ESET PROTECT MDR Ultimate
スターターガイド

キヤノンマーケティングジャパン株式会社

第15版 2024年11月29日

はじめに

近年のサイバー攻撃は、非常に複雑かつ巧妙化されているため、
従来のセキュリティ対策だけでは防ぎきれないケースも多く見られるようになってきました。

そこで注目されているのが **XDR(eXtended Detection & Response)**です。
XDR は、「攻撃を防ぐこと」を目的とした従来のアンチウイルスソフト等のセキュリティ対策製品とは違い、
異なるセキュリティ製品・レイヤーで収集された様々な種類のイベントデータを統合して、エンドポイントでの調査、対応、
ハンティングを適切かつ迅速に行うことを目的としています。

したがって、近年のサイバー攻撃への対策では、従来の「事前対策」に加え、XDR による「事後対策」を合わせる方策が必要とされています。

XDRは様々なレイヤーで常時データを収集し、それらを分析して怪しい挙動を発見するため、日々の監視や運用が重要です。
そこで、XDRを導入する企業は、その運用負荷を軽減するため、セキュリティ会社が提供する **MDR(Managed Detection & Response)**を利用して、XDRの監視や運用をアウトソーシングすることが求められています。

本資料では、ESETのXDRコンポーネントである**「ESET Inspect」**と、MDRを含んだ**「セキュリティサービス」**を合わせてご提供するXDRソリューション**「ESET PROTECT MDR Ultimate」**についてご紹介します。

はじめに

本資料は、 ESET PROTECTソリューションのうち、 ESET PROTECT MDRをご検討いただいているお客様に、ご利用可能なプログラムやサービス、セキュリティサービスの概要、製品の利用開始方法などをご理解いただくことを目的としております。

- 対象ソリューション：**ESET PROTECT MDR Ultimate**
- 対象プログラムとサービス

プログラム名/サービス名	プログラム/サービス概要	XDRによる管理
ESET Endpoint Security (EES)	Windowsクライアント用	●
ESET Endpoint アンチウイルス (EEA)		
ESET Endpoint Security for OS X (EESM)	Macクライアント用	●
ESET Endpoint アンチウイルスfor OS X (EEAM)		
ESET Endpoint アンチウイルス for Linux (EEAL)	Linuxデスクトップ用	●
ESET Endpoint Security for Android (EESA)	Android用	×
ESET Server Security for Microsoft Windows Server (ESSW)	Windowsサーバー用	●
ESET Server Security for Linux (ESSL)	Linuxサーバー用	●
ESET LiveGuard Advanced (ELGA)	クラウドサンドボックス	-
ESET Full Disk Encryption (EFDE)	フルディスク暗号化	-
ESET Inspect (EI)	クラウド型XDR	-
ESET Inspect on-prem (EI on-prem)	オンプレミス型XDR	-
ESET PROTECT (EP)	クラウド型セキュリティ管理ツール	-
ESET PROTECT on-prem (EP on-prem)	オンプレミス型セキュリティ管理ツール	-
セキュリティサービス	MDRサービス+ プレミアムサポートサービス	-

※ご利用いただく各プログラムは最新バージョンのご利用を推奨しております。
（サポートより最新へバージョンアップのお願いをする場合もございます。）

もくじ

Ⅰ．セキュリティサービスご利用の流れ

セキュリティサービスのタイムラインについて

	納品月	納品月 ~1ケ月後~	納品月 ~2ケ月後~	納品月 ~3ケ月後~	…	納品月 ~9ケ月後~	…	納品月 ~11ケ月後~	納品月 ~12ケ月後~
発注～納品フェーズ	初期フェーズ			運用フェーズ					

ご発注～製品ライセンス納品

ご発注書のほか本サービス所定の申込書(Sales Order Form)をご提出ください。
Sales Order Formのご提出をもってESET所定のサービス規約(Terms)に
ご同意いただいたものとみなします。
ライセンス納品時から本ソリューションの利用が開始されます。
お客様には「利用開始案内付き納品メール」「パスワード案内メール」の2通が送信されます。

アセスメント

本サービスご利用に必要なアセスメントフォームを記入いただき、ミーティングを実施します。

EP/EI利用開始

ESET PROTECT と ESET Inspectのアクティベーションしていただきます。

ESET Services Hub 利用開始

お問い合わせにご利用いただくServices Hubのアカウントを開設していただきます。

D&U (希望される場合)

「デプロイメント&アップグレード」をご利用いただくことで、エンジニアがお客様環境にESETを導入します。

初期最適化 (チューニング)

約1カ月でEIの初期最適化を実施します。
約1週間のログ集期間を経て、1~2週間かけて最適化を行い、効果測定実施後にレポートを提出します。

脅威モニタリング（日次）

エンジニアによる毎営業日ごとのモニタリングが開始されます。
重要なアラートが発見された場合は、ご担当者様にご連絡します。
また、定期的なモニタリングレポートの提出が実施されます。
XDRによって、インシデントの影響が広範囲におよぶと判断された場合には、
被害拡大を未然に防ぐために、XDRの自動アクション機能で端末全体に対して
初動対応(プロセスの停止やDLLの実行ブロック)が行われることがあります。

脅威ハンティング（四半期ごとおよびスポット）

お客様のEIにログインし、脅威ハンティングを行います。
任意のタイミングで年1回ご利用いただけるオンデマンドと
年4回（四半期ごと）ご利用いただけるプロアクティブがございます。

HealthCheck Service

お客様環境にインストールされたESETの構成や設定を確認します。
本サービスはお客様の任意のタイミングでご利用可能です。

2年目以降 サービス継続

ESET PROTECT MDR有効期限（製品・サービスのご契約期間）

1. アセスメント

STEP1	アセスメント
STEP2	ESET PROTECT HUBの開設
STEP3	ライセンスの登録
STEP4	EP/EIのアクティベーション
STEP5	ESET Services Hubの開設
STEP6	デプロイメント&アップグレード
STEP7	初期最適化（チューニング）

セキュリティサービス
で提供する作業内容

1. アセスメント

- アセスメントの流れは以下になります。

1.　アセスメントフォームの入力

2.　アセスメントMTGの実施

- ご契約完了後、弊社サポートより、アセスメントフォームを送付いたします。アセスメントフォームへはお客さまの環境や構成をご記入いただきます。

  <アセスメントフォームにご記入いただく主な内容>
  - 導入環境（拠点数やネットワーク構成、ネットワーク機器の有無など）
  - ご利用端末のOSと台数
  - 各ユーザーのアクセス権
  - ユーザーのリモートアクセスの有無
  - お客様のセキュリティポリシーや注意が必要な環境
  - 利用アプリケーションのホワイトリスト　　など

