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1版
2024年2月5日

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(本資料について)
2. ランサムウェアの脅威と被害
3. ESETの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(本資料について)

1.はじめに(本資料について)

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）」、「トリプルエクストーション（三重の脅迫）」といったように、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、万が一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、ランサムウェア対策の機能が搭載されております。

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 クライアント端末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 クライアント端末OS向け ウイルス・スパイウェア対策プログラム

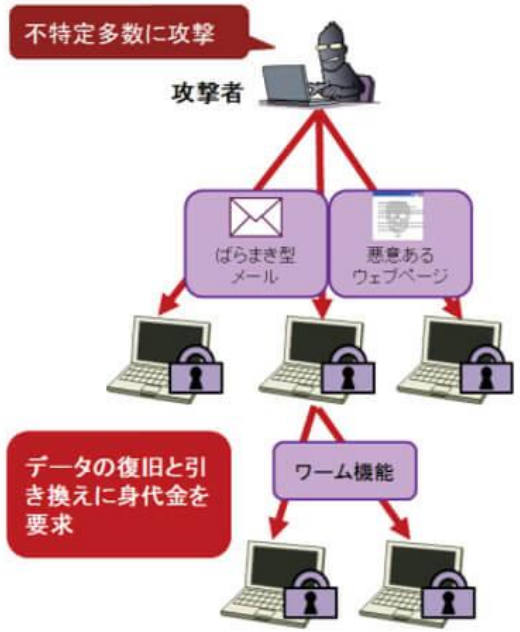
- 本資料は、本資料作成時のソフトウェア及びハードウェアの情報に基づき作成されています。
  ソフトウェアのバージョンアップなどにより、記載内容とソフトウェアに記載されている機能、名称及び画面などが異なっている場合があります。また、本資料の内容は将来予告なく変更することがあります。
- 本製品の一部またはすべてを無断で複写、複製、改変することはその形態に問わず、禁じます。
- ESET、LiveGrid、ESET Endpoint Security、ESET Endpoint アンチウイルス、ESET Server Security、ESET PROTECT Cloud 、 ESET PROTECT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（Ransomware）は、マルウェアの一種です。
感染するとPCやデバイス内に保存しているデータが勝手に暗号化されてアクセスできなくなったり、
PCやデバイスが操作不能に陥ったりします。暗号化を解除するために、身代金を要求することから、
「Ransom（身代金）」と「Software（ソフトウェア）」を組み合わせた「ランサムウェア（Ransomware）」と命名されました。



出典：https://www.ipa.go.jp/files/000084974.pdf

出典：https://www.police.pref.osaka.lg.jp/seikatsu/saiba/cyber_cyuikanki/6936.htm

2.ランサムウェアの脅威と被害

(2)多様化するランサムウェア

ランサムウェアが急増した背景には、ランサムウェアの多様化があります。
サイバー犯罪者から見れば、ランサムウェアは一つのビジネスとして成り立っており、手を変え品を変え、
被害者からいかに金銭を巻き上げるかを考え、日々開発が続けられています。以下はその代表例です。

・二重脅迫型ランサムウェア

二重脅迫型ランサムウェアの場合は、「データを取り戻したければ、身代金を払え」と1度目の脅迫をした後、
さらに「身代金の支払いを拒むようなら、暗号化したデータを外部に公開する」と2度目の脅迫を行います。

