ESET PROTECTソリューション ESET PROTECT Elite / Enterprise スターターガイド

第10版

2023年10月23日

Canon

キヤノンマーケティングジャパン株式会社



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である「ESET Inspect Cloud/ESET Inspect」がご利用いただける「ESET PROTECT Elite」、「ESET PROTECT Enterprise」についてご紹介します。

※本資料はクラウド型XDRである「ESET Inspect Cloud」をメインに記載してあります。

※ ESETが提供するMDRをご利用いただくには、「ESET PROTECT MDR Ultimate」または「ESET PROTECT MDR Advanced」をご契約いただく必要があります。

はじめに



本資料は、ESET PROTECTソリューションのうち、ESET PROTECT EliteまたはESET PROTECT Enterpriseをご検討いただいている お客様に、本ソリューションで利用可能なプログラムやサービス、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 Elite / ESET PROTECT Enterprise

● 対象プログラムとサービス (2023年10月時点)

プログラム名/サービス名	プログラム/サービス概要	最新バージョン	XDRによる管理
ESET Endpoint Security (EES)	Windows クライマント田	V10 1	
ESET Endpoint アンチウイルス (EEA)		V 10.1	•
ESET Endpoint Security for OS X (EESM)		V6.11	
ESET Endpoint アンチウイルスfor OS X (EEAM)		V7.4	
ESET Endpoint アンチウイルス for Linux (EEAL)	Linuxデスクトップ用	V10.1	•
ESET Endpoint Security for Android (EESA)	Android用	V4.0	×
ESET Server Security for Microsoft Windows Server (ESSW)	Windowsサーバー用	V10.0	•
ESET Server Security for Linux (ESSL)	Linuxサーバー用	V10.0	•
ESET LiveGuard Advanced (ELGA)	クラウドサンドボックス	常に最新版を提供	-
ESET Full Disk Encryption (EFDE)	フルディスク暗号化	V1.3	-
ESET Cloud Office Security (ECOS) ※Eliteのみ	クラウドアプリケーションセキュリティ	常に最新版を提供	-
ESET Vulnerability & Patch Management (VAPM) ※Eliteのみ	脆弱性とパッチ管理	常に最新版を提供	-
ESET Inspect Cloud (EIC)	クラウド型XDR	常に最新版を提供	-
ESET Inspect (EI)	オンプレミス型XDR	V1.11	-
ESET PROTECT Cloud (EPC)	クラウド型セキュリティ管理ツール	常に最新版を提供	-
ESET PROTECT (EP)	オンプレミス型セキュリティ管理ツール	V10.1	-





I. セキュリティの考え方について

- 1. eXtended Detection & Responseとは
- 2. サイバー攻撃の流れについて
- 3. ESET社が提供するXDRソリューション

- Ⅳ. その他の情報
 - 1. EPCとEICのバージョンアップについて
 - 2. サポート情報

- ||. 主な機能の紹介
 - 1. ソリューションの概要
 - 2. 製品概要
 - 3. 主な機能
 - 4. システム構成
- |||. ご利用の流れ(※)
 - 1. ESET Business Accountの開設
 - 2. ライセンスの登録
 - 3. EPC/EICのアクティベーション
 - 4. プログラムの展開
 - 5. 初期最適化(チューニング)

※ オンプレミス型のセキュリティ管理ツールとXDRコンポーネントをご利用いただく場合は、 ユーザーズサイトに掲載されているプログラムをダウンロードいただき、それぞれの構築資料をご参照ください。



I. セキュリティの考え方について

I.セキュリティの考え方について **1. eXtended Detection & Responseとは**



EPPの防御をすり抜けた攻撃を検知して封じ込め、調査から復旧までを行うソリューション!



I.セキュリティの考え方について 2. サイバー攻撃の流れについて



発見が遅れると命取りに!早期対処にはXDRの活用が効果的!



大切な資産に脅威が及ぶ前に対処できれば、攻撃の成立を阻止できる

I.セキュリティの考え方について 3. ESETが提供するXDRソリューション



ESETなら各種対策をパッケージ化した包括的なエンドポイントセキュリティソリューションをご提供!



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XDR

エンドポイント対策から高度サイバー攻撃に対応する クラウドサンドボックス、端末持ち出し時の情報漏洩 対策、Microsoft365へのクラウドアプリケーション セキュリティをワンストップでご提供 ※クラウドアプリケーションセキュリティはEliteライセンスの場合 のみ利用可能

インストールしているアプリケーションを自動スキャンし、 アプリケーションとデバイスの脆弱性を検出、修正パッチ の適用を実施 ※Eliteライセンスの場合のみ利用可能



Ⅱ. 主な機能の紹介





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

- 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
- セキュリティインシデント対応(影響調査や原因調査)を高速化・効率化したい
- 万が一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ができる仕組みを備えたい
- 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

XDR運用のニーズ

専門家へのアウトソース

- 24/365の運用を委託したい
- XDRのアラート**分析を専門家に**任せたい
- インシデント対応や復旧、調査分析に専門家の協力を得たい

自社運用

- **自社ポリシーに沿って**運用したい
- 自社のSOCやCSIRTで運用したい

		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
PROTECT MDR	専門家への アウトソース	•	•	•	•	•	•	-	-	•	•	•
PROTECT ELITE	₼ ₩₽ ਜ਼	•	•	•	•	•	•	•	•	•	-	-
PROTECT ENTERPRISE	日仜連用	•	•	•	•	•	•	-	-	•	-	-

* 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。 * XDRはクラウド/オンプレミスどちらも利用できます。XDRの利用環境(クラウド/オンプレミス)とセキュリティ管理ツールの利用環境(クラウド/オンプレミス)は同一が前提となります。

Canon Marketing Japan Inc.

I. 主な機能の紹介 2. 製品概要 - Endpoint Protection Platform- (1/2)



エンドポイント保護の特徴

多層防御で新種の脅威に対する保護を強化



高度化・巧妙化する脅威に対抗するため、マルウェアの起動時だけではなく、その前後も含めた複数のタイミングで攻撃の手法に 合わせた方法で検査を行います。新バージョンで新たに加わった高度な機械学習機能は、従来ESET社のクラウド環境でおこなっていた 機械学習による解析をユーザーのローカル環境で実施し、より迅速にマルウェアかどうか判定できるようになりました。

※ Windowsクライアント用/Windowsサーバー用プログラムの最新バージョンではすべての機能が搭載されています。 ただし、その他のプログラムや旧バージョンにおいては一部の機能が搭載されていない場合があります。

Canon Marketing Japan Inc.

2. 製品概要 - Endpoint Protection Platform- (2/2)



ESET PROTECT Cloudの特徴



管理サーバー不要で早期に運用開始

EPCはSaaS型であるため、サーバーの機器の購入や定期的なメンテナン スによる手間とコストを削減することができます。また、セットアップ もWebブラウザ経由で10分程度で実施することが可能なため、すぐに運 用を開始させることができます。

社内外問わず一元管理

インターネットに接続できるクライアント端末であれば社内外問わず に一元管理することができます。また、管理者はWebブラウザ経由で いつでもどこでもEPCへアクセスでき、クライアント端末を管理する ことができます。

クラウドベースで常に最新な環境

EPCのバージョン管理はESET社にて行われるため、お客様によるバー ジョンアップ作業は不要で常に最新の状態で利用することができます。 また、EMエージェントも自動でバージョンアップされるため、お客様の 運用やメンテナンスの負荷を減らすことができます。





ESET LiveGuard Advancedの特徴

ESET LiveGuard Advanced (旧名称: ESET Dynamic Threat Defense) は、未知の高度なマルウェアに対する検出力・防御力をさらに高める クラウドサービスです。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、 ユーザーは、端末への新規プログラムインストールをする必要がなく、手軽に多層防御の強化を行うことが可能です。







ESET Full Disk Encryptionの特徴

ESET Full Disk Encryptionは、リモート勤務や社内で利用するクライアントPCのディスク全体、またはブートディスク(**)を 暗号化するディスク暗号化ソフトウェアです。 暗号化実施後、クライアント端末にはプリブート認証が付与されるため、 端末の紛失・盗難時の情報漏洩対策を行うことができます。 また、ESET PROTECTソリューションシリーズのセキュリティ管理ツールであるESET PROTECT Cloud/ESET PROTECTを使用して、 各クライアント端末の暗号化状況の確認や復号、プリブート認証パスワードの回復などを行うことができます。



