Supported by 日本財団 THE NIPPON FOUNDATION

東京オリンピック・パラリンピックに向けた 交通機関へのサイバーテロ対策に関する調査研究

（一般財団法人）運輸総合研究所
研究員　町山　友和

2017年5月23日

本日の報告内容

1. はじめに
2. 近年におけるサイバー攻撃事例
3. 国内の鉄道、航空分野における事業者実態調査（2015年度実施）
4. 鉄道、航空分野におけるサイバーテロ対策
5. おわりに

本日の報告内容

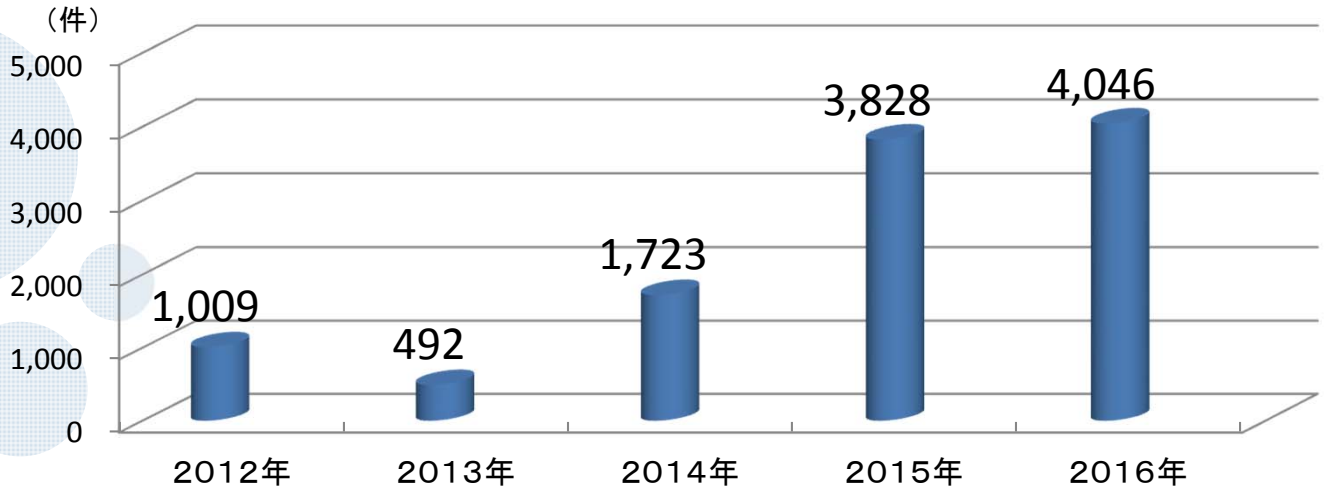
1. はじめに
2. 近年におけるサイバー攻撃事例
3. 国内の鉄道、航空分野における事業者実態調査（2015年度実施）
4. 鉄道、航空分野におけるサイバーテロ対策
5. おわりに

1. はじめに

【研究の背景】我が国に対するサイバー攻撃

近年、政府機関、企業に対するサイバー攻撃が急増

- 2015年；日本年金機構へのサイバー攻撃
- 2016年；大手旅行会社関連会社へのサイバー攻撃
- 2017年；某ホテルや政府・企業へのサイバー攻撃、ランサムウェア・・・



