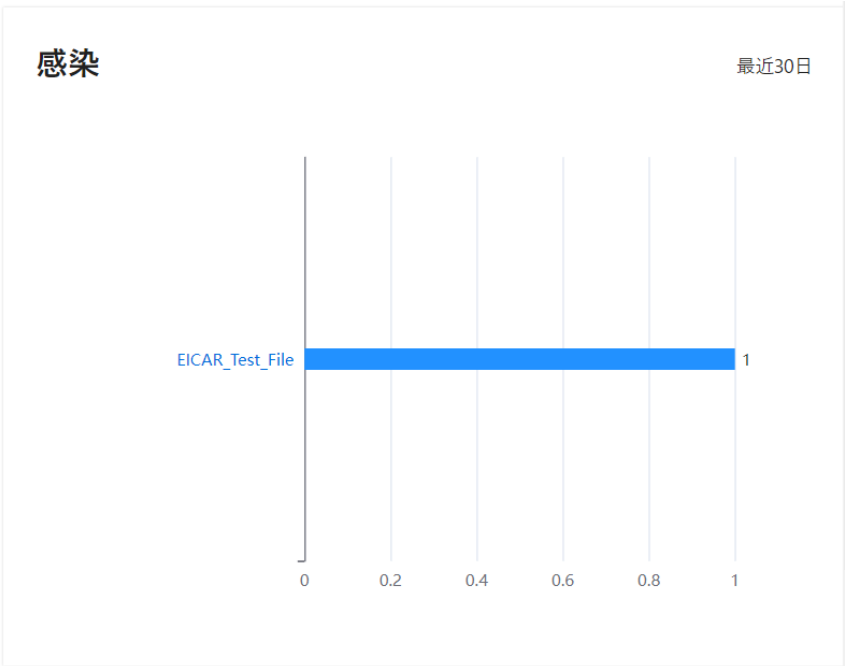
10.6.1. ブロックした脅威- コンピュータ（上位）

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。



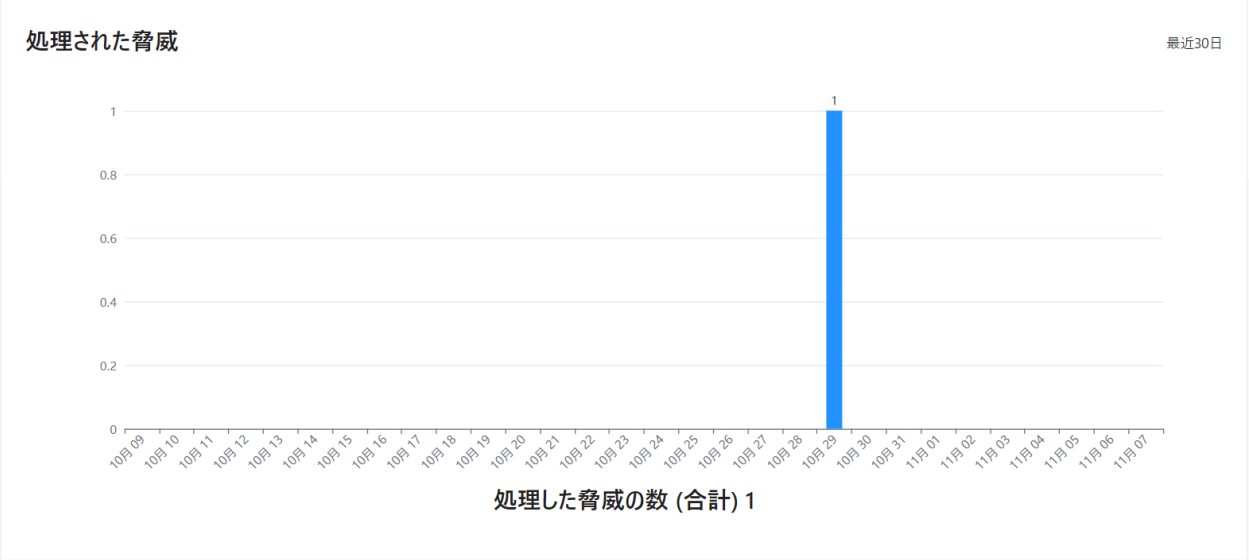
10.6.2. 感染

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

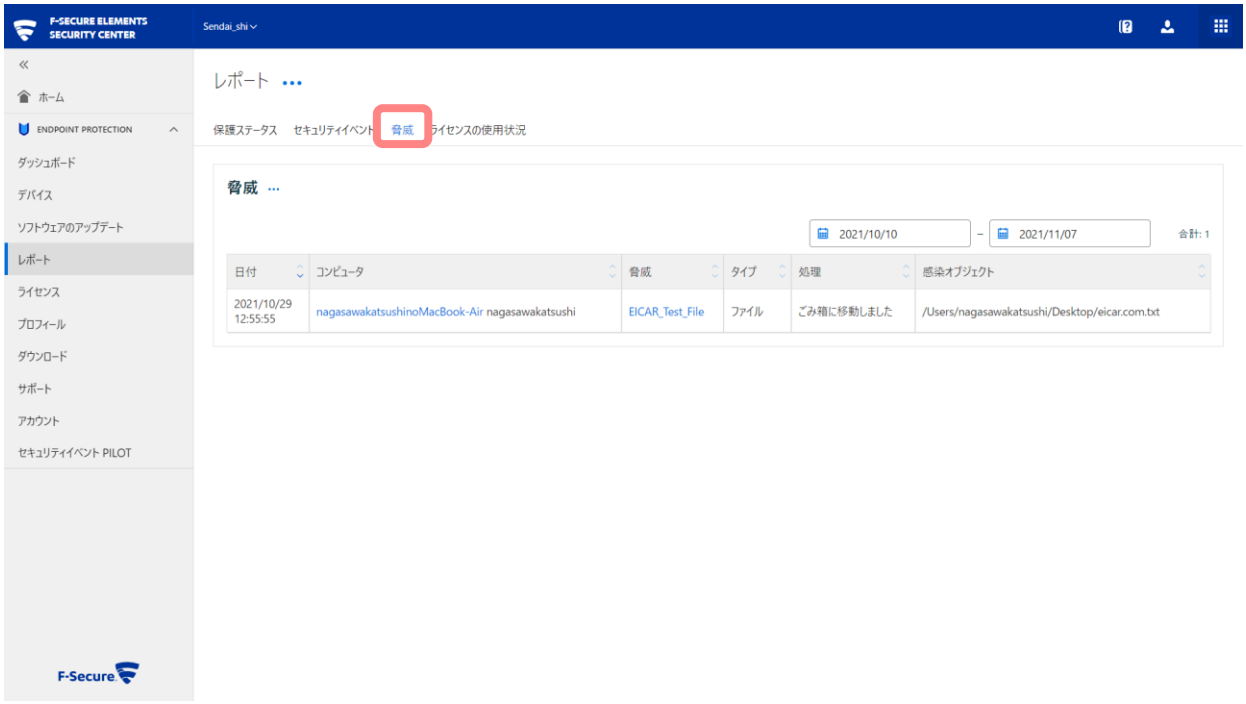
直近の 30 日の間に検知されたマルウェアの上位トップ 10 までを表示します。数字は、検知された数です。



10.7. 脅威

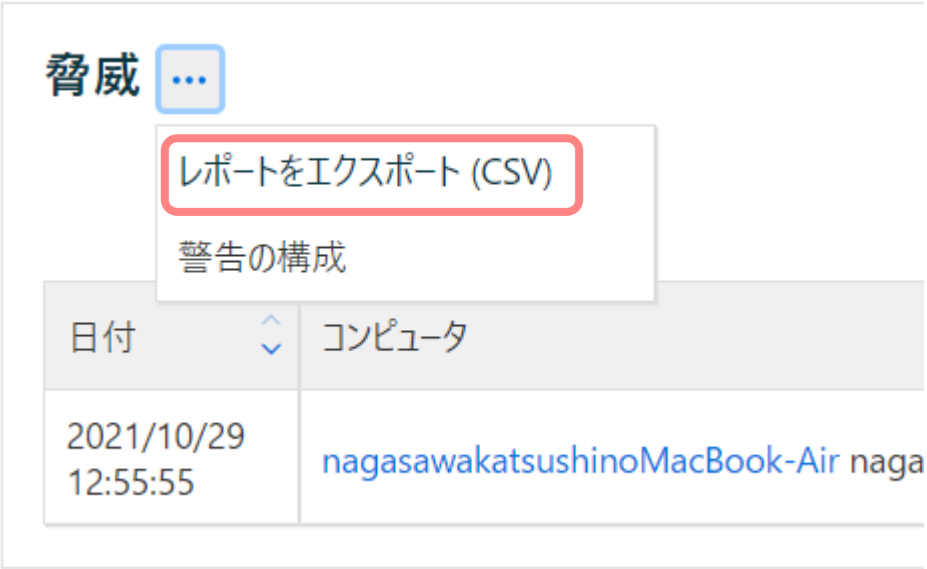
[脅威] タブをクリックするとマルウェアの検知した履歴が一覧で表示されます。

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

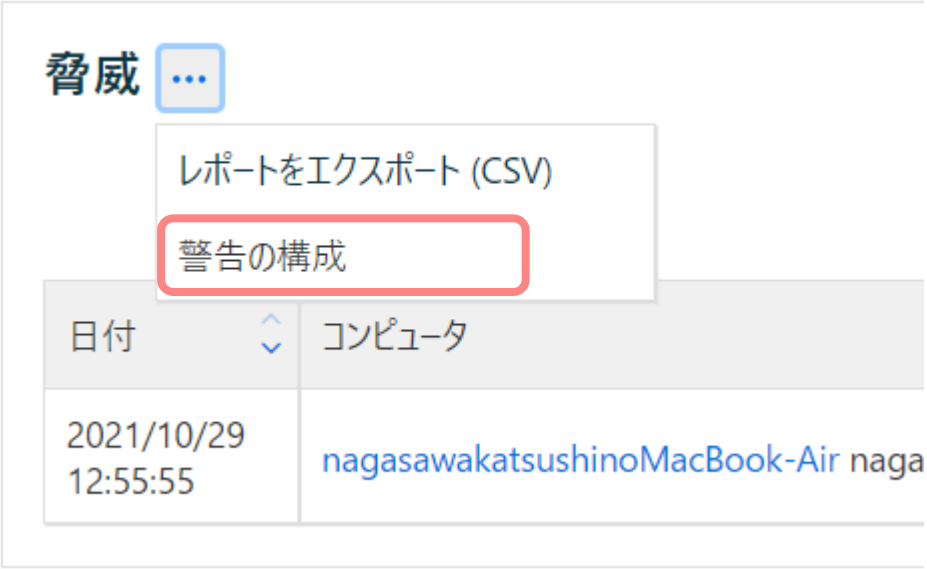
「脅威」見出し横のアクションメニューボタンをクリックし、[レポートをエクスポート（CSV）]をクリックすると CSV 形式でのレポートがダウンロードされます。



