経済産業省

資料３

サブワーキンググループ等の設置・検討状況

平成30年12月25日

経済産業省　商務情報政策局

サイバーセキュリティ課

産業分野ごとの検討の促進：分野別のSWGの設置

- WG1で検討する『サイバー・フィジカル・セキュリティ対策フレームワーク』を、産業分野別に順次展開し、具体的適用のためのセキュリティポリシーを検討。

WG１　制度・技術・標準化

2/7 第1回会合, 3/29 第2回会合,
8/3 第3回会合, **12/25 第4回会合開催**

標準モデル

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

ビル（エレベーター、エネルギー管理等）

2/28 第1回会合, 4/16 第2回会合, 6/11 第3回会合,
7/12 第4回会合,**8/10 第5回会合,**
10/31 第6回会合, 1/9 第7回会合開催予定

電力

6/12 第1回会合, **9/4 第2回会合,**
11/21 第3回会合開催

防衛産業

3/29 第1回会合, **9/5 第2回会合開催**
(防衛装備庁 情報セキュリティ官民検討会)

自動車産業

設置に向けた検討中

スマートホーム

3/13 第1回会合, 4/5 第2回会合, 6/13 第3回会合,
7/18 第4回会合, **9/19 第5回会合, 10/24 第6回会合,**
12/19 第7回会合開催
(JEITA スマートホーム部会 スマートホームサイバーセキュリティWG)

その他コネイン関係分野

コラボレーション・プラットフォーム

ビルSWG（座長：江崎 浩 東京大学 教授）

- ビルの管理・制御システムに係る各種サイバー攻撃のリスクと、それに対するサイバーセキュリティ対策を整理し、ビルに関わるステークホルダーが活用できる**ガイドラインをとりまとめる**。
- オリパラに向けて、**各事業者において実施できる分野から実装**を目指す。

＜構成員＞

有識者、ビルオーナー、ゼネコン、サブコン、設計事務所、個別システム事業者（ビル管理、空調、エレベーター、ビデオ監視、電力・熱供給 等）、自治体、関係省庁 等

＜ガイドラインのとりまとめイメージ＞

- ビルシステム全体に**共通する最低限の要求**をまとめたもの＋**より詳細な方策**を示したものの二階建て構成
- ガイドラインでは、多くの事業者の取組の参考となるよう**優先順位を示した選択肢を提供**

内容項目例

- ビルに係わるサイバーセキュリティ上の脅威の現状
- ビルシステムに対して起こりえる攻撃とその影響の予測
- サイバーセキュリティ確保のための対策の概要
- 対策の具体的内容
- 対策実施に向けたチェックリスト

フェーズ	主な要求概要	関係するステークホルダー
設計・仕様	機器、ネットワーク、物理セキュリティへの要求	設計事務所、オーナー、ゼネコン、サブコン、ベンダー
建設	機器単位、システム単位の施工プロセスへの要求	ゼネコン、サブコン、ベンダー
竣工検査	全体管理体制、管理結果、受入検査への要求	オーナー、ゼネコン、サブコン、ベンダー
運用	管理体制への要求	オーナー、管理運用事業者、ベンダー
改修・廃棄	機器、ネットワーク、物理セキュリティ、管理体制への要求	設計事務所、オーナー、管理運用事業者、ベンダー

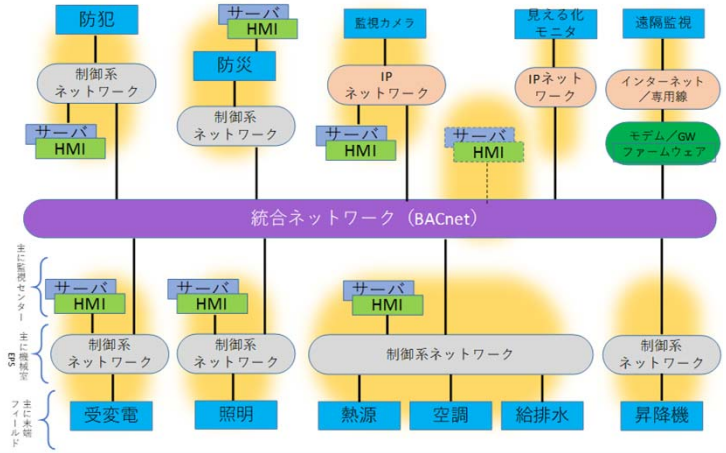
＜検討スケジュールイメージ＞

- **2018年9月：ガイドライン（β版）を公開**
- 2018年度中：β版を用いたトライアル・モデル評価とフィードバック、内容の修正、増強によるガイドライン共通編の完成
- 2019年度以降：ガイドライン共通編（完成版）の本格活用開始、個別編のモデル評価とフィードバック、完成

