サイバー攻撃に対する
セキュリティ情報共有組織（ISAC）の構築
に関する調査研究

平成 30 年 3 月

一般財団法人　運輸総合研究所

はじめに

本報告書は、平成 29 年度日本財団助成事業として実施した「サイバー攻撃に対するセキュリティ情報共有組織（ISAC）の構築に関する調査研究」の成果の一部をまとめたものである。

近年急増しているサイバー攻撃は、我が国にとって大きな脅威となっている。実際に、近年開催されたオリンピック・パラリンピックにおいても、システム障害などのサイバー攻撃の被害が報告されている。鉄道、航空といった交通分野はサイバーセキュリティ戦略において重要インフラ分野に特定されているが、海外では攻撃事例も散見されており、仮に 2020 年東京オリンピック・パラリンピック開催期間中にサイバー攻撃が発生した場合、影響が甚大となる恐れがある。

実際の攻撃には事業者が対応するが、攻撃手法がより複雑化しているため、近年では業界全体でセキュリティ情報を共有する組織を構築した上で対応する体制が求められている。

当研究所では、平成 27 年度からの 2 年間で「東京オリンピック・パラリンピックに向けた交通機関へのサイバーテロ対策に関する調査研究」を実施し、鉄道分野及び航空分野を対象として、事業者のサイバーセキュリティに対する取組の実態を評価、検証するとともに、国内外の対策ガイドラインなどの整理やリスク分析を踏まえ、我が国に適応した対策手引きの作成を行った。

本年度は、鉄道分野及び航空分野における ISAC 構築に向けた基本方針、組織構成、構築手順等の研究を行うため、国内外の情報共有組織におけるセキュリティ情報の収集、分析、提供の実態、ニーズや課題について把握し、鉄道分野及び航空分野における ISAC の実現に向けた検討等を行った。本報告書が鉄道分野及び航空分野における ISAC の構築やセキュリティ情報共有活動を行う際の参考資料となれば幸いである。

本研究の実施にあたっては、株式会社三菱総合研究所にご協力を頂いた。ここに改めて深く感謝の意を表す次第である。

平成 30 年 3 月

一般財団法人　運輸総合研究所
会長　　黒野　匡彦

目次

第１章　調査概要

１．１　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・パラリンピックが開催されるが、過去のオリンピックでは幾度となくサイバーテロの標的となっている。そのため、2020年東京オリンピック・パラリンピック大会の成功に向けて、サイバーテロ対策は重要な課題となっている。

鉄道分野・航空分野は、我が国のサイバーセキュリティ戦略において重要インフラ分野に特定されており、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。最近では、鉄道分野・航空分野でも制御システムのIoT（Internet of Things）化の波が進む中、新しい脅威が生まれている。国内では、現時点においては大規模なサイバー攻撃は報告されていないが、海外では鉄道分野・航空分野においても被害が報告されるようになってきていることからも、対策は急務となっている。

重要インフラ事業者等のサービスの維持・復旧能力の向上のためには、IT障害に関する情報の共有することが重要と考えられている。日本国内では、内閣官房情報セキュリティセンター（現：内閣サイバーセキュリティセンター（NISC））のIT戦略本部の下に設置された「情報セキュリティ政策会議」において決定された、「重要インフラの情報セキュリティ対策に係る行動計画」（2005 年）に基づき、重要インフラ分野ごとに政府等からの情報を共有・分析を行うセプター（CEPTOAR：Capability for Engineering of Protection, Technical Operation, Analysis and Response）が整備されている。

米国では、1998年の大統領令において、重要インフラ分野におけるセキュリティ向上のために、重要インフラ分野ごとにセキュリティに関する情報を共有するISAC（Information Sharing and Analysis Center）の概念が示され、セキュリティ対策の向上に一定の成果を上げている。セキュリティに関する情報を共有することで、ISACに加盟する企業の多様な知見を相互に活用し、直面する脅威に対する防御をより一層強化することが可能となる。

１．２　目的

上記の背景を受け、鉄道分野及び航空分野におけるISAC構築に向けた基本方針、組織構成、構築手順等の研究を行うため、国内外の情報共有組織におけるセキュリティ情報の収集、分析、提供の実態、ニーズや課題について把握し、鉄道分野及び航空分野におけるISACの実現に向けた検討等を行う。

