ランサムウェア対策ソフト

AppCheck

AppCheck（アップチェック） 製品紹介資料

株式会社JSecurity

JSECURITY

目次

株式会社JSecuriy

1994年から続く、韓国JIRAN（ジラン）のグループ会社で、
日本国内では2004年からビジネスを展開しています。
2018年1月、Jiransoft Japan（現Jiran Japan）の分社化により、
セキュリティ事業をメインに行う会社としてJSecurityは新たにスタートしました。

設立日　2018年1月

資本金　102,923,900円

決算期　12月

本　社　東京都港区浜松町2-4-1
世界貿易センタービルディング南館17階

代　表　今村 誉一

事　業　情報セキュリティ製品・サービスの開発および販売

会社概要

JSecurity 取扱製品およびソリューション

標的型攻撃対策

MudFIX

メールセキュリティ対策

SPAMSNIPER　　MAILSCREEN

運用管理ツール

FIREMON　　PCFILTER　　SERVERFILTER

ファイル共有サービス

GIGAPOD　　Gate4Mobile

ソフトウェア開発キット（SDK）

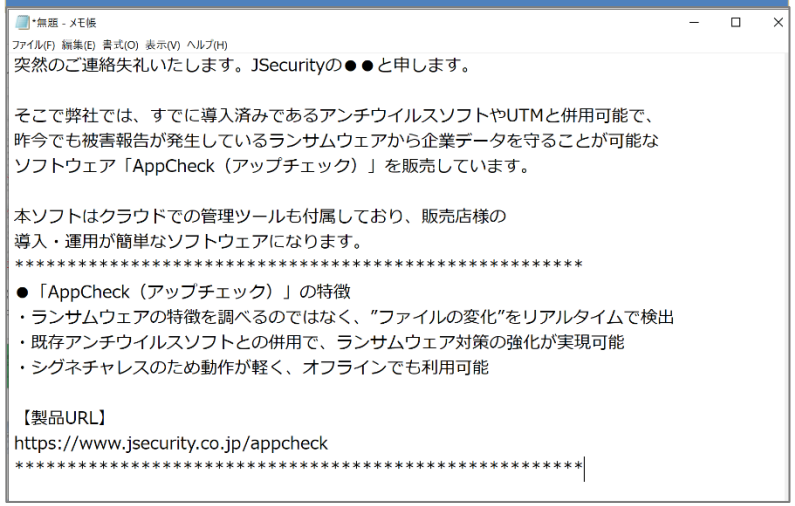
CYREN

１．ランサムウェアの脅威と被害

ランサムウェアとは

ランサムウェアとは、身代金(Ransom)とソフトウェア(Software)の合成語で、パソコンのシステムをロックしたり大切な**ファイルを暗号化して**開けなくした後、それらの**解除費用として金銭を要求するマルウェア**の一種です。

感染前の文書



感染後の文書

主にPCやサーバーに保存している文書や画像ファイルが対象

ランサムウェアは、公開鍵暗号アルゴリズムの**RSA-2048**を利用するためほぼ復元不可能

ランサムウェアは2022年企業で最も被害が多い脅威

■「情報セキュリティ10大脅威 2022」

NEW：初めてランクインした脅威

昨年順位	個人	順位	組織	昨年順位
2位	フィッシングによる個人情報等の詐取	**1位**	ランサムウェアによる被害	1位
3位	ネット上の誹謗・中傷・デマ	**2位**	標的型攻撃による機密情報の窃取	2位
4位	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	**3位**	サプライチェーンの弱点を悪用した攻撃	4位
5位	クレジットカード情報の不正利用	**4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	3位
1位	スマホ決済の不正利用	**5位**	内部不正による情報漏えい	6位
8位	偽警告によるインターネット詐欺	**6位**	脆弱性対策情報の公開に伴う悪用増加	10位
9位	不正アプリによるスマートフォン利用者への被害	**7位**	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	NEW
7位	インターネット上のサービスからの個人情報の窃取	**8位**	ビジネスメール詐欺による金銭被害	5位
6位	インターネットバンキングの不正利用	**9位**	予期せぬIT基盤の障害に伴う業務停止	7位
10位	インターネット上のサービスへの不正ログイン	**10位**	不注意による情報漏えい等の被害	9位

昨今は、個人ではなくお金を持っている（支払う力のある）

企業を狙う傾向にある

引用：IPA「情報セキュリティ10大脅威 2022」 https://www.ipa.go.jp/security/vuln/10threats2022.html

実際の国内の被害事例

ホンダを標的に開発か、ランサムウエア「EKANS」解析で見えた新たな脅威

外薗 祐理子　日経クロステック／日経コンピュータ

2020.06.26
有料会員限定

全4004文字

パソコンやサーバーのファイルを暗号化し、解除のための身代金を要求するランサムウエアが、特定の企業を狙う標的型に進化している。ホンダを襲ったとされるランサムウエアを解析した日本のセキュリティー技術者は工場を持つ製造業や医療機関などが狙われると警鐘を鳴らす。

サイバー攻撃でホンダの工場が停止

ホンダは2020年6月8日にサイバー攻撃を受け、世界的な大規模システム障害を起こした。国内外の工場で生産や出荷が一時止まったほか、本社などで働く従業員のパソコンが使えなくなるなどオフィス系のネットワークシステムにも影響が出た。この影響で生産を停止した米オハイオ州の乗用車工場やブラジルの二輪工場は現地時間の6月11日までに復旧した。

スニーカーダンクで不正アクセス、顧客情報275万件漏えいか

6/15(水) 11:15 配信　46

FASHIONSNAP.COM

スニーカーダンク公式サイトより

スニーカーフリマアプリ「スニーカーダンク（SNKRDUNK）」が、外部からの不正アクセスを受け、一部顧客の個人情報が漏えいした可能性があると公式サイトで公表した。被害件数は275万3400件。その内約6割の顧客については生年月日、メールアドレス、パスワードのみが漏えい。10件が口座情報漏えいのおそれがある。なお、クレジットカード番号や本人確認書類に関しては本件には該当しておらず、海外で利用可能なスニーカダンク（英語版）についても影響はないという。

トヨタ取引先にサイバー攻撃、データ流出か

2020/7/16 18:18｜日本経済新聞　電子版

保存　共有　その他

トヨタ自動車などと取引があり、金型の設計や製造を手掛けるTMW（愛知県稲沢市）がサイバー攻撃の被害に遭ったことが16日分かった。特定の組織を狙う標的型のランサムウエア（身代金要求ウイルス）による攻撃を受け、データが盗み取られたとみられる。サイバー対策の専門家は警戒強化を呼びかけている。

