2. 中小企業のサイバー攻撃に対するセキュリティ対策
－最新の脅威動向と実効的な対策の提案－

研究委員レポート

紀陽情報システム株式会社 代表取締役副社長
〔(一財)和歌山社会経済研究所 研究委員〕 大西 徹

はじめに

近年のICT活用の加速は、企業の業務効率化や新たなビジネス機会の創出を可能にする一方で、サイバー空間に潜む脅威の多様化と複雑化をもたらしています。情報システムの高度化に伴い、攻撃者の手口も洗練され、従来の防御策では十分に対応できない場面が増えてきました。特に、社会経済活動の基盤となる中小企業にとっては、情報漏洩や業務の停止が生じるリスクが現実的な課題となっています。リスクマネジメントの観点からも、最新の脅威動向や効果的な対策の把握が不可欠です。

1．本レポートの目的

近年、デジタル化の進展とともにサイバー攻撃の脅威が増大し、規模を問わずあらゆる企業がその標的となっています。特に中小企業は、人的・技術的・財政的なリソースの制約から大企業に比べて脆弱性が高い傾向にあります。本レポートでは、中小企業が直面するサイバー攻撃の最新トレンドや主要な攻撃手口、現状把握のための方法を解説します。そして、最終的に、今後の展望と推奨事項を提示し、中小企業が自社の情報資産を守るための一助となることを目的とします。

2．サイバー攻撃の現状

（1）最新のサイバー攻撃のトレンド

サイバー攻撃は年々高度化・巧妙化しています。例えば、標的型攻撃やランサムウェアの拡散、クラウドサービスを狙った侵害など、従来の手法に加えて新たな攻撃が増加傾向にあります。独立行政法人情報処理推進機構の「情報セキュリティ 10大脅威（2025)」によると、特に「ランサムウェア攻撃による被害」や、「サプライチェーンや委託先を狙った攻撃」が急増しています。

順位	「組織」向け脅威	初選出年	10大脅威での取り扱い
1	ランサム攻撃による被害	2016年	10年連続10回目
2	サプライチェーンや委託先を狙った攻撃	2019年	7年連続7回目
3	システムの脆弱性を突いた攻撃	2016年	5年連続8回目
4	内部不正による情報漏えい等	2016年	10年連続10回目
5	機密情報等を狙った標的型攻撃	2016年	10年連続10回目
6	リモートワーク等の環境や仕組みを狙った攻撃	2021年	5年連続5回目
7	地政学的リスクに起因するサイバー攻撃	2025年	初選出
8	分散型サービス妨害攻撃（DDoS攻撃）	2016年	5年ぶり6回目
9	ビジネスメール詐欺	2018年	8年連続8回目
10	不注意による情報漏えい等	2016年	7年連続8回目

（独立行政法人情報処理推進機構「情報セキュリティ10大脅威2025」より）

（2）中小企業が直面する脅威

中小企業は「セキュリティ対策は自社には必要ない」といった誤った認識を持つことがありますが、実は攻撃者にとっては狙いやすいターゲットとなっています。理由として、脆弱なセキュリティ体制、古いシステムの使用、従業員の意識不足などが挙げられます。結果として、情報漏洩や業務停止といった深刻な被害に繋がるケースが増えています。

３．サイバー攻撃の種類と手口

（１）ランサムウェア

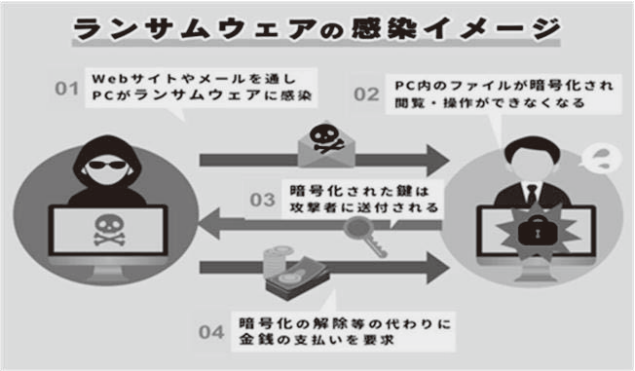
システムやファイルを暗号化し、復号のための身代金を要求する攻撃です。中小企業はバックアップ体制が不十分な場合が多く、復旧困難となる事例が目立ちます。

① 攻撃手口（ランサムウェアに感染させて金銭を要求）

・ソフトウェアの脆弱性を悪用し、ＰＣ やサーバーをランサムウェアに感染させる。
・意図せず公開されているポート(リモートデスクトップ等)を利用した不正アクセスからマルウェアに感染させる。
・ランサムウェアをダウンロードさせるようにＷｅｂサイトの脆弱性を悪用して改ざんし、閲覧した際に感染させる、またはメールで悪意のあるリンクを仕込んだり、不正な添付ファイルを開かせて感染させる。

② 最近の事例（ランサムウェア感染による被害と二次被害）

・2024年6月、KADOKAWAがランサムウェア攻撃を含む大規模なサイバー攻撃にあった。フィッシング攻撃等により従業員のアカウント情報が窃取され、社内ネットワークに侵入されたことが原因と推測。複数のサービスが停止したほか、約25万4,000人分の個人情報や企業情報の漏えいが判明した。また、攻撃組織が公開したとされる情報が、SNS 等を通じて拡散された。
・2025年9月、飲料メーカーであるアサヒグループホールディングスが大規模なサイバー攻撃を受け、国内の業務システムが停止。
・2025年10月、オフィス用品通販大手のアスクルが、ランサムウェア攻撃によって顧客などの情報が外部に流出したことを公表。



