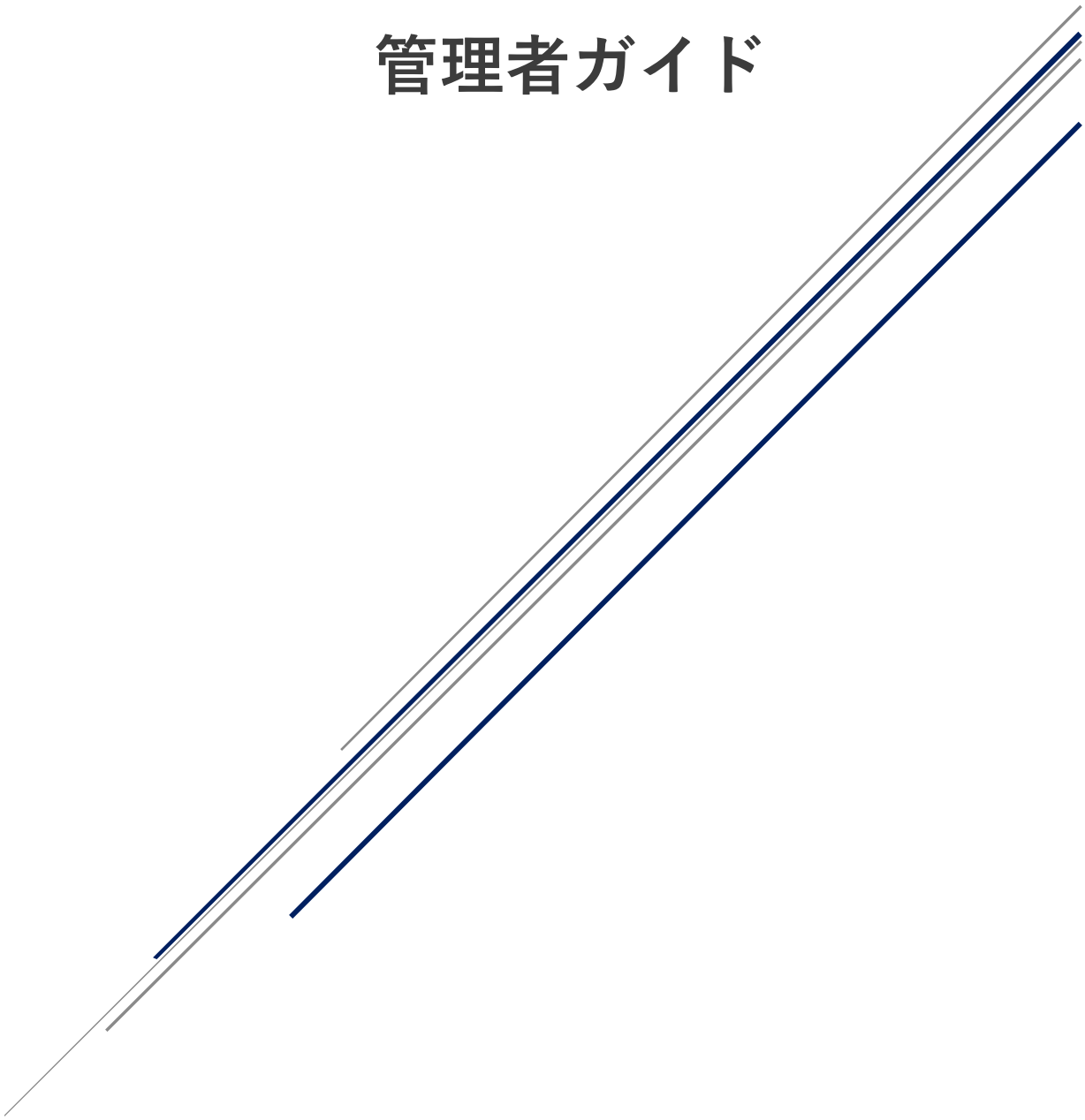
WithSecure™ Elements Security Center

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
機能の追加/削除	1.1	2022/11/11
ログイン URL の変更	1.2	2022/11/20
ESC の変更に伴う全面改訂	1.3	2024/05/13

●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 2024 年 5 月現在の情報を基に記述されております

●商標

WithSecure™及びそのロゴ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。

内容

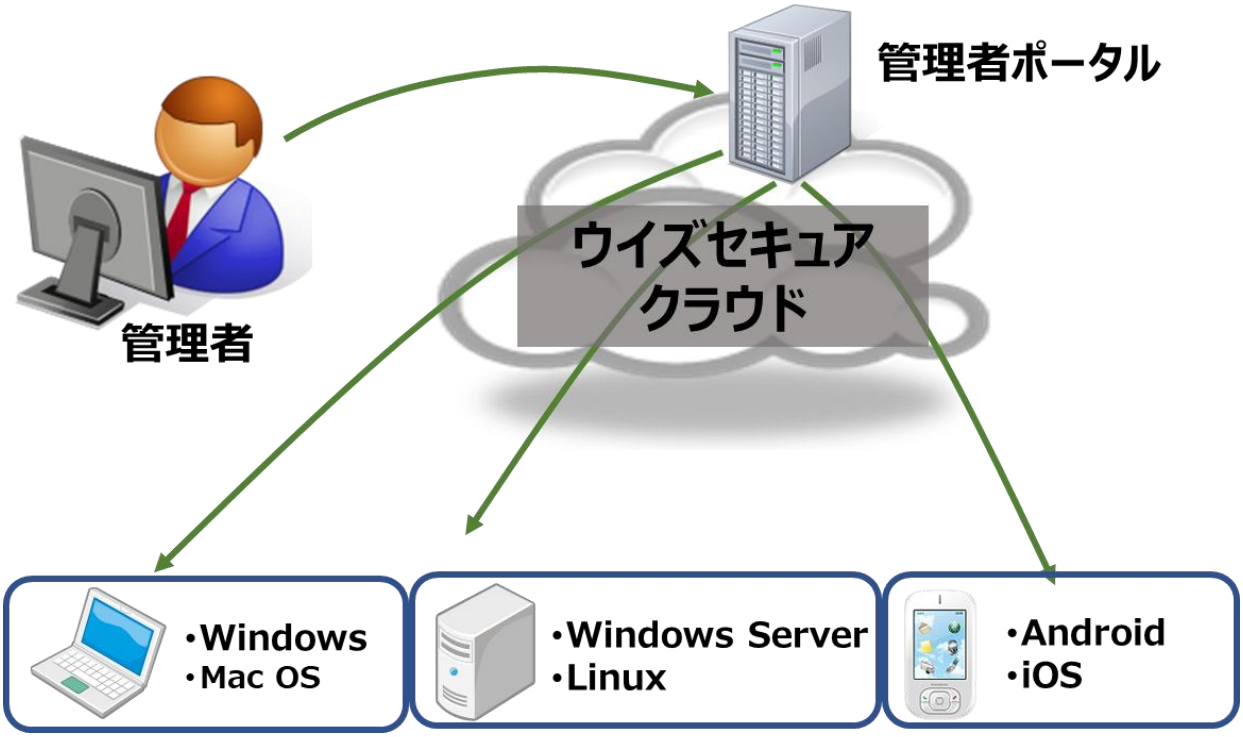
1. はじめに

本書は WithSecure™ Elements EPP for Computers（以下、「Elements EPP」）の契約ユーザー、または評価ユーザーとしてお使いくださるお客様を対象とした、WithSecure™ Elements Security Center（以下「ESC」）のガイドです。
まず、「2.Elements Security Center 概要」において、ESC 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. Elements Security Center への接続とログイン」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 2024 年 2 月現在の情報を基に記述されています。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、下図の構成概念図に従って、ESC の概要について説明します。



2.1. 対応ブラウザ

ESC は、以下のブラウザに対応しています。

- Microsoft Edge の最新のバージョン
- Google Chrome の最新のバージョン
- Mozilla 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 ESC 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。

  - クライアント用エージェント

    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。
  - サーバー用エージェント

    サーバーOS 向けのソフトウェアです。Windows Server 用、Linux 用があります。
  - モバイル用エージェント

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。
  ESC 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、ESC 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 アカウントの概念

ESC 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 つの企業アカウントを保持します。
  企業アカウントの中に、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**
  ESC 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 ESC 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。

  ➢ 管理者

  すべての ESC 機能を使用できます。

  ➢ 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ください。

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。
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す。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、利用可能な台数は契約により決められています。
- 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(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

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。

- ESC へアクセスする為のユーザアカウントを作成します
- ESC からインストールプログラムをダウンロードし、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 ESC へ自動登録され、集中管理ができるようになります。

3. Elements Security Center への接続とログイン

ESC 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.withsecure.com/

以下の画面が開きますので、ここから「ユーザー名」と「パスワード」を入力し、ログインボタンをクリックします。

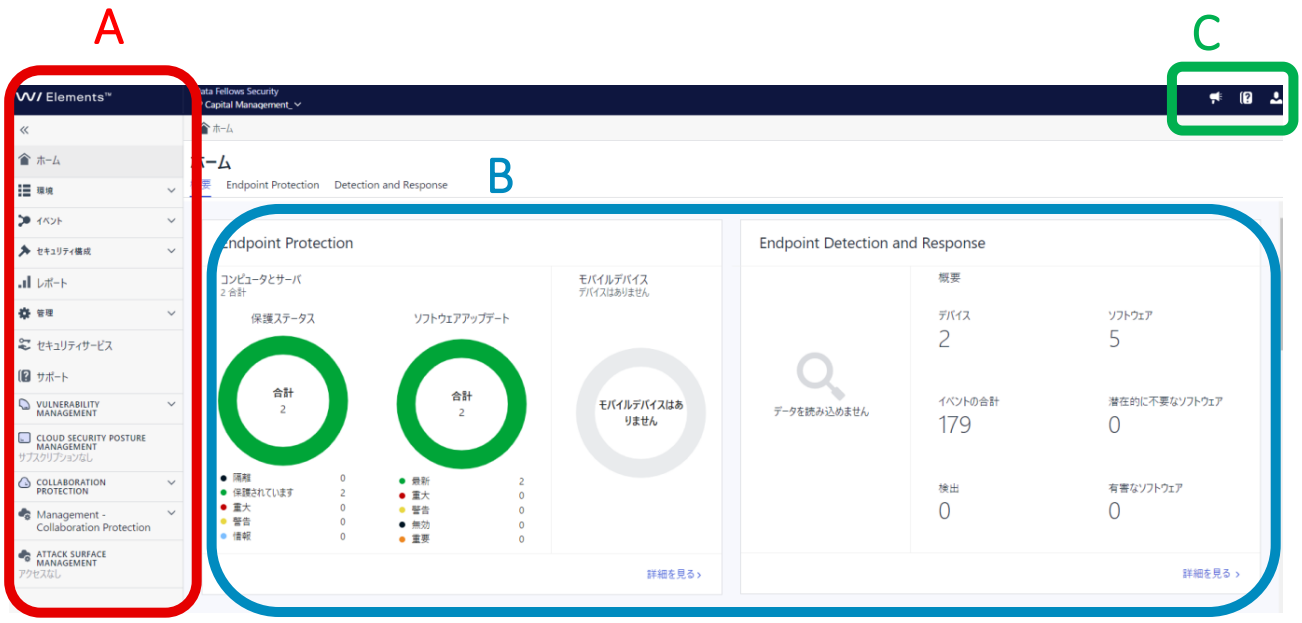
※2024 年 6 月 30 日以降ユーザー名が廃止となります為、メールアドレスをご利用ください。

