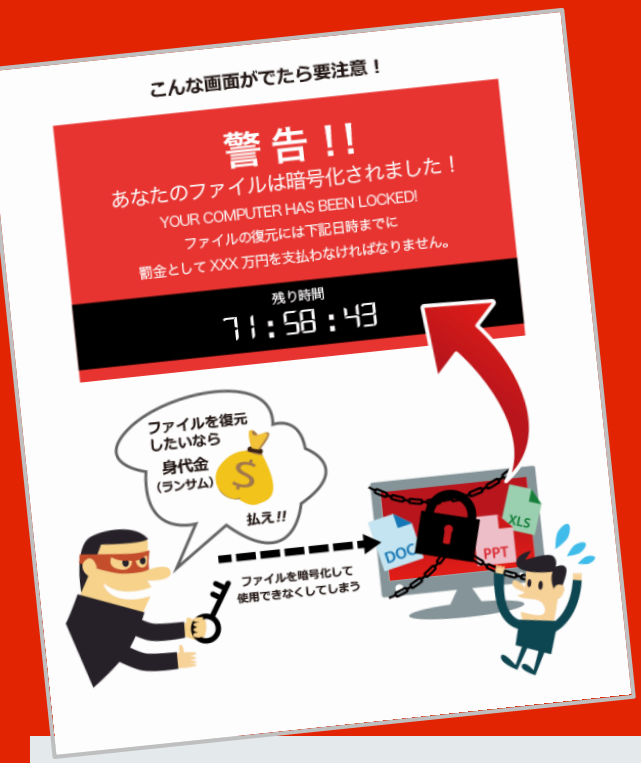
セキュリティ～バックアップまで
ネットワールドの
ランサムウェア対策



ランサムウェアとは?

ランサムウェアとは、ユーザーの同意なくユーザーのコンピューターに違法にインストールされる マルウェア (悪意のあるソフトウェア) の一種で、コンピューターのファイルを暗号化して“人質”にとった上で、「復号するパスワードを教えるから身代金（ランサム）を出せ」等の要求をする非常に悪質なプログラムです。

感染ルートは?

■メールから
主な感染源。メールに添付されたファイルを開くことで感染

■Webサイトから
改ざんされ、ウイルスが仕込まれてしまったWebサイトにアクセスすることで感染

ターゲットは?

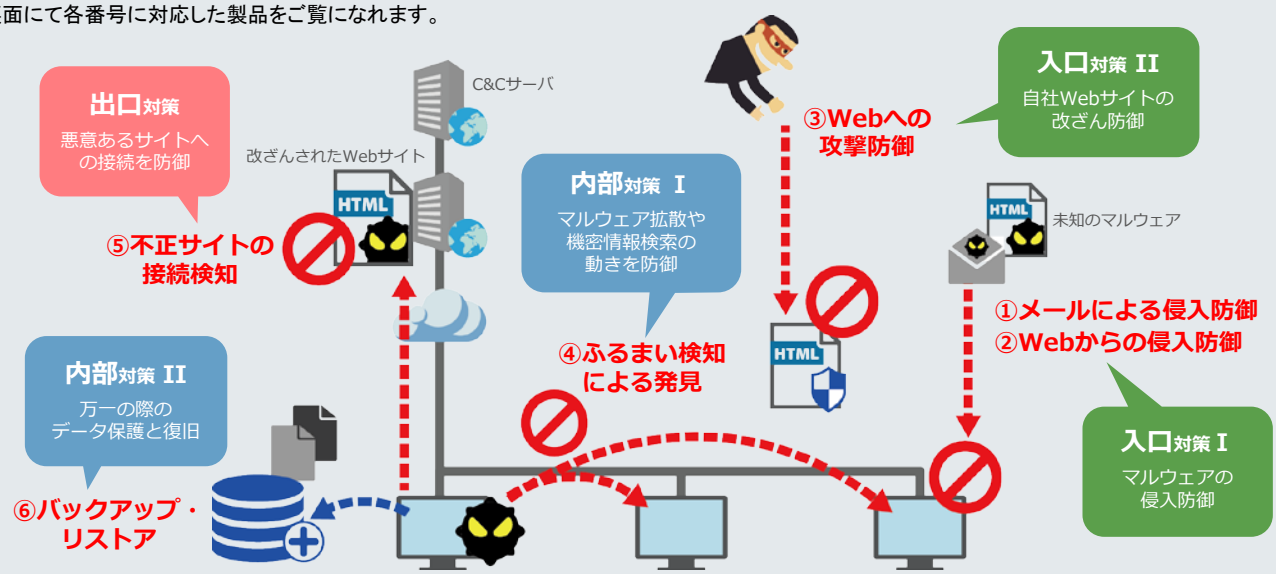
サイバー犯罪者は、多くの標的に攻撃を仕掛けてより多くの金銭的利益を得ようとするため、企業でも個人ユーザーでもどちらもが標的になる可能性があります。
従来は個人利用者を標的に犯罪を行うものが主流でしたが、日本国内では、2015年より民間企業をはじめとした法人組織におけるランサムウェアの被害が顕在化し始めています。

感染被害や影響は?