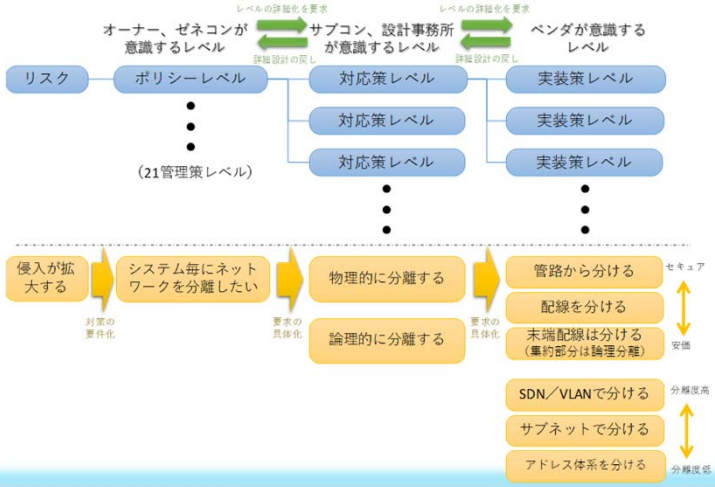
ビルSWG：最新の進捗状況 ～ビルガイドラインβ版を公開（9/3）～

- 前提となるシステムモデルを整理、それぞれの場所や機器へのリスクを抽出。
- 必要な対策をポリシーレベルで整理し、更に具体化、ライフサイクルを越えて対策を整理。

1．検討の前提として標準的なモデル構成を整理

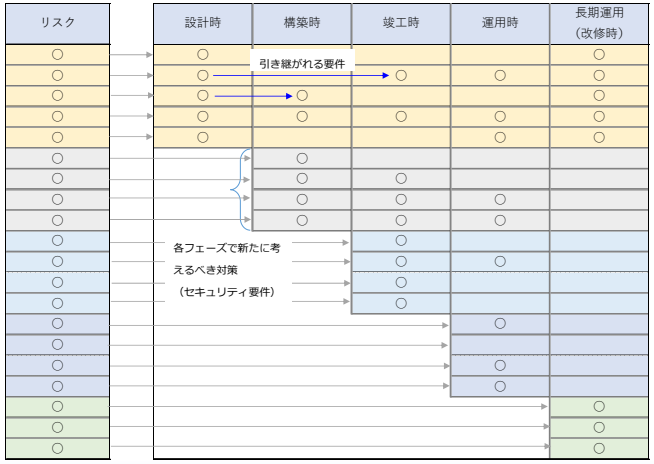


2．対策の階層構造とステークホルダの関係を整理



3．ビルのライフサイクルを意識した対策の整理

場所	対象装置
ネットワーク	
監視センター	HMI
	保守端末
	ネットワーク機器
	サーバ（BA装置）
機械室	
EPS	
末端の設置場所	
その他	



4．ポリシーレベルでの対策の列挙

No.	場所	No.	対象装置／場所	No.	リスク要因・対策の統合	参照No.	No.	脅威が現実化する要因（手段）	参照No.
1	ネットワーク（クラウド、情報系NW、BACnet）	10	ネットワーク						
		11	クラウドサーバ	111	外部ネットワークとの接続があり、情報を遣り取りする通信があるため、その通信を偽装して外部からの侵入を受ける可能性がある。		1111	外部との接続を持つシステムにおいて、システムの脆弱性チェックやセキュリティ対策が十分ではない。	
		12	情報系端末	121	BAシステムと外部システムの接続に当たって十分なセキュリティ確保が行われず、攻撃を受けたり、侵入、悪っ取りを受ける可能性がある。		1211	外部との接続を持つシステムにおいて、システムの脆弱性チェックやセキュリティ対策が十分ではない。	1111
		13	外部接続用ネットワーク機器（FW、ルータ）	131	外部接続を前提とした十分なシステムとしての脆弱性の確認が行われず、脆弱性が放置されたままの状態のため、攻撃を受けたり、侵入、悪っ取りを受ける可能性がある。		1311	外部との接続を持つシステムにおいて、システムの脆弱性チェックやセキュリティ対策が十分ではない。	1111
		14	BAシステム間相互接続（BACnet等）	141	他の設備システムとBACnetを介した相互接続があり、ある設備への侵入が発生すると別の設備に拡大する恐れがある		1411	BACnetによる設備システム間の相互接続において、感染拡大防止等のセキュリティ対策が十分ではない。	
				142	他の設備システムと警報等を伝える物理的接続があり、ある設備の不具合が接続された別の設備に影響を与える恐れがある		1421	他の設備システムとの接続において、不具合による影響発生の排除対策が十分ではない。	
		15	BAネットワークシステム全体	151	システムに対するセキュリティ監視が十分でなく、攻撃の発見や対応が遅れる可能性がある。		1511	システムへのセキュリティ監視が十分ではない。	
2	監視センター（中央制御室）	20	監視センター	201	重要情報やBAシステムの設置・保管場所に、許可を受けた者以外の入室を許してしまい、システム画面の盗み見、端末／制御盤への不用意な操作をされる恐れがある。		2011	監視センター（中央制御室）に対して、許可された入退室に限定するような管理ができていない。	
				202	重要情報やBAシステムの設置・保管場所において、作業員（運用員、保守要員）の権限を超えて、システムや端末／制御盤に対して不要な操作をされる恐れがある。		2021	監視センター（中央制御室）に対して、作業員が許可された以外の作業をすることを防げない。またその作業によって、実際にシステムや端末が操作できてしまうことを防げない。	