4. Elements Security Center の画面

ここでは、ESC 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 メニュー概要

ESC へログインをすると、以下の画面が表示されます。



A.　サイドメニュー

機能ごとにメニューがまとめられています。所持している製品によりアクセスできるメニューに制限があります。

B.　表示画面

選択したサイドメニューの情報を表示します。

C.　その他メニュー

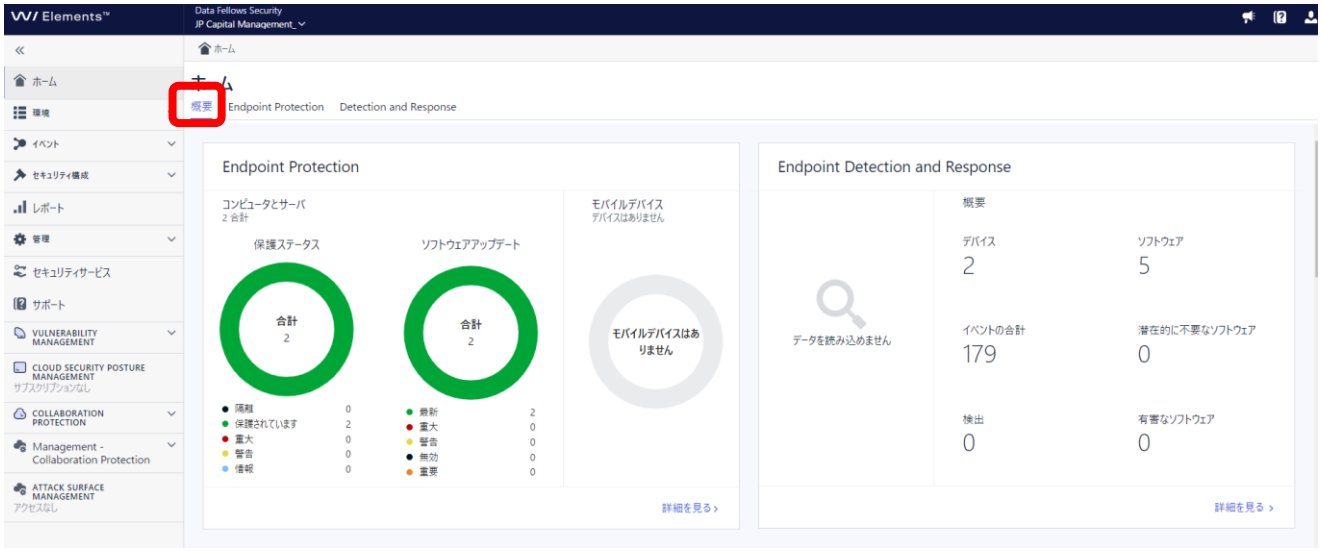
その他のメニューボタンです。

5. ホーム

ここでは、ESC のホームについて説明します。

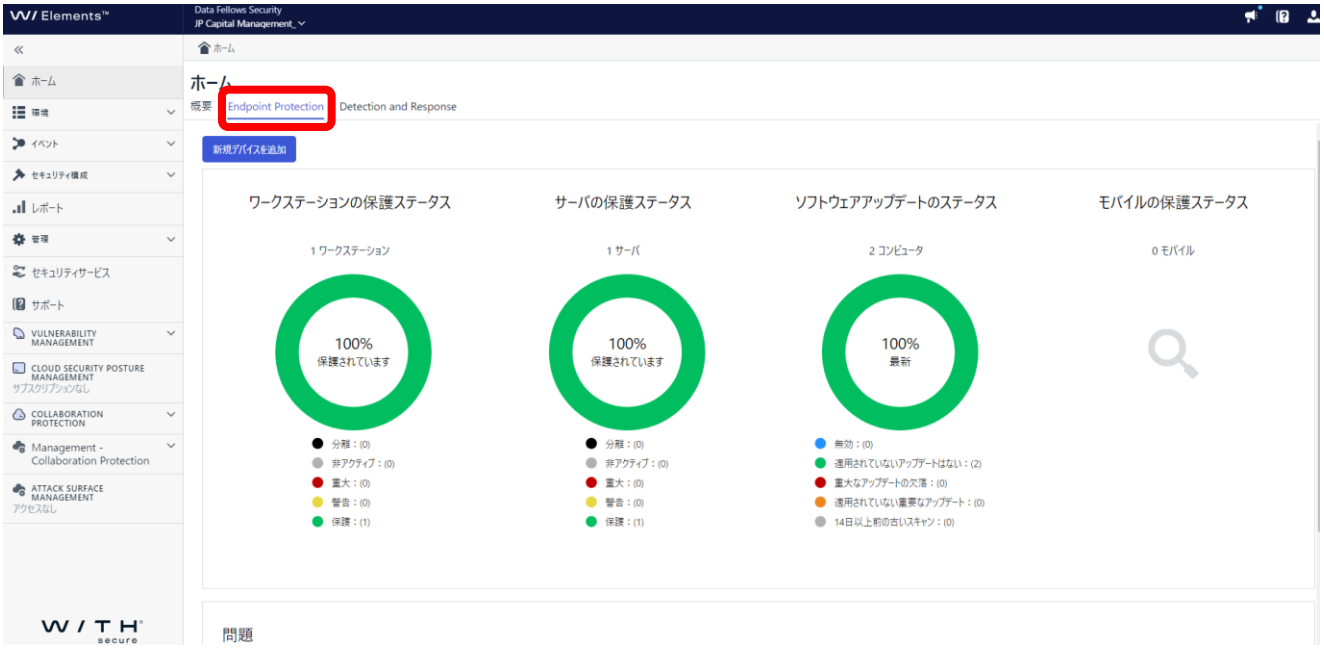
5.1.　Elements Security Center ホーム概要

ESC のホームを選択すると、以下の画面が表示されます。



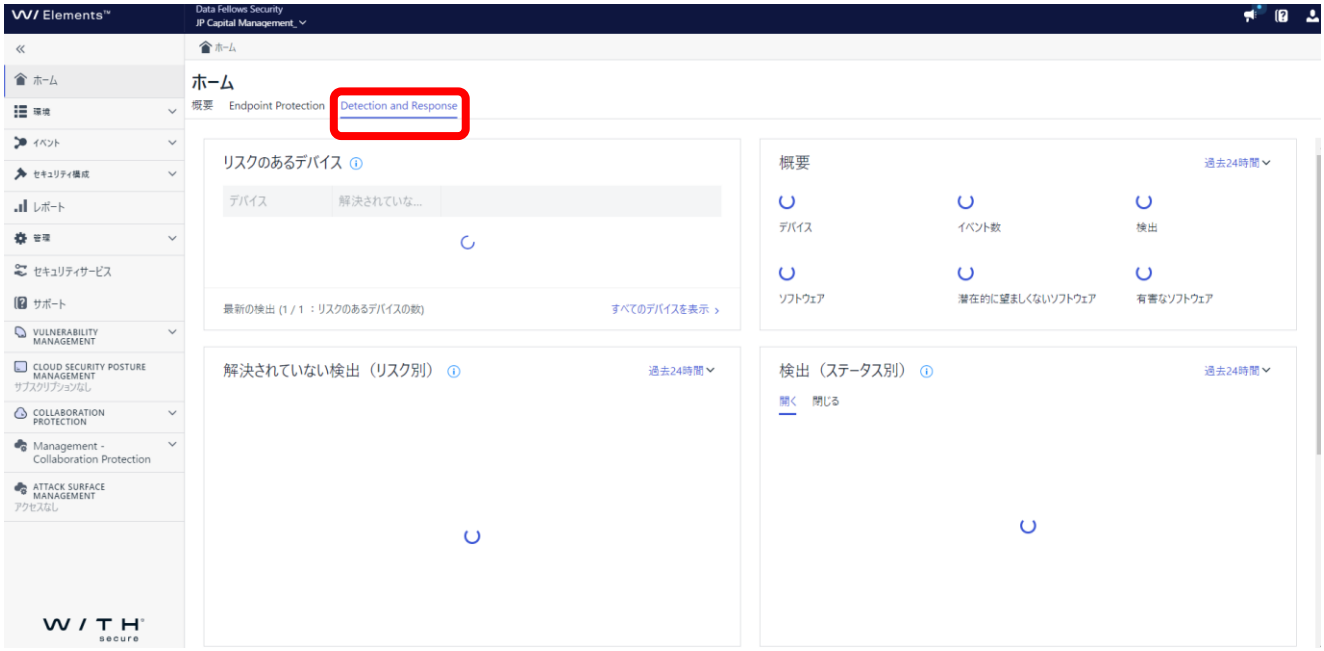
➢　概要

Elements 製品の全体的な状況を把握できます。



➢ Endpoint Protection

Elements Endpoint Protection に関するダッシュボードです。
端末やサーバーの状況をグラフィカルに把握することができます。
また、下部にある問題の項目では、対処が必要な可能性のある事象が記載されています。

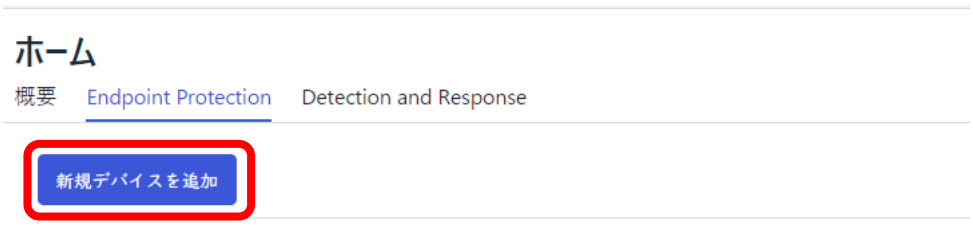


➢ Detection and Response

Elements Endpoint Detection and Response に関するダッシュボードです。
インシデントの発生や対応の状況を概観することができます。

5.2. 新規デバイスの追加

Endpoint Protection の画面では管理するデバイスを新規に追加することができます。
この項目では、対象のデバイスを使用しているユーザーにライセンスキーとインストールモジュールをダウンロードできる URL を送信することができます。
ユーザーは受信したメールに記載されている URL から、自分自身でエージェントをインストール必要があります。



① 追加する製品を選択します。

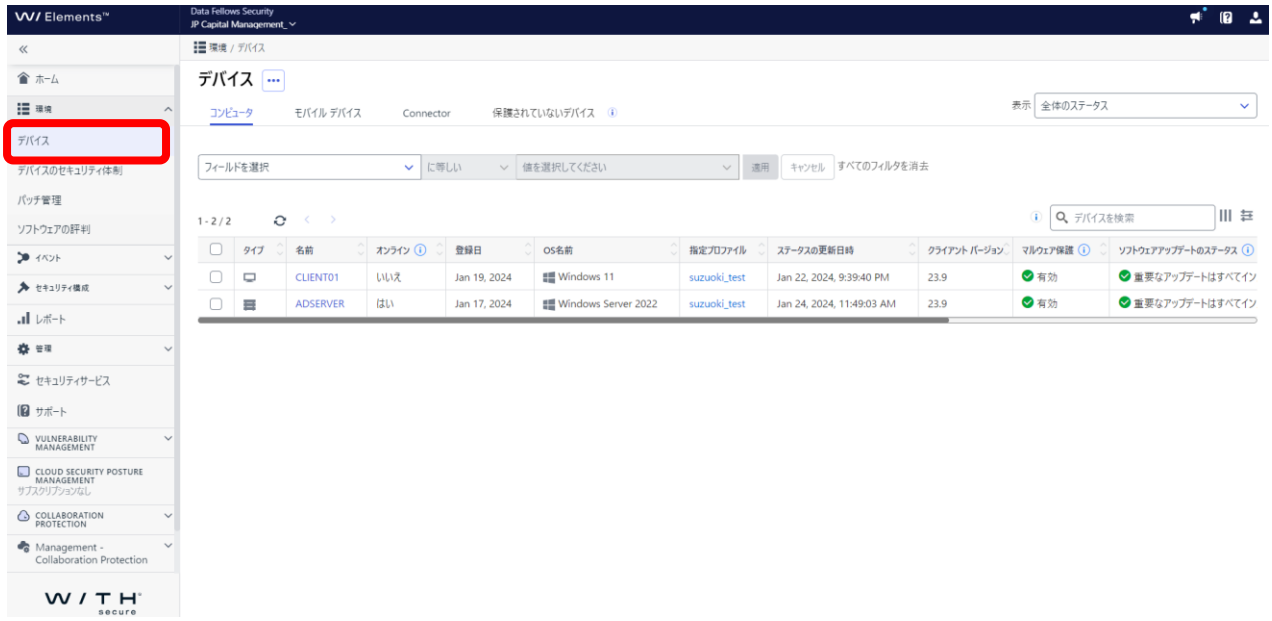
② インストールリンクを送信するメールアドレスを入力し、送信ボタンをクリックします。

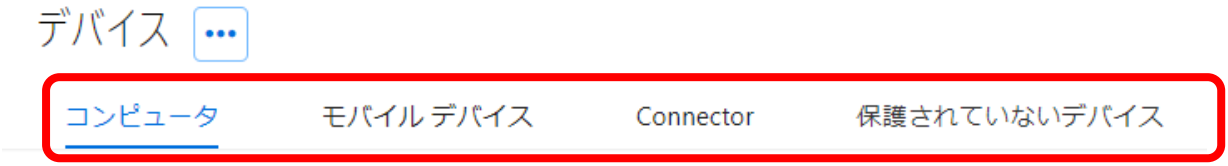
- 複数のメールアドレスに送る際は複数のメール アドレスをカンマ、セミコロン、新しい行で区切りことができます。これにより複数のメールアドレスへ一度に送信できます。
- 送信先を CSV ファイルからインポートすることも可能です。
- [送信]ボタンを押すことで対象のメールアドレスにメールが送信されます。

6. 環境

6.1.　デバイス

[デバイス] では、登録されているデバイスのステータス情報を確認することができます。





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	企業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	企業アカウント内の全てのモバイルが一覧で表示
Connector	企業アカウント内の全ての Connector が一覧で表示
保護されていないデバイス	Active Directory を使用した際に EPP がインストールされていない端末を一覧で表示

6.1.1. 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]画面に移動します。 「5.2 新規デバイスの追加」を参照
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]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]画面に移動します。
運用の管理	[運用の管理]画面に移動します。
削除されたデバイスの管理	[削除されたデバイスの管理]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。

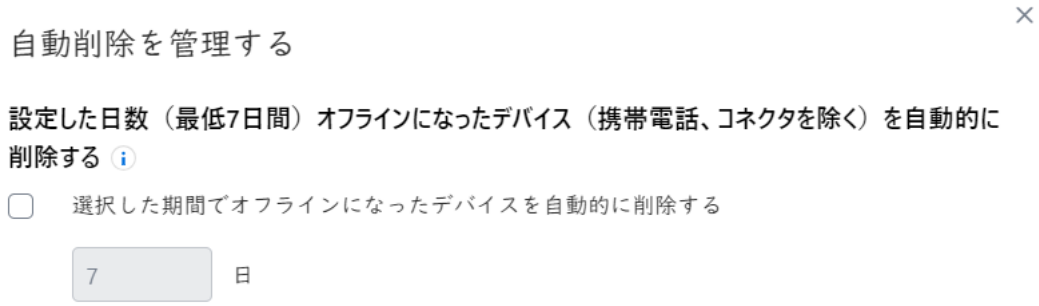
- **デバイスの招待状を管理する**

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。

➢ 送信したメールの無効化、再送を実施することができます。

- **自動削除を管理する**

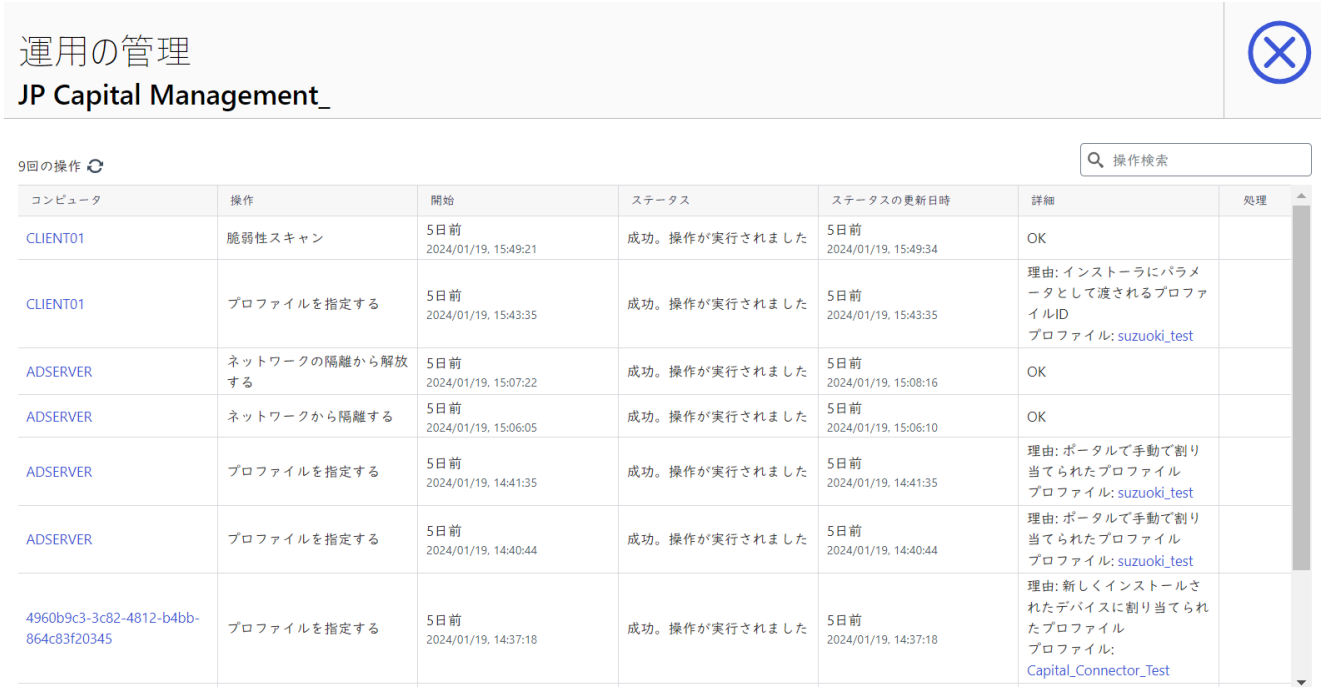
オフラインのデバイスを自動的にポータルから削除する機能です。デバイスが削除されるまでのオフラインの期間を定義することができます。



- 設定可能な期間は 7 日から 365 日です。
- 削除されたデバイスがオンラインになった場合、ライセンス数に空きがあれば、再びポータルに登録されます。空きが無い場合は、ライセンスは無効のままとなり、端末は保護されません。

- **運用の管理**

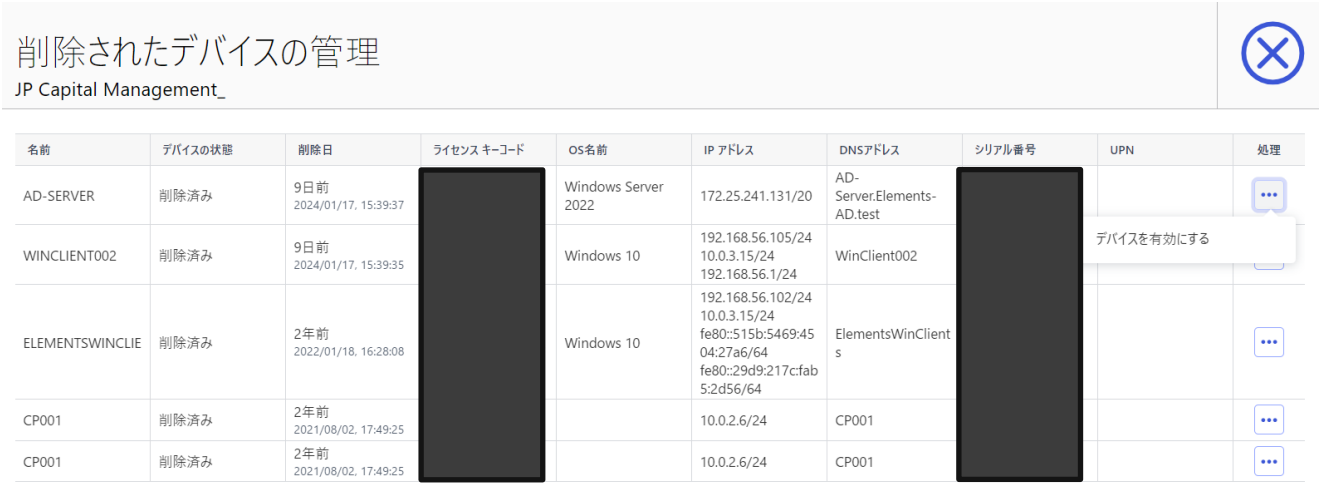
端末への操作の履歴を確認できます。



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
CLIENT01	脆弱性スキャン	5日前 2024/01/19, 15:49:21	成功。操作が実行されました	5日前 2024/01/19, 15:49:34	OK	
CLIENT01	プロファイルを指定する	5日前 2024/01/19, 15:43:35	成功。操作が実行されました	5日前 2024/01/19, 15:43:35	理由: インストーラにパラメータとして渡されるプロファイルID プロファイル: suzuoki_test	
ADSERVER	ネットワークの隔離から解放する	5日前 2024/01/19, 15:07:22	成功。操作が実行されました	5日前 2024/01/19, 15:08:16	OK	
ADSERVER	ネットワークから隔離する	5日前 2024/01/19, 15:06:05	成功。操作が実行されました	5日前 2024/01/19, 15:06:10	OK	
ADSERVER	プロファイルを指定する	5日前 2024/01/19, 14:41:35	成功。操作が実行されました	5日前 2024/01/19, 14:41:35	理由: ポータルで手動で割り当てられたプロファイル プロファイル: suzuoki_test	
ADSERVER	プロファイルを指定する	5日前 2024/01/19, 14:40:44	成功。操作が実行されました	5日前 2024/01/19, 14:40:44	理由: ポータルで手動で割り当てられたプロファイル プロファイル: suzuoki_test	
4960b9c3-3c82-4812-b4bb-864c83f20345	プロファイルを指定する	5日前 2024/01/19, 14:37:18	成功。操作が実行されました	5日前 2024/01/19, 14:37:18	理由: 新しくインストールされたデバイスに割り当てられたプロファイル プロファイル: Capital_Connector_Test	

