JPCERT Coordination Center

電子署名者 : JPCERT Coordination Center
DN : c=JP, st=Tokyo, l=Chuo-ku, o=Japan Computer Emergency Response Team Coordination Center, cn=JPCERT Coordination Center, email=office@jpcert.or.jp
日付 : 2019.03.25 12:00:35 +09'00'

鉄道分野における制御システム セキュリティ対策の検討

２０１９年２月１５日
独立行政法人情報処理推進機構（IPA）
産業サイバーセキュリティセンター（ICSCoE）
中核人材育成プログラム受講生
別所 佑樹

目次

© Information-technology Promotion Agency, Japan Industrial Cyber Security Center of Excellence

１．ICSCoEの概要と中核人材育成プログラム

© Information-technology Promotion Agency, Japan　Industrial Cyber Security Center of Excellence

産業サイバーセキュリティセンター

Industrial Cyber Security Center of Excellence（ICSCoE）

【事業内容】
- 人材育成事業
- 実際の制御システムの安全性・信頼性検証事業
- 攻撃情報の調査・分析事業

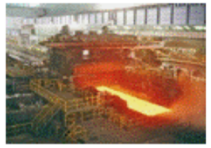
- ✓ 海外では**サイバー攻撃**により重要インフラ・社会基盤の**安全が脅かされる事案**が発生
- ✓ 我が国の経済・社会を支える重要インフラや産業基盤の**サイバー攻撃に対する防御力**を抜本的に強化する必要性
- ✓ ２０１７年４月１日発足

原発の制御システム停止（米国、2003年）

発電所の制御システムがウィルスに感染。制御システムが約５時間にわたって停止。

製鉄所の溶鉱炉損傷（ドイツ、2014年）

何者かが製鉄所の制御システムに侵入し、不正操作をしたため、生産設備が損傷。



大規模停電の発生（ウクライナ、2015年）

マルウェアの感染により、変電所が遠隔制御された結果、数万世帯で3～6時間にわたる大停電が発生。

※ IPAの資料を参考に記載

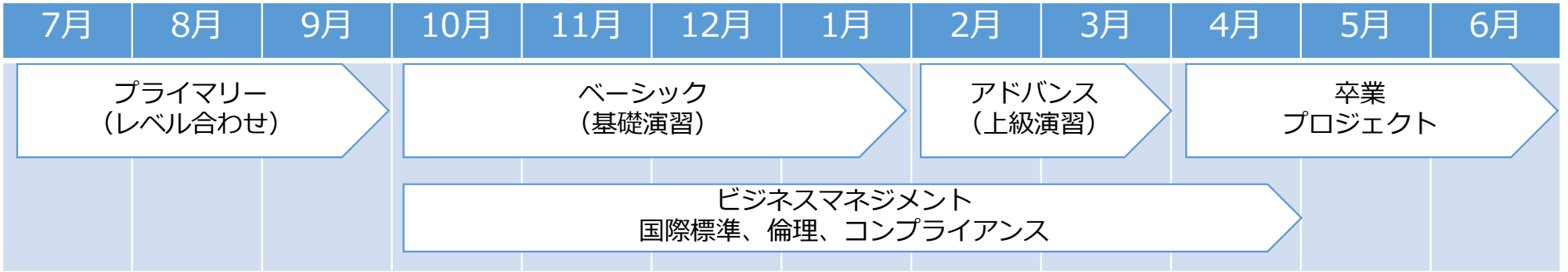
© Information-technology Promotion Agency, Japan　Industrial Cyber Security Center of Excellence

中核人材育成プログラム

中核人材
育成プログラム

- 将来、企業などの経営層と現場担当者を繋ぐ、”中核人材”を担う方を対象としたプログラム
- テクノロジー（OT・IT）、マネジメント、ビジネス分野を総合的に学ぶ１年間のトレーニング

- ✓ ２０１７年７月 第１期 開講
- ✓ 参加者数：
  【第１期】７６名
  【第２期】８３名



※ IPAの資料を参考に記載

© Information-technology Promotion Agency, Japan　Industrial Cyber Security Center of Excellence

２．鉄道分野におけるサイバーセキュリティ

© Information-technology Promotion Agency, Japan　Industrial Cyber Security Center of Excellence

鉄道分野におけるサイバー攻撃事例①

◘ ウクライナにおけるサイバー攻撃【2015年12月】

KillDisk and BlackEnergy Are Not Just Energy Sector Threats

Posted on: February 11, 2016 at 10:47 am **Posted in:** Malware, Targeted Attacks
Author: Kyle Wilhoit (Senior Threat Researcher)

Our new intelligence on BlackEnergy expands previous findings on the first wide-scale coordinated attack against industrial networks. Based on our research that we will further outline below, attackers behind the outages in two power facilities in Ukraine in December likely attempted similar attacks against a mining company and a large railway operator in Ukraine.

