

ESET PROTECTソリューション ランサムウェア対策の機能について

第3版
2025年3月27日

Canon

キヤノンマーケティングジャパン株式会社

もくじ

1. はじめに
2. ランサムウェアの脅威と被害
3. ランサムウェア対策機能について
4. 参考情報

1. はじめに

1.はじめに

ランサムウェア攻撃の手法は年々、高度化・巧妙化しており、近年は「ダブルエクストーション(二重の脅迫)」といった、ファイルの暗号化に加えて幾重にもわたって脅迫を行うような手法も多く確認されています。

そのためランサムウェア被害に対しての事前対策や、攻撃を受けてしまった場合の復旧対応が必要です。

ESET PROTECTソリューションでは、ランサムウェアに対して侵入や実行を防ぐ保護機能から万が一暗号化されてしまった際のファイルの修復機能までを提供します。

本資料はESET PROTECTソリューションの以下の製品を対象としております。

プログラム名	備考
ESET Endpoint Security	Windows クライアントOS向け総合セキュリティプログラム
ESET Endpoint アンチウイルス	Windows クライアントOS向けウイルス・スパイウェア対策プログラム

- 本資料は、本資料作成時のソフトウェア及びハードウェアの情報に基づき作成されています。ソフトウェアのバージョンアップなどにより、記載内容とソフトウェアに記載されている機能、名称及び画面などが異なっている場合があります。また、本資料の内容は将来予告なく変更することがあります。
- 本製品の一部またはすべてを無断で複写、複製、改変することはその形態に問わず、禁じます。
- ESET、LiveGrid、ESET Endpoint Security、ESET Endpoint アンチウイルス、ESET Server Security、ESET PROTECTは、ESET, spol. s r.o. の商標です。
- Microsoft、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。

2. ランサムウェアの脅威と被害

2.ランサムウェアの脅威と被害

(1) ランサムウェアとは？

ランサムウェアはマルウェアの一種であり、PCやサーバー内に保存しているデータを暗号化し使用不能にしてしまうため、最悪の場合業務停止に陥ってしまうこともあります。「この暗号化を解除するためには身代金を払え」と要求することから、**Ransom(身代金)**と**Software(ソフトウェア)**を組み合わせ、**Ransomware(ランサムウェア)**と命名されました。近年、このランサムウェアを使用した攻撃が非常に多く発生しており、**社会問題化**しています。

支払期限をカウントダウン表示し、被害者の焦燥感を煽ります。



脅迫文はあらゆる言語で表示できるようになっており、全世界的に流行していることがわかります。

600ドルをbitcoinで支払えというメッセージと共に送信先のアドレスが記載されています。

2.ランサムウェアの脅威と被害

(2)「情報セキュリティ10大脅威」から見るランサムウェアの流行

下記は2021～25年までの情報セキュリティ10大脅威(組織)の結果から1～3位を抜粋したものです。

2025年

- 1位. **ランサム攻撃による被害**
- 2位. サプライチェーンや委託先を狙った攻撃
- 3位. システムの脆弱性を突いた攻撃

2024年

- 1位. **ランサムウェアによる被害**
- 2位. サプライチェーンの弱点を悪用した攻撃
- 3位. 内部不正による情報漏えい

2021年～2025年まで**5年連続1位**

2023年

- 1位. **ランサムウェアによる被害**
- 2位. サプライチェーンの弱点を悪用した攻撃
- 3位. 標的型攻撃による機密情報の窃取

2022年

- 1位. **ランサムウェアによる被害**
- 2位. 標的型攻撃による機密情報の窃取
- 3位. サプライチェーンの弱点を悪用した攻撃

2021年

- 1位. **ランサムウェアによる被害**
- 2位. 標的型攻撃による機密情報の窃取
- 3位. テレワーク等のニューノーマルな働き方を狙った攻撃

Point

ここまでランサムウェア被害が蔓延、常態化した背景には**RaaS** ※のような専門知識がなくても誰でもランサムウェア攻撃を仕掛けることが可能になる悪質なサービスが広まったことが一因として挙げられます。

