制御システムセキュリティセンター　ISASecure SSA/SDLA/EDSA認証 説明会

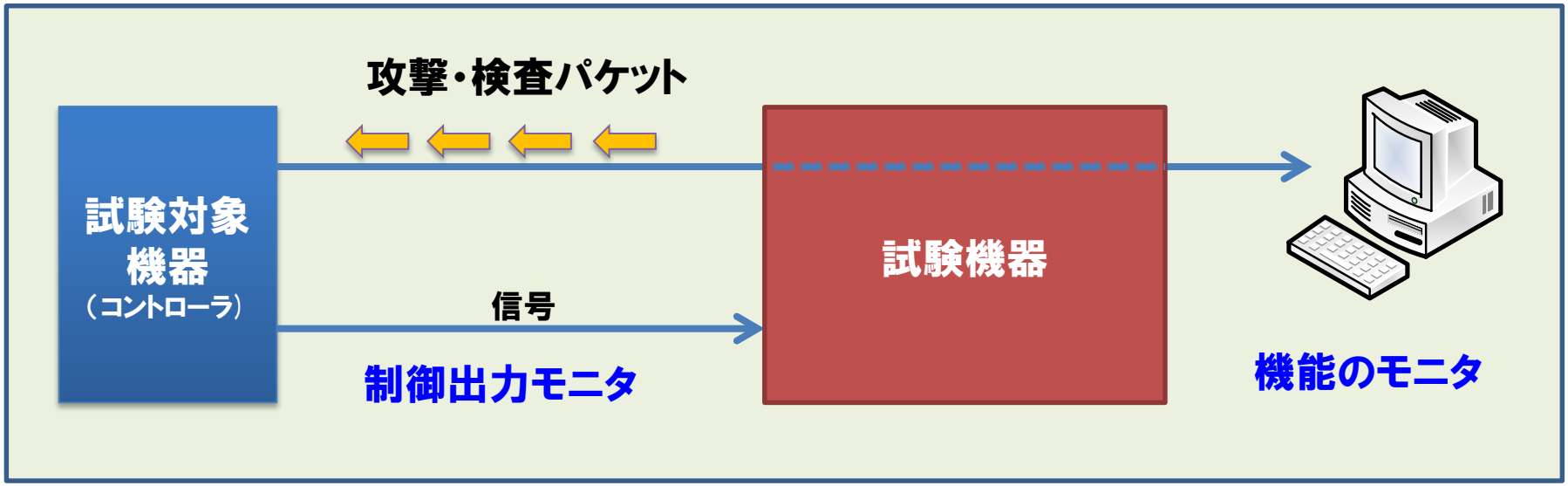
ISASecure EDSA 説明
「制御機器認証と拡張について」
EDSA2.0.0対応ERTについて

2015年5月14日（東京）、5月22日（大阪）
技術研究組合制御システムセキュリティセンター
研究員　市川　幸宏

目　次

1．ERT試験とは・・・ ERT試験の概要

- 制御セキュリティは、**可用性**＞完全性＞機密性　である
  （どんなことがあっても機能が維持されるべき）
- どんなこと？⇒膨大＆多様な**既知**攻撃を機器が受信しても
- 維持？⇒機器が提供する機能が**停止しない＆自動復旧**できる



