特集／AIとサイバーセキュリティを巡る動向と対応

〈1〉サイバーセキュリティを巡る動向と経営層がリードすべきサイバーリスクへのマネジメント

東海大学　情報通信学部　教授
元内閣審議官・内閣サイバーセキュリティセンター副センター長
元経済産業省サイバーセキュリティ・情報化審議官
三角　育生

1　はじめに

近年、企業・組織のビジネス活動に対するサイバー脅威は一層深刻化している。ランサムウェアによる被害、分散型サービス妨害（DDoS）攻撃、さらには金融取引などを標的としたサイバー犯罪など、被害の形態も多様化している。デジタルトランスフォーメーション（DX）が進展するなか、企業・組織の活動がデジタル環境への依存を深めていることから、サイバー攻撃が発生した場合の影響は、事業継続、経営に対する信頼、さらには社会的な信用にまで及ぶ可能性がある。

しかしながら、こうしたリスクについて、実際に被害が発生するまで、企業・組織の経営層にその深刻さが十分に認識されず、対応がIT部門やセキュリティ専門部門に限定されてしまっている事例も散見される。その結果、企業・組織全体としてのセキュリティ対応が後追いとなり、対応の遅れや被害の拡大を招くことがある。

こうした状況を背景に、我が国でもサイバーセキュリティに関するガイドライン策定などの政策的取組が実施されつつあり、それらにおいて、企業・組織の経営層が自ら責任を持ち、全社的なリスクマネジメントの観点からサイバーリスクに取り組む姿勢が求められている。

本稿では、こうした社会的要請やビジネス環境の変化を踏まえ、経営層の視点からサイバーリスクをどのように捉え、どのような枠組みの中でリスクマネジメントを実践していくべきについて、その考え方と経営層がどうリードすべきかの観点から概説する。

2　企業・組織にとっての課題

2.1　サイバーセキュリティ上の脅威

経営層がリードするにあたって、まず、企業、組織にとってサイバーセキュリティ[1]を巡る脅威としてどの様なものがあるかを知ることが大切である。そのため、サイバーセキュリティに係る動向を概観する。

一般に、報道などは個別のサイバー攻撃事案などを取り上げ、その攻撃の手段や被害・影響などに焦点を当てているものが多い。そして、内閣サイバー

[1] サイバーセキュリティ基本法では、「サイバーセキュリティ」を「電子的方式、磁気的方式その他人の知覚によっては認識することができない方式により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置（情報通信ネットワーク又は電磁的方式で作られた記録に係る記録媒体を通じた電子計算機に対する不正な活動による被害の防止のために必要な措置を含む。）が講じられ、その状態が適切に維持管理されていることをいう。」と定義している。

セキュリティセンター（NISC。※ 2025 年 7 月 1 日に国家サイバー統括室に改組）や警察庁といった政府機関や、独立行政法人情報処理推進機構（IPA）などサイバーセキュリティ関連機関は、顕著な事件や複数のサイバー攻撃事件の傾向や対策をまとめた注意喚起の発出などをしている[2]。これらの多くは、企業、組織におけるサイバーセキュリティ担当部門などによる対策を促す効果も狙っていると考えられ、サイバー攻撃手法のタイプ別に技術的側面なども詳しく説明する傾向がある。そこで、まずは、サイバー攻撃手法のタイプ別に、極力平易な説明となるように心がけ、これらを概観することから始める。

我が国の最近のサイバーセキュリティを巡る脅威について、IPA が毎年、前年度のサイバーセキュリティに係る事件などを踏まえて有識者による議論の結果を情報セキュリティ 10 大脅威として公表している。2025 年 2 月に公表されたものによれば組織向け脅威はランサムウェアによる被害等が挙げられている（表 1）（注「個人」向け脅威については順位表示ではなく、五十音順での掲載となっている）。[IPA, 2025]

表 1　情報セキュリティ 10 大脅威 2025 [IPA, 2025]

「個人」向け脅威	順位	「組織」向け脅威
インターネット上のサービスからの個人情報の窃取	1	ランサムウェアによる被害
インターネット上のサービスへの不正ログイン	2	サプライチェーンや委託先を狙った攻撃
クレジットカード情報の不正利用	3	システムの脆弱性を突いた攻撃
スマホ決済の不正利用	4	内部不正による情報漏えい等
偽警告によるインターネット詐欺	5	機密情報等を狙った標的型攻撃
ネット上の誹謗・中傷・デマ	6	リモートワーク等の環境や仕組みを狙った攻撃
フィッシングによる個人情報等の詐取	7	地政学的リスクに起因するサイバー攻撃
不正アプリによるスマートフォン利用者への被害	8	分散型サービス妨害攻撃（DDoS攻撃）
メールやSMS等を使った脅迫・詐欺の手口による金銭要求	9	ビジネスメール詐欺
ワンクリック請求等の不当請求による金銭被害	１０	不注意による情報漏えい等

