2024.2.1

サイバーセキュリティニュース ＜2023 No.002＞

さらに活発化するランサムウェア攻撃
2023 年の動向を振り返る

【要旨】
■ ランサムウェア攻撃被害は業種・事業規模問わず発生している。IT システムの停止に伴い発生する被害は甚大であり、経営課題の一つとなっている。
■ ランサムウェア攻撃の侵入経路はパターン化している。セキュリティ対策が進んでいない企業や組織が標的となっており、基本的なサイバーセキュリティ対策の実施が急務である。
■ 「身代金の支払いは避けるべき」と 50 か国・機関の共同声明が発表された。ランサムウェアをはじめとしたサイバー攻撃に対しては、業界・社会全体で対応することが求められる。

1．ランサムウェア攻撃とは

医療機関やインフラ事業者をはじめとした企業・組織に対するサイバー攻撃被害がマスメディアで度々報道されている。不正アクセスによる情報漏えいや不審メール開封によるマルウェア感染、偽サポート画面を通じた金銭盗取などの被害は日々発生しており、サイバー攻撃は日常の一部となっている。

独立行政法人情報処理推進機構（IPA）は、前年に発生した情報セキュリティ事故や攻撃の状況等から注意すべき脅威を選出した「情報セキュリティ 10 大脅威」を公開している。その中で、「ランサムウェアによる被害」は 2021 年から 3 年連続で 1 位にランクされている。

ランサムウェアとは、身代金を意味する「Ransom」と「Software（あるいは Malware）」を組み合わせた造語であり、攻撃先の PC やサーバ内にあるデータを暗号化し、データの復号（回復）と引き換えに身代金を要求するマルウェアとして、ここ数年の間で大きな脅威となっている。

	2019	2020	2021	2022	2023
1位	標的型攻撃による被害	標的型攻撃による機密情報の窃取	ランサムウェアによる被害	ランサムウェアによる被害	ランサムウェアによる被害
2位	ビジネスメール詐欺による被害	内部不正による情報漏えい	標的型攻撃による機密情報の窃取	標的型攻撃による機密情報の窃取	サプライチェーンの弱点を悪用した攻撃
3位	ランサムウェアによる被害	ビジネスメール詐欺による金銭被害	テレワーク等ニューノーマルな働き方を狙った攻撃	サプライチェーンの弱点を悪用した攻撃	標的型攻撃による機密情報の窃取
4位	サプライチェーンの弱点を悪用した攻撃の高まり	サプライチェーンの弱点を悪用した攻撃	サプライチェーンの弱点を悪用した攻撃	テレワーク等ニューノーマルな働き方を狙った攻撃	内部不正による情報漏えい
5位	内部不正による情報漏えい	ランサムウェアによる被害	ビジネスメール詐欺による金銭被害	内部不正による情報漏えい	テレワーク等のニューノーマルな働き方を狙った攻撃
6位	サービス妨害攻撃によるサービスの停止	予期せぬIT基盤の障害に伴う業務停止	内部不正による情報漏えい	脆弱性対策情報の公開に伴う悪用増加	修正プログラムの公開前を狙う攻撃(ゼロデイ攻撃)
7位	インターネットサービスからの個人情報の窃取	不注意による情報漏えい（規則は遵守）	予期せぬIT基盤の障害に伴う業務停止	修正プログラムの公開前を狙う攻撃(ゼロデイ攻撃)	ビジネスメール詐欺による金銭被害
8位	IoT機器の脆弱性の顕在化	インターネット上のサービスからの個人情報の窃取	インターネット上のサービスへの不正ログイン	ビジネスメール詐欺による金銭被害	脆弱性対策情報の公開に伴う悪用増加
9位	脆弱性対策情報の公開に伴う悪用増加	IoT機器の不正利用	不注意による情報漏えい等の被害	予期せぬIT基盤の障害に伴う業務停止	不注意による情報漏えい等の被害
10位	不注意による情報漏えい	サービス妨害攻撃によるサービスの停止	脆弱性対策情報の公開に伴う悪用増加	不注意による情報漏えい等の被害	犯罪のビジネス化（アンダーグラウンドサービス）

