Supported by 日本財団 THE NIPPON FOUNDATION

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。

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研究

－人材育成と情報共有－

平成３０年５月１５日（火）

一般財団法人運輸総合研究所

総務部企画室参事　深　作　和　久

本日の報告

1．背景と目的

2．近年におけるサイバー攻撃の事例

3．鉄道、航空システムの特徴と対策

4．人材育成カリキュラム

5．情報共有のあるべき姿

6．今後の取り組み

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研究

－ 背景と目的 －

想定される脅威

- 我が国へのサイバー攻撃の増加
- 鉄道、航空への攻撃
- IOT機器の普及に伴う新たな脅威
- オリンピック・パラリンピック特有の攻撃

東京オリンピック・パラリンピックに向けて、鉄道、航空分野へのサイバー攻撃の防御に向けて人材育成カリキュラムの作成と情報共有のあるべき姿を検討

研究体制

Supported by 日本財団 THE NIPPON FOUNDATION

検討会の設置（平成29年度）

委員長	**田　中　英　彦**	学校法人岩崎学園理事 情報セキュリティ大学院大学 名誉教授・東京大学　名誉教授
委　員	**名　和　利　男**	株式会社サイバーディフェンス研究所　専務理事／上級分析官
〃	**大久保　隆　夫**	情報セキュリティ大学院大学 情報セキュリティ研究科　教授
〃	**古　関　隆　章**	東京大学大学院　工学系研究科　電気系工学専攻　教授
〃	**林　　泰　三**	内閣官房　内閣サイバーセキュリティセンター　参事官
〃	**藤　田　礼　子**	国土交通省　総合政策局　情報政策課長
〃	**舘　　剛　司**	公益財団法人東京オリンピック・パラリンピック競技大会 組織委員会テクノロジーサービス局長
〃	**交通事業者**	鉄道、航空・空港事業者

