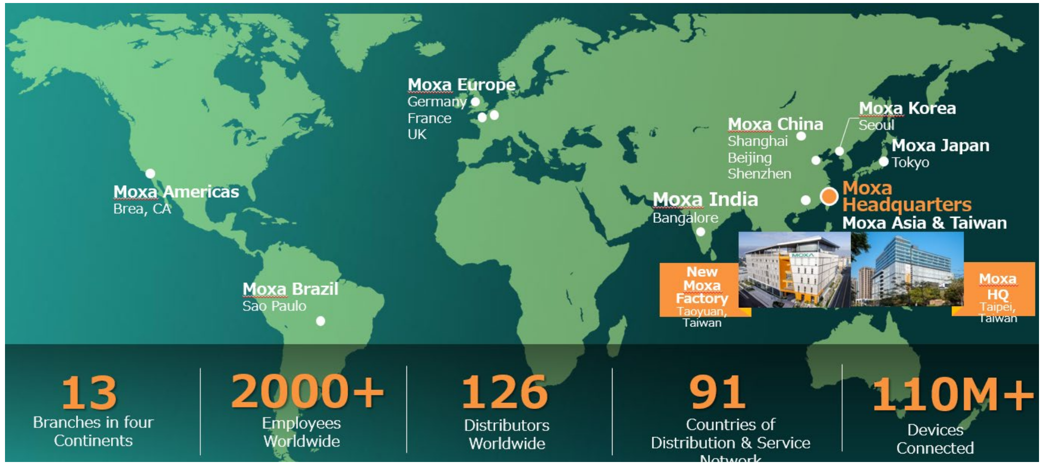
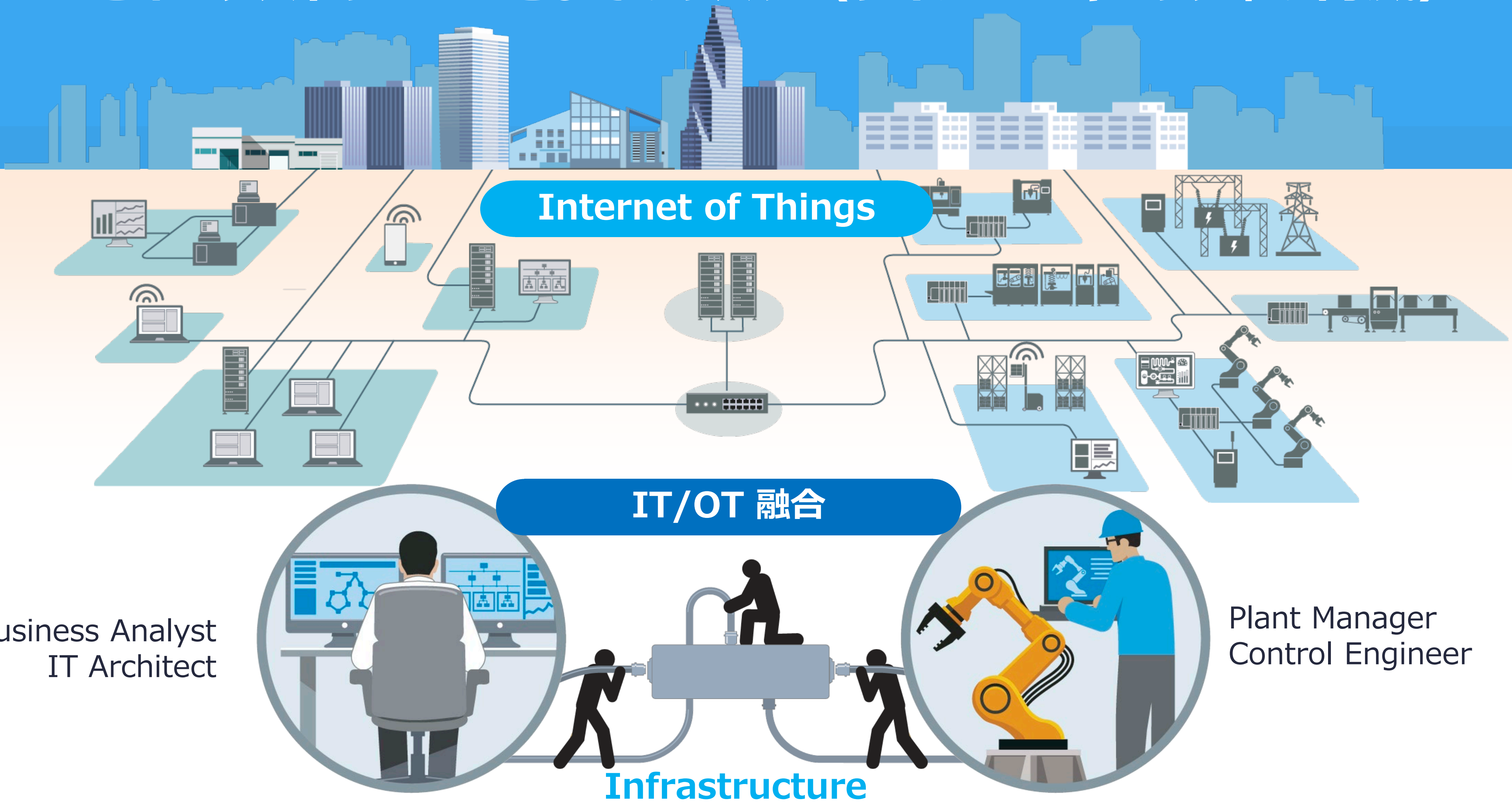
【産業制御系】「産業システムに求められるサイバーセキュリティ対策」

- Moxa Japan 合同会社　出口　博一
  - EBG（Energy Business Group）担当

  - UL サイバーセキュリティ ISA/IEC62443-4 技術者認定

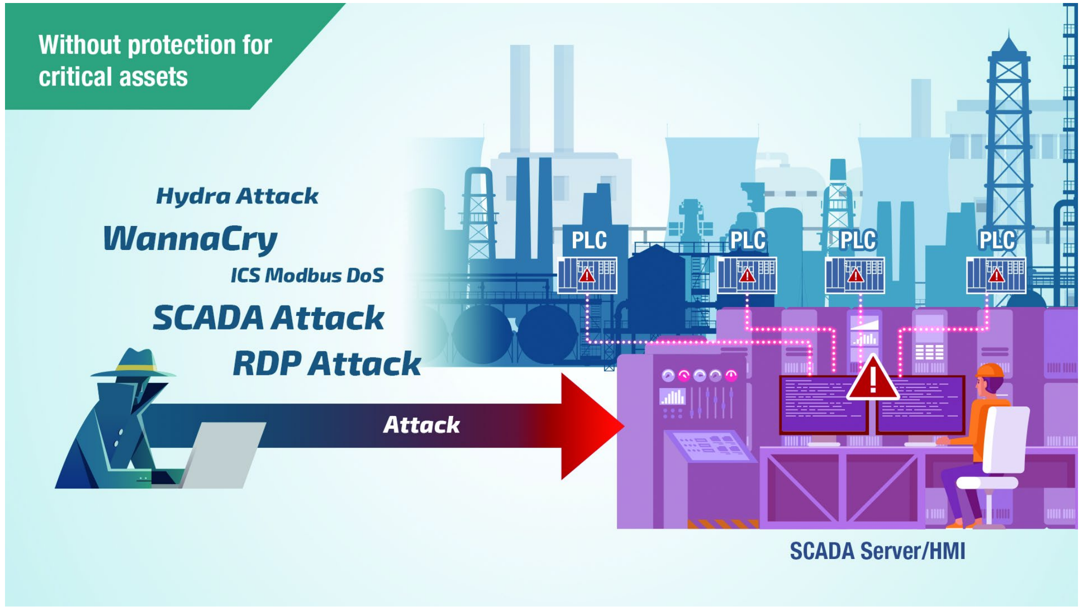

Moxa Europe
Germany
France
UK
Moxa China
Shanghai
Beijing
Shenzhen
Moxa Korea
Seoul
Moxa Japan
Tokyo
Moxa Americas
Brea, CA
Moxa India
Bangalore
Moxa Headquarters
Moxa Asia & Taiwan
New Moxa Factory
Taoyuan, Taiwan
Moxa HQ
Taipei, Taiwan
Moxa Brazil
Sao Paulo
13
Branches in four Continents
2000+
Employees Worldwide
126
Distributors Worldwide
91
Countries of Distribution & Service Network
110M+
Devices Connected

