交通分野へのサイバー攻撃に対する
セキュリティ人材育成に関する調査研究

報告書

平成 31 年 3 月

一般財団法人　運輸総合研究所

はじめに

本報告書は、平成 30 年度日本財団助成事業として実施した「交通分野へのサイバー攻撃に対するセキュリティ人材育成に関する調査研究」の成果をまとめたものである。

運輸総合研究所では、平成 27 年度からの 2 年間で「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」を実施し、交通事業者のセキュリティリスク分析を踏まえ、国内外の対策ガイドラインなどを整理し、それらに基づいて、鉄道分野と航空分野の対策をとりまとめた手引きの作成を行った。この成果を踏まえて、平成 29 年度には、作成した手引きを実践する人材を育成することを目指し、鉄道分野と航空分野の人材育成カリキュラムの作成を行った。

本年度調査では、昨年度調査で作成した人材育成カリキュラムに基づき、鉄道分野及び航空分野の教材を作成し、システム維持管理者を対象として、作成した教材を用いた教育の実施、ならびに CSIRT 要員を対象とした机上演習の実施による人材の育成に取り組んだ。また、サイバーセキュリティへの意識・理解向上を目的として経営層を対象としたセミナーを実施した。

本研究の実施にあたっては、田中英彦 岩崎学園理事（情報セキュリティ大学院名誉教授・東京大学名誉教授）を委員長とする委員会を設置し、我が国の交通分野のサイバーセキュリティにかかわる委員の皆様に多大なるご助言をいただいた。また、一般社団法人 日本生活問題研究所のご協力に対し、ここに改めて深く感謝の意を表す次第である。

平成 31 年 3 月

一般財団法人　運輸総合研究所
会長　　宿利　正史

「平成 30 年度　鉄道のサイバー攻撃に対する人材育成に関する調査研究」検討委員会

名　　簿

＜敬称略・順不同＞　※（　）内は上記の前任者

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
		鉄道関係者
〃	金子　修久 （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
〃	蔭山　良幸 （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
〃	春成　　誠	一般財団法人運輸総合研究所　理事長
事務局		一般財団法人　運輸総合研究所
作業協力		一般社団法人　日本生活問題研究所サイバーセキュリティ支援センター

「平成 30 年度　航空のサイバー攻撃に対する人材育成に関する調査研究」検討委員会

名　　簿

＜敬称略・順不同＞　※（　）内は上記の前任者

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
〃		航空・空港関係者
〃	金子　修久 （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
〃	蔭山　良幸 （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
〃	春成　　誠	一般財団法人運輸総合研究所　理事長
事務局		一般財団法人　運輸総合研究所
作業協力		一般社団法人　日本生活問題研究所サイバーセキュリティ支援センター

目次

第１章.　　序文

１．１.研究背景

近年急増しているサイバー攻撃は、我が国にとっても大きな脅威となっている。また、我が国では 2020 年に東京オリンピック・パラリンピック（以下、2020 年東京五輪大会）が開催されるが、過去のオリンピックでは､大会そのものが幾度となくサイバーテロの標的となっている｡そのため、2020 年東京五輪大会の成功に向けて、サイバーテロ対策は重要な課題と考える。

鉄道分野、航空分野[1]は、我が国の第 4 次行動計画において重要インフラ分野に指定されており、サイバー攻撃により安全・安定な運行/運航が妨げられると、その影響は甚大になる恐れがある。鉄道分野及び航空分野において、国内では、現時点においては大規模なサイバー攻撃は報告されていないが、海外ではサイバー攻撃被害が報告されており、国内においても脅威が増していると考えられる。また、制御システムの IoT（Internet of Things）化など更なる技術発展により、さらに脅威が増す可能性がある。

鉄道分野及び航空分野においても、サイバーセキュリティ人材の不足が懸念されており、過去の研究では、研究対象とした鉄道分野及び航空分野の事業者の７割以上が人材育成に課題があると回答があった。このため、鉄道分野及び航空分野においても、サイバー攻撃に対応できる人材の育成が急務であると考える。

サイバーセキュリティ人材の育成は、各交通事業者の実態に応じて実施していくことになるが、これまで、鉄道分野及び航空分野のサイバーセキュリティ人材育成に関するカリキュラムの研究はあまり進んでいない。そのため、鉄道及び航空などの事業者各々でサイバーセキュリティ人材を育成するために参考となるカリキュラムとこれに基づく教材資料を作成し、鉄道分野及び航空分野の事業者向けに教育の試行を実施した。

１．２.研究目的

本研究では、2020 年東京五輪大会に向け、①昨年度作成したカリキュラムに基づく鉄道分野及び航空分野の教材の作成、②サイバー攻撃の最前線で業務に従事する現場担当者（システム維持管理者）を主な対象者とした教育（①で作成した教材を使用)、ならびにサイバー攻撃対策を主導する CSIRT 要員を対象とした机上演習による人材育成、③経営層を対象としたセミナーの実施による経営層のサイバーセキュリティへの意識・理解向上を目的とする。

1)本調査研究における「航空分野」とは、航空輸送事業者及び空港運営事業者のことをいう。

１．３．これまでの研究成果

１．３．１．　前提条件

平成 29 年度に運輸総合研究所が実施した研究において、人材育成カリキュラム（教育課程）を作成した。カリキュラムの作成の前提条件として、本カリキュラムにおける、求められる人材像と能力の定義を行なった。

求められる人材像は、以下のとおりである。

・インシデント[2]発生の際、その原因がサイバー攻撃である疑いを考慮し、適切に対応できる人材

・サイバー攻撃に対処（原因究明、復旧など）する専門機関と連携して、インシデント対応を実行（支援）できる人材

必要となる能力は、以下のとおりである。

・サイバー攻撃に関わるインシデント対応に関する能力

・上記に関わる情報技術（IT）に関する能力

これを踏まえ、本カリキュラムの育成対象者は、事業部門のシステムの維持管理を担う担当者とした。

[2] ）本調査研究における「インシデント」とは、IT 用語における「セキュリティインシデント」を指し、鉄道運行／航空運航の遅延、運休／欠航、及び鉄道／航空の安全輸送に対する支障などの影響を及ぼす、または、その恐れのあるシステムの不具合が発生した状態や現象をいう。

１．３．２．　カリキュラムの構成

国内外の人材育成カリキュラム事例収集や机上演習の実施結果などを基に学習内容を検討し、鉄道分野及び航空分野の事業者がサイバーセキュリティ人材を育成する際の参考資料となり得るカリキュラムを作成した。カリキュラムの構成と学習内容を下表に示す。

表1.1　カリキュラムの構成（各講座120分）

	講座名	目　標
第１回	サイバー攻撃の現状	サイバー攻撃により、業務に関わるシステムの停止や誤作動が生じると、社会的混乱や人的被害をもたらす可能性があり、その対策が急務であることを認識する。
第２回	サイバー攻撃の手法と脆弱性	鉄道分野及び航空分野において発生する可能性のあるサイバー攻撃の手法と脆弱性を理解する。
第３回	サイバーセキュリティ基礎	サイバーセキュリティ対応の基礎となる考え方や手法の概要とその重要性を理解する。
第４回	ネットワーク基礎	サイバー攻撃の概要を把握するため、また、サイバー攻撃に対処（原因究明、復旧など）する専門機関と連携し、対応（支援）するために必要となるネットワークの知識を学習する。
第５回	セキュリティ技術	サイバー攻撃に対処（原因究明、復旧など）する専門機関と連携し、対応（支援）するために必要となるセキュリティ技術の用語と概要を学習する。
第６回	サイバー攻撃対策	手引き[3]をもとに、主なセキュリティ対策の概要を学習する。
第７回	サプライチェーンのセキュリティ対策	サプライチェーンのセキュリティ対策の重要性とインシデント対応に備えるための重要なポイントを学習する。
第８回	インシデント対応	インシデント発生の際、その原因がサイバー攻撃である疑いを考慮し、迅速かつ適切に対応（支援）するためのポイントを学習する。
第９回	学習の振り返り	学習の振り返りを通して本カリキュラムを総括する。

[3]）本項における「手引書」とは、平成 28 年度に（一財）運輸総合研究所の調査研究において策定された「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」をいう。

表1.2　カリキュラム内容の整理結果

No.	講座名	学習内容
第１回	サイバー攻撃の現状	（１）サイバーセキュリティに関する動向 （２）脅威とインシデント （３）想定される攻撃手法 （４）セキュリティ確保への取り組みの状況
第２回	サイバー攻撃の手法と脆弱性	（１）サイバー攻撃の脅威 （２）脆弱性
第３回	サイバーセキュリティ基礎	（１）セキュリティマネジメント （２）資産管理の重要性 （３）リスク評価の重要性
第４回	ネットワーク基礎	（１）ネットワークとプロトコル （２）TCP/IP の概要 （３）ネットワーク接続機器
第５回	セキュリティ技術	（１）対策技術の用語と概要 （２）多層防御 （３）フォレンジックの概要
第６回	サイバー攻撃対策	（１）設備・システムのセキュリティ対策 （２）運用・管理のセキュリティ対策
第７回	サプライチェーンのセキュリティ対策	（１）サプライチェーンのセキュリティ対策の重要性 （２）外部委託範囲の特定と管理 （３）情報の入手とその有効活用
第８回	インシデント対応	（１）インシデント発生時の対応手順 （２）インシデント対応体制 （３）初動対応のポイント
第９回	学習の振り返り	（１）コースのまとめと振り返り （２）質疑応答

交通事業者各々で、対象となるシステムや必要となる知識や役割、対応方法などにも違いがあると思われるため、学習内容は、本カリキュラムの内容を参考にしつつ、鉄道分野及び航空分野などの事業者の実態を鑑み、必要に応じて取捨選択することを推奨することとした。このため、講座を取捨選択する際の参考となるよう、以下に各講座の関係を示した。

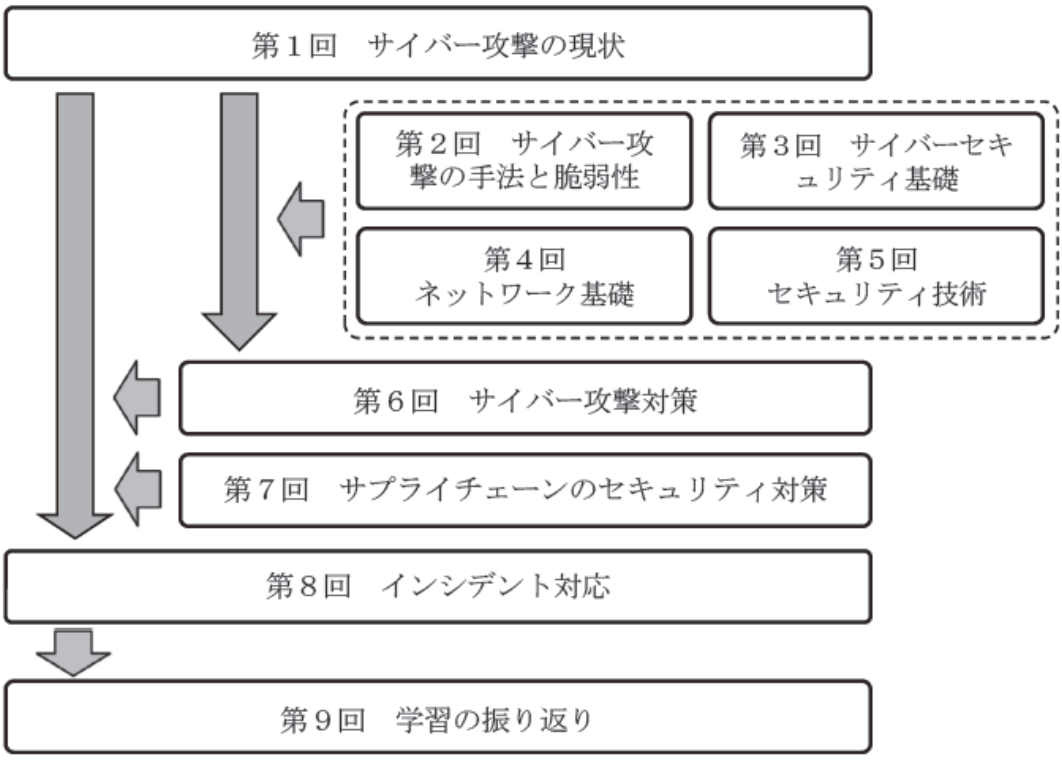


図1.1　各講座の関係

本カリキュラムは、第１回～第９回までの一連の講座を受講することを前提としているが、その内の第１回、第８回、第９回の３講座のみの受講は、目的を達成するための最小の構成としている。この構成では、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た上で、現状を正確に関係部署に報告できることを目標とするレベルを目指している。

上記の構成に第６回と第７回の講座を追加する構成は、サイバー攻撃に対応するための一連の対策を学習することを目指している。当該システムを熟知する立場から、サイバー攻撃発生の際に関係各所と連携して対処できることを目標とするレベルを目指している。第７回のサプライチェーンのセキュリティ対策は、最近のサイバー攻撃の脅威として特に注目される対策であるため、カリキュラムに追加したものである。

第２回～第５回の講座は、サイバー攻撃対策についてより深く理解するための基礎的内容を追加する構成である。社会的・技術的側面からサイバー攻撃及びその対策を理解し、運用としてのシステム維持管理方針を立案することを目標とするレベルを目指している。

１．４．研究フロー

本研究の検討フローを以下に示す。

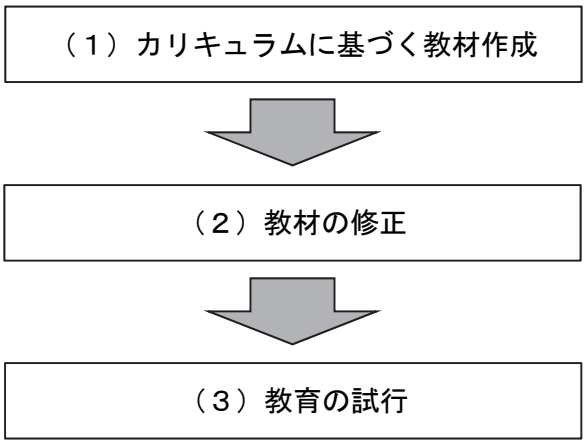


図1.2　本研究の検討フロー

（１）　カリキュラムに基づく教材作成

人材育成カリキュラムに基づき教材を作成する。人材育成カリキュラムを構成する各講座については参考となる教育教材が既存しているため、これらを参考とし、本カリキュラムの育成対象者、求められる人材像と能力を考慮して教材化する。

（２）　教材の修正

（１）の結果を踏まえ、作成した教材に対して検討委員のレビューによる意見集約を行い、教材資料の修正を行う。併せて、教材の在り方を検討し、各事業者が実施する教材の取捨選択及びカスタマイズの方針を検討する。

（３）　教育の試行

（２）の結果を踏まえ、鉄道分野及び航空分野の事業者より受講者を募り、作成した教材資料を用いて教育を試行する。教育の試行時において受講者へのアンケートを実施し、作成教材の実効性を確認する。

１．５．作成した教材とその取扱い

作成した教材は、鉄道編及び航空編それぞれを別冊として取りまとめている。

また、作成した教材はセキュリティ人材育成のために、自社社員や関連会社社員への教育など幅広く活用できるように電子データを提供している。提供依頼や二次利用を希望される場合は、本報告書最終項に記載の連絡先までお問合せいただきたい。

第２章.　　教材作成

２．１.教材構成

本教材は、各事業者が自社において実施する要員教育に使用することを想定しているため、講師向けあるいは教育を企画立案する担当者向けの指導要領を含めることとした。本研究において作成する教材の内訳を下記に示す。

（１）　指導要領

- 講師が講座についての理解を深め、講義を行う際に参照するもの。
- 教育を企画立案する担当者が、講座についての理解を深め、企画立案の際の参考とするもの。

（２）　教材資料（スライド）

- 講義の際にスライド投影及び受講者に配布するもの。
- 講師が講義の際に参考とする説明文をノート部分に付記しているもの。

（３）　アンケート用紙

- 第１～８回の各講座終了後に実施し、受講者の理解度と意識付けを確認するもの。

２．２.指導要領

指導要領として以下を作成した。

- 鉄道分野における指導要領
- 航空分野における指導要領

指導要領は、事業者において教育プログラムを立案する者及びトレーニングを実施する講師を対象読者としている。主な記載事項を以下に示す。

- 教育の目的、対象者、達成目標及び講座の構成について
- トレーニングの概要と実施方法について
- 講座の構成と解説ポイントについて
- 参考となる資料について

２．３．教材資料とアンケート

鉄道分野の教材として、以下を作成した。

- 第１回：サイバー攻撃の現状【鉄道編】
- 第２回：サイバー攻撃の手法と脆弱性【鉄道編】
- 第３回：サイバーセキュリティ基礎【鉄道編】
- 第４回：ネットワーク基礎【鉄道編】
- 第５回：セキュリティ技術【鉄道編】
- 第６回：サイバー攻撃対策【鉄道編】
- 第７回：サプライチェーンのセキュリティ対策【鉄道編】
- 第８回：インシデント対応【鉄道編】
- 第９回：学習の振り返り【鉄道編】

航空分野の教材として、以下を作成した。

- 第１回：サイバー攻撃の現状【航空編】
- 第２回：サイバー攻撃の手法と脆弱性【航空編】
- 第３回：サイバーセキュリティ基礎【航空編】
- 第４回：ネットワーク基礎【航空編】
- 第５回：セキュリティ技術【航空編】
- 第６回：サイバー攻撃対策【航空編】
- 第７回：サプライチェーンのセキュリティ対策【航空編】
- 第８回：インシデント対応【航空編】
- 第９回：学習の振り返り【航空編】

教材は、講座毎に、受講者に提示するスライドとしてマイクロソフト社の PowerPoint を利用して作成し、各スライドのメモ欄に講義のポイント及び解説を付記している。また、各講座において、受講者の意見を収集するためのアンケート実行用紙を作成した。

第３章.　　教材修正

３．１.修正方針

３．１．１．　意見収集

作成した教材に対して検討委員のレビューによる意見集約を行なった。主な意見は以下のとおりである。

（１）　鉄道分野

鉄道分野における主な意見を以下に示す。

- 全体を通じて内容を盛り込みすぎではないかと感じました。カリキュラムの時間内でこれだけの文字の詰まったスライドを提示されても消化不良になるのではないかと思います。もう少し全体的に要点を絞って、補足資料的なスライドを増やすのもよいのではないかと感じました。
- 鉄道従事者の理解を得るため、サイバー攻撃は鉄道の本分である「安全」としての取り組みであることを示すべきではないか。(例えば「ホーム事故にはホームドア、踏切事故には障害物検知装置や警報機があるように、サイバー攻撃対策として鉄道のシステムにファイアウォールやアンチウイルスソフトが必要である」といった論調を入れるなど)
- 留意すべきポイントが通常業務と何が違うのかわかりません。(サイバーセキュリティの視点で何が必要なのかを明確にした方がよいと思います。)
- 「システムがネットワークにつながり、便利になった反面、悪いことをする人にとっても、システムへの不正アクセスが容易な世の中となってきた」というような、2000 年以降のインターネットの出現により、誰もがサイバーセキュリティを気にする必要性が出てきたことを説明いただけないか？
- インターネットと分離されているシステムであっても、気にしなければならない理由を記載してもらいたい。鉄道システムは往々にして「分離されているから大丈夫」という認識のもとに構築されている部分が非常に多い。
- 「なぜサイバー攻撃かを見極めないとならないのか」、「サイバー攻撃とわかるとその後の対応として何が変わってくるのか」「そのためにはどこがポイントなのか」という話をもっと盛り込むようにお願いいたします。

（２）　航空分野

航空分野における主な意見を以下に示す。

- 全体感として、どの章で何をどの粒度で語るべきなのかの整合性が取れていないと思います。重複があったり、不足があったり。また、大局から詳細へむけて語っていくという統一感のある全体シナリオが見えません。ひとつひとつのコンテンツはそれなりなのですが、全体シナリオに問題があります。
- 受講者の教育後に期待するは何でしょうか？誰かに（決して自分ではない。）させなきゃ、という危機感でしょうか。それがこの教育の目的でしょうか。オリジナルの目的には「急

務であることを学習します」というのがゴールになっていますが、それが是だとすると、何のための教育かわからない。

- この回は目的からすると「航空分野において発生する可能性のあるサイバー攻撃の手法と脆弱性を学習します」とありますが、航空分野に関する内容は一切ありません。ここに書かれているのは一般的なサイバーセキュリティの話ですので、第一回とかぶります。もしくは第一回の詳細版でしょうか。航空分野において、を出すならば、航空独特の業務に照らし合わせて記載すべきです。
- 教育の教材案についてですが、コンテンツとしては辞書的で用語集としては、活用できますが、今回の演習の全体からそれぞれがどの部分のことをいっているのか、参考となるシステム構成のどの部分のことを説明しようとしているのかを充実してほしいです。

３．１．２．　修正方針の検討

検討委員のレビューから得られた意見をもとに、教材修正方針を検討した。主な内容は、以下のとおりである。

（１）　各講座のポイントの明確化

「留意すべきポイントが不明である、全体として整合性が取れていない」等の意見を踏まえ、各講座のポイントを明確化するための修正を以下のとおり実施することとした。

- 対象者がシステム維持管理者であることを踏まえて、各講座の位置付けを再度検討する。特に、システム維持管理者が関係者と連携するために理解しておく必要のある用語等、各講座における基礎的内容の抽出と整理を行う。
- 本教材の目的を踏まえて各講座の関係性を整理し、講座毎の目的達成のために必要となる知識の抽出と整理を行う。
- 目的達成のために必要となる「重要な項目」の抽出と整理を行う。
- 「重要項目」等の抽出・整理を踏まえて、教材内容の絞り込みを図る。

（２）　業種に則した内容の記載

「業務従事者の理解を得るための修正が必要である」との意見を踏まえ、業種に則した内容を記載するための整理を実施する。具体的には、以下の点に留意して教材内容の精査を実施する。

- 鉄道分野及び航空分野においても起こり得ると思われるサイバー攻撃の事例について、その根拠も含めて解説することを検討する。
- 教材において使用する用語等については、鉄道分野及び航空分野の用語用法に合わせて使用することを検討する。
- 教材において紹介するネットワーク構成例等について、鉄道分野及び航空分野において採用されている既存構成に合わせて採用することを検討する。

３．２．教材の修正

３．２．１．　各講座の位置付け

対象者がシステム維持管理者であることを踏まえて、各講座の位置付けを再度検討した。各講座の位置付けを以下に示す。

（１）　第１回（サイバー攻撃の現状）

第１回の位置付けは、サイバー攻撃の現状を理解し、本講義の受講の必要性を受講者に意識づけることにある。このため、受講者に対策の必要性を訴求するための社外動向と攻撃事例の紹介が重要となる。また、攻撃事例については、事例に見られる攻撃手法と脆弱性及び攻撃に対応するために必要となる対策の解説を行うことにより、システム維持管理者としての役割を意識付けする一助となる。

（２）　第２回（サイバー攻撃の手法と脆弱性）

第２回の講座では、第１回で紹介した攻撃事例を踏まえて、サイバー攻撃の手法と脆弱性を解説する。特に、典型的な外部からの攻撃手法の概要とマルウェアに関する基礎的な知識が必要である。

（３）　第３回（サイバーセキュリティ基礎）

第３回の講座では、システム維持管理者が、その役割を実行するために必要な基礎的知識を解説することを目的としている。基礎的知識としては、サイバーセキュリティ対応に必要となるセキュリティ管理の基本的な枠組みとリスク評価の手法が重要事項となる。実際のサイバー攻撃への対応時においては、資産の把握が重要となるため、資産管理の手法を学ぶことが重要となる。また、システム維持管理者が対象システムのリスク評価を体系的に実施することはないが、日々の業務におけるリスクへの気付きのために、リスクの評価手法を学ぶことは重要である。

（４）　第４回（ネットワーク基礎）

ネットワーク基礎知識は、セキュリティ技術を理解するために必要となる知識である。特にIP パケットの構造を理解することは、後述するセキュリティ技術を理解するために必要な知識である。また、システム維持管理者がその役割を実行するためには、対象となるネットワークの構成や構成機器の配置と役割に関する知識が重要である。

（５）　第５回（セキュリティ技術）

システム維持管理者がその役割を実行するためには、サイバーセキュリティ対策に必要となる技術的な基礎知識が必要である。セキュリティ技術の基礎としては、ファイアウォールに代表されるフィルタリング技術、認証技術、暗号化と電子署名、VPN があり、これらを含む基礎的なセキュリティ技術とこれらの技術を多層的に活用することの重要性を理解する必要があ

る。また、攻撃への対応においてはセキュリティベンダーが実施するフォレンジックについても、基礎的な知識が必要である。

（6） 第６回（サイバー攻撃対策）

サイバー攻撃への対策は、技術的対策のみならず、人的・組織的対策を含む体系的な対策が必要となる。このため、鉄道分野、航空分野のサイバーセキュリティ対策をまとめた手引書をもとに、サイバー攻撃への体系的な攻撃手法を解説する。

（7） 第７回（サプライチェーンのセキュリティ対策）

サプライチェーンのセキュリティ対策は、最近のサイバーセキュリティ対策において重要なトピックとなっている。このため、サプライチェーンのセキュリティ対策とは何かということについて理解するとともに、特に委託事業者との連携等、システム維持管理者がその役割を実行するために理解すべき事項を解説している。

（8） 第８回（インシデント対応）

本カリキュラムの目的は、システム維持管理者が迅速かつ適切にサイバー攻撃のインシデント対応を支援できるようになることである。このため、第８回の講座は、本カリキュラムで最も重要な講座である。本講座では、まず IT 部門が実施するサイバー攻撃によるインシデント対応の典型的な対応手順を学習し、これを踏まえたシステム維持管理者の役割について、インシデント対応の実行時のポイントについて解説している。

（9） 第９回（学習の振り返り）

第９回の講座では、本カリキュラムの目的を踏まえて、第１回から第８回までの学習内容の振り返りを実施している。前述したように、第８回のインシデント対応が本カリキュラムで最も重要な講座であることを踏まえ、第１回と第８回を総括した後に、第２回から第７回までの講座の振り返りを実施している。また、サイバー攻撃のシナリオをもとに、グループディスカッションを実施する構成としている。グループディスカッションにおいて学習内容の振り返りができるよう、シナリオは各講座の内容を含む内容としている。

３．２．２．　講座間の関係性の整理

講座間の関係のうち、重要と考えるものを以下にピックアップした。本カリキュラムの主題は第８回であり、インシデント対応が最も重要な回となる。このため、第８回を本カリキュラムの最も重要な講座と位置付けている。

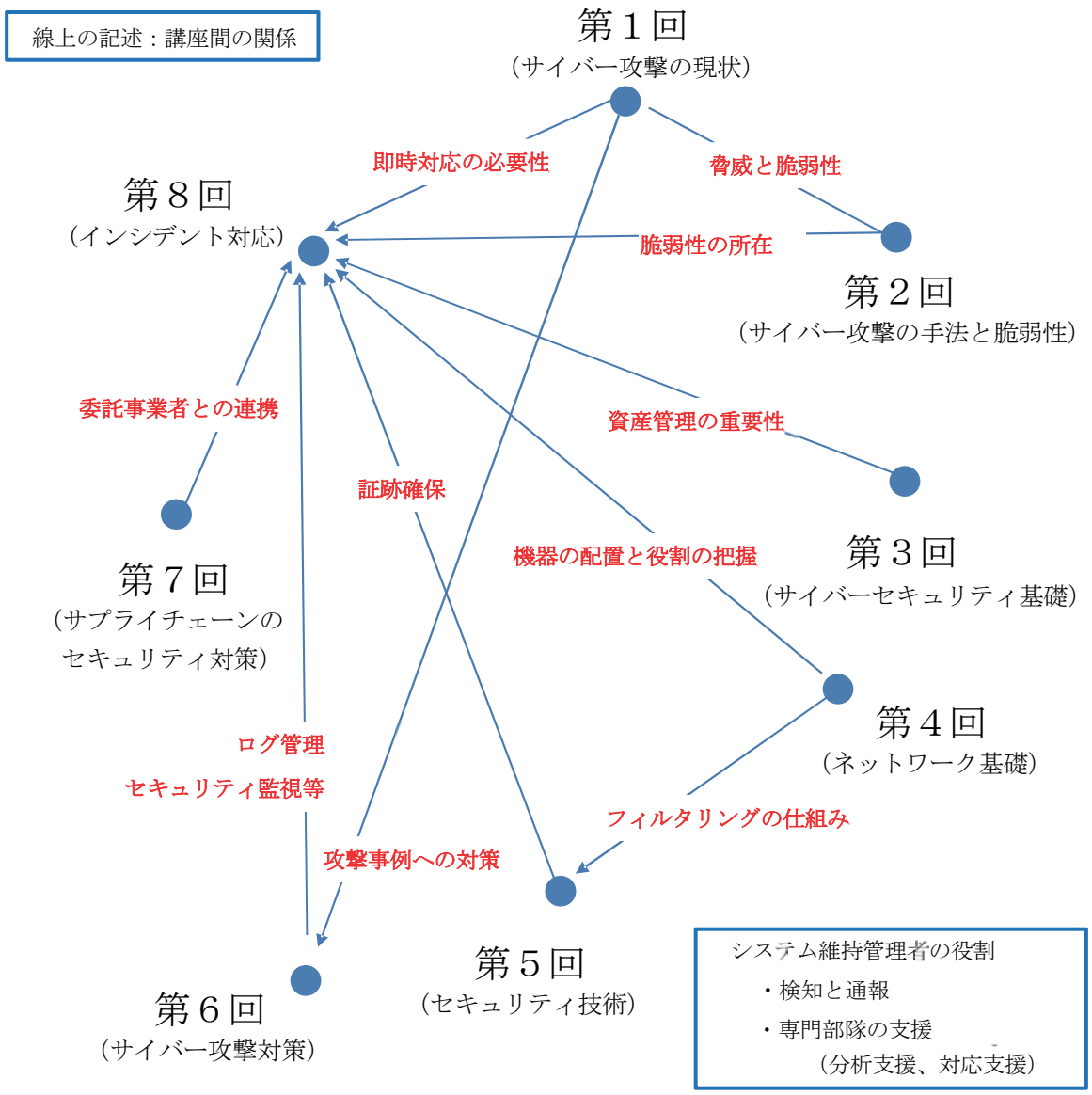


図 3.1　講座間の関係

（１）　第１回と第８回との関係

第１回において即時対応の必要性を解説することにより、インシデント対応の重要性を強く意識付けることを目的としている。

（２）　第２回と第８回との関係

セキュリティインシデントに適切に対応するためには、脆弱性の所在を理解することが必要となる。例えば再発防止策を実施する際には、どこにどのような脆弱性があったのか、といった脆弱性の所在を理解している必要がある。このために、第２回において学習する攻撃事例に見られる手法と脆弱性の知識が参考になる。

（３）　第３回と第８回との関係

セキュリティインシデントに適切に対応するためには、資産管理の重要性を理解することが必要である。インシデント対応においては、例えば、セキュリティ監視より判明した IP アドレスからマルウェア感染端末を特定するといった作業が必要となる。この場合、資産管理に不備があった場合には、速やかに感染端末を特定することができなくなる恐れがある。

（４）　第４回と第８回との関係

セキュリティインシデントに適切に対応するためには、ネットワークを構成する機器の役割を理解し、機器の配置を把握することが必要である。例えば、セキュリティ監視より判明したマルウェア感染端末の感染経路を調査するといった作業が必要となる。この場合、ネットワークを構成する機器の役割と機器の配置を把握できていない場合には、速やかに感染経路を調査することができなくなる恐れがある。

（５）　第５回と第８回との関係

セキュリティインシデントに適切に対応するためには、証跡確保が不可欠である。例えば、セキュリティベンダーによるフォレンジック調査において、各種ログ等の証跡の提示を求められる場合がある。この場合、証跡確保ができていない場合には、フォレンジック調査に支障を来す恐れがある。

（６）　第６回と第８回との関係

セキュリティインシデントに適切に対応するためには、一連のサイバー攻撃対策について理解していることが望ましい。サイバー攻撃対策には、ログ取得等のシステムに関係するセキュリティ対策に加えて、セキュリティ監視等の運用管理に関係するセキュリティ対策が必要となる。このため、例えば再発防止策を実施する際には、サイバー攻撃対策の知識に基づき、どのような防止策が必要であるかを理解している必要がある。

（７）　第７回と第８回との関係

セキュリティインシデントに適切に対応するためには、サプライチェーンのセキュリティ対策について理解していることが望ましい。最近のサイバー攻撃の傾向としては、サプライチェーンの脆弱性を利用したと想定される攻撃手法が増えている。このため、セキュリティインシデントが発生した場合には、システムの保守・運用等の委託事業者のシステムが関与する場合についても想定が必要である。

