経済産業省

資料3

『第2層：フィジカル空間とサイバー空間のつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォースの検討の方向性

令和2年3月2日

経済産業省 商務情報政策局

サイバーセキュリティ課

1. サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）とその実装へ向けた取組の方向性

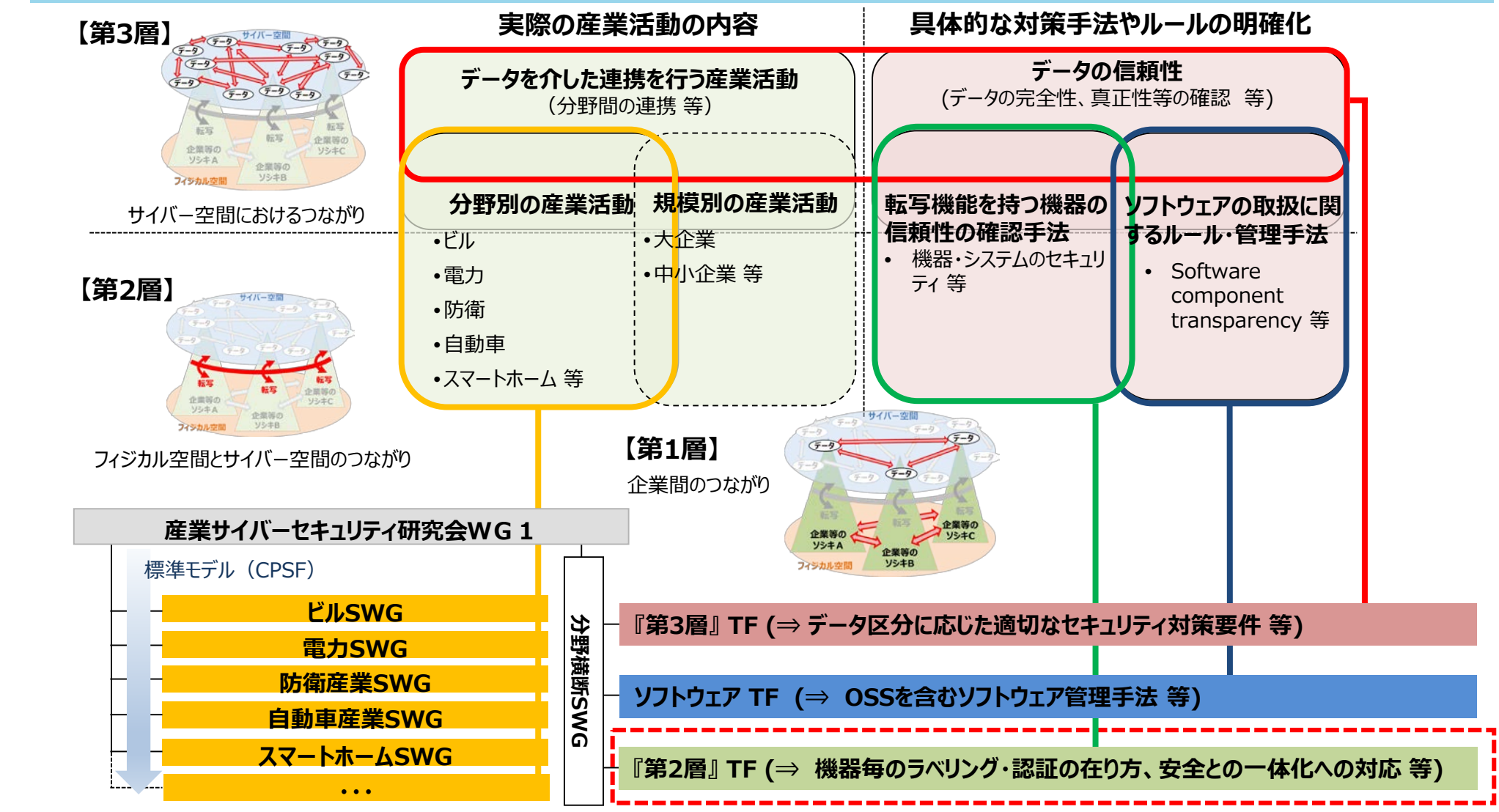
2. サイバー・フィジカル間の転写機能を持つ機器に対する攻撃事案

3. サイバー・フィジカル間の転写機能を持つ機器の信頼性確保に向けた諸外国の検討状況

4. 本タスクフォースにおける検討事項

CPSFに基づくセキュリティ対策の具体化・実装の推進

- CPSFに基づくセキュリティ対策の具体化・実装を推進するため、検討すべき項目ごとに焦点を絞った**タスクフォース（TF）を新たに設置。**



テーマ別TFの検討状況

- CPSFに基づくセキュリティ対策の具体化・実装を推進するため、検討すべき項目ごとに焦点を絞った**タスクフォース（TF）を新たに設置。**

産業サイバーセキュリティ研究会ＷＧ１（制度・技術・標準化）

標準モデル（CPSF）

Industry by Industryで検討
（分野ごとに検討するためのSWGを設置）

- ビルSWG
- 電力SWG
- 防衛産業SWG
- 自動車産業SWG
- スマートホームSWG
- ・・・

分野横断SWG

『第3層』TF

【論点】： データの信頼性確保のための、データの区分に応じた適切なセキュリティ対策要件等。
【展望】： データマネジメントの捉え方を整理し、それに応じたセキュリティ要求の考え方を整理する。

