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31年3月27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, 2/25 第8回会合**
- **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, 2/22第4回会合開催**
- **防衛産業**
  **3/29 第1回会合, 9/5 第2回会合,
  2/28 第3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**
  設置準備中
- **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, 2/20 第8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・制御を行うビル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	江崎浩東京大学大学院教授、松浦知史東京工業大学准教授、制御システムセキュリティセンター
ビルオーナー	日本生命、三井不動産、三菱地所、森ビル（イーヒルズ）、横浜市、日本ビルヂング協会連合会、不動産協会
ゼネコン、サブコン、設計事務所	鹿島建設、竹中工務店、きんでん、九電工、日建設計
個別システム事業者	アズビル、セコム、ダイキン工業、NTT、日立製作所、三菱電機、ビルディング・オートメーション協会

＜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
- 多くの事業者の取組の参考となるように、サイバーセキュリティ対策として**複数の選択肢を提供**
- 記載内容の概要
  - ビルシステムに係わるサイバーセキュリティ上の脅威増大の現状
  - ビルシステムに対して起こりえる攻撃と想定される影響
  - ガイドラインの位置づけや利用法の説明
  - ビルシステムのリスクとサイバーセキュリティ確保のための対策概要
  - ビルのライフサイクルの各段階に合わせた対策の具体的内容
- 具体事例等の知見は関係者のみ共有のレポジトリとして整理

ビルのライフサイクル	主な要求概要	関係する主なステークホルダー
設計・仕様	機器、ネットワーク、物理セキュリティへの要求	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
建設	施工プロセスや管理体制への要求	ゼネコン、サブコン、個別システム事業者
竣工検査	仕様を満たすことを確認する受入検査への要求	オーナー、ゼネコン、サブコン、個別システム事業者
運用	運用プロセスやチェック体制、管理体制への要求	オーナー、運用事業者、個別システム事業者
改修・廃棄	機器、ネットワーク、物理セキュリティ、管理体制等への見直しポイントの要求	オーナー、設計事務所、運用事業者、個別システム事業者

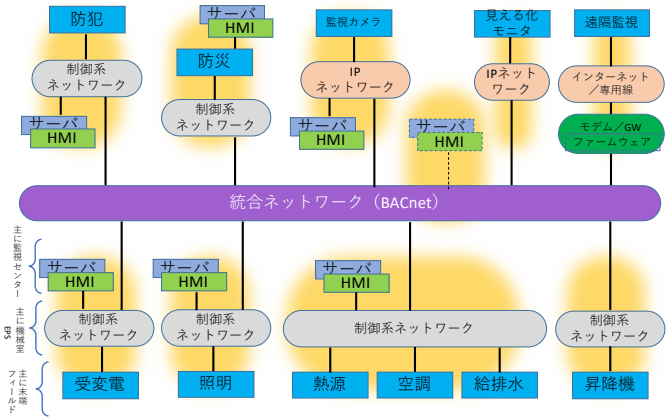
＜検討スケジュール＞

- 2018年9月：ガイドライン（β版）を公開
- **2019年3月：ガイドライン第1版（案）についてパブコメを実施中（3/11~4/9）**
- 2019年度以降：パブコメを踏まえてガイドライン第1版（共通編）を公開・本格活用開始、さらに個別編の作成を目指す

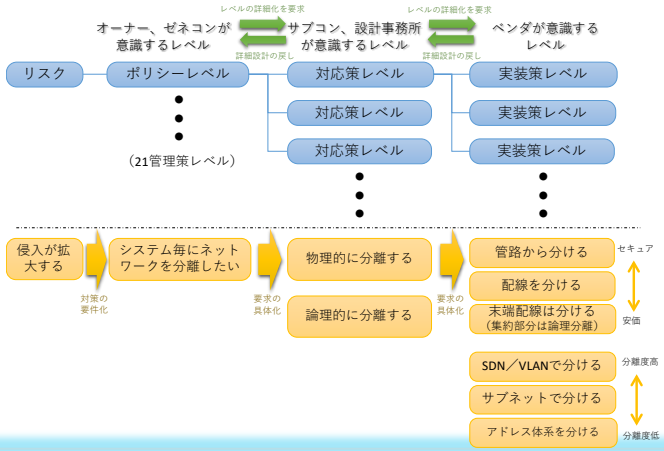
ビルSWG：ビルガイドラインの作成方針概要

- 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物理、システム、管理上のリスクを抽出。
- 各リスクへの必要な対策をまずポリシーレベルで整理、更にライフサイクルを意識した対策を整理。