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。

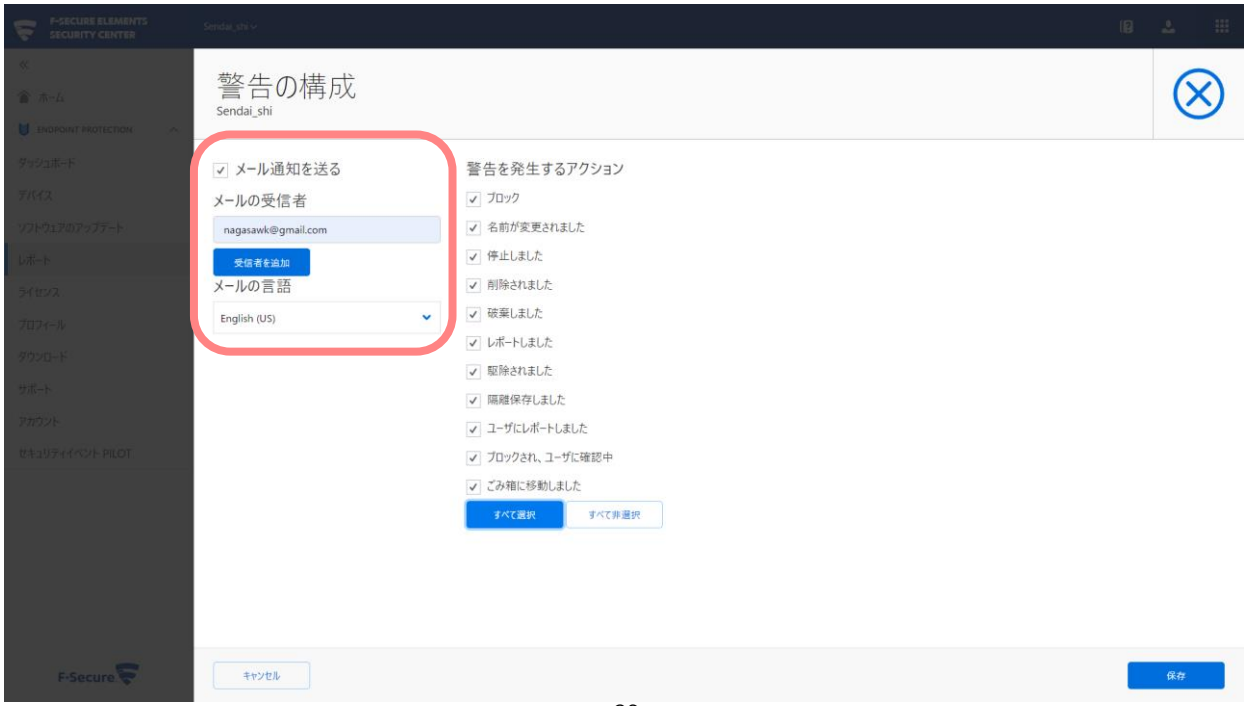


「メール通知を送る」にチェックを入れると、メールによる警告転送機能が有効になります。

「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。

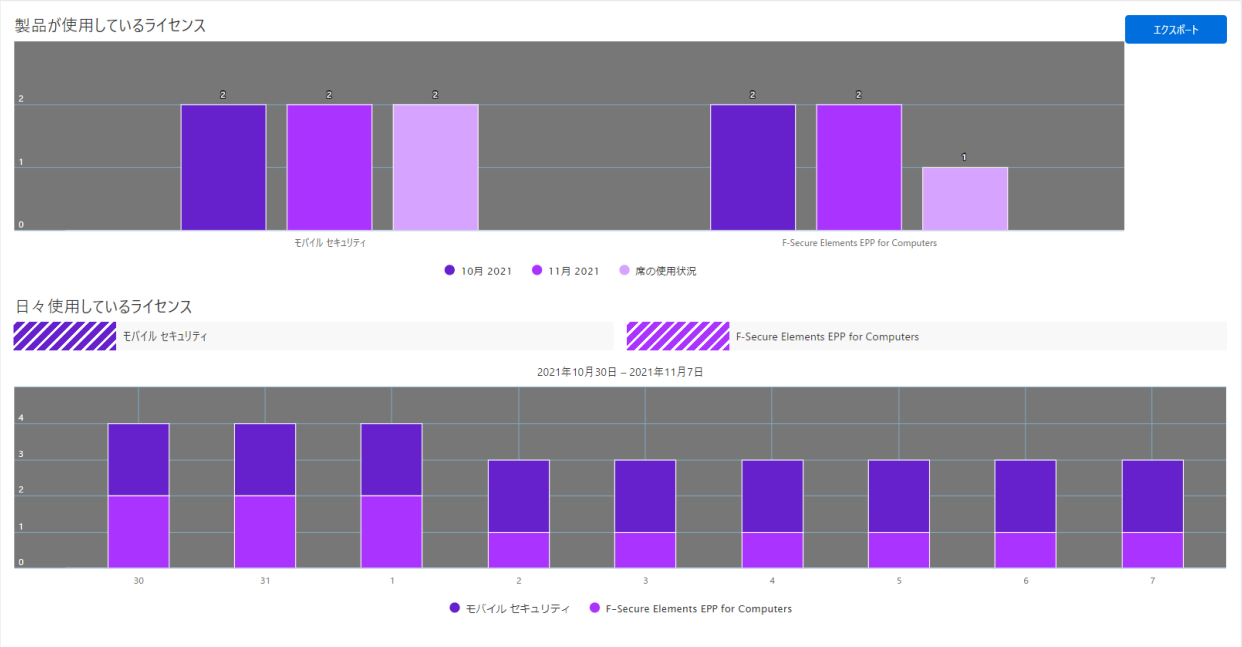
・隔離保存しました
検知されたマルウェアに対し、隔離保存を行いました。

・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

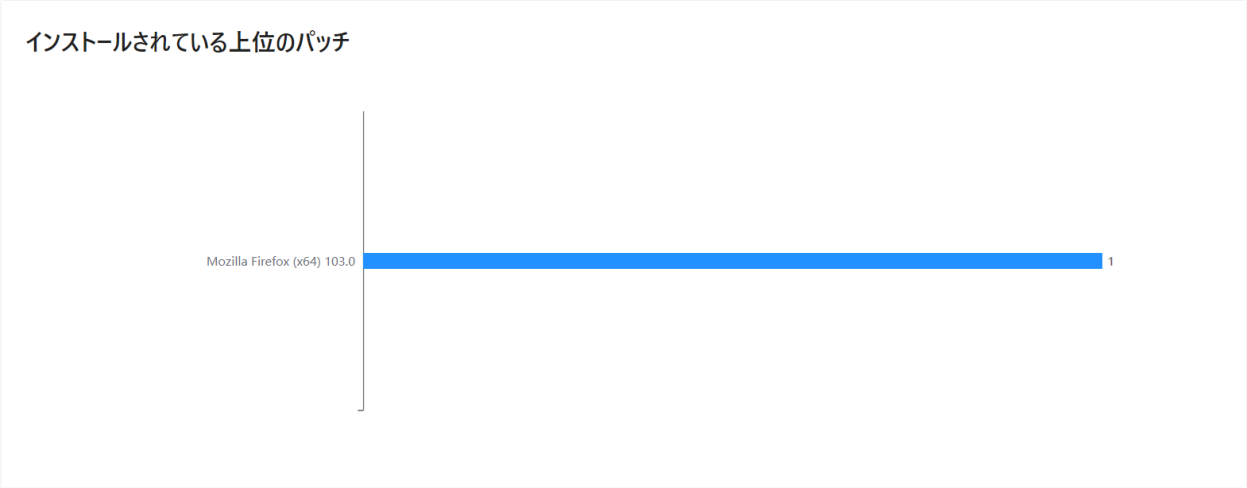
[ライセンスの使用状況] タブをクリックし、[エクスポート] ボタンをクリックすると、CSV ファイルがダウンロードできます。

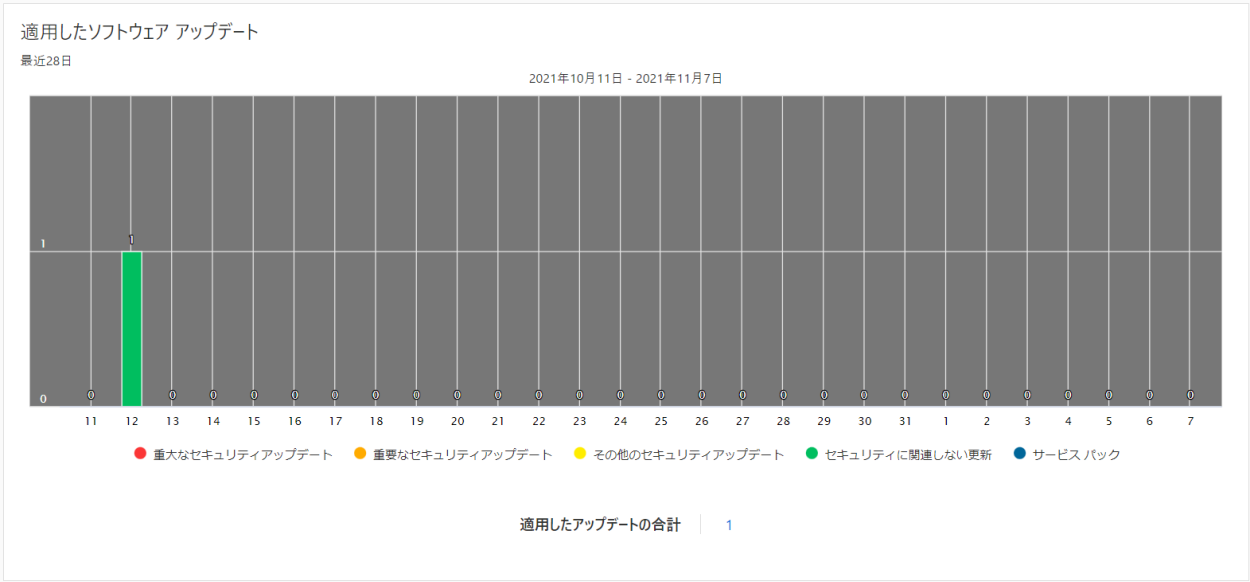


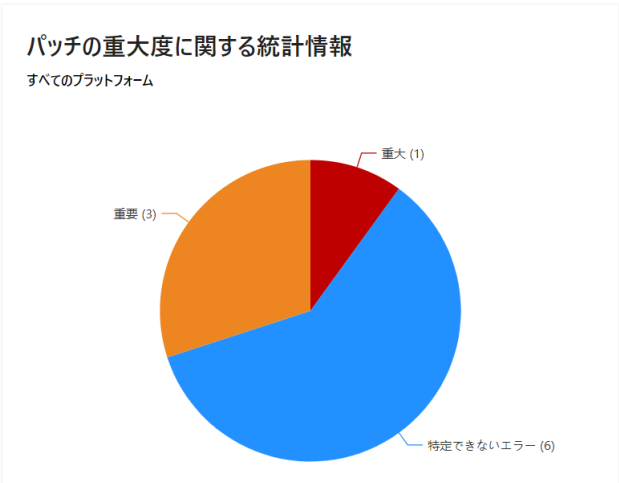
＊お客様の設定状況においては表示されない場合がございます。

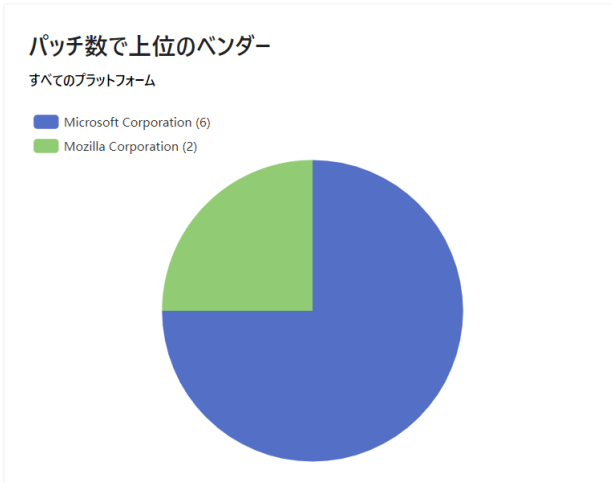
10.9. ソフトウエア　アップデート

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。



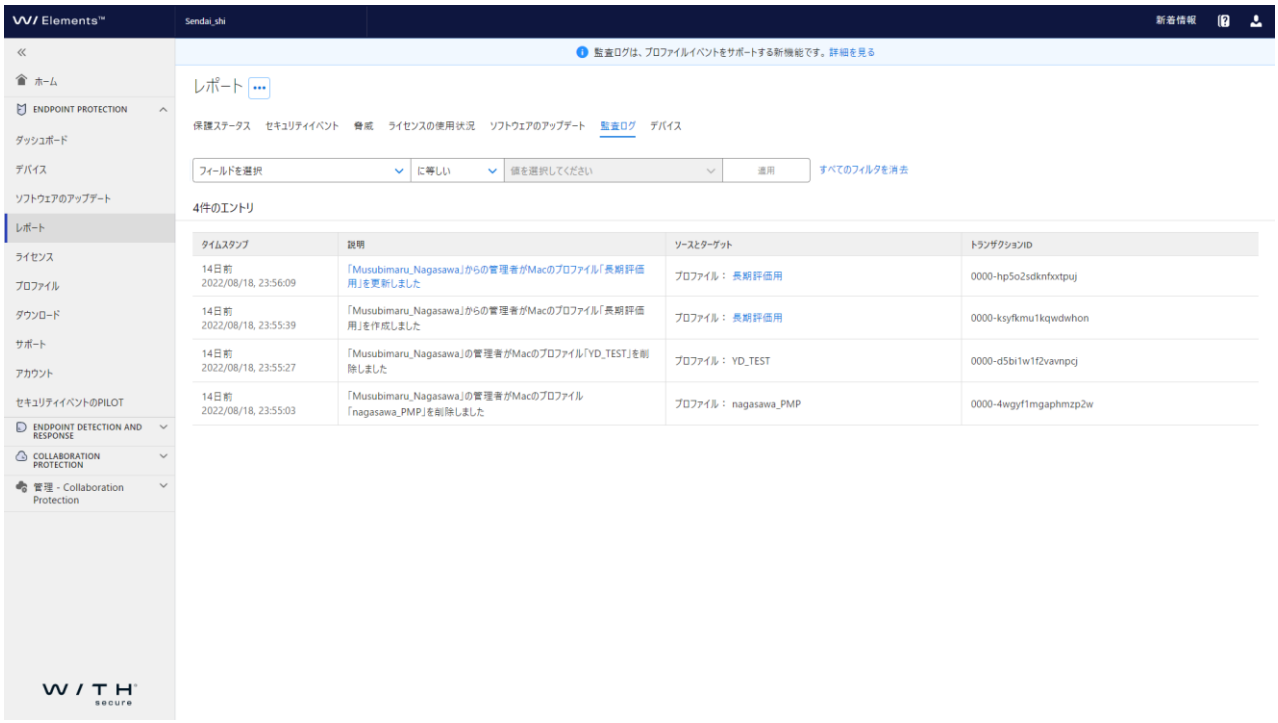






10.10. 監査ログ

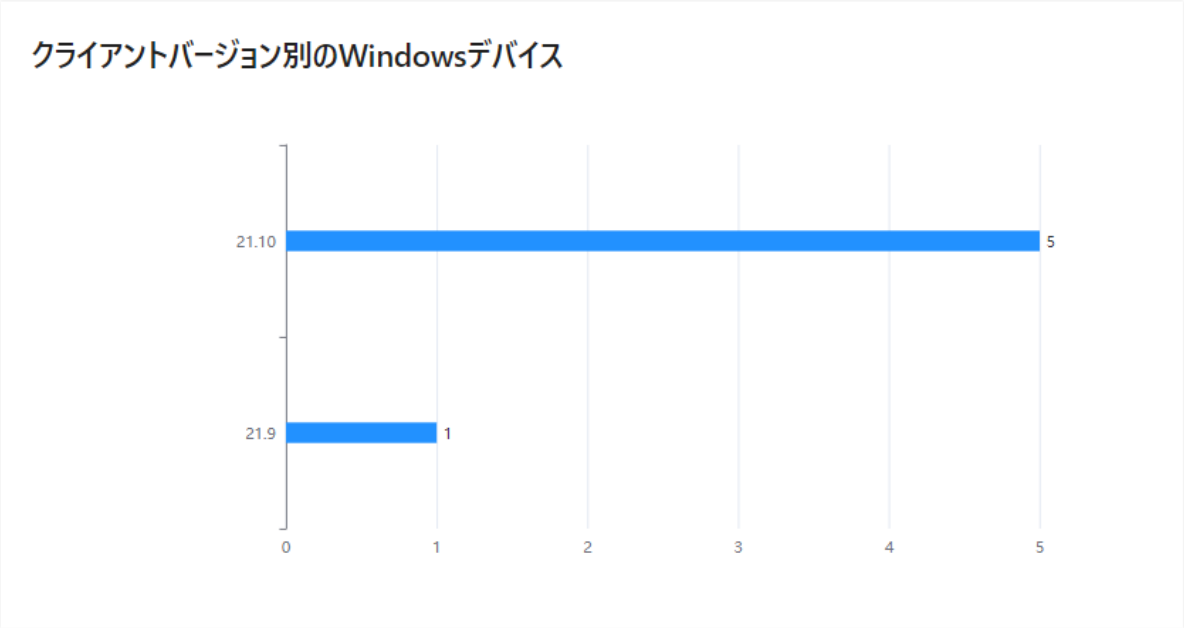
監査ログは、プロファイルの作成/削除/更新などのイベントをサポートする機能です。



