URL https://journal.ntt.co.jp/article/30161
DOI https://doi.org/10.60249/24112001

ビジネスのイネーブラーとしてのセキュリティ ー前編ー

サイバー攻撃の規模が拡大し，手法も高度化し，これらにより新たな脅威も発生しています．大きな被害をもたらす事件も引き続き発生しています．また，デジタル化によってITシステムが社会で重要な役割を果たしていることから，ITシステムの障害は重大な社会的影響を及ぼします．一方で各国政府などにおけるITに関する取り組みも進化しています．こうした環境の変化の中で，セキュリティの位置付けは，脅威への対応コストという概念から，ビジネスのイネーブラーへと変化しつつあります．

セキュリティの意義の変化

デジタル化やAI（人工知能）の活用が進む一方，サイバー攻撃の件数や被害金額も世界的に増加しています．それだけではなく，新たな攻撃手法が現れ，これらは技術的にも高度化しています．厳しさを増す国際情勢などを反映し，政府や重要インフラへの攻撃，AIシステムへの攻撃など，新たな脅威も生まれています．

セキュリティといえば，どうしてもこのような負の側面と，それをどうやって防ぐかということに注目が集まりがちです．もちろんこれは目を背けることのできない社会の重要課題であることは間違いありません．

しかし，それだけではなく，セキュリティによりビジネスに新たな価値がもたらされる事例も生まれてきています．セキュリティもデジタル化における不可欠な基盤の1つであり，高品質なセキュリティはビジネスの付加価値になるとの考え方です．2021年に閣議決定された「サイバーセキュリティ戦略」で，政府は「デジタル改革を踏まえたデジタルトランスフォーメーションとサイバーセキュリティの同時推進」の方向性を明確にし，「デジタル化進展の中で，IT システムやデジタル化への対応能力が，業務，製品・サービス等の有する付加価値の源泉となっていくと想定される中で，サイバーセキュリティの確保は企業価値に直結する営為となる」と述べています．

本稿では全2回にわたり，セキュリティの現状を踏まえつつ，セキュリティがビジネスのイネーブラーとなっている動きについて紹介します．

表1 「情報セキュリティ10大脅威2024」（組織）

順位	「組織」向け脅威
1	ランサムウェアによる被害
2	サプライチェーンの弱点を悪用した攻撃
3	内部不正による情報漏洩等の被害
4	標的型攻撃による機密情報の窃取
5	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
6	不注意による情報漏洩等の被害
7	脆弱性対策情報の公開に伴う悪用増加
8	ビジネスメール詐欺による金銭被害
9	テレワーク等のニューノーマルな働き方を狙った攻撃
10	犯罪のビジネス化（アンダーグラウンドサービス）

