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8月6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

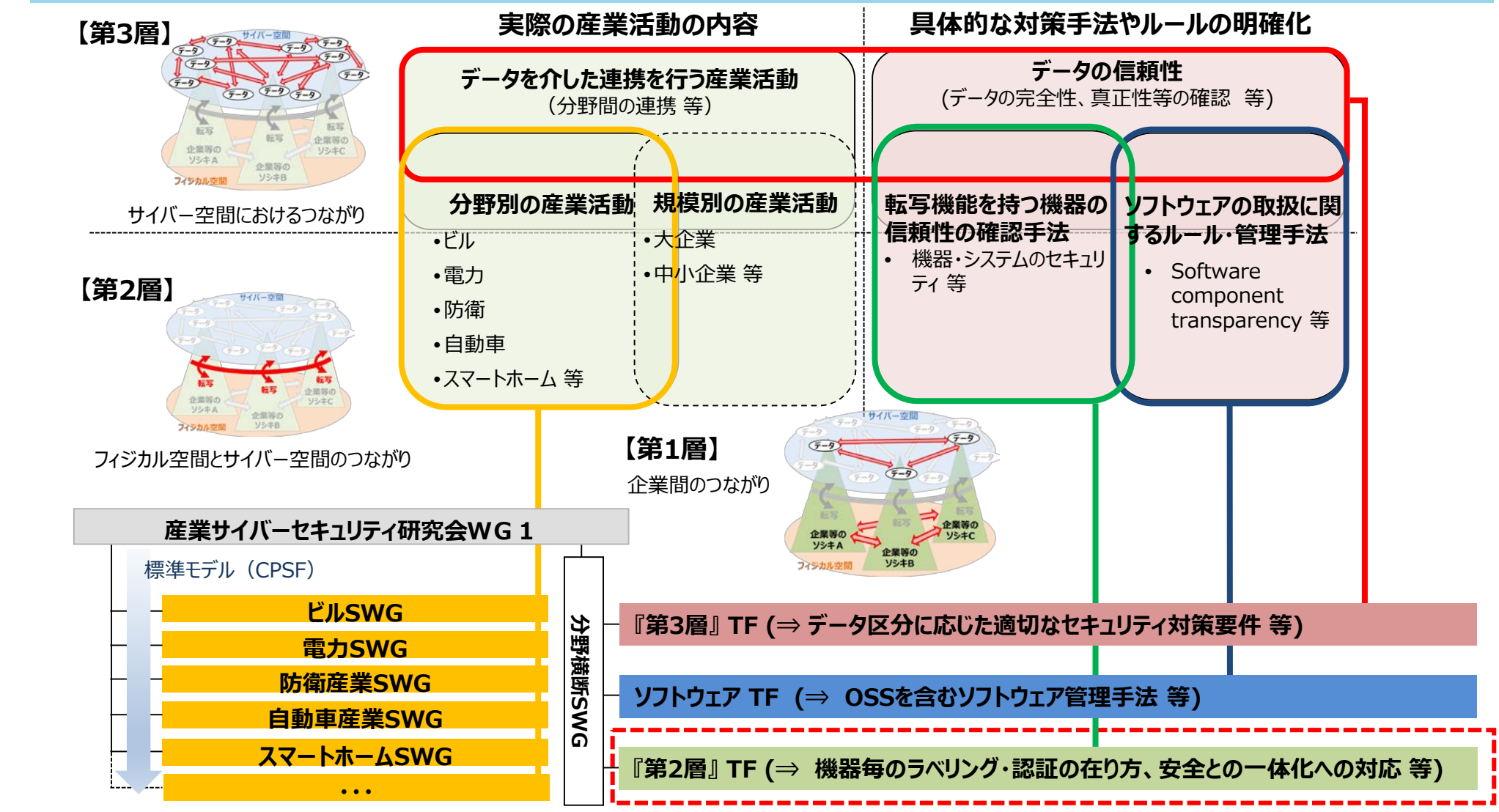
2. サイバー・フィジカル間の転写機能を持つ機器に対する攻撃事案

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）にて議論。**



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）にて議論。**

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**
  - ガイドライン第1版の策定
- **電力SWG**
  - 既存ガイドラインの強化
- **防衛産業SWG**
- **自動車産業SWG**
  - ガイドラインを公表
- **スマートホームSWG**
  - ガイドライン案パブコメ中
- ・・・

分野横断SWG

『第3層』TF：『サイバー空間におけるつながり』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

検討事項：
データマネジメントを俯瞰するモデルを提案し、データの信頼性確保に求められる要件を検討

ソフトウェアTF：サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォース

検討事項：
OSSの管理手法に関するプラクティス集の策定等

『第2層』TF：『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

検討事項：
フィジカル空間とサイバー空間のつながりの信頼性の確保するための「IoTセキュリティ・セーフティ・フレームワーク(IoT-SSF)」のドラフト策定

（参考）スマートホーム、自動車業界におけるCPSFをベースにしたガイドライン策定

- 策定・公表済みのビルガイドライン以外に、**CPSFをベースにした業界別ガイドラインの策定が進行**。
- 特に、**スマートホーム、自動車業界では、ガイドラインの公表に向けた準備が進捗**。

スマートホームSWG

ガイドライン案のパブコメを実施中（～8/31）

目的

- スマートホームにおける安全で安心な生活の実現のため、**幅広いステークホルダーに必要なセキュリティ対策の指針を示す**。

対象範囲

- IoT に対応した住宅設備・家電機器などがサービスと連携することで様々な便益が提供されるスマートホームにおける**多様なステークホルダーが対象**
  - スマートホーム向けの **IoT 機器関連事業者**
  - スマートホーム向けの**サービス事業者**
  - スマートホームの**管理者・住まい手**　　等

ポイント

- 知識やバックグラウンドが様々なステークホルダーに対応するため、ユースケースから想定されるインシデントを基に、**シンプルな対策ガイドから、具体的な対策要件や他の標準との対比まで、階層的に整理**。

今後の方針

- パブコメの意見を踏まえ、正式版公表を目指し、更なるブラッシュアップを進める。

参考：https://www.meti.go.jp/press/2020/07/20200729002/20200729002.html

自動車産業SWG

5/28 ガイドラインを公表

目的

- **業界全体のセキュリティのレベルアップ**
- 対策レベルの効率的な点検の推進

対象範囲

- 自動車業界の全ての企業の**エンタープライズ領域**
- OEMから小規模会社で最低限必要な必須項目を策定（ただし、強制するものではない）。

ポイント

- 部品やサービス/ソフトウェアのサプライチェーン対応
- **CPSFの対策要件をベースに、業界の実態に即した実施事項レベルや記載方法を検討**して作成。
- チェックリストを活用することにより、各社が自社**の取組状況をセルフチェックできる**。