※ブートディスク…Windowsのブートドライブとして使用される物理ディスクです。同一ディスク内にWindowsのブートドライブとその他のドライブが存在する場合は、そのディスク全体が暗号化されます。





ESET Cloud Office Securityの特徴

ESET Cloud Office Securityは、お客様がご利用のMicrosoft 365サービスと連携させてすぐに、マルウェア対策、スパムメール 対策、フィッシング対策を行うことができるクラウドサービスです。企業の通信とクラウドストレージを保護し、検出した メールやファイルの確認だけではなく、検出が発生するとすぐに管理者に通知することができます。 ※ESET PROTECT Eliteライセンスでのみご利用可能です。



導入が簡単

✓ Microsoft 365とAPI連携を行うため、お客様のサービスに影響を与えることなく利用可能
 ✓ API連携型のサービスであるため、お客様環境のMXレコードやDNSの書き換えが不要
 ✓ ポリシー設定を行うだけで、ESET LiveGuard Advancedが利用可能

• 運用が容易

- ✓ Microsoft 365からユーザ/グループ情報を自動取得
- ✓ ESET Cloud Office Securityの保対象を絞ることができるため、スモールスタートが可能
- ✓ ESETが管理するクラウドサービスであるため、お客様によるECOSのバージョンアップが不要





ESET Vulnerability & Patch Managementの特徴

ESET Vulnerability & Patch Managementは、OSとアプリケーションの脆弱性*1とパッチ*2適用状況を管理するソリューションです。 古いオペレーティングシステムやアプリケーションを狙った脅威からクライアントを守ります。

クライアントの脆弱性情報は重大度(リスクスコア)が付与されるため、重大度の高いものから脆弱性対応するといった運用が できます。

また、パッチ管理につきましては手動またはスケジューリングして自動で適用させることもできます。 ※ESET PROTECT Eliteライセンスでのみご利用可能です。

œs	et PROTECT cloub					ιζι 🔎 λητεει	·弗克提出。	0 ¹⁰ 01000	sø≠ (9 ~67 × × 8	マプレチーム	אפינים 🗄
		胞弱性	1	2%	~76.808 🔍 🚺	●1 サブグループの表示	🖸 🗈 🕬 🕬 🕅		~		(1) I < 1, /9	O P MAR
5		グループ	p		△ アプリケーション名	アプリケーションペンダー	アプリケーションバージー	リスクスコア	CVE	コンピューター名	873'9	Nilioa 🔅 🅯
A		へ 白 すべて (208)	0 -		Microsoft Windows 10 Pri	Microsoft Corporation	22H2 (10.0.19045.2006)		CVE-2023-3	口回 @ @ test	オペレーティー	2023年8月9日
	85.0512	~ 尚 会社(0)			Microsoft Windows 10 Pr	Microsoft Corporation	22H2 (10.0.19045.2006)	60	CVE-2023-3	🗆 🗇 🕲 🕲 test	オペレーティー	2023年8月9日
		Android (2)	- 1		Microsoft Windows 10 Pr	Microsoft Corporation	22H2 (10.0.19045.2006)	60	CVE-2023-3	다 (1) 등 (2) test	オペレーティー	2023年8月9日
		ESET inspect Cloud ID	- 1		Microsoft Windows 10 Pr	Microsoft Corporation	22H2 (10.0.19045.2006)		CVE-2023-3	□ □ ♥ ♥ test	オペレーディー	2023年8月9日
			- 1		Microsoft Windows 10 Pn	Microsoft Corporation	22H2 (10.0.19045.2006)	60	CVE-2023-3.,	🖵 🗊 🕲 🗷 test	オペレーティー	2023年8月9日
		The second se	- 1		Microsoft Windows 10 Pr	Microsoft Corporation	22H2 (10.0.19045.2006)	60	CVE-2023-3	🖵 (5) 🕲 @ test	オペレーディー	2023年8月9日
		Contract local	- 1		Microsoft Windows 10 Pr	Microsoft Corporation	22H2 (10.0.19045.2006)	60	CVE-2023-3	💭 😳 🐨 😨 text	オペレーティー	2023年8月9日
		1			Microsoft Windows 10 Pn	Microsoft Corporation	22H2 (10.0.19045.3086)	60	CVE-2023-2	D (D & C test-pc	オペレーティー	2023年8月9日
		~			Microsoft Windows 10 Pr	Microsoft Corporation	22H2 (10.0.19045.2006)		CVE-2023-3	10 (1) (2) (2) (1) (1)	オペレーディー	2023年8月9日
		Trans.			Microsoft Windows 10 Pr	Microsoft Corporation	22H2 (10.0.19045.2006)	60	CVE-2023-3.,	(1) (1) (2) (2) (2)	オペレーティー	2023年8月9日
		S			Microsoft Windows 10 Pr	Microsoft Corporation	22H2 (10.0.19045-2006)	- 53	CVE-2023-3	💭 (1) 🛞 🕲 test	オペレーディー	2023年8月9日
		12.00			Microsoft Windows 10 Pn	Microsoft Corporation	22H2 (10.0.19045.2006)	57	CVE-2023-3.,	다 (1) (1) (2) (1)	オペレーティー	2023年8月9日
		1.000			Microsoft Windows 10 Pr	Microsoft Corporation	22H2 (10.0.19045.2006)	60	CVE-2023-3	🖵 🗐 🕲 🕲 test	オペレーディー	2023年8月9日
		1 - 4844 (11 - 1			Microsoft Windows 10 Pr	Microsoft Corporation	22H2 (10.0.19045.2006)	-	CVE-2023-3	1100 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	オペレーティー	2023年8月9日
		×			Microsoft Windows 10 Pr	Microsoft Corporation	22H2 (10.0.19045.2006)	31	CVE-2023-3		オペレーティー	2023年8月9日
		90	,o		Microsoft Windows 10 Pr	Microsoft Corporation	22H2 (10.0.19045.2006)		CVE-2023-3	C C S C test	オペレーディー	2023年8月9日
			-		Microsoft Windows 10 Pr	Microsoft Corporation	22H2 (10.0.19045.2006)	20	CVE-2022-3	□ (0 % @ test	オペレーティー	2023年8月9日
			- 1		Microsoft Windows 10 Pri	Microsoft Corporation	22H2 (10.0.19045-2006)	24	CVE-2023-3	💭 (12) 🏵 😢 test	オペレーディー	2023年8月9日 。

セキュリティ管理ツールでの「脆弱性とパッチ管理」のイメージ

- ESET Vulnerability & Patch Managementの 主な機能
 - ✓ クライアントの脆弱性情報を自動で収集
 - ✓ 自動および手動でのパッチ適用
 - ✓ 脆弱性の重大度のレベルづけ
 - ✓ 対象のクライアントのリストの表示 など

※1 脆弱性…コンピュータ関連のプログラムに潜む欠点や盲点、弱点のことで、「セキュリティ・ホール」とも呼ばれます。 ※2 パッチ… OSやソフトウェアに存在する脆弱性やバグを修正するプログラムを指します。「修正プログラム」「更新プログラム」「アップデート」などと呼ばれることもあります。 Canon Marketing Japan Inc.





