

ランサムウェア*の情勢

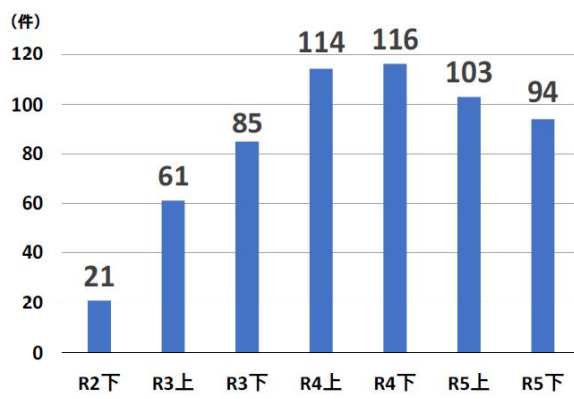
ランサムウェア感染被害の拡大やサイバー攻撃など、サイバー空間をめぐる脅威は、依然として深刻な情勢が続いています。

本号では、近年のランサムウェアの情勢などについてご紹介しますので、参考としてください。

※ 感染すると端末等に保存されているデータを暗号化して使用できない状態にした上で、そのデータを復号する対価（金銭又は暗号資産）を要求する不正プログラム。

■ 被害の情勢等

【企業・団体等におけるランサムウェア被害件数の推移】

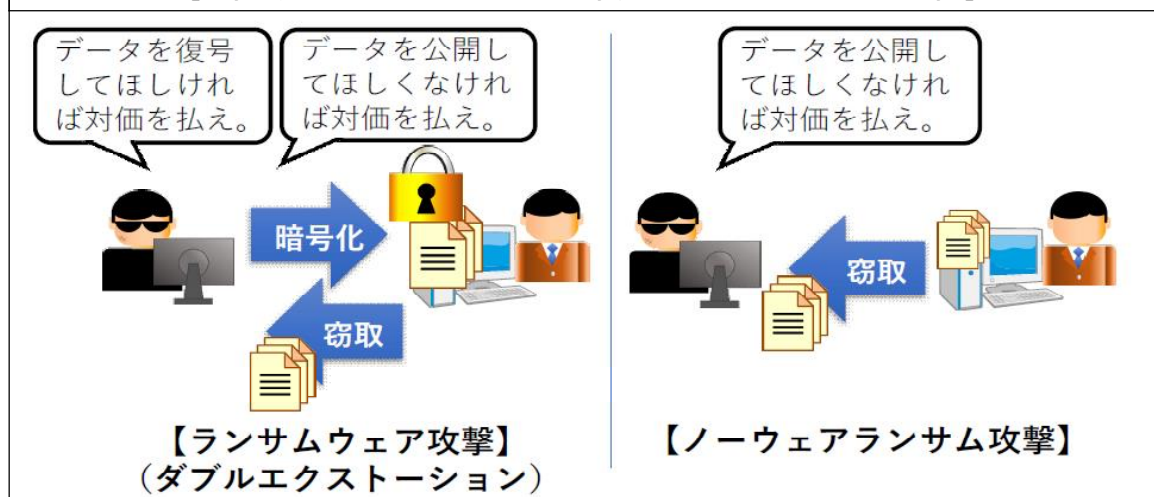


- 企業・団体における令和5年中の被害件数は197件で、令和4年上半期以降、高水準で推移している。
- 手口としては、データの暗号化のみならずデータを窃取の上「対価を支払わなければデータを公開する」などと要求する二重恐喝（ダブルエクストーション）が多くを占める。
- 令和5年中は、左グラフのほか、暗号化することなくデータを窃取し対価を要求する手口（ノーウェアランサム）による被害が30件確認されている。

