交通分野へのサイバー攻撃に対する
セキュリティ人材育成等に関する調査研究

報告書

2020 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、令和元年度日本財団助成事業として実施した「交通分野へのサイバー攻撃に対するセキュリティ人材育成等に関する調査研究」の成果をまとめたものである。

サイバーセキュリティについて、政府においては、東京オリンピック・パラリンピックの開催にあたり、過去のオリンピック大会期間中に大規模なサイバー攻撃を受けていることを踏まえ、平成 27 年にサイバーセキュリティ戦略本部会合において安倍晋三内閣総理大臣が関係閣僚に指示を出し、サイバー攻撃対策の検討・準備を進めてきたところである。

運輸総合研究所では、平成 27 年度から 5 年にわたってサイバーセキュリティの調査研究を行ってきた。平成 27 年度・28 年度の 2 年間で「東京オリンピック・パラリンピックに向けた交通機関へのサイバーテロ対策に関する調査研究」を実施し、交通事業者のセキュリティリスク分析を踏まえ、国内外の対策ガイドラインなどを整理し、それらに基づいて、鉄道分野と航空分野の対策をとりまとめた手引きの作成を行った。

この成果を踏まえて、平成 29 年度には、作成した手引きを実践する人材を育成することを目指し、人材育成カリキュラムの作成を行い、平成 30 年度には当該カリキュラムに基づき、鉄道分野・航空分野の人材育成の教材を作成し、教育を実施した。

本年度調査では、昨年度調査で作成した鉄道分野及び航空分野の教材を用い、システム維持管理者を対象とした教育の実施、CSIRT 要員を対象とした机上演習の実施、ならびに最新情報提供セミナーを実施し、エキスパート人材の育成に取り組んだ。また、経営層をターゲットと位置付けてサイバーセキュリティ対策として経営層がとるべき施策について検討を行い、10 の施策として取りまとめ、監査役・経営層を対象としたセミナーを実施して幅広く周知するとともに、サイバーセキュリティへの意識・理解の向上に取り組んだ。

本研究の実施にあたっては、田中英彦 岩崎学園理事・情報セキュリティ大学院大学名誉教授・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くとともに、一般社団法人 日本生活問題研究所のご協力をいただいた。

ここにこれらの皆様方に対して、改めて深く感謝の意を表す次第である。

令和 2 年 3 月

一般財団法人　運輸総合研究所
会長　　宿利　正史

「令和元年度　サイバー攻撃に対する人材育成に関する調査研究」検討委員会
名　　簿

＜敬称略・順不同＞　※（　）内は上記の前任者

委員長	田中　英彦	学校法人 岩崎学園理事 情報セキュリティ大学院大学 名誉教授・東京大学　名誉教授
委　員	大久保 隆夫	情報セキュリティ大学院大学 情報セキュリティ研究科　教授
〃	古関　隆章	東京大学大学院　工学系研究科　電気系工学専攻　教授
〃	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
〃	大嶋　孝友	国土交通省　総合政策局　情報政策課　サイバーセキュリティ対策室 室長
〃	金子　修久	内閣官房　内閣サイバーセキュリティセンター　参事官
〃	舘　剛司	公益財団法人 東京オリンピック・パラリンピック競技大会組織委員会　テクノロジーサービス局　局長
〃		鉄道関係者
〃		航空・空港関係者
〃	宿利　正史	一般財団法人　運輸総合研究所　会長
〃	佐藤　善信 （春成　誠）	一般財団法人　運輸総合研究所　理事長
事務局		一般財団法人　運輸総合研究所
作業協力		一般社団法人　日本生活問題研究所　サイバーセキュリティ支援センター

目次

第１章　序文 1
１．１．研究背景 1
１．２．研究目的 2
１．３．これまでの研究成果 2
１．４．本年度の研究内容 3
第２章　経営層がとるべきサイバーセキュリティ対策に関する検討 4
２．１．目的 4
２．２．施策整理の観点 5
２．３．進め方 7
２．４．ヒアリング調査及び事例収集 8
２．４．１．ヒアリング調査 8
２．４．２．政府施策の動向 10
２．４．３．企業を取り巻く市場動向 24
２．４．４．監査等の手法の活用 29
２．４．５．国内外の事例（公開資料より） 34
２．５．サイバーセキュリティ対策推進のための施策検討 40
２．５．１．検討方針の設定 40
２．５．２．施策の検討 42
２．５．３．検討結果 46
２．６．経営層がとるべきサイバーセキュリティ対策の具体的施策 47
２．６．１．施策 47
２．６．２．施策間の関係とポイント 59
２．７．施策の評価 61
２．７．１．施策の特徴 61
２．７．２．サイバーセキュリティ経営ガイドラインとの関係 62
２．８．オリパラ対策の検討 71
２．９．まとめ 72
第３章　経営層を対象とした啓発セミナーの実施 74
３．１．啓発セミナー 74
第４章　エキスパート人材の育成 75
４．１．最新情報提供セミナー 75
４．２．机上演習の実施 76
４．２．１．日程 76
４．２．２．演習１日目 76
４．２．３．演習２日目 77
４．２．４．得られた知見 78
４．３．教育（本格実施） 79

４．３．１．日程 79
４．３．２．アンケート結果（鉄道分野） 80
４．３．３．アンケート結果（航空分野） 83
第５章　総括 86
５．１．本研究の総括 86
５．２．サイバーセキュリティ対策に関する提言 87
５．３．鉄道分野 90
５．４．航空分野 90
おわりに 92
参考資料 93
用語の定義 95

セミナー資料

第１章　序文

１．１．研究背景

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

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

鉄道分野、航空・空港分野においては、サイバーセキュリティ戦略本部において「重要インフラ分野における情報セキュリティ確保に係る安全基準等策定指針（第 5 版）」[1]が改定されたことに伴い、「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 4 版」[2]、「航空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 5 版」[3]、「空港分野における情報セキュリティ確保に係る安全ガイドライン第 2 版」[4]が改訂されている。これらの安全ガイドラインでは、情報セキュリティに係るリスクへの必要な備えや有事の際の適切な対処等を実現するために、特に、経営層が積極的に関与し、情報セキュリティに係るリスクへの備えを経営戦略として位置付け、情報セキュリティに係るリスクマネジメントの実施等により、重要インフラ事業者等自らが自己検証を行いつつ、対策を進めていくことが必要としている。

[1] https://www.nisc.go.jp/active/infra/pdf/shishin5.pdf
[2] https://www.mlit.go.jp/common/001283894.pdf
[3] https://www.mlit.go.jp/common/001283895.pdf
[4] https://www.mlit.go.jp/common/001283896.pdf

１．２．研究目的

本研究では、2020 年東京五輪大会に向け、①経営者、管理者などサイバー対策についての認識向上や責任を確立するための手法の検討、②経営層や監査役を対象としたセミナーの実施によるサイバーセキュリティへの意識や理解度の向上、③サイバー攻撃の最前線で業務に従事する現場担当者（システム維持管理者）を主な対象者とした教育による人材育成と情報提供セミナーの実施、④サイバー攻撃対策を主導する CSIRT 要員を対象とした机上演習による人材育成、ならびに過年度の成果を総括したサイバー対策に関する提言のまとめを目的とする。

１．３．これまでの研究成果

運輸総合研究所では、平成 27 年度より交通分野へのサイバー攻撃対策を対象とした調査研究を実施しており、本年度はその最終年度となる。運輸総合研究所における過年度の研究は下記のとおり。

平成 27 年度　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
平成 28 年度　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
平成 29 年度　サイバー攻撃に対する人材育成に関する調査研究
平成 30 年度　サイバー攻撃に対する人材の育成及び経営層の意識向上に関する調査研究

調査研究は、平成 27 年度「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」の実態調査に始まった。研究においては、事業者におけるシステムを対象とした脆弱性検査を実施した。

この調査をもとに、平成 28 年度は、「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（以下、手引書)」として、サイバーセキュリティ対策をとりまとめ、情報セキュリティ対策の手引きを作成した。

平成 29 年度は、この手引書を実践できる人材の育成を目指し、「鉄道／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（以下、人材育成カリキュラム)」を策定した。カリキュラムの作成の前提条件として、求められる人材像と能力の定義を行い、これをもとにカリキュラムを作成した。求められる人材像は、インシデント発生の際にその原因がサイバー攻撃である疑いを考慮して適切に対応でき、サイバー攻撃に対処（原因究明、復旧など）する専門機関と連携してインシデント対応を実行（支援）できる人材とした。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の維持管理を担う担当者とした。

平成 30 年度の研究においては、前年度の研究成果である人材育成カリキュラムをもとに教材を作成して教育を試行した。サイバー攻撃が発生した場合には、サイバー攻撃に関わる事象の検知から対応に至るリードタイムを短くすることが、影響の拡大の阻止、被害軽減、迅速な

復旧等に繋がると考えられることから、人材育成カリキュラムの対象者を鉄道分野及び航空・空港分野の事業部門における「システム維持管理者」とした。合わせて、CSIRT 要員を対象とする机上演習、経営層セミナーを実施した。

１．４．本年度の研究内容

これまでの研究成果を踏まえ、最終年度となる本年度の調査研究では、企業のサイバーセキュリティ対策を実行する上で特に重要となる経営層の役割に焦点を当てたテーマに取り組むとともに、これまで実施してきた育成人材に対して継続した情報提供を行うこととした。本年度の研究内容は以下のとおり。

〇経営層の認識向上

- **経営層がとるべきサイバーセキュリティ対策に関する検討**
  国土交通省の「鉄道／航空／空港分野における情報セキュリティ確保に係る安全ガイドライン（以下、安全ガイドライン)」に則して、特に経営者に求められるサイバーセキュリティ対策について具体的な施策を検討する。
- **経営層、監査役を対象とした啓発セミナーの実施**
  経営者、橋渡し人材層などを対象としたセミナーの実施により、サイバー攻撃の脅威に対する経営層の意識を醸成する。

〇エキスパート人材の育成

- **現場担当者教育の実施**
  昨年度の研究成果である人材育成教材を活用した教育の実施。
- **実践的演習の実施**
  鉄道・航空分野の技術者に向けた実践演習の実施。技術者層（システム維持管理者）を対象とした演習を実施することにより、主要な鉄道・航空事業者のなかにエキスパート人材を育成する。
- **サイバーセキュリティに関する最新情報等に関するセミナー**
  サイバー攻撃の実態と対応に関する情報や国内外のサイバー攻撃に関する最新情報収集に基づき、鉄道・航空事業者への有益な情報提供を図る。

第２章　経営層がとるべきサイバーセキュリティ対策に関する検討

２．１．目的

サイバーセキュリティ対策については、企業の経営層が責任を持って実行する必要がある。サイバーセキュリティ経営ガイドラインの改訂もあり、近年ではサイバーセキュリティに係るリスクへの必要な備えや有事の際の適切な対処等について、経営層が社内で指示すべき施策項目等に関する情報提供が進んできている。これに伴い、情報セキュリティ対策の必要性に関する経営層の理解は高まっているが、現状は十分といえる状況にはないと想定される。さらに、対策項目は一律に全ての企業に適用できるものではないため､理解を深めた経営層においても、サイバーセキュリティ対策についてどのように指示すべきか苦慮しているのが現状と思われる。このため、サイバーセキュリティ対策を実施する上での指示を確たるものとするための施策が必要となってきている。

このような背景の下、本研究では、会社法において役員として定義される取締役と監査役を経営層の主たる対象とし、経営層がとるべきサイバーセキュリティ対策の具体的な施策を検討することを目的とする。経営層がとるべき施策については、経営ガイドラインにおいて原則及び指示の提示はあるものの、原則を踏まえて各会社独自の状況に合わせた指示を出すための施策についての提示例は少ない。そのため、この部分に焦点を当てた施策について具体的に提示することを目的とした。

経営層の役割は、組織規模や置かれている環境に関わらず、リスクを回避して事業を継続するための経営判断を行うことである。辞書によれば、「経営」の意味は以下のとおりとなる。

- 事業目的を達成するために、継続的・計画的に意思決定を行って実行に移し、事業を管理・遂行すること。また、そのための組織体。[5]
- 方針を定め、組織を整えて、目的を達成するよう持続的に事を行うこと。[6]

上記を踏まえ、サイバーセキュリティ対策を推進する上での経営層の役割は、以下のように考えられる。

1. **組織作り**
   サイバーセキュリティ対策を推進するための組織を整えること。
2. **状況把握**
   継続的・計画的に意思決定を行うために社内外の状況を把握すること。
3. **指示**
   サイバーセキュリティ対策を遂行するための指示を出すこと。
4. **確認**

[5] デジタル大辞泉
[6] 三省堂大辞林第三版

サイバーセキュリティ対策を管理するための確認を行うこと。

5. **情報発信**

意思決定を実行に移すために情報発信を行うこと。

今日ではサイバー攻撃が高度化・巧妙化し、サイバーセキュリティリスクが重要な経営課題となっていることから、経営層がサイバーセキュリティリスクを認識し、適切な経営判断を行動に移すための施策についても具体的に示すことを目的とした。

なお、サイバーセキュリティに関する経営者の施策については経営ガイドラインにおいて述べられている。経営ガイドラインで示された施策は、主として経営層が組織内において指示して実現すべき対策を指すが、本研究では、経営層が自ら実行することが望まれる行動指針についても施策に含めた。経営層がとるべきサイバーセキュリティ対策は、組織規模や組織が置かれている環境により千差万別であり、実現すべき対策を一律に定めることが難しい。このため、施策の具体化に際しては、組織規模や組織環境に依存しない記載に努めた。

２．２．施策整理の観点

過年度の研究成果より、経営層がなすべき施策を以下のとおり整理した。

- **経営層の役割と責任**

  経営層がなすべき具体的な施策を検討するためには、その役割と責任を考慮に入れる必要がある。施策整理の観点としては、企業経営に責任を有する取締役と監査役を経営層として主たる対象者としたが、経営層の役割を考慮すると、執行役等の経営層に近い役職層にも対象を広げる必要がある。このため、経営層を支え、経営層の指示を執行する役員や役職者等についても施策整理の観点に加えて検討することとした。

- **橋渡し人材（CISO や CISO を支えるチーム）を有効活用するための経営層の施策**

  経営層が具体的な施策を実行するためには、橋渡し人材（CISO や CISO を支えるチーム）を有効活用することが不可欠である。このため、橋渡し人材をどのように活用すべきかについて施策整理の観点とした。

- **現場（事業部門を含む）それぞれの役割・責任を明確にし、適切な人材配置を実現するための施策**

  サイバーセキュリティリスクが・高度化・巧妙化していることに伴い、事業の広範囲に影響を及ぼすようになってきている。このため、サイバーセキュリティリスクの対象は、従来のシステムリスクに加えて、ビジネスリスクやオペレーショナルリスクに拡大している。このため、サイバーセキュリティリスクへの対応には、情報システム部門、危機管理部門、現場（事業部門）が、それぞれの役割・責任を明確にして連携する必要がある。このため、適切な人材配置を実現することを施策整理の観点とした。

- **有事への備えと平時における対応強化のための経営層の施策**

例えば、機器障害とサイバー攻撃とでシステム不具合の発生時に違いが特定できないことが示すように、サイバーセキュリティリスクは、その他のリスク（大規模災害等）と同列に扱う必要がある。このため、企業活動において実施されている通常のリスク対応にサイバー攻撃による有事への備えと平時における対応強化を位置づけることを施策整理の観点とした。

２．３．進め方

研究フローを以下に示す。

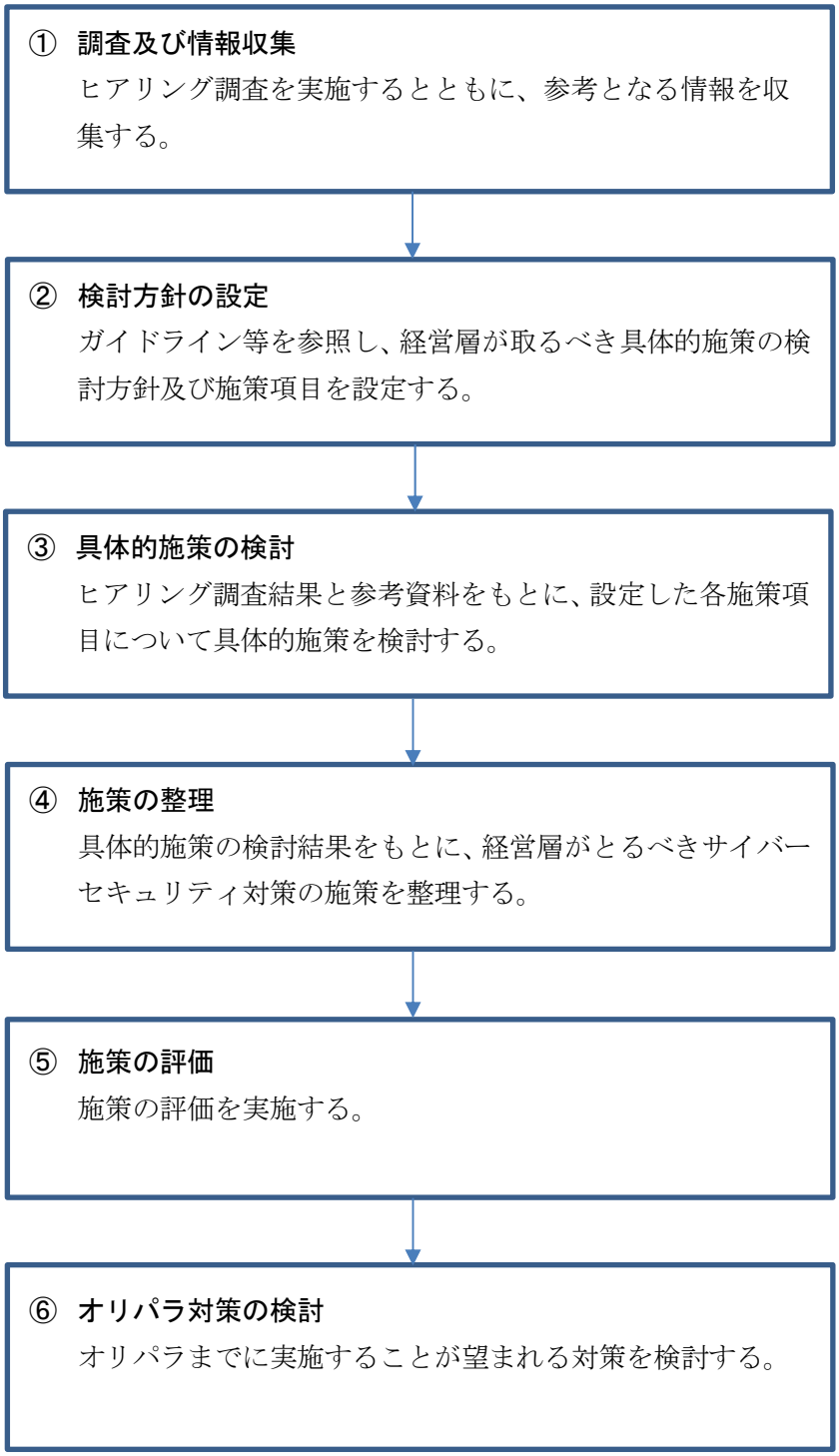


図２－１　研究フロー

２．４．ヒアリング調査及び事例収集

２．４．１．ヒアリング調査

経営層の施策を検討する際にどのような事項がポイントになるのかを確認するために、下記に示す組織を対象としてヒアリング調査を実施した。対象組織は、監査関係３組織とコンサルティング会社１社とした。監査関係は、セキュリティ監査、システム監査、監査役監査に携わる組織を選定した。また、株式会社アイ・アール ジャパンは、経済産業省　産業サイバーセキュリティ研究会 ワーキンググループ２（経営・人材・国際）のオブザーバーであり、経営層を取り巻く環境変化に精通していることから、ヒアリングの対象とした。

（１）特定非営利活動法人　日本セキュリティ監査協会（JASA）[7]

情報セキュリティに関連する法人・組織・個人に対し、情報セキュリティ監査を含む情報セキュリティサービスの普及・啓発、教育、調査研究及び情報提供に関する事業を実施し、同時に情報セキュリティサービス並びに情報セキュリティサービスに携わる専門技術者の質の確保を行うことにより、公正で信頼される情報セキュリティサービスが提供されることをもって、公益の増進に寄与することを目的としている。（定款より）

ヒアリング調査により得られた知見を以下に示す。

- セキュリティ対策を実効性のあるものにするために、経営層の理解は不可欠である。特に、取締役会の構成メンバー間において、サイバーセキュリティ対策の重要性について共通認識を持つことが重要である。この共通認識がない場合には、セキュリティ対策の実効性が損なわれる場合が多い。
- 情報セキュリティ対策とサイバーセキュリティ対策を区別して認識する必要がある。一つの考え方として、情報セキュリティ対策として情報資産のセキュリティを確保する施策を実施し、これを前提として、攻撃者による事業妨害を阻止するための対策としてサイバーセキュリティ対策が位置付けられる。
- 監査、特に内部監査を企業活動維持のツールとして活用すべきである。被監査部門においては、監査対応は厄介であるとの認識があり、監査対応に積極的に関与するといった姿勢が見られない場合が多い。このような現状を打破するためには、経営層の積極的な関与が必要である。

（２）特定非営利活動法人　日本システム監査人協会（SAAJ）[8]

システム監査を社会一般に普及させるとともに、システム監査人の育成、認定、監査技法の維持・向上を図り、よって、健全な情報化社会の発展に寄与することを目的としている。（定款より）公認システム監査人（CSA）は、日本システム監査人協会（SAAJ）による公認システム監査人認定制度に基づくシステム監査人である。

[7] http://www.jasa.jp/
[8] https://www.saaj.or.jp/

ヒアリング調査により得られた知見を以下に示す。

- システム監査は主としてシステムの健全性（正常稼働）を確保することを目的としているが、近年ではサイバーセキュリティ対策がこの目的を達成する上で不可欠となっている。監査人によるサイバーセキュリティ対策の勉強会も活発に実施されている。
- システム監査は会社で定められた文書を確認していく作業であり、文書整備に不備不足がある場合には有効な監査を実施することができない。このため、システムに係る各種文書が整備され、適切に維持管理されていることが必要不可欠である。
- システム監査には、従前より情報セキュリティの観点（システムの正常性の阻害による情報の毀損等）が含まれているが、近年ではサイバーセキュリティの観点（悪意を持つ者による情報の改ざんや搾取等）も含まれるようになりつつある。このため、複雑化するセキュリティ侵害に対応できるシステム監査人の育成が課題となっている。

（３）公益社団法人　日本監査役協会[9]

監査役監査制度（監査委員会監査制度及び監査等委員会監査制度を含む。）の調査、研究、普及・啓発活動等を通じて、監査品質の向上を図り、企業の健全性の確保に努めるとともに、公正かつ自由な経済活動の機会の確保及び促進並びにその活性化による国民生活の安定向上に寄与し、日本経済の健全な発展に貢献することを目的としている。（定款より）

ヒアリング調査により得られた知見を以下に示す。

- 監査役は、取締役とともに、経営層として企業の経営責任を担っている。監査役の主な役割は、自社の経営リスクを確認すること、及び経営リスクへの対応のための手続きが有効に機能していることの確認である。
- サイバーセキュリティに係るリスクが経営リスクとして重要となっている今日では、監査役も役割を遂行するために、サイバーセキュリティに係る知識を修得しておく必要が高まっている。
- 監査役協会では、「監査役監査チェックリスト」の公開等、サイバーリスクの重要性を監査役がチェックできるような施策を実施して、監査役の支援を行っている。

（４）株式会社　アイ・アール ジャパン[10]

株式公開企業の IR・SR（株主関連）活動を支援するコンサルタント会社。株主判明調査、議決権行使促進活動、取締役会評価や役員報酬などのコーポレートガバナンス・コード対応に関するコンサルティング、等を行っている。（同社ホームページより）

ヒアリング調査により得られた知見を以下に示す。

- 企業における ESG 要素への関心は近年高まっているが、G（ガバナンス）要素の一つとしてサイバーセキュリティ対策を位置付けている企業は少数である。

[9] http://www.kansa.or.jp/
[10] https://www.irjapan.net/

- 取締役会におけるサイバーセキュリティリスクの確認は、年に 2 回程度が限界であると思われる。株主総会直前の取締役会において確認を実施することとし、それ以外に 1 回程度確認を実施するといったやり方が現実的である。サイバーセキュリティリスク単体として取締役会で議論されることは稀であると思われるため、重要な事業リスクの一環として議論することになると思われる。
- IR 対応（投資家対応）と SR 対応（株主対応）は分けて考える必要がある。株主は配当性向上に注視しており、安定した企業価値の向上を志向している。一方で、投資家は株価の上昇可能性に注視しており、企業価値向上の将来性を志向している。このため、IR 対応としてのサイバーセキュリティ対策と SR 対応としてのサイバーセキュリティ対策がある。SR 対応の具体例としては、サイバーセキュリティ対策の実施によってグローバルなデータ流通が可能となり、新たな事業領域に参入できる、等が考えられる。

２．４．２．政府施策の動向

サイバーセキュリティ対策に係る経営層の役割について、政府の動向を把握するため各組織の公開情報を調査した。

（１）内閣サイバーセキュリティセンター

サイバーセキュリティ戦略本部が実施する施策について、「サイバーセキュリティ 2019」[11]の記述を以下に示す。政府の方針として、サイバーセキュリティを進めるための戦略マネジメント層の確保・育成を推進することが述べられている。

> 経営層に関しては、意識改革に向け、産業界とも連携した取組を引き続き進める。特に、サイバーセキュリティ対策の観点を含めたグループガバナンスの在り方に関するガイドラインの策定や、サイバーセキュリティ関係法令集に関するハンドブックの取りまとめに向けて、取組を進める。また、デジタルトランスフォーメーション（DX）の進展や、サイバー空間における脅威の高まりといった状況も踏まえ、**DX とサイバーセキュリティを一体的に進める戦略マネジメント層**の確保・育成に向け、2018 年度に作成したモデルカリキュラムも活用した戦略マネジメント層の普及・育成の促進や、独立行政法人情報処理推進機構（IPA）を中心に、「産業サイバーセキュリティセンター」における短期プログラムや「戦略マネジメント系セミナー」、将来、戦略マネジメント層になることも見込まれる中核人材を育成する「中核人材育成プログラム」のカリキュラムのさらなる充実を目指す。

出典：サイバーセキュリティ 2019、サイバーセキュリティ戦略本部、令和元年 5 月 23 日、
https://www.nisc.go.jp/active/kihon/pdf/cs2019.pdf

重要インフラグループは、我が国の国民生活と社会経済活動が大きく依存する重要イン

[11] サイバーセキュリティ 2019、サイバーセキュリティ戦略本部、令和元年 5 月 23 日、
https://www.nisc.go.jp/active/kihon/pdf/cs2019.pdf

フラの情報セキュリティ対策を推進するため、第４次行動計画に基づき施策を進めている[12]。第４次行動計画における重要インフラ防護に関する施策について、以下に示す。ここでは、重要インフラ事業者における経営層の在り方について述べられている。

Ⅱ．本行動計画の要点

本行動計画を推進するに当たっての、①「重要インフラ防護」の目的、②基本的な考え方、③重要インフラ事業者等・政府機関・情報セキュリティ関係機関等の関係主体の在り方、その中でも④重要インフラ事業者等の経営層に期待する在り方を以下に示す。

① 「重要インフラ防護」の目的（省略）

② 基本的な考え方（省略）

③ 関係主体の在り方

- 自らの状況を正しく認識し、活動目標を主体的に策定するとともに、各々必要な取組の中で定 期的に自らの対策・施策の進捗状況を確認する。また、他の関係主体の活動状況の把握に努め、相互に自主的に協力する。
- 重要インフラサービス障害の規模に応じて、情報に基づく対応の５Ｗ１Ｈを理解しており、重要インフラサービス障害の予兆及び発生に対し冷静に対処ができる。多様な関係主体間でのコミュニケーションが充実し、自主的な対応に加え、他の関係主体との連携や統制の取れた対応ができる。

④ 重要インフラ事業者等の経営層の在り方

経営層は、上記の在り方に加え、以下の項目の必要性を認識し、実践すること。

- 情報セキュリティの確保は経営層が果たすべき責任であり、経営者自らがリーダーシップを発揮し、機能保証の観点から情報セキュリティ対策に取り組むこと。
- 自社の取組が社会全体の発展にも寄与することを認識し、サプライチェーン（ビジネスパートナーや子会社、関連会社）を含めた情報セキュリティ対策に取り組むこと。
- 情報セキュリティに関してステークホルダーの信頼・安心感を醸成する観点から、平時における情報セキュリティ対策に対する姿勢やインシデント発生時の対応に関する情報の開示等に取り組むこと。
- 上記の各取組に必要な予算・体制・人材等の経営資源を継続的に確保し、リスクベースの考え方により適切に配分すること。

出典：重要インフラの情報セキュリティ対策に係る第４次行動計画、サイバーセキュリティ戦略本部、平成 30 年 7 月 25 日改訂、https://www.nisc.go.jp/active/infra/pdf/infra_rt4_r1.pdf

重要インフラの情報セキュリティ対策に係る第４次行動計画[13]においては、上記の他に、経営層の関与として以下の記述がある。

[12] https://www.nisc.go.jp/active/infra/outline.html
[13] https://www.nisc.go.jp/active/infra/pdf/infra_rt4_r1.pdf

Ⅰ.4.2.1.（1）重要インフラ事業者等に求められる取組

重要インフラ事業者等にあっては、**経営層が積極的に関与し、情報セキュリティに係るリスクへの備えを経営戦略として位置付け、リスクアセスメントの結果を踏まえたリスク低減等の対応を戦略的に講じる**とともに、サイバー攻撃等に遭遇した場合であっても、重要インフラサービスの安全を確保し、かつ、自ら及びステークホルダーが許容できない停止・品質低下を可能な限り生じさせずに重要インフラサービスの提供を継続できるように、**適切な対処態勢を整備する**ことなどが求められる。また、**経営層は、情報セキュリティ対策に係る内部統制システムを整備した上、こうした機能保証のための取組が適切に講じられていることについて、自らのステークホルダーに対するアカウンタビリティを果たす**ことが重要である。

Ⅲ. 4.2.1.リスクアセスメントの浸透

重要インフラサービスは、社会経済システムにおいて不可欠な役割・機能を担っていることから、安全かつ持続的に提供されている状態が維持されることが必要である。このため、各重要インフラ事業者等が自らの役割・機能を発揮し、その提供する重要インフラサービスの安全を確保し、かつ、自ら及びそのステークホルダーが許容できない停止・品質低下を可能な限り生じさせずに重要インフラサービスの提供を継続させるということを目的としたリスクアセスメントを行い、その実施結果を踏まえた**経営層による総合的な判断に基づくリスク対応を進めていく**ことにより、その目的達成を目指していくという「機能保証」の考え方が重要となる。

Ⅲ. 4.2.3.対処態勢整備の推進

機能保証のためには、重要インフラサービス障害により影響を受けた重要インフラサービスについて、 安全を確保するとともに、許容可能な時間内に許容可能な水準まで復旧させることが求められることから、 重要インフラ事業者等にあっては、重要インフラサービス障害が発生した際に備えた対処態勢を整備することが必要である。

このことから、重要インフラ事業者等における対処態勢の整備を推進する。また、オリパラ大会も見据え、その関係主体における対処態勢の整備についても推進する。具体的には、次の施策を講じる。

① 重要インフラ事業者等における機能保証の考え方を踏まえた事業継続計画及びコンティンジェンシープランの整備並びに当該計画を実行するための組織体制の構築を推進する。この際、事業継続計画及びコンティンジェンシープランが想定どおりに実行できないことがリスクとなり得ることから、これらの実行性を確保し、また検証するための教育、演習等の取組を講じることも重要である。このため、こうした取組についても併せて推進する。

② オリパラ大会も見据え、各関係主体におけるインシデント情報の共有等を担う中核的な組織体制（オリンピック・パラリンピックＣＳＩＲＴ（仮））を構築する。また、当該組織体制の整備において政府及び関連主体の役割を整理するなどの取組で得られた知見をレガシーとして上記①の施策に活用する。

なお、本行動計画において、**「コンティンジェンシープラン」とは、重要インフラ事業者等が重要インフラサービス障害の発生又はそのおそれがあることを認識した後に経営層や職員等が行うべき初動対応（緊急時対応）に関する方針、手順、態勢等をあらかじめ実行面から具体的に定めたものをいい、これに基づいて適切な対応を行うことにより重要インフラサービス障害による影響を最小限に抑えることを目的**とする。初動対応（緊急時対応）には、重要インフラの性質やリスクアセスメントの結果に応じて、安全を確保するために重要インフラサービスの提供を停止するなどの対応についても含まれる。また、「事業継続計画」とは、機能保証の観点から、重要インフラ事業者等が重要インフラサービス障害により影響を受けた重要インフラサービスを許容可能な時間内に許容可能な水準まで復旧させることを目的して、その復旧に向けた目標水準、優先順位その他の方針、手順、態勢等をあらかじめ定めたものをいう。

Ⅲ. 4.2.4.リスクコミュニケーション及び協議の推進

リスクコミュニケーション及び協議とは、「リスクの運用管理について、情報の提供、共有又は取得、及びステークホルダーとの対話を行うために、組織が継続的に及び繰り返し行うプロセス。」と定義されている。このプロセスは、機能保証の観点からは、サービス維持の水準等として表現される重要インフラサービスに係る組織の目的設定並びにその目的に対するリスク及びその運用管理に関する組織の意思決定を行う上で必要である。また、到来しつつある連接融合情報社会においては、重要インフラ事業者等がステークホルダーとの間においてリスクに関する役割や責任の分担等に係る合意形成を行い、重要インフラサービスの提供に関して期待される責任を果たす上でも重要となる。

このことから、重要インフラ事業者等における内部ステークホルダー間の情報や意見の交換及び関係主体間による分野横断的な情報や意見の交換の充実に資することを目的に、重要インフラ防護に関連する者によるリスクコミュニケーション及び協議を推進する。具体的には、次の施策を講じる。

① 経営層、情報セキュリティ部門、情報システムや制御システムを所管する部門、ユーザ部門その他内部ステークホルダー相互間のリスクコミュニケーション及び協議を推進する。

② セプターカウンシル及び分野横断的演習を利用し、各関係主体と協力しつつ、情報や意見の交換の充実を推進する。また、これにより、新たなリスク源・リスクに関する調査・分析に必要となる情報の収集を図る。

Ⅲ. 5.5.経営層への働きかけ

「サイバーセキュリティ経営ガイドライン」や「企業経営のためのサイバーセキュリティの考え方」等に見られるように、情報セキュリティ対策が経営課題として重要な位置付けを持っていることが強調されるようになってきている。こうした中、重要インフラ事業者等の経営層については、その在り方として、以下の項目の必要性を認識し、実践することが期待される。

① 情報セキュリティの確保は経営層が果たすべき責任であり、経営者自らがリーダー

シップを発揮し、機能保証の観点から情報セキュリティ対策に取り組むこと。

② 自社の取組が社会全体の発展にも寄与することを認識し、サプライチェーン（ビジネスパートナーや子会社、関連会社）を含めた情報セキュリティ対策に取り組むこと。

③ 情報セキュリティに関してステークホルダーの信頼・安心感を醸成する観点から、平時における情報セキュリティ対策に対する姿勢やインシデント発生時の対応に関する情報の開示等に取り組むこと。

④ 上記の各取組に必要な予算・体制・人材等の経営資源を継続的に確保し、リスクベースの考え方により適切に配分すること。なお、重要インフラにおいては、システムの規模が大きく、かつ、そのライフサイクルが長期に及ぶ傾向があることも考慮し、経営層が率先して中長期的な視点で経営資源の確保・配分を計画的に行うことが重要である。

以上を踏まえ、内閣官房及び重要インフラ所管省庁は、重要インフラ事業者等の経営層に対して情報セキュリティに関する意識を高めるように働きかけを行うとともに、そのような働きかけを通して知見を得て、重要インフラ防護施策を実態に即した実効的なものとする。

Ⅲ．5.6.人材育成等の推進

各関係主体において、「サイバーセキュリティ人材育成総合強化方針」（平成 28 年３月サイバーセキュリティ戦略本部決定）に基づく取組を推進する。また、「サイバーセキュリティ人材育成プログラム」（平成 29 年４月サイバーセキュリティ戦略本部決定）に基づく具体的な取組を推進する。具体的には、人材育成に関する次の施策を講じる。

① 重要インフラ事業者等において、経営層の意識を高め、理解を促進する。その上で、**自組織の経営方針に基づく情報セキュリティ対策を提示**するとともに、**組織内の情報セキュリティに関係する部署間の総合調整や実務者層を指揮することができる橋渡し人材の育成**を進める。

② ＩＴの管理部門に限らず、ＯＴの管理部門や法務部門等の間接部門においても情報セキュリティ対策が要求されるようになっている昨今の状況を踏まえ、**様々な役割や能力を持つ人材が組織横断的に連携し、情報セキュリティ対策に当たることを可能とする体制の構築**を推進する。

③ 産学官が互いに連携し、必要なセキュリティ人材像の定義、情報セキュリティに係る訓練・演習、資格取得等の具体的な人材育成策を推進する。

出典：重要インフラの情報セキュリティ対策に係る第４次行動計画、サイバーセキュリティ戦略本部、平成 30 年 7 月 25 日改訂、https://www.nisc.go.jp/active/infra/pdf/infra_rt4_r1.pdf

サイバーセキュリティ戦略本部令（平成 26 年政令第 400 号）第２条の規定に基づき、我が国全体の重要インフラ防護に資するサイバーセキュリティに係る事項について、調査検討を行うため、重要インフラ専門調査会が設置されている。この重要インフラ専門調査会の検討を経てサイバーセキュリティ戦略本部で決定された「重要インフラ分野における情

報セキュリティ確保に係る安全基準等策定指針（第５版）」における、経営層に求められる行動に関する記載を下記に示す。

【情報セキュリティ対策のＰＤＣＡサイクルに取り組む際の重要事項】
経営層に求められる行動

「情報セキュリティリスク」は「機能保証の考え方」を踏まえた**事業運営を不確かにする影響力があることを認識**し、その対処の在り方を判断するために必要な**情報セキュリティリスクアセスメントの実施を指示**すること。また、情報セキュリティ対策のＰＤＣＡサイクル推進に当たり、**必要な資源（予算・体制・人材等）の継続的な確保及び適切な配分に努める**こと。さらに、**情報セキュリティリスクへの対応結果が事業に与えた効果と影響を定期的に検証**し、情報セキュリティリスク対応戦略の見直しの必要性等について意思決定を行うこと。

これらの取組に際して、「企業経営のためのサイバーセキュリティの考え方」、「サイバーセキュリティ経営ガイドライン」等を参照すること。

出典：重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第５版）、サイバーセキュリティ戦略本部、令和元年５月 23 日改定、https://www.nisc.go.jp/active/infra/pdf/shishin5rev.pdf

（２）国土交通省

鉄道分野及び航空分野においては、サイバーセキュリティ戦略本部において「重要インフラ分野における情報セキュリティ確保に係る安全基準等策定指針（第５版）」に改定されたことに伴い、「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４版」、「航空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５版」、「空港分野における情報セキュリティ確保に係る安全ガイドライン第２版」が改訂されている。

「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４版」、「航空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５版」、「空港分野における情報セキュリティ確保に係る安全ガイドライン第２版」（以下、これらを総称して「安全ガイドライン」という）に記載のある経営層に求められる行動を下記に示す。

なお、下記に示した記載については、３分野の安全ガイドラインで違いは無かった。

1.1.6 責任者・組織等の役割

各重要インフラ事業者等内における責任者・組織等の役割を以下のとおり定義する。なお、該当する責任者・組織等そのものが存在しない場合、同様の役割を担っている役割・組織等に読み替えること。

(1) 経営層

経営層は、重要インフラ事業者等の社会的責任として、情報セキュリティを確保するよう情報セキュリティ対策に取り組むこと。また、自らがリーダーシップを発揮し、機能保証の考え方を踏まえて対応すること。

3.1.2.2 情報セキュリティ方針の策定・見直し

【主旨・目的】

重要インフラ防護のためには、情報セキュリティ対策における根本的な考え方(以下、情報セキュリティ方針)を示す必要がある。

【対策項目】

最高情報セキュリティ責任者は、重要インフラ防護の目的、目指す方向、情報セキュリティ対策にて守るべき対象等を明らかにし、情報セキュリティへの取組姿勢を情報セキュリティ方針として規定すること。また、情報セキュリティ方針の策定・見直しに係る主管組織、目的、権限、構成員、見直し要件等についても規定すること。

経営層は、情報セキュリティの確保のため、情報セキュリティ対策に取り組むことを情報セキュリティ方針等に含め、組織の内外に対して宣言する。

情報セキュリティ方針が妥当かつ有効であることを定期的な間隔で確認するとともに、自組織を取り巻く状況に大きな変化が発生した場合にも確認する。

3.2.1.2 情報セキュリティ対策の運用状況把握

【対策の指針】

経営層は、情報セキュリティ対策の運用状況について、把握する。

【主旨・目的】

情報セキュリティ対策は、事業継続を念頭に置いた全社的なリスクマネジメントの一部であることを踏まえ、リスクマネジメントと情報セキュリティ対策が整合する取組となるように留意する。これらが整合するよう情報セキュリティ対策を経営層が担う全社的なリスクマネジメントの一部と位置付けるとともに、担当者のみならず経営層も関与した全社的な体制の下で情報セキュリティ対策に取り組む必要がある。

【対策項目】

情報セキュリティ責任者は、情報セキュリティ対策の運用状況や対応状況を定期的に経営層に報告すること。

経営層は、定期的にPDCAサイクルの取組状況を確認し、関係主体等の対話の機会等を通じて改善を行う。また、情報セキュリティリスクへの対応結果が事業に与えた効果と影響を検証すること。

経営層は、情報セキュリティに対する取組みが、適切及び有効であることを確実にするために、システム監査その他のリソースを活用して、レビューを実施する。レビュー結果は文書化するとともに改善や見直しを指示すること。

3.2.3.1 重要インフラサービス障害に対する防護・回復

【対策の指針】

策定したIT-BCP等又はBCP等を発動し、規定に沿った業務継続を進めるとともに、早期復旧に向けた対応を行う。その際、原因究明等に必要なログ等の電子的記録を収集・分析し、重要インフラサービス障害をもたらした原因への適切な対処を可能とする。

（中略）

(2)対外的な情報発信及び情報共有

【主旨・目的】

緊急事態発生後は、事業者活動が関係者から見えなくなる、何をしているのか全然わからないといった、いわゆるブラックアウトを防ぐための対策を講ずる必要がある。

【対策項目】

最高情報セキュリティ責任者は、緊急事態発生後に、取引先、顧客、取扱者、株主、地域住民、政府・自治体などと情報を共有するために、3.1.4.1(3)(b)で定める必要な対策を講ずること。

経営層は、情報セキュリティに関してステークホルダーの信頼・安心感を醸成する観点から、平時における情報セキュリティ対策に対する姿勢やインシデント発生時の対応に関する情報の開示等に取り組むこと。

3.3.1.1 内部監査や外部監査を通じた課題抽出

（中略）

(2) 情報セキュリティ対策の監査

【主旨・目的】

情報セキュリティの確保のためには､本ガイドラインに準拠して対策が適切に策定され、かつ運用されることによりその実効性を確保することが重要であって、その準拠性、実効性及び対策の妥当性の有無が確認されなければならない。そのためには、取扱者による自己点検だけでなく、独立性を有する者による情報セキュリティ監査を実施することが必要である。

【対策項目】

（中略）

経営層は、監査の結果等から、目標未達や進捗遅延、セキュリティ管理策の要改善点等が確認された場合は、改善指示を行い、今後に向けた再発防止策を立案する。これらを繰り返し実施し、情報セキュリティ対策の取組の効果を高める。

出典：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4版、国土交通省、平成31年3月29日改訂

航空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5版、国土交通省、平成31年3月29日改訂

空港分野における情報セキュリティ確保に係る安全ガイドライン第2版、国土交通省、平成31年3月29日制定

http://www.mlit.go.jp/sogoseisaku/jouhouka/sosei_jouhouka9999.html

これらの安全ガイドラインでは、情報セキュリティに係るリスクへの必要な備えや有事の際の適切な対処等を実現するために、特に、経営層が積極的に関与し、情報セキュリティに係るリスクへの備えを経営戦略として位置付け、情報セキュリティに係るリスクマネジメントの実施等により、重要インフラ事業者等自らが自己検証を行いつつ、対策を進めていくことが必要としている。安全ガイドラインに記載された、経営層に求められる対策項目は、以下のとおり。

１）情報セキュリティ方針の策定・見直し

経営層は、情報セキュリティの確保のため、情報セキュリティ対策に取り組むことを情報セキュリティ方針等に含め、組織の内外に対して宣言する。情報セキュリティ方針が妥当かつ有効であることを定期的な間隔で確認するとともに、自組織を取り巻く状況に大きな変化が発生した場合にも確認する。

２）情報セキュリティ対策の運用状況把握

経営層は、定期的にPDCAサイクルの取組状況を確認し、関係主体等の対話の機会等を通じて改善を行う。また、情報セキュリティリスクへの対応結果が事業に与えた効果と影響を検証すること。経営層は、情報セキュリティに対する取組みが、適切及び有効であることを確実にするために、システム監査その他のリソースを活用して、レビューを実施する。レビュー結果は文書化するとともに改善や見直しを指示すること。

３）重要インフラサービス障害に対する防護・回復

経営層は、情報セキュリティに関してステークホルダーの信頼・安心感を醸成する観点から、平時における情報セキュリティ対策に対する姿勢やインシデント発生時の対応に関する情報の開示等に取り組むこと。

４）内部監査や外部監査を通じた課題抽出

経営層は、監査の結果等から、目標未達や進捗遅延、セキュリティ管理策の要改善点等が確認された場合は、改善指示を行い、今後に向けた再発防止策を立案する。これらを繰り返し実施し、情報セキュリティ対策の取組の効果を高める。

サイバーセキュリティに関する記述は見られないが、「運輸事業者における安全管理の進め方に関するガイドライン」[14]を作成し、事業者における安全管理体制の構築・改善に係る取組のねらいとその進め方の参考例を示している。サイバー攻撃がテロに利用され得る現状を鑑みると、サイバーセキュリティ対策についても、本ガイドラインに則した対策が必要と考えられる。

（３）経済産業省

サイバーセキュリティに関する課題が多岐に及ぶ中、経済産業省では、産業界が直面するサイバーセキュリティの課題を洗い出し、関連政策を推進していくため、経営者、学識者等から構成される「産業サイバーセキュリティ研究会」[15]を設置し、研究を行なっている。また、研究会で示された政府として取り組むべき政策の方向性を踏まえ、研究会の下にワーキンググループを設置し、関係省庁と連携して政策の具体化を進めている。また、サイバーセキュリティを直接扱うものではないが、「CGS研究会（コーポレート・ガバナンス・システム研究会)」において、企業統治の在り方を検討している。

[14] https://www.mlit.go.jp/common/001217521.pdf
[15] https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/index.html

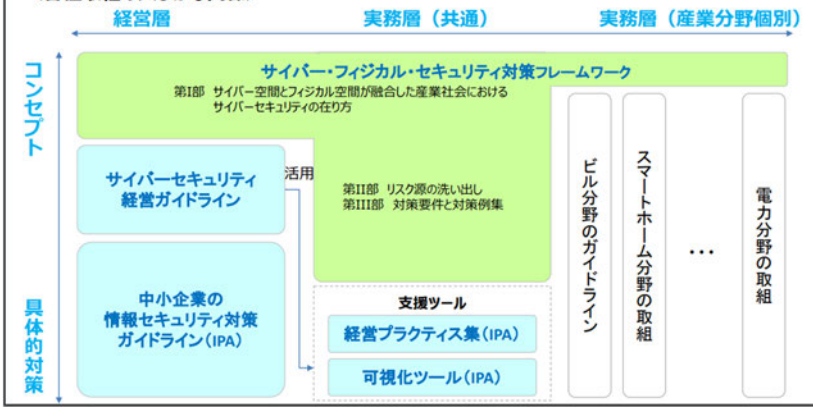
1）産業サイバーセキュリティ研究会

ワーキンググループ２（経営・人材・国際）においては、産業サイバーセキュリティ研究会で整理した政策の方向性の４．基盤の整備のうち、①経営者の意識喚起、②多様なサイバーセキュリティ人材の育成、③サイバーセキュリティ分野の「国際協力基盤の整備」に関する施策を検討している。第４回資料からの抜粋を以下に示す。

サイバー・フィジカル・セキュリティ対策フレームワークを軸とした各種取組

●「サイバー・フィジカル・セキュリティ対策フレームワーク」では、Society5.0における産業社会でのセキュリティ対策の全体枠組みを提示。
●全体の枠組みに沿って、対象者や具体的な対策を整理し、『サイバーセキュリティ経営ガイドライン』や産業分野別のガイドラインなどの実践的なガイドラインを整備。

<各種取組の大まかな関係>



2

サイバーセキュリティ経営における全体像

第二回WGの再掲

● 経営層向け、現場向け、中小企業向けの３つの視点で、サイバーセキュリティ経営を促進するための施策を検討。

経営層向け

サイバーセキュリティ経営ガイドラインを軸として経営者の意識向上を図るとともに、将来的にセキュリティの高い企業が投資家の評価を受けられる枠組みの構築を支援する。

現場向け

サイバーセキュリティ経営ガイドラインの実践規範となるプラクティスや、対策状況の可視化ツールの提供により対策の実行を支援する。

中小企業向け

サイバー保険との連動も検討しつつ、中小企業におけるセキュリティに関するトラブルの相談対応を支援する。

4

段階的なサイバーセキュリティ経営の実現

第二回WGの再掲

● 以下の3Stepにより、サイバーセキュリティ経営の定着を目指す。

1st Step

サイバーセキュリティ経営の明確化

- サイバーセキュリティ経営ガイドラインの普及・定着

2nd Step

サイバーセキュリティ経営の実践

- CGS(コーポレート・ガバナンス・システム)ガイドラインにサイバーセキュリティを反映
- IRの観点から、サイバーリスクを経営リスクとして認識・自己確認することの重要性を啓発
- 取締役会実効性評価の項目にサイバーリスクを位置づけ
- 投資家に対してもサイバーセキュリティの重要性を啓発

3rd Step

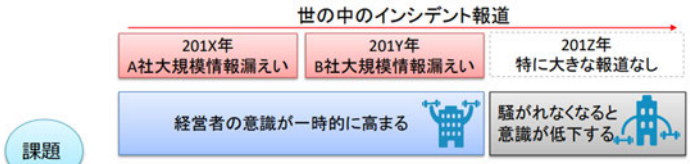
セキュリティの高い企業であることの可視化

- セキュリティの高い企業であることを投資家が評価できるようにするための、サイバーセキュリティ経営に関する情報の開示の在り方の検討

6

サイバーセキュリティ経営ガイドラインの見直しに向けて ～サイバー・フィジカル・セキュリティ対策フレームワークのコンセプトの反映等

● 産業社会全体におけるリスクを捉えたサイバー・フィジカル・セキュリティ対策フレームワークのコンセプトも踏まえ、経営層のサイバーセキュリティに対する意識の定着を図るために、サイバーセキュリティ経営ガイドラインの改訂を含めた検討を開始する。



課題

インシデントに係る報道により、経営層の意識は高まるものの、一時的なものとなる場合がある

対応

◆ フレームワークの考え方をベースとし、サイバーセキュリティ対策が事業継続や新たな価値創出のために不可欠な「投資」と捉える意識改革が必要。
◆ 経営ガイドラインにおいて、事業の中での必要性を強くメッセージ出しすることで、一時的な危機意識でなく、恒久的な必要性について認識の促進を目指す

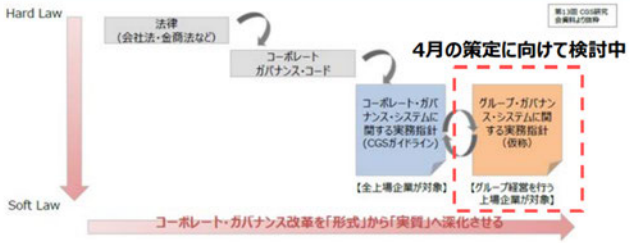
<サイバーセキュリティ経営ガイドラインの改訂に向けた検討項目>
・サイバー・フィジカルセキュリティ対策フレームワークをベースとした再整理
・可視化ツールの作成にあわせて、付録A（サイバーセキュリティ経営チェックシート）の項目を見直し
・経営者へのメッセージの出し方を見直し（リスクベースの議論だと恒久的な意識が根付かないため）

7

グループ・ガバナンスシステムに関する実務指針へサイバーセキュリティを位置づけ① ～コーポレートガバナンスコードと実務指針の関係

●平成29年12月から、CGS研究会（コーポレート・ガバナンス・システム研究会第2期）において、企業グループ全体の価値向上を図る観点からグループガバナンスの在り方を検討。

●特に、グループ経営を行う上場企業を主たる対象とし、グループ全体の価値向上を図る観点からグループガバナンスの在り方を示す「グループ・ガバナンスシステムに関する実務指針（仮称）」を、平成31年6月を目処に策定予定。



CGS研究会（第2期） <平成29年12月に第一回を開催し、平成31年3月までに15回開催>

直近のスケジュール： 第14回（2/12）ガイドライン骨子
第15回（3/15）ガイドラインとりまとめ素案
第16回（4/18）ガイドラインとりまとめ（予定）

8

グループ・ガバナンスシステムに関する実務指針へサイバーセキュリティを位置づけ② ～サイバーセキュリティ経営を内部統制システムとして明記

● 「グループ・ガバナンス・システムに関する実務指針（仮称）」において、**グループ内部統制システムの一つとして、サイバーセキュリティ対策の在り方を位置づけ。**

● 親会社の**取締役会レベルで、子会社も含めたグループ全体、更には関連するサプライチェーンも考慮に入れてセキュリティ対策を行うことを検討すべき**ことを明記。

「グループ・ガバナンス・システムに関する実務指針（仮称）」の目次案

1．はじめに
2．グループ設計の在り方
3．事業ポートフォリオマネジメントの在り方
4．グループ内部統制システムの在り方
　4．1　内部統制システムの意義
　4．2　内部統制システムに関する現状と課題
　4．3　内部統制システムに関する取締役会の役割
　4．4　内部統制システムに関する監査役等の役割等
　4．5　実効的な内部統制システムの構築・運営の在り方
　4．6　監査役等や第2線・第3線における人材育成の在り方
　4．7　ITを活用した内部監査の効率化と精度向上
　4．8　サイバーセキュリティ対策の在り方
　4．9　有事対応の在り方
5．子会社経営陣の指名・報酬の在り方
6．上場子会社の在り方
7．おわりに

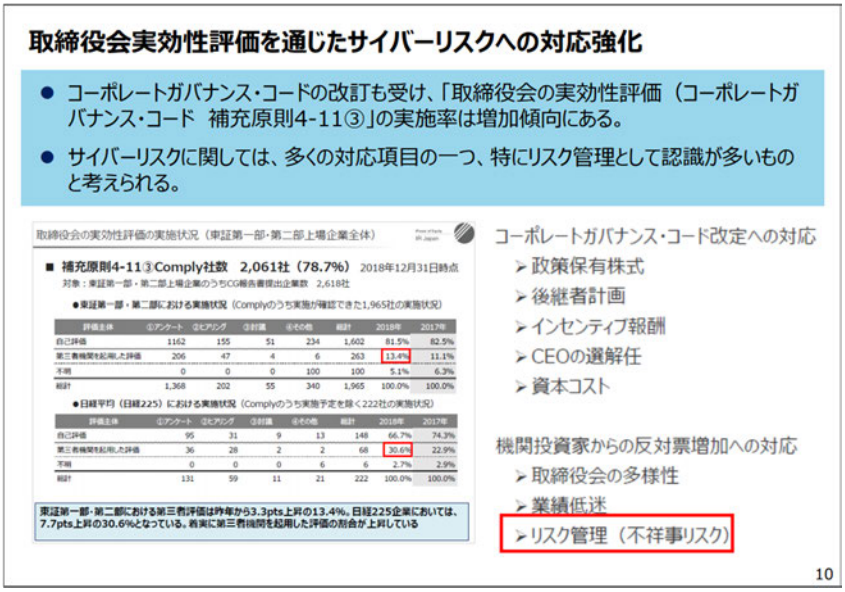
サイバーセキュリティ対策の在り方（案）

- サイバーセキュリティ対策については、内部統制システム上の重要なリスク項目として認識し、サイバー攻撃を受けた場合のダメージの甚大さに鑑み、**親会社の取締役会レベルで、子会社も含めたグループ全体、更には関連するサプライチェーンも考慮に入れてセキュリティ対策を行うことを検討すべきである。**

実務指針の案より抜粋

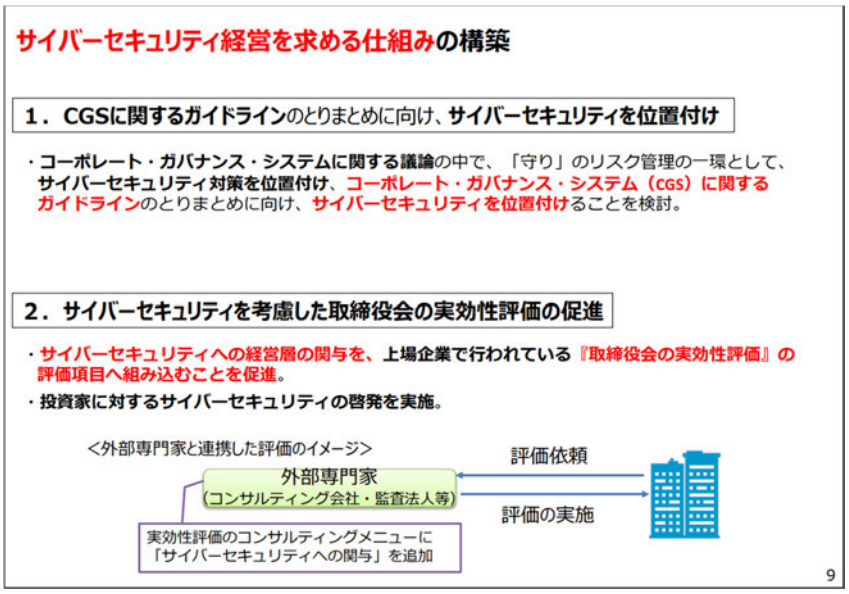
- サイバーセキュリティ経営ガイドラインの概要として以下を記載
  - ✓ グループ会社等における対策も、基本的には親会社も責任が問われる。
  - ✓ サイバーセキュリティ経営ガイドラインに従った対応を行うことが重要。
  - ✓ グループ会社等に対策の実施を指示するとともに、着実に対策が実施されていることの確認が重要。
  - ✓ グループ会社等に中小企業がいる場合は、SECURITY ACTIONの宣言の有無を確認することも有効。
  - ✓ 投資家等からの信頼性を高めるために、情報開示を行うことも考えられる。

9



出典：第４回 産業サイバーセキュリティ研究会 ワーキンググループ２（経営・人材・国際）、資料３ 事務局説明資料、経済産業省商務情報政策局サイバーセキュリティ課、2019 年 3 月 29 日、https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_keiei/pdf/004_03_00.pdf

産業サイバーセキュリティの加速化指針[16]では、産業サイバーセキュリティ強化へ向けたアクションプランの主な進捗を参考として提示している。



出典：第２回 産業サイバーセキュリティ研究会 ワーキンググループ２（経営・人材・国際）、資料３ 事務局説明資料、経済産業省商務情報政策局サイバーセキュリティ課、2018 年 5 月 22 日、https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/pdf/002_03_00.pdf

[16] https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/pdf/002_03_00.pdf

２）CGS 研究会

CGS 研究会（第２期）では、2017 年 12 月に第 1 回を開催し、2019 年 4 月までに 16 回開催。2019 年 6 月に「グループ・ガバナンス・システムに関する実務指針（グループガイドライン)」[17]を公開し、この中で「サイバーセキュリティ対策の在り方」として、グループ全体やサプライチェーンも考慮に入れた対策の在り方の検討を経営層に求めている。

（４）総務省

総務省では、2017 年 12 月より、総務省サイバーセキュリティ統括官の私的懇談会である「サイバーセキュリティタスクフォース（座長：東京電機大学安田浩学長)」の下で「情報開示分科会（主査：弁護士法人英知法律事務所 岡村久道弁護士)」を開催し、民間企業におけるサイバーセキュリティ対策の情報開示を促進するため、議論を進めてきた。この分科会において、企業が自らのサイバーセキュリティ対策の情報開示の在り方を検討する上で参考となる手引きとして「サイバーセキュリティ対策情報開示の手引き」[18]をとりまとめている。

また、「民間企業におけるセキュリティ対策に関する情報開示の現状について」[19]において、情報開示の現状について報告している。

（５）その他

重要インフラ 14 分野において、今後サイバーセキュリティ対策の義務付けが強化されることが想定される。自民党サイバーセキュリティ対策本部より政府への提言書において、サイバーセキュリティ庁の新設が提言されたが、この提言書において、現行法でサイバーセキュリティ対策が義務付けられている電気事業とガス事業に加えて情報通信や金融などの分野でも対策を取ることや、重大事案が発生した際に遅滞なく政府に報告することが求められている。サイバーセキュリティ庁は、中央省庁のサイバー対策を担う内閣官房の「内閣サイバーセキュリティセンター（NISC)」の機能を拡充するものとして提言書で位置付けられている。[20][21]

[17] https://www.meti.go.jp/policy/economy/keiei_innovation/keizaihousei/pdf/ggs/190628ggsguideline.pdf
[18] http://www.soumu.go.jp/main_content/000630516.pdf
[19] http://www.soumu.go.jp/main_content/000528734.pdf
[20] https://www.jiji.com/jc/article?k=2019051401171&g=pol
[21] https://www.sankei.com/economy/news/190920/ecn1909200031-n1.html

２．４．３．企業を取り巻く市場動向

サイバーセキュリティ対策に係る経営層の施策について検討するため、企業を取り巻く市場動向について参考になると思われる公開情報を調査した。

（１）改訂コーポレートガバナンス・コードと経営課題への対応の現状

コーポレートガバナンス・コードが 2018 年 6 月に改訂されたことに伴い、KPMG は、レポートにおいて、コーポレートガバナンス・コード改訂で経営に求められる進化の方向性と、日本企業が直面している様々な課題への対応との関連性について解説している。今回のコーポレートガバナンス・コード改訂が求める方向性は、「株主・投資家との間での課題の共有」と「よりアカウンタビリティある経営の追究」であり、改訂により求められる事項のうち、取締役会及び経営陣幹部の役割に大きく影響を与える項目として、取締役会の機能発揮と多様性の確保、ESG 情報の開示を行うことが挙げられるとしている。

「改訂コーポレートガバナンス・コードと経営課題への対応、2018 年 9 月、KPMG」[22]に以下の記載がある。

> **Ⅱ．３．（2）サイバーセキュリティへの対応**
>
> 企業のデジタル技術活用が進展するのに従い、サイバー攻撃にさらされるリスクも増大しています。またクラウド化の進展により「ITのサービス化」が進み、サイバー攻撃の戦線は拡大するとともにビジネスの最前線がセキュリティの最前線となってきています。防御のための投資意思決定を含め、取締役会及び経営陣幹部のリーダーシップが問われるテーマとなっています。
>
> **1. 取締役会の機能発揮・多様性確保との関係**
>
> 経済産業省が公表している「産業サイバーセキュリティ強化へ向けたアクションプラン」には、4つの柱となる政策パッケージが記載されていますが、その1つに「サイバーセキュリティ経営強化パッケージ」があります。そこでは、サイバーセキュリティ経営を求める仕組みの構築として、サイバーセキュリティを考慮した取締役会の実効性評価の促進といった施策が盛り込まれています。企業の重要リスクであるサイバーセキュリティへの対応について、取締役会にて実効性ある議論が行われているか、取締役会の実効性評価の中で検証することも考えられます。
>
> **2. ESG情報開示との関係**
>
> 企業の管理する施設等へのサイバーテロが発生した場合、社会的に大きな影響が発生する可能性があります。改訂コードでは、いわゆるESG要素に関する情報を含む非財務情報の積極的な開示が求められていますので、前述の「サイバーセキュリティ経営強化パッケージ」に対応した取組みを推進し、その状況を開示することなどが考えられます。
>
> ※ ESG：環境（Environment）、社会（Social）、ガバナンス（Governance）の頭文字を取ったもの。投資の意思決定において、従来型の財務情報だけを重視するだけ

[22] https://home.kpmg/jp/ja/home/insights/2018/09/corporate-governance-20180914.html

でなく、ESGも考慮に入れる手法は「ESG投資」と呼ばれている。

（２）グループ・ガバナンス・システムに関する実務指針（案）[23]

グループ・ガバナンス・システムに関する実務指針（案）は、主として単体としての企業経営を念頭に作成されたコーポレートガバナンス・コードの趣旨を敷衍し、子会社を保有してグループ経営を行う企業においてグループ全体の企業価値向上を図るガバナンスの在り方をコードと整合性を保ちつつ示すことで、コーポレートガバナンス・コードを補完するものである。

