2024 年 11 月 28 日
No.2024-049

EU のサイバーセキュリティ規制動向と日本への示唆

調査部　主席研究員　森口善正

《要　点》

- EU は、経済・社会のデジタル化と相互接続の進展、さらにはロシアによるウクライナ侵攻等を背景とするサイバー脅威の増大を背景に、企業に対するサイバーセキュリティ規制を強化しており、環境規制と同様、当該分野においても世界をリードする存在となっている。
- 具体的に EU は、2016 年 7 月に採択した「ネットワーク・情報システムのセキュリティに関する指令」（NIS 指令）を一段と強化する「NIS2 指令」を 2022 年 12 月に採択した（2023 年 1 月発効）。NIS2 指令は、NIS 指令よりも幅広い事業者を対象に、最低限のサイバーセキュリティ・リスク管理措置の実施や加盟国政府（CSIRT または所管官庁）への迅速なインシデント報告を義務づける。
- 2024 年 10 月には「サイバーレジリエンス法」（Cyber Resilience Act：CRA）を採択し（2024 年 12 月発効）、最低限のサイバーセキュリティ要件を満たさないデジタル製品（ハードウェア、ソフトウェア）の域内流通を 2027 年 12 月以降禁止する。
- EU の規制動向を踏まえると、日本への示唆として、①経済・社会に大きな影響を与え得る重要事業者に対する最低限のサイバーセキュリティ対策の義務づけ、②重要事業者に対する重大インシデント報告の義務づけ、③2025 年 3 月から運用が開始される IoT 製品のセキュリティラベリング制度（JC-STAR）に対する消費者や中小企業の認知度向上と将来的なラベル取得の義務づけ、の 3 点を指摘できる。
- 脆弱なサイバーセキュリティはもはや自組織だけの問題ではなく、消費者や取引先企業、地域社会・経済への悪影響、さらには国家安全保障上の懸念すら惹起させ得る。また、わが国経済・社会の DX を阻む大きな要因ともなり得る。それだけに、より幅広い重要事業者やデジタル製品の製造業者が、サイバーセキュリティの強化に向けて一定の社会的責任を果たしていくことが望まれる。
- 政府としても、サイバー脅威がますます高まるなか、企業の報告負担を軽減しつつ効率的、効果的なインシデント即応体制を構築するとともに、リソースに乏しい中小企業のコンプライアンスやサイバーセキュリティ・リスク管理を資金面やノウハウ面でこれまで以上に支援していく必要がある。

本件に関するご照会は、調査部・主席研究員・森口善正宛にお願いいたします。

Tel：080-4169-4499
Mail：moriguchi.yoshimasa@jri.co.jp

日本総研・調査部の「経済・政策情報メールマガジン」はこちらから登録できます。
https://www.jri.co.jp/company/business/research/mailmagazine/form/

１．はじめに

経済・社会のデジタル化と相互接続が急速に進展するなか、サイバー攻撃が大規模化、複雑化、巧妙化する傾向が顕著となっている。とりわけ、欧州ではロシアによるウクライナ侵攻を背景にサイバー脅威が増大していることもあり、EU は企業に対するサイバーセキュリティ規制を強化している。具体的に EU は、重要業種の幅広い事業者に対して、最低限のサイバーセキュリティ・リスク管理措置の実施や重大インシデントの加盟国政府（CSIRT[1]または所管官庁等）への迅速な報告を義務づけるほか、最低限のサイバーセキュリティ要件を満たさないデジタル製品の域内流通を 2027 年 12 月以降禁止する。

地政学的リスクが世界的に高まるなか、わが国として経済・社会の DX を一層推進するとともに、そのセキュリティとレジリエンスを確保していくためにも、経済・社会に大きな影響を及ぼし得る重要事業者や一定のデジタル製品における最低限のサイバーセキュリティの確保と、政府による重大インシデント情報の迅速な集約は不可欠である。そこで以下、EU の取り組みを整理し、日本への示唆を検討する。

２．EU におけるサイバーセキュリティ規制の強化

欧州委員会は 2020 年 12 月、①レジリエンス（強靭性）、技術的主権とリーダーシップの確保、②加盟国における予防、抑止、対応のための運用能力の構築、③グローバルで開かれたサイバー空間の推進という三つの課題に取り組むため、新たなサイバーセキュリティ戦略「The EU's Cybersecurity Strategy for the Digital Decade」を公表した。欧州委員会は、このなかで①の課題について、「サイバーセキュリティにおけるレジリエンスと産業・技術力の強化を確保するためには、必要なすべての規制、投資、政策手段を動員すべきである」と述べ、サイバーセキュリティ規制を強化していく方針を提示した。

これを受け、EU は 2022 年 12 月、2016 年 7 月に採択した「ネットワーク・情報システムのセキュリティに関する指令」（Directive on the Security of Network and Information Systems：NIS 指令）を一段と強化する NIS2 指令を採択した（2023 年 1 月発効）。2024 年 10 月には、「サイバーレジリエンス法」（Cyber Resilience Act：CRA）を採択した（2024 年 12 月発効）。これら EU 規制の概要は以下の通りである。

（1）NIS 指令をさらに強化する NIS2 指令

EU 域内がネットワークや情報システムで相互接続されるなか、事業者に求めるサイバーセキュリティ・リスク対策の水準やインシデントへの対処能力が加盟国によって大きく異なっていると、脆弱な企業等に対するサイバー攻撃を突破口として、域内のネットワーク・情報システム全体がサイバー脅威に晒されることになる。そこで EU は 2016 年 7 月、域内のネットワーク・情報システムのセキュリティ水準の向上を図るため、「ネットワーク・情報システムのセキュリティに関する指令」（Directive on the Security of Network and Information Systems：NIS 指令）を採択した（2016 年 8 月発効）。

NIS 指令は、①全加盟国が、ネットワーク・情報システムのセキュリティに関する国家戦略を採択するとともに、本指令の適用を監視する所管官庁とインシデントの防止・対応を担う CSIRT を

[1] セキュリティインシデント発生時に対応するチーム（Computer Security Incident Response Team）。ここでは加盟国が設立ないし指定した国レベルの CSIRT（National CSIRT）を指す。

指定すること、②加盟国間の戦略的協力や情報交換の支援・促進等を目的として加盟国、欧州委員会、欧州ネットワーク情報セキュリティ庁（ENISA）で構成される「協力グループ」と、インシデントに関する情報共有や対応支援を行う「CSIRTs ネットワーク」を設置すること、③「基幹サービス運営者」との「デジタルサービス提供者」[2]に対し、最低限の「セキュリティ要件」の実施とサービスの提供に影響を及ぼす重大インシデント[3]の所管官庁または CSIRT への報告義務を課すこと（図表 1）、等を定めた[4]。

