重要インフラ等における サイバーセキュリティの確保と セキュリティ人材育成

情報セキュリティ大学院大学

学術会議連携会員（23-24期）

内閣府 政策参与（PD候補）

後藤 厚宏

重要インフラ等へのサイバーセキュリティ攻撃の脅威は現実のもの

重要インフラ等のサイバーセキュリティ確保

重要インフラ等（ex 通信・放送、エネルギー、交通　他）






IoTシステム

サイバー攻撃
（内部犯行, 侵入者）

制御ネットワーク

サイバー攻撃
（遠隔保守時）

重要インフラの
制御・監視

インフラ事業者の
業務用ネットワーク

外部ネットワーク
（インターネット等）

事業者オフィス

サイバー攻撃

	発生国	インシデント	被害
電力	ブラジル	製鉄所内発電所の制御システムのワーム感染	発電所の数ヶ月停止
ガス	米国	制御システムのマルウェア感染	制御システムへアクセスする資格情報等の漏えい
鉄道	米国	内部システムのマルウェア蔓延	鉄道運行の6時間停止
石油化学	サウジアラビア	制御システムのPC 3万台がマルウェア感染。	内部ネットワークの1週間以上停止、PCデータの全削除

敵を知る（攻撃者の分類）

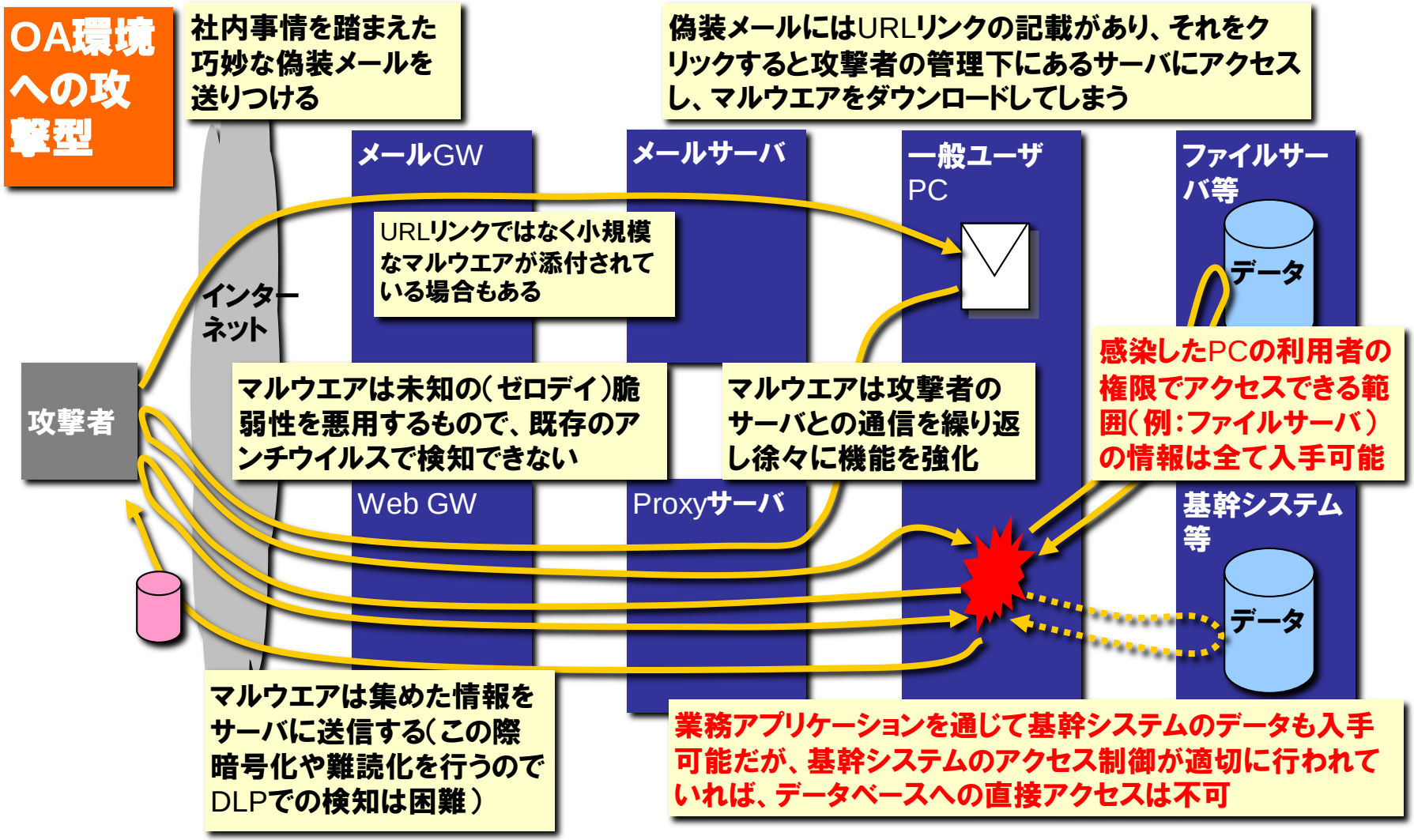
数年前まではCのタイプしか存在しなかったが、AタイプやBタイプの出現に伴って、技術的に高度化するとともに、活動が組織化・執拗化してきている ⇒ 社会経済的背景。

攻撃技術のコモディティ化

攻撃者タイプ	技術力	目的	代表例	被害例
A（コスト度外視）	極めて高度な技術を有する	政治的・軍事的動機の下、標的の活動を妨害することを狙う	不明なるも、軍や情報機関が関係しているとの見方あり	イラン核施設 三菱重工（?） 米国連邦政府職員録（家族含む）（?） 韓国の金融混乱（?）
B（元々得るものなし）	高度な技術を有し、執拗に攻撃する	動機は様々だが、標的にダメージを与えることを狙う	Anonymous 紅客（ホンカ） 等（Hactivist）	Google ソニー子会社 衆議院
C（費用対効果考える）	必ずしも技術的に高度であるとは限らないが、巧妙である等秀でた部分あり	主として金銭的動機に基づき、顧客データ等、価値のある情報の入手を狙う	フィッシング犯 産業スパイ　等	各金融機関等の顧客口座 各技術系企業等