【図 1】情報セキュリティ 10 大脅威の過去 5 年間のまとめ
（出典：IPA「情報セキュリティ 10 大脅威」をもとに弊社が作成）

ランサムウェア攻撃は、ランサムウェアのプログラムを開発する者、企業の脆弱性を探索する者、実際に攻撃を実施する者など、攻撃者がそれぞれの役割を分業化し、セキュリティ対策が不十分な企業・組織に対して組織的に行われている。

ランサムウェアに感染すると、システムの復旧対応や取引先・関係者に対する適切な情報開示・対話が求められる。また、身代金の支払いは攻撃者に資金を提供することとなり、更なる犯罪行為を助長する可能性があるため、慎重な判断が求められる。このように、ランサムウェアに感染すると様々な意思決定が求められることからランサムウェア攻撃は単なる情報セキュリティ上の課題だけではなく、経営課題の一つと認識した上で対策を検討する必要がある。

２．ランサムウェア攻撃が企業や組織に与える影響

現代社会はITシステムに強く依存しており、ITシステムの可用性と引き換えに身代金を要求するランサムウェア攻撃は企業の事業継続および我々の社会生活に対して大きな影響を与えている。ITシステムへの依存は医療機関も例外ではなく、電子カルテシステムをはじめとする医療システムが機能不全に陥ると、日常の診療すらままならない状態となってしまう。国内において、ランサムウェア感染した医療機関では、ほとんどの診療業務が機能不全となり、感染の原因調査や復旧に数億円の費用が発生したことに加えて、数か月に及ぶ新規患者の受け入れ制限や手術の延期等により数億円以上の機会損失が発生した。

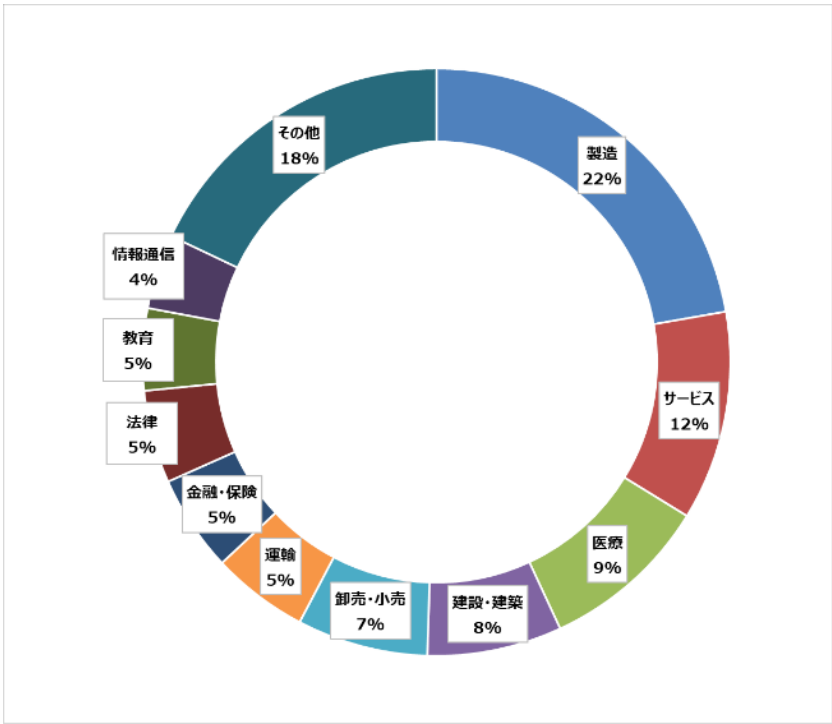
海外では、医療機関のランサムウェア感染により地域社会に発生する影響について研究[1]が行われている。研究では、救急診療を行っている病院でランサムウェア感染が発生した場合、正常に機能している近隣の病院への救急車到着数、待合室における待ち時間や平均入院期間の増加が確認されており、ランサムウェア感染が地域全体の医療の障害となってしまうことが分かっている。