（２）サプライチェーンや委託先を狙った攻撃

調達から販売、業務委託等一連の商流において、セキュリティ対策が甘い組織が攻撃の足掛かりとして攻撃される事例が増えています。

① 攻撃手口

・セキュリティが脆弱な取引先や委託先、国内外の子会社等を攻撃し、標的組織の機密情報を狙う。
・ソフトウェアやサービスを改ざんしてマルウェアを仕込み、インストールやサービス利用の際に顧客にマルウェアを感染させる。

② 最近の事例（業務委託先業者からの顧客情報漏えい）

・2024年5月、イセトーは VPN 経由の不正アクセスを受け、端末やサーバー等がランサムウェア攻撃を受けたと公表した。2024年6月、攻撃者が窃取したとされる情報のダウンロード用 URL が攻撃者グループのリークサイトに掲載された。自治体だけでも約 50 万件以上の個人情報が漏えいした。また業務委託元より損害賠償請求の予定も報告された。

（3）内部不正による情報漏洩

従業員や関係者による情報漏洩や不正アクセスも重大な脅威です。退職者のアカウント管理や権限設定の不備がきっかけとなることがあります。

① 攻撃手口

・付与されたパスワードを悪用し、組織の重要情報を取得する。また、必要以上のアクセス権限を付与していると被害が大きくなる。
・在職中に使用していたアカウントを使って不正に情報を取得する。

② 最近の事例（顧客情報を転職先に持ち出し、営業活動に使用）

・2024年4月、プルデンシャル生命保険は元社員が退職時に顧客情報を不正に持ち出し、転職先で使用したと公表した（約970件）。
・2024年8月、東急リバブルも元社員が個人情報を不正に持ち出し、転職先でDM（ダイレクトメール）に利用したことを公表した（約2万5千件）。

4．現状把握の方法

セキュリティ対策を講じるためにも、現状の自社の状況を把握することが必要です。

（1）セキュリティ診断

外部専門機関による脆弱性診断やペネトレーションテストを受けることで、現状の問題点を明らかにします。無料診断を提供する自治体や団体も増えており、積極的に利用することが推奨されます。保険会社の無料診断サービスなどを利用することも有効です。

（2）リスクアセスメント

自社でシステム部門がある場合は、自社の情報資産と脅威、脆弱性の洗い出しを行うことが有効です。課題がある場合に、すべての対策を同時に実施することは難しいので、リスクの優先順位を決定する必要があります。

5．対策の具体例

サイバー攻撃の対策として、「人的・組織的対策」、「技術的対策」、「物理的対策」の実施が推奨される。一方で、サプライチェーン上のサイバーセキュリティリスクが増大していることも踏まえ、対策ガイドラインの整備が業界単位で進んできている。

（1）人的・組織的対策

セキュリティポリシーの策定や、情報資産管理台帳の作成、従業員向けの教育・訓練（フィッシング対策、パスワード管理等）など、社員に、なぜセキュリティが重要かということを認識してもらい、どこに重要な情報があるかを管理することが必要です。

（2）技術的対策

データの暗号化、アクセス権限の適切な管理や、ファイアウォールなどのネットワークの監視、アンチウイルスソフトの導入、データのバックアップなど、システム面でデータを守る対策が必要です。

（3）物理的対策

入退室管理システムの導入や重要機器の施錠と監視カメラの設置など、物理的に、不正にシステムにアクセスできないような対策を講じることが必要です。

6．まとめ

サイバー攻撃は今後も進化し続け、特に中小企業にとっては重大なリスクとなり得ます。攻撃手法は日々巧妙化し、標的型攻撃やランサムウェア、サプライチェーン攻撃など、組織の規模や業種を問わず被害が拡大しています。こうした状況の中で、組織的・技術的・物理的な対策を三位一体で講じることが、防御力向上の鍵となります。

さらに、公的機関が提供する最新情報や支援策を活用することは、組織の防御力強化に役立ちます。たとえば、IPA（情報処理推進機構）や警察庁が発信する脅威情報やガイドライン、サイバーセキュリティお助け隊などの支援サービスを積極的に利用することも有効です。リスクアセスメントや教育・訓練は一度で終わるものではなく、継続的かつ定期的な実施が重要です。

今後は「ゼロトラスト」や「クラウドセキュリティ」といった新しいセキュリティ概念への理解を深めるとともに、AIを活用した脅威検知や自動化された防御体制の構築も求められます。サプライチェーンの多様化に伴い、取引先や外部パートナーとのセキュリティ連携も不可欠です。将来的には、変化する脅威環境に柔軟かつ迅速に対応できる体制を整え、組織の安全と事業継続を守ることがより一層重要となります。

しかしながら、自社にセキュリティに詳しい人材がいない企業は少なくありません。地域のIT企業やコンサルなど、セキュリティの知見のある企業と連携しながら、自社のセキュリティレベルを上げていくことが必要です。

以上

CHECK

情報セキュリティ対策の第一歩は、現状を正しく把握することです。
まずは、次項に 03付録 として掲載している「５分でできる！情報セキュリティ自社診断」を活用し、自社の現状を簡単に確認してみて下さい。