10.11. デバイス

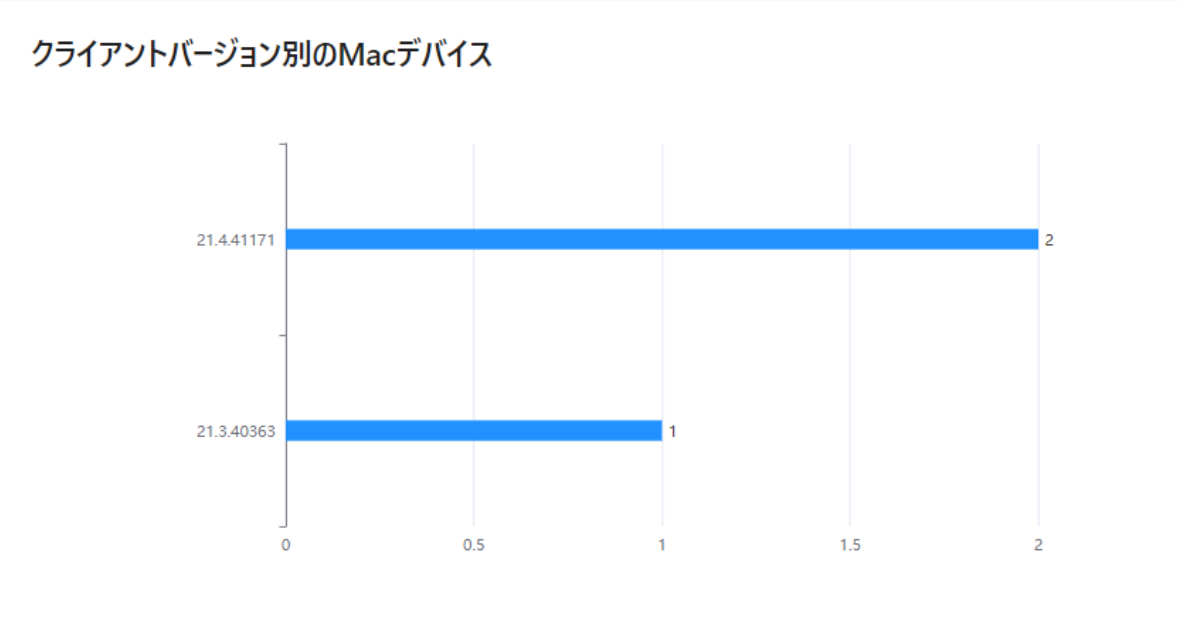
10.11.1. クライアントバージョン別の Windows デバイス

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。



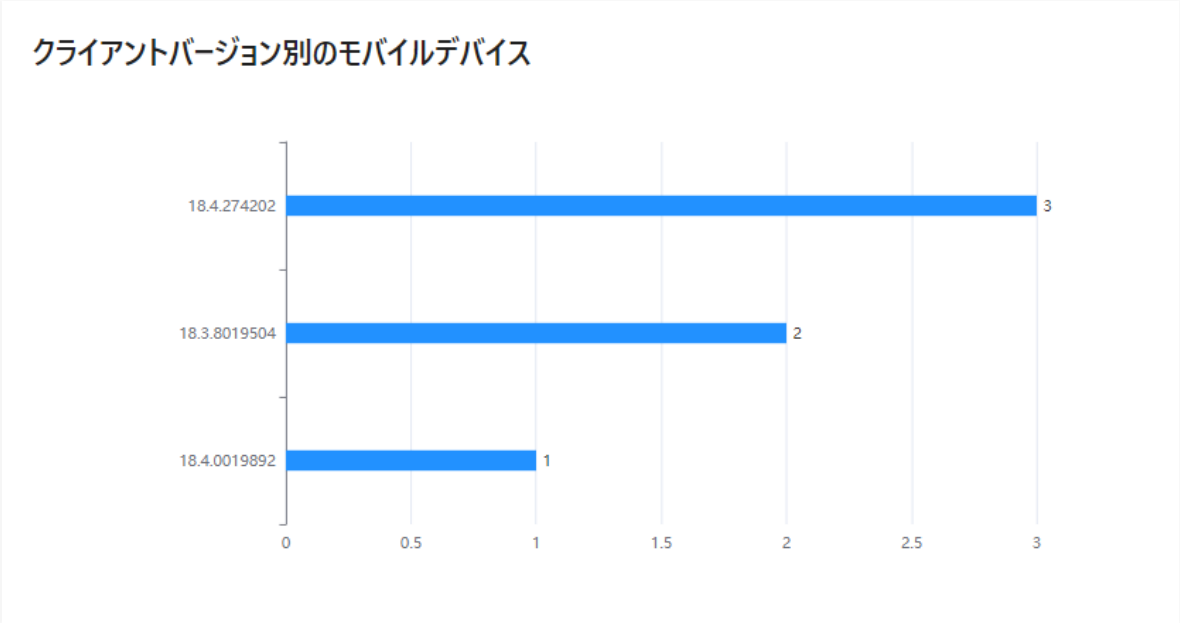
10.11.2. クライアントバージョン別の Mac デバイス

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。

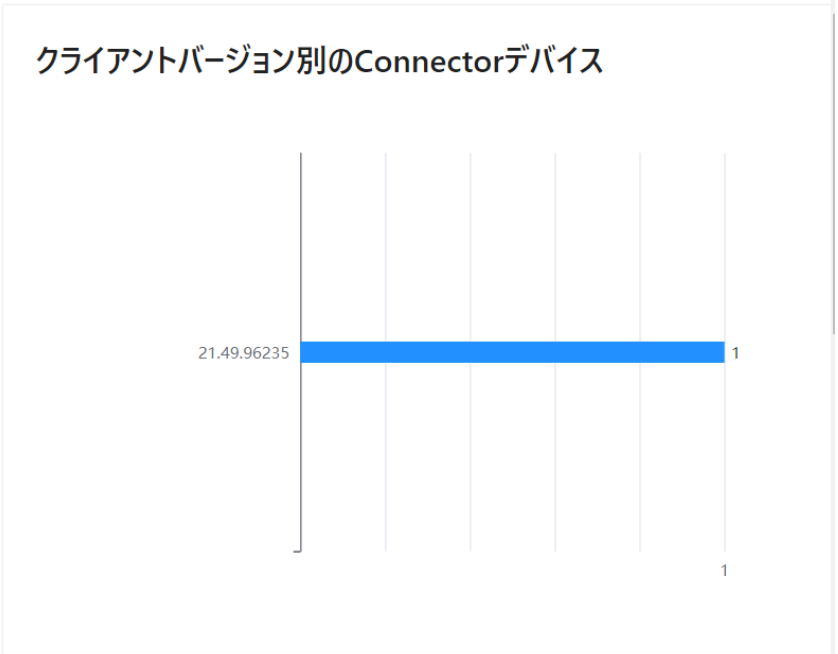


10.11.3. クライアントバージョン別のモバイルデバイス

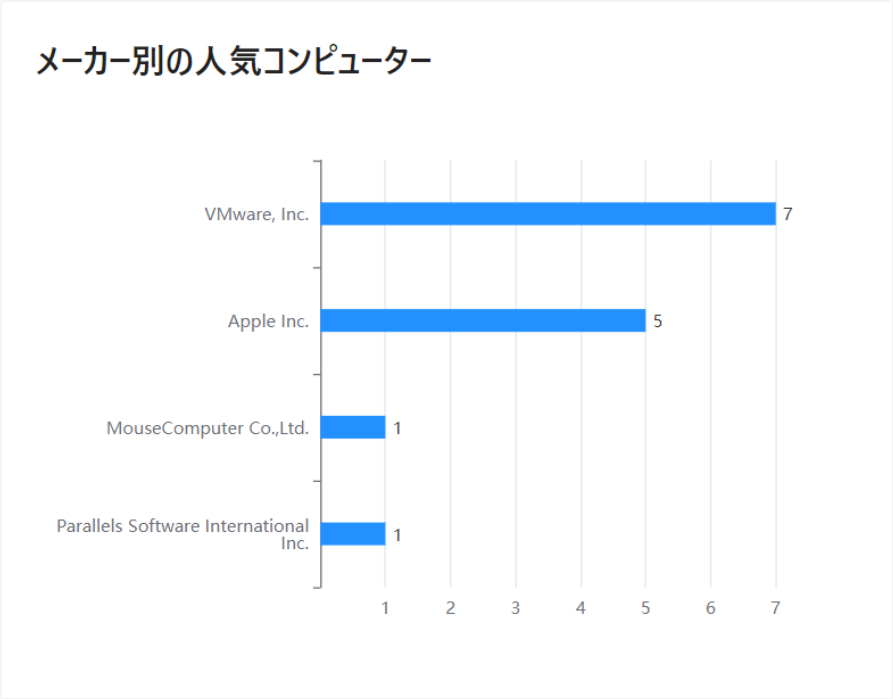
モバイルデバイスにインストールしているクライアントモジュールのバージョンを確認できます。



