情報セキュリティ白書

Information Security White Paper

2023

進む技術と未知の世界：新時代の脅威に備えよ

IPA 独立行政法人 情報処理推進機構
Information-technology Promotion Agency, Japan

「情報セキュリティ白書2023」の刊行にあたって

2022 年を振り返ると、2 月に発生したロシアのウクライナ侵攻は、近隣諸国や支援国、そして食料やエネルギー等の経済的つながりを持つ国々にまで影響を及ぼしました。この紛争は武力戦にサイバー空間を含む情報戦を加えたハイブリッド戦と呼ばれるものとなり、関係各国はランサムウェアを始めとするサイバー攻撃や、世論誘導を意図する虚偽情報拡散等の対応に追われました。米国では CISA、FBI 等によりサイバー攻撃への注意喚起が繰り返されました。日本では、9 月に政府機関や企業のホームページ等を標的とした DDoS 攻撃と思われるサービス不能攻撃により、業務継続に影響のある事案も発生したほか、国家等が背景にあると考えられる攻撃者による暗号資産取引事業者等を狙ったサイバー攻撃や、一定の集団によるものとみられる学術関係者等を標的としたサイバー攻撃も明らかとなり、国民の誰もがサイバー攻撃の懸念に直面することとなりました。政府からも関係省庁等々の合同による注意喚起が多数出されました。

この間、国内では、ランサムウェア攻撃による大きな被害が報告されました。2 月には自動車部品工場が攻撃を受け、出荷先の工場が稼働停止しました。10 月には自治体の医療センターのサーバーが取引先の給食提供業者を経由した攻撃を受け、電子カルテシステムが利用できなくなりました。サプライチェーン全体のセキュリティ対策、事業継続計画、インシデント対応等の重要性が再認識されました。

一方政策面では、「サイバーセキュリティ 2022」「重要インフラのサイバーセキュリティに係る行動計画」「国家安全保障戦略」 等が公表され、サイバー警察局、サイバー特別捜査隊等の設置等が実施されました。6 月に閣議決定された「デジタル社会の実現に向けた重点計画」では、利便性の向上とサイバーセキュリティ確保の両立に向け、官民の緊密な連携を進めていくことが示されました。

そして、2022 年は AI への注目が集まった年でもありました。特に生成系 AI の技術的な発展は目覚ましく、ビジネスにおける業務革新等への期待が高まる一方、AI の利用による人権、プライバシー、知的財産権等の保護が課題として顕在化しました。更にウクライナ侵攻では、虚偽情報生成に AI が利用され、情報の信頼性に対する課題が深刻化しました。このような AI の課題に対して EU では、AI の安全で遵法的な利用に関する規則が策定されました。また米国も「AI 権利章典」を公開して人権や安全に配慮した AI の利用を宣言しました。

AI 利用を起点とする IT 環境の革新は、確かに大きな可能性があるようですが、セキュリティやプライバシーの脅威も大きくなると思われます。では、私達はどうすればよいのでしょうか。

まずはリスクを正しく知ることから始めましょう。何が重大なリスクなのかを特定した上で、変化に対応してセキュリティ対策の基本を継続的に実践していくとともに、未知の脅威に対しては情報共有し、適切な利用について議論を重ね、安全、安心なデジタル社会の実現を目指していくことが重要です。