（図表 1）NIS 指令の適用対象事業者

部門		サブセクター／業種
基幹サービス運営者（Operator of Essential Services）	エネルギー	電力、石油、ガス
	輸送	航空輸送・空港・管制、鉄道輸送、水運・港湾運営、道路交通管理・高度道路交通システム（ITS）運営
	銀行	
	金融市場インフラ	取引所、中央清算機関
	ヘルスケア	保健医療機関（病院、クリニックを含む）
	飲料水供給・配給	
	デジタルインフラ	インターネット相互接続点（IXP）、ドメインネームシステム（DNS）サービス提供者、トップレベルドメイン（TLD）名レジストリ
デジタルサービス提供者（Digital Service Provider）		オンラインマーケットプレイス オンライン検索エンジン クラウドコンピューティングサービス

（資料）EU NIS 指令を基に日本総合研究所作成
（注）基幹サービス運営者は、対象事業に従事し、かつ一定の基準を満たす事業者を加盟国政府が特定する。デジタルサービス提供者は、対象のデジタルサービスを提供する全事業者（小規模・零細企業は除く）。

NIS 指令について、欧州委員会は、加盟国および EU レベルでのサイバーセキュリティ協力の全体的な枠組みを提供したほか、多くの加盟国のサイバーセキュリティに対するマインドセットや制度・規制上のアプローチに大きな変化をもたらした、と評価している。もっとも、NIS 指令の適用対象企業の範囲やインシデント報告の期限や内容が明示されず、加盟国の裁量に委ねられた結果、①EU で事業を展開する企業のサイバーレジリエンスの水準が依然として低いままである、②加盟国や産業セクター間でレジリエンスの水準に大きなばらつきがある、③加盟国間の情報共有は限定的で、加盟国共同の状況認識の水準は低く、共同危機対応も欠如している、等の問題があるとする。そこで欧州委員会は 2020 年 12 月、NIS 指令を代替する NIS2 指令案を公表し、EU は 2022 年 11 月に同指令を採択した（2023 年 1 月発効）[5]。

NIS2 指令は、①NIS 指令よりも適用対象事業者を拡大したうえで、②これらの企業に最低限の「サイバーセキュリティ・リスク管理措置」の実施を義務づける。さらに、③「サービスの提供に重大な（significant）影響を及ぼすインシデント」が生じた際の加盟国の CSIRT または所管官庁

[2] オンラインマーケットプレイス、オンライン検索エンジン、クラウドコンピューティングサービスの 3 業種に従事する事業者が該当。
[3] 基幹サービス運営者については、「基幹サービスの継続性に重大な（significant）影響を及ぼすインシデント」、デジタルサービス提供者には「サービスの提供に相当程度の（substantial）影響を及ぼすインシデント」の報告を義務づけた。
[4] 基幹サービス運営者にはデジタルサービス提供者よりも厳しいセキュリティ対策が求められ、所管官庁による積極的な監督の対象となる。
[5] NIS2 指令と同日、重要事業者レジリエンス指令（CER 指令）が発効。CER 指令は、自然災害、テロ攻撃、内部脅威、破壊工作等、物理的な非サイバーの脅威に対する重要インフラのレジリエンスを強化するため、加盟国と重要事業者の義務を定める。

への報告を明確な報告期限とともに義務づける。同時に、④所管官庁による監督や義務違反企業に対する罰則を強化する[6]。

具体的に NIS2 指令は、NIS 指令の適用対象である「基幹サービス運営者」と「デジタルサービス提供者」という分類を、「基幹事業者」（essential entity）と「重要事業者」（important entity）という分類に変更し、業種や企業規模等に応じて NIS2 指令の適用対象事業者とした（小規模・零細企業は原則 NIS2 指令の対象外）（図表 2）[7]。その結果、EU 域内における NIS2 指令適用対象企業は約 16 万社と、NIS 指令の約 1 万 5,000 社から大幅に増加するとされる[8]。

（図表 2）NIS2 指令の適用対象事業者

	セクター	サブセクター／業種	大企業	中規模企業	小規模・零細企業
重要度の高いセクター（Sectors of High Criticality）	エネルギー	電力、地域冷暖房、石油、ガス、水素	基幹事業者	重要事業者	対象外
	交通・運輸	航空会社・空港運営・管制、鉄道、水運・港湾、道路管理運営	基幹事業者	重要事業者	対象外
	銀行		基幹事業者	重要事業者	対象外
	金融インフラ	取引所、中央清算機関	基幹事業者	重要事業者	対象外
	ヘルスケア	医療機関、医薬品研究・製造、医療機器製造	基幹事業者	重要事業者	対象外
	飲料水		基幹事業者	重要事業者	対象外
	下水道		基幹事業者	重要事業者	対象外
	デジタルインフラ	適格信託サービス、DNSサービス、TLD名登録	基幹事業者	基幹事業者	基幹事業者
		公衆電子通信ネットワーク提供者	基幹事業者	基幹事業者	重要事業者
		非適格信託サービス提供者	基幹事業者	重要事業者	重要事業者
		IXP、クラウドコンピューティング、データセンター、コンテンツデリバリーネットワーク	基幹事業者	重要事業者	対象外
	ICTサービス管理(BtoB)	マネージドサービス、マネージドセキュリティサービス	基幹事業者	重要事業者	対象外
	行政	中央政府	基幹事業者	基幹事業者	基幹事業者
		地方政府	重要事業者	重要事業者	重要事業者
	宇宙	宇宙ベースサービスの提供を支援する地上インフラ運営者	基幹事業者	重要事業者	対象外
その他の重要なセクター（Other Critical Sectors）	郵便・宅配便		重要事業者	重要事業者	対象外
	廃棄物管理		重要事業者	重要事業者	対象外
	化学品製造・流通		重要事業者	重要事業者	対象外
	食品製造・加工・流通		重要事業者	重要事業者	対象外
	製造業	医療機器、コンピュータ・電子・光学機器、電気設備、機械設備、自動車、その他輸送機器	重要事業者	重要事業者	対象外
	デジタルプロバイダー	オンラインマーケットプレイス、インターネット検索エンジン、SNSプラットフォーム	重要事業者	重要事業者	対象外
	研究機関	（除く教育機関）	重要事業者	重要事業者	対象外

（資料）ベルギーの NIS2 法（2024 年 4 月成立、10 月施行）を基に日本総合研究所作成

（注）「小規模・零細企業」は、①従業員 50 人未満、かつ、②年間売上高 1,000 万ユーロ以下もしくは年間貸借対照表合計 1,000 万ユーロ以下の要件を満たす企業（EU 基準）。この基準のいずれかを上回る企業は中規模企業ないしは大企業に分類される。したがって、日本において中小企業とされる企業であっても NIS2 指令の適用対象となり得ることに注意が必要。