（８）　第１回と第２回との関係

第１回では鉄道分野と航空分野のサイバー攻撃を、両分野のテキストで共に解説し、第２回では、この事例を含むサイバー攻撃の手法と脆弱性について、他分野での事例も踏まえて解説している。サイバー攻撃の手法と脆弱性については、分野に特化した事例と分野横断的な手法等を関連づけて理解することが望まれる。

（９）　第１回と第６回との関係

第１回において鉄道分野と航空分野のサイバー攻撃を解説し、第６回では、一般的な一連のサイバー攻撃対策について解説している。このため、分野に特化した事例に関連した対策について理解することが重要となる。

（１０）第４回と第５回との関係

第５回で解説するセキュリティ技術のうち、フィルタリング技術を理解するためには、通信パケットの構造を理解する必要がある。例えば、OS の脆弱性を狙う攻撃と Web アプリケーションの脆弱性を狙う攻撃に対するフィルタリング技術の違いは、ネットワークのレイヤー構造とこれに関係するパケットの構造の違いに関係している。

３．２．３．　重要スライドの選出

教材内容の絞り込みを図るために、重要スライドの選出を行なった。講座間の関係を踏まえ、重要スライドの選出基準の概念図を以下に示す。

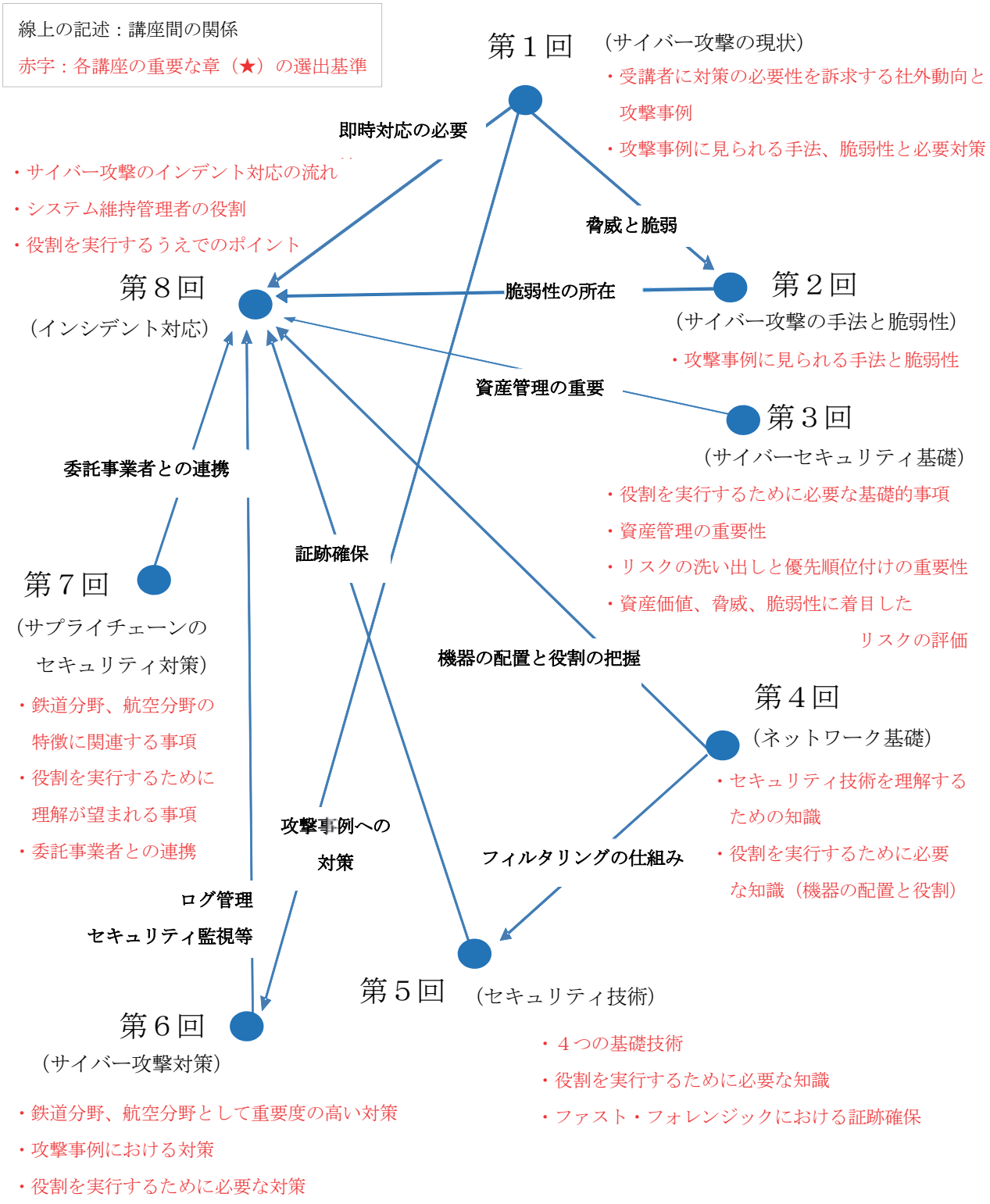


図 3.2　重要スライド選出基準の概念図

（1） 第１回（サイバー攻撃の現状）

第１回の位置付けは、サイバー攻撃の現状を理解し、本講義の受講の必要性を受講者に意識付けることにある。このため、第１回の講座においては、受講者に対策の必要性を訴求するために重要となる社外動向と攻撃事例に関するスライドを選出した。攻撃事例については、手法、事例に見られる脆弱性と必要対策について解説する。

（2） 第２回（サイバー攻撃の手法と脆弱性）

第２回の講座においては、典型的な攻撃手法を理解する上で重要となるスライドを選出した。特にマルウェアに関するスライドは重要である。

（3） 第３回（サイバーセキュリティ基礎）

第３回の講座においては、PDCA サイクル等のサイバーセキュリティの基礎的事項についてのスライドを選出した。また、サイバーセキュリティ対策で重要となる資産管理とリスク分析に関するスライドを選出した。

（4） 第４回（ネットワーク基礎）

第４回の講座においては、セキュリティ技術、特にフィルタリング技術を理解するために必要となるネットワーク知識に関するスライドを選出した。また、ネットワーク機器の配置と役割等の基礎的なスライドを選出した。

（5） 第５回（セキュリティ技術）

第５回の講座においては、４つの基礎技術（フィルタリング技術、認証技術、暗号化と電子署名、VPN）に関するスライドを選出した。また、多層防御とフォレンジックに関するスライドを選出した。

（6） 第６回（サイバー攻撃対策）

第６回の講座においては、鉄道分野、航空分野として重要度の高い対策に関するスライドを選出した。

（7） 第７回（サプライチェーンのセキュリティ対策）

第７回の講座においては、鉄道分野、航空分野の特徴に関するスライドを選出した。また、教育対象者が身近に接することになる、委託事業者との連携に関するスライドを選出した。

（8） 第８回（インシデント対応）

第８回の講座においては、インシデント対応におけるシステム維持管理者の役割及び役割を実行するうえでのポイントに関するスライドを選出した。

表3.1　重要スライドの選出基準

No.	講座名	重要スライドの選出基準
第１回	サイバー攻撃の現状	● 受講者に対策の必要性を訴求する社外動向と攻撃事例 ● 攻撃事例に見られる手法、脆弱性と必要対策
第２回	サイバー攻撃の手法と脆弱性	● 攻撃事例に見られる手法と脆弱性
第３回	サイバーセキュリティ基礎	● 役割を実行するために必要な基礎的事項 資産管理の重要性 リスクの洗い出しと優先順位付けの重要性 資産価値、脅威、脆弱性に着目したリスクの評価
第４回	ネットワーク基礎	● セキュリティ技術を理解するための知識 ● 役割を実行するために必要な知識（機器の配置と役割）
第５回	セキュリティ技術	● ４つの基礎技術 ● 役割を実行するために必要な知識 （ファスト・フォレンジックにおける証跡確保）
第６回	サイバー攻撃対策	● 鉄道分野、航空分野として重要度の高い対策 ● 攻撃事例における対策 ● 役割を実行するために必要な対策
第７回	サプライチェーンのセキュリティ対策	● 鉄道分野、航空分野の特徴に関連する事項 ● 役割を実行するために理解が望まれる事項 （委託事業者との連携）
第８回	インシデント対応	● サイバー攻撃のインデント対応の流れ ● システム維持管理者の役割 ● 役割を実行するうえでのポイント

３．２．４．　教材修正のポイント

以上の結果をもとに、教材修正を実施した。主な修正ポイントは以下のとおりである。

（１）　「ねらい」と「ポイント」の明示

各回における「ねらい」と「ポイント」を記載した。また、「ねらい」と「ポイント」に基づき、指導要領の「講義のポイント」を修正するとともに、教材（スライドとメモ欄）の修正を実施した。

（２）　重要箇所の明示

各回のスライドについて、重要度に応じて★印を付与した。重要箇所の選出のポイントについては、鉄道分野と航空分野に分けて、次節において解説している。

（３）　分野に則した内容への修正

鉄道分野及び航空分野に則した内容となるよう修正を実施した。

３．２．５．　事業者における教材修正について

委員からの意見を参考に教材修正を実施したが、以下については交通事業者が教育を実施する際の教材修正の参考にしていただきたい。

（１）　講座の取捨選択

交通事業者各々で、対象となるシステムや必要となる知識や役割、対応方法などにも違いがあると思われるため、前述した各講座の関係を参考に、必要に応じて講座を取捨選択することを推奨している。各講座の構成において、第２回から第５回までは基礎的な事項であり優先順位を低く設定しているが、育成対象者の現状や役割によって部分的に選択する講座を決定することを推奨する。

（２）　重要事項の取捨選択

各回におけるスライドについて、重要度に応じて★印を付与したが、選出のポイントを参考にして自社内における教育対象者の役割を踏まえて重要事項の絞り込みを実施することを推奨する。

３．３．重要箇所の選出

３．３．１．　鉄道分野

鉄道分野の各講座において選出した重要スライドと選出のポイントを以下に示す。

（1）　第１回　サイバー攻撃の現状

重要スライドの選出基準を以下に示す。

- 受講者に対策の必要性を訴求するサイバーセキュリティの動向と攻撃事例
- 攻撃事例に見られる手法、脆弱性と必要な対策

表 3.2「重要」の位置付けとしたスライド（第１回）

番号	スライドの概要	選出のポイント
5～8	★サイバーセキュリティの必要性①～④	サイバーセキュリティ対策の必要性を解説している。サイバーセキュリティ対策とは何か、なぜ対策を講ずる必要性があるのかを教育対象者に理解してもらい、積極的な学習を訴求するうえで重要である。
9～10	★国内のサイバーセキュリティに関する動向①～②	サイバーセキュリティの動向について解説している。こうした動向を踏まえて、教育対象者に積極的な学習を訴求することが重要である。
12～13	★脅威・インシデントとは①～②	攻撃事例を解説している。事例を用いることにより、サイバーセキュリティ対策を具体的な問題として教育対象者に認識してもらうために重要である。
14～15	★事例１	
16～19	★事例２	
20～24	★事例３	
26	★攻撃の背景と特徴（経路・手法）	事例から想定される攻撃方法について解説している。事例をもとに、具体的な攻撃方法を教育対象者に認識してもらうために重要である。
28	★想定される攻撃方法	
30	★USB メモリを利用した攻撃	攻撃の概要と攻撃から受ける影響について解説している。事例をもとに、具体的なサイバー攻撃の影響を教育対象者に認識してもらうために重要である。
31	★サプライチェーン攻撃	
32	★フィッシングメール	
34	★通信センター、無線 LAN 等からの不正アクセス	
36	★事例の概要	事例に対する対策について解説している。事例をもとに、具体的なサイバー攻撃の対策例を教育対象者に認識してもらうために重要である。
37	★外部記憶媒体もしくは外部業者を利用した攻撃	
38	★メールを中心とした攻撃	
39	★無線・赤外線等を通信経路とした攻撃	

（2） 第２回　サイバー攻撃の手法と脆弱性

重要スライドの選出基準を以下に示す。

- 攻撃事例に見られる手法と脆弱性

表 3.3 「重要」の位置付けとしたスライド（第２回）

番号	スライドの概要	選出のポイント
5	★脅威とは	典型的な攻撃の流れを解説している。今後も様々なサイバー攻撃の手法が登場すると考えられることから、教育対象者が今後の様々な状況に柔軟に対応するために理解しておくことが望まれる。
6	★攻撃手法	
7	★事前調査	
8	★権限取得	
9	★不正実行	
11	★不正アクセス	具体的な攻撃方法について解説している。
12	★Pass the hash 攻撃	
19	★マルウェアとは？	代表的な攻撃方法であるマルウェアについて解説している。今後マルウェアは、様々なサイバー攻撃で用いられることが想定されるため、マルウェアとは何か、どのような攻撃手法に利用されているのかを理解しておくことが望まれる。
20	★マルウェアは何をするの？	
21	★マルウェア:情報漏えい	
22	★マルウェア:ポートスキャン	
23	★マルウェア:機能妨害	
24	★マルウェア:悪意のあるサイトへ誘導	
26	★マルウェア:ランサムウェア	
27	★マイニング（仮想通貨マイナー）	
29	★高度な攻撃:ゼロデイ攻撃	
31	★DoS 攻撃	DoS 攻撃について解説している。DoS 攻撃は、サイバー攻撃手法の代表例である。
34	★脆弱性とは	脆弱性について解説している。脆弱性とは何か、サイバー攻撃において利用される脆弱性にはどのようなものがあるかを理解しておくことは、教育対象者がサイバー攻撃への対応を実施するうえで重要な知識となる。
35	★脆弱性を狙ったサイバー攻撃とその対応	
36	★脆弱性:OS・PC 本体	
37	★脆弱性: ネットワーク機器類	
41	★マルウェア感染の原因（経路）	
42	★脆弱性:メール・Web サイト	
43	★感染経路：メール・Web サイトによる	
44	★感染経路：USB メモリ	
45	★感染経路：ネットワーク（サプライチェーン）	
46	★脆弱性：業務機器類	
47	★脆弱性：無線 LAN・無線通信	
48	★脆弱性：モバイル機器	
49	★脆弱性:人や組織の脆弱性	

（3） 第３回 サイバーセキュリティ基礎

重要スライドの選出基準を以下に示す。

- 役割を実行するために必要な基礎的事項

  資産管理の重要性

  リスクの洗い出しと優先順位付けの重要性

  資産価値、脅威、脆弱性に着目したリスクの評価

表 3.4 「重要」の位置付けとしたスライド（第３回）

番号	スライドの概要	選出のポイント
5	★セキュリティ対策の必要性	教育対象者が役割を実行するために必要な基礎的事項として PDCA サイクル、リスクアセスメント、セキュリティマネジメントについて解説している。教育対象者が対策を実行するうえで、上記を理解していることが望まれる。
6	★サイバーセキュリティ管理	
10	★リスクアセスメントとは	
17	★セキュリティマネジメントのまとめ	
19	★資産とは	資産管理の重要性について解説している。サイバーセキュリティ対策を実行するうえで、資産管理は最も重要であり、教育対象者がその重要性を理解しておく必要がある。
20	★資産分類	
21	★資産管理とは	
23	★資産の洗い出し②	
27～28	★資産重要度の判断①～②	
29	★資産管理の不備がもたらす影響	
32	★リスク評価とは	リスクの洗い出しと優先順位付けの重要性について解説している。教育対象者が体系に則してリスク分析を行わない場合であっても、リスク評価の手法を学ぶことにより、優先度の高いリスクへの気付きの一助となる。
33	★リスク評価の重要性	
34	★資産管理ベースのリスク評価	
35	★脅威レベルの定義	
37	★脆弱性レベルの定義	
38	★リスク値の判定	
40	★リスク評価結果の解釈活用	
41	★クラウドとリスク評価	

（4） 第４回　ネットワーク基礎

重要スライドの選出基準を以下に示す。

- セキュリティ技術を理解するための知識
- 役割を実行するために必要な知識（機器の配置と役割）

表 3.5 「重要」の位置付けとしたスライド（第４回）

番号	スライドの概要	選出のポイント
6	★プロトコル	ネットワークの基礎であるプロトコルについて解説している。第５回のセキュリティ技術を理解するためにはネットワークの知識、特にネットワーを構成するパケット交換の基礎知識について、教育対象者が理解していることが望まれる。
7	★パケット交換とプロトコル	
8	★OSI 参照モデル	
9	★LAN の規格	ネットワーク構成の基本について解説している。インシデント対応を支援する際に、教育対象者がネットワーク構成の基本知識を理解していることが望まれる。
10	★LAN と WAN①	
16	★無線 LAN②	無線 LAN のセキュリティ対策について解説している。無線 LAN は、今後活用範囲の拡大が想定されるため、基本知識を理解していることが望まれる。
18	★TCP/IP とは	セキュリティ技術（特にフィルタリング技術）を理解するための知識として、TCP/IP によるデータ通信の流れやデータリンクを流れるパケットの構造について解説している。教育対象者がセキュリティ技術の理解を深めるために重要である。
22	★ネットワーク層	
23	★IP アドレス	
24	★ネットワーク層のプロトコル	
25	★トランスポート層	
26	★階層化によるパケットの構造	
27～29	★アプリケーション層のプロトコル①～③	代表的なアプリケーション層のプロトコルである DNS、WWW、SNMP について説明している。教育対象者がセキュリティ技術の理解を深めるために重要である。
33	★ネットワーク接続機器とは	ネットワーク接続機器の概要、配置と役割について解説している。教育対象者がインシデント対応支援等を実行するために必要な知識である。
35	★ハブ・スイッチングハブ	
36	★L2・L3 スイッチ	
37	★ルーター	
38	★無線アクセスポイント	
39	★IoT 機器とは	
43～45	★IoT 機器に関する脅威①～③	最新の攻撃事例について解説している。IoT 機器は、今後活用範囲の拡大が想定されるため、基本知識を理解していることが望まれる。

（5） 第５回 セキュリティ技術

重要スライドの選出基準を以下に示す。

- ４つの基礎技術
  （フィルタリング技術、認証技術、暗号化と電子署名、VPN）
- 役割を実行するために必要な知識
  （ファスト・フォレンジックにおける証跡確保）

表 3.6 「重要」の位置付けとしたスライド（第５回）

番号	スライドの概要	選出のポイント
7	★ファイアウォール	フィルタリング技術の代表であるファイアウォールの機能について解説している。教育対象者がインシデント対応や支援を実行するために、ファイアウォールの機能について理解していることが望まれる。
9	★ファイアウォールとは	
10	ファイアウォールの役割①	
11	★ファイアウォールの役割②	
12	★ファイアウォールの役割③	
13	★ファイアウォールの役割④	
14	★ファイアウォールの役割⑤	
17	★不正侵入検知（IDS） 不正侵入防御（IPS）	ファイアウォール以外のフィルタリング技術について解説している。フィルタリング技術の応用例を理解することにより、セキュリティ技術の基本的な理解を深めることが望まれる。
21	★アンチウイルス（アンチマルウェア）	
24	★Web フィルタリング	
25	★認証①	認証技術について解説している。認証技術は代表的なセキュリティ技術であるため、教育対象者が基本知識を理解していることが望まれる。
26	★認証②	
27	★暗号化・電子署名	暗号化・電子署名技術について解説している。暗号化・電子署名技術は代表的なセキュリティ技術であるため、教育対象者が基本知識を理解していることが望まれる。
28	★暗号技術①	
29	★暗号技術②	
30	★暗号技術③	
31	★暗号化	
32	★電子署名	
33	★VPN	VPN 技術について解説している。VPN 技術は代表的なセキュリティ技術であるため、教育対象者が基本知識を理解していることが望まれる。
34	★SSL/TLS	
35	★ハードニング①	その他のセキュリティ技術のうち重要と思われるものを解説している。
42	★パケット監視技術	
43	★SIEM①	
47	★多層防御とは	役割を実行するために必要な知識として、多層防御について解説している。サイバー攻撃対策には多層的な防御が不可欠であるため、教育対象者その必要性を理解していることが望まれる。
48	★多層防御の必要性①	
51	★その他の多層防御①	

54	★フォレンジックとは	役割を実行するために必要な知識として、フォレンジックについて解説している。サイバー攻撃対応においてフォレンジックは不可欠であるが、フォレンジックを有効活用するためには、教育対象者がファスト・フォレンジック等の活用方法を理解していることが望まれる。
56	★ファスト・フォレンジックとは	
58	★ファスト・フォレンジックの必要性	

（6） 第６回　サイバー攻撃対策

重要スライドの選出基準を以下に示す。

- 鉄道分野として重要度の高い対策
- 攻撃事例における対策
- 役割を実行するために必要な対策

表 3.7 「重要」の位置付けとしたスライド（第６回）

番号	スライドの概要	選出のポイント
5～6	★外部ネットワークとの分離	鉄道分野のシステム（特に制御系システム）は、クローズドシステムの優位性を維持するために、可能な限り外部ネットワークと分離することが望ましいことを解説している。
7～8	★他ネットワークとの接続	鉄道分野のシステム（特に制御系システム）は、他ネットワークとの接続における対策が重要となっていることを解説している。
11～12	★マルウェア対策	攻撃事例も多く報告されており、マルウェア対策は非常に重要であることを解説している。
17～18	★ログの取得・保管・保全	サイバー攻撃に対応する際にはシステムのログが不可欠であるため、その取得・保管・保全が重要であることを解説している。
22	★機器等の構成・変更管理	維持管理対象システムの構成管理と変更管理が重要であることを解説している。
23～24	★外部記憶媒体のマルウェア対策	外部記憶媒体を用いたサイバー攻撃事例は国内外で多く報告されているため、対策が重要であることを解説している。
25～26	★権限の適切な割当	管理者権限取得はサイバー攻撃手法の最も重要な段階となるため、権限の適切な割当が重要であることを解説している。
27～28	★修正プログラムの適用	PC の脆弱性対策の遅れがマルウェア感染拡大を招いた事例があり、修正プログラムの適用の重要性について解説している。
29	★入退管理	物理的なシステムへのアクセスについて、入退管理の重要性について解説している。
31～32	★セキュリティ監視	システムの稼働状況に関する監視に加えて、セキュリティに関する監視を実施する必要があることを解説している。

（7） 第７回　サプライチェーンのセキュリティ対策

重要スライドの選出基準を以下に示す。

- 鉄道分野の特徴に関連する事項
- 役割を実行するために理解が望まれる事項
  （委託事業者との連携）

表 3.8 「重要」の位置付けとしたスライド（第７回）

番号	スライドの概要	選出のポイント
5～6	★サプライチェーンとは 鉄道におけるサプライチェーンの一部の例	鉄道分野の特徴に関連するサプライチェーンのセキュリティ対策事項を解説している。サプライチェーンのセキュリティ対策は、最近のサイバー攻撃の脅威として特に注目される対策であるため、教育対象者がその概要と対策の必要性を理解していることが望まれる。
8	★サイバーセキュリティ対策の実施と状況把握	
9	★サプライチェーン対策を怠った場合のシナリオ	
12	★外部委託管理のポイント	役割を実行するために理解が望まれる事項として、委託先事業者との連携について解説している。サプライチェーンのセキュリティ対策の内、外部委託先に関わる対策は、教育対象者の身近な対策であるため、具体的な対策について解していることが望まれる。
13	★委託範囲の特定	
14	★アクセス権限管理	
15	★委託先要員のデバイス管理	
16	★端末管理	
18	★クラウドサービス利用の例	
24	★情報共有活動とは	昨今の複雑化・巧妙化するサイバー攻撃対応においては、適切な情報共有が重要となっている。教育対象者がその役割を実行するために、情報共有活動の重要性について理解していることが望まれる。
25	★情報共有の重要性	
28	★ベンダーからの情報提供・サポートの活用	

（8） 第８回　インシデント対応

重要スライドの選出基準を以下に示す。

- サイバー攻撃のインデント対応の流れ
- システム維持管理者の役割
- 役割を実行するうえでのポイント

表 3.9 「重要」の位置付けとしたスライド（第８回）

番号	スライドの概要	選出のポイント
6	★インシデント対応プロセス	IT 分野の対応手法をもとに、サイバー攻撃のインシデント対応の流れについて解説している。IT 分野の手法を学習することにより、教育対象者がサイバー攻撃におけるインシデント対応の基本的な流れを理解しておくことが望まれる。
7	★インシデント対応の概要①	
8	★インシデント対応の概要②	
9	★インシデント発生時の対応手順	
13	★各担当者における対応の必要性	
15 ～ 16	★セキュリティインシデントの位置付け①～②	
17	★担当者の役割	インシデント対応におけるシステム維持管理者の役割について解説している。教育対象者がインシデント対応において果たす役割について理解する必要がある。
18	★社内外との連携	
19	★責任と手順の明確化	
23	★各担当者における対応の必要性	
25	★インシデント対応の概要	システム維持管理者が役割を実行するうえでのポイントを解説している。教育対象者がインシデント対応においてその役割を実行するうえで重要である。
26	★インシデントの検知と通報	
27	★インシデント対応の支援:サービス停止有無の判断	
28	★インシデント対応の支援:外部専門機関・ベンダーへの調査依頼	
29	★インシデント対応の支援:関係各所への連絡	
30	★インシデント対応の支援:利用者への対応	
31	★インシデント対応時に確認すべき連絡事項	

３．３．２．　航空分野

航空分野の各講座において選出した重要スライドと選出のポイントを以下に示す。

（１）　第１回　サイバー攻撃の現状

重要スライドの選出基準を以下に示す。

- 受講者に対策の必要性を訴求するサイバーセキュリティの動向と攻撃事例
- 攻撃事例に見られる手法、脆弱性と必要な対策

表 3.10　「重要」の位置付けとしたスライド（第１回）

番号	スライドの概要	選出のポイント
5～8	★サイバーセキュリティの必要性①～④	サイバーセキュリティ対策の必要性を解説している。サイバーセキュリティ対策とは何か、なぜ対策を講ずる必要性があるのかを教育対象者に理解してもらい、積極的な学習を訴求するうえで重要である。
9～10	★国内のサイバーセキュリティに関する動向①～②	サイバーセキュリティの動向について解説している。こうした動向を踏まえて、教育対象者に積極的な学習を訴求するうえで重要である。
12～13	★脅威・インシデントとは①～②	攻撃事例を解説している。事例を用いることにより、サイバーセキュリティ対策を具体的な問題として教育対象者に認識してもらうために重要である。
14～16	★事例１	
17	★事例２	
18	★事例２（参考）	
19～20	★事例３	
21	★攻撃の背景と特徴（経路・手法）	事例から想定される攻撃方法について解説している。事例をもとに、具体的な攻撃方法を教育対象者に認識してもらうために重要である。
23	★想定される攻撃方法	
25	★サプライチェーン攻撃	事例に対する対策について解説している。事例をもとに、具体的なサイバー攻撃の対策を教育対象者に認識してもらうために重要である。
26	★USB メモリを利用した攻撃	
27	★フィッシングメール	
29	★通信センサー、無線 LAN 等からの不正アクセス	
33	★インターネットを含む外部との接続先からの攻撃	事例に対する対策について解説している。事例をもとに、具体的なサイバー攻撃の対策を教育対象者に認識してもらうために重要である。
34	★メールを中心とした攻撃	
35	★外部もしくは内部からの特定の企業や機器を狙った集中攻撃	

（2） 第２回 サイバー攻撃の手法と脆弱性

重要スライドの選出基準を以下に示す。

- 攻撃事例に見られる手法と脆弱性

表 3.11 「重要」の位置付けとしたスライド（第２回）

番号	スライドの概要	選出のポイント
5	★脅威とは	典型的な攻撃の流れを解説している。今後も様々なサイバー攻撃の手法が登場すると考えられることから、教育対象者が様々な状況に柔軟に対応するために理解しておくことが望まれる。
6	★攻撃手法	
7	★事前調査	
8	★権限取得	
9	★不正実行	
11	★不正アクセス	具体的な攻撃方法について解説している。航空分野においては、システム維持管理者が業務アプリケーションの維持管理に携わる可能性が高いことから、アプリケーションの脆弱性を突いた攻撃についての解説を多く選出している。
12	★Pass the hash 攻撃	
14	★中間者攻撃	
15	★バッファオーバーフロー攻撃	
16	★クロスサイトスクリプティング攻撃	
17	★SQL インジェクション攻撃	
18	★DNS キャッシュポイズニング攻撃	
26	★マルウェア:ランサムウェア	代表的な攻撃方法であるマルウェアについて解説している。今後マルウェアは、様々なサイバー攻撃で用いられることが想定されるため、マルウェアとは何か、どのような攻撃手法に利用されているのかを理解しておくことが望まれる。
27	★マイニング（仮想通貨マイナー）	
28	★高度な攻撃:シーケンシャルマルウェア	
29	★高度な攻撃:ゼロデイ攻撃	
30	★高度な攻撃:ファイルレス攻撃	
31	DoS 攻撃	DoS 攻撃について解説している。DoS 攻撃は、サイバー攻撃手法の代表例である。
32	★DDoS 攻撃	
34	★脆弱性とは	脆弱性について解説している。脆弱性とは何か、サイバー攻撃において利用される脆弱性にはどのようなものがあるかを理解しておくことは、教育対象者がサイバー攻撃への対応を実施するうえで重要な知識となる。
35	★脆弱性を狙ったサイバー攻撃とその対応	
38	★①アクセス権限の設定が不十分	
39	★②メンテナンス用 PC 等の外部持込機器の取り扱い	
40	★③インターネット接続の存在	
41	★④脆弱性パッチ適用の遅れ	
43	★ポートと脆弱性②	
44	★ポートと脆弱性③	
46	★脆弱性:メール・Web サイト	
47	★感染経路：メール・Web サイトによる	
48	★感染経路：ネットワーク（サプライチェーン）	
49	★感染経路：USB メモリ	

（3） 第３回 サイバーセキュリティ基礎

重要スライドの選出基準を以下に示す。

- 役割を実行するために必要な基礎的事項

  資産管理の重要性

  リスクの洗い出しと優先順位付けの重要性

  資産価値、脅威、脆弱性に着目したリスクの評価

表 3.12 「重要」の位置付けとしたスライド（第３回）

番号	スライドの概要	選出のポイント
5	★セキュリティ対策の必要性	教育対象者が、役割を実行するために必要な基礎的事項として PDCA サイクル、リスクアセスメント、セキュリティマネジメントについて解説している。教育対象者が対策を実行するうえで、上記を理解していることが望まれる。
6	★サイバーセキュリティ管理	
11	★リスクアセスメントとは	
18	★セキュリティマネジメントのまとめ	
20	★資産とは	資産管理の重要性について解説している。サイバーセキュリティ対策を実行するうえで、資産管理は最も重要であり、教育対象者がその重要性を理解しておく必要がある。
21	★資産分類	
22	★資産管理とは	
24	★資産の洗い出し②	
28～29	★資産重要度の判断①～②	
30	★資産管理の不備がもたらす影響	
33	★リスク評価とは	リスクの洗い出しと優先順位付けの重要性について解説している。教育対象者が体系に則してリスク分析を行わない場合であっても、リスク評価の手法を学ぶことにより、優先度の高いリスクへの気付きの一助となる。
34	★リスク評価の重要性	
35	★資産管理ベースのリスク評価	
36	★脅威レベルの定義	
38	★脆弱性レベルの定義	
39	★リスク値の判定	
41	★リスク評価結果の解釈活用	
42	★クラウドとリスク評価	

（4） 第４回　ネットワーク基礎

重要スライドの選出基準を以下に示す。

- セキュリティ技術を理解するための知識
- 役割を実行するために必要な知識（機器の配置と役割）

表 3.13 「重要」の位置付けとしたスライド（第４回）

番号	スライドの概要	選出のポイント
6	★プロトコル	ネットワークの基礎であるプロトコルについて解説している。第５回のセキュリティ技術を理解するためにはネットワークの知識、特にネットワーを構成するパケット交換の基礎知識について、教育対象者が理解していることが望まれる。
7	★パケット交換とプロトコル	
8	★OSI 参照モデル	
9	★LAN の規格	ネットワーク構成の基本について解説している。インシデント対応を支援する際に、教育対象者がネットワーク構成の基本知識を理解していることが望まれる。
10	★LAN と WAN①	
16	★無線 LAN②	無線 LAN のセキュリティ対策について解説している。無線 LAN は、今後活用範囲の拡大が想定されるため、基本知識を理解していることが望まれる。
18	★TCP/IP とは	セキュリティ技術（特にフィルタリング技術）を理解するための知識として、TCP/IP によるデータ通信の流れやデータリンクを流れるパケットの構造について解説している。教育対象者がセキュリティ技術の理解を深めるために重要である。
22	★ネットワーク層	
23	★IP アドレス	
24	★ネットワーク層のプロトコル	
25	★トランスポート層	
26	★階層化によるパケットの構造	
27～29	★アプリケーション層のプロトコル①～③	代表的なアプリケーション層のプロトコルである DNS、WWW、SNMP について説明している。教育対象者がセキュリティ技術の理解を深めるために重要である。
33	★ネットワーク接続機器とは	ネットワーク接続機器の概要、配置と役割について解説している。教育対象者がインシデント対応や支援等を実行するために必要な知識である。
34	★ハブ・スイッチングハブ	
35	★L2・L3 スイッチ	
36	★ルーター	
37	★無線アクセスポイント	
38	★IoT 機器とは	
42～44	★IoT 機器に関する脅威①～③	最新の攻撃事例について解説している。IoT 機器は、今後活用範囲の拡大が想定されるため、基本知識を理解していることが望まれる。