- アセスメントMTGとは、初期最適化や脅威モニタリング時に発生したアラートに対する判断材料とするため、サービス導入前にお客様環境をヒアリングさせていただくミーティングです。
- ご記入いただいたアセスメントフォームをもとに、内容の確認や運用に関するミーティングを実施いたします。（2時間程度）

2. ESET PROTECT HUBの開設

STEP1 アセスメント

STEP2 ESET PROTECT HUBの開設

※ESET Business Accountをすでに開設済みの場合はSTEP3へお進みください

STEP3 ライセンスの登録

STEP4 EP/EIのアクティベーション

STEP5 ESET Services Hubの開設

STEP6 デプロイメント&アップグレード

STEP7 初期最適化（チューニング）

セキュリティサービス
で提供する作業内容

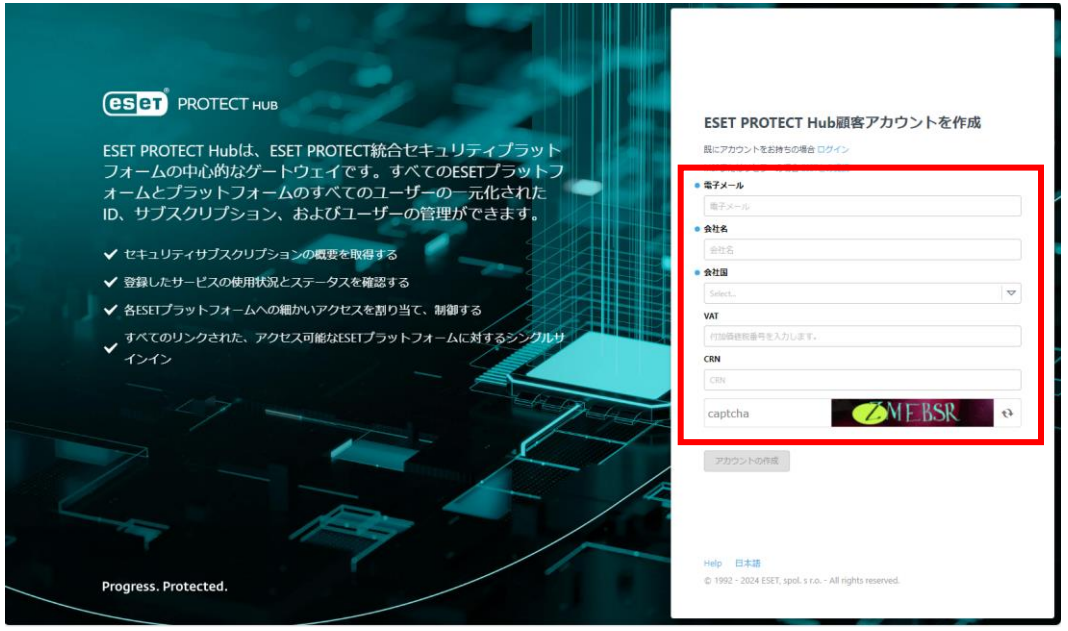
2. ESET PROTECT HUBの開設

※ESET Business Accountをすでに開設済みの場合はSTEP3(p13)へお進みください

1. https://protecthub.eset.com/にアクセスし、ログイン画面で「無料で登録」をクリックしアカウント作成を開始
2. 画面に表示される説明に沿ってお客様情報を入力
   ※ 電子メールアドレスやパスワード、名前、電話番号、お客様企業名などを入力します
   ※ 本手順で設定した電子メールアドレスとパスワードはEPHログイン時に使用します

■ログイン画面

■アカウント作成画面

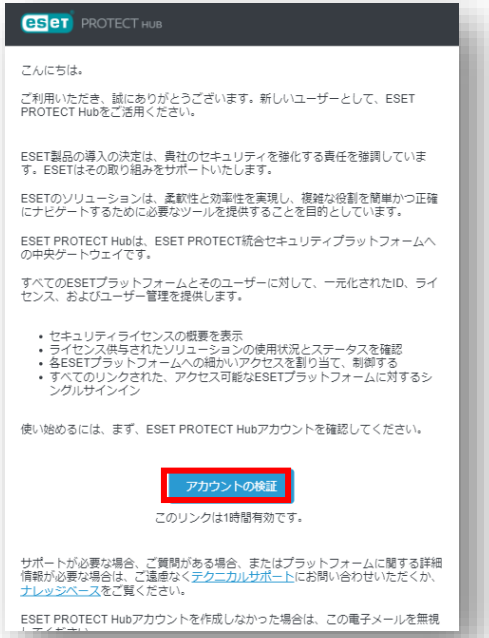


2. ESET PROTECT HUBの開設

3. アカウントのアクティベーション
※ 登録した電子メールアドレスに「@eset.com」からメールが届きます
※メール内の「アカウントの検証」をクリックします

■確認メール送信の完了画面

■アクティベーション用メール



2. ESET PROTECT HUBの開設

4. 名前(名)、名前(姓)、パスワードを入力し、「続行」をクリック

5. ユーザーの国、言語、電話番号(任意)を入力し、「ESETに同意する」にチェックが入っていることを確認後、「アカウントをアクティベーションする」をクリックアカウントがアクティベーションされたことの確認
※ 登録した電子メールアドレスに「@eset.com」からメールが届きます

■アカウントをアクティベーションする(1/2)

■アカウントをアクティベーションする(2/2)