第三者がモニタを通し客観的に機能が問題ないことを確認

1．ERT試験とは・・・ ERT試験の位置づけ

評価ではなく試験⇒申請者の仕様に基づき、第三者が事実を確認

EDSA 2.0.0

セキュリティ開発ライフサイクル
プロセス評価（SDLPA）
組込み機器
セキュリティ開発成果物（SDA-E）

組込み機器
機能セキュリティ評価
（FSA-E）

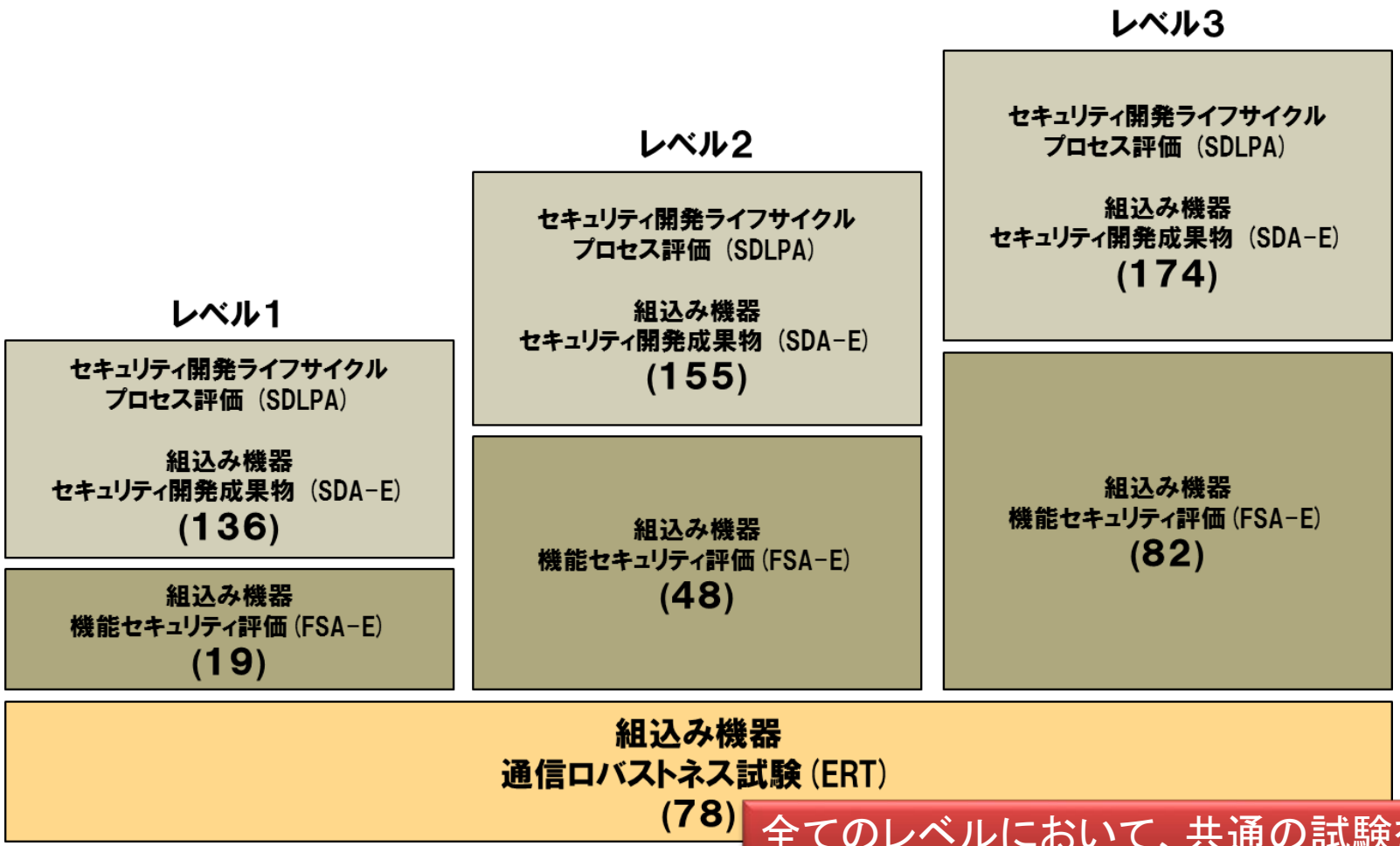
組込み機器
ロバストネス**試験**
（ERT）

⟶ **デバイスの堅牢性を試験**

EDSA：Embedded Device Security Assurance

SDLPA：Security Development Lifecycle Process Assessment，SDA-E：Security Development Artifacts for Embedded Devices，
FSA-E：Functional Security Assessment for Embedded Devices，ERT：Embedded Device Robustness Testing