ソフトウェア TF

【論点】： ソフトウェア管理手法、脆弱性対応、OSSの利活用等。
【展望】： OSSの利活用に係るプラクティス集を編纂。OSSの利活用に伴うリスクを軽減しつつ、OSSのメリットを享受するためのプラクティスを示すことで、OSSの利活用の拡大につなげる。

『第2層』TF

【論点】： サイバー・フィジカル間をつなぐ機器やシステム（IoT機器・システム）に潜むリスクに応じてカテゴライズを行い、セキュリティ・セーフティ要求を検討する必要性、及びその検討に活用可能なフレームワークの検討。
【展望】： パブコメの結果を踏まえ、フレームワークを策定。各主体がフレームワークを活用することで、IoTを社会として効果的に受容することにつなげる。

1. サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）と
   その実装へ向けた取組の方向性

2. サイバー・フィジカル間の転写機能を持つ機器に対する攻撃事案

3. サイバー・フィジカル間の転写機能を持つ機器の信頼性確保に
   向けた諸外国の検討状況

4. 本タスクフォースにおける検討事項

スマートスピーカーを悪用したフィッシング攻撃

- 2019年10月、ドイツのセキュリティ研究機関 SRLabs（Security Research Labs）が、スマートスピーカーの機能を悪用し、ユーザのパスワードの窃取や会話の盗聴が可能であることを公表。
- スマートスピーカーは、特定のフレーズを認識することでそれに対応した機能を実行するが、特定のフレーズに続く内容をテキスト化してサーバに送信する機能がある。
- スマートスピーカーのアプリストアに相当するAlexa SkillやGoogle Assistantの審査を、無害なアプリを装って通過した後に、メッセージを改変する手法によるフィッシングなど（※）、当該機能を利用してユーザの個人情報等を窃取するスマートスピーカーを通じた攻撃手法が実証された。

※攻撃プロセスの概要

●偽のメッセージでフィッシング

1．特定のフレーズ（e.g.「Start」）に続く内容をサーバに送信する、一見して無害なアプリを作成。
2．審査通過後、最初のメッセージをエラーメッセージのように改変（e.g.「現在この機能は利用できません。」）。
3．スピーカーにフィッシングメッセージを発声させる（e.g.「重要なアップデートがあります。Start updateに続いてパスワードを発声してください。」）　。
4．「Start」の後にユーザが発声したパスワードがサーバに送信される。

●アプリの終了を誤認させて盗聴

1．一見して無害なアプリを作成。
2．審査通過後、アプリの終了時等に「Good Bye」と発声させた後、スピーカーが音声化できない文字列（e.g.“ . “）を繰り返すことで、アプリの動作を継続させるようアプリを改変。
3．２．の終了音やメッセージを聞いたユーザは、アプリが停止したと錯覚。
4．アプリが動作している間にユーザが特定のキーワードを発声した場合、それがサーバへ送信される。

https://srlabs.de/bites/smart-spies/

Medtronic社の電気手術器に複数の脆弱性

- 2019年11月、US-CERTは、Medtronic社製の電気手術器に複数の脆弱性（CVE-2019-13543、CVE-2019-13539、CVE-2019-3464）が存在するとして、注意喚起を行った。これらの脆弱性により、攻撃者はリモートから特定の攻撃コードを送信することで、ファイルの上書きや不正コードの実行等を行うことが可能とされる。
- 該当するデバイスのネットワーク接続はデフォルトでは無効であり、再起動時にもイーサネットポートが無効になる構成となってはいるが、多くの場合、ネットワークに接続して利用されているため、Medtronic社はパッチを適用するまで、当該デバイスをネットワークに接続しないことを推奨している。

電気手術器の3つの脆弱性

ハードコードされた資格情報の使用	デバイスにハードコードされた資格情報が発見された場合、それらを使用して機器のファイルを読み取られる可能性がある。
脆弱なハッシュアルゴリズムを使用している問題	OSパスワードに脆弱なハッシュアルゴリズムを利用しており、開示されている他の脆弱性と組み合わせて、これらのハッシュを取得される可能性がある。
適切でない入力確認	脆弱なバージョンのrsshユーティリティを使用してファイルのアップロードが可能であることから、ファイルにアクセスされたり、任意のコードを実行されたりする可能性がある。

