ESET PROTECT MDR Ultimate
サービス詳細資料

キヤノンマーケティングジャパン株式会社

第1版 2024年8月22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 PROTECT (EP)	クラウド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について

1. ソリューションの概要

Digital Security
Progress. Protected.

ESETが提供するXDRソリューションについて

事後対策のニーズ	XDR運用のニーズ	ソリューション
● 社内に潜む潜在的な**脅威を早期に発見**したい ● 社内ネットワークで何が起きているかを**リアルタイムで可視化**したい ● 脅威発生時の**インシデント対応**（影響調査や原因調査）を**高速化・効率化**したい ● 侵害が発生した際の**被害の抑制**（封じ込めや除去）を短時間で行いたい ● ランサムウェアによる**データ流出の防止や早期発見**の仕組みを備え，セキュリティを強化したい ● 事前対策(EPP)から事後対策(XDR)まで、**ワンベンダー**でまとめて効率的に運用したい	**専門家への完全アウトソース** ● セキュリティサービスを**フルメニュー**で提供 ● 侵入時には**お客さまと連携しながらセキュリティエンジニアが脅威封じ込め**などの初動対応	**ESET PROTECT MDR Ultimate**
	脅威の初動対応のアウトソース ● 提供メニューを厳選した**ベーシックなメニュー**で提供 ● 侵入時には**自動化したシステムとセキュリティエンジニア作業により脅威封じ込め**などの初動対応	**ESET PROTECT MDR Lite**

	クラウド型セキュリティ管理ツール	オンプレミス型セキュリティ管理ツール	基本的なエンドポイント保護	総合的なエンドポイント保護	クラウドサンドボックス	フルディスク暗号化	クラウドアプリケーションセキュリティ	脆弱性とパッチ管理	XDR	MDRサービス	プレミアムサポートサービス
ESET PROTECT MDR 専門家へのアウトソース	●		●	●	●	●	-	-	●	●	●

* MDRサービスおよびプレミアムサポートサービスを利用される際はセキュリティ管理ツールおよびXDRともクラウド利用が前提となります。
* 別途ESET PROTECT MDR Liteについての資料もご用意しております。

1. ソリューションの概要

ESETの強み

- 同一ベンダーだからこそできる、未然対策と事後対策のシームレスな統合

- 事前防御も事後対策もその運用サポートもオールインワンでご提供

強力な事前防御 ＋ XDRによる事後対策

駆除、NW隔離まで支援する充実の運用メニュー

日本語での手厚いサポート体制

1. ソリューションの概要

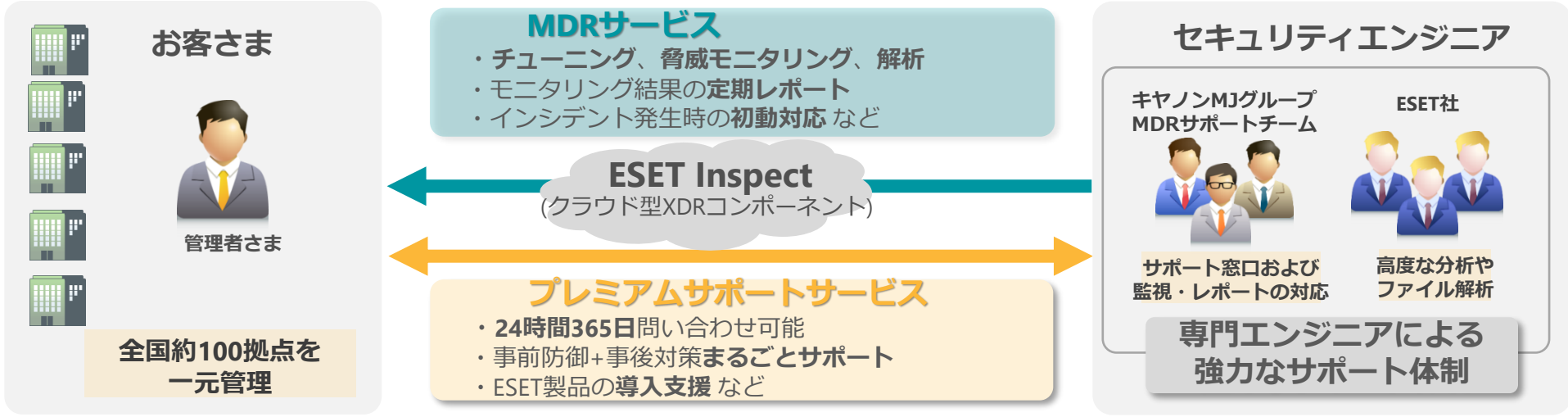
導入事例 (1/3)

- 株式会社ヴィアックス

「ESET PROTECT MDR」が、全国100拠点のセキュリティ強化と運用・監視業務の効率化を実現！

選定ポイント！

①スムーズなデモと対応と小工数の移行作業
②国内における監視＆サポートの充実



課題

- 全国約100拠点のセキュリティ対策が一様でなく、外部からの攻撃を防ぐには必ずしも十分でない場合があった
- 本社システム部門のリソースだけでは全拠点のセキュリティ状態をくまなく監視することが困難だった
- 拠点で発生している事象の状態を即座に把握できず、対処や復旧に時間を要する場合があった

効果

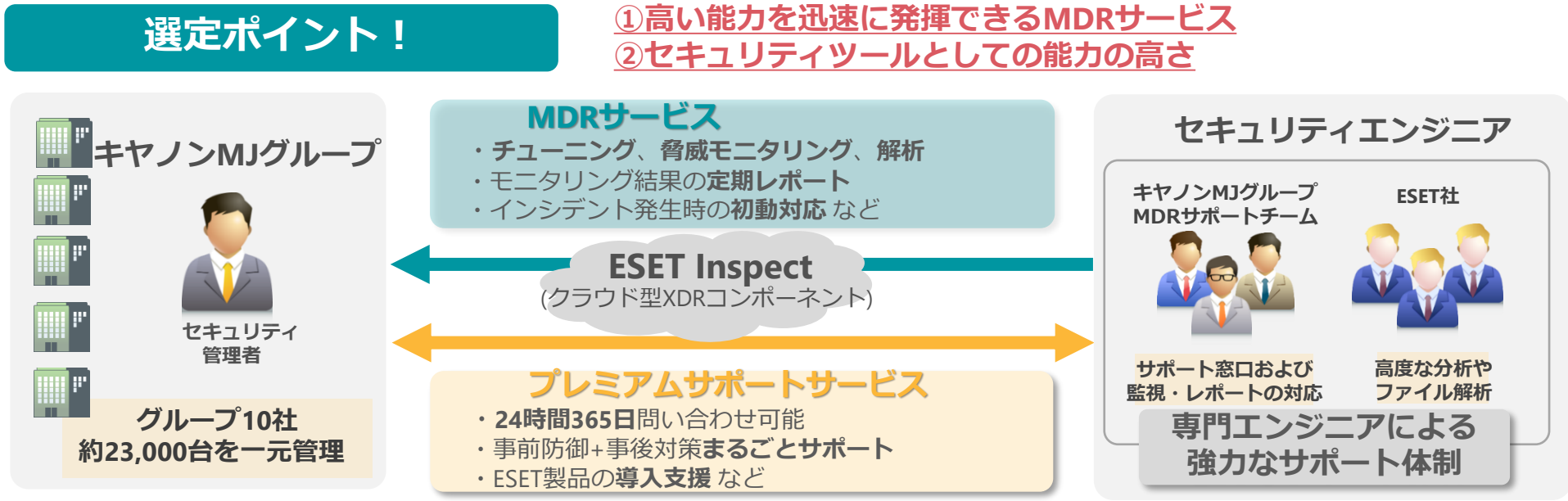
- MDRサービスを活用することで、**最低限の投資とリソースで24時間365日の高精度のセキュリティを確保**できるように
- 全拠点を一元的に管理可能となり、遠隔の本社からでも**各拠点の具体的な状況を把握**、かつ、**素早く事態の解決が可能に**
- MDRのサービスである、**脅威モニタリングレポートと脅威ハンティングレポートが担当者のスキルアップのみならず、自社のアピールにも有効に**

1. ソリューションの概要

導入事例 (2/3)

- キヤノンマーケティングジャパン株式会社

  約23,000台へのEDR/XDR導入を4ヶ月で実現！高度な運用/監視を短期でスタートしたカギはMDRサービス活用にあり



課題

- 近年の脅威拡大や業務環境の変化に対応した、セキュリティ強化の必要性を感じていた
- EDRを運用するには知識ある人員の確保が必要だが、育成するには時間がかかり新システム導入が遅れる
- キヤノンMJグループ10社の約23,000台が対象となる大規模な導入を、確実な作業で進行/短期間で完了させることが求められた

効果

- **予防・検知の仕組みについて納得のいく説明があり安心感が高まった**
  導入後は**アラートの検知数に加え、似た振る舞いをしたプロセスやPCも把握**
- **MDRサービスで自部門の負荷が最小限**になり、本来の業務への注力が可能に
  専門エンジニアならではの高いスキルにも期待できる
- MDRサービスで**人員確保・育成が不要となり、約23,000台への導入を大幅短縮**
  その後、大きな問題もなく、セキュリティ事故も発生していない