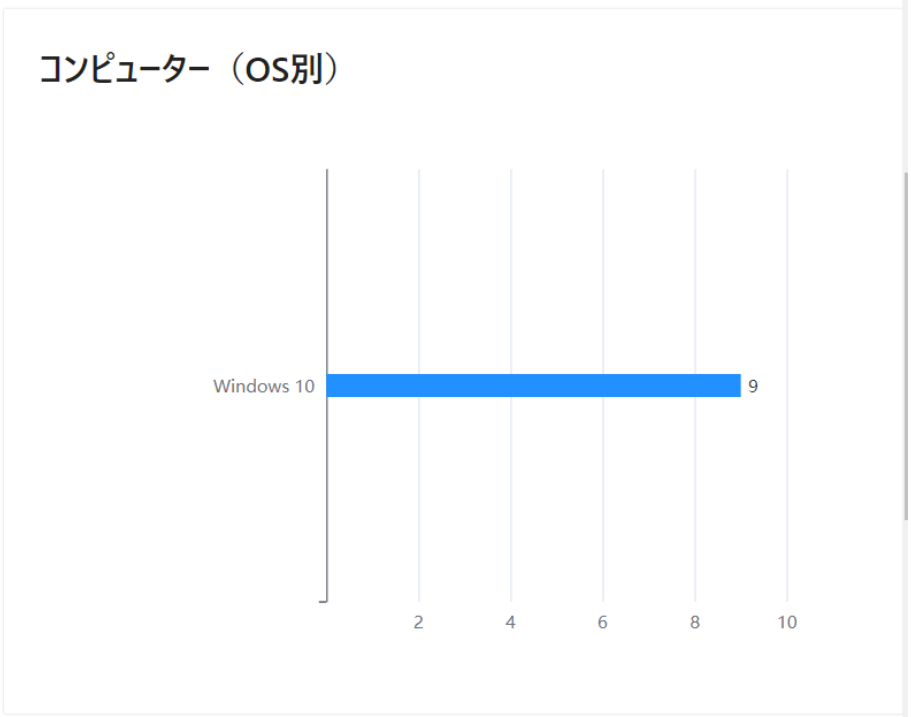
10.11.4. クライアントバージョン別の Connector デバイス



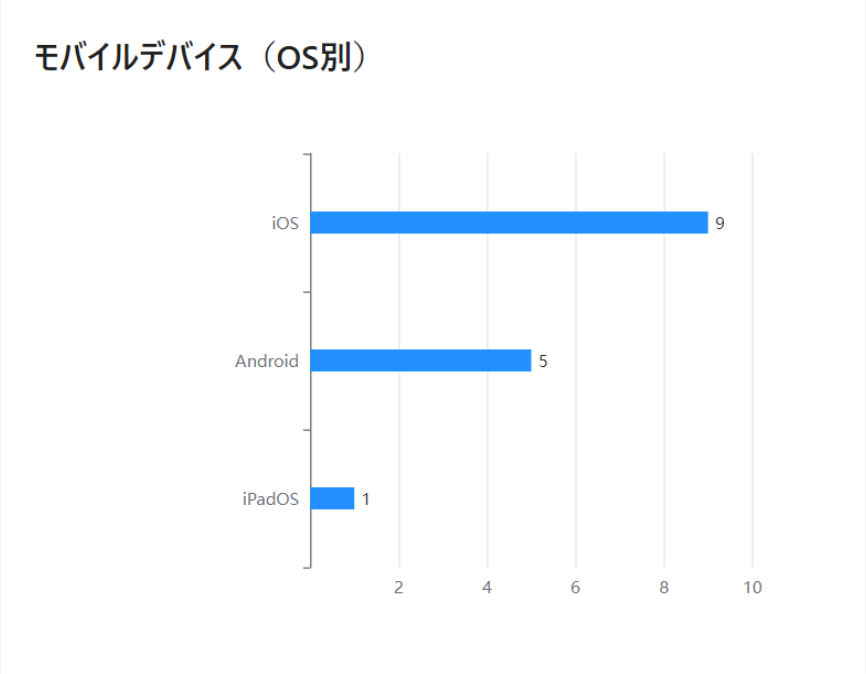
10.11.5. メーカー別の人気コンピュータ



10.11.6. コンピュータ（OS 別）

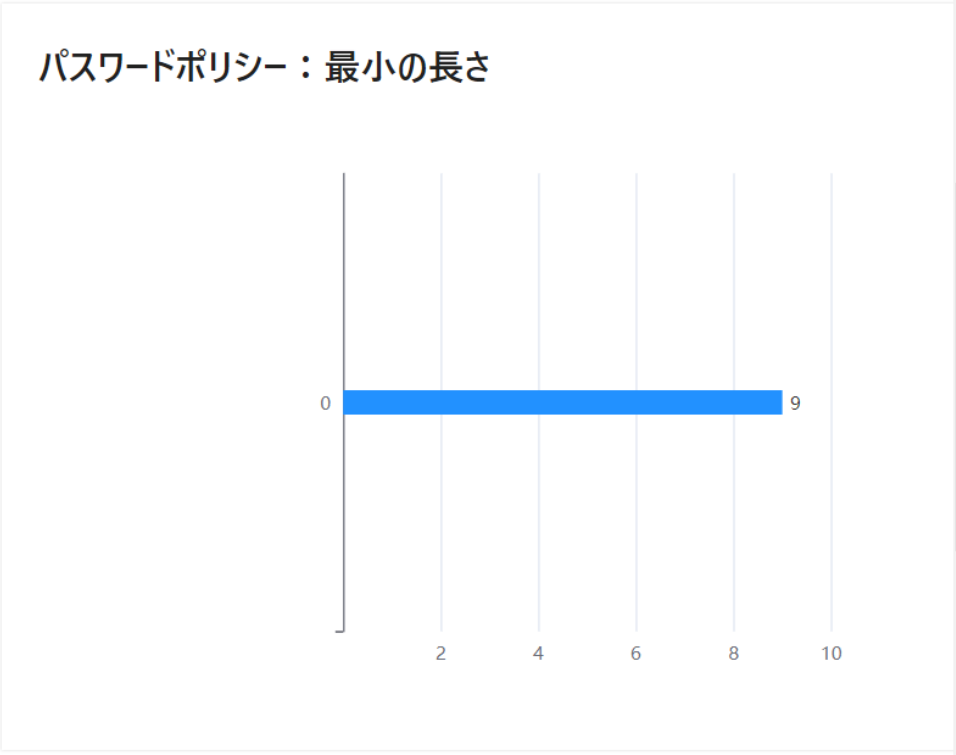


10.11.7. モバイルデバイス（OS 別）

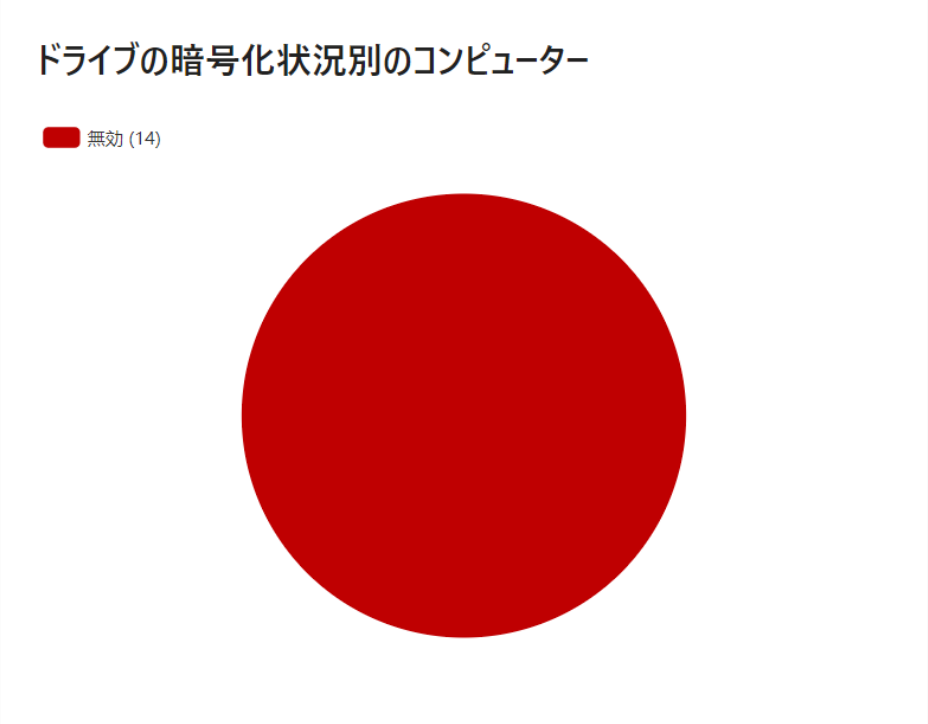


10.11.8. パスワードポリシー：最小の長さ

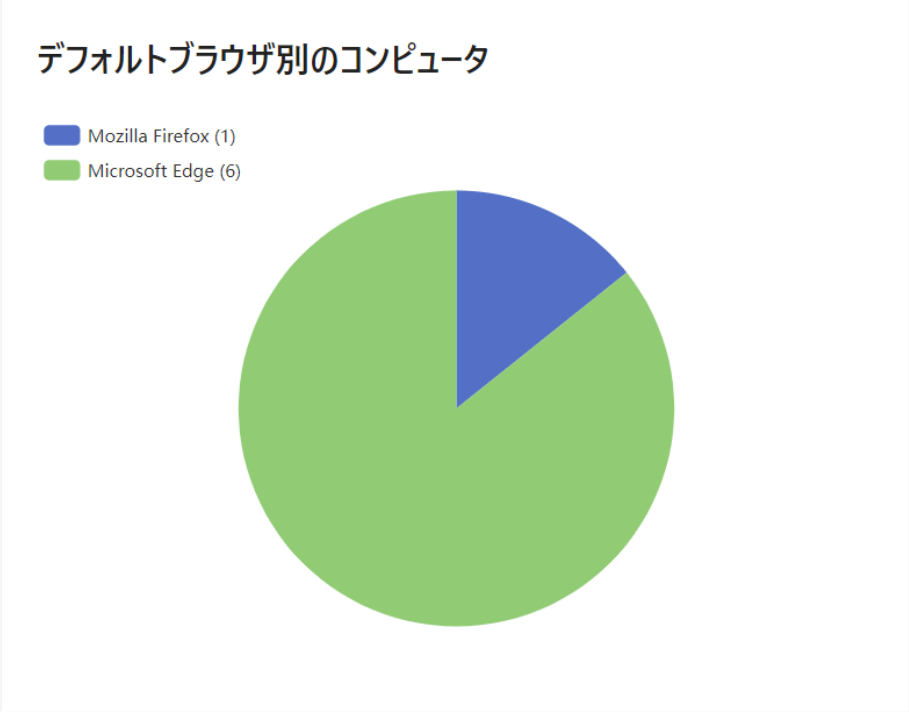
設定されているパスワードの字数と端末の台数



10.11.9. ドライブの暗号化状況別のコンピュータ

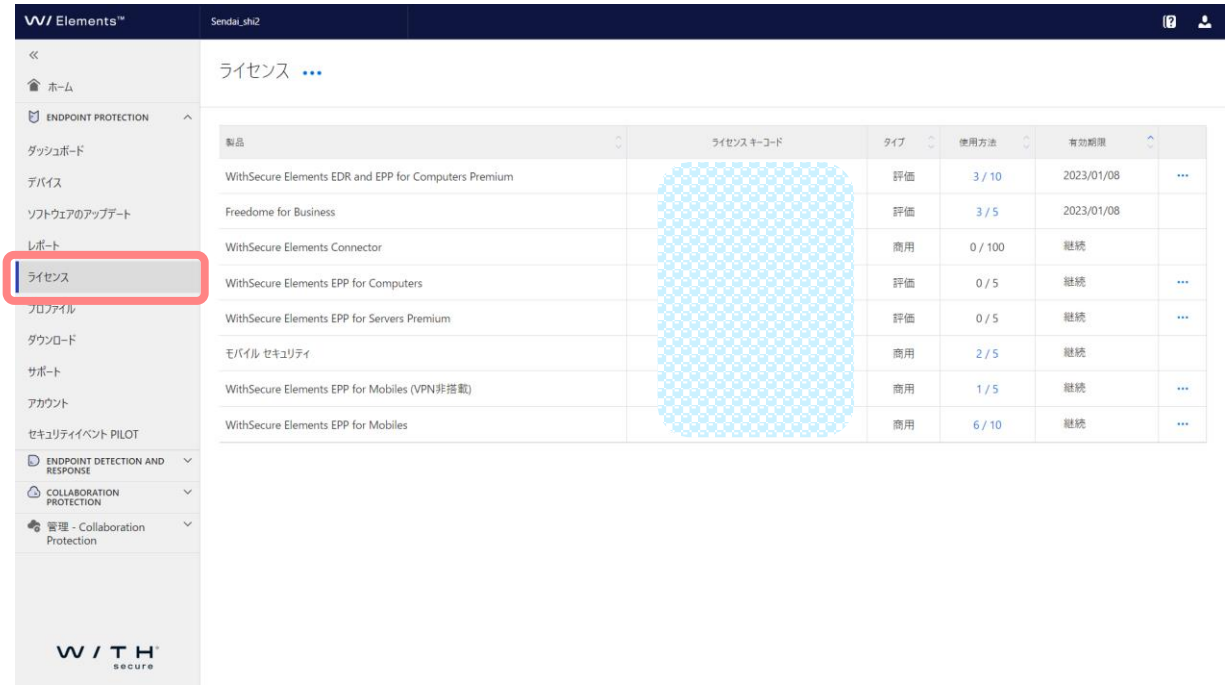


10.11.10. デフォルトブラウザ別のコンピュータ



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

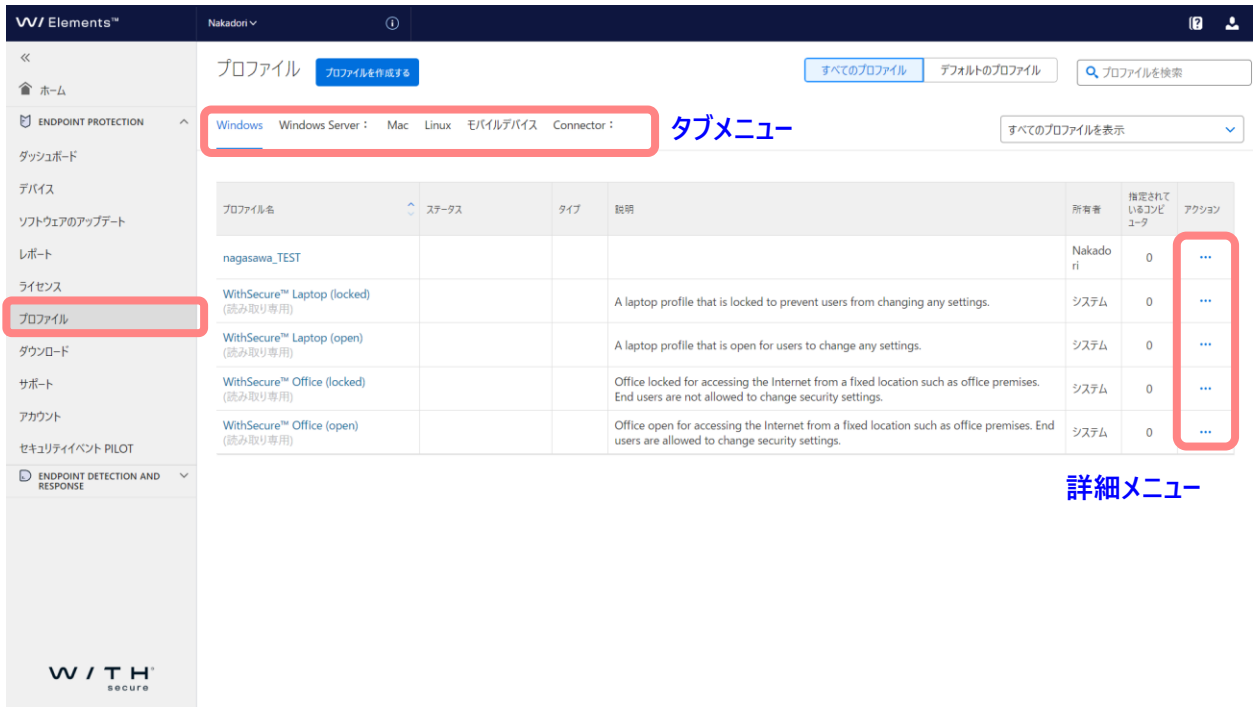
項目名	内容
ライセンスキーコードを追加	キーコードを入力することで追加できます

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。



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

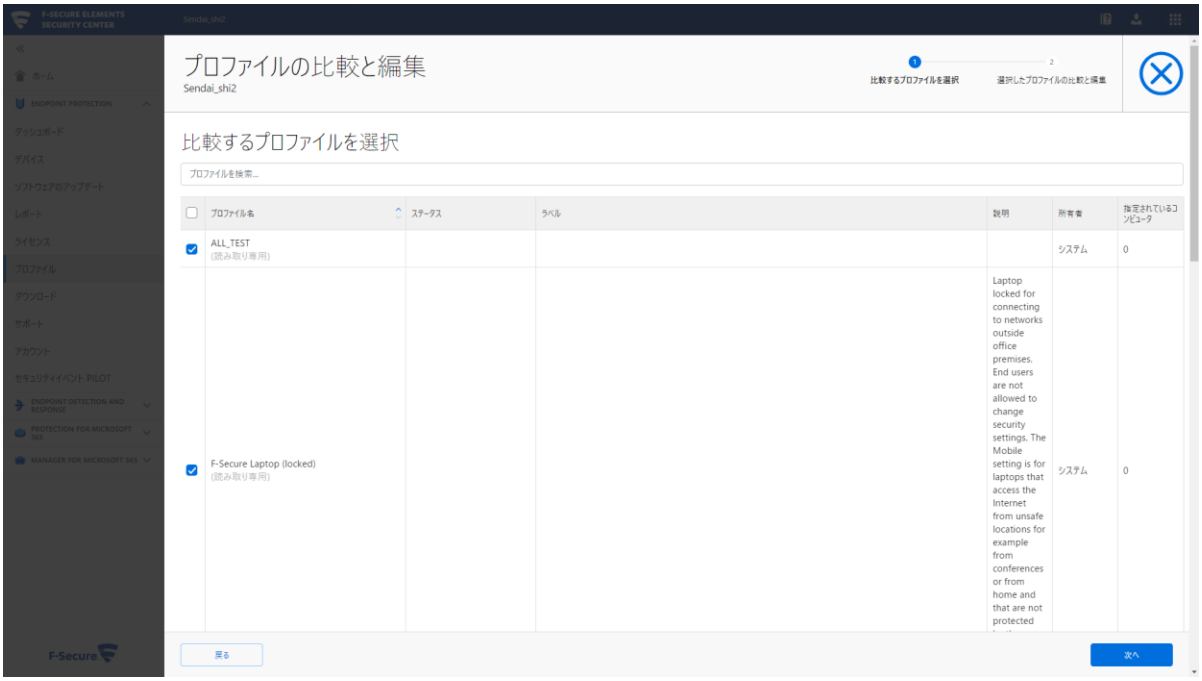
[アクションメニュー] をクリックすると、操作メニューが表示されます。

プロファイル 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）

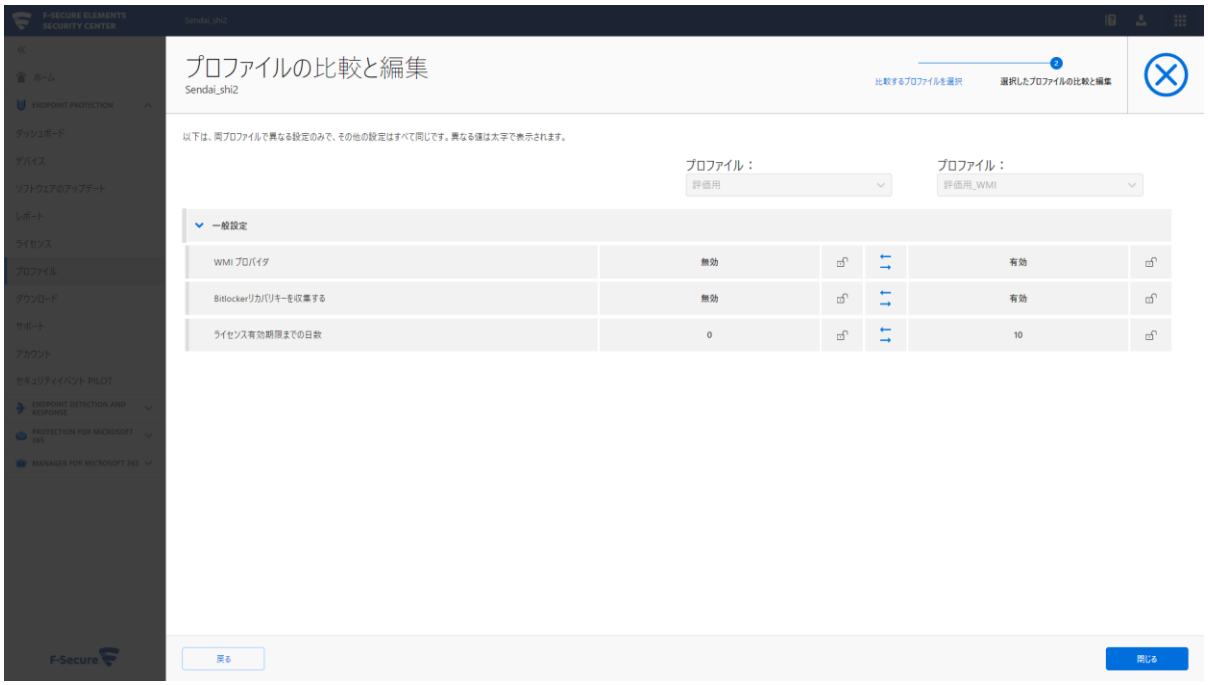
項目名	内容
プロファイルをクローンする	選択中のプロファイルを基に新たなプロファイルを作成します。
プロファイルを削除	選択中のプロファイルを削除します。
プロファイルの比較と編集	選択中のプロファイルと選択可能なプロファイルを比較できます。
「Windows　Server」プロファイルにコピーする	選択中のプロファイルをサーバのデフォルトプロファイルにコピーできます。