1．検討の前提として標準的なモデル構成を整理

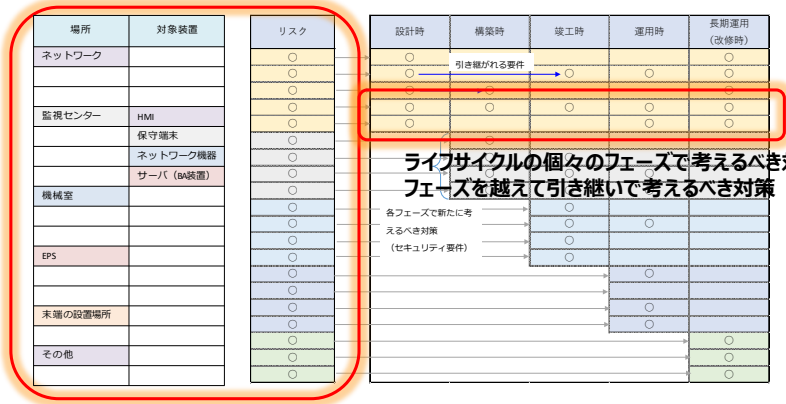


2．対策の階層構造とステークホルダの関係を整理



3．ビルのライフサイクルを意識した対策へと展開

場所や機器に応じたリスク、対策のポリシー



4．具体的な対策記述をポリシーレベルで列挙

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、乗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、乗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緩和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）の権限を越えて、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。	

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記述を具体化
- 個別事例をレポジトリとして整理

ビルガイドラインの構成と記載内容①

ガイドライン第1版(案)の構成

目次

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第1版案（パブコメ版）の策定にあたって

1．はじめに
- 1．1．ガイドラインを策定する目的
- 1．2．ガイドラインの適用範囲と位置づけ
- 1．3．本ガイドラインの構成

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
- 2．3．ビルシステムにおけるサイバー攻撃の影響

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
- 3．1．一般的なサイバーセキュリティ対策のスキーム
- 3．2．ビルシステムの構成の整理
- 3．3．ビルシステムの特徴
- 3．4．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
- 3．5．ガイドラインの想定する使い方例

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

付録A　用語集
付録B　JDCCの建物設備システムリファレンスガイドとの関係
付録C　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考え方とビルシステムにおけるユースケース
付録D　参考文献