1. ソリューションの概要

導入事例 (3/3)

- 国内での導入実績一例（ ESET MDR Ultimate）

業種・業界、導入規模に依らない導入実績

No	業種・業界	ライセンス数
1	物流関連会社	約1400
2	サービス関連会社	約700
3	電気設備関連会社	約250
4	学校・教育関連団体	約300

- グローバルでの導入実績一例

No	会社名	業種	ライセンス数	導入メリット
1	Royal Swinkels Family Brewers （オランダ第2位のビールメーカー）	飲料	約2300	・24/365の監視と管理 ・ESETのサイバーセキュリティ専門家へのアクセス ・安心感
2	RAICAM （イタリアの自動車部品メーカー）	自動車	約500	・24/365のサポート体制 ・管理の容易さ ・コストとリソースの効率化

1. ソリューションの概要

第三者機関からの評価 (1/2)

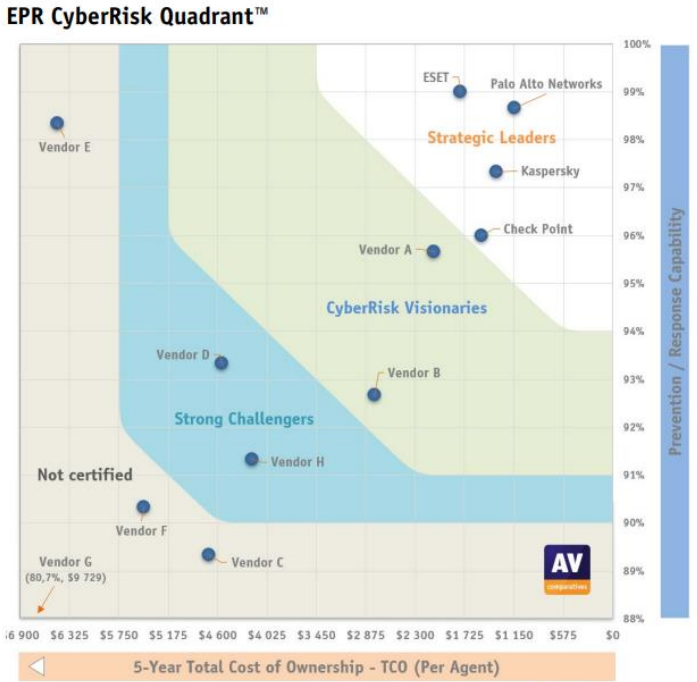
- ESETのEPPは「高い検出率」/「低い誤検知率」として高い評価を受賞
  MDRにおいて強力なEPPが導入されていることが、EDR運用の前提です

AV-comparatives

世界有数の独立系テスト機関AV-Comparativesにおいて、ESETは「Endpoint Prevention and Response(EPR) Test 2023」で**Strategic Leader**として認められています。

本テストでは、防御と対応能力について実環境に合わせた50のシナリオでテストを行い評価します。ESETは特に検出率、誤検知の少なさ、および直感的なデザインについて高いスコアを獲得しています。

なお、ESETは本EPRテストが開始されてから4年連続で認定を受けています。



1. ソリューションの概要

第三者機関からの評価 (2/2)

その他多く機関で高い評価を獲得

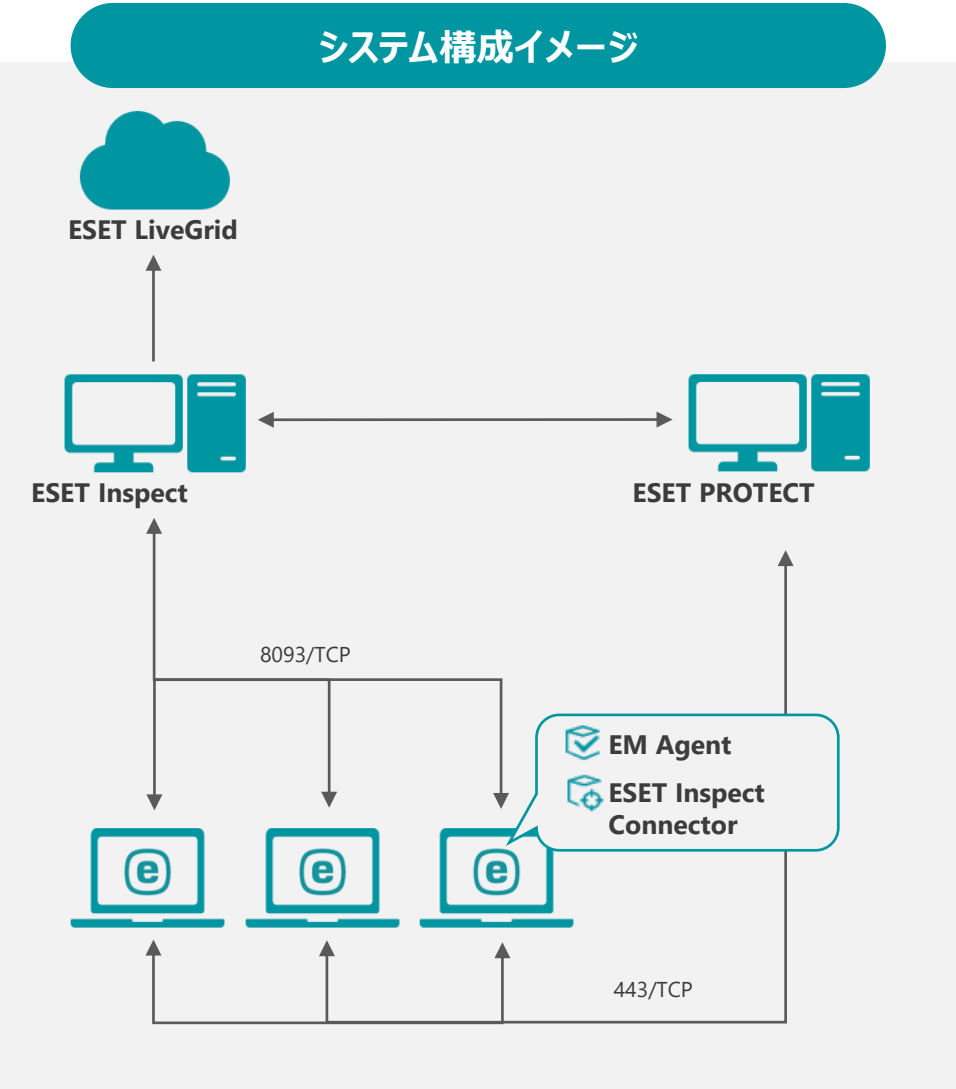
2023 Gartner Peer Insightsの「Voice of the Customer for Endpoint Protection Platforms」レポートで、Customers' Choiceとしてピア認定されました。

5年連続Champion
Cybersecurity Leadership Matrixは、直近12か月間のチャネル・プログラムを確立した主要なサイバーセキュリティ・ベンダーの評価です。

The Forrester Wave™: Endpoint Security, Q4 2023レポートで「Strong Performer」の評価を受けました。

etc...

2. システム構成(1/2)



ESET Inspect (EI)

EI/EI on-premはEI Connectorを使用してエンドポイントデバイスでリアルタイムにデータを収集します。データは一連のEI/EI on-prem内のルールと照合され、疑わしいアクティビティが自動的に検出されます。この集約されたデータにより、異常で疑わしいアクティビティをより効率的に検索し、正確なインシデント対応、管理、およびレポートの作成ができます。

ESET PROTECT (EP)

EP/EP on-premはクライアントプログラムの情報収集や設定の変更、インストーラーの作成、タスク配布などを行います。クライアントとの通信はEM Agentを経由して行います。

ESET Inspect Connector (EI Connector)

