

原子力安全セミナー2026

原子力施設におけるサイバーセキュリティ対策

株式会社 東芝 原子力事業部

原子力電気システム設計部 電気システム設計第三グループ

富永 真哉

目次

- 01 原子力施設におけるサイバーセキュリティの現状
- 02 国内外のサイバーセキュリティに関する規格・ガイド
- 03 原子力施設におけるサイバーセキュリティ対策

01

原子力施設におけるサイバーセキュリティの現状

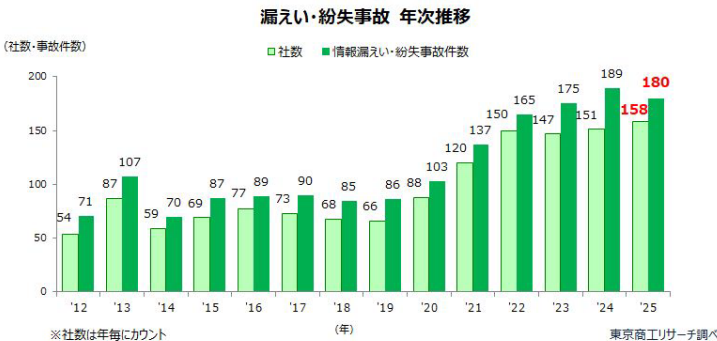
原子力発電所のサイバーセキュリティの現状

組織を取り巻く背景：脅威の動向

■企業への攻撃が頻発、漏洩個人情報情報は累計最大2億1,313万人
(国民一人当たりの個人情報情報が2回漏洩した計算)

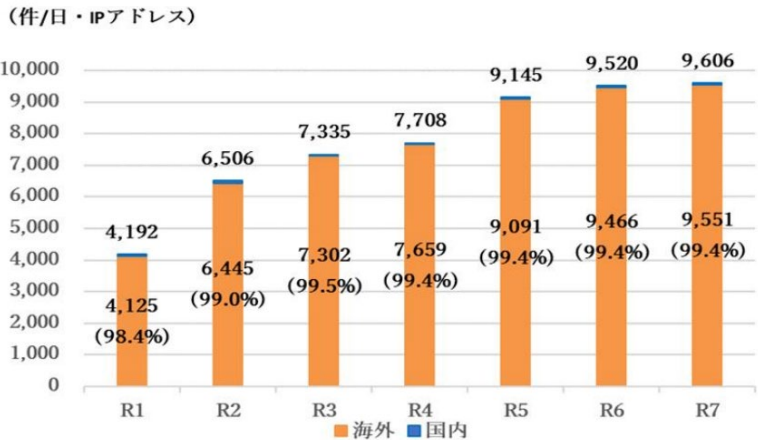
➤公表企業：158社 事故件数：180

出典：東京商工リサーチ社「上場企業と主要子会社での個人情報の漏えい・紛失事故調査（2025年）」



■警察庁サイバーポリスからの報告（R7）では、
探索行為も含めた攻撃は、1IP当たり約9600件にのぼる

出典：警察庁「令和7年におけるサイバー空間をめぐる脅威の情勢等について」



脅威の深刻化は著しく、眼前に迫っている

原子力発電所のサイバーセキュリティの現状

組織を取り巻く背景：日本政府の動向

2014

- サイバーセキュリティ戦略（CS戦略）が閣議決定
- サイバーセキュリティ基本法が施行
- サイバーセキュリティ戦略本部を設立、日本のサイバーセキュリティを推進する権限を集約・強化

2015

- **重要インフラの第3次行動計画**（改定版）が公開
- 日本再興戦略 改訂2015 IT利用の安全・安心の確保が成長戦略を確固たるものにする」と明記

2016

- 経済産業省から経営者が実施すべき要件を纏めた「サイバーセキュリティー経営ガイドライン」が発行
- サイバーセキュリティ基本法 改定案が国会承認

2017

- **重要インフラの第4次行動計画**が公開
- 2020年までの重要インフラの取組み方針が明示

2018

- サイバーセキュリティ戦略（2018-2021） 重要インフラ防護強化、OTへの対策強化

2020

- **重要インフラの第5次行動計画**（改定版）が公開
電気・ガス・水道など重要インフラのリスク管理強化

2021

- サイバーセキュリティ戦略（2021-2024）
DX推進に伴う重要インフラのリスク対策を明確化

2022

- 国家安全保障戦略 改訂
- **経済安全保障推進法**
基幹インフラ設備の事前審査制度導入、重要設備のサプライチェーン管理強化

2023

- 電気事業法等 改正
原子力・電力インフラに対するサイバーセキュリティ要求強化

2024

- 重要インフラのサイバーセキュリティに係る安全基準等改訂

2025

- サイバー対処能力強化法・同整備法 成立
- 国家サイバー統括室（NCO）発足

原子力発電所は重要インフラの一つとして政府方針を考慮した責任ある取組みが必要

攻撃者の動機・目的と攻撃手法

脅威実行者の目的と攻撃手法

脅威実行者	動機・目的	主な活動内容や攻撃手法
 国家型攻撃グループ	■ 政治・軍事等の国家意思	➢ スパイ活動・破壊活動 ➢ DDoS攻撃、標的型サイバー攻撃
 サイバーテロリスト	■ テロの実行や思想の普及	➢ Webサイト改ざん、DDoS攻撃といったサイバー攻撃 ➢ テロの呼びかけやテロ実行マニュアルの配布、プロパガンダ活動（物理的テロの促進）
 ハクティビスト	■ 思想・信条	➢ Webサイト改ざんやDDoS攻撃といったサイバー攻撃 ➢ イベント・製品に対するボイコットの呼びかけ
 サイバー犯罪者	■ 金銭獲得	➢ マルウェア送付（直接的な攻撃） ➢ ダークWeb上のフォーラム運営、マルウェア販売など（間接的）
 悪意のあるハッカー（クラッカー）	■ 知識欲、自己顕示等の個人的欲求	➢ 不正アクセス、DDoS攻撃など（直接的な攻撃） ➢ 攻撃コードの開発、流出データの共有など（間接的）

上記に加え、原子力施設においては内部の犯行者も考慮し内部不正対策を検討する必要がある

サイバー攻撃脅威の進化

サイバー攻撃の目的が、金銭目的へと変わりランサムウェア（身代金要求）が増加

政治目的・特化型から

金銭を狙った **経済目的・汎用型へ** 変化

2026年1位になったのは「ランサムウェアによる被害」、2021年ランキングから6年連続 1 位となりました。ランサムウェア関連のサイバー攻撃は、これまでの一般人向け大量バラマキ型から、企業を標的にするケースが増えてきています。

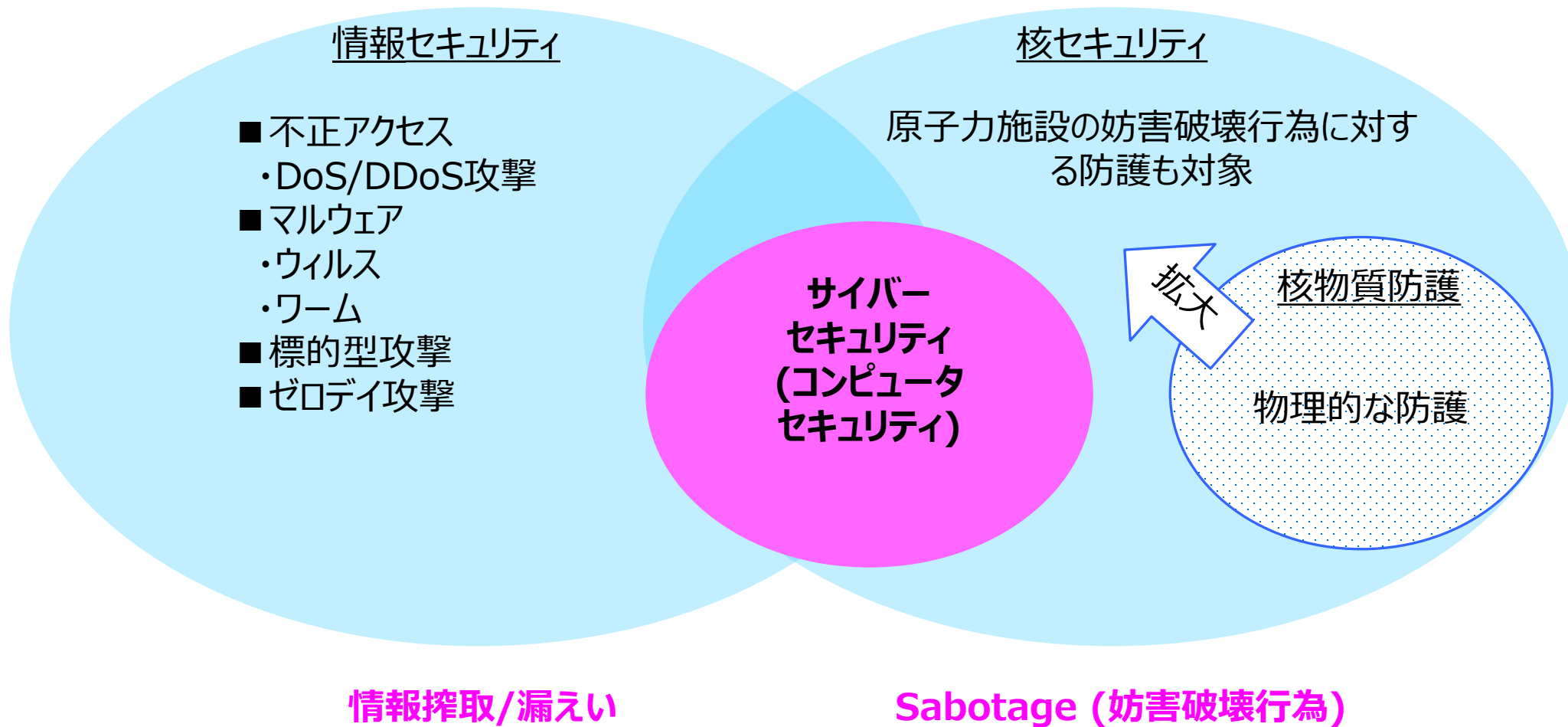
「AIの利用をめぐるサイバーリスク」が2026年初登場。今後増加していくことが想定されます。

