一般財団法人 日欧産業協力センター　レポート
欧州デジタル政策　EU Policy Insights

Vol.7　2022 年 6 月
「サイバーセキュリティ政策の概要とその進捗」

■ 本資料は、当センターの公式見解を示すものではありません。
■ 本レポートの内容は別途記載がない限り執筆時点で入手している情報に基づくものであり、その後の状況変化や追加政策発表により変わる場合があります。
■ 本レポートへのご意見、取り上げて欲しいトピック等、お寄せください。
eujp-info@eu-japan.or.jp

一般財団法人 日欧産業協力センター
〒108-0072　東京都港区白金 1-27-6　白金高輪ステーションビル 4 階
TEL: 03-6408-0281　FAX: 03-6408-0283
E-MAIL : eujp-info@eu-japan.or.jp

1. サマリ

- EU のサイバーセキュリティに関する取り組みは、2004 年の欧州ネットワーク情報セキュリティ庁(ENISA)設立より着実に進み、近年は社会の急速なデジタル化やパンデミック、地政学的緊張の高まりにより加速。
- 2013 年に策定された旧サイバーセキュリティ戦略をベースとし、フォンデアライエン政権は 2020 年 12 月に新サイバーセキュリティ戦略を策定。幅広いデジタル製品を対象にサイバーセキュリティ認証の策定を進めつつ、2022 年 9 月には左記の認証を法定要件化することを可能としたサイバーレジリエンス法を提案するなど対策の強化を推進中。
- ウクライナ侵攻発生以降、欧州では重要インフラの守りに対する意識は更に高まっており、当面はインフラ分野を優先的に強化された標準や認証の策定が進む見込み。
- 長期的には欧州標準がグローバルデファクトする可能性も秘めており、関連する分野の国際標準も含め動向注視が重要。

2. EU のサイバーセキュリティ政策

1) これまでの経緯と背景

EU のサイバーセキュリティにおける取り組みは 2004 年の ENISA 創設以降、着実に進んできた。

2013 年には同分野初の包括戦略である EU サイバーセキュリティ戦略が採択され、2016 年にはネットワークおよび情報セキュリティ指令(NIS 指令)を施行、2019 年 6 月には ENISA の権限拡大とサイバーセキュリティ認証制度を柱としたサイバーセキュリティ法を施行するなど、ENISA を中核組織とし、EU 各加盟国における取組を支援してきた。

一方で近年、社会のデジタル化が急速に進み課題も生じてきた。あらゆる重要サービスやモノにおいてコネクテッド化・自律化が進展する中で、パンデミックがリモートワークを迫るなどデジタルツールやサービスへの依存度を高めたのは欧州においても同様である。

また地政学的要因も見逃せない。ロシアと国境を隔てる EU は、(特に旧共産政権の影響下にあった東欧諸国において)情報管理に対し高い感度を持つ。ほか、2016 年の中国家電大手によるドイツ産業用ロボット大手 KUKA 買収を契機に、先端技術の流出のみならず、5G・通信インフラを中心とした社会・経済・防衛インフラに対して中国が影響力を保持することに懸念を示すようになった。

このような要因を踏まえ、前ユンカー政権の時代より、サイバーセキュリティ対応力の強化や EU 全体としての統一運用などが課題として認識されてきた背景がある。

2) 新サイバーセキュリティ戦略

(1) 概要

こうした状況を受けてフォンデアライエン政権は、新デジタル戦略「欧州のデジタル未来の形成」に基づき、2020 年 12 月に新たなサイバーセキュリティ戦略を策定した。

目的は、欧州の価値観に沿ったサイバー脅威へのレジリエンス確保、市民と企業にデジタル技術の便益を確保することである。ほか、グローバルでオープンなインターネットの保護を実現するための国際協力も志向する。