- **削除されたデバイスの管理**

削除されたデバイスを再度有効にすることができます。



- **デバイスをエクスポート（CSV）**

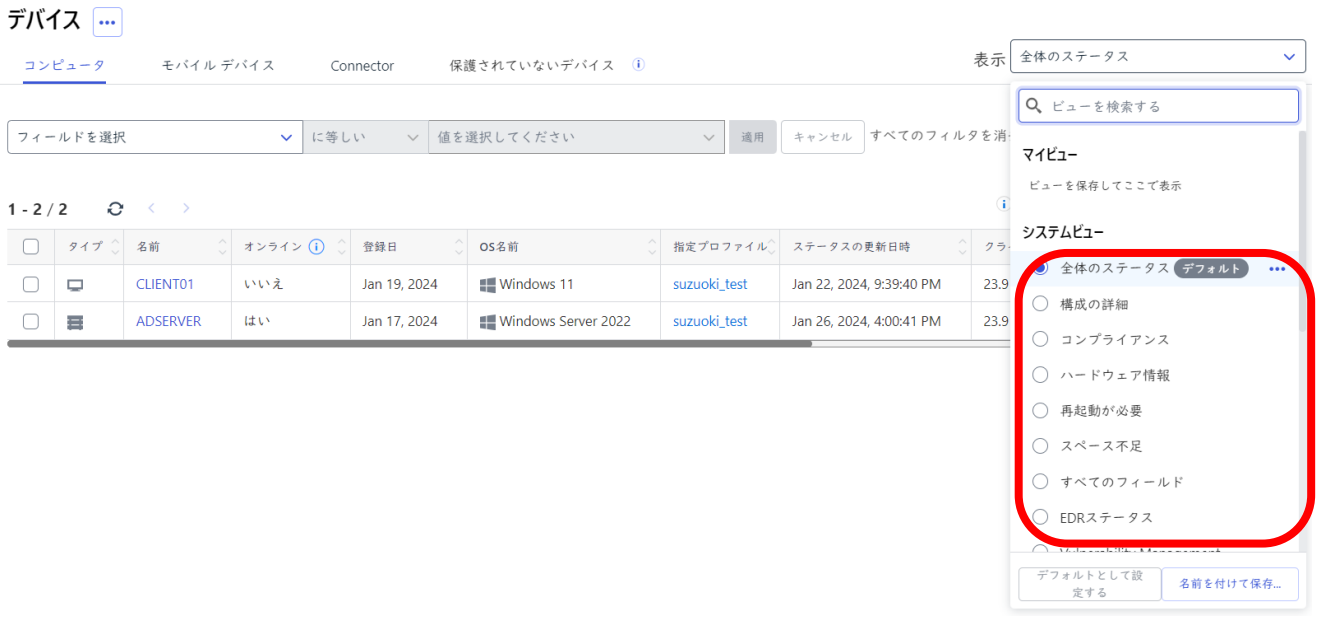
登録されているデバイス一覧を CSV でエクスポートすることができます。

6.1.2. ステータス表示のカスタマイズ

デバイスのステータス表示をカスタマイズすることができます。

- **ビルトインのステータスセット**

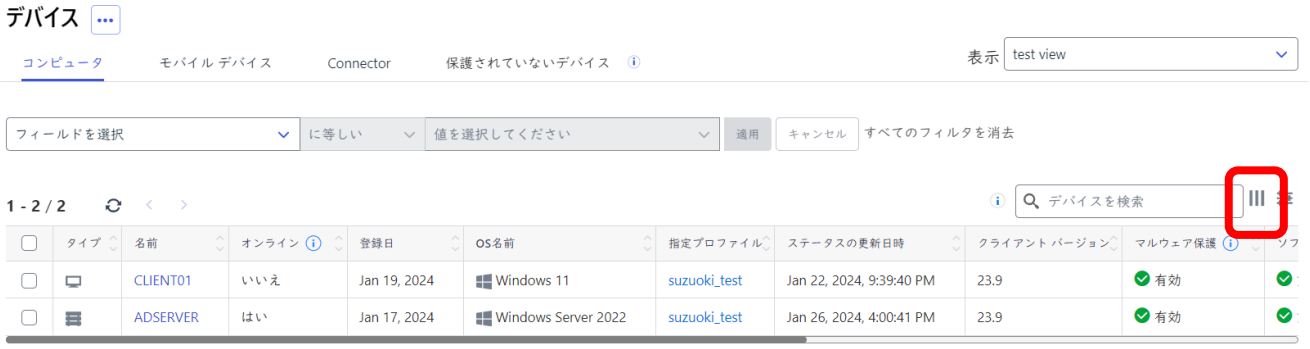
ビルトインのステータスセットを変更することで、表示するステータスを変更することができます。コンピュータ・モバイルデバイス・Connector の各タブで表示される内容は異なります。



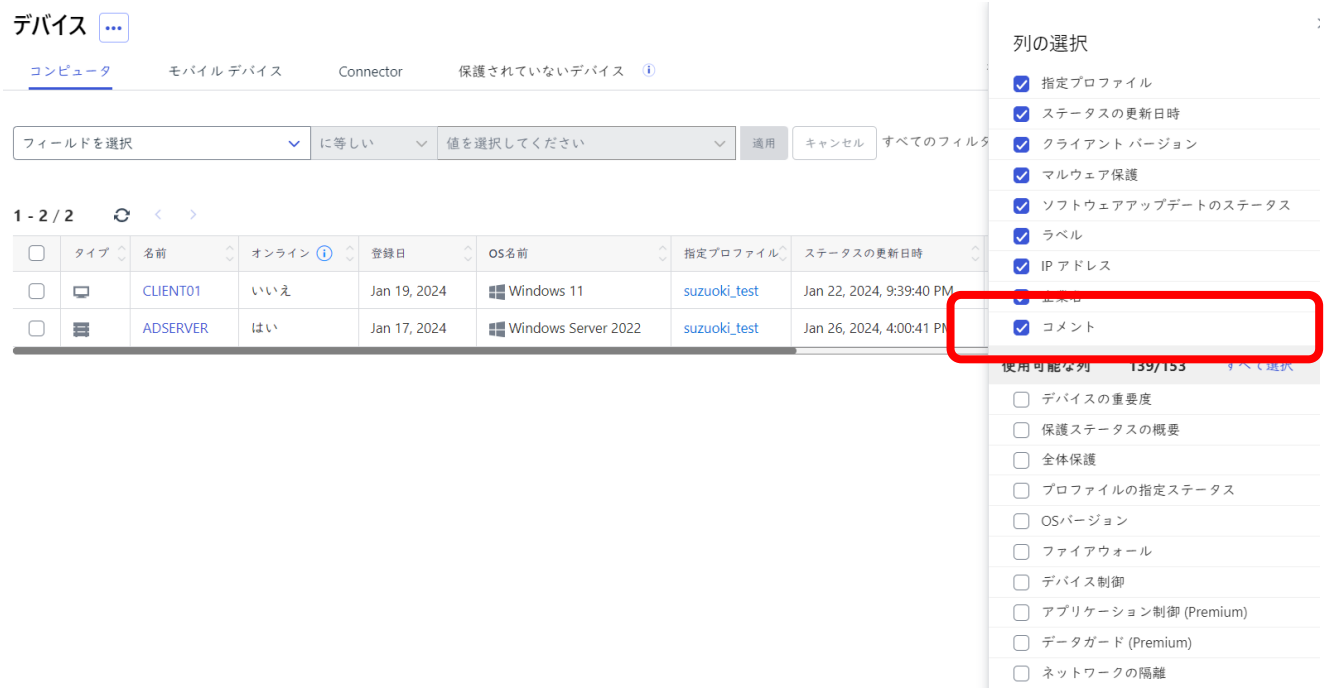
- **カスタマイズビューの設定**

ビューをカスタマイズして保存することができます。

① 列の選択のボタンをクリックします。



② 表示したい列を選択します。

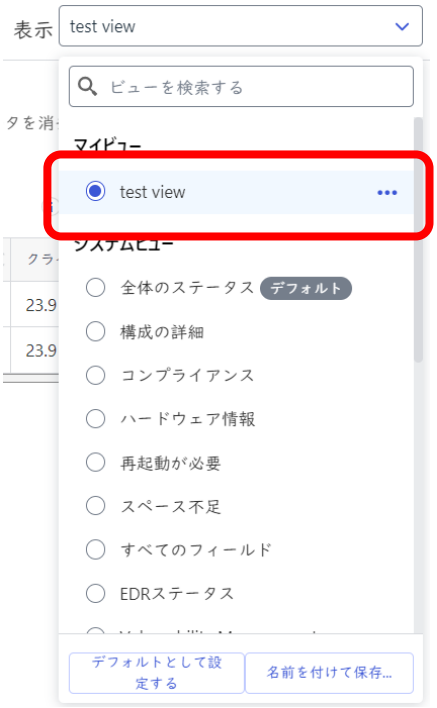


➢ [列の選択]でドラッグアンドドロップすることでステータステーブルでの表示位置を変更することができます。

③ [名前を付けて保存]をクリックします。

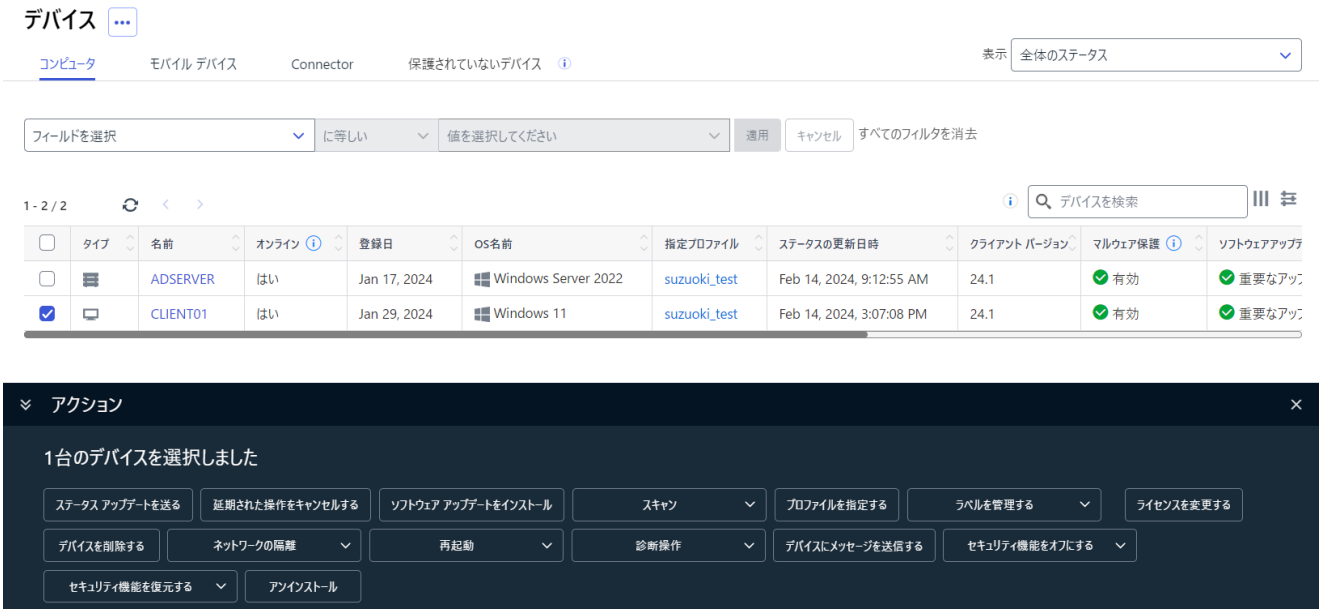
④ ビュー名を入力し[保存]をクリックします。

⑤ [マイビュー]に作成したビューが保存されます。



6.1.3. [コンピュータ]タブ

Windows、Mac、Linux に関する情報を一覧で見ることができます。また、デバイスを選択することで対象端末へのアクションを実施することができます。



- **アクション**

項目名	内容
ステータスアップデートを送る	ESC に登録されているデバイス情報を最新の状態にアップデートします。
延期された操作をキャンセルする	[アクション]で指定した操作をキャンセルします。
ソフトウェアアップデートをインストール	[パッチ管理]に表示されているパッチをインストールします。
スキャン	ウイルススキャンやパッチ管理対象のソフトウェアのスキャンをします。
プロファイルを指定する	適用するプロファイルの変更をします。
ラベルを管理する	ラベルの追加、交換、削除をします。
ライセンスを変更する	デバイスに適用するライセンスキーコードを変更します。
デバイスを削除する	ESC から登録されているデバイスを削除します。
ネットワークの隔離	ネットワークからデバイスの隔離、解放をします。
再起動	デバイスの再起動、もしくは WithSecure Agent の再起動をします。
診断操作	診断ファイルのリモート取得、もしくは、デバッグログの有効化をします。
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、ポップアップ表示させます。
セキュリティ機能をオフにする	Elements EPP の各機能を無効化にします。
セキュリティ機能を復元する	無効化にした Elements EPP の各機能を有効化します。

アンインストール	デバイスにインストールした Elements Agent をアンインストールします。

- ステータスアップデートを送る

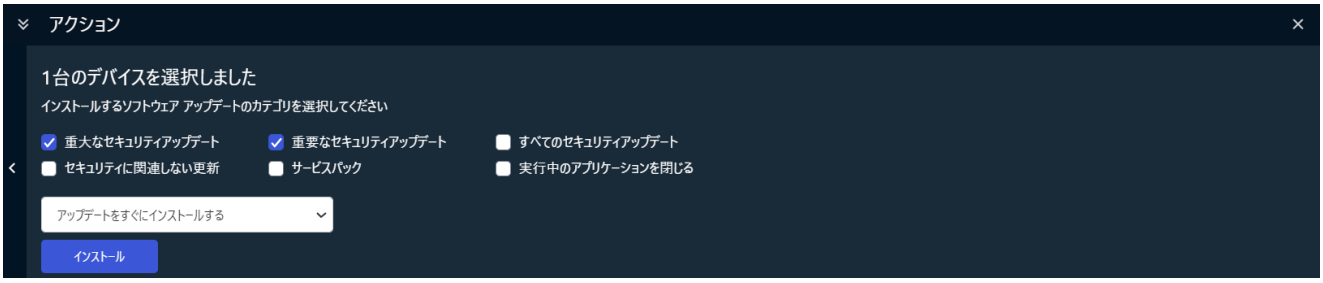
デバイスの情報を ESC に送信し、ステータスを最新にします。

- 延期された操作をキャンセルする

[デバイスにメッセージを送信する]、[ソフトウェア アップデートをインストール]のアクションをキャンセルすることができます。

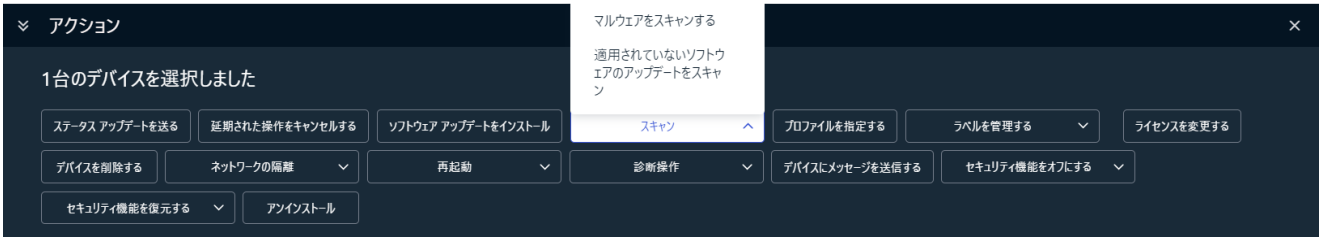
- ソフトウェアアップデートをインストール

ソフトウェアアップデートのインストールを指示することができます。ここのパッチを指定するのではなく、重大度などのカテゴリを指定します。また、インストールのスケジュールを指定することもできます。