今後の方針

- トライアルを行い自動車産業としての共通のセキュリティガイドラインとして、本格運用を目指す。
- **今後、工場やコネクティッド等へ対象を拡大**する方針。

参考：http://www.jama.or.jp/it/cyb_sec/cyb_sec_guideline.html

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

IoT機器に対する攻撃の状況

- 近年、IoT機器を狙った攻撃は、汎用的なものから、**複数の脆弱性や、特定機器の脆弱性を悪用するものへと攻撃対象や手法の幅を拡大**している。
- 2016年に猛威を振るったMiraiの亜種による攻撃も発生。

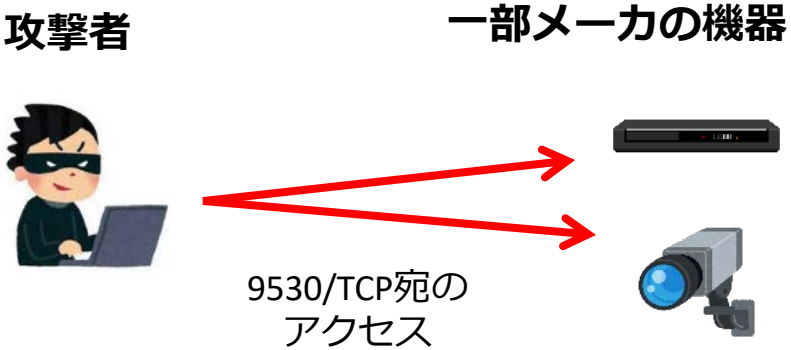
直近のIoT機器を狙った脅威事例(Mirai亜種)

■Mirai亜種(XTC)による感染活動の活発化

➢4月以降、DDoS攻撃実行機能を備えるMirai亜種(XTC)により用いられる9673/TCPに対するアクセス数が急増

■9530/TCPへのMiraiの特徴を有するアクセス

➢2月以降、**一部ビデオレコーダ等の脆弱性**を狙った9530/TCP通信(※)が急増、警察庁等が注意喚起を発出



※特定のデータを送り込むことで、Telnetが有効になる脆弱性を悪用

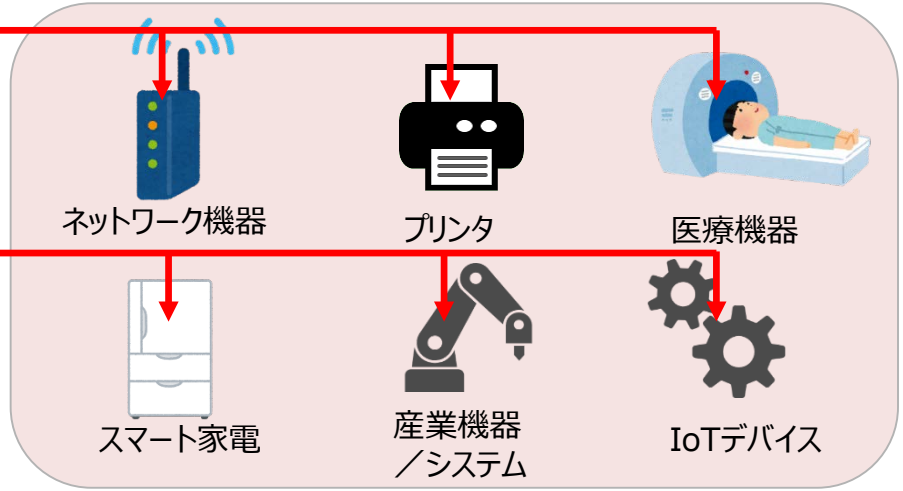
プロトコルスタックの脆弱性：“Ripple20”

- 2020年6月、JSOF社は、**Treck社※1が開発したTCP/IPプロトコルスタック※2「Treck TCP/IP Stack」に複数の脆弱性**があることを発表（発表年や当スタックが20年以上前から存在していること等に由来し、19の脆弱性の総称をRipple20と命名）。遠隔の第三者によって、**任意のコード実行、情報の窃取、サービス運用妨害（DoS）等の攻撃を受ける可能性**があり、最新バージョンへの更新やパッチの適用、IPパケットのフィルタリング等の対策を呼び掛けている。
- Treck TCP/IP Stackは多数の企業が製品に採用しており、数億台かそれ以上の機器が影響を受けるとされ、家庭向けデバイス、ネットワーク機器、医療機器、産業制御機器／システム、重要インフラ分野などの幅広い領域への影響が懸念される。

◆攻撃イメージ／影響範囲の例

想定被害：任意のコード実行、情報漏えい、DoS

Treck TCP/IP Stackの採用製品は、下図以外にも多岐に渡る



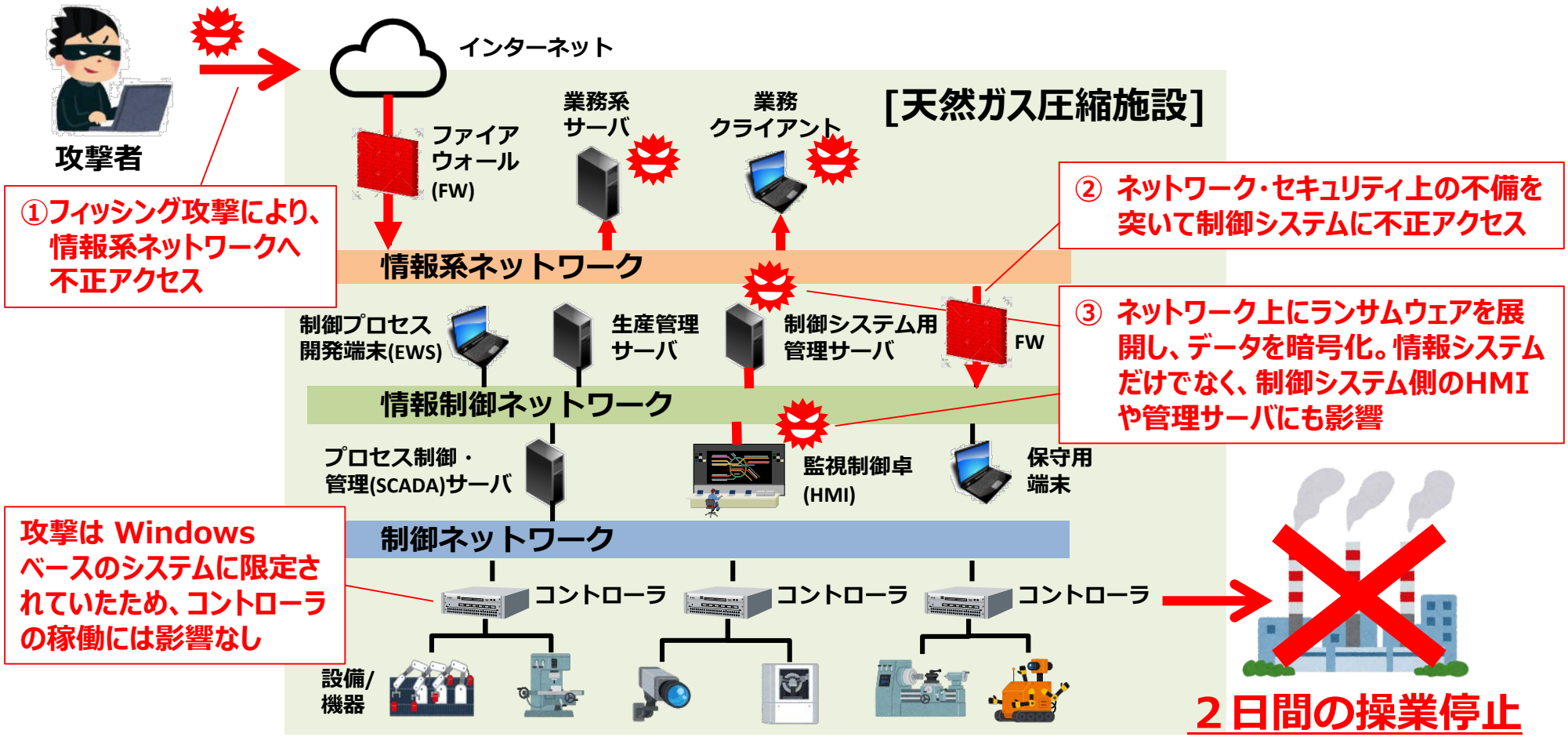
- ✓ Treck TCP/IP StackはHP社、Schneider Electric社、Intel社、Rockwell Automation社、Caterpillar社、Baxter社等の製品が採用。
- ✓ 同様の脆弱性が、関連する他のTCP/IPスタックにも存在することが報告されている。

