Japan Transport and Tourism Research Institute

Supported by THE NIPPON FOUNDATION

東京オリンピック・パラリンピックに向けた サイバー攻撃に対する人材育成に関する調査研究

平成３０年１１月２１日（水）

一般財団法人運輸総合研究所
企画室参事　　深　作　和　久

Japan Transport and Tourism Research Institute

Supported by THE NIPPON FOUNDATION

東京オリンピック・パラリンピックに向けた サイバー攻撃に対する人材育成に関する研究

－ 背景と目的 －

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
- IOT機器, Wi-Fiなどの普及に伴う新たな脅威
- 鉄道、航空への攻撃
- 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関する調査研究を実施

研究体制

検討会の設置（平成30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
〃	**金　子　修　久**	内閣官房　内閣サイバーセキュリティセンター　参事官
〃	**蔭　山　良　幸**	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

■調査研究の内容

【平成27年度】

■鉄道、航空事業者のシステムの強度を把握するために、運行・運航システムに対してペネトレーションテスト（侵入テスト）を実施しシステムの脆弱性等について検証

【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

【平成30年度】

■カリキュラムに基づいた教材を作成し、教育（試行）を実施予定
■経営層を対象とした啓蒙セミナーを実施予定

本日の報告内容

１．サイバー攻撃の動向（教材より）

２．人材育成カリキュラム

３．サイバー攻撃対策　（教材より）

４．経営を取り巻く外部環境リスク

５．今後の取り組み

Japan Transport and Tourism Research Institute

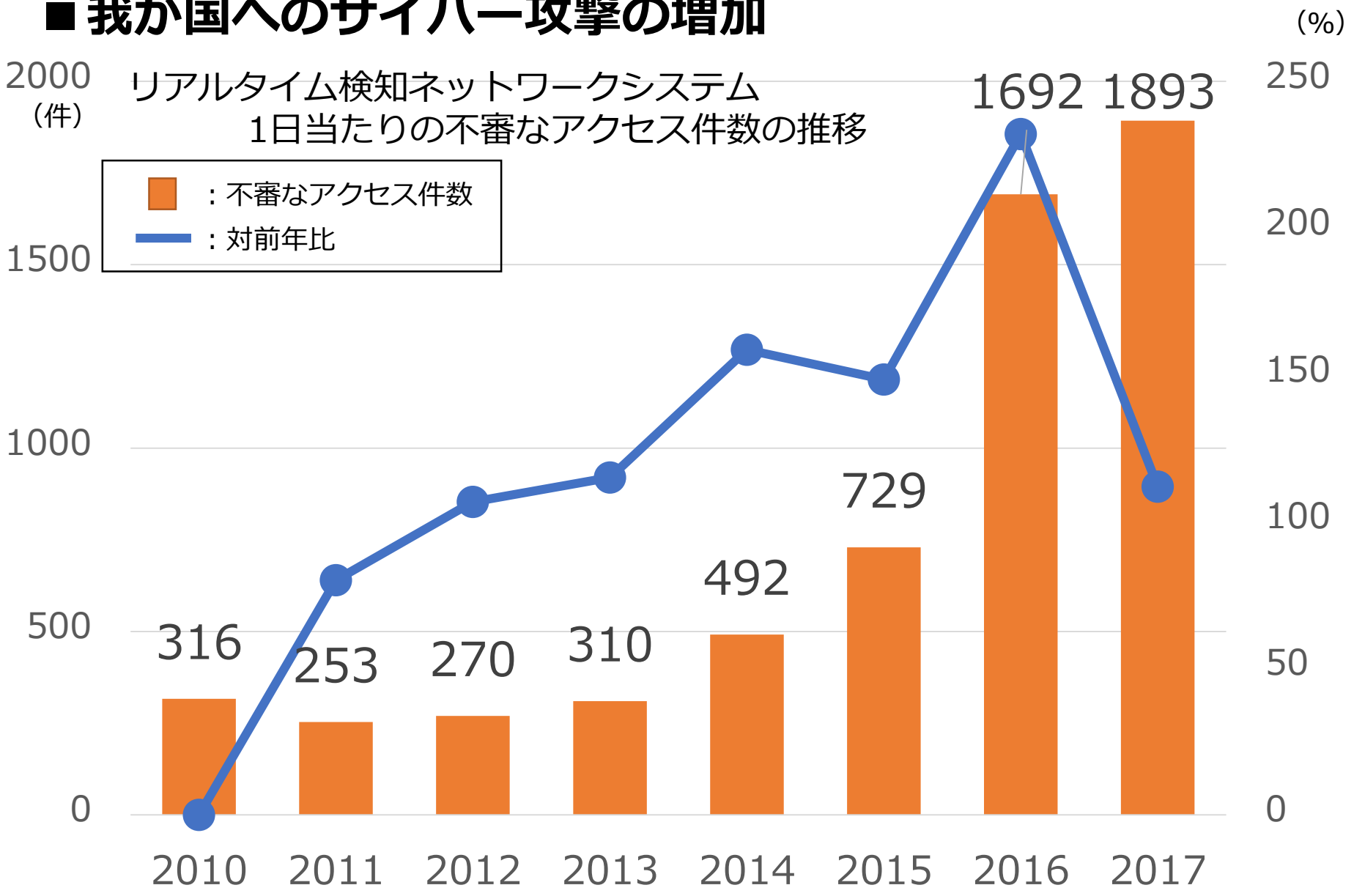
Supported by THE NIPPON FOUNDATION

東京オリンピック・パラリンピックに向けた サイバー攻撃に対する人材育成に関する研究

– サイバー攻撃の動向（教材より） –

サイバー攻撃の動向

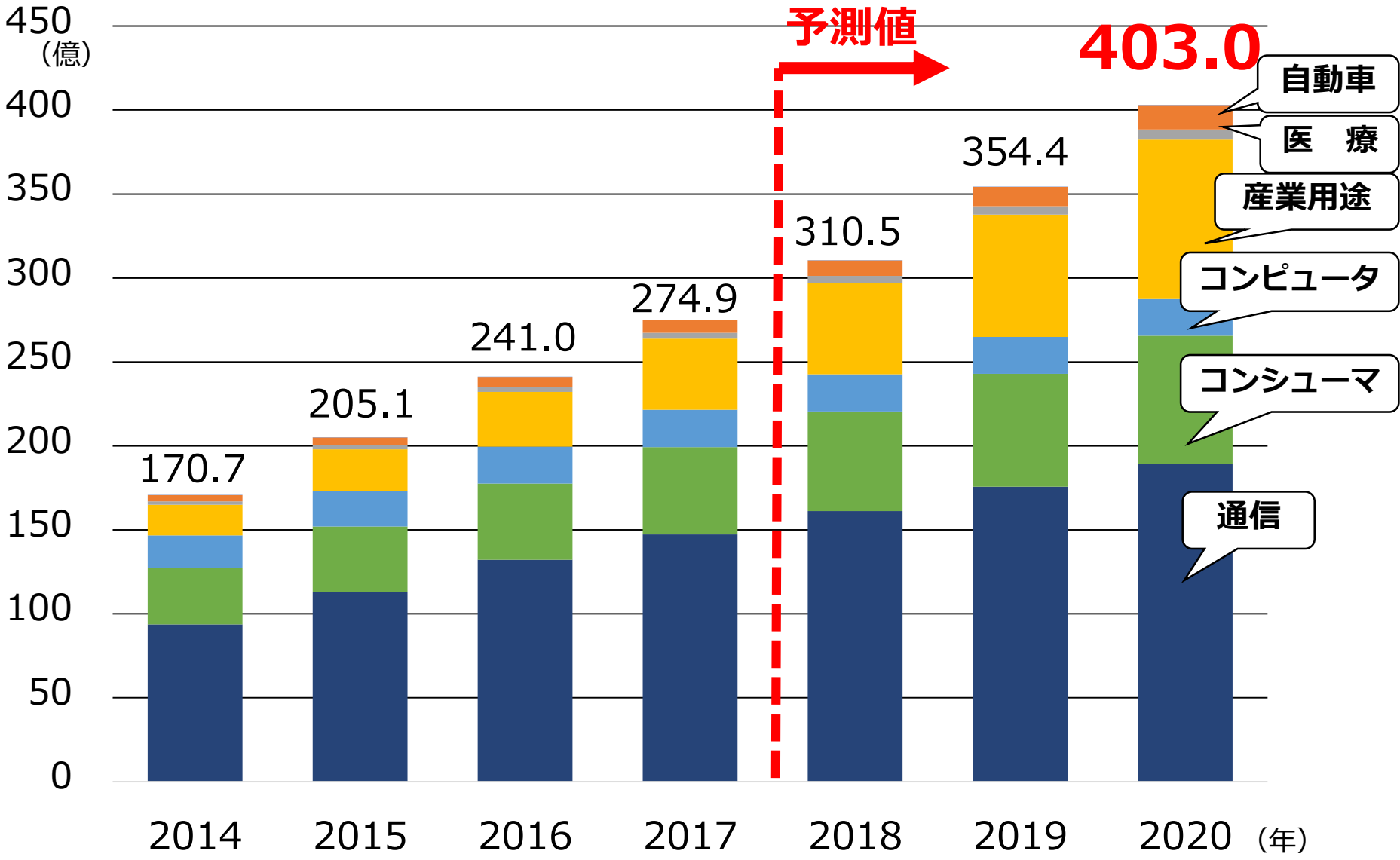
■我が国へのサイバー攻撃の増加



警察庁資料より作成

サイバー攻撃の動向

■世界のIoTデバイスの数の推移及び予測



出典：平成29年度情報通信白書（総務省）

サイバー攻撃の動向
■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

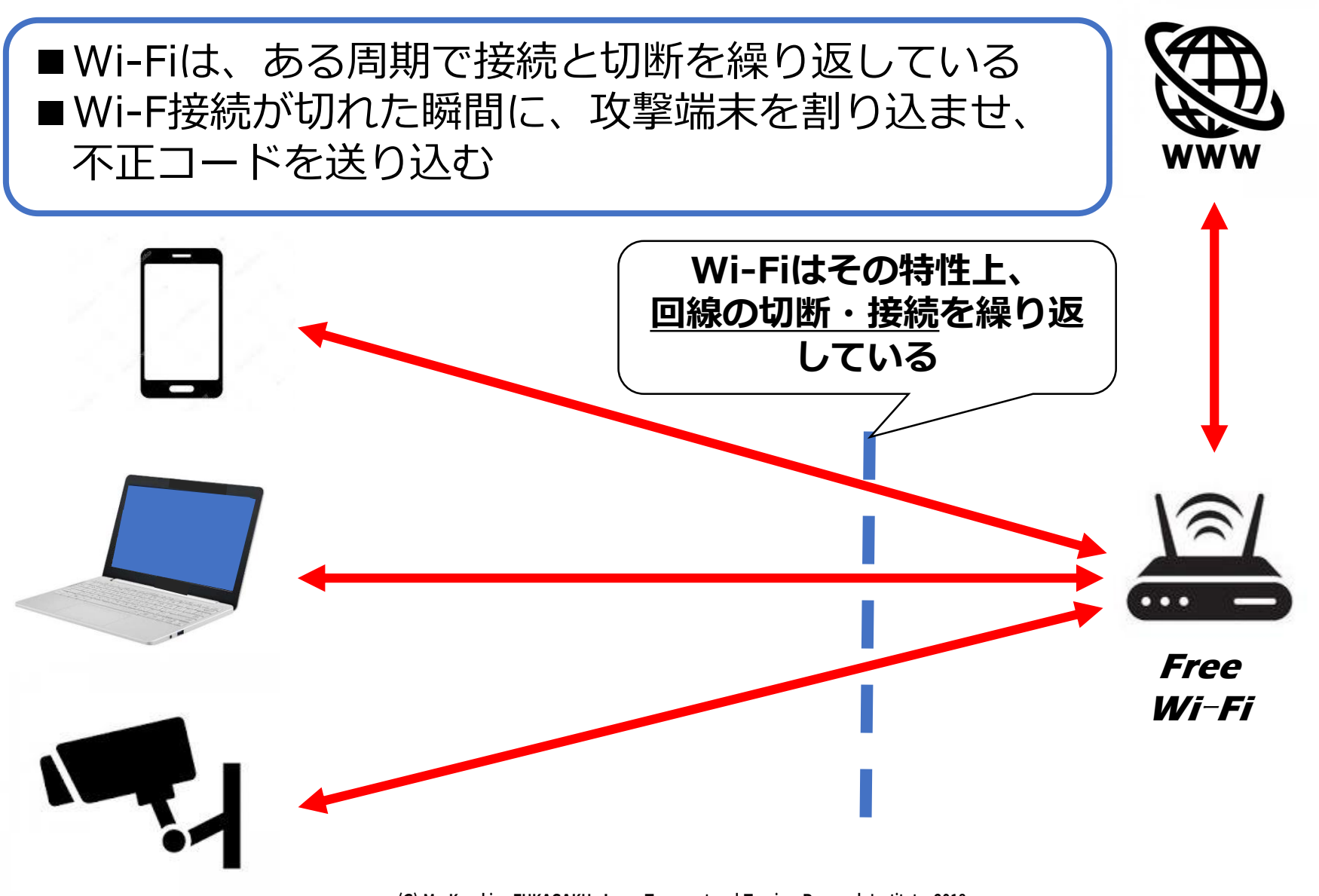
- IPカメラを踏み台としたDDoS攻撃 ➡ **業務停止の可能性**
- 画像無断公開サイト ➡ **情報漏えいの可能性**

