4. 国内におけるランサムウェアを巡る情勢と政策動向

要約

- 国内におけるランサムウェアの被害件数は高止まりの状況であり、攻撃の手口も進化している。
- 重要インフラ事業者がランサムウェアの被害に遭うことで、国民生活や社会経済活動に多大な影響が及ぶ事案も発生しているため、政府も重要インフラ事業者に対するサイバーセキュリティ対策の強化に取り組んでいる。

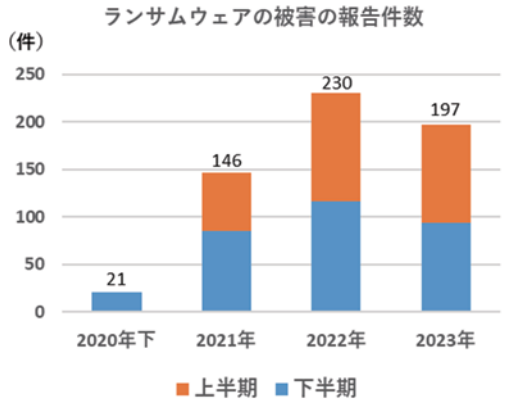
はじめに

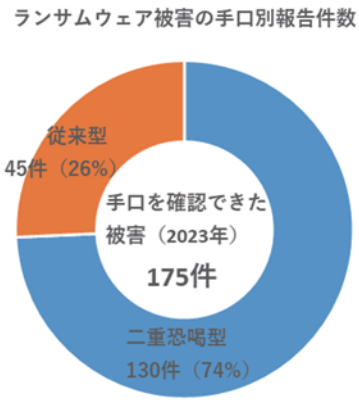
ランサムウェアは長年にわたりセキュリティ上の深刻な脅威として認識されており、情報処理推進機構（IPA）の「情報セキュリティ 10 大脅威」でも、組織向けの脅威において 4 年連続で 1 位にランクインしています。第 2 部のインシデント事例でも取り上げたように、今年に入ってからも国内で多数の組織が被害に遭っていることが確認されており、その脅威は収まる気配がみられません。近年、特に重要インフラ事業者などの社会インフラを支える組織がランサムウェアの被害に遭うことでシステムが機能不全に陥り、国民生活に多大な影響を及ぼす事例が相次いでいることから、各組織が自主的な対策を行うだけでなく、政府も国内におけるサイバーセキュリティの対策強化を図るべく、様々な取り組みを行っています。

そこで本記事では、国内で発生したランサムウェアによる被害の現状や過去の重大な被害事例について取り上げるとともに、政府のランサムウェアに関連する施策を紹介します。

ランサムウェア被害の現状

警察庁が公表した『令和5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』(*1)によると、2023 年における国内のランサムウェア被害の報告件数は 197 件となっており、過去最高を記録した 2022 年の 230 件からはやや減少したものの、依然として高止まりの状況が続いています。また、攻撃の手口として、従来は暗号化したデータを復号する代わりに身代金を要求していたところ、現在はデータを窃取した上で被害組織に対して「身代金を支払わなければ、データを公開する」と脅迫する二重恐喝（ダブルエクストーション）が主流となっています。ランサムウェアの被害が後を絶たない原因として、このような攻撃の手口の進化によって、被害組織は身代金の支払いを拒否することがますます困難になり、攻撃者にとって都合の良いビジネスとして成り立っていることがあげられます。





出典：『令和5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』(*1)を基に大和総研作成

(*1) 警察庁『令和5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』

このようにランサムウェアによるサイバー攻撃が猛威を振るう中、過去には下表のような重要インフラ事業者などの社会インフラを支える組織が標的となり、システムが停止する事案も発生しています。これらの事案では国民生活や社会経済活動に多大な影響が及んだことから、当時は報道機関でも頻繁に取り上げられ、広く世間の注目を集めました。

発生年月	対象	事案概要
2021 年 10 月	徳島県つるぎ町立半田病院	院内のシステムがランサムウェアに感染したことで、電子カルテが暗号化され閲覧不可になったほか、電子カルテのデータを参照する会計システムなども連鎖的に使用不能になり、新規患者の受け入れを停止するなど、業務が大幅に制限された。 復旧には約 2 か月を要した。
2022 年 10 月	大阪急性期・総合医療センター	調理を委託していた給食事業者のシステムを経由して、医療センターのシステムがランサムウェアに感染し、電子カルテなどが暗号化された。これにより、同センターでは新規患者の受け入れの停止や、緊急性が低い入院患者の自宅退院、周辺病院への転院を進めるなどの対応が必要となった。 復旧には約 2 か月を要した。
2023 年 7 月	名古屋港	総取り扱い貨物量日本一である名古屋港のコンテナターミナルを管理する中央システム「名古屋港統一ターミナルシステム（NUTS：Nagoya United Terminal System）」がランサムウェア感染により停止し、トレーラーを使用するターミナルでのコンテナの搬出入作業が全て中止された。 復旧には約 2 日半を要した。

出典：大和総研作成

ランサムウェアに関連する国内の政策

上記の事案のように重要インフラ事業者などの社会インフラを支える組織が被るランサムウェアの被害は、その影響の大きさから、同様の被害を防止するため、政府のサイバーセキュリティに対する施策にも大いに反映されています。以下では、前述の事案を受けて政府がどのような施策を行っているかを紹介します。