そのうえで NIS2 指令は、これら対象事業者に最低限の「サイバーセキュリティ・リスク管理措置」として 10 項目の対策の実施を義務づける（図表 3）。もっとも、事業者ごとに実施すべき措置は異なることから、NIS2 指令は管理措置を詳細に規定することは避けている[9]。

---

[6] その他、NIS2 指令は、国境を越えるような大規模サイバーセキュリティ・インシデントと危機の管理を強化するため、加盟国に「サイバー危機管理当局」の指定・設立を義務づけるとともに、その協力ネットワークとして ENISA が事務局を務める「欧州サイバー危機連絡機関ネットワーク」（EU CyCLONe）の構築を規定する。EU CyCLONe は、インシデントに技術面で対応する CSIRTs ネットワーク（事務局：ENISA）と協力し、大規模インシデントや危機の運用面における協調的管理の支援、加盟国・EU 機関間の情報共有、政治レベルの意思決定支援等に従事する。

[7] 加盟国は国内立法を通じて対象業種を独自に追加することが可能。

[8] NIS2 指令は、加盟国に対し、2025 年 4 月までに適用対象事業者のリストを作成するよう義務づける。

[9] 改正前の NIS 指令は、「基幹サービス運営者は、使用するネットワーク・情報システムのセキュリティに対するリスクに対処するため、適切かつ均衡の取れた技術的および組織的措置を講じなければならない。当該措置は、最新技術を考慮して、リスクに対して適切なネットワーク・情報システムのセキュリティ水準を確保するものでなけれ

また、「サービスの提供に重大な（significant）影響を及ぼすインシデント」の発生に適用対象事業者が気づいた場合、24 時間以内に「早期警告」を、72 時間以内に「インシデント通知」を、「インシデント通知」から 1 カ月以内に「最終報告」を加盟国の CSIRT または所管官庁に提出するよう義務づけ、報告期限を明確化する（図表 3）。

（図表3）NIS2指令の適用対象事業者の義務

サイバーセキュリティ・リスク管理措置の実施義務	重大インシデントの報告義務
対象事業者は、オールハザードアプローチに基づき、適切かつ相応の技術的、運用上、および組織的な措置をとる。措置には、少なくとも以下のものを含む。 ①リスク分析と情報システムセキュリティに関する指針 ②インシデント対応 ③バックアップ管理や災害復旧、危機管理等の事業継続 ④直接サプライヤーやサービスプロバイダーとの関係におけるサプライチェーン・セキュリティ ⑤ネットワークや情報システムの取得・開発・保守におけるセキュリティ（脆弱性への対処や脆弱性開示を含む） ⑥サイバーセキュリティ・リスク管理措置の有効性を評価するための指針と手続き ⑦基本的なサイバー衛生実務とサイバーセキュリティ・トレーニング ⑧暗号の使用に関する指針と手順 ⑨人的資源のセキュリティ、アクセス管理指針および資産管理 ⑩多要素認証もしくは継続的認証、安全な音声・ビデオ・テキスト通信、緊急内部通信システムの使用	対象事業者は重大なインシデントが発生した場合、加盟国のCSIRTもしくは所管官庁に遅滞なく報告する義務を負う。報告のタイミング、内容は以下の通り。 ①重大なインシデントに気づいてから24時間以内に、違法または悪意ある行為によるものか、クロスボーダーの影響を及ぼす可能性があるのか、という点を含む「早期警告」を報告 ②重大なインシデントに気づいてから72時間以内に、早期警戒情報の更新、重大度や影響の大きさ等の初期評価を含む「インシデント通知」を報告 ③CSIRTまたは所管官庁の要請に基づき「中間報告」を提出 ④インシデント通知から1カ月以内に、インシデントの詳細な説明、脅威のタイプや根本原因、適用された軽減措置、クロスボーダー影響等を含む「最終報告」を提出 ⑤インシデント通知から1カ月時点でインシデントが進行中の場合は、「進捗報告」を提出し、インシデントの処理から1カ月以内に「最終報告」を提出

（資料）NIS2指令を基に日本総合研究所作成

NIS2 指令の適用対象となる「基幹事業者」と「重要事業者」の差異は、当局による監督措置と執行措置の違いにある。具体的に、「基幹事業者」に対しては、監督当局が包括的な事前・事後の監督（オンサイト検査、オフサイト監督を行うほか、定期的もしくはアドホック（臨時）なセキュリティ監査等）を行う。これに対し「重要事業者」に対しては、義務を遵守していないという証拠、表示、情報が提供された場合に事後的に監督（オンサイト検査、オフサイト監督等）を実施する。

NIS2 指令の義務に違反する事業者に対しては、監督当局が是正命令を発出したり、制裁金を科したりすることができる。制裁金の最高額は、「基幹事業者」の場合、1,000 万ユーロ、または世界全体の年間売上高の 2.0%のいずれか高い方、「重要事業者」の場合は、700 万ユーロ、または世界全体の年間売上高の 1.4%のいずれか高い方となっている。

NIS2 指令は加盟国に 2024 年 10 月までの国内立法化を求めており、ベルギーは国内立法として NIS2 法を 2024 年 4 月に成立させた（2024 年 10 月施行）。ベルギー政府は適用対象事業者に対し政府ポータルサイトへの登録を義務づけたうえで、2024 年 10 月よりサイバーセキュリティ・リスク管理措置の実施と重大インシデントのベルギー・サイバーセキュリティセンター（CCB）への報告義務づけを開始した。基幹事業者に対する監督については段階的に強化していくこととしている。

ばならない」と規定するにとどまっていた。

これに対し、ドイツやフランス等の EU 主要国の国内立法は遅れている。ドイツ政府は 2024 年 7 月、「NIS-2 実施およびサイバーセキュリティ強化法」（NIS2UmsuCG）草案を公表したものの、法案の成立は 2025 年初頭を見込んでいる。NIS2UmsuCG は約 3 万の事業者に対しサイバーセキュリティ・リスク管理措置の実施と重大インシデントのドイツ連邦情報セキュリティ庁（BSI）への報告義務を課す予定である。