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/10548

サイバー攻撃の動向

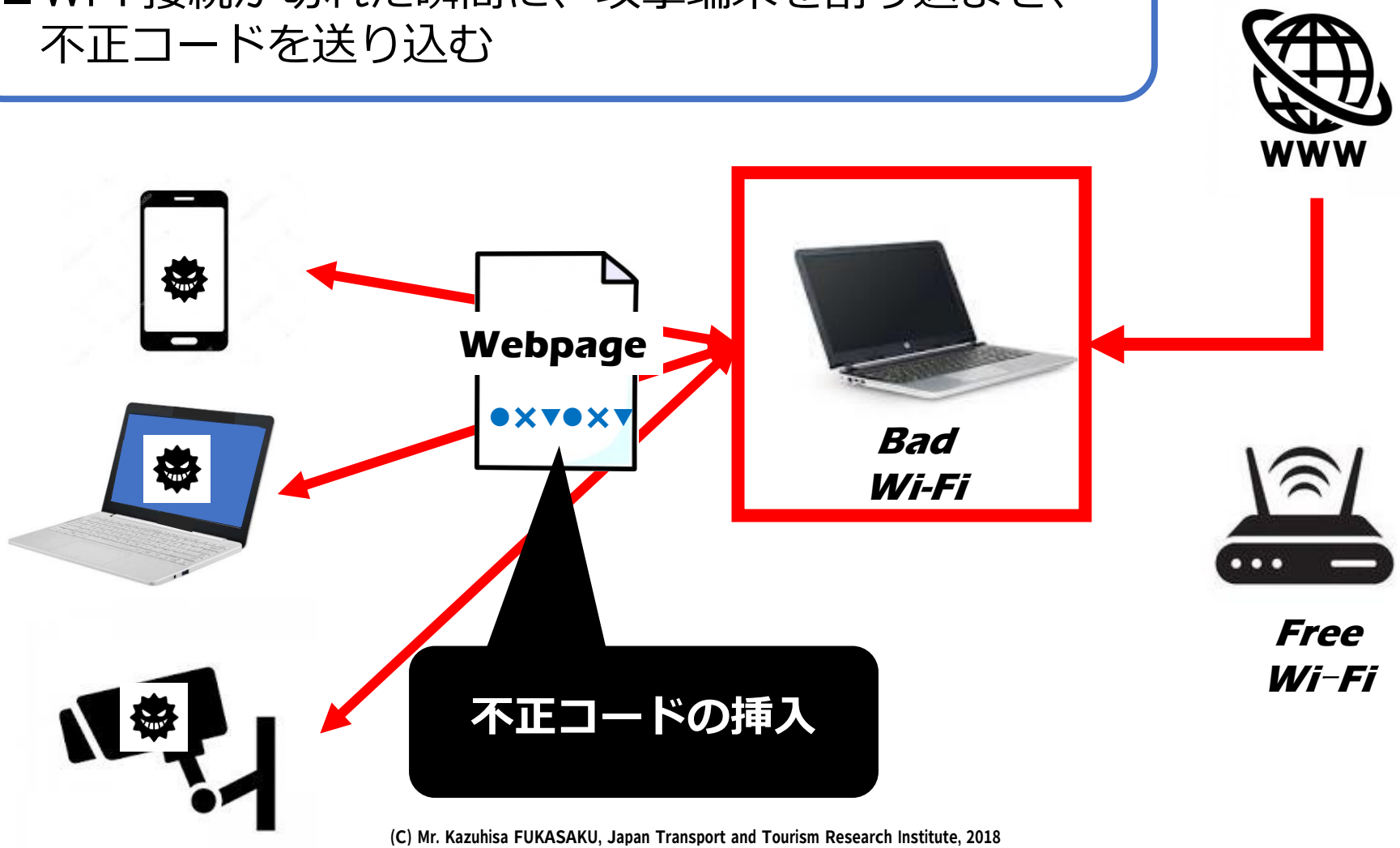
■Wi-Fiを活用した攻撃

■Wi-Fiは、ある周期で接続と切断を繰り返している
■Wi-F接続が切れた瞬間に、攻撃端末を割り込ませ、不正コードを送り込む



サイバー攻撃の動向

- Wi-Fiは、ある周期で接続と切断を繰り返している
- Wi-F接続が切れた瞬間に、攻撃端末を割り込ませ、不正コードを送り込む



サイバー攻撃の動向

■サイバー攻撃の代表的な事例（2015年～）

【鉄道分野】

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）
解雇された従業員がネットワークパスワード書き換え、コアシステムにアクセス出来なくなった。
サンフランシスコ市営鉄道でランサムウェアMamba感染（2016年）
Mambaによる攻撃を受け、 コンピュータや発券機が停止した。
ドイツ鉄道でランサムウェアWannaCry感染（2017年）
WannaCryによる攻撃を受け、発着時刻を表示する駅の電光掲示版が停止した。