（5） 第５回 セキュリティ技術

重要スライドの選出基準を以下に示す。

- ４つの基礎技術
  （フィルタリング技術、認証技術、暗号化と電子署名、VPN）
- 役割を実行するために必要な知識
  （ファスト・フォレンジックにおける証跡確保）

表 3.14 「重要」の位置付けとしたスライド（第５回）

番号	スライドの概要	選出のポイント
7	★ファイアウォール	フィルタリング技術の代表であるファイアウォールの機能について解説している。教育対象者がインシデント対応や支援等を実行するために、ファイアウォールの機能について理解していることが望まれる。
9	★ファイアウォールとは	
11	★ファイアウォールの役割②	
12	★ファイアウォールの役割③	
13	★ファイアウォールの役割④	
14	★ファイアウォールの役割⑤	
17	★不正侵入検知（IDS） 不正侵入防御（IPS）	ファイアウォール以外のフィルタリング技術について解説している。フィルタリング技術の応用例を理解することにより、セキュリティ技術の基本的な理解を深めることが望まれる。
18	★WAF①	
19	★WAF②	
20	サンドボックス	
21	★アンチウイルス（アンチマルウェア）	
24	★Web フィルタリング	
25	★認証①	認証技術について解説している。認証技術は代表的なセキュリティ技術であるため、教育対象者が基本知識を理解していることが望まれる。
26	★認証②	
27	★暗号化・電子署名	暗号化・電子署名技術について解説している。暗号化・電子署名技術は代表的なセキュリティ技術であるため、教育対象者が基本知識を理解していることが望まれる。
28	★暗号技術①	
29	★暗号技術②	
30	★暗号技術③	
31	★暗号化	
32	★電子署名	
33	★VPN	VPN 技術について解説している。VPN 技術は代表的なセキュリティ技術であるため、教育対象者が基本知識を理解していることが望まれる。
34	★SSL/TLS	
35	★ハードニング①	その他のセキュリティ技術のうち重要と思われるものを解説している。
36～37	★ハードニング②～③	
42	★パケット監視技術	
43	★SIEM①	
47	★多層防御とは	役割を実行するために必要な知識として、多層防

48	★多層防御の必要性①	御について解説している。サイバー攻撃対策には多層的な防御が不可欠であるため、教育対象者その必要性を理解していることが望まれる。
51	★その他の多層防御①	
52	★その他の多層防御②	
54	★フォレンジックとは	役割を実行するために必要な知識として、フォレンジックについて解説している。サイバー攻撃対応においてフォレンジックは不可欠であるが、フォレンジックを有効活用するためには、教育対象者がファスト・フォレンジック等の活用方法を理解していることが望まれる。
56	★ファスト・フォレンジックとは	
58	★ファスト・フォレンジックの必要性	

（6） 第６回 サイバー攻撃対策

重要スライドの選出基準を以下に示す。

- 航空分野として重要度の高い対策
- 攻撃事例における対策
- 役割を実行するために必要な対策

表 3.15 「重要」の位置付けとしたスライド（第６回）

番号	スライドの概要	選出のポイント
5～6	★外部ネットワークとの分離	クローズドシステムの優位性を維持するために、可能な限り外部ネットワークと分離することが望ましいことを解説している。
7～8	★他ネットワークとの接続	航空分野のシステムは、他ネットワークとの接続における対策が重要となることを解説している。
11～12	★マルウェア対策	攻撃事例も多く報告されており、マルウェア対策は非常に重要であることを解説している。
17～19	★ログの取得・保管・保全	サイバー攻撃に対応する際にはシステムのログが不可欠であるため、その取得・保管・保全が重要であることを解説している。
21～22	★セキュリティ仕様の確認	維持管理対象のシステムについて、セキュリティ仕様の確認が重要であることを解説している。
23	★機器等の構成・変更管理	維持管理対象システムの構成管理と変更管理が重要であることを解説している。
24～25	★外部記憶媒体のマルウェア対策	外部記憶媒体を用いたサイバー攻撃事例は国内外で多く報告されているため、対策が重要であることを解説している。
26～27	★権限の適切な割当	管理者権限取得はサイバー攻撃手法の最も重要な段階となるため、権限の適切な割当が重要であることを解説している。
28～29	★セキュリティパッチの適用	Windows の脆弱性対策の遅れがマルウェア感染拡大を招いた事例があり、セキュリティパッチの適用の重要性について解説している。

（7） 第７回　サプライチェーンのセキュリティ対策

重要スライドの選出基準を以下に示す。

- 航空分野の特徴に関連する事項
- 役割を実行するために理解が望まれる事項
  （委託事業者との連携）

表 3.16 「重要」の位置付けとしたスライド（第７回）

番号	スライドの概要	選出のポイント
5～6	★サプライチェーンとは 航空におけるサプライチェーンの一部の例	航空分野の特徴に関連するサプライチェーンのセキュリティ対策事項を解説している。サプライチェーンのセキュリティ対策は、最近のサイバー攻撃の脅威として特に注目される対策であるため、教育対象者がその概要と対策の必要性を理解していることが望まれる。
8	★サイバーセキュリティ対策の実施と状況把握	
9	★サプライチェーン対策を怠った場合のシナリオ	
12	★外部委託管理のポイント	役割を実行するために理解が望まれる事項として、委託先事業者との連携について解説している。サプライチェーンのセキュリティ対策のうち、外部委託先に関わる対策は、教育対象者の身近な対策であるため、具体的な対策について解していることが望まれる。
13	★委託範囲の特定	
14	★アクセス権限管理	
15	★委託先要員のデバイス管理	
16	★端末管理	
17	★その他の外部委託管理①	
18	★その他の外部委託管理②	
19	★クラウドサービス利用の例	
20	★契約のセキュリティ項目確認ポイント	
25	★情報共有活動とは	昨今の複雑化・巧妙化するサイバー攻撃対応においては、適切な情報共有が重要となっている。教育対象者がその役割を実行するために、情報共有活動の重要性について理解していることが望まれる。
26	★情報共有の重要性	
29	★ベンダーからの情報提供・サポートの活用	

（8） 第８回　インシデント対応

重要スライドの選出基準を以下に示す。

- サイバー攻撃のインデント対応の流れ
- システム維持管理者の役割
- 役割を実行するうえでのポイント

表 3.17 「重要」の位置付けとしたスライド（第８回）

番号	スライドの概要	選出のポイント
6	★インシデント対応プロセス	サイバー攻撃のインシデント対応の流れについて解説している。教育対象者がサイバー攻撃におけるインシデント対応の基本的な流れを理解しておくことが望まれる。
7	★インシデント対応の概要①	
8	★インシデント対応の概要②	
9	★インシデント発生時の対応手順	
13	★各担当者における対応の必要性	
17	★担当者の役割	インシデント対応におけるシステム維持管理者の役割について解説している。教育対象者がインシデント対応において果たす役割について理解する必要がある。
18	★社内外との連携	
19	★責任と手順の明確化	
25	★インシデント対応の概要	システム維持管理者が役割を実行するうえでのポイントを解説している。教育対象者がインシデント対応においてその役割を実行するうえで重要である。
26	★インシデントの検知と通報	
27	★インシデント対応の支援:サービス停止有無の判断	
28	★インシデント対応の支援:外部専門機関・ベンダーへの調査依頼	
29	★インシデント対応の支援:関係各所への連絡	
30	★インシデント対応の支援:利用者への対応	
31	★インシデント対応時に確認すべき連絡事項	

第４章.　　教育の試行

４．１．実施内容

教育の試行は、鉄道分野と航空分野に分けて、以下の日程で実施した。

受講者：システム維持管理及びシステム障害対応の担当者、講師予定者、等
会場：　運輸総合研究所 ２階会議室

鉄道分野
- 日程：12 月５日、６日、７日
- 参加者： 12 名（８社）（所属部署は電気部、企画部、調達担当等、多岐に亘っていた）

航空分野
- 日程：12 月 12 日、13 日、14 日
- 参加者：３名（３社）（講師予定者または教育に関わる方の参加であった）

講義スケジュールは以下のとおりである。

表 4.1　講義スケジュール

日程	内容	講師
１日目	第１回　サイバー攻撃の現状 第２回　サイバー攻撃の手法と脆弱性 第３回　サイバーセキュリティ基礎	鉄道、航空：富田一成氏 （株式会社ラック）
２日目	第４回　ネットワーク基礎 第５回　セキュリティ技術 第６回　サイバー攻撃対策	鉄道、航空：長谷川長一氏 （株式会社ラック）
３日目	第７回　サプライチェーンのセキュリティ対策 第８回　インシデント対応 第９回　学習の振り返り コースのまとめと振り返り 質疑応答 グループディスカッション	鉄道：山田英史氏 （株式会社ディアイティ） 航空：大竹章裕氏 （株式会社ラック）

各講義の終了時に、アンケートを実施した。また、第９回の学習の振り返りにおいては、第１回から第８回までのコースのまとめと振り返りに加えて、質疑応答とグループディスカッションを実施した。以下において、アンケートの結果とグループディスカッションの状況についてまとめる。

４．２．鉄道分野の試行

４．２．１．　アンケートの結果

各講座に対して受講後にアンケートを実施した。

（１）　理解度評価

各講座に対する受講者の理解度について、アンケートを実施した。

アンケートの結果より、全体的には６割以上の受講者から理解できたとの回答が得られた。第２回（サイバー攻撃の手法と脆弱性）、第５回（セキュリティ技術）、第８回（インシデント対応）について理解する事ができなかったとの回答があった。第２回、第５回、第８回には、サイバー攻撃に対する技術的知識が主であったことが要因と考えられる。

Q:今回の学習のあなたの理解度を自己評価してください。

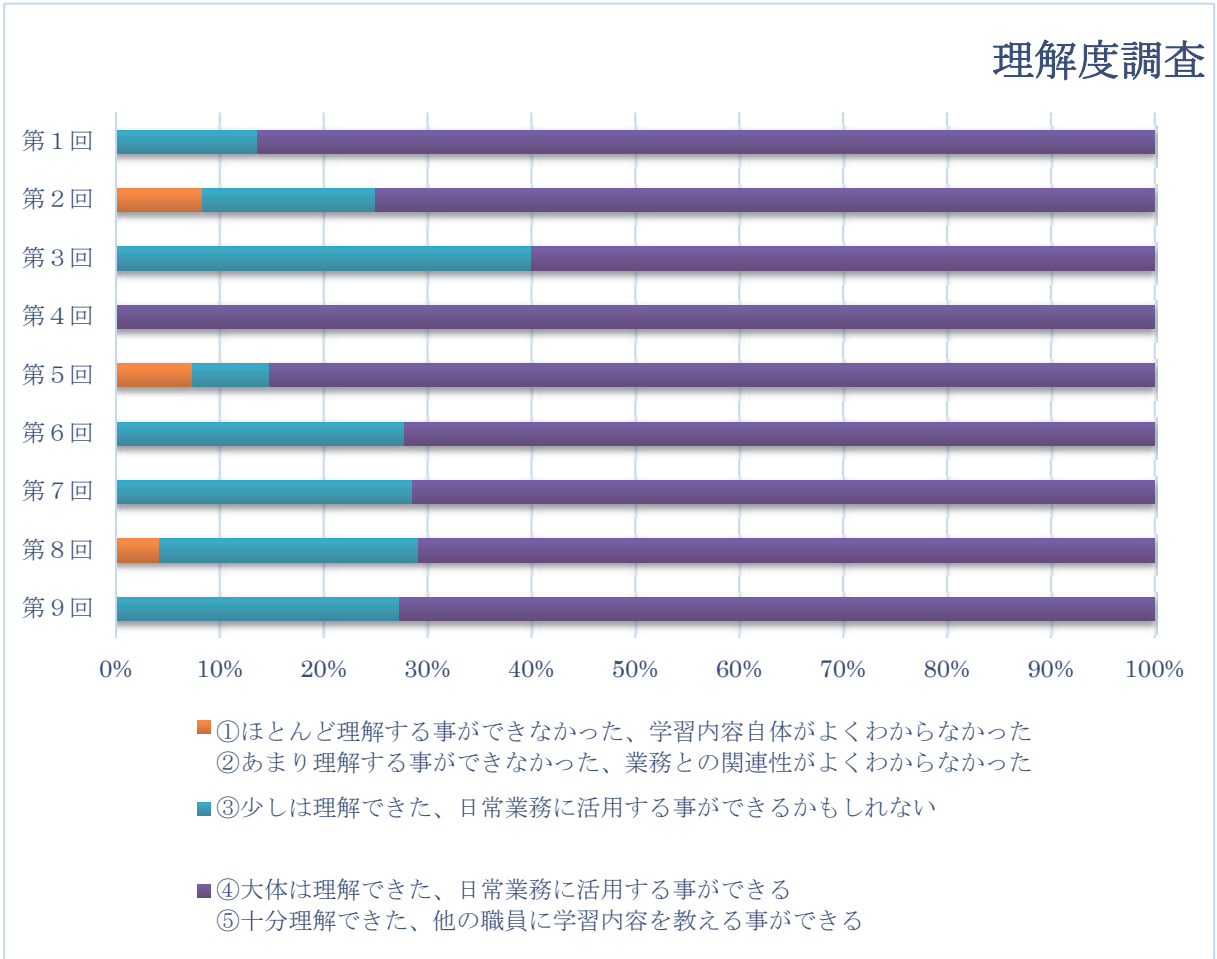


図 4.1　理解度評価

（２）　意識評価

各講座に対する受講者の意識について、アンケートを実施した。

アンケートの結果より、全体的には７割以上の受講者から重要事項であるとの回答が得られた。第２回（サイバー攻撃の手法と脆弱性）、第５回（セキュリティ技術）について自分の業務に関係しないとの回答があった。

Q：今回の学習に関してあなたの率直な気持ちを選んでください。

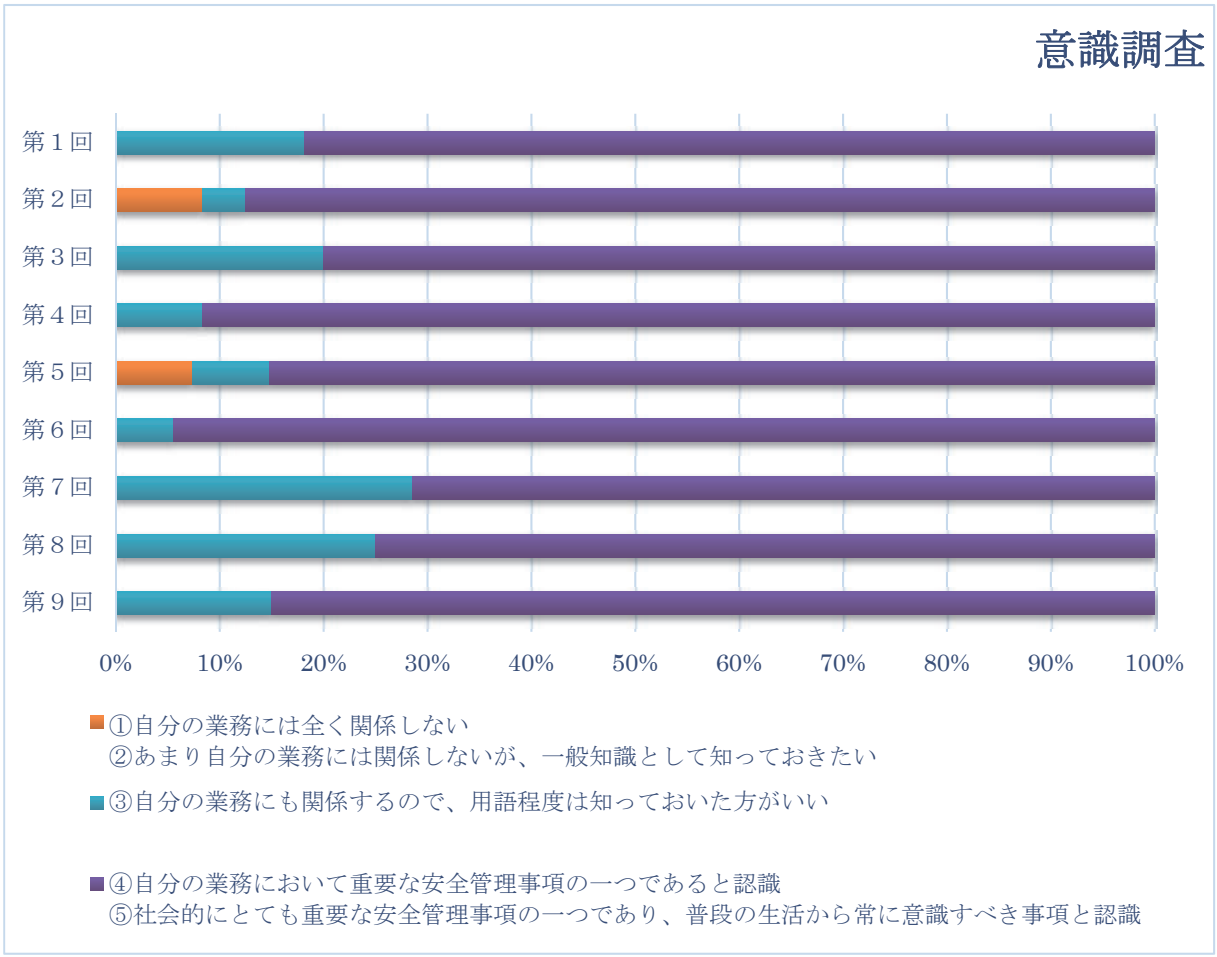


図 4.2　意識評価

（３）　難度評価

各講座に対する受講者の難度について、アンケートを実施した。

アンケートの結果より、第２回（サイバー攻撃の手法と脆弱性）、第３回（サイバーセキュリティ基礎）について、難度が高いとの回答があった。これらの講座については、特に用語と事例が難しいとの評価があり、サイバー攻撃の内容やサイバーセキュリティ管理の基本的な考え方には馴染みがなく、より丁寧な解説が必要であると考えられる。特にサイバー攻撃事例については図の表現が難しいとの回答が多くあり、図を用いた攻撃手法の説明が課題になると考えられる。

Q:今回の学習に関して難しい・分かりにくいと思われるところにチェックをしてください。（複数選択可能、該当がない場合はチェックを無視してください）

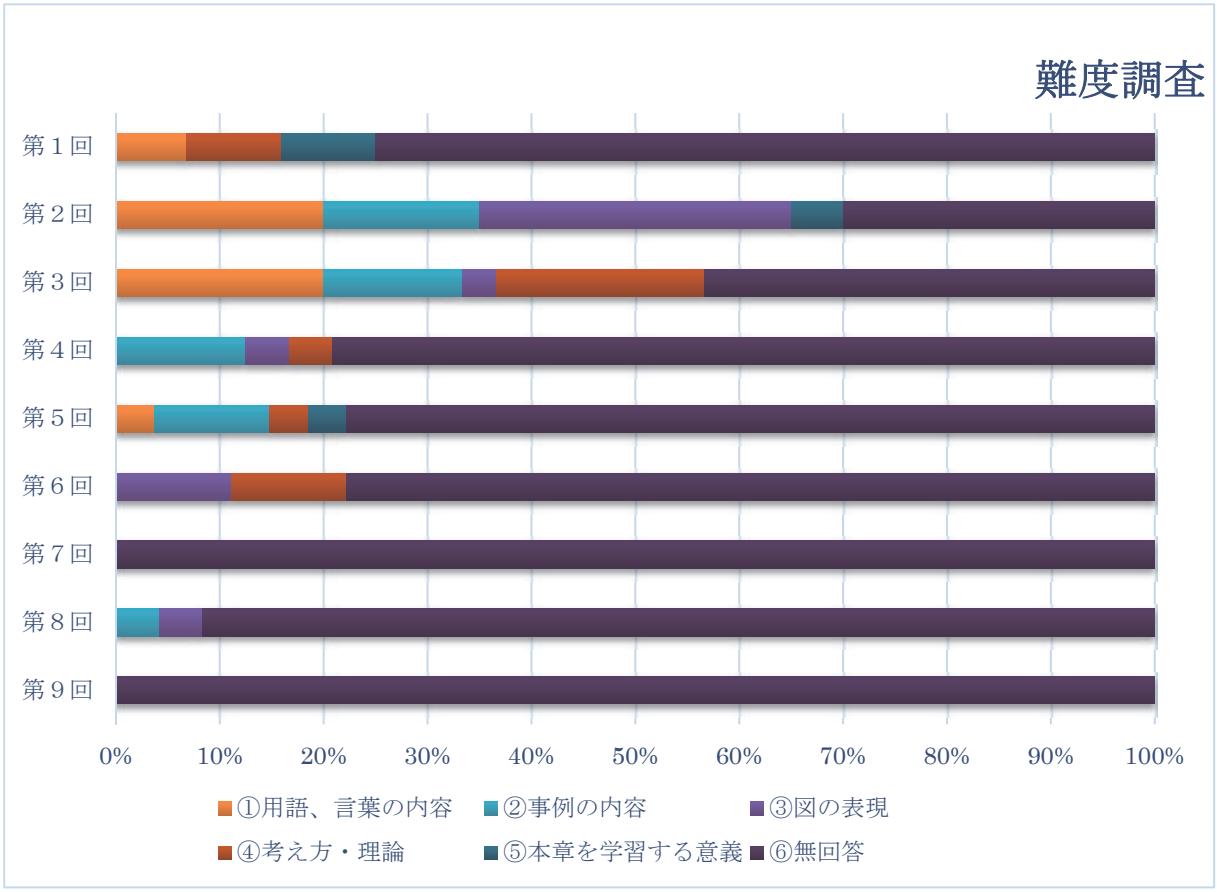


図 4.3　難度評価

４．２．２．　アンケート（感想）

各講座に対する受講者アンケートの感想について以下に示す。

（１）　教材評価について

本年度作成した教材については、サイバーセキュリティ教育の基礎教材としては概ね良い評価が得られている。以下に感想を抜粋する。

- 鉄道分野に沿ったセキュリティテキストは、事例紹介はあっても、担当者目線からのものがなくフィットしないものが多かったが、今回のテキストは、改良の余地は残すにせよ、ベースのテキストとして、とても参考になるものと感じた。（第１回）
- 実例をあげたりして分かりやすく、興味を持つ事ができた。（第３回）
- 今まで良く分からなかった内容が、スッキリと理解できた。資料が良く出来ていると思った。（第４回）
- 用語についての解説がとても参考になった。（第５回）

（２）　事業分野への適合状況について

鉄道分野に則した内容にすべきとの感想があった。

- 講師から補足があったが、手法としての脆弱性の認識と、実際に発生する被害は、対象により異なるため、鉄道業に則した対象について説明であれば、より理解が進むと思われる。（第２回）
- 全体的に鉄道へのサイバー攻撃というのは、OT、IT 関係ないということを理解したが、OT をより強固にするためには、という内容もほしかった。（第９回）

（３）　情報量について

情報量が多かったとの感想があった。以下に感想を抜粋する。

- インシデント対応のポイントは文字が多く集中力が続かない。（第８回）
- 情報量が多く感じた。インシデント対応は実際に発生した内容を紹介しても良いと思った（理解を深めるために）。（第８回）

（４）　講師について

講師の質が高かったことについて感想があった。特に、実例や体験に基づく説明が好評であった。以下に感想を抜粋する。

- 大変わかりやすい説明であった。（第１回）
- 実例をあげたりして分かりやすく、興味を持つ事ができた。（第２回）
- 資料がやや難しかったが、丁寧な解説だった。（第５回）
- 資料にない実例等の話もあり、分かり易かった。（第６回）

（５）　インシデント対応について

インシデント対応については、各事業者の実情にあった改変が必要になる。

・　システム維持管理者が実施することがもう少し明確に書かれているとよいと思う。どうしてもCSIRTがやることの話がメインになってしまう。（第８回）

（６）　グループディスカッションについて

グループディスカッションについては、必要であるとの意見が多かった。

・　グループディスカッションは適宜入れた方が良いと思う。一方向の座学では飽きてしまう。質疑も適宜入れないと聞きたいことを忘れてしまう。（第９回）

・　グループディスカッションは具体的シナリオのため、話がしやすかった。こういったケースをたくさん話ができると良いと思った。（第９回）

（７）　その他

その他、現状課題に関する感想があった。

・　セキュリティの実務担当者として抱えている課題の内容だったため、集中して受講した。サプライヤ、委託先との契約や責任の明確化は必要とわかっていても、厳格な定めを定義するには時間・労力がかかるし、担当者の移動によってそれらの理解をゼロから始めるのは大変であると感じる。（第７回）

・　Windows,ITに少々寄った内容である。Linux,OTとバランスをとると良い。

４．２．３．　グループディスカッション

第９回の学習の振り返りにおけるグループディスカッションで使用した検討シナリオを以下に示す。検討シナリオとディスカッションのテーマを提示し、グループ討議を実施した。

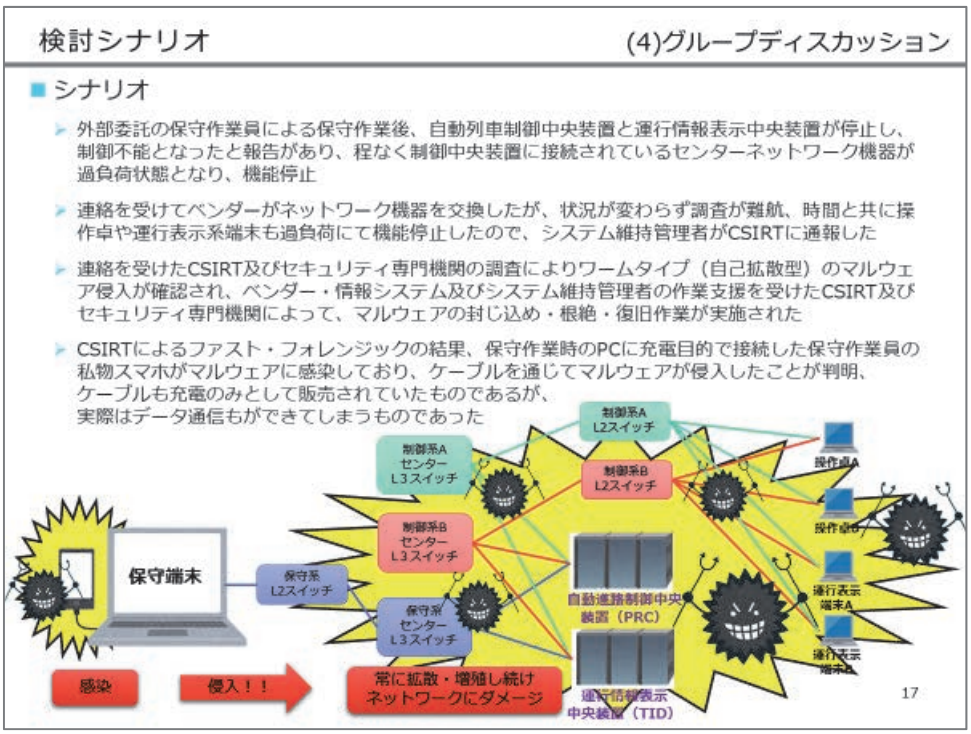


図 4.4　第９回　学習の振り返り（スライド 17）

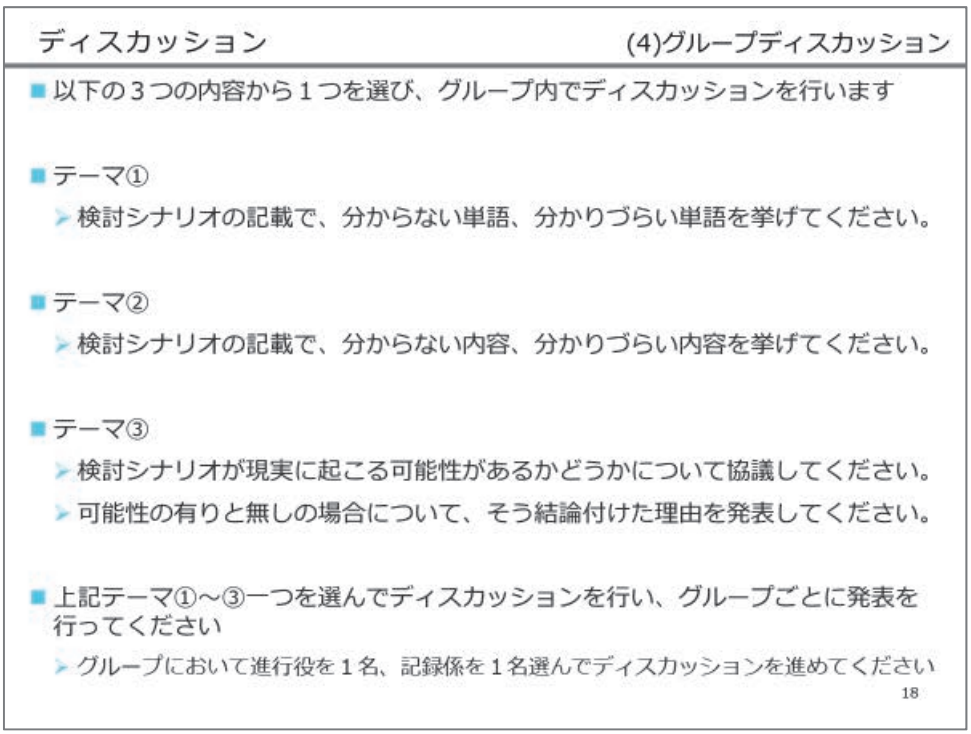


図 4.5　第９回　学習の振り返り（スライド 18）

鉄道分野におけるグループディスカッションは、２グループに別れて実施した。テーマについては、①から③までの全てを対象として実施した。ディスカッションの結果、シナリオで提示したようなサイバー攻撃が「起こり得る」としたグループと「起こり得るがここまでの状況には至らない」とするグループに分かれた。「起こり得る」としたグループからは、ルールの徹底を含めて端末の利用方法を制御することが難しいとの意見があった。また、「起こり得るがここまでの状況には至らない」としたグループからは、ウイルスチェックの実施やネットワークの分離、複数 OS が存在していることなどから、影響は限定的との意見があった。

各グループとも、グループディスカッションでは積極的な討議が見られた。討議の過程で、各参加者のシナリオに対する内容理解が深められていた。紙面の都合もありシナリオに関する掲載情報は不足していたが、参加者がこの不足部分を仮定し、補完することにより、討議が進行した。討議の結果がグループにより異なっていたのは、この補完部分の条件の違いによるものと思われる。このようなシナリオ検討の過程を経ることにより、シナリオと与えられた情報との差異を補完しつつ討議が進められることとなり、結果として脆弱性への気付き（仮定した前提条件の下ではシナリオにある結果が起こり得る、との気付き）が得られた。参加者同士の討議により、他社の状況も含めた参加者間の情報共有が深められた。

シナリオに対する参加者の所感として、サイバー攻撃対策の難しさに関して以下の意見があった。

- 故意の犯罪は防ぐことが難しい。
- リスクが高いところは性悪説で対応すべきである。
- 全ての対策をシステム化することは困難であり、手動を含めた対応が必要である。

その他、サプライチェーンのセキュリティ対策に関連し、以下の意見があった。

- サイバー攻撃発生時における委託先への対応依頼については、契約にないことを理由に断られるケースが有り得るため、対策が必要となる。
- 委託先の実施業務においてリスクを検知した場合には、対応を要求する必要がある。このため、リスクの検知と委託先への対応依頼が課題となる。
- 保守端末は、セキュリティ対策を講じた専用端末を準備すべきである。
- サプライチェーン対策として、セキュリティ侵害が疑われる製品は調達しない方針を徹底する必要がある。
- 今後、サイバー・フィジカル・システムの利活用に係るセキュリティ対策が必要となる。
- サプライチェーンのセキュリティ対策に関連し、フレームワーク（全社的な対策の枠組み）の整備が必要である。