本ガイドラインは、一般的なベストプラクティスを示すものであり、各企業の個別の状況に応じた多様なガバナンスの在り方を想定しており、これに沿った対応を行わなかったことが取締役等の善管注意義務違反を構成するものではないが、反対に、本ガイドラインに沿った対応を行った場合には、他に特段の事情がない限り、通常は善管注意義務を十分に果たしていると評価されるであろうと考えられる。

内部統制システムの在り方においてサイバーセキュリティ対策の在り方について言及している。

（３）コーポレートガバナンス・コード

2013 年に日本政府が閣議決定した「日本再興戦略(Japan is Back)」及び 2014 年の改定版で、成長戦略として掲げた３つのアクションプランの１つ「日本産業再興プラン」の具体的施策である「コーポレートガバナンス（企業統治)」の強化を官民挙げて実行する上での規範。「コード」は規則を意味するが、細則の規定集ではなく原則を示したものである。2015 年 6 月から適用されている。

本コードは大きく５つの基本原則で構成され、(1)株主の権利・平等性の確保、(2)株主以外のステークホルダーとの適切な協働、(3)適切な情報開示と透明性の確保、(4)取締役会等の責務、(5)株主の対話、に関する指針が示されている。

「日本版スチュワードシップ・コード」が機関投資家や投資信託の運用会社、年金基金などの責任原則であるのに対し、本コードは上場企業に適用される。両コードともに法的拘束力は無いが、「コンプライ・オア・エクスプレイン(Comply or Explain)」の精神の下、原則を実施するか、さもなければ実施しない理由を説明するか求めている。

本コードの策定を受け、東京証券取引所は上場制度を一部見直し、同様に 2015 年 6 月から制度改正が適用となっている[24]。従来からあるコーポレートガバナンス報告書に本コードの実施に関する情報開示を義務付け、実施しない場合はその理由の明記が必要である。政策保有株（持ち合い株）に関する方針や取締役会に関する開示などが中心であり、会社の持続的成長・中長期的企業価値向上に寄与する独立社外取締役を 2 名以上選任することも新たな上場制度に盛り込まれた。

[23] https://www.meti.go.jp/shingikai/economy/cgs_kenkyukai/pdf/2_016_04_00.pdf
[24] コーポレートガバナンス・コード、株式会社東京証券取引所、2018 年 6 月 1 日、
https://www.jpx.co.jp/equities/listing/cg/tvdivq0000008jdy-att/nlsgeu000000xdn5.pdf

【原則4－3. 取締役会の役割・責務(3)】
取締役会は、独立した客観的な立場から、経営陣・取締役に対する実効性の高い監督を行うことを主要な役割・責務の一つと捉え、適切に会社の業績等の評価を行い、その評価を経営陣幹部の人事に適切に反映すべきである。
また、取締役会は、適時かつ正確な情報開示が行われるよう監督を行うとともに、内部統制やリスク管理体制を適切に整備すべきである。
更に、取締役会は、経営陣・支配株主等の関連当事者と会社との間に生じ得る利益相反を適切に管理すべきである。

出典：コーポレートガバナンス・コード、株式会社東京証券取引所、2018 年 6 月 1 日、
https://www.jpx.co.jp/equities/listing/cg/tvdivq0000008jdy-att/nlsgeu000000xdn5.pdf

（4）サイバーセキュリティ経営ガイドライン Ver2.0 実践のための経営プラクティス集[25]

2019 年 3 月、「サイバーセキュリティ経営ガイドライン Ver2.0 実践のための経営プラクティス集」を公開した。経営ガイドラインの重要 10 項目の実践事例に加え、セキュリティ担当者の日常業務における悩みに対する具体的対応策を提示している。

（5）産業横断サイバーセキュリティ人材育成検討会（CRIF CSF）[26]

産業横断サイバーセキュリティ人材育成検討会は、2015 年 6 月に重要インフラ分野を中心とした企業により発足し、人材の確保（育成と雇用）を主テーマとし、情報共有の仕組みの醸成、必要なセキュリティ能力の明確化、教育プログラム／ツール等の共有、教育の支援策の検討等に取り組んでいる。平成 30 年 11 月に公開された第 2 期最終報告書では、適切なサイバー攻撃対策を推進するには経営者の強いリーダーシップが不可欠であるとし、経営者を支援する組織として「セキュリティ統括（室等）」が必要としている。「セキュリティ統括（室等）」は、経営的な知見とサイバー攻撃やネットワークインフラなどの専門的な知見を有する人材によって構成され、経営を支援しながら関係部署をリードする組織と位置付けている。

検討会では、求められる人物像やスキルに加えて、その業務運用手順を定めた「ユーザ企業のためのセキュリティ統括室構築・運用キット」を作成し、公開している。Part2【統括室編】[27]において提示されているセキュリティ統括室の機能を図に示す。「セキュリティ統括（室等）」が担うべき主な役割は、以下のとおり。

- 情報収集及びセキュリティ戦略の立案
- セキュリティ戦略の推進に向けた報告・調整
- 新規技術・サービスに対するセキュリティ検証
- アウトソーシング及び調達に関するセキュリティ要件の策定

報告においては、「セキュリティ統括（室等）」の組織的な在り方についても言及している。「セキュリティ統括（室等）」は必ずしも部署化する必要はなく、チーム体制での運用も想定しており、想定する体制案を以下としている。

[25] https://www.ipa.go.jp/security/fy30/reports/ciso/index.html
[26] https://cyber-risk.or.jp/
[27] https://cyber-risk.or.jp/contents/Security-Supervisor_Toolkit_Part2_v1.0.pdf

- 委員会型
- CSIRT 型
- 専任組織型



図２−２　セキュリティ統括室の機能

（６）法人組織におけるセキュリティ実態調査 2019 年版[28]

トレンドマイクロ株式会社は、日本国内の官公庁自治体および民間企業における情報セキュリティ対策の意思決定者および意思決定関与者を対象に、セキュリティインシデントによる被害とセキュリティ対策の実態を明らかにする調査「法人組織におけるセキュリティ実態調査 2019 年版」を 2019 年 6 月に実施した。報告書によれば、国内法人組織の

[28] https://www.trendmicro.com/ja_jp/about/press-release/2019/pr-20191015-01.html

36.3%が 2018 年 4 月～2019 年 3 月の 1 年間にセキュリティインシデントに起因した情報漏えいやデータの破壊などの重大被害を経験し、原因究明のための調査費用、改善策の導入、損害賠償といった事後対応を含めた年間平均被害総額は約 2.4 億円となり、4 年連続で 2 億円を超える結果になったとしている。

法人組織における経営層・上層部のサイバーセキュリティに関するリスク認識の調査では、経営層がセキュリティに十分関与できていない状況であるとしている。経営層・上層部は、セキュリティインシデントによる被害内容次第ではシステムやサービスの停止、ブランドイメージ・信用低下につながり自法人の事業に大きな影響をおよぼす可能性があることを理解し、セキュリティに対するリスク認識を改めることが求められるとしている。

（7）サイバー保険

サイバー攻撃への対策として、損害保険会社よりサイバー保険[29]が商品化されている。主なサイバー保険取り扱い会社は以下のとおり。

- あいおいニッセイ同和損保[30]
- AIG 損保[31]
- 共栄火災[32]
- 損保ジャパン日本興亜[33]
- 大同火災
- 東京海上日動[34]
- 三井住友海上[35]

各社のサイバー保険では、損害や費用の賠償に加えて、教育訓練等のリスク低減策やフォレンジック調査等の事後対策等、サイバーセキュリティ対応に関する付帯サービスを提供しているものが多い。また、あいおいニッセイ同和損保のサイバーセキュリティ保険では、高度なセキュリティ対策を行っている場合に割引を適用している。

[29] http://www.sonpo.or.jp/cyber-hoken/
[30] https://www.ad-cyber.com/insurance/compensation.html
[31] https://www.aig.co.jp/sonpo/business/product/cyberedge
[32] https://www.kyoeikasai.co.jp/corp/liability/roei.html
[33] https://www.sjnk.co.jp/hinsurance/cyber/
[34] https://www.tokiomarine-nichido.co.jp/hojin/baiseki/cyber/
[35] https://www.ms-ins.com/business/indemnity/pd-protector/

２．４．４．監査等の手法の活用

サイバーセキュリティ対策に係る経営層の施策について検討するため、監査等の手法の活用について参考になると思われる公開情報を調査した。

以下に、参考となる基準等を示す。

（１）システム監査基準[36]

システム監査基準は、情報システムのガバナンス、マネジメント又はコントロールを点検・評価・検証する業務（以下「システム監査業務」という。）の品質を確保し、有効かつ効率的な監査を実現するためのシステム監査人の行為規範である。経済産業省より発行されており、最新版は 2018 年改訂である。

（２）システム管理基準（経済産業省 2018 年改訂）

システム管理基準は、前述のシステム監査基準に基づき、システム監査人の判断の尺度を規定するものである。経済産業省より発行されており、最新版は 2018 年改訂である。

（３）監査役監査チェックリスト[37]

日本監査役協会では、「監査役監査チェックリスト④【上場会社編】」を取りまとめてインターネット上に公開している。このチェックリストは、新任監査役が何をどのような視点で監査するのか、といった基本事項の確認も含め、就任後すぐに使えるチェックリストとすること、期末の監査報告書作成に向けて期中監査のツールとなるチェックリストとすること等を基本的な考え方としている。以下、本チェックリストにおいてサイバーセキュリティに係る項目を抜粋する。

No.1807 取締役のセルフチェックリスト

ＸＩ．IT ガバナンス、情報セキュリティ

１．　コーポレートガバナンスの一側面として、ＩＴガバナンスの重要性を認識しているか

２．　対処すべき重要な経営リスクとして、ＩＴリスク・サイバーリスク・情報セキュリティリスクを認識しているか

（１）　ＩＴが組み込まれた業務の性質や重要性に応じてＩＴ活用に係わるリスクを認識しているか

（２）　（１）のリスクの影響を部門横断的に把握できる仕組みを設けているか

No.1816 ＩＴガバナンスのチェックリスト

Ｉ．基本事項の確認

IT ガバナンスとは、コーポレート・ガバナンスの一側面であって、企業価値の向上を

[36] システム管理基準（経済産業省 2018 年改訂）

[37] http://www.kansa.or.jp/support/el009_190111_1.pdf

目指しつつ企業の社会的責任を果たし、かつ事業継続と業務の有効性及び効率性を達成するために、IT の戦略的利活用とそれに伴うリスクに対して、全社的に対処するための取締役の職能と責任の明確化、及びそれを独立した立場から監視・検証する監査役の職能と責任を通じて、企業グループ全体としての IT 利活用の適切な推進と IT 利活用をめぐるリスク対処を効果的にするための仕組み、ないしは活動をいう。〔「監査役に期待されるＩＴガバナンスの実践」（日本監査役協会ＩＴガバナンス研究会 H23.8.25）より引用〕

１．代表取締役等及び監査役は、コーポレートガバナンスの一側面として、ＩＴガバナンスの重要性を認識しているか

２．監査役は、ＩＴガバナンスにおける重大なリスクとして、次の事項を認識しているか

（１） 取締役がＩＴリスク・サイバーリスクの管理・対処を現場任せにした結果、リスクの顕在化により会社に著しい損害が生じるリスク

（２） ＩＴ戦略の曖昧さにより、ＩＴの投資の失敗が招くリスク

（３） ＩＴ戦略が企業の事業戦略と融合されていない結果、事業戦略を効果的に達成できないリスク

３．代表取締役等は、対処すべき重要な経営リスクとして、ITリスク・サイバーリスクを認識しているか

（１） ＩＴが組み込まれた業務の性質や重要性に応じてＩＴ活用に係わるリスクを認識しているか

（２） （１）のリスクの影響を部門横断的に把握できる仕組みを設けているか

Ⅳ．ＩＴリスク・サイバーリスクの評価

１．ＩＴリスク・サイバーリスクの評価結果について、そのリスクが事業経営にいかなる影響を及ぼす可能性があるかという視点でみられているか

２．取引先や業務委託先等を含めたサプライチェーン全体での IT リスク・サイバーリスクの影響が把握されているか

３．子会社等におけるＩＴリスク・サイバーリスクが顕在化したときの企業グループへの影響が把握されているか

４．システム開発のリスクについて留意されているか

（1）開発プロジェクトのミッションが明確でプロジェクト関係者で共有されているか

（2）開発の範囲及びレベルが明確か

（3）開発コストの見積りは実績のある方法で、複数の手法で実施されているか

（4）プロジェクト計画が作成され、承認されているか

（5）プロジェクト計画をベースに進捗管理されているか

（6）問題発生時にその内容と原因が代表取締役等に正しく報告され、適切なアクションがとられているか

（7）大規模基幹システムの開発状況については、定期的に取締役会等に報告されてい

るか

Ⅴ．ＩＴ管理

１．平時においてもサイバーセキュリティリスクや対策に係わる情報開示など関係者とのコミュニケーションを図っているか

２．ＩＴ管理の方針やＩＴ管理のプロセスが、ＩＴ戦略とＩＴリスク・サイバーリスクの評価結果に基づくものとなっているか

３．ＩＴ管理プロセスの定期的チェックが行われているか（情報システム部門管理者からだけではなく、ユーザー部門管理者からも報告を受けていること）

４．情報システムを悪用した不正行為、事故が発生した場合、代表取締役等や監査役への通報体制があるか

Ⅶ. 事業継続管理

7. 災害時のセキュリティ水準（サイバーセキュリティを含む）の低下が想定されているか

No.1819 情報セキュリティのチェックリスト

Ⅰ．基本事項の確認

１．代表取締役等及び監査役は、情報セキュリティリスク・サイバーセキュリティリスクを経営リスクとして認識しているか

「情報セキュリティリスク」：情報の機密性、情報資産の保護、運用システム等が維持されないことにより発生するリスク

「サイバーセキュリティリスク」：コンピュータネットワークから不正侵入され、コンピュータウィルス感染、情報漏えい、改ざん、破壊等されるリスクであり、この対策が不十分な場合、自社が被害にあうだけではなく、サイバー攻撃の踏み台にされ（又はサイバー攻撃に利用され）、自社が加害者となり取引先や顧客に被害を与えることもある

Ⅱ．組織的セキュリティ対策

１．代表取締役等の主導で情報セキュリティ・サイバーセキュリティ（以下「セキュリティ」という）の方針が示されているか

２．代表取締役等は、定期的にセキュリティ対策の状況の報告を受け、把握しているか

３．セキュリティの方針に基づき、具体的な管理体制が構築されているか

４．セキュリティ対策を実施するための体制を整備し、各関係者の責任が明確にされているか

５．セキュリティ対策のためのリソース（人材、費用）の割当てが行われ人材育成されているか

６．グループ会社やサプライチェーンのセキュリティ対策状況の報告を受けている

か
７． 外部監査（第三者の視点で監査、海外拠点整備等のため）が行われているか
８． 各種団体が提供するセキュリティに関する注意喚起情報等を自社のセキュリティ対策に活かしているか

Ⅶ. ＩＴ基盤運用管理（ＩＴ部門が管理するようなシステム管理）
１１． 自社のＩＴ基盤が第三者に対するサイバー攻撃の踏み台に利用されないよう対策が講じられているか
１２． 最新の脅威やサイバー攻撃についての情報収集を行い、リスクや脅威を適時に見直し、必要に応じて社内で共有されているか

出典：監査役監査チェックリスト④【上場会社編】、公益社団法人 日本監査役協会中部支部、2019 年 1 月 11 日、http://www.kansa.or.jp/support/el009_190111_1.pdf

（４）ISMS

ISMS とは、組織内での情報の取り扱いについて、機密性、完全性、可用性を一定の水準で確保するための仕組みのことであり、組織の管理の一環として、取り扱う情報の種類などから確保すべきセキュリティの水準を定め、計画や規約を整備して情報システムの運用などに反映させる取り組みの総体のことである。ISMS においては、情報セキュリティ上のリスクについて、アセスメント（特定・分析・評価）を行って対応方針を決め、実際に現場で起きる様々なリスクへ対応し、一定期間状況を監視・記録（モニタリング）して検証（レビュー）し、結果を元に再度アセスメントから一連のプロセスを繰り返すというサイクルを継続的に実施することが求められる。

リスクアセスメントについては、資産ベースと事業被害ベース（シナリオベース）の分析手法[38]がある。重要インフラ分野においては、機能保障の考え方に基づく事業被害ベースの分析手法の採用が望まれる。[39]

（５）サイバーセキュリティフレームワーク

サイバーセキュリティフレームワーク（CSF）[40]とは、サイバーセキュリティ管理のためのツールのひとつであり、リスクの観点から見たサイバーセキュリティ管理手法である。米国国立標準技術研究所（NIST）が 2014 年 2 月に発表した「重要インフラのサイバーセキュリティを向上させるためのフレームワーク」が正式な名称であり、2013 年 2 月に米国で発布された大統領令第 13636 号「重要インフラのサイバーセキュリティの向上」を受けて作成されたものである。

１）フレームワークコア

5 つの機能［特定、防御、検知、対処（対応）、復旧］ごとにカテゴリー・サブカテゴリ

[38] https://www.ipa.go.jp/files/000069436.pdf
[39] https://www.nisc.go.jp/active/infra/pdf/pubcom_tebikisho.pdf
[40] 重要インフラのサイバーセキュリティを改善するためのフレームワーク、IPA 翻訳版 https://www.ipa.go.jp/files/000071204.pdf

ーで細かく規定されたリスク項目のリストであり、項目を取捨選択して後述のプロファイルを作成する。

２）フレームワーク・インプリメンテーション・ティア

フレームワークコア項目の評価指数で、ティア１～ティア４の４段階から構成される。自組織がサイバーセキュリティをどのように捉え、そうしたリスクを管理するためにどのようなプロセスを実施しているかを示したもの。

３）フレームワークプロファイル

コアから自組織に必要なコア項目を選択し、現在（AsIs）と目標（ToBe）にそれぞれのティア（1～4）を設定したもの「現在のプロファイル」と「目標のプロファイル」を作成して自組織のサイバーセキュリティ対策の状況を表すことができる。

（６）制御システムのセキュリティリスク分析ガイド[41]

このガイドは、重要インフラを支える様々な分野の制御システムのリスク分析でのノウハウをもとに、リスク分析を具体的に実施するための手順や手引きを示すことを目的として、IPA において作成されたものである。

本書では、制御システムを対象とした詳細リスク分析の手法について解説している。脅威と対策の網羅的な把握のためには、資産ベースのリスク分析が適している。しかし、一次の脅威を洗い出すことはできても、攻撃の連鎖で生じ得る事業被害の回避を検証することは困難である。それを補完する手法としては、シナリオベースのリスク分析を用いる必要が出てくる。一方で、このシナリオベースのリスク分析を全て詳細に実施するとなると、システムによっては膨大な工数となり、現実的な工数では目的を達成できないことが想定される。

このため、制御システムにおいては事業被害の回避の検証が重要であるとして、資産ベースと事業被害ベースの２通りのリスク分析を相互補完的に用いることを解説している。

[41] https://www.ipa.go.jp/files/000069436.pdf

２．４．５．国内外の事例（公開資料より）

（１）米国における電力インフラと IT をめぐる動向[42]

NIST CSF は、様々な企業で導入が進んでおり、米セキュリティ企業 Tenable Network Security 社と米調査会社 Dimensional Research 社が米国内の IT 技術者 300 人に対して行った調査によると、84%の企業が NIST CSF をサイバーセキュリティ・フレームワークの 1 つとして採用しており、約 70%が最も良いフレームワークと捉えている。また、NIST CSF を採用している企業のうち 29%が他社からビジネス要件として求められ、28%が政府との調達契約の要件として求められたため導入したという。NIST CSF をサイバー保険に活用する動きも出ており、2016 年 4 月に開催された Cybersecurity Framework Workshop 2016 では、Zurich Insurance 社など複数の保険会社が NIST CSF のサイバー保険のリスク査定への活用について議論した。その内容によると、NIST CSF を活用することでサイバーセキュリティのリスクについて業界の共通基準が生まれ、保険会社、ブローカー、保険の引き受け企業などの間で議論をしやすくなり、より良い保険商品を低価格で出すことにつながるのではないかと見ている。

出典：米国における電力インフラと IT をめぐる動向、独立行政法人情報処理推進機構、ニューヨークだより 2016 年 6 月号、https://www.ipa.go.jp/files/000053295.pdf

（２）企業の CISO や CSIRT に関する実態調査 2016[43]

4.2.3.結果の考察

米欧企業のヒアリング結果から得られた知見は次のとおりである。

ポイント 1.経営層がサイバーリスクを経営上の重大なリスクとして認識

今回ヒアリングを実施した全ての企業が、サイバーリスクを事業リスクや財務リスクと同等の重大なリスクと捉えている。経営層の間でも、サイバーインシデントがビジネスを継続する上で大きな影響を与えること、経営陣の評価に直接影響を及ぼすことが理解されている。特に、E 社や G 社等のように、情報資産が自社の競争力の源泉となっている企業ほど、セキュリティを重要視している。

セキュリティ投資に関しては、ヒアリング先企業は経営層の理解があり、その多くは ROI 等の投資評価指標を重要視しておらず、必要な対策は実施する方針で進めている。セキュリティ予算を獲得するにあたっては、自社が抱えるリスク状況や対策を実施しない場合の影響度、同業他社や同規模企業とのベンチマーク結果を経営層に提示することで、理解を得たうえで対策を進めている。

[42] https://www.ipa.go.jp/files/000053295.pdf

[43] 独立行政法人情報処理推進機構「企業の CISO や CSIRT に関する実態調査２０１６-調査報告書-」（2016 年 5 月 10 日）https://www.ipa.go.jp/security/fy27/reports/ciso-csirt/index.html

ポイント 2.CISO には技術とマネジメントの知識が求められる

今回ヒアリングに協力いただいた CISO 等は全員、自社のサイバーセキュリティに責任を持っていた。主な責務としては、サイバーセキュリティプログラムやポリシーの策定、経営陣への定期的な報告と理解の促進、予算の獲得がある。

今回ヒアリングした CISO は何れも経営層には入っておらず、CTO や CFO 等の下に位置づけられるケースが多い。G 社のように CEO の直下におかれ、必要に応じて CEO に直接報告できるケースもある。

CISO のキャリアパスについては、技術出身がよいかマネジメント出身がよいかで意見が分かれた。技術出身がよいとの意見では、技術の詳細を理解していないと適切な対策の策定や管理、技術者のマネジメントができないとの指摘があった。一方、マネジメント出身がよいとする意見では、サイバーリスクの重要性が高まる中で、経営の観点から経営陣やステークホルダーに説明する能力が必要であるとの指摘があった。意見が分かれたものの、CISO には技術とマネジメント両方のスキルが求められる点では共通していた。

出典：独立行政法人情報処理推進機構「企業の CISO や CSIRT に関する実態調査２０１６-調査報告書-」、2016 年 5 月 10 日、https://www.ipa.go.jp/files/000052362.pdf

（３）取締役会の機能向上等に関するコーポレートガバナンス実態調査報告書[44]

取締役会の機能向上等に関するコーポレートガバナンス実態調査報告書において、以下の記載がある。

海外事例（サイバー被害に対する法的責任）

米国:
金融サービス企業に対するサイバーセキュリティ要件（ニューヨーク州金融サービス局(DFS)）、2017 年 3 月
セキュリティ事故検知後の 72 時間以内に監督当局に通知する義務等、厳しい規制が課されており、違反した場合はニューヨーク州での金融サービス免許を無効化する。

英国:
サイバーセキュリティ法、2018 年 1 月
英国の重要インフラ事業者が効果的なサイバーセキュリティ対策を怠った場合、最大 1700 万ポンド（日本円:約 26 億円）の制裁金が課される

シンガポール:
サイバーセキュリティ法、2018 年 2 月
重要インフラ事業者は、セキュリティ事故発生時に CSA へ報告する義務があるとした。違反した事業者には、10 万シンガポールドル（約 820 万円）以下の制裁金、2 年以内の懲役という罰

[44] https://www.j-cic.com/pdf/report/CybersecurityInformationSharingSurvey-20180309(JP).pdf

則が課される。

出典：諸外国におけるサイバーセキュリティの情報共有に関する調査、一般社団法人 日本サイバーセキュリティ・イノベーション委員会、2018 年 3 月 9 日[45]、
https://www.j-cic.com/pdf/report/CybersecurityInformationSharingSurvey-20180309(JP).pdf

（4）会社事例

経営層がサイバーセキュリティ対策に積極的に関与していると考えられる会社事例を示す。

1）石油資源開発会社[46]

各種社内委員会として「情報セキュリティ委員会」を設置している。

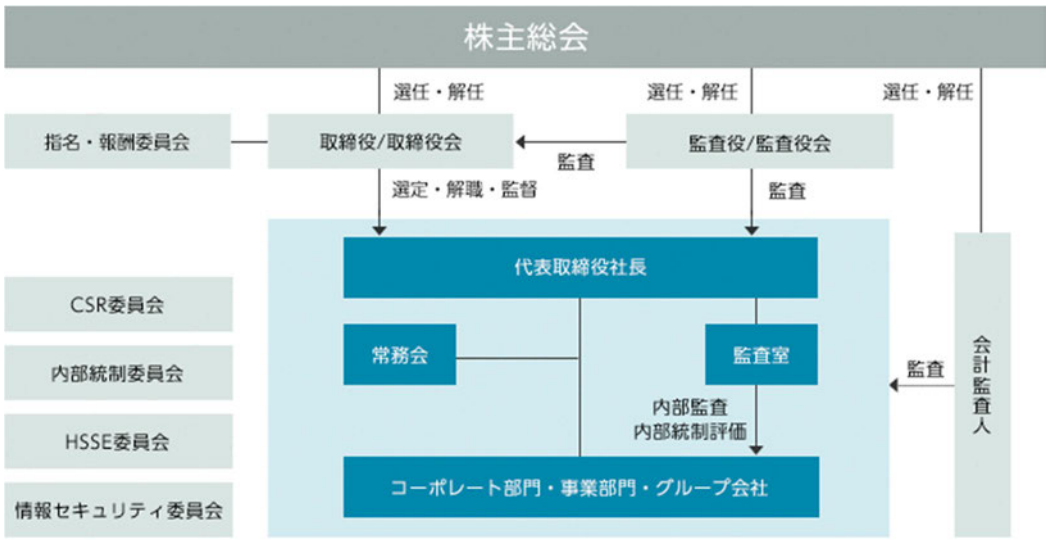


図２-３　石油資源開発会社のコーポレートガバナンス体制図

2）株式会社富士電機[47]

株主・投資家情報のリスクマネジメントにおいて、「リスクの種類と管理体制」、「情報セキュリティに対する取り組み」をホームページに掲載している。サイバーセキュリティ脅威への対応のため、対策システムの整備及びセキュリティセンター（CSIRT/SOC）を設置し、攻撃の監視・防御を実施していることを掲載している。

---

45 諸外国におけるサイバーセキュリティの情報共有に関する調査、一般社団法人 日本サイバーセキュリティ・イノベーション委員会、2018 年 3 月 9 日、
https://www.j-cic.com/pdf/report/CybersecurityInformationSharingSurvey-20180309(JP).pdf

46 https://www.japex.co.jp/company/governance.html

47 https://www.fujielectric.co.jp/about/ir/policy/governance/risk_management.html

３）株式会社電通国際情報サービス[48]

コーポレートガバナンスにおける情報セキュリティの取り組みとして、サイバー攻撃から情報資産を守るためのサイバーセキュリティ対策を推進していることをホームページに掲載している。

４）マネックスグループ株式会社[49]

ESG 情報としてサイバーセキュリティ対策についてホームページに掲載している。サイバーセキュリティ体制として、NIST800 シリーズを参照して包括的なサイバーセキュリティ対策の強化に努めていること、サイバーセキュリティ体制として CEO 直下にサイバーセキュリティ責任者（危機管理執行役）を置きマネックスグループ CSIRT 事務局を統括していること、等をホームページに掲載している。

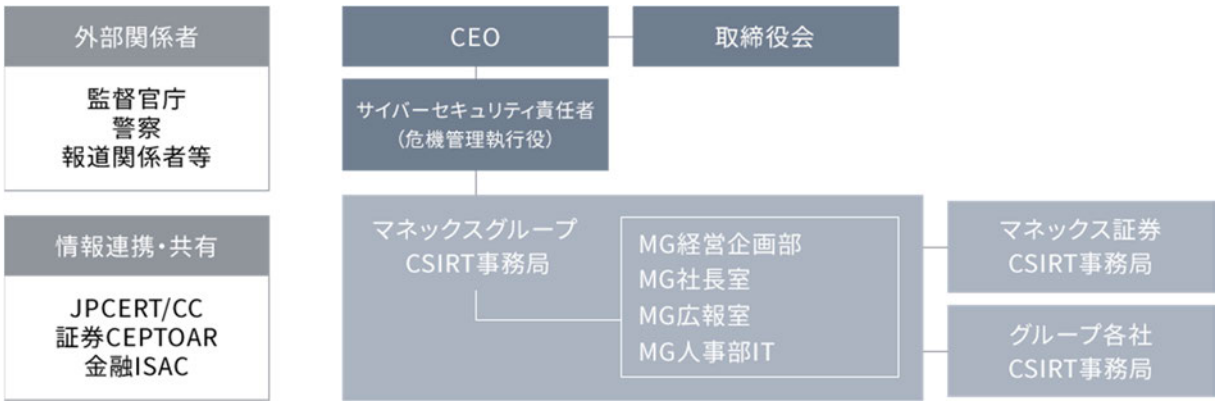


図２−４　マネックスグループのサイバーセキュリティ体制

５）東ソー株式会社[50]

ガバナンスの一環として、サイバーセキュリティの脅威の高まりに対応したセキュリティ強化施策についてホームページに掲載している。

６）昭和電線ホールディングス株式会社[51]

コーポレートガバナンスの一環として、ESG の重点課題としてサイバーセキュリティ対策の強化を挙げ、対策に取り組んでいる。情報セキュリティ管理体制として、CSR 委員会の配下に IT 戦略推進委員会を置き、グループ会社の IT 管理者で構成した委員会組織とし、情報セキュリティ対策の整備、セキュリティ教育計画及び実施、セキュリティ対策への投資提案を行っている。また、サプライチェーン CSR 推進ガイドを作成し、グループ会社を含むサプライチェーン対策に取り組んでいる。

---

[48] https://www.isid.co.jp/isid/csr/governance.html
[49] https://www.monexgroup.jp/jp/esg.html
[50] https://www.tosoh.co.jp/csr/governance/
[51] http://www.swcc.co.jp/environment/csr/governance.html

7）古河電気工業株式会社[52]

サイバーセキュリティ体制として、CSR・リスクマネジメント委員会配下の中央防災・BCM 推進委員会にサイバーセキュリティ専門部会を置き、「古河電工 CSIRT」を設置している。

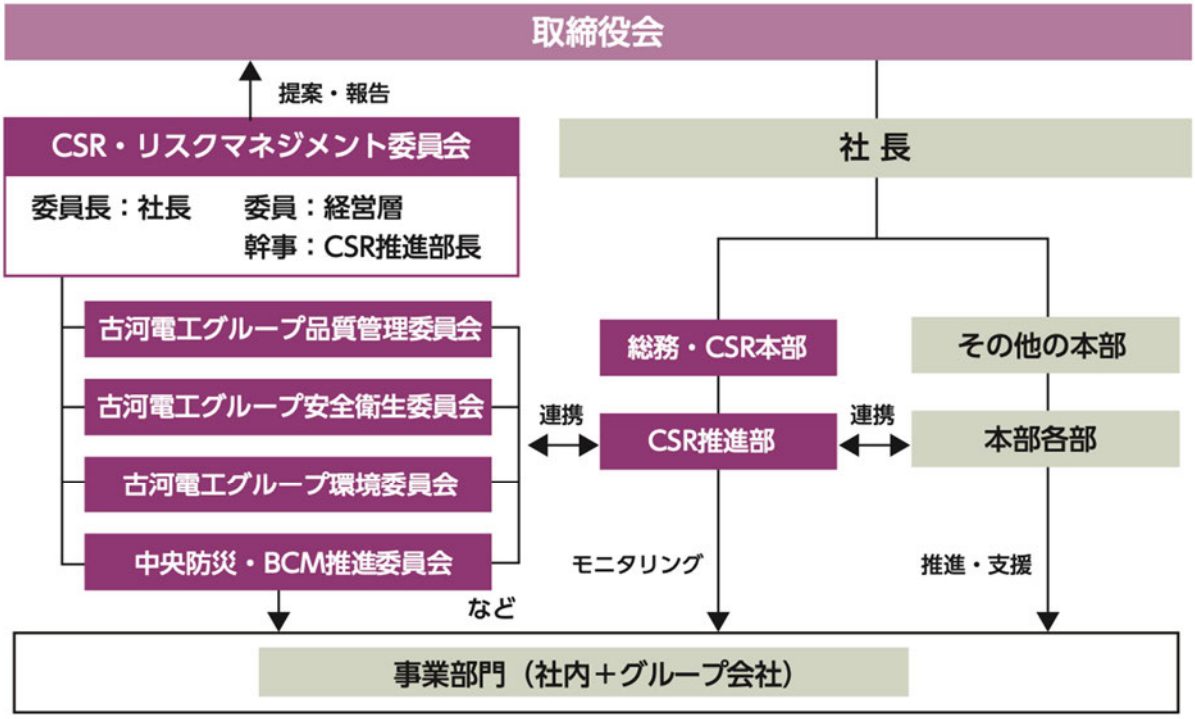


図２−５　古河電気工業の推進体制図

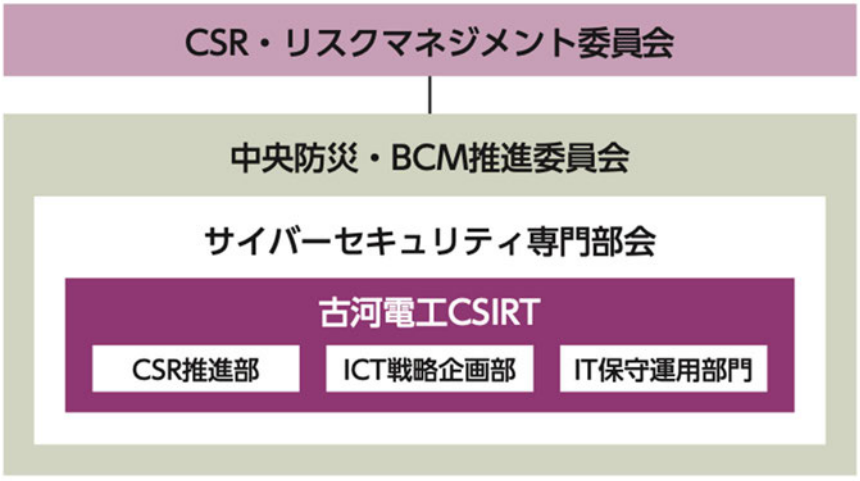


図２−６　サイバーセキュリティに関する組織構成

[52] https://www.furukawa.co.jp/csr/report/pdf/sustainability/2018/2018_11.pdf

８）JFE ホールディングス株式会社[53]

コーポレートガバナンス体制としてグループ情報セキュリティ委員会を設置している。コーポレートガバナンス報告書において、サイバーセキュリティ対策について言及している。

９）JR 西日本グループ

「JR 西日本 CSR REPORT 2018」[54]においてサイバーセキュリティ対策に言及している。

[53] https://www.jfe-holdings.co.jp/company/governance/index.html
[54] https://www.westjr.co.jp/company/action/csr_report/2018/pdf/csr2018.pdf

２．５．サイバーセキュリティ対策推進のための施策検討

調査結果に基づき、サイバーセキュリティの観点から、事業経営において対策の推進強化に効果のある施策を検討する。

２．５．１．検討方針の設定

前述したとおり、国土交通省が作成した安全ガイドラインにおいて、経営層に求められている対策項目は、下記の４点６項目である。

① 情報セキュリティ方針の策定・見直し

- 経営層は、情報セキュリティの確保のため、情報セキュリティ対策に取り組むことを情報セキュリティ方針等に含め、組織の内外に対して宣言する。
- 経営層は、情報セキュリティ方針が妥当かつ有効であることを定期的に確認するとともに、自組織を取り巻く状況に大きな変化が生じた場合にも確認する。

② 情報セキュリティ対策の運用状況把握

- 経営層は、定期的に PDCA サイクルの取組状況を確認し、関係主体等と調整し改善を行う。また、情報セキュリティリスクへの対応結果が事業に与えた効果と影響を検証する。
- 経営層は、情報セキュリティに対する取り組みが、適切及び有効であることを確実にするために、システム監査やその他のリソースを活用してレビューを実施する。レビュー結果は文書化するとともに改善や見直しを指示する。

③ 重要インフラサービス障害に対する防護・回復

- 経営層は、情報セキュリティに関してステークホルダーの信頼・安心感を醸成する観点から、平時における情報セキュリティ対策に対する姿勢やインシデント発生時の対応に関する情報の開示等に取り組む。

④ 内部監査や外部監査を通じた課題抽出

- 経営層は、監査の結果等から、目標未達や進捗遅延、セキュリティ対策の改善点等が確認された場合は、今後に向けた再発防止策を立案し、改善を指示する。これらを繰り返し実施し、情報セキュリティ対策の取り組みの効果を高める。

以上を踏まえ、サイバーセキュリティ対策推進のために経営層が取るべき具体的な施策について、これらの観点で整理することとした。検討項目は、下記のとおり。

① 情報セキュリティ方針の策定・見直し

- 情報セキュリティ方針を定め、組織の内外に宣言するための施策
- 情報セキュリティ方針の妥当性及び有効性を定期的な間隔で確認するための施策
- 自組織を取り巻く状況変化が発生した場合の確認のための施策

② 情報セキュリティ対策の運用状況把握

- 定期的に PDCA サイクルの取組状況を確認し、関係主体等の対話の機会等を通じて改善を行うための施策
- 情報セキュリティリスクへの対応結果が事業に与えた効果と影響を検証するための施策
- システム監査、その他のリソースを活用したレビューを実施するための施策

③ 重要インフラサービス障害に対する防護・回復

- 平時における情報セキュリティ対策に対する姿勢の開示等に関わる施策
- インシデント発生時の対応に関する情報の開示等に関わる施策

④ 内部監査や外部監査を通じた課題抽出

- 監査の結果等から、目標未達や進捗遅延、セキュリティ管理策の要改善点等を確認するための施策
- 要改善点等が確認された場合に、改善指示を行い、今後に向けた再発防止策を立案するための施策

２．５．２．施策の検討

（１）情報セキュリティ方針の策定・見直し

１）セキュリティ方針を定め、組織の内外に宣言するための施策

経営者がサイバーセキュリティリスクへの対応方針を策定し、宣言していないと、サイバーセキュリティ対策などの実行が組織の方針に基づき一貫したものとならない。また、セキュリティ方針を定め、経営者が宣言することにより、ステークホルダー（株主、顧客、取引先など）の信頼性を高め、企業価値向上につながるが、宣言がない場合は、企業におけるサイバーセキュリティへの重要度がステークホルダーに伝わらず信頼性を高める根拠がないこととなる。このため、サイバーセキュリティリスクを経営リスクの一つとして認識し、組織全体での対応方針を策定し、コーポレートガバナンス報告書等においてその取り組みを公開することが重要である。

「経営層は、サイバーセキュリティリスクの重要性について経営会議において認識を共有する（施策案１）」ことが必要となることから、セキュリティ方針の策定、社外公開は取締役会等の経営会議[55]の決議事項とすることが望まれる。

２）情報セキュリティ方針の妥当性及び有効性を定期的な間隔で確認するための施策

KPMG の報告にあるように、経済産業省が公表している「産業サイバーセキュリティ強化へ向けたアクションプラン」において、サイバーセキュリティを考慮した取締役会での実効性評価の促進といった施策が重視されている。このため、経営層が実施すべき具体的な施策として、**サイバーセキュリティへの対応について、取締役会審議事項に含めること**が挙げられる。

主な審議事項としては、セキュリティリスクの識別が挙げられる。特にサイバーセキュリティリスクが経営上の重大なリスクであることを踏まえ、自社が置かれた環境において経営に影響を与えるサイバーリスクを特定し、取締役会等の経営会議において認識を共有し、自社の情報セキュリティ方針の妥当性や有効性を確認することが望まれる。また、取締役としての善管注意義務を果たしていることを証明するために取締役会における議事について、「取締役会の実効性評価」として外部専門家による評価を受けてエビデンスを残すことが望ましい。「企業の CISO や CSIRT に関する実態調査 2016」によれば、米欧企業のヒアリング結果から、経営層がサイバーリスクを経営上の重大なリスクとして認識し、委員会等を設置して取締役会による審議を実施している。国内においても、情報セキュリティリスクに関わる委員会を設置している事例もある。このため、経営層は、サイバーセキュリティリスクに関する委員会を設置することを検討すべきである。（施策案２）

委員会構成メンバーには、橋渡し人材である CISO や情報システム部門を所管する役職者の他に、事業継続や危機管理を所管する役職者等の参画が望まれる。委員会においては、対処すべき重要な経営リスクとしてサイバーセキュリティリスクを識別し、評価するとともに、サイバーセキュリティリスクに係る社内外の状況変化を踏まえた上で、評価結果を

[55] 経営層による意思決定の場は「取締役会」に限定されないため、本報告書では「経営会議」と総称することとした。

取締役にインプットすることが望まれる。

３）自組織を取り巻く状況変化が発生した場合の確認のための施策

情報共有体制の確立を目的とした施策として、ISAC の設立がある。例えば、電力分野においては 2017 年に電力 ISAC が設立されており、国内外の関係機関からの情報収集と分析のほかに、電力会社や大規模発電事業者等の会員同士において様々な WG が設置され情報共有が行われている[56]。こうした情報共有は経営層も例外ではなく、各種の会合等において、取締役レベルでのサイバーセキュリティ対策に係る情報共有が行われている。

こうしたことから、共有すべき情報については、攻撃事例や脆弱性情報等の現場担当者レベルから、より上位の役職者が共有すべき事業リスクに関する情報まで様々なものがある。このため、自組織を取り巻く状況変化が発生する場合に備えて、経営層自らが情報共有に努める必要がある。（施策案３）

なお、電力分野においては、サイバーセキュリティ対策が法制化されていることにより、経営層における情報共有が活発に行われる環境下にあるが、他の重要インフラ事業分野においても同様に法制化される動きがあり、今後、経営層自らが情報共有する場が増えるものと考えられる。

（２） 情報セキュリティ対策の運用状況把握

１）定期的に PDCA サイクルの取組状況を確認し、関係主体等の対話の機会等を通じて改善を行うための施策

PDCA（Plan[計画]、Do[実行]、Check[実施状況の確認・評価]、Act[改善]）を実施する体制が構築できていないと、立案された計画の確実な実行や継続的な業務改善がなされない恐れがある。このため、経営層は計画を確実に実施し、改善していくため、サイバーセキュリティ対策を PDCA サイクルで運用する必要があり、**経営層が主体となって PDCA サイクルを実施する組織を発足し定期的な報告を受ける**必要がある。（施策案４）

PDCA サイクルの実施に際しては、リスクアセスメントを行うことによりリスクを特定し、それに対する対応策を立案することが必要となる。重要インフラ分野におけるリスクアセスメントにおいては事業被害ベースの分析手法を採用することが推奨されているため、組織の発足に際してはサイバー攻撃による事業被害を評価することのできる橋渡し人材（CISO を支えるチーム）を登用する必要がある。

２）情報セキュリティリスクへの対応結果が事業に与えた効果と影響を検証するための施策

PDCA サイクルの実施に際しては、橋渡し人材が、現場担当者をはじめとする関係主体と対話し、改善を行う必要がある。このためには、橋渡し人材の育成に加え、現場担当者の教育を強化する必要がある。現場担当者は IT に係る十分な知識を有していない場合が多いため、橋渡し人材がサイバー攻撃による事業被害を適切に評価するためには、橋渡し人材が現場担当者から的確に情報収集できるよう、IT の基礎知識やサイバー攻撃対策に係る知

[56] https://www.meti.go.jp/shingikai/sankoshin/hoan_shohi/denryoku_anzen/pdf/019_04_00.pdf

識が現場担当者にも必要である。（施策案５）

３）システム監査その他のリソースを活用したレビューを実施するための施策

PDCA サイクルの実施に際しては、システム監査人等、内部監査を実施するための人材を育成する必要がある。内部のシステム監査を行う人材についても、サイバー攻撃対策に係る知識が必要である。（施策案５）

（３） 重要インフラサービス障害に対する防護・回復

１）平時における情報セキュリティ対策に対する姿勢の開示等に関わる施策

ESG とは、環境（Environment）、社会（Social）、ガバナンス（Governance）の頭文字を取ったものである。今日、企業の持続的な成長のためには、ESG が示す 3 つの観点が必要だという考え方が世界的に広まってきており、ESG の観点は、企業の株主である投資家の間で急速に広がってきている。投資の意思決定において、従来型の財務情報だけを重視するのでなく、ESG も考慮に入れる手法は「ESG 投資」と呼ばれており[57]、ESG は、平時における企業の姿勢の開示に関わる施策の重要な要素である。このため、ESG 要素に関する情報開示を検討することが望まれる。（施策案６）

サイバーセキュリティ対策は、ガバナンス（Governance）に位置付けられる。例えば、マネックスグループは、ESG 要素の一環としてサイバーセキュリティ対策に関する情報開示を行なっている[58]。

２）インシデント発生時の対応に関する情報の開示等に関わる施策

これまで事故や不祥事が発生した際、情報の発信の内容、タイミング、方法などを誤り、企業イメージやブランドを毀損する企業が多く見られる。特に初動対応を誤ったことによりメディアから多くの批判を浴び、経営トップの責任まで問われるケースも珍しくない。インシデント発生時におけるマイナスイメージの拡散を防ぐ情報発信のあり方や記者会見の対応など、危機管理コミュニケーション（クライシス・コミュニケーション）について平素からの準備が必要である。このため、コンティンジェンシープランに基づき経営としての適切な情報開示を実施するために、経営層自身が危機管理コミュニケーション力を高めることが重要である。（施策案７）

サイバー攻撃対する組織的対応として、CSIRT（Computer Security Insident Response Team）を設置する企業が増えている。CSIRT は、その名が示すとおり、コンピュータセキュリティに関するインシデント対応組織であり、企業の社内情報システム担当部門が所管することが多い。一方で、重要インフラ分野のコンピュータセキュリティに対するインシデント対応は、事業を所管する部門ごとに行われる縦割りになっており、社内情報システム担当部門と連携がとれていない場合がある。このため、今後サイバー攻撃対策に係る CSIRT 組織の新設や見直しの際に、縦割りの解消や部門間の連携強化が課題となる。

---

[57] https://www.meti.go.jp/policy/energy_environment/global_warming/esg_investment.html
[58] https://www.monexgroup.jp/jp/esg/cyber_security.html

CSIRT 拡大の一例としては、日立グループの CSIRT の事例が参考になる[59]。日立グループの CSIRT の組織構成は、日立グループの SI ベンダーIRT、製品ベンダーIRT、社内ユーザーIRT 及びこれらの組織間の連携調整を行う HIRT/CC の 4 組織から構成され、CSIRT 機能から組織間の相互連携を行う機能を独立させその傘下に情報システム部門や事業部門のインシデント対応組織が入ることにより、部門間の連携調整機能の強化が図られている。今後、重要インフラ分野においても、部門間の連携調整機能の強化が重要となることから、日立グループの事例の様に、部門間の連携調整機能を強化する体制が主流になるものと考えられる。また、サイバーセキュリティリスクが事業継続における重要な要素であることから、分離された統括組織はサイバーセキュリティに係る危機管理機能を担うことになる。このため、危機管理を統括する部門の役割を強化する必要がある。（施策案８）

（４） 内部監査や外部監査を通じた課題抽出

１）監査の結果等から、目標未達や進捗遅延、セキュリティ管理策の要改善点等を確認するための施策

サイバーセキュリティ対策に関わるガバナンス等の強化を図るために、監査機能を活用する。（施策案９）監査役は、コーポレートガバナンスの一側面として、IT ガバナンスの重要性を認識し、経営層の施策をチェックする機能を有している。このため、監査役自身がサイバーセキュリティの重要性を理解するとともに、経営層は、監査役が有効に機能する環境を構築する必要がある。

２）要改善点等が確認された場合に、改善指示を行い、今後に向けた再発防止策を立案するための施策

IT の爆発的な普及に伴い、昨今においては、すべての経営資源がサイバー攻撃の脅威に晒されていると言っても過言ではない。このような状況下、付け焼き刃的な対処療法ではサイバー攻撃に対抗することができなくなっている。このため、サイバーセキュリティ対策を自社の経営計画と紐付け、中長期の視点で対策を講ずることが重要となる。サイバーセキュリティフレームワークを活用して自社のセキュリティ状況の現状と将来目標を定め、これに基づき目標未達や進捗遅延を管理する。（施策案１０）

[59] http://www.hitachi.co.jp/hirt/about/index.html

２．５．３．検討結果

以上までの検討結果をもとに、経営層がとるべきサイバーセキュリティ対策の具体的施策について１０項目に取りまとめた。

情報セキュリティ方針の策定・見直しに係る施策
（経営層におけるセキュリティ方針の合意形成）

施策案１　サイバーセキュリティリスクの重要性について経営会議において情報を分析する。

施策案２　サイバーセキュリティリスクに関する検討組織を設置する。

施策案３　経営層として情報共有に努める。

情報セキュリティ対策の運用状況把握に係る施策

施策案４　PDCA サイクルを実施する組織からリスク対応について定期的な報告を受ける。

施策案５　有事に備えた現場担当者教育を強化する。

重要インフラサービス障害に対する防護・回復に係る施策
（平時の対策と有事への対応強化）

施策案６　サイバーセキュリティリスクへの取り組みについて積極的な情報開示に努める。

施策案７　危機管理コミュニケーション力を高める。

施策案８　危機管理を統括する既存部門と CSIRT の連携を強化する。

内部監査や外部監査を通じた課題抽出に係る施策

施策案９　監査機能を積極活用する。

施策案１０　自社のセキュリティ水準の将来目標を定め目標達成や進捗状況を管理する。

２．６．経営層がとるべきサイバーセキュリティ対策の具体的施策

２．６．１．施策

２．２節に示した経営層の役割を踏まえ、経営層がとるべきサイバーセキュリティ対策の具体的施策を以下とした。

組織作りに係る施策

施策１　サイバーセキュリティリスクの重要性について経営会議において情報を分析する。
施策２　サイバーセキュリティリスクに関する検討組織を設置する。
施策３　危機管理を統括する既存部門と CSIRT の連携を強化する。

状況把握に係る施策

施策４　PDCA サイクルを実施する組織からリスク対応について定期的な報告を受ける。
施策５　経営層として情報共有に努める。
施策６　危機管理コミュニケーション力を高める。

指示に係る施策

施策７　有事に備えた現場担当者教育を強化する。

確認に係る施策

施策８　監査機能を積極活用する。

情報発信に係る施策

施策９　サイバーセキュリティリスクへの取り組みについて積極的な情報開示に努める。
施策１０　自社のセキュリティ水準の将来目標を定め目標達成や進捗状況を管理する。

施策１ サイバーセキュリティリスクの重要性について経営会議において情報を分析する。

サイバーセキュリティリスクの重要性について取締役会等の経営会議において協議・分析し、その結果に基づき、経営層が共通した認識の下で意思決定を行う。

施策例

- 発生し得る重大なサイバーセキュリティリスク（例えば、サイバーテロによる業務妨害、経営戦略上において重要な秘密の流出、ビジネスメール詐欺）を経営リスクとして認識する。
- 重大なサイバーセキュリティリスクについて、取締役及び監査役間において意見交換する等、経営層の間で日頃より認識の共有に努める。
- 重大なサイバーセキュリティリスクへの対応について、取締役会等の経営会議における審議事項に含める。特にサイバーリスクが経営上の重大なリスクであることを踏まえ、経営会議において認識を共有し、自社の情報セキュリティ方針の妥当性及び有効性を会議体において確認する。審議は、株主総会直前の経営会議を含む年２回程度が望まれる、また重大なリスクが発生した場合は、その都度リスクの所在と対応状況を確認することが望まれる。
- 情報セキュリティ対策（社内の情報資産の機密性、完全性、可用性の確保）の不備がサイバーセキュリティリスク発現の端緒となることを踏まえ、自組織における情報セキュリティ対策にも留意する。

施策を怠った場合のシナリオ

- 経営層が自らの状況認識を高めることを放棄し、積極的に脅威情報の収集を怠ることにより、組織全体がサイバーセキュリティリスクに目を向けなくなり、対策が停滞する。
- 経営者が宣言するサイバーセキュリティリスクへの対応方針が総花的になり、実効性が乏しくなる。
- サイバーセキュリティ対策の優先順位が不明確になり、投資対効果の低下を招く。
- サイバーセキュリティ対策などの実行が組織の方針と一貫したものとならない。
- サイバー攻撃による事故が発生した場合に、企業としての管理責任が問われる。取締役会における協議・分析の議事等のエビデンスを残していないことにより、取締役としてのサイバーセキュリティリスク対応における善管注意義務を問われる。

参考までに、経営リスクの分析例を下表に示す。この表は、「重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書（第１版）改定版」[60]の「別紙１　業務の阻害につながる事象の結果の例」における運輸分野の例を抜粋したものである。この表をもとに、自社において発生し得る重大なサイバーセキュリティリスクを分析することが望まれる。

表２－１　経営リスクの分析（例）

経営資源 （情報資産）	業務の阻害につながる事象 （サイバー攻撃により発生する事象）	事象発生による影響 （重大なサイバーセキュリティリスク）
運行管理・電力管理システム	システム・装置が停止する。	－ 交通機関の運行が停止し、旅客等の移動に影響を及ぼす。 － 物流機能が停止し、貨物等の輸送に影響を及ぼす。 － 安全な運行に支障が生じた場合には、人命にも影響を及ぼす。 － 左記の結果事象やその影響により、レピュテーション（社会的評価）が低下する。
	運行制御の機能が喪失する。	
	中央管理表示の機能が喪失する。	
	異常な運行情報が表示される。	
	ダイヤ選択に誤りが生じる。	
	設定データが喪失する。	
	設定データに誤ったデータが記録される。	
	設定データから誤ったデータが応答される。	
	設定データが社外に流出する。	
予約(荷受)データベース	システム・装置が停止する。	－ 予約業務が停止し、旅客等の移動に影響を及ぼす。 － 荷受業務が停止し、貨物等の輸送に影響を及ぼす。 － 左記の結果事象やその影響により、レピュテーション（社会的評価）が低下する。
	データベース上のデータが喪失する。	
	データベースの応答が滞る。	
	データベースに誤ったデータが記録される。	
	データベースから誤ったデータが応答される。	
	データベース上の情報が社外に流出する。	

具体的な分析手順としては、まず「事象発生による影響（重大なサイバーセキュリティリスク)」について経営層における共通認識を確認する。次に「経営資源（情報資産)」ごとに「業務の阻害につながる事象（サイバー攻撃により発生する事象)」について分析する。

なお、本表は、施策２に示す検討組織が作成するインプット情報の一例であるとともに、施策８に示す監査における重要なインプット情報となる。

[60] https://www.mlit.go.jp/sogoseisaku/jouhouka/sosei_jouhouka9999.html

施策２ サイバーセキュリティリスクに関する検討組織を設置する。

経営層が情報を分析して施策に反映させるために専門の検討機能を組織し、自社におけるサイバーセキュリティリスクの評価を行う。評価結果を経営会議におけるインプット資料として活用して経営方針を立案し、予算確保等、対策推進のための社内資産を確保する。

施策例

- サイバーセキュリティリスクに関する検討組織を設置し、サイバーセキュリティリスクについて検討する。
- 重大なサイバーセキュリティリスクについて、事業被害ベースのリスク分析を実施する。
- 検討組織メンバーには、サイバーセキュリティに知見を持つ者（CISO、橋渡し人材等）と危機管理担当役員を含める。
- 検討組織において以下を検討し、経営会議におけるインプット情報とする。
  - 重視すべきサイバーセキュリティリスクの選定と対策の優先順位付け
  - リスクの発生確率や発生したときの損害試算
  - サイバーセキュリティに係る法令対応の必要性
  - セキュリティポリシー策定あるいは修正方針の立案
  - リスクマネジメント、事業継続計画（BCP）とサイバーセキュリティリスクの関係
  - 組織体制・職務権限・業務分掌のあるべき姿
  - セキュリティ基準・政府ガイドラインへの対応方針
  - リスクに対して実施すべきサイバーセキュリティ対策と費用試算
  - サイバーセキュリティ対策への専門ベンダーの活用等
- 検討組織からのインプット情報をもとに、ヒト、組織、予算等の社内資産を確保する。

施策を怠った場合のシナリオ

- サイバーセキュリティリスクの管理体制を整備していない場合、組織的なサイバーセキュリティリスクの把握が出来ない。
- 適切な予算確保が出来ていない場合、組織内でのサイバーセキュリティ対策の実施や人材の確保が困難となるほか、信頼できる外部のベンダーへの委託が困難となる恐れがある。
- 適切な処遇の維持、改善ができないと、有能なサイバーセキュリティ人材を自社にとどめておくことができない。
- 経営方針に基づく適切な処遇の維持、改善ができないと、有能なサイバーセキュリティ人材を確保することができない。

施策３　危機管理を統括する既存部門と CSIRT の連携を強化する。

経営リスクとサイバーセキュリティリスクを統括管理するために組織連携を強化する。サイバー攻撃が発生した際のシナリオを事業継続計画に含め、その発動の際には、危機管理を統括する既存部門と CSIRT が連携するよう組織を整備する。

施策例

- 事業部門におけるサイバー攻撃への対応において、迅速に CSIRT と連携できるよう組織を整備する。
- サイバー攻撃が発生した際に、危機管理を統括する既存部門と CSIRT が連携できるよう組織を整備する。
- サイバー攻撃により業務停止に至った場合、速やかに業務を再開するため、関係機関との連携や復旧作業を実施できる管理体制を構築する。
- 構築した管理体制の下、重要な業務をいつまでに復旧すべきかの目標について、組織全体として整合をとる（例えば BCP で定めている目標との整合等)。
- サイバー攻撃による被害を受けた場合、被害原因の特定や解析を速やかに実施するため、各種ログの保全や感染端末の確保等の証拠保全が行える体制を構築するとともに、関係機関との連携による調査が行える管理体制を構築する。
- 初動対応時の業務への影響について検討し、緊急時に組織内の各部署(総務、企画、営業等)が速やかに連携できるよう予め取り決めをしておく。
- 原因特定などにおいて、必要に応じて、速やかに安全推進を所管する部署と連携できる管理体制を構築する。

施策を怠った場合のシナリオ

- 事業部門のサイバーセキュリティ対応により CSIRT 組織の構成員の数が増大し、効率的な組織運営ができなくなる。
- 地震、水害等の自然災害リスクや社内不正等のオペレーショナルリスク等、社内における既存のリスク管理体制との整合を取らないと、組織全体としてのリスク管理の方針と不整合が生じる恐れがある。
- 重要な業務が適切な時間内に復旧できず、企業経営に致命的な影響を与える恐れがある。
- サイバーセキュリティリスクに応じた適切な対策が行われていない場合、サイバー攻撃が発生した場合の被害が拡大する可能性がある。
- サイバー攻撃の検知・分析など技術的な取り組みを行っていても、適切な運用が行われていなければ、致命的な被害に発展する恐れがある。
- 事業部門を含む緊急時の対応体制を整備していないと、原因特定のための調査や復旧作業において、組織の内外の関係者間のコミュニケーションが取れず、速やかな対処ができない。

施策４　PDCA サイクルを実施する組織からリスク対応について定期的な報告を受ける。

情報セキュリティの改善活動を統括する立場として、橋渡し人材を主体とする PDCA サイクルを実施する組織を発足し、経営層として直接進捗を確認する。最新動向、世間のインシデント状況、自社の対応状況等を踏まえて、重視するサイバーセキュリティリスクへの対応状況について定期的に報告を受ける。報告をもとに、経営層が重視するサイバーセキュリティリスクへの対応状況を確認する。

施策例

- サイバーセキュリティリスクに継続して対応可能な体制（プロセス）を整備する（PDCA の実施体制の整備）。
- PDCA サイクルにおいて実施するリスク分析について、事業被害ベースのリスク分析を実施することを担当組織に指示する。
- 経営層として重視するサイバーセキュリティリスクについて、リスク分析に反映させる。
- 経営層として重視するサイバーセキュリティリスクについて、対応状況を報告させる。
- サイバーセキュリティリスク管理に関する KPI を定め、組織内の経営リスクに関する委員会においてその状況を経営者に報告する。
- 必要に応じて、セキュリティ診断や監査を受け、現状のシステムやサイバーセキュリティ対策の問題点を把握し、改善を行う。
- 新たなサイバーセキュリティリスクの発見等により、追加的に対応が必要な場合には、速やかに対処方針を策定し、改善を行う。

施策を怠った場合のシナリオ

- PDCA（Plan[計画]、Do[実行]、Check[実施状況の確認・評価]、Act[改善]）を実施する体制が出来ていないと、立てた計画が確実に実行されない恐れがある。
- 事業被害ベースのリスク分析を採用しないことにより、経営層として重視するサイバーセキュリティリスクの対策状況が十分なものか判断できなくなる。
- 最新の脅威への対応ができているかといった視点も踏まえて組織のサイバーセキュリティ対策を定期的に見直さないと、サイバーセキュリティを巡る環境変化に対応できず、新たに発生した脅威に対応できない恐れがある。

施策５ 経営層として情報共有に努める。

経営層が関与することの組織的な効果を踏まえ、サイバーセキュリティリスクに関わる情報共有に努める。

施策例

- サイバーセキュリティリスクに関する検討組織から情報を入手する。
- PDCA を実施する組織から定期報告を受け、社内の情報セキュリティ対策の現状を把握する。
- サイバーセキュリティに関する知見を有する者が誰であるかを確認しておく。
- 経営層として認識する重要なサイバーセキュリティリスクについて社内に周知する。
- 現場に赴き、サイバーセキュリティリスクについて担当者と対話する。
- 経営層に向けたセミナー等に参加し、情報を収集する。
- 自社インシデントの報告等により、同業他社の経営層や所管省庁（該当する場合には、サイバーセキュリティ対処調整センター、サイバーセキュリティ協議会、交通 ISAC 等）との間で、自社のインシデント情報を共有して、サイバーセキュリティリスクに係る情報共有に努める。

施策を怠った場合のシナリオ

- 経営層としての重要情報を見落とすことにより、経営判断を誤る。
- 経営層としての情報共有を怠ることにより、社内のサイバーセキュリティ対策の方針が徹底しない。

施策６　危機管理コミュニケーション力を高める。

危機が発生した際に適切な情報開示ができるよう、危機管理コミュニケーション力を高める。経営層自身が適切な有事対応できるよう、平時より能力を高める。

施策例

- 危機管理コミュニケーションの事例を集め、失敗事例の要因等を参考にする。
- サイバー攻撃が発生した際に、助言を求める者が誰であるかを予め確認しておく。
- 既存の事業継続計画にサイバー攻撃に起因するリスクシナリオを追加する。追加シナリオに沿ってマニュアルを改定する。
- 経営層を含む関係者により、インシデントが発生した際における社外への情報開示に関するマニュアルを作成し、これに沿った模擬訓練を行う。

施策を怠った場合のシナリオ

- 速やかな情報開示が行われない場合、顧客や取引先等にも被害が及ぶ恐れがあり、損害賠償請求などの責任を問われる場合がある。
- 法的な取り決めがあり、所管省庁等への報告が義務づけられている場合、速やかな通知がないことにより、取引の停止や罰則等を受ける場合がある。
- 記者会見での失言、情報を隠蔽しているような誤解を与えてしまうことによって、事態が悪化してしまうことがある。
- ネガティブな印象によって企業価値の低下を招く恐れがある。

施策７　有事に備えた現場担当者教育を強化する。

サイバー攻撃等の有事に備えて、日頃から現場担当者・管理者の教育を行い、体制を強化する。攻撃を最初に検知するのは現場担当者であり、これを踏まえた教育を行う。

施策例

- 現場担当者に対する教育・訓練を行い、重大なサイバーセキュリティリスクが発生した際に迅速かつ適切な対応が行えるよう日頃から備える。
- サイバー攻撃が発生した際に適切に関係部門と連携ができるよう、現場担当者と関係部門を交えた演習・訓練を実施する。
- 体制について検証するために、社外の演習・訓練への参加を促進する。
- 現場担当者向け研修のための予算を確保し、それぞれの役割に応じたセキュリティ教育を継続的に実施する。
- セキュリティポリシーは現場担当者が容易にアクセス可能な場所(社内ポータルサイト等)へ掲載し、定期的な講習を通じて理解する場や機会を設け、自社のセキュリティ対策方針の周知徹底を図る。
- 経営層が重視するサイバーセキュリティリスクについて、社内に周知・徹底する。