IIoTとインダストリー4.0としてのリスク（サイバーセキュリティの脅威）

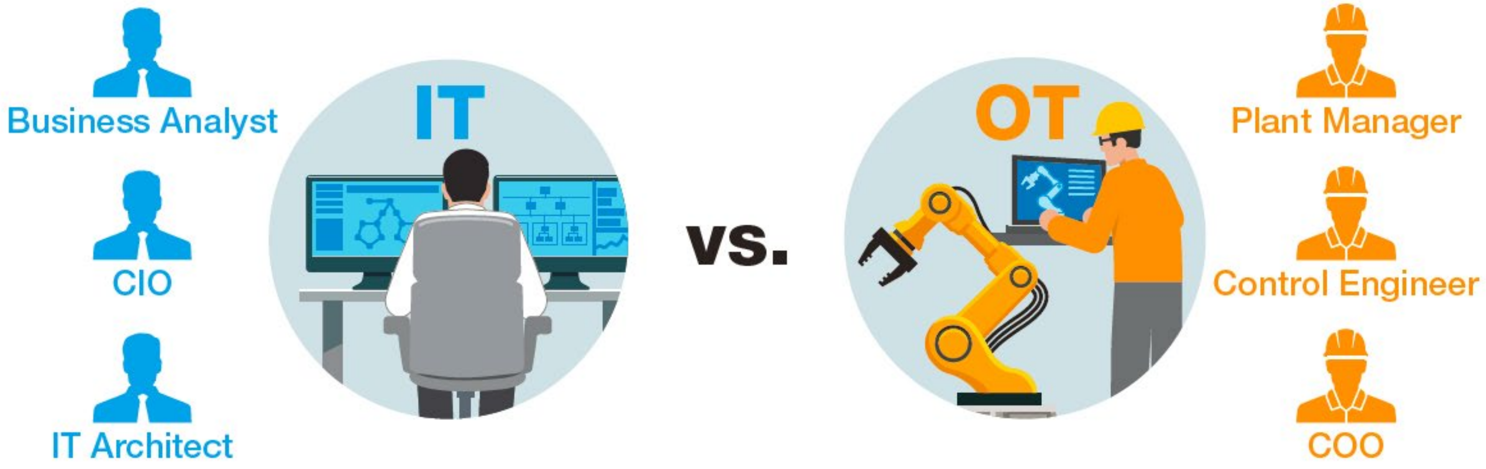

Internet of Things
IT/OT 融合
Business Analyst
IT Architect
Plant Manager
Control Engineer
Infrastructure

セキュリティ インシデントの生産設備への影響

- 工場停止時間
- ノウハウの流出（デザイン、エンジニアリング）
- OT機器へのランサムウェアの侵入
- データの紛失
- 風評被害


Without protection for critical assets
Hydra Attack
WannaCry
ICS Modbus DoS
SCADA Attack
RDP Attack
Attack
PLC
PLC
PLC
PLC
SCADA Server/HMI

ITとOTはサイバーセキュリティの比較


Business Analyst
CIO
IT Architect
IT
vs.
OT
Plant Manager
Control Engineer
COO

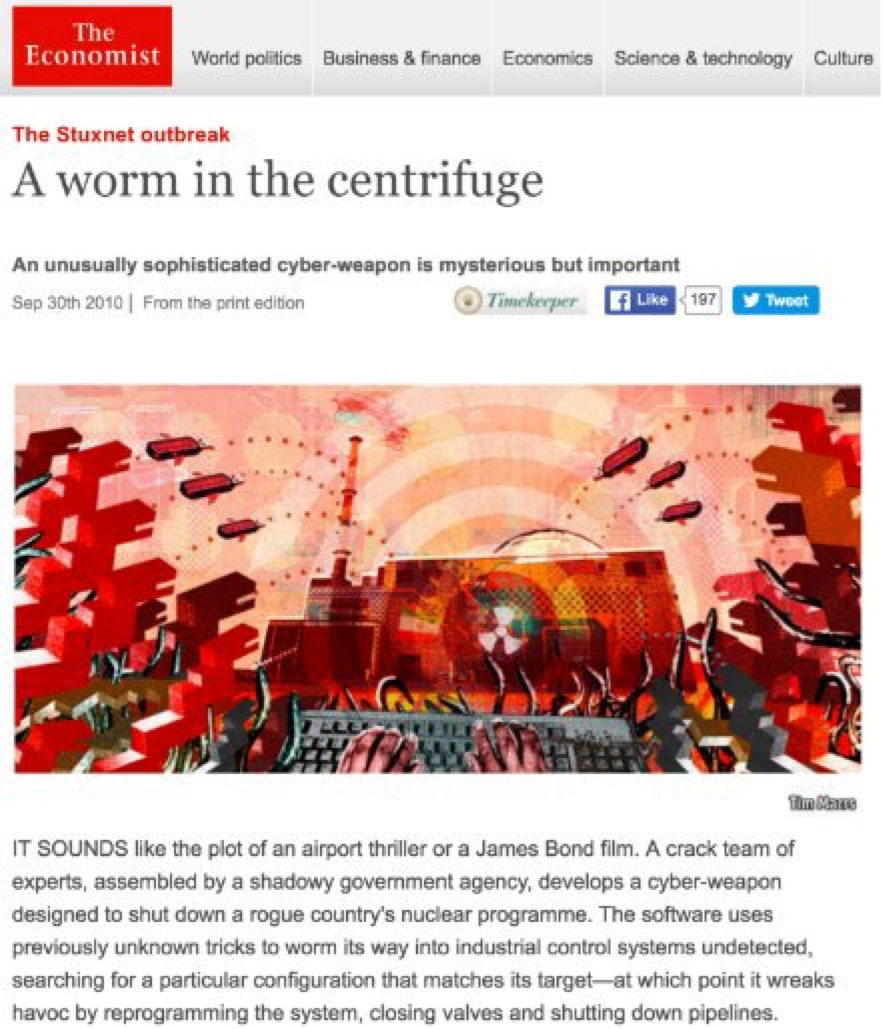
ビジネスの優先事項	機密性	可用性
主な焦点	データの整合性が重要	制御プロセスはダウンタイムを許容できない
保護対象	Windows computers, servers	Industrial devices: PLC, HMI, meters
環境条件	空調が利いている環境	過酷な環境: 極端な温度、振動、衝撃

2010 年以降、Stuxnet などの ICS ネットワークを標的とした高度なサイバー攻撃がいくつか発生しています。

Year	Major ICS Security Incidents	Attack Targets	
2010	Stuxnet	PLC	(Nuclear Power Plant in Iran)
2011	Duqu	Computer/Server	(Public Utility in Multiple Countries)
2012	Disttrack/Shamoon	Computer/Server	(Oil Company in Saudi Arabia)
2014	Sandworm	SCADA/HMI	(Factory Floor in Multiple Countries)
2015	BlackEnergy / Killdisk	HMI/Serial Device	(Power Grid in Ukraine)
2016	Industroyer	Circuit Breaker	(Power Substation in Ukraine)
2017	Dragonfly	Computer/Server	(Public Utility in US/EU)
2018	WannaCry	Computer/Server	(Factory Machines in Asia)

OT（ICS）にセキュリティが求められる事になった背景

- イランの各燃焼施設への攻撃（2010年）
  - 関連企業に勤める外部業者が”Stuxnet”に感染したUSBメモリをSCADAに接続
  - StuxnetがPLCを介して、周波数変換装置を操作
  - 結果、8400台の遠心分離機を破壊


The Economist
World politics
Business & finance
Economics
Science & technology
Culture

The Stuxnet outbreak

A worm in the centrifuge

An unusually sophisticated cyber-weapon is mysterious but important

Sep 30th 2010 | From the print edition

Timekeeper
Like
197
Tweet
Tim Marrs

IT SOUNDS like the plot of an airport thriller or a James Bond film. A crack team of experts, assembled by a shadowy government agency, develops a cyber-weapon designed to shut down a rogue country's nuclear programme. The software uses previously unknown tricks to worm its way into industrial control systems undetected, searching for a particular configuration that matches its target—at which point it wreaks havoc by reprogramming the system, closing valves and shutting down pipelines.

電力以外の業界例（船舶）

- 2023年1月16日、DNV船級協会は、船舶管理・運航プラットフォーム「ShipManager」へのサイバー攻撃を報告
- この攻撃は約1,000隻の船舶に影響を与え、ITサーバーの一時的な停止を引き起こした
- 海運業界を標的とした標的型ランサムウェア攻撃

Stuxnet
- Sabotage Iran's nuclear

Duqu
- Targeting Europe, Asia and North ICS
- Mainly for Inteligrnce gathering

Flame

Gauss

Shamoon
- Targeting Middle East
- Mainly for inteligrnce gathering

Havex/Dragonfly
- Watering Hole tavties
- Trejan attack OPC
- Targeting European ICS (mainly energy)

Triton/Trisis
- Troj_Trisis_A
- Attack Triconex (SIS) to halt plant operation in watershad factory

