事務所News
2025.11
K-075
発行：ふじわら税理士事務所　兵庫県高砂市神爪1丁目12番18号 高田ビル2F　Tel.079(433)0030　Fax.079(433)0020

経営バイタルの強化書 KEIEI VITAL

情報セキュリティインシデント状況とAIリスクを知っておきましょう!

情報セキュリティ白書2025

情報セキュリティ白書は200頁を超える分量ですが、情報セキュリティにおける近年の重要事項を網羅しており、概要を把握しておくことは重要です。今回は、国内における情報セキュリティインシデント状況と最近のサイバー空間を巡る注目事象 AIリスクについて説明します。

1 情報セキュリティ白書2025の概要

独立行政法人情報処理推進機構セキュリティセンター（以下「IPA」という）は、9月10日「情報セキュリティ白書」の2025年版を刊行しました※。

「情報セキュリティ白書」は、2008年以降毎年刊行されており、サイバーセキュリティ分野におけるインシデントや被害の実態、脅威の動向、最近の注目事象、国内外の政策や制度、調査報告書、セキュリティ関連組織が提供する各種セキュリティ対策向けの施策など、多岐にわたる内容が網羅されています。

2024年以降も引き続き、ランサムウェア攻撃、標的型攻撃、DDoS攻撃などが国内外で多数観測されるとともに、攻撃の手口の巧妙化・高度化も確認されるなど、サイバー空間における脅威は増大しています。国際的には、地政学リスクに起因するサイバー攻撃や偽情報の拡散など認知領域における情報戦なども観測されています。さらに、生成AIをはじめとするAI関連技術の進展に伴い、サイバー攻撃によるAIシステムへの攻撃や悪用、認知領域への攻撃が懸念されてきています。

国内では、サイバー対処能力強化法及び同整備法、国家サイバー統括室の設置など、「国民生活や経済活動の基盤」と「国家及び国民の安全」をサイバー攻撃から守るための能動的なサイバー防御を実施する体制の整備が進められています。

「情報セキュリティ白書」は、序章 2024年度の情報セキュリティの概況、第1章 国内外のサイバー脅威の動向、第2章 最近のサイバー空間を巡る注目事象、第3章 国内の政策及び取り組みの動向、第4章 国際的な政策及び取り組みの動向から構成されており、全体で200頁を超える内容となっています。

以下では「情報セキュリティ白書」の内、第1章 国内外のサイバー脅威の動向 国内における情報セキュリティインシデント状況、第2章 最近のサイバー空間を巡る注目事象 AIリスクの概要を説明します。

2 国内外のサイバー脅威の動向

● 国内における情報セキュリティインシデント状況

① フィッシングによる被害

フィッシング対策協議会への2024年度のフィッシング報告件数は200万6,872件で、2023年度（126万513件）から59.2%増となり、初めて200万件を超える結果となりました。

フィッシングサイトのURL件数では、2022年度をピークに2023年度は減少傾向だったものの、2024年度は再度69万3,499件と大幅な増加に転じました。

フィッシング被害に遭わないためにも、手口等の最新情報を知ることや、メール等に記載されているURL、QRコード、知らない番号からの着信にはより慎重になることが求められています。

② 情報漏えいと内部不正による被害

株式会社東京商工リサーチが2025年1月に公開した「2024年『上場企業の個人情報漏えい・紛失事故』調査」によると、2024年に上場企業とその子会社から公表された個人情報の漏えい・紛失事故の件数は189件でした。漏えいした個人情報は1,586万5,611人分であり、大規模な漏えい事故が相次いだ2023年に比べ38.8%に減少しました。

内部不正と関連するものとして、「不正持ち出し・盗難」による情報漏えいと、不正競争防止法違反（営業秘密の領得）が挙げられています。前者の「不正持ち出し・盗難」が原因で個人情報が漏えい・紛失した件数は、同調査では2024年は14件となり、2023年の24件より減少しました。後者に関しては、警察庁によれば、2024年の営業秘密侵害事犯の検挙事件数は22件で、2022年の29件をピークに減少傾向にあります。一方、営業秘密侵害事犯に関する相談受理件数は2023年の78件を上回り、2024年は79件と過去最多となりました。

③ DDoS攻撃による被害

株式会社インターネットイニシアティブ（IIJ社）では、月次の観測レポートとして、IIJ社のサービスから検出されたDDoS攻撃の観測情報を取りまとめています。同レポートによると、2024年度は合計3,462件のDDoS攻撃が検出されており、年度別の検出件数で見ると2021年度を境に減少傾向にあります。

裏面へ続く→

DDoS攻撃の検出数には増加が見られないものの、2024年12月末から2025年年始にかけては、日本国内において航空事業者や金融機関を狙ったDDoS攻撃が相次ぎ、多数の被害が発生しました。これを受けて、2025年2月には、内閣サイバーセキュリティセンター（現国家サイバー統括室（NCO））から、DDoS攻撃に関する注意喚起が発出されました。