1．ERT試験とは・・・ ISASecureレベルとERT試験



全てのレベルにおいて、共通の試験を実施

対象機器のすべてのインシデント（既知の課題）は当然対策すべき

1．ERT試験とは ・・・ 試験の目的と要件

■ **ERT試験の目的は、**組込み機器の堅牢性を**2つ**の試験で確認する。

1)**Communication Robustness Testing（EDSA-CRT）**

EDSA-CRTとは、IPベースの受信した異常又は意図的な悪意のトラフィックに対して,自分自身及び他のデバイス機能を防御する程度を測定することで、

デバイス内部の潜在的なセキュリティ脆弱性の存在を検査する。

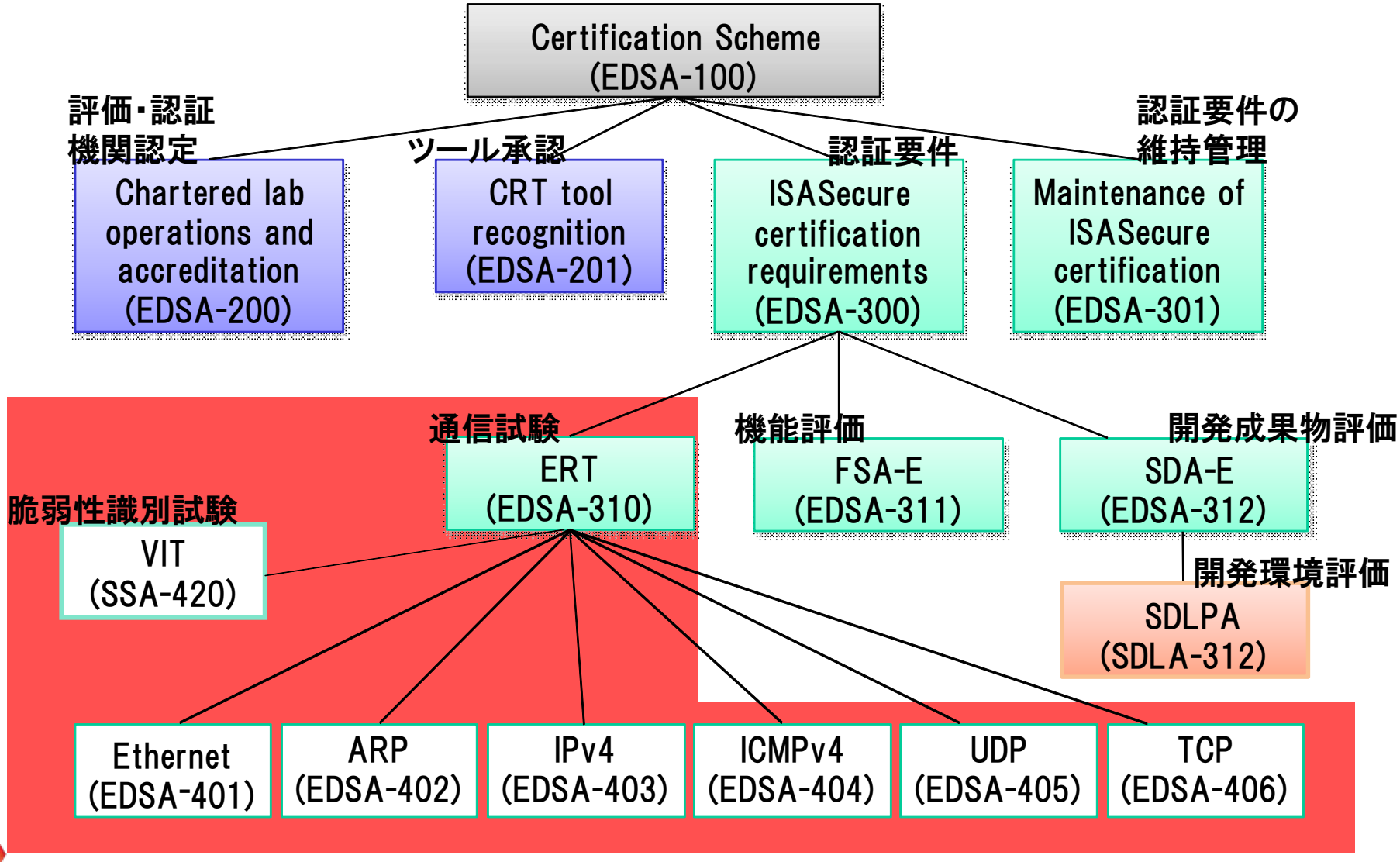
2)Vulnerability Identification Testing（VIT）

VITとは既知の脆弱性の存在を検査する。

■**ERT 要件**

- **EDSA-310(ERT)：IPベースのプロトコル実装用のEDSA-CRTとVIT共通要件**
- **SSA-420(VIT)：脆弱性スキャンツール(NESSUS)の設定要件**
- **EDSA-401～406(EDSA-CRT)：コアプロトコルに対する要件**