出典：警察庁「平成28年中のサイバー空間をめぐる脅威の情勢について」

サイバーセキュリティ対策は重要な課題

1. はじめに

【研究の背景】過去のオリンピックへのテロ攻撃

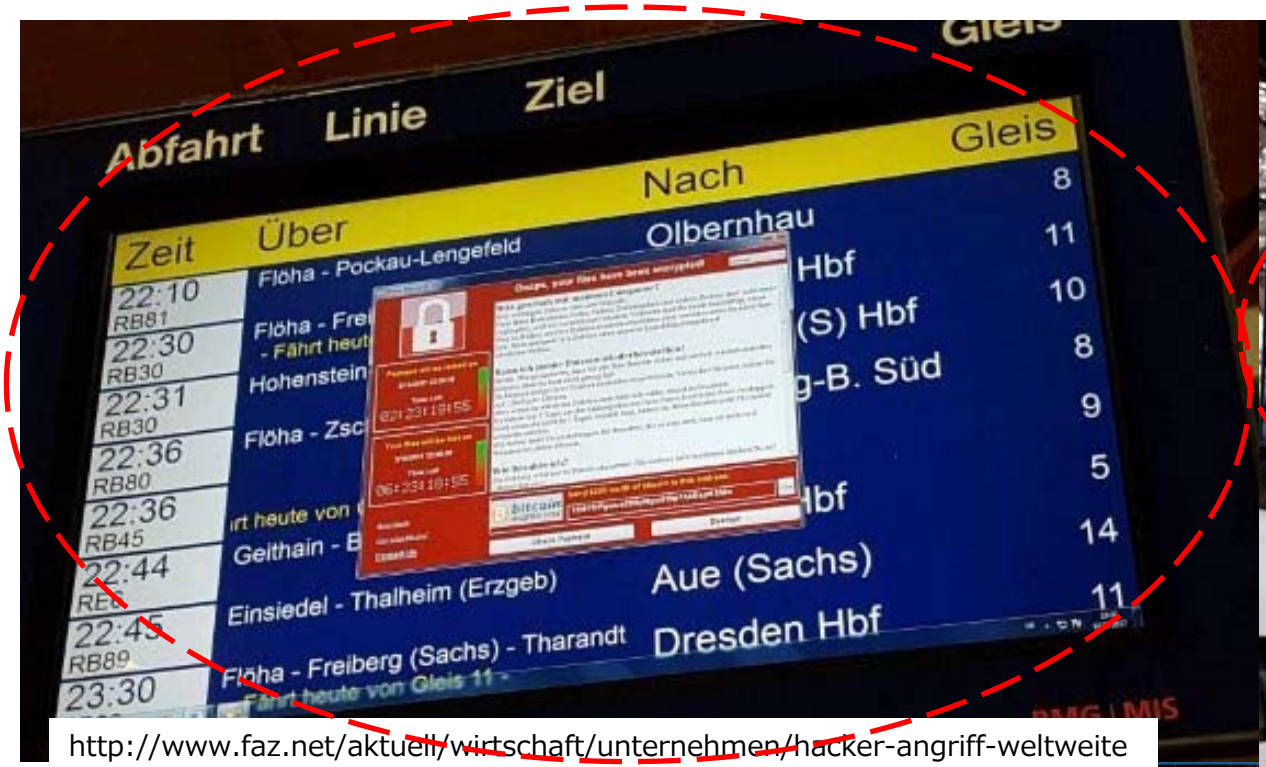
社会的な影響から、テロの標的になる・・・サイバーテロでは？

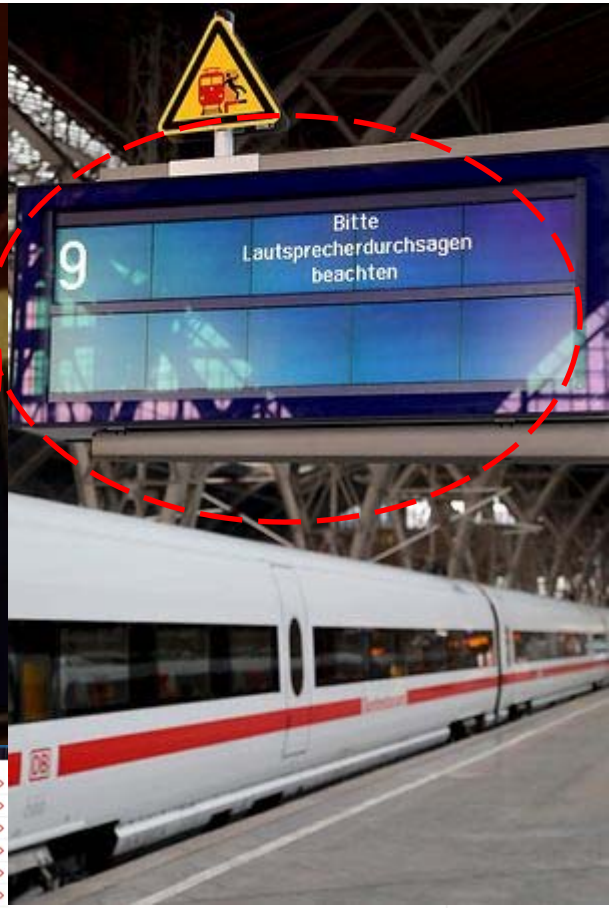
- ロンドン大会　サイバー攻撃
  ⇒公式サイトに2億回超の不正アクセス
- リオ大会　サイバー攻撃
  ⇒2千万回以上不正アクセスや大規模なDDoS攻撃

東京大会においては、更なる攻撃が懸念される

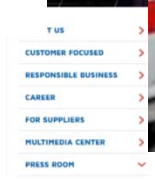
1. はじめに

【研究の背景】鉄道、航空への輸送に対するサイバー攻撃





http://www.faz.net/aktuell/wirtschaft/unternehmen/hacker-angriff-weltweite-cyberattacke-trifft-computer-der-deutschen-bahn-15013583.html



我が国においても重大な脅威と考えられる

Supported by 日本財団 THE NIPPON FOUNDATION

1. はじめに

【研究の目的】

想定される脅威

- 近年、我が国へのサイバー攻撃が頻発
- 過去の五輪大会では多くの攻撃
- 海外では鉄道、航空へも攻撃

東京オリンピック・パラリンピックに向けて、交通機関へのサイバー攻撃を「正しく脅威」し、「必要な対策」を整理することを目的

1. はじめに

【研究の内容】

対象：鉄道、航空分野へのサイバー攻撃

1カ年目（2015年度）
サイバー攻撃への脅威を正しく認識する
事例調査、実態調査、海外調査等

2カ年目（2016年度）
サイバー攻撃へ必要な対策を整理する
リスク分析、国内外のガイドラインの整理等

1. はじめに

【研究の体制】

検討委員会の設置

（2016年度時）

【委　　員　　長】 田中　英彦　情報セキュリティ大学院大学学長（研究当時）

【委員メンバー】 学識経験者；古関隆章　東京大学教授
大久保隆夫　情報セキュリティ大学院大学教授
専　門　家；名和利男　㈱ｻｲﾊﾞｰﾃﾞｨﾌｪﾝｽ研究所　専務理事
政府関係者；内閣サイバーセキュリティセンター、警察庁
国土交通省
交通事業者；鉄道事業者、航空事業者、空港事業者