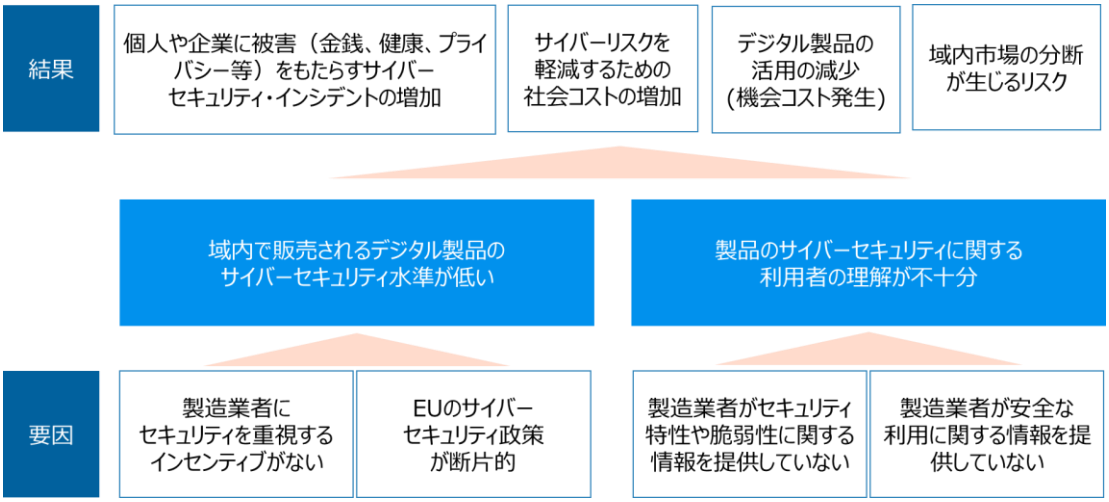
NIS2 指令は NIS 指令同様、加盟国がより厳しい規定を定めることを許容しているため、各国の規制が細部において異なり、その結果、域内に多数の子会社を有する多国籍企業にとっては規制遵守が複雑なものとなり、国際競争力を削ぎかねない、との批判がなされている。また、適用対象企業とサプライチェーンでつながる小規模・零細企業に対する支援も大きな課題となっており、各国政府は、財政面やノウハウ面から支援を行うことで、小規模・零細企業におけるサイバーセキュリティの強化を支援していく方針である。

（２）サイバーレジリエンス法（CRA）によるセキュリティ要件を満たさないデジタル製品の流通禁止

欧州委員会は 2022 年 9 月、最低限のサイバーセキュリティ要件を満たさないデジタル製品（ハードウェアやソフトウェア）の域内流通を禁止する「サイバーレジリエンス法」（Cyber Resilience Act：CRA）を提案し、2024 年 10 月に採択された（2024 年 12 月発効）[10]。CRA の適用開始は、デジタル製品の製造業者等に対応のための十分な時間を与えるため、発効の 3 年後（2027 年 12 月）となっているが、「実際に悪用された脆弱性（actively exploited vulnerability）」や「重大（severe）インシデント」に対する製造業者の報告義務については発効の 21 カ月後（2026 年 9 月）となっている。

CRA は、①域内で販売されるデジタル製品のサイバーセキュリティが脆弱であるにもかかわらず、多くの製造業者が脆弱性に対処するためのセキュリティ・アップデートを提供していない、②ほとんどの企業や消費者はデジタル製品の選択に際してサイバーセキュリティに関する十分で正確な情報を持っておらず、製品を適切に選択できていない、といった課題への対処を目的とする（図表 4）。

（図表 4）CRA 制定の背景となったデジタル製品の脆弱性を巡る問題



（資料）欧州委員会「COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT REPORT」（2022 年 9 月）を基に日本総合研究所作成

[10] CRA は指令（Directive）ではなく規則（Regulation）。加盟国内の立法手続を経ずに、直接適用される点で、加盟国による国内法制化が必要な指令よりも法的拘束力が強い。

欧州委員会は、こうした課題に対処するため、①従来通りガイダンスや推奨等を通じたソフトローで対応する、②特定の個別製品規制にサイバーセキュリティ規制を追加する、③ハードウェアのみを先行して規制し、その後ソフトウェアを規制する、④重要なデジタル製品（ハードウェアとソフトウェア）のみを規制する、⑤デジタル製品全般を規制する、という 5 つの政策オプションについて費用対効果を検討した。その結果、⑤のデジタル製品全般を規制する、という選択肢が、企業や市場監視当局の規制遵守コストを増加させ、短期的に製品価格の上昇をもたらす可能性がある一方で、サイバーインシデントの抑制やデジタル製品の活用進展等のメリットが最も大きいと結論づけた。

そこで CRA は、域内で流通する全てのデジタル製品に対して「サイバーセキュリティ必須要件」を満たすことを求め、要件を満たさないデジタル製品の市場流通を禁止する（図表 5）。サイバーセキュリティ必須要件は、①製品特性に関するセキュリティ要件（Cybersecurity requirements relating to the properties of products with digital elements）と、②製造業者による脆弱性対応要件（Vulnerability Handling Requirements）で構成される。製品特性に関するセキュリティ要件として、リスク対比適切な水準のサイバーセキュリティを確保するよう設計、開発、および製造されること（いわゆる Security by Design）やデフォルト状態でセキュリティ機能が備わっていること（Secure-by-Default）等を求める。また、製造業者による脆弱性対応要件として、製品に含まれる脆弱性とコンポーネント（部品）を文書化する、セキュリティ・アップデートにより脆弱性に遅滞なく対処、修復する、等の要件を満たすことを求める。

（図表 5）EU で流通するデジタル製品が満たすべき「サイバーセキュリティ必須要件」

デジタル製品特性に関するセキュリティ要件	製造業者による脆弱性対応要件
①リスク対比適切な水準のサイバーセキュリティを確保するよう設計、開発、製造されていること（Security by Design） ②サイバーセキュリティ・リスク評価に基づいて、デジタル製品が以下の要件を満たすこと ・既知の悪用可能な脆弱性（known exploitable vulnerabilities）が存在しない状態で提供されること ・デフォルト状態でセキュリティ機能が備わっていること（secure-by-default） ・自動セキュリティ・アップデート等、セキュリティ・アップデートを通じて脆弱性に対処できること ・認証や ID、アクセス管理システム、不正アクセス報告等で不正アクセスから保護されていること ・暗号化等を通じてデータ等の機密性（confidentiality）を保護すること ・データ等の完全性（integrity）を保護すること ・製品の目的との関連で適切で関連する必要最小限のデータのみを取り扱うこと ・不可欠で基本的な機能の可用性（availability）を保護すること ・デジタル製品や接続された製品による他の製品やネットワークへの影響を最小化すること	①製品に含まれる脆弱性とコンポーネント（部品）を特定して文書化すること（ソフトウェア部品表 <SBOM> の作成を含む） ②デジタル製品の脆弱性に対し、セキュリティ・アップデート等を通じて遅滞なく対処、修復すること ③デジタル製品のセキュリティに関する効果的で定期的なテストとレビューを実施すること ④セキュリティ・アップデートが利用可能になった時点で脆弱性に関する情報を公開すること（脆弱性の説明、影響を受けるデジタル製品を識別する情報、脆弱性の影響、深刻度、および脆弱性の修正に役立つ情報等） ⑤「協調的脆弱性開示」（Coordinated Vulnerability Disclosure）に関するポリシーを導入、実施する ⑥製品に含まれるサードパーティ・コンポーネントの潜在的な脆弱性に関する情報共有を促す措置を講じる ⑦脆弱性が迅速に修復、軽減されることを確保するため、セキュリティ・アップデートを安全に配布するメカニズムを提供する ⑧特定されたセキュリティ問題に対するセキュリティ・アップデートが利用可能な場合、ユーザーにアドバイスとともに遅滞なく無料で配布する