医療機関だけではなく、国内の港湾ターミナルで利用しているシステムがランサムウェアに感染したことにより、数日間に渡り港湾の機能が停止し、物流に大きな混乱が生じた事案も記憶に新しい。海外では石油パイプライン会社や公共交通機関を対象とした攻撃が発生しており、「社会インフラの稼働が停止すると、多くの市民が困る＝身代金を支払わざるを得ない」といった攻撃者の仮説のもと、我々の社会基盤が攻撃の標的となっている。三井物産セキュアディレクション社の調査[2]によると、ランサムウェア攻撃は製造業、サービス業や情報通信業など、業種を問わずターゲットになっていることが分かる。また、日本国内におけるランサムウェア攻撃の被害組織の資本金を確認すると、大企業から中小企業まで、事業規模問わずその被害に遭っていることが分かる。

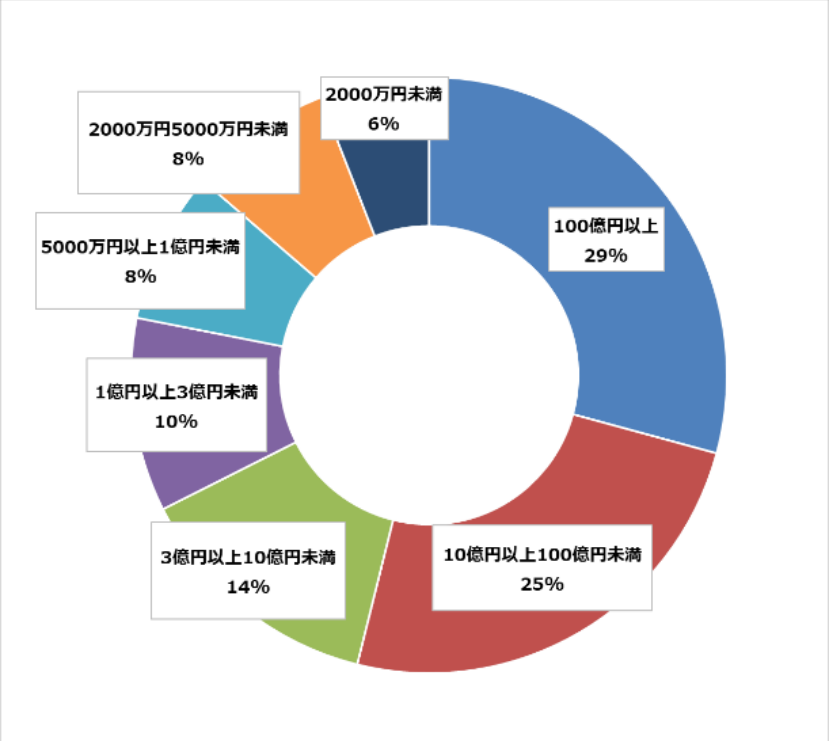
---

1 「Ransomware Attack Associated With Disruptions at Adjacent Emergency Departments in the US」,Christian Dameff, Jeffrey Tully （2023年5月8日）

2 「【2023年11月号】暴露型ランサムウェア攻撃統計CIGマンスリーレポート」 https://www.mbsd.jp/research/20231208/cig-monthly/（2023年12月8日公開）



