Dr.WEB®
Anti-virus

ランサムウェアの種類と対策

株式会社Doctor Web Pacific

www.drweb.com

Dr.WEB®
Anti-virus

今回のテーマ

- ランサムウェアの種類
- 攻撃の特徴
- 攻撃に備えた対策
- Dr.Webでできること

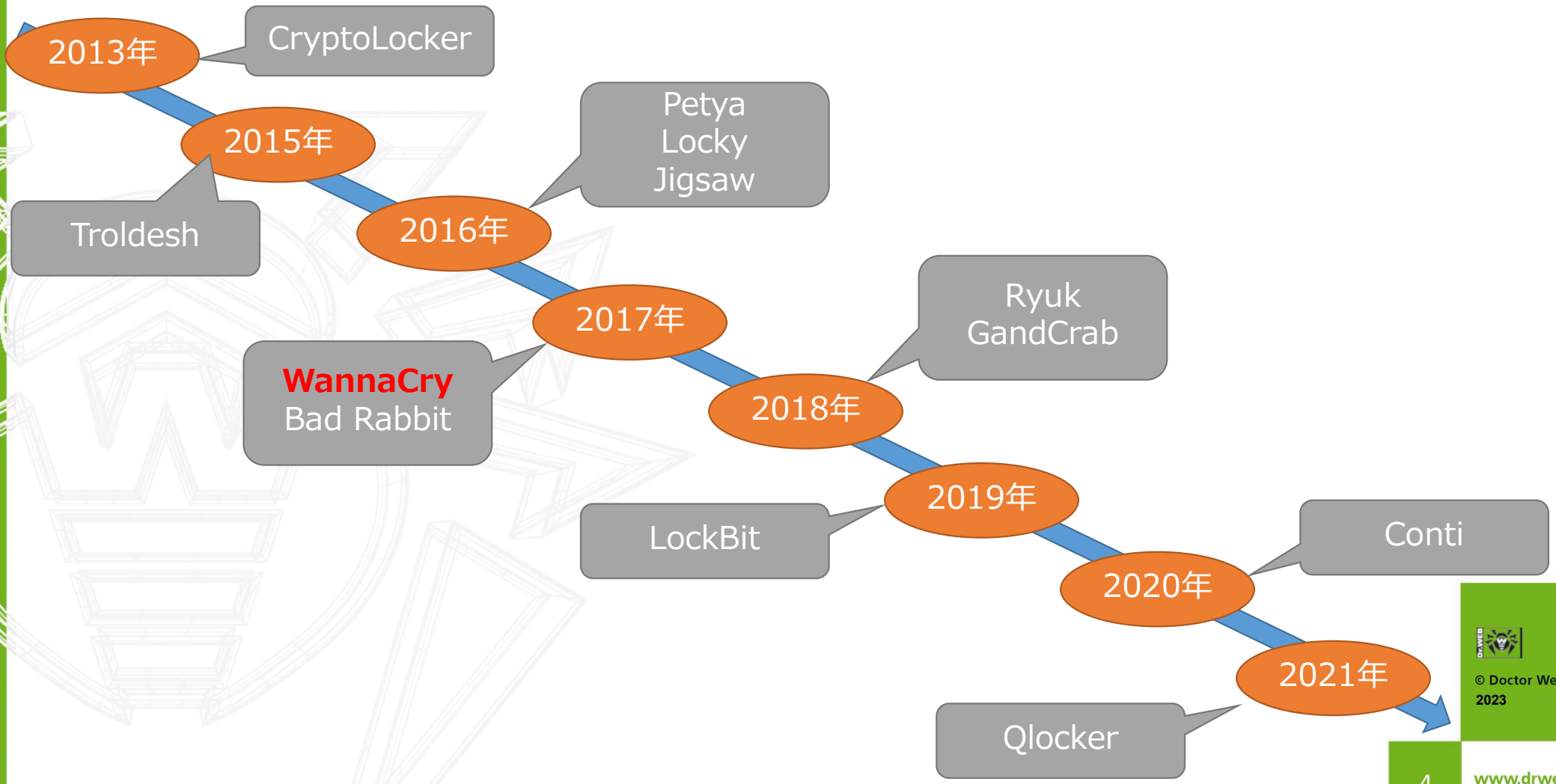
Dr.WEB®
Anti-virus