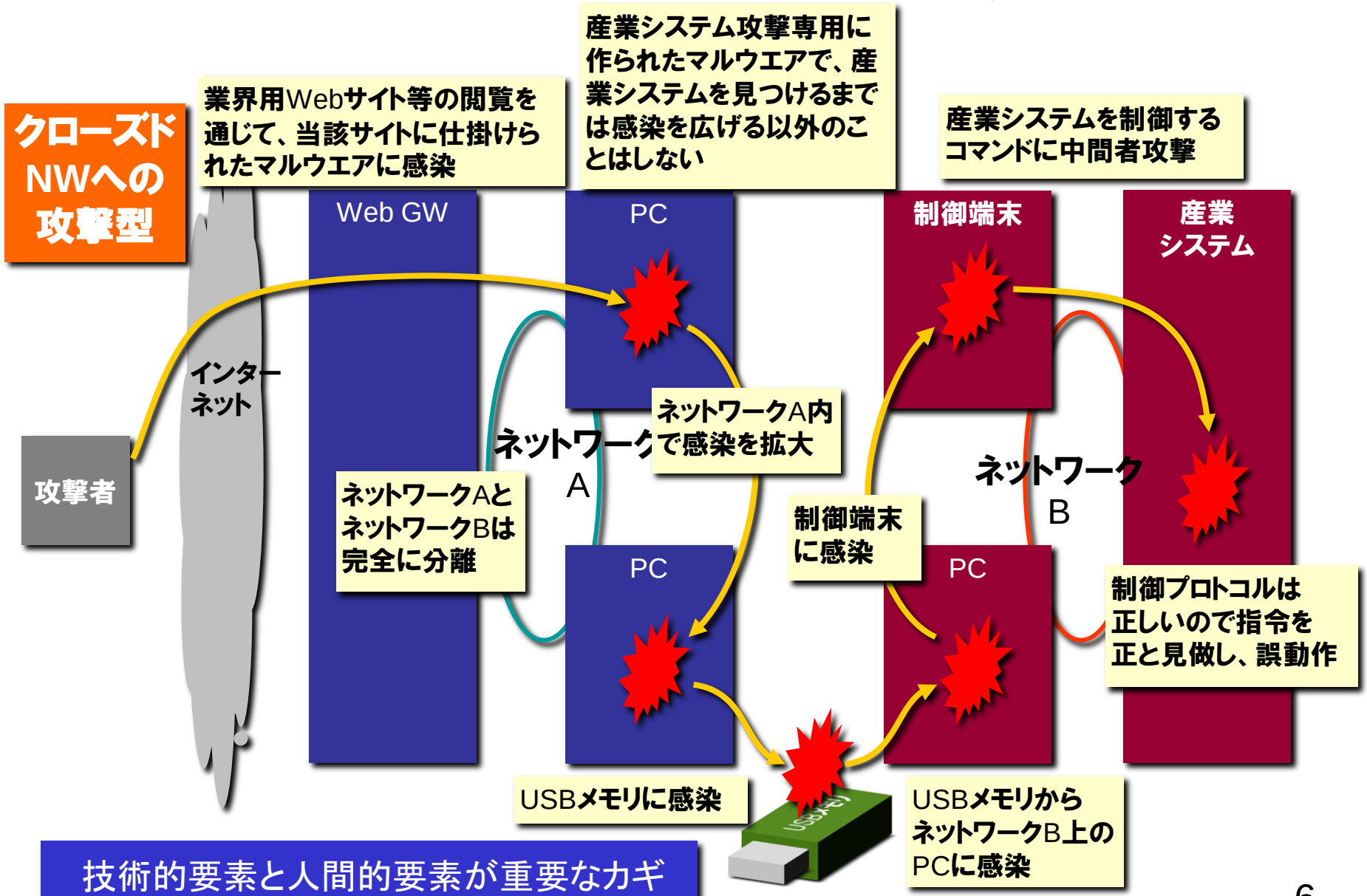
どのような企業でもサイバー攻撃に遭遇する可能性があり、かつ、その時の攻撃者の攻撃技術は決して侮れない。