・攻撃対象領域を限定するよう設計、開発、製造されていること ・適切な軽減メカニズムや技術の採用を通じてインシデントの影響を低減させるよう設計、開発、製造されていること ・内部活動の記録や監視により、セキュリティ関連情報を提供すること（ただし、ユーザーにオプトアウトを付与） ・ユーザーがすべてのデータと設定を安全かつ簡単に恒久的に削除できること。データを他の製品やシステムに転送できる場合は安全な方法で行えること	

（資料）EU CRA を基に日本総合研究所作成

デジタル製品が CRA のサイバーセキュリティ必須要件を満たしていると評価される場合（適合性評価）、製造業者は EU 適合宣言書を作成し、「CE マーク」（図表 6）[11]を製品に貼付する。適合性評価の方式としては、デジタル製品の約 9 割が「通常の製品」に該当し、製造業者自身による自己適合宣言によって CE マークを付与できる。重要（important）ないしは極めて重要な（critical）製品については、第三者認証が求められる（図表 7）。

（図表 6）取得が義務づけられる EU の「CE マーク」

（資料）EU サイトより抜粋

（図表 7）製品分類と適合性評価方法

対象製品		概要	評価方式
通常の製品		下記以外のすべてのデジタル製品	自己適合宣言、第三者認証、
重要な（important）製品	Class1（低リスク）製品	ID・アクセス管理ソフト／ハードウェア、ネットワーク管理システム、OS、ルーター、モデム等	EUCC（10 頁参照）や EN 規格（11 頁参照）への適合、もしくは、第三者認証
	Class2（高リスク）製品	ファイヤーウォール、不正防止機能を備えたマイクロプロセッサ等	第三者認証
極めて重要な（critical）製品		セキュリティボックスを含むハードウェア製品、スマートメーターシステム、スマートカード等	

（資料）EU CRA を基に日本総合研究所作成

CRA はサイバーセキュリティ必須要件を満たさないデジタル製品の域内流通を禁止するのみならず、デジタル製品の製造業者や輸入業者、販売業者に対しても一定の義務を課す。具体的に、製造業者に対しては、①デジタル製品を市場に投入する際、当該製品の「セキュリティ要件」に従って設計、開発、生産すること、②デジタル製品のサポート期間が終了するまで、製品の脆弱性に対し先述の「製造業者の脆弱性対応要件」に従って効果的に対処すること、③市場投入前に「技術文書」[12]を作成すること、④市場投入後、製品がサイバーセキュリティ必須要件を満たしていないことを認識した場合、リコールや回収を含む必要な是正措置を迅速に講ずること、等の義務を列挙する。

さらに製造業者は、デジタル製品について「実際に悪用された脆弱性」や「デジタル製品のセキ

[11] 商品が EU 指令、基準をすべて満たしていることを示す基準適合マーク。CE マーク表示は強制。製品が、高い安全性、健康、環境保護の要件を満たしていると評価されていることを意味する。
[12] 技術文書の一部として、SBOM（ソフトウェア部品表）を含むデジタル製品の設計、開発、製造および脆弱性処理プロセスの説明が求められる。

ュリティに影響を与える重大（severe）インシデント」を認知した場合、24 時間以内に各国 CSIRT と ENISA に対し、新たに構築する「単一報告プラットフォーム」を通じて早期警戒通知を行うこと、等を義務づける（図表 8）。

（図表 8）製造業者の脆弱性やインシデントの報告義務

デジタル製品の脆弱性やインシデントの報告義務	①デジタル製品に「実際に悪用された脆弱性」（actively exploited vulnerability）に気づいた場合、指定された CSIRT と ENISA に対し単一の報告プラットフォームを通じて同時に報告する（24 時間以内に「早期警戒通知」、72 時間以内に「脆弱性通知」、是正・軽減措置が利用できるようになってから 14 日以内に「最終報告」を提出） ②デジタル製品のセキュリティに影響を与える重大な（severe）インシデントに気づいた場合、指定された CSIRT と ENISA に対し単一の報告プラットフォームを通じて同時に報告する（24 時間以内に「早期警戒通知」、72 時間以内に「インシデント通知」、インシデント通知から 1 カ月以内に「最終報告」を提出） ③デジタル製品のセキュリティに影響を与える「積極的に悪用された脆弱性」もしくは「重大インシデント」を認識後、影響を受けた利用者に対し、脆弱性やインシデントについて、必要な場合はそれらの影響を軽減できるリスク軽減・是正措置を通知する

（資料）EU CRA を基に日本総合研究所作成

製造業者の上記義務違反に対しては、加盟国の市場監視当局[13]が製造業者に対し不遵守を是正してリスクを排除することや、デジタル製品の販売禁止や制限、回収、リコールを命じることができる。さらに市場監視当局は、義務違反企業に対し、1,500 万ユーロもしくは全世界売上高の 2.5%のいずれか高い方を上限として制裁金を科すことができる（加盟国の国内法で規定）。

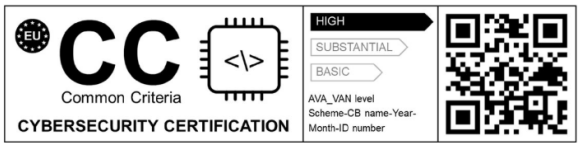
製造業者に対する義務づけは、CRA の発効から 3 年間猶予される[14]。日本企業が製造する EU 向けデジタル製品に対しても CRA の適用があるため、2027 年 12 月より開始される義務づけに向けて早い段階からサイバーセキュリティ対策を着実に進めていく必要がある。なお、CRA により ENISA の業務負担が増加することから、欧州議会、EU 理事会、欧州委員会は連名で ENISA の専門性を持つ人員の増員を図る方針で合意している。