ESET Inspect Cloudの特徴

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



競合リスクやリソース消費量を抑えて多層防御をさらに強化



ESET Inspect Cloudの特徴

ESETのクラウドベースシステムとの連携



ESET Augur(機械学習エンジン)

ESET内部の機械学習エンジンでは、ニューラルネットワーク(ディープラーニングおよびLSTM)と 厳選されたアルゴリズムを組み合わせ、統合されたアウトプットを生成し、受信したサンプルを 「クリーン」、「望ましくない可能性がある」または「悪意がある」ものとして正確にラベル付けを行います。



ESET LiveGrid[®] (Reputation & Feedback)

ESET LiveGrid®は、世界中のESETユーザーから脅威に関する情報を収集するための予防システムです。 LiveGrid®のデータベースには、潜在的な脅威に関する評価情報が含まれており、 最新の脅威を検知しブロックするので、急速に変化する脅威に対してきわめて効果的です。

I.主な機能の紹介 2.製品概要 -eXtended Detection & Response- (3/4)



ESET Inspect Cloudの特徴

EICの検出アラートから、攻撃に使用されたテクニックの詳細を参照可能

< BACK DAIL > DSites > D]Slovalcia (HQ) 🔿 🛅 EEI Demo 🖒 💭 wir	7-5 > Eddef87bd3.exe > > exe1.exe
ESET LiveGrid®	•	win7-5 PARENT GROUP EEI Demo LAST CONNECTED 9 minutes ago - 2020/#12/917/E1 10:34:30 LAST EVENT 10 minutes ago - 2020/#12/917/E1 10:33:12 AGENT VERSION THE EXECUTION 05/11 OPENT VERSION THE EXECUTION 05/11
CATEGORY	Ransomware / Filecoders	5. In case of incident with ranso
EXPLANATION	The process may write a ransomn	5. In case of incident with ransomy
··· > MALICIOUS CAUSES	Filecoder activity.	7. If encrypted files have been found
BENIGN CAUSES	Clean file is being saved.	
RECOMMENDED ACTIONS	Scan the related applicat If antivirus scan did not application module in you Submit the executable fr. Checkerh folder where r Incase of incident with ra f. In case of incident with ra	Rule was activated
MITRE ATT&CK [™] TECHNIQUES	T1486 - Data Encrypted for Impa Rule was activated	Ransomnote behavioral detectio
SOURCE RULE	Rensomnote behavioral detection - filecode	
OCCURRED	12 days ago - 20 20年 12月5日 00:28:40	ago - 2020年125



MITRE ATT&CK			Matrices	Tactics -	Techniques -	Data Sources	Mitigations -	Groups	Software	Resources -	Blog 🛛	Contribute	Search Q
T	The new v11.0 release	of MITRE AT	FT&CK contains a be	ta version of Sub	o-Techniques for M	obile. The current,	table Mobile cont	ent can be a	ccessed via th	e v10 release URI			
TECHNIQUES		Home > T	echniques > Enterpris	e > Data Encrypt	ed for Impact								
Enterprise Reconnaissance Resource Development Initial Access Execution Persistence Privilege Escalation Defense Evasion Credential Access Discovery Lateral Movement Collection		Data Adversarie system ar remote dri from a vic cases whe In the case source co first emplo unlock and partitions, To maxim	a Encryptia s may encryptiata d network resources d network resources the key is not saw e of ransonware, it is d files will be encryp y other behaviors, st d/or gain access to n and the MBR. ^[3] izze impact on the tar accross a network by	ted for They can atten access to a deci- decryption or a d ad or transmitter typical that cor- oted (and often r uch as File and D nanipulate these get organization leveraging othe	Impact is or on large numb ipt to render stored ryption key. This m ecryption key (rans a_10120914) mmon user files likk enamed and/or tag practory Permissio files. ^[5] In some ca	ters of systems in a data inaccessible ay be done in order onnware) or to reno Office documents uged with specific f ns Modification or ses, adversaries m I for encrypting dat like Valid Account	network to intern by encrypting files to extract moneta er data permanen PDFs, images, vi le markers). Adve System Shutdown ay encrypt critical a may have worm s. OS Gredential D	upt availabilit is or data on lo rry compensa- ttly inaccessil deos, audio, t rsaries may r <i>(Reboot, in o</i> system files, - like features umping. and	y to boal and tition lele in ext, and eed to rder to disk to	ID: T1486 Sub-techni O Tactic: Imp O Platforms: O Impact Typ Contribution Mayuresh D Travis Smith Version: 1.3 Created: 15 Last Modifi	ques: No su act laaS, Linux, I laaS, Linux, I laas, Linux, I e: Availabilit rs: Harshal T rs: Harshal T rs: Janux, I rs: Janux, I si a March 2015 ied: 19 April	b-techniques Vindows, mac(y pupsamudre, Qu puleg Kolesnikov 2022	DS Jalys; 4, Securonix;
Exfiltration Impact Account Access Removal Data Destruction Data Encrypted for Impact	~	SMB/Wind wallpapers "print bom In cloud er	dows Admin Shares, [®] s, or otherwise intimi libing ⁻). ^[6] nvironments, storage edure Exan	ate victims by solution of a constraints of the solution of th	nalware may also le sending ransom no compromised accor	everage Internal De tes or other messa unts may also be e	facement, such as ges to connected ncrypted. ^[7]	: changing vid printers (kno	stim wn as		Version P	ermalink	
Data Manipulation	~	ID	Name	Description									
Defacement Disk Wipe Endpoint Denial of Service	~	60082 APT38 APT38 has used Hermes ransomware to encrypt files with AES256. ^[1] 60086 APT41 APT41 used a renormware called Encrypt Files on the tweated surface and provide a renorm note to the user ^[3]											
Firmware Corruption Inhibit System Recovery Network Denial of Service	~	S0640 S0638	Avaddon Babuk	Avaddon encry Babuk can use	pts the victim syste ChaCha8 and ECD	em using a combin H to encrypt data.[ation of AES256 a	nd RSA encry	ption scheme	_{'S.} [10]			

ATT&CK





ESET Inspect Cloudの特徴

VirusTotalにハッシュ値を用いたカスタムリンクを設定可能

PROTECT & INSPECT CLOUD III	
1 Details Statistics ▲ Detections G Seen on ▷ Sources ef87bd3.exe PE: Unknown Select Tags Select Tags signature type None Signer NAME None SEEN ON 2 computers First SEEN 2 years ago - 2018年7月11日 17:07:47 LAST EXECUTED 12 days ago - 2020年12月5日 00:28:40	ESET LiveGrid® REPUTATION POPULARITY FIRST SEEN 2 years ar)F740B27B9BA45BB7 \ Virus Total
NAMES	def87bd3.exe exe1.exe Copy to clipboard
SHA-1	3A95ED603E7B5392186575CBF740B27B9BA45BB7
SHA-256	Unknown Virus Total Copy to clipboar.
MD5	Unknown
SIGNATURE TYPE	None
 SIGNER NAME	None



47 0	47 engines detected this file		
7 63 3 351d tsect community v	aa68bbs03b0f5709fcfb356dsae87d7b40b7f89f95e53629d6cee01e4951 .rene #		86.50 KB 2020-09-14 18:22:3 UTC Size 3 months ago
DETECTION DETAIL	S RELATIONS BEHAVIOR COMMUNITY		
Ad-Aware	Gen:Variant.Ransom.Mole.4	AegisLab	① Trojan.Win32.Deshacop.4lc
AhnLab-V3	① Trojan/Win32.Deshacop.R198537	Antiy-AVL	Trojan/Win32.Deshacop
SecureAge APEX	() Malicious	Arcabit	Trojan.Ransom.Mole.4
AVG	FileRepMalware	Avira (no cloud)	() HEUR/AGEN.1121419
BitDefender	Gen:Variant.Ransom.Mole.4	BitDefenderTheta	① Gen:NN.ZexaF.34242.fu0@ayzBw3aO
Bkav	W32.AlDetectVM.malware1	Comodo	() Malware@#h7mvd3xrlco0
CrowdStrike Falcon	() Win/malicious_confidence_100% (D)	Cybereason	 Malicious.0f0aaf
Cynet	Malicious (score: 100)	DrWeb	Trojan.DownLoader24.40005
eGambit	Unsafe_Al_Score_99%	Elastic	 Malicious (high Confidence)
eScan	Gen:Variant.Ransom.Mole.4	ESET-NOD32	() Win32/Filecoder.HydraCrypt.H
F-Secure	Heuristic.HEUR/AGEN.1121419	FireEye	① Generic.mg.638cb5a0f0aaf6cc
Fortinet	W32/HydraCrypt.Httsransom	GData	Gen:Variant.Ransorm.Mole.4
Ikarus	1 Trojan.Win32.Filecoder	K7AntiVirus	 Trojan (0050b9ba1)
K7GW	() Trojan (0050b9ba1)	MAX	Malware (ai Score=89)
McAfee	GenericR-JPA\638CB5A0F0AA	Microsoft	① TrojanSpy:MSIL/Omaneat.B
NANO-Antivirus	() Trojan.Win32.Deshacop.entzyt	Palo Alto Networks	() Generic.ml
Panda	() Tr/CLA	Qihoo-360	() Win32/Trojan.7cd

