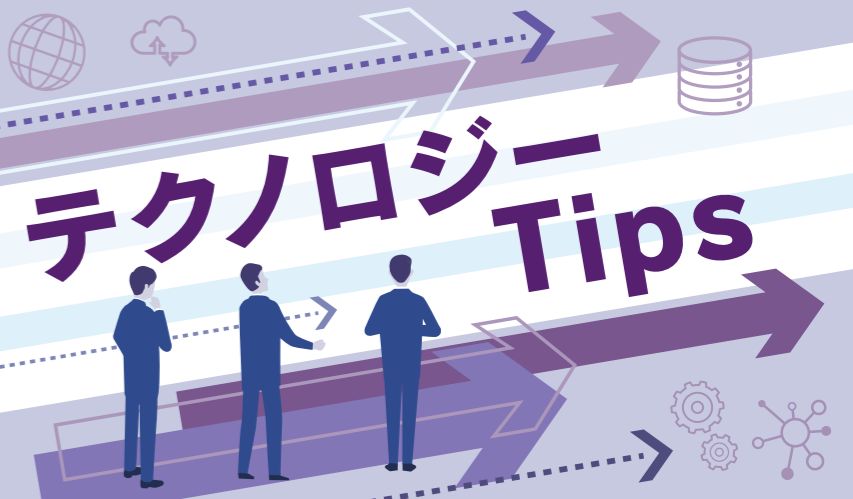




# もはや「当社は関係ない」なんて思ったり、言ったりしていませんか… セキュリティ対策はデジタル社会に おけるマナー・ルール・経営課題です!

担当者レベルの「問題」ではなく、「経営の課題」。  
つまり経営者の責任で、体制構築し、適切な投資をするべき重要事項です。

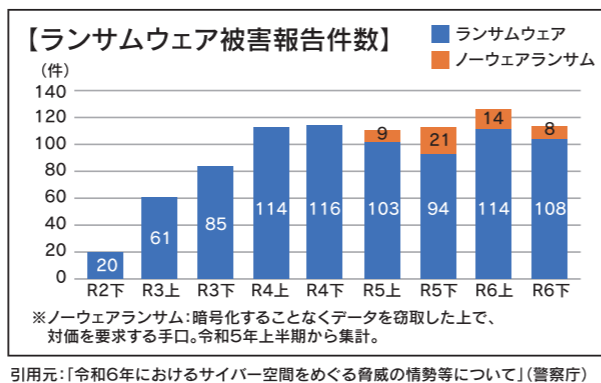


「セキュリティ対策は重要です!」と言われてから10年以上…。インシデントは減少するどころか増加傾向…。  
さらに、昨今は対策の強化を迫られています。その背景を3つのポイントに絞ってご説明します。

**POINT 1** 「IPA 情報セキュリティ10大脅威 2025」が発表する脅威の頂点に君臨するのは、やはりランサム攻撃です。10年連続で首位の座を譲らないこの脅威が、今、どのようにその姿を変え、牙を剥いているのか…しっかり知っておくことが重要です。

オレンジ色の部分は  
「**ノーウェアランサム**」と言われる攻撃です。

**ノーウェアランサム (No-ware Ransomware) って?**  
データを暗号化せず、盗むだけの新しいタイプのサイバー攻撃です。盗んだ機密情報を公開すると脅迫し、金銭を要求します。



## なぜ流行しているの?

- 1 簡単だから** 高度な技術がなくても攻撃できます。
- 2 バックアップが効かないから** データが盗まれるため、バックアップがあっても情報漏洩の被害は防げません。
- 3 気づかれにくいから** 暗号化しないので、被害に気づくまで時間がかかります。

つまり、攻撃者にとって効率が良く、防御側には厄介なため、被害が増えています。  
さらにさらに…「技術」がなくても、攻撃者になれる??  
「Ransomware as a Service: RaaS」って知っていますか?  
高度なランサムウェア攻撃に必要なツール一式を、  
～専門知識のない人でも使えるよう「サービス」として販売するビジネスモデル～です。

## 想像してみてください!!

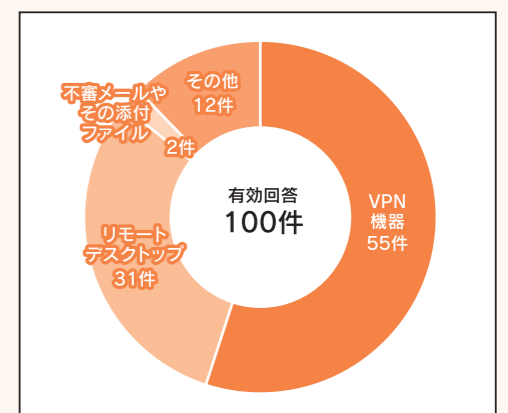


サイバー攻撃を仕掛けるために、もう高度なハッキング技術は必要ありません。  
誰でも、手軽な料金で「ランサムウェアの攻撃キット」をダークウェブ上で購入できる時代です。  
そこには、攻撃用のマルウェアだけでなく、ターゲットの探し方、身代金の要求方法、さらには支払い交渉のサポートまで、すべてが含まれています。かつては一部の専門的で高度な技術を持つハッカーしか行えなかったランサムウェア攻撃が、「誰でもボタン一つで実行できる」危険なサービスとして広まっています。  
「ちょっとしたお金稼ぎ」や「簡単な投資」、「冒険や悪ふざけ」の感覚で、サイバー犯罪に手を染めてしまう可能性も増えています。