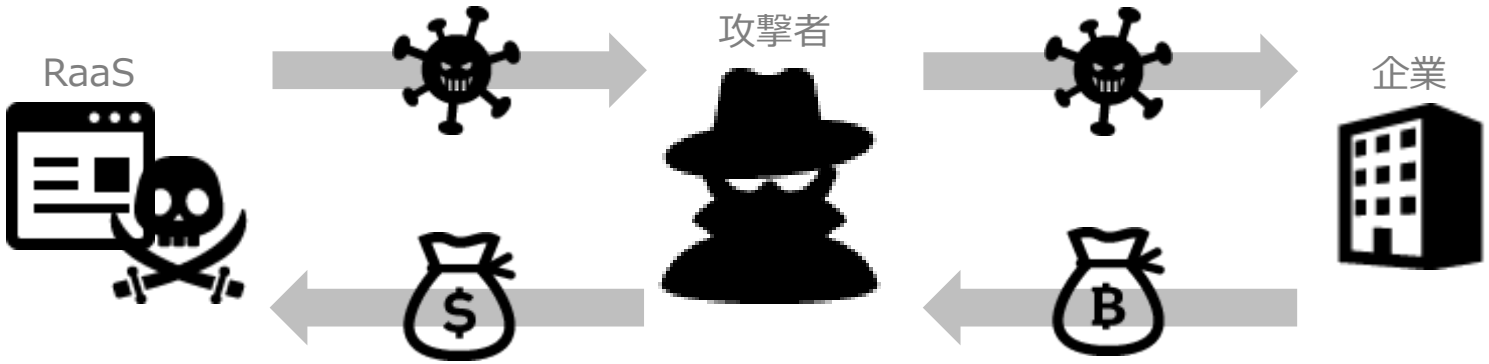
■引用URL

左上：
https://xtech.nikkei.com/atcl/nxt/column/18/00989/062400028/
右上：
https://news.yahoo.co.jp/articles/7b917c68d2e4df02fcca0ad2659b27784e91124c
左下：
https://www.nikkei.com/article/DGXMZO61601890W0A710C2TJ2000/

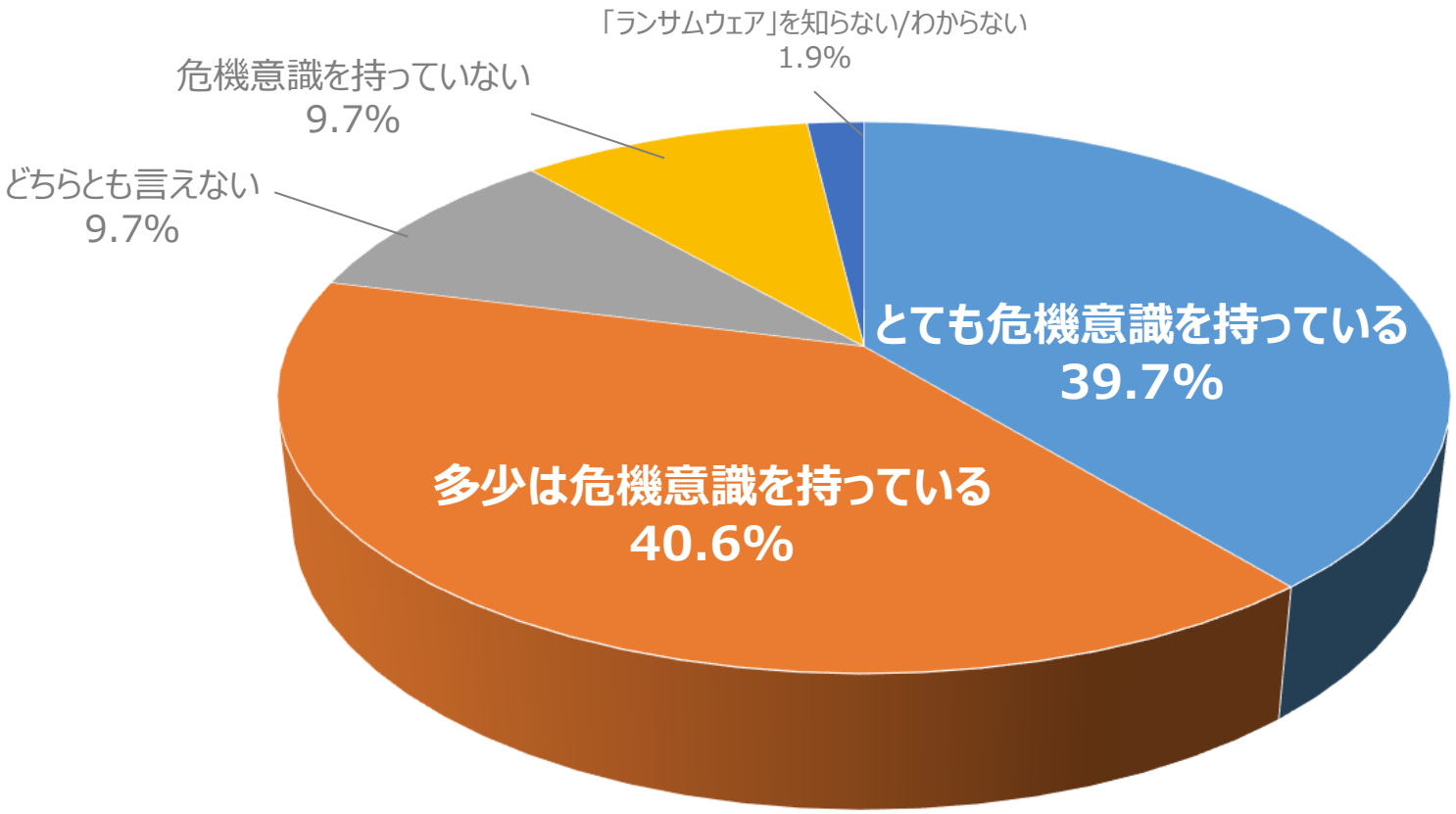
なぜ？誰が？ランサムウェアを使って攻撃をするのか

金銭目的で、誰もが攻撃者になれます

従来は特殊なスキルを持った人物のみ攻撃者となっていたが、
RaaS（Ramsomeware as a Service）という、ランサムウェアを売買するサービスが
ブラックマーケットで普及したことで、誰もがランサムウェアを簡単に作成することができています。
ランサムウェアによって得た金銭は、提供者と利用者で分配されます。