- スキャン

マルウェアのスキャンもしくは未適用のソフトウェアアップデートのスキャンを指示することができます。



- プロファイルを指定する

プロファイルを変更することができます。

- ラベルを管理する

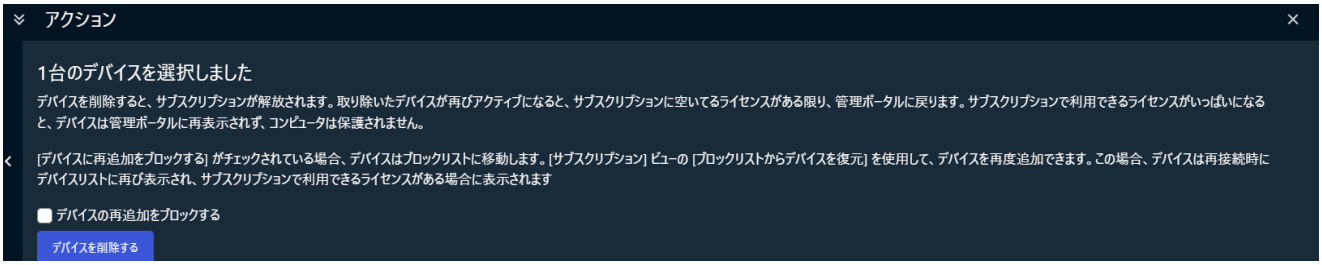
ラベルの追加、交換、削除をできます。

- ライセンスを変更する

Windows、Mac デバイスで使用するライセンスを変更することができます。

- デバイスを削除する

ESC から登録されているデバイスを削除します。通常は、デバイスが再度 ESC に接続された場合、そのデバイスは再登録されます。[デバイスの再追加をブロックする]オプションを指定すると、デバイスは再登録されません。



- ネットワークの隔離

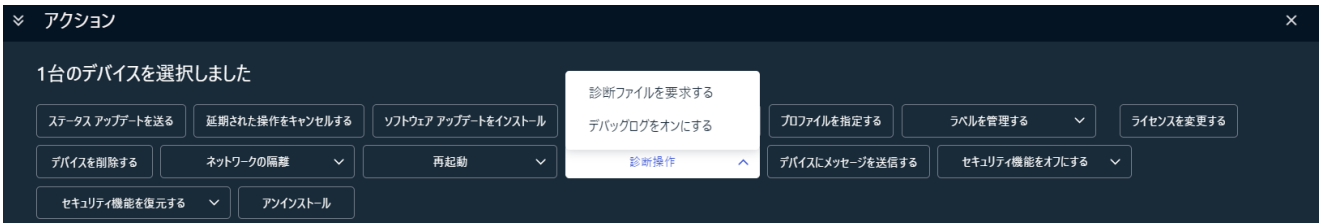
デバイスをネットワークから隔離と、隔離されたデバイスの開放をすることができます。

- 再起動

OS の再起動、もしくは Elements Agent のみの再起動をすることができます。

- 診断操作

不具合解析に必要な診断情報を取得することができます。取得した診断情報は、ESC へ自動的にアップロードされます。また、デバッグログを有効にすることで、通常の診断情報以上の情報を得ることができます。



- 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できます。メッセージの送信は、即時とスケジュールのどちらも可能です。

➢ 送信されたメッセージは、下図のようにポップアップ表示されます。

- セキュリティ機能をオフにする

Elements EPP で提供しているセキュリティ機能をオフにすることができます。

- セキュリティ機能を復元する

オフにしたセキュリティ機能を再度有効化することができます。

- アンインストール

デバイスから Elements EPP をアンインストールし、ESC からデバイスを削除します。対象デバイスに関する ESC 上のデータも全て削除されます。

6.1.4. [モバイルデバイス]タブ

モバイルデバイスに関する情報を一覧で見ることができます。また、デバイスを選択することで対象端末へのアクションを実施することができます。

- **アクション**

項目名	内容
ステータスアップデートを送る	ESC に登録されているデバイス情報を最新の状態にアップデートします。
スキャン	ウイルススキャンやパッチ管理対象のソフトウェアのスキャンをします。
ラベルを管理する	ラベルの追加、交換、削除をします。
デバイスを削除する	ESC から登録されているデバイスを削除します。
診断操作	診断ファイルのリモート取得、もしくは、デバッグログの有効化をします。
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、ポップアップ表示させます。

6.1.5. [Connector]タブ

Elements Connector に関する情報を一覧で見ることができます。また、デバイスを選択することで対象端末へのアクションを実施することができます。

- **アクション**

項目名	内容
プロファイルを指定する	適用するプロファイルの変更をします。
ラベルを管理する	ラベルの追加、交換、削除をします。
デバイスを削除する	ESC から登録されているデバイスを削除します。

6.1.6. [保護されていないデバイス]タブ

Active Directory 内の保護されていないデバイスを検索します。この機能を利用するためにはドメインコントローラが ESC に登録されている必要があります。

➢ [スキャン開始]をクリックすると、AD の端末情報と ESC の端末情報を比較し、登録されていない端末を表示します。

6.2.　デバイスのセキュリティ態勢

セキュリティ態勢（Security Posture）は、利用しているデバイスとプロファイルを分析し、デバイスの侵害や機密データの漏えいにつながる問題を表示します。

- 各項目をクリックすると、詳しい説明や手順が表示されます。
- 表示される項目は随時変更されます。

6.3. パッチ管理

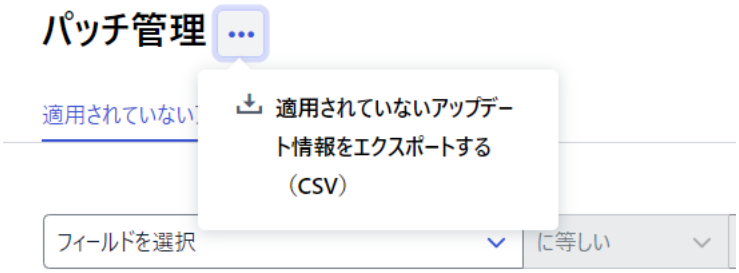
適用されていない OS やアプリケーションのパッチを管理することができます。

6.3.1. 適用されていないアップデート

適用されていないパッチの一覧です。

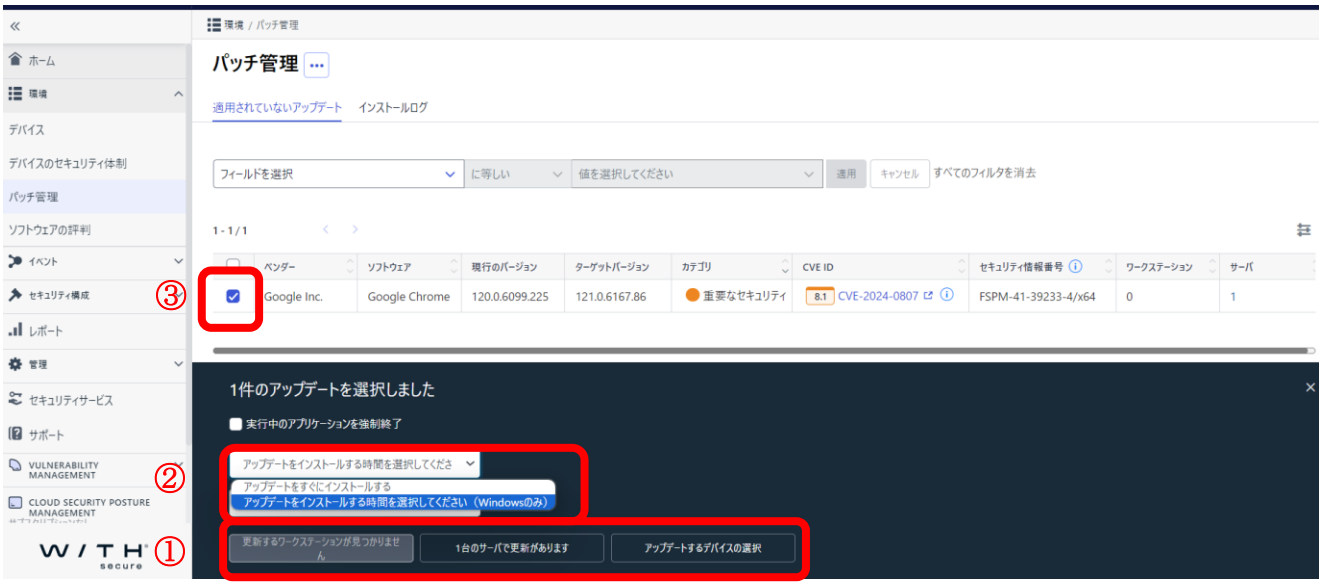
- **アクションメニュー**

未適用パッチ一覧を CSV で出力できます。



- **アップデートのインストール**

この画面からアップデートをインストールすることができます。



① 適用したいアップデートにチェックを入れます。

② インストールするタイミングを選択します。

- Windows の場合のみ日時を選択してインストール可能です。

③ インストールする端末を選択します。

- ワークステーション、サーバーごとの一括インストールが可能です。
- インストールする端末を個別に選択することも可能です。その場合、[アップデートするデバイスの選択]をクリック後、下の画面から対象デバイスを選択します。

6.3.2. インストールログ

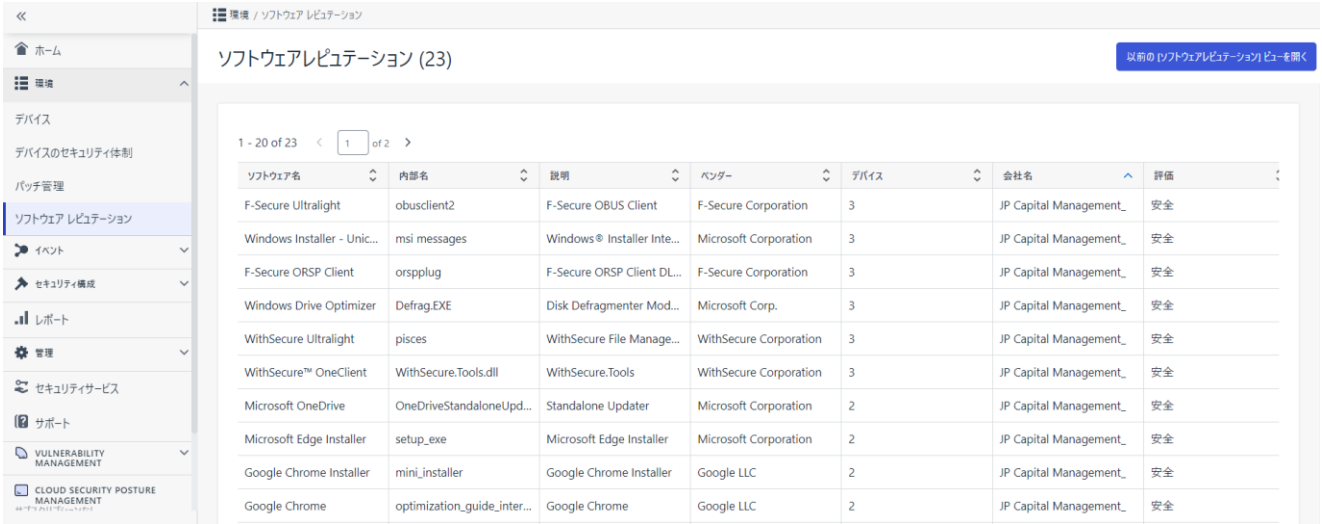
インストール操作やその進行状況を確認することができます。

- **アクションメニュー**

インストールログの一覧を CSV で出力できます。

6.4. ソフトウェアレピュテーション

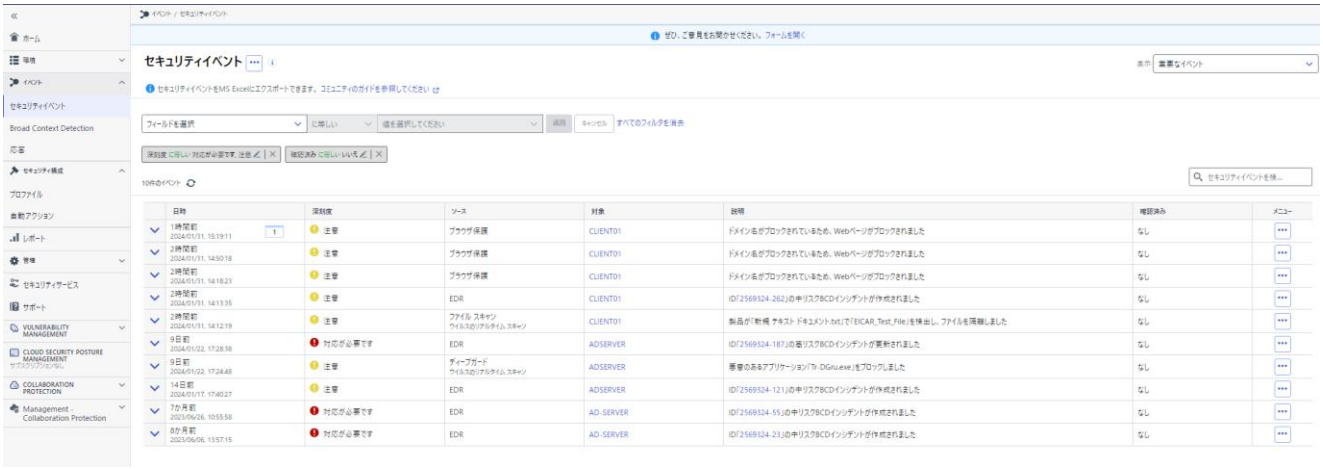
デバイスにインストールされているソフトウェアの評価を表示します。評価は弊社クラウド上の DB を参照します。



7. イベント

7.1. セキュリティイベント

各デバイスで発生したセキュリティのイベント一覧を確認できます。セキュリティイベントには EPP の様々な機能による検知、EDR のインシデント概要が表示されます。表示させる情報を制限したい場合は、フィルタ機能を利用してください。



- セキュリティイベントの保存期間は深刻度に依存します。
  - 情報：7 日間
  - 注意：6 か月
  - 対応が必要：13 か月

- **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を JSON 形式でエクスポートします。
感染警告の構成	ウイルススキャンやパッチ管理対象のソフトウェアのスキャンをします。