本文には**対策のポリシーまで**を記載

詳細な対応策は、設計・仕様～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**

場所によらない全体的事項をリストアップ

対象を場所の概念で抽出・列挙

場所及びその場所に設置される機器をリストアップ

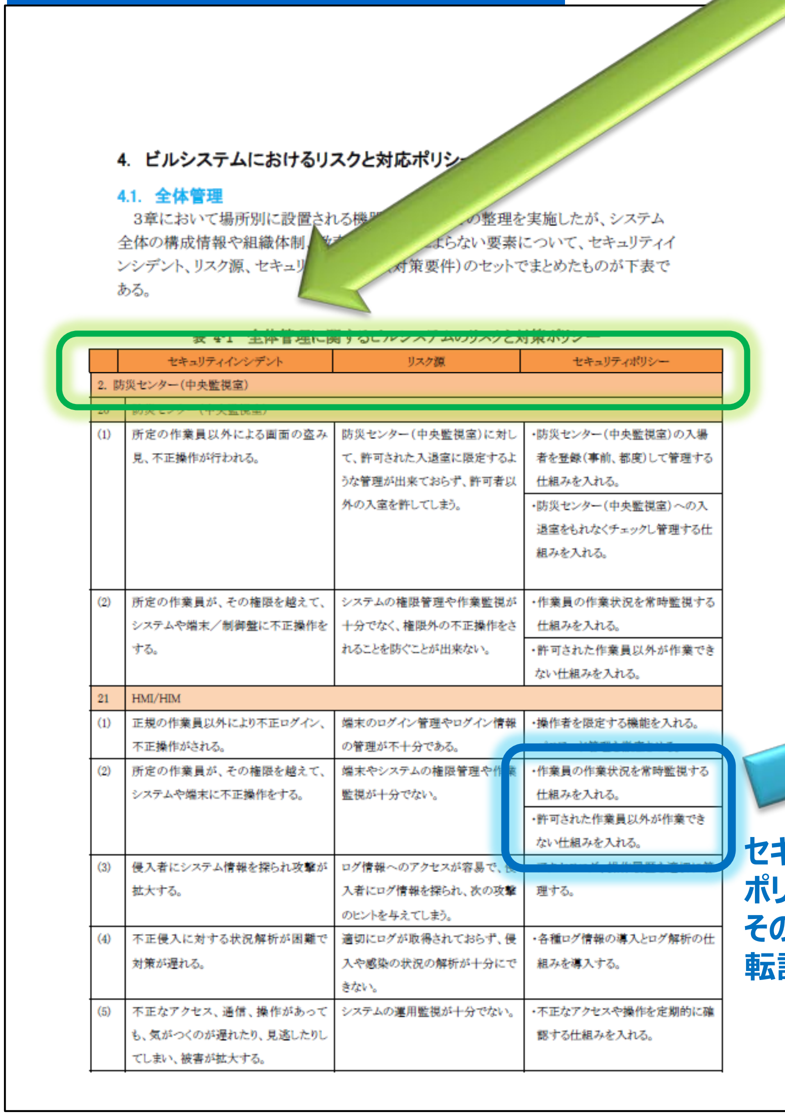
セキュリティ対策の対象として場所及び設置される機器を列挙

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	ビルシステム間相互接続
2.	防災センター（中央監視室）	
	20	防災センター（中央監視室）
	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（ビルシステム主装置）
3.	機械室／制御盤ボックス	
	30	機械室
	31	コントローラ（DDC、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類）
5.	末端装置が置かれる場所	
	50	末端装置

（次スライドへ）

ビルガイドラインの構成と記載内容②

具体的な対策（ポリシーレベル）の記載



4. ビルシステムにおけるリスクと対応ポリシ[illegible]

4.1. 全体管理

3章において場所別に設置される機[illegible]の整理を実施したが、システム全体の構成情報や組織体制[illegible]ばならない要素について、セキュリティインシデント、リスク源、セキュリ[illegible]対策要件)のセットでまとめたものが下表である。