４．３．航空分野の試行

４．３．１．　アンケート

各講座に対して受講後にアンケートを実施した。

（１）　理解度

各講座に対する受講者の理解度について、アンケートを実施した。

アンケートの結果より、全体的には６割以上の受講者から理解できたとの回答が得られたが、第４回（ネットワーク基礎)、第５回（セキュリティ技術)、第６回（サイバー攻撃対策）について理解不足との回答があった。第４回と第５回については技術的な内容が主であったことが要因と考えられる。第６回についてはサイバー攻撃対策を複数の観点から説明していることから、一部の対策について理解不足になってしまったことが要因と考えられる。

Q:今回の学習のあなたの理解度を自己評価してください。

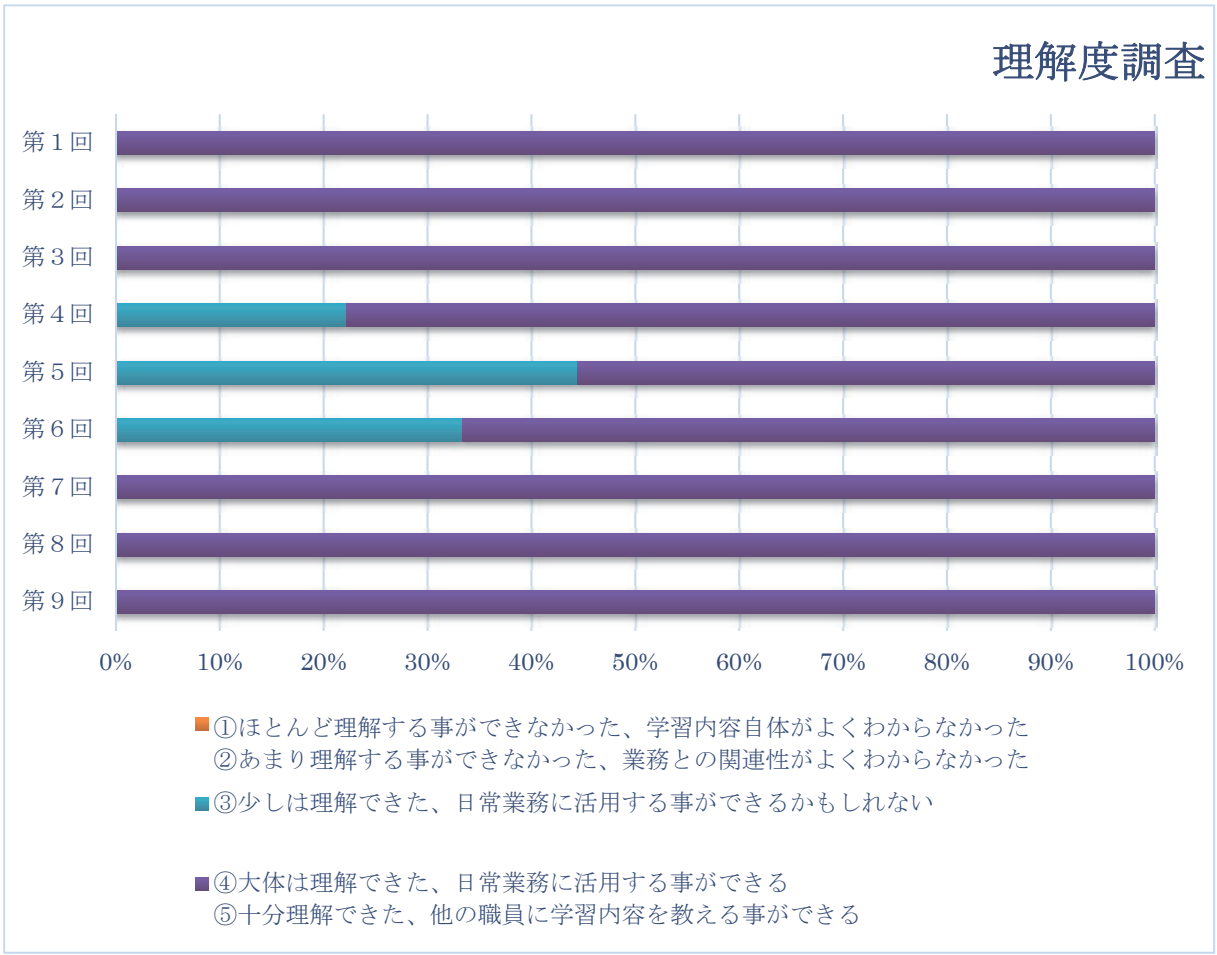


図 4.6　理解度評価

（２）　意識評価

各講座に対する受講者の意識について、アンケートを実施した。

アンケートの結果より、教材の内容についてはほぼ全ての受講者から重要事項であるとの回答が得られた。このため、教材の内容については特に問題はなかったと判断できる。

Q：今回の学習に関してあなたの率直な気持ちを選んでください。

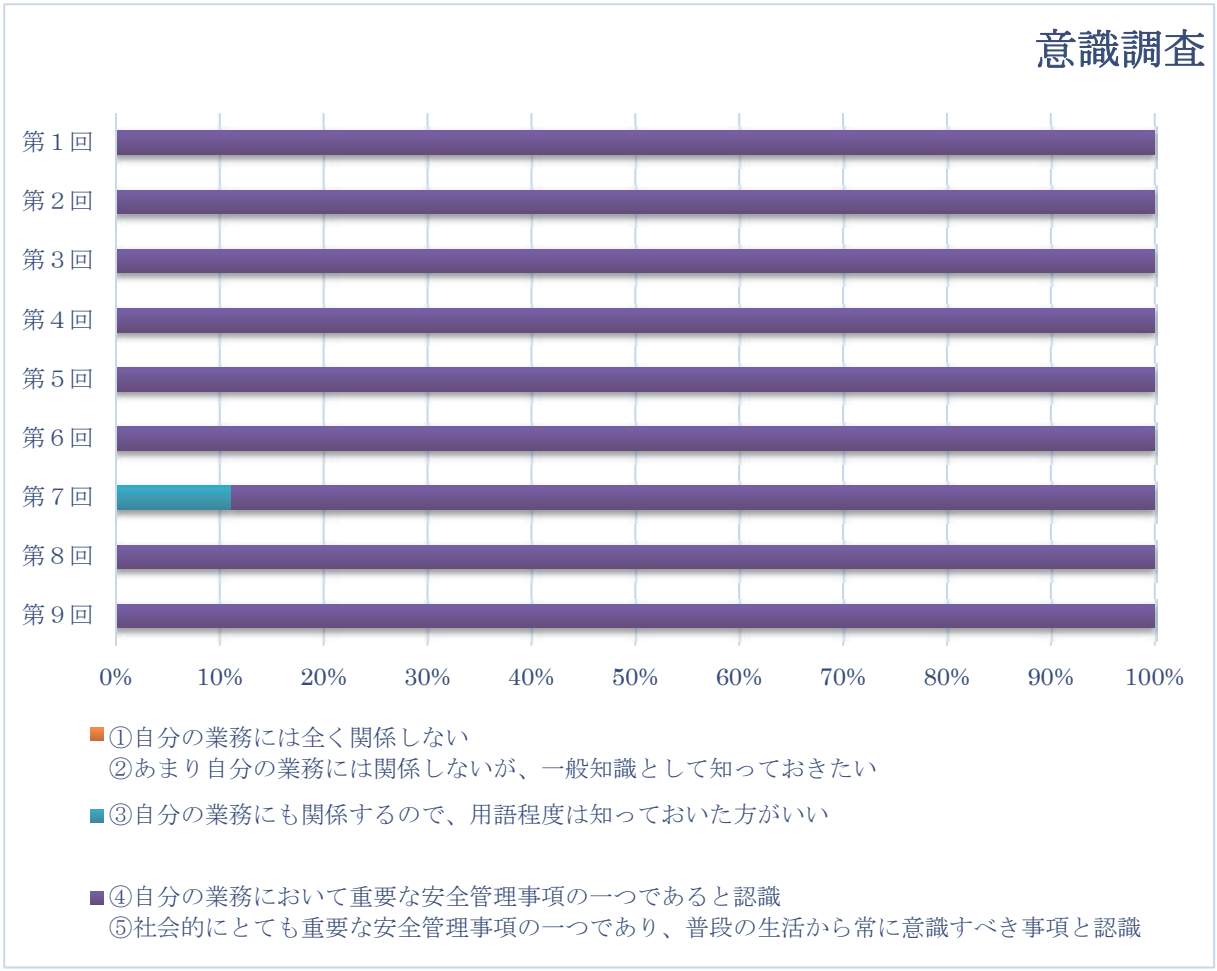


図 4.7　意識評価

（３）　難度評価

各講座に対する受講者の難度について、アンケートを実施した。

アンケートの結果より、第４回（ネットワーク基礎）、第６回（サイバーセキュリティ対策）について、難度が高いとの回答があった。第４回については用語が難しいとの回答であったが、この要因としては、サイバー攻撃対応にネットワークの知識が必要であるとの認識が浸透していないことが挙げられる。このため、ネットワーク基礎を学ぶ必要性についての説明が必要であると考えられる。第６回はサイバー攻撃対策についてより広範に解説をしているが、用語とともに考え方や理論について難しいとの回答が多かった。この講座で解説するサイバー攻撃対策は手引書をもとにしているが、対策種別毎に解説しているため、相関関係を理解することが難しいことが要因と考えられる。第６回で解説する対策は手引書に記載のあるものであるため、手引書自体の解説を冒頭に行い、対策の必要性を補足する必要があると考えられる。

Q:今回の学習に関して難しい・分かりにくいと思われるところにチェックをしてください。（複数選択可能、該当がない場合はチェックを無視してください）

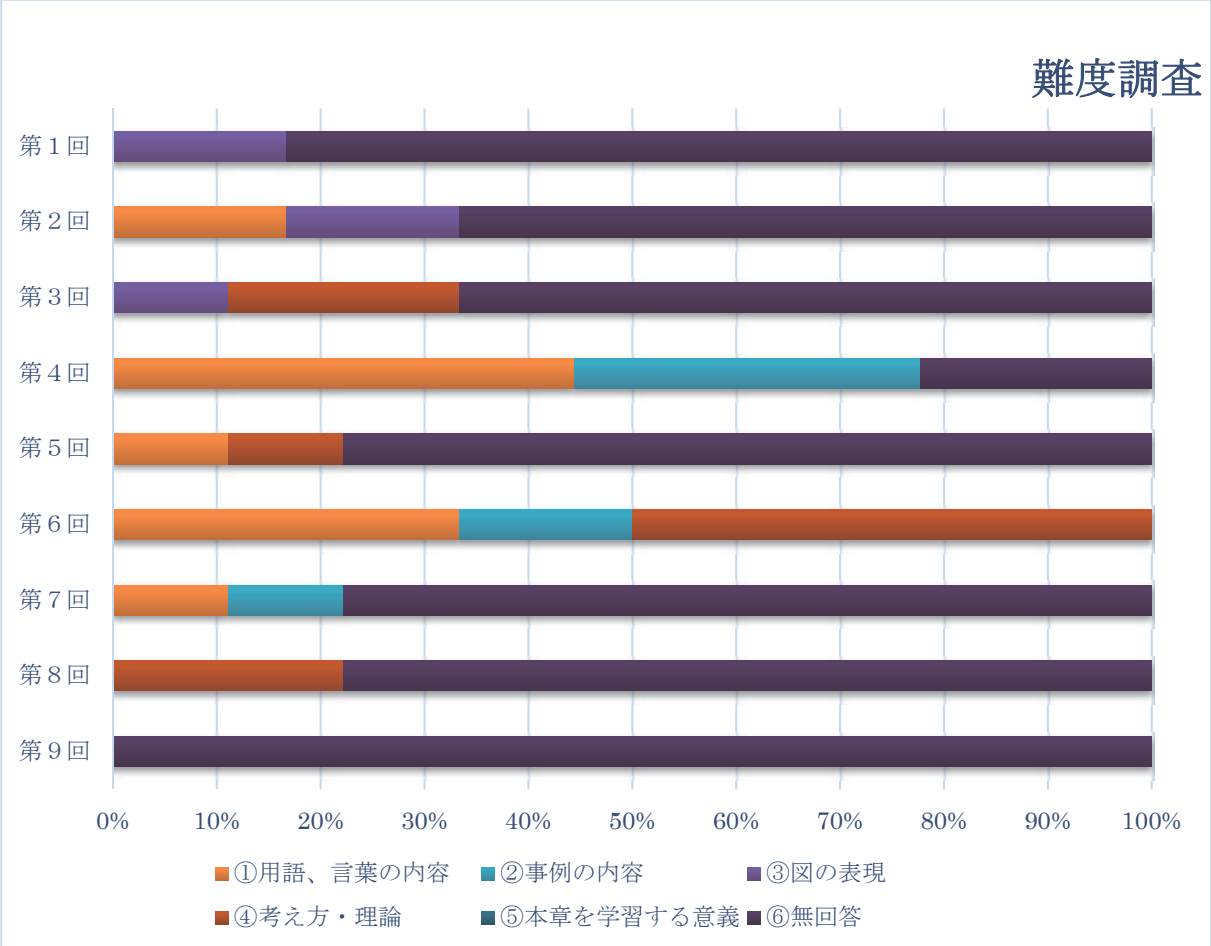


図 4.8　難度評価

４．３．２．　アンケート（感想）

各講座に対する受講者アンケートの感想について以下に示す。

（１）　教材評価について

本年度作成した教材については、サイバーセキュリティ教育の基礎教材としては概ね良い評価が得られている。以下に感想を抜粋する。

- 本日、1 日受講し、基礎知識を整理できたと思う。これまでは（0JT のように）点の対応で、細切れの知識であった。（第３回）
- 内容は素晴らしい。（第４回）
- サイバーセキュリティとしてカバーすべき範囲がまとめられており、全体としてとても活用できる内容であると感じた。セキュリティとして、何をすべきであるか、基本的な学習内容になると思った。（第９回）

（２）　情報量について

情報量が多かったとの感想があった。以下に感想を抜粋する。

- 第２回は量が多く、少し消化していない部分もある。（第２回）
- 量もたくさんあり、スピード（講義）も速いため、メモが追い付かない。もう少し遅いと嬉しい。（第４回）
- 第５日と第６日だけで３日間ぐらいかかる内容かと思われる。今回のテーマを深めた講義が聞きたい。（第５回、第６回）

（３）　講師について

講師の質が高かったことについて感想があった。特に、web サイトを見せながらの説明、実例や体験に基づく説明が好評であった。以下に感想を抜粋する。

- 講師の方の説明の仕方、話し方、web サイトを見せながらの説明はとても聞きやすく、またわかりやすかった。（第１回）
- とても丁寧な説明で、また実例、実体験があり、理解しやすい内容だった。（第２回）

（４）　インシデント対応について

インシデント対応については、各事業者の実情にあった改変が必要になる。

- インシデント対応手順、体制、連絡先は文書化されているものの、頭に入っていないため、ある程度は、復習として文書を定期的に見直す必要性を感じた。また見直しのタイミングで文書の更新点を確認できると思った。（第８回）
- システム維持管理者が実施することがもう少し明確に書かれているとよいと思う。どうしても CSIRT がやることの話がメインになってしまう。（第８回）

（５）　グループディスカッションについて

グループディスカッションについては、必要であるとの意見が多かった。

・　各会社によって環境が全く違うので、グループディスカッション等でもっと個別の環境に応じた対策の「考え方」を聞いてみたいと思った。（第９回）

（６）　その他

その他、現状課題に関する感想があった。

・　個人所有端末の社内持込など BYOD 環境における対策事例があれば、もう少し知りたい。昨今、コストの問題から、会社が社員の端末を全て準備することが、なくなりつつあるように思われるため。（第２回）
・　リスク値の判定において、会社ではどうしても全員一律の定量分析ルールを適用せざるを得ないため、実態と異なる場合がある。このため、何かいい方法があれば知りたい。（第３回）
・　様々な部署で、システム＆委託会社を利用しており、それらを網羅的に管理できればいいが、現実的ではなく、サプライチェーンは非常に難しい問題だと考える。（第７回）
・　自社の契約書チェックで、セキュリティの観点が含まれているのかが気になった。今回参加して、少なくとも自分自身が関わる契約では意識するきっかけになった。（第７回）
・　ページ毎の資料は分かりやすいが、その回の全体像が分かる資料がないため、全体像が分かりにくい。

４．３．３．　グループディスカッション

第９回の学習の振り返りにおけるグループディスカッションで使用した検討シナリオを以下に示す。検討シナリオとディスカッションのテーマを提示し、グループ討議を実施した。

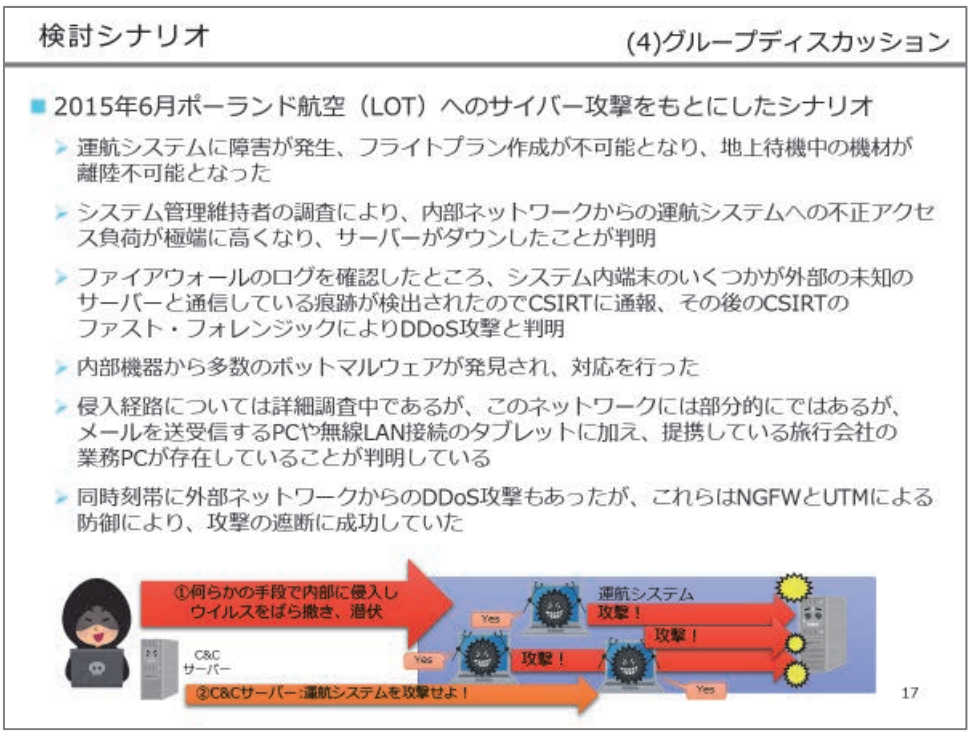


図 4.9　第９回　学習の振り返り（スライド 17）

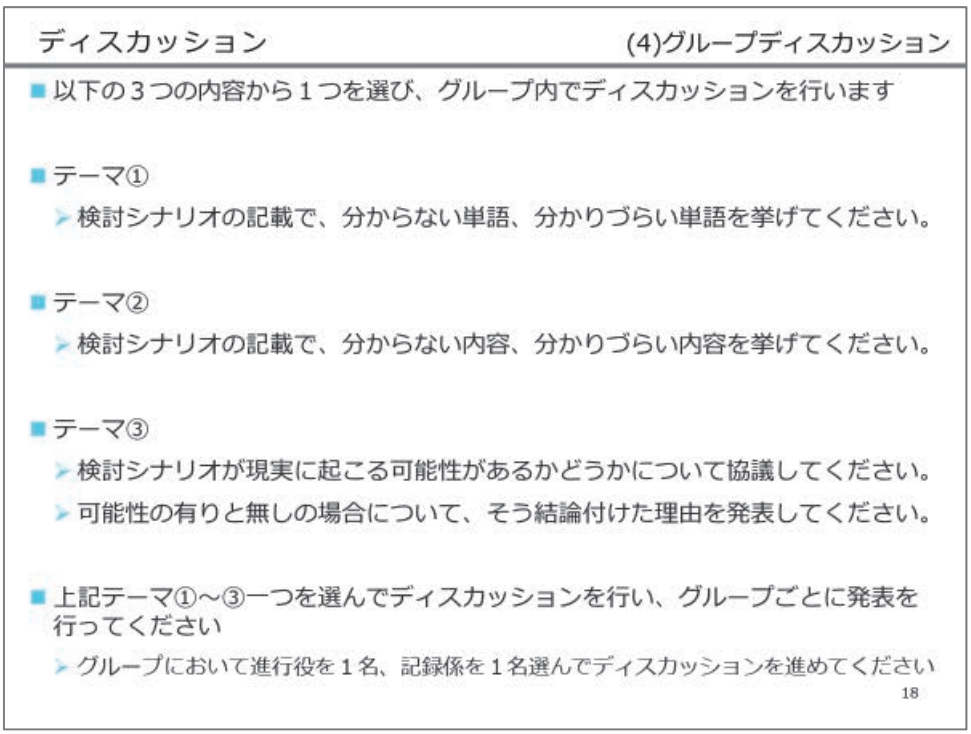


図 4.10　第９回　学習の振り返り（スライド 18）

航空分野の参加者は３名であったため、グループディスカッションは１グループで実施した。テーマについては、①から③までの全てを対象として実施した。ディスカッションの結果、シナリオで提示したようなサイバー攻撃は、「可能性がある」としつつも「シナリオ通りの状況は発生しない」との結論となった。端末の利用方法を制御することが難しいため、発生の可能性はあるが、対象システムは分離されていることが主な理由として挙げられた。

グループディスカッションでは積極的な討議が見られた。討議の過程により、各参加者のシナリオに対する内容理解が深められていた。紙面の都合もありシナリオに関する掲載情報は不足していたが、参加者がこの不足部分を仮定し、補完することにより、討議が進行した。このようなシナリオ検討の過程を経ることにより、シナリオと与えられた情報の差異を補完しつつ討議が進められることとなり、結果として脆弱性への気付き（仮定した前提条件の下ではシナリオにある結果が起こり得る、との気付き）が得られた。併せて、参加者同士の討議が活発化するとともに、他社の状況も含めた参加者間の情報共有が深められた。

シナリオにおける掲載情報の不足については、参加者からその旨の質問があった。このことについては、前述のとおり、情報不足を参加者が補完することにより、討議が活性化することを意図している。サイバー攻撃は悪意のある攻撃者の存在があり、攻撃手法を巧妙に変化させてくることから、インシデント対応は一律のやり方では対応できない。このため、掲載情報が不足したシナリオを用いることで、参加者に様々な状況設定を想定させることが可能となる。

この他に、参加者からは、旅行会社の PC をシナリオに入れた意図についての質問があった。このことについては、サプライチェーン対策の一環として旅行会社を取り入れている。また、無線やネットワーク分離についての要素もシナリオに加え、討議活性化の試みとしている。

その他、参加者から以下の意見があった。サイバー攻撃対策における人材育成の重要性を示す意見である。

- サイバー攻撃対策に正解はなく、対策と演習を繰り返す必要がある。
- 決められた手順を正確に履行することが必要である。

４．４．得られた知見

４．４．１．　鉄道分野と航空分野の違いについて

航空分野の業務システムは、IT 系の汎用技術を採用しているものが多く、事業者間において国を跨ぐような各種のシステム連携が大規模に構築されている。このため、サイバー攻撃対応の必要性を強く意識しており、システム維持管理者も IT 技術に精通している場合が多い。このため、航空分野の教材内容については、より高度なセキュリティ技術及び対応手法を盛り込む必要がある。さらに、システム維持管理者が担うべき対象範囲も拡大してきており、対応のための優先順位をシステム維持管理者が各自で判断して柔軟な対応ができる人材を育成することが必要となってきている。

一方で、鉄道分野の業務システムは、IT 系の汎用技術の採用と事業者間におけるシステム連携が進行中であるが、現時点では OT 系はクローズドシステムであるためサイバー攻撃の影響は限定的であるとの意識が高い状況にある。このため、鉄道分野の教材の内容については、これらの現状の変化についての教育対象者の理解を深め、サイバーセキュリティ対策の重要性を訴求する内容とする必要がある。

なお、鉄道分野（実務担当者がメイン受講者）と航空分野（教育関係者がメイン受講者）のアンケート回答結果の全体的な傾向としては、理解度調査については、「大体理解できた、十分理解できた」の割合が鉄道分野に比べて航空分野で高い。意識調査については、「業務・社会的に重要な安全管理事項の一つ」との認識割合が鉄道分野に比べて航空分野で高い。難度調査については、鉄道分野ではサイバー攻撃の手法と脆弱性（第 2 回）やサイバーセキュリティ基礎（第 3 回）の難度が高いと感じている（攻撃の内容や管理などの基本的な考え方になじみがないため）が、航空分野ではネットワーク基礎（第 4 回）やサイバーセキュリティ対策（第 6 回）の難度が高いと感じている（サイバー攻撃対応にネットワークの知識が必要であるとの認識不足のため）結果となった。ただし、今回の教育の試行では参加人数が少なかったこともあり、あくまでも今回の参加者の結果との認識が必要である。

４．４．２．　課題等

以下、課題等について記載する。

（１）　教材の内容について

本教材の利用方法については、受講者に求めるレベルなど各事業者の実情に応じた講座を検討するとともに、講座の内容に合致した教材の取捨選択を実施する必要がある。このため、教材の内容については、情報量が多いものとして各事業者に提供し、各講座の内容についての取捨選択は各事業者の判断に委ねることとした。

（２）　インシデント対応について

アンケートの結果に見られるように、インシデント対応（第８回）は、システム維持管理者が実施することを明確に記載すべきとの意見があった。一方で、インシデント対応については、各事業者の既存の障害対応手順と整合した内容に修正することが望まれるため、過度にシステム維持管

理者の対応手順として規定することは望ましくないと考えられる。このため、各社における自社の体制を教材に取り入れ、実際の連携体制、役割を確認して教材を修正し、利用することを推奨する。

（３） グループディスカッションについて

アンケートの結果に見られるように、グループディスカッションの導入は有効であった。このため、教育に際してはグループディスカッションを積極的に取り入れることを推奨する。グループディスカッションを取り入れることで、社内のコミュニケーションや連携にも繋がることが期待できる。

（４） 最新事例の紹介について

アンケートの結果に見られるように、分かりやすい講義を行うためには、最新事例を紹介することが有効である。本教育は、サイバー攻撃の可能性を検知する際に重要な役割を担う現場のシステム維持管理者を対象としているが、教育対象者への講義を有効なものとするためには、より身近な事例や最新事例を紹介することが望ましい。

第５章.　　机上演習の実施

５．１.実施内容

５．１．１．　日程

机上演習は、鉄道分野と航空分野に分けて、以下の日程で実施した。

（１）　鉄道分野

日程１：8 月 24 日、9 月 11 日
参加者：８名（４社）

日程２：9 月 10 日、9 月 14 日
参加者：９名（５社）

（２）　航空分野

日程　：8 月 24 日、9 月 14 日
参加者：13 名（８社）

５．１．２．　演習１日目

（１）　概要説明

講師より、CSIRT の概要を説明するとともに、CSIRT の成り立ちや経緯を説明した。また、インシデント発生前と発生後の CSIRT の機能について解説した。

インシデント発生前

- 予報センター機能
- 監視センター機能

インシデント発生後

- ファーストレスポンダー機能
- 調整センター機能
- 対策支援センター機能

CSIRT の説明の後に、最近の攻撃についての注意点を説明した。攻撃者は既知の攻撃に対する対応手法を学習しているため、最新の攻撃の在り方を知る必要がある。このため、想定シナリオには、最新の攻撃の在り方を取り入れているとの説明があった。

この後に、サポートプレーヤー（CSIRT）とレスポンスプレーヤー（現場のチーム）に分かれて演習を実施。サポートプレーヤーは多数の情報を保有（矛盾する内容を包含している）しており、レスポンスプレーヤーは情報不足であることが前提となっている。このような状況下において、双方が協力してインシデントに対応するシナリオとなっている。

（2） シナリオ１によるディスカッション

スピアフィッシングによるサイバー攻撃を想定シナリオとし、与えられた資料をもとにサポートプレーヤーがチーム内で協議し、その後にレスポンスプレーヤーに対して助言を実施する流れの演習であった。

シナリオにおいては、仮想マシン（検証環境）と実機マシン（実機環境）におけるマルウエア挙動の違いを利用して、マルウエア解析情報を攻撃者が偽装している状況が作り込まれており、双方が内容の異なる情報に基づき対応する中で、コミュニケーションの取り方も含めた実践的な内容となっていた。

（3） シナリオ２によるディスカッション

中間者攻撃によるマイニングを想定シナリオとし、与えられた資料をもとにサポートプレーヤーがチーム内で協議し、その後にレスポンスプレーヤーに対して助言を実施する流れの演習であった。

５．１．３． 演習２日目

第１回の机上演習の結果を踏まえ、解説を実施した。この目的は、現場での正しい判断に結びつけるためのヒントを得ることであった。正しく状況を認識し、今何を実施すべきか、何を優先すべきかについて演習をもとに学習した。以下、解説の例を示す。

どのような情報に注目し、どのようなアクションを実施するのかを考えることは重要である。特にサポートプレーヤー（CSIRT）は、入手した情報がどのように作成され、どのように活用すべきかを理解した上で、レスポンスプレーヤー（現場のチーム）に対するアクションを決定すべきである。

ファスト・フォレンジックの理解が必要である。最近のサイバー攻撃に対するインシデントレスポンスの傾向は、複雑な攻撃に速やかに対処する必要があり、これまでのフォレンジックの手法は、予算と時間的に現実的ではなくなっている。このため、調査の目的、範囲を絞って実施するファスト・フォレンジックが必要である。

５．２．得られた知見

５．２．１．　鉄道分野と航空分野の違い

演習２日目については、鉄道分野と航空分野で解説の内容を分けた。具体的には、鉄道分野における解説は、シナリオ１によるディスカッションの内容を主体とし、航空分野における解説は、シナリオ２によるディスカッションの内容を主体としたものであった。このことは、鉄道分野と航空分野で前提とすべき知識や対象とするシステムや業務環境が異なることに起因するものである。鉄道分野においては、サポートプレーヤー（CSIRT）とレスポンスプレーヤー（現場のチーム）の役割分担が明確になることが想定され、双方のコミュニケーションギャップが課題となると想定される。

一方、航空分野においては、サポートプレーヤー（CSIRT）とレスポンスプレーヤー（現場のチーム）の役割分担は鉄道分野ほど明確にはならず、レスポンスプレーヤー（現場のチーム）にも高度なサイバー攻撃対応力が求められると想定される。このような分野の違いによる人材育成方針の違いについても、教育教材に反映することが望まれる。

５．２．２．　教材へのフィードバック

机上演習の結果より、システム維持管理者が認識すべきこととして以下の知見が得られた。これらの知見については教材の内容を修正する、項目として追記する等して、教材へ反映させることとした。

- サイバー攻撃対策は重大な経営課題である。
- 対策が急務である。
- 対策には迅速性が要求される。
- サイバー攻撃が発生した際の通報先（情報システム部門、CSIRT）を徹底する必要がある。
- 対応においては組織連携を伴う。（対応不能の場合にはより上位にエスカレーション）
- スマートフォン、無線接続等の脅威を理解する。
- サイバー領域の概念、用語を理解する。（指示する、指示される、両方の立場において情報共有を効率化するため）
- 最近のサイバー攻撃の傾向から、スピアフィッシング攻撃、マイニング、Pass the Hash 攻撃についての理解が必要である。
- 防御策は各レイヤーに対して実施する必要があり、このためにネットワークの知識(OSI 参照モデル)の知識が必要となる。
- スマートフォンの脆弱性、アプリに付随するソフトにマルウェアが混在している可能性が高いことを認識すべきである。

第６章.　　旅客輸送サービスにおける安全対策

教育の試行及び机上演習から、鉄道分野と航空分野ではシステム維持管理者のサイバー攻撃対策に対する認識が異なるとの知見が得られた。具体的には、航空分野においては、サイバー攻撃対策が大きな脅威と認識されている一方で、鉄道分野においては、サイバー攻撃対策は対岸の火事といった認識がシステム担当者にあり、教育の実施に際してサイバー攻撃対策の必要性を強く訴求する必要がある。この主な理由としては、航空分野のシステムは既に IT 化が進んでおり、社内外の様々なシステムと連携しているのに対して、鉄道分野のシステムは独自プロトコルによるクローズドシステムであることが挙げられる。しかしながら、鉄道分野のシステムについても、IT 化及びシステム連携が進んでおり、サイバー攻撃対策が急務となっている。このような背景のもと、サイバー攻撃対策の必要性を教育対象者に対して訴求することを目的として、鉄道分野を対象とした説明資料を作成した。必要に応じて、ご活用いただきたい。

