標準化で、世界をつなげる。
JSAGROUP
日本規格協会グループ SINCE 1945

経済産業省
Ministry of Economy, Trade and Industry

経済産業省　基準認証政策課　御中

海外標準化動向調査（9月）

令和6年度エネルギー需給構造高度化基準認証推進事業費（我が国の国際標準化戦略を強化するための体制構築）
2024年9月1日

一般財団法人日本規格協会

ピックアップ：サイバーセキュリティ （関連ニュース番号11）

トピック	ゼロトラスト、先端航空交通セキュリティなどのサイバーセキュリティに関する国際標準を韓国が主導
推進組織	**韓国科学技術情報通信部、国際電気通信連合電気通信標準化部門(ITU-T)情報保護研究委員(SG17)**

内容

ポイント

ITU-Tおよび世界標準化機構初のゼロトラストセキュリティに対する新規標準化提案を、韓国主導で米国、英国、中国などの協力のもと採択にこぎつけた。
韓国にとって、サイバーセキュリティ分野での国際標準化における大きな成果であり、韓国はさらにこの分野で、国際協力を得て国際標準化活動をリードする意向。

背景

韓国は2023年8月に、韓国の一山キンテックスで開催された前回のSG17国際会議で、ゼロトラスト、ソフトウェアサプライチェーンセキュリティ、人工知能セキュリティなど次世代標準化 テーマに対するグローバルレベルでの同意を取り付けており、今回の国際会議はそのフォローアップ。全世界で330人の専門家が参加する中、韓国は50人余りが参加。

概要

- 韓国は、2024年2月20日から3月1日までスイスジュネーブで開催された国際電気通信連合電気通信標準化部門(ITU-T)情報保護研究委員会(SG17)の国際会議で、ゼロトラストセキュリティ、先端航空交通データセキュリティなどの9件の案件が新規標準課題として承認され、車両用 エッジコンピューティングセキュリティなど計6件の標準化承認成果(事前採択2件、最終承認4件、※1)があったと明らかにした。韓国は2023年8月に、韓国の一山キンテックスで開催された前回のSG17国際会議で、ゼロトラスト、ソフトウェアサプライチェーンセキュリティ、人工知能セキュリティなど次世代標準化テーマに対するグローバル合意を取り付けており、これに対するフォローアップとして、今回のSG17国際会議で、米国との緊密な協力も通じて、ゼロトラストセキュリティに関する標準課題を含む9件の新規標準課題提案を行い、すべて承認される成果を得たもの。
  （※1） ITU-Tの標準化過程は、新規標準課題承認→標準開発→標準事前採択→ITU-T加盟国回覧→標準最終承認(ITU-T)などの手続きを経る。
- 今回の国際会議には、全世界55の加盟国から330人余りの専門家(オンライン・オフライン並行)が参加する中、韓国は50人余りの多数の専門家が参加し、国内のサイバーセキュリティ技術を 国際標準に反映させるために熱心な議論を展開した。
- 韓国科学技術情報通信部のリュ・ジェミョンネットワーク政策室長は「韓国の12大国家戦略技術の一つであるサイバーセキュリティに対する グローバル標準化リーダーシップを徐々に拡大し、産・学・研とも継続的に協力し、ゼロトラストセキュリティ(※2)、AIセキュリティ、SW サプライチェーンセキュリティなど次世代のセキュリティ標準化を国際社会で引き続き、主導できるように支援したい。」とのコメントを発表した。
  (※2)ゼロトラストセキュリティ：ネットワークがすでに侵害されたものとみなし、「絶対に信用せず、常に検証する」というセキュリティ概念(Never Trust, Always Verify)

出所:韓国科学技術情報通信省（Ministry of Science and IC）2024年3月6日付けニュースリリース https://www.msit.go.kr/bbs/view.do?sCode=user&mId=113&mPid=238&bbsSeqNo=94&nttSeqNo=3184145

© 2023 Japanese Standards Association. All Rights Reserved.

【サイバーセキュリティ】関連記事詳細（１/24）

番号	地域・国	情報記事・タイトル	発行日	要旨	情報源（機関・団体名／URL）	
1	国際	ISO/IEC JTC1/SC27（サイバーセキュリティ）について	2024/7/19	• ISOにおけるサイバーセキュリティに関する標準化は、IECとのジョイント委員会であるJTC1/SC27で行われている。議長国はドイツ、事務局はドイツ規格協会（DIN）が務める。国内の審議団体は、（一社）情報処理学会である。 • 2024年7月16日現在、開発済みの規格が245件、開発中の規格が70件ある。 • SC27のワーキンググループは以下のとおり。 ISO/IEC JTC 1/SC 27/AG 2　信頼性 ISO/IEC JTC 1/SC 27/AG 5　ストラテジー ISO/IEC JTC 1/SC 27/AG 6　オペレーション ISO/IEC JTC 1/SC 27/AG 7　コミュニケーションとアウトリーチ (AG-CO) ISO/IEC JTC 1/SC 27/AG 8　適合性評価に関する諮問グループ ISO/IEC JTC 1/SC 27/AG 9　多様性に関する諮問グループ ISO/IEC JTC 1/SC 27/AHG 1　解像度の製図 ISO/IEC JTC 1/SC 27/AHG 2　IoT とデジタル ツインにおけるセキュリティとプライバシー ISO/IEC JTC 1/SC 27/AHG 3　AI とビッグデータ (BD) におけるセキュリティとプライバシー ISO/IEC JTC 1/SC 27/CAG　議長の諮問グループ ISO/IEC JTC 1/SC 27/JWG 6　共同 ISO/IEC JTC1/SC 27 - ISO/TC 22/SC 32 WG：コネクテッド カー デバイスのサイバーセキュリティ要件と評価活動 ISO/IEC JTC 1/SC 27/WG 1　情報セキュリティ管理体制 ISO/IEC JTC 1/SC 27/WG 2　暗号化とセキュリティのメカニズム ISO/IEC JTC 1/SC 27/WG 3　セキュリティの評価、テスト、仕様 ISO/IEC JTC 1/SC 27/WG 4　セキュリティ管理とサービス ISO/IEC JTC 1/SC 27/WG 5　アイデンティティ管理とプライバシーのテクノロジー • 別のTCとの共同作業グループとして以下がある。 ISO/TC 307/JWG 4　ISO/TC 307 - ISO/IEC JTC 1/SC 27 WG 共同: ブロックチェーンと DLT のセキュリティ、プライバシー、アイデンティティ	International Organization for Standardization（ISO）	https://www.iso.org/committee/45306.html

© 2023 Japanese Standards Association. All Rights Reserved.

【サイバーセキュリティ】関連記事詳細（2/24）

番号	地域・国	情報記事・タイトル	発行日	要旨	情報源（機関・団体名／URL）	
2	アメリカ	サイバーインシデントの事件開示規則に関する司法省とFBIが新たなガイドラインを公表した	2024/01/03	• このほど、FBI は、サイバー インシデント開示の延期を要求するプロセスを詳述した ポリシー通知 を発行した。また、アメリカ合衆国司法省(以下、DOJ) は サイバー インシデント開示の延期を要求するプロセスを概説した 省庁ガイドライン を発表した。ISC2(※）が以前、 サイバーインシデント開示規則 と、用語の定義をめぐる不確実性や曖昧なプロセス に関する懸念を明らかにしていた。 • 事件の開示を延期するよう要請するには、企業はFBIに直接連絡することができる。 遅延リクエストには特定の情報を含める必要がある。司法省によると、 報告の延期が認められる可能性のある事案の例としては 、以下のものが挙げられる。 ➢ よく知られた緩和策のない技術 （パッチがまだ提供されていないソフトウェアの脆弱性など）が関与し、公共の安全や国家の安全保障上のリスクをもたらすサイバーセキュリティ インシデント ➢ 事件が公表されると、機密情報や情報源が漏洩したり、重要なインフラや公共の安全が危険にさらされる可能性がある事案 ➢ 政府の機密情報を保有する企業に対する攻撃を公表すると、さらなる攻撃や脆弱性が生じる可能性がある事案 • 2023年7月に発行されたSECの最終規則では、すべての上場企業に重大なサイバーインシデントを4日以内に報告するよう義務付けられ、この要件は2023年12月18日に発効。なお、小規模企業には、インシデント報告の提出開始までに180日間の延長が与えられている。FBIと司法省は、例外は限られた状況でのみ認められるものであり、例外を検討する際にはFBIに速やかに通知することがポイントになると指摘する。 （※）ISC2:1989年米国で設立、セキュリティに対する網羅的で実用的な認定資格であるCISSP資格などの認定で知られる非営利団体	International Information Systems Security Certification Consortium （ISC）	https://www.isc2.org/Insights/2024/01/New-Guidance-from-DOJ-and-FBI-on-SEC-Incident-Disclosure-Rules?queryID=9334db6b840e1de0e9bd73cb9a21e5fd

© 2023 Japanese Standards Association. All Rights Reserved.

【サイバーセキュリティ】関連記事詳細（3/24）

番号	地域・国	情報記事・タイトル	発行日	要旨	情報源（機関・団体名／URL）	
3	アメリカ	CISAとFBIは、「サイバーセキュリティガイダンス: 中国製無人航空機システム」を発表した	2024/01/17	• サイバーセキュリティ・インフラストラクチャセキュリティ庁 (CISA) と連邦捜査局 (FBI) は、中国製の無人航空機システム(UAS、※)がもたらす脅威に対する認識を高め、重要なインフラストラクチャと州、地方、部族、領土 (SLTT) のパートナーに、ネットワークと機密情報へのリスクを軽減するための推奨サイバーセキュリティ保護策を提供することを目的とした「サイバーセキュリティガイダンス: 中国製無人航空機システム」を発表した。重要なインフラの運用において中国製の UAS を使用すると、機密情報が 中華人民共和国当局に漏洩するリスクがある。このガイダンスでは、適切なサイバーセキュリティプロトコルを使用せずに運用した場合のネットワークと機密情報の潜在的な脆弱性と、その結果生じる事項について説明する。 • 重要なインフラストラクチャ組織は、設計段階からセキュリティが確保され、米国企業が製造した UAS を運用することが推奨される。このガイダンスでは、組織が UAS プログラム、ポリシー、手順の一部として検討すべきサイバーセキュリティに関する推奨事項を示している。 (※)無人航空機システム（UAS）:操縦士を乗せずに飛行する航空機、およびその航空機を制御するシステムの総称	Cybersecurity and Infrastructure Security Agency （CISA）	https://www.cisa.gov/news-events/news/release-cybersecurity-guidance-chinese-manufactured-uas-critical-infrastructure-owners-and-operators
4	アメリカ	NIST が企業のサイバーセキュリティ プログラムの測定と改善に関するガイダンスを提供	2024/01/17	• 国立標準技術研究所 (NIST) が新しく改訂した、NIST特別出版物 (SP) 800-55 改訂 2:情報セキュリティ測定ガイドは、実用的な情報セキュリティ測定プログラムを作成するための効果的なガイダンスと、組織のパフォーマンス目標を満たす情報セキュリティ対策を開発するための柔軟なアプローチを提供する。この出版物は、NIST のサイバーセキュリティフレームワークやリスク管理フレームワークなどのあらゆるリスク管理フレームワークと併用できるように設計されている。 • この2巻からなるドキュメントは、組織の異なる読者を対象としている。1 巻目は主に情報セキュリティの専門家向けに書かれており、組織が特定の対策として優先順位付け、選択、評価して、すでに導入しているセキュリティの妥当性を判断する方法についてのガイダンスを提供する。2巻目は主に経営幹部を対象としており、組織が情報セキュリティ測定プログラムを開発する方法の概要を示し、時間をかけてそれを実装するための複数のステップのワークフローを提供する。NIST は、レビューの担当者に対して、情報セキュリティ測定に関心のある人々が協力して専門知識を共有し、知識とリソースを磨き、成長と改善の機会を特定するための利益共同体(CoI) の設立を提案している。	National Institute of Standards and Technology (NIST)	https://www.nist.gov/news-events/news/2024/01/nist-offers-guidance-measuring-and-improving-your-companys-cybersecurity

© 2023 Japanese Standards Association. All Rights Reserved.

【サイバーセキュリティ】関連記事詳細（4/24）

番号	地域・国	情報記事・タイトル	発行日	要旨	情報源（機関・団体名／URL）	
5	イギリス、フィリピン	マニラ駐英大使館は、初の包括的なサイバーセキュリティイベントを通じて、フィリピンにおけるサイバーセキュリティの回復力に対するサポートを強化	2024/01/17	• 2024年1月16日にマニラ駐在英国大使館で開催された、サイバーセキュリティのシンポジウムイベントで、英国とフィリピンの第一線の専門家、政府関係者、業界リーダーたちが参集し、サイバー脅威の頻度と高度化の増加に対処し、デジタル防御を強化するための戦略を共同で策定した。また、サイバーセキュリティの課題に取り組む上で政府機関、民間企業、学界の連携の重要性についてのパネルディスカッションが行われ、サイバーセキュリティ ソリューションの大手プロバイダーである BT、CyberQ Group、NCC Group、英国規格協会（BSI)などが、デジタル資産を保護するために設計された革新的なテクノロジーとツールを紹介した。 • イベントの中で、駐フィリピン英国大使ローレ・ボーフィス氏から、英国政府による初の英国・東南アジア「Women in Cyber Networkイベント」に、グローブ・テレコムの最高プライバシー責任者であるアイリッシュ・サランダナン・アルメイダ弁護士とサイバー犯罪捜査調整センターの次官補メアリー・ローズ・マグサイサイ氏の参加が発表された。このWomen in Cyber Network（英国-東南アジア女性サイバーフェローシッププログラム）は、支援的コミュニティを形成し、参加者に、貴重な自己啓発の機会や、常に変化し続けるこの業界をリードするスキルを磨く機会を提供することを目的としている。これらは、ネットワーキングの機会、この分野の専門家によるトレーニングワークショップ、英国のベストプラクティス、メンターシップ、そして1年を通しての実践的なグループプロジェクトを通じて提供される。	GOV.UK	https://www.gov.uk/government/news/british-embassy-manila-unites-uk-and-ph-cybersecurity-leaders-to-fortify-digital-defences
6	国際	再生可能エネルギーシステムのサイバーセキュリティ	2024/01/23	• 再生可能エネルギーシステムは、サイバー犯罪者から電力網の弱点と見なされることが多くなっている。この問題に対処するために、IEC は、標準規格と適合性評価を組み合わせた、サイバー犯罪を阻止するためのソリューションを数多く提供している。IEC は、電力会社、公共交通機関、医療施設など、あらゆる重要なインフラ施設に適用される IEC 62443シリーズやシステムの構築前にシステムと運用にセキュリティを設計するためのガイダンスとサイバー セキュリティ要件を提供する IEC 62351シリース など、いくつかの重要な標準を作成。これらの標準は、通信プロトコルからデータ保護まで、再生可能エネルギーシステムのさまざまな側面を保護するためのガイドラインと要件を提供する。 • さらに、IEC は IECEE CBスキームを通じて適合性評価サービスを提供しており、これによりメーカーは IEC サイバー セキュリティ標準への準拠を表す証明書を取得できる。この認証プロセスにより、再生可能エネルギーシステムが現場に導入される前に、厳格なセキュリティ要件を満たしていることを確認できる。IECは、共通のフレームワークと認証プロセスを提供することで、サイバー脅威に対する再生可能エネルギーシステムの耐性を強化し、電力網の完全性を維持することを目指す。	e-Tech (IEC)	https://etech.iec.ch/issue/2024-01/cyber-security-for-renewable-energy-systems

© 2023 Japanese Standards Association. All Rights Reserved.