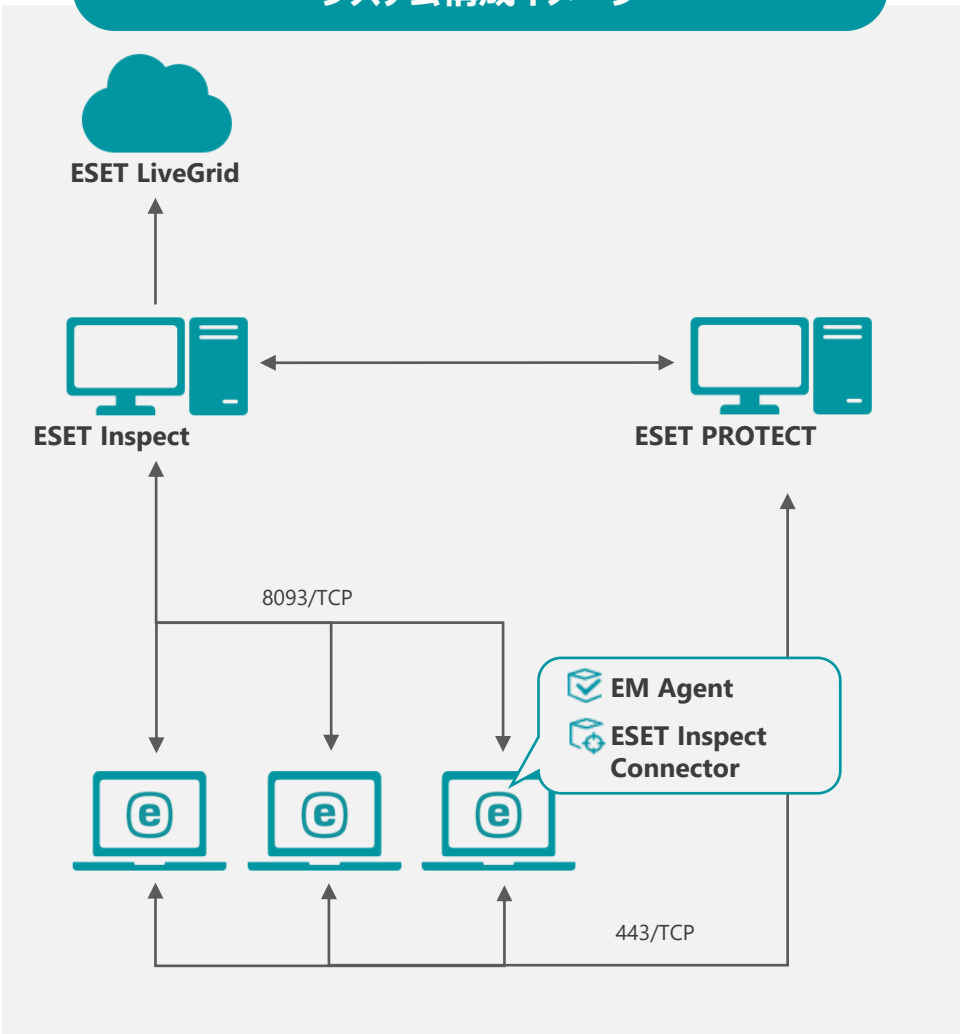
EI Connectorはクライアントのデータを収集し7分間隔でEIへデータを送信します。また、悪意のあるコンポーネントを削除し、これらのコンポーネントの実行をブロックします。

ESET Managementエージェント (EM Agent)

EM Agentは、クライアントから情報を収集し、10分間隔でEPへデータを送信します。また、EPからのタスク配布などはEM Agentへ送信されたのち、EM Agentがクライアントへ送信します。

2. システム構成(2/2)

システム構成イメージ



システム構成に関連する主な通信ポート

ポート	用途
443/TCP	EM AgentとESET PROTECT 間の通信に使用
8093/TCP	ESET Inspect ConnectorとESET Inspect 間の通信に使用

サポートされるプログラム

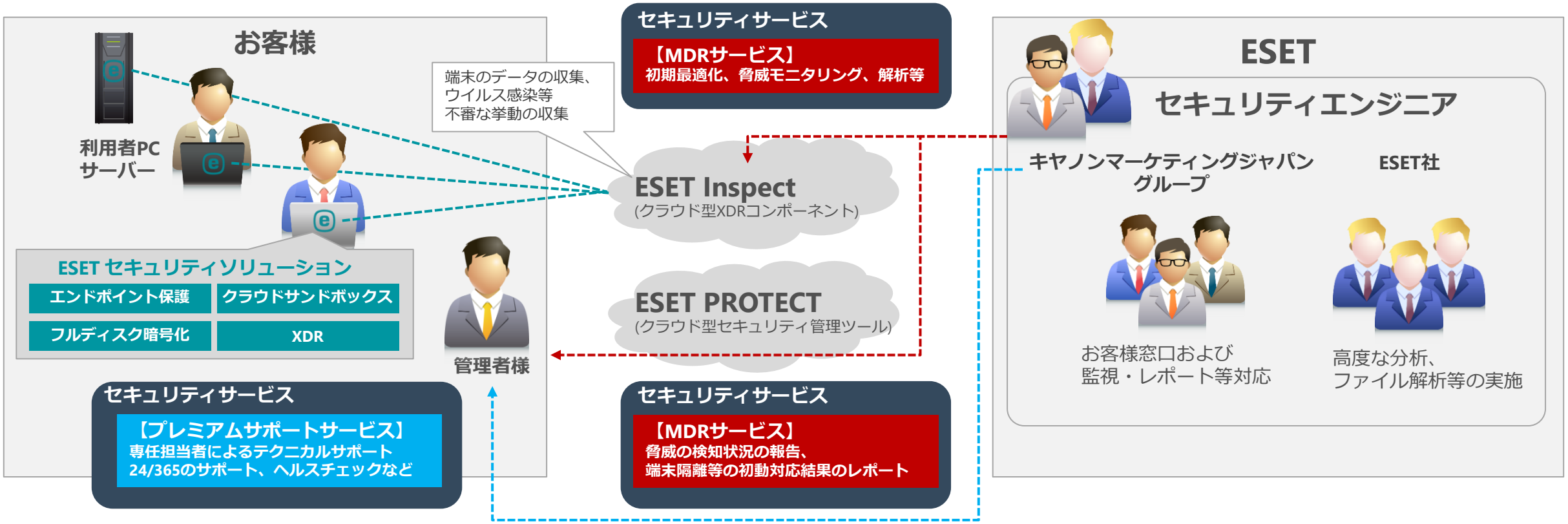
アプリケーション名
ESET Endpoint Security / アンチウイルス
ESET Endpoint Security / アンチウイルス for OS X
ESET Endpoint アンチウイルス for Linux
ESET Server Security for Microsoft Windows Server
ESET Server Security for Linux

※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。）

ログの格納期間

ログの種類	データ保持期間
生ログ（検知の有無に関係なくEIに集められたすべてのログ）	7日間
検出ログ（EIの検知ルールによって検出されたログ）	31日間

3. セキュリティサービス概要図



セキュリティサービスには以下の２つのサービスが含まれます。

- XDRの**初期最適化（チューニング）**、**脅威モニタリング**を行う**「MDRサービス」**
- 各プログラムの利用を**24/365体制**で支援する**「プレミアムサポートサービス」**

4. MDRサービスについて

サービスカテゴリ	項目	内容例
XDRセキュリティサポート	EI：初期最適化（チューニング）	EI導入直後に発生する誤検知抑制のため、検知ルールや除外ルールの作成を行います。
	EI：検知ルールサポート	**特定の挙動を検知するためのルール作成・修正**等を支援します。
	EI：除外ルールサポート	**除外ルールの作成・修正**等を支援します。
	EI：セキュリティに関する一般的な質問	EIに関するお客様からの質問に対して検証・回答を行います。
	EI：脅威ハンティング（オンデマンド）	EIを用いてお客様環境を調査し、**潜在的な脅威・弱点に関するレポートや改善点のアドバイス**を行います。 ＊お客様からのご依頼をもとに実施します。
XDRセキュリティサービス(※)	EI：脅威モニタリング	日次でEIコンソールを監視し発生した**アラートを調査し重大度に応じてお客様に通知**します。
	EI：脅威ハンティング（プロアクティブ）	EIを用いてお客様環境を調査し、**潜在的な脅威・弱点に関するレポートや改善点のアドバイス**を行います。
インシデント調査・対応	基本的なファイル解析	お客様から提供されたファイルが**マルウェアであるかどうかの解析**を行います。
	詳細なファイル解析	お客様から提供されたファイルを解析し、**マルウェアの場合はファイルに関する詳細な情報を提供**します。
	デジタルフォレンジック分析	**インシデント後の調査支援**として、EIからの情報やメモリダンプ・レジストリ等の情報を解析し**レポートをご提供**します。
	デジタルフォレンジック・インシデントレスポンス支援	**現在進行中のインシデント**に対し、EIからの情報やメモリダンプ・レジストリ等の情報をもとに、**インシデント対応を支援**します。 ＊復旧等の対応はお客様ご自身でお願いいたします。
プロフェッショナルサービス(※)	デプロイメント＆アップグレード	ESETプログラムの**デプロイメントまたはアップグレード作業**を支援します。
エンドポイントセキュリティサポート	マルウェア対応：検出漏れ	ファイル/URL/ドメイン/IPアドレスを解析し、**マルウェアである場合は検出エンジンへの追加**などの対応を行います。
	マルウェア対応：駆除に関する問題	**マルウェアの駆除に問題がある場合にその解消**を行います。特殊なケースでは削除ツールをご提供する場合もあります。
	マルウェア対応：ランサムウェア感染	**ランサムウェア感染を調査**し緩和策と予防のための提案を行います。**復号が可能な場合は復号ツールをご提供**します。
	誤検知への対応	ファイル、URL、ドメイン、IPアドレスを解析し、**誤検知の場合は対応**を行います。
	一般：不審な挙動の調査	製品の不具合など上記に属さない不審な動作に対して、お客様から提供されたデータをもとに解決策をご提示します。