IPA「情報セキュリティ10大脅威2026」

出典：<https://www.ipa.go.jp/security/10threats/10threats2026.html>

順位	「組織」向け脅威	初選出年	10大脅威での取り扱い (2016年以降)
	ランサム攻撃による被害	2016年	11年連続11回目
2	サプライチェーンや委託先を狙った攻撃	2019年	8年連続8回目
3	AIの利用をめぐるサイバーリスク	2026年	初選出
4	システムの脆弱性を悪用した攻撃	2016年	6年連続9回目
5	機密情報を狙った標的型攻撃	2016年	11年連続11回目
6	地政学的リスクに起因するサイバー攻撃（情報戦を含む）	2025年	2年連続2回目
7	内部不正による情報漏えい等	2016年	11年連続11回目
8	リモートワーク等の環境や仕組みを狙った攻撃	2021年	6年連続6回目
9	DDoS攻撃（分散型サービス妨害攻撃）	2016年	2年連続7回目
10	ビジネスメール詐欺	2018年	9年連続9回目

原子力施設におけるサイバーセキュリティ



原子力関連のサイバーインシデント事例（1/3）

#	発生年	国	対象施設	内容
1	2026	インド	クダンクラム原子力発電所	ランサムウェア組織による情報流出（原子炉安全、核セキュリティにかかわる情報流出は無し）
2	2026	ポーランド	国立原子力研究センター	サイバー攻撃未遂。MARIAプロジェクト研究路を含む運用・研究プロセスへの影響なし
3	2025	日本	日本原子力研究開発機構	外部ベンダー（委託先）運用サーバにおけるデータ侵害、一部従業員の個人情報流出
4	2025	米国	カンザスシティ国家安全保障キャンパス	SharePoint経由で内部に侵入
5	2024	英国	セラフィールド社	2019～2023年にわたるサイバー管理不備に対するONRの罰金事例。脆弱性が悪用された証拠はない一方、攻撃成功時の運用影響が指摘されている
6	2023	米国	アイダホ国立研究所	外部ベンダーHRシステムにおけるデータ侵害、一部従業員の個人情報流出。本体ネットワークには影響なし
7	2022	イラン	イラン原子力庁	メールサーバが侵害され、約8.5万件のメールが流出
8	2019	インド	クダンクラム原子力発電所	Lazarus系DTrackマルウェア感染

原子力関連のサイバーインシデント事例（2/3）

#	発生年	国	対象施設	内容
9	2017	米国	ウルフクリーク原子力発電所	APT攻撃による発電所情報システムへのサイバー攻撃（具体的な被害なし）
10	2016	日本	富山大学水素同位体化学研究センター	標的型メールによる情報漏えい
11	2016	ドイツ	グンドルミンゲン原子力発電所	燃料管理システムのNWから2つ（Conficker、W.32Ramnit）のマルウェアが確認。侵入経路はUSBメモリと推測
12	2016	米国	原子力規制委員会／エネルギー省	元原子力規制委員会従業員が原子力規制委員会およびエネルギー省のコンピュータシステムを混乱させるためにNRCおよびDoEの従業員へ標的型メールを送付
13	2015	日本	核物質管理センター	標的型メールによる職員のPCから情報流出
14	2014	韓国	水力・原子力発電会社	標的型メールに仕込まれたマルウェアによる情報流出（社員情報、教材、設計図等）
15	2014	日本	もんじゅ原子力発電所	標的型メールによる情報流出とGOMプレーヤーアップデートによる情報流出の可能性
16	2012	米国	サスケハナ原子力発電所	タービンの蒸気をコントロールするコンピュータシステムの誤動作により作動油漏れのため運転員が手動で原子炉を停止
17	2012	イラン	ナタンズ原子力施設	Flame：イランの核関連施設の制御システムの偵察に利用されたといわれるマルウェア。ファイルサイズは20Mあり、すべての機能を解読するためには多くの年月がかかる見通し
18	2011	イラン	ナタンズ原子力施設	Duqu：標的型メールでMSWordの脆弱性を利用し、機密情報を漏えいさせることが目的
19	2011	フランス	アレバ	インシデント発覚2年前からハッカー集団によるコンピュータNWへの不正アクセス

原子力関連のサイバーインシデント事例（3/3）

#	発生年	国	対象施設	内容
20	2011	米国	オークリッジ国立研究所	標的型メール攻撃により送りつけられたマルウェアがIEの脆弱性を悪用しユーザーのマシンに追加コードをダウンロード、2台のマシンが感染。インターネットのアクセス遮断をするまでに情報流出が発生
21	2010	イラン	ナタンズ原子力施設	Stuxnetによる濃縮ウラン遠心分離機の破壊
22	2009	米国	テキサス電力会社	解雇された元従業員による不正アクセスにより計画発電量ファイルの改ざんおよび原子力発電所の従業員へメール（解雇された従業員のIDが即削除されなかったため、自宅からVPNで会社のNWに侵入）
23	2008	米国	エドウィンハッチ原子力発電所	制御システムのコンピュータとITシステムのコンピュータのデータ同期がうまくいかずに同期プログラムにより、制御システムのコンピュータのデータ消失のため、安全システムが動作し、プラントをシャットダウン
24	2006	シリア	建設中の核関連施設	イスラエルの諜報員がシリア政府当局者のコンピュータをハッキングし、シリアに建設中の不法な核関連施設（と思われる）の写真や建設にまつわるメールを取得
25	2006	米国	ブラウンズフェリー原子力発電所	凝縮液脱塩装置のPLCと再循環ポンプの可変周波数駆動装置コントローラは接続されているNWのトラフィックが溢れて正常に動作しなくなったため、運転員は手動にて原子炉をシャットダウン。この原因がサイバー攻撃であるかは不明
26	2005	日本	三菱電機プラントエンジニアリング	日本国内のPWRプラントの情報が個人パソコンにて業務をするために情報をコピーしたため、この個人パソコンのWinnyの暴露ウィルスにより情報が漏えい
27	2003	米国	デービスベッセ原子力発電所	Slammerワームは、コンサルタントのNWから企業NW、発電所NW、プロセス制御NWに移動して、企業NW、制御NWを詰まらせ、約5時間の間プラントパラメータ表示システムにアクセス

インシデント事例 1 Stuxnet

制御システムを標的とする初めてのマルウェア

- 2010年9月に、**イランの核燃料施設のウラン濃縮用遠心分離機を標的としたサイバー攻撃**により、約8,400台の遠心分離機のうち約1,000台が稼働不能に陥り、操業が一時停止する事態となりました。
- イランの核燃料施設はネットワーク的に隔離されていたが、Stuxnetと呼ばれるマルウェアがUSBメモリによって持ち込まれ感染したとされています。

