経済産業省

資料7

サイバー・フィジカル・セキュリティの確保に向けた取組

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

1. 研究開発の動向

- SIP第2期「IoT社会に対応したサイバー・フィジカル・セキュリティ」
- 中核的な研究開発拠点の設置
  ～ 産総研 サイバーフィジカルセキュリティ研究センター
- 高度なIoT社会の実現に向けた技術開発

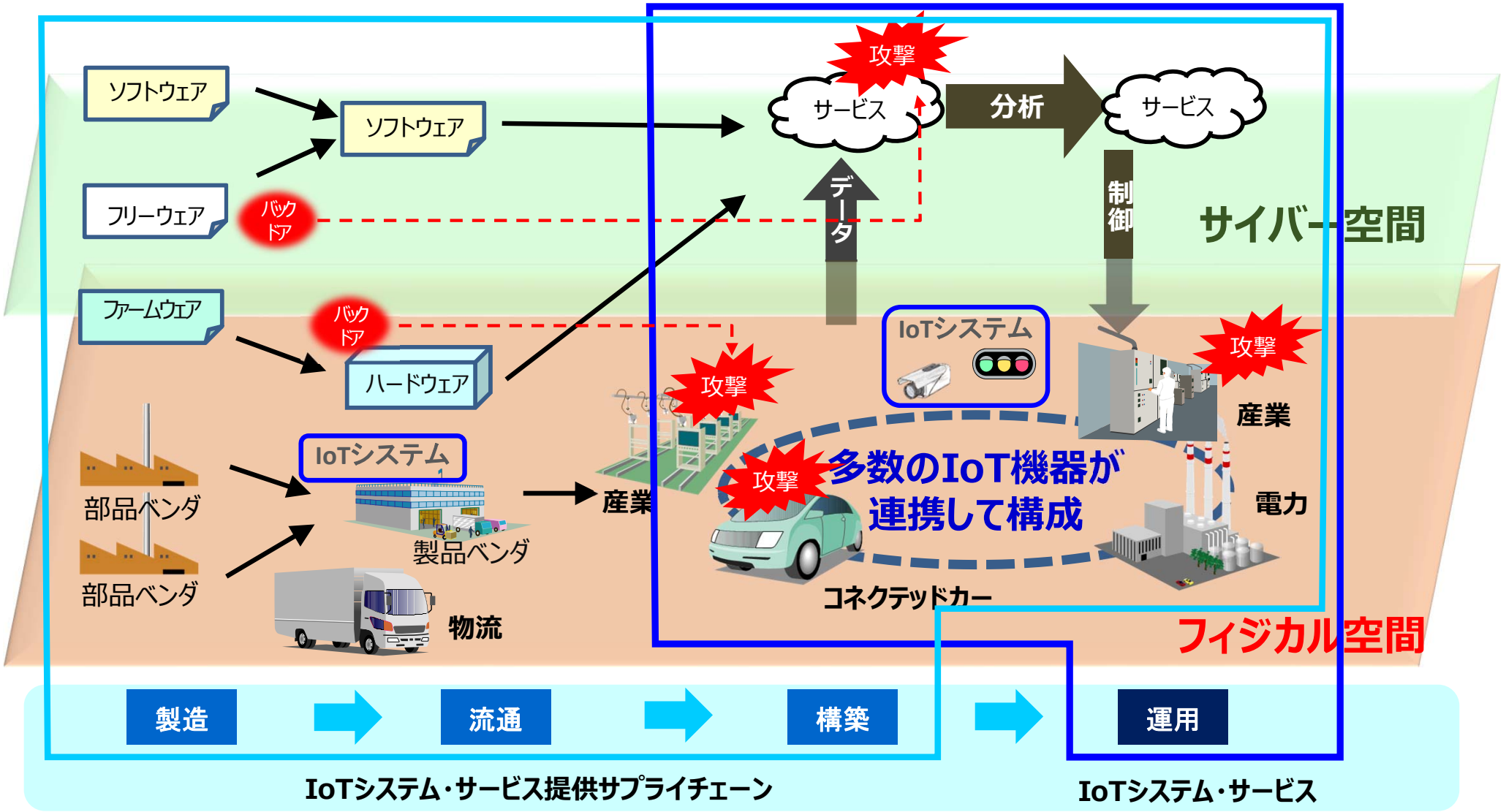
2. 検証基盤の構築に向けた検討（WG3）

SIP第2期 「IoT社会に対応したサイバー・フィジカル・セキュリティ」

複雑につながるサプライチェーン
⇒ 影響範囲が拡大

フィジカルとサイバーの融合 ⇒
- **サイバー攻撃がフィジカル空間まで到達**
- **フィジカルから侵入しサイバー空間への攻撃も**
- **フィジカルとサイバーの間の情報伝達への攻撃**