ランサムウェアの種類

株式会社Doctor Web Pacific

www.drweb.com

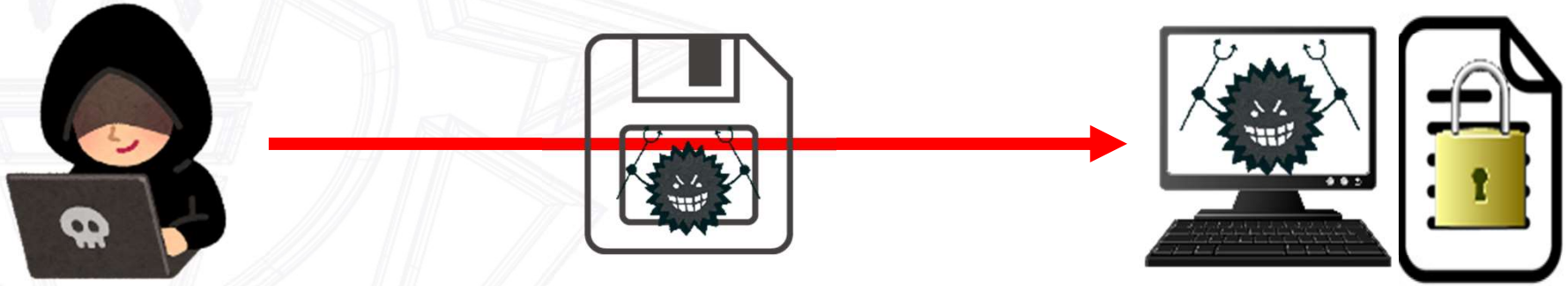
代表的なランサムウェア



一番古いランサムウェア

◆ AIDS Trojan

1989年に被害が確認されています。 郵便によって配布されたフロッピーディスクが媒体であった。



Dr.WEB®
Anti-virus

ランサムウェア攻撃の特徴