https://www.jsof-tech.com/ripple20/

※1　組み込み機器向けのインターネットプロトコルスタックを設計・開発する米国の企業
※2　階層構造で構成されるインターネットプロトコル群

ランサムウェアによる制御システムへの被害

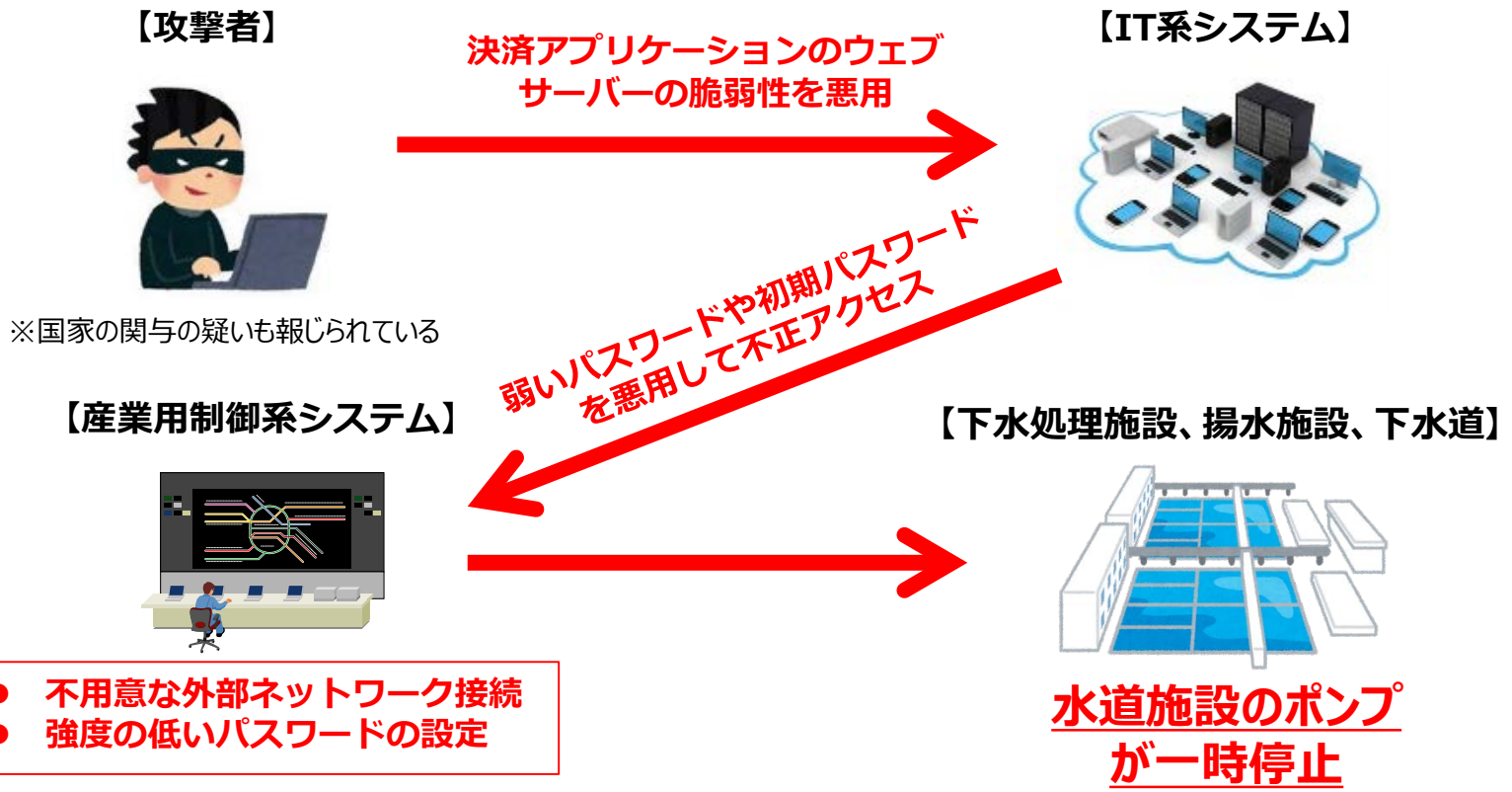
- ランサムウェアによる制御システムや事業継続への被害は継続的に発生している状況にある。
- 米国サイバーセキュリティ・インフラセキュリティ局(CISA)は、今年2月に同国の**天然ガス圧縮施設がランサムウェアを使った攻撃を受け、2日間の操業停止に追い込まれた**と報告している。



（出典）CISA ”Alert (AA20-049A) Ransomware Impacting Pipeline Operations”

イスラエル水道システムへの組織的サイバー攻撃

- 2020年4月、イスラエル政府は、**廃水処理場、ポンプ場、下水施設の監視制御・データ収集(SCADA)システムを狙った組織的な攻撃**があったとの報告を受けたと発表。
- 同国政府から、事前に制御システムや塩素制御装置のパスワードを変更するよう指示が出ていたが、**適切な対策が取られていなかった水道施設のポンプが一時停止**。攻撃の最終目的は、同国の家庭用水道水に入る塩素量の増加だった、との見方が一部メディアで紹介されている。