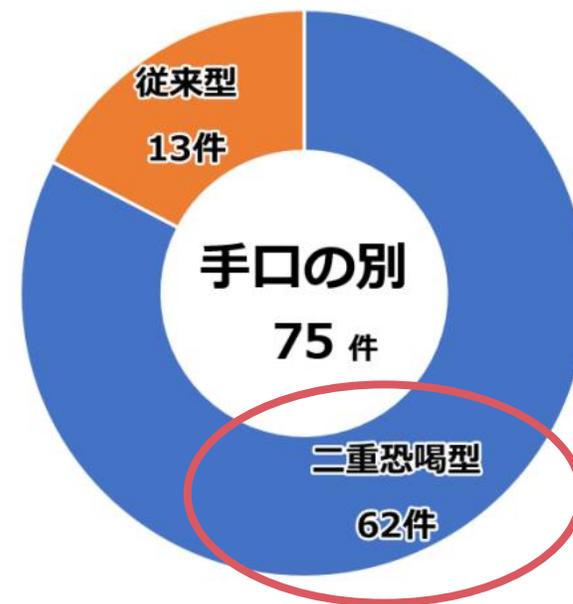
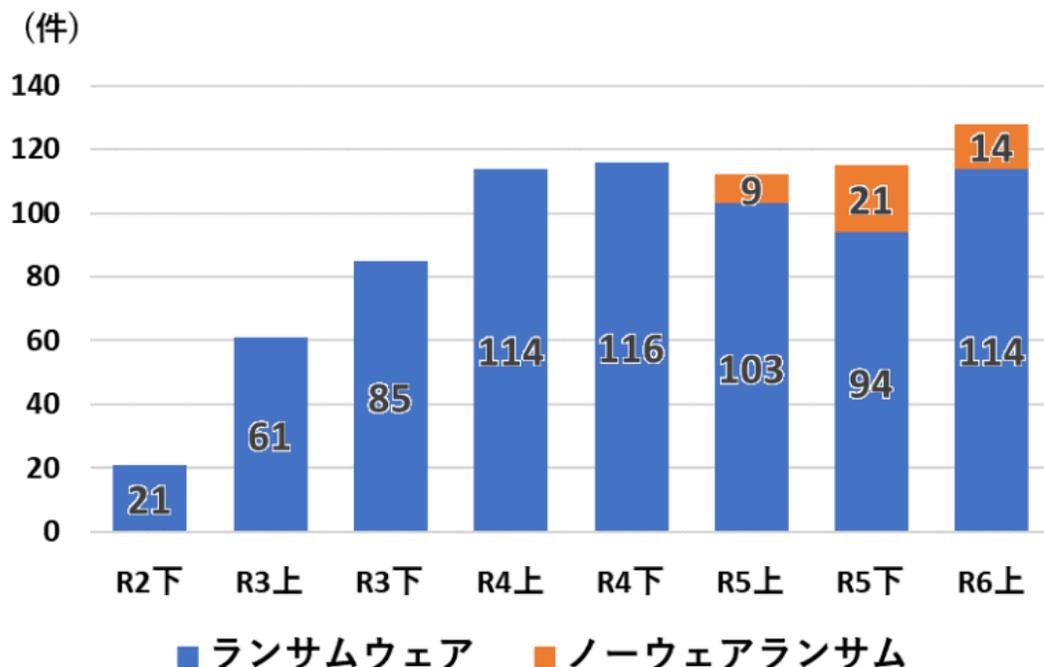
※情報セキュリティ10大脅威・・・その年ごとに発生した社会的に影響が大きかったと考えられる情報セキュリティにおける事案から、IPAが脅威候補を選出し、専門家約200名のメンバーからなる「10大脅威選考会」が脅威候補に対して審議・投票を行い決定したものを。

※Ransomware as a Service・・・サイバー犯罪者がランサムウェアによる攻撃をサービスとして提供・実行するビジネスモデル

2.ランサムウェアの脅威と被害

(3)ランサムウェアの被害報告件数推移と手法

企業・団体などにおけるランサムウェア被害の報告件数は2021年に急激に増加し、近年は**高止まり傾向**にあります。そのほとんどの場合は、暗号化を実施したうえで窃取した情報を公開すると迫ってくる「**二重恐喝型ランサムウェア**」と呼ばれる手法がとられています。さらに、近年は従来のランサムウェアとは異なり、暗号化せずにデータを盗み、身代金を払わなければダークウェブ上に公開すると脅す「**ノーウェアランサム**」と呼ばれるランサムウェアまで登場しています。



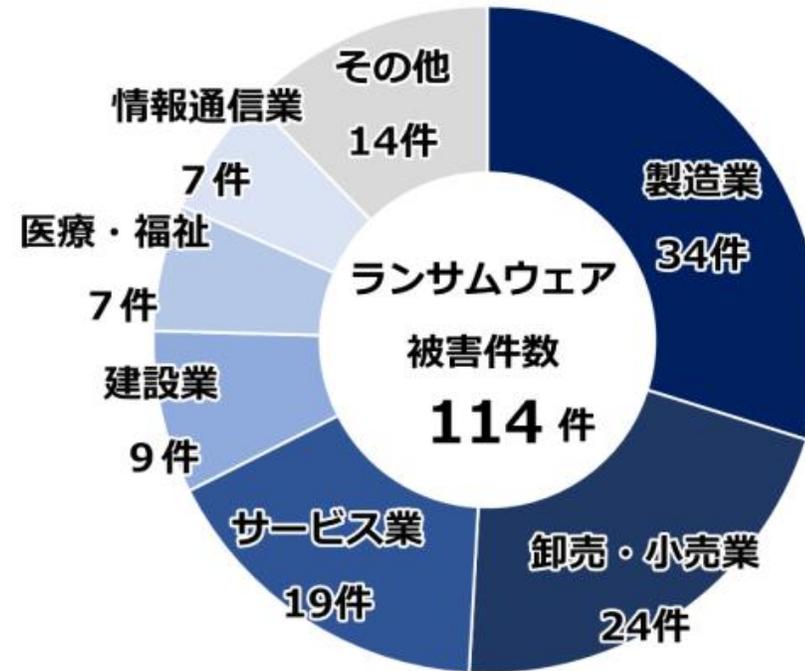
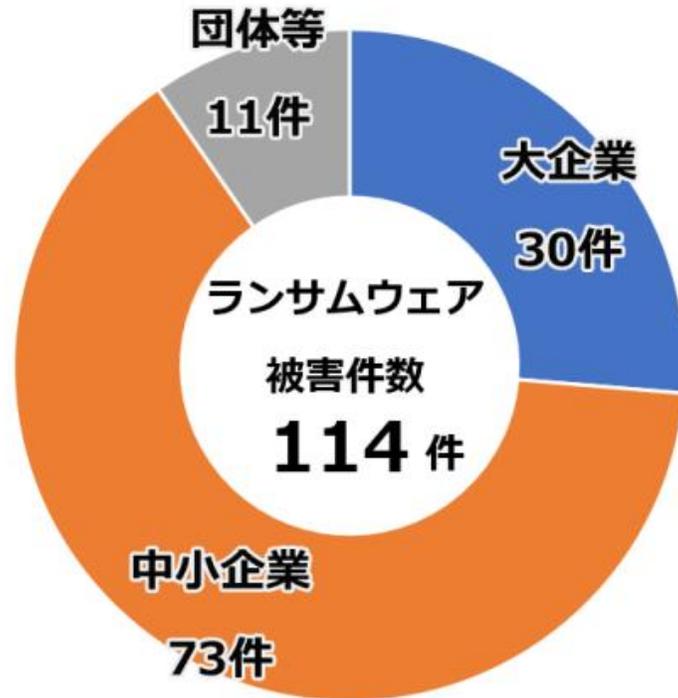
約8割が二重恐喝型