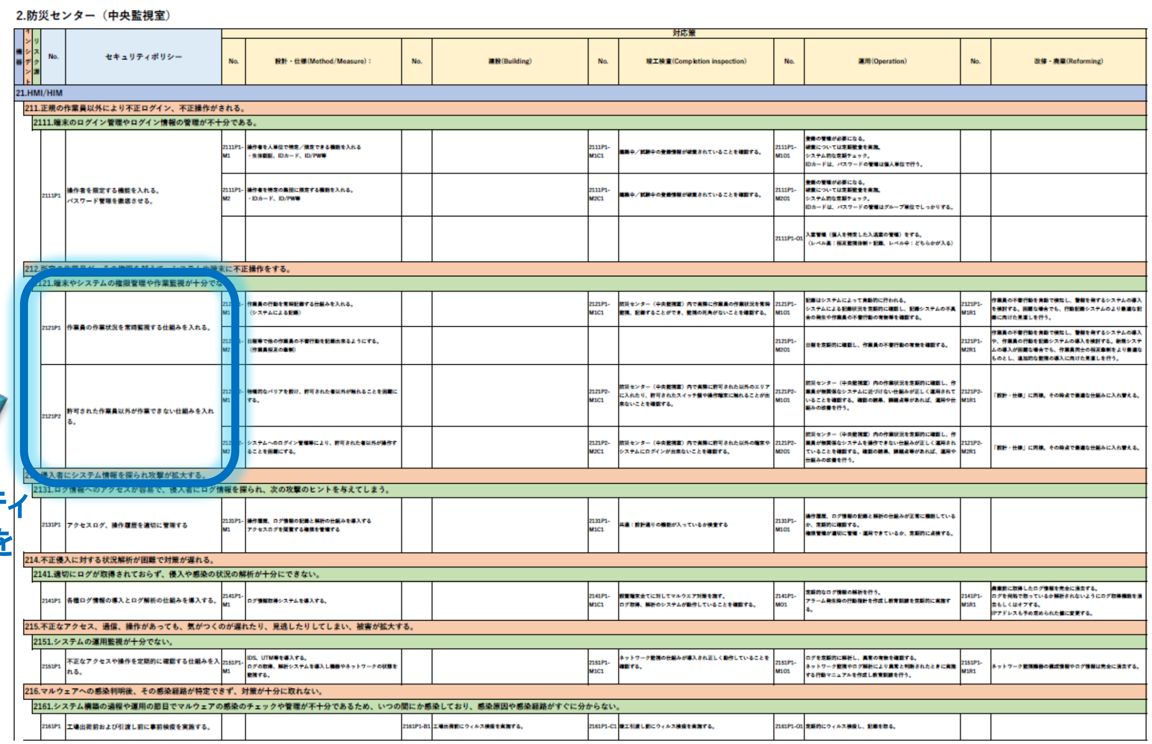
表 4-1 全体管理に関するビルシステムのリスクと対策ポリシー

	セキュリティインシデント	リスク源	セキュリティポリシー
2. 防災センター（中央監視室）			
(1)	所定の作業員以外による画面の盗み見、不正操作が行われる。	防災センター（中央監視室）に対して、許可された入退室に限定するような管理が出来ておらず、許可者以外の入室を許してしまう。	･防災センター（中央監視室）の入場者を登録（事前、都度）して管理する仕組みを入れる。 ･防災センター（中央監視室）への入退室をもれなくチェックし管理する仕組みを入れる。
(2)	所定の作業員が、その権限を超えて、システムや端末／制御盤に不正操作をする。	システムの権限管理や作業監視が十分でなく、権限外の不正操作をされることを防ぐことが出来ない。	･作業員の作業状況を常時監視する仕組みを入れる。 ･許可された作業員以外が作業できない仕組みを入れる。
21	HMI/HIM		
(1)	正規の作業員以外により不正ログイン、不正操作がされる。	端末のログイン管理やログイン情報の管理が不十分である。	･操作者を限定する機能を入れる。
(2)	所定の作業員が、その権限を超えて、システムや端末に不正操作をする。	端末やシステムの権限管理や作業監視が十分でない。	･作業員の作業状況を常時監視する仕組みを入れる。 ･許可された作業員以外が作業できない仕組みを入れる。
(3)	侵入者にシステム情報を探られ攻撃が拡大する。	ログ情報へのアクセスが容易で、侵入者にログ情報を探られ、次の攻撃のヒントを与えてしまう。	[illegible]理する。
(4)	不正侵入に対する状況解析が困難で対策が遅れる。	適切にログが取得されておらず、侵入や感染の状況の解析が十分にできない。	･各種ログ情報の導入とログ解析の仕組みを導入する。
(5)	不正なアクセス、通信、操作があっても、気がつくのが遅れたり、見逃したりしてしまい、被害が拡大する。	システムの運用監視が十分でない。	･不正なアクセスや操作を定期的に確認する仕組みを入れる。

対象の単位でインシデント、リスク源、対策ポリシーを整理

セキュリティポリシーをそのまま転記

具体的な対策（ライフサイクル別）の記載



2.防災センター（中央監視室）

No.	セキュリティポリシー	対応策: No.	設計・仕様(Method/Measure)	No.	建設(Building)	No.	竣工検査(Completion inspection)	No.	運用(Operation)	No.	改修・廃棄(Reforming)

21.HMI/HIM

211.正規の作業員以外により不正ログイン、不正操作がされる。

2111.端末のログイン管理やログイン情報の管理が不十分である。

2111P1 操作者を限定する機能を入れる。パスワード管理を徹底させる。

212.[illegible]不正操作をする。

2121.端末やシステムの権限管理や作業監視が十分で[illegible]

2121P1 作業員の作業状況を常時監視する仕組みを入れる。

2121P2 許可された作業員以外が作業できない仕組みを入れる。

213.侵入者にシステム情報を探られ攻撃が拡大する。

2131.ログ情報へのアクセスが容易で、侵入者にログ情報を探られ、次の攻撃のヒントを与えてしまう。

2131P1 アクセスログ、操作履歴を適切に管理する

214.不正侵入に対する状況解析が困難で対策が遅れる。

2141.適切にログが取得されておらず、侵入や感染の状況の解析が十分にできない。

2141P1 各種ログ情報の導入とログ解析の仕組みを導入する。

215.不正なアクセス、通信、操作があっても、気がつくのが遅れたり、見逃したりしてしまい、被害が拡大する。

2151.システムの運用監視が十分でない。

2151P1 不正なアクセスや操作を定期的に確認する仕組みを入れる。

216.マルウェアへの感染判明後、その感染経路が特定できず、対策が十分に取れない。

2161.システム機器の過程や運用の節目でマルウェアの感染のチェックや管理が不十分であるため、いつの間にか感染しており、感染原因や感染経路がすぐに分からない。

2161P1 工場出荷前および引渡し前に事前検査を実施する。

ビルガイドラインの構成と記載内容③

具体的な対策（ライフサイクル別）の記載

設計において盛り込むべき対策 / **建設時に盛り込むべき対策** / **竣工検査で盛り込むべき対策** / **運用時に盛り込むべき対策** / **改修・廃棄の際に盛り込むべき対策**