【図２】全世界ランサムウェア被害組織の業種内訳（11 月）



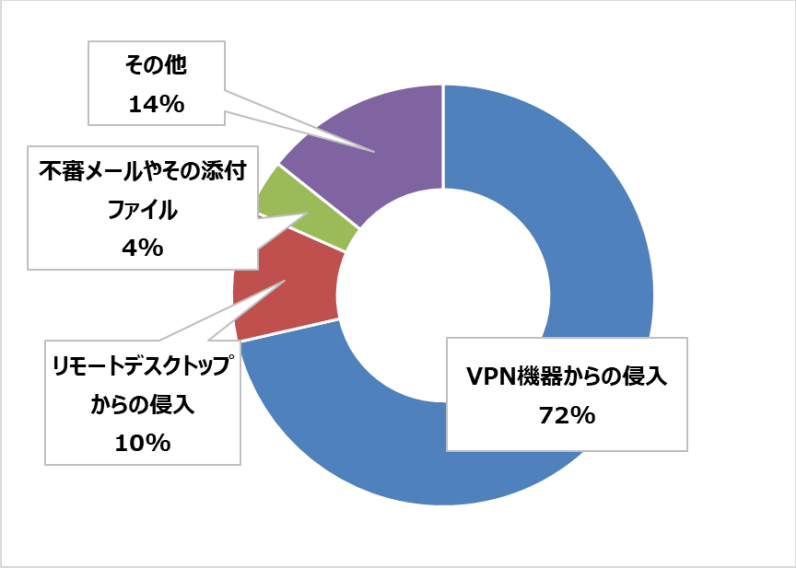
【図３】資本金別（国内）ランサムウェア被害統計(11 月)
（出典：三井物産セキュアディレクション株式会社
「暴露型ランサムウェア攻撃統計 CIG マンスリーレポート（12 月版)」をもとに弊社が作成）

３．ランサムウェア攻撃に関する最新情報

攻撃者は、日々新たな攻撃手法や金銭要求の方法を生み出しており、攻撃と防御の「イタチごっこ」が続いている。ランサムウェア攻撃は他所事ではなく、攻撃に関する最新動向を確認した上で、感染しないための対策、万が一感染してしまった際の対応方針等を予め検討しておくことが求められる。

（１）パターン化する侵入方法

警察庁が公開したランサムウェア攻撃の感染経路に関する調査結果[3]によると、VPN 機器からの侵入が全体の 72%、リモートデスクトップからの侵入が 10%とリモート接続機器からの感染が全体の 82%を占めている。VPN 機器等のリモート接続機器においてセキュリティ上の脆弱性が発見された場合、提供ベンダーより脆弱性の修正パッチが公開されるが、リモート接続機器が適切なタイミングでアップデートされず、修正パッチが適用されないままの場合、攻撃者よりセキュリティ上の脆弱性を悪用されて攻撃が成功する可能性が高まる。そのため、リモート接続機器のバージョンや修正パッチ適用の有無を確認の上、常に最新のバージョンを利用することがランサムウェア感染への対策およびサイバーセキュリティ対策として極めて重要となる。



【図４】ランサムウェア攻撃の侵入経路
（出典：警察庁「令和５年上半期におけるサイバー空間をめぐる脅威の情勢等について」をもとに弊社が作成）

また、企業が利用しているリモート接続機器の製品やバージョンは、インターネット上の公開情報により分析が可能となっている。これは、攻撃者も同様の分析が可能であることを意味し、企業が利用している古いバージョンのリモート接続機器等の脆弱性を分析しているとされる。特に、組織的な攻撃が行われているランサムウェア攻撃は、企業が持つ脆弱性の分析を主として行う者が存在し、脆弱性を抱えた環境は絶好の標的となる。かかる背景を踏まえた対策として、ASM（Attack Surface Management。公開情報から自社の資産に対してセキュリティ評価を行うことができる）ツールの活用など、自社のリスク評価とリスクの低減に向けた取り組みが有効である。

[3] 警察庁「令和５年上半期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/index.html（2023 年 9 月 21 日公開）

（２）身代金支払いの是非について

ランサムウェア感染時の復旧を支援する米国 COVEWARE 社の調査[4]によると、2023 年第 3 四半期において、ランサムウェア感染時に身代金の支払いを選択した企業は 41%、平均身代金支払い額は 850,700 ドル、身代金支払い額の中央値が 200,000 ドルとなっている。平均額と中央値に乖離が存在する理由として、攻撃者が攻撃の対象やその範囲に応じて金銭を獲得できる可能性を最大化するための戦略を持つ故だと考えられる。例えば、攻撃者はランサムウェア攻撃に成功した際、当該企業の財務情報を分析の上、現実的に支払い可能な身代金を要求しているとされる。また、攻撃者が広範囲なランサムウェア攻撃を実行し成功した場合は、被害企業が受ける影響が大きくなるため、高額な身代金を要求し、一方で、局所的な範囲でランサムウェア攻撃を実行した場合は比較的少額の身代金を要求している。