1. ERT試験とは ・・・ EDSA規格のドキュメント体系とERT要件



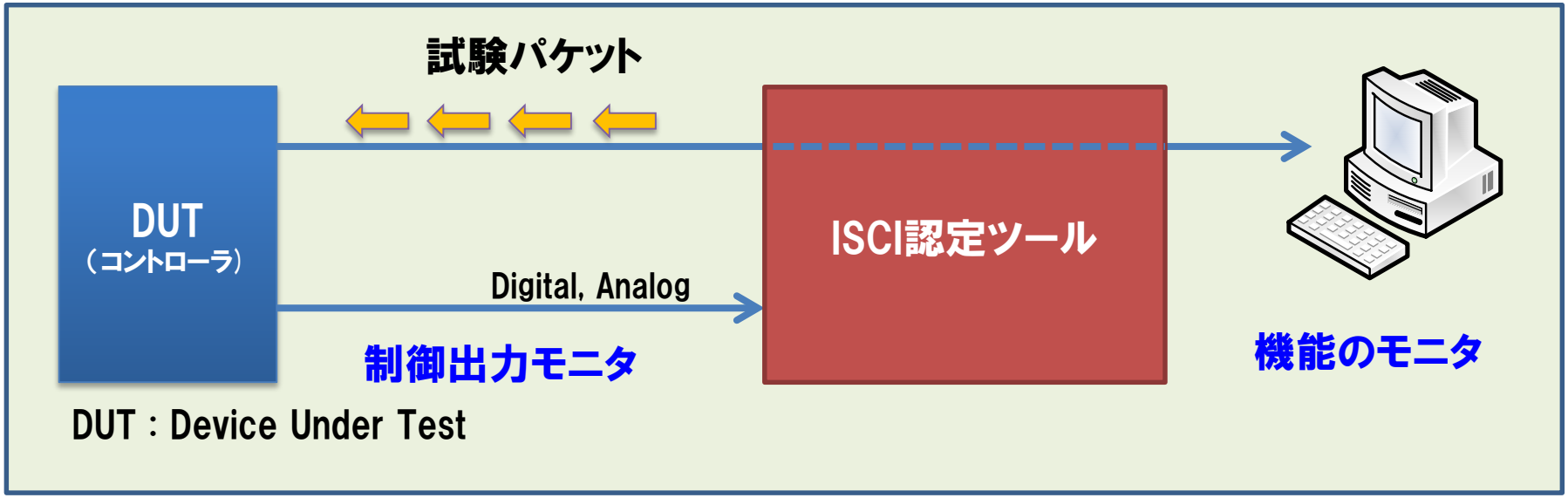
1．ERT試験とは ･･･ EDSA-CRTの試験対象プロトコル

- EDSA-CRTの試験対象プロトコルの要件は、EDSA 401～406で規定
  - EDSA 401 : IEEE 802.3(Ethernet)
  - EDSA 402 : ARP
  - EDSA 403 : IPv4
  - EDSA 404 : ICMPv4
  - EDSA 405 : UDP
  - EDSA 406 : TCP
- その他のプロトコルについては、EDSA-CRT試験の対象外
- （対象外のプロトコルはSDLA-SIT 要求事項で評価）

すべての通信試験の実施は前提で、第三者試験としてコアプロトコルのみを試験

2. ERT試験の内容 ・・・ EDSA-CRT試験機器構成

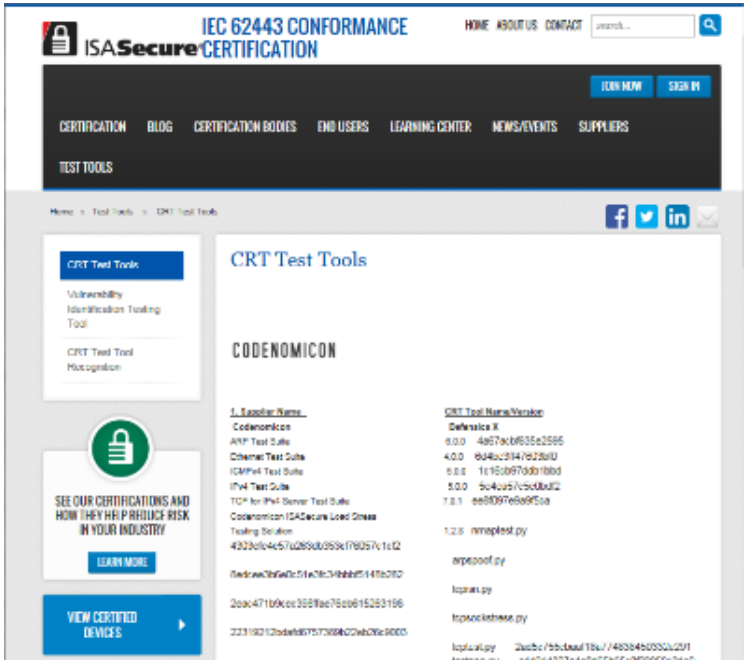
- ISCI認定ツールにより試験パケットをDUTに対して送信し、機能の維持を確認
- 6つの必須機能（機器の提供する機能）の維持が合否判定基準
  ⇒DUTだけではなく、事実上HMI側の用意も必要
- DUTは、エンドユーザ文書で推奨されている最大の負荷下で試験を実施する



