vigilantplant.™

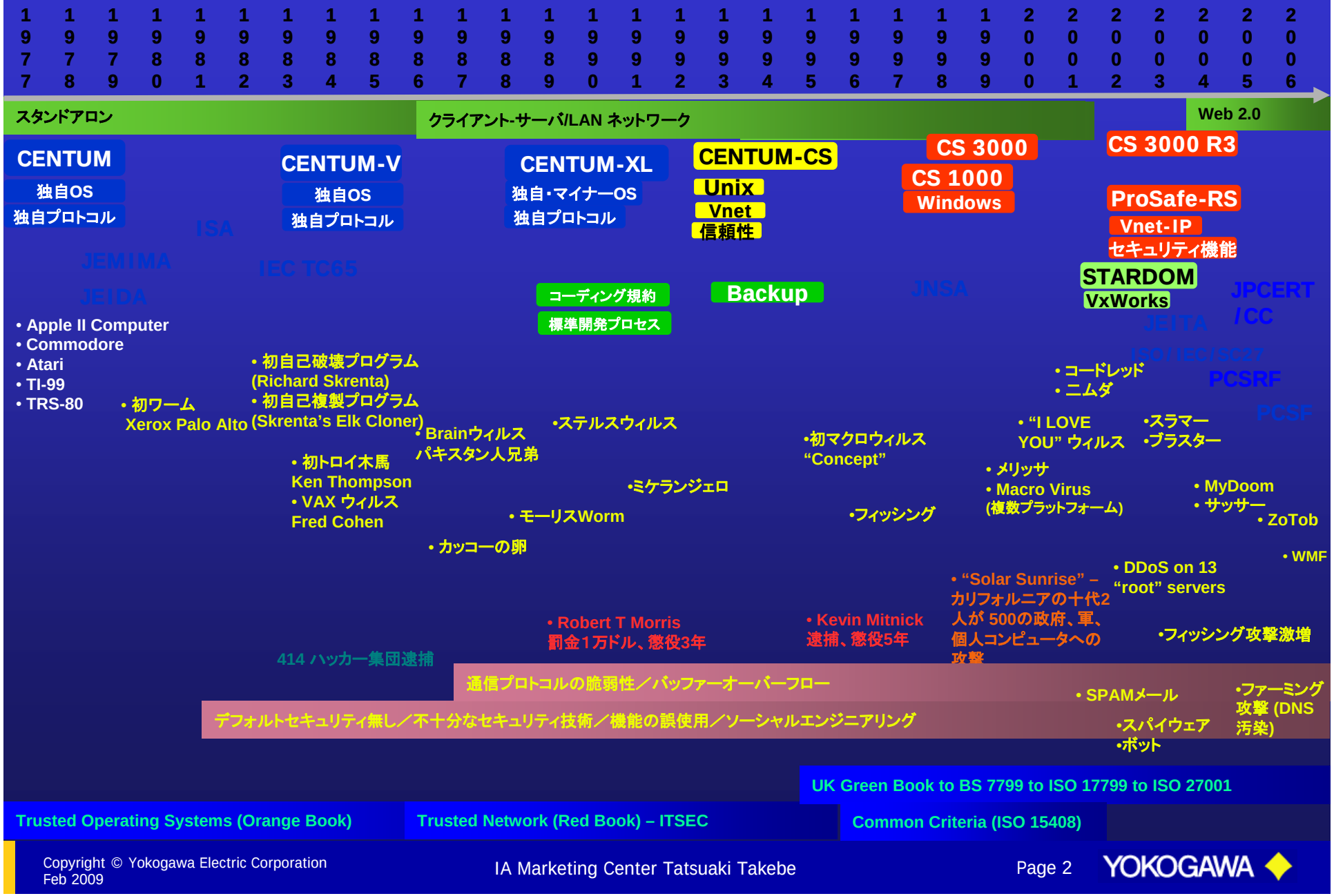
The clear path to operational excellence

制御システムに対するセキュリティ課題への取組みと展望

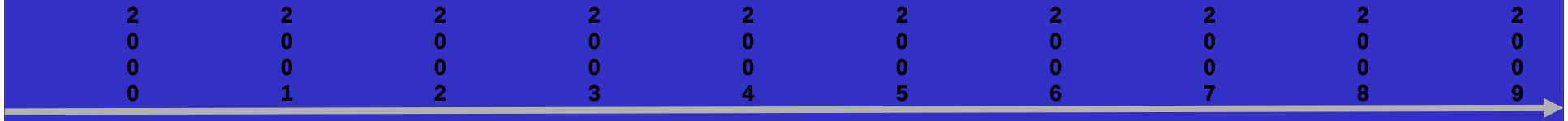
横河電機
IAマーケティングセンター
武部 達明

YOKOGAWA

横河の制御システムとセキュリティ 1



横河の制御システムとセキュリティ 2



CS 3000 R3
ProSafe-RS
Vnet-IP
セキュリティ機能

CENTUM-VP

NWScanner

Achilles
CS 3000

Achilles
STARDOM

CS 3000 R3
Achilles

IT事業部
FW、IDS、ISS

SecureTicket

SecureTicket Core
ISO/IEC 15408 EAL3+

AntiVirus

FireWall

Reverse Proxy

VPN

MSセキュリティ
パッチ

S95 NW
アーキテクチャ
モデル

要塞化

セキュアコーディング

WSUS

ISA(SP99)

PCSRF

JPCERT/CC

PCSF

ISCI

ISA Security
Compliance
Institute

JNSA

JEITA ITSC

ISO/IEC
JTC1/SC27 WG3

ISO27001、27002、27003、27004、27005、...