④ ランサムウェアによる被害

2024年に警察庁に報告された国内のランサムウェアによる被害件数は222件で前年比12.7%増となり、依然として被害が多いことがうかがえます。

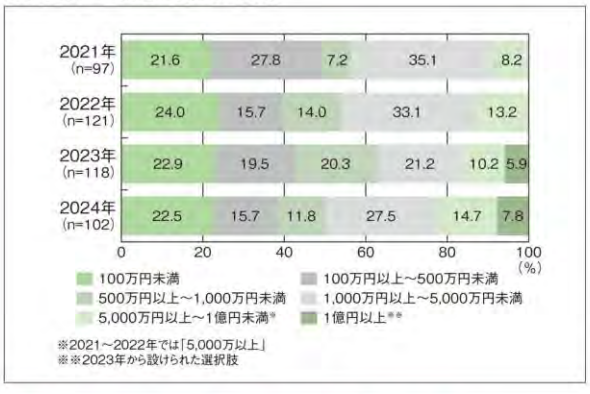
件数の内訳を企業・団体等の規模別で見ると、2024年は中小企業の被害件数が増加していることが分かります。

2024年の被害件数を業種別で見ると、「製造業」の割合が最も大きく29.3%（65件）で、次いで「卸売・小売業」が19.4%（43件）、「サービス業」が14.9%（33件）と続きます。それ以降は「建設業」「運輸・郵便業」「情報通信業」「医療・福祉」がそれぞれ10%未満で続いています。

「製造業」は2021年に調査を開始して以降4年連続で被害件数が最も多いという結果となりましたが、業種を問わず被害が発生している傾向は変わっていません。また、2024年に被害の報告があった222件のうち手口を確認できたのは134件で、そのうちデータを暗号化、窃取した上で対価を要求する「二重恐喝型」が82.8%（111件）を占め、2021年に調査を開始して以降4年連続で半数以上の割合を占める手口となっています。

【図1】国内のランサムウェアによる被害件数

【図2】調査・復旧に要した費用



⑤ 中小企業におけるインシデント発生状況

2025年にIPAが実施した「2024年度中小企業における情報セキュリティ対策に関する実態調査」によると、2023年度にサイバーインシデントが発生した、もしくは発生があった可能性が高い経験をした中小企業は、975件（23.3%）でした。具体的な被害としては、データの破壊が348件（35.7%）、個人情報の漏えいが342件（35.1%）と多く、次いでウイルスメール等の発信が210件（21.5%）、業務情報（営業秘密を除く）の漏えいが208件（21.3%）となりました。更に、サイバーインシデントが発生もしくは発生があった可能性が高い経験をした中小企業のうち、約7割がサイバーインシデントにより取引先（サプライチェーン）に影響があったと回答しています。

3 最近のサイバー空間を巡る注目事象

AIリスク

AIの利用の拡大や社会への浸透に伴って何らかの危害が人間や社会に生じるリスクをAIリスクと呼びます。

2025年1月末に英国科学技術イノベーション省（DSIT）が発表した報告書では、AIリスクを

① AIの悪用がもたらすリスク
② AIの不適切動作によるリスク
③ システミックリスク

に分けて説明されています。

AIの悪用がもたらすリスクには、下記のようなリスクがあるとされています。

(1) フェイク画像等がもたらす個人への被害

生成AIが生み出す、本物と見分けがつかない偽の画像や動画、音声、及びその生成技術を「ディープフェイク」と呼びます。人物の写真を与えてその顔を入れ替えたり表情を変えたりといった加工が行えるだけでなく、まったく架空の画像を作り出すこともできます。ディープフェイクはディープラーニングの登場から程なくして発達し、ディープフェイクを悪用した詐欺や恐喝、個人や組織の評判を傷つけるための偽情報の拡散、心理的な虐待といった悪用がFBIにより警告されています。

日本においても、子供達が性的虐待コンテンツをAIで生成した・生成された事例が報道されており、問題は深刻化の一途をたどっています。

(2) 世論操作

ディープフェイクの増加は、偽情報による世論操作のリスクも深刻化させています。

悪意のある人物や団体がAIで生成された偽情報を用いることで、大規模かつ巧妙な世論操作が可能になるのではないかという議論があり、懸念が高まっています。日本でも、東京電力ホールディングス株式会社福島第一原子力発電所の処理水の海洋放出に合わせるように、「処理水ではなく核汚染水だ」という言説とともに不安を煽る偽情報がSNSを中心に広がった事例がOpenAI社により報告されています。

(3) AIを悪用したサイバー攻撃

標的型攻撃のような高度なサイバー攻撃が汎用的AIによって完全に自動化されるのではないかという懸念があります。幸いなことに、2024年夏の時点ではAIの能力はその水準に達していないと評価されていますが、他方で、ChatGPTのようなAIサービスを活用することで、手動で行うサイバー攻撃を効率化する試みが、OpenAI社とMicrosoft社によって確認・摘発されています。

汎用的AIを利用することで、高度な技能を持たない人物であってもサイバー攻撃を実践できると指摘されており、サイバー犯罪ビジネスへの参入障壁を引き下げてしまうことが、目下の大きな懸念となっています。日本においても、中高生3人が汎用的AIを悪用してハッキング行為を行い、携帯電話会社の契約システムに不正ログインを繰り返し、利益を上げていたという事例が2025年2月に報道されています。

※ 情報セキュリティ白書2025（IPA）（URL：https://www.ipa.go.jp/publish/wp-security/2025.html）