（出典）各種公開情報に基づき経済産業省作成

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**
- **EUCC Candidate Scheme**
- 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
→ **EN 303 645**

消費者向けIoT製品のセキュリティに関する行動規範

Arm：PSA Certified

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

州・大学・団体 等
- カリフォルニア州：IoTセキュリティ法
- **CSDE：The C2 Consensus on IoT Device Security Baseline Capabilities**

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 – Foundational Cybersecurity Activities for IoT Device Manufacturers

- 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5月に最終版を公開**)。なお、関連文書であるNISTIR 8259Aにて、**6つのサイバーセキュリティ機能※をIoT機器が備えるべきベースラインと定義**した上で、当該機能を達成するために実装すべき共通の要素や、既存のIoTセキュリティガイダンスへの参照を記載。

※ なお、NISTIR 8259Aではこれらのサイバーセキュリティの機能の実装を必須としていない。

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：想定顧客の特定、想定ユースケースの定義 活動2：顧客が有するサイバーセキュリティのニーズ及び目的の調査 活動3：顧客のニーズ及び目的への対処方法の決定（NISTIR 8259Aにてベースラインとなるコアサイバーセキュリティ機能を定義） 活動4：顧客のニーズ及び目的の適切なサポートに向けた計画（ハードウェア、ソフトウェアの適切なプロビジョニング、ビジネスリソースの考慮）
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手段の定義 活動6：顧客に伝える内容と伝達方法の決定（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、デバイス構成・機能、ソフトウェアの更新、デバイスの廃止オプション、技術的及び非技術的手段）

6つのコアサイバーセキュリティ機能（NISTIR 8259Aにて定義）

（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正規のエンティティのみに制限できる。
（2）**デバイスの構成**： IoT機器のソフトウェアの構成変更を、正規のエンティティのみが行うことができる。	（5）**ソフトウェアの更新**： IoT機器のソフトウェアは、安全かつ設定可能なメカニズムを用いる正規のエンティティにみによってのみ更新できる。
（3）**データ保護**： IoT機器が保存・伝送するデータを不正アクセス及び改ざん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機器は自身のセキュリティに関する状態を報告し、その情報に対するアクセスを正規のエンティティのみに制限する。

（参考）NIST - Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF)

- NISTは、セキュリティに配慮したソフトウェア開発手法を既存の標準やガイドライン等を参照する形でSecure Software Development Framework (SSDF)として整理（2020年4月に最終版を公開）。
- SSDFでは、各手法を「組織構築」「ソフトウェア保護」「セキュアなソフトウェア」「脆弱性対応」の4つに分類の上、何をすべきか（Practice-Taskの2階層）、事例、参照文書について体系化。

【 SSDFにおける各手法の分類】

分類	分類（英語名）	概要	手法例	備考
組織構築	Prepare the Organization（PO）	人材、処理能力、技術等のソフトウェア開発リソース確保	• ソフトウェア開発におけるセキュリティ要件を定義 • 各役割と責任の実装	• PSの中でSBOMの作成と維持について言及あり • 参照文書（Reference）は、ISO、BSA、NIST CSF 等
ソフトウェア保護	Protect the Software（PS）	ソフトウェアの全てのコンポーネントを改ざんや不正アクセスから保護	• 全ての形式のコードを改ざんや不正アクセスから保護	
セキュアなソフトウェア	Produce Well-Secured Software（PW）	ソフトウェアリリース時のセキュリティに関する脆弱性を最小化	• ソフトウェアデザインにおけるセキュリティ要件への合致とリスク低減	
脆弱性対応	Respond to Vulnerabilities（RV）	ソフトウェアセキュリティの脆弱性の認識、適切な対応、将来にわたる予防策	• 継続的な脆弱性の特定・確認 • 脆弱性の評価・優先付け・修正	

CSDE : The C2 Consensus on IoT Device Security Baseline Capabilities

- セキュアなデジタル経済に向けた評議会（CSDE: Council to Secure the Digital Economy）※1が、IoT機器を対象に、セキュリティ機能のベースラインを産業界や政府に提供することを目的として発行。（2019年9月発行）
- IoT機器の機能、及び組織におけるプロダクトライフサイクルの管理機能の面から、分野横断的に広く適用可能なベストプラクティスとして13項目のベースラインを特定。各項目毎に留意すべき論点を列記。

※1 ベライゾン、AT&T、NTT、テレフォニカ、IBM、インテル、オラクル、サムスン、エリクソン、SAP、シスコ等が参画

IoT機器セキュリティ機能の合意された※2ベースライン

No	種類	定義	No	種類	定義
1	セキュアなIoT機器の機能	機器のID	8	セキュアなIoT機器の機能	暗号技術
2		セキュアなアクセス	9		パッチ適用性
3		通信中のデータの保護	10		リプロビジョニング
4		保管中のデータの保護	11	プロダクトライフサイクルの管理機能	脆弱性の提出と処理プロセス
5		産業界に認められた通信プロトコルの使用	12		ライフサイクルの終了(EoL)/サービス終了(EoS)の更新と開示
6		データ検証	13		機器利用目的の文書化
7		イベントログ			

※2 合意された（consensus）について、満場一致（unanimity）の意味ではなく、完全な合意が得られなかった場合には主な長所と短所を記すとの記載がある。

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。
- 2020年2月、ENISAがIoT、クラウドインフラ及びクラウドサービス、電子医療記録、トラストサービス等の4分野について、欧州サイバーセキュリティ認証フレームワークの「候補スキーム(Candidate Scheme)」を提案するホワイトペーパーを公開。
- 2020年6月、利害関係者サイバーセキュリティ認証グループ(SCCG)を設置し、「Union rolling work programme」の議論を加速。
- 2020年7月、**ENISAがCommon Criteria等を参照した認証フレームワークにおける最初の候補スキームである「EUCC」のドラフト版を公開。**プレスリリースには、2つ目の候補スキームとしてクラウドサービスに関連するものを準備中であるとの記載も。

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）

ENISA：Cybersecurity Certification （EUCC Candidate Scheme）

- EUCC Candidate Schemeは、ICT製品を対象とするCommon Criteria（CC：ISO/IEC15408）と、関連する共通評価方法（ISO/IEC 18045）に基づく**欧州サイバーセキュリティ認証フレームワークにおける最初の候補スキーム**（2020年7月ドラフト版発行）。欧州においてSOG-IS※1の下で運用されていた**既存のCCのスキームの後継**として機能させることが目的。
- 本文書では、評価はCCに基づくものであること（3章）、保証レベルは「substantial」か「high」の2段階であること（4章）、自己適合性評価は認められないこと（5章）、認証証明書の有効期間は最長5年間であること（20章）等、**Cybersecurity Actにより候補スキームに必要とされる要件**（認証取得の際に実装すべき要求事項やその評価プロセス、認証制度の運用等に関する事項等）**を網羅的に規定**。

