クラウドサンドボックス

ESET LiveGuard Advanced

機能紹介資料

第27版

2025年2月

Canon

キヤノンマーケティングジャパン株式会社





- 1. はじめに (本資料について)
- 2. ESET LiveGuard Advanced(ELGA)とは (1)ELGAとは? (2)特長
 - (3)導入の効果
- ESET LiveGuard Advancedの構成 (1)動作環境 (2)コンポーネント
- 4. ELGAの機能紹介
 - (1)エンドポイントプログラムの主な設定
 (2)プロアクティブ保護機能
 (3)送信したサンプルファイルの一覧
 (4)送信したサンプルファイルの詳細
 (5)分析結果のレポート
 (6)テレワークへの対応について
- 5. ELGAの有効化手順
 - (1)アクティベーションタスクの実行
 - プラットフォームモジュールから実行する場合
 - タスクから実行する場合
 - (2) ELGA機能の有効化
- 6. 参考情報
- 7. マルウェアの検出事例
 - (1)解析の迅速性
 - (2)高度な解析技術

1. はじめに(本資料について)



本資料はクラウドサンドボックス「ESET LiveGuard Advanced」の機能を紹介した資料です。

- ESET LiveGuard Advancedを利用いただくには、オンプレミス型セキュリティ管理ツールであるESET PROTECT on-prem V9以降、 またはクラウド型セキュリティ管理ツールであるESET PROTECT(※EP)での管理が必要です。
- ESET LiveGuard Advancedにて作成できる動作レポートですが、XDRソリューション(ESET Inspect または ESET Inspect onprem)の利用可否により、異なりますのでご注意ください。詳細は本資料のP12-13を確認ください。
- 本資料で使用している画面イメージは使用するOSにより異なる場合があります。また、今後画面イメージや文言が変更される可能性があります。
- ESET PROTECTソリューションではクライアントOSおよびサーバーOSの端末に導入する プログラムとしてWindows、Mac、Linux、 Android OS向けプログラムをご使用いただけます。また、上記のプログラムを管理するセキュリティ管理ツールをご使用いただけます。各プロ グラムの機能紹介は別資料でご用意しています。
- Windows, Windows Serverは、米国Microsoft Corporationの、米国、日本およびその他の国における登録商標または商標です。
- ESET LiveGuard Advancedの導入方法は以下を参照ください。
 https://eset-info.canon-its.jp/files/user/pdf/manual/guide_edtd.pdf





(1) ELGAとは?

ゼロデイ攻撃に用いられるような未知の高度なマルウェアに対する検出・防御の即時性を高めるクラウドサンドボックスです。 エンドポイント(クライアント)プログラムが不審なファイル(サンプル)を発見すると、クラウド上の解析環境であるESET Cloudへ自動送信 (手動も可)を行い、解析を依頼します。ESET CloudではESETの最新テクノロジーを用いた多段階での分析が行われます。解析結果 はセキュリティ管理ツールより、レポートで確認できます。

悪質と判断されたファイルに対しては、エンドポイントで駆除、ブロックなどの防御処理を全社レベルで自動的に行います。







(2) 特長

①未知の脅威を自動解析、自動防御

不審なサンプルをクラウドベースの解析環境「ESET Cloud」へ自動で送信、大半のサンプルは数分内で解析でき、悪質と判断したファイルは 全社レベルで自動的にブロックします。

②最新テクノロジーによる解析

「ESET Cloud」での分析には、3つの機械学習モデルを用いたサンプル比較、サンドボックスによるシミュレーション、最新のスキャンエンジンによる異常分析など、ESETの最新テクノロジーが用いられています。

③解析結果のレポート

サンプルの解析結果はセキュリティ管理ツールである「ESET PROTECT」または「ESET PROTECT on-prem」より閲覧可能です。悪質な ものであるかどうかの判断や、サンドボックスシミュレーションで観察された挙動などを把握できます。





(3) 導入の効果

①ゼロデイ攻撃に速やかに対処したい

未知の脅威をクラウド上で自動解析し大半のサンプルは数分内に自動で駆除します。

②ESETの保護機能を手軽に強化したい

ESET PROTECTソリューションを既に使用しており、セキュリティ管理ツールでエンドポイントの管理を行っていれば、ライセンスを追加して機能を有効にすることで追加のエージェント不要で未知の脅威に対する対策を強化できます。

③サンドボックス機能を手軽に構築したい

セキュリティ管理ツールで管理を行っていれば、ハードウェアとエージェント不要で手軽かつ安価にサンドボックス環境を実装できます。

3. ESET LiveGuard Advancedの構成

(1) 動作環境

ESET LiveGuard Advancedの利用にあたっては、以下の環境が必要です。

①セキュリティ管理ツールが構築されていること

②セキュリティ管理ツールでエンドポイントの管理が行われていること

③セキュリティ管理ツールとエンドポイントがインターネットに接続されていること

④エンドポイントにはELGAに対応したプログラムが導入されていること
 対応プログラムは下記ページの[動作環境]よりご確認ください
 https://canon.jp/business/solution/it-sec/lineup/eset/feature/cloud-sandbox