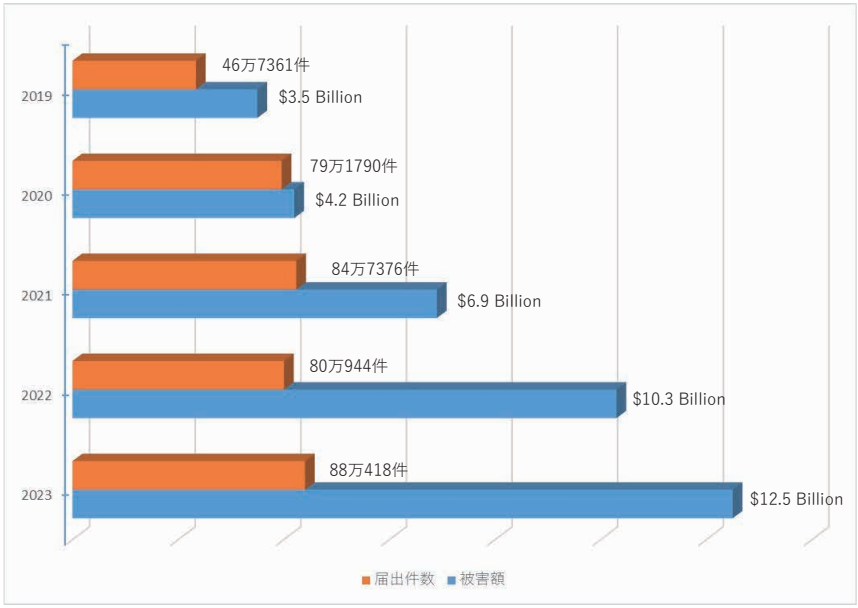
出典：IPA「情報セキュリティ10大脅威2024」を基に情報通信総合研究所作成

セキュリティをめぐる現状

■現状と課題

まずは現状をみておきましょう．2024年1月，独立行政法人情報処理推進機構（IPA）は，「情報セキュリティ10大脅威2024」を発表しました[1]．これは，IPAが毎年，社会的に影響が大きかったと考えられる事案を10個，「個人」と「組織」それぞれについて選出，発表しているものですが，「組織」についてみると，1位が「ランサムウェアによる被害」，2位が「サプライチェーンの弱点を悪用した攻撃」，3位が「内部不正による情報漏洩等の被害」となっています（**表1**）．いずれについても，最近，大きな事件が報じられています．

2024年6月，社会的影響が大きく，大きな話題の1つとなったのが，ランサムウェアによるKADOKAWAとそのグループ企業への攻撃でした[2],[3]．ランサムウェアとは，「ランサム（身代金）」と「ソフトウェア」を組み合わせてできた言葉で，悪質なソフトウェアにより攻撃先のデータを暗号化したり，盗み出したりして，暗号化されたデータの復元や，他へ漏洩しな



出典：FBIインターネット犯罪苦情センター「Internet Crime Report 2023」を基に情報通信総合研究所作成

図　米国におけるサイバー犯罪被害と被害額の推移

いことへの対価としての「身代金」を要求する不正なプログラムです．出版大手企業であり，子会社ドワンゴが動画投稿サイト「ニコニコ動画」を運営していることでも知られる同社では，グループ企業のデータセンタのサーバがサイバー攻撃を受け，データを暗号化されるとともに，社内外合わせて25万人分を超える個人情報が流出しました．また，これにより，出版事業に関するシステムが停止し，出荷数量の減少，「ニコニコ動画」などのオンラインサービス停止，学校法人角川ドワンゴ学園の学生情報の漏洩など深刻な被害も出ており，事業活動への影響は数カ月に及んでいます．さらに，同社は攻撃者側に身代金を支払ったとの複数の報道もあり，これも大きな問題となっています．KADOKAWAとドワンゴはシステムの再構築などを行って順次事業活動を再開していますが，その後の8月下旬にも，犯行グループによる新たな脅迫が行われており（犯行グループは身代金の受け取りを否定しています），本稿執筆時点では，解決には遠い状況とみられます．

世界的にも，年々被害が拡大しています．米国でFBIのインターネット犯罪苦情センターに届け出のあったサイバー犯罪被害は，2023年に件数88万件，被害額125億ドルに達しています[4]．これを2019年と比べると，件数は約1.9倍になっているのに対し，金額では約3.6倍となっています（**図**）．被害1件当りの被害額が増えていることが分かります．この多くはフィッシングと個人情報漏洩とみられています．

被害者はこのような犯罪に巻き込まれると，時間を浪費するだけでなく，例えばクレジットカードの凍結などで，社会的なダメージを受けます．また，漏洩した情報を悪用され，次の犯罪につながるおそれもあります．

このような現実を踏まえ，ビジネスパーソンにも，サイバーインシデントのリスクが，他のリスクと比較しても大きなものと認識されています．保険会社Allianzが世界の法人顧客に対し行った調査（2024年1月発表）では，ビジネスに対するリスクとして「サイバーインシデント」が3年連続でトップとなりました[5]（**表2**）．