※1欧州におけるCC加盟国の認証機関間の調整を行う組織

本文書の目次と、関連するCybersecurity Act 54条1項の項目 a – v の対応*

章	目次	*
1	主題とスコープ	a
2	本スキームの目的	b
3	評価標準	c
4	保証レベル	d
5	自己適合性評価	e
6	認証機関向けの具体的な要求事項	f
7	認証機関の通知と認可	f
8	具体的な評価基準及び評価手法	g
9	認証に必要な情報	h

章	目次	*
10	マークとラベル	i
11	コンプライアンスを監視するための規則	j
12	認証証明書の発行、維持、継続および更新の条件	k
13	違反に関する規則	l
14	脆弱性管理に関する規則	m
15	パッチ管理	m
16	認証機関による記録の保持	n
17	国家的または国際的なスキーム	o
18	認証証明書の内容とフォーマット	p

章	目次	*
19	情報の可用性	q
20	認証証明書の有効期間	r
21	認証証明書の開示ポリシー	s
22	第三国との相互認証	t
23	ピア評価	u
24	補足的なサイバーセキュリティ情報—第55条	v
25	スキームの追加要素	a
26	アドホックWGからの推奨事項	-
27	参考	-

（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

EN 303 645 – Cyber Security for Consumer Internet of Things: Baseline Requirements(ETSI)

- 2018年10月に、英国で策定された「消費者向けIoT製品のセキュリティに関する行動規範」に基づく欧州標準。本文書は**消費者向けIoT製品のセキュリティベースラインを確立**し、**今後のIoT認証スキームの基礎を提供する**としている。（2020年6月に最終版を公開）
- 消費者向けIoT製品のセキュリティを確保するための開発・製造者向けガイダンスであり、消費者IoTのためのサイバーセキュリティ規定（1-13）及びデータ保護規定（14）を記載している。
- 現時点では推奨事項であるが、将来の改訂において義務化される可能性も言及されている。また、別添で各規定は必須要件(M)と推奨要件(R)、条件付き必須要件(MC)等に細分化されている。

消費者IoTのためのサイバーセキュリティ規定及びデータ保護規定

No	規定内容	No	規定内容
1	単一のデフォルトパスワードを使用しない	8	パーソナルデータの安全性を確保する
2	脆弱性の報告管理手段を実装する	9	ネットワークの停止・停電等に対するシステムのレジリエンスを確保する
3	ソフトウェアを定期的に更新する	10	システムの遠隔データを調査する
4	機密性の高いセキュリティパラメータを安全に保存する	11	ユーザーが自身のデータを容易に削除できるようにする
5	安全に通信する	12	機器の設置とメンテナンスを容易にできるようにする
6	攻撃対象になる場所を最小限に抑える	13	入力データを検証する
7	ソフトウェアの完全性を確保する	14	個人データを保護するための機能を提供する

規定内容の例

「ソフトウェアを定期的に更新する」の例

必須要件(M)
ネットワークインタフェース上でアップデートが配信される場合、機器は信頼関係（トラストリレーションシップ）を通じて真正性と完全性を検証しなければならない。

推奨要件(R)
消費者IoT機器における全てのソフトウェアコンポーネントが、安全にアップデートできるようにすべきである。

条件付き必須要件(MC)
制約を受けた機器ではない場合、機器は安全にアップデートをインストールするための仕組みを有しなければならない。

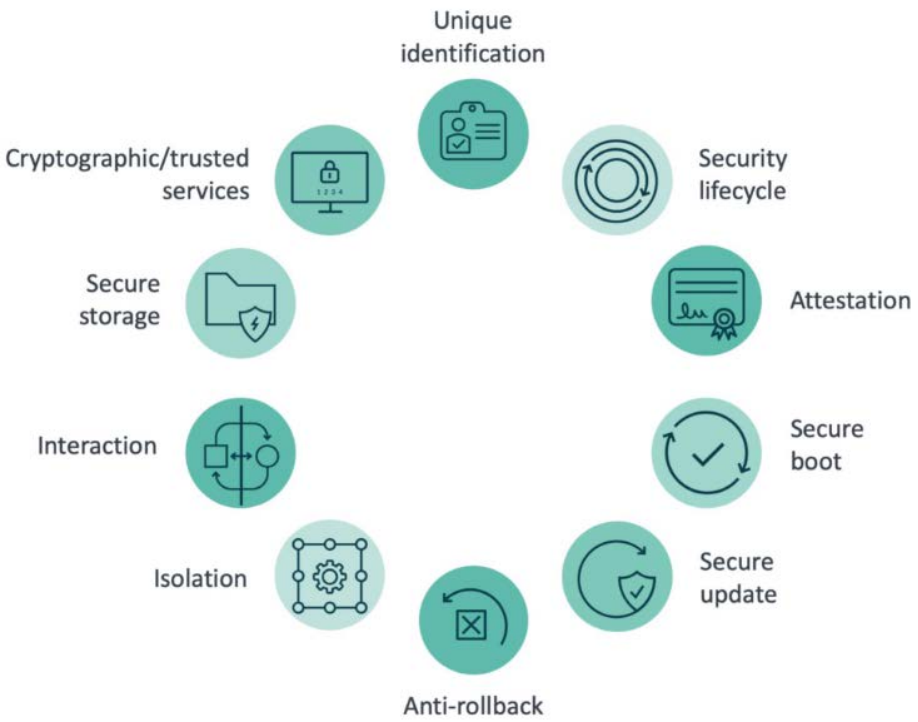
条件付き推奨要件(RC)
ソフトウェアのアップデートに、自動的なアップデートの仕組みが用いられるべきである。

民間におけるIoT製品認定の取組み (PSA Certified)