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研究

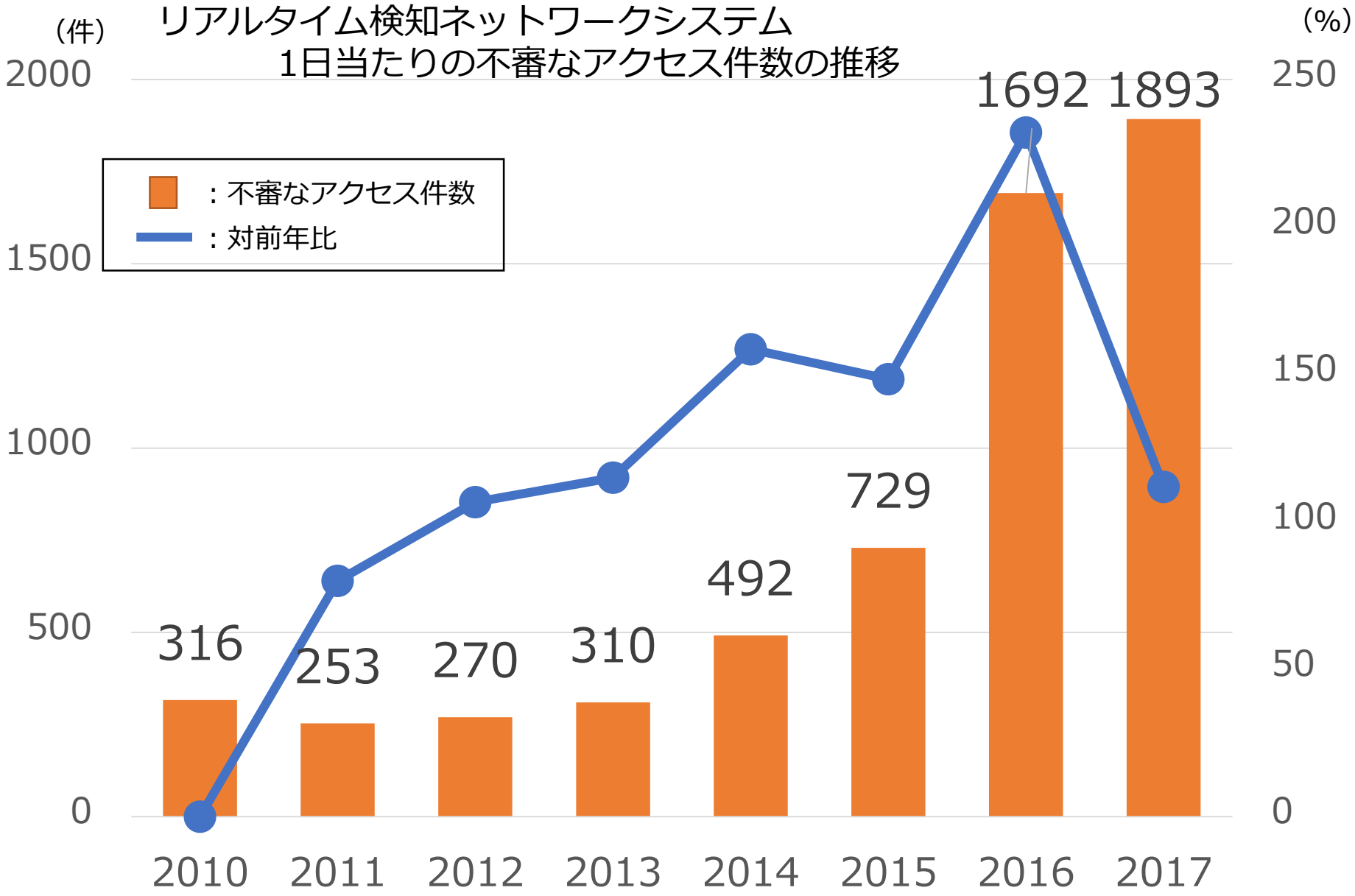
－近年におけるサイバー攻撃の事例 －

近年のサイバー攻撃の事例

想定される脅威

- 我が国へのサイバー攻撃の増加
- 鉄道、航空への攻撃と攻撃の高度化
- IOT機器の普及に伴う新たな脅威
- オリンピック・パラリンピック特有の攻撃

我が国へのサイバー攻撃の増加



警察庁資料より作成

我が国へのサイバー攻撃の増加

	政府等の主な動向
2014年9月	■サイバーセキュリティ戦略（CS戦略）が閣議決定 ■2020年オリンピック・パラリンピック競技大会を参るストーンとした対策強化取組み方針が明示
2014年11月	■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年6月	■日本再興戦略 改訂2015 ■IT利活用の安全・安心の確保が成長戦略を確固たるものにすると明記
2016年1月	■経済産業省から経営者が実施すべき要件を纏め「サイバーセキュリティー経営ガイドライン」が発行 ■NISC「我が国のサイバーセキュリティ推進体制の更なる機能強化に関する方針」を発表
2016年10月	■サイバーセキュリティ基本法 改定案が施行

近年におけるサイバー攻撃の事例

想定される脅威

- 我が国へのサイバー攻撃の増加
- 鉄道、航空への攻撃と攻撃の高度化
- IOT機器の普及に伴う新たな脅威
- オリンピック・パラリンピック特有の攻撃

サイバー攻撃の代表的な事例（2014年～）

Supported by 日本財団 THE NIPPON FOUNDATION

【鉄道分野】

ソウルメトロに対するサイバー攻撃（2014年）

韓国ソウル特別市で地下鉄1～4号線を運営するソウルメトロがサイバー攻撃を受け、PC管理プログラム運用サーバが、少なくとも5ヶ月以上、攻撃者に掌握されていた状態であったことが、2015年10月明らかとなった。

カナディアンパシフィック鉄道での元従業員による不正（2015年）

カナディアンパシフィック鉄道で解雇されたIT業務の従業員が、退職前に管理者アカウント削除、パスワード書き換えにより、ネットワークのコアスイッチにアクセスできないようにした。

サンフランシスコ市営鉄道でランサムウェア感染（2016年）

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。

ドイツ鉄道でランサムウェアWannaCry感染（2017年）

金曜日(5/12)の夜から土曜日(5/13)にかけて被害が発生した。発着時刻を表示する駅の電光掲示版に影響を与えた。

サイバー攻撃の代表的な事例（2014年～）

Supported by 日本財団 THE NIPPON FOUNDATION

【航空分野】

ベトナム航空へのサイバー攻撃（2016年）

南シナ海の領海における国際司法裁判所の判決を不服として、ハクティビストがベトナム航空のシステムへ侵入し、フライトインフォメーションのウェブページの改ざん、顧客情報の公表、空港内放送システムの乗っ取り、チェックインカウンターのシステム障害をおこした。

スウェーデンの航空管制業務公社（LFV）への高度標的型攻撃（APT）

某国による標的型攻撃を受け、航空管制センターのシステムが停止

LOTポーランド航空へのサイバー攻撃（2015年）

地上運航システムがサイバー攻撃をうけ、フライトプランの作成が出来なくなる。

【国　内】

JTBへの高度標的型攻撃（APT）

2016年、Elirks(エリークス）と呼ばれるハッカーグループより高度標的型攻撃をうけ、顧客情報が流失

空港ビル会社への継続的なサイバー攻撃

ハッカーグループより継続的にサイバー攻撃を受けていることを確認。

インシデント事例（被害）

Supported by 日本財団 THE NIPPON FOUNDATION

サンフランシスコ市営鉄道でランサムウェアMamba感染

　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、 券売機などが不正にロックされ、約3日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いものの、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となる。