大量のデータの流通・連携
⇒ データ管理の重要性が増大



SIP第2期 - 研究開発の取組内容・実施体制

A.信頼の創出・証明

ECSEC, 産総研, NTT, NEC, 日立製作所, KDDI総研 等

多様なIoTシステム・サービスやサプライチェーン全体のセキュリティ確保に必要な信頼の創出・証明技術

B.信頼チェーンの構築・流通

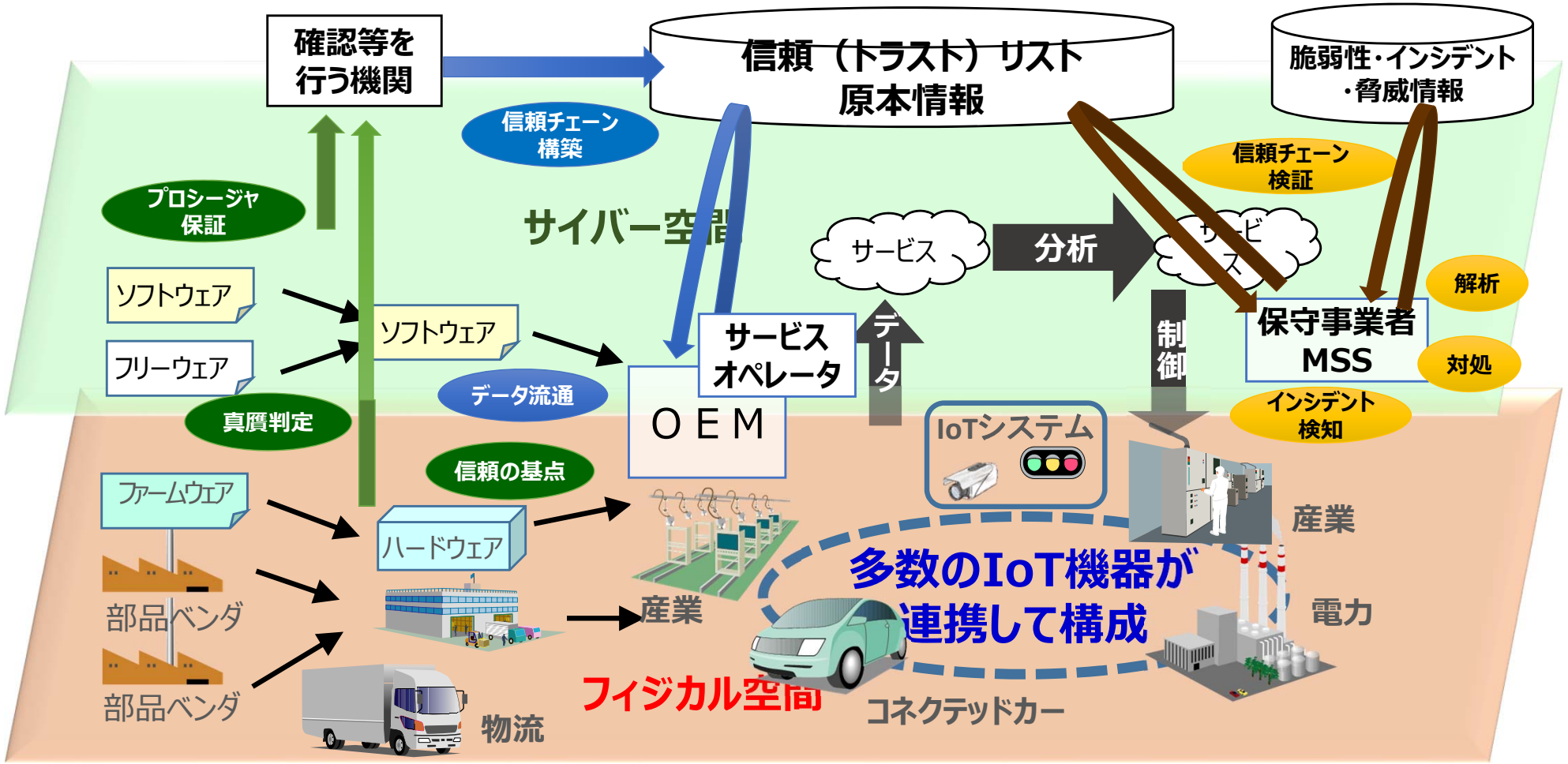
日立製作所, NEC, KDDI総研, 富士通 等

信頼チェーンを構築し、必要な情報をセキュアに流通させる技術

C.信頼チェーンの検証・維持