１．３　情報共有組織（ISAC）の検討フロー

本調査の検討フローは下図の通り。

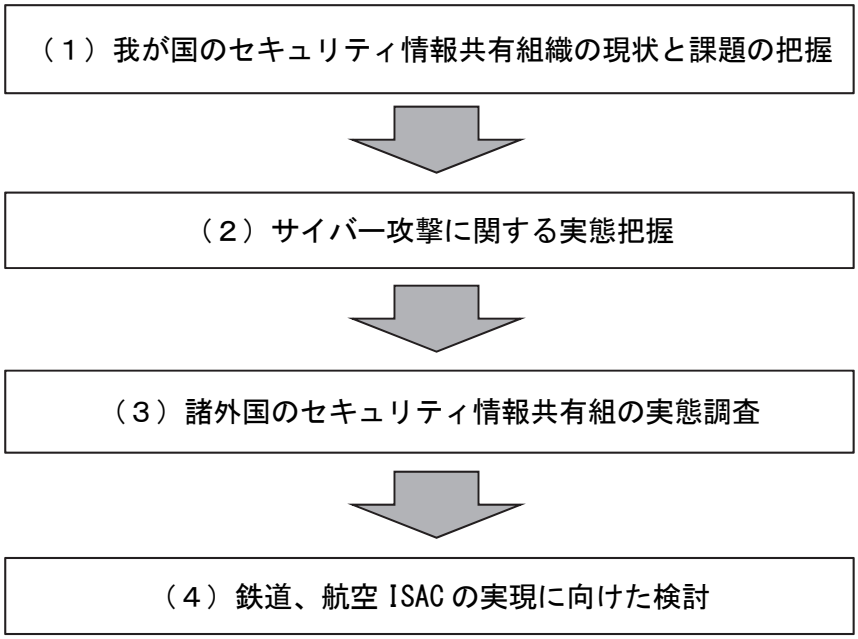


図　本研究の検討フロー

（１）我が国のセキュリティ情報共有組織の現状と課題の把握

セキュリティ情報の収集、分析、提供等の現状、ニーズや課題について、既存文献調査、国内のセキュリティ情報共有組織へのヒアリング、事業者へのアンケートから把握する。

（２）サイバー攻撃に関する実態把握

近年の起こったサイバー攻撃（特に本年５月に世界で流行したランサムウェア）に関する事例をヒアリングなどから収集し、国内外のセキュリティ情報組織が実施した対応について整理を行う。

（３）諸外国のセキュリティ情報共有組の実態調査

諸外国のセキュリティ情報組織の実態やロンドン五輪、リオデジャネイロ五輪での取組みについて既存文献等から把握する。

（４）鉄道、航空 ISAC の実現に向けた検討

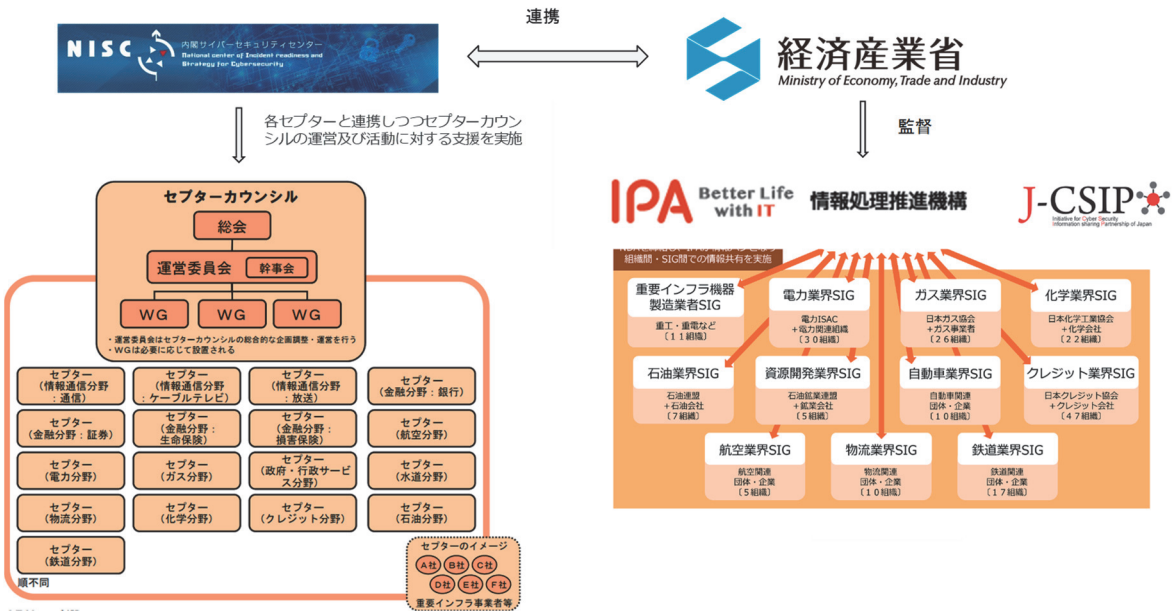
鉄道、航空 ISAC の課題の整理と解決策の検討を行い、ISAC の基本方針、業務内容、組織構成、構築手順など組織構築に向けた検討を行う。