この実現に向けて、それまでの旧サイバーセキュリティ戦略の取組みをベースとし更なる強化をめざすべく、新戦略では三つの柱と施策を掲げた。

表 1: 新サイバーセキュリティ戦略の 3 つの柱と主な施策

	施策
レジリエンス技術	• ネットワーク通信システム指令(NIS)の改定 • ICT 製品などのサイバーセキュリティ認証制度(EUCC など)の導入 • 欧州サイバーシールドとセキュリティオペレーションセンターの創設 • 自動車のサイバーセキュリティ対策（2022 年 7 月から自動運転車と車両ソフトウェアアップデート等について導入） • サイバーセキュリティのスキル強化
予防・防止・対応の運用能力強化	• EU ワイドのサイバー攻撃対策組織「共同サイバーユニット」の創設 • サイバー攻撃を防止、抑止、対応するための EU サイバー外交ツールボックスの強化
オープンなサイバースペースの確保	• サイバー空間の国際安全保障に取り組む新たな国連行動計画（POA： Programme of Action to Advance Responsible State Behaviour）の提唱 • 第三国、地域機関および国際機関とのサイバー対話の強化、サイバー防衛の互換性要件など、NATO との協力強化

出典: JETRO 資料「EU デジタル政策の最新概要」(2021 年 10 月)より抜粋

同戦略は現在も、EU のサイバーセキュリティに関する最新の戦略に位置付けられており、現在もこれに基づき各施策が進められている。その中で 2022 年 2 月の口

シアによるウクライナ侵攻発生以降、安全保障上の要請からサイバーセキュリティの重要性が増し、取り組みが加速している状況にある。

(2) 主な法令

新サイバーセキュリティ戦略に柱の中で、民間事業者と関連が深い主な法令は以下の通り。

表 2: 新サイバーセキュリティ戦略の関連法令

	主な適用対象	アプローチ	施行状況
NIS から NIS2 への改正	重要インフラ事業者	• スコープとなる重要インフラ事業を拡大 • 事業者に対し、強化されたセキュリティガバナンスの実施を義務付け	施行済
サイバーセキュリティ法	ENISA	• ENISA の権限・体制強化を規定 • ENISA に対し、デジタル製品のサイバーセキュリティ認証制度の策定を義務付け	施行済
サイバーレジリエンス法	デジタル要素を備えた全ての製品、及びその事業者	• 対象製品にセキュリティ要件への適合と CE マークの付与を義務化 • 事業者にインシデント発生時の当局への報告を義務化	未施行 (2022 年 9 月提案)
NLF (新たな法的枠組)	各分野の製品の製造業者	• 各分野の業法にてサイバーセキュリティを含む指定される認証の取得を義務付け	分野による
サイバーソリダリティー法	EU 加盟国のサイバーセキュリティ当局	• EU 当局のサイバー防衛力強化を目的に、EU 資金より 11 億€を投資し、官民でセキュリティ専門組織設立を設立	未施行 (2023 年 4 月提案)

うち、本稿ではサイバーセキュリティに主眼を置く法令である NIS/NIS2、サイバーセキュリティ法、サイバーレジリエンス法の概要を解説する。

a) サイバーセキュリティ法と認証制度

i. 概要

サイバーセキュリティ法とは、2019 年 6 月に初めて施行された EU 一律のサイバーセキュリティ認証の策定を促進することを目的とした EU 規則である。

背景として、元々は民間の認証機関が乱立し、ユーザーから見て認証の一貫性が保たれない課題があったのに対し、EU で統一された認証を確保すべく ENISA の権限の強化を図った上でこれにサイバーセキュリティ認証制度の策定を義務付け

たもの。これにより ENISA は、認証制度のドラフトを相次いで公開しており、実際に促進につながっている効果が認められる。

一方、本法は「ほかの EU 法令で規定されない限り認証の取得はあくまで任意」と定めており、本法自体は事業者などに対して認証の取得を迫る強制力を持たないことを注記しておく。

ii. 主な規定

認証の策定促進に向けて、本法はまず ENISA にセキュリティ管理体制に関する EU ガイドラインの策定やサイバーセキュリティ認証・標準化の整備・運用などを役割として新たに課したほか、マネジメントボードや恒久的な事務局の設置を規定するなど、EU ワイドの認証を策定する主体としての権限強化を定めた。