施策を怠った場合のシナリオ

- 現場担当者教育を怠ることにより、サイバー攻撃が発生した際の初動対応が遅れ、被害が拡大する。
- 経営層が重視するサイバーセキュリティリスクが現場担当者に周知されないことにより、サイバー攻撃対策が徹底されない。

施策８　監査機能を積極活用する。

経営層が重視するサイバーセキュリティリスクに対応した対策を確実に実施するために、システム監査やセキュリティ監査等の監査機能を積極的に活用する。監査を忌避する風潮を打破し、ガバナンス強化の仕組みとしての活用を図る。

施策例

- 経営層が重視するサイバーセキュリティリスクに適切に対処しているかどうかを点検・評価・検証するよう監査人に指示する。あるいは、経営層が重視するサイバーセキュリティリスクを監査の項目に加えるよう、システム監査やセキュリティ監査を主管する部門に対して指示する。
- 監査機能を活用することにより、サイバーセキュリティ対策に関わるガバナンス等の強化を図る。
- サイバーセキュリティ対策のチェックを実施することができる内部監査人の育成を行う。
- 系列企業、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の委託先等のサイバーセキュリティ対策についての報告を受け把握する。（監査を含む）
- 個人情報や技術情報等の重要な情報を委託先に預ける場合は、委託先の経営状況等も踏まえて、情報の安全性の確保が可能であるかどうかを定期的に確認する。

施策を怠った場合のシナリオ

- 経営層が重視するサイバーセキュリティリスクについての対策が徹底されない。
- 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ことにより、これらの企業を踏み台にして自社が攻撃される。
- システム管理などの委託業務において、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。

施策９　サイバーセキュリティリスクへの取り組みについて積極的な情報開示に努める。

株主や投資家等を含め、多様な利害関係者に向け、サイバーセキュリティリスクへの取り組みについて積極的な情報開示に努める。

施策例

- 情報セキュリティポリシーを含むサイバーセキュリティリスクへの取り組みについて、株主、投資家、業務従事者、その他の利害関係者等の視座を考慮し、総合的な見地に基づいて情報を開示する。
- 経営者が組織全体の対応方針を組織の内外に宣言できるよう、企業の経営方針と整合を取り、サイバーセキュリティリスクを考慮したセキュリティポリシーを策定する。その際、情報システムのみではなく、製造、販売、サービス等、事業に応じた対応方針を検討する。
- 株主・投資家向け情報として、サイバーセキュリティリスクへの取り組みを企業のホームページにおいて公開することを検討する。
- コーポレートガバナンス報告書にサイバーセキュリティリスクへの取り組みを記載することを検討する。
- サイバーセキュリティ対策の状況について、サイバーセキュリティリスクが影響する事業領域や度合いに応じて、情報セキュリティ報告書、CSR 報告書、サステナビリティレポートや有価証券報告書等への記載を通じて開示を検討する。

施策を怠った場合のシナリオ

- トップの宣言により、ステークホルダー（株主、顧客、取引先など）の信頼性を高め、企業価値向上につながるが、宣言がない場合は、企業におけるサイバーセキュリティへの重要度がステークホルダーに伝わらず信頼性を高める根拠がないこととなる。
- 適切な開示を行わなかった場合、社会的責任の観点から、事業のサイバーセキュリティリスク対応についてステークホルダーの信頼を失う。

施策１０　自社のセキュリティ水準の将来目標を定め目標達成や進捗状況を管理する。

中長期の事業計画と整合したサイバーセキュリティ対策を計画し、実行する。自社が目標とする中長期のセキュリティ水準を定め、目標達成や進捗状況を内部監査の実施を通じて確認する。

施策例

- 中長期の事業計画において達成することが必要となる自社のセキュリティ水準を定める。
  自社のセキュリティ水準については、組織的対策、人的対策、物理的対策、技術的対策が含まれる。
- 自社のセキュリティ水準の将来目標を定め、中長期の事業計画と整合させる。
  対象となる事業計画には、新規事業も含まれる。
- 内部監査の実施に際して、目標とすべきセキュリティ水準の達成度を確認する。

施策を怠った場合のシナリオ

- 企業の経営戦略に基づき、各企業の状況に応じた適切なリスク対応を実施しなければ、過度な対策により通常の業務遂行に支障をきたすなどの不都合が生じる恐れがある。
- 受容できないリスクが残る場合、想定外の損失を被る恐れがある。

２．６．２．施策間の関係とポイント

経営層がとるべきサイバーセキュリティ対策の具体的施策のうち、最も重要なものは施策１である。

施策１　サイバーセキュリティリスクの重要性について経営会議において情報を分析する。

多くの資料において指摘されているように、経営層がサイバーセキュリティリスクの重要性について認識することが最も重要な施策項目である。経営層は、企業経営の意思決定組織である取締役会等の経営会議において認識を共有し、各種の施策を実行するとともに、リスクが発現する局面において迅速かつ適切な意思決定を行うことが求められる。IT が企業の経営活動の隅々まで浸透しつつある今日においては、サイバーセキュリティリスクは単に企業内の IT システムに止まらず、重大インシデントを引き起こす可能性のあるリスクとして捉える必要がある。重要インフラ事業者として、サイバー攻撃が物理的なテロとの組み合わせにより実行される可能性があることにも留意する必要がある。

施策１とその他施策間には、経営層からのアウトプットの観点とインプットの観点がある。それぞれの関係について下記に示す。

（１）経営層からのアウトプットの観点

経営層は、企業活動において重要視すべきサイバーセキュリティリスクに基づき、以下に示す各種の施策を経営層の具体的な指示のもと実施する必要がある。サイバーセキュリティリスクの認識が共有されていない場合には、以下の関連施策が形骸化してしまい、実効性のあるものにならない。

施策１　サイバーセキュリティリスクの重要性について経営会議において情報を分析する。
→施策２　サイバーセキュリティリスクに関する検討組織を設置する。
→施策３　危機管理を統括する既存部門と CSIRT の連携を強化する。
施策４　PDCA サイクルを実施する組織からリスク対応について定期的な報告を受ける。
施策５　経営層として情報共有に努める。
施策６　危機管理コミュニケーション力を高める。
→施策７　有事に備えた現場担当者教育を強化する。
→施策８　監査機能を積極活用する。
→施策９　サイバーセキュリティリスクへの取り組みについて積極的な情報開示に努める。
→施策１０　自社のセキュリティ水準の将来目標を定め目標達成や進捗状況を管理する。

（２）経営層へのインプットの観点

経営層が、サイバーセキュリティリスクの重要性を認識し、適切な施策を実施するためには、以下に示す各種の施策を実施し、経営層へインプットする必要がある。以下の関連施策を経営層が適切に活用できない場合には、適切な意思決定や施策判断ができなくなる。

施策１　サイバーセキュリティリスクの重要性について経営会議において情報を分析する。
施策２　サイバーセキュリティリスクに関する検討組織を設置する。
施策３　危機管理を統括する既存部門と CSIRT の連携を強化する。
施策４　PDCA サイクルを実施する組織からリスク対応について定期的な報告を受ける。
施策５　経営層として情報共有に努める。
施策６　危機管理コミュニケーション力を高める。
施策７　有事に備えた現場担当者教育を強化する。
施策８　監査機能を積極活用する。
施策９　サイバーセキュリティリスクへの取り組みについて積極的な情報開示に努める。
施策１０　自社のセキュリティ水準の将来目標を定め目標達成や進捗状況を管理する。

これらの施策間の関係において、施策２と施策８は、経営層へのインプットとアウトプットの双方向の関係性がある。経営層は、サイバーセキュリティに関する意思決定を支援するための専門組織を設置するとともに、監査機能を活用し、各種の施策を社内に浸透、定着させる必要がある。

施策のポイントとしては、以下が挙げられる。

- 経営層は、サイバーセキュリティリスクを重要な事業リスクの一環として捉え、他の事業リスクとともに危機管理の対象として認識すること
- 経営層は、サイバーセキュリティリスクの重要性について分析し理解すること
- 経営層は、それぞれの施策を実行するとともに、それぞれの内容や進捗状況等について確認すること
- 施策の実施に際しては、意思決定を支援する組織（検討組織、委員会等）及び施策を徹底する組織（監査等）と密に連携すること
- 施策の実施に際しては、IT 部門と他部門の連携強化を推進すること

２．７．施策の評価

２．７．１．施策の特徴

- 経営層がサイバーセキュリティリスクを重要な事業リスクの一つとして捉え、取締役会等の経営会議において共通認識を持つことを施策の重点ポイントとした。この具体的施策として、株主総会前を含む年２回程度の経営会議における議事として、サイバーセキュリティリスクを含む事業リスクについて協議することを示した。協議すべきサイバーセキュリティリスクに関わる事業リスクの一例としては、サプライチェーンリスクが挙げられる。

- 経営層がサイバーセキュリティリスクを重要な事業リスクとして認識するために、検討組織を設置することを施策とした。検討組織は、サイバーセキュリティ対策に知見を持つ CISO 等の有識者と危機管理担当役員を主な構成メンバーとし、自社の事業リスクに与えるサイバーセキュリティリスクの影響を分析・評価し、経営層に助言することを主たる役割としている。企業規模等により検討組織の形態は異なるが、以下の形態が想定される。
  - 社内に委員会組織を設置する。
  - PDCA サイクルを実施する組織を活用する。

- サイバー攻撃への態勢を従来からの危機管理態勢に組み入れることを施策とした。具体的には、危機管理を統括する既存部門と CSIRT の連携を強化するとともに、既存の事業継続計画にサイバー攻撃の要素を追加することを施策とした。

- サイバーセキュリティリスクへの取り組みに関する情報開示について、情報セキュリティポリシーに加えて、以下の手法を施策として提示した。
  - コーポレートガバナンス報告書に記載する。
  - ESG 要素の一つとして IR 情報を公開する。

- 現場担当者がいち早く初動対応できるようにするために、有事に備えた現場担当者教育の強化を施策とした。具体的施策としての教育教材は、平成 30 年度の研究成果物として作成している。

- 経営会議において認識されたサイバーセキュリティリスクへの対応方針を全社に周知し、監査や内部チェックを通してサイバーセキュリティリスク・マネジメントを推進することを施策とした。

- 中長期事業計画を策定する際にサイバーセキュリティリスクを考慮するとともに、同計画とサイバーセキュリティ対策の到達目標と整合させる。具体的には、中長期において展開する全ての事業についてサイバーセキュリティリスクの所在を確認するとともに、

事業計画と整合したサイバーセキュリティ対策を計画に組み入れることを施策とした。

２．７．２．サイバーセキュリティ経営ガイドラインとの関係

サイバーセキュリティ経営ガイドラインでは、経営者が CISO 等に対して指示すべき実施項目を、サイバーセキュリティ経営の重要１０項目として提示している。以下に、サイバーセキュリティ経営ガイドラインにおいて提示されている指示及び対策例と本調査研究における経営層の施策との関係を示す。対策例については、施策との関連するものを抜粋している。

施策１　サイバーセキュリティリスクの重要性について経営会議において情報を分析する。

指示１　サイバーセキュリティリスクの認識、組織全体での対応方針の策定 ・ 経営者が組織全体の対応方針を組織の内外に宣言できるよう、企業の経営方針と整合を取り、サイバーセキュリティリスクを考慮したセキュリティポリシーを策定する。その際、情報システムのみではなく、製造、販売、サービス等、事業に応じた対応方針を検討する。

指示４　サイバーセキュリティリスクの把握とリスク対応に関する計画の策定 ・ 守るべき情報に対して、発生しうるサイバーセキュリティリスク（例えば、経営戦略上重要な営業秘密の流出による損害）を把握する。

経営ガイドラインでは、経営層自身がサイバーセキュリティリスクを認識し、組織全体での対応方針（セキュリティポリシー）を策定し、この方針を組織内外に宣言することを求めている。セキュリティポリシーの宣言については、特に社外に宣言することになるため、その宣言内容について取締役会等の経営会議において合意する必要がある。このため、サイバーセキュリティリスクの重要性について、経営会議において認識を共有し分析することが非常に重要である。経営ガイドラインでは、サイバーセキュリティリスクの例として、経営戦略上重要な営業秘密の流出による損害を挙げているが、重要インフラを提供する企業においては、利用者へのサービス提供を阻害するリスク、ひいては人命につながりかねないような事故を引き起こすリスクについて、経営会議において情報を分析する必要がある。

このため、経営層が実施すべき施策は、この情報を分析するために、経営会議をファシリテートすることであり、日常における取締役間の会話においても、サイバーセキュリティリスクを話題にするような環境を醸成することである。

施策２ サイバーセキュリティリスクに関する検討組織を設置する。

指示２ サイバーセキュリティリスク管理体制の構築 ・ 担当幹部（CISO 等）が、組織内に設置された経営リスクに関する委員会に参加する。

指示９ ビジネスパートナーや委託先等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、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の委託先等のサイバーセキュリティ対策状況（監査を含む）の報告を受け、把握する。

経営ガイドラインにおいて求められるセキュリティポリシーの宣言に際して、経営層は、サイバーセキュリティの現状評価を行うことが重要である。このことの一環として、経営ガイドラインにおいては、担当幹部（CISO 等）が組織内に設置された経営リスクに関する委員会に参加することとしている。

このため、経営層が実施すべき施策は、経営リスク、特にサイバーセキュリティリスクに関する検討組織を設置して現状評価を確認することである。現状評価においては、ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握も重要な確認項目であることを意識すべきである。

施策３　危機管理を統括する既存部門と CSIRT の連携を強化する。

指示２ サイバーセキュリティリスク管理体制の構築 ・ CISO 等は、サイバーセキュリティリスク管理体制を構築し責任範囲を明確にする。 ・ CISO 等が、組織内に設置された経営リスクに関する委員会に参加する。 ・ 取締役、監査役はサイバーセキュリティリスク管理体制が構築、運用されているかを監査する。

指示８ インシデントによる被害に備えた復旧体制の整備 ・ 業務停止等に至った場合に、以下を実施できるような復旧体制を構築する。 －サイバー攻撃により業務停止に至った場合、速やかに復旧するため、関係機関との連携や復旧作業を実施できるよう指示する。また、対応担当者には復旧手順に従った演習を実施させる。 －重要な業務をいつまでに復旧すべきかの目標について、組織全体として整合をとる（例えば BCP で定めている目標との整合等)。

経営ガイドラインにおいては、サイバーセキュリティリスク管理体制を構築するとともに、インシデントに備えた復旧体制を整備することが求められている。特に重要インフラにおけるサイバーセキュリティリスク管理は、事業サービスの提供に直結するものであり、事業部門を交えた復旧体制を整備する必要がある。

このため、経営層が実施すべき施策は、危機管理を統括する部門の役割を強化し、サイバーセキュリティリスクの管理体制と危機管理を統括する部門の連携を強化する組織体制を整備することが重要となる。

施策４　PDCA サイクルを実施する組織からリスク対応について定期的な報告を受ける。

指示６ サイバーセキュリティ対策における PDCA サイクルの実施 ・ サイバーセキュリティリスクに継続して対応可能な体制（プロセス）を整備する（PDCA の実施体制の整備）。 ・ サイバーセキュリティリスク管理に関する KPI を定め、組織内の経営リスクに関する委員会においてその状況を経営者に報告する。KPI としては、リスク分析での指摘事項数、組織内のセキュリティ教育の受講率、インシデントの発生数等が考えられる。

経営ガイドラインにおいては、サイバーセキュリティ対策における PDCA サイクルを実施する仕組みを構築し、組織内の経営リスクに関する委員会においてその状況を経営者に報告することを求めている。

このため、経営層が実施すべき施策は、経営層自らがサイバーセキュリティの現状評価を確認するために PDCA サイクルを実施する組織を発足し、定期的な報告を受けることである。現状評価においては、ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握も重要な確認項目であることを意識すべきである。

施策５　経営層として情報共有に努める。

指示１０ 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及び提供 ・ 情報の入手と提供という双方向の情報共有を通じて、社会全体でサイバー攻撃の防御につなげることが重要。情報共有を通じたサイバー攻撃の防御につなげていくため、情報を入手するのみならず、積極的に情報を提供する。

経営ガイドラインでは、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及び提供を求めているが、経営層においては、サイバーセキュリティリスクの所在やその対策方針について、他社の経営者や有識者との情報共有を行うことが重要である。

このため、経営層が実施すべき施策は、情報共有活動への参加を通じたサイバーセキュリティリスクの所在やその対策情報の入手とその有効活用及び提供を行うことである。経営層自らが、企業経営の観点より、情報の入手と提供という双方向の情報共有を通じて、社会全体でサイバー攻撃の防御につなげることが重要である。

施策６　危機管理コミュニケーション力を高める。

指示７ インシデント発生時の緊急対応体制の整備 ・ 緊急時において、インシデントに関する被害状況、他社への影響等について経営者に報告する対応体制を整備する。

経営ガイドラインにおいては、インシデント発生時の緊急対応体制を整備することが求められている。緊急時においては、インシデントに関する被害状況、他社への影響等について経営者に報告する対応体制を整備するとともに、インシデント発生における現状認識や対応方針について、経営層自らが情報発信することが求められる。

このため、経営層が実施すべき施策は、インシデント発生時の情報開示方針を把握し、適時適切な情報発信が可能となるよう、日頃より準備しておくことである。

施策７　有事に備えた現場担当者教育を強化する。

指示３ サイバーセキュリティ対策のための資源（予算、人材等）確保 ・ 必要なサイバーセキュリティ対策を明確にし、それに要する費用を確保する。 ・ 従業員向けやセキュリティ担当者向けなどの研修等のための予算を確保し、継続的に役割に応じたセキュリティ教育を実施する。

指示５ サイバーセキュリティリスクに対応するための仕組みの構築 ・ 従業員に対する教育を行い、適切な対応が行えるよう日頃から備える。

経営ガイドラインにおいては、サイバーセキュリティ対策のための資源（予算、人材等）確保し、サイバーセキュリティリスクに対応するための仕組みを構築することを求めている。

このため、経営層が実施すべき施策は、有事に備えた現場担当者教育を強化することである。

施策８　監査機能を積極活用する。

指示２ サイバーセキュリティリスク管理体制の構築 ・ 取締役、監査役はサイバーセキュリティリスク管理体制が構築、運用されているかを監査する。

指示６ サイバーセキュリティ対策における PDCA サイクルの実施 ・ 必要に応じて、セキュリティ診断や監査を受け、現状のシステムやサイバーセキュリティ対策の問題点を検出し、改善を行う。

指示９ ビジネスパートナーや委託先等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、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の委託先等のサイバーセキュリティ対策状況（監査を含む）の報告を受け、把握する。

経営ガイドラインにおいては、サイバーセキュリティリスク管理体制の構築の一環として、サイバーセキュリティリスク管理体制が構築、運用されているかを監査役によって監査することを求めている。

このため、経営層が実施すべき施策は、サイバーセキュリティリスク管理体制が構築、運用されているかを監査するために、監査役及び内部監査人の育成を行うことである。

施策９　サイバーセキュリティリスクへの取り組みについて積極的な情報開示に努める。

指示１ サイバーセキュリティリスクの認識、組織全体での対応方針の策定 ・ セキュリティポリシーを一般公開することでステークホルダーや社会に対する企業としての姿勢を示し、信頼性を高める。

指示６ サイバーセキュリティ対策における PDCA サイクルの実施 ・ サイバーセキュリティ対策の状況について、サイバーセキュリティリスクの性質・度合いに応じて、情報セキュリティ報告書、CSR 報告書、サステナビリティレポートや有価証券報告書等への記載を通じて開示を検討する。

経営ガイドラインにおいては、セキュリティポリシーを一般公開することでステークホルダーや社会に対する企業としての姿勢を示し、信頼性を高めることを求めている。近年においては、ESG 要素を重視するステークホルダーが増えていることから、特にガバナンスの観点においてサイバーセキュリティ対策への取り組み状況について情報開示することが求められる。

このため、経営層が実施すべき施策は、サイバーセキュリティリスクへの取り組みに関する情報開示に努めることである。

施策１０　自社のセキュリティ水準の将来目標を定め目標達成や進捗状況を管理する。

指示１　サイバーセキュリティリスクの認識、組織全体での対応方針の策定 ・　経営者が組織全体の対応方針を組織の内外に宣言できるよう、企業の経営方針と整合を取り、サイバーセキュリティリスクを考慮したセキュリティポリシーを策定する。その際、情報システムのみではなく、製造、販売、サービス等、事業に応じた対応方針を検討する。

経営ガイドラインにおいては、企業の経営方針と整合を取り、サイバーセキュリティリスクを考慮したセキュリティポリシーを策定することを求めている。サイバーセキュリティリスクへの対応は短期間に達成できるものではないため、企業の経営方針と整合を取り、中長期の展望を持って対策を講ずる必要がある。

このため、経営層が実施すべき施策は、自社のセキュリティ状況の将来目標を定め、これに基づき目標達成や進捗状況を管理する体制を構築することである。

表２−２　経営ガイドラインにおける原則と施策の関係

経営ガイドラインにおける原則	本報告書における施策
(1) 経営者は、サイバーセキュリティリスクを認識し、リーダーシップによって対策を進めることが必要（経営者はリーダーシップをとってサイバー攻撃のリスクと企業への影響を考慮したサイバーセキュリティ対策を推進するとともに、企業の成長のためのセキュリティ投資を実施すべきである。）	施策１　サイバーセキュリティリスクの重要性について経営会議において情報を分析する。
	施策２ サイバーセキュリティリスクに関する検討組織を設置する。
	施策３　危機管理を統括する既存部門とCSIRTの連携を強化する。
	施策４　PDCA サイクルを実施する組織からリスク対応について定期的な報告を受ける。
	施策７　有事に備えた現場担当者教育を強化する。
	施策８　監査機能を積極活用する。
	施策１０　自社のセキュリティ水準の将来目標を定め目標達成や進捗状況を管理する。
(2) 自社は勿論のこと、ビジネスパートナーや委託先も含めたサプライチェーンに対するセキュリティ対策が必要（自社のサイバーセキュリティ対策にとどまらず、サプライチェーンのビジネスパートナーや委託先も含めた総合的なサイバーセキュリティ対策を実施すべきである。）	施策１　サイバーセキュリティリスクの重要性について経営会議において情報を分析する。

(3) 平時及び緊急時のいずれにおいても、サイバーセキュリティリスクや対策に係る情報開示など、関係者との適切なコミュニケーションが必要（平時からステークホルダー（顧客や株主など）を含めた関係者にサイバーセキュリティ対策に関する情報開示を行うことなどで信頼関係を醸成し、インシデント発生時にもコミュニケーションが円滑に進むよう備えるべきである。）	施策５　経営層として情報共有に努める。
	施策６　危機管理コミュニケーション力を高める。
	施策９　サイバーセキュリティリスクへの取り組みについて積極的な情報開示に努める。

表２−３　施策と経営ガイドラインにおける指示の関係

本報告書における施策	経営ガイドラインにおける指示
施策１　サイバーセキュリティリスクの重要性について経営会議において情報を分析する。	指示１ サイバーセキュリティリスクの認識、組織全体での対応方針の策定
	指示４ サイバーセキュリティリスクの把握とリスク対応に関する計画の策定
施策２ サイバーセキュリティリスクに関する検討組織を設置する。	指示２ サイバーセキュリティリスク管理体制の構築
	指示９ ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握
施策３　危機管理を統括する既存部門とCSIRT の連携を強化する。	指示２ サイバーセキュリティリスク管理体制の構築
	指示８ インシデントによる被害に備えた復旧体制の整備
施策４　PDCA サイクルを実施する組織からリスク対応について定期的な報告を受ける。	指示６ サイバーセキュリティ対策における PDCA サイクルの実施
施策５　経営層として情報共有に努める。	指示１０ 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及び提供
施策６　危機管理コミュニケーション力を高める。	指示７ インシデント発生時の緊急対応体制の整備
施策７　有事に備えた現場担当者教育を強化する。	指示３ サイバーセキュリティ対策のための資源（予算、人材等）確保
	指示５ サイバーセキュリティリスクに対応するための仕組みの構築
施策８　監査機能を積極活用する。	指示２ サイバーセキュリティリスク管理体制の構築
	指示６ サイバーセキュリティ対策における PDCA サイクルの実施
	指示９ ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握
施策９　サイバーセキュリティリスクへの取り組みについて積極的な情報開示に努める。	指示１ サイバーセキュリティリスクの認識、組織全体での対応方針の策定
	指示６ サイバーセキュリティ対策における PDCA サイクルの実施
施策１０　自社のセキュリティ水準の将来目標を定め目標達成や進捗状況を管理する。	指示１ サイバーセキュリティリスクの認識、組織全体での対応方針の策定

２．８．オリパラ対策の検討

提示した 10 の施策は、継続して実施することを前提とするものであるが、2020 年に東京オリンピック･パラリンピック競技大会が開催されるが､過去のオリンピックにおける傾向から、大会中にサイバー攻撃を受ける可能性が考えられる。10 の施策のうち、オリパラでの有事に備えて実施することにより効果が期待できると想定される対策及び内容は以下のとおりである。

施策１　サイバーセキュリティリスクの重要性について経営会議において情報を分析する。

重大なサイバーセキュリティリスクについて、大会前の経営会議において分析結果を再確認することが望まれる。この場合の分析結果には、オリパラ大会特有の要素（開会式や閉会式の開催に係る要人の移動、等）を考慮する必要がある。

施策４　PDCA サイクルを実施する組織からリスク対応について定期的な報告を受ける。

PDCA サイクルを実施する組織から、大会前のリスク対応の状況について報告を受け、現状を確認する。

施策５　経営層として情報共有に努める。

経営層として積極的にオリパラ関係の情報収集と共有に努める。所管省庁へのインシデント報告の確実な履行等、関係組織とインシデント関連情報の共有に努める。

施策６　危機管理コミュニケーション力を高める。

オリパラに特化した危機管理コミュニケーションの実施方法について検討する。具体的には、オリパラ開催時におけるインシデント関連情報の連携先や連携方法、大会の開催を考慮した場合に社会的インパクトの高い発生事象の特定、大会期間中にインシデントが発生した場合の情報公開のタイミングや手法、等がある。

施策７　有事に備えた現場担当者教育を強化する。

現場担当者に教育を実施することが望ましい。また、重大なサイバーセキュリティリスクへの対応について、現場担当者に向けた注意喚起を指示する等、経営層としての認識や方針を社内に発信することが望まれる。

２．９．まとめ

以上までの検討結果についてまとめる。

（１）調査及び情報収集

ヒアリング調査を実施するとともに、参考となる情報収集を実施した。

- 監査（セキュリティ監査、システム監査、監査役監査)、株主対応の観点から４組織を選定してヒアリング調査を実施
- 政府施策、市場動向、監査等の手法の活用、国内外の事例、の観点から公開資料をもとに情報を収集

（２）検討方針の設定

国交省安全ガイドラインより、対策の大項目を抽出し、検討指針とした。抽出した項目を以下に示す。

- 情報セキュリティ方針の策定・見直し
- 情報セキュリティ対策の運用状況把握
- 重要インフラサービス障害に対する防護・回復
- 内部監査や外部監査を通じた課題抽出

（３）具体的施策の検討

ヒアリング結果と収集情報をもとに、各施策項目について具体的な施策を検討した。

（４）施策の整理

検討結果をもとに、経営層がとるべきサイバーセキュリティ対策の具体的施策について１０項目に取りまとめた。

施策１　サイバーセキュリティリスクの重要性について経営会議において情報を分析する。
施策２　サイバーセキュリティリスクに関する検討組織を設置する。
施策３　危機管理を統括する既存部門と CSIRT の連携を強化する。
施策４　PDCA サイクルを実施する組織からリスク対応について定期的な報告を受ける。
施策５　経営層として情報共有に努める。
施策６　危機管理コミュニケーション力を高める。
施策７　有事に備えた現場担当者教育を強化する。
施策８　監査機能を積極活用する。
施策９　サイバーセキュリティリスクへの取り組みについて積極的な情報開示に努める。
施策１０　自社のセキュリティ水準の将来目標を定め目標達成や進捗状況を管理する。

また、各項目の施策例と実施しなかった場合のシナリオを検討した。

（５）施策の評価

サイバーセキュリティ経営ガイドラインの指示項目と比較し、施策評価を実施した。

（６）オリパラ対策の検討

オリパラまでに実施することが望まれる対策を検討した。

施策１　サイバーセキュリティリスクの重要性について経営会議において情報を分析する。
施策４　PDCA サイクルを実施する組織からリスク対応について報告を受ける。
施策５　経営層として情報共有に努める。
施策６　危機管理コミュニケーション力を高める。
施策７　有事に備えた現場担当者教育を強化する。

第３章　経営層を対象とした啓発セミナーの実施

３．１．啓発セミナー

2020 年東京五輪大会の開催を直前に控え、サイバーセキュリティ対策の準備は最終局面に入っている。サイバー攻撃対策の必要性についての経営層の理解は深まって来ており、各事業者ともその対策に積極的に取り組みつつある。一方で、サイバーセキュリティ対策の意思決定では、経営層が強いリーダーシップを発揮することが強く求められる。このような背景の下、本調査研究では、経営層がサイバー攻撃を重要な経営リスクの１つと認識したうえで適切な経営判断を行動に移すための一助として、鉄道及び航空事業者の経営層に向けた交通セキュリティセミナーを実施した。本セミナーでは、取締役と監査役が企業経営の両輪であることを踏まえ、取締役と監査役が認識すべきサイバーセキュリティを取り巻く環境変化を交え、強いリーダーシップを発揮するための施策について解説を行なった。

講演内容については、参考資料に掲載している。

第４章　エキスパート人材の育成

４．１．最新情報提供セミナー

鉄道分野、航空・空港分野のシステム維持管理者、システム障害対応実施者、情報システム担当技術者、異常を検知した際の初動対応の実施者、等を対象に、サイバーセキュリティに関する最新情報提供セミナーを開催した。鉄道事業者に向けては、これまでに発生した代表的な鉄道分野に関連するインシデントを題材に、セキュリティインシデントからの学びを目的とした内容とした。航空事業者に向けては、サイバー攻撃の最新事例を踏まえ、早急に検討すべきリスクと対策を解説する内容とした。本セミナーは、昨年度までに運輸総合研究所が実施した人材育成教育の受講者に対して、サイバーセキュリティに関わる最新情報を提供することも意図している。

講演内容については、参考資料に掲載している。

４．２．机上演習の実施

４．２．１．日程

机上演習は、鉄道分野と航空分野に分けて、以下の日程で実施した。

（１）鉄道分野

日程：第１回　10 月 8 日（火）13 時 30 分～15 時 30 分
　　第２回　10 月 15 日（火）13 時 30 分～15 時 30 分
参加者：　6 名（6 社）

（２）航空分野

日程：第１回　10 月 8 日（火）10 時～12 時
　　第２回　10 月 15 日（火）10 時～12 時
参加者：　7 名（5 社）

４．２．２．演習１日目

（１）概要説明

講師より、机上演習の概要を説明した。アジェンダは、以下のとおり。

1. 「サイバー脅威主体」に対する認識
2. シナリオ：サイバー脅威主体（状況前提）
3. シナリオ：サプライヤからの攻撃侵入
4. シナリオ：特に注目すべきラテラルムーブメント
5. シナリオ：特に注目すべき閉鎖網内 DOS

鉄道分野ではディープウェブの説明、航空分野においては最近の脅威事例（無人航空機システムに関する警告）説明があった。

（２）シナリオによるディスカッション

シナリオ説明の後に、グループに別れてディスカッションを実施した。ディスカッションのテーマは以下の２つである。

- 本シナリオを想定した、サプライヤ（メーカー、保守管理業者等）に対して要求すべき「セキュリティ要件」を検討及び発表する。
- 本シナリオを想定した、サプライヤに起因するセキュリティインシデントが発生した場合、重要インフラサービスの障害を最小限にするための方策を検討及び発表する。

４．２．３．演習 2 日目

（1）概要説明

サイバー脅威主体について、現状の状況前提について講師より説明した。第 1 回の振り返りの後に、本日のシナリオについての状況解説を実施した。

（2）シナリオによるディスカッション

シナリオ説明の後に、グループに別れてディスカッションを実施した。ディスカッションのテーマは以下である。

A) 製品認証、安定運用、ソフトウェア管理の限界等の都合で、セキュリティパッチを適用することが難しい「リモートデスクトップサービスが動作している可能性のある汎用システム」に対するセキュリティ対策について、下記の前提条件の下で検討し、発表する。

- 重要インフラ事業者及びサプライヤが把握できていない「リモートデスクトップサービスが動作している可能性のある汎用システム」が内在しており、特定することが困難である。
- サプライヤから侵入攻撃を完全に防ぐことができない。

B) コストや仕様の都合により、非正規アクセスに対する厳格なセキュリティコントロールの機能を実装することが難しい特徴を持つ「施設・設備点検において導入している IoT 化した計測器」に対するセキュリティ対策について、下記の前提条件の下で検討し、発表する。

- 重要インフラ分野における施設・設備の調達部門は、閉鎖網 DoS 攻撃の発生予見可能性を判断することが難しいため、（コストメリットが高いとされている IoT 化された）計測器に対するセキュリティコストの上乗せの許可を出さない。
- 営利企業であるサプライヤは、回収することのできないセキュリティコストを受け入れることはできない。
- 施設・設備部門の担当者は、サイバーセキュリティの知見やリテラシーを十分に持っていない。

４．２．４．得られた知見

本年度の机上演習では、昨今の国内外の状況を踏まえ、国家が関与する高度かつ組織的なサイバー攻撃を題材としている。演習前半において、このような攻撃が現実に起こり得ることを解説し、後半において以下の観点の検討討議を行った。

- サプライヤが関与するサイバー攻撃への対策
- パッチ適用が困難、コストや仕様の都合といった制約条件下における対策

いずれのシナリオについても模範解答はなく、最悪の状況下を想定したシナリオを前提として机上演習を実施することの重要性を示唆するものである。

机上演習を通じて得られた知見は以下のとおり。

- サイバーセキュリティ対策の実効性及び適正性を確保するためには、現実的な運用やさまざまな環境的制約に配慮する必要がある。
- これらの配慮事項は、サイバーセキュリティ対策を実行する上で″トレードオフとなる阻害事由″となるため、このことを念頭においたセキュリティ設計を行う必要がある。
- サプライヤが関与する複雑化した環境下において、″トレードオフとなる阻害事由″も含め、上層部（経営層/意思決定層）を巻き込んだ状況認識を共有することが必要である。

４．３．教育（本格実施）

４．３．１．日程

教育（本格実施）は、鉄道分野と航空分野に分けて、以下の日程で実施した。

表 4.1　スケジュール

日程	内容	航空	鉄道
１日目	第１回　サイバー攻撃の現状 第２回　サイバー攻撃の手法と脆弱性 第３回　サイバーセキュリティ基礎	9 月 2 日（月） 《参加者》 15 社 18 名	9 月 9 日（月） 《参加者》 18 社局 45 名
２日目	第４回　ネットワーク基礎 第５回　セキュリティ技術 第６回　サイバー攻撃対策	9 月 3 日（火） 《参加者》 11 社 14 名	9 月 10 日（火） 《参加者》 22 社局 47 名
３日目	第７回　サプライチェーンのセキュリティ対策 第８回　インシデント対応 第９回　学習の振り返り コースのまとめと振り返り 質疑応答 グループディスカッション	9 月 4 日（水） 《参加者》 10 社 15 名	9 月 11 日（水） 《参加者》 18 社局 34 名

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

４．３．２．アンケート結果（鉄道分野）

（１）理解度評価

各講座に対する受講者の理解度について、アンケートを実施した。

アンケートの結果より、各回での「ほとんど理解できなかった」「あまり理解できなかった」の割合はいずれも 10%未満である。一方で、第 4 回「ネットワーク基礎」や第 6 回「サイバー攻撃対策」では、「十分理解できた」「大体は理解できた」の合計が 80%を超えているのに対して、第 3 回「サイバーセキュリティ基礎」や第 8 回「インシデント対応」では 60%に満たない割合であり、講義回によって理解度に差がみられる結果となった。

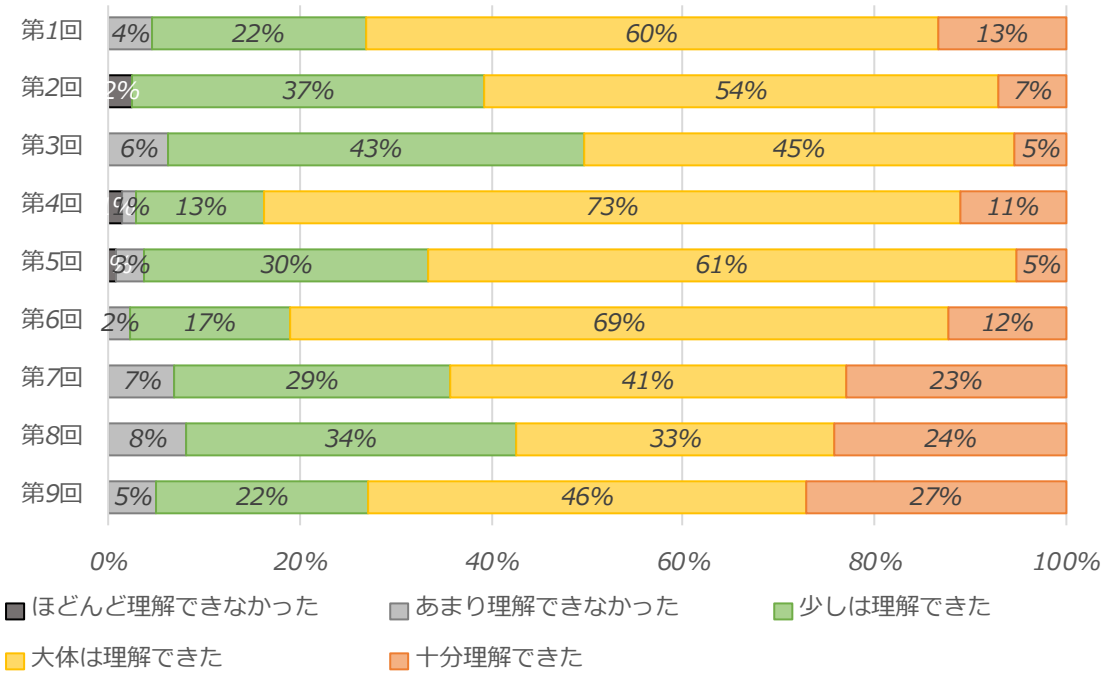


図 4.1　理解度評価

（２）意識評価

各講座に対する受講者の意識について、アンケートを実施した。

アンケートの結果より、各回で 10%未満が「自分の業務に関係しない」「あまり関係しないが一般知識として知っておきたい」との回答で、ほとんどが自身の業務とサイバーセキュリティが関係していることがうかがえる。また「社会的にとても重要な安全管理事項の一つで常に意識すべき事項」との意識は、各回 20%前後で、重要インフラである鉄道分野でのサイバーセキュリティ人材育成や対策の重要性がうかがえる結果となった。

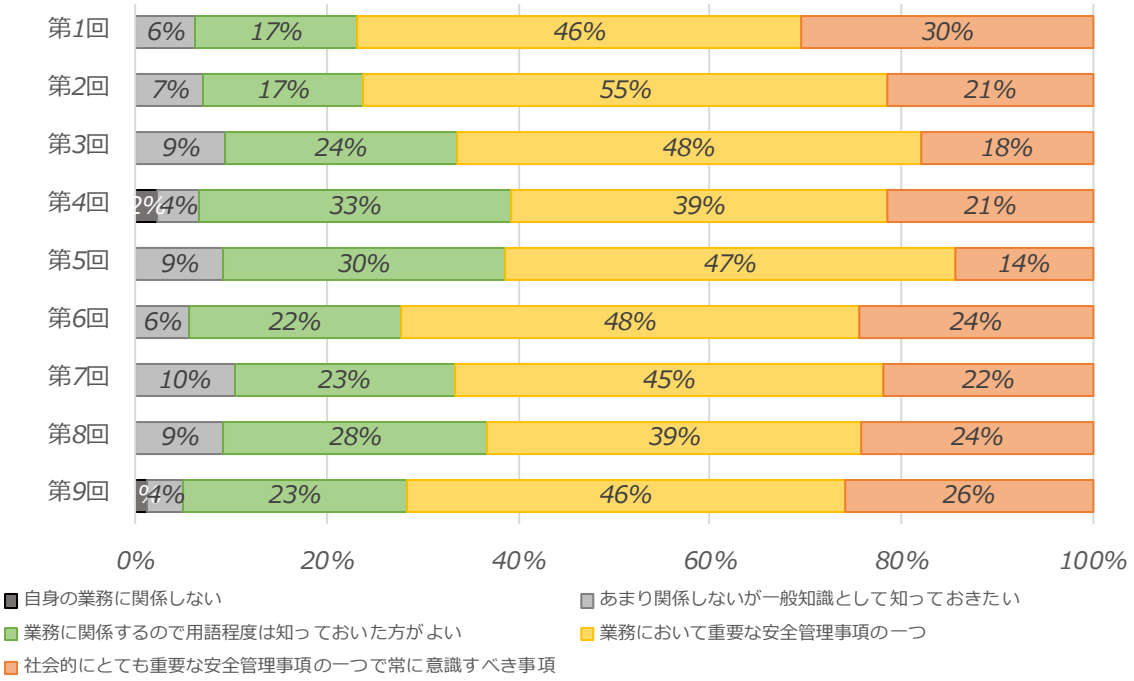


図 4.2　意識評価

（3）講義への主な意見

教育受講者から得られた主な意見や感想を以下に示す。

回/タイトル	主な意見・感想
第 1 回/サイバー攻撃の現状	・文章と図、それぞれで説明されており、理解しやすい。 ・事例も鉄道に関するものをあげていただき、理解しやすかった。 ・IT 用語を少し「こんなもの」というのを言っていただければよかった。
第 2 回/サイバー攻撃の手法と脆弱性	・情報セキュリティの教育担当でもあり、今回の内容は自分にとって、再勉強のつもりで学習することができた。 ・最後に実例を聞けて、よりセキュリティの重要性を理解できた。 ・監視（管理）の重要性を社内で再度周知したい。
第 3 回/サイバーセキュリティ基礎	・初めて聞く言葉も多く、少し難しく感じたが、重要な内容だと思うので覚えておきたい。 ・自社でも数年前から点検・評価をシステム単位で行っているため、勉強になった。 ・リスク評価は少々わかりにくかった。
第 4 回/ネットワーク基礎	・基礎を受講する前に、ある程度の用語、内容は知っておくと良いと思った。 ・実際の事例を交えての説明が多かったので、内容がスッと入ってきた。自社の教育や説明の参考にしたい。 ・ネットワーク管理の仕事ではないので、普段の仕事に結びつかない。基礎がないため理解ができない。
第 5 回/セキュリティ技術	・とてもわかりやすかった。業務に活かしたい。 ・対策技術の用語と概要について、細かく説明されたが、他と比べて内容が多く感じた。
第 6 回/サイバー攻撃対策	・わかりやすい内容であった。 ・分からない部分もあったが、資料にキーワードがあり、自己学習でカバーできそう。
第 7 回/サプライチェーンのセキュリティ対策	・CSIRT 担当として普段の事務を行っているため、とても参考になった。
第 8 回/インシデント対応	・サイバー攻撃と通常の故障の判断が難しく苦慮している。また、CSIRT の役割についても社内で理解を得にくい状況である。具体的な事例の紹介があると、もっと理解度が上がると思った。
第 9 回/学習の振り返り	・グループディスカッションは同じ業種の方とあたったので、参考になる話を聞けた。

４．３．３．アンケート結果（航空分野）

（１）理解度評価

各講座に対する受講者の理解度について、アンケートを実施した。

アンケートの結果より、各回で「十分に理解できた」「大体は理解できた」が約 90%を占めており、概ねサイバーセキュリティ対策の基礎については理解がされたものと推察できる。ただし、第 3 回「サイバーセキュリティ基礎」は他の回に比べて、「十分理解できた」「大体は理解できた」の回答割合が少なく、鉄道分野の教育後アンケートにおいても、第 3 回は同様に理解できた割合が低かったことから、リスクマネジメントやリスク評価、重要度の判断などについて、分かってはいても体系的に理解するのか難しいことが推察される。

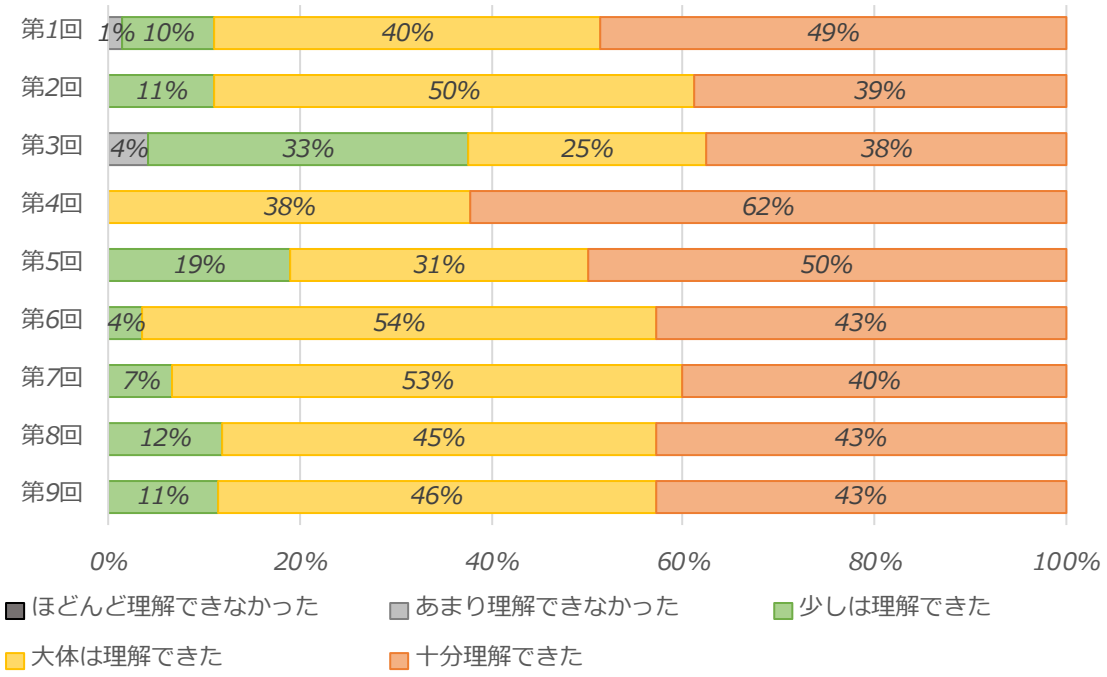


図 4.3　理解度評価

（２）意識評価

各講座に対する受講者の意識について、アンケートを実施した。

アンケートの結果より、各回で「社会において重要な安全管理事項」「業務において重要な安全管理事項」が 80～90%を占めており、自社のみならず、社会的にサイバーセキュリティ対策を重要と考えていることがうかがえる。特に航空分野においては IT 化が進み、外部との接続も多くなっていることが想定されるため、重要インフラ事業者として、意識が高くなっているものと推察される。

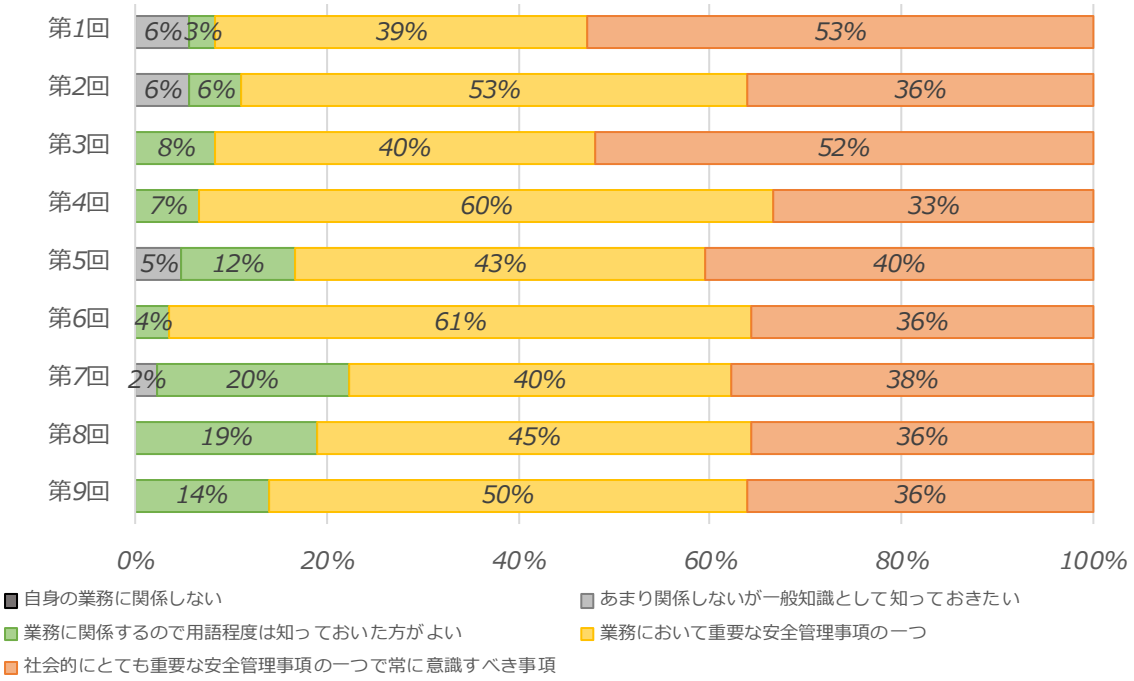


図 4.4　意識評価

（3）講義への主な意見

各講座に対する受講者の意識について、アンケートを実施した。

回/タイトル	主な意見・感想
第 1 回/サイバー攻撃の現状	・非常にわかりやすい講義で、部に共有すべきことについて得られた知識が多く助かった。 ・50 代～役員は、説明しても理解してもらえない。この年代へ分かるように説明できる例などあれば次回講座などで聞きたい。
第 2 回/サイバー攻撃の手法と脆弱性	・攻撃に対し、どういう対策が必要か理解できた。 ・考え方として非常に役立つ話であった。部内で展開したい。
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マネジメントについて体系的に理解できた。クラウドセキュリティも最近よくトピックとして取り上げられるため、非常に参考になった。 ・話が区切りなく続くので、ポイントを自分で作るのが難しかった。アウトプットする機会が欲しい。
第 4 回/ネットワーク基礎	・わかりやすい表現がされていて、理解しやすい。
第 5 回/セキュリティ技術	・講義の時間に対してテキストの情報量が多いと感じた。そのため、技術的な話が省略されていたように感じた。 ・インシデント発生時に、どのように企業が対応したのか、すべきであるのか、事例を交えて説明いただけると助かる。
第 6 回/サイバー攻撃対策	・なし
第 7 回/サプライチェーンのセキュリティ対策	・契約担当であるが、とても参考になった。 ・とてもわかりやすい講義であった。
第 8 回/インシデント対応	・資料に実例を多く取り入れてほしい。
第 9 回/学習の振り返り	・サイバーセキュリティについて基礎から体系的に学ぶことができる有意義な機会であった。

第５章　総括

５．１．本研究の総括

経営者がサイバーセキュリティ対策について指示を出す際に重要となる事項を検討し、経営層がとるべきサイバーセキュリティの具体的施策として１０項目に取りまとめた。

施策１　サイバーセキュリティリスクの重要性について経営会議において情報を分析する。
施策２　サイバーセキュリティリスクに関する検討組織を設置する。
施策３　危機管理を統括する既存部門と CSIRT の連携を強化する。
施策４　PDCA サイクルを実施する組織からリスク対応について定期的な報告を受ける。
施策５　経営層として情報共有に努める。
施策６　危機管理コミュニケーション力を高める。
施策７　有事に備えた現場担当者教育を強化する。
施策８　監査機能を積極活用する。
施策９　サイバーセキュリティリスクへの取り組みについて積極的な情報開示に努める。
施策１０　自社のセキュリティ水準の将来目標を定め目標達成や進捗状況を管理する。

これらの施策のうち、オリパラまでに実施することが望まれる対策は以下のとおり。
施策１　重大なサイバーセキュリティリスクについて、大会前の経営会議において分析結果を再確認する。
施策４　PDCA サイクルを実施する組織から、大会前のリスク対応の状況について報告を受け、現状を確認する。
施策５　経営層として積極的にオリパラ関係の情報収集と情報共有に努める。
施策６　オリパラに特化した危機管理コミュニケーションの実施方法について検討する。
施策７　重大なサイバーセキュリティリスクへの対応について、現場担当者に向けた注意喚起を指示する。

取締役と監査役を対象とした啓発セミナーを実施した。

エキスパート人材の育成教育を実施した。

サイバーセキュリティに関する最新情報等に関するセミナーを実施した。

机上演習を実施した。サイバー脅威主体について、現状の状況前提について講師より説明した後に、シナリオに基づきグループディスカッションを実施した。

５．２．サイバーセキュリティ対策に関する提言

（１）東京五輪を見据えた対策

2020 年東京五輪大会を控え、組織委員会や各省庁、重要インフラ事業者はサイバー領域を含む様々な観点でセキュリティ対策の強化を図っている。現在の社会情勢を勘案すると、2020 年東京五輪大会は平昌冬季オリンピックよりも政治的側面が強く、サイバー攻撃リスクの高い大会となると予想される。特に、改善の兆しが見られない日韓関係は、サイバー領域においても影響を与えることは想像に難くない。加えて、過去事例に鑑みると、北朝鮮やロシアからのサイバー攻撃、さらに日本固有の問題として、反捕鯨国による日本バッシングに便乗したサイバー攻撃も考えられる。

昨今の急速な技術革新（IOT、５G、クラウド)、経営の合理化による脅威の増大（サプライチェーン、システムの IT 化)、執務環境の変化（在宅勤務によるセキュリティの脅威)、攻撃の高度化（ファイルレス攻撃)、攻撃者の多様化（国家、ダークウェブによる裾野の広がり）などの脅威の高まりも踏まえると、2020 年東京五輪大会におけるサイバー攻撃については、過去のサイバー攻撃事案の関係組織や時代の潮流を踏まえた上で対策を講ずる必要がある。このため、関係事業者は早期にこれらの事案発生時の対応手順等を検討する必要がある。過去のオリンピック・パラリンピックの際に発生したサイバー攻撃が特定国の公的組織が関与していたことに鑑みると、関係事業者はこの脅威の変化を重く受け止めるべきである。我が国のライフラインを担う交通分野の事業者は、サイバーセキュリティを広義に捉え、物理及びサイバーの両面から統合的に対策強化に努めなければならない。

本調査研究は、2015 年からサイバー攻撃対策をテーマとし、初年度におけるリスク分析の結果を踏まえてサイバーセキュリティの課題を把握し、経営層への啓蒙と技術者層の育成を目的として活動した。2020 年東京五輪大会における対策の一環として、サイバーセキュリティ対策の手引書作成、人材育成のためのカリキュラムと教育用コンテンツの作成、机上演習を含む人材育成の実施、等を実施してきた。2020 年東京五輪大会まで残り数か月の現状で、交通分野の事業者が優先的に取り組むべき対策は、物理及びサイバーの両面での復旧・回復能力の強化と継続的な脅威分析である。目まぐるしく変化する社会的背景を勘案すると、2020 年東京五輪大会は最悪の事態を踏まえたリスクシナリオを想定しておくことが望まれる。現状までの脅威分析に基づき、東京五輪大会における自社に固有のリスクを勘案し、手引書における対策の優先順位を定めるとともに、現場担当者を含む広範な社内人材に対して、重要なリスクへの注意喚起や初動対応の周知徹底、等の人的対策を実施することが望まれる。2018 年の平昌冬季オリンピックの際は、「Olympic Destroyer（オリンピックデストロイヤー)」という標的型のマルウエア（悪意あるソフト）の攻撃を受け、ウェブサイトやプレスセンターなどのシステムに障害が起きた。関連組織へのサイバー攻撃は、少なくとも 12 か月前にはが発生していたことが、当時のセキュリティ対策担当企業から報告されている。この事実を加味すると、事案は既に発生しているものと捉えることが重要であり、復旧・回復能力の強化が望まれる。

（２）東京五輪以降を見据えた対策

急速な技術革新、経営の合理化による脅威の増大、執務環境の変化、攻撃の高度化、攻撃者の多様化などの脅威の高まりも踏まえると、2019 年は、各国のサイバー攻撃対策が大きく変遷

するきっかけとなった年である。そのひとつは、中国、ロシア、イラン、北朝鮮が EMP（電磁パルス）攻撃の兵器を完成させていることが明らかとなり、各国で EMP 攻撃を含むサイバーセキュリティ対策が急務となっていることが報じられたことである。この EMP 攻撃対策とサイバー攻撃対策の統合は日本政府も同様の方針であり、極めて重要な認識の変化といえる。また、この例が示すように、今日におけるサイバーセキュリティ攻撃は国家レベルとなっていることから、国際的な連携・枠組みの下、安全保障の観点で国が率先して対策を主導することが望まれる。

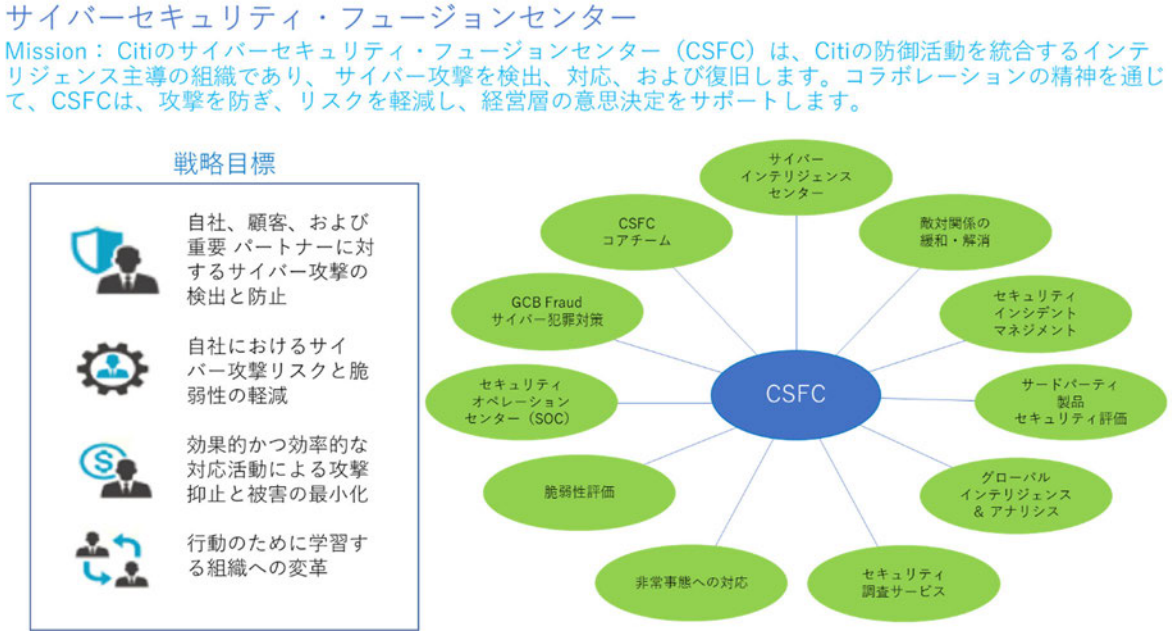
米国が作成したリスクシナリオによれば、東京は北朝鮮の EMP 攻撃及びサイバー攻撃の標的の一つとなっている。また、米国の公共機関への注意喚起からも推察できるように、今日におけるサイバーセキュリティは、サプライチェーンを含めた複雑なものとなっている。さらには、昨今の IoT、５G、クラウドサービスの利用等、新技術の導入に伴うサイバーセキュリティリスクの増大や脅威の深刻化に対する注意喚起の報告例は、枚挙にいとまがない。一方で、国民生活及び社会経済活動の基盤となる鉄道分野・航空分野においては、近い将来、物理及びサイバー領域リスクを統合的に管理することが望まれている。このような状況下、個別企業が単独でサイバーセキュリティ対策を講ずることの限界が露呈しつつある。

物理及びサイバー領域を統合したリスク管理の実現を図り、一層の事業継続の強化を推進するために、セキュリティ・フュージョンセンターなどの設立がある。フュージョンセンター[61]とは、事業被害を招く可能性のあるすべての脅威関連情報を収集、分析、整理、共有するための運営センターのことである。セキュリティ・フュージョンセンターは、企業レベル、業界レベル、国家レベル、等の様々な規模において設立可能な組織である。サイバー攻撃が国家レベルとなっている現状を鑑みると、セキュリティ・フュージョンセンターは国家レベルで運営されることが望まれるが、重要インフラ事業者においては、国家基盤を守るための組織要素として、企業レベルあるいは業界レベルのセキュリティ・フュージョンセンター構築に向けた準備を進めることが求められる。

企業レベルの一例として、米国 Citi グループにおけるサイバーセキュリティ・フュージョンセンターの例[62]を以下に示す。

[61] https://www.dhs.gov/fusion-centers

[62]https://www.citibank.com/tts/insights/eSource_academy/docs/emea_compliance_summit_2017/Cybersecurity.pdf



（引用資料の邦語訳）

物理及びサイバー領域を統合したリスク管理の実現には、攻撃手法に関する技術論だけでなく、政治・社会情勢、各国の攻撃能力やサイバー領域における活動状況等の情報も併せた統合分析力に基づく脅威インテリジェンスの活用が求められる。近年、米国などの先進国においては、セキュリティ・フュージョンセンターのような、脅威インテリジェンスを基として対策検討を行う組織体制の構築が進められている。このようなセンターに必要となるのは、知識だけでなく、脅威インテリジェンスの作成やインテリジェンスの分析能力、実務経験等を有し、戦略的判断のできるセキュリティ人材である。現在、我が国においては、そのような人材の育成が課題となっており、脅威インテリジェンスを活用できる人材を有する組織は非常に少ない。世界における脅威動向を加味すると、我が国においては、技術論だけでなく物理や周辺国動向、社会的側面等を含む他要素を統合分析のできるセキュリティ人材の育成が急務である。

５．３．鉄道分野

欧州の鉄道分野における取り組みとしては、2012 年から 2015 年にかけて実施された SECRET プロジェクト[6364]と 2016 年から 2018 年にかけて実施された CYRAIL プロジェクト[6566]が挙げられる。SECRET(SECurity of Railways against Electromagnetic aTtacks)プロジェクトでは、電子伝送を妨害したり、電子システムを損傷する可能性のある EMP（電磁パルス）攻撃に関する脅威シナリオを作成し、これに基づく防止策及び復旧ソリューションを調査レポートとして取りまとめている。CYRAIL(CYbersecurity in the RAILway sector)プロジェクトでは、鉄道の信号及び通信システムを対象に、運用シナリオ、セキュリティ評価、脅威分析、攻撃検出、早期警告、緩和と対策、保護プロファイルなど、鉄道のサイバーセキュリティ評価に関する推奨事項をまとめ報告している。これらプロジェクトの背景には、国境を越えても相互運用可能で、ヨーロッパ全体で共通に使用できる信号保安システム ERTMS(European Rail Traffic Management System)の構築と、ERTMS の中で GSM(Global System for Mobile communications)に由来する無線技術ならびに TCP/IP 技術が普及していることにより、サイバー攻撃の脅威が現実味を帯びてきたことが挙げられる。

国際鉄道連合(International Union of Railways)[67]では、2018 年 6 月に発行した Guidelines for Cyber-Security in Railways の中で、鉄道のサイバーセキュリティは、新しいセキュリティリスクを想定しなければならないと述べている。具体的には、インターロック（連動）システム、自動列車保安(ATP：Autometic Train Protecter)、自動列車運行管理(ATS：Autometic Train Superrision)、自動列車運転(ATO：Autometic Train Operation)、SCADA（産業監視制御システム：Supervisory Control And Data Acquisition)、換気、遠隔監視、鉄道の管理システム、通信など、幅広い対象に範囲が及ぶこと、これに加えて信号システムに関しては、IP ネットワークなどの IT システムの積極的な取り込みが行われていることが挙げられる。特に、信号システムでの IP ネットワークなどの IT システムの積極的な取り込みは、汎用プロトコルや機器を使用することによる仕様面でのオープン化が進むことを、さらに、接続の拡張によってもたらされる国を越えた分散ネットワークは接続ポイントを多数提供することになるため、接続面でのオープン化が進むことを指摘している。

欧州の事例をみると、今後の鉄道システムの方向性は、IT システムの取り込みによって、接続面、仕様面ともにオープン化に向かっていることを示唆している。鉄道システムにおける接続面でのオープン化は外部から侵入される可能性、仕様面でのオープン化は侵入されてから被害の拡大につながる可能性を示しており、サイバーセキュリティ対策が必要不可欠となる。

５．４．航空分野

航空分野におけるセキュリティは、航空機に導入される技術の高度化や空港ターミナルの

[63] https://secret-project.eu
[64] https://secret-project.eu/Public-Deliverables-16
[65] https://cyrail.eu/about-cyrail-project-1
[66] https://cyrail.eu/IMG/pdf/final_recommendations_cyrail.pdf
[67] https://uic.org

