制御システムセキュリティ
動向と我々の取り組み

セキュアシステム研究部門
制御システムセキュリティ研究グループ
グループ長 古原 和邦

制御ネットワークの一例

DCS: Distributed Control System
PLC: Programmable Logic Controller
SCADA: Supervisory Control And Data Acquisition

HMI: Human Machine Interface
EWS: Engineering Work Station

制御システムの特徴

- 重要インフラで利用されており攻撃された場合のインパクトが大きい

- 独自プロトコル/OS
- インターネットからは隔離

これらの理由により従来は攻撃対象にはなり難かった

- 可用性重視
- 更新期間が長い

制御システムの特徴

昔

- 独自プロトコル/OS
- インターネットからは隔離

- 可用性重視
- 更新期間が長い

現在

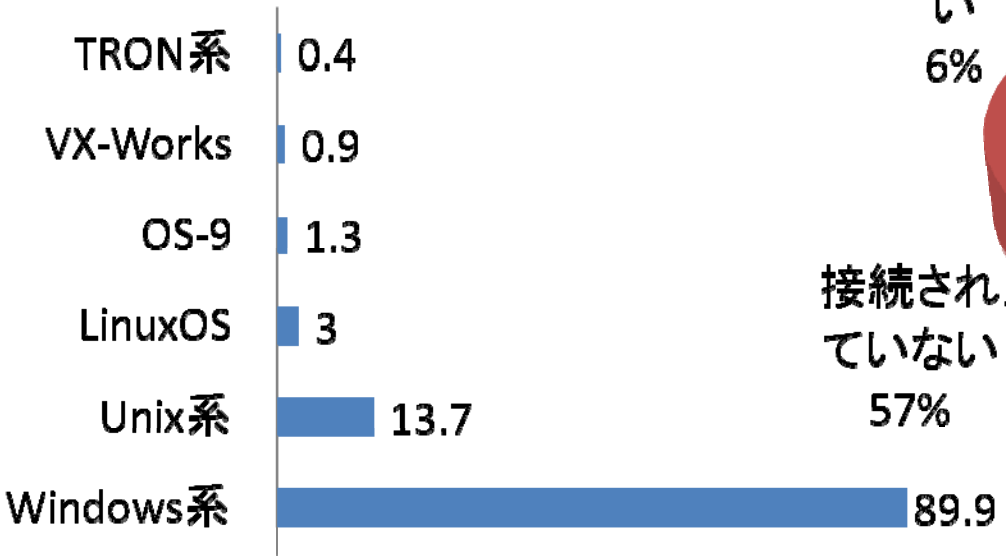
- 汎用的なプロトコル/OSの普及
  - +独自環境も解析対象
- ネットにつながりつつある
  - +隔離環境も攻撃対象

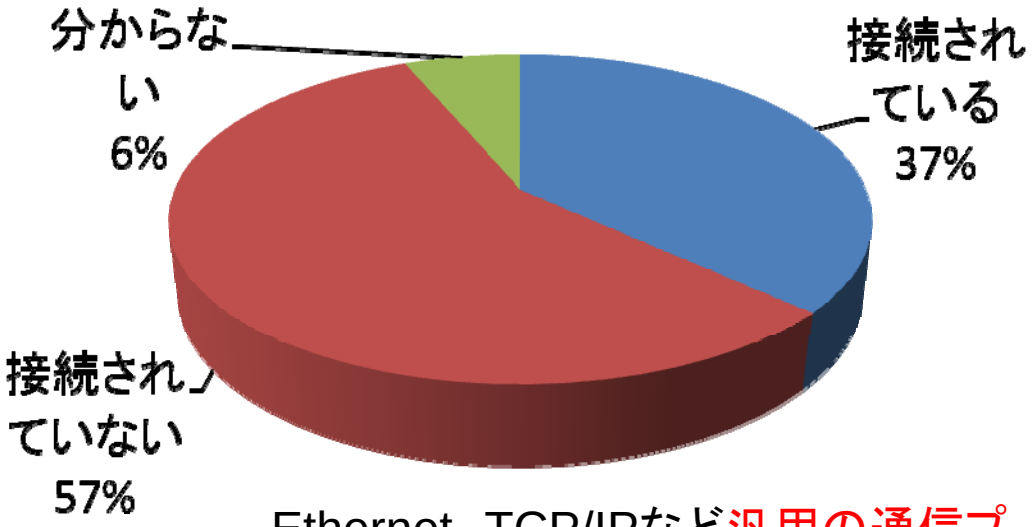
汎用的な対策を適用し難く、対策を吟味する必要がある

- 可用性に影響を与える対策を入れ難い
- 先を見越して対策を入れておかなければならない

制御システムの汎用化

- 制御システムにおけるOSの導入割合(%)
- ネットワークへの接続率





Ethernet、TCP/IPなど汎用の通信プロトコルや無線の導入も進みつつある

出典：工業用装置等における 汎用IT技術応用に起因する脅威と対策に関する実態調査事業 報告書（2009.3）、母数234

インターネット側から接続可能な制御装置

- かなり存在
  - 簡単に見つけることが可能
  - 脆弱性な装置のIPアドレスをリストアップすることも可能
- 多くの場合、無認証もしくは簡易な認証でログイン可能
  - デフォルトパスワード
  - 推測可能なパスワード
  - 平文でのパスワード送信
  - 迂回手段の提供

攻撃側の状況

興味本位

愉快犯

金銭目的

部外者

不特定多数

工作活動(テロ、
サイバーウォーなど)

金銭目的

内部犯

標的型

重要インフラ

過去 → 未来

2010 Stuxnet事件:イランのウラン濃縮施設にて

1. USBなど複数の経路でWindows PCに感染するコンピュータウィルスの広がり

2.通常は停止する前に警告が発せられるのだが。。。

オフィスネットワーク

SCADA/HMI

EWS

3.周波数変換装置のコントローラの設定を変更

制御系情報ネットワーク

2. 特定の制御ソフトを標的

DCS

PLC

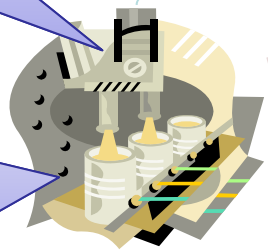
4. 正常に動作しているように表示

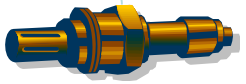
0. 遠心分離機の周波数が上下に変動を繰り返す

制御ネットワーク

制御ネットワーク

1.ウラン濃縮用遠心分離機が停止





エラーや障害のための冗長構成、監視システムが無力化されており、新たな視点での対応策が必要！！

Post Stuxnet Malwares

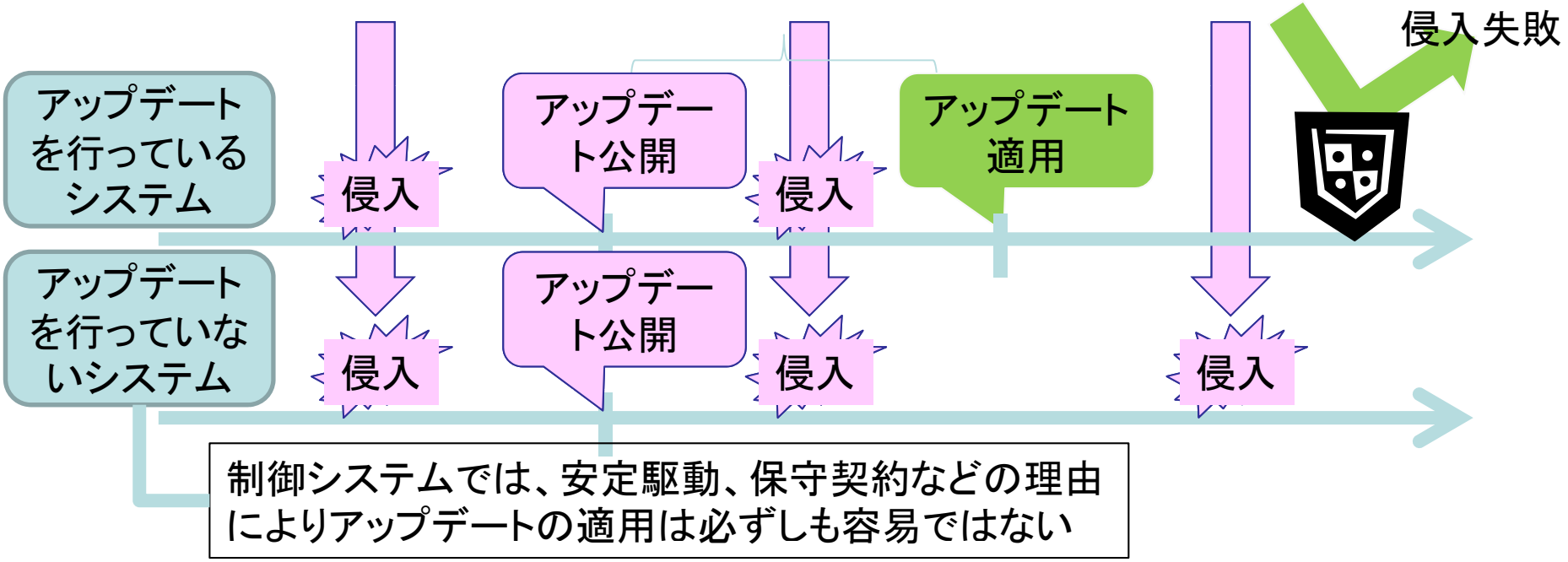
- Duqu, Flame, ZeroAccess, Gaussなど
- 大規模かつ巧妙
  - モジュール化
  - ゼロデイ
  - 特定環境も標的
- ステルス
  - 検出し難い
  - 真の目的が不明確