【航空分野】

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った。
ベトナム航空へのサイバー攻撃（2016年）
システムへ侵入され、ウェブページの改ざん、顧客情報の漏えい、空港内放送システムが乗っ取られた。
ウクライナ空港へのサイバー攻撃（2017年）
世界的な大規模サイバー攻撃により、空港のWebサイトなどが使用不能になった。

サイバー攻撃の動向

■攻撃者、攻撃目的、攻撃対象

攻撃者	攻撃目的	攻撃対象
個　　人	技術誇示 愉快犯	不特定多数
特定組織や 国家による犯行	政治要求 金銭要求 情報搾取	国家、企業、個人 などを標的とした 攻撃

攻撃が専門的・組織的になってきており、明確な目的のもと、特定のターゲットを標的に狙う方向にシフト

サイバー攻撃の動向

■攻撃経路と手法

攻撃経路

フロッピーディスク
メール
ネットワーク（有線）

攻撃経路の多様化

メール
ネットワーク（有線+Wi-Fi）
USBメモリ
Webページ
IoT機器

攻撃手法

ウィルス/ワーム
スパムメール、スパイウェア
Dos攻撃等

攻撃の高度化

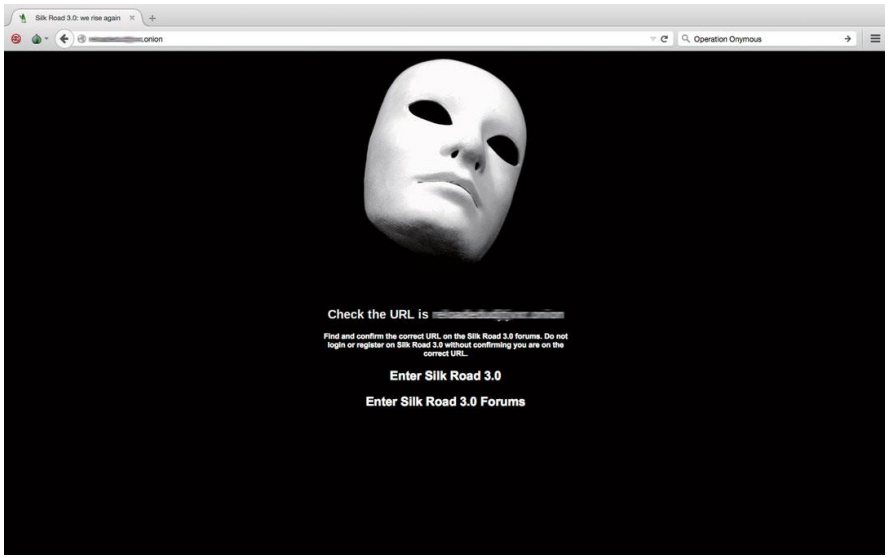
ウィルス/ワームの進化
(マクロウイルス、ランサムウェア)
フィッシングメール
メール搾取/スパムメール
DDos攻撃/不正アクセス

サイバー攻撃の動向

■攻撃経路と手法

【ダークウェッブ】

■グーグルなど通常のブラウザではアクセスできない
■ウィルスなどのプログラムを販売
■ID、パスワードなどの個人情報の販売
■ハッカーの情報交換のフォーラム　など



