

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



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。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観点からは、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せら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、その信頼性を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のように対応すればよいのでしょうか。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

序章 2021年度の情報セキュリティの概況	6
第1章 情報セキュリティインシデント・脆弱性の現状と対策	8
1.1 2021年度に観測されたインシデント状況	8
1.1.1 世界における情報セキュリティインシデント状況	8
1.1.2 国内における情報セキュリティインシデント状況	11
1.2 情報セキュリティインシデント別の手口と対策	16
1.2.1 標的型攻撃	16
1.2.2 ランサムウェア攻撃	21
1.2.3 ビジネスメール詐欺(BEC)	26
1.2.4 DDoS攻撃	31
1.2.5 ソフトウェアの脆弱性を悪用した攻撃	33
1.2.6 ばらまき型メールによる攻撃	36
1.2.7 個人をターゲットにした騙しの手口	39
1.2.8 情報漏えいによる被害	49
1.3 情報システムの脆弱性の動向	55
1.3.1 JVN iPediaの登録情報から見る脆弱性の傾向	55
1.3.2 早期警戒パートナーシップの届出状況から見る脆弱性の動向	59
第2章 情報セキュリティを支える基盤の動向	70
2.1 国内の情報セキュリティ政策の状況	70
2.1.1 政府全体の政策動向	70
2.1.2 経済産業省の政策	74
2.1.3 総務省の政策	81
2.1.4 警察によるサイバー犯罪対策	87
2.1.5 CRYPTRECの動向	91
2.2 国外の情報セキュリティ政策の状況	94
2.2.1 国際社会と連携した取り組み	94
2.2.2 アジア太平洋地域でのCSIRTの動向	98
2.3 情報セキュリティ人材の現状と育成	101
2.3.1 情報セキュリティ人材の状況	101
2.3.2 産業サイバーセキュリティセンター	105
2.3.3 情報セキュリティ人材育成のための国家試験、国家資格制度	107
2.3.4 情報セキュリティ人材育成のための活動	108
2.4 組織・個人における情報セキュリティの取り組み	112
2.4.1 企業等における対策状況	112
2.4.2 中小企業に向けた情報セキュリティ支援策	115
2.4.3 教育機関・政府及び地方公共団体等法人における対策状況	120
2.4.4 一般利用者における対策状況	123

2.5	情報セキュリティの普及啓発活動	127
2.5.1	ネットリテラシーの重要性	127
2.5.2	恒常的な啓発活動	129
2.5.3	インターネットがもたらす未来	131
2.6	国際標準化活動	133
2.6.1	様々な標準化団体の活動	133
2.6.2	情報セキュリティ、サイバーセキュリティ、プライバシー保護関係の規格の標準化 (ISO/IEC JTC 1/SC 27)	134
2.7	安全な政府調達に向けて	143
2.7.1	ITセキュリティ評価及び認証制度	143
2.7.2	暗号モジュール試験及び認証制度	146
2.7.3	政府情報システムのためのセキュリティ評価制度(ISMAP)	148
2.8	その他の情報セキュリティ動向	150
2.8.1	個人情報保護法改正	150
2.8.2	内部不正防止対策の動向	152
2.8.3	暗号技術の動向	155
第3章	個別テーマ	164
3.1	制御システムの情報セキュリティ	164
3.1.1	インシデントの発生状況と動向	164
3.1.2	脆弱性及び脅威の動向	167
3.1.3	海外の制御システムのセキュリティ強化の取り組み	169
3.1.4	国内の制御システムのセキュリティ強化の取り組み	171
3.2	IoTの情報セキュリティ	173
3.2.1	残存するIoTのセキュリティ脅威	173
3.2.2	サプライチェーンとEOLのリスク	177
3.2.3	脆弱なIoT機器とウイルス感染の実態	182
3.2.4	セキュリティ対策強化の取り組み	183
3.3	クラウドの情報セキュリティ	186
3.3.1	クラウドサービスの利用状況	186
3.3.2	クラウドサービスのインシデント被害	187
3.3.3	クラウドサービスのセキュリティの課題と対策	189
3.3.4	クラウドの情報セキュリティに対する政府の取り組み	193
3.4	米国・欧州の情報セキュリティ政策	195
3.4.1	米国の政策	195
3.4.2	欧州の政策	201