・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

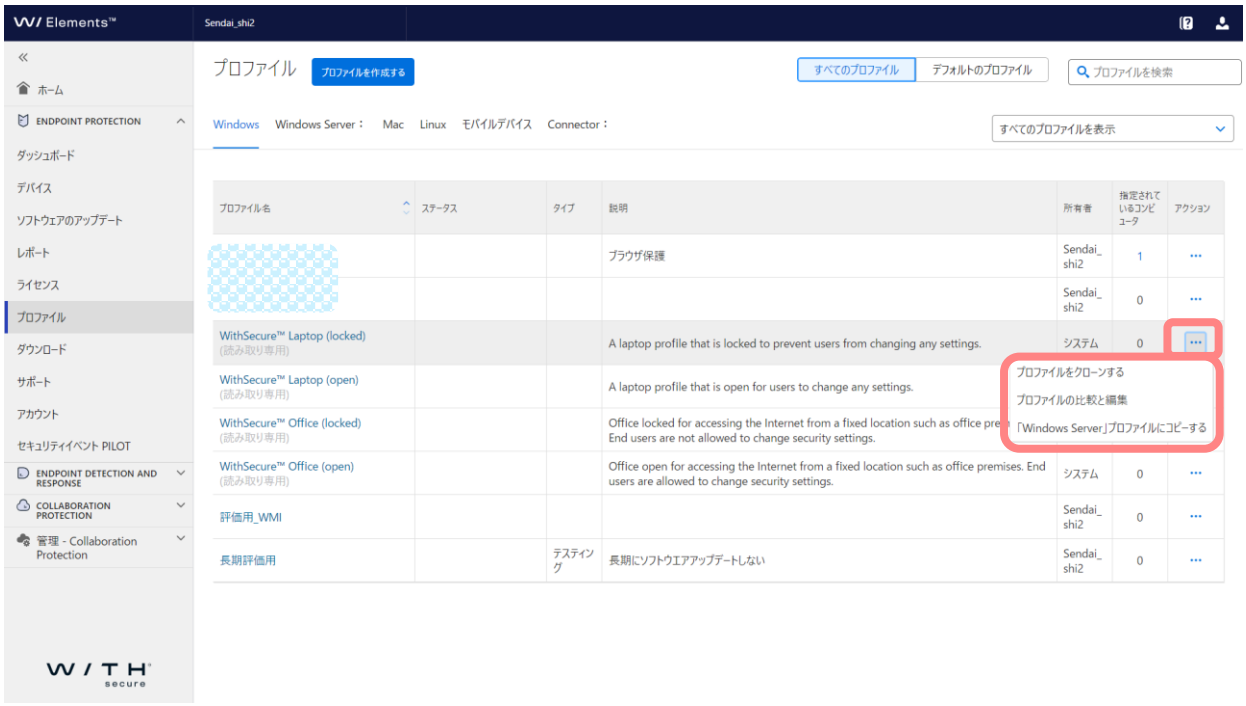
ロック

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

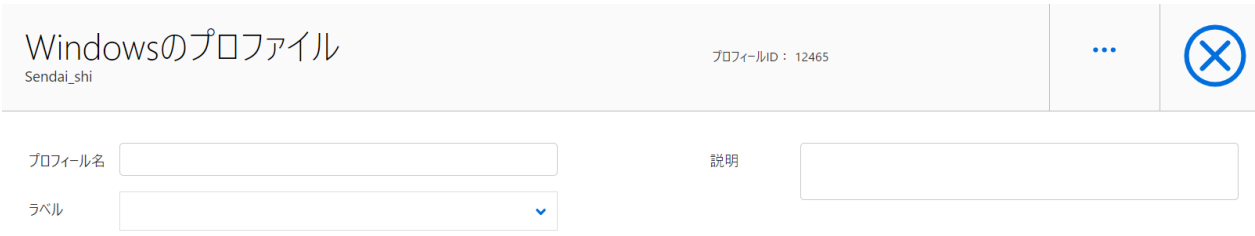
独自の設定値からなるカスタムプロファイルを作成することができます。基本のプロファイルでは自社の用途に合わない場合等などに使用します。



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

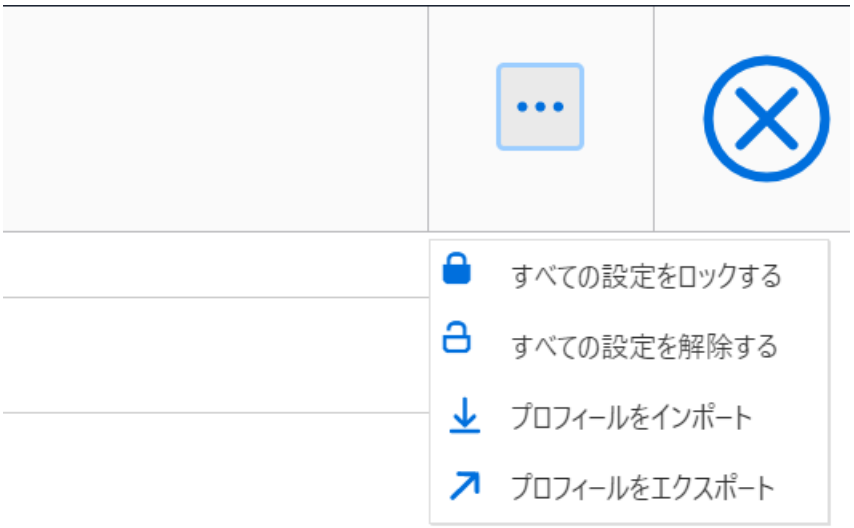


ルが作成されます。

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
プロファイルをインポート	json 形式のプロファイルをインポートする
プロファイルをエクスポート	プロファイルを 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

項目名	内容
クライアント ソフトウエアを誰よりも早く利用する	クライアント ソフトウエ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	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

12.6.2. ウイルスのリアルタイム スキャン

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
リスクウエ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	
スパイウエ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。
すべてのリスクウエアを除外する	すべてのリスクウエアのスキャンをスキップできます。	
すべてのスパイウエアを除外する	すべてのスパイウエアのスキャンをスキップします。	

除外されたリスクウエア/スパイウエア

項目名	内容
除外されたリスクウエア/スパイウエア	スパイウエアまたはリスクウエアをリアルタイム 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。

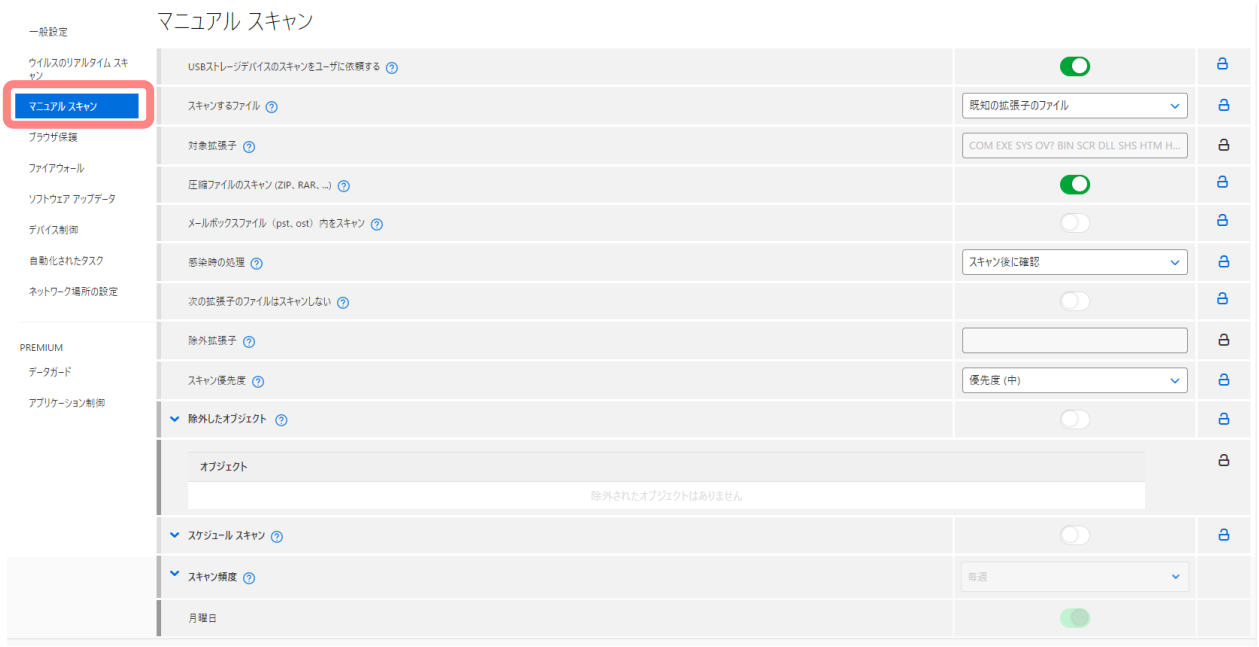
ディープガード

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、およびスパイウエ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

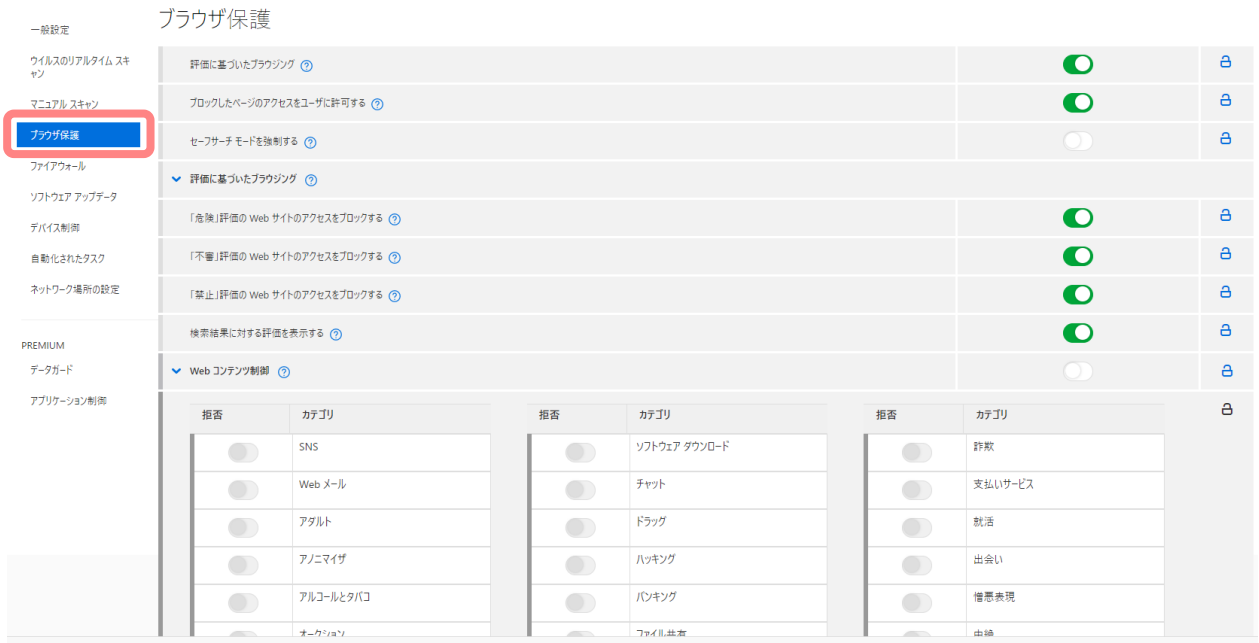
項目名	内容
スキャンを低い優先度で実行する	有効な場合、スケジュールスキャンに割り当てられる CPU のリソースの優先度が下げられます。
指定ファイルのみスキャン(高速)	有効な場合、主要なファイルのみをスキャンし、短時間でスキャンを終了します。
圧縮ファイルをスキャン(低速)	有効な場合、圧縮ファイルのスキャンを行うため、スキャンが要する時間が長くなります。
通知をユーザに表示する	スケジュールスキャンの通知を表示します

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。	
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

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	ndows 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 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タ

項目名	内容
ソフトウェアアップデータ	ソフトウェアアップデータの機能の有効/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エ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	ソフトウエ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エアアップデータをオンにします。
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エアを含める

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

ソフトウエアを自動インストールから除外

項目名	内容
ソフトウエ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タによって自動的にインストールさせないソフトウエアの名前を入力します。名前に一致するソフトウエアは、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、ソフトウエアアップデータと 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タ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	ソフトウエ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	ソフトウエ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タ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。