- 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を JSON 形式でエクスポートします。エクスポートした JSON ファイルをエクセルにインポートする場合には、以下のコミュニティ記事を参照してください。

security events JSON ファイルを Microsoft Excel にインポートする

- 感染の警告

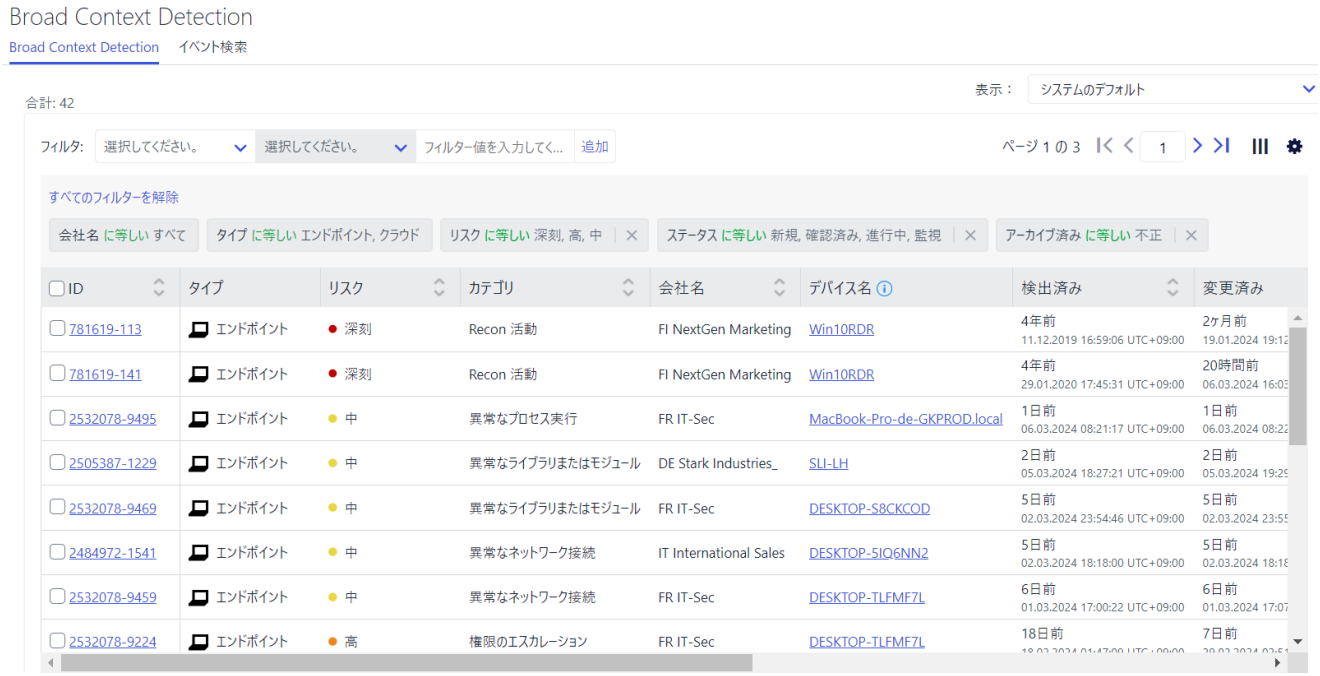
Elements EPP でマルウェアなどを検知した際に、登録したメールアドレスへ通知をする設定です。

7.2. Broad Context Detection

Elements EDR にて検知したインシデントを表示します。

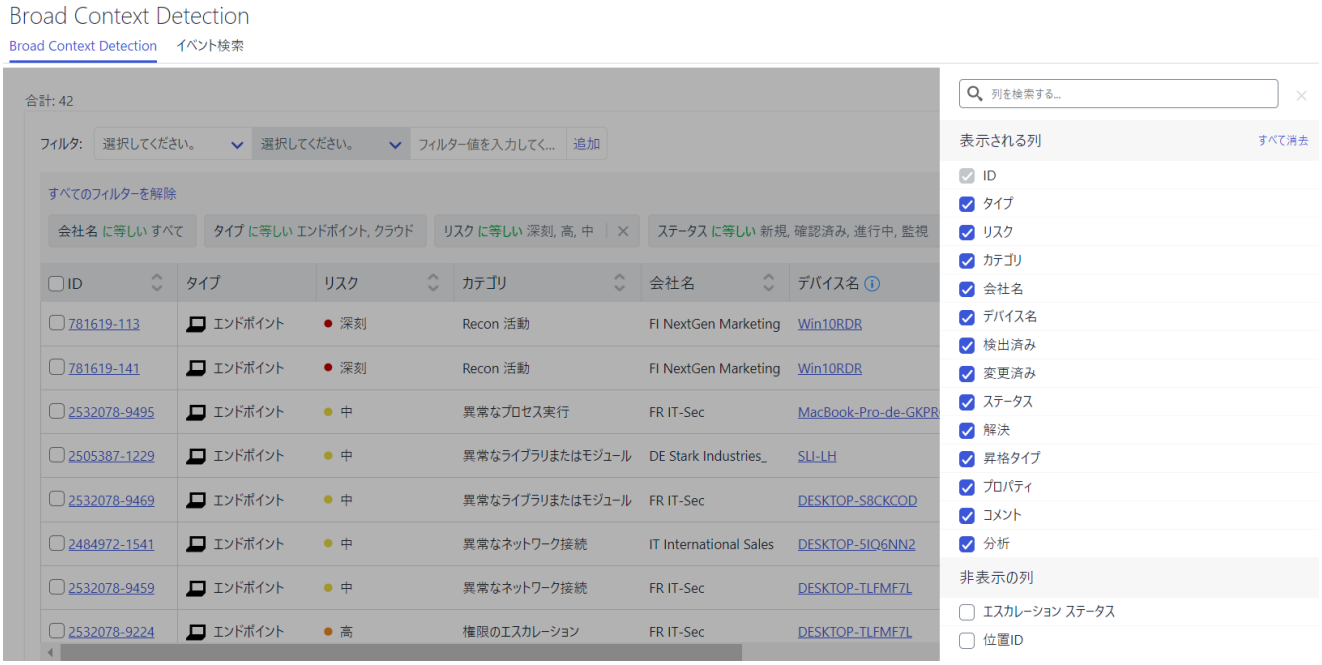
7.2.1. Broad Context Detection

検知したインシデント（Broad Context Detection : BCD)の一覧です。表示させる情報を制限したい場合は、フィルタ機能を利用してください。

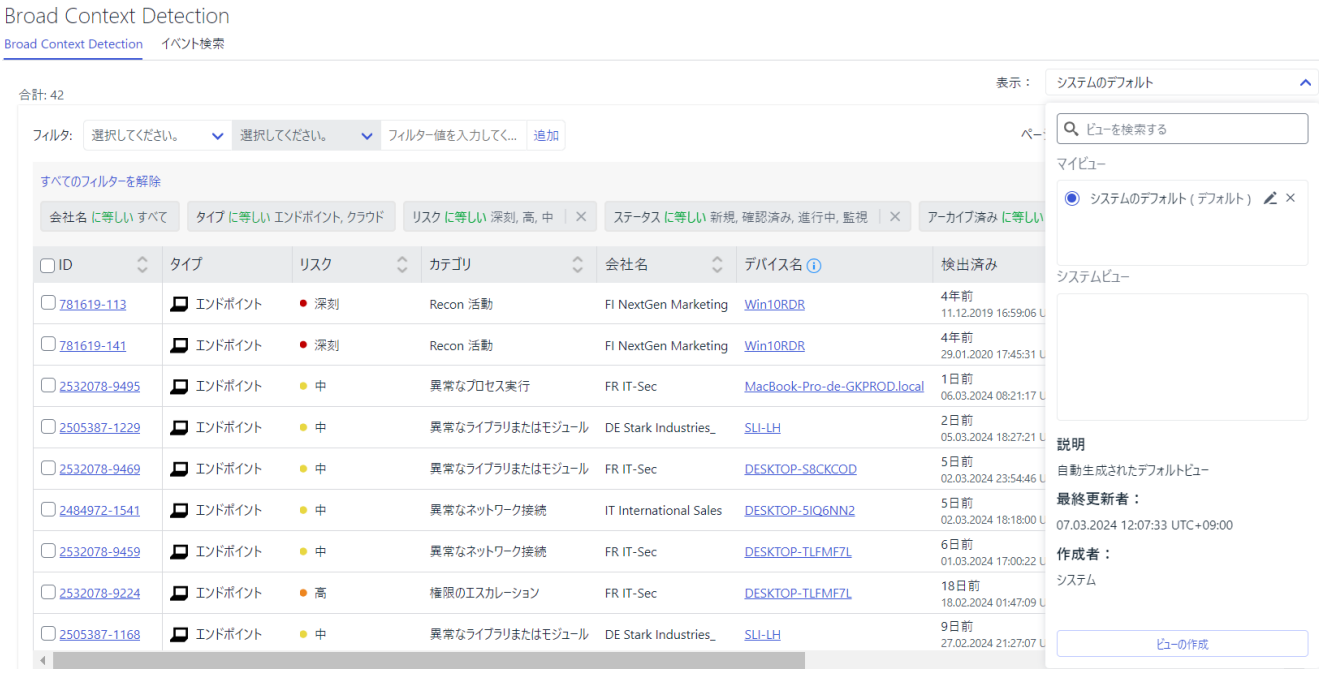


- BCD の ID をクリックすることで、その BCD の詳細を確認することができます。BCD の確認の仕方などは、弊社トレーニング資料などを参照ください。

- 右上にある ||| メニューにて表示する項目を変更することができます。

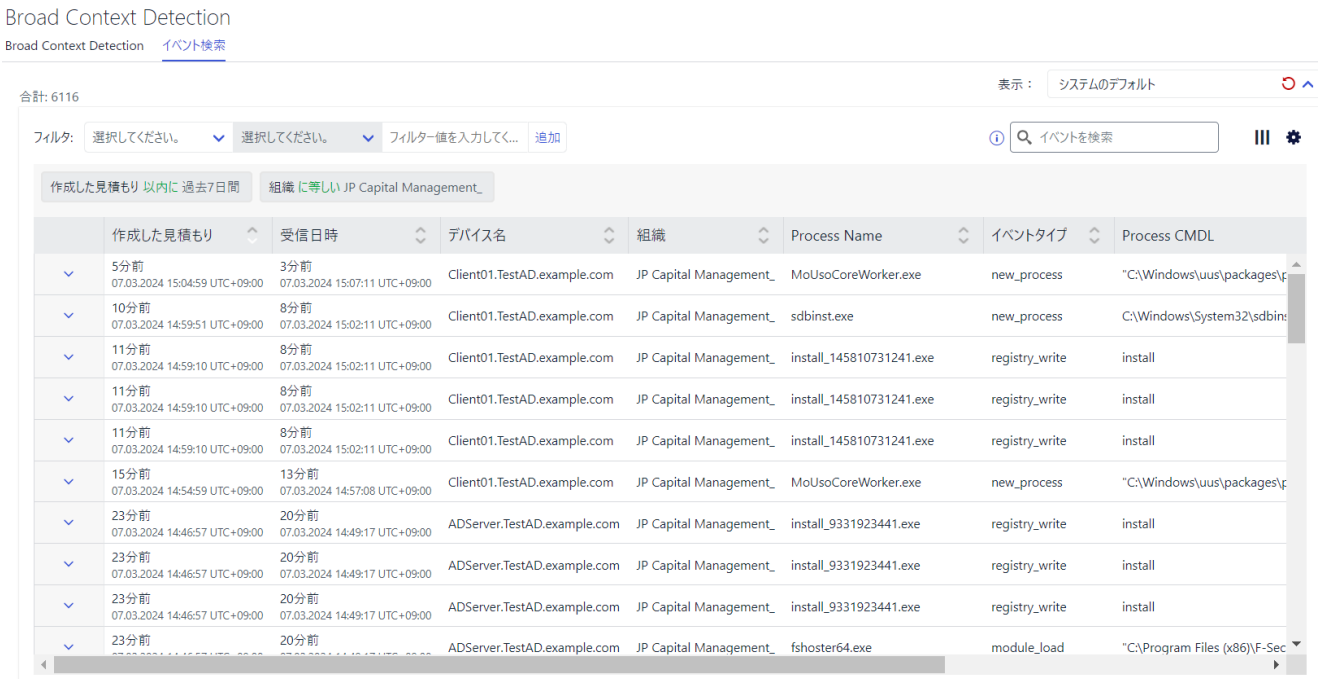


- 現在表示されている画面構成を保存し、次回から同じ内容を表示させることができます。



7.2.2. イベント検索

Elements EDR で収集したイベントを検索することができます。表示させる情報を制限したい場合は、フィルタ機能を利用してください。



- 検索可能期間は最大で過去 7 日間です。

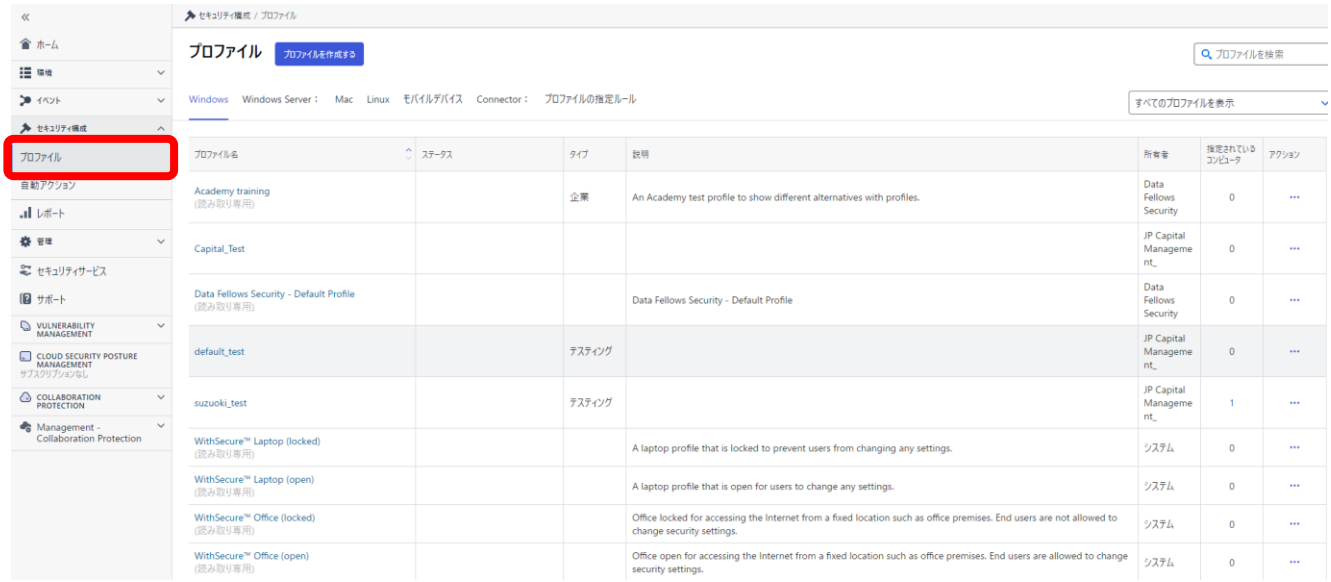
7.3. 応答

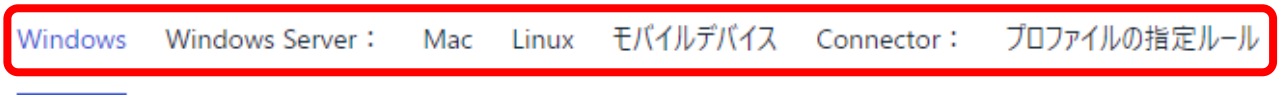
Elements EDR の[応答]機能を利用できます。[応答]機能はインシデントレスポンスのための機能で、ファイルの削除やサービス一覧の取得など、様々な機能を活用できます。[応答]機能の詳細は、弊社トレーニング資料などを参照ください。

8. セキュリティ構成

8.1. プロファイル

プロファイルとは、Elements EPP の設定のことです。各 Elements EPP クライアントや Elements Connector へプロファイルを適用することで、設定を一元管理することができます。プロファイルの設定項目の詳細な説明については、プロファイル画面にある?ボタンで確認できます。