Common Criteria (ISO 15408)

YOKOGAWA

セキュリティ対策について

A Yokogawa Commitment to Industry vigilance®

- Backup/Recovery
- アンチウィルス
- FireWall
- セキュリティパッチ
- VPN
- Reverse Proxy
- ネットワークトポロジー
- ネットワーク脆弱性スキャン
- プロによるセキュリティテスト（Achilles→ISCI）
- セキュアコーディング
- 要塞化（LockDown）
- WSUS（Windows Server Update Services）
- セキュリティ Best Practice（BP）の 蓄積と展開
- 先進例の調査・研究、適用
  - ITセキュリティ、米国ICS・SCADAセキュリティ

PCSにとってセキュリティとは何か？

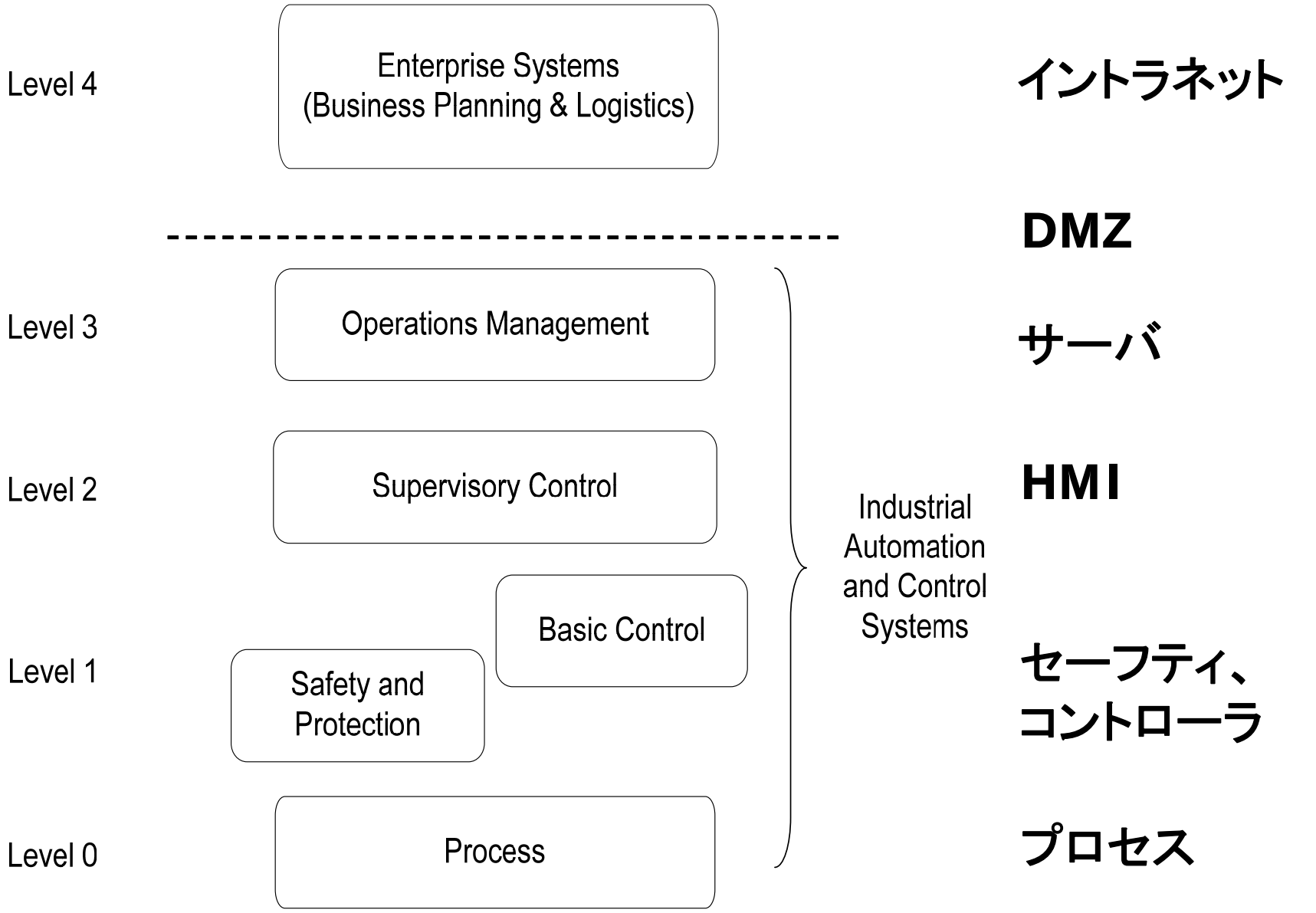
A Yokogawa Commitment to Industry vigilance®

- センサ、アクチュエータ、制御アルゴリズム、パラメータ、データ、アプリケーション、情報、通信、制御・監視・エンジニアリングステーション、同プラットフォームなど、制御に不可欠な要素に攻撃（悪影響）が及んでも、PCS全体で期待される動作が阻害されないよう護ること。
- すべての要素の役割が正しく連携されねばならない。
- どこに問題が発生しても、阻害要因になるため、すべての要素の動作の保証を求められる。