今後さらに．．．
- ポリシーレベルから対応策レベル、実装策レベルへと対策案を具体化
- トライアルによるフィードバック

ビルガイドラインβ版の記載内容

ガイドラインβ版の構成

目次 （※実際の公開版は非公開部分を削除し目次番号を繰り上げています）

ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドラインの策定にあたって
1．はじめに
1．1．目的及び適用範囲
1．2．対象者
1．3．サイバー・フィジカル・セキュリティ対策フレームワークとの関係
1．4．文書の構成
2．ビルシステムを巡る状況の変化
2．1．ビルシステムを含む制御システム全般の特徴と脅威の増大
2．2．ビルシステムにおける攻撃事例
3．ビルシステムにおけるサイバーセキュリティ対策の考え方
3．1．ビルシステムの構成の整理
3．2．ビルシステムの特徴
3．3．ビルシステムにおけるサイバーセキュリティ対策の整理方針
4．ビルシステムにおけるリスクと対応ポリシー
4．1．全体管理
4．2．機器ごとの管理策
5．ライフサイクルを考慮したセキュリティ対応策【別紙】※非公開部分
6．セキュリティ対策の具体的内容　※非公開部分
7．本ガイドラインの使い方
7．1．新築の大規模オーナービルにおける使い方
7．2．既存の中規模[redacted]ビルをクラウド移行する際の使い方
7．3．既存ビルへの[redacted]セスメントと対策立案での使い方
付録A　用語集
付録B　JDCCのリファレ[redacted]との関係
付録C　サイバー・フィ[redacted]キュリティ対策フレームワークの考え方とビルシステム[redacted]対策との関係
付録D　参考文献
付録E　経験のレポジト[redacted]

ガイドラインの中心部分

ドキュメントとしては、対策のポリシーまでを記載

詳細な対応策は、設計～改修・廃棄までのビルのライフサイクルのそれぞれの場面でブレークダウンして別表としてインデックス化

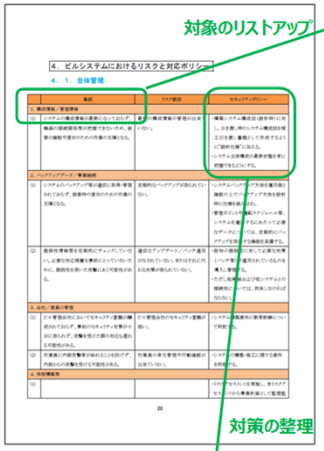
詳細な対応策について、それぞれの解説をさらに本文に記載

実装レベルの対策や実地の経験的対策は、レポジトリとして集積

具体的な対策（ポリシーレベル）の記載

第4章ビルシステムにおけるリスクと対応ポリシー

- 場所や機器毎の脅威／リスク要因を整理し、その対策についてのポリシーを整理



4.1 全体管理		
1.	構成情報／管理情報	
2.	バックアップデータ／事業継続	
3.	会社／要員の管理	
4.	体制 構築等	
4.2 機器		
1.	ネットワーク（クラウド、情報系NW、BACnet）	
	10	ネットワーク
	11	クラウドサーバ・Webサーバ
	12	情報系端末
	13	外部接続用ネットワーク機器（FW、ルータ）
	14	BAシステム間相互接続（BACnet等）
2.	監視センター（中央制御室）	
	20	監視センター
	21	HMI/HIM
	22	保守用持ち込み端末
	23	統合NWにつながるネットワーク機器（FW、ルータ、SW）
	24	システム管理用サーバ（BA主装置）
3.	機械室／制御盤ボックス	
	30	機械室
	31	コントローラ（DCM、PLC等）
	32	ネットワーク機器（FW、ルータ、SW）
	33	ゲートウェイ機器
	34	各種制御盤・分電盤
4.	配線経路（MDF室、EPS、天井裏ラック）	
	40	MDF室／EPS／天井裏ラック
	41	内部に置かれたネットワーク機器（SW等）
5.	末端装置が置かれる場所	
	51	フィールド機器類（センサー、アクチュエータ等）
	52	IPネットワークに直結する機器類（IPカメラ）

場所によらない全体的事項をリストアップ

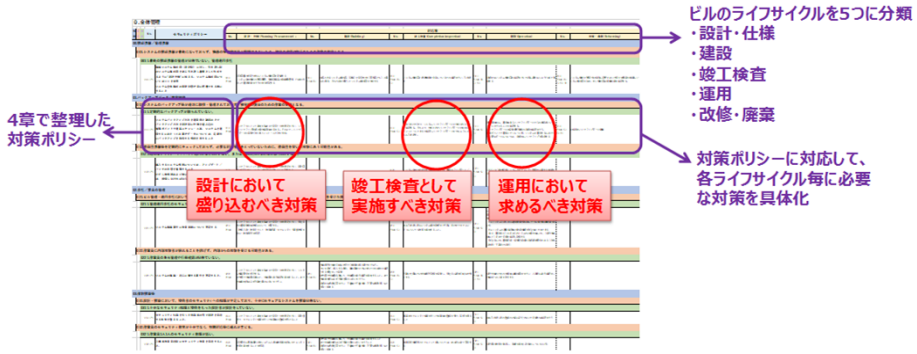
場所及び場所に係わる機器をリストアップ

それぞれの場所、機器毎の脅威やリスクへの対策をポリシーレベルで記載
（例：システムの構成情報を常に最新状態で把握できるようにする。）← 満たすべき要件を記載、具体的方法論までは書かない