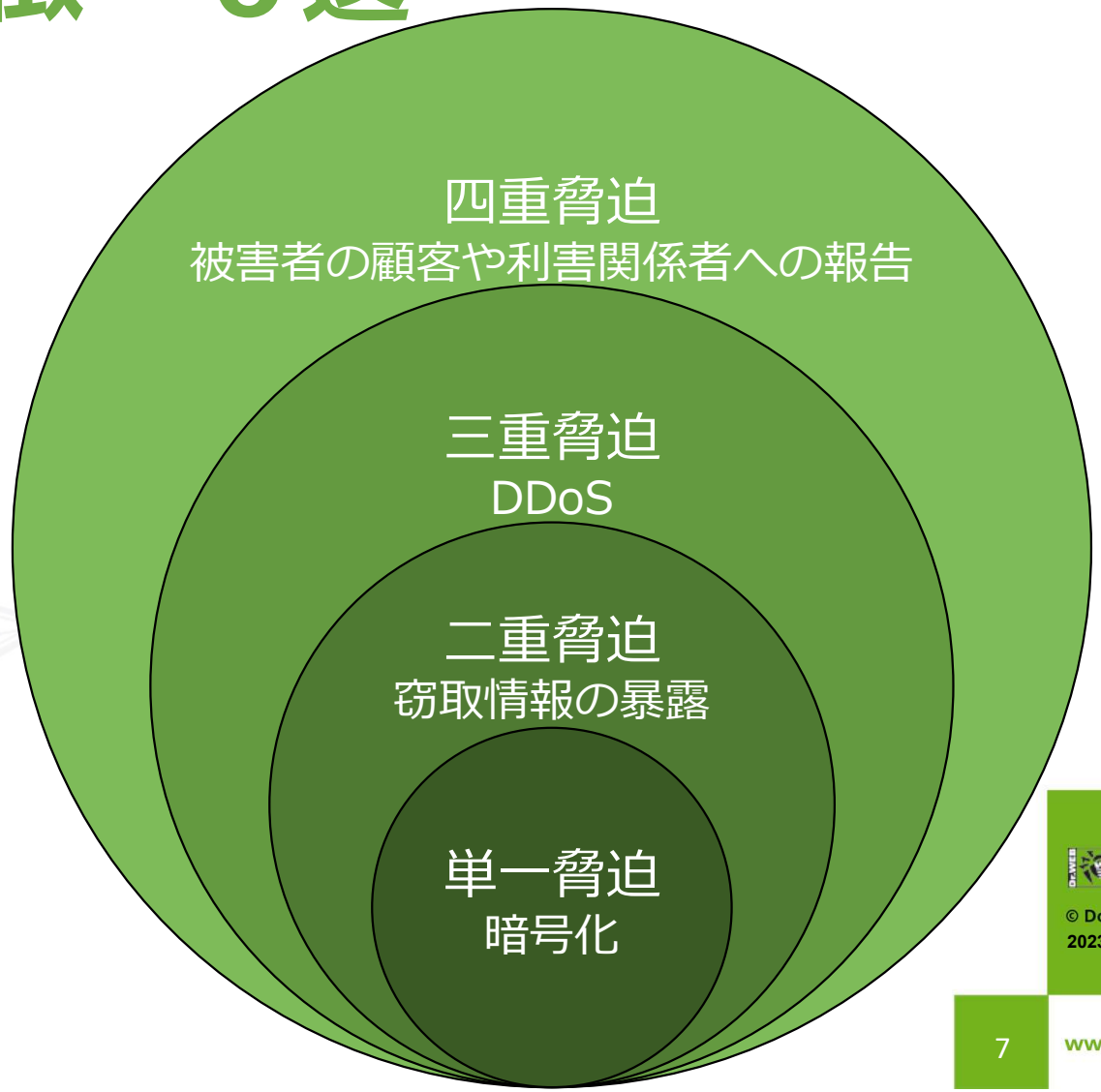
株式会社Doctor Web Pacific

www.drweb.com

攻撃の特徴　６選

◆ 多重脅迫型

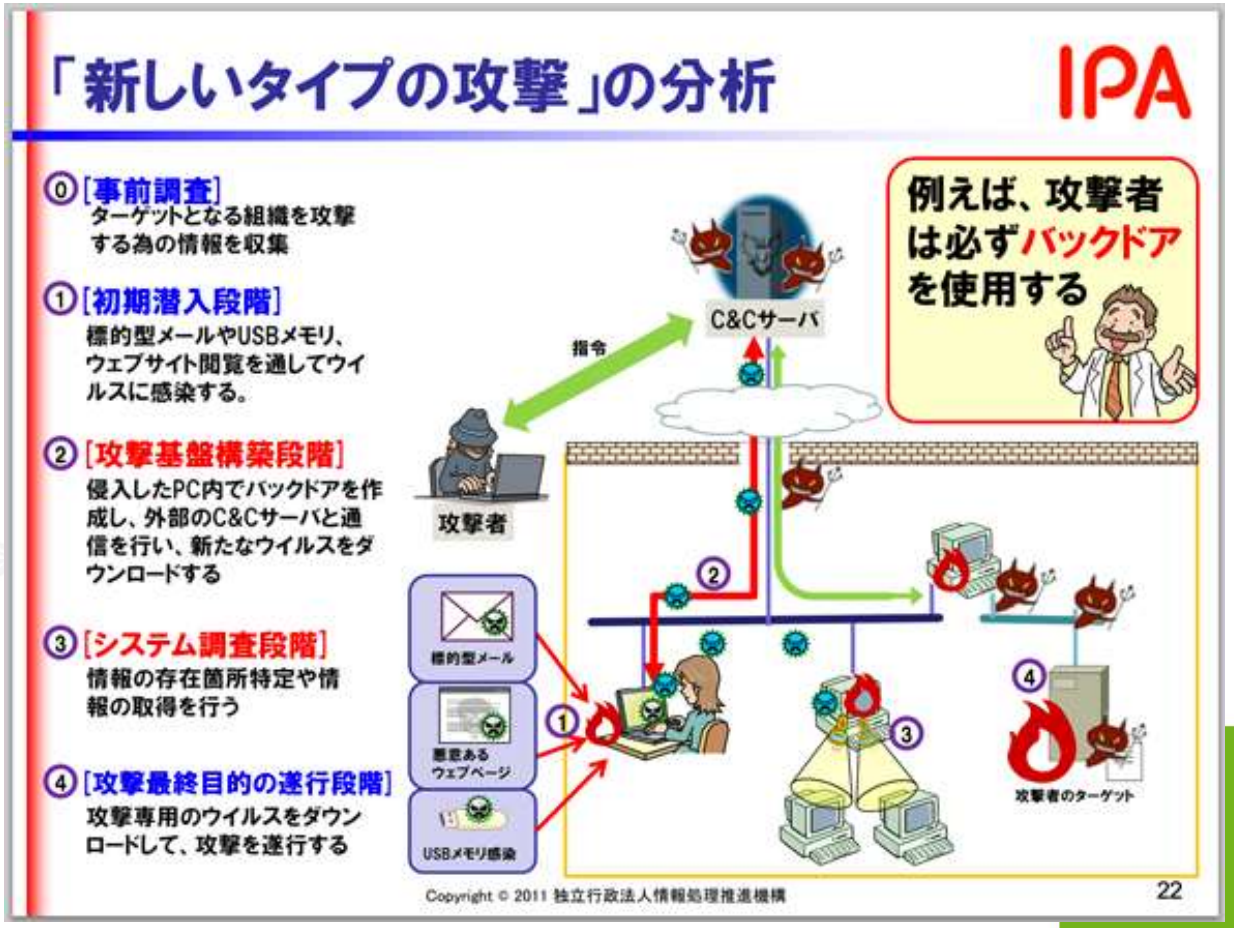
多重脅迫型は、破壊型と暴露型を融合させたランサムウェアの手口です。データの暗号化および破壊をしつつ、重要なデータの公開をほのめかし脅迫します。