12.6.7. デバイス制御

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。

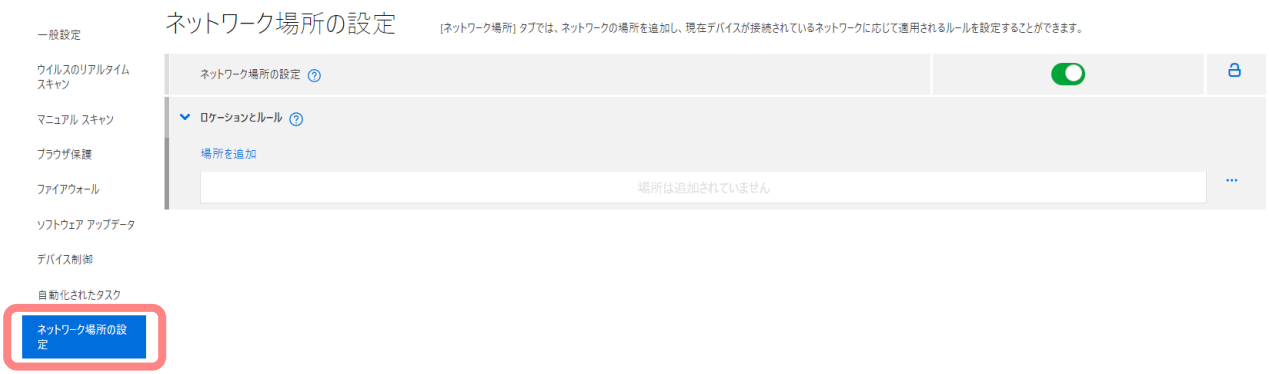
デバイスのアクセスルール

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



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に適用されます。

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適用されます。

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

項目名	内容
クライアント ソフトウエアを誰よりも早く利用する	クライアント ソフトウエ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

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
リスクウエ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	
スパイウエ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。
すべてのリスクウエアを除外する	すべてのリスクウエアのスキャンをスキップできます。	
すべてのスパイウエアを除外する	すべてのスパイウエアのスキャンをスキップします。	

除外されたリスクウエア/スパイウエア

項目名	内容
除外されたリスクウエア/スパイウエア	スパイウエアまたはリスクウエアをリアルタイム 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。

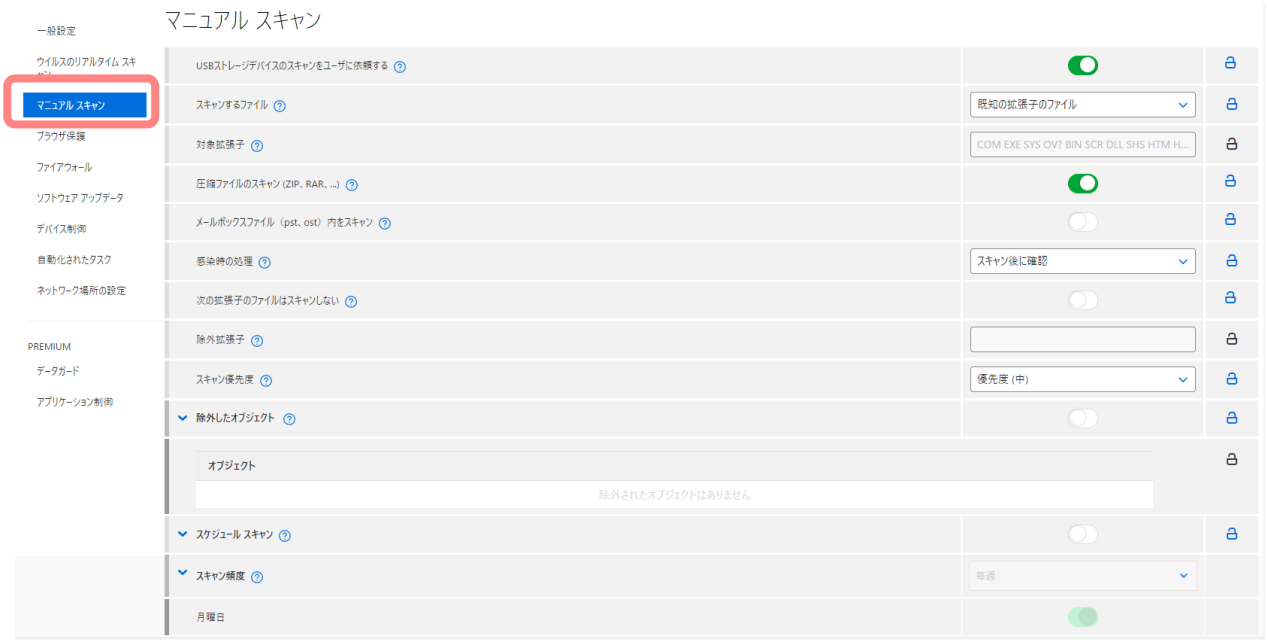
ディープガード

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。

12.7.3. 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	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、およびスパイウエ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。

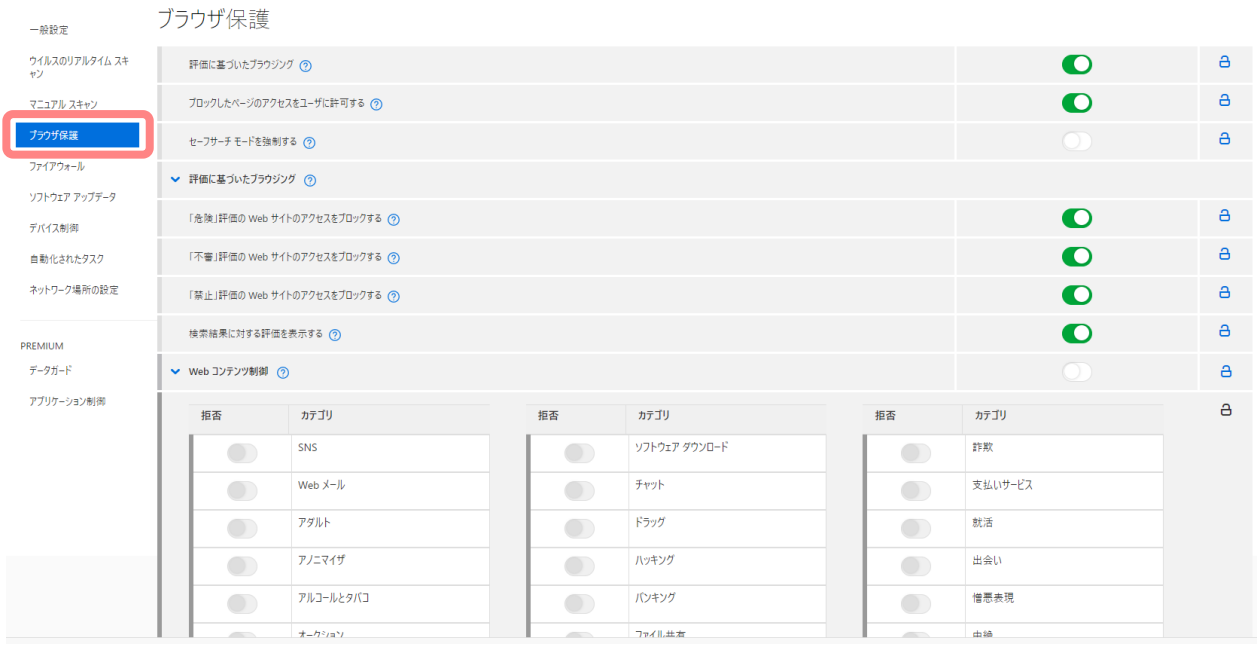
指定ファイルのみスキャン(高速)	有効な場合、主要なファイルのみをスキャンし、短時間でスキャンを終了します。
圧縮ファイルをスキャン(低速)	有効な場合、圧縮ファイルのスキャンを行うため、スキャンが要する時間が長くなります。
通知をユーザに表示する	スケジュールスキャンの通知を表示します

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



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

項目名	内容	
WithSecure™ファイアウォールプモード	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 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。

12.7.6. ソフトウェアアップデータ

項目名	内容
ソフトウェアアップデータ	ソフトウェアアップデータの機能の有効/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エ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	ソフトウエア 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エア アップデータをオンにします。
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エアを含める

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

ソフトウエアを自動インストールから除外

項目名	内容
ソフトウエ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タによって自動的にインストールさせないソフトウエアの名前を入力します。名前に一致するソフトウエアは、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、ソフトウエア 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タ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	ソフトウエ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	ソフトウエア 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タ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
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
リムーバブル大容量ストレージデバイス
書込みアクセスを許可
実行可能ファイルの実行を許可
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

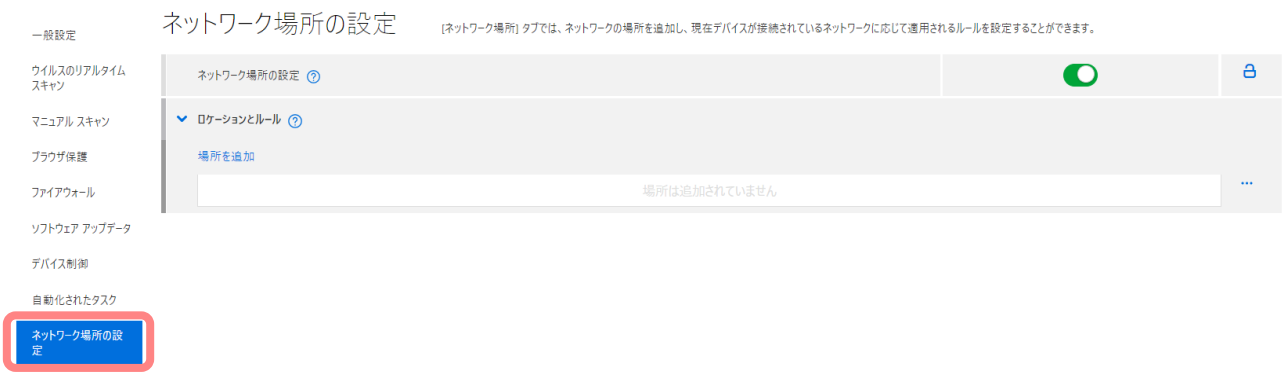
項目名	内容
デバイスのアクセスルール	USB デバイスへのアクセスルールを許可またはブロックで設定します。 USB デバイスは、ハードウェア ID で指定します。USB デバイスのハードウェア ID を確認するには、当該デバイスを接続した Windows PC で、デバイスマネージャでデバイスのプロパティを確認します。

12.7.8.　自動化されたタスク

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



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に適用されます。

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

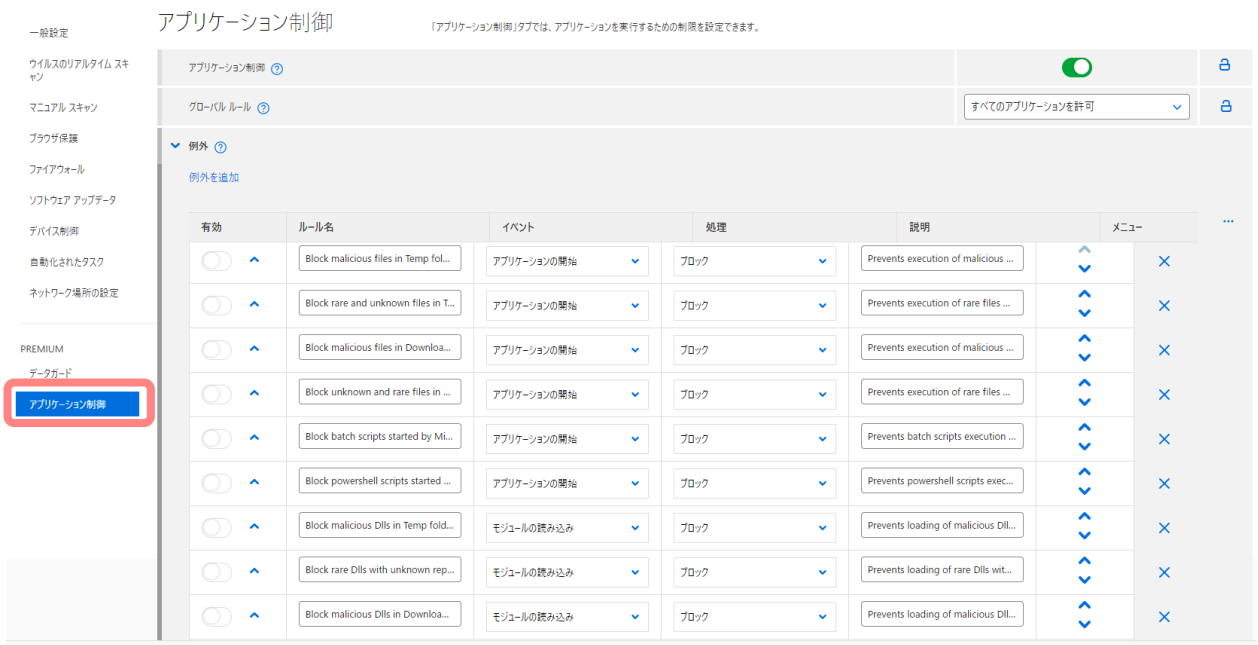
項目名	内容
アクセス制御	データガードが保護しているファイルやフォルダを変更できるアクセス権をアプリケーションに指定できます。
信頼済みのアプリケーションを自動的に検出する	信頼できるアプリケーションを自動的に検出することができます
手動で追加された信頼済みのアプリケーションとフォルダ	信頼できる実行可能ファイルと信頼できる実行可能ファイルを含むフォルダを手動で定義することができます。

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に適用されます。



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

項目名	内容
クライアント ソフトウエアを誰よりも早く利用する	クライアント ソフトウエ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出来ます。
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