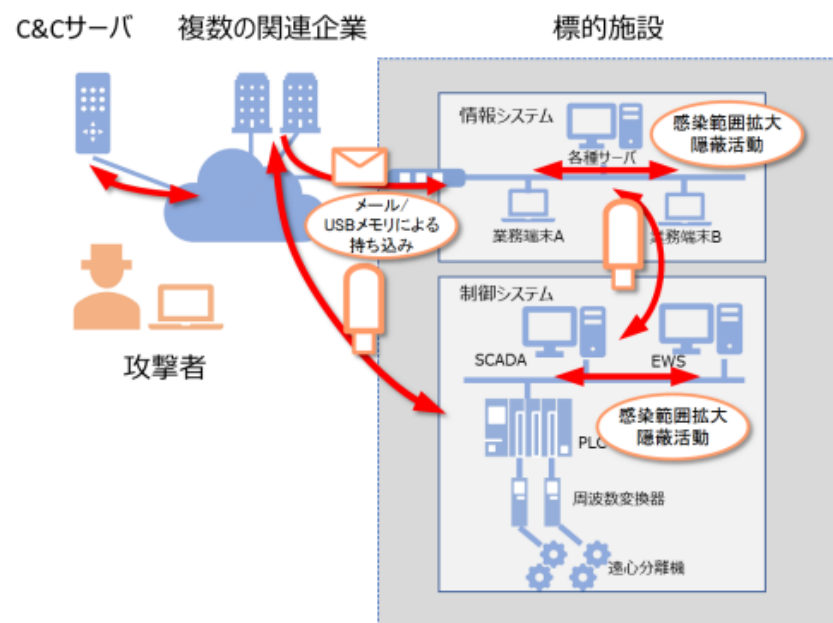


図 1-5 【攻撃局面 A】 制御ネットワーク環境までの攻撃局面-3

出典：IPA「制御システム関連のサイバーインシデント事例」

制御ネットワークに侵入したStuxnetは、標的となるSCADAを発見すると攻撃を開始。PLCのプログラムファイルを改ざんし、周波数変換器の出力周波数を短時間に変化させて遠心分離器に高い負荷をかけ破壊した。

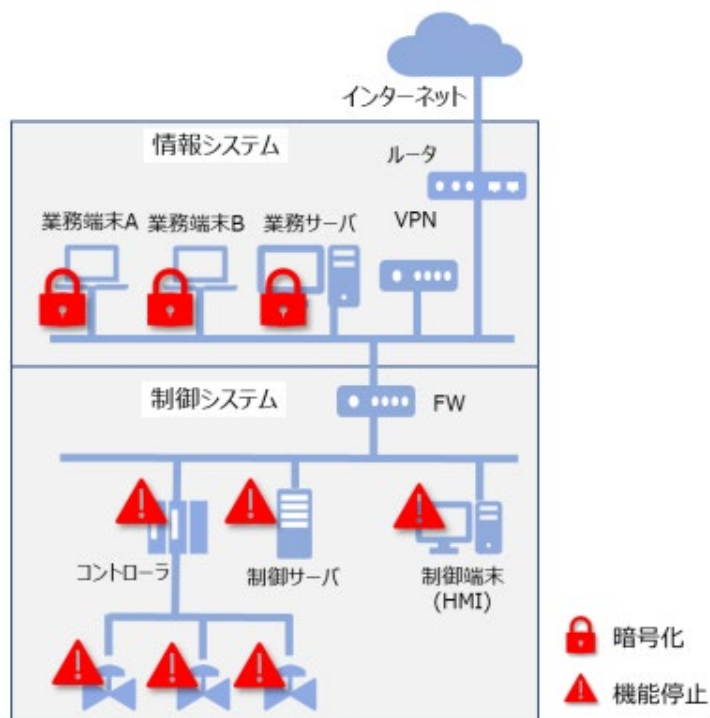
本マルウェアは、感染を検知されないように、制御システムの監視画面をダミー表示したり、警報を停止したりする機能を持つことが特徴的。

後年、Stuxnetは米国とイスラエルによるサイバー攻撃によるものであり、イランの核開発を遅らせることが目的であったと報道された。

インシデント事例 2 ランサムウェア

米国最大手のパイプラインがランサムウェア被害に遭い操業停止

- 2021年5月7日、米国の石油パイプライン企業Colonial Pipelineは**ランサムウェア**による影響を受け**1週間にわたって操業停止**に追い込まれました。12日に操業再開され、15日までに供給網全体が復旧しました。
- 身代金として約5億円を支払った**とされています。



攻撃を受けたのは情報系であり、パイプライン制御システムは直接の影響を受けなかったが、予め決められていた全社的なインシデント対応プロセスに則って、パイプラインは予防保全的に停止された。

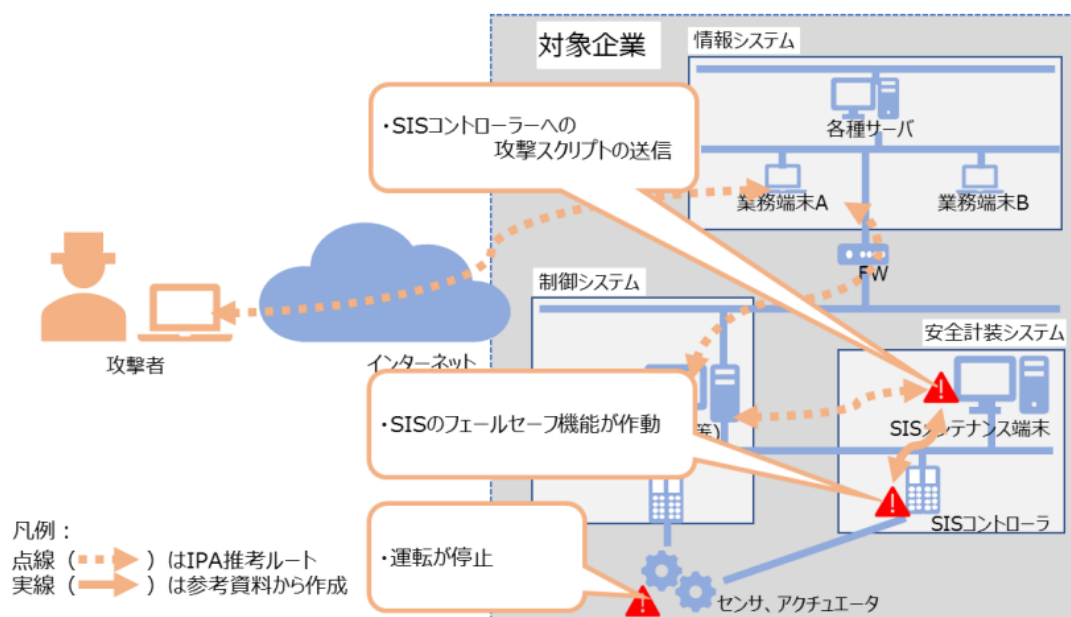
攻撃グループDarkSideは、活動目的は金銭であり、社会的問題を起こすことではないと声明を出している。

米国の関与により、DarkSideはテイクダウンされ、身代金の一部はFBIによって回収された。

インシデント事例 3 制御システム向けマルウェア

安全計装システム(SIS)を標的としたマルウェアにより石油化学プラントが停止

- 2017年12月、中東の石油化学プラントにおいて、**安全計装システム(SIS)を狙ったマルウェア**が感染し、SISのフェールセーフ機能が作動して生産プロセスを自動停止させるに至っていたことが公表されました。
- 本マルウェア(TRITONまたはTRISIS)は、Schneider Electric社製**SISコントローラ(Triconex)**や**PLC等の関連製品向けに作成**されたものであり、攻撃者は**物理的破壊を引き起こす**準備をしていたと考えられています。



攻撃者はエンジニアリングワークステーションにリモートからのアクセスを確立してTRITONマルウェアを仕込み、コントローラのプログラムを改ざんしたとされている。

Schneider Electric社のPLCは日本企業でも多く使用され、SISは世界中のプラントで採用されているシステムであり脅威は深刻。

本インシデントは国家支援型ハッカーグループによるものであり金銭目的ではない。

02

国内外のサイバーセキュリティに関する規格・ガイド

原子力分野の規格・ガイド



原子力施設情報システムセキュリティ対策ガイドライン



原子力発電所におけるサイバーセキュリティ対策導入自主ガイド

主たる外国規格・ガイド



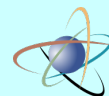
IAEA
International Atomic Energy Agency

NSS No.17
No.8, No.24



米国

原子力規制委員会



U.S. NRC

R.G 5.71
R.G 1.152



原子力エネルギー協会

NUCLEAR ENERGY INSTITUTE

NEI08-09
NEI13-10

その他各国の原子力規制当局



フランス



英国



Office for
Nuclear Regulation



フィンランド



Radiation and Nuclear Safety Authority (STUK)