ドイツ鉄道でランサムウェアWannaCry感染

発着時刻を表示する駅の電光掲示版が、ランサムウェアによる攻撃を受け、不正にロックされる。スタッフを増員配備することで対応した。

インシデント事例

感染の影響でサービスを停止した券売機

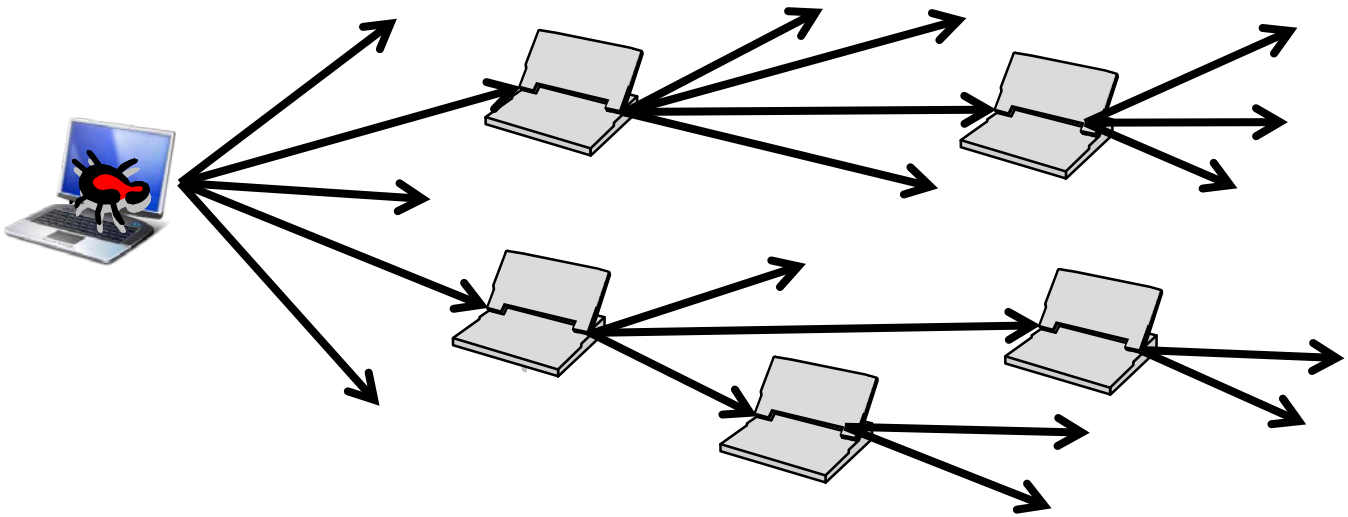
感染した駅の電光掲示板

https://www.sfmta.com/about-sfmta/blog/update-sfmta-ransomware-attack
http://www.deutschebahn.com/de/presse/pr...20170513.html　等

インシデント事例（原因：ワーム）

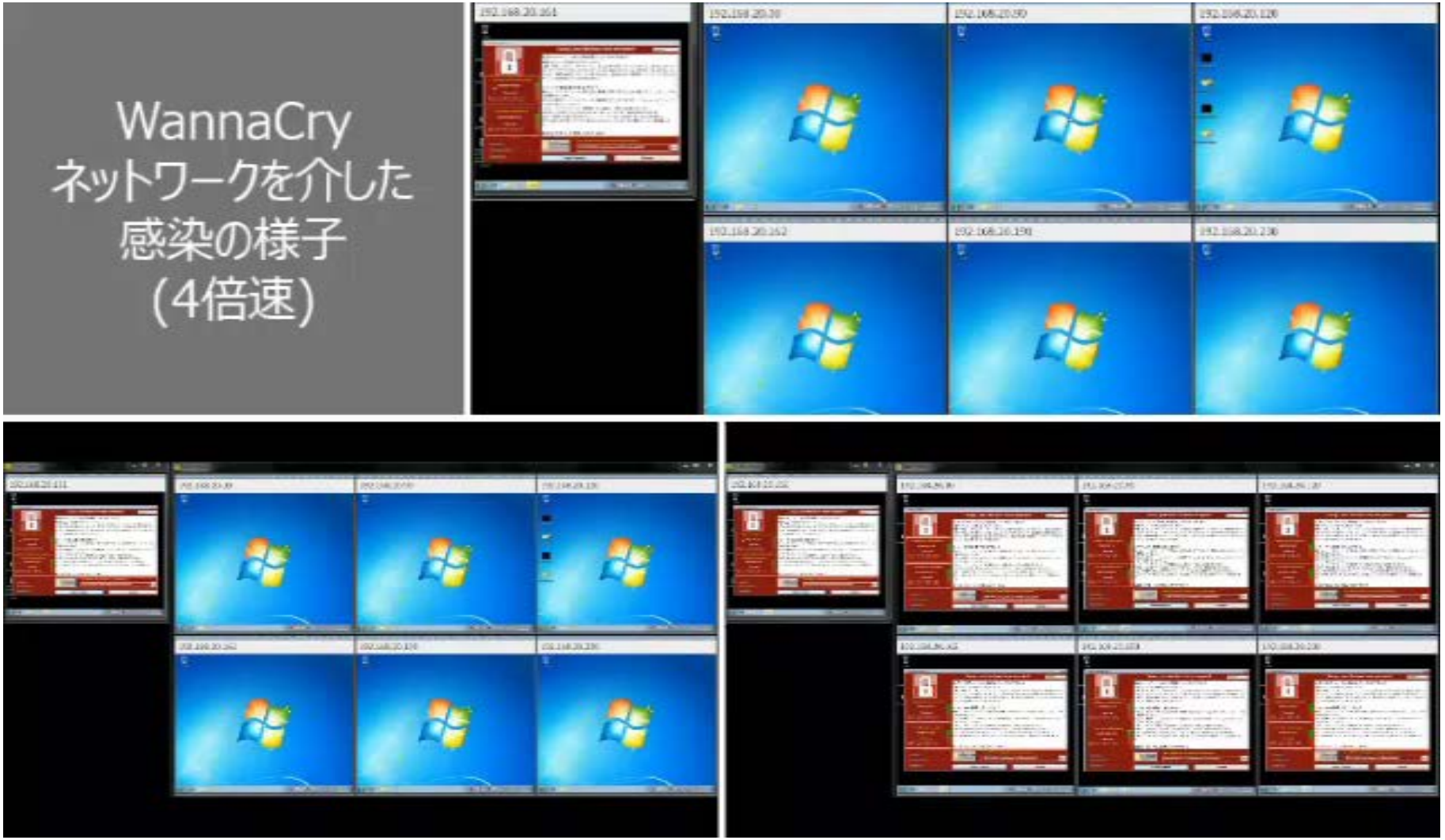
- **自身を複製して他のシステムに拡散する性質を持ったマルウエア、他の脆弱なシステムに感染していくことで自己増殖を試みる。**

時期	名称	ワーム型	被害
2000/07	**CodeRed I/II**	○	DoS攻撃
2003/02	**Slammer**	○	DoS攻撃
2003/08	**MSBlaster**	○	システムが再起動を繰り返す
2017/05	**WannaCry**	○	**身代金**