VirusTotal





① リアルタイム保護

■ ファイル検査

■ メモリー検査



- :ファイルを作成時や実行時に検査し、悪意のあるファイルを検出します。
- : メモリー内で展開されたデータを検査し、悪意のあるデータを検出します。
- 電子メールクライアント保護:メール受信時に検査し、悪意のあるメールや添付ファイルを検出します。
 - Webアクセス保護 : HTTP/HTTPSプロトコルに対応しており、Webアクセス時にダウンロードされる コンテンツやファイルを検査します。
- ドキュメント保護 : Microsoft Office 形式ファイルに含まれる不正プログラムの有無を検査します。
- ② 新種・亜種のマルウェアの検出(ヒューリスティック技術) EES EEA ESSW

ヒューリスティック技術は、遺伝子技術を応用したマルウェア検出方法です。従来の検出エンジンを使用した パターンマッチングなどでは検出できない新種や亜種のマルウェアも、「静的解析(プログラムコード解析)」、 「動的解析(エミュレータ)」、「遺伝子工学的解析(ジェネリックシグネチャ)」の3つの機能により、 詳細な分析の実行と悪意のある振る舞いの特性を識別することができます。

③ 機械学習保護

EES EEA ESSW

機械学習保護は、リアルタイムスキャンやオンデマンドスキャンでの検出に利用できます。 ESET独自の機械学習アルゴリズムにより、クラウド環境に接続できないオフライン環境でも、 定義データベースにない未知のマルウェアを検出できます。

3. 主な機能の紹介 3. 主な機能 - クライアント用プログラム(2/4)-

④ HIPS

コンピューターのセキュリティに悪影響を与えようとする望ましくない活動およびマルウェアからシステムを保護します。 また、高度な動作分析とネットワークフィルタリングの検出機能を連携し、実行中のプロセスやファイル、レジストリキー を監視します。

⑤ エクスプロイトブロック

ブラウザー、メールソフトウェア、PDFリーダー、JAVAなどの アプリケーションの脆弱性を悪用する動作を監視しブロックします。 これにより脆弱性を悪用して個人情報やFTPアカウントなどを盗もうとするウイルスを検知することが可能です。

⑥ アドバンストメモリスキャナー

実行中のメモリの詳細な検査を実施し、難読化や巧妙な手法で偽装されたウィルスの検出が可能です。 これにより、ヒューリスティック検査でも検出が難しい難読化・暗号化されたウイルスについての検出します。

7 ESET LiveGrid

クラウドを利用してより速くより正確にマルウェアを検出します。 また、使用しているプログラムの安全性を評価します。

⑧ ランサムウェア保護

データを修正しようとするアプリケーションとプロセスの動作を監視し、 悪意のあるアプリケーションからデータを保護します。

EES EEA ESSW





21



EEA

EEA

ESSW

ESSW



3. 主な機能の紹介 3. 主な機能 - クライアント用プログラム(3/4)-

⑨ フィッシング対策

フィッシングサイトのリスト、シグネチャと照合・検査を行います。 電子メールなどに埋め込まれているフィッシングサイトへのアクセスを抑止します。

10 デバイスコントロール

CD/DVDドライブ、USB接続のストレージデバイスなどの利用を制御できます。 CD/DVDの挿入時や外部ストレージデバイスの接続時に、自動的に中身を検査することも可能です。

⑪ 不正侵入対策/パーソナルファイアウォール

IPv6対応のファイアウォール機能により、ワーム、RPC/DCOM攻撃、DNS Poisoning攻撃、 ポートスキャン攻撃、SMB Relay攻撃、TCP非同期攻撃、リバースTCP非同期攻撃、ICMP攻撃などを検出します。 また、社内LAN、公衆無線LANなど、接続するネットワークごとに 異なるファイアウォールポリシーのプロファイルを作成できます。 WindowsのV6以降のプログラムではボットなどによる外部の通信を検出・防御する「ボットネット保護」機能や、 IDS機能を強化して、各種攻撃と脆弱性を検出する「バルナラビリティシールド」機能が追加されました。 MacのV6のプログラムはパーソナルファイアウォール機能のみが実装されており、 指定したフィルタリングルールに基づいたネットワーク接続の可否の設定が可能です。







EES

3. 主な機能 - クライアント用プログラム(4/4)-

Canon Marketing Japan Inc.

Ⅱ. 主な機能の紹介

迷惑メール対策エンジンによる検出とブラックリスト・ホワイトリストの設定が可能です。 スパム判定された電子メールを指定のフォルダへ振り分けます。

③ Webコントロール

ユーザーがアクセスできるWebサイトをカテゴリ指定またはURL指定で制限できます。 制限されているサイトにアクセスした場合、ブロック用ページを表示してユーザーに通知します。

ゆ セキュアブラウザー

コンピューターで実行中の他のプロセスからWebブラウザーを保護します。 ゼロトラストアプローチであり、コンピューターまたはその保護機能が危険にさらされている、または不十分である という前提でブラウザーのメモリ空間や結果的にブラウザーウィンドウの内容が改ざんされることを防止します。

15 自動アップデート機能

随時公開される最新バージョンへのバージョンアップ負荷を軽減するため、これまでセキュリティ管理ツールや ユーザー自身が手動で行っていたバージョンアップ作業を実施することなく、プログラムが自動でバージョンアップされる 機能です。本機能により、管理者やユーザーに負荷をかけることなく、常に最新のプログラムを使用したウイルス対策が可 能になります。



23





3. 主な機能の紹介 3. 主な機能 - セキュリティ管理ツール-

① ログ管理機能

ログ管理機能はセキュリティ管理ツールの最も重要な機能の1つで、 クライアントから収集したログや設定情報の表示、 レポートの作成などを行うことができます。

② クライアント管理機能

クライアント管理機能を使用すると、端末にインストールした クライアント用プログラムの設定をリモートで変更することが可能です。 また、クライアントをグループ化することや管理している クライアントを指定してタスクを実行することもできます。

③ 運用管理機能

運用管理機能は、セキュリティ管理ツールが 円滑に運用できるように保守を行う機能です。 セキュリティ管理ツールへのログインユーザーの管理を行ったり、 管理者によって実施されたセキュリティ管理ツールの 操作内容の確認をすることが可能です。





I. 主な機能の紹介 3. 主な機能 - eXtended Detection and Response(1/5)-



①Webコンソール

ダッシュボードを起点にあらゆる角度から調査を開始可能です。 可視化機能や高度な検索機能が対応を強力にサポートしているため、 1つのWebコンソールだけでミクロ・マクロ両方の視点から調査が可能です。 脅威が発見された場合は、すぐにネットワークやコンピューターの保護を実行できます。







②ハッシュ値によるブロック, プロセスの強制停止

ハッシュブロックではハッシュ値(SHA-1)を利用して特定のファイルの利用を禁止することができます。 またブロックされたファイルが作成・修正したレジストリを削除でき、プロセスキルはプロセスを強制終了させることが可能です。





③ネットワーク隔離

侵害端末を素早くネットワークから隔離し、被害の拡大を抑制することができます。 隔離中でもWebコンソールからのリモート調査が可能であるため、 Remote PowerShellと組み合わせることで、より柔軟な対応を実施可能です。 ※ESET関連の通信のみ可能