サイバー攻撃の動向

◆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

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 サイバー攻撃に対する人材育成に関する研究

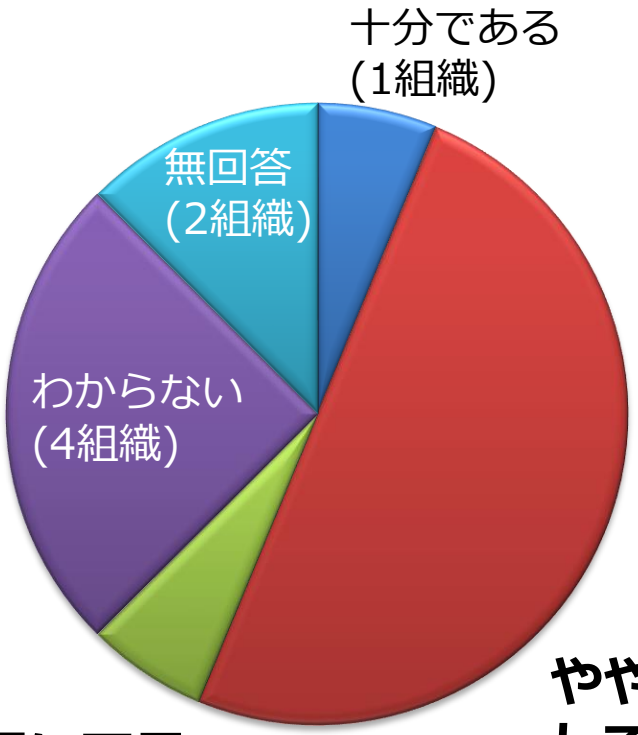
－ 人材育成カリキュラム－

人材育成カリキュラム

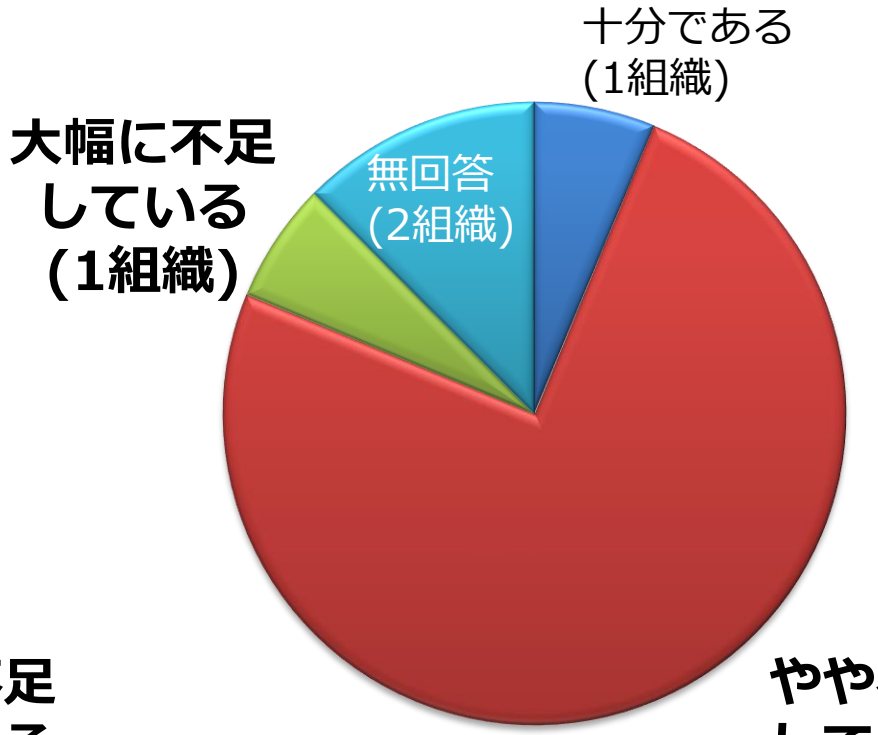
■セキュリティに携わる人員、スキル面での充足度ともに不足

セキュリティ業務担当者の充足度（平成27年度）

【人員】



【スキル】



人材育成カリキュラム

■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）

サイバー攻撃の際の対応手順

対応	担当部署		サイバー攻撃の際の役割
	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

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**

■演習での主な討議内容

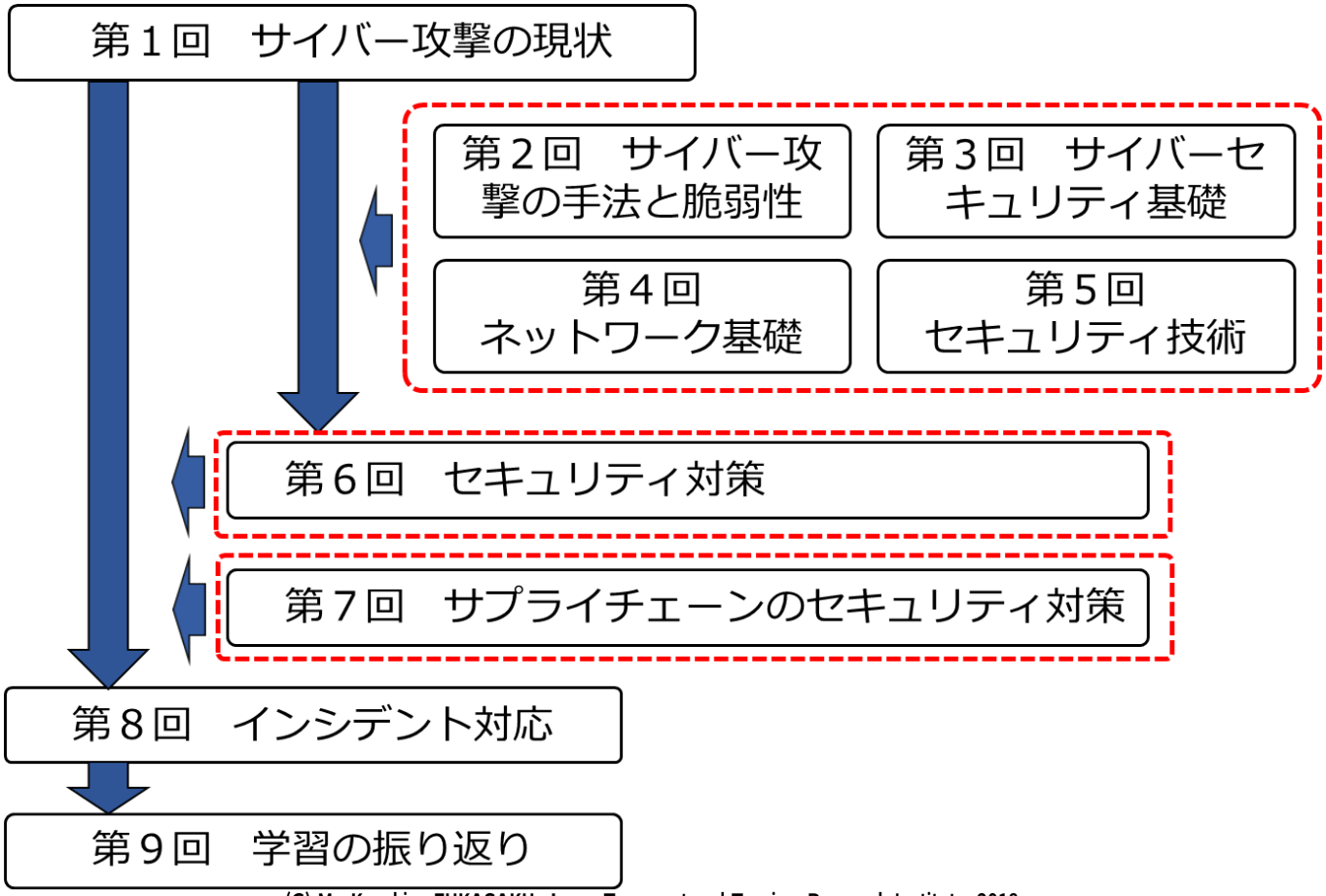
初動対応	■ 感染拡大を防ぐために何をしなければならないか ■ 他部門への報告、委託業者への指示内容
エスカレーション	■ 具体的に想定される被害と範囲 ■ 上層部へ何をどう説明するのか
原因特定	■ 証拠保全をどう実施するか ■ 攻撃方法の特定
今後の対策	■ 再発防止策の立案 （技術、人的管理、法務に対して、 短期、中期、長期の視点から）