- 例外動作を定義し、対応できること。
- 品質保証問題と同じ。→きりがない対応が求められる。
- 対応の単位をうまく考える。
- ランクの高い問題から、対処していく。リスク対応。

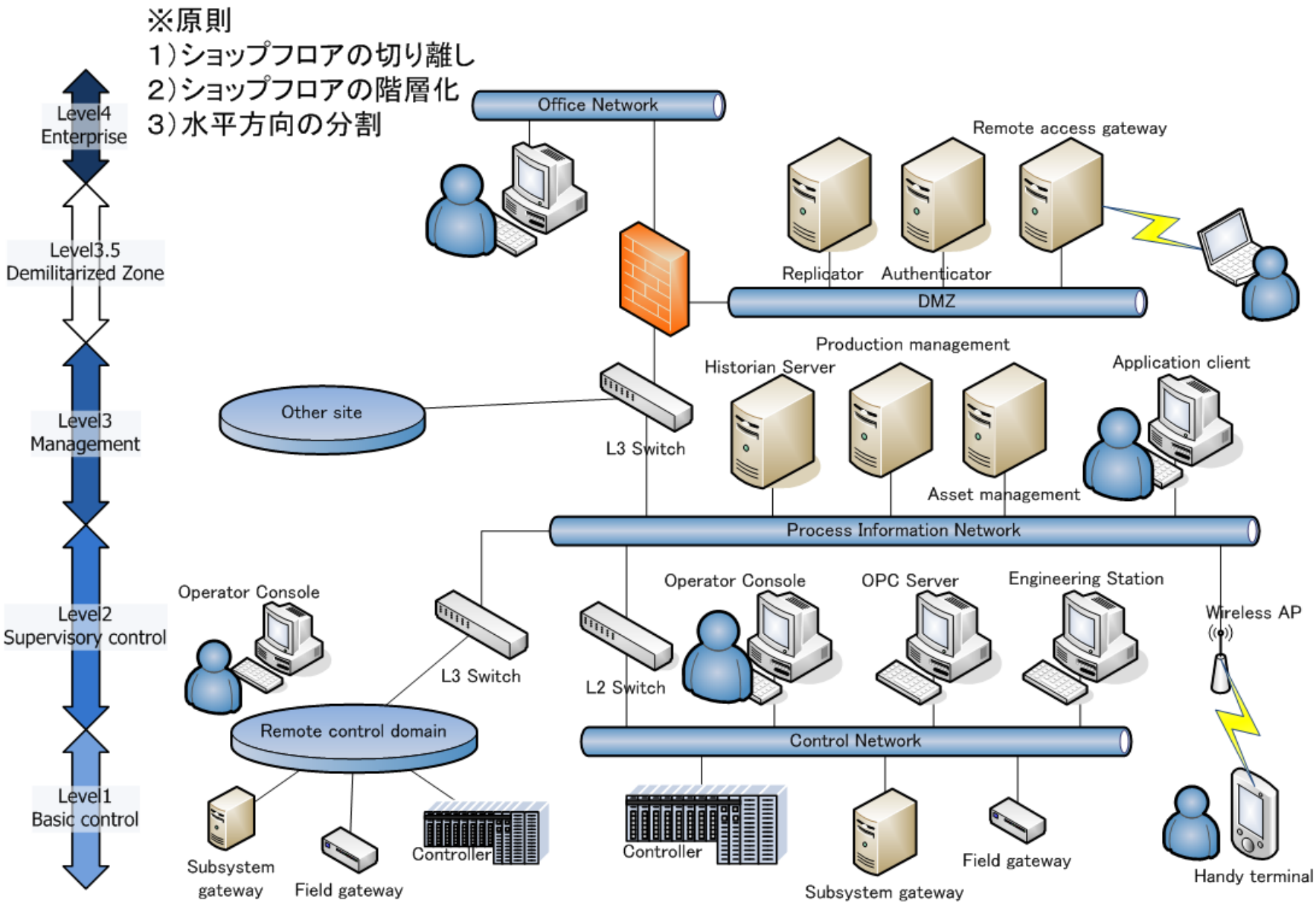
- 関係者が集まる場所での決定をよりどころにする。
- PCSと操作する人、規則、運用で対処すべき問題。
- ベンダが解決する問題、インテグレータが解決すべき問題、PCS所有者が解決すべき問題がある。
- リスクを評価して、合意を取り付け、予算を確保して、実践。