※EESM V8を管理される場合、クラウド型セキュリティ管理ツールをご利用ください。 オンプレミス型セキュリティ管理ツールでは、ELGAをご利用いただけません。(2024年12月現在)



3. ESET LiveGuard Advancedの構成



(2) コンポーネント

ESET LiveGuard Advancedは以下のコンポーネントから構成されています。



コンポーネント	
Webコンソール	管理者がセキュリティ管理ツールにログインして、分析情報やクライアントの情報を確認
EMエージェント	アップロードしたサンプルのリストをセキュリティ管理ツールに送信。Webコンソールから実施した設定変更や タスクの実行をESETクライアントプログラムに送信
ESETクライアントプログラム	サンプルのアップロード。分析情報の確認、悪質なファイルのブロック
セキュリティ管理ツール (ESET PROTECTまたはESET PROTECT on-prem)	分析結果の確認、管理端末へのタスクやポリシーの配布に使用
ESET Cloud	サンドボックス技術などでサンプルの分析(ライセンス毎に分離された環境)

©Canon Marketing Japan Inc.



(1) エンドポイントプログラムの主な設定

サンプルの送信内容及び、分析で脅威と検出された場合の動作を指定します。

設定項目	内容
検出しきい値	分析結果に対して脅威として処理を行う際のしきい値を選択。 しきい値は「不審」、「非常に不審」、「悪意」の3段階より選択。
検出後のアクション	検出しきい値以上の脅威が検出された場合のアクションを選択。 「実行中の処理を停止して駆除」、「次回アクセス時に駆除」より選択。
不審なサンプルの自動送信	実行ファイル、アーカイブ、スクリプト、その他、考えられる迷惑メール、文書より選択。
サンプルの最大サイズ(MB)	1~64MBより指定。
ESETのサーバーから実行ファイル、アーカイブ、スクリプト、 他のサンプル、および可能性がある迷惑メールを削除	送信したサンプルをESETのサーバーから削除するタイミングを設定。 追加しない(※ESETのサーバーから削除しない)、30日後、分析後即時より選択。
除外	特定のファイルおよびフォルダをサンプルの送信対象から除外が可能。

エンドポイントプログラム(ESET Endpoint Security V11)の設定画面



※本設定はエンドポイント毎に設定を行います。設定はセキュリティ管理ツールのポリシーを使用することでグループ毎または全台に一括で適用することができます。 ※EEALはセキュリティ管理ツールのポリシーでのみ設定可能です。



(2) プロアクティブ保護機能

メールまたはブラウザ経由でダウンロードされたファイルに関しては、分析結果が受信できるまで実行を保留させることができます。

設定項目	内容
分析結果の最大待機時間(分)	ESET Cloudの分析結果を受信するまでファイルの実行を待機させる最大待機時間を設定。 5分~60分より指定。
プロアクティブ保護	メールまたはブラウザ経由でダウンロードされたファイルの実行を、ESET Cloudの分析結果が 確認できるまで保留することが可能。 「実行をただちに許可する」、「分析結果を受信するまで実行をブロックする」より選択。

分析中のポップアップ画面	エンドポー	イントプログラム(ESET Endpoint Securi	ty V11)の設定画面	
(INDEPOINT SECURITY V X	ESET LiveGuard			5
1 ファイルを分析中です	検出しきい値	フロアクティフ保護機能により、分析中に端末 が不審なサンプルにアクセスし	非常に不審 ~	0
cmd.exeはマルウェアの分析中であるファイル(eicar.bat)にア クセスレよっとしました。これに仕数分かかる場合があります。	検出後のアクション	感染することを防ぎます。	実行中の処理を停止して駆除 ~	
ファイルの準備が完了したら、通知されます。	プロアクティブ保護		分析結果を受信するまで実行をブロック ~	0
このメッセージの詳細を見る	分析結果の最大待機時間(分)	5	0

本機能の詳細は下記をご確認ください。 https://help.eset.com/elga/ja-JP/proactive protection.html



(3) 送信したサンプルファイルの一覧

セキュリティ管理ツールより、クライアントが送付したファイルの一覧及び分析情報を確認することができます。 並べ替え、ステータス・状態毎の表示、フィルタで特定の値のみを抽出して表示できます。





(4) 送信したサンプルファイルの詳細

セキュリティ管理ツールよりクライアントが送付したサンプルファイルの詳細情報を確認することができます。

ese	🗊 PROTECT 🛛 ∷	(1) P 入力すると検索を開始 ⑦ ワイックリンクマ ⑦ ヘルプマ 冬 ESET プレチーム ∃ ログアウト
	検出 送信されたファイル	< 戻る 送信されたファイル 〉 - ファイルの詳細
8 A 99+	BADF 隔離 コンビューター	
*	コンピュータユーザー 動的グループテンプレート	ステータス ▲ 状況悪意 コンビューター 状態 ② 完了 ユーザー
ľ٤ ه	ライセンス ライセンス管理	前回処理日 2023年12月14日 14:55:11 理由 自動 送信日 2023年12月14日 14:53:15 送信先 ESET LiveGuard 学動を表示で パッシュ FBRCF64AA7F6C6A721CFBD02D40183FFFBERD856
ŭ ©	アクセス権 ユ ーザー	● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●
ф 17 п.	権限セット	ク分析 マさます。
9 ⁶	アクティビティ監査 監査ログ	txe ② 完了
··· >	管理 設定	送信日 2023年12月14日 14:53:15
		の分析 シンジンナードションドロ (4/33)・11
	● 閉じる	開じる