スウェーデン



I o T、産業分野の規格・基準類



IEC62645
Ed.2

セキュリティレベルとゾーン分けの考え方

IEC62859
Ed.1.1

Safetyとサイバーの協調

IEC63096
Ed.1

事業者のセキュリティ管理

原子力関連

その他分野

I o T、産業分野の規格・基準類



IEC62443

汎用制御システムのセキュリティ基準

ISO/IEC
27000
シリーズ

情報セキュリティ認証



NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

電力向け

北米電力
信頼度協議会

NERC
CIP-002
~011



I T 向け

米国国立標準技術研究所

NIST
SP-800-
82他

FISMA

情報セキュリティの法規制

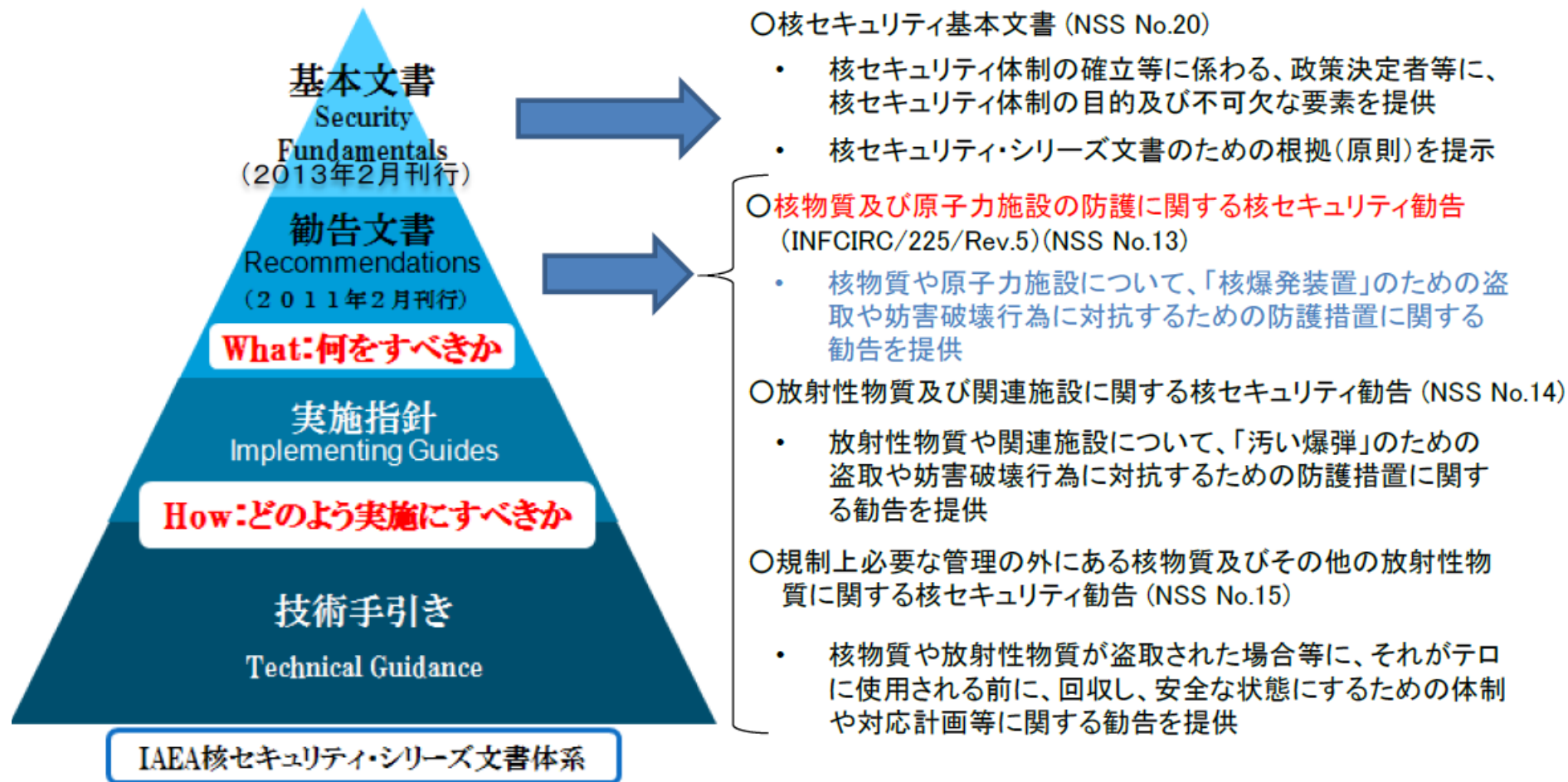
NIST SP-
800-171
800-53
800-63
他



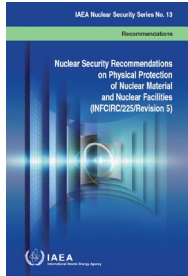
欧州 ネットワーク
情報セキュリティ庁

(参考) IAEA Nuclear Security Series (NSS) 文書体系

IAEAは核セキュリティを確立、実装、維持するための推奨事項・ガイダンスをNuclear Security Series(NSS)として発行



主たる外国規格・ガイドライン -IAEA-

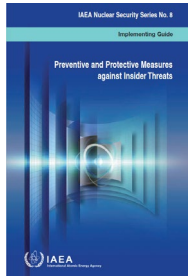


IAEA Nuclear Security Series No. 13

Recommendations

Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5)

4.10項や5.19項に侵害行為（例えばサイバー攻撃、ごまかし又は偽造）に対してコンピュータシステムが防護されるべきであることを規定

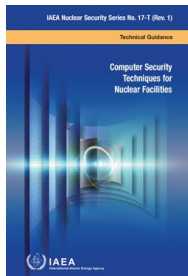


IAEA Nuclear Security Series No. 8

Implementing Guide

Preventive and Protective Measures against Insider Threats

4.7項、4.33項、5.14項、5.26項にて内部脅威としてサイバー攻撃を考慮するよう規定



IAEA Nuclear Security Series No. 17-T

Technical Guidance Reference Manual

Computer Security Techniques for Nuclear Facilities

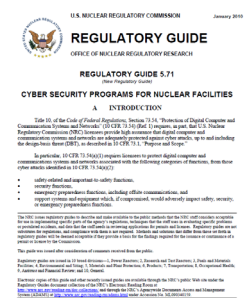
コンピュータセキュリティプログラムの実装、既存のプログラムの評価、重要なデジタル資産の評価、適切なリスク低減対策手段を規定

主たる外国規格・ガイドライン -米国-



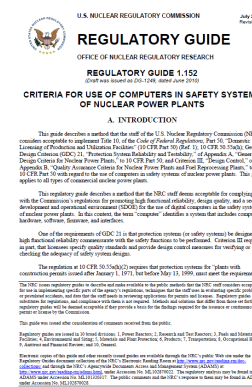
10 CFR Part 73.54 Protection of Digital Computer and Communication Systems and Networks

デジタルコンピュータとコミュニケーションシステム・ネットワークを、設計基準脅威 (Design Basis Threat, DBT)に該当するサイバー攻撃から適切に保護することを規定



U.S. NUCLEAR REGULATORY COMMISSION REGULATORY GUIDE 5.71 CYBER SECURITY PROGRAMS FOR NUCLEAR FACILITIES

10 CFR 50 73.54記載の要求事項に対応するために制定・維持が必要なサイバーセキュリティプログラムの内容、およびその制定、維持や取り扱い方法をまとめたサイバーセキュリティプランの作成について記載



U.S. NUCLEAR REGULATORY COMMISSION REGULATORY GUIDE 1.152 CRITERIA FOR USE OF COMPUTERS IN SAFETY SYSTEMS OF NUCLEAR POWER PLANTS

原子力発電所の安全系に計算機を使用する場合のセキュアな開発・運転環境（SDOE: Secure Development and Operation Environment）、設計品質、機能信頼性を促進するためにNRCスタッフにとって許容可能な手法を述べたもの。“安全系”とは、原子力発電所の安全を担保するために設けられている系統（計測制御系を含む）を言う。安全系のSDOEは、他のネットワークから区別して管理されるということが基本理念。

原子力施設情報システムセキュリティ対策ガイドライン -位置付け-

原子力発電所の情報システムセキュリティに関する規制体系

【法律】

核原料物質、核燃料物質及び原子炉の規制に関する法律（炉規制法）
（第43条の3の2第2項）

【規則】

実用発電用原子炉の設置、運転等に関する規則（実用炉規則）
（第91条第2項第18号及び第19号）

【審査基準】

原子力規制委員会が別に定める基準

【ガイドライン】

原子力施設情報システムセキュリティ対策ガイドライン【新規】

出典：原子力規制委員会ホームページ：<https://www.da.nra.go.jp/detail/NRA001001390>

資料3 原子力施設情報システムセキュリティ対策ガイドラインの策定について 注：核物質防護のため内容は非公開

原子力に関する法規制の動向（国内）

- 核原料物質、核燃料物質及び原子炉の規制に関する法律（炉規制法）第43条 3の22第2項に以下の記載があり
 - － 発電用原子炉設置者は、発電用原子炉施設を設置した工場又は事業所において特定核燃料物質を取り扱う場合で政令で定める場合には、原子力規制委員会規則で定めるところにより、防護措置を講じなければならない。
- 実用発電用原子炉の設置、運転等に関する規則（実用炉規則）
第91条：防護措置 にてサイバーセキュリティに関する要求を規定
 - － 2-18 発電用原子炉施設及び特定核燃料物質の防護のために必要な設備又は装置の操作に係る情報システムは、電気通信回線を通じて妨害行為又は破壊行為を受けることがないように、電気通信回線を通じた当該情報システムに対する外部からのアクセスを遮断すること。
→外部からの通信の遮断
 - － 2-19 前号の情報システムに対する妨害行為又は破壊行為が行われるおそれがある場合又は行われた場合において迅速かつ確実に対応できるように適切な計画（第96条第1項において「情報システムセキュリティ計画」という。）を作成すること。
→サイバーセキュリティに関する対応計画の策定