ランサムウェアに対する危機意識



ランサムウェアへの危機意識を持っている企業は80.3%と大多数

＊出典：Tech Target　身代金ウイルス「ランサムウェア」に関する アンケート調査　<https://techtarget.itmedia.co.jp/tt/news/1610/03/news02.html>

ランサムウェアがマルウェアの一部なら・・

アンチウイルスソフトの導入で十分では？

ではなぜアンチウイルスを導入している大企業でも被害がおきるのでしょう？

攻撃者はターゲットを良く調べます

アンチウイルスで検知できない新種や亜種のランサムウェアを利用します

アンチウイルスソフトだけでは対策として不十分な場合があるってことですね・・

一般的なアンチウイルスソフト

ランサムウェアの作成者は、開発したランサムウェアが既存のアンチウイルスソフトで検出できないことを十分にチェックしてからリリースします

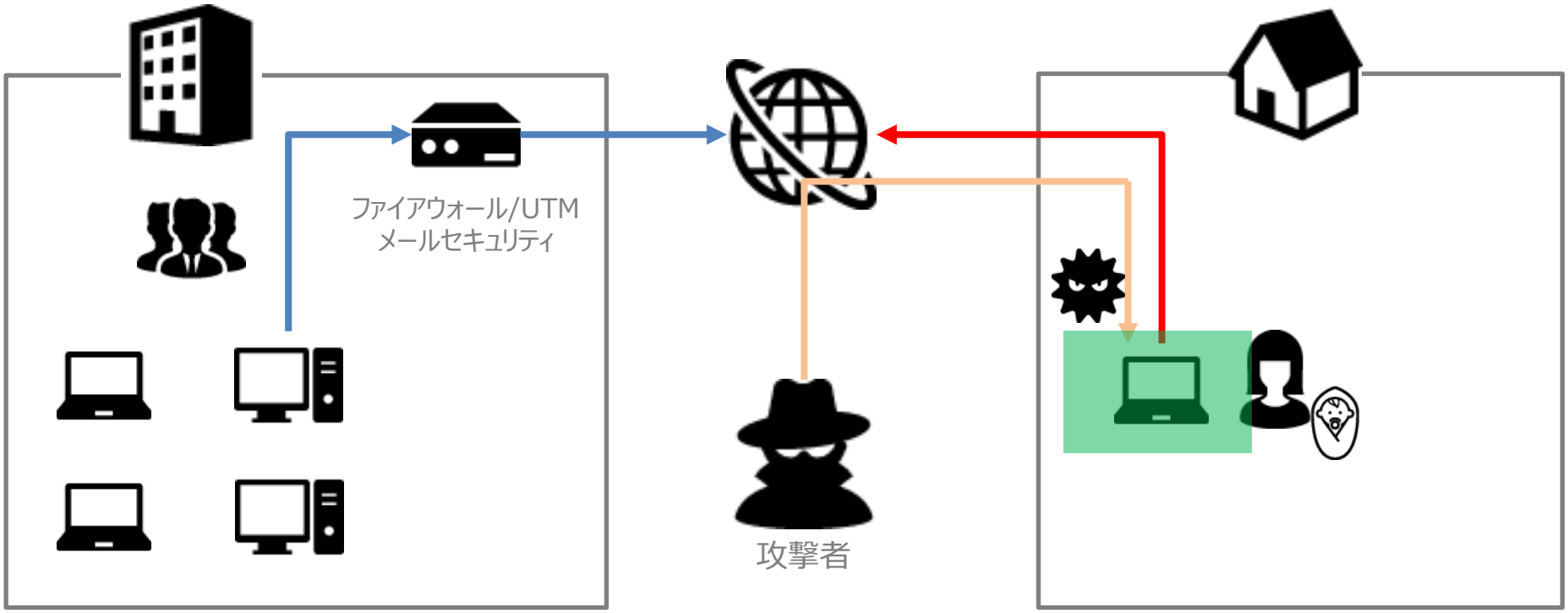
アンチウイルスソフトによる課題

新種や亜種のランサムウェアへの**リアルタイムでの対応**

補足：働く環境の変化にも注意が必要

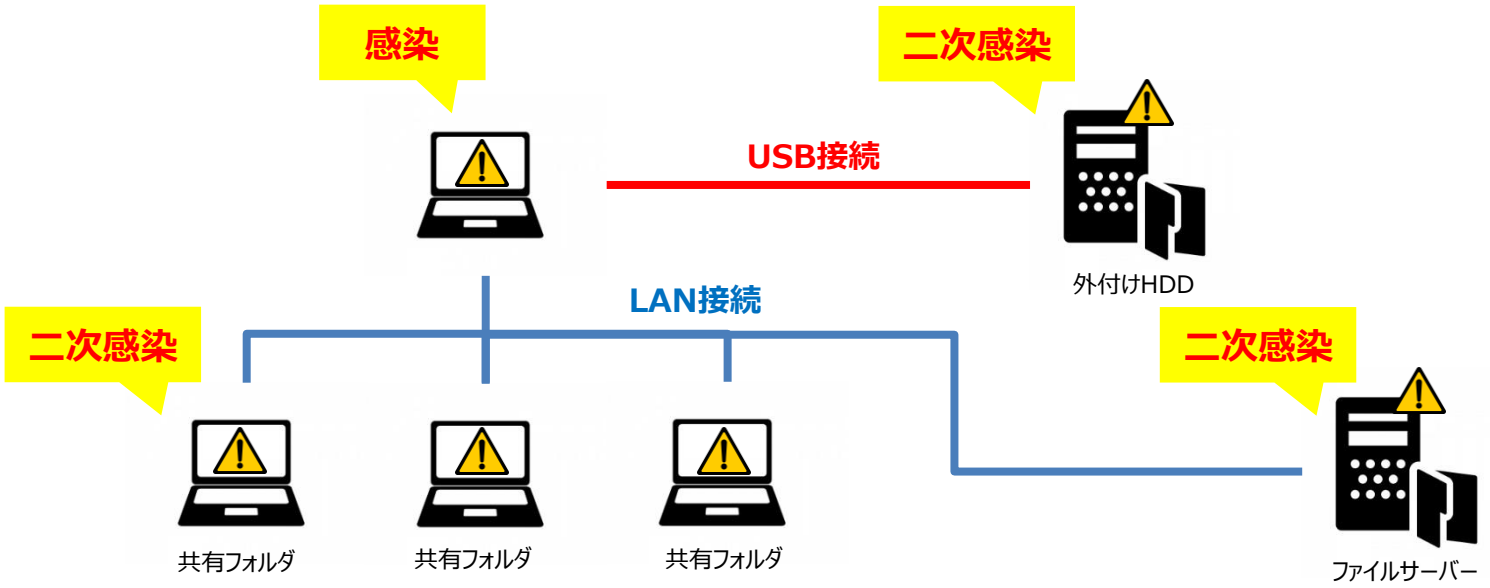
テレワークが進む中での課題

2021年は、新型コロナウイルスの発生により、多くの企業でテレワークが進みました。
様々なセキュリティ対策を実施している組織のネットワーク以外（自宅、カフェ）から、
インターネットへ接続する機会が増えつつあります。



