

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



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の安全で合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 齊藤 裕

序章 2022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 2022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の発生状況	8
1.1.2 国内における情報セキュリティインシデントの発生状況	10
1.2 情報セキュリティインシデント、手口、対策	15
1.2.1 ランサムウェア攻撃	15
1.2.2 標的型攻撃	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	34
1.2.6 ばらまき型メールによる攻撃	36
1.2.7 個人を狙うSMS・SNS・メールを悪用した手口	40
1.2.8 個人を狙う様々な騙しと悪用の手口	45
1.2.9 情報漏えいによる被害	51
1.3 情報システムの脆弱性の動向	56
1.3.1 JVN iPediaの登録情報から見る脆弱性の傾向	56
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	60
第2章 情報セキュリティを支える基盤の動向	72
2.1 国内の情報セキュリティ政策の状況	72
2.1.1 政府全体の政策動向	72
2.1.2 デジタル庁の政策	76
2.1.3 経済産業省の政策	79
2.1.4 総務省の政策	87
2.1.5 警察によるサイバー犯罪対策	90
2.1.6 CRYPTRECの動向	95
2.2 国外の情報セキュリティ政策の状況	97
2.2.1 国際社会と連携した取り組み	97
2.2.2 米国の政策	101
2.2.3 欧州の政策	107
2.2.4 アジア太平洋地域でのCSIRTの動向	112
2.3 情報セキュリティ人材の現状と育成	116
2.3.1 デジタル人材としての情報セキュリティ人材育成	116
2.3.2 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	120
2.3.3 情報セキュリティ人材育成のための活動	121
2.4 組織・個人における情報セキュリティの取り組み	128
2.4.1 企業・組織における対策状況	128
2.4.2 中小企業に向けた情報セキュリティ支援策	130
2.4.3 公共機関における対策状況	134
2.4.4 一般利用者における対策状況	138

2.5	情報セキュリティの普及啓発活動	144
2.5.1	不適切事例とネットリテラシーの必要性	144
2.5.2	恒常的な啓発活動	146
2.5.3	誰一人取り残されないデジタル化に向けて	148
2.6	国際標準化活動	150
2.6.1	様々な標準化団体の活動	150
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)	151
2.7	安全な政府調達に向けて	160
2.7.1	ITセキュリティ評価及び認証制度	160
2.7.2	暗号モジュール試験及び認証制度	163
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)	164
2.8	その他の情報セキュリティ動向	167
2.8.1	内部不正防止対策の動向	167
2.8.2	暗号技術の動向	169
第3章	個別テーマ	182
3.1	制御システムの情報セキュリティ	182
3.1.1	インシデントの発生状況と動向	182
3.1.2	脆弱性及び脅威の動向	185
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	186
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	188
3.2	IoTの情報セキュリティ	190
3.2.1	IoTに対するセキュリティ脅威の動向	190
3.2.2	進化の止まらないIoTウイルスの動向	194
3.2.3	IoTセキュリティのサプライチェーンとEOLのリスク	196
3.2.4	脆弱なIoT機器のウイルス感染と感染機器悪用の実態	198
3.2.5	各国のセキュリティ対策強化の取り組み	201
3.3	クラウドの情報セキュリティ	204
3.3.1	クラウドサービスの利用状況	204
3.3.2	クラウドサービスのインシデント事例	205
3.3.3	クラウドサービスのセキュリティの課題と対策	207
3.3.4	クラウドサービスの情報セキュリティに対する政府・関連団体の取り組み	211
3.4	虚偽情報拡散の脅威と対策の状況	214
3.4.1	虚偽情報とは	214
3.4.2	虚偽情報生成・拡散の事例	215
3.4.3	虚偽情報生成・拡散の流れ	219
3.4.4	日本国内の状況	220
3.4.5	虚偽情報の対応状況	221
3.4.6	まとめと今後の見通し	223

付録 資料	233
資料A 2022年のコンピュータウイルス届出状況	234
資料B 2022年のコンピュータ不正アクセス届出状況	235
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	237
資料D 2022年の情報セキュリティ安心相談窓口の相談状況	240
第18回IPA「ひろげよう情報モラル・セキュリティコンクール」2022受賞作品	242
IPAの便利なツールとコンテンツ	244
索引	249