2018年3月 原子力規制委員会第74回会議にて制定について言及

資料 3

原子力施設情報システムセキュリティ対策ガイドラインの策定について

平成30年3月20日
原子力規制庁

1. 目的

原子力施設における情報システムセキュリティの重要性は高く、近年における情報システムセキュリティ対策（以下「セキュリティ対策」という。）に関する技術的知見の進展、IAEAのセキュリティ対策に関する新規ガイダンスの策定作業の進捗、国内事業者のセキュリティ対策に関する経験の蓄積を踏まえ、今般、「原子力施設情報システムセキュリティ対策ガイドライン」（以下「ガイドライン」という。）を策定し、事業者自身によるセキュリティ対策の継続的な改善を実施する上で参考となる資料とするもの。

2. ガイドラインの構成

(1) はじめに

背景、構成、適用対象、目的、留意点

(2) 用語の定義

(3) 情報システムセキュリティ計画

(4) 対策編

①脅威及び脆弱性情報の評価

②管理的対策（体制、教育、訓練、調達）

③技術的対策（システム構成、データ入力制限、外部からの不正なアクセスの排除、ライフサイクル管理等）

④異常時対応（異常時対応計画、運用継続対策、バックアップ）

⑤防護措置の有効性評価

(5) 別冊資料

情報システムセキュリティ対策例

原子力施設情報システムセキュリティ対策ガイドラインの審査基準化

2021年4月 原子力規制委員会第4回臨時会議にて審査基準に位置付ける形で改正することを決定

資料2

原子力施設の核物質防護措置に係る審査基準の改正について（その2）

令和3年4月20日
原子力規制庁

1. 現行の情報システムセキュリティに関する制度について

原子力施設における情報システムセキュリティ対策については、核原料物質、核燃料物質及び原子炉の規制に関する法律（昭和32年法律第166号。以下「原子炉等規制法」という。）に基づく防護措置として、各事業規則及びその認可等の基準である核物質防護措置に係る審査基準（以下「審査基準」という。）において、次の事項を求めている。

（1）情報システムに対する外部からのアクセス遮断

（2）情報システムセキュリティ計画の作成

さらに、事業者が自主的に情報システムセキュリティ対策の向上を図ることを促すため、法令及び審査基準を補足するものとして「原子力施設情報システムセキュリティ対策ガイドライン」^{（注）}（以下「ガイドライン」という。）を制定している。

（注）原子力規制庁長官官房放射線防護グループ核セキュリティ部門「原子力施設情報システムセキュリティ対策ガイドライン」。平成30年3月15日第73回原子力規制委員会において了承されたもの。

2. 制度改正の経緯・背景について

平成30年にガイドラインを策定した際、事業者に対して、ガイドラインに記載されている対策の自主的な実施を促すとともに、今後、規制要求化する予定であることを説明した。また、同年のIAEAのIPPASフォローアップミッションにおいて、ガイドラインの規定事項の規制要求化の検討について助言があった。

今般、ガイドラインを参考にしつつ、発電用原子炉施設の情報システムセキュリティ対策について検査において確認を進めたところ、ガイドラインで示す情報システムセキュリティ対策は、施設が実施する情報システムセキュリティ対策の一環として定着しつつあることが確認できた。このため、ガイドラインの規定内容を審査基準に位置付ける改正を行うこととしたい。

原子力エネルギー協議会(ATENA)による自主ガイド ～目的～

- 2019年7月に第9回主要原子力施設設置者の原子力部門の責任者と原子力規制委員会との意見交換会にて、以下を目的として自主ガイドを策定していることを公表
- 本自主ガイドは2020年3月に発刊され、事業者は2022年度末までに各原子力事業者が自主ガイドに沿った安全対策を完了させることを第21回 総合資源エネルギー調査会 電力・ガス事業分科会 原子力小委員会にて公表

ATENA自主ガイド策定の目的

- ③ 海外の原子力規格であるIAEAガイドやNEIガイドは近年強化されており、ATENAは、それぞれの最新知見を踏まえ国内原子力産業界共通の基本方針や性能規定を具現化・明文化することが、サイバー攻撃の脅威に対する防護強化に有効であると考え、発電用原子炉施設のコンピュータ設備、特に、原子炉安全に関わるコンピュータ設備をサイバー攻撃から多層的に守ることを目的として、自主ガイド（案）を作成している。

原子力エネルギー協議会(ATENA)による自主ガイド ～構成～

マネジメント・
設備両面での
対策を規定

1. サイバーセキュリティマネジメント

- 組織及び責任
- 資産管理
- リスク及び適合性の評価
- 要員管理
- 調達管理

2. セキュリティ要件

- 多層防護
- セキュリティレベルについて

添付資料 セキュリティ対策

- セキュリティ対策の基本設計
- 技術対策例

3. 運用管理

- ライフサイクルのセキュリティ
発注(調達)／製作／輸送／運
用／保管／廃棄
- 既存設備の評価

4. インシデント対応

- インシデントの判別
- 異常時の対処

■ 設備対策

■ マネジメント対策

国内外の規格とガイドライン（まとめ）

	日本	IAEA	米国
勧告文書 Recommendations		IAEA Nuclear Security Series (NSS) No.13 "Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities"	
法、規制 Legal	・発電用原子炉施設への人の不法な侵入等の防止 ・実用発電用原子炉の設置、運転等に関する規則 ・実用発電用原子炉及びその附属施設の技術基準に関する規則		NRC 10 CFR 73.54 "Protection of digital computer and communication systems and networks"
ガイダンス Implementing Guides	原子力規制庁 「原子力施設情報システムセキュリティ対策ガイドライン」 「妨害破壊行為等の脅威」	IAEA NSS No.17-T "Computer Security Technique for Nuclear Facilities" IAEA NSS No.33-T "Computer Security of Instrumentation and Control Systems at Nuclear Facilities"	NRC REGULATORY GUIDE 5.71 "CYBER SECURITY PROGRAMS FOR NUCLEAR FACILITIES"
業界指針 Guideline	ATENA 「原子力発電所におけるサイバーセキュリティ対策導入自主ガイド」		NEI 08-09 "Cyber Security Plan for Nuclear Power Reactors"

03

原子力施設におけるサイバーセキュリティ対策

セキュリティ対策の基本的な考え方

1 ライフサイクル対策

設計から廃棄に至るまでライフサイクル全体にわたる対策が必要
(一度対策すれば終わりというものではない)