・Ransomware as a Service（RaaS）

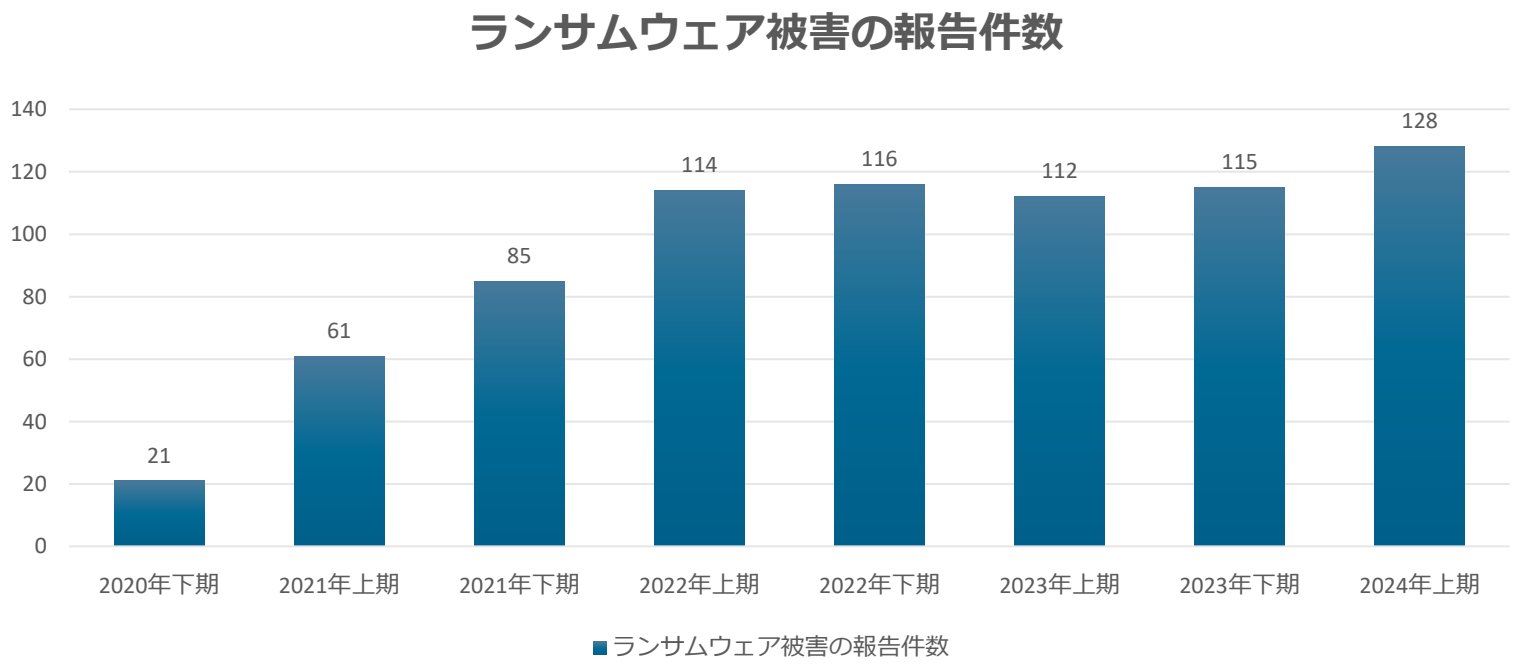
RaaSとは、ランサムウェア攻撃をクラウドサービス化したものです。
サイバー犯罪者がランサムウェアを販売したり、攻撃に成功した場合の利益を分配する条件で攻撃を代行したりするものを指します。
“知識がなくても・誰でも・簡単に“ランサムウェア攻撃を仕掛けることができます。

▽ランサムウェアのキホン
https://www.eset.com/jp/topics-business/new-double-extortion-ransomware/?srsltid=AfmBOop5wH3vk7FVFAe-i7rNtv3y5OADuaVtP0yL2rq5hHO1WenHJS87

2.ランサムウェアの脅威と被害

(3)ランサムウェアの流行について

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年々増加しております。
ランサムウェアによって流出したとみらえる事業者などの情報がダークウェブなど不正なサイトに掲載されていたことが確認されており、
端末暗号化以外の被害も発生しております。