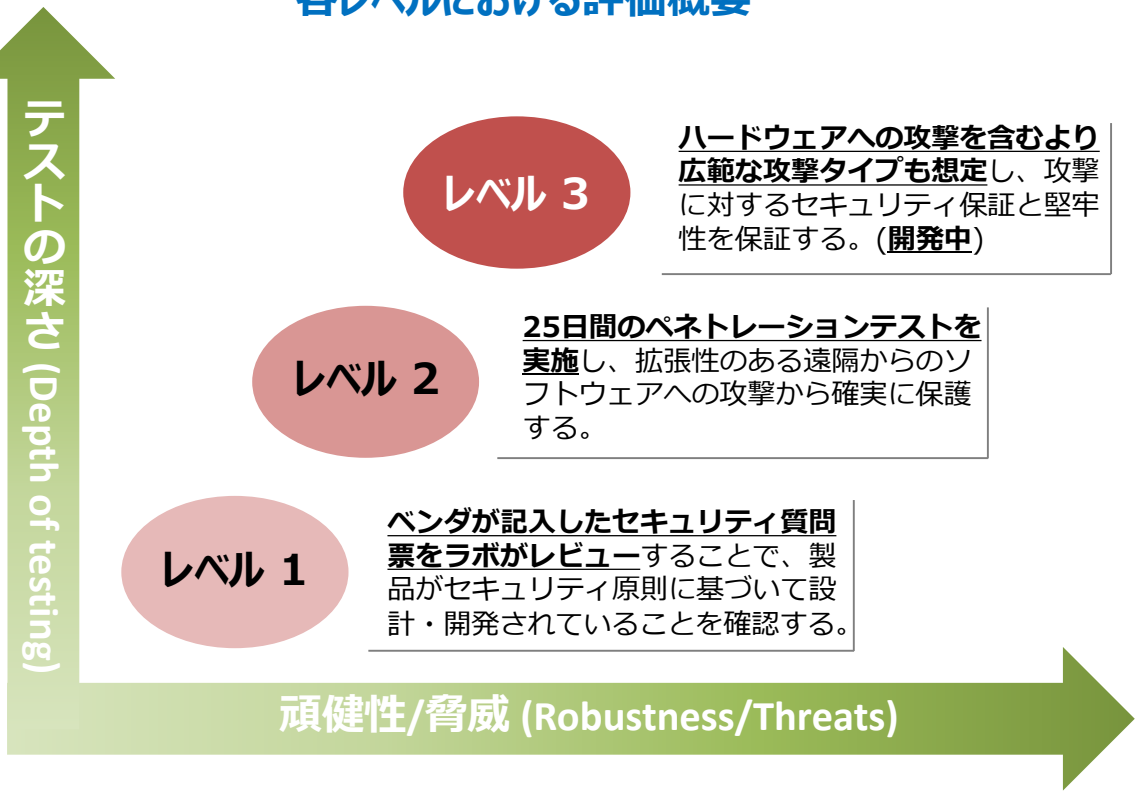
- PSA (Platform Security Architecture) Certifiedは、Armが複数のセキュリティテストラボや認証機関と立ち上げたIoT製品におけるチップ※に対する認定スキーム。
- IoTにおける脅威モデルや、PSA Security Model documentにおける10のゴールから開発された40問程度の質問票とインタビューからなるレベル1に対し、レベル2では25日間のペネトレーションテストを実施するなど、段階に応じた評価を行う構成になっている。

※ レベル1ではRTOSやデバイスも対象

PSA Security Model - 10のゴール



各レベルにおける評価概要



（出典）「PSA Certified™」(https://www.psacertified.org/)

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

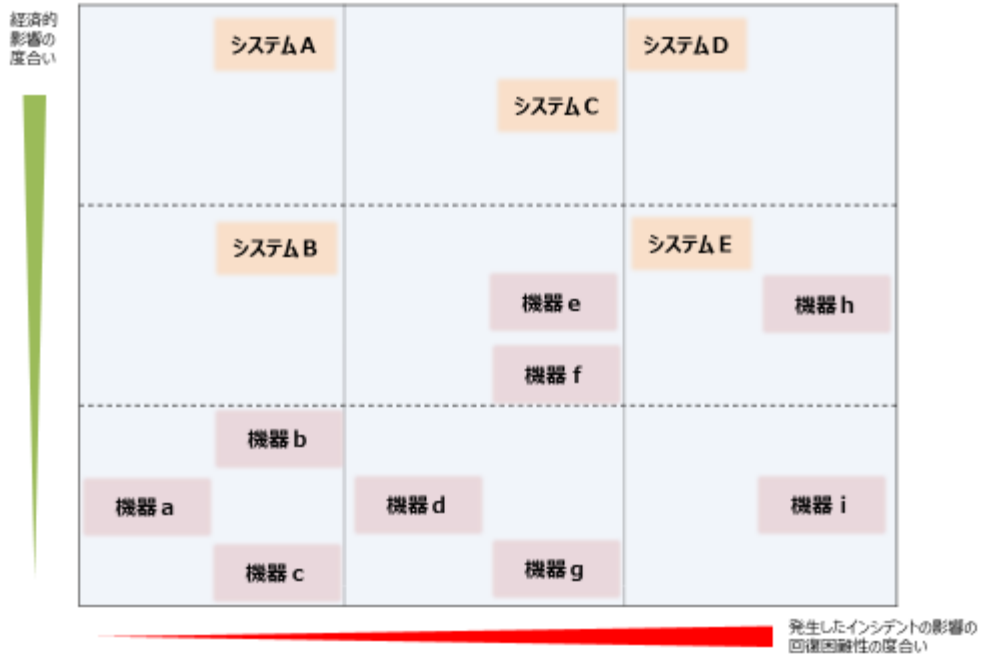
3. サイバー・フィジカル間の転写機能を持つ機器の信頼性確保に
   向けた諸外国の検討状況

4. 本タスクフォースにおける検討事項

IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF）の案の策定

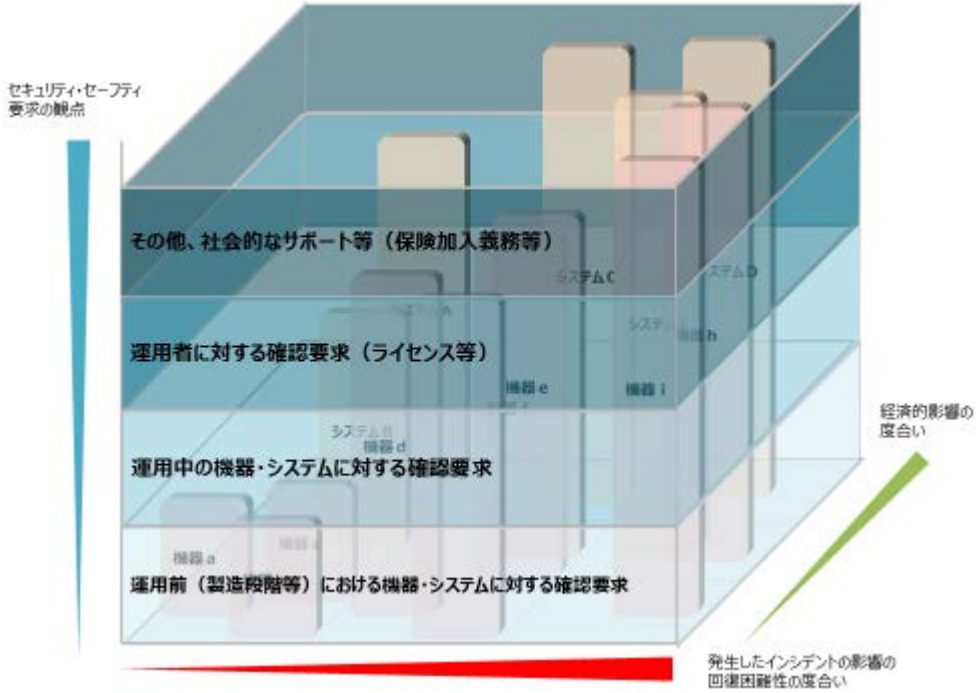
- IoT機器・システムの性質や利用環境によって課題が一様ではないことに着目し、IoT機器・システムをリスクに応じてカテゴライズした上で、それぞれに対するセキュリティ・セーフティ要求を検討することが重要。
- IoT機器・システムのカテゴライズやセキュリティ・セーフティ要求の検討に資するフレームワーク「IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF）」の案を策定。世界中から幅広く意見を収集するため、日本語版・英語版のパブコメを実施（2020年3月31日～6月24日）。