This proves that BlackEnergy has evolved from being just an energy sector problem; now it is a threat that organizations in all sectors—public *and* private—should be aware of and be prepared to defend themselves from. While the motivation for the said attacks has been the subject of heavy speculation, these appear to be aimed at crippling Ukrainian public and criticial infrastructure in what could only be a politically motivated strike.

出典：“KillDisk and BlackEnergy Are Not Just Energy Sector Threats”. TREND MICRO SECURITY INTELIGENCE Blog. https://blog.trendmicro.com/trendlabs-security-intelligence/killdisk-and-blackenergy-are-not-just-energy-sector-threats/, (2018-10-1).

- 「BlackEnergy」及び「KillDisk」を用いたサイバー攻撃により、ウクライナの電力発電所２ヶ所で稼働停止が発生
- 大手鉱業会社に対する攻撃において「BlackEnergy」や「KillDisk」関連の検体が確認された
- 大手鉄道会社に対する攻撃においても「KillDisk」関連の検体が確認された

© Information-technology Promotion Agency, Japan Industrial Cyber Security Center of Excellence

鉄道分野におけるサイバー攻撃事例②

◘ デンマーク国鉄(DSB)へのDDoS攻撃【2018年5月10日】

Cyber attack hits Danish rail network

Ritzau/The Local
news.denmark@thelocal.com
@thelocaldenmark

14 May 2018
10:55 CEST+02:00

cyber security
dsb
rail

Share this article

File photo: Henning Bagger/Ritzau Scanpix

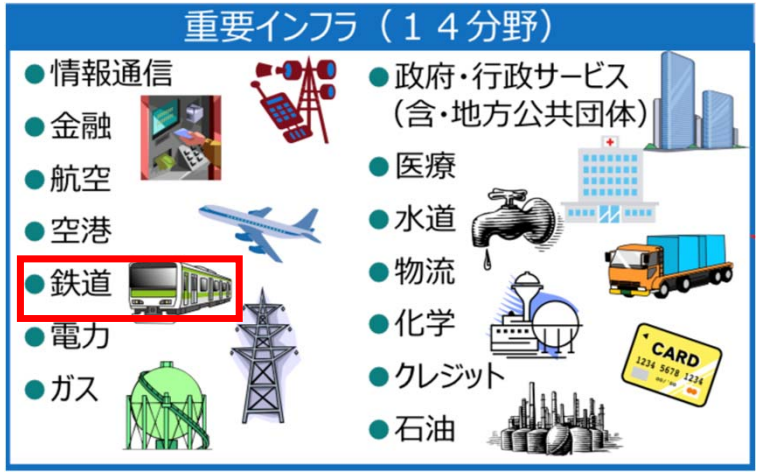
Danish state rail operator DSB was the victim of an unprecedented DDoS cyber attack, the company confirmed on Monday.

- デンマーク国鉄（DSB）が大規模DDoS攻撃を受けた
- アプリ、券売機、ウェブサイト経由、セブンイレブン店舗でも切符を購入できない状態が続いた
- 社内メールや電話システムも影響を受けた

出典：“Cyber attack hits Danish rail network”. The Local. https://www.thelocal.dk/20180514/cyber-attack-hits-danish-rail-network, (2018-5-14).

© Information-technology Promotion Agency, Japan Industrial Cyber Security Center of Excellence

鉄道分野における制御システム



出典: NISC “重要インフラの情報セキュリティ対策に係る第４次行動計画の概要”
(https://www.nisc.go.jp/active/infra/pdf/infra_rt4_abst.pdf)

◘ 列車運行管理システム

・列車の運行を集中して自動制御するシステム
・列車集中制御装置（CTC）、自動進路制御装置（PRC）などから構成される

◘ 電力管理システム

・車両等に電力を供給するため、変電所を監視制御するシステム

◘ 座席予約システム

・座席指定券の予約、発券等を行うシステム

<u>様々なシステムの安定稼働により安全・安定輸送を確保</u>

※事業者によって、システムの構成や備える機能は様々

© Information-technology Promotion Agency, Japan　Industrial Cyber Security Center of Excellence