【サイバーセキュリティ】関連記事詳細（5/24）

番号	地域・国	情報記事・タイトル	発行日	要旨	情報源（機関・団体名／URL）	
7	EU	EUが初のサイバーセキュリティ認証制度に関する実施規則を導入	2024/01/31	• 欧州委員会は、EU の Common Criteria (EUCC、※1) に基づくサイバーセキュリティ認証制度に関する実施規則を採択した。これは、欧州委員会の要請に応じてENISAが起草したEUCCに関するサイバーセキュリティ認証スキーム案に沿うもの。候補案の起草にあたり、ENISA は業界全体および EU 加盟国の国家サイバーセキュリティ認証機関 (NCCA、※2) の専門家で構成される特別作業グループ (AHWG) の支援を受けている。EU のサイバーセキュリティ認証スキームとなるEUCCは、これまでの SOG-IS 協定(※3)に基づく国家認証スキームに取って代わることになる。 • 自主的な新しい EUCC スキームでは、保証証明を示そうとする ICT サプライヤーが、EU で一般的に理解されている評価プロセスを経て、技術コンポーネント 、ハードウェア、ソフトウェアなどの ICT 製品を認証できる。このスキームは、17 の EU 加盟国ですでに使用されている実績のある SOG-IS Common Criteria 評価フレームワークに基づいている。 (※1)Common Criteria (EUCC) : コンピュータセキュリティのための国際規格(ISO/IEC 15408) 。 IT 製品に対して、情報セキュリティを評価し認証するための評価基準を定めている。 (※2)NCCA:加盟国の 適合性評価機関 (CAB) が発行する証明書のスキーム準拠の監視機関 (※3)SOG-IS 協定：欧州の複数国間における相互承認協定（又はそれを管理するグループ）	European Union Agency for Cybersecurity (ENISA)	https://www.enisa.europa.eu/news/an-eu-prime-eu-adopts-first-cybersecurity-certification-scheme
8	アメリカ	サイバーセキュリティ・インフラセキュリティ庁 (CISA) と環境保護庁 (EPA) は、「水道分野のサイバーセキュリティの強化」と題した CISA ライブイベントを開催	2024/02/07	• 2024年1月30日、「水道分野のサイバーセキュリティの強化」と題した CISA ライブイベントで、サイバーセキュリティおよびインフラストラクチャセキュリティ庁 （CISA） と環境保護庁 （EPA） が共同でリリースした「水道・廃水セクターサイバーセキュリティツールキット」が紹介された。このツールキットは、実用的な保護手段とソリューションを提供することで、進化するサイバーセキュリティの課題に対するセクターの回復力を強化するための重要なステップとなる。 • 水道セクターは、国家の健康、安全、経済、セキュリティの基盤である。しかし、資源の制約の中で、重大なサイバーリスクと物理的リスクに直面している。このツールキットは、水道セクターのメンバーがサイバーセキュリティの態勢を強化するための実用的な洞察を提供し、サイバーセキュリティの態勢を強化するようになっている。水セクターのサイバーセキュリティ ツールキットの主な特徴には、新たに発行されたサイバーセキュリティインシデント対応ガイドや、無料のサイバーセキュリティ評価サービス、脆弱性スキャン評価サービス、技術支援サポート、サイバーセキュリティ パフォーマンス目標の調整、サイバー衛生ツールなどの重要なサービスが含まれている。	Cybersecurity and Infrastructure Security Agency (CISA)	https://www.cisa.gov/news-events/news/cisa-and-epa-collaborate-water-and-wastewater-sector-cyber-resources

© 2023 Japanese Standards Association. All Rights Reserved.

【サイバーセキュリティ】関連記事詳細（6/24）

番号	地域・国	情報記事・タイトル	発行日	要旨	情報源（機関・団体名／URL）	
9	アメリカ，国際	米国と国際パートナーが、中華人民共和国による米国重要インフラへのハッキングに関するサイバーセキュリティ勧告を発表	2024/02/07	• サイバーセキュリティ・インフラストラクチャセキュリティ庁 (CISA)、国家安全保障局 (NSA)、連邦捜査局 (FBI) は、主要な米国政府機関および国際政府機関と共同で、中華人民共和国 (PRC) の国家支援を受けたサイバー攻撃者 (Volt Typhoon として知られる) による、重要なインフラストラクチャへの不正アクセスを目的とした悪意のある活動と、すべての組織が緊急に取り組むべき関連措置に関する共同サイバーセキュリティ勧告を２月７日に発表した。 • 共同サイバーセキュリティ勧告に加えて、CISA と各パートナーは、Volt Typhoon （※1）などの攻撃者が使用する「Living Off the Land」(※2)と呼ばれる高度な手法をすべての組織が効果的に探知および検出できるようにするための補足的な共同ガイダンスも発表した。近年、米国では、中国のサイバー脅威活動が、スパイ活動に重点を置くものから、米国の重要インフラに対する破壊的なサイバー攻撃に備えて事前準備するものへと戦略的にシフトしている。なお、新しい勧告とガイドは、CISA、オーストラリア ACSC、カナダCCCS、イギリスNCSC-UK、ニュージーランドNCSC-NZなど各国サイバーセキュリティセンターの共同で発行された。 （※1）Volt Typhoon：中国国家の支援を受けて、特定の組織に対し高度な技術で継続的なサイバー攻 撃を行う集団。侵入後の検出を回避するための高度な手法「Living off the Land」を使いながら、主に米軍の行動を妨害する。 (※2)Living Off The Land（環境寄生型攻撃）:対策側の監視や調査を回避し、被害者の環境にあるシステムを悪用する、痕跡を残さない攻撃手法	Cybersecurity and Infrastructure Security Agency (CISA)	https://www.cisa.gov/news-events/news/us-and-international-partners-publish-cybersecurity-advisory-peoples-republic-china-state-sponsored

© 2023 Japanese Standards Association. All Rights Reserved.

【サイバーセキュリティ】関連記事詳細（7/24）

番号	地域・国	情報記事・タイトル	発行日	要旨	情報源（機関・団体名／URL）	
10	アメリカ	JFHQ-DODINが新たなサイバー運用準備評価プログラム（CORA）を正式に開始	2024/03/01	• 国防総省（DOD）は、統合部隊本部・国防総省情報ネットワーク（JFHQ-DODIN）を通じて、新たなサイバー作戦準備評価プログラム（CORA）を正式に開始した。CORA は、アクセス制御、異常の検出、敵の脅威情報への適応、サイバー命令の実行など、多くのリスク要因を融合することにより、サイバーの態勢を継続的に把握するための重要な評価。最終的に、この評価により、ネットワークの作戦地域の司令官とディレクターは、優先度の高いサイバー領域と全体的なサイバーセキュリティおよび防御態勢をより正確に理解できるようになり、指揮統制が強化され意思決定が強化される。 • CORAは、JFHQ-DODINのリスクベースの指標を通じて、国防総省情報ネットワーク(DODIN)に対する敵対的リスクを最小限に抑えるために、MITRE ATT&CK（※）の緩和策を優先する。司令部は、初期アクセス、持続性、権限昇格、横方向の移動、および流出に関するMITRE ATT&CKの戦術、手法、手順を分析した後、リスクベースの指標を作成した。CORA は、DOD が継続的に領域を監視および評価し、DODIN 全体のリスクを評価および軽減するのに役立つ。 （※）MITRE ATT&CK ：米国連邦政府が資金提供している非営利組織MITREが開発した、CVE（共通脆弱性識別子）を運用したサイバー攻撃を分類・説明するためのガイドライン	Department of Defense provides the military forces（DOD、国防総省）	https://www.defense.gov/News/News-Stories/Article/Article/3691583/jfhq-dodin-officially-launches-its-new-cyber-operational-readiness-assessment-p/
11	韓国	ゼロトラスト先端航空交通セキュリティなどサイバーセキュリティ国際標準を韓国が先導	2024/03/06	• 科学技術情報通信部(以下、「科技通信部」)は、2月20日から3月1日までスイス・ジュネーブで開催された 国際電気通信連合電気通信標準化部門(ITU-T)情報保護研究委員会(SG17、議長：順天郷大学鑾興烈教授)の国際会議で、韓国が提案した ゼロトラストセキュリティ（※1）、先端航空交通データ セキュリティなど 新規標準課題 9 件が承認され 、車両用エッジコンピューティングセキュリティなど計6件の 標準化*承認成果(事前採択2件、最終承認4件)が あったと公表した。 • 韓国で開催された前回のSG17国際会議(2023年8月、一山キンテックス)では、ゼロトラスト、ソフトウェアサプライチェーンセキュリティ、人工知能セキュリティなど次世代標準化 テーマに対するグローバル 合意を導き出した。これに対するフォローアップとして、今回のSG17国際会議で、韓国は米国などとの緊密な協力を通じて開発した・ゼロトラストセキュリティ (※)に関する標準 課題を新規提案し、承認された。これを含め、・先端航空交通 (AAM)環境でのデータセキュリティ、・遠隔生体認証などに関する 新規標準課題 9件を 提案し、すべてが 承認される成果を得た。 （※1） ゼロトラストセキュリティ：ネットワークがすでに侵害されたものとみなし、「絶対に信用せず、常に検証する」という新しいセキュリティ概念(Never Trust, Always Verify)	Ministry of Science and ICT（韓国科学技術情報通信省）	https://www.msit.go.kr/bbs/view.do?sCode=user&mId=113&mPid=238&bbsSeqNo=94&nttSeqNo=3184145

© 2023 Japanese Standards Association. All Rights Reserved.

【サイバーセキュリティ】関連記事詳細（8/24）

番号	地域・国	情報記事・タイトル	発行日	要旨	情報源（機関・団体名／URL）	
12	EU	選挙の完全性を守るための新しいサイバーセキュリティ概要が出版された	2024/03/06	• EU加盟国は、欧州委員会およびEUサイバーセキュリティ機関(ENISA)の支援を受けて、サイバーセキュリティの観点から「選挙の完全性を保護する方法に関する新しい概要」を発表した。2019年の前回のEU選挙以来、ハクティビストの活動が加速し、脅威の主体が使用する手法がますます巧妙化するなど、脅威の状況は悪化している。 • 一方で、選挙プロセスは技術的に進歩しており、この新版には、選挙の脅威の状況の最新情報、新規および改訂されたケーススタディ、サイバーセキュリティのベストプラクティス、および選挙の回復力に影響を与える可能性のある新興技術から生じる潜在的な脅威、具体的には外国情報操作干渉、ソーシャルメディア上の偽情報、AI、ディープフェイクの調査が含まれる。 • この新しい概要では、選挙プロセス全体を通じて起こり得るサイバーインシデントを管理するために加盟国に推奨される措置や役立つガイダンスが提示されている。対策の中には、情報共有、意識向上、トレーニング、リスク管理、選挙運動、政党、候補者に対するサイバーセキュリティ支援、電子投票技術に関するベストプラクティスが含まれている。	European (EC)	https://digital-strategy.ec.europa.eu/en/news/new-cybersecurity-compendium-how-protect-integrity-elections-published
13	国際	欧州標準化機構（ESO）のCEN、CENELEC、ETSIは、欧州連合サイバーセキュリティ機関のENISAと協力し、第8回サイバーセキュリティ標準化会議を開催した	2024/03/07	• この会議は、 EUのサイバーセキュリティ法の効果的な実施を念頭に、政策立案者、業界、研究機関、標準化団体の間で対話を促進することを目的としており、欧州連合および国際社会から200人以上の現地参加者と2,000人以上のオンライン参加者が集まった。会議は4つのパネルで構成され、民間および公共の幅広い組織からの講演者が参加して、現在、進行中および計画中の標準化作業や将来の要件について議論がなされた。４つのパネルの主なテーマは以下のとおり。 パネル①：欧州標準化の将来像 パネル②：新しい法律に関連する標準化の課題 パネル③：デジタル製品に関する新たな基準の要件 パネル④：新たな法的枠組みや利害関係者から生じるサイバー セキュリティの要件を満たす方法（サプライ チェーンのセキュリティの標準化）	CEN/CENELEC	https://www.cencenelec.eu/news-and-events/news/2024/brief-news/2024-03-07-enisa-conference-2024/

© 2023 Japanese Standards Association. All Rights Reserved.

【サイバーセキュリティ】関連記事詳細（9/24）

番号	地域・国	情報記事・タイトル	発行日	要旨	情報源（機関・団体名／URL）	
14	オーストラリア	慈善団体および非営利団体向けのサイバーセキュリティ	2024/03/18	• 慈善団体や非営利団体は、強力なサイバー セキュリティ対策を実施するためのリソースがない場合があり、サイバー インシデントに対して脆弱になる可能性がある。これらの組織にとって、サイバー インシデントはコストがかかることが多く、機密性の高い貴重な情報の損失、サービスの中断、システムの不正変更、評判の低下、長期にわたる復旧プロセスにつながるため、オーストラリア通信信号局（ASD）は慈善団体や非営利団体に対し、オンラインシステムを保護するための対策を講じるよう奨励する。 • そのため、ASDは、慈善団体および非営利団体向けサイバー セキュリティ チェックリストを策定しており、わかりやすい手順とベスト プラクティス アドバイスへのリンクを通じて、慈善団体および非営利団体がサイバー セキュリティ能力を向上させるのを支援。ASDは、顧客データの保護、組織に対するサイバー脅威の理解、サイバー脅威を軽減するための演習の実施など、さまざまなサイバー セキュリティの取り組みを推進する。また、慈善団体や非営利団体は、ASD の無料のサイバー セキュリティ パートナーシップ プログラムにネットワーク パートナーとして参加して、最新のサイバー セキュリティに関する洞察やアドバイスを受け取ることができる。	Australian Signals Directorate（ASD、オーストラリア通信信号局）	https://www.cyber.gov.au/about-us/view-all-content/news-and-media/cyber-security-charities-and-not-for-profit-organisations
15	オーストラリア	オーストラリア サイバー セキュリティ センター（ACSC)は、「中国国家主導のサイバー活動：重要インフラのリーダーのための行動」ファクトシートを発表した	2024/03/20	• オーストラリア サイバー セキュリティ センター（ACSC）は、米国エネルギー省（DOE）やカナダサイバーセキュリティセンター（CCCS）などの国際的なパートナーと協力し「中国国家主導のサイバー活動：重要インフラのリーダーのための行動」ファクトシートを発表した。 • このファクトシートは、重要なインフラストラクチャのリーダーに対し、中華人民共和国（PRC）とつながりのある国家支援型のサイバー攻撃者 Volt Typhoon（ボルトタイフーン、※） からインフラストラクチャと重要な機能を保護するためのガイダンスを提供する。 • Volt Typhoon は通常、「Living off the Land」手法を使用して、運用技術を含む重要なインフラストラクチャ システムにアクセスし、これを妨害して検出を回避しようとするが、このファクトシートでは、情報に基づいた積極的なリソースの決定、サプライチェーンの保護、サイバーセキュリティ文化の推進など、重要なインフラストラクチャのリーダーがこれらの脅威に備え、その影響を軽減するために実行できる手順を概説している。 （※）Volt Typhoon：中国国家の支援を受けて、特定の組織に対し高度な技術で継続的なサイバー攻 撃を行う集団。侵入後の検出を回避するための高度な手法「Living off the Land」を使いながら、主に米軍の行動を妨害する。	Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC、ｵｰｽﾄﾗﾘｱ ｻｲﾊﾞｰｾｷｭﾘﾃｨ ｾﾝﾀｰ)	https://www.cyber.gov.au/about-us/view-all-content/news-and-media/new-fact-sheet-critical-infrastructure-leaders-actions-mitigate-prc-state-sponsored-cyber-activity

© 2023 Japanese Standards Association. All Rights Reserved.

【サイバーセキュリティ】関連記事詳細（10/24）

番号	地域・国	情報記事・タイトル	発行日	要旨	情報源（機関・団体名／URL）	
16	イギリス、中国	英国は、民主的な機関や国会議員を標的とした中国政府系組織や個人による悪質なサイバー活動のパターンを非難した	2024/03/25	• イギリス国家サイバーセキュリティセンター（NCSC）が、イギリス選挙管理委員会のシステムが2021年から2022年の間に中国政府系組織によって侵害された可能性が高いと評価していることを公表。NCSCは、中国政府系の高度脅威(ハッカー) 集団31（APT31）が、2021年中に英国国会議員に対して偵察活動を行ったことはほぼ確実であるとし、標的となった人々の大半は、中国の悪意ある活動を非難する著名人だったことを明らかにした。 • これを受けて、イギリス外務省・連邦政府・開発省は、駐英中国大使を召喚し、APT31のメンバーであるフロント企業と個人2名に制裁を科した。同時に、米国も同じ人物と団体を悪質なサイバー活動の容疑者に指定している。オーストラリア、欧州連合、ニュージーランド、スロバキア、米国を含む合計16か国が、中国政府支援の攻撃者による悪質なサイバー活動について深刻な懸念を表明する声明を出した。これらの声明は、国際社会が中国政府に対し、責任あるサイバー活動家としての信頼性を示すよう改めて求めるものである。	GOV.UK	https://www.gov.uk/government/news/uk-holds-china-state-affiliated-organisations-and-individuals-responsible-for-malicious-cyber-activity
17	アメリカ	CISA はサイバーインシデントへの対応において、CIRCIAの規則制定案の通知に対する意見を求める	2024/03/27	• 国土安全保障省（DHS）のサイバーセキュリティ・インフラセキュリティ庁（CISA）は、CISAに策定が義務付けられていた規則策定提案公告（NPRM）を一般公開した。これは、2022年重要インフラ向けサイバーインシデント報告法（CIRCIA、※）により、アメリカのサイバーセキュリティ強化のためにCISAが策定を義務付けられたものである。 • 2022 年 9 月以降、CISA は NPRM を策定するにあたり、重要インフラ コミュニティを含む公共部門と民間部門の利害関係者からの意見を求めてきた。この公開コメント期間は、利害関係者が NPRM に関するコメント書面を提出する機会でもある。NPRM には、サイバー インシデントおよび身代金支払い報告に関する規制案のほか、CIRCIA 規制プログラムのその他の側面が含まれる。CIRCIA の実施により、CISA はサイバー脅威の状況に関する洞察を深め、全国のサイバー リスク削減を推進し、標的となるリスクのある組織に早期警告を提供できるようになる。 （※）重要インフラのサイバーインシデント報告法（CIRCIA）：サイバーインシデントやランサムウェアの支払いをCISAに報告することを、対象となる組織に対して求める規制の策定と実施を義務付ける法律（2022年3月大統領署名）	Cybersecurity and Infrastructure Security Agency (CISA)	https://www.cisa.gov/news-events/news/cisa-marks-important-milestone-addressing-cyber-incidents-seeks-input-circia-notice-proposed

© 2023 Japanese Standards Association. All Rights Reserved.

