

# ESET PROTECT MDR Lite ~インシデン<mark>ト発生時のオペ</mark>レーション~



第4版 2025年5月30日

# 目次



### . 概要

- 1. ESET MDR Lite とは
- 2. インシデント発生時の対応フロー
- II. インシデント発生時のオペレーション
  - 1. インシデント発生とメール通知
  - 2. インシデント対応状況の確認
  - 3. NW隔離からの復旧【補足】
  - 4. インシデントクローズ

### Ⅲ. まとめ

本資料について



● 本資料はEPPをすり抜けてしまった場合を前提としています。













「ESET PROTECT MDR Lite」は、ESET社運用のもと提供されるMDR(Managed Detection and Response)サービス。 低コストですぐに運用開始でき、万が一の初動対応もESET社が自動で実施。問い合わせはキヤノンマーケティング ジャパングループのエンジニアより日本語で対応・サポートいたします。





# I. 概要 ESET PROTECT MDR Liteとは

### 最短20分での脅威への対応



- 脅威が発生した場合、 最短20分で初動対応
- 例)NW隔離 →クライアント上で アラートが表示されます
- 脅威の詳細(英語)の
   確認が可能

### 24時間365日体制の脅威監視



 24時間365日お客様 環境を監視、分析

日本語でのサポート



 Webシステムより 24時間365日 お問い合わせ可能



#### 環境内で発生した インシデントの状況や EPPの状態が把握可能

セキュリティ管理 ツールよりレポート ダウンロード可能

•

I. 概要 インシデント発生時の対応フロー





Canon Marketing Japan Inc.

## <sup>I. 概要</sup> ESET Inspectご確認時の注意事項

ESET Inspectをご確認いただく際、ご注意いただきたい点をご案内いたします。 ※ESET社で脅威監視を実施しておりますので基本的にはお客さま側でESET Inspectの検知状況の確認は不要です。

#### ・「検出」アラート

一定のルールに基づいて、PCのイベントが検出されます。 検出内容はESET社で確認しているため、**アラートが上がっていてもユーザーさま側で何か対処いただく必要はありません**。 対処が必要なアラートが発生した場合は「インシデント」として作成されます。

#### ・「インシデント」について

#### 対応が必要なものは、「インシデントにユーザーのアクションが必要です」という通知が届いたインシデントのみです。 ツール(EI)上で上記以外のインシデントも自動処理により作成されますが、ESET社による確認を行っているため対応不要です。

インシデント通知は2種類あります。

- ・「インシデントにユーザーのアクションが必要です」 EI上でのステータス:「処理中」(Waiting for input) ESET側での調査の結果、お客さま側で対応が必要です。 必ずインシデントの内容確認と対処を実施ください。お客さま側で対応完了後、 ステータスを「閉じる」に設定変更をお願いいたします。 手順についてはp18をご確認ください。
- ・「ESET MDRインシデントに応答しました」

EI上でのステータス:「閉じる」

ESET側で対応完了済みですが、お客さま側で発生したインシデント内容について ご確認ください。



インシデント 🗉 🔺 😞 岁 💿 🔿 ⊘

重大度

A m

ステータス

O Waiting for input

(の)オープン

○ 閉じる
 ③ オープン



024年11月29日 16:165

24年11月29日 16:16:9

24年11月29日 15:51:4

0.4E11E12E 12:20-1



# II. インシデント発生時のオペレーション





#### ①、2 脅威監視と初動対応

通常、ESET社よりお客様環境を24時間365日脅威監視を行います。※お客様端末にインストールされたESETのログを元に監視します。 お客様環境でESETの検知ルールに引っかかる脅威の疑いがあるものが検出された場合、インシデント作成が自動で実行されます。 本サービスはそのまま初動対応まで自動で実行されますが、インシデント発生時のメール通知によりインシデントの疑いがあるものの 検知をお客様が迅速に把握することが可能です。



1. インシデント発生時のオペレーション



#### ③ メールによるインシデント把握

インシデントのメール通知によりインシデントの疑いがあるものの検知を把握し「ESET Inspect」にログインします。 ※通知メールにある「インシデントの概要を開く」をクリックいただければ「ESET Inspect」のログイン画面が表示されます。 ログイン情報を入力してログインいただければ、そのままインシデントのタイムライン画面に移動できます。