(INSP	ECT CLOUD :::			DISABLED ③ HELP ♥	🖂 ьосоит	(In the second s	γ 🖃 ιοσουτ
DASHBOARD	Computers	: ▲ ● i ✓ ○ Tags	SHOW SUBGROUPS ADD FILTER	PR	esets 🗢 🛛 Protect 🕘 📿		PROTECT
	Groups	2				COMPUTERS 1 Details & Terminal 🔺 Alerts 🛦 Detections 🖸 Executables 😨 Scripts 🗘 Events	
	Cloups All Computers	• NAME (6)	STATUS TAGS	✓ LAST CONNECTED	LAST EVENT (9)	CETECTIONS Win10 5 Unresolved Detections	
O SEARCH	LOST+FOUND	Win10.5	▲	Jun 14, 2022, 542300 AM	Jun 14, 2022, 9:38:03 AM	Stanch Select Tags	
		Win10-2	•	Jun 8, 2022, 9:13:33 PM	Jun 8, 2022, 9:13:19 PM		
		Win10_1	0	Jun 8, 2022, 9:09:51 PM	Jun 8, 2022, 9:09:51 PM	Flow Desktor-revenu D Executive Parent Group /序へて/東京	
		Win10_4	9	Jun 5, 2022, 4:50:12 AM	Jun 5, 2022, 4:50:04 AM	Last Connected 3 minutes ago - Jun 14, 2022 94/502 AM.	i
		Win10_6	9	Jun 1. 2022, 12:16:42 AM	Jun 1, 2022, 12:16:39 AM	Oursitions EST Inspect Connector 1/1 0	Informational 0
	>					More > OS Name Microsoft Windows 10 Pro	
COLLAPSE	Tags Alternate Dat., X. Common File., X. Common File., X. Credential Ac., X. Credential Ac., X. Data Encrypt., X. DLL Resolution, X. DLL Pensiteroo X.	P SELECTED FIEMS: 1/6 COMPUTERS * INCODENT *	Network holdston g ^{ol} totale Ø End solation SCAN NETWORK ISOLATION * PC	Network Isolation		OS Version 10.13024.1705 Group パマペ元原 Isolated from Network No Lat Connected 3 minutes ago - Jun 14.2022. 94.502 AM Lat Event 3 minutes ago - Jun 14.2022. 94.501 AM Received Events From Today 1458 Stored Events From Today 1458 EST Inspect Connector Version 1 00 Houlds COMPUTER * NOVER SOLATION *	RK TASS
						一覧画面や詳細画面から	
					1	クリック でネットリーク隔離を実施 —————	





④Remote PowerShell Interface

リモートからエンドポイントへ直接接続してインシデントレスポンスが可能です。 同一の管理コンソールからリアルタイムでユーザーのワークフローを止めることなく、 侵害端末へのきめ細かな調査・対応・修復などが実施できます。

Image: Selection selectio	CT CLOUD III QUESTIONS @ Learning mode enabled DISABLED ● HELP マ E LOGOUT BACK ロすべて > 白東京 > Wint0-2 i Details [®] Terminal A Alerts A Detections E Executables E Scripts 中 Events PS C: \WINDOWS\system32> S	 リモートからのライブレスポンスをサポート 詳細調査のための情報取得 システムのイベントログ取得 重要ファイルのバックアップ 攻撃者が生成したファイル等の削除 攻撃者が変更したレジストリキーの復旧 など
••• More >	CONNECT	 ライブレスポンスとは? コンソールへ直接接続してコマンドやツールを実行し、 システムを稼働させたまま情報収集を行う手法 主にメモリ上に展開されているプロセス、ファイル、 レジストリ、ネットワークなどの揮発性の情報取得に使用する

I. 主な機能の紹介 3. 主な機能 - eXtended Detection and Response(5/5)-



⑤アクションの自動化

検知ルールに事前にアクションを定義しておくことで、 検出アラートがトリガーされたタイミングで任意のアクションを自動実行可能です。



検出時には定義済みアクションを自動実行

- ネットワーク隔離
- ハッシュ値によるブロック
- 各種マーカーの付与
- イベントのドロップ
- 検出アラートのトリガー など

	-							
	DETECTIONS	BACK [edit]Archive Utility (B1) enco	ypting files [E0609]					
G	Rules Exclusions	i Details 🔯 Edit ▷ Rerun Tasks	i Exclusions					
A	Blocked Hashes	Rule	[edit]Archive Utility (B1) encrypting files [E0609]					
0	ADMIN	Author	ESET					
~	Tasks Settings	Last edit	4 minutes ago - Jul 21, 2022, 7:59:30 PM					
Ŷ		Category	Ransomware / Filecoders					
▶	Audit Log	Severity	Threat					
#_		Severity score	70					
ф … >		Explanation	The 'B1' archive utility was executed via the command line via 'java -jar', and instructed to password-protect an archive. If the user isn't aware of the activity, it may indicate ransomware or collection activity.					
		Remediation actions	Built-in actions Report detect Block executa Isolate comp Store event User actions					
		-	Select user actions					
		Malicious causes	Can be used by adversaries to compress and encrypt data discovered as a means of collection (e.g. intellectual property), to be likely staged and later exfiltrated. It is common for the resulting archive files to be named in a manner as to blend in as a normal temp file to try slip by unnoticed.					
	CLOSE	Benign causes	Can be a legitimate action performed by a user to protect data by encrypting it, perhaps, before sending it.					







ESET Inspect Cloud (EIC)

EIC/EI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EIC/EI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 Cloud (EPC)

EPC/EP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 (El Connector)

El Connectorはクライアントのデータを収集し7分間隔でEIC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EPCヘデータを 送信します。また、EPC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。









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

サポートされるアプリケーションバージョン※

アプリケーション名	EPCによる管理	EICによる管理
ESET Endpoint Security / アンチウイルス	7.3以降	10.0.2045.1以降
ESET Endpoint Security / アンチウイルス for OS X	6.10以降 / 6.11以降	6.11.606.0以降
ESET Endpoint アンチウイルス for Linux	8.1以降	9.1.4.0以降
ESET Endpoint Security for Android	3.3以降	-
ESET Server Security for Microsoft Windows Server	7.3以降	10.0.12010.1以降
ESET Server Security for Linux	7.2以降	9.1.91.0以降

※VAPMの対象プログラムは、ESET Endpoint Security / アンチウイルス V10.1以降です。

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EICに集められたすべてのログ)	7日間
検出ログ(EICの検知ルールによって検出されたログ)	31日間



Ⅲ.ご利用の流れ

^{II.} I. ESET Business Accountの開設





Ⅲ.ご利用の流れ 1. ESET Business Accountの開設



- https://eba.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 1.
- 画面に表示される説明に沿ってお客様情報を入力 2. ※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EBAログイン時に使用します



■ログイン画面

^{II.}ご利用の流れ 1. ESET Business Accountの開設

- 3. 利用規約をご確認いただき「ESETに同意」にチェックし「登録ボタン」をクリック
- 4. 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

■利用規約への同意画面

	会社の住所を追加
eset BUSINESS ACCOUNT	会社の住所を入力し、登録を確定してください。
	垂地 1
ESET Business Accountは、すべてのESETビジネスソリューションのライセンス 茨畑プロットフィー しゃまり corruptionを出し ビス ゆすい トレー ポイント	任意
官理ノラットフォームであり、ESEIクラウトリーと入へのエントリールイント です。	香地 2
(3.	任意
✔ 完全に機能する無料試用版を作成する(購入義務なし)	市区町村
✔ すべてのセキュリティライセンスの概要を確認する	任意
✔ 使用済みシートのリアルタイムステータスを確認する	州/県
✔ 即時のアクティベーション解除と回復	任意
	郵便量号
	任意
	eseric同意する利用規約 C
	戻る 登録
	ヘルプ • 日本語 (Japanese)
	© 1992 - 2021 ESET, spol. s r.o 不好複製 · 效無對新配紙

■アクティベーション用メール





I. ESET Business Accountの開設

- 5. 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
- 6. EBAにログインできることの確認 ※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メール



■EBAにログインできることの確認









Canon Marketing Japan Inc.