また、CRA による最低限のサイバーセキュリティ・リスク管理措置の義務づけを補完するものとして、EU は ICT 製品を対象とするサイバーセキュリティ認証制度（EU Cybersecurity Certification：EUCC）を 2025 年 2 月よりスタートさせる[15]。

従来、欧州におけるサイバーセキュリティ認証は、各加盟国や業界主導のスキームとなっており、相互認証の仕組みはあっても、複数の認証の取得が事業者にコストの上昇をもたらすほか、各認証が求めるセキュリティ水準もまちまちとなっていた。そこで ENISA が ICT 製品について確立された国際基準に従って域内共通のセキュリティ認証基準を EUCC として開発した。

企業の認証取得は任意で、適合性評価は第三者認証による。基準への適合性が認められ

（図表 9）EUCC に基づき認証を受けた ICT 製品に添付されるマークとラベル



（資料）EUCC

[13] デジタル製品の CRA 適合性を評価・監視する責任を負う。
[14] 活発に悪用された脆弱性やインシデントに対する報告義務は CRA 発効の 21 カ月後に適用される。
[15] 2019 年 4 月に採択され同年 6 月に施行された「EU サイバーセキュリティ法」が定める「サイバーセキュリティ認証フレームワーク」に基づく認証制度。

れば「EUCC 証明書」が発行される。EUCC 認証書の保有者は、認証を受けた ICT 製品にマークとラベルを貼付することができる（前頁図表 9）。

（参考）消費者向けデジタル製品に最低限のサイバーセキュリティ要件を義務づける英国の PSTI 法

英国は 2023 年 9 月、「製品セキュリティおよび通信インフラストラクチャ法」（Product Security and Telecommunication Infrastructure Bill：PSTI 法）を制定し、2024 年 4 月に施行した。PSTI 法は、インタネットもしくはその他のネットワークに接続でき、デジタルデータを送受信できる消費者向け製品の製造業者や輸入業者、販売業者に対し、最低限の「サイバーセキュリティ要件」を製品に実装することを義務づける。

英国政府は 2018 年 10 月に「消費者向け IoT セキュリティのための自主的な行動規範」を公表し、消費者向け IoT 製品の製造業者に対して設計の段階から製品にセキュリティを組み込むよう促すとともに、欧州電気通信標準化協会（ETSI）と協力して、本行動規範の 13 の原則と一致する新しい技術規格 ETSI EN 303 645:Cyber Security for Consumer Internet of Things: Baseline Requirements を作成し、同規格の採用を業界に奨励した。もっとも、その後も製造業者による行動規範の遵守や同規格の採用が進まなかったため、英国政府が PSTI 法を提案したという経緯がある。

PSTI 法が義務づけるサイバーセキュリティ要件は、EU の CRA と比較すると非常に限定的で、現状、以下の 3 つの基本的な要件に絞られている。

①ユニバーサルデフォルトおよび簡単に推測できるパスワードの禁止

製品が単一の共通パスワード（ユニバーサル・デフォルト・パスワード）や「admin」等の容易に推測可能なパスワードをデフォルトで持つことを禁止する。個々の製品が推測されにくい固有のパスワードを有するか、もしくはユーザーがパスワードを設定できるようにする必要がある。

②セキュリティ問題のユーザーへの報告方法の公開

ユーザーがバグ等のセキュリティ問題を製造業者に報告できるよう、製造業者は自らの連絡先を提供する必要がある。また、問題報告の受領確認や報告された問題が解決されるまでの状況アップデートを報告者がいつ受け取るかを公開しなければならない。

③セキュリティ更新の提供期間に関する情報の公開

製造業者と小売業者は、セキュリティ更新プログラムが提供される最短の期間に関する情報を消費者に明確でアクセス可能かつ透明性のある方法で提供する必要がある。

PSTI 法のサイバーセキュリティ要件への適合評価は自己申告で行われ、第三者による監査や認証は不要となっている。しかし、対象製品の製造業者は、製品情報や製造業者の名前と住所、コンプライアンス宣言、セキュリティ更新プログラムの提供期間等を含む「コンプライアンス宣言書」（statement of compliance）を作成し、製品に添付する必要がある。輸入業者と販売業者は、コンプライアンス宣言書が添付されていない製品を流通させることはできない。

英国ビジネス貿易省の製品安全基準局（OPSS）は、PSTI 法に関し、業界にガイダンスを提供する一方、義務違反の製造業者や輸入業者、販売業者に対しては、販売停止やリコール等、製品が英国の消費者に提供されるのを防ぐためのすべての合理的な措置を講じることができる。さらに、OPSS は、義務違反の事業者に対し金銭的ペナルティを科すことができ、最高額は 1,000 万ポンド、または当該事業者の直近の会計年度の全世界総売上高の 4%のいずれか高い方となっている。

４．日本のサイバーセキュリティ規制への示唆

EU のサイバーセキュリティ規制動向を踏まえると、日本へのインプリケーションとして、以下の 3 点を指摘できる。

①重要事業者に対する最低限のサイバーセキュリティ対策の義務づけ

第一は、経済・社会に大きな影響を与え得る「重要事業者」に対して最低限のサイバーセキュリティ対策の実施を義務づけることである。

日本のサイバーセキュリティ基本法第 6 条は、「重要社会基盤事業者」（重要インフラ事業者）[16]の責務として、「そのサービスを安定的かつ適切に提供するため、サイバーセキュリティの重要性に関する関心と理解を深め、自主的かつ積極的にサイバーセキュリティの確保に努める」と規定されており、サイバーセキュリティの確保は、法的義務ではなく、努力義務として位置づけられている。実際、電気事業法の省令がサイバーセキュリティ実施義務を定める等の例外を除いて、最低限の実施義務は定められておらず、重要インフラ事業者に対しては、基本的に情報セキュリティ対策を盛り込んだ安全基準やガイドライン、監督指針等のソフトローに基づき所管省庁が監督し、個別・具体的な状況があれば行政処分の対象となるにとどまる。

しかし、近年の世界的な地政学的リスクの高まりとサイバー脅威の増大に鑑みると、重要インフラ事業者よりもより幅広い「重要事業者」を対象に、最低限のサイバーセキュリティ・リスク管理措置の実施を義務づけ、所管省庁等による事前ないしは事後監督の対象としていくことを検討すべきであろう[17]。

②重要事業者に対する重大インシデント報告の義務づけ

第二に、上述の重要事業者に対して重大インシデントの NISC への迅速かつ直接の報告を義務づけることである。

そもそもサイバー攻撃の標的となった事業者は、風評被害や顧客・株主の批判、監督官庁による行政処分、さらには新たな攻撃対象となることを恐れて、重大インシデントの報告や開示に消極的となりがちである。その結果として、サイバー脅威が迅速かつ正確に把握されないまま、被害を拡大させてしまう恐れがある。