組織外での利用に関して、端末に対するセキュリティ配慮が一層重要になります

1台感染すればサーバーも感染する危険がある



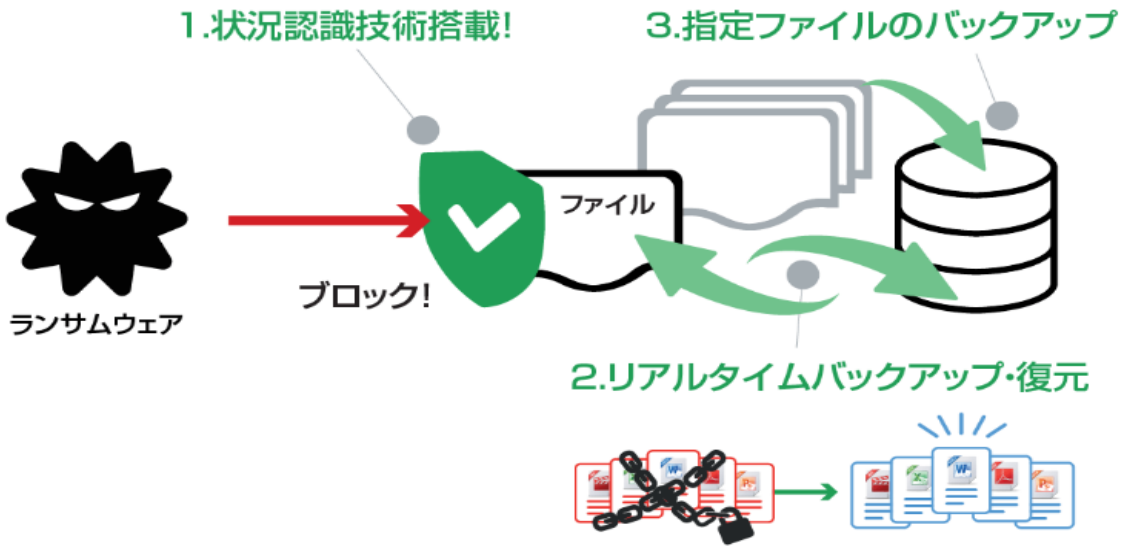
⚠ 感染したパソコンからアクセス可能なデバイスに感染する

⚠ サーバーには企業の重要なデータが沢山含まれているため対策が必要

パソコンだけでなくサーバーのランサムウェア対策も重要

2．「AppCheck（アップチェック）」の概要

AppCheckの特徴



1. 防御

状況認識技術（特許）によるランサムウェアの毀損行為を遮断

2. リアルタイムバックアップ

ファイル毀損時に、**リアルタイム**で元のファイルのバックアップを実施

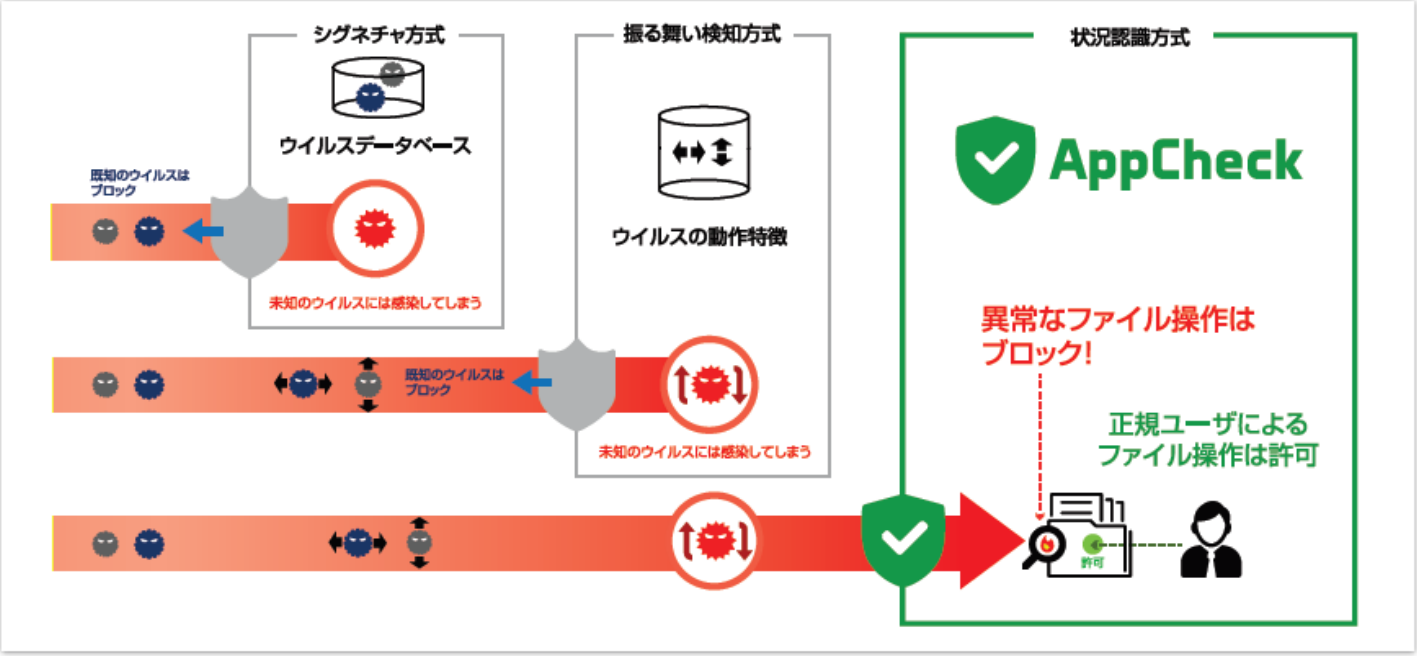
3. 自動バックアップ