国際標準・業界標準

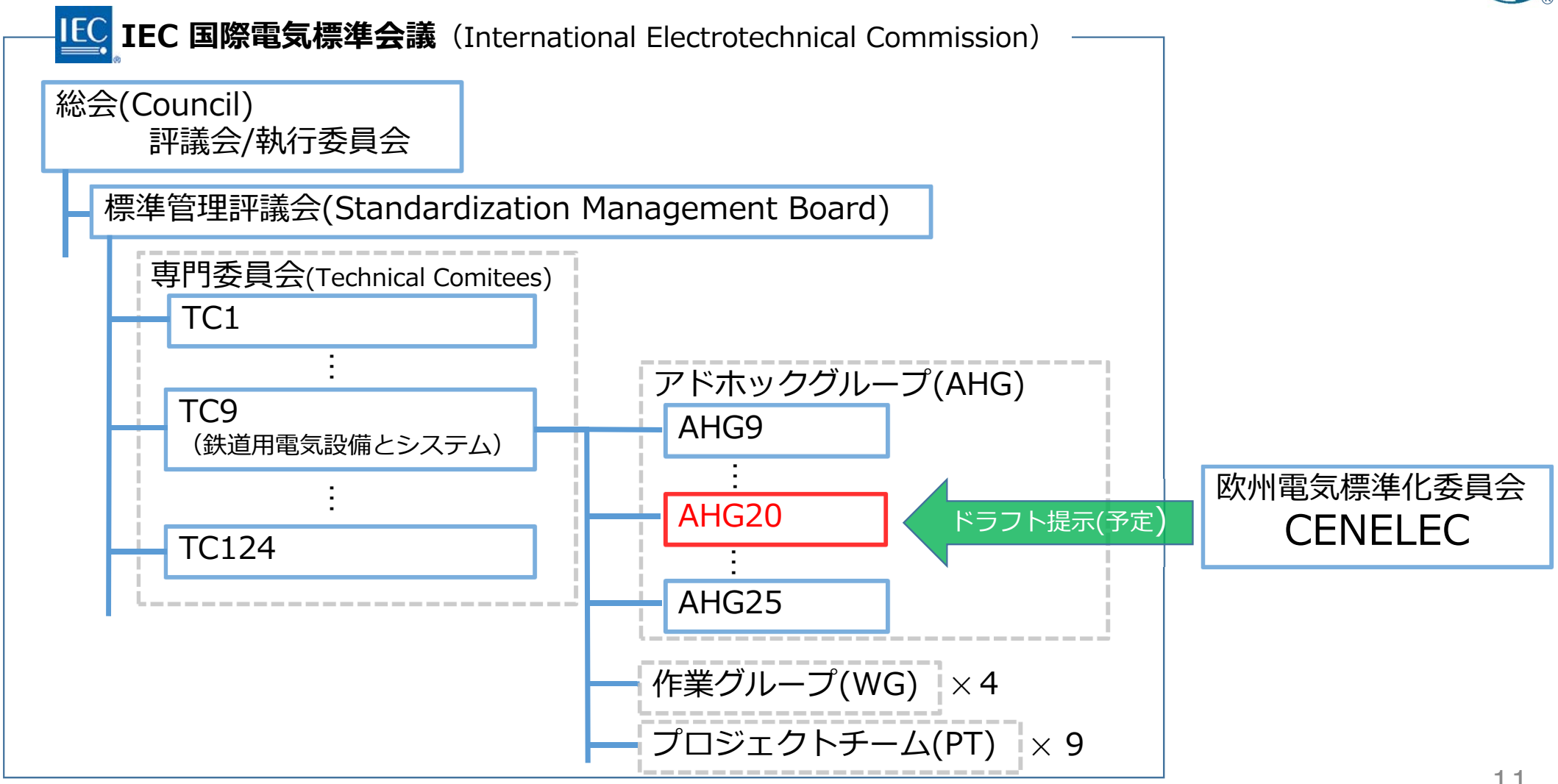
	汎用制御システム	電力	石油・化学プラント	鉄道システム
組織	IEC 62443 / SSA / NIST SP800-82	IAEA 核セキュリティ勧告Rev.05 / NERC CIP / NIST IR 7628	WIB	ISO/IEC 62278 (RAMS)
システム	IEC 62443 / SSA / NIST SP800-82		WIB	ISO/IEC 62280
装置・デバイス	IEC 62443 / ISCI EDSA / NIST SP800-82	IEEE 1686	WIB	
技術（暗号など）	ISO/IEC 29192	IEC 61850 / IEC 62351		IEC 62279
【参考】国内ガイドライン		・電力制御システムセキュリティガイドライン【JESC】 ・スマートメータシステムセキュリティガイドライン【JESC】	・石油分野における情報セキュリティ確保に係る安全ガイドライン【石油連盟】 ・石油化学分野における情報セキュリティ確保に係る安全基準【石油化学工業協会】	・鉄道分野における情報セキュリティ確保に係る安全ガイドライン【国土交通省】

出典：「制御システムにおけるセキュリティマネジメントの構築に向けて～IEC62443 2-1の活用のアプローチ」(情報処理推進機構)を基に作成
https://www.ipa.go.jp/files/000014265.pdf

国際標準　業界標準（規格）

© Information-technology Promotion Agency, Japan　Industrial Cyber Security Center of Excellence

鉄道分野における標準化の動向



2019年1月24日時点

© Information-technology Promotion Agency, Japan Industrial Cyber Security Center of Excellence

国内の指針・ガイドライン等

【法律】サイバーセキュリティ基本法（平成２８年４月２２日公布、平成２８年１０月２１日施行）

【戦略】サイバーセキュリティ戦略（平成３０年７月２７日閣議決定）

重要インフラ
１４分野

【行動計画】重要インフラの情報セキュリティ対策に係る第４次行動計画

平成２９年４月１８日サイバーセキュリティ戦略本部決定
平成３０年７月２５日サイバーセキュリティ戦略本部改定

- 先導的取組の推進
- オリパラ大会も見据えた情報共有体制の強化
- リスクマネジメントを踏まえた 対処態勢整備の推進

安全基準等の策定 | 情報共有体制の強化 | 障害対応体制の強化

リスクマネジメント及び対処態勢の整備 | 防護基盤の強化

【指針】重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針
（平成３０年４月４日サイバーセキュリティ戦略本部）