第２章　我が国のセキュリティ情報共有組織の現状と課題の把握

鉄道及び航空分野における ISAC 構築に向けた検討を行うため、我が国のセキュリティ情報共有組織におけるセキュリティ情報の収集、分析、提供等の現状、ニーズや課題について把握する。

２．１　国内のセキュリティ情報共有組織の整理

日本国内の代表的なセキュリティ情報共有組織としては、経済産業省と情報処理推進機構（IPA）が主導する、①サイバー情報共有イニシアティブ（J-CSIP: Initiative for Cyber Security Information sharing Partnership of Japan）[1]と内閣サイバーセキュリティセンター(IPA)が事務局支援を行う、②セプター(CEPTOAR:Capability for Engineering of Protection, Technical Operation, Analysis and Response の略称）[2]がある。J-CSIP やセプターは政府機関との情報共有が主となっている。



注１）「サイバー情報共有イニシアティブ（J-CSIP）運用状況[2017 年 7 月～9 月]」
（https://www.ipa.go.jp/files/000062172.pdf）より作成
「セプターカウンシル総会第 9 回会合の開催について」
（https://www.nisc.go.jp/active/infra/pdf/cc_dai9.pdf）より作成

図　J-CSIP 及びセプターの組織概要

[1] 参考：https://www.ipa.go.jp/security/J-CSIP/
[2] 参考：https://www.nisc.go.jp/active/infra/shisaku2.html

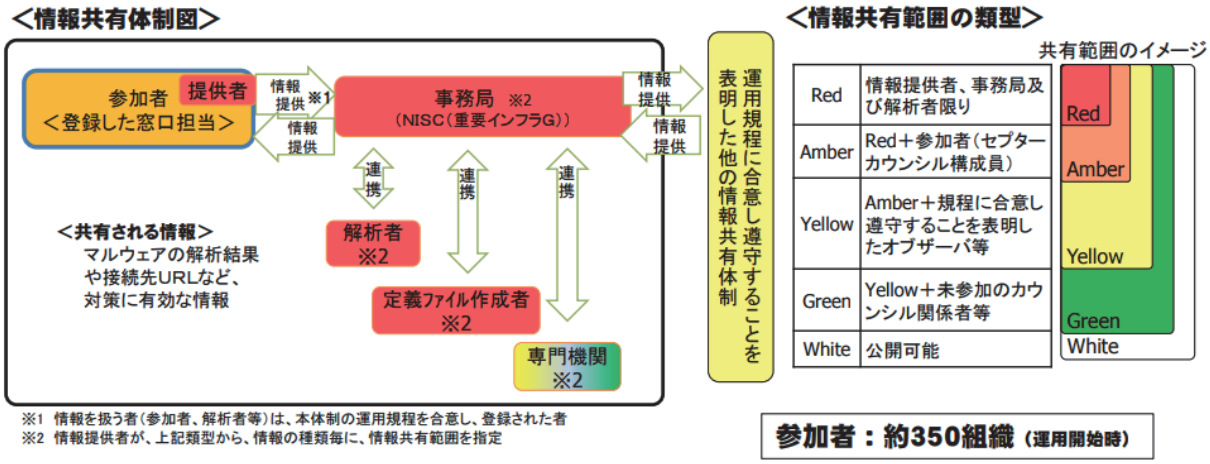
２．１．１　サイバー情報共有イニシアティブ（J-CSIP）

J-CSIP は、IPA に集約された、参加組織及びそのグループ企業において発生したサイバー攻撃の情報を分析・匿名化し参加組織間で共有する取組みを実施している。重要インフラ事業者がセクターごとに SIG（Special Interest Group）を構成[3]しており、2018 年 2 月現在、11 業界の SIG、227 の組織が参加している。