【サイバーセキュリティ】関連記事詳細（11/24）

番号	地域・国	情報記事・タイトル	発行日	要旨	情報源（機関・団体名／URL）	
18	アメリカ	国防総省、産業基盤全体のサイバーセキュリティ強化戦略を発表	2024/03/28	• 国防総省（DOD）は、国家安全保障における防衛産業基盤の重要な役割を認識し、国防総省と米国の防衛産業基盤の間でサイバーセキュリティの取り組みに重点を置く、「産業基盤全体のサイバーセキュリティを強化するための包括的な戦略」を発表した。この戦略は、米国の戦闘力の優位性を確保するために、安全で強靭かつ技術的に優れた米国防衛産業基盤を構築するという、今後3年間の国防総省のビジョンを示している。 このビジョンに沿った 4 つの目標は以下のとおり。 ➢サイバーセキュリティ要件の確立と実装の評価 ➢サイバーセキュリティ投資の奨励 ➢情報共有とコラボレーションの強化 ➢監督と説明責任の改善 • これらの目標を達成するために、国防総省は以下を含むさまざまな対策を実施する予定。 ➢明確なサイバーセキュリティの標準と要件の策定 ➢請負業者がサイバーセキュリティに投資するためのインセンティブの創出 ➢政府と産業界間の情報共有の改善 ➢監視と説明責任の仕組みの強化 • 国防総省のサイバーセキュリティガバナンス構造を強化するという目標の中心となるのは、省庁間の連携を強化し、請負業者と下請け業者のサイバーセキュリティ責任をさらに管理する規制を策定する取り組みである。 • 米国軍需産業（DIB） のサイバーセキュリティ体制を強化するという観点から、この戦略では、部門のサイバーセキュリティ要件への準拠を評価し、規制と要件の有効性を評価する手順を概説している。また、業界パートナーと協力してサイバー関連の脅威とインテリジェンス情報を改善し、脆弱性を特定し、悪意のあるサイバー活動から回復するための手順も概説している。	Department of Defense provides the military forces（DOD、米国国防総省）	https://www.defense.gov/News/News-Stories/Article/Article/3724118/dod-releases-strategy-to-bolster-cybersecurity-across-industrial-base/

© 2023 Japanese Standards Association. All Rights Reserved.

【サイバーセキュリティ】関連記事詳細（12/24）

番号	地域・国	情報記事・タイトル	発行日	要旨	情報源（機関・団体名／URL）	
19	アメリカ	NISTは、コミュニティベースのサイバーセキュリティ人材育成の取り組みに対して、360万ドルを授与	2024/04/03	• 国立標準技術研究所 (NIST) は、サイバーセキュリティのリスクから企業を守るために必要な人材の育成を目的とした、総額約 360 万ドルの協力協定を締結した。約 20 万ドルの助成金は、国内の熟練サイバーセキュリティ人材不足の解消に取り組んでいる 15 州の 18 の教育機関およびコミュニティ組織に支給された。 • サイバーセキュリティの求人市場に関するデータを分析するCyberSeekツールによると、2023年1月から2024年1月の間に米国ではサイバーセキュリティの求人が約45万件あったことが判明した。 • 助成金を受けた組織は、サイバーセキュリティ教育と人材育成を促進する地域同盟およびマルチステークホルダーパートナーシップ (RAMPS、※) を構築。これらの RAMPSプロジェクトは、地元の企業や非営利団体の人材ニーズを、NICE サイバーセキュリティ人材フレームワークの目標と一致させる。 (※)RAMPS：サイバーセキュリティ業務の役割においてスキルが不足している複数の雇用主を組織化し、地域経済内の業界のニーズを満たす熟練労働力の育成に焦点を当てるパートナーシップ	National Institute of Standards and Technology (NIST)	https://www.nist.gov/news-events/news/2024/04/nist-awards-36-million-community-based-cybersecurity-workforce-development
20	アメリカ	CISAは、ロシア政府が支援するサイバー脅威による重大なリスクを直ちに軽減するよう連邦機関に指示	2024/04/11	• サイバーセキュリティおよびインフラストラクチャセキュリティ庁 (CISA) は、ロシア政府の支援を受けたサイバーアクター Midnight Blizzard （ハッカー集団）による最近のキャンペーン行動に対応して、「緊急指令 24-02 」を公表した。このキャンペーン行動は、Microsoft の企業メールアカウントをターゲットにし、連邦文民行政機関 (FCEB) との通信にアクセスする可能性がある。指令は、現在入手可能な脅威情報と、Microsoft による漏洩した資格情報の通知を前提とする関連措置の限定的な適用性に基づいて、4 月 2 日に連邦機関に最初に発行された。この指令は、影響を受ける可能性のある電子メールを分析し、漏洩した認証情報をリセットし、Microsoft Azureアカウントを保護するための追加措置を講じることを連邦文民行政機関 (FCEB)に求めている。 • Midnight Blizzard は、Microsoft の企業メール システムから最初に流出した情報 (Microsoft の顧客と Microsoft の間でメールで共有された認証の詳細を含む) を使用して、特定の Microsoft の顧客システムへの追加アクセスを取得、または取得しようとしている。Microsoft と CISA は、Midnight Blizzard によってMicrosoft とのメール通信が情報流出したことが確認されたすべての連邦機関に通知した。	Cybersecurity and Infrastructure Security Agency (CISA)	https://www.cisa.gov/news-events/news/cisa-directs-federal-agencies-immediately-mitigate-significant-risk-russian-state-sponsored-cyber

© 2023 Japanese Standards Association. All Rights Reserved.

【サイバーセキュリティ】関連記事詳細（13/24）

番号	地域・国	情報記事・タイトル	発行日	要旨	情報源（機関・団体名／URL）	
21	国際	G7サイバー専門家グループが金融分野で国境を越えた調整演習を実施した	2024/04/24	• G7サイバー専門家グループ（※）による、この演習の主な目的は、金融セクターに影響を及ぼす重大な国境を越えたサイバーインシデントが発生した場合に、G7の金融当局がそれぞれの対応を効果的に伝達・調整し、危機管理を促進する能力を強化すること。 • G7金融当局間の連携を最適化するため、この演習ではG7全管轄区域の金融市場インフラと金融主体に対する大規模なサイバー攻撃を想定する。この演習には、財務省、中央銀行、銀行監督当局、市場当局を含む23の金融当局と民間業界関係者が参加。このような演習を実施することで、金融セクターの回復力を強化し、G7各国（日本、英国、フランス、ドイツ、イタリア、カナダ、米国）の管轄区域全体で混乱を最小限に抑えることを目指す。国境を越えた調整、インシデント対応の準備、情報交換を行うことは、G7 の優先事項である。 （※）G7 サイバー専門家グループ：8つの G7 管轄区域にわたるサイバーセキュリティ ポリシーと戦略を調整する複数年にわたる作業グループで、イングランド銀行とイギリス財務省がこの作業グループの共同議長を務める。	GOV.UK	https://www.gov.uk/government/news/g7-cyber-expert-group-conducts-cross-border-coordination-exercise-in-the-financial-sector
22	中国	中国サイバースペース局が企業関連のオンライン侵害の報告に関するシンポジウムを開催	2024/04/28	• 4月25日、中国サイバースペース局は習近平総書記の重要な指示の精神と、全国人民代表大会と中央経済工作会議の精神を実施するための特別シンポジウムを開催し、一部の企業や企業の代表者の意見を聞いた。シンポジウムでは、中国電子技術、iFlytek、BYD、SenseTime、Xiaomiなどの企業のトップが参加した。 • 会議では、企業関連のオンライン侵害を報告する取り組みをさらに強化すること、企業関連の侵害を報告するための特別エリアを有効に活用すること、報告ガイドラインを改善すること、事件のガイダンスを強化すること、証拠要件の標準化は、企業の効果的な報告を支援するものであることなどが確認された。企業関連の報告を厳格に監督・検査し、作業台帳を確立し、企業関連ネットワーク侵害通報の有効性を高める必要がある。企業関連の報告方針と措置を改善し、「オンライン侵害情報の報告のさらなる強化に関する指導意見」および「企業関連のオンライン侵害情報の報告の受理および処理に関するウェブサイトプラットフォームの基準」の実施を浸透させる必要がある。中国は、組織規範を改善し、ルールを制定し、侵害アカウントに対する処罰を強化、典型的なケースとアカウントの公表を強化し、コミュニティを改善する。	中央网络安全和信息化委员会办公室	https://www.cac.gov.cn/2024-04/28/c_1715980166621143.htm

© 2023 Japanese Standards Association. All Rights Reserved.

【サイバーセキュリティ】関連記事詳細（14/24）

番号	地域・国	情報記事・タイトル	発行日	要旨	情報源（機関・団体名／URL）	
23	EU	第2回交通サイバーセキュリティ会議が開催された	2024/05/02	• 欧州連合のモビリティ・運輸総局(DG MOVE)が主催する、第2回運輸サイバーセキュリティ会議が2024年5月2日にブリュッセルで開催され、運輸部門から約300名の参加者を集めた。講演者とパネリストは、脅威評価、規制の枠組み、業界の慣行、国際協力など、運輸におけるサイバーセキュリティのさまざまな側面について議論した。 • 本イベントは、交通分野における将来のサイバーセキュリティの優先事項を形成するための重要なプラットフォームとして機能し、引き続き協力してサイバーセキュリティの課題を前進させることを呼びかけることで終了した。会議における議論に基づき、以下の重要なメッセージが確認された。 ➢ 運輸部門におけるサイバーセキュリティの脅威 ➢ 脆弱性の修正とインシデントからの回復能力 ➢ 輸送システム運用の回復力強化、先行投資と定期的なテスト・演習実施 ➢ （ICAO や IMO などとの）コラボレーションと国際協力 ➢ 規制当局、業界、その他の関係者間の連携 ➢ 運輸部門におけるサイバーセキュリティのスキル不足への対応	European Commission(EC)	https://transport.ec.europa.eu/news-events/main-events/2nd-transport-cybersecurity-conference_en
24	アメリカ	良好なサイバー衛生は、米国のインフラへの敵対者の干渉を阻止する	2024/05/02	• アヴリル・D・ヘインズ国家情報長官は上院軍事委員会の委員らに対し、「米国の敵対勢力が、電力、水道、ガスなどの米国のインフラシステムにハッキングしたことが明らかな多くのケースでは、定期的なパスワードの変更やソフトウェアのセキュリティパッチの適用などの適切なサイバー衛生管理によってハッキングは防げたはずだ。」と語った。 • ヘインズ氏は、「ランサムウェア攻撃の数は世界全体で昨年は、前年度比4%増加した。一方、米国の重要インフラに対する攻撃のほとんどすべてにおいて、サイバー攻撃者は、デフォルトのパスワードや脆弱なパスワード、パッチが適用されていない既知の脆弱性、セキュリティが不十分なネットワーク接続を利用して、比較的単純な攻撃を仕掛けてきた。そのため、特に重要インフラの所有者と運営者は、サイバーセキュリティ対策を改善し、こうした攻撃に対する脆弱性を減らすことが重要である。」と述べた。 • 国防情報局長のジェフリー・A・クルーズ空軍中将は上院議員らに対し、「外国の情報機関や内部の脅威を含む幅広い主体によるサイバー攻撃から国防情報局のネットワークを保護する必要性が、引き続き国防情報局の最大の懸念事項である。」と語り、「これには、ロシアや中国などの国家主体の高度な能力集団だけでなく、政府と緩く連携しているサイバー犯罪者も含まれる。」と述べた。	Department of Defense provides the military forces（DOD、米国国防総省）	https://www.defense.gov/News/News-Stories/Article/Article/3763862/good-cyber-hygiene-can-impede-adversary-meddling-in-us-infrastructure/

© 2023 Japanese Standards Association. All Rights Reserved.

【サイバーセキュリティ】関連記事詳細（15/24）

番号	地域・国	情報記事・タイトル	発行日	要旨	情報源（機関・団体名／URL）	
25	オーストラリア	オーストラリア史上2度目のサイバー制裁	2024/05/08	• オーストラリアの自主的なサイバー制裁枠組みの2度目の適用が実行された。現在行われている国際的な協調的法執行活動の一環である。最初の制裁は2024年1月に、2022年のメディバンクへの不正アクセスとオーストラリア人の健康保険記録約1,000万件の盗難に関与したロシア国籍のアレクサンドル・エルマコフ氏に課された。また、オーストラリア通信信号局（ASD）とオーストラリア連邦警察（AFP）は、英国や米国の国際パートナーと協力し、ドミトリー・ユリエビッチ・ホロシェフがLockBitアクター（※）の上級幹部の一員であることを特定した。 • サイバー制裁の適用を受けて、オーストラリア通信信号局（ASD）のオーストラリアサイバーセキュリティセンター（ACSC）は、LockBitアクター（※）から身を守るための最新のアドバイスを含む「LockBitアドバイザリ」を公開した。 • すべてのサイバー犯罪およびサイバー セキュリティ インシデントは、オーストラリア通信信号局（ASD） の サイバー セキュリティ センター (ACSC) に報告する必要があり、ACSC は、インシデントの解決に役立つアドバイスを提供する。この報告は、ASD がサイバー脅威を理解するのに役立ち、オーストラリアのサイバーセキュリティを強化するための防御アドバイスや運用上の決定に役立つ。 （※）LockBitアクター：データ復号化の見返りとして金銭の支払いを要求する「暗号化ウイルス」であるランサムウェアの一種を使い、主要セクターを不安定化させ、混乱させる集団	Australian Signals Directorate（ASD、オーストラリア通信信号局）	https://www.cyber.gov.au/about-us/view-all-content/news-and-media/australias-second-ever-cyber-sanction-imposed
26	アメリカ	NISTが、機密情報保護に関するガイドラインを更新した	2024/05/14	• 連邦政府と取引を行う場合、請負業者やその他の組織は、取り扱う機密情報を保護するための米国国立標準技術研究所(NIST)ガイドラインに従う必要がある。NISTはこのほど、制御された非機密情報 (CUI) と呼ばれるこのデータを保護するためにガイドラインを更新し、2 つの出版物「非連邦システムおよび組織における制御された非機密情報の保護 (NIST 特別出版物 [SP] 800-171、改訂 3)」と、「制御された非機密情報のセキュリティ要件の評価 (NIST SP 800-171A、改訂 3)」を更新した。 • 2 つの出版物は、NIST のセキュリティおよびプライバシー管理のソース カタログ (NIST SP 800-53、※1) と評価手順 (NIST SP 800-53 A、※2) に基づいている。今回の更新以前は、これらのドキュメントの文言がソース カタログの言語と一致していなかったため、セキュリティ要件に曖昧さが生じ、セキュリティ要件の評価に不確実性が生じる可能性があった。今回の更新は、これらの問題に対処し、NIST のサイバーセキュリティ ガイダンスのポートフォリオを合理的に整合させるように設計されている。	National Institute of Standards and Technology (NIST)	https://www.nist.gov/news-events/news/2024/05/nist-finalizes-updated-guidelines-protecting-sensitive-information

© 2023 Japanese Standards Association. All Rights Reserved.