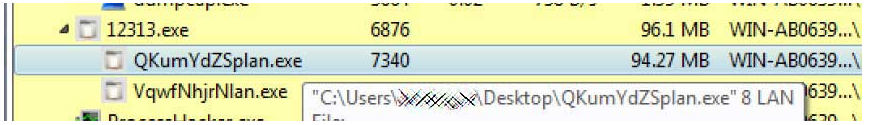
https://www.us-cert.gov/ics/advisories/icsma-19-311-02

ランサムウェア「Ryuk」がWake-On-Lanを利用して電源オフのデバイスを暗号化

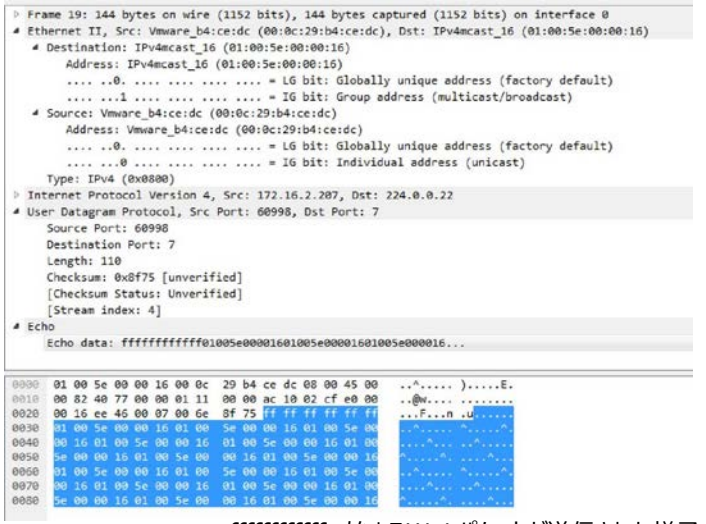
- 2018年夏頃から存在が確認されている標的型ランサムウェア「Ryuk」は、これまでも海外の多くの企業・行政機関に被害を与えているが、少しずつ新しい機能が追加されている。
- 2019年10月頃に出現したRyukの新しい機能は、ネットワーク上の電源がオフになっているデバイスを起動できるWake-On-Lan(WOL)機能を利用し、電源がオフになっている端末ですら暗号化できるため、企業内ネットワーク等において感染が広がる恐れがある。

攻撃プロセスの概要

①サブプロセスの作成	・マルウェアが実行されると、自身のコピーであるサブプロセスを、特別なモードで実行。
②ネットワークの確認	・特別なモードで実行された場合、デバイスのARPテーブルをスキャンし、プライベートネットワークを確認。
③WoLパケットを送信、デバイスを起動	・デバイスのMACアドレスにWake-on-Lan（WoL）パケットを送信して起動を試みる。
④ドライブをマウントし、暗号化	・起動に成功した場合、そのデバイスのドライブの暗号化を試みる。



特別なモード（実行引数「8 LAN」）でサブプロセスが実行された様子



ffffffffffffで始まるWoLパケットが送信された様子

https://www.bleepingcomputer.com/news/security/ryuk-ransomware-uses-wake-on-lan-to-encrypt-offline-devices/

1. サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）と
   その実装へ向けた取組の方向性

2. サイバー・フィジカル間の転写機能を持つ機器に対する攻撃事案

**3. サイバー・フィジカル間の転写機能を持つ機器の信頼性確保に
   向けた諸外国の検討状況**

4. 本タスクフォースにおける検討事項

諸外国の検討状況（概要）

- 各国・地域において、様々な検討が行われている。

- 欧州サイバーセキュリティ認証フレームワーク
- **Standardisation in support of the Cybersecurity Certification**
- **Good Practices for Security of IoT - Secure Software Development Lifecycle**

ETSI

Cyber Security for Consumer Internet of Things

消費者向けIoT製品のセキュリティに関する行動規範

セキュアルータの技術ガイドライン

OECD

OECD 製品安全作業部会・デジタル経済セキュリティ・プライバシー作業部会

NIST

- Considerations for a Core IoT Cybersecurity Capabilities Baseline
- Security for IoT Sensor Networks
- **NISTIR** 8200, 8228, **8259**, 8267, **8276**
- Secure Software Development Framework 等

カリフォルニア州のIoTセキュリティ法

IoT機器の購入に当たりセキュリティ等の情報やラベリングが与える効果についての研究

Internet Society

IoT Security Policy Platform

※ 黒字が前回TFから、新たに公開された、又は更新された文献

NISTIR 8259 2nd draft - Core Cybersecurity Feature Baseline for Securable IoT Devices: A Starting Point for IoT Device Manufactures