日立製作所, NEC, KDDI総研, NTT, 三菱電機 等

信頼チェーンが安全に運用されていることを検証し、維持することを可能にする技術



SIP第2期 - 取組の特徴

実証実験から社会実装へ

- 効果測定：実証実験において実用性や実効性の効果測定調査
- 海外発信：国際シンポジウムの開催
- SIPの課題間、他国プロ等との連携

技術成果の継続性・発展性の確保

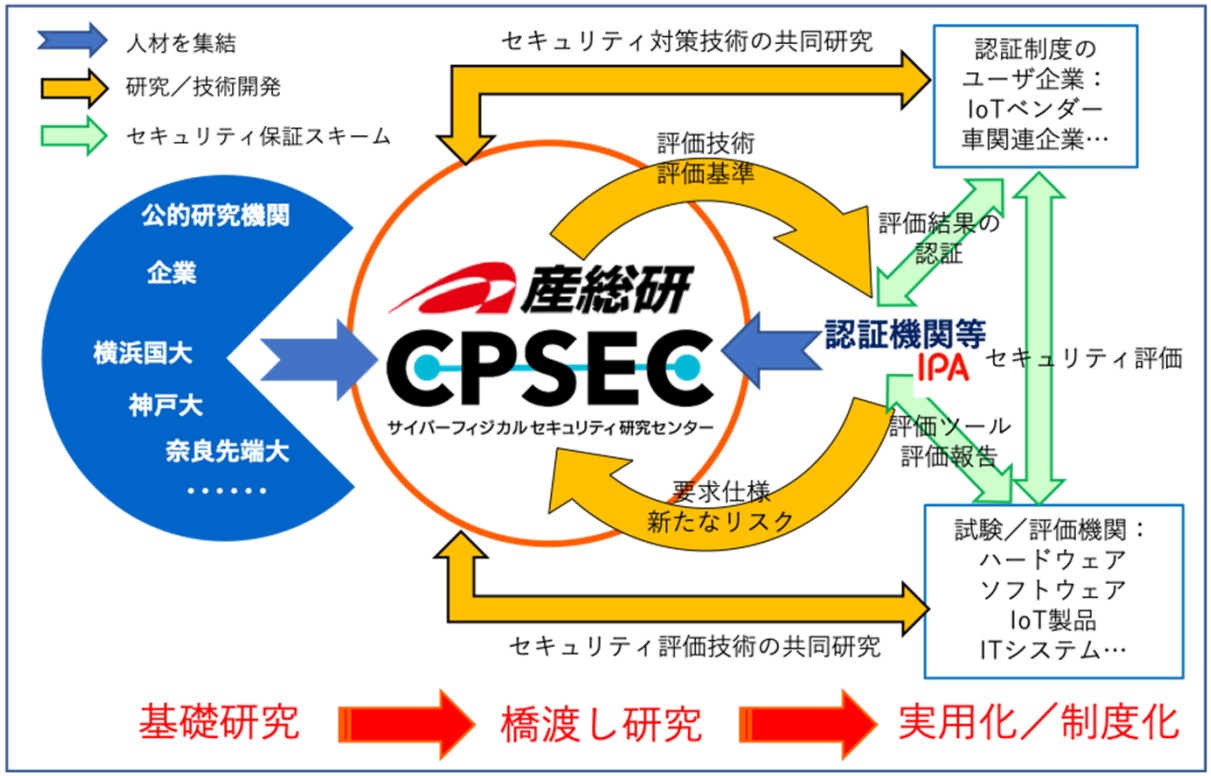
- 参画企業による事業化（製品化）と各産業分野へ導入推進
- 共用検証センター（自主評価用）等の立上げ