【サイバーセキュリティ】関連記事詳細（16/24）

番号	地域・国	情報記事・タイトル	発行日	要旨	情報源（機関・団体名／URL）	
		（続き）		• 付属の出版物であるSP 800-171A は、ユーザーが SP 800-171 のセキュリティ要件を評価し、要件が満たされているかを判断できるように設計されており、セキュリティ要件の変更に対応する更新された評価手順のセットと、セキュリティ要件評価の実施方法を示す新しい資料が含まれている。 (※1,2)NIST SP 800-53, SP 800-53A:NISTが開発した、サイバーセキュリティおよびコンプライアンスのフレームワーク。連邦政府機関および請負業者は、システムを保護するために NIST SP 800-53 に準拠する必要がある。またNIST SP 800-53に基づく評価手順が、NIST SP 800-53Aである		
27	イギリス	AIモデルのハッキングや妨害行為に対する保護を強化するためのベンチマークと期待される新たな措置が、英国政府によって発表された	2024/05/15	• 英国政府の主要サイバーセキュリティ会議であるCYBERUKでの演説で、技術大臣のサキブ・バッティ氏は、開発者がAIモデルとソフトウェアのサイバーセキュリティを向上させるのに役立つ新しい行動規範を発表した。この規範は、開発者が自社製品を改ざん、ハッキング、妨害行為に対して耐性を持たせるための要件を定めており、ほとんどの業界でAIモデルの使用に対する信頼性を高め、企業の効率性向上、成長の促進、イノベーションの加速に貢献する。 • 政府の年次サイバー部門分析報告書によれば、サイバーセキュリティ部門は、企業数が1,979社（前回調査）→2,091社（今回調査）となり約６%の増加。雇用者数は、58,005人（前回）→60,689人（今回）で、約５%の増加。また推定年間収益は、105億ポンド（前回）→119億ポンド（今回）となり、前回比＋13%の大幅な増加となり、現在その価値は自動車産業などの部門と同等の水準に達している。 • 今回発表された、新たな行動規範により、AIとソフトウェアのサイバーセキュリティが向上する一方、バッティ技術大臣は、政府の採用や人事政策にサイバー関連の役割を組み込むなど、政府と規制当局がサイバーセキュリティ部門を専門化するための新たな取り組みを発表した。これらのサイバースキルに関する政府の新たな措置により、サイバー人材の育成が促進され、英国がオンラインで国家を守るために必要な人材を確保できるようになる。	GOV.UK	https://www.gov.uk/government/news/developers-given-new-tools-to-boost-cyber-security-in-ai-models-as-cyber-security-sector-sees-record-growth

© 2023 Japanese Standards Association. All Rights Reserved.

【サイバーセキュリティ】関連記事詳細（17/24）

番号	地域・国	情報記事・タイトル	発行日	要旨	情報源（機関・団体名／URL）	
28	アメリカ	国防総省（DoD）は、2021年の大統領令で定められた目標を国防総省が達成するのを支援する文書「ゼロトラスト・オーバーレイ」を公開した	2024/06/04	• 国防総省（DOD）は、2027年までにゼロトラストサイバーセキュリティモデルへの移行をガイドする新しい「ゼロトラスト・オーバーレイ」を公開した。国防情報システム局（DISA）と国家安全保障局（NSA）によって開発されたこのガイドは、国防総省（DoD）の広大なネットワークインフラストラクチャ全体にゼロトラスト原則を実装するためのロードマップを提供する。 • ゼロトラストとは、いかなるユーザー、デバイス、ネットワークも本質的に信頼できるものではないと想定し、リソースへのアクセスには継続的な検証を必要とするセキュリティアプローチ。国防総省がこのモデルを採用したのは、従来の境界ベースの防御から脱却し、サイバーセキュリティ体制を強化するため。 • ゼロトラストはまだ国防総省全体に導入されていないが、2027年度までには一定の実装目標レベルに達すると予想されている。DODゼロトラスト・ポートフォリオ管理オフィスの部門長ウィル・シュミット氏によると、DODが2022年11月に発表した、「ゼロトラスト戦略とロードマップ」の紙面23ページ、付録B「国防総省のゼロ・トラスト活動」に記載された152の目標活動（外側の濃い青色の円弧内）のうち、91の活動（内側の水色の円弧内）を実施することを意味する。「ゼロトラスト・オーバーレイ」は、アイデンティティ管理、デバイスセキュリティ、ネットワークセグメンテーション、データ保護など、さまざまな技術分野でゼロトラストを実装するための特定の要件とベストプラクティスを概説。この取り組みは、サイバーセキュリティを近代化し、進化する脅威から米国を守る国防総省の取り組みの一環である。	Department of Defense provides the military forces（DOD、国防総省）	https://www.defense.gov/News/News-Stories/Article/Article/3795170/new-overlays-provide-guide-on-path-to-zero-trust/
29	韓国	実践型サイバーセキュリティ専門人材の集中育成	2024/06/04	• 科学技術情報通信部は、韓国インターネット振興院と一緒にサイバーセキュリティ現場の実力を強化するための「実践型サイバー訓練場(Security-Gym、セキュリティージム)」の教育過程を拡大運営すると公表した。 • 実戦型サイバー訓練場は、在職者及び求職者を対象に、実際に発生したハッキング事件を分析して仮想の侵害事故環境を構築し、侵害事故調査 、侵害攻撃・防御訓練、商用情報保護製品に対する実習など、レベル別の教育課程を編成して支援しており、 首都圏(板橋)と東南圏(釜山、2023年12月開所)に現場訓練場を運営しながら、オンライン教育課程も並行して提供している。 • 2016年に訓練場を構築した後、昨年までの累計の研修生目標5,820人に対し、139%の達成となる8,091人の研修生を輩出した。また各年度ごとに見ても実績が、目標を上回っており、在職者及び求職者などからは、教育回数及び教育課程の拡大に対する要望が寄せられている。	Ministry of Science and IC（韓国科学技術情報通信省）	https://www.msit.go.kr/bbs/view.do?sCode=user&mId=113&mPid=238&bbsSeqNo=94&nttSeqNo=3184576

© 2023 Japanese Standards Association. All Rights Reserved.

【サイバーセキュリティ】関連記事詳細（18/24）

番号	地域・国	情報記事・タイトル	発行日	要旨	情報源（機関・団体名／URL）	
30	EU	ESAとENISAが情報交換、協力関係を強化するための覚書に署名	2024/06/05	• 欧州監督局(ESA)と欧州連合サイバーセキュリティ機関(ENISA)が締結した覚書は、政策実施、インシデント報告、重要な情報通信技術 (ICT) の第三者プロバイダーの監視など、相互に関心のあるタスクに関する協力と情報交換の枠組みを定めている。また、相互に関心のある分野における分野横断的な学習と能力構築を促進し、新興技術に関する情報交換を促進する。 • 「新しい協力協定は、金融分野のサイバーセキュリティリスクに取り組むESAとEUのサイバーセキュリティ機関であるENISAを結集することで、金融システムを情報セキュリティリスクから保護するというEUの取り組みがさらに強化される。」と、ESA合同委員会議長兼ESMA議長のベレーナ・ロス氏は述べた。 • 「インシデント報告などに関するNIS2(※1)およびDORA規定(※2)の実施と調和に向けた両者の取り組みは、金融ICTシステムにおけるサイバーセキュリティの堅牢なメカニズムを構築する道を切り開く。」とENISAのユハン・レパサール事務局長はコメントした。 (※1)NIS2:EU域内でサービスを提供する又は活動を行う中規模（従業員50名）以上の主要又は重要エンティティを対象にしたネットワーク通信システム指令。2022年12月に、①大幅な対象拡大、②サイバーセキュリティ・リスクマネジメントの強化、③インシデント報告内容・時限の明確化、④厳しい罰則金の観点で改正がなされ、2024年10月18日より施行予定。 (※2)DORA規定：EUの金融業界のデジタルオペレーショナルレジリエンスに関する新しい規制であり、EU内に拠点を置いている金融機関は2025年初頭までに本規制に準拠する必要がある。	European Union Agency for Cybersecurity (ENISA)	https://www.enisa.europa.eu/news/esas-and-enisa-sign-a-memorandum-of-understanding-to-strengthen-cooperation-and-information-exchange
31	アメリカ	NISTは、公共給付の安全な提供を支援するデジタル ID に関する共同研究を開始	2024/06/10	• 米国商務省の国立標準技術研究所 (NIST)は、NIST のデジタル ID ガイドライン (特別出版物 800-63)を、受給者の食費、住宅費、医療費、その他の基本的な生活費の支払いを支援するための公的給付プログラムをサポートするために適応させる共同プロジェクトを開始した。NIST は共同研究開発契約を通じて、デジタル給付ネットワーク（DBN）と協力する。	National Institute of Standards and Technology (NIST)	https://www.nist.gov/news-events/news/2024/06/nist-launches-collaborative-research-effort-digital-identity-support-secure

© 2023 Japanese Standards Association. All Rights Reserved.

【サイバーセキュリティ】関連記事詳細（19/24）

番号	地域・国	情報記事・タイトル	発行日	要旨	情報源（機関・団体名／URL）	
		（続き）		• COVID-19パンデミックによる詐欺や関連するサイバーセキュリティの脅威の高まりに対応して、一部の給付金管理機関は、個人のデジタルアカウントや本人確認（IDプルーフィングとも呼ばれる）などの新しい安全策をオンライン申請に組み込み始めた。しかし、顔認識やデータブローカーに依存するような特定のアプローチの使用は、プライバシーとデータセキュリティ、適正手続きの問題、有色人種や社会的弱者のコミュニティに不適切な影響を与える、システムの潜在的な偏見に関する疑念を引き起こしている。 • このNISTの取り組みでは、連邦政府のパートナー、州の給付プログラム管理者、IT およびサイバーセキュリティリーダーなどの公共給付の状況を直接把握している人々から意見を収集する。このようにして、サービスの管理と提供のためのデータ、設計、テクノロジーの使用に関連する最新のプラクティスとコミュニティ リソースを含む、公共給付のポリシーと提供に関する専門知識を活用する。その結果、実務家と公共部門のリーダーが、給付の提供に際し、どのタイプの ID 証明が必要なのかを評価するのに役立つ。		
32	アメリカ	CISAが、公衆コミュニケーションを通じて選挙のセキュリティを強化するためのガイドを発表	2024/06/17	• サイバーセキュリティ・インフラストラクチャセキュリティ庁 (CISA) と米国選挙支援委員会 (EAC) は、選挙に関する公式情報の主な情報源となる州、地方、部族、および領土の選挙管理官向けのガイド「公開コミュニケーションによる選挙セキュリティの強化」のリリースを発表した。選挙管理官は、選挙の管理とセキュリティの確保方法に関する正確な情報を伝える公開コミュニケーション計画を作成し、チームが効果的にコミュニケーションできるよう準備することで、選挙のインフラと運営に対するリスクを軽減できる。 • 選挙管理官は、選挙日や選挙期限、有権者登録、候補者の提出書類、投票場所、選挙スタッフの募集、セキュリティ対策、選挙結果の公表など、幅広いトピックについて、頻繁に公のコミュニケーションに携わり、メディアや国民からの質問に答えている。この重要な機能を果たす選挙管理官を支援するため、CISA と EAC はこのガイドを作成し、年間を通じてのコミュニケーション計画の策定と実施のためのフレームワークと実用的なツールを提供する。	Cybersecurity and Infrastructure Security Agency (CISA)	https://www.cisa.gov/news-events/news/cisa-releases-guide-enhance-election-security-through-public-communications

© 2023 Japanese Standards Association. All Rights Reserved.

【サイバーセキュリティ】関連記事詳細（20/24）

番号	地域・国	情報記事・タイトル	発行日	要旨	情報源（機関・団体名／URL）	
33	アメリカ，日本	第9回日米サイバー対話の開催	2024/06/27	• 6月26日、ワシントンD.C.において、第9回日米サイバー対話が開催された。今回の対話では、日米両国の政府横断的な取組の必要性を踏まえ、日米双方の幅広い関係者が、両国におけるサイバー政策、二国間協力及び国際場裡における能力構築支援を含む協力等、サイバー政策に関する日米協力について幅広く議論した。 • 今回の対話においては、日本側から、熊谷直樹外務省総合外交政策局審議官兼サイバー政策担当大使を筆頭に、外務省、内閣サイバーセキュリティセンター、公安調査庁、総務省、経済産業省、防衛省を含む幅広い政府関係者が、また、アメリカ側から、リーシル・フランツ国務省サイバー空間・デジタル政策局次官補代理を筆頭に、国務省、国防省を含む幅広い政府関係者がそれぞれ出席した。日米両国は、今後も日米サイバー対話を継続し、一層の協力に努めていくことを確認した。	Ministry of Foreign Affairs of Japan（外務省）	https://www.mofa.go.jp/mofaj/press/release/pressit_000001_00828.html
34	アメリカ	CIS、全国規模で現実世界の脅威に対処するためのアイデアを発表	2024/06/27	• 米国の重要インフラに対するサイバー攻撃、ロシアによる米国選挙への干渉、ミシガン州とニューヨーク州での反ユダヤ主義攻撃、 AIを利用した詐欺など、これらは「多次元の脅威」として知られており、多くの場合オンラインで始まる。このほどインターネット セキュリティ センター (CIS) の国家安全保障およびサイバー セキュリティの専門家は、「つながる世界における安全性の強化: 国家行動枠組み」を発表した。この枠組みでは、悪意のあるサイバー要素と物理的要素の両方を含む多次元攻撃を特定して防止するための具体的な推奨事項が、法執行機関やセキュリティ専門家に提供されている。 • 主な推奨事項は以下のとおり。 ➢ オンライン脅威情報センターインフラの構築 ➢ 新たな脅威に関する情報共有の改善 ➢ 意識を高め、回復力を構築するための官民パートナーシップ ➢ 地域社会を支援し、オンライン活動に起因する犯罪行為や暴力を防止するための支援 • サイバー空間はもはや物理的な世界から切り離されたものではなく、両者は深く結びついており、それらを守る方法は従来の戦術や技術を超える必要がある。	Center for Internet Security(CIS)	https://www.cisecurity.org/about-us/media/press-release/cis-publishes-ideas-to-address-real-world-threats-nationwide-amid-rising-cybersecurity-concerns

© 2023 Japanese Standards Association. All Rights Reserved.

【サイバーセキュリティ】関連記事詳細（21/24）

番号	地域・国	情報記事・タイトル	発行日	要旨	情報源（機関・団体名／URL）	
35	カナダ	ISC2は、カナダの思想的リーダーシップイベントで国際パートナー、連邦政府、州政府を結集	2024/07/01	• ISC2（※1） は米国商務省と共同で、カナダのトロントにあるオンタリオ投資貿易センターでサイバーセキュリティに関する思想的リーダーシップ イベントを主催した。このイベントには、カナダの連邦、州、地方レベルの政府リーダーが一堂に会し、北米の労働力開発に焦点を当てた議論とネットワーキングが行われた。特に議論は、カナダ全土の学術的課題と、政府、大学、ISC2 の共同の取り組みによってそれらの課題をどう解決できるかに焦点が当てられた。 • 調達担当大臣のトッド・J・マッカーシー氏が、オンタリオ州政府の取り組み、特に法案194「サイバーセキュリティの強化と公共部門の信頼構築に関する2024年法」について講演した。この法案は、デジタルセキュリティと信頼の強化に関する2024年法（「EDSTA」、※2）を提案し、情報公開およびプライバシー保護法（「FIPPA」）の改正を目指している。 • このイベントは、学界、政府、企業、ISC2（支部やトレーニング パートナーを含む）の代表者が一堂に会し、相互接続された世界におけるサイバーの安全性とセキュリティを促進する支援、専門知識、および従業員のエンパワーメントを通じて、この分野の影響力、多様性、および活力を強化するというISC2 の使命遂行をサポートするもの。 （※1） ISC2：1989年米国で設立、セキュリティに対する網羅的で実用的なアプローチであるCISSP資格などのポートフォリオで知られる非営利団体 （※2） 「EDSTA」：サイバー セキュリティ、人工知能 (AI)、未成年者 (18 歳未満の個人と定義) に影響を与えるテクノロジーに関する新しい要件を公共部門全体に導入することを目指すオンタリオ州政府の法案	International Information Systems Security Certification Consortium（ISC2）	https://www.isc2.org/Insights/2024/07/ISC2-Brings-Together-Government-Leaders-in-Canadian-Thought-Leadership-Event?queryID=d6204cc931e1112501f810fad72eeefd

© 2023 Japanese Standards Association. All Rights Reserved.