ランサムウエアWannaCryの感染速度

- 8倍速のMP4ファイルのムービーで、6台のPCが感染するまでの時間は、5分程度



日立実験施設でのデモ結果

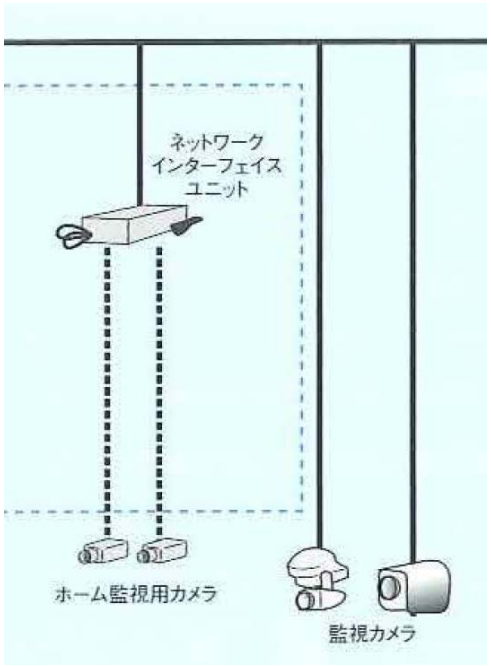
近年におけるサイバー攻撃の事例

想定される脅威

- 我が国へのサイバー攻撃の増加
- 鉄道、航空への攻撃と攻撃の高度化
- IOT機器の普及に伴う新たな脅威
- オリンピック・パラリンピック特有の攻撃

IOT機器の普及に伴う新たな脅威

- **近年IPカメラが関わるサイバー攻撃が発生**
  - IPカメラを踏み台とした大規模DDoS攻撃 ➡ **業務停止の可能性**
  - 「画像無断公開サイト」 ➡ **情報漏えいの可能性**



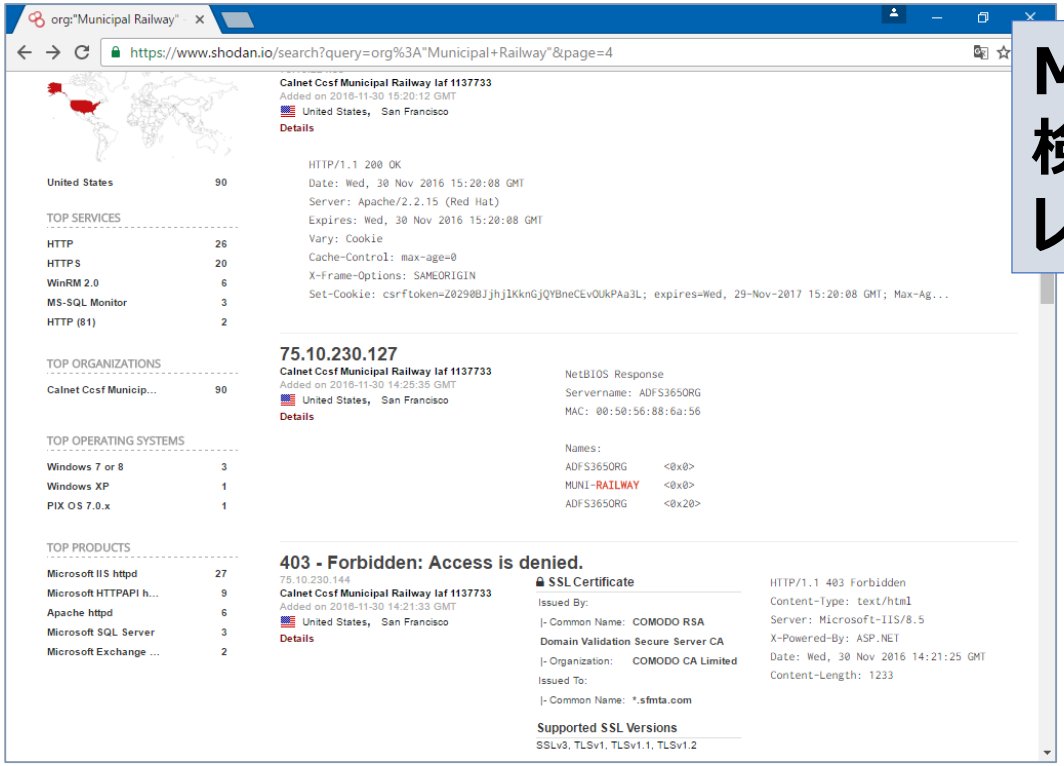
http://www.itmedia.co.jp/enterprise/articles/1610/25/news059.html
http://itpro.nikkeibp.co.jp/atcl/watcher/14/334361/102000701/
http://blog.trendmicro.co.jp/archives/10540

IOT機器の普及に伴う新たな脅威

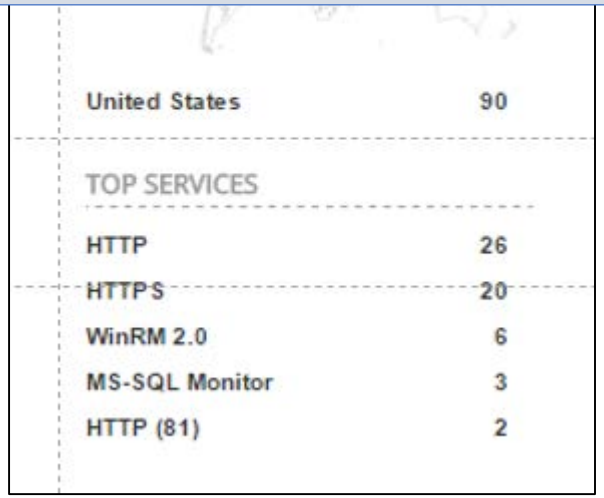
Supported by 日本財団 THE NIPPON FOUNDATION

- **2016年、意図しないインターネット接続端末の存在**

米国サンフランシスコ市営鉄道の端末がインターネットに繋がっていた。
(2016年12月2日時点)