旅客輸送サービスにおける安全対策

～ITセキュリティ目線から見た鉄道分野～

背景・世の中の流れ

- 鉄道分野では、旅客輸送サービスを脅かす外部環境リスクについて継続的に対策を実施し、安全かつ安定した輸送を実現していく必要がある。
  特に、昨今IT技術の進捗に伴い、新しいITサービスの取り込みによる旅客輸送サービスの向上が図られている。その一方で、鉄道システムにおいては電子技術が導入され、鉄道システムとITシステムとの差が少なくなってきたことから、新たなリスクとして、サイバー攻撃の存在を認識し、継続的に対策を実施しなければならない状況にある。

新たなリスク(サイバー攻撃)の顕在化
～何が変わったのか？～

- 連動装置も電子化により便利になったが、列車運行管理システムの一部としてつながっているために、サイバー攻撃の影響を受ける可能性がある。

  - 電子連動装置
    - マイクロコンピュータによる制御
    - 標準結線をプログラム化

  ⇧

  - 継電連動装置
    - リレー回路により構成
    - 標準結線が定まっている

出典：連動装置 日本信号株式会社 鉄道信号事業部
http://www.signal.co.jp/products/railway/productsinfo/2010/03/post-4.php

新たなリスク(サイバー攻撃)の顕在化
～何が変わったのか？～

- 電子化により便利になったが、プログラムの不具合により障害が発生することとなった。サイバー攻撃はプログラムの不具合を故意に顕在化させたり、不具合へのサイバー攻撃は故意に障害事象を発生させたりする可能性がある。

プログラムの不具合による障害事例　(サイバー攻撃は、同様な障害事象を発生させる可能性がある)

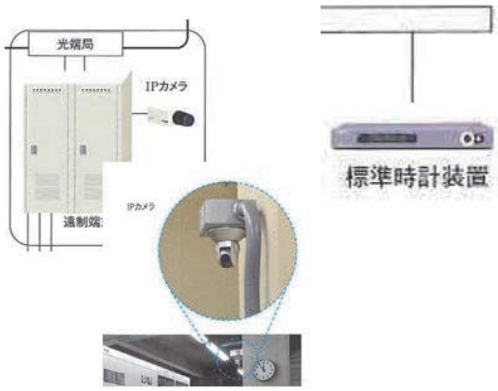
障害事例	発生日	障害の概要	主な原因	影響範囲	開発時期	原因フェーズ
JR東日本のSuicaで初の大規模トラブル	2006/12/1	12月1日に日付が変わった時点で利用者が改札を通過できなくなり、ゲートを開放することで対処。	自動改札機にインストールしているプログラムミス。Suicaの状態をチェックするフラグが誤って設定され、ゲートが閉鎖された。	184駅で発生した。	2001年サービス開始	保守
緊急地震速報誤報で電車止まる影響	2007/7/24	気象庁は24日正午前、神奈川県西部で震度5強～6弱という誤った情報を流した。	システム上のプログラムの不具合。共通地震規模計算の際、40秒前の別の地震データを誤って取り込んでしまったことが原因。	この影響で小田急電鉄の全ての電車を停止したが大きな揺れは無かったことから4分後に運転を再開。		開発
JRなどの自動改札の障害	2007/10/12	10月12日朝、首都圏のJRなど662駅で、「日本信号」製の自動改札機が使えなくなった。4400台の改札機が動かず、約260万人に影響。	自動改札機の組み込みソフトのバグ。センタからクレジットカードの特定データ件数が送られてくると電源を切るバグがあった。	約260万人に影響。		開発
JR西日本、特急列車が誤進入	2008/1/18	京都発新宮行き特急列車が新今宮駅を通過する際、本来大和路線(関西線)ルートに進入すべきところ、誤って大阪環状線ルートに進入。	メーカーにおいて自動進路制御装置を製作した際、プログラムが正しく製作されず、機能検査が不十分であったこと。列車ごとの進路は、ダイヤに基づく列車の順序にしたがって制御するよう製造する仕様のはずが、そのようになっておらず、新今宮駅手前に設置した制御点に早く到着した列車の進行方向にあわせて、出発側の分岐器が切り替わるプログラム仕様になっていたため。	運休計31本、遅れ計26本、影響人員約3万人。		開発

「重要インフラ情報システム信頼性研究会」報告書付録から転記

出典：「重要インフラ情報システム信頼性研究会」報告書(平成21年度)の公開
https://www.ipa.go.jp/sec/softwareengineering/reports/20100427.html

新たなリスク(サイバー攻撃)の顕在化
～何が変わったのか？～

- 列車運行管理/電力管理システムでは、インターネットでも利用されているIT製品が使われている場合があり、サイバー攻撃の影響を受ける可能性がある。
  - 監視カメラ(IPカメラ)
  - 時計装置
  - ディスプレイなど、既製品で販売が可能となっているソフトウェア製品やハードウェア製品の利用



マルチディスプレイ

京都鉄道博物館　運転指令所

出典：http://www.fun-toy-life.com/entry/2016/05/24/181811#運転指令所
http://www.mitsubishielectric.co.jp/society/traffic/product/yusou/y01.html

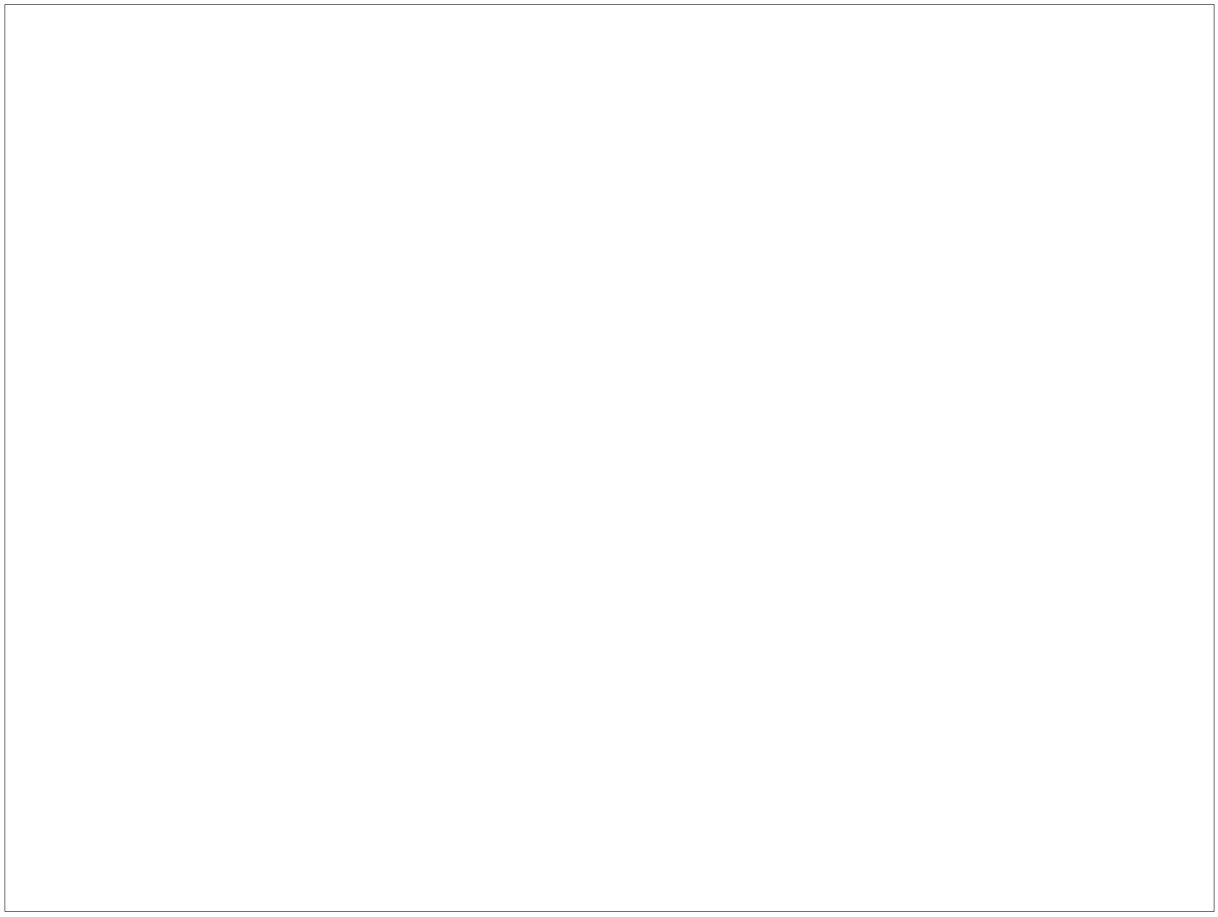
新たなリスク(サイバー攻撃)の顕在化
～何が変わったのか？～

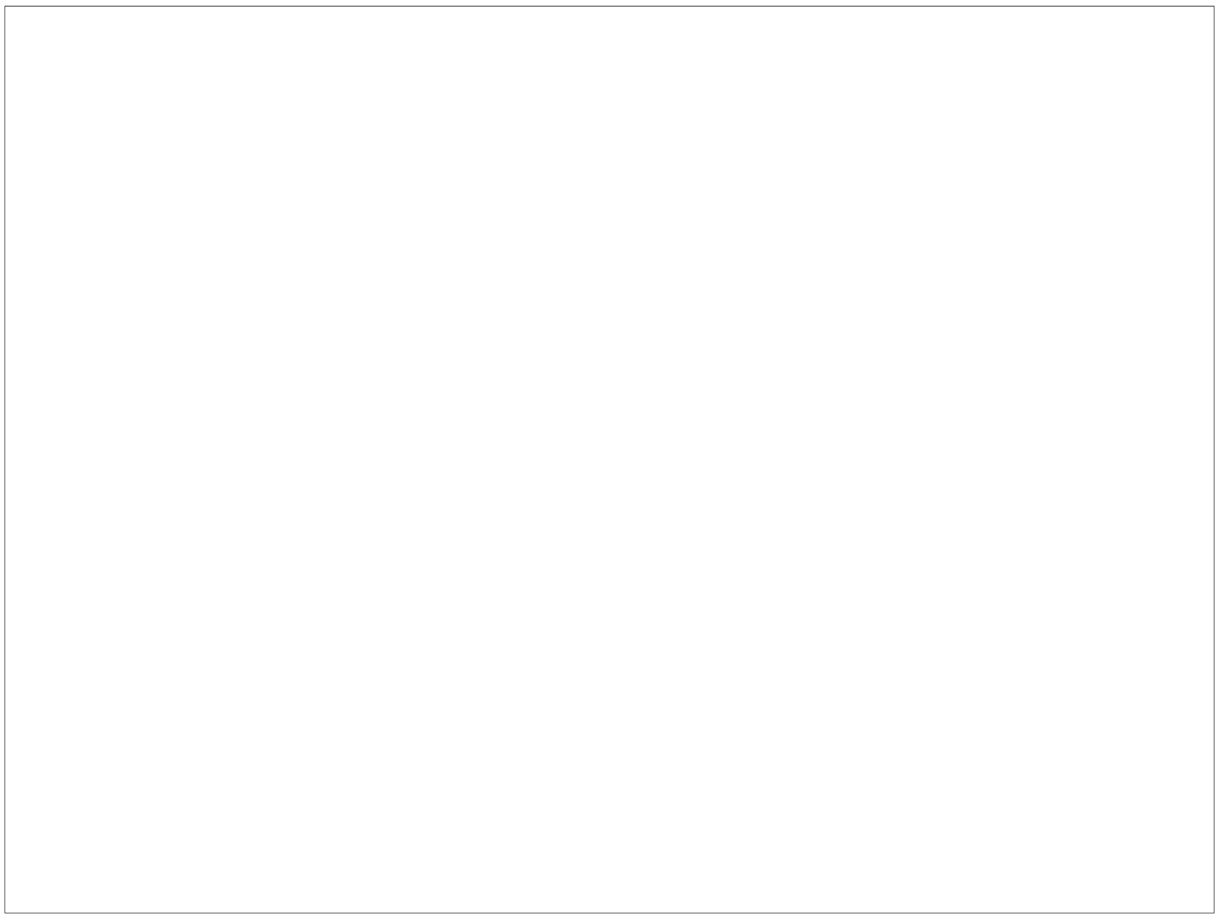
- 列車運行管理/電力管理システムはクローズドなネットワークで構成されているが、サイバー攻撃の影響を受ける可能性がある。

① **ネットワーク延長(外部から侵入される可能性)**
業者による遠隔保守だけではなく、相互乗り入れに伴いシステムの一部が他社に接続することも多い。また、ネットワーク延長先の変電所や踏切の遠隔監視システム等の設備が必ずしも物理的に十分に防護されていない場所に存在する場合もある。中央指令所以外にも、サイバー攻撃の侵入口となりえる設備が多数存在するようになった。

② **制御伝送系と制御表示系の混成(侵入されてから被害につながる可能性)**
サイバー攻撃の対象となりやすい制御表示系(列車情報処理装置など)と、鉄道システムの根幹である制御伝送系(連動装置など)とが、システムとして全て分離(独立)して構成されているわけではない。

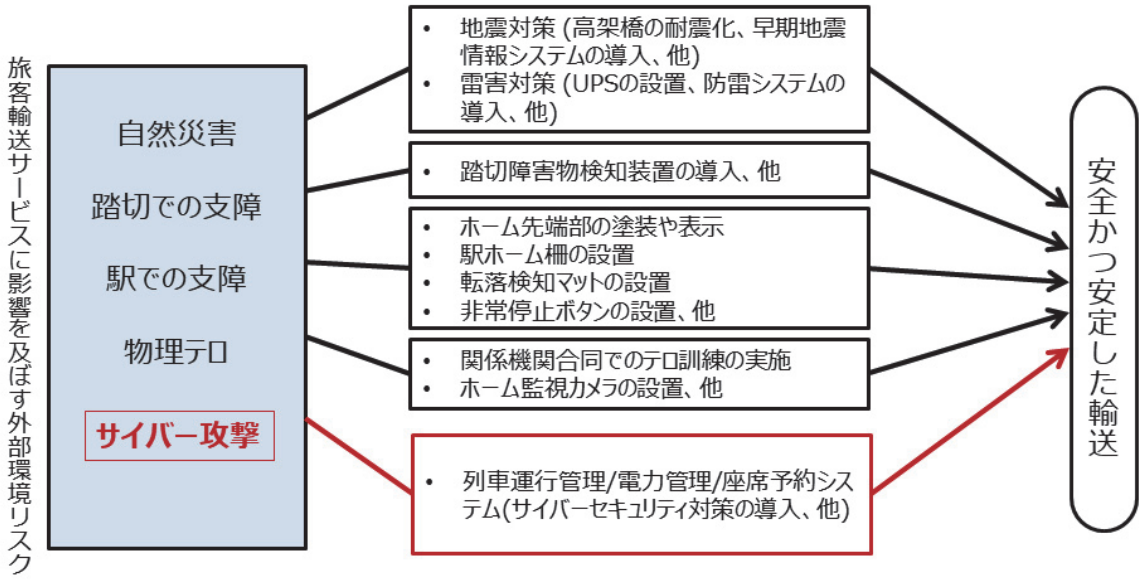
③ **帳票手続きの電子化/自動化(侵入されてから被害につながる可能性)**
変電所単位に予め登録した基本運転パターンにより、当日の運転パターンを作成する定時停送電機能など、これまでの紙の帳票手続きが電子化されただけではなく、さらに、自動化され、ネットワーク経由で制御されるようになった。





旅客輸送サービスにおける安全対策

- 旅客輸送サービスにおいては、外部環境リスクのひとつとしてサイバー攻撃を捉え、対策を行うことで、安全かつ安定した輸送を実現していく必要がある。



旅客輸送サービスにおける安全対策

- サイバー攻撃と言っても、いろいろな種別の攻撃があり、攻撃による障害事象も異なってくる。代表的な攻撃種別としては、機密性を脅かす攻撃(不正アクセス等)、完全性を脅かす攻撃(改ざんや消去等)、可用性を脅かす攻撃(システム停止等)がある。

種別	目的	システム	攻撃	影響
データが漏えいする可能性 (機密性を脅かす攻撃)	不正アクセス	列車運行管理	内部犯行 保守PCの悪用	漏洩した設計/構成情報を悪用した不正制御により列車が遅延する
		電力管理		漏洩した設計/構成情報を悪用した不正制御により電力供給が停止する
データが改ざんされる可能性 (完全性を脅かす攻撃)	データ改ざん	列車運行管理	USB経由でのマルウェア感染	ダイヤデータの改ざんにより列車が遅延する
		電力管理		保守作業データの改ざんにより夜間作業が中止される
業務が遅延・停止する可能性 (可用性を脅かす攻撃)	システム停止	列車運行管理	中央処理装置に処理量を超える大量データ送信	システム停止により列車が遅延する
		電力管理		システム停止により電力供給が停止する

旅客輸送サービスにおける安全対策

- 鉄道システムでも、ITシステムでのサイバーセキュリティ対策アプローチを活用していくことが有効である。

鉄道目線分類	指令所、変電所、駅舎に設置した中央装置、端末などを対象としたサイバーセキュリティ対策	運行管理、電力管理システムなどのシステム間、指令所、変電所、駅舎、他社などの設備・施設間の接続方法を対象としたサイバーセキュリティ対策	システム、設備、施設の運用・管理を対象としたサイバーセキュリティ対策
IT目線分類	エンドシステム対策	ネットワーク対策	運用/管理対策
対策の考え方	機器のマルウェア対策 不正処理防止策 アクセス制御 ログの取得/保管/保全	外部ネットワークとの分離 他ネットワークとの接続制御 通信のセキュリティ確保	セキュリティ仕様の確認 外部記憶媒体等のマルウェア対策 権限の適切な割当 脅威/脆弱性情報の収集 セキュリティ更新プログラムの適用 重要システムの監視
対策の具体事例	機器単体で実施する対策 • PCの不要なUSB挿入口を塞ぐ • USB等外部メモリのウイルスチェック • USBメモリの専用化 • PWの定期更新実施 • 重要データの暗号化/パスワードによる保護	ネットワークで実施する対策 • 外部システムとの境界線にFW設置 • IDSやIPS通信の監視防御装置の導入 • 片方向ゲートウェイの導入 • セキュリティ機能付スイッチの導入(ホワイトリストフィルタリング) • ログの定期的な分析機能の実装 • 通信の暗号化	体制/教育で行う対策 • CSIRT体制整備 • セキュリティ関係規則の整備(USB取扱い規則、ID/PW管理規則等) • 担当者に対する教育実施 • メーカー(業者)に対する教育 • 発注時のシステム要件定義にセキュリティ関連事項の記載 • メーカー(業者)との情報交換実施

第７章.　　交通セキュリティセミナー

2020 年東京五輪大会の開催を来年に控え、人材育成は愁眉の急となっている。サイバー攻撃対策に関わる人材育成、特に本研究において対象とするシステム維持管理者の育成については、教育の実施が日常業務への負担となることもあり、その必要性についての経営層の理解が必要不可欠である。また、サイバー攻撃の手法がより高度化、複雑化し、サイバー攻撃の脅威が拡大している現状では、サイバー攻撃による影響が事業継続を脅かすような事態に備え、経営層の強いリーダーシップが必要となって来ている。特に、サイバー攻撃対策を主導する CISO については、想定外の攻撃を受けた場合においても的確な状況判断と意思決定ができるようになることが望まれる。

サイバー攻撃対策の必要性についての経営層の理解は深まって来ており、各事業者とも人材育成に積極的に取り組みつつある。一方で、経営層が強いリーダーシップを発揮するためには、経営層においてもサイバー攻撃に関わる技術的知識を持つことが必要となる。

このような背景の下、本調査研究では、教材を作成するとともに鉄道及び航空事業者の経営層に向けた交通セキュリティセミナーを実施した。本セミナーでは、経営層が知識として持っておくことが望まれる技術的な知識を交え、強いリーダーシップを発揮するために経営層が意識しておくべき内容について解説を行なった。

プログラムと講演内容の一部を以下に掲載する。

（1）　交通セキュリティセミナーのプログラム

交通セキュリティセミナー

交通分野のサイバーセキュリティ対策における経営層の役割

○主　催：一般財団法人　運輸総合研究所
○後　援：国土交通省、サイバーセキュリティ戦略本部
○協　力：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
○日　時：**2019年2月18日（月）　14:30～18:00（14:00開場）**
○会　場：ホテル グランドアーク半蔵門　4階 富士東の間　（千代田区隼町1番1号）
○入場料：セミナー、懇親会ともに無料　　※セミナー終了後、3階 華の間にて懇親会を実施

プログラム

主催者挨拶　　**春成　誠**　一般財団法人 運輸総合研究所　理事長　　***14:30 ～ 14:35***

講演１「東京２０２０大会に向けたサイバーセキュリティのチャレンジ　　***14:35 ～ 15:35***
～ 経営リスクマネジメントの実践的ケーススタディ ～」

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　局長

《講演概要》
すでに１年半後に迫った東京２０２０大会は、真夏の過密都市東京の中において、大量の観客や関係者を安全・確実に輸送することが最重要の課題の一つであることはもちろんですが、一方で５０年前の大会と最も異なる側面として、これまでのオリンピックで最もデジタル技術やインターネットが使われる大会になる、とも言われています。本講演では、サイバーセキュリティの脅威・攻撃手法がより広域化・高度化する中で、「いかに限られた時間で大会運営に向けたITガバナンスを強化できるか」「いかに（組織委員会だけでなく）都市インフラを担うさまざまな事業者（パートナー）と連携して対策をとれるか」「限られたリソースをどのセキュリティ対策に投資すべきか」など、これからの時代の経営リスクマネジメントの課題を象徴するテーマを取り上げ、経営者として必要な視点についてケーススタディを展開します。

講演２「インフラに対するサイバー攻撃の脅威と対処方法　　***15:35 ～ 16:35***
～ 経営者に求められる強いリーダーシップ ～」

山崎　文明　情報安全保障研究所　首席研究員

《講演概要》
過去に実際に起こったインフラを狙ったサイバー攻撃の事例を振り返りながら、その手口を具体的に学習し、防御策について考えます。そして、今後起こり得るサイバー攻撃とその脅威を回避する手段について考えるとともに、経営者としての強いリーダーシップの必要性について理解します。

～　コーヒーブレイク　～　　***16:35 ～ 16:55***

講演３「これからの経営層が担うべきセキュリティ統制力向上への役割について　***16:55 ～ 17:55***
～ 徹底的な現状認識に基づく事前準備と事後判断における重要ポイントとは？ ～」

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

《講演概要》
事業活動におけるITやインターネットへの依存がますます高まっていく一方で、回避・検知することの難しい攻撃手法の常態化が進んでおり、発生要因の調査や解析が一層困難になっています。
このような状況下、サイバー攻撃による被害の発生を完全に回避することは不可能であり、経営に責任を持つ層（経営層）の積極的な関与と対応が求められています。
すなわち、経営層は、その準備段階においてサイバー攻撃対策に関する投資判断を行うとともに、深刻な被害に遭遇した場合において自ら陣頭指揮を取ることが求められています。
そこで、本セミナーは、このような事前準備の重要性と即検討を自らの判断で実施していただけるよう「徹底的な現状認識と会社全体のセキュリティ統制力の向上」を目的とします。

閉会挨拶　　**春成　誠**　一般財団法人 運輸総合研究所　理事長　　***17:55 ～ 18:00***

司会　**吉見　昌宏**　一般財団法人 運輸総合研究所　調査事業部長

Supported by 日本財団 THE NIPPON FOUNDATION

※　会場内での撮影・録音は禁止させて頂きます（主催者が許可した場合を除く）

（２）　東京 2020 大会に向けたサイバーセキュリティのチャレンジ
～経営リスクマネジメントの実践的ケーススタディ～

交通セキュリティセミナー講演
「交通分野のサイバーセキュリティ対策における経営層の役割」

TOKYO 2020

TOKYO 2020
PARALYMPIC GAMES

東京2020大会に向けた サイバーセキュリティのチャレンジ
～経営リスクマネジメントの実践的ケーススタディ～

平成31年2月18日
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員会
テクノロジーサービス局　局長　　舘　剛司

1

自己紹介

舘　剛司（たち　たけし）
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　局長

略歴：

1989年、大阪大学大学院・修士課程修了。同年、日本電信電話株式会社（NTT）入社。

映像伝送システム・次世代IPネットワークの開発、サイバーセキュリティ分野の研究開発戦略の策定などに従事。米国カリフォルニア大学バークレー校　経営工学・修士課程修了。

2013年より、米国のR&D子会社（NTT Innovation Institute, Inc.）設立とサイバーセキュリティ分野のR&Dプロジェクトに従事。

2014年より組織委員会へ出向し、東京2020大会の運営や準備活動に必要なネットワーク・情報システムなど技術全般に関する計画策定、開発、運用、サポートなどを統括。

2

TOKYO 2020

本日の視点

- ✓ 『オリンピックに向けた準備・運営（テクノロジー面）というプロジェクトの全権を任された際に、責任者・経営者として、サイバーセキュリティをどのように捉え、どのように対策に取り組むのか？』
- ✓ この実践的ケーススタディをもとに、組織・企業として抱えるサイバーセキュリティの本質的・共通的な課題に迫ってみます。

アジェンダ

- ✓ ケーススタディの前提条件（東京2020大会とは？）
- ✓ ポイント１：課題の定義（なにを守るのか？）
- ✓ ポイント２：CISOの役割（なにをすべきなのか？）
- ✓ ポイント３：組織全体の課題（だれの責任なのか？）
- ✓ ポイント４：守りと攻め（攻撃者の目線）
- ✓ 最後に（リーダーの資質）

ケーススタディの前提条件
（東京2020大会とは？）

リオ2016大会開会式の日本選手団入場行進

大会規模の比較

TOKYO 1964

競技数	20
種目数	163
参加選手	5,152
会場数	34
内:都内	22
チケット枚数	202万枚

TOKYO 2020

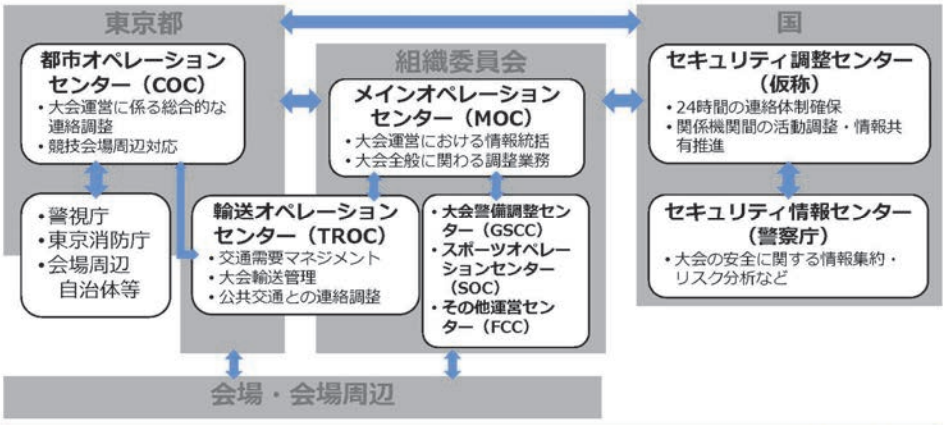
競技数	33
種目数	339
参加選手	11,090
会場数	42
内:都内	25
チケット枚数	1,010万枚

大会運営業務とその規模感（例）

- ✓ イベントオペレーション（モノの調達・流通）
  - ➢ 競技用具、計測機器・PC・通信機、競技用什器類、医療用品など／大会関係者に提供する食事：**1,400万食**（オリンピックのみ）、ピーク時は**30分で1万食提供**
- ✓ イベントオペレーション（ヒトの移動・輸送）
  - ➢ **観客：780万人**（オリンピック）、**230万人**（パラリンピック）／アクレディテーションカード発行枚数：**20万枚**／関係者・観客の輸送に必要な**バス：2,000台**／開催都市を訪れる**期間中の観光客2,000万人**
- ✓ スポーツオペレーション（競技運営）
  - ➢選手･役員数：**18,200人**／33競技（オリンピック）、**8,000人**／22競技（パラリンピック）
- ✓ ファシリティオペレーション（会場設置・運営）
  - ➢ **選手村16,000人収容**／**国際放送センター75,000㎡**／必要な**倉庫面積80,000以上**
- ✓ ビジネスオペレーション（販売・顧客管理）
  - ➢ チケット販売総数**1,010万枚**、公式モバイルアプリダウンロード数**最大2,000万**

オペレーションセンターを中心とした体制

✓ **大量の物流、関係者や観客の輸送・誘導、猛暑への対策、台風やゲリラ豪雨への対応、急なスケジュール変更、**など、さまざまな課題やインシデントに対処するための集中管理体制が必要。



ロンドン2012大会の サイバーセキュリティインシデント

- ✓ 大会公式サイトに2週間の開催期間で2億2,100万のサイバー攻撃
- ✓ 7月26日（開会式前日）に、東欧のハッカー集団が大会のITインフラに対して数10分間に渡って脆弱性を探すためのスキャン実行。
- ✓ 7月27日（開会式当日）に、**電力システムを狙った攻撃の情報を受け、多くの技術者を要所ごとに配置するマニュアル操作に切替え。**
- ✓ 同日午後5時には、（大会公式サイトへの）DDoS攻撃がピークに達し、北米および欧州の90のIPアドレスから1千万リクエストのDDoS攻撃が40分間にわたって継続。
- ✓ 8月3日（大会終了間近）には、一秒あたり30万パケットのDDoS攻撃が同じIPアドレスから送付。このアドレスはプレス向けに用意され共同利用されていたもの。

リオ2016大会のトラブル概観

- ✓ テレビでは放映されない数々のトラブルが発生。
  - ➢ 「（ゴルフ）競技中に過負荷による競技情報システムダウン」「大会初日の過負荷によるモバイルアプリダウン」**「インターネット回線トラブル」「停電・電源トラブル（五輪閉会式時間中の会場一帯の停電も含む）」**「多発するサイバー犯罪（なりすましWi-Fi、ATMスキミング）」など。
- ✓ 競技会場のIT環境はかなり貧弱。
  - ➢ 「観客向けWi-Fiはかなり限定的」「特にパラリンピックでは大型ディスプレイもかなり撤去」「競技がどう進行しているのか、見ていてもよくわからない」
- ✓ 競技運営だけはほぼ完ぺき。それ以外**（特に輸送・警備・サイネージ）はかなり関係者に不評。**
  - ➢ ギリギリまで予算削減・人員削減を行い、大会関係者や観客の満足度・サービスレベルを犠牲に。

平昌2018大会・開会式で発生したインシデントに関するおもな経緯・報道(1/2)

- ✓ 2018/1/6：米マカフィー社が、平昌冬季五輪の関連機関を標的にしたサイバー攻撃が確認されたと明らかに。
  - ➢ 2017年12月下旬の対テロ訓練期間中に、関係機関からを装った標的型メール攻撃を観測。
- ✓ 2018/2/9：開会式の45分前から、**プレス関係者向けの通信環境や映像配信、大会Webサイトなどに影響**。
  - ➢ **これまでオリンピックを標的としてきたサイバー攻撃と比べ、明らかに影響範囲が広い。**
- ✓ 2018/2/10：平昌大会組織員会が、大会開会式で発生したサイバー攻撃について正式発表。
  - ➢ 『開会式運営や競技運営に直接影響を与えるものではなく、システムは数時間で回復した。詳しい原因は解析中。』

平昌2018大会・開会式で発生したインシデントに関するおもな経緯・報道(2/2)

- ✓ 2018/2/12：米シスコシステムズ社の情報分析チーム（Cisco Talos）が、攻撃に用いたとみられるマルウェアの検体サンプルを確認したと報告。
  - ➢ マルウェアからはシステム破壊の機能のみが確認されている。
  - ➢ マルウェアには**44個の平昌五輪関連の資格情報（ユーザー名、パスワード等）とみられる文字列がハードコーディング**されている。
- ✓ 2018/2/14：Cyber Scoop社の報道によると、『Atos社内の複数のシステムが、2017年12月からすでに侵入されていた可能性が高い。』
  - ➢ Virus Totalにポストされたファイルをもとに、Cyber Scoop社が分析。
- ✓ 2018/2/25：米紙ワシントンポストが、『ロシア軍スパイが平昌組織委員会のコンピュータ数百台をハッキングし、北朝鮮の仕業と見せかけようとした』との米国情報当局者の話を報告。
  - ➢ コンピュータ用のルータ（通信機器）をハッキングし、ネットワークを麻痺させるマルウエアを埋め込んだとの分析。