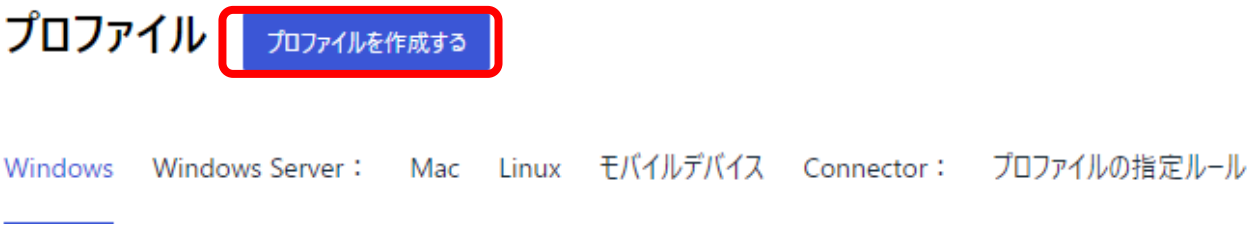
Elements EPP 製品ごとにプロファイルを作成できます。[プロファイルの指定ルール]では、クライアントが ESC に登録された時、もしくは、クライアントのデータに変更があった時に、自動的にプロファイルを適用することができます。

項目名	内容
Windows	Windows クライアント用のプロファイル
Windows Server	Windows サーバー用のプロファイル
Mac	Mac クライアント用のプロファイル
Linux	Linux サーバー用のプロファイル
モバイルデバイス	Elements Mobile Protection 用のプロファイル
Connector	Elements Connector 用のプロファイル
プロファイルの指定ルール	自動的にプロファイルを適用させるためのルール

8.1.1. プロファイルの作成

新規にプロファイルを作成する際に利用します。

① [プロファイルを作成する]をクリックします。



② 必要な設定を入力し、[保存して発行]をクリックすると、新規プロファイルが作成されます。

- プロファイル名は必須項目です。
- タイプをプルダウンメニューから選択します。
- 必要に応じて説明を記載します。
- ?ボタンをクリックすると詳細な説明が表示されます。

8.1.2. プロファイル設定項目のロック

プロファイルの設定項目はユーザーが変更できないようにロックすることができます。

- **プロファイルのロック**

設定項目の右にある鍵マークをクリックすることで、ロック状態にできます。

- **プロファイルの一括ロック**

全ての設定項目を一括でロックすることができます。

8.1.3. プロファイルのエクスポート / インポート

プロファイル設定を json ファイル形式でエクスポートすることができます。エクスポートした json ファイルをインポートすることができます。

8.1.4. プロファイルの指定ルール

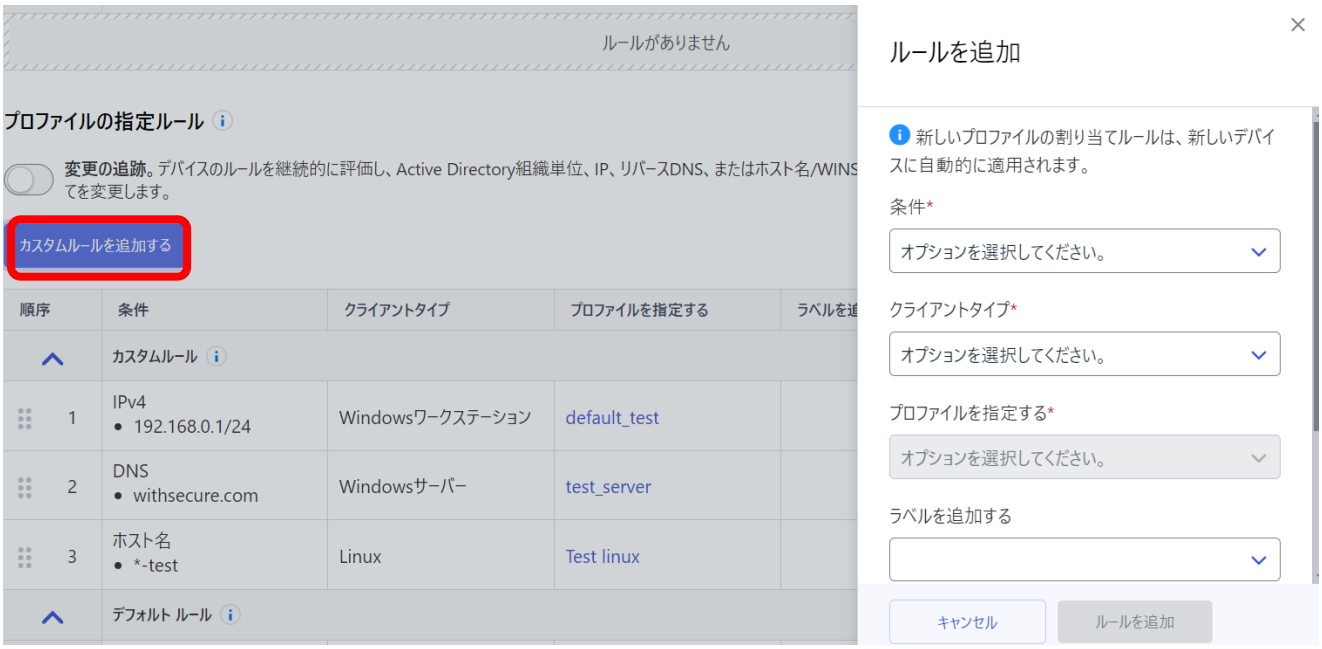
クライアントが登録された際に指定されるデフォルトルールや、クライアントの設定が変更された際に適用されるプロファイルを自動的に変更します。

- **カスタムルール**

新しいクライアントが ESC に登録された際に自動的に適用されるプロファイルを決定するルールです。ルールは上から順番に評価され、ルールが合致した際にそのプロファイルが適用されます。

- **カスタムルールの作成**

[カスタムルールを追加する]をクリックし、新しいルールを作成することができます。

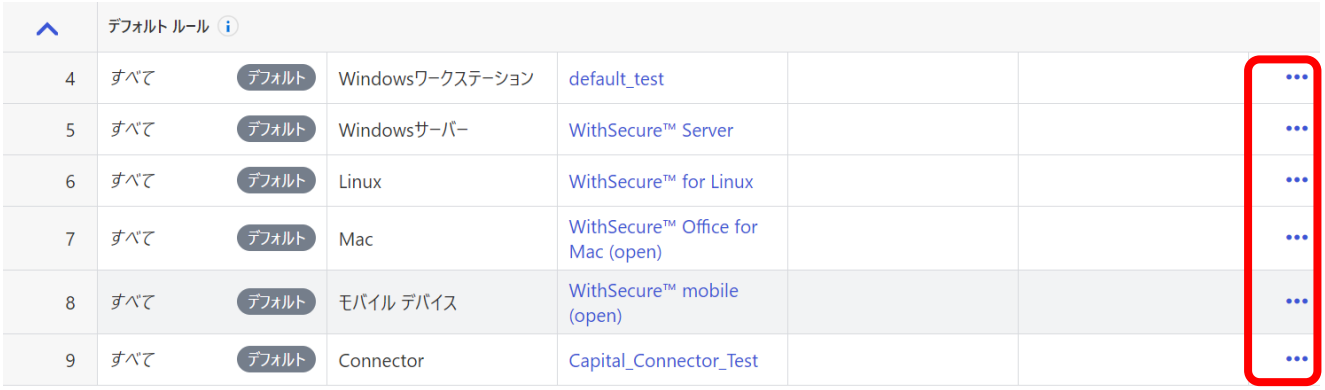


➢ ルール作成時には以下の条件を指定します。

項目名	内容
条件	合致する条件を選択します。 IPv4、DNS、ホスト名、AD OU マニュアル、AD の OU ツリー
クライアントタイプ	対象のクライアント OS を選択します。 Windows ワークステーション、Windows サーバー、Linux、Mac
プロファイルを指定する	適用するプロファイルを選択します。
ラベルを追加する	該当ルールを適用する際にラベルを追加します。
説明	必要に応じて説明を記載します。

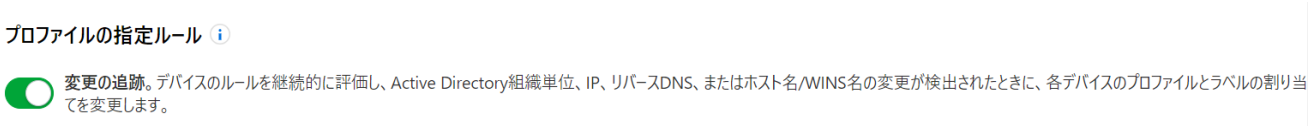
- **デフォルトルール**

カスタムルールに合致するものがない場合、デフォルトルールで指定したプロファイルが適用されます。デフォルトルールはクライアントタイプごとに指定できます。指定は[…]メニューから実施します。



- **変更の追跡**

クライアントの設定が変更された際に、条件との比較を実施し自動的に適用するプロファイルを変更するための機能です。



8.1.5. プロファイルのアクションメニュー

プロファイルの右にある[…]メニューから各種アクションを実行できます。

- **アクションメニュー**

項目名	内容
プロファイルをクローンする	作成済みのプロファイルと同じ設定のプロファイルを作成します。
プロファイルを削除	不要になったプロファイルを削除することができます。
プロファイルの比較と編集	2 つのプロファイルを比較し、その違いを確認することができます。また、異なるプロファイル設定を一方から他方へコピーすることができます。
「Windows Server」プロファイルにコピーする	Windows クライアントと Windows サーバー間でプロファイルをコピーすることができます。
プロファイルを別のアカウントにコピーする	SoP や SeP のユーザーアカウントでログインしている際、他の企業アカウントへプロファイルをコピーすることができます。

- プロファイルの比較と編集

① 右の[…]メニューから[プロファイルの比較と編集]を選択します。

② 比較したいプロファイルを選択し[次へ]をクリックします。

③ 設定が異なる項目が表示されます。

➢ 矢印をクリックすると設定をコピーすることができます。

8.1.6. アウトブレイクルール

ESC に登録済みのクライアントが特定の条件に合致した場合に適用する特別なプロファイルです。

項目名	内容
条件	合致する条件を選択します。 未解決の EDR インシデント、公共のインターネット上、ダイナミックリスクスコア
クライアントタイプ	対象のクライアント OS を選択します。 Windows ワークステーション、Windows サーバー、Linux、Mac
プロファイルを指定する	適用するプロファイルを選択します。
ラベルを追加する	該当ルールを適用する際にラベルを追加します。
説明	必要に応じて説明を記載します。