(5) 解析結果のレポート(1/2)

セキュリティ管理ツールよりサンプルの解析結果のレポートを閲覧できます。状態より悪意があるかの判断、検出された挙動や特徴よりサンド ボックスシミュレーションで観察された挙動などを把握できます。サンプルファイルによっては複数の挙動が含まれる場合があります。 ※本画像はXDRソリューションが利用できない環境のレポート画面となります。XDRソリューションが利用できる環境は表示できるレポート画面異なります。詳細は次のページを確認ください。

ファイルの挙動分析レポート例 (ESET Inspect が利用できない環境の場合)

マルウェア SUB3 33355555553557557563257958664251454	ンプルのハッシュ値などが 建認できます。	常期的な構成エンラン サンプルは、本地的ルローザーデバイスに非可にない、他から高心のみ お桁小心的はが影響される、「anuflows or densids」 CMA されま ド、 サンプルは感染していません
カテゴリ その地 j度な検査エンジン		
高度な解凍と検査 サンプルは静的分析と最先端の解凍が実行され、強化され た骨成データペースに対して担合されます。 サンプルは悪意があります。	· · · · · · · · · · · · · · · · · · ·	マルウェアロ素行せずに増出されました サンプルは実行せずに使出されました。
高度な機械学習検出 i 静的および動的分析は、深層学習を含む機械学習アルゴリ ズムを使用して実行されます。		あたたらも時代のM マルウェアは支付けていたには接合エンジンによって統治されました。 正当な時代の例 マルウェアに感染していないアプリケーションは過点にの総合を行いま ぜん。



(5) 解析結果のレポート(2/2)

本画像はXDRソリューションが利用可能な環境のレポート画面となります。XDRソリューションが利用できない場合は表示できるレポート 画面が異なります。詳細は前のページを確認ください。

オペアのプロセス

7° 827

操作

APIログ

ファイルの挙動分析レポート例 (XDRソリューションが利用可能な環境の場合)

	40 <u>* ЮКФダウンロード</u> 995EC2FE2A2C4538AABF651FD0F	プロセスの作成 POWERSHELLEXE (6184) *C\Windows/system32\WindowsPowerShell.exe* *C\Users\Administrator\Desktop\ <sample>* プロセス 1 プロセス 1 プロセス 1 プロレス 1</sample>
ファイル あからF34.88からF32.88からF32.88からF34.50t アルイス あからF34.88からF32.88からF34.50t SHA-1 1990560CE1F387580D1617002579866405*14140 の SHA-256 2754.001189F56486210-4719897D880166856055E25F28.82468588A8F651FD カデゴリ スクリプト サイズ G8	サンドボックス 前日 詳細 レプリケーションは実行されませんでした。	Ciller(Administrator/AppData)Local(Temp_ASScriptPolicy Ciller(Administrator/AppData)Local(Temp_ASScriptPolicy Ciller(Administrator/AppData)Local(Temp_ASScriptPolicy Ciller(Administrator/AppData)Local(Temp_ASScriptPolicy Ciller(Administrator/AppData)Local(Temp_ASScriptPolicy Ciller(Administrator/AppData)Local(Temp_ASScriptPolicy Ciller(Administrator/AppData)Local(Temp_ASScriptPolicy Ciller(Administrator/AppData)Local(Temp_ASScriptPolicy Ciller(Administrator/AppData)Local(Temp_ASScriptPolicy Ciller(Administrator/AppData)Local(Temp_ASScriptPolicy Ciller(Administrator/AppData)Local(Temp_ASScriptPolicy Ciller(Administrator/AppData)Local(Temp_ASScriptPolicy Ciller(Administrator/AppData)Local(Temp_ASScriptPolicy Ciller(Administrator/AppData)Local(Temp_ASScriptPolicy Ciller(Administrator/AppData)Local(Temp_ASScriptPolicy Ciller(Administrator)Ciller(Ciller(Ciller)) Ciller(Administrator)Ciller(Ciller) Ciller(Administrator)Ciller(Ciller) Ciller(Administrator)Ciller(Ciller) Ciller(Administrator)Ciller(Ciller) Ciller(Administrator)Ciller(Ciller) Ciller(Administrator)Ciller(Ciller) Ciller(Administrator)Ciller(Ciller) Ciller(Administrator)Ciller(Ciller) Ciller(Administrator)Ciller(Ciller) Ciller(Administrator)Ciller(Ciller) Ciller(Administrator)Ciller(Ciller) Ciller(Administrator)Ciller(Ciller) Ciller(Cill
MTされた動作 1 株当 詳細 マルウェアは実行せずに検出されました サンプルは実行せずにマル Elcar test file	理由の件数 ウェアとして検出されました。 1 へ	KOLAHREKON KOLAHREKON K KOL