## 実は!知っていますか?

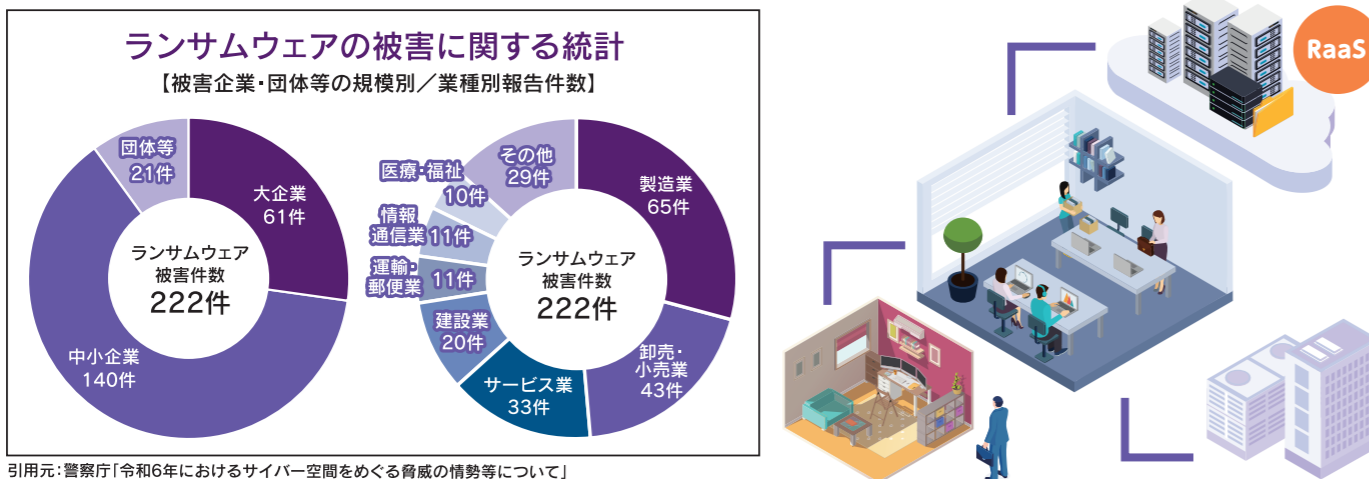
意外にも「ランサムウェア」の感染経路は**80%以上が「VPN機器」「リモートデスクトップ」**です。不審メールや添付ファイルなどを開いて感染するケースが多いように見受けられやすいですが、コロナ禍以降のテレワークなどの働き方の変化に応じ、新たな侵入経路が出てきたと考えられます。**ネットワークの構築方法、VPNの設定やクライアント、ルーターなどの機器にも対策が迫られています。**



引用元:警察庁「令和6年におけるサイバー空間をめぐる脅威の情勢等について」

## POINT 2 「IPA 情報セキュリティ10大脅威 2025」の第2位、サプライチェーンや委託先を狙った攻撃。

- 知っていますか？被害の6割以上が中小企業！！
- 業種は関係ありません。特定の組織を狙うのではないバラマキ型がトレンドです。
- 2024年の中小企業の被害件数は、前年に比べて37%増加しています！
- RaaS(ランサムウェア・アズ・サービス)により、攻撃実行者の裾野が広がり、対策が比較的手薄な中小企業の被害増加につながっていると警察庁も強く警鐘を鳴らしています。

