S&J

インシデント0に、本気。

EDRを導入していても防げないリスクとは

ランサムウェア対策の空白領域を埋める「暗号化対策」という新しい視点

EDR を導入していても
被害は発生している

ランサムウェア対策として、EDRやSOC、バックアップの導入を進める企業は年々増加しています。
しかし、実際にはこうした対策を実施している企業であっても、事業停止や長期の復旧対応を伴う被害が継続的に発生しています。

なぜ、対策済み企業でも被害が発生するのでしょうか。

その理由は、攻撃を「検知すること」と、事業停止の原因となる「暗号化を防ぐこと」が同じではないからです。

多くの企業が侵入防止や検知には投資しています。
しかし、攻撃者が最終的に狙う「暗号化」そのものへの対策については十分に検討されていないケースが少なくありません。

＜掲載内容について＞
本資料は2026年7月時点の自社調査情報に基づいて作成しています。
記載内容は予告なく変更される場合があります。

目次

ランサムウェア被害は今も高水準で続いている

「対策している企業」も例外ではない

ランサムウェアは依然として企業経営に大きな影響を与えるサイバーリスクの一つです。

近年は、大企業だけでなく中堅・中小企業も積極的に標的とされています。攻撃者は、企業規模ではなく「身代金を支払う可能性」「サプライチェーンへ与える影響」を重視して、攻撃対象を選定しています。

また、**被害企業の多くは全く対策をしていなかったわけではありません。ファイアウォール、EDR、バックアップなど、一定の対策を講じていた企業でも被害が発生しています。**

つまり、現在問われているのは、対策の有無ではなく「実際に被害を防げるかどうか」です。

2025年国内ランサムウェア被害報告件数

226件

高水準が継続

被害組織は中小企業が中心

約6割

規模を問わず

- 被害件数は減っておらず、**対策不足の企業が狙われやすい**
- サプライチェーン攻撃対象のため**中堅・中小企業も標的**になる
- 「起こさない」対策だけではなく**「起きた瞬間に止める」対策**も必要

国内被害報告件数の推移（半期別）

出典：警察庁令和７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
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R7/R07_cyber_jousei.pdf

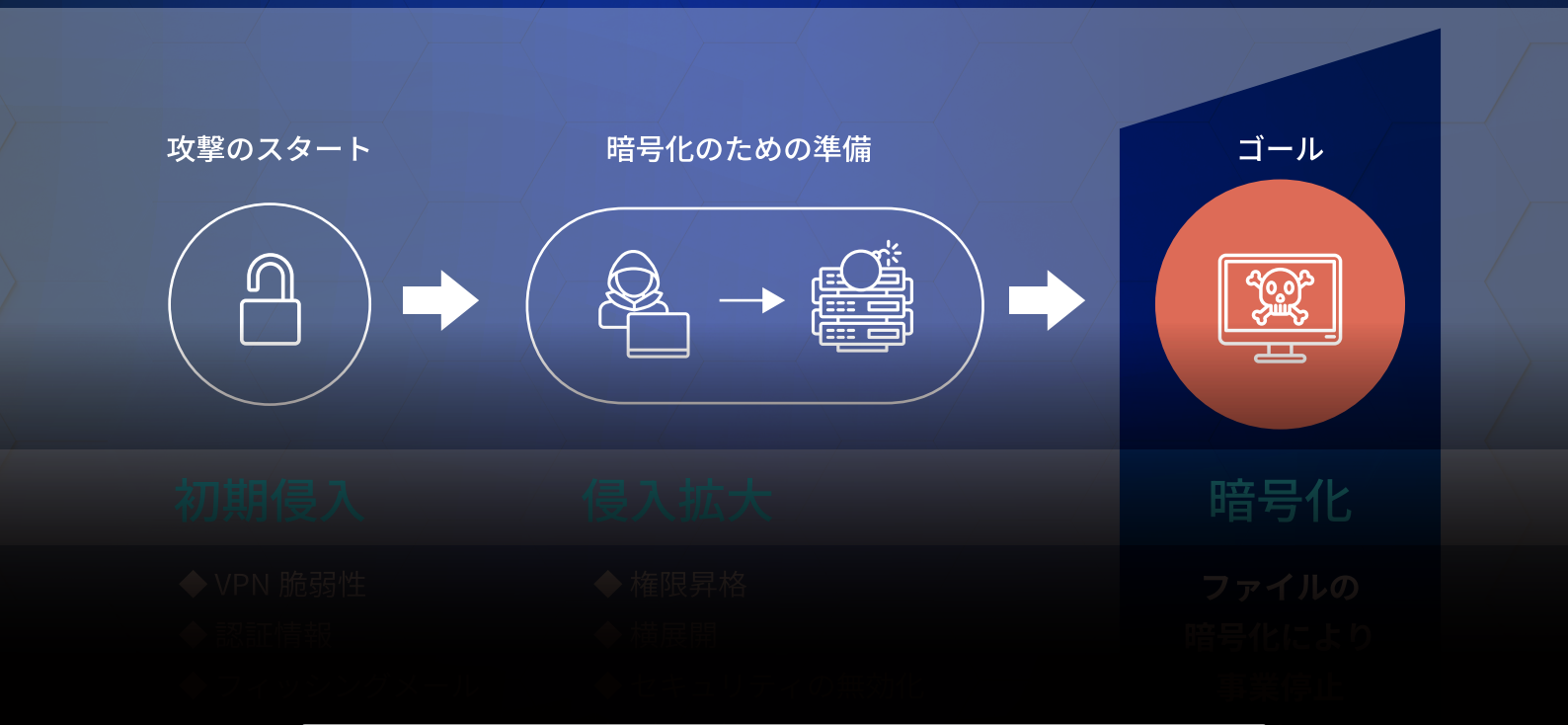
攻撃者はどのように暗号化へ到達するのか

暗号化は攻撃のスタートではなくゴール

ランサムウェア攻撃は、侵入した瞬間に始まるわけではありません。攻撃者はまず認証情報やVPN、フィッシングメールなどを悪用して侵入します。

その後、権限昇格や横展開を行い、重要サーバーへアクセスできる状態を構築します。さらに復旧手段を無効化するための活動やバックアップ環境への攻撃を行い、被害を最大化できる状態を構築します。そして、最後に実行されるのが暗号化です。

攻撃者にとって最も重要なのは侵入ではなく、暗号化を成功させることなのです。



本編は以下のお役立ち資料ページから
ダウンロードいただけます。

https://www.sandj.co.jp/download/