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のイメージ



※ 同じ機器でも使用形態などによってマッピング先が異なり得る。
例えば、機器gと機器hが同じ機器で異なる使用形態である場合などがあり得る。）

カテゴリに応じて求められる
セキュリティ・セーフティ要求の観点のイメージ



IoTセキュリティ・セーフティ・フレームワークのパブコメ概要

- **IoTセキュリティ・セーフティ・フレームワーク**の原案に対するパブリックコメントを令和2年3月31日～6月24日に実施。
- 海外からの関心が高く、英語版パブコメも実施。
- **国内15、海外10の組織・個人より、約100件の意見提出**あり。

主な御意見

① **IoT-SSFのコンセプトやスコープ**に関する御意見
② **リスクに基づく機器・システムのカテゴライズ**に関する御意見
③ **求められるセキュリティ・セーフティ要求の観点**に関する御意見
④ **具体的な実装や要求事項**に関する御意見
⑤ **国際規格やガイドライン等との関係**に関する御意見
⑥ **用語の定義**に関する御意見
⑦ **今後の取り組み**に関する御意見

主な御意見とそれに対する考え方①：IoT-SSFのコンセプトやスコープに関する御意見

いただいた御意見

- **IoT-SSFのコンセプトやスコープ**に関する御意見。
  - 本フレームワークの目的は、貴省が進めたいと考えている政策的な介入に関する情報提供を意図しているのか。あるいは、産業界がリスク管理に役立てるために利用することを意図しているのか。【16-2】
  - IoT機器・システムの商業用・運用アプリケーションと、消費者・家庭用製品の両分野に適用されるかどうか、及びどのように適用されるかをより明確にし、これらの分野が各軸にどのような影響を与えるか記述することを助言する。【22-3】
  - 文書全体で明確に強調されている国際的な整合性を確保することを目的に、確認要求が必要とされるのか、あるいは奨励されるのかの文脈について、より明確にすることを提言する。【22-10】
  - IoT機器が動作する複雑なエコシステムを考慮する重要性を認識し、ネットワークレベルを含めて、政策立案者に対してIoTセキュリティへの包括的なアプローチを奨励している本フレームワークのアプローチを高く評価する。【24-1】

御意見に対する考え方

- 本フレームワークの目的は、IoT機器・システムにおけるセキュリティ・セーフティの検討に資する枠組みを共有することで、産業界での議論を促進すること。
- 本文113行目にも記載の通り、本フレームワークは様々な分野におけるIoT機器を想定。
- いただいた御意見を踏まえ、**本フレームワークが強制力を持つものでは無いことを明確化**するため、下記のとおり修正。
  - 129行目に「IoT機器・システムに対する具体的な要求の一律の規定を目的に定めるものではない。」と追記

主な御意見とそれに対する考え方②：リスクに基づく機器・システムのカテゴライズに関する御意見

いただいた御意見

- **リスクに基づく機器・システムのカテゴライズ**に関する御意見。
  - 機器をマッピングするのではなく、機器の機能・リスクをマッピングするべき。【5-1】
  - 「同じ機器でも利用形態などによりマッピング先が異なりえることに留意する必要がある。」とあるが、マッピング先が異なったら何を考慮しなければならないのかについても示唆いただきたい。【10-3】

御意見に対する考え方

- 機器・システムをマッピングすることとした理由は、同じIoT機器であっても、その使われる環境等により、課題やインシデントによる影響等が大きく異なることを示すため。
- 一般的に、マッピング先により必要なセキュリティ・セーフティ要求が異なり得ると考えられるが、具体的にどのような要求が必要かについては、産業分野等により異なるものであり、産業界等での議論を踏まえた上で、引き続き検討。
- いただいた御意見を踏まえ、マッピングの対象が機器であることを明確化するため、下記のとおり修正。
  - 181行目の記載を「フィジカル・サイバー間をつなぐ機器・システムを当該機器・システムに潜むリスクに基づいてカテゴライズし、マッピングする2つの軸として設定することとした」に修正。

主な御意見とそれに対する考え方③：求められるセキュリティ・セーフティ要求の観点に関する御意見（1/3）

いただいた御意見

- **求められるセキュリティ・セーフティ要求の観点**に関する御意見。
  - 殆どの国際規格やガイドラインでは、「リスク」という用語を「起こり易さ（発生確率）」との関係で定義しており、「起こり易さ」を除外した時点で、本フレームワークで「リスク」という用語を使うことは混乱を生じさせるものと思われるため、除外しても差し支えがない根拠を明示するか、注記が必要ではないか。【3-3】
  - 第3軸として上げられている4つの観点が、これら自体に順序関係や包含関係があるのか否かが分かり難い。【3-5】

御意見に対する考え方

- いただいた御意見を踏まえ、本フレームワークにおける**「発生確率」の取扱や各観点の関係性をより詳細に説明**するため、下記のとおり修正。
  - 204行目に「なお、本フレームワークに基づき、産業界での議論等を踏まえた上で具体的な要求を整理する際には、発生確率についても考慮することが適切であることに留意されたい。」を追記。
  - 326行目に「なお、対策の実施はコストに直結することから、求められるセキュリティ・セーフティ要求に対しどのような対策を取るかは、インシデントの発生確率等も踏まえた上で決定されることが適当である。」を追記。
  - 図6「カテゴリに応じて求められるセキュリティ・セーフティ要求の観点のイメージ」における青矢印を削除し、第1の観点～第4の観点という文字に修正。
  - 308行目に「なお、第3軸における4つの観点は、それぞれが必ずしも完全に独立したものではない。」と追記。
  - 313行目に「また、必ずしも全ての観点での要求が求められるものではなく、例えば第2の観点に係る要求が無くとも、第1や第3の観点に係る要求により対策を構成することも考え得る。」と追記。

主な御意見とそれに対する考え方③：求められるセキュリティ・セーフティ要求の観点に関する御意見（2/3）

いただいた御意見

- **求められるセキュリティ・セーフティ要求の観点**に関する御意見。
  - 「セキュリティ・セーフティ要求の観点」においては、運用前の部分と運用中の部分の関係性の明確化が必要【9-3】
  - 製造段階と運用段階の間にある統合という中間のステージも考慮する必要がある。【18-1】
  - 運用前と運用中の要件を含め、様々な観点から望ましいIoTセキュリティ・セーフティ要求を見ることを提案しており、両フェーズにおけるセキュリティ要求が重要であることに同意。【20-4】