付録 資料・ツール	221
資料A 2021年のコンピュータウイルス届出状況	222
資料B 2021年のコンピュータ不正アクセス届出状況	223
資料C ソフトウェア等の脆弱性関連情報に関する届出状況	225
資料D 2021年の情報セキュリティ安心相談窓口の相談状況	228
IPAの便利なセキュリティツール	230
第17回IPA「ひろげよう情報モラル・セキュリティコンクール」2021受賞作品	234
索引	246

コラム

知ってる人は知っている、知らない人は多分ぜんぜん知らない 情報セキュリティの10大脅威	15
子どもへの情報リテラシー教育のために	54
多様化する「だまし」の手口に対抗するには	63
デジタル庁が進めるシステム検証とは?	93
高齢者層の情報セキュリティ	126
インターネット上の戦い	132
DXとセキュリティの相性は悪いのか	194
Disinformationの脅威とは	209



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
- **第1章** 情報セキュリティインシデント・脆弱性の現状と対策
 - 1.1 2021年度に観測されたインシデント状況
 - 1.2 情報セキュリティインシデント別の手口と対策
 - 1.3 情報システムの脆弱性の動向
- **第2章** 情報セキュリティを支える基盤の動向
 - 2.1 国内の情報セキュリティ政策の状況
 - 2.2 国外の情報セキュリティ政策の状況
 - 2.3 情報セキュリティ人材の現状と育成
 - 2.4 組織・個人における情報セキュリティの取り組み
 - 2.5 情報セキュリティの普及啓発活動
 - 2.6 国際標準化活動
 - 2.7 安全な政府調達に向けて
 - 2.8 その他の情報セキュリティ動向
- **第3章** 個別テーマ
 - 3.1 制御システムの情報セキュリティ
 - 3.2 IoTの情報セキュリティ
 - 3.3 クラウドの情報セキュリティ
 - 3.4 米国・欧州の情報セキュリティ政策

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月の医薬品メーカー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ーの工場が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・防衛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	<ul style="list-style-type: none"> ● 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) 	<ul style="list-style-type: none"> ■ 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	<ul style="list-style-type: none"> ● 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(3.4.1) 	<ul style="list-style-type: none"> ■ 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	<ul style="list-style-type: none"> ● 無線通信機器メーカー、2017 年に不正アクセス確認から 3 年以上報告せず(1.2.8) ● 電子部品メーカー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) 	<ul style="list-style-type: none"> ■ 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	<ul style="list-style-type: none"> ● 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) 	<ul style="list-style-type: none"> ■ 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	<ul style="list-style-type: none"> ● ProxyShell の脆弱性を公表(1.2.5) 	<ul style="list-style-type: none"> ■ 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		<ul style="list-style-type: none"> ■ 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	<ul style="list-style-type: none"> ● 徳島の町立病院でランサムウェアの被害発生(1.2.2) ● 医薬品メーカーの国内外の拠点に不正アクセス(1.2.8) 	<ul style="list-style-type: none"> ■ 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	<ul style="list-style-type: none"> ● 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) 	<ul style="list-style-type: none"> ■ NISC「クラウドを利用したシステム運用に関するガイドランス」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	<ul style="list-style-type: none"> ● ログインライブラリ 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) 	<ul style="list-style-type: none"> ■ 米 Biden 大統領が国防授權法に署名、アジア太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	<ul style="list-style-type: none"> ● 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	<ul style="list-style-type: none"> ● 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) 	<ul style="list-style-type: none"> ■ NIST「ソフトウェアサプライチェーンセキュリティガイドランス」、NIST SP800-218 Ver.1.1 公開(3.4.1)
3 月	<ul style="list-style-type: none"> ● 自動車部品会社がサイバー攻撃を受け、自動車メーカーが国内工場停止(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 万件的迷惑メール発信(3.3.2) 	<ul style="list-style-type: none"> ■ 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

A

- Active Directory サーバ…………… 24
- AIを用いたクラウドサービスの安全・信頼性に係る
情報開示指針(ASP・SaaS 編)…………… 192
- Apache HTTP Server の脆弱性…………… 58
- Apache Log4j の脆弱性……………10, 59
- APCERT(Asia Pacific Computer Emergency
Response Team : アジア太平洋コンピュータ緊
急対応チーム)……………98, 99
- APT40…………… 88
- Artificial Intelligence Act(AI 法)…………… 205
- ASEAN 地域フォーラム(ARF : ASEAN Regional
Forum)……………97
- ATT&CK…………… 170