攻撃の特徴　６選

◆ 標的型

標的型は無差別・ばらまき型で感染を広げるのではなく、特定の企業を標的にすることで、効率的に身代金を手に入れようとする手口です。身代金を支払った企業があると、同じような企業が狙われます



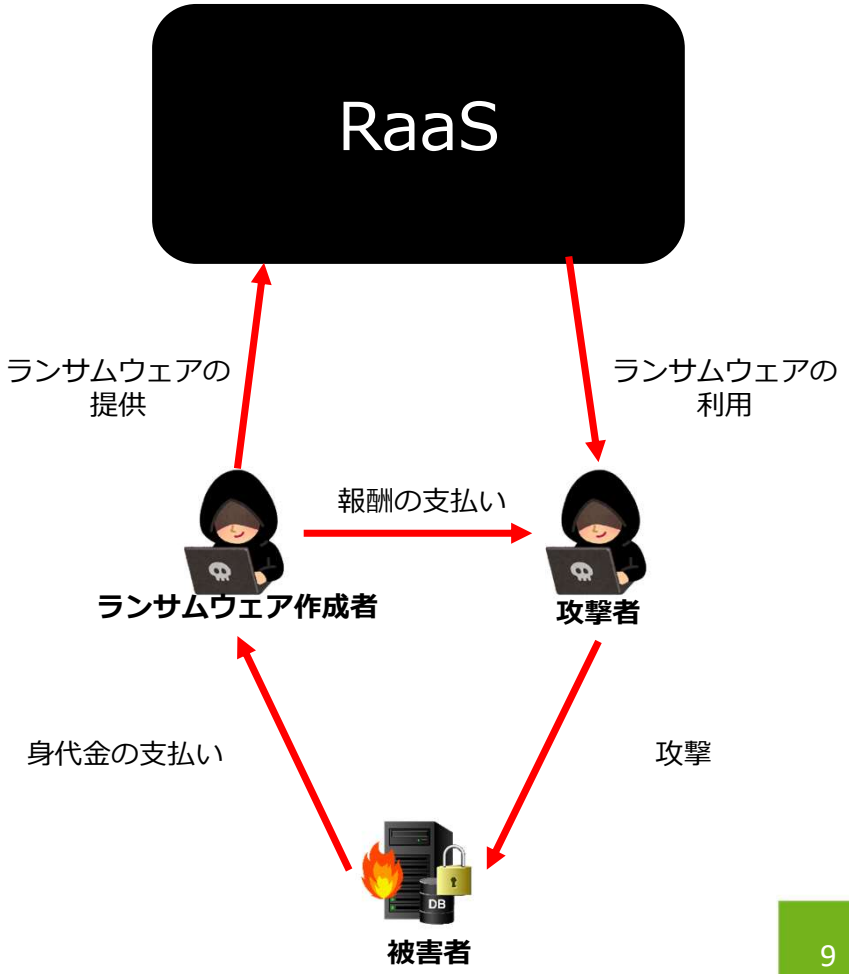
独立行政法人情報処理推進機構「標的型攻撃／新しいタイプの攻撃の実態と対策」より
https://www.ipa.go.jp/security/j-csip/ug65p9000000nkvm-att/000024542.pdf