また，世界経済フォーラムが2024年1月に発表した報告書でも，サイバー攻撃・犯罪が，「現在」「今後2年間」「今後10年間」いずれにおいても，グローバルリスクのトップ10位以内に入っています．「AI技術がもたらす悪影響」「誤報と偽情報」といった関連する項目も含め，サイバーインシデントが，事業に大きな影響を及ぼすリスクと認識されていることが分かります．

■新たな脅威

新たな脅威も指摘されています．新技術，サービスが生まれれば，それが標的となりますし，攻撃を行う側がそれらを利用することもあります．

ここではAIに関する脅威を例に挙げます．コンテンツ生成が可能な生成AIは，膨大なデータを学習し問題を解決できる手段として，さまざまな分野での活用が期待されていますが，その一方で，生成AIそのものが攻撃対象となる危険性と，生成AIを利用した攻撃が行われる可能性が指摘されています．

生成AIそのものが攻撃対象となる危険性としては，例えば，AIモデルの学習に使用するデータを取り換え，「汚染」されたデータを与える「データポイズニング」で，生成AIに誤った結果を出力させることができます．偽情報を与えて，動作を変更させ，ヘイトスピーチや陰謀論を生成させることも可能になるのです．最近では，大規模言語モデルのパフォーマンスを向上させるため，追加の外部データの情報を検索して補完する「検索拡張生成」技術を組み合わせることも多くなっていますが，これは「データポイズニング」に対し特に脆弱ともいわれています．追加データの管理が適切でない場合，悪質な情報が含まれる可能性があるからです．

また，生成AIを利用して従来からある攻撃をより「効率化」し，拡大させることも可能です．IBMの報告によれば，従来，経験豊富な攻撃者が16時間をかけて作成していたのと同じくらい巧妙な，相手企業の情報を用いたフィッシングメールを，生成AIを用いることにより，わずか5分程度で作成できたとされています．

ITシステムとデータの重要性

■ITシステムの社会的重要性の増加

最近では，デジタルトランスフォーメーション（DX）も進み，ITシステムがあら

表2　グローバルビジネスにおけるリスク要因

順位	リスク	%	2023年
1	サイバーインシデント（サイバー犯罪，ITネットワーク，サービス障害，マルウェア，ランサムウェア，データ侵害等）	36%	1位（34%）
2	ビジネス停止（サプライチェーン障害を含む）	31%	2位（34%）
3	自然災害（嵐，洪水，地震，山火事）	26%	6位（19%）
4	法制度，規制の変化（料金，経済制裁，保護主義）	19%	5位（19%）
5	マクロ経済変化（インフレーション，デフレーション，金融政策）	19%	3位（25%）
6	火災，爆発	19%	9位（14%）
7	気候変動（地球温暖化に伴う物理的，金銭的リスク）	18%	7位（17%）
8	政治的リスク，暴動（政治不安定，戦争，テロ，クーデター）	14%	10位（13%）
9	市場変化（競争激化，新規参入，M&A）	13%	11位（11%）
10	スキルのある労働力の不足	12%	8位（14%）

出典：Allianz「Allianz Risk Barometer Results appendix」を基に情報通信総合研究所作成

ゆる社会生活を支えています．これは社会の進歩と効率化に大きく貢献していますが，その分ITへの依存が大きくなり，ITに障害が発生したときには，社会活動にも悪影響が発生します．これを如実に示したのが2024年7月に発生した全世界的なシステム障害でしょう．米国のサイバーセキュリティ技術企業クラウドストライクが，欠陥のあるセキュリティソフトウェアアップデートを行ったことにより，運輸，病院，銀行，放送局，そして政府や多くの産業等が被害を受けたのは記憶に新しいところです．この事件では，Windowsコンピュータで「ブルースクリーン」エラーが相次いで発生し，Microsoftの推定によれば，世界で約850万台が影響を受けました．これにより，米デルタ航空では約7000便が欠航しました．また，英国など複数の国で病院が予約をキャンセルしたほか，米国の緊急通報用の電話番号「911」にも問題が生じました．生放送ができなくなったテレビ局もありました．