【オブザーバー】 東京五輪組織委員会、国土交通省鉄道局、航空局
日本民営鉄道協会、鉄道総合技術研究所

本日の報告内容

1. はじめに
2. 近年におけるサイバー攻撃事例
3. 国内の鉄道、航空分野における事業者実態調査（2015年度実施）
4. 鉄道、航空分野におけるサイバーテロ対策
5. おわりに

2. 近年におけるサイバー攻撃事例

(1).SFMTA(サンフランシスコ市営鉄道)の事例

- 米国サンフランシスコ市営鉄道がランサムウェアによる攻撃を受け、2,112台のコンピュータが不正にロックされ、ロックを解くまでの間乗車無料にすることを余儀なくされた。
- 安全・安定輸送には影響しなかったものの、他分野で発生している攻撃が、鉄道事業者でも発生した事例。

https://www.sfmta.com/about-sfmta/blog/update-sfmta-ransomware-attack
https://twitter.com/LisaAminABC7/status/802693810983579648/

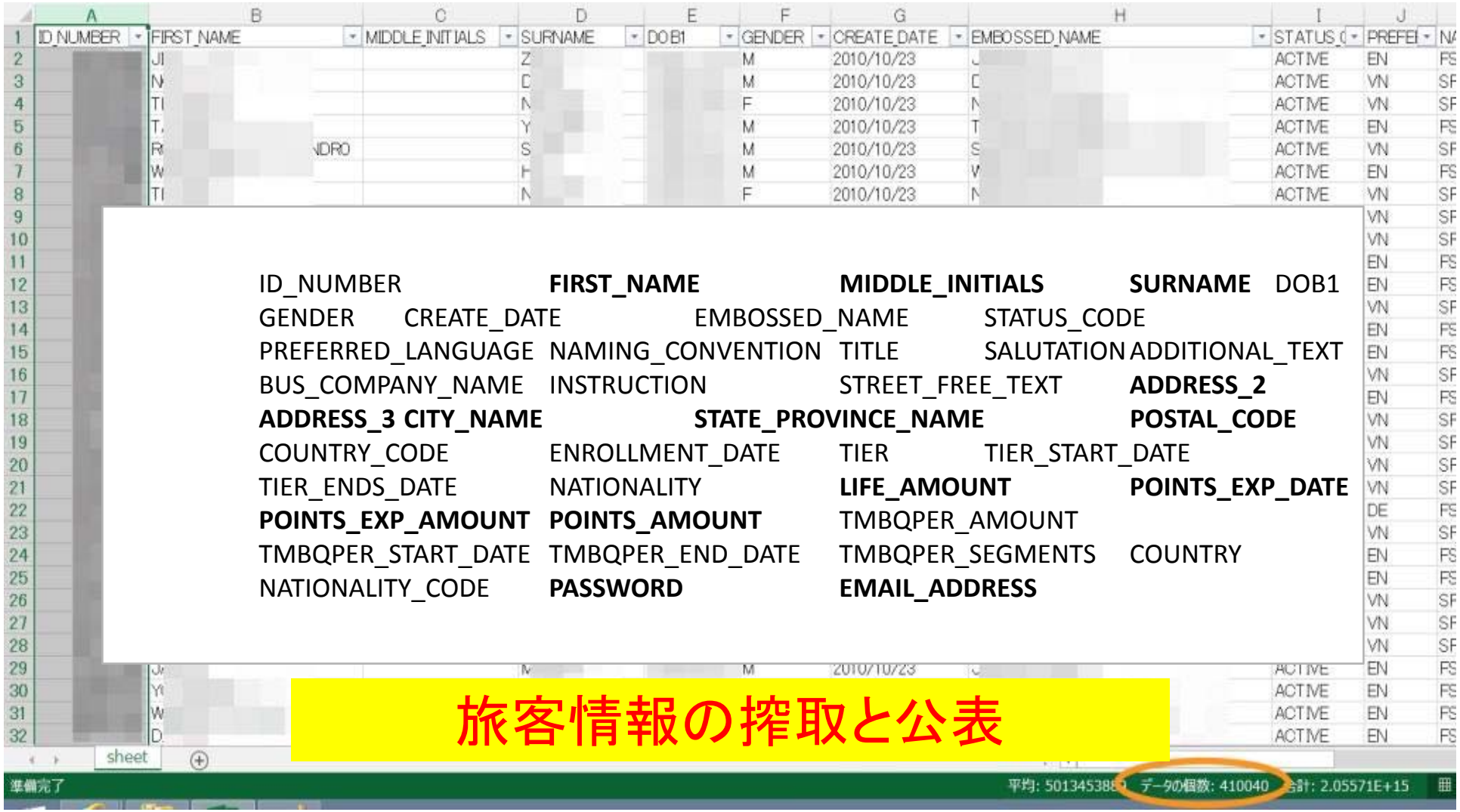
2. 近年におけるサイバー攻撃事例

(2). ベトナム航空の事例①ウェブサイト改竄

ウェブサイト改竄され、制御不能な状態

2. 近年におけるサイバー攻撃事例

（3）. ベトナム航空の事例②旅客情報の窃取および公表



本日の報告内容

1. はじめに
2. 近年におけるサイバー攻撃事例
3. **国内の鉄道、航空分野における事業者実態調査（2015年度実施）**
4. 海外の鉄道、航空分野におけるサイバーセキュリティの現状
5. 鉄道、航空分野におけるサイバーテロ対策
6. おわりに