図：CRT試験環境のイメージ

2. ERT試験の内容 ･･･ EDSA-CRTの3つのISCI認定ツール

EDSA-CRT試験利用できるのは、ISCI 認定ツールのみである。



ISASecure : Recognized Test Platforms for CRT
http://www.isasecure.org/Test-Tools/CRT-Test-Tools

- **Wurldtech社**
  http://www.wurldtech.com/
- **Codenomicon社**
  http://www.codenomicon.com/
- **FFRI.Inc社 http://www.ffri.jp/**

2. ERT試験の内容・・・ERT試験の 6つの必須機能

■ 6つの必須機能(停止すると困る機能)

次の機能を用いた機能が適切に維持されていることを確認する。6つの内、1つの機能でもあれば、ERT試験できる。

① 制御機能
- 規定の信号を出力する機能

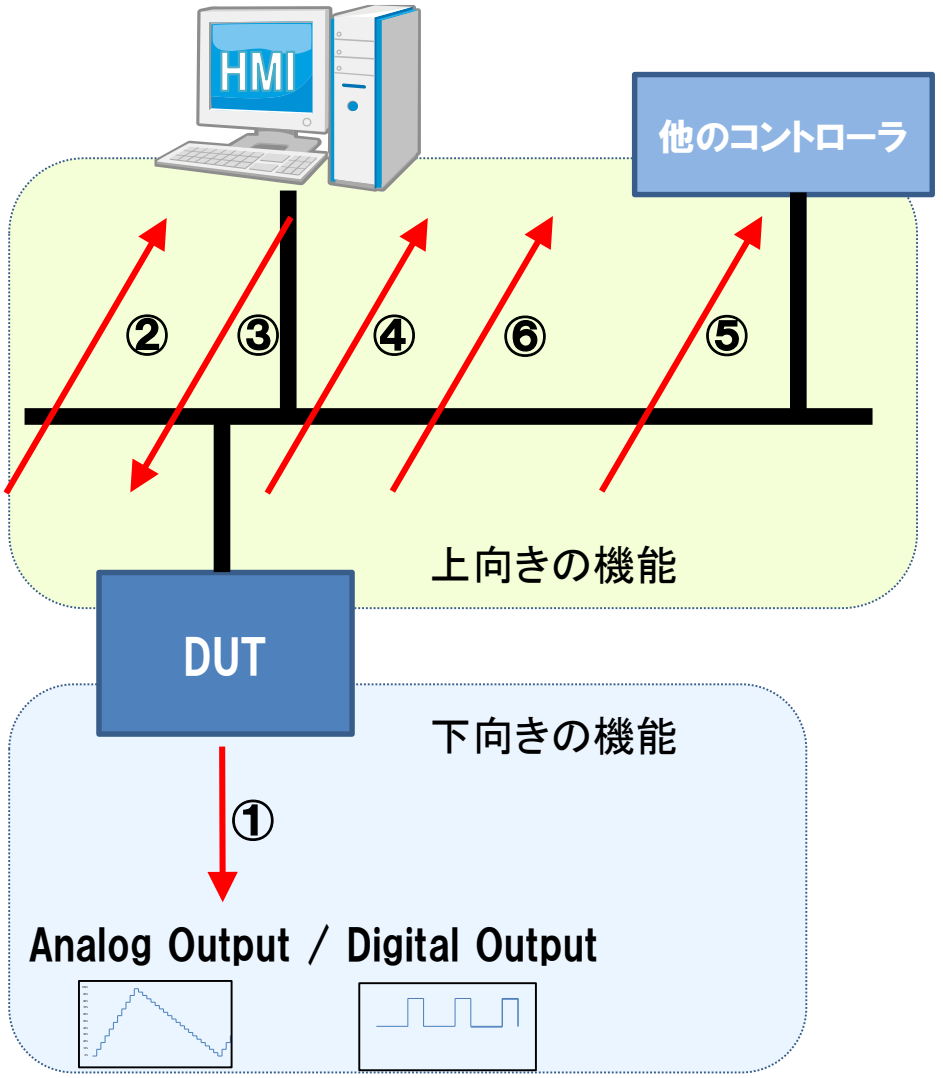
② プロセスのビュー
- プロセスビューを適切なタイミングで提供する機能

③ プロセスコマンド
- 上位システムからの命令に適切なタイミングで応答する機能

④ プロセスアラーム
- プロセスアラームを適切なタイミングで送信する機能

⑤ ピアツーピア制御通信
- ピアツーピア制御通信を送信する機能
- 適用除外可能

⑥ 必須履歴データ
- 必須履歴データを適切なタイミングで送信する機能
  例:製薬事業におけるFDA対応
- 適用除外可能



2. ERT試験の内容 ・・・ ERT試験の6つの必須機能

■ 6つの必須機能

次の機能を用いた機能が適切に維持されていることを確認する

上向きの機能は、申請者が設計に基づき定義する

- 「機能」の具体的内容
- 「機能の維持」とはどのような状態なの、定量的に判別する方法

試験所と合意

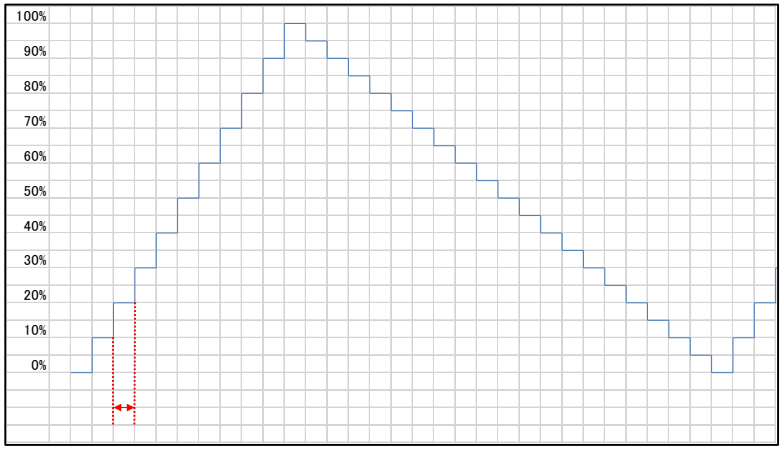
「上向きの必須機能を適切に維持する」の判定基準

2. ERT試験の内容 ・・・ 下向きの機能（制御ループ）の定義と維持