B

- BadAlloc…………… 168, 178
- BadUSB 攻撃…………… 167
- BYOD(Bring Your Own Device)……………21, 85

C

- C&C(Command and Control)サーバ
……………16, 32, 82, 89, 173
- CCRA(Common Criteria Recognition
Arrangement)…………… 144
- CEO 詐欺…………… 30
- CISA Global…………… 169
- CISO(Chief Information Security Officer :
最高情報セキュリティ責任者)
……………98, 102, 106, 113,115
- CMS(Contents Management System)…………… 60
- CMVP(Cryptographic Module Validation
Program)……………146, 147
- CNA(CVE Numbering Authority)…………… 55
- Colonial Pipeline Company……………8, 165, 170, 195
- CRYPTREC…………… 91
- CSIRT(Computer Security Incident Response
Team)…………… 19, 30, 96, 98, 99, 171
- CVE(Common Vulnerabilities and Exposures :
共通脆弱性識別子)……………55, 168
- CYDER……………84, 85

- CYROP(CYDERANGE as an Open Platform)
……………85, 111
- CYNEX(Cybersecurity Nexus)……………85, 111

D

- DDoS 攻撃…………… 31, 174, 201
- Disinformation……………198, 205
- DX(デジタルトランスフォーメーション)
…………… 58, 70, 77, 83, 101, 112
- DX with Cybersecurity……………70, 101
- DX 時代における企業のプライバシーガバナンスガイ
ドブック…………… 77
- DX リテラシー標準…………… 105

E

- ECDSA…………… 91, 147, 156
- EdDSA…………… 91
- Emotet…………… 36, 79, 89, 98
- enPiT(Education Network for Practical
Information Technologies)…………… 109
- EO 14028…………… 170, 183, 196
- ERAB サイバーセキュリティトレーニング…………… 107
- EUCC scheme(Common Criteria based
European candidate cybersecurity
certification scheme)…………… 137, 185, 204
- EwDoor…………… 177
- e シール…………… 83
- e-ネットキャラバン……………71, 85

F

- FedRAMP(Federal Risk and Authorization
Management Program)…………… 196
- FragAttacks…………… 181

G

- G7 首脳会合・外相会合…………… 94
- GAFA…………… 199
- Gafgyt……………173, 175
- GDPR(General Data Protection Regulation :
一般データ保護規則)……………115, 151, 199, 206
- GIGA スクール構想…………… 71, 121, 128
- GIGA スクールにおけるセキュリティ実態調査 2021
…………… 128

GitHub52, 189

I

ICT サイバーセキュリティ総合対策 202181, 184

IEEE(The Institute of Electrical and
Electronics Engineers, Inc.) 134

IETF(Internet Engineering Task Force) 134

INFRA:HALT168, 179

IoT 32, 35, 81, 124, 137, 173

IoT・5G セキュリティ総合対策 2020 81

IoT-domotics 139

IoT セキュリティガイドライン 137

IoT セキュリティ・セーフティ・フレームワーク
(IoT-SSF) 75

ISMAP 管理基準 148

ISMAP クラウドサービスリスト72, 148

ISO/IEC 27000 ファミリー135, 136

ISO/IEC JTC 1/SC 27 74, 134

ISP(Internet Services Provider)33, 84, 89

ITSS+ 102

ITU-T(International Telecommunication Union
Telecommunication Standardization Sector :
国際電気通信連合 電気通信標準化部門) 134

IT 製品の調達におけるセキュリティ要件リスト 143

IT セキュリティ評価及び認証制度
(JISEC : Japan Information Technology
Security Evaluation and Certification
Scheme)143, 146

J

J-CRAT(Cyber Rescue and Advice Team
against targeted attack of Japan :
サイバーレスキュー隊) 80

Joint Cyber Defense Collaborative(JCDC)
..... 170

JVN iPedia35, 55

K

KOSEN Security Educational Community
(K-SEC) 111

L

LeetHozer 174

Log4Shell 168

M

Matryosh 174

Mēris 32

Microsoft Exchange Server 8, 34, 195

Microsoft Windows 11 の脆弱性 57

Mirai32, 173

Mirai の亜種174, 175

Moobot 174

Mozi 176

N

NAME:WRECK 35, 168, 178

Necro 175, 176

NICTER(Network Incident analysis Center for
Tactical Emergency Response)84, 85, 183