2 深層防護対策

重要度に応じ多重・多層の対策をとる



3 段階的対策

防止→監視→検知→復旧→防止→・・・
のサイクル

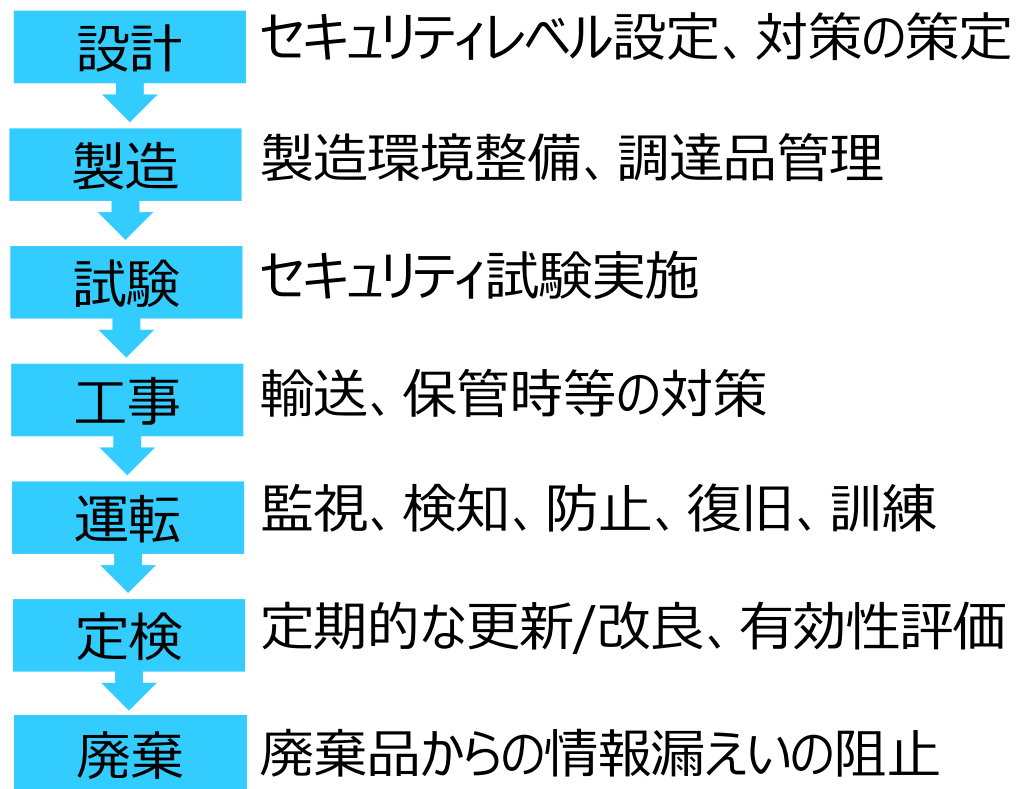


4 物理的対策／運用対策との連携

技術的な対策だけでなく物理的な対策、
運用対策も必要



ライフサイクル対策



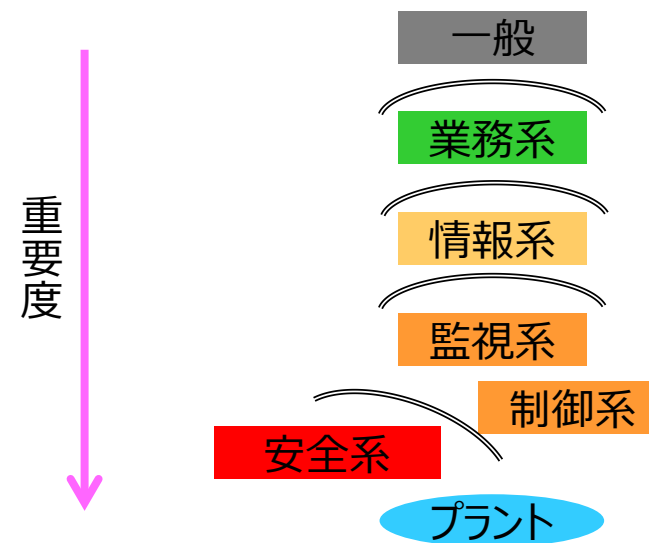
設計から廃棄までライフサイクル全体について対策が必要

深層防護対策：セキュリティレベル

設備の重要度に応じたセキュリティレベルを割り当て、レベルに応じた対策をとる

原子力のサイバーセキュリティに関する考え方は安全確保の考え方と同様の「深層防護」

設備の重要度に応じた「セキュリティレベル」を割り当て、レベル（重要度）の高さに応じた対策をとることとしている

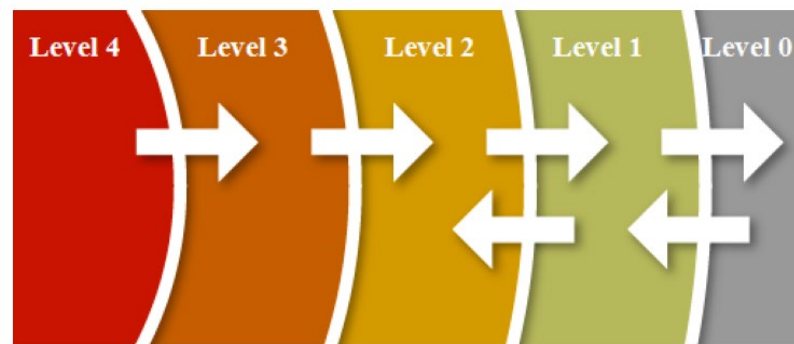


設備の重要度に応じたセキュリティレベルを割り当て、レベルに応じた対策をとる

RG5.71においてはレベル4（最重要）からレベル0の5段階にレベルが設定されており、また図に示す如くデータ方向に制限を設けている

（低いレベル（重要でない設備）から高いレベル（重要な設備）への情報の流れを許容しない）

R.G. 5.71による分類



※矢印はデータ方向の制限を表す

深層防護対策：セキュリティレベル

設備の重要度に応じたセキュリティレベルを割り当て、レベルに応じた対策をとる

IAEA NSS No.17においても同様に
5段階のレベルが規定されている
(レベル1が最重要：RGとは逆)

- レベル1：安全保護系
- レベル2：原子炉制御システム
- レベル3：中央制御室のプロセス監視設備
- レベル4：中央ハードコピー機や技術データベース等
- レベル5：OA機器等