ポイント１：課題の定義
（なにを守るのか？）

リオ2016大会のカヌー競技会場

インシデントに関する考察(1)

✓ **攻撃目的の変化・攻撃手法の進化**

- これまでの大会では、インターネットに晒されるWebサイトへの攻撃が主流だった。これに伴って、大会ボイコットキャンペーンも盛んだった。
- 今回は大会前の表立った活動はあまり見られなかったが、（おそらくは標的型攻撃を経て）明らかに**内部に侵入されてピンポイントでの攻撃**を許している。
- 自らの主張を世の中に訴える（ハクティビスト）というよりは、**目的を持った攻撃**に近い印象。

攻撃目的の変化・攻撃手法の進化

✓ “ハクティビストの攻撃”のレベルから、“サイバーテロ”と呼べる攻撃レベルへと、進化している。

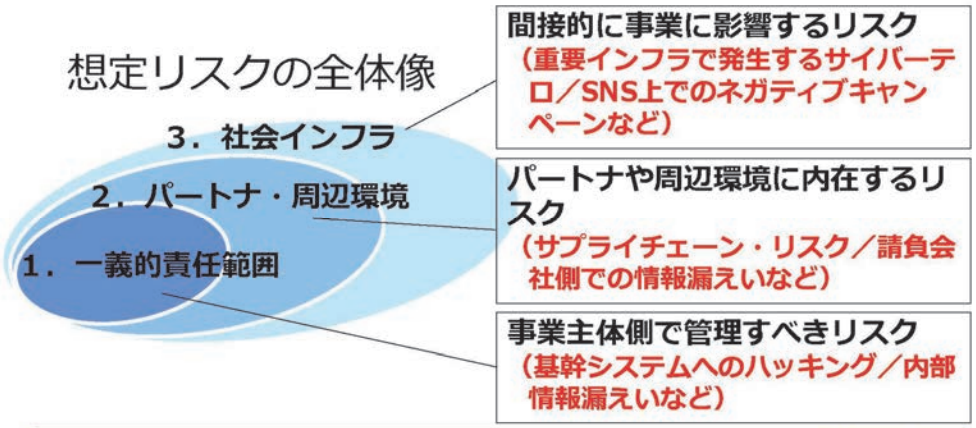
分類	項目	
金銭目的のサイバー犯罪	偽チケット販売サイト	各大会で必ず顕在化するリスク
	フィッシング、偽サイト、偽アクセスポイントなどによる個人情報の搾取	
	ランサムウェアによる脅迫	
ハクティビストの攻撃	大会サイトへの攻撃（DoS攻撃、改ざん）	
	スポンサーや開催都市など関連サイトへの攻撃	
	競技対戦国の関連サイトへの攻撃	
サイバーテロ	大会システムへの侵入・乗っ取りによるシステム破壊、データ破壊	よりビジネスインパクトが大きいリスク
	重要インフラへのサイバー攻撃	
サイバー戦争	多数来日する海外要人を狙ったサイバースパイ	
	リアルテロの手段としてのサイバー（認証カード改ざん、セキュリティカメラへのハッキングなど）	

ポイント１：課題の定義

- ✓ これまでにない危機感の高まりを受けて、まずは取り組むべき課題をどう定義するか。
- ✓ ITの世界では時間軸が早い、これまでの事業での常識が通用するとは限らない。
- ✓ 「今まで事故が起きていないから大丈夫」「この対策で、これまで大丈夫だったから」という判断は根拠がない。

なにを守るべきなのか？

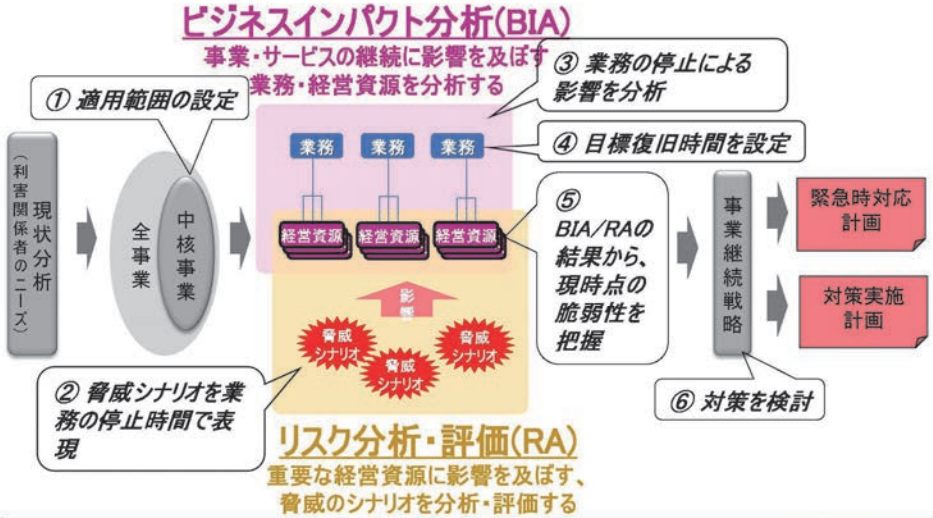
- ✓ 自社で運用する業務システム・ネットワークだけを守っても、事業を守ることにはならない。
- ✓ 事業委託先や社会的レピュテーションも含めて、総合的に守る観点が必要。



TOKYO 2020

リスク評価と対策立案

- ✓ ISO22320（社会セキュリティ緊急事態管理）にもとづく分析フロー。



TOKYO 2020

ポイント２：CISOの役割
（なにをすべきなのか？）

平昌2018大会の国際放送センター

インシデントに関する考察(2)

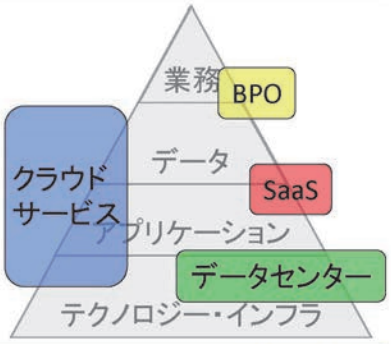
✓ **上流工程での検討・対策の重要性**

- 大会直前のタイミングで、国が関与して大会のサイバーセキュリティ対策を強化しても、事故は防げなかった。
- インシデント対応やフォレンジック対策など事後対策に関心が集まり勝ちだが、まずはネットワークや情報システムの**基本設計段階から、セキュリティ要件や運用体制のガバナンスについての考慮・徹底・定期的棚卸し**が重要。
- 高度な対策の前に、まず優先すべき対策：①サーバ堅牢化・管理者アカウント管理強化／②アウトソーシング事業者へのガバナンス強化／③エンドユーザ対策
- より高度なエンドポイントセキュリティ対策の導入にあたっては、作業の手戻り防止と全体費用の最適化のために、**実施時期・順序について十分な考慮が必要**。
- 組織として未成熟な段階でのソリューション導入は無駄な投資になりかねない。

ITガバナンスの課題

✓ 組織委員会における前提条件
- なるべくIT資産を持ちたくない。
- 多岐にわたる業務、関係組織との連携、失敗は許されない。
- 限られたリソースの中、スポンサー企業や関連組織の協力を最大限に仰ぎたい。
- つまり、クラウド、SaaS、BPOを最大限に活用したい。

✓ 課題
- ヘテロジニアスな環境において、**統一的なITセキュリティ・ポリシー、情報セキュリティ管理、迅速なインシデント対応**などをいかに実現するか？
- アウトソーシング先のＩＴ基盤、運用も含めた**ガバナンス強化**が必要。



ポイント２：CISOの役割

✓ **「すでにできあがったシステム、組織、業務フローにおいて情報セキュリティを確保する」だけでは不十分。**

✓ **「これから変化するシステム・組織において、情報セキュリティの確保のために、もっとも最適なプロセス・アプローチ・リソース計画を策定・実践する。」業務システム全体のアーキテクチャ設計がポイント。**

✓ **さらに、ITセキュリティ投資の優先度の見極めがポイント。（なにを捨てて、なにを救うか）**

ポイント３：組織全体の課題（だれの責任なのか？）

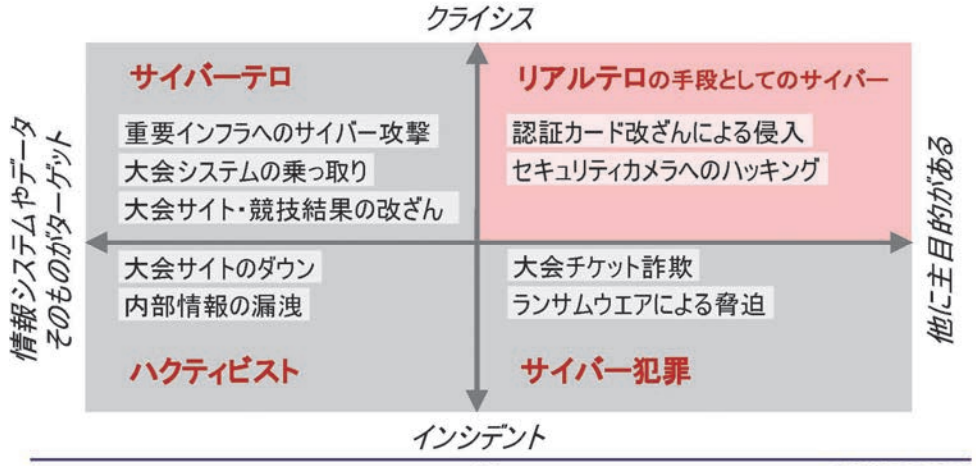
平昌2018大会のテクノロジーオペレーションセンター

実は現実空間で起きていることが、サイバー空間でも起きているだけ

- ✓ **ロンドン**：プロテスト集団による政治的主張、アラブ・イスラム武装勢力によるテロ
- ✓ **ソチ**：イスラム武装勢力、国内分離独立勢力などによるテロ
- ✓ **リオデジャネイロ**：麻薬組織、マフィアなどによる犯罪
- ✓ **平昌**：隣国との関係、ドーピング疑惑に関わる国家的関与
- ✓ **東京（予想）**：
  - ➢ 海外での模造品流通（偽サイト、偽チケットなど）
  - ➢ インバウンドのハクティビスト（過激な自然保護団体など）
  - ➢ インバウンドのテロリスト・犯罪者
  - ➢ ホームグローン・テロ

手段としてのサイバー

✓テロ・業務妨害の手段として、サイバー攻撃のコストパフォーマンスが非常に高いため、これまで想定する必要がなかったリスク要因となってきた。



ポイント３：組織全体の課題(1/2)

✓もはや情報システム部門の所掌範囲を超えた課題であり、業務部門をまたがった関与が必要。

- 警備部門：リアルテロの手段としてのサイバーセキュリティ対策
- 総務部門：情報漏えい事故に際しての対外的説明責任／真に有効な情報セキュリティのガバナンスルール
- 調達部門：業務委託先の情報セキュリティ管理義務条項
- 法務部門：サイバー攻撃による事業損失に対する適切な免責条項
- 広報部門：ネット上の公開情報の適切な管理（デマ、詐欺情報などの監視）／レピュテーションモニタリング

✓社内で必要なのは、サイバーセキュリティ分野の専門家の育成ではなく、各業務における専門家にITやサイバーに関する知見、それに付随するリスクに関する知識、を身に着けさせること。そのためのモチベーションを持たせること。

ポイント３：組織全体の課題(2/2)

- ✓ **組織として重要なのは、事業リスク全体の観点から、サイバーセキュリティ対策の優先順位や投資バランスを正しく判断できること。**
  - **『情報セキュリティ』vs.『事業継続性』／『レピュテーション対策』vs.『業務効率性』／『社員教育コスト』vs.『システム更改コスト』**
  - **得てして、見積もりが難しい項目（サイバーセキュリティリスク＆対策）は低く評価される傾向がある。**

ポイント４：守りと攻め（攻撃者の目線）

リオ2016大会の近代五種競技

インシデントに関する考察(3)

- ✓ 実はサイバーセキュリティのインシデント以外にも、放送コメンテーター用システムなど主要システムでトラブルが多発。
- ✓ これらの課題、ITガバナンスの欠如、などは、サイバーセキュリティ面にも影響。
- ✓ 一方で、大会におけるITの活用は大会ごとにますます増加傾向。

テクノロジー諮問委員会提言書（平成30年6月28日）より

アクション１（運営のスマート化）

準備 → 実行 → 後始末

- ✓ 大量の物流・輸送をスマートにこなす
  - ➢ **水素エネルギーや再生可能エネルギーの活用**により、カーボン排出量を最小化する大会運営を実現する。
  - ➢ **大量の交通データ分析**に基づくきめ細かい渋滞予測、急な競技スケジュール変更などにも**迅速に対応できる**関係者車両の最適配置、などITを最大限活用して実現する。
- ✓ 現場ボランティアを支えるモバイル
  - ➢ **モバイルデバイスを活用し状況を見える化**することで、現場の最適判断と快適な業務環境を実現する。
- ✓ 観客の快適をサポートするＡＩ
  - ➢ **ロボット・多言語翻訳**によるフレンドリーな会場案内や競技解説、**チャットボット**による迅速な問い合わせ応答（コールセンターなどのオペレーションコストの削減）、トイレや売店の待ち時間予測など、**課題解決のためのAI活用**を実現する。
- ✓ 会場の警備をサポートするテクノロジー
  - ➢ **生体認証**を活用した迅速・安全な関係者の入退場管理、セキュリティカメラと画像処理技術による**混雑度モニタリング**、などにより警備員業務を効率化する。
- ✓ 大量の物品調達の後始末は？
  - ➢ 大会後の物品二次利用やオークション販売を支える、**リユース支援プラットフォーム**を活用する。

ポイント４：守りと攻め

- ✓守りのサイバーセキュリティ対策：穴を防ぐだけの仕事であれば、モチベーションが長続きしない、言い訳を考える状況に追い込まれる。
- ✓攻めのサイバーセキュリティ対策：情報システムを活用するからこそのサイバーセキュリティ。サイバーセキュリティを、もっとクリエーティブな仕事にするべき。
- ✓まずは経営層に、もっと情報システムについて攻めの正しい姿勢が欲しい。＝サイバーセキュリティにも意識の高い経営者
- ✓情報システムのトラブルの９０％以上は、サイバーセキュリティ以外。まずは情報システムとその設計・運用に関する理解を。

攻撃者目線の重要性

- ✓ システム全体の複雑性が増すにしたがい、すべてのリスクを洗い出す作業がますます困難に。
  - ➢ 「穴を見つけてふさぐ」という終わりのない作業だけを繰り返しても、モチベーションが下がる、どこかで妥協したくなる。
- ✓ むしろ「新しい穴を見つける」「誰も気づかなかった抜け道を探す」という**“クリエーティビティ”が重要。**
  - ➢ 特にIoTのような新しいインフラを対象とする際には、「守る」だけでなく、「攻める」ためのアイディア出しこそが近道。最初からすべての穴を見つける必要などない。
  - ➢ 取り組むべき課題は、「組織をまたがって必要な情報にアクセスできる仕組み・権限をいかに持たせるか？」、「攻撃専門チームの知見をいかに安全に管理・継承するか？」

最後に（リーダーの資質）

リオ2016大会の7人制ラグビー

現場のリーダーに求められる資質

- ✓ オリンピック・パラリンピックの準備・運営とは、すべてにおいてグローバルクラスのプロジェクト。
  - ➢ 関与する人材・組織／プロジェクト管理の方法論／指揮命令系統／狙ってくる団体（自然保護団体、ハッカーコミュニティなど）
- ✓ 現場のリーダーには、単にITセキュリティの専門家であるだけでなく、リーダーとしての資質や実戦経験が求められる。
  - ① **技術的スキル・経験**＝情報セキュリティ対策とサイバー犯罪対策（攻撃予兆分析、フォレンジック対策など）の両スキルを備える。
  - ② **リーダーシップ**＝大会時に発生するインシデントに対して迅速・的確な判断・決断ができる。
  - ③ **コミュニケーション力・人脈**＝ハッカーコミュニティや海外主要機関のキーメンバーと顔が見える信頼関係を持つ。（英語力・コミュニケーション力も重要）

インシデントに関する考察(4)

✓ **本当の意味での連携のむずかしさ**

- 英語でのコミュニケーション、業務の進め方の閉鎖性、などにも起因して、組織をまたがった連携・コミュニケーションに課題がなかったか？
- 大会運営においてサイバーインシデントが発生した際には、『競技運営の継続』『重要な情報システムの復旧』こそが最優先であり、情報システム部門責任者の迅速・適切な判断と、それを支えるガバナンス体制が重要なはずだが。。。
- 組織をまたがったシステム監査、ログ情報の統合的な収集分析、事前合同演習の実施、などに課題がなかったか？
- 意識していても、**ついつい縦割り組織の弊害、互いの領域に踏み込まない妥協、などがまかり通っていないか？**

ご清聴ありがとうございました。

（３）　重要インフラに対するサイバー攻撃の脅威と対処方法
～経営者に求められる強いリーダーシップ～

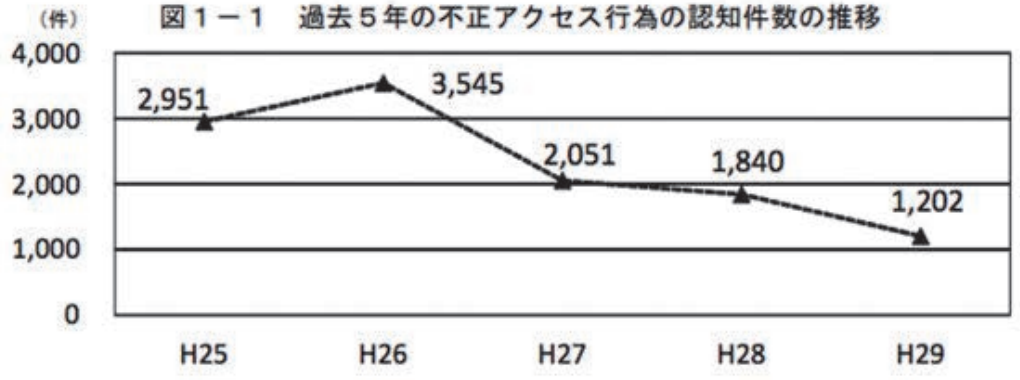
重要インフラに対する
サイバー攻撃の脅威と対処方法

2019年2月18日
情報安全保障研究所
首席研究員　山崎　文明

減少傾向にある不正アクセス

平成29年における不正アクセス行為の認知件数[注1]は1,202件であり、前年と比べ、638件減少した。

図１－１　過去５年の不正アクセス行為の認知件数の推移



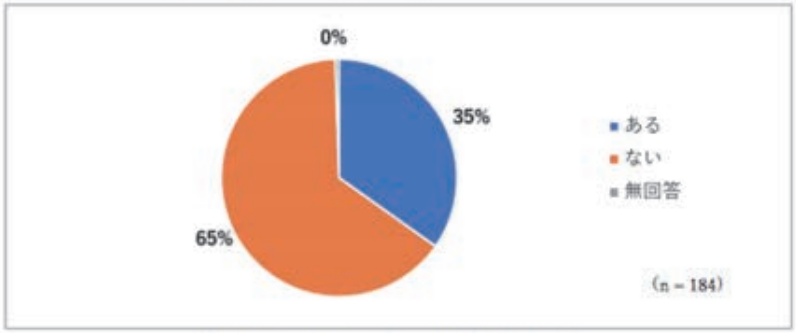
2018年3月22日（平成30年）不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況
国家公安委員会

2

JPCERT/CCの調査では3社に1社が感染

■ ランサムウェアの被害にあったことはありますか？

調査方法	アンケート調査
調査対象	国内の重要インフラなどの組織
調査期間	2017年9月19日～2017年10月17日
回答組織数	184組織
調査目的	各組織におけるランサムウェアの被害実態や対策などについて状況を把握するために実施



［図2-3　ランサムウェアの感染被害の有無］

【出典】2018年7月30日　一般社団法人JPCERTコーディネーションセンター
「ランサムウェアの脅威動向および被害実態報告書」

3

ドイツ鉄道Deutsche BahaがWannaCryに感染

■ 2017年5月

✓ 不特定多数を狙った犯行、身代金として＄300を要求

✓ロシアの鉄道会社の感染

4

日本に向けたウイルスも存在

5

奈良県宇陀市立病院でランサムウェアに感染

■ 2018年10月16日午前5時40分頃ウイルス感染
- 医療基幹系システムの初めての感染例

■ 50時間のシステム中断
- 10月18日午前7時復旧

■ 来院患者3,835名の内、1,133名の診療記録が部分的に参照できない事態に

■ 原因はシステム会社の不備により
- 最新のウイルスソフトがインストールされていなかった
- バックアップに必要な磁気テープが装填されていなかった


NHK NEWS WEB

関西 NEWS WEB

病院の電子カルテ ウイルス感染

10月23日 19時04分

奈良県宇陀市の市立病院で、電子カルテのシステムがコンピューターウイルスに感染し、患者１１００人余りの診療記録の一部が開けなくなりました。
病院によりますと、個人情報の流出はなく、現在は平常どおり診療を行っているということです。

宇陀市立病院によりますと、今月１６日、電子カルテのシステムが使えなくなったことに職員が気づき、システム会社に連絡したところ、コンピューターウイルスに感染していることがわかったということです。
病院ではシステムを停止させて対応にあたり、２日後には復旧しましたが今月１日から１５日までに作成した患者１１００人余りの問診でのやり取りの記録に暗号がかけられた状態となっていて開けなくなっているということです。
このトラブルによる個人情報の流出はなく、現在は平常どおり診療を行っているということです。
病院によりますと、システムは今月１日に導入したばかりで、最新のウイルス対策ソフトが入っておらずデータのバックアップも取っていなかったということです。
宇陀市立病院は「市民の皆様にご心配とご迷惑をおかけし大変申し訳なく深くおわび申し上げます」としています。

6

奈良県宇陀市立病院でランサムウェアに感染

- GandCrab（ガンドクラブ） V5.02
  - ✓ Windows XP、Vista、Windows 7、8、10に感染
  - ✓ 頻繁にアップデートを繰り返している
  - ✓ 支払いは仮想通貨DUSHで
- ルーマニアのBitdefender社無償除去ツール公開
  - ✓ 10月25日　V1、V4、V5に対応
  - ✓ Bitdefender GrandCrab V1,V4,V5 Decryptor
    - https://labs.bitdefender.com/category/free-tools/
- 「無償除去ツール」を騙った有償サイトが多数乱立
  - Data Recovery Pro
  - GridinSoft Anti-Malware
  - Loaris Trojan Remover
  - Reimage Repair
  - Plumbytes Anti-Malware
  - SpyHunter
  - WiperSoft

7

ランサムウェア対策は「データバックアップ」

- 警視庁はデータのバックアップを推奨

- ランサムウェアの新しい傾向
  - ✓ 復号ツールを使ってもランサムウェアが子供を隠しファイルに作成、しばらくして再暗号化
  - ✓ 原則は全システムの上書き

8

ランサムウェアより恐ろしいドクスウェア

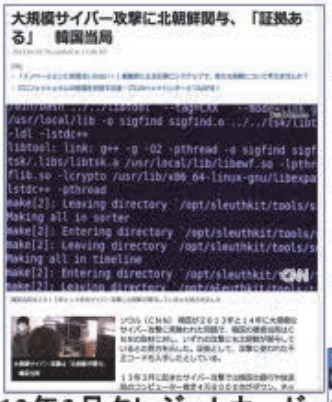
- doxing（ドクシング）
  - ✓ 個人攻撃のためにその人の個人情報をWeb上で公開するいわゆる「晒し」を意味する英語のインターネットスラングである。日本語では「晒し」。
- Doxware（ドクスウェア）
  - ✓ ランサムウェア（ransomware）の反対語。ランサムウェア攻撃では、マルウェアは被害者のデータを暗号化し、支払いを要求して必要な解読鍵を提供する。ドクスウェア攻撃では、攻撃者またはマルウェアは被害者のデータを盗み、手数料が支払われない限り公開すると脅かす。
  - ✓ 医療機関では特に警戒を要す
- 医療機関から漏えいした65万件のデータWebで販売される
  - ✓ 2016年6月28日(米国時間)、データ漏えいが発生したのは米国ミズーリ州ファーミントンの医療機関、米国中央/中央西部の医療機関、米国ジョージア州の医療機関で、それぞれ4万8000人、21万人、39万5000人の患者の医療記録データが漏えいしたとされている。
    医療機関は支払を拒否。結果として窃取された医療機関データはダークWebで151ビットコイン(1千万円ほど)から607ビットコイン(4千万円ほど)で売りに出され、すでに一部は売買が成立したようだと指摘がある。

9

DMARC

Domain-based Message Authentication, Reporting and Conformance

問題の本質は同根



2013年3月クレジットカード会社からの月次明細

2015年6月公開メールアドレス

2015年7月
人事部からのメール

2016年6月
電子チケット

メールアドレスにまつわる問題

■公開されているメールアドレス
- ✓お問い合わせメールアドレス　info@nenkin.go.jp
- ✓別ドメインとしていれば感染は広がらなかった
  - info@nenkin.go.jp →　postmaster@info.nenkin.go.jp

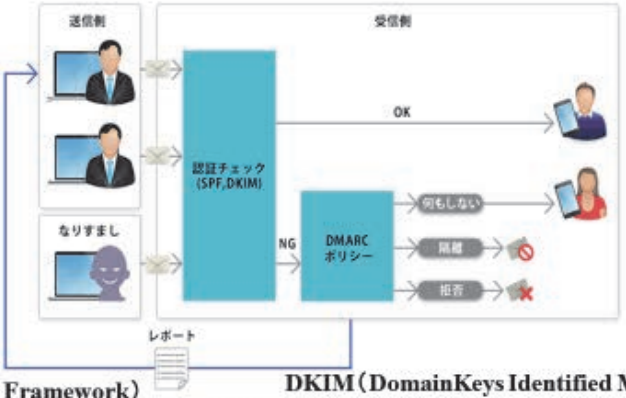
■売買されているメールアドレス
- ✓セミナー参加申込者のメールアドレス
- ✓エイリアスの利用
  - f-yamasaki-seminar@nenkin.go.jp

■ 推測できないメールアドレス体系
- ✓f-yamasaki@nenkin.go.jp
  - →f-yamasaki89@nenkin.go.jp

そもそも偽メールが届かない仕組み構築

■ **DMARC（Domain-based Message Authentication, Reporting & Conformance）**

- ✓ 2012年1月30日にGoogle、Facebook、Microsoftなどがスパムやフィッシングの脅威撲滅を目的としたワーキンググループ「DMARC.org」を発表
- ✓ 米国や英国を中心に急速に広まっているメールの判別システム



SPF（Sender Policy Framework）
送信元のIPアドレスが送信者名と整合するか確認する仕組み

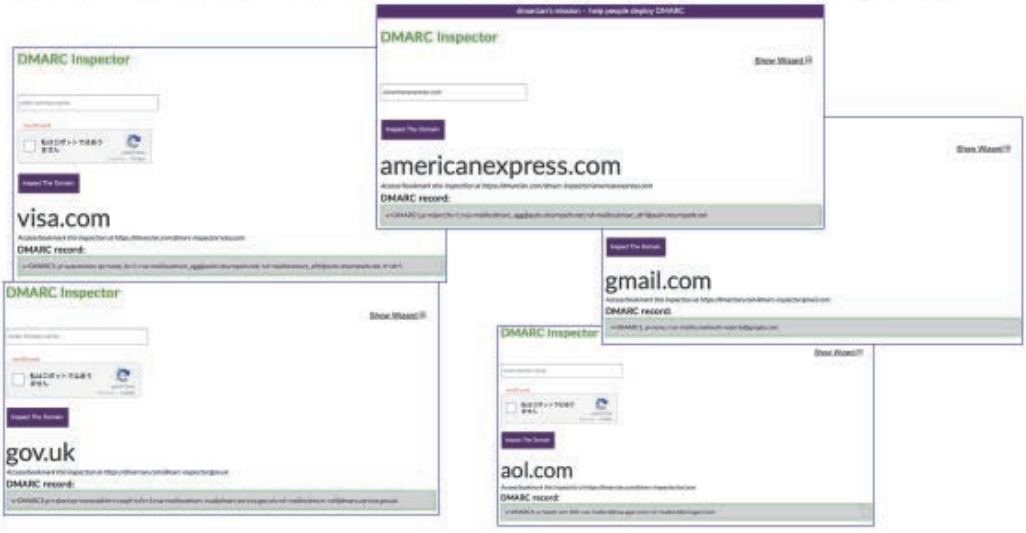
DKIM（DomainKeys Identified Mail）
電子メールに電子署名を行なって詐称を防止する仕組み

【出典】http://www.cuenote.jp/library/marketing/dmarc.html

13

米国や英国では政府主導でDMARC

- ■ 米国の大手クラウドサービス事業者やペイメント事業者が対応済
- ■ 英国政府がサイバー防衛国家戦略として対応済
- ■ DMARCに対応しているか調査できるサイト　DMARC Inspector



14

BECの被害とDMARCの限界

■ 正規のフリーメールアドレスには無力のDMARC

この企業の社長のメールアドレスから同社の財務担当の幹部に対して送られたものでしたが、日本人同士のメールにも関わらず件名が英語で緊急を意味する「Urgent(ASAP)」となっており、また返信先として指定されているメールアドレスにはCEOを想起させるGmailのアドレスが設定されていました。このケースでは、社長の正規のメールアドレスから送信されていたため、サイバー犯罪者によって何らかの手法で社長のメールアカウントが乗っ取られていたものと考えられます。(2017年3月13日トレンドマイクロ)

■ 業務命令にフリーメールアドレスは使用しない

- ✓ 業務連絡には正規メールアドレスで
- ✓ 重要な伝達には電話を使用する

■ 内部統制上、複数者の承認を経て振込を行う仕組みとする

■ 社外から送られてきたメールのFromに自己ドメインを含む場合はブロックする

■ 類似ドメイン名はできるだけ取得する

- ✓ yamada@example.co.jp→yamada@example.com yamada@example.net yamada@exarnple.co.jp yamada@examp1e.co.jp

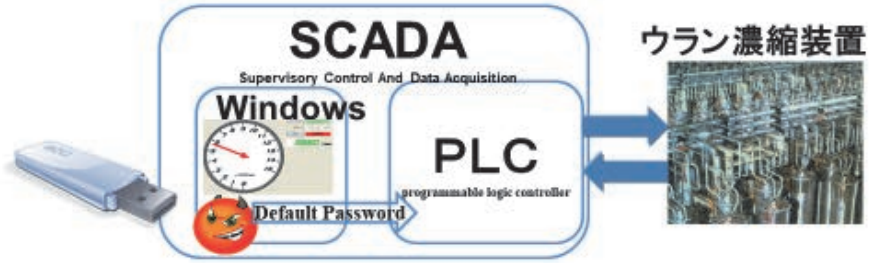
■ 関係先を騙ったメールはDMARCで拒否

15

Data Diode

スタックスネット(Stuxnet)は本当に脅威か

■ 原因はデフォルトパスワード

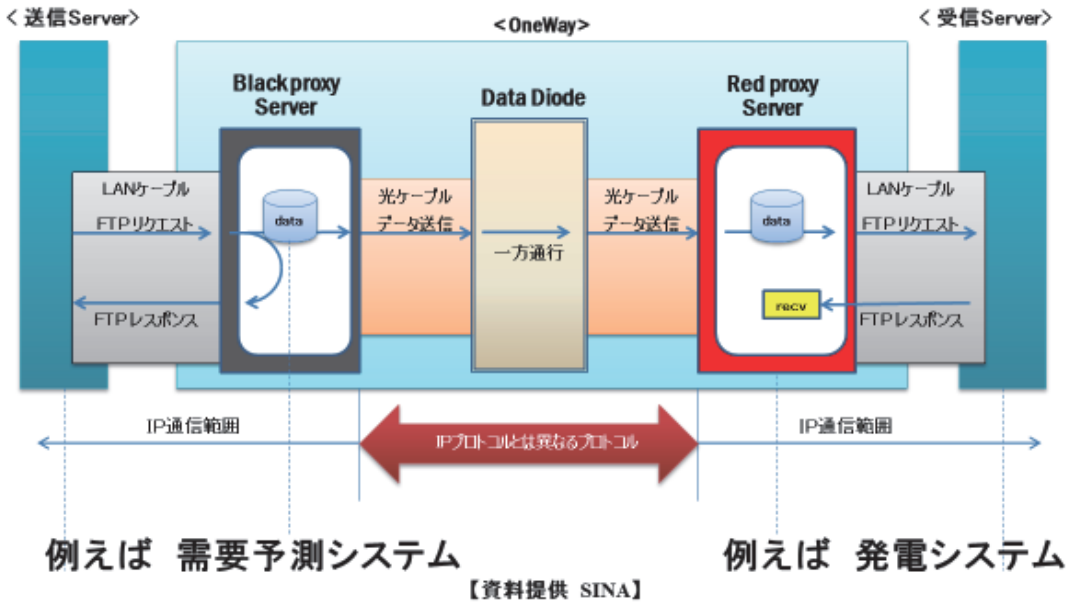


■ 真実が語られないウイルスの本質
- ✓ デフォルトパスワードを使用するウイルス（ワーム：Worm）
  - ・ Voyager Alpha Force/Zotob/My Spooler

17

普及が望まれるデータダイオード

FTP送信を例にOneWayの構成図
データは左側から右側に一方通行で逆流しないことを保証する高度なセキュリティレベルを実現

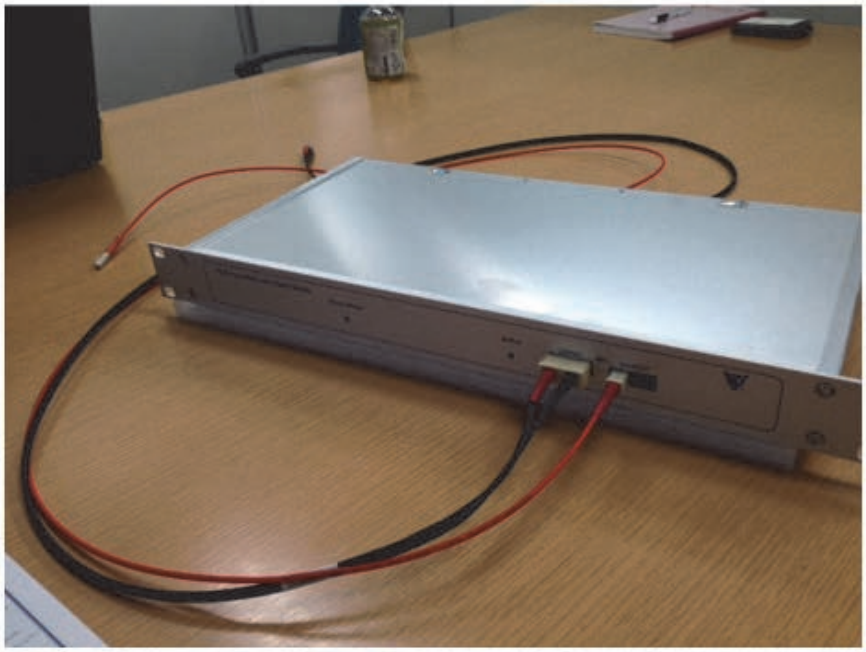


例えば 需要予測システム　　例えば 発電システム

【資料提供 SINA】

18

一方向ネットワークとデータダイオード



19

物理切断やファイアウォールよりも合理的なダイオード

■ 確実なセキュリティ

- ✓ 完全な外部ネットワークとの隔離
  - データもコマンドも外部から内部ネットワークに流入することはできない
  - マルウェアのC&C通信も攻撃司令パケット(外部からのAckパケット)が流入できず活動が抑制される
- ✓ 物理的な切断に伴うリスク
  - 情報共有のためにUSBなどの可搬性記録媒体の使用が想定されるが、媒体の盗難、紛失、ウイルス感染などかえってリスクが増加する
- ✓ 設定ミスによる脆弱性誘発がない
  - 設定にミスが発生した場合にも外部から侵入できる脆弱性は発生しない

■ 運用負荷・コスト削減が期待できる

- ✓ アドレス・ポートによるACLやアクセスログ、ユーザアカウントの管理が不要/簡易になることで、運用負荷・コストが軽減される
- ✓ 外部から内部への通信ログが発生しないため、モニタリングの運用負荷・コストが軽減
- ✓ 複雑なファイアウォールの設定がないため、定期的な脆弱性診断コストが軽減される
- ✓ セキュリティドキュメント量を大幅に削減
- ✓ 監査対象の少量化に伴う、外部監査の対応コスト削減

20

米国連邦政府が推奨するデータダイオード

■米国国土安全保障省　制御システムを守る7つの戦略

3. REDUCE YOUR ATTACK SURFACE AREA

Isolate ICS networks from any untrusted networks, especially the Internet.b Lock down all unused ports. Turn off all unused services. Only allow real-time connectivity to external networks if there is a defined business requirement or control function. If one-way communication can accomplish a task, use optical separation ("data diode"). If bidirectional communication is necessary, then use a single open port over a restricted network path.