2.防災センター（中央監視室）

機器	インシデント	リスク源	No.	セキュリティポリシー	No.	設計・仕様(Method/Measure)：	No.	建設(Building)	No.	竣工検査(Completion inspection)	No.	運用(Operation)	No.	改修・廃棄(Reforming)
21.HMI/HIM														
211.正規の作業員以外により不正ログイン、不正操作がされる。														
2111.端末のログイン管理やログイン情報の管理が不十分である。														
			2111P1	操作者を限定する機能を入れる。 パスワード管理を徹底させる。					2111P1-M1C1	竣工検査／試験中の登録情報が確実されていることを確認する。	2111P1-M1O1	登録の管理が必要になる。 確実については定期監査を実施。 システム的な定期チェック。 IDカードは、パスワードの管理は個人単位で行う。		
									2111P1-M2C1	竣工検査／試験中の登録情報が確実されていることを確認する。	2111P1-M2O1	登録の管理が必要になる。 確実については定期監査を実施。 システム的な定期チェック。 IDカードは、パスワードの管理はグループ単位でしっかりする。		
											2111P1-O1	入室管理（個人を特定した入退室の管理）をする。 （レベル高：指紋認識体制＋記載、レベル中：どちらかが入る）		
212.所定の作業員が、その権限を越えて、システムや端末に不正操作をする。														
2121.端末やシステムの権限管理や作業監視が十分でない。														
			2121P1	作業員の作業状況を常時監視する仕組みを入れる。	2121P1-M1	作業員の行動を常時記録する仕組みを入れる。 （システムによる記録）			2121P1-M1C1	防災センター（中央監視室）内で実際に作業員の作業状況を常時監視、記録することができ、監視の死角がないことを確認する。	2121P1-M1O1	記録はシステムによって自動的に行われる。 システムによる記録状況を定期的に確認し、記録システムの不具合の発生や作業員の不審行動の有無等を確認する。	2121P1-M1R1	作業員の不審行動を自動で検知し、警報を発するシステムの導入を検討する。困難な場合でも、行動記録システムのより普遍な記録に向けた見直しを行う。
					2121P1-M2	目視等で他の作業員の不審行動を記録出来るようにする。 （作業員相互の連絡）					2121P1-M2O1	目視を定期的に確認し、作業員の不審行動の有無を確認する。	2121P1-M2R1	作業員の不審行動を自動で検知し、警報を発するシステムの導入や、作業員の行動を記録システムの導入を検討する。記録システムの導入が困難な場合でも、作業員同士の相互連絡をより普遍なものとし、追加的な記録の導入に向けた見直しを行う。
			2121P2	許可された作業員以外が作業できない仕組みを入れる。	2121P2-M1	物理的なバリアを設け、許可された者以外が触れることを困難にする。			2121P2-M1C1	防災センター（中央監視室）内で実際に許可された以外のエリアに入れたり、許可されたスイッチ盤や操作端末に触れることが出来ないことを確認する。	2121P2-M1O1	防災センター（中央監視室）内の作業状況を定期的に確認し、作業員が物質等なシステムに近づけない仕組みが正しく運用されていることを確認する。確認の結果、課題点等があれば、運用や仕組みの改善を行う。	2121P2-M1R1	「設計・仕様」に同様。その時点で最適な仕組みに入れ替える。
					2121P2-M2	システムへのログイン管理等により、許可された者以外が操作することを困難にする。			2121P2-M2C1	防災センター（中央監視室）内で実際に許可された以外の端末やシステムにログインが出来ないことを確認する。	2121P2-M2O1	業員が物質等なシステムを操作できない仕組みが正しく運用されていることを確認する。確認の結果、課題点等があれば、運用や仕組みの改善を行う。	2121P2-M2R1	「設計・仕様」に同様。その時点で最適な仕組みに入れ替える。
213.侵入者にシステム情報を探られ攻撃が拡大する。														
2131.ログ情報へのアクセスが容易で、侵入者にログ情報を探られ、次の攻撃のヒントを与えてしまう。														
			2131P1	アクセスログ、操作履歴を適切に管理する	2131P1-M1	操作履歴、ログ情報の記録と解析の仕組みを導入する アクセスログを閲覧する権限を管理する								
214.不正侵入に対する状況解析が困難で対策が遅れる。														
2141.適切にログが取得されておらず、侵入や感染の状況の解析が十分にできない。														
			2141P1	各種ログ情報の導入とログ解析の仕組みを導入する。	2141P1-M1	ログ情報取得システムを導入する。			2141P1-M1C1	脆弱性完全てに対してマルウェア対策を施す。 ログ取得、解析のシステムが動作していることを確認する。	2141P1-M01	定期的なログ情報の解析を行う。 アラーム発生時の行動指針を作成し教育訓練を定期的に実施する。	2141P1-M1R1	廃棄前に取得したログ情報を完全に消去する。 ログを何時で取っているか解析されないようにログ取得機能を消去もしくはオフする。 IPアドレスも予め定められた値に変更する。
215.不正なアクセス、通信、操作があっても、気がつくのが遅れたり、見逃したりしてしまい、被害が拡大する。														
2151.システムの運用監視が十分でない。														
			2151P1	不正なアクセスや操作を定期的に確認する仕組みを入れる。	2151P1-M1	IDS、UTM等を導入する。 ログの取得、解析システムを導入し機器やネットワークの状態を監視する。			2151P1-M1C1	ネットワーク監視の仕組みが導入され正しく動作していることを確認する。	2151P1-M1O1	ログを定期的に解析し、異常の有無を確認する。 ネットワーク監視やログ解析により異常と判断されたときに実施する行動マニュアルを作成し教育訓練を行う。	2151P1-M1R1	ネットワーク監視機器の構成情報やログ情報は完全に消去する。
216.マルウェアへの感染判明後、その感染経路が特定できず、対策が十分に取れない。														
2161.システム構築の過程や運用の節目でマルウェアの感染のチェックや管理が不十分であるため、いつの間にか感染しており、感染原因や感染経路がすぐに分からない。														
			2161P1	工場出荷前および引渡し前に事前検疫を実施する。			2161P1-R1	工場出荷前にウィルス検疫を実施する。	2161P1-C1	竣工引渡し前にウィルス検疫を実施する。	2161P1-O1	定期的にウィルス検疫し、記録を取る。		

