研究開発計画の概要

アウトプット目標①（コア技術）

バックドア混入（機器・ソフトウェアの改ざん）を検知する**真贋判定技術**

（システム構築時～運用時）

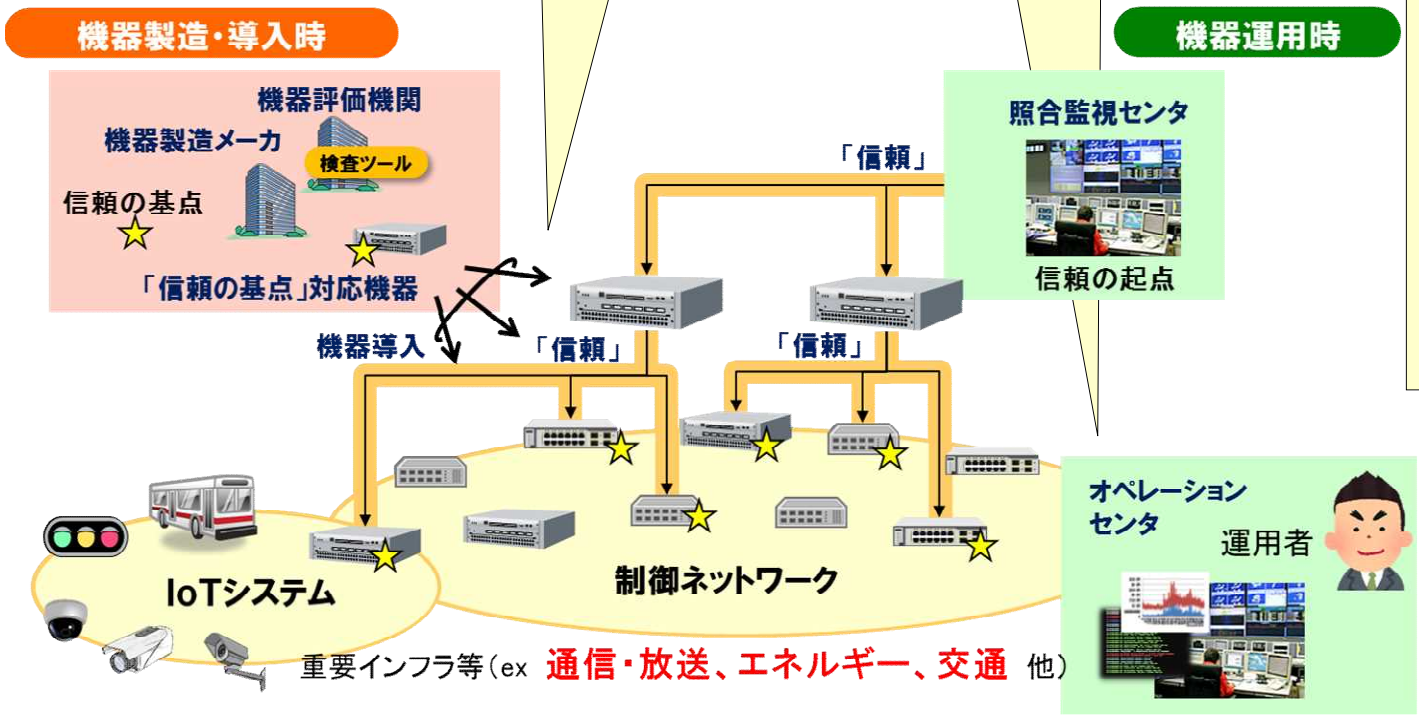
アウトプット目標②（コア技術）

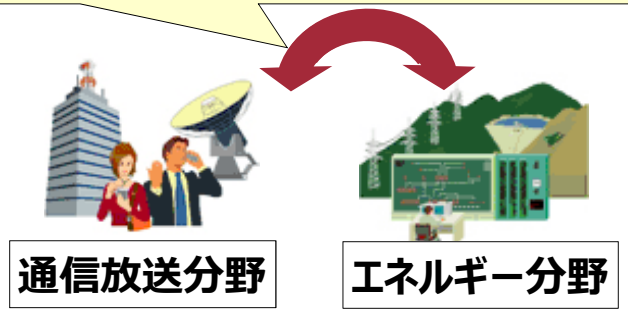
制御ネットワークシステムの異常動作を早期に検知し防御する**動作監視・解析・防御技術**