3. 国内事業者実態調査（2015年度実施）

（1）. 調査概要

- **目的**
  交通事業者のサイバーセキュリティへの取り組み状況についてアンケートにより現状把握

- **調査対象**
  鉄道；関東地方に路線を持つ11社局
  航空；羽田空港と成田空港に運航路線を持つ5社

- **調査期間**
  実施期間：2015年 9月～10月

- **対象システム**
  鉄道；運行管理,電力管理,営業系システムおよび社内OAシステム
  航空；運航,営業系システム、社内OAシステム

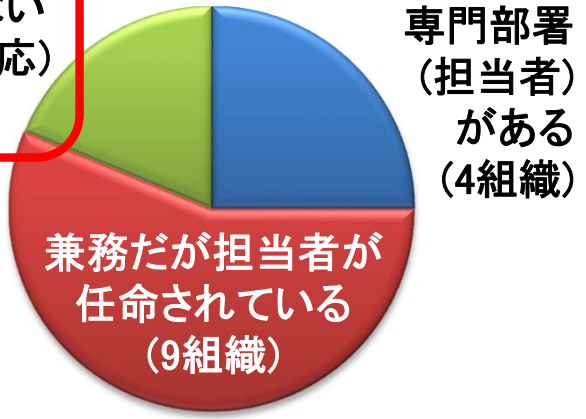
- **調査内容**
  セキュリティ体制の現状、セキュリティ対策、サイバー攻撃の被害状況等

3. 国内事業者実態調査（2015年度実施）

（2）. セキュリティ体制

- セキュリティ対策に取り組む基本的な方針の公開

- セキュリティ対策管理の社内体制



- CISOの有無

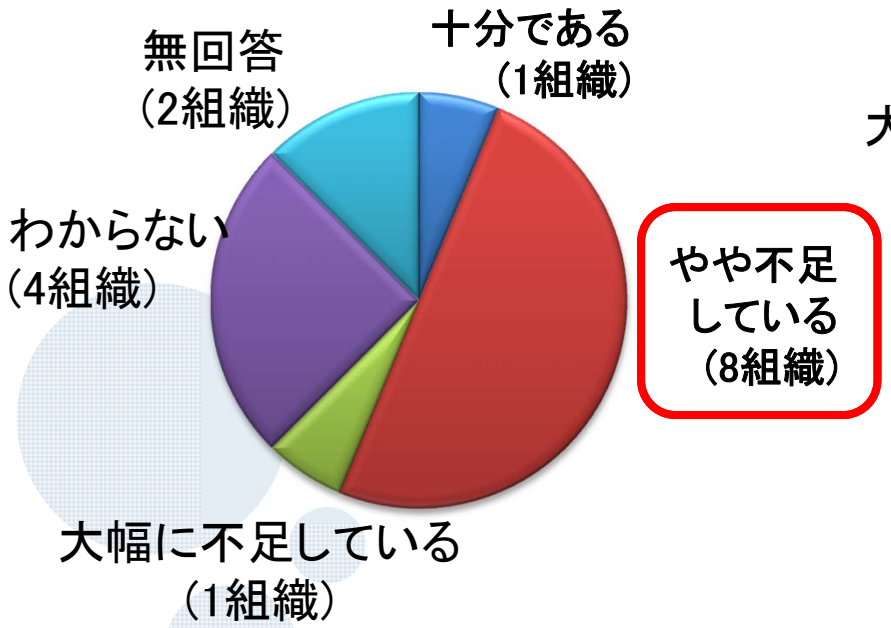
- セキュリティ対策に取り組む基本的な方針の公開は2組織、CISO専任者の組織はゼロ
- セキュリティ対策管理の社内体制が、組織的ではないという回答が3組織あり