【サイバーセキュリティ】関連記事詳細（22/24）

番号	地域・国	情報記事・タイトル	発行日	要旨	情報源（機関・団体名／URL）	
36	EU	欧州委員会は、デジタルヨーロッパプログラムに基づき、サイバーセキュリティ、デジタル能力、テクノロジーに2億1000万ユーロ以上を投資	2024/07/04	• 欧州委員会は、デジタル・ヨーロッパ・プログラム（DEP）の下で、EU全体のサイバーセキュリティとデジタル能力を強化するための提案を募集し、総額2億1,000万ユーロ以上を募集した。そのうち、サイバーセキュリティ関連の資金として手当てされているのは、以下のとおり。 ➢ サイバーセキュリティに関する大規模な産業施設や重要インフラを保護するプロジェクトへの充当(3,500万ユーロ) ➢ 国内および国境を越えたサイバーセキュリティオペレーションセンター（SOC）のさらなる設立、サポート、拡張投資資金(1,280万ユーロ) ➢ 最先端のサイバーセキュリティ技術とツールの導入(3,500万ユーロ) ➢ 加盟国によるサイバーセキュリティに関するEU法および国家サイバーセキュリティ戦略の実施支援資金(2,000万ユーロ) • この公募により資金提供されるプロジェクトは、欧州サイバーセキュリティ能力センター（ECCC）によって管理される。この公募は、EU 加盟国および 欧州経済地域諸国の企業、中小企業、行政機関、その他の団体を対象とする。 • サイバーセキュリティ関連の資金の他にも、欧州のローカルデジタルツイン（地域社会のデジタル版）の開発資金など、欧州のデジタルスキルの能力開発に関する資金として、計１億800万ユーロの資金に対し提案が募集される。	European Commission (EC)	https://digital-strategy.ec.europa.eu/en/news/commission-invest-over-eu210-million-cybersecurity-digital-capacities-and-technology-under-digital

© 2023 Japanese Standards Association. All Rights Reserved.

【サイバーセキュリティ】関連記事詳細（23/24）

番号	地域・国	情報記事・タイトル	発行日	要旨	情報源（機関・団体名／URL）	
37	アメリカ	CISAが、選挙管理官向け運用セキュリティガイドを発表	2024/07/05	• サイバーセキュリティおよびインフラセキュリティ機関（CISA）は、「選挙関係者のための運用セキュリティガイド」を発表した。この重要なガイドは、選挙におけるオペレーショナル・セキュリティ（OPSEC、※）の概要を提供し、潜在的なリスクを強調し、実践的な緩和策を提示することで、選挙インフラのセキュリティ強化を目的とする。 • 運用上のセキュリティとは、組織内の機密情報、データ、または能力を特定し、保護するための体系的なアプローチ。 強固な保護措置がなければ、機密情報は不注意または意図的に暴露され、脅威行為者に悪用される可能性があり、選挙作業員の職務遂行能力に影響を与えたり、有権者の個人識別情報（PII）を暴露したり、内部システムや施設への不正アクセスを可能にしたりする可能性がある。このガイドでは、敵対者の視点からデータを見て、潜在的な脅威を総合的に評価し、軽減することの重要性を強調している。 • 本ガイドの要点は以下のとおり。 ➢ このガイドでは、運用セキュリティを強化するための実際の例と緩和活動を紹介する。 ➢ OPSEC は、選挙インフラを潜在的な脅威アクターの攻撃から保護するために不可欠。 ➢ OPSEC の原則を日常業務に組み込むと、機密情報への不正アクセスを防ぐ。 ➢ OPSEC の原則に関するトレーニングと認識により、選挙スタッフは集約されたリスクを効果的に理解し、管理できる。 （※）OPSEC:組織内の機密情報、データ、または能力を特定し、保護するための体系的なプロセス	Cybersecurity and Infrastructure Security Agency (CISA)	https://www.cisa.gov/news-events/news/cisa-releases-guide-operational-security-election-officials

© 2023 Japanese Standards Association. All Rights Reserved.

【サイバーセキュリティ】関連記事詳細（24/24）

番号	地域・国	情報記事・タイトル	発行日	要旨	情報源（機関・団体名／URL）	
38	インド	第3回GCTCサイバーセキュリティ会議における副大統領の演説内容	2024/07/13	• インドのジャグディープ・ダンカール副大統領は、ニューデリーのヴィギャン・バワンで世界テロ対策協議会（GCTC）が主催した第3回サイバーセキュリティ会議の閉会式で演説し、国土の最も辺鄙な場所であってもデータ保護意識の重要性を強調した。サイバーセキュリティに関する主な演説内容は以下のとおり。 ➢ インドはデジタル防御を強化するためにさまざまな対策を実施してきた。なかでも、国家サイバーセキュリティ政策、インドコンピュータ緊急対応チームの設立、情報技術法の改正、国家重要情報インフラ保護センター、デジタル個人データ保護法、官民パートナーシップの推進などの取り組みは極めて重要。 ➢ サイバー セキュリティを確保するには、多様な利害関係者による多次元的なアプローチと、世界的な協力が必要。産業界、学界、政府、専門機関、市民社会、NGO、国際機関、すべてがこの脅威と戦うために団結しなければならない。そのためには、このような会議を年に 1 回開催することは重要だが、それだけでは十分ではなく、メディア、学界、国会議員をパートナーとして確保する必要がある。 ➢ サイバーセキュリティのリーダーシップの文化を促進し、進化するサイバー攻撃に対抗することに重点を置いたリーダーシップを育成することが急務。従来のサイバー問題の捜査では、特別捜査班（SIT） が結成され、また秘密警察（SOG） が存在したが、サイバー問題、サイバー犯罪では、脆弱性を悪用されたサイバー状況に直面する個人が、冷静に対応できない可能性がある。したがって、サイバーセキュリティにおいては、個人を支援する法的支援が必要であり、それが人々に勇気を与え、このような犯罪に対する国民の士気を高める事にもつながる。	Vice President's Secretariat（インド副大統領事務局）	https://pib.gov.in/PressReleasePage.aspx?PRID=2033016

© 2023 Japanese Standards Association. All Rights Reserved.

経済産業省　基準認証政策課　御中

海外標準化動向調査（2月）

令和6年度エネルギー需給構造高度化基準認証推進事業費（我が国の国際標準化戦略を強化するための体制構築）
2025年2月1日

一般財団法人日本規格協会

ピックアップ：サイバーセキュリティ　(関連ニュース番号13)

トピック	シンガポールが、自主的な医療機器向けサイバーセキュリティラベル制度を開始した。
推進組織	シンガポールのサイバーセキュリティ庁（CSA）、保健省（MOH）、保健科学庁（HSA）、Synapxe

内容

ポイント

- **シンガポールは、CSAが他の機関と共同で医療機器向けにサイバーセキュリティラベリングスキーム［CLS(MD)］を開発。このスキームは、医療機器をサーバーセキュリティの機能・強度のレベルに応じて評価するもので、マルチ（複数）レベルのサイバーセキュリティラベル制度を医療機器向けに導入した世界初のアプローチである。**

背景

- シンガポールは、医療の先進的な取り組みを進めている国の一つ。医療におけるテクノロジーの統合が進む中、医療機器が病院や家庭のネットワークに接続される機会が増え、サイバーリスクが高まる可能性があるため、医療機器のサイバーセキュリティ保護を強化するための対策として、製造業者、業界団体とも連携し、このスキームを開発した。

概要

- シンガポールのサイバーセキュリティ庁（CSA）、保健省（MOH）、保健科学庁（HSA）、および Synapxe は共同で、医療機器向けサイバーセキュリティラベリングスキーム [CLS(MD)] を開発した。このCLS（MD）スキームでは、医療機器がサイバーセキュリティ機能の強度に応じて評価され、１から４までの4つののレベルにわたって、ラベルが付与される。レベルの数字が大きくなるほど、セキュリティ機能が強化されているため、消費者がデバイスを購入する前にそのデバイスの安全性を理解するのに役立つ。
- シンガポールでは現在、医療機器を輸入、流通、国内で販売する前に、保健科学庁（HSA） に登録し、サイバーセキュリティを含む規制要件を満たす必要があり、HSA のサイバーセキュリティ要件は、世界的な規制の調和を目指す国際医療機器規制当局フォーラム（IMDRF、※1）が定める推奨事項と一致している。
- このスキームは、メーカーにセキュリティバイデザインアプローチ（※2）を採用するよう奨励することで、医療機器のセキュリティ向上を目指す。これにより、消費者と医療提供者は、医療機器の購入および使用前に、そのようなデバイスのセキュリティについてより多くの情報に基づいた決定を下すことができる。
- CLS(MD)の立ち上げは、2023年10月から2024年7月までのサンドボックス(※3）フェーズを経てのもので、サンドボックスには、医療機器としてのソフトウェアなどの機器を製造する19社のメーカーから、4つのレベルすべてにわたって47件の申請があった。これらのメーカーから集められたフィードバックに基づいて、スキームの要件とプロセスが改良され、業界が要件を満たす方法をガイドするためのテンプレートを使用した申請プロセスと評価方法が開発された。

（※1）国際医療機器規制当局フォーラム(IMDRF)：国際的な医療機器規制の調和と収束を加速することを目指す世界中の医療機器規制当局の自主的なグループ
（※2）セキュリティ・バイ・デザイン(Security by Design)：IoT製品やシステム、ソフトウェア等について企画・設計段階からセキュリティ対策を組み込むアプローチのこと
（※3）サンドボックス　：セキュリティ技術において、外部から受け取ったプログラムを保護された領域で動作させることで、システムが不正に操作されるのを防ぐセキュリティ機構

出所：シンガポール政府機関CSAウェブサイト、https://www.csa.gov.sg/News-Events/Press-Releases/2024/launch-of-cybersecurity-labelling-scheme-for-medical-devicesなどの公開情報等に基づきJSAグループ作成。

© 2024 Japanese Standards Association. All Rights Reserved.

ピックアップ：サイバーセキュリティ　(関連ニュース番号14)

トピック	欧州委員会は、NIS2指令に基づき、重要な組織およびネットワークのサイバーセキュリティに関する実施規則を採択
推進組織	欧州委員会、EU加盟国など

内容

ポイント

- **サイバーセキュリティに関する実施規則（施行法）は、企業に課せられるセキュリティ要件を強化し、サプライチェーンとサプライヤー関係のセキュリティに対処するもの。**
- **報告義務を合理化し、国家当局に対するより厳格な監督措置と執行要件を導入し、EUレベルでのサイバー危機管理に関する情報共有と協力の強化に貢献する。**

背景

- サイバーセキュリティに関する最初のEU全体の法律であるNIS指令（2016年発効）は、ヨーロッパをデジタル時代に適合させるという主要な政策目標の一環として、その後改正の手続きを経て、2023年にNIS2指令が発効した。この指令に基づき、EU加盟国は2024年10月17日までにNIS2指令を国内法に転換する必要があったもの。

概要

- 欧州委員会は2024年10月17日、EU全域におけるサイバーセキュリティの高水準共通化措置に関する指令（NIS2指令）に基づく、重要な組織およびネットワークのサイバーセキュリティに関する最初の実施規則を採択した。この実施法は、サイバーセキュリティのリスク管理措置のほか、インシデントを重大とみなすべきケース、デジタルインフラおよびサービスを提供する企業が国家当局に報告すべきケースを詳述しており、欧州の重要なデジタルインフラのサイバーレジリエンスを高めるための大きな一歩である。
- NIS2 指令は、EU 全体で高いレベルのサイバーセキュリティを確保することを目的としており、公共電子通信サービス、ICTサービス管理、デジタルサービス、廃水および廃棄物管理、宇宙、医療、エネルギー、輸送、重要製品の製造、郵便および宅配便サービス、行政などのプロバイダーを含む、経済と社会にとって重要な分野で活動するあらゆる組織を対象とし、企業に課せられるセキュリティ要件を強化し、サプライチェーンとサプライヤー関係のセキュリティに対処する。
- また、実施規則の採択により、セイバーセキキュリティに関する報告義務の合理化と加盟国間の制裁制度の調和が図られ、EU全体でサイバーセキュリティに対するより統一されたアプローチが確保されることで、国家レベルおよびEU全体レベルでのサイバー危機管理に関する情報共有と協力の強化実現に繋がる。

出所:欧州委員会 https://digital-strategy.ec.europa.eu/en/news/new-rules-boost-cybersecurity-eus-critical-entities-and-networks 、その他の公開情報等に基づきJSAグループが作成。

© 2024 Japanese Standards Association. All Rights Reserved.

ピックアップ：サイバーセキュリティ　(関連ニュース番号27、14)

トピック	オーストラリアで「諜報機関及びその他の法律改正（サイバーセキュリティ）法2024」が発効
推進組織	オーストラリア信号局（ASD）

内容

ポイント

- **サイバーセキュリティ法2024に定められたサイバーセキュリティ情報の限定使用義務は、オーストラリア信号局（ASD）と自発的に共有されたサイバーセキュリティ情報、または影響を受ける組織の同意を得て ASD が取得または準備したサイバー セキュリティ情報が保護されることをさらに保証することを目的としている。**

背景

- この法案は、オーストラリアの2023～2030年のサイバーセキュリティ戦略に基づく7つのイニシアチブを実施することを目的とするサイバーセキュリティ立法パッケージ2024の一部であり、立法上のギャップを解消して、オーストラリアがサイバーセキュリティの世界的リーダーになるための施策の一環である。

概要

- オーストラリアで2024年11月29日、「諜報機関及びその他の法律改正（サイバーセキュリティ）法2024」が発効した。この法案は、サイバーセキュリティ法2024を含むサイバーセキュリティ立法パッケージの一部。サイバーセキュリティ法2024では、その他の重要法案とともに、国家サイバーセキュリティコーディネーターとオーストラリア信号局（ASD）に自主的に報告されたサイバーインシデント情報に対する限定的な使用義務が法制化された。限定使用義務は、ASD と自発的に共有されたサイバー セキュリティ情報、または影響を受ける組織の同意を得て ASD が取得または準備したサイバー セキュリティ情報が保護されることをさらに保証することを目的とするもの。
- サイバーセキュリティ法2024のその他の法案としては、スマートデバイスのセキュリティ基準を義務付ける大臣権限の付与、ランサムウェアやサイバー恐喝の支払いに関する報告義務の導入、重大なサイバーセキュリティインシデントに関する事後レビューを実施する委員会を設立する法案などがある。
- オーストラリアでサイバーセキュリティ法2024が発効したのと、ほぼ同じタイミングの2024年10月に、欧州でもNIS2指令に基づくサイバーセキュリティ実施規則が採択されており、この度のオーストラリアのサイバーセキュリティ情報に対する「限定的使用義務」は、EUの機密データを保護しながら情報共有を促進するというアプローチとほぼ一致。その他にも、この二つのサイバーセキュリティに関する法律には、重要なデジタルインフラとサービスの保護、サイバーセキュリティインシデント報告の重要性強調など共通する部分があり、これらの法制化の動向は、世界中で急速に深刻化するサイバーセキュリティの課題に対処すべく法制化の勢いが増していることを示している。

出所：オーストラリアASD https://www.cyber.gov.au/about-us/view-all-content/news-and-media/limited-use-obligation-now-law 、などの公開情報等に基づきJSAグループ作成。

© 2024 Japanese Standards Association. All Rights Reserved.