[3] 各 SIG において必要に応じ会合を持ち、事例の紹介や、複数の攻撃情報の横断的な分析、情報共有ルールの見直し、そして各参加組織での標的型攻撃対策や情報セキュリティの取組み状況に関する情報交換を行っている。（出典：サイバー情報共有イニシアティブ（J-CSIP） 2014 年度 活動レポート，https://www.ipa.go.jp/about/press/20150527.html）

２．１．２　セプター（CEPTOAR）

セプターは、重要インフラ事業者等の情報共有・分析機能を担う組織であり、重要インフラサービス障害の未然防止、発生時の被害拡大防止、迅速な復旧や再発防止のため、政府等から提供される情報について、重要インフラ事業者等に提供し、関係者間で情報を共有している。NISC 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」（第４次行動計画）等に基づき、各セプターと連携しつつセプターカウンシルの運営及び活動に対する支援を行っている。2017 年 9 月現在、各重要インフラ分野の業界団体等が事務局となり、全 13 分野で、計 18 のセプターが活動している。また、各重要インフラ分野で整備されたセプターの代表で構成される協議会として、2009 年 2 月 26 日にセプターカウンシルが設立されている。セプターカウンシルでは、重要インフラ事業者等に密接に関連する情報を提供するための体制の調整等に取り組んでいる。具体的なプロジェクトとして、Web サイト応答時間計測システムや C4TAP（セプターカウンシルにおける標的型攻撃に関する情報共有体制）を運用し、情報共有を推進している。Web サイト応答時間計測システムでは、重要インフラサービス等の被害軽減、サービスの維持、早期復旧を容易にすることを目的として、重要インフラ事業者が登録する Web サイトの応答時間を定期的に計測することで､動作異常や外部からの大量のトラフィック等を検知し、異常の早期発見・事実の確認、原因推測を行っている。C4TAP では、重要インフラサービスへの標的型攻撃の未然防止、若しくは被害軽減、サービスの維持、早期復旧を容易にすることを目的として、重要インフラ事業者において、標的型攻撃が疑われるメールについての一定情報を共有している。



注２）「標的型攻撃に関する情報共有体制」（https://www.nisc.go.jp/active/infra/pdf/cc_c4tap.pdf）より抜粋

図　C4TAP の仕組み

J-CSIP やセプターは政府機関との情報共有が主となっている。一方で、同じ業界内でのサイバーセキュリティ情報に関する情報を共有する組織として ISAC（Information Sharing and Analysis Center）がある。2018 年 2 月現在、日本国内には、①一般社団法人金融 ISAC、②一般社団法人 ICT-ISAC、③電力 ISAC の 3 つの ISAC が存在する。２．１．３～２．１．５において、3 つの ISAC についての設立経緯や活動内容について整理する。

２．１．３　一般社団法人金融 ISAC

一般社団法人金融 ISAC[4]は、銀行・証券・保険等の金融機関が中心となり、2014 年 8 月に設立された。情報・物理セキュリティに関する情報収集・分析・共有の他、安全対策に関するコンセンサスの形成、セキュリティ啓発活動、年 1 度のカンファレンスなどを実施している。

会員には、正会員、準会員、アフィリエイト会員（Gold、Silver、Bronze）があり、正会員と準会員の年会費についてはそれぞれ 80 万円、18 万円（全て非課税）となっている。正会員は、銀行、証券、生保、損保、クレジットカード業を中心とした金融機関が対象となっている。準会員は、正会員としての加盟を検討している機関が対象となっている。アフィリエイト会員は ISAC の活動をサポートするセキュリティベンダーが対象となっている。2018 年 1 月現在、正会員は 330 社、準会員は 13 社、アフィリエイト会員 23 社、賛助会員は 1 団体となっている。会員種別ごとに享受できるサービスを下表に示す。