NIS 指令(NIS Directive) 203

NOTICE(National Operation Towards IoT
Clean Environment)84, 182

NUCLEUS:13 169, 181

NUMBER:JACK 177

NVD(National Vulnerability Database) 55

O

OSS の利活用及びそのセキュリティ確保に向けた
管理手法に関する事例集75, 193

P

PIMS(Privacy Information Management
System : プライバシー情報マネジメントシステム)
..... 141

PowerShell21, 167

ProxyLogon8, 34, 195

ProxyShell 8, 34

Pulse Secure, LLC. 34

R

RaaS(Ransomware as a Service) 196

Ransom Disclosure Act 196

Rising Ransomware Threat to Operational
Technology Assets 169

S	
SaaS	9, 186
SCADA(Supervisory Control And Data Acquisition : 監視制御及びデータ収集)システム	164
SECCON	110
SECURITY ACTION	119
SHIELDS UP	198
SMS(Short Message Service)	39, 41, 89
SMS 認証代行	90
Society 5.0	71
Software Bill of Materials (SBOM : ソフトウェア部品表)	75, 193
SolarWinds Worldwide, LLC	9, 195
SQL インジェクション	34, 50, 62, 169
T	
TCG(Trusted Computing Group)	133
Tor(The Onion Router)	174, 175
U	
Ursnif	79
V	
VPN	14, 16, 22, 33, 73, 116
VPNFilter	173
W	
WannaCry	21
Web 会議	85, 108, 187
Web サイト改ざん	11, 59
Wi-Fi 提供者向けセキュリティ対策の手引き	86
Wi-Fi 利用者向け簡易マニュアル	86
Windows	22, 24, 45, 57, 176
Z	
ZHtrap	174
あ	
アイデンティティ管理	141
アグリゲーション攻撃(aggregation attack)	181
アプリ誘導	46

暗号鍵管理システム設計指針(基本編)	91, 92
暗号資産	16, 42, 176, 196
暗号モジュール試験及び認証制度(JCMVP : Japan Cryptographic Module Validation Program)	146
安心相談窓口	39, 45
一般財団法人日本サイバー犯罪対策センター (JC3 : Japan Cybercrime Control Center)	13, 89
インターネットトラブル事例集(2021 年度版)	71
インド太平洋地域向け日米 EU 産業制御システムサイバーセキュリティウィーク	97, 105
インド太平洋に関する ASEAN アウトルック(AOIP : ASEAN Outlook on the Indo-Pacific)	95, 97
インフォデミック	205
ウクライナ侵攻	94, 195, 199
営業秘密	52, 152
エクспロイトキット	24
エネルギー・リソース・アグリゲーション・ビジネスに関するサイバーセキュリティガイドライン	107
遠隔操作ウイルス(RAT : Remote Access Trojan)	16
欧州民主主義行動計画(European Democracy Action Plan)	205
オープンソースソフトウェア	58, 75, 191
オンラインゲーム	130
オンライン授業	128, 136
か	
各府省情報化統括責任者(CIO)連絡会議	146
叶会	106
ガバメントクラウド	72, 86
機器乗っ取り型ウイルス	173
機器破壊型ウイルス	173
機器保護型ウイルス	173
技術等情報管理認証制度	77
教育情報セキュリティポリシーに関するガイドライン	121
教育ネットワーク情報セキュリティ推進委員会 (ISEN : Information Security for Education Network)	120
業界別サイバーレジリエンス強化演習(CyberREX)	106