Municipal Railwayで検索すると、90件のIPアドレスが存在



近年におけるサイバー攻撃の事例

想定される脅威

- 我が国へのサイバー攻撃の増加
- 鉄道、航空への攻撃と攻撃の高度化
- IOT機器の普及に伴う新たな脅威
- オリンピック・パラリンピック特有の攻撃

オリンピック・パラリンピック特有の攻撃

◆過去のオリンピックでの主なサイバー攻撃

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

まとめ　-2020年東京大会の成功に向けて-

Supported by 日本財団 THE NIPPON FOUNDATION

東京大会においての更なる攻撃が懸念

■本格的なサイバー攻撃が起きると想定した上で、対策を講じる必要がある。

■鉄道、航空など大量輸送機関に対するサイバー攻撃は、人命に関わる重大な侵害、社会的な混乱をきたす恐れがある。

【平成28年度】

鉄道、航空事業者が実施すべき**具体的なセキュリティ対策をまとめた手引書**を作成

【平成29年度】

■**手引書にあるセキュリティ対策が実践できる人材育成カリキュラム**の作成

■**情報共有組織（ISAC)のあるべき姿**の検討

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研究

－ 鉄道、航空システムの特徴とサイバーセキュリティ対策 －

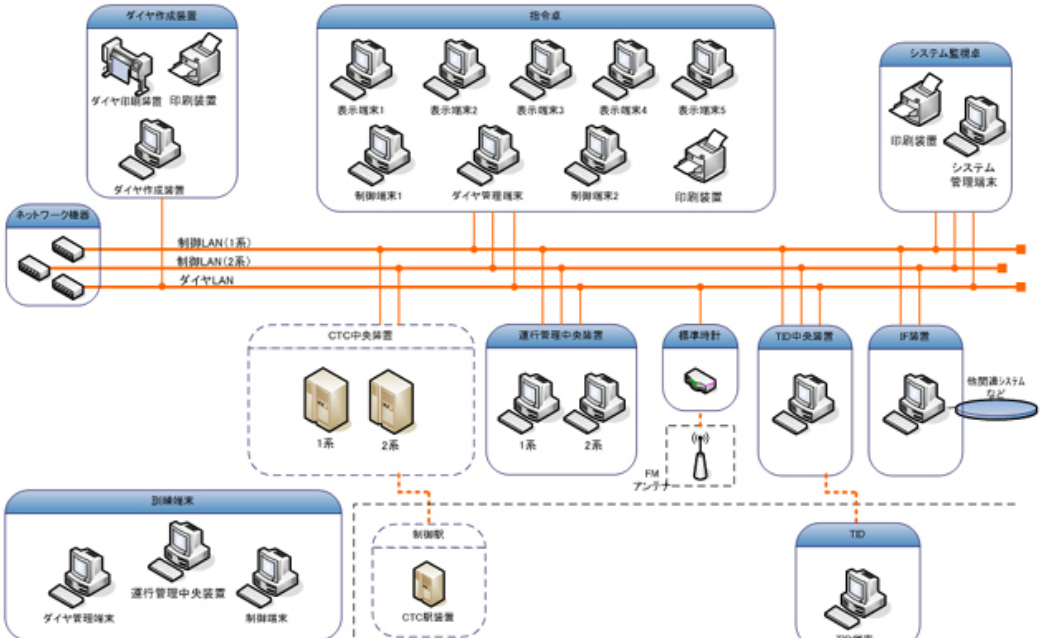
鉄道、航空システムの特徴と対策

Supported by 日本財団 THE NIPPON FOUNDATION

■鉄道システムの特徴

対象システム：**運行管理システム、電力管理システム、座席予約システム**

◆複数のシステムが相互に接続し連携している
◆基本的に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

鉄道、航空システムの特徴と対策

Supported by 日本財団 THE NIPPON FOUNDATION

■航空システムの特徴

対象システム：**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

◆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

鉄道、航空システムの特徴と対策

Supported by 日本財団 THE NIPPON FOUNDATION

■安全・安定輸送に資するサイバーセキュリティ対策の手引書

第1章	概要	・前提、リスクの現状
第2章	鉄道、航空分野を取り巻く脅威と想定される事態	・サイバー攻撃の攻撃方法 ・オリンピックで想定される攻撃
第3章	組織	・組織と役割、サイバーセキュリティ教育
第4章	文書管理	・セキュリティ情報の文書化と適切な管理
第5章	サイバーセキュリティ管理	・リスクアセスメントに基づく対策立案 ・PDCAサイクルでの管理
第6章	システムのセキュリティ	・セキュリティ対策
第7章	セキュリティの管理	・人的防御、情報収集、監視 ・調達時のセキュリティ仕様の明確化
第8章	インシデントの対応	・インシデント対応の体制・手順、情報共有
第9章	今後強化すべき対策	・今後重視すべき事項