IAEA NSS No.17による分類



深層防護対策：セキュリティレベル

レベル 1（例：安全保護系）

レベル 2 以降との情報の受信は不可。発信のみ可。

厳格なアクセス管理（遠隔アクセスは不可、物理的アクセスやアクセス可能なスタッフの制限、ツーマンルールの適用等）

レベル 2（例：原子炉制御システム）

レベル 2 ⇒ 3 への 1 方向通信のみ許容。なお、必要最小限の情報のみ受信可。

厳格なアクセス管理（遠隔アクセスは厳格な対策実施の上、特定ケースに限り受容、アクセス可能なスタッフの制限等）

レベル 3（例：中央制御室のプロセス監視設備）

外部への接続禁止。

キーリソースへのアクセスを監視。

システムへの物理的アクセスを管理する。

レベル 4 からの不正なトラフィックを防護するためゲートウェイを設置。

レベル 4（例：中央ハードコピー機や技術データベース等）

承認されたスタッフのみがシステムの変更を可能とする。

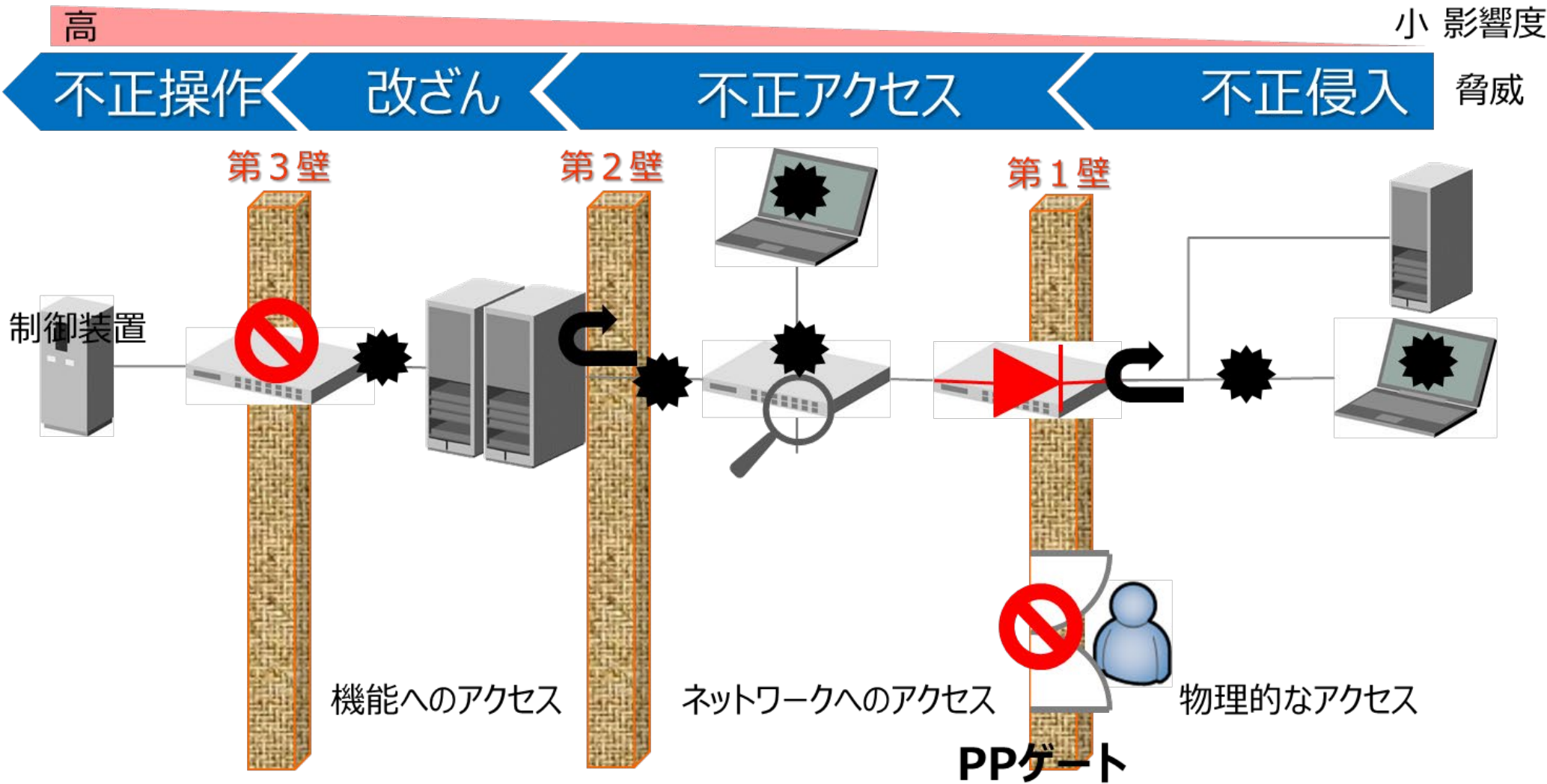
外部とのアクセスにあたり防護措置が講じられている。

外部からの不正なトラフィックを防護するためゲートウェイを設置。

レベル 5（例：OA機器等）

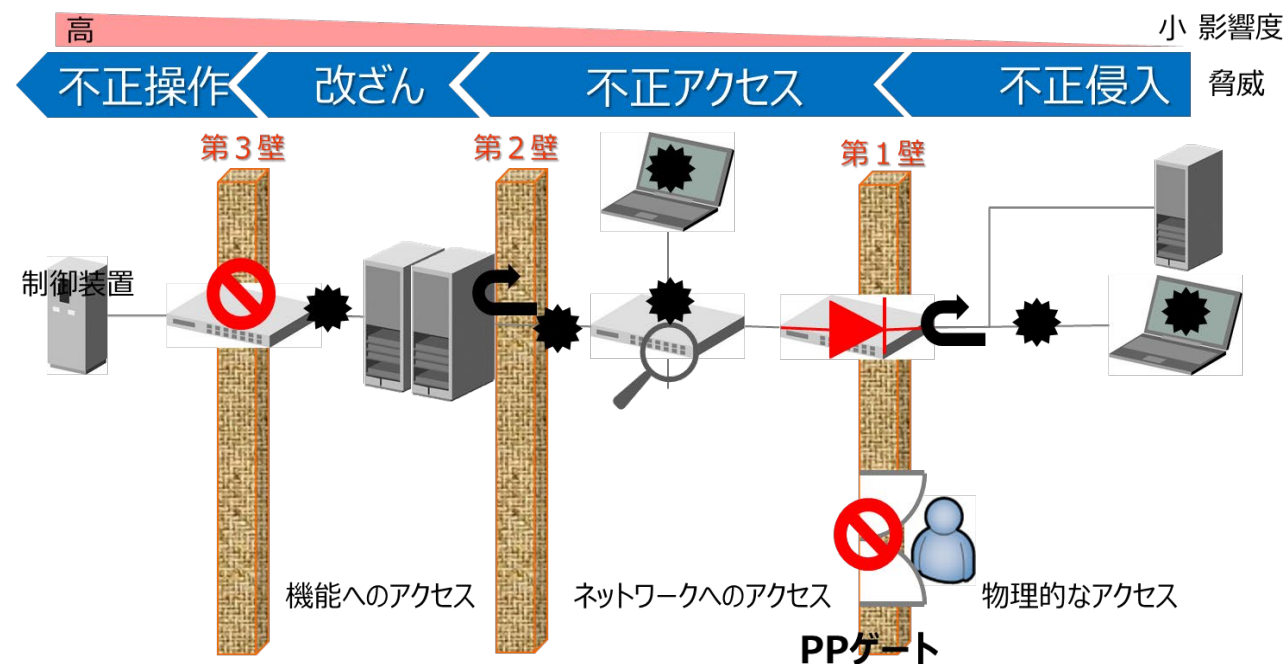
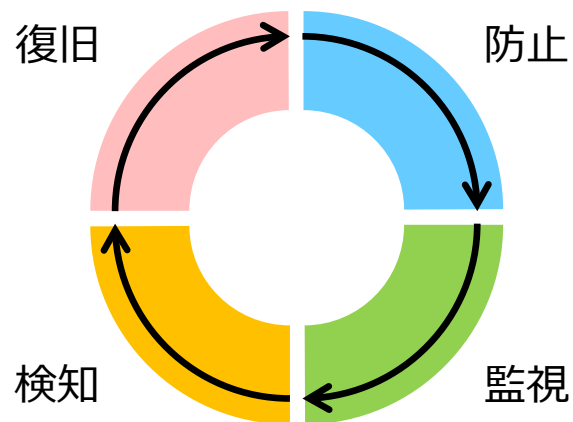
承認されたスタッフのみがシステムの変更を可能とする。

原子力発電所におけるサイバー攻撃の基本プロセス



段階的対策

1. 不正侵入を防止する
2. 不正アクセスされたことを監視する
3. 改ざんされたことを検知する
4. 不正操作されたものを復旧する



物理的対策／運用対策との連携

セキュリティ対策例（R.G. 5.71より）

・ 技術的なセキュリティ対策

- ✓ アクセス管理 : ログイン、ロック、プロトコル制限、等
- ✓ 通信の防護 : 送信の健全性、暗号の使用、等
- ✓ 識別と認証 : ユーザー識別、パスワード、認証コード、等
- ✓ システムの安全強化 : 不要なサービス除去、侵入検出、等

・ 物理的対策、運用対策

- ✓ 媒体の防護 : 媒体のアクセス、輸送、機密情報、等
- ✓ システム/情報の健全性 : 監視ツール、警報、等
- ✓ 保守 : 保守ツール、保守要員、等
- ✓ 物理的防護と環境防護 : エスコート、ビジター管理、等
- ✓ 防護戦略 : Security levelに応じた対策立案の要求
- ✓ 多重防護 : 同一Level内、Level間のルールを記載
- ✓ 異常事態対応 : 訓練、試験とドリル、対応、監視、報告、等
- ✓ 緊急時対応方策と対応機能 : 計画、試験、訓練、回復、等
- ✓ 認識と訓練 : 認識の訓練、教育、専門的な訓練、等
- ✓ 構成管理 : ベースライン、変更管理、等
- ✓ システムとサービスの購入 : Supply chain threat対策等
- ✓ セキュリティ評価とリスク管理

物理的対策／運用対策との連携

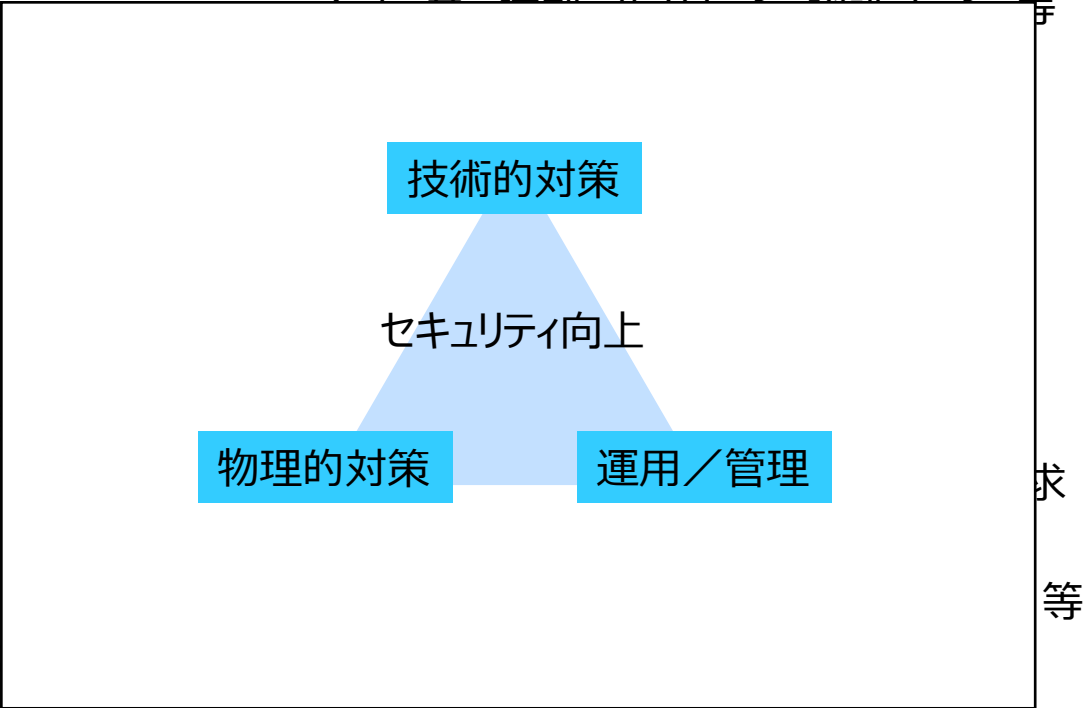
セキュリティ対策技術的対策だけでなく、物理的対策、運用対策との連携が必要

• 技術的なセキュリティ対策

- ✓ アクセス管理 : ログイン、ロック、プロトコル制限、等
- ✓ 通信の防護 : 送信の健全性、暗号の使用、等
- ✓ 識別と認証 : ユーザー識別、パスワード、証明書、等
- ✓ システムの安全強化