人材育成カリキュラム

【求められる人材像】

■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

■ 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



東京オリンピック・パラリンピックに向けた サイバー攻撃に対する人材育成に関する研究

– サイバー攻撃対策（教材より） –

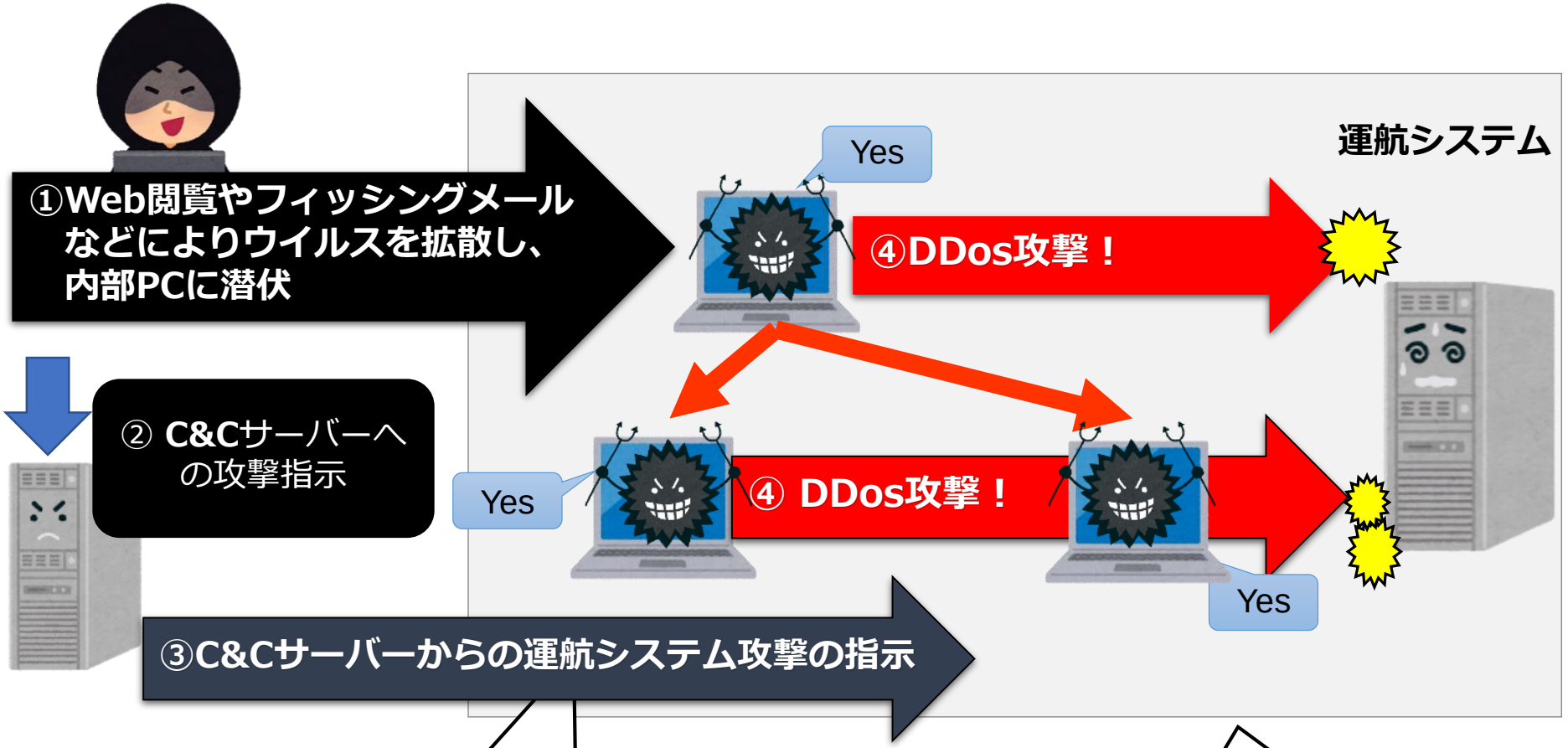
サイバー攻撃対策

■サイバー攻撃の事例と対策

	内容
1)攻撃対象	■ポーランド航空の運航システム
2)攻撃手法	■**Web閲覧やフィッシングメール**などにより、**内部のPCがウィル感染**、感染した内部のPCから運航システムへDDos攻撃
3)被　　害	■DDos攻撃により、ネットワークに過大な負荷がかかり、**地上運航システムに障害が発生し、フライトプランが作成できなくなった。** ■この結果、**ワルシャワ・ショパン空港出発便のフライトプランが作成不可能となり、10便が欠航**、乗客1,400人が空港に足止めとなり、システム復旧に5時間を要した。 ■空港システムに影響はなく、ポーランド航空のみが攻撃された。