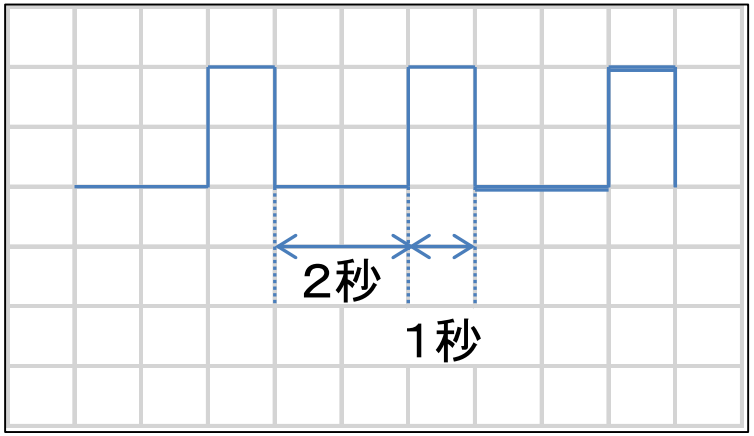
■下向きの必須機能の定義（存在すれば必須）

①制御機能（プロセス制御ループ、安全実装機能）

- 出力する信号は、EDSA-310に定義されている
- 下向きの機能は、常に維持されている必要がある



アナログ信号



デジタル信号

項目	値
制御ジッタ	1秒±100ms

試験対象のコントローラのスペックから定義

2. ERT試験の内容 ・・・ 上向きの必須機能の定義

■上向きの必須機能（②③④:存在すれば必須　⑤⑥：任意）

② プロセスのビュー
例：「プロセス制御・安全ループ」で出力しているデジタル信号・アナログ信号のトレンド表示・記録

③ プロセスコマンド
例：HMIからプロセスパラメータを一定周期で自動的に変更し、その結果がわかるログを記録

④ プロセスアラーム
例：：「プロセス制御・安全ループ」で出力しているアナログ信号出力にたいして、50%以上でアラームが発生するように設定。そのアラームを記録。

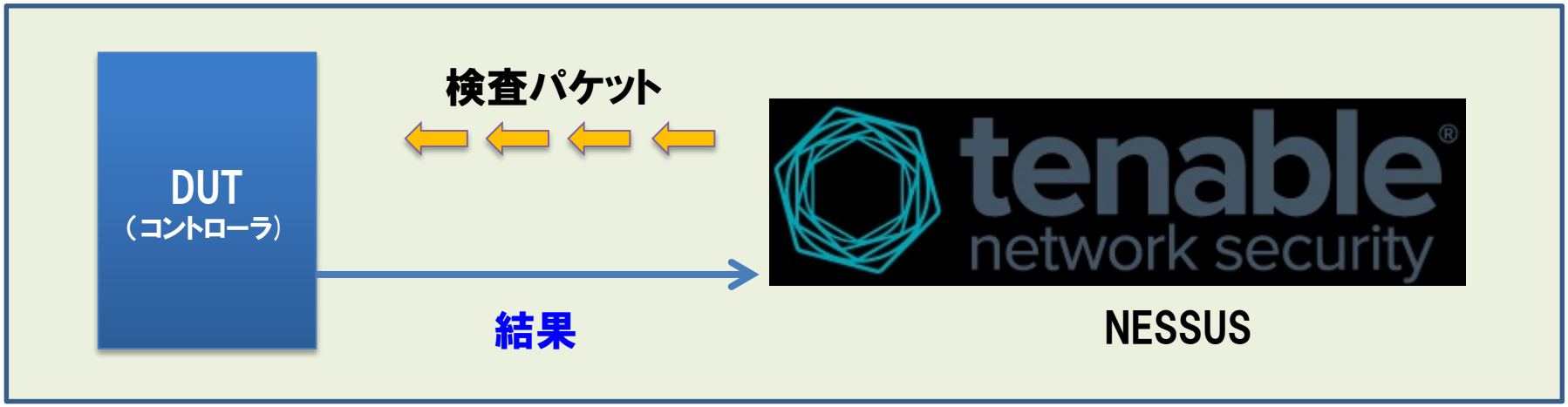
⑤ ピアツーピア制御通信
例：一定周期で、他のコントローラ間に対して制御通信（コマンド送信）が発生するようにし、その結果がわかるログを記録

⑥ 必須履歴データ
例：一定周期でプロセスパラメータ変更操作をおこない、その操作履歴が発生するようにし、ログに記録

- **フラッディングによる干渉が原因で機能が失われることは許容される**
- **ただし、仕様（タイミング等）にもとづき復帰する必要がある。**

2. ERT試験の内容 ・・・ VIT試験機器構成

- NESSUSにより検査パケットをDUTに対して送信し、既知の脆弱性を検査する。合わせて6つの必須機能の維持を確認
- 検査結果に従いVIT試験合格を以下とする。
  - 1つでもCritical or Highリスクが発見された場合⇒不合格
  - Mediumリスクが発見された場合⇒脆弱性の緩和を実現すること
  - Lowリスクが発見された場合⇒FSA-Eの要求事項に従い分析して、要求事項を満たすことを示す



図：VIT試験環境のイメージ

2. ERT試験の内容 ・・・ 試験の流れ