(6) テレワークへの対応について

インターネットに接続できればESET Cloudへ不審なサンプルを送信できるため、外出時やテレワーク時も全社レベルで端末を保護することが 可能です。クラウド型セキュリティ管理ツール「ESET PROTECT」を利用するなど、クライアント端末とセキュリティ管理ツールが通信できる場 合は、管理者はESET Cloudに送信されたファイル情報や解析結果を社外からも確認することができます。





(1) アクティベーションタスクの実行 – プラットフォームモジュールから実行する場合 -

ELGAをご利用いただくためにアクティベーションの実施が必要です。以下のいずれかで実施ください。 ・「プラットフォームモジュール」から実行する場合(本手順) ・タスクから実行する場合(p16~20)

 ESET PROTECTメインメニューの[プラットフォームモジュール]を 選択し、ESET LiveGuard Advancedの[有効]をクリックします。

ese	🗊 PROTECT ∷	🏟 🔎 入力すると検索を開始	⑦ び クイックリンク マ			
		プラットフォームモジュール				
" " G						
A		ESET LiveGuard Advanced ゼロデイ保護				0 0
**		クラウドサンドボックスは、不審なプログラムが実行されて、その動作が自動的に戦際、分析、および		● 有効	74	
		報告される、隔離された強力なテスト環境を提供します。これは、ランサムウェアを含むゼロディ脅威 に対して特に便利です。	74	● 有効化中	0	
ž		有効 詳細を見る	74	● 削除中	0	
۹				● まだ有効では	ありません 128	
ä		セキュリティ製品をアップデートし、その他のコンピューターでESET LiveGuard Advanced 更新 を使用				
٢						
φ 1 .						
е (,	ステータス概要 プラットフォームモジュール	ESET Full Disk Encryption				0 🕸
	詳細 >			● 有効	0	
		に対応するために組織のデータセキュリティを高めます。		● 有効化中	6	
		有効詳細を見る		● 削除中	0	
		1 2台の推興コンピューターで有効にする 有効		● まだ有効では	ありません 16	
	フィードバックを送信					

 ② 設定とターゲット(ELGAを有効化するデバイス)を選択し、 [有効]をクリックします。

Γ	ESET LiveGuard Advancedを有効にする ×
	ESET LiveGuard Advancedを有効にするコンピューターを選択 します。ライセンスとポリシーは自動的に割り当てられます。 正規ライセンスがない場合は、試用ライセンスが使用されま す。 ライセンスの選択方法 ^③
	 最適な保護 推奨 マクロをサポートするドキュメントタイプを含む危険なファイルは、自動検査と動作分析のために安全なESETサーバーに送信されます。ファイルへのアクセスは、安全だと評価されるまで制限されます。ESET LiveGrid®フィードバックシステムが有効になります。 基本保護 これにより、基本的なレベルのセキュリティが提供されます。このセキュリティレベルでは、制限されたファイルのセットのみが検査されます。#EBET LiveGrid®フィードバックシステムが有効になります。
•	'ターゲット すべてのデバイス×
	▼ 新しいデバイスで常に有効にする
	有効キャンセル



(1) アクティベーションタスクの実行 – タスクから実行する場合 (1/5) -

① ESET PROTECTメインメニューの[タスク]-[新規作成]-[クライアントタスク]をクリックします。 ② [名前]欄に任意のタスク名を入力します。[タスク]欄では
 「製品のアクティベーション」を選択し、[続行]をクリックします。

63 0	T PROTECT			ዖ እታታቆሪ	検索を開始	イックリンクマ	◎ ヘルプマ	G 0/	リアウト
		タスク	:	● ▷ ⊙ ✓	アクセスグループ 選択 會	む 製品のアク	(232) <i>91</i> . V	◎ フィルタの追加	00
~		タスクタイプ	p	名前		97	進行状況	タイプ	0
* 🔺 ***		0) 隠離ファイルのアップロード 1) 隠離管理	^	製品のア 新規タス	"クティベーション - ESET絶弱性 ペク	とパッ	©(製品のアクティベ・ 製品のアクティベ・	-シ_ -シ_
0		D 診断 D 製品のアクティベーション	ĺ	 新規タス 新規タス 	19 19			製品のアクティベー 製品のアクティベー	-シ
20 00	9 7 0	 2 製品のアップデートの確認 2 胞弱性検査 	Ĭ	 新規タス 	10		v 1	製品のアクティベー	->
0		へ DD ESET PROTECT DD Rogue Detection Sensorデータベー		新規タス ELGA有効	() MC		G 5 23	製品のアクティベー 製品のアクティベー	-9
• •		© エーシェントのアップクレード © クローンされたエージェントのリ	¥	EIアクテ EIアクテ EIアクテ	ィベーション ィベーション			製品のアクティベ・ 製品のアクティベ・	-シ -シ
9947 17		99	۹ •	 製品のア 新規タス 	?クティベーション (絶弱性とパッ ?ク	/チ管		製品のアクティベ・ 製品のアクティベ・	-シ -シ
			ľ	ElConnec	ctorアクティベーション			製品のアクティベー	-シ >.
_			ł	+ 25472219	22		× 1	製品のアクティベー	->
8	新りたたみ		+	+ サーバータスク 新規作成。*	アクション *			N (0)	100