これはサイバー攻撃によるものではありませんでしたが，原因を問わず，ITシステムの可用性が大きく損なわれることになれば，広範な社会活動が影響を受けます．これは企業にとっては，事業における損害を意味します．復旧に要する費用だけでなく，損害が発生している間，そして将来得られるはずだった利益も失うことになるのです．

この事件の難しさは，影響の大きさ，深刻さに加えて，直接被害を受けた企業が，セキュリティ対策を怠ってはいなかったということにあります．むしろ，今回に関しては，先進的な対策を行っていた企業が大きな影響を受けました．ソフトウェアアップデートのリリース体制など，セキュリティサービスのあり方はもちろん，特定システムへの依存など，さまざまな問題が明らかになりました．もちろん，事故は起こるものであり，ゼロにすることはできません．もしこのような事態が発生した場合でもいかにして被害を最小化し，事業を継続するかも新たな課題となったといえるでしょう．

■各国政府の取り組み

ITが社会的に重要な存在となったことを受けて，世界各国で，政府としてのサイバーセキュリティへの取り組みも進んでいます．本稿の冒頭で日本の取り組みに触れましたが，ここでは，米国・欧州の取り組みについてみていきます．

米国では，2022年3月，重要インフラでのサイバーインシデントの報告を義務付ける法律が制定されました．これは，対象となる重要インフラ事業者に，重大なサイバーインシデントやランサムウェア攻撃に対する身代金支払いに関し，CISA（Cybersecurity and Infrastructure Security Agency：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）への報告を義務付けるものです．対象となる事業者は，政府，防衛，医療，緊急サービス，エネルギー，通信，情報技術，重要製造，輸送システム，金融サービスなど16部門にわたります．

また，2023年3月には米国政府が「国家サイバーセキュリティ戦略」を発表しました．これは，同国ですでに存在するサイバーセキュリティ対策を前提として，「サイバー空間はそれ自体の目的のために存在するのではなく，我々の最も高い理想を追求するための手段として存在する」と述べ，差し迫った脅威への即応と同時に，将来を見据えた戦略的計画と投資のバランスを取りながら，長期的な投資を促すようインセンティブを再調整するとして，脅威に対処しつつ，デジタル時代の未来の可能性を確保するとの考え方を明確にしています．

欧州においても類似の法整備が進んでいます．欧州委員会によって2020年12月に公表された「欧州サイバーセキュリティ戦略」では，サイバーセキュリティが「欧州のデジタルの未来」の重要な構成要素と位置付けています．そして，これに基づき，2022年11月，「ネットワーク情報セキュリティ（NIS）指令」の改正案（いわゆる「NIS2」）が採択され，対象15分野におけるリスク管理対策と，重大なサイバーインシデントに関する報告要件を定めています．

なお，政府への報告義務に関しては，日本においても，「サイバーセキュリティ基本法」で「重要社会基盤事業者」の責務が示されており，これに基づき策定される2024年3月の「重要インフラのサイバーセキュリティに係る行動計画」（5次行動計画）では，情報通信，金融，医療，運輸関係など15の分野が指定されています．政府への情報共有義務についても，「国家安全保障戦略 2022」で「能動的サイバー防御」の1つとして言及されており，検討段階にあるとみられます．

このように，各政府において細かなアプローチの違いはあるものの，いずれも，政府としてITを社会の基盤と位置付け，社会基盤に関する関係者のサイバーセキュリ

ティ関連対策義務を明確にするとともに，「もぐらたたき」的な脅威への対処だけでなく，あるべきデジタル社会の進展に向けた投資を促進し，エコシステムの形成を図る点が共通しています．