コラム

情報セキュリティ10大脅威 2023 ～全部担当のせいとせず、組織的にセキュリティ対策の足固めを～	14
便利な技術は悪用される	55
CODE BLUEが挑戦してきた、日本のサイバーセキュリティの多様性とエコシステム	65
インターネットに投稿するということは	149
情報セキュリティポリシー見直しのススメ ～「とりあえずセキュリティ」からの脱却～	203



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
- **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 2022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、手口、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 虚偽情報拡散の脅威と対策の状況

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 の安全で合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)	<ul style="list-style-type: none"> 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		<ul style="list-style-type: none"> 「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	<ul style="list-style-type: none"> 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) 	<ul style="list-style-type: none"> 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		<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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) 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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) 	<ul style="list-style-type: none"> 米国、「AI権利章典」公開(2.2.3)
11月	<ul style="list-style-type: none"> 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) 	<ul style="list-style-type: none"> 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)	<ul style="list-style-type: none"> 安全保障関連3文書が閣議決定(2.1.1) 米国、国防授權法2023成立(2.2.2)
2023年 1月	<ul style="list-style-type: none"> 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) 	<ul style="list-style-type: none"> 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		<ul style="list-style-type: none"> 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)	<ul style="list-style-type: none"> 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

A

Access:7 185, 196
Active Directory 20, 24
AI 権利章典(AI Bill of Rights) 111, 223
Apache Log4J 35, 104, 195
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) 114
Artificial Intelligence Act(AI 法) 110
ASEAN 地域フォーラム(ARF : ASEAN Regional
Forum) 101

B

B1txor20 195
BlackTech 22
BYOD(Bring Your Own Device) 26

C

C&C(Command and Control) サーバー
..... 21, 32, 93, 191, 194
CCRA(Common Criteria Recognition
Arrangement) 153, 160
CEO 詐欺 30
Chaos 196
CISO(Chief Information Security Officer : 最高
情報セキュリティ責任者) 124, 127, 128
CMVP(Cryptographic Module Validation
Program) 163
CNA(CVE Numbering Authority) 56, 62
CRYPTREC 95
CSIRT(Computer Security Incident Response
Team) 24, 112, 129, 188
CSO ワークショップ 150
CVE(Common Vulnerabilities and Exposures :
共通識別子) 56, 62, 185
Cyclops Blink 191
CYDER サテライト 89
CYNEX(Cybersecurity Nexus) 75, 88, 125
CYROP(CYDERANGE as an Open Platform)
..... 125

D

DDoS Extortion 31
DDoS 攻撃 9, 18, 31, 195, 199
DeadBolt 190
Disinformation 110, 214
DX(デジタルトランスフォーメーション)
..... 76, 116, 127, 137
DX with Cybersecurity 116
DX 推進スキル標準 116
DX リテラシー標準 116

E

Earth Yako 22
ECDSA 170
EC サイト構築・運用セキュリティガイドライン 134
Emotet 36, 85, 93
EnemyBot 194
enPiT(Education Network for Practical
Information Technologies) 123
EO 14028 101
ERAB サイバーセキュリティトレーニング 127
EUCC scheme(Common Criteria based
European candidate cybersecurity
certification scheme) 108
Evil PLC 185

F

FedRAMP(Federal Risk and Authorization
Management Program) 104
Fodcha 195

G

G7 首脳会合 97
Gafgyt 194
GDPR(General Data Protection Regulation :
一般データ保護規則) 109, 111
GIGA スクール構想 74, 137, 146
GIGA ワークブック 146
GitHub 192

H

HTML Smuggling 39

I

ICT サイバーセキュリティ総合対策 2022	87
IEEE(The Institute of Electrical and Electronics Engineers, Inc.)	151
IETF(Internet Engineering Task Force)	151
Industroyer2	186
IoT	32, 87, 108, 154, 190
IoT-domotics	156
IoT セキュリティガイドライン	155
IoT セキュリティ・セーフティ・フレームワーク(IoT-SSF)	81
IRM(Information Rights Management)	20
(ISC) ² Cybersecurity Workforce Study 2022	116
ISMAP-LIU(イスマップ・エルアイユー: ISMAP for Low-Impact Use)	165, 212
ISMAP-LIU クラウドサービス登録規則	212
ISMAP 管理基準	165
ISMAP クラウドサービスリスト	165
ISO/IEC 27000 ファミリー	152
ISO/IEC JTC 1/SC 27	151
ISP(Internet Services Provider)	33, 87, 198
ITSS+	116
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)	151
IT 製品の調達におけるセキュリティ要件リスト	160
IT セキュリティ評価及び認証制度(JISEC: Japan Information Technology Security Evaluation and Certification Scheme)	160, 164