2.ランサムウェアの脅威と被害

(4)ランサムウェアの被害を受けている企業・業種について

企業の規模・業種問わず、多種多様な企業でランサムウェアの被害事例が報告されています。

万が一ランサムウェアに感染してしまうと、自身の企業だけではなく**サプライチェーン全体の業務や取引にまで被害が及んでしまう**可能性があります。



出典：▽令和6年上半期におけるサイバー空間をめぐる脅威の情勢等について

https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6kami/R06_kami_cyber_jousei.pdf

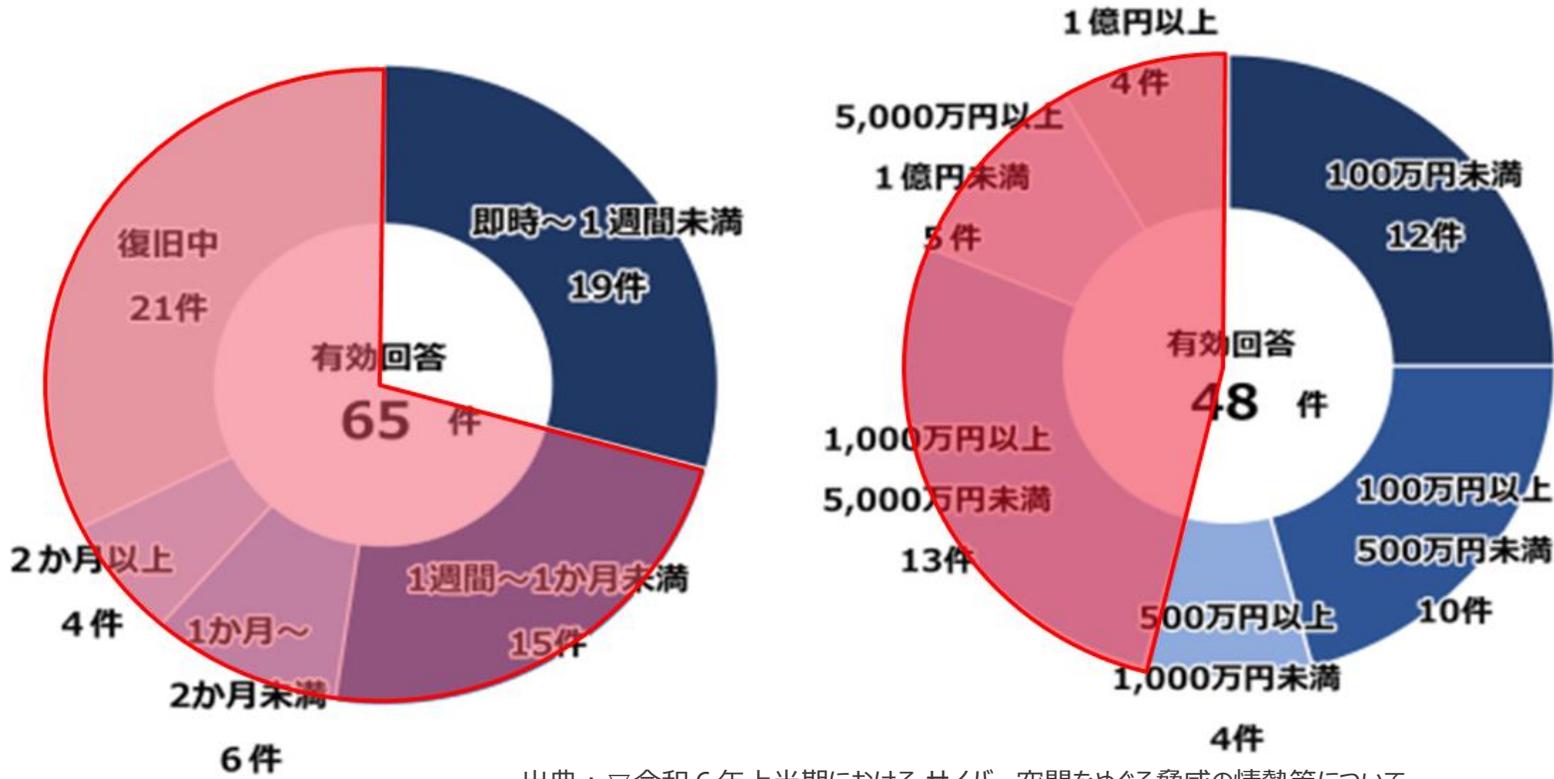
2.ランサムウェアの脅威と被害

(5)ランサムウェア被害からの復旧期間と費用について