表　一般社団法人金融 ISAC の提供サービスと会員クラス別の受けられるサービスの違い

項目/内容	正会員	準会員	アフィリエイト会員
ポータルサイト インシデントや脆弱性情報等の共有や、各種ガイドライン等の蓄積	対象	対象外	非公開
ワーキンググループ 特定の重要課題の分析、対策検討、共同演習・勉強会への参加	参加可能	WG 座長が指名した場合のみ参加可能	WG 座長が指名した場合のみ参加可能
レポート配信 共有された情報のまとめや、連携する FS-ISAC[5]、アフィリエイト各社からの情報やレポートの配信	対象	一部のみ配信	脅威・脆弱性情報等のレポート配信
アニュアルカンファレンス 年 1 回開催	対象	対象（除く総会）	講演・出展
ワークショップ 年 2 回開催。アニュアルカンファレンスよりも濃い内容が議論される。	対象	対象	講演・出展

注３）「活動概要」（http://www.f-isac.jp/institute/activities.html）より一部改変

[4] 参考：http://www.f-isac.jp/index.html
[5] 米国の金融分野の ISAC

ワーキンググループの活動概況は下表の通り。

表　一般社団法人金融 ISAC のワーキンググループ活動概況

WG 名称	活動概要
インシデント対応 WG	「インシデント対応マニュアル」作成 情報共有プロトコルの検討
脆弱性対応 WG	脆弱性情報の配信 脆弱性対応のノウハウ集の作成（「システムの脆弱性とは何か」「脆弱性評価フレームワーク」「脆弱性対応マニュアル」「会員間の情報共有と有事の運用ルール」）
不正送金対策 WG	銀行の不正送金事案の情報交換 不正送金対策のベストプラクティスの検討 「不正王金対策グッドプラクティスガイド」作成
インテリジェンス WG	「インテリジェンスレポート」の作成 情報元・分析ノウハウの共有推進
ベストプラクティス WG	対策のベストプラクティスの取りまとめ（「DDoS 対策」「メールエンドポイントのマルウェア対策」）
グローバル情報連携 WG	米国 FS-ISAC との情報共有範囲の拡大検討 共有可能な各種情報の日本語化
共同演習 WG	共同サイバー演習「FIRE」の企画・運営及び、サイバー演習のノウハウ収集・共有 地域演習の企画・運営及び、分野横断的演習や他団体の演習の共催・支援活動の実施
スキルアップ WG	セキュリティ担当のスキル向上を目指した各種勉強会の企画・実施 人材ロードマップ E-ラーニング環境の企画・構築 合同合宿形式の勉強会「Cyber Quest」の実施
Fintech Security WG	Fintech 領域でのセキュリティ対策の企画、検討等を実施

注４）「平成 29 年度交通 ISAC 創設に向けた検討会及び合同部会（第１回）」資料より一部改変

一般社団法人金融 ISAC は運営規則において、ISAC で共有された情報に基づく損失については重過失並びに故意の場合を除いて ISAC 及び会員は責任を負わないとしている。

一般社団法人金融 ISAC 内で情報共有する上での注意点として、情報受信側及び情報発信側に以下が求められている。

表　一般社団法人金融 ISAC 内で情報共有する上での注意点[6]

情報受信側	情報元が付与する TLP（Traffic Light Protocol7）により、利用時範囲を遵守する 原則として自組織のサービス・システムを守る目的以外には利用しない 委託先に連携可能な情報を伝える際は、発信元情報は除去し、攻撃元情報など自組織のサービス・システムを守るために必要な情報のみとする
情報発信側	発信に必要な情報としては、攻撃元情報（IP アドレスなど）、攻撃の手口、攻撃の狙い、有効な策・無効化された策のうち、判明しているもの（顧客情報は発信不可） 情報発信のための整理を行う（情報発信についての組織決定、脅威レベルに応じた情報発信が可能な職員の決定）