IoT、５Ｇなどの IT 技術の導入に伴い、サイバー攻撃のリスクが増大している。近年では、2016 年に、ベトナム航空がサイバー攻撃[68]を受け、ウェブサイトの改ざん、顧客情報の漏えい（約 41 万件）、空港ターミナル内のサウンドシステムの乗っ取り、チェックインカウンターの障害と大規模な被害を受けた。2018 年には、キャセイパシフィック航空が顧客情報の漏えい（最大 940 万件）を発表[69]し、航空分野が永続的なサイバー攻撃の対象であることが明らかとなった。2019 年には、エアバス社がサイバー攻撃を受けたことを公表[70]する中で特定国からの攻撃を示唆し、クリーブランド・ホプキンス国際空港ではランサムウェアの感染被害に遭ったことが報じられている[71]。

航空分野の特徴は、航空機の運航において、航空機の製造会社、運航会社、空港ターミナルが密接に連携している点にある。そして、あらゆるリスクが物理面とサイバー面の両面に影響することは容易に想像のつくものである。特に、近年の航空分野におけるサイバー攻撃のインシデントは、僅かなセキュリティ対策の見落としから侵害を受けていることから、各社の早急なセキュリティ対策強化と関係主体の連携が重要となる。

こうしたことから近年、米国[72]や英国[73]、日本[74]などにおいて、サイバーセキュリティの対策強化の指針を打ち出している。これらの多くは、個別企業の対応だけではなく、顧客やサプライチェーン（サプライヤ、委託先等）のリスクを含めてのものとなっており、より広範なセキュリティ管理体制が求められている。

サフラン社や General Electric 社の事案[75]で発覚したように、従業員などによる内部不正を絡めたサイバー攻撃も十分に予想できることから、セキュリティ強化の対象範囲としてエアギャップ（隔離されたネットワークにおける不正対策）が含まれることは論をまたない。日本では、2019 年８月に電気通信設備の保守業務受託者がサイバー攻撃による被害を報告[76]しており、同様の内部犯行によるリスクシナリオを想定しておくことが必要である。

現在までに報告されているインシデントの実態に鑑みると、航空分野におけるセキュリティ対策は、政府等の対策ガイドラインを基盤として業界全体での連携を強化することが強く望まれる。これは、サイバー領域だけに限らず、物理面におけるセキュリティ対策も含めることが望ましいと考えられる。

---

[68] https://e.vnexpress.net/news/news/cyber-terrorists-attack-flight-info-screens-at-vietnam-s-2-major-airports-3444504.html

[69] https://www.pcpd.org.hk/english/news_events/media_statements/files/PCPD_Investigation_Report_R19_15281_E.pdf

[70] https://www.airbus.com/content/dam/corporate-topics/publications/press-release/EN-Airbus-Cyber-Security-Statement.pdf

[71] https://www.cbsnews.com/news/cleveland-hopkins-international-airport-computer-systems-malware-attack-hack-fbi-investigating/

[72] https://www.tsa.gov/sites/default/files/2017_ga_security_guidelines.pdf

[73] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/726561/aviation-cyber-security-strategy.pdf

[74] http://www.mlit.go.jp/common/001283895.pdf

[75] https://www.crowdstrike.com/resources/wp-content/brochures/reports/huge-fan-of-your-work-intelligence-report.pdf

[76] https://www.kkr.mlit.go.jp/news/top/press/2019/20190820-1.html

おわりに

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

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

運輸総合研究所では、平成 27 年度からの 2 年間で「東京オリンピック・パラリンピックに向けた交通機関へのサイバーテロ対策に関する調査研究」が実施され、交通事業のセキュリティリスク分析を踏まえ、国内外の対策ガイドラインなどの整理、及び、それらに基づいて、我が国に適応した鉄道分野と航空分野の対策手引きの作成を行った。

平成 29 年度は、作成した対策手引きを実践する人材を育成することを目指し、必要となる人材像や育成対象者の検討、学習内容の定義、国内外の人材育成カリキュラムの事例収集、机上演習の実施、及び、それらに基づいて、我が国に適応した鉄道分野と航空分野の人材育成カリキュラムの作成を行い、昨年度は作成した人材育成カリキュラムを実行する上での教材の具体化を目指し、机上演習の実施、及び、鉄道分野と航空分野の教育用教材作成とそれを用いた教育の試行を行った。

本年度は、昨年度に引き続き教材を用いた教育や机上演習を実施するとともに、最新情報提供セミナーも実施し、エキスパート人材の育成を行った。また経営層をターゲットに、サイバーセキュリティについて経営層がとるべき施策を検討し、10 の施策を取りまとめ、監査役・経営層セミナーにて周知を図るとともに、引き続き経営層の意識向上に努めた。

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。

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。

令和 2 年 3 月

「交通分野へのサイバー攻撃に対するセキュリティ人材育成等に関する調査研究」
検討委員会　委員長
田中　英彦

参考資料

1) 重要インフラ分野における情報セキュリティ確保に係る安全基準等策定指針（第5版)、サイバーセキュリティ戦略本部、令和元年5月23日改訂
2) 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4版、国土交通省、平成31年3月29日改訂
3) 航空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5版、国土交通省、平成31年3月29日改訂
4) 空港分野における情報セキュリティ確保に係る安全ガイドライン第2版、国土交通省、平成31年3月29日制定
5) サイバーセキュリティ2019、サイバーセキュリティ戦略本部、令和元年5月23日
6) 重要インフラの情報セキュリティ対策に係る第４次行動計画、サイバーセキュリティ戦略本部、平成30年7月25日改訂、
7) 運輸事業者における安全管理の進め方に関するガイドライン ～輸送の安全性の更なる向上に向けて～、国土交通省大臣官房　運輸安全監理官、平成29年7月改訂
8) サイバーセキュリティ経営ガイドラインVer2.0、経済産業省　独立行政法人情報処理推進機構、平成29年11月16日
9) サイバーセキュリティ経営ガイドラインVer2.0実践のための経営プラクティス集、独立行政法人情報処理推進機構、平成31年3月25日改訂
10) 第4回 産業サイバーセキュリティ研究会 ワーキンググループ2（経営・人材・国際)、資料３ 事務局説明資料、経済産業省商務情報政策局サイバーセキュリティ課、2019年3月29日
11) 第２回 産業サイバーセキュリティ研究会、資料３ 産業サイバーセキュリティ強化へ向けたアクションプラン、経済産業省商務情報政策局、平成30年5月30日
12) グループ・ガバナンス・システムに関する実務指針、経済産業省、2019年6月28日策定
13) サイバーセキュリティ対策情報開示の手引き、総務省　サイバーセキュリティ統括官、令和元年6月
14) 民間企業におけるセキュリティ対策に関する情報開示の現状について、総務省　サイバーセキュリティタスクフォース　情報開示分科会、平成29年12月
15) 改訂コーポレートガバナンス・コードと経営課題への対応、2018年9月、KPMGジャパン
16) グループ・ガバナンス・システムに関する実務指針、経済産業省、2019年6月28日策定
17) コーポレートガバナンス・コード、株式会社東京証券取引所、2018年6月1日
18) 産業横断サイバーセキュリティ人材育成検討会　第二期最終報告書、一般社団法人サイバーリスク情報センター 産業横断サイバーセキュリティ人材育成検討会、2018年11月21日
19) ユーザ企業のためのセキュリティ統括室　構築・運用キットPart2【統括室編】、産業横断サイバーセキュリティ人材育成検討会　人材育成WG、2018年11月21日

20) 法人組織におけるセキュリティ実態調査 2019 年版、トレンドマイクロ株式会社、
21) システム管理基準、経済産業省、2018 年改訂
22) 監査役監査チェックリスト④【上場会社編】、公益社団法人日本監査役協会中部支部、2019 年 1 月 11 日
23) 重要インフラのサイバーセキュリティを改善するためのフレームワーク、独立行政法人情報処理推進機構による翻訳文書、2019 年 1 月掲載
24) 制御システムのセキュリティリスク分析ガイド　第２版、独立行政法人情報処理推進機構、2018 年 10 月
25) 米国における電力インフラと IT をめぐる動向、独立行政法人情報処理推進機構、ニューヨークだより 2016 年 6 月号
26) 企業の CISO や CSIRT に関する実態調査２０１６-調査報告書-、独立行政法人情報処理推進機構、2016 年 5 月 10 日
27) 取締役会の機能向上等に関するコーポレートガバナンス実態調査報告書、有限責任監査法人トーマツ、平成 29 年 3 月
28) 諸外国におけるサイバーセキュリティの情報共有に関する調査、一般社団法人 日本サイバーセキュリティ・イノベーション委員会、2018 年 3 月 9 日
29) 電力分野におけるサイバーセキュリティ対策と「産業サイバーセキュリティ研究会 電力 SWG」での検討状況、経済産業省 産業保安グループ 電力安全課、2019 年 3 月 15 日
30) 重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書（第 1 版）、サイバーセキュリティ戦略本部 重要インフラ専門調査会、令和元年 5 月 23 日改定

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) 「危機管理コミュニケーション」とは、非常事態の発生によって企業が危機的状況に直面した場合に、その被害を最小限に抑えるために行う、情報開示を基本としたコミュニケーション活動のことである。

(2) 「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。

(3) 「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。

(4) 「経営会議」とは、取締役会、等の経営層による意思決定の場を総称する。

(5) 「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。

(6) 「コンティンジェンシープラン」とは、重要インフラの情報セキュリティ対策に係る第４次行動計画によると、重要インフラ事業者等が重要インフラサービス障害の発生又はそのおそれがあることを認識した後に経営層や職員等が行うべき初動対応（緊急時対応）に関する方針、手順、態勢等をあらかじめ実行面から具体的に定めたものをいい、これに基づいて適切な対応を行うことにより重要インフラサービス障害による影響を最小限に抑えることを目的とする。

(7) 「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。

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

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

(10) 「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。

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

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

(13)「脆弱性」とは、ソフトウェアやアプリケーション等において、システムへの不正アクセスやマルウェア等の攻撃により、その機能や性能を損なう原因となり得るセキュリティ上の問題箇所をいう。
(14)「セキュリティインシデント」とは、意図的なサイバー攻撃により、鉄道運行の遅延、運休、及び鉄道の安全輸送に対する支障等の影響を及ぼす、又はその恐れのあるシステムの不具合が発生した事象をいう。
(15)「フォレンジック」とは、セキュリティインシデントや法的紛争・訴訟に際し、電磁的記録の証拠保全及び調査・分析、及び電磁的記録の改ざん・毀損等についての分析・情報収集等を行う調査手法・技術をいう。
(16)「不正侵入」とは、通信回線・ネットワークを通じてコンピュータに接触し、本来の権限では認められていない操作を行ったり、本来触れることの許されていない情報の取得や改ざん、消去等を行ったりすることをいう。
(17)「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。
(18)「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。
(19)「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。
(20)「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。
(21)「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。
(22)「CSIRT」とは、Computer Security Incident Response Team の略で、セキュリティインシデント等サイバーセキュリティに関するトラブルに対処するための体制をいう。
(23)「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。

セミナー資料

１．航空分野のサイバーセキュリティに関する最新情報提供セミナー…… 97

２．セキュリティインシデントから学べること
～鉄道分野に関連するインシデント事例～ …… 119

３．2020 年サイバーテロの可能性と経営としての監査役の役割 …… 155

４．サイバーセキュリティの監査 …… 173

５．企業と経営層の法的責任の問題…… 189

６．緊急事態の対処能力の向上策に類似する「サイバー攻撃対処態勢の整備」…… 203

７．「交通分野へのサイバー攻撃に対するセキュリティ人材育成に関する調査研究」
経営層がとるべきサイバーセキュリティ対策について …… 223



1 航空分野へのサイバー攻撃

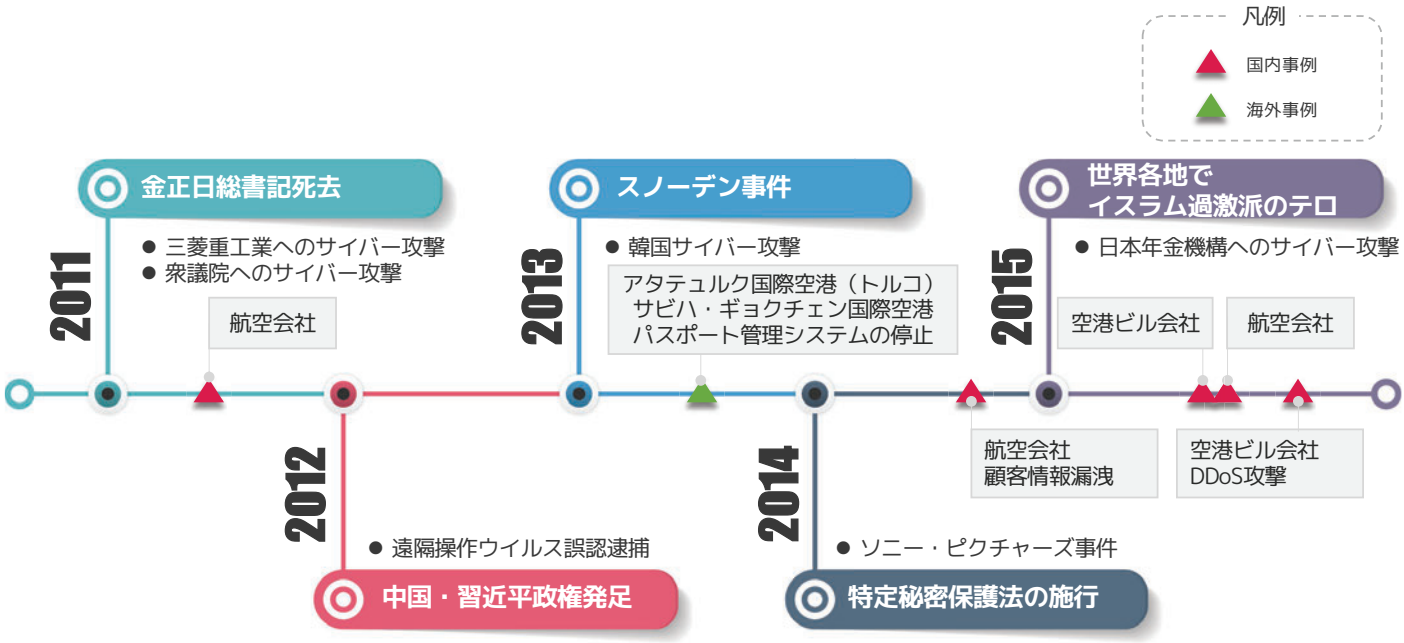
サイバー攻撃事案の実態解明

SIGNT
JAPAN INTELLIGENCE

© 2019 SIGNT JAPAN

THREAT HUNTING AND INTELLIGENCE

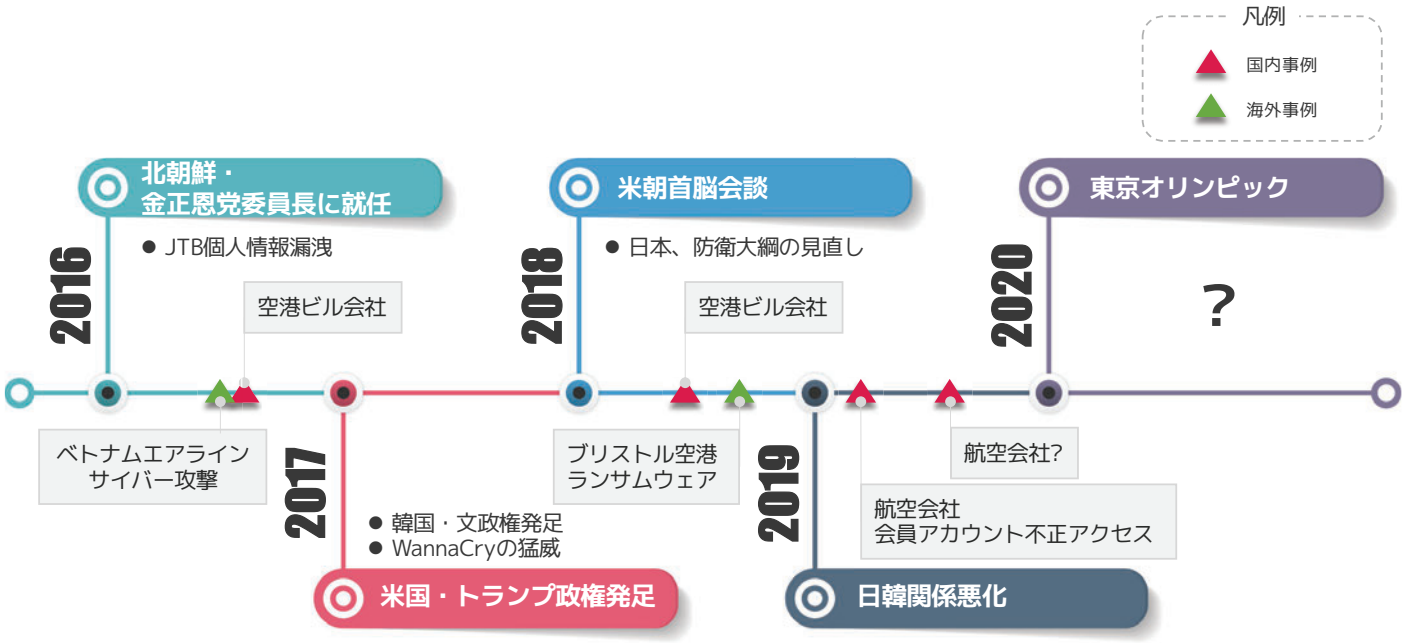
（2015年以前）航空業界におけるサイバー攻撃例



© 2019 SIGHNT, INC

THREAT HUNTING AND INTELLIGENCE

航空業界におけるサイバー攻撃例（2016年以降）

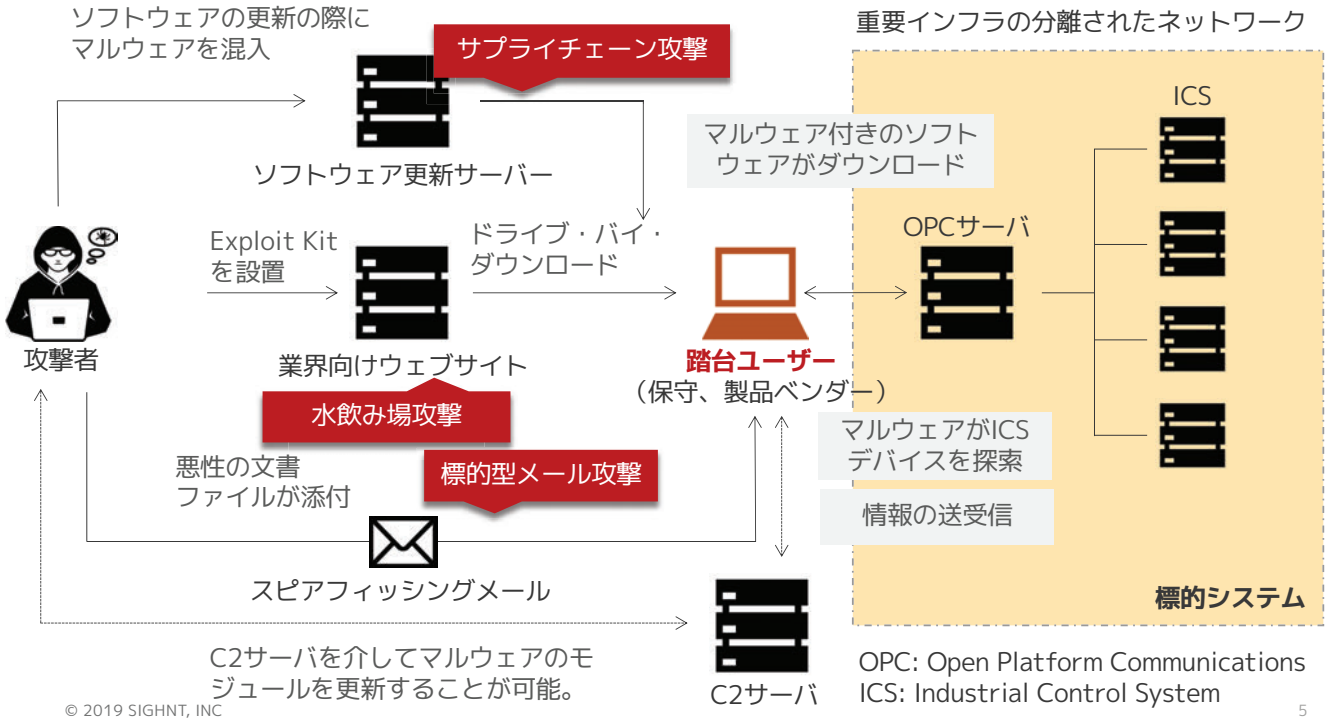


© 2019 SIGHNT, INC

「サイバー攻撃」の事例からみる全体像

THREAT HUNTING AND INTELLIGENCE

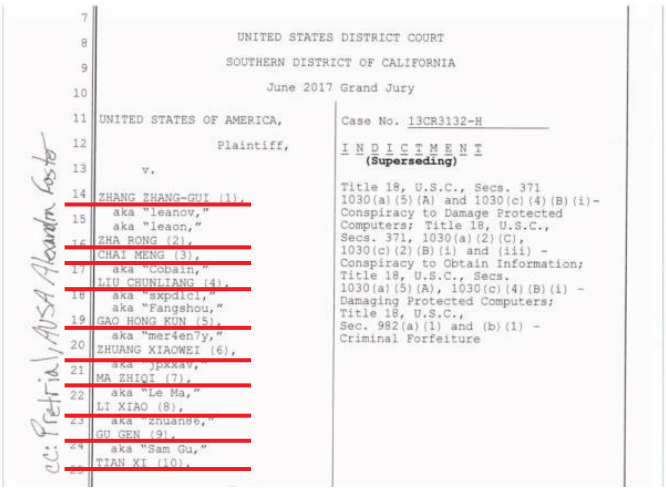
（ロシア）重要インフラを狙ったサイバー攻撃事例



© 2019 SIGHNT, INC

（中国）航空機技術を狙ったサイバー攻撃

2018年10月にMSS JSSD（江蘇省国家安全部）の徐彦君（XU Yanjun）がベルギーで身柄を拘束され、米国に引き渡されました。容疑は、GEアビエーションを含む複数の航空宇宙関連企業の機密情報の窃盗です。その際、サイバー攻撃担当を含め、10名の中国人関係者が起訴されました。その全体像は、サイバーとインサイダーの担当チームが連携した攻撃であったことが明らかとなりました。



UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF CALIFORNIA

June 2017 Grand Jury

UNITED STATES OF AMERICA,

Plaintiff,

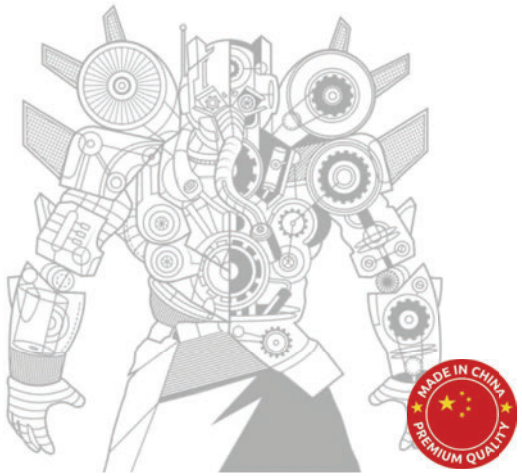
v.

ZHANG ZHANG-GUI (1),
aka "leanov,"
aka "leaon,"
ZHA RONG (2),
CHAI MENG (3),
aka "Cobain,"
LIU CHUNLIANG (4),
aka "sxpdlcl,"
aka "Fangshou,"
GAO HONG KUN (5),
aka "mer4en7y,"
ZHUANG XIAOWEI (6),
aka "jpxxav,"
MA ZHIQI (7),
aka "Le Ma,"
LI XIAO (8),
aka "zhuane6,"
GU GEN (9),
aka "Sam Gu,"
TIAN XI (10),

Case No. 13CR3132-H

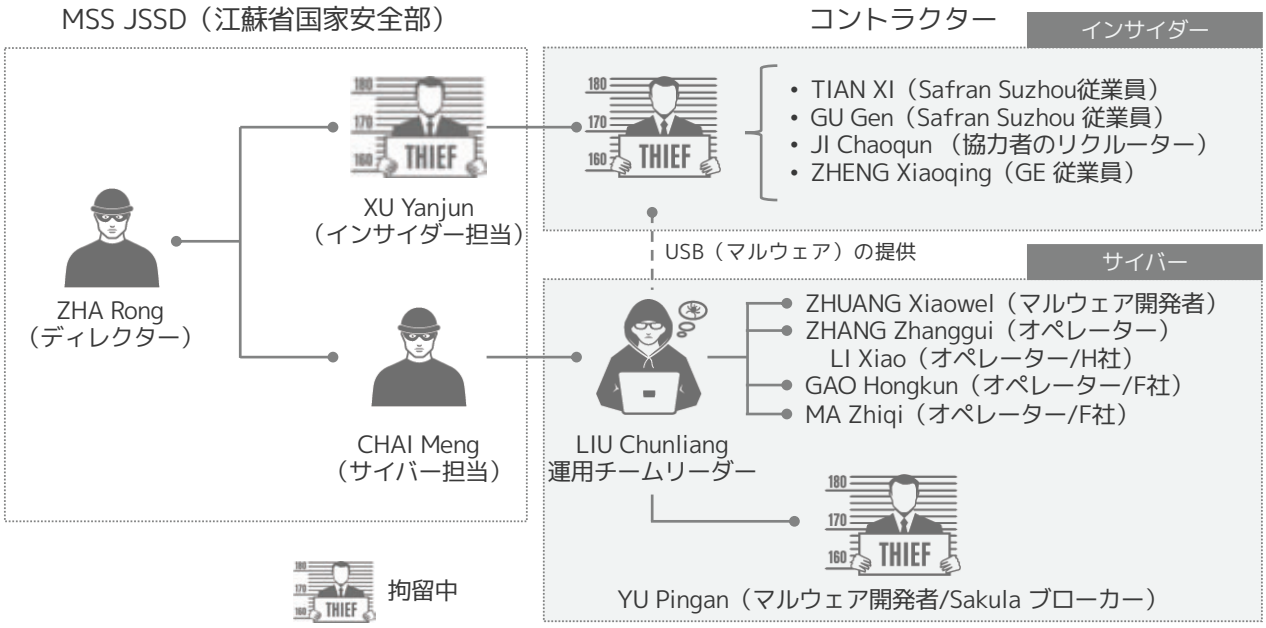
INDICTMENT
(Superseding)

Title 18, U.S.C., Secs. 371 1030(a)(5)(A) and 1030(c)(4)(B)(i)- Conspiracy to Damage Protected Computers; Title 18, U.S.C., Secs. 371, 1030(a)(2)(C), 1030(c)(2)(B)(i) and (iii) - Conspiracy to Obtain Information; Title 18, U.S.C., Secs. 1030(a)(5)(A), 1030(c)(4)(B)(i) - Damaging Protected Computers; Title 18, U.S.C., Sec. 982(a)(1) and (b)(1) - Criminal Forfeiture



© 2019 SIGHNT, INC

（中国）航空機技術を狙ったサイバー攻撃



© 2019 SIGHNT, INC

（中国）DNSハイジャッキング

173.252.252.204 のドメイン履歴

Show : 25 ◂ 1-25 of 43 ▸ Sort : First Seen Ascending ▾ Download Copy

Resolve	First	Last	Source	Tags
fab7a.com	2010-11-29	2011-06-01	riskiq	
www.louisvuitton-rabatt.biz	2012-04-22	2013-02-09	riskiq	
www.qxgxxq.com	2013-07-16	2013-07-16	riskiq	
icbctjr.com	2013-11-03	2013-11-03	riskiq	
secure.safran-group.com	2013-11-23	2014-02-08	riskiq	
ameteksen.com	2013-12-06	2014-02-16	emerging_threats, riskiq, virustotal	
oa.ameteksen.com	2013-12-06	2013-12-06	virustotal	

Safran Suzhou のドメイン

- 173.252.252.204 は、Sakulaマルウェアの攻撃用サーバ
- Safran SuzhouのDNSサーバは、2013/11/23～2014/02/08の期間に乗っ取られていた可能性が高い。

© 2019 SIGHNT, INC

（2016）ベトナム航空の事案

報道によれば、ベトナム航空は、2016年の南シナ海の領海に関する国際司法の判決を不服とし、中国のハクティビスト（社会的な主義主張を行うハッカー）である「1937CN」によりサイバー攻撃を受けました。ウェブ改竄、旅客情報の窃取、館内放送の乗っ取りの被害を受けています。

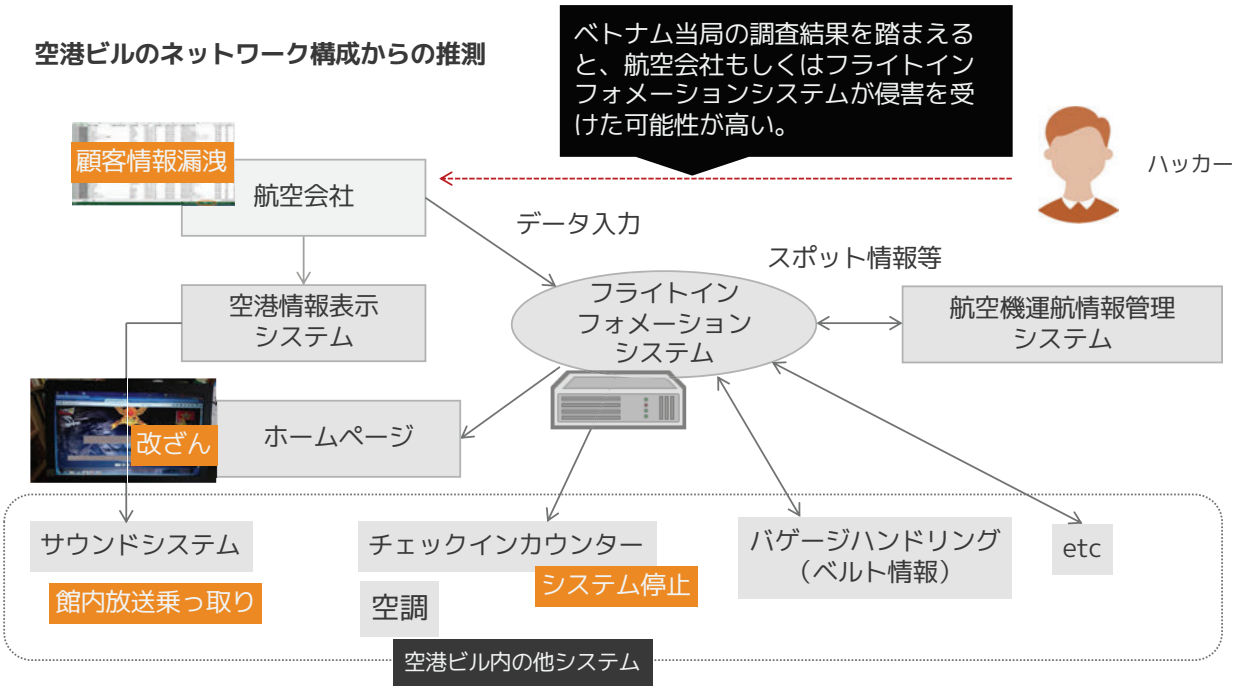




© 2019 SIGHNT, INC

（2016）ベトナム航空の事案

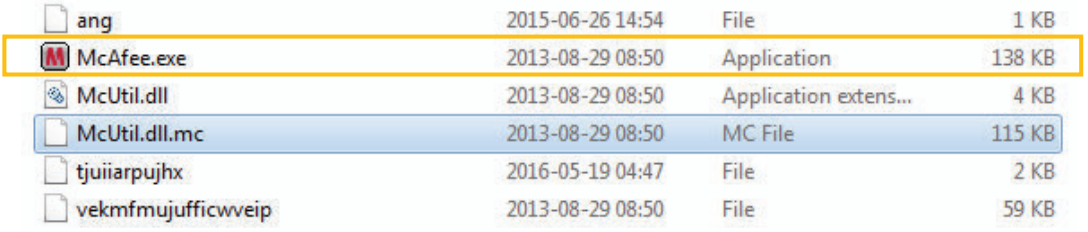
空港ビルのネットワーク構成からの推測



© 2019 SIGHNT, INC

（2016）ベトナム航空の事案

マカフィー社のソフトウェアを装った不正プログラムが悪用されました。PlugXと呼ばれる中国製のマルウェアの１つで、過去には日本へのサイバー攻撃でも悪用されたものです。これらが、どのシステムから発見されたのかは明らかにされていません。



注意！！
セキュリティ製品やソフトウェアのアップデートを装ったサイバー攻撃は、しばしば利用される手口の1つです。これらの連絡を受け取った際は、情報発信者の公式ウェブサイトで確認するなどの確認を行ってください。

© 2019 SIGHNT, INC

（2016）ベトナム航空の事案



航空分野を標的とするサイバー攻撃の特徴

航空分野を標的としたサイバー攻撃の主な目的は、「軍事」「テロ行為」の支援であることは明らかです。その手段は「システム停止」「情報窃取」などがあります。
また、海外の過去事案の一部は、侵入経路の特定に至っていないものがあります。その要因の一つとして、サプライチェーン連携の多い産業であることから、管理体制が不足がちになっている実状がある可能性があります。

01

「軍」が主導でサイバー攻撃に関与している可能性
特定国からのサイバー攻撃は、軍もしくは情報機関が関与していることが判明しており、航空分野はその典型です。その主な任務は、プロジェクトの全体支援です。

02

永続的な情報収集を実施
標的企業のネットワーク環境、請負事業者などを把握している可能性が高いです。

03

海外拠点を含めての侵入
被害企業の一部は、海外拠点に対して横展開が行われていました。航空会社はグローバルのネットワークを持っていることを理解しての活動とみられます。

© 2019 SIGHNT, INC



「軍」が関与したサイバー攻撃の特徴とは？

SIGHNT JAPAN INTELLIGENCE

THREAT HUNTING AND INTELLIGENCE

（参考）中国のサイバー部隊は主に３タイプ

SIGHNT JAPAN INTELLIGENCE

军队专业网络战力量	授权力量	民间力量
中国人民解放軍（PLA）のサイバー部隊のことである。 現在は、**戦略支援部隊（SSF）**として宇宙、サイバー、電子は統合されている。 脅威グループの多くは、ここに属しているとされる。**軍民融合策**の影響で国営企業などの支援もあるとみられる。 脅威グループ例： Blacktech（Plead） DragonOK	中国人民解放軍（PLA）の権限を付与されたサイバー部隊である。 **国家安全保障部（MSS）、公安部（MPS）**、およびその他のサイバー攻撃活動を承認された**民間組織**のチームである。 米国が訴追しているのは、これに該当するサイバー部隊である。 脅威グループ例： APT10（Menupass） APT3	非政府軍（民間）のサイバー部隊である。 自発的にサイバー攻撃と防御を行う外部組織である。 ただし、**サイバー攻撃のために組織化され動員されている可能性がある。** 脅威グループ例： 1937CN Winnti

© 2019 SIGHNT, INC



（2019）戦略支援部隊は約900人の新兵を募集

© 2019 SIGHNT, INC

THREAT HUNTING AND INTELLIGENCE

（参考）戦略支援部隊直属の教育機関



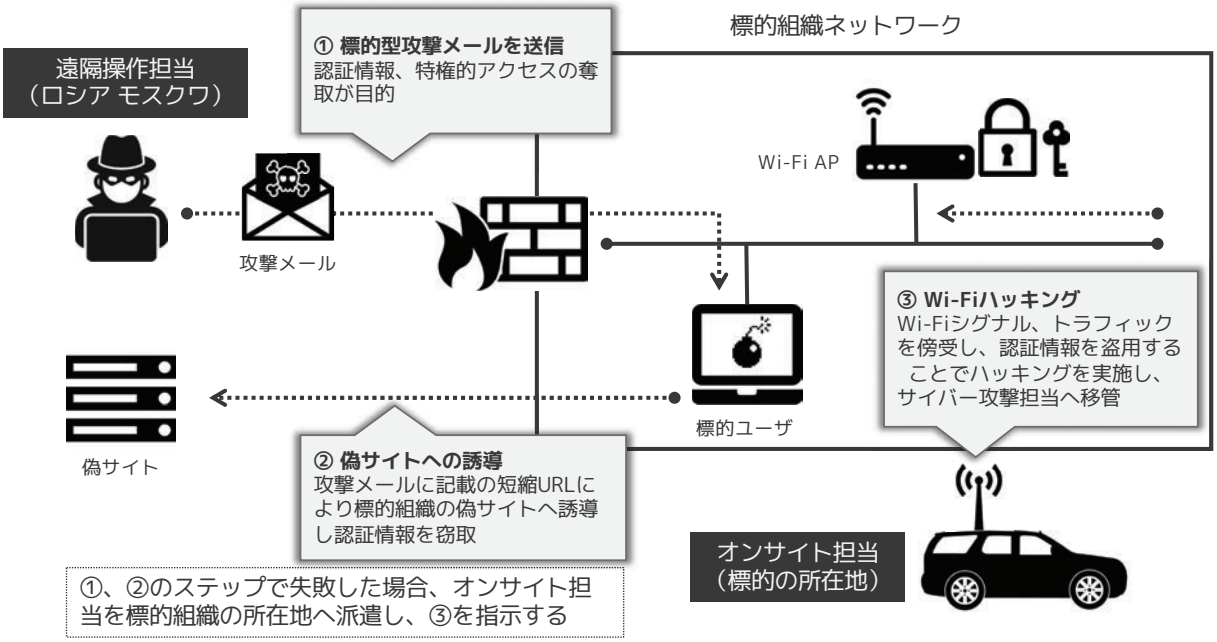
© 2019 SIGHNT, INC

ロシア連邦軍参謀本部情報総局の事例



© 2019 SIGHNT, INC

ロシア連邦軍参謀本部情報総局の事例



© 2019 SIGHNT, INC

THREAT HUNTING AND INTELLIGENCE

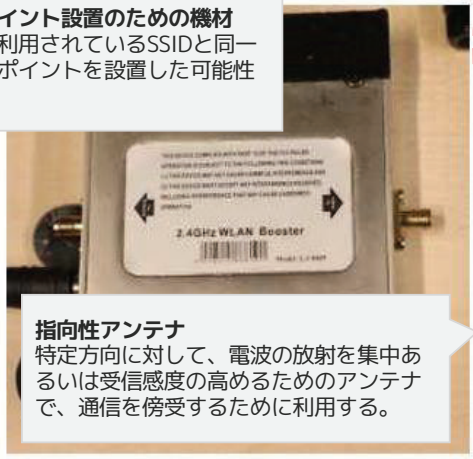
ロシア連邦軍参謀本部情報総局の事例





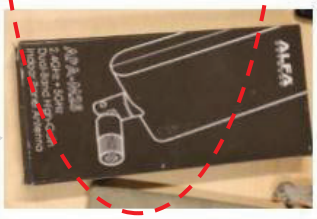


偽アクセスポイント設置のための機材
標的組織内で利用されているSSIDと同一の偽アクセスポイントを設置した可能性が高い。





指向性アンテナ
特定方向に対して、電波の放射を集中あるいは受信感度の高めるためのアンテナで、通信を傍受するために利用する。

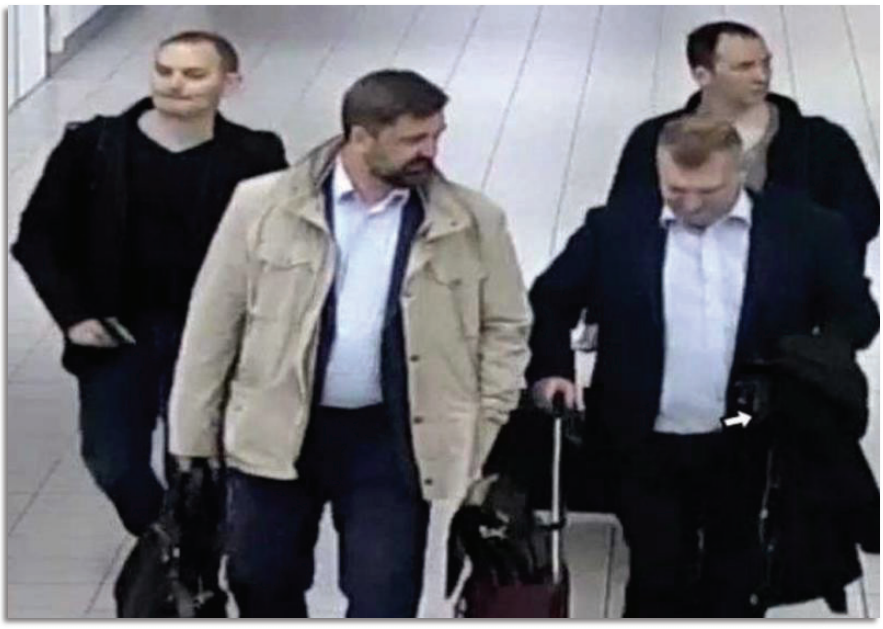


© 2019 SIGHNT, INC

THREAT HUNTING AND INTELLIGENCE

ロシア連邦軍参謀本部情報総局の事例

オンサイト部隊は、２チームで構成されていました。前の２名は、標的組織の関係者とコンタクトを取ることで、認証情報などの機微情報を引き出すことを任務としています。また、後ろの２名は、無線LANのハッキングを行う技術者で、標的組織内の認証情報の窃取を行うことを任務としています。



© 2019 SIGHNT, INC

過去にオリンピックに活動した脅威グループ

サイバー部隊母体	国	推測されるグループ
軍	米国	Equation Group
	中国	Plead, Taidoor, DragonOK, Tick, Roaming Tiger など
	ロシア	Fancy Bear (APT28)
	北朝鮮	Group 123 (APT37)
党	北朝鮮	Lazarus (APT38)
政府機関（情報機関、公安など）＋民間	米国	Equation Group
	中国	Menupass (ATP10) , APT3 , APT17 , Turbine Panda
	ロシア	Cozy Bear（APT29）, Turla
	韓国	Darkhotel
	ベトナム	Ocean Lotus (APT32)
民間	中国	Winnti

2018年の平昌冬季オリンピックでサイバー攻撃を行なったとされるグループ。

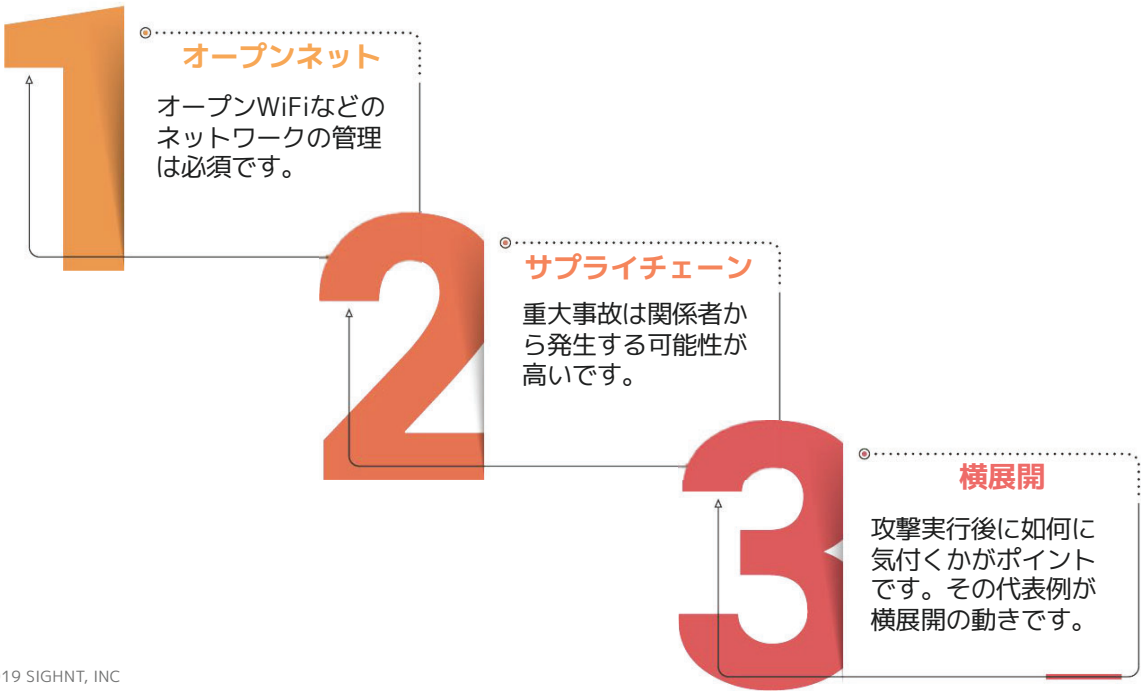
© 2019 SIGHNT, INC

2 オリンピックに向けて

攻撃証跡からみる重要セキュリティ対策

© 2019 SIGHNT, INC

オリンピック対策へのキーワード



© 2019 SIGHNT, INC

（参考）脅威グループから学ぶ最低限の対策例

ファイル名 / フォルダ名	概説
shell.jpg	1.phpが埋め込まれたGIFファイル
123.exe	PETool v1.0.0.5 PEファイルビューワー
123123/	PeHider32.exe、PeHider64.exe、encoder.exe が含まれるフォルダ
BvSshServer-Inst.exe	Bitvise SSH Server UNIXライクなコマンドも使えるWindows用SSHサーバー
CVE-2019-0708.txt	Metasploit Frameworkのモジュールへのリンクのメモ
Invoke-mimikittenz.ps1	Powershellベースのペネトレーションツール「nishang」のコマンドの一つで、メモリ上から認証情報を窃取するためのツール
invoke-mimikatz.ps1	PowerSploitのモジュール 機能は上述のInvoke-mimikittenz.ps1と同じ
ListAllUsers.ps1	レジストリキーからリモートデスクトップの接続履歴を収集する
ListLogged-inUsers.ps1	ListAllUsers.ps1とセットで配布されているツールで、リモートデスクトップのログインユーザの履歴をレジストリキーから収集する
VigorScan.py	DrayTek社のルーターである「Vigor」のの管理ページを探索するPythonベースのスキャナー
aaa/	111.txtが含まれるフォルダ 111.txtは、VigorScan.pyのスキャン結果
Windows全版本激活.exe	Windows全バージョンのアクティベーションツール
domain0829.txt	日本の攻撃対象（SSL VPN）のWhois情報を調査した結果
python-2.7.15.amd64.msi	Pythonのインストーラー

© 2019 SIGHNT, INC

（参考）脅威グループから学ぶ最低限の対策例

ツール群は、（１）サーバアプリケーション、（２）PowerShellベースのペネトレーションテストツール、（３）ネットワーク機器のスキャンツールの３つに分類できます。それぞれに対し、対策を施すことで最近の攻撃への対策として効果が期待できると考えます。

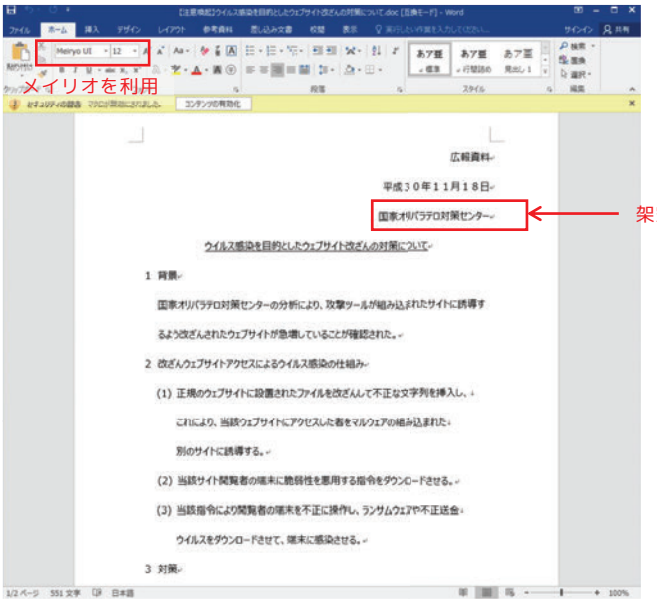
No.	対策例	備考
1	サーバアプリケーションの不正インストールの有無のチェック	SSH,VNC,TeamViewer リモートデスクトップなど
	サーバに不要なプログラミング言語のインストールの有無のチェック	Python,ruby,Perlなど
	サーバへのアクセス制御	
	サーバのアカウント管理	管理者権限は要注意
	外部からのスキャンの確認	Shodan,nmapなどでチェック
2	Powershellの実行制御	
	Powershellのバージョンアップ	最新版の利用を推奨
	ユーザ権限の管理	ユーザへ管理者権限を付与しないなど
	ログの取得	Eventlogなどへの出力など
3	ネットワーク機器へのパッチ適用	ネットワーク機器のファームウェアのバージョン管理
	ネットワーク機器の管理画面へのアクセス制御	インターネットからアクセスできないか
	外部からのスキャンツールによる見え方のチェック	Shodan,nmapなどでチェック

© 2019 SIGHNT, INC

オリンピック関連のサイバー攻撃

東京オリンピックに絡むサイバー攻撃

東京オリンピック・パラリンピック競技大会の関係者、もしくは重要インフラ企業を標的としたとみられる攻撃が確認されています。囮ファイルの内容は、「国家オリパラテロ対策センター」という架空組織を名乗り、警察庁が2017年に日本サイバー犯罪対策センター（JC3）と連携して公表した同名資料を編集したものでした。



© 2019 SIGHNT, INC

THREAT HUNTING AND INTELLIGENCE

東京オリンピックに絡むサイバー攻撃

New cyberattacks targeting sporting and anti-doping organizations

Oct 28, 2019 | Tom Burt - Corporate Vice President, Customer Security & Trust



© 2019 SIGHNT, INC

出所：https://blogs.microsoft.com/on-the-issues/2019/10/28/cyberattacks-sporting-anti-doping/

ネットワーク機器への攻撃事例

攻撃が成功した場合、バージョン情報が変更されます。一見、正規のファームウェアの更新のようにみえますが、その前後の時間にコマンドが実行されていることが多いようです。
多くの場合は、標的の機器の再起動後に、動作が不安定になります。

正規の状態

```
------------------ show clock ------------------

10:44:16.635 JST Mon Jun 8 2015

------------------ show version ------------------

Cisco IOS Software, C3560 Software (C3560-IPBASEK9-M), Version 12.2(58)SE1, RELEAS
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2011 by Cisco Systems, Inc.
Compiled Thu 05-May-11 02:18 by prod_rel_team

ROM: Bootstrap program is C3560 boot loader
BOOTLDR: C3560 Boot Loader (C3560-HBOOT-M) Version 12.2(53r)SEY4, RELEASE SOFTWARE

[redacted] uptime is 1 year, 13 weeks, 6 days, 8 hours, 12 minutes
System returned to ROM by power-on
System restarted at 02:27:11 JST Mon Mar 3 2014
System image file is "flash:/c3560-ipbasek9-mz.122-58.SE1/c3560-ipbasek9-mz.122-58

Switch Ports Model              SW Version            SW Image
------ ----- -----              ----------            ----------
*    1 26    WS-C3560V2-24TS    12.2(58)SE1           C3560-IPBASEK9-M
```

不正ファームウェアのアップデート

```
------------------ show clock ------------------

07:59:25.761 JST Wed [redacted] 2018

------------------ show version ------------------

Cisco IOS Software, C3560 Software (C3560-IPBASEK9-M), Version 12.2(58)SE2, RELEAS
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2011 by Cisco Systems, Inc.
Compiled Thu 21-Jul-11 01:44 by prod_rel_team

ROM: Bootstrap program is C3560 boot loader
BOOTLDR: C3560 Boot Loader (C3560-HBOOT-M) Version 12.2(53r)SEY4, RELEASE SOFTWARE

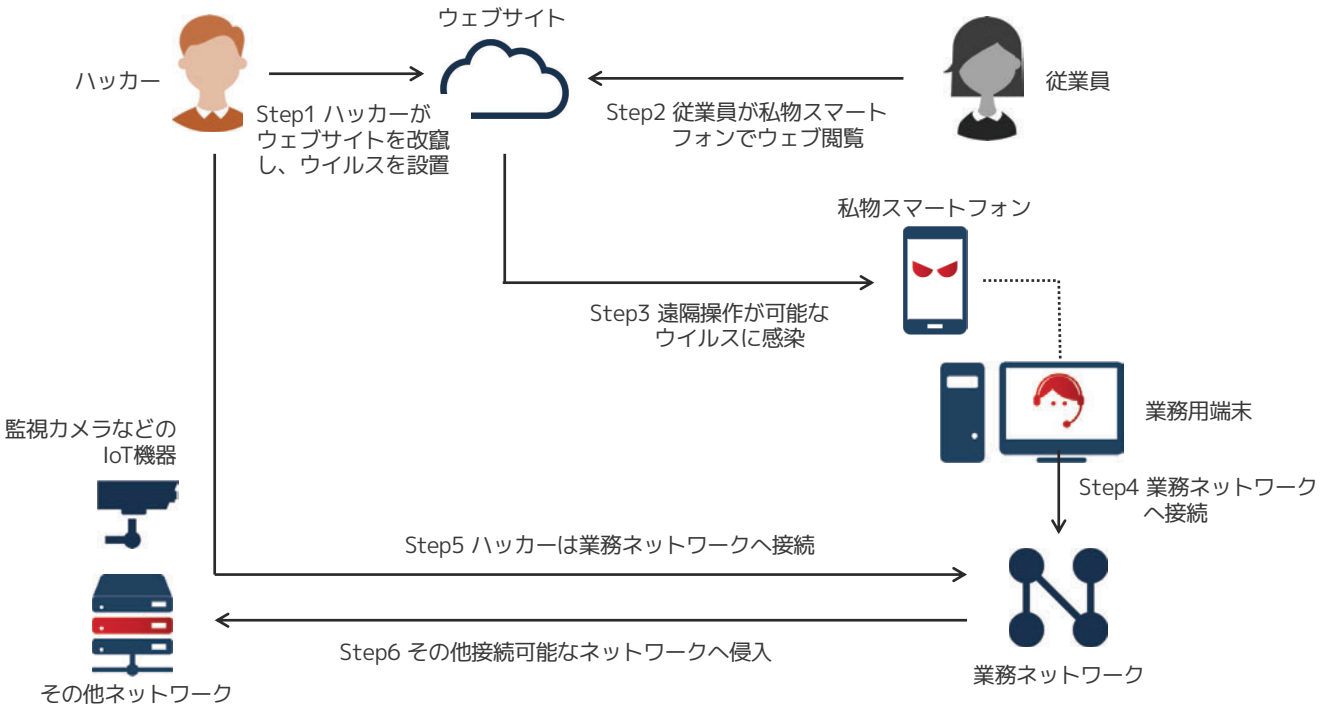
[redacted] uptime is 6 hours, 4 minutes
System returned to ROM by power-on
System restarted at 01:54:31 JST Wed [redacted] 2018
System image file is "flash:/c3560-ipbasek9-mz.122-58.SE1/c3560-ipbasek9-mz.122-58

Switch Ports Model              SW Version            SW Image
------ ----- -----              ----------            ----------
*    1 26    WS-C3560V2-24TS    12.2(58)SE2           C3560-IPBASEK9-M
```

バージョン が変更されている

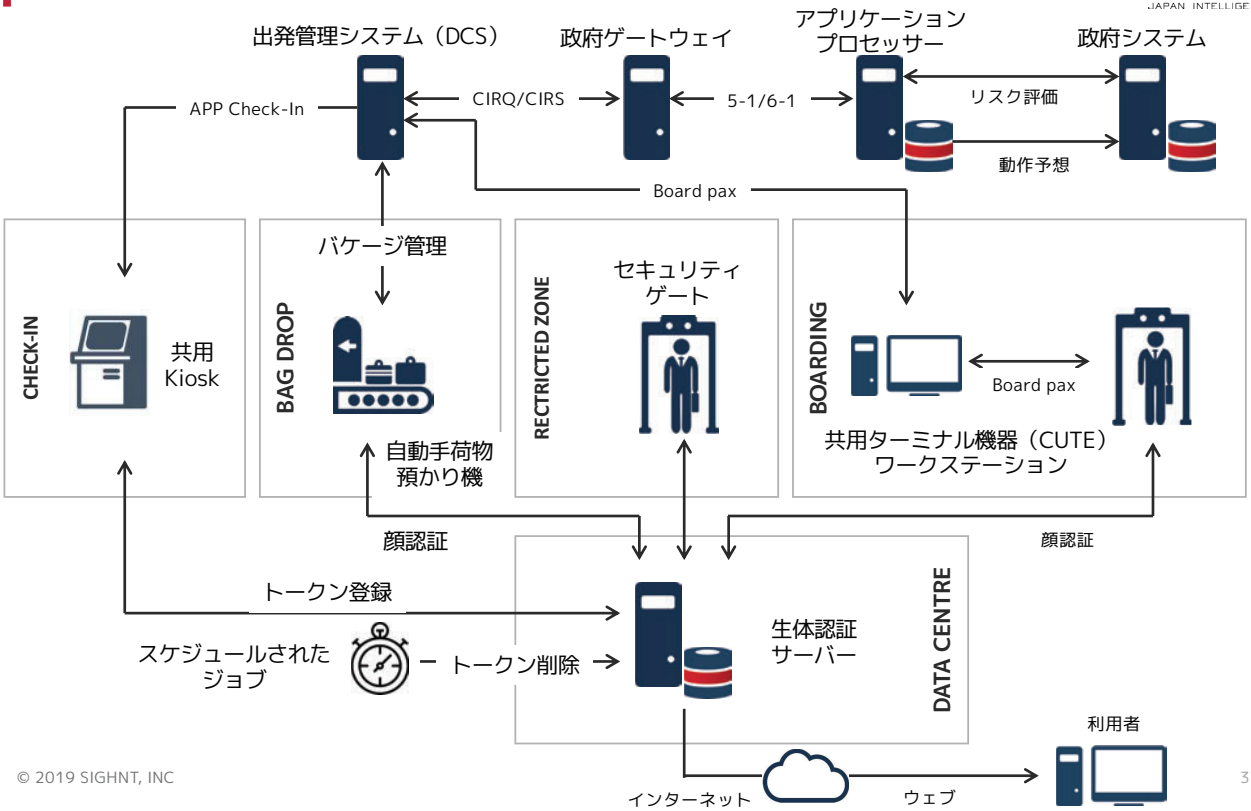
© 2019 SIGHNT, INC

（運用）BYODのリスク管理の重要性



© 2019 SIGHNT, INC

（管理）障害ポイントの想定（自動チェックイン）



© 2019 SIGHNT, INC

標的が開発や保守に携わるユーザーへと移行

01

サプライチェーンを介して本丸へサイバー攻撃を実施

開発関係者や保守担当者は、インターネットから隔離された重要システムにおいてもアクセスすることができる数少ないユーザーです。重要システムを狙うハッカーは、彼らに不正プログラムを運ばせることでサイバー攻撃を実現しようとすることは自然の流れです。

02

セキュリティ事故はシステム運用ルールと実態のギャップから発生

サイバー攻撃は、運用上のミスを狙ったものが少なくありません。特に、業務が多忙で、担当者に無理が生じたことから発生していることが多いです。例えば、一人の担当者がセキュリティ対策を後回し（もしくは失念）としたことが原因での事故は多い例です。

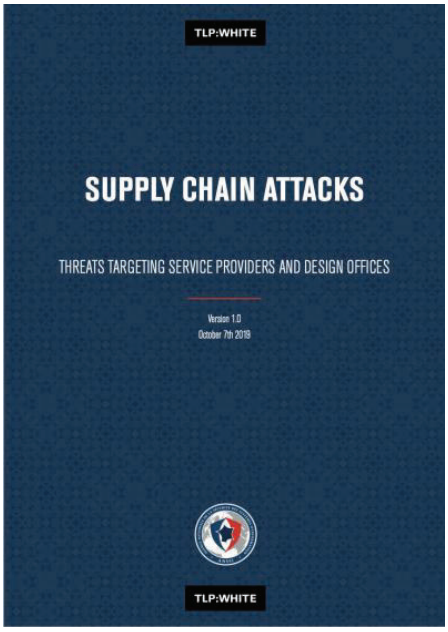
03

「暗黙の信頼」が生じる箇所が標的

一般に、日常的に利用しているソフトウェアは、正常動作を疑うことをしません。これは、組織内に働く多数派同調バイアスと正常性バイアスの影響が大きいです。ハッカーが、正規ソフトウェアに細工をしたり、標的を限定的とするのも同様の効果を狙ってのものです。

© 2019 SIGHNT, INC

サプライチェーン攻撃への警戒を強化



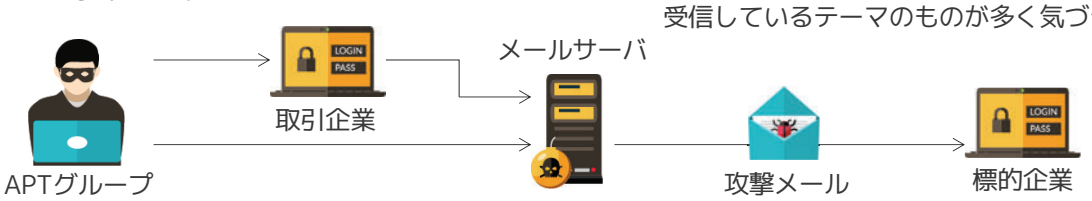
1. 概要
   - サービスプロバイダーと設計事務所を標的としたサイバー攻撃への警告
     ※特定国や攻撃者像の記載は無し
2. マルウェア
   - 主に**PlugX**を利用
   - Webshell
3. 権限昇格
   - ProcDump
   - Certmig
4. 横展開
   - RDP
   - NetScan
   - WMIExec
5. 攻撃者の接続元
   - VPNプロバイダー
   - TORネットワーク

© 2019 SIGHNT, INC

標的型メールの動向変化

① 取引企業のメールアカウントをハッキング

③ 攻撃メールに添付される囮ファイルは、継続的に受信しているテーマのものが多く気づきづらい。



② 標的企業とのメールのやり取りに合わせハッキングしたメールアカウントを利用して攻撃メールを送信

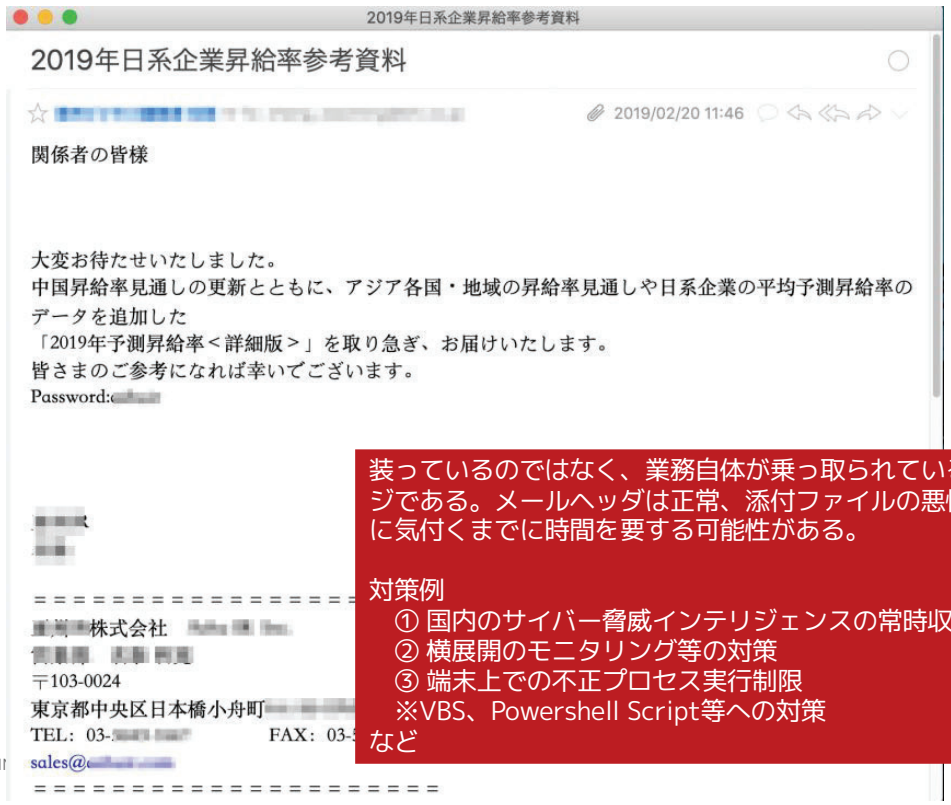
01 **取引先のメールアカウントの乗っ取り**
標的型メールで、取引先のメールアカウントが乗っ取られている事案が継続している。
メールのヘッダ情報のみでは、攻撃メールを見抜くことが困難になってきた。

02 **関連会社を標的としたサイバー攻撃の増加**
海外に現地法人や合弁会社を設置している組織において、国外の拠点が標的となったケースが増加傾向である。

03 **標的ユーザー層の変化**
攻撃対象として、人事担当者や海外担当者が狙われた事案が散見されています。今まで以上に事業に関連したテーマの囮ファイルが利用されるようになってきています。