厄介になってきている点

ディープクラッカー
標的型攻撃

上級クラッカー
ゼロデイ

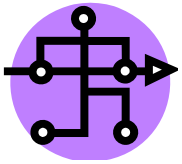
カジュアルクラッカー
脆弱性チェック



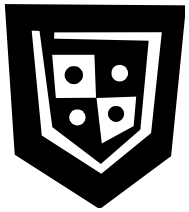
アップデートを適用するだけでは対処しきれなくなってきている！！

我々の取り組み

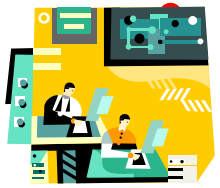
- 最先端の攻撃技術の把握



  - 有効な対応策検討のため
  - 管理された状態でのノウハウの蓄積
- 対応策の網羅的な把握



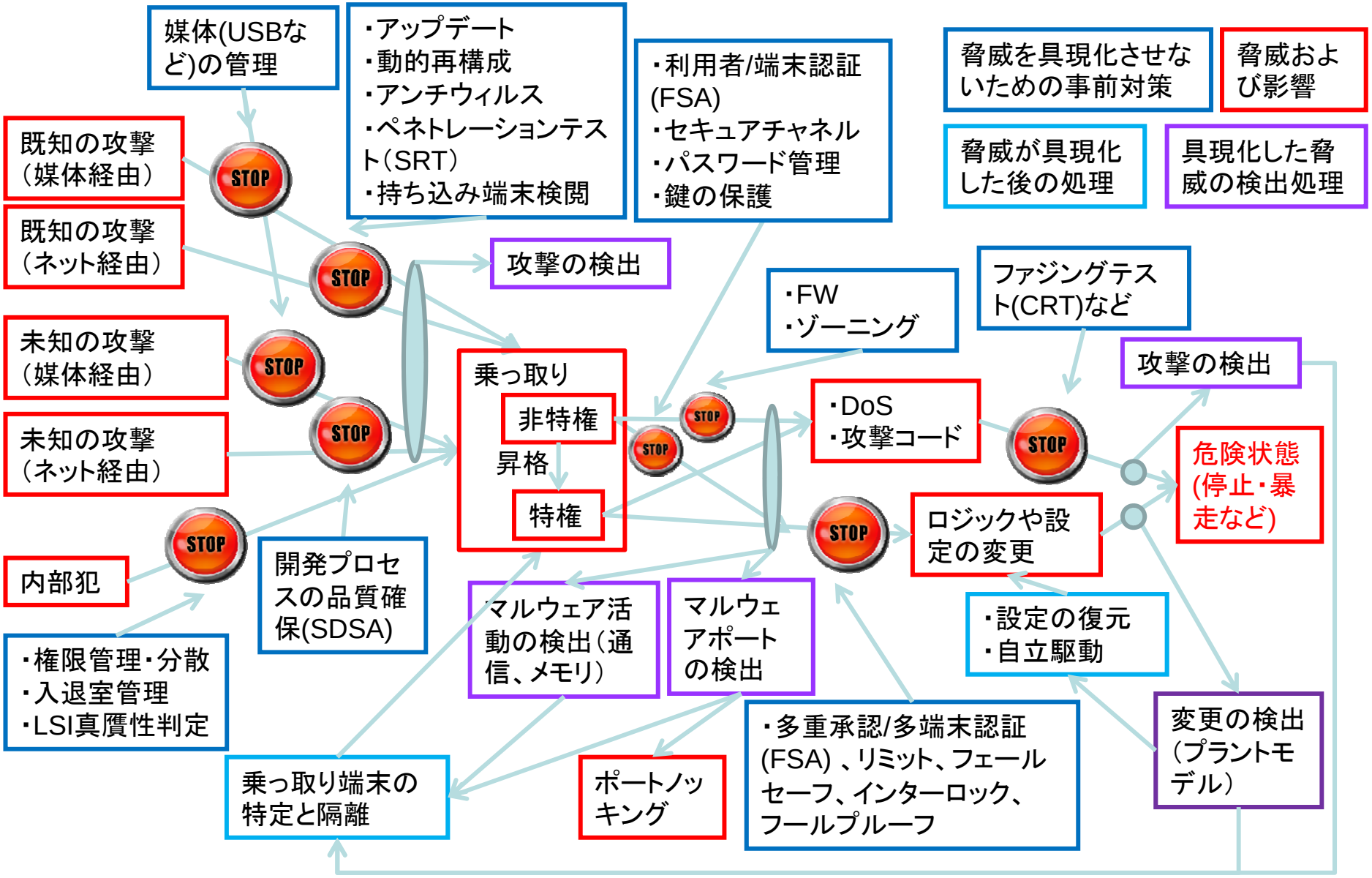
  - 抜けの無いように
  - 現場での状況や制約条件は千差万別、
    - 各状況における費用対効果を最大にするため