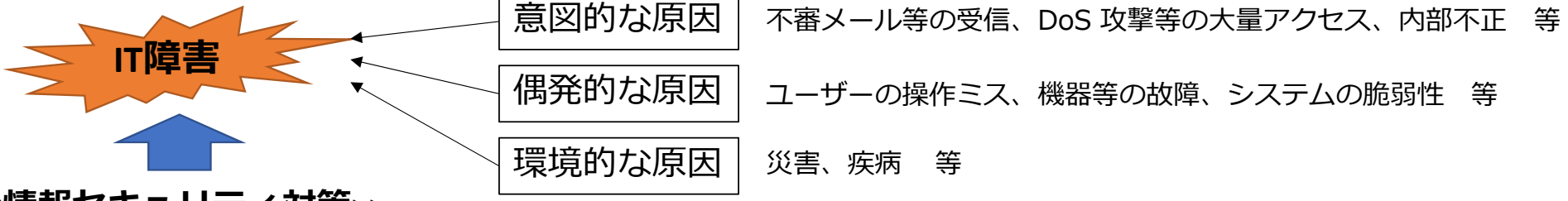
鉄道分野

【ガイドライン】鉄道分野における情報セキュリティ確保に係る安全ガイドライン
（平成２８年４月１日国土交通省改定）

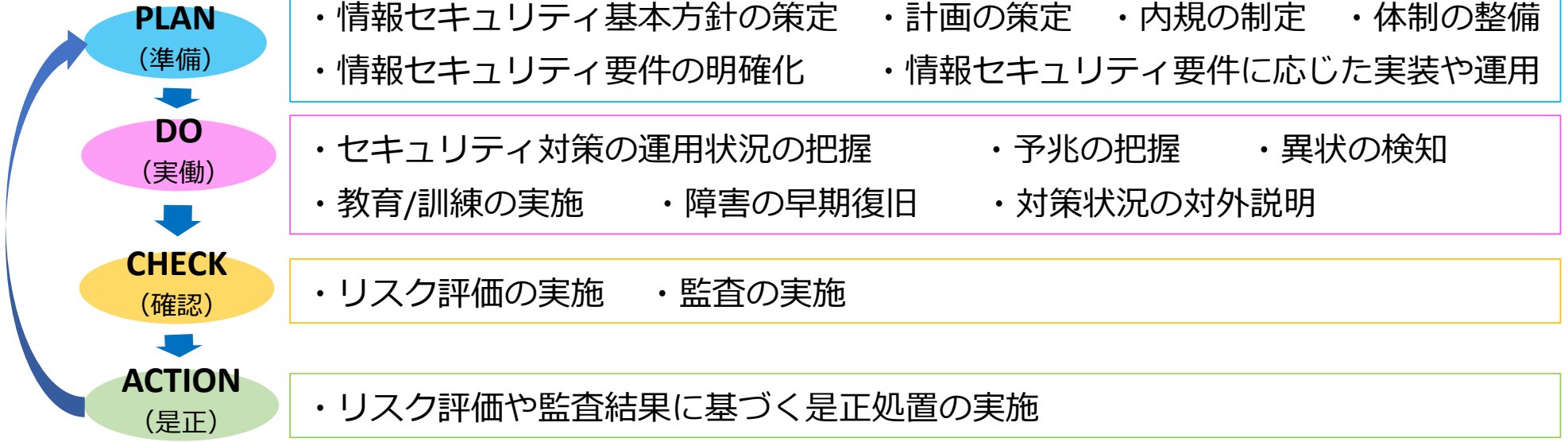
© Information-technology Promotion Agency, Japan Industrial Cyber Security Center of Excellence

鉄道分野における情報セキュリティ確保に係る安全ガイドライン

- ✓ 各事業者が、重要インフラの担い手としての意識に基づいて自主的な取り組みにおける努力や検証をするための目標を定めるもの
- ✓ 鉄道分野における情報セキュリティ対策の現状と課題を踏まえ、事業特性に応じた対策項目を推奨基準としてまとめたもの



<<情報セキュリティ対策>>



© Information-technology Promotion Agency, Japan　Industrial Cyber Security Center of Excellence

制御システムと情報システムの違い

カテゴリ	制御システム（OT）	情報システム（IT）
可用性（A）	必要性　高 ２４時間３６５日稼働など	必要性　中 休止や遅れが許容される場合あり
完全性（I）	必要性 高	必要性 中
機密性（C）	必要性 低～中	必要性 高
リアルタイム性	必要性　高 遅れが許容されない場合が多い	必要性　中 遅れが許容される場合あり
システム利用期間	１０～２０年	３～５年
プロトコルの種類	限定的	非常に多い
パッチ適用	容易に適用不可	定期的に適用
ウイルス対策	一般的ではない	一般的