CISO: Chief Information Security Officer
（最高情報セキュリティ責任者）

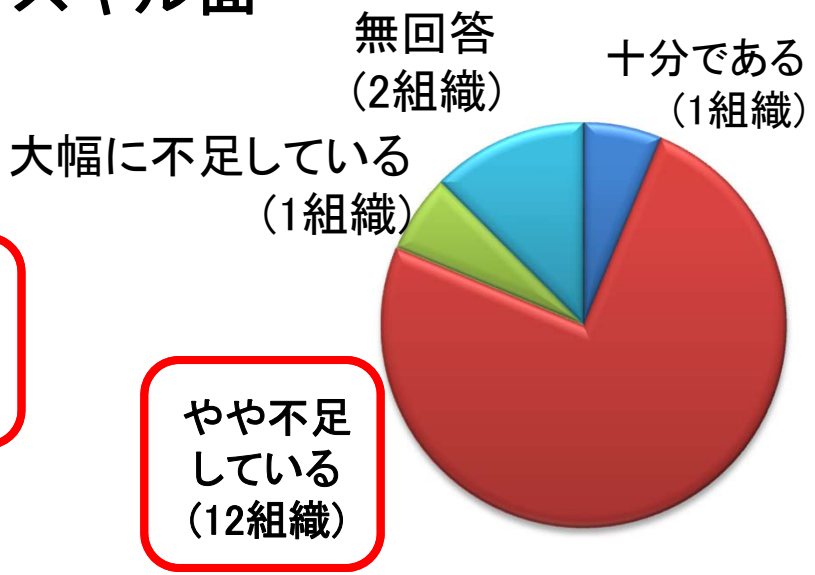
3. 国内事業者実態調査（2015年度実施）

（3）.セキュリティ業務の担当者の充足度

量的



スキル面

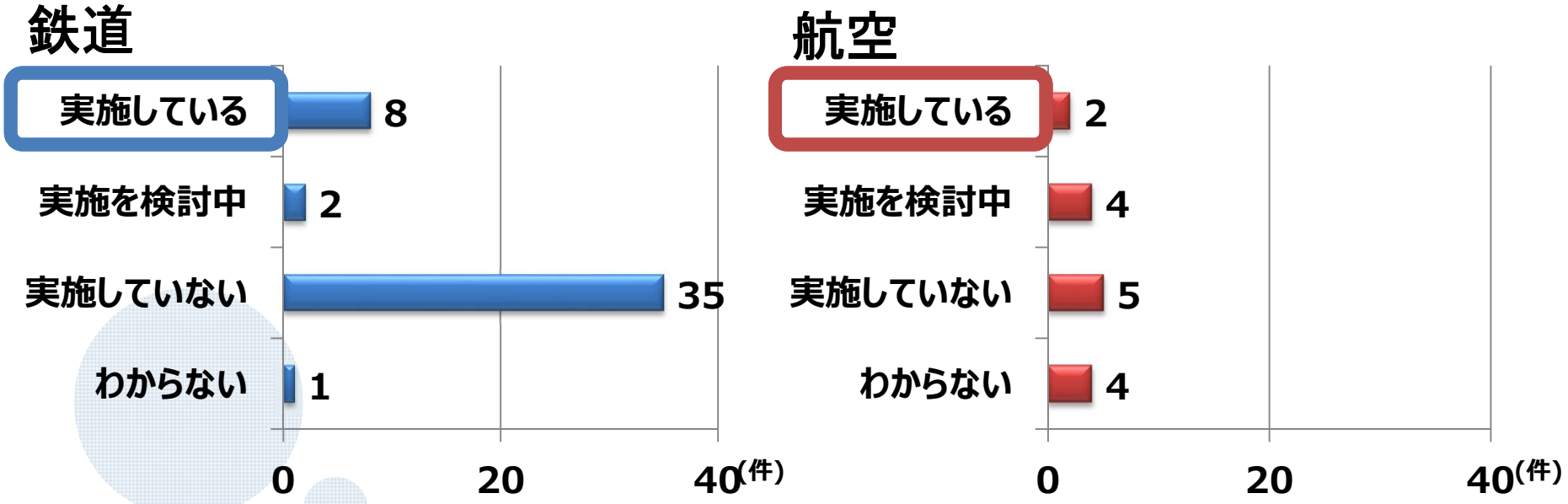


- セキュリティ対策部門の人数ならびにスキル面での充足度については、不足を感じている状態にある

3. 国内事業者実態調査（2015年度実施）

（4）.個別システムへのセキュリティ対策

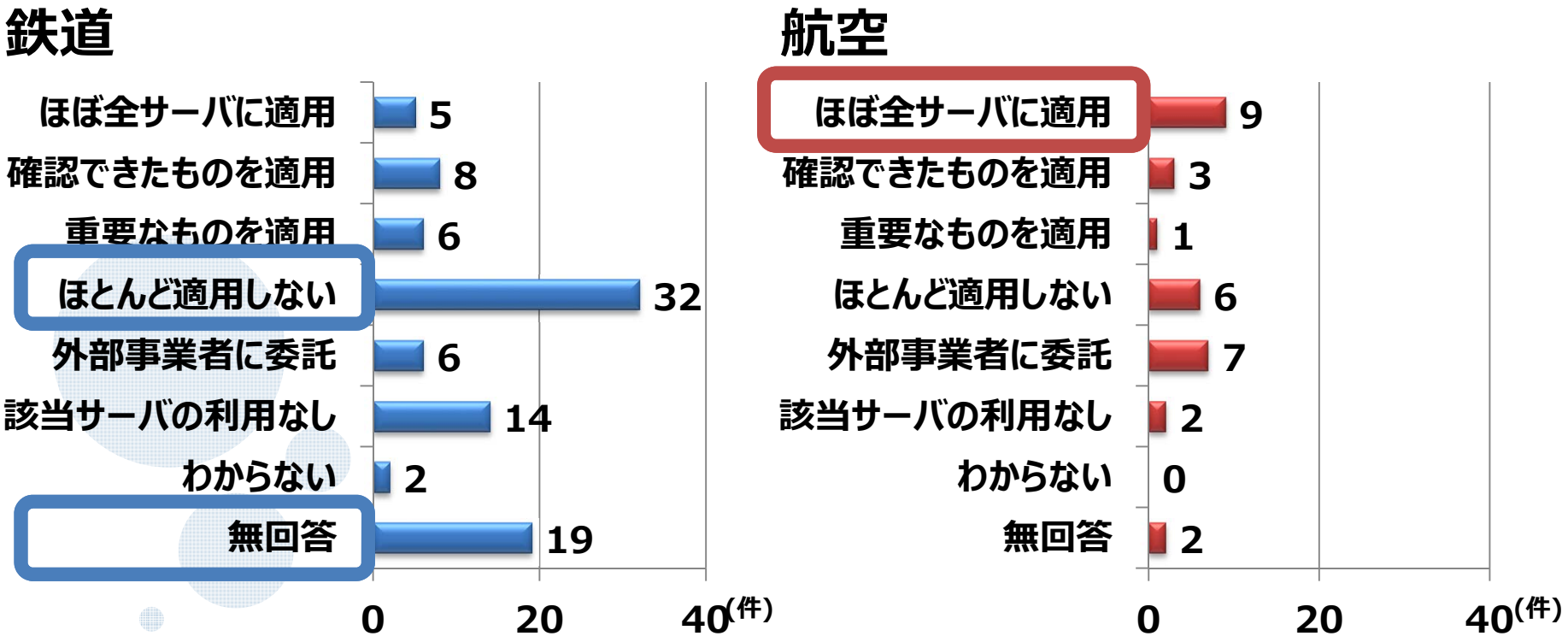
（脆弱性検査の実施）



- 鉄道　営業系(5件)、社内OA(2件)、電力管理(1件)
- 航空　運航系(1件)、営業系(1件)
