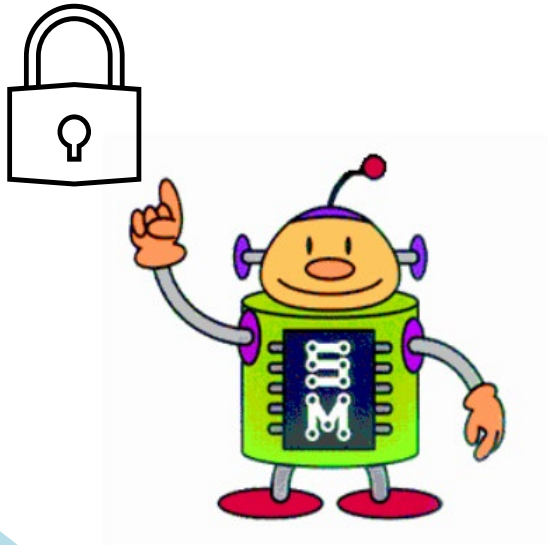
サイバーセキュリティに関する現状調査



2024年4月

はじめに

私たちの生活は、デジタル技術と深く結びついています。インターネットに接続された製品やサービスは、日常生活を豊かにし、ビジネスの効率化をもたらしています。しかし、このデジタル化の波は、新たな脅威をもたらしています。サイバー攻撃は、個人のプライバシーを侵害し、企業の知的財産を盗み出し、時には国家の安全保障にまで影響を及ぼす可能性があります。

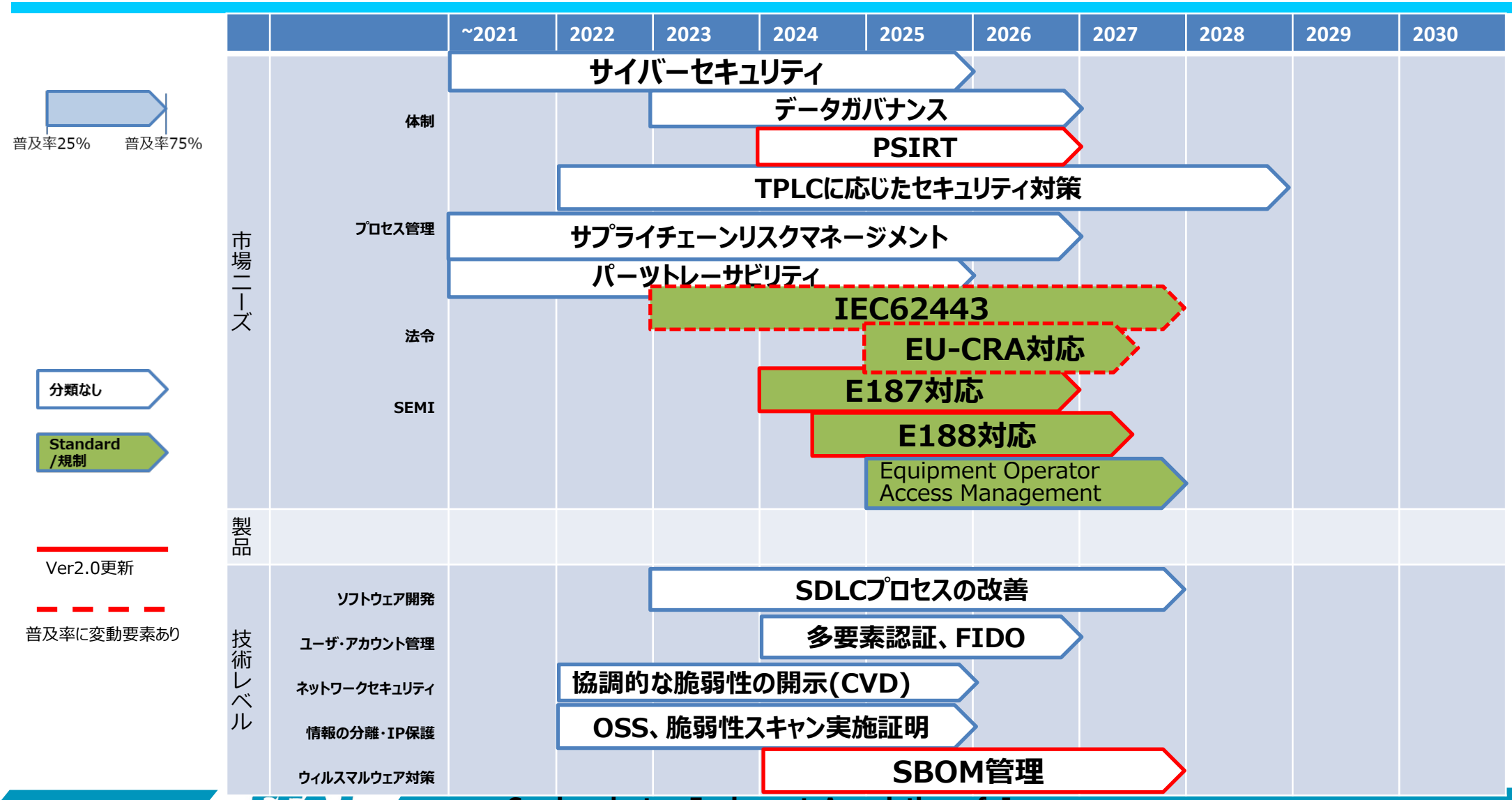
このような背景のもと、サイバーセキュリティは単なるIT部門の課題ではなく、組織全体、さらには社会全体が直面する重要な問題となっています。**特に自社が販売する製品やサービスに対するサイバー攻撃のリスクが高まる中、各国政府もこの問題に対処するための規制を強化しています。**