情報システムのセキュリティ対策を制御システムへ容易に適用することは困難

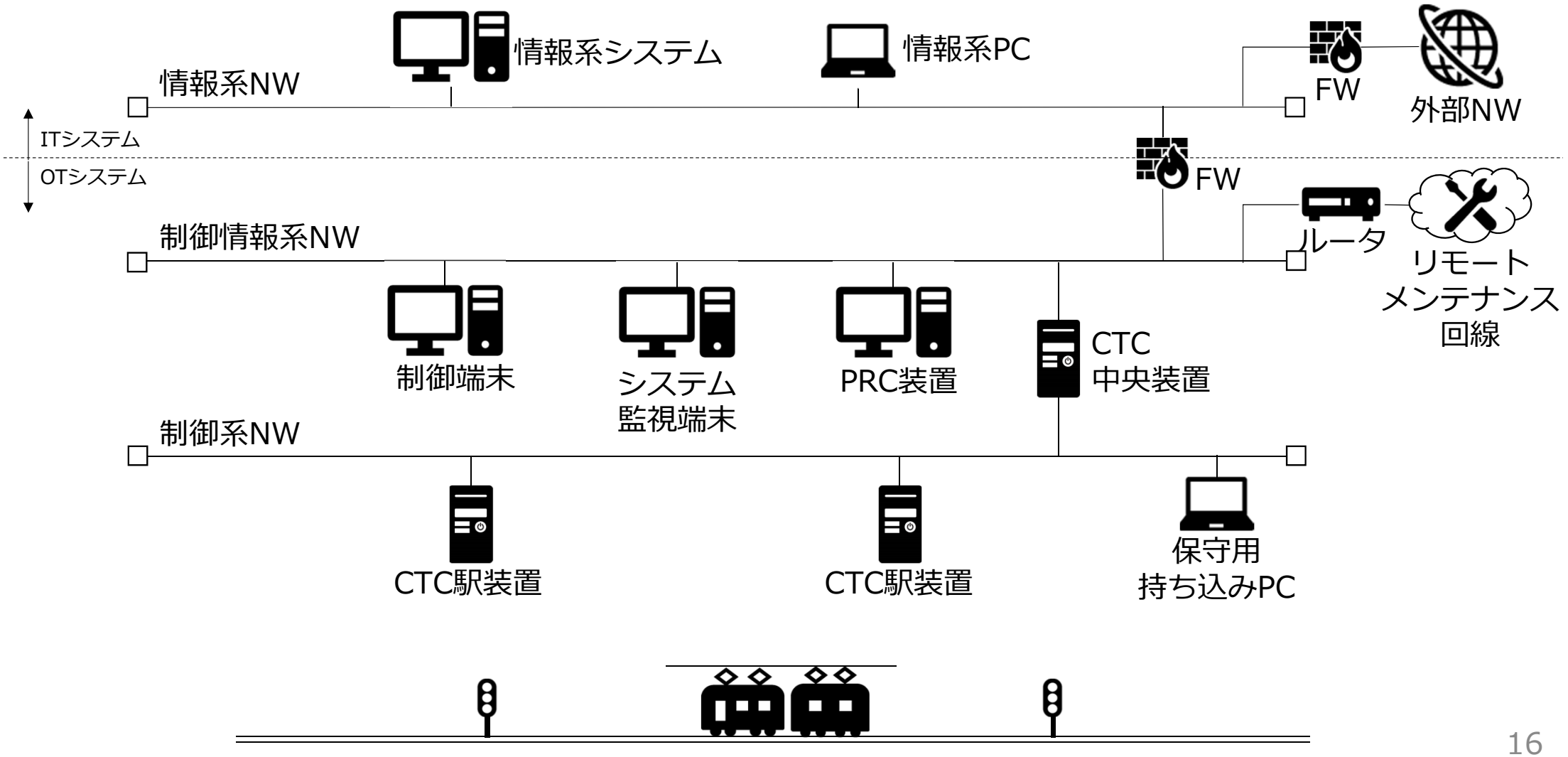
各システムに応じたセキュリティ対策の検討が必要

© Information-technology Promotion Agency, Japan　Industrial Cyber Security Center of Excellence