表　一般社団法人金融 ISAC 運営規則で定められた TLP

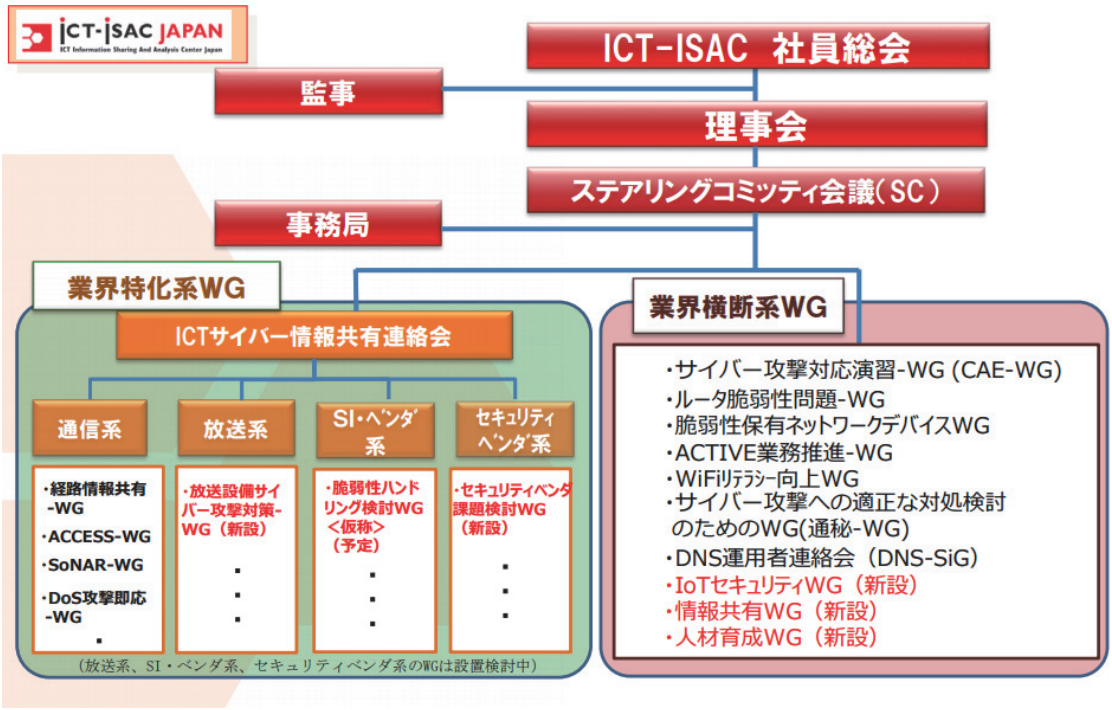
TLP 区分	会員活動上の情報の取扱い	会員個社における情報の取扱い
Red/赤	特定のグループ（会議参加者等）の受信者のみとし、当該グループ外への転送を禁ずる	必要最小限の範囲内で共有することができる
Amber/黄	金融 ISAC 会員限りで共有する	発信者情報を適切に削除等した上で、必要に応じて、会員個社及びグループ子会社内で共有することができる
Green/緑	金融 ISAC 会員及び予め理事会が定める業界団体等の外部組織との共有 を行うことが可能	発信者情報を適切に削除等した上で、必要に応じて、Amber/黄で定められた共有範囲に加え、情報セキュリティ、物理セキュリティ対応に関連する外部委託先を含めた範囲で共有することができる
White/白	公知の情報として扱う ※著作権法その他の法令を遵守する	常識的な範囲で共有することができる

注５）一般社団法人金融 ISAC 運営規則より一部改変

[6] 参考：「平成 29 年度交通 ISAC 創設に向けた検討会及び合同部会（第 1 回）」資料
[7] 情報共有レベル区分のこと

２．１．４　一般社団法人 ICT-ISAC

一般社団法人 ICT-ISAC[8]は前身である Telecom-ISAC の会員に放送・ベンダー企業を加える形で 2016 年 3 月設立された。ICT 分野のセキュリティに関する情報収集・分析・共有の他、セキュリティ対策に関するガイドラインの検討や人材育成、啓発活動などを行う。事務局は通信分野のセプター事務局を兼ねている。一般社団法人 ICT-ISAC の組織体制は下図のようになっている。