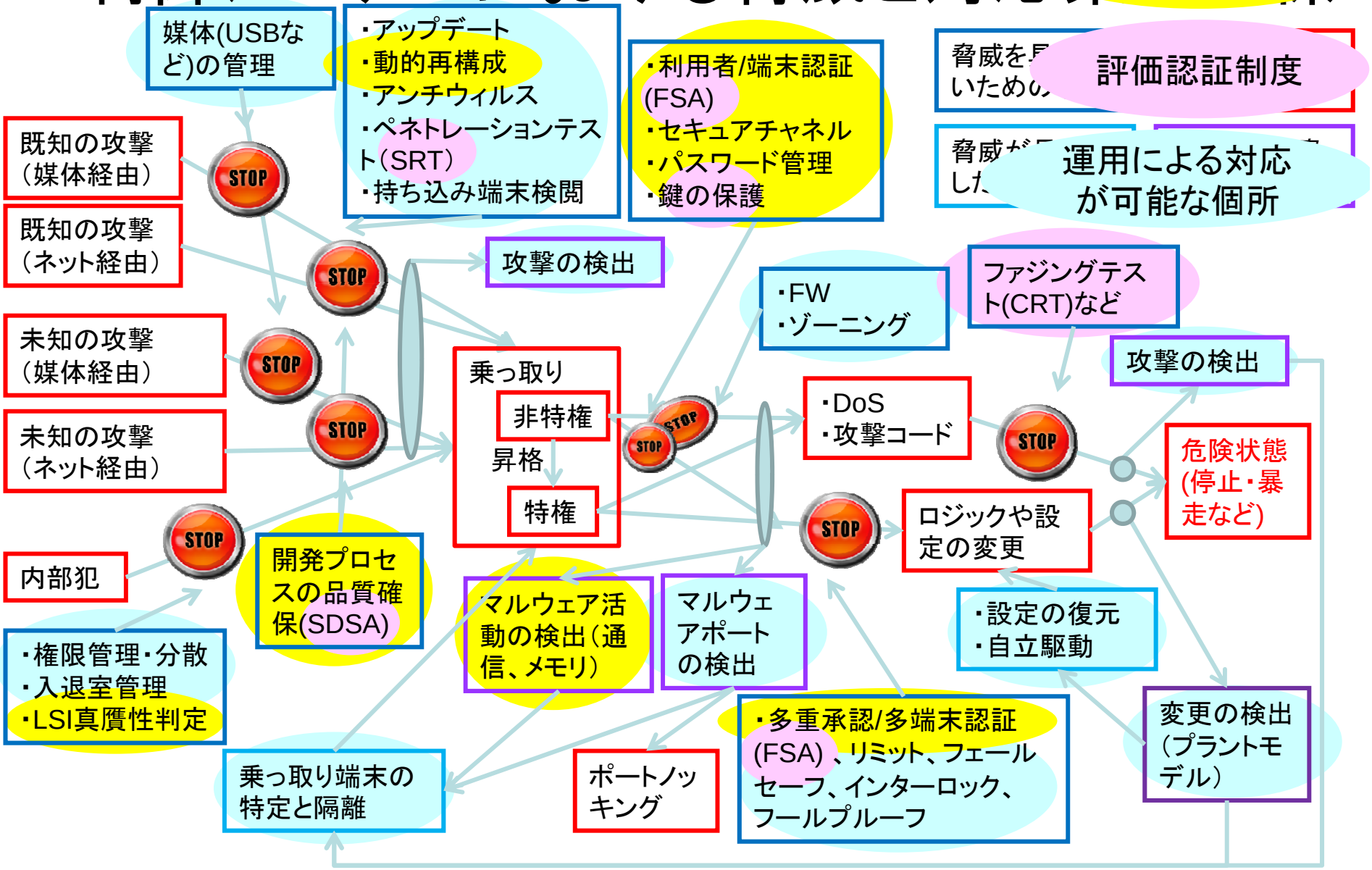
先進的な対策技術の研究開発

  - 現在欠けている技術
  - 将来必要となる技術

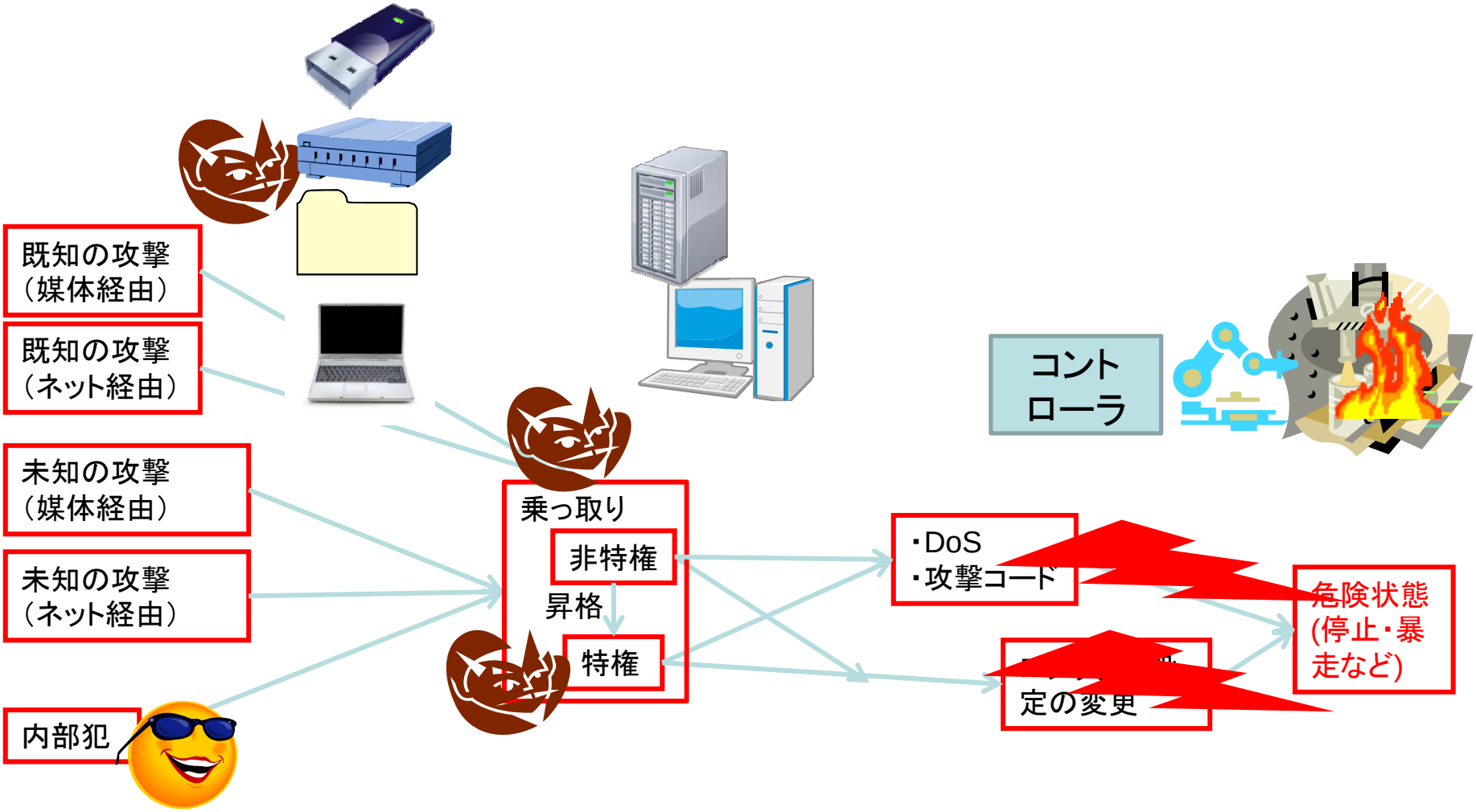
制御システムにおける脅威と対応策の関係



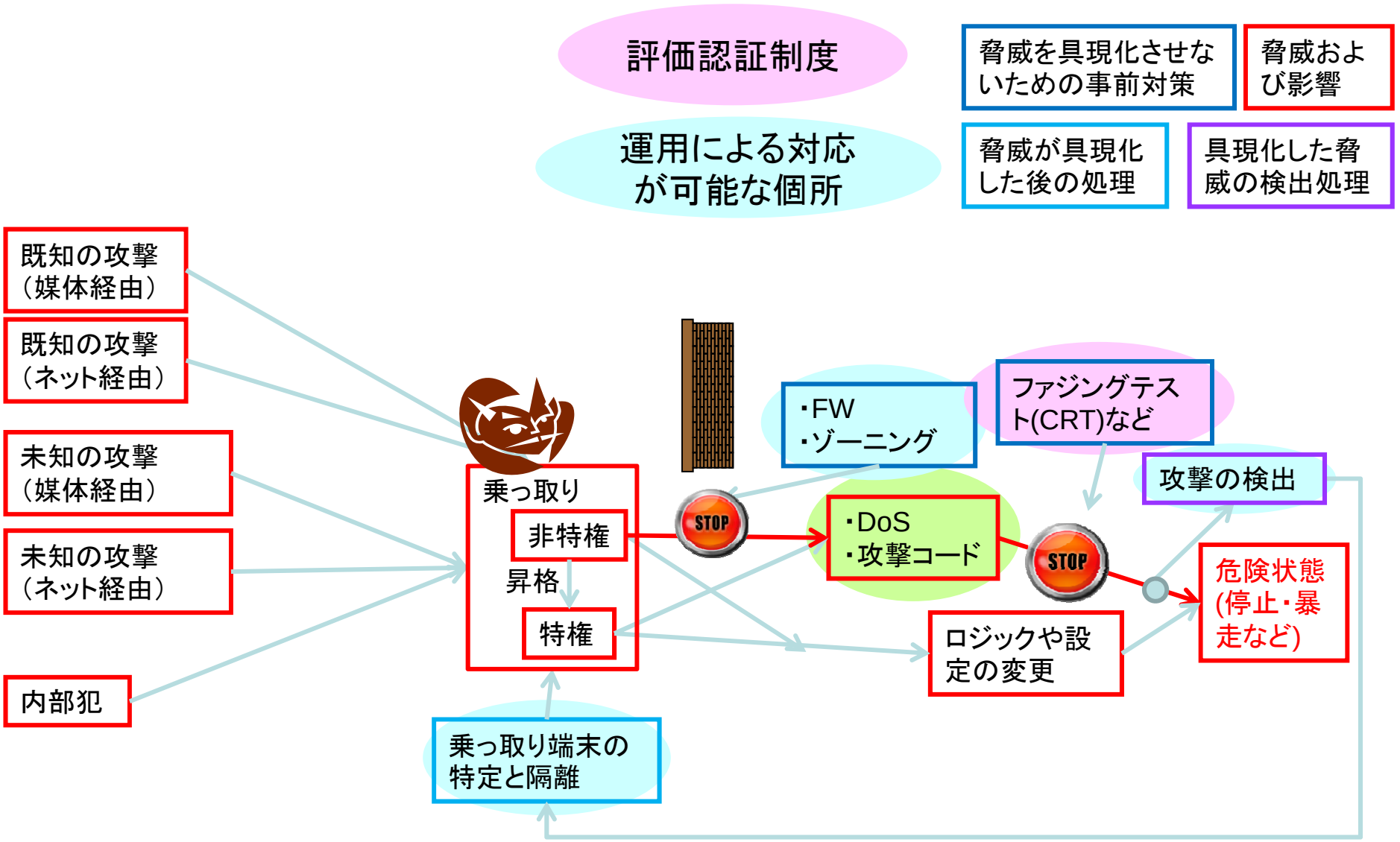
制御システムにおける脅威と対応



制御システムに対する
典型的な攻撃進展パターン



制御システムにおける脅威と対応策の関係

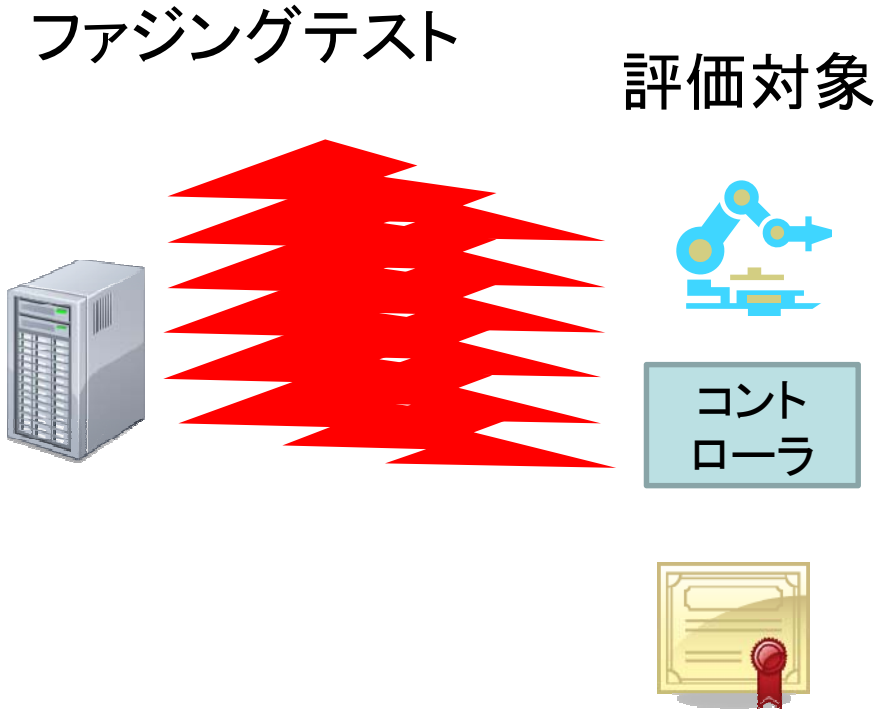


Communication Robustness Testing (CRT)