■米国原子力規制委員会　規制ガイドラインNRC RG5.71

Only one-way data flow is allowed from Level 4 to Level 3 and from Level 3 to Level 2.


REGULATORY GUIDE

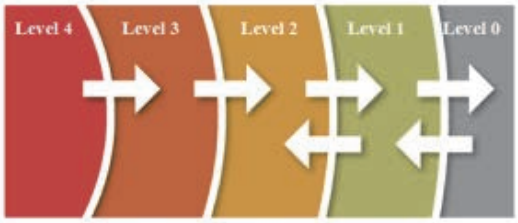


Figure 5 Simplified cyber security defensive architecture

21

Supply Chain Problem

Chinese Telecom Provider Says "Goodbye to Cisco Gear"

■ 中国最大手ISPがシスコ製品のリプレイスを完了 2012年10月

- ✓ China Unicomが思科製品の脆弱性とバックドア（后门）という<u>セキュリティ上の理由</u>でリプレイスを進めてきたプロジェクトが完了
- ✓ バックボーン163、169で中国のインターネットのトラフィックの80%を処理
- ✓ 突然の停止（<u>Kill Switch</u>）を警戒

23

中華人民共和国国家情報法の制定

- ■ 2017年6月26日制定、翌6月27日施行
- ■ 国の情報活動の基本方針、実施体制、情報機関の職権、法的責任について定める
- ■ 第1条　国の情報活動を強化及び保証し、国の安全と利益を守ることを目的とする
- ■ 第7条　いかなる組織及び個人も法に基づき国の情報活動に協力し、国の情報活動に関する秘密を守る義務を有し、国は情報活動に協力した組織及び個人を保護する
- ■ 第9条　国は、国の情報活動に大きな貢献のあった個人及び組織に対し表彰及び報奨を行う
- ■ 第25条　国の情報活動への支援・協力により財産の損失が生じた個人及び組織に対しては国の関係規定に基づき補償を行う

24

政府の重要インフラ「安全基準等策定指針」今春改定

■ 2019年1月17日専門調査会会合開催

■ 国内サーバーでの保管を求める
- ✓ 国際動向も踏まえた望ましいデータ管理
  - 海外のデータセンターに個人情報を保管することを禁じる法律を制定する国が大半
- ✓ インフラ事業者が持つ重要データについては、サイバー攻撃から保護するため、国内サーバーでの保管を求める規定を設ける方向に

25

もう一つの戦争 Supply Chain Problem

■ 特殊作戦ヘリのユニットや海軍のポセイドン偵察機で、空軍のC-130J輸送機で中国からの偽造電子部品発見される（2012年5月米上院軍事委員会報告）

【総括】

「当軍事委員会は2009年から2010年までの2年間に国防総省に供給された兵器を対象とした調査で、合計1800件の偽造電子部品を発見した。この偽造品は部品の個数にして100万点以上となった。これら偽造品の製造元に関して約100件を追跡調査した結果、70%以上が中国であることが確認された。その他の国としてはイギリスやカナダ、日本も浮上したが、そもそもの製造国から転売された形跡が濃く、ここでも世界の偽造品大国である中国の影が大きい」

■ たった10ドルの部品で数百万ドルのミサイルが役立たずになってしまう現実

26

もう一つの戦争 Supply Chain Problem

- 製造・物流にかかわる多くの中国人
  - ✓ 中国国内生産
    - 人民解放軍から外資合弁企業へ派遣される社員
    - 結成が義務付けられている中国共産党労働組合
  - ✓ 米国国内生産
    - 愛国心と金銭による誘惑

Chisco

Michael A. Aisenberg
Principal Cyber Policy
MITRE

27

重要インフラ産業の従業員の採用要件

- 米国防総省のクリアランスとポリグラフ検査
  - ✓Secrete Clearance
    - **TS/SCI (Top Secret/Sensitive Compartmented Information)**
    - **SIGINTや核兵器開発、核開発従事者に求められるクリアランスレベル**
  - ✓ポリグラフ検査
    - 国防総省指令5210.48 国防総省規則5320.48R
    - DoD NSA CIAで義務化

- 我が国でも確立されなければならない民間の採用手続き
  - ✓ 少なくとも複数のリファレンスをとりましょう
    - 大学の複数の教授、ゼミの教授、複数の昔の上司など
- 我が国でも必要なOPSEC教育

28

求められる経営者の強力なリーダシップ

- DMARCを国家戦略と位置づけて推進しよう
- データダイオードを普及させよう
- サプライチェーン問題に注意
- 採用手続きに工夫を

自己紹介

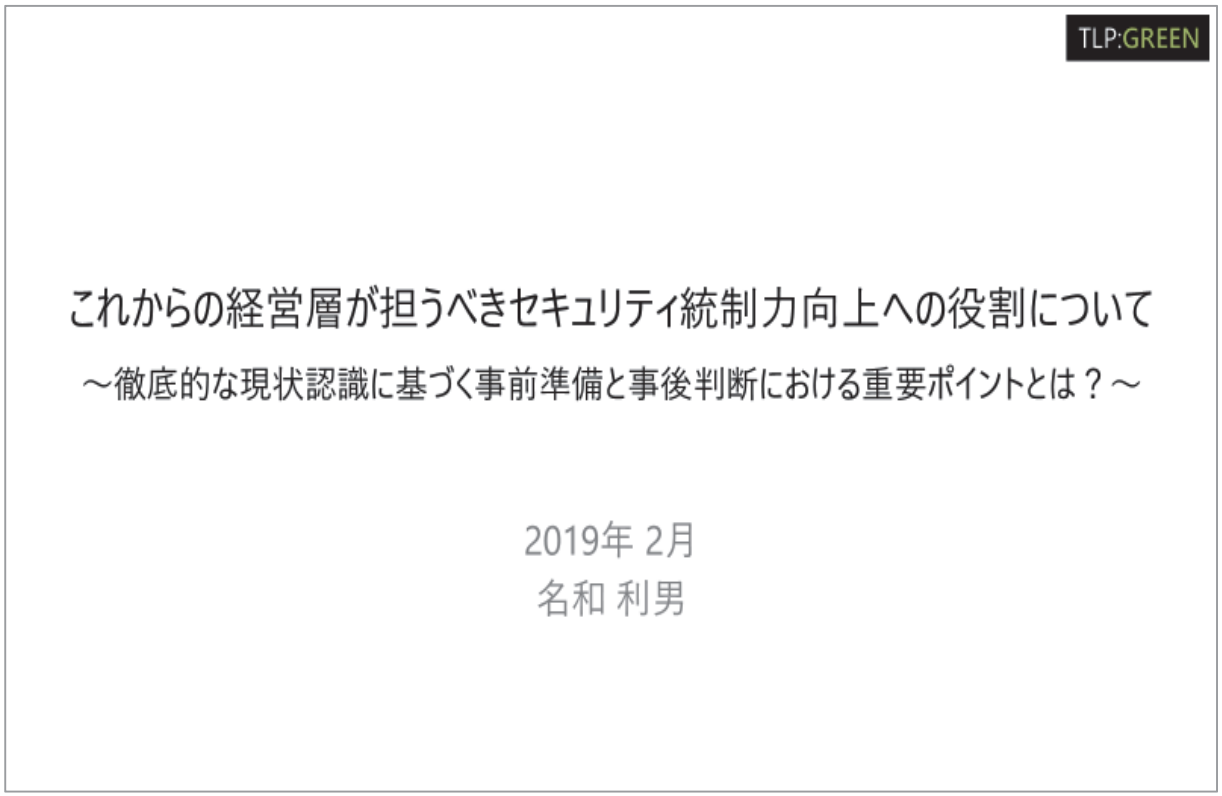
山崎　文明(やまさき　ふみあき)
情報安全保障研究所　首席研究員
メディカルITセキュリティフォーラム理事
サイバーディフェンス研究会　理事
PCISSC PO Japan 連絡会会長/IT-ADRセンター専門委員
システム監査技術者(経済産業省)/医療情報システム監査技術者/医療情報技師
英国規格協会認定BS7799情報セキュリティ・スペシャリスト/CISM
システム監査、ネットワークセキュリティ、セキュリティポリシーに関する専門家。

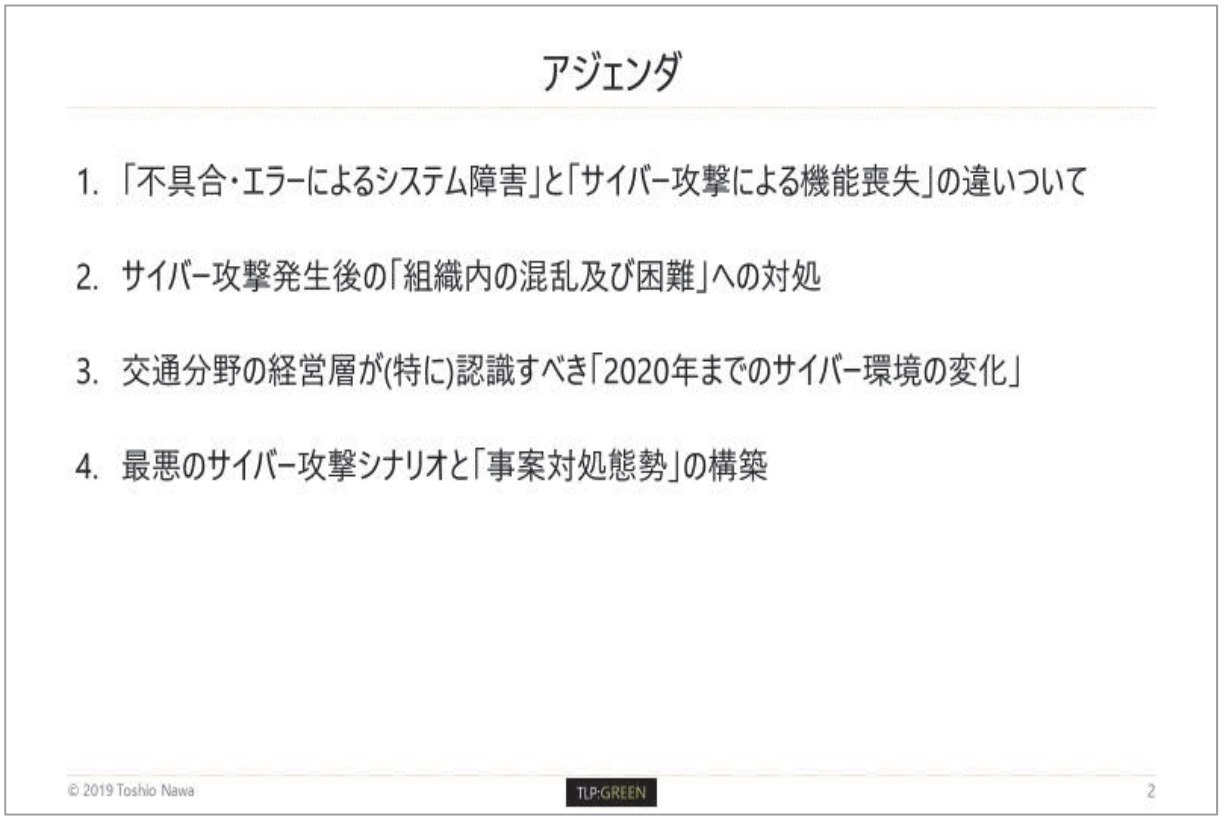
【政府関連委員会委員就任歴】
(現任)文部科学賞　教育情報セキュリティ推進チーム　主査
内閣官房情報セキュリティ社会推進協議会 産学官人材育成WG委員
文部科学省「2020年代に向けた教育の情報化に関する懇談会」スマートスクール構想検討WG委員
内閣官房情報セキュリティセンター　情報セキュリティ社会推進協議会産学官人材育成WG委員
内閣官房　安全保障危機管理室　情報セキュリティ対策推進室WG委員
警察庁不正アクセス犯罪等対策専科講師
学校セキュリティ検討委員会委員
経済産業省サイバーテロ実験評価委員
警察庁不正プログラム調査研究委員会委員
警察庁サイバーセキュリティ調査研究委員会委員　他

【加盟学会】
警察政策学会正会員/日本セキュリティ・マネジメント学会正会員/日本安全保障・危機管理学会正会員
【著書】「情報立国-日本の戦争」(角川新書)「PCIデータセキュリティ基準 完全対策」(日経BP社)、「すべてわかる個人情報保護」(日経BP社)、「情報セキュリティハンドブック」(オーム社)、「情報セキュリティと個人情報保護 完全対策」(日経BP社)、「システム監査の方法」(中央経済社)、「コンティンジェンシー・プランニング」(日経BP社)、「セキュリティマネジメント・ハンドブック」(日刊工業新聞社)等。

ADR: Alternative Dispute Resolution「裁判外紛争解決手続の利用の促進に関する法律」

（４）　これからの経営層が担うべきセキュリティ統制力向上への役割について
～徹底的な現状認識に基づく事前準備と事後判断における重要ポイントとは？～





TLP:GREEN

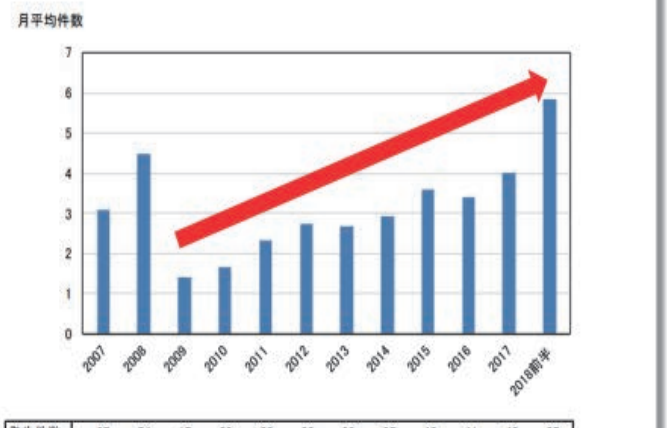
トピック 1

「不具合・エラーによるシステム障害」と「サイバー攻撃による機能喪失」の違いついて

3

システム障害発生の件数は増加傾向

2018 年の前半に報道された障害 35 件の概要は表 1 に示すとおりである。今期の発生件数は月平均 5.8 件と、かなり高い水準である（図 1）。なお、別表 1 は障害の影響範囲が特定の自治体に閉じ、広域にわたる影響はなかったものの、その地域にとっては影響が大きかった事例を取りまとめたものである。



発生件数	37	54	17	20	28	33	32	35	43	41	48	35

出典: IPA 情報システムの障害状況 2018 年前半データ https://www.ipa.go.jp/files/000070130.pdf

TLP:GREEN

4

(10年前から指摘されている)経営層によるシステム(障害)への積極的関与 (1)

連載 2012/10/29 08:00:00
システム障害はなぜ繰り返されるのか?

第1回

システム障害は経営者の責任だ!

重要情報を扱うITシステムを第三者に任せていいの?

ITシステムの開発や運用を子会社やITベンダーといった第三者に任せてしまう(アウトソーシング)企業があるが、本当にそれでよいのだろうか?

日本企業がシステム開発や運用をアウトソーシングしてしまう理由として、IT部門の人材不足を挙げることがよくある。実際、日本のIT部門の人員は少なく、役割はIT企画やプロジェクト管理、運用管理が多く、実際のプログラム開発やアーキテクチャの構築などは行わない。

米国企業はITシステムが経営を左右していることを十分理解しているため、他人に任せるようなことはしない。自分で運転する米国企業と、タクシーに乗って後部座席で行き先を指示している日本企業では大きな差となり、この差が企業競争力、企業価値の差を生んでいるとも言えるのではないだろうか?

https://news.mynavi.jp/article/sysfailure-1/

2009/10/22 00:00
すごい現場

[なぜ繰り返すのか?システム障害] 経営陣がシステムに無関心

https://tech.nikkeibp.co.jp/it/article/COLUMN/20090323/327025/

(10年前から指摘されている)経営層によるシステム(障害)への積極的関与 (2)

2017/09/19 05:00
木村岳史の極言暴論!

「システム障害は絶対に起こしてはならぬ」と叫ぶ馬鹿に付ける薬

「馬鹿に付ける薬はない」ということわざがある。思慮が足らず物事の道理が分からない人は救いようがないとの意味だが、「システム障害は絶対に起こしてはならぬ」と声高に叫ぶような"馬鹿"に付ける薬はないものだろうか。もしそうだとすると本当に困る。この手の主張は、言っている本人が救いようのないだけでは済まされない。こんな論がまかり通っていると、多くの人を不幸にし続けるので、ぜひとも完治させる薬が欲しい。

https://tech.nikkeibp.co.jp/it/atcl/column/14/463805/091400156/

2017.8.10

「経営者」が本気にならないプロジェクトが泥沼化する理由

「システムに欠陥が多すぎて使えない!」
「開発や保守・運用費用が高すぎる!」
「なぜか社員が協力してくれない……」
「経営者がシステムのことを全然わかってない……」

簡単に言えば、「ITシステムの導入によってコスト削減や売上向上に成功し、**会社が利益を増やすことができたとき**」に、初めて成功と言えるわけです。

当然のことと思われるかもしれませんが、そもそもシステムの企画に誤りがあって、**導入しても効果のないシステムを導入したら、いくらQCDを遵守したところで「成功」したことにはなりません。**

逆に、**大幅に納期が遅れたり、不具合のあるシステムだったとしても、経営に貢するならプロジェクトは成功したと言える**のです。

しかし、こういうものの見方や判断、システム担当者レベルは難しいでしょう。

https://diamond.jp/articles/-/137866

(10年前から指摘されている)経営層によるシステム(障害)への積極的関与 (3)

システム障害は、経営層と業務部門の責任

今やITシステムはビジネスの遂行に不可欠なもの。その要件をビジネスサイドの人間がしっかりと考えなければ、ビジネスに役立つシステムなど作れるわけがない。

[@IT情報マネジメント編集部, @IT]

言ってみれば、ITシステムはビジネスそのものであり、テクノロジはビジネスを遂行するための手段に過ぎない。にもかかわらず、多くの場合、システムを使う側が考えるべきことを考えず、システム導入時には不毛な機能比較や価格比較に陥り、障害時には「開発した会社はどこか」といった犯人探しが始まる――本書を読めば、こうした丸投げ体質の異常さを客観的に理解できるのではないだろうか。

なお、本書では事例の分析を基に、「動かないコンピュータ撲滅のための十カ条」と題し、「経営トップが先頭に立ってシステム導入の指揮を執る」「自社のシステム構築に関する力を見極め、無理のない計画を立てる」など、あるべきシステム開発のポイントを詳細にまとめている。事例と合わせて読めば、ビジネスサイドの人、システム関係者、双方にさまざまな気付きをもたらしてくれるはずである。ぜひ手に取ってみてはいかがだろうか。

http://www.itmedia.co.jp/im/articles/1108/09/news106.html

2017/11/30 05:00

システム開発トラブルに見舞われたら…

経営者の思い付きがシステム開発を迷走させる、完成後も問題が多発

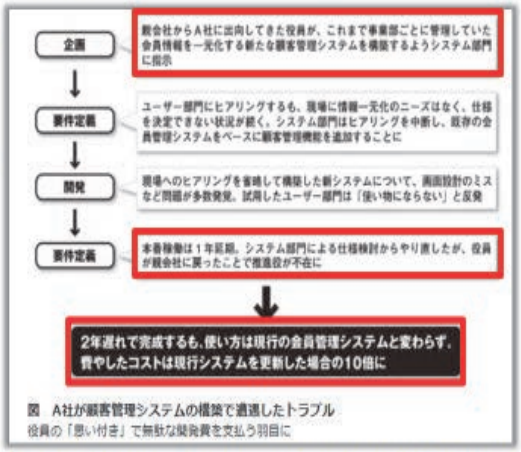


図　A社が顧客管理システムの構築で遭遇したトラブル
役員の「思い付き」で無駄な開発費を支払う羽目に

https://tech.nikkeibp.co.jp/it/atcl/column/17/110600484/110900008/

最近の「サイバー攻撃による機能喪失」の例：2018年5月 デンマークの鉄道会社DSBへのDDoS攻撃

- 2018年5月13日(日曜日)の夜、デンマークの鉄道会社DSB(Danske Statsbaner)がDDoS攻撃を受け、**DSBアプリ、Webサイト、チケット販売機、駅構内のセブンイレブンのキオスクで切符購入ができなくなった**。
  - Rejsekortトラベルカードを持っていた乗客は、列車内の乗務員から切符を購入できたが、約15,000の顧客が影響を受けたと推定。
  - これに対し、DSBの広報担当は、「本事案に関する専門家を迎え入れており、明日の朝までに、すべてのシステムを通常稼働にする」と伝えた。
- このDDoS攻撃の発生と同時に、**内部メールシステムと電話インフラが使用不能**になった。
  - そのため、顧客とコミュニケーションをとる方法は、ソーシャルメディアのみとなった。

https://twitter.com/omDSB/status/995711445454196737

現在、dsb.dkサイト、販売チャネル、交通情報、電話回線に関する技術的な問題が発生しています。私たちはこのエラーを解決するために取り組んでいます。

https://twitter.com/omDSB/status/995898708700123136

dsb.dkサイトへのアクセスエラーが継続して発生していることを認識しました。一部誤解されていますが、私たちはその問題に取り組んでいます。

最近の「サイバー攻撃による機能喪失」の例：
【背景】デンマークにおけるデジタル化とサイバー脅威の高まり

- 2018年、**デンマークは国家戦略「デジタル化のフロントランナーになる」**を発表し、2025年までに約170億円を確保し、デジタル化を推進している。
  - デンマークは、3年連続EU内で最もデジタル化が進んでいる国として有名
- デンマークにおけるデジタル化の特徴
  - 小国(小さいところに多くの要素が集積しているため、アクションを取りやすい)、社会保障国家、民主主義国家であること
  - ビッグデータ(スマートフォンから得られる位置情報や、サーバー上のメール、カード会員情報など、ビジネスに役立てるための膨大で複雑な情報)が集積している
  - オープンイノベーション(自社だけでなく他社や大学、自治体など、外部のテクノロジーやアイデア、ノウハウ、データなどを組み合わせイノベーションを促進していくビジネスモデル)

オープンイノベーションが進展していくと同時に、
攻撃者は、重要インフラ分野で実装された(新しい)技術情報を得やすくなる。

TLP:GREEN

「不具合・エラーによるシステム障害」vs「サイバー攻撃による機能喪失」

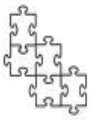
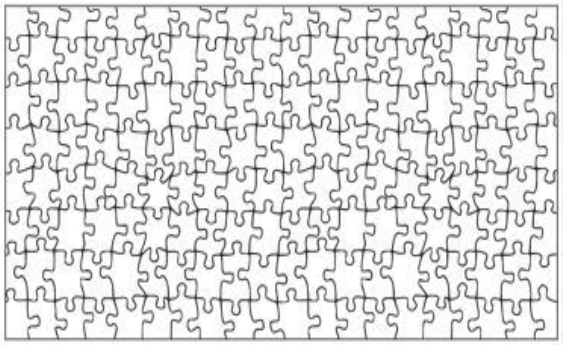
	「不具合・エラーによるシステム障害」	「サイバー攻撃による機能喪失」
経営層の指示	原因究明、早期復旧、再発防止	原因究明、早期復旧、再発防止
インシデントの**特性**	• メカニズムは固定的 • 偶発的に発生 • 原因は(以前から)システム内に存在	• メカニズムは**変動的(第三者が変化させる)** • **第三者の悪意のある活動**により発生 • 原因は**(第三者により)システム外で作られる**
現場に必要な**経験・能力**	• システム及びネットワーク構成に関する知識と設定状況の即時把握(ほぼ固定的) • システムが業務に与える影響(ほぼ固定的)	• システム及びネットワーク構成に関する知識と設定状況の即時把握(ほぼ固定的) • システムが業務に与える影響(ほぼ固定的) • **サイバー攻撃の知識(日々更新する)** • **フォレンジックの知識とリテラシー(日々更新する)** • **セキュリティ対策の知識とリテラシー(日々更新する)** • **説明力及びプレゼンテーション力(相手により変化)**
主な**再発防止策**	• 開発及び保守の体制・プロセスの厳格化	• 開発及び保守の体制・プロセスの厳格化 • **監視強化、サイバー能力構築、連携強化(訓練)等**

TLP:GREEN

「不具合・エラーによるシステム障害」vs「サイバー攻撃による機能喪失」

	「不具合・エラーによるシステム障害」	「サイバー攻撃による機能喪失」
現場に(必然的に)求められる**スキル・能力**	• インターネットのアーキテクチャ、理念、将来像に関する知識 • ネットワークインフラのリテラシーと設計思想の理解 • ネットワークプロトコルの深い理解 • ネットワークアプリケーション、サービス、関連プロトコルの理解	• インターネットのアーキテクチャ、理念、将来像に関する知識 • ネットワークインフラのリテラシーと設計思想の理解 • ネットワークプロトコルの深い理解 • ネットワークアプリケーション、サービス、関連プロトコルの理解 • セキュリティの基本原則 • コンピュータ及びネットワークに対するリスクと脅威の理解 • セキュリティの脆弱性及びそれを利用した攻撃の理解 • ネットワーク及びネットワークのためのセキュリティ対策、及びそれらの問題に関する知識と理解 • 暗号化技術、デジタル署名、ハッシュアルゴリズムの理解 • プログラミング、ネットワークコンポーネント、基本ソフトウェアの理解と経験 • コミュニケーション(対人)能力 • 言語能力 • 作業編成及びスタッフの統率に係る実務能力 • 強い目的意識と不屈の精神

「不具合・エラーによるシステム障害」vs「サイバー攻撃による機能喪失」

	「不具合・エラーによるシステム障害」	「サイバー攻撃による機能喪失」
現場における対処の**難易度**(イメージ)		

「不具合・エラーによるシステム障害」vs「サイバー攻撃による機能喪失」

	「不具合・エラーによるシステム障害」	「サイバー攻撃による機能喪失」
現場が**立ち向かう対象**(イメージ)		

TLP:GREEN

「不具合・エラーによるシステム障害」vs「サイバー攻撃による機能喪失」

	「不具合・エラーによるシステム障害」	「サイバー攻撃による機能喪失」
インシデント対処に**巻き込まれる範囲**(イメージ)		

TLP:GREEN

TLP:GREEN

トピック 2

サイバー攻撃発生後の「組織内の混乱及び困難」への対処

15

経営層が持つべき「サイバー攻撃による機能喪失」に備えた心構え

- 企業内のそれぞれの部門は、**ICTへの依存や認識・理解の違い、所掌や責任範囲の割り当ての偏り**などが大きい。
  - サイバー攻撃発生時における迅速かつ円滑な対処を実現するには、部門間の相互理解を前提とした緊密連携(阿吽の呼吸)が必要になってくる。
- 「サイバー攻撃による機能喪失」の事態において、経営層(強い権限を持つリーダー)による陣頭指揮が不在である場合、**部門間のコンフリクトに起因した混乱や困難が発生**することが多い。
  - 深刻な被害を発生させたサイバー攻撃を経験した組織の経営層は、事前の心構え(態勢)やセキュリティ対策の不足よりも、インシデント発生直後の部門間の対処行動の不整合による(机上で見積もった計画)の遅延の繰り返しに苛立ちを感じる。
- 一般的に、経営層はサイバー攻撃に対してテクニカルな対処を主導することは難しいと言われている。しかし、対処活動を妨げるような**部門間のコンフリクトに起因した混乱や困難を解決する権限や能力を有している。**
  - リスクアセスメントで得られた脅威シナリオに基づいた訓練を、経営層を巻き込んで実施すべきである。

TLP:GREEN

16

TLP:GREEN

トピック 3

交通分野の経営層が(特に)認識すべき「2020年までのサイバー環境の変化」

17

今後の日本における**サイバー環境(Cyber Environment)**の変化

【テクノロジー】

- **USBグッズ**のオフィス利用
- ノートPCの**SSD**採用率の増加
- **ビジネスチャット**の利用拡大
- **RCS準拠**のメッセージングサービスの増加
- **キャッシュレス**取引の拡大
- **4K 8Kテレビ**放送の開始
- PSTNから**IP網への移行**
- 高速通信規格**5G**の導入
- 新たな**IoT用無線通信サービス**(LPWA等)
- 次世代無線規格 **Wi-Fi 6**