*	名前
定	ELGAアクティベーション
20-	99
	タワを選択
	說明
	タスク分類
	すべてのタスク >
	920
	製品のアクティベーション >



(1) アクティベーションタスクの実行 – タスクから実行する場合 (2/5) -

③ [ESETライセンス]の下のライセンスをクリックします。

 ④ 「ESET LiveGuard Advanced for Endpoint Security + Server Security」を選択し、[OK]をクリッ クします。

基本	製品のアクティベーション設定	
設定	ESETライセンス ①	
989-		

ライセンスを選択して	てくださ	<u>م</u>	×
9Ø	م	● ●	0
		△ 連絡先 製品名 ◎	1
		ESET LIVEGUARD Advanced for Endpoint Security + Server Security	
		ESET Endpoint Security + ESET Server Security	
		ESET Mail Security	
		ESET Full Disk Encryption	
		ESET Vulnerability & Patch Management	
		ESET Mobile Threat Defense	
		ESET LiveGuard Advanced for Mail Security	
		ESET Full Disk Encryption	
		ESET Endpoint Security + ESET Server Security	
		ESET Inspect	4
		ESET LiveGuard Advanced for Endpoint Security + Server Security	
		OK キャンセル	,]



(1) アクティベーションタスクの実行 – タスクから実行する場合 (3/5) -

⑤ [終了]をクリックします。

⑥ [トリガーの作成]をクリックします。

基本	製品のアクティベーション設定
82	ESETライセンス ①
サマリー	





(1) アクティベーションタスクの実行 – タスクから実行する場合 (4/5) -

⑦ [対象]-[ターゲットの追加]をクリックします。

⑧ アクティベーション対象のPC、またはグループを選択し、[OK]をクリックします。

新しいトリガーの追加			保存先の設定						×
タスク > 新しいトリガー説明の.	λ,ŋ		グループ	$P \otimes \otimes$	▲ ● ✓ ○	タグ マ	フィルタの追加	プリセッ	v ト マ
■本 ▲ 対象 トリガー 注明の支 - 調整	ターグットの総計 ターグットの総計 ▲ 使用できるデータがありません	•	 ▲ ロ すべて (257) ◇ 通 会社 (0) △ Android (1) △ Computers (0) ○ ESET Inspect Cloud (0) ◇ └ LOST+FOUND (169) ◇ └ maeda_test (1) □ m-test (1) 	Î	□ コンピューター名 □ □ □ □ □	<i>91</i> a	ス. ミ. ♥ ● ● ● ▲ ● ▲ ●	モ . 更新 更新 更新 更新	 ✓ 前回の接続 ※ 2024年8月19日 18-27 2024年8月19日 16-27 2024年8月19日 10:11 2024年8月19日 10:11 2024年8月6日 20:11 2024年8月1日 14:1
			 □ OJTグルーブ (0) □ tasaki (6) ターグット名 		ターゲット説明		ターゲットタイプ コンピューター		
	R5 87 9v>tth		削除 すべて削除						OK キャンセル

R5 86 87 8+>t//



(1) アクティベーションタスクの実行 – タスクから実行する場合 (5/5) -

⑨ [終了]をクリックします。

 KLいトリカーの通知 クスク 3 新しいトリカー 読用の入力 また ア・グラト C dd 3 ア・グト C

ese	PROTECT				入力すると検索を開始 ⑦ 70				
		タスク	:	θ	▷ ◎ ✔ アクセスグループ 選択 創	回 製品のアク… (2	33) <i>90_</i> V	⊕ フィルタの追加	00
" @		タスクタイプ	p		名前	タヴ	進行状況	タイプ	۰
A			*		MDM登録アクティベーション			製品のアクティベー	· · ·
19+ ()		 D モジュールアップテートロールバ D 隔離ファイルのアップロード 			MDM登録アクティベーション			製品のアクティベー	<u>ک</u> ۔
۵		D 隔離管理	I.		製品のアクティベーション(脆弱性とパッ	ソチ管	× 1	製品のアクティベー	S
1		D 診断			MDM登録アクティベーション			製品のアクティベー	<u>ک</u> ۔
(b)	タスク	D 製品のアクティベーション た 朝日のマップデートの特別			MDM登録アクティベーション			製品のアクティベー	э
_		回義面のアップテートの推送			MDM登録アクティベーション		()	製品のアクティベー	2
0				(D -	ELGAアクティベーション		¥ 1	製品のアクティベー	≥
0		■ Rogue Detection Sensorデータペー			自動アクティベーションタスク EFDE		S 2	製品のアクティベー	Э
🛡 😵		D エージェントのアップグレード	*		MDM登録アクティベーション			製品のアクティベー	Э
12+5		タグ	٩		新規タスク			製品のアクティベー	≥
7			4		MDM登録アクティベーション			製品のアクティベー	Э
					MDM登録アクティベーション			製品のアクティベー	Э
			L		MDM登録アクティベーション			製品のアクティベー	≥
			U		MDM登録アクティベーション			製品のアクティベー	ž 🖕
				-		_			•
ø	折りたたみ		Ŧ	M	規作成 ▼ アクション ▼			K @ 1	0



