Dr.WEB®
Anti-virus

ランサムウェア入門

株式会社Doctor Web Pacific

www.drweb.com

Dr.WEB®
Anti-virus

今回のテーマ

- ランサムウェアとは
- 海外での被害事例
- 感染経路、攻撃の手口
- Dr.Webでできること

Dr.WEB®
Anti-virus

ランサムウェアとは

株式会社Doctor Web Pacific

ランサムウェアとは

◆ランサムウェア（英語：ransaomware）

マルウェアの一種です。

●マルウェア（malware）

不正かつ有害に動作させる意図で作成された悪意ある

ソフトウェアや悪質なコードの総称

- コンピュータウィルス
- ワーム
- スパイウェア

：

- ランサムウェア

ランサムウェアとは

◆感染したコンピュータは、ファイル及びデータを**暗号化**し、ファイルやシステムなどを利用できなくなる。

◆暗号化を解除するため、被害者に**身代金（ransom、ランサム）を**ビットコインなどで**要求する。**

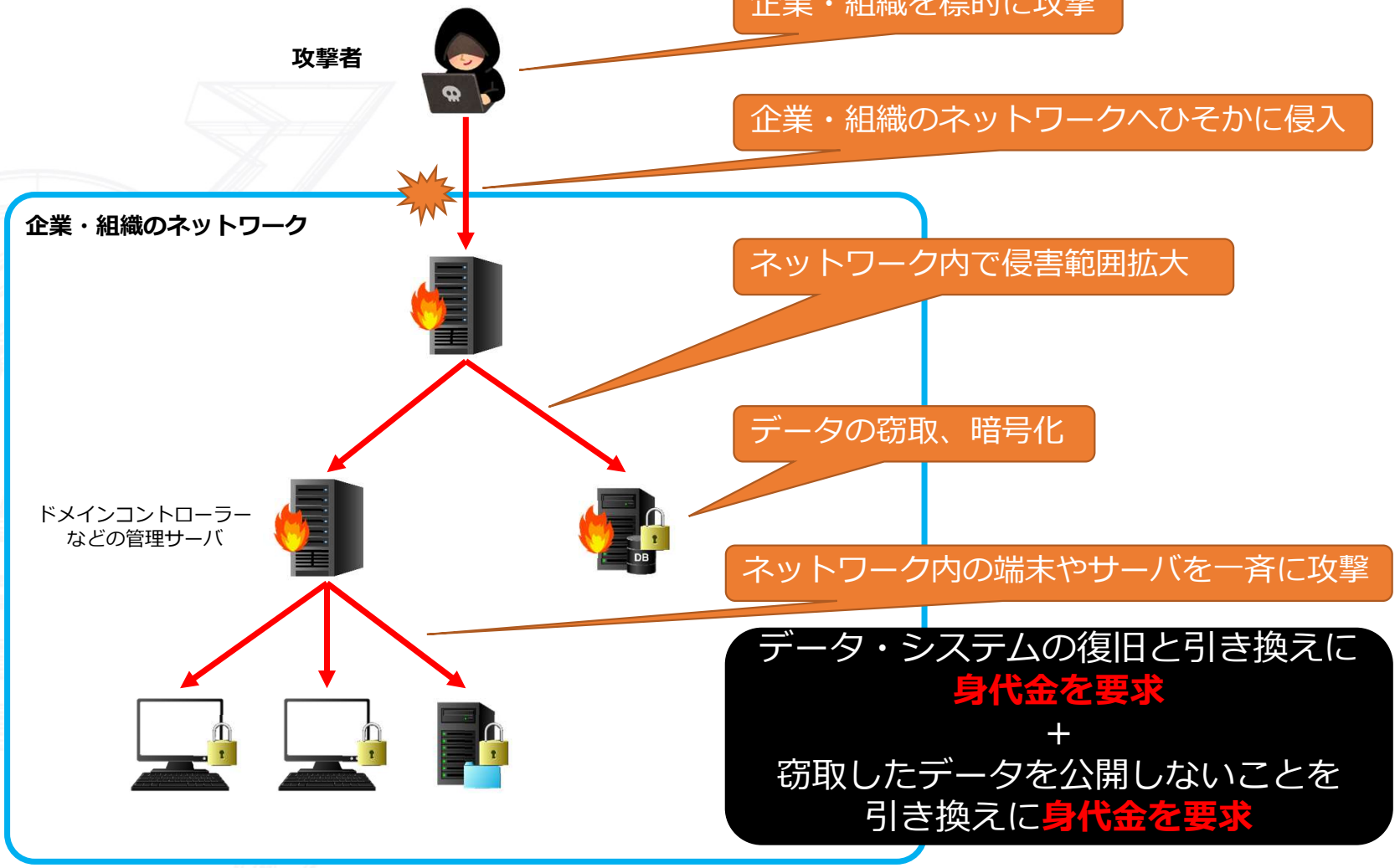
◆感染したファイルを窃取して、機密情報などをダークウェブに開示するという**脅迫**を行うことにより、**身代金（ransom、ランサム）を要求する。**