（運用時）

アウトプット目標③（社会実装技術）

- **適合性確認のあり方と仕組み**
- 重要インフラの環境下での**評価検証技術**
- 重要インフラ分野内・分野間の**情報共有基盤**
- システム運用者の**セキュリティ対応能力**を継続的に向上できる環境整備
- IoT技術の活用ニーズの急速な高まりを踏まえたIoTセキュリティ社会実装技術





アウトカム目標

① 2020年**東京オリンピック・パラリンピック競技大会**の安全な開催

② 将来にわたる**国内重要インフラ**の安定運用と**インフラ輸出**の拡大に寄与

SIP

サイバーセキュリティを確保する仕組み

機器の製造
（機器ベンダー）

ソフトウェア

不正機能検出

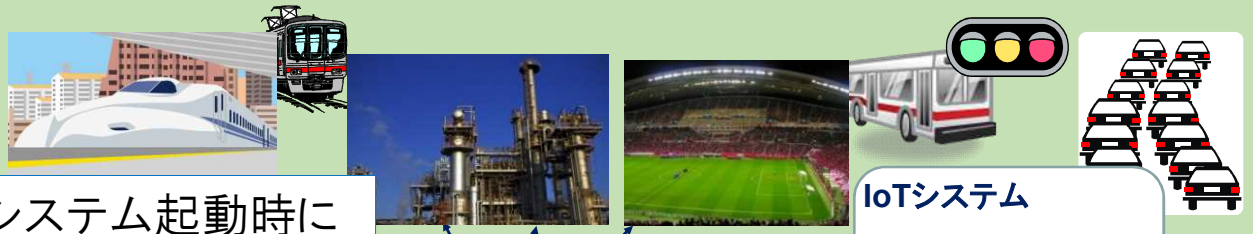
「信頼の基点」を機器に作り込み

セキュリティの作り込み

重要インフラ等
（ex　通信･放送、エネルギー、交通　他）

新旧設備が混在

強弱機器が混在



IoTシステム

システム起動時にセキュリティを確認

確認後になりすまされる可能性

運用時にもセキュリティ確認

安全にシステム更新

確認後に侵害される可能性

動作監視･解析
「信頼」できる機器での分析により迅速対処

安全にシステム防御

制御ネットワーク

「信頼」

「信頼」

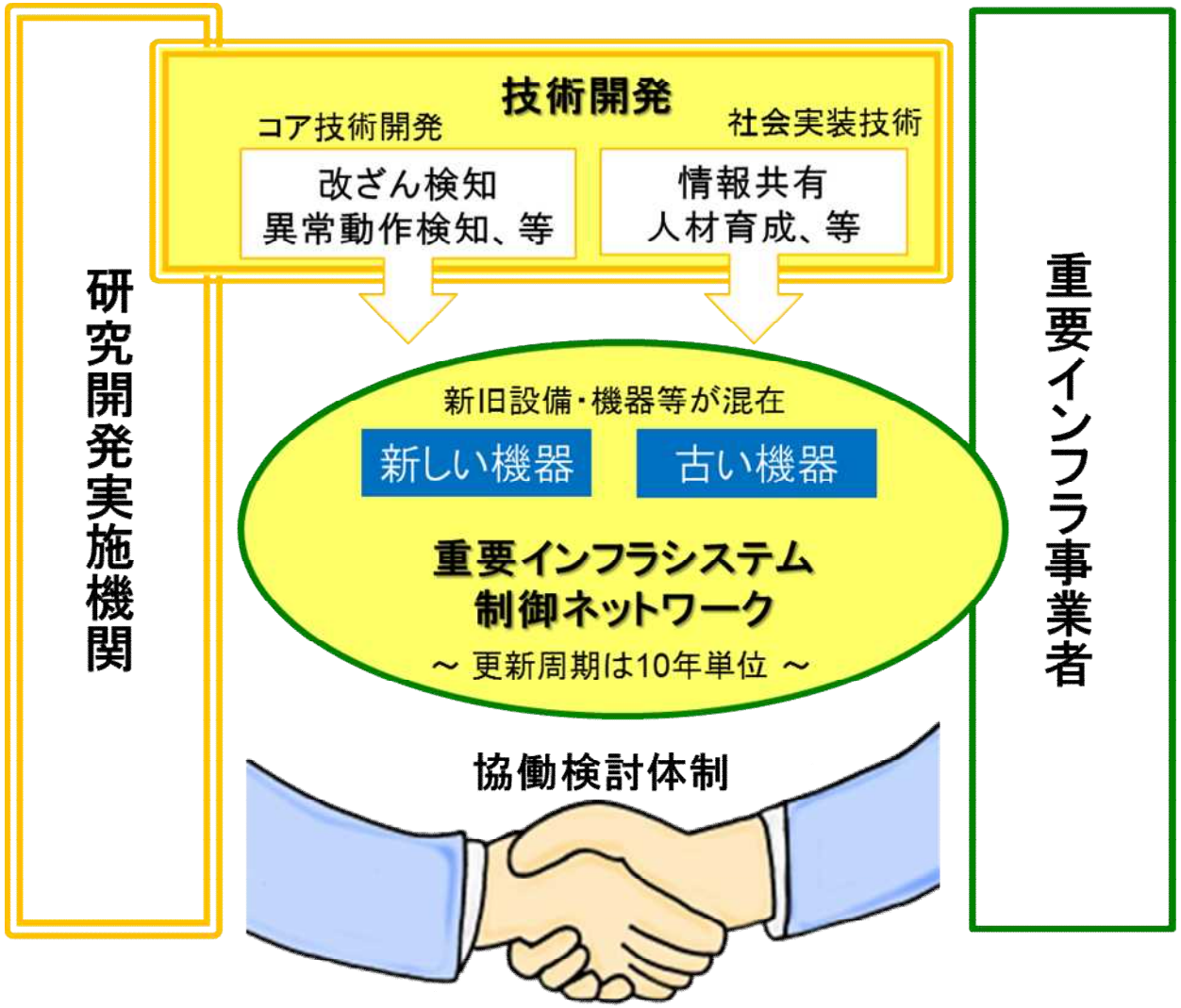
IoT機器の動作監視･解析