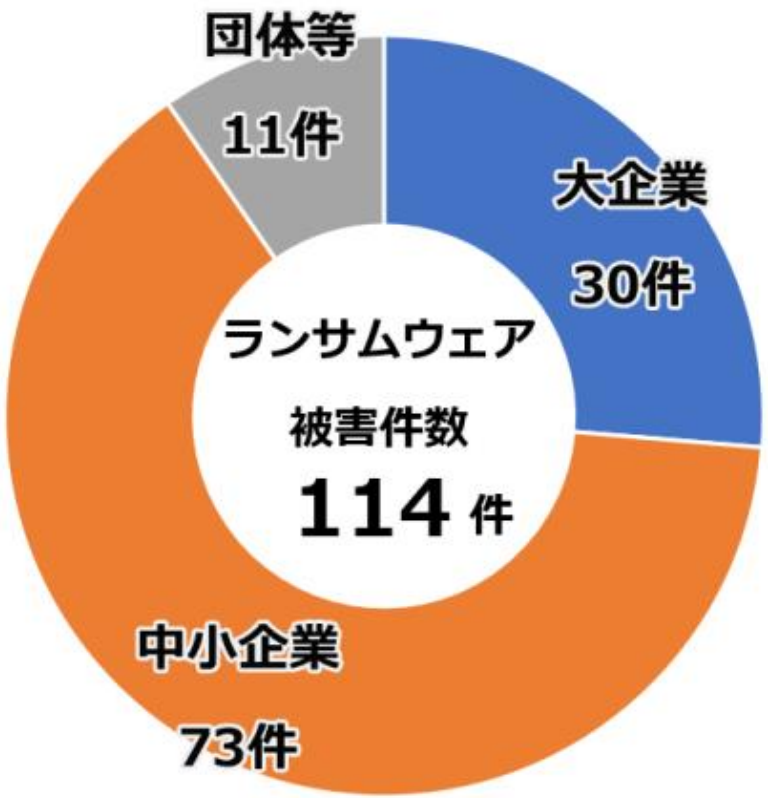


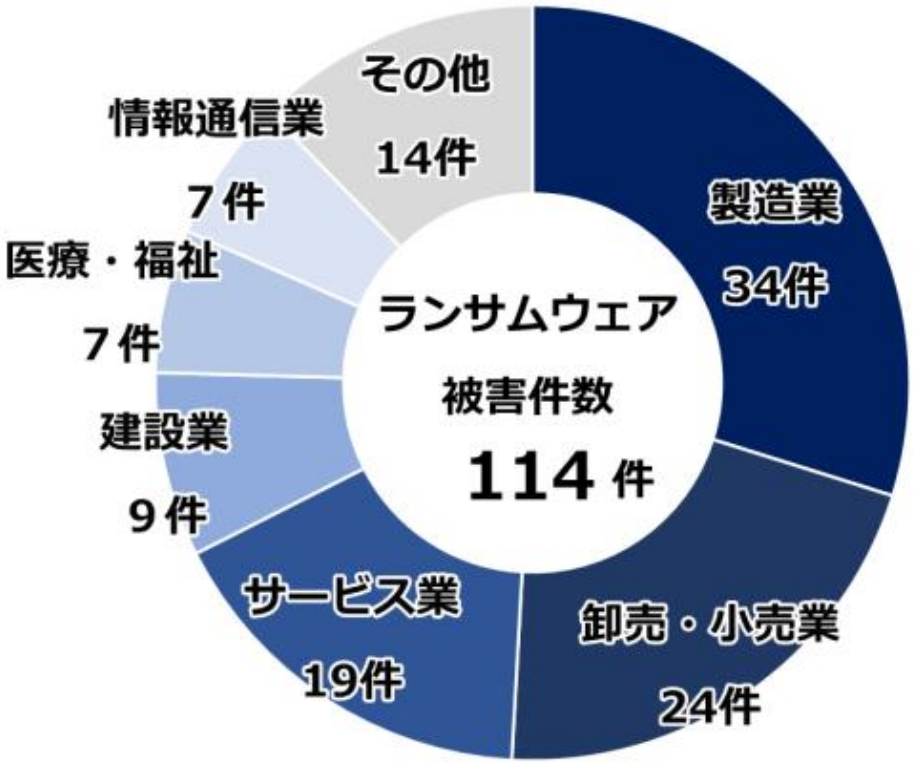
▽令和６年上半期における サイバー空間をめぐる脅威の情勢等について
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6kami/R06_kami_cyber_jousei.pdf