制御デバイスに対する認証制度が2010年より北米でスタート

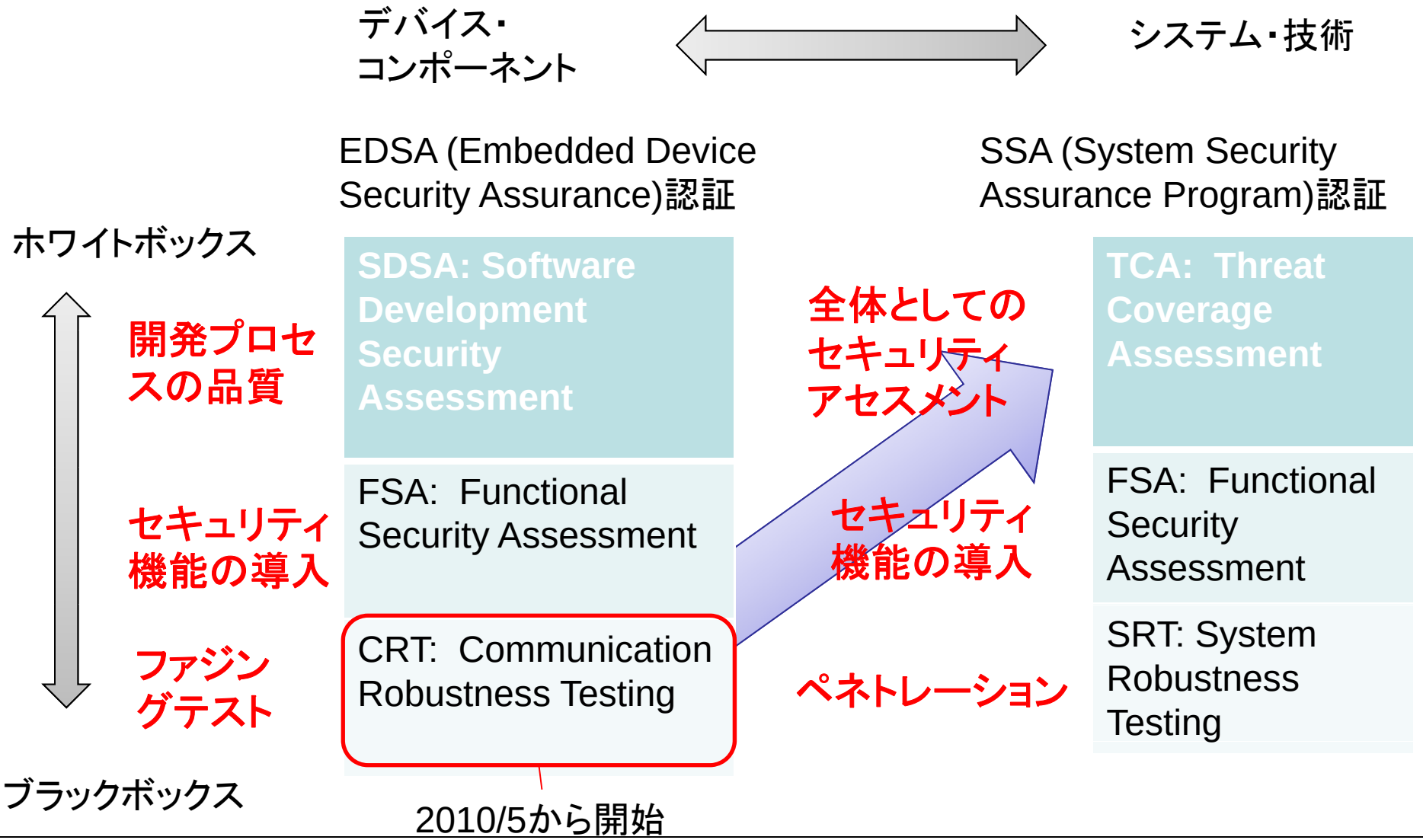
数社が機器調達時に認定製品を求めることを表明

機器ベンダー/メーカーはコストを掛けて認証制度に対応する必要が



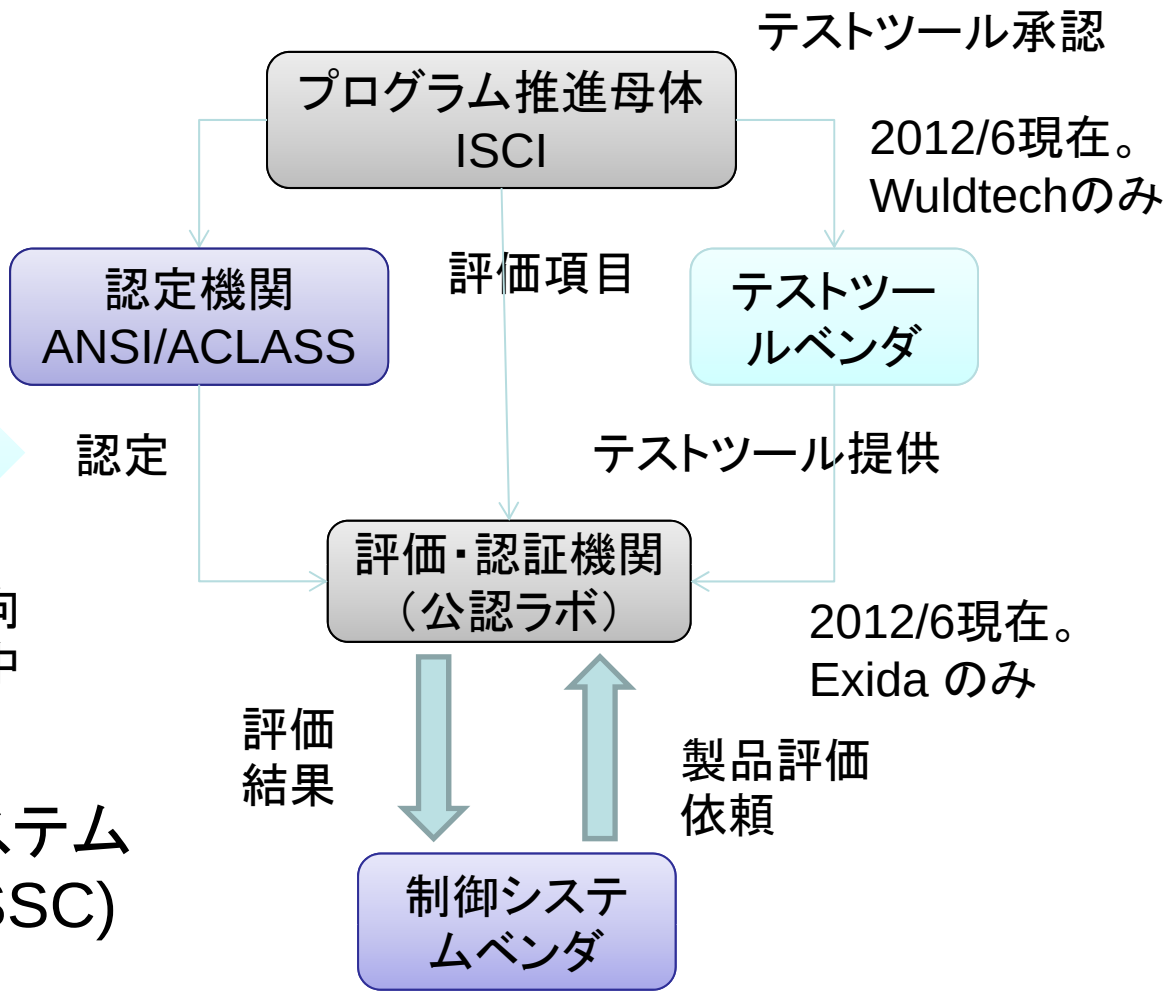
組込み機器セキュリティ認証認定製品

制御システムに対する評価認証制度(ISASecure/IEC62443)



ISA Secure 認証プログラム

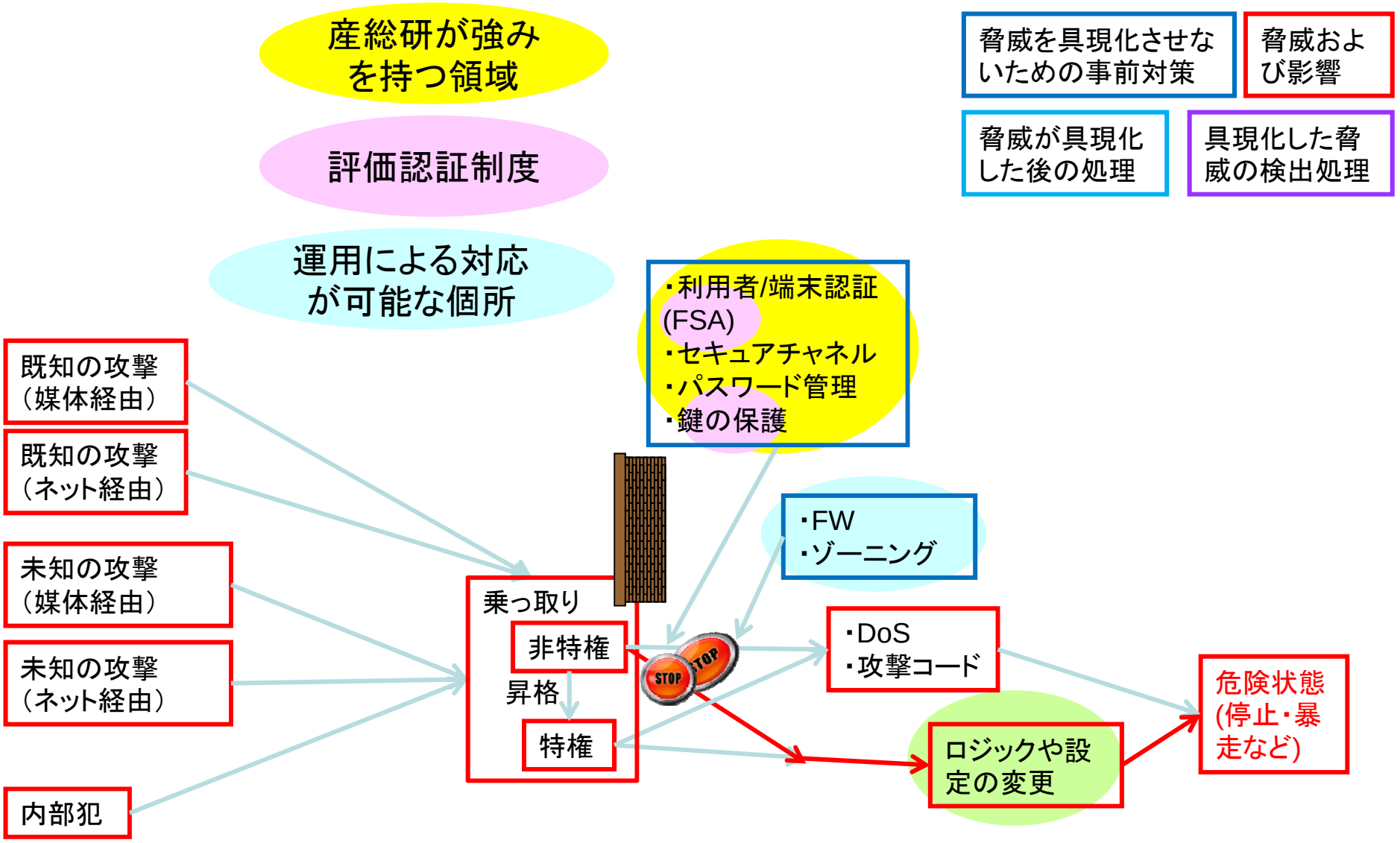
連携に向け調整中



技術研究組合：制御システムセキュリティセンター(CSSC)が2012年3月に設立

ACLASS：ANSI-ASQ National Accreditation Board

制御システムにおける脅威と対応策の関係

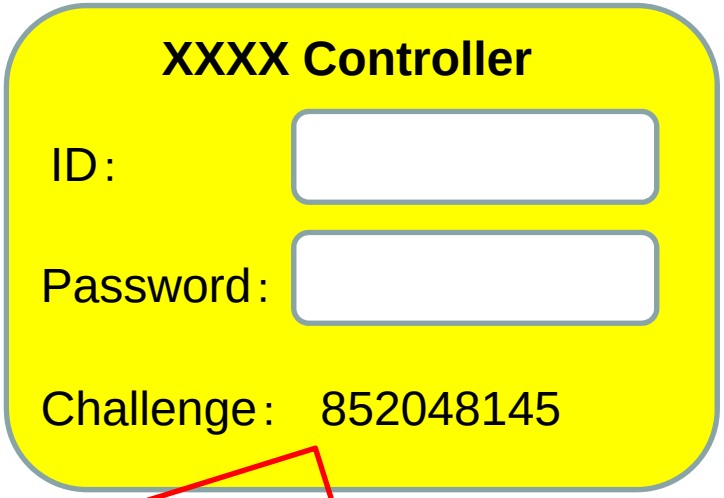


利用者/端末認証

- 運用で対処する場合
  - 機能や運用面に問題が無いことを確認
- 問題のある例
  - 運用面
    - デフォルトパスワード
    - 推測可能なパスワード
    - 共通パスワード
      - 弱いところからパスワードが抜かれ、それが悪用され他に侵入
  - 機能面
    - 平文でのパスワード送信
    - 迂回手段の提供

迂回手段の例

- 例１）



この値のハッシュ値が管理者パスワードとなっている（しかもID不要）

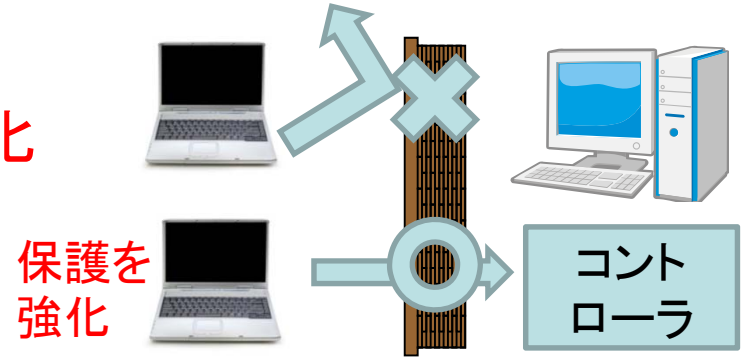
- 例２）
  - 一定回数パスワードを間違えると、
    - 正規の利用者がパスワードを忘れてしまったと判断して！？
  - パスワードを上書きできるようになる。