2. ESET PROTECT HUBの開設

6. アカウントがアクティベーションされたことの確認

7. EPHにログインできることの確認
※「アカウントをアクティベーションする(1/2) 」で登録した電子メールアドレスとパスワードを使用します

■アクティベーション完了確認用画面

■EPHにログインできることの確認

3. ライセンスの登録

STEP1 アセスメント

STEP2 ESET PROTECT HUBの開設

STEP3 ライセンスの登録

STEP4 EP/EIのアクティベーション

STEP5 ESET Services Hubの開設

STEP6 デプロイメント&アップグレード

STEP7 初期最適化（チューニング）

セキュリティサービス
で提供する作業内容

3. ライセンスの登録

- **EBAをご利用の場合は本スライドp14-15、EPHをご利用の場合はp16-17の手順を実施ください**

EBAご利用の場合

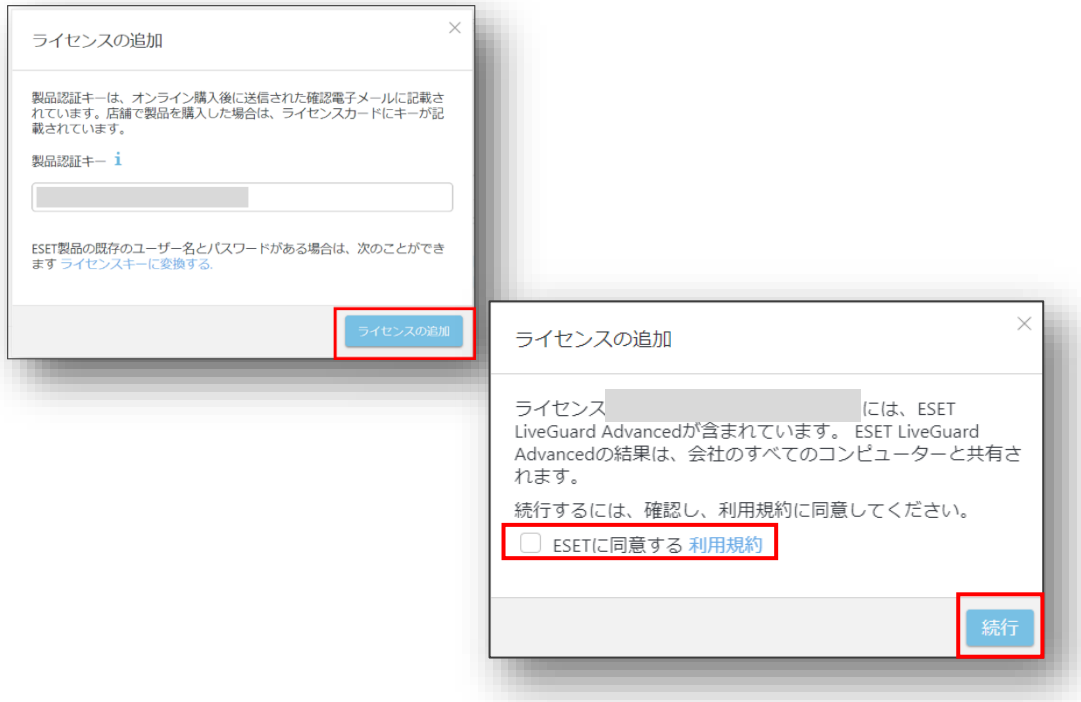
1. EBAへのライセンスの登録

※ 弊社ユーザーズサイトで確認できる以下の情報をご用意ください。
- 製品認証キー

※ 「ライセンスの追加」画面ではESETの利用規約へご同意いただく必要がございます。
※ ユーザーズサイトでのライセンス情報確認の方法は以下をご参照ください。
https://eset-support.canon-its.jp/faq/show/82?site_domain=business

①[ダッシュボード]内の[最初のライセンスを追加する]