S95システム階層モデル ← S99 参照モデル



S95システム階層モデルを基にしたNWアーキテクチャ

A Yokogawa Commitment to Industry vigilance®

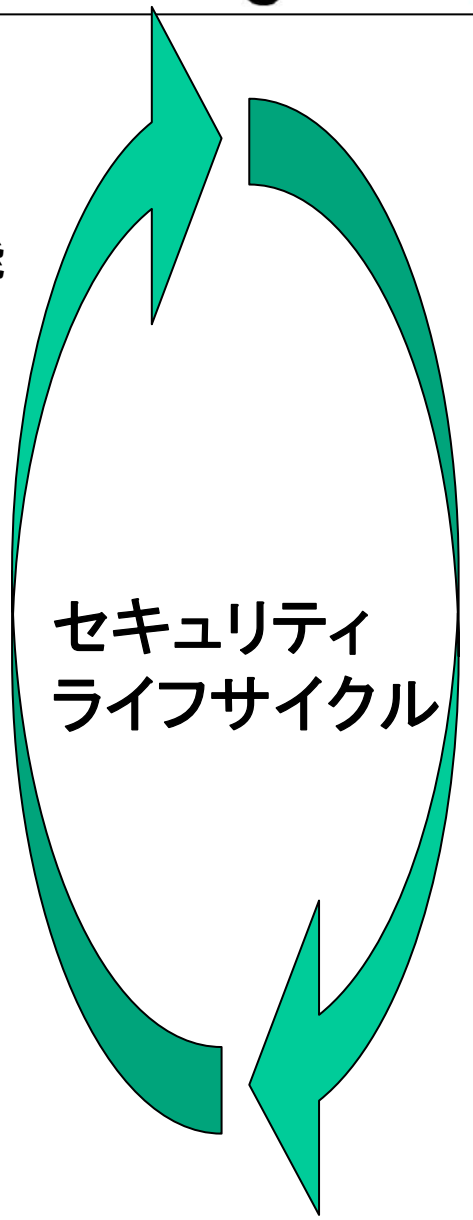


YOKOGAWA

セキュリティ確保のための努力

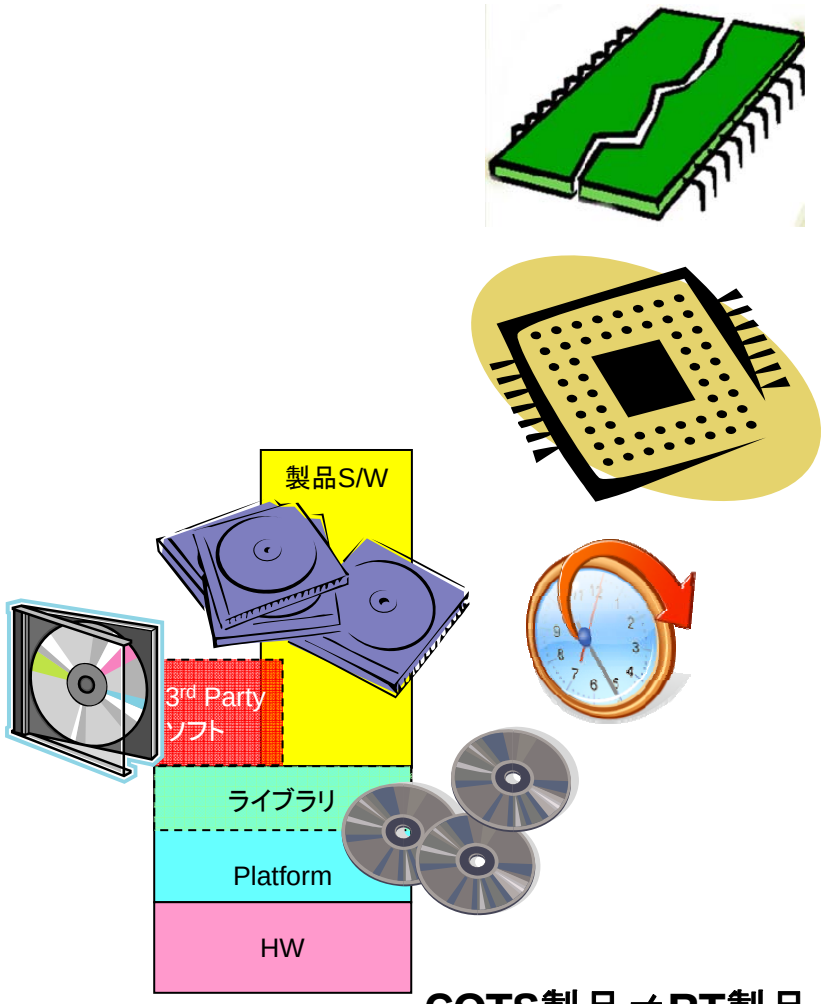
A Yokogawa Commitment to Industry vigilance®

- 単体製品でのセキュリティ
  - セキュリティリスク評価・対応
    - 認証、アクセス制御、ログ、バックアップ・リストア機能
    - ウィルス対策
    - 要塞化
  - セキュリティ評価
- インテグレーションでのセキュリティ
  - セキュリティリスク評価・対応
    - ネットワークアーキテクチャ
    - セキュリティエンジニアリング(FW、IDS etc)
  - セキュリティ評価
- 操業セキュリティ
  - バックアップ、セキュリティアップデート
  - イベント監視、インシデント対応
  - セキュリティ評価



3rd パーティソフトの問題

A Yokogawa Commitment to Industry vigilance®

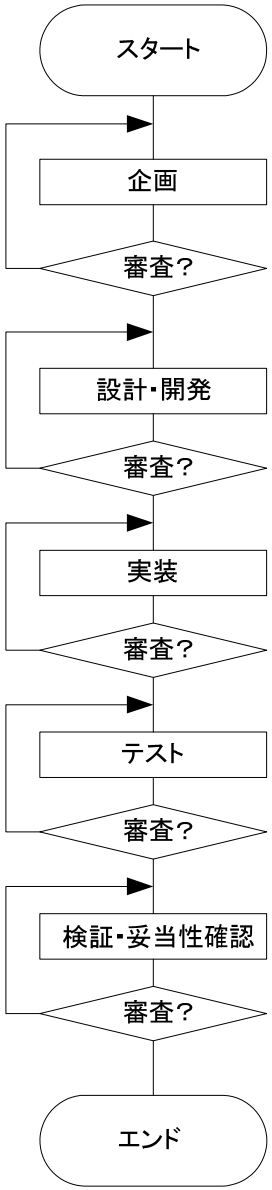


COTS製品≠RT製品

- 3rd パーティソフトは、メモリ、CPUパワー、CPU時間の消費量、品質を見極める必要がある。
- 3rd パーティソフトが、制御システムソフトと喧嘩しないことを確認する。
- 通常オペレーション＋念入りな異常ケース設計が、鍵。
- パッチ確認も同じ。