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研究

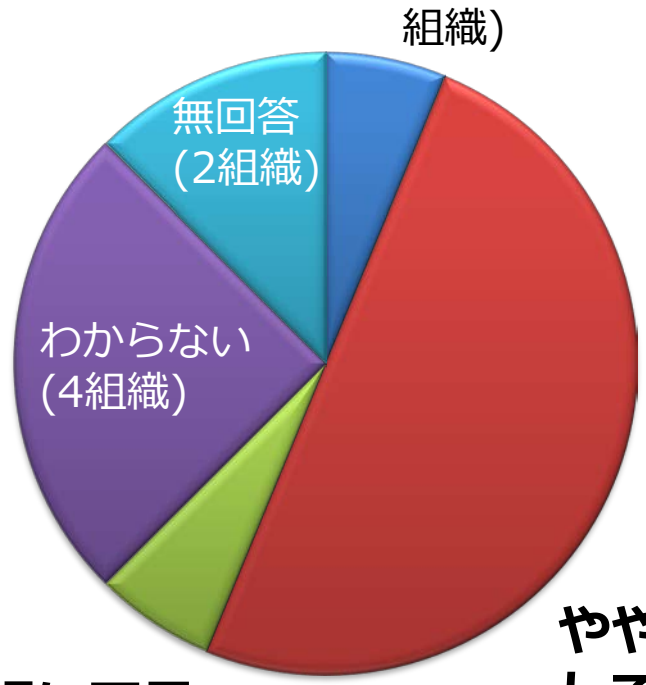
－ 人材育成カリキュラム －

人材育成カリキュラム

■セキュリティ業務担当者の充足度（平成27年度）

セキュリティに携わる人員数、スキル面での充足度に課題。

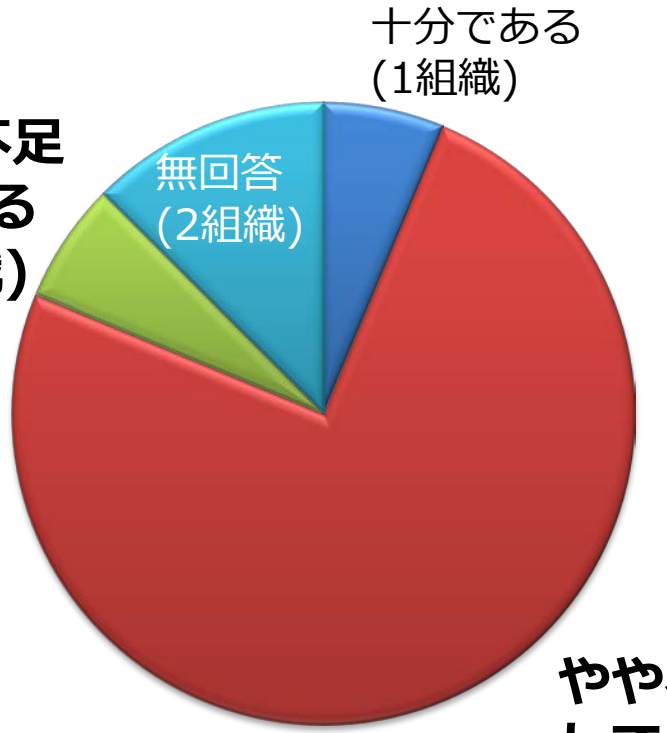
【人員】



大幅に不足している（1組織）

やや不足している（8組織）

【スキル】



大幅に不足している（1組織）

やや不足している（12組織）

人材育成カリキュラム

Supported by 日本財団 THE NIPPON FOUNDATION

【人材育成の目標】

「鉄道、航空の安全・安定輸送に資する**サイバーセキュリティ対策の手引き**」にある対策の実践

【育成対象者の検討】

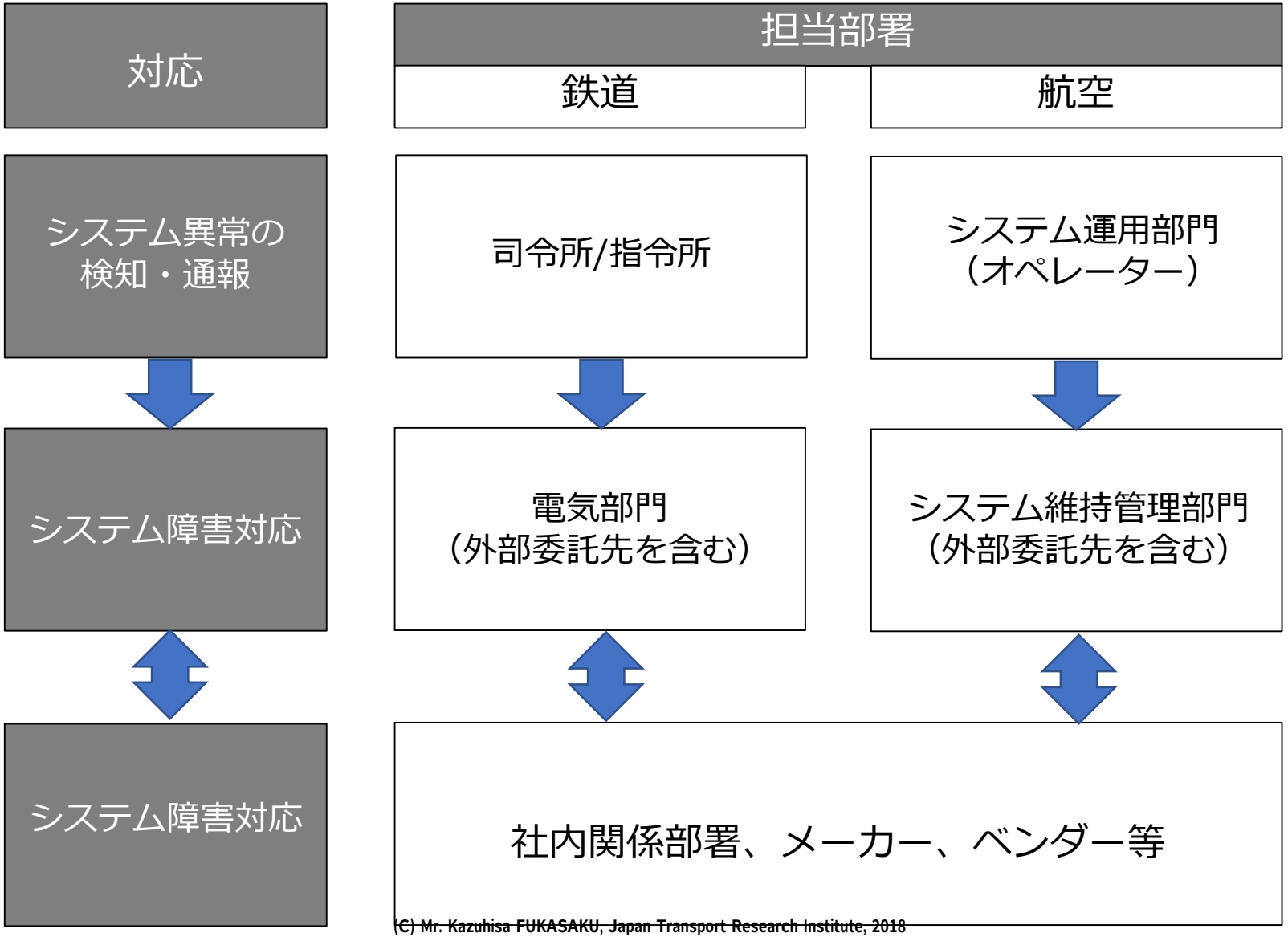
（１）人材像や育成対象の明確化

（２）事業者の実態を踏まえた育成対象の明確化

（３）事業者の現状を踏まえたカリキュラム

人材育成カリキュラム

■通常のシステム障害の対応手順



人材育成カリキュラム

Supported by 日本財団 THE NIPPON FOUNDATION

■サイバー攻撃によるシステム障害の対応手順

育成対象：**システム維持管理部門の技術者層**
（鉄道：電気部門、航空：システム維持管理部門）

対応	担当部署		役割
	鉄道	航空	