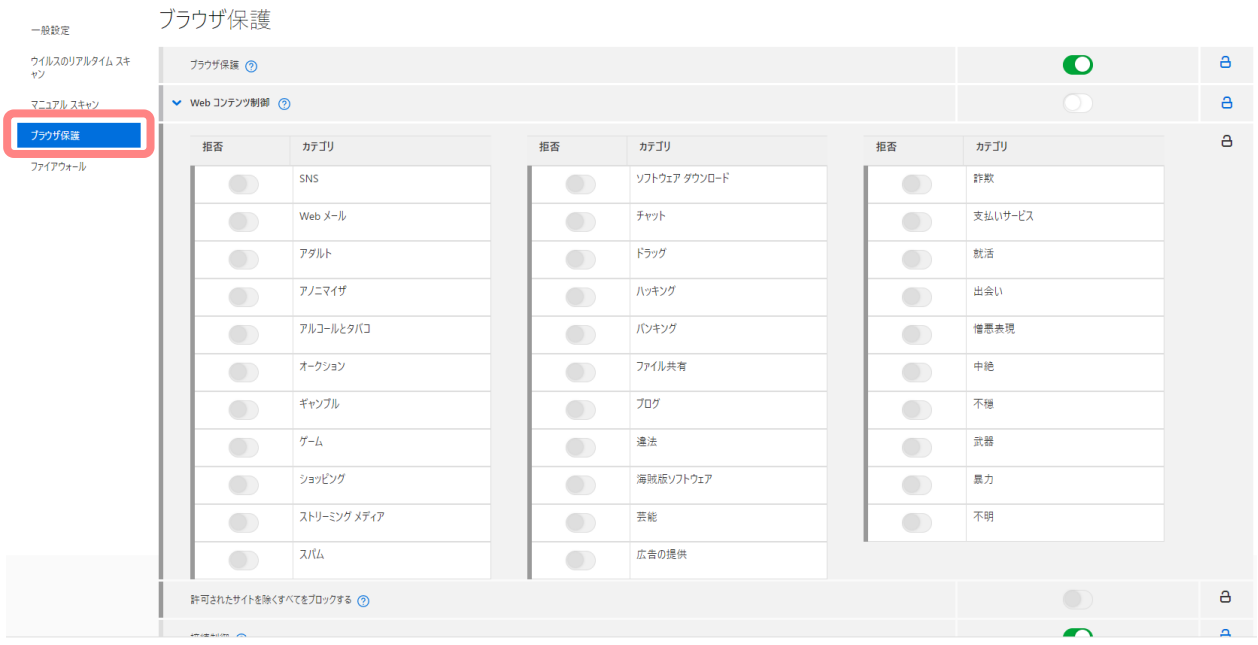
項目名	内容
ウイルスのリアルタイム スキャン	リアルタイム スキャンの有効/無効を設定します。
Security Cloud (ORSP)	リアルタイム スキャン時に、Security Cloud のファイルレピュテーションを使用するかどうかを設定します。
XFence	Mac の振る舞い検知機能である XFence を使用するかどうかを設定します。

12.8.3. マニュアルスキャン

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



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。

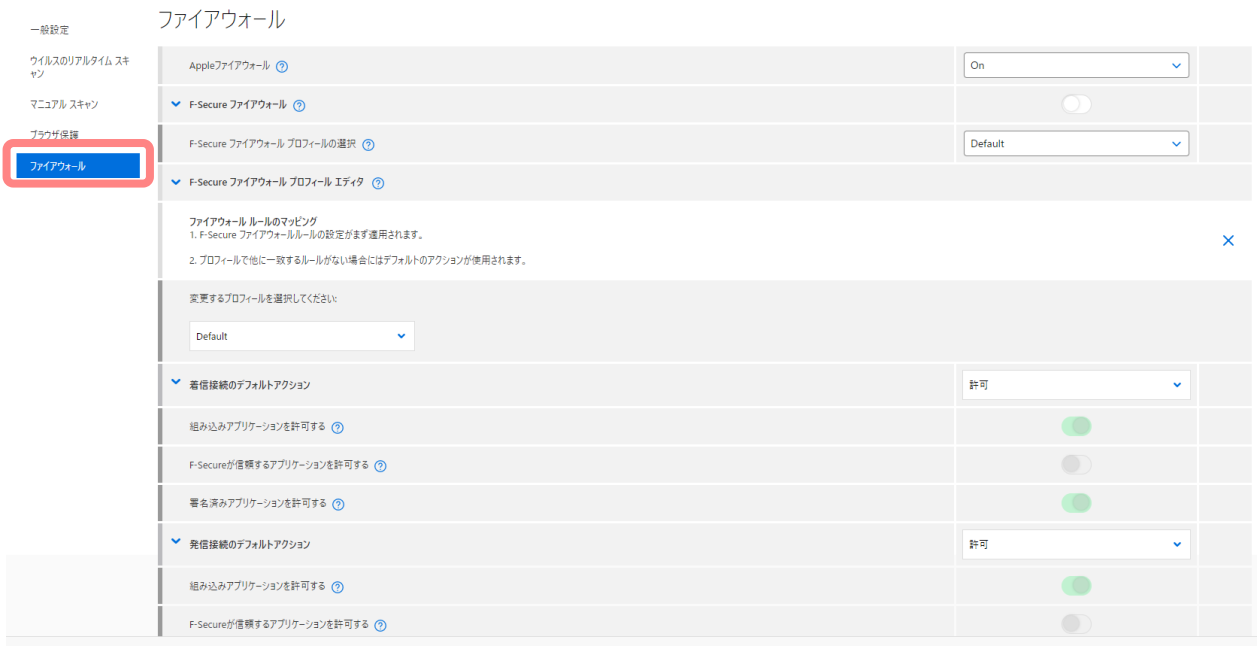
Web サイトの例外

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



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

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

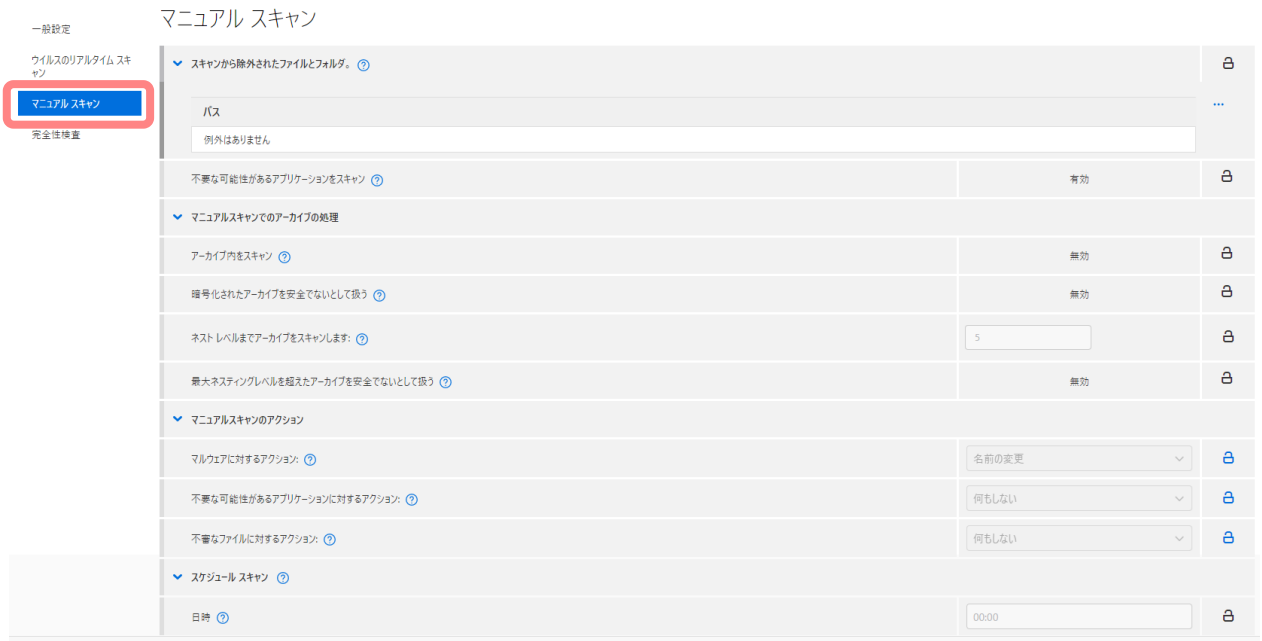
12.9.2. ウイルスのリアルタイム スキャン

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	不要の可能性が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



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。
不要な可能性があるアプリケーションをスキャン	この設定により、不要の可能性が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。
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。
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。

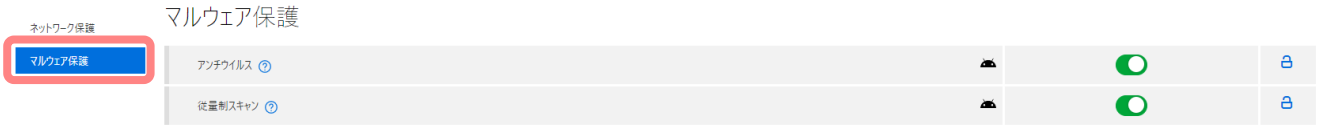
12.10. モバイルデバイス プロファイル

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

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

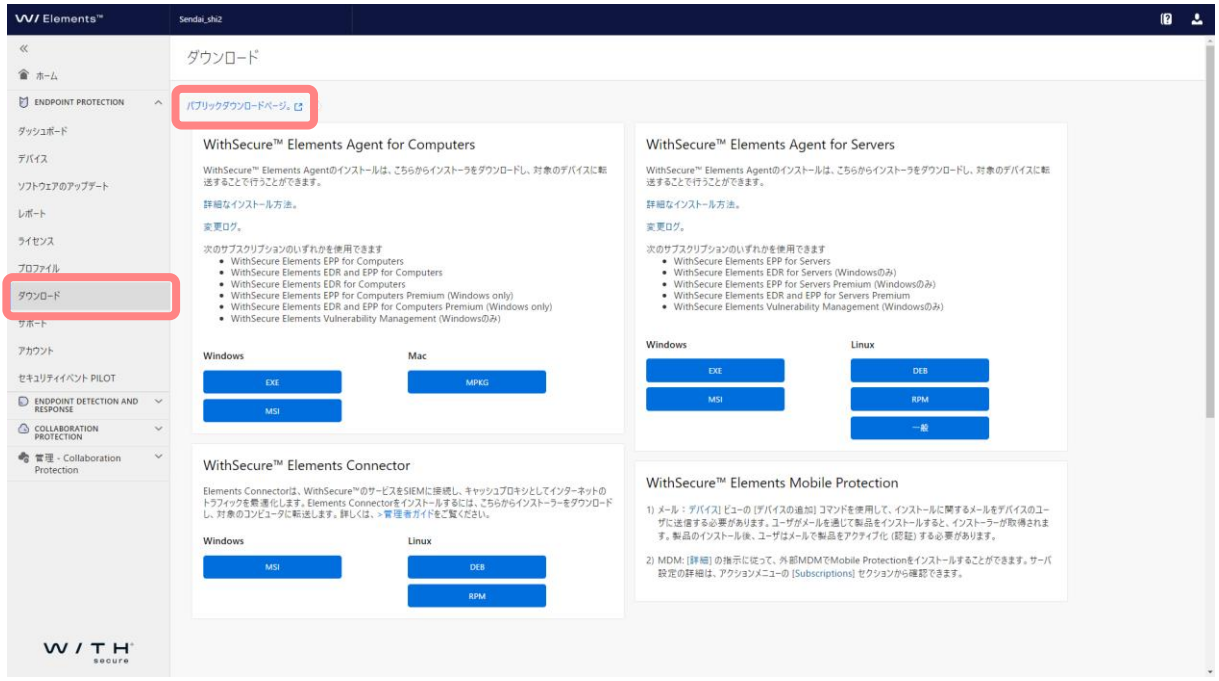
項目名	内容
通信設定	マルウェア定義の自動更新を処理設定
ポーリング間隔	サーバをポーリングする頻度
最大ディスク容量（MB）	プロキシがソフトウエアの更新に割り当てることができる最大ディスク容量
データベースが古くなっている日数	最後にインストールされたウイルス署名データベースの更新からの日数がこの値を超えると、ユーザに警告が表示されます。
HTTP プロキシ	HTTP プロキシ設定
手動で定義されたプロキシアドレス	HTTP プロキシの手動設定

12.11.2. イベント転送

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

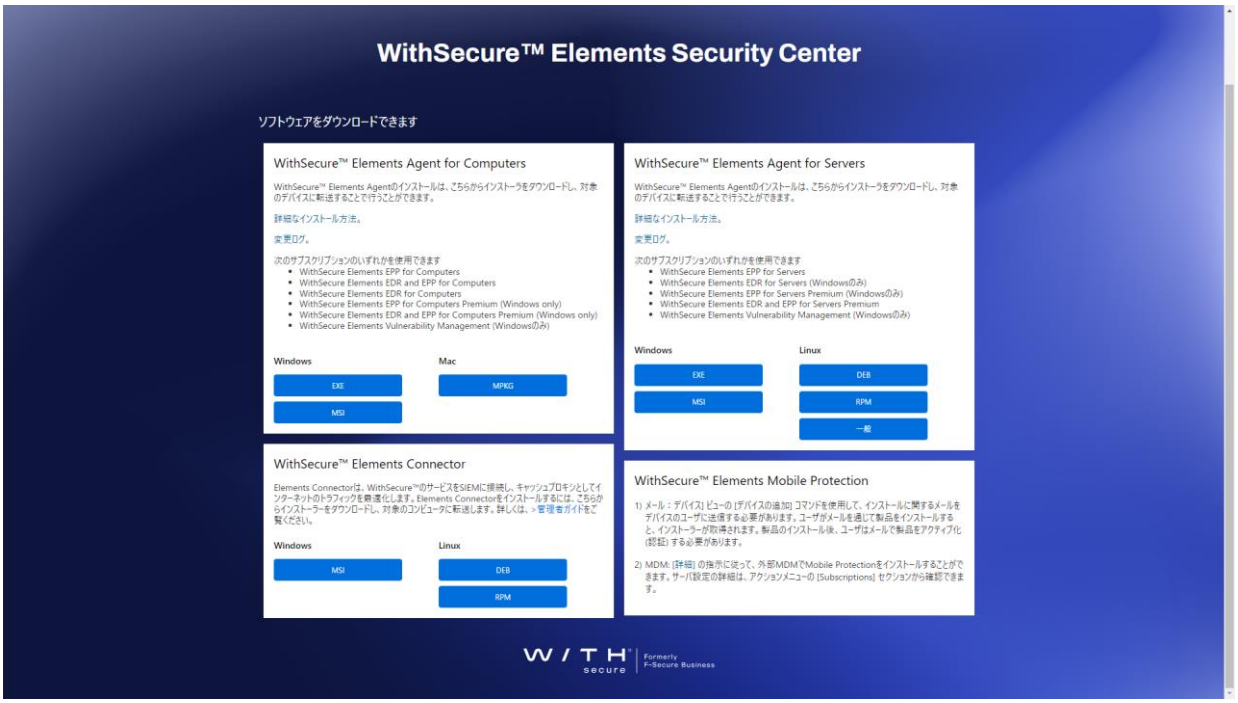
[ダウンロード] ボタンをクリックすると以下の画面が表示されます。ボタンクリックで各種ソフトウエアのダウンロードができます。ご利用の環境に合ったソフトウエアをお使いください。なお、ライセンスを保持していない製品については、ダウンロードリンクが表示されません。