BlackEnergy3
Ukrainian PowerGrid

WannaCry
NotPetya
LockerGoga

2010 2011 2012 2013 2014 2015 2017 **2018-2024**

攻撃手法は標的型から非標的型も
（ピンポイント攻撃型から、無差別や利益追求型）

標的型サイバー攻撃
（重要インフラ）

非標的型、利益目的のサイバー攻撃
（スマート製造）

Iran-Linked Actor
Targets U.S
ectric
Firms, AUG 201

WannyCry Hits
Plants of Chip Giant
TSM
AUG

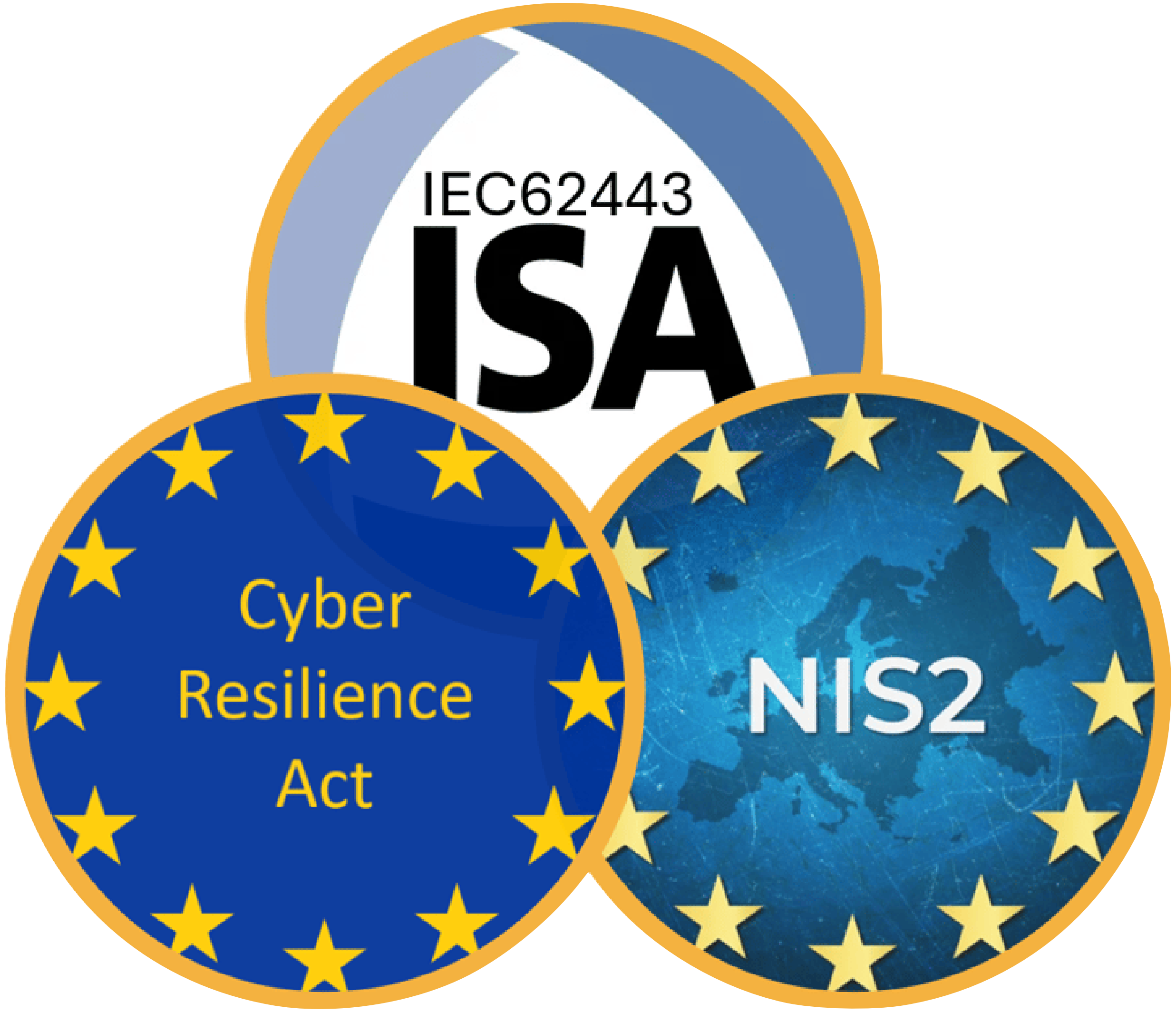
LockerGoga:
APT with hackers act behind;
2018/E-2019

Russian Critical Infrastructure Targeted by Profit-Driven Cybererirninals, DEC 2018

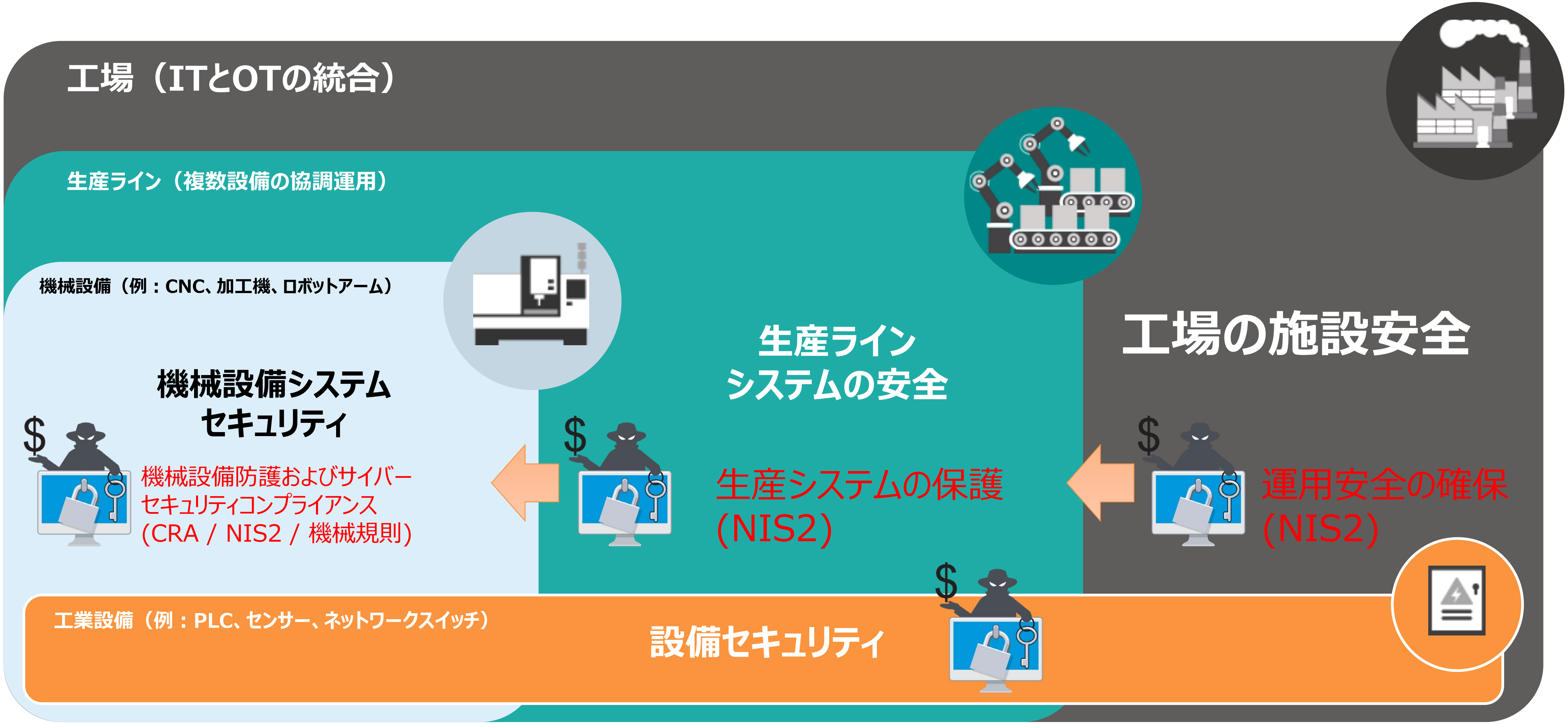
A.P. Moller-Maersk NotPetya; 200M loss, JUN 2017