(2) ELGA機能の有効化(1/4)

① ESET PROTECTメインメニューの[ポリシー]-[新しいポリ シー]をクリックします。

65 0	PROTECT		2	0 እታ)すると検索を開始	始	⑦ ¹¹ ワイッ	クリンクマ	◎ ヘルプ マ		6 ログフ	ややト
		ポリシー	:	アク	セスグループ 適	HR 8	🔯 ESET Mana	. (38) タグ	V	⊛ 7×	ハレタの追加	0 0
⁹⁷ -23		ポリシー	Q		名前				ボリ	リシー製品		0
"▲		へ すべて							ESE	T Management Agent		
⁹⁹⁺		^ ⊘ カスタムポリシー							ESE	ET Management Agent		
0		Common features							ESE	ET Management Agent		
~		ESET Endpoint for Linux (V7+)							ESE	ET Management Agent		
Đ		ESET Endpoint for macOS (V6) and Linux (V4)	U.						ESE	T Management Agent		
A		EST Endpoint for MacOS (V/+) EST Endpoint for Windows							ESE	ET Management Agent		
۲		ESET Endpoint for Windows Security for Android							ESE	ET Management Agent		
÷		ESET Full Disk Encryption							ESE	ET Management Agent		_
1 ⊮		S ESET Inspect Connector							ESE	T Management Agent		_
99.+_j		90	2						ESE	T Management Agent		
1			-						ESE	ET Management Agent		
			÷						ESE	ET Management Agent		
			÷						I ESE	ET Management Agent		
									I ESE	ET Management Agent		
<u> </u>												•
Ξ	折りたたみ		Ŧ	7	クションマー	新しいオ	(リシー) 8	別り当て ▽			⊠ 0 1	9

2 [名前]欄に任意のタスク名を入力し、[続行]をクリックします。

本	名前
定	ELGAポリシー
り当て	説明
X 2	
	タグ
	タグを選択



(2) ELGA機能の有効化(2/4)

