情報セキュリティ白書

Information Security White Paper

2022

ゆらぐ常識、強まる脅威：想定外にたちむかえ

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2022」の刊行にあたって

2021 年も新型コロナウイルス変異株による感染拡大が継続しました。米欧では対策緩和の方針がとられましたが、ワクチン接種やそれに基づく移動許可等の可否について多くの議論を呼びました。日本は、厳しい規制の中で東京 2020 オリンピック・パラリンピック競技大会を無観客で開催、成功させましたが、その後も規制はゆるまず、テレワーク等の新しい業務形態が定着していきました。

この間、重要な組織やインフラを狙った攻撃も続きました。特に目立ったのがランサムウェア被害です。米国では 2021 年 5 月にエネルギー事業者が攻撃を受け、米国東部の石油供給が一時ストップしました。国内では 7 月に食品事業者がバックアップデータまで暗号化され、事業再開が遅れました。10 月には病院が攻撃を受けて診療に支障が出ました。2022 年 2 月には製造事業者が攻撃を受け、納入先の事業者の生産に影響が出ました。昨年の巻頭言で申し上げたとおり、こうした攻撃は巧妙化しており、システムの脆弱性やサプライチェーンを介して侵入し、情報を盗んで二重の脅迫を行う等、深刻な脅威となっています。一方脆弱性については、テレワークで活用が進んだ VPN 等の対策がまだ十分でなく、12 月には広範囲の Web システムに影響を及ぼす Log4j の脆弱性が報告されました。こうした懸念もあり、2022 年の 10 大脅威では修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）が初めてランクインしました。テレワークや DX 推進等によって生活や業務の各場面でデジタル化が進む中、安全で信頼できると思っていた機器やシステムに脆弱性が見つかり、ゼロデイ攻撃され、生活の一部が突然立ち行かなくなるかもしれない、そういう時代を私達は迎えつつあります。

更に 2021 年後半以降のウクライナ危機は、「まさかこのような事態が起こるとは」を私達に痛切に感じさせました。ロシアとウクライナの紛争は、情報セキュリティの視点からは、三つの点が特に注目されます。一つ目は、紛争が武力とサイバー空間上の攻防が組み合わされたハイブリッドな戦いであること。二つ目は、ネット等で配信される紛争関連情報が急増し、その信頼性の見極めが難しいこと。最後は、サイバー空間の攻防において、民間組織や個人が簡単に当事者になってしまうこと。私達は国家間の分断や物的な流通分断のリスクに加え、虚偽の情報に誘導される、サイバー攻撃の対象になる、等のリスクに直面することとなりました。

半年前まで想定できなかったこうした状況に私達はどう対応すればよいでしょうか。申し上げてきたことの繰り返しになりますが、リスク対応の基本が大切であると思います。情報セキュリティに関しては、機器やシステムの脆弱性をなくすこと、このサービスが止まったときにどうするか、の想像力を持つことは大変重要です。また虚偽の情報に惑わされないために、様々なソースの情報を参照し、視野を広く持つことも大切になるでしょう。本白書が、多くの方々に広く利用され、新しい生活や働き方のリスクに対する意識を高め、備えを実践するための一助となることを祈念します。

2022年7月

独立行政法人情報処理推進機構（IPA）

理事長　富田達夫

目次

コラム

情報セキュリティ白書

序章

2021年度の情報セキュリティの概況

2020年から世界中で流行した新型コロナウイルス感染症については、日本・米国・欧州ではワクチン接種が進み、感染者の増減はあるものの、経済活動は徐々に以前の状態に戻りつつある。国内では、感染拡大防止対策として実施されたテレワークやオンライン会議等が新しい働き方として定着しつつある。こうした業務の見直し、デジタル化は、組織におけるDX（デジタルトランスフォーメーション）の推進を後押しする形となっている。

2021年はランサムウェアの手口が巧妙化して被害が拡大し、サプライチェーンに関連したインシデントや脆弱性を狙った攻撃も引き続き発生した。警察庁によれば、2021年下期の被害報告件数は2020年下期の4倍となった。また、2021年7月の製粉会社、10月の病院の事案では、バックアップデータも暗号化されたために早期復旧が困難であった。データ保管方法の見直しや復旧計画の重要性が再確認された。