攻撃の特徴　６選

◆ RaaS

RaaS（Ransomware-as-a-Service）は、ランサムウェア攻撃を容易に行うために必要なものをまとめたクラウドサービスのことを指します。

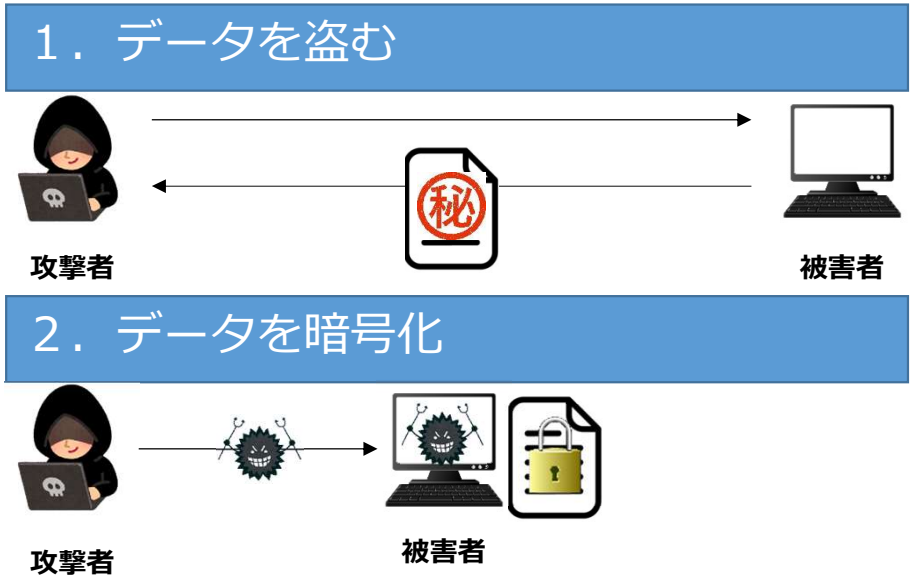
ランサムウェアを実装する手間が軽減される分、より多くのサイバー犯罪者がランサムウェアを気軽に扱えるようになりました。



攻撃の特徴　６選

◆ 暴露型

暴露型のランサムウェアは、盗んだ企業情報を公開すると脅迫するランサムウェアです。実際にWebサイト（ダークウェブ）にデータの一部を公開して、期限までに身代金を支払うように要求します。