J

J-CRAT(Cyber Rescue and Advice Team against targeted attack of Japan: サイバーレスキュー隊)	22, 85
JVN iPedia	56

K

KOSEN Security Educational Community (K-SEC)	124
----------------------------------------------	-----

L

Lattice Attack	170
LODEINFO	22
Log4Shell	35

M

Malinformation	214
Mantis	33
MCCrash	200
Mëris	33
Microsoft Exchange Server の脆弱性	59
Microsoft Support Diagnostic Tool(MSDT)の脆弱性	34
Mirai	33, 36, 191
Mirai の亜種	191, 194, 199
Misinformation	214
Moobot	191
Mozi	199, 200

N

NICTER(Network Incident analysis Center for Tactical Emergency Response)	88, 199
NIS 2	108, 187
NIS 指令(Network and Information Systems Directive)	108, 187
Nord Stream 2	107, 112
NOTICE(National Operation Towards IoT Clean Environment)	87, 198
NVD(National Vulnerability Database)	56

O

Op.EneLink	22
Operation Killer Bee	27
OT:ICEFALL	185

P

persistent fault injection analysis	170
PIMS(Privacy Information Management System: プライバシー情報マネジメントシステム)	159
Pipedream/Incontroller	186
PowerShell	26

ProxyNotShell 59

R

R4IoT 200

RaaS (Ransomware as a Service) 15

RapperBot 194

RobbinHood 16

RSOCKS 202

S

SaaS 165, 204

SCADA (Supervisory Control And Data Acquisition) 183, 186

SECCON 123

SecHack365 122

SECURITY ACTION 133

SHIELDS UP 105

Shikitega 196

SLA (Service Level Agreement : サービス品質保証) 208

SMS (Short Message Service) 11, 40, 94, 192

Software Bill of Materials (SBOM : ソフトウェア部品表) 36, 80

Spring Framework の脆弱性 35, 194

Spring4Shell 35, 194

SQL インジェクション 63

STOP. THINK. CONNECT. 50

T

TCG (Trusted Computing Group) 151

Telegram 32, 218

Tor (The Onion Router) 194

V

VPN 12, 16, 17, 31, 34, 60, 182

W

Web サイト改ざん 11, 60

WhisperGate 9, 105

Windows 18, 35, 38, 47, 59, 196, 200

Z

ZouRAT 192

あ

アイデンティティ管理 159

暗号鍵管理システム設計指針 (基本編) 95

暗号資産 26, 36, 92, 94, 144, 196

暗号モジュール試験及び認証制度 (JCMVP : Japan Cryptographic Module Validation Program) 163

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) 50, 91, 94

医療情報システムの安全管理に関するガイドライン 74, 184

インターネットトラブル事例集 2022 年版 147

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 101, 188

インド太平洋に関する ASEAN アウトルック (AOIP : ASEAN Outlook on the Indo-Pacific) 101

インフォデミック 216

ウクライナ侵攻 9, 32, 97, 182, 190, 214

営業秘密 54, 167

エクスプロイト 194

エコーチェンバー現象 220, 223

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 127

