経済産業省

資料３－１

サブワーキンググループ等の設置・検討状況

平成30年8月3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回会合開催
- **電力**
  6/12 第1回会合開催
- **防衛産業**
  3/29 第1回会合開催
  (防衛装備庁 第6回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

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実装の方向性

- 『サイバー・フィジカル・セキュリティ対策フレームワーク』は、**対策の枠組み(チェックポイント)を示したものであり、セキュリティ水準(対策の強度)を示すものではない。**
- 産業分野ごとに守るべきものやリスクに違いも存在するため、**産業分野別にセキュリティ水準の検討を進めていく。**また、分野ごとの検討を進めた上で、**分野横断的課題を相互にフィードバックし、各産業分野に共通する対策を洗い出す等の取組を進めていく。**

『サイバー・フィジカル・セキュリティ対策フレームワーク』と分野別におけるセキュリティ対策のイメージ

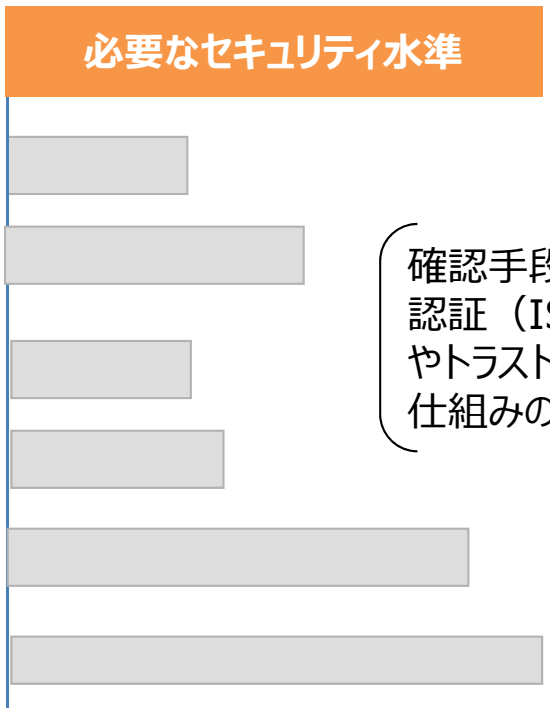
サイバー・フィジカル・セキュリティ対策フレームワーク

三層別アプローチ	必要な対策のポイント
1. 企業間のつながり (主体の信頼)	セキュリティポリシーの策定、体制の整備
	事業継続計画又はコンティンジェンシープランへの反映
	・・
2. フィジカル空間とサイバー空間のつながり (機能の信頼)	セキュリティ対策が施されたIoT機器の導入
	セキュリティバイデザインの実践
	・・
3. サイバー空間におけるつながり (データの信頼)	信頼できるサービスサプライヤーの選定
	サイバー空間における接続相手の認証
	・・

対策のポイントを踏えて産業分野ごとに検討

また、分野ごとの検討を踏まえて、分野横断的課題を相互にフィードバックしながら取り組みを推進

産業分野別セキュリティガイドライン



確認手段として、認証（ISMS、CC等）やトラストリスト等の仕組みの検討

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	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
施工／建築	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	ベンダー、ゼネコン、サブコン、オーナー、設計事務所
運用・保守	管理体制への要求	オーナー、サブコン、ベンダー

