サイバー攻撃に対する人材育成に関する
調査研究
報告書

平成 30 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 29 年度日本財団助成事業として実施した「サイバー攻撃に対するセキュリティ情報共有組織（ISAC）の構築、人材育成に関する調査研究」の成果の内、「サイバー攻撃に対する人材育成に関する調査研究」について、まとめたものである。

近年急増しているサイバー攻撃は、本年度に発生した「WannaCry」と呼ばれる身代金攻撃（ランサムウェア)）に代表されるように、世界規模で拡大しており、我が国にとっても大きな脅威になりつつある。

鉄道分野及び航空分野は我が国のサイバーセキュリティ戦略において重要インフラ分野に特定されているが、海外ではこれらの分野に関するサイバー攻撃事例も散見されており、仮に 2020 年東京オリンピック・パラリンピック開催期間中にサイバー攻撃が発生した場合、影響が甚大となるおそれがある。

当研究所では、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、鉄道分野及び航空分野を対象として、事業者のサイバーセキュリティに対する取組の実態を評価、検証するとともに、国内外の対策ガイドラインなどの整理やリスク分析を踏まえ、我が国に適応した対策手引きの作成を行った。

本年度は、2020 年東京オリンピック・パラリンピックに向けて、我が国の鉄道分野及び航空分野の事業者において更なるサイバーセキュリティ体制の強化に役立てるため、昨年度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、事業者がサイバーセキュリティ人材を育成する際に参考となるカリキュラムの作成を行った。

本調査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大学名誉教授・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 30 年 3 月

一般財団法人　運輸総合研究所
会長　　黒野　匡彦

「平成 29 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＞

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
〃	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
〃	林　泰三	内閣官房　内閣サイバーセキュリティセンター　参事官
〃	藤田　礼子	国土交通省　総合政策局　情報政策課長
〃	舘　剛司	公益財団法人東京オリンピック・パラリンピック競技大会組織委員会 テクノロジーサービス局長
〃	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 29 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＞

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
〃	林　泰三	内閣官房　内閣サイバーセキュリティセンター　参事官
〃	藤田　礼子	国土交通省　総合政策局　情報政策課長
〃	舘　剛司	公益財団法人東京オリンピック・パラリンピック競技大会組織委員会 テクノロジーサービス局長
〃	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

注）本報告書において、番号が付与されている用語については、巻末の「用語の定義」に説明文を記載している。

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[1]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幾度となくサイバーテロ[2]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。

鉄道分野及び航空分野は、我が国のサイバーセキュリティ戦略において重要インフラ[3]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おそれがある。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[4]（Internet of Things）化など更なる技術発展も考えられ、さらに脅威が増す可能性がある。

鉄道分野及び航空分野では、サイバーセキュリティ[5]人材の不足が懸念されており、過去の研究[注1)]では、研究対象とした鉄道分野及び航空分野[注2)]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、鉄道分野及び航空分野の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、鉄道分野及び航空分野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が必要であると考えた。

１．２　研究目的

本調査研究では、東京圏・首都圏内あるいは発着する鉄道分野及び航空分野の事業者を対象として、2020 年東京五輪大会に向け、鉄道分野及び航空分野において必要となるサイバーセキュリティ人材の定義及び人材育成カリキュラムを研究することを目的とする。

注1）東京オリンピック・パラリンピックに向けた交通機関へのサイバーテロ対策に関する調査研究、（一財）運輸政策研究機構、平成 28 年 3 月

注2）本調査研究における「航空事業者」は、航空輸送事業者及び空港運営事業者を想定している。また、これらの事業者の業種全般を「航空分野」と称する。

１．３　研究フロー

本調査研究の検討フローを以下に示す。

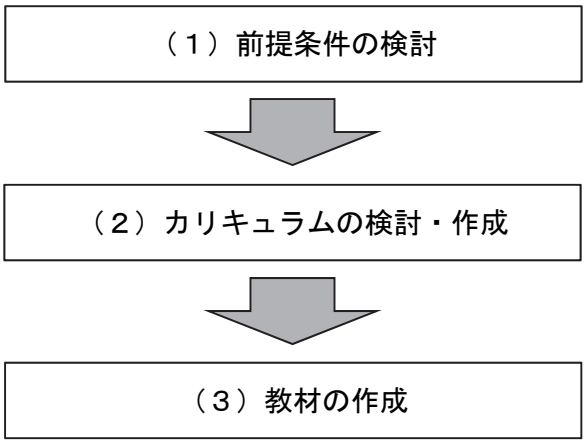


図　本調査研究の検討フロー

（１）前提条件の検討

カリキュラム作成の前提として、鉄道分野及び航空分野の事業者が置かれている状況の整理や将来望ましい状況を検討し、求められる人材像と必要となる能力を検討する。また、それを踏まえて、カリキュラムの育成対象者について検討する。

（２）カリキュラムの検討・作成

（１）の結果を踏まえ、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もと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に参考となるカリキュラムを作成する。

（３）教材の作成

カリキュラムをもとにした人材育成を実施するための教材（簡易版）を作成する。

第２章　前提条件の検討

２．１　前提条件の検討フロー

カリキュラムの前提条件の検討フローは以下のとおりである。

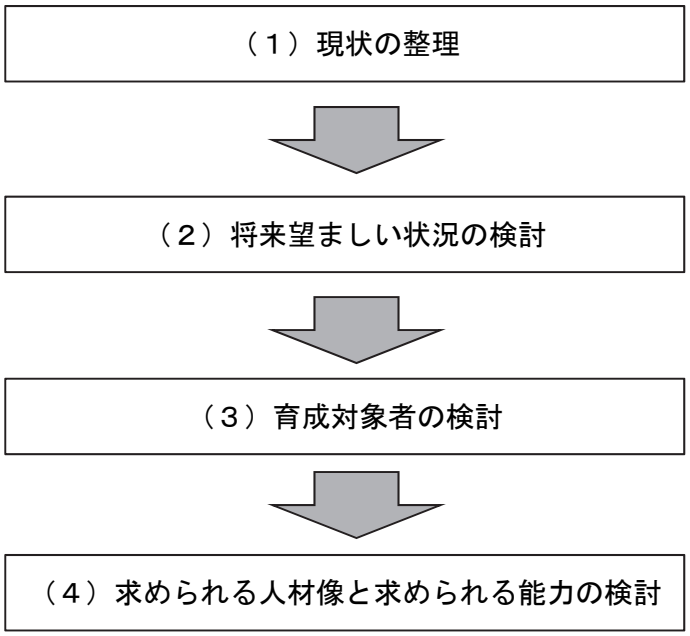


図　本調査研究の検討フロー

（１）現状の整理

サイバー攻撃の脅威などを踏まえて、鉄道分野及び航空分野の事業者が置かれている状況を整理する。

（２）将来望ましい状況の検討

（１）の結果を踏まえ、2020 年東京五輪大会に向けて、鉄道分野及び航空分野の事業者において、サイバーセキュリティ対策の将来望ましい状況を検討する。

（３）育成対象者の検討

（１）及び（２）の状況を踏まえ、カリキュラムの育成対象者を検討する。

（４）求められる人材像と求められる能力の検討

カリキュラムの育成対象者に求められる人材像と求められる能力を検討する。

２．２　現状の整理

現在までに発生したサイバー攻撃の脅威などを踏まえて、鉄道分野及び航空分野の事業者が置かれている状況は以下のとおりである。

・重要インフラにおける制御システムは、従来、サイバー攻撃を受ける可能性は低いと考えられてきたが、Stuxnet[6]やWannaCry[7]に代表されるように、システムのＩＴ化、他システムとの連携、クローズドシステム[8]に対する攻撃手法の高度化など、脅威は増大していると考えられる。

・標的型攻撃[9]の進化あるいはワーム機能[10]を有したランサムウェア[11]の登場により、海外では鉄道分野及び航空分野でもサイバー攻撃の被害事例が報告されている。また、ワーム機能を有することにより、マルウェア[12]の感染は瞬時に拡大する。このため、サイバー攻撃が発生した際には迅速かつ適切な対応が求められる。

・鉄道分野及び航空分野の制御システムがサイバー攻撃を受けた事例は国内では報告はされておらず、サイバー攻撃を受けた際に、現場で適切な対応が取れるか現状では不明な状態にあると考えられる。

・サイバー攻撃と従来のシステム障害などによる異常には、明確な違いはないと考えられ、システムを維持管理する人材が、サイバー攻撃に関する基礎知識を持たない場合、サイバー攻撃であることに気付くのが遅れる可能性もあり、その場合、さらに他のシステムへ影響が波及するなど、初動対応に遅れを生じることが懸念される。

・一般にサイバー攻撃の場合、より高度な知識と適切な対応が必要となるため、サイバー攻撃から防護することを鑑みると、サイバー攻撃に対処（原因究明、復旧など）する専門機関（社内外のセキュリティ担当、CSIRT[13]、セキュリティベンダー[14]など）との連携により対応することが望ましいが、システムを維持管理する人材が、サイバー攻撃に関わる基礎知識を持たない場合、うまく連携がとれないことが懸念される。

２．３　将来望ましい状況の検討

システムのＩＴ化、他システムとの連携、クローズドシステムに対する攻撃手法の高度化など鉄道分野及び航空分野の事業者の潜在的な脅威は増大している。このような状況を踏まえ、鉄道分野及び航空分野の事業者においては、将来的に以下の状況にあることが望ましい。

（１）インシデント[注1)]発生の際、その原因がサイバー攻撃である可能性を考慮し、適切に対応できる人材が現場に配置されている。

鉄道事業者及び航空事業者の制御システムがサイバー攻撃を受けた事例は国内で報告されておらず、サイバー攻撃を受けた際に、現場で適切な対応が取れるか現状では不明な状態にあると考えられる。そのため、サイバー攻撃に関する基礎知識を有し、インシデント発生の際、その原因がサイバー攻撃である可能性を考慮し、適切に対応できる人材が現場に配置されていることが望ましい。

（２）仮にサイバー攻撃を受けた場合でも対応可能となる体制が整備されている。

インシデントが発生した時点では、サイバー攻撃が原因か否かは判断できない場合も予想されるため、サイバー攻撃が疑われる場合の報告先を明示するなど、サイバー攻撃を受けた場合でも対応可能となる体制が整備されていることが望ましい。また、自社内においてサイバー攻撃に対応するための計画、実行、評価、改善を繰り返し、体制を継続的に改善することが望ましい。

（３）サイバー攻撃に対処する専門機関と連携して対処できる体制が整備されている。

サイバー攻撃に対処（原因究明、復旧など）する専門機関に、当該システムの知識が不足していた場合、対処が遅れることも予想されるため、より迅速な対処をするために、システムを熟知する人材とサイバー攻撃に対処する専門機関が連携して対処できる体制が整備されていることが望ましい。

（４）インシデント対応に従事する全ての要員がサイバー攻撃の脅威を認識している。

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ることから、インシデント対応に従事する全ての要員がサイバー攻撃の脅威を認識していることが望ましい。

注1）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、意図的なサイバー攻撃により、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、そのおそ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。なお、国土交通省の外局である運輸安全委員会が調査する「重大インシデント」は、「事故が発生するおそれがあると認められる事態」を指し、鉄道運転事故/航空事故には至らずに済んだものの一歩間違えれば事故が発生していたという状況をいい、本調査における「インシデント」とは意味合いが異なる。

２．４　求められる人材像と必要となる能力の検討

「2.3 将来望ましい状況」で示した状況を実現するために、求められる人材像は、「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」（発行：平成 28 年度、(一財) 運輸総合研究所)）の対策を実践できる人材とした。具体的には、下表のような定義とした。

表　本カリキュラムにおける、求められる人材像とそのために必要となる能力

（1） 求められる 人材像	・インシデント発生の際、その原因がサイバー攻撃である可能性を考慮し、適切に「対応」[注1)]できる人材。 ・「インシデント対応」[注2)]を、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「対応」できる人材。
（2） 必要となる 能力	1）サイバー攻撃に関わるインシデント対応に関する能力 ・インシデント発生時の対応手順を理解し、適切に「対応」できる能力。 ・サイバー攻撃対策を理解し、一連の「対応」ができる能力。 ・サプライチェーンのセキュリティ対策の重要性を理解し、サイバー攻撃に備えた「対応」ができる能力。 2）上記に関わる情報技術（ＩＴ）に関する能力 ・「インシデント対応」を行うために必要な情報技術（ＩＴ）に関する知識と能力。

注1）本頁における「対応」とは、対象となるシステムを維持管理する人材が、サイバーに対処（原因究明、復旧など）する専門機関の助言を受けて、システムの復旧につなげる活動などにあたる他、システムを熟知する立場から、サイバーに対処（原因究明、復旧など）する専門機関と連携して、システムに関する助言や援助を行うことを指す。

注2）本調査研究における「インシデント対応」には、以下の活動が含まれる。
①インシデント発生時：インシデント発生時に、被害を局限化、最小化し、速やかな復旧につなげる活動
②インシデント発生後：インシデントから復旧し、再発を防止することを目的とする活動
③インシデント発生前：インシデント発生に備えた「準備」の活動

２．５　育成対象者の検討

２．５．１　鉄道分野

各鉄道事業者の組織（役職と部門）において、本カリキュラムの育成対象者は下表のとおりであり、鉄道事業部門のシステムを維持管理する人材（技術者層）である。（凡例：「○」）

なお、経営者層と管理者層は、サイバーセキュリティに対する意識改革の必要性などが指摘されているが、優先順位を踏まえ本カリキュラムでは対象外とした。また、鉄道事業部門のシステム担当以外も対象外とした。なお、管理者層は、将来的には技術者層と経営層との間のコミュニケーションを円滑にする「橋渡し人材」の一翼を担うことが期待される。（凡例：「-」）

情報システム部門は、本カリキュラムで必要とされる能力を既に有していると考えられるため、対象外とした。ただし、より高度な連携をするために内容を理解しておくことを推奨する。（凡例：「△」）

表　本カリキュラムの鉄道分野における育成対象者（凡例：○）

部門 / 役職	情報システム部門	鉄道事業部門（システム担当）	鉄道事業部門（システム担当以外）
経営者層	－		
管理者層[注1)]	－	－	－
技術者層[注2)]	△	○	－

なお、サイバー攻撃に対応する一連の役割とそれを担当する部署は、各鉄道事業者で異なると思われるため、本カリキュラムにおける想定を以下の表に示す。

表　サイバー攻撃に対応する一連の役割と担当部署の想定（鉄道分野/運行管理システムの例）[注3)]

役割	担当部署	望まれる能力
システム操作 システム異常の検知・通報	司令所/指令所	異常の原因としてサイバー攻撃があるという意識をもち、適切に連絡ができる能力
システム維持管理 システム障害対応	電気部門 （外部委託先を含む）	サイバー攻撃に備えた準備、インシデント発生時の対応、サイバー攻撃対策などの一連の活動に「対応」[注4)]できる能力
サイバー攻撃の インシデント対応の立案、実行	セキュリティ担当部門 CSIRT・情報システム部門 セキュリティベンダー	サイバー攻撃に備えた準備、インシデント対応、サイバー攻撃対策などの一連の活動を立案、実行できる能力

注1）本調査研究における「管理者層」とは、現場から報告を受け、各所に報告をする方を指す。
注2）本調査研究における「技術者層」とは、システムを扱う現場において、実際にシステムの維持管理などをする方を指す。
注3）表内の黒枠は本カリキュラムで想定する育成対象者を指す。
注4）本頁における「対応」とは、対象となるシステムを維持管理する人材が、サイバーに対処（原因究明、復旧など）する専門機関の助言を受けて、システムの復旧につなげる活動などにあたる他、システムを熟知する立場から、サイバーに対処（原因究明、復旧など）する専門機関と連携して、システムに関する助言や援助を行うことを指す。

２．５．２　航空分野

各航空事業者の組織（役職と部門）において、本カリキュラムの育成対象者は下表のとおりであり、事業部門のシステムを維持管理する人材である。（凡例：「○」）

なお、経営者層、管理者層、事業部門のシステム担当以外の扱いについては、鉄道分野と同様、対象外である。（凡例：「-」）

表　本カリキュラムの航空分野における育成対象者（凡例：○）

部門 / 役職	事業部門（システム担当）	事業部門（システム担当以外）
経営者層	－	
管理者層	－	－
技術者層	○	－

なお、サイバー攻撃に対応する一連の役割とそれを担当する部署は、各航空事業者で異なると思われるため、本カリキュラムにおける想定を以下の表に示す。

表　サイバー攻撃に対応する一連の役割と担当部署の想定（航空分野/運航システムの場合） 注1)

役割	担当部署	望まれる能力
システム操作 システム異常の検知・通報	システム運用部門 （オペレーター）	異常の原因としてサイバー攻撃があるという意識をもち、適切に連絡ができる能力
システム維持管理 システム障害対応	システム維持管理部門 （外部委託先を含む）	サイバー攻撃に備えた準備、インシデント発生時の対応、サイバー攻撃対策などの一連の活動に「対応」注2)できる能力
サイバー攻撃の インシデント対応の立案、実行	セキュリティ担当部門 CSIRT・情報システム部門 セキュリティベンダー	サイバー攻撃に備えた準備、インシデント対応、サイバー攻撃対策などの一連の活動を立案、実行できる能力

注1）表内の黒枠は本カリキュラムで想定する育成対象者を指す。

注2）本頁における「対応」とは、対象となるシステムを維持管理する人材が、サイバーに対処（原因究明、復旧など）する専門機関の助言を受けて、システムの復旧につなげる活動などにあたる他、システムを熟知する立場から、サイバーに対処（原因究明、復旧など）する専門機関と連携して、システムに関する助言や援助を行うことを指す。

第３章　カリキュラムの検討・作成

３．１　カリキュラムの検討フロー

カリキュラムの検討フローは以下のとおりである。

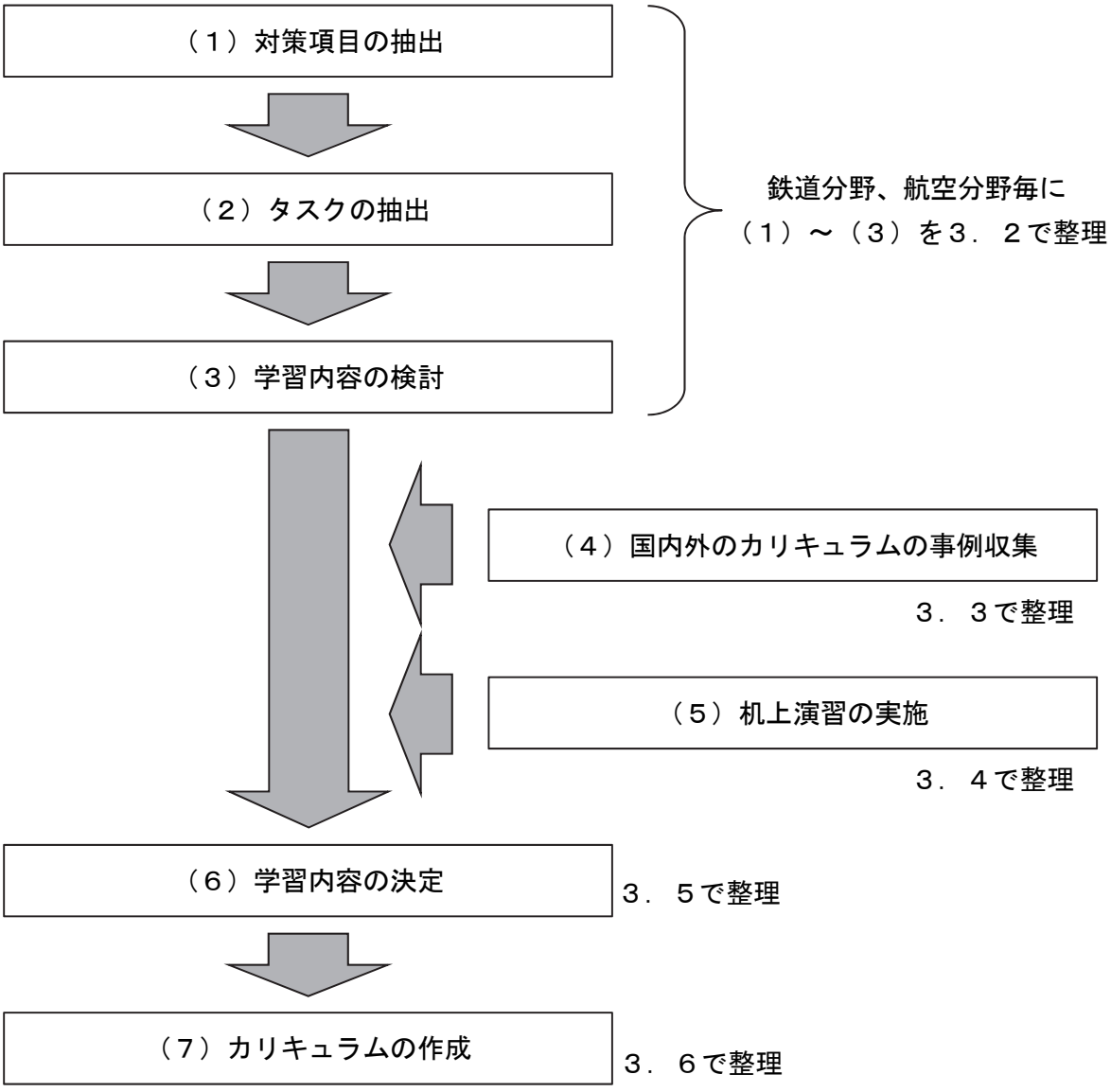


図　カリキュラムの検討フロー

（１）学習内容の検討

学習内容について、以下の１）～３）を検討する

１）対策項目の抽出

育成対象者に必要となる能力を習得するために必要となる対策項目を抽出する。

２）タスクの抽出

「i コンピテンシディクショナリ」（発行：2017 年６月 20 日改訂、（独）情報処理推進機構）[注1)]の「タスクディクショナリ」[注2)]を参照し、１）で抽出した対策項目を実践するためのタスク[15]を抽出する。

３）学習内容の整理

「i コンピテンシディクショナリ」の「スキルディクショナリ」[注3)]を参照し、２）で抽出したタスクから、スキル[16]を抽出し、学習内容を整理する。

（２）国内外のカリキュラムの事例収集

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の作成に資するため、国内外のサイバーセキュリティ人材育成に関する事例などを整理する。

（３）机上演習の実施

本カリキュラムの学習内容を検討する際の知見を得るために、机上演習[17]を実施する。

（４）学習内容の決定

（２）及び（３）で得られた知見をもとに、（１）のカリキュラム構成の精査を行うとともに、対象となる人材の役割を考慮した上で学習内容を決定する。

（５）カリキュラムの作成

（１）及び（２）の検討結果をもとに、カリキュラム作成を行う。

注1)「i コンピテンシディクショナリ」とは、企業において IT を利活用するビジネスに求められる業務（タスク）と、それを支える人材の能力や素養（スキル）を「タスクディクショナリ」、「スキルディクショナリ」として体系化したものである。

注2)「タスクディクショナリ」とは、どのような企業・組織でも利活用が可能となるように広範囲で網羅的なタスク群である。

注3)「スキルディクショナリ」とは、「タスクディクショナリ」との連係情報を利用して、そのスキルが、どのタスクの遂行に有効なのかを判断するために利用することが可能であり、スキル標準、情報処理技術者試験の知識項目例や主要知識体系を参照元とし、IT 関連業務の遂行に必要なスキル・知識項目を集約し一覧化したものである。

３．２　学習内容の検討

「2.4 求められる人材像と必要となる能力の検討」で示したように、求められる人材像は、「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」（発行：平成 28 年度、（一財）運輸総合研究所））（以下、手引書）の対策を実践できる人材である。

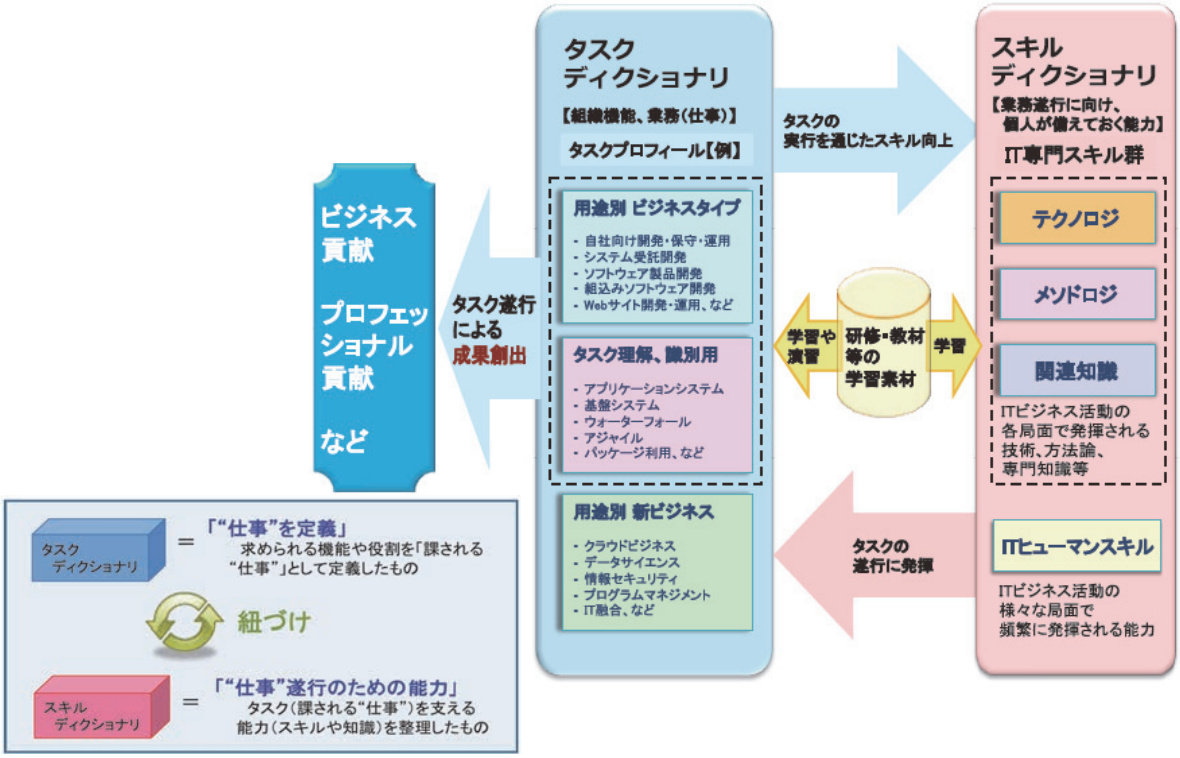
手引書を実践するための人材育成カリキュラムを作成するにあたっては、必要となるタスクとスキルを抽出し、学習内容として整理する。

具体的には、同手引書に記載された対策項目から、育成対象者の役割を考慮して項目を抽出し、この項目について、「i コンピテンシディクショナリ」を用いて、具体的なタスクとスキルの抽出を行い、学習内容の整理を行う。

（参考）ｉコンピテンシディクショナリについて

「i コンピテンシディクショナリ」は、企業においてＩＴを利活用するビジネスに求められる業務（タスク）と、それを支える人材の能力や素養（スキル）を「タスクディクショナリ」、「スキルディクショナリ」として体系化したものである。

「i コンピテンシディクショナリ」の活用を通じ、人材育成戦略の立案（Plan）、育成施策の実行（Do）、自組織のリソース状況の把握（Check）、目標の再設定（Act）といった組織における人材育成のＰＤＣＡサイクルを回す活動の手助けになることが期待されている。



出典：iCD ポケットハンドブック、（独）情報処理推進機構、
https://icd.ipa.go.jp/icd/application/files/4815/0104/6947/iCD2017_pocket_handbook.pdf

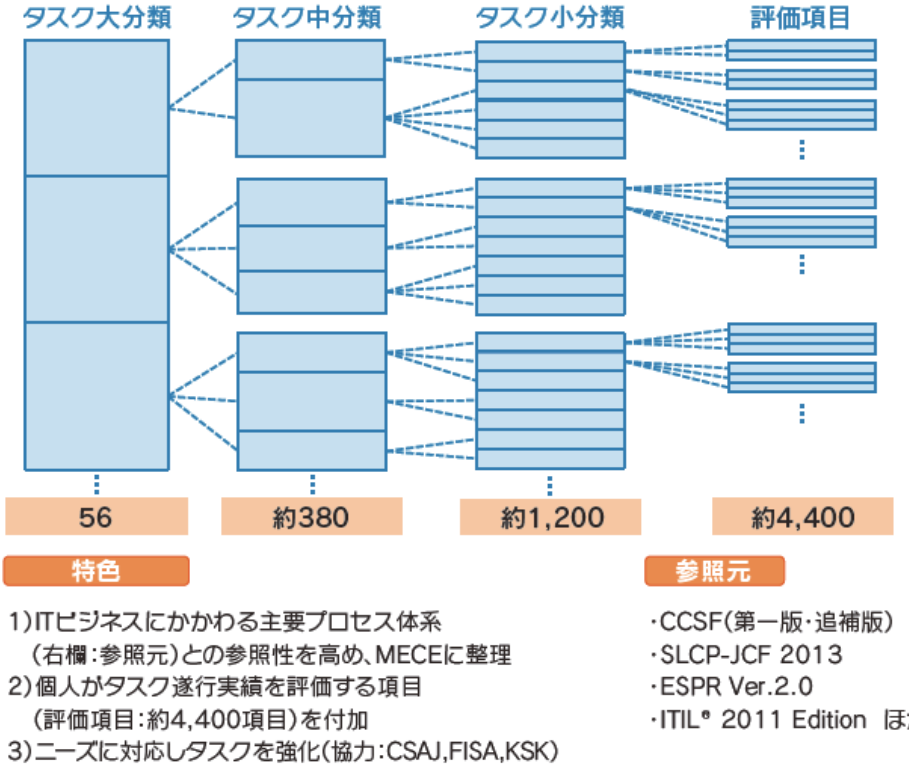
図　ｉコンピテンシディクショナリの概要

（１）タスクディクショナリ

「タスクディクショナリ」は、どのような企業・組織でも利活用が可能となるように広範囲で網羅的なタスク群を提供したものである。

「タスク」は、人材育成の推進において重要な位置づけであるが、企業や組織が、経営戦略や事業計画をもとにした、あるべき「タスク」を定義するのは難しいと考えられる。

企業や組織は、この「タスクディクショナリ」を参照し、自社・自組織のビジネスモデル、経営戦略や事業計画、及び現状の業務に基づいて取捨選択することで、あるべき自社・自組織のタスクを定めることができる。

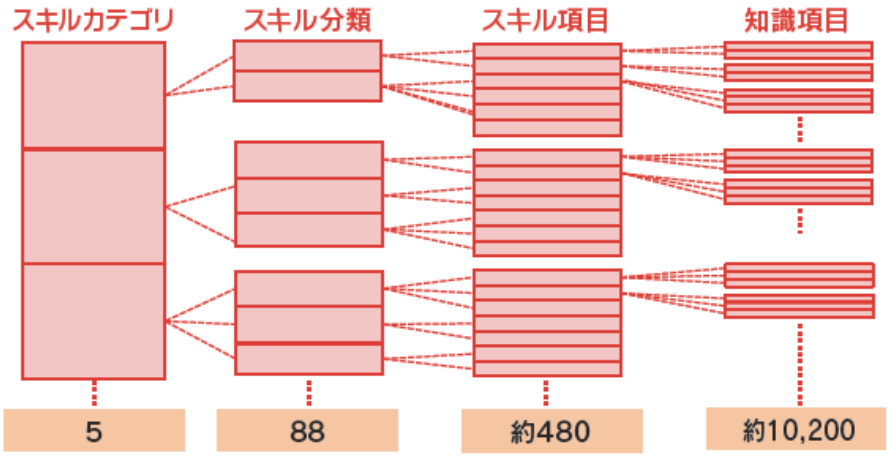


出典：iCD ポケットハンドブック、(独) 情報処理推進機構、
https://icd.ipa.go.jp/icd/application/files/4815/0104/6947/iCD2017_pocket_handbook.pdf