(1987) PROTECT		<ul> <li>して、紙価単純とおびGOO内を照例でき</li> <li>ジョットワークの2000時</li> <li>ジョントワークの2000時</li> <li>ジョントワークの2000時</li> <li>ジョントワークの2000時</li> </ul>	£\$.		
		◆ GBRUTHADSアイング ◆ AGBUTHADSアイング ◆ AGBUTHADEDスタダイズのスプション ◆ マログプショドフォーム対応	SIL SUSTAINE FUE	ログイン インPREET (JRXのつクドンUA - S-#ンを1082-4- アントを目 製ザーム	- )*
新しい通知 インシデントにユーザーのアクションが必要です				r(7)-P	
名前がRenamed PowerShell Execution [D0411]のインシデントは2025/05/22 11:52:10 U 対応する必要があります。	TC+9にESET MDRサービスによって作成され、すぐに			Control of the second sec	
重大度:高 影響を受けるコンビューター:				7>1:03.00001x30153055-00500009-1:33:00.7 w70-03809100343235 (6500)	( <b>2</b> H)
Oī说明:			Ing states methods are	Service and An and the service of th	Recursion and the second constraints
MDR analyst processed one of the incidents created by ESET Inspect built-in rule and	deemed necessary to provide additional conte			(anotation 	** 0** *** **
More information is provided in the Comments section of this incident.			anvina. a an	anned an The X Table Constant of the	
次のリンクからログインルで、このインシデントをすみやかに確認り、対処してください。			BY, Constitution of the anti- cold (DFC) and the anti-	An A. SALAHAR, ON FRANK, ANN ANN Y CLUB, CARE BRANCHARD, YANN ANN MENNERYLY, A	88(258-9-1) (1)(0)(0)(0)(0)(0)(0)(0)(0)(0)(0)(0)(0)(0)
https://protect.eset.com/era/webconsole/#id=INCIDENTS:id=INCIDENT_DETAILS;oid= 4753a4d69c0e:tid=34e64bf7-35ef-47aa-b652-deeeeca598e6	= <u>b530e266-e3ed-4tt4-9294-</u>		pperplant, runge		1990 - 19900 - 19900 - 19900 - 1990 - 1990 - 1990 - 1990 - 1990 - 1990 - 1990 -
			browning reads	the desired states with the second states that the desired states are stated as the desired states are states as the second states are states as the second states are states are states as the second states are states ar	Constants In the
			subject over	Contract Con	
このメッセージはESET PROTECTIこよって送信さ	hatlt				2013 m
ESET PROTECT	bonod				-
© 1352-2023 EGET, apol. 51.0. All rughts re-					
			( Income and Income an	Transferrer (1997) (1997)	