© 2019 SIGHNT, INC

（参考）サービスベンダーからの標的型攻撃例



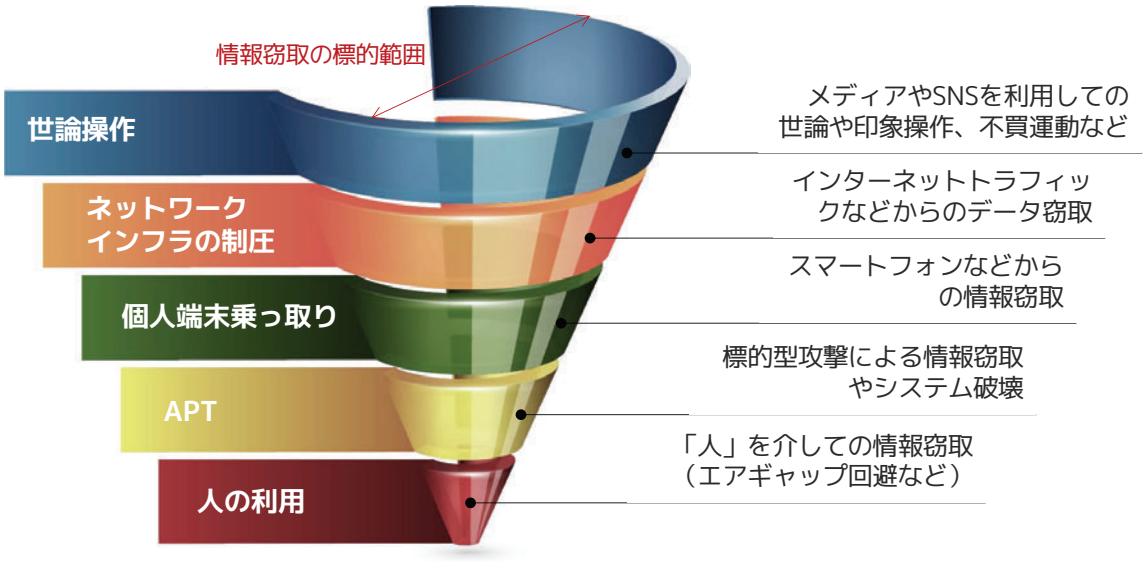
装っているのではなく、業務自体が乗っ取られているイメージである。メールヘッダは正常、添付ファイルの悪性コードに気付くまでに時間を要する可能性がある。

対策例
① 国内のサイバー脅威インテリジェンスの常時収集
② 横展開のモニタリング等の対策
③ 端末上での不正プロセス実行制限
※VBS、Powershell Script等への対策
など

© 2019 SIGHNT, I

オリンピック等の政治絡みのサイバー脅威の全体像

国家として関心度の高いテーマに関しては、フェイクニュースやSNSへの書き込みによる世論操作が発生する。政治的要素の高い場合は、ネットワークインフラのレベルで盗聴を試みるなどする。
日本ではあまり話題にはならないが、スマートフォンへのサイバー攻撃などは要注意である。



© 2019 SIGHNT, INC

まとめ

01 **継続的に行われている航空分野へのサイバー攻撃の認識が必要**
APTグループによる攻撃が散見されることから、長期に渡っての攻撃対象となっている可能性が高いです。オリンピックだけでなく、社会情勢に鑑みたセキュリティ対策が必要であることを認識してください。

02 **サイバー攻撃は技術・物理・人の観点からの対策が重要**
各国のサイバー攻撃の位置付けは、目的達成のための支援策であり、並行して人的脅威が関係していることが判明しています。そのため、企業におけるサイバー衛生管理の重要性が高まっています。

03 **オリンピック関連の攻撃準備は開催前に完了と捉えるべし**
既にオリンピック関連のサイバー攻撃が観測されていることを踏まえますと、既に国内外に関わらず、侵害を受けているシステムがあることを前提に準備が必要です。

© 2019 SIGHNT, INC

株式会社サイント

情報をみんなのチカラへ

国家間の駆け引きやビジネスに限らず、情報とその分析情報はあらゆる場面での重要な要素となります。特に、インプットとなる情報は、時に偽りの情報であることもあります。そのため、情報は多角的に分析し、精度の高い知識へと昇華させる必要があります。そこで、初めて活用可能な知恵となり、組織の力となります。

ビジネスの国際競争は、事前に情報操作や諜報活動が行われていることは珍しくありません。しかし、日本で得られる脅威情報の多くは海外発ものが多く、殆どの日本組織が事実を知る術がありません。私たちは、日本は独自の脅威分析を行うことで、正しく危機管理と経営判断を行うべきと考えています。

私たちが目指すのは、日本が世界と対等に戦うための「アタリマエの情報環境」の構築です。

© 2019 SIGHNT, INC

商号	株式会社サイント SIGHNT, Inc.
設立	2018年2月5日
代表取締役	岩井　博樹
事業内容	脅威インテリジェンスの提供 セキュリティ運用支援 セキュリティ・アドバイザリー業務 など
窓口	info@sighnt.com
HP	https://www.sighnt.com


株式会社 サイント
URL: www.sighnt.com
Mail: info@sighnt.com

セキュリティインシデントから学べること
～鉄道分野に関連するインシデント事例～

2019年11月05日

(c) Institution For Transport Policy Studies, inc. 2019

- 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
- セキュリティ確保への取り組み

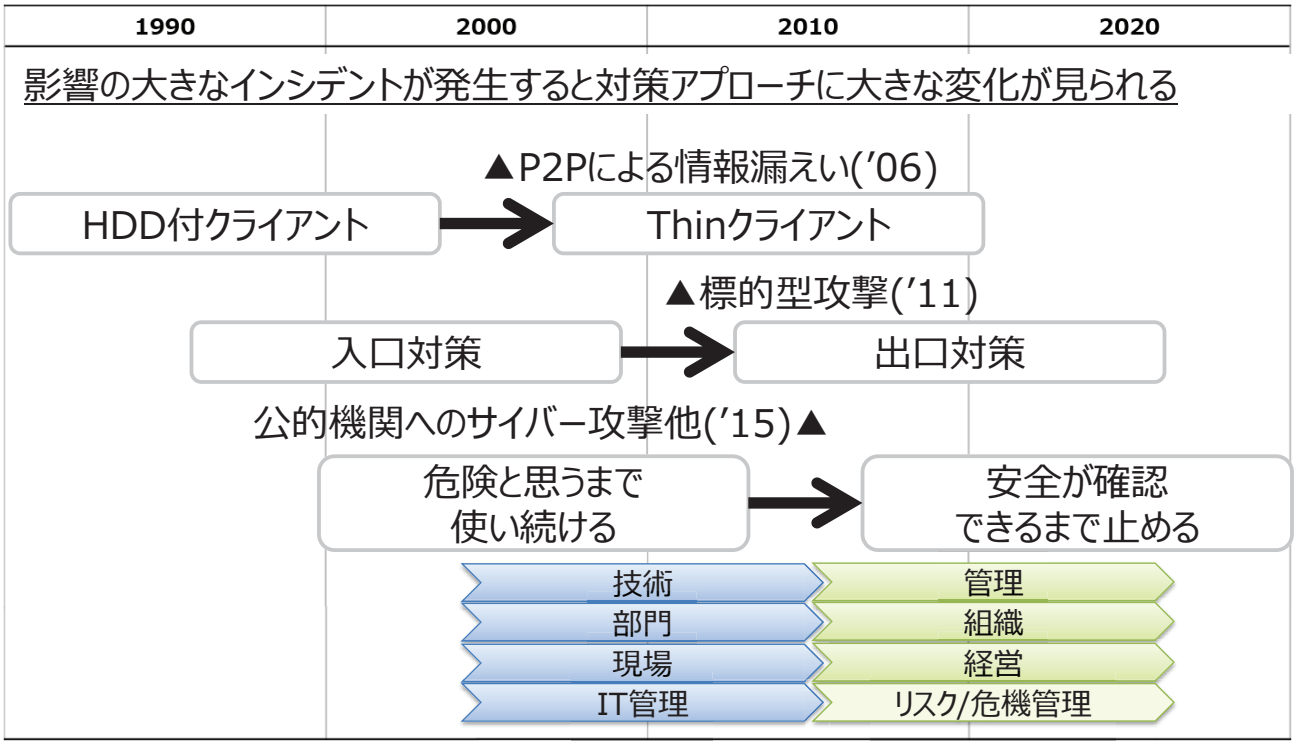
(c) Institution For Transport Policy Studies, inc. 2019

- 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
- セキュリティ確保への取り組み

(c) Institution For Transport Policy Studies, inc. 2019

サイバーセキュリティに関する動向

- 【変化】「安全が確認できるまで止める」という考え方への対処



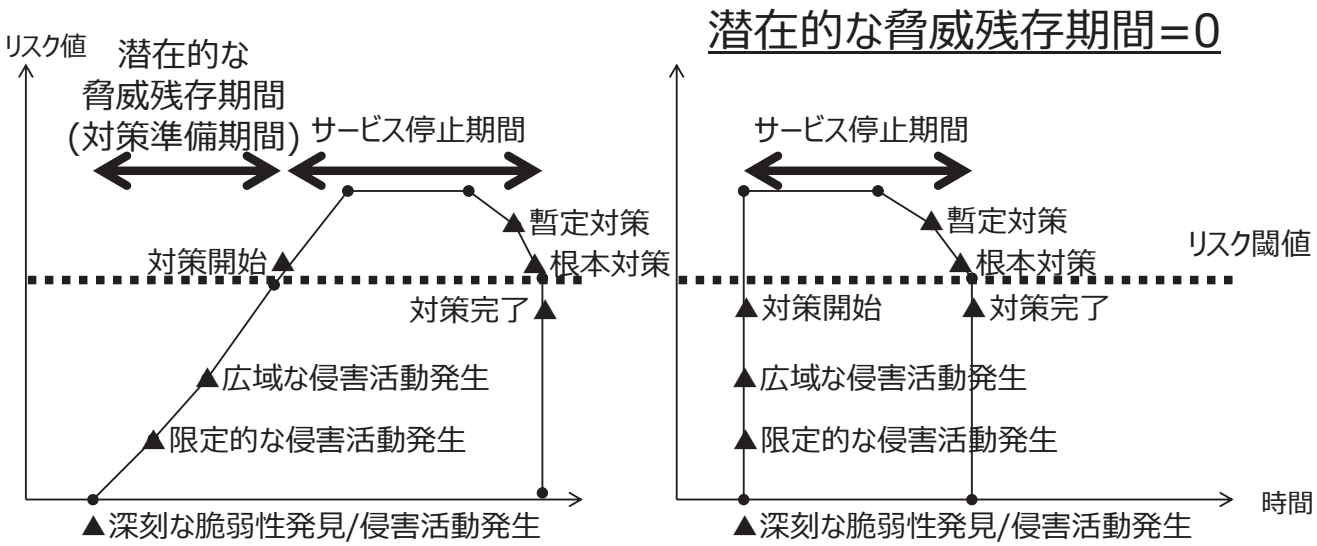
(c) Institution For Transport Policy Studies, inc. 2019

サイバーセキュリティに関する動向

- 【変化】「安全が確認できるまで止める」という考え方への対処

危険と思うまで使い続ける

安全が確認できるまで止める



(c) Institution For Transport Policy Studies, inc. 2019

サイバーセキュリティに関する動向

- 【変化】「？？？」
  - 代表的なサイバーセキュリティイベント

時期	イベント
2010年08月	Stuxnetによるイランのウラン濃縮施設へのサイバー攻撃
2010年09月	グルジアにおけるサイバー攻撃によって、米国や北大西洋条約機構に関する文書の窃取が発生
2016年	米国大統領選挙におけるロシアの干渉
2016年12月	ウクライナにおけるサイバー攻撃によって、数時間に渡る停電が発生
2017年05月	NSA製バックドアツールを悪用したWannaCryの流布
2017年06月	NSA製バックドアツールを悪用したNotPetyaの流布
2017年06月	脆弱性　Spectre、Meltdown の発見と脆弱性開示のための調整プロセスの開始
2018年01月	脆弱性　Spectre、Meltdown の公開
2018年02月	Charter of Trust (Private Sectorからの規範の提唱)
2018年04月	Cybersecurity Tech Accord (Private Sectorからの規範の提唱)
2018年07月	米上院商務・科学・運輸委員会において公聴会 “Complex Cybersecurity Vulnerabilities: Lessons Learned from Spectre and Meltdown“ 開催 脆弱性　Spectre、Meltdown に関する公聴会については、米国内での対策が不十分な状態で、国外、特に、中国に対して、その脆弱性情報が展開されたことへの懸念と、脆弱性開示のための調整プロセスに対する理解を深めることを目的として開催された。

(c) Institution For Transport Policy Studies, inc. 2019

サイバーセキュリティに関する動向

- 【変化】「？？？」
  - Spectre、Meltdownとは?
    CPUの脆弱性とも言われている。

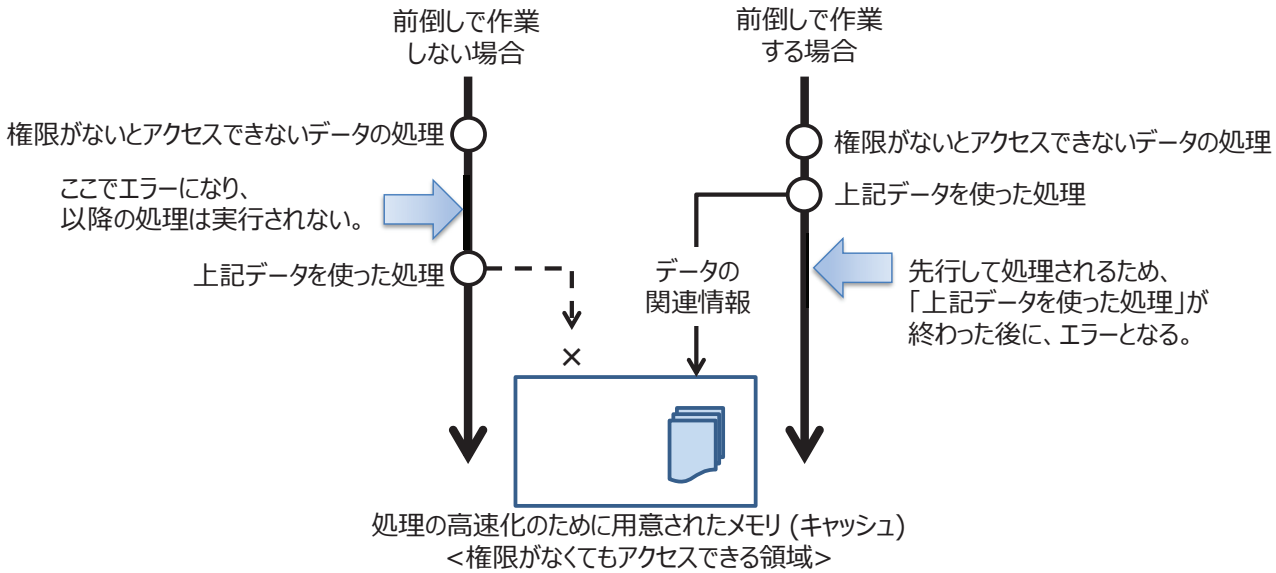
    - 高速なCPUを最大限活用するために、命令を順番に処理するのではなく、処理できる命令は先物であっても先行して処理などをしている。このような機能のことを、総称して、投機的実行(Speculative Execution)と呼ぶ。
    - 前倒しで作業をすることになるため、処理の効率化には有効であるが、当然、結果が無効であったり、処理する必要のない命令が実行されてしまったりするなどのイレギュラーな状態が発生することになる。

      ⇒ここで、情報漏えいなどのセキュリティ上の問題が指摘された。

(c) Institution For Transport Policy Studies, inc. 2019

サイバーセキュリティに関する動向

- 【変化】「？？？」
  - Meltdownと呼ばれた脆弱性は、、、
    本来だとアクセスできないデータが、権限がなくてもアクセスできる領域に格納されることでアクセス可能に!



(c) Institution For Transport Policy Studies, inc. 2019

サイバーセキュリティに関する動向

- 【変化】「？？？」

HEARINGS

HOME / HEARINGS

July 11, 2018

Complex Cybersecurity Vulnerabilities: Lessons Learned from Spectre and Meltdown

253 Russell

U.S. Sen. John Thune (R-S.D.), chairman of the Committee on Commerce, Science, and Transportation, will convene a hearing entitled, "Complex Cybersecurity Vulnerabilities: Lessons Learned from Spectre and Meltdown," at 10:00 a.m. on Wednesday, July 11, 2018. The hearing will review cybersecurity issues raised in response to the Spectre and Meltdown vulnerabilities, such as challenges with conducting complex coordinated vulnerability disclosure and supply chain cybersecurity, and how best to coordinate cybersecurity efforts going forward. This hearing follows **a letter** sent by Sens. John Thune (R-S.D.) and Bill Nelson (D-Fla.) to 12 organizations about the Spectre and Meltdown vulnerabilities and the steps taken to mitigate these vulnerabilities.

Witnesses:

- Ms. Donna Dodson, Chief Cybersecurity Advisor and Director of the National Cybersecurity Center of Excellence, National Institute of Standards and Technology, U.S. Department of Commerce
- Dr. José-Marie Griffiths, President, Dakota State University
- Ms. Joyce Kim, Chief Marketing Officer, ARM
- Mr. Art Manion, Senior Vulnerability Analyst, CERT Coordination Center, Software Engineering Institute, Carnegie Mellon University
- Mr. Sri Sridharan, Managing Director, Florida Center for Cybersecurity, University of South Florida

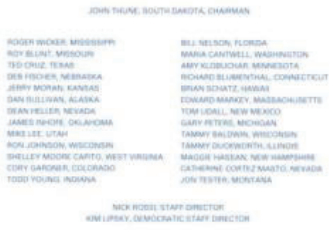
米上院商務・科学・運輸委員会のJohn Thune上院議員は、2018年7月11日(水)の午前10:00から"Complex Cybersecurity Vulnerabilities: Lessons Learned from Spectre and Meltdown"と題する聴聞会を開催する。

この公聴会では、協調的な脆弱性の開示(Coordinated Vulnerability Disclosure)とサプライチェーンのサイバーセキュリティの実施に伴う課題とその対応など、SpectreおよびMeltdownの脆弱性を通して提起されたサイバーセキュリティの問題について検討する。

この公聴会は、John Thune上院議員とBill Nelson上院議員がSpecterとMeltdownの脆弱性およびこれらの脆弱性を緩和するために講じた措置について12の組織に送った手紙に続く。

サイバーセキュリティに関する動向

- 【変化】「？？？」



United States Senate

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

WASHINGTON, DC 20510-6125

WEBSITE: http://commerce.senate.gov

<送付先>
アマゾン、アップル、NVIDIA、インテル、マイクロソフト、グーグル、シスコシステムズ、IBM、ARM、Advanced Micro Devices、Lenovo、HuaweiのCEO

February 15, 2018

Mr. Jeffrey P. Bezos
President, Chief Executive Officer,
and Chairman of the Board
Amazon.com, Inc.
410 Terry Avenue North
Seattle, WA 98109

<質問内容>
1. When and how did you first become aware of these vulnerabilities?
2. Which of your products are affected by these vulnerabilities and how are they affected?

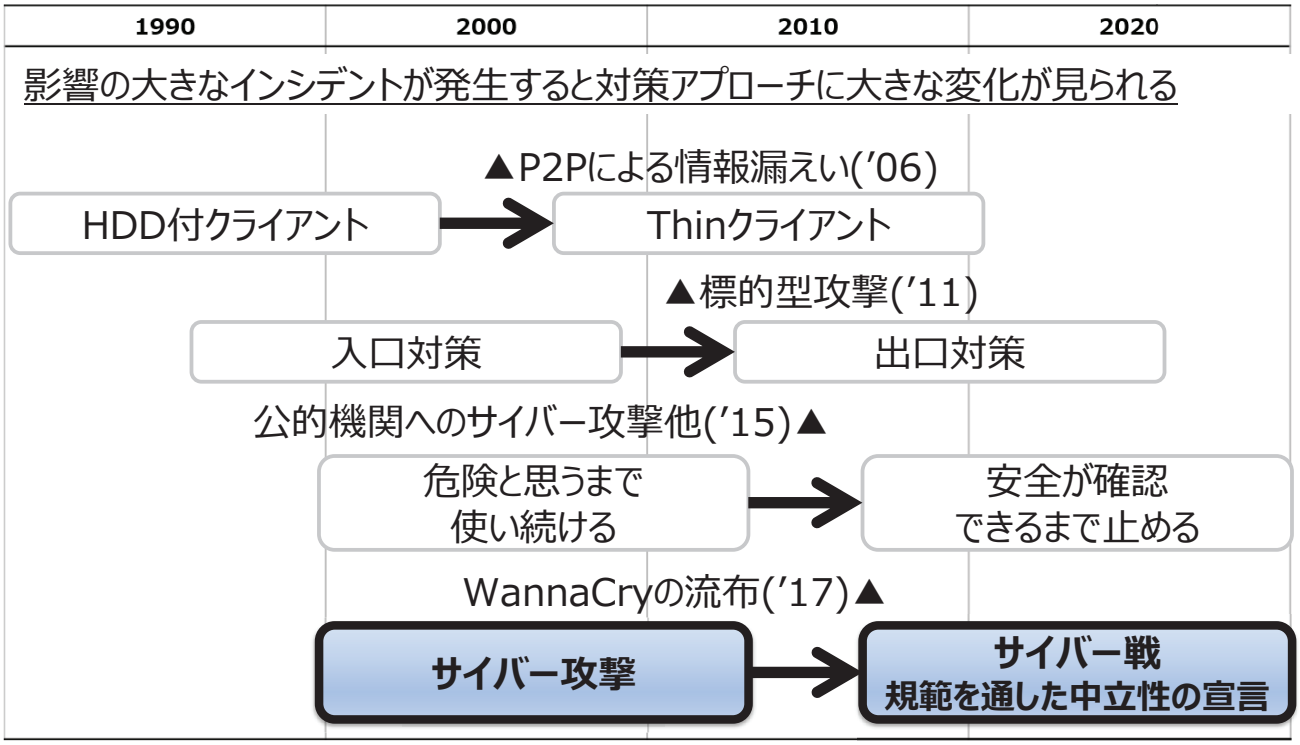
3-10.<snip>

Dear Mr. Bezos:

Academic and independent security researchers,[1] some of whom were federally-funded,[2] recently discovered three vulnerabilities in modern computer processers that have existed for more than two decades.[3] These side-channel vulnerabilities,[4] which researchers have named "Meltdown" and "Spectre," could allow sophisticated hackers access to stored passwords, encryption keys, and other highly sensitive information.[5]

サイバーセキュリティに関する動向

- 【変化】「規範を通した中立性の宣言」



(c) Institution For Transport Policy Studies, inc. 2019

サイバーセキュリティに関する動向

- 【変化】「規範を通した中立性の宣言」… Public Sectorの動き
  - UN Group of Governmental Experts
    - GGE(国際連合の政府専門家会合)は、ロシア政府が呼びかけたもので、2004年以降、これまでに5回開催されている。第1回から第3回までは国際連合加盟国から15カ国ずつ参加し、第4回は20カ国、第5回は25カ国が参加した。
    - 第4回(2015年)の会合で、Norms, rules and principles for the responsible behavior of Statesについて言及

国家は、重要インフラに対して意図的に損害や障害を与えるようなICT活動を行ったり、支援したりしてはならない。
One important recommendation was that a State should not conduct or knowingly support ICT activity that intentionally damages or otherwise impairs the use and operation of critical infrastructure.

United Nations Group of Governmental Experts
http://www.un.org/

(c) Institution For Transport Policy Studies, inc. 2019

サイバーセキュリティに関する動向

- 【変化】「規範を通した中立性の宣言」… Public Sectorの動き
  - Internet Governance Forum
    - IGF(インターネットガバナンスフォーラム)は、2005年の「チュニス・アジェンダ(Tunis Agenda for the Information Society)」によって国際連合の下に設置された。マルチステークホルダーがインターネットに関する公共政策課題を議論するために、2006年以降毎年1回開催されている。
    - IGF2018において、エマニュエル・マクロン大統領が、サイバー空間の信頼性と安全性のためのParis Callを発表(フランス政府主導で提唱)

- 悪意あるオンライン活動の予防と強靭性を向上
- インターネットのアクセシビリティと完全性を保護
- 選挙プロセスへの干渉を防ぐために協力
- サイバー空間を通した知的財産権侵害に協力して対抗
- 悪意あるプログラムやオンライン技術の拡散を防止
- デジタル製品やデジタルサービスの安全性ならびにすべての人の「サイバー衛生」を向上
- サイバー傭兵や非国家主体の攻撃に対する対抗措置を実施
- 適切な国際規範の強化に協力して取り組む

Internet Governance Forum
https://www.intgovforum.org/multilingual/

(c) Institution For Transport Policy Studies, inc. 2019

サイバーセキュリティに関する動向

- 【変化】「規範を通した中立性の宣言」… Public Sectorの動き
  - Global Commission on the Stability of Cyberspace
    - GCSC(サイバー空間の安定性に関するグローバル委員会)は、2017年にオランダ政府が支援して設立された。
    - 2017年、Non-Interference with the Public Core(インターネットルーティング、ドメインネームシステム、証明書と信頼、通信ケーブル)を宣言
    - 2018年、Norm Package Singaporeを発表

1. 改ざんを回避するための規範
   Norm to Avoid Tampering
2. ICT機器をボットとして使用することに反対する規範
   Norm Against Commandeering of ICT Devices into Botnets
3. 脆弱性開示プロセスを国家が創設するにあたっての規範
   Norm for States to Create a Vulnerability Equities Process
4. 深刻な脆弱性の影響を低減・軽減するための規範
   Norm to Reduce and Mitigate Significant Vulnerabilities
5. 基礎的な防衛手段としての基本的なサイバー公衆衛生に関する規範
   Norm on Basic Cyber Hygiene as Foundational Defense
6. 国家以外の関係者による攻撃的なサイバー操作に反対する規範
   Norm Against Offensive Cyber Operations by Non-State Actors

Global Commission on the Stability of Cyberspace
https://cyberstability.org/

(c) Institution For Transport Policy Studies, inc. 2019

サイバーセキュリティに関する動向

- 【変化】「規範を通した中立性の宣言」… Private Sectorの動き
  - Charter of Trust
    - 2018年2月16日、独シーメンスが中心となって推進、エアバス、アリアンツ、ダイムラー、IBM、ドイツテレコム、SGSなど9社が憲章に賛同している。2019年3月11日時点で16社、日本からは三菱重工が憲章に賛同している。

1. サイバーとITセキュリティのオーナーシップ	Ownership of cyber and IT security
2. デジタルサプライチェーン全体の責任	Responsibility throughout the digital supply chain
3. セキュリティのデフォルト化	Security by default
4. ユーザ中心	User-centricity
5. イノベーションと共創	Innovation and co-creation
6. 教育	Education
7. 重要なインフラストラクチャとソリューションの認証	Certification for critical infrastructure and solutions
8. 透明性と対応	Transparency and response
9. 規制の枠組み	Regulatory framework
10. 共同の取り組み	Joint initiatives

Charter of Trust
http://charter-of-trust.com/

(c) Institution For Transport Policy Studies, inc. 2019

サイバーセキュリティに関する動向

- 【変化】「規範を通した中立性の宣言」… Private Sectorの動き
  - Cybersecurity Tech Accord
    - 2018年4月17日、米マイクロソフトが中心となって推進、ABB、Arm、シスコ、フェイスブック、HP、HPE、ノキア、オラクル、トレンドマイクロなど34社が協定に賛同、日本からは、日立、パナソニックが賛同している。2019年3月11日時点で89社、日本からは新たにNTTが賛同している。
    - アップル、アマゾン、グーグルは不参加

1. あらゆるユーザと顧客の保護
   We will protect all of our users and customers everywhere.
2. 罪のないユーザや企業に対するあらゆるサイバー攻撃への反対
   We will oppose cyberattacks on innocent citizens and enterprises from anywhere.
3. ユーザ、顧客および開発者のサイバーセキュリティ保護強化の奨励
   We will help empower users, customers and developers to strengthen cybersecurity protection.
4. サイバーセキュリティを強化するための提携
   We will partner with each other and with likeminded groups to enhance cybersecurity.

Cybersecurity Tech Accord
https://cybertechaccord.org/

(c) Institution For Transport Policy Studies, inc. 2019

サイバーセキュリティに関する動向

- 【変化】「規範を通した中立性の宣言」… 関連する動き
  - 2019年1月、米上院議員がワシントン首都圏交通局に書簡を送り、その中で、最新の地下鉄車両8000系導入に際して、中国の製造業社と契約を結ぶ可能性について安全上の懸念を表明すると共に、これらの車両に対するサイバーリスクを軽減するために必要な措置を講じることを求めた。

US Senators fear Chinese-made metro rail cars could be used for surveillance
https://www.zdnet.com/article/us-senators-fear-chinese-made-metro-rail-cars-could-be-used-for-surveillance/

(c) Institution For Transport Policy Studies, inc. 2019

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
セキュリティ確保への取り組み

(c) Institution For Transport Policy Studies, inc. 2019

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**
  - 米国鉄道会社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、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

(c) Institution For Transport Policy Studies, inc. 2019

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

(c) Institution For Transport Policy Studies, inc. 2019

鉄道分野におけるインシデント事例

- **2008年、ポーランド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、ポーランド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

(c) Institution For Transport Policy Studies, inc. 2019

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。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。



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

(c) Institution For Transport Policy Studies, inc. 2019

鉄道分野におけるインシデント事例

- **2014年、ソウルメトロに対するサイバー攻撃**
  - 韓国ソウル特別市で地下鉄1～4号線を運営するソウルメトロがサイバー攻撃を受け、PC管理プログラム運用サーバが、少なくとも5ヶ月以上、攻撃者に掌握されていた状態であったことが、2015年10月明らかとなった。

[2015年8月の国家サイバー安全センターによる調査結果]

- PCのマルウェア感染：58台
  - 地下鉄の運行を監視する総合指令所、電力供給を担当する電気通信事業所などのPCが含まれていた。
- PCへの不正アクセス：213台
- サーバの権限奪取：2台
  - PC管理プログラム運用サーバ：1台
  - 会社のWebマガジン運用サーバ：1台
- 業務関連資料の流出：12件

http://news.chosun.com/site/data/html_dir/2015/10/05/2015100500286.html

(c) Institution For Transport Policy Studies, inc. 2019

鉄道分野におけるインシデント事例

- **2014年、ソウルメトロに対するサイバー攻撃**
  - 韓国ソウル特別市で地下鉄1～4号線を運営するソウルメトロがサイバー攻撃を

2015年10月のソウルメトロの報道発表によれば、
『**列車の運行に直接関連する統合指令システムは、業務ネットワークとは一切接続がない、独立したクローズドネットワークで運用されている。**ハッキングはインターネットを介して行われる場合が一般的であり、(接続がないため)問題がない。流出した資料も、列車の業務とは無関係の一般的な業務PCから流出した、業務計画や促進計画などといった、重要性が低い資料である』とのこと。

- サーバの権限奪取：2台
  - PC管理プログラム運用サーバ：1台
  - 会社のWebマガジン運用サーバ：1台
- 業務関連資料の流出：12件

http://www.boannews.com/media/view.asp?idx=48090

(c) Institution For Transport Policy Studies, inc. 2019

鉄道分野におけるインシデント事例

- **2014年、ソウルメトロに対するサイバー攻撃**
  - 攻
    - 業務関連資料の流出：12件

2016年2月のソウル市監査委員会による「都市鉄道の安全とメンテナンスの実態監査結果」によれば、『**クローズドネットワークにウィルスが侵入した痕跡が発見される**など、ハッキングに対して無防備であった』とのこと。

#4. 列車運行制御コンピュータ(TCC)悪性コードの感染放置
#5. 個人情報の録画映像ストレージ管理の不適正
#6. 列車信号・通信閉鎖網管理の不足
#7. 重要な設備保護区域のセキュリティ管理の不適正
#8. ▲▲管制センターサイバーセキュリティ対策の不履行
#9. 個人情報の録画映像ストレージ管理の不適正
#25. 列車信号制御システムのソフトウェアセキュリティ管理不足

http://gov.seoul.go.kr/files/2016/02/56b44ae5bbcfa8.55745107.pdf

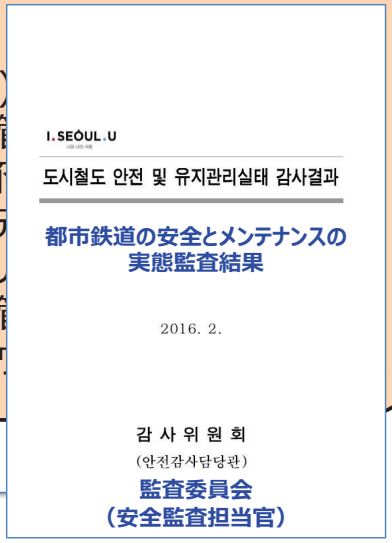
(c) Institution For Transport Policy Studies, inc. 2019

鉄道分野におけるインシデント事例

- **2014年、ソウルメトロに対するサイバー攻撃**
  - 攻
    - 業務関連資料の流出：12件

2016年2月のソウル市監査委員会による「都市鉄道の安全とメンテナンスの実態監査結果」によれば、『**クローズドネットワークにウィルスが侵入した痕跡が発見される**など、ハッキングに対して無防備であった』とのこと。

#4. 列車運行制御コンピュータ(TCC)
#5. 個人情報の録画映像ストレージ管
#6. 列車信号・通信閉鎖網管理の不
#7. 重要な設備保護区域のセキュリテ
#8. ▲▲管制センターサイバーセキュリ
#9. 個人情報の録画映像ストレージ管
#25. 列車信号制御システムのソフトウ



http://gov.seoul.go.kr/files/2016/02/56b44ae5bbcfa8.55745107.pdf

(c) Institution For Transport Policy Studies, inc. 2019

鉄道分野におけるインシデント事例

- **2014年、ソウルメトロに対するサイバー攻撃**
  - 攻

2016年2月のソウル市監査委員会による「都市鉄道の安全とメンテナンスの実態監査結果」によれば、『**<u>クローズドネットワークにウィルスが侵入した痕跡が発見される</u>**など、ハッキングに対して無防備であった』とのこと。

#4. 列車運行制御コンピュータ(TCC)悪性コードの感染放置
#5. 個人情報の録画映像ストレージ管理の不適正

#4. 列車運行制御コンピュータ(TCC)悪性コードの感染放置
信号制御閉鎖ネットワーク内に様々なウイルス(Win32/kido.worm、Conficker.wormなど)が存在していたこと、ウイルス感染監視機能が有効でなかったことなどを指摘。

[コメント] サイバー攻撃とは直接的な関係はないと思われる。

http://gov.seoul.go.kr/files/2016/02/56b44ae5bbcfa8.55745107.pdf

(c) Institution For Transport Policy Studies, inc. 2019

鉄道分野におけるインシデント事例

- **2014年、ソウルメトロに対するサイバー攻撃**
  - 攻

#6. 列車信号・通信閉鎖網管理の不足
列車信号制御独立閉鎖ネットワーク内の信号監視用管理PCが他の外部ネットワークと通信できるLANカードを搭載し、さらに、リモートPCとの大容量ファイル転送が可能であったことなどを指摘。

[コメント] サイバー攻撃とは直接的な関係はないと思われる。

#6. 列車信号・通信閉鎖網管理の不足
#7. 重要な設備保護区域のセキュリティ管理の不適正
#8. ▲▲管制センターサイバーセキュリティ対策の不履行
#9. 個人情報の録画映像ストレージ管理の不適正
#25. 列車信号制御システムのソフトウェアセキュリティ管理不足

- 業務関連資料の流出：12件

http://gov.seoul.go.kr/files/2016/02/56b44ae5bbcfa8.55745107.pdf

(c) Institution For Transport Policy Studies, inc. 2019

鉄道分野におけるインシデント事例

- **2015年12月、カナディアンパシフィック鉄道での元従業員による不正**
  - カナディアンパシフィック鉄道で解雇を宣告されたIT業務の従業員が、退職前にネットワークコアスイッチからファイル削除、管理者アカウント削除、パスワード書き換えにより、スイッチにアクセスできないようにした。さらに自分のPCのハードディスクをワイプして証拠を隠滅した。
  - 再起動手順が功を奏してスイッチへのアクセスを回復した。また、スイッチに残っていたログ等から、FBIのフォレンジック部門の助けを得て、元従業員の犯行を特定した。

https://www.justice.gov/opa/pr/former-it-employee-transcontinental-railroad-sentenced-prison-damaging-ex-employer-s-computer

(c) Institution For Transport Policy Studies, inc. 2019

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。



ランサムウェア感染を
明らかにした
サンフランシスコ市交通局



感染の影響で
サービスを
停止した券売機

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

(c) Institution For Transport Policy Studies, inc. 2019

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月12日)の夜から土曜日(5月13日)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板に影響したが、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/

(c) Institution For Transport Policy Studies, inc. 2019

鉄道分野におけるインシデント事例

- **2017年、米国ワシントンDCユニオン駅、インドニューデリーRajiv Chowk駅の駅構内電光掲示板の乗っ取り**
  - 米国ワシントンDCユニオン駅
    - 月曜日(5月15日)の夕方、数分間、導入から数か月しか経っていない駅構内のいくつかの電光掲示板が乗っ取られた。
  - インドニューデリーRajiv Chowk駅
    - 2017年4月、駅構内のコマーシャルや広告用の大画面テレビが乗っ取られた。Wi-Fiネットワークを適切に保護しなかったことを原因としている。

https://www.usatoday.com/story/news/nation-now/2017/05/17/porn-plays-screens-d-c-s-union-station/327411001/
https://www.hackread.com/hackers-played-hardcore-porn-on-train-stations-screen/

(c) Institution For Transport Policy Studies, inc. 2019

鉄道分野におけるインシデント事例

- **2018年、イギリスGreat Western Railway、ユーロスターポータルサイトへの不正アクセス**
  - Great Western Railway
    - 2018年4月、ポータルサイトGWR.comの約1,000アカウントに対して不正アクセスが発生した。
  - ユーロスター
    - 2018年10月中旬、ポータルサイトeurostar.comに対して不正アクセスが発生した。

https://home.bt.com/tech-gadgets/tech-news/great-western-railway-cyber-attack-11364263869710
https://www.bbc.com/news/technology-46048597

(c) Institution For Transport Policy Studies, inc. 2019

鉄道分野におけるインシデント事例

- **2018年5月、デンマーク国営鉄道へのDDos攻撃**
  - 日曜日(5月13日)、DDoS攻撃によりシステム故障が発生し、同社のアプリ、チケット販売機、ウェブサイト、店舗でのチケット購入ができなくなった。

https://www.thelocal.dk/20180514/cyber-attack-hits-danish-rail-network

(c) Institution For Transport Policy Studies, inc. 2019

その他の事例

- **2009年、Norfolk Southern in Hobart 4/10/09 (Plus crossing gate hack)**



踏切警報機を
ハッキング

https://www.youtube.com/watch?v=DnTISVwQepA

(c) Institution For Transport Policy Studies, inc. 2019

その他の事例

- **2008年、Hacked the Dutch Railways - subtitled**



駅構内放送と
行先掲示板を
ハッキング

https://www.youtube.com/watch?v=9WxOo5u2dkM

(c) Institution For Transport Policy Studies, inc. 2019

その他の事例

- **2008年、Hacking a Train-Station screen with N95 Nokia**



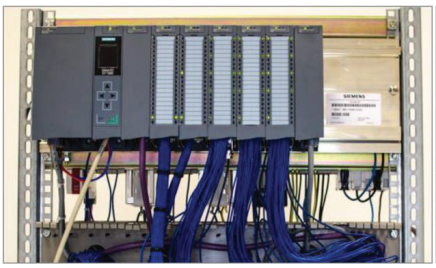
電光掲示板を
ハッキング

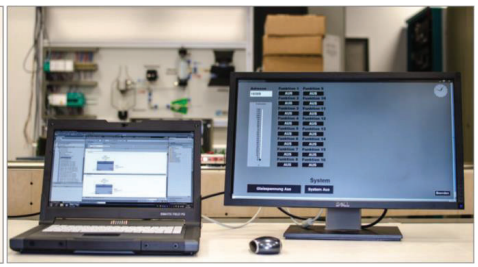
https://www.youtube.com/watch?v=K2y4lujgEVs

(c) Institution For Transport Policy Studies, inc. 2019

その他の事例

- **2015年、プロジェクト HoneyTrain**
  - 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Web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。



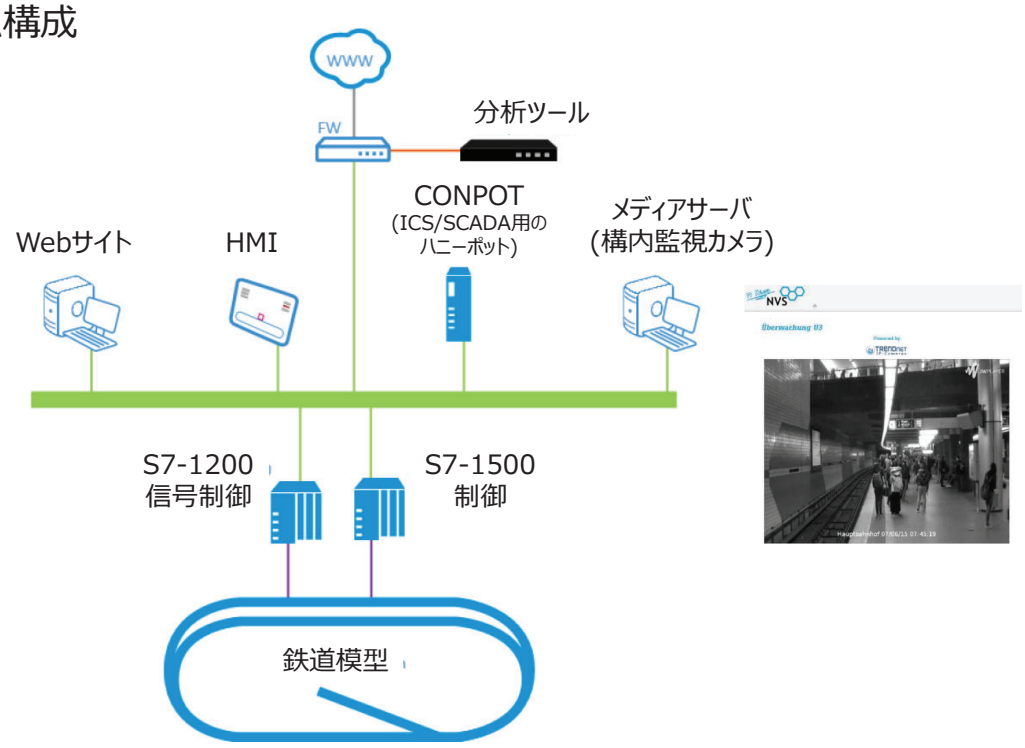


https://www.railengineer.uk/2017/05/30/hacking-the-railway/
https://www.sophos-events.com/honeytrain/downloads/Sophos_HoneyTrain_WP_EN.pdf

(c) Institution For Transport Policy Studies, inc. 2019

その他の事例

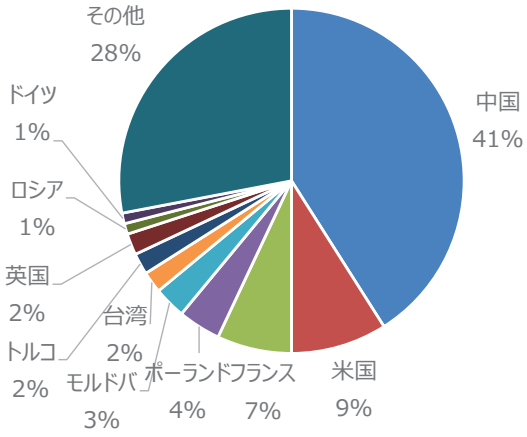
- **2015年、プロジェクト HoneyTrain**
  - システム構成



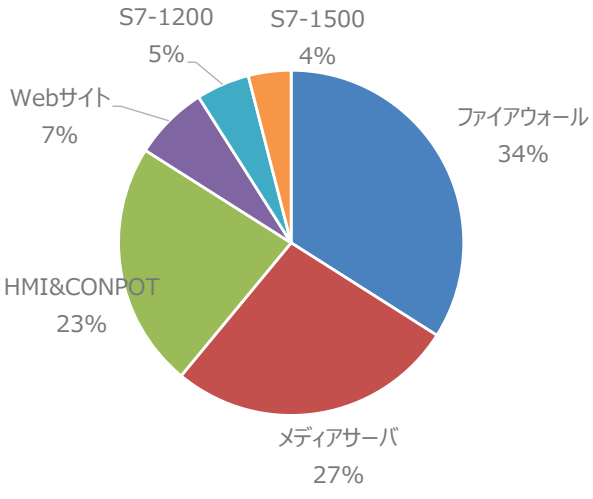
(c) Institution For Transport Policy Studies, inc. 2019

その他の事例

- **2015年、プロジェクト HoneyTrain**
  - 6週間で、計2,745,267件のサイバー攻撃を検知



攻撃元

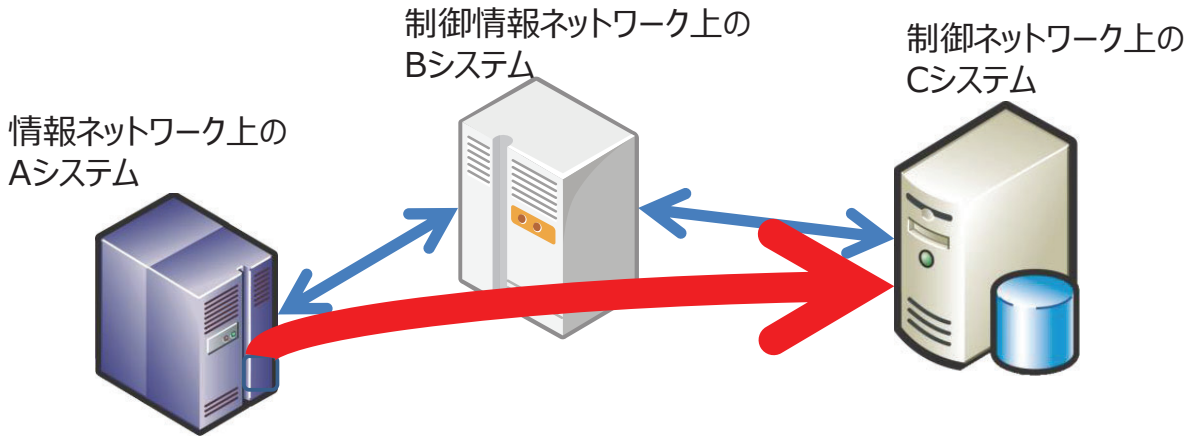


攻撃対象

(c) Institution For Transport Policy Studies, inc. 2019

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/

(c) Institution For Transport Policy Studies, inc. 2019

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**

2010年7月、イランの原子力施設を狙った攻撃(スタクスネット)
- イランの原子力施設の動作を不正に変更
  - 開発系装置をターゲットとし、実機(コントローラ)に対し、正規の手順を悪用し不正プログラムを送信
  - 監視画面上では異常検知不可(正常動作を模擬)
- マイクロソフトWindowsと独シーメンス社製ソフトウェアの脆弱性を悪用
  - 情報系(情報ネットワーク)から制御系(制御ネットワーク)まで自律的に進行

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

(c) Institution For Transport Policy Studies, inc. 2019

おさえておきたいインシデント事例

- **スタクスネットの攻撃シナリオ**

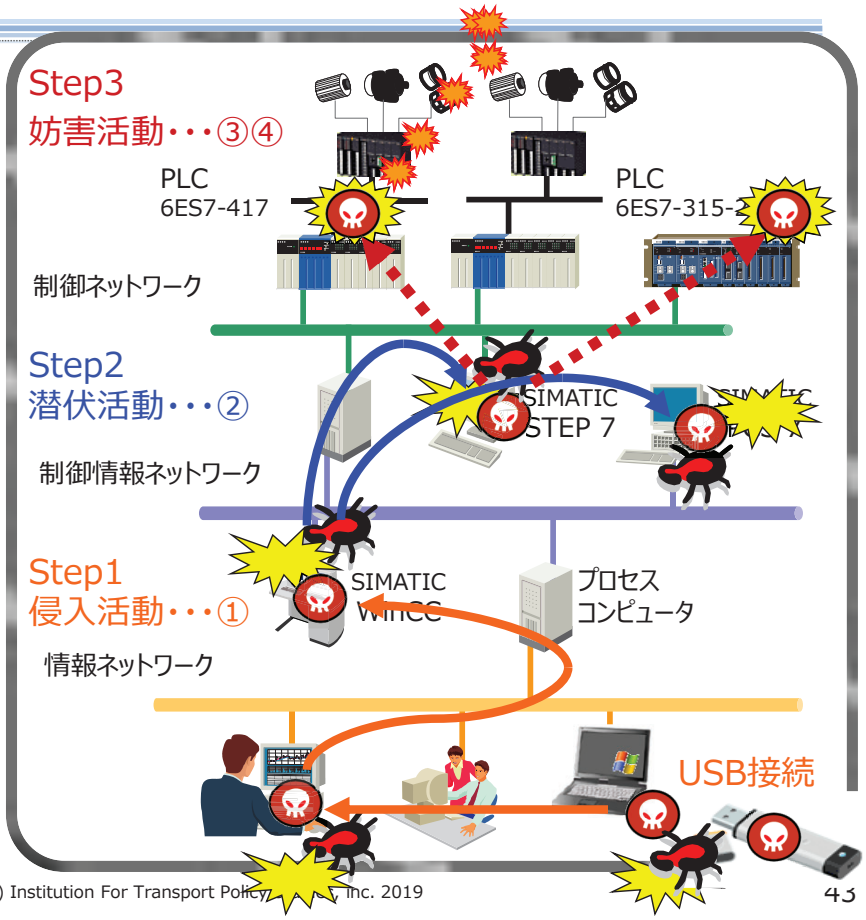
①Windowsの脆弱性を悪用してシステムに侵入

②Windows、独シーメンス社製ソフトウェアの脆弱性を悪用して感染拡大

③独シーメンス社製ソフトウェアを悪用して、PLC（プログラマブルロジックコントローラ)を侵害

④長期に渡り出力周波数を短時間のうちに変化させる
⇒制御システムの動作妨害

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



(c) Institution For Transport Policy Studies, inc. 2019

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**
- **「IPカメラ　サイバー攻撃」での検索結果**
  - 大規模DDoS攻撃は防犯カメラが踏み台に
  - 監視カメラから“史上最大級”のサイバー攻撃
  - 「ネットワークカメラ画像無断公開サイト」報道から考えるべきこと

} 可用性（業務停止の可能性）
} 機密性（情報漏えいの可能性）

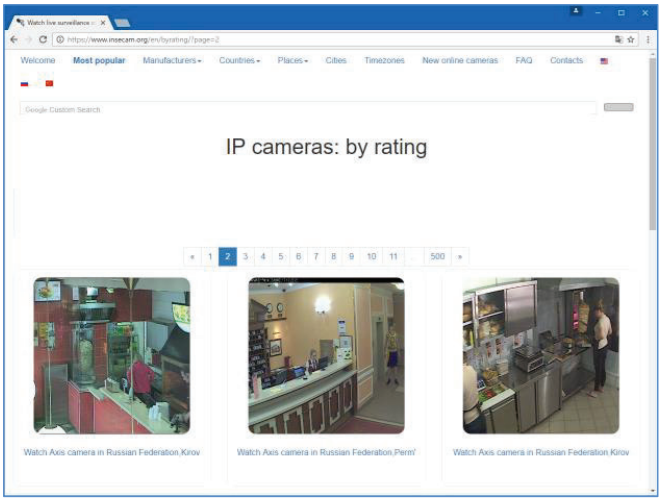
DoS攻撃(Denial of Service)は、サーバやネットワークなどに過剰な負荷をかける事でWebサービスの稼働を妨害する攻撃です。
DDoS攻撃(Distributed Denial of Service)は、攻撃元の数を増やすことで過剰な負荷をn倍化させる攻撃です。

http://www.itmedia.co.jp/enterprise/articles/1610/25/news059.html
http://itpro.nikkeibp.co.jp/atcl/watcher/14/334361/102000701/
http://blog.trendmicro.co.jp/archives/10546

(c) Institution For Transport Policy Studies, inc. 2019

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



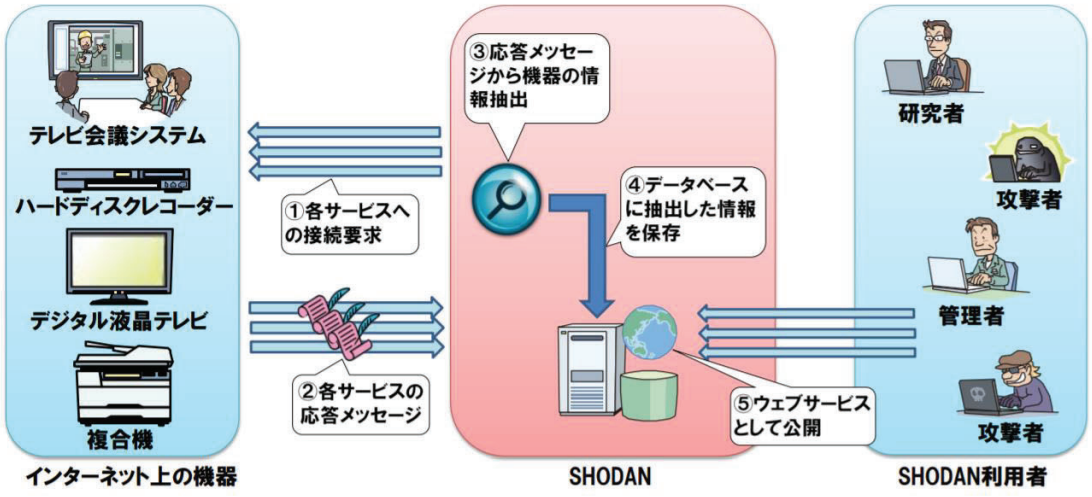


http://www.insecam.org/

(c) Institution For Transport Policy Studies, inc. 2019

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



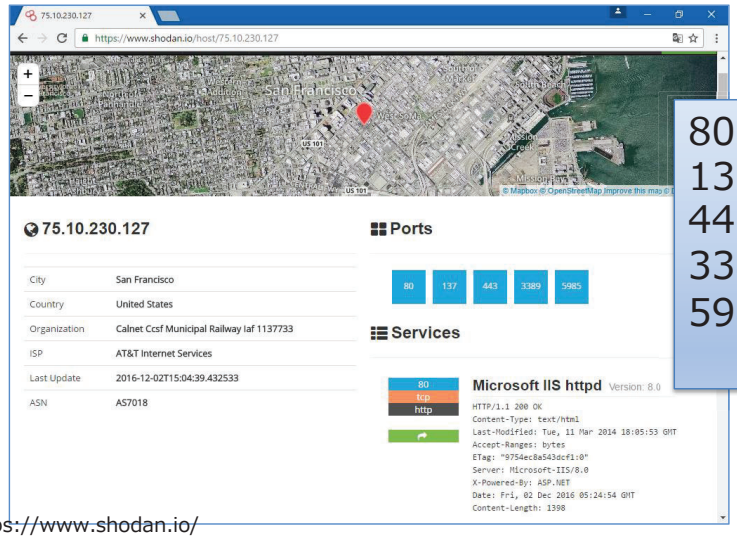
https://www.ipa.go.jp/files/000052712.pdf

(c) Institution For Transport Policy Studies, inc. 2019

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

思った以上に、米国サンフランシスコ市営鉄道の端末がインターネットに繋がっていたという事実(2016年12月2日時点)



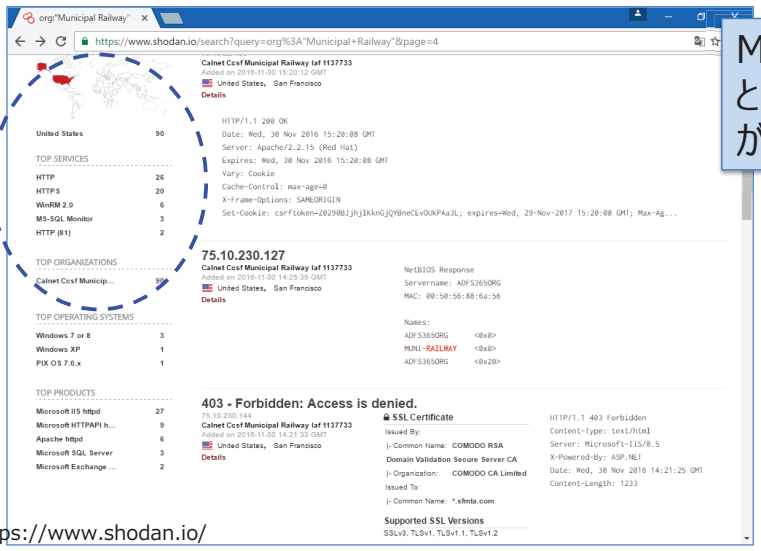
80：Web
137：NetBIOS
443：セキュアWeb
3389：リモートデスクトップ
5985：Windowsリモート管理(WinRM)

https://www.shodan.io/

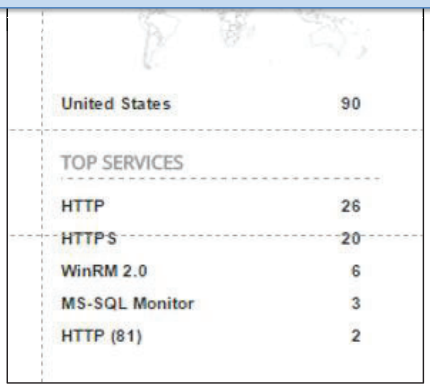
おさえておきたいインシデント事例

- **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

思った以上に、米国サンフランシスコ市営鉄道の端末がインターネットに繋がっていたという事実(2016年12月2日時点)



Municipal Railwayで検索すると、米国だけで90件のIPアドレスが存在

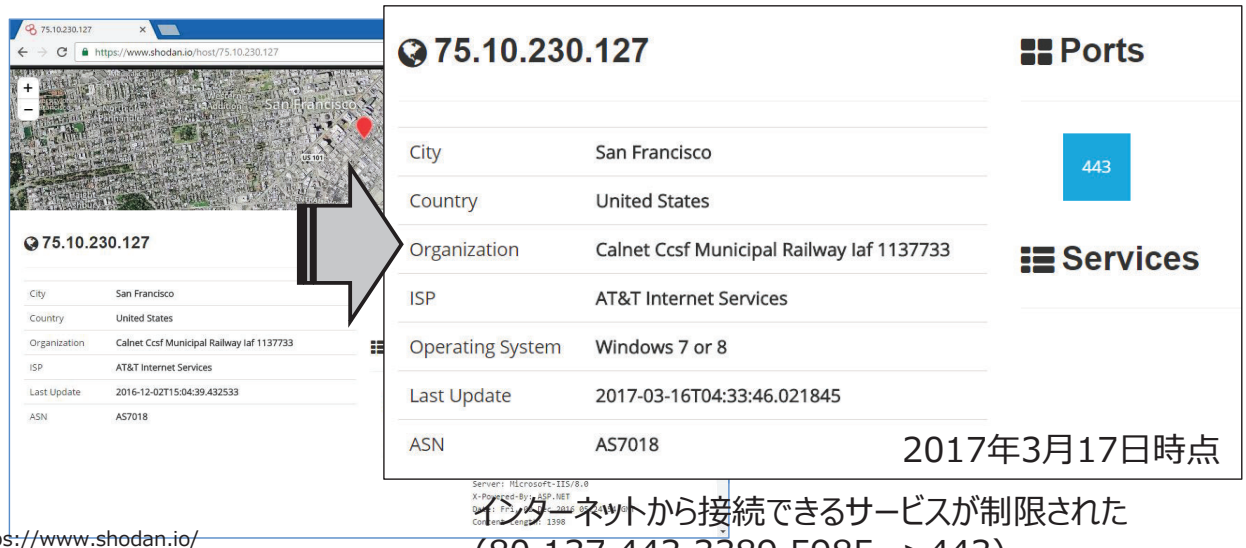


https://www.shodan.io/

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

思った以上に、米国サンフランシスコ市営鉄道の端末がインターネットに繋がっていたという事実



2017年3月17日時点

インターネットから接続できるサービスが制限された(80,137,443,3389,5985=>443)。

https://www.shodan.io/

(c) Institution For Transport Policy Studies, inc. 2019

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

思った以上に、米国サンフランシスコ市営鉄道の端末がインターネットに繋がっていたという事実



2017年3月17日時点

インターネットから接続できるIPアドレスが制限された。

https://www.shodan.io/

(c) Institution For Transport Policy Studies, inc. 2019

- 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
- **セキュリティ確保への取り組み**

旅客輸送サービスにおける安全対策
～ITセキュリティ目線から見た鉄道分野～

(c) Institution For Transport Policy Studies, inc. 2019

背景・世の中の流れ

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

(c) Institution For Transport Policy Studies, inc. 2019

新たなリスク(サイバー攻撃)の顕在化
～何が変わったのか？～

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

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

  ⇧

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



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

(c) Institution For Transport Policy Studies, inc. 2019

新たなリスク(サイバー攻撃)の顕在化
～何が変わったのか？～

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

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

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

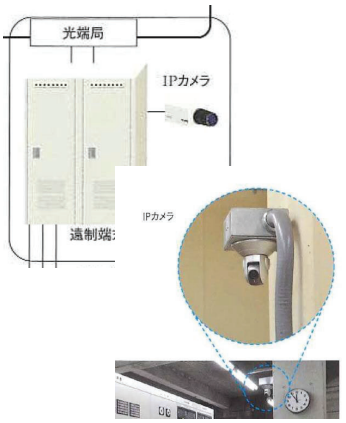
「重要インフラ情報システム信頼性研究会」報告書付録から転記

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

(c) Institution For Transport Policy Studies, inc. 2019

新たなリスク(サイバー攻撃)の顕在化
～何が変わったのか？～

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







マルチディスプレイ



京都鉄道博物館　運転指令所

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

(c) Institution For Transport Policy Studies, inc. 2019

新たなリスク(サイバー攻撃)の顕在化
～何が変わったのか？～

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

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

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

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

(c) Institution For Transport Policy Studies, inc. 2019

新たなリスク(サイバー攻撃)の顕在化
～何が変わったのか？～

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

④ **既設システムとの連携(外部から侵入される可能性)**
旅客輸送サービスの向上にあわせて、座席予約システムと改札ゲート、車両内情報表示など既設システムとの連携が進んだことにより、サイバー攻撃の影響を受ける可能性がある。さらに、にせ情報の表示による乗客の混乱や揺動など、間接的なサイバー攻撃にも配慮する必要が出てきた。

(c) Institution For Transport Policy Studies, inc. 2019

新たなリスク(サイバー攻撃)の顕在化
～何が変わったのか？～

- 欧州の鉄道分野
  国境を越えても相互運用を可能なヨーロッパ全体で共通に使用できる信号保安システムERTMS(European Rail Traffic Management System)の構築と、その中でGSM(Global System for Mobile communications)に由来する無線技術ならびにTCP/IP技術が使われ、普及している。

  - **SECRET(SECurity of Railways against Electromagnetic aTtacks)プロジェクト(2012年～2015年)**
    電子伝送を妨害したり、電子システムを損傷したりする可能性のある電磁攻撃(EM)について検討を行い、脅威のシナリオ、結果、予防および復旧ソリューションを調査レポートとして報告している。
  - **CYRAIL(CYbersecurity in the RAILway sector)プロジェクト(2016年～2018年)**
    鉄道の信号および通信システムを対象に、運用シナリオ、セキュリティ評価、脅威分析、攻撃検出、早期警告、緩和と対策、保護プロファイルなど、鉄道のサイバーセキュリティ評価に関する推奨事項をまとめ報告している。

https://cordis.europa.eu/project/rcn/104352/reporting/de
http://cyrail.eu/IMG/pdf/final_recommendations_cyrail.pdf

(c) Institution For Transport Policy Studies, inc. 2019

新たなリスク(サイバー攻撃)の顕在化
～何が変わったのか？～

- 国際鉄道連合(International Union of Railways)
  鉄道のサイバーセキュリティは、インターロックシステム、速度制御(ATP)、トラフィック管理(ATS)、自動運転(ATO)、SCADA、換気、遠隔監視、鉄道の管理システム、インフラとしての通信など対象範囲が幅広いことと共に、信号システムに関しては、IPネットワークなどのITシステムの積極的な取り込みによるメリット享受だけではなく、新しいセキュリティリスクを想定しなければならない。特に、信号システムでのIPネットワークなどのITシステムの積極的な取り込みは、汎用のプロトコルや機器を使用することによる仕様面でのオープン化、接続の拡張によってもたらされる国を越えた分散ネットワークは、接続ポイントを多数提供することとなり、接続面でのオープン化が進むことを指摘している。