図　タスクディクショナリの構造

（２）スキルディクショナリ

「スキルディクショナリ」は、検討するスキルが、どのタスクの遂行に有効なのかを判断するために利用することが可能であり、スキル標準、情報処理技術者試験の知識項目例や主要知識体系を参照元とし、ＩＴ関連業務の遂行に必要なスキル・知識項目を集約し一覧化したものである。



特色

1)IT業務に必要なスキルと知識を、主要な参照元の知識項目に基づき網羅的に構造化
2)スキルカテゴリは、「メソドロジ」「テクノロジ」「関連知識」「ITヒューマンスキル」「企業固有スキル(ユーザ独自設定領域)」の5分類から構成
3)情報処理技術者試験「〔午前の試験〕出題分野」に準じた整理体系

参照元

・情報処理技術者試験
・J07
・PMBOK
・BABOK　ほか

注）企業固有スキルは、個々の企業が自社のビジネスや業務の遂行に必要なスキルを独自に定義する

出典：iCD ポケットハンドブック、（独）情報処理推進機構、
https://icd.ipa.go.jp/icd/application/files/4815/0104/6947/iCD2017_pocket_handbook.pdf

その内容については、スキルの特性に基づき「メソドロジ」、「テクノロジ」、「関連知識」、「ＩＴヒューマンスキル」の４つのカテゴリに分類されている。

１）スキル特性に基づく分類

① メソドロジ

「メソドロジ」カテゴリは、ＩＴビジネス活動の様々な局面で発揮される手法、方法などで、発揮される対象領域が広く、汎用性、応用性が高いスキルを集めたものである。

② テクノロジ

「テクノロジ」カテゴリは、ＩＴビジネス活動の様々な局面で発揮されるＩＴ関連技法などで、対象領域が特定されるものが多いスキルを集めたものである。

③ 関連知識

「関連知識」カテゴリは、ＩＴビジネス活動の様々な局面で活用される、「メソドロジ」、「テクノロジ」以外の関連業務知識を集めたものである。

④ ＩＴヒューマンスキル

「ＩＴヒューマンスキル」カテゴリは、ＩＴビジネス活動の様々な局面で頻繁に発揮される基本スキルカテゴリである。３分類、12 スキル項目で構成され、「メソドロジ」、「テクノロジ」、「関連知識」と同様にタスクの遂行において発揮されるスキルカテゴリとして定義されている。

２）スキル体系の分類

・スキルカテゴリ：スキルの特性に基づく分類
・スキル分類
・スキル項目：個人に求められる能力
・知識項目：個人に求められる知識

３．２．１　鉄道分野

（1）対策項目の抽出

「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」（発行：平成 28 年度、（一財）運輸総合研究所）に記載されている以下の３つのカテゴリからなる対策から、それぞれ、システムの維持管理及びインシデント対応に必要と考えられる対策項目を抽出し、その対策項目について想定される対策を整理した。対策項目の抽出結果を下表に示す。

・機器・システムのセキュリティ対策
・運用・管理のセキュリティ対策
・セキュリティインシデントのセキュリティ対策

表　「機器・システムのセキュリティ対策」における対策項目の抽出結果

対策項目	想定される対策
外部ネットワークとの分離	外部ネットワーク[18]との接続の排除
	意図しない通信の排除
他ネットワークとの接続	接続先の把握
	接続先の技術面の把握
	接続先の分類
	接続点での防御
マルウェア対策	機器のマルウェア対策
	重要データのバックアップ
ログの取得・保管・保全	ログ[19]の取得と保管

表　「運用・管理のセキュリティ対策」における対策項目の抽出結果

対策項目	想定される対策
外部記憶媒体[20]のマルウェア感染	運用方針の策定
権限[21]の適切な割当	管理者権限の適切な割当
	管理者権限の利用に対する証人と監視
修正プログラム[22]の適用	脆弱性情報[23]の収集
	修正プログラム管理の実施
	ファームウェア[24]のアップデートの実施
情報の収集	脆弱性情報の収集

表　「セキュリティインシデントのセキュリティ対策」における対策項目の抽出結果

対策項目	想定される対策
セキュリティインシデントの対応	責任と手順の明確化
	セキュリティインシデントの対応の明確化

（２）タスクの抽出

１）対策項目に基づく抽出されたタスク

「i コンピテンシディクショナリ」の「タスクディクショナリ」を参照し、（１）で抽出した対策項目を実践するためのタスクを選択する。なお、「タスクディクショナリ」には、「対策項目」に紐づく「タスク」が収録されており、ここで選択されるタスクは、「タスクディクショナリ」から自動的に選択されるものである。

対策項目と抽出されたタスクの対応関係は下表のとおりである。

表　対策項目と抽出されたタスクの対応表

対策	想定される対策	ﾀｽｸ小分類ｺｰﾄﾞ	抽出されたタスク小分類
機器・システムのセキュリティ対策	外部ネットワークとの接続の排除	DV04.4.2	ネットワークの運用管理・保守の設計
		US02.2.2	情報セキュリティの評価と検証
		US03.7.4	ネットワーク資源の管理
	意図しない通信の排除	US02.2.2	情報セキュリティの評価と検証
	接続先の把握	EV06.1.1	資産管理方針と体制の策定
	接続先の技術面の把握	US03.8.6	セキュリティの評価
	接続先の分類	MC03.1.4	リスクの評価
	接続点での防御	US03.8.6	セキュリティの評価
		DV01.3.2	セキュリティ要件の定義
	機器のマルウェア対策	US03.10.2	ソフトウェアの予防保守
		DV01.3.2	セキュリティ要件の定義
	重要データのバックアップ	US03.7.3	データの管理
	ログの取得と保管	US03.8.1	事故の検知
運用・管理のセキュリティ対策	運用方針の策定	US03.7.3	データの管理
	管理者権限の適切な割当	MC07.7.1	要員の責任及び権限の定義
		MC07.7.2	要員の責任及び権限の随時見直し
	管理者権限の利用に対する承認と監視	MC07.7.1	要員の責任及び権限の定義
		MC07.7.2	要員の責任及び権限の随時見直し
	脆弱性情報の収集	MC03.3.1	情報の収集と評価
	修正プログラム管理の実施	US03.2.2	変更の実施
		US03.7.2	ソフトウェアの管理
	ファームウェアのアップデートの実施	US02.2.1	情報セキュリティの運用
		DV12.2.1	問題の把握
	脆弱性情報の収集	MC03.3.1	情報の収集と評価
セキュリティインシデントのセキュリティ対策	責任と手順の明確化	US03.8.2	事故の初動処理
	セキュリティインシデントの対応の明確化	US03.9.1	問題発生時のコントロール（問題・障害管理）

2）抽出したタスクの整理

対策項目と抽出されたタスクの対応表において、抽出したタスク小分類の重複を除き、タスク小分類コードで並べ替えると、下表のとおりとなる。

表　抽出したタスク

タスク小分類コード	タスク小分類
DV01.3.2	セキュリティ要件の定義
DV04.4.2	ネットワークの運用管理・保守の設計
DV12.2.1	問題の把握
US02.2.1	情報セキュリティの運用
US02.2.2	情報セキュリティの評価と検証
US03.2.2	変更の実施
US03.7.2	ソフトウェアの管理
US03.7.3	データの管理
US03.7.4	ネットワーク資源の管理
US03.8.1	事故の検知
US03.8.2	事故の初動処理
US03.8.6	セキュリティの評価
US03.9.1	問題発生時のコントロール（問題・障害管理）
US03.10.2	ソフトウェアの予防保守
EV06.1.1	資産管理方針と体制の策定
MC03.1.4	リスクの評価
MC03.3.1	情報の収集と評価
MC07.7.1	要員の責任及び権限の定義
MC07.7.2	要員の責任及び権限の随時見直し

（３）学習内容の整理

１）求められるスキルの抽出

「i コンピテンシディクショナリ」に収録されている「ディクショナリ間連係」をもとに、（２）で抽出されたタスク小分類に対応するスキル項目を抽出し、以下の３つのスキルの特性に基づくカテゴリごとに整理した。求められるスキル項目の抽出結果を次頁表に示す。

なお、「ディクショナリ間連係」は、「タスクディクショナリ」と「スキルディクショナリ」の連係が収録されており、タスク小分類とスキル項

目の間に強い関係があるものを対応付けたものである。ここで選択されるスキル項目は、「ディクショナリ間連係」から自動的に選択されるものである。（下図参照）

- メソトロジ
- テクノロジ
- 関連知識

表記説明 タスクディクショナリとスキルディクショナリの連係情報 タスク小分類とスキル項目の間に強い関係があるものに◎を記載 （テクノロジのIT基礎は、基本となるスキルのため除いている）			スキル項目コード	S1100101010	S1100101020	S1100101030	S1100101040	S1100101050	S1100101060
			スキルカテゴリ	メソドロジ	メソドロジ	メソドロジ	メソドロジ	メソドロジ	メソドロジ
			スキル分類	（戦略）市場機会の評価と選定	（戦略）市場機会の評価と選定	（戦略）市場機会の評価と選定	（戦略）市場機会の評価と選定	（戦略）市場機会の評価と選定	（戦略）市場機会の評価と選定
タスク小分類コード	タスク大分類	タスク中分類	スキル項目 / タスク小分類	ビジネス環境分析手法	ビジネス戦略と目標・評価	業界動向把握の手法	経営管理システム	経営戦略手法	最新動向の手法
ST01.1.1	事業戦略策定	事業環境の分析	経営方針の確認		◎			◎	
ST01.1.2			外部環境の分析	◎		◎			◎
ST01.1.3			内部環境の分析		◎		◎	◎	
ST01.2.1		事業戦略の策定	基本構想の策定	◎	◎	◎		◎	
ST01.2.2			アクションプランの策定						
ST01.2.3			売上計画の策定						
ST01.2.4			費用計画の策定						
ST01.2.5			利益計画の策定						
ST01.2.6			資金計画の策定						
ST01.3.1		事業戦略実行体制の確立	実現可能性の検証	◎	◎		◎	◎	◎
ST01.3.2			実施準備		◎			◎	
ST02.1.1	事業戦略把握・策定支援	要求（構想）の確認	経営要求の確認		◎			◎	
ST02.1.2			経営環境の調査・分析と課題の抽出	◎	◎	◎	◎	◎	
ST02.2.1		新ビジネスモデルへの提言	業界動向の調査・分析	◎	◎	◎	◎	◎	◎
ST02.2.2			ビジネスモデル策定への助言	◎	◎		◎	◎	◎
ST02.3.1		事業戦略の実現シナリオへの提言	実現可能性の確認		◎		◎		◎
ST02.3.2			全社戦略の展開における活動・成果指標の設定		◎			◎	
ST02.3.3			課題とリスクの洗い出し		◎	◎	◎		
ST02.3.4			超概算予算の算出		◎				
ST03.1.1	IT製品・サービス戦略策定	市場動向の調査・分析・予測	市場機会の発見と選択						
ST03.1.2			ターゲット市場のビジネス手法の分析						

図　ディクショナリ間連係（一部）[注1]

注1)ディクショナリ間連係，（独）情報処理推進機構,https://www.ipa.go.jp/files/000060167.xlsx

表　求められるスキル（メソドロジ）

スキル項目コード	スキル分類	スキル項目
S120030010	（企画） 要求分析手法	要求の抽出手法
S120030020		要求の整理手法
S120030030		要求の仕様化手法
S120030040		要求の評価手法
S120030050		要件定義
S120040010	（企画） 非機能要件設計手法	プラットフォーム要件定義手法
S120040020		システム基盤の非機能要件設計
S130010010	（実装） アーキテクチャ 設計手法	アーキテクチャ設計手法
S130010040		インフラストラクチャアーキテクチャ設計手法
S130020100	（実装） ソフトウェア エンジニアリング手法	保守サービス提供手法
S140040010	（利活用） サービスの運用	サービスの運用手法
S140040020		システム運用管理手法
S140040050		運用支援ツール手法
S130050030	（実装） カスタマーサービス手法	予防保守手法
S150010010	（支援活動） 品質マネジメント手法	テスト技術・手法
S150010020		テストのマネジメント手法
S150030010	（支援活動） リスクマネジメント手法	リスク管理手法
S150030020		情報セキュリティ管理手法
S150060010	（支援活動） 資産管理手法	資産管理に関する手法
S150120050	（支援活動） 情報セキュリティ	リスク分析手法
S150120060		情報セキュリティポリシー策定手法

表　求められるスキル（テクノロジ）

スキル項目コード	スキル分類	スキル項目
S210160010	（システム）ネットワークの基礎技術	ネットワーク
S210160020		ネットワークコンピューティング
S210160030		ネットワークシステムの技術動向
S210160040		ネットワーク標準
S210160050		ネットワーク方式
S210160060		通信プロトコル
S210160070		データ通信と制御
S210170010	（システム）ネットワークの構築技術	ネットワークシステムの要件定義
S210170020		ネットワーク設計
S210170030		ネットワークシステムの実装技術
S210170040		ネットワークシステムの導入と移行
S210170050		ネットワークシステムの受け入れ
S210170060		ネットワークシステムの運用・保守・管理
S210180010	（システム）ネットワークの利用技術	ネットワーク管理
S210180020		ネットワーク応用
S210180030		ネットワーク製品知識
S210180040		業界固有のセキュリティ要件、事例
S210180060		テレコミュニケーション
S210210010	（システム）クラウドコンピューティングの利用技術	インタークラウド技術
S220010010	（開発）システムアーキテクティング技術	システム要件定義
S220010020		システムインテグレーションとアーキテクチャ
S220010030		アプリケーション共通基盤要件定義手法
S220010050		IT 基盤構築プロセス
S230030050	（保守・運用）システム保守・運用・評価	アプリケーションシステムの受け入れ
S230030080		システム運用方式技法
S230030100		システム管理計画
S230030110		システム管理技術
S230030140		システム管理製品
S230030150		運用管理ソフト製品
S230030170		運用システムの改善
S230030180		運用に関するシステム評価
S230030190		性能管理

S230030200		障害時運用方式
S230030220		構成管理
S230030230		保守技術
S230030240		メンテナンス
S230030250		保守・廃棄
S240020010	(非機能要件) セキュリティ の基礎技術	情報セキュリティ
S240020020		情報保証と情報セキュリティ
S240020030		情報倫理とセキュリティ
S240020050		アプリケーションセキュリティ
S240020060		情報プラットフォームのセキュリティ技術
S240020070		ネットワークのセキュリティリスク
S240020080		暗号技術
S240020090		セキュリティと個人情報
S240020100		保証、信用、信頼のメカニズム
S240020110		セキュリティ技術の理解と活用
S240030010	(非機能要件) セキュリティ の構築技術	セキュリティ方針の策定
S240030020		セキュリティ対策基準の策定
S240030030		情報セキュリティ対策
S240030050		セキュリティシステムの計画策定
S240030060		セキュリティシステムの要件定義
S240030090		コンピュータ・フォレンジクス（証拠保全追跡）
S240040010	(非機能要件) セキュリティ の利用技術	セキュリティシステムの運用管理
S240040030		システム運用・保守技術（セキュリティ）
S240040040		セキュリティ障害（事件事故/ｲﾝｼﾃﾞﾝﾄ）管理
S240040050		情報セキュリティ管理
S240040060		情報セキュリティ監査の実施・支援
S240040070		セキュリティ技術評価
S240040080		セキュリティの分析
S240040090		セキュリティの見直し（ｾｷｭﾘﾃｨｼｽﾃﾑの評価と改善）
S240040100		コンテンツセキュリティ技術

表　求められるスキル（関連知識）

スキル項目コード	スキル分類	スキル項目
S310020050	企業活動	情報セキュリティ監査
S310030010	法規・基準・標準	セキュリティ関連法規
S310030040		労働関連・取引関連法規

2）抽出したスキルの整理

抽出したスキル項目から、スキル分類の重複を除き、並べ替えると、下表のとおりとなる。

表　抽出したスキルの整理結果

スキルカテゴリ	分類	スキル分類
メソドロジ	（企画）	要求分析手法
		非機能要件設計手法
	（実装）	アーキテクチャ設計手法
		ソフトウェアエンジニアリング手法
		カスタマーサービス手法
	（利活用）	サービスの運用
	（支援活動）	品質マネジメント手法
		リスクマネジメント手法
		資産管理手法
		事業継続計画
		情報セキュリティ
テクノロジ	（システム）	ネットワークの基礎技術
		ネットワークの構築技術
		ネットワークの利用技術
		クラウドコンピューティングの利用技術
	（開発）	システムアーキテクティング技術
	（保守・運用）	システム保守・運用・評価
	（非機能要件）	セキュリティの基礎技術
		セキュリティの構築技術
		セキュリティの利用技術
関連知識		企業活動
		法規・基準・標準

3）学習内容の整理

抽出したスキルから、システムの維持管理及びインシデント対応に必要と考えられる学習内容を整理する。整理にあたってのポイントは以下のとおりである。

・インシデント対応が主な役割となるため、「メソドロジ」の「企画」、「実装」、「利活用」分類の全てを除外した。

・ネットワークの構築者の育成を目的としていないため、「テクノロジ」の「システム」分類の「ネットワークの構築技術」を除外した。

・開発業務、保守・運用業務の能力向上を目的としていないため、「テクノロジ」の「開発」、「保守・運用」分類の全てを除外した。

・セキュリティの構築者の育成を目的としていないため、「テクノロジ」の「非機能要件」分類の「セキュリティの構築技術」を除外した。

学習内容（スキル分類）を整理した結果を以下の表に示す。

表　学習内容（スキル分類）の整理結果

スキルカテゴリ	分類	スキル分類
メソドロジ	（支援活動）	品質マネジメント手法
		リスクマネジメント手法
		資産管理手法
		事業継続計画
		情報セキュリティ
テクノロジ	（システム）	ネットワークの基礎技術
		ネットワークの利用技術
		クラウドコンピューティングの利用技術
	（非機能要件）	セキュリティの基礎技術
		セキュリティの利用技術
関連知識		企業活動
		法規・基準・標準

この結果をもとに、カリキュラム作成の方針を以下のとおりとした。

・「i コンピテンシディクショナリ」は、スキル特性に応じてスキル体系を「メソドロジ」、「テクノロジ」、「関連知識」の３つに分類している。学習内容の整理の結果から、この３つの分類のそれぞれに該当する項目があったため、この体系に対応した講座を設ける。

・「テクノロジ」に関しては、大別して、「ネットワークの知識」と「セキュリティの知識」に関する講座を設ける。クラウドコンピューティングの利用技術に関しては、「ネットワークの知識」に含めることにする。

この方針をもとに、学習内容（スキル分類とスキル項目）は次頁表のとおりとする。
スキル分類とスキル項目の関連は、「１）求められるスキルの抽出」を参照されたい。

表　学習内容の整理結果

スキル項目コード	スキル分類	スキル項目
S150010010	(メソドロジ) 品質マネジメント手法	テスト技術・手法
S150010020		テストのマネジメント手法
S150030010	(メソドロジ) リスクマネジメント手法	リスク管理手法
S150030020		情報セキュリティ管理手法
S150060010	(メソドロジ) 資産管理手法	資産管理に関する手法
S150080010	(メソドロジ) 事業継続計画	BCP 策定手法
S150080020		災害対策管理手法
S150120050	(メソドロジ) 情報セキュリティ	リスク分析手法
S150120060		情報セキュリティポリシー策定手法
S210160010	(テクノロジ・システム) ネットワークの基礎技術	ネットワーク
S210160050		ネットワーク方式
S210160060		通信プロトコル
S210160070		データ通信と制御
S210180010	(テクノロジ・システム) ネットワークの利用技術	ネットワーク管理
S210180030		ネットワーク製品知識
S210180040		業界固有のセキュリティ要件、事例
S210210010	(テクノロジ・システム) クラウドコンピューティングの利用技術	インタークラウド技術
S210210020		クラウドコンピューティング利用
S210210030		クラウドシステムの監視技術
S240020010	(テクノロジ・非機能要件) セキュリティの基礎技術	情報セキュリティ
S240020020		情報保証と情報セキュリティ
S240020030		情報倫理とセキュリティ
S240020050		アプリケーションセキュリティ
S240020060		情報プラットフォームのセキュリティ技術
S240020070		ネットワークのセキュリティリスク
S240020080		暗号技術
S240020090		セキュリティと個人情報
S240020100		保証、信用、信頼のメカニズム
S240020110		セキュリティ技術の理解と活用
S240040010	(テクノロジ・非機能要件) セキュリティの利用技術	セキュリティシステムの運用管理
S240040040		セキュリティ障害（事件事故/インシデント）管理
S240040050		情報セキュリティ管理
S310020050	(知識関連) 企業活動	情報セキュリティ監査
S310030010	(知識関連) 法規・基準・標準	セキュリティ関連法規
S310030040		労働関連・取引関連法規

３．２．２　航空分野

（１）対策項目の抽出

「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」（発行：平成 28 年度、（一財）運輸総合研究所）に記載されている以下の３つのカテゴリからなる対策から、鉄道分野と同様に、それぞれ、システムの維持管理及びインシデント対応に必要と考えられる対策項目を抽出し、その対策項目について想定される対策を整理した。対策項目の抽出結果を下表に示す。

・設備・システムのセキュリティ対策
・運用・管理のセキュリティ対策
・セキュリティインシデントのセキュリティ対策

表　「設備・システムのセキュリティ対策」における対策項目の抽出結果

対策項目	想定される対策
外部ネットワークとの分離	外部ネットワークとの接続の排除
	意図しない通信の排除
他ネットワークとの接続	接続先の把握
	接続先の分類
	接続点での防御
マルウェア感染	機器のマルウェア対策
	不正プログラム対策
	低レイヤ層[25]での監視
	エンドポイント[26]対策の強化
不正処理防止策	サーバーのハードニング[27]
	OS でのプログラム自動起動の無効化
	専用ツールの導入
アクセス制御	接続制御
	未認可端末の可視化
ログの取得・保管・保全	ログの取得と保管

表　「運用・管理のセキュリティ対策」における対策項目の抽出結果

対策項目	想定される対策
セキュリティ仕様の確認	セキュリティ仕様の明確化
外部記憶媒体のマルウェア対策	PC 運用ポリシーの見直し
	外部記憶媒体上のプログラムの実行制御
	改ざんされたファームウェアなどの検出
権限の適切な割当	管理者権限の適切な割当
	管理者権限の利用への承認と監視
セキュリティパッチ[28]の適用	脆弱性情報の収集
	パッチマネジメント[29]の実施
	ファームウェアのアップデートの実施

表　「セキュリティインシデントのセキュリティ対策」における対策項目の抽出結果

対策項目	想定される対策
セキュリティインシデントへの準備と対応	責任と手順の明確化
	セキュリティインシデントの対応の明確化
	臨時サイトによる再開策を含む対応手順の作成

（2）タスクの抽出

鉄道分野と同様に、「i コンピテンシディクショナリ」の「タスクディクショナリ」を参照し、（1）で抽出した対策項目を実践するためのタスクを選択する。

対策項目と抽出されたタスクの対応関係は下表のとおりである。

表　対策項目と抽出されたタスク小分類の対応表

対策	想定される対策	ﾀｽｸ小分類ｺｰﾄﾞ	抽出されたタスク小分類
設備・システムのセキュリティ対策	外部ネットワークとの接続の排除	DV04.4.2	ネットワークの運用管理・保守の設計
		US02.2.2	情報セキュリティの評価と検証
		US03.7.4	ネットワーク資源の管理
	意図しない通信の排除	US02.2.2	情報セキュリティの評価と検証
	接続先の把握	EV06.1.1	資産管理方針と体制の策定
	接続先の分類	MC03.1.4	リスクの評価
	接続点での防御	US03.8.6	セキュリティの評価
		DV01.3.2	セキュリティ要件の定義
	機器のマルウェア対策	US03.10.2	ソフトウェアの予防保守
		DV01.3.2	セキュリティ要件の定義
		DV04.11.1	セキュリティの実装
	不正プログラム対策	DV01.3.2	セキュリティ要件の定義
		DV04.6.1	セキュリティの設計
		DV04.11.1	セキュリティの実装
	低レイヤ層での監視	DV01.3.2	セキュリティ要件の定義
		DV04.11.1	セキュリティの実装
	エンドポイント対策の強化	DV01.3.2	セキュリティ要件の定義
		DV04.11.1	セキュリティの実装
	サーバーのハードニング	DV01.3.2	セキュリティ要件の定義
		US03.10.1	ハードウェアの予防保守
	OS でのプログラム自動起動の無効化	DV01.3.2	セキュリティ要件の定義
	専用ツールの導入	DV01.3.2	セキュリティ要件の定義
		DV04.11.1	セキュリティの実装
	接続制御	US02.1.1	ユーザー管理
	未認可端末の可視化	DV01.3.2	セキュリティ要件の定義
	ログの取得と保管	US03.8.1	事故の検知
運用・管理のセキュリティ対策	セキュリティ仕様の明確化	DV01.3.2	セキュリティ要件の定義
		US02.2.2	情報セキュリティの評価と検証
	PC 運用ポリシーの見直し	DV01.3.2	セキュリティ要件の定義

	外部記憶媒体上のプログラムの実行制御	DV01.3.2	セキュリティ要件の定義
		DV04.6.1	セキュリティの設計
		DV04.11.1	セキュリティの実装
	改ざんされたファームウェアなどの検出	DV01.3.2	セキュリティ要件の定義
		DV04.6.1	セキュリティの設計
		DV04.11.1	セキュリティの実装
	管理者権限の適切な割当	MC07.7.1	要員の責任及び権限の定義
		MC07.7.2	要員の責任及び権限の随時見直し
	管理者権限の利用に対する承認と監視	MC07.7.1	要員の責任及び権限の定義
		MC07.7.2	要員の責任及び権限の随時見直し
	脆弱性情報の収集	MC03.3.1	情報の収集と評価
	パッチマネジメントの実施	US03.2.2	変更の実施
		US03.7.2	ソフトウェアの管理
	ファームウェアのアップデートの実施	US02.2.1	情報セキュリティの運用
セキュリティインシデントのセキュリティ対策	責任と手順の明確化	US03.8.2	事故の初動処理
	セキュリティインシデントの対応の明確化	US03.9.1	問題発生時のコントロール（問題・障害管理）
	臨時サイトによる再開策を含む対応手順の作成	MC02.1.3	事業継続計画の策定
		MC02.2.2	事業継続のためのリソースの確保

2）抽出したタスクの整理

鉄道分野と同様に、対策項目と抽出されたタスクの対応表において、抽出したタスク小分類の重複を除き、タスク小分類コードで並べ替えると、下表のとおりとなる。

表　抽出したタスク小分類

タスク小分類コード	タスク小分類
DV01.3.2	セキュリティ要件の定義
DV04.4.2	ネットワークの運用管理・保守の設計
DV04.6.1	セキュリティの設計
DV04.11.1	セキュリティの実装
US02.1.1	ユーザー管理
US02.2.1	情報セキュリティの運用
US02.2.2	情報セキュリティの評価と検証
US03.2.2	変更の実施
US03.7.2	ソフトウェアの管理
US03.7.4	ネットワーク資源の管理
US03.8.1	事故の検知
US03.8.2	事故の初動処理
US03.8.6	セキュリティの評価
US03.9.1	問題発生時のコントロール（問題・障害管理）
US03.10.1	ハードウェアの予防保守
US03.10.2	ソフトウェアの予防保守
EV06.1.1	資産管理方針と体制の策定
MC02.1.3	事業継続計画の策定
MC02.2.2	事業継続のためのリソースの確保
MC03.1.4	リスクの評価
MC03.3.1	情報の収集と評価
MC07.7.1	要員の責任及び権限の定義
MC07.7.2	要員の責任及び権限の随時見直し

（3）学習内容の整理

鉄道分野と同様に、「i コンピテンシディクショナリ」に収録されている「ディクショナリ間連係」をもとに、（2）で抽出されたタスク小分類に対応するスキル項目を抽出し、スキルの特性に基づく以下の３つのカテゴリごとに整理した。

・メソトロジ
・テクノロジ
・関連知識

表　求められるスキル（メソドロジ）

スキル項目コード	スキル分類	スキル項目
S120030010	（企画） 要求分析手法	要求の抽出手法
S120030020		要求の整理手法
S120030030		要求の仕様化手法
S120030040		要求の評価手法
S120030050		要件定義
S120040010	（企画） 非機能要件設計手法	プラットフォーム要件定義手法
S120040020		システム基盤の非機能要件設計
S130010010	（実装） アーキテクチャ設計手法	アーキテクチャ設計手法
S130010040		インフラストラクチャアーキテクチャ設計手法
S130020100	（実装） ソフトウェアエンジニアリング手法	保守サービス提供手法
S140040010	（利活用） サービスの運用	サービスの運用手法
S140040020		システム運用管理手法
S140040040		運用オペレーション手法
S140040050		運用支援ツール手法
S130050030	（実装） カスタマーサービス手法	予防保守手法
S150010010	（支援活動） 品質マネジメント手法	テスト技術・手法
S150010020		テストのマネジメント手法
S150030010	（支援活動） リスクマネジメント手法	リスク管理手法
S150030020		情報セキュリティ管理手法
S150060010	（支援活動） 資産管理手法	資産管理に関する手法
S150080010	（支援活動）事業継続計画	BCP 策定手法
S150080020		災害対策管理手法
S150120050	（支援活動） 情報セキュリティ	リスク分析手法
S150080060		情報セキュリティポリシー策定手法

表　求められるスキル（テクノロジ）

スキル項目コード	スキル分類	スキル項目
S210160010	（システム）ネットワークの基礎技術	ネットワーク
S210160020		ネットワークコンピューティング
S210160030		ネットワークシステムの技術動向
S210160040		ネットワーク標準
S210160050		ネットワーク方式
S210160060		通信プロトコル
S210160070		データ通信と制御
S210170010	（システム）ネットワークの構築技術	ネットワークシステムの要件定義
S210170020		ネットワーク設計
S210170030		ネットワークシステムの実装技術
S210170040		ネットワークシステムの導入と移行
S210170050		ネットワークシステムの受け入れ
S210170060		ネットワークシステムの運用・保守・管理
S210180010	（システム）ネットワークの利用技術	ネットワーク管理
S210180020		ネットワーク応用
S210180030		ネットワーク製品知識
S210180040		業界固有のセキュリティ要件、事例
S210180060		テレコミュニケーション
S210210010	（システム）クラウドコンピューティングの利用技術	インタークラウド技術
S210210030		クラウドシステムの監視技術
S220010010	（開発）システムアーキテクティング技術	システム要件定義
S220010020		システムインテグレーションとアーキテクチャ
S220010030		アプリケーション共通基盤要件定義手法
S220010050		IT 基盤構築プロセス
S230030050	（保守・運用）システム保守・運用・評価	アプリケーションシステムの受け入れ
S230030080		システム運用方式技法
S230030100		システム管理計画
S230030110		システム管理技術
S230030140		システム管理製品
S230030150		運用管理ソフト製品
S230030170		運用システムの改善
S230030180		運用に関するシステム評価
S230030190		性能管理
S230030200		障害時運用方式
S230030210		災害対策
S230030220		構成管理