また，米欧日の取り組みには，国家間の協調も含まれています．例えば，北大西洋条約機構（NATO）のCCDCOE（Cooperative Cyber Defence Centre of Excellence：サイバー防衛協力センター）には，NATO加盟国以外に，「貢献国」として，日本を含む7カ国が参加しています（2024年8月現在）．そして，CCDCOEが主催する世界最大規模の国際サイバー防衛演習「Locked Shields」には，近年，日本の政府機関や，NTTなどの重要インフラ事業者等も参加しています．この演習は，サイバーセキュリティの専門家が，リアルタイムの攻撃下にある国家のITシステムや重要インフラを防御するスキルを向上させることを目的としています．参加者は「レッドチーム」（攻撃側）と「ブルーチーム」（防御側）に分かれて，多数のシステムの保護だけでなく，証拠保全・分析や法的課題への対処，情報運用の課題などに迅速に対応しなくてはならない危機的状況での対処について，実践的な演習を行います．国家間，かつ官民で強調して社会を守る重要な取り組みといえるでしょう．

セキュリティの意義の転換

■「追加負担」から必要な原価へ

セキュリティといえば，脅威に対応するものであり，コストは必要悪である，との考えが一般的でした．ウイルス対策ソフトもサイバーセキュリティ保険もセキュリティ教育の費用や時間も，組織や個人にとっては，より大きな被害を防ぐためのコストであり，事業に対する成果はない（見えない）にもかかわらず，やむを得ず支払う「追加負担」でした．このことが，特に体力の弱い中小企業にセキュリティ投資をためらわせてきました．

しかし，この考え方は過去のものです．例えば，今，自動車のシートベルトを「追加負担」だと考える人はまずいないでしょう．昔は面倒と思う人も多かったのですが，最近ではシートベルトを装着するのは当たり前であり，むしろ，ドライブをより安全にし，万一の場合にも命や身体を守るために，さまざまな装備（エアバッグなど）が追加され，それが新たな価値となっています．

セキュリティもこれと同じです．セキュリティを，ITサービスをより快適に，より良く活用するための付加価値としてとらえ直す必要があるのではないでしょうか．セキュリティにおいては，まず，守るべきものを定義しなくてはなりません．例えば，「PCを暗号化し，盗難の際の情報漏洩を防ぐ」など，今の会社の資産を守る（前述の例でいえば，シートベルトにより，万一衝突しても命に別条がないようにする）ことが第一歩ではありますが，それだけでなく，セキュリティをより高品質なものとすることで，会社の将来の成長を守り，ひいては事業を拡大することにもつながるのです．

■ビジネス戦略としてのセキュリティ

最近では，ビジネス戦略の中で，自社のセキュリティに関する品質，サービスを，高付加価値化の源泉とする動きが出てきています．

まず，高品質なセキュリティに基づく信頼構築はビジネスの重要な基礎となります．顧客は，データ（特に，個人情報などの秘密を保ちたい情報）を他社に預けることにリスクを感じています．正しいデータを安全にやり取りし，安定的に運用できる企業として認められることは，顧客のロイヤリティ，関係の継続，そしてブランドの評価につながります．

さらに，DX化が進む中では，正しいデータに基づく事業運営が，より高品質なサービスにつながります．「Data is new oil」とよくいわれますが，基になるデータが正確であることで，データを新たな価値の源泉として，新たな発見や分析による質の高い意思決定を行うことが可能になります．データの正確さを保つことも，セキュリティにほかなりません．

後編では，このような，セキュリティをビジネスのイネーブラーとする例について取り上げます．

■参考文献

(1) 独立行政法人情報処理推進機構（IPA）：“情報セキュリティ10大脅威 2024，”2024年1月．
(2) Piyolog：“KADOKAWAグループへのサイバー攻撃や悪質な情報拡散についてまとめてみた，”2024年8月19日．
(3) 共同通信：“「交渉決裂」とロシア系ハッカーKADOKAWA障害，再攻撃も，”2024年8月27日．
(4) FBI Internet Crime Complaint Center：“Internet Crime Report 2023，”2024年3月．https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf
(5) Allianz：“Allianz Risk Barometer Results appendix 2024，” 2024年1月．https://allianzcommercial.nl/content/dam/onemarketing/commercial/commercial/reports/Allianz-Risk-Barometer-2024-Appendix.pdf

株式会社 情報通信総合研究所
左高大平