ランサムウェアに感染した際の復旧には時間と多額の費用が必要になります。

7割以上の企業で復旧には**1週間以上**、約半数の企業で**1000万円以上**の費用がかかっています。

また、**1度被害に遭ってしまった企業は攻撃が成功しやすい企業として何度も狙われてしまう可能性が高い**ともいわれています。



**復旧に1週間以上
71% (復旧中含む)**

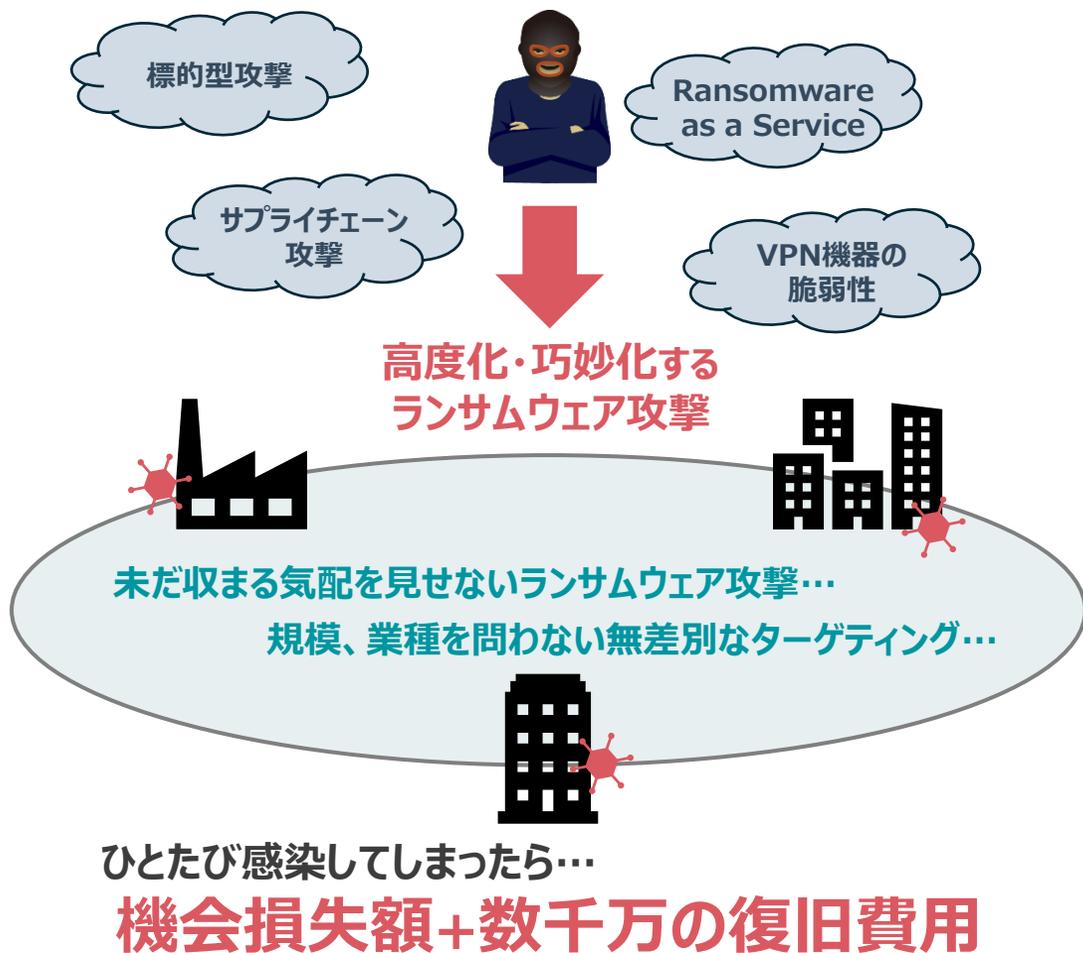
**復旧費用
100万円以上
46%**

出典：▽令和6年上半期におけるサイバー空間をめぐる脅威の情勢等について

https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6kami/R06_kami_cyber_jousei.pdf