S230030230		保守技術
S230030240		メンテナンス
S230030250		保守・廃棄
S240020010	(非機能要件) セキュリティ の基礎技術	情報セキュリティ
S240020020		情報保証と情報セキュリティ
S240020030		情報倫理とセキュリティ
S240020040		セキュリティ・アーキテクチャ技術
S240020050		アプリケーションセキュリティ
S240020060		情報プラットフォームのセキュリティ技術
S240020070		ネットワークのセキュリティリスク
S240020080		暗号技術
S240020090		セキュリティと個人情報
S240020100		保証、信用、信頼のメカニズム
S240020110		セキュリティ技術の理解と活用
S240030010	(非機能要件) セキュリティ の構築技術	セキュリティ方針の策定
S240030020		セキュリティ対策基準の策定
S240030030		情報セキュリティ対策
S240030040		セキュリティ実装技術
S240030050		セキュリティシステムの計画策定
S240030060		セキュリティシステムの要件定義
S240030070		セキュリティシステムの設計
S240030080		セキュリティシステムの実装、検査
S240030090		コンピュータ・フォレンジクス（証拠保全追跡）
S240040010	(非機能要件) セキュリティ の利用技術	セキュリティシステムの運用管理
S240040030		システム運用・保守技術（セキュリティ）
S240040040		セキュリティ障害（事件事故/ｲﾝｼﾃﾞﾝﾄ）管理
S240040050		情報セキュリティ管理
S240040060		情報セキュリティ監査の実施・支援
S240040070		セキュリティ技術評価
S240040080		セキュリティの分析
S240040090		セキュリティの見直し（ｾｷｭﾘﾃｨｼｽﾃﾑの評価と改善）
S240040100		コンテンツセキュリティ技術

表　求められるスキル（関連知識）

スキル項目コード	スキル分類	スキル項目
S310020050	企業活動	情報セキュリティ監査
S310030010	法規・基準・標準	セキュリティ関連法規
S310030040		労働関連・取引関連法規

2）抽出スキルの整理

鉄道分野と同様に、抽出したスキル項目から、スキル分類の重複を除き、並べ替えると、下表のとおりとなる。

表　抽出スキルの整理結果

スキルカテゴリ	分類	スキル分類
メソドロジ	（企画）	要求分析手法
		非機能要件設計手法
	（実装）	アーキテクチャ設計手法
		ソフトウェアエンジニアリング手法
		カスタマーサービス手法
	（利活用）	サービスの運用
	（支援活動）	品質マネジメント手法
		リスクマネジメント手法
		資産管理手法
		事業継続計画
		情報セキュリティ
テクノロジ	（システム）	ネットワークの基礎技術
		ネットワークの構築技術
		ネットワークの利用技術
		クラウドコンピューティングの利用技術
	（開発）	システムアーキテクティング技術
	（保守・運用）	システム保守・運用・評価
	（非機能要件）	セキュリティの基礎技術
		セキュリティの構築技術
		セキュリティの利用技術
関連知識		企業活動
		法規・基準・標準

3）学習内容の整理

鉄道分野と同様に、抽出したスキルから、システムの維持管理及びインシデント対応に必要と考えられる学習内容を整理する。

学習内容（スキル分類）を整理した結果を以下の表に示す。

表　学習内容（スキル分類）の整理

スキルカテゴリ	分類	スキル分類
メソドロジ	（支援活動）	品質マネジメント手法
		リスクマネジメント手法
		資産管理手法
		事業継続計画
		情報セキュリティ
テクノロジ	（システム）	ネットワークの基礎技術
		ネットワークの利用技術
		クラウドコンピューティングの利用技術
	（非機能要件）	セキュリティの基礎技術
		セキュリティの利用技術
関連知識		企業活動
		法規・基準・標準

この結果をもとに、鉄道分野と同様の方針で学習内容を整理した。なお、鉄道分野においても、同様の手順で、学習内容としてスキル分類とスキル項目を定義したが、スキル項目レベルまでの抽出の結果は航空分野と共通となった。

表　学習内容の定義

スキル項目コード	スキル分類	スキル項目
S150010010	(メソドロジ) 品質マネジメント手法	テスト技術・手法
S150010020		テストのマネジメント手法
S150030010	(メソドロジ) リスクマネジメント手法	リスク管理手法
S150030020		情報セキュリティ管理手法
S150060010	(メソドロジ) 資産管理手法	資産管理に関する手法
S150080010	(メソドロジ) 事業継続計画	BCP 策定手法
S150080020		災害対策管理手法
S150120050	(メソドロジ) 情報セキュリティ	リスク分析手法
S150120060		情報セキュリティポリシー策定手法
S210160010	(テクノロジ・システム) ネットワークの基礎技術	ネットワーク
S210160050		ネットワーク方式
S210160060		通信プロトコル
S210160070		データ通信と制御
S210180010	(テクノロジ・システム) ネットワークの利用技術	ネットワーク管理
S210180030		ネットワーク製品知識
S210180040		業界固有のセキュリティ要件、事例
S210210010	(テクノロジ・システム) クラウドコンピューティングの利用技術	インタークラウド技術
S210210020		クラウドコンピューティング利用
S210210030		クラウドシステムの監視技術
S240020010	(テクノロジ・非機能要件) セキュリティの基礎技術	情報セキュリティ
S240020020		情報保証と情報セキュリティ
S240020030		情報倫理とセキュリティ
S240020050		アプリケーションセキュリティ
S240020060		情報プラットフォームのセキュリティ技術
S240020070		ネットワークのセキュリティリスク
S240020080		暗号技術
S240020090		セキュリティと個人情報
S240020100		保証、信用、信頼のメカニズム
S240020110		セキュリティ技術の理解と活用
S240040010	(テクノロジ・非機能要件) セキュリティの利用技術	セキュリティシステムの運用管理
S240040040		セキュリティ障害（事件事故/ｲﾝｼﾃﾞﾝﾄ）管理
S240040050		情報セキュリティ管理
S310020050	(知識関連) 企業活動	情報セキュリティ監査
S310030010	(知識関連) 法規・基準・標準	セキュリティ関連法規
S310030040		労働関連・取引関連法規

３．３　国内外のカリキュラムの事例収集

「3.2 学習内容の検討」では、昨年度の手引書の対策をもとに、i コンピデンシディクショナリからある程度自動的に学習する項目が抽出されたが、これに対して、不足する点や修正すべき点などを確認し、カリキュラムをさらに優れたものとするために、既存の国内外のサイバーセキュリティ人材育成に関する事例などを収集して、各分野共通、鉄道分野、航空分野ごとで整理する。また、海外事例の一環として、International Security & Defense Systems Ltd.（ISDS 社）へのヒアリングを実施する。

なお、これらの事例整理で得られた知見は、後述の「3.5　学習内容の決定」にて、学習内容の整理結果に反映させる。

３．３．１　各分野共通

各分野共通の事例として、以下の資料を収集した。

（1）中核人材育成プログラム（独立行政法人情報処理推進機構）
（2）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
（3）サイバーセキュリティ人材育成プログラム
（4）情報セキュリティ読本　プレゼン資料
（5）工学分野における理工系人材育成の在り方に関する調査研究
（6）サイバーセキュリティ経営ガイドライン

（1）中核人材育成プログラム

資料名：中核人材育成プログラム　カリキュラム全体像
発行元：独立行政法人情報処理推進機構
発行日：2017 年
参照先：http://www.ipa.go.jp/files/000057330.pdf

概要を以下に示す。

中核人材育成プログラムについては、通常、テクノロジ（OT・IT)、マネジメント、ビジネス分野を総合的に学ぶ１年程度のトレーニングとなっている。将来、企業などの経営層と現場担当者を繋ぐ中核人材を担う人材を対象とし、受講者が自社に近い環境での演習を体験できるよう、各業界のシステムを想定した模擬システムを使用している。

同プログラムは開講式後、３か月間はプライマリー（レベル合わせ）とし IT セキュリティ基礎と OT セキュリティ基礎を学習する。次の４か月間は、ベーシック（基礎演習）とし制御システムセキュリティ・IT セキュリティ・事業継続計画（BCP）などの考え方を網羅的に学ぶ。その後の３か月はアドバンス（上級演習）とし、実践的なトレーニング及び演習を実施し、更なる知見の向上を目指す。最後の２か月間は卒業プロジェクトとし、習得した知識や経験を活かし、個人及びグループで演習を企画立案し修了式を迎える流れとなる。

受講期間中には、海外のトップレベルのセキュリティ対策ノウハウの獲得などを目的に、海外関連機関との連携トレーニングも行っている。具体的には、米国国土安全保障省（DHS）の制御システムセキュリティの担当部門である Industrial Control System Computer Emergency Response Team（ICS-CERT）が提供するプログラムを、米国から招聘した講師の指導のもと、本場のトレーニングを体験する。制御システムに対する攻撃が実際にどのように開始され、どのように行われるかを理解するとともに、制御システムのサイバーセキュリティ対策を向上する戦略を紹介している。

また、海外におけるサイバーセキュリティを直接学ぶための派遣演習も行われている。現地の産業界・大学の研究者や行政担当者による講演や、意見交換を通じて、欧州の最先端の知見を習得し、サイバーセキュリティの国際的な標準を理解するとともに、現地のキーパーソンとの人脈を構築する内容である。

本プログラムを受講することによる効果として以下が挙げられている。

・自社システムの安全性・信頼性を客観的に評価し、自社のサイバーセキュリティ戦略の立案や経営リスク・財務リスクなどを含めた自社内幹部への説明が可能となる。
・リスク評価の結果に基づき、影響の大きさや緊急性を見極め、対策の要不要や優先順位を養う判断が身に付く。
・経営層と現場担当者の双方とのコミュニケーションを円滑にし、必要な対策を素早く確実に実行に移すことできる。
・最新のサイバー攻撃の傾向に精通し、他業界や海外の対策状況などを把握し、自社の対策

立案に効果的に反映できる。

・他業界、海外の関係業界、専門家などにネットワークを持ち、最新かつ正確な情報を収集できる。

・実装するサイバーセキュリティ対策の安全性・信頼性や必要な技術・コストを精査でき、内製化すべきもの・外部委託すべきものを見極めて、対策を効率的かつ確実に導入できる。

・自社の業務やシステムの特徴を踏まえ、必要な要求事項を盛り込んだ仕様書を作成できる。

・提供サービスの質を適切に評価（担当者の技量に依存せず必要な観点をカバーしているか、信頼できる製品を使用している否か、コストに見合う内容など）でき、外部委託先を適切に管理できる。

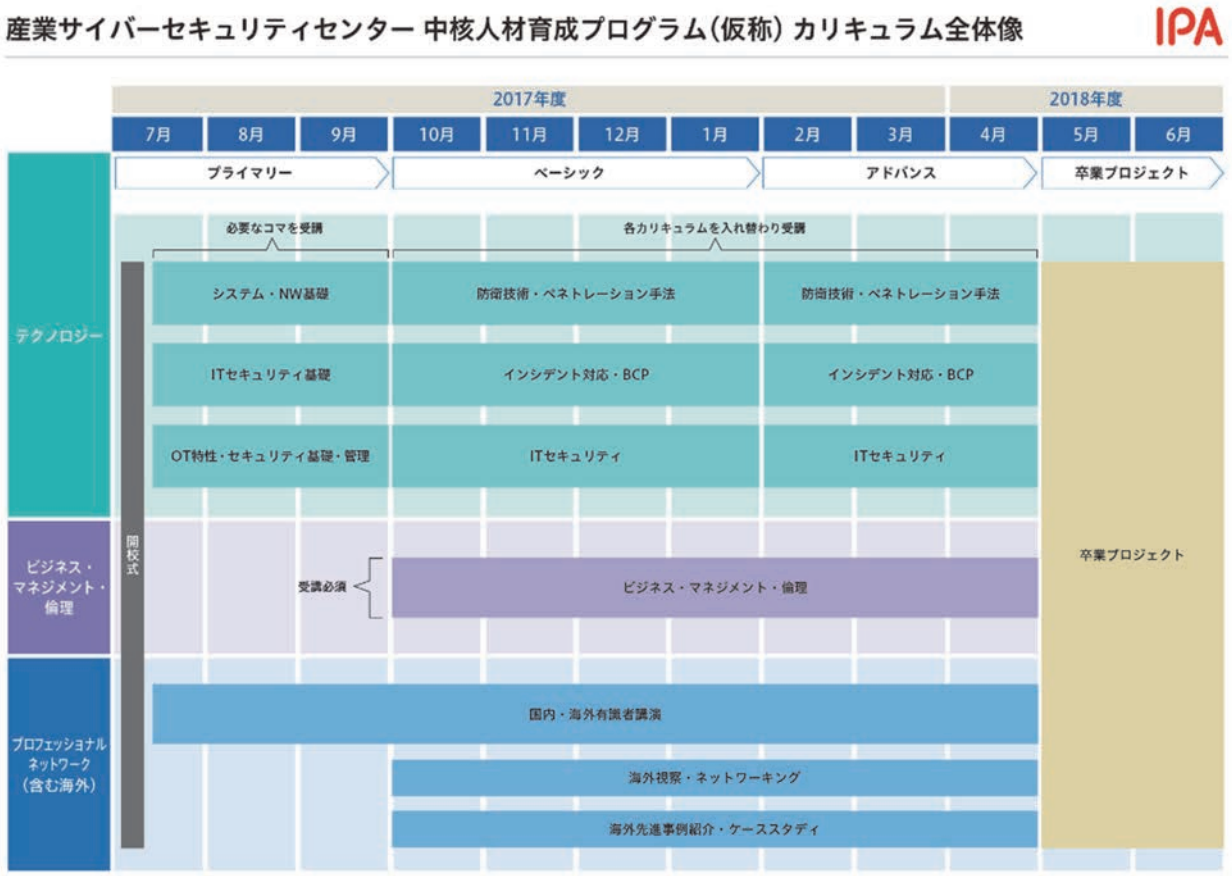


図　中核人材育成プログラム　カリキュラム全体像[注1)]

注1）中核人材育成プログラム　カリキュラム全体像、独立行政法人情報処理推進機構、(http://www.ipa.go.jp/files/000057330.pdf)

（２）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

資料名：「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
発行元：独立行政法人情報処理推進機構
発行日：2013 年 4 月
参照先：https://www.ipa.go.jp/security/fy24/reports/jinzai/index.html

概要を以下に示す。

平成 23 年度に実施された経済産業省「制御システムセキュリティ検討タスクフォース」での議論において、制御システムのセキュリティ対策を行う人材育成の必要性が挙げられている。

このような状況を踏まえ、我が国の制御システム分野の情報セキュリティ人材育成の促進を目的に、制御システム分野の人材に必要な情報セキュリティに関する知識やスキルを調査するとともに、人材育成のためのモデルカリキュラムなどの作成が行われている。

国内調査では、制御システムを扱う分野に属し、制御システムの運用や開発を行う民間企業、または地方公共団体、公益法人の 15 組織を対象に、制御システムのセキュリティ確保への取組み、セキュリティ人材を中心とした人材育成の実態についてインタビュー調査を行っている。

制御システムにおけるセキュリティ確保の取組みについては、「現場での気付き」「ログによる検知」「隔離し、機器の接続前にチェックする」といった運用上の対策が実施されていることが明らかとなっている。

制御システムに関わる人材に対するセキュリティ教育については、ベンダ・ユーザのいずれにおいても、カリキュラムは整備されておらず、社内の少数の専門家の指導や社外講習が主になっていることが明らかとなっている。

モデルカリキュラムは、制御システムの運用や構築に従事する者に必要な情報セキュリティに関する知識項目・スキルについての整理をもとにしたカリキュラムを作成するための雛形をとりまとめたものであり、制御システムのユーザー企業の技術者と制御システムのベンダー企業の技術者を主な対象者に想定し、対象の立場と職務の内容を大掴みに捉えて、4 コース（基礎 1 コース及び応用 3 コース）を作成している。

１）制御システムセキュリティ（基礎）
２）制御システムセキュリティマネジメント
３）制御システムセキュリティ技術（運用・保守）
４）制御システムセキュリティ技術（開発・構築）

９制御システムセキュリティ（基礎）コースの冒頭の３講座は、制御システムを取り巻く現状認識と脅威について取り扱うもので、経営層やオペレーターに向けた普及啓発資料を作成する際に活用可能であるとしている。また、教育を推進する上での課題として下記の点が挙げている。

１）制御システムセキュリティの特徴的知識の継続的な抽出
２）経営者層への普及啓発（理解の促進及び危機意識の醸成）

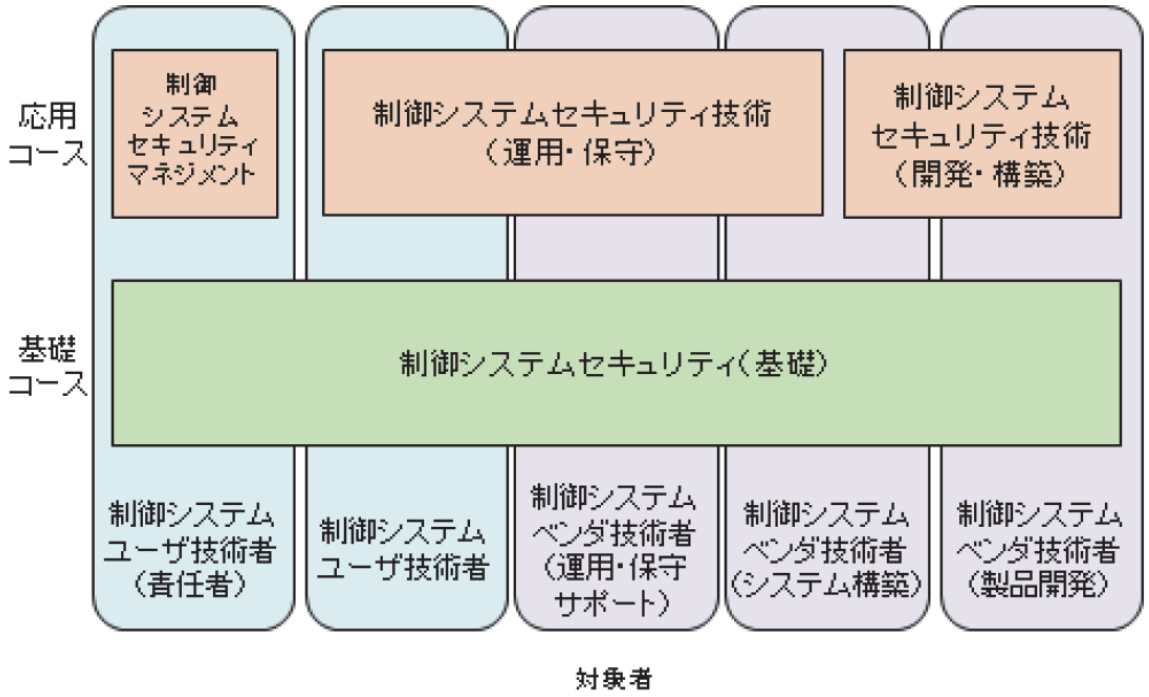


図　モデルカリキュラムのコースと対象者[注1)]

注1）「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　研修モデルカリキュラム、独立行政法人情報処理推進機構、（https://www.ipa.go.jp/files/000026688.pdf）

（3）サイバーセキュリティ人材育成プログラム

資料名：サイバーセキュリティ人材育成プログラム
発行元：内閣府サイバーセキュリティセンター
発行日：2017 年 4 月
参照先：www.nisc.go.jp/active/kihon/pdf/jinzai2017.pdf

概要を以下に示す。

サイバー攻撃は、情報などの窃取、社会システムの機能不全により、国民生活、さらには国際社会が危機にさらされる原因となり得るため、あらゆる主体がサイバーセキュリティに対する認識を深め、各主体の協力的かつ自発的な取組を通じて、その脅威に対処できる安全な空間としていかなければならない、という認識のもと、同プログラムは、企業をはじめとする社会で活躍できるサイバーセキュリティに関連する人材育成の方向性を示すことにより、安全な経済社会の活動基盤としてのサイバー空間の形成に向けた環境整備を図るものであるとしている。

具体的には、産学官の連携により、サイバーセキュリティ人材の「需要」と「供給」の好循環を形成するため、サイバーセキュリティ人材を取り巻く課題を明らかにし、それに対する産学官の人材育成戦略の方向性を示しており、さらに、将来を視野に入れて、ビジネスにおけるイノベーション（革新）を実現するために必要なサイバーセキュリティ人材の育成や、若年層に必要な教育の在り方についても示している。

対象については、企業をはじめとする社会で活躍できる人材の育成に向け、サイバーセキュリティを専門とする人材のみならず、ユーザー企業なども含めた幅広い役割を持つサイバーセキュリティに係る人材育成を想定している。

同プログラムの基本方針として、適切な認識の下でサイバーセキュリティ人材が活躍できるような雇用とキャリアパスを確保するという人材の「需要」と、教育などを通じ、確かな知識と実践力を備え、こうした知識や能力が資格・評価基準などによって可視化され、業務経験を積み重ねることによる人材の「供給」を相応させ、好循環の形成を促進することとしている。

同プログラムで示された課題には、

・サイバー攻撃の脅威が高まっている中、2020 年東京五輪大会を見据え、サイバーセキュリティ技術の専門人材の確保は引き続き重要な課題である
・近年では、サイバーセキュリティ人材の育成を含めた体制の構築が課題となっている
・経営層のリーダーシップがこれまで以上に求められるほか、経営層と現場担当者との橋渡し人材層の配置・育成や、様々な役割を持った人材がチームとなってサイバーセキュリティに取り組めるようにしていくことが必要である

と記載されている。

（4）情報セキュリティ読本　プレゼン資料

資料名：情報セキュリティ読本　教育用プレゼン資料 発行元：独立行政法人情報処理推進機構 発行日：2014 年 参照先：https://www.ipa.go.jp/securITy/publications/dokuhon/ppt.html

概要を以下に示す。

情報セキュリティ読本　教育用プレゼン資料は、独立行政法人情報処理推進機構が企業内の社員教育、学校での授業、各種セミナーや研修などで利用できるように作成した教育用スライド資料である。

具体的には、Web サイトの改ざん、インターネットに潜む危険、迷惑メール、マルウェアによる感染などの対処法として、情報セキュリティの基本や情報通信社会で必要とされる道徳やモラルを知る情報倫理が不可欠であるという認識から、企業内での社員教育、学校での授業、各種セミナーや研修などで利用できるよう、同機構「情報セキュリティ読本 四訂版-IT 時代の危機管理入門-」に準拠した教育用スライド資料を作成している。

第 1 章では今日のセキュリティリスクとして、各種の事例が紹介されセキュリティリスクにおける危険の認識と対策が書かれている。

第 2 章では、情報セキュリティの基礎の説明や外部、内部のリスク要因、情報リテラシーと情報倫理などが明記されている。

第 3 章では、見えない脅威とその対策として、個人レベルのセキュリティ対策、検出されにくいマルウェアの紹介やスマートフォンや、無線 LAN に潜む脅威とその対策などが書かれている。

第 4 章では、組織の一員としての情報セキュリティ対策として、従業員としての心得や情報漏えいなど、情報セキュリティを推進するための体制を組織内に作ることが出発点であることが書かれている。

第 5 章では、セキュリティ技術の活用が紹介されており、アカウント、ID、パスワードの重要性、攻撃の手法や脆弱性を悪用する攻撃、ファイアウォールの仕組み、暗号とデジタル署名について説明がされている。

第 6 章では、情報セキュリティ関連の法規と制度が紹介され、情報セキュリティの国際標準、情報セキュリティに関する法律、知的財産を守る法律、迷惑メール関連法、情報セキュリティ関連制度が書かれている。

なお、第１章、第２章、第４章は、今日の情報セキュリティが置かれている状況、心構えなど、で構成されており、基礎的な内容とされている、また、第３章、第５章は、基礎を踏まえた上での技術的な解説であり、第６章は、法規や制度といった管理者として必要な内容としている。

（５）工学分野における理工系人材育成の在り方に関する調査研究

資料名：工学分野における理工系人材育成の在り方に関する調査研究
発行元：情報セキュリティ大学院大学
発行日：2017 年 3 月

概要を以下に示す。

平成 29 年３月、情報セキュリティ大学院大学が実施した「工学分野における理工系人材育成の在り方に関する調査研究」では、各理工系大学の学部・大学院のカリキュラムが、どの程度産業界のニーズと合っているのか、これらのカリキュラムのどのような点が問題となり得るのかなど、従来の理工系大学教育が抱える問題点などの検証実施が、理工系大学教育のシステム改革を達成する観点から課題となっているという認識から、理工系大学教育のうち近年、特に早急な人材育成システムの確立が求められている情報セキュリティ分野に焦点を絞り、目指すべき情報セキュリティ人材像を検証し、各大学での人材育成に資することを目的としている。

同研究では、政府機関や重要インフラ事業者などへのサイバー攻撃の激化、個人情報漏えい事案の多発化など、情報セキュリティの確保は国家課題となっており、大学における人材育成を推進していくために、国内外の教育の状況を調査するとともに、情報セキュリティに関する知識体系を整理し、教育現場が参照可能な「モデル・コア・カリキュラム」の開発を進めるものある。

同調査研究によって開発する「モデル・コア・カリキュラム」は、教育内容を精選し、学生が学ぶべき知識や技能などの到達目標をわかりやすく提示することにより、教育内容とレベルを確保することを目指すものとしている。今後、「モデル・コア・カリキュラム」を活用した高など教育機関における情報セキュリティ教育について、以下のような方向性に関する提言が行われている。

（抜粋）「情報セキュリティ分野を正しく理解するためには、暗号の基盤となる数学的知識、コンピュータやインターネットの動作原理などの工学的知識、個人情報保護法や不正アクセス禁止法などの法律的知識、さらにサイバー攻撃に関わる国際情勢など、さまざまな学問領域にまたがる知識を総合する必要がある。さらに、社会生活や産業経済において情報セキュリティ分野が関わる脅威は日々増加・深刻化しており、その対策にも取組みが求められている。今回策定されたカリキュラムについても、永続的に有効なものとみなさず、社会のニーズに応じて適宜更新を図っていくことで、人材育成の効果もより高まるものと期待される。

情報セキュリティ分野は複数の学問領域にわたり、教育対象となる知識項目が非常に多いが各々の学問に取り組む中で情報セキュリティ分野の学習に割ける時間には限界があり、産業界ほか社会における活躍の場に応じて、情報の安全な管理や相手を認証するための方法、インシデントへの対応の考え方など、ニーズにあった教育を行う必要がある。」

（6）サイバーセキュリティ経営ガイドライン

資料名：サイバーセキュリティ経営ガイドライン 発行元：経済産業省、独立行政法人情報処理推進機構 発行日：2017 年 11 月 16 日 参照先：http://www.meti.go.jp/policy/netsecurity/downloadfiles /CSM_Guideline_v2.0.pdf

概要を以下に示す。

近年、企業や団体を狙うサイバー攻撃が増加し、情報の漏えいや不正利用により、経営や事業に大きなダメージを与える事故や事件が発生しており、サイバーセキュリティの確保は企業や団体が IT を利活用し、ビジネスを発展させるとともに経営者が果たすべき責任のひとつとして、サイバーセキュリティ対策を講じる必要があるとの認識から、同ガイドラインでは、サイバー攻撃から企業を守る観点で、以下の図に示す、経営者が認識する必要のある「3 原則」、経営者が情報セキュリティ対策を実施する上での責任者となる担当幹部（CISO など）に指示すべき「重要 10 項目」をまとめている。

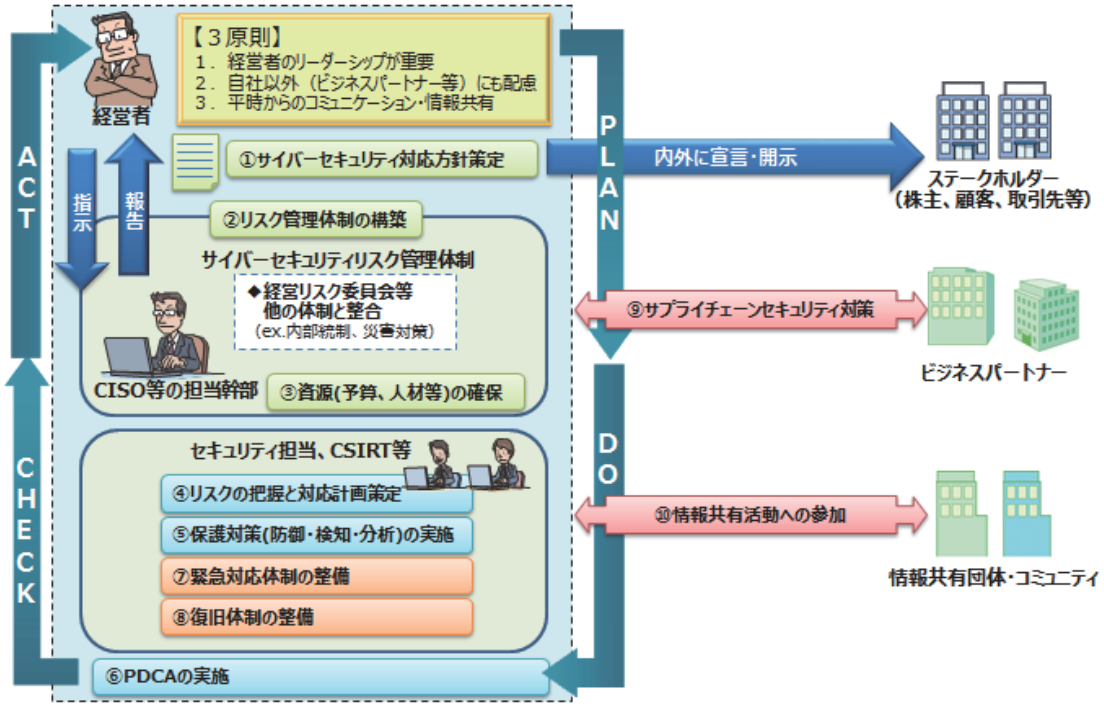


図　サイバーセキュリティ経営ガイドラインの概要図[注1)]

注1）サイバーセキュリティ経営ガイドライン、独立行政法人情報処理推進機構、
（http://www.meti.go.jp/policy/netsecurity/mng_guide.html）

３．３．２　鉄道分野

鉄道分野の事例として、以下の資料を収集した。

（１）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
（２）Rail Cyber Security　Guidance to Industry
（３）Rail Cyber Security Strategy

（1）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

資料名：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
発行元：国土交通省
発行日：2016 年４月１日改訂
参照先：http://www.mlit.go.jp/common/001127563.pdf

概要を以下に示す。

当安全ガイドラインは、同文書において、それぞれの事業分野の特性に応じて必要又は望ましい情報セキュリティの水準を明示することで、個々の事業者が、重要インフラの担い手としての意識に基づいて自主的な取り組みにおける努力や検証をするための目標を定めることを目的としている。

具体的には、重要インフラ分野においてサービス提供継続及び重要インフラ利用者の信頼性に応えるとの観点から、サイバーテロ対策をはじめとして、災害や非意図的要因などサービス提供に影響を及ぼす可能性のある様々な事象を念頭に置き、情報セキュリティ対策を実施する場合に何らかの対処がなされていることが望ましい項目、及び対処すべき内容を列挙している。また、それぞれの事業分野の特性に応じて事業者などが活用し易い基準などとするとの視点から、各事業分野の特性や現状をもとにした、想定事象、対処方針などについて記載されている。