その上で ENISA に対し、ICT 製品やサービス及びその開発・提供行為をスコープとしたサイバーセキュリティ認証制度の枠組みの策定を義務づけた。このスコープは、IoT 製品やクラウド、5G などの通信インフラや AI が含まれるなど、非常に広範な製品・サービスに適用でき、広い分野の認証の策定を可能とする基本法的性格を有している。

また、スコープ下にある製品やサービスに対し、各認証が共通して確保すべきセキュリティ要件や保証レベル、各 EU 加盟国の評価機関や認証機関が担うべき役割や認証プロセスなどのガバナンスの枠組みを定めており、EU ワイドでの共通の基準や仕組みを示した。これにより、ある EU 加盟国において取得した認証が EU 全域で有効となるための素地を整える内容となっている。

iii. これまでに公開された主な認証

ICT 製品を対象とする認証として最初に具体化したものが、2020 年 7 月にドラフトが公開された EUCC (European Cybersecurity Certification Scheme for Common Criteria)である。

以降、2020 年 12 月にはクラウドサービスを対象とする EUCS – Cloud Services Scheme、2021 年には 5G の認証スキームのドラフトを公開するなど、着実に認証策定を進めている。

ENISA は認証策定を着実に進行

- **2019/6　サイバーセキュリティ法施行**
- **2020/7　EUCC 策定**
- **2020/12 クラウドペンタ認証スキーム**
- **2021/12 5G 認証スキーム策定**

重要インフラ分野を中心に拡大?

直近は 2023 年 5 月にサイバーセキュリティ監視サービス事業者への認証制度を提案した。また前述の通りウクライナ侵攻発生以降はインフラ保護の機運が高まっており、今後も安全保障上の要請の高い重要インフラ分野から優先的に認証制度が策定されるものと見込まれている。

(参考事例) ENISA：EUCS – Cloud Services Scheme の要件と保証レベル

認証取得するために満たすべき技術的要件(大項目)

No.	項目	No.	項目
1	情報セキュリティのための組織	11	ポータビリティ及び相互運用性
2	情報セキュリティポリシー	12	変更管理及び構成管理
3	リスクマネジメント	13	情報システムの開発
4	人的資源	14	調達管理
5	資産の管理	15	インシデント管理
6	物理的セキュリティ	16	事業継続
7	運用のセキュリティ	17	順守
8	ID、認証及びアクセス管理	18	ユーザードキュメント
9	暗号化及び鍵管理	19	政府機関からの調査依頼への対応
10	通信のセキュリティ	20	製品のセーフティ及びセキュリティ

3つの保証レベル

保証レベル	説明
high	**<対象> mission-criticalなデータ、システムを扱うサービス** <攻撃者プロファイル> 高度なスキルを持ったチーム <評価> substancialに加え、管理策の自動監視及び適切な要員によって実施される**複数年に渡り計画されるペンテストや技術的レビュー**
substantial	**<対象> business-criticalなデータ、システムを扱うサービス** <攻撃者プロファイル> 様々な既知のハッキング手法にアクセスできるが、リソースが限られている小さなチーム <評価> basicに加え、インタビューやサンプル検査、**設計どおり実装されているかの検証**を含むオンサイト監査、**既知の攻撃手法を使ったペンテスト**
basic	**<対象> 重要でないデータ、システムを扱うサービス** <攻撃者プロファイル> 限られたスキルのみを有し、限られたリソースにより既知の攻撃を繰り返す一人の人物 <評価> 事前定義された監査計画に沿った、技術的・組織的な措置(CSP自身による**自動化された既知の脆弱性やコンプライアンスに係る検査**を含む)の履行を確認するための**書類確認**