ある3rd Partyソフトの例：
自動的に配信される更新ソフトウェアのテストが不十分な場合があり、それらが自動更新された多くのユーザのパソコンが動作不良・起動不能になったり誤検出するなど、まるでウイルスに感染したかのようなトラブルが発生することがある。

設計・開発ライフサイクルでの考慮



企画時に脅威分析、リスク評価、悪用（攻撃）シナリオ。
どうやって守るか、対策（セキュリティ要件）。

要塞化

コードレビュー

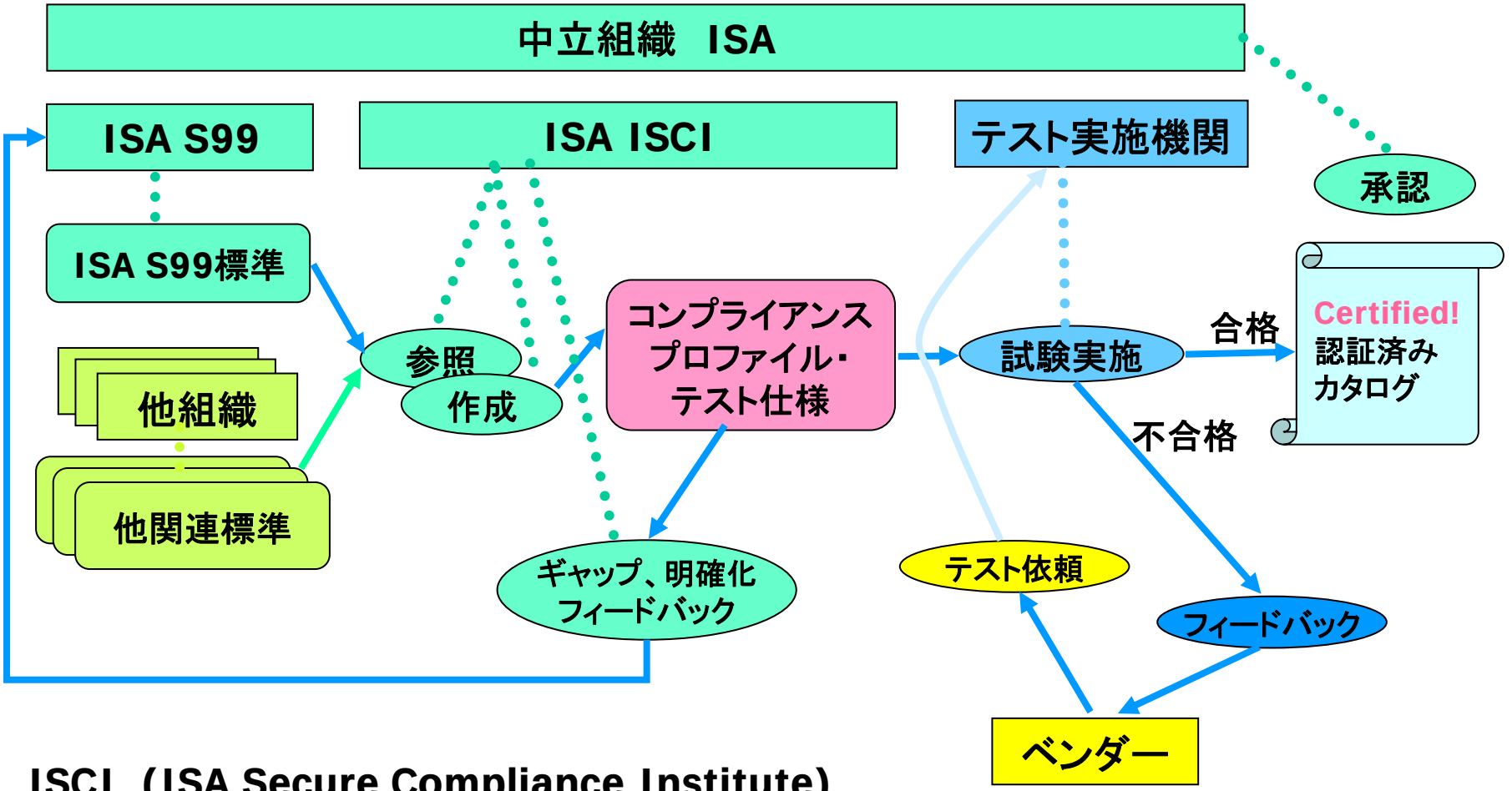
オープンポート検査

異常系テスト　ネットワークセキュリティテスト

セキュリティ評価

ISCI の 活動　プロファイル・テスト仕様作成と評価認証

A Yokogawa Commitment to Industry vigilance®



ISCI　(ISA Secure Compliance Institute)

IPボックス認証→システム認証→オペレーショナル認証（予定）

http://www.isa.org/isasecure/ISASecurityComplianceInstituteMembershipProspectusOctober2007.pdf