②[ライセンスの追加]画面

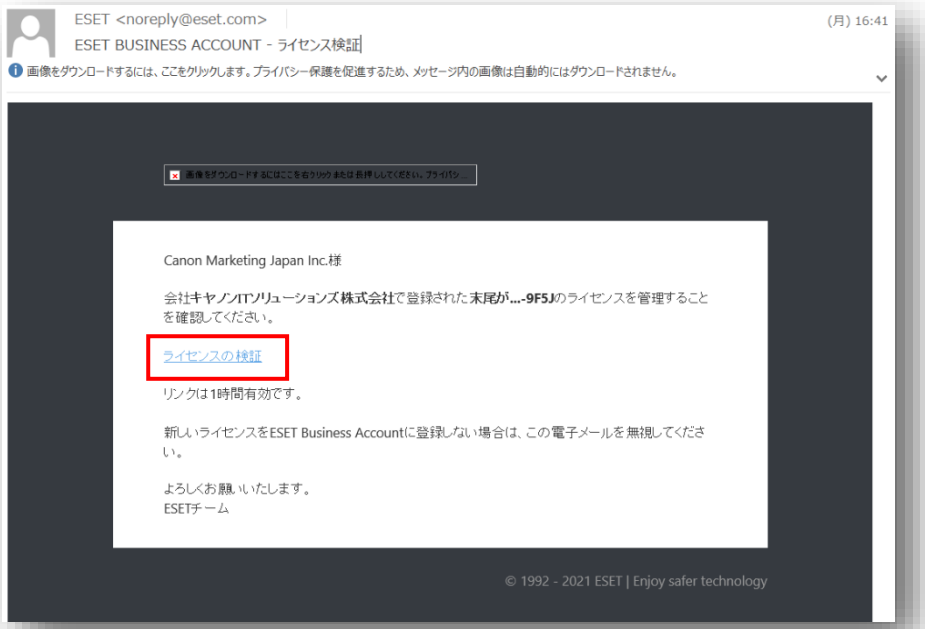


3. ライセンスの登録

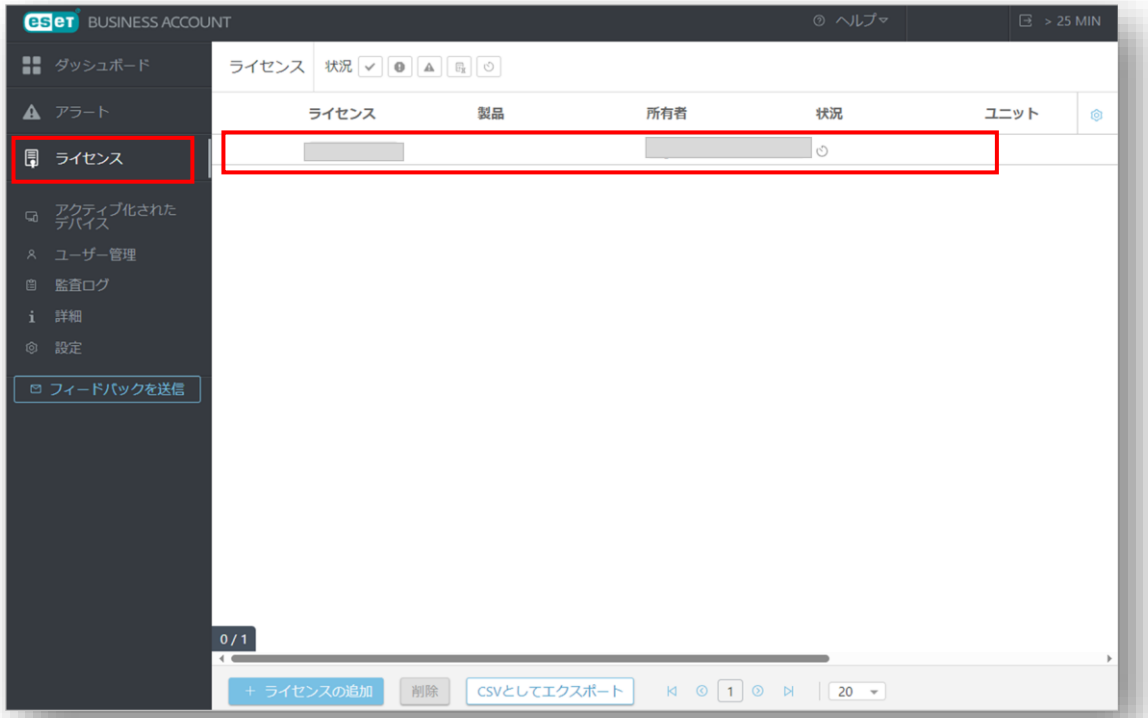
EBAご利用の場合

2. ライセンスのアクティベーション
   ※ ライセンス契約時の電子メールアドレスにアクティベーションメールが送信されます。
3. ライセンスが追加されたことの確認

■ライセンスアクティベーション時のメール例



■ライセンスが登録されたことの確認画面例



3. ライセンスの登録

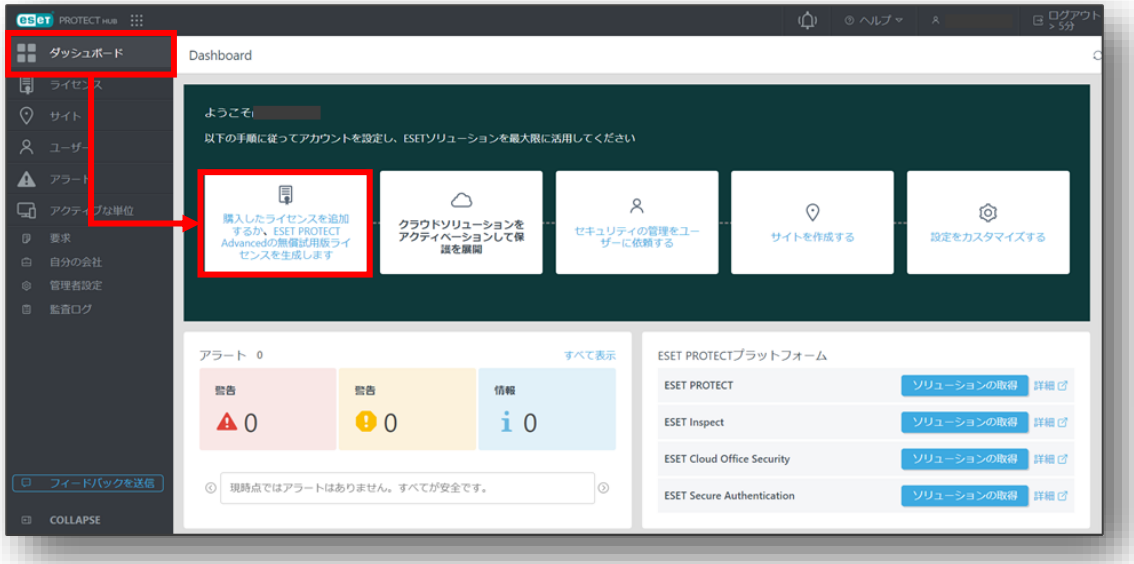
1. EPHへのライセンスの登録

EPHご利用の場合

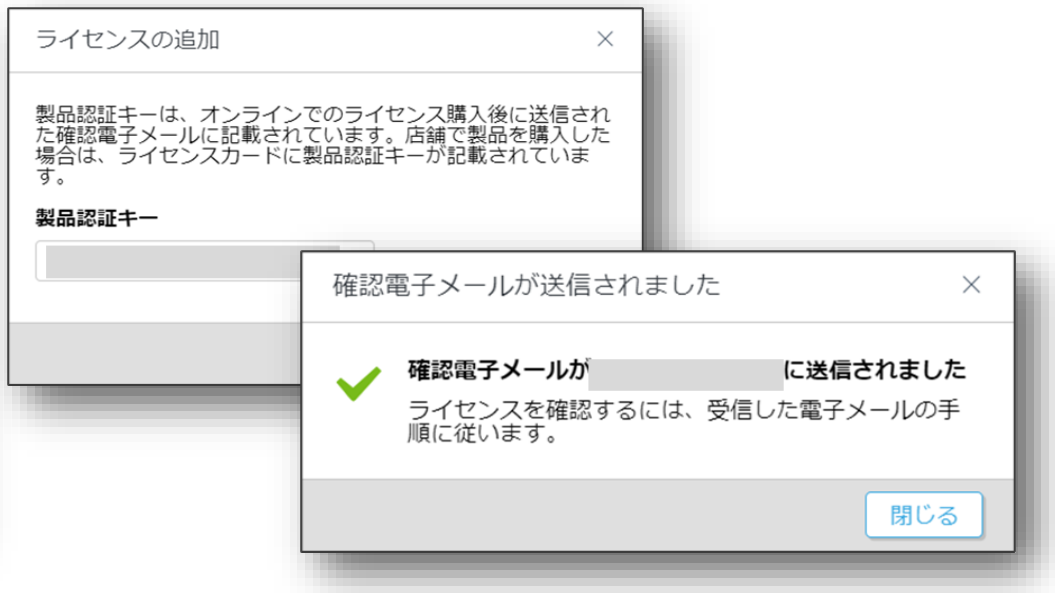
※ 弊社ユーザーズサイトで確認できる以下の情報をご用意ください。
- 製品認証キー

※ 「ライセンスの追加」画面ではESETの利用規約へご同意いただく必要がございます。
※ ユーザーズサイトでのライセンス情報確認の方法は以下をご参照ください。
https://eset-support.canon-its.jp/faq/show/82?site_domain=business