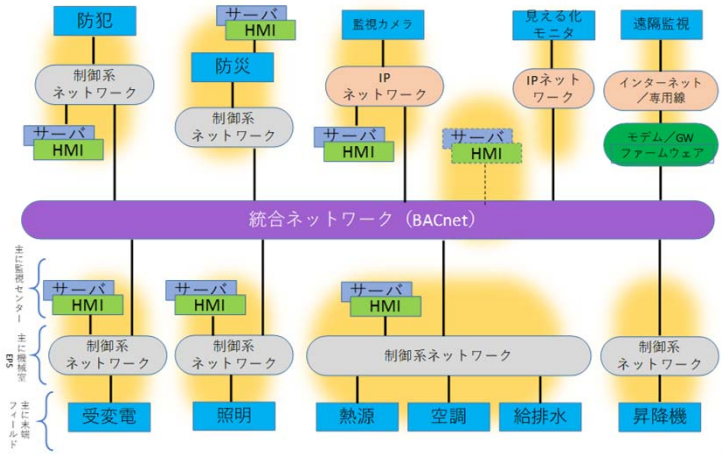
＜検討スケジュールイメージ＞

- **2018年夏：ガイドライン共通編（骨子）を作成**
- 2018年度中：骨子を用いたモデル評価（2サンプル程度）とフィードバック、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

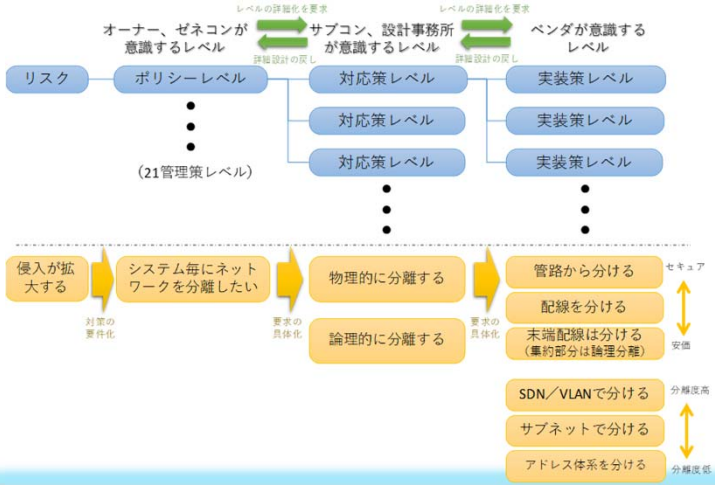
ビルSWG：最新の進捗状況

- 少人数の作業グループでガイドラインの叩き台作成に向けた作業を開始。
- 作業結果をもとにSWGにおいて議論を行い、**まずはガイドライン共通編（骨子）を作成する。**

1．検討の前提として標準的なモデル構成を整理

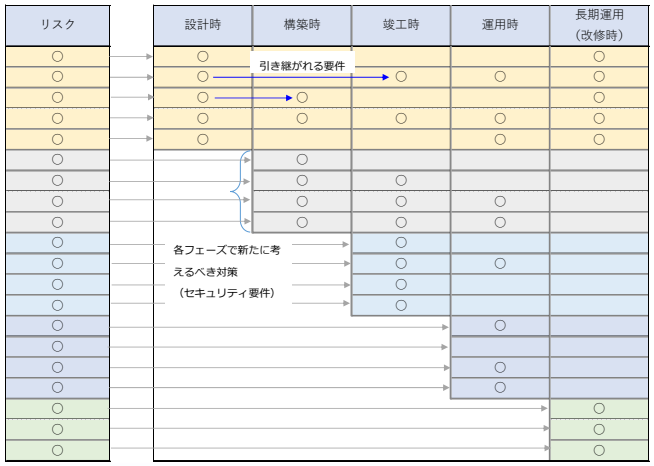


2．対策の階層構造とステークホルダの関係を整理



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

今後さらに．．．

- 各ライフサイクルのステージ毎の対策への展開
- ポリシーレベルから対応策レベルへの対策案の具体化

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

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（２２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。