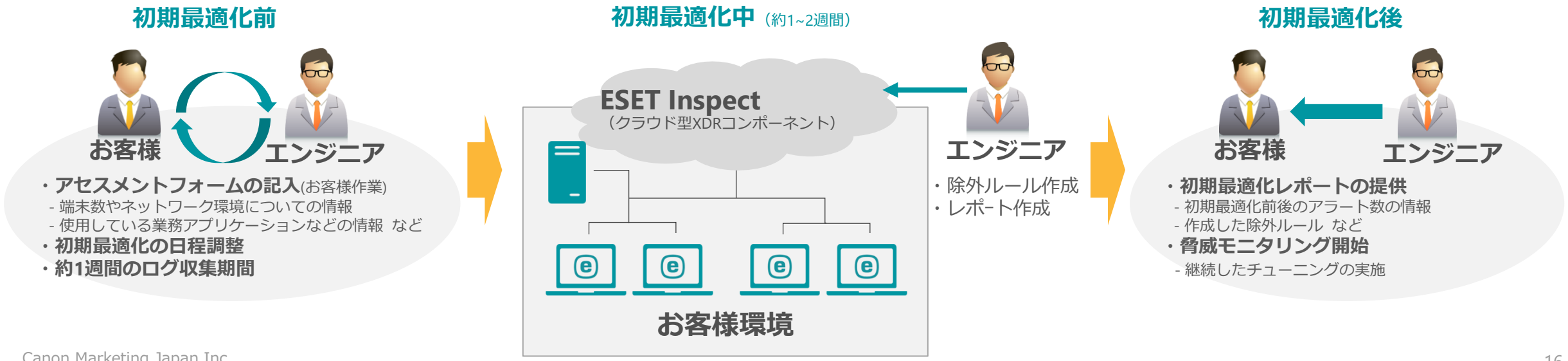
4. MDRサービスについて

XDRセキュリティサポート

EI：初期最適化（チューニング）

本サービスは、お客様に代わってEI導入後の初期最適化を実施します。（本サービスはEI導入時のみご利用いただけます。）
XDRはその製品の性質上、導入後に多くの誤検出のアラートが表示されます。そのため、お客様の通常業務で発生するアラートを検出から除外し、脅威発生時のアラートを見つけやすくするためのチューニングが必要です。
お客様に記入いただいたアセスメントフォームの情報をもとに、EIの自動除外作成機能(rule learning mode)や、エンジニアによる手動チューニングにより最適化を行います。（約1週間お客様環境のログを収集してから初期最適化を実施します。）
初期最適化後は、最適化前後のアラート数や、最適化によって作成された除外ルールなどをまとめた、初期最適化レポートをご提供します。

平日日中に実施する初期最適化の作業中、万が一インシデントを発見した場合はご担当者様へご連絡いたします。
※初期最適化は重大なアラートや優先度の高いアラートから実施しているため、インシデントの発見までに時間を要する場合がございます。



4. MDRサービスについて

XDRセキュリティサポート

EI：検知ルールサポート(※)
特定のマルウェアの挙動を検出するなど、EIの検知ルールの作成、変更、機能停止に関するサポートを行います。
EIの検知ルールや動作を分析し、お客様へのアドバイスや修正されたルールのご提供、必要に応じて開発者へのバク報告を行います。

EI：除外ルールサポート(※)
EIの除外ルールの作成、変更、機能停止に関するサポートを行います。
除外ルールを作成する対象のアプリケーションやその動作に関する情報をご提供いただく場合がございます。
また、除外を作成することがお客様環境のセキュリティに影響を及ぼす場合は、
お客様とご相談のうえ新たな解決策をご提示します。

EI：セキュリティに関する一般的な質問
EIセキュリティ関連の質問で、他のカテゴリに該当しないものに対し、指定された動作を分析します。
分析結果は、お客様へのアドバイスや開発者によるバグの改善に役立つ場合があります。

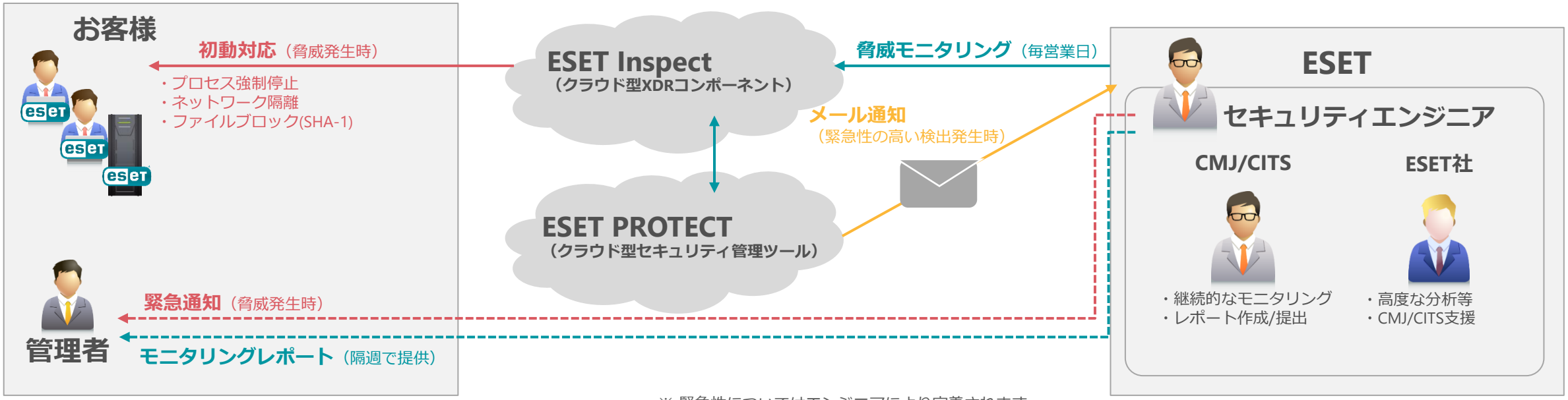
※ 脅威モニタリングの中で、必要な検知ルールや除外ルールはエンジニアが作成します。
※ 脅威モニタリング以外でのルール作成はお客様自身に実施いただきます。
お客様独自のルールを作成される場合はエンジニアにご相談ください。

4. MDRサービスについて

XDRセキュリティサービス

EI：脅威モニタリング

脅威モニタリングは、お客様のEIを継続的に監視するサービスです。
お客様のESET環境で緊急性の高い検出があった場合は、必要に応じて初動対応（プロセス強制停止、ネットワーク隔離、ファイルブロック）を行い、お客様へ緊急連絡を実施します。（エンジニアによる初動対応実施の要否については、予めお客様に同意いただいたうえで実施します。）
また、エンジニアはお客様の環境に定期的にアクセスし（毎営業日: 月~金）、疑わしい動作やアラートの分析を行い、継続的にEIを最適化（ルール設定等）します。
本サービスでは、定期的にモニタリング状況を把握いただくため、隔週でレポートをご提供します。



※ 緊急性についてはエンジニアにより定義されます。
緊急性が高い検出があった場合はエンジニアに通知され、エンジニアが内容を確認後にお客様にご連絡いたします。

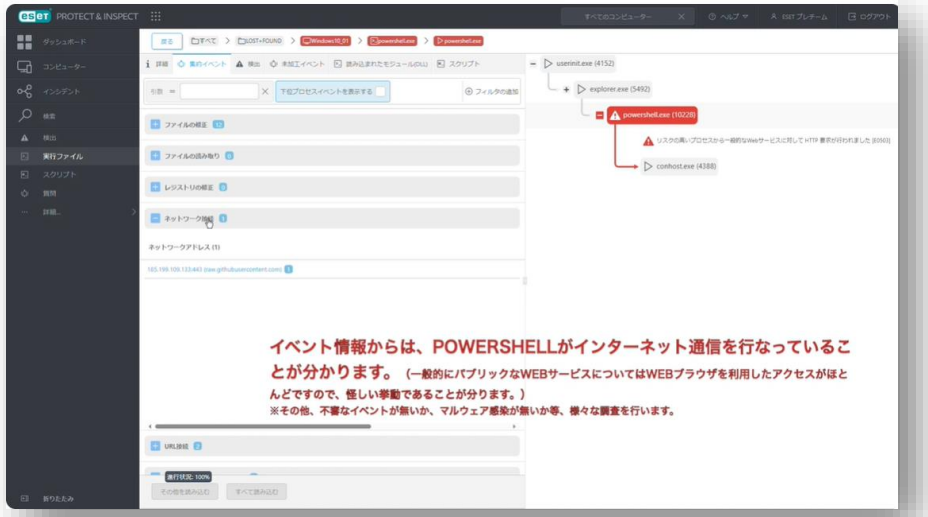
4. MDRサービスについて

XDRセキュリティサービス

EI：脅威モニタリング
動画にてご紹介しております。

【ESET Inspect】インシデントレスポンスデモ動画①
https://www.youtube.com/watch?v=KMIcfBqjYZU:

Emotetへの感染を模した検体を例に、 脅威の検出から調査、初動対応や影響範囲の調査などをご説明した動画です。



【ESET Inspect】インシデントレスポンスデモ動画②
https://www.youtube.com/watch?v=SGWKGa65v3o

永続化を狙ったサイバー攻撃による不正なユーザー作成を例に、 脅威の検出から調査、初動対応や影響範囲の調査などをご説明した動画です。

4. MDRサービスについて

XDRセキュリティサポート / XDRセキュリティサービス

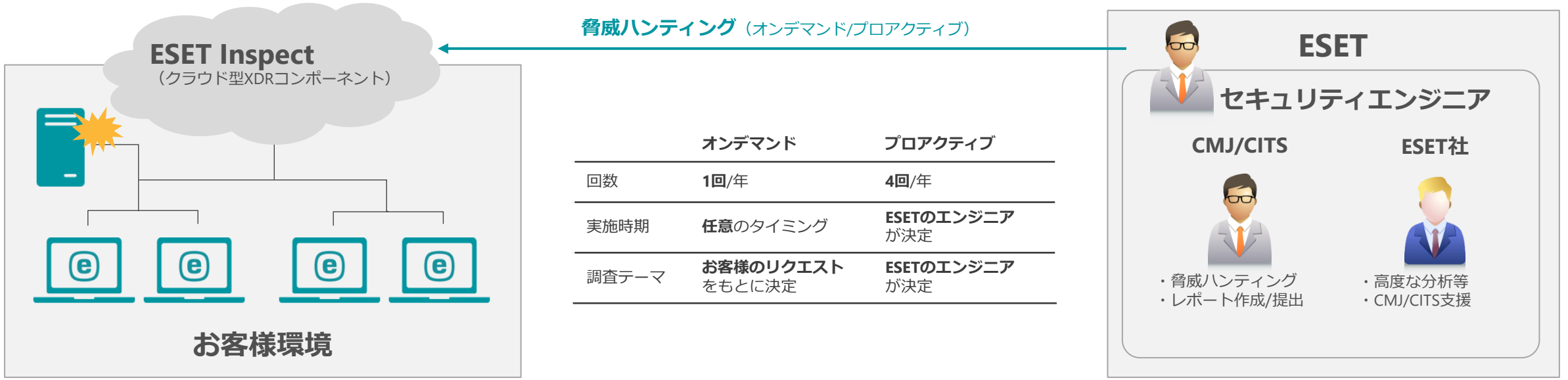
EI：脅威ハンティング（オンデマンド:任意のタイミングで年1回 / プロアクティブ:年4回）

脅威ハンティングはお客様環境の潜在的な脅威を調査する「事前対応型」のサービスです。
メニューは2種類あり、お客様が任意のテーマ、タイミングを指定できる「オンデマンド」と、
四半期に一度、ESET社により厳選された脅威トレンドをテーマにして実施する「プロアクティブ」があります。
いずれも、調査テーマに関連するイベントやアラートをエンジニアが調査・分析し、結果をレポートとして提出します。

※ エンジニアが新たにEIに検知ルールを追加する場合がございます。
※ 脅威が発見された場合はデジタルフォレンジック・インシデントレスポンス支援による対応支援を実施します。

◆調査例

“過去にドメインコントローラーを狙った攻撃の被害にあっているためドメインコントローラーを中心に調査してほしい”
“社内のセキュリティ訓練で疑似マルウェアメールを開いた社員が多かったため全社的にマルウェアが潜んでいないか調査してほしい”
“〇〇の脆弱性を狙った攻撃が流行しているので自社もそのような攻撃の被害に遭っていないか調査してほしい”



	オンデマンド	プロアクティブ
回数	**1回**/年	**4回**/年
実施時期	**任意**のタイミング	**ESETのエンジニア**が決定
調査テーマ	**お客様のリクエスト**をもとに決定	**ESETのエンジニア**が決定

4. MDRサービスについて

インシデント調査・対応

基本的なファイル解析(※)
お客様からご提出いただいたファイルを解析し、マルウェアであるかどうかの正誤判定を行いその結果をお伝えします。
解析のために、お客様には該当のファイルまたはハッシュ値(SHA-1/MD5)をご提出いただきます。

詳細なファイル解析(※)
お客様からご提出いただいたファイルを解析します。
マルウェアであるかどうかの正誤判定に加え、悪意のある場合はファイルに関する詳細な情報をレポートでご提供します。

デジタルフォレンジック分析
デジタルフォレンジックはインシデント発生後の調査です。
EIや、お客様に取得していただく(取得ツールはエンジニアから提供)端末情報(レジストリ、メモリダンプなど)をもとに分析を行います。
感染経路や影響範囲などの分析後はお客様に調査結果のレポートをご提供します。

デジタルフォレンジック・インシデントレスポンス支援
デジタルフォレンジック・インシデントレスポンス支援は、現在進行中のインシデントに対し、
お客様からご提出いただいく情報をもとに調査や対応を支援します。（復旧などの対応はお客様にご対応いただきます。）
本サービスはお客様へのコンサルティングや他サービスへのリダイレクトに繋がります。

※ ご依頼内容によってはESETのエンジニアの判断によりお受けできない場合がございます。

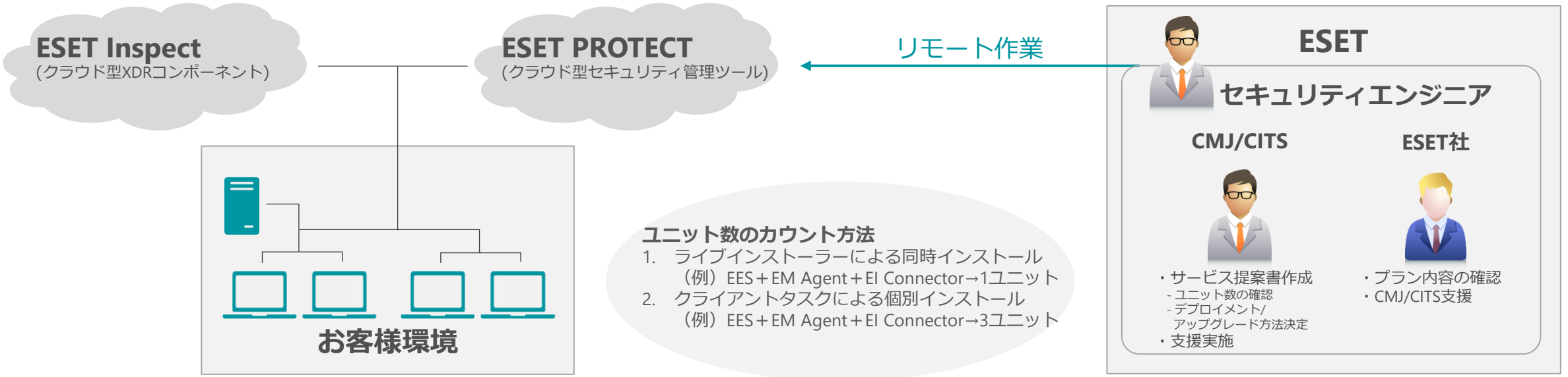
4. MDRサービスについて

プロフェッショナルサービス

デプロイメント&アップグレード

エンジニアがお客様の環境にリモートアクセスし、100ユニット分のESETプログラムのデプロイメントやアップグレードを支援します。お客様にはターゲットとなるプログラムやユニット数、対象範囲(EPのグループなど)、実施日などをアセスメントフォームに記入していただき、エンジニアがデプロイメント方法などを記載したサービス提案書を作成してお客様に提出します。
サービス提案書に沿って、エンジニアがインストーラーの作成から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。
支援後、実施内容を記載した書類にお客様の承認を頂くことで、本サービスは完了となります。

※ エンジニアがお客様端末でインストーラーを実行するため、お客様端末へのVPNアクセスなどをご用意いただく場合があります。
※ 本サービスにおけるユニット数とは、クライアントにインストールを行うプログラム、エージェント、コネクターの数量単位となります。
※ ポリシーによる設定はお客様にてご対応をお願いします。（EP/EIとの接続に必要なプロキシ設定は除く）



4. MDRサービスについて

エンドポイントセキュリティサポート

マルウェア対応：検出漏れ
EPPでの検出漏れが疑われるファイル、URL、ドメイン、IPアドレスを解析します。
悪意があると判断された場合、検出エンジンに追加され、マルウェアファミリーに関する情報をご提供します。

マルウェア対応：駆除に関する問題
マルウェアと検出されたが駆除できなかった場合、
お客様から提出いただいたファイルの駆除をテストし、問題がある場合は改善されます。
一部のケースでは、スタンドアロンの駆除ツールをご提供することもあります。

マルウェア対応：ランサムウェア感染
ランサムウェアへの感染が確認された場合、復号が可能な場合は復号ツール、
それ以外の場合は緩和策や予防策をご提供します。
解析のため、お客様からはランサムウェアによって暗号化されたファイルや、
ランサムウェアによって生成されたファイルなどをご提出いただきます。

誤検知への対応
ご提出いただいたファイル、URL、ドメイン、IPアドレスを解析し、誤検知と確認された場合は検出エンジンを修正します。
お客様には誤検知が疑われるソフトウェア名やベンダー名、利用目的などの情報も併せてご提出いただきます。

一般：不審な挙動の調査
エンドポイントセキュリティ関連の質問で、他のカテゴリに該当しないものに対し、指定された動作を分析します。
分析結果は、お客様へのアドバイスや開発者によるバグの改善に役立つ場合があります。

5. 各種レポートの紹介

初期最適化レポート

✓ レポート概要

初期最適化レポートには、チューニング前後の検出数や検出密度（件/日）、作成された除外についての情報が記載されます。
除外については、EIの除外ルールに記載された内容が記載されるため、どのようなイベントが検出から除外されるか確認できます。