・パブリックダウンロードページ

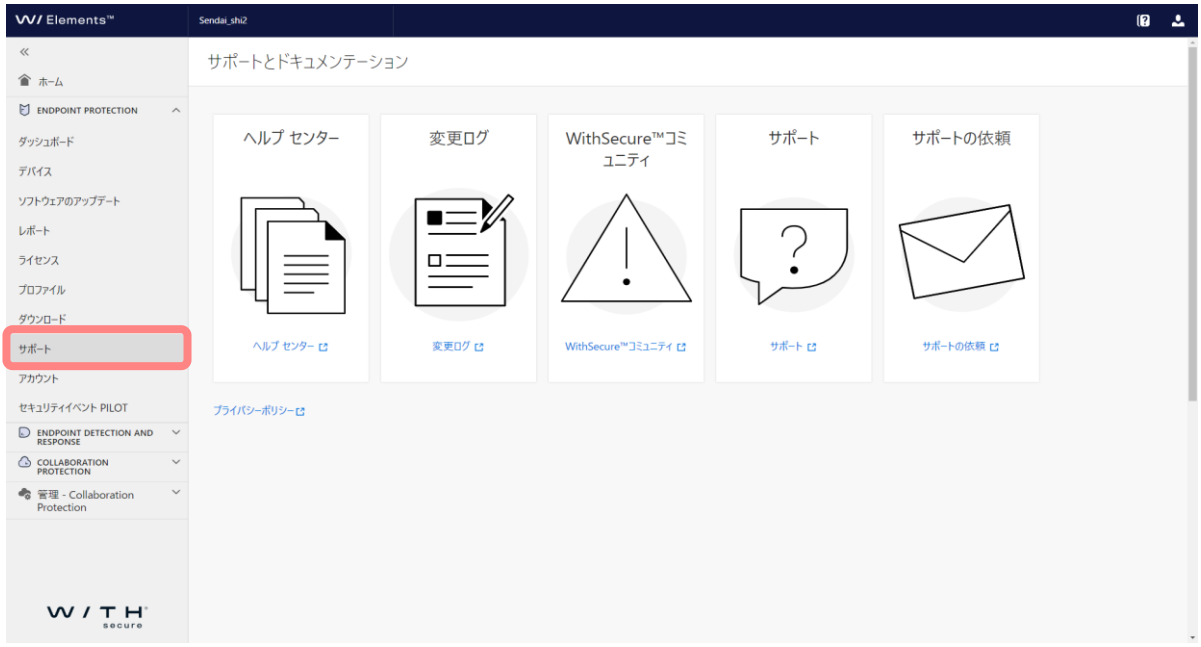
パブリックダウンロードは、展開ツールや IT 担当者がサブスクリプションキーを持っているが Elements Security Center にはアクセスできず、常に最新版をダウンロードするようにしたい場合に URL をご案下さい。

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



14. サポート

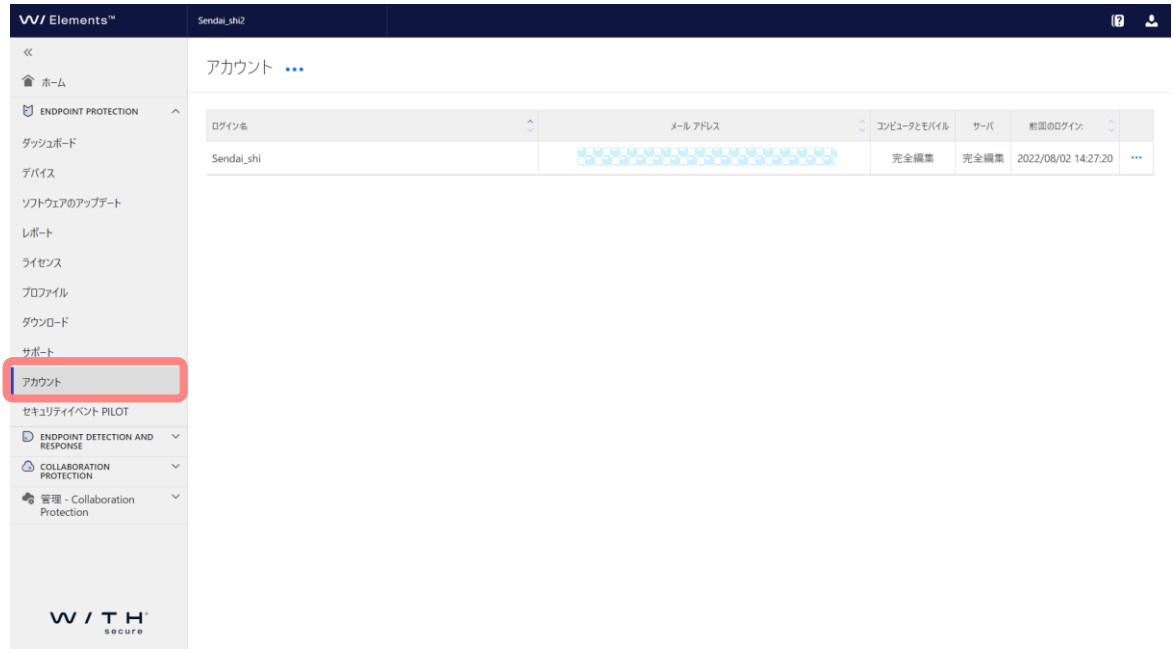
[サポート] ボタンをクリックすると以下の画面が表示されます。リンクをクリックすると各サポートに関する Web サイトが表示されます。



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。

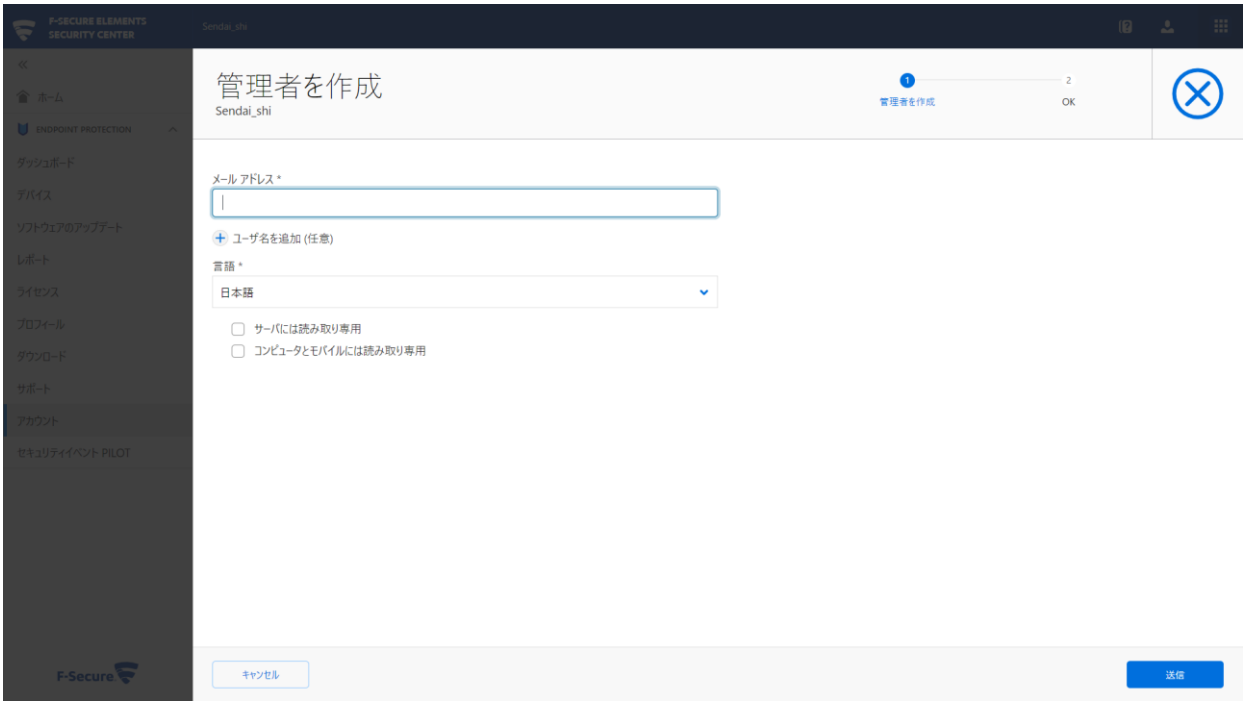
15.2. アカウント管理　[管理者]　タブメニュー

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。



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。

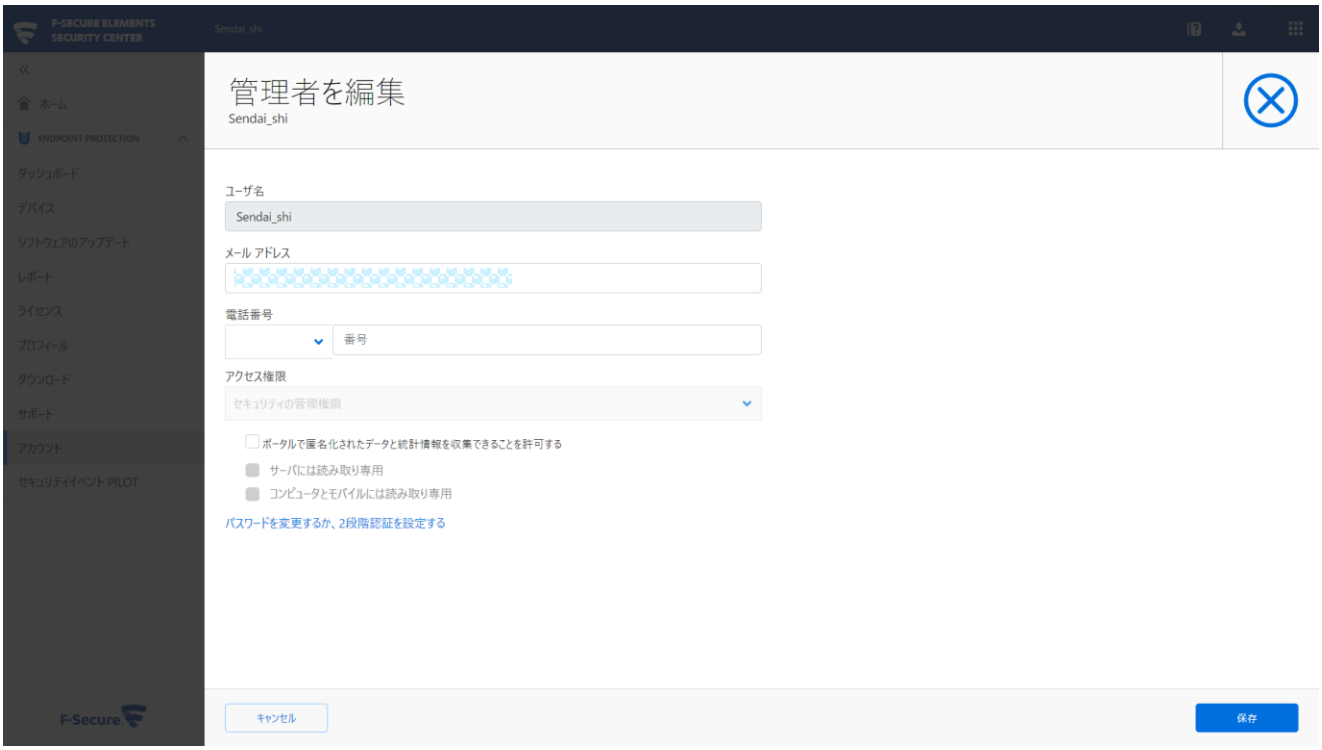
15.2.2. 管理者を編集する

「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。

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。



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

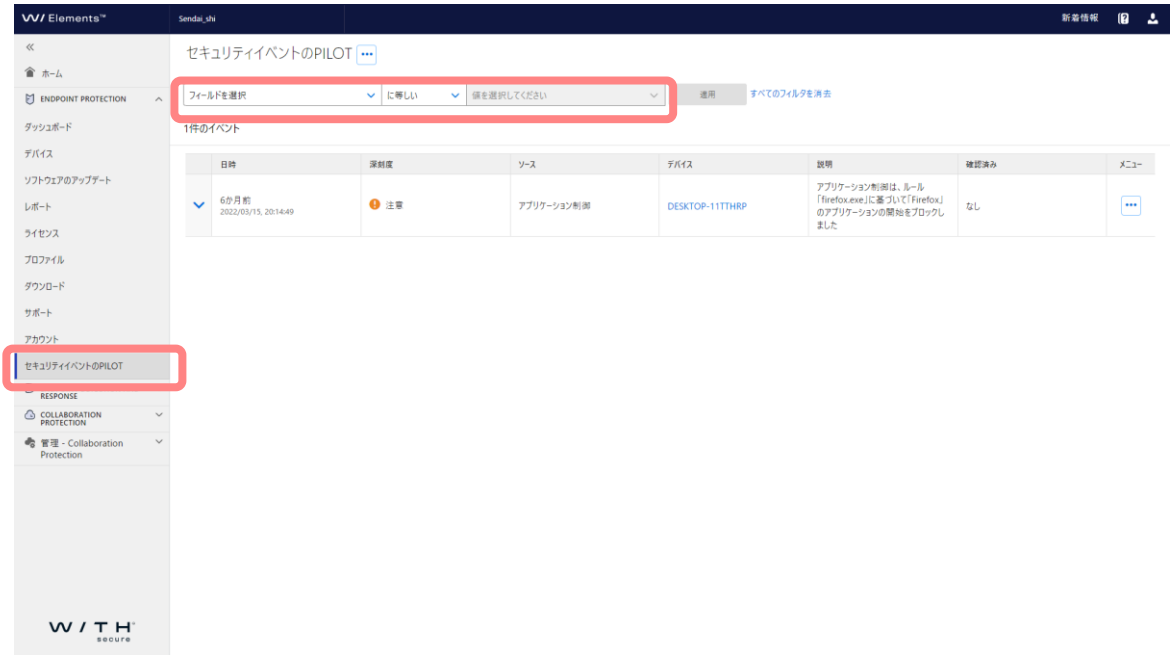
①「アカウント管理」画面にて、削除するユーザの [アクションメニュー] をクリックします。
②[管理者を削除] をクリックします。
③メッセージを確認し [OK] をクリックします。

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

*.fsapi.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