- 場所／機器
- インシデント
- リスク源
- 対策ポリシー

5つのライフサイクルに分類

対策として複数の選択肢を提示
設計の選択によって、後フェーズで必要な対策が異なる

4章で整理した対策ポリシー

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）、電気事業者、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っている。**

＜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（**危機管理体制等の連携強化、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

＜中長期視点から対応すべき事項の検討（第3回以降）＞

検討すべき事項

- **サプライチェーンリスクへの対応**について
  - ・海外の事業者や国内他分野の動向を踏まえると、日本の電力分野においてはどのようなリスクが存在するか。
  - ・日本の電力分野の関係者が継続的に取り組むべき事項は何か。
- **大手電気事業者**のサイバーセキュリティ対策について
  - ・大手電気事業者のサイバーセキュリティ対策の取組の現状分析と、今後取り組むべき事項は何か。
- **新規プレーヤー**のサイバーセキュリティ対策について
  - ・新規プレーヤー等のサイバーセキュリティ対策の取組の現状分析と、今後取り組むべき事項は何か。

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８回	平成３１年　２月２８日	サイバー攻撃に関する留意事項、米国企業のNIST SP800-171対応状況

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**

JEITA スマートホームサイバーセキュリティWG（主査：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、IT・エレクトロニクス企業のみならず、人々の暮らしに関わる様々なメンバーが、それぞれの知見を結集して、スマートホームのセキュリティ対策の検討を実施。
- 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（戸建て／マンション）・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

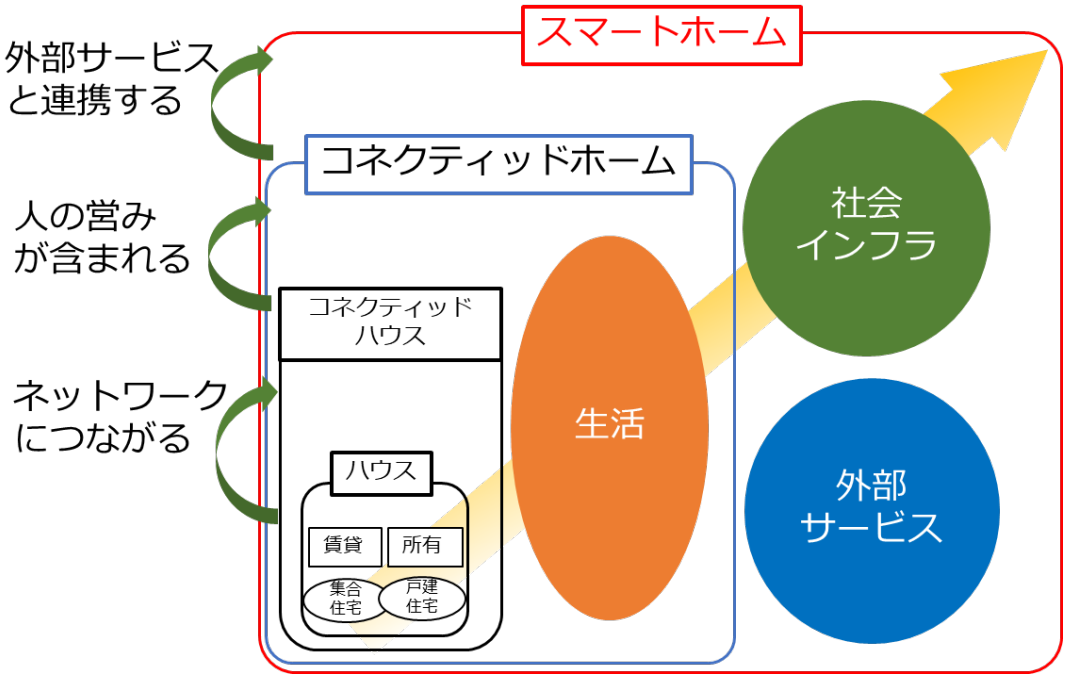
＜進捗＞

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・サービス事業者等の様々な視点から検討。

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の検討を実施中。



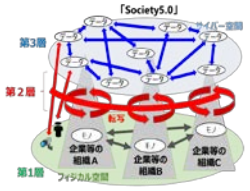
＜JEITAが目指すスマートホームビジョン＞

スマートホーム実現に向けたサイバーフィジカルセキュリティ対策ガイドライン整備に向けた取組み

- スマートホームの実現のためには、多種多様な人間の営み、マネジメント形態、ライフスタイル等が起因したスマートホーム特有の脅威への対策が必要である。
- Society5.0社会の基盤となるスマートホームは、社会インフラや様々な産業、サービスが結節した、住まい手を中心としたサービスチェーンにより構成され、あらゆるステークホルダーが参照可能なガイドラインが求められている。
- JEITAでは、スマートホーム分野のセキュリティガイドラインの整備に加えて、日々のオペレーションレベルでもセキュリティを担保するためのガイドライン運用のあり方についても纏めていく。