■[ダッシュボード]内の[購入したライセンスを追加する]をクリック



■[ライセンスの追加]画面



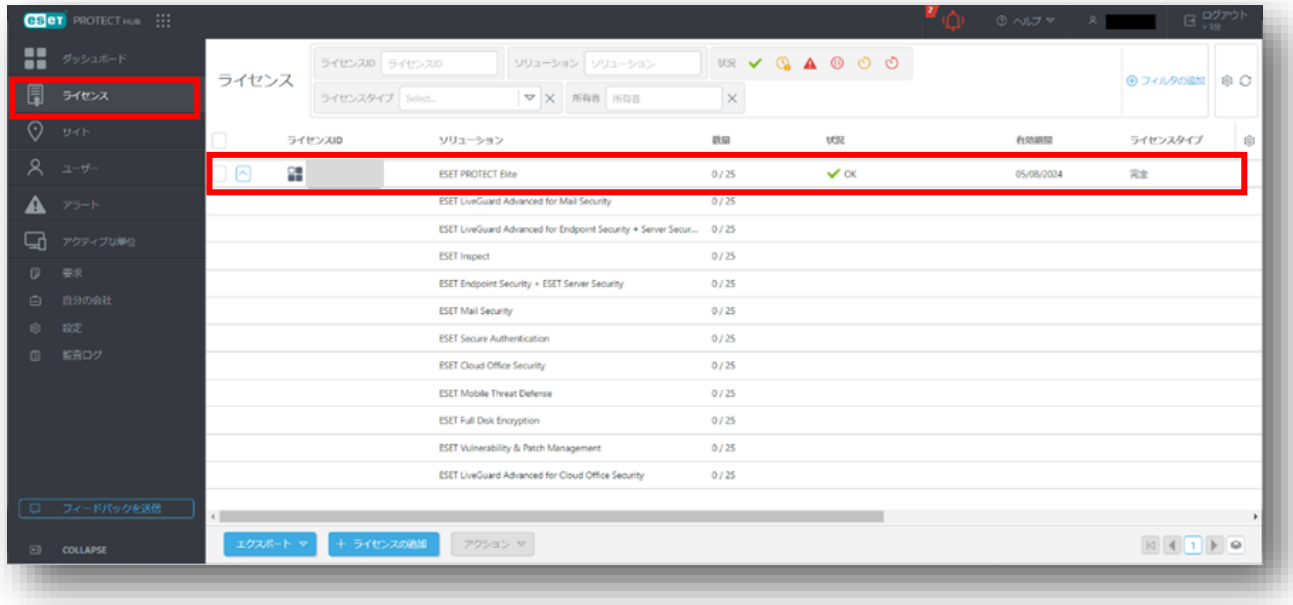
3. ライセンスの登録

EPHご利用の場合

2. ライセンスのアクティベーション
   ※ ライセンス契約時の電子メールアドレスにアクティベーションメールが送信されます。
3. ライセンスが追加されたことの確認

■ライセンスアクティベーション時のメール例

■ライセンスが登録されたことの確認画面例



4. EP/EIのアクティベーション

Digital Security
Progress. Protected.

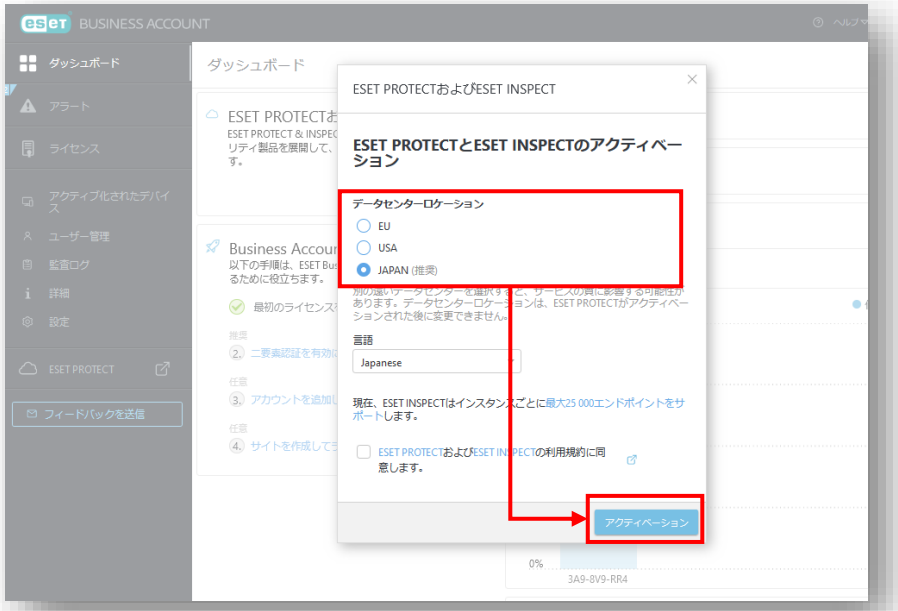
- STEP1 アセスメント
- STEP2 ESET PROTECT HUBの開設
- STEP3 ライセンスの登録
- **STEP4 EP/EIのアクティベーション**
- STEP5 ESET Services Hubの開設
- STEP6 デプロイメント&アップグレード
- STEP7 初期最適化（チューニング）

セキュリティサービス
で提供する作業内容

4. EP/EIのアクティベーション

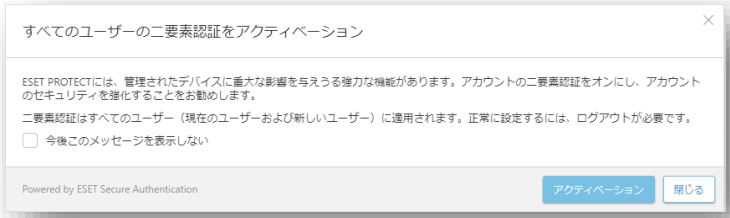
1. EPとEIのアクティベーション（左側メインメニューの「ESET PROTECT 」をクリックして開始します）
2. 10分～15分でアクティベーション完了
   ※ データセンターのロケーション選択画面では必ずJAPANを選択してください。
   ※ ESET PROTECT とESET Inspect が同時にアクティベーションされます。
3. 二要素認証の設定
   ※ EP/EIのアクティベーション完了後にポップアップが表示されますので設定をお願いいいたします。

■データセンターのロケーション選択画面



■ESET PROTECT アクティベーション画面

■ESET PROTECT 二要素認証設定画面



5. ESET Services Hubの開設

Digital Security
Progress. Protected.