サイバー攻撃の事例と対策の概要

■攻撃の流れ（ポーランド航空へのサイバー攻撃）



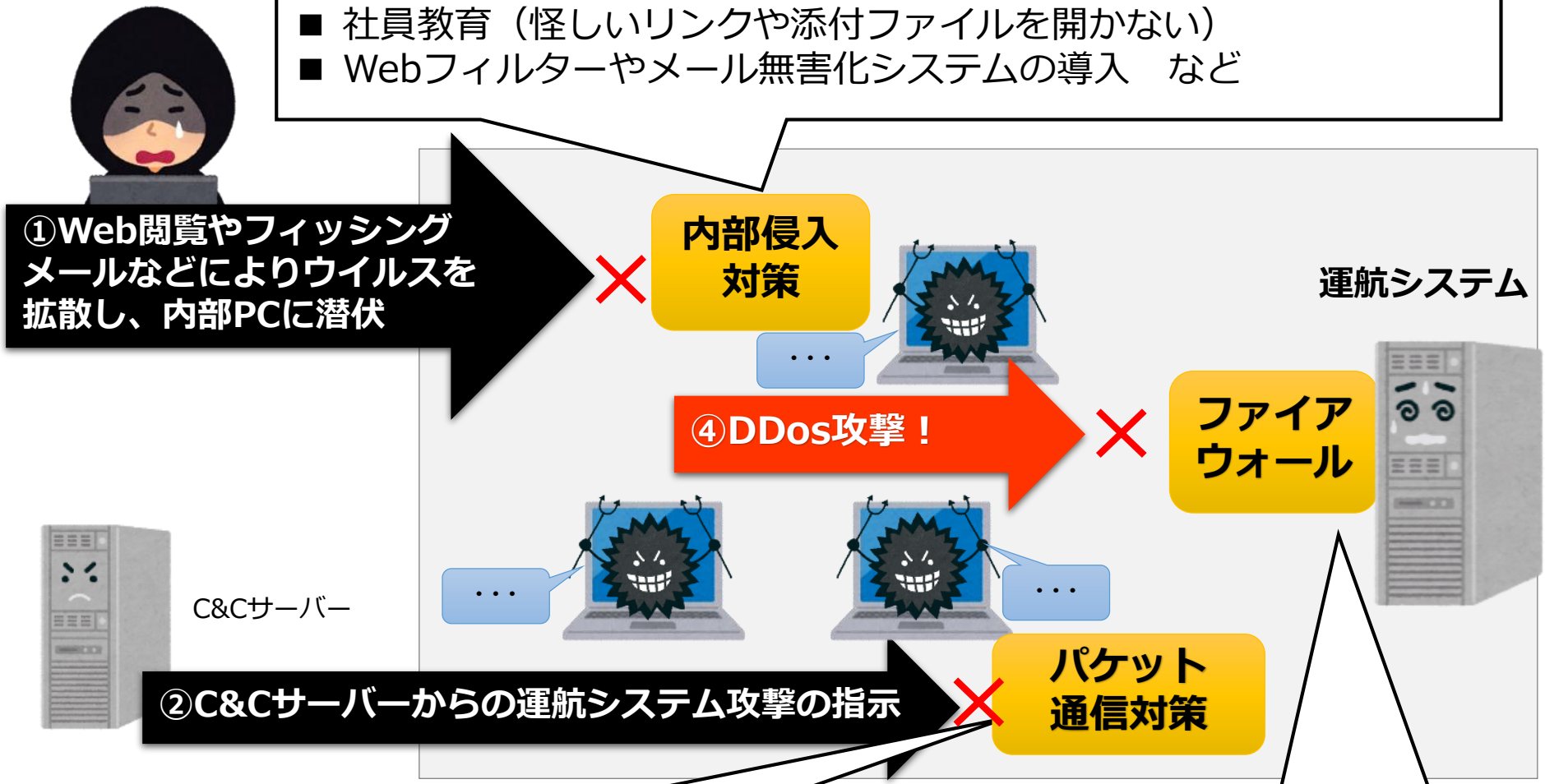
- 内部侵入対策不備
- ウイルス対策不備

- ウイルス対策及び拡散対策がされていない
- C&Cサーバーとの不正な通信を検知する仕組みがなく発見されていない

サイバー攻撃の事例と対策の概要

■主な攻撃対策（ポーランド航空へのサイバー攻撃）

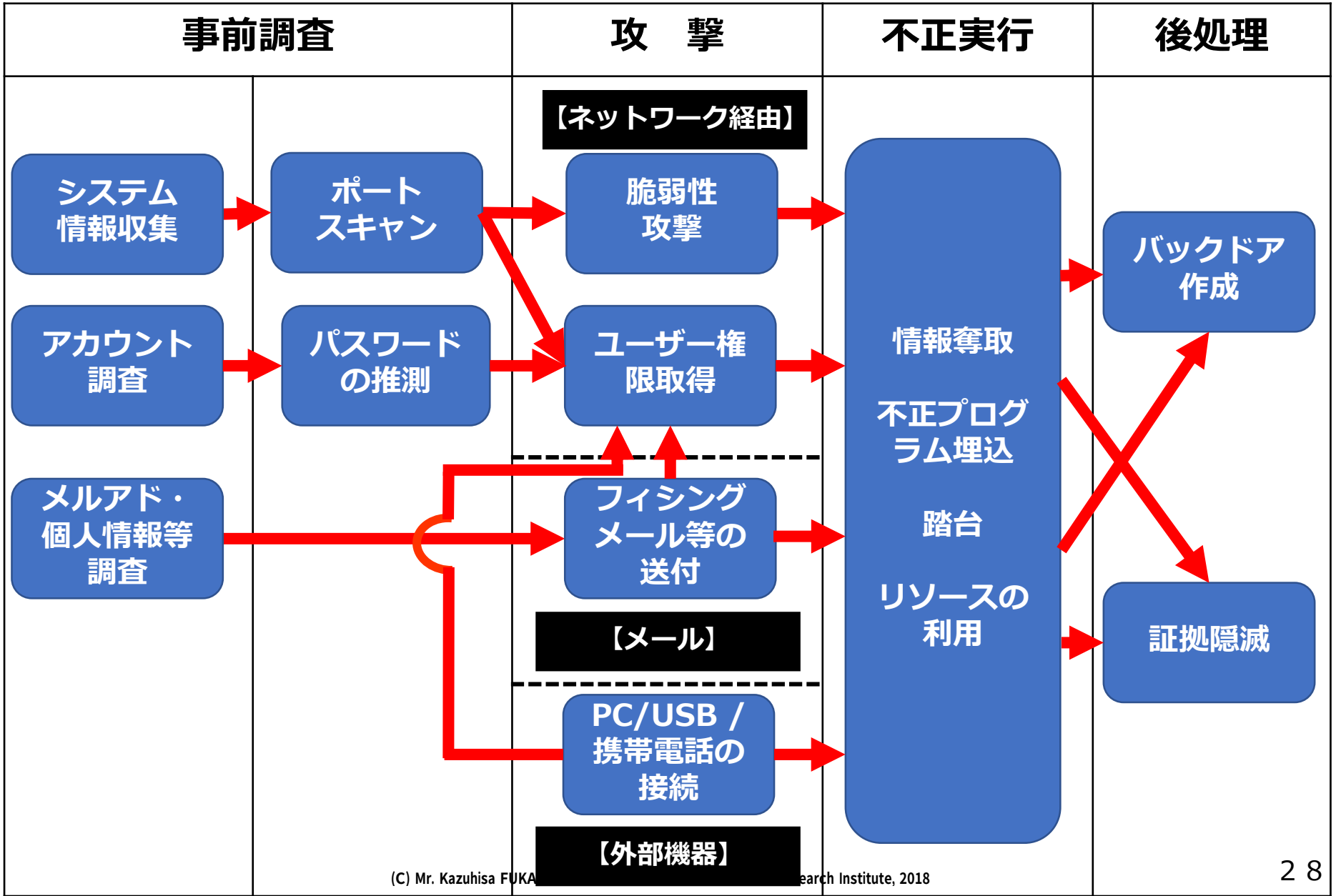
■ パソコンのウイルス対策（アンチウイルスソフト及びOSの更新）
■ 社員教育（怪しいリンクや添付ファイルを開かない）
■ Webフィルターやメール無害化システムの導入　など



■パケット監視システムの導入による不正通信の監視と無効化　など

■ファイアウォールの設置による攻撃の遮断　など

サイバー攻撃の事例と対策の概要
■攻撃の流れ



サイバー攻撃に対する主な対策

内　容	手引書（H28年）をもとにセキュリティ対策の概要を学習
ねらい	■手引書の概要の理解すること ■主なサイバー攻撃対策の概要を把握し、システム維持管理者が日常業務に活用できるようになること