攻撃の手口



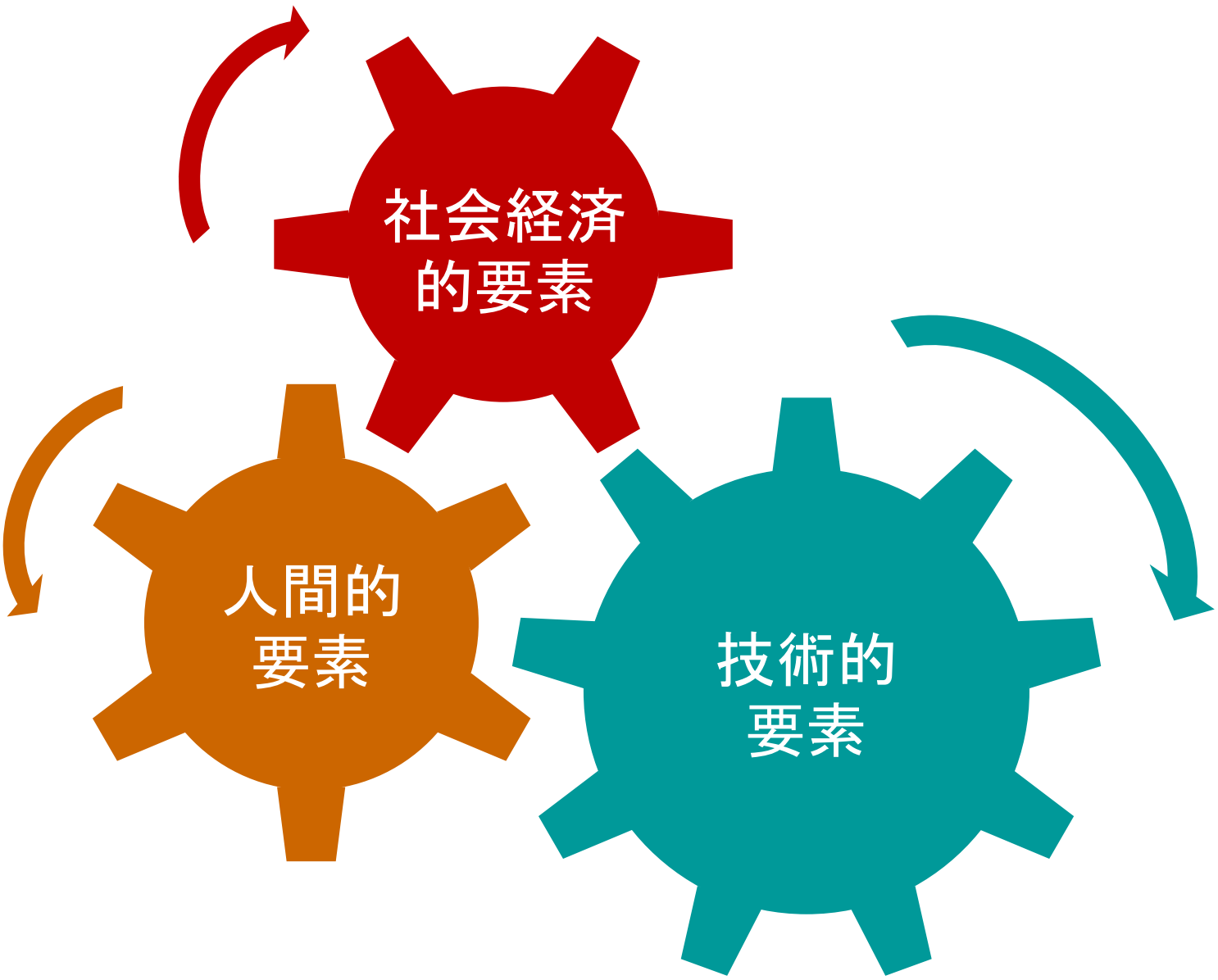
技術的要素と人間的要素が重要なカギ

攻撃の手口



技術的要素と人間的要素が重要なカギ

サイバーセキュリティの3つの要素（要因も対策も）



社会経済的要素

- 重要インフラは社会を支える産業（規模180兆円）
- インフラシステムは輸出産業として期待（2020年目標30兆円）第6回経協インフラ戦略会議
- 2020年オリンピック・パラリンピック東京大会
- コアとなるセキュリティ製品・技術の自給の確保
- 将来のIoT (Internet of Things)普及に向けたセキュリティの先行的（proactive)取組

エス・アイ・ピー
内閣府 SIP プログラム

重要インフラ等における サイバーセキュリティの確保

SIPプログラムの概要

- 社会的に不可欠で、日本の経済・産業競争力にとって重要な課題をCSTIが選定。
- 府省・分野横断的な取組み。
- 基礎研究から実用化・事業化までを見据えて一気通貫で研究開発を推進。
- 企業が研究成果を戦略的に活用しやすい知財システム
- H26年度より10課題スタート：革新的燃焼技術，革新的構造材料，次世代海洋資源調査技術，インフラ維持管理・更新・マネジメント技術，次世代農林水産業創造技術，次世代パワーエレクトロニクス，エネルギーキャリア（水素社会），自動走行（自動運転）システム，レジリエントな防災・減災機能の強化，革新的設計生産技術

11課題め **重要インフラ等におけるサイバーセキュリティの確保**

SIP課題の目標

■ 技術的目標

- 重要インフラのセキュリティ確保のために
  - ◆システム**構築時**に悪意のある機能を**持ち込ませない**
  - ◆システム**運用時**に悪意のある動作を**いち早く発見する**

■ 社会経済的の目標

- **勘所となる**セキュリティ製品・技術の**国内自給を確保**する
- セキュリティ技術を**梃（差異化）**にして重要インフラ産業の**競争力強化**とインフラシステムの輸出増
- 世界で**最も安全**な社会基盤の確立
- 2020年オリンピック・パラリンピック東京大会の**安心安全な開催**