鉄道分野において、国民生活や社会経済活動に影響を及ぼし事業継続の取り組み対象となるような重要システムには、「列車運行管理システム」、「電力管理システム」及び「座席予約システム」などが挙げられており、これらのシステムの障害に対して、緊急の対応として人手による運用が可能であるものの、代替運用時においては作業効率が低下するため、運行ダイヤが乱れるなどの影響が起こることが想定されると記載されている。

また、マルウェア感染や外部からの攻撃を防止する対策については各々実施されているが、昨今の複雑・巧妙化するサイバー攻撃すべてを防ぐことは困難であるため、攻撃され内部に侵入などされることを前提とした情報セキュリティ対策が必要であると記載されている。

さらに、一部の事業者では情報セキュリティ対策の継続的改善の取組みが実施されているものの、実施が不十分という事業者も多いことが想定されるため、ＰＤＣＡサイクルに沿った情報セキュリティ対策の継続的改善の実施が必要であると記載されている。

（2）Rail Cyber Security　Guidance to Industry

資料名：Rail Cyber Security　Guidance to Industry 発行元：英国鉄道標準化委員会 発行日：2016 年 2 月 参照先：https://www.rssb.co.uk/Library/improving-industry-performance/2016-02-cyber-security-rail-cyber-security-guidance-to-industry.pdf

概要を以下に示す。

同ガイダンスでは、サイバーセキュリティに関する継続的な取り組みにより、従業者は以下に必要な知識を得ることができると記載されている。

・自らの役割に応じて適切にサイバーリスクを管理するための情報に基づく意思決定を行う。
・システムのライフサイクル全体を通じてリスクの発生を最小限に抑えて、鉄道を保護する。
・サイバーセキュリティのリスクが鉄道の安全性と信頼性に及ぼす影響を理解する。
・サイバーセキュリティイベント、インシデント、及び疑わしい動作を認識、検出、報告することで、サイバーセキュリティイベントの影響と期間を最小限に抑えることができることを理解する。

サイバーセキュリティに関する能力の育成には、以下のような事柄について取り組むことと記載されている。

・組織や個人の役割に関連するサイバーセキュリティトレーニングプログラムを開発し、既存の知識とスキルを認識し、補完する。
・システムに関わるすべてのライフサイクルフェーズで、異なるトレーニングや模範となる行動規範を満たすようにする。
・サイバーセキュリティの責任を果たす役割の経験、認定または職業化を提供するフレームワーク及び業界見習い制度を検討する。
・サプライチェーンを構成するビジネスパートナーの継続的なサイバーセキュリティに関する取り組みを評価する。
・サイバーセキュリティの有能な才能を自社で開発し、育成し、維持するか、必要に応じて新しい才能を採用する。
・能力の育成方法と模範となる行動規範の枠組みを、組織や幅広い業界で共有する。安全、物理的なセキュリティ及びその他の作業実務のための行動規範の管理は、サイバーセキュリティトレーニングと従業員の行動規範を管理するモデルとして使用できる。

トレーニングには、必要な知識のレベルと範囲に応じて以下を含める必要があると記載されている。

・サイバーセキュリティの意識
・問題の内容の理解
・安全性と安全性を考慮する必要がある理由の理解
・制御システムのセキュリティがＩＴシステムのセキュリティと異なる理由の理解
・展開、運用、保守だけでなく、ライフサイクル全体を考慮する必要性
・継続的な侵入テストの要件
・安全性ケースへの影響を最小限に抑えること
・他のセクターとの比較
・脆弱性管理（パッチ適用、オペレーティングシステム（OS)、ファームウェア及びアプリケーションコードを含む)
・インストールされたウイルス対策ソフトウェアによるチェック、システム変更の問題、システム／ネットワーク境界の認識を取得する前に、メーカーの機器テストの重要性

（3）Rail Cyber Security Strategy

資料名：Rail Cyber Security　Guidance to Industry
発行元：英国鉄道標準化委員会
発行日：2016 年 2 月
参照先：https://www.rssb.co.uk/Library/improving-industry-performance/2016-02-cyber-security-rail-cyber-security-guidance-to-industry.pdf

概要を以下に示す。

同文書では、以下の実施を推奨している。

・組織内のサイバーセキュリティの現状を理解し、それを改善する手法を定義する。
・サイバーセキュリティへの意識と決まり事を積極的に実証することによって、組織のあらゆるレベルで模範を作成し、良好なセキュリティ動作を奨励する。
・サイバーインシデントの報告が奨励され、社員の信頼に基づいた文化を創造する。
・社内外の利害関係者と良好な作業の実践と経験を共有して、鉄道業界において優れた事例を確立する。

さらに、重要なこととして、適切なサイバーセキュリティ機能を開発する企業担当者が、鉄道の運用システムを担当する鉄道会社社員に対し、それらを適切に取り扱う方法を指導し、理解させる訓練を実施することで、サイバーセキュリティの向上、サイバー攻撃による脅威への意識向上、担当者による情報に基づく意思決定が可能となると記載されている。
同文書では、サイバーセキュリティのリスクを管理する上で重要なことは、極めて有能に訓練された鉄道会社の担当者が職務を担うことであるとしている。なお、担当者の継続的な訓練内容には、以下のような知識が含まれる事が望ましいと記載されている。

・自らの役割に応じて、適切に意思決定を行う必要があることを理解する。
・鉄道のサイバーセキュリティリスク、技術環境及び事業目的、及び事象を特定し、適切に対処する方法を理解する。
・システムのライフサイクル全体を通して、リスクの発生を最小限に抑えて、鉄道を保護する。
・サイバーセキュリティのリスクが、鉄道の安全性と信頼性に及ぼす影響を理解する。
・サイバーセキュリティイベント、インシデント、及び疑わしい動作を認識、検出、報告することで、サイバーセキュリティイベントの影響と期間を最小限に抑えることが可能となることを理解する。
・サプライチェーンの管理など、サプライチェーンのセキュリティ対策をすることの重要性を理解する。

３．３．３　航空分野

航空分野の事例として、以下の資料を収集した。

（１）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
（２）Aviation Cyber Security Toolkit

（1）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

資料名：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 発行元：国土交通省 発行日：2016 年４月１日改訂 参照先：http://www.mlit.go.jp/common/001127526.pdf

概要を以下に示す。

当安全ガイドラインは、同文書において、それぞれの事業分野の特性に応じて必要又は望ましい情報セキュリティの水準を明示することで、個々の事業者が、重要インフラの担い手としての意識に基づいて自主的な取り組みにおける努力や検証をするための目標を定めることを目的としている。

具体的には、重要インフラ分野においてサービス提供継続及び重要インフラ利用者の信頼性に応えるとの観点から、サイバーテロ対策を初めとして、災害や非意図的要因などサービス提供に影響を及ぼす可能性のある様々な事象を念頭に置き、情報セキュリティ対策を実施する場合に何らかの対処がなされていることが望ましい項目、及び対処すべき内容を列挙している。また、それぞれの事業分野の特性に応じて事業者などが活用し易い基準などとするとの視点から、各事業分野の特性や現状をもとにした、想定事象、対処方針などについて記載されている。

航空運送分野において、国民生活や社会経済活動に影響を及ぼし事業継続の取り組み対象となるような重要システムは、「運航システム」、「予約・搭乗システム」、「整備システム」、「貨物システム」などが挙げられており、これら重要システムの障害については、緊急の対応として手作業などによる代替の運用が可能であるものの、代替運用時においては作業効率が低下するため、システム利用頻度の高い大空港などでは時間とともに運航などへの支障が発生することが想定されると記載されている。

航空運送分野はその事業特性から、顧客向けのウェブサービス（座席予約など）を保有している事業者も多いが、昨今パスワードリスト攻撃[30]による顧客情報の流出・不正操作というＩＴ障害が発生しているとし、情報セキュリティ対策については、各事業者において情報セキュリティに対応する文書や組織体制の整備・見直し、事業者内ネットワーク及び情報システムの情報セキュリティ対策強化・見直し、職員への啓発活動など、セキュリティ基準（ISMS[31]など）をベースにした対策が進められていると記載されている。

航空分野の情報セキュリティ対策における課題として、航空運送分野の事業者は、マルウェア感染や外部からの攻撃を防止する対策については各々実施しているが、パスワードリスト攻撃や標的型攻撃をはじめとする昨今の複雑、巧妙化するサイバー攻撃すべてを防ぐことは困難であるため、攻撃され内部に侵入などされることを前提とした情報セキュリティ対策が必要であると記載されている。

また、情報セキュリティ対策の継続的改善の実施が不十分という課題認識があるとし、ＰＤＣＡサイクルに沿った情報セキュリティ対策の継続的改善の実施が必要であると記載されている。

（２）Aviation Cyber Security Toolkit

資料名：Aviation Cyber Security Toolkit
発行元：国際航空運送協会（IATA）
参照先：http：//www.iata.org/publications/store/Pages/aviation-cyber-security-toolkit.aspx

概要を以下に示す。

同ツールキットは、国際航空運送協会（IATA）が航空業界向けサイバーセキュリティ対策として提供している。

同ツールキットは、所属する組織が情報やシステムを保護するための判断を決定する際に役立つものとされており、これを用いて、サイバー犯罪を防止するための第一の重要なステップである意識啓発トレーニングから、今日のサイバー犯罪者が使用する一般的な攻撃方法と、航空システムの潜在的な脆弱性について学ぶことが可能である。また、事例やＩＴの専門家による予行演習から得た知見を使用して、航空ビジネスでリスク評価を実施する際の正しい質問方法を学習することが可能である。

多くの航空会社や空港には、一般的なハッキング[32]の脅威に対処するための堅牢なシステムが備わっているが、より広範な航空ＩＴインフラへの全体的な取り組みが更に必要であるとの認識から、同ツールキットは、主要な利害関係者が共通の枠組みに向けて作業するためのプラットフォームとして以下のような内容を提供している。

・現在のサイバー脅威の状況
・スニファ攻撃[33]、内部脅威[34]、トロイの木馬[35]、アイデンティティのなりすまし[36]、及びアップストリーム攻撃[37]を含む一般的な攻撃方法
・航空会社のシステムと脆弱性
・実際のサイバーセキュリティ事件から学んだ教訓
・国際民間航空機関（ICAO）の付属書、EUの共通安全保障、防衛政策を含む国際的な規則や法律
・サイバー脅威評価とリスク管理

また、当ツールキットに記載されたカリキュラムは、下記のとおりである。

・航空分野の現状
・サイバーセキュリティの脅威
・サイバーセキュリティリスクとその軽減策
・サイバーセキュリティ管理システムの実装方法
・リスク評価と優先順位付けの指示を行うための教材へのアクセス提供

３．３．４　International Security & Defense Systems Ltd.へのヒアリング

対応者：	International Security & Defense Systems Ltd（ISDS） トマー・フルマン，CEO， シャロム・ドレフ，Director Security Systems，
目　的：	世界的メガスポーツイベントのセキュリティに関わった経験から、サイバーセキュリティにおける人材育成についての知見を得ること
日　時：	2017 年 12 月 8 日
場　所：	一般財団法人運輸総合研究所

（１）概要

リオオリンピック・パラリンピック（以下、リオ五輪大会）を始め、多くの世界的メガスポーツイベントにおいて、セキュリティに関わっている ISDS 社に、サイバーセキュリティにおける人材育成についてヒアリングを実施した。

（２）ISDS 社について

ISDS 社は、イスラエルの警備会社である。国土安全保障、防衛、海事及び航空安全保障、インフラ、メガイベントなどのセキュリティ分野において、世界的に展開するセキュリティコンサルタント及びインテグレータである。

リオ五輪大会では、オリンピック公式スポンサー並びに公式サプライヤーに選ばれている。

（３）ヒアリング内容

１）インシデント対応に関わる現場の社員教育について

サイバーセキュリティにおいて、制御系システムのオペレーションについては、ベンダーに頼らないことを推奨する。その理由は、制御系システムのオペレーションや堅牢さについては信頼できるベンダーであっても、サイバーセキュリティの意識や理解をもっているかどうかについては分からないからである。そういったリスクを軽減するために、多層防御[38]が重要である。

また、制御系システムは散在しており、複数分野の専門家で体制を構築する必要があること、各専門家は理論ではなく実際の攻撃者の視点を理解する必要があること、専門家はチーム対応を基本としてリスク評価を実施し、是正の提案を行うことが必要である。

２）現場の社員の能力について

リオ五輪大会において、言語も文化も異なる人を対象に、どういった教育や訓練を実施したのか、その留意点については、重要ポジションである現地の人々に対して、充分な教育や訓練を実施するには、充分な時間がないというのが正直な感想である。リオ大会においては、現場の社員の能力の開発に取り組んだ。トレーニング実施者がいれば、適切な方法論を用い、それを踏襲することで、人々を適切なレベルまで向上させることができる。

現場の社員の育成対象は、大きく３つあり、その教育内容は、次のようなものである。

①コンピュータシステム全てのユーザー

職場環境に応じたサイバーセキュリティの意識教育

②IT 専門家

サイバーセキュリティの側面（例えば、ネットワークやシステムなどの問題）の教育

③サイバーセキュリティの専門家

・セキュリティ実装とオペレーション：サンドボックス[39]やファイアウォールなどのセキュリティシステムの検証やルール設定、矛盾なく可用なオペレーション

・監査：脆弱性評価

・CSOC[40]：検出、リスク分析、レスポンス責任者（誤検知の判断、回復）

・コンピュータ・フォレンジック[41]

3）経営者層に対する啓発について

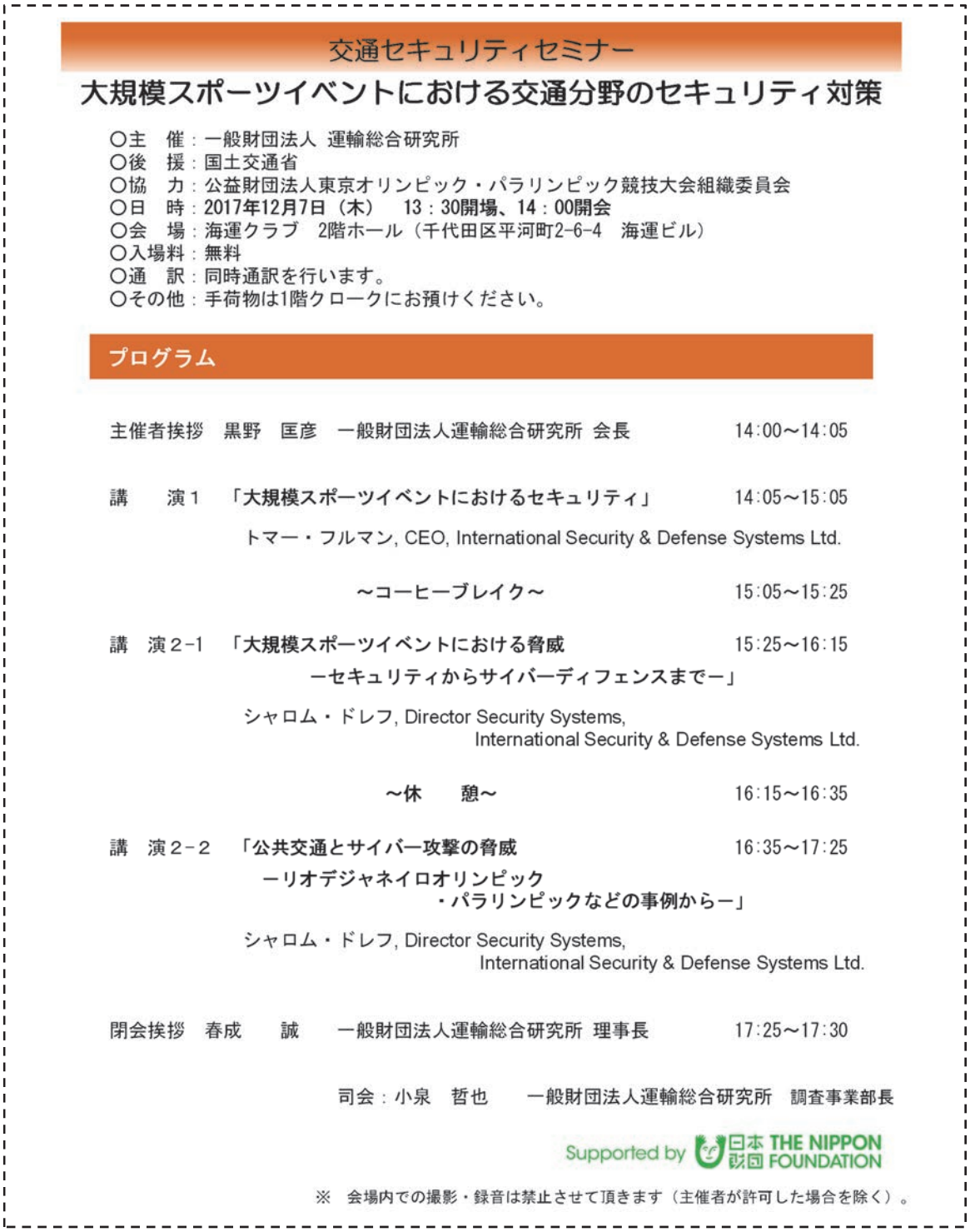
経営者層に対する啓発については、リスク解析の実施が最も重要であると考える。リスク解析によって、自社の脆弱性による影響損失を可視化・定量化し、その要約した情報を経営者にエスカレーション[42]することが必要である。影響損失は、①物理的損失、②経済的損失、③潜在的損失、がある。これらを具体的な数字、図表、写真、実際の事例を用いてレポートを作成し、適切なコストを投資しなかったために生じる損失を明らかにすることによって、経営者の責任ある経営判断を醸成することが可能になると考える。もう一つの方法は、「ホワイトハッカー[43]による訓練」である。例えば、不審なメールを送付し、クリックしてしまったらどうなるかを体験してもらう。実際に訓練をすることによって、（どれだけ脅威に晒されているか）現状を知る機会となる。

4）制御システムのオペレーターに対するサイバーセキュリティ対策の教育について

昨今は産業用制御システム（ICS）に対する重大な攻撃事例も出ている。コントロールシステムのメンテナンス担当者に対して、サイバーセキュリティのトレーニングは、大変重要である。メンテナンス担当者へのトレーニングは、前述の現場の社員の能力における「①コンピュータシステム全てのユーザー」に該当し、職場環境に応じたサイバーセキュリティの意識教育は、非常に重要である。事例を詳細に技術的に見せ、注意深く対応しなくてはいけないことを喚起し、テストを実施する。

各事業者のシステムに対する①規則、②手順、③優良事例、を調査し、それらを踏まえた上で、実践的トレーニングの策定が必要である。ICS は多様である。20 年以上が経過するレガシーシステム[44]も、構築して間もない新しいシステムも存在する。様々なシステムが混在している。個別の状況に合わせる必要がある。

本調査研究では、ヒアリングとともに、鉄道分野、航空分野のサイバーセキュリティ対策の必要性、重要性を広く周知することを目的として、ISDS 社のヒアリング対応者を講師として招き、同社のリオ五輪大会でのセキュリティ対策の経験等を講演する、「交通セキュリティセミナー　大規模スポーツイベントにおける交通分野のセキュリティ対策に関するセミナー」を実施している。プログラムを以下に示す。



交通セキュリティセミナー

大規模スポーツイベントにおける交通分野のセキュリティ対策

○主　催：一般財団法人 運輸総合研究所
○後　援：国土交通省
○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：2017年12月7日（木）　13：30開場、14：00開会
○会　場：海運クラブ　2階ホール（千代田区平河町2-6-4　海運ビル）
○入場料：無料
○通　訳：同時通訳を行います。
○その他：手荷物は1階クロークにお預けください。

プログラム

主催者挨拶　黒野　匡彦　一般財団法人運輸総合研究所 会長　14:00～14:05

講　演１　「大規模スポーツイベントにおけるセキュリティ」　14:05～15:05
トマー・フルマン, CEO, International Security & Defense Systems Ltd.

～コーヒーブレイク～　15:05～15:25

講　演２-１　「大規模スポーツイベントにおける脅威　15:25～16:15
ーセキュリティからサイバーディフェンスまでー」
シャロム・ドレフ, Director Security Systems,
International Security & Defense Systems Ltd.

～休　憩～　16:15～16:35

講　演２-２　「公共交通とサイバー攻撃の脅威　16:35～17:25
ーリオデジャネイロオリンピック
・パラリンピックなどの事例からー」
シャロム・ドレフ, Director Security Systems,
International Security & Defense Systems Ltd.

閉会挨拶　春成　誠　一般財団法人運輸総合研究所 理事長　17:25～17:30

司会：小泉　哲也　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）。

図　交通セキュリティセミナーのプログラム

３．３．５　得られた知見

（1）各分野共通

1）中核人材育成プログラム

サイバーセキュリティに対応するため人材の育成に関し、中核人材の育成の考え方を参考にした。得られた知見は以下のとおりである。

・プライマリー（レベル合わせ）な知識として、下記から必要なものを受講するようにしている。
  ・システム・ネットワーク基礎
  ・IT セキュリティ基礎
  ・OT 特性・セキュリティ基礎・管理
・ベーシック（基礎演習）な知識として、下記を受講するようにしている。
  ・防衛技術・ペネトレーション手法[45]
  ・インシデント対応
  ・事業継続計画（BCP）
  ・IT セキュリティ
  ・ビジネス・マネジメント・倫理

2）「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

制御システム情報セキュリティ人材の育成に関するモデルカリキュラムの内容を参考とした。得られた知見は以下のとおりである。

・より明確に脅威・リスクを伝えるための工夫が必要との見解があり、攻撃事例を解説する講座を設けている。
・オペレーターについては、期待する役割（必要な教育）は業種や規模により異なる。オペレーターには現場で異常に気付き、担当者を呼ぶことを期待されるため、セキュリティに関する啓発と現場のマニュアル整備が必要としている。技術について知識をつけようとするオペレーターが基礎的なコースを受講・参照することも想定し、特に「現場での気付き」の重要性について記載している。
・モデルカリキュラムは、下記のコースから構成されている。
  ・制御システムセキュリティ（基礎）
  ・制御システムセキュリティマネジメント
  ・制御システムセキュリティ技術（運用・保守）
  ・制御システムセキュリティ技術（開発・構築）
・本カリキュラムにおいては、オペレーターを主対象とはしないが、受講対象者は同様のスキルが必要と考えられる。

3）サイバーセキュリティ人材育成プログラム

サイバーセキュリティに対応するため人材の育成に関し、基本的な考え方を参考にした。得られた知見は以下のとおりである。

・サイバー攻撃の脅威が高まっている中、2020 年の東京五輪大会を見据え、サイバーセキュリティ技術の専門人材の確保は重要な課題である。
・経営層と現場担当者との橋渡し人材層の配置・育成が重要である。
・様々な役割を持った人材がチームとなってサイバーセキュリティに取り組む必要がある。

4）情報セキュリティ読本　プレゼン資料

本カリキュラムの受講に際して受講者が有する前提知識について、参考にした。得られた知見は以下のとおりである。

・受講者は、「第１章　今日のセキュリティリスク」を理解していることが望ましい。
・受講者は、「第２章　情報セキュリティの基礎」を理解していることが望ましい。
・受講者は、「第４章　組織の一員としての情報セキュリティ対策」を理解していることが望ましい。

5）工学分野における理工系人材育成の在り方に関する調査研究

カリキュラム構成の参考とした。得られた知見は以下のとおりである。

本調査研究によって開発する「モデル・コア・カリキュラム」は、教育内容を精選し、学生が学ぶべき知識や技能などの到達目標をわかりやすく提示することにより、教育内容とレベルを確保することを目指す。

6）サイバーセキュリティ経営ガイドライン

カリキュラム構成の参考とした。得られた知見は以下のとおりである。

・ビジネスパートナーや委託先などを含めたサプライチェーン全体の対策及び状況把握
・系列企業やサプライチェーンのビジネスパートナーにおいて適切なサイバーセキュリティ対策が行われていないと、これらの企業を踏み台にして自社が攻撃されることもある
・緊急時の原因特定などの際に、これらの企業からの協力を得られないことにより事業継続に支障が生ずる恐れがある
・システム管理などの委託業務においては、自組織で対応する部分と委託する部分の境界が不明確となり、対策漏れが生じる恐れがある

（２）鉄道分野

１）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

人材育成について言及しており、教育として含むことが望ましい項目として参考にした。得られた知見は以下のとおりである。

・情報の取扱い（格付け及び取扱制限）
・情報セキュリティポリシー
・情報セキュリティへの脅威と対策
・ＩＴ障害発生時の対処手順及び体制

２）Rail Cyber Security　Guidance to Industry

鉄道分野におけるサイバーセキュリティ対応の基本方針を参考とした。得られた知見は以下のとおりである。

・疑わしい場合を含む、サイバー攻撃の事象を迅速に識別するためのメカニズム（事象の検知）を確立する必要がある。
・システムに対して確認されたセキュリティインシデントに対応して適切な措置を取る（インシデント対応）必要がある。
・トレーニングには、必要な知識のレベルと範囲に応じて以下を含める必要がある。
  - サイバーセキュリティの意識
  - 問題の内容の理解
  - セキュリティと安全性を考慮する必要がある理由の理解
  - 制御システムのセキュリティがＩＴシステムのセキュリティと異なる理由の理解
  - 展開、運用、保守だけでなくライフサイクル全体を考慮する必要性
  - 継続的な侵入テストの要件
  - 安全性ケースへの影響を最小限に抑えること
  - 脆弱性管理
  - インストールされたウイルス対策ソフトのチェック、システム変更の問題、システム/ネットワーク境界の認識を取得する前に、メーカーの機器のテストの重要性

３）Rail Cyber Security Strategy

鉄道分野における人材育成の基本的な考え方を参考とした。得られた知見は以下のとおりである。

・自らの役割に応じて適切に意思決定を行う必要があることを理解する。
・鉄道のサイバーセキュリティリスク、技術環境及び事業目的、及び事象を特定し、適切に対応する方法を理解する。
・システムのライフサイクル全体を通じてリスクの発生を最小限に抑えて、鉄道を保護する。
・サイバーセキュリティのリスクが鉄道の安全性と信頼性に及ぼす影響を理解する。
・サイバーセキュリティイベント、インシデント、及び疑わしい動作を認識、検出、報告することで、サイバーセキュリティイベントの影響と期間を最小限に抑えることが可能となることを理解する。
・サプライチェーンのセキュリティ対策をすることの重要性を理解する。

（３）航空分野

１）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

人材育成について言及しており、教育として含むことが望ましい項目として参考にした。得られた知見は以下のとおりである。

・情報の取扱い（格付け及び取扱制限）
・情報セキュリティポリシー
・情報セキュリティへの脅威と対策
・ＩＴ障害発生時の対処手順及び体制

２）Aviation Cyber Security Toolkit

航空分野の人材育成カリキュラムとして、カリキュラムに含めるべき項目の参考にした。得られた知見は以下のとおりである。

・航空分野の現状説明を行う
・サイバーセキュリティの脅威を説明する
・サイバーセキュリティリスクとその軽減策を説明する
・サイバーセキュリティ管理システムの実装方法について説明する

（４）ISDS 社ヒアリング

カリキュラムの構成や留意点に含めるべき項目の参考にした。得られた知見は以下のとおりである。

・昨今は ICS に対する重大な攻撃事例も出ているため、コントロールシステムのメンテナンス担当者に対して、サイバーセキュリティのトレーニングは、大変重要である。
・コンピュータシステム全てのユーザーに対して、職場環境に応じたサイバーセキュリティの意識教育が非常に重要な教育であり、事例を詳細に技術的に見せ、注意深く対応しなくてはいけないことを喚起し、テストを実施することが望まれる。
・各事業者のシステムに対する①規則、②手順、③優良事例、を調査し、それらを踏まえた上で、実践的トレーニングの策定が必要である。

３．４　机上演習の実施

「3.2 学習内容の検討」及び「3.3 国内外の人材育成カリキュラムの事例収集」により、学習内容について既存文献から理論的な整理が出来たものと考えるが、我が国の鉄道分野と航空分野特有の実際の事情が考慮できているかを確認する必要があると考えた。そのため、現時点の学習内容の改善点を洗い出し、それをカリキュラム作成の際に活用することを目的に、それぞれの分野で机上演習を実施した。

なお、机上演習とは、インシデント発生を想定したシナリオに基づき、参加者がそれぞれの立場による討議を展開することにより、既存の対応体制、連絡調整、復旧手順、課題点などを洗い出すものである。ここで得られた知見は、後述の「3.5　学習内容の決定」にて、学習内容の整理結果に反映させる。

３．４．１　実施概要

（１）鉄道分野

第１回：平成 29 年 11 月 1 日（水）　10：00～12：00
内　容：サイバー攻撃への対応基礎能力（勘所）の獲得　など
参加者：19 名（9 社）

第２回：平成 29 年 11 月 21 日（火）　10：00～12：00
内　容：最新の脅威に対応したインシデント調査（攻撃経路や被害範囲の特定）　など
参加者：18 名（9 社）

第３回：平成 29 年 12 月 19 日（火）　10：00～12：00
内　容：サイバー脅威の収集と分析の実践　など
参加者：16 名（8 社）

（２）航空分野

第１回：平成 29 年 10 月 30 日（月）　10：00～12：00
内　容：サイバー攻撃への対応基礎能力（勘所）の獲得　など
参加者：13 名（７社）

第２回：平成 29 年 11 月 20 日（月）　10：00～12：00
内　容：最新の脅威に対応したインシデント調査手法（攻撃経路や被害範囲の特定）　など
参加者：14 名（７社）

第３回：平成 29 年 12 月 13 日（水）　15：00～17：00
内　容：サイバー脅威の収集と分析の実践　など
参加者：14 名（７社）

（参考）机上演習の一般的な流れ

机上演習は通常、討議形式で行なう。ファシリテータ（討議進行担当）は、参加者に対する質問をきっかけとして参加者の発言を促し、参加者間の討議の統制を行う。

討議の基本的な流れとして、まずファシリテータが、参加者に対しスライドや資料配布などを用いて事象発生に至るまでのストーリーを説明する。これは、参加者に対する議論対象の定義を定めるためである。

次に、ファシリテータより、事象への対処検討などに関する質問を参加者に投げかけ討議を開始する。参加者に対し、自由闊達な発言を促すようにする。その後ファシリテータは適宜、討議内容をまとめる。

次に、想定したシナリオに沿って、次のフェーズに移行させるよう統率を行なう。その際ファシリテータは参加者に対し、独自性がある観点の回答を求める。もしくは、新しい討議用の質問をファシリテータは参加者へ提供する。そして、ファシリテータは討議時間を見計らい、参加者による議論の収束をもって、当該シナリオを終了もしくは休憩とする。

最後にファシリテータは、参加者に対し演習の目的達成をフィードバックする。

（参考）机上演習の有用性について

一般に、万が一のインシデント発生に備え、さまざまな取り決めや体制の準備がされ始めている状況の中、特に、事業継続計画（BCP）においては、災害、事故、装置の故障及び悪意による行為などの緊急事態の発生時を想定し、事業の中断を防ぐ措置や、中断した場合でも、組織の被る損失を極小化するための復旧対応をあらかじめ取り決める計画が策定されている。

これらの体制や計画の実効性を高めるためには、テストを重ねる必要があり、さらに、最近の情報システムへの依存度の高まりや組織間情報ネットワークの複雑化、操作の容易性、そして技術の高度化を鑑みると、情報セキュリティに係るインシデント（あるいは、BCP における緊急事態）の発生に対するテスト及び検証、さらには改善を検討する場の必要性はより高くなってきている。

机上演習とは、公開されている関連情報をもとに、自己が所属する組織への影響の有無や発生したインシデントに対する問題抑止のためのセキュリティ対策を検討するものであり、インシデント発生に対する対策のテスト及び検証、さらには改善を検討する場として、有用であるとされている。