本白書が、多くの方々に広く利用され、技術の進展とそれに伴う未知の脅威、リスクに対する備えを実践するための一助となることを祈念します。

2023年7月

独立行政法人情報処理推進機構（IPA）

理事長 齋藤 裕

目次

コラム

2023

情報セキュリティ白書

序章

2022年度の情報セキュリティの概況

2022 年はウクライナ侵攻による安全面や経済面の不安が継続する一方、生成系 AI の急激な普及等で IT 環境の革新を予感させる年となった。国内では、企業・団体におけるランサムウェア被害が増え続けた。攻撃の手口では、窃取したデータを暴露する「二重の脅迫」に加え、被害組織への DDoS 攻撃や、被害の事実を被害組織の顧客や利害関係者に連絡する等の脅迫手法も確認されている。ここ数年で被害が急増している要因として、ランサムウェア攻撃をサービスとして提供する「RaaS（Ransomware as a Service）」の普及や、攻撃者の組織化・分業化が挙げられる。2022 年 2 月の自動車部品会社へのランサムウェア攻撃では、部品供給先である自動車工場の稼働が 1 日停止した。同年 10 月の大阪市の医療センターへのランサムウェア攻撃では、VPN でつながる給食提供業者から侵入され、サーバーを介して医療センターの電子カルテシステムに障害が及んだ。同システムはバックアップが保管されていたが復旧に 2 ヵ月を要した。これらの事案から、サプライチェーン全体での脆弱性対策、データ保護、復旧計画の必要性等が再認識された。

情報漏えいの被害について、調査会社の調査によれば、漏えい・紛失事故を公表した社数、事故件数はともに 2 年連続で最多となった。2022 年 6 月には、地方自治体の業務委託先の従業員が、46 万人余りの個人情報を含む USB メモリーを紛失した。USB メモリーは回収され、漏えいの痕跡はないとされたが、記録媒体管理の重要性を再認識させられる事案であった。

個人を狙ったフィッシング等の被害については、2022 年度は通信事業者をかたる偽 SMS が減少した一方、宅配便業者や公的機関をかたる偽 SMS が増加、または新たに出現した。また、パソコン利用者に対する偽のセキュリティ警告について IPA に寄せられた相談件数は過去 4 年間で最多となった。

海外においても、様々なサイバー攻撃の脅威がより深刻になっている。米国連邦捜査局（FBI）の年次報告書によると、2022 年に報告されたビジネスメール詐欺の被害総額は、前年比約 15% 増の約 27 億 4,200 万ドルであった。セキュリティベンダーが 2022 年上半期に全世界で確認した DDoS 攻撃は、過去最多となる約 602 万回で、前年同期比で 205% であった。ランサムウェア攻撃も世界中で起きており、イタリアでは地方行政機関の通信インフラのサービスが全面中断し、フランスでは病院が被害を受け手術の中止や入院患者の移送等、生活や治療に影響を及ぼす被害が報告されている。

セキュリティ政策面では、国内ではサイバー警察局、サイバー特別捜査隊等の体制面の強化、「サイバー攻撃被害に係る情報の共有・公表ガイダンス」の公開、業界ごとのサイバー・フィジカル・セキュリティ対策ガイドラインの公開等で、より実践的な対策を推進した。また、経済安全保障推進法や安全保障関連 3 文書の中でもサイバーセキュリティ対策強化の方向性が示された。

世界的には、2022 年 2 月のウクライナ侵攻以降、安全保障面の緊張、エネルギー・食料不足等で予断を許さない状況が続いている。ウクライナでの戦いは、国家間の武力攻撃とサイバー攻撃のハイブリッド戦、及びサイバー空間での情報宣伝戦が特徴となっている。サイバー攻撃について、米国はサイバー軍による諜報面のウクライナ支援、国内におけるサイバー攻撃注意喚起、大統領令 14028 に基づくサプライチェーン防御強化等を継続した。また EU は、重要インフラの統一セキュリティ規格である「NIS 2」を 2022 年 11 月に成立させた。

情報宣伝戦について、ロシアは虚偽情報を多用したが、ウクライナも SNS 等で情報を発信して対抗した。技術面では、生成系 AI の急速な発展や広告配信等の IT 基盤の普及により、虚偽情報の容易な生成・配信が可能となった。虚偽情報の識別は難しく、拡散にどう対応するかは今後の課題である。AI の関連政策として、EU は、AI の安全で遵法的な利用に関する規則「Artificial Intelligence Act」（AI 法）を公表、2023 年 6 月には生成系 AI の利用や学習に関する規制を追加した修正案を採択した。米国は 2022 年 10 月、「AI 権利章典」を公開した。欧米それぞれで人権や安全に関する AI の不適切な利用への対処に進展が見られた。