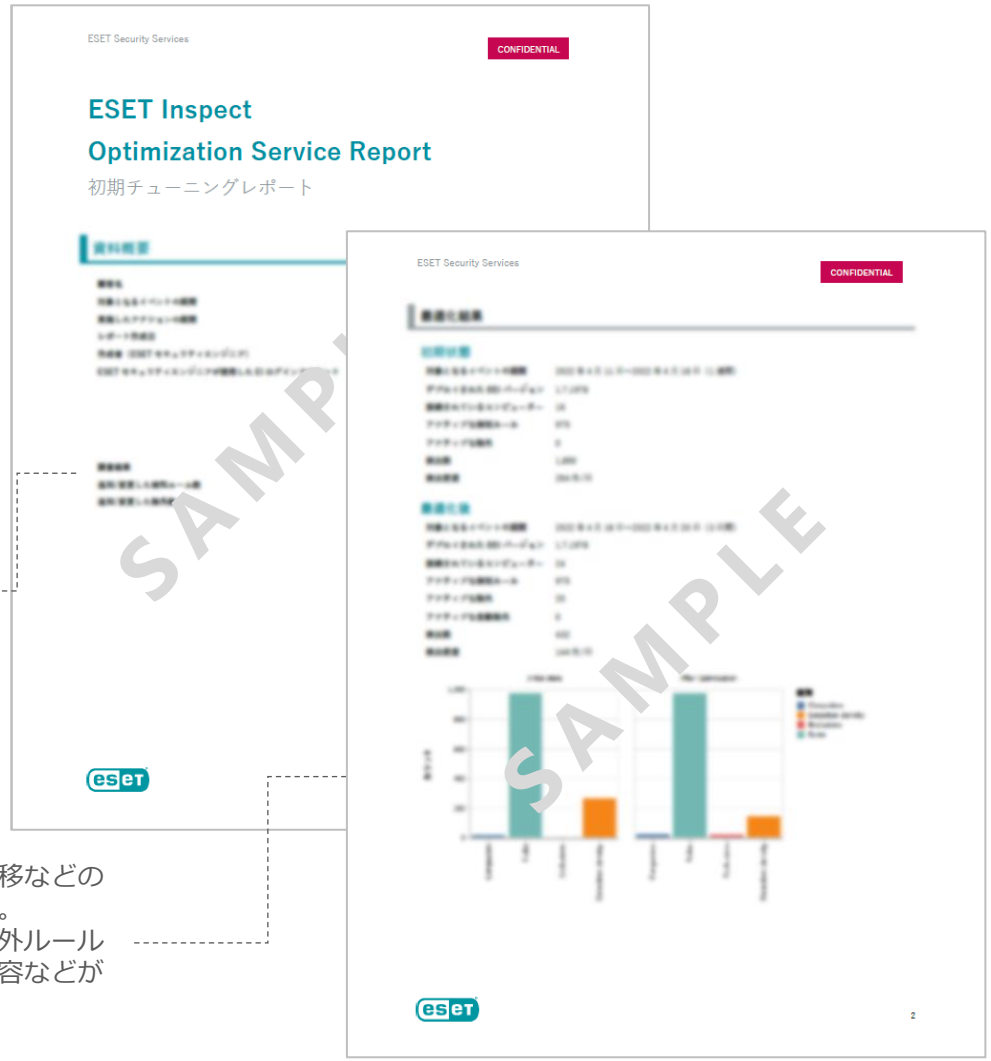
✓ 提供頻度

提供サービス… EI：初期最適化（チューニング）
提供タイミング…初期導入時の1回のみ

✓ 確認ポイント

エンジニアがどのような理由で除外ルールを作成したのかご確認いただくことができます。
また、アセスメントフォームにてお客様にヒアリングさせていただいたホワイトリストのアプリケーションが除外されているかもご確認ください。

※ 除外ルールはアセスメントフォームの情報を踏まえて作成いたします。



チューニングを実施した期間や、エンジニアにより作成された除外数などの情報が記載されます。

チューニング前後の検出数の推移などの情報はグラフにまとめられます。
レポート後半には作成された除外ルールについて、作成理由やルール内容などが記載されます。

※ 運用状況や調査内容によってレポートへの記載量は変動します。

5. 各種レポートの紹介

脅威モニタリングレポート

✓ レポート概要

脅威モニタリングレポートには、毎営業日（土日祝日は対応外）のモニタリングで作成された除外ルールや発見された検出、その検出に対する対応やお客様への提言などが記載されます。
脅威モニタリングレポートは隔週でのご提供となります。

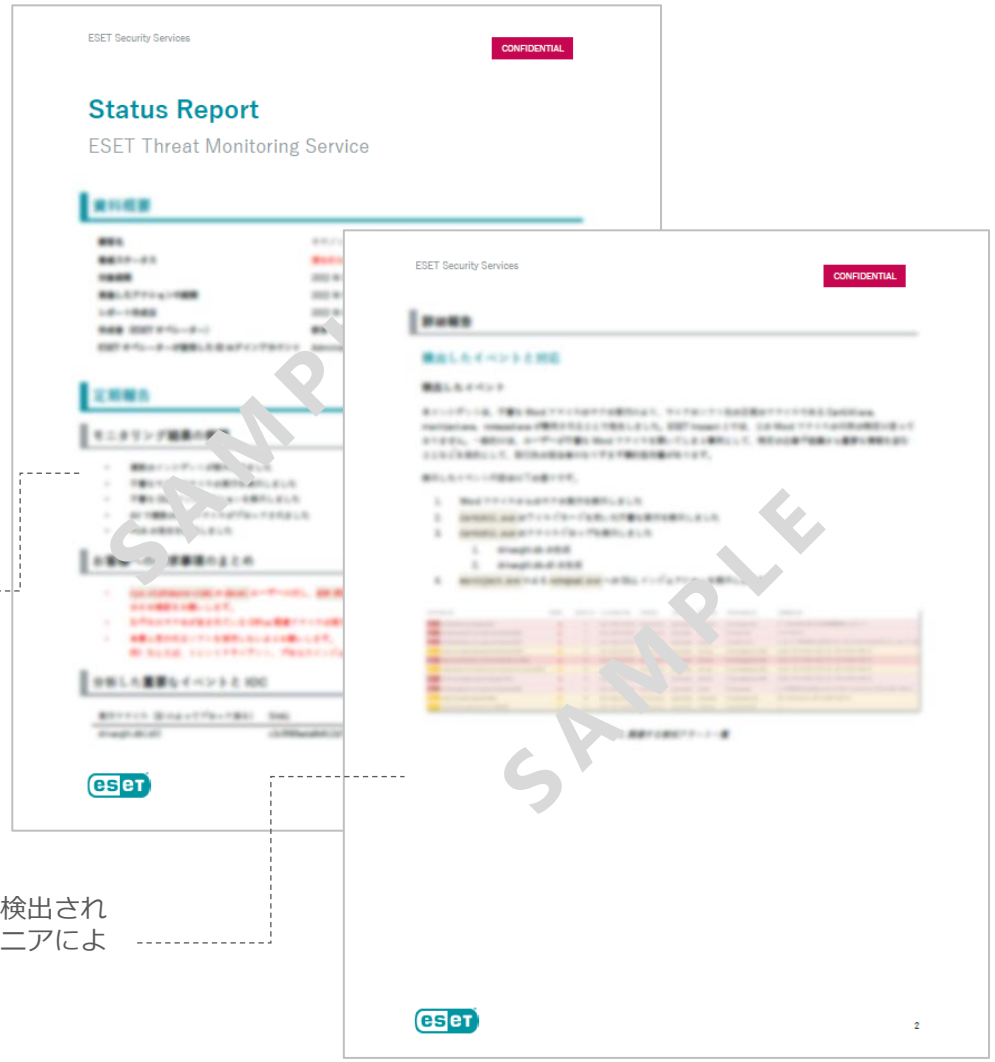
✓ 提供頻度

提供サービス… EI：脅威モニタリング
提供タイミング…隔週

✓ 確認ポイント

モニタリング時に発見された脅威に対するお客様への提言をご確認いただき、日々のセキュリティ対策にお役立てください。
また、本レポートをもとに、脅威発生時の初動対応に関するご相談をいただくことも可能です。

モニタリング期間に検出された脅威の概要やお客様への提言などが記載されます。
レポート内では、EPPでブロックされたマルウェアやPUA含め、検出された脅威の詳細情報が記載されます。



詳細報告として、お客様環境で検出されたイベントの調査内容とエンジニアによる対応内容が記載されます。

※ 運用状況や調査内容によってレポートへの記載量は変動します。

5. 各種レポートの紹介

脅威ハンティングレポート

✓ レポート概要

脅威ハンティングレポートには、お客様環境の潜在的な脅威をEIを使用して調査した結果が記載されます。
お客様の任意のタイミングでご利用いただける「オンデマンド」と、年4回ご利用いただける「プロアクティブ」がございます。