具体的な対策（ライフサイクル別）の記載

5章ライフサイクルを考慮したセキュリティ対応策【別紙・非公開】

- 対象毎の脅威・リスク・対策ポリシーに対応して、ライフサイクルを意識した具体的対策を列挙



- 5章は対策ポリシーよりも詳細な具体的対策を別表の形で整理（**現時点では非公開**）
- 別表は具体的対策のインデックスとして使えるものとし、その解説やさらにブレークダウンした実装レベルの対策を6章に掲載（**こちらも非公開**）
- また実際の個別対策例などを付録のレポジトリに収容し、他の参考と出来るように整理

それぞれの利用イメージ

想定する主な用途

- 4章まで
  - ✓ 場所や機器毎の脅威／リスク要因を整理し、その対策についてのポリシーを整理
    - ⇨ ポリシーレベルでの記述なので、ビルのアセスメント評価のチェック表としての利用を想定
- 5章別紙（非公開部分）、付録E経験のリポジトリ
  - ✓ 対象毎の脅威・リスク・対策ポリシーに対応して、ライフサイクルを意識した具体的対策を列挙
  - ✓ 実際の個別対策例などを収容し、他の参考と出来るように整理
    - ⇨ 各ライフサイクル毎の調達仕様への参考情報（一部は直接転記利用）としての利用を想定（設計への要求仕様、システムの調達仕様、運用委託の調達仕様等）
    - ⇨ 調達仕様に関する具体的な条件指定の情報としての利用を想定

多くのビル関係者によるトライアル利用を期待
課題、要改善点等のフィードバックをもとに修正を行い正式版へ

電力SWG（座長：渡辺 研司 名古屋工業大学大学院 教授）

- 電力分野のサイバーセキュリティを取り巻く現状、諸外国の状況を分析し、**官民が取り組むべき課題と方向性**について、**短期・中長期という時間軸を加味**しつつ、広く検討。
- **サイバー・フィジカル・セキュリティ対策フレームワークを踏まえ、電力分野におけるセキュリティ向上を目指す。**

＜構成員＞

有識者（大学教授、弁護士等）、電力事業者、業界団体

＜検討項目＞

- 電力制御系システムに関するセキュリティ向上策
  → **「電力制御システムセキュリティガイドライン」への提言**（サプライチェーンのリスクマネジメントや緊急時対応の強化）
  →2020年**東京オリパラへの対応を視野に、短期的に対応すべき事項と、より中長期で見て対応すべき事項を整理**して検討

- 電力自由化等に伴う多種多様なプレイヤー参入による、制御系システム周辺に拡がりつつあるサイバーセキュリティリスクへの対応策
  →**制御系システムに関連した分野・事業者におけるセキュリティ向上**のあり方を検討

- 業界全体の取組向上に資する基盤整備
  → **情報共有の更なる強化、諸外国との連携強化、人材育成基盤の強化** 等

電力SWG（座長：渡辺 研司 名古屋工業大学大学院 教授）

- 電力ＳＷＧでは、第2回（9/4開催）までは2020年東京オリンピック・パラリンピックへの対応を視野に**短期的に対応すべき事項として、電力制御システムに関するセキュリティ向上策について議論を行い、提言を取りまとめた**ところ。
- 第3回（11/21開催）以降は、**より中長期的視点から対応すべき事項として、電力分野における新たなサイバーリスクや海外連携等について議論を行う。**

＜電力制御システムのセキュリティ向上策に関する提言（第2回まで）＞

- サイバーインシデントに対応する体制の強化
  →**危機管理体制とサイバーインシデント対応体制の連携強化**、**ＩＴ部門とＯＴ部門の密な連携**
- 人材の育成・確保
  → **「戦略マネジメント層」の育成**、**セキュリティ人材の確保**
- 事象発生時の対応強化
  → 地域や警察・セキュリティ専門機関等、**社外との連携の強化**、演習の実施による**危機管理体制の実効性向上**

電気設備の技術基準の解釈にも引用されている**電力制御システムセキュリティガイドラインの見直しを含め**、効果的かつ実効性のある方法を検討・導入

＜第3回以降＞

- 電力制御システムのリスクアセスメント、中期課題の洗い出し（ex.サプライチェーンリスク対策）
- 新規プレイヤーに求められる事項
- これらを踏まえた政策のあるべき姿

防衛産業SWG（防衛装備庁 情報セキュリティ官民検討会）

● 我が国の防衛調達におけるセキュリティ強化の方策について検討

我が国の防衛調達における情報セキュリティ強化の方策について、防衛装備庁と主要な防衛関連企業（２３社４団体）との間で「**防衛調達における情報セキュリティ強化に関する官民検討会**」を開催

＜検討の背景＞

1. **我が国におけるサイバー攻撃の増大**：高度化するサイバー攻撃により、我が国のサプライチェーンが標的となる可能性。
2. **米国の情報セキュリティ強化の動き**：米国の新標準（NIST SP800-171）を満たすことが、今後の米国をはじめとする国際共同研究・開発への参加を継続する最低条件となる可能性。