３．４．２　事前アンケート

実施に際しては、机上演習の適切性及び有効性を高めるために、参加者に事前アンケートを依頼し、以下の３つに対する質問について、参加者の関心を調査した。これらのアンケート結果を踏まえ、机上演習のシナリオに反映を行った。

（１）サイバー攻撃に関する対応として、どの内容に関心があるか。

・サイバー攻撃の事前兆候の把握やサイバー攻撃を受けた時の検知
・不測の事態が発生した際に、サイバー攻撃かどうかの判断
・サイバー攻撃がされた場合の対処方法の設計及び対処担当者への指示方法
・サイバー攻撃を受けた際の関係部署とのやり取りの仕方
・その他

（２）サイバー攻撃の具体的な内容として、関心があるのはどれか。

・悪意のあるプログラム（マルウェア）などの感染（システムのっとり、被害拡散、など）
・内部情報（個人情報、知的財産、営業秘密情報など）の窃取
・重要システムに対するデータ破壊
・重要オンラインサービスに対するインターネット上からの攻撃
・わからない
・その他

（３）机上演習により獲得したい知見・経験として、期待されることは何か。

・サイバー攻撃が発生した際に対処する現場担当者に対して、指示するための「基本的事項」及び「実施上の知見」
・不測の事態が発生した際に、サイバー攻撃かどうかの審議を推論し、判断できる能力の獲得・そのための勉強方法や講習資料などの紹介
・サイバー攻撃に対する分析能力（被害状況の把握及びその後の被害の想定方法など）の獲得・そのための勉強方法や講習資料などの紹介
・社内におけるサイバー攻撃対策組織のメンバーの構成及び実行能力の向上のための必要能力の確保策
・その他

３．４．３　実施内容

（１）第１回

机上演習第１回では、制御システムに特化しない一般的なサイバー攻撃を受けた場合のシナリオに基づき、その対処についての議論を行った。

１）フェーズ１

・攻撃により業務に対してどのような被害が発生すると想定されるか。
・その想定される被害を回避あるいは拡大抑止するために、どのような緊急対応が考えられるか。

２）フェーズ２

・即座にとるべき行動は何か。特に上層部に対する説明を想定して、理由及び根拠を明確にする。
・推定された原因に紐づく対処のための行動は何か。

３）本シナリオにおいて望まれる知識あるいは能力

・最新の攻撃ベクトル（経路と手段）[46]に関する知識（巧妙化したスピア型メール[47]、ファイルレス攻撃[48]、モバイルデバイスの乗っ取り、正規サービスの不正利用）
・クラウド[49]サービス特有のリスクに関する知識
・インシデント対応不備による影響（ソーシャルネットワーキングサービス（SNS）による炎上）に対する理解と対処方法に関する知識
・最新の攻撃手法を理解し対処する能力
・社内関連部門と連携するために、事象を把握しエスカレーションする能力
・インシデント対応に影響を与える法制度に関する知識

（２）第２回

机上演習第２回では、第１回と類似の攻撃手法を用いて「運行／運航関係部門の制御・計測システム」に対する攻撃を行うシナリオに基づき、ネットワーク構成を提示した上で、発生したインシデントへの対応について議論を行った。

１）フェーズ１

・発生した事象に対して、「ＩＴ部門」、「運行／運航関係部門」、「委託業者など」はどのような初動対処をとるべきか。

２）フェーズ２

・セキュリティ専門業者に委託するフォレンジック調査の要求事項を明確化する。

３）本シナリオにおいて望まれる知識あるいは能力

・状況を把握するための知識（通信状況を把握するために必要となるネットワークの知識）
・攻撃経路及び影響範囲の特定のために必要となる知識（ログ分析など）
・把握した情報に基づき適切な対応（ネットワークの遮断、機器の隔離、ホワイトリスト[50]の適用）を実施する能力
・利害関係者に依頼すべき事項を含む、インシデントへの初動対処を立案する能力
・フォレンジック調査についての知識
・適切な調査依頼を実施する能力

（３）第３回

机上演習第３回では、発生したサイバー攻撃に対するフォレンジック調査及び通信ログに対する調査の実施により見出された痕跡及び発生事象に基づき、議論を行った。

１）フェーズ１

・調査結果から得られた判明事項をもとに、本攻撃のメカニズムを推定する。

２）フェーズ２

・本攻撃のメカニズムに対して、再発防止及び安全管理の徹底のための対策を立案する。（短期及び中・長期の観点、技術、管理（人的）及び法務の観点）

３）本シナリオにおいて望まれる知識あるいは能力

・フォレンジック調査の結果を分析・評価する能力
・システム構成に基づき攻撃事象を把握する能力
・対策を立案するうえでの技術的知識（ネットワークに関する知識を含む）
・業務への影響を考慮したうえで対策の可否あるいは有効性を判断する能力

３．４．４　得られた知見

鉄道分野と航空分野における机上演習を実施した結果､得られた知見は以下のとおりである。

なお、今回のシナリオにおいては、鉄道分野と航空分野の参加者では、得られた知見に大きな差異は見られなかった。

・状況認識の徹底に向けた努力の重要性
・発生事象を「点」で捉えるのではなく「面」で捉えること
・隣接する領域（ＩＴ部門及び委託業者）と緊密連携
・意思決定の責任を持つ経営層への報告要領の事前策定と習熟訓練
・サイバー攻撃の事象特性を理解した事業継続計画（BCP）策定
・緊急時におけるツーマン・ルール（相互監視規制）などの徹底

また、机上演習で得られた知見から、カリキュラムに追加する必要があると考えられる事項は以下のとおりである。

・最新の攻撃ベクトル（経路と手段）に関する知識
・クラウドサービス特有のリスクに関する知識
・適切にインシデント対応を行うための知識（社内外連携とエスカレーションなど）
・インシデント対応に影響を与える法制度に関する知識
・状況把握、対策立案のための知識（ネットワークの知識を含む）
・攻撃経路及び影響範囲の特定のために必要となる知識（ログ分析など）
・把握した情報に基づき適切な対応を実施するための知識
・フォレンジック調査についての知識
・サプライチェーンのセキュリティ対策の重要性に関する理解

３．５　学習内容の決定

前節までの検討結果に基づき、学習内容は以下のとおりとした。

（１）第１回　サイバー攻撃の現状

第１回は、サイバー攻撃の現状を解説するものとした。国内外の人材育成カリキュラムの事例収集の結果を踏まえ、内容としては、サイバーセキュリティに関する政府動向、サイバー攻撃事例をもとにした脅威とインシデント、想定される攻撃手法、セキュリティ確保の取り組み状況とした。

（２）第２回　サイバー攻撃の手法と脆弱性

第２回は、サイバー攻撃の手法と脆弱性を解説するものとした。国内外の人材育成カリキュラムの事例収集を踏まえ、内容としては、第１回で解説した攻撃事例を含む代表的なサイバー攻撃の脅威とその要因となる脆弱性の解説とした。

（３）第３回　サイバーセキュリティ基礎

第３回は、サイバー攻撃に対応するための基礎知識として、サイバーセキュリティ基礎を解説するものとした。学習内容の定義の結果を踏まえ、内容としては、セキュリティマネジメントの概要、その一環として資産管理の重要性及びリスク評価の重要性の解説とした。

（４）第４回　ネットワーク基礎

第４回は、サイバー攻撃に対応するための基礎知識として、ネットワークの基礎を解説するものとした。学習内容の定義の結果を踏まえ、内容としては、ネットワーク構成と動作原理などの概要、代表的なネットワーク接続機器の解説とした。

（５）第５回　セキュリティ技術

第５回は、サイバー攻撃に対応するための基礎知識として、セキュリティ技術を解説するものとした。学習内容の定義の結果を踏まえ、内容としては、サイバー攻撃対策を支援することを目的として、サイバー攻撃に対する対策技術の用語と概要の解説、多層防御の考え方、フォレンジックの概要の解説とした。

（６）第６回　サイバー攻撃対策

第６回は、サイバー攻撃対策を解説するものとした。国内外の人材育成カリキュラムの事例収集の結果を踏まえ、内容としては、手引書に記載された対策を解説するものとし、鉄道分野については、機器・システム及び運用・管理のセキュリティ対策の解説とした。航空分野については、設備・システム及び運用・管理のセキュリティ対策の解説とした。

（7）第7回　サプライチェーンのセキュリティ対策

第7回は、サプライチェーンのセキュリティ対策を解説するものとした。学習内容の定義及び机上演習の結果を踏まえ、内容としては、サプライチェーンのセキュリティ対策の重要性、外部委託範囲の特定と管理、情報の入手とその有効活用の解説とした。

（8）第8回　インシデント対応

第8回は、インシデント対応を解説するものとした。学習内容の定義及び机上演習の結果を踏まえ、内容としては、インシデント発生時の対応手順、インシデント対応体制、対処時のポイントの解説とした。

（9）第9回　学習の振り返り

第9回は、本カリキュラムの学習内容を総括するための学習の振り返りを行うものとした。内容としては、コースのまとめと振り返り、質疑応答を行うものとした。

３．６　カリキュラムの作成

学習内容に基づく、カリキュラム内容の整理結果を以下の表に示す。なお、カリキュラムの詳細については

「参考資料１：鉄道のサイバーセキュリティに関する人材育成カリキュラム」

「参考資料２：航空のサイバーセキュリティに関する人材育成カリキュラム」

を確認されたい。

講座の構成及び学習内容のレベルでは、鉄道分野と航空分野は共通の整理内容となった。

表　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

第４章　教材の作成

４．１　教材の作成にあたって

本調査研究で作成したカリキュラムによって人材育成を実施する際には、教材を作成する必要がある。本カリキュラムにおける各講座の説明において、教材を作成する際にポイントとなる事項を記載しているため､教材の作成に際しては､この留意点の記載内容を参考にされたい。

４．２　教材の例

本調査研究においては、第１回（サイバー攻撃の現状）の講座において使用することを想定した教材イメージを作成した。内容としては、脅威とインシデント、想定される攻撃手法、セキュリティ確保への取り組みの状況とし、鉄道分野と航空分野の最近の事例に基づき教材化を行なっている。

（１）鉄道分野

鉄道のサイバーセキュリティに関する人材育成カリキュラム
第1回 サイバー攻撃の現状

- サイバーセキュリティに関する動向
- 脅威とインシデント
- 想定される攻撃手法
- セキュリティ確保への取り組みの状況

- **サイバーセキュリティに関する動向**
- 脅威とインシデント
- 想定される攻撃手法
- セキュリティ確保への取り組みの状況

サイバーセキュリティに関する日本政府の動向

サイバーリスクの深刻化を受け法制度を強化

脅威の動向

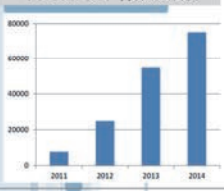
■ 企業への攻撃が頻発、漏洩個人情報は累計最大7,148万人
- ➢ 公表企業：179社　事故件数：288件
  - ・ 日本年金機構への標的型サイバー攻撃
  - ・ 大手教育会社における内部不正　等

出所： 商工リサーチ社「上場企業と主要子会社での個人情報の漏えい・紛失事故調査（2012年1月～2015年6月5日）（可能性含む）

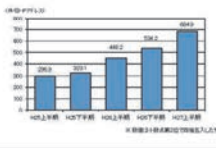
■ 警察庁サイバーポリスからの報告（H27上半期）では、探索行為も含めた攻撃は、1 IP当たり約680件にのぼる

出所：警察庁「平成27年上半期のサイバー空間をめぐる脅威の情勢について」

インシデント件数の増加



攻撃件数の増加



サイバーリスクの深刻化は著しく、眼前に迫っている

政府の動向

2014年9月	■ サイバーセキュリティ戦略（CS戦略）が閣議決定 ■ 2020年オリンピック・パラリンピック競技大会を参るストーンとした対策強化取組み方針が明示
2014年11月	■ サイバーセキュリティ基本法が施行 ■ サイバーセキュリティ戦略本部を設立、日本のサイバーセキュリティを推進する権限を集約・強化
2015年6月	■ 日本再興戦略 改訂2015 ■ IT利活用の安全・安心の確保が成長戦略を確固たるものにすると明記
2016年1月	■ 経済産業省から経営者が実施すべき要件を纏め「サイバーセキュリティー経営ガイドライン」が発行 ■ NISC「我が国のサイバーセキュリティ推進体制の更なる機能強化に関する方針」を発表
2016年4月	■ サイバーセキュリティ基本法 改定案が国会承認

企業は、政府方針を考慮した責任ある取組みが求められている

- サイバーセキュリティに関する動向
- **脅威とインシデント**
- 想定される攻撃手法
- セキュリティ確保への取り組みの状況

鉄道分野におけるインシデント事例

- **2003年8月、マルウェアBlaster感染による列車運行の阻害**
  - 米鉄道会社CSXのネットワークがマルウェアBlasterワームに感染し、一部列車の運行に障害が発生した。
  - 同社の発表によれば、世界規模で感染を広げているワームに感染したためとしており、BlasterワームかNachiワーム、またはSobig.Fに感染した疑いがある。また、第1報では信号システムの問題が原因とされていたが、その後の調べで信号や配車のシステムなどの重要システムをつなぐネットワーク部分が、ワームによって断絶されたことが原因としている。

ワームとは、独立したプログラムであり、自身を複製して他のシステムに拡散する性質を持ったマルウェアです。

http://news.mynavi.jp/news/2003/08/21/20.html

鉄道分野におけるインシデント事例

- **2004年5月、マルウェアSasser感染による列車運行の阻害**
  - マルウェアSasser感染により、シドニーの列車無線ネットワークの利用ができなくなり、運転手と信号手との通信が途絶えた。これにより、運行が通常の20%に制限され、30万人の利用者に影響が出た。

Sasser（サッサー）とは、Windows XP、2000の脆弱性「MS04-011」を悪用したワームの一種です。

http://news.bbc.co.uk/2/hi/technology/3682537.stm
https://www.sophos.com/en-us/press-office/press-releases/2004/05/va_sassertrain.aspx

鉄道分野におけるインシデント事例

- **2008年、路面電車システムに侵入し、4車両を脱線**
  - 14歳の少年が路面電車システムに侵入し、4車両を脱線させ、12人が負傷した。少年は、Lodz市のトラックポイントを操縦するためにTVリモコンを改造し、その装置を作成するために必要な情報と装置を集めるために市内の路面電車所に侵入していた。

http://www.telegraph.co.uk/news/worldnews/1575293/Schoolboy-hacks-into-citys-tram-system.html

鉄道分野におけるインシデント事例

- **2011年12月、米国北西部の鉄道会社へのサイバー攻撃**
  - 米国北西部のある鉄道会社のコンピュータがサイバー攻撃を受け、2日間にわたって列車の運行に混乱が生じた。
  - 12月1日、システムへの侵入が発生し、その結果列車の運行スケジュールに15分ほどの遅延が生じた。また翌日もラッシュアワーの少し前に同様の干渉が行われたが、ただしこの日は運行スケジュールへの影響は生じなかった。
  - DHSでは、今回の攻撃は鉄道を標的にしてサービス停止を狙ったものというより、むしろ無作為に行った攻撃の対象が交通機関であった可能性のほうが高いとしている。

（DHS：米国国土安全保障省）

http://www.nextgov.com/cybersecurity/2012/01/hackers-manipulated-railway-computers-tsa-memo-says/50498/
http://wired.jp/2012/01/27/railyway-hack/

鉄道分野におけるインシデント事例

- **2016年11月、サンフランシスコ市営鉄道でランサムウェア感染**
  - 米国サンフランシスコ市営鉄道がランサムウェアによる攻撃を受け、2,112台のコンピュータが不正にロックされ、ロックを解くまでの間乗車無料にすることを余儀なくされた。
  - 安全・安定輸送には影響しないものの、他分野で発生している攻撃が、鉄道事業者でも発生した事例となる。

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

鉄道分野におけるインシデント事例

- **2017年5月、ドイツ鉄道でランサムウェアWannaCry感染**
  - 金曜日(5/12)の夜から土曜日(5/13)にかけて被害が発生した。発着時刻を表示する駅の電光掲示版に影響したが、運行業務やその他の事業には影響はなかった。
  - 乗降客の多い駅についてはスタッフを増員配備することで対応した。
  - 国内の鉄道事業者でも感染が報告されたが、運行業務等への影響に至るものはなかった。

ランサムウェアとは、感染したPCをロックしたり、ファイルを暗号化したりすることによって使用不能にしたのち、元に戻すことと引き換えに「身代金」を要求する不正プログラムです。

http://www.deutschebahn.com/de/presse/pressestart_zentrales_uebersicht/14176018/h20170513.html
https://railway-news.com/global-cyber-attack-hits-deutsche-bahn/

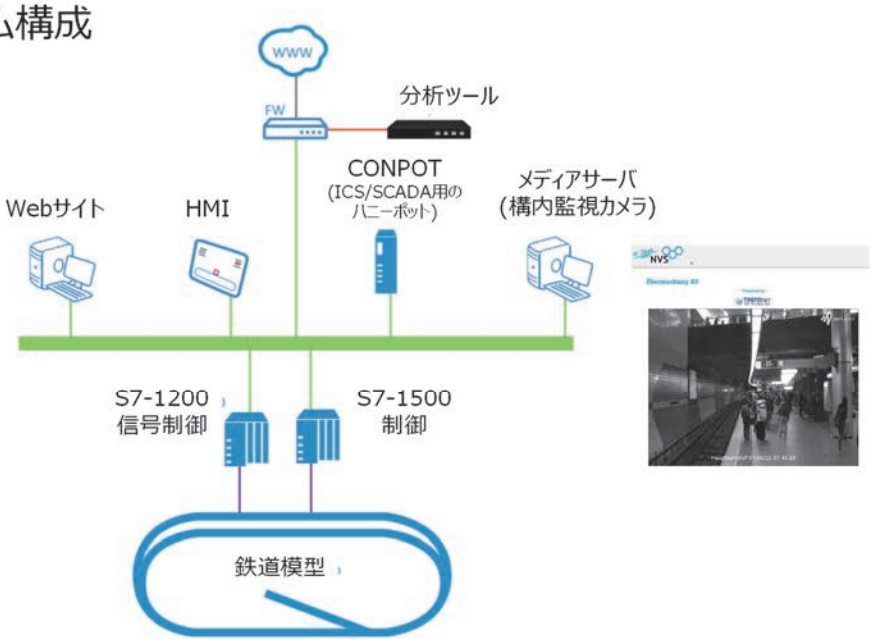
その他の事例

- **2015年、プロジェクト HaneyTrain**
  - 独Koramis社と英ソフォス社による鉄道システムへのサイバー攻撃を検証するプロジェクト。運行管理システム、構内ビデオ監視システム、一般的な情報、時刻表、発券および列車運行に関する情報を掲載したウェブサイトを用意し、架空の鉄道システムを構築した。
  - 全てのシステムは、製造業者の指示に従って構築した。指示がない場合は、デフォルトのパスワードを保持し、無効化されていないすべてのサービスにアクセス可能とした。

https://www.railengineer.uk/2017/05/30/hacking-the-railway/
https://www.sophos-events.com/honeytrain/downloads/Sophos_HoneyTrain_WP_EN.pdf

その他の事例

- **2015年、プロジェクト HaneyTrain**
  - システム構成



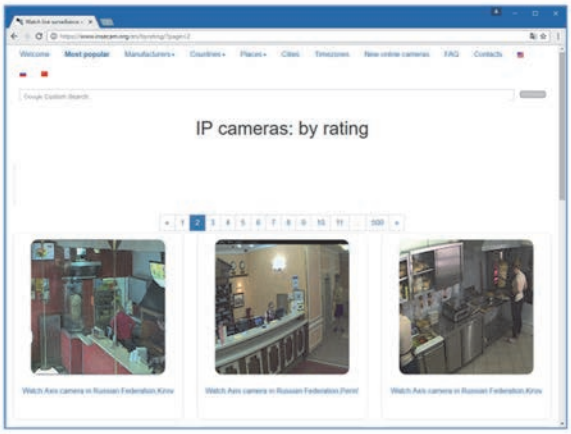
おさえておきたいインシデント事例

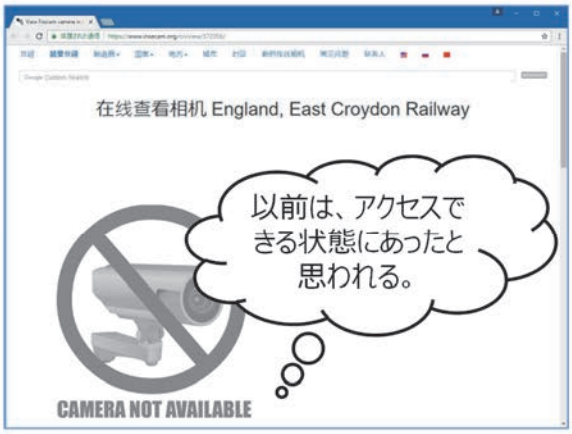
- **2010年7月、マルウェアStuxnet(スタクスネット)によるクローズドネットワークへのサイバー攻撃**
  - クローズドネットワークであっても、複数のシステムを連携させて構築している場合には、情報ネットワークへの侵入を起点に制御ネットワークにサイバー攻撃が進行することがある。

http://www.nca.gr.jp/2010/stuxnet/

おさえておきたいインシデント事例

- **2016年、監視カメラが関わるサイバー攻撃が発生**
- **監視カメラからの情報漏えい**
  - 名前を覚えておきたいサイト：Insecam
    世界中の無防備なWebカメラを見せるサイト

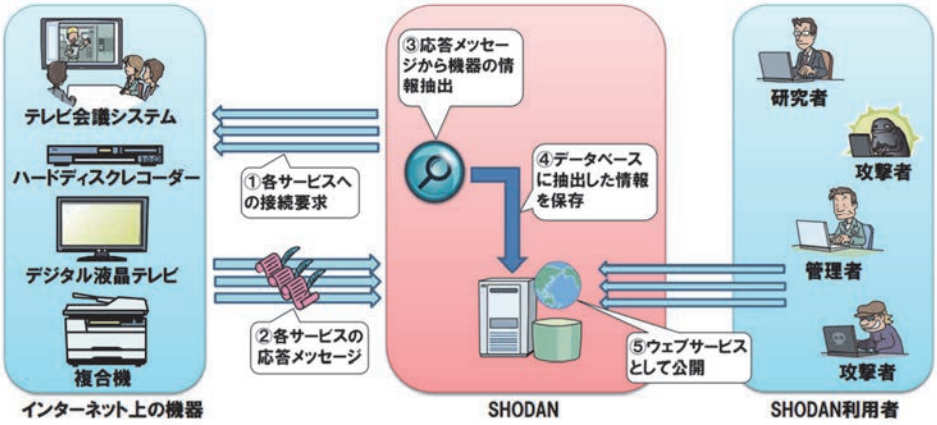




http://www.insecam.org/

おさえておきたいインシデント事例

- **2016年、意図しないインターネット接続機器の存在**
  - 名前を覚えておきたいサイト：SHODAN
    インターネットに接続された機器情報を集積し、集積した機器情報を検索できるサイト



https://www.ipa.go.jp/files/000052712.pdf

- サイバーセキュリティに関する動向
- 脅威とインシデント
- **想定される攻撃手法**
- セキュリティ確保への取り組みの状況

脆弱性(ぜいじゃくせい)とは・・・

- **OSやソフトウエアなどのセキュリティ上の欠陥**
  家に例えると、ドアの鍵穴の劣化、鍵そのものの"弱さ"

  脆弱性があると(鍵が付いていない、鍵をかけていないのと同じこと)・・・侵入者(攻撃者)によって家(PC・サーバ)に容易に入られてしまうことに。

- **ウイルス対策と脆弱性対策は、同じではない。**
  - **脆弱性対策**
    劣化した鍵穴を修繕したり、鍵そのものを防犯性の高いものに交換すること。
  - **ウイルス対策**
    警備員を雇う(ウイルス対策ソフトを導入)こと。ただし、警備員がよそ見するなどの隙(ウイルス定義ファイルの未更新など)を利用されると、脆弱性を悪用されて侵入されてしまう可能性がある。

- サイバーセキュリティに関する動向
- 脅威とインシデント
- 想定される攻撃手法
- **セキュリティ確保への取り組みの状況**

対策にあたり留意しておきたいポイント

(1)ネットワークを介した攻撃を踏まえたセキュリティ対策

- **クローズドなネットワークで構成されているが、他社ネットワークとの接続などもあることから、ネットワークを介した攻撃に対して留意することが必要である。**

鉄道分野では、相互乗り入れに伴い運行管理システム、電力管理システムが他社ネットワークに接続することも多い。また、変電所や踏切の遠隔監視システム等、ネットワークの端点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。このため、サイバー攻撃の侵入口になる可能性を踏まえて、リスクの大きさに応じて適切に対策を講ずる必要がある。

対策にあたり留意しておきたいポイント

(2)事案発生時の対応

- **対処の遅れによる、被害の拡大や二次被害の誘引を防ぐためにも、機器故障がサイバー攻撃等に起因することを想定して対策を準備しておく必要がある。**

発生した事象がサイバー攻撃等に起因するものなのかを判断し対応を開始するまでに時間が掛かり、被害の拡大や二次被害を誘引する可能性がある。特に、発生した事象がサイバー攻撃によるものであった場合には、事案発生時の対応を想定した対策を準備しておかないと、対処完了までに時間を要するおそれがある。

鉄道のサイバーセキュリティに関する人材育成カリキュラム
第1回 サイバー攻撃の現状

END

（２）航空分野


航空のサイバーセキュリティに関する人材育成カリキュラム
第１回　サイバー攻撃の現状


項目
航空分野におけるサイバー攻撃の現状
00
サイバーセキュリティに関する動向
サイバーセキュリティに関する日本政府の動向
01
脅威とインシデント
航空分野を標的とする脅威と過去事例
02
想定される攻撃手法
標的型攻撃、サプライチェーン攻撃には要注意
03
セキュリティ強化への推奨事項（セキュリティ確保への取り組みの状況）
組織内システムの通信や操作の監視、制御がポイント

0 サイバーセキュリティに関する動向

サイバーセキュリティに関する日本政府の動向

サイバーセキュリティに関する日本政府の動向

サイバーリスクの深刻化を受け法制度を強化

脅威の動向

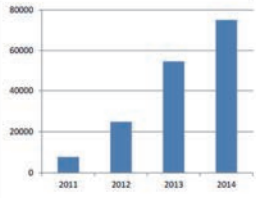
■ 企業への攻撃が頻発、漏洩個人情報は累計最大7,148万人
- ➢ 公表企業：179社　事故件数：288件
  - ・ 日本年金機構への標的型サイバー攻撃
  - ・ 大手教育会社における内部不正　等

出所： 商工リサーチ社「上場企業と主要子会社での個人情報の漏えい・紛失事故調査（2012年1月～2015年6月5日）（可能性含む）

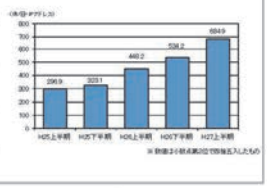
■ 警察庁サイバーポリスからの報告（H27上半期）では、探索行為も含めた攻撃は、1 IP当たり約680件にのぼる

出所：警察庁「平成27年上半期のサイバー空間をめぐる脅威の情勢について」

インシデント件数の増加



攻撃件数の増加



政府の動向

2014年9月	■ サイバーセキュリティ戦略（CS戦略）が閣議決定 ■ 2020年オリンピック・パラリンピック競技大会を参るストーンとした対策強化取組み方針が明示
2014年11月	■ サイバーセキュリティ基本法が施行 ■ サイバーセキュリティ戦略本部を設立、日本のサイバーセキュリティを推進する権限を集約・強化
2015年6月	■ 日本再興戦略 改訂2015 ■ IT利活用の安全・安心の確保が成長戦略を確固たるものにすると明記
2016年1月	■ 経済産業省から経営者が実施すべき要件を纏めた「サイバーセキュリティー経営ガイドライン」が発行 ■ NISC「我が国のサイバーセキュリティ推進体制の更なる機能強化に関する方針」を発表
2016年4月	■ サイバーセキュリティ基本法 改定案が国会承認

サイバーリスクの深刻化は著しく、眼前に迫っている

企業は、政府方針を考慮した責任ある取組みが求められている

1 脅威とインシデント

航空分野を標的とする脅威と過去事例

海外の航空分野の事例

近年の航空分野を狙ったサイバー攻撃は政治的要素が強い

ベトナム航空へのサイバー攻撃
南シナ海の領海における国際司法の判決を不服とし、中国のハクティビストがベトナム航空のシステムへ侵入を行なったと報道される。フライトインフォメーションのウェブページ改ざん、顧客情報件の公表、館内放送システムの乗っ取り、チェックインカウンターのシステム障害が確認されている。実際は中国人民解放軍の南シナ海を担当する部隊の関与の可能性が高いとみられている。

スウェーデンのLuftfartsverket（LFV）へのAPT攻撃
GRU（ロシア連邦軍参謀本部情報総局）によるAPT攻撃をうけ、航空管制センターのシステムがダウンした。関係は不明であるが、Arlanda、Landvetter、Brommaでは飛行機の交通量をスクリーンで見ることができなくなった。

LOTポーランド航空へのサイバー攻撃
地上運航システムがサイバー攻撃をうけ、フライトプランの作成ができなくなった。脅威アクターは不明のままである。

APT攻撃（Advanced Persistent Threat）とは、高度な持続的な脅威の総称のことです。日本においては高度標的型攻撃などと言われています。

国内の交通分野の攻撃動向

国内においての事例も単なるサイバー犯罪ではない

JTBへのAPT攻撃
2016年、Elirks（エリークス）と呼ばれるハッカーグループよりサイバー攻撃をうけ、顧客情報が窃取された可能性の報道があった。このグループは中国人民解放軍の配下のハッカーグループとして知られる。

某空港ビル会社への継続的なサイバー攻撃
中国人民解放軍に関係する研究所配下のハッカーグループより継続的にサイバー攻撃を受けていることが確認されている。自衛隊に関係する情報が目的であったと考えられる。
非公開情報であるため、被害の詳細は不明である。

セキュリティツールの脆弱性を悪用してのサイバー攻撃
中国人民解放軍をスポンサーに持つとされるハッカーグループが、セキュリティツールの脆弱性を悪用し、情報を目的とした攻撃を行った。交通分野に限らず、複数の企業が侵害を受けている。窃取された情報を収集しているサーバは、中国以外の国に押さえられており、日本国内の窃取情報が多方面へ流出した可能性が高い。