可用性超重視！？パスワードを忘れても困らないようにマニュアルで迂回方法が説明してある場合もある。

教訓

- 一見、対策が講じられているようでも、実は無効な場合もある
  - 対策の有効性については精査が必要

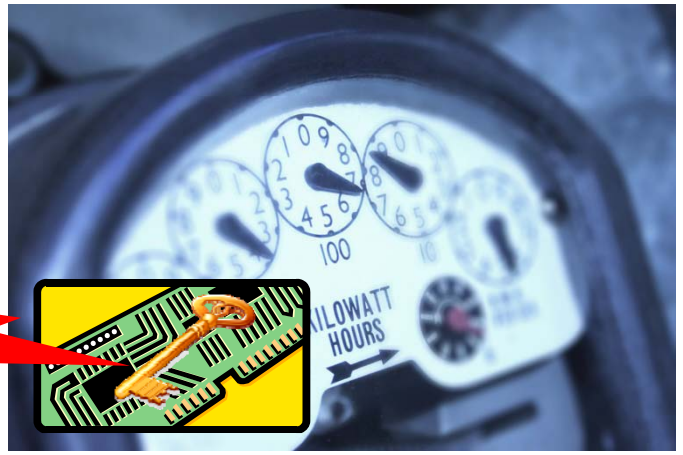
- 有効な利用者/端末認証機能が提供されていない場合
  - ファイアーウォール(FW)などで接続可能な端末を限定し、
  - その接続可能端末の保護を強化



物理的な保護区画外に設置される場合

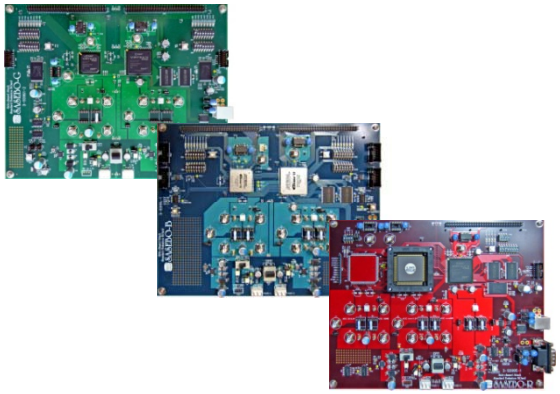
- 消費電力
- 漏えい電磁波
- などから鍵を推測する攻撃に十分な耐性を持つ必要がある

鍵の保護も重要



鍵の用途：
- 機器認証
- データの保護（暗号化、改ざん検出）

鍵の保護レベル評価ボード（対消費電力解析用）

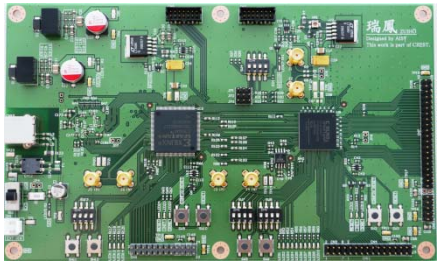


SASEBO-R/-G/-B/-GII
(discontinued)

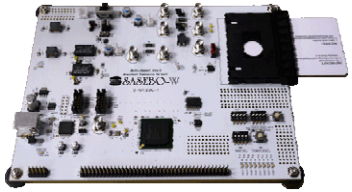
低消費電力環境版

SASEBO-GIII
(28-nm Kintex-7 FPGA)

廉価版

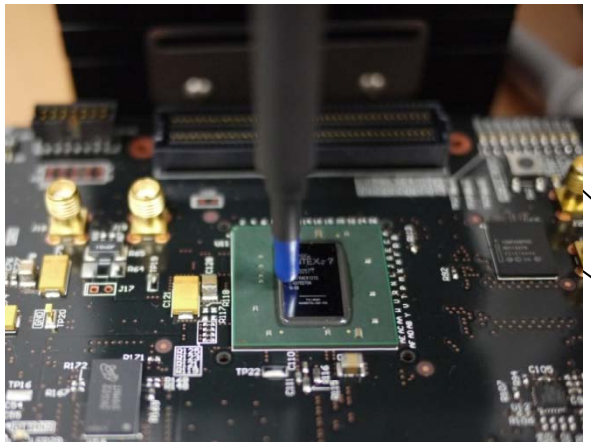


ZUIHO experimental board
for education and training.
(Spartan-3A FPGA)

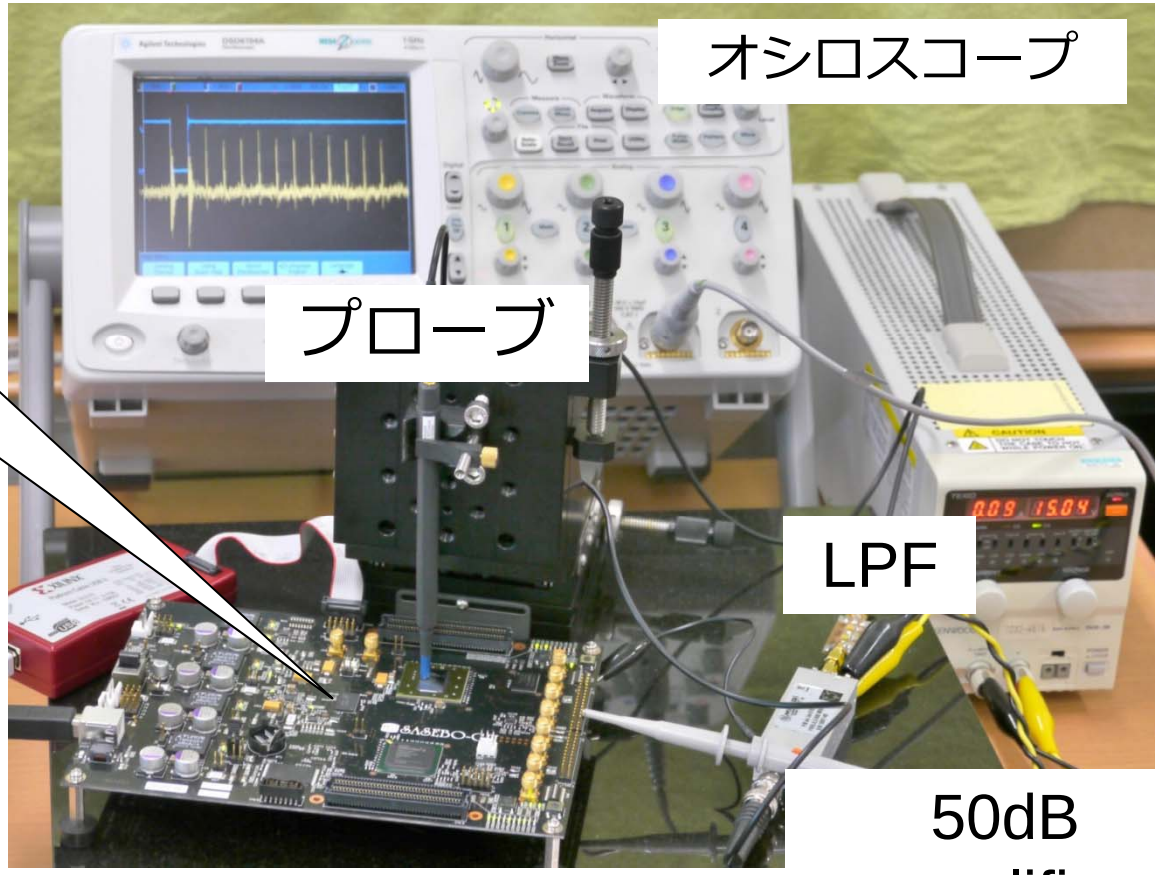


SASEBO-W for smartcards,
and daughter board for LSIs.