出典: 経産省資料「サイバーセキュリティに関連する海外の動き(2021 年 3 月)

b) NIS/NIS2

i. 概要

NIS とは、2016 年 8 月に重要インフラのセキュリティ強化を目的に初めて施行された EU 指令で、EU 域内の重要インフラ事業者に対しセキュリティガバナンスの強化と問題発生時の当局への報告義務などを定めたもの。NIS 自体は指令であることから、これに基づく国内法が各加盟国で整備され、2020 年には各国で運用が開始されている。

しかし一方で、EU 加盟国間でのセキュリティ対策の一貫性の欠如と社会のデジタル化の進展に伴う広い分野でのサイバー脅威の高まりを背景に、既存の NIS では対応できない、EU 全体で高い共通レベルのサイバーセキュリティ対策が求められる様になった。

これを受けて欧州委員会は、2020 年 12 月に NIS2 指令の改正を提案した。同改正案は、スコープの拡大と加盟国間での連携向上を主眼においている。対象分野の事業者にセキュリティリガバナンスの実施を引続き法定義務として求めつつ、罰則を設けられている点にも特徴がある。

改正案は、欧州議会と EU 理事会の審議を経て 2023 年 1 月に施行開始。各 EU

加盟国には施行時点から 21 ヶ月間の準備期間が設けられており、2024 年 10 月までに国内法の整備をすることが求められている。

現在は各加盟国が準備に取り組む状況となっている。

ii. 改正のポイント

ポイントは、社会インフラ分野のみを対象としていた NIS よりスコープを拡大した点だ。経済・社会的観点から極めて高い重要性を持つ必須組織と、NIS2 で新たに重要分野として追加した重要組織の 2 つの分類を設け、分類に応じて義務を調整しながらも、より広範な事業者に対策を迫る内容となっている。

表 3:規制にかかる NIS2 の追加(網掛け部分)

	必須組織	重要組織
対象分野	**NIS の対象セクター** エネルギー(電力・石油・ガス)、ヘルスケア（医療機関）、交通、銀行、金融市場インフラ、デジタル・インフラ、インターネットイクスチェンジ、クラウドサービス、水道など	**新たに拡大** 郵便・宅配、廃棄物処理、化学品製造・生産・流通、食品製造・加工・流通、重要製造業(医療機器、コンピュータ・電子製品・光学製品、電気機器)など
	新たに拡大 エネルギー(石油備蓄、水素など)、ヘルスケア(医薬品の研究開発、基礎医薬品・調剤)、行政機関、宇宙（地上インフラ）、下水処理	
義務	**NIS の義務を踏襲** • 監督官庁による立入検査や内部文書の提供 • セキュリティリスク監査 • サプライチェーンも含めたサイバーセキュリティ点検 • コンプライアンス責任体制の構築など	**一部義務を免除** • セキュリティリスク監査 • サプライチェーンも含めたサイバーセキュリティ点検 • コンプライアンス責任体制の構築など

また一方、EU 全体で高い共通水準を確保すべく、各 EU 加盟国に国家のサイバーセキュリティ戦略の策定を求めたほか、各加盟国間の協調的連携を促進する枠組みとして EUCyCLONe(欧州サイバー危機連絡組織ネットワーク)の設立を規定した。

このように社会のデジタル化の進展を受けて分野・地域にともに網羅性を広げつつ、強化された基準を確保する内容となっている。

c) サイバーレジリエンス法

i. 概要

サイバーレジリエンス法は、2022 年 9 月に欧州委員会が提案した EU 規則である。目的はデジタル要素を含む製品のライフサイクル全体でのセキュリティ向上にある。