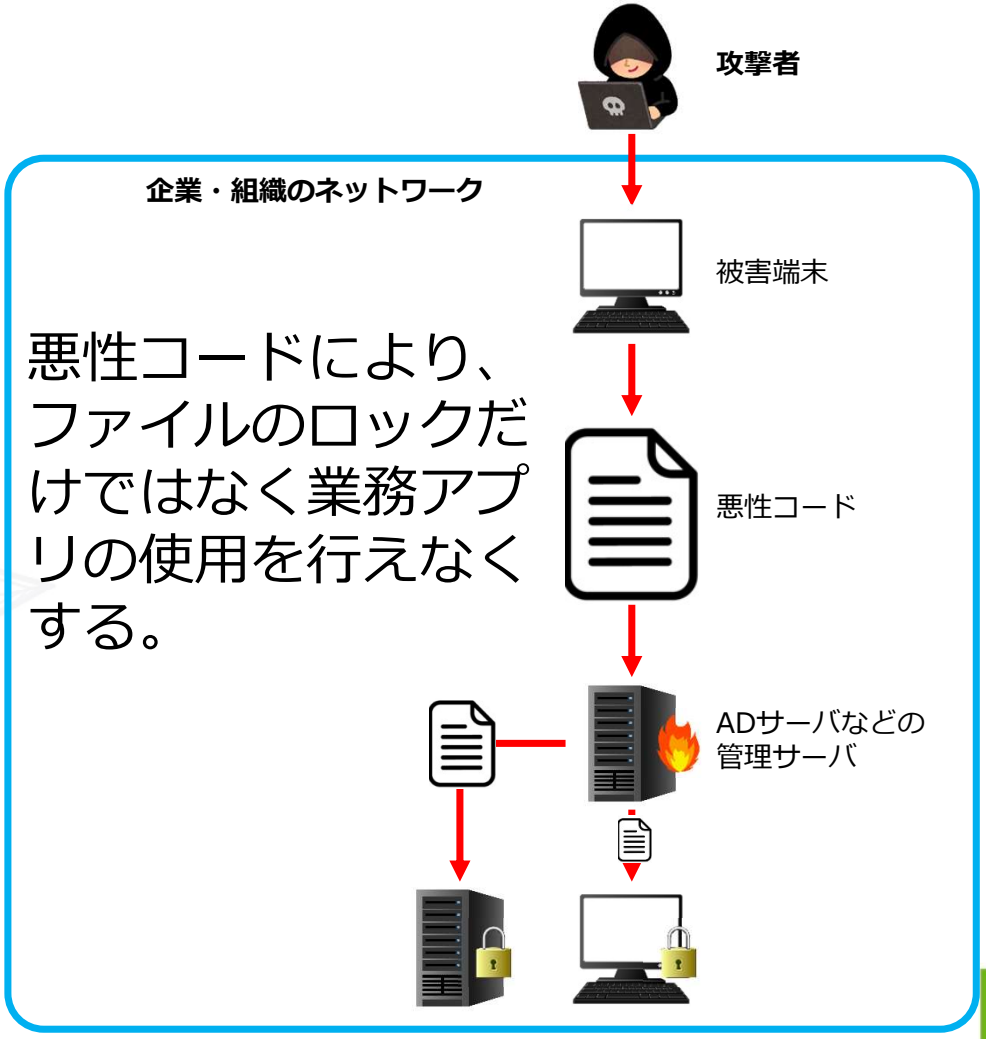


1．ファイル復元の脅迫
2．企業情報公開の脅迫

攻撃の特徴　６選

◆ 破壊型

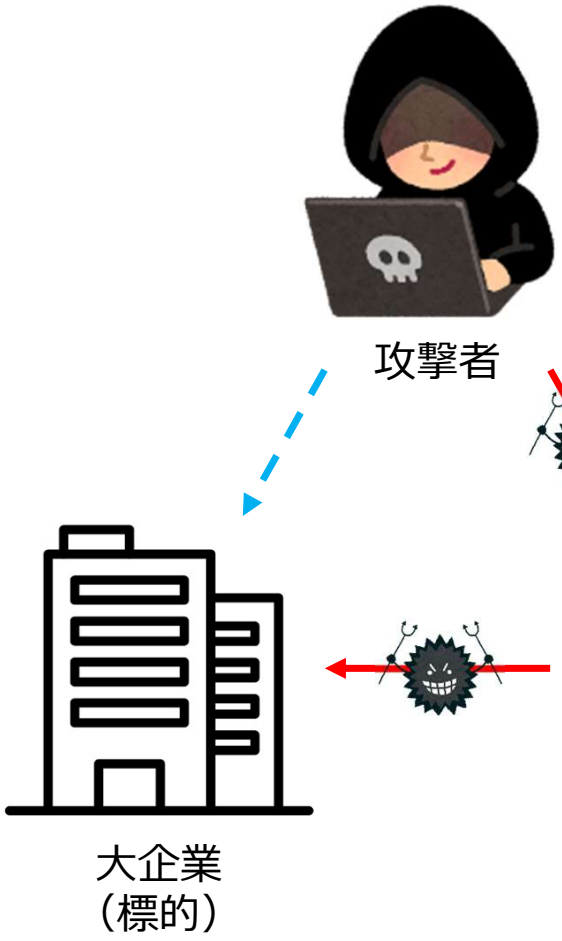
破壊型のランサムウェアは、ファイルやシステムにダメージを与えることを目的としています。「Ryuk」のようにファイルの単一のバックアップだけでは回復不可能な状態になり、企業の操業が停止する恐れがあります。



攻撃の特徴　６選

◆サプライチェーン攻撃

大企業への攻撃をするのではなく、その子会社や関連会社への攻撃をすることで、大企業を間接的に攻撃しようとするランサムウェアです。ランサムウェア攻撃によりサプライチェーンの下流企業の操業が停止すれば、上流企業も影響を受けます。大規模な被害を計画し、その分高額な身代金を要求します。