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

①[ダッシュボード]内の[最初のライセンスを追加する]

eser BUSINESS ACC	DUNT			→ > 25 MIN
ダッシュボード	ダッシュボード			- 1
▲ <i>ア</i> ラ−ト	ESET PROTECT Cloud シンプルなクラウドベースのソリューションで会社ネッ	0 5 7222		<u>^</u>
	トワークで簡単にセキュリティを管理します。 無償試用版の開始 ライセンス募入[2]	1 管理されたユーザー		
	 ✓ Business Accountの設定 以下の手順は、EST Business Accountを最大限に活用す ストルに協立ちます ● 日、最初のライセンスを追加する ● 二要素認証を有効にしてセキュリティを強化する ● 二要素認証を有効にしてセキュリティを強化する ● アカウントを完成して会社を管理する 	 アクティブ化されたデバイス ライセンス使用状況 	● 使用酒み ◎ 利用可 1a]	能●使用超過
_	任!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!	表示するデー 1 ライセンスがまだ追 状況を確認するには く1	-タはまだありま せん 加されていません。使用 、ライセンスを追加して ささい。	

②[ライセンスの追加]画面







- 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

es	BUSINESS ACCO	DUNT										b,
	ダッシュポード	ライセンス	秋況 🗸		0							
A	アラート		ライセンス		11 D 8 60	所有者	状況	עבב	Þ	サブ単位	Ô	
Ę	ライセンス			NFR EPC	ESET PROTECT Complete	Canon Marke	×					
	アクティブ化されたデバイ ス											1
	ユーザー管理											
	監査ログ											Ľ
	詳細											
	設定											
	ESET PROTECT CLOUD											I
	ESET CLOUD OFFICE D											I
	フィードパックを送信											
		0/1										
		4										2
		+ ライセン	·スの追加	iilik CSV2	としてエクスポート N (0 1 0 0 20	. v					
		_	_							_	_	











- 1. EPCとEICのアクティベーション(左側メインメニューの「ESET PROTECT CLOUD」をクリックして開始します)
- 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 CloudとESET Inspect Cloudが同時にアクティベーションされます。



	ESET PROTECT Cloud & CrESET Inspect Cloud	
△ ESET PROTECT CloudおよびES		1 管理されたユ
Inspect Cloud ESET PROTECT & Inspect Cloudインスタンスを キュリティ製品を展開して、セキュリティの制	ESET PROTECT CloudとESET Inspect CloudをBusiness Accountに追加しました。	
します。	2. ESET PROTECT CloudとESET Inspect Cloudのアクティベーション	
	セットアップを完了するには、最適なデータセンターの場所を選 択してください。	
	テータセンターロケーション ○ EU	
	O USA	
	● APAN (推写) 別の通いデータセンターを選択すると、サービスの質に影響する可能性 があります。ラータセンターロケーションは、ESET PROTECT Cloudが アクティペーションされた後の変更できません。	
	言語	
	Japanese 👻	
	✓ ESET PRO ECT CloudおよびESET Inspect Cloudの利 用規約に計算します。	
	アクティペーション	
	製品の使用状況	
	et a.	









^{II.ご利用の流れ} 4. プログラムの展開



プログラムの展開の流れは以下になります。

※ EPCとEICをご利用いただくにはクライアント用プログラムの他に以下のプログラムのインストールが必要です。

- EMエージェント (クライアントとEPCの接続に使用)
- El Connector (クライアントとEICの接続に使用)



追加インストールする場合(EMエージェントインストール済)

ソフトウェアインストールタスクでクライアントにEI Connectorをインストールします。 EI Connector/クライアント用プログラムのバージョンアップもソフトウェアインストールタスクを使用した 本手順で対応が可能です。

^{エ.ご利用の流れ} 4. プログラムの展開



1. 静的グループの作成

静的グループはメインメニュー「コンピューター」から作成可能です。

グループは階層構造も可能なため、柔軟に組織構造的を作成することができます。

1. メインメニューの「コンピューター」画面より、静的グループを作成する親グループの歯車マークを選択し、「新しい静的グループ」をクリックします。

2. 作成する静的グループの「名前」(必須)と「説明」(任意)を入力し、「終了」をクリックします。

 ・ クッシュホード ・ コンビューター ・ ゴ が能せ ・ ロ ホード ・ ロ ホー ・ ロ ・ ロ ・ ロ	eset	PROTECT CLOUD	:		LOST+FOUND		Φ	□マ コンピューター名		クイック
□ 3ンビューター ● 101-7 ● 102-7 ● 100-7 ● 100-7 ● 100-7 ● 100-7 ● 100-7 ● 100-7 ● 100-7 ● 100-7 ● 100-7 ● 100-7 ● 100-7 ● 100-7 ● 100-7 ● <t< td=""><td></td><td></td><td>コンピューター</td><td>:</td><td> i 詳細を表示 自 監査ログ </td><td>「グループの表示 🔽</td><td>LOST+FOU</td><td>ND (1) タグ</td><td>_</td><td>フィルタの</td></t<>			コンピューター	:	 i 詳細を表示 自 監査ログ 	「グループの表示 🔽	LOST+FOU	ND (1) タグ	_	フィルタの
 ▲ ● ○ 町へて(1) ● タスク ● タスク ● タスク ● タスク ● タスク ● マスク ● 9270 ● 192:162:25:133 ● 2021 ● マスク ● マスク ● マスク ● マスク ● ロルコンピューター ● 100:12:21:2-9- ● 100:12:2:2:2:2:2:2:2:2:2:2:2:2:2:2:2:2:2	돠	コンピューター	グループ	Q	+ 新しい静的グループ + 新しい動的グループ	<u>ع</u>	ルンドレス	タグ	ステー	前回の
 □ K/L-K □ LUST-FOLND(1) ○ LUT-K ○ LUT-K ○ LUST-FOLND(1) ○ LUT-K ○ LUST-FOLND(1) ○ LUT-K ○ MUSONS 32-21-9- ○ MUSONS 32-21-10 ○ MUSONS			へ 亡 すべて (1)		▷ 9スク ▷	1	192.168.254.133		~	2022
 ▶ 972 ▶ 972 ▲ 12,7k-5- ▶ 10 Mindows 32/E1-9- ▶ 10 Min			LOST+FOUND (1)	Ø	③ レポート ▷					- 8
 ○ パントーラ- ○ パリシー ○ ぷコ > パシー ○ ぷコ > パラークス規長 ○ パンソリニーション > 市場のあるデバス ● アクティペーション割れていたのビリュー > ① アクティペーション割れていたのビリュー > ○ ピレイバレデバイス > ○ ピレイバレデバクを送名 ● パリたみ > ○ パントークー > ○ パントクー			✓ Im Windows コンピューター		100 水500 00 国産					
 ボリシー ・ボリシー ・ボリシー ・ゴーボレマシュールのデバイス ・ゴーボレマシュールのデバイス ・ゴーボレマシュールのデバイス ・ゴーボレマシューン ・ゴーボレマション ・ 「「「「「「「」」」」」 ・ 「「「」」」」 ・ 「「」」」 ・ 「「」」」 ・ 「「」」」 ・ 「「」」」 ・ 「「」」」 ・ 「」」」 ・ 「」」」」 ・ 「」」」 ・ 「」」」」 ・ 「」」」 ・ 「」」 ・ 「」」」 ・ 「」」」 ・ 「」」」 ・ 「」」」 ・ 「」」」 ・ 「」」 ・ 「」」」 ・ 「」」」 ・ 「」」 ・ 「」」」 ・ 「」」 ・ 「」」 ・ 「」」 ・ 「」」 ・ 「」」 ・ 「」」」 ・ 「」」」 ・ 「」」」 ・ 「」」」 ・ 「」」」」 ・ 「」」」 ・ 「」」」 ・ 「」」」 ・ 「」」」 ・ 「」」」 ・ 「」」」 ・ 「」」」 ・ 「」」」 ・ 「」」 ・ 「」」 ・ 「」」 ・ 「」」 ・ 「」」 ・ 「」」 ・ 「」」 ・ 「」」」 ・ 「」」」 ・ 「」」」 ・ 「」」」 ・ 「」」」 ・ 「」」」 ・ 「」」			∨ 🛅 Linux⊐ンピューター							
 NOS- ・			∨ 🖿 Mac コンピューター							
 ◎ 払知 ● ステータス概要 ● SETソリューション ● 第日バリルデリイス ● アクティヘーションされていないをする ● アクティヘーションされていないをする ● アクティートコンされていないをする ● アクティーションされていないをする ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●			🗈 古いモジュールのデバイス	歯車	ミマークをク し	リックする	ことで			
 ☆ ステータス概要 ○ EST/ソリューション ① アクティペーションされていないですユニ ⑦ 正じパリルデバイス ⑦ ゴイードパックを送信 ○ 折りたたみ ● 「加いた」の ● 「「「「「「」」」」 			🞦 古いオペレーティングシステ	静的	マグループが作	成できま	व.			
 ● ESTYUJユーション ● アクティベーションされているのですユー ● アクティベーションされているのですユー ● アクティベーションされているのですユー ● タグ ● タグ ● タグ ● タグ ● アイードパシクを送居 ● 新りたたみ 			💽 問題のあるデバイス					J		
詳細 >> > ♪ ♪ ♪ ♪ ♪ ♪ ♪ ♪ ♪ ♪ ♪ ♪ ♪ ♪ ♪ ♪ ♪	•		🖸 アクティベーションされていない							
タグ タ Canon Canon Cano										
Canon Canon C フィードバックを送信 ・ 新規会加 アクション マ ミュート マ			タグ	Q						
□ フィードバックを送信 □ 新りたたみ ミュート マ			Canon							
回 新りたたみ 新規追加 アグション マ ミュート マ					4					-1
					新規追加アクション	マ < <p>ミュート</p>	~			- 1