### ④-1 タイムラインに記載された実施対応・推奨対応を確認

発生したインシデントに対するESET社の対応状況をESET Inspectのタイムライン上で確認することができます。

			/ 対応状況に応じてESET社かステータスを設定します。
2024年5月24日, 17:03:09	Closed by ESET MDR.		こちらの「状況」を確認いただくことでインシデント
	ESET MDR コメントしました ESEI在の対応	心が元子した場合、	対応フニークフを確認することができます
	💙 クローズのコ	コメントが入ります。	
2024年5月24日, 17:03:08	୦୫ Certutil has dropped a suspicious executable		■設定される人ナーダ人一覧
1111 A 1	ESET MDR ステータスが変更されました 〇 閉じる		・進行中・・・・インシテント対応中
			・保留・・・・インンテント対応保留
2024年5月24日, 17:02:49	Cartutil dropped a suspicious executable, which was subsequently blocked. No actions needed		・ 解決 ・・・インシテント 対応元
		■ ESET Inspectタイムライン画面	・閉じる・・・・ユーサー影響かないと判断された場合
	List Work Live Togote	OSIET PROTECT& INSPECT :::	・冉度開く・・・・冉度インシテント作成された場合
		Certutil has dropped a suspicious executable	・無効 ・・・調査によりインシテントではなかった場合
2024年5月24日, 16:59:41	▷ certutil.exe	▲ インシテントグラフ 1 9イムライン ▲ 株本 Q コンピューター ④ 東市ファイル ▷ プロセス	
	ESET MDR プロセスが追加されました	Coord by ESET MOR.	Certati has dropped a surptious resonable
		A 2024/85/92423 1203.00 (ref Central has despend a sugestar rescalable)	
2024年5月24日, 16:59:39	Lest1-VM	BETMON 27-92/FReenaute O MCB	20年間 ロレ タグ タウ生産所
	ESET MDR コンピューターが追加されました	Central dropped a surpicious evectable, which was subsequently blocked. No actions rended     EXEMPLE INSERTION, ILXS-H-URUE	IRM MCR analysis processed one of incidents coulded by USE Inspect basis in our and deemed necessary to provide additional content for it.
		202483592483 165941 D centralese	第16(スタブーター): ▲ 2010年20、1000127年頃(1月)年登32 - 5.4 F(2) y プレルした(4011)] 1500年4004/9727 - 9.7
2024年5月24日, 16:59:39	▲ ルール - Certutilが不審な実行モジュールをドロップしました[A0313]	RETARK FORTHERENELS	11106 - Ingres Tool Toorler 11108 - Constantial Observat File or Information
	ESET MDR 検出が追加されました	2024年5月24日、16593日 💭 BHTY WM HST MDB、コンピューターが発展されました	718 
		2014年1月24日、1659.30 ▲ ホール・Cartad27年夏な東行モジュール本ドロップしました(A0211) 1017 MOR 年度が2014年1月した	
2024年5月24日, 16:59:38	> certutil.exe	2024/4/5724E.155938 El centralieur	<b>8(7.27 - 4 A</b> (1)
	ESET MDR モジュールが追加されました	ISET MORI €91-3.0 <sup>4</sup> ADEnt#Lt	(3) writiee
		2024年5月24日, 165937	70bX(0)
2024年5月24日, 16:59:37	କଟି Certutil has dropped a suspicious executable	2014年5月24日、165.0551 (ネルース・Constitが多期がおりてジュールをドロップしょくした(4011日)	Providence (REM)
	ESET MDR インシデント 作成済み	Mitre anticket*P2/2::>2 T105 - Legner Los for Andre T1140 - Decidement/Orende Titre or Information	
		Testive Demotore (748) 10: Testiticity custandemotoremetere	
2024年5月24日, 16:50:51	▲ ルール - Certutilが不審な実行モジュールをドロップしました[A0313]	Contraction (Marcon Contraction) JUEC/Marco (Contraction)	
	Mitre att&ck™テクニック		
	T1105 - Ingress Tool Transfer T1140 - Deobfuscate/Decode Files or Information こちらのタ	イムラインよりプロセスキルなど	
	してりりのフィート (Last 1-vm) (Last		
2024年5月24日, 16:49:32	▶ certutil.exe (7488) プロセスが開始されました	メントばと唯認りることかでさまり。	
	utest1-vm ≥ certutil.exe & test1-vm\eset		





#### ④-2タイムライン上に記載されたESET社のコメントを確認

インシデント対応を進める中でESET社のセキュリティエンジニアから発生したインシデントに対する、分析結果と推奨対応に関するコメント がタイムライン上に記載されます。ESET社のコメントを確認して推奨対応を実施してください。※ESET社のコメントは英語で記載されます。



12





#### 【参考】ESET社のコメント翻訳

ESET社のコメントは英語での記載になりますがブラウザ標準の翻訳機能などで簡単に日本語訳可能です。

### 例:「Google chrome」ご利用の場合

コメントを範囲選択して右クリックし、「選択範囲を日本語に翻訳」をクリック ※「Microsoft edge」なども同様に右クリックから翻訳することが可能。

2024年5月24日, 17:03:08	ब्द Certutil F	as dropped a suspicious executable ステータスが変更されました 🔵 閉じる	
2024年5月24日, 17:02:49	Certutil drop	ped a suspicious executable, which was subsequently blocked. No action	ns needed
	ESET MDR	コピー 選択箇所へのリンクをコピー	Ctrl+C
2024年5月24日, 16:59:41	Certutil	Google で「Certutil dropped a suspicious executable, which]を検索 印刷	Ctrl+P
		選択範囲を日本語に翻訳	
2024年5月24日, 16:59:39	🖵 takaha	リーディング モードで開く 新規	_
	ESET MDR	検証	
2024年5日24日 16:50:20	<b>A</b> 11 11	こう いまて変わまたて ごうし ませつい デレキレ ちゅうくつ	

## 1. インシデント発生時のオペレーション 2. インシデント対応状況の確認

【参考】インシデント発生時のお問い合わせ ご不明点等ございましたら問い合わせWebシステム「ESET Services Hub」よりお問い合わせ下さい。 キヤノンマーケティングジャパングループのエンジニアがサポートいたします。 お問い合わせの際は、ESET社のコメント全文とインスタンスIDの記載をお願いいたします。