Saipem Middle East Servers Targeted, DEC 2018

欧州の規制の法制化と規格（NIS2/CRA/IEC62443 ）


IEC62443
ISA
Cyber
Resilience
Act
NIS2

CRA / NIS2 法規対応の概略図



工場（ITとOTの統合）

生産ライン（複数設備の協調運用）

機械設備（例：CNC、加工機、ロボットアーム）

**機械設備システム
セキュリティ**

機械設備防護およびサイバーセキュリティコンプライアンス（CRA / NIS2 / 機械規則）

**生産ライン
システムの安全**

生産システムの保護（NIS2）

工場の施設安全

運用安全の確保（NIS2）

工業設備（例：PLC、センサー、ネットワークスイッチ）

設備セキュリティ

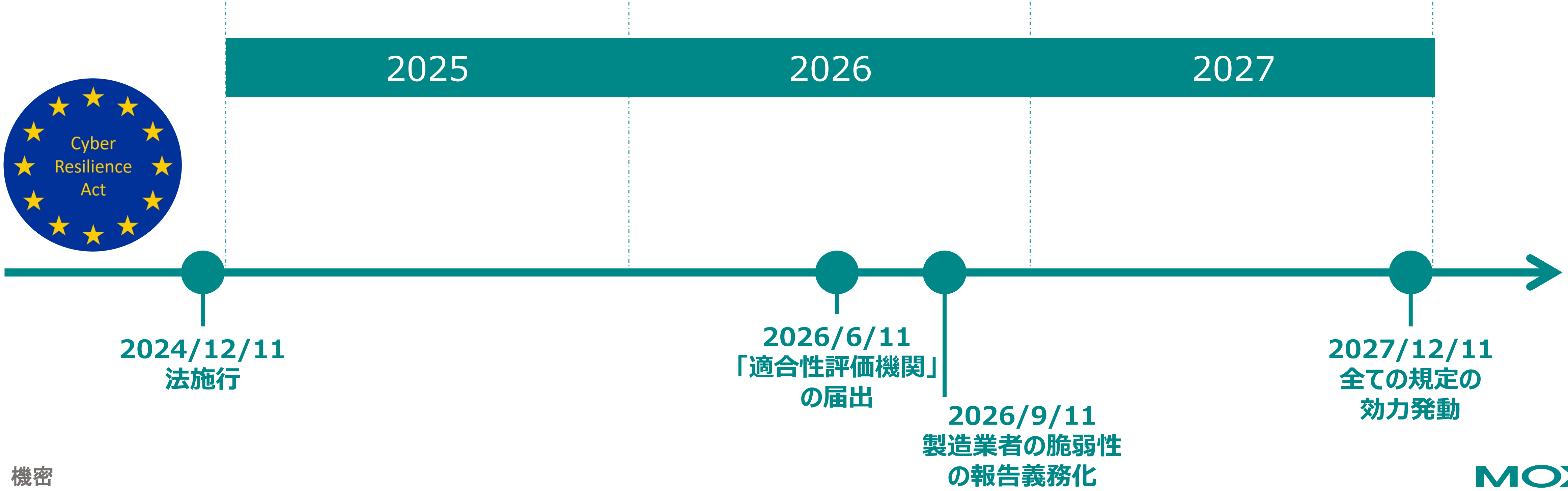
NIS2指令は2022年12月に《欧州連合官報》で公布され、2023年1月16日に正式に発効した。本指令はEU全体のサイバーセキュリティレジリエンス強化を目的としており、《ネットワークレジリエンス法案（Cyber Resilience Act, CRA）》の政策方針と整合している。各加盟国は指令発効後21か月以内、すなわち2024年10月17日までに、これを国内法規に取り入れなければならない。

CRAは「デジタル要素を有する製品」に対して初めてサイバーセキュリティ要件を定めた世界初の法規であり、指令は運用者（製造者、輸入業者、販売業者を含む）に対して包括的な義務を課している。主な重点は以下の通りである：

製品ライフサイクル責任：経済事業者は製品のライフサイクル全体にわたりサイバーセキュリティ規範を遵守する必要があり、最長で製品の生産終了後10年まで延長される。

ガバナンスおよび技術の二軌道要求：指令はリスクレベルに応じたガバナンスおよび技術的措置の実施を求めており、バランスの取れたサイバーセキュリティ防護を実現する。

サイバーセキュリティリスクレベルに焦点を当てる：すべてのセキュリティ要件は製品に関連するネットワークリスクレベルに基づいて調整され、一律適用されるものではない。



2024/12/11
法施行

2026/6/11
「適合性評価機関」の届出

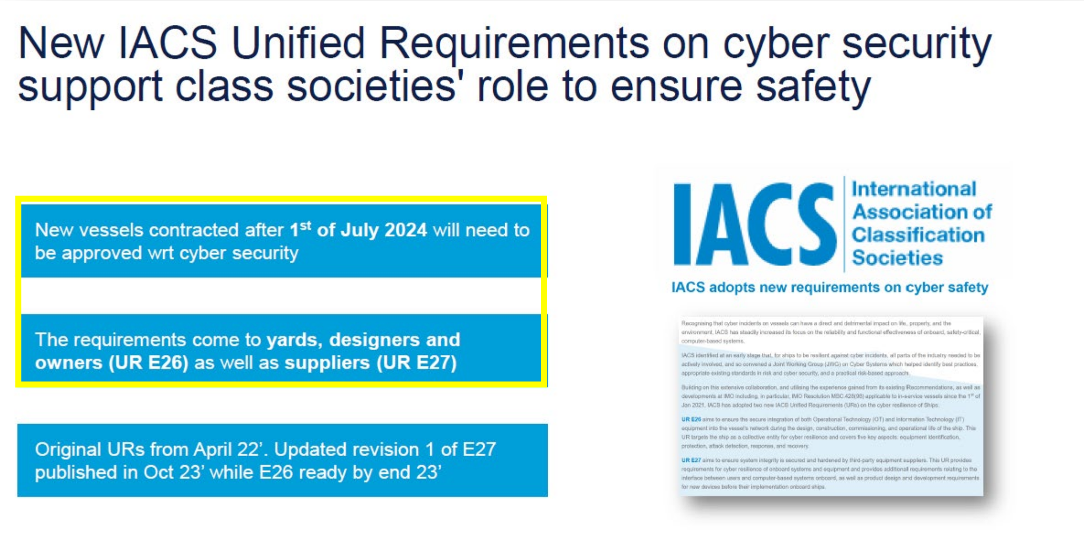
2026/9/11
製造業者の脆弱性の報告義務化

2027/12/11
全ての規定の効力発動

NIS2 / CRA 対応 – IEC 62443 Standards

Security Topics	NIS2	CRA		IEC 62443-4-1	IEC 62443-4-2
Risk Management	✓	✓	●	✓	✓
Incident Response	✓	✓	●	✓	✓
Security Measures	✓	✓	●	✓	✓
Supply Chain Security	✓	✓	●	✓	✓
Secure Product Development	-	✓	●	✓	✓
Technical Security Requirements	-	✓	●	✓	✓
Vulnerability Management	✓	✓	●	✓	✓
Compliance and Certification	✓	✓	●	✓	✓
Network Security and Resilience	✓	-	●	✓	✓
Information Sharing and Cooperation	✓	-		-	-
Monitoring and Logging	✓	-	●	✓	✓
User Awareness and Training	✓	-	●	✓	-
Data Protection and Confidentiality	✓	-	●	-	✓

船舶におけるサイバーセキュリティ規制-IACS UR E26/E27



New IACS Unified Requirements on cyber security support class societies' role to ensure safety

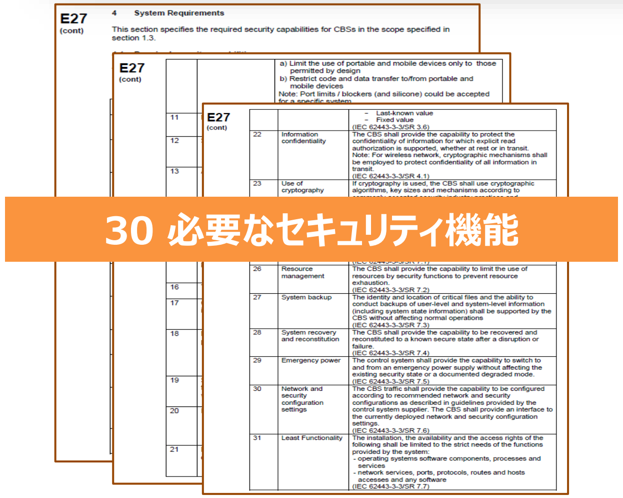
New vessels contracted after 1st of July 2024 will need to be approved wrt cyber security

The requirements come to **yards, designers and owners (UR E26)** as well as **suppliers (UR E27)**

Original URs from April 22'. Updated revision 1 of E27 published in Oct 23' while E26 ready by end 23'

IACS International Association of Classification Societies

IACS adopts new requirements on cyber safety



E27 (cont)

4 System Requirements

This section specifies the required security capabilities for CBSs in the scope specified in section 1.3.

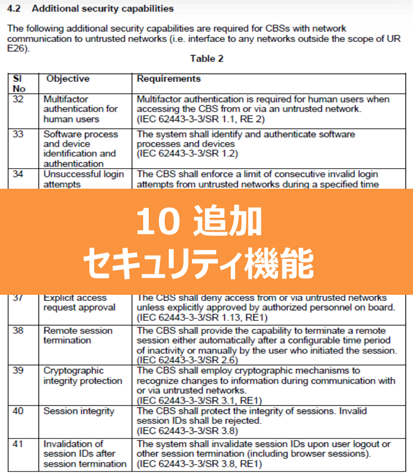
E27 (cont)

a) Limit the use of portable and mobile devices only to those permitted by design
b) Restrict code and data transfer to/from portable and mobile devices
Note: Port limits / blockers (and silicone) could be accepted for a specific system

E27 (cont)

		– Last-known value – Fixed value (IEC 62443-3-3/SR 3.6)
22	Information confidentiality	The CBS shall provide the capability to protect the confidentiality of information for which explicit read authorization is supported, whether at rest or in transit. Note: For wireless network, cryptographic mechanisms shall be employed to protect confidentiality of all information in transit. (IEC 62443-3-3/SR 4.1)
23	Use of cryptography	If cryptography is used, the CBS shall use cryptographic algorithms, key sizes and mechanisms according to
26	Resource management	The CBS shall provide the capability to limit the use of resources by security functions to prevent resource exhaustion. (IEC 62443-3-3/SR 7.2)
27	System backup	The identity and location of critical files and the ability to conduct backups of user-level and system-level information (including system state information) shall be supported by the CBS without affecting normal operations (IEC 62443-3-3/SR 7.3)
28	System recovery and reconstitution	The CBS shall provide the capability to be recovered and reconstituted to a known secure state after a disruption or failure. (IEC 62443-3-3/SR 7.4)
29	Emergency power	The control system shall provide the capability to switch to and from an emergency power supply without affecting the existing security state or a documented degraded mode. (IEC 62443-3-3/SR 7.5)
30	Network and security configuration settings	The CBS traffic shall provide the capability to be configured according to recommended network and security configurations as described in guidelines provided by the control system supplier. The CBS shall provide an interface to the currently deployed network and security configuration settings. (IEC 62443-3-3/SR 7.6)
31	Least Functionality	The installation, the availability and the access rights of the following shall be limited to the strict needs of the functions provided by the system: - operating systems software components, processes and services - network services, ports, protocols, routes and hosts accesses and any software (IEC 62443-3-3/SR 7.7)