2 想定される攻撃手法

過去事例から予測される具体的な攻撃手法

航空分野を狙う代表的な攻撃手法

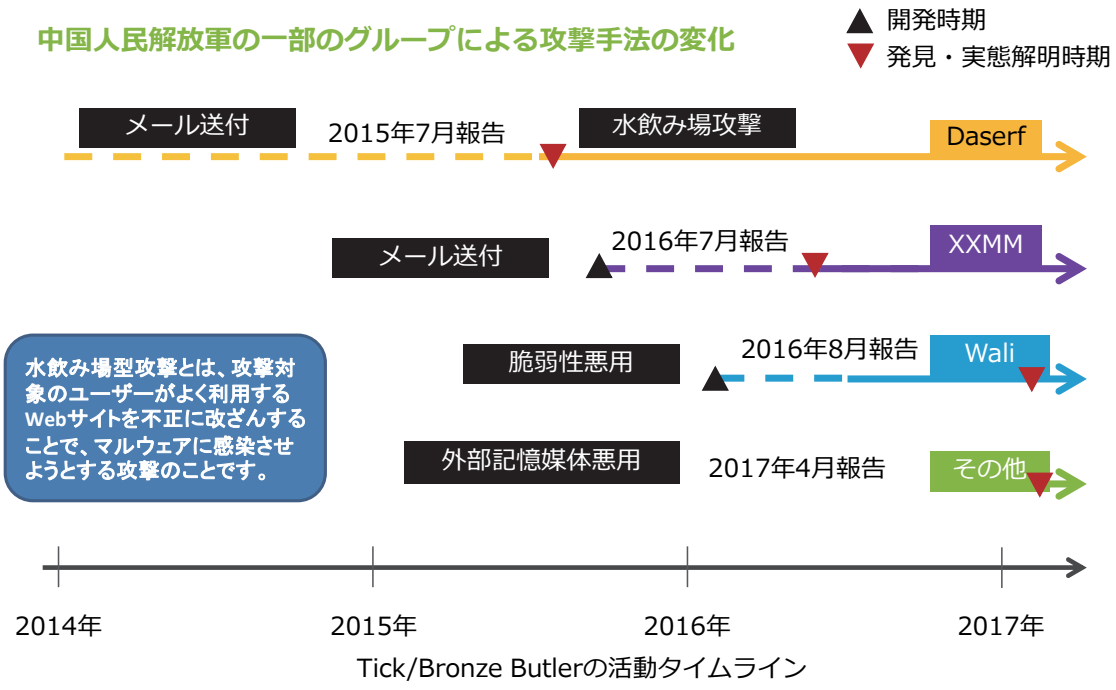
気をつけておきたい５つの手口

No.	攻撃手法	備考
1	スピア型メール	標的型攻撃を示すが、標的は航空会社のグループ会社や取引先も含まれる。
2	サプライチェーン攻撃	ソフトウェアの開発工程における範囲での攻撃が注目される。例えば、ソフトウェアのアップデートなどの悪用が考えられる。
3	メールの窃取	メールサーバへの侵入は攻撃手口の王道
4	USBドロップ攻撃	エアギャップ（物理的および論理的にパブリックなネットワークから分離されているネットワーク）への攻撃で利用される。保守業者が標的となることがある。
5	DoS攻撃	公開サービスの停止を目的とした攻撃。

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です。

＜参考＞マルウェアの開発時期と実態解明の時期

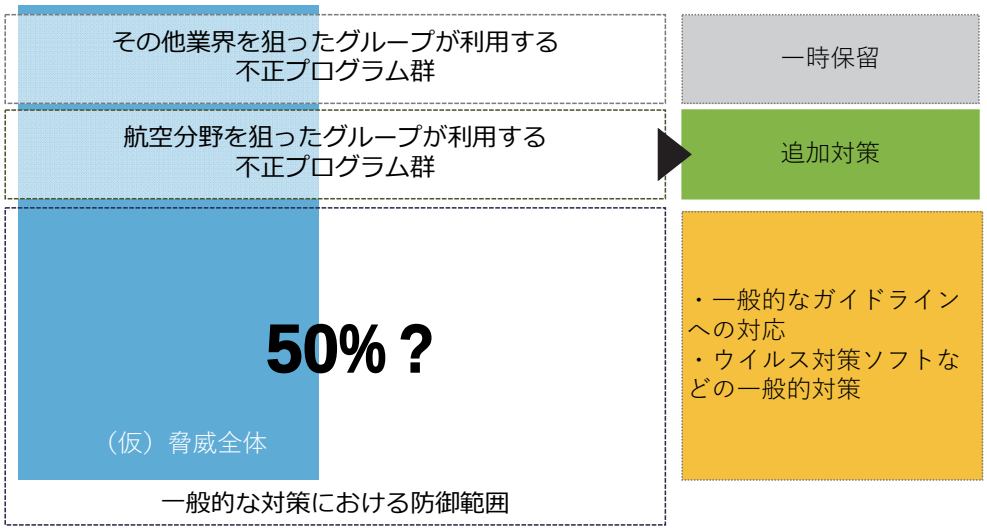
中国人民解放軍の一部のグループによる攻撃手法の変化



Tick/Bronze Butlerの活動タイムライン

基本的対策と分野特有の対策強化のイメージ

標的となる可能性のある分野への対策



3 セキュリティ確保への取り組みの一例

攻撃フェーズと事故発生に着眼した優先度の選定

対策アプローチの一案

一般的なPC上での多層防御

	対策製品例	検知期待値	
	ネットワーク監視	LOW	ほぼ検知は期待できない
	ウイルス対策ソフトウェア （セカンド）ウイルス対策ソフトウェア	LOW	
	デジタル署名のチェック ホワイトリスティング製品	MID	
	Endpoint Protection Platform 製品 Endpoint Detection & Response 製品	MID	

対策実施の最適化と優先度の順位付け

侵害を受けることを前提とした優先順位

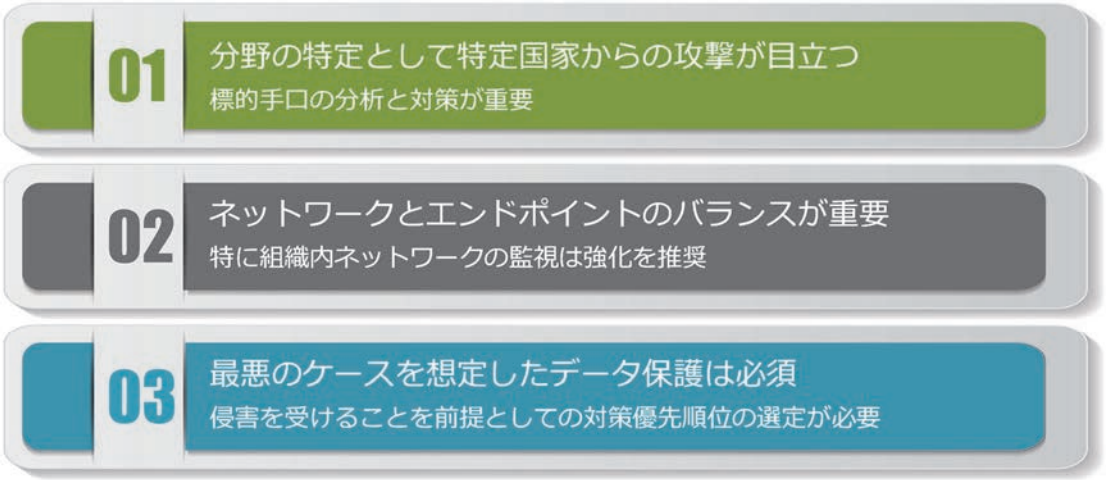
1	リスク高、実現可能 （費用対効果等）な対策 （各事業者により異なるためアセスメントが必要）
2	リスクが変動しずらい恒久的対策 （データ保護、ログ保全　等）
3	事後対応等の共通の対策項目 （インデント対応　等）

サプライチェーン攻撃への対応の心得

見えない脅威への対応

まとめ

航空分野における脅威とその対策



第５章　まとめと今後の課題

５．１　まとめ

サイバーセキュリティ人材の育成は、鉄道分野及び航空分野の事業者各々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、サイバーセキュリティ対策の人材育成カリキュラムの研究はあまり進んでいないため、本調査研究では、鉄道分野及び航空分野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を作成した。

（１）前提条件の検討

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、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、インシデント対応ができる人材

とし、必要となる能力は、

・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

と定義した。また、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を維持管理する人材とした。

（２）カリキュラムの検討・作成

（１）の結果を踏まえ、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もと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となるカリキュラムを作成した。なお、鉄道分野及び航空分野の事業者各々で、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の事業者各々の実態を鑑み、必要に応じて取捨選択することを推奨している。なお、新たなサイバーに関する脅威、攻撃が登場した際は、従来の対策では対応できないことも懸念されるため、最新事例の収集や必要な情報を関係者間で共有するなど、情報更新する必要が生じる。

（３）教材の作成

カリキュラムをもとにした人材育成を実施するための教材（簡易版）として、第１回（サイバー攻撃の現状）の講座において使用することを想定した教材イメージを作成した。

５．２　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）最新事例の収集

人材育成において最新の事例を具体的に提示することは、育成対象者の意識向上を図るとともに対象者が有効な対応を実行する上で重要であるが、現時点ではサイバー攻撃の事例の開示及び共有はあまり進んでいないため、最新事例の収集は大きな課題であると思われる。

（２）教育・訓練の実施

本調査研究では、主に講義形式を念頭に講座を作成したが、より有効な教育・訓練を実施するためには、講義形式のみではなく、演習形式を取り入れることが望ましい。一般的な情報セキュリティやＩＴ基礎知識など、汎用的な内容の講座については既存の e-learning を活用するなど、受講者の負担軽減を図ることも検討することが望ましい。

（３）講師の育成

講座の内容によっては組織固有の内容を解説するものがあるため、自組織において講師を育成することが望ましいが、前述した演習形式による教育・訓練を実施するためには、単に講座内容の知識だけではなく、ファシリテータ（学習や議論の進行役）としての力量が講師に求められるため、講師の育成は課題であると思われる。

（４）教材の作成

講座の内容によっては組織固有の内容を解説するものがあるため、その講座の教材作成においては自組織固有の内容を盛り込む必要がある。その際は、自組織においてサイバー攻撃を受けた際の受講対象者の役割を明確にしておくとともに、自組織の技術的対策の内容把握、サプライチェーンのセキュリティ対策の状況把握などの自組織内の現状を把握する内容を盛り込むことが望ましい。

（５）経営層への啓発

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備えるためには、様々な役割を持った人材がチームとなってサイバーセキュリティに取り組むとともに、社外の関係者とも連携して対応することが望ましい。サイバー攻撃による影響を考慮し、このような社内外の組織連携を実現するためには、組織横断的な体制の構築が必要であり、自社における投資をどうするかの経営判断が求められる。このため、経営層への啓発が重要であると考える。

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「サイバー攻撃に対する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。

この調査研究は、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カリキュラム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。

本年度は、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、国内外の事例収集、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。

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。

平成 29 年は、身代金攻撃（ランサムウエア）が世界的に蔓延し、重要インフラを含む多くの組織に大きな被害を与えた。また、ネットワークに様々なモノが繋がる今後のシステムへの攻撃脅威が認識されるとともに、国家によるサイバー攻撃が常態化した年であった。リオオリンピック・パラリンピックでは、大きな問題には至らなかったものの、公式及び関連 Web サイトに対する多くの DDoS 攻撃や Web アプリケーションへの攻撃がなされ、平昌オリンピック・パラリンピックでは、システム障害などが続々と報告された。我が国は 2020 年に東京オリンピック・パラリンピックの開催を迎えるが、本大会で大規模なサイバー攻撃を受けることは必至であり、それに対する備えを万全にすることが求められる。

サイバーセキュリティ人材の育成は、情報システム分野をはじめとして、様々な分野で既に取り組みが始まっている。本調査研究では、「鉄道分野」と「航空分野」において、具体的に育成対象者を選定した上で、どのような内容で教育を進めるべきかについてカリキュラムを作成している。

その作成にあたっては、国内外のカリキュラム事例を収集し、サイバーディフェンス研究所の名和氏を講師とした机上演習の実施を踏まえ、これらの対象分野における事業者の実態に即したものを目指した。各事業者には、サイバー攻撃の脅威が身近にあることの認識を深め、本カリキュラムを参考に、自社のシステムや管理の状況を踏まえ、人材育成を進めることを期待したい。

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 30 年 3 月

「鉄道/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　委員長
田中 英彦

用語の定義

本報告書において提示する用語の定義を以下に示す。

(1)**「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。

(2)**「サイバーテロ」**とは、インターネットなど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。

(3)**「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おそ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」、「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 13 分野をいう。

(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など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。

(6)**「Stuxnet」**とは、イランの核燃料施設を攻撃するために用いられたマルウェアのことをいう。USB メモリを経由し、物理的に隔離されたネットワークにおいて感染するように設計されている。

(7)**「WannaCry」**とは、Microsoft Windows を標的としたワーム型ランサムウェアのことをいう。

(8)**「クローズドシステム」**とは、インターネットなど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。

(9)**「標的型攻撃」**とは、特定の組織に狙いを絞り、その組織の業務習慣など内部情報について事前に入念な調査を行った上で、様々な攻撃手法を組み合わせ、その組織に最適化した方法を用いて、執拗に行われる攻撃をいう。典型的なものとしては、組織内部に潜入し、侵入範囲を拡大し、重要な情報を窃取又は破壊する攻撃活動が考えられる。

(10)**「ワーム機能」**とは、対象プログラムを必要とせず、自己複製し、自己増殖するコンピュータプログラムをいう。ネットワークに接続されている他のマシンに出現する。

(11)**「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など特定の制限をかけ、その制限の解除と引き換えに金銭を要求する。

(12)**「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。

(13)**「CSIRT」**とは、Computer Security Incident Response Team の略で、セキュリティインシデントなど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。

(14)**「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・分析などを行う事業者も該当する。

(15)**「タスク」**とは、IPA が提供する「i コンピテンシディクショナリ」の定義に基づき、企業において IT を利活用するビジネスに求められる業務のことをいう。

(16)**「スキル」**とは、「タスク」を支える IT 人材の能力や素養のことをいう。

(17)**「机上演習」**とは、本報告書においては、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。

(18)**「外部ネットワーク」**とは、不特定多数が接続できる回線で接続するネットワーク（主にインターネット）のうち、他ネットワーク以外のものをいう。

(19)**「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。

(20)**「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。

(21)**「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。

(22)**「修正プログラム」**とは、コンピュータやスマートフォンなどのシステム上に開いたセキュリティの欠陥を塞ぐために、メーカーなどから提供されるプログラムをいう。

(23)**「脆弱性情報」**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に関する情報の注意喚起または情報支援サービスをいう。

(24)**「ファームウェア」**とは、機器内部に固定的に組み込まれ、機器を直接制御するソフトウェアをいう。ハードウェアとソフトウェアの中間に位置付けられる。

(25)**「低レイヤ層」**とは、ネットワークを構成する各レイヤのうち、第 1 層に近い層をいう。低レイヤ層での監視とは、例えば、第 2 層での監視（通信パケットの監視）のことをいう。

(26)**「エンドポイント」**とは、ネットワークに接続されたパソコンや PDA、携帯電話などのネットワーク端末の総称をいう。

(27)**「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。

(28)**「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。

(29)**「パッチマネジメント」**とは、セキュリティパッチの適用についての管理をいう。

(30)**「パスワードリスト攻撃」**とは、攻撃者が何らかの方法で事前に入手した ID とパスワードのリストを使用し、ログイン機能を持つインターネットサービスに不正にログインを試みる攻撃手法をいう。

(31)**「ISMS」**とは、Information Security Management System の略で、情報セキュリティを管理するための枠組みをいう。

(32)**「ハッキング」**とは、コンピュータシステムや通信システムの動作を解析したりプログラムを改造・改良したりすること。転じて、他人のシステムを不正な手段で操作したり不正に機密情報を入手したりすること。

(33)**「スニファ攻撃」**とは、ネットワーク上を流れるパケットをモニタリングし、盗聴する攻撃手法をいう。

(34)**「内部脅威」**とは、外部からの侵入や攻撃を意味する「外部脅威」に対して、組織や施設の内部で働く従事者による不正行為等により生ずる脅威をいう。

(35)**「トロイの木馬」**とは、一見正当なプログラムを装っている不正なプログラムをいう。

(36)**「なりすまし」**とは、インターネット等の本人確認において、第三者が、特定の個人、組織またはネットワーク上の機器を装った行動をとることをいう。

(37)**「アップストリーム攻撃」**とは、エンドユーザー顧客でなくサービスプロバイダーを標的にした攻撃をいう。

(38)**「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。

(39)**「サンドボックス」**とは、未確認ファイルや疑わしいデータを隔離して安全に検証することを目的に構築された仮想環境をいう。

(40)**「CSOC」**とは、Cyber Security Operation Center の略で、コンピュータシステムへの脅威の監視や分析などを行う役割や専門組織のことをいう。

(41)**「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、およ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。

(42)**「エスカレーション」**とは、問題について、より上位の存在に対応を要請することをいう。

(43)**「ホワイトハッカー」**とは、コンピュータやネットワークに関する高度や知識や技術を持つ者を指す呼び名である「ハッカー」のうち、特にその技術を善良な目的に活かす者をいう。

(44)**「レガシーシステム」**とは、技術革新による代替技術が広く普及した段階で、旧来の技術基盤により構築されているコンピュータシステムをいう。

(45)**「ペネトレーション手法」**とは、コンピュータシステムに対して攻撃者の視点で侵入を試みることで、不正アクセスの可能性やシステムの脆弱性を洗い出す手法のことをいう。

(46)**「攻撃ベクトル」**とは、攻撃の経路（脆弱性のある箇所をどこから攻撃するか）と手段（脆弱性のある箇所をどのような手法で攻撃するか）を組み合わせた攻撃の説明のことをいう。

(47)**「スピア型メール」**とは、特定のターゲットに対して重要なデータや個人情報を奪う目的で送付されるメールのことをいう。

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

(49)**「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。

(50)**「ホワイトリスト」**とは、注意・警戒の必要があるか否かを示す一覧（リスト）のうち、特に注意・警戒が不要である対象を列挙したリストのことをいう。

参考資料１

「鉄道のサイバーセキュリティに関する人材育成カリキュラム」

鉄道のサイバーセキュリティに関する
人材育成カリキュラム

平成 30 年 3 月

一般財団法人　運輸総合研究所

目次

カリキュラム要旨

本文書（以下、「本カリキュラム」という）は、鉄道分野において、運行に関わる制御システムがサイバー攻撃を受けたときに、迅速かつ適切に対応すべく、実際に対応する人材を育成することに主眼を置いている。迅速かつ適切な対応をするためには、システムを維持管理する人材が、システムに異常が発生した際、その原因がサイバー攻撃[1]である可能性を考慮することが重要である。しかしながら、サイバー攻撃と従来のシステム障害などによる異常には、明確な違いはないと考えられ、システムを維持管理する人材が、サイバー攻撃に関する基礎知識を持たない場合、サイバー攻撃であることに気付くのが遅れる可能性もあり、その場合、さらに他のシステムに影響が波及するなど、初動対応に遅れを生じることが懸念される。

また、一般にサイバー攻撃の場合、より高度な知識と適切な対応が必要となるため、サイバー攻撃から防護することを鑑みると、サイバー攻撃に対処（原因究明、復旧など）する専門機関（社内外のセキュリティ担当、CSIRT[2]、セキュリティベンダー[3]など）との連携により対応することが望ましいが、システムを維持管理する人材が、サイバー攻撃に関する基礎知識を持たない場合、適切に連携できないことが懸念される。

鉄道分野をはじめとする重要インフラ[4]における制御システムは、従来サイバー攻撃を受ける可能性は低いと考えられてきた。国内の鉄道分野では、サイバー攻撃被害の報告はされていないが、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。ネットワークを介したサイバー攻撃や、ＩＴを用いたシステムの開発など今後の技術発展を考えると、さらに脅威が増す可能性がある。

このような状況を踏まえ、各鉄道事業者において、サイバー攻撃に対応する人材の育成が急務であると考え、これを促すために参考となるカリキュラムを検討した。

本カリキュラムが目標とする人材には、平成 28 年度に（一財）運輸総合研究所が作成した「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[注1)]」の対策を実践できる人材としている。このため、本カリキュラムの育成対象者は、各鉄道事業者が保有する以下のシステムの維持管理あるいは障害対応に従事する人材を想定している。

・運行管理システム
・電力管理システム
・座席予約システム

ただし、鉄道事業者が扱う機器・システムは上記以外にも多数存在し、また、保有するシステムも異なるため、鉄道事業者により、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。そのため、学習内容は、本カリキュラムの内容を参考にしつつ、各鉄道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。

なお、新たなサイバーに関する脅威、攻撃が登場した際は、従来の対策では対応できないことも懸念されるため、最新事例の収集や必要な情報を関係者間で共有するなど、情報更新する必要が生じる。

注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」とは、平成 28 年度日本財団助成事業として実施した、「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」における、情報セキュリティ大学院大学の田中英彦学長（当時）を委員長とした検討委員会で付議了承を得た文章であり、鉄道分野において調査当時に考えられたサイバーセキュリティ対策をまとめたものである。

注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、意図的なサイバー攻撃により、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、そのおそ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。なお、国土交通省の外局である運輸安全委員会が調査する「重大インシデント」は、「事故が発生するおそれがあると認められる事態」を指し、鉄道運転事故/航空事故には至らずに済んだものの一歩間違えれば事故が発生していたという状況をいい、本調査における「インシデント」とは意味合いが異なる。

注３）本カリキュラムにおいて、番号が付与されている用語については、巻末の「用語の定義」に説明文を記載している。

１．カリキュラム作成の背景

本カリキュラムは、以下に示す背景から、鉄道分野のサイバーセキュリティ[5]に関する人材を育成するための参考資料としてとりまとめたものである。
（１）2020 年東京五輪大会の成功に向けて、サイバーテロ[6]対策は重要な課題の一つである。
（２）鉄道分野におけるサイバーテロは甚大な影響をもたらすおそれがある。
（３）鉄道分野におけるサイバーセキュリティ人材が不足している。
（４）鉄道事業者各々で人材を育成するため、参考となるカリキュラムが必要である。

［ 解説 ］

（１）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の一つである。

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サイバーテロ対策が開催国において懸案となっていた。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。

（２）鉄道分野におけるサイバーテロは甚大な影響をもたらすおそれがある。

鉄道分野は、我が国のサイバーセキュリティ戦略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・安定な運行が妨げられると、その影響は甚大になるおそれがある。国内ではサイバー攻撃被害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。ネットワークを介したサイバー攻撃や、ＩＴを用いたシステムの開発など、今後の技術発展を考えると、さらに脅威が増す可能性がある。

（３）鉄道分野におけるサイバーセキュリティ人材が不足している。

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[注)]では、研究対象とした鉄道分野、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。

注）東京オリンピック・パラリンピックに向けた交通機関へのサイバーテロ対策に関する調査研究、（一財）運輸政策研究機構、平成 28 年 3 月

（４）鉄道事業者各々で人材を育成するため、参考となるカリキュラムが必要である。

サイバーセキュリティ人材の育成は、各鉄道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が必要であると考えた。

２．鉄道事業者の将来望ましい状況

システムのＩＴ化、他システムとの連携、クローズドシステム[7]に対する攻撃手法の高度化など鉄道事業者の潜在的な脅威は増大している。このような状況を踏まえ、鉄道事業者においては、将来的に以下の状況にあることが望ましい。

（１）インシデント発生の際、その原因がサイバー攻撃である可能性を考慮し、適切に対応できる人材が現場に配置されている。

（２）仮にサイバー攻撃を受けた場合でも対応可能となる体制が整備されている。

（３）サイバー攻撃に対処する専門機関と連携して対処できる体制が整備されている。

（４）インシデント対応に関与する全ての要員がサイバー攻撃の脅威を認識している。

［ 解説 ］

（１）インシデント発生の際、その原因がサイバー攻撃である可能性を考慮し、適切に対応できる人材が現場に配置されている。

鉄道分野の制御システムがサイバー攻撃を受けた事例は国内では報告されておらず、サイバー攻撃を受けた際に、現場で適切な対応が取れるか現状では不明な状態にあると考えられる。そのため、サイバー攻撃に関する基礎知識を有し、インシデント発生の際、その原因がサイバー攻撃である可能性を考慮し、適切に対応できる人材が現場に配置されていることが望ましい。

（２）仮にサイバー攻撃を受けた場合でも対応可能となる体制が整備されている。

インシデントが発生した時点では、サイバー攻撃が原因か否かは判断できない場合も予想されるため、サイバー攻撃が疑われる場合の報告先を明示するなど、サイバー攻撃を受けた場合でも対応可能となる体制が整備されていることが望ましい。また、自社内においてサイバー攻撃に対応するための計画、実行、評価、改善を繰り返し、体制を継続的に改善することが望ましい。

（３）サイバー攻撃に対処する専門機関と連携して対処できる体制が整備されている。

サイバー攻撃に対処（原因究明、復旧など）する専門機関に当該システムの知識が不足していた場合、対処が遅れることも予想されるため、より迅速な対処をするためには、システムを熟知する人材とサイバー攻撃に対処する専門機関が連携して対処ができる体制が整備されていることが望ましい。

（４）インシデント対応に従事する全ての要員がサイバー攻撃の脅威を認識している。

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ることから、インシデント対応に従事する全ての要員がサイバー攻撃の脅威を認識していることが望ましい。

３．求められる人材像と必要となる能力

本カリキュラムにおける、求められる人材像とそのために必要となる能力は、以下のとおりである。

（１）求められる人材像

・インシデント発生の際、サイバー攻撃である可能性を考慮し、適切に対応できる人材

・インシデント対応を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、対応できる人材

（２）必要となる能力

・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

［ 解説 ］

「２．鉄道事業者の将来望ましい状況」で示した状況を実現するために、求められる人材像は、「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」（発行：平成 28 年度、（一財）運輸総合研究所））の対策を実践できる人材とした。具体的には、下表のような定義とした。

表　本カリキュラムにおける、求められる人材像とそのために必要となる能力

（１） 求められる 人材像	・インシデント発生の際、その原因がサイバー攻撃である可能性を考慮し、適切に「対応」[注1)] できる人材。 ・「インシデント対応」[注2)] を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「対応」できる人材。
（２） 必要となる 能力	１）サイバー攻撃に関わるインシデント対応に関する能力 ・インシデント発生時の対応手順を理解し、「対応」できる能力。 ・サイバー攻撃対策を理解し、一連の「対応」ができる能力。 ・サプライチェーンのセキュリティ対策の重要性を理解し、サイバー攻撃に備えた準備ができる能力。 ２）上記に関わる情報技術（ＩＴ）に関する能力 ・「インシデント対応」を行うために必要な情報技術（ＩＴ）に関する知識と能力。

注１）本頁における「対応」とは、対象となるシステムを維持管理する人材が、サイバーに対処（原因究明、復旧など）する専門機関の助言を受けて、システムの復旧につなげる活動などにあたる他、システムを熟知する立場から、サイバーに対処（原因究明、復旧など）する専門機関にシステムに関する助言や援助を行うことを指す。

注２）本頁における「インシデント対応」には、以下の活動が含まれる。

①インシデント発生時：インシデント発生時に、被害を局限化、最小化し、速やかな復旧につなげる活動

②インシデント発生後：インシデントから復旧し、再発を防止することを目的とする活動

③インシデント発生前：インシデント発生に備えた「準備」の活動

４．育成対象者

本カリキュラムの育成対象者は、鉄道事業部門のシステムを維持管理する人材である。インシデントが発生した場合、その原因がサイバー攻撃か否か判断できない場合も含め、対応する人材を想定する。

[解説]

各鉄道事業者の組織（役職と部門）において、本カリキュラムの育成対象者は下表のとおりであり、鉄道事業部門のシステムを維持管理する人材（技術者層）である。（凡例：「○」）

なお、経営者層と管理者層は、サイバーセキュリティに対する意識改革の必要性などが指摘されているが、優先順位を踏まえ本カリキュラムでは対象外とした。また、鉄道事業部門のシステム担当以外も対象外とした。なお、管理者層は、将来的には技術者層と経営層との間のコミュニケーションを円滑にする「橋渡し人材」の一翼を担うことが期待される。（凡例：「-」）

情報システム部門は、本カリキュラムで必要とされる能力を既に有していると考えられるため、対象外とした。ただし、より高度な連携をするために内容を理解しておくことを推奨する。（凡例：「△」）

表　本カリキュラムの育成対象者（凡例：○）

部門 / 役職	情報システム部門	鉄道事業部門（システム担当）	鉄道事業部門（システム担当以外）
経営者層	－		
管理者層	－	－	－
技術者層	△	○	－

注１）管理者層とは、現場から報告を受け、各所に報告をする方を指す。
注２）技術者層とは、システムを扱う現場において、実際にシステムの維持管理などをする方を指す。

なお、サイバー攻撃に対応する一連の役割とそれを担当する部署は、各鉄道事業者で異なると思われるため、本カリキュラムにおける想定を以下の表に示す。

表　サイバー攻撃に対応する一連の役割と担当部署の想定（運行管理システムの例） 注1)

役割	担当部署	望まれる能力
システム操作 システム異常の検知・通報	司令所/指令所	異常の原因としてサイバー攻撃があるという意識をもち、適切に連絡ができる能力
システム維持管理 システム障害対応	電気部門 （外部委託先を含む）	サイバー攻撃に備えた準備、インシデント発生時の対応、サイバー攻撃対策などの一連の活動に「対応」注2)できる能力
サイバー攻撃の インシデント対応の立案、実行	セキュリティ担当部門 C-SIRT、情報システム部門 セキュリティベンダー	サイバー攻撃に備えた準備、インシデント発生時の対応、サイバー攻撃対策などの一連の活動を立案、実行できる能力

注１）黒枠は本カリキュラムで想定する育成対象者を指す。
注２）本頁における「対応」とは、対象となるシステムを維持管理する人材が、サイバーに対処（原因究明、復旧など）する専門機関の助言を受けて、システムの復旧につなげる活動などにあたる他、システムを熟知する立場から、サイバーに対処（原因究明、復旧など）する専門機関と連携して、システムに関する助言や援助を行うことを指す。

５．カリキュラムの特徴

本カリキュラムの特徴は以下のとおりである。
（１）鉄道事業者の実態を踏まえ、必要と思われる項目を選定
（２）サイバー攻撃の被害事例を活用した構成
（３）最新のサイバー攻撃の動向を踏まえた内容を含む記載

［ 解説 ］

本カリキュラムの特徴は以下のとおりである。

（１）鉄道事業者の実態を踏まえ、必要と思われる項目を選定

2020 年東京五輪大会までに人材育成を行う必要があることから、昨年度の研究成果である「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」（発行：平成 28 年度、（一財）運輸総合研究所））に記載されている対策や今年度実施した机上演習[8]の知見などを踏まえ、必要と思われる項目を選定した。

（２）サイバー攻撃の被害事例を活用した構成

海外の人材育成カリキュラムによると、サイバー攻撃の被害事例を活用すると、サイバー攻撃の脅威を効果的に認識できるとあることから、学習の初期段階（第１回）において、海外の鉄道分野におけるサイバー攻撃の被害事例を紹介し、以降の学習の段階に繋げる構成とした。

（３）最新のサイバー攻撃の動向を踏まえた内容を含む記載

標的型攻撃[9]の進化あるいはワーム機能[10]を有したランサムウェア[11]、ファイルレス攻撃[12]の登場など、脅威は日々複雑化、高度化していることから、現時点で把握できる最新のサイバー攻撃手法の内容を含む記載とした。

６．カリキュラム作成にあたっての前提条件

本カリキュラムは以下のような前提に基づいて作成している。
（１）受講者は、情報セキュリティ[13]に関する基礎知識を有している。
（２）講座は、各鉄道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。

［ 解説 ］

（１）受講者は、情報セキュリティに関する基礎知識を有している。

本カリキュラムの受講者は、情報セキュリティに関する基礎知識を有していることを前提としている。具体的には、以下の内容を理解していることを想定している。

・情報セキュリティ読本　教育用プレゼン資料　第１章 今日のセキュリティリスク
（https://www.ipa.go.jp/files/000015327.ppt）
・情報セキュリティ読本　教育用プレゼン資料　第２章 情報セキュリティの基礎
（https://www.ipa.go.jp/files/000015328.ppt）
・情報セキュリティ読本　教育用プレゼン資料　第 4 章 組織の一員としての情報セキュリティ対策
（https://www.ipa.go.jp/files/000015330.ppt）