ISCIの目指すもの（現在、実際のテストはできていませんが）

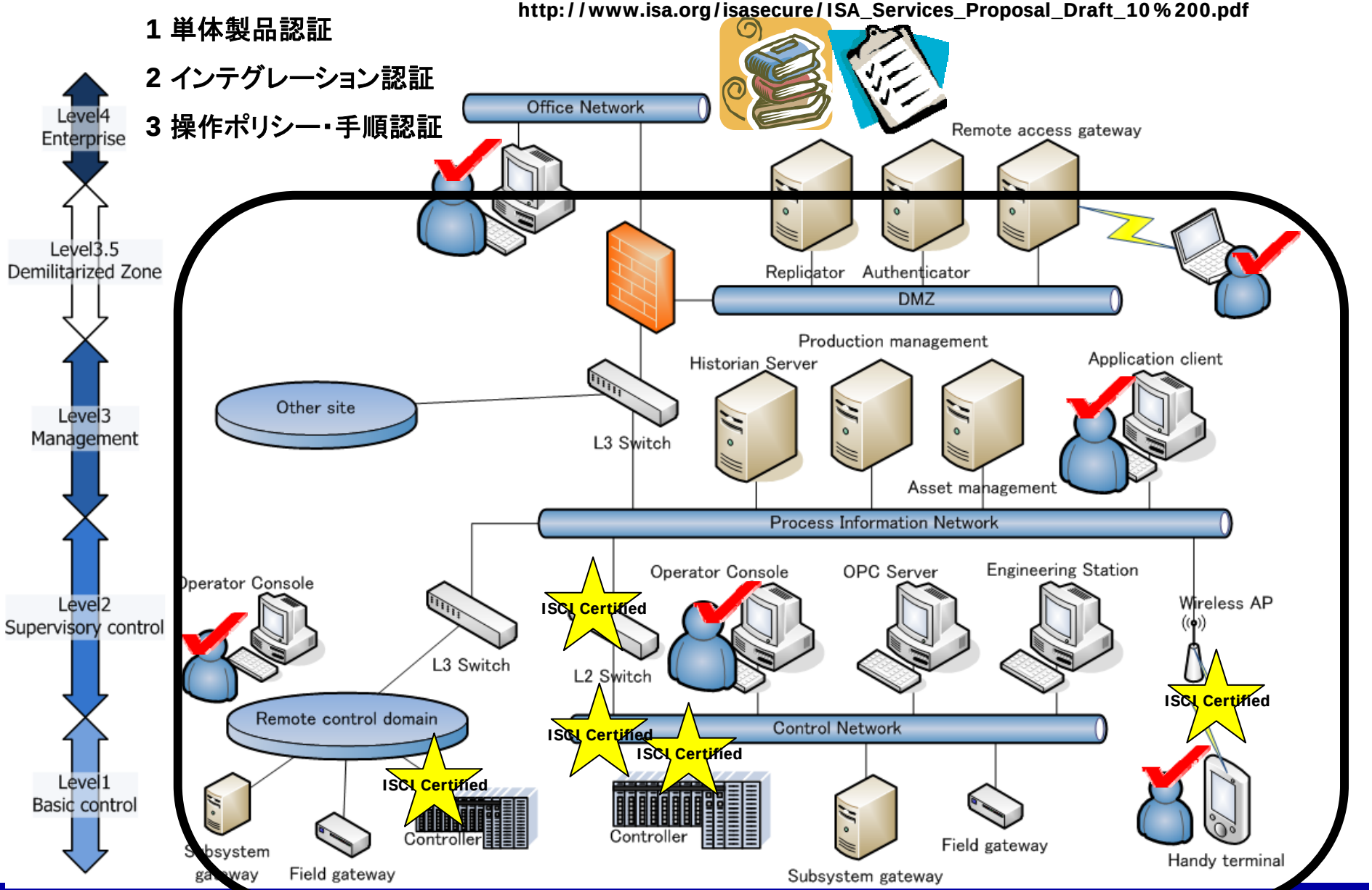
A Yokogawa Commitment to Industry vigilance®