システム異常の検知・通報	司令所/指令所	システム運用部門（オペレーター）	■発生事象の適切な通報
システム障害対応	電気部門（外部委託先を含む）	システム維持管理部門（外部委託先を含む）	■サイバー攻撃かどうかの判断 ■サイバー攻撃対策の対応・支援
サイバー攻撃のインシデント対応立案、実行	セキュリティ担当部門 C-SIRT セキュリティベンダー等		■サイバー攻撃対策の立案・実行

人材育成カリキュラム

育成対象者と求められる人材像・能力

【求められる人材像】

(1) インシデント発生の際、その原因がサイバー攻撃である可能性を考慮し、適切に対応できる人材

(2) サイバー攻撃に関わるインシデント対応を、サイバー攻撃に対処する専門機関と連携して対応・支援できる人材

【必要となる能力】

(1) サイバー攻撃対するインシデント対応能力

(2) 上記に関わる情報技術（ＩＴ）に関する能力

人材育成カリキュラム

Supported by 日本財団 THE NIPPON FOUNDATION

机上演習によるカリキュラムの拡充

鉄道	第１回	平成29年11月1日（水） **サイバー攻撃への対応基礎能力（勘所）**	航空	第１回	平成29年10月30日（月） **サイバー攻撃への対応基礎能力（勘所）**
	第２回	平成29年11月21日（火） **攻撃経路や被害範囲の特定**		第２回	平成29年11月20日（月） **攻撃経路や被害範囲の特定**
	第３回	平成29年12月19日（火） **サイバー脅威の収集と分析の実践**		第３回	平成29年12月13日（水） **サイバー脅威の収集と分析の実践**