- IoT機器を管理する組織向けの推奨事項をまとめたNISTIR 8228に対し、**IoT機器の製造者に任意だが推奨される6つのサイバーセキュリティに関連する活動**を整理(2020年1月ドラフト第2版公開)。**6つのコアサイバーセキュリティ機能をベースラインと定義**し、当該機能を達成するために実装すべき重要要素や、既存のIoTセキュリティガイダンスへの参照がまとめられている。
- ベースラインを元に、産業分野により異なるセキュリティ要求を踏まえた機能の特定が必要としている。

製造者に推奨されるサイバーセキュリティ関連活動

販売前に影響する活動	活動1：予想される顧客特定、ユースケース定義 活動2：顧客のサイバーセキュリティの目標調査 活動3：顧客目標に対処する方法決定（6つのコアサイバーセキュリティ機能） 活動4：顧客目標の適切なサポート計画（ハード、ソフト、ファームウェア、ビジネスリソースの適切なプロビジョニング）
販売後に影響する活動	活動5：顧客とのコミュニケーションアプローチ定義 活動6：顧客に伝える内容と伝達方法決定（製造業者の設計・開発時のリスク関連の仮説、サポートと寿命、提供するデバイスセキュリティ機能、デバイス構成・機能、ソフトウェア及びファームウェアの更新、デバイスの廃止オプション）

6つのコアサイバーセキュリティ機能

（１）機器の識別：IoT機器を論理的・物理的に一意に識別できる。	（４）インターフェイスへの論理アクセス：IoT機器のインターフェースへの論理アクセス、及びこれらインターフェイスで利用されるプロトコルとサービスを認可エンティティのみに制限可。
（２）デバイスの構成：IoT機器のソフトウェア・ファームウェアの構成変更が可能。変更は、認可エンティティのみが行うことができる。	（５）ソフトウェア等の更新：IoT機器のソフトウェア・ファームウェア更新は、認可エンティティによって安全かつ構成可能なメカニズムを用いてのみ実行できる。
（３）データ保護：IoT機器が保存・送信するデータを不正なアクセス及び変更から保護することができる。	（６）サイバーセキュリティ状態認識：IoT機器はセキュリティ状態を報告し、認可エンティティのみにアクセスを許可。

NISTIR 8276 draft - Key Practices in Cyber Supply Chain Risk Management: Observations from Industry

- NISTが2015年と2019年に実施したサイバーサプライチェーンリスク管理(C-SCRM)に関するケーススタディをベースに、8つのキープラクティスを提示（2020年2月ドラフト公開 ）。
- 「2 Problem Definition」の項には、デジタル化の進展に伴い、昨今では**サイバーセキュリティイベントの影響が、データの損失だけでなく、重大な経済的損失、安全性の侵害や人命の損失にまで繋がり得る**との、本TFにおける議論と類似する記載がある。

米国におけるサイバーサプライチェーンリスク管理(C-SCRM)に係るこれまでの検討プロセス

2008年1月 包括的サイバーセキュリティイニシアチブ(CNCI) #11「グローバルサプライチェーンのリスク管理のための多方向からのアプローチの開発」

2012年10月 NIST IR 7622「連邦情報システムのための国家サプライチェーンリスク管理プラクティス」公開

2015年4月 NIST SP 800-161「連邦情報システム/組織向けサプライチェーンリスク管理プラクティス」公開

2015年9月 サイバーサプライチェーンリスク管理に関する民間事業者の対応におけるケーススタディ(18件)を公開

2018年4月 NIST Cybersecurity Framework Ver.1.1 公開 (サプライチェーンリスク管理に関する対策カテゴリーを新たに追加)

2020年2月 Draft NIST IR 8276「サイバーサプライチェーンリスク管理におけるキープラクティス」公開

C-SCRMにおける8つのキープラクティス

1. 組織をまたいだサイバーサプライチェーンを統合する
2. C-SCRMに関する公式のプログラムを設置する
3. 自組織の重要なサプライヤーを認識し、管理する
4. 自組織のサプライチェーンを理解する
5. 重要なサプライヤーと密接に協力する
6. 重要なサプライヤーを自組織のレジリエンス、改善活動に含める
7. サプライヤーとの関係全体を通じて評価と監視を行う
8. 事業継続を保証するためのライフサイクル全体に対する計画を立てる

ENISA : Standardisation in support of the Cybersecurity Certification

- サイバーセキュリティは分野横断的であるにもかかわらず、業界毎に垂直的で一貫性のない標準が作成されると、チップメーカ等が同等の要件をもつ複数の認証を受けなければならなくなることへの懸念から、標準化組織（Standardisation Developing Organisations、特に欧州のCEN、CENELEC、ETSI）に対し、標準化と認証スキームの間の重複する矛盾または非互換性を回避することを求めている（2020年2月公開）。
- 認証のためのサイバーセキュリティの標準化の取組みの有用性や、標準化組織の役割と責任を提示し、標準化組織と将来的な認証スキームの作成差に対する推奨事項を示している。