情報セキュリティ10大脅威 2023

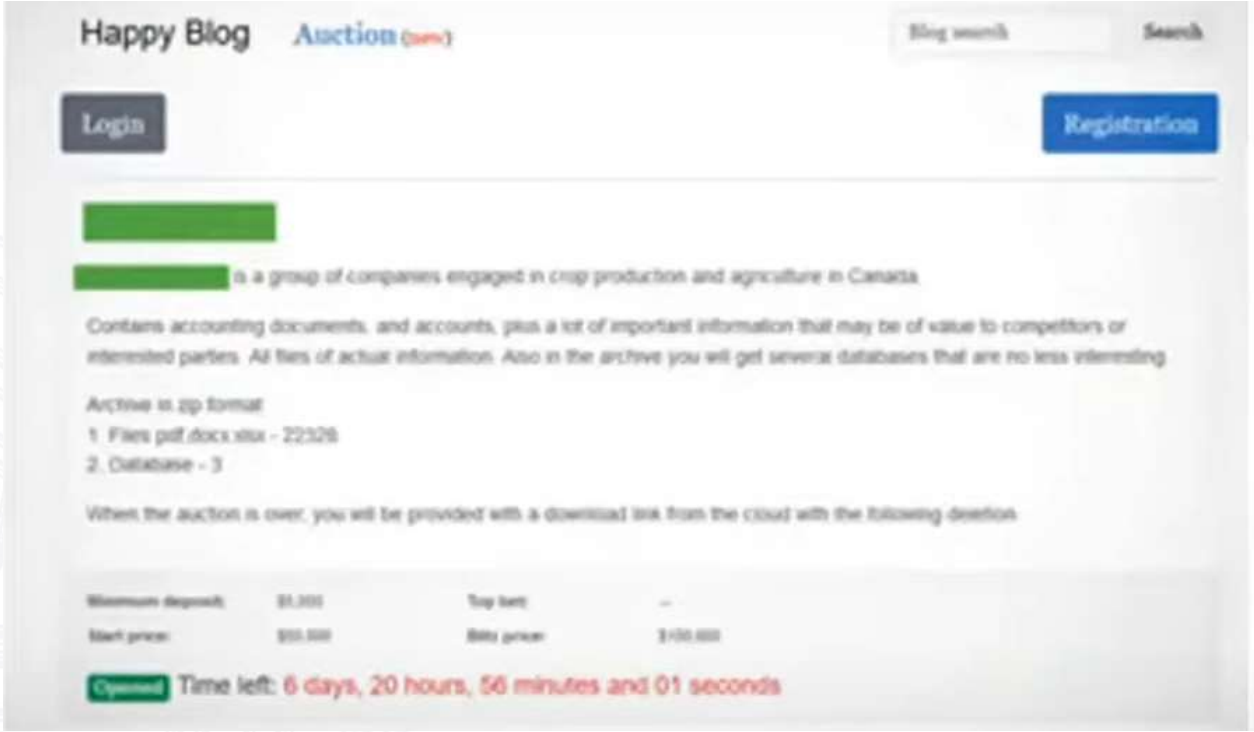
前年順位	個人	順位	組織	前年順位
1位	フィッシングによる個人情報等の詐取	1位	ランサムウェアによる被害	1位
2位	ネット上の誹謗・中傷・デマ	2位	サプライチェーンの弱点を悪用した攻撃	3位
3位	メールやSMS等を使った 脅迫・詐欺の手口による金銭要求	3位	標的型攻撃による機密情報の窃取	2位
4位	クレジットカード情報の不正利用	4位	内部不正による情報漏えい	5位
5位	スマホ決済の不正利用	5位	テレワーク等の ニューノーマルな働き方を狙った攻撃	4位
7位	不正アプリによる スマートフォン利用者への被害	6位	修正プログラムの公開前を狙う攻撃 （ゼロデイ攻撃）	7位
6位	偽警告によるインターネット詐欺	7位	ビジネスメール詐欺による金銭被害	8位
8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	脆弱性対策情報の公開に伴う悪用増加	6位
10位	インターネット上のサービスへの 不正ログイン	9位	不注意による情報漏えい等の被害	10位
圏外	ワンクリック請求等の 不当請求による金銭被害	10位	犯罪のビジネス化 （アンダーグラウンドサービス）	圏外