本資料では、サイバーセキュリティの現状と、世界各国で進行中の規制の動向とそのロードマップについて概観します。

本資料を参考にされる方々が、**この情報を基に適切なリスク管理と対策を講じるための理解を深めることができるよう、最新の知見を提供することを目指しています。**

セキュリティ

Ver.2.0



EU法CRAについて

CRA (Cyber Resilience Act) サイバーレジリエンス法

EU圏内で販売する製品の脆弱性対応を義務付けるサイバーセキュリティに関する法令

※CEマーキングにCRAが含まれる

※CRAは規則(Regulation)に位置づけされ、法的強制力が発生します

- **適用範囲**　：CE宣言を実施している全てのデジタル製品の製造業者や小売業者に指定のサイバーセキュリティ要件を満たすことが義務付けられる。
- **要求項目**　：脆弱性に関する報告窓口の情報やSBOM、適合宣言書などの情報を提供
- **義務**　・脆弱性発見やセキュリティ事故が発生した場合には、72時間以内に通知
  ・セキュリティアップデートは製造業者が無償負担
  ・CRA適合エビデンスは製造業者が無償提供
- **罰則**　：有り　悪質な場合、社名公表（従来のCEマーキングにも適用されている）
  1,500万ユーロまたはグローバル年間売上高の2.5%のいずれか高い方