大企業には、直接攻撃できないため、セキュリティ対策が手薄な子会社を踏み台にして攻撃。

Dr.WEB®
Anti-virus

ランサムウェア攻撃に備えた対策

株式会社Doctor Web Pacific

www.drweb.com

実施すべき対策①

攻撃の糸口	情報セキュリティ対策の基本
ソフトウェアの脆弱性	**ソフトウェアの更新**
ウイルス感染	**セキュリティソフトの利用**
パスワード窃取	**パスワードの管理・認証の強化**
設定不備	**設定の見直し**
誘導（罠にはめる）	**脅威・手口をしる**

実施すべき対策②

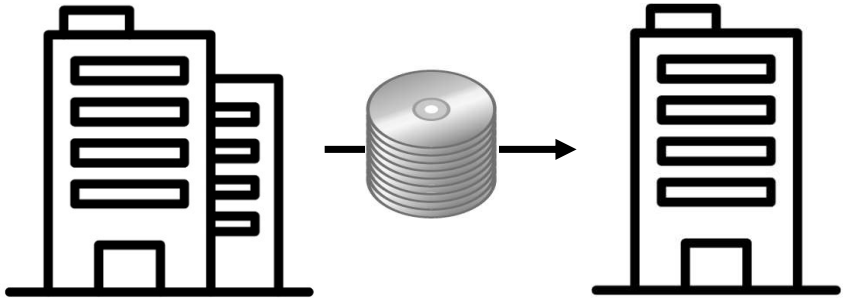
◆ 3－2－1　ルール

あらゆるデータ消失シナリオに対応するため「バックアップの冗長性」を重視したバックアップ方式です。

1．データは少なくとも「3つ」持つ

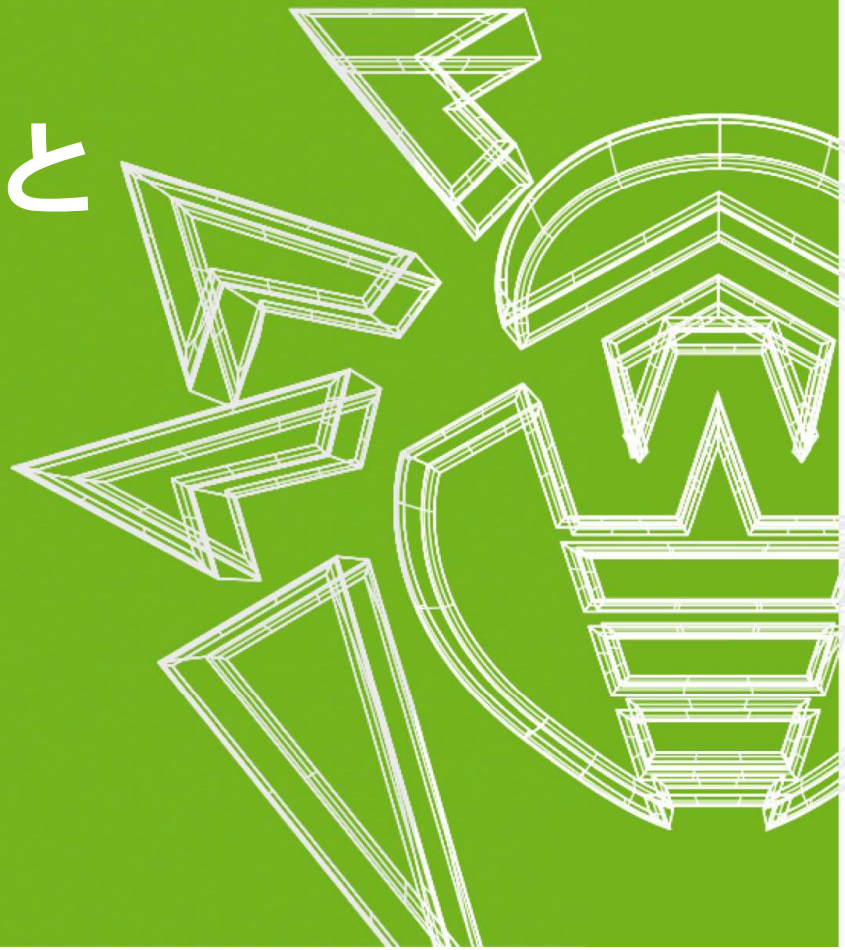
2．「2つ」の異なる媒体に保存する

3．「1つ」のバックアップを別場所に保管



Dr.WEB®
Anti-virus

Dr.Webができること



株式会社Doctor Web Pacific

www.drweb.com

Dr.Webができること

用途	製品名	対応OS等	コメント
エンドポイント	**Dr.Web Desktop Security Suite**	Windows Linux macOS	ふるまい検知を搭載したPC端末用 総合アンチウィルス
	Dr.Web Katana	Windows	ふるまい検知のみ提供
モバイル	**Dr.Web Mobile Security Suite**	Android	世界で1億6000万DLの実績
サーバー	**Dr.Web Server Security Suite**	Windows Linux macOS	Windows向けはふるまい検知搭載 国内ISP/CATVでも実績多数
メールサーバー	**Dr.Web Mail Security Suite**	Unix	国内ISP/CATVでも実績多数 アンチスパムオプションあり
Webプロキシー	**Dr.Web Gateway Security Suite**	Unix	Proxyと連携
修復ユーティリティ	**Dr.Web CureIt!** **Dr.Web CureNet!**	Windows	他社AV搭載の環境で簡単スキャン セカンドオピニオン
無制限ライセンス	**オフィスマルチパック**	Windows Linux macOS Android	中小企業向けデバイス無制限パック
	公共マルチパック		公共期間向けデバイス部制限パック
	小中高等学校向け無制限ライセンス		学校向け無制限パック（学校単位）
	大学専門学校向け無制限ライセンス		大学向け無制限パック（人数単位）
インテリジェント アナライザー	**Dr.Web vxCube**	Windows Android	オブジェクト解析クラウド 未知の脅威に対するワクチン提供