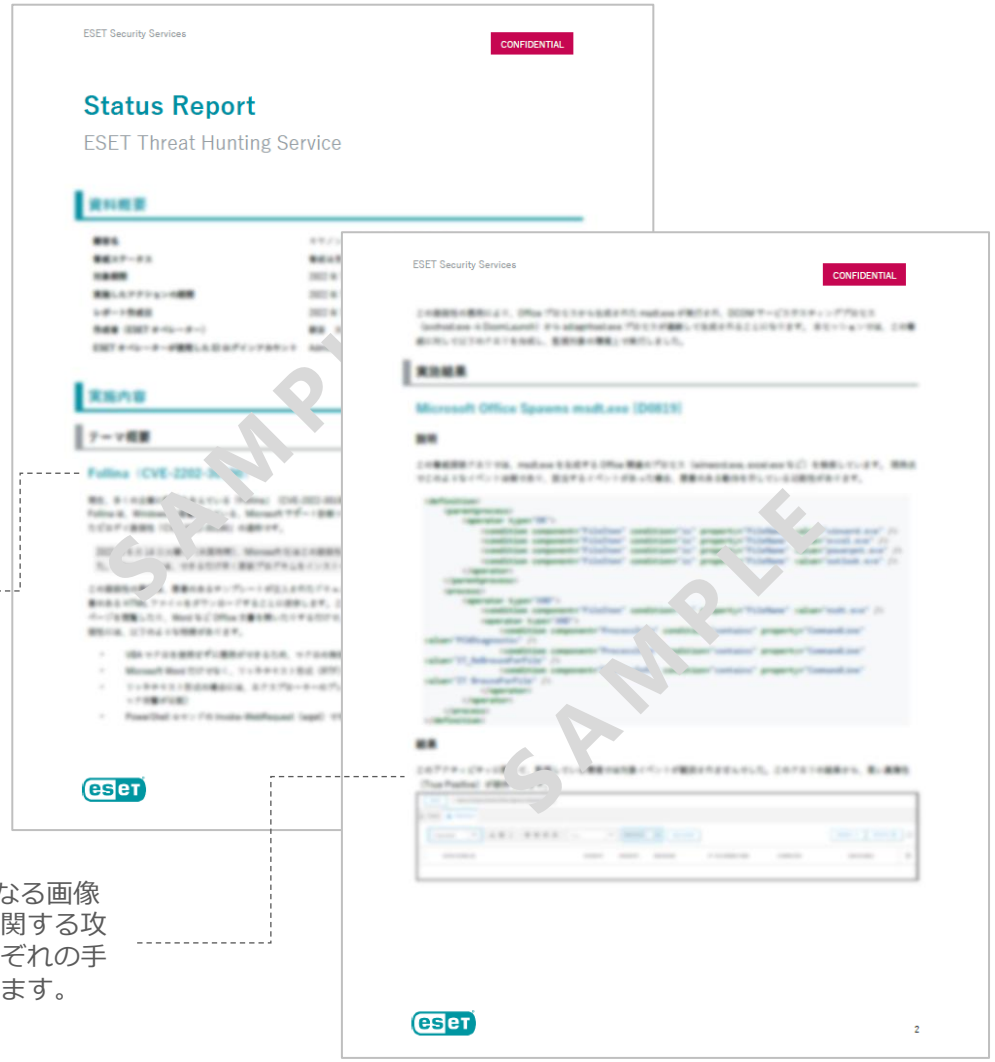
✓ 提供頻度

提供サービス…脅威ハンティング
提供タイミング…オンデマンド　:年1回
　　プロアクティブ　:年4回
※ オンデマンド: お客様の任意のタイミング
※ プロアクティブ: ESETのエンジニアによる タイミング

✓ 確認ポイント

エンジニアが選定する脅威ハンティングのテーマには、流行している脆弱性やお客様に注意していただきたい脅威などが選ばれます。
ハンティング結果をご確認いただくだけではなく、テーマとなった脆弱性に関する情報収集としてもご活用ください。

脅威ハンティングで調査したテーマについて、脆弱性の特徴や悪用された場合に想定される被害などの情報が記載されます。



EIを使用した調査結果が証跡となる画像と共に記載されます。テーマに関する攻撃手法が複数ある場合は、それぞれの手法に関する調査結果が記載されます。

※ 運用状況や調査内容によってレポートへの記載量は変動します。

5. 各種レポートの紹介

各種レポート概要

■ 詳細なファイル解析レポート

✓ **レポート概要**

詳細なファイル解析レポートには、お客様よりご提出いただいたファイルのマルウェアかどうかの正誤判定に加え、悪意のある場合はそのファイルに関する詳細な情報が記載されます。

✓ **提供頻度**

提供サービス…詳細なファイル解析
提供タイミング…本サービス利用時（任意のタイミング）

✓ **確認ポイント**

お客様環境で発見された脅威の詳細について、感染方法や挙動、想定される被害などをご確認いただき、社内での注意喚起や教育、報告にご活用ください。

■ フォレンジックレポート

✓ **レポート概要**

フォレンジックレポートには、インシデント発生後に行われたEIによる調査や、お客様に取得していただいたメモリダンプやレジストリ情報などの分析結果から、感染経路や影響範囲などの内容が記載されます。

✓ **提供頻度**

提供サービス…デジタルフォレンジック分析
提供タイミング…本サービス利用時（任意のタイミング）

✓ **確認ポイント**

被害を受けた原因や影響範囲などの情報から、脆弱性への対策や社内教育などのセキュリティ対策を見直し、再発防止にご活用ください。
また、インシデント時にデジタルフォレンジックが行える体制を整えることで、内部不正の抑止にも繋がります。

■ Suggestions & Recommendations文書

✓ **レポート概要**

Suggestions & Recommendations文書には、HealthCheck Serviceによって確認されたお客様への提言や推奨事項などが記載されます。

✓ **提供頻度**

提供サービス…HealthCheck Service
提供タイミング…本サービス利用時（任意のタイミング）

✓ **確認ポイント**

お客様のESET環境が正常稼働するための提言や推奨事項が記載されています。
定期スキャンや検出エンジンのアップデートが滞っている端末があった場合には、EP側からタスクを実行するなどの対応をご検討ください。

※ 運用状況や調査内容によってレポートへの記載量は変動します。

6. セキュリティサービスご利用時の注意事項

お客様に実施いただく必要がある作業

✓ 製品利用開始時の作業

セキュリティサービスの開始までに、**EBAの開設**から**ECとEIのアクティベーション**までを実施いただきます。

※ 詳細は本資料「Ⅲ. セキュリティサービスご利用の流れ」をご参照ください。

✓ エンジニア用 ESET PROTECT HUBのアカウント作成

エンジニアが脅威モニタリングなどでお客様のEIにアクセスするため、お客様に**エンジニア用のアカウントを作成**していただきます。

※ お客様にエンジニア用アカウントのメールアドレスをご用意いただきます。ご用意が難しい場合はエンジニアにご相談ください。
※ESET Business Account(EBA)のアカウントをすでにお持ちの場合はEBAにてエンジニア用アカウントを作成をいただきます。

✓ ESET Services Hubのアカウント開設

セキュリティサービスの問い合わせシステムである**ESET Services Hubのアカウントを作成**していただきます。

✓ 各種サービス利用時のアセスメントフォーム記入

一部のMDRサービスやHealthCheck Serviceのご利用時には、**アセスメントフォームにお客様情報を記入**のうえご提出していただきます。

✓ 脅威モニタリングで検知されたアラートへの対応

対応が必要と思われるアラートが確認されると、**お客様へ対応をご依頼する場合**がございます。

※ 脅威モニタリングレポートの内容をもとに、エンジニアによる初動対応の方針を検討することも可能です。

✓ 脅威モニタリング中に作成された除外ルールの有効化の判断

初期最適化完了後も、継続してEIの最適化を行います。
お客様にはエンジニアが作成した除外ルールの有効化を判断いただく場合があります。

✓ ログや検体の提出

セキュリティサービスご利用時のお問い合わせの際は、**お客様自身にログや検体を取得していただき、弊社にご提出**いただく場合があります。

※ エンジニアが提出必要と判断した場合、提出先URLをお知らせいたします。

※ エンジニア用アカウント作成手順やEP通知メール設定手順は、
エンジニアより提供させていただくアセスメントフォームに記載されています。

7. 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

「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。

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

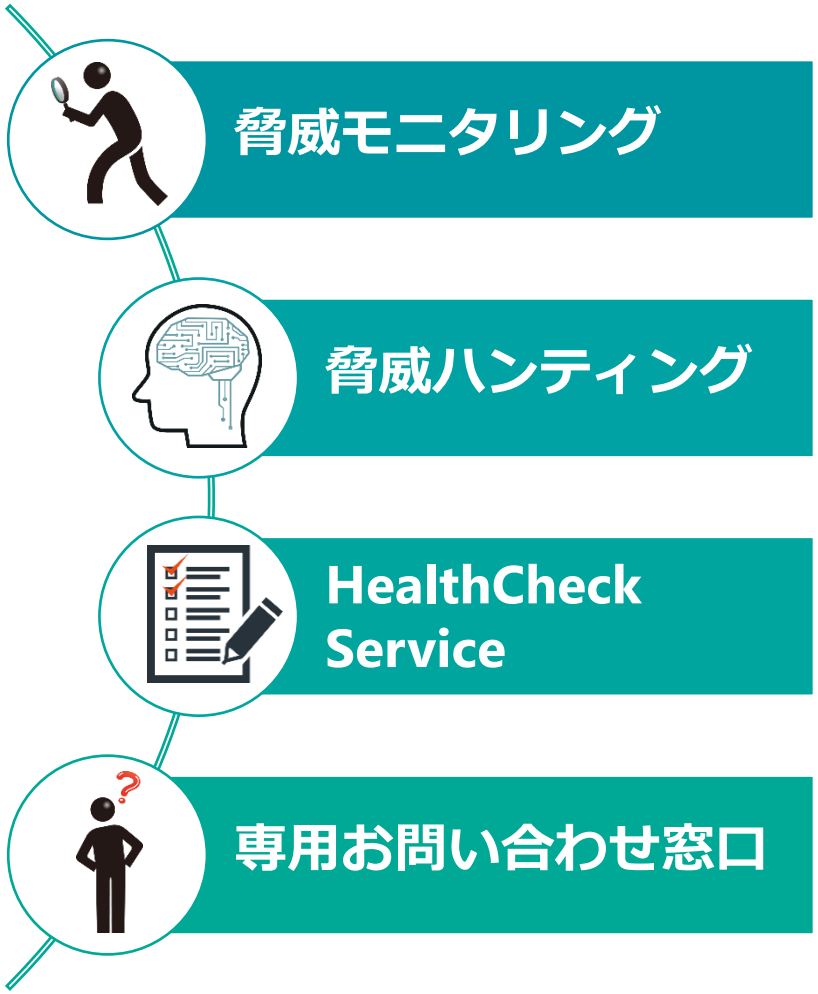
お客様環境にインストールされたESETの構成や設定を確認します。
本サービスはお客様の任意のタイミングでご利用可能です。