評価機器情報シート

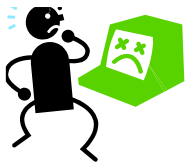
準備・計画

- ERT試験の実施に必要な環境準備
- 実施プランの作成

試験実施計画書

実施

- 試験機器を用いて、試験の実施
  - 試験環境セットアップ
  - EDSA-CRT
  - VIT



試験結果

レポート

- 試験結果のまとめ

ERT試験報告書

2. ERT試験の内容 ・・・ 試験環境

●試験の実施場所
- –CSSC東北多賀城本部

<u>試験対象機器を持ち込んで試験</u>

●試験可能機器
- –10/100/1000Base-T I/F
- –電源 100V/50Hz

条件は変更される可能性があります。最新の条件は、お問い合わせください。

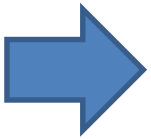
3. ERT試験の準備 ・・・ ERT試験実施に向けて

① 「DUT」の定義
② 通信条件の仕様整理
  – アクセス可能なネットワークインタフェース
  – 通常のトラフィック
  – 防御機能と回復条件
③ 上向きの必須機能の定義
④ 6つの必須機能の実現と監視基準の定義

3. ERT試験の準備 ・・・ ERT試験実施に向けて

①「DUT」の定義

- ●認定の対象とする「DUT」の範囲を定義する
  - –１つの製品として定義可能であること
  - –物理的に単体であることは必須ではない。
    （外付けFirewall等との組み合わせでも可）
- ●製品としてとりうる、CPU、ネットワークインタフェースの冗長構成を整理



どのインタフェースに対して、どういう状態で試験を実施するかが決まる

3. ERT試験の準備 ・・・ ERT試験実施に向けて

② 通信条件の仕様確認

●アクセス可能なネットワークインタフェース一覧の作成

i. ①で作成したそれぞれの構成に対して、インタフェース一覧を作成する

ii. その中から、対象となるインタフェース、対象外のインタフェースを決める
対象外となるインタフェースには、その除外理由を申請する必要がある
例:「メンテナンス用のインタフェースで、通常はロックされている」
「イーサネットインタフェースではない」