攻撃経路として、海外拠点、海外子会社、取引先が攻撃され、被害を受ける事案も多くみられた。2021年10月の医薬品メーカの情報漏えい事案は海外拠点が攻撃対象であった。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、部品供給先の自動車メーカの工場が1日停止した。サプライチェーン全体のセキュリティ強化が求められている。情報漏えい事案としては、マッチングアプリや大手製菓製造会社への不正アクセスにより合わせて300万件以上の大量の個人情報が流出した。

ソフトウェアの脆弱性を悪用した攻撃も継続して報告された。2021年に報告された脆弱性としては、VPN製品、Microsoft Exchange Serverの脆弱性、多くの製品やソフトウェアで使用されるJavaベースのロギングライブラリApache Log4jの脆弱性等、影響範囲が広く、攻撃により大きな被害が予想されるものが目立った。このほか、2021年初頭に欧州司法機関の一斉テイクダウンにより沈静化したウイルス「Emotet（エモテット）」の感染が再拡大し、2022年に入り注意喚起された。

セキュリティ政策面では、国内では2021年9月に「サイバーセキュリティ戦略」が閣議決定された。同戦略では「DX with Cybersecurity」として、デジタル社会の進展と併せてサイバーセキュリティ確保の取り組み推進が重要とされた。また同月にデジタル庁が発足、政府のIT基盤とセキュリティの整備を統括することとなった。サプライチェーンセキュリティについては、経済産業省がサプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）等を継続的に推進した。

米国では、重要インフラやライフラインに関わる制御システムへの攻撃が相次ぎ、水道や浄水場等の制御システムへの攻撃、石油供給事業者へのランサムウェア攻撃が報告された。米国Biden政権は重要インフラのセキュリティ対策強化を打ち出し、これを受けた米国国立標準技術研究所（NIST）は、重要ソフトウェア調達におけるセキュリティガイドライン策定、消費者向けIoT製品のラベリング制度の検討等を実施した。NISTはまたサプライチェーンセキュリティに関する官民連携イニシアティブ（NIICS）の設置、サプライチェーンリスク管理の標準ガイド（NIST SP800-161）の改訂を進めた。今後の動向が注目される。

欧州では、欧州ネットワーク・情報セキュリティ機関（ENISA）が主導し、重要インフラに関するサイバーセキュリティ準拠法の改訂案（NIS2 Directive）審議、あるいは域内の製品・サービスのセキュリティを担保するサイバーセキュリティ認証スキーム（EUCC scheme V1.1.1）の構築等を中心としてセキュリティ政策を推進した。また欧州委員会は2021年4月、AI利用リスクへの対処に関する法案を公表した。同法は罰則を伴う初のAI利用規格として注目される。

このように、各国とも重要インフラやサプライチェーンへのセキュリティ対策強化を進めてきたが、2021年後半以降はウクライナ情勢が悪化、2022年2月のロシアのウクライナ侵攻により、世界は新たな緊張に直面している。この紛争は、武力とサイバー攻撃・防御あるいはサイバー空間での情報戦が組み合わさったハイブリッドな戦いが特徴であり、サイバー空間上では政府に加えて民間組織・個人が参画する、というまったく新たな状況が生まれている。政府の安全保障政策・サイバーセキュリティ政策は言うまでもなく、企業や個人がこのリスクへの対応、例えば、親ロシア系ハッカーの攻撃への備え、紛争に関連する情報の信頼度の見極め等をどうするべきか、が問われている。