2022年度の情報セキュリティの概況

	主な情報セキュリティインシデント・事件	主な情報セキュリティ政策・イベント
2022年 4月	● CISA、ロシアのウクライナに対するサイバー攻撃情報開示（2.2.2）	● IPA、「組織における内部不正防止ガイドライン」第5版を公開（2.8.1） ● 警察庁にサイバー警察局、関東管区警察局にサイバー特別捜査隊を新設（2.1.5）
5月		● 「経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律案」成立（2.1.1） ● 第28回日EU定期首脳協議開催、デジタルパートナーシップ合意（2.2.1）
6月	● 地方自治体の業務委託先が個人情報を保存したUSBメモリーを紛失（1.2.9） ● イタリアの地方行政機関がランサムウェア攻撃でサービス停止（3.1.1）	● G7エルマウサミット開催（2.2.1） ● 「デジタル社会の実現に向けた重点計画」が閣議決定（2.1.1） ● NISC、「重要インフラのサイバーセキュリティに係る行動計画」公開（2.1.1）
7月	● ENISA、ランサムウェア脅威実態を報告（2.2.3）	
8月		● 総務省、「ICTサイバーセキュリティ総合対策2022」公開（2.1.4）
9月	● 親ロシア系攻撃集団、国内組織にDDoS攻撃（1.2.4） ● 家具製造小売業の持株会社が不正アクセスを受け、約13万2,000アカウント分の個人情報が流出（1.2.9）	● IPA、ビジネスメール詐欺の特設ページを開設（1.2.3） ● EU、デジタル製品の「サイバーレジリエンス法案」公開（2.2.3） ● ISMAP-LIU運用開始（2.7.3）
10月	● 大阪府の病院にランサムウェア攻撃、電子カルテシステムに障害が発生（1.2.1） ● 入力フォーム支援サービス事業者のサービスが不正アクセスを受け、入力情報が流出（1.2.9）	● 米国、「AI権利章典」公開（2.2.3）
11月	● IPA、学術関係者・シンクタンク研究員等を標的としたサイバー攻撃について注意喚起（1.2.2） ● 厚生労働省、医療機関等のサイバーセキュリティ対策で注意喚起（2.1.1） ● オーストラリアの保険会社の個人情報970万人分が漏えい（1.1.1）	● 経済産業省、「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」公開（2.1.3） ● EUの重要インフラの統一セキュリティ規格「NIS 2」が成立（2.2.3） ● EU、AI法修正案を公開（2.2.3）
12月	● フランスの病院がランサムウェア攻撃により患者を緊急移送（3.1.1）	● 安全保障関連3文書が閣議決定（2.1.1） ● 米国、国防授権法2023成立（2.2.2）
2023年 1月	● 保険会社の委託先に不正アクセス、顧客情報が流出（1.2.9） ● 米国ソーシャルテクノロジー企業にGDPR違反で3億9,000万ユーロの制裁金（2.2.3）	● 経済産業省、「クレジットカード決済システムのセキュリティ対策強化検討会 報告書」公開（2.1.3）
2月		● 日米豪印の4ヵ国（QUAD）で連携したサイバーセキュリティ月間実施（2.1.1）
3月	● IPA、Emotetの攻撃活動再開を観測（1.2.6）	● 経済産業省、「サイバー攻撃被害に係る情報の共有・公表ガイダンス」公開（2.1.1、2.1.3） ● IPA、「サイバーセキュリティ経営ガイドライン」改訂（2.1.3） ● 米国、新サイバーセキュリティ戦略を公開（2.2.2）

※ 2022年度の主な情報セキュリティインシデント・事件、及び主な情報セキュリティ政策・イベントを示している。ランサムウェア攻撃、標的型攻撃、ビジネスメール詐欺、DDoS攻撃、Web改ざん、フィッシング等の被害は通年で発生している。表中の数字は本白書中に掲載している項目番号である。特に注目されたもののみを挙げた。他のインシデントや手口と対策、及び政策・イベント等については本文を参照されたい。

索引

さ

た

な

は

ま

ら

わ