人材育成カリキュラム

机上演習によるカリキュラムの拡充

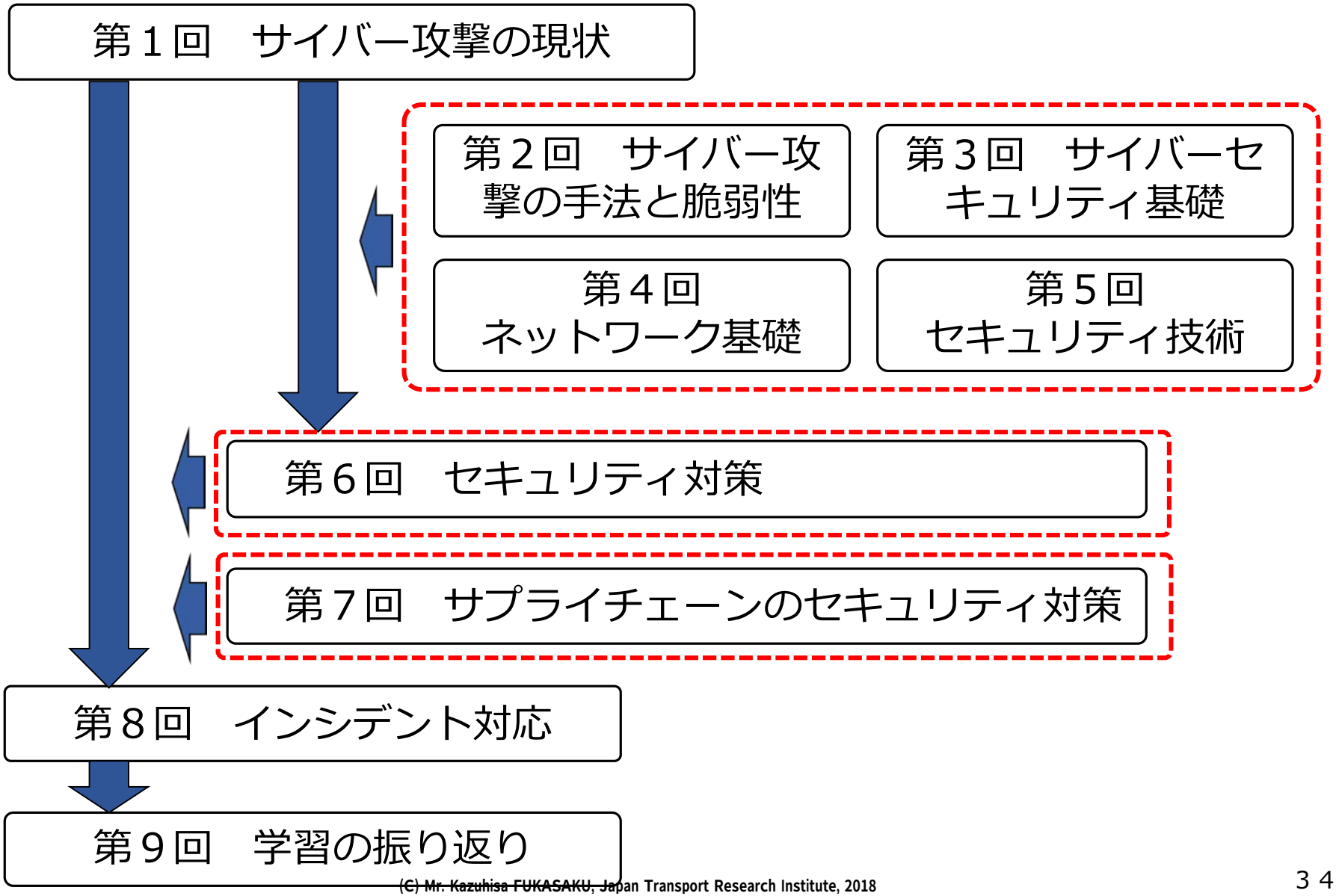
■演習での主な討議内容

初動対応	■ 感染拡大を防ぐために何をしなければならないか ■ 他部門への報告、委託業者への指示内容
エスカレーション	■ 具体的に想定される被害と範囲 ■ 上層部へ何をどう説明するのか
原因特定	■ 証拠保全をどう実施するか ■ 攻撃方法の特定
今後の対策	■ 再発防止策の立案 （技術、人的管理、法務に対して、 短期、中期、長期の視点から）

人材育成カリキュラム

Supported by 日本財団 THE NIPPON FOUNDATION

各講座の関係



人材育成カリキュラム

Supported by 日本財団 THE NIPPON FOUNDATION

講座の概要（第8回インシデント対応）

目標	インシデント発生の際、その原因がサイバー攻撃である可能性を考慮し、迅速かつ適切に対応するためのポイントを学習する。

学習項目	概要	内容
インシデント発生時の対応手順	・インシデント対応の概要 ・インシデント発生時の対応手順と役割分担	・インシデント発生の際に担当者が取る対応の必要性を中心に解説する。 ・インシデント発生の際に、どのような手順で対応していくかを解説する。
インシデント対応体制	・セキュリティインシデントの位置付け ・担当者の役割 ・社内外との連携	・自社におけるセキュリティインシデントの対応と従来のシステム障害時の対応との相違点について解説する。 ・自社の体制に基づき、担当者の役割や社内外の連携について解説する。
対処時のポイント	・初動の重要性 ・連絡事項 （初動対応時に把握すべき事項）	・インシデント対処時のポイントについて解説する。

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研究

－ 情報共有のあるべき姿 －

情報共有のあるべき姿

Supported by 日本財団 THE NIPPON FOUNDATION

情報共有組織（ISAC：Information Sharing and Analysis Center）

サイバーセキュリティーに関する情報を共有し、サイバー攻撃への防御力を高めることを目指して活動する組織

■一般社団法人 金融ISAC

- 銀行・証券・保険等の金融機関が2014年8月設立
- 情報・物理セキュリティに関する情報収集・分析・共有の他、安全対策に関するコンセンサスの形成、セキュリティ啓発活動、年1度のカンファレンスなどを行う

■一般社団法人 ICT-ISAC

- Telecom-ISAC会員に放送・ベンダー企業を加え2016年3月設立
- ICT分野のセキュリティに関する情報収集・分析・共有の他、安全対策に関するガイドラインの検討や人材育成、啓発活動などを行う
- 通信分野のセプター事務局を兼ねる

■電力ISAC

- 電力事業者が2017年3月設立
- サイバーセキュリティに関する情報収集・分析・共有の他、情報共有に向けたルール策定などを行う
- 電力分野のセプター事務局を兼ねる

情報共有のあるべき姿

【情報の内容】

現状	政府機関などから脆弱性情報やインジケータ、会員から提供されたインシデント情報を共有
検討	■情報提供する際に、具体的な対策について提供 ■攻撃についての被害状況や被害の範囲などについて提供

【情報共有の方法】

現状	多くの情報共有組織では、情報共有の手段としてメールを利用
検討	■ポータルサイトの利用 共有された情報に対する質問のやりとりなど双方向の意見交換が可能 過去に共有されたインシデント情報、ガイドライン等の検索が可能

【参加資格】

現状	普段からシステムの不具合情報等について、ベンダーやメーカーと密接に情報共有をしている
検討	■必要に応じてベンダーやメーカーも参加

【情報共有の活性化に向けて】

検討	■情報を出しやすい雰囲気に繋がる信頼関係の醸成 ・総会、WG及び懇親会など会員同士が顔を合わせる機会を作る
	■ISACの付加価値向上 ・教育プログラムの実施（スキルアップ講座、演習、勉強会の開催） ・セキュリティガイドラインの作成

今後の取り組み

サイバー人材の育成（試行）

知識の向上

机上演習の実施

対応能力の向上

経営、管理者等への啓発セミナー

経営者の理解

全社的な対応

Supported by 日本財団 THE NIPPON FOUNDATION

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。

ご清聴ありがとうございました。