指定ファイルを**定期的に**任意フォルダーやローカルフォルダーにバックアップ

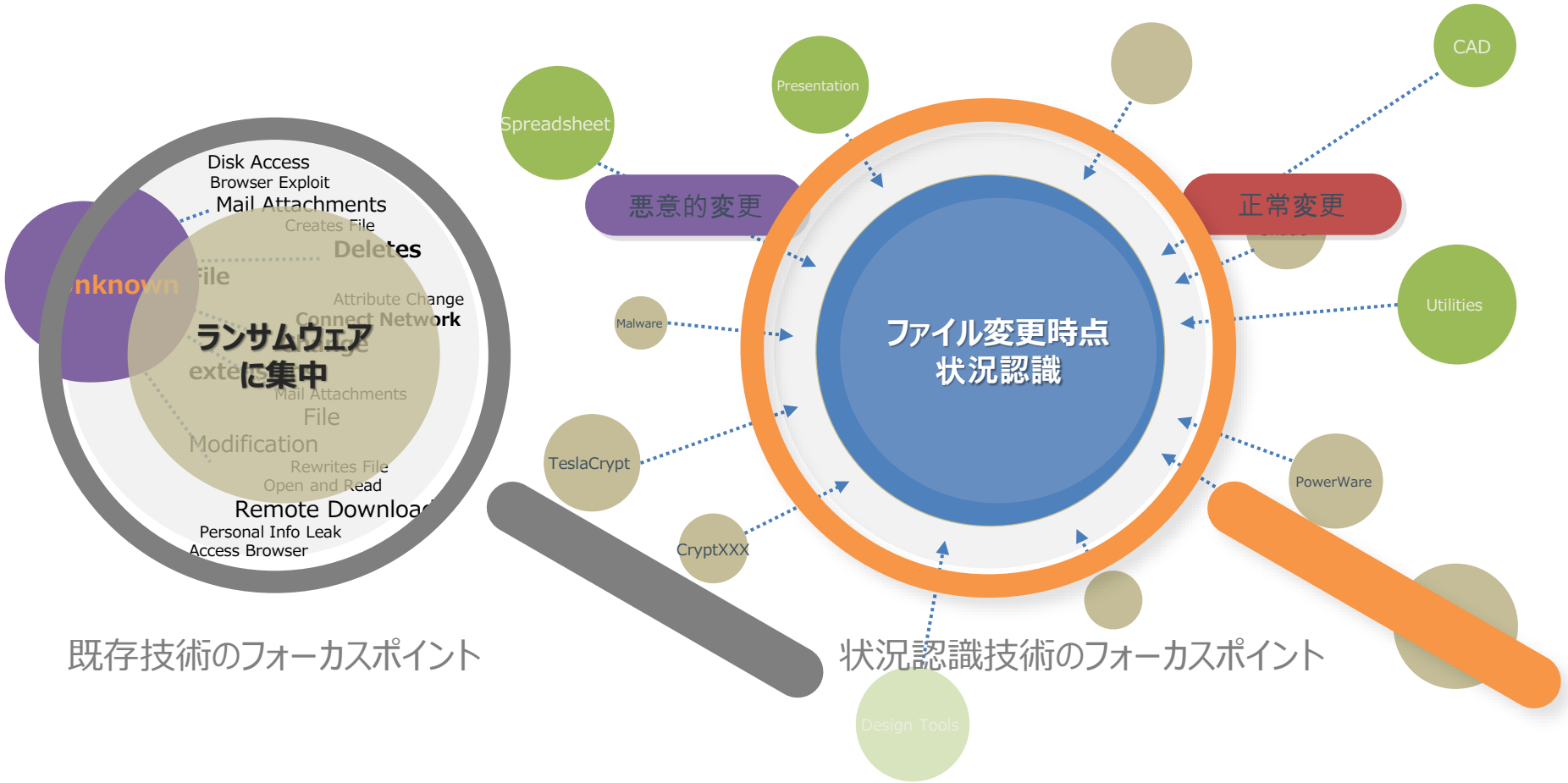
AppCheckの状況認識技術

AppCheckはランサムウェアの特徴を調べるのではなく、**状況認識技術によりファイルの変化をリアルタイムで検出し、ランサムウェアによるファイル毀損をブロック**します。

状況認識技術とは、周辺の状況や環境等のすべての情報を総合して認知し、その状況に最適な対応を行う技術です。また、シグネチャを持たないため、更新の必要もなく軽快な動作を提供します。



状況認識技術とは



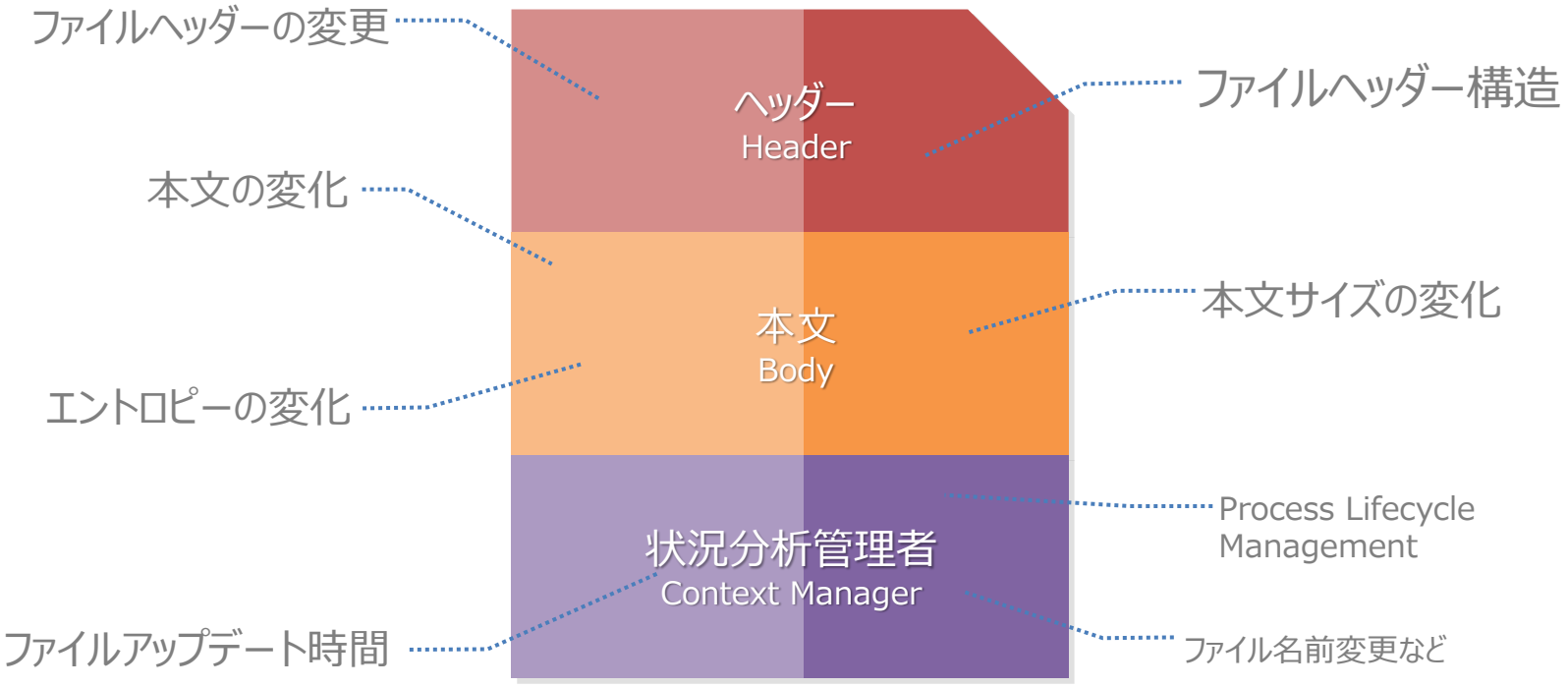
ランサムウエア自体を見るのではなく、**ファイル変更時に正常な変更か悪意のある変更かを判断**