＜対応方針＞

契約企業が保護すべき情報を取り扱う際に適用される情報セキュリティ基準を、**米国の新標準と同程度まで強化した新情報セキュリティ基準を策定**する。

＜開催の状況＞

	開催日	検討テーマ
第１回	平成２９年　２月２８日	米国の防衛調達における情報セキュリティ強化の動向
		我が国の防衛調達における情報セキュリティ強化の方向
第２回	平成２９年　４月　５日	情報セキュリティ強化のためのルールのあり方
第３回	平成２９年　５月１９日	
第４回	平成２９年　６月１５日	中間的論点整理
第５回	平成２９年１１月２８日	これまでの振り返り及び現在の検討状況
第６回	平成３０年　３月２９日	新基準適合に向けた取り組み
第７回	平成３０年　９月　５日	防衛調達におけるサイバーセキュリティの強化に向けて

第６回検討会より、経済産業省産業サイバーセキュリティ研究会と連携を図るため「**産業サイバーセキュリティ研究会WG1防衛産業SWG** 」として実施。

＜作業部会の設置＞

第７回検討会以降10/15より、情報セキュリティ官民検討会における検討を促進していくための枠組みとして、作業部会を設置
→11/22までに計４回の作業部会を実施し、情報セキュリティ基準改正の考え方に関する、**技術的・専門的観点からの認識を共有**

スマートホームSWG（座長：小松崎 常夫 セコム株式会社 顧問）

- JEITAでは、Society5.0の実現を目指し、スマートホームのセキュリティ対策の検討を実施。
- ハウスメーカ、システム・インテグレータ、機器メーカ等の住まいに関わる企業、業界団体も参加。
- 安心・安全なスマートホーム構築を目指し、セキュリティ対策に加え、スマートライフの在り方、システム連携の製品安全対策やデータ連携の仕組み等の課題において、経済産業政策に協力。

＜構成員＞

企業）家電・AV関連、IT・通信関連、車載関連、住宅設備・サービス関連
団体・機関）住宅・住宅設備分野、電機・通信分野、医療分野、研究機関
スマートホーム部会長の丹 康雄教授（北陸先端大）も委員として参画

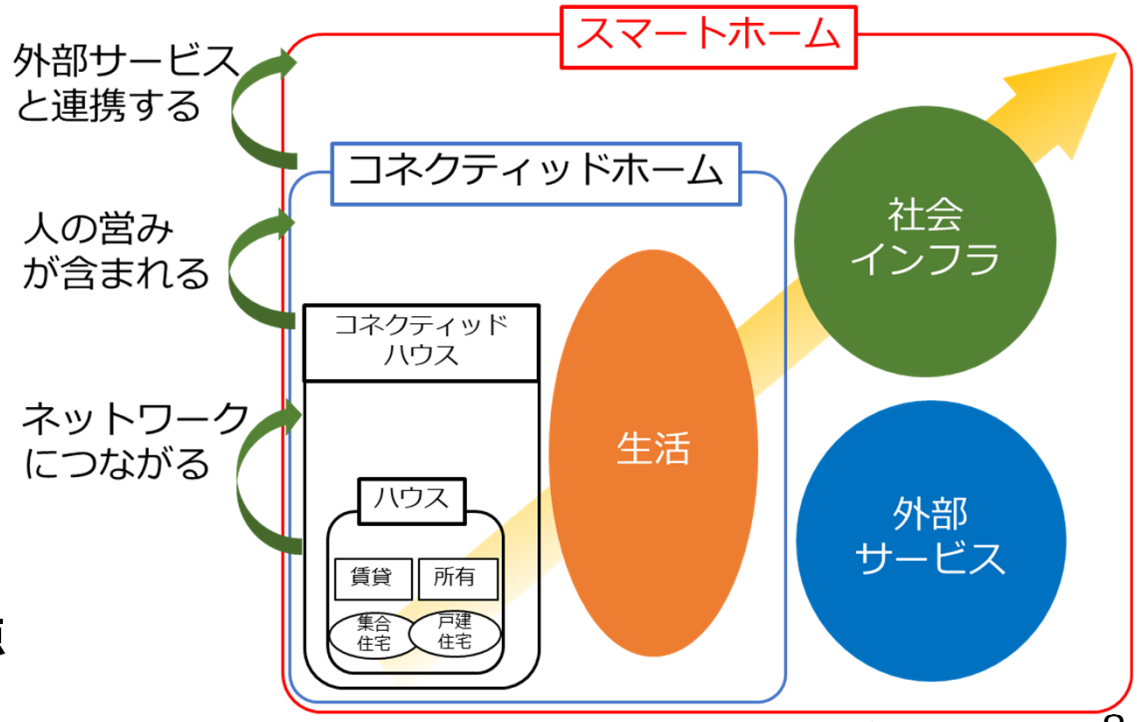
＜進捗＞

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**の策定に協力。

2．**スマートホームのあるべき姿**の共有と、機器やネットワーク接続に留まらない、人の生活や社会インフラとの連携を見据えた**スマートホームの捉え方**を整理。

