SUNSYSTEM
創業1991年
2025年11月号

クラウドサービスも
サンシステムへ

オフィスのパートナー
有限会社サンシステム
三田市東本庄2070番地の5
TEL079-556-7663 FAX079-556-7664
E-mail:oa-shop@oa-sunsystem.co.jp
URL:www.oa-sunsystem.co.jp

重要なお知らせ

ランサムウエアについて！

最近アサヒGHD、アスクルが甚大な被害に遭遇しておりますランサムウエアにつきまして、考えてみましょう。

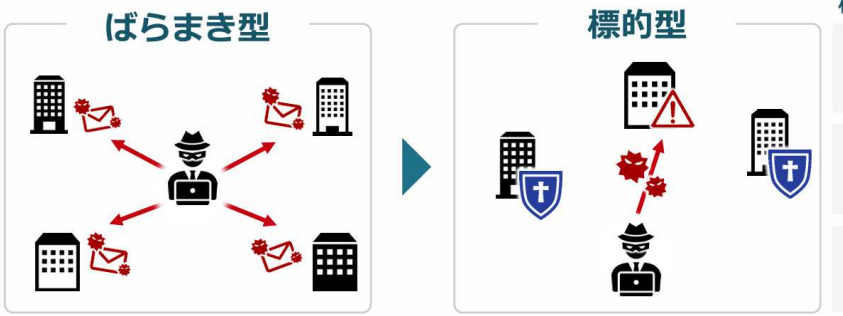
ランサムウェアとは

Ransom(身代金)を要求してくる不正プログラム
感染したPC・ハードディスク・データなどを**使用不能**にし、
それらの復旧と引き換えに**金銭の支払いを要求**するという手口が主流のマルウェア

ランサムウェアに感染すると…

1つの機器が感染すると、同じネットワークに繋がっているPC、NASといった**別の機器の共有フォルダーにも拡散、感染**し、ネットワーク全体へ被害をもたらします。

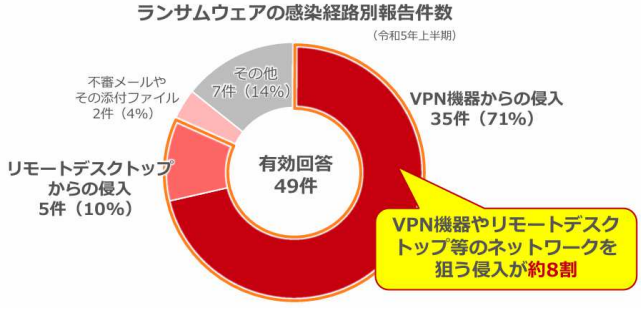
従来は電子メールなどを不特定多数へ拡散し、感染を狙う「ばらまき型」が一般的でしたが、
近年では**システムの脆弱な組織をピンポイントで狙った「標的型」**の手法が増えています。