（※）非政府機関がＣＵＩ（注）を扱う場合について、その機密性の確保のために推奨される14分野、110項目の具体的なセキュリティ要件を明らかにしたもの

（注）Controlled Unclassified Information　機密指定はされていないが管理が必要な情報

＜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＞

平成３０年３月までに計６回の検討会を開催。

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。

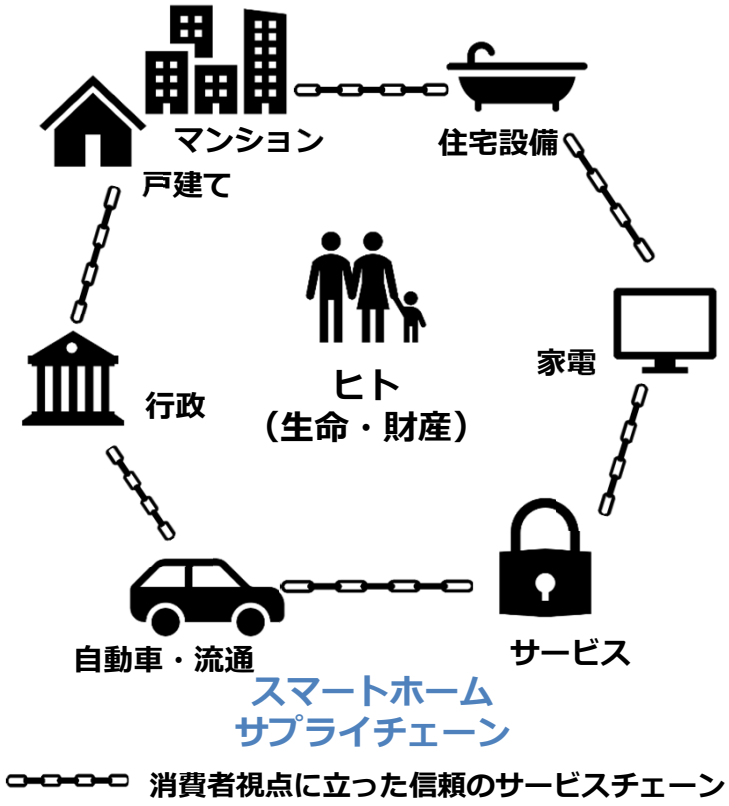
	開催日	検討テーマ
第１回	平成２９年　２月２８日	米国の防衛調達における情報セキュリティ強化の動向
		我が国の防衛調達における情報セキュリティ強化の方向
第２回	平成２９年　４月　５日	情報セキュリティ強化のためのルールのあり方
第３回	平成２９年　５月１９日	
第４回	平成２９年　６月１５日	中間的論点整理
第５回	平成２９年１１月２８日	これまでの振り返り及び現在の検討状況
第６回	平成３０年　３月２９日	新基準適合に向けた取り組み

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 スマートホーム部会内にスマートホームサイバーセキュリティWGを新たに設置
- 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、業界団体が参加