産業競争力 UP!のビジョン

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

サイバー犯罪が世界経済損失　年間53.4兆円
（インターネット創造価値の15～20%程度）
McAfee and CSIS 2014

国内インフラ産業規模：180兆円
市場規模マップ2015

インフラ産業の損失低減 ← 守り ← サイバーセキュリティの確保 → 攻め → インフラ産業の規模拡大

国内市場180兆円・2015年　＋　30兆円・2020年

第6回経協インフラ戦略会議

重要インフラのサイバーセキュリティ対策

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

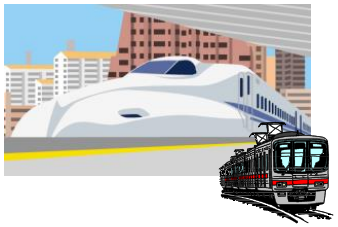
社会実装
（重要インフラ）

政府系

通信・放送

エネルギー

交通



本計画

コア技術

制御・通信機器，IoT機器の
セキュリティ確認技術

**システムの
動作監視・解析・防御技術**

社会実装
技術

認証制度の設計

**情報共有・評価
検証プラット
フォーム技術**

**重要インフ
ラセキュリ
ティ人材の**

マルウェア分析　**物理セキュリティ**

内部統制　**データセキュリティ**

ファイアウォール　**入口出口対策**

現在広く取り組まれている対策技術

既存の認証制度