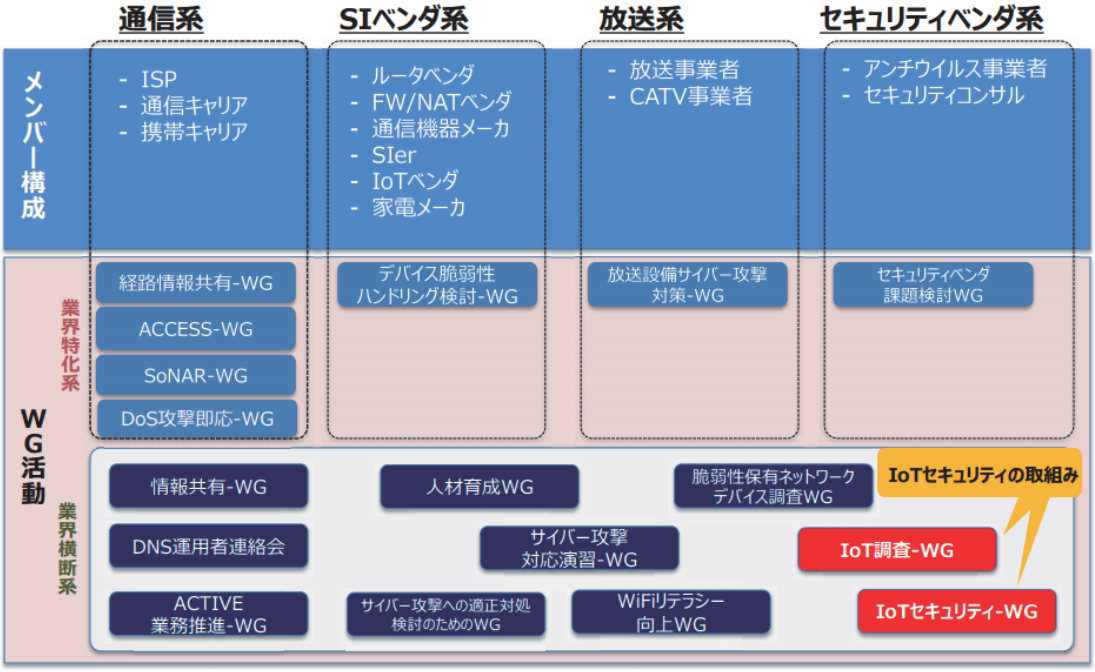


注６）「ICT-ISAC の概要」（http://www.soumu.go.jp/main_content/000452772.pdf）より抜粋

図　一般社団法人 ICT-ISAC の組織体制

[8] 参考：https://www.ict-isac.jp/

2017 年 11 月現在のワーキンググループ活動状況は下図の通り。



注７）「ICT-ISAC における IoT セキュリティの取組みについて」（https://igcj.jp/meetings/2017/1130/igcj22-1-4-4-noritake.pdf）より抜粋

図　一般社団法人 ICT-ISAC のワーキンググループ活動

２．１．５　電力 ISAC

電力 ISAC[9]は、電力事業者が中心となり、2017 年 3 月に設立された。サイバーセキュリティに関する情報収集・分析・共有の他、情報共有に向けたルール策定などを行う。電力 ISAC の規約では、会員資格として正会員は以下のように定められている。

・一般送配電事業者
・送電事業者、特定送配電事業者及び発電事業者
・上記 2 点までに掲げる者の発行済み株式の全部または持分の全部を有する者
・上記 3 点に掲げる者が営む事業と関連する事業を営む者であって、電力 ISAC の規約前文及び電力 ISAC の目的に照らし、特にその入会が望ましいと理事会が判断した者

2017 年 3 月現在、正会員は 26 社、特別会員は 1 機関となっている。事務局は電力分野のセプター事務局を兼ねる。

日本国内の既存の ISAC では、総会における会員の議決権割り振り方法が 3 団体とも異なる。金融 ISAC では会員 1 社につき議決権は 1 票で、ICT-ISAC では会員社の会費 1 口につき議決権 1 票、電力 ISAC では系統運用者（電圧・周波数の維持やオープンアクセスが可能な系統設備の運用等の一般送配電事業を営む事業者）と系統連系者（発電事業等の電力系統に連系する事業者）の議決権数が等しくなるよう各社に配分している。