標的型の攻撃

- VPN機器やRDPの脆弱性を突いて侵入
- マルウェアを実行し、情報を窃取・データの暗号化
- 情報流出・データ復旧の2点から脅迫

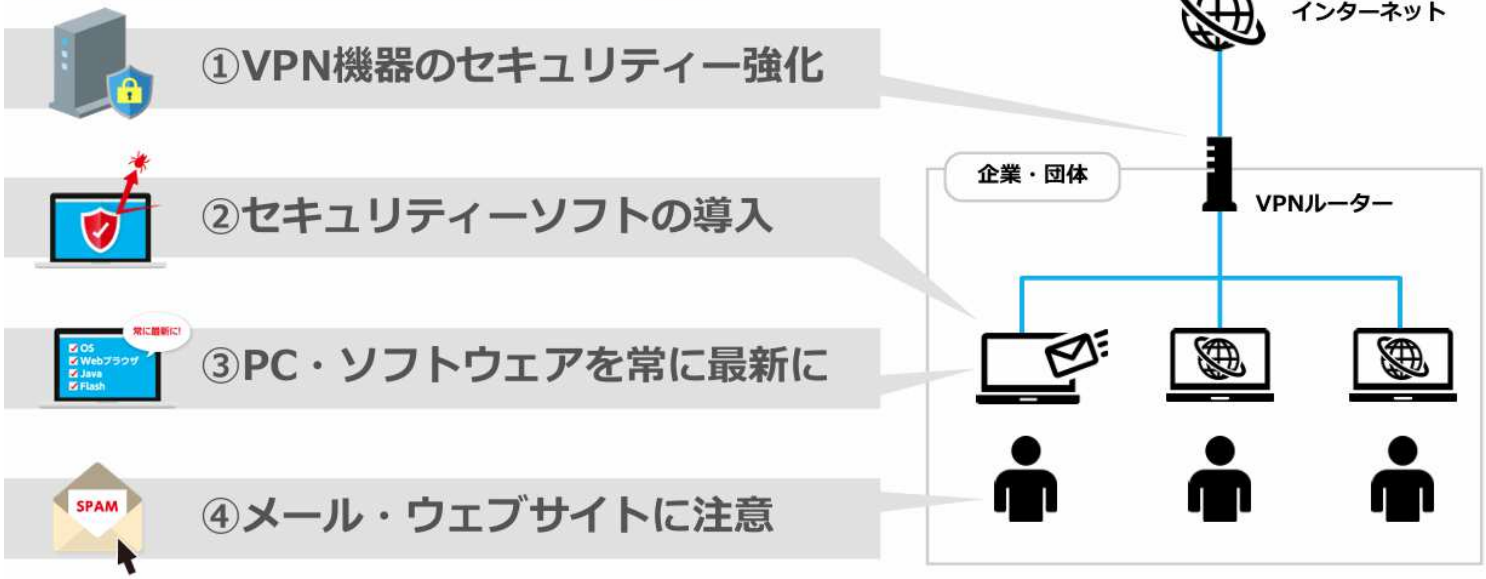
感染経路別報告件数を見ると、VPN機器やリモートデスクトップを狙った手口が約8割を占めます。
Chapter01で紹介した国内医療機関 A病院、自動車部品メーカー B社の事例も、VPN機器が原因だったとされています。



従来のばらまき型への対応点

- メールやSMSなどの添付ファイルやリンク
  （請求書/宅配通知/ポイント付与を装うものなど）
- 正規サイトを模した偽サイトへのアクセス
  限りなく本物のサイトに似せた偽サイト）
- 感染したUSBメモリや外付けストレージの利用

感染前の予防



ランサムウェア対策チェックリスト

No	チェック項目	チェック
1	VPN機器のセキュリティーを強化する	
2	ウイルス対策ソフト(EPP：Endpoint Protection Platform)や、エンドポイント上でのセキュリティーインシデントの検出と対応を行うEDR（Endpoint Detection and Response）を導入する	
3	PC・ソフトウェアを常に最新状態に保つ	
4	メールの添付ファイル・ウェブサイトに注意する	
5	社内教育・啓発を定期的に行う	
6	感染したPCを隔離する/隔離する方法を把握しておく	
7	書き換えができない形式でのデータのバックアップをこまめにとる	
8	感染を想定した対応訓練を行う	

もし感染してしまったら

まずネットワーク接続を切断（LANケーブルをパソコンから外す、Wi－Fiの場合は無線を切る）し、パソコンをシャットダウンしてご連絡下さい。

Q&A

Q. ランサムウェアに感染しても、お金を払えばデータは戻るの？

A.ほとんどの場合、支払ってもデータは戻りません。再び標的にされるリスクも高まります。

Q. 無料のウイルス対策ソフトでも防げますか？

A.一定の防御効果はありますが、十分ではありません。
リアルタイム保護や不審な通信のブロック機能が限定されることがあります。
できれば信頼性の高い有料版、またはWindows標準の「Microsoft Defender」を最新の状態で使うことをおすすめします。

Q. バックアップはどれくらいの頻度で行えばいいですか？

A.理想は週1回程度ですが、頻繁にファイルを更新する場合は毎日でも構いません。
写真や仕事用データなど、失うと困るものは定期的に外部ストレージやクラウドに保存しておくと安心です。

対策方法は12月号でご紹介いたします