■PCの操作ができなくなる
■ローカルデータだけでなく、感染したPCにネットワークで接続したドライブや共有フォルダ、クラウドの同期ドライブ等も利用できなくなるため、全社的に使用不能になる可能性がある。
■グループアドレス宛てのメールから感染することも多く複数台が感染する。
■「身代金」を支払うことにより金銭的な被害を被る

企業に求められる安全対策

セキュリティとバックアップの2大対策が必要。さらに入口・出口・内部にそれぞれ対策を講じ、万全な体制にしましょう。
裏面にて各番号に対応した製品をご覧になれます。



企業に求められる安全対策⑴　セキュリティソフトの導入

ランサムウェアに限らず、どのようなマルウェアに対してもセキュリティソフトの導入は不可欠です。
以下のようなポイントをふまえた導入を検討しましょう。

1 ウイルス検知
ランサムウェア本体を検出、パターンマッチングだけでなく、怪しい動きを監視してブロックする「ふるまい検知」と、ウェブサイトでの表示で問題のあるURLをブロックする機能があるウイルス対策ソフトが好ましい。
無料ウイルス対策ソフトは機能が弱いため、お薦めできない。

2 メールセキュリティ
メールの添付ファイルへのウイルス検出とスパム対策機能により、電子メール経由での不正プログラム侵入を防ぐ。
安易に添付ファイルを開かないことも覚えておきたい。知り合いや取引先でも信用せず、本物かどうか問い合わせてから開くぐらいの警戒心を持つことが重要。

3 不正サイトアクセス制限
ユーザーが気付かずに不正Webサイトにアクセスすると、ランサムウェアに感染したドライバを自動的にダウンロードし、不正プログラムが実行されてしまう。
不正サイトへのアクセス自体をブロックすることで、ランサムウェアや他の不正プログラムの侵入、認証情報の送信等を防ぐ。

4 脆弱性のアップデート
脆弱性を狙った攻撃が多く報告されているため、クライアントPCのOS、Flash、Java、PDF表示、ブラウザなどのソフトを常に最新版にしておく必要がある。
自動更新の設定をして通知が出たら即座にアップデート出来るような状態にしておく。

おすすめのセキュリティ対策製品

入口対策		
① メールによる侵入防御	Fortinet FortiMail + Fortinet FortiSandbox	Symantec.cloud（Email.cloud/Web Security.cloud）
	Trend Micro Deep Discovery Email Inspector	GUARDIANWALL
	Trend Micro InterScan Messaging Security Virtual Appliance	SpamSniper
	Trend Micro Cloud App Security	
② Webからの侵入防御	Fortinet FortiGate + Fortinet FortiSandbox	DELL SonicWALL
	Clavister	Check Point Gateway Appliance/vSEC
③ Webへの攻撃防御	F5 BIG-IP Application Security Manager（ASM）	
内部対策		
④ ふるまい検知等による発見や制御	Trend Micro ウイルスバスター コーポレートエディション Plus	Symantec Advanced Threat Protection
	Trend Micro ウイルスバスター ビジネスセキュリティ	Soliton Zerona PLUS
	Trend Micro Deep Discovery Inspector	Fortinet FortiClient
	Trend Micro Deep Security	ESET セキュリティ ソフトウェア シリーズ
	Kaspersky Security for File Server	Faronics Deep Freeze
	Kaspersky Endpoint Security for Business – Advanced/Select	PFU iNetSec IntraWall / 標的型サイバー攻撃対策支援サービス
	Carbon Black CB Defense	Check Point SandBlast Agent
出口対策		
⑤ 不正サイト接続防御	RedSocks Malicious Threat Detection (MTD)	Trend Micro InterScan Web Security Virtual Appliance

企業に求められる安全対策⑵　バックアップの取得

万が一、感染してしまっても感染前の状態に復元できるように定期的なバックアップ取得は必須です。
一般的にバックアップは普及していますが、ランサムウェア対策としては以下のポイントをおさえておきましょう。

1 全領域のバックアップ
感染前の環境を丸ごと再現するには、データ領域だけでなく、システム領域を含めたバックアップをとることがおすすめ。そうすることで、復旧のスピードも各段に速くなる。
また、サーバだけでなくクライアントPCも同様に保護しておけば、いずれの場合でも感染前の状態に簡単に復元することが可能。

2 世代管理を行う
1世代のみのバックアップでは、感染後にバックアップが実行されてしまうとデータを取り戻す手段はなくなるため、
少なくとも2世代以上はバックアップをとるのが良い。
感染の発見が遅れた場合でも、希望のデータを復旧できる可能性は大きい。

3 アクセスできない場所に保存
ランサムウェアはネットワークドライブも暗号化するため、パソコンに接続したままのドライブへのバックアップは意味がない。
やるべきことは取り外せるドライブへのバックアップ、クラウドなら同期しない形でのバックアップを取る。

おすすめのバックアップ対策製品

内部対策				
⑥ バックアップ・リストア	Veritas System Recovery	Arcserve UDP	Veeam Backup & Replication	Acronis Backup Service
	RDX QuikStor	Air Back Plusシリーズ	Secure Back	

Networld
株式会社ネットワールド　http://www.networld.co.jp/

お問い合わせ　security-info@networld.co.jp

本　　社　〒101-0051 東京都千代田区神田神保町2-11-15 住友商事神保町ビル　TEL:03-5210-5020,5031,5095
関 西 支 店　〒530-0001 大阪市北区梅田3-3-20 明治安田生命大阪梅田ビル 24F　TEL:06-7664-5400
中 部 支 店　〒451-6008 名古屋市西区牛島町6-1 名古屋ルーセントタワー 8F　TEL:052-588-7611
九 州 支 店　〒812-0013 福岡市博多区博多駅東2-6-1 九勧筑紫通ビル 3F　TEL:092-461-7815

2018年 1月