３．鉄道分野の制御システムに対する代表的なサイバー攻撃の侵入経路

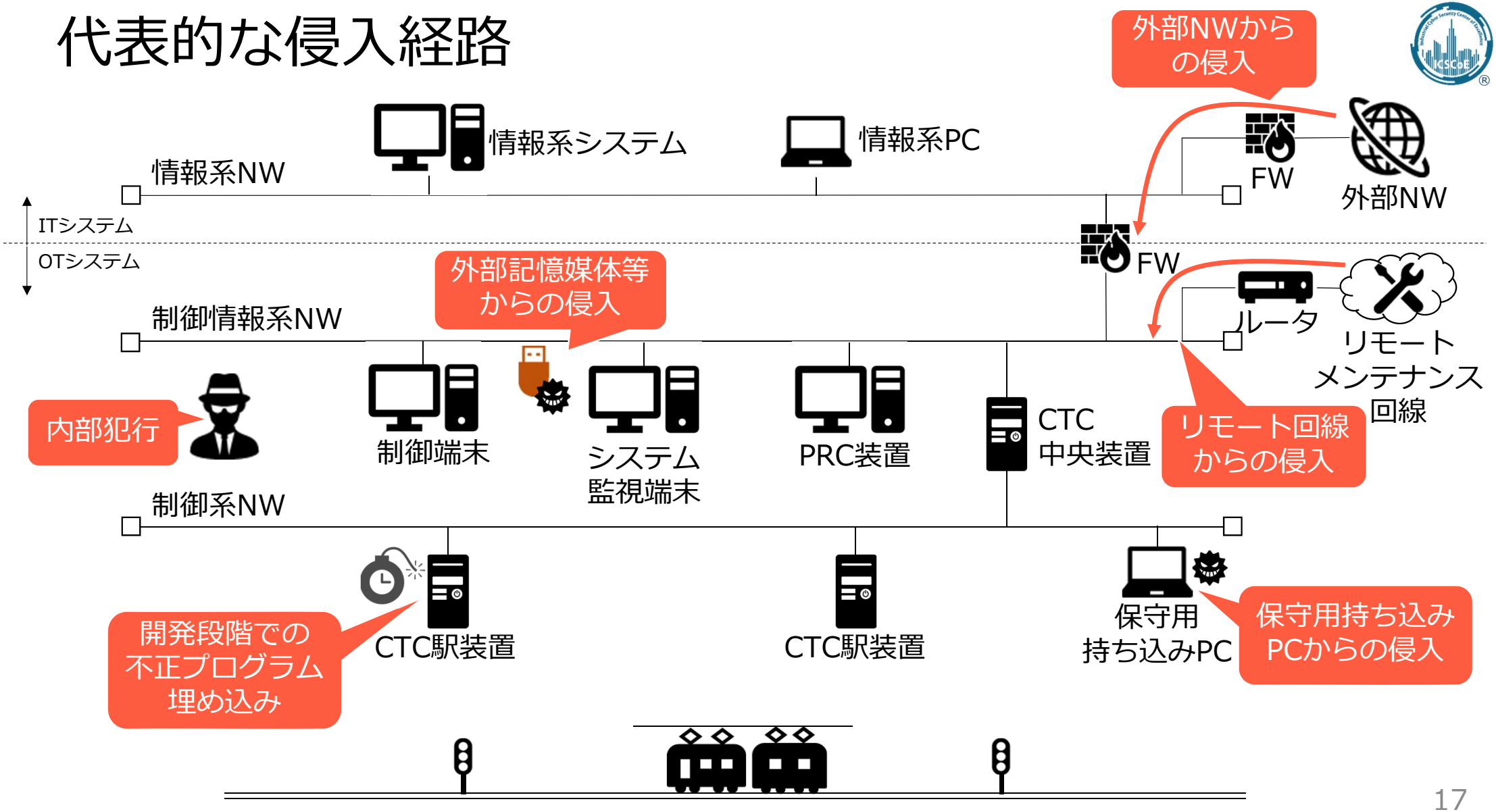
© Information-technology Promotion Agency, Japan　Industrial Cyber Security Center of Excellence