【サイバーセキュリティ】関連記事詳細（1/20）

番号	地域・国	情報記事・タイトル	発行日	要旨	情報源（機関・団体名／URL）	
1	国際	ISO/IEC JTC1/SC27（サイバーセキュリティ）について	2024/12/13	• ISOにおけるサイバーセキュリティに関する標準化は、IECとのジョイント委員会であるJTC1/SC27で行われている。議長国はドイツ、事務局はドイツ規格協会（DIN）が務める。国内の審議団体は、（一社）情報処理学会である。 • 2024年12月13日現在、開発済みの規格が242件、開発中の規格が68件ある。 • SC27のワーキンググループは以下のとおり。 ISO/IEC JTC 1/SC 27/AG 2　信頼性 ISO/IEC JTC 1/SC 27/AG 5　ストラテジー ISO/IEC JTC 1/SC 27/AG 6　オペレーション ISO/IEC JTC 1/SC 27/AG 7　コミュニケーションとアウトリーチ (AG-CO) ISO/IEC JTC 1/SC 27/AG 8　適合性評価に関する諮問グループ ISO/IEC JTC 1/SC 27/AG 9　多様性に関する諮問グループ ISO/IEC JTC 1/SC 27/AHG 1　決議案の作成 ISO/IEC JTC 1/SC 27/AHG 3　AI とビッグデータ (BD) におけるセキュリティとプライバシー ISO/IEC JTC 1/SC 27/CAG　議長の諮問グループ ISO/IEC JTC 1/SC 27/JWG 7　合同 ISO/IEC JTC1/SC 27 - ISO/IEC JTC1/SC 37 ワーキンググループ: 生体認証のサイバーセキュリティテストと評価 ISO/IEC JTC 1/SC 27/WG 1　情報セキュリティ管理体制 ISO/IEC JTC 1/SC 27/WG 2　暗号化とセキュリティのメカニズム ISO/IEC JTC 1/SC 27/WG 3　セキュリティの評価、テスト、仕様 ISO/IEC JTC 1/SC 27/WG 4　セキュリティ管理とサービス ISO/IEC JTC 1/SC 27/WG 5　アイデンティティ管理とプライバシーのテクノロジー • 別のTCとの共同作業グループとして以下がある。 ISO/TC 307/JWG 4　ISO/TC 307 - ISO/IEC JTC 1/SC 27 WG 共同: ブロックチェーンと DLT のセキュリティ、プライバシー、アイデンティティ	International Organization for Standardization（ISO）	https://www.iso.org/committee/45306.html

© 2023 Japanese Standards Association. All Rights Reserved.

【サイバーセキュリティ】関連記事詳細（2/20）

番号	地域・国	情報記事・タイトル	発行日	要旨	情報源（機関・団体名／URL）	
2	アメリカ	CISA と FBI が共同広告を発表し、2024 年の選挙期間中に起こり得る DDoS 攻撃について解説	2024/7/31	サイバーセキュリティ・インフラストラクチャセキュリティ庁 (CISA) と連邦捜査局 (FBI) は、2024 年の選挙サイクルに向けた一連の公共広告の一環として、「DDoS 攻撃は選挙情報へのアクセスを妨げる可能性があるが、投票を妨げることはない。」と共同で発表した。 この公共広告は、安全で安心な選挙を運営するために必要な情報を一般市民に提供し、選挙インフラストラクチャ コミュニティにサポートを提供するという、両機関の継続的な取り組みの一環である。 この出版物は、DDoS 攻撃とは何か、それが選挙インフラに与える影響、有権者への推奨事項、被害者の報告情報について一般の人々を啓蒙することを目的としている。	Cybersecurity and Infrastructure Security Agency (CISA)	https://www.cisa.gov/news-events/news/cisa-and-fbi-release-joint-psa-putting-potential-ddos-attacks-during-2024-election-cycle-context
3	アメリカ	CISA が Secure by Demand ガイドを公開	2024/8/6	サイバーセキュリティ・インフラストラクチャセキュリティ庁 (CISA) と連邦捜査局 (FBI) は、「Secure by Demand ガイド: ソフトウェア顧客が安全なテクノロジー エコシステムを推進する方法」を発表した。このガイドはソフトウェアを購入する組織にとって、設計によるセキュリティがソフトウェアメーカーのサイバーセキュリティへのアプローチをより深く理解するための主要な考慮事項の一つであることを保証する。 このガイドは、ソフトウェアを購入する際に尋ねるべき質問、調達ライフサイクルのさまざまな段階に製品セキュリティを統合するための考慮事項、および設計によるセキュリティの原則に沿って、製品セキュリティの成熟度を評価するためのリソースを組織に提供し、脅威の状況に基づいて分類された、一連のアクションを提供する。これらが正しく実行されると、ソフトウェア メーカーが悪用可能な欠陥や構成ミスを削減するアクションを実行していることが顧客に示されるため、顧客にとってより安全な製品になる。	Cybersecurity and Infrastructure Security Agency (CISA)	https://www.cisa.gov/news-events/news/cisa-releases-secure-demand-guide

© 2024 Japanese Standards Association. All Rights Reserved.

【サイバーセキュリティ】関連記事詳細（3/20）

番号	地域・国	情報記事・タイトル	発行日	要旨	情報源（機関・団体名／URL）	
4	アメリカ	CISA、サイバー報告の改善に向けた新ポータルを立ち上げ	2024/8/29	サイバーセキュリティおよびインフラストラクチャセキュリティ庁 (CISA) は、サイバーインシデント報告の改善に向けた継続的な取り組みの一環として、サイバーインシデント報告フォームを、新しいCISA サービスポータルに移行したことを発表した。 新ポータルは、login.gov（※） 認証情報との統合など、サイバーインシデント報告のための機能が強化された安全なプラットフォームで、新しいコラボレーション機能により、ユーザーは CISA と非公式に話し合うこともできる。 （※）login.gov：公共サービスへのアクセスを、サービス機関が違っても、同じユーザネーム、パスワードで行えるシングルサインオンの仕組み CISA は、インシデント報告者の報告プロセスをガイドするために、「自主的なサイバーインシデント報告リソース」もリリースした。これは、組織が「誰が」インシデントを報告すべきか、「なぜ、いつ」報告すべきか、「何をどのように報告すべきか」を理解するのに役立つ。	Cybersecurity and Infrastructure Security Agency (CISA)	https://www.cisa.gov/news-events/news/cisa-launches-new-portal-improve-cyber-reporting
5	オーストラリア	オーストラリア信号局（ASD）は、ロシア軍のサイバー戦術に関する新たな共同勧告を発表	2024/9/6	オーストラリア通信信号局（ASD）は、連邦捜査局（FBI）、サイバーセキュリティ・インフラストラクチャセキュリティ庁（CISA）などの国際パートナーと協力して、共同サイバーセキュリティ勧告「ロシア軍のサイバー攻撃者が米国と世界の重要インフラを標的に」を発表した。 この勧告では、ロシアのサイバー攻撃者が世界の重要なインフラに対してスパイ活動、破壊活動、評判の毀損を行うための戦術、技術、手順について概説している。ASDは、国際パートナーと共に、以下の行動を推奨する。 ・定期的なシステムアップデートの優先 ・悪用された既知の脆弱性の修正 ・悪意のある活動の拡散を防ぐためのネットワークセグメント化 ・ウェブメールや VPN などの外部向けサービスに対してフィッシング耐性のある 多要素認証（MFA、※）の有効化。 ・ASD の Essential Eight ガイダンスの実装 （※）多要素認証（MFA）：アプリケーション、オンラインアカウント、VPNなどのリソースへのアクセスを許可する前に、ユーザに2つ以上の認証要素の提供を求める認証方法	Australian Signals Directorate（ASD、オーストラリア通信信号局）	https://www.cyber.gov.au/about-us/view-all-content/news-and-media/new-joint-advisory-on-russian-military-cyber-tactics-released

© 2024 Japanese Standards Association. All Rights Reserved.

【サイバーセキュリティ】関連記事詳細（4/20）

番号	地域・国	情報記事・タイトル	発行日	要旨	情報源（機関・団体名／URL）	
6	中国	2024年国家サイバーセキュリティ啓発週間プロモーションビデオ「サイバーセキュリティは安心して暮らす」を公開	2024/9/8	9月9日から15日までの期間、2024年全国サイバーセキュリティ広報週間が全国で実施され、9月8日に、広州南沙市で2024年国家サイバーセキュリティ広報週間の開会式が開催された。そこで「サイバーセキュリティ、安全に暮らす」をテーマとしたカンファレンスのプロモーションビデオが正式に公開された。 プロモーションフィルムは、街の「灯台」を「守る」ためのものとして、ネットワークセキュリティとデジタル技術の双方向の発展のストーリーを伝えている。プロモーション ビデオでは、都市の誰もが精神的な故郷の守護者でもあり、より良い生活を一緒に築き、共有し、「サイバーセキュリティは人々のものであり、サイバーセキュリティは人々に依存する」という深い意味合いが込められている。広州はネットワークセキュリティ分野で継続的な革新と精力的な取り組みを追求し、デジタルチャイナの構築に向けた良好なエコシステムの構築に貢献している。	中央サイバーセキュリティ情報化委員会事務局	https://www.cac.gov.cn/2024-09/10/c_1727655115279580.htm
7	アメリカ	CISA、連邦政府機関のサイバーセキュリティ運用の優先順位を統一する計画を発表	2024/9/16	サイバーセキュリティおよびインフラストラクチャセキュリティ庁（CISA）は、連邦文民行政部門（FCEB）の「サイバーセキュリティ運用調整（FOCAL）プラン」を発表した。各FCEB機関には独自のミッションがあり、重要な業務を進めるために独立したネットワークとシステムアーキテクチャを備えている。この独立性は、機関ごとにサイバーリスクの許容度と戦略が異なることを意味する。ただし、サイバー セキュリティに対する共同アプローチにより、機関全体および各機関固有のリスクが軽減され、FOCAL プランではこれを実現することが概説されている。 FOCAL計画は、機関の指標と報告要件に一致する、①資産管理、②脆弱性管理、③防御可能なアーキテクチャ、④サイバー サプライ チェーン リスク管理、⑤インシデントの検出と対応の5つの優先分野に分かれている。これには、普遍的なサイバーセキュリティの課題への対処から、進化するセキュリティインシデントに対して耐性のある防御可能なアーキテクチャの構築を含む長期的な取り組みまで、さまざまな目標がある。 FOCAL計画はFCEB 機関向けに開発されたが、公共部門および民間部門の組織にとっても、企業のセキュリティ機能の調整を強化するための独自の計画を策定するためのロードマップとして役立つ。	Cybersecurity and Infrastructure Security Agency (CISA)	https://www.cisa.gov/news-events/news/cisa-releases-plan-align-operational-cybersecurity-priorities-federal-agencies

© 2024 Japanese Standards Association. All Rights Reserved.

【サイバーセキュリティ】関連記事詳細（5/20）

番号	地域・国	情報記事・タイトル	発行日	要旨	情報源（機関・団体名／URL）	
8	アメリカ	ODNI、FBI、CISA の共同声明	2024/9/18	国家情報長官室 (ODNI)、連邦捜査局 (FBI)、サイバーセキュリティ・インフラストラクチャセキュリティ庁 (CISA) は、「2024年8月19日のイランの選挙影響活動に関するODNI、FBI、CISAの共同声明」以来、FBIは不和を煽り米国選挙の結果を左右しようとするイランの活動についてさらなる詳細を把握した。」との声明を発表した。 この悪意あるサイバー活動は、8月の共同声明で指摘されているように、不和を煽り、選挙プロセスへの信頼を損なおうとするイランの多面的なアプローチの最新例。脅威対応のリーダーとして、FBIはこの活動を追跡し、被害者と連絡を取り、引き続き調査と情報収集を行い、責任ある脅威アクターを追跡して阻止する。11月が近づくにつれて、外国のアクターは選挙への影響活動を活発化させている。特に、ロシア、イラン、中国は、何らかの方法で、米国社会の分裂を自分たちの利益のために悪化させようとしており、選挙期間を脆弱な時期と見ている。 FBIとCISAは、選挙運動や選挙インフラの利害関係者に対し、疑わしい活動や犯罪行為に関する情報を、FBI現地事務所（https://www.fbi.gov/fieldoffices）、1-800-CALL-FBI（1-800-225-5324）、またはオンライン（ https://www.ic3.gov ）を通じて、地元の選挙犯罪コーディネーターに報告するよう奨励している。	Cybersecurity and Infrastructure Security Agency (CISA)	https://www.cisa.gov/news-events/news/joint-odni-fbi-and-cisa-statement

© 2024 Japanese Standards Association. All Rights Reserved.

【サイバーセキュリティ】関連記事詳細（6/20）

番号	地域・国	情報記事・タイトル	発行日	要旨	情報源（機関・団体名／URL）	
9	EU	欧州連合サイバーセキュリティ機関（ENISA）は、サイバーセキュリティの脅威予測に関する主要会議「Threathunt 2030」の2024年版をアテネで開催	2024/9/19	欧州サイバーセキュリティ機関（ENISA）が開催した「Threathunt 2030」会議では、2030年までのサイバー脅威の将来予測と対策が議論された。この会議では、地政学的状況の変化が新たな脅威主体と標的の出現に繋がっていること、AIや耐量子計算機暗号(PQC、※1)が新たなサイバー脅威を生み出す可能性、そして将来の脅威への備えとして、先見性と長期戦略的思考をサイバーセキュリティ枠組みに組み込む必要性などが強調された。 （※1）耐量子計算機暗号(PQC）：量子計算機が実用化されても、安全性を保つことができる暗号技術のこと。現在は量子計算機の性能が十分でないため暗号を破ることができなくても、その性能が向上した時点で解読を試みる攻撃が脅威と捉えられ始めている。 今回、「Threathunt 2030」の開催と同時期に、「ENISA脅威ランドスケープ2024レポート」が発行され、議論に大きく貢献した。分析を通じて特定されたサイバーセキュリティの脅威グループとして、ランサムウェアとマルウェア、ソーシャルエンジニアリング、データに対する脅威と可用性に対する脅威（DDoS攻撃、※2）、情報操作と干渉、サプライチェーン攻撃などが挙げられた。「ENISA脅威ランドスケープ2024レポート」には7つの主要なサイバーセキュリティの脅威が特定されるなど、公開されている数千件のサイバーセキュリティインシデントとイベントを分析し、それぞれの脅威について詳細な分析を行っている。 （※2）DDoS（Distributed Denial of Service）攻撃：攻撃対象となるWebサーバーなどに対し、複数のコンピューターから大量のパケットを送りつけることで、正常なサービス提供を妨げる行為	European Union Agency for Cybersecurity (ENISA)	https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024
10	イギリス アメリカ カナダ	英国、米国、カナダがサイバーセキュリティとAI研究で協力	2024/9/20	英国国防科学技術研究所（DSTL）、米国国防高等研究計画局（DARPA）、カナダ国防研究開発省（DRDC）は、人工知能（AI）、サイバーセキュリティ、レジリエントシステム、情報領域関連技術の研究、開発、試験、評価技術を共同で推進する三国協定に署名した。作成された方法論、アルゴリズム、機能、ツールは、現実世界の課題に焦点を当てた、新しい運用コンセプトの開発に活用される。 すでに進行中の研究プロジェクトの一つに、セキュリティテストおよび学習環境のためのサイバーエージェント（CASTLE）プログラム（※）があり、これは高度で持続的なサイバー脅威からネットワークを自律的に防御できるようAI を訓練するもの。その他にも、熟練したリソース豊富な敵からの攻撃に直面しても信頼できるAIシステムを定義および作成する研究や、ソフトウェアの迅速な認証など、より回復力とセキュリティの高いシステムを実現するツールや技術を開発する研究などがある。 （※）サイバーエージェント（CASTLE）プログラム：現実的なネットワーク環境をインスタンス化し、高度な持続的サイバー脅威（APT）から防御できるように AIエージェントをトレーニングするツール開発プログラム	GOV.UK	https://www.gov.uk/government/news/uk-us-and-canada-to-collaborate-on-cybersecurity-and-ai-research

© 2024 Japanese Standards Association. All Rights Reserved.

【サイバーセキュリティ】関連記事詳細（7/20）

番号	地域・国	情報記事・タイトル	発行日	要旨	情報源（機関・団体名／URL）	
11	アメリカ	CISAとFBI、米国の民主制度を弱体化させる、イラン国家支援のサイバー活動について警告	2024/10/8	サイバーセキュリティ・インフラストラクチャセキュリティ庁 (CISA) と連邦捜査局 (FBI) は、「国家政治組織に関連するアカウントに対するイランの攻撃から身を守る方法」というファクトシートを公開した。イスラム革命防衛隊 (IRGC、※) に所属するアクターは、電子メールやチャット アプリケーションでソーシャル エンジニアリングの手法を使用しており、おそらく不和を煽り、米国の民主的制度に対する信頼を損なおうとしていると思われる。 IRGC の攻撃者は、特に米国人の個人アカウントやビジネス アカウントを標的にし、侵害している。特に、国家政治組織に関係する個人。また、イランや中東情勢に関連する問題に取り組んでいる、または取り組んでいた個人や組織も標的にしている。 CISA と FBI は、アプリケーションとオペレーティング システムを最新の状態に保つこと、ビジネスには公式アカウントのみを使用するようにスタッフをトレーニングすること、フィッシング耐性のある多要素認証 (MFA、※) を実装することなど、組織や個人のセキュリティと回復力を強化するのに役立つ緩和策とベスト プラクティスを推奨している。 （※）イスラム革命防衛隊（IRGC）：イランの正式な軍隊の一部で、イラン国策の重要なツールであるテロ利用に中心的な役割を果たす。 （※）多要素認証 (MFA)：ユーザーが単なるパスワードよりも多くの情報を入力する必要がある複数ステップのアカウントログインプロセス。	Cybersecurity and Infrastructure Security Agency (CISA)	https://www.cisa.gov/news-events/news/cisa-and-fbi-warn-iranian-backed-cyber-activity-undermine-us-democratic-institutions

© 2024 Japanese Standards Association. All Rights Reserved.