その特徴として、製品やサービス等の認証策定を促進(ただし認証取得への強制力なし)するサイバーセキュリティ法、インフラ事業者自身のセキュリティガバナンス強化に主眼のある NIS/NIS2 に比べ、サイバーレジリエンス法はデジタル製品自体のセキュリティ強化に主眼がある。ENISA が策定した EUCC などの認証取得を法定義務化することを可能とし、これまでの EU サイバー法を補完するものとして位置付けられる。

スコープに含まれる製品は、ソフトウェアコンポーネント一覧(SBOM)作成や更新プログラム提供等のセキュリティ要件への適合と、上市にあたりその証明として CE マークの付与が求められる。脆弱性の悪用やインシデント発見後 24 時間以内に ENISA への報告も義務化されており、違反時の罰則(1,500 万ユーロ、又は前年度世界売上高の 2.5%のいずれか高い金額)も設けられている。

現時点で法案審議の見通しは不透明だが、欧州議会は 2024 年 6 月に改選されるため、審議が実質可能な 2023 年末までの採択を急いでおり、今年中に成立する可能性も否定はできない。

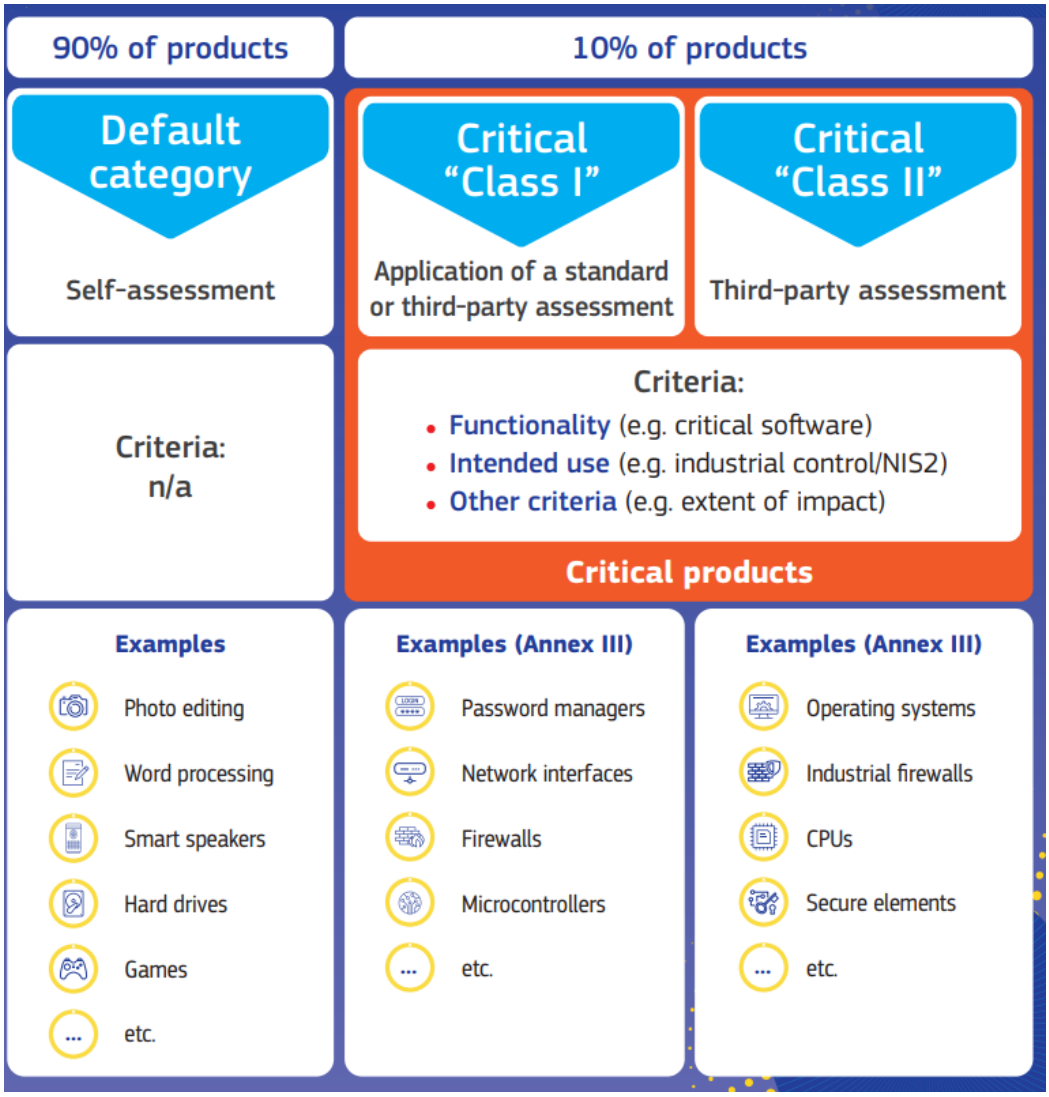
なお、EU サイバーレジリエンス法のスコープに含まれる既存の製品安全規制におけるセキュリティ条項との整合性は、今後図られる見込みとなっている。