https://www.ipa.go.jp/security/vuln/10threats2023.html 参照

ランサムウェア攻撃



ダークウェブのオークション



「某国の穀物生産・加工を行う企業Aに関する重要情報を販売。
会計監査に関するドキュメントやアカウント情報に加え、
多数の重要情報を含むファイル。競合他社には有益」
「スタート価格50,000ドルから」と紹介し、オークション形式で購入者を募っている。

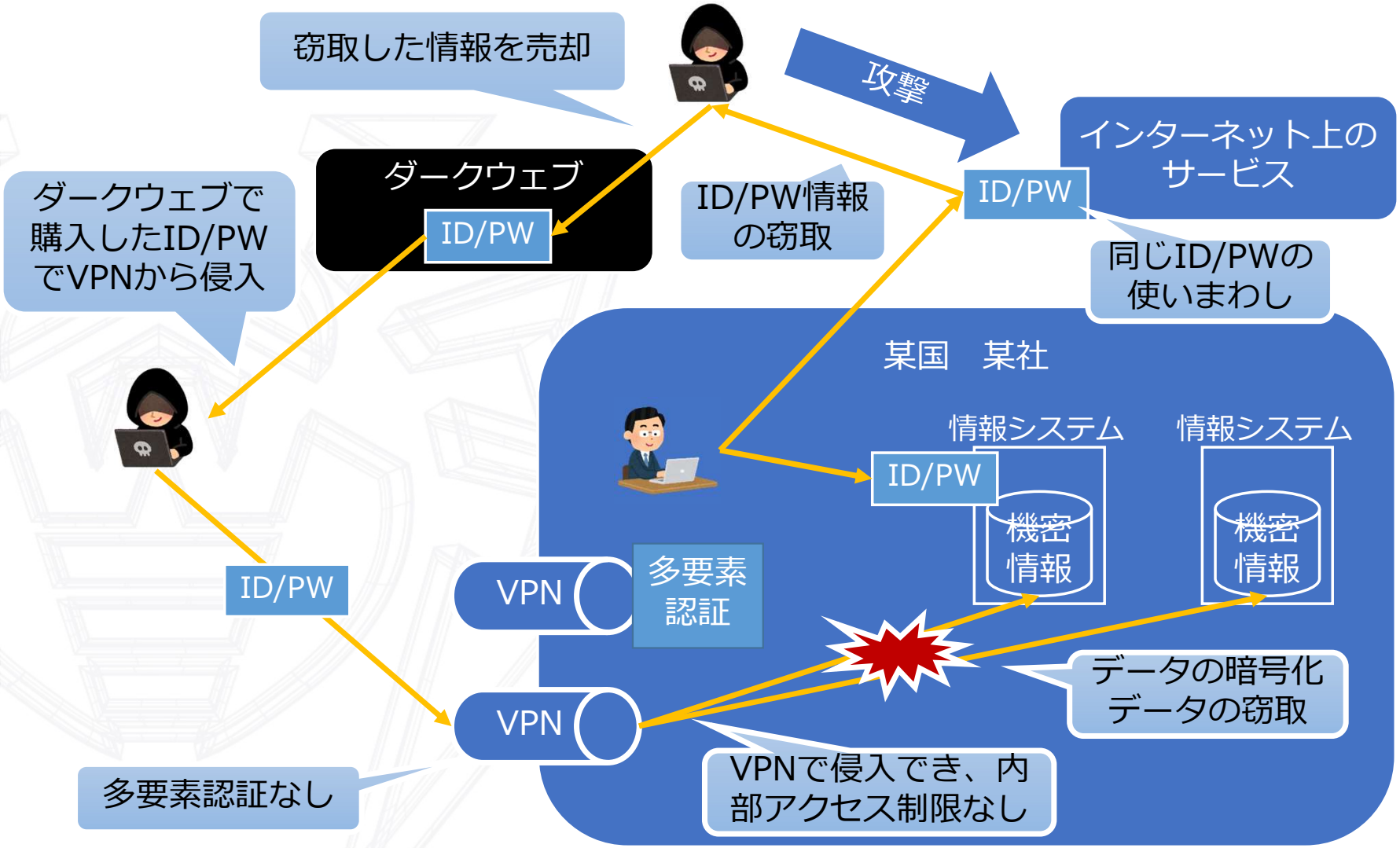
Dr.WEB®
Anti-virus

海外での被害事例

株式会社Doctor Web Pacific

www.drweb.com

海外での被害事例



Dr.WEB®
Anti-virus

感染経路
攻撃の手口

株式会社Doctor Web Pacific

www.drweb.com

感染経路

- メール開封、添付ファイルのダウンロード
- Webサイト（不正サイト）の閲覧
- ソフトウェアのダウンロード
- USBメモリ

攻撃の手口

- ネットワークへの侵入
  - リモートデスクトップサービス（ID、パスワード）
  - VPN装置の脆弱性
  - 遠隔操作マルウェアの感染
- ネットワーク内の侵害範囲拡大
  - ネットワーク構成の把握、管理者権限の奪取
  - ADを乗っ取り、AD管理下のPCの感染
  - 機密情報の探索
  - バックアップの破壊
- データの持出
- PCやサーバのデータ暗号化・業務アプリなどの停止
- 身代金の要求
- ダークウェブなどで、データの販売

Dr.WEB®
Anti-virus

Dr.Webでできること

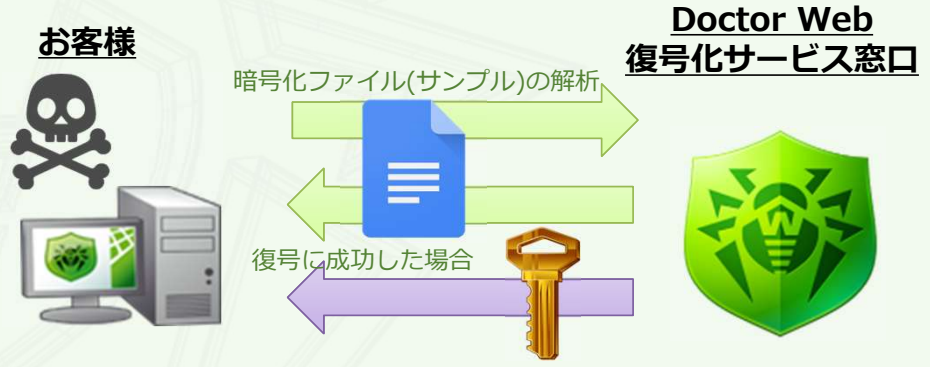
株式会社Doctor Web Pacific

www.drweb.com

Dr.Webでできること

ランサムウェア被害救済サービス（Rescue Pack）

お使いのアンチウイルスソフトを問わずどなたでもご利用頂ける
ランサムウェアによる暗号化被害ファイルの復号化サービスです。
Doctor Webウイルスラボでは2014年からファイル復号化ルーチンを
徹底的に研究しております。
マルウェアインテリジェンスで得られる情報を掛け合わせ高い確率で
多くの暗号化ファイルを救済しております。



Dr.Webユーザは
無償対応
(条件による)

※2022年は、2021年と比較して**2.3倍のお問合せ**が有りました。

Dr.Webでできること

Dr.Web CureIt! / CureNet!

PC及びサーバーのウィルス検知・修復。既存アンチウィルスソフトでは検知出来ないマルウェアを炙り出す非常駐型スキャナ。他社アンチウィルスと共存可。
インストール不要。

ご利用中のアンチウイルスソフトで発見できなかった
マルウェアを、検知・駆除を行います。
セカンドオピニオンツールとして
ご活用ください。

Dr.WEB®
Anti-virus

Dr.Web製品

株式会社Doctor Web Pacific

www.drweb.com

Dr.Webの製品

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	**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

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/