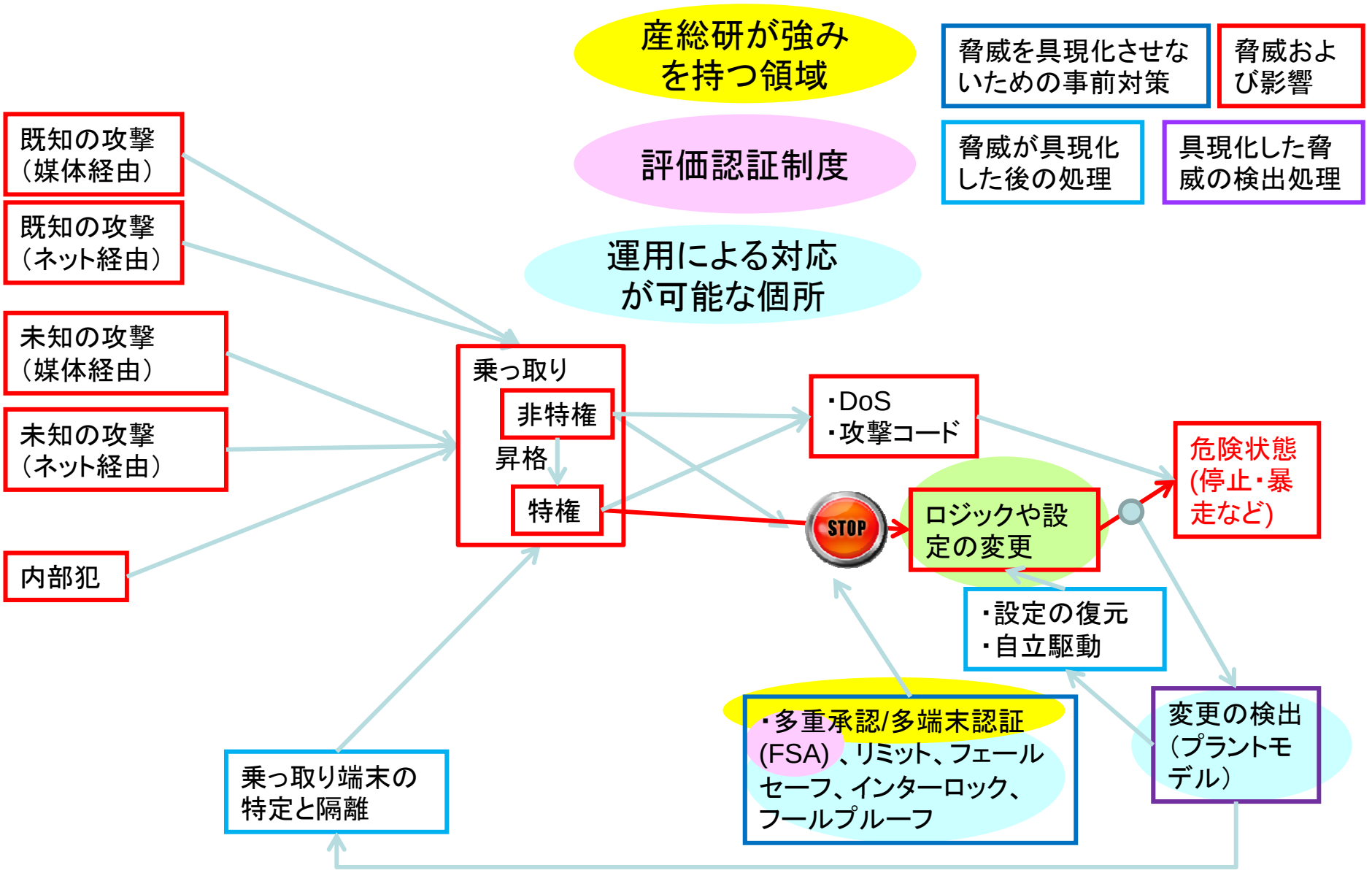
漏えい電磁波解析耐性計測環境



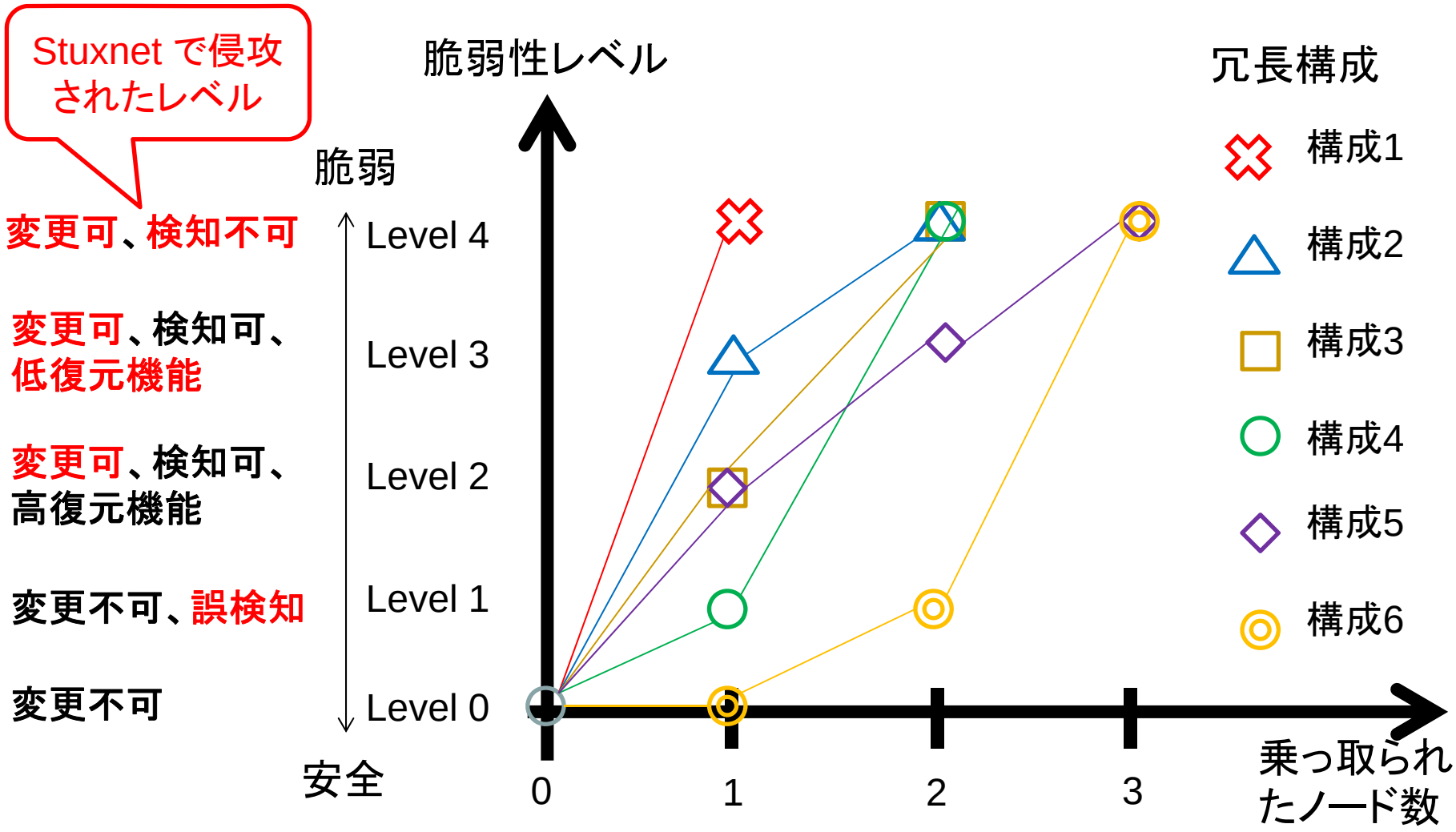
Kintex-7 without heat spreader is mounted.