【Deep Web】

- **オンラインゲーム上のチャット**で闇取引
- オルトコイン情報の流通基盤(**Telegram**)

【対策】

- **CASB**(クラウドセキュリティ)
- EPP/**EDR**(エンドポイントセキュリティ)
- **カード決済のIC対応**(改正割賦販売法)
- **サプライチェーンリスク**の対策(SP800-171)
- **有給休暇**の義務化(働き方改革関連法)

【ビジネス等】

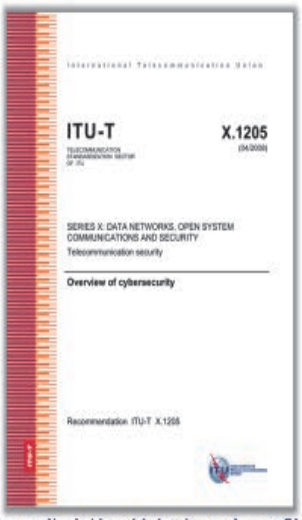
- 少子高齢化に伴う**労働人口の急減**
- ERAB/**ネガワット取引**
- 「**全銀EDIシステム**」の稼働
- **OTT事業**(スポーツ等)の拡大
- 「**スポーツホスピタリティ**」の開始
- **外国人受け入れ**拡大(出入国管理法改正)
- **水道民営化**(水道法改正)

TLP:GREEN

18

【参考】サイバー環境(Cyber Environment)とは

- サイバー環境(Cyber Environment)には、次の構成要素があると定義されている。
  - ユーザー
  - ネットワーク
  - デバイス
  - 全てのソフトウェア
  - プロセス
  - ストレージ(記憶媒体)或いは経路上の情報
  - アプリーション(特定の作業や業務を目的として基本ソフトウェア上で動作するソフトウェア)
  - ネットワークに直接的及び間接的に接続されることのあるシステム



https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1205-200804-I!!PDF-E&type=items

TLP:GREEN

交通分野の経営層が(特に)認識すべき「2020年までのサイバー環境の変化」

【テクノロジー】
- USBグッズのオフィス利用
- ノートPCのSSD採用率の増加
- ビジネスチャットの利用拡大
- RCS準拠のメッセージングサービスの増加
- キャッシュレス取引の拡大
- 4K 8Kテレビ放送の開始
- PSTNからIP網への移行
- 高速通信規格5Gの導入
- 新たなIoT用無線通信サービス(LPWA等)
- 次世代無線規格 Wi-Fi 6

【Deep Web】
- オンラインゲーム上のチャットで闇取引
- オルトコイン情報の流通基盤(Telegram)

【対策】
- CASB(クラウドセキュリティ)
- EPP/EDR(エンドポイントセキュリティ)
- カード決済のIC対応(改正割賦販売法)
- サプライチェーンリスクの対策(SP800-171)
- 有給休暇の義務化(働き方改革関連法)

【ビジネス等】
- 少子高齢化に伴う労働人口の急減
- ERAB/ネガワット取引
- 「全銀EDIシステム」の稼働
- OTT事業(スポーツ等)の拡大
- 「スポーツホスピタリティ」の開始
- 外国人受け入れ拡大(出入国管理法改正)
- 水道民営化(水道法改正)

TLP:GREEN

TLP:GREEN

トピック 4

最悪のサイバー攻撃シナリオと「事案対処態勢」の構築

21

最悪のサイバー攻撃(事案)シナリオの例

- 「USBグッズのオフィス利用」
  - BadUSBによるデータ破壊を利用した誘導工作
- 「ノートPCのSSD採用率の増加」+「次世代無線規格 Wi-Fi 6」
  - 痕跡及びログの不足によるインシデントの原因究明の困難化
- 「少子高齢化に伴う労働人口の急減」+「外国人受け入れ拡大(出入国管理法改正)」
  - 不十分な個人信頼性確認のまま採用した経験の浅い技術者の早期退職による内部情報流出
  - メーカー技術者の常駐困難化により(徐々に)利用が始まる(セキュリティレベルの低い)リモート保守への攻撃
- 「4K 8Kテレビ放送の開始」
  - PTP(高精度時間プロトコル)の周波数ソースGPS/GNSSに対するタイムスプーフィング攻撃
- 「サプライチェーンリスクの対策(SP800-171)」
  - 制御システムの周辺システム(自動消火、警備、ビル管理、防災等)に対するソフトウェアサプライチェーン攻撃
- 「水道民営化(水道法改正)」
  - 浄水場の遠隔監視システムのアカウントハイジャックや中間者攻撃による毒物投入

TLP:GREEN

22

「情報セキュリティ体制」と「事案対処態勢」の違い

- 「情報セキュリティ体制」は管理策(Security Control)に基づいた各担当者の役割分担を重要視するが、**「事案対処態勢」は想定事案に相応する対処行動及びその能力維持を重要視**する。

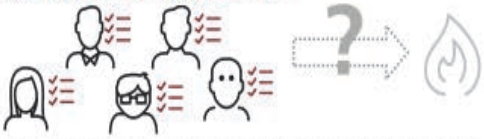
❖ 「態勢」と「体制」は、***取るべき準備行動*** が大きく異なる。

– 態勢: 事態に対処するための準備ができている状態のこと。（前もっての身構え）

本当に事態対処できるかどうかが重要

– 体制: 基本原理・方針によって秩序づけられている組織のこと。（政治支配の様式）

組織内の役割分担（責任所在）が重要



TLP:GREEN

「事案対処態勢」の構築のための重要ポイント (1)

- 全ての関係者が、**徹底的な状況認識(Situation Awareness)**を行うこと。

- インシデント発生時においてやり取りする**相手の顔**が見える
- やり取りにおいて必要となる**認識・教養の統一化**を図ることができる
- インシデントハンドリングの流れや**規定等の改善**を図ることができる
- **上層部の考え方**を把握することができる
- **発生した事例**を把握することができる

- 連絡先の**疎通確認**をすることができる(異動等による疎通不能の回避)
- サイバー脅威の**変動状況**に(ある程度)追いつくことができる
- メンバー間の**一体感**を感じることができる
- 潜在化した可能性のあるイベント(事象)を検知する**トリガー**となる
- **教養不足を補う**ことができる

TLP:GREEN

「事案対処態勢」の構築のための重要ポイント (2)

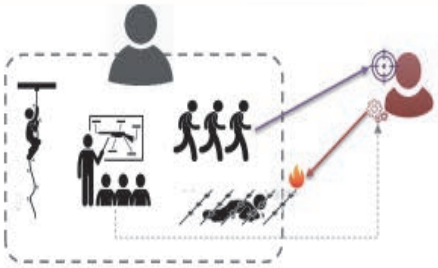
- 専任されたチームが、**検知(Detect)⇒トリアージ(Triage)⇒対処行動(Respond)**の各プロセスを確立及び実務能力の構築を行うこと。
  - 「人間の行動原理(認知⇒判断⇒動作)」をベースにして、「組織／単一分野」及び「複数分野」における**各フェーズ(認知検知⇒意思決定⇒対処)で実施される行動**を特定した上で、それを実現可能にする**能力スキルや情報・知見(ノウハウ)等**を見出し、実施可能な状況にしておくこと。

TLP:GREEN

「事案対処態勢」の継続強化ためのアクションアイテム

- 状況認識(Situation Awareness)の共有や向上のために、サイバーセキュリティ事案への対処態勢関係者による定例会及び外部の専門家を招聘した**勉強会**を実施。
- 連絡体制の維持のために、定期的な**疎通確認訓練**(Communication Check Drill)或いは**電話会議**(Teleconference)を実施。
- 意思決定能力の向上及び最新の脅威動向の把握のために、脅威シナリオをベースにした**TTX**(Table Top Exercise; 机上演習)を実施。

- メンバー間の**関係性強化**を図ることができる
- 教養に加え、**(擬似)経験**を積み上げることができる
- メンバー間で流通する情報に対する**関心が向上**する
- インシデントハンドリングや規定等の**具体的な改善点**を見出せる
- 全般的なインシデント対応に係る**時間を短縮**できる



TLP:GREEN

第８章.　　まとめと今後の課題

８．１．まとめ

高度化、複雑化するサイバー攻撃に対応するためには、全社一丸となって各種対策に取り組む必要がある。このためには、サイバー攻撃の最前線で業務に従事する現場担当者、サイバー攻撃対策を主導するCSIRT要員、予算、及び要員確保とサイバー攻撃発生時の意思決定を担う経営層の役割が重要となる。このことから、今年度の調査研究においては、経営層セミナー、CSIRT 要員を対象とする机上演習、現場担当者向けの教材作成とそれを用いた教育の試行を実施した。

サイバーセキュリティ人材の育成は、各交通事業者の実態に応じて実施していくことになるが、鉄道分野及び航空分野において、事業部門のシステムの維持管理を担う担当者に向けた人材育成教材として提供されているものは存在していない。このため、本研究では、昨年度の研究成果であるカリキュラムをもとに、事業者各々でサイバーセキュリティ人材を育成するために参考となる教材を作成した。

育成対象の人材像は、次のとおりである。

- インシデント発生の際、その原因がサイバー攻撃である疑いを考慮し、適切に対応できる人材
- サイバー攻撃に対処（原因究明、復旧など）する専門機関と連携して、インシデント対応を実行（支援）できる人材

必要となる能力は、次のとおりである。

- サイバー攻撃に関わるインシデント対応に関する能力
- 上記に関わる情報技術（IT）に関する能力

（１）　教材の作成

昨年度の研究成果であるカリキュラムを基に、人材育成を実施するための教材として、第１回（サイバー攻撃の現状）から第９回（振り返り）までの各講座において使用する教材と講師用の指導要領を作成した。教材の作成に際しては、机上演習の結果を参考にした。

（２）　教育の試行

（１）の結果を踏まえ、鉄道分野及び航空分野について教育の試行を実施した。教育の実施は各交通事業者に委ねられることになるため、教育の立案あるいは講師となる方を受講対象として実施した。

（３）　教材見直し方針の提示

本研究において作成した教材は、交通事業者において汎用的に使用することを目的としているため、交通事業者各々で、学習内容を取捨選択することを推奨している。このため、本研究にて得られた知見をもとに、各交通事業者が実施する教材見直し方針を提示した。

（４）　経営層セミナーの実施

昨今のサイバー攻撃の脅威の増大に伴い、サイバー攻撃に対応するための人材育成の必要性についての経営層の理解は深まっていると考えられる。しかしながら、日々高度化、複雑化するサイバ

ー攻撃の脅威に対応するためには、自社における投資をどうするかの経営判断とともに、サイバー攻撃が発生した際における強いリーダーシップが求められる。このため、経営層への啓蒙が重要であると考える。

８．２．今後の課題

サイバー攻撃は日々巧妙化され、今後も新たな手法を用いた攻撃が行われることが予想される。このような観点から、より効果的にサイバーセキュリティ対策を進めるための課題を以下に示す。

（１）　教材の活用

サイバー攻撃の事例等については、最新のものに更新することが望まれる。例えば、第１回の講座においてサイバー攻撃事例を紹介しているが、最新の動向を踏まえたものに差し替えることが望まれる。このため、教材の更新をどのように実施するかが課題となる。鉄道、航空の違いで得られる知見を教材／カリキュラムにフィードバックさせ、より活用し易い教材に更新していくことが望まれる。

（２）　教育・訓練の実施

本研究では、主に講義形式を念頭に教材を作成したが、適宜グループディスカッション等を取り入れたプログラムとすることが望まれる。このため、教育・訓練の実施の際には、グループディスカッション等をどのように取り入れるかが課題となる。

（３）　クラウドサービス利用への対応

鉄道分野、航空分野とも、クラウドサービスの利活用への対応が必要となってきている。このため、クラウドサービス利用におけるサイバーセキュリティ対策について、どのように教材に取り入れるかが課題となる。

（４）　現場担当者の負荷軽減

サイバー攻撃手法は、年々高度化・巧妙化している。その一方で、システムは複雑化し、サプライチェーンの対策も含め、対応が広範化している。このため、現場担当者の守備範囲が広範になってきており負荷が増大している。インシデントが発生した際にはより優先度の高いシステムの防衛に特化する等、現場担当者の負荷軽減策が課題となる。

（５）　人材育成対象の拡大

本研究では、事業部門のシステムの維持管理を担う担当者に向けた教材を作成したが、これ以外にも、例えばシステムの開発担当者、調達担当者等、サイバー攻撃対応の際に関係する要員についても教育が必要である。このため、システム維持管理者以外の対象者向け教育をどのように実施するかが課題となる。

おわりに

この報告書は、運輸総合研究所が日本財団助成事業として実施した調査研究「交通分野へのサイバー攻撃に対するセキュリティ人材育成に関する調査研究」の成果をまとめたものである。

この研究は、2020 年に開催される東京オリンピック・パラリンピックを念頭にサイバー攻撃やサイバーテロ対策を進める上で必要となる人材を育成することを目指し、その際の参考となる教育ツールを研究することを大きな目的としている。調査対象は「鉄道分野」と「航空分野」を主な対象とした。

運輸総合研究所では、平成 27 年度からの 2 年間で「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」が実施され、交通事業のセキュリティリスク分析を踏まえ、国内外の対策ガイドラインなどの整理、及び、それらに基づいて、我が国に適応した鉄道分野と航空分野の対策手引きの作成を行った。

昨年度は、作成した対策手引きを実践する人材を育成することを目指し、必要となる人材像や育成対象者の検討、学習内容の定義、国内外の人材育成カリキュラムの事例収集、机上演習の実施、及び、それらに基づいて、我が国に適応した鉄道分野と航空分野の人材育成カリキュラムの作成を行った。

本年度は、作成した人材育成カリキュラムを実行する上での教材の具体化を目指し、机上演習の実施、及び、鉄道分野と航空分野の教育用教材作成とそれを用いた教育の試行を行った。

活動は、昨年と同様、検討委員会に事務局が案を提示しそれを議論して修正や追加方向を固め、それに基づいて事務局と研究実施主体とが活動を進めるという形を取った。また、事務局として一般財団法人運輸総合研究所、実施主体として一般社団法人日本生活問題研究所が協力して検討を重ねた。

本調査研究で作成した教材は、国内外のカリキュラム事例や、実施した机上演習と教育の試行結果を踏まえ、なるべく関係事業者の実態に即したものとなることを目指した。各事業者には、サイバー攻撃の脅威が身近に迫りつつあるとの認識を持ち、本教材を参考に、自社のシステムや管理の状況を踏まえ、人材育成を進めていただくことを期待したい。

最後に、この報告書をまとめるにあたり、活動を支援頂いた日本財団と、ご協力いただいた多くの方々に感謝を申し上げる。

平成 31 年 3 月

「鉄道/航空分野のサイバー攻撃に対するセキュリティ人材育成に関する調査研究」
検討委員会　委員長
田中　英彦

本調査研究にあたっての参考資料

1) 鉄道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、運輸総合研究所
2) 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、運輸総合研究所
3) 重大な経営課題となる制御システムのセキュリティリスク、IPA
https://www.ipa.go.jp/files/000044733.pdf
4) インシデント対応報告レポート JPCERT/CC
https://www.jpcert.or.jp/ir/report.html
5) 情報セキュリティ読本 教育用プレゼン資料、IPA
https://www.ipa.go.jp/security/publications/dokuhon/ppt.html
6) 脆弱性対策情報データベース、JVN iPedia
http://jvndb.jvn.jp/index.html
7) 「制御システム情報セキュリティ人材の育成に関する調査及びモデルカリキュラム作成」報告書について、IPA
https://www.ipa.go.jp/security/fy24/reports/jinzai/index.html
8) 制御システムにおけるセキュリティマネジメントシステムの構築に向けて ～ IEC62443-2-1 の活用のアプローチ ～、IPA
https://www.ipa.go.jp/files/000014265.pdf
9) 制御システムの セキュリティリスク分析ガイド、IPA (3～5)
https://www.ipa.go.jp/files/000061925.pdf
10) OSS モデルカリキュラム V2 ネットワークアーキテクチャに関する知識(基礎レベル)、IPA
https://www.ipa.go.jp/software/open/ossc/oss_jinzai/curriculum_v2.html
11) インシデントハンドリングマニュアル、JPCERT/CC
https://www.jpcert.or.jp/csirt_material/files/manual_ver1.0_20151126.pdf
12) サイバーセキュリティ経営ガイドライン Ver.2.0 付録 C インシデント発生時に組織内で整理しておくべき事項、IPA
http://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_app_C.xlsx
13) サイバーセキュリティ経営ガイドライン 解説書 Ver.1.0、IPA
https://www.ipa.go.jp/files/000056148.pdf
14) サイバーセキュリティ経営ガイドライン Ver.2.0,IPA
http://www.meti.go.jp/press/2017/11/20171116003/20171116003-1.pdf
15) 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第 3 版、国土交通省 (1～8)
http://www.mlit.go.jp/common/001127563.pdf
16) 航空運送事業者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 第 4 版、国土交通省 http://www.mlit.go.jp/common/001127526.pdf
17) 空港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 第 1 版、国土交通省
http://www.mlit.go.jp/common/001229687.pdf
18) Rail Cyber Security Strategy, Rail Delivery Group (1～3)
https://www.raildeliverygroup.com/component/arkhive/?task=file.download&id=469772253

19) Cybersecurity For Rail: Not A Single-Shot Approach, THALES Ground Transportation
https://www.thalesgroup.com/sites/default/files/database/d7/asset/document/cyber_security_whitepaper_hires_0.pdf
20) Aviation Cyber Security Toolkit, IATA
http://www.iata.org/publications/store/Pages/aviation-cyber-security-toolkit.aspx
21) 重要インフラに対するサイバー攻撃の実態と分析、NEC
https://jpn.nec.com/techrep/journal/g17/n02/pdf/170204.pdf
22) Malware Statistics、AV-TEST
https://www.av-test.org/en/statistics/malware/
23) サイバー犯罪とサイバー戦争の違いとは、トレンドマイクロ
http://blog.trendmicro.co.jp/archives/7025
24) マルウェアとウイルス、違いは何ですか？、EMSI-SOFT
https://emsisoft.jp/faq/faq013/
25) スウェーデンの交通機関が DDoS 攻撃を受け運航不能に陥る、The ZERO/ONE
https://the01.jp/p0005941/
26) 情報セキュリティ 10 大脅威 2018、IPA
https://www.ipa.go.jp/security/vuln/10threats2018.html
27) 3-1-基. ネットワークアーキテクチャに関する知識、IPA
https://www.ipa.go.jp/files/000056028.pdf
28) セキュリティ対応組織（SOC/CSIRT)強化に向けたサイバーセキュリティ情報共有の「 5W1H 」第 1.0 版
http://isog-j.org/output/2017/5W1H-Cyber_Threat_Information_Sharing_v1.html
29) 今、現場で求められる Fast Forensics
https://digitalforensic.jp/wp-content/uploads/2014/06/66396c87002dedfdb1d230e7db8f891a.pdf
30) 「証拠保全ガイドライン 第 6 版」、デジタルフォレンジック研究会
https://digitalforensic.jp/wp-content/uploads/2017/05/idf-guideline-6-20170509.pdf
31) 初動対応とファストフォレンジック、デジタルフォレンジック研究会「技術」分科会（5)
https://digitalforensic.jp/wp-content/uploads/2018/02/tech-14-4-resume.pdf
32) サイバーセキュリティ経営ガイドライン　付録 C インシデント発生時に組織内で整理しておくべき事項、経済産業省
http://www.meti.go.jp/policy/netsecurity/mng_guide.html
33) サイバー攻撃の動向とインシデント対応の状況、JPCERT コーディネーションセンターNISC
http://www.nisc.go.jp/security-site/files/presen2-2.pdf
34) インシデント対応マニュアルの作成について、JPCERT コーディネーションセンター
https://www.jpcert.or.jp/csirt_material/files/18_incident_response_manual_20151126.pdf
35) 多要素認証の種類と方法、GMO/SKUID

https://sku.id/catalog/skuid_whitepaper02.pdf
36) EDR とは何か、Cybereason
https://www.cybereason.co.jp/blog/edr/2224/
37) サイバーセキュリティ 2018. NISC
https://www.nisc.go.jp/active/kihon/pdf/cs2018.pdf
38) 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、NISC
https://www.nisc.go.jp/active/infra/pdf/infra_rt4_r1.pdf
39) 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（第５版)、NISC
https://www.nisc.go.jp/active/infra/pdf/shishin5.pdf
40) 重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書（第１版)、NISC
https://www.nisc.go.jp/active/infra/files/tebikisho.zip
41) Framework for Improving Critical Infrastructure Cybersecurity Version 1.1
National Institute of Standards and Technology April 16, 2018
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
42) 重要インフラ等で利用される IoT 機器の調査、総務省
http://www.soumu.go.jp/main_content/000561906.pdf
43) すぐわかる！DNS のしくみ
http://xn--u8j7eobcu7j2kyg7f.jp/special/dns/page_02.html
44) Insecam https://www.insecam.org/
45) 制御システムのセキュリティリスク分析ガイド ～詳細リスク分析手法の解説と分析結果の活用～、IPA
https://www.ipa.go.jp/files/000067954.pdf
46) 制御システムのセキュリティリスク分析ガイド ～セキュリティ対策におけるリスク分析実施のススメ～、IPA
https://www.ipa.go.jp/files/000063124.pdf
47) クラウドセキュリティガイドライン 活用ガイドブック、経産省
http://www.meti.go.jp/policy/netsecurity/downloadfiles/cloudseckatsuyou2013fy.pdf
48) 実践クラウドセキュリティ、情報科学専門学校
http://isc.iwasaki.ac.jp/monka_itaku/cloudsecurity_kyokasyo_A4.pdf
49) 国民のための情報セキュリティサイト、総務省
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/basic/structure/02.html
50) 情報セキュリティ読本 教育用プレゼン資料-第３章 見えない脅威とその対策 -個人レベルのセキュリティ対策-、IPA https://www.ipa.go.jp/files/000015329.ppt
51) 国内標的型サイバー攻撃分析レポート 2018 年版～「正規」を隠れ蓑にする攻撃者～、トレンドマイクロ
https://resources.trendmicro.com/jp-docdownload-form-m077-sem-apt-2018.html?gclid=CjwKCAjw14rbBRB3EiwAKeoG_6Jlh54vh2itVyDh0bovHDpH5FkKHDD2Q2amIEPD-XzG9oJUGMi3PxoC05cQAvD_BwE

52) ScanNetSecurity 脆弱性と脅威 脅威動向ニュース記事一覧、IID
https://scan.netsecurity.ne.jp/category/threat/threat/latest/
53) ScanNetSecurity 脆弱性と脅威 セキュリティホール・脆弱性ニュース記事一覧、IID
https://scan.netsecurity.ne.jp/category/threat/vulnerability/latest/
54) クラウドサービス提供における情報セキュリティ対策ガイドライン、総務省
http://www.soumu.go.jp/main_content/000283647.pdf
55) クラウドサービス提供における情報セキュリティ対策ガイドライン（第2版)、総務省
http://www.soumu.go.jp/main_content/000566969.pdf
56) ATI Cloud、SITA
https://www.sita.aero/solutions-and-services/ati-cloud
57) クラウド型輸送計画作成システム、東芝
https://www.toshiba.co.jp/tech/review/2013/04/68_04pdf/a04.pdf
58) 事例：埼玉高速鉄道様、東芝
https://www.toshiba-sol.co.jp/casestudy/articles/s-rail_01.htm

用語の定義

本調査研究において提示する用語の定義を以下に示す。

(1) **「重要インフラ」**とは、他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び社会経済活動の基盤であり、その機能が停止、低下又は利用不可能な状態に陥った場合に、わが国の国民生活又は社会経済活動に多大なる影響を及ぼす恐れが生じるものをいう。第４次行動計画では、「情報通信」、「金融」、「航空」、「空港」、「鉄道」、「電力」、「ガス」、「政府・行政サービス（地方公共団体を含む）」、「医療」、「水道」、「物流」、「化学」、「クレジット」及び「石油」の 14 分野をいう。

(2) **「サイバー攻撃」**とは、システムに対する悪意ある電子的攻撃をいう。本カリキュラムでは、ネットワークを介した外部からの攻撃の他、施設内部への物理的な侵入による攻撃や内部不正も含む。

(3) **「サイバーセキュリティ」**とは、サイバー攻撃により、期待されていた情報システム等の機能が果たされないといった不具合が生じないように安全に守られていることをいう。

(4) **「IoT」**とは、Internet of Things の略を指す。多様な「モノ」が通信機能をもち、ネットワークに接続して動作する仕組みをいう。

(5) **「サイバーテロ」**とは、インターネット等のコンピュータネットワーク上で行われる大規模な破壊活動。政治的な示威行為として行われるもので、人に危害を加えたり、社会機能に打撃を与えたりするような、深刻かつ悪質なものをいう。

(6) **「クローズドシステム」**とは、インターネット等に直接は繋がれておらず、限られた利用者や地点の間のみを接続する広域通信ネットワークで構成されたシステムをいう。

(7) **「CSIRT」**とは、Computer Security Incident Response Team の略で、セキュリティインシデント等サイバーセキュリティに関するトラブルに対処するための体制をいう。

(8) **「セキュリティベンダー」**とは、セキュリティ対策ソフトウェアや関連サービスを開発・提供している事業者のことをいう。例えば、システム開発、システム構築、あるいは調査・分析等を行う事業者も該当する。

(9) **「ランサムウェア」**とは、「Ransom（身代金）」と「Software（ソフトウェア）」を組み合わせた造語である。コンピュータのファイルを暗号化する等特定の制限をかけ、その制限の解除と引き換えに金銭を要求する。

(10) **「ファイルレス攻撃」**とは、コンピュータのメモリ空間等で不正なコードを実行する攻撃手法のことをいう。

(11) **「机上演習」**とは、本カリキュラムにおいては、サイバー攻撃を想定したシナリオに沿ってインシデント対応のシミュレーションを行う演習をいう。

(12) **「情報セキュリティ」**とは、情報の機密性、完全性、可用性の維持をいう。

(13) **「サプライチェーン攻撃」**とは、ソフトウェアやハードウェアの製造過程で製品にマルウェアを感染させる攻撃のことをいう。

(14) **「DDoS 攻撃」**とは、ネットワーク上に分散する大量のコンピュータが特定のネットワークやシステムに対して一斉に要求等を送出し、通信容量やシステムの能力を超えて機能を停止させてしまう攻撃をいう。

(15) **「ネットワーク機器」**とは、IT 技術を使って通信を中継する機器をいう。

(16)**「脆弱性」**とは、ソフトウェアやアプリケーション等において、システムへの不正アクセスやマルウェア等の攻撃により、その機能や性能を損なう原因となり得るセキュリティ上の問題箇所をいう。

(17)**「マルウェア」**とは、不正かつ有害な動作を行う意図で作成された悪意のあるソフトウェアや悪質なコードの総称をいう。

(18)**「不正侵入」**とは、通信回線・ネットワークを通じてコンピュータに接触し、本来の権限では認められていない操作を行ったり、本来触れることの許されていない情報の取得や改ざん、消去等を行ったりすることをいう。

(19)**「中間者攻撃」**とは、暗号通信を盗聴したり介入したりする手法の一つ。通信を行う二者の間に割り込んで、両者が交換する公開情報を自分のものとすりかえることにより、気付かれることなく盗聴したり、通信内容に介入したりする手法をいう。

(20)**「ゼロデイ攻撃」**とは、ソフトウェアにセキュリティ上の脆弱性(セキュリティホール)が発見されたときに、問題の存在自体が広く公表される前にその脆弱性を悪用して行われる攻撃をいう。

(21)**「リスク」**とは、発生する可能性のある損害をいう。サイバーセキュリティに対するリスクとは、サイバー攻撃を原因として発生する可能性のある損害をいう。

(22)**「資産」**とは、本カリキュラムにおいては IT 資産をいう。主にハードウェア、ソフトウェア、ライセンスに分類される。

(23)**「リスク評価」**とは、リスクの重大さを決定するために、算定されたリスクを与えられたリスク基準と比較するプロセスをいう。

(24)**「クラウド」**とは、コンピュータネットワークを経由して、コンピュータ資源をサービスの形で提供する利用形態のことをいう。

(25)**「OSI 参照モデル」**とは、国際標準化機構(ISO)により制定された、異機種間のデータ通信を実現するためのネットワーク構造の設計方針「OSI」に基づき、コンピュータ等の通信機器の持つべき機能を階層構造に分割したモデルをいう。

(26)**「プロコトル」**とは、手順、手続き、外交儀礼、議定書、協定等の意味を持つ英単語。通信におけるプロトコルとは、複数の主体が滞りなく信号やデータ、情報を相互に伝送できるよう、あらかじめ決められた約束事や手順の集合のことをいう。

(27)**「LAN」**とは、限られた範囲内にあるコンピュータや通信機器、情報機器等をケーブルや無線電波等で接続し、相互にデータ通信できるようにしたネットワークのこと。概ね室内あるいは建物内程度の広さで構築されるものを指す。

(28)**「WAN」**とは、地理的に離れた地点間を結ぶ通信ネットワークのこと。建物内や敷地(キャンパス)内を結ぶ LAN(Local Area Network)と対比される用語。

(29)**「ネットワーク層」**とは、通信プロトコル(通信手順/通信規約)の機能や役割を階層構造で整理したモデルを構成する層の一つで、単一の、あるいは相互接続された複合的なネットワークの上で末端から末端までデータを送り届ける役割を担うものをいう。

(30)**「トランスポート層」**とは、通信プロトコル(通信手順/通信規約)の機能や役割を階層構造で整理したモデルを構成する層の一つで、データの送信元と送信先の間での制御や通知、交渉等を担うものをいう。

(31)**「スイッチ」**とは、受信した信号から宛先等を解析して必要な機器にのみ転送する機能をもった装置のことをいう。

(32)**「ルーター」**とは、コンピュータネットワークの中継・転送機器の一つで、データの転送経路を選択・制御する機能を持ち、複数の異なるネットワーク間の接続・中継に用いられるものをいう。

(33)**「アクセスポイント」**とは、通信ネットワークの末端でコンピュータ等からの接続要求を受け付け、ネットワークへの通信を仲介する施設や機器のことをいう。

(34)**「IoT 機器」**とは、IT 機器以外のインターネットに接続されたあらゆる機器をいう。

(35)**「SIEM」**とは、Security Information and Event Management の略で、サーバー、ネットワーク、セキュリティ等の機器、ツールや各種アプリケーションから集められたログ情報に基づいて、異常があった場合に管理者に通知する仕組みをいう。

(36)**「EDR」**とは、Endpoint Detection and Response の略で、エンドポイントの情報（インストールされているアプリケーション、ログ、起動プロセス等）を収集し、不正な挙動の検知及びマルウェアに感染した後の対応を迅速に行うツールをいう。

(37)**「ハードニング」**とは、コンピュータの脆弱性を解消することで、セキュリティ的により堅牢なものにすることをいう。

(38)**「データダイオード」**とは、ハードウェアで片方向通信のみ可能にするよう工夫された特殊なファイアウォールをいう。

(39)**「多層防御」**とは、１つの手段だけでなく分散して多層に防御するという考え方をいう。

(40)**「フォレンジック」**とは、セキュリティインシデントや法的紛争・訴訟に際し、電磁的記録の証拠保全及び調査・分析、及び電磁的記録の改ざん・毀損等についての分析・情報収集等を行う調査手法・技術をいう。

(41)**「ファスト・フォレンジック」**とは、インシデント発生時において、早急な原因究明や侵入経路の解明等を目的として、最低限のデータを短期間で解析するフォレンジックの技法あるいは考え方をいう。

(42)**「ログ」**とは、コンピュータや通信機器が一定の処理を実行したこと（または実行できなかったこと）を記録したデータを指す。

(43)**「外部記憶媒体」**とは、コンピュータシステムに接続してそのデータを保存するための可搬型の装置をいう。

(44)**「権限」**とは、職務や職責に応じて正当に与えられた行為や能力、またその範囲をいう。

(45)**「セキュリティパッチ」**とは、セキュリティ脆弱性等の不具合を解消するためのプログラムをいう。

(46)**「セキュリティインシデント」**とは、意図的なサイバー攻撃により、鉄道運行の遅延、運休、及び鉄道の安全輸送に対する支障等の影響を及ぼす、又はその恐れのあるシステムの不具合が発生した事象をいう。

(47)**「ベンダー」**とは、英語で「売り手」を意味し、IT 用語としては製品やシステム、サービスの提供を行っている事業者を全般的に指す。

(48)**「サイバー・フィジカル・システム」**とは、実世界（フィジカル空間）にある多様なデータをセンサーネットワーク等で収集し、サイバー空間で大規模データ処理技術等を駆使して分析／知識化を行い、活用を図るシステムをいう。