8.2. 自動アクション

Elements EDR にて BCD を検知した際の自動応答ルールを作成します。詳細については、弊社トレーニング資料などを参照ください。

9. レポート

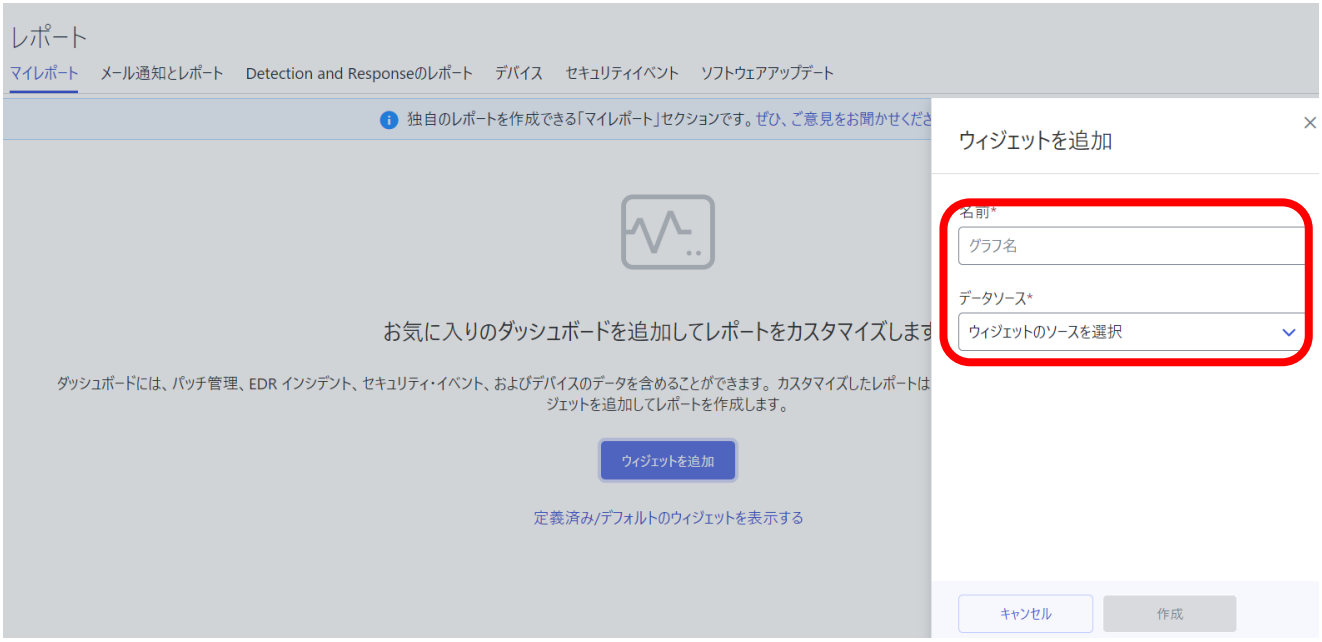
各種グラフィカルレポートを確認することができます。

9.1.　マイレポート

ウィジェットを追加して表示するレポートをカスタマイズすることができます。

① [ウィジェットを追加]をクリックします。

② 名前を記入し、データソースなどを選択します。

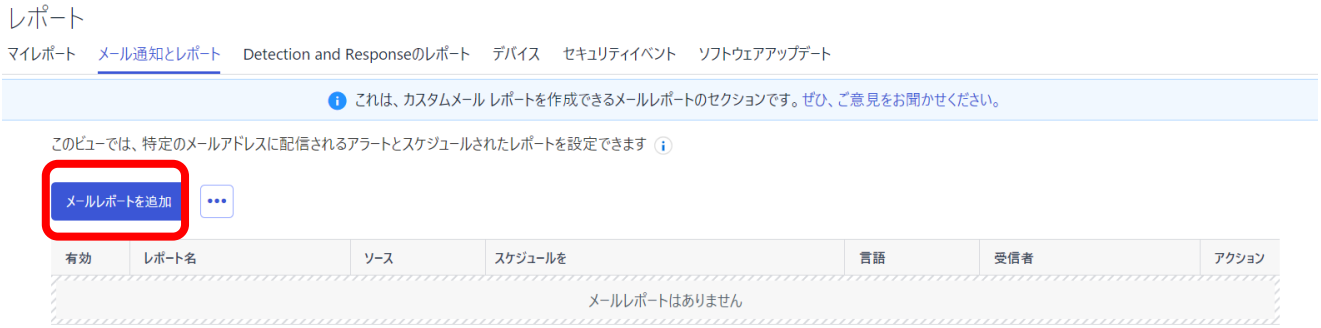


③　表示したいレポートをすべて追加します。

9.2.　メールと通知

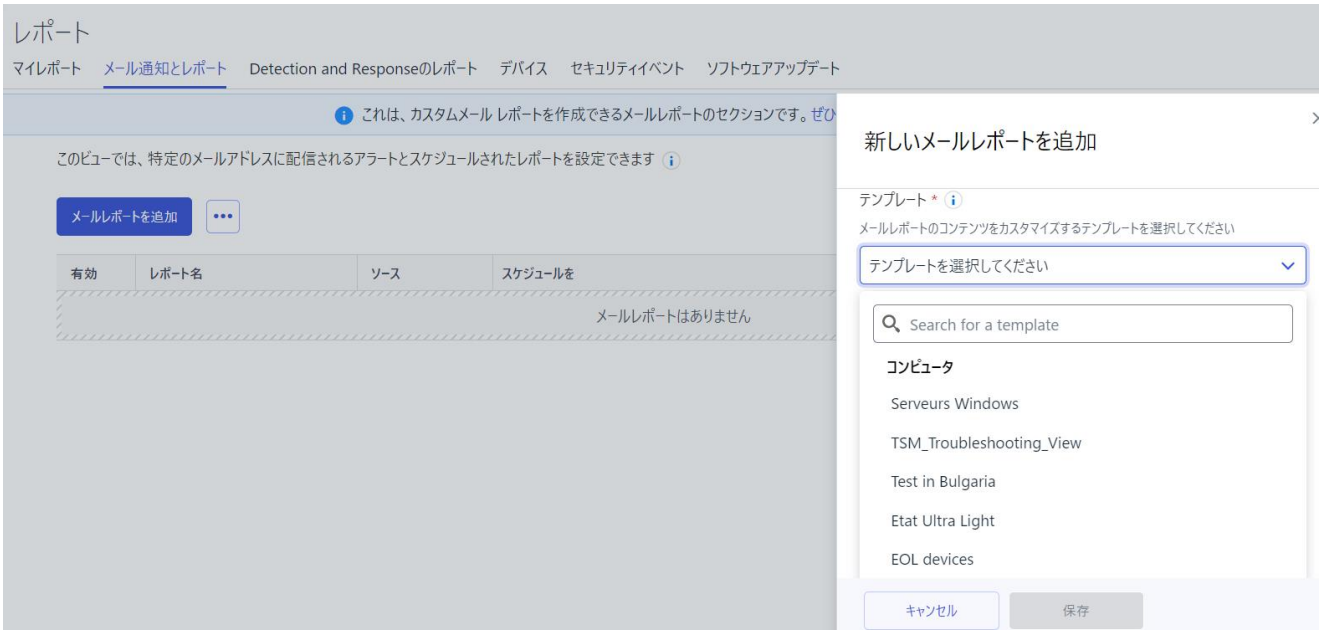
カスタムレポートをメールで送信することができます。

①　[メールレポートを追加]をクリックします。



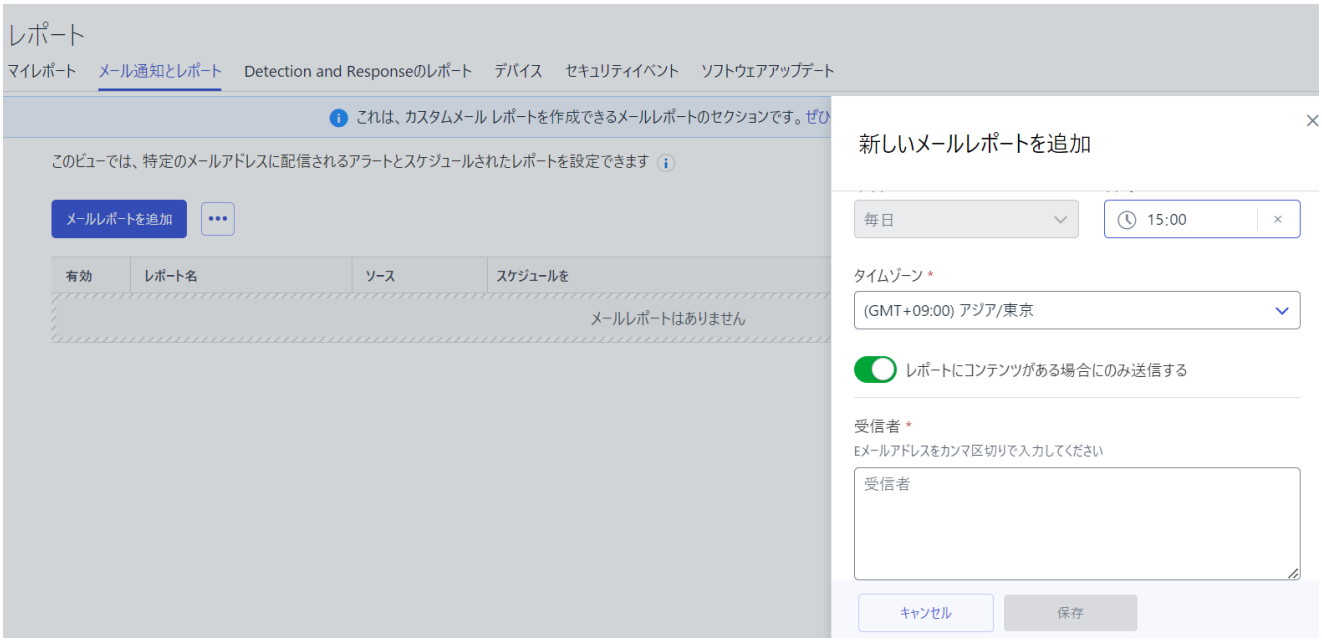
② レポート名を入力し、データソースを選択します。

③ テンプレートをを選択します。テンプレートはデバイスやセキュリティイベントで保存されたビューから選択します。



④　言語とスケジュールを設定します。

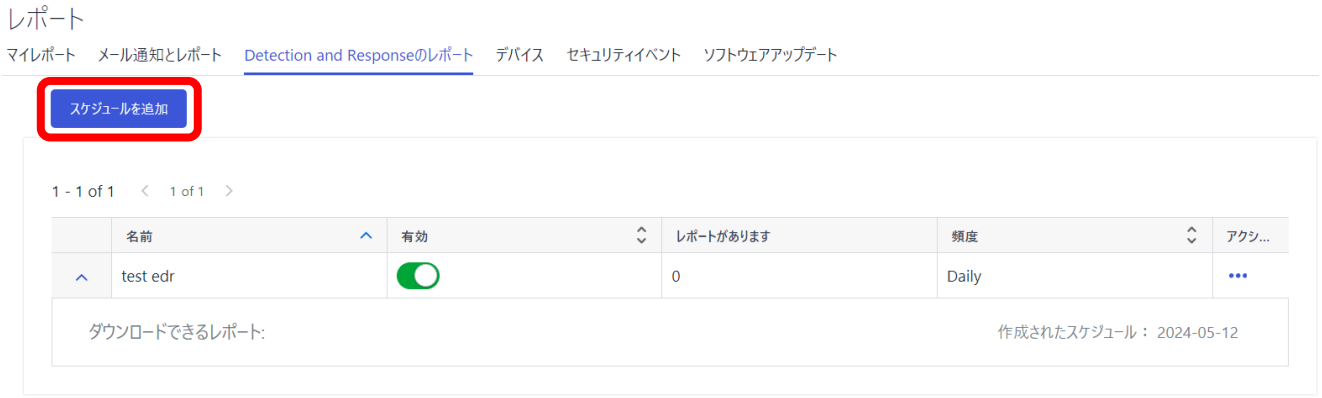
⑤　タイムゾーンを選択し、送信先メールアドレスを入力します。



9.3.　Detection and Response のレポート

Elements EDR に関するレポートを作成することができます。

① [スケジュールを追加]をクリックします。

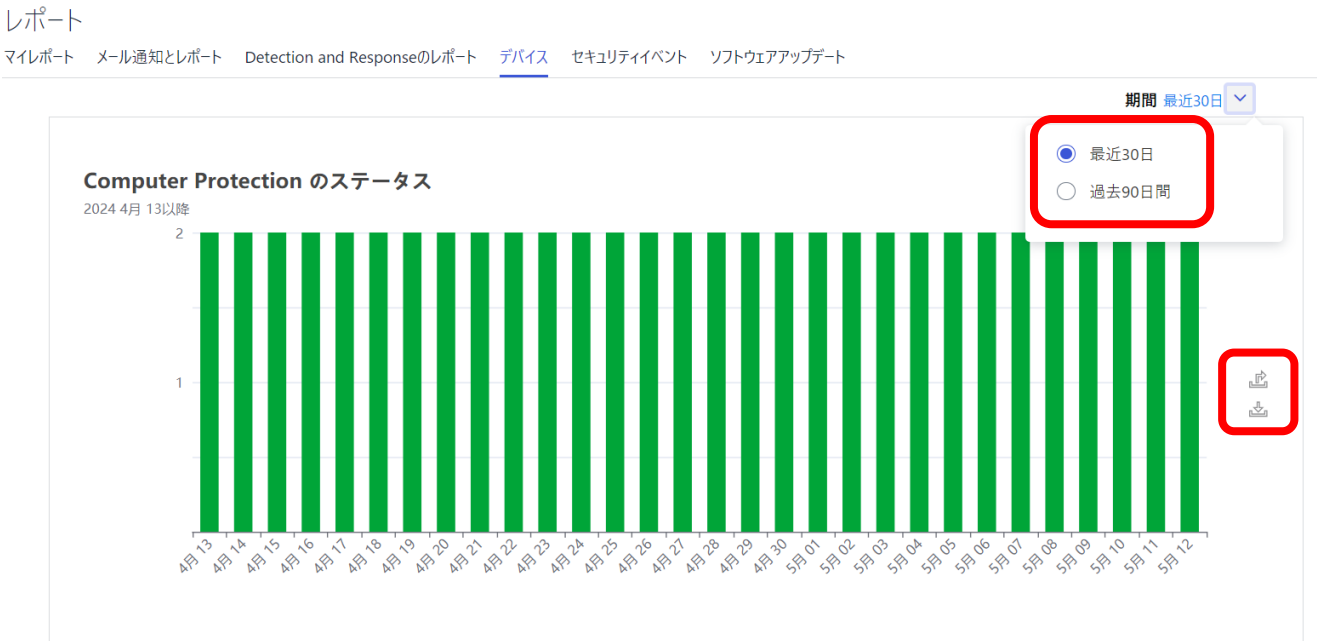


② レポート名、スケジュール、タイムゾーンを設定します。

③　レポートが作成されるとダウンロードリンクが作成されます。

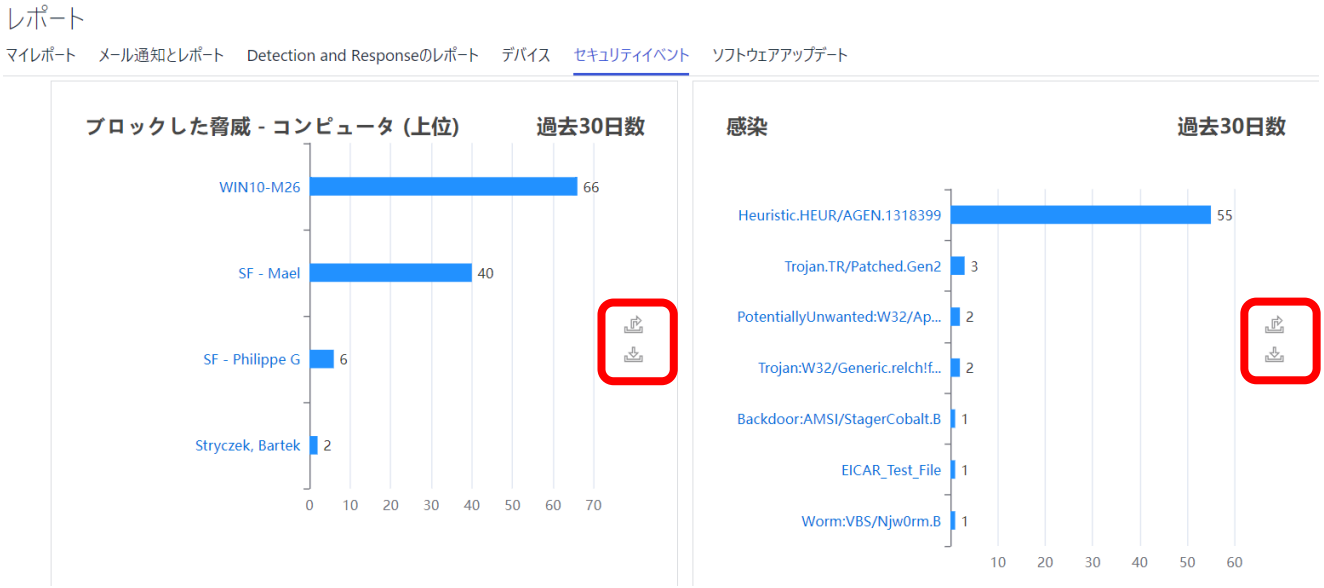
9.4.　デバイス

Elements EPP に関する情報を確認することができます。期間は、直近 30 日もしくは 90 日を選択できます。表示されているレポートは画像、もしくは CSV で保存することができます。