サブスクリプション	**Dr.Web Premium** **サブスプリクションサービス**	Windows Linux macOS	欧州・ロシア初のクラウド型 アンチウイルス

セキュリティソフトの導入！

PC端末のコンポーネント

コンポーネント	説明
SpIDer Guard：リアルタイムスキャン	メモリに常駐し、プロセスとファイルの起動と作成に対して、悪意のあるアクティビティを検出します。
SpIDer Gate：トラフィックスキャン	アクセス先のURLが危険か判断し、ブロックします。
SpIDer Mail：メールスキャン	送受信時のメールウイルスを検出駆除。
Dr.Web Firewall	不正アクセスから保護し、重要なデータがネットワークを通じて漏洩するのを防ぐパーソナルファイアーウォール。
Office Control	Webサイト、ファイル、フォルダへのアクセス制限や、利用デバイスの制限、インターネット接続時間制限などの設定ができます。
動作解析 ：ふるまい検知機能 （Behavior Analysis）	HOSTSファイルや重要なシステムレジストリキーの変更などを監視し、ブロックします。
ランサムウェア保護 ：ふるまい検知機能 （Ransomware Protection）	ランサムウェアをブロックします。
エクスプロイト防止 ：ふるまい検知機能 （Exploit Prevention）	アプリケーションの脆弱性を利用する悪意のあるオブジェクトをブロックします。
Scanner：手動スキャン	ユーザが任意タイミングでスキャンを行います。
Application Control	業務に関係ないアプリケーションの利用をブロックすることができます。

サーバーのコンポーネント

コンポーネント	説明
SpIDer Guard：リアルタイムスキャン	メモリに常駐し、プロセスとファイルの起動と作成に対して、悪意のあるアクティビティを検出します。
SpIDer Guard for SMB ：リアルタイムスキャン	Samba共有ディレクトリ内のファイルに適用されたアクションをモニタリングします。常駐モニターとして機能し、保護対象のファイルシステム内の基本的なアクション（作成、開く、閉じる、読み取り、書き込みの操作）を制御します。
動作解析 ：ふるまい検知機能 （Behavior Analysis）	HOSTSファイルや重要なシステムレジストリキーの変更などを監視し、ブロックします。
ランサムウェア保護 ：ふるまい検知機能 （Ransomware Protection）	ランサムウェアをブロックします。
エクスプロイト防止 ：ふるまい検知機能 （Exploit Prevention）	アプリケーションの脆弱性を利用する悪意のあるオブジェクトをブロックします。
Scanner：手動スキャン	ユーザが任意のタイミングでスキャンを行います。

※OSによって、利用できないコンポーネントがございます。

Dr.WEB®
Anti-virus

www.drweb.com
www.drweb.co.jp/
drweb-antivirus.jp/