2021 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
2021 年　4 月	● VPN 製品「Pulse Connect Secure」ゼロデイ攻撃発生（1.2.5） ● ファーストフードチェーン店でランサムウェア被害（1.2.8） ● マッチングアプリが不正アクセスを受け約 171 万件の個人情報流出（1.2.8、3.3.2）	■ 経済産業省「サイバーセキュリティ体制構築・人材確保の手引き」（第 1.1 版）改訂（2.1.2、2.3.1） ■ 欧州委員会「Artificial Intelligence Act」（AI 法）提出（3.4.2）
5 月	● 米石油供給事業者へのサイバー攻撃、身代金 500 万ドル相当を支払いか（3.4.1）	■ サプライチェーンセキュリティ強化を目指した米国大統領令 EO 14028 発表（3.4.1） ■ EU 域内のセキュリティ認証スキーム（EUCC scheme V1.1.1）公開（3.4.2）
6 月	● 無線通信機器メーカ、2017 年に不正アクセス確認から 3 年以上報告せず（1.2.8） ● 電子部品メーカの再委託先社員が取引先情報約 3 万件、従業員関連情報約 4 万件を不正持ち出し（1.2.8）	■ 総務省「スマートシティセキュリティガイドライン（第 2.0 版）」公開（2.1.3）
7 月	● 大手製粉会社がサイバー攻撃を受けシステム障害（1.2.2） ● IT 管理ツールをランサムウェア攻撃に悪用（1.1.1）	■ NISC「政府機関等のサイバーセキュリティ対策のための統一基準（令和3年度版）」公開（2.1.1） ■ 総務省「ICT サイバーセキュリティ総合対策 2021」公開（2.1.3）
8 月	● ProxyShell の脆弱性を公表(1.2.5)	■ IPA「サイバーセキュリティ経営可視化ツール」公開（2.1.1） ■ NIST が「サプライチェーンセキュリティに関する官民を推進する国家イニシアティブ」を設置（3.4.1）
9 月		■ デジタル庁発足（2.1.1） ■ NISC「サイバーセキュリティ戦略」「サイバーセキュリティ 2021」決定（2.1.1）
10 月	● 徳島の町立病院でランサムウェアの被害発生（1.2.2） ● 医薬品メーカの国内外の拠点に不正アクセス（1.2.8）	■ NISC、第 14 回「日・ASEAN サイバーセキュリティ政策会議」開催（2.2.1） ■ Ransom Disclosure Act 米国議会に提出（3.4.1）
11 月	● 大手眼鏡販売チェーン持株会社で約 1 億円のビジネスメール詐欺被害（1.2.3） ● Emotet（エモテット）の攻撃活動再開（1.2.6）	■ NISC「クラウドを利用したシステム運用に関するガイダンス」公開（2.1.1、3.3.4） ■ CISA が既知の脆弱性悪用に関する重大リスクの削減に関する運用指令を公開（3.4.1）
12 月	● ロギングライブラリ Apache Log4j の任意のコード実行の脆弱性に関する注意喚起（1.1.1、1.3.2） ● スマホ決済のキャンペーン関係識別情報 13 万 3,484 件が GitHub 上で閲覧可能になっていたと発表（1.2.8）	■ 米 Biden 大統領が国防授権法に署名、アジア大平洋地域やウクライナ・NATO への関与を強化（3.4.1）
2022 年　1 月	● 決済サービス事業者不正アクセスによる情報漏えい公表（1.2.8）	
2 月	● ロシアがウクライナに侵攻（3.4.1） ● CISA、FBI がウクライナで使用された破壊的ウイルスに関し注意喚起（3.4.1）	■ NIST「ソフトウェアサプライチェーンセキュリティガイダンス」、NIST SP800-218 Ver.1.1 公開（3.4.1）
3 月	● 自動車部品会社がサイバー攻撃を受け、自動車メーカが国内工場停止（1.2.2） ● 大手製菓製造会社への不正アクセス（1.2.8） ● 複数の自治体で利用するクラウドが踏み台となり約 91 万件の迷惑メール発信（3.3.2）	■ CISA がウクライナ関連攻撃対策サイト「SHIELDS UP」を公開（3.4.1） ■ 総務省「地方公共団体における情報セキュリティポリシーに関するガイドライン」改訂版等公開（2.1.3）

※ 2021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。標的型攻撃、ランサムウェア被害、ビジネスメール詐欺、DDoS 攻撃、Web 改ざん、フィッシング等の攻撃や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していただきたい。

索引

I

J

K

L

M

N

O

P

R

さ

た

な

は

ま

ら