＜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



＜検討項目＞

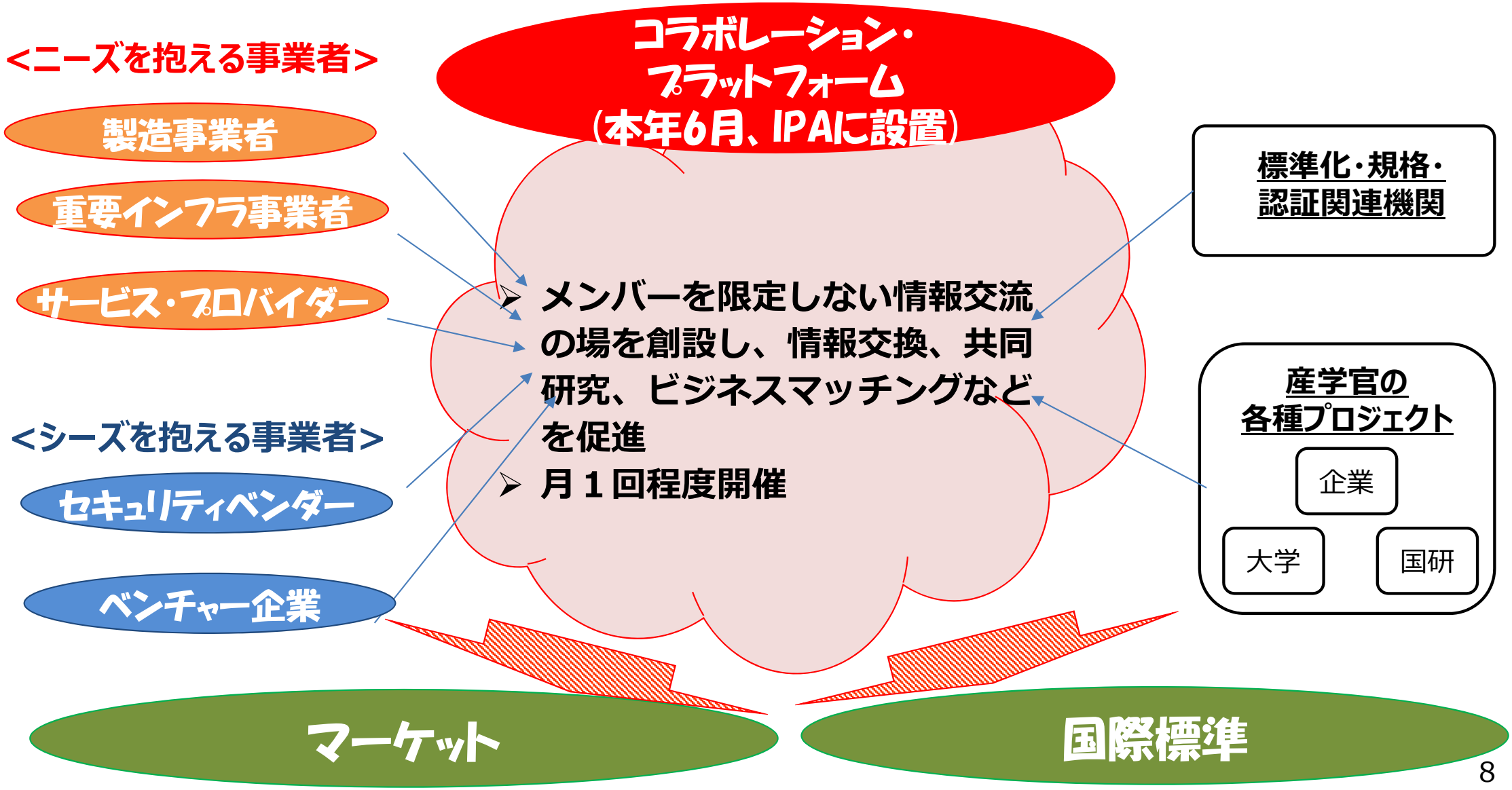
Step1　“スマートホーム産業”に求められるセキュリティ対策像を整理し、**住宅・住設・家電・サービス等のスマートホームサプライチェーンで活用できる「サイバー・フィジカル・セキュリティ対策フレームワーク」**を策定する。

Step2　「サイバー・フィジカル・セキュリティ対策フレームワーク」を概念としてだけではなく、各事業者が実際のセキュリティ対策オペレーションレベルで活用できるよう、実効的な施策について検討を行い、必要に応じて、政府への政策提言を行う。

Step3　実運用に向けて、消費者へのリスク周知や免責事項、モニタリングの在り方、事業者間の信頼の創出方法等について検討。さらには、スマートホームからスマートライフ分野（街・社会インフラ）に対応したセキュリティ対策についても検討を進めていく。

(参考)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。



コラボレーション・プラットフォームの開催状況


富田理事長(IPA)ご挨拶


前田審議官(経済産業省)ご挨拶

第一回

日時：6月13日（14:00～17:00）
参加人数：179名（情報交換会：99名）
主なテーマ：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・フィジカル・セキュリティ対策FW**、
セキュリティビジネスの活性化）


パネルディスカッション(第一回)

第二回

日時：7月23日（14:00～17:00）
参加人数：104名（情報交換会：74名）
主なテーマ：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）


グループディスカッション(第二回)

＜参加者の声＞

- 最新動向の情報収集、人脈形成等、様々な視点で有益。
- ディスカッションを通じ、他業界の考え方が参考になった。
- 官民対話の機会として有益。政策や戦略への反映を期待。

(*)第二回はグループディスカッション実施のため、第一回よりも定員を少なく設定。