共通鍵暗号	155	サイバー情報共有イニシアティブ (J-CSIP : Initiative for Cyber Security Information Sharing Partnership of Japan)	27, 78
共通脆弱性タイプ一覧(CWE : Common Weakness Enumeration)	55	サイバーセキュリティ 2021	70, 152, 171
共通脆弱性評価システム(CVSS : Common Vulnerability Scoring System)	8, 56	サイバーセキュリティお助け隊サービス	71, 118
緊急事態宣言	37, 187	サイバーセキュリティお助け隊サービス基準	76, 118
組み込み機器	35, 181	サイバーセキュリティ関係法令 Q & A ハンドブック	154
クラウドサービス	17, 39, 121, 143, 148, 186	サイバーセキュリティ経営ガイドライン	70, 75, 114
クラウドサービス提供における情報セキュリティ対策 ガイドライン	84, 191, 193	サイバーセキュリティ経営ガイドライン Ver2.0 実践の ためのプラクティス集	70, 75
クラウドサービスの安全・信頼性に係る情報開示指 針	192, 193	サイバーセキュリティ経営可視化ツール	70, 76, 114
クラウドサービスの安全性評価に関する検討会	148	サイバーセキュリティ経営戦略コース	110
クラウドサービスの安全性評価に関する検討会とりま とめ	148, 149	サイバーセキュリティ国際シンポジウム	97
クラウド・バイ・デフォルト原則	148	サイバーセキュリティ重点施策	87
クラウドを利用したシステム運用に関するガイダンス	71, 193	サイバーセキュリティ戦略	70, 73, 101, 171, 193
グループ・ガバナンス・システムに関する実務指針	70	サイバーセキュリティ体制構築・人材確保の手引き	76, 77, 102
クレジットカード	13, 40, 50, 60, 89, 129	サイバーフィジカルシステム (CPS : Cyber Physical System)	71, 140
クロスサイト・スクリプティング	51, 55, 60	サイバー・フィジカル・セキュリティ対策基盤	71
警察におけるサイバーセキュリティ戦略	87	サイバー・フィジカル・セキュリティ対策フレームワーク (CPSF : The Cyber/Physical Security Framework)	74, 140
公開鍵暗号	92, 155	サブスクリプション詐欺	47
攻撃対象領域	25	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 : Supply Chain Cybersecurity Consortium)	76, 118
公表判定委員会	59, 61	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 (NIICS : National Initiative for Improving Cybersecurity in Supply Chains)	197
小売電気事業者のためのサイバーセキュリティ対策 ガイドライン Ver.1.0	75	サプライチェーンリスク	73, 153, 177, 195
国際標準化活動	133	サポート詐欺	45
国立研究開発法人情報通信研究機構(NICT : National Institute of Information and Communications Technology)	73, 84, 91, 111, 182	産学情報セキュリティ人材育成交流会	110
個人情報保護法	82, 150	産業競争力強化法等の一部を改正する法律	77
個人情報保護法制 2000 個問題	151	産業サイバーセキュリティ研究会	74
コモンクライテリア(共通基準)	143, 204	産業サイバーセキュリティセンター	105, 171
コラボレーション・プラットフォーム	77	三層の対策	86
混合キー攻撃(mixed key attack)	181	自工会／部工会・サイバーセキュリティガイドライン 2.0 版	75
さ		自治体情報セキュリティクラウド	86, 189
サイドチャネル攻撃	155		
サイバー・イニシアチブ東京 2021	97		
サイバー危機対応机上演習(CyberCREST)	106		