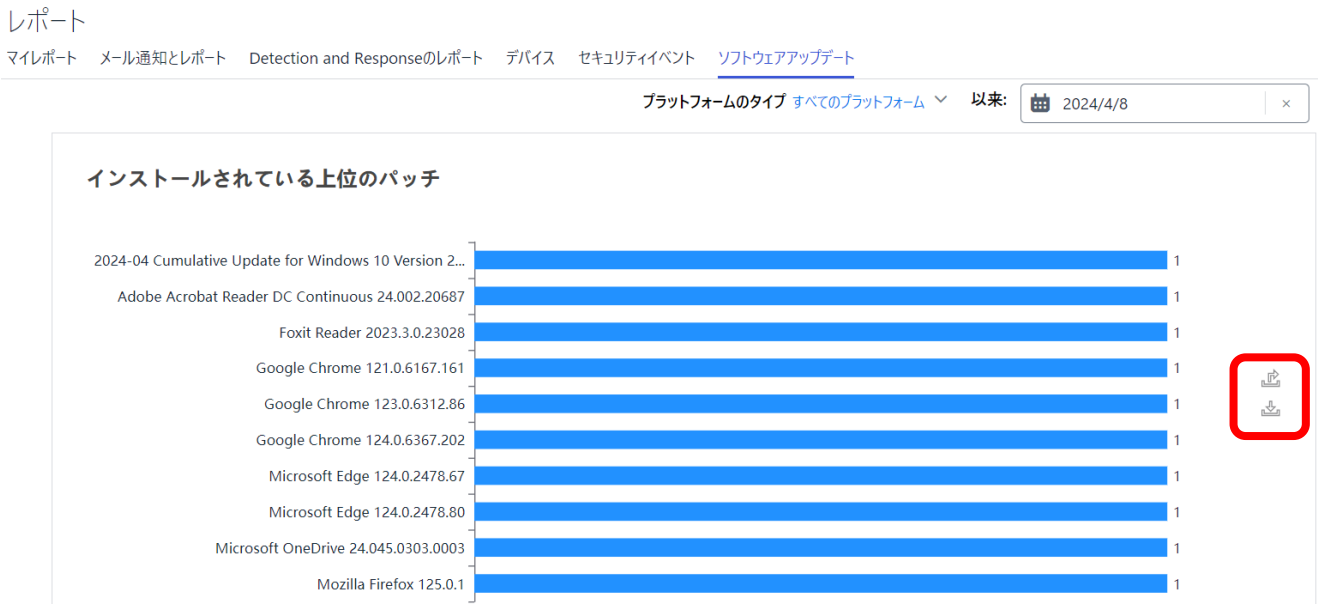
9.5.　セキュリティイベント

過去 30 日間のセキュリティイベントの情報を確認することができます。表示されているレポートは画像、もしくは CSV で保存することができます。



9.6. ソフトウェアアップデート

パッチ管理の情報を確認することができます。表示されているレポートは画像、もしくはCSVで保存することができます。



10. 管理

10.1. 組織の設定

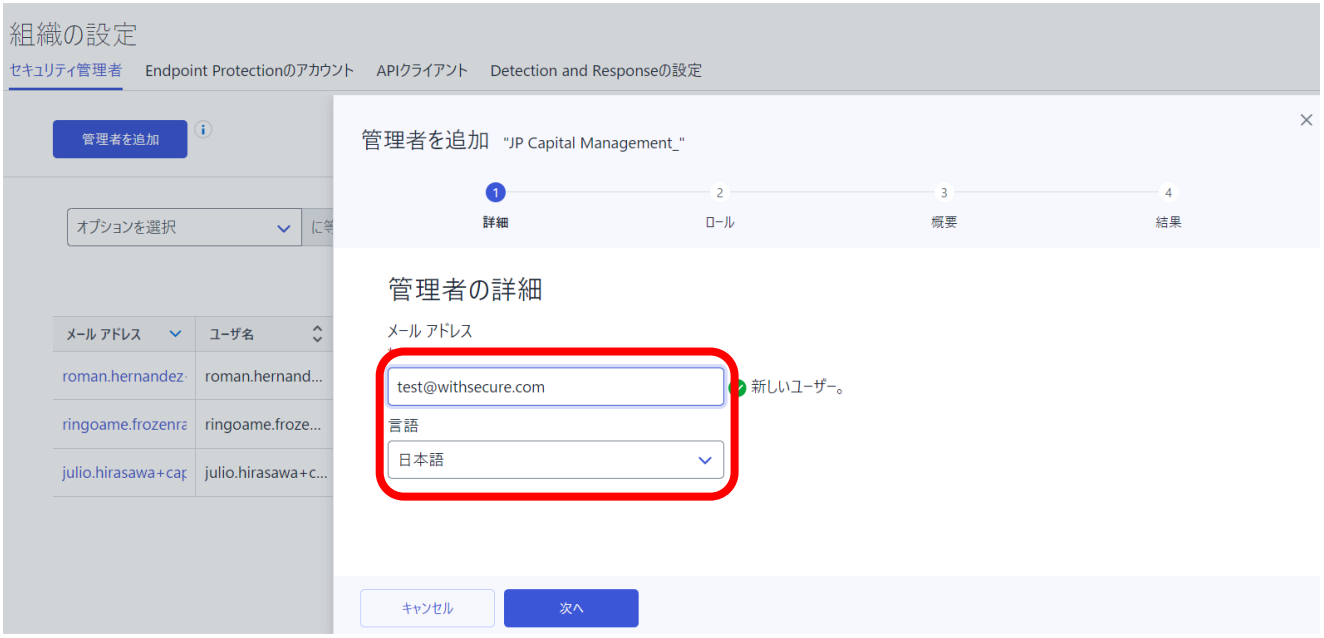
10.1.1. セキュリティ管理者

ESC の管理者の確認や追加を行うことができます。

- **管理者の追加**

① [管理者の追加]をクリックします。

② メールアドレスを入力します。



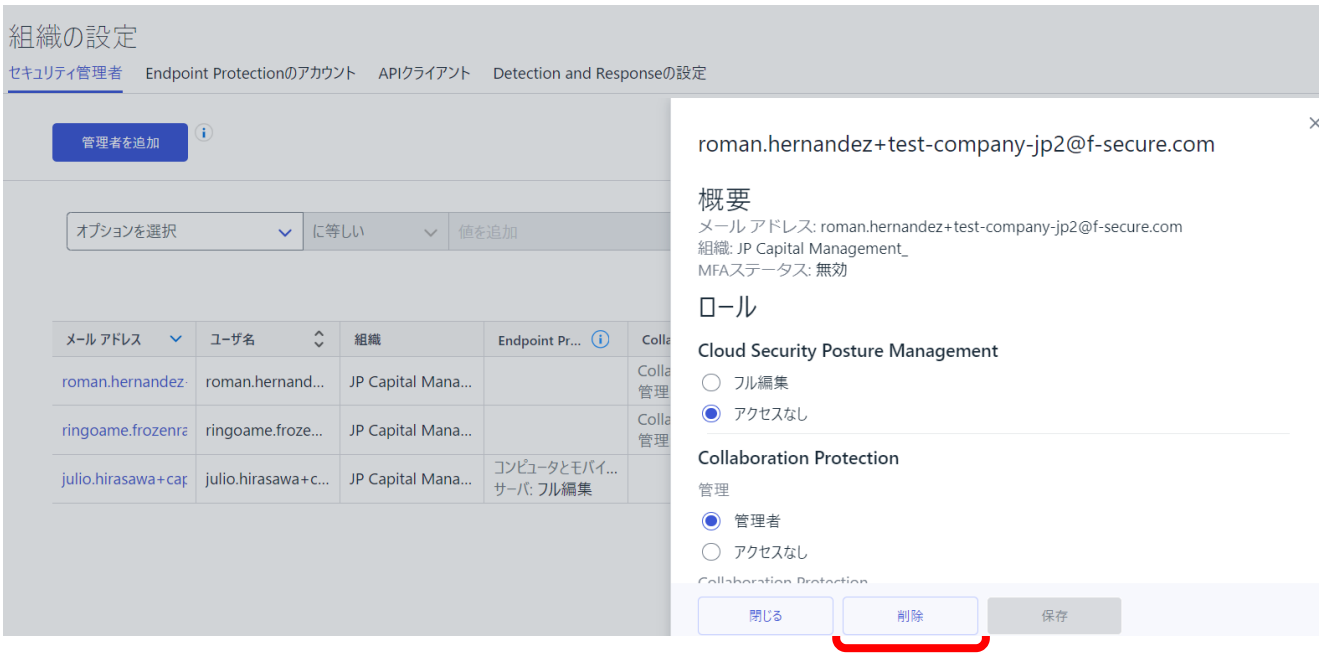
③ 各製品の権限を設定します。ライセンスを保有していない製品には権限の設定はできません。

④ 登録したメールアドレスへ以下のメールが送信されます。ワンタイムパスワードでログインしてください。

- **管理者の削除**

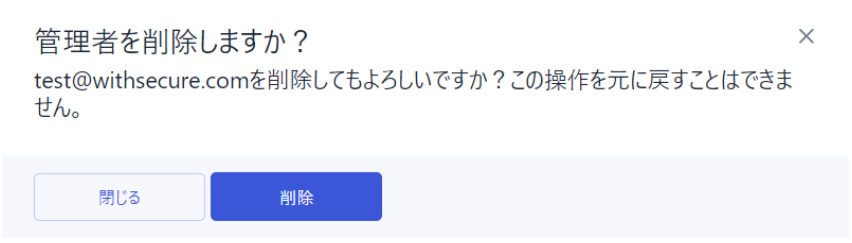
① 削除したい管理者をクリックします。

② 削除をクリックします。



➢ [削除]グレーアウトしている場合は、すべて[アクセスなし]を選択し、一度保存してください。

③ [削除]をクリックします。



10.1.2. Endpoint Protection のアカウント

Elements EPP の管理者を作成できます。ただし、現在は[10.1.1 セキュリティ管理者]で実行可能なため、こちらの項目は利用する必要はありません。

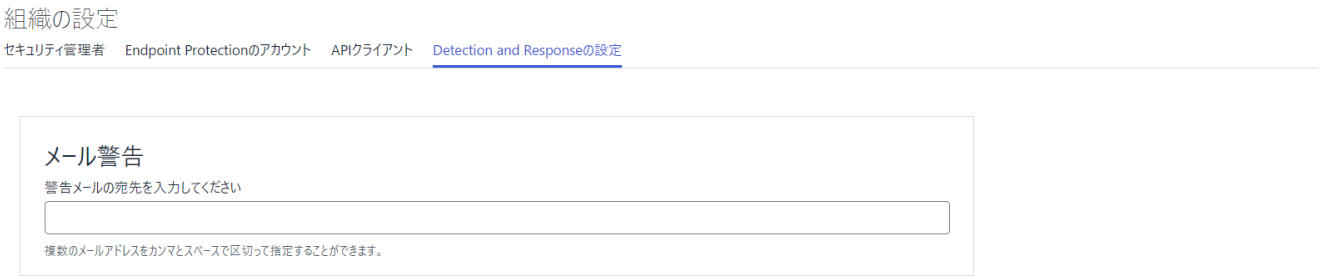
10.1.3. API クライアント

Elements API を利用するための API クライアントを発行することができます。Elements API の詳細については、以下の URL を参照してください。

https://connect.withsecure.com/

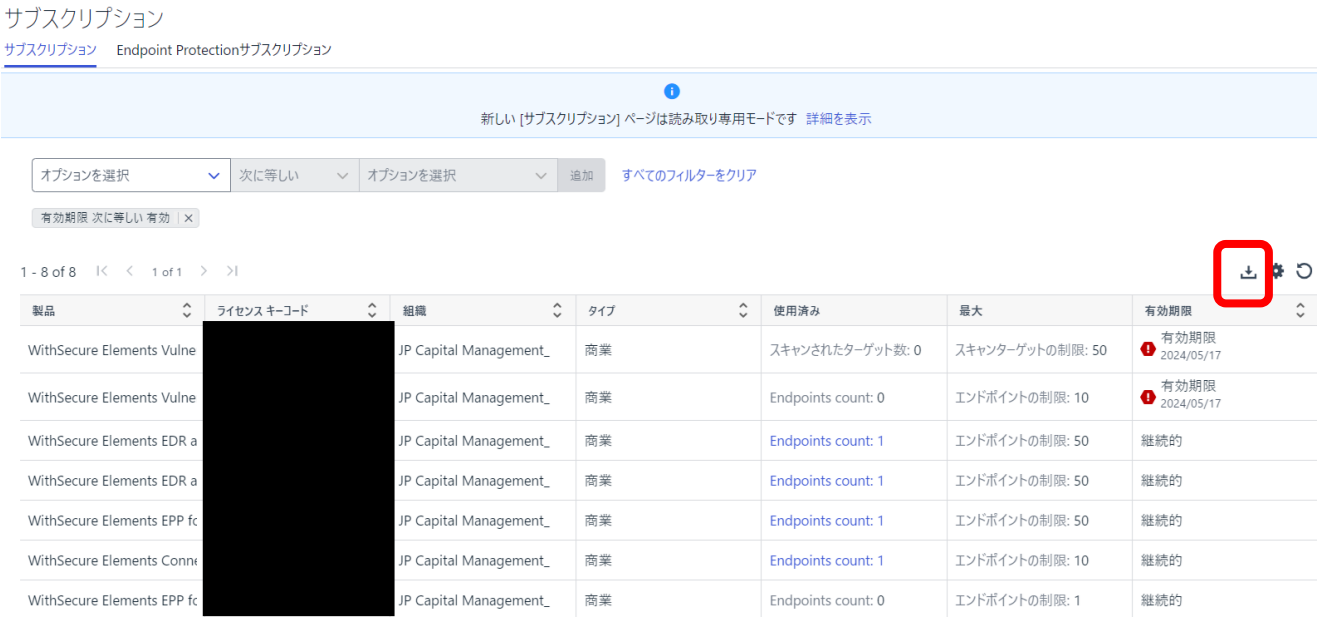
10.1.4. Detection and Response の設定

Elements EDR の警告メールを送信するメールアドレスを設定できます。



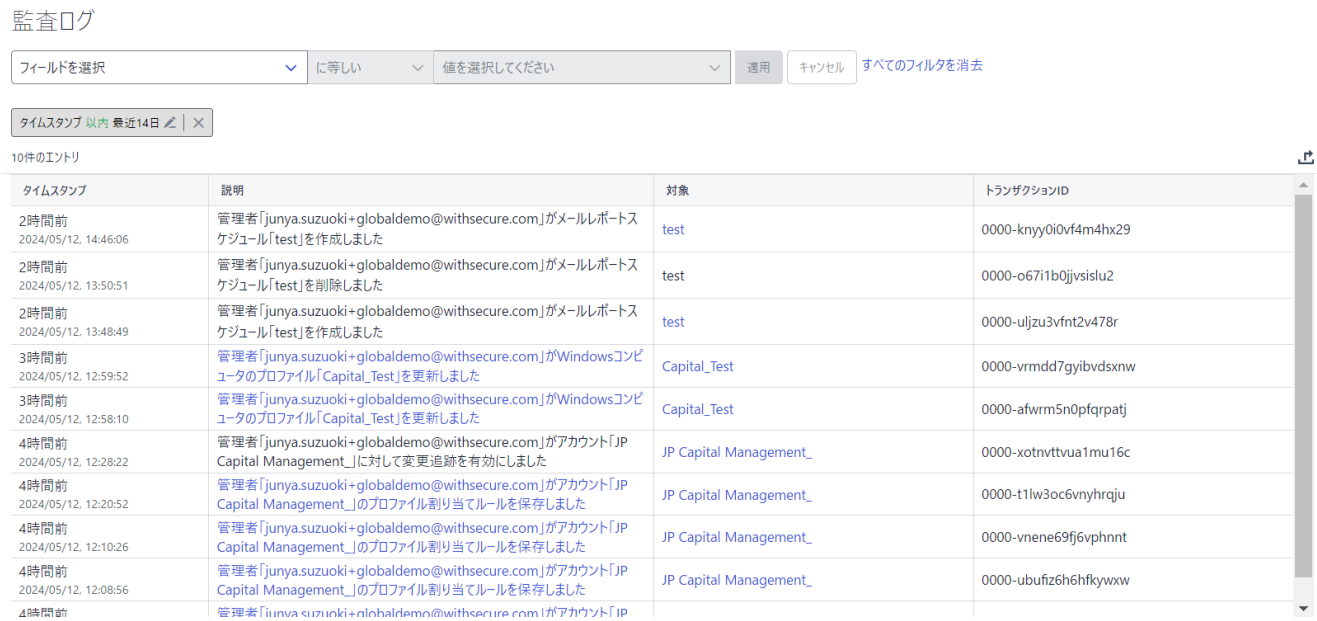
10.2. サブスクリプション

契約しているライセンスの情報を確認できます。
サブスクリプションの情報は、csv と json 形式でダウンロードできます。



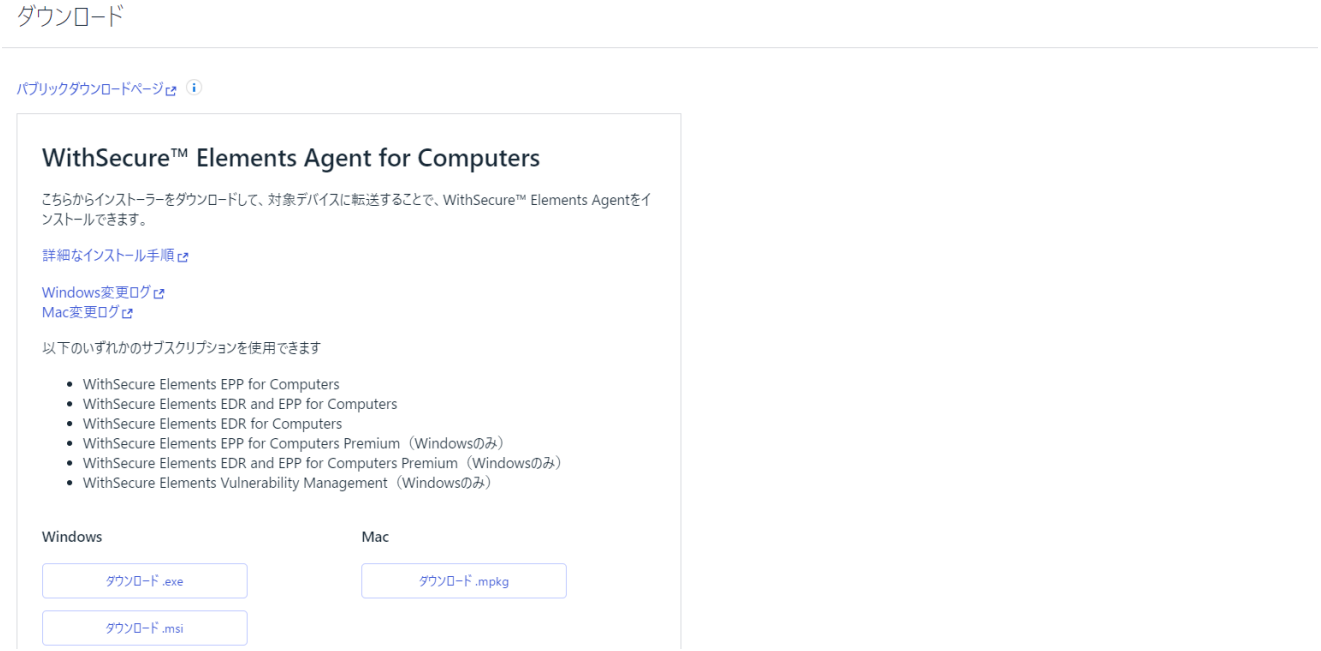
10.3. 監査ログ

ESC への管理者ログインやプロファイルの変更など、ESC に関する監査ログを確認することができます。



10.4. ダウンロード

Elements 製品のインストーラをダウンロードすることができます。表示される製品は、契約のあるもののみです。



11. セキュリティサービス

WithSecure が提供しているサービスについての一覧を記載しています。契約がある場合、以下のように表示されます。

12. サポート

パートナーポータルやサポートリクエストページのリンクなどをまとめています。また、障害情報を表示するシステムステータスへのリンクも記載しています。

13. Appendix

Elements 製品が利用する URL
インターネット接続を制限している環境において Elements 製品を使用するためには、、弊社 URL への接続を許可する必要があります。以下のコミュニティ記事を参照し、必要な URL への接続を許可してください。

参考 URL：
withsecure-elements-のネットワークアドレス-クラウド管理製品

http://community.withsecure.com/ja/kb/articles/31217-withsecure-elements-のネットワークアドレス-クラウド管理製品