【インスタンスID確認方法】

1. ESET Business AccountもしくはESET PROTECT Hubにログインします。

2. 画面右上 [ヘルプ]-[バージョン情報]を押下します。

3.「ESET PROTECT」、「ESET Inspect」のID情報をご連絡ください。



※ここではESET PROTECT Hubを例にご案内しておりますが、 ESET Business Accountをご利用の場合でも確認手順は同じです。





## I. インシデント発生時のオペレーション 3. NW隔離からの復旧【補足】



#### ⑤-1 NW隔離実行の把握とその対応

インシデントの初動対応は基本的に脅威駆除などが実行されますが、NW隔離が実施される場合もございます。NW隔離からの復旧 作業はお客様作業になりますので、ESET社からの推奨対応を実施したのちにNW復旧作業を実施してください。 ※NW隔離の通知設定を実施いただければ、迅速に隔離された端末を把握することが可能です。設定手順はMDR Liteスターターガイドをご参照ください。



# <sup>I. インシデント発生時のオペレーション</sup> 参考:初動対応から除外している場合 1/2



クリティカルなサーバーなどESET社による初動対応を希望しないクライアントがある場合、「MDR対応アクションの抑制」という設定を該当 クライアントまたはグループに対して有効にしておくことでESET社によるプロセス停止やネットワーク隔離などの初動対応から除外されます。

初動対応からの除外については、いつでも除外グループへの登録や解除が可能ですので、一定期間除外し問題がなさそうであればグループから外して初動対応の対象にするといった運用も可能です。

※初動対応から除外するグループの作成方法については、スターターガイドをご参照ください。

※初動対応から除外したクライアントについては、インシデント発生時の対応をお客様にて対処いただく必要がありますので、初動対応から除外するかどうかは 慎重にご判断ください。







#### 対応例: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ESET Inspect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



I. インシデント発生時のオペレーション 4. インシデントクローズ



#### ⑤-2 インシデント対応完了後の作業

インシデントに対する推奨対応の実施や復旧等完了しましたら、ESET Inspect上でインシデントのステータス設定をご変更ください。 ステータス変更にあたり不明点や疑問点等ありましたらESET Services Hubよりお問い合わせください。

			無効	Ø	<ul> <li>◎ ヘレブマ</li> <li>パ</li> <li>ペ</li> <li>8</li> <li>.</li> <li>.</li></ul>
●● ダッシュボード	戻る 検出の	インシデント: コマンドラインからのユーザー/グループの管理[B1003]		(	
□ □ □ □ □ □ □ □ 2 2 - 9-	☆ インシデントグラス	ステータスと担当者の変更	×		1. ESET Inspectへログインします。
・     インシテント       ・     検索       ・     検出       ・     実行ファイル       ・     スクリプト       ・     減知	2025年2月26日, 09:47:2 2025年2月26日, 09:47:2 2025年2月26日, 09:47:2	ステータス 閉じる このインシデントをクローズするための解決策を選択してください	₩.	0125721	<ul> <li>2. 画面左側のメニューより「インシデント」をクリックし、 該当のインシデントを選択します。</li> <li>3. 画面下部の「ステータスと担当者の変更」をクリックします。 表示項目に沿って入力します。</li> <li>■ステータス: "閉じる"を選択します。</li> </ul>
··· 詳細 〉	> 2025年2月26日, 09:47:1	<ul> <li>              兵陽性(実际の攻撃)      </li> <li>             不審(実際の攻撃であった可能性があります)         </li> <li>             設検知または無効         </li> </ul>	= . 	- <b>タ</b> − (1) コマンドライン :ck <sup>™</sup> テクニック	■このインシデントをクローズするための解決策の選択: インシデントの状況に合わせて以下3つの項目より設定します。
	2025年2月26日, 09:47:1 2025年2月25日, 18:37:5	コメント - 仕息 ここに任意のコメントを入力します(最大4000文字)。	kcci	count Manipulat eate Account count Access Re - (1)	anplate       1. 実际の以事であった場合         ount       : 攻撃であった可能性がある場合         ・ 沢検知または無効: 誤検知または問題がなかった場合         ※選択に迷う場合は、"不審"をご選択ください。
					■ <b>コメント</b> :任意でご入力ください。
	2025年2月25日, 18:34:4			(1) I.exe	<ol> <li>「保存」をクリックして完了です。</li> <li>該当インシデントのステータスが「閉じる」に変更されている</li> <li>ことをご確認ください。</li> </ol>
三 折りたたみ	1>57>下▼		Powershell.	.exe (3376)	



# 11.まとめ

まとめ





本資料はインシデント発生時のお客様対応を中心にお伝えした内容となっておりますが、 負荷の高い常時監視やインシデント発生時の初動対応などはESET社で対応いたしますのでご安心ください。