30 必要なセキュリティ機能



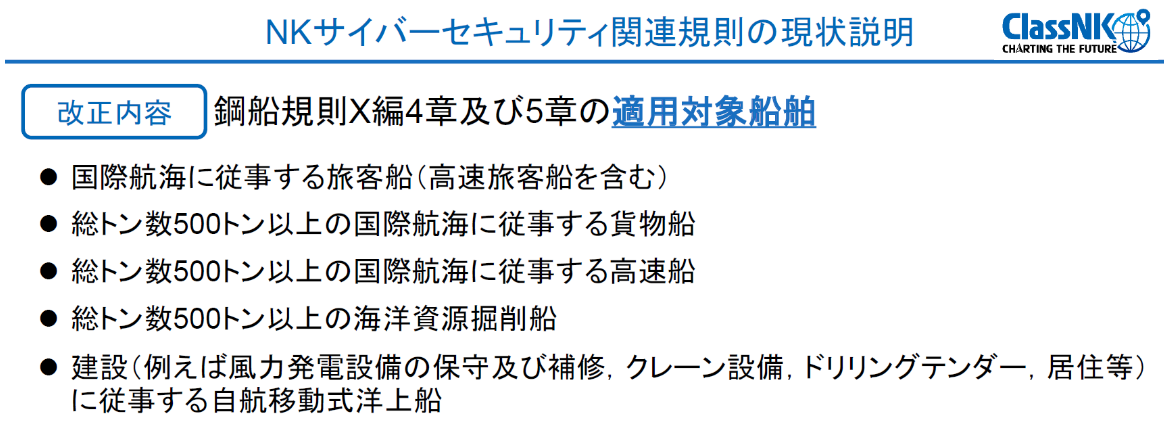
4.2 Additional security capabilities

The following additional security capabilities are required for CBSs with network communication to untrusted networks (i.e. interface to any networks outside the scope of UR E26).

Table 2

Sl No	Objective	Requirements
32	Multifactor authentication for human users	Multifactor authentication is required for human users when accessing the CBS from or via an untrusted network. (IEC 62443-3-3/SR 1.1, RE 2)
33	Software process and device identification and authentication	The system shall identify and authenticate software processes and devices (IEC 62443-3-3/SR 1.2)
34	Unsuccessful login attempts	The CBS shall enforce a limit of consecutive invalid login attempts from untrusted networks during a specified time
37	Explicit access request approval	The CBS shall deny access from or via untrusted networks unless explicitly approved by authorized personnel on board. (IEC 62443-3-3/SR 1.13, RE1)
38	Remote session termination	The CBS shall provide the capability to terminate a remote session either automatically after a configurable time period of inactivity or manually by the user who initiated the session. (IEC 62443-3-3/SR 2.6)
39	Cryptographic integrity protection	The CBS shall employ cryptographic mechanisms to recognize changes to information during communication with or via untrusted networks. (IEC 62443-3-3/SR 3.1, RE1)
40	Session integrity	The CBS shall protect the integrity of sessions. Invalid session IDs shall be rejected. (IEC 62443-3-3/SR 3.8)
41	Invalidation of session IDs after session termination	The system shall invalidate session IDs upon user logout or other session termination (including browser sessions). (IEC 62443-3-3/SR 3.8, RE1)

10 追加
セキュリティ機能

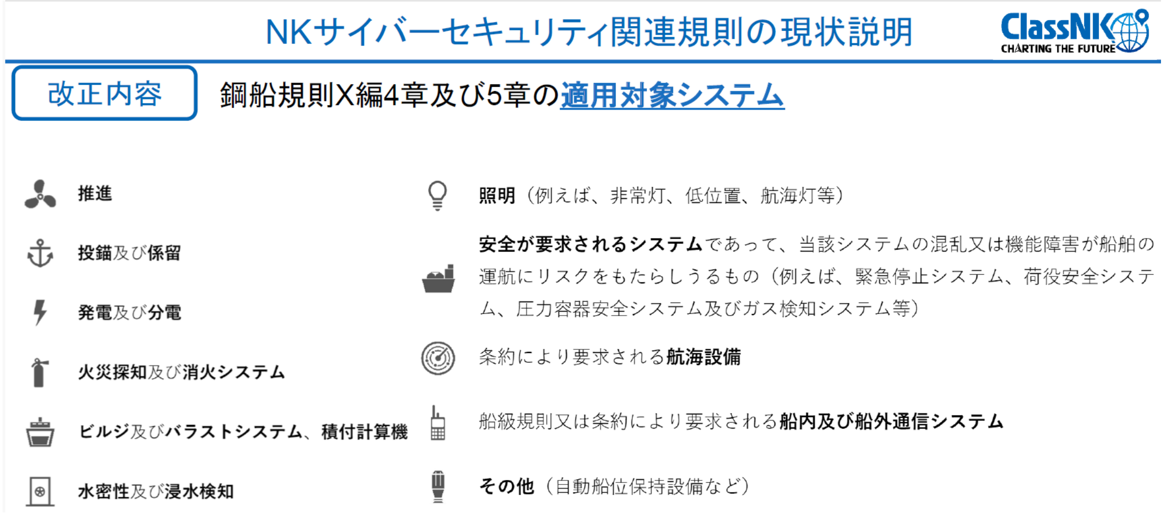


NKサイバーセキュリティ関連規則の現状説明

ClassNK CHARTING THE FUTURE

改正内容　鋼船規則X編4章及び5章の**適用対象船舶**

- 国際航海に従事する旅客船（高速旅客船を含む）
- 総トン数500トン以上の国際航海に従事する貨物船
- 総トン数500トン以上の国際航海に従事する高速船
- 総トン数500トン以上の海洋資源掘削船
- 建設（例えば風力発電設備の保守及び補修，クレーン設備，ドリリングテンダー，居住等）に従事する自航移動式洋上船



NKサイバーセキュリティ関連規則の現状説明

ClassNK CHARTING THE FUTURE

改正内容　鋼船規則X編4章及び5章の**適用対象システム**

- **推進**
- **投錨**及び**係留**
- **発電**及び**分電**
- **火災探知**及び**消火システム**
- **ビルジ**及び**バラストシステム**、**積付計算機**
- **水密性**及び**浸水検知**
- **照明**（例えば、非常灯、低位置、航海灯等）
- **安全が要求されるシステム**であって、当該システムの混乱又は機能障害が船舶の運航にリスクをもたらしうるもの（例えば、緊急停止システム、荷役安全システム、圧力容器安全システム及びガス検知システム等）
- 条約により要求される**航海設備**
- 船級規則又は条約により要求される**船内及び船外通信システム**
- **その他**（自動船位保持設備など）

IEC 62443 Overview

IEC 62443-1　概要

- パート1
コンセプトとモデル
- パート2
用語・略語集
- パート3
システムセキュリティ適合の測定基準
- パート4
産業制御システムのセキュリティライフサイクルとユースケース

IEC 62443-2　ポリシー・手順

アセットオーナ（運用）

- パート1
産業制御システムオーナー向けのセキュリティ要件
- パート2
セキュリティプロテクションレベル
- パート3
産業制御システム環境におけるパッチ管理
- パート4
産業制御システムサービス・プロバイダ向け要件
- パート5
産業制御システムオーナー向けの実装ガイド