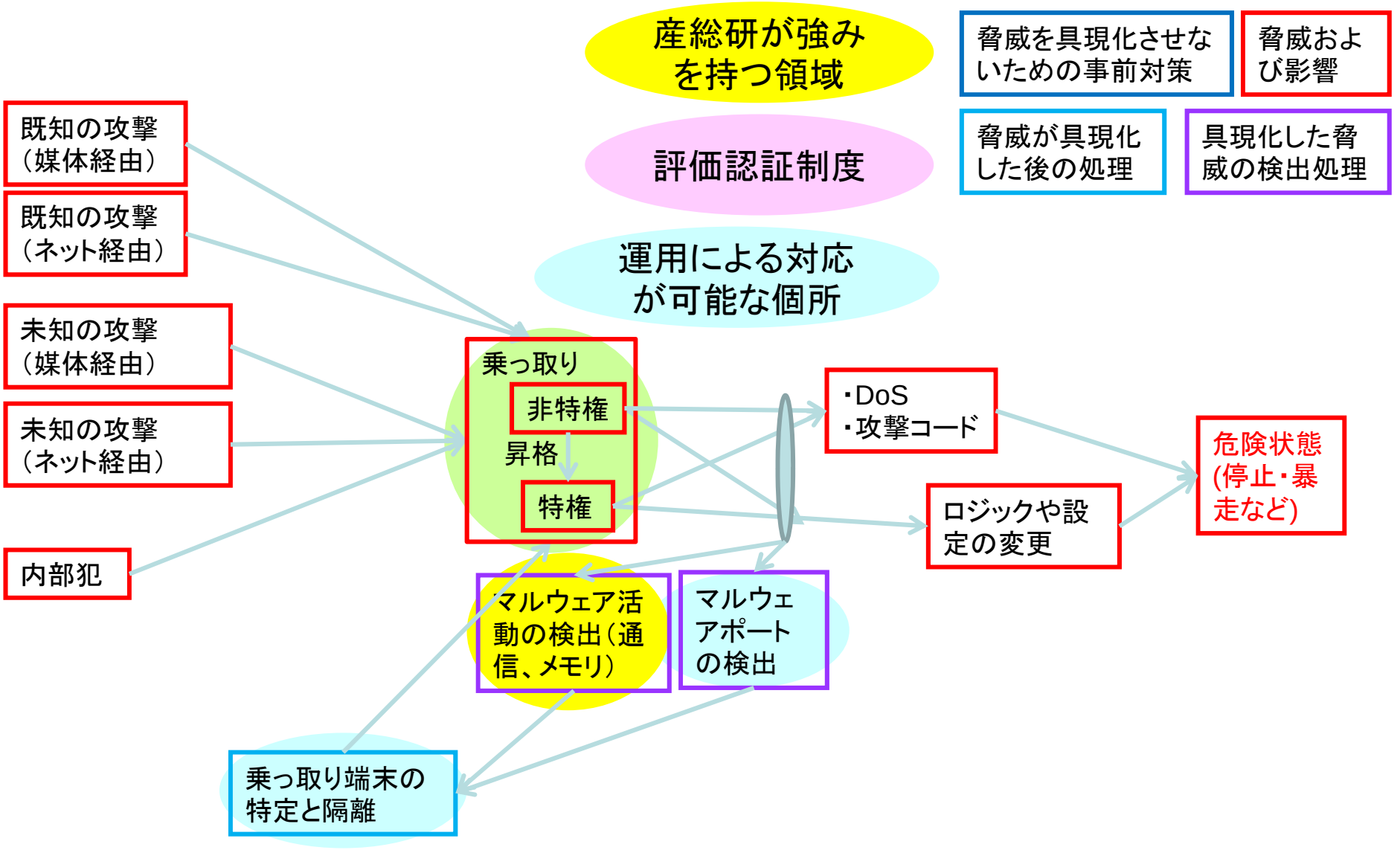
制御システムにおける脅威と対応策の関係



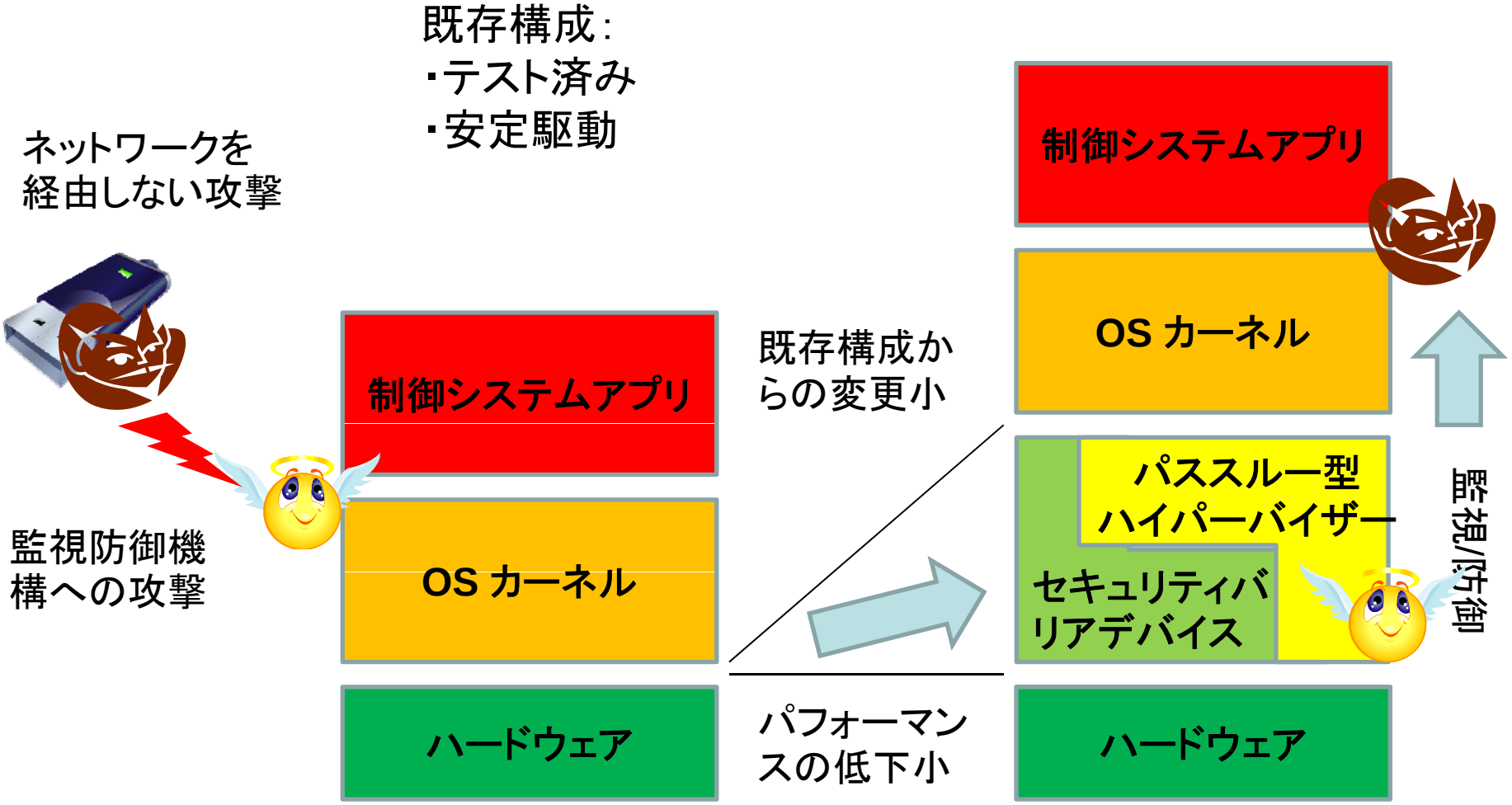
各冗長構成における乗っ取りノード数と脆弱性レベルの違い



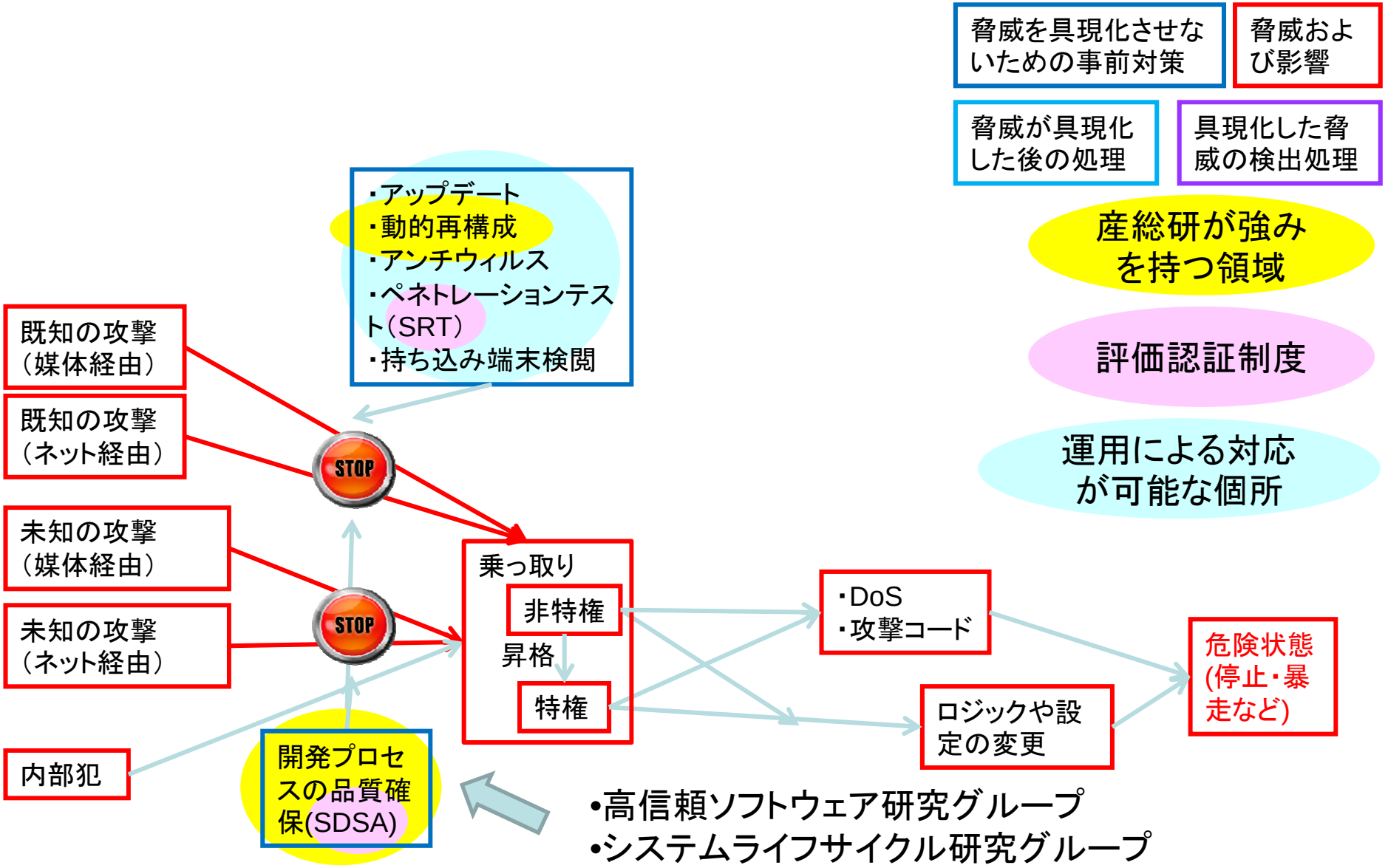
制御システムにおける脅威と対応策の関係



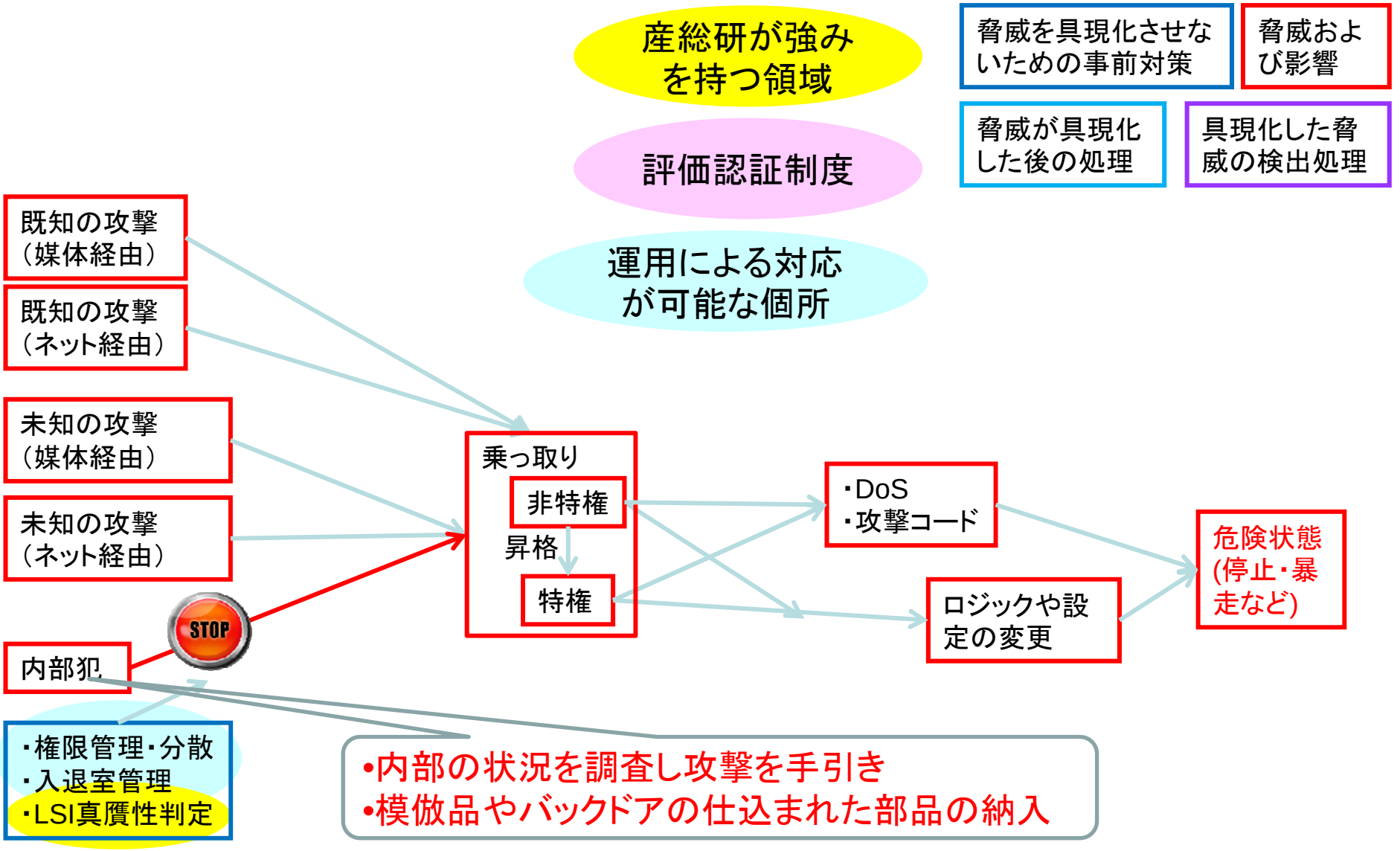
下位レイヤからのホストベースIDS/IPSに関する研究



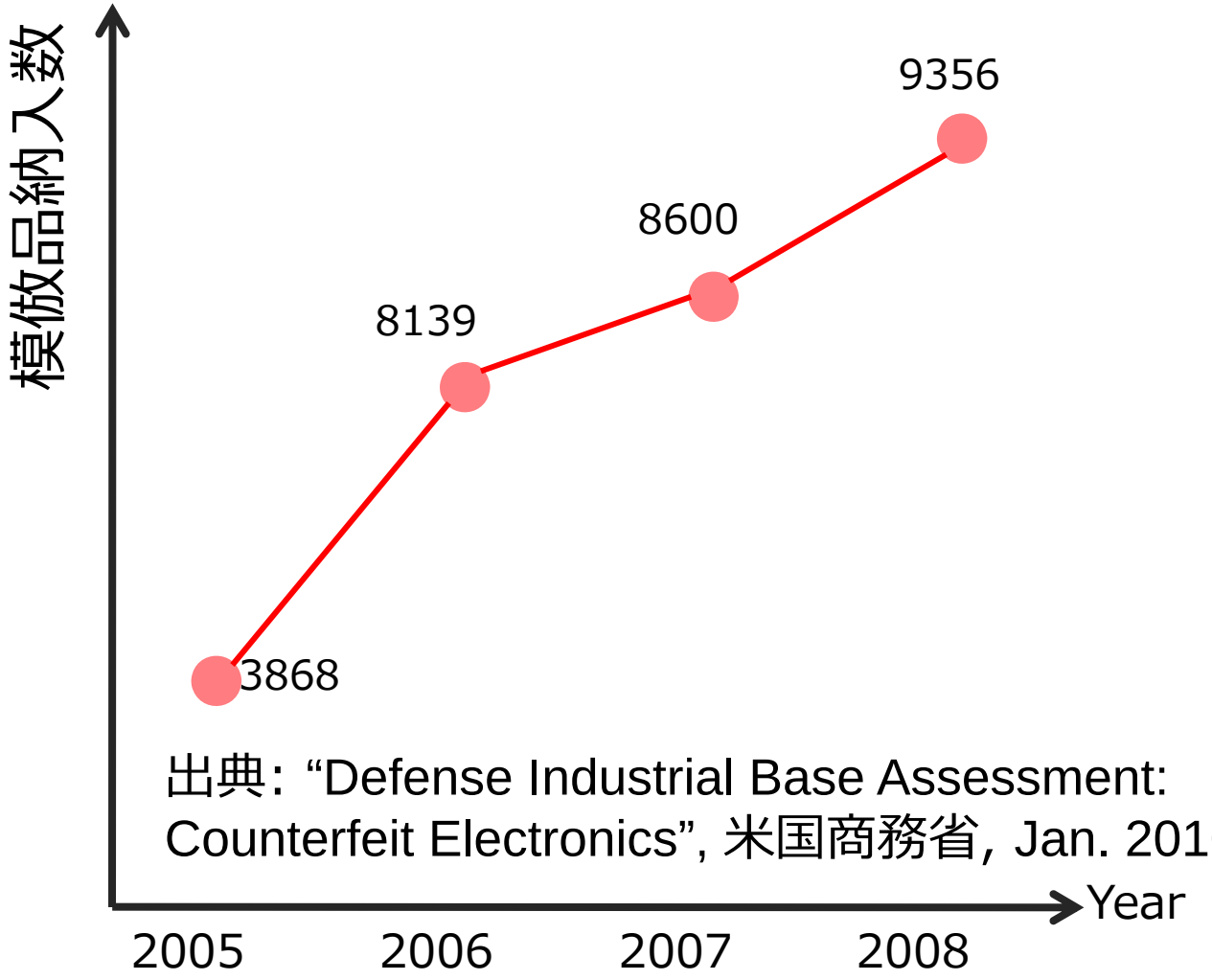
制御システムにおける脅威と対応策の関係



制御システムにおける脅威と対応策の関係



米国国防総省へ納入された模倣品の数

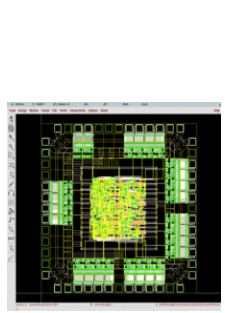


出典: “Defense Industrial Base Assessment: Counterfeit Electronics”, 米国商務省, Jan. 2010.

2012/5 大量の偽造電子部品が米軍機に利用されていることが判明（計1800件で、100万個以上の疑い）

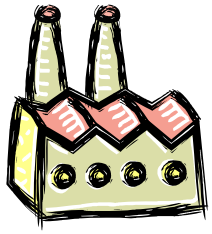
国防授権法（NDAA: National Defence Authorization Act）改正/強化の方向

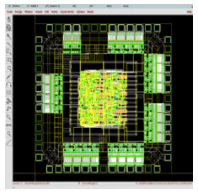
LSI 製造・流通のセキュリティ問題



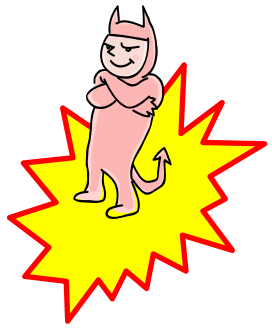
1.設計
データ