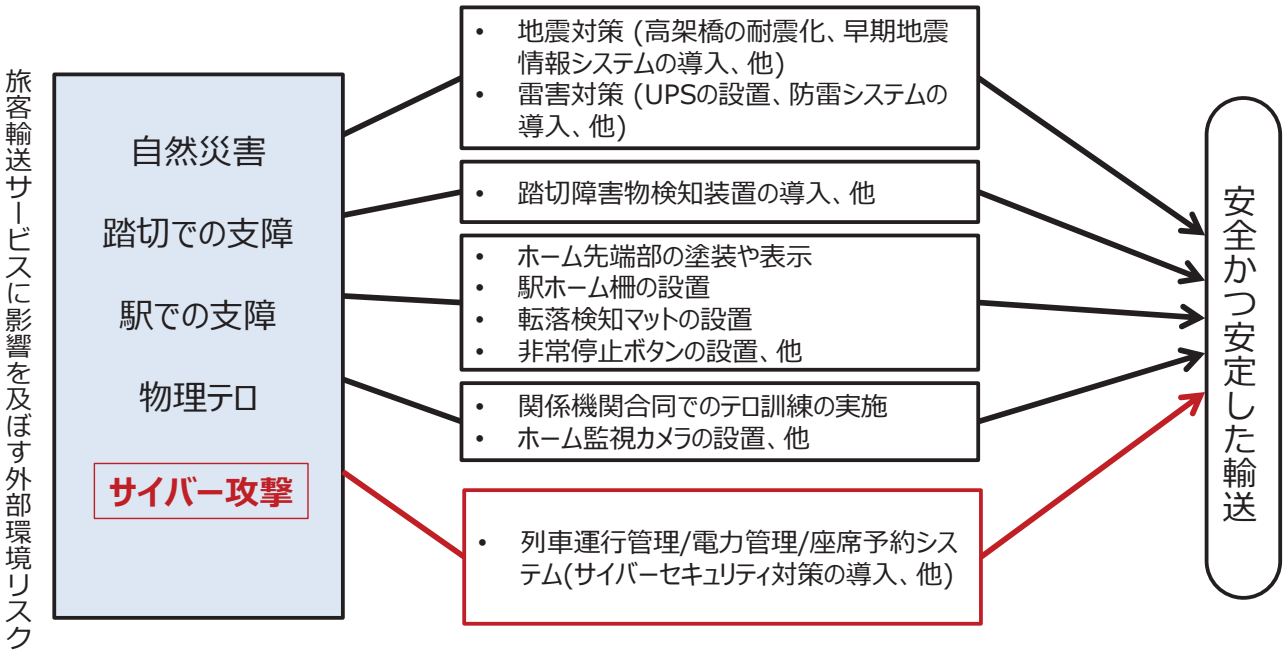
  - **Guidelines for Cyber-Security in Railways(2018年6月)**
    鉄道の信号システムと通信システムを対象として、「システム設計」を考慮したISO27001を用いたセキュリティ評価についてまとめている。

Guidelines for Cyber-Security in Railways
https://www.shop-etf.com/en/guidelines-for-cyber-security-in-railways

(c) Institution For Transport Policy Studies, inc. 2019

旅客輸送サービスにおける安全対策

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



(c) Institution For Transport Policy Studies, inc. 2019

旅客輸送サービスにおける安全対策

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

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

(c) Institution For Transport Policy Studies, inc. 2019

旅客輸送サービスにおける安全対策

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

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

(c) Institution For Transport Policy Studies, inc. 2019

旅客輸送サービスにおける安全対策
~対策にあたり留意しておきたいポイント~

- **外部から侵入される可能性**
  - 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。

(c) Institution For Transport Policy Studies, inc. 2019

旅客輸送サービスにおける安全対策
～対策にあたり留意しておきたいポイント～

- **侵入されてから被害につながる可能性**
  - 複数のシステム連携を踏まえたセキュリティ対策
    - 鉄道分野の主要なシステムは、複数のシステムを連携させて構築していることから、複数のシステムが連携することを踏まえたセキュリティ対策の推進が必要である。

AシステムとBシステム間のセキュリティ対策、BシステムとCシステム間のセキュリティ対策だけではなく、Bシステムを介したAシステムとCシステムのセキュリティ対策など、踏み台攻撃に備えた対策を考慮しておく必要がある。

(c) Institution For Transport Policy Studies, inc. 2019

旅客輸送サービスにおける安全対策
～対策にあたり留意しておきたいポイント～

- **事案が発生する可能性**
  - 事案発生時の対応を踏まえたセキュリティ対策
    - 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。

(c) Institution For Transport Policy Studies, inc. 2019

セキュリティインシデントから学べること
～鉄道分野に関連するインシデント事例～

END

(c) Institution For Transport Policy Studies, inc. 2019

2020年
サイバーテロの可能性と経営としての監査役の役割

2020年1月29日（水）
丸山司郎

ねらい

SEからセキュリティ専門家を経て社長を経験した者として

サイバーテロへの対策と発生した場合の対応について

経営者に求められる責任を説明し

自社に準備に役立ていただく。



東京
オリンピック

2020年
7月24日（金）～8月9日（日）

あと 177日

約 半年



混雑予想
8月7日
8:00～9:00

駅 朝ラッシュ時間帯（7:00～10:00）
- ● 普段の朝ラッシュよりも混雑（観客等の影響がかなりある）
- ● 普段の朝ラッシュよりも混雑（観客等の影響がある）

駅 朝ラッシュ以外の時間帯（5:00～7:00、10:00～24:00）
- ○ 普段の朝ラッシュ並みに混雑（観客等の影響がかなりある）
- ○ 普段の朝ラッシュ並みに混雑（観客等の影響がある）

路線
- かなり混雑（観客等の影響がある）
- かなり混雑（観客等の影響がほとんどない）
- やや混雑（観客等の影響がある）

大会輸送影響度マップ
https://2020tdm-tokyo.maps.arcgis.com/apps/opsdashboard/index.html#/634ef9f430514f0caebf27e0277c178a



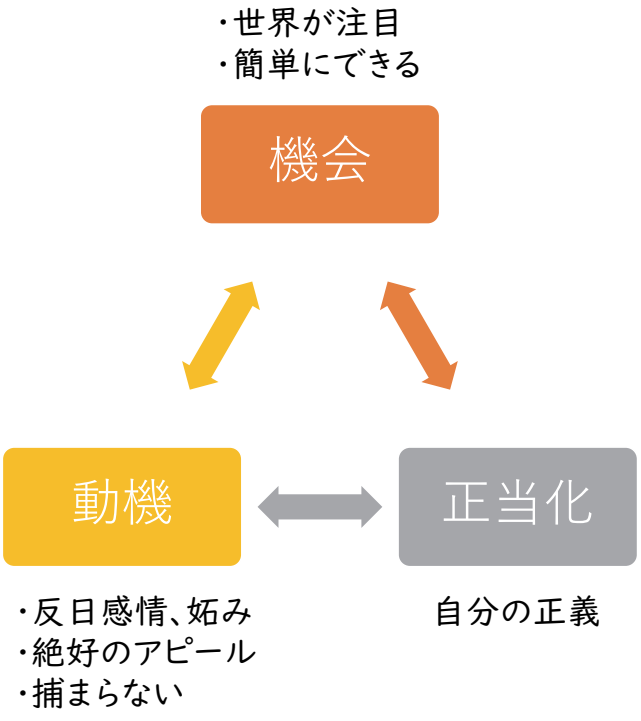
サイバー攻撃対策

Q１：経営会議で毎月、対策会議を開催している。

Q２：昨年よりサイバーセキュリティ予算がかなり増加している。

Q３：昨年より情報セキュリティ部門の要員が増加している。

サイバーテロの可能性



	脅威	理由
1	好き嫌い 悪ふざけ	極端な好き嫌いや、悪ふざけが度を越すと、常識を超えた行動につながる。
2	貧困	インターネットが世界をつなげたことで、 つかまることのない犯罪が可能になった。
3	組織犯罪	アングラ経済は実在し、犯罪活動の道具としてインターネットを活用している。 カード詐欺、麻薬売買、武器、人身売買
4	貿易・経済行為	国境のないインターネット上で行われる貿易や経済行為に、各国の法制度が追い付けない。税制、為替、情報保護、産業スパイ
5	イデオロギー	宗教、民族、主義などが過激になると、テロ行為が正当化され英雄視される。アノニマス、など
6	戦争・紛争	インターネットは第5の戦場と呼ばれ、すでに国家間の戦争が行われているが、表面化しない。Wikileaksなどで暴露される





ロシア
東京五輪参加禁止

- 11月28日、世界反ドーピング機関（ＷＡＤＡ）が、２０２０年東京五輪・パラリンピックを含む主要大会からロシア選手団を４年間排除する処分を決めた。
- 12月24日、ロシアは不服申し立て
- 1月9日、スポーツ仲裁裁判所に（ＣＡＳ）に仲裁を要請する手続き
- 最終的な判断は３月から４月ごろになるという見方



最悪の日韓関係

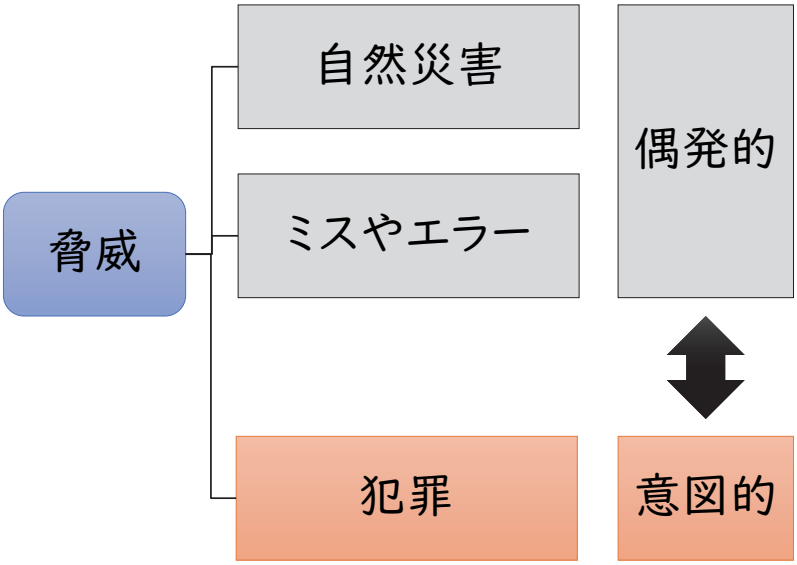
- 2018年、新日鐵住金を被告とした「徴用工」による損害賠償の判決
- 韓国政府、「日韓請求権協定」の外交的協議に応じることはなく、この問題を放置
- 8月2日、日本政府が一部半導体関連物品の輸出規制措置（いわゆる「ホワイト国除外」）
- 日本製品の不買運動と日本への旅行中止を呼びかける「NO JAPAN」運動
- 2020年に開かれる東京オリンピック・パラリンピックのボイコット論
- 8月22日、韓国政府が日韓両国間のGSOMIA（軍事情報包括保護協定）の破棄を通告することで安全保障分野にまで拡大
- 協定失効直前の11月22日、韓国政府が「破棄通告の効力を停止」を発表



トランプ大統領 イラン司令官の殺害指示

- 12月27日、武装勢力ヒズボラが、イラク軍基地をがロケット弾で攻撃。アメリカの民間人1人が死亡、アメリカ兵4人とイラク治安部隊2人が負傷
- 12月31日、シーア派成員、バグダード市内で数千人の抗議活動を展開。アメリカ大使館前に集結して放火、侵入を試みるなどして暴徒化
- 1月3日、イランのバグダード国際空港付近にて、ロケット弾3発による攻撃を受けヒズボラの最高指導者アブ・マフディ・ムハンディスとイランのソレイマニ司令官ら8名が死亡
- 1月3日、トランプ大統領は自らの指示でアメリカが攻撃を加えたことを発表
- 1月4日、米、イラク国内の緊張を受けて第82空挺師団の増派を決定
- 1月8日、イスラム革命防衛隊は報復として在イラク米軍基地を弾道ミサイルで攻撃
- 1月8日　イラン戦争間近？　twitterで＃WW3がトレンド入り
- イランは親日とはいわれれいるが、テロ組織の「ヒズボラ」や「ハマス」に資金や武器を与えている。
- DDoS流れ弾・便乗サイト改ざん

コンピュータ・セキュリティ 犯罪対策と災害対策　1981年

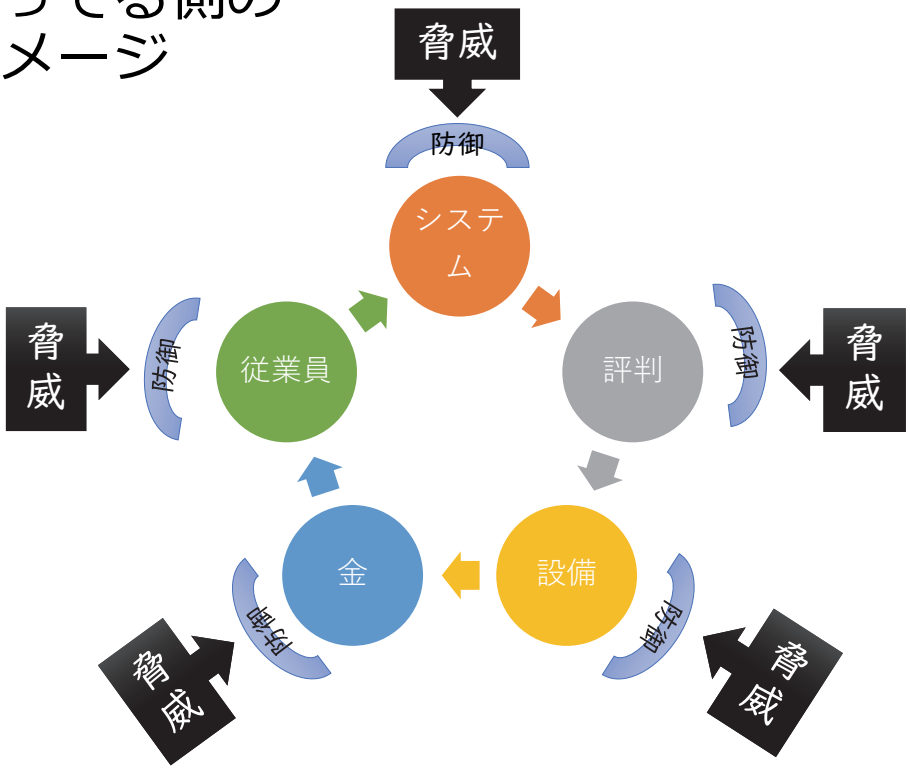


今までの経験則から予測することができる。

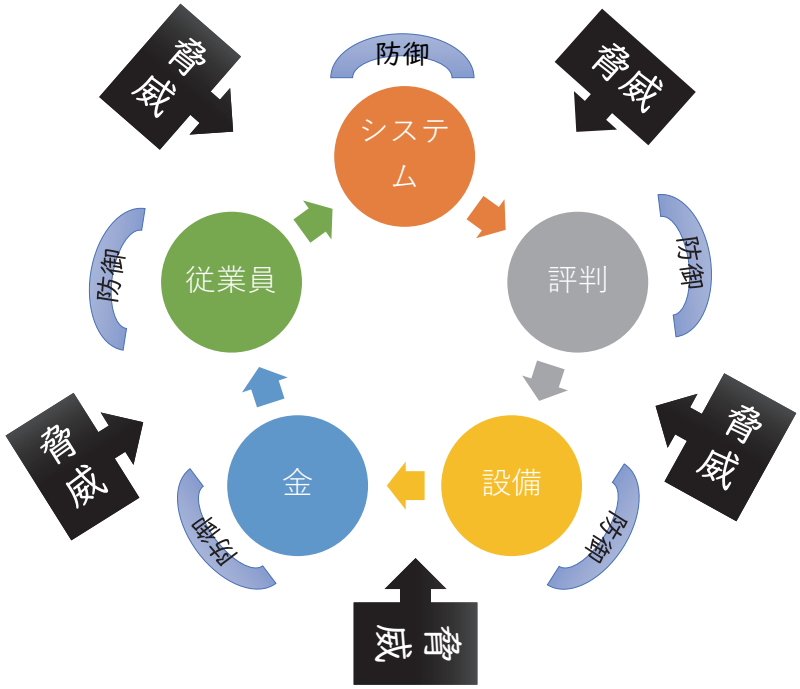
□ チェックリスト的対策

安全対策の裏をかこうとするため、強化した場所を避けて**防備の不充分な所から攻撃**をしかける。

守ってる側のイメージ



現実



サイバー攻撃の実例

2019年ラグビー
ワールドカップ

2018年
平昌オリンピック

ラグビー　ワールドカップ

【社会】

ラグビーW杯期間中、サイバー攻撃相次ぐ　五輪中継妨害への準備か

ツイート B! 0 シェア 0

2019年12月17日 朝刊

ラグビー・ワールドカップ（W杯）の日本大会期間中に、テレビ放送システムを狙ったサイバー攻撃が相次いだことが、大会組織委員会への取材で分かった。政府関係者は「来年の東京五輪・パラリンピックのテレビ中継を妨害する準備が行われている」と警戒を強めている。

組織委によると、サイバー攻撃はシステムに大量のデータを送りつけて機能を停止させる「ＤＤｏＳ（ディードス）攻撃」。大会期間中に十二回あり、主に放送局が使う組織委のシステムが狙われたが、実害はなかった。

攻撃の多くに日本国内の機器が使われたが、実際の攻撃元は判明していない。情報セキュリティーの専門家は「多くの人が視聴するテレビ放送が止まれば影響は甚大だ」と懸念した。

ラグビーW杯では他に、偽メールを送って大会職員のパスワードを盗もうとする「フィッシング」や、大会職員が海外サイトを閲覧してウイルス感染する被害もあった。

平昌　オリンピック

【平昌五輪】

サイバー攻撃か？！　開会式のさなかにネットがダウン　国防省も巻き込んで原因調査中

平昌五輪スタジアムで平昌冬季五輪の開会式が行われていた最中、五輪組織委員会がサイバー攻撃を受けていた可能性が浮上し、専門家が原因などの調査を進めていることが１０日、明らかになった。

韓国メディアなどの報道によると、開会式が始まる４５分前の９日午後７時１５分ごろから、組織委内部のインターネットやＷｉ－Ｆｉ（ワイファイ）がダウンした。１０日正午の時点ではまだ完全復旧に至っていないと報じられた。

組織委の宋百裕報道官は報道陣に対し、「重要性が低いシステムのいくつかが影響を受ける事案があった。不便をかけたことを陳謝する」と述べたうえで、「開会式へは影響がなかった。選手や観客の安全にもまったく影響がなかった」と強調した。

しかし、ロイター通信によると、開会式では予定していた小型無人機（ドローン）を飛ばすことができず、事前に録画した映像を使用した。システム障害との関連は明らかになっていないが、国際オリンピック委員会（ＩＯＣ）の広報担当者は「突然の計画変更でドローンを展開することができなかった」と、サイバー攻撃の影響を匂わせた。

https://www.sankei.com/pyeongchang2018/news/180210/pye1802100060-n1.html

産経ニュース

サイカル journal by NHK
SCIENCE & CULTURE

“オリンピックを破壊する”～サイバー攻撃、驚愕の実態～

攻撃は、突然に始まった

「リオ、ロンドンとは全く違う、オリンピックを妨害する明確な目的をもった攻撃だったと思う。ピョンチャンオリンピックが成功しないおそれもあっただろう」



https://www.nhk.or.jp/d-navi/sci_cul/2019/06/story/story_190613/

サイバー攻撃対応チームの総括責任者
「イグルーセキュリティ」チョ・チャンソブ副社長

「最初に異変についての情報がもたらされたのは、去年２月９日の午後７時頃、**開会式の１時間前**でした」

ＩＴサービス会社が運用する大会のシステムの一部に不具合が起きたが、「システム障害」との報告だったため、サイバー攻撃対応チームは出動しなかった。

しかし、開会式が始まった午後８時、会場の無線ＬＡＮが使えなくなったり、チケットの印刷が出来なくなったりするなど、トラブルが相次ぐ。

「多数のシステムが同時多発的に問題を起こし、**大会のサーバーの画面が青一色になって再起動も出来なくなった**。ウイルスによるサイバー攻撃と判断しました」

分析したところ、攻撃を受けたのは、観客の入退場から大会関係者のインターネット接続まで、あらゆる認証作業に必要な、大会の根幹を担うサーバーだと分かった。

開会式が終わるのは夜１０時。混乱を防ぐため、無線ＬＡＮや入退場システムなど、最低限の応急処置した上で、バックアップのサーバーを使って全体の復旧作業を急ぐことにした。

データセンターには、ネットワーク構築やサーバー管理など、各分野のプロおよそ２５０人が続々と駆けつけた。

ところが、作業開始後、さらに深刻な事態が判明した。**サーバーを１台復旧すると、ウイルスの変種が現れて別のサーバーに感染**していったのだ。

攻撃に使われたのは、「拡散型」と呼ばれる極めて悪質なウイルスだった。現場では驚きの声があがったという。

「攻撃は認証システムを通じて、ＩＤとパスワードを乗っ取った状態で始まりました。乗っ取ったアカウントから認証システムを破壊し、その認証システムがウイルスを連鎖的に伝播する攻撃となったのです」

被害は、認証用のサーバーを発信源に５０のサーバーに及び、大会に関わる５２のサービスが影響を受けた。

攻撃者の狙いは、単なる示威行為ではなく、**大会の破壊にある**ことは明らかだ。

このままでは、大会そのものに影響が出かねない。午前０時、これ以上の拡散を防ぐため、大会のインターネットを遮断した。

「これは時間との闘いだから、人員を追加投入して、変種のウイルスをひとつずつ見つけて治療する作業を繰り返しました。最終的に検出されたウイルスは、およそ４０種にのぼったのです」

復旧作業が終わったのは、競技開始が１時間後に迫った翌日の午前８時。徹夜で対応にあたった結果、競技の運営に支障が出る最悪の事態は避けられた。

今回の攻撃を分析した結果、ウイルスの感染は、オリンピックの組織委員会の内部ではなく、大会に関連する**海外のＩＴサービス会社から始まっていた**。

ウイルスは、ここの端末に保管されたＩＤやパスワードを盗み、組織委員会のサーバーへ移動していた。

こうした動きは、大会の**少なくとも３か月前から始まり、開会式に合わせてウイルスが作動する**ように仕組まれていたとみられている。

「いくら準備しても攻撃は必ずある。国家的行事では最悪のシナリオを想定して訓練すべきだ」

https://www.nhk.or.jp/d-navi/sci_cul/2019/06/story/story_190613/



サイバー紛争の真実

32件の現実に発生した、サイバーにおける紛争事例

https://drive.google.com/file/d/1wYaGNbrQXyJuDjrrOoRWIv99f9PX_N5C/view

The New York Times

U.S. Cyberattack Hurt Iran's Ability to Target Oil Tankers, Officials Say



By Julian E. Barnes

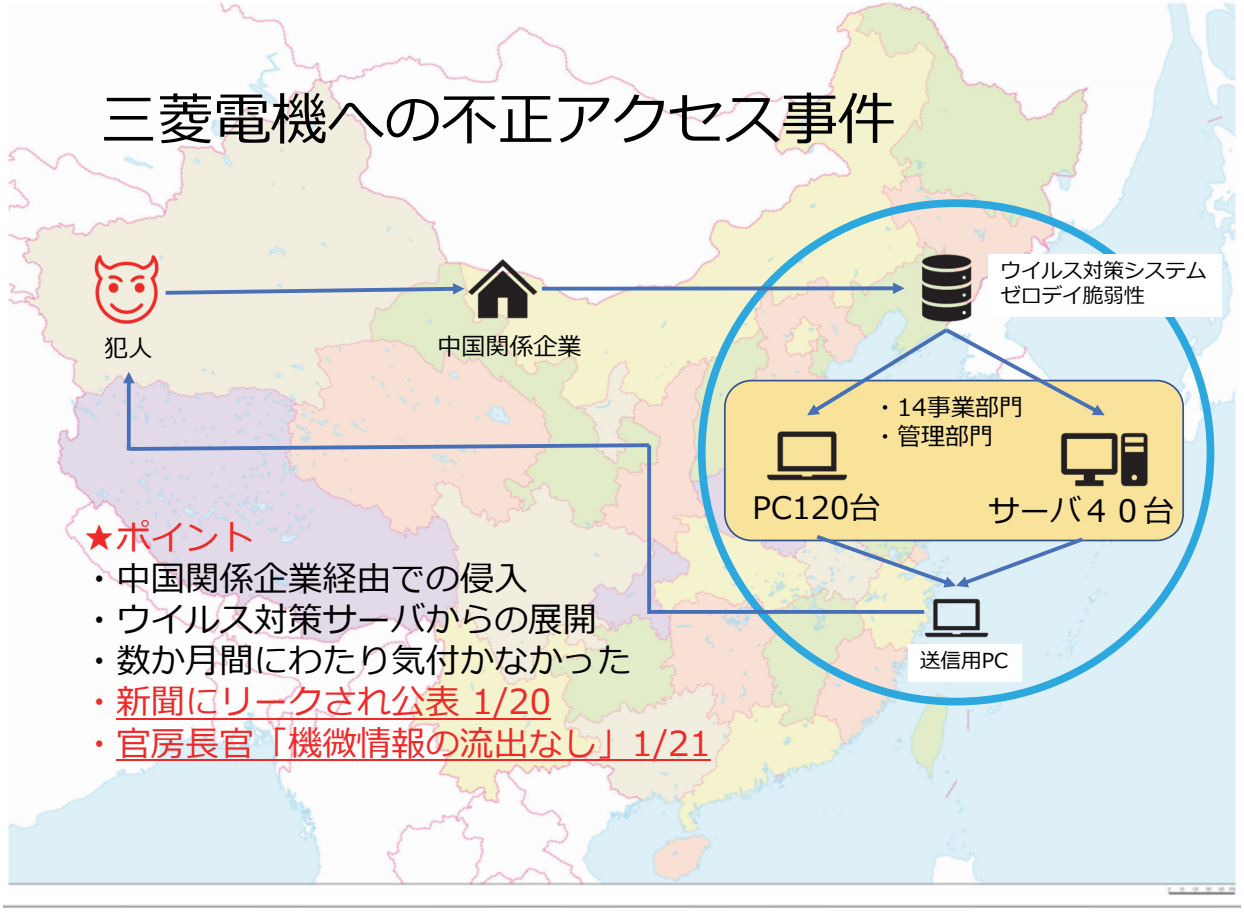
Aug. 28, 2019

WASHINGTON — A secret cyberattack against Iran in June **wiped out a critical database** used by Iran's paramilitary arm to plot attacks against oil tankers and degraded Tehran's ability to covertly target shipping traffic in the Persian Gulf, at least temporarily, according to senior American officials.

Iran is still trying to recover information destroyed in the June 20 attack and restart some of the computer systems — including military communications networks — taken offline, the officials said.

https://www.nytimes.com/2019/08/28/us/politics/us-iran-cyber-attack.html

三菱電機への不正アクセス事件

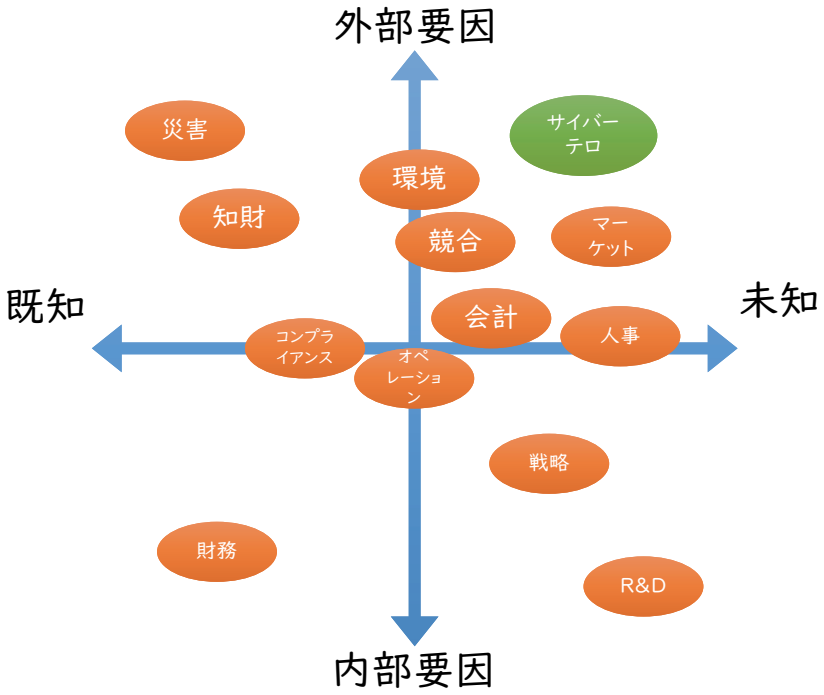


★ポイント
- 中国関係企業経由での侵入
- ウイルス対策サーバからの展開
- 数か月間にわたり気付かなかった
- 新聞にリークされ公表 1/20
- 官房長官「機微情報の流出なし」1/21

重要インフラ企業の経営者に求められる責任

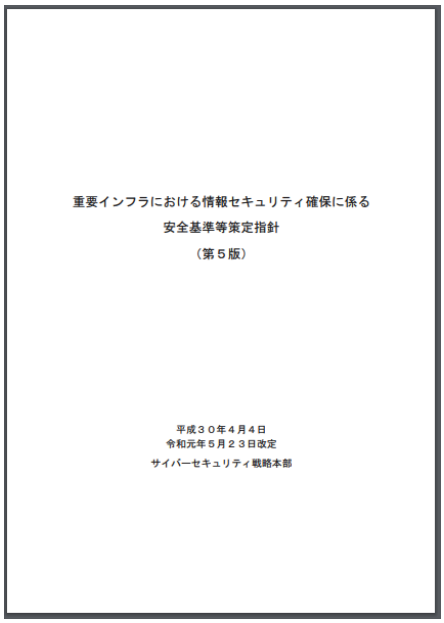
- 経営リスクに占める、サイバーテロの位置づけ
- 善管注意義務を果たしているか
- ちゃんとやったと、説明できるか
- クライシスコミュニケーションの体制は

経営リスクに占める、サイバーテロの位置づけ



内閣官房　サイバーセキュリティ戦略本部

重要インフラにおける情報セキュリティ確保に係る安全基準策定指針（第5版）


重要インフラにおける情報セキュリティ確保に係る
安全基準等策定指針
（第５版）

平成３０年４月４日
令和元年５月２３日改定
サイバーセキュリティ戦略本部

● **経営層に求められる行動**

「情報セキュリティリスク」は「機能保証の考え方」を踏まえた事業運営を不確かにする影
響力があることを認識し、その対処の在り方を判断するために必要な情報セキュリティリス
クアセスメントの実施を指示すること。また、情報セキュリティ対策のＰＤＣＡサイクル推進に当たり、必要な資源（予算・体制・人材等）の継続的な確保及び適切な配分に努めること。
さらに、情報セキュリティリスクへの対応結果が事業に与えた効果と影響を定期的に検証し、情報セキュリティリスク対応戦略の見直しの必要性等について意思決定を行うこと。これらの取組に際して、「企業経営のためのサイバーセキュリティの考え方」、「**サイバーセキュリティ経営ガイドライン**」等を参照すること。

次ページへ

機能保証の考え方

重要インフラサービスは、それ自体が国民生活及び社会経済活動を支える基盤となっており、その提供に支障が生じると国民の安全・安心に直接的かつ深刻な負の影響が生じる可能性がある。このため、各関係主体は、重要インフラサービスを安全かつ持続的に提供するための取組（機能保証）が求められる。

なお、本行動計画において、「機能保証」とは、各関係主体が重要インフラサービスの防護や機能維持を**確約することではなく**、各関係主体が重要インフラサービスの防護や機能維持のためのプロセスについて責任を持って請け合うことを意図している。すなわち、各関係主体が重要インフラ防護の目的を果たすために、情報セキュリティ対策に関する**必要な努力を適切に払うこと**を求める考え方である。

（「重要インフラの情報セキュリティ対策に係る第４次行動計画」からの抜粋）

サイバーセキュリティ経営ガイドライン

経営者が認識すべき3原則

1. 経営者は、サイバーセキュリティリスクを認識しリーダーシップによって対策を進めることが必要

特徴

2. 自社のみならず、ビジネスパートナーや委託先も含めたセキュリティ対策が必要

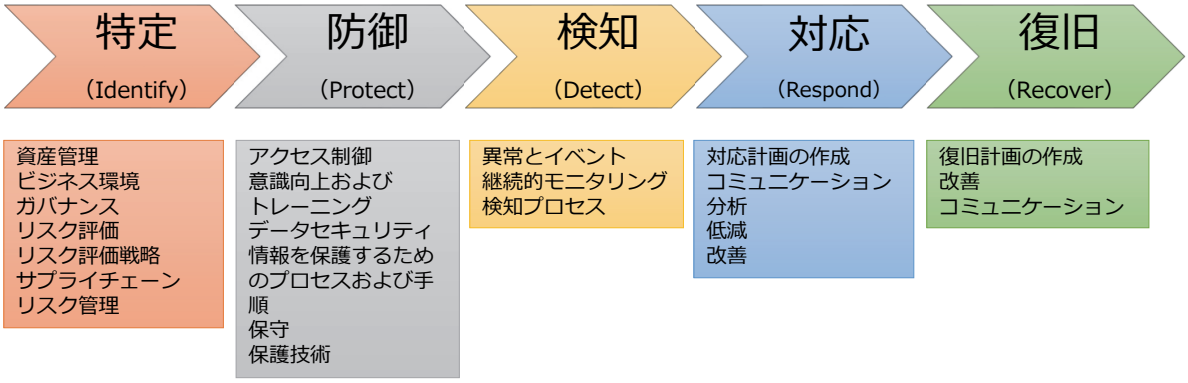
3. 平時及び緊急時のいずれにおいても、関係者との適切なコミュニケーションが必要

サイバーセキュリティ経営ガイドライン

実質的な意味

1. サイバーセキュリティは経営者の責任であると**国が明言**した。
2. 炎上する事件が起きた場合に、経営者に対して**善管注意義務**を果たせと国が指導できる。
3. 将来、**裁判**が起きた場合に、2015年時点でこのようなガイドがあったと**判断材料**として経営者の責任が問われる。

NIST
サイバーセキュリティ・フレームワーク



サブカテゴリ
(108 のアクティビティ)

監査役

権限

- 取締役の職務執行を監査すること

役割

- 将来の不祥事につながると思われるリスクに対しては、監査を通じて、取締役をはじめ各事業部門に対して適時・適切に監査意見を述べたり注意喚起をすることにより、不祥事を防止する

義務

- 仮に、監査役が取締役の不正行為もしくは法令・定款違反の事実やそのおそれがあると認めたときには、取締役（会）に報告する

株主代表訴訟と監査役

1．株主が取締役の責任を追及する場合、**まず、監査役に対して**取締役の責任を追及するように書面により提訴請求する

2．監査役は、株主からの提訴請求に対して**60日間で調査し、結論**を出さなければならない。法務部門や内部監査部門に調査を依頼したり、結論を求めることはできない。

3．監査役が取締役の責任追及をしないと判断した場合、当該株主は裁判所に対して、取締役の責任追及の訴えを提起することができる。

4．仮に、監査役が調査した結果、提訴請求対象取締役に法的責任があり、会社の損害と違法行為との間に相当の因果関係が存在すると判断すれば、監査役が会社を代表して、当該取締役の責任追及の訴えの提起を裁判所に対して行う。



東京
オリンピック

あと 177日

- 時間がない
- 人が足りない
- 専門家がいない

プラン B
大きなミスを避けて、無難にいきましょう作戦

ちゃんとやっているか、現場に確認する。

サイバー保険に入る。

何かあった時の言い訳を考える。

プラン A
オリンピック後も役立つ節目作戦



経営者が直接セキュリティの現場に行って、
毎月（６回）話を聞く



経営者がインシデント事例３つ（DDoS、平昌、三菱）の
訓練をする



外部のプロに、穴を探してもらう。
（ペネトレーションテスト）

ありがとうございました。

サイバーセキュリティの監査

1月29日
特定非営利活動法人日本セキュリティ監査協会
エグゼクティブフェロー
永宮直史

Copyright2020 Japan Information Security Association All rights reserved

CONTENTS

0. 自己紹介
1. 情報セキュリティとサイバーセキュリティ
2. サイバーセキュリティのリスク判断
3. ガバナンス・マネジメント・コントロール
4. 基本となる情報セキュリティ監査
5. サイバーセキュリティの監査
6. 監査役の役割

Copyright2020 Japan Information Security Association All rights reserved

自己紹介

■ 永宮　直史　（ながみやただし）

- 特定非営利活動法人　日本セキュリティ監査協会　エグゼクティブフェロー
- 公認情報セキュリティ主席監査人
- 委員等
  - ◆ 政府機関におけるクラウドサービスの安全性評価に関する検討会委員
  - ◆ 産業サイバーセキュリティ研究会WG1第３層TF　構成員
  - ◆ エネルギー・リソース・アグリゲーション・ビジネス検討会サーバーセキュリティWG委員
  - ◆ ISO/IEC JTC1 SC27 WG1及びWG4国内委員
  - ◆ クラウドセキュリティコントロール標準化専門委員会委員（2016年度まで）
  - ◆ IoTセキュリティガイドライン SC 27/WG 4対応 小委員会委員
- 2015年　情報セキュリティ文化賞受賞、2019年　標準化貢献賞受賞
- 略歴
  - ◆ 1973年野村総合研究所入社；公共政策立案等のコンサルティング
  - ◆ 1996年インターネット事業関連部署の事業企画室長（セキュリティ事業立上）
  - ◆ 1999-2002年ソウル支店長（地域計画、インターネット事業調査）
  - ◆ 2002-2006年日米合弁のセキュリティベンチャー企業CTO、CSO
  - ◆ 2006-2011年金融持ち株会社情報セキュリティ事務局
  - ◆ 2011-2019年8月　日本セキュリティ監査協会事務局長
  - ◆ 2019年9月-　現職

Copyright2020 Japan Information Security Association All rights reserved

1.情報セキュリティとサイバーセキュリティ

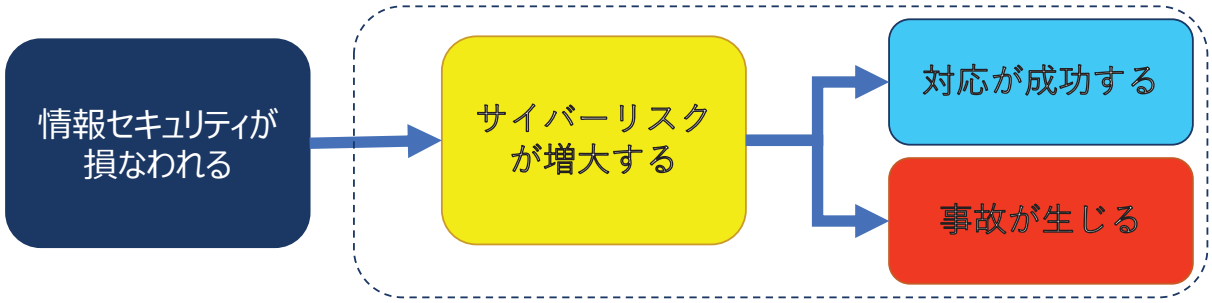
2. サイバーセキュリティのリスク判断
3. ガバナンス・マネジメント・コントロール
4. 基本となる情報セキュリティ監査
5. サイバーセキュリティの監査
6. 監査役の役割

Copyright2020 Japan Information Security Association All rights reserved

概念の比較

	情報セキュリティ	サイバーセキュリティ
定義	機密性・完全性・可用性を守ること	サイバーリスクから人・組織・社会の安全を保つこと
範囲	情報（デジタル、アナログ、物理媒体）	サイバー空間
リスク	情報の棄損	人的・物的損害

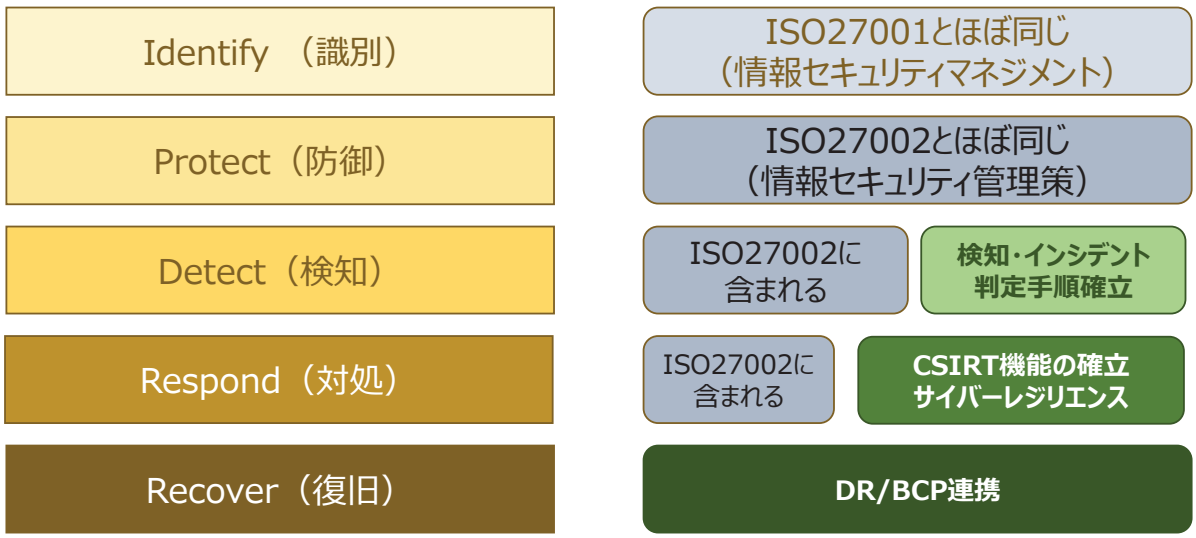
※サイバーリスク：サイバー空間における脅威がもたらすリスク
サイバー空間：ネットワーク、サービス、システム及びプロセスにより相互接続されたデジタル空間
事件事故の対処は既存のフィジカルな対応で行う



【情報セキュリティ】　【サイバーセキュリティ】

Copyright2020 Japan Information Security Association All rights reserved

サイバーセキュリティとISMS



（サイバーセキュリティフレームワーク）　（ISMS）

Copyright2020 Japan Information Security Association All rights reserved

サイバーセキュリティの要点

要点１

リスク評価

- ■ 人的・物的被害に着目したリスク評価
  - ◘ ISO31000に基づくリスク評価を追加
    - ✓ めったに生じないが、甚大な被害が生じるリスク（想定外を想定する）

要点2

情報セキュリティ防御ができなかった場合の対策を強化

- ■ 検知手順・インシデント判定手順の確立
- ■ CSIRTの確立
- ■ 事業継続：物理的対処チームや復旧プロセス等との連携及びサイバーレジリエンスの確立

※サイバーレジリエンス：
損害を被ったシステム部分を除いて、業務を継続する仕組みがあること

Copyright2020 Japan Information Security Association All rights reserved

2.サイバーセキュリティのリスク判断

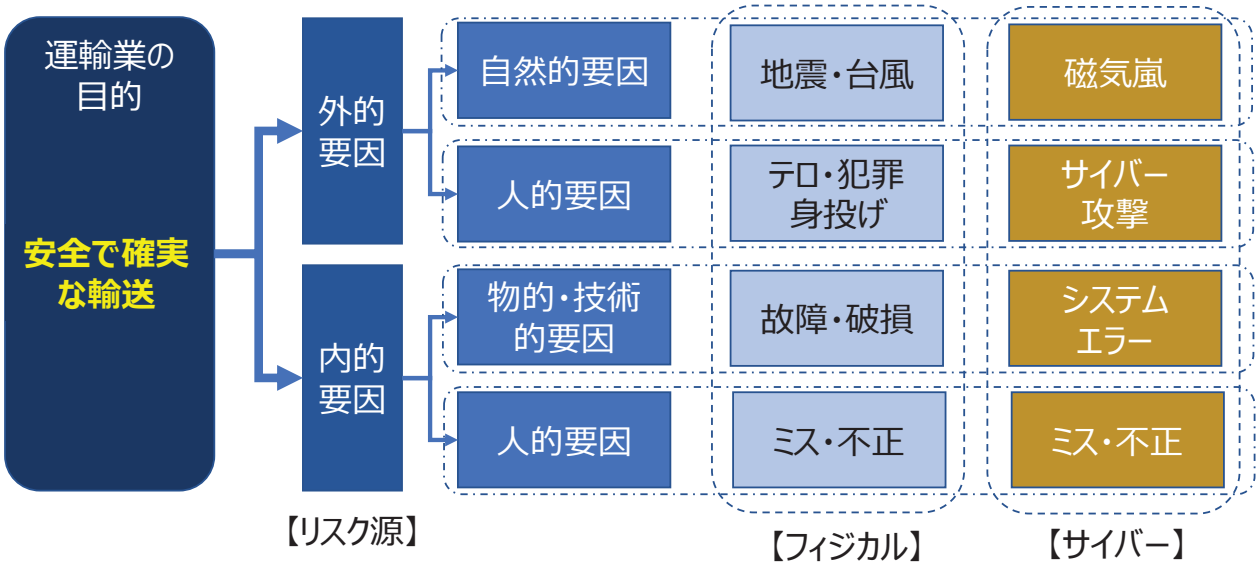
1. 情報セキュリティとサイバーセキュリティ

3. ガバナンス・マネジメント・コントロール
4. 基本となる情報セキュリティ監査
5. サイバーセキュリティの監査
6. 監査役の役割

Copyright2020 Japan Information Security Association All rights reserved

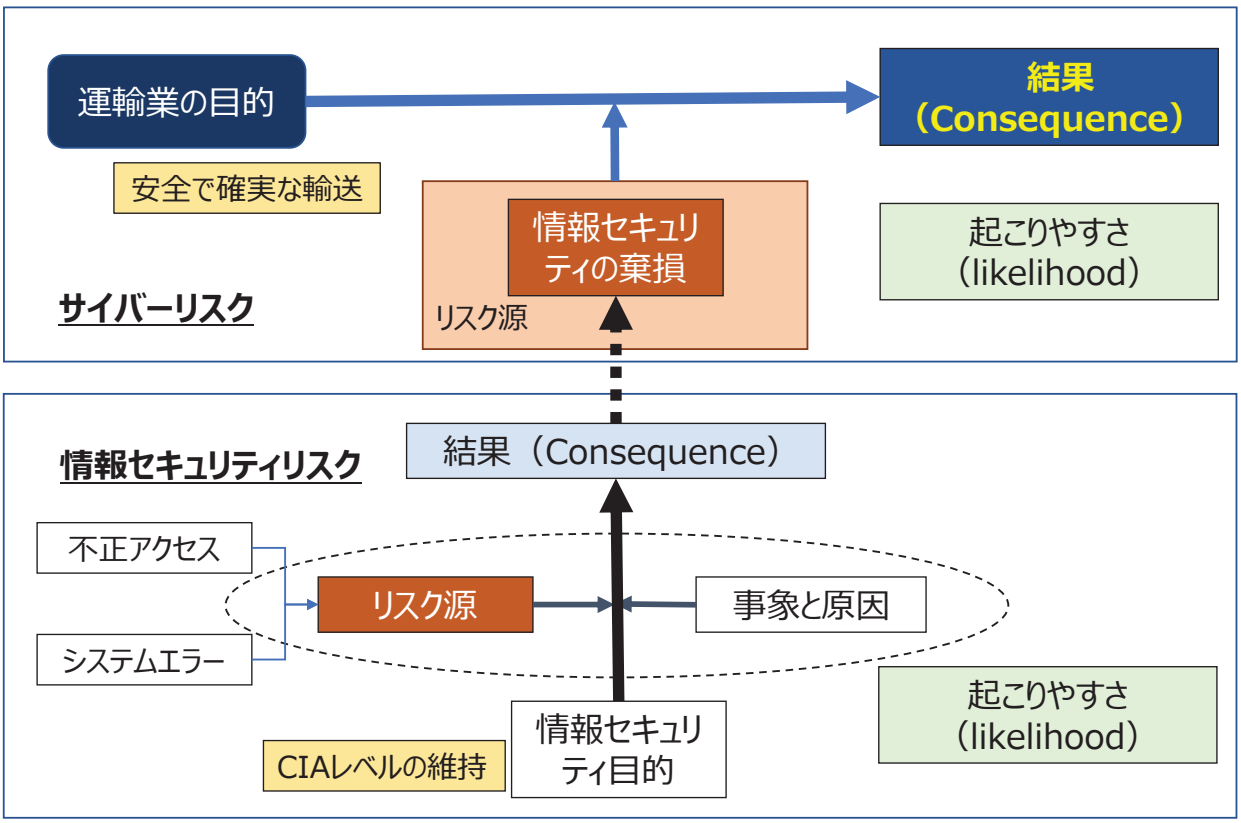
リスクとは

リスク：目的に対する不確かさの影響
（ISO31000）



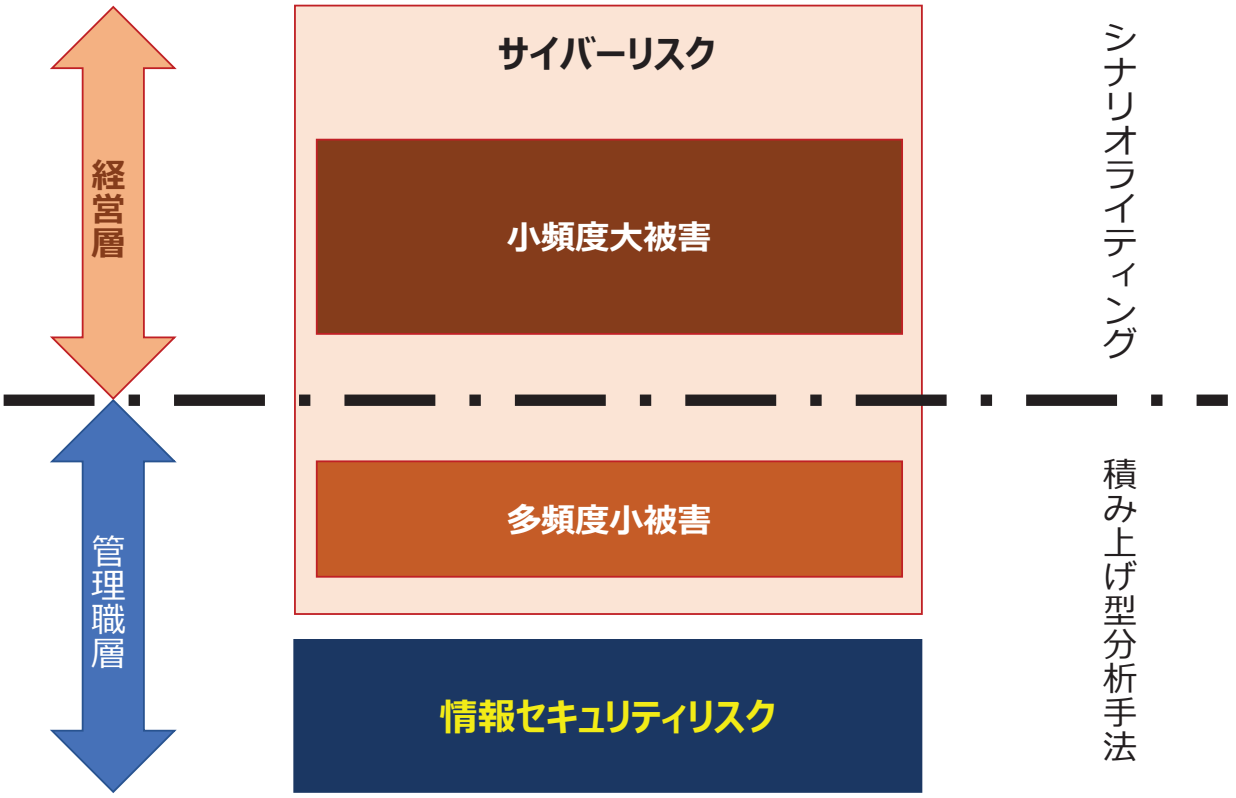
Copyright2020 Japan Information Security Association All rights reserved

情報セキュリティリスクとサイバーリスク



Copyright2020 Japan Information Security Association All rights reserved

サイバーリスク判断における経営の役割

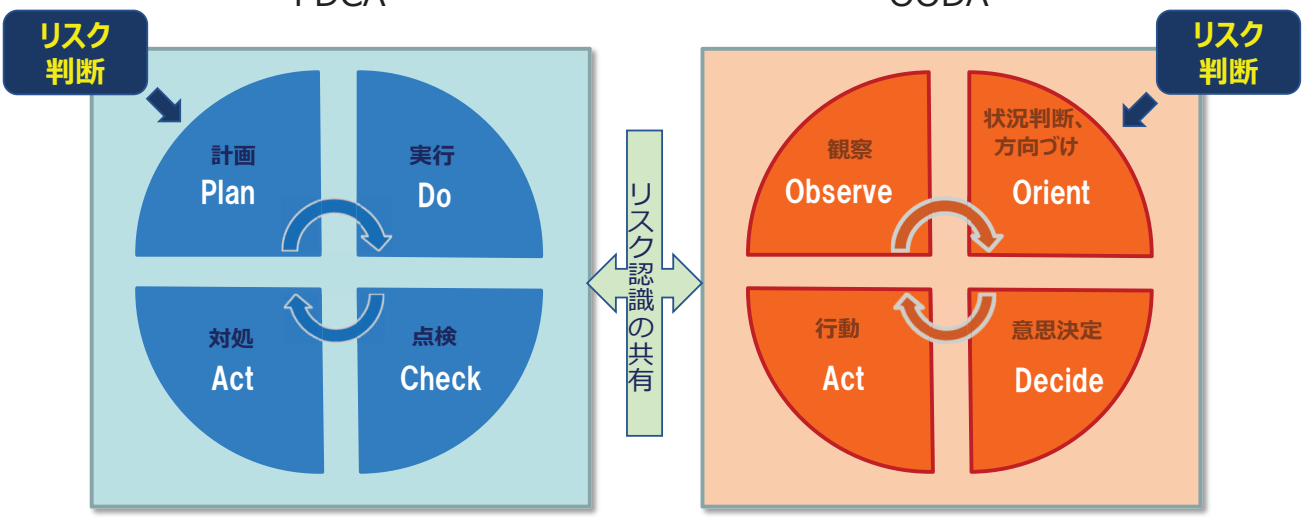


Copyright2020 Japan Information Security Association All rights reserved

二つの活動とリスク判断

組織中枢
-PDCA-

サイバー前線
-OODA-



組織戦略としてのリスク判断
長いサイクル（1年間など）

事故回避のためのリスク判断
短いサイクル（数時間～数日）

Copyright2020 Japan Information Security Association All rights reserved

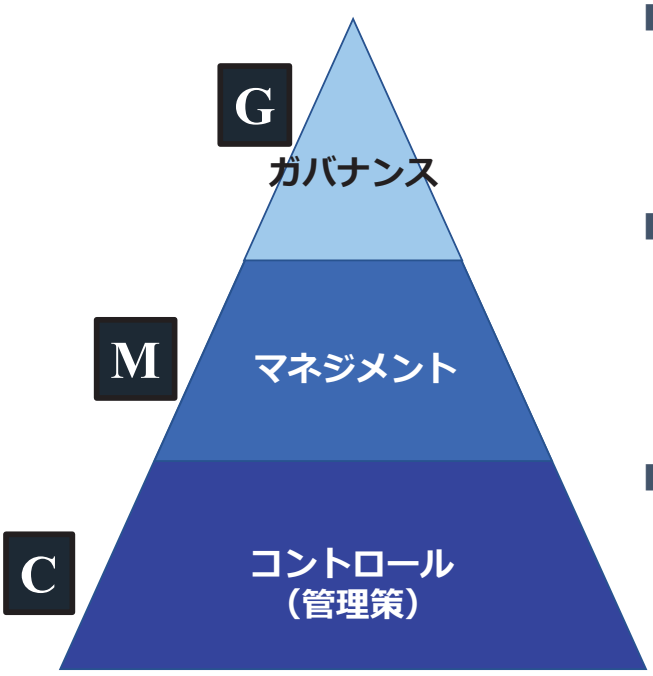
3. ガバナンス・マネジメント・コントロール

1. 情報セキュリティとサイバーセキュリティ
2. サイバーセキュリティのリスク判断

4. 基本となる情報セキュリティ監査
5. サイバーセキュリティの監査
6. 監査役の役割

Copyright2020 Japan Information Security Association All rights reserved

GMC



■ガバナンス
- □経営が企業全体としての意思を明確にし、それを貫徹する

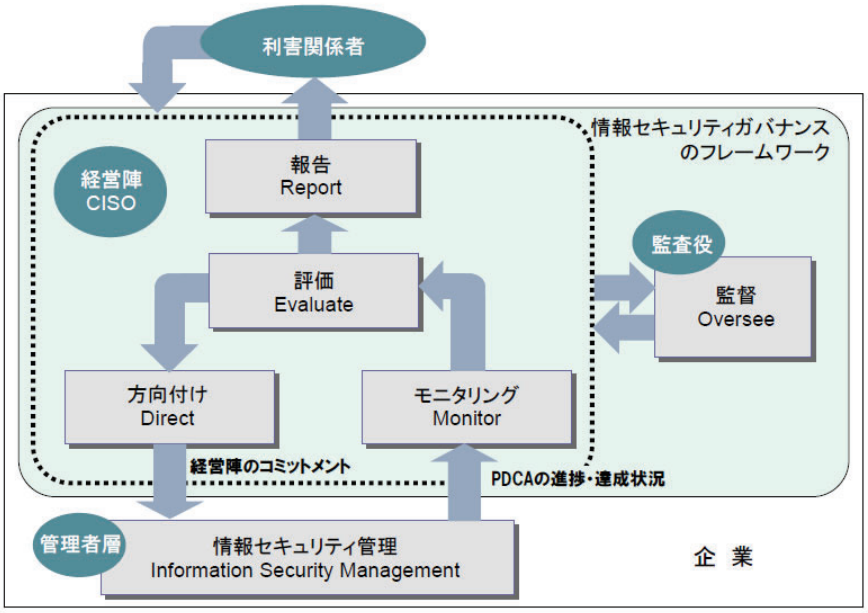
■マネジメント
- □管理職が管掌する範囲で経営の意思を反映した成果をだすようにする

■コントロール
- □担当者が定められたことに従って行動する

Copyright2020 Japan Information Security Association All rights reserved

セキュリティガバナンスの構造

情報セキュリティガバナンスのフレームワークはサイバーセキュリティガバナンスにも適用できる



- 方向づけ（Direct）
- モニタリング（Monitor）
- 評価（Evaluate）
- 報告（Report）
- 監督（Oversee）

「情報セキュリティガバナンス導入ガイダンス」

Copyright2020 Japan Information Security Association All rights reserved

重要なリスクコミュニケーション

組織全体でリスク認識が共有されていると、ガバナンスが利きやすい

■リスクコミュニケーション※の意義：
- 組織内外の関係者が「リスク」「意思決定の根拠」「特定の活動が必要な理由」についての理解が容易になる

■リスクコミュニケーションの実施段階
- リスクアセスメントのみではなく、リスク対策の実施、レビュー、記録等リスクマネジメントのあらゆるプロセスで行う
- サイバーセキュリティ対策もリスクマネジメントプロセスとして行われる

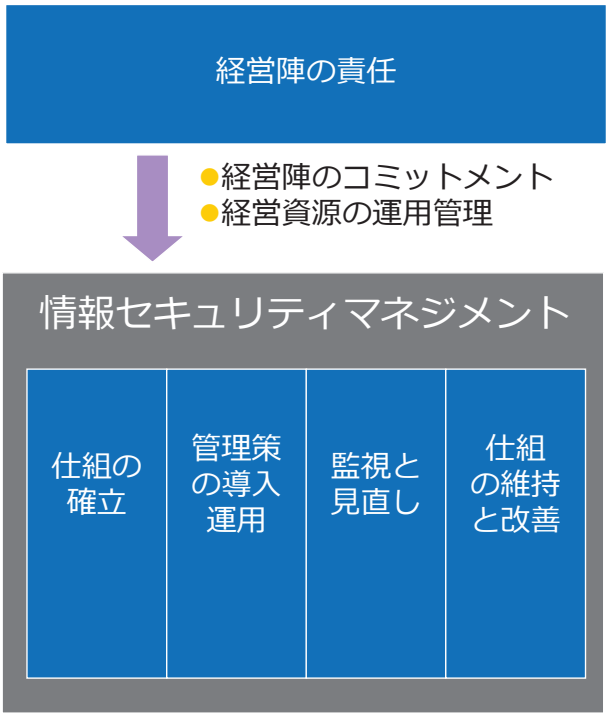
■リスクコミュニケーションのねらい
- プロセスの各段階で組織内外の専門家の知識を集める
- リスク基準を定め、リスク評価の場合に異なる見解に考慮する
- リスク監視及び意思決定を行うための十分な情報を提供する
- **リスクの影響を受ける者たちの一体感と当事者意識を醸成する**

（注）ISO31000：2018に基づき加工

※ ISO31000では「リスクコミュニケーション及び協議」

Copyright2020 Japan Information Security Association All rights reserved

セキュリティマネジメントシステム



a. 基本方針を確立する
b. 目的を定め、計画の策定を指示する
c. 情報セキュリティに対する役割や責任を定める
d. 情報セキュリティの重要性を組織内に周知する
e. 必要な経営資源を提供する
f. リスク受容の基準、受容可能なリスクの水準を決める
g. 内部監査の実施を指示し支援する
h. 経営者の視点からレビューを実施する

（ISO/IEC27001：2005による）

Copyright2020 Japan Information Security Association All rights reserved

4.基本となる情報セキュリティ監査

1. 情報セキュリティとサイバーセキュリティ
2. サイバーセキュリティのリスク判断
3. ガバナンス・マネジメント・コントロール

5. サイバーセキュリティの監査
6. 監査役の役割

Copyright2020 Japan Information Security Association All rights reserved

監査とISMS

■監査の目的
- □情報セキュリティマネジメントが効果的か

■監査の方法
- □準拠性監査
  - ◆組織が定めたルールに準拠しているか
- □有効性（妥当性）監査
  - ◆リスク管理が有効か（管理策がリスクに対して妥当か）

⇨ 有効性監査が必要

■ ISMS適合性評価制度の限界
- □ 監査の方法等は経営者が決める
- □ ISO27006により審査工数の上限がある

Copyright2020 Japan Information Security Association All rights reserved

情報セキュリティ監査のしくみ

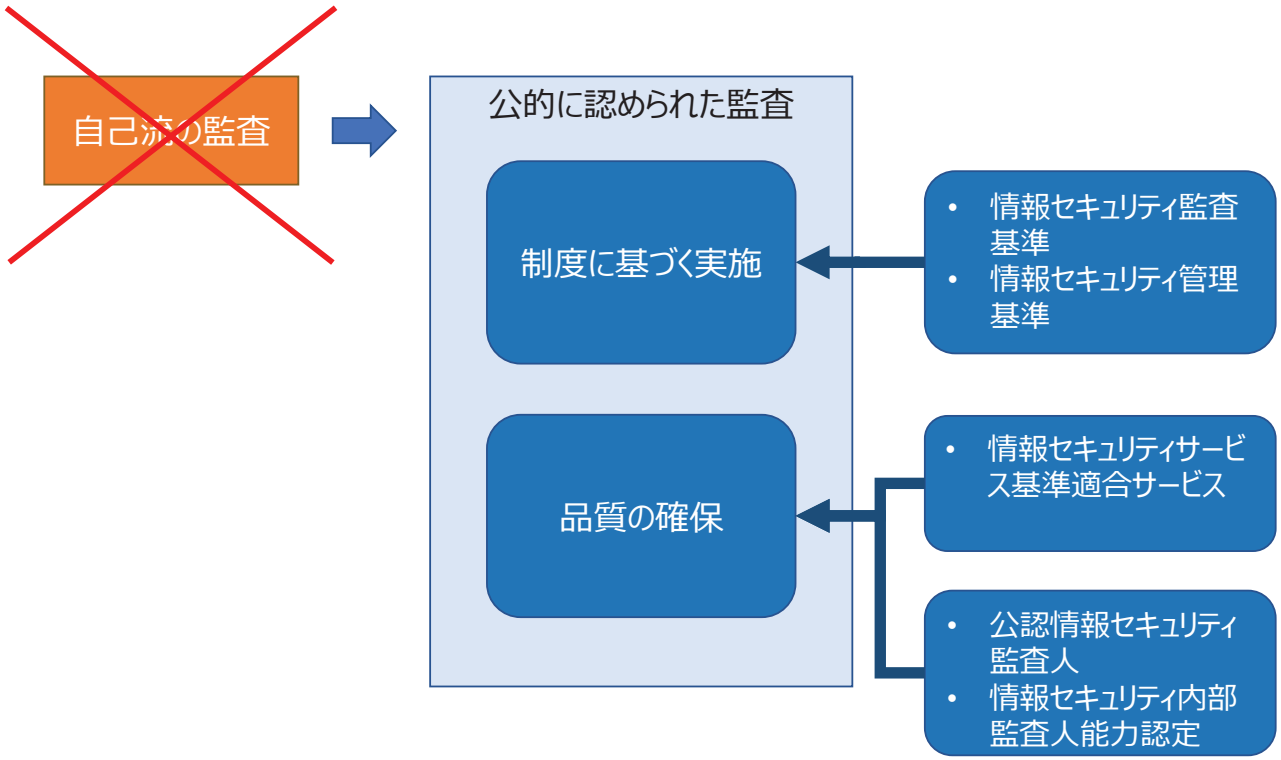
マネジメントに対する合理的評価のしくみ

要点	解説	具体的内容	必要な人材
基準	基準を満たしているかを判断	情報セキュリティ管理基準※1（個別管理基準）	「情報セキュリティ」と「監査」の知識を共に有する 専門家 （公認情報セキュリティ監査人）
証拠	客観的証拠に基づく事実認識	証拠の評価（証拠能力・証拠力） 証拠に基づくアプローチ	
アプローチ	体系化されたアプローチ	フェーズアプローチ ①方針②計画③実施④意見⑤報告	
評価者	独立した者	行為規範（情報セキュリティ監査基準※2）	
実証	追跡可能なプロセス	文書化：監査報告書、監査調書（情報セキュリティ監査基準※2）	