アセットオーナー

IEC 62443-3　　システム

システムインテグレータ（設計・開発）

- パート1
産業制御システムのセキュリティ技術
- パート2
セキリティリスクアセスメントと設計
- パート3
システムセキュリティ要件とセキュリティレベル

システムインテグレータ

IEC 62443-4　　コンポーネント

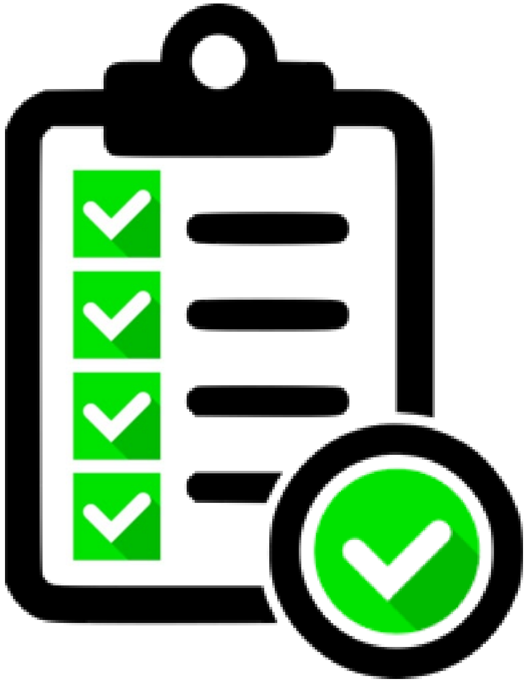
製品供給者（製品開発）

- パート1
セキュア製品開発ライフサイクル
- パート 2
産業制御システム向けセキュリティ技術要件

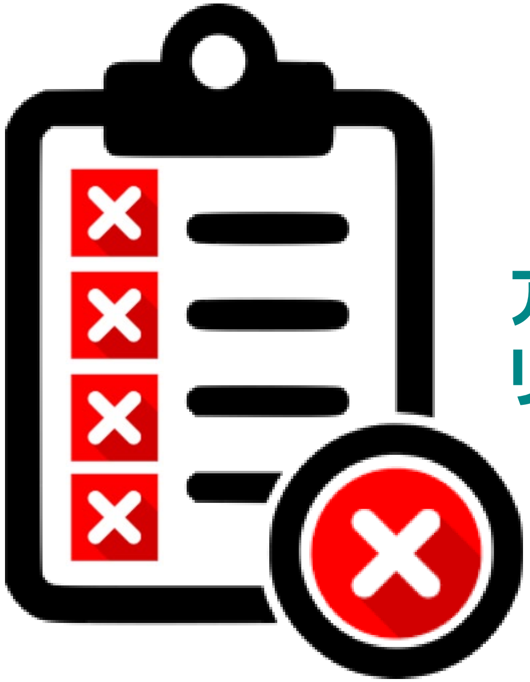
製品供給者

ホワイトリストとブラックリストの考え方

アクセスを許された
リスト



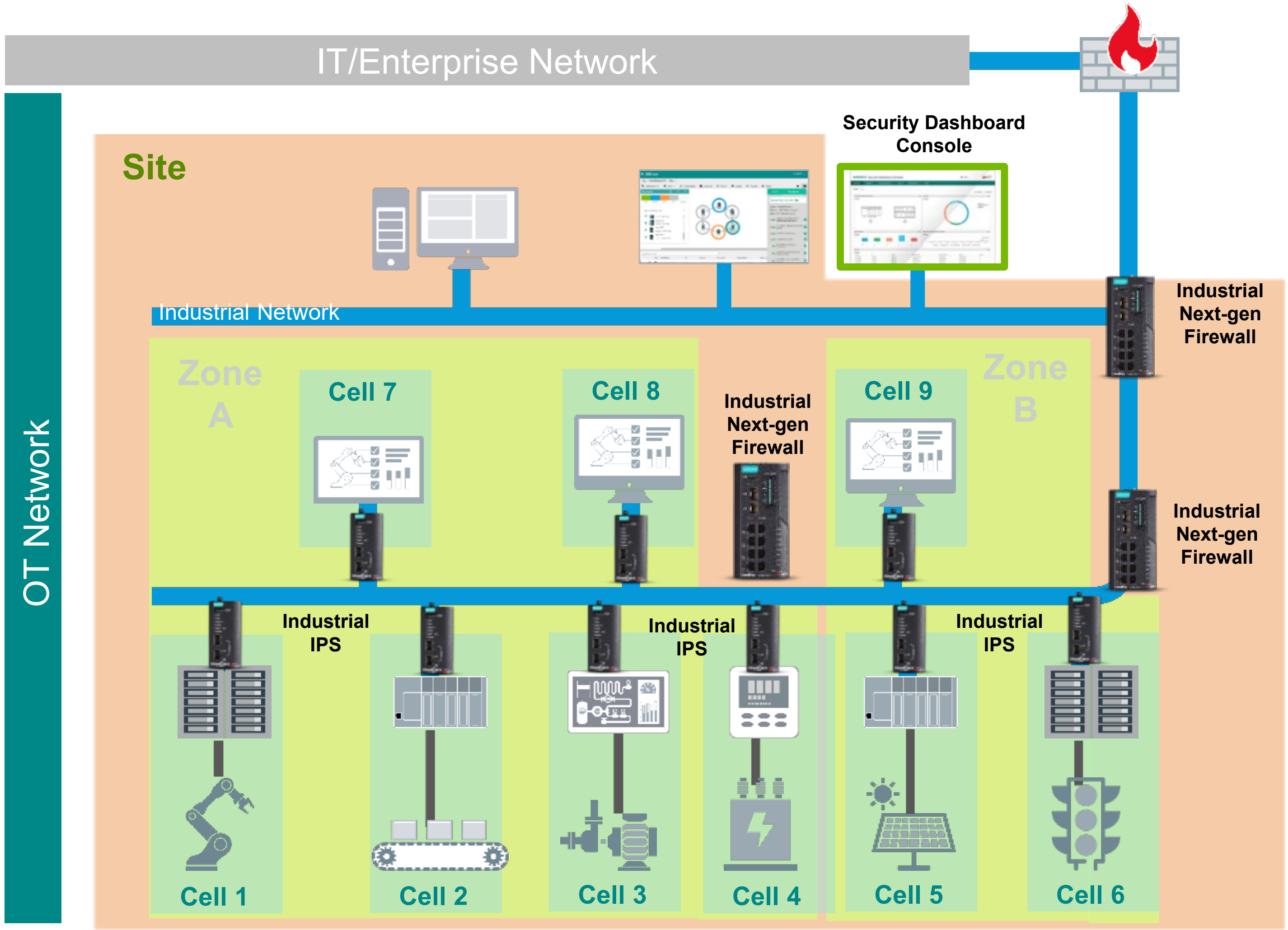
ホワイトリスト
Whitelisting



ブラックリスト
Blacklisting

アクセスを拒絶された
リスト

ネットワークソリューション　アーキテクチャ



IT/Enterprise Network
OT Network
Site
Security Dashboard Console
Industrial Network
Industrial Next-gen Firewall
Zone A
Cell 7
Cell 8
Industrial Next-gen Firewall
Cell 9
Zone B
Industrial Next-gen Firewall
Industrial IPS
Industrial IPS
Industrial IPS
Cell 1
Cell 2
Cell 3
Cell 4
Cell 5
Cell 6

Site Protection

Security Dashboard Console (SDC)

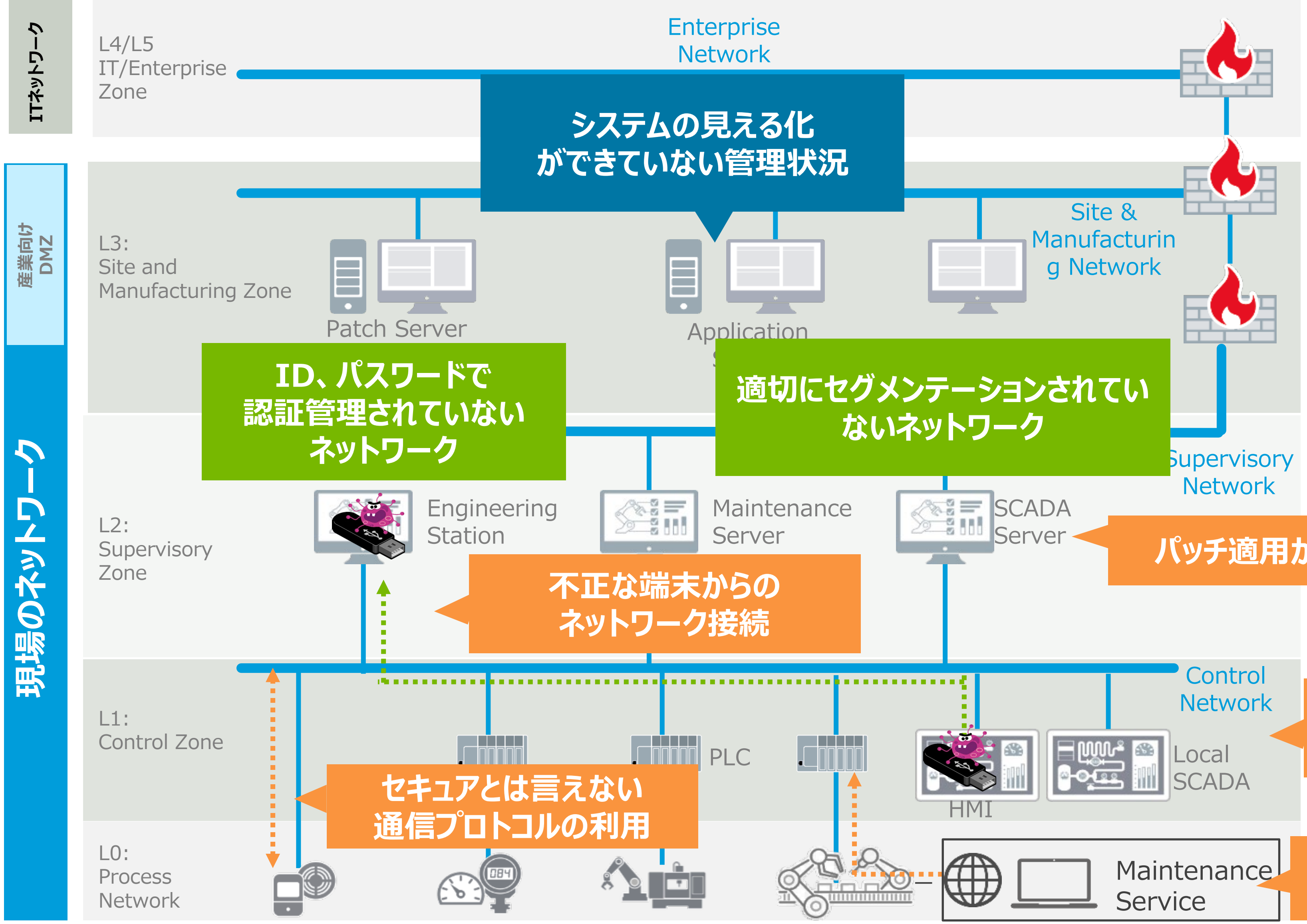
Zone Protection

Industrial Next-Gen Firewall (NGFW)