御意見に対する考え方

- 運用前、運用中など、**ライフサイクルのステージの整理の仕方は、業界や対象とする機器・システムによって異なる**と考えられ、各産業界や機器・システムの性質等を踏まえて、ステージを整理し、各ステージで求められるセキュリティ・セーフティ要求を検討していただくことになる。
- いただいた御意見を踏まえ、下記のとおり修正。
  - 265行目および図6の記載を「運用前（製造段階等）」から「運用前（設計・製造段階等）」に修正。

主な御意見とそれに対する考え方③：求められるセキュリティ・セーフティ要求の観点に関する御意見（3/3）

いただいた御意見

- **求められるセキュリティ・セーフティ要求の観点**に関する御意見。
  - 「運用者」とはサービスを提供する人なのか、オペレータなのか、また「使用者」とはサービス利用者なのかサービス提供者なのかの定義が明確になっていない。【9-4】

御意見に対する考え方

- 運用者とは主にオペレータを、IoT機器・システムを使用する者とは利用者を想定しているが、例えば、システムを所有している者が、システムの運用を他の者に委託しているケースなど、**様々なケースが考えられる。ステークホルダーの関係が整理されることが重要**である。
- いただいた御意見を踏まえ、IoT機器・システムのリスクに対して**幅広いステークホルダーが負担を検討し、合意する必要があることを明確化**するため、下記のとおり修正。
  - 297行目に「なお、ここでいう運用者には、サービス提供者のようなシステムを直接操作するわけではない者も含みうる。」を追記。
  - 312行目に「使用方法等の情報を提供する際には、どのようにしてその情報へのアクセシビリティを向上させるかも検討する必要がある。」を追記。
  - 315行目に「この例のように、複数のステークホルダーが関係するリスクへの対処は、複数の観点から行えることから、関係するステークホルダーにおける負担について、各ステークホルダーが機器・システムのリスクに関連する情報を可視化・共有する等の方法を通じて、総合的に検討し、ステークホルダー間で合意する必要がある。したがって、単独のステークホルダーが全ての要求に対処する必要はなく、また、ある観点内であらゆるケースで必須に求められる具体的な要求の規定を一律に求めることは困難である。」を追記。

主な御意見とそれに対する考え方④：具体的な実装や要求事項に関する御意見

いただいた御意見

- **具体的な実装や要求事項**に関する御意見。
  - 要求がカテゴライズされているだけで、「回復困難性が高いシステムはここまで要求する必要がある」ということが分からない。高中低などである程度要求事項を整理しないと活用できるフレームワークにならないのではないか。【3-6】
  - コンセプトや課題の提案にとどまっているように思われ、具体的な対策をまとめている部分が読み取れなかった。このフレームワークの発行後、なんらか具体的なメソッド、基準などを出していただけると開発者は助かる。【10-1】
  - IoTセキュリティを向上させるネットワークレベルでの技術的な推奨事項（機器の常時監視やセグメンテーション等）を、本フレームワークに含めることを推奨する。【24-5】

御意見に対する考え方

- 本フレームワークは、**IoT機器・システムにおけるセキュリティ・セーフティの検討に資する枠組みを共有することを目的**としている。具体的な実装や要求事項は、IoT機器の特性や産業分野等により異なるものであり、ユースケースの取組などによる具体化などについて、引き続き検討。

主な御意見とそれに対する考え方⑤：国際規格やガイドライン等との関係に関する御意見

いただいた御意見

- **国際規格やガイドライン等との関係**に関する御意見。
  - 政府の IoT セキュリティ政策は、世界中の他の同様の取り組みを参考にし、可能な限りそれに沿ったものとすべき。国際的に認められた標準があればそれに基づくべき。【21-1】
  - 本フレームワークは、IoT機器やシステムのセキュリティに対処するための素晴らしい出発点を提示している。しかし、その有用性は最終的には国際的な整合性に依存し、その整合性がなければ貿易とセキュリティの障壁が本フレームワークのドラフト案の提示する多くの利点に勝ってしまう可能性がある。【23-4】

御意見に対する考え方

- 本フレームワーク策定にあたっては、**主要な国際規格等も参照**している。なお、それらの規格の多くは主に機器・システムに対する要求を定めたものと認識しているが、本フレームワークでは、機器・システムだけでなく運用者や社会制度に対する要求についても併せて検討する必要性を強調するなど、より広い視点からIoTセキュリティ・セーフティの検討に資する枠組みを提供している。
- 本フレームワークはIoTセキュリティ・セーフティを社会としてどう捉えるべきかについて考え方を示すものであり、例えば製造者に対する考え方を示した**NISTIR 8259等とは、補完的な役割を担うことができる**と考えている。
- いただいた御意見を踏まえ、**「5. リファレンス」を追加**し、本フレームワーク作成にあたり参照した規格等の文書を記載。

主な御意見とそれに対する考え方⑥：用語の定義に関する御意見

いただいた御意見

- **用語の定義**に関する御意見。
  - セーフティの確保”の”セーフティ”が“セキュリティ・セーフティ”の意味であれば“セキュリティ・セーフティ”にしてほしい。工場、社会インフラ等の安全の意味であれば“安全”とすべき。【9-6】
  - どの機器が対象となるかを可能な限り具体的かつ明確に定義することを推奨する。一般的に、IoT セキュリティポリシーは、国際的に認知された標準に基づいた「IoT 機器」と「IoT システム」の定義を使用すべき。【21-2】

御意見に対する考え方

- 本フレームワークでは「安全性」を「セーフティ」という用語で統一している。107行目は、セーフティとセキュリティの組み合わせが重要である旨を本文中で初めて述べている箇所であることから「セーフティ」を単独で用いている。
- 本フレームワークでは、ISO/IEC 20924:2018におけるIoT機器、システムの定義を準用している。

主な御意見とそれに対する考え方⑦：今後の取り組みに関する御意見

いただいた御意見

- **今後の取り組み**に関する御意見。
  - 今後のユースケースの整理を通して、マッピングやカテゴライズ手法の指針やガイドラインなどの整備が必要【8-2】
  - ユースケースの整理・蓄積において、手法や内容のブラッシュアップのみではなく、人・組織間における連携・統制・体制などにも着目頂ければ、主に新たな仕組み・サービスを実現・管理する読者にとって参考になる。【14-3】
  - 本フレームワークの次のステップを明確にすべき。本フレームワークは自発的なガイダンスと理解した。本フレームワークに関連する法律を検討している場合など、フレームワークの次のステップが明確になれば、企業が次のステップを検討する際に役立つだろう。【19-4】

御意見に対する考え方

- 本フレームワークを有効に活用していくためには、ユースケースの整理が必要。**今後、本フレームワークに基づいて、具体的な仕組み・サービスをユースケースとして整理していく**。