 ③ プルダウンメニューより、ご利用のプログラムを選択します。
 ※本手順では、[ESET Endpoint for Windows]を 選択します。

基本 ESET Management Agent ESET Management Agent ESET Management Agent #		
認定 認定 認定 かマリー SET Endpoint for Windows ESET Endpoint for Mindows ESET Endpoint for macOS (V/+) ESET Endpoint for Linux (V7+) サーバー ESET Server/File Security for Linux (V7+) ESET Server/File Security for Linux (V7+) ESET Mail Security for Microsoft Exchange Server (V6+) ESET Mail Security for Microsoft Exchange Server (V6+) ESET Endpoint Security for Microsoft SharePoint Server (V6+) ESET Endpoint Security for Android ESET MoDM for iOS & iPadOS 管理 ESET Management Agent	基本	ESET Management Agent
部り当て ・ Common features ・ Exclusion ・ Ex	設定	機能
B ジョン ESEF Endpoint for Windows ESEF Endpoint for macOs (V/+) ESET Endpoint for macOs (V/+) ESET Endpoint for Linux (V7+) サーバー ESET Server/File Security for Microsoft Windows Server (V/- ESET Server/File Security for Inux (V7+) ESET Mail Security for Microsoft Exchange Server (V6+) ESET Mail Security for Microsoft Exchange Server (V6+) ESET Server/File Security for Inux (V7+) ESET Endpoint Security for Addroid ESET Endpoint Security for Addroid ESET Endpoint Security for Addroid ESET Management Agent ESET Management Agent	割り出て	Common features
サマリー ESET Endpoint for Windows ESE Endpoint for macOS (V/+) ESET Endpoint for macOS (V/s) ESET Endpoint for Linux (V7+) サーバー ESET Server/File Security for Microsoft Windows Server (Vi ESET Server/File Security for Microsoft Exchange Server (V6+) ESET Mail Security for IBM Domino (V6+) ESET Security for Microsoft Exchange Server (V6+) ESET Security for Microsoft SharePoint Server (V6+) ESET Security for Microsoft SharePoint Server (V6+) ESET Mail Security for Android ESET MDM for iOS & iPadOS 管理 ESET Management Agent ESET Management Agent	and a c	Endpoint
ESET Endpoint for macOS (V/+) ESET Endpoint for InacOS (V/+) ESET Endpoint for Linux (V7+) サーバー ESET Server/File Security for Microsoft Windows Server (Vi ESET Server/File Security for Linux (V7+) ESET Mail Security for Microsoft Exchange Server (V6+) ESET Mail Security for Microsoft SharePoint Server (V6+) ESET Endpoint Security for Android ESET Endpoint Security for Android ESET Management Agent ESET Management Agent	サマリー	ESET Endpoint for Windows
ESET Endpoint for macOS (V6) ESET Endpoint for Linux (V7+) サーバー ESET Server/File Security for Microsoft Windows Server (Vf ESET Server/File Security for Microsoft Exchange Server (V6+) ESET Mail Security for Microsoft Exchange Server (V6+) ESET Mail Security for Microsoft SharePoint Server (V6+) ESET Endpoint Security for Android ESET Endpoint Security for Android ESET Endpoint Security for Android ESET Management Agent ESET Management Agent		ESET Endpoint for macOS (V7+)
ESET Endpoint for Linux (V7+) サーバー ESET Server/File Security for Microsoft Windows Server (Vi ESET Server/File Security for Linux (V7+) ESET Mail Security for IBM Domino (V6+) ESET Server/V for IBM Domino (V6+) ESET Security for Microsoft SharePoint Server (V6+) モ ノイイル ESET Endpoint Security for Android ESET MDM for iOS & iPadOS 管理 ESET Management Agent ESET Management Agent		ESET Endpoint for macOS (V6)
サーハー ESET Server/File Security for Microsoft Windows Server (W ESET Server/File Security for Linux (V7+) ESET Mail Security for Microsoft Exchange Server (V6+) ESET Mail Security for IBM Domino (V6+) ESET Security for Microsoft SharePoint Server (V6+) モノ・イル ESET Endpoint Security for Android ESET MDM for iOS & iPadOS 管理 ESET Management Agent ESET Management Agent		ESET Endpoint for Linux (V7+)
ESET Server/File Security for Microsoft Windows Server (Vi ESET Server/File Security for Inux (V7+) ESET Mail Security for Microsoft Exchange Server (V6+) ESET Mail Security for Microsoft SharePoint Server (V6+) ESET Security for Microsoft SharePoint Server (V6+) ESET Endpoint Security for Android ESET Endpoint Security for Android ESET Management Agent ESET Management Agent		サーバー
ESET Server/File Security for Linux (V /+) ESET Mail Security for Microsoft Exchange Server (V6+) ESET Mail Security for Microsoft SharePoint Server (V6+) モノイル ESET Endpoint Security for Android ESET MDM for iOS & iPadOS 管理 ESET Management Agent ESET Management Agent		ESET Server/File Security for Microsoft Windows Server (V6+)
ESET Mail Security for Microsoft Exchange Server (Vo+) ESET Mail Security for IBM Domino (Vo+) ESET Security for Microsoft SharePoint Server (Vo+) モノイイル ESET Endpoint Security for Android ESET MDM for iOS & iPadOS 管理 ESET Management Agent ESET Management Agent		ESET Server/File Security for Linux (V/+)
ESEL Mail Security for IMM Dominio (V6+) ESET Security for Microsoft SharePoint Server (V6+) モバイル ESET Endpoint Security for Android ESET MDM for iOS & iPadOS 管理 ESET Management Agent ESET Management Agent		ESET Mail Security for Microsoft Exchange Server (V6+)
ESET Security for Microsoft SharePoint Server (vo+) モバイル ESET Endpoint Security for Android ESET MDM for IOS & iPadOS 管理 ESET Management Agent ESET Poeus Patietics Server		ESET Mail Security for IBM Domino (V6+)
ESET Endpoint Security for Android ESET MDM for iOS & iPadOS 管理 ESET Management Agent ESET Poeuw Detection Seasor		ESET Security for Microsoft SharePoint Server (VO+)
ESET MDM for iOS & iPadOS 管理 ESET Management Agent ESET Management Agent		ESET Endpoint Security for Android
ESET Management Agent		ESET MDM for iOS & iPadOS
ESET Management Agent		管理
ESET Reque Detection Soncor		ESET Management Agent
E SEL DURINE DE PERINA		ESET Roque Detection Sensor
その他		その他
		ESET INSPECT Connector

 ④ [保護]-[クラウドベース保護]を選択します。[ESET LiveGridフィードバックシステムを有効にする]を有効にし、 「サンプルの送信」、「ESET LIVEGUARD」の各項目の 設定を行います。設定が完了したら、[続行]をクリックしま す。

基本	ESET Endpoint for Windows	▼ Q 入力すると検索を開始	
没定			
^{割り当て} ナマリー	リアルタイムファイルシステム保護	 Comparing ● ビュテーションシステムに参加す ス(推身) 	0
	HIPS クラウドベース保護 ネットワークアクセス保護	● GEW/ ● チ ESET LiveGrid®フィードバックシステムを 有効にする	-
	電子メールクライアント保護 Webアクセス保護	○ ● ケ クラッシュレポートと診断データを送信 ◎ ≥ 7.0	0
	ブラウザーの保護 デバイスコントロール	 ● チ 匿名で統計情報を送付する ● チ 連絡先の電子メールアドレス(任意) 	0
	ドキュメント保護		• • /
	検査	+ ESET LIVEGUARD	0 • 4
	アップデート		
	接続		