2.ランサムウェアの脅威と被害

(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おり、その対策は急務といえます。



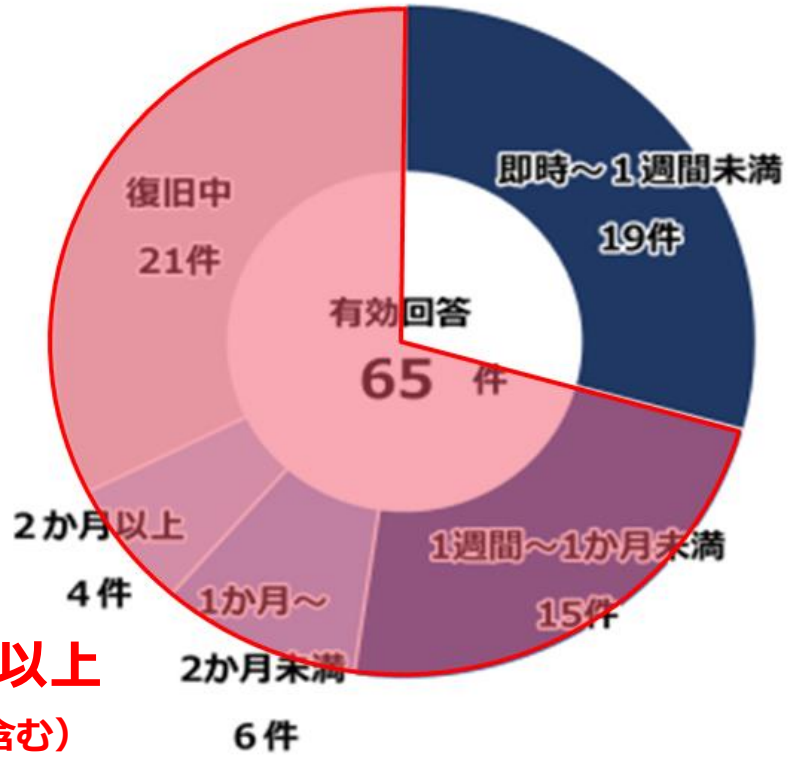


▽令和６年上半期における サイバー空間をめぐる脅威の情勢等について
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6kami/R06_kami_cyber_jousei.pdf