【サイバーセキュリティ】関連記事詳細（8/20）

番号	地域・国	情報記事・タイトル	発行日	要旨	情報源（機関・団体名／URL）	
12	ヨーロッパ	欧州サイバーセキュリティチャレンジ(ECSC)2024で、ドイツが優勝し、イタリアが2位、ポーランドが3位となった。	2024/10/15	2024 年欧州サイバーセキュリティ チャレンジ (ECSC、※) は、EU サイバーセキュリティ機関 (ENISA) と欧州委員会の支援を受けて、イタリア国立サイバーセキュリティ機関 (ACN) と サイバーセキュリティ国立研究所(CINI)が主催し、2024 年10月8日から11日までトリノで開催された。EU加盟国と欧州自由貿易連合（EFTA）諸国を代表する合計31チームと、オーストラリア、カナダ、コスタリカ、コソボ、シンガポール、米国の6つの国際ゲストチームが参加した競技の結果は、1位: ドイツ、2位：イタリア、3位: ポーランドとなった。 （※）欧州サイバーセキュリティ チャレンジ (ECSC) ：ヨーロッパのサイバーセキュリティのトップ人材を集めてサイバーセキュリティの専門知識を養成することを目的とした ENISA の主要イニシアチブ。 ECSC では、ハードウェア タスク、Web およびモバイル セキュリティ、暗号化、リバース エンジニアリング、バイナリ エクスプロイト、フォレンジックなど、セキュリティ関連のさまざまな CTF チャレンジが 2 日間にわたって実施された。CINIの所長アレッサンドロ・アルマンド氏は、「ECSCは今回も、ヨーロッパ各地や海外から何百人もの優秀な人材を集め、サイバーセキュリティのさまざまな課題を解決してスキルを試すことに成功した。」と述べた。2025 年版のECSCは、2025年10月に、ポーランドのワルシャワで開催される。	European Union Agency for Cybersecurity (ENISA)	https://www.enisa.europa.eu/news/germany-wins-first-place-in-the-european-cybersecurity-challenge-2024

© 2024 Japanese Standards Association. All Rights Reserved.

【サイバーセキュリティ】関連記事詳細（9/20）

番号	地域・国	情報記事・タイトル	発行日	要旨	情報源（機関・団体名／URL）	
13	シンガポール	シンガポールの医療分野のサイバーセキュリティ強化を支援する取り組み	2024/10/16	シンガポールのサイバーセキュリティ庁（CSA）、保健省（MOH）、保健科学庁（HSA）、および Synapxe は共同で、医療機器向けサイバーセキュリティ ラベリング スキーム [CLS(MD)] を開発した。これは、医療機器をサイバーセキュリティ規定のレベルに応じて評価する自主的なスキーム。 シンガポールでは現在、医療機器を輸入、流通、国内で販売する前に、HSA に登録し、サイバーセキュリティを含む規制要件を満たす必要がある。HSA のサイバーセキュリティ要件は、国際的な医療機器規制当局のグループである国際医療機器規制当局フォーラムが定めた推奨事項と一致している。 シンガポールサイバーセキュリティ庁（CSA）が開発したこのスキームは、メーカーにセキュリティバイデザインアプローチ（※）を採用するよう奨励することで、医療機器のセキュリティを向上させることを目指す。これにより、消費者と医療提供者は、医療機器の購入および使用前に、そのようなデバイスのセキュリティについてより多くの情報に基づいた決定を下すことが可能となる。 （※）セキュリティ・バイ・デザイン(Security by Design)：IoT製品やシステム、ソフトウェア等について企画・設計段階からセキュリティ対策を組み込むアプローチのこと	Cyber Security Agency of Singapore (CSA)	https://www.csa.gov.sg/News-Events/Press-Releases/2024/launch-of-cybersecurity-labelling-scheme-for-medical-devices

© 2024 Japanese Standards Association. All Rights Reserved.

【サイバーセキュリティ】関連記事詳細（10/20）

番号	地域・国	情報記事・タイトル	発行日	要旨	情報源（機関・団体名／URL）	
14	EU	欧州委員会が、EUの重要な組織とネットワークのサイバーセキュリティを強化するための新しい規則を採択した	2024/10/17	欧州委員会は10月17日、EU全域におけるサイバーセキュリティの高水準共通化措置に関する指令（NIS2指令）に基づく、重要な組織およびネットワークのサイバーセキュリティに関する最初の実施規則を採択した。この実施法は、サイバーセキュリティのリスク管理措置のほか、インシデントを重大とみなすべきケース、デジタルインフラおよびサービスを提供する企業が国家当局に報告すべきケースを詳述している。採択された施行規則は、クラウド コンピューティング サービス プロバイダーなどのデジタルサービスを提供する特定のカテゴリの企業に適用される。施行法では、サービス プロバイダーの各カテゴリについて、インシデントが重大と見なされる場合も規定している。10月18日以降、すべての加盟国は、監督措置および執行措置を含むNIS2サイバーセキュリティ規則に準拠するために必要な措置を適用する必要がある。 サイバーセキュリティに関する最初のEU全体の法律であるNIS指令は2016年に発効し、欧州委員会は、2020年12月にNIS指令の改正を提案。2023年1月に発効した後、加盟国は2024年10月17日までにNIS2指令を国内法に転換する必要がある。NIS2 指令は、企業に課せられるセキュリティ要件を強化し、サプライチェーンとサプライヤー関係のセキュリティに対処する。報告義務を合理化し、国家当局に対するより厳格な監督措置とより厳格な執行要件を導入し、加盟国間の制裁制度の調和を目指す。	European Commission	https://ec.europa.eu/commission/presscorner/detail/en/ip_24_5342
15	EU	欧州連合サイバーセキュリティ機関 (ENISA) は、EUデジタル ID ウォレットの認証に関する特別作業部会を設立するための関心表明の呼びかけを開始した	2024/10/18	欧州連合サイバーセキュリティ機関 (ENISA) は、EUDI ウォレット（※）のサイバーセキュリティ認証スキームを準備する目的で、機関を支援するための専用の特別作業部会を設立する呼びかけを開始。EU デジタル ID ウォレットは、個人データを保護すると同時に、市民や企業がオンラインで ID を確認し、EU 全体で電子文書を共有するための便利な方法を提供する。 （※）EUDI ウォレット：ヨーロッパのすべての人に提供される、安全で信頼性が高く、プライベートなデジタル ID の制度。個人識別データと文書の保存、提示、共有を、すべて1つのアクセスしやすいアプリケーションで実現。 この関心表明の呼びかけにより、EUDI ウォレットスキームの準備を支援するための特別作業部会 (AHWG) が設立され、AHWG メンバーは、EUDI ウォレットの認証スキームの開発につながるすべてのプロジェクト フェーズで、会議に積極的に参加し、AHWG の作業に貢献することが期待される。既存の関連する認証スキーム、標準、技術仕様を考慮しながら、欧州デジタルアイデンティティフレームワーク（EDIF)の要件を満たすための検討が行われる。	European Union Agency for Cybersecurity (ENISA)	https://www.enisa.europa.eu/news/call-for-experts-join-the-enisa-ad-hoc-working-group-on-eu-digital-identity-wallets-cybersecurity-certification

© 2024 Japanese Standards Association. All Rights Reserved.

【サイバーセキュリティ】関連記事詳細（11/20）

番号	地域・国	情報記事・タイトル	発行日	要旨	情報源（機関・団体名／URL）	
16	アメリカ	CISA と USPIS が、選挙メールセキュリティに関する公共広告および選挙管理官向けビデオをリリース	2024/10/22	サイバーセキュリティ・インフラストラクチャセキュリティ庁（CISA）と米国郵政検査局（USPIS）が協力し、選挙郵便のセキュリティに関する公共広告 (PSA) と、選挙郵便に含まれる潜在的な有毒物質を安全に取り扱うための選挙管理官向けのトレーニングビデオを発表した。CISA は、選挙管理官が、選挙インフラストラクチャに対するさまざまなサイバーおよび物理的脅威から身を守るために必要なリソースを確保するための連邦政府の取り組みを主導し、USPIS は選挙郵便の安全で確実な配達と、潜在的に危険な郵便物から選挙管理官を保護する。 USPISは、以下の通り、選挙郵便の安全で確実な配達の確保に協力することを呼びかけた。①受信メールや送信メールをメールボックスに放置しない、②郵便物を長期間放置しない、③選挙郵便物を地元の郵便局に返送するか、郵便局員に直接手渡す、④投票用紙の受領または配達に問題があると思われる場合は、USPS に連絡する前に、地元の選挙事務所に連絡して投票用紙のステータスを確認するなど。	Cybersecurity and Infrastructure Security Agency (CISA)	https://www.cisa.gov/news-events/news/cisa-and-uspis-release-two-election-mail-security-resources
17	アメリカ	FBIとCISAによる通信業界を標的とした中国の活動に関する共同声明	2024/10/25	米国政府は、中華人民共和国と関係のある者による商用通信インフラへの不正アクセスを調査している。 FBI がこの分野を狙った特定の悪意ある活動を特定した後、FBI とサイバーセキュリティおよびインフラストラクチャセキュリティ庁 (CISA) は、影響を受けた企業に直ちに通知し、技術支援を提供し、他の潜在的な被害者を支援するために情報を迅速に共有した。調査は継続中であり、被害者である可能性があると考える組織は、地元の FBI支局または CISA に連絡することを推奨する。 米国政府機関は、この脅威を積極的に軽減するために協力しており、業界パートナーと連携して商用通信部門全体のサイバー防御を強化。	Cybersecurity and Infrastructure Security Agency (CISA)	https://www.cisa.gov/news-events/news/joint-statement-fbi-and-cisa-prc-activity-targeting-telecommunications

© 2024 Japanese Standards Association. All Rights Reserved.

【サイバーセキュリティ】関連記事詳細（12/20）

番号	地域・国	情報記事・タイトル	発行日	要旨	情報源（機関・団体名／URL）	
18	アメリカ	CISAが初の国際戦略計画を発表	2024/10/29	サイバーセキュリティ・インフラセキュリティ庁（CISA）は 、同庁として初となる 2025～2026年国際戦略計画を発表した。この計画は、重要インフラのセキュリティとレジリエンスに関する国家安全保障覚書に沿ったもの。 この計画では、米国と国際パートナーが直面する絶えず変化し、ダイナミックな課題に対処するために、CISA が達成しなければならない以下の3つの目標を概説している。 ①米国が依存する海外インフラの強靭性を強化する。 ②統合サイバー防衛を強化する。 ③国際活動の機関調整を統一する。	Cybersecurity and Infrastructure Security Agency (CISA)	https://www.cisa.gov/news-events/news/cisa-releases-its-first-ever-international-strategic-plan
19	アメリカ 中国	中華人民共和国（PRC）による商用通信インフラへの攻撃に関するFBIとCISAの共同声明	2024/11/13	中華人民共和国（PRC）による商用通信インフラへの攻撃に関する米国政府の継続的な調査により、広範かつ重大なサイバースパイ活動が明らかになった。 具体的には、中国関連の攻撃者が複数の通信会社のネットワークを侵害し、顧客の通話記録データの盗難、主に政府または政治活動に関与している限られた数の個人のプライベート通信の侵害、裁判所命令に基づく米国法執行機関の要請の対象となった特定の情報のコピーを可能にしたことなどが判明。 連邦捜査局 (FBI) とサイバーセキュリティおよびインフラストラクチャセキュリティ庁 (CISA) は、引き続き技術支援を提供し、他の潜在的な被害者を支援するために情報を迅速に共有し、商用通信セクター全体のサイバー防御を強化する取り組みを行っている。	Cybersecurity and Infrastructure Security Agency (CISA)	https://www.cisa.gov/news-events/news/joint-statement-fbi-and-cisa-peoples-republic-china-prc-targeting-commercial-telecommunications

© 2024 Japanese Standards Association. All Rights Reserved.

【サイバーセキュリティ】関連記事詳細（13/20）

番号	地域・国	情報記事・タイトル	発行日	要旨	情報源（機関・団体名／URL）	
20	オーストラリア	オーストラリア通信信号局（ASD）は、第5回ASDサイバー脅威レポート（ACTR）を発表	2024/11/20	オーストラリア通信信号局（ASD）は、第5回ASDサイバー脅威レポート（ACTR）を発表した。ACTRでは、オーストラリアの企業や組織、重要なインフラ、個人に影響を及ぼす最新のサイバー脅威を、詳しく説明されており、調査結果では、オーストラリアのネットワークが継続的に悪用されていることが浮き彫りになっている。 ASDは、サイバー脅威が広がり進化するスピードは速いため、個人や組織が単独ですべての脅威を効果的に防御することはむずかしく、国家規模での協力は、悪意のあるサイバー活動に対するオーストラリアの最大の強みの 1つとしている。	Australian Signals Directorate（ASD、オーストラリア通信信号局）	https://www.cyber.gov.au/about-us/view-all-content/news-and-media/australian-signals-directorate-releases-the-annual-cyber-threat-report-2023-24
21	中国	中国の浙江省烏鎮で、2024年世界インターネット会議烏鎮サミットサイバーセキュリティ技術開発と国際協力フォーラムが開催された	2024/11/21	11月21日、浙江省烏鎮で2024年世界インターネット会議烏鎮サミットサイバーセキュリティ技術開発・国際協力フォーラムが開催された。「善のためのインテリジェンス、人工知能のセキュリティリスクとガバナンス」をテーマとするこのフォーラムは、現在の人工知能関連のセキュリティとガバナンスの問題の解決策を模索し、オープンで公平かつ効果的なガバナンスメカニズムの構築を促進する。中国サイバースペース局副局長の王京濤氏と中国工程院院士の呉建平氏がフォーラムに出席し、講演した。 このフォーラムは、国家コンピューター ネットワーク緊急対応技術調整センター（CNCERT/CC）と中関村研究所（ZGC LAB）が主催し、エチオピア情報ネットワークセキュリティ省、国際電気通信連合、アラブ情報通信技術機関、アラブ首長国連邦コンピュータ緊急対応チーム、パキスタン情報セキュリティを含む多くの国際機関と国内外の有名企業の代表が、フォーラムのテーマに沿って基調講演を行い、国内外の経験と成功事例を共有し、各国・地域の人工知能セキュリティとガバナンスの最新動向について議論し、国際的な視点から人工知能とネットワークセキュリティの統合とイノベーションの機会と課題についての考察を探めた。 フォーラムにおいて、中国国家コンピューター ネットワーク緊急対応技術調整センター（CNCERT/CC)は、人工知能によるネットワークセキュリティ緊急対応能力の構築を促進する、「人工知能によるネットワークセキュリティ緊急対応協力イニシアティブ」を発表した。	中央サイバーセキュリティ情報化委員会事務局	https://www.cac.gov.cn/2024-11/21/c_1733880920271242.htm

© 2024 Japanese Standards Association. All Rights Reserved.