運用時のセキュリティ監視と対処

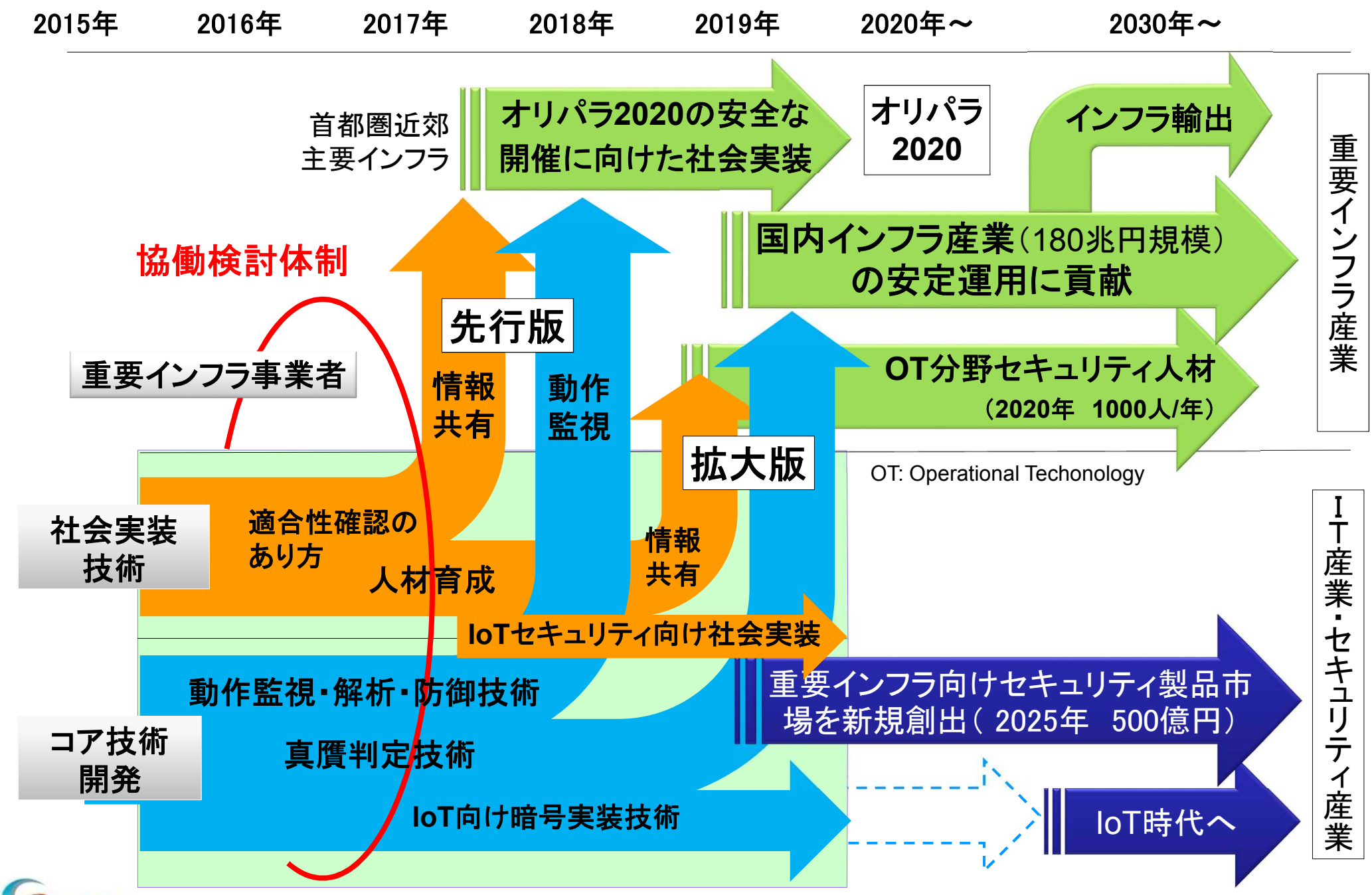
ユーザと一体となった検討体制

重要インフラ事業者との実検証を経て早期の製品化を実現

「優先度の高い対策の早期導入」「事業者側の検証環境での評価」といった重要インフラ事業者からの要望に基づき、先行して実装可能な一部技術の実検証を推進している。その一例が動作監視・解析技術で、旧式の設備と新型の設備が混在する重要インフラ制御システムおいて、セキュリティ攻撃を効果的に検知可能な技術の有効性を確認、2017年末に製品化した。また、人材育成では、実業務に即した教育カリキュラムを策定、重要インフラ事業者と協働で評価とそのフィードバックを進めている。