2.工場での製造組立

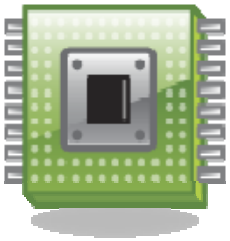




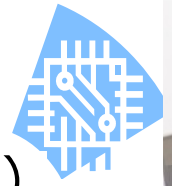
Trojan H/Wの混入

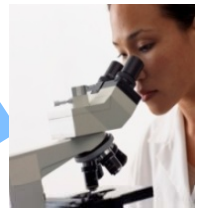


設計データ
流出



4. 納品

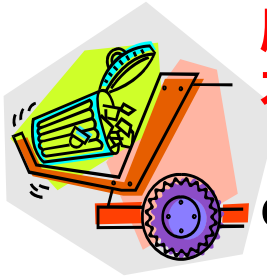




(Pass)

3. 品質検査

(Fail)



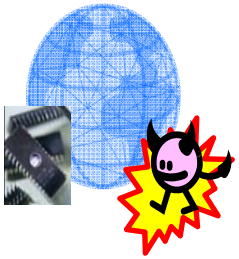
廃棄品の
不正流通

e-waste

窃取・
すり替え

余剰品販売

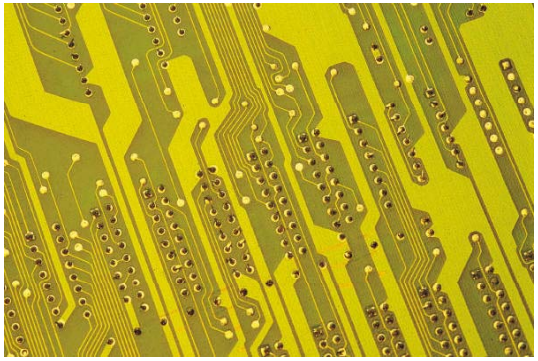
本物?

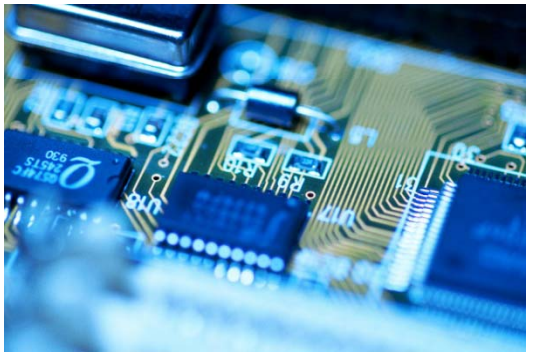


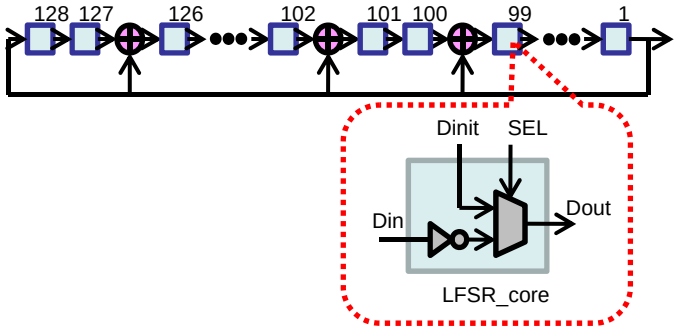
オンライン発注

製造時に制御できない物理的特徴の応用

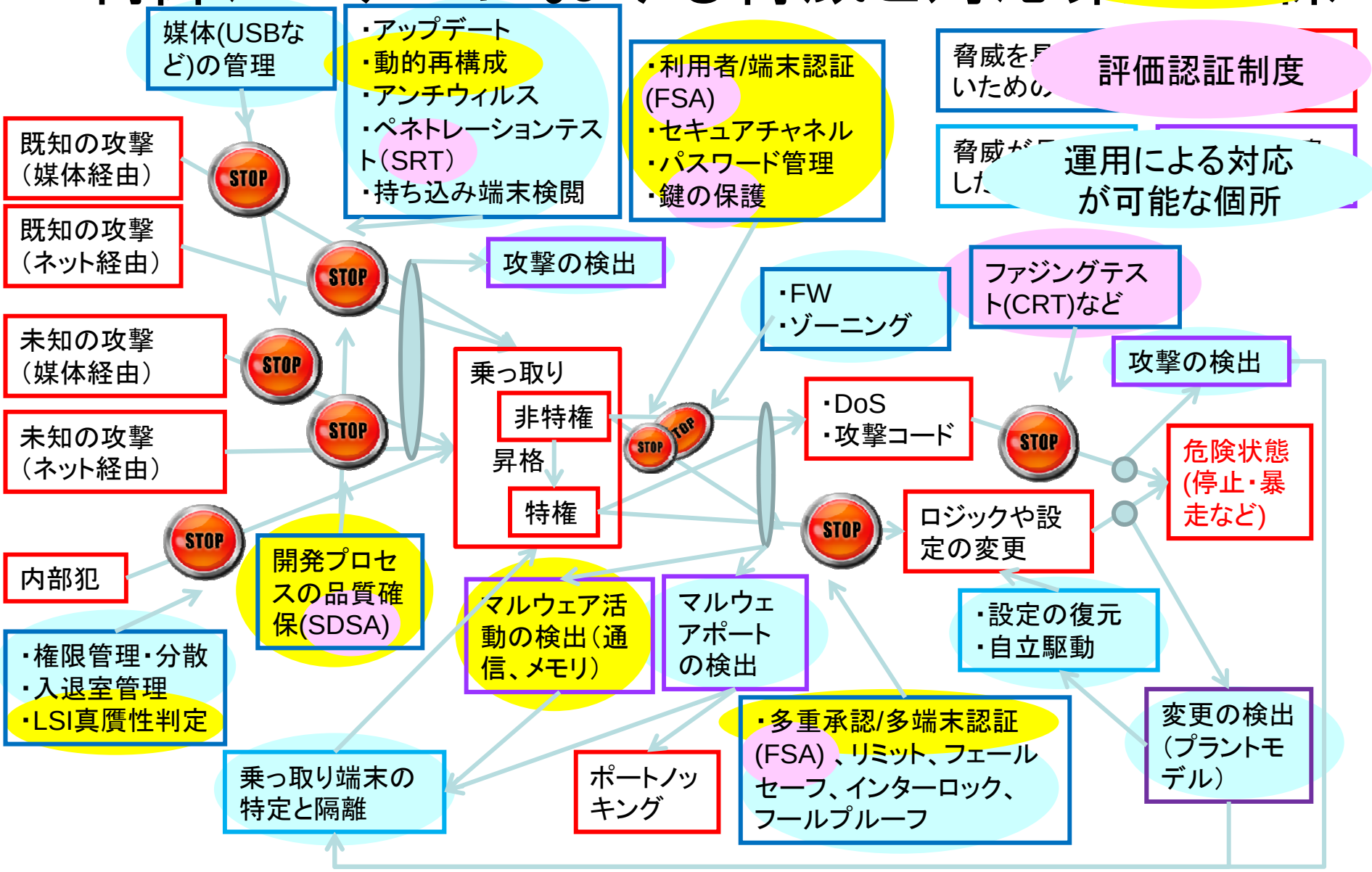
- 製造時に制御できない物理的特徴
  - Physical Unclonable Function (PUF)
  - 例：紙の繊維構造
- Silicon PUF: 半導体のばらつきを利用
  - ゲート長，閾値電圧，不純物濃度等
- RISECでの取り組み
  - PUFの特性の定量的評価手法の提案
  - 高効率で安全な PUFの提案
    - Pseudo-LFSR PUF







制御システムにおける脅威と対応



ご清聴ありがとうございました。

質問等ございましたら、
お気軽にご相談ください