3．**「家」の在り方は、非常に多岐にわたるもの**であり、その実態を把握・理解するために、住宅関連業界、住宅設備業界・サービス事業者等にヒアリングを実施。

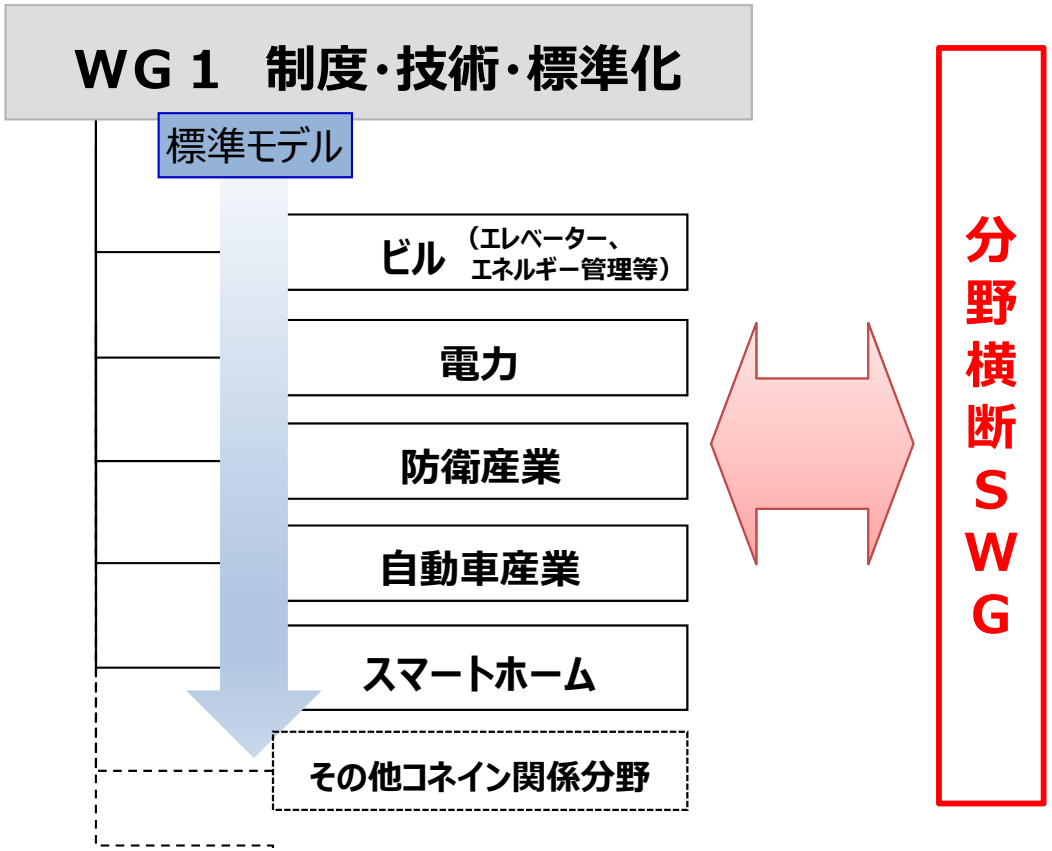
4．**社会インフラや外部サービスとの連携を見据えた視点**でセキュリティ要件を検討。