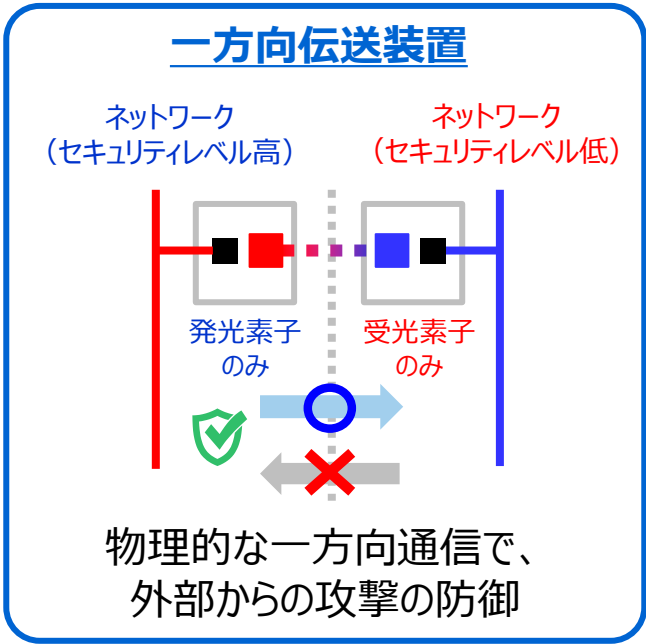
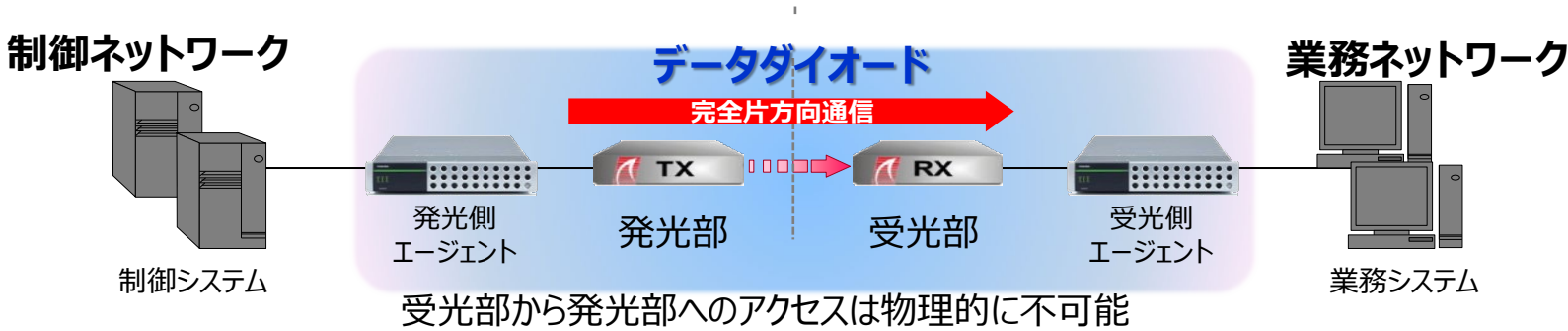
• 物理的対策、運用対策

- ✓ 媒体の防護
- ✓ システム/情報の健全性
- ✓ 保守
- ✓ 物理的防護と環境防護
- ✓ 防護戦略
- ✓ 多重防護
- ✓ 異常事態対応
- ✓ 緊急時対応方策と対応
- ✓ 認識と訓練 : 認識の訓練、教育、専門的な訓練、等
- ✓ 構成管理 : ベースライン、変更管理、等
- ✓ システムとサービスの購入 : Supply chain threat対策等
- ✓ セキュリティ評価とリスク管理



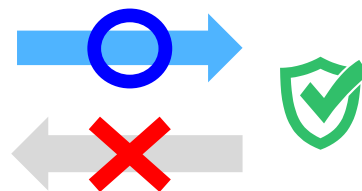
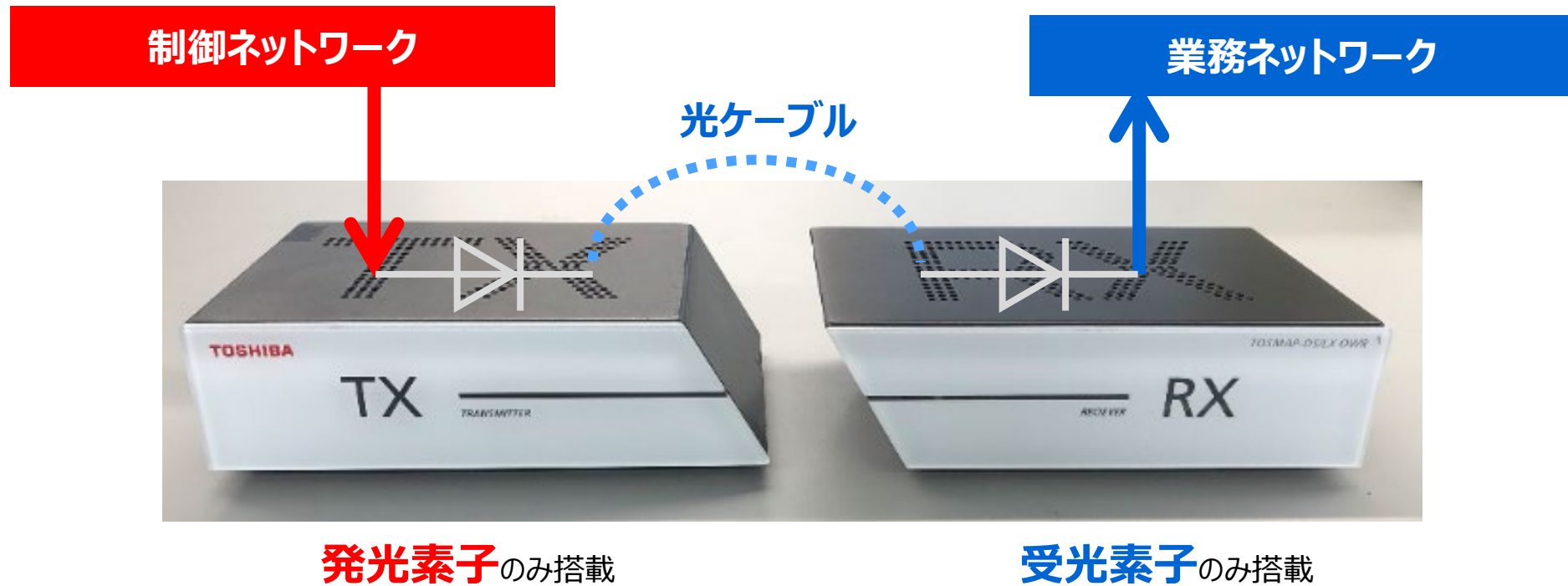
技術的セキュリティ対策の一例（データダイオード）

データダイオード・・・片方向通信を物理的に実現



データダイオードの製品例：TOSMAP-LX OWR

データダイオード・・・片方向通信を物理的に実現



セキュリティ運用対策の一例（セキュリティ訓練）

運転訓練シミュレータを用いたサイバーセキュリティ訓練の提供

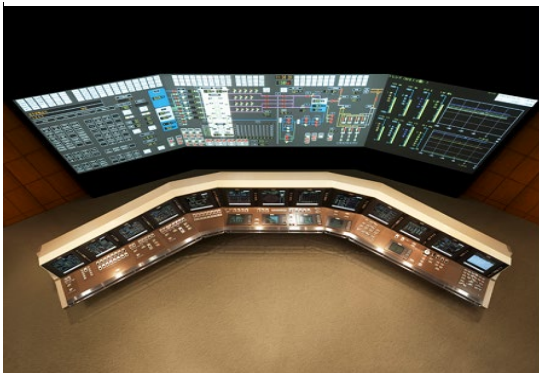
PCシミュレータ



運転員と関連部署との連携を主目的とした訓練に有効です。

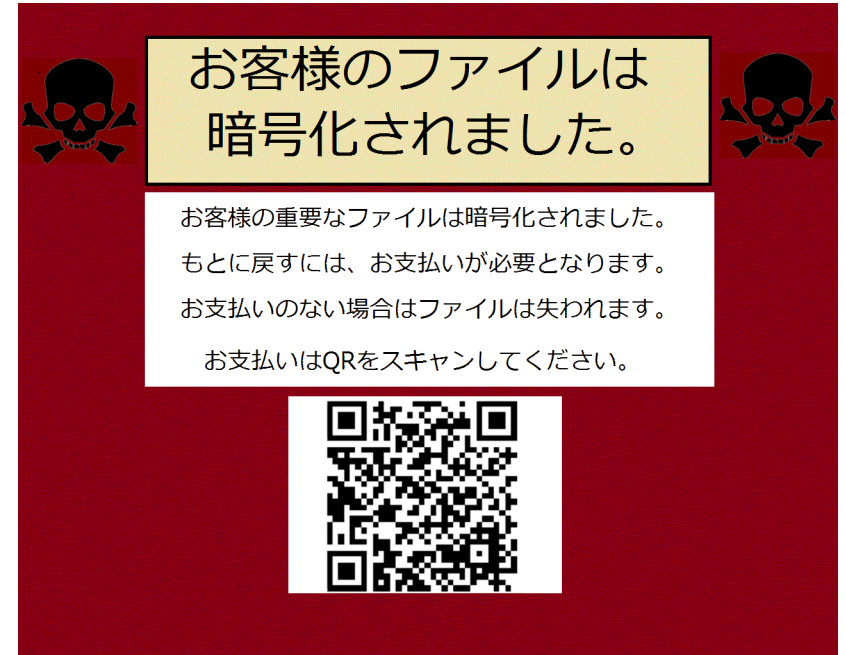
PCシミュレータはフルスコープと同等の機能を可搬型のPCで実現するものであり、各サイトへの持ち込み及びリモートでの実施に対応できます。

運転訓練シミュレータ設備



運転員の対応及び中操内の連携を主目的とした訓練において有効です。

実際の運用に近い環境（機器及び人員）において臨場感の高い訓練を実現します。



運転訓練シミュレータ上でランサムウェアによる攻撃も模擬可能

TOSHIBA