経済産業省
Ministry of Economy, Trade and Industry

サイバー・フィジカル・セキュリティ
対策フレームワーク



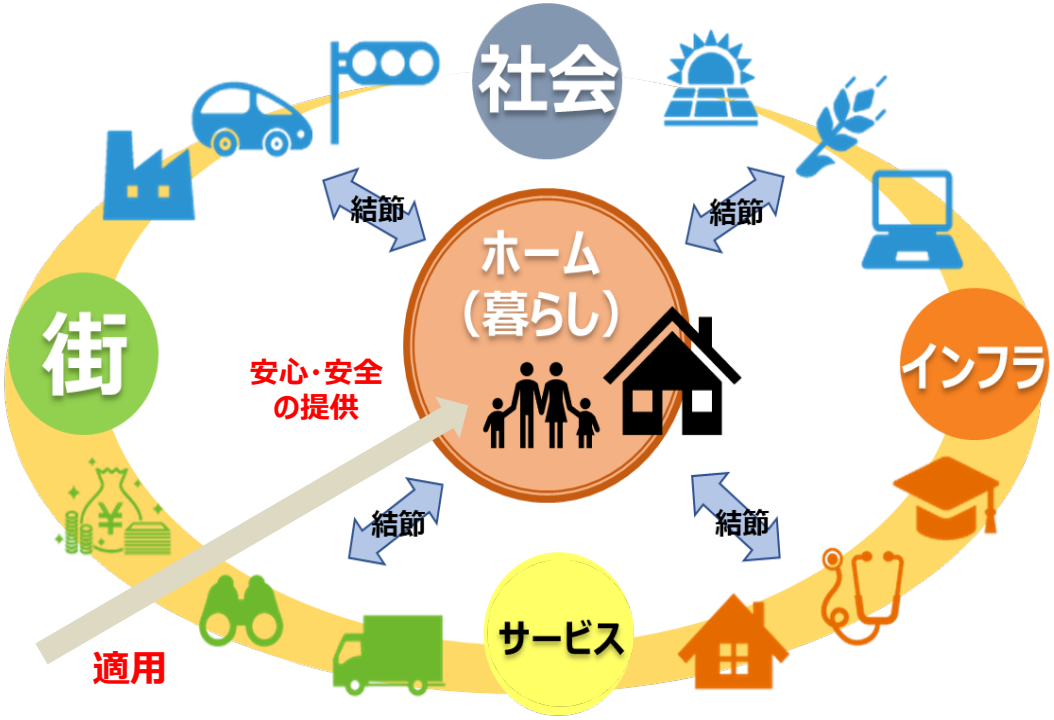
・三層構造での脅威分析

・サプライチェーン全体でのセキュリティ対策

参照

JEITA 一般社団法人 電子情報技術産業協会

スマートホーム実現に向けた
サイバーフィジカルセキュリティ
対策ガイドライン



スマートホーム特有の脅威

① 膨大な攻撃対象 (世帯数はおよそ5300万世帯)
② マネジメント不在に起因する脆弱性
③ 利用者側の誤操作等による想定外のインシデント

（参考）クラウドサービスの安全性評価に関する検討会のスコープ

- 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行う。
- 上記に加えて検討すべき事項については、継続的な検討事項として項目整理を行う。