一般的な列車運行管理システムの構成例



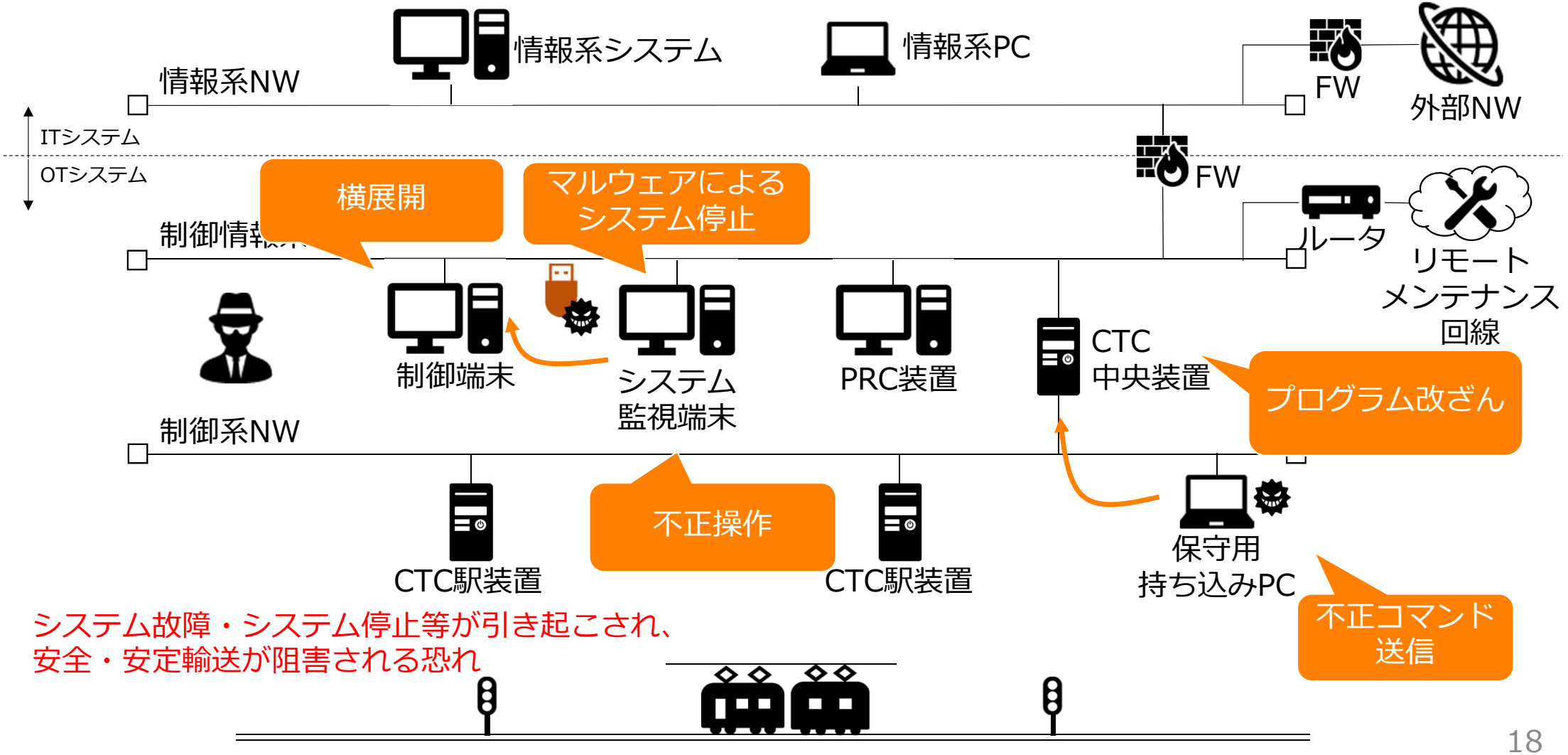
© Information-technology Promotion Agency, Japan Industrial Cyber Security Center of Excellence

代表的な侵入経路



© Information-technology Promotion Agency, Japan Industrial Cyber Security Center of Excellence

侵入後の脅威例



システム故障・システム停止等が引き起こされ、
安全・安定輸送が阻害される恐れ

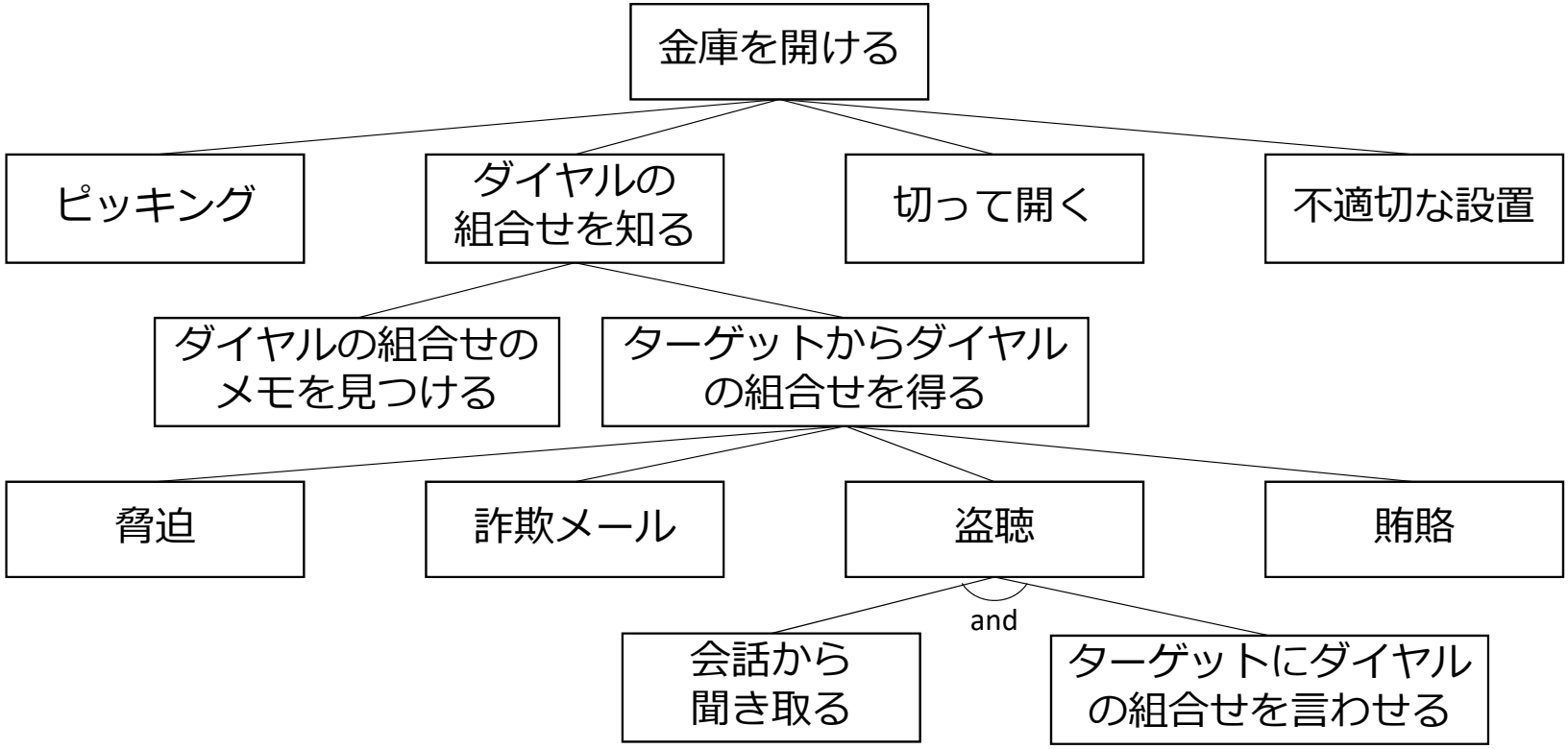
© Information-technology Promotion Agency, Japan Industrial Cyber Security Center of Excellence