STEP1	アセスメント
STEP2	ESET PROTECT HUBの開設
STEP3	ライセンスの登録
STEP4	EP/EIのアクティベーション
STEP5	**ESET Services Hubの開設**
STEP6	デプロイメント&アップグレード
STEP7	初期最適化（チューニング）

セキュリティサービス
で提供する作業内容

5. ESET Services Hubの開設

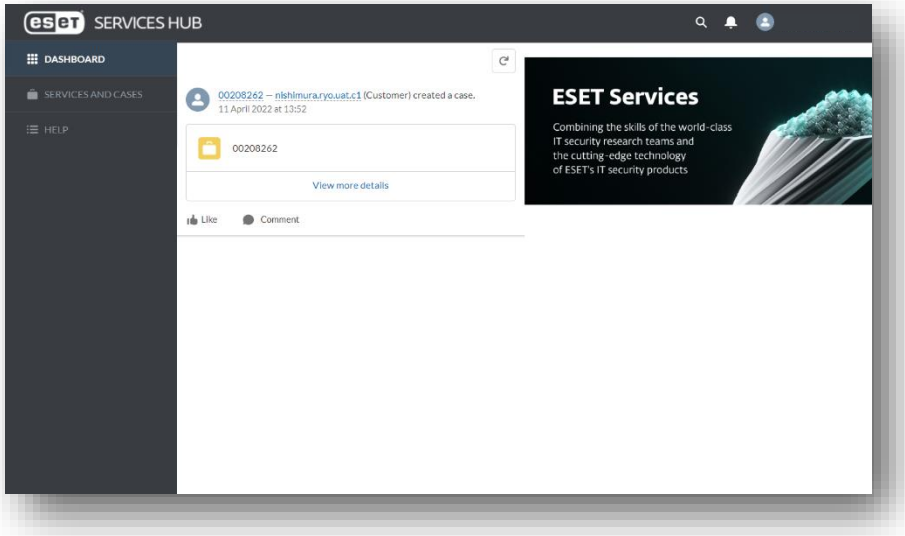
- ESET Services Hubの概要

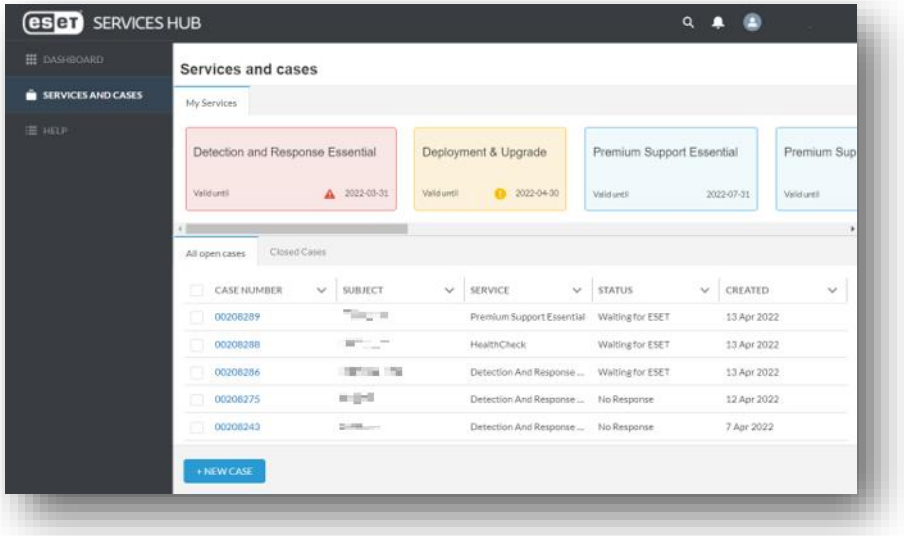
ESET Services Hubとは

「ESET Services Hub」とは、お客様のお問い合わせチケットを作成および管理するESET社が提供するWebサービスです。
セキュリティサービスに関するお問い合わせについては、本Webサービスをご利用ください。

ESET Services Hubで実施できること

- セキュリティサービスに関するお問い合わせチケットの作成
- お問い合わせチケットの継続のご対応
- お問い合わせチケットの管理





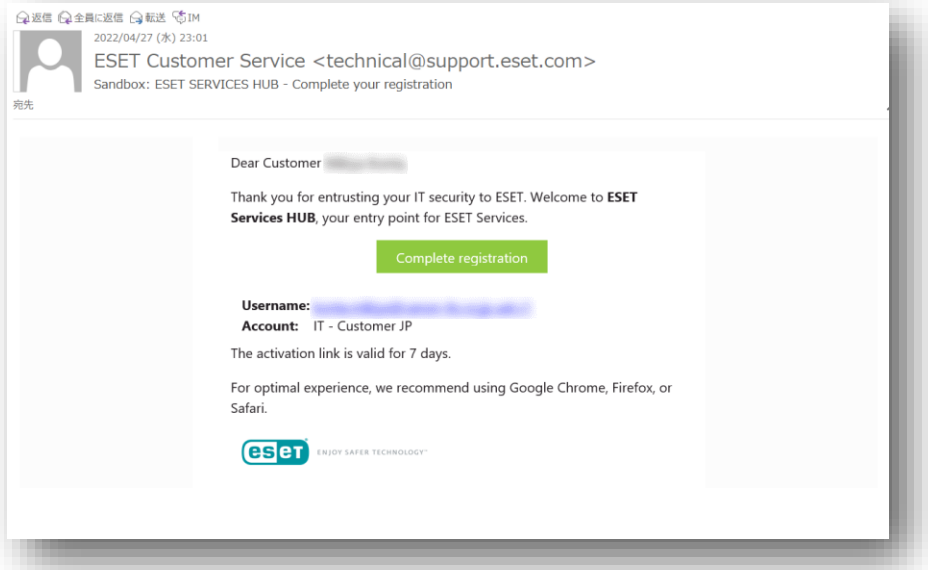
5. ESET Services Hubの開設

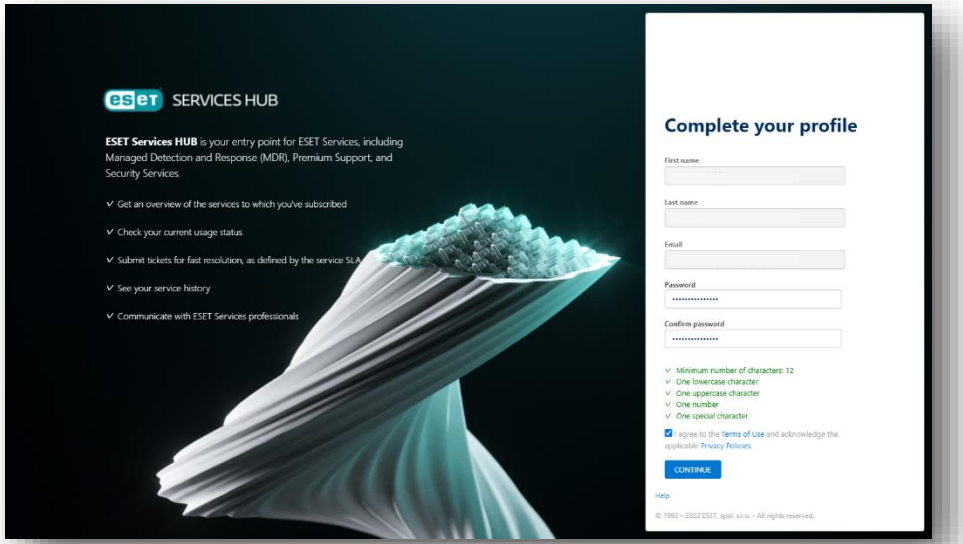
- ESET Services Hubの利用方法

アカウント開設方法

1. 件名「ESET Services HUB – Complete your registration」の招待メールを開き、
   メール内に記載されている「Complete Registration」をクリックします。