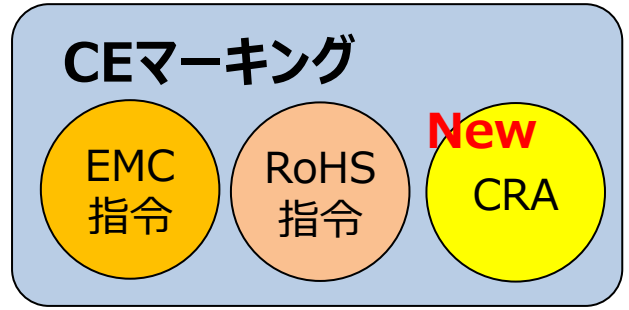
- **スケジュール**（2024年3月情報）

  2023年12月：立法手続き開始

  2024年3月　：本会議承認（最終ガイドライン発行時期：未定）

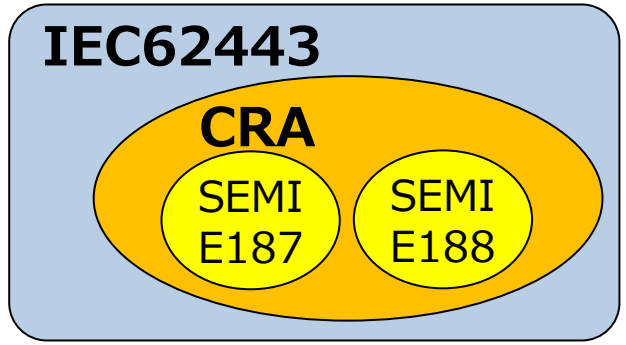
  2025年末：製造業者の報告義務開始

  2027年春：適用開始



安全の概念にサイバーセキュリティが組み込まれる

■　産業用製品
サイバーセキュリティプログラム



出典：European Union　CRA　EU法案進捗

EU法CRA　製造業者の義務（抜粋）

- サイバーセキュリティを確保するように設計、開発、生産されていること
- サイバーセキュリティ上のリスクアセスメント実施と技術文書への記録
- 第三者から提供された部品によるセキュリティリスクを高めない事の保証
- SBOM（ソフトウェア部品表）導入により脆弱性箇所の特定・開示
- CEマーキングの貼付および技術文書・適合証明書の保管・提供
- 製品セキュリティ担当窓口（PSIRT）の設立と公開
- 脆弱性発見やセキュリティ事故が発生した時の通知（対象：EU当局　72時間以内）
- セキュリティ事故対策と製品対応は製造業者が無償で実施する
- セキュリティ要件への未遵守に係る是正措置と製品撤回またはリコール実施

EU法CRAに関しての懸念点

- 継続的なセキュリティ管理義務
  - 市場投入期間中（製品寿命もしくは５年間の長い方）での継続的なセキュリティ管理
- 情報の公開
  - 脆弱性情報の72時間以内の報告義務
  - 脆弱性のトリアージの基準（CVSSだけでなくリスクアセスが必要？）
  - 開示方法、タイミング
- リスク評価と対応計画・対策
  - セキュアプロセス
  - リスクアセスメント
  - サプライヤマネジメント
- SBOM生成、管理
  - 単位は？（コンポーネント、モジュール、ライブラリ．．．）
  - 汎用化された自動生成ツールは？
  - サプライチェーンのSBOMも管理？

SEMIスタンダードの動向

- **SEMI E187** ; Specification for Cybersecurity of Equipment (2022/1)
  - サポート終了したOSの搭載禁止を含む装置搭載のOSに関する要求
  - 影響範囲(Windows/Linux等のコンピュータデバイス)
  - **台湾が主導（TSMC）**

- **SEMI E188** ; Specification for Malware Free Equipment Integration (2022/2)
  - 影響範囲

    装置およびその付帯システム、サブシステム上のコンピューティングデバイス、ストレージデバイスに適用
  - **米国が主導（Intel）**

グローバルの動向

- EU
  - EUサイバーレジリエンス法案　EU 2022/0271　（2022/9初版）
  - 機械規則案　EU 2023/1230　（2023/06官報）
  - 無線機器指令　EU 2022/30　（2021/10官報）

- 英国
  - PSTI法　（2022/12/7）

- 米国
  - IoT Cybersecurity Improvement Act of 2020　（2020/12/4）
  - NIST SP 800-213（2020/12/15）
  - NISTIR 8259　（2020/5/29）

- 日本
  - IoT製品に対するセキュリティ適合性評価制度構築方針案　（2024/03）

IEC62443

- スマートファクトリーを担う(ソフトウェアおよびソフトウェアを組み込んだ)**工場設備**・**産業機器**に対する**サイバーセキュリティ対策の指針**となる国際標準規格

- 各国の法規制に対して、セキュリティガイドラインとして幅広く活用されているのが、この**「IEC62443」**となる。

経産省　サイバーセキュリティ経営ガイドライン Ver3.0

- 経済産業省でも、独立行政法人情報処理推進機構（IPA）とともに、サイバー攻撃から企業を守る観点で、経営者が認識する必要がある事項及び経営者が情報セキュリティ対策を実施する上での責任者となるCISO（Chief Information Security Officer：最高情報セキュリティ責任者）等に指示すべき事項をまとめたサイバーセキュリティ経営ガイドラインを策定し、その普及を行っている。