ゆえにAppCheckは新種・亜種のランサムウェアにも対応

状況認識技術のフォーカスポイント

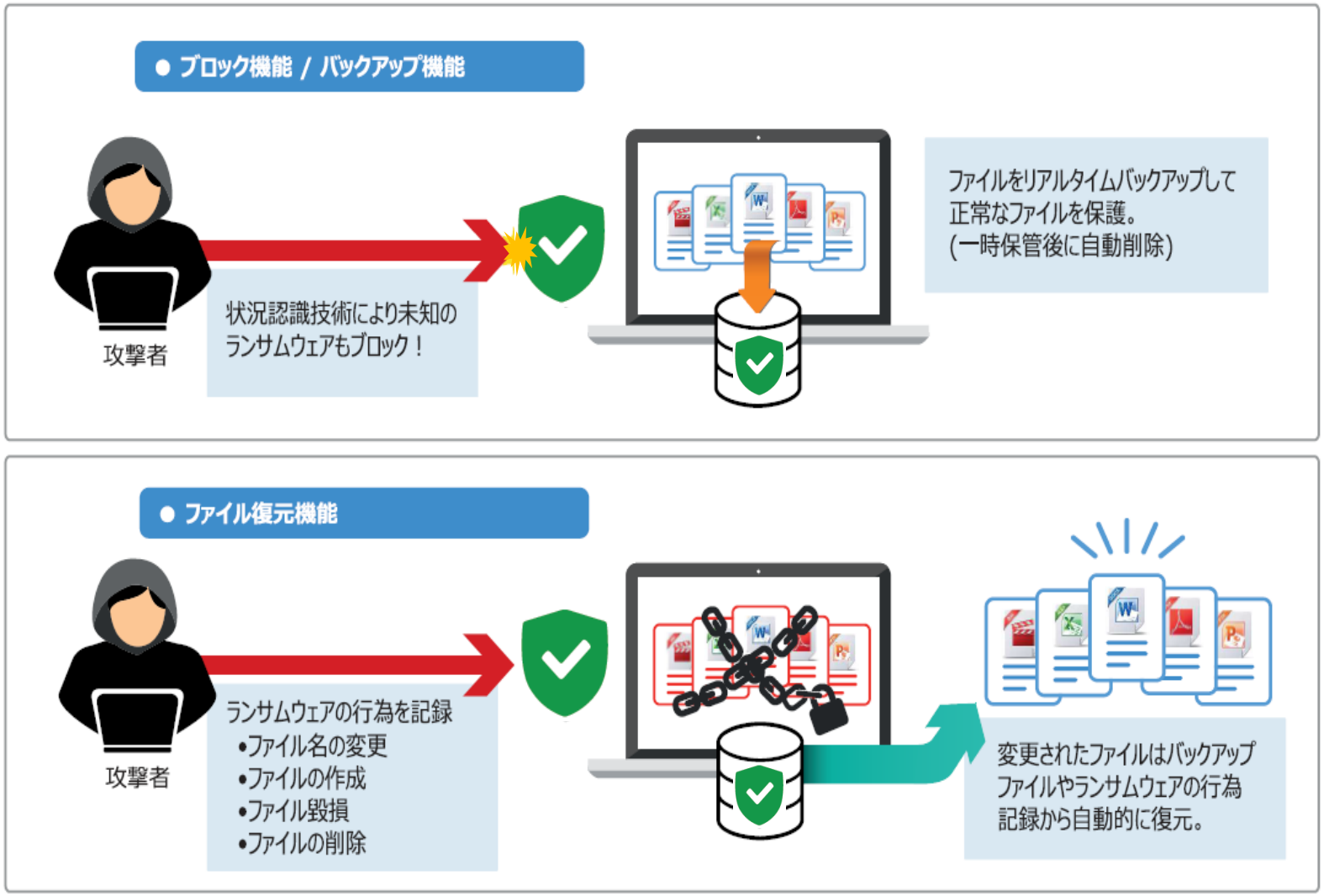
ファイルが変更されるとき確認できる情報は非常に多く、これを追跡することで

正常なファイルの変更とマルウェアによる変更の区分が可能です。



CARBエンジンの主要なフォーカスポイント
Context Awareness Ransomware Behavior detection engine
状況認識ランサムウエア行動検出エンジン