2. Webブラウザに表示された「Complete your profile」画面で、パスワードの設定および利用規約に同意します。
   ※次回以降のログインでは2要素認証の設定が必要となります。
   再ログイン時に表示される、画面「Connect Salesforce Authenticator」の手順に従って設定します。





6. デプロイメント&アップグレード

6. デプロイメント&アップグレード

- デプロイメント&アップグレード(以降D&U)の利用をご希望の場合、プログラムの展開の流れは以下になります。
  ※D&Uとは、エンジニアがお客様の環境にリモートアクセスし、ESETプログラムの展開を支援するサービスです
  ※本サービスをご利用の場合、アセスメントシート入力から作業完了まで約1ヵ月程度かかります

1. お客さまによるアセスメントフォームの入力

- 弊社サポートより、アセスメントフォームを送付いたします。アセスメントフォームへはお客さまの環境やESETの導入状況などをご記入いただきます。

  <アセスメントフォームにご記入いただく主な内容>
  - ご利用端末のOSや台数
  - 環境情報（端末の利用状況や勤務形態など）
  - 実施希望日
  - 現在ESETがインストールされている場合プログラムのバージョン

2. サービス提案書の提出

- ご記入いただいたアセスメントフォームをもとに、エンジニアが展開方法などを記載したサービス提案書を作成し、お客さまへ提出いたします。

3. エンジニアによる作業実施

- サービス提案書に沿ってエンジニアより以下いずれかを実施します。
  ・インストーラーを作成しリモートインストール
  ・クライアントタスクによるリモートインストール
  またはインストール支援を実施します

7. 初期最適化（チューニング）

STEP1 アセスメント

STEP2 ESET PROTECT HUBの開設

STEP3 ライセンスの登録

STEP4 EP/EIのアクティベーション

STEP5 ESET Services Hubの開設

STEP6 デプロイメント&アップグレード

STEP7 初期最適化（チューニング）

セキュリティサービスで提供する作業内容

7. 初期最適化（チューニング）

- 初期最適化は以下の2つの方法で行います。

※ 初期最適化とはお客様業務により発生するアラートをEIの各検出ルールから除外することで、脅威により発生したアラートを見つけやすくする作業です。
※ 一度きりの検出を除外するのではなく、何度も繰り返し発生しているアラートを中心に除外を作成します。
※ 初期最適化完了後も脅威モニタリング時の継続したチューニングを実施します。
※ 初期最適化中のモニタリングはベストエフォートでの対応になります

「ルール学習モード」によるチューニング

- EIには、自動で除外を作成できる「ルール学習モード」が搭載されています。
初期チューニング時には、本機能を有効化し、お客様業務により発生する
アラートを一定期間EIに認識させることで自動で除外を作成します。
「ルール学習モード」の期間が終了したら、EIが作成した除外を有効化するか
を選択します。

＋

手動による初期チューニング

- EIで発生したアラートを確認し、お客様業務により発生している
アラートであることが確認できた場合は除外を作成します。
※ LiveGridによるReputationやPopularity、親プロセスなどの情報を除外ルールに含めることで、
よりセキュアな除外が作成できます。