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）

8. 日々の運用イメージの紹介

運用フェーズで利用可能なサービス



提供されるサービス内容	必要なお客様作業 （チケット作成はServices Hubを利用）
• お客様EI環境の監視とチューニング • 緊急性の高いアラート発生時のご連絡 • 隔週でのモニタリングレポートの提供	• 緊急性の高いアラート発生時のセキュリティエンジニア側からの連絡への対応 （初動対応の確認やその後の対応などについて） • 脅威モニタリングレポートの確認
• プロアクティブでの実施（4回/年） • オンデマンドでの実施（1回/年） • 脅威ハンティングレポートの提供	• 脅威ハンティング利用時のチケット作成 • オンデマンドの脅威ハンティング利用時のテーマ選定 • 脅威ハンティングレポートの確認
• HealthCheck Service用アセスメントフォームの送付 • ヘルスチェックプランの作成と提供 • お客様ESET環境のヘルスチェック実施（1回/年） • Suggestions & Recommendations文書の作成	• HealthCheck Service利用時のチケット作成 • HealthCheck Service用アセスメントフォームの記入 • ヘルスチェックプランの確認 • Suggestions & Recommendations文書の確認

• お客様からのお問い合わせへの対応
  • エンドポイントセキュリティサポート
  • XDRセキュリティサポート
  • 基本的なファイル解析/詳細なファイル解析
  • デジタルフォレンジック分析
  • デジタルフォレンジック・インシデントレスポンス支援
	• チケット作成による各種お問い合わせ
	  • エンドポイントに関するお問い合わせ
	  • XDRに関するお問い合わせ
	  • 不審なファイル発見時のお問い合わせ
	  • インシデント発生時のログ取得やセキュリティエンジニア側とのやりとり

9. インシデント発生時の対応フロー

	お客様側	セキュリティサービスセンター側
ESET Inspect による検出	★お客様端末での検出発生★	1. サービスセンターのセキュリティエンジニアによる検出内容の確認
お客様への事象報告とネットワーク隔離許可	3. セキュリティサービスセンター側からの報告をもとに、NWからの端末隔離についての可否を判断 ※ 夜間・休日についての端末の自動隔離は別途打合せにて調整可能	脅威の場合 2. ご担当者様へ電話連絡し詳細をご報告 事象報告とネットワーク隔離等の初動対応の許可
端末の隔離と脅威の駆除		4. ESET Inspect を使用し該当端末をネットワークから隔離、端末内に潜む脅威を駆除
端末の隔離からの復旧		5. 対象端末のネットワーク隔離からの復旧 お客様への対応完了のご連絡
脅威モニタリングレポートの提出	7. 脅威モニタリングレポートのご確認	6. お客様環境で検知された脅威や作業内容、推奨対応、エンドポイント製品での検出内容などをまとめた脅威モニタリングレポートを提出

脅威未検出の場合

※ 事前にお客様とセキュリティサービスセンターで事前に対応内容を決めておくことで、端末の隔離まで完了してからのご報告も可能です。
※ 全ての事象が上記フローに該当することを保証するものではありません。

10. プレミアムサポートサービスについて

ESETプログラムに関する問合せ対応を行うサービスです。
サービス専用の窓口で、ESET社の教育を受けたメンバーが管理する窓口として対応を実施します。

項目	内容
24時間365日対応	24時間365日で対応します。
重大度レベルに応じた対応	対応までの人的初期レスポンス時間は重大度レベルに応じて定義されます。 重大度A：2時間　重大度B：4時間　重大度C：1実働日 ※ 重大度は最終的にESET社によって定義されます。
優先度を上げた対応	本サービスの問合せは、ESET社によって優先的に対応されます。
登録者制サポート	加入時にアセスメントフォームにより本サービスの担当者を登録していただきます。 サービス窓口では、登録いただいたご担当者の方からの問合せのみ受付ます。 また、緊急対応が必要な場合など、サービス窓口側からご連絡する場合があります。
サポート対象製品とプログラム	ESET PROTECT MDR製品で利用可能なプログラムが対象となります。 また、各プログラムのサポートポリシーはライフサイクルポリシーに準拠します。 https://eset-info.canon-its.jp/business/info/lifecycle-eol/
HealthCheck Service	年に1回、お客様の環境でESET製品が正常に利用されているかチェックを実施します。
デプロイメント＆アップグレード	エンジニアがお客様の環境にリモートアクセスし、 100ユニット分のESETプログラムのデプロイメントやアップグレードを支援します。 ※ 後述するMDRサービスでも本サービスは提供されます。詳細はP16をご参照ください。 ※ ESET PROTECT MDR Ultimateでは、プレミアムサポートサービスとMDRサービスの計2回分が利用可能です。

Severity Response Timeにおける重大度
・重大度A（重大）…本製品またはその主要機能が動作しないか、または本製品の使用に重大な影響を与える定期的/断続的な問題が発生している場合
・重大度B（深刻）…製品の機能に欠陥があるか、欠落しているか、または製品の使用を困難にする問題が発生しているが、使用できないわけではない場合
・重大度C（一般）…わずかなパフォーマンスの低下や、製品やドキュメントの修正を必要とするマイナーな問題がお客様に発生している場合

10. プレミアムサポートサービスについて

HealthCheck Service

HealthCheck Serviceは、お客様環境のESET製品が正常に動作しているか検査するサービスです。
お客様に記入いただいたアセスメントフォームをもとに、エンジニアが作成したヘルスチェックプランに沿って実施され、
改善策の提案などを記載したレポートをご提供します。

◆ヘルスチェックは以下のステップで実施されます。

1. アセスメントフォームの記入…お客様の環境に導入されているESET製品の情報や本サービスのスコープ(台数および範囲)を記入していただきます。
2. ヘルスチェックプランの作成…アセスメントフォームをもとに、ヘルスチェックの実施内容や作業予定日を決定します。
3. ヘルスチェックの実施…お客様のEPにアクセスし、アラートが表示されていないかなどの確認を行います。(※)
4. Suggestions & Recommendations文書の提供…ヘルスチェックの結果をもとにお客様へレポートをご提供します。

※ お客様のEPを操作し、ヘルスチェックに必要なタスクやレポートの作成を行う場合があります。

Ⅱ. その他の情報

1. EPとEIのバージョンアップについて

- **ESET PROTECT とESET Inspect のバージョンアップ**
  EPとEIのバージョンアップはESET社にて実施されるためお客様による作業は不要です。
  ※ バージョンアップの個別対応は不可となります。
- **ESET PROTECT のバージョンアップ作業に関して**
  EPのバージョンアップはESET社により段階的に行われ、バージョンアップ中は2~3分程度
  EPにアクセスできなくなります。
  EM Agentはログを溜め込む機能があるため、EPバージョンアップ後にEPにログ転送を再開します。
- **ESET Inspect のバージョンアップ作業に関して**
  EIのバージョンアップはESET社により段階的に行われ、バージョンアップ中は2~5分程度
  EIにアクセスできなくなります。
  EI Connectorはログを溜め込む機能があるため、EIバージョンアップ後にEIにログ転送を再開します。
- **ESET Management Agentのバージョンアップ**
  EM Agentは自動バージョンアップに対応しています。
  新しいバージョンのEM Agentがリリースされると、その2週間後から自動アップグレードがトリガーされます。
- **ESET Inspect Connectorのバージョンアップ**
  EI Connectorのバージョンアップはお客様自身で実施いただく必要がございます。
  EPのソフトウェアインストールタスクを利用してバージョンアップをお願いいたします。

2. サポート情報

- **弊社Webページにてサポート情報を記載しております。**
  ESET PROTECTソリューションシリーズ サポート情報(Q&A)
  https://eset-support.canon-its.jp/?site_domain=business
- **ESET PROTECTソリューションシリーズの**
  プラグラムおよびマニュアルはユーザーズサイトにてご提供しております。
  ESET PROTECTソリューション ユーザーズサイト
  https://canon-its.jp/product/eset/users/index.html
- **以下の各種オンラインヘルプもご確認ください。**
  ESET PROTECT のオンラインヘルプ
  https://help.eset.com/protect_cloud/ja-JP/

  ESET Inspect のオンラインヘルプ
  https://help.eset.com/ei_cloud/ja-JP/