新しい静的グループ <u>コンピューター</u> > 3課	
基本	3課 3課 週間 第0 第2000000000000000000000000000000000000
	戻る 続行 終了 キャンセル

^{II.ご利用の流れ} 4. プログラムの展開



2. ポリシーの作成

■メインメニュー「ポリシー」 画面

クライアント用プログラムやEM Agent、El Connectorに対して、検査の除外設定、 検出エンジンのアップデート先の設定、プロキシ設定など各種プログラムの設定を行います。

- 1. メインメニューの「ポリシー」画面より、「新しいポリシー」をクリックします。
- 2. 「基本」画面にて、ポリシーの「名前」を入力します。
- 3. 「設定」画面にて、ポリシーを作成するプログラムを選択し、各種設定を行います。
 (例:クライアント用プログラムの検査の除外設定やアップデート先の変更、プロキシの設定など)

11 9		ポリシー	:	アクセス	グループ 選択 曽	未割り当ての項目を表示 🔽	酒 すべて (36) タグ
⊐ •		ポリシー	م		名前	ポリシー製品	タグ
		へ すべて	1		ウイルス対策 - バランス	重視 ESET Endpoint for macOS (
ぶ レ 回 タ		 			ウイルス対策 - 最大限の	tz ESET Endpoint for macOS (
<u>⊟</u> 1		 Auto-updates ESET Endpoint for Linux (V7+) 			デバイスコントロール・	読 ESET Endpoint for Windows	
◎ ポ 心 遥	リシー 痴	 ESET Endpoint for macOS (V6) an ESET Endpoint for Windows 			ファイアウォール - ESET ログ - 完全診断ログ	P ESET Endpoint for Windows ESET Endpoint for Windows	
ר לי 10 ס פו		 ESET Endpoint Security for Andro ESET Full Disk Encryption 			ログ - 重要なイベントの	み ESET Endpoint for Windows	
··· 31		ESET Mail Security for Microsoft	•		ウイルス対策 - 最大限の	번 ESET Endpoint for Windows	
		Canon			表示 - バランス重視 表示 - 非表示モード	ESET Endpoint for Windows	
					表示 - ユーザーの操作を	减 ESET Endpoint for Windows	
					ウイルス対策 - リアルタ ウイルス対策 - 最大限の	イ ESET Server/File Security fo セ ESET Server/File Security fo	14
™ 小リミ ™ 作成さ	シーを作成す されているポ [」]	ることも可能ですが リシーを使用・編集	`		表示 - サイレントモード	ESET Server/File Security fo.	
ことも同	可能です。				クラウドベースのレビュ	ESET Mail Security for Micr	
				יאלא די		<u>制的地で マ</u>	



^{エ.ご利用の流れ} 4. プログラムの展開



クライアントが所属する親グループや事前に作成したポリシーを設定に含めることが可能です。

((ESETセキュリティ製品をインストールしてデバイスを管理および保護 会社ネットワーク全体でセキュリティ製品を配布します。ESETセキュリティ製品を展開し、オペレーティングシステムに基づいてデバイスをESET PROTECT Cloudに接続するには、さまざまな方法があります。ESETヘルプの評無	
	インストーラーが作成されていません 単内した5511間急をタウンロードして、アクティベーションし、デバイスを55511 MODICCTに接触する <u>インスト</u> <u>ーデーを内部</u> します。	Windows Windows	
フィードバックを送信	インストーラーのA版	 Characterial Control (1997)の La Faxility of URAN Control (1997)	<u>、</u> みます
三 折りたたみ		インストーラーのカスタマイズ 閉じる	

■インストーラー作成画面(1/4)

■メインメニュー「インストーラー」画面

※複数の静的グループがある場合は、静的グループごとにインストーラーを分けて作成する必要があります。

エ.ご利用の流れ 4. プログラムの展開



3. インストーラーの作成を行う場合(2/3)

インストーラーに含めるコンポーネントやポリシー、親グループなどの各種設定を行います。

- 3. 「基本」画面では、インストーラーに含めるコンポーネントや親グループ、インストーラー名、ESET Management Agentに関する設定を行います。
- 4. 「製品の設定」画面では、インストーラー含めるセキュリティ製品のバージョンやポリシーの組み込みなどを行います。



^{エ.ご利用の流れ} 4. プログラムの展開



3. インストーラーの作成を行う場合(3/3)

「配布」画面では作成したインストーラーの配布方法を検討します。

- インストーラーのダウンロードリンクが表示されるため、ダウンロードリンクのコピーやブラウザから直接ダウンロードが可能です。
- 電子メールアドレスを登録してメールでURLを配布することも可能です。(CSVで一括で電子メールアドレスを登録することも可能です。)



^{II.ご利用の流れ} 4. プログラムの展開



3. ソフトウェアインストールタスクを利用する場合

EPCメインメニュー「タスク」より、「新規作成」-「クライアントタスク」を作成します。

メインメニューの「ポリシー」画面より、「新しいポリシー」をクリックします。

- 1. 基本画面でタスク分類を「すべてのタスク」または「ESETセキュリティ製品」、タスクを「ソフトウェアインストールタスク」を選択します。
- 2. 設定画面でインストールするパッケージから「ESET Inspect Connector」を選択し、ESETライセンスで「ESET Inspect」が選択されていることを確認します。
- 3. トリガー作成では、El Connectorをインストールするクライアントまたはグループを選択し、タスク実行のタイミングであるトリガーを設定します。

PROTECT CLOUD		φ	□ コンピューター名	クイックリンク マ 💿 ヘルプ マ	A ISETプレ 🕞 ログアウト						
	新規タスク										
	タスク 〉 ESET Inspect Connectorイン	レストール									
	基本	名前			🏟 🖬マ コンピューター	¹¹ クイックリンク マ	③ ヘルプ マ 糸 ESET プレ	ログアウト			
	設定	ESET Inspect Connector-1	ダッシュボード	新規タスク							
	サマリー	タヴ	-9- 	タスク 〉 ESET Inspect Connectorイン	レストール			_			
		ジクを選択説明	▲ 検出 ☆ Lat-ト	基本	ソフトウェアインストール設	(ESET) PROTECT CLOUD		גיירב ⊽נים	ーター名 び クイックリンク マ	③ ヘルプ マ	ログアウ
				設定	インストールするパッケージ ③	ダッシュボード	新しいトリガーの追加				
		タスク分類		サマリー	○ リボジトリからパッケージをインストールESET		タスク 〉 ESET Inspect Connectorインスト				
		ESETセキュリティ製品			 	A 88:5					
		タスク			ESETライセンス ③		□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	ターゲットの追加 ターゲットの削除	A		
		シンドウェアイシストー	 		ESET Inspect, ライセンスID 3AS-83R-72X, 所有者Cano 2023年3月31日 21:00:00		トリガー	ターゲット名	ターゲット説明	ターゲットタイプ	10
				>	✓ エンドユーザーライセンス装約に同意し、ブライ		詳細設定 - 調整		使用できるデータがありません		
					インストールパラメータ ③						
りたたみ		戻る。続行				℃ ステータス概要					
					必要なときに自動的に再起動	 ESETソリューション ******* 					
					戻る 統行 終了 キャン						
								展る 統行 終了	キャンセル		
						11910100					_