これを踏まえて、組織に係る 10 大脅威として挙げられたもののうち主だったものについて概説する。

2.1.1　ランサムウェア

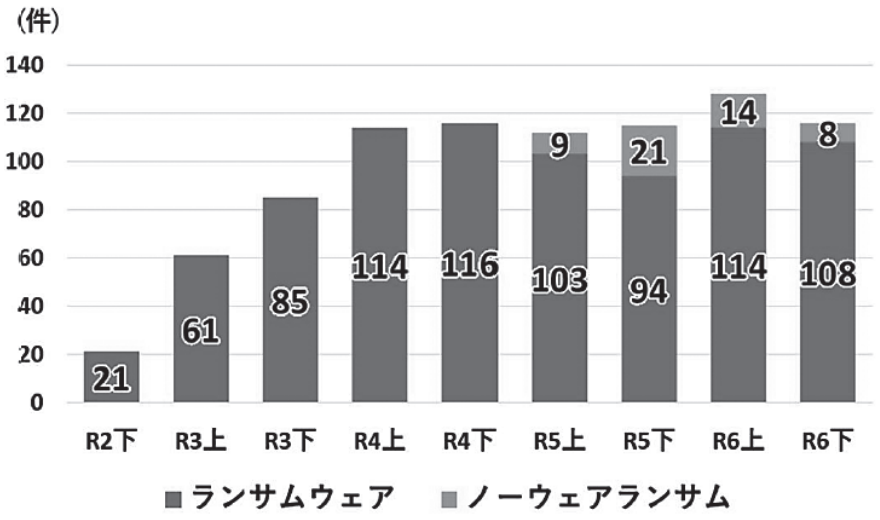
ランサムウェアによる被害の例として、港湾のシステム[3]を狙ったもの、大規模な病院[4]を狙ったものなどあるが、最近の例として、2024 年 6 月に障害が発生したオンライン配信・大手出版社の事件が強く記憶にあろう。サイバー攻撃の結果、縮退したサービスとせざるをえなくなり、復旧まで約 2 か月を要している。オンライン事業のみならずリアルの事業にも支障が生じた。さらに、ランサムウェアによるファイルの暗号化のみならず、情報を窃取し、それを暴露するという脅迫もなされた。現に、顧客の個人情報などがインターネット上に曝露された。この攻撃により 25 万人分を超える個人情報や企業情報が漏えいしたことが確認された [KADOKAWA, 2024]。

また、国際的にランサムウェア対策の重要性を政治的にも強く認識させた顕著な事件の例としては、2021 年 5 月にロシアの犯罪者集団が米国のパイプライン会社のネットワークから約 100GB のデータを窃取した事件を挙げられる。攻撃認識後、同社はパイプラインをシャットダウンし、また、連邦捜査

[2] 例えば、内閣サイバーセキュリティセンターが 2024 年 6 月に発出した「Living Off The Land 戦術等を含む最近のサイバー攻撃に関する注意喚起」（https://www.nisc.go.jp/pdf/news/press/240625NISC_press.pdf）など。
[3] 具体的には、国土交通省「コンテナターミナルにおける情報セキュリティ対策等検討委員会について」（https://www.mlit.go.jp/kowan/kowan_mn2_000006.html）を参照。
[4] 例えば、2022 年 10 月に発生した大阪急性期・総合医療センターへのサイバー攻撃により電子カルテを含めた総合情報システムが利用できなくなり、救急診療や外来診療、予定手術などの診療機能に大きな支障が生じた事件（https://www.gh.opho.jp/incident/1.html）など。

局 FBI にランサムウェア攻撃を受けたことを報告している。その後、米国上院国土安全保障・政府問題委員会公聴会にて同社 CEO が次のように状況を説明している。すなわち、従業員、地域、環境に危害を与えないよう、安全なオペレーション状態であると考えるときにのみパイプラインのオペレーションをできる。いかなる従業員も「停止権限」を有し、リスクを特定したときには、直ちにリスクを封じ込めることが従業員の業務となっている。コントロールルームのスクリーン上にランサムウェアの表示が出現したため、スーパーバイザが直ちにパイプラインのシャットダウンを決めた [NPR, 2021] [BankInfoSecurity, 2021] ということである。また同 CEO は暗号資産によって身代金を支払っているが、その行為が安全保障上正当なものと認識しているとの説明もしている。同事件は、結局、バックアップなどからの再構築によりシステムを復旧しており、また、同社が暗号資産で支払った身代金の多くは FBI が押収している。

警察庁によれば、ランサムウェアの警察への被害届出が 2020 年上旬以後増加し、近年高止まりしている（図 1）。被害者の過半は中小企業である。その手口の大半は、被害者のネットワーク内にあるファイルを暗号化するのみならず情報を窃取し、それを曝露して欲しくなければ身代金を支払うことを要求する二重恐喝型である。ランサムウェアの感染経路の大半は VPN（Virtual Private Network。外部から社内のネットワークに安全に接続するための仮想専用線）などの脆弱性（セキュリティ上の弱点）を悪用するものである [警察庁 , 2025]。2020 年上旬、新型コロナウイルスの蔓延からリモートワークなどが短期間で広く実施されるようになり、そのために VPN の導入、拡充などが進んだ。しかしそのような VPN などの脆弱性管理が十分に行われていないことなどから攻撃を許してしまったといえよう。あらたなテクノロジーの適用や適用範囲の拡大などがあったときに、そうした部分でサイバーセキュリティインシデントが起こり勝ちであるが、近年のランサムウェアの被害拡大は、そうしたケースの一例といえよう。



※　ノーウェアランサム：暗号化することなくデータを窃取した上で、対価を要求する手口。令和 5 年上半期から集計。

図 1　ランサムウェア等の被害報告件数の推移　[警察庁 , 2025]

2.1.2　標的型攻撃

標的型攻撃とは、国の機関や機微なビジネスに携わる民間企業等、特定の組織を狙う攻撃のことであり、機密情報等の窃取や破壊などを目的とするものである。

例えば、本年 (2025 年) 1 月、警察庁・内閣サイバーセキュリティセンターから標的型攻撃の注意喚起がなされた。具体的には、2019 年以降、日本の研究機関、政治家、政府関係者、マスコミ関係者などに対して、実在の人物になりすましたメールが送ら