●通常のトラフィックの定義

どのような通信が行われても、必須機能が維持されるトラフィック量を仕様化
例:1Mbps 以下

●防御機能と回復条件

特定の条件下で防御機能が働く等により上向きの機能が一時的に停止または提供できなくなる場合、その機能と発動条件、および回復条件を定義。

3. ERT試験の準備 ・・・ ERT試験実施に向けて

③　上向きの必須機能の定義

④　6つの必須機能の実現と監視基準の定義

申請者は、製品の持つ機能のうち、なにが「必須機能」に該当し、「期待された動作」なのかを申請する必要がある。

まとめ　～ ERT 試験に当たって～

- ERT 試験環境の理解
- 「6つの必須機能」という概念の理解
- 受験にむけての準備のポイント
  - 「DUT」の定義
  - 通信条件の仕様整理
  - 上向きの必須機能の定義
  - 6つの必須機能の実現と監視基準の定義
- セキュアな製品設計と実装
  - 期待しない通信相手の存在を想定する（脅威の存在）
  - 境界でのパラメータのチェック
  - ネットワーク通信に対するファジング試験の導入
  - 既知の脆弱性に対する検知試験の導入

ご清聴ありがとうございました。

EDSA認証(EDSA-CRT試験)とAchilles認証

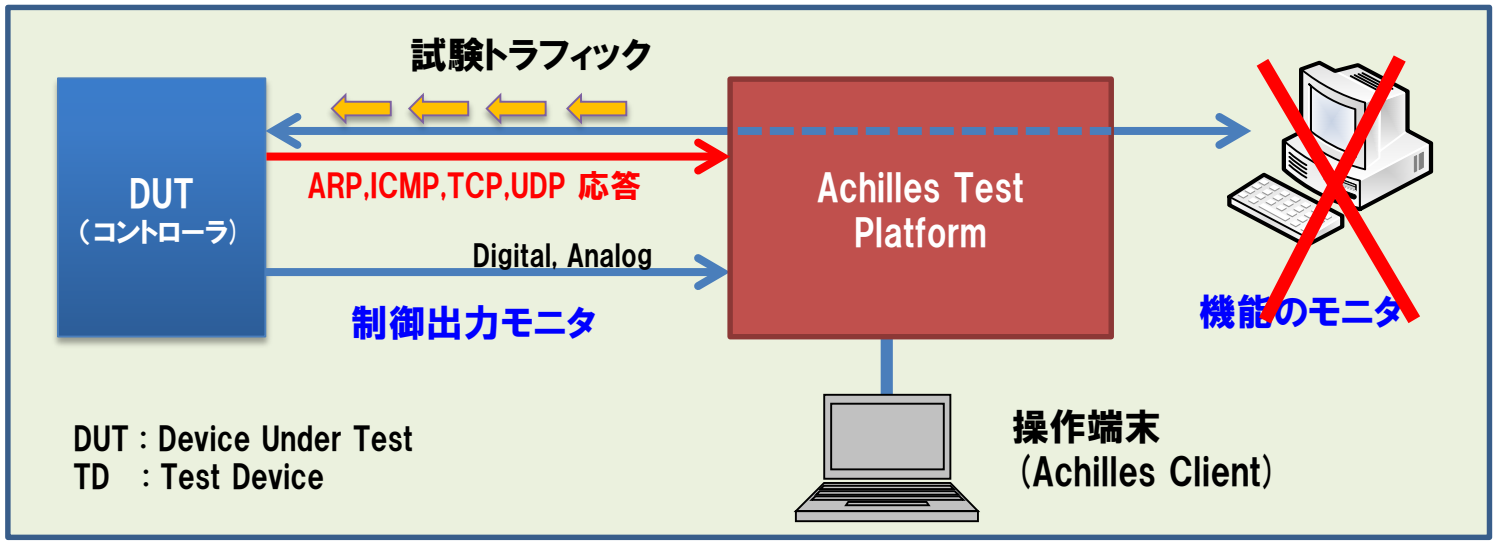
■ Wurldtech社 Achilles 認証（Achilles Communication Certification）との差異

●試験トラフィックの内容は、試験デバイスにAchilles Test Platformを利用した場合、Achilles Level 2とほぼ同一内容

●判定基準

A)制御出力モニタに関する判定基準は、ほぼ同一

B)Achilles 認証では、通信機能の維持が判定基準となっているが、EDSA認証では、機能の維持が判定基準となっている



図：Achilles認証試験環境のイメージ