■ソフトウェアインストールタスク画面











初期最適化は以下の流れで行います。
 ※初期最適化とはお客様業務により発生するアラートをEIC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が必要です。



 EICには、自動で除外を作成できる「rule learning mode」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EICに認識させることで自動で除外を作成できます。
 「rule learning mode」の期間が終了したら、EICが作成した除外を
 有効化するかを選択します。



 EIC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含めることで、 よりセキュアな除外が作成できます。



- 「rule learning mode」によるチューニング(1/2)
 EICには自動で除外を作成できる「rule learning mode」が搭載されています。
 - 1. EICにログイン時に表示される「Enable rule learning mode」から、「SELECT COMPUTERS」をクリックします。
 - 2. 除外作成の対象とするグループとその期間を設定し、「ENABLE LEARNING MODE」をクリックします。

■ 「rule learning mode」設定画面



■「rule learning mode」設定画面





1. 「rule learning mode」によるチューニング(2/2)

「rule learning mode」の期間が終了したら、メインメニューの「Questions」より有効化する除外を選択します。

- 3. メインメニューの「Questions」より、「rule learning mode」により作成された除外を確認します。
- 4. 作成された除外を有効化する場合は「ACCEPT EXCLUSION」をクリックします。

eser	PROTECT & INSPEC		I,
		Questions ADD FILTER C	,
G		DESCRIPTION (6)	
▲		Learning mode created an automatic exclusion for the following rule: w32tm.exe executed [C0425] Review the created exclusion and verify if it works as expected.	ł
Q		Learning mode created an automatic exclusion for the following rule: Software vendor Masquerading - creation [F0302] Review the created exclusion and verify if it w	orks
		Learning mode created an automatic exclusion for the following rule: Service failure command [C0448] Review the created exclusion and verify if it works as expected.	
		Learning mode created an automatic exclusion for the following rule: Appinit_DIIs registry was modified [A0101a] Review the created exclusion and verify if it works as Some detections could be automatically silenced by an exclusion that is currently disabled: Various, legit software - [F0436a] Consider whether the exclusion should be	e en
		Some detections could be automatically silenced by an exclusion that is currently disabled: RemoteConnector, Loading untrusted dlls by Trusted processes - [80406a]	[80
E	COLLAPSE	4	×

■メインメニュー「Questions」 画面

■除外ルール有効化画面





2. 手動によるチューニング(1/3)

EICで表示されているアラートを確認し、お客様の業務により発生しているアラートである場合は手動で除外を作成します。 アラートは「DASHBOARD」や「DETECTIONS」から確認できます。

1. 「ダッシュボード」からアラートを確認する場合は、発生しているアラートTOP10の円グラフ、または画面下部のタイムラインをクリックします。 「DETECTIONS」からアラートを確認する場合は、画面上部のフィルターを使用し、「Rules」や「Executables」などでアラートを確認します。





■メインメニュー「DETECTIONS」画面



2. 手動によるチューニング(2/3)

検出を除外しても問題ないことを十分確認してから作成します。

※プロセスツリーやESET LiveGridによるレピュテーションの評価、検出されたファイルのシグネチャーの有無などをもとに判断します。

2. 除外を作成するアラートを選択し、「CREATE EXCLUSION」をクリックします。

(複数の検出を選択して「CREATE EXCLUSION」をクリックすることで、検出情報をマージした除外が作成できます。)

3. 「Basics」画面では、作成する除外の名前や説明を入力します。

eser	PROTECT & INSPEC	Tcloud !!!			ALL COMPUTER	× a	③ HELP マ	ESET プレ	⊡ LOGOUT
		BACK w32tm.e:	ve executed [C0425]	ESET Inspect Dete	ections				
G		ſ	Ungrouped 🗢	A O i •	0 0 0	Tags	~		
▲	DETECTIONS	Detections 🖽 🦷		ECTED DETECTIONS ×	ADD FILTER			PF	
Q			S (22)	SEVERITY	PRIORITY	RESOLVED	OCCURRED TIM	1E	cc (©
უ		Rule w32tn	n.exe executed [C0425]	i			Apr 21, 2022, 4:1	1:25 PM	Win10_3
		Rule w32tn	n.exe executed [C0425]	i			Apr 22, 2022, 8:5	1:21 PM	Win10_3
		Rule w32tn	n.exe executed [C0425]	i			Apr 23, 2022, 8:1	9:09 AM	Win10_3
		Rule w32tn	n.exe executed [C0425]	i			Apr 24, 2022, 7:5	8:27 PM	Win10_3
		Rule w32tn	n.exe executed [C0425]	i			Apr 25, 2022, 1:0	7:28 PM	Win10_3
		Rule w32tn	n.exe executed [C0425]	i			Apr 26, 2022, 6:4	8:43 PM	Win10_3
		Rule w32tn	n.exe executed [C0425]	i			Apr 27, 2022, 3:5	2:23 PM	Win10_3
		Rule w32tn	n.exe executed [C0425]	i			Apr 28, 2022, 2:1	4:36 PM	Win10_3
		Rule w32tn	n.exe executed [C0425]	i			Apr 29, 2022, 7:3	6:06 AM	Win10_3
		Rule w32tn	n.exe executed [C0425]	i			Apr 30, 2022, 9:1	7:38 PM	Win10_3
		SELECTED ITEMS: 22 / 22							÷
	COLLAPSE		INCIDENT 🗢	MARK AS RESOLVED	MARK AS NOT	RESOLVED	CREATE EXCLUSION		TAGS

■メインメニュー「DETECTIONS」画面

BACK Create rule exclusion						
Basics	Neg					
Criteria	Name					
Rules	Exclusion name					
Summary	Note (optional)					
	Enter note here (max 2048 characters).					
	Continue to: Criteria					
	BACK CONTINUE CANCEL CREATE EXCLUSION					

■メインメニュー「DETECTIONS」画面





2. 手動によるチューニング(3/3)

除外のルールを設定します。

※ プロセスツリーやESET LiveGridによるレピュテーションの評価、検出されたファイルのシグネチャーの有無などをもとに判断します。

4. 「Criteria」画面では、除外のルールを作成します。 ※ 除外はプリセットされた項目からチェックボックスで条件を選択して作成できる「Basic Exclusion」とXMLで記述する自由度の高い「Advanced Exclusion」の2種類があります。

5. 除外のルールを作成したら「Rules」画面にて、「Resolve matching detections」にチェックが入っていることを確認して、 「CREATE EXCLUSION | をクリックします。

■Basic Exclusion画面			■ Advanced Exclusion画面	
Rules	Exclude processes that match one of the entered values for all selected conditions.		Criteria	Exclusion expression
Jannay			Rules Summary	Events that match the expression will not trigger detection {definition {definition
_	Entrode Processes whose will be TRUTED Elements tred is greater than or equal than TRUTED Process Newl is on d with even argone whole that with EDITEM Process whole that with EDITEM CML rel, contains /earry /status /writice EACK CONTRAL CANCEL COLATE ENCLUSION		_	BACK CONTINUE CANCEL CREATE EXCLUSION

※Advanced Exclusionでの除外の記述方法に関しては以下のPDFをご参照ください。 https://help.eset.com/tools/ei/ei rules guide 1.7.pdf



Ⅳ. その他の情報

■ EPCとEICのバージョンアップについて



- ESET PROTECT CloudとESET Inspect Cloudのバージョンアップ
 EPCとEIC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 Cloudのバージョンアップ作業に関して
 EPC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
 EPC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、EPCバージョンアップ後にEPCにログ転送を再開します。
- ・ ESET Inspect Cloudのバージョンアップ作業に関して

EIC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 EIC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、EICバージョンアップ後にEIC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。 EPC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。

▼.その他の情報 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 Cloudのオンラインヘルプ https://help.eset.com/protect_cloud/ja-JP/

ESET Inspect Cloudのオンラインヘルプ https://help.eset.com/ei_cloud/en-US/