http://www.isa.org/isasecure/ISA_Services_Proposal_Draft_10%200.pdf

1 単体製品認証

2 インテグレーション認証

3 操作ポリシー・手順認証



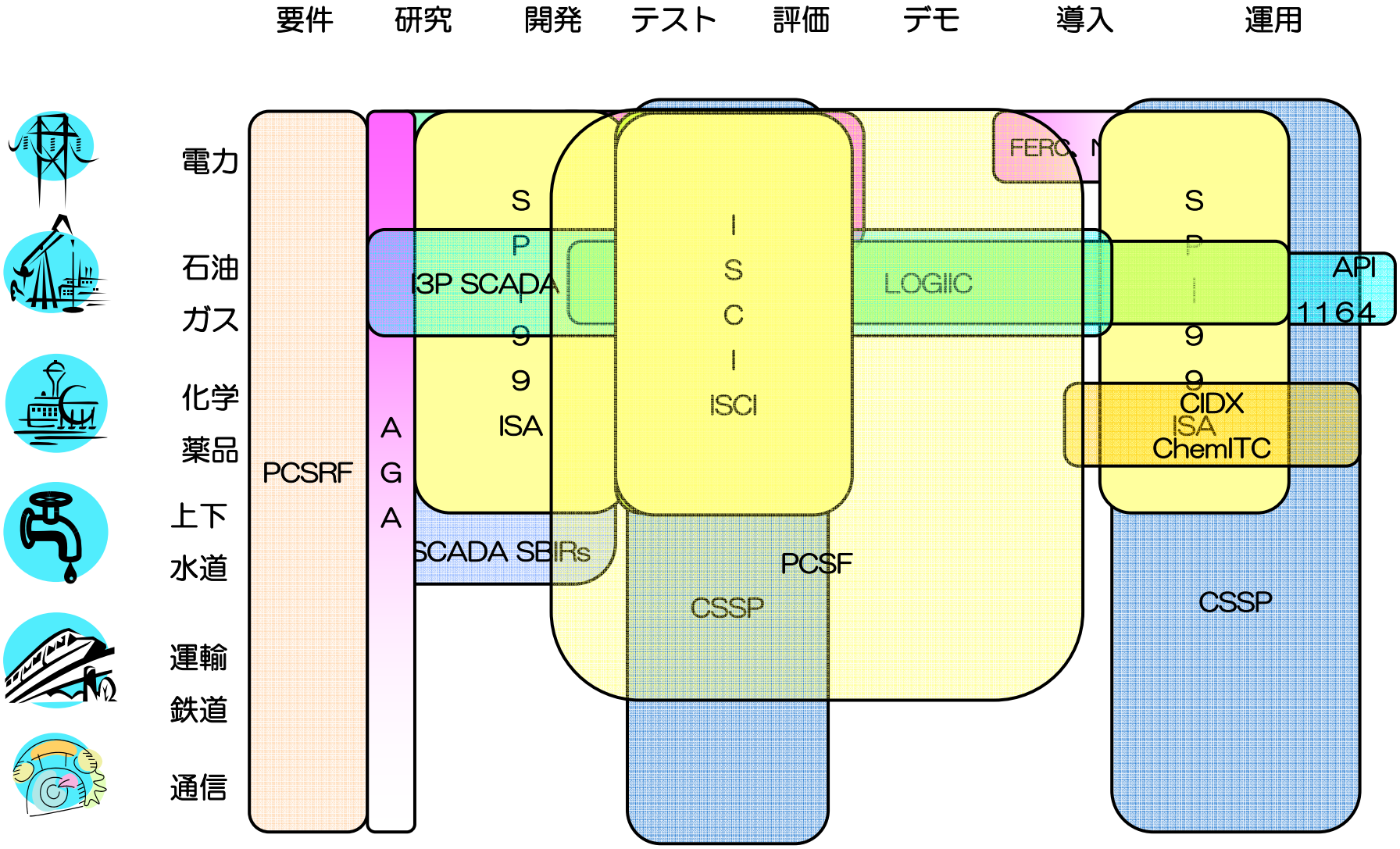
ISCI基本要件

A Yokogawa Commitment to Industry vigilance®

- http://www.isa.org/asci/CFI-Embedded_Controller_QOS-07282008.pdf
- FR 1 - デバイス、情報への不許可アクセス、問い合わせ防止
- FR 2 - 指定通信チャネルのデータ変更防止による不許可デバイス操作防止
- FR 3 - 指定通信チャネルデータの改竄防止
- FR 4 - 指定通信チャネルからのデータ漏洩防止
- FR 5 - 通信チャネルのデータフロー制御による不許可情報漏洩防止
- FR 6 - セキュリティ違反時に、担当に通報し、緊急事態に、自動応答によりフォレンジックエビデンスを報告する。
- FR 7 - DOS攻撃から全ネットワークリソースを保護し、可用性を保証する。

米国制御システムセキュリティカバレッジ

A Yokogawa Commitment to Industry vigilance®



重要インフラと主軸の管轄組織・業界団体

A Yokogawa Commitment to Industry vigilance®

国際 International
政府系 Govmtl
業界 Industry

IEC TC57,TC65　ISO/IEC/JTC1 SC27 WG1~5

DoD (Department of Defense)
NSA (National Security Agency)

CPNI (Centre 4 Protc Natl Infra)

DOC (Department Of Commerce)
NIST (National Institute of Standards and Technology)
PCSRF (Process Control Security Requirements Forum)

共通
DHS (Department of Homeland Security)
S&T (Science and Technology Directorate)
PCSF (Process Control Systems Forum)

NSTB (National Scada Test Bed)
CSSP (Control Systems Security Program)
INL (Idaho National Laboratory)

ISA99 WG1-6 ISCI
ISA100, WCI

DOE (Department Of Energy)

電力
FERC (Federal Energy Regulatory Commission)
NERC (North American Electric Reliability Corporation)
EPRI (Electric Power Research Institute)
CIGRE (Counseil International des Grands Reseaux Electriques)
IEEE

石油 ガス
API (American Petroleum Institute)
AGA (American Gas Association)
LOGIIC (Lnk Oil Gas Ind 2 Imprv Cyb Sec)
I3P (Institute for Info Infra Prot)

化学 薬品
~~CIDX (Chemical Industry Data Exchange)~~
ChemITC (Chemical ITCenter)
American Chemistry Council