（EDSA, JISEC, JCMVP, ・・・）

ICTや金融のISAC　**IT人材**

コア技術：セキュリティ確認技術の役割

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

構築時のセキュリティの作り込み

履歴書の内容チェック

ソフトウェア

不正機能検出

入試合格、採用合格

適合性確認

「信頼の基点」を機器に作り込み

身分証明書、実印の準備

運用時のセキュリティ監視と対処

入国時・入館時の身分証明書確認

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

いつでも！身分証明書の確認

運用時にもセキュリティ確認

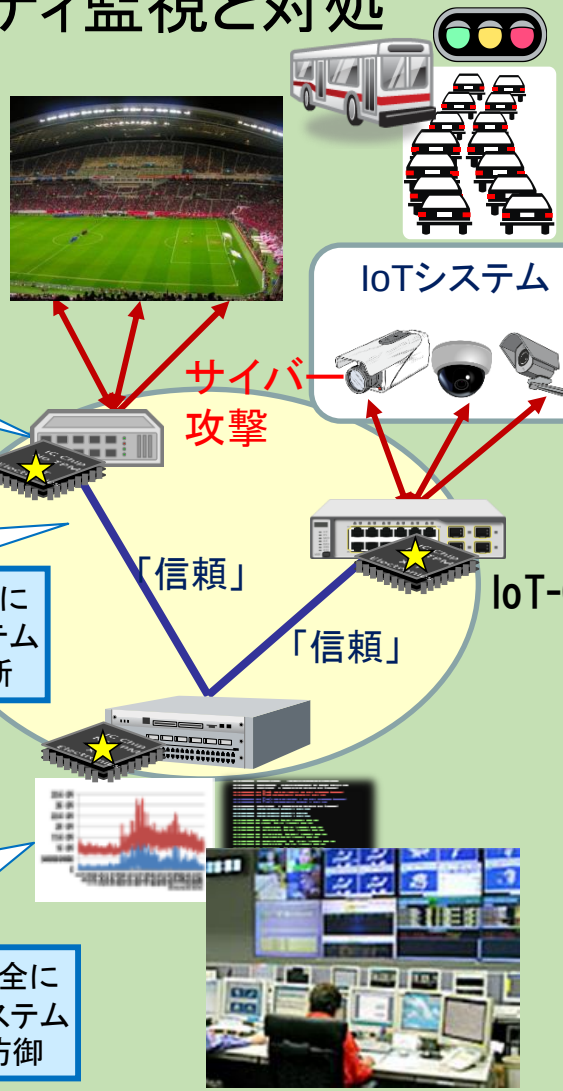
安全にシステム更新

確認後に侵害される可能性

正しい健康診断！

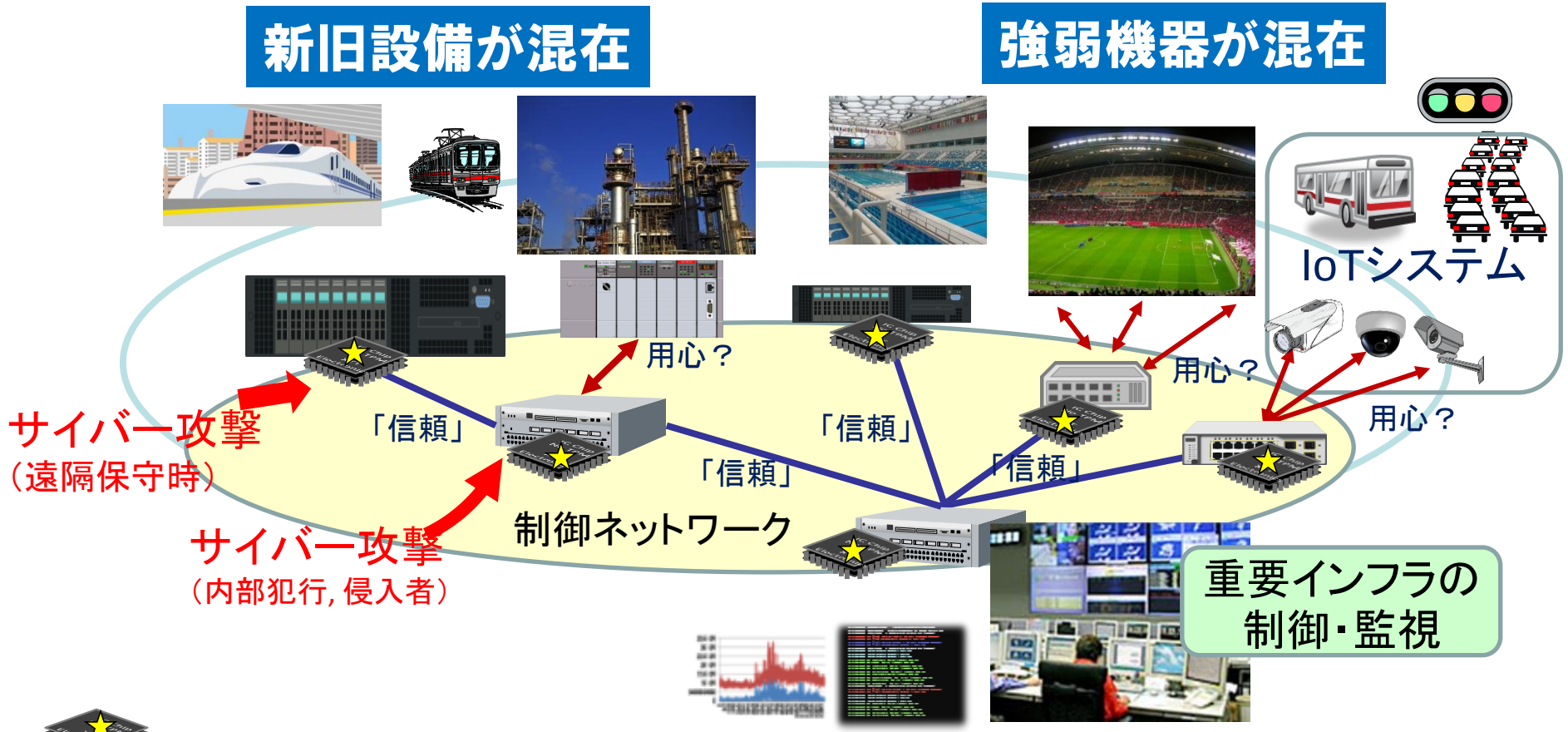
動作監視・解析
「信頼」できる機器での分析により迅速対処

安全にシステム防御



コア技術：動作監視・解析技術の役割

重要インフラ等（ex　通信・放送、エネルギー、交通　他）



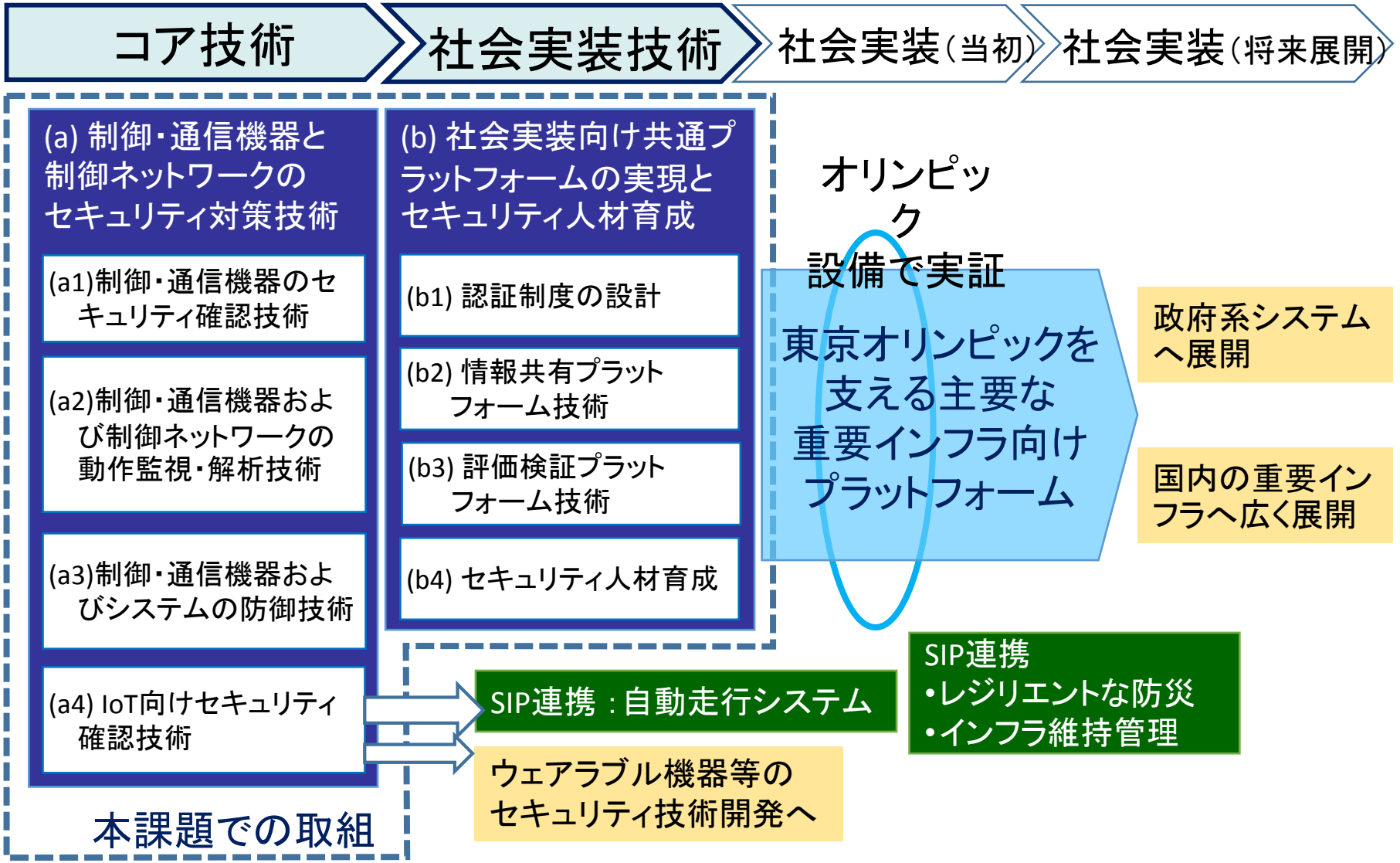
「信頼の基点☆」が入るチップ

制御ネットワークの動作監視と解析