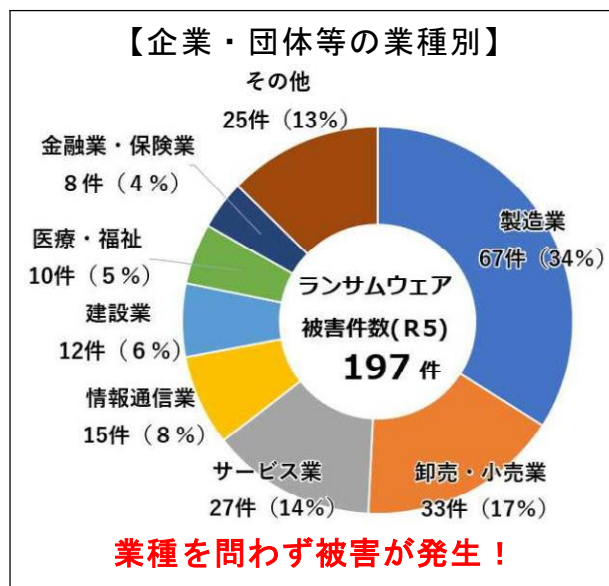
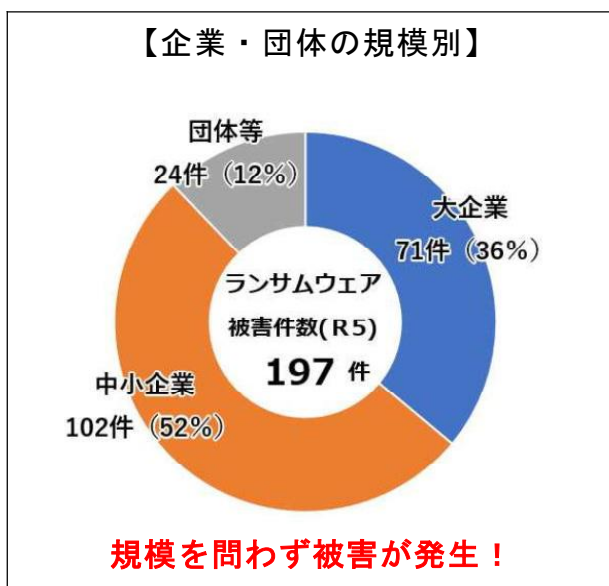
＜特徴（令和5年中）＞

- 二重恐喝による被害が多くを占める
手口を確認できた175件のうち、二重恐喝の手口は130件で74%を占めた。
- 暗号資産による対価要求が多くを占める
直接的な対価の要求を確認できた31件のうち、暗号資産による支払の要求があったものは27件で87%を占めた。

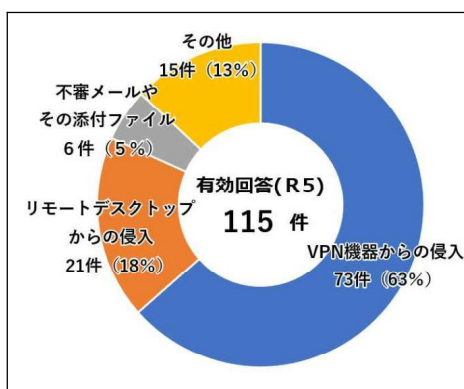
【攻撃の流れ（左：ランサムウェア攻撃、右：ノーウェアランサム攻撃）】



■ 被害企業・団体等の規模・業種別被害件数



■ 感染経路



ランサムウェアによる被害（197件）のあった企業・団体等に対するアンケート調査結果（有効回答115件）を分析したところ、

- ・VPN機器からの侵入 ～73件（63%）
- ・リモートデスクトップからの侵入～21件（18%）

で、テレワーク等に利用される機器等のぜい弱性や、強度の弱い認証情報等を利用して侵入したと考えられるものが約82%と大半を占めた。

■ 復旧等に要した期間・費用

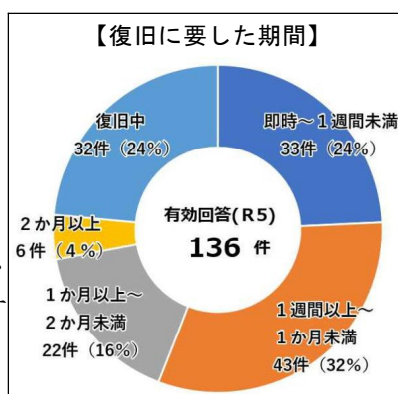
◎復旧に要した期間

⇒ 1か月以上が28件

◎調査・復旧費用の総額

⇒ 1,000万円以上が44件

など、被害に遭ってしまうと、復旧までに多大な労力を要することが見てとれます。



サイバー攻撃への備えとしては、「3つの基本的対策」（①リスク低減のための措置、②インシデントの早期検知、③インシデント発生時の適切な対処・回復）などがあります。

詳しくは、過去の本通信や、警察庁・福島県警のホームページをご参照いただき、被害の防止に努めましょう。



技術流出の防止に向けて

本年第1号で、情報漏えいを防ぐための「5つの漏えい対策」をご紹介しましたが、本号からは、その5つの対策を個別に詳しくみていきます。

はじめは、「**秘密情報に『近寄りにくくする』ための対策（接近の制御）**」についてご紹介します。



秘密情報への接近の制御について

秘密情報を閲覧・利用できる者（アクセス権者）の範囲を適切に設定した上で、施錠管理や入退室制限といった区域制限等により、アクセス権限を有しない者を近づけないようにすることを目的としています。