遠隔操作アプリ 49

遠隔操作ウイルス (RAT : Remote Access Trojan) 21

オープンソースソフトウェア (OSS : Open Source Software) 22, 24, 81

オンラインゲーム 31, 94

か

各府省情報化統括責任者 (CIO) 連絡会議 165

叶会 126

ガバメントクラウド 137

機器乗っ取り型ウイルス 199

技術情報管理認証制度 83

教育情報セキュリティポリシーに関するガイドライン 74, 137

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) 135

業界別サイバーレジリエンス強化演習(CyberREX : Cyber Resilience Enhancement eXercise by industry)	127	サイドチャンネル攻撃	163, 169
共通鍵暗号	169	サイバー危機対応机上演習(CyberCREST : Cyber Crisis RESponse Table top exercise)	126
共通脆弱性タイプ一覧(CWE : Common Weakness Enumeration)	56	サイバー警察局	90
共通脆弱性評価システム(CVSS : Common Vulnerability Scoring System)	57, 185	サイバー攻撃被害に係る情報の共有・公表ガイダンス	73
クラウドサービス	31, 52, 72, 138, 165, 204	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, 84
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	207, 212	サイバーセキュリティ2022	72, 188
クラウドサービスの安全・信頼性に係る情報開示指 針	208	サイバーセキュリティ意識・行動強化プログラム	75
クラウドサービスの安全性評価に関する検討会	165	サイバーセキュリティお助け隊サービス	134
クラウドサービス利用・提供における適切な設定のた めのガイドライン	212	サイバーセキュリティお助け隊サービス基準	134
クラウド・バイ・デフォルト原則	165	サイバーセキュリティ経営ガイドライン	72, 75, 81, 129
クレジットカード	11, 43, 51, 60, 83, 93	サイバーセキュリティ経営可視化ツール	82, 129
クロスサイト・スクリプティング	57, 63	サイバーセキュリティ経営戦略コース	124
経済安全保障推進法	75, 188	サイバーセキュリティ戦略	72, 75, 87, 116, 188
公開鍵暗号	96, 169	サイバーセキュリティ体制構築・人材確保の手引き	116, 129
攻撃対象領域(アタックサーフェス)	19	サイバー特別捜査隊	90
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 Ver1.0	81, 188	サイバーフィジカルシステム(CPS : Cyber Physical System)	158
国際銀行間通信協会(SWIFT : Society for Worldwide Interbank Financial Telecommunication)	112	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)	80, 158
国際標準化活動	150	サイバーレジリエンス	25, 77, 108
国立研究開発法人情報通信研究機構(NICT : National Institute of Information and Communications Technology)	87, 95, 122, 125, 198	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)	72, 118, 132
故障利用攻撃(fault injection analysis)	170	サプライチェーンリスク	99, 102, 132, 196, 208
個人情報保護委員会	52, 206, 208	サポート詐欺	45
「個人情報の保護に関する法律についてのガイドラ イン」に関する Q&A	208	産学情報セキュリティ人材育成交流会	124
個人情報保護法	167, 208	産業競争力強化法等の一部を改正する法律	83
コネクテッドカー	192	産業サイバーセキュリティ研究会	80, 201
コモンクライテリア(共通基準)	153, 160	産業サイバーセキュリティセンター(ICSCoE : Industrial Cyber Security Center of Excellence)	125, 188
コラボレーション・プラットフォーム	82	事業継続計画(BCP : Business Continuity Plan)	19
さ		実践的サイバー防御演習(CYDER : Cyber Defense Exercise with Recurrence)	72, 89
サイバーフォースセンター	90		