ii. スコープと適合評価

対象となる「デジタル要素を含む製品」のスコープに含まれる製品が多岐に渡る中で、製品を重要度やリスクの高さに応じて 3 段階に分類し、基準への適合評価の手法に差異を設けている点が特徴である。

具体的には、重要度かつリスクの高い製品として分類されるクラス II には第三者評価を義務付ける一方で、重要度の高いクラス I には EUCC や EN 規格外の製品のみ第三者表を求める規定になっている。一般のデジタル製品が含まれるデフォルトカテゴリーには自己評価のみを求める。

図 1: サイバーレジリエンス法の分類と適合評価の違い(オレンジ背景部分)



出典: 欧州委員会公式サイト: サイバーセキュリティ法ファクトシート

90%以上の製品はデフォルトカテゴリーに含まれ、自己評価のみの実施を課す一方、クラス I・II の製品は既存の製品安全規格や NIS2 によるガバナンスなどとの整合性も含め、果たすべき義務に係る整理が重要となる。

3. 日本企業に与える影響

以上で見てきた様に、 欧州のサイバーセキュリティに関する取り組みは、ENISA が認証を定め、重要度の高いインフラ分野にスコープを広げ、製品規格と事業者のセキュリティガバナンスの両面から要件強化を図り、サイバーレジリエンス法を以てそれらを法定要件化していく流れにある。ウクライナ侵攻発生後の目下の地政学状況を踏まえると、今後も安全保障上の要請が高い分野から優先的に認証の策定が進みつつ、並行して法定要件化

に向けた動きが継続していくものとみられる。

これらの動きに対し、欧州企業は合理的に反応している。欧州の主要産業団体であるビジネスヨーロッパは、2023 年 3 月に公開したサイバーレジリエンス法に対する声明で、欧州委員会が提示した欧州のサイバーレジリエンス強化の方向性に賛同する一方で、既存の製品安全規格(NLF)にて要求されるセキュリティ要件との整合性を確保し不要な行政手続き負担が生じないように注文をつけたほか、適用開始となるまでに十分な準備期間の確保を要請した。また、主要 IT 業界団体であるデジタルヨーロッパを含む 5 団体は、2023 年 5 月の声明に於いて上記 2 点を述べるとともに、効果的な適用にあたって産業界の意見を踏まえた具体的なガイドライン整備が不可欠との意見を表明している。

このように欧州ではサイバーセキュリティのスタンダードの作り込みが具体化しつつある状況で、特に重要インフラ分野や欧州が強みを持つ製造業やヘルスケアなどの分野では力強い動きになる可能性を秘めている。こうした動きが世界に先行した場合、幅広い領域でデファクトスタンダード化する可能性もある。

デジタル製品・サービスの提供に関わるプレイヤーにとっては、欧州基準と自社事業が関連する国際基準との整合性や策定動向を注視する必要性が高まっていると言えるだろう。

以上