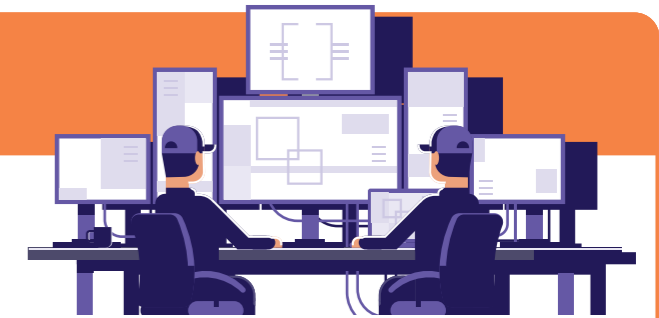


### サプライチェーンの弱点を悪用した攻撃事例

発生年月	攻撃対象企業名	攻撃経路・踏み台	被害内容
2020年1月	三菱電機株式会社	協力企業アカウントの不正利用 - 中国にある子会社・協力会社への攻撃を踏み台に、本社の社内ネットワークへ侵入	機密情報および最大約8,000人分の個人情報外部に流出した可能性
2021年11月	パナソニック株式会社	海外子会社サーバ経由の侵入 - 海外子会社のサーバを経由して本社のファイルサーバに不正アクセス	採用応募者・インターン参加者・取引先役員の個人情報などが保存された社内ファイルに不正アクセスされ、一部データが読み出された可能性
2022年2月	トヨタ自動車株式会社	取引先企業へのランサムウェア攻撃 - 一次仕入先の小島プレス工業の子会社で使用していたリモート接続機器の脆弱性を悪用され、同社ネットワーク経由でトヨタのシステムに侵入	小島プレス工業内のサーバ・PCがランサムウェアにより一部暗号化され、トヨタの国内全14工場28ラインが2022年3月1日に稼働停止(翌日再開)に追い込まれた。 ※情報流出は確認されず
2022年10月	大阪急性期・総合医療センター	取引先業者のVPN悪用 - 病院と取引のある給食業者(委託先)のVPN機器の脆弱性を突かれ、そこから院内ネットワークに不正侵入	病院の基幹システムにランサムウェア感染。サーバやPC計約1,300台のファイルが暗号化され、電子カルテ等が使用不能に。緊急以外の手術・外来診療を停止し、基幹システム再稼働に43日、全復旧に73日を要した(推計被害額:十数億円)
2023年11月	LINEヤフー株式会社	外部委託先PCのマルウェア感染 - 委託先企業の従業員PCがマルウェア感染し、関連企業であるNAVER Cloud社のシステム経由でLINEヤフー内部に不正アクセス	ユーザー・従業員・取引先に関する約44万件の個人情報流出したと公表

## POINT 3 AIがサイバー犯罪の武器となる時代へ。

2023年以降、「生成AI」の爆発的な普及は、私たちの働き方を一変させました。しかし、この革新的な技術は、セキュリティの脅威を劇的に加速させています。いまや攻撃者は、生成AIを悪用し、人間の手では不可能だった速度と精度で、巧妙なサイバー攻撃を生み出すようになっています。**AIがもたらす新たなリスクを理解し、その進化に備えなければなりません。**



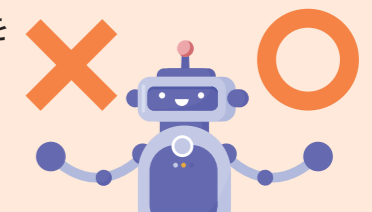
### 1 情報漏洩のリスク

生成AIに機密情報や顧客データを入力すると、その内容が外部のAIサービス提供者側に保存され、第三者に推測されたり再利用されたりする可能性があります。



### 2 誤情報(ハルシネーション)のリスク

もっともらしい回答を返しますが、事実に基づかない誤った情報を含むことがあります。



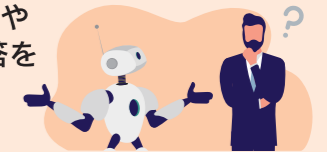
### 3 著作権・知的財産侵害のリスク

生成AIが作成した文章や画像には、既存の著作物と類似した内容が含まれる場合があります。



### 4 不適切な回答のリスク

インターネット上の多種多様なデータを学習しているため、差別的な表現やバイアスのかかった回答を生成してしまう場合があります。

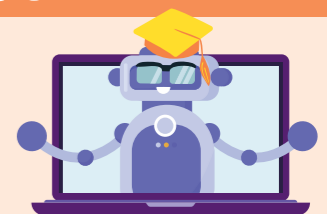


### 5 従来の攻撃手法のAIによる強化

人手をAIで代替することにより攻撃力を増強することができます。また、ターゲットの調査やプログラミング等にAIを利用すれば、より簡易・効率化が可能になり、攻撃がさらに巧妙化・効率化し、裾野が拡大する恐れがあります。

### 6 言葉の壁がなくなる

言葉の壁もなくなり、AIにより文面が巧妙化し、攻撃を見抜くことも難しくなります。



### 7 AIによるディープフェイクを利用するケースも

電話で、社長のディープフェイク音声により、送金を指示することや、ビデオ会議で、本人そっくりなディープフェイク動画により送金を指示したりして、資産やお金を搾取することも簡単になります。



もはや、サイバーセキュリティは一部の専門家や担当者だけの問題ではありません。デジタル社会の健全な発展のためには、すべての企業が果たすべき「マナー」であり「ルール」です。そして、このルールを守ることは、企業の信用を築き、未来の成長を守るための最優先の「経営課題」にほかなりません。今こそ、経営者の方がその責任を自覚し、適切な投資と体制構築を、会社の最重要事項として実行すべき時です。



当社がしっかりご提案、導入サポートいたします！



当社にご相談ください！