自由で開かれたインド太平洋	97	レームワーク導入に関する技術レポート	79
重要 10 項目	130	政府情報システムにおける脆弱性診断導入ガイドライン	78
重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書	74	政府情報システムにおけるセキュリティ・バイ・デザインガイドライン	77
重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針	74, 166	政府情報システムにおけるセキュリティリスク分析ガイドライン	78
重要インフラのサイバーセキュリティに係る行動計画	74, 188	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))	164
常時リスク診断・対処(CRSA)システムアーキテクチャ	77	セキュリティ・キャンプ	121
情報処理安全確保支援士(登録セキスベ)	121, 127	セキュリティ統制のカatalog化に関する技術レポート	79
情報セキュリティ安心相談窓口	36, 40, 45, 49	セキュリティ・バイ・デザイン	77
情報セキュリティサービス基準	82	ゼロデイ脆弱性	190, 193, 194, 198
情報セキュリティサービス基準適合サービスリスト	83	ゼロトラストアーキテクチャ	74, 76, 77, 79, 105
情報セキュリティサービス審査登録制度	73, 82, 83	ゼロトラストアーキテクチャ適用方針	77
情報セキュリティサービスに関する審査登録機関基準	83	戦略マネジメント系セミナー	127
情報セキュリティ早期警戒パートナーシップ	60	ソーシャルエンジニアリング	23
情報セキュリティマネジメント試験	120	組織における内部不正防止ガイドライン	54, 167
情報セキュリティマネジメントシステム (ISMS : Information Security Management System)	152, 212		
情報漏えい	10, 51, 72, 135, 167, 206	た	
新型コロナウイルス	22, 42, 45, 64, 85, 108, 216	ダークウェブ	18, 93
侵入型ランサムウェア攻撃	15	大西洋横断データプライバシーフレームワーク	111
スマートカード	154, 160, 162	大統領令 14028	101
制御・運用技術 (OT : Operational Technology)	125, 182	耐量子計算機暗号	95, 153, 170
制御システム (ICS : Industrial Control System)	182	地域 SECURITY	72, 82, 133
制御システムのセキュリティリスク分析ガイド	189	中核人材育成プログラム	125
制御システム向けサイバーセキュリティ演習 (CyberSTIX : Cyber Security practical eXercise for industrial control system)	127	中小企業の情報セキュリティ対策ガイドライン	75, 133, 211
脆弱性	19, 22, 25, 34, 56, 77, 92, 104, 185	テイクダウン	93, 194
生成系 AI	214, 220, 223	データガバナンス法 (Data Governance Act)	109
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	74, 160	デジタルサービス法 (DSA : Digital Services Act)	109, 222
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	77	デジタル市場法 (DMA : Digital Markets Act)	109
政府機関等の対策基準策定のためのガイドライン	83, 163	デジタル社会の実現に向けた重点計画	73, 79, 137, 212
政府情報システムにおけるサイバーセキュリティフ		デジタル人材育成プラットフォーム	116, 120
		デジタルスキル標準	116, 120
		デジタル庁	76
		デジタル田園都市国家構想	116
		デジュール標準 (de jure standard)	150
		デファクト標準 (de facto standard)	150

出前 CYDER	89
テレワーク	15, 34, 133, 167
電子署名	163
東京 2020 オリンピック・パラリンピック競技大会	87, 89
ドメインコントローラー	18, 20, 200

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)	23, 73, 147, 188
内部不正	54, 167
ナラティブ (Narrative)	214
なりすまし	27, 40, 183, 216
二重恐喝	12, 92
二重の脅迫	15, 18
偽 EC サイト	49
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	74, 101
日 ASEAN 首脳会議	101
日 EU 定期首脳協議	100
日英サイバー協議	100
日米安全保障協議委員会	99
日米豪印 (QUAD : Quadrilateral Security Dialogue) 首脳会合	74, 98
日米首脳会談	99
ニューノーマル	167
ネット・スマホのある時代の子育て (乳幼児編)	147

は

パートナーシップ構築宣言	133
バイオメトリクス	159
パスワード設定	87, 141
ばらまき型メール	36, 85
万博向けサイバー防御演習 (CIDLE)	90
ビジネスメール詐欺 (BEC : Business Email Compromise)	26, 85
ビッグデータ	157
標的型攻撃	21, 59, 84, 200
標的型サイバー攻撃特別相談窓口	86
ビル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	81
ファイルレスマルウェア	21, 26
ファクトチェック	145, 215, 221

フィッシング	9, 11, 26, 31, 40, 85, 94
フェイクニュース	214, 220
フォーラム標準 (forum standard)	150
不正アクセス	11, 23, 31, 51, 93
不正送金	11, 94
プラス・セキュリティ	72, 75, 116
プラットフォームサービスに関する研究会	220, 222
プロテクションプロファイル (PP : Protection Profile)	154, 161, 164
米国国立標準技術研究所 (NIST : National Institute of Standards and Technology)	56, 79, 101, 153, 155, 163, 186
ボットネット	32, 36, 190, 194, 199, 202

ま

マイクロターゲティング	216, 220
マクロ	37, 59
マナビ DX (マナビ・デラックス)	116
民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン Ver1.0	81

ら

ランサムウェア	9, 12, 15, 92, 104, 109, 183, 186, 190, 205
リフレクション攻撃	32, 88
リモートデスクトップサービス	16, 200
ロックダウン	107

わ

ワイパー型ウイルス	9, 184, 186
-----------	-------------