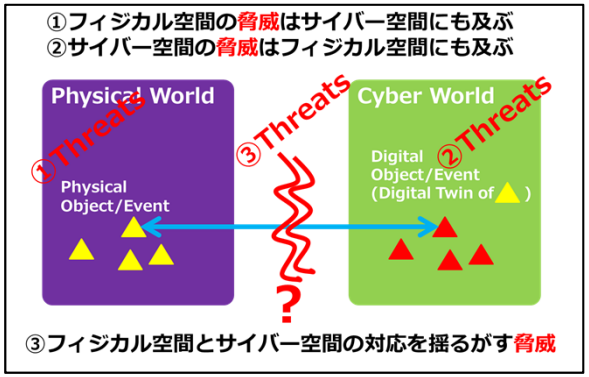
普及のための方策

- 技術動向および政策動向調査
- 関連府省庁の規制・制度改革等における施策連携
- 国際連携：米国NIST, 欧州ENISA等へ積極的な提言

中核的な研究開発拠点の設置
～ 産総研 サイバーフィジカルセキュリティ研究センター（CPSEC）

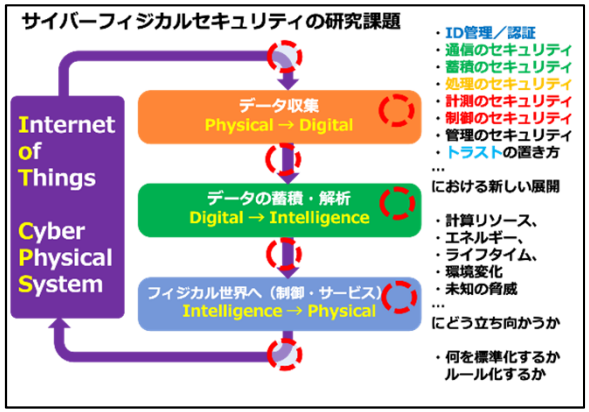
- サイバーフィジカルセキュリティの研究拠点として設置（2018年11月～2025年3月）
- 研究センター長　松本　勉（横浜国立大学とクロスアポイントメント）
- 産総研、企業、大学、試験／評価機関等から研究者や技術者をセンターに集結
  総員115名 = 職員等(産総研の身分を有する者)88名+外来研究員等(含む学生)27名（12月17日時点）
- ７研究チーム（**セキュリティ保証スキーム／高機能暗号／暗号プラットフォーム／ハードウェアセキュリティ／インフラ防護セキュリティ／ソフトウェア品質保証／ソフトウェアアナリティクス**）及び企業との連携研究室で構成
- バリューチェーンにおけるセキュリティで必要となる「研究開発」～「評価制度」までを技術面からサポート
- セキュリティを測定可能とする研究、継続的な最新技術／知見の蓄積