＜JEITAが目指すスマートホームビジョン＞

分野横断SWGの設置（座長：佐々木 良一 東京電機大学特命教授）

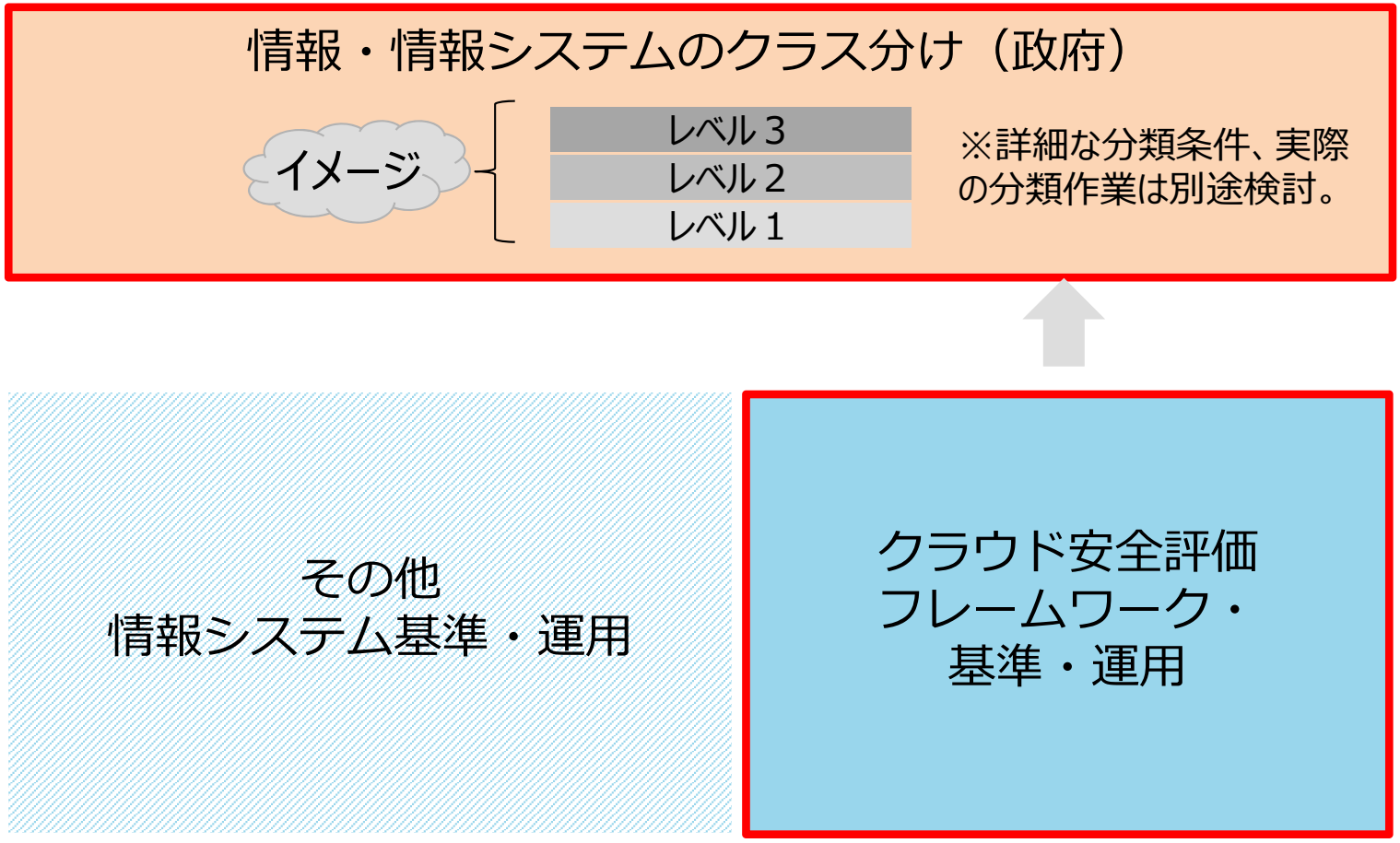
- 産業分野別の課題や対策等を相互に持ち寄り、**分野を横断して共通するセキュリティ課題の洗い出しやその対策について検討するSWGを設置**。検討の結果は、適宜、産業分野別SWGにフィードバック。
- 当面は、産業分野別SWGの検討状況も踏まえ、現在の『サイバー・フィジカル・セキュリティ対策フレームワーク』の見直しを中心とした検討を実施。



1. **分野を横断して共通するセキュリティ課題の検討**
   - 産業分野別SWGの検討状況に応じて、検討課題を選定する
   - 検討結果は産業分野別SWGにフィードバック
2. **現在の『サイバー・フィジカル・セキュリティ対策フレームワーク』の見直し**
   - 国内外からのパブリックコメントの意見を踏まえた修正について検討

（参考）クラウドサービスに係る世界の潮流（海外政府調達について）

- 2018年8月から、NISC、IT室の協力の下で、**経済産業省と総務省が共同で「クラウドサービスの安全性評価に関する検討会」を開催。**（座長：大木 榮二郎工学院大学名誉教授）
- **①基準活用の前提となる情報・情報システムのクラス分けに関する議論**と、**②クラウド調達の基準等に関する議論**を実施中。