※１：情報セキュリティ管理基準（平成28年経済産業省告示第37号）
※２：情報セキュリティ監査基準（平成15年経済産業省告示第114号）

Copyright2020 Japan Information Security Association All rights reserved

活用すべき情報セキュリティ監査



Copyright2020 Japan Information Security Association All rights reserved

5. サイバーセキュリティの監査

1. 情報セキュリティとサイバーセキュリティ
2. サイバーセキュリティのリスク判断
3. ガバナンス・マネジメント・コントロール
4. 基本となる情報セキュリティ監査

6. 監査役の役割

Copyright2020 Japan Information Security Association All rights reserved

サイバーセキュリティ監査の確認事項

■企業がサイバーセキュリティに的確に対応できているかの確認
- □リスク認識の共有：組織末端までサイバーリスクの理解が共有できているか？
- □組織態勢の確立：平時も異常時も円滑に全員が動けるか？
- □事　業　継　続　：異常時に事業活動が途切れないか？

■企業態勢がしっかりしているかの確認
- □経営者が役割を果たしているか
  - ◆企業存続に影響するサイバーリスクを常に見直しているか？
  - ◆リスク認識の共有を図っているか？
  - ◆適切なガバナンスを行っているか？
- □管理者が適切に管理しているか
  - ◆PDCAがしっかり回っているか？
- □技術者が適切に対処しているか
  - ◆OODAによりインシデント検知が行われているか？
  - ◆インシデント対応態勢が動くか？

Copyright2020 Japan Information Security Association All rights reserved

サイバーセキュリティ管理基準

■判断の尺度としての管理基準
- □情報セキュリティ管理基準+サイバーセキュリティ固有の基準

■サイバーセキュリティ対策マネジメントガイドライン
- □ISO/IEC27001及び27002とNIST SP800-53の差分を整理
- □このガイドラインをベースに個別管理基準を組織に合わせて作成できる
- □Ver1.0を公開済み
  （https://www.jasa.jp/information/public_doc.html ）
- □Ver2.0策定中

■ガバナンス基準
- □「情報セキュリティガバナンス導入ガイダンス」（経済産業省平成16年度）に基づき、以下の4つを監査
- □方向づけ（Direct)、モニタリング（Monitor)、評価（Evaluate)、報告（Report)

Copyright2020 Japan Information Security Association All rights reserved

6. 監査役の役割

1. 情報セキュリティとサイバーセキュリティ
2. サイバーセキュリティのリスク判断
3. ガバナンス・マネジメント・コントロール
4. 基本となる情報セキュリティ監査
5. サイバーセキュリティの監査

Copyright2020 Japan Information Security Association All rights reserved

監査役の行うべきこと

■経営者がサイバーセキュリティに適切に対応しているかを利害関係者に説明できるようにすること
- サイバーリスクが常に見直されているか
- 組織におけるサイバーセキュリティリスクコミュニケーションができているか
- サイバーセキュリティのガバナンスが有効か

■各現場において、サイバーセキュリティのマネジメントが的確に機能しているかを確認すること
- マネジメント監査が適切に行われているか
- 監査人の力量（特に技術的な力量）が十分か

参考：情報セキュリティ監査人資格制度
https://www.jasa.jp/qualification/about.html

Copyright2020 Japan Information Security Association All rights reserved

参考資料

Copyright2020 Japan Information Security Association All rights reserved

ガバナンスとマネジメント、コントロールの意味

- ガバナンスの語源はラテン語の船を操舵する（gubernare）⇒**方向を示し、導く**
  - 船を操舵するは単に舵をとるという意味ではなく、船に加え、乗組員や船荷に配慮し、暗礁や悪天候の中でも安全に目的地に着くことを意味している。
- マネジメントの由来は「手」を意味するラテン語「manus」⇒**操作して、目的を達成する**
  - もともと何かをモノを扱うという意味である。その名残として馬を扱う調馬場を指す言葉として「マネージュ」が国際的に使われている。
- コントロールはラテン語の”contrarotulus“に由来する⇒**管理のための目録（具体的な方法のリスト）**
  - "Contra (～に対する)" + "Rotulus (巻物、目録、台帳）"

Copyright2020 Japan Information Security Association All rights reserved

【独自】行政文書が大量流出　納税記録などのＨＤＤ転売

神奈川ＨＤＤ流出

茂木克信　2019年12月6日05時00分

シェア　ツイート　Bookmark　メール　印刷
list　987

組織名称	株式会社ブロードリンク
組織部門名称	－
所在地	東京都中央区日本橋室町4丁目3番18号東京建物室町ビル8F
認証基準	JIS Q 27001:2014(ISO/IEC 27001:2013)
認証登録番号	IS 517544
	・中古パソコン・OA機器の買取販売及びデータ消去サービス・オフィス内装工事・情報機器の設定、設置及び修理・産業廃棄物のリサイクル業務（中間処理） 2014年09月01日付適用宣言書 第9版

（出典）ISMSマネジメントシステム認定センター

納税などに関する大量の個人情報や秘密情報を含む神奈川県庁の行政文書が蓄積されたハードディスク（ＨＤＤ）が、ネットオークションを通じて転売され、流出していたことが朝日新聞の取材で分かった。県のサーバーから取り外されたＨＤＤのデータ消去が不十分なまま、中古品として出回っていた。県によると、データの消去から廃棄までを請け負った業者の社員が、転売に関与したことを認めているという。

（出典）https://www.asahi.com/articles/ASMD57WSXMD5UTIL065.html

Copyright2020 Japan Information Security Association All rights reserved





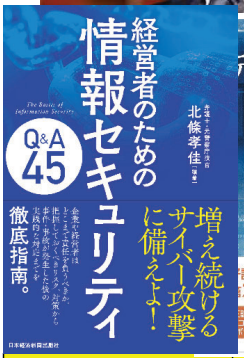
企業と経営層の法的責任の問題

2020年2月26日(水)
西村あさひ法律事務所
弁 護 士　北 條 孝 佳

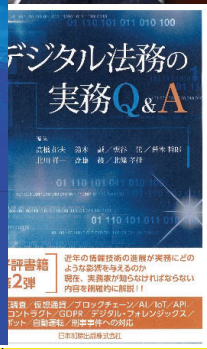
北條 孝佳
ほうじょう　たかよし



- 元警察庁技官(10年以上)
- 東京弁護士会所属
- NCA(日本シーサート協議会)
  専門委員
- NICT(情報通信研究機構)
  招へい専門員
- JNSA(ネットワークセキュリティ協会)
  適正な事業遂行検討会　委員
- NISC(内閣サイバーセキュリティセンター)法令集　TF構成員
- IDF(デジタル・フォレンジック研究会)　幹事
- 全国都道府県警察での講演、経営者向け講演等



経営者のための情報セキュリティ　Q&A45



デジタル法務の実務Q&A

1. 事前対策の必要性
取り巻く環境

3



ゼロトラスト：信頼しないことを前提とし、全てを確認する
DFFT：Data Free Flow with Trust(情報の自由な流通)

1. 事前対策の必要性
重要インフラ事業者

4

- 「重要インフラ」
  - ✓ 代替困難なサービスを提供する事業
  - ✓ 機能が停止等の状態に陥った場合、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
- 内閣サイバーセキュリティセンター(NISC)が公表した第4次行動計画(2018年7月25日)では、重要インフラ分野として、「情報通信」、「金融」、「航空」、「空港」、「鉄道」、「電力」、「ガス」、「政府・行政サービス（地方公共団体を含む）」、「医療」、「水道」、「物流」、「化学」、「クレジット」及び「石油」の14分野を特定

1. 事前対策の必要性
重要インフラ事業者

5

重要インフラ事業者等の経営層は、以下の項目の必要性を認識し、実施できていることが求められている

- 情報セキュリティの確保は経営層が果たすべき責任であり、経営者自らがリーダーシップを発揮し、機能保証の観点から情報セキュリティ対策に取り組むこと
- 自社の取組が社会全体の発展にも寄与することを認識し、サプライチェーン(ビジネスパートナーや子会社、関連会社)を含めた情報セキュリティ対策に取り組むこと
- 情報セキュリティに関してステークホルダーの信頼・安心感を醸成する観点から、平時における情報セキュリティ対策に対する姿勢やインシデント発生時の対応に関する情報の開示等に取り組むこと
- 上記の各取組に必要な予算・体制・人材等の経営資源を継続的に確保し、リスクベースの考え方により適切に配分すること

1. 事前対策の必要性
時代の変化

6

・世界の時価総額ランキング

	平成元年(億ドル)	平成30年(億ドル)
1	NTT(1638.6)	アップル(9409.5)
2	日本興業銀行(715.9)	アマゾン・ドット・コム(8800.6)
3	住友銀行(695.9)	アルファベット(8336.6)
4	富士銀行(670.8)	マイクロソフト(8158.4)
5	第一勧業銀行(660.9)	フェイスブック(6092.5)

出典：ダイヤモンドオンライン
https://diamond.jp/articles/-/177641?page=2

2. 経営層が意識すべきこと①
デジタル化・IT化

7

- 時代が変化、企業は全てIT化
  →デジタライゼーションへ対応
  - デジタイゼーション
  - デジタルトランスフォーメーション
- 次々と登場する新たなサービスの**提供**、
  新たなサービスを**取り入れる**際の**注意**
- 先端技術やサービスの導入にはリスク・脅威も
  含まれる
- 試験的導入＋リスクの低減方策
  (被害の最小化、代替手段の検討・準備)
- 導入に際する議論(範囲、責任)

2. 経営層が意識すべきこと①
リスクマネジメント

8

- **リスクマネジメント**の必要性
  - 企業の価値を維持・増大するため、**リスク**と**影響**を**正確に把握**し、事前対策を講じることで**危機発生の回避**＋**危機発生時の損失最小化・極小化**
  - 業務の複雑化によりアウトソーシング
    →外注先の業務停止が自社にも影響
  - 従業員の法令違反により企業の経営をゆるがす
- リスクとは…
  - 従来は、**悪い事象が起こる可能性**のこと
    →ダウンサイドリスクのみ
  - 現在は、**将来の不確実性**のこと
    →アップサイドリスクも含む

2. 経営層が意識すべきこと①
リスクの種類

9

- リスクの種類
  - ☑環境リスク・災害リスク
  - ☑戦略リスク・開発リスク
  - ☑法務リスク・財務リスク
  - ☑システムリスク
  - ☑犯罪リスクなど
- サイバーセキュリティの確保は
  - ☑外部からの対策
  - ☑内部からの対策

2. 経営層が意識すべきこと①
サイバー攻撃に遭う確率

10

- サイバー攻撃の被害に遭う確率
  - 情報処理推進機構(IPA)
    - 2014年度　調査対象企業全体の19.3%
  - トレンドマイクロ社
    - 2015年　調査対象企業全体の38.5%
    - 2016年　調査対象企業全体の41.9%
    - 2017年　調査対象企業全体の42.3%
    - 2018年　調査対象企業全体の36.3%
  - 英国デジタル・文化・メディア・スポーツ省
    - 2018年　調査対象企業1,566社の32%

2. 経営層が意識すべきこと②
クラウドへのデータ移行

11

- クラウドにデータが集約され始めている
- クラウドサービスの提供事業者視点
  - これまでとは異なるサービス体系
  - これまでとは異なる開発体系
  - クラウドサービスは複数の顧客に同一のサービスを提供
- クラウドサービスの利用事業者視点
  - クラウドサービスに対応可能な知識や能力が必要
  - 多様化するクラウドサービスの選定
  - 進化に追随する変革意識

2. 経営層が意識すべきこと②
サイバーセキュリティの確保

12

- 全てがつながるシステム・機器の登場・導入(OA機器、IoT機器、自動運転車等)
- 利用者、利用企業、社会生活、経済活動への影響大
- 様々な機器がネットワーク化、脆弱な部分が増加するおそれ
  →攻撃されれば、他のシステムへの被害拡大と他社/他者への損害が発生するおそれ
- 対策の必要性
  - ➢近時の脅威動向の把握
  - ➢体制整備、組織改革、規程類の見直し
  - ➢人材育成など

2. 経営層が意識すべきこと③ 内部不正(インサイダー取引)

13

- 世界有数のセキュリティ企業P社のIT部門従業員が、インサイダー取引により$700万(約7億6000万円)の利益を不正に取得
- 米司法省はP社に関連する証券詐欺で2名を起訴したと発表(2019/12/17)
- 四半期ごとの財務実績に関する機密情報へアクセスして悪用
- 3年間で不正な800回の株取引



U.S. Attorneys » Northern District of California » News

Department of Justice

U.S. Attorney's Office

Northern District of California

SHARE

FOR IMMEDIATE RELEASE

Tuesday, December 17, 2019

Two South Bay Residents Indicted For Securities Fraud Relating To Palo Alto Networks, Inc.

The Insider Trading Scheme Allegedly Generated $7 Million in Illegal Profits

出典：米司法省
https://www.justice.gov/usao-ndca/pr/former-it-administrator-pleads-guilty-insider-trading-conspiracy-relating-palo-alto

2. 経営層が意識すべきこと③ 内部不正対策

14

- 情報の持ち出し、機器の持ち出し
  例)教育関連企業、HDD廃棄企業
- 情報の売却、腹いせのためデータ削除
- 転職時のお土産
- 退職者、短期アルバイト等、利用していない者のアカウント管理
- 委託先管理、再委託先管理、再々委託先管理、再々々…
- インターネットの炎上(SNS利用)
  内部からの炎上、部外者による炎上
- データ改ざん、不正取引

2. 経営層が意識すべきこと③
内部不正:従業員、元従業員

15

- 2019年　不正アクセス禁止法違反
  - 子会社の従業員による犯行
  - 135人のIDを使って電子ギフト券を不正に入手
  - お金が欲しかったという動機
- 2019年　電子計算機損壊等業務妨害罪
  - 社長や会社の対応に不満があり、建設会社のパソコンに不正にアクセスし、全データ消去
  - 退職後もIDやパスワードの変更をしていなかったため、不正アクスが可能
- 2019年　窃盗罪
  - 神奈川県がリースしていたHDDがオークションで転売され、情報流出
  - リース会社の委託先従業員を窃盗で逮捕

3. 内部統制システムの構築
内部統制の意義

16

- サイバーセキュリティの確保は、適切なリスク管理の実施→内部統制システムの構築・運用
- 内部統制の意義は…
  消極的意義：法令遵守や不正防止
  積極的意義：業務の有効性や効率性の確保
- 内部統制システムを適切に構築・運用することは、取引先や消費者等を含む多様なステークホルダーへの利益にもつながる
  - ☑信用の確保、取引先との良好な関係構築
  - ☑企業価値を支える社会的責任
  - ☑ブランド価値・レピュテーションの維持や向上

3. 内部統制システムの構築
内部通報制度

17

- 内部通報制度…公益通報者保護法を踏まえ、従業員が企業内の不正を発見したり、コンプライアンス違反の疑いがあったりする場合に企業内外に設置された窓口に通報する制度
- 整備
  - 窓口、内部規程、経営幹部からの独立、通報者の保護、不利益取扱の禁止
- 運用
  - 通報の受領、通報内容の検討・調査、是正措置、通報制度の評価や改善

3. 内部統制システムの構築
コーポレートガバナンスコード

18

- コーポレートガバナンスコード　原則2-5

上場会社は、その従業員等が、不利益を被る危険を懸念することなく、違法または不適切な行為・情報開示に関する情報や真摯な疑念を伝えることができるよう、また、伝えられた情報や疑念が客観的に検証され適切に活用されるよう、内部通報に係る適切な体制整備を行うべきである。取締役会は、こうした体制整備を実現する責務を負うとともに、その運用状況を監督すべきである。
補充原則２－５① 上場会社は、内部通報に係る体制整備の一環として、経営陣から独立した窓口の設置（例えば、社外取締役と監査役による合議体を窓口とする等）を行うべきであり、また、情報提供者の秘匿と不利益取扱の禁止に関する規律を整備すべきである。

3. 内部統制システムの構築
内部通報制度認証

19

- 内部通報制度認証(自己適合宣言登録制度)
  - 事業者が自らの内部統制制度を評価して認証基準に適合している場合
  - 事業者からの申請に基づき指定登録機関がその内容を確認した結果を登録し、WCMSマークの使用を許諾する制度
- 自己適合宣言制度
- 今後は第三者認証制度

商事法務研究会：https://wcmsmark.secure.force.com/

4. 経営者らが考慮すべき責任
2種類の責任

20

- 責任
  - ① 企業が負う責任
    相手方や第三者に損害が発生した場合には、企業が損害賠償責任を負う可能性
  - ② 経営者らが負う責任
    会社に損害が生じ、経営者らが負う善管注意義務に違反した場合、
    会社に対して負う責任＋
    第三者に対して負う責任の両方の責任を負う可能性

4. 経営者らが考慮すべき責任
①企業が負う責任

21

- 企業の行為(管理義務違反も含む)により、相手方や第三者に損害が発生した場合には、企業が損害賠償責任を負う可能性
  - 個人情報、クレジットカード情報の流出
  - 開発企業として開発した納品物の不備
  - 運用、保守管理による対策不備
- 内部不正も同じ
  - データ改ざん、粉飾決算等の不正会計、情報の不正な持出し

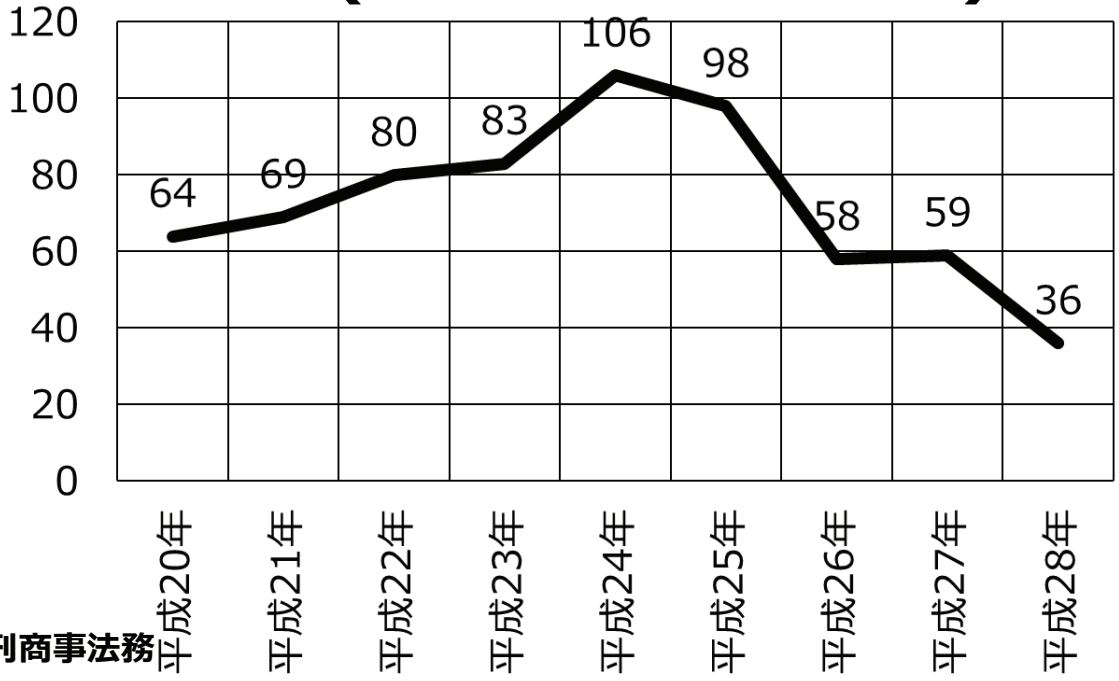
→製品の認証、認定の取消、上場廃止・停止

→情報の主体からの損害賠償請求

4. 経営者らが考慮すべき責任
②経営者らが負う責任

22

- 株主代表訴訟(経営者への責任追及)



引用元：旬刊商事法務

4. 経営者らが考慮すべき責任 ②経営者らが負う責任 23

- 会社に損害が生じ、経営者らが善管注意義務に違反する場合には、経営者らも責任を負う可能性
  - ☑ 会社から委任を受け、善良な管理者として注意義務(会社法330条、民法644条、会社法355条)
  - ☑ 法令、定款等を遵守し、会社や株主に対して最も有利となるように職務遂行
    →経営者らは法令を遵守し、会社にできるだけ損失を与えないように適切なリスクマネジメントを行うこと
  - ☑ グループ会社のガバナンスも必要
  - ☑ 具体的法令違反
  - ☑ 抽象的法令違反

A) 経営判断の原則(責任を否定する方向に働く)
B) 監視・監督義務違反
C) 内部統制システム構築義務違反

4. 経営者らが考慮すべき責任 ②経営者らが負う責任 24

C)内部統制システム構築義務

- ☑ セキュリティ脅威の把握
- ☑ セキュリティリスクの内部チェック
- ☑ セキュリティリスクの第三者チェック
- ☑ 同業他社のセキュリティ事案の分析
- ☑ セキュリティ脅威に対する対策
- ☑ セキュリティ対策のガイドラインの把握
- ☑ セキュリティ対策の知識や理解
- ☑ セキュリティ対策の検討、採用、運用
- ☑ 運用状況、不足状況、修正可能性
- ☑ 適合性、充足性、過剰性

4. 経営者らが考慮すべき責任
サイバーリスクハンドブック日本版(経団連)

25

原則1：取締役は、サイバーセキュリティを、単なるITの問題としてではなく、全社的なリスク管理の問題として理解し、対処する必要

原則2：取締役は、自社固有の状況と関連付けて、サイバーリスクの法的意味を理解すべき

原則3：取締役会は、サイバーセキュリティに関する十分な専門知識を利用できるようにしておくとともに、取締役会の議題としてサイバーリスク管理を定期的に取り挙げ、十分な時間をかけて議論を行うべき

原則4：取締役は、十分な人員と予算を投じて、全社的なサイバーリスク管理の枠組みを確立すべき

原則5：サイバーリスクに関する取締役会における議論の内容として、回避すべきリスク、許容するリスク、保険等によって軽減・移転すべきリスクの特定や、それぞれのリスクへの対処方法に関する具体的計画等を含めるべき

5. サイバーセキュリティの確保
具体的内容

26

- 事前対策・準備として
  - ☑ 法務部、顧問弁護士・専門弁護士との連携＋管理・対応体制の構築
    例)データ利活用の企画・設計、取得、加工・分析、実装・運用、廃棄の全ての管理・対応体制
  - ☑ チェック＝技術的【内部・外部】チェック＋法的評価
    規程の整備は当然、その内容・中身の網羅性や技術的・法的・経営的視点
  - ☑ 契約書関連(守秘義務、誓約書)
  - ☑ 訴訟関連(適切な証拠保存の整備、ログ集約)
  - ☑ インシデント対応業者の選定
  - ☑ 模擬的内部不正を行い、不備のある箇所の見直し・改善など

5. サイバーセキュリティの確保 具体的内容

27

- 事後対応として
  - ☑ インシデント対応業者への依頼
  - ☑ 被害に遭った情報・機器の主体・手段・開示・使用等の特定
  - ☑ インシデント発生の原因・分析
  - ☑ 訴訟を見据えた情報収集・証拠収集
  - ☑ 法執行機関との連携、監督官庁等への報告・連絡
  - ☑ 広報活動・公表活動
  - ☑ 情報の取り戻し・使用禁止の検討
  - ☑ 再発防止策の提案(技術面、体制面)
  - ☑ 被害賠償、補償問題

    など

5. サイバーセキュリティの確保 CISOの設置

28

- CISOを設置するに当たり地位と権限を決定
  →取締役か執行役か執行役員か
- CISOはサイバーセキュリティのプロフェッショナルでなくても構わない
  →配下にプロフェッショナル人材を確保
- 現在のシステムのセキュリティ確保＋将来のシステムのセキュリティ確保のために最適となる計画(プロセス、リソースの確保)の策定及び計画に沿って実現
- 各部門へサイバーセキュリティを確保する意識、リスクを認識させること

TLP:GREEN

緊急事態の対処能力の向上策に類似する「サイバー攻撃対処態勢の整備」

2020年 2月

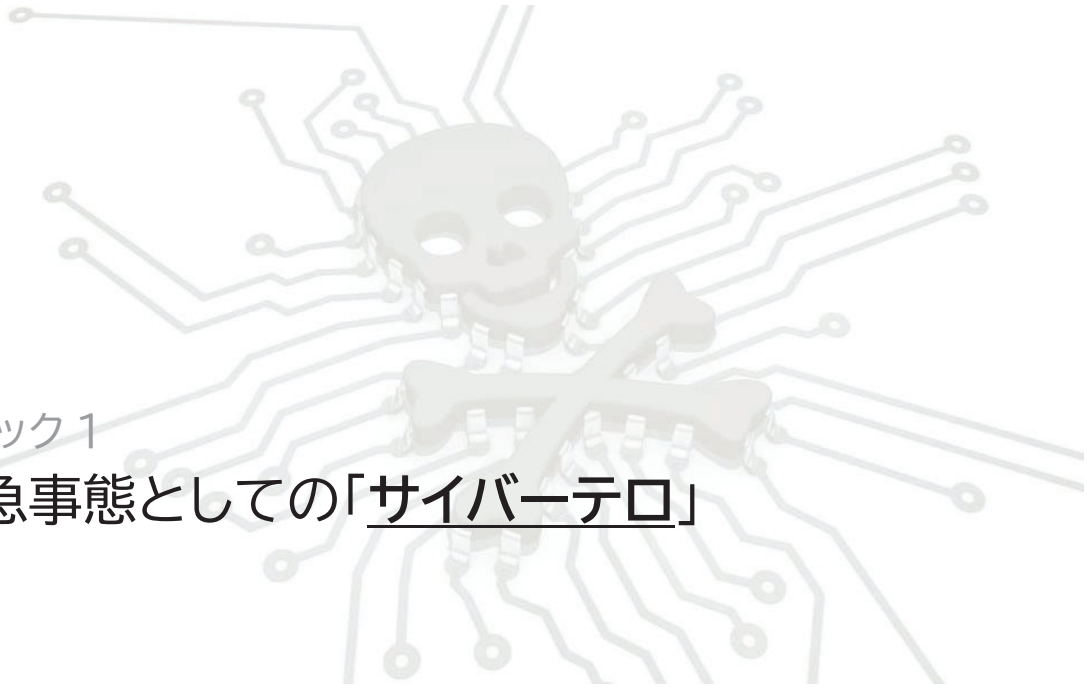
名和 利男

アジェンダ

1. 緊急事態としての「**サイバーテロ**」
2. 民間分野では回避・防御することが困難な
   サイバーテロ事態への対策 = **対処能力の構築**
3. 構築した**対処能力の維持・向上**

© 2020 Toshio Nawa

TLP:GREEN



トピック１

緊急事態としての「サイバーテロ」

「緊急事態」とは

- 緊急事態（Emergency）：一般に、健康（身体）・生命・財産・環境に危険が差し迫っている緊急の状態のこと。

【判断の観点】

- 「（自然災害のような）明らかに多くの生命が脅かされる事態」は、**あらゆる主体者が迅速に判断する。**
- 「（サイバーテロのような）緊急性の有無を判断するために必要な事態」は、**観察者（あるいは当事者）による主観的な評価を必要とする。**

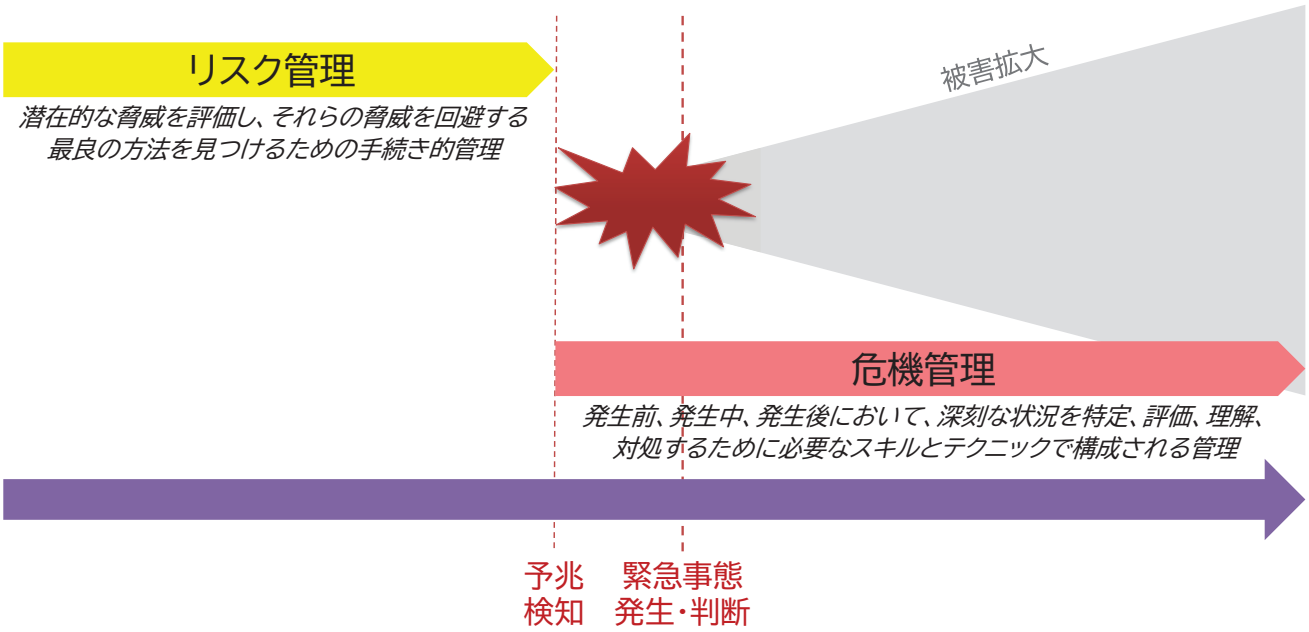
【対処の観点】

- 「事態の悪化を防ぐための介入等」に急を要するケースが多い。
- 「事態が自然に収束するのを待ってから緩和措置を取る（事後処理）」しか手段がないケースもある。

© 2020 Toshio Nawa

TLP:GREEN

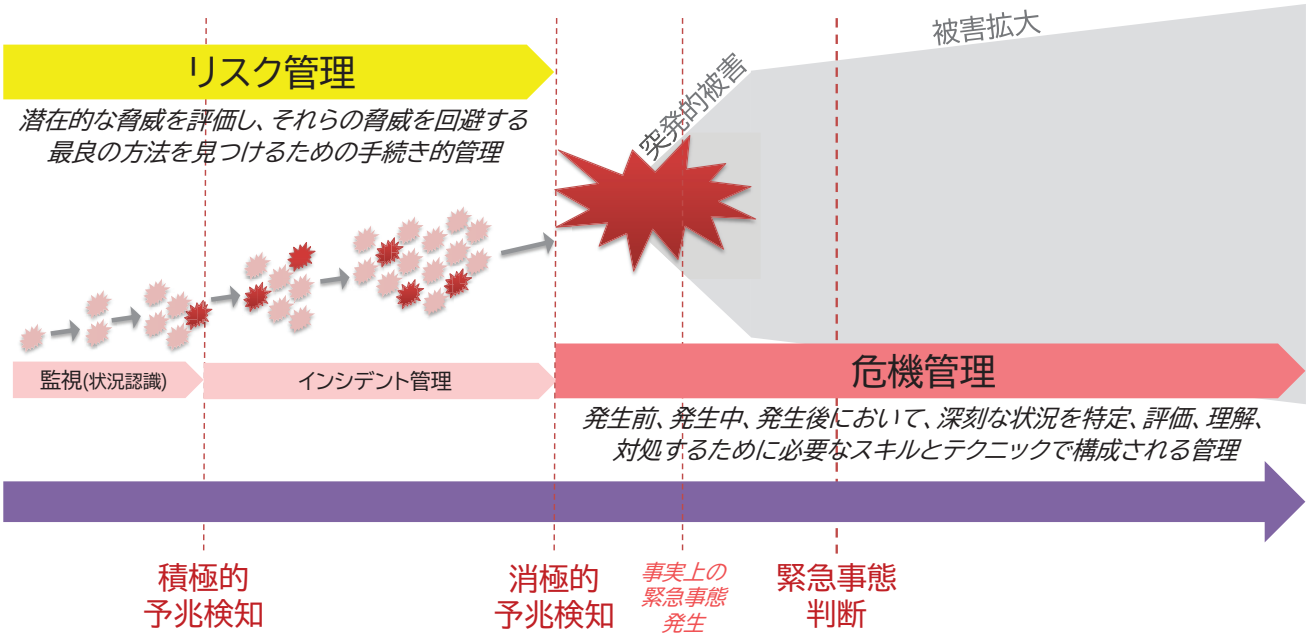
自然災害のような「明らかに多くの生命が脅かされる緊急事態」



© 2020 Toshio Nawa

TLP:GREEN

サイバーテロのような「緊急性の有無を判断するために必要な事態」



© 2020 Toshio Nawa

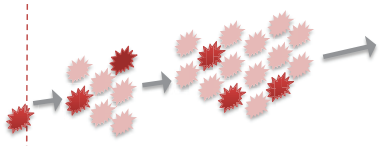
TLP:GREEN

サイバーテロのような「緊急性の有無を判断するために必要な事態」

サイバー攻撃の態様変化による「リスク管理」の限界

リスク管理

潜在的な脅威を評価し、それらの脅威を回避する最良の方法を見つけるための手続き的管理



インシデント管理

積極的
予兆検知

- サイバー攻撃の態様が急激に変化している。
  - ✓ サイバー攻撃が、極めて複雑化(sophisticated)・大規模化(large-scale)
  - ✓ 攻撃対象領域(Attack Surface)が、拡大・深化
  - ✓ 攻撃戦略(Attack Strategies)が、多様化・重層化・個別化・高度化・弾力化
- 旧来の体制と能力では、「潜在的な脅威」の見出し・識別・特定・評価は困難になってきた。
- 「最良の回避方法」の適用可能な範囲は、急速に縮小する。(すぐに最良でなくなる)

リスク管理領域のセキュリティ投資を強化!

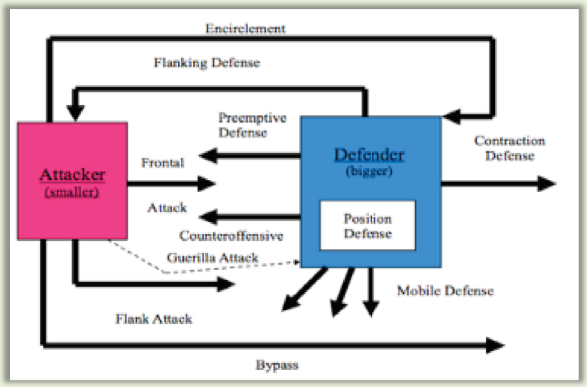
© 2020 Toshio Nawa
TLP:GREEN

【参考】攻撃対象領域(Attack Surface)と攻撃戦略(Attack Strategies)

- 攻撃対象領域(Attack Surface)とは
  - 主にソフトウェア環境を攻撃対象として、許可されていないユーザー(攻撃者)が当該環境にデータを入力する或いはデータを抽出することを可能とするさまざまなポイント(攻撃ベクトル)の総計のこと。



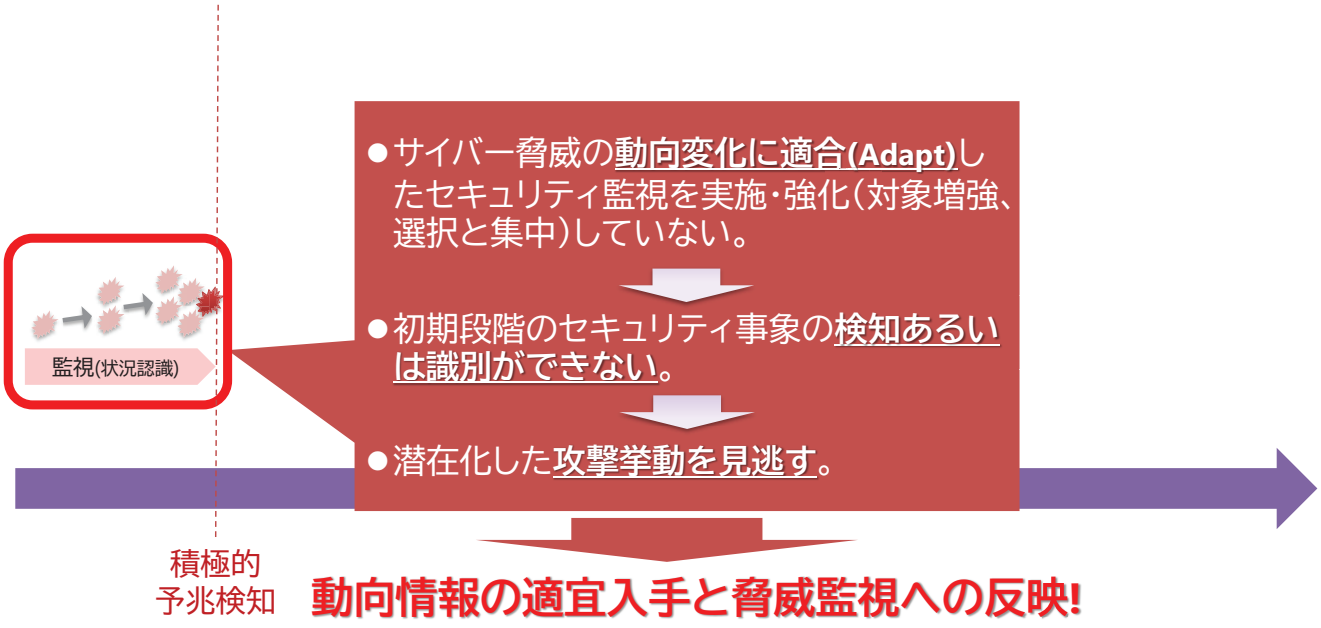
- 攻撃戦略(Attack Strategies)とは
  - 攻撃対象における不確実性の条件下で1つ以上の攻撃目標を達成するための高レベルの計画のこと。



© 2020 Toshio Nawa
TLP:GREEN

サイバーテロのような「緊急性の有無を判断するために必要な事態」

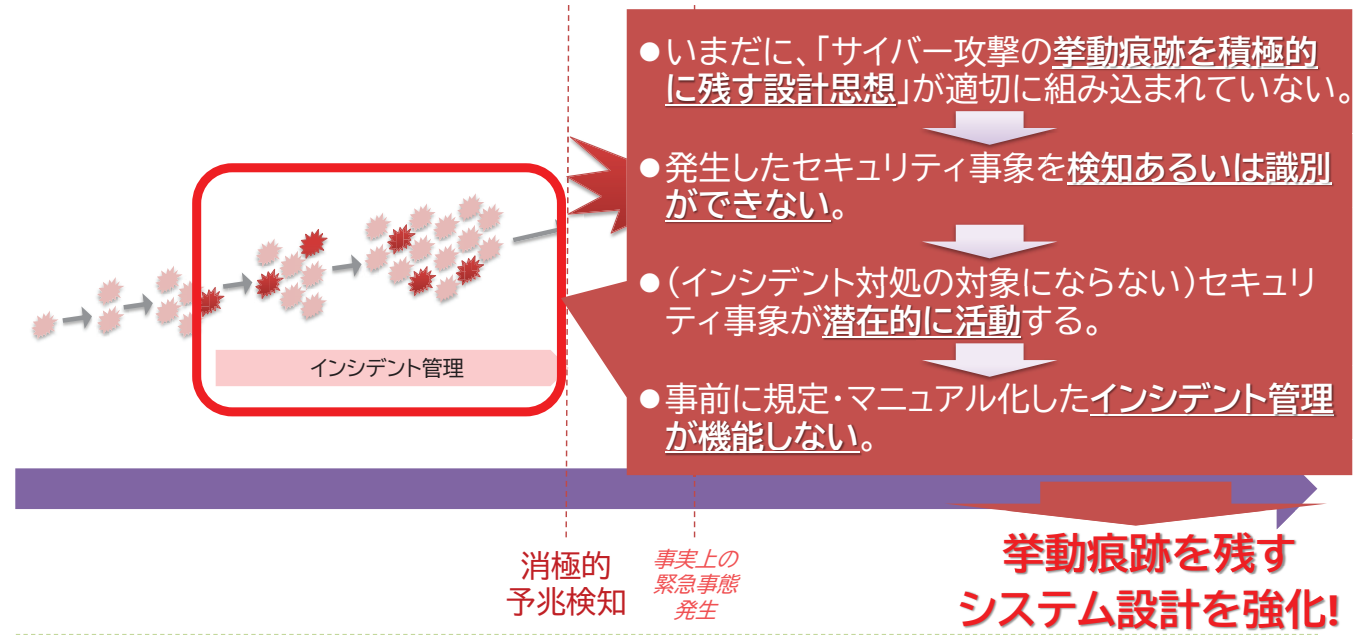
サイバー脅威に適合しない「監視」は、攻撃挙動を見逃す



© 2020 Toshio Nawa
TLP:GREEN

サイバーテロのような「緊急性の有無を判断するために必要な事態」

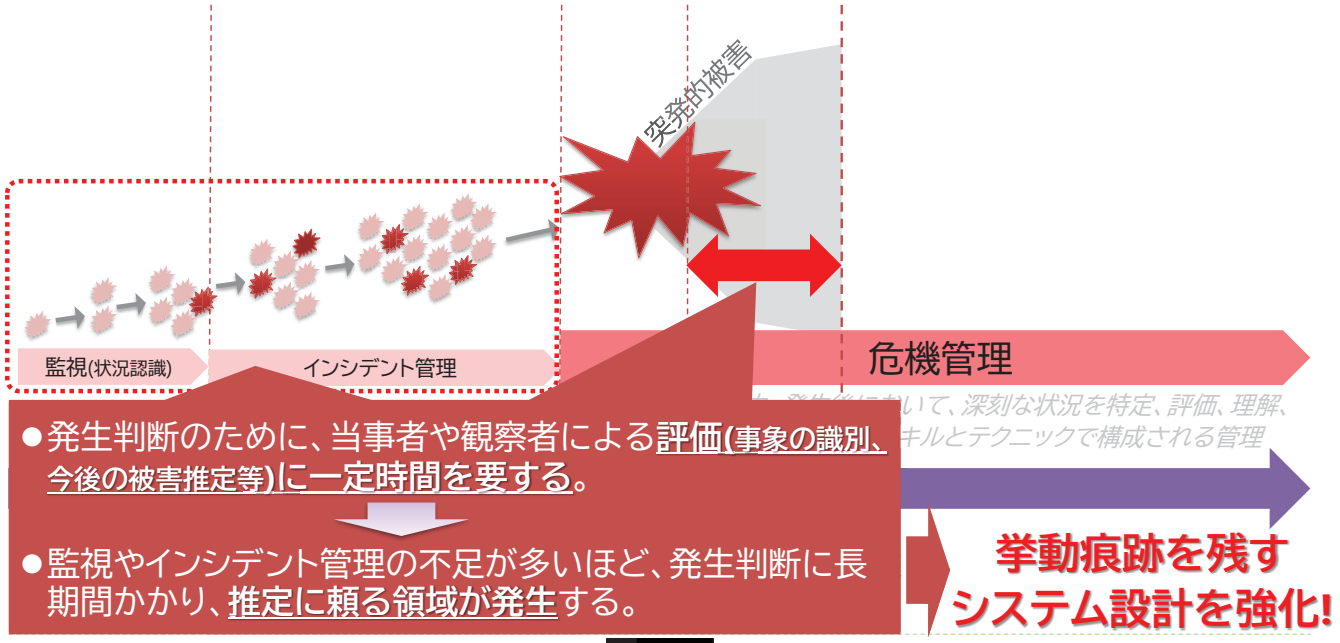
挙動痕跡を残す設計思想のない「インシデント管理」は、機能不全になる



© 2020 Toshio Nawa
TLP:GREEN

サイバーテロのような「緊急性の有無を判断するために必要な事態」

監視やインシデント管理の不足は、「発生判断」を遅延させる



- 発生判断のために、当事者や観察者による評価(事象の識別、今後の被害推定等)に一定時間を要する。
- 監視やインシデント管理の不足が多いほど、発生判断に長期間かかり、推定に頼る領域が発生する。

挙動痕跡を残すシステム設計を強化!

© 2020 Toshio Nawa

TLP:GREEN

サイバーテロのような「緊急性の有無を判断するために必要な事態」

監視やインシデント管理の不足は、「被害拡大」を止められない



- 事実解明のために、当事者や観察者(専門家)による対処(調査、識別・特定、分析、報告・説明)に一定時間を要する。
- 監視やインシデント管理の不足が多いほど、事実解明に長期間かかり、未対処の領域(被害)が拡大する。

挙動痕跡を残すシステム設計を強化!

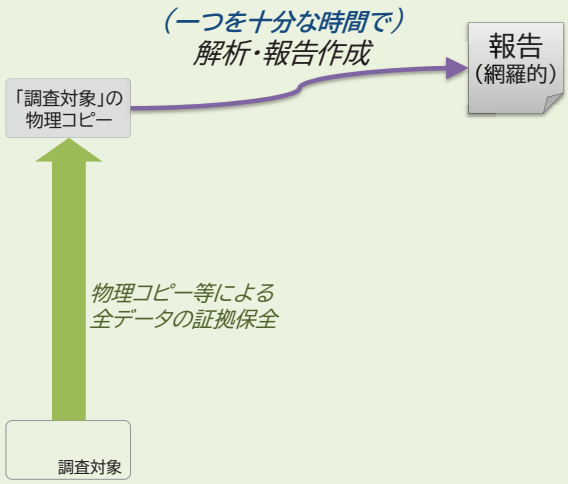
© 2020 Toshio Nawa

TLP:GREEN

【参考】最近の観察者(専門家)による対処(調査、識別・特定、分析、報告・説明)

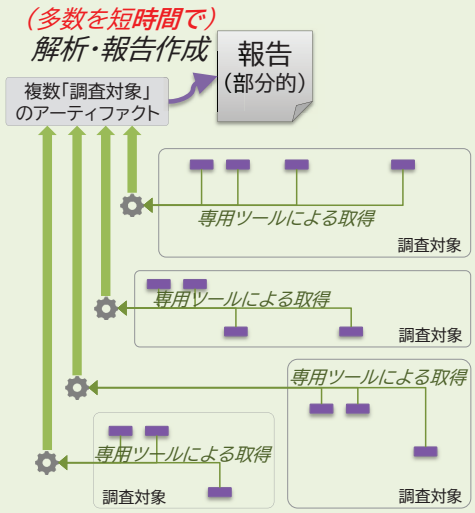
従来の「デジタル・フォレンジック」

単体の調査対象、全データの抽出と解析、長い(十分な)時間



「ファスト・フォレンジック」

複数の調査対象、アーティファクトのみの抽出と解析、短い時間



© 2020 Toshio Nawa
TLP:GREEN

「緊急事態」とは

- 緊急事態(Emergency):一般に、健康(身体)・生命・財産・環境に危険が差し迫っている緊急の状態のこと。

【判断の観点】

- 「(自然災害のような)明らかに多くの生命が脅かされる事態」は、あらゆる主体者が迅速に判断する。
- 「(サイバーテロのような)緊急性の有無を判断するために必要な事態」は、観察者(あるいは当事者)による主観的な評価を必要とする。

【対処の観点】

- **「事態の悪化を防ぐための介入等」に急を要するケースが多い。**
- 「事態が自然に収束するのを待ってから緩和措置を取る(事後処理)」しか手段がないケースもある。

© 2020 Toshio Nawa
TLP:GREEN

「事態の悪化を防ぐための介入等」のケース

2019年11月 オランダNCSCがランサムウェア攻撃状況を公表

- オランダの国家サイバーセキュリティセンター(NCSC)が公開した機密文書によると、世界中の企業少なくとも1800社が3種類のランサムウェア(LockerGoga、MegaCortex、Ryuk)に感染していたことが明らかになった。
- 感染した企業名については明らかにされていないが、自動車、建設、化学、医療、食品等、様々な業種の企業が含まれる。
  - また、多国籍企業の支社も含まれており、オランダの重要インフラのサプライヤである米国の化学企業のオランダ支社も含まれている。
- マルウェアのキャンペーンは2018年7月に開始された可能性が高く、NCSCの専門家は、ゼロデイの脆弱性を悪用した可能性があるとみている。



https://nos.nl/artikel/2312363-nederlandse-bedrijven-slachtoffer-van-geavanceerde-gijzelsoftware.html

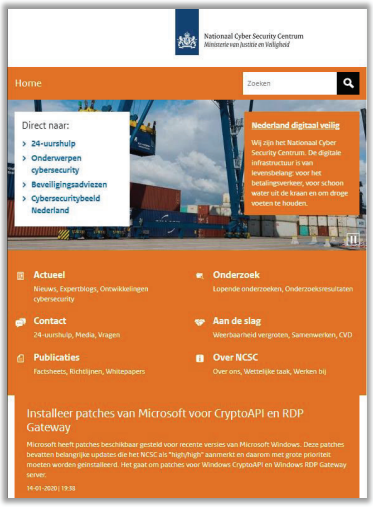
© 2020 Toshio Nawa
TLP:GREEN

「事態の悪化を防ぐための介入等」のケース

2019年11月 オランダNCSCがランサムウェア攻撃状況を公表

コメント:

- *この情報源であるオランダの国家サイバーセキュリティセンター(NCSC)は、安全保障・法務省(Ministry of Security and Justice)内に設置されている政府機関で、オランダのサイバーセキュリティ分野で中心的な役割を果たしており、担当分野の研究だけでなく、情報のハブとしての機能を併せ持つ。ミッションは、デジタル領域におけるオランダのレジリエンスの向上の貢献し、安全かつオープンで安定した情報社会を創出することである。*
- *このような位置づけと必要能力を有するNCSCは、このようなランサムウェア攻撃のレベルを「独自のロケットランチャーを保有する麻薬犯罪者に匹敵する」とみている。*
- *また、「企業はまだすべての基本的な対策を講じていない」と分析し、「アップデートを実行し、社員がデジタル脅威を認識していることを確認し、バックアップを作成してほしい」と強調している。*



https://www.ncsc.nl/

© 2020 Toshio Nawa
TLP:GREEN

「事態の悪化を防ぐための介入等」のケース

2019年11月 フランスANSSIが病院のランサム攻撃対処に介入

- 2019年11月15日夕方、スタッフ数1万人、ベッド数2,500のヨーロッパ最大級の医療施設であるフランス・ルーアン大学病院センターがランサムウェアによる攻撃を受け、6,000台のコンピュータが感染。
  - 多くのファイルがロックされ、外部ストレージのデータも破損した。
  - 病院スタッフはペンと紙による作業を余儀なくされ、3日間、通常のサービスが提供できない状態となった。
- フランスの国家情報システム・セキュリティ庁(ANSSI)が介入し、18日月曜午後までに、影響を受けたアプリケーションの少なくとも4分の1を通常の状態に回復した。
- 約1週間後、CryptoMix Clopランサムウェアが使用され、身代金40ビットコイン(約3200万円)を要求されていたことが報じられた。


Bon sang! French hospital contracts 6,000 PC-locking ransomware infection

Good news? They're not paying the ransom

By Gareth Corfield 21 Nov 2019 at 17:15 45 SHARE

https://www.theregister.co.uk/2019/11/21/french_hospital_rouen_ransomware/

「事態の悪化を防ぐための介入等」のケース

2019年11月 フランスANSSIが病院のランサム攻撃対処に介入

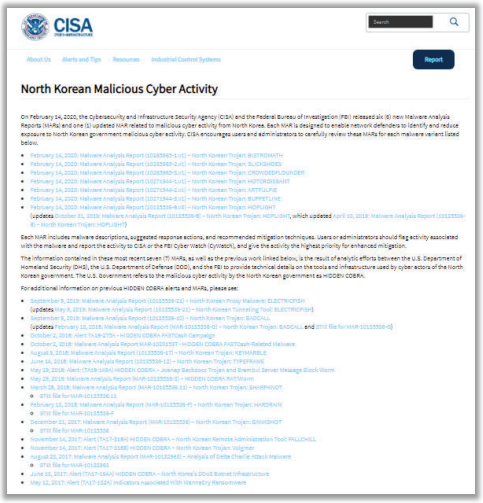
コメント:

- *フランスの国家情報システム・セキュリティ庁(ANSSI)は、**国家情報システムの保護に関する規則の提案や採用された対策の実施を検証する責任を持つ**。また、**サイバー防衛の分野では、監視、検出を提供し、特に国のネットワーク上でのコンピュータ攻撃に対する警告と対処**を行っている。*
- *一般的に、**病院は、その専門性の発揮を優先し、多忙を極めているため、サイバーセキュリティに関する知識が不足しがち**であり、一般的なセキュリティ教育では十分に啓発することが難しい。*
- *それに関わらず、**最近の病院は、医療事務の迅速化・効率化のためにコンピュータ化・ネットワーク化を推進**しており、その依存度をますます高めている。*
- *そのため、ランサムウェア攻撃で使用不能になったコンピュータやネットワークにより医療行為(診断や治療)が困難になると認識した病院は、他の分野に比べて、**復旧を確実にしようと身代金を支払おうとする傾向が強い**。*
- *攻撃者は、このような身代金を支払う傾向の強い分野を標的とした**ランサムウェア攻撃を継続・増強していく**とみられている。*

「事態の悪化を防ぐための介入等」のケース

2020年2月 米国CISA等が北朝鮮マルウェアに関する情報開示

- 米国サイバーセキュリティ・インフラストラクチャセキュリティ庁(CISA)及びFBIは、北朝鮮からの悪意のあるサイバー活動に関連する6つの新規および更新されたマルウェア分析レポート(MAR)を含む北朝鮮マルウェアに関する情報をリリースした。
  - 各MARは、手作業によるリバースエンジニアリングによって取得された詳細な分析情報を組織に提供するように設計されたものである。
  - また、米国政府が北朝鮮政府の悪意のある活動に言及していることを鑑み、ネットワーク防御者によるHIDDEN COBRAの悪意のあるサイバー活動の検出及び減少・緩和を支援するために発行されたものである。



https://www.us-cert.gov/northkorea

© 2020 Toshio Nawa
TLP:GREEN

「事態の悪化を防ぐための介入等」のケース

2020年2月 米国CISA等が北朝鮮マルウェアに関する情報開示

コメント:

- *このレポートの中で、サイバーセキュリティ・インフラストラクチャセキュリティ庁(CISA)は、組織に対して、セキュリティ体制を強化するためのベストプラクティス推奨した。*
  - *最新のウイルス対策シグネチャとエンジンを維持する。*
  - *オペレーティングシステムのパッチを最新の状態に保つ。*
  - *ファイルとプリンターの共有サービスを無効にする。これらのサービスが必要な場合は、強力なパスワードまたはActive Directory認証を使用する。*
  - *不要なソフトウェアアプリケーションをインストールして実行するユーザーの能力(許可)を制限する。必要な場合を除き、ユーザーをローカル管理者グループに追加しない。*
  - *強力なパスワードポリシーを適用し、定期的なパスワード変更を実施する。*
  - *添付ファイルが予期され、送信者がわかっているように見える場合でも、電子メールの添付ファイルを開くときは注意する。*
  - *未承諾の接続要求を拒否するように構成された、管理されたワークステーションであってもパーソナルファイアウォールを有効にする。*
  - *管理されたワークステーションおよびサーバーであっても不要なサービスを無効にする。*
  - *疑わしい電子メールの添付ファイルをスキャンして削除する。スキャンされた添付ファイルが「真のファイルタイプ」であることを確認する(つまり、拡張子がファイルヘッダーとの一致)。*
  - *ユーザーのWebブラウジング習慣を監視する。不適切なコンテンツを含むサイトへのアクセスを制限する。*
  - *リムーバブルメディア(USBサムドライブ、外部ドライブ、CDなど)を使用する場合は注意する。*
  - *実行する前に、インターネットからダウンロードしたすべてのソフトウェアをスキャンする。*
  - *最新の脅威に対する状況認識を維持し、適切なアクセス制御リスト(ACL)を実装する。*

© 2020 Toshio Nawa
TLP:GREEN

【参考】米国のサイバーセキュリティ・インフラセキュリティ庁(CISA)

- 2017年12月11日、CISA(サイバーセキュリティ・インフラセキュリティ庁)法(H.R. 3359: CISAA31)が、下院を通過した。
  - 元の法案である**2002年の国土安全保障法**を改正して、国家防護計画局(NPPD)を格上げして、その名称を「サイバーセキュリティインフラ防護庁(CIPA)」に変更することであったが、2017年にCISA (Cybersecurity and Infrastructure Security Agency)法案に改称された。
- 主な狙いは、サイバー脅威と物理的脅威から**連邦ネットワークと重要インフラを防護することを任務とする国家防護計画局(NPPD)を政策実施機関へと再編**し、**新たにサイバーセキュリティ・インフラセキュリティ庁(CISA)として出発**させることにある。
- CISAの長官には米国のサイバーセキュリティ、緊急時通信および重要インフラの**セキュリティとレジリエンスを防護・強化する全米努力を主導する国家サイバーセキュリティ・インフラセキュリティ局長**が就任した。

「国家サイバーセキュリティ・インフラセキュリティ局長」の主な責務

① CISAのサイバーセキュリティ及び重要インフラセキュリティプログラム、オペレーションおよび関連政策(国家サイバーセキュリティアセットレスポンス活動を含む)を主導すること。

② CISAのサイバーセキュリティおよび重要インフラ活動を実施するために、**SSA(セクター別所轄官庁)を含む連邦省庁と国際機関を含む非連邦機関の調整活動を履行**すること。

③ 2015年のサイバーセキュリティ法などの法律を遵守し、連邦の情報及び情報システムのセキュリティを確保する責任を履行すること。

④ 重要インフラリスクに対して、セキュリティの確保及び防護のための全米努力を調整すること。

⑤ 重要インフラの所有者及び運用者に対して、脅威等の分析結果、知見及びテクニカルアシスタンスなどを提供すること。

© 2020 Toshio Nawa
TLP:GREEN

【参考】日本のNISC(内閣サイバーセキュリティセンター)について

- NISCの所掌業務は、**行政各部における情報システム、サイバーセキュリティ、施策に関する事項**に限られている。
  - 情報通信ネットワーク又は電磁的記録媒体(電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であつて、電子計算機による情報処理の用に供されるものに係る記録媒体をいう。)を通じて行われる行政各部の情報システムに対する不正な活動の監視及び分析に関すること。
  - 行政各部におけるサイバーセキュリティ(サイバーセキュリティ基本法(平成二十六年法律第百四号)第二条に規定するサイバーセキュリティをいう。以下この項において同じ。)の確保に支障を及ぼし 、又は及ぼすおそれがある重大な事象の原因究明のための調査に関すること(内閣情報調査室においてつかさどるものを除く。)。
  - 行政各部におけるサイバーセキュリティの確保に関し必要な助言、情報の提供その他の援助に関する こと。
  - 行政各部におけるサイバーセキュリティの確保に関し必要な監査に関すること。
  - 前各号に掲げるもののほか、行政各部の施策に関するその統一保持上必要な企画及び立案並びに総合調整に関する事務のうちサイバーセキュリティの確保に関するもの(国家安全保障局、内閣広報室及び 内閣情報調査室においてつかさどるものを除く。)

出典: 内閣官房組織令第四条の二（昭和三十二年政令第二百十九号）

「内閣サイバーセキュリティセンター長」の責務

① 内閣サイバーセキュリティセンター長は、内閣官房長官、内閣官房副長官、内閣危機管理監及び内閣情報通信政策監を助ける。

② 内閣サイバーセキュリティセンターの事務を掌理する。

© 2020 Toshio Nawa
TLP:GREEN

TLP:GREEN

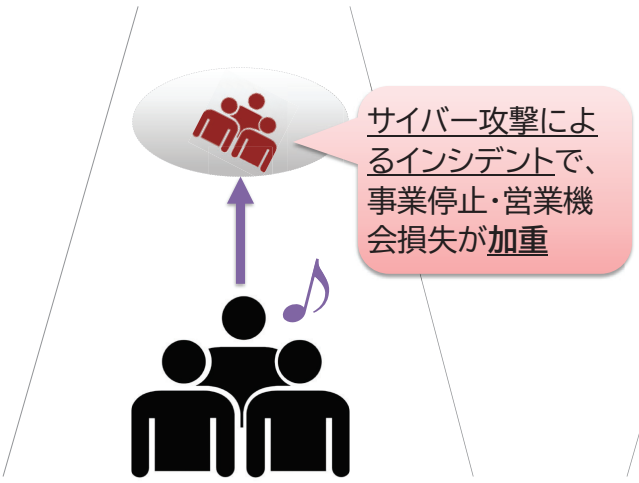
トピック 2

民間分野では回避・防御することが困難なサイバーテロ事態への対策 = 対処能力の構築

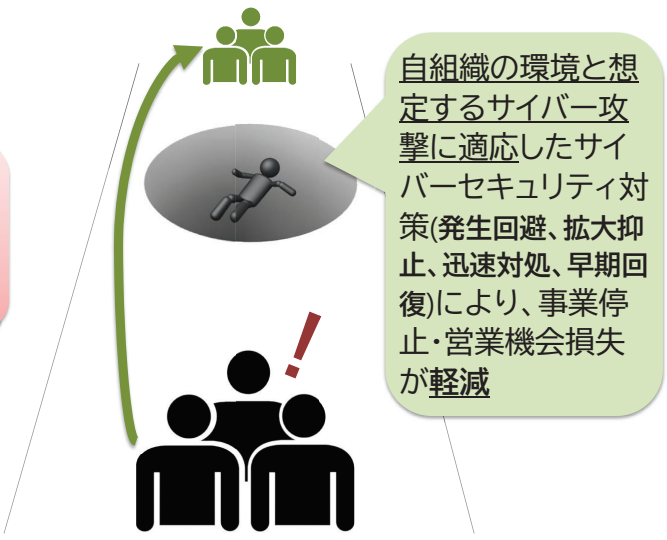
23

「不十分な状況認識」と「適切な状況認識」の領域を特定する

不十分な状況認識



適切な状況認識



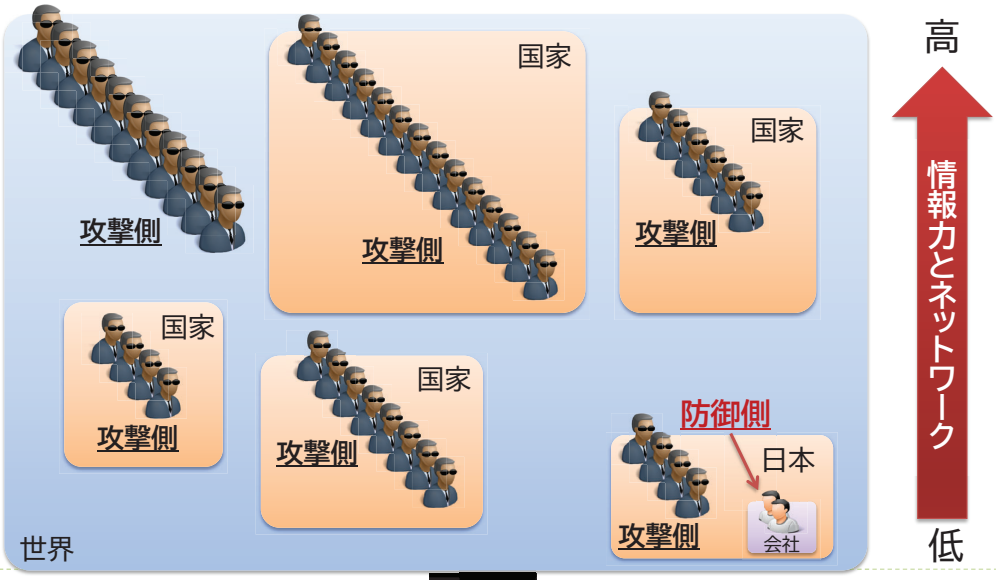
© 2020 Toshio Nawa

TLP:GREEN

24

「防御側」における情報力とネットワークの圧倒的な低さを知る

- サイバー攻撃は、攻撃側の事前偵察(窃取)した情報と互助関係にあるネットワークで増大。
- サイバー攻撃は「非対称」であるが、**攻撃側と防御側の情報力とネットワークは「対称」**。