(2) ELGA機能の有効化(3/4)

⑤ [割り当て]をクリックします。

⑥ ポリシーを割り当てたいコンピューターを[グループ]もしくは[コンピューター名]から選択し、[OK]をクリックします。

基本	割り当て一割り当て解除			
設定				
割り当て	ターゲット名	ターゲット説明	ターゲットタイプ	
サマリー		使用できるデータがありませ	ŧん	





(2) ELGA機能の有効化(4/4)

⑦ [終了]をクリックします。

【参考】

メインメニューの[コンピューター]画面にて、各コンピューターの [詳細を表示]-[概要]-[ESET LiveGuard Advanced]の 「有効」ボタンより、ELGA機能の有効化を行うことも可能です。

	割り当て、割り当て解除			
没定				
目り当て	ターゲット名	ターゲット説明	ターゲットタイプ	٢
ナマリー	0		コンピューター	







ESET LiveGridとの違い

ESET製品では以前よりESET LiveGridを使用してクラウド環境に不審なファイルの自動送信や手動による分析を依頼できました。 ELGAを使用することで分析結果の閲覧および、悪意があると判断された場合に自動保護を即時に実施することができるようになりました。

項目	ESET LiveGuard Advanced	ESET LiveGrid
ファイルの提出	自動/手動	自動/手動
分析結果	ESET PROTECT / ESET PROTECT on-prem のレポートで確認可能	分析結果は未公開
結果の種類	未感染、不審、非常に不審、悪意	なし
提供される情報	ファイルの動作結果と詳細な記述	なし
分析に使用される技術	サンドボックスを用いた高度な検出手法と 行動分析および機械学習を組み合わせた 多段分析を使用	DNA検出や様々な機械学習モデルを用いた ファジーハッシングを使用
サンプル分析の優先順位	高	低
インタフェース	EP Web Console / EP on-prem Web Console	なし
サポートされる ESET製品	下記ページの[動作環境]をご確認ください https://canon.jp/business/solution/it- sec/lineup/eset/feature/cloud-sandbox	すべてのESETセキュリティ製品
会社全体の自動保護	あり	なし



7. マルウェアの検出事例

(1) 解析の迅速性

弊社の検証環境で検出された「ステガノグラフィー」を用いた実際のマルウェアの検出事例をもとに 「ELGAの解析の迅速性と高度な解析技術」の2点をご紹介します。

(マルウェア検出までの流れ) ①「ばらまき型メール攻撃」でメールを受信 ②メールに添付されたExcelファイルをESET Cloudに自動送信、解析を依頼 ③解析の結果「悪意」と認定、各エンドポイントでブロックを実施。 ※本マルウェアは弊社ELGA検証環境での検知3時間後に検出エンジンに追加。エンドポイント製品でも検知可能に。

	グループ 動的グループテンプレー	送信	きれたファイル 🛕 🛛 🗸 🕚	0 \$	フィルタの追加	プリセット	ファイルの受けの理由を決	受信から
	ト 送信されたファイル		ファイル	八ッシュ	ステータス	状態	↓ (本事例では約8種	沙で解析完了) ◎
A	隔離		mailto:?to=info01_536_3679.XLS	234A3A1		◎ 完了	2019年 6月 17日 19:56:32	2019年 6月 17日 19:56:40
	ライセンス管理		mailto:?to=info7307_60_001.XLS	56C6E1E		◎ 完了	2019年 6月 17日 17:45:47	2019年 6月 17日 17:45:55

ポイント

・メールに添付されていたExcelファイルを自動的に解析を依頼

・複数の高度な手法を用いて検出の回避を狙ったファイルを迅速に解析 (詳細は次ページ参照)



7. マルウェアの検出事例

(2) 高度な解析技術

検出されたマルウェア(DOC/Agent.DZ)には、高度に解析を妨害・回避する処理が複数存在

※マルウェア(DOC/Agent.DZ)の詳細な情報は、弊社マルウェアレポート2019年6月号を参照

https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware1906.html

【本マルウェア(DOC/Agent.DZ)に実施されていた主な解析の妨害・回避手法】

- ・ExcelファイルのVBAのコードにロックを掛け解析を妨害
- ・VBAが実行された環境が日本語環境でない場合、処理を終了させることで解析を回避
- ・PowerShellコマンドを多重に難読化し解析を妨害
- ・PowerShell v3.0以降がインストールされている環境のみで稼働、それ以外は処理を終了させることで解析を回避
- ・攻撃用データを画像ファイルに高度に隠蔽(ステガノグラフィー)し、検出と解析を回避

ポイント

エンドポイント製品やサンドボックス製品で検知が行われないように、高度で巧妙な解析の妨害・回避処理が複数 実施されていたが、ELGAは「悪意」があるマルウェアとして検出を実施。

※ステガノグラフィーとは (詳細は2018年10月マルウェアレポートを参照) https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware1810.html#anc_02