身代金支払いの是非については、2023 年 11 月に米国、英国や日本等合計 50 か国・機関が参画したカウンターランサムウェア・イニシアティブ会合において、「ランサムウェアへの身代金支払いは発生した事案の収束を保証するものではなく、攻撃者が次の攻撃を実行するインセンティブとなってしまうことから、ランサムウェアの要求に対し金銭支払を避けることを強く推奨する」という声明[5]を発表した。ランサムウェア攻撃の脅威に対して国家間のパートナシップを構築の上、毅然とした態度で攻撃者と向き合っていくことも宣言されており、本声明の趣旨を理解した上で、ランサムウェア攻撃への対応が求められることになる。

（３）#StopRansomware ガイド

ランサムウェア攻撃の対策に向け、米国サイバーセキュリティ・インフラストラクチャセキュリティ庁(CISA)は、米国政府としてランサムウェア攻撃対策をより効率的に実施するための情報を集約した特設サイト[6]を公開している。サイト内では対策に活用可能な#StopRansomware ガイドが掲載されており、2023 年 10 月には国家安全保障局(NSA)、連邦捜査局(FBI)、および多国間情報共有分析センター(MS-ISAC)と共同で #StopRansomware ガイドの更新版がリリースされた。

更新された#StopRansomware ガイドは、ランサムウェア対策のベストプラクティスとランサムウェアに感染した際の対応チェックリストで構成されている。

ランサムウェア対策のベストプラクティスとしては、「重要データのオフライン環境へのバックアップを維持する」「サイバー攻撃が発生した際の対応計画を作成し、定期的な訓練を実施する」「ゼロトラスト環境の構築」などが挙げられている。その他、社外に公開されている脆弱性の悪用やクレデンシャル情報（ID やパスワードをはじめとする、ユーザ等の認証に用いられる情報）の不正利用、フィッシング等、それぞれの侵入方法ごとに求められるベストプラクティスを公開している。

ランサムウェア攻撃に限らず、サイバー攻撃は基本的な対策を積み重ねることで、攻撃被害から自社を守ることができる。本ガイドを参考に、セキュリティ対策の抜け漏れがないか確認いただきたい。

ランサムウェアに感染した際の対応チェックリストは、全 21 個の項目で構成されており、「1.影響が起きたシステムを特定の上、即座にネットワークから分離する」「2.ランサムウェア感染の拡大を防

---

[4] Coveware「Scattered Ransomware Attribution Blurs Focus on IR Fundamentals」https://www.coveware.com/blog/2023/10/27/scattered-ransomware-attribution-blurs-focus-on-ir-fundamentals（2023 年 10 月 30 日公開）

[5] 総務省「『カウンターランサムウェア・イニシアティブ会合』への参加」https://www.mofa.go.jp/mofaj/press/release/press5_000145.html（2023 年 11 月 2 日公開）

[6] CISA「Stop Ransomware」https://www.cisa.gov/stopransomware（2023 年 12 月 13 日閲覧）

止するため、ネットワークからの分離ができない場合は端末の電源を切る」「3. システムの復旧ため、影響を受けたシステムのトリアージを行う」の 3 つの項目をはじめに確認した上で、残りの項目を確認することが推奨されている。本チェックリストは万が一ランサムウェアに感染してしまった際に参照できる実践的なチェックリストであり、予め本チェックリストからランサムウェア感染時の対応を学び、確認しておくことが有効である。

４．関係者とのコミュニケーションの重要性

猛威を振るうランサムウェアをはじめとしたサイバー攻撃に対しては、単一の企業・組織だけではなく業界・社会全体で対応することが求められる。例えば、CSIRT 間における情報共有や、日本シーサート協議会、業種内でのセキュリティ情報共有組織（ISAC）等のコミュニティ活動への参加による情報収集等が有効である。このようなコミュニケーションの仕組みがインシデント発生時に連絡体制として機能することで、迅速な報告や状況把握が可能となり、速やかな事態の収束が期待される。

ＭＳ＆ＡＤインターリスク総研株式会社
リスクマネジメント第三部 サイバーリスクグループ
コンサルタント　辻本　竜一