医療機関に対する施策

政府は 2024 年 7 月 10 日、『サイバーセキュリティ 2024（2023 年度年次報告・2024 年度年次計画）』（以降、「サイバーセキュリティ 2024」）を決定し、公表しました(*1)。「サイバーセキュリティ 2024」では、政府がサイバーセキュリティに関して特に強力に取り組む施策がまとめられており、現在における課題やそれらを解決するための取り組みについて概要が示されています。その中でも近年、医療機関においてランサムウェアの感染などによるシステムの機能停止や長期にわたる診療停止の事例が相次いでいることから、政府は特に医療機関を中心とした、以下の施策を進めています。

背景及び課題	取り組みの概要
医療機関のセキュリティ対策は、これまで各医療機関が自主的に取組を進めていたが、サイバー攻撃により長期に診療が停止する事案が発生したことから自主的な取組だけでは不十分と考えられる。医療機関におけるサイバーセキュリティ対策を強力に推進することが必要である。	・サイバーセキュリティインシデントが発生した医療機関に対する初動対応支援や、医療機関がサイバーセキュリティ対策を講じるに当たっての相談・助言、医療機関に特化したサイバーセキュリティ演習プログラム作成・実施を行う。また、「医療機関向けセキュリティ教育支援ポータルサイト」において、職員を対象とした研修にも活用できるコンテンツ等の作成・掲載を行う。 ・「医療情報システムの安全管理に関するガイドライン」第 6.0 版について、医療機関における研修の実施や普及啓発に取り組む。また、「医療機関におけるサイバーセキュリティ対策チェックリスト」において、医療機関における日々のセキュリティ対策を推進するとともに、チェックリストを用いた立入検査を行う。 ・厚生労働省委託事業において、病院の外部ネットワークとの接続の安全性の検証・検査や、オフライン・バックアップ体制の整備の支援を実施する。
医療機関等の重要インフラ事業者がサイバー攻撃により機能停止する事態が相次ぎ、当該分野のセキュリティ人材不足も原因の一つとなっている。行政が支援し、当該分野の実態を踏まえた早急な人材育成が必要である。	・NICT が保有する人材育成やサイバーセキュリティ研究の実績・知見を活用し、厚生労働省等と連携して、各分野に特化したものを含む新たな演習プログラムを開発し、民間企業・団体等に提供できる体制を構築・強化する。講師人材の育成も併せて行う。

出典：「サイバーセキュリティ 2024」(*1)を基に大和総研作成

(*1) NISC『サイバーセキュリティ 2024（2023 年度年次報告・2024 年度年次計画）』

これらの施策が示すとおり、政府による取り組みはインシデント発生時の初動対応支援やセキュリティ対策の相談・助言、人材育成など多岐にわたっています。特に昨年は医療法施行規則の改正により、医療機関の管理者はサイバーセキュリティ対策において必要な措置を講じることが義務化されたことに加え、その対策状況について行政による医療機関への立入検査が行われるようになったことで、より一層、政府によるセキュリティ対策への関与が高まっています。

港湾に対する施策

2023 年 7 月に発生した名古屋港コンテナターミナルへのランサムウェアによるサイバー攻撃は、2 日以上にわたり物流に大きな影響を与えましたが、この攻撃が発生した時点では「港湾」はサイバーセキュリティ基本法の「重要インフラ事業者」と経済安全保障推進法の「基幹インフラ事業者」の、いずれにも含まれていませんでした。

しかし、この事案によって港湾が果たす役割の重要性が再認識され、政府は有識者によるセキュリティ対策の検討委員会を設置し、港湾の位置付けを見直すこととなりました。その結果、2024 年 3 月 8 日にサイバーセキュリティ基本法において「港湾」が「重要インフラ事業者」の対象に追加され、官民一体となった迅速な情報共有体制の整備など、政府との連携が強化されました。

また、2024 年 5 月 10 日には経済安全保障推進法の改正案が参議院本会議で可決・成立し、「基幹インフラ事業者」の対象にコンテナターミナルで貨物の受け渡しを行う「港湾運送」が新たに追加されました。この改正により、今後、重要な設備を導入する際には、サイバー攻撃を防止するための適切な措置が講じられているかなどについて、政府による事前審査が必要となり、審査の結果、不備があると判断された場合は、設備の変更などを求める勧告や命令が出されることとなりました。

	サイバーセキュリティ基本法	経済安全保障推進法
法律の概要	国民生活や社会経済活動の基盤となるインフラのうち、機能が停止・低下すれば多大な影響を及ぼす恐れがある事業者を「重要インフラ事業者」として指定し、事業者が適切なサイバーセキュリティの確保に努めるように対策を講じている。	インフラサービスの安定的な提供を確保するため、基幹インフラを担う事業者のうち、一定の基準を満たす事業者を「特定社会基盤事業者（通称：基幹インフラ事業者）」として指定し、重要な設備の導入などを行う際に政府の審査を必要とするよう定めている。
対象の業種	情報通信、金融、航空、空港、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流、化学、クレジット、石油、**港湾**	電気、ガス、石油、水道、鉄道、貨物自動車運送、外航貨物、**港湾運送**、航空、空港、電気通信、放送、郵便、金融、クレジットカード

※赤字が事案発生後、新たに追加された業種

出典：大和総研作成

最後に

本記事で紹介した政府の施策は数ある中のごく一部であり、他にも、ランサムウェアをはじめとしたサイバー攻撃への対策を強化するため、重要インフラ事業者における被害発生を想定した演習や海外機関との連携などを通じて、国内全体のサイバーセキュリティの底上げを図っています。

前述した「サイバーセキュリティ 2024」には、サイバー空間の現下の情勢や、政府が昨年度取り組んできた施策、今年度特に力を入れて取り組む施策が網羅的にまとめられており、国内におけるサイバーセキュリティの動向を把握する上で大変参考になります。一度ご確認いただくことをお勧めします。

（横平　健）