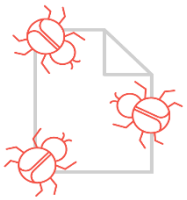
AppCheckの主たる動作



AppCheckの検査方式

1. ファイルモニタリング

ユーザのファイルをモニタリングして
変更時点に「正規変更」か「悪意のある変更」
かを判断します。



2.リアルタイムバックアップ
（疑わしいファイル変更を発見）

原本ファイルをリアルタイムバックアップ
フォルダにバックアップして、ファイルを変更
するプロセスについて継続モニタリング

3. ファイル毀損プロセスの検知

断続的なファイル毀損が検出されると、
そのプロセスをランサムウェアとみなして検知します。

4. プロセス遮断、削除および復旧

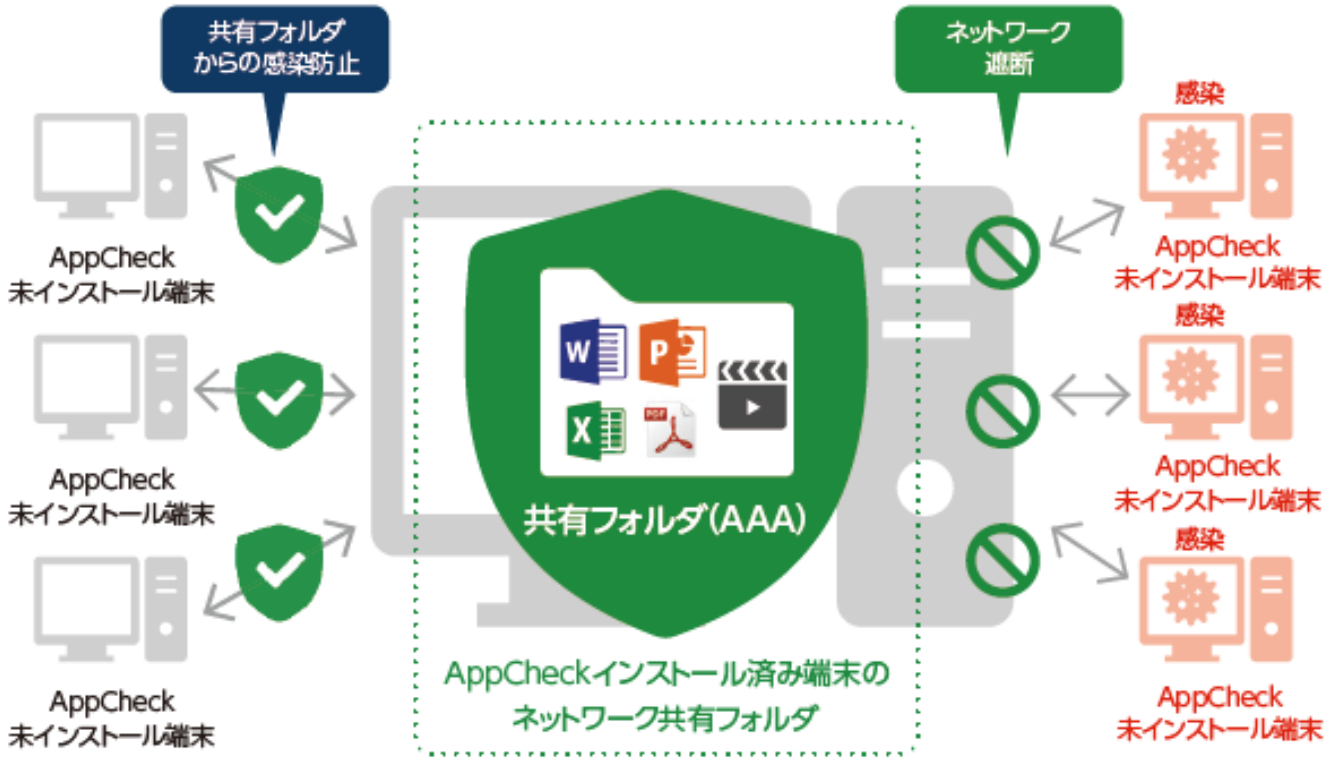
ランサムウェアとして検知された**プロセスを終了後**
毀損されたファイルを全て復旧します。

5. ユーザー業務の継続

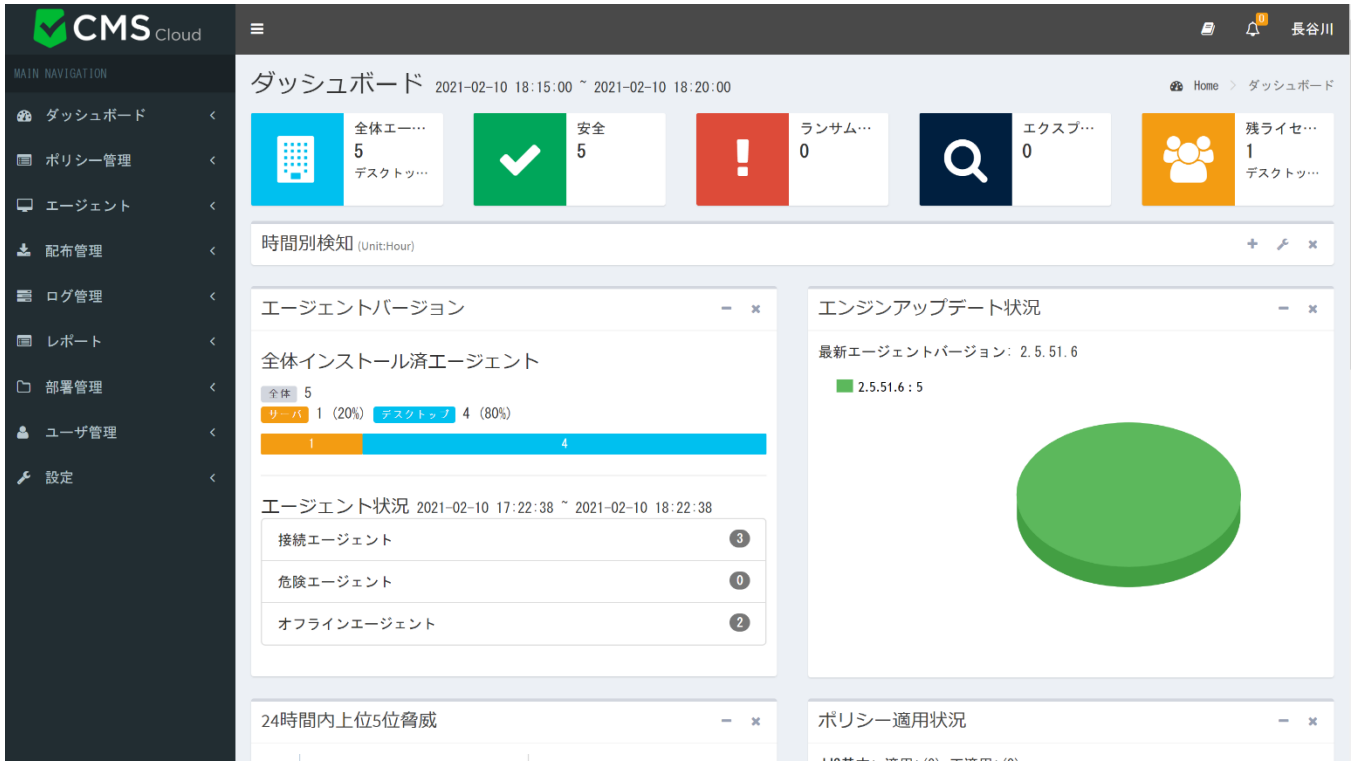
別途処理なしに既存業務を
継続することができます。

その他：共有フォルダ保護機能

AppCheckがインストールされたPCが共有設定をしているフォルダは、AppCheckの感染防止機能、ネットワーク遮断機能によって守られます。AppCheckがインストールされていない端末がランサムウェアに感染したとしても、共有フォルダ内のファイルは保護されます。また、共有フォルダ経由による ランサムウェア**感染の拡大を遮断**します。