新しい認証スキームを定義するステップ

セキュリティ目的の定義

↓

既存の関連標準の特定

技術要求仕様	評価手法	適合性評価

↓

ギャップ分析

技術要求仕様	評価手法	適合性評価

↓

不足する要件の準備

技術要求仕様	評価手法	適合性評価

↓

認証スキームの検証と正式な採用

標準化組織	認証機関

主な提言

- 標準化組織間の競合を避けることが重要である。
- 特定の領域に国際標準がある場合、優先選択する必要がある。
- ISO / IEC JTC1 / SC27は、サイバーセキュリティ標準化の最初の参考資料として検討すべき。
- ISO/IEC 15408/18045：Common Criteriaと評価方法、IEC 62443 Part4-2：産業オートメーションおよび制御システムのセキュリティ - IACSコンポーネントの技術的セキュリティ要求事項、EN 303 645：コンシューマIoTためのサイバーセキュリティ、これらは競合しておらず補完的なものと見なすことができ、すべてのサイバーセキュリティの評価の基礎となり得る。

（参考）欧州サイバーセキュリティ認証フレームワーク

- 「Cybersecurity Certification Framework」の創設を含む「Cybersecurity Act」は、2019年4月9日に欧州理事会で採択され、6月27日に発効。
- 「Cybersecurity Act」に基づき、ENISAが具体的な産業分野毎に「候補スキーム(Candidate Scheme)」を欧州委員会に提案し、順次、認証フレームワークが策定される予定。

欧州委員会、ENISAの動向

- 2019年4月、Cybersecurity Act が欧州理事会で採択、6月27日に発効。
- **2019年9月、ENISAがサイバーセキュリティ認証スキームの候補を準備するためのアドホックワーキンググループの設立を呼びかけ。候補スキームとしてCommon Criteria(ISO/IEC 15408)も考えられるとの記載もある。**

Cybersecurity Actの概要

- 欧州委員会は、欧州サイバーセキュリティ認証スキームの対象となるICT製品、サービス、プロセス、カテゴリのリストを含む「Union rolling work programme」を発行。最初の「Union rolling work programme」 は2020年6月28日までに発行される（Article 47）。
- 本スキームでは、ICT製品等について、インシデントの可能性と影響の観点を考慮し、「basic」、「substantial」または「high」のいずれかの保証レベルを1つ以上特定する（Article 52）。
- ICT製品等の製造者又は提供者は、保証レベル「basic」に対応する低リスクを示すICT製品等について、本スキームに示されている要件の充足が実証されていることを示すEU適合宣言をボランタリーに発行することができる（Article 53）。
- 本スキームには、評価に適用される国際規格、欧州規格又は国内規格への参照及び第三国との認証制度の相互承認のための条件等が含まれる（Article 54）。
- 欧州委員会は、サイバーセキュリティ認証スキームが義務づけられることによって、ICT製品等の適切なレベルのサイバーセキュリティを確保し、国内市場の機能を改善することに効果があるか定期的にアセスメントを行う。最初のアセスメントは2023年末までに行われ、その後は少なくとも2年ごとに行われる（Article 56）

（参考）NIS指令

- 2016年8月、EUにおいてネットワークと情報システムのセキュリティに関する指令（**NIS指令**）が発効。
- NIS指令は、サイバーセキュリティに関するEU最初の指令であり、EU全体のセイバーセキュリティレベルを高める法的措置を提供。
- **2018年5月9日までに**、EU各国に対して、NIS指令に基づく**国内法の整備を要求**。
- **2018年11月9日までに、重要インフラ事業者やデジタルサービス提供者等に対して、リスクマネジメントやインシデント報告の義務を要求**。

NIS指令の目的

（１）国家レベルでのサイバーセキュリティ能力向上。

（２）EUレベルの協力強化。

（３）重要インフラ事業者やデジタルサービス提供者等に対するリスクマネジメントやインシデント報告義務化。

対象事業者の義務

・適切なセキュリティ対策。

・各国当局へのインシデントの通報。

以下のセキュリティ対策を含む。

① リスクの予防

② ネットワークと情報システムのセキュリティ確保

③ インシデントハンドリング

ENISA : Good Practice for security of IoT
- Secure Software Development Lifecycle

- IoT製品やサービスのための安全なソフトウェア開発ライフサイクル（SDLC）に焦点を当てたプラクティス集（2019年11月公開）。IoTソフトウェア開発者、インテグレーター、プラットフォーム・システムエンジニアを対象とし、要件定義、ソフトウェア設計から保守や廃棄に至るまで、IoTソフトウェア開発のすべてのフェーズにおけるセキュリティ上の懸念や考慮すべき重要なポイントを整理。セキュリティを強化するための具体的なプラクティスや関連する既存の標準やガイドラインがまとめられている。