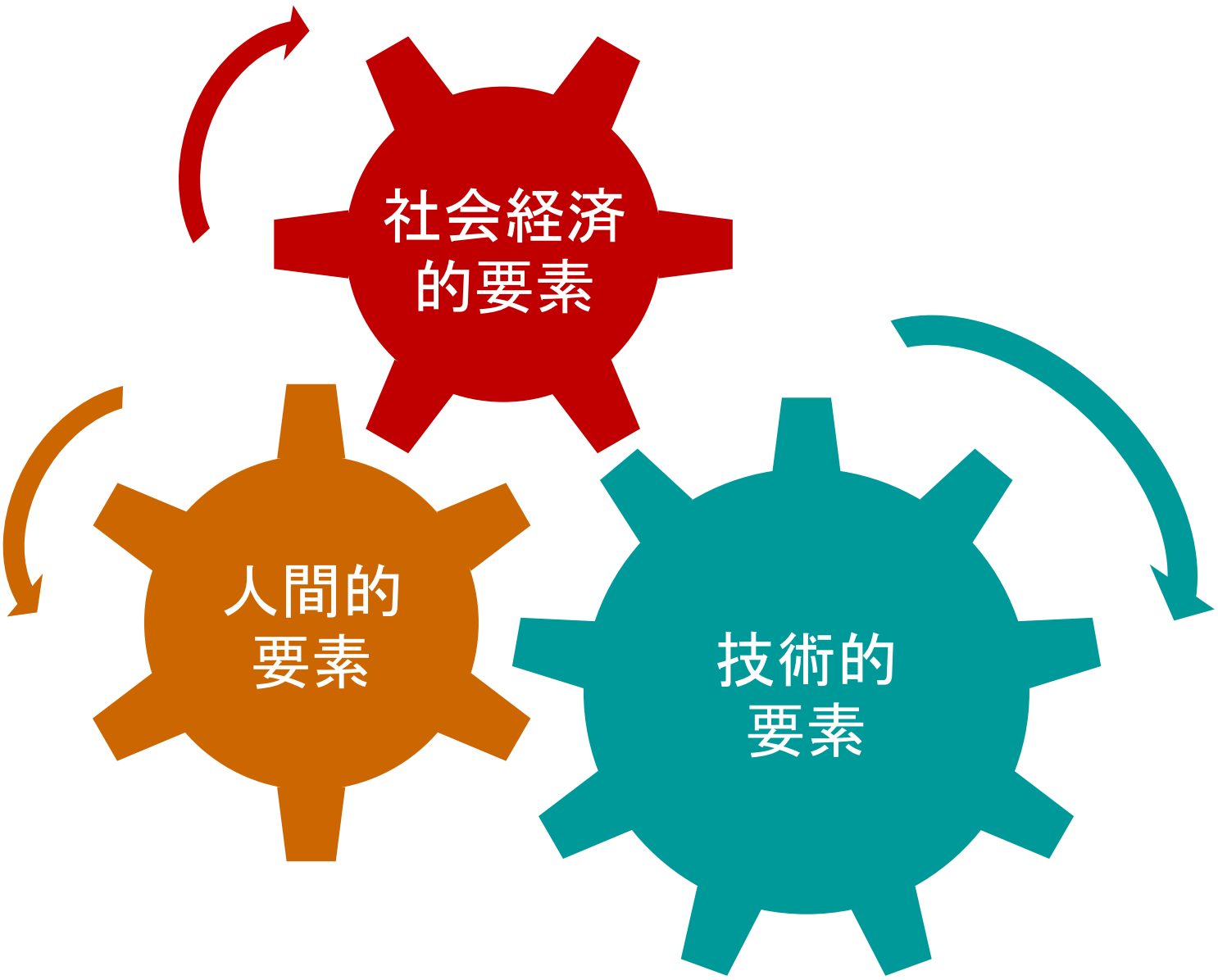
社会実装技術の役割と取組み

- 適切な社会的マネジメントに必要な制度設計と適合性検証技術への取組
- 分野毎・分野間での柔軟な情報共有のプラットフォーム作り
- コア技術の評価検証プラットフォームと重大インシデントにも対応できる準備
- 重要インフラを支えるセキュリティ人材育成

計画の全体像


コア技術
社会実装技術
社会実装（当初）
社会実装（将来展開）
(a) 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
(a1)制御・通信機器のセキュリティ確認技術
(a2)制御・通信機器および制御ネットワークの動作監視・解析技術
(a3)制御・通信機器およびシステムの防御技術
(a4) IoT向けセキュリティ確認技術
(b) 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
(b1) 認証制度の設計
(b2) 情報共有プラットフォーム技術
(b3) 評価検証プラットフォーム技術
(b4) セキュリティ人材育成
本課題での取組
オリンピック設備で実証
東京オリンピックを支える主要な重要インフラ向けプラットフォーム
政府系システムへ展開
国内の重要インフラへ広く展開
SIP連携：自動走行システム
ウェアラブル機器等のセキュリティ技術開発へ
SIP連携
•レジリエントな防災
•インフラ維持管理