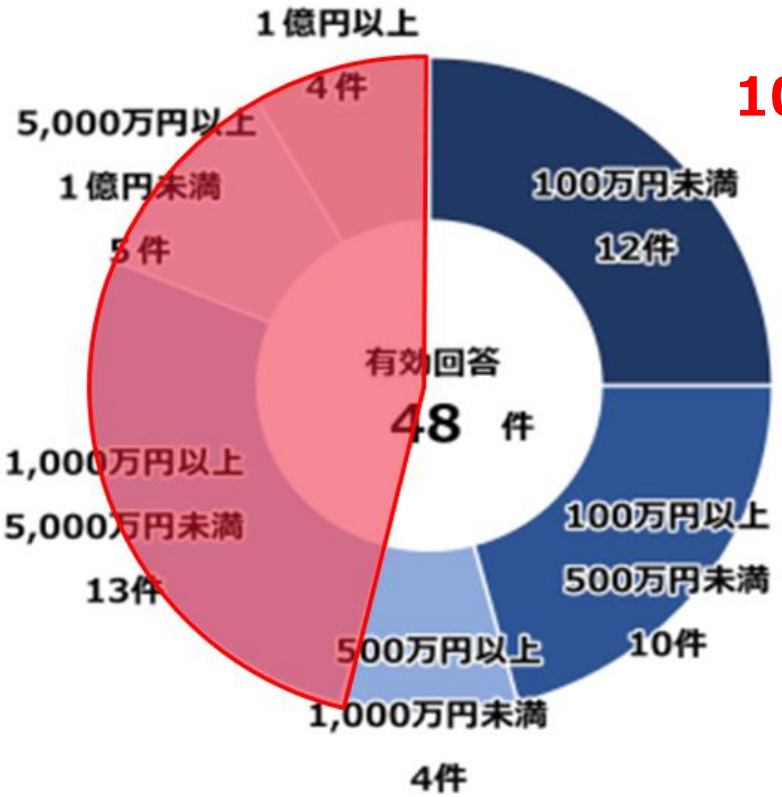
2.ランサムウェアの脅威と被害

(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費用が発生します。



復旧に1週間以上
71%（復旧中含む）



復旧費用
1000万円以上
46%

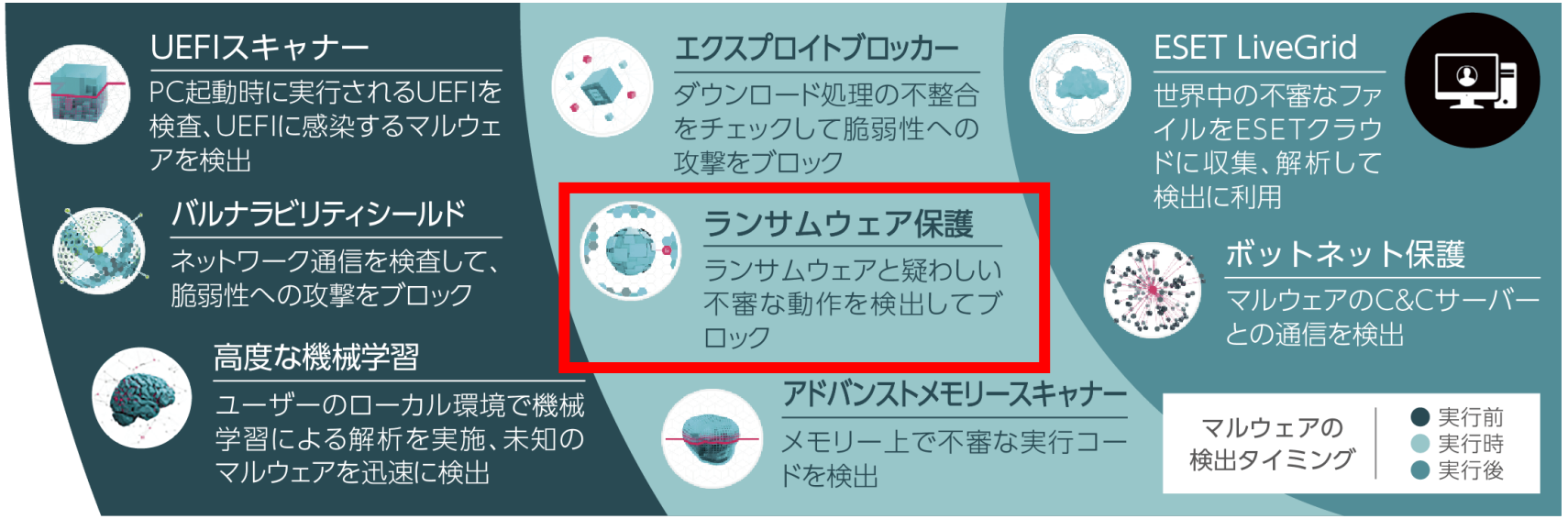
▽令和６年上半期における サイバー空間をめぐる脅威の情勢等について
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6kami/R06_kami_cyber_jousei.pdf

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製品には多層防御システムを搭載しており、その1つとしてランサムウェア保護機能があります。
ランサムウェア保護機能やゼロデイ攻撃対策として、複数のAIアルゴリズムを搭載したクラウドサンドボックス機能が組み込まれており、未知の脅威を含んだ侵入の試みをブロックします。
これらの技術はすべてAIによって支えられており、AIが自動的に脅威を検出し、適切なインシデント対応を可能とします。
高い検出率だけでなく、極めて低い誤検知率も第三者機関によって評価されています。