この点、日本では、重要インフラ事業者等は、まず所管省庁に報告し、所管省庁が NISC に連絡する。そのうえで NISC は、所管省庁およびセプター[18]を経由して他の重要インフラ事業者等へ情報提供を行う[19]。しかし、個人情報保護法やマイナンバー法、その他一部業法に基づく報告義務等

---

16 国民生活および経済活動の基盤であって、その機能が停止・低下した場合に国民生活や経済活動に多大な影響を及ぼすおそれが生ずるものに関する事業を行う者。「重要インフラのサイバーセキュリティに係る行動計画」において「重要インフラ分野」として、情報通信、金融、航空、空港、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流、化学、クレジット、石油、港湾の 15 分野を特定。

17 2022 年 5 月に制定された経済安全保障推進法は基幹インフラの重要設備がサイバー攻撃等を受け、役務の安定的な提供が妨害されることを防止するため、「基幹インフラ役務の安定的な提供の確保に関する制度」を創設した。もっとも、重要設備の導入・維持管理などの委託時の対応であって、重要インフラのサイバーセキュリティ・リスク管理措置としては狭すぎる。また、同制度の対象となる特定社会基盤事業者（基幹インフラ事業者）については 15 の対象事業について所管大臣が指定することとしており、2024 年 9 月時点で 210 者と極めて限定的である。

18 重要インフラ事業者等の情報共有・分析機能および当該機能を担う組織。業界団体等が事務局となって全 15 分野で計 21 のセプターが活動している（2024 年 9 月末時点）。

19 個人データやマイナンバー等の漏洩といった法令等で報告が義務づけられているもインシデントについては、セプター経由で情報連絡元の匿名化等を行ったうえで所管省庁に報告することも可能。

を除き、事業者の報告はあくまで任意であり、報告期限も定められていない[20]。こうしたなかでは、NISC による迅速かつ一元的な情報集約にも限界があり、サイバー攻撃情報や脆弱性情報の速やかな周知と防護策の即時横展開に支障を来す。

既にみたように、EU では NIS2 指令が幅広い重要事業者に加盟国の CSIRT や所管官庁へのインシデント報告義務を課しているほか、米国においても 2022 年 3 月に「2022 年重要インフラに関するサイバーインシデント報告法」（CIRCIA）が超党派の賛成で成立し、幅広い重要事業者に対して重大インシデントの米国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）への速やかな報告を義務づけている（図表 10）[21]。英国も、NIS2 指令同様、従来のネットワーク・情報システム規制の適用対象事業者を拡大したうえで、より厳格なインシデント報告義務を課す「サイバーセキュリティ・レジリエンス法案」を 2025 年に議会に提出する予定としている[22]。

サイバー攻撃による国家安全保障上の懸念が高まり、国際的な情報連携も重視されるなかでは、日本においても、重要インフラ事業者よりもより幅広い重要事業者に対して重大インシデントの迅速な報告義務を課すとともに、NISC が事業者から直接、情報を集約し迅速に対策等を横展開できる体制を構築すべきであろう。その場合、NISC の体制強化も重要課題となる。

（図表 10）米国 CIRCIA によるインシデント報告の義務づけ（規制案ベース）

対象事業者	①16 の重要インフラセクターに属し、中小企業庁が指定する中小企業ではない事業者、もしくは ②各重要インフラセクターベースの基準に一つ以上合致している事業者
重要インフラセクター	化学、商業施設、通信、重要製造業、ダム、防衛産業基盤、緊急サービス、エネルギー、金融サービス、食品・農業、政府サービス・施設、ヘルスケア・公衆衛生、IT、原子炉・核物質・核廃棄物、交通システム、上下水道システム、
義務	①相当程度の（substantial）サイバーインシデント：認知して以降 72 時間以内に CISA に報告 ②身代金を支払った場合に支払いから 24 時間以内に CISA に報告 ③最大 1 年間のデータと記録を保持
実効性の確保	CISA に執行権限あり（情報提供要請、召喚状の発行、訴訟提起、入札停止） 虚偽の陳述・表明に対する罰則あり

（資料）CISA CIRCIA 報告要件規則案（2024 年 4 月公表）を基に日本総合研究所作成
（注）CISA は本規制案の適用対象事業者数を 316,000 と推定しており、事業者団体は対象が広過ぎると批判している。今後公表される最終規則において、適用対象事業者の範囲や報告を義務づけるインシデントの範囲を狭める可能性がある。

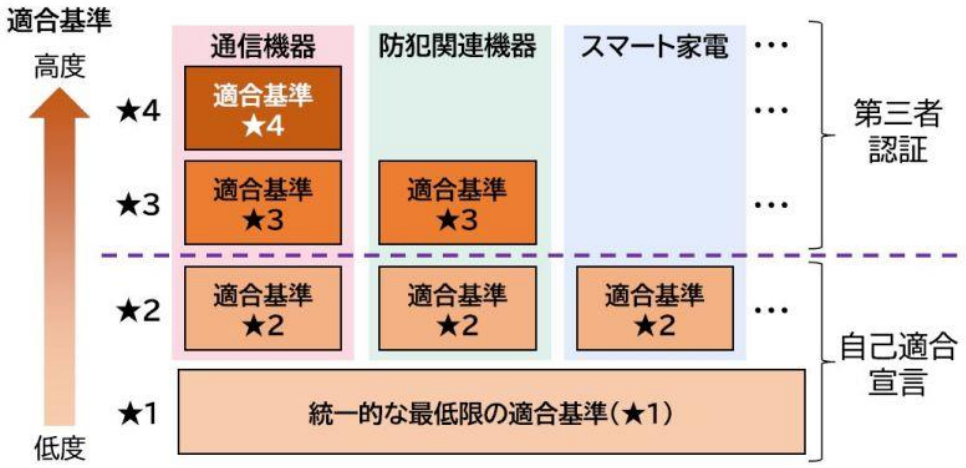
③日本の JC-STAR 制度に対する消費者や中小企業の認知度向上と将来的なラベル取得の義務づけ

第三に、EU の CRA や英国の PSTI 法と同様に、デジタル製品に最低限のサイバーセキュリティ要件を課し、サイバー攻撃に脆弱なデジタル製品を国内市場から排除することである。もっとも、わが国では、2025 年 3 月から IoT 製品の「セキュリティ要件適合評価及びラベリング制度（JC-STAR：Labeling Scheme based on Japan Cyber-Security Technical Assessment Requirements）」の運用が開始される予定となっていることを踏まえると、当該制度に対する消費者や中小企業の認知度向上が喫緊の課題といえる。