SDLCの各フェーズと主なセキュリティ考慮事項

開発フェーズ	セキュリティ考慮事項
分析・要件	セキュリティ要件、ハードウェア制限、プロトコル、脅威モデリング
ソフトウェア設計	アタックサーフェス分析、セキュアデザイン
開発/実装	フレームワーク、ライブラリ、ビルトインセキュリティ、ガイドライン、外部（ライブラリ等）のチェック
テスト/受入	デザインレビュー、コード検証、セキュリティ要求テスト、ペネトレーションテスト
開発/統合	ハードニング環境、コンフィグレーションと脆弱性管理、変更管理
維持/廃棄	インシデント管理、廃棄処分の管理、リモートソフトウェアアップデート

プラクティス：3グループ－16ドメイン

人	教育と意識付け
	役割と特権
	セキュリティ文化
プロセス	サードパーティ管理
	オペレーション管理
	SDLC手法
	セキュア開発
	セキュアデザイン
	内部ポリシー

技術	アクセスコントロール
	サードパーティソフトウェア
	セキュア通信
	セキュアコード
	セキュリティレビュー
	SDLC環境のセキュリティ
	セキュリティ実装

※プラクティスの例
4.2.3.2 サードパーティソフトウェア
TC-06：最新の既知の脆弱性にパッチを当てたライブラリやサードパーティコンポーネントを利用する
TC-07：長期サポートがあるよく知られた安全なフレームワークを利用する

消費者向けIoT製品のセキュリティに関する行動規範（英国）

- 英国デジタル・文化・メディア・スポーツ省（DCMS）が、消費者向けIoT製品の開発、製造及び販売の段階で安全が確保されるよう、**製造メーカー等が実践すべき対策を13項目のガイドライン**にまとめ、2018年10月に公表。
- 一部の項目の義務化法案について2019年5月～6月にかけてパブリックコメントを実施。コメントを踏まえた**ドラフト法案を2020年1月に公開。**

ベストプラクティス一覧（13項目）

1. デフォルトパスワードを使用しない
2. 脆弱性の情報公開ポリシを策定する
3. ソフトウェアを定期的に更新する
4. 認証情報とセキュリティ上重要な情報を安全に保存する
5. 安全に通信する
6. 攻撃対象になる場所を最小限に抑える
7. ソフトウェアの整合性を確認する
8. 個人データの保護を徹底する
9. 機能停止時の復旧性を確保する
10. システムの遠隔データを監視する
11. 消費者が個人データを容易に削除できるように配慮する
12. デバイスの設置とメンテナンスを容易にできるように配慮する
13. 入力データを検証する

義務化項目の案（3項目）

① IoTデバイスのパスワードはユニークにする、かつ工場出荷時の共通設定にリセットできないようにする

② IoT製品メーカーは脆弱性開示ポリシーの一部として連絡先を提供する

③ IoT製品メーカーはデバイスに対するセキュリティアップデートを提供する最低期間を明示する

1. サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）と
   その実装へ向けた取組の方向性

2. サイバー・フィジカル間の転写機能を持つ機器に対する攻撃事案

3. サイバー・フィジカル間の転写機能を持つ機器の信頼性確保に
   向けた諸外国の検討状況

4. 本タスクフォースにおける検討事項

サイバー・フィジカル間をつなげる機器・システムをカテゴライズする際の軸の設定について

第2回TF資料（再掲）

- 機器のカテゴライズについて、前回TFでの議論を踏まえ、以下のように再整理し、仮のフレームワークを提案したい。
- 転写機能を持つ機器・システムに求められる安全を考慮に入れるという第2層TFの趣旨に鑑み、**危害が発生した際にリカバリできるダメージかどうか**を最重要視し、第1軸を『**人へのダメージに対するリカバリの困難性の度合い**』と再定義。
- 他方、TFで指摘があった観点全てを軸に落とし込むと複雑になってしまうことから、それらの観点の多くは、便宜上、「リカバリ可能性が高く、金銭的価値に換算可能なもの」であると考え、第2軸を『**経済的影響の度合い**』と定義し、第2軸に各観点を写像することを考える。

＜第1回TFでの指摘＞

○安全といっても、人命や資産という物理的な影響以外にも、経済性の混乱や生活の不便性等、様々ある。

○プライバシーの問題が発生したときに、プライバシー侵害は、事案によっては極めて大きな損害につながるケースがある。最近の精神的損害や刑事責任との関係の位置づけ、さらに、法的な責任とは別に事故が起きた場合のレピュテーションリスクをどこに置くべきなのか等、気になっている。