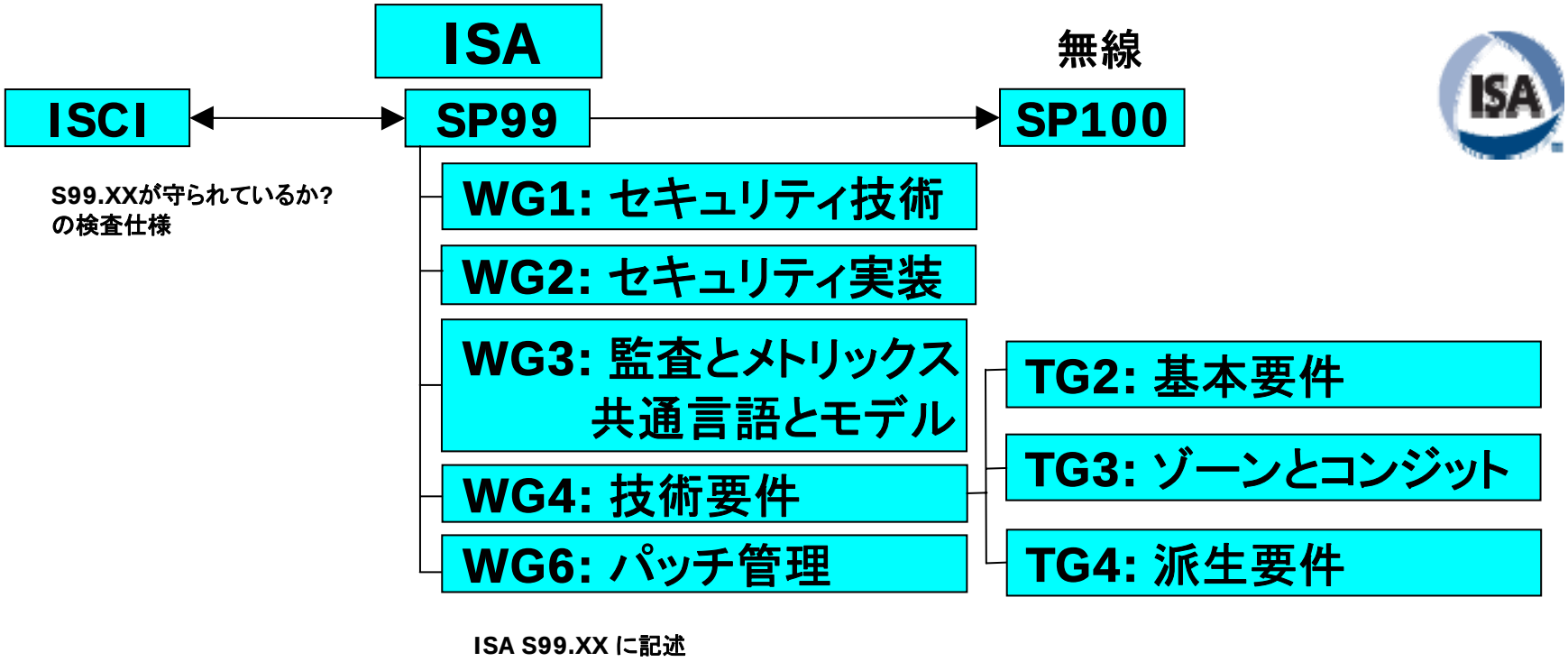
上下 水道
AWWA (American Water Works Association)

運輸 鉄道
RAA (Regional Airline Association)
APTA (American Public Transportation Association)
RTCA (Radio Technical Commission for Aeronautics)
AAR (Association of American Railroad)

通信
OTA (O Telephone Association)

IEC/WG10

ISAセキュリティ標準関連WG



ISA99 セキュリティ標準

A Yokogawa Commitment to Industry vigilance®

ISA99 Security for Industrial Automation and Control Systems

- ISA 99.00.01 - 用語、概念、モデル (WG3)
- ISA 99.00.02 – 製造システム、制御システムのセキュリティプログラムの確立(WG2)
- ISA 99.00.03 - 製造システム、制御システムのセキュリティプログラムの運用
- ISA 99.00.04 –製造システム、制御システムの規定セキュリティ要件 (WG4)
- ISA TR99.00.01 - 製造システム、制御システム防御技術(WG1)
- ISA TR99.00.02 - 製造システム、制御システム環境への電子的セキュリティの組込み

http://www.isa.org/Content/Microsites988/SP99,_Manufacturing_and_Control_Systems_Security1/Home964/Guide_to_the_ISA-99_Standards.pdf

S99ドキュメントは、IEC 62443 に取り込まれる予定です。
IEC/TC65/WG10 Network and System Security

DCS/SCADAシステムセキュリティの展望

A Yokogawa Commitment to Industry vigilance®

- DCS/SCADAは、IT技術を取り入れてきた。
- その結果、セキュリティ問題に直面した。
- セキュリティ問題への解は、ITセキュリティ技術に見出せる。
- ITセキュリティ技術の適用方法を考慮することで見えてくる。
- IT技術は寿命が短く品質水準が異なるため、
  - ライフサイクルを考慮すること、
  - 軽量・省メモリのものを選定すること、
  - 適用する単位を考慮すること、
  - 十分なQAで品質を確保すること、

  が必要。
- 同じ問題解決を行っている先進的組織が数多く存在する。
- 先進的組織と歩調を合わせ、情報共有し、問題を解決する。
- 脅威・脆弱性分析、リスク分析、対策決定、セキュリティ要件抽出、実装、セキュリティテストの反復、誤用・攻撃手法分析を行うことで、解決策が見えてくる。
- 従って、国際レベルで情報共有をし、協力しながら、前に進むことが必要。

*)本資料中の製品名及び名称は、各社の商標または登録商標です。