【サイバーセキュリティ】関連記事詳細（14/20）

番号	地域・国	情報記事・タイトル	発行日	要旨	情報源（機関・団体名／URL）	
22	EU	欧州連合サイバーセキュリティ機関 (ENISA) の最新レポートは、現在の EU サイバーセキュリティ フレームワーク、特に NIS 2 指令がサイバーセキュリティ投資と対象組織の全体的な成熟度に与える影響を評価	2024/11/22	欧州連合サイバーセキュリティ機関 (ENISA) は、11月22日にNIS投資レポート2024(第 5 版)を発表した。調査サンプルを拡張して、NIS2（※）の対象分野と事業体を含めるなど、以前のバージョンに比べて大幅に強化されている。主な内容は以下のとおり。 • 情報セキュリティは現在、EUのIT投資全体の9%を占めており、2022年から1.9ポイントの大幅な増加となり、パンデミック後のサイバーセキュリティ投資は2年連続で増加 • 情報セキュリティに専念する IT専従者 (FTE) の割合は、4 年連続で減少。企業全体の32%、中小企業の 59% が、特に技術的な専門知識を必要とするサイバーセキュリティ職の充足に苦労しており、企業全体の 89%が NIS2に準拠するために追加のスタッフが必要になると予想 • NIS2対象の新規セクターも既存セクターと同程度の投資を行っているものの、ポスト量子暗号など新興分野への投資は限定的であり、大多数の企業は、NIS 2への準拠のためにサイバーセキュリティ予算が一時的または恒久的に増加すると予想 • 企業全体の90%が、来年はサイバー攻撃が増加すると予想。一方で、74%の企業がサイバーセキュリティ対策を社内だけに集中させており、国家またはEU レベルの取り組みへの参加は少ない • NIS が既に対象としているセクターの企業は、サイバーセキュリティのガバナンス、リスク、コンプライアンスのさまざまな指標において、NIS2 が新たに対象とするセクターの企業よりも優れた成果を上げており、NIS 指令が既存セクターに与えたプラスの影響を強調 (※)NIS2：EU域内でサービスを提供する又は活動を行う中規模（従業員50名）以上の主要又は重要エンティティを対象にしたネットワーク通信システム指令。2022年12月に、①大幅な対象拡大、②サイバーセキュリティ・リスクマネジメントの強化、③インシデント報告内容・時限の明確化、④厳しい罰則金の観点で改正がなされ、2024年10月18日より施行。	European Union Agency for Cybersecurity (ENISA)	https://www.enisa.europa.eu/news/navigating-cybersecurity-investments-in-the-time-of-nis-2

© 2024 Japanese Standards Association. All Rights Reserved.

【サイバーセキュリティ】関連記事詳細（15/20）

番号	地域・国	情報記事・タイトル	発行日	要旨	情報源（機関・団体名／URL）	
23	韓国 アメリカ	韓国科学技術情報通信部、米国国土安全保障省（DHS）とサイバーセキュリティ分野の技術協力を強化	2024/11/27	韓国科学技術情報通信部は、米国国土安全保障部(DHS)とサイバーセキュリティ技術共同研究のための技術付属書(TA)を11月27日(水)に締結し、2つの技術に対する共同研究を開始すると発表した。2023年4月に、両国の大統領は、米国と韓国の同盟70周年を記念する首脳共同 声明の中で、「韓米間の戦略的サイバーセキュリティ協力枠組み(フレームワーク)」の構築を約束するなど、サイバーセキュリティ分野でも緊密な協力関係を続けている。 韓米間の戦略的サイバーセキュリティ協力枠組み(フレームワーク)のフォローアップとして、韓国科技通信部と米国国土安全保障省（DHS）は、「デジタル資産違法取引行為追跡技術」、「大規模群衆内の異常行動識別・追跡技術」など2つの技術に対する具体的な研究範囲、目的、両国間の課題配分、研究成果物に対する規定などを盛り込んだ技術付属書(TA)を締結した。 韓国のユ・サンイム科学技術情報通信部長官は、「全世界がデジタルで接続され、サイバー脅威はもはや一国だけの対応だけでは不十分であり、他の国との協力及び共助が不可欠」と述べた。	韓国科学技術情報通信部	https://www.msit.go.kr/bbs/view.do?sCode=user&mId=307&mPid=208&bbsSeqNo=94&nttSeqNo=3185176
24	アメリカ	CISA、NSA、FBI、国際パートナーが通信インフラ保護ガイドを公開	2024/12/3	サイバーセキュリティ・インフラストラクチャセキュリティ庁 (CISA)、国家安全保障局 (NSA)、連邦捜査局 (FBI) および国際パートナーは、共同ガイド「通信インフラストラクチャの可視性強化および強化ガイダンス」を公開した。 このガイドは、主要な世界的通信プロバイダーのネットワークを侵害した中華人民共和国 (PRC) 関連の脅威アクターから保護するためのベストプラクティスを示し、この推奨プラクティスは、ネットワークエンジニアと通信インフラストラクチャの防御者が、この広範かつ重大なサイバースパイ活動に対して可視性を強化し、ネットワークデバイスを強化するためのもの。 中華人民共和国（PRC）と関係のある脅威アクターは、機密データを侵害し、サイバースパイ活動を行うために商用通信プロバイダーを標的にしている。このガイダンスは通信インフラストラクチャセクター向けに調整されているが、オンプレミスのエンタープライズ機器を持つ組織にも適用される。CISA は、すべての重要なインフラストラクチャ組織にセキュリティのベストプラクティスを実装することを推奨する。	Cybersecurity and Infrastructure Security Agency (CISA)	https://www.cisa.gov/news-events/news/cisa-nsa-fbi-and-international-partners-publish-guide-protecting-communications-infrastructure

© 2024 Japanese Standards Association. All Rights Reserved.

【サイバーセキュリティ】関連記事詳細（16/20）

番号	地域・国	情報記事・タイトル	発行日	要旨	情報源（機関・団体名／URL）	
25	EU	欧州連合サイバーセキュリティ機関(ENISA) は、EUのサイバーセキュリティの現状に関する初の報告書を発表した。	2024/12/3	この2024年版 EUにおけるサイバーセキュリティの現状に関する報告書は、欧州連合サイバーセキュリティ機関 (ENISA)がNIS 2指令第18条に従い2年ごとに作成する、サイバーセキュリティの状況に関する報告書その中でENISAは、以下の6つの政策提言を行っている。 ① 欧州連合の機関、団体、および政府機関と各国の所管当局、および NIS2 指令の範囲内の組織に対する技術的および財政的支援を強化し、進化する EU サイバーセキュリティ ポリシー フレームワークの調和のとれた、包括的で、タイムリーで一貫した実装を確保 ② 大規模サイバーインシデントへの協調的対応のためのEUの青写真を改訂し、国家とEUの両方のサイバーセキュリティ能力を強化 ③ サイバーセキュリティトレーニングに対するEU共通のアプローチを確立し、将来のスキルニーズを特定し、スキルギャップに対処するためサイバーセキュリティスキルの欧州認証制度を確立することで、EUのサイバー人材を強化 ④ 公共部門と民間部門の両方が直面するサイバーセキュリティの課題に対処することを目的としたサプライチェーン セキュリティに関するEUの横断的な政策フレームワークを開発 ⑤ サイバー連帯法に基づいて設立される将来のサイバーセキュリティ緊急メカニズム（※）を活用して、EU全体のリスク評価を通じ特定された脆弱または敏感なセクターとリスクに焦点をあて、セクターの準備と回復力を強化 ⑥ 既存の政策イニシアチブを基盤として、国家の取り組みを調和させ、専門家と国民の間で共通の高いレベルのサイバーセキュリティ意識とサイバー衛生を達成 （※）サイバー緊急メカニズム：サイバーセキュリティインシデントへの備えと対応の改善を確実にする三つの分野からなる。①潜在的な脆弱性のテスト、②EU サイバーセキュリティ準備金の創設、③加盟国同士の相互援助の確保）	European Union Agency for Cybersecurity (ENISA)	https://www.enisa.europa.eu/news/eus-first-ever-report-on-the-state-of-cybersecurity-in-the-union

© 2024 Japanese Standards Association. All Rights Reserved.

【サイバーセキュリティ】関連記事詳細（17/20）

番号	地域・国	情報記事・タイトル	発行日	要旨	情報源（機関・団体名／URL）	
26	アメリカ	NIST が情報セキュリティの測定ガイド NIST SP 800-55 の第 1 巻と第 2 巻を公開	2024/12/4	米国国立標準技術研究所（NIST） は、次の内容を含む特別刊行物 (SP) 800-55「情報セキュリティの測定ガイド」の最終版を公開した。 SP 800-55v1、第1巻 ― 対策の特定と選択・ SP 800-55v2、第2巻 - 情報セキュリティ測定プログラムの開発 第 1 巻「対策の特定と選択」では、情報セキュリティ対策の開発、選択、優先順位付けに対する柔軟なアプローチが提供される。この巻では、定量的評価と定性評価の両方について検討し、データ分析手法、影響と可能性のモデリングに関する基本的なガイダンスを提供する。SP 800-55v1 の主な更新内容は次のとおり。 • 統計分析入門 • 情報技術の測定と分析に関連する用語の探求 • 対策文書、報告、データ品質、不確実性に関する新しい情報 • 対策の開発、テスト、検証、対策と評価結果の比較、対策の優先順位付け、可能性と影響のモデリングの使用、計量スケール、継続的な改善をサポートするための方法の評価に関する情報を含む、対策の選択と優先順位付けに関する詳細情報 第 2 巻「情報セキュリティ測定プログラムの開発」では、柔軟な方法論とワークフローが提供されている。SP 800-55v2 の主な更新内容は次のとおり。 • 情報セキュリティ測定プログラムの開発と実装のための新しいワークフロー • 測定プログラムの利点、プログラムの範囲、成功するプログラムの基礎、役割と責任、測定基準のプログラム的価値、測定のコミュニケーション、組織上の考慮事項、管理性、データ管理の懸念事項に関するセクションを拡張 NIST は、2025 年に専門家によるパネル会議を開催し、指標と測定に関する関心コミュニティも導入する予定。	National Institute of Standards and Technology (NIST、米国国立標準技術研究所)	https://csrc.nist.gov/News/2024/nist-releases-volumes-1-and-2-of-sp-800-55#

© 2024 Japanese Standards Association. All Rights Reserved.

【サイバーセキュリティ】関連記事詳細（18/20）

番号	地域・国	情報記事・タイトル	発行日	要旨	情報源（機関・団体名／URL）	
27	オーストラリア	「諜報機関及びその他の法律改正（サイバーセキュリティ）法2024」が発効	2024/12/10	2024年11月29日、「諜報機関及びその他の法律改正（サイバーセキュリティ）法2024」が法律として発効した。この法案は、サイバーセキュリティ法2024を含むサイバーセキュリティ立法パッケージの一部であり、国家サイバーセキュリティコーディネーターの限定的な使用義務を別途規定している。諜報機関およびその他の法律改正（サイバーセキュリティ法2024）は、第6部に新しい第1A項を追加することにより、オーストラリア通信信号局（ASD）の限定的な使用義務を法制化する。限定使用義務とは、ASD と自発的に共有されたサイバー セキュリティ情報、または影響を受ける組織の同意を得て ASD が取得または準備したサイバーセキュリティ情報が保護されることをさらに保証することを目的とするもの。 限定使用義務によって保護される情報は、特定の状況を除き、規制措置に使用したり、影響を受けた組織に対する民事または刑事訴訟の証拠として認められたりすることは出来ない。サイバーセキュリティの影響を受ける組織は、ASD による情報の使用制限を理解した上で、ASD に情報を提供することが出来る。組織からの情報の保護に対する信頼が高まることで、ASD がより迅速により多くの技術情報を受け取ることができるようになり、サイバー セキュリティに関するアドバイスと支援を向上させることができる。	Australian Signals Directorate（ASD、オーストラリア通信信号局）	https://www.cyber.gov.au/about-us/view-all-content/news-and-media/limited-use-obligation-now-law
28	EU	欧州のサイバー空間をより安全かつセキュアにするため、サイバーレジリエンス法が施行された	2024/12/10	2024年12月11日に、サイバーレジリエンス法が施行された。サイバーレジリエンス法(CRA)は 、デジタル要素を含む製品にサイバーセキュリティ要件を義務付ける初のEU法である。 この法律の中心となるのは、消費者にセキュリティの脆弱性を修正するソフトウェア アップデートを提供し、セキュリティ サポートを提供するという、製造業者に対する新しい義務。この法律で、サイバーリスクと製品セキュリティに関する透明性を高めることにより、消費者がEU市場において入手可能な製品について、より多くの情報に基づいて選択ができるようになる。なお、製品には、規制の要件に準拠していることを示す CE マークが付けられる。 サイバーレジリエンス法は 、2023年発効したNIS2サイバーセキュリティフレームワークを補完するものであり、デジタル化と接続化が進むヨーロッパのサイバーセキュリティを強化するためにEUが展開している一連の包括的対策の一部である。	European Commission	https://digital-strategy.ec.europa.eu/en/news/cyber-resilience-act-enters-force-make-europes-cyberspace-safer-and-more-secure

© 2024 Japanese Standards Association. All Rights Reserved.

【サイバーセキュリティ】関連記事詳細（19/20）

番号	地域・国	情報記事・タイトル	発行日	要旨	情報源（機関・団体名／URL）	
29	ドイツ	ドイツ連邦情報セキュリティ局（BSI）は、コネクテッド製品の市場監督を申請	2024/12/11	サイバーレジリエンス法（CRA）が発効し、この法的革新により、EU市場におけるコネクテッド製品のサイバーセキュリティの最低レベルが規定される。メーカーは現在、製品を新しい要件に適応させるまでに 36 か月の猶予が与えられている。CRA は製品情報に関する透明性を高め、最小限のサイバーセキュリティ要件への準拠を要求する。早ければ2026年9月までに、EUの製造業者は、自社のデジタル製品に関連して積極的に悪用された場合の脆弱性や重大なセキュリティインシデントを、ドイツ連邦情報セキュリティ局(BSI)のCSIRT（コンピュータセキュリティインシデント対応チーム）などの責任当局に報告する必要がある。 集中的で効率的な市場監視は、ネットワーク化された製品のセキュリティを確実に確保するため、デジタル消費者保護の不可欠な部分であり、EU内の競争条件の標準化に役立つが、ドイツでは、製造業者と小売業者が CRA で策定された要件を遵守することを保証する国家市場監視当局が明確になっていない。ドイツ連邦情報セキュリティ局（BSI）は、メーカーおよびその製品に対するCRAの要件が明確に記述および説明された技術ガイドライン「TR-03183」を策定し、これに対応する。	ドイツ連邦情報セキュリティ局（BSI）	https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2024/241211_Inkrafttreten-CRA.html

© 2024 Japanese Standards Association. All Rights Reserved.

【サイバーセキュリティ】関連記事詳細（20/20）

番号	地域・国	情報記事・タイトル	発行日	要旨	情報源（機関・団体名／URL）	
30	中国	2024年国家サイバーセキュリティ標準化技術委員会の第2回「標準週間」イベントが海口で開催された	2024/12/12	2024年12月8日から11日まで、2024年国家サイバーセキュリティ標準化技術委員会の第2回「標準週間」イベント（※）が海南省海口市で開催され、中国サイバースペース局副局長、サイバーセキュリティ標準委員会委員長の汪京濤氏、海南省党委員会常務委員会委員の王斌氏などが、本会議に出席し、演説を行った。 （※）「標準週間」イベント：サイバーセキュリティ標準委員会事務局、中国電子技術標準化研究院、海南省党委員会サイバースペース事務弁公室が共催し、人工知能セキュリティ標準の研究と応用、電子政府アプリケーションのセキュリティと標準などのセミナーを開催するもの。 サイバーセキュリティ標準委員会委員長の汪京濤氏は、演説の中で「サイバーセキュリティ標準委員会は、サイバーセキュリティ業務に関する習近平総書記の重要な指示と党中央第20期三中全会の精神を徹底的に研究し、サイバーセキュリティの標準化作業に取り組まなければならない。」と発言した。 サイバーセキュリティの標準化作業で取り組む事項は以下のとおり。 ① 国家的なネットワークセキュリティ防御システムを構築し、重要な情報インフラストラクチャの境界決定方法、セキュリティ保護能力指標システム、ネットワークセキュリティ製品の警報情報フォーマット、資産管理などの標準開発と実装を促進する ② データセキュリティのガバナンスと監督を支援するために、データ分類や階層的保護要件、個人情報保護コンプライアンス監査などの標準の開発を加速する ③ 「人工知能生成合成コンテンツ識別方法」などの新技術と新しいアプリケーションの安全かつ秩序ある開発を主導する ④ 標準を利用して、中国のネットワークセキュリティの国際的影響力を促進し、2025年下半期のSC27国際会議の成功に全力を尽くし、カンファレンスの組織化とカンファレンスの技術的な成果の二重の収穫を達成する	中央サイバーセキュリティ情報化委員会事務局	https://www.cac.gov.cn/2024-12/12/c_1735697530755124.htm

© 2024 Japanese Standards Association. All Rights Reserved.