（２）講座は、各鉄道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。

鉄道事業者により、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。そのため、講座は、本カリキュラムの内容を参考にしつつ、各鉄道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。

ただし、新たなサイバーに関する脅威、攻撃が登場した際は、従来の対策では対応できないことも懸念されるため、最新事例の収集や必要な情報を関係者間で共有するなど、情報更新する必要が生じる。

手引書の内容を教育するには、自社の資産（システム構成など）に応じて特化した内容となるため、原則として、講師は自社の社員が望ましい。しかしながら、講師としての能力を持つ人材の不足や講義の準備にかかる講師の負担など、各鉄道事業者で状況は異なるため、汎用的な内容については、既存の e-learning[14]の活用や、講師を外部委託するなど、適宜、講師を効率的に選択することを推奨する。

また、講義形式は、講義（座学）だけではなく、演習を取り入れると効果的であると思われる。

なお、カリキュラムを作成する上では所要時間の想定が必要であると思われたため、必要と考える教育項目と、各鉄道事業者の業務の状況などを勘案して、カリキュラム全体で３日（20 時間程度）を想定した。ここで示した所要時間はあくまで目安であり、各鉄道事業者が必要に応じて、学習項目を追加、削除、修正することになるため、実際の教育時間は変動することになる。

７．カリキュラムの構成

カリキュラムの構成は下表のとおりである。

表　カリキュラムの構成

	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	手引書をもとに、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可能性を考慮し、迅速かつ適切に対応するためのポイントを学習する。
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。

［ 解説 ］

本カリキュラムは、サイバー攻撃を受けた際に迅速かつ適切に対応する人材を育成することに主眼を置いている。そのため、「第１回　サイバー攻撃の現状」及び「第８回　インシデント対応」の２講座に関する知識及び能力の習得が主な目標と考えている。

目標である、サイバー攻撃を受けた際に迅速かつ適切に実行するためには、サイバー攻撃対策について理解していることが望ましく、「第８回　インシデント対応」の前に、「第６回　サイバー攻撃対策」を学習することが望ましい。

また、必要に応じて、サイバー攻撃に対応するための基礎知識を学習する講座として、「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」を学習することが望ましい。

さらに、サイバー攻撃対策を実行するために、外部委託先などの様々な外部組織との連携が必要になる場合は、「第７回　サプライチェーンのセキュリティ対策」を学習することが望ましい。

なお、「第９回　学習の振り返り」は、学習した内容を再確認するための講座をとしている。

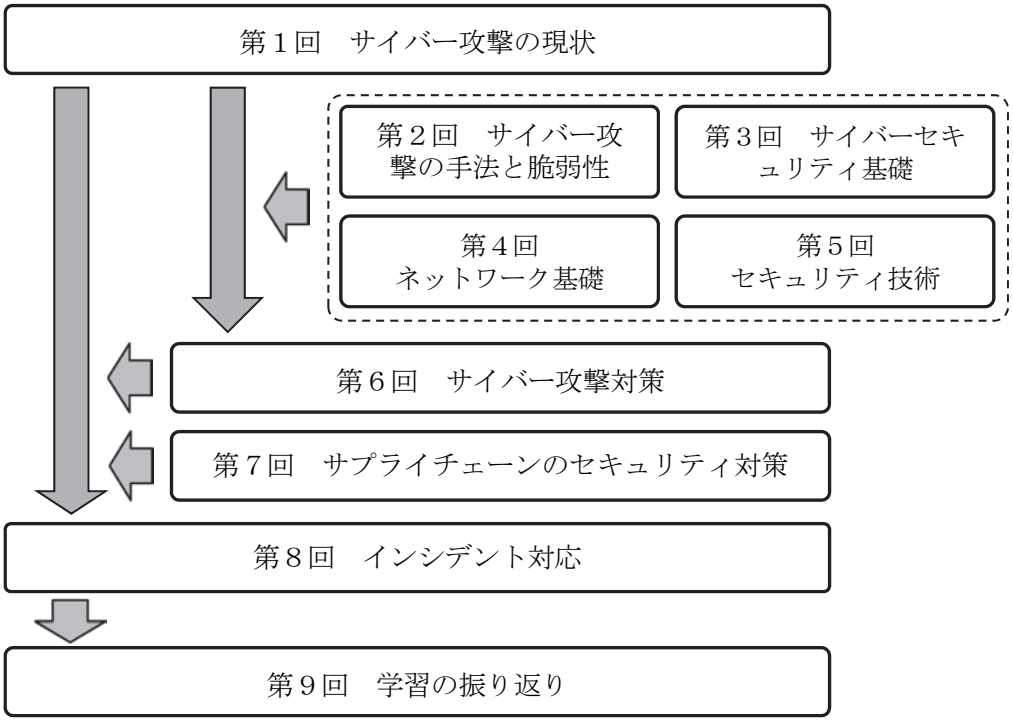


図　各講座の関係図

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、講座は、各鉄道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している。

例えば、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できることを目標とする受講者に対しては、第１回、第８回、第９回の講座を対象とし、鉄道事業者が置かれたサイバー攻撃に関する現状確認とインシデント対応のポイント学習に特化するカリキュラム構成が考えられる。

上記に加え、当該システムを熟知する立場から、サイバー攻撃に対処する専門機関と連携して対応することを目標とする受講者に対しては、第１回、第６回～第９回の講座を対象とし、例えば、サイバー攻撃対策の概要理解に重点を置いたカリキュラム構成が考えられる。この場合、受講者の必要に応じて、第２回～第５回の講座を追加することが考えられる。

８．講座の内容

第１回～第９回までの各講座の内容を次頁より記載する。なお、各講座における構成は以下のとおりである。

［ 解説 ］

各講座における構成は以下のとおりである。

①（講座名）：回数と講座名
② 目　標：習得するスキルの目標を示している。
③ 項目名：講座の目次項目の名称を記載している。
④ 項目の概要：各項目の学習内容のキーワードを記載している。
⑤ 留意点：教材を作成する際にポイントとなる事項を記載している。
⑥ 参考資料：教材を作成する際の参考資料を記載している。

表　各講座における構成イメージ

①　（講座名）		
② 目標		
③ 項目名	④ 項目の概要	⑤ 留意点
⑥【参考資料】		

第１回　サイバー攻撃の現状		
目標	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。	
項目名	項目の概要	留意点
(1) サイバーセキュリティに関する動向	・サイバーセキュリティの必要性 ・国内外のサイバーセキュリティに関する動向	・サイバーセキュリティの必要性や内閣府サイバーセキュリティセンター（NISC)、国土交通省など、国内外のサイバーセキュリティに関する動向を紹介する。
(2) 脅威とインシデント	・鉄道分野におけるインシデント事例 ➢ マルウェア Blaster 感染による列車運行の阻害（2003 年 8 月） ➢ ソウルメトロに対するサイバー攻撃（2014 年 7 月） ➢ サンフランシスコ市営鉄道でランサムウェア感染（2016 年 11 月） ・その他のハッキング[15]事例（周辺システムへの攻撃の波及など） ・攻撃の背景と特徴	・鉄道分野におけるインシデント事例を紹介し、サイバー攻撃対策の重要性を解説する。 ・項目の概要に示した事例は参考であるため、その時点での最新の事例について紹介する。 ・特に、攻撃ベクトル[16]（経路と手段）について解説する。 ・事例から得られた知見や気付きを入れることが望ましい。
(3) 想定される攻撃手法	・システム構成の概要 ・想定される攻撃方法 ➢ スピア型メール[17] ➢ サプライチェーン攻撃[18] ➢ メールの窃取[19] ➢ USB ドロップ攻撃[20] ➢ DDos 攻撃[21]　など	・典型的なシステム構成例を示し、攻撃対象となるネットワーク機器[22]、サーバー機器[23]、ソフトウェア[24]について解説する。 ・システム構成例に基づき、想定される攻撃ベクトル（経路と手段）を解説する。
(4) セキュリティ確保への取り組みの状況	・対策技術 ・対策手法 ・セキュリティ対策のポイント	・セキュリティ確保への対策技術や対策手法を解説する。 ・セキュリティ対策のポイントとなる事項について解説する。
【参考資料】 ・ 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） ・ インシデント対応報告レポート　JPCERT/CC （https://www.jpcert.or.jp/ir/report.html）		

第２回　サイバー攻撃の手法と脆弱性		
目標	鉄道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[25]を理解する。	
項目名	項目の概要	留意点
(1) サイバー攻撃の脅威	・代表的なサイバー攻撃の脅威 ➢ マルウェア[26]感染（マルウェアの種類と感染経路） ➢ DDoS 攻撃 ➢ 不正侵入[27] ➢ リプレイ攻撃[28] ➢ 伝送情報の傍受[29] ➢ 中間者攻撃[30] ➢ ゼロデイ攻撃[31] ➢ ランサム攻撃[32]（ランサムウェア、ランサム DDoS[33]） ➢ ファイルレス攻撃 ➢ アカウントハイジャック[34]	・代表的なサイバー攻撃の脅威について解説する。 ・項目の概要に示した脅威は参考であるため、その時点での最新の脅威情報に基づき解説する。
(2) 脆弱性	・脆弱性とは ・脆弱性を狙ったサイバー攻撃 ・脆弱性への対応	・脆弱性について、リスク[35]を回避するための対応方法について解説する。
【参考資料】 ・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） ・脆弱性対策情報データベース、JVN　iPedia（http://jvndb.jvn.jp/index.html）		

第３回　サイバーセキュリティ基礎		
目標	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。	
項目名	項目の概要	留意点
(1)セキュリティマネジメント	・サイバーセキュリティマネジメントシステム（CSMS[36]）の概要	・サイバーセキュリティマネジメントの基本的な考え方を解説する。 ・PDCA サイクルの確立が重要であることを解説する。 ・規程類の構成について解説する。
(2)資産管理の重要性	・資産[37]とは ・保護すべき資産の識別 ・資産管理の不備がもたらす影響について	・サイバーセキュリティマネジメントの基本となる資産管理の重要性について解説する。
(3)リスク評価の重要性	・リスク評価[38]の概要 ・資産、リスク、脅威、脆弱性を把握することの重要性 ・クラウド[39]利用のリスク	・リスク評価の重要性について解説する。 ・クラウド利用のリスクについて解説する。

【参考資料】

・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）

・制御システムの セキュリティリスク分析ガイド、IPA（https://www.ipa.go.jp/files/000061925.pdf）

第４回　ネットワーク基礎		
目標	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、対応するために必要となるネットワークの知識を学習する。	
項目名	項目の概要	留意点
(1) ネットワークとプロトコル	・OSI 参照モデル[40] ・プロトコル[41] ・LAN[42] と WAN[43] ・LAN の種類とトポロジ[44] ・無線	・ネットワーク構成と動作原理について解説する。 ・サイバー攻撃の概要を把握するために、ネットワークとプロトコルについての基礎知識を解説する。
(2) TCP/IP の概要	・OSI 参照モデルと TCP/IP の関連 ・IP アドレス ・TCP/IP の概要 ➢ 物理層[45] ➢ データリンク層[46] ➢ ネットワーク層[47] ➢ トランスポート層[48]	・ネットワークの基本となる OSI 参照モデルと TCP/IP の関連について解説する。 ・サイバー攻撃の対応を実施するために、TCP/IP の概要についての基礎知識を解説する。
(3) ネットワーク接続機器	・ネットワーク接続機器の種類と役割 ➢ スイッチ[49] ➢ ルータ[50] ➢ アクセスポイント[51] ・IoT 機器[52] に関する脅威	・代表的なネットワーク接続機器について解説し、これらの機器の役割を解説する。 ・代表的な IoT 機器（監視カメラなど）を紹介し、脅威となり得ることを解説する。
【参考資料】 ・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/files/000018486.pdf）		

第５回　セキュリティ技術		
目標	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。	
項目名	項目の概要	留意点
(1) 対策技術の用語と概要	・ファイアウォール（NGFW[53]） ・SIEM[54]（Security Information and Event Management） ・EDR[55]（Endpoint Detection and Response） ・ハードニング[56] ・データダイオード[57]	・手引書の内容を参考に、サイバー攻撃に対する対策技術の用語と概要について解説する。
(2) 多層防御	・多層防御[58]の考え方 ・サイバーセキュリティフレームワーク[59]（特定、防御、検知、対処、復旧）	・サイバー攻撃の対策には多層的に防御することが重要であることを解説する。
(3) フォレンジックの概要	・フォレンジック[60]の概要 ・ファスト・フォレンジック[61]の必要性 ・フォレンジックを実施する際の留意点	・フォレンジックの概要について解説する。 ・ファスト・フォレンジックの必要性について解説する。 ・フォレンジックの目的を明確にし、社内外と連携して期待した時間内に目的とする結果を得るための留意事項について解説する。
【参考資料】 ・情報セキュリティ読本　教育用プレゼン資料　第５章　もっと知りたいセキュリティ技術、IPA（https://www.ipa.go.jp/files/000015331.ppt）		

第６回　サイバー攻撃対策		
目標	手引書をもとに、主なセキュリティ対策の概要を学習する。	
項目名	項目の概要	留意点
(1) 機器・システムのセキュリティ対策	・外部ネットワークとの分離通信のセキュリティ ・他ネットワークとの分離 ・通信のセキュリティ ・マルウェア対策 ・不正処理防止策 ・アクセス制御 ・ログ[62]の取得・保管・保全	・手引書に記載されたサイバー攻撃に対する技術的対策について解説する。 ・外部ネットワークとの分離などのクローズドシステムに関係する対策に重点を置いて解説する。
(2) 運用・管理のセキュリティ対策	・セキュリティ仕様の確認 ・機器などの構成・変更管理 ・外部記憶媒体[63]などのマルウェア対策 ・権限[64]の適切な割当て ・修正プログラムの適用 ・入退管理 ・情報の収集 ・セキュリティ監視	・手引書に記載されたサイバー攻撃に対する運用・管理面での対策について解説する。 ・外部記憶媒体などのマルウェア対策、権限の適切な割当て、入退管理などのクローズドシステムに関係する対策に重点を置いて解説する。
【参考資料】 ・ 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		

第７回　サプライチェーンのセキュリティ対策		
目標	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。	
項目名	項目の概要	留意点
(1) サプライチェーンのセキュリティ対策の重要性	・サプライチェーンの構成（系列企業、ビジネスパートナー、外部委託先） ・サイバーセキュリティ対策の実施及び状況把握 ・対策を怠った場合のシナリオ	・サプライチェーンの管理として実施すべきことの概要を解説する。 ・対策を怠った場合のシナリオを提示し、サプライチェーンのセキュリティ対策の重要性を解説する。（例.サプライチェーンのビジネスパートナーやシステム管理などの委託先がサイバー攻撃に対して無防備であった場合、影響が自社に波及する可能性など）
(2) 外部委託範囲の特定と管理	・供給者[65]との合意（契約）におけるセキュリティの取扱い ・供給者のサービス提供の管理及びレビュー ・供給者のサービス提供の変更に対する管理	・ＩＴシステム管理の外部委託範囲の特定と委託業務を管理することの重要性を解説する。 ・委託範囲、賠償内容、クラウド利用の責任分界点など、確認すべき契約内容のポイントについて解説する。
(3) 情報の入手とその有効活用	・関係当局[66]との連絡 ・専門組織[67]との連絡 ・ベンダー[68]からの情報提供 ・ベンダーサポート[69]	・情報共有活動への参加を通じた攻撃情報の入手とその有効活用のための環境整備の重要性を解説する。 ・ベンダーから提供される脆弱性情報[70]及びサポート内容[71]を確認することの重要性を解説する。
【参考資料】 ・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） ・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）		

第８回　インシデント対応		
目標	インシデント発生の際、その原因がサイバー攻撃である可能性を考慮し、迅速かつ適切に対応するためのポイントを学習する。	
項目名	項目の概要	留意点
(1) インシデント発生時の対応手順	・インシデント対応の概要 ・インシデント発生時の対応手順と役割分担	・インシデント発生の際に担当者（育成対象者を指す。例えば、システム維持管理者）が取る対応の必要性を中心に解説する。 ・インシデント発生の際に、どのような手順で対応していくかを解説する。
(2) インシデント対応体制	・セキュリティインシデントの位置付け ・担当者の役割 ・社内外との連携	・自社におけるセキュリティインシデント（サイバー攻撃に起因する各種の不具合）の対応と従来のシステム障害時の対応との相違点について解説する。 ・自社の体制に基づき、担当者（育成対象者を指す。例えば、システム維持管理者）の役割や社内外の連携について解説する。
(3) 対処時のポイント	・初動の重要性 ・連絡事項（初動対応時に把握すべき事項）	・インシデント対処時のポイントについて解説する。

【参考資料】

・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）

・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）

第９回　学習の振り返り		
目標	学習の振り返りを通して本カリキュラムを総括する。	
項目名	項目の概要	留意点
(1) コースのまとめと振り返り	・コースのまとめと振り返り	・コースの内容の振り返りを行う。 ・受講者の役割を再確認し、役割を実行するために必要となる知識について振り返りを行う。 ・特に、サイバー攻撃に対処（原因究明、復旧）する専門機関と連携し、対応する場合には、用語や攻撃対策の概要について理解しておく必要があることを説明する。
(2) 質疑応答	・質疑応答	・質疑を通じてポイントとなる事項を確認する。 ・事例において紹介した攻撃を受けた場合にどのように対処するかについて、演習形式での討議を実施すると効果が高い。
【参考資料】		

本カリキュラム作成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) 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
3) インシデント対応報告レポート JPCERT/CC
https://www.jpcert.or.jp/ir/report.html
4) 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
5) 脆弱性対策情報データベース、JVN iPedia
http://jvndb.jvn.jp/index.html
6) 「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
7) 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
8) 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
9) 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
10) 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
11) 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
12) 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
13) 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
http://www.mlit.go.jp/common/001127563.pdf
14) Rail Cyber Security Strategy, Rail Delivery Group
https://www.raildeliverygroup.com/about-us/publications.html?task=file.download&id=469772253
15) Cybersecurity For Rail: Not A Single-Shot Approach, THALES Ground Transportation
https://www.thalesgroup.com/sites/default/files/asset/document/cyber_security_whitepaper_hires_0.pdf

用語の定義

本カリキュラムにおいて提示する用語の定義を以下に示す。

(1)**「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。

(2)**「CSIRT」**とは、Computer Security Incident Response Team の略で、セキュリティインシデントなど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。

(3)**「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・分析などを行う事業者も該当する。

(4)**「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おそ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」、「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 13 分野をいう。

(5)**「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など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。

(6)**「サイバーテロ」**とは、インターネットなど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。

(7)**「クローズドシステム」**とは、インターネットなど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。

(8) **「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。

(9) **「標的型攻撃」**とは、特定の組織に狙いを絞り、その組織の業務習慣など内部情報について事前に入念な調査を行った上で、様々な攻撃手法を組み合わせ、その組織に最適化した方法を用いて、執拗に行われる攻撃をいう。典型的なものとしては、組織内部に潜入し、侵入範囲を拡大し、重要な情報を窃取又は破壊する攻撃活動が考えられる。

(10)**「ワーム機能」**とは、対象プログラムを必要とせず、自己複製し、自己増殖するコンピュータプログラムをいう。ネットワークに接続されている他のマシンに出現する。

(11)**「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など特定の制限をかけ、その制限の解除と引き換えに金銭を要求する。

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

(13)**「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。

(14)**「e-learning」**とは、インターネットなどのネットワークを介して学習プロセス、学習状況の進捗管理などを完遂する教育形態をいう。

(15)**「ハッキング」**とは、コンピュータシステムや通信システムの動作を解析したりプログラムを改造・改良したりすること。転じて、他人のシステムを不正な手段で操作したり不正に機密情報を入手したりすること。

(16)**「攻撃ベクトル」**とは、攻撃の経路（脆弱性のある箇所をどこから攻撃するか）と 手段（脆弱性のある箇所をどのような手法で攻撃するか） を組み合わせた攻撃の説明のことをいう。

(17)**「スピア型メール」**とは、特定のターゲットに対して重要なデータや個人情報を奪う目的で送付されるメールのことをいう。

(18)**「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。

(19)**「メールの窃取」**とは、メールが不正に閲覧または取得されること。(個人情報や機密情報の取得あるいは標的型攻撃などに悪用されるおそれがある。)

(20)**「USB ドロップ攻撃」**とは、USB を接続することでマルウェアなどに感染をする攻撃をいう。

(21)**「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などを送出し、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。

(22)**「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。

(23)**「サーバー機器」**とは、他のコンピュータに対し、機能やサービス、データなどを提供する機器のことをいう。

(24)**「ソフトウェア」**とは、コンピュータを動作させる命令や処理手順のまとまり(コンピュータプログラム)。

(25)**「脆弱性」**とは、ソフトウェアやアプリケーションなどにおいて、システムへの不正アクセスやマルウェアなどの攻撃により、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。

(26)**「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。

(27)**「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竄、消去などを行ったりすることをいう。

(28)**「リプレイ攻撃」**とは、不正侵入の手段の一つで、パスワードや暗号鍵などを盗聴し、そのまま再利用することでそのユーザになりすます方法のことをいう。

(29)**「伝送情報の傍受」**とは、情報の送受信において、不正に受信されることをいう。

(30)**「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。

(31)**「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。

(32)**「ランサム攻撃」**とは、ランサムウェアを利用した攻撃をいう。
(33)**「ランサム DDoS」**とは、DDoS 攻撃によって身代金を要求する脅迫型攻撃
(34)**「アカウントハイジャック」**とは、例えば ID やパスワードを不正に取得され、のっとられてしまうことをいう。
(35)**「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。
(36)**「CSMS」**とは、Cyber Security Management System の略で、制御システムを運用する組織や、制御システムの構築・提供を行う組織に対するセキュリティを実現するための考え方をいう。
(37)**「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。
(38)**「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。
(39)**「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。
(40)**「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、コンピュータなど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。
(41)**「プロトコル」**とは、手順、手続き、外交儀礼、議定書、協定など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。
(42)**「LAN」**とは、限られた範囲内にあるコンピュータや通信機器、情報機器などをケーブルや無線電波などで接続し、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。
(43)**「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。
(44)**「トポロジ」**とは、通信ネットワーク上での機器間の接続形態の分類で、ネットワークを構成する機器(ノード)同士がどのような規則性に基づいて繋がれているかを模式的に表したものをいう。
(45)**「物理層」**とは、OSI 参照モデルの第 1 層に位置し、ネットワークの物理的な接続・伝送方式を定めたものをいう。
(46)**「データリンク層」**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、回線やネットワークで物理的に繋がれた二台の機器の間でデータの受け渡しを行うものをいう。
(47)**「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。

(48)**「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、交渉などを担うものをいう。

(49)**「スイッチ」**とは、受信した信号から宛先など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。

(50)**「ルータ」**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。

(51)**「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など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。

(52)**「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。

(53)**「NGFW」**とは、Next Generation Firewall の略で、従来のポートの開閉に加え、トラフィック内のアプリケーションを識別して制御する次世代ファイアウォールのことをいう。

(54)**「SIEM」**とは、Security Information and Event Management の略で、サーバー、ネットワーク、セキュリティなどの機器、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。

(55)**「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、起動プロセスなど）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。

(56)**「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。

(57)**「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。

(58)**「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。

(59)**「サイバーセキュリティフレームワーク」**とは、サイバーセキュリティに関する基本的な考え方や取り組みをいう。

(60)**「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・毀損などについての分析・情報収集などを行う調査手法・技術をいう。

(61)**「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などを目的として、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。

(62)**「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。

(63)**「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。

(64)**「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。

(65)**「供給者」**とは、自社にサービスを提供する事業者をいう。

(66)**「関係当局」**とは、事業に関連した行政上の関係官庁をいう。

(67)**「専門組織」**とは、サイバー攻撃に関する情報提供先をいう。例えば、IPA、JPCERT/CC などである。

(68)**「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。

(69)**「ベンダーサポート」**とは、ベンダーが製品やシステム、サービス提供した後の支援サービスをいう。

(70)**「脆弱性情報」**とは、ソフトウェアやアプリケーションなどにおいて、システムへの不正アクセスやマルウェアなどの攻撃により、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に関する情報の注意喚起または情報支援サービスをいう。

(71)**「サポート内容」**とは、ベンダーの支援サービスのことで、例えば、脆弱性情報に対する質疑など、対応内容をいう。

参考資料２

「航空のサイバーセキュリティに関する人材育成カリキュラム」

航空のサイバーセキュリティに関する
人材育成カリキュラム

平成 30 年 3 月

一般財団法人　運輸総合研究所

目次

カリキュラム要旨

本文書（以下、「本カリキュラム」という）は、航空分野[注1)]の制御システムがサイバー攻撃を受けたときに、迅速かつ適切に対応すべく、実際に対応する人材を育成することに主眼を置いている。迅速かつ適切な対応をするためには、システムを維持管理する人材が、システムに異常が発生した際、その原因がサイバー攻撃[1]である可能性を考慮することが重要である。しかしながら、サイバー攻撃と従来のシステム障害などによる異常には、明確な違いはないと考えられ、システムを維持管理する人材が、サイバー攻撃に関する基礎知識を持たない場合、サイバー攻撃であることに気付くのが遅れる可能性があり、その場合、さらに他のシステムに影響が波及するなど、初動対応に遅れを生じることが懸念される。

また、一般にサイバー攻撃の場合、より高度な知識と適切な対応が必要となるため、サイバー攻撃から防護することを鑑みると、サイバー攻撃に対処（原因究明、復旧など）する専門機関（社内外のセキュリティ担当、CSIRT[2]、セキュリティベンダー[3]など）との連携により対応することが望ましいが、システムを維持管理する人材が、サイバー攻撃に関する基礎知識を持たない場合、適切に連携できないことが懸念される。

国内の航空分野では、業務に関わるシステムは既にＩＴ化されたものも多く、また、今後はＩｏＴ（Internet of Things）[4]化など更なる技術発展を考えると、ＩＴ及びサイバー攻撃に関する基礎知識は必要不可欠であると思われる。

このような状況を踏まえ、各航空事業者[注1)]において、サイバー攻撃を受けた際に初動対応にあたる人材のサイバー攻撃に対する能力の向上が急務であると考え、これを促すために参考となるカリキュラムを検討した。

本カリキュラムが目標とする人材には、平成 28 年度に（一財）運輸総合研究所が作成した「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[注2)]」の対策を実践できる人材としている。このため、本カリキュラムの育成対象者は、各航空事業者が保有する以下のシステムの維持管理あるいは障害対応に従事する人材を想定している。

・運航システム
・予約システム
・フライトインフォメーションシステム

ただし、航空事業者が扱う設備・システムは上記以外にも多数存在し、また、保有するシステムも異なるため、航空事業者により、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。そのため、学習内容は、本カリキュラムの内容を参考にしつつ、各航空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。

なお、新たなサイバーに関する脅威、攻撃が登場した際は、従来の対策では対応できないことも懸念されるため、最新の事例収集や必要な情報を関係者間で共有するなど、情報更新する必要が生じる。

注１）本カリキュラムにおける「航空事業者」は、航空輸送事業者及び空港運営事業者を想定している。また、これらの事業者の業種全般を「航空分野」と称する。

注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」とは、平成 28 年度日本財団助成事業として実施した、「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」における、情報セキュリティ大学院大学の田中英彦学長（当時）を委員長とした検討委員会で付議了承を得た文章であり、航空分野において調査当時に考えられたサイバーセキュリティ対策をまとめたものである。

注３）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、意図的なサイバー攻撃により、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、そのおそ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。なお、国土交通省の外局である運輸安全委員会が調査する「重大インシデント」は、「事故が発生するおそれがあると認められる事態」を指し、鉄道運転事故/航空事故には至らずに済んだものの一歩間違えれば事故が発生していたという状況をいい、本調査における「インシデント」とは意味合いが異なる。

注４）本カリキュラムにおいて、番号が付与されている用語については、巻末の「用語の定義」に説明文を記載している。

１．カリキュラム作成の背景

本カリキュラムは、以下に示す背景から、航空分野のサイバーセキュリティ[5]に関する人材を育成するための参考資料としてとりまとめたものである。
（１）2020 年東京五輪大会の成功に向けて、サイバーテロ[6]対策は重要な課題の一つである。
（２）航空分野におけるサイバーテロは甚大な影響をもたらすおそれがある。
（３）航空分野におけるサイバーセキュリティ人材が不足している。
（４）航空事業者各々で人材を育成するため、参考となるカリキュラムが必要である。

［ 解説 ］

（１）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の一つである。

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サイバーテロ対策が開催国において懸案となっていた。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。

（２）航空分野におけるサイバーテロは甚大な影響をもたらすおそれがある。

航空分野は、我が国のサイバーセキュリティ戦略において重要インフラ[7]分野に指定されており、サイバー攻撃により安全・安定な運航が妨げられると、その影響は甚大になるおそれがある。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。制御システムのＩｏＴ（Internet of Things）化など更なる技術発展を考えると、さらに脅威が増す可能性がある。

（３）航空分野におけるサイバーセキュリティ人材が不足している。

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[注)]では、研究対象とした鉄道分野、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、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。

注）東京オリンピック・パラリンピックに向けた交通機関へのサイバーテロ対策に関する調査研究、（一財）運輸政策研究機構、平成 28 年 3 月

（４）航空事業者各々で人材を育成するため、参考となるカリキュラムが必要である。

サイバーセキュリティ対策は、各航空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、航空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が必要であると考えた。

２．航空事業者の将来望ましい状況

システムのＩＴ化、他システムとの連携、クローズドシステム[8]に対する攻撃手法の高度化など航空事業者の潜在的な脅威は増大していると考えられる。このような状況を踏まえ、航空事業者においては、将来的に以下の状況にあることが望ましい。

（１）インシデント発生の際、その原因がサイバー攻撃である可能性を考慮し、適切に対応できる人材が現場に配置されている。

（２）仮にサイバー攻撃を受けた場合でも対応可能となる体制が整備されている。

（３）サイバー攻撃に対処する専門機関と連携して対処できる体制が整備されている。

（４）インシデント対応に関与する全ての要員がサイバー攻撃の脅威を認識している。

［ 解説 ］

（１）インシデント発生の際、その原因がサイバー攻撃である可能性を考慮し、適切に対応できる人材が現場に配置されている。

航空分野の制御システムがサイバー攻撃を受けた事例は国内で報告されておらず、サイバー攻撃を受けた際に、現場で適切な対応が取れるか現状では不明な状態にあると考えられる。そのため、サイバー攻撃に関する基礎知識を有し、インシデント発生の際、その原因がサイバー攻撃である可能性を考慮し、適切に対応できる人材が現場に配置されていることが望ましい。

（２）仮にサイバー攻撃を受けた場合でも対応可能となる体制が整備されている。

インシデントが発生した時点では、サイバー攻撃が原因か否かは判断できない場合も予想されるため、サイバー攻撃が疑われる場合の報告先を明示するなど、サイバー攻撃を受けた場合でも対応可能となる体制が整備されていることが望ましい。また、自社内においてサイバー攻撃に対応するための計画、実行、評価、改善を繰り返し、体制を継続的に改善することが望ましい。

（３）サイバー攻撃に対処する専門機関と連携して対処できる体制が整備されている。

サイバー攻撃に対処（原因究明、復旧など）する専門機関に、当該システムの知識が不足していた場合、対処が遅れることも予想されるため、より迅速な対処をするためには、システムを熟知する人材とサイバー攻撃に対処する専門機関が連携して対処ができる体制が整備されていることが望ましい。

（４）インシデント対応に従事する全ての要員がサイバー攻撃の脅威を認識している。

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ることから、インシデント対応に従事する全ての要員がサイバー攻撃の脅威を認識していることが望ましい。