2.ランサムウェアの脅威と被害

(6)ランサムウェアの被害を防ぐには



警察庁が公開している

「ランサムウェア被害防止対策」

- ✓ VPN機器等の脆弱性を塞ぐ
- ✓ 認証情報を適切に管理する
- ✓ アクセス権等の権限を最小化する

各種セキュリティ対策や
設定の見直し

- ✓ ウイルス対策ソフト等を導入する ☆
- ✓ 電子メール等を警戒する ☆
- ✓ ネットワークを監視する ☆
- ✓ データ等のバックアップを取得する ☆

ESETの各種機能で
対策可能！

本資料でご紹介！

エンドポイント対策が
最後の砦です！

出典：警察庁「ランサムウェア被害防止対策」

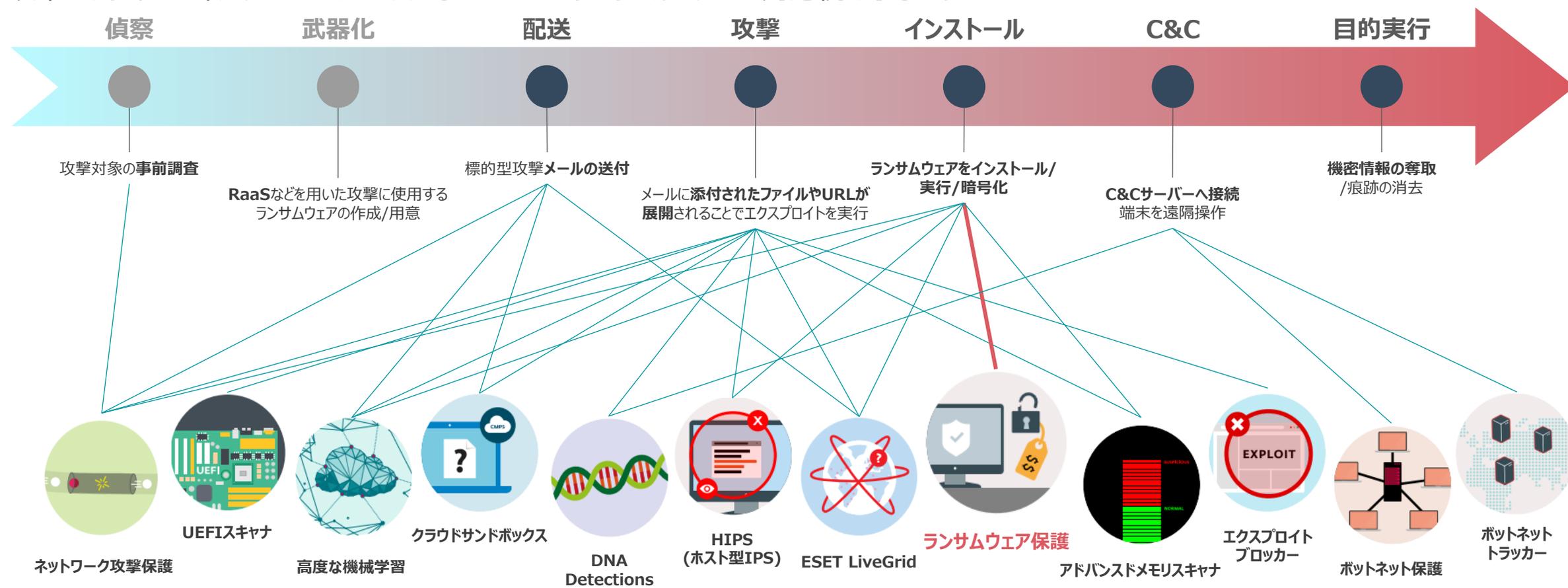
<https://www.npa.go.jp/bureau/cyber/countermeasures/ransom.html>