サイバーセキュリティの3つの要素（要因も対策も）



セキュリティ人材育成の取組み

社会・産業からの期待される人材像

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

家庭環境，モバイル，交通・自動車，医療，エネルギー・・・
社会全体の『守り』のセキュリティを担える人材

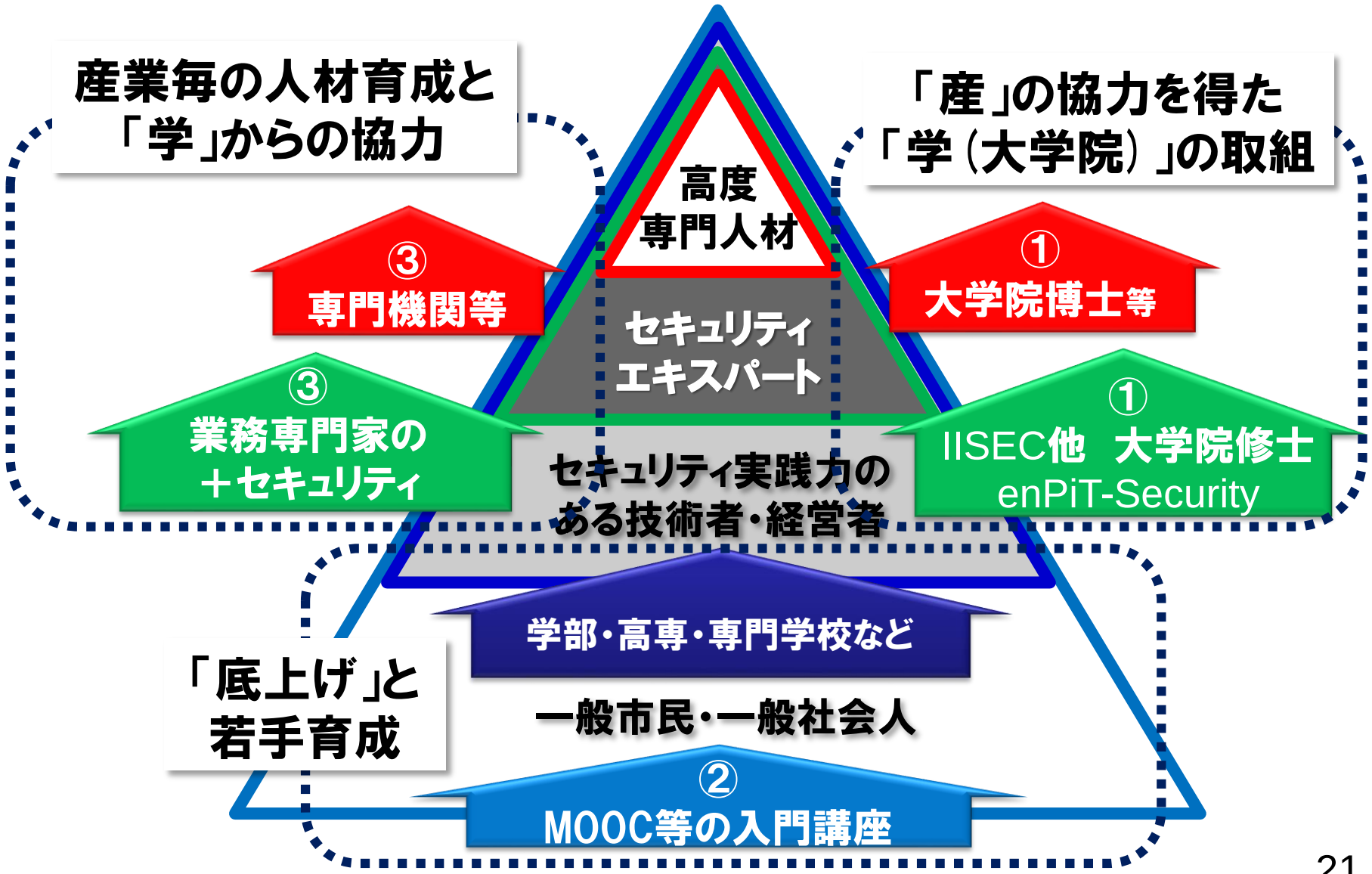
リスクマネジメントを担う人材・経営幹部（CISO）人材

企業の基幹サービス、主要製品の競争力強化に
向けた『攻め』のセキュリティを担える人材

企業のITシステム部門の『守り』の情報セキュリティ人材

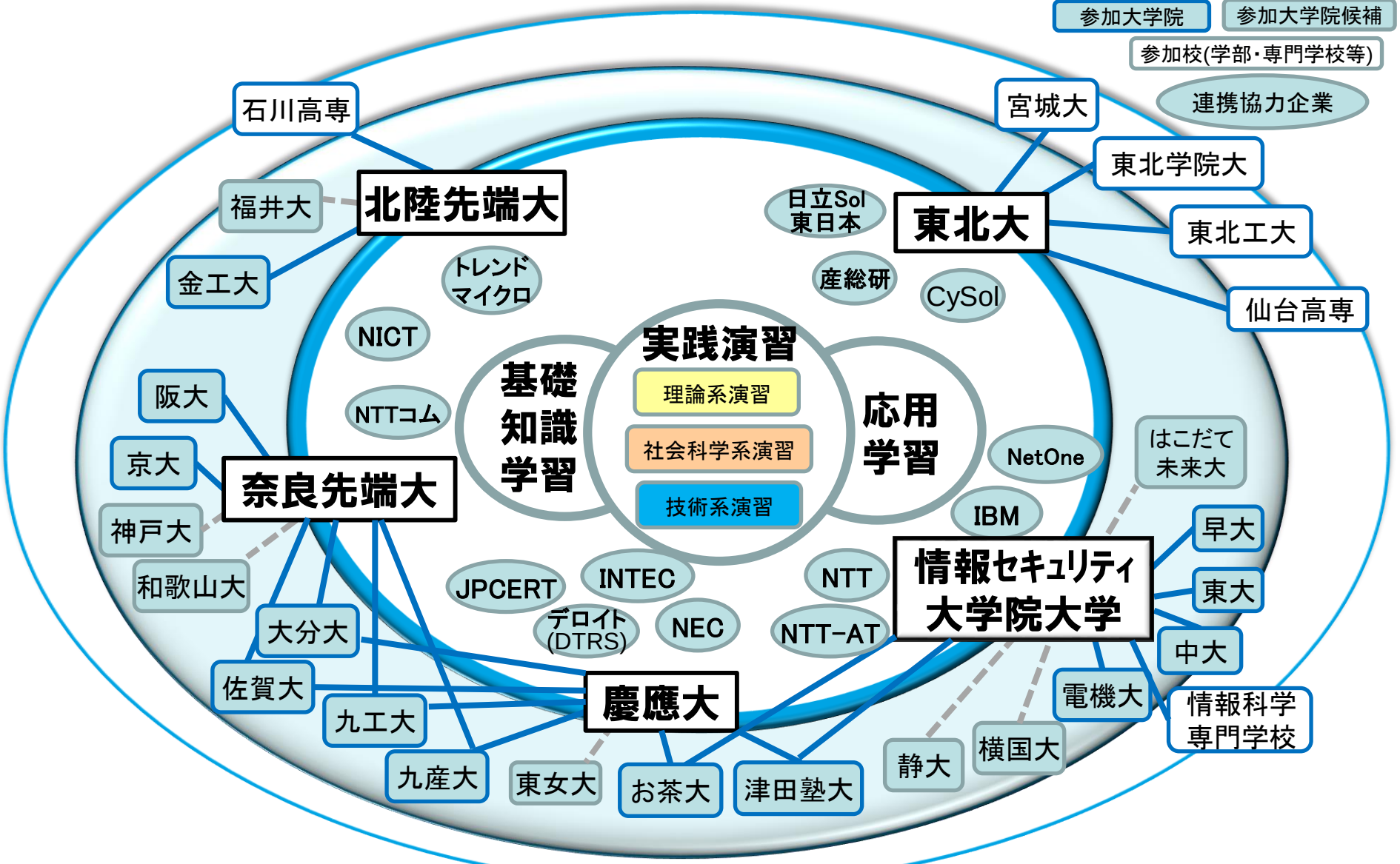
セキュリティ人材育成の取組み

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY



①大学院の取組み：enPiT-Security
（文科省事業 2012～2016）

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY



大学院　修士 主体（＋学部、高専、専門学校）

②MOOCによる幅の拡大と普及啓発

- 一般社会人・大学生・専門学校生向け情報セキュリティの「超入門」講座。2015年5月13日開講（約4週間）