＜ISO/IEC GUIDE 51:2014（JIS Z 8051:2015)＞

3.14
安全（safety）
許容不可能なリスク（3.9）がないこと。

3.9
リスク（risk）
危害（3.1）の発生確率及びその危害の度合いの組合せ。

3.1
危害（harm）
人への傷害若しくは健康障害、又は財産及び環境への損害。

前回TF等でのご意見について

いただいた御意見

- **カテゴライズ、マッピングの考え方**に関する御意見。
  - 同じ機器でも、システムの中で重要な位置づけのものもあれば、別のものでリカバー出来るものもあり、影響が異なるのではないか。機器単体ではなくシステムで捉えるべきではないか。
  - 本TFの対象は第2層であり製品だけでなくサービスも関連するため、製品ではなく機能的な部分で整理した方が良いのではないか。
  - リカバリの困難性や、尺度の定義など整理する必要があるのではないか。

今後の方針（案）

- 同じ機器であったとしても、その用途により、重要性や課題、インシデントによる影響等が大きく異なるため、使用形態などによってマッピング先が異なり得ることに留意する必要がある旨、整理。
- マッピングの単位として、機器やシステムだけでなく、機能に着目してマッピングを行うこともできることを明確化。
- 算出が比較的難しい発生確率は考慮せず、インシデントが発生した場合の影響の度合いからカテゴライズを行うアプローチを採用。

前回TF等でのご意見について

いただいた御意見

- **カテゴライズ、マッピングの考え方**に関する御意見。
  - 名誉とプライバシーは違う概念であるので、プライバシー/名誉というような位置づけにした方がより正確ではないか。
  - 回復できる/できないという観点と、回復が早い/遅いという観点があるのではないか。
  - 資産やレピュテーションに対し、生活への影響や社会的な影響はもう少し上位の概念に属しており、資産やレピュテーションに何が起きているのかというような波及効果的なものがあるのではないか。
  - リカバリの困難性と経済影響の2軸の整理は非常に分かりやすい。

今後の方針（案）

- プライバシーと名誉について、並列に扱う。
- 回復の可能性だけでなく、回復の早さについても言及。
- 金銭的価値に換算可能なリスクについて、様々な可能性が考えられ、その波及についても際限がないため、今回は具体化せず包括的に整理。

前回TF等でのご意見について

いただいた御意見

- **セキュリティ・セーフティ要求の考え方**に関する御意見。
  - セキュリティ・セーフティ要求として、運用者の認証は必要。自主検査や検査員の資格についても考慮が必要。
  - セキュリティ・セーフティ要求の中のどこかにライフサイクル管理を入れるべき。エンドオブライフ（EOL）やエンドオブサービス（EOS）、耐用年数など定義も様々。
  - セーフティ、セキュリティ、利便性というものに対してはコストがかかるという共通理解は重要ではないか。

今後の方針（案）

- セキュリティ・セーフティ要求を検討する軸を、運用前、運用中、運用者、その他（社会的なサポート）の4つの観点として再整理。
- 運用中の確認要求として、ライフサイクルやサービス期間を考慮して検討する必要があることを明示。
- セキュリティ・セーフティ要求の強度について、コストがかかるものであることについて触れる。

フィジカル空間とサイバー空間のつながりの信頼性を確保するための フレームワークの提案について

- これまでのTFでの議論を踏まえ、フィジカル・サイバー間をつなげる機器・システムにおけるセキュリティ・セーフティ要求の強度を適切に検討するため、それらの**機器・システムのカテゴライズおよびセキュリティ・セーフティ要求の検討に資するフレームワーク**を提案する。

<目次>

1. 本フレームワークの必要性
1-1 CPSFにおける第2層（フィジカル空間とサイバー空間のつながり）
1-1-1 CPSF概論
1-1-2 第2層の位置づけ
1-2 本フレームワークの目的
2. 本フレームワークの想定読者
3. 本フレームワークの基本構成
3-1 基本構成の背景にある考え方
3-2 フィジカル・サイバー間をつなげる機器・システムに潜むリスクの整理
3-2-1 第1軸：発生したインシデントの影響の回復困難性の度合い
3-2-2 第2軸：発生したインシデントの経済的影響の度合い（金銭的価値への換算）
3-2-3 フィジカル・サイバー間をつなげる機器・システムのカテゴライズ
3-3 求められるセキュリティ・セーフティ要求の整理
3-3-1 第1の観点：フィジカル・サイバー間をつなぐ機器・システムの運用前における確認要求
3-3-2 第2の観点：フィジカル・サイバー間をつなぐ機器・システムの運用中の確認要求
3-3-3 第3の観点：機器・システムの運用・管理を行う者の能力に関する確認要求
3-3-4 第4の観点：その他、社会的なサポート等の仕組みの要求
4. 本フレームワークの活用方法

フレームワークの必要性、想定読者

- IoT等の新たな仕組み・サービスに関するセキュリティ・セーフティについて、**包括的に課題を捉える統一的な手法が欠如**しており、対応策が不整合となること等による社会として新たな仕組みを**受容・管理していくためのコストが増大する恐れ**がある。
- 新たな仕組みによってもたらされる新たなリスクに着目し、リスク形態及びそうしたリスクに対応するセキュリティ・セーフティ対策の類型化の手法を提示。サイバー空間とフィジカル空間をつなぐ、新たな仕組みを**社会として効果的に受容していくことができるようにするための基本的共通基盤を提供する**ことを目的とする。