3. ESETのランサムウェア対策機能について

3.ランサムウェア対策機能の概要

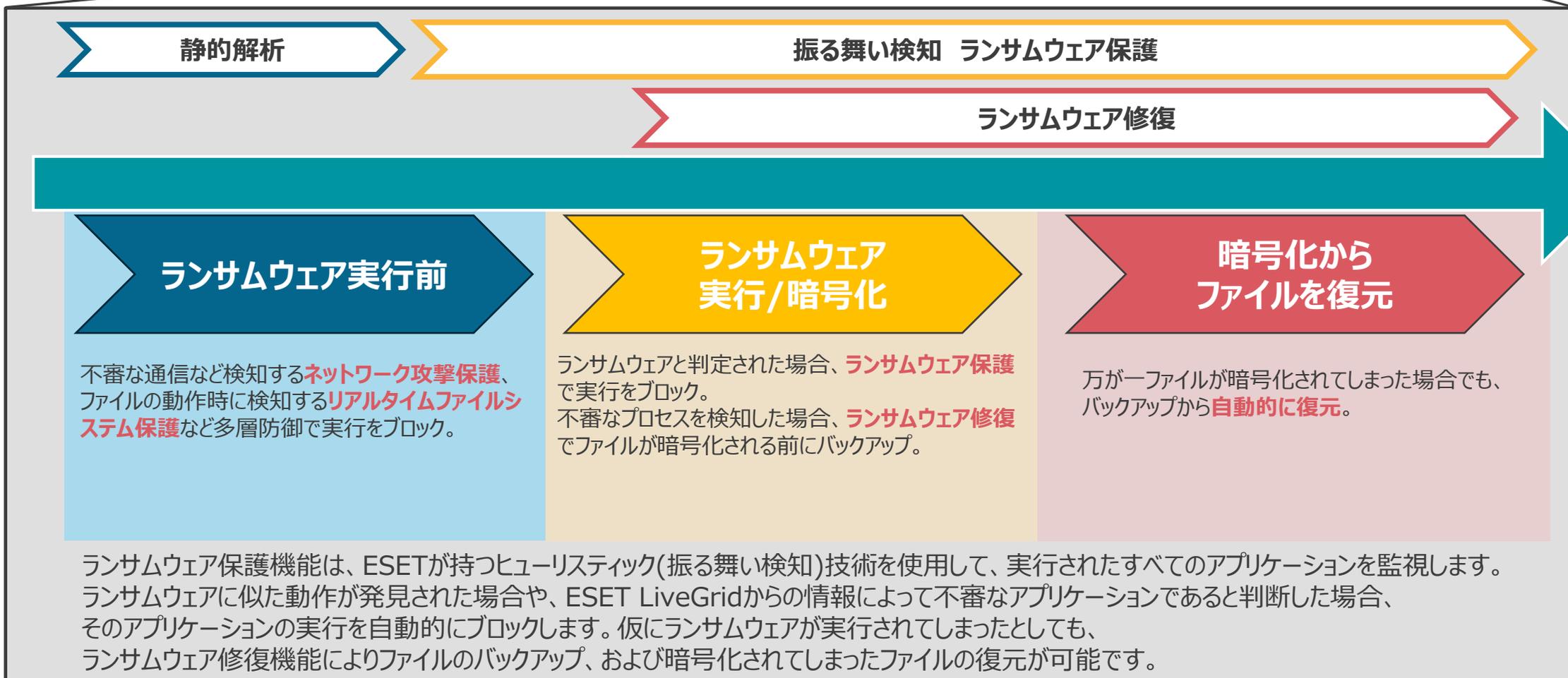
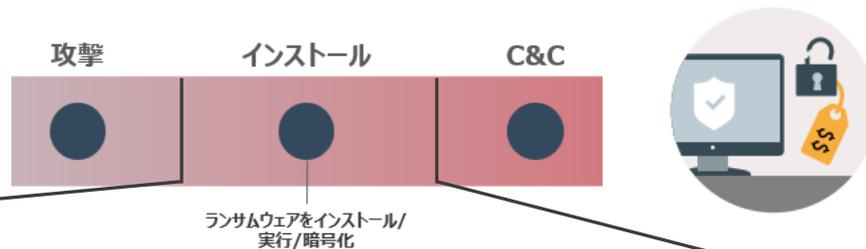
(1)ESETの多層防御について

ESET製品はランサムウェアなどのマルウェアに対し、多層防御による様々なタイミングのアプローチで対応します。以下に、サイバーキルチェーンをベースにしたESETのランサムウェアへの対応例を示します。



3.ランサムウェア対策機能の概要

(2) ランサムウェア対策機能について

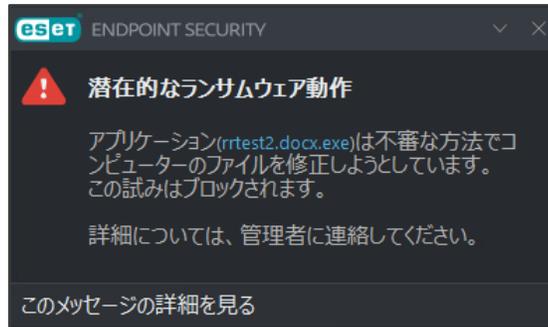


3.ランサムウェア対策機能の概要

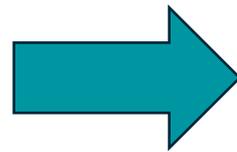
(3) 検知時のポップアップについて

ESETのランサムウェア対策機能には「ランサムウェア保護機能」、「ランサムウェア修復機能」の2つがあります。各機能が実行された際はそれぞれ以下のポップアップ画面が表示されます。また復元されたファイルの一覧についても確認できます。

ランサムウェア保護機能のポップアップ



ランサムウェア修復機能のポップアップ



ランサムウェア修復機能によって復元されたファイルの一覧画面

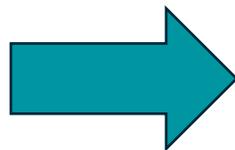
ファイル	最終変更日時
C:\temp\confidential\個人情報_1.docx	2025/02/06 10:14:00
C:\temp\confidential\個人情報_10.docx	2025/02/06 10:14:00
C:\temp\confidential\個人情報_2.docx	2025/02/06 10:14:01
C:\temp\confidential\個人情報_3.docx	2025/02/06 10:14:01
C:\temp\confidential\個人情報_4.docx	2025/02/06 10:14:01
C:\temp\confidential\個人情報_5.docx	2025/02/06 10:14:01
C:\temp\confidential\個人情報_6.docx	2025/02/06 10:14:01
C:\temp\confidential\個人情報_7.docx	2025/02/06 10:14:01
C:\temp\confidential\個人情報_8.docx	2025/02/06 10:14:01
C:\temp\confidential\個人情報_9.docx	2025/02/06 10:14:01
C:\temp\confidential\機密情報_1.docx	2025/02/06 10:14:01
C:\temp\confidential\機密情報_10.docx	2025/02/06 10:14:01
C:\temp\confidential\機密情報_2.docx	2025/02/06 10:14:01