Cell Protection

Industrial Intrusion Prevention System (IPS)

産業現場のサイバー攻撃・脆弱性例


ITネットワーク
産業向け DMZ
現場のネットワーク
L4/L5
IT/Enterprise
Zone
Enterprise
Network
L3:
Site and
Manufacturing Zone
Patch Server
Application
Site &
Manufacturin
g Network
L2:
Supervisory
Zone
Engineering
Station
Maintenance
Server
SCADA
Server
upervisory
Network
Control
Network
L1:
Control Zone
PLC
HMI
Local
SCADA
L0:
Process
Network
Maintenance
Service

システムの見える化
ができていない管理状況

ID、パスワードで
認証管理されていない
ネットワーク

適切にセグメンテーションされてい
ないネットワーク

不正な端末からの
ネットワーク接続

セキュアとは言えない
通信プロトコルの利用

外部からのIoT機器の不正操作

他ネットワークから
ウィルス感染

境界ファイアウォールは
内部の対策はできない

無線LANに不正接続してネ
ットワーク侵入

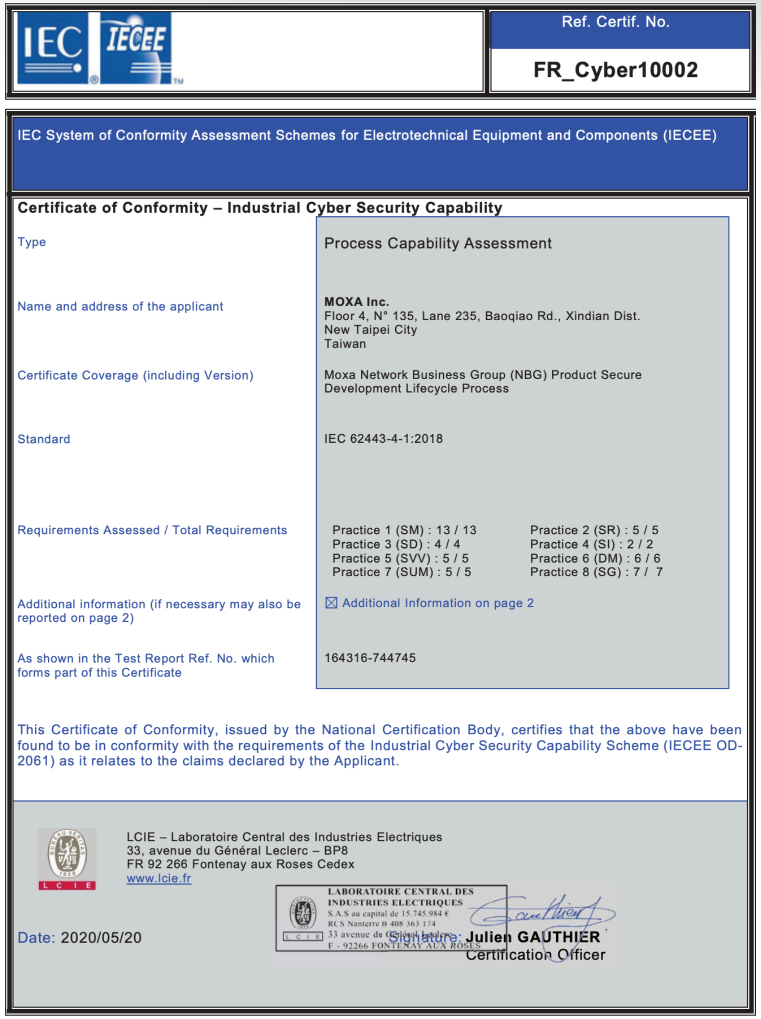
パッチ適用ができない

外部メディアからウィルス
感染（USB 、SDカード等）

外部パソコンからウィルス感染

セキュアバイデザイン

IEC 62443-4-1認証取得



Ref. Certif. No.

FR_Cyber10002

IEC System of Conformity Assessment Schemes for Electrotechnical Equipment and Components (IECEE)

Certificate of Conformity – Industrial Cyber Security Capability

Type	Process Capability Assessment
Name and address of the applicant	**MOXA Inc.** Floor 4, N° 135, Lane 235, Baoqiao Rd., Xindian Dist. New Taipei City Taiwan
Certificate Coverage (including Version)	Moxa Network Business Group (NBG) Product Secure Development Lifecycle Process
Standard	IEC 62443-4-1:2018
Requirements Assessed / Total Requirements	Practice 1 (SM) : 13 / 13 Practice 2 (SR) : 5 / 5 Practice 3 (SD) : 4 / 4 Practice 4 (SI) : 2 / 2 Practice 5 (SVV) : 5 / 5 Practice 6 (DM) : 6 / 6 Practice 7 (SUM) : 5 / 5 Practice 8 (SG) : 7 / 7
Additional information (if necessary may also be reported on page 2)	☒ Additional Information on page 2
As shown in the Test Report Ref. No. which forms part of this Certificate	164316-744745

This Certificate of Conformity, issued by the National Certification Body, certifies that the above have been found to be in conformity with the requirements of the Industrial Cyber Security Capability Scheme (IECEE OD-2061) as it relates to the claims declared by the Applicant.

LCIE – Laboratoire Central des Industries Electriques
33, avenue du Général Leclerc – BP8
FR 92 266 Fontenay aux Roses Cedex
www.lcie.fr

LABORATOIRE CENTRAL DES
INDUSTRIES ELECTRIQUES
S.A.S au capital de 15.745.984 €
RCS Nanterre B 408 363 174
33 avenue du Général Leclerc
F - 92266 FONTENAY AUX ROSES

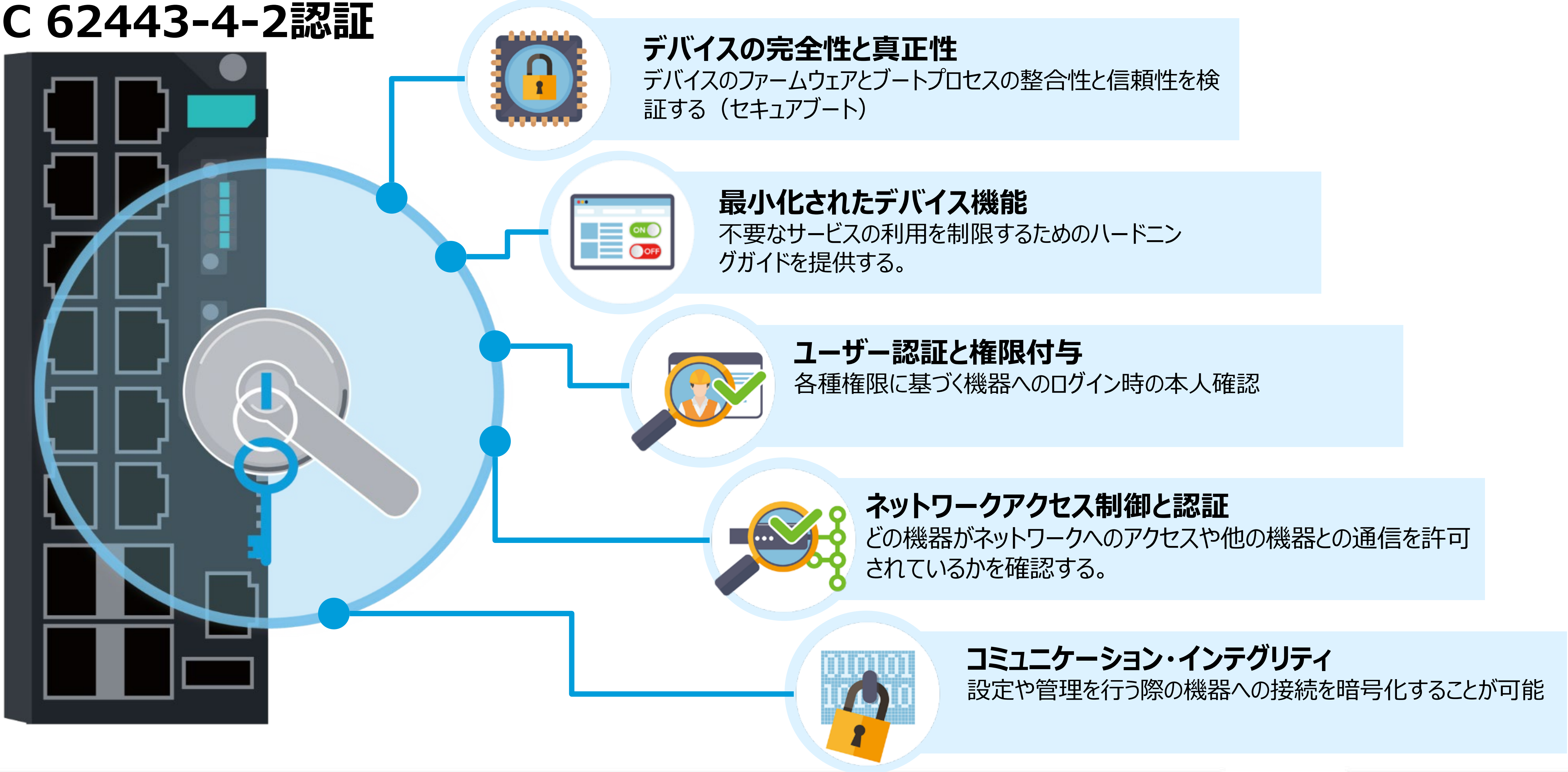
Date: 2020/05/20

Signature: **Julien GAUTHIER**
Certification Officer

- Moxaは、2020年5月にIEC 62443-4-1適合証明書を取得し、OTネットワーキング企業としていち早く、栄誉を手にしました。
- IEC 62443-4-1 は、産業オートメーションや制御システムで使用されるセキュアな製品を開発・維持することを目的とし、セキュア開発ライフサイクルを定義しています。
- この証明書は、Moxaが製品開発プロセスにおいて一貫してからセキュアバイデザイン手法を実装していることを確認するものです。また、Moxaが脆弱性を特定し、対応し、顧客と協力してリスクを軽減する能力があることを証明もしています。