赤字部分が検討会のスコープ

情報・情報システムのクラス分け（政府）

イメージ

レベル３
レベル２
レベル１

※詳細な分類条件、実際の分類作業は別途検討。

参照（P）

情報・情報システムのクラス分け（産業）

①基準活用の前提となるデータ分類の必要性
分類の際のセキュリティ要求事項の整理、報告

その他
情報システム基準・運用

クラウド基準・運用

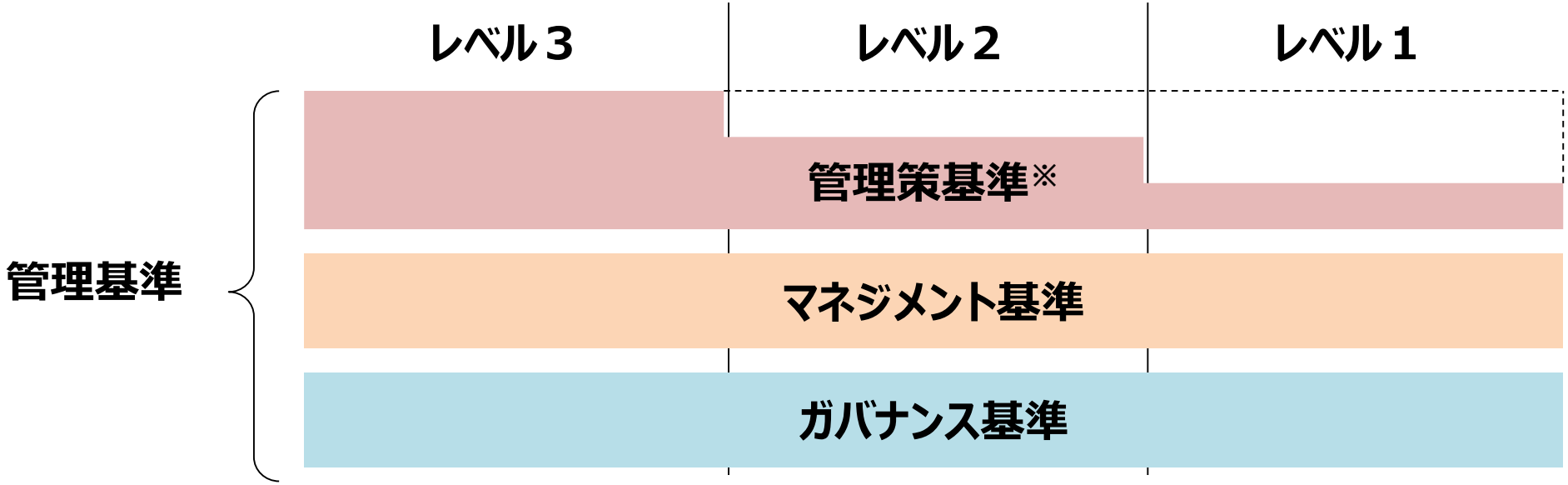
②・既存の基準＋αの安全性評価方法
・評価の実効性
・運用方法
等を整理、策定。

推奨

重要産業分野等

（参考）管理基準項目のイメージ

- ガバナンス基準、マネジメント基準、管理策基準からなる管理基準を策定する。管理策基準を中心に、レベルに応じて項目数・強度・内部監査の活用等に差異を設ける。



※個別のサービス単位で具体的なリスクを低減するために必要な管理策を位置づけたもの。

＜参考となる基準等(例)＞

・JIS Q 27001 (ISO/IEC 27001)　・JIS Q 27002 (ISO/IEC 2700 2)
・JIS Q 27017 (ISO/IEC 27017)　・NIST SP800-53 rev.4
・Australian Government Information Security Manual (ISM)
・サイバーセキュリティ戦略本部　政府機関等の情報セキュリティ対策のための統一基準（平成30年度版）
・日本セキュリティ監査協会　クラウド情報セキュリティ管理基準（平成28年改正版）
（経済産業省　情報セキュリティ管理基準（平成28年度版））
・総務省　クラウドサービス提供における情報セキュリティ対策ガイドライン（第2版）

この他に、データセンターの物理的な基準等も検討する必要がある。

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

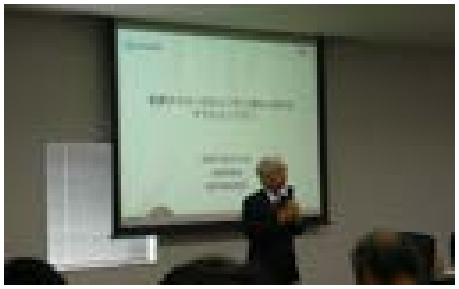
- 各WGの活動などを通じて顕在化したニーズとシーズをマッチングする“場”となる『**コラボレーション・プラットフォーム**』を**IPAに設置し、6月から活動を開始。**

（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
第二回	7月23日	104名（74名）	サプライチェーン対策、人材育成、つながる世界の脅威と対策
第三回	9月3日	132名（69名）	業界別のセキュリティ対策、セキュリティ検証基盤、セキュリティ経営
第四回	10月16日	151名（56名）	中小企業のセキュリティ対策
第五回	11月30日	98名（40名）	IoTの技術・標準化動向
第六回	1月25日	108名（48名）	サイバー・フィジカル・セキュリティ対策フレームワーク
第七回	3月4日	114名（42名）	IoT導入、課題解決に向けた対策技術の紹介
第八回	4月23日	4月上旬募集開始	2019年度の経済産業省の政策紹介

(*)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)

（詳細はIPAのサイトを参照） https://www.ipa.go.jp/security/announce/collapla_index.html