３．求められる人材像と必要となる能力

本カリキュラムにおける、求められる人材像とそのために必要となる能力は、以下のとおりである。

（１）求められる人材像

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

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

（２）必要となる能力

・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

［ 解説 ］

「２．航空事業者の将来望ましい状況」で示した状況を実現するために、求められる人材像は、「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」（発行：平成 28 年度、（一財）運輸総合研究所））の対策を実践できる人材とした。具体的には、下表のような定義とした。

表　本カリキュラムにおける、求められる人材像とそのために必要となる能力

（１） 求められる 人材像	・インシデント発生の際、その原因がサイバー攻撃である可能性を考慮し、適切に「対応」[注1)]できる人材。 ・「インシデント対応」[注2)]を、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「対応」できる人材。
（２） 必要となる 能力	１）サイバー攻撃に関わるインシデント対応に関する能力 ・サイバー攻撃に関するインシデント発生時の対応手順を理解し、「対応」できる能力。 ・サイバー攻撃対策を理解し、一連の「対応」ができる能力。 ・サプライチェーンのセキュリティ対策の重要性を理解し、サイバー攻撃に備えた準備ができる能力。 ２）上記に関わる情報技術（ＩＴ）に関する能力 ・「インシデント対応」を行うために必要な情報技術（ＩＴ）に関する知識と能力。

注１）本頁における「対応」とは、対象となるシステムを維持管理する人材が、サイバーに対処（原因究明、復旧など）する専門機関の助言を受けて、システムの復旧につなげる活動などにあたる他、システムを熟知する立場から、サイバーに対処（原因究明、復旧など）する専門機関にシステムに関する助言や援助を行うことを指す。

注２）「インシデント対応」には、以下の活動が含まれる。

①インシデント発生時：インシデント発生時に、被害を局限化、最小化し、速やかな復旧につなげる活動

②インシデント発生後：インシデントから復旧し、再発を防止することを目的とする活動

③インシデント発生前：インシデント発生に備えた「準備」の活動

４．育成対象者

本カリキュラムの育成対象者は、事業部門のシステムを維持管理する人材である。インシデントが発生した場合、その原因がサイバー攻撃か否か判断できない場合も含め、対応する人材を想定する。

［ 解説 ］

各航空事業者の組織（役職と部門）において、本カリキュラムの育成対象者は下表のとおりであり、事業部門のシステムを維持管理する人材である。（凡例：「○」）

なお、経営者層と管理者層は、サイバーセキュリティに対する意識改革の必要性などが指摘されているが、優先順位を踏まえ本カリキュラムでは対象外とした。また、事業部門のシステム担当以外も対象外とした。なお、管理者層は、将来的には技術者層と経営層との間のコミュニケーションを円滑にする「橋渡し人材」の一翼を担うことが期待される。（凡例：「-」）

表　本カリキュラムの育成対象者（凡例：○）

部門 / 役職	事業部門（システム担当）	事業部門（システム担当以外）
経営者層	－	
管理者層	－	－
技術者層	○	－

注１）管理者層とは、現場から報告を受け、各所に報告をする方を指す。
注２）技術者層とは、システムを扱う現場において、実際にシステムの維持管理などをする方を指す。

なお、サイバー攻撃に対応する一連の役割とそれを担当する部署は、各航空事業者で異なると思われるため、本カリキュラムにおける想定を以下の表に示す。

表　サイバー攻撃に対応する一連の役割と担当部署の想定（運航システムの例） 注1)

役割	担当部署	望まれる能力
システム操作 システム異常の検知・通報	システム運用部門 （オペレーター）	異常の原因としてサイバー攻撃があるという意識をもち、適切に連絡ができる能力
システム維持管理 システム障害対応	システム維持管理部門 （外部委託先を含む）	サイバー攻撃に備えた準備、インシデント発生時の対応、サイバー攻撃対策などの一連の活動に「対応」注2)できる能力
サイバー攻撃の インシデント対応の立案、実行	セキュリティ担当部門 CSIRT・情報システム部門 セキュリティベンダー	サイバー攻撃に備えた準備、インシデント発生時の対応、サイバー攻撃対策などの一連の活動を立案、実行できる能力

注 1）黒枠は本カリキュラムで想定する育成対象者を指す。
注 2）本頁における「対応」とは、対象となるシステムを維持管理する人材が、サイバーに対処（原因究明、復旧など）する専門機関の助言を受けて、システムの復旧につなげる活動などにあたる他、システムを熟知する立場から、サイバーに対処（原因究明、復旧など）する専門機関にシステムに関する助言や援助を行うことを指す。

５．カリキュラムの特徴

本カリキュラムの特徴は以下のとおりである。
（１）航空事業者の実態を踏まえ、必要と思われる項目を選定
（２）サイバー攻撃の被害事例を活用した構成
（３）最新のサイバー攻撃の動向を踏まえた内容を含む記載

［ 解説 ］

本カリキュラムの特徴は以下のとおりである。

（１）航空事業者の実態を踏まえ、必要と思われる項目を選定

2020 年東京五輪大会までに人材育成を行う必要があることから、昨年度の研究成果である「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」（発行：平成 28 年度、（一財）運輸総合研究所））」に記載されている対策や今年度実施した机上演習[9]の知見などを踏まえ、必要と思われる項目を選定した。

（２）サイバー攻撃の被害事例を活用した構成

海外の人材育成カリキュラムによると、サイバー攻撃の被害事例を活用すると、サイバー攻撃の脅威を効果的に認識できるとあることから、学習の初期段階（第１回）において、サイバー攻撃の被害事例を紹介し、以降の学習の段階に繋げる構成とした。

（３）最新のサイバー攻撃の動向を踏まえた内容を含む記載

標的型攻撃[10]の進化あるいはワーム機能[11]を有したランサムウェア[12]、ファイルレス攻撃[13]の登場など、脅威は複雑化、高度化していることから、現時点で把握できる最新のサイバー攻撃手法の内容を含む記載とした。

６．カリキュラム作成にあたっての前提条件

本カリキュラムは以下のような前提に基づいて作成している。
（２）受講者は、情報セキュリティ[14]に関する基礎知識を有している。
（２）講座は、各航空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。

［ 解説 ］

（１）受講者は、情報セキュリティに関する基礎知識を有している。

本カリキュラムの受講者は、情報セキュリティに関する基礎知識を有していることを前提としている。具体的には、以下の内容を理解していることを想定している。

・情報セキュリティ読本　教育用プレゼン資料　第１章 今日のセキュリティリスク
（https://www.ipa.go.jp/files/000015327.ppt）
・情報セキュリティ読本　教育用プレゼン資料　第２章 情報セキュリティの基礎
（https://www.ipa.go.jp/files/000015328.ppt）
・情報セキュリティ読本　教育用プレゼン資料　第 4 章 組織の一員としての情報セキュリティ対策
（https://www.ipa.go.jp/files/000015330.ppt）

（２）講座は、各航空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。

航空事業者により、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。そのため、講座は、各航空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

ただし、新たなサイバーに関する脅威、攻撃が登場した際は、従来の対策では対応できないことも懸念されるため、最新事例の収集や必要な情報を関係者間で共有するなど、情報更新する必要が生じる。

手引書の内容を教育するには、自社の資産（システム構成など）に応じて特化した内容となるため、原則として、講師は自社の社員が望ましい。しかしながら、講師としての能力を持つ人材の不足や講義の準備にかかる講師の負担など、各航空事業者で状況は異なるため、汎用的な内容については、既存の e-learning[15]の活用や、講師を外部委託するなど、適宜、講師を効率的に選択することを推奨する。

また、講義形式は、講義（座学）だけではなく、演習を取り入れると効果的であると思われる。

なお、カリキュラムを作成する上では所要時間の想定が必要であると思われたため、必要と考える教育項目と、各航空事業者の業務の状況などを勘案して、カリキュラム全体で３日（20 時間程度）を想定した。ここで示した所要時間はあくまで目安であり、各航空事業者が必要に応じて、学習項目を追加、削除、修正することになるため、実際の教育時間は変動することになる。

７．カリキュラムの構成

カリキュラムの構成は下表のとおりである。

表　カリキュラムの構成

	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	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する専門機関と連携し、対応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	手引書をもとに、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	インシデントが発生した際、その原因がサイバー攻撃である可能性を考慮し、迅速かつ適切に対応するためのポイントを学習する。
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。

［ 解説 ］

本カリキュラムは、サイバー攻撃を受けた際に迅速かつ適切に対応する人材を育成することに主眼を置いている。そのため、「第１回　サイバー攻撃の現状」及び「第８回　インシデント対応」の２講座に関する知識及び能力の習得が主な目標と考えている。

目標である、サイバー攻撃を受けた際に迅速かつ適切に実行するためには、サイバー攻撃対策について理解していることが望ましく、「第８回　インシデント対応」の前に、「第６回　サイバー攻撃対策」を学習することが望ましい。

また、必要に応じて、サイバー攻撃に対応するための基礎知識を学習する講座として、「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」を学習することが望ましい。

さらに、サイバー攻撃対策を実行するために、外部委託先などの様々な外部組織との連携が必要になる場合は、「第７回　サプライチェーンのセキュリティ対策」を学習することが望ましい。

なお、「第９回　学習の振り返り」は、学習した内容を再確認するための講座をとしている。

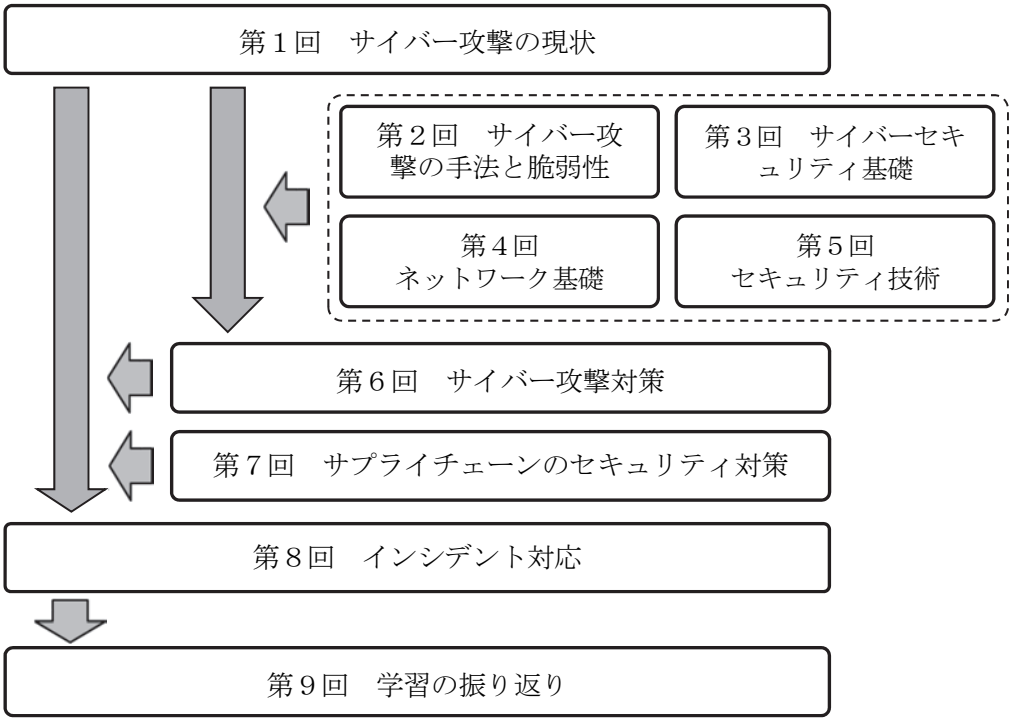


図　各講座の関係図

［ 解説 ］

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、講座は、各航空事業者の実態を鑑み、必要に応じて取捨選択することも可能である。

例えば、航空分野の業務に関わるシステムはＩＴ技術を基盤としている場合が多いため、ネットワーク技術に精通した受講者に対しては、第４回の講座を対象外とすることも考えられる。

また、サイバー攻撃対策やサイバー攻撃の準備に関する知識を有している受講者に対しては、第１回、第８回、第９回の講座を対象とし、航空事業者が置かれたサイバー攻撃に関する現状確認とインシデント対応のポイント学習に特化するカリキュラム構成も考えられる。

さらに、新規配属者への導入教育のように、必ずしもサイバー攻撃対策に関する基礎知識を有さない受講者に対しては、第１回、第６回～第９回の講座を対象とし、例えば、サイバー攻撃対策の概要理解に重点を置いたカリキュラム構成が考えられる。この場合、受講者の必要に応じて、第２回～第５回の講座追加することが考えられる。

８．講座の内容

第１回～第９回までの各講座の内容を次頁より記載する。なお、各講座における構成は以下のとおりである。

［ 解説 ］

各講座における構成（下表参照）は以下のとおりである。

①（講座名）：回数と講座名
② 目　標：習得するスキルの目標を示している。
③ 項目名：講座の目次項目の名称を記載している。
④ 項目の概要：各項目の学習内容のキーワードを記載している。
⑤ 留意点：教材を作成する際にポイントとなる事項を記載している。
⑥ 参考資料：教材を作成する際の参考資料を記載している。

表　各講座における構成イメージ

<table>
<tr><td colspan="3">①　（講座名）</td></tr>
<tr><td>② 目標</td><td colspan="2"></td></tr>
<tr><td>③ 項目名</td><td>④ 項目の概要</td><td>⑤ 留意点</td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td colspan="3">⑥【参考資料】</td></tr>
</table>

第１回　サイバー攻撃の現状		
目標	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。	
項目名	項目の概要	留意点
(1) サイバーセキュリティに関する動向	・サイバーセキュリティの必要性 ・国内外のサイバーセキュリティに関する動向	・サイバーセキュリティの必要性や内閣府サイバーセキュリティセンター（NISC）、国土交通省など、国内外のサイバーセキュリティに関する動向を紹介する。
(2) 脅威とインシデント	・航空分野におけるインシデント事例 ➢ ベトナム航空へのサイバー攻撃（2016 年 7 月） ➢ ポーランド航空へのサイバー攻撃（2016 年 6 月） ・その他のハッキング[16]事例（周辺システムへの攻撃の波及など） ・攻撃の背景と特徴	・航空分野におけるインシデント事例を紹介し、サイバー攻撃対策の重要性を解説する。 ・項目の概要に示した事例は参考であるため、その時点での最新の事例について紹介する。 ・攻撃ベクトル[17]（経路と手段）について解説する。 ・事例から得られた知見や気付きを入れることが望ましい。
(3) 想定される攻撃手法	・システム構成の概要 ・想定される攻撃方法 ➢ スピア型メール[18] ➢ サプライチェーン攻撃[19] ➢ メールの窃取[20] ➢ USB ドロップ攻撃[21] ➢ DDoS 攻撃[22]　など	・典型的なシステム構成例を示し、攻撃対象となるネットワーク機器[23]、サーバー機器[24]、ソフトウェア[25]について解説する。 ・システム構成例に基づき、想定される攻撃ベクトル（経路と手段）を解説する。
(4) セキュリティ確保への取り組みの状況	・対策技術 ・対策手法 ・セキュリティ対策のポイント	・セキュリティ確保への対策技術や対策手法を解説する。 ・セキュリティ対策のポイントとなる事項について解説する。

【参考資料】
・ 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）
・ インシデント対応報告レポート　JPCERT/CC
（https://www.jpcert.or.jp/ir/report.html）

第２回　サイバー攻撃の手法と脆弱性		
目標	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[26]を理解する。	
項目名	項目の概要	留意点
(1) サイバー攻撃の脅威	・代表的なサイバー攻撃の脅威 ➢ マルウェア[27]感染（マルウェアの種類と感染経路） ➢ DDoS 攻撃 ➢ 不正侵入[28] ➢ リプレイ攻撃[29] ➢ 伝送情報の傍受[30] ➢ 中間者攻撃[31] ➢ ゼロデイ攻撃[32] ➢ ランサム攻撃[33]（ランサムウェア、ランサム DDoS[34]） ➢ ファイルレス攻撃 ➢ アカウントハイジャック[35]	・代表的なサイバー攻撃の脅威について解説する。 ・項目の概要に示した脅威は参考であるため、その時点での最新の脅威情報に基づき解説する。
(2) 脆弱性	・脆弱性とは ・脆弱性を狙ったサイバー攻撃 ・脆弱性への対応	・脆弱性について、リスク[36]を回避するための対応方法について解説する。
【参考資料】 ・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） ・脆弱性対策情報データベース、JVN　iPedia（http://jvndb.jvn.jp/index.html）		

第３回　サイバーセキュリティ基礎		
目標	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。	
項目名	項目の概要	留意点
(1)セキュリティマネジメント	・サイバーセキュリティマネジメントシステム（CSMS[37]）の概要	・サイバーセキュリティマネジメントの基本的な考え方を解説する。 ・PDCA サイクルの確立が重要であることを解説する。 ・規程類の構成について解説する。
(2)資産管理の重要性	・資産[38]とは ・保護すべき資産の識別 ・資産管理の不備がもたらす影響について	・サイバーセキュリティマネジメントの基本となる資産管理の重要性について解説する。
(3)リスク評価の重要性	・リスク評価[39]の概要 ・資産、リスク、脅威、脆弱性を把握することの重要性 ・クラウド[40]利用のリスク	・リスク評価の重要性について解説する。 ・クラウド利用のリスクについて解説する。

【参考資料】

・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）

・制御システムの セキュリティリスク分析ガイド、IPA（https://www.ipa.go.jp/files/000061925.pdf）

第４回　ネットワーク基礎		
目標	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、対応するために必要となるネットワークの知識を学習する。	
項目名	項目の概要	留意点
(1) ネットワークとプロトコル	・OSI 参照モデル[41] ・プロトコル[42] ・LAN[43] と WAN[44] ・LAN の種類とトポロジ[45] ・無線	・ネットワーク構成と動作原理について解説する。 ・サイバー攻撃の概要を把握するために、ネットワークとプロトコルについての基礎知識を解説する。
(2) TCP/IP の概要	・OSI 参照モデルと TCP/IP の関連 ・IP アドレス ・TCP/IP の概要 ➢ 物理層[46] ➢ データリンク層[47] ➢ ネットワーク層[48] ➢ トランスポート層[49]	・ネットワークの基本となる OSI 参照モデルと TCP/IP の関連について解説する。 ・サイバー攻撃の対応を実施するために、TCP/IP の概要についての基礎知識を解説する。
(3) ネットワーク接続機器	・ネットワーク接続機器の種類と役割 ➢ スイッチ[50] ➢ ルータ[51] ➢ アクセスポイント[52] ・IoT 機器[53] に関する脅威	・代表的なネットワーク接続機器について解説し、これらの機器の役割を解説する。 ・代表的な IoT 機器（監視カメラなど）を紹介し、今後脅威となり得ることを解説する。
【参考資料】 ・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/files/000018486.pdf)		

第５回　セキュリティ技術		
目標	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。	
項目名	項目の概要	留意点
(1) 対策技術の用語と概要	・ファイアウォール（NGFW[54]） ・SIEM[55]（Security Information and Event Management） ・EDR[56]（Endpoint Detection and Response） ・ハードニング[57] ・データダイオード[58]	・手引書の内容を参考に、サイバー攻撃に対する対策技術の用語と概要について解説する。
(2) 多層防御	・多層防御[59]の考え方 ・サイバーセキュリティフレームワーク[60]（特定、防御、検知、対処、復旧）	・サイバー攻撃の対策には多層的に防御することが重要であることを解説する。
(3) フォレンジックの概要	・フォレンジック[61]の概要 ・ファスト・フォレンジック[62]の必要性 ・フォレンジックを実施する際の留意点	・フォレンジックの概要について解説する。 ・ファスト・フォレンジックの必要性について解説する。 ・フォレンジックの目的を明確にし、社内外と連携して期待した時間内に目的とする結果を得るための留意事項について解説する。
【参考資料】 ・情報セキュリティ読本　教育用プレゼン資料　第５章　もっと知りたいセキュリティ技術、IPA（https://www.ipa.go.jp/files/000015331.ppt）		

第６回　サイバー攻撃対策		
目標	手引書をもとに、主なセキュリティ対策の概要を学習する。	
項目名	項目の概要	留意点
(1) 設備・システムのセキュリティ対策	・外部ネットワークとの分離 ・他ネットワークとの接続 ・通信のセキュリティ ・マルウェア対策 ・不正処理防止策 ・アクセス制御 ・ログ[63]の取得・保管・保全	・手引書に記載されたサイバー攻撃に対する技術的対策について解説する。 ・他ネットワークとの接続、マルウェア対策、ログの取得・保管・保全などのシステム維持管理者が理解しておくべき対策に重点を置いて解説する。
(2) 運用・管理のセキュリティ対策	・セキュリティ仕様の確認 ・機器・外部記憶媒体[64]及びデータの管理 ・外部記憶媒体のマルウェア対策 ・権限[65]の適切な割当 ・セキュリティパッチ[66]の適用 ・入退管理 ・情報の収集 ・セキュリティ監視 ・内部不正[67]対策	・手引書に記載されたサイバー攻撃に対する運用・管理面での対策について解説する。 ・外部記憶媒体のマルウェア対策、セキュリティパッチの適用、情報の収集などのシステム維持管理者が理解しておくべき対策に重点を置いて解説する。
【参考資料】 ・ 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		

第７回　サプライチェーンのセキュリティ対策		
目標	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。	
項目名	項目の概要	留意点
(1) サプライチェーンのセキュリティ対策の重要性	・サプライチェーンの構成（系列企業、ビジネスパートナー、外部委託先） ・サイバーセキュリティ対策の実施及び状況把握 ・対策を怠った場合のシナリオ	・サプライチェーンの管理として実施すべきことの概要を解説する。 ・対策を怠った場合のシナリオを提示し、サプライチェーンのセキュリティ対策の重要性を解説する。（例.サプライチェーンのビジネスパートナーやシステム管理などの委託先がサイバー攻撃に対して無防備であった場合、影響が自社に波及する可能性など）
(2) 外部委託範囲の特定と管理	・供給者[68]との合意（契約）におけるセキュリティの取扱い ・供給者のサービス提供の管理及びレビュー ・供給者のサービス提供の変更に対する管理	・ＩＴシステム管理の外部委託範囲の特定と委託業務を管理することの重要性を解説する。 ・委託範囲、賠償内容、クラウド利用の責任分界点など、確認すべき契約内容のポイントについて解説する。
(3) 情報の入手とその有効活用	・関係当局との連絡[69] ・専門組織との連絡[70] ・ベンダー[71]からの情報提供 ・ベンダーサポート[72]	・情報共有活動への参加を通じた攻撃情報の入手とその有効活用のための環境整備の重要性を解説する。 ・ベンダーから提供される脆弱性情報[73]及びサポート内容[74]を確認することの重要性を解説する。

【参考資料】
・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）
・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）

第８回　インシデント対応		
目標	インシデント発生の際、その原因がサイバー攻撃である可能性を考慮し、迅速かつ適切に対応するためのポイントを学習する。	
項目名	項目の概要	留意点
(1) インシデント発生時の対応手順	・インシデント対応の概要 ・インシデント発生時の対応手順と役割分担	・インシデント発生の際に担当者（育成対象者を指す。例えば、システム維持管理者）が取る対応の必要性を中心に解説する。 ・インシデント発生の際に、どのような手順で対応していくかを解説する。
(2) インシデント対応体制	・セキュリティインシデントの位置付け ・担当者の役割 ・社内外との連携	・自社におけるセキュリティインシデント（サイバー攻撃に起因する各種の不具合）の対応と従来のシステム障害時の対応との相違点について解説する。 ・自社の体制に基づき、担当者（育成対象者を指す。例えば、システム維持管理者）の役割や社内外の連携について解説する。
(3) 初動対応のポイント	・初動対応の重要性 ・連絡事項（初動対応時に把握すべき事項）	・インシデント発生時の初動対応のポイントについて解説する。

【参考資料】

・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）

・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）

第９回　学習の振り返り		
目標	学習の振り返りを通して本カリキュラムを総括する。	
項目名	項目の概要	留意点
(1) コースのまとめと振り返り	・コースのまとめと振り返り	・コースの内容の振り返りを行う。 ・受講者の役割を再確認し、役割を実行するために必要となる知識について振り返りを行う。 ・特に、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する場合には、用語や攻撃対策の概要について理解しておく必要があることを説明する。
(2) 質疑応答	・質疑応答	・質疑を通じてポイントとなる事項を確認する。 ・事例において紹介した攻撃を受けた場合にどのように対処するかについて、演習形式での討議を実施すると効果が高い。
【参考資料】		

本カリキュラム作成にあたっての参考資料

1) 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
2) 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
3) インシデント対応報告レポート JPCERT/CC
https://www.jpcert.or.jp/ir/report.html
4) 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
5) 脆弱性対策情報データベース、JVN iPedia
http://jvndb.jvn.jp/index.html
6) 「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
7) 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
8) 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
9) 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
10) 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
11) 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
12) 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
13) 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
14) Aviation Cyber Security Toolkit, IATA
http://www.iata.org/publications/store/Pages/aviation-cyber-security-toolkit.aspx

用語の定義

本カリキュラムにおいて提示する用語の定義を以下に示す。

(1) **「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。

(2) **「CSIRT」**とは、Computer Security Incident Response Team の略で、セキュリティインシデントなど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。

(3) **「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・分析などを行う事業者も該当する。

(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など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。

(6) **「サイバーテロ」**とは、インターネットなど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。

(7) **「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おそ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」、「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 13 分野をいう。

(8) **「クローズドシステム」**とは、インターネットなど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。

(9) **「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。

(10) **「標的型攻撃」**とは、特定の組織に狙いを絞り、その組織の業務習慣など内部情報について事前に入念な調査を行った上で、様々な攻撃手法を組み合わせ、その組織に最適化した方法を用いて、執拗に行われる攻撃をいう。典型的なものとしては、組織内部に潜入し、侵入範囲を拡大し、重要な情報を窃取又は破壊する攻撃活動が考えられる。

(11) **「ワーム機能」**とは、対象プログラムを必要とせず、自己複製し、自己増殖するコンピュータプログラムをいう。ネットワークに接続されている他のマシンに出現する。

(12) **「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など特定の制限をかけ、その制限の解除と引き換えに金銭を要求する。

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

(14) **「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。

(15)**「e-learning」**とは、インターネットなどのネットワークを介して学習プロセス、学習状況の進捗管理などを完遂する教育形態をいう。

(16)**「ハッキング」**とは、コンピュータシステムや通信システムの動作を解析したりプログラムを改造・改良したりすること。転じて、他人のシステムを不正な手段で操作したり不正に機密情報を入手したりすること。

(17)**「攻撃ベクトル」**とは、攻撃の経路（脆弱性のある箇所をどこから攻撃するか）と 手段（脆弱性のある箇所をどのような手法で攻撃するか） を組み合わせた攻撃の説明のことをいう。

(18)**「スピア型メール」**とは、特定のターゲットに対して重要なデータや個人情報を奪う目的で送付されるメールのことをいう。

(19)**「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。

(20)**「メールの窃取」**とは、メールが不正に閲覧または取得されること。(個人情報や機密情報の取得あるいは標的型攻撃などに悪用される恐れがある。)

(21)**「USB ドロップ攻撃」**とは、USB を接続することでマルウェアなどに感染をする攻撃をいう。

(22)**「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などを送出し、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。

(23)**「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。

(24)**「サーバー機器」**とは、他のコンピュータに対し、機能やサービス、データなどを提供する機器のことをいう。

(25)**「ソフトウェア」**とは、コンピュータを動作させる命令や処理手順のまとまり(コンピュータプログラム)。

(26)**「脆弱性」**とは、ソフトウェアやアプリケーションなどにおいて、システムへの不正アクセスやマルウェアなどの攻撃により、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。

(27)**「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。

(28)**「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竄、消去などを行ったりすることをいう。

(29)**「リプレイ攻撃」**とは、不正侵入の手段の一つで、パスワードや暗号鍵などを盗聴し、そのまま再利用することでそのユーザになりすます方法のことをいう。

(30)**「伝送情報の傍受」**とは、情報の送受信において、不正に受信されることをいう。

(31)**「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。

(32)**「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。

(33)**「ランサム攻撃」**とは、ランサムウェアを利用した攻撃をいう。

(34)**「ランサム DDoS」**とは、DDoS 攻撃によって身代金を要求する脅迫型攻撃

(35)**「アカウントハイジャック」**とは、例えば ID やパスワードを不正に取得され、のっとられてしまうことをいう。

(36)**「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。

(37)**「CSMS」**とは、Cyber Security Management System の略で、制御システムを運用する組織や、制御システムの構築・提供を行う組織に対するセキュリティを実現するための考え方をいう。

(38)**「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。

(39)**「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。

(40)**「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。

(41)**「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、コンピュータなど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。

(42)**「プロトコル」**とは、手順、手続き、外交儀礼、議定書、協定など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。

(43)**「LAN」**とは、限られた範囲内にあるコンピュータや通信機器、情報機器などをケーブルや無線電波などで接続し、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。

(44)**「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。

(45)**「トポロジ」**とは、通信ネットワーク上での機器間の接続形態の分類で、ネットワークを構成する機器(ノード)同士がどのような規則性に基づいて繋がれているかを模式的に表したものをいう。

(46)**「物理層」**とは、OSI 参照モデルの第 1 層に位置し、ネットワークの物理的な接続・伝送方式を定めたものをいう。

(47)**「データリンク層」**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、回線やネットワークで物理的に繋がれた二台の機器の間でデータの受け渡しを行うものをいう。

(48)**「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。

(49)**「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、交渉などを担うものをいう。

(50)**「スイッチ」**とは、受信した信号から宛先など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。

(51)**「ルータ」**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。

(52)**「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など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。

(53)**「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。

(54)**「NGFW」**とは、Next Generation Firewall の略で、従来のポートの開閉に加え、トラフィック内のアプリケーションを識別して制御する次世代ファイアウォールのことをいう。

(55)**「SIEM」**とは、Security Information and Event Management の略で、サーバー、ネットワーク、セキュリティなどの機器、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。

(56)**「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、起動プロセスなど）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。

(57)**「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。

(58)**「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。

(59)**「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。

(60)**「サイバーセキュリティフレームワーク」**とは、サイバーセキュリティに関する基本的な考え方や取り組みをいう。

(61)**「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・毀損などについての分析・情報収集などを行う調査手法・技術をいう。

(62)**「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などを目的として、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。

(63)**「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。

(64)**「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。

(65)**「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。
(66)**「セキュリティパッチ」**とは、セキュリティ脆弱性などの不具合を解消するためのプログラムをいう。
(67)**「内部不正」**とは、本カリキュラムでは内部者（役員・職員、又は元役員・元職員で離職した者）が、重要情報や情報システムなどの情報資産の窃取、持ち出し、漏えい、消去・破壊などを行うことをいう。内部者が退職後に在職中に得ていた情報を漏えいする行為などについても対象とする。
(68)**「供給者」**とは、自社にサービスを提供する事業者をいう。
(69)**「関係当局」**とは、事業に関連した行政上の関係官庁をいう。
(70)**「専門組織」**とは、サイバー攻撃に関する情報提供先をいう。例えば、IPA、JPCERT/CC などである。
(71)**「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。
(72)**「ベンダーサポート」**とは、ベンダーが製品やシステム、サービス提供した後の支援サービスをいう。
(73)**「脆弱性情報」**とは、ソフトウェアやアプリケーションなどにおいて、システムへの不正アクセスやマルウェアなどの攻撃により、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に関する情報の注意喚起または情報支援サービスをいう。
(74)**「サポート内容」**とは、ベンダーの支援サービスのことで、例えば、脆弱性情報に対する質疑など、対応内容をいう。