サイバーフィジカルセキュリティとは

セキュリティを考慮すべき対象と研究課題

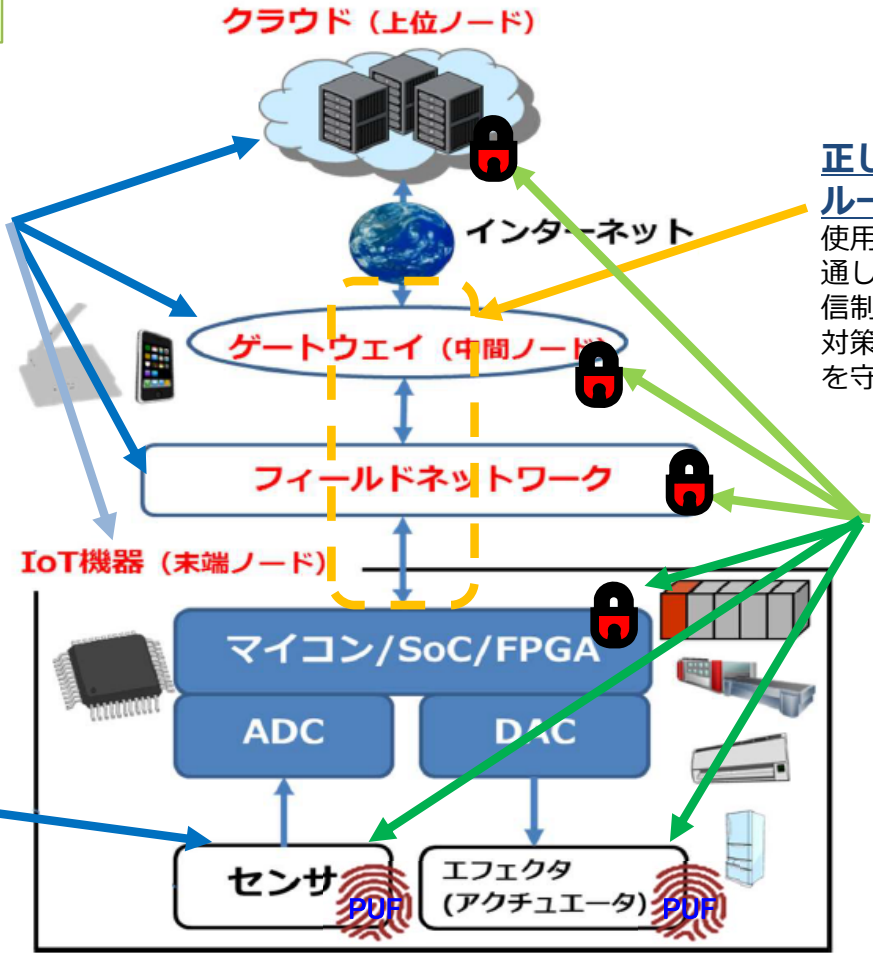


（参考）高度なIoT社会の実現に向けた技術開発（経済産業省）

- 高機能暗号や計測セキュリティ、通信制御機器、複製不可能デバイスなどの**ハードウェアセキュリティ基盤を構築することで、多様なIoT機器からクラウドまでセキュアな環境を実現。**

IoT時代における
ハードウェアセキュリティ基盤の構築

高機能暗号
クラウドからフィールドネットワークまでのセキュリティ課題を解決する為の、高機能暗号を高速・低消費エネルギーで実現するチップとソフトウェアの要素技術の開発。



正しい通信だけを許可するルータ等の通信機器
使用するサービスを元に自動で通してよい通信のみを通す「通信制御」により、セキュリティ対策を個別に実施できない機器を守る。

複製不可能デバイス
製造プロセス中のゆらぎなど複製困難な特性(PUFなど)を利用して実現。デバイス固有のIDや暗号鍵に利用することで、安価に機器認証・偽造品防止する要素技術の開発。

(PUF: Physical Unclonable Function)

計測セキュリティ
センサ等による情報取得に対する脅威への対策に関する要素技術の開発。

（参考）日本特有のセキュリティ要求に応えた製品・サービスの活用を進める『実戦的サイバーセキュリティ検証基盤』の構築

産業サイバーセキュリティ研究会（第2回）資料より

- 日本のセキュリティニーズに応じた日本発の**サイバーセキュリティ製品の有効性等を実機を通じて検証するための『実戦的サイバーセキュリティ検証基盤』**を構築。

実戦的サイバーセキュリティ検証基盤の全体像

1．セキュリティ製品の有効性検証 ＜性能評価＞

＜イメージ＞

- 検証機関が、**セキュリティ製品の有効性を検証し、お墨付きを与えることで、マーケットインを促進。**

2．実環境における試行検証 ＜信頼性評価＞

＜イメージ＞

- ベンチャー等が、**製品の信頼性等を検証するために、製品を民間事業者等へ提供し、実績を作る。**

3．ホワイトハッカーの実攻撃検証 ＜ハイレベルなリスク評価＞

＜イメージ＞

- **ホワイトハッカーによる自由な攻撃**を通じて、**実際の制御系システムのセキュリティを検証。**