<目次>

1. 本フレームワークの必要性

1-1 CPSFにおける第2層
（フィジカル空間とサイバー空間のつながり）

1-1-1 CPSF概論

1-1-2 第2層の位置づけ

1-2 本フレームワークの目的

2. 本フレームワークの想定読者

想定読者

- IoTを活用してサイバー空間とフィジカル空間をつなぐ新たな仕組み・サービスを実現しようとする者
- そのような新たな仕組み・サービスで活用されるIoT機器・システムの開発を行う者
- そのような新たな仕組み・サービスを適切に管理していく制度・環境を実現していこうとする者
- IoTによる新たな仕組み・サービスを受ける者

フレームワークの基本構成（機器・システムのカテゴライズ）

- IoT機器・システムにおけるセキュリティ上の課題は多様であり、**一律のセキュリティ要求を課すのは適切ではない。**多様性に対してどうアプローチするかが重要。
- そこで、発生したインシデントによる人命/身体に対する影響を表す**「回復困難性の度合い」**と、回復の可能性・困難性という観点を除いて影響の大きさを金銭的価値に換算した**「経済的影響の度合い」**の2軸を用い、フィジカル・サイバー間をつなげる機器・システムに潜むリスクを整理。**リスクに応じて機器・システムをカテゴライズ**。
- 同じ機器であったとしても、**その用途等により、**重要性や課題、インシデントによる影響等は大きく異なるため、**マッピング先が異なり得る**ことに留意。

<目次>

3.　本フレームワークの基本構成

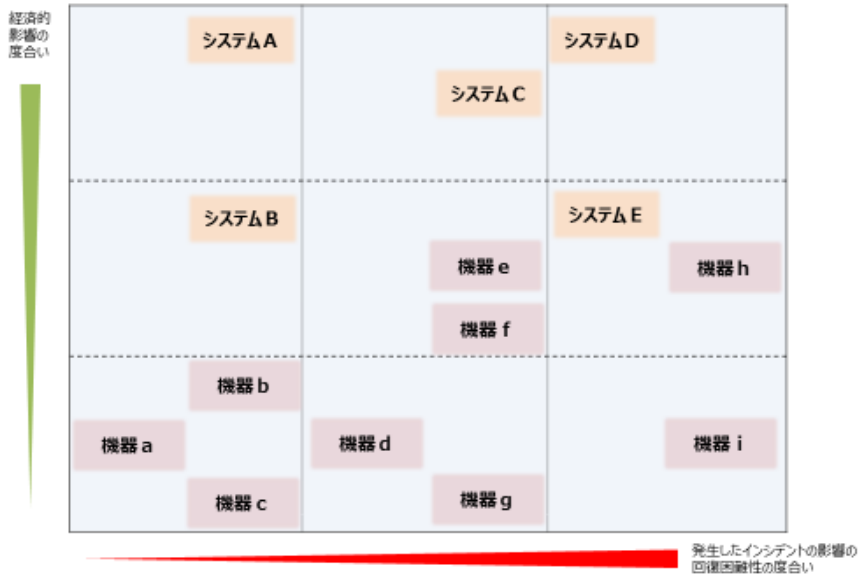
3-1 基本構成の背景にある考え方

3-2 フィジカル・サイバー間をつなげる機器・システムに潜むリスクの整理

3-2-1 第1軸：発生したインシデントの影響の回復困難性の度合い

3-2-2 第2軸：発生したインシデントの経済的影響の度合い（金銭的価値への換算）

3-2-3 フィジカル・サイバー間をつなげる機器・システムのカテゴライズ



フレームワークの基本構成（セキュリティ・セーフティ要求）、活用方法

- セキュリティ・セーフティを確保するための手法を、**運用前、運用中、運用者、社会的なサポートの4つの観点**から整理。
- 各観点はセキュリティ・セーフティ要求に関する内容の考え方の違いに基づいて設定されたものであって、**同じ観点であっても具体的に要求される個々のセキュリティ・セーフティ対策は一様ではない**ことに留意し、**セキュリティ・セーフティ要求の強度を適切に検討するための枠組みとして利用されることを期待**。

<目次>

3.　本フレームワークの基本構成

3-3 求められるセキュリティ・セーフティ要求の整理

3-3-1 第1の観点：フィジカル・サイバー間をつなぐ機器・システムの運用前における確認要求

3-3-2 第2の観点：フィジカル・サイバー間をつなぐ機器・システムの運用中の確認要求

3-3-3 第3の観点：機器・システムの運用・管理を行う者の能力に関する確認要求

3-3-4 第4の観点：その他、社会的なサポート等の仕組みの要求

4.　本フレームワークの活用方法