  ⇒約1万人が受講

- 情報セキュリティ「超」入門のステップアップ版として、企業研修向け『情報セキュリティ初級』が10月8日開講。内容は8週分。

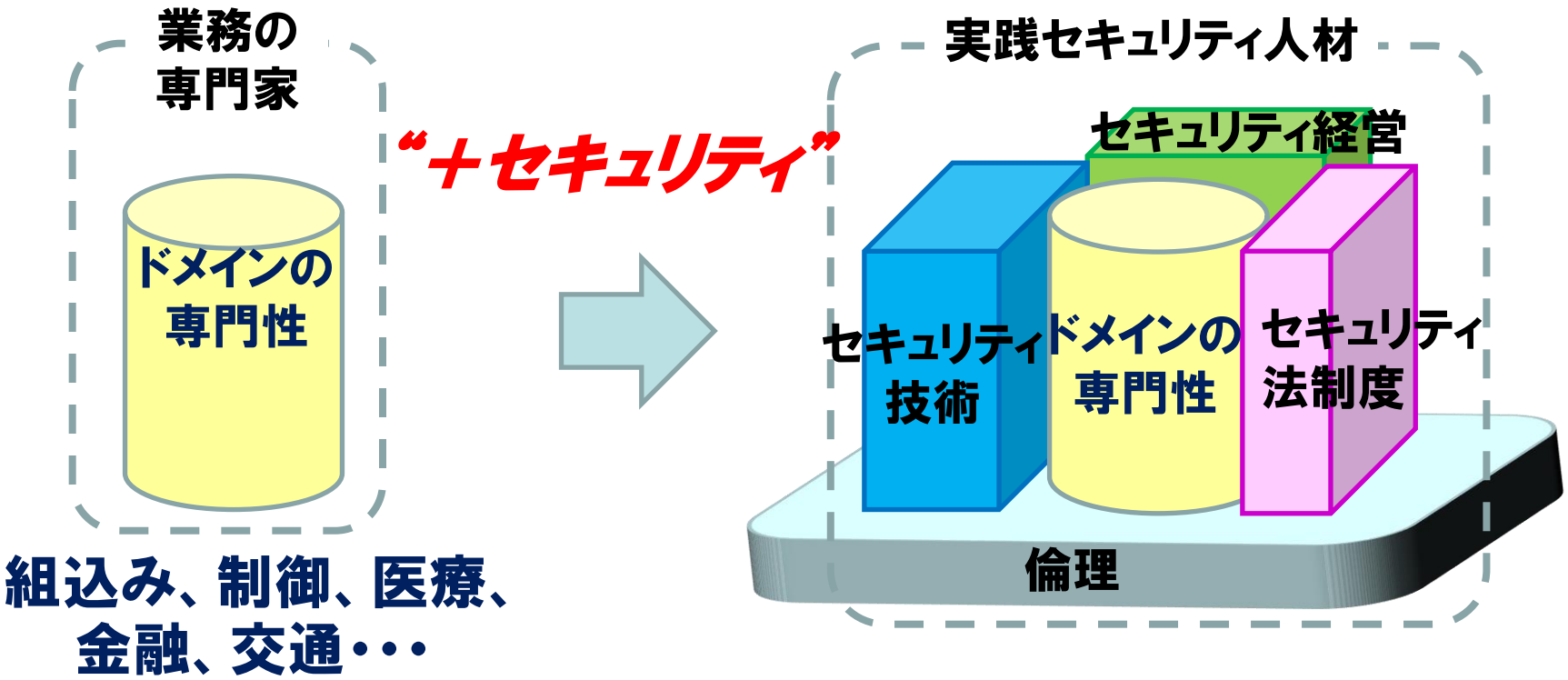
  ⇒約5,000人が受講中

http://gacco.org/

③領域毎の“＋セキュリティ”による実践セキュリティ人材育成

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

ドメイン毎の違い
- ◆ 機密性⇒可用性重視
- ◆ 個別の法制度（医療、金融、他）



組込み、制御、医療、
金融、交通・・・

③産業毎の人材育成と「学」からの協力

産業界の取組み

■ 経団連　2015年2月17日
「サイバーセキュリティ対策の強化に向けた提言」

■ 産業横断サイバーセキュリティ人材育成検討会

「学」からの協力

■ ドメインに応じた“セキュリティ”カリキュラムの対応

- 多様なセキュリティ技術における優先度付け（例：機密性⇒可用性重視）
- 領域毎の法制度や産業構造（経営）の盛り込み

まとめ

- 重要インフラのセキュリティ強靭化が社会・経済的に必須
- まずは2020年オリンピック・パラリンピック東京大会の安心・安全な開催
- 『学』の取組み、『産』の取組みの相互協力

ご清聴ありがとうございました。