セキュリティ機能を内蔵

IEC 62443-4-2認証



デバイスの完全性と真正性
デバイスのファームウェアとブートプロセスの整合性と信頼性を検証する（セキュアブート）

最小化されたデバイス機能
不要なサービスの利用を制限するためのハードニングガイドを提供する。

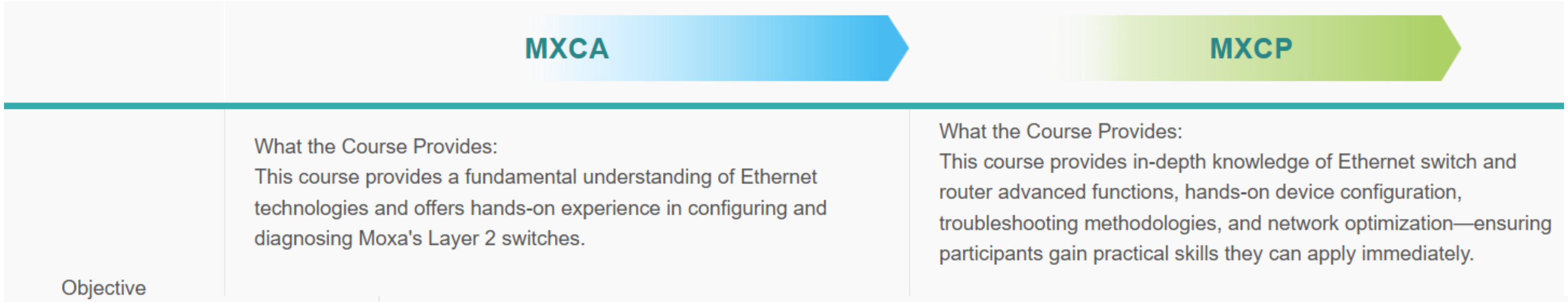
ユーザー認証と権限付与
各種権限に基づく機器へのログイン時の本人確認

ネットワークアクセス制御と認証
どの機器がネットワークへのアクセスや他の機器との通信を許可されているかを確認する。

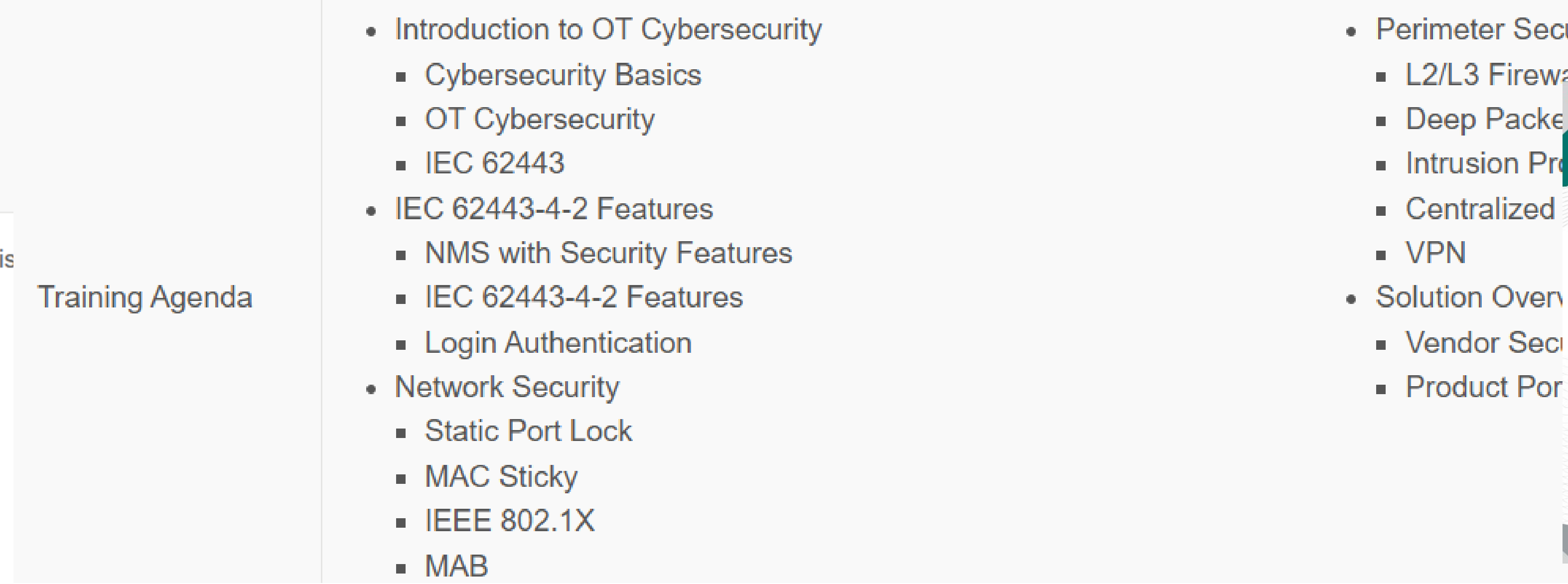
コミュニケーション・インテグリティ
設定や管理を行う際の機器への接続を暗号化することが可能

産業ネットワークソリューションの人材・教育に関して

- **ネットワーク技術認定制度（社内・社外）**



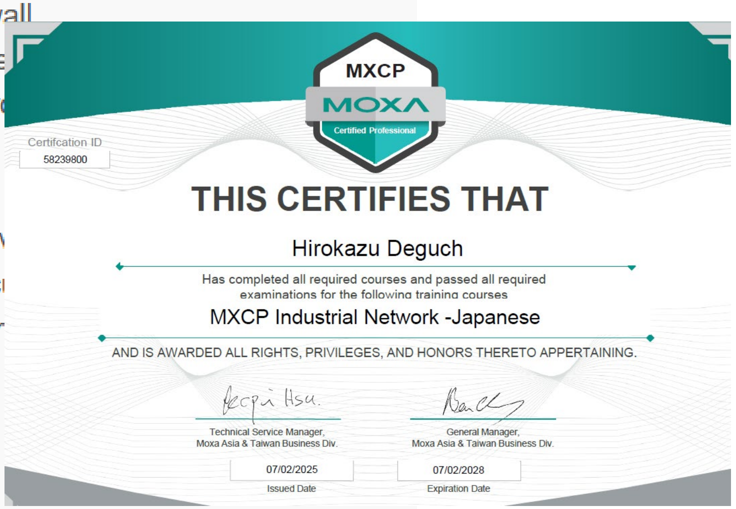
	MXCA	MXCP
Objective	What the Course Provides: This course provides a fundamental understanding of Ethernet technologies and offers hands-on experience in configuring and diagnosing Moxa's Layer 2 switches.	What the Course Provides: This course provides in-depth knowledge of Ethernet switch and router advanced functions, hands-on device configuration, troubleshooting methodologies, and network optimization—ensuring participants gain practical skills they can apply immediately.
Prerequis		



Training Agenda

- Introduction to OT Cybersecurity
  - Cybersecurity Basics
  - OT Cybersecurity
  - IEC 62443
- IEC 62443-4-2 Features
  - NMS with Security Features
  - IEC 62443-4-2 Features
  - Login Authentication
- Network Security
  - Static Port Lock
  - MAC Sticky
  - IEEE 802.1X
  - MAB

- Perimeter Security
  - L2/L3 Firewall
  - Deep Packe
  - Intrusion Pr
  - Centralized
  - VPN
- Solution Overv
  - Vendor Sec
  - Product Por



MXCP
MOXA
Certified Professional

Certifcation ID
58239800

THIS CERTIFIES THAT

Hirokazu Deguch

Has completed all required courses and passed all required examinations for the following training courses

MXCP Industrial Network -Japanese

AND IS AWARDED ALL RIGHTS, PRIVILEGES, AND HONORS THERETO APPERTAINING.

Technical Service Manager,
Moxa Asia & Taiwan Business Div.

General Manager,
Moxa Asia & Taiwan Business Div.

07/02/2025
Issued Date

07/02/2028
Expiration Date

MOXA