[20] 一部の法律、例えば、電気通信事業法第 28 条は事故報告制度を定め、通信の秘密の漏洩その他総務省令で定める重大な事故が生じたときは、その理由または原因とともに、遅滞なく総務大臣に報告する義務を課している。。
[21] 米国 SEC が 2023 年 12 月より適用を開始したサイバーセキュリティ開示規則は、上場企業に対し、インシデントを material（重要）と判断してから 4 営業日以内の適時開示を求める。これは投資家保護とインサイダー取引の防止を目的としたもので、CIRCIA の目的とは異なるものである。
[22] https://www.gov.uk/government/collections/cyber-security-and-resilience-bill

独立行政法人情報処理推進機構（IPA）が運用する JC-STAR 制度は、①求められるセキュリティ水準に応じたセキュリティ要件として、最低限の脅威に対抗するための製品共通の統一的な適合基準・評価手順（★1（レベル 1））と製品類型ごとの特徴に応じた適合基準・評価手順（★2（レベル 2）、★3（レベル 3）、★4（レベル 4））を設定する（図表 11）、そのうえで、②それぞれの基準に適合すると評価された IoT 製品に対し IPA が二次元バーコード付きの適合ラベルを付与し、製品詳細や適合評価、セキュリティ情報・問合せ先等の情報を調達企業や消費者が簡単に取得できるようにするものである。

（図表 11）JC-STAR 適合基準と評価方式



（資料）IPA ホームページより抜粋

JC-STAR 適合ラベルの取得は、あくまで IoT 製品の製造業者の任意に委ねられ、国内流通する IoT 製品が一定のセキュリティ要件を満たすことを強制力を持って義務づけられるわけではない[23]。その結果、EU の CRA や英国 PSTI 法制定に至る経緯にみられるように、JC-STAR 制度がスタートしても、消費者や中小企業が安全性を正しく判断して適合製品を購入するのではなく、比較的安価に流通する非適合製品を購入してしまう可能性は残る[24]。とすれば、とりわけ消費者や中小企業に対する JC-STAR 適合ラベルの周知徹底が強く求められる。脆弱な非適合製品の製造、流通が情報システムやネットワーク全体を脆弱にする可能性を踏まえれば、将来的には、市場における JC-STAR 制度の浸透度を踏まえたうえで、EU や英国と同様、国内に流通するすべての IoT 製品が統一的な最低限のセキュリティ要件を満たすよう、ラベル取得の義務づけを実施すべきである。

[23] 2024 年 7 月改定の NISC「政府機関等の対策基準策定のためのガイドライン（令和 5 年度版）」は、政府調達等における JC-STAR 制度の活用と、制度普及後の政府機関等によるラベル付与製品の調達必須化の方針を示す。
[24] 米国では、連邦通信委員会（FCC）がバイデン政権のイニシアチブに基づき新たな規則を制定し、消費者向けワイヤレス IoT 製品を対象とするサイバーセキュリティ・ラベリングプログラム「U.S. Cyber Trust Mark」の立ち上げを進めている。ラベルの取得は事業者の任意で適合性評価は第三者認証となっている。FCC は、ラベル取得を義務化しない理由として、リソースが限られる中小企業がラベルを取得しないリスクがあるものの、取得を任意とすることで利害関係者の関与と協力が得られやすいこと、製品の市場投入までの時間の短縮やリソースの効率的活用を図り得ること、さらには時間が経過すれば消費者がラベルの取得を求める可能性もあり、メリットがリスクを上回るとする。ただし、共和党が企業に対する規制負担の削減を重視しており、ねじれ議会の下、企業に対するラベル取得の義務化は困難という実情があったと考えられる。

４．おわりに

EU においては、サイバーセキュリティ規制の細部の運用が基本的に各加盟国に委ねられているため、加盟国によるまちまちな対応が欧州のネットワーク全体の脆弱化をもたらしやすい、という EU 特有の問題がある。さらに、ロシアのウクライナ侵攻を契機に、軍事攻撃と基幹インフラや経済・社会への非軍事的な攻撃を織り交ぜる、いわゆるハイブリッド攻撃に対する懸念も高まっている。こうしたなかで、EU がより幅広い事業者を対象とするサイバーセキュリティ規制を世界をリードする形で打ち出してきていることは理解できる。

日本においても、近年のサイバー攻撃の大規模化や巧妙化、組織化、さらにはアジアにおける地政学的リスクの高まりを踏まえると、脆弱なサイバーセキュリティはもはや自組織だけの問題ではなく、消費者や取引先企業、地域社会・経済への悪影響や、国家安全保障上の懸念すら生じさせる恐れがあるほか、経済・社会の DX を阻む大きな要因となりかねない。こうしたなかでは、重要事業者やデジタル製品（ハードウェア、ソフトウェア）の製造業者は、サイバーセキュリティの強化に向けて一定の社会的責任を果たしていくことが求められる。

同時に、政府としても、サイバー脅威がますます高まるなか、企業の報告負担を軽減しつつ効率的、効果的なインシデント即応体制を構築することが求められる。加えて、リソースに乏しい中小企業のコンプライアンスやサイバーセキュリティ・リスク管理を税制優遇や補助金、ガイダンスやノウハウの提供等を通じて、これまで以上に支援していく必要がある。

以　上

参考文献･HP 一覧

［1］EU NIS 指令（https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32016L1148）※国立国会図書館による解説あり（https://dl.ndl.go.jp/view/download/digidepo_11152345_po_02770001.pdf?contentNo=1）
［2］EU NIS2 指令（https://digital-strategy.ec.europa.eu/en/policies/nis2-directive）
※ベルギーNIS2 法（https://ccb.belgium.be/en/nis2）
［3］EU サイバーレジリエンス法（https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act）
［4］EU 理事会（閣僚理事会）「サイバーセキュリティの将来に関する理事会の結論：実装と保護の両立」（https://data.consilium.europa.eu/doc/document/ST-10133-2024-INIT/en/pdf）
［5］英国政府 PSTI 法（https://www.gov.uk/government/publications/the-uk-product-security-and-telecommunications-infrastructure-product-security-regime）
［6］米国 CISA：CIRSIA（https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia）
［7］内閣サイバーセキュリティセンター（NISC）:「サイバーセキュリティ 2024」（2024 年 7 月）（https://www.nisc.go.jp/pdf/policy/kihon-s/cs2024.pdf）
［8］情報処理推進機構（IPA）JC-STAR（https://www.ipa.go.jp/security/jc-star/index.html）
［9］内閣官房「サイバー安全保障分野での対応能力の向上に向けた有識者会議」（https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo/index.html）