- 鉄道、航空各々1件ではあるが、業界特有の個別システムに対して脆弱性検査が実施されている

3. 国内事業者実態調査（2015年度実施）

（5）.個別システムへのセキュリティ対策
（サーバーでのセキュリティパッチの適用）

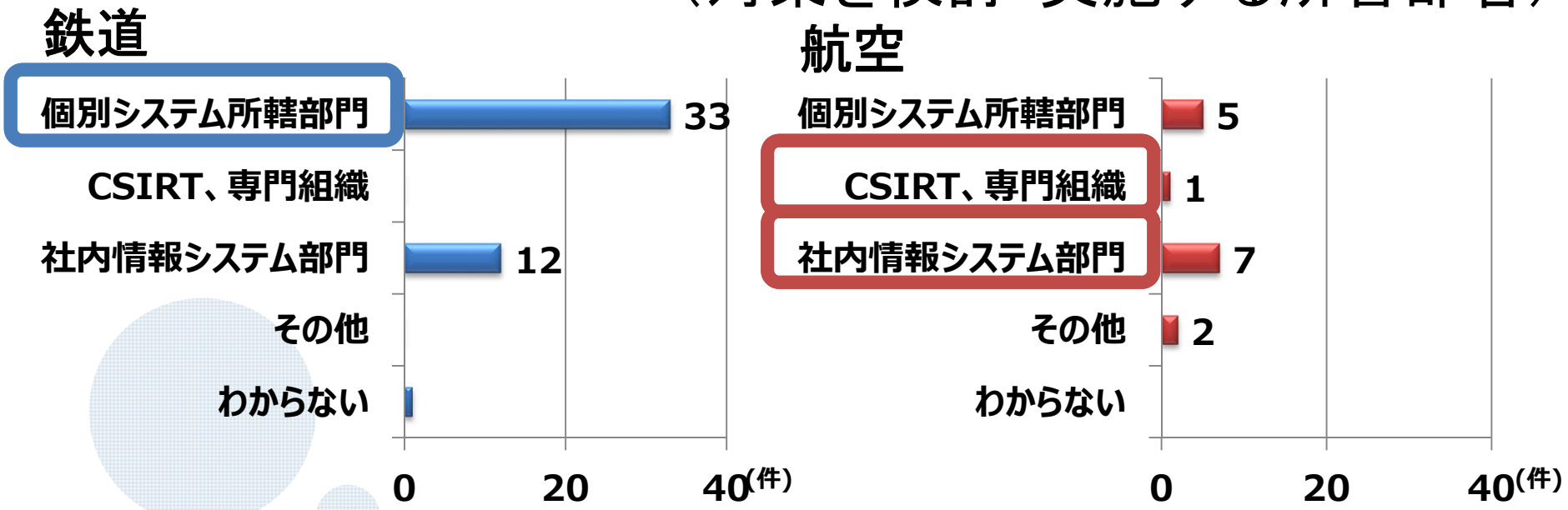


- **鉄道**　セキュリティパッチの適用によるシステム停止のリスクを回避するため代替策を実施（追加調査で判明）

3. 国内事業者実態調査（2015年度実施）

（6）.個別システムへのセキュリティ対策

（対策を検討・実施する所管部署）



- 鉄道　運行管理、電力管理、営業系(35件)のうち、33件は、個別システムを所管する部署が担当
- 航空　運航系、営業系(10件)では、社内情報システム部門(2件)、CSIRTなどの専門組織(1件)が担当