3.ランサムウェア対策機能の概要

(4) 復元されたファイルについて

ランサムウェア修復機能によって復元されたファイルは元ファイル名の末尾に「_restored」が追加され、元々存在していたフォルダ内に復元されます。

名前	更新日時	サイズ
機密情報_1.docx	2025/02/06 9:11	1 KB
機密情報_2.docx	2025/02/06 9:11	1 KB
機密情報_3.docx	2025/02/06 9:11	1 KB
機密情報_4.docx	2025/02/06 9:11	1 KB
機密情報_5.docx	2025/02/06 9:11	1 KB
機密情報_6.docx	2025/02/06 9:11	1 KB
機密情報_7.docx	2025/02/06 9:11	1 KB
機密情報_8.docx	2025/02/06 9:11	1 KB
機密情報_9.docx	2025/02/06 9:11	1 KB
機密情報_10.docx	2025/02/06 9:11	1 KB
個人情報_1.docx	2025/02/06 9:21	1 KB
個人情報_2.docx	2025/02/06 9:21	1 KB



名前	更新日時	サイズ
機密情報_1.docx	2025/02/06 10:13	1 KB
機密情報_1_restored.docx	2025/02/06 10:14	1 KB
機密情報_2.docx	2025/02/06 10:13	1 KB
機密情報_2_restored.docx	2025/02/06 10:14	1 KB
機密情報_3.docx	2025/02/06 10:13	1 KB
機密情報_3_restored.docx	2025/02/06 10:14	1 KB
機密情報_4.docx	2025/02/06 10:13	1 KB
機密情報_4_restored.docx	2025/02/06 10:14	1 KB
機密情報_5.docx	2025/02/06 9:11	1 KB

 機密情報_1.docx	…暗号化されたファイル	2025/02/06 10:13	1 KB
 機密情報_1_restored.docx	…復元されたファイル	2025/02/06 10:14	1 KB

3.ランサムウェア対策機能の概要

(5) ESETのバックアップ技術について

ESETは独自のバックアップ技術を採用しており、一般的なバックアップ技術であるボリュームシャドウコピーサービス※(VSS)とは異なる方法でファイルをバックアップします。

バックアップとしてVSSの使用を避けるべき理由

- 一般的な技術のため、攻撃者側も対策が容易であり、バックアップファイルが**破損・消去・無効化**される可能性がある
 - Microsoftの正規のツールを悪用して**バックアップデータの制御が可能**
 - ランサムウェアによっては**VSSを無効化**した上で暗号化を行ったり、VSS内のファイルまで暗号化し、**元データを削除する機能**を持つ場合もある

ESETはVSS未使用かつ、多段構えでバックアップデータを保護

- VSSとは**異なる独自の技術でバックアップ**しており、バックアップデータは自己防衛機能にて保護
 - ☆自己防衛機能：悪意のあるソフトウェアによってESET自身の保護機能が**無効化**されたり、改ざんされたりしないようにする機能
 - 特定のフォルダにデータをバックアップし、自己防衛機能で**不正なプロセスによるバックアップフォルダへの干渉を防止**

補足：ランサムウェア保護機能について

ランサムウェア保護機能詳細

ランサムウェア保護は、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ます。

悪意のあるアプリケーションの動作が発見された場合や、ESET LiveGridからの情報によって不審なアプリケーションであると判断した場合、そのアプリケーションを自動的にブロックします。 ※この機能の精度を高めるには、ESET LiveGridを有効にする必要があります。

詳細設定(HIPS画面)



「ランサムウェア保護」
ファイルに対して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検出します。該当のアプリケーションをブロックします。

補足：ランサムウェア修復機能

ランサムウェア修復機能詳細

ランサムウェア修復は実行ファイルに変更を加えた場合など、不審なプロセスを検知した際にファイルをバックアップし、ランサムウェア検出後に暗号化されたファイルを復元することが可能です。

本機能は、ESET PROTECT Advanced、Complete、Enterprise、Eliteのいずれかのライセンス、かつセキュリティ管理ツール※で管理している環境でご利用いただけます。対応OSはWindows クライアントのみとなります。(2025年3月現在) ※ESET Management エージェント V12.0以降での管理が必要です。



詳細設定(HIPS画面)

「ランサムウェア攻撃後にファイルを復元」
ランサムウェア対策機能を強化するため、ドキュメントのバックアップを実行し、検出後に暗号化されたファイルを復元します。

「保護されているファイルタイプのリスト」
ランサムウェア修復機能の対象のファイルタイプを設定することができますを追加したり、一般的に保護および監視されるファイルタイプの既存のリストを編集したりできます。

