経済産業省

EU　NIS2指令概要

※NIS2指令：改正ネットワーク及び情報システム指令

2023年５月

経済産業省

サイバーセキュリティ課

＜本資料の背景＞

- EUがNIS２指令（改正ネットワーク及び情報システム指令）を改正し、2022年12月に官報掲載、2023年10月18日より施行予定。
- NIS２指令は、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）以上の主要エンティティ又は重要エンティティを対象にした規制であり、化学、医療機器、電気電子機器、光学機器、機械、自動車、輸送機器、宇宙、研究などの幅広い分野を対象に義務がかかるため、経済産業省関係の産業界に幅広くご認識いただきたい。

NIS2指令：官報掲載

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555&qid=1684136497194

EUサイバーセキュリティ戦略

- 2020年12月、欧州委員会は、欧州の安全・価値・基本的権利を保護をしたグローバルでオープンなインターネットを確立することを目的とした**サイバーセキュリティ戦略**を発表。

1．強靭・技術的主権・リーダーシップ

- **ネットワーク通信システム指令（NIS）の改正**
  - 対象拡大
  - サイバーセキュリティ・マネージメントの強化　など
- **欧州サイバー・シールド**
  - セキュリティ・オペレーション・センター（SOC）の創設（AIも駆使したサイバー攻撃の監視体制）
- **５Gネットワークのセキュリティ強化**
  - 2021年２Qまでに「５G ツール・ボックス」の完全執行。
- **インターネットにつながる機器等のセキュリティ強化**
  - ICT製品等の**サイバーセキュリティ認証制度**の導入
  - **NLF関連指令等**へのサイバーセキュリティ要件の導入
  - 自動車のサイバーセキュリティ対策の導入（2022年７月から）
- **サイバーセキュリティ・スキルの強化**

2．防御・抑止・対応ｵﾍﾟﾚｰｼｮﾝ強化

- EU全体の様々な主体が連携してサイバー攻撃への能力（準備・察知・対応能力）を強化するため、運用・技術面での連携を図るためのプラットフォーム**「共同サイバー・ユニット（Joint Cyber Unit）」**を創設。2021年２月までにに同ユニット設立に向けた計画を発表。

3．グローバルでオープンなサイバー空間の推進

- 国際連携の推進（国連「PoA: Programme of Action to Advance Responsible State Behavior in Cyberspace」を通じた連携）
- 第三国との連携強化（「EU Cyber Diplomacy Network」の創設）

ネットワーク通信システム指令改正（NIS2）

- 2020年12月、欧州委員会がNIS（ネットワーク情報システム）指令の**改訂案（NIS2）を発表。**
- NIS2での変更点は、**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**。
- 2022年12月、**NIS２指令官報掲載。2024年10月18日より施行。**

	NIS	NIS2
スコープ	ヘルスケア、交通、金融、デジタルインフラ、水道、エネルギー、デジタルサービスプロバイダー	**＜主要エンティティ＞**：エネルギー、**運輸**、銀行、金融市場インフラ、ヘルスケア、飲料水、下水、デジタルインフラ、ICTサービスマネジメント、公的サービス、**宇宙** **＜重要エンティティ＞**：**郵便・宅配、廃棄物管理、化学品、食品、製造業（医療機器、コンピュータ・電気電子・光学製品、機械、自動車・トレーラー、輸送機器）**、デジタルプロバイダー、**研究**
要件	•各社のサイバーセキュリティ対策 •重大事件が起きた際の当局への通報　等	**＜リスク管理（21条）＞** •リスクマネジメント及び情報セキュリティ対策 •インシデントハンドリング •ビジネス継続性 •サプライチェーンセキュリティ •ネットワークやシステムのセキュリティ •サイバーセキュリティリスクマネジメントの効率性評価 •サイバー衛生の実施及びサイバーセキュリティ教育 •暗号技術の活用 •アクセスコントロール等の人的セキュリティ •多要素認証の活用 **＜報告義務（23条）＞** **インシデント通報（24時間以内に早期警告、72時間以内にインシデント通知）** ＜その他＞**サイバーセキュリティ認証制度（EUCC）の活用**　等 ※EU加盟各国や、CSIRT、DNSサービスプロバイダー等に課される義務や対策については割愛し、日本企業に直接影響のある点だけを抜粋。
罰則	罰則額は加盟国の裁量	**•違反した場合には、売上げの最大２%又は1000万ユーロの罰金**

重大なインシデントの定義

- 事業体に重大なサービス運営上の混乱や経済的損失を引き起こすもの
- 他の自然人又は法人に影響を与えるもの

報告の流れ

- 重大なインシデントを認識してから24時間以内に早期警告を行う。
- 重大なインシデントを認識してから72時間以内に、上記の早期警告の情報を更新し、重大なインシデントの重大度・影響・侵害の兆候などについての初期評価を行うためのインシデント通知を行う。
- 必要に応じて中間報告を行う。
- インシデント通知後1か月以内に、インシデントの重大度・影響についての詳細、根本原因、緩和策、国外への影響を含む最終報告書を提出する。

EUサイバーレジリエンス法（草案）

- 2022年9月に草案提出。2023年後半の発効、**2025年後半の適用**を目指す。
- 例外を除き、**デジタル要素を備えた全ての製品が対象。SBOM作成や更新プログラム提供等セキュリティ要件への適合（自己適合宣言/第三者認証）が求められる。**
- **重要なデジタル製品について、低リスク製品でEUCCやEN規格対象外の製品は第三者認証を、高リスク製品には第三者認証を求める。**（中小企業の認証手続き減額）
- 適合性評価証明書にはEU適合宣言書（CEマーク）/EUCC証明書を用いる。
- **脆弱性の悪用やインシデント発見後24時間以内にENISAへの報告を義務化。**
- **罰則あり。**（最高1,500万ユーロ又は当該企業の全世界売上高の2.5%以内）

注：EUCCとは、IoT製品を対象とする欧州サイバーセキュリティ認証。
EN規格とは、欧州整合化規格

【対象】デジタル要素を備えた全ての製品

・デバイスやネットワークに直接的/間接的に接続されるものも含む。
・医療機器規則、体外診断用医療機器規則、民間航空機規則、自動車の型式承認規則の対象製品は適用除外。
・国家安全保障に関するデジタル製品や軍事目的・機密情報処理目的のものは除外。
・SaaSなどのソフトウェアサービスは対象外。研究開発目的のOSSなども対象外。

【適合性評価】使用環境等のリスクレベル毎に以下を求める。

- **「デジタル製品」　・・・　自己適合宣言か第三者認証を選択**
- **「重要なデジタル製品」のうちクラスI（低リスク）・・・EUCCやEN規格の対象外は第三者認証**
- **「重要なデジタル製品」のうちクラスII（高リスク）・・・第三者認証**

【適合性評価証明書】

・EU適合宣言書（CEマーク）に基づく証明書
・EUCCに基づく証明書（必要に応じてEUCCを必要とする製品を指定）
※この他、市場サーベイランスも行われる。
※第三国（日本も含む）との相互承認も可能。※条文上は見当たらず。

CEマーク