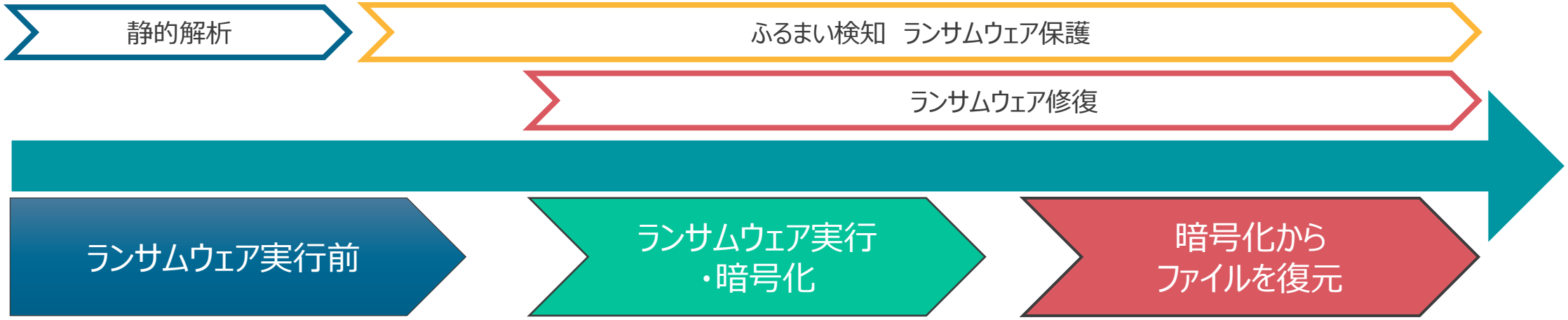


3.ランサムウェア対策機能の概要

(2) ランサムウェア保護機能について

ランサムウェア保護は、動作ベースとレピュテーションベースのヒューリスティックを使用して、実行されたすべてのアプリケーションを監視します。ランサムウェアに似た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示された場合、そのアプリケーションを自動的にブロックすることが可能です。

ランサムウェアの動作中でも、ランサムウェア修復機能により暗号化のブロックやファイルのバックアップと復元が可能です。



不審な通信など検知する**ネットワーク保護**、ファイルの動作時に検知する**リアルタイム保護**など多層防御で実行をブロック

ランサムウェアと判定された場合、**ランサムウェア保護**でブロックする
不審なプロセスを検知したら、**ランサムウェア修復**にてファイルをバックアップする

万が一暗号化されてしまった場合でも、バックアップから**自動的にファイルの復元**

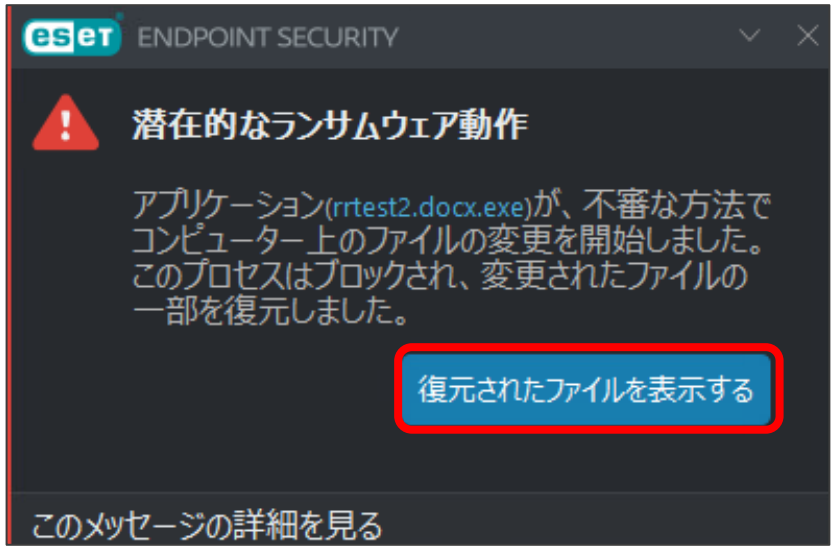
補足:ランサムウェア対策機能のポップアップ

ランサムウェア対策機能のポップアップ

ESETソリューション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つございます。
各機能が実行された際には以下のポップアップ画面が表示されます。