「除外されたフォルダーのリスト」
特定のフォルダをバックアップ対象外に設定できます。

※既定でのバックアップ対象拡張子は以下の通りです。対象の拡張子はカスタマイズ可能です。

"aif","cda","mid","midi","mp3","ogg","wav","wma","wpl","7z","arj","deb","pkg","rar","tar","gz","z","zip","csv","dat","db","dbf","mdb","sav","sql","tar","xml","bat","bin","py","wsf","com","jar","bat","cgi","pl","ai","bmp","gif","ico","jpeg","jpg","png","ps","psd","svg","tif","tiff","asp","aspx","css","htm","html","js","jsp","php","ppt","pps","odp","key","pptx","c","class","cpp","cs","h","java","sh","swift","vb","ods","xlr","xls","xlsx","3g2","3gp","avi","flv","h264","m4v","mkv","mov","mp4","mpg","mpeg","rm","swf","vob","wmv","doc","docx","odt","pdf","rtf","tex","txt","wks","wps","wpd"

補足：ランサムウェア対策機能

ランサムウェア対策機能の利用条件詳細

ランサムウェア対策機能利用にあたり、以下の環境が必要です。

○ランサムウェア保護

- ① Windowsクライアント向け、またはWindowsサーバー向けESETプログラムを利用している

○ランサムウェア修復

- ① Windowsクライアント向けESETプログラムを利用している
- ② セキュリティ管理ツールが構築されている
- ③ ESET Management エージェント V12.0以降にてエンドポイントの管理が行われている
- ④ ESET PROTECT Advanced、Complete、Enterprise、Eliteのいずれかのライセンスを利用している

プログラム名		バージョン	
		V11.1以下	V12.0以降
ESET Endpoint Security (EES)	Windowsクライアント向け総合セキュリティプログラム	×	○
ESET Endpoint アンチウイルス (EEA)	Windowsクライアント向けウイルス・スパイウェア対策プログラム	×	○

補足：上位ライセンスのご紹介

上位ライセンスを利用するメリットについて

ランサムウェア修復機能はAdvanced以上のライセンスで利用可能です。

上位ライセンスはランサムウェア修復機能に加えて様々なセキュリティ対策機能が利用可能であるため、併せてご検討ください。

- 各ラインアップで利用できる機能

	セキュリティ管理ツール	ウイルス対策プログラム	ランサムウェア保護機能	ランサムウェア修復機能	フルディスク暗号化	クラウドサンドボックス	クラウドアプリケーションセキュリティ	脆弱性・パッチ管理	XDR (侵入検知)	多要素認証
ESET PROTECT MDR	○	○	○	○	○	○	—	—	○	—
ESET PROTECT Elite	○	○	○	○	○	○	○	○	○	○
ESET PROTECT Complete	○	○	○	○	○	○	○	○	—	—
ESET PROTECT Advanced	○	○	○	○	○	○	—	—	—	—
ESET PROTECT Entry	○	○	○	—	—	—	—	—	—	—

⇒Advanced以上のライセンスでは、クラウドサンドボックス、フルディスク暗号化、XDRをはじめとした様々なソリューションが利用できます。上位ライセンスをご利用いただくと、強力なランサムウェア対策に加え、標的型攻撃対策や脆弱性管理、侵入後の対策まで**トータルでのセキュリティ対策が可能**になります。

4. 参考情報

4. 参考情報

よくある質問集

- Q. ランサムウェア修復機能のバックアップは手動または自動のどちらで実行されますか？
A. 自動でバックアップ、修復が実行されます。
- Q. ランサムウェア修復機能で保護できるファイルタイプ(拡張子)の設定はできますか？
A. 設定可能です。
- Q. ランサムウェア修復機能には除外設定はできますか？
A. フォルダ単位で除外の設定が可能です。
- Q. ランサムウェア修復機能をセキュリティ管理ツールを利用せずにクライアント単独で利用することができますか？
A. いいえ、できません。セキュリティ管理ツールによる管理を実施する必要があります。
- Q. ランサムウェア修復機能にて保存されるバックアップファイルはどのように保存されますか？
A. バックアップファイルは暗号化されて保存されます。

4. 参考情報

よくある質問集

Q. ランサムウェア修復機能で保護できるサイズの上限はありますか？

A. 30MBが上限です。1ファイルにつき30MBより小さいファイルのみバックアップされます。バックアップファイルの総容量についての制限はなく、ディスク容量があればバックアップ可能ですが、ローカルシステムドライブに空き容量がない場合はバックアップできませんのでご注意ください。

Q. バックアップ用に確保すべき空き容量の目安はありますか？

A. 1ファイルあたりのファイルサイズを500KBとした場合、約12.5GB程度確保されていることが望ましいです。
※Lockbitが1分間に暗号化できるファイル数(約25000ファイル)を元に算出

Q. ランサムウェア修復機能の実際の挙動を確認する方法はありますか？

A. デモ動画(英語)で挙動をご確認ください。
▽ESET Ransomware Remediation Demo
<https://www.youtube.com/watch?v=ifMOvoHEVbQ>