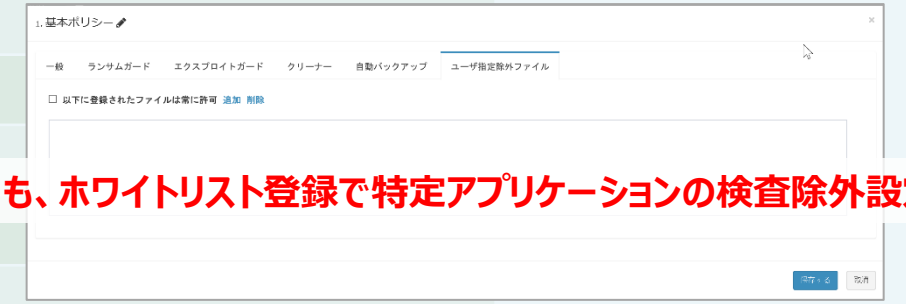
その他：中央管理機能（CMS）コンソール画面



機能	説明
一括ポリシー設定	クライアント端末をランサムウェアから保護するためのポリシーを、一斉に配布することができるため効率的な管理・運用が可能。
バックアップ機能	様々なバックアップオプションとネットワークドライブへのバックアップ機能で、他のバックアップソリューションがなくても指定したファイルサーバにファイルバックアップが可能。
モニタリング	ダッシュボード、ログ管理、リアルタイムでのランサムウェア検知情報の確認が可能。
レポート機能	期間別報告書、統計およびログデータを提供し簡単にレポートの出力が可能。

アンチウイルス製品との互換性（共存確認済一覧）

メーカ名
AhnLab V3
Avast
AVG
Avira
ESET
BitDefender
Kaspersky
Malwarebytes
McAfee
Quick Heal
Sophos
Symantec Norton
Trend Micro
Windows Defender & Microsoft Security Client
F-Secure



左記以外でも、ホワイトリスト登録で特定アプリケーションの検査除外設定も可能

AppCheck製品構成

		AppCheck Pro	AppCheck Pro for Windows Server
価格 ※年次サブスクリプションとなります ※次年度以降も同額となります		5ライセンスより購入可能	1ライセンスより購入可能
		オープン価格	オープン価格
ランサムウェア対策	検疫・復旧	○	○
	フォルダ保護	○	○
	ログ提供	○	○
中央管理機能（CMS）	一括ポリシー設定	○	○
	バックアップ機能	○	○
	モニタリング機能	○	○
	レポート機能	○	○
稼働ＯＳ		Microsoft Windows 7 / 8 / 8.1 / 10 (32/64bit) / 11	Microsoft Windows Server 2008 R2以降

（*）CMSは、オプションで販売しております。（2022.1現在）

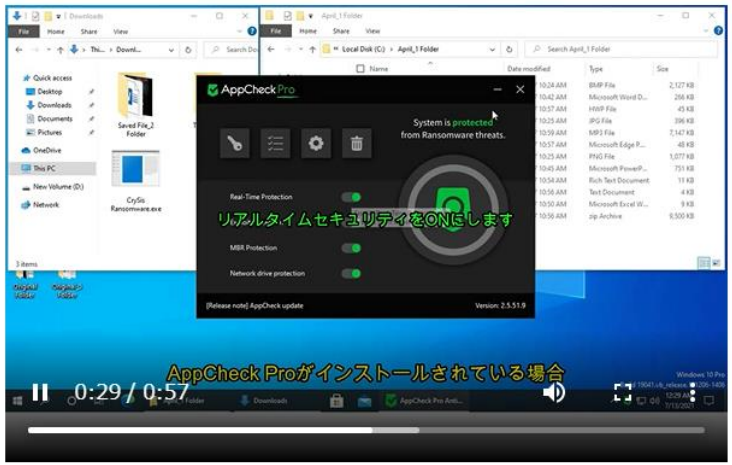
動作環境

OS	AppCheck Pro	AppCheck Pro for Windows Server
Windows 7（32/64ビット）	○	×
Windows 8（32/64ビット）	○	×
Windows 8.1（32/64ビット）	○	×
Windows 10（32/64ビット）	○	×
Windows 11（64ビット）	○	×
Windows server 2008 R2 SP1（*1） / Windows server 2008 SP2	×	○
Windows server 2012	×	○
Windows server 2012 R2	×	○
Windows server 2016	×	○
Windows server 2019	×	○
Windows server 2022	×	○
Windows storage server 2012	×	○
Windows storage server 2012 R2	×	○
Windows storage server 2016	×	○
Windows Server IoT 2019 for Storage	×	○
Windows Server IoT 2022 for Storage	×	○

*1　SHA-2認証書のMicrosoft最新パッチがインストールされていること

参考：AppCheckによるランサムウェア遮断動画

https://www.jsecurity.co.jp/blog/index/search_category_id/587/page/1



・**配布方式：**未確認

・**MD5：**076de296092c44e7fb36684454349bf4

・**検知名：**Trojan.Ransom.Crysis.E (BitDefender), W32/Crysis.W!tr.ransom (Fortinet)

・**ファイル暗号化パターン：**.id-<Random>.[trupm@protonmail.com].com

3．まとめ：「AppCheck」選定のポイント

シグネチャレス

シグネチャを持たないため、AppCheckインストール後も、PCやサーバーに負荷をかけません。また、シグネチャの更新もないため、定期的な更新作業も不要です。

バックアップ

ランサムウェアが侵入し不正なプロセスが実行された際、リアルタイムで対象データをバックアップします。ランサムウェアを削除したあと、従来のファイルを元に戻します。

ランサム専用

ランサムウェア専用ソフトウェアのため、アンチウイルスソフトと共存可能です。アンチウイルスソフトと一緒に利用することでPCおよびサーバーのセキュリティを向上させることが可能です。

ランサムウェア対策なら「AppCheck」！

デモライセンスの提供

AppCheckは、デモライセンスを提供しています。

PC向け5ライセンス、サーバー向け1ライセンスが1か月間無償で利用可能です。

●以下フォームよりお問合せください

https://www.jsecurity.co.jp/contact

インストールも非常に簡単、ご連絡お待ちしております

ありがとうございました