シャドー IT	85, 189	セキュリティ・キャンプ	108
重要 10 項目	75, 114	セキュリティガバナンス	205
重要インフラにおける情報セキュリティ確保に係る		セキュリティ・バイ・デザイン	83
安全基準等策定指針	149	ゼロデイ脆弱性	35, 175
情報処理安全確保支援士(登録セキスペ)	107	ゼロトラストアーキテクチャ	72, 196
情報セキュリティサービス基準	77	戦略マネジメント系セミナー	106
情報セキュリティサービス基準適合サービスリスト	78	ソーシャルエンジニアリング	18
情報セキュリティサービス審査登録制度	71, 77	組織における内部不正防止ガイドライン	53, 152
情報セキュリティサービスに関する審査登録機関基 準	77		
情報セキュリティサービス普及促進に関する検討会	71	た	
情報セキュリティ早期警戒パートナーシップ	59	ダーク Web	24, 87, 166, 192
情報セキュリティマネジメント試験	107	耐量子計算機暗号	
情報セキュリティマネジメントシステム(ISMS : Information Security Management System)	135, 192	(PQC : Post-Quantum Cryptography)	91, 155
情報漏えい	9, 20, 49, 52, 120, 153	地域 SECURITY	76, 118
新型コロナウイルス	14, 21, 27, 37, 44, 83, 129, 202	チート行為	130
侵入型ランサムウェア攻撃	21, 23, 25, 26	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	85
スマートカード	143, 204	中核人材育成プログラム	105, 172
スマートシティセキュリティガイドライン(第 2.0 版)	84	中小企業等担当者向けテレワークセキュリティの手 引き(チェックリスト)	83
スマートホームの安心・安全に向けたサイバー・フィ ジカル・セキュリティ対策ガイドライン Ver1.0	75	テイクダウン	36, 89, 173
制御・運用技術(OT : Operational Technology)	164	データ利活用	77, 150
制御システム(ICS : Industrial Control System)	164	デジタルサービス法(DSA : Digital Services Act)	205
制御システムのセキュリティリスク分析ガイド	171	デジタル市場法(DMA : Digital Markets Act)	205
制御システム向けサイバーセキュリティ演習	107	デジタル社会の実現に向けた重点計画	86, 121
脆弱性	8, 16, 24, 33, 55, 126, 136	デジタル人材育成プラットフォーム	76, 104
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	72, 143	デジタル庁	72, 82, 91, 121, 149
政府機関等のサイバーセキュリティ対策のための 統一基準群	85	デジュール標準(de jure standard)	133
政府機関等の対策基準策定のためのガイドライン	72, 78, 146	デファクト標準(de facto standard)	133
政府情報システムのためのセキュリティ評価制度 (Information system Security Management and Assessment Program : 通称、ISMAP (イスマップ))	72, 78, 143, 148, 192	テレワーク	14, 18, 21, 33, 52, 58, 153
		テレワークセキュリティガイドライン	83
		電気通信事業における個人情報保護に関する ガイドライン	87
		電気通信事業法に基づく端末機器の基準認証に 関するガイドライン	84
		電子署名	31, 83, 146, 155
		東京 2020 オリンピック・パラリンピック競技大会	32, 88, 95
		東商サイバーセキュリティコンソーシアム	119
		特定非営利活動法人日本ネットワークセキュリティ協 会(JNSA : Japan Network Security	

Association)	110
ドメインコントローラ	23, 24
ドライブ・バイ・ダウンロード攻撃	16
トラストサービス	83
トラストサービス検討ワーキンググループ	83

な

内閣サイバーセキュリティセンター(NISC : National center of Incident readiness and Strategy for Cybersecurity)	22, 51, 70, 131, 149, 171, 188, 193
内部不正	52, 152
なりすまし	27, 31, 83
二重恐喝	13
二重の脅迫	13, 22
偽警告	45
偽セキュリティソフト	45
偽のセキュリティ警告	45
日・ASEAN サイバーセキュリティ政策会議	97
日 ASEAN 首脳会議	96
日 EU 定期首脳協議	96
日英サイバー協議	96
日エストニア・サイバー協議	96
日米安全保障協議委員会	96
日米豪印首脳会合	95
日米首脳会談	96
ニューノーマル	153

は

バイオメトリクス	142
パスワード設定	124
ハニーポット	174
ばらまき型メール	21, 24, 36, 38, 79
ビジネスメール詐欺(BEC : Business Email Compromise)	26, 30, 79, 125
ビッグデータ	139
人手によるランサムウェア攻撃	21
標的型攻撃	16, 34, 78, 125, 195
標的型サイバー攻撃特別相談窓口	80
ファイルの誤った公開	62
ファイルレスマルウェア	16, 21
フィッシング	9, 11, 26, 31, 125
フェイクニュース	199, 205
フォーラム標準(forum standard)	133

不正アクセス	11, 17, 23, 31, 49, 107, 188
不正アプリ	24, 25, 128
不正送金	12, 73, 89
プラクティス・ナビ	76
フラグメントキャッシュ攻撃 (fragment cache attack)	181
プラス・セキュリティ	70, 76, 101
プラットフォームサービスに関する研究会	83
ふるまい検知	122, 154
プロテクションプロファイル	144, 146, 147
米国国立標準技術研究所(NIST : National Institute of Standards and Technology)	55, 133, 146, 155, 170, 195
ベストレポーター賞	61
ボットネット	32, 36, 175

ま

マクロ機能	38
マナビ DX(デラックス)	105
みんなで使おうサイバーセキュリティ・ポータルサイト	71

ら

ランサムウェア	8, 9, 13, 21, 123, 165, 171, 177
リフレクション攻撃	32
リモートデスクトップサービス	22, 23, 25
ローカル 5G	82
ロックダウン	31, 94, 202