４．脅威分析と対策の検討

© Information-technology Promotion Agency, Japan　Industrial Cyber Security Center of Excellence

Attack Tree Analysis

システムのセキュリティを分析する脅威分析手法の１つ。[1]
システムに対する攻撃を、木構造でより詳細な手段へと分解。
その攻撃の組み合わせや実現可能性など様々な切り口で攻撃の特性を分析することが可能。
各ノードはANDノードとORノードからなり、ANDノードはその攻撃を実現するための異なるステップを表す。



[1] B.Schneier, “Attack trees: modeling security threats,” Dr. Dobb’s Journal December 1999.

© Information-technology Promotion Agency, Japan Industrial Cyber Security Center of Excellence

侵入経路ごとの脅威分析の例

投影のみ

投影のみとさせていただきます。

© Information-technology Promotion Agency, Japan　Industrial Cyber Security Center of Excellence

侵入経路ごとの攻撃手段と対策例

投影のみ

投影のみとさせていただきます。

© Information-technology Promotion Agency, Japan　Industrial Cyber Security Center of Excellence

侵入後の脅威と対策例

投影のみ

投影のみとさせていただきます。

© Information-technology Promotion Agency, Japan　Industrial Cyber Security Center of Excellence

５．優先的に実施すべき対策の検討

© Information-technology Promotion Agency, Japan　Industrial Cyber Security Center of Excellence

優先順位の選定基準

1　攻撃の実現可能性

攻撃手段のうち、比較的実現可能性が高い攻撃への対策を優先する。

2　対策に要する期間

世界が日本に注目する大規模イベントを見据え、比較的短期に実施できる対策を優先する。

3　対策に要するコスト

運用改善や設定の見直し等、対策コストが比較的低い対策を優先する。

© Information-technology Promotion Agency, Japan　Industrial Cyber Security Center of Excellence

優先的に実施すべき対策例

セキュリティの現状確認

- リスクアセスメントやセキュリティ診断、機器の設定や運用の見直し

セキュリティ管理体制の強化

- NW構成管理や脆弱性情報管理

物理セキュリティ対策

- 入退室管理の徹底、ポート閉塞

社員に対するセキュリティ教育

- 外部記憶媒体等の取扱いやソーシャルエンジニアリングの危険性等

外部委託における対策

- 保守用持込PCの管理状況やログ監査、複数人作業の徹底

© Information-technology Promotion Agency, Japan　Industrial Cyber Security Center of Excellence

6．まとめ

© Information-technology Promotion Agency, Japan　Industrial Cyber Security Center of Excellence

まとめ

- 鉄道分野におけるサイバーセキュリティ
  - ✓ 鉄道分野もサイバー攻撃の標的になると認識する
  - ✓ 鉄道分野の制御システムセキュリティにも標準化の動き

- 鉄道分野の制御システム
  - ✓ システムにより構成や備える機能などは様々
  - ✓ 各システムごとにセキュリティ対策の検討が必要
    - ⇒ 今回はその一例として、列車運行管理システムの一般的な構成例を基に脅威分析・対策の検討について紹介

<u>各システムに応じた対策の検討と継続的な改善により</u>
<u>安全で安定した輸送サービスを提供する</u>

© Information-technology Promotion Agency, Japan Industrial Cyber Security Center of Excellence