社会実装に向けた展開計画



SIPサイバーの取り組み

「砦」技術＋「免疫」技術の組合せで多層防御

コア技術開発 → 真贋判定技術
動作監視解析防御技術
IoT向け暗号実装技術

組織の対応能力向上
・情報共有基盤技術
・セキュリティ人材育成
社会実装を促す仕組み

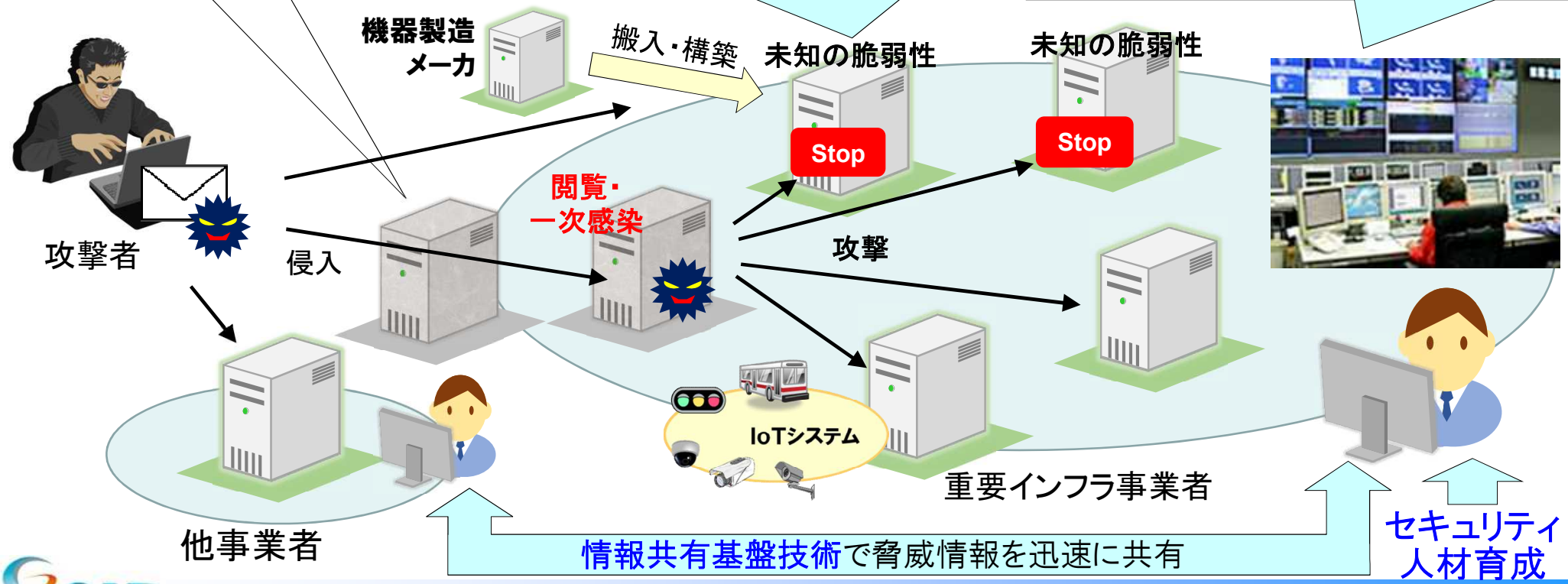
外部からの侵入を防止する
「砦」技術（市中技術）

侵入を前提に内部の耐性を強化する
「免疫」技術（SIPコア技術）

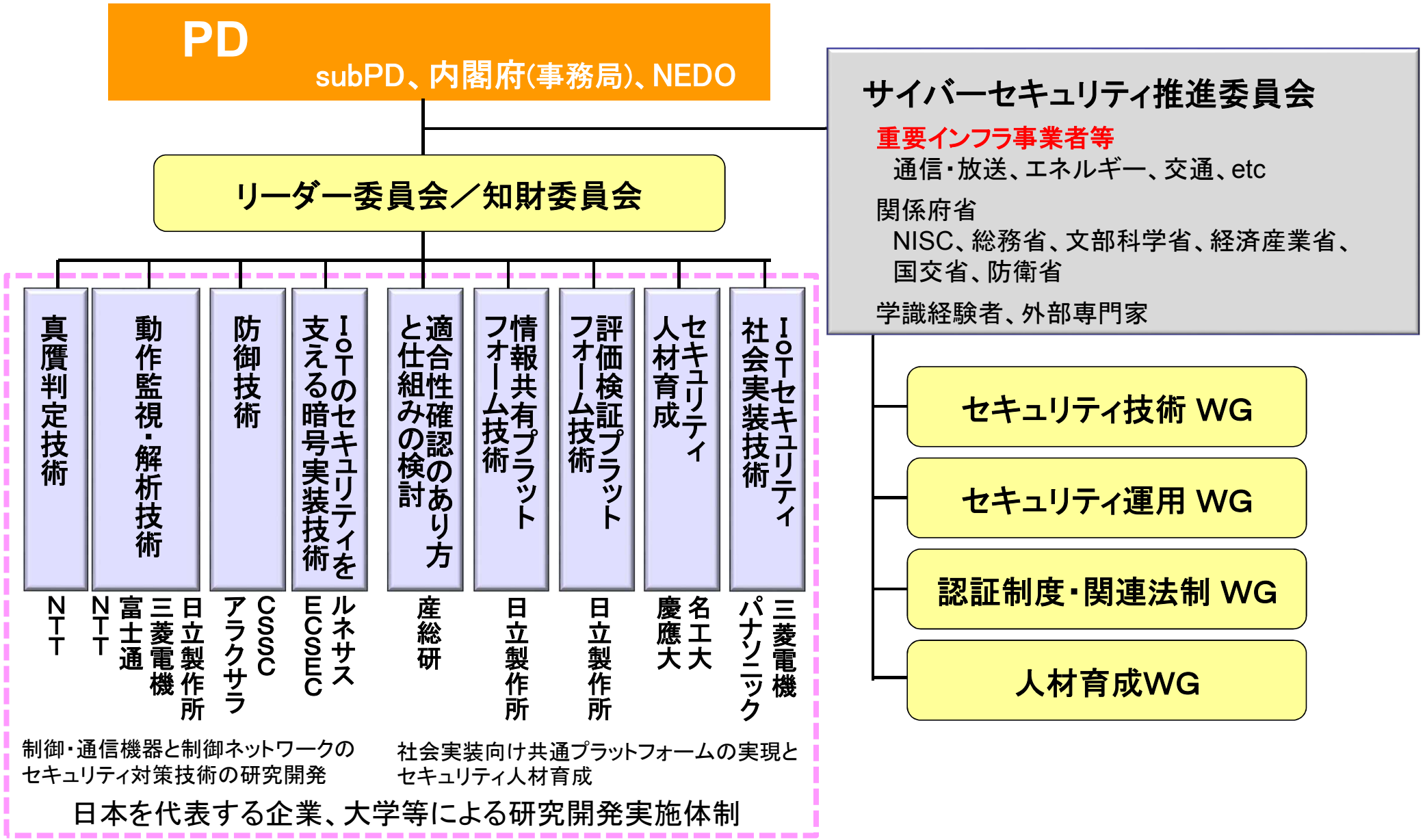
ファイアウォール
ウイルス対策ソフト等

「ビルトイン型」真贋判定技術
未知の脆弱性を突く攻撃でもソフトウェアの改変を常時検知し不正な動作を未然に阻止

「ボルトオン型」動作監視解析技術
通信状態を監視、微細な挙動変化から異常を早期に検知し被害拡大を防止



実施体制


PD
subPD、内閣府(事務局)、NEDO
リーダー委員会／知財委員会
サイバーセキュリティ推進委員会
重要インフラ事業者等
通信・放送、エネルギー、交通、etc
関係府省
NISC、総務省、文部科学省、経済産業省、
国交省、防衛省
学識経験者、外部専門家
セキュリティ技術 WG
セキュリティ運用 WG
認証制度・関連法制 WG
人材育成WG
真贋判定技術
NTT
動作監視・解析技術
NTT
富士通
三菱電機
日立製作所
防御技術
CSSC
アラクサラ
IoTのセキュリティを支える暗号実装技術
ルネサス
ECSEC
適合性確認のあり方と仕組みの検討
産総研
情報共有プラットフォーム技術
日立製作所
評価検証プラットフォーム技術
日立製作所
セキュリティ人材育成
名工大
慶應大
IoTセキュリティ社会実装技術
三菱電機
パナソニック
制御・通信機器と制御ネットワークのセキュリティ対策技術の研究開発
社会実装向け共通プラットフォームの実現とセキュリティ人材育成
日本を代表する企業、大学等による研究開発実施体制