•ランサムウェア保護機能のポップアップ画面

•ランサムウェア修復機能のポップアップ画面



3.ランサムウェア対策機能の概要

(3)ランサムウェア保護機能

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示された場合、そのアプリケーションを、自動的にブロックすることが可能です。　※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。

※ランサムウェア
ファイルを暗号化するなどの障害を意図的に発生させ、その解決のための身代金を要求するマルウェアのことです。詳細はサイバーセキュリティ情報局、キーワード辞典をご参照ください。
https://eset-info.canon-its.jp/malware_info/term/detail/00104.html

3.ランサムウェア対策機能の概要

(4)ランサムウェア修復機能

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OSのみとなります。(2025年2月現在) ※ESET Management エージェント V12.0以降での管理が必要です。

「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。

詳細設定(HIPS画面)

「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"

3.ランサムウェア対策機能の概要

(5) ランサムウェア修復機能でのバックアップについて

よく使用されるバックアップ機能にボリュームシャドウコピーサービス(VSS)※があります。

VSSを利用したバックアップは以下のリスクがあります。

バックアップファイルの破損・消去・無効化される可能性あり
→VSSの許可されたプロセスやスクリプトによって制御できる危険性があります。
　更にランサムウェアによってはファイルの暗号化されたコピーを作成し、オリジナルを削除する機能を持つ場合もあります。

ESETは **VSSを利用していないので、上記リスクがありません。**

VSSとは別の仕組みでバックアップしており、バックアップデータは以下の機能にてランサムウェアから保護されております。
・自己防衛機能：悪意のあるソフトウェアによって破損されたりしないように保護する機能
・ACL(アクセスコントロールリスト)：アクセス権限を管理し、不審なプロセスがアクセスできないように保護する機能

※ボリュームシャドウコピーサービス
　Windowsの機能の１つで、ハードディスクの中身を丸ごとコピーして保存する機能です。

3.ランサムウェア対策機能の概要

(6)ランサムウェア対策機能の利用条件について

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。

〇ランサムウェア保護

① Windowsクライアント向けESETプログラムを利用している

〇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こと
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こと
④ ESET PROTECT Advanced、Complete、Enterprise、Eliteのいずれかのライセンスを利用する

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OS向け総合セキュリティプログラム	×	〇
ESET Endpoint アンチウイルス (EEA)	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	×	〇

補足:上位製品のご紹介

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を利用するにはいくつか条件があります。
条件の１つにAdvanced以上のライセンスを購入する必要があります。その他の条件は前のページをご参照ください。

- 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	ウィルス対策プログラム	ランサムウェア機能	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/Essential	○	○	○	–	–	–	–	–	–	–

⇒ランサムウェア修復はAdvanced以上のライセンスで利用できるため、クラウド版のセキュリティ管理ツールやクラウドサンドボックスなどのソリューションが利用できます。
ESETソリューションであれば上位製品をご利用いただくとランサムウェア対策も含めて一元管理ができます。

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。
総合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. 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. 設定できます。

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設定が行えます。

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行っている、かつAdvanced以上のライセンスを利用している必要があります。

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。また、NTFSファイルシステムで動作します。

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いずれかでしょうか？
A. 自動でバックアップ、修復されます。

Q. ランサムウェア修復機能の実際の動きをみたいのですが？
A. 動画(英語)でご用意しております。
▽ESET Ransomware Remediation Demo
https://www.youtube.com/watch?v=ifMOvoHEVbQ