- 経営者が認識すべき3原則と指示すべき重要10項目
  ① サイバー攻撃から企業を守る観点で経営者が認識すべき「3原則」
    1. 経営者のリーダーシップが重要
    2. サプライチェーン全体にわたる対策への目配り
    3. 社内外関係者との積極的なコミュニケーション

経済産業省HP
https://www.meti.go.jp/press/2022/03/20230324002/20230324002.html
https://www.meti.go.jp/press/2022/03/20230324002/20230324002-1.pdf
https://www.ipa.go.jp/security/economics/hjuojm00000044dc-att/cms_practice_v4.pdf

経産省　サイバーセキュリティ経営ガイドライン Ver3.0

- 経営者が認識すべき3原則と指示すべき重要10項目
  - ② CISO等に対し指示すべきサイバーセキュリティ経営の「重要10項目」
    - 指示１　：　サイバーセキュリティリスクの認識、組織全体での対応方針の策定
    - 指示２　：　サイバーセキュリティリスク管理体制の構築
    - 指示３　：　サイバーセキュリティ対策のための資源（予算、人材等）確保
    - 指示４　：　サイバーセキュリティリスクの把握とリスク対応に関する計画の策定
    - 指示５　：　サイバーセキュリティリスクに効果的に対応する仕組みの構築
    - 指示６　：　PDCA サイクルによるサイバーセキュリティ対策の継続的改善
    - 指示７　：　インシデント発生時の緊急対応体制の整備
    - 指示８　：　インシデントによる被害に備えた事業継続・復旧体制の整備
    - 指示９　：　ビジネスパートナーや委託先等を含めたサプライチェーン全体の状況把握及び対策
    - 指示１０　：　サイバーセキュリティに関する情報の収集、共有及び開示の促進

経済産業省HP
https://www.meti.go.jp/press/2022/03/20230324002/20230324002.html
https://www.meti.go.jp/press/2022/03/20230324002/20230324002-1.pdf
https://www.ipa.go.jp/security/economics/hjuojm00000044dc-att/cms_practice_v4.pdf

経産省　今後のサイバーセキュリティ政策

- 経済産業省が令和6年4月5日に「第８回　産業サイバーセキュリティ研究会　事務局説明資料」を公開
- 今後の産業サーバーセキュリティ政策、産業界へのメッセージを発表
  - ガイドライン等の実効性の強化
  - **IoTセキュリティ適合性評価制度**の検討
    - 幅広いIoT製品を対象として、一定のセキュリティ基準を満たすものを認証し、ラベルを付与する制度の整備に向けて、検討を実施。その結果を2024年３月に取りまとめ、2024年度中に一部運用を開始予定。
  - **半導体関連産業において求められるセキュリティ対策を具体化　など**

経済産業省HP
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/pdf/008_03_00.pdf

用語集

◆ サイバーセキュリティを維持運用するための上位組織の管理体制

- CISO：（Chief Information Security Officer）最高情報セキュリティ責任者
- PSIRT：（Product Security Incident Response Team：ピーサート）

  自社で製造・開発する製品・サービスに対するセキュリティの向上や、インシデント（不具合や障害など）への対応を目的とする組織
- TPLC：（Total Product Life Cycle）

  TPLCに応じたセキュリティ対策。（設計・開発期間、サポート期間、サポート終了など）
- サプライチェーンリスクマネージメント

  対象が自社だけではなくサプライチェーンを構成する全てとなること。

用語集

◆ 製品セキュリティを確保するための対策

- SDLC（Software Development Life Cycle）

  ソフトウェアの企画段階から、要件定義、システム開発、保守・ 運用を経て、システム廃棄に至るまでの工程全体

- SBOM（ソフトウェア部品表）

  SBOMを収集し常時新たな脅威を調査し評価を実施。

- OSS（Open Source Software）管理

  ソースコードが公開されていて、利用者の目的を問わず、利用、改変、頒布 が自由に認められている。

  無料で使えるが、無条件で使えるソフトウェアではない。

- 協調的な脆弱性の開示（CVD）

  規制当局等と連携した脆弱性の開示（CVD：Coordinated Vulnerability Disclosure）プロセス。

  ステークホルダーに対する情報の提供。