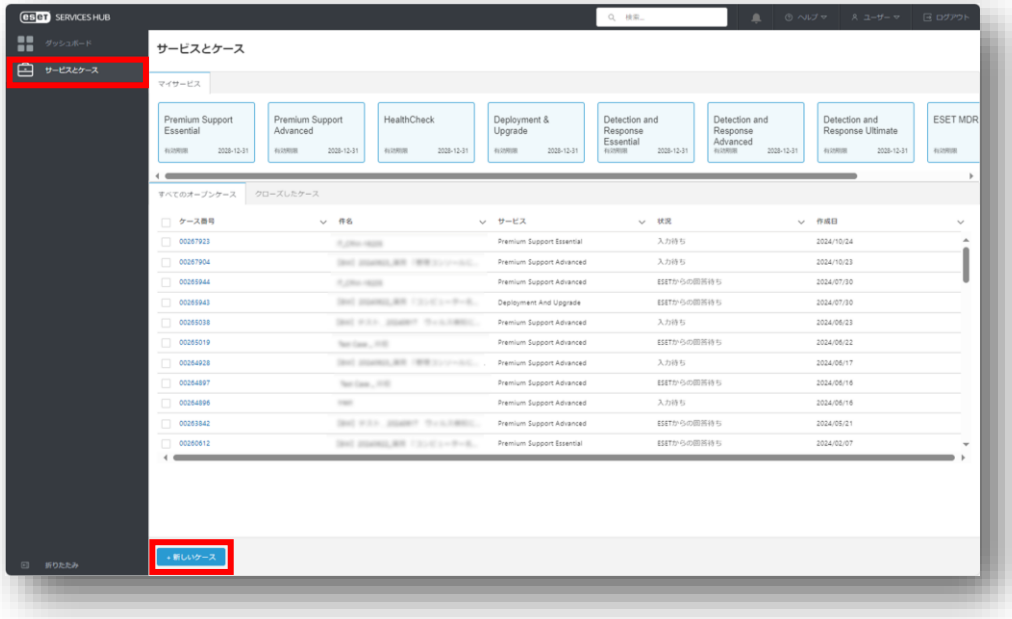
Ⅱ. セキュリティサービスのお問い合わせ方法

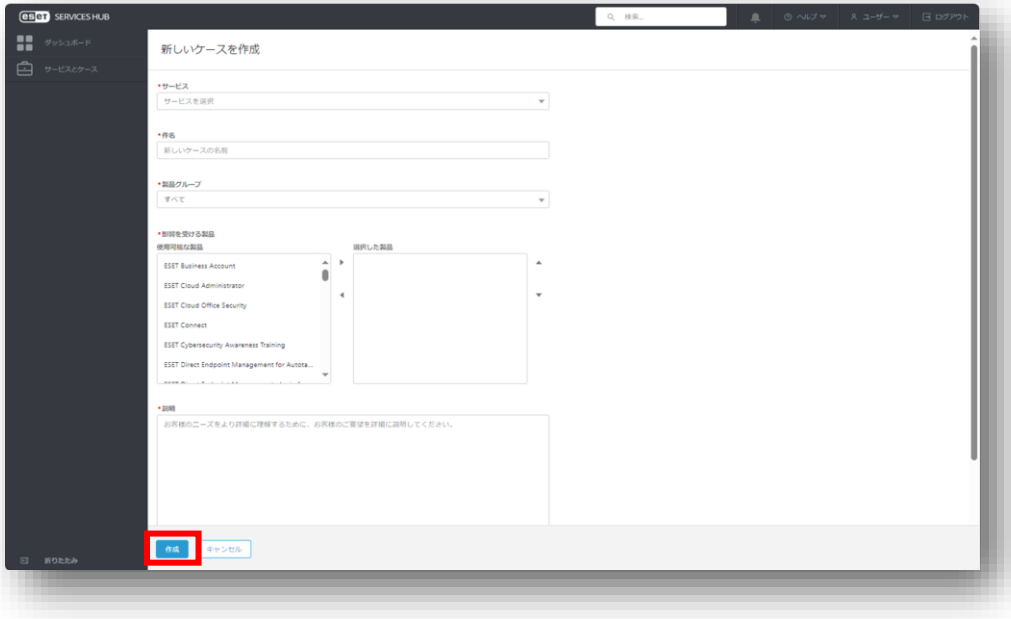
1. ESET Services Hubについて

ESET Services Hubの利用方法

お問い合わせチケットの作成方法

1. 画面左側の「サービスとケース」を開き、画面下部の[新しいケース]をクリックしてお問い合わせチケットを作成します。
2. 必要項目をすべて入力し、[作成]をクリックしチケット作成を完了します。
   ※添付ファイルはチケット作成後に別途添付可能です。



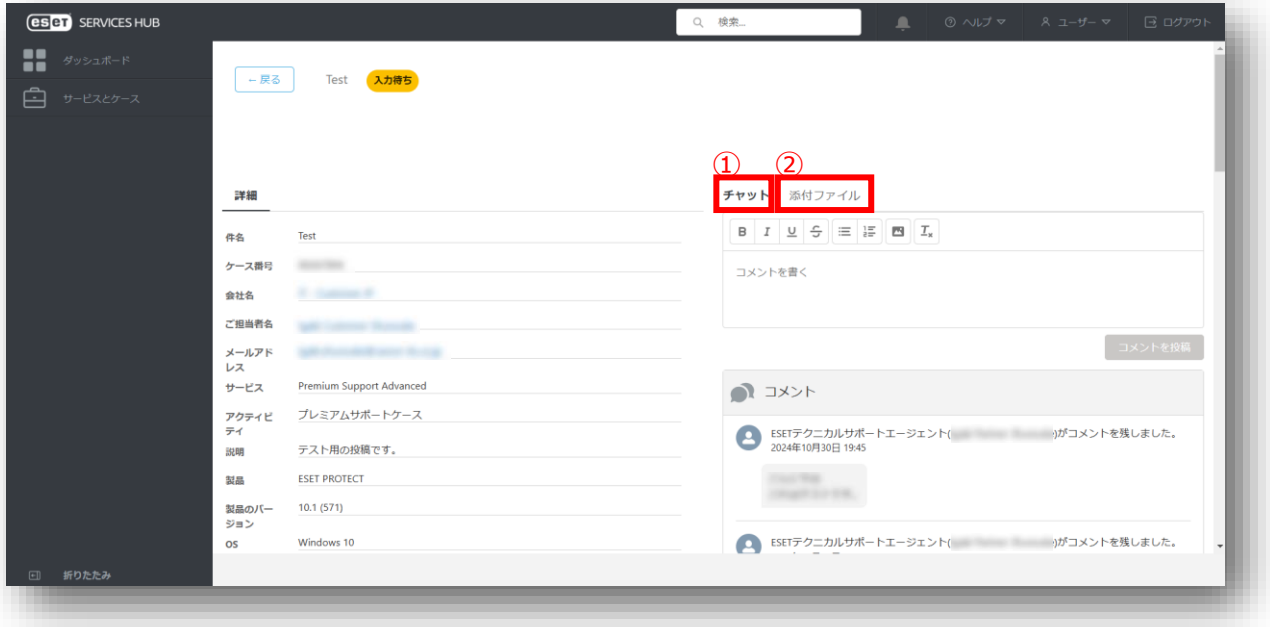


1. ESET Services Hubについて

ESET Services Hubの利用方法

オープン中のお問い合わせチケットの対応方法

1. 画面左側の「サービスとケース」を開き、表示されたお問い合わせチケットから対応を行いたいものをクリックします。
2. 選択したお問い合わせチケットに関して、チャットの返信や添付ファイルの送付などの各種対応を行います。



① チャット

お問い合わせチケットに対してのオペレーターからの連絡に返信することができます。

② 添付ファイル

お問い合わせチケット作成後に、問い合わせに関連するファイルを添付することができます。

2. よくあるお問い合わせ

よくあるお問い合わせ

Q. ESETのMDRの強みを教えてください。
A. 1) XDRだけでなく、エンドポイント保護（EPP）も対象とする包括的な監視サービスです。
2) 24時間・365日の監視・運用サービスで、国内拠点で日本語応答しますのでいざという時にも安心です。
3) インシデント発生時の駆除・ネットワーク隔離までサポートします。

Q. ESETを既に利用中ですが、エンドポイントのプログラムは入れ替えが必要ですか？
A. 現在ご利用のプログラムはそのままお使いいただけます。上位プログラムへの変更も上書きインストールが可能です。

Q. オフライン環境ですが、MDRの導入は可能ですか？
A. プロキシ導入と必要な通信の許可をいただければ導入可能です。

Q. ネットワーク隔離が実施された場合、全ての通信を止めるのですか？
A. ESETの管理ツール、XDRとの通信以外を遮断しますので、横展開を防ぎつつリモートでのインシデント対応が可能です。

Q. XDRのセンサーを入れると端末の負荷は上がるのでしょうか？
A. 通信量は多少増えますが、ESETではEPPがセンサーも兼ねているので負荷はほとんど変わりません。