CSIRT: Computer Security Response Team(緊急対応チーム)

本日の報告内容

1. はじめに
2. 近年におけるサイバー攻撃事例
3. 国内の鉄道、航空分野における事業者実態調査（2015年度実施）
4. 鉄道、航空分野におけるサイバーテロ対策
5. おわりに

4.鉄道、航空分野におけるサイバーテロ対策

(1).対策のまとめ方

リスクの分析

主要なシステムに関するリスクを分析し対策を検討

【鉄道分野】
列車運行システム、電力管理システム、座席予約システム

【航空分野】
運航システム、予約システム、フライトインフォメーションシステム(空港)

国内外のガイドライン等の整理

既存の国内外のガイドライン等を参考

(例)

・日本
情報セキュリティに係わる安全ガイドライン
国土交通省(2016年)等

・米国
Framework for Improving Critical Infrastructure Cybersecurity Ver1.0
NIST(米国国立標準技術研究所)(2014年)

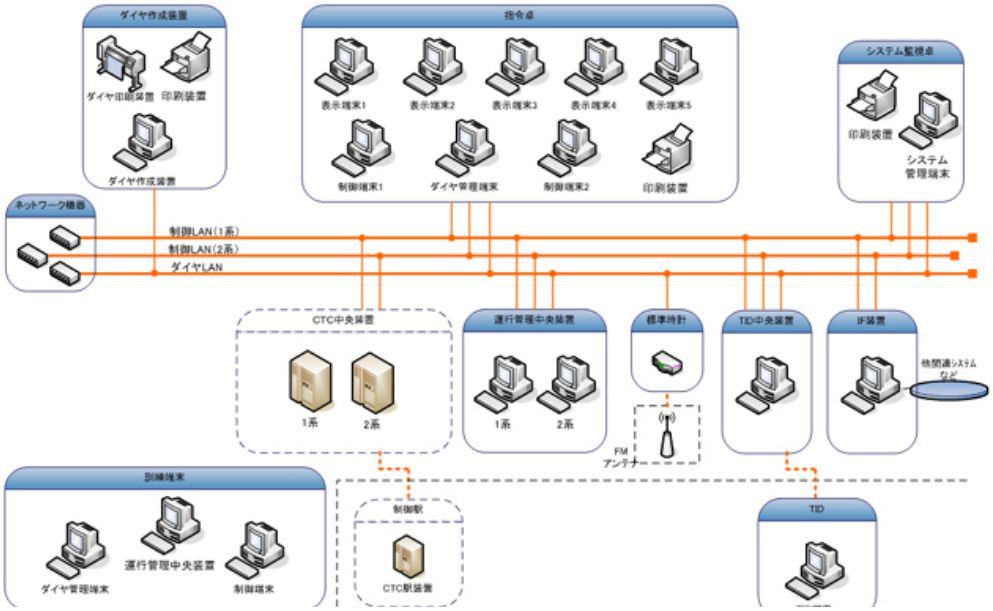
事業者が参考とすべくセキュリティ対策を提案

組織、文書化	設備・機器・運用	インシデント対応
必要な組織、文書化、サイバーセキュリティ管理の方法	運行(運航)、電力、予約等のシステムを想定した対策	緊急時や大規模イベント時の対応

4.鉄道、航空分野におけるサイバーテロ対策

(2).鉄道分野のシステムの特徴

- 複数のシステムが相互に接続し連携する
- クローズドだが他社と専用ネットワークがある



https://www.toshiba.co.jp/sis/railwaysystem/jp/products/information/traffic.html
http://www.mitsubishielectric.co.jp/society/traffic/product/yusou/y01.html