© 2020 Toshio Nawa
TLP:GREEN

「防御側」における情報保証(IA)に偏重 した認知バイアスを知る

- APT攻撃の重点事項は、CND(Computer Network Defense)概念に基づく「システムによる多層的な防御」である。
- IA(Information Assurance)概念に基づいたセキュリティ対策は、「情報資産の単層的な防御」になりがちである。(IAを重点事項にした場合、システム管理者に対し「*適切に・・・せよ。*」という現場任せの指示になりやすい。)

- 「外部漏洩させない」セキュリティ対策
- 「IA的なインシデント ＝ **情報漏えい**」
- 攻撃プロセスの**後半で認識**
- **システム所有者(発注者)が対応**



「情報資産」をベースにしたセキュリティ対策

- 「侵入させない」セキュリティ対策
- 「CND的なインシデント ＝ **侵入**」
- 攻撃プロセスの**前半で認識**
- **システム保守管理者(委託者)が対応**



「システム防護」をベースにしたセキュリティ対策

© 2020 Toshio Nawa
TLP:GREEN

「防御側」における厳しい環境と現実を認識する



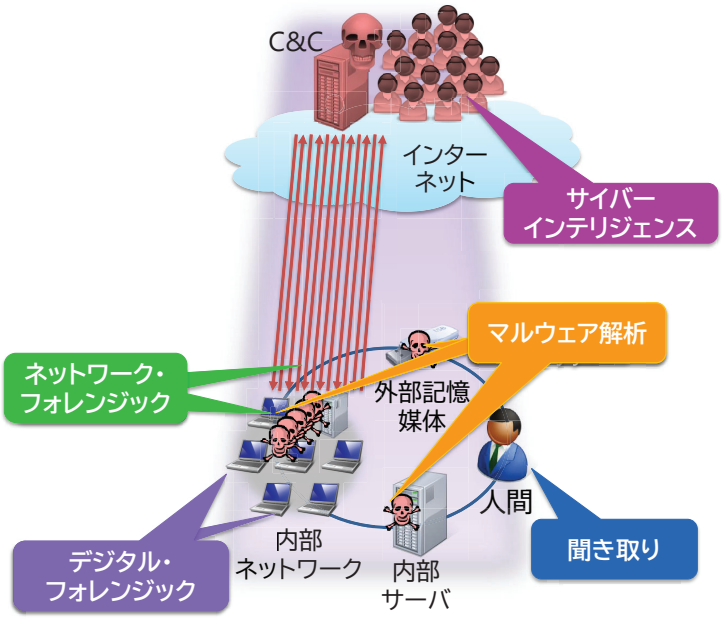


攻撃側	防御側 (インシデントレスポンダー)
攻撃の**強い意図や目的**を有する （経済的利得、主義主張の達成等） ➢攻撃者は、利己的行動の特性を持つ	(組織)防御に係る高い目的意識と **活動意欲を有する** ➢防御者は、利他的行動の特性を持つ
試行錯誤の侵入行為や マルウェア作成等による**経験の蓄積** ➢攻撃者は、豊富な(攻撃)経験を持つ	インシデント対処の**経験の蓄積** （サイバー演習による擬似的経験） ➢防御者は、豊富な(防御活動)経験を持つ
攻撃技術や対象組織に関する情報を **円滑かつ迅速に共有** ➢攻撃者は、互いの情報共有が活発	防御技術や攻撃主体に関する情報を **円滑かつ迅速に共有** ➢防御者は、他と情報共有を活発にする
攻撃を実施しやすい **IT環境の獲得と積極的な利用** ➢攻撃者は、ITリテラシーを高く発揮できる環境	防御を実施しやすい **IT環境の獲得と積極的な利用** ➢防御者は、ITリテラシーを高く発揮できる環境
経済的困窮や利益確保のための **攻撃者の急激な増加** ➢攻撃者は、インセンティブを得やすい環境	防御活動によるインセンティブのある **対処要員の増強** ➢防御者は、インセンティブを得やすい環境

© 2020 Toshio Nawa

TLP:GREEN

インシデントの現場で求められる対処能力を構築・獲得する



現場で必要な対処能力

=

デジタル・フォレンジック

＋

ネットワーク・フォレンジック

＋

マルウェア解析

＋

聞き取り

＋

サイバーインテリジェンス

© 2020 Toshio Nawa

TLP:GREEN

インシデントの現場で求められる対処能力を構築・獲得する

以前までの対処活動

最近の対処活動

デジタル・フォレンジック	コンピュータシステム上の痕跡(特にファイルシステムの履歴)、及び搭載されているソフトウェアによる様々な記録情報を分析すること。
聞き取り	
マルウェア解析	残存していたマルウェアの静的及び動的解析により、マルウェアの活動実態やその目的を把握するために行う分析のこと。
インシデントハンドリング／コーディネーション	現場の運用者や技術者だけではなく、責任を持つ管理職や経営層がどのような方針や手順でインシデント解決までの道筋(インシデントハンドリング)を立てるか、または、解決のために複数の組織や部署を巻き込む必要のある場合の組織間連携(インシデントコーディネーション)をどのようにすべきかなどのアドバイスや方法論・ノウハウを提供すること。
ネットワーク・フォレンジック	マルウェアの挙動や内部データ(ファイル)の流出経路などを解明する、或いは不正な挙動を確認するも、マルウェアが発見できない場合などに、サーバ／プロキシ／ファイアウォール等のログを分析したり、コンピュータシステムにおいてネットワークコマンドやシステム管理コマンドで得られる全ての出力データを総合的に分析すること。
サイバーインテリジェンス	技術的な分析のみでは解明が困難な場合、同じ分野のレスポンスチームやCSIRTで経験して明らかになっている攻撃手法や技術、攻撃者コミュニティで流通している手法、その他、類似したマルウェアによる事例等を収集し、それらの情報との類似性に着目して分析すること。

© 2020 Toshio Nawa

TLP:GREEN

インシデントの現場で求められる対処能力を構築・獲得する

以前までの対処活動

最近の対処活動

デジタル・フォレンジック

聞き取り

マルウェア解析

インシデントハンドリング／コーディネーション

ネットワーク・フォレンジック

サイバーインテリジェンス

(技術的能力)

- インターネットのアーキテクチャ、理念、将来像に関する知識
- ネットワークインフラのリテラシーと設計思想の理解
- ネットワークプロトコルの深い理解
- ネットワークアプリケーション、サービス、関連プロトコルの理解
- セキュリティの基本原則
- コンピュータ及びネットワークに対するリスクと脅威の理解
- セキュリティの脆弱性や弱点、及びそれを利用した攻撃の理解
- ネットワークセキュリティ対策とその問題に関する知識と理解
- 暗号化技術、デジタル署名、ハッシュアルゴリズムの理解
- プログラミング、ネットワークコンポーネント、基本ソフトの理解と経験

(管理的能力)

- **安全管理/危機管理/危機対応能力**
- コミュニケーション(対人)能力、言語能力
- 作業編成能力
- 強い目的意識と不屈の精神



防御側

© 2020 Toshio Nawa

TLP:GREEN

TLP:GREEN

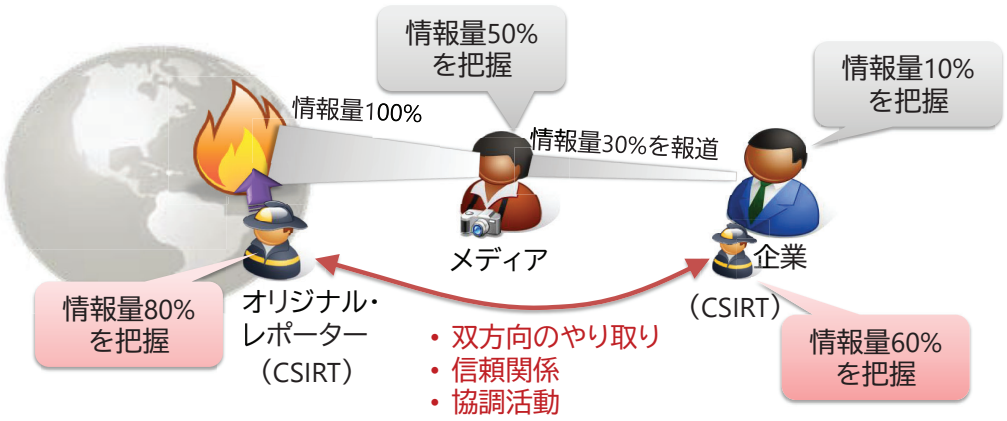
トピック３

構築した対処能力の維持・向上

31

① サイバー攻撃に関する正確な事実把握を行う

- 一般メディア等が発信する情報を鵜呑みにしてはいけない。
- オジリナル・レポーター(Original Reporter)が発信する情報を追求する。

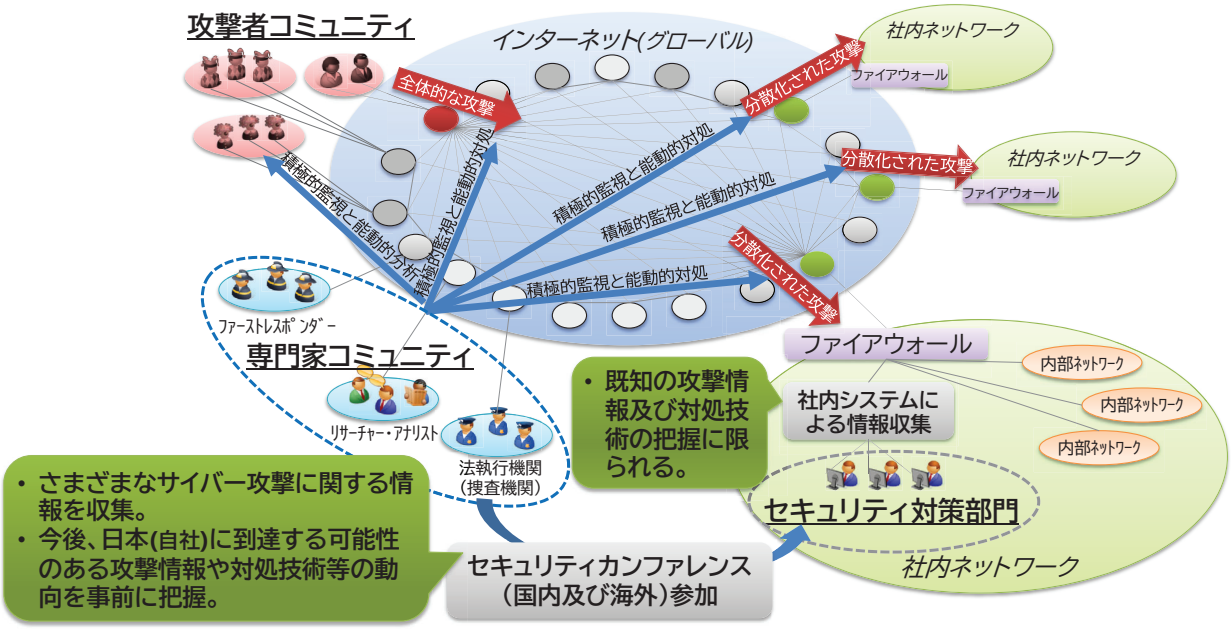


© 2020 Toshio Nawa

TLP:GREEN

32

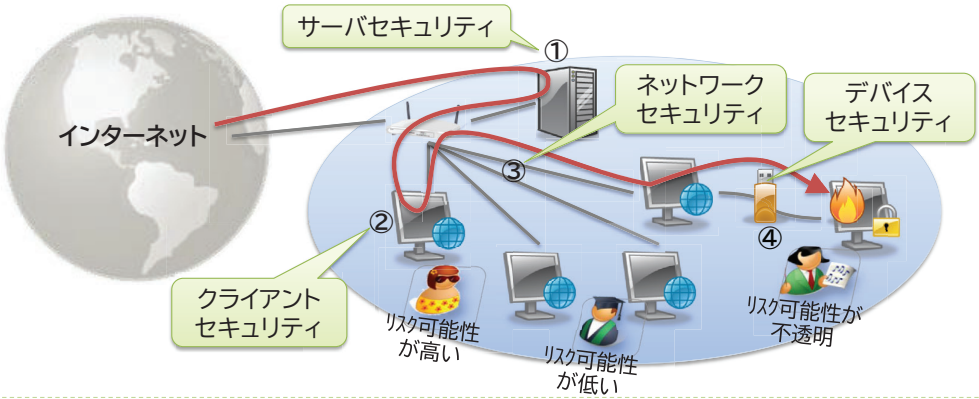
② サイバー空間における動向情報を積極的に収集する



© 2020 Toshio Nawa
TLP:GREEN

③ 攻撃経路を見出した上で、多層防御を実装する

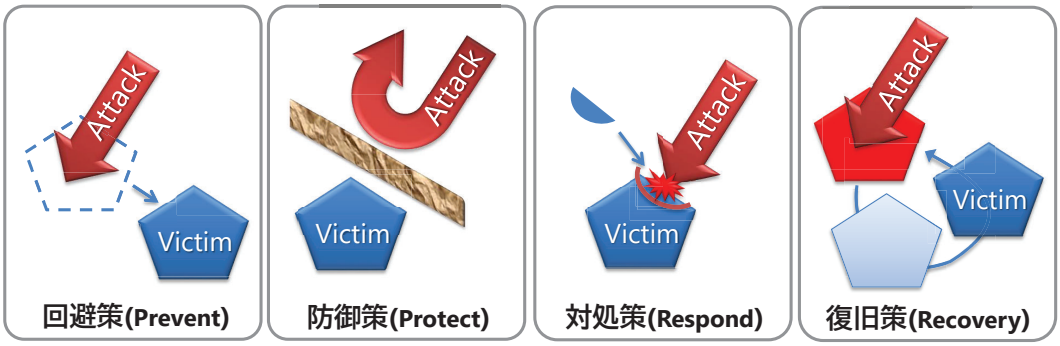
- ある程度の攻撃の仕組みを理解すること
  - サイバー攻撃を「静的な絵」として理解するのではなく、組織全般に渡る＆時間の流れのある「動的ストーリー」として理解することが必要
  - 主要な(攻撃)経路ポイントにおけるセキュリティ対策の要否及びレベルの設定には、業務慣習や部署風土も考慮することが必要



© 2020 Toshio Nawa
TLP:GREEN

④ すべてのサイバー攻撃対処に明確な目的を設定する

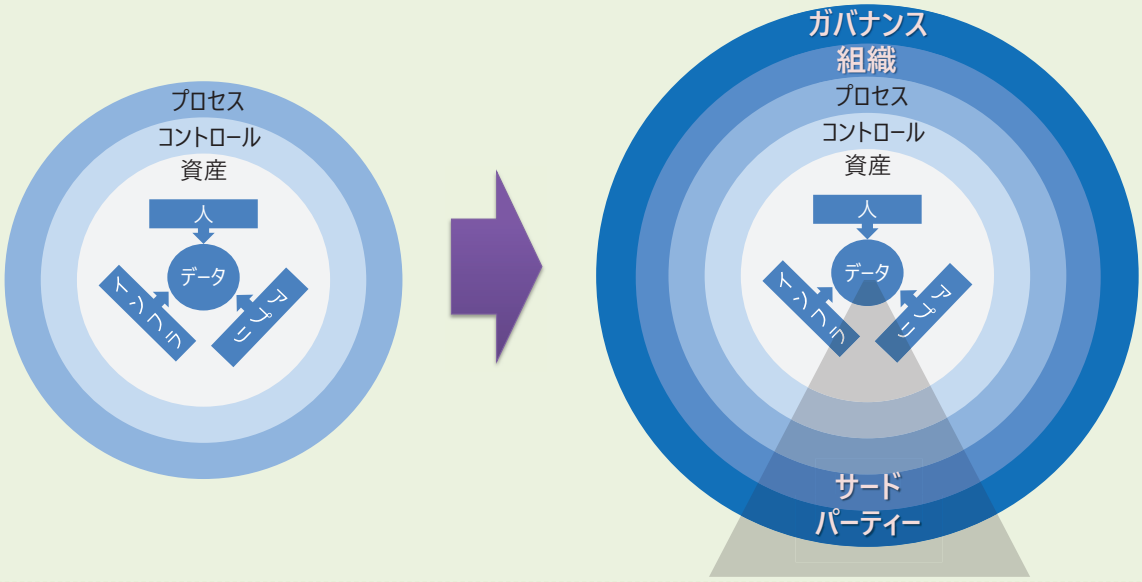
- サイバー脅威に対して、網羅性の高い対策を検討し、実装及び確実な運用をすること。
  - 日本国内の対策は、「防御策(Protect)に偏重」しているため、いたずらにコストがかかる。
  - 最近のサイバー防衛策における最善策(Best Practice)は、対処策(Respond)である。
    (最低限のリスクを受容し、実質的な被害を発生させないことで、結果的に有効な防衛策となる。)
  - 基本的な対策コンセプトは、次の4つのとおり。



© 2020 Toshio Nawa
TLP:GREEN

【参考】組織が実施すべきサイバーリスク・マネジメントのアプローチ

古典的なサイバーセキュリティの焦点　包括的なサイバーリスク・マネジメントのアプローチ



© 2020 Toshio Nawa
TLP:GREEN

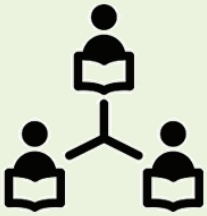
【参考】事態対処の能力を維持・向上させるプログラム



オンライン・セミナー



カンファレンス／セミナー



オンライン・コラボレーション



サイバー・レンジ



アナリスト・ミーティング



オンライン・カンファレンス



ミーティング



セキュリティ評価

© 2020 Toshio Nawa

TLP:GREEN

本資料に関する連絡先

名和 利男（Toshio NAWA）

SITE: https://www.nawa.to

PGP: 0xE38B4E01

© 2020 Toshio Nawa

TLP:GREEN

「交通分野へのサイバー攻撃に対する セキュリティ人材育成に関する調査研究」

経営層がとるべきサイバーセキュリティ対策について

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
田中　英彦

サイバーセキュリティの現状と対応

- 現状
  - 国際社会を跨るGAFA問題
  - 国間の攻撃が現実：物理攻撃の前にサイバー攻撃が日常
  - サイバーによるフェイクニュースと世論の制御
  - サイバー攻撃と被害の流布
  - 専守防衛の日本：牽制活動と陸海空に宇宙、サイバー・電磁波
- 情報共有の重要性
  - 情報寡占問題：便利の裏にある寡占の排除、連携による透明性確保
  - 企業間秘密とサイバー攻撃情報の共有問題
  - 情報共有に向けた法制度の担保：攻撃情報・マルウエア共有による対策向上の実施、対策実施及び研究の保護

経営者向けサイバーセキュリティ対策

- 情報時代の認識
  - IoEverything, DX, データ/情報の力で経験を置き換える
- リスクの拡大に向けた経営の再考
  - 物理的リスク、論理的リスク（距離・時間・規模越え）
- 膨大な責任を負う経営者の実質的心構えと為すべきこと
  - 善管注意義務にセキュリティも含まれる
  - 必ず実施の最小限/チェック項目
- 眼の前にあるオリンピック・パラリンピック
  - 攻撃は必至、既に織り込まれている

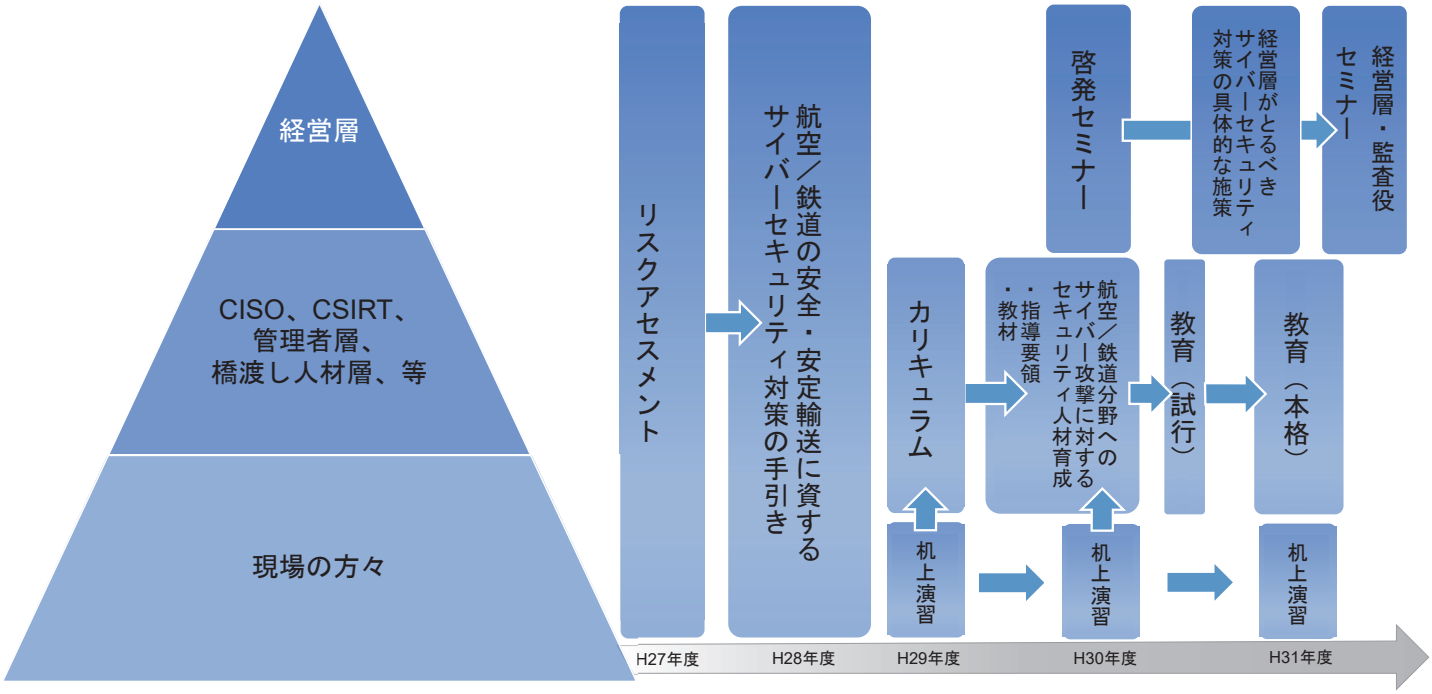
本日の内容

１．これまでの主な調査研究

２．経営層がとるべきサイバーセキュリティ対策について

２−１．背景
２−２．目的
２−３．10の施策案
２−４．各施策の関係図
２−５．施策案のポイントと位置づけ
２−６．オリンピック・パラリンピック対策に向けた施策

1．これまでの主な調査研究



2．経営層がとるべきサイバーセキュリティ対策について

2－1　背景

- サイバーセキュリティ対策の必要性：経営層の理解は高まり、経営層が社内で指示すべき対策項目の情報提供が進む

- 一方、対策項目は、全企業で一律に適用できず、対策を実施する上で分野に応じた現実的な心構えと施策を示す必要がある

（例）政府動向について

インフラ事業者に対策義務付け＝サイバー攻撃、司令塔を新設ー自民提言

自民党サイバーセキュリティ対策本部の高市早苗本部長らは１４日、安倍晋三首相に首相官邸で会い、サイバー攻撃への対応に関する提言書を手渡した。**重要インフラ事業者**に対して対策を義務付ける法律の制定や、司令塔となる「サイバーセキュリティ庁」の新設を盛り込んだ。

国民生活や経済活動に大きく関わるとして政府が指定する重要インフラ１４分野のうち、現行法でサイバー対策を義務付けられているのは電気とガスの二つだけ。提言書は、情報通信や金融など**他の分野でも対策**を取ることや、重大事案が発生した際に遅滞なく**政府に報告**することを求めた。

サイバーセキュリティ庁は、中央省庁のサイバー対策を担う内閣官房の「内閣サイバーセキュリティセンター（ＮＩＳＣ）」を拡充するもの。大阪・関西万博が開かれる２０２５年をめどに内閣府の外局として設置するよう要請した。

出典：時事通信（2019年5月14日付）、
https://www.jiji.com/jc/article?k=2019051401171&g=pol

（例）事業被害について①

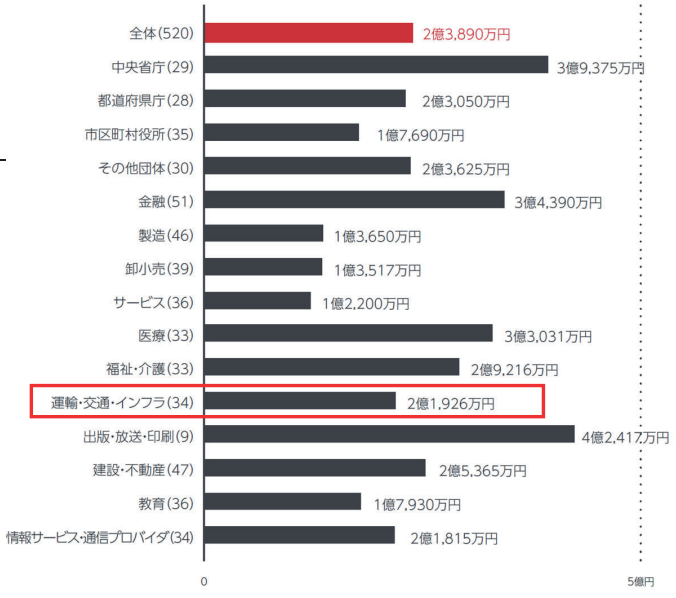
運輸・交通・インフラの年間平均被害総額は、約２．２億円

トレンドマイクロが2019年6月、国内の民間企業や官公庁自治体を対象に行った「法人組織におけるセキュリティ実態調査2019年版」によると、セキュリティインシデントによる年間平均被害総額は約2.4億円、4年連続2億円を超える結果と発表した。

特筆すべき点として、重大被害発生率が業種全体で最も低い出版・放送・印刷の年間平均被害総額が、昨年調査の約1億円から約4.2億円と急増し、他業種よりも高い結果となっていること、重大被害発生率がそれほど高くない医療の年間平均被害総額が約3.3億円と全体平均を大きく上回る結果となっていることを挙げ、セキュリティインシデントによる被害の発生率が低い業種の場合でも、実被害額という観点では、事業を脅かす深刻な結果につながる可能性があることを示唆している。

出典：トレンドマイクロ株式会社、法人組織におけるセキュリティ実態調査2019年版

・重大被害による年間平均被害総額（業種別）

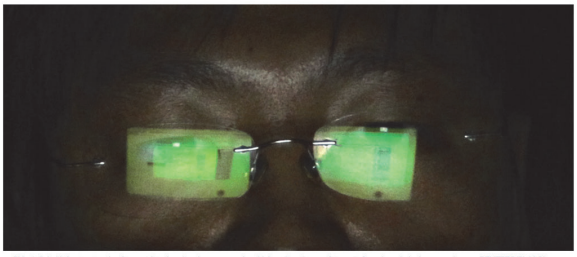


※（ ）内の数字はサンプル数

（例）事業被害について②

ロイズは、ニューヨーク市だけでも2020年にサイバー関連の損失が23億ドルを超える可能性があると見積もっている。

Cities are easy prey for cybercriminals. Here's how they can fight back



Cities' digital infrastructure is often outdated and under-resourced - which makes them soft targets for cybercriminals. Image: REUTERS/Pichi Chuang

30 Sep 2019

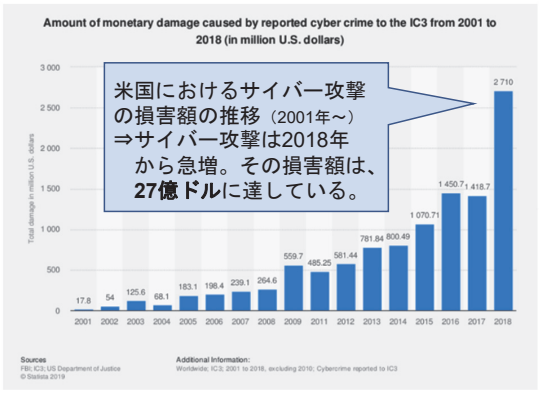
Robert Muggah
Principal, SecDev Group

Marc Goodman
Founder, Future Crimes Institute

Make no mistake: the world is in the early stages of a techno-war against city governments and urban infrastructure. And while some cities have bolstered their capabilities to patch their vulnerabilities, they are entirely unprepared for the scale of cyberthreats that are coming.

The scope of the cyber threat to cities is becoming clearer. According to industry experts, more than 70 percent all reported ransomware attacks in the U.S. target state and local governments. At least 180 public safety call centers were also targeted in the last two years. （中略）The impacts of the cyber threat should not be taken lightly.

Lloyds estimates that New York city alone could face over $2.3 billion in cyber-related losses in 2020. Given their snowballing deficits, cities can ill afford the burgeoning costs of these digital incursions.



出典：WORLD ECONOMIC FORUM、
https://www.weforum.org/agenda/2019/09/our-cities-are-increasingly-vulnerable-to-cyberattacks-heres-how-they-can-fight-back/

２ － ２．目的

◆目的：3月末に報告書提出予定

本研究では、2020年東京五輪大会に向け、経営者がとるべきサイバーセキュリティ対策についての具体的な施策の検討、ならびに過年度の成果物を総括したサイバーセキュリティ対策に関する提言のまとめを目的とする。

経営層の役割は、組織規模や置かれている環境に関わらず、リスクを回避して事業を継続するための経営判断を行うことである。今日では、サイバーセキュリティリスクが重要な経営リスクとなっていることから、経営層がサイバーセキュリティリスクの重要性を認識し、これを踏まえた上で経営判断を行うために必要となる施策について、具体的に示すことを目的とした。

なお、施策は、主として経営層が組織内において指示して実現すべき対策を指すが、本研究では、経営層が自ら実行することが望まれる行動指針についても施策に含めた。経営層がとるべきサイバーセキュリティ対策は、組織規模や組織が置かれている環境により千差万別であり、実現すべき対策を一律に定めることは難しい。このため、施策の具体化に際しては、これらの差異に配慮する記載に努めた。

２ － ３．　１０の施策案

施策１　サイバーセキュリティリスクの重要性について経営会議において情報を分析する。

施策２　サイバーセキュリティリスクに関する検討組織を設置する。

施策３　危機管理を統括する既存部門とCSIRTの連携を強化する。

施策４　PDCAサイクルを実施する組織からリスク対応について定期的な報告を受ける。

施策５　経営層として情報共有に努める。

施策６　危機管理コミュニケーション力を高める。

施策７　有事に備えた現場担当者教育を強化する。

施策８　監査機能を積極活用する。

施策９　サイバーセキュリティリスクへの取り組みについて積極的な情報開示に努める。

施策10　自社のセキュリティ水準の将来目標を定め目標達成や進捗状況を管理する。

１０の施策案
1/１０

施策１　サイバーセキュリティリスクの重要性について経営会議において情報を分析する。

分析結果に基づき、経営層が共通した認識の下で意思決定を行う。

〇施策例

- 発生し得る重大なサイバーセキュリティリスク（例えば、サイバーテロによる業務妨害、経営戦略上において重要な営業秘密の流出による損害、ビジネスメール詐欺）を経営リスクとして認識する。
- 重大なサイバーセキュリティリスクについて、取締役及び監査役間において意見交換する等、経営層の間で日頃より認識の共有に努める。
- サイバーセキュリティリスクの重要性と対応について、取締役会等の経営会議における審議事項に含め、協議・分析を行う。年2回程度の集中審議を行い、対応状況を確認する。
- 情報セキュリティ対策の不備がサイバーセキュリティリスク発言の端緒となることを踏まえ、自組織における情報セキュリティ対策にも留意する。

〇施策を怠った場合のシナリオ

- 経営層が自らの状況認識を高めることを放棄し、積極的に脅威情報を収集を怠ることにより、組織全体がサイバーセキュリティリスクに目を向けなくなり、対策が停滞する。
- サイバーセキュリティ対策などの実行が組織の方針と一貫したものとならない。
- サイバー攻撃による事故が発生した場合に、**善管注意義務違反を問われる**。

サイバーセキュリティ経営ガイドライン

経営者が認識すべき3原則

1. 経営者は、サイバーセキュリティリスクを認識しリーダーシップによって対策を進めることが必要

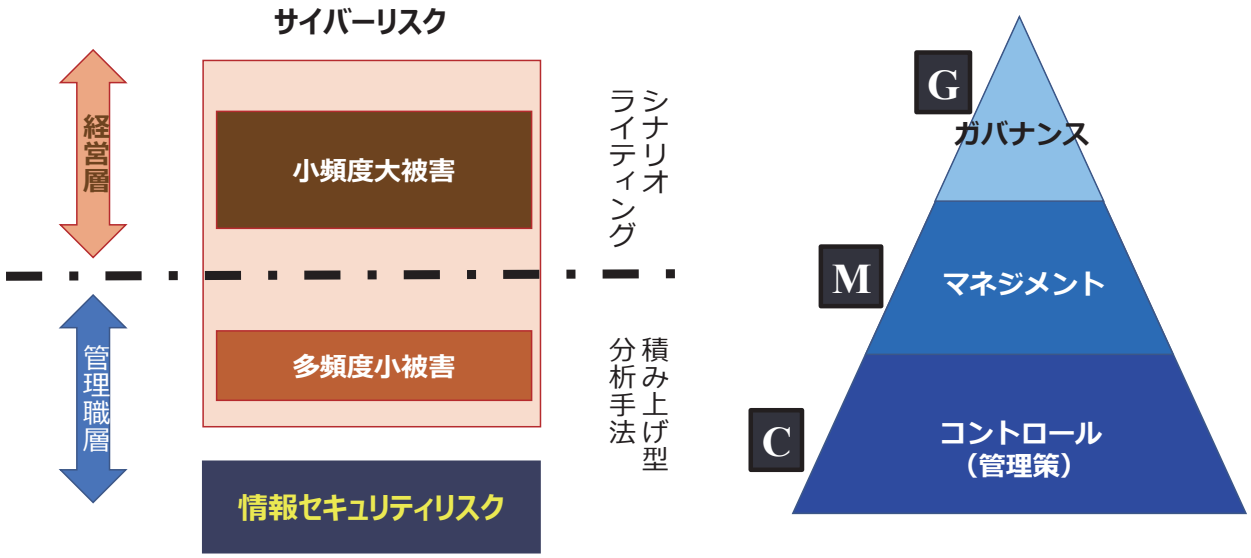
特徴

2. 自社のみならず、ビジネスパートナーや委託先も含めたセキュリティ対策が必要

3. 平時及び緊急時のいずれにおいても、関係者との適切なコミュニケーションが必要

交通セキュリティセミナー　交通分野のサイバーセキュリティ対策における監査役の役割（令和2年1月29日開催）
講演１「サイバーテロの可能性と経営としての監査役の役割」株式会社ベネッセホールディングス　顧問　丸山司郎氏　講演資料より

サイバーリスク判断における経営の役割



交通セキュリティセミナー　交通分野のサイバーセキュリティ対策における監査役の役割（令和2年1月29日開催）
講演２「サイバーセキュリティの監査」NPO 日本セキュリティ監査協会　エグゼクティブフェロー　永宮直史氏　講演資料より

重要インフラ企業の経営者に求められる責任

- 経営リスクに占める、サイバーテロの位置づけ
- 善管注意義務を果たしているか
- ちゃんとやったと、説明できるか
- クライシスコミュニケーションの体制は

交通セキュリティセミナー　交通分野のサイバーセキュリティ対策における監査役の役割（令和2年1月29日開催）
講演１「サイバーテロの可能性と経営としての監査役の役割」株式会社ベネッセホールディングス　顧問　丸山司郎氏　講演資料より

１０の施策案
2/１０

施策２　サイバーセキュリティリスクに関する検討組織を設置する

経営層が情報を分析して施策に反映させるために、専門の検討機能を組織する。

○施策例

- サイバーセキュリティリスクに関する検討組織を設置し、経営会議における**協議・分析を支援する組織**として活用する。
- 検討組織において以下を検討し、経営会議におけるインプット情報とする。
  - 重視すべきサイバーセキュリティリスクの選定と優先順位付け
  - リスクの発生確率や発生したときの損害試算
  - セキュリティポリシー策定あるいは修正方針の立案
  - リスクマネジメント、事業継続計画（BCP）とサイバーセキュリティリスクの関係
- 検討組織からのインプット情報をもとに、ヒト、組織、予算、等の社内**資産を確保**する。

○施策を怠った場合のシナリオ

- サイバーセキュリティリスクの管理体制を整備していない場合、組織としてサイバーセキュリティリスクの把握が出来ない。
- 適切な予算確保が出来ていない場合、組織内でのサイバーセキュリティ対策の実施や人材の確保が困難となるほか、信頼できる外部のベンダーへの委託が困難となる恐れがある。

１０の施策案
3/１０

施策３　危機管理を統括する既存部門とCSIRTの連携を強化する。

経営リスクとサイバーリスクを統括管理するために組織連携を強化する。

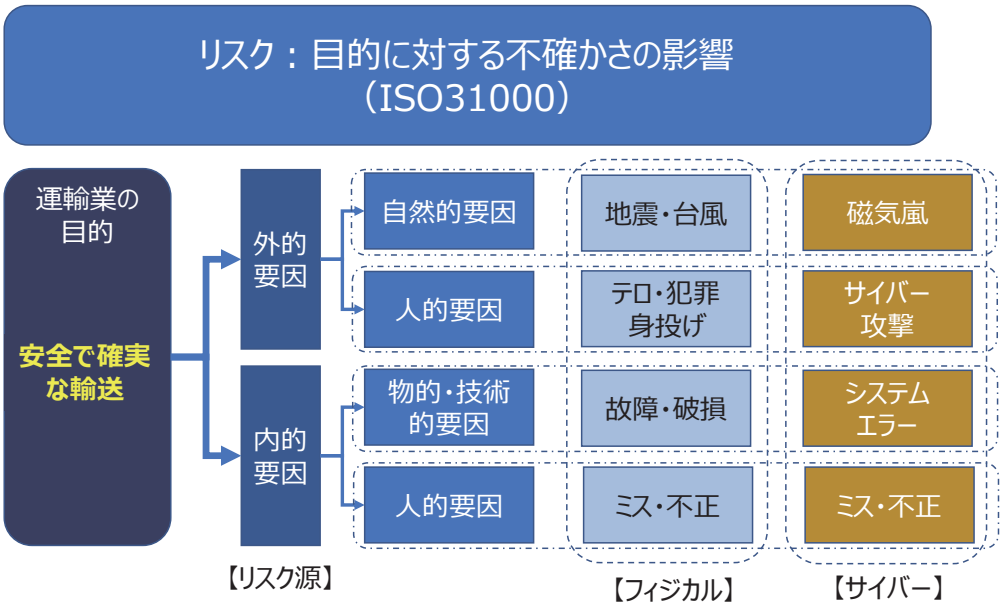
○施策例

- 事業部門におけるサイバー攻撃対応において、迅速にCSIRTと連携できるよう組織を整備する。
- サイバー攻撃の発生に備えて、**危機管理を統括する部門とCSIRT**が連携できるよう組織を整備する。
- サイバー攻撃により業務停止に至った場合、**速やかに再開**するため、関係機関との連携や復旧作業を実施できる管理体制を構築する。
- 構築した管理体制の下、重要な業務をいつまでに復旧すべきかの目標について、組織全体として整合をとる（例えばBCPで定めている目標との整合等）。
- 必要に応じて、速やかに安全推進を所管する部署と連携できる管理体制を構築する。

○施策を怠った場合のシナリオ

- 重要な業務が適切な時間内に復旧できず、企業経営に致命的な影響を与える恐れがある。
- サイバーセキュリティリスクに応じた適切な対策が行われていない場合、サイバー攻撃が発生した場合の被害が**拡大する可能性**がある。
- 事業部門を含む緊急時の対応体制を整備していないと、原因特定のための調査作業において、組織の内外の関係者間のコミュニケーションが取れず、速やかな対処ができない。

リスクとは



交通セキュリティセミナー　交通分野のサイバーセキュリティ対策における監査役の役割（令和2年1月29日開催）
講演２「サイバーセキュリティの監査」NPO 日本セキュリティ監査協会　エグゼクティブフェロー　永宮直史氏　講演資料より

サイバーセキュリティの要点

要点１

リスク評価

- ■ 人的・物的被害に着目したリスク評価
  - □ ISO31000に基づくリスク評価を追加
    - ✓ めったに生じないが、甚大な被害が生じるリスク（想定外を想定する）

要点2

情報セキュリティ防御ができなかった場合の対策を強化

- ■ 検知手順・インシデント判定手順の確立
- ■ CSIRTの確立
- ■ 事業継続：物理的対処チームや復旧プロセス等との連携及びサイバーレジリエンスの確立

※サイバーレジリエンス：
損害を被ったシステム部分を除いて、業務を継続する仕組みがあること

交通セキュリティセミナー　交通分野のサイバーセキュリティ対策における監査役の役割（令和2年1月29日開催）
講演２「サイバーセキュリティの監査」NPO 日本セキュリティ監査協会　エグゼクティブフェロー　永宮直史氏　講演資料より

１０の施策案
4/１０

施策４　PDCAサイクルを実施する組織からリスク対応について定期的な報告を受ける。

報告をもとに、経営層が重視するサイバーリスクへの対応状況を定期的に確認する。

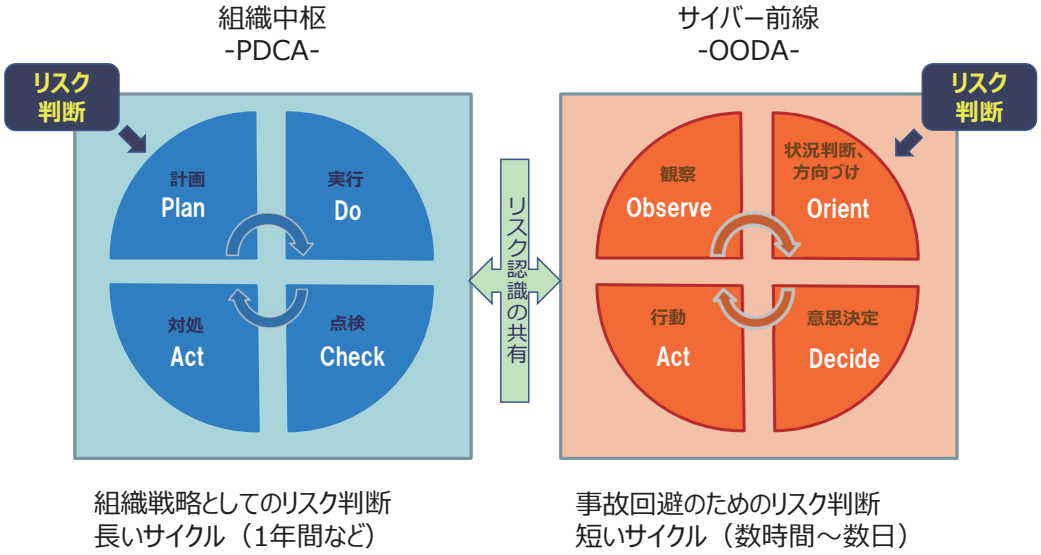
○施策例

- PDCAサイクルにおいて実施するリスク分析について、事業被害ベースのリスク分析手法を実施することを担当組織に指示する。
- 経営層として重視するサイバーセキュリティリスクについて、リスク分析に反映させる。
- 経営層として重視するサイバーセキュリティリスクについて、対応状況を報告させる。

○施策を怠った場合のシナリオ

- PDCA（Plan[計画]、Do[実行]、Check[実施状況の確認・評価]、Act[改善]）を実施する体制が出来ていないと、立てた計画が確実に実行されない恐れがある。
- 事業被害ベースのリスク分析を採用しないことにより、経営層として重視するサイバーセキュリティリスクの対策状況が十分なものか判断できなくなる。
- 最新の脅威への対応ができているかといった視点も踏まえて組織のサイバーセキュリティ対策を定期的に見直さないと、サイバーセキュリティを巡る環境変化に対応できず、新たに発生した脅威に対応できない恐れがある。

二つの活動とリスク判断



交通セキュリティセミナー　交通分野のサイバーセキュリティ対策における監査役の役割（令和2年1月29日開催）
講演２「サイバーセキュリティの監査」NPO 日本セキュリティ監査協会　エグゼクティブフェロー　永宮直史氏　講演資料より

１０の施策案
5/１０

施策５　経営層として情報共有に努める。

経営層が関与することの組織的な効果を踏まえ、積極的な情報共有に努める。

〇施策例

- サイバーセキュリティリスクに関する検討組織から情報を入手する。
- PDCAを実施する組織から定期報告を受け、社内の情報セキュリティ対策の現状を把握する。
- サイバーセキュリティに関する知見を有する者が誰であるか確認しておく。
- 経営層として認識する重要なサイバーセキュリティリスクについて**社内に周知**する。
- 現場に赴き、サイバーセキュリティリスクについて担当者と対話する。
- 経営層に向けたセミナー等に参加し、情報を収集する。
- 同業他社の経営層や所管省庁との間で、サイバーセキュリティリスクに係る**情報共有**に努める。

〇施策を怠った場合のシナリオ

- 経営層としての重要情報を見落とすことにより、経営判断を誤る。
- 経営層としての情報共有を怠ることにより、社内のサイバーセキュリティ対策の方針が徹底しない。

重要なリスクコミュニケーション

組織全体でリスク認識が共有されていると、ガバナンスが利きやすい

- リスクコミュニケーション※の意義：
  - 組織内外の関係者が「リスク」「意思決定の根拠」「特定の活動が必要な理由」についての理解が容易になる
- リスクコミュニケーションの実施段階
  - リスクアセスメントのみではなく、リスク対策の実施、レビュー、記録等リスクマネジメントのあらゆるプロセスで行う
  - サイバーセキュリティ対策もリスクマネジメントプロセスとして行われる
- リスクコミュニケーションのねらい
  - プロセスの各段階で組織内外の専門家の知識を集める
  - リスク基準を定め、リスク評価の場合に異なる見解に考慮する
  - リスク監視及び意思決定を行うための十分な情報を提供する
  - **リスクの影響を受ける者たちの一体感と当事者意識を醸成する**

（注）ISO31000：2018に基づき加工

※ ISO31000では「リスクコミュニケーション及び協議」

交通セキュリティセミナー　交通分野のサイバーセキュリティ対策における監査役の役割（令和2年1月29日開催）
講演２「サイバーセキュリティの監査」NPO 日本セキュリティ監査協会　エグゼクティブフェロー　永宮直史氏　講演資料より

オリンピック後も役立つ節目作戦



経営者が直接セキュリティの現場に行って、
毎月（６回）話を聞く



経営者がインシデント事例３つの訓練をする
（DDoS、平昌、三菱）



外部のプロに、穴を探してもらう。
（ペネトレーションテスト）

交通セキュリティセミナー　交通分野のサイバーセキュリティ対策における監査役の役割（令和2年1月29日開催）
講演１「サイバーテロの可能性と経営としての監査役の役割」株式会社ベネッセホールディングス　顧問　丸山司郎氏　講演資料より

１０の施策案
6/１０

施策６　危機管理コミュニケーション力を高める。

経営層自身が適切な有事対応できるよう、平時より能力を高める。

○施策例

- 危機管理コミュニケーションの事例を集め、失敗事例の要因等を参考にする。
- 特にサイバー攻撃が発生した際に、**助言を求める者**が誰であるかを予め確認しておく。
- 既存の事業継続計画にサイバー攻撃に起因するシナリオを追加する。追加シナリオに沿ってマニュアルを改定する。
- 経営層を含む関係者により、マニュアルに沿った**模擬訓練**を行う。

○施策を怠った場合のシナリオ

- 速やかな情報開示が行われない場合、顧客や取引先等にも被害が及ぶ恐れがあり、損害賠償請求など責任を問われる場合がある。
- 記者会見での**失言、情報を隠蔽**しているような誤解を与えてしまうことによって、事態が悪化してしまうことがある。
- ネガティブな印象によって企業価値の低下を招く恐れがある。

１０の施策案
7/１０

施策７　有事に備えた現場担当者教育を強化する。

攻撃を最初に検知するのは現場担当者であり、これを踏まえた教育を行う。

○施策例

- **現場担当者に対する教育**を行い、重大なサイバーセキュリティリスクが発生した際に迅速かつ適切な対応が行えるよう日頃から備える。
- サイバー攻撃が発生した際に適切に関係部門と連携ができるよう、現場担当者と関係部門を交えた演習・訓練を実施する。
- 体制について検証するために、社外の演習・訓練への参加を促進する。
- 現場担当者向け研修のための**予算**を確保し、継続的に役割に応じたセキュリティ教育を実施する。
- 経営層が重視するサイバーセキュリティリスクについて、社内に積極的に発信する。

○施策を怠った場合のシナリオ

- 現場担当者教育を怠ることにより、サイバー攻撃が発生した際の**初動対応**が遅れ、被害が拡大する。
- 経営層が重視するサイバーセキュリティリスクが現場担当者に周知されないことにより、サイバー攻撃対策が徹底されない。

１０の施策案
8/１０

施策８　監査機能を積極活用する。

監査を忌避する風潮を打破し、ガバナンス強化の仕組みとしての活用を図る。

〇施策例

- 経営層が重視するサイバーセキュリティリスクに適切に対処しているかどうかを点検・評価・検証するよう、監査人に指示する。あるいは、経営層が重視するサイバーセキュリティリスクを**監査の観点に加える**よう、システム監査やセキュリティ監査を主管する部門に対して指示する。
- サイバーセキュリティ対策のチェックを実施することができる内部監査人の育成を行う。
- 系列企業、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の委託先等のサイバーセキュリティ対策状況（監査を含む）の報告を受け、把握する。

〇施策を怠った場合のシナリオ

- 経営層が重視するサイバーセキュリティリスクについての対策が徹底されない。
- 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ことにより、これらの企業を踏み台にして自社が攻撃される。
- システム管理などの委託業務において、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。

サイバーセキュリティ監査の確認事項

- 企業がサイバーセキュリティに的確に対応できているかの確認
  - リスク認識の共有：組織末端までサイバーリスクの理解が共有できているか？
  - 組織態勢の確立　：平時も異常時も円滑に全員が動けるか？
  - 事　業　継　続　：異常時に事業活動が途切れないか？

- 企業態勢がしっかりしているかの確認
  - 経営者が役割を果たしているか
    - 企業存続に影響するサイバーリスクを常に見直しているか？
    - リスク認識の共有を図っているか？
    - 適切なガバナンスを行っているか？
  - 管理者が適切に管理しているか
    - PDCAがしっかり回っているか？
  - 技術者が適切に対処しているか
    - OODAによりインシデント検知が行われているか？
    - インシデント対応態勢が動くか？

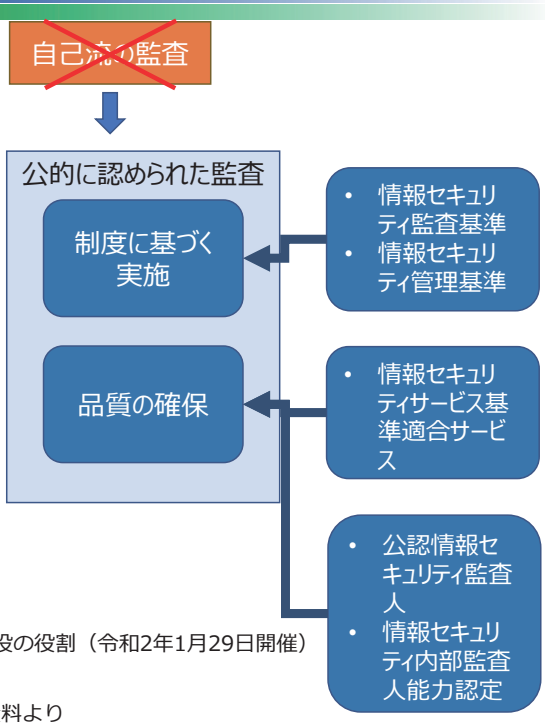
交通セキュリティセミナー　交通分野のサイバーセキュリティ対策における監査役の役割（令和2年1月29日開催）
講演２「サイバーセキュリティの監査」NPO 日本セキュリティ監査協会　エグゼクティブフェロー　永宮直史氏　講演資料より

基本となる情報セキュリティ監査

■監査の目的
- □情報セキュリティマネジメントが効果的か

■監査の方法
- □準拠性監査
  - ◆組織が定めたルールに準拠しているか
- □**有効性（妥当性）監査**
  - ◆**リスク管理が有効か（管理策がリスクに対して妥当か）**

■ **ISMS適合性評価制度の限界**
- □ 監査の方法等は経営者が決める
- □ ISO27006により審査工数の上限がある



交通セキュリティセミナー　交通分野のサイバーセキュリティ対策における監査役の役割（令和2年1月29日開催）
講演２「サイバーセキュリティの監査」
NPO 日本セキュリティ監査協会　エグゼクティブフェロー　永宮直史氏　講演資料より

１０の施策案
9/１０

施策９　サイバーセキュリティリスクへの取組について積極的な情報開示に努める。

株主や投資家等を含め、多様な利害関係者に向けた積極的な情報開示を行う。

○施策例

- サイバーセキュリティリスクを考慮した**セキュリティポリシーを策定**する。その際、情報システムのみではなく、製造、販売、サービス等、事業に応じた対応方針を検討する。
- コーポレートガバナンス報告書にサイバーセキュリティリスクへの取り組みを記載することを検討する。
- サイバーセキュリティリスクへの取り組みを一般公開することでステークホルダーや社会に対する企業としての姿勢を示し、信頼性を高める。
- サイバーセキュリティ対策の状況について、サイバーセキュリティリスクの性質・度合いに応じて、情報セキュリティ報告書、CSR 報告書、サステナビリティレポートや**有価証券報告書等**への記載を通じて開示を検討する。

○施策を怠った場合のシナリオ

- 適切な開示を行わなかった場合、社会的責任の観点から、事業のサイバーセキュリティリスク対応についてステークホルダーの信頼を失うとともに、インシデント発生時に企業価値が大きく低下する恐れがある。

１０の施策案
１０/１０

施策１０　自社のセキュリティ水準の将来目標を定め、目標達成や進捗状況を管理する。

中長期の事業計画と整合したサイバーセキュリティ対策を計画し、実行する。

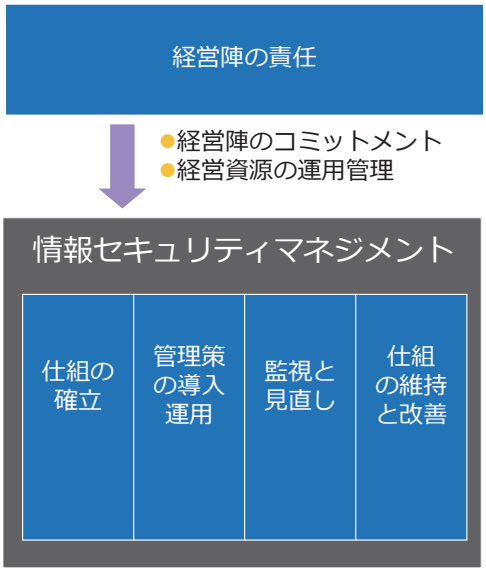
○施策例

- 中長期の事業計画において達成することが必要となる自社の**セキュリティ水準**（組織的、人的、技術的対策水準）を定める。
- 自社のセキュリティ水準の**将来目標**を定め、中長期の事業計画と整合させる。
- 対象となる事業計画には、新規事業も含まれる。
- 自社のセキュリティ水準については、組織的対策、人的対策、技術的対策が含まれる。
- 内部監査の実施に際して、目標とすべきセキュリティ水準の達成度を確認する。

○施策を怠った場合のシナリオ

- 企業の経営戦略に基づき、各企業の状況に応じた適切なリスク対応を実施しなければ、**過度な対策**により通常の業務遂行に支障をきたすなどの不都合が生じる恐れがある。
- 受容できないリスクが残る場合、想定外の損失を被る恐れがある。

セキュリティマネジメントシステム



a. 基本方針を確立する
b. 目的を定め、計画の策定を指示する
c. 情報セキュリティに対する役割や責任を定める
d. 情報セキュリティの重要性を組織内に周知する
e. 必要な経営資源を提供する
f. リスク受容の基準、受容可能なリスクの水準を決める
g. 内部監査の実施を指示し支援する
h. 経営者の視点からレビューを実施する

（ISO/IEC27001：2005による）

交通セキュリティセミナー　交通分野のサイバーセキュリティ対策における監査役の役割（令和2年1月29日開催）
講演２「サイバーセキュリティの監査」NPO 日本セキュリティ監査協会　エグゼクティブフェロー　永宮直史氏　講演資料より

２ － ４． 各施策案の関係図

（経営層からの）
アウトプットの観点

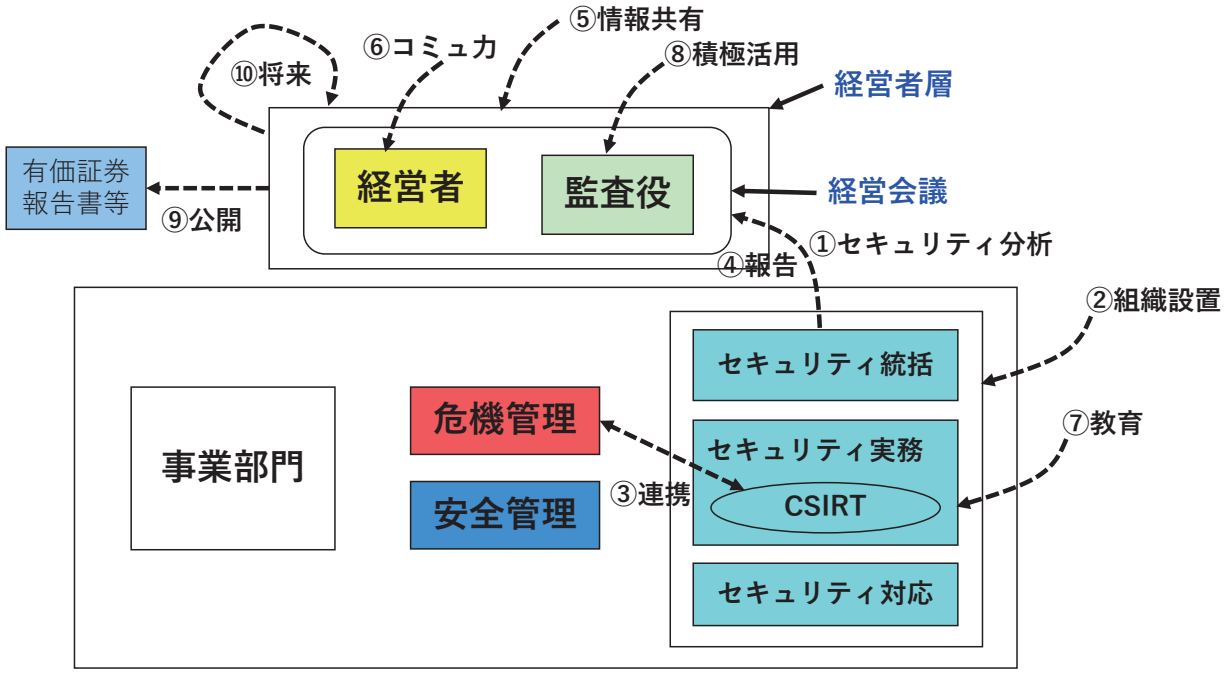
（経営層への）
インプットの観点

施策１	サイバーセキュリティリスクの重要性について経営会議において情報を分析する。
施策２	サイバーセキュリティリスクに関する検討組織を設置する。
施策３	危機管理を統括する既存部門とCSIRTの連携を強化する
施策４	PDCAサイクルを実施する組織からリスク対応について定期的な報告を受ける。
施策５	経営層として情報共有に努める。
施策６	危機管理コミュニケーション力を高める。
施策７	有事に備えた現場担当者教育を強化する。
施策８	監査機能を積極活用する。
施策９	サイバーセキュリティリスクへの取り組みについて積極的な情報開示に努める。
施策10	自社のセキュリティ水準の将来目標を定め目標達成や進捗状況を管理する。

２ － ５． 施策案のポイント

- 経営層（監査役を含む）は、サイバーセキュリティリスクを重要な事業リスクの一環として捉え、他の事業リスクとともに危機管理の対象として認識する必要がある。
- 経営層は、組織整備、情報把握、指示、確認、情報発信、といった一連の経営活動に即して、重大なサイバーセキュリティリスクに対処するための施策を実施する必要がある。
- 施策の実施に際しては、意思決定を支援する組織（検討組織）及び施策を徹底する組織（監査等）と密に連携することが望まれる。

各施策の位置づけ

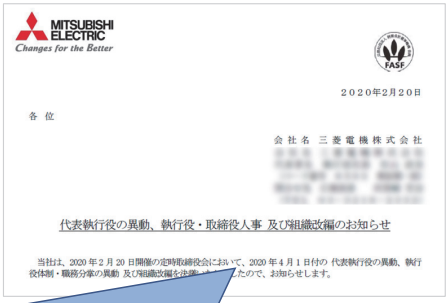


セキュリティ統括室の事例

- 事例①三菱電機

三菱電機がセキュリティ統括室、元エネ庁長官も迎える

三菱電機は20日、同社がサイバー攻撃を受けたことなどから、4月1日に「情報セキュリティ統括室」を新設すると発表した。今回の攻撃への対応の教訓を生かし、社長直轄で一元的に対策を担うようにする。渉外などを担当する常務執行役に、経済産業省の資源エネルギー庁長官を2018年に退官した日下部聡氏が同日付で就く人事も発表した。（日本経済新聞 2020/2/20付）


MITSUBISHI ELECTRIC
Changes for the Better

2020年2月20日

各 位

会社名 三菱電機株式会社

代表執行役の異動、執行役・取締役人事 及び組織改編のお知らせ

当社は、2020年2月20日開催の定時取締役会において、2020年4月1日付の 代表執行役の異動、執行役体制・職務分掌の異動 及び組織改編を決議いたしましたので、お知らせします。

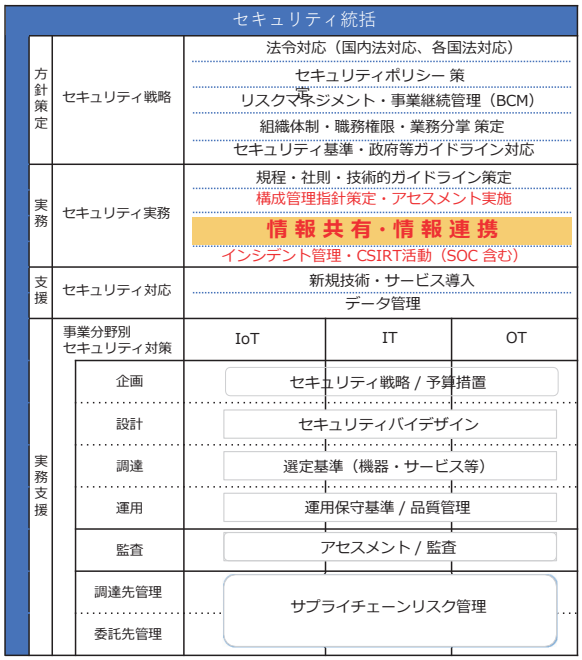
5．組織改編（2020 年4 月1 日付）

（1）**情報セキュリティ統括室の新設**

当社グループ全体の情報セキュリティ体制強化に向け、迅速な判断とインシデント発生時のお客様や関係機関との早期情報共有等を目的に、**情報セキュリティ全般の企画・構築・運営の機能を一元的に担う社長直轄の情報セキュリティ統括室を新設する。**

（三菱電機株式会社公式HPより）

今後：セキュリティ統括室における情報共有・情報連携機能の拡充



セキュリティ統括室の機能
（産業横断サイバーセキュリティ人材育成検討会（CRIF CSF）資料より転載）



フュージョンセンターの概念図
（Citi の公開資料より和訳転載）

２－６．オリンピック・パラリンピック対策に向けた施策

施策１　サイバーセキュリティリスクの重要性について経営会議において情報を分析する。

施策２　サイバーセキュリティリスクに関する検討組織を設置する。

施策３　危機管理を統括する既存部門とCSIRTの連携を強化する。

施策４　PDCAサイクルを実施する組織からリスク対応について定期的な報告を受ける。

施策５　経営層として情報共有に努める。

施策６　危機管理コミュニケーション力を高める。

施策７　有事に備えた現場担当者教育を強化する。

施策８　監査機能を積極活用する。

施策９　サイバーセキュリティリスクへの取り組みについて積極的な情報開示に努める。

施策10　自社のセキュリティ水準の将来目標を定め目標達成や進捗状況を管理する。

おわり