ポイントは、「**アクセス権者が、本当にその情報を知るべき者か**」という観点から、適切に限定されることです。その前提として、まずは、社内の規程（就業規則や情報管理規程など）等でアクセス権設定に関するルールを策定することが必要となります。



社内規程の策定

規程の策定は、秘密情報の取扱い等に関するルールを周知する効果的な手段です。従業員等が、秘密情報の取扱いや秘密保持義務が課されていることを理解できるよう、次のような内容を盛り込んでおくとい良いでしょう。

- ①**適用範囲**：本規程を守らなければならない者を明確にする
- ②**秘密情報の定義**：規程の対象となる情報の定義を明確化する
- ③**秘密情報の分類**
 - ：分類の名称（「役員外秘」「部外秘」「社外秘」など）と、各分類の対象となる秘密情報について説明する。
- ④**分類ごとに講ずる対策**
 - ：「秘密情報が記録された媒体に、分類ごとの表示をする」
 - 「アクセス権者の範囲の設定」
 - 「秘密情報が記録された書類の保管庫を施錠管理して、持出を禁止する」
 - 「私物のUSBメモリの持込みを制限し、複製を禁止する」 など
- ⑤**管理責任者**
 - ：秘密情報の管理を統括する者（担当役員など）を規定する
- ⑥**秘密情報及びアクセス権の指定に関する責任者**
 - ：分類ごとの秘密情報の指定やアクセス権付与を実施する責任者を規定する
- ⑦**秘密保持義務**
 - ：秘密情報をアクセス権者以外に開示してはならない旨を規定する

ふくしま技術情報不正流出防止ネットワーク

Fukushima Prevention Network for Illegal Leakage of Technological Information

技術流出の防止に向けて

本年第5号では、情報漏えいを防ぐための「5つの漏えい対策」のうち「秘密情報に『近寄りにくくする』ための対策」についてご紹介しましたが、今回は、

「秘密情報の『持出しを困難にする』ための対策」（持出し困難化）
についてご紹介します。

自社の事情に照らして対策を検討するなど、参考にしてください。



目的

持出し困難化は、秘密情報を無断で複製したり持ち出したりすることを、物理的、技術的に阻止することを目的としています。

対策の具体例

○ 持出しを困難にするための対策としては、

- ・ 秘密情報が記載された会議資料の回収
- ・ テレワーク・オンライン会議でのアクセス（投影）制限
- ・ 保有するノートパソコンの固定や持出の制限
- ・ 記録媒体への複製制限
- ・ 組織が許可した以外のオンラインストレージの利用制限
- ・ 従業員の私物USBメモリ等の持込み・利用の制限

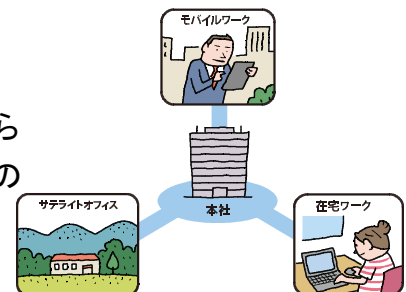


などがあげられます。

○ 特に、テレワークの実施との関係では、

- ・ 重要情報のレベルに応じたアクセス制限
- ・ パソコン等への格納制限
- ・ 実施を認める場所の吟味（自宅等の周囲の目から遮断が可能・容易な環境なのか、カフェ等の周囲の目がある環境なのか）
- ・ 画面の覗き込み防止フィルムの活用
- ・ オンライン会議等の際は大声での会話を避ける
- ・ 組織ネットワークに接続する際にはVPN等を用いて暗号化する

などの対策を講じることが重要です。



（詳細は、経済産業省「秘密情報の保護ハンドブック」をご参照ください）