4.鉄道、航空分野におけるサイバーテロ対策

（3）.鉄道分野におけるポイントとなる対策

複数のシステムを連携させて構築していることから、複数のシステムが連携することを踏まえたセキュリティ対策の推進が望まれる

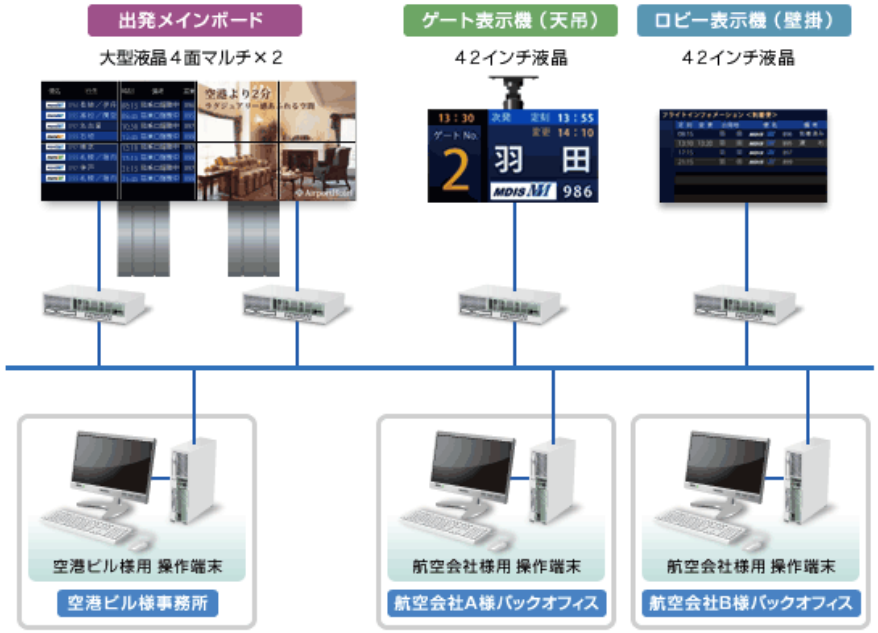
他社ネットワークとの接続などもあることから、ネットワークを介した攻撃に留意することが望まれる

被害の拡大や二次被害の誘引を防ぐためにも、機器故障がサイバー攻撃等に起因することを想定して対策を準備しておくことが望まれる

4.鉄道、航空分野におけるサイバーテロ対策

（4）.航空分野のシステムの特徴

- 制御システムではなく巨大なITシステム
- 航空会社と空港会社で連携



http://www.mdis.co.jp/products/flightvision/application/fis.html

4.鉄道、航空分野におけるサイバーセキュリティ対策

(5).航空分野におけるポイントとなる対策

対処困難な事案を想定し、グローバルで推奨されるセキュリティフレームワーク、ガイドラインを活用したアセスメントや対策の実装が望まれる

事例に基づき、侵入経路に加えて侵入後の影響を留意しての攻撃フェーズごとの多層防御の実装が望まれる

システムへのアクセスはゼロでは無いことから、人を媒介するなどのクローズドネットワークに対する脅威への対策強化が望まれる

4.鉄道、航空分野におけるサイバーテロ対策

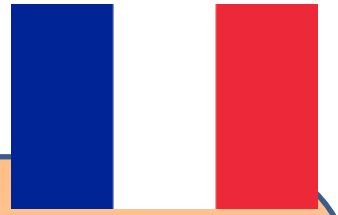
（6）.鉄道、航空分野の手引きの構成

第1章	概要	前提、リスクの現状
第2章	分野を取り巻く脅威と想定される事態	
第3章	組織	組織的対策を既存のガイドライン等から構成
第4章	文書管理	
第5章	サイバーセキュリティ管理	
第6章	機器（設備）・システムのセキュリティ	技術的な内容を中心にリスクの分析結果や既存のガイドライン等から構成
第7章	運用・管理のセキュリティ	
第8章	セキュリティインシデントの対応	
第9章	今後強化すべき対策	既存のガイドラインでの記載が乏しいが、今後重視すべき事項

以下に示す海外の国際標準や最新のガイドライン等を参考
【鉄道分野】APTA(米国公共輸送協会)やRSSB(英国鉄道安全標準化委員会)等
【航空分野】IATA(国際航空運送協会)やNIST(米国国立標準技術研究所)等

4.鉄道、航空分野におけるサイバーテロ対策

（7）.大規模イベントに必要と思われる主な対策
（フランス国鉄の事例）



リスクシナリオと対応の想定例

- 駅案内表示のハッキング　⇒　代替策の準備
- 改札のハッキング　⇒　人力で対応可に改良
- 駅構内のブラックアウト　⇒　非常用発電機を配備
- 危機対策室の通信のハッキング　⇒　二重系統化

…

事前に十分な準備と訓練が必要

本日の報告内容

1. はじめに
2. 近年におけるサイバー攻撃事例
3. 国内の鉄道、航空分野における事業者実態調査
4. 鉄道、航空分野におけるサイバーテロ対策
5. おわりに

5.おわりに

【本日の報告のまとめ】

1. 近年におけるサイバー攻撃事例
   - ➢ 輸送に影響を与える攻撃があり手法が巧妙化
   - ☆ あらゆるリスクを想定する必要がある
2. 国内の事業者実態調査
   - ➢ 「セキュリティ体制」、「担当者の充足度」に課題
   - ➢ 対策の実施に分野の違いはある
   - ☆ 組織体制、人材育成に注力が必要
3. 鉄道、航空分野におけるサイバーテロ対策
   - ➢ 異なる特徴に応じた対策が必要
   - ☆ 組織的、技術的な各対策が継続的に求められる

5.おわりに

【今後必要と思われる主な課題】

組織・体制の対応

経営者理解

全社的対応

セキュリティ人材育成

対応能力向上

演習・訓練の充実

緊急時対応

情報共有体制

脅威

脆弱性

Supported by 日本財団 THE NIPPON FOUNDATION

ご清聴ありがとうございました

本研究は田中英彦情報セキュリティ大学院大学学長（研究当時）を委員長とする検討委員会での議論を経て進めたものです。
ここに記して感謝の意を表します。

本研究は日本財団による支援に基づいて実施しているものです。