学習項目	内容
システム・機器のセキュリティ対策	■マルウェア対策 ■外部ネットワークとの分離 ■他ネットワークとの接続 ■通信のセキュリティ ■不正処理防止策 ■アクセス制御 ■ログの取得・保管・保全　等
運用・管理のセキュリティ対策	■セキュリティ仕様の確認 ■機器等の構成・変更管理 ■管理者権限の割当 ■外部記憶媒体のマルウェア対策 ■修正プログラムの適用 ■セキュリティ監視　　等

東京オリンピック・パラリンピックに向けた サイバー攻撃に対する人材育成に関する研究

－経営を取り巻く外部環境リスク－

経営を取り巻く外部環境リスク（情報漏洩）

A社（金融代行業）

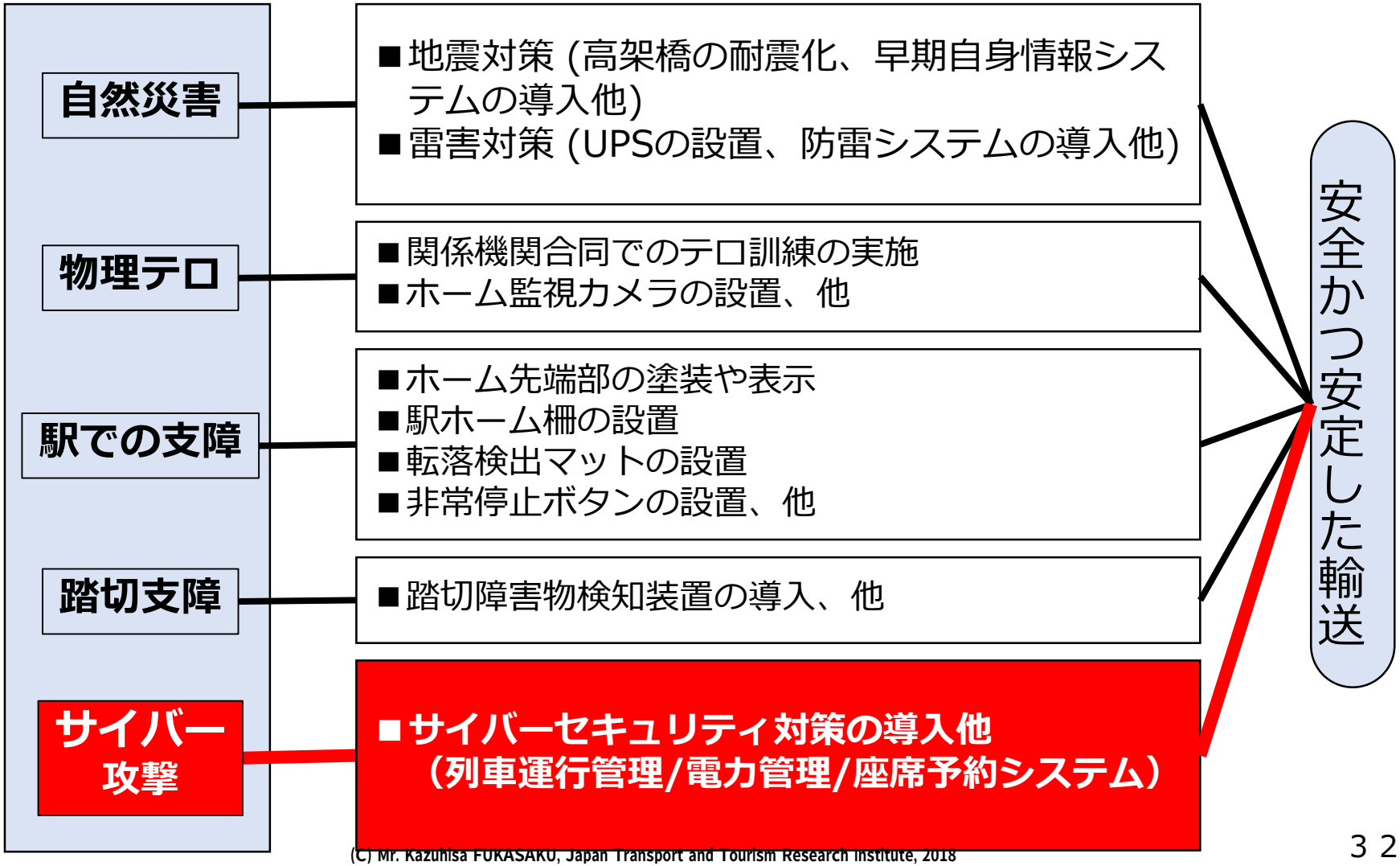
概　　要	運営を委託しているクレジットカード支払いサイトから**約70万件の個人情報が漏洩**。
流出経路	サーバーの脆弱性を利用したバックドアプログラムにより情報漏洩
対　応	■報酬の減額 ・代表取締役社長、取締役副社長⇒**月次報酬の30%を3か月減額** ・取締役⇒**月次報酬の10%を1か月減額** ■インシデント対応等で**2億7000万円の特別損失を計上**。

B社（情報・通信業）

概　　要	通信サービス利用者の氏名、**メールアドレスなど約460万件が流出**
流出経路	恐喝未遂の容疑者が、退職者から管理権限のあるユーザIDとパスワードを入手し、情報搾取
対　応	■報酬の減額 ・代表取締役⇒**６か月間５０%減給** ・取締役副社長兼取締役ＣＴＯ⇒**３か月間３０%減給** ■**１００億円以上のインシデント対応費用**が発生 ■漏えいが発覚した２月２４日に**株価が３００円下落**

サイバー攻撃に対する経営リスク

外部環境リスクのひとつとしてサイバー攻撃を位置づけ、対策を実施し、安全かつ安定した輸送を実現していく必要がある。



今後の取り組み

教材を用いた教育（試行）

経営層への啓発セミナー

Japan Transport and Tourism Research Institute

Supported by THE NIPPON FOUNDATION

ご清聴ありがとうございました。

この調査研究は、日本財団の助成事業により実施したものです。