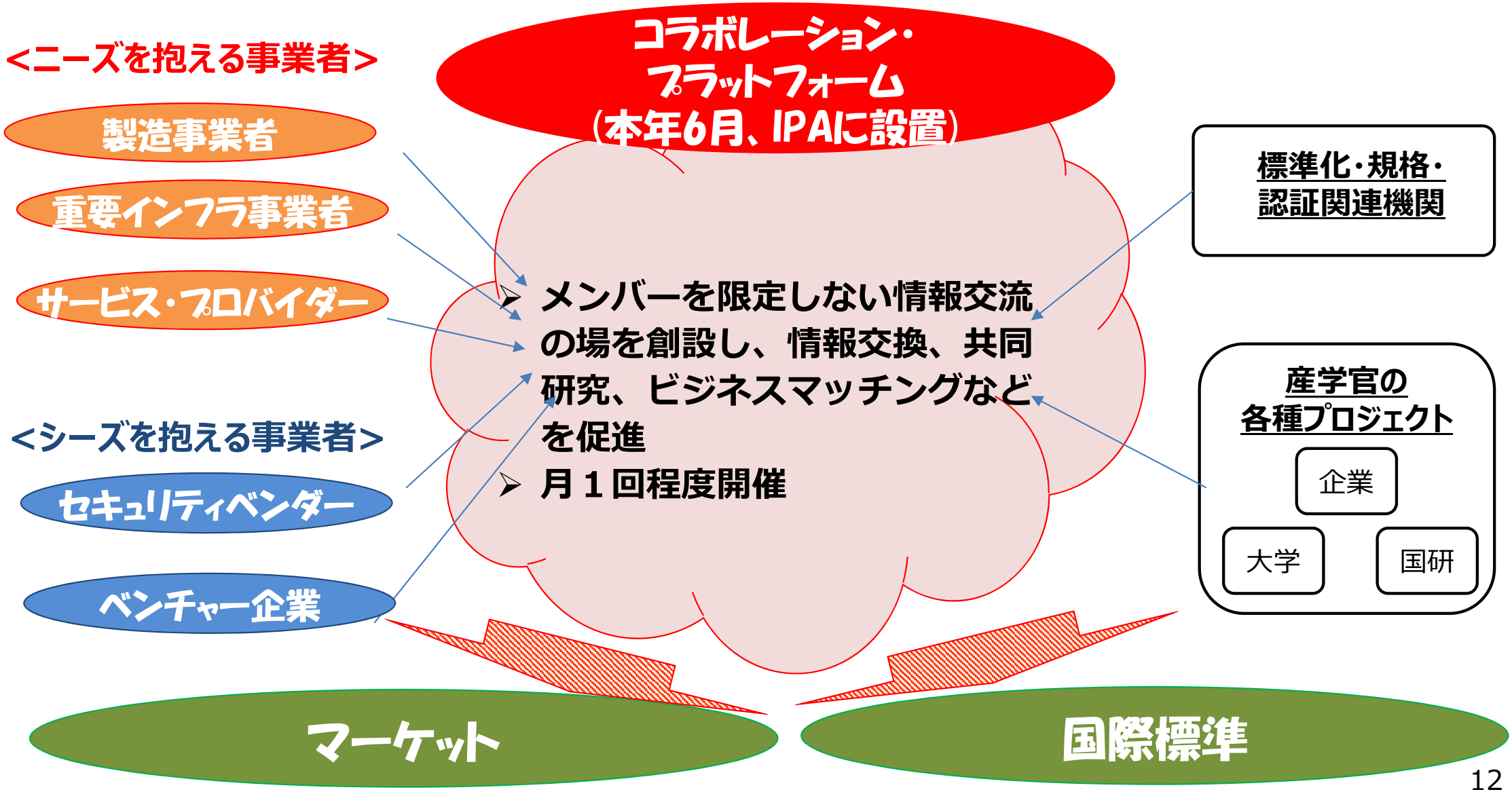
（参考）クラウドサービスに係る世界の潮流（海外政府調達について）

- 海外の政府調達では、多くが①クラウドファーストを掲げ、②その直後にクラウドサービスの政府調達に係る認証制度を導入。
- 日本では、2018年6月にクラウド・バイ・デフォルト原則を採用したところ、安全性評価の仕組みの検討が必要。

	クラウド利用の方針	政府のクラウド評価制度	主な関連機関
	**2010年** 「25 POINT IMPLEMENTATION PLAN TO REFORM FEDERAL INFORMATION TECHNOLOGY MANAGEMENT」 →**クラウドファースト**(cloud first)	**2011年～** Federal Risk and Authorization Management Program FedRAMP	General Services Administration （※独立政府機関） GSA
	**2011年** 「Government Cloud Strategy」 →**クラウドファースト**(a public cloud solution first policy)	**2013年～** G-Cloud framework	Government Digital Services （※内閣府管轄） GDS
	**2014年** 「Australian Government Cloud Computing Policy」 →**クラウドファースト**(cloud first)	**2014年～** Information Security Registered Assessors Program irap	Australian Signals Directorate （※防衛大臣管轄） DEFENCE SIGNALS DIRECTORATE AUSTRALIA
	**2011年** 「e-Government masterplan 2011-2015」 →**政府プライベートラウドの構築、移行（G-Cloud）**	**2013年～** Multi-Tier Cloud Security（MTCS:SS584）	Infocomm Media Development Authority （※情報通信省管轄） IMDA
	**2018年** 「政府情報システムにおけるクラウドサービスの利用に係る基本方針」 →**クラウド・バイ・デフォルト**	整備中	整備中

官民の対話の場としてのコラボレーション・プラットフォームの開催

- 各WGの活動などを通じて顕在化したニーズとシーズをマッチングする“場”となる『**コラボレーション・プラットフォーム**』を**IPAに設置し、6月から活動を開始。**



（参考）コラボレーション・プラットフォームの開催状況

- 各回、予定定員以上の申込みがあり、参加者からは政府との意見交換、最新動向の情報収集、人脈形成等、様々な視点で有益との声。

	日にち	参加人数(*)	主なテーマ
第一回	6月13日	179名（99名）	経済産業省の政策動向、パネルディスカッション（サイバーセキュリティビジネス、サプライチェーンセキュリティ）
第二回	7月23日	104名（74名）	IoTの発展に潜むリスクと対策、グループディスカッション（サプライチェーン、人材、つながる世界の脅威と対策）
第三回	9月3日	132名（69名）	経済産業省の新政策、ビル分野のサイバーセキュリティ対策、企業の取り組み事例、グループディスカッション（業界別セキュリィ対策、セキュリティ検証基盤、サイバーセキュリティ経営）
第四回	10月16日	151名（56名）	中小企業におけるサイバーセキュリティリスク、ウイルス感染デモ、中小企業向けサイバーセキュリティ対策、企業の取り組み事例
第五回	11月30日	98名（40名）	IoTの技術・標準化動向、スマートホームのサイバーセキュリティ対策、グループディスカッション（標準化、IoT導入における課題と対策）

(*)括弧内の人数はコラボレーション・プラットフォーム後に開催した情報交換会の出席者数


富田理事長(IPA)ご挨拶

三角審議官(経済産業省)ご挨拶


パネルディスカッション(第一回)


グループディスカッション(第二回)