また、2017 年 7 月現在のワーキンググループ活動状況は下図の通り。

カテゴリ	WGテーマ	
専門分野（Ⅰ）	Ⅰ－1. 課題検討WG	電気事業の各分野（発電、送配電、ITなど）の取組みで、サイバーセキュリティに係る課題事項に関する意見交換
情報交換（Ⅱ）	Ⅱ－1. ベストプラクティス共有WG	JESCガイドラインへの対応や取組みの外部有識者を交えた客観的レビューおよびベストプラクティスに関する会員間の情報交換
	Ⅱ－2. セキュリティ教育WG	社内のセキュリティ教育やそのコンテンツ等に関する情報交換
	Ⅱ－3. セキュリティ製品WG	ベンダーが提供するセキュリティ製品のベンチマーク、評価に関する情報共有
情報解説（Ⅲ）	Ⅲ－1. セキュリティトレンドWG	定期レポートの内容に関する解説およびサイバー攻撃のトレンドや各社の対応状況に関する情報交換

注 8）総合資源エネルギー調査会 電力・ガス事業分科会　電力・ガス基本政策小委員会（第 4 回）配布資料「電力 ISAC の設立について」（http://www.meti.go.jp/committee/sougouenergy/denryoku_gas/denryoku_gas_kihon/pdf/004_07_02.pdf）より抜粋

図　電力 ISAC のワーキンググループ活動

[9] 参考：https://www.je-isac.jp/index.html

２．２　国内のセキュリティ情報共有組織へのヒアリング

２．２．１　調査方針

国内のセキュリティ情報共有組織におけるセキュリティ情報の収集、分析、提供の実態、ニーズや課題について把握するために国内のセキュリティ情報共有組織を対象にヒアリングを行った。ヒアリングは 2017 年 11 月～12 月に実施した。

表　国内のセキュリティ情報共有組織へのヒアリング調査概要

調査対象	■　国内のセキュリティ情報共有組織 7 団体
調査項目	■　セキュリティ情報共有の仕組み ■　セキュリティ情報共有組織の運用実態 ■　運用時の工夫や課題等
調査期間	2017 年 11 月～12 月

２．２．２　セキュリティ情報共有組織（ISAC 除く）のヒアリング結果

政府機関との情報共有が主となっているセキュリティ情報共有組織（ISAC 除く）へのヒアリング結果を以下に示す。

（１）セキュリティ情報共有の仕組み

情報の種類	**・脆弱性[10]情報等** 鉄道・航空分野のシステムに特化した形で流通する情報はほぼない
共有手順	**・政府機関から事務局に情報提供され、事務局から事業者に当該情報を発信** **・事務局から事業者に発信され、事業者からグループ企業の事業者に当該情報を発信**
受信者の制限	**・ベンダーへの展開** 可能だが、秘密保持契約相当を必要としている事例がある。 また、TLP で制限をかける場合がある、とした事例もある。 **・送信者側からの制限** 外部組織から事務局に情報提供された段階で制限が定められている
共有手法	**・メール** 内容に応じてポータルを使用して共有する事例もある。
情報の取捨選択や分類	**・TLP を付与している** **・重要度等のランク分けはない** 上記の双方の事例がある。ただし、後者についても、外部組織から事務局に情報提供された段階で重要度が定められている場合は、その情報を踏襲している。

（２）セキュリティ情報共有組織の運用実態

情報の収集方法	**・参加組織からの情報提供** **・政府機関からの情報提供** 政府機関からの情報提供の場合、主体的に事務局がセキュリティに関する情報を取りまとめることはない一方で、確実に情報を事業者に通知する必要がある。
加盟企業の窓口	**・主に IT 担当部門** **・IT 担当部門に加え、安全部門、電気部門等**
運営人員 資金	**・全体の事務局はなく、WG に一般的な事務局機能を持たせている** **・WG の事務局は輪番・非常勤制** **・事務局は 1～4 名（兼任）/資金は事務局を担っている団体の予算より運営/会費は徴収していないという事例が複数あった**

[10] ソフトウェア等におけるセキュリティ上の弱点

刊行物の発行	・HP 上でレポートを発行 ・セキュリティに関する定期的な刊行物は特にない
他情報共有団体とのすみ分け	・すみ分けはない 様々なルートで同じ情報が流れることもあり、少々煩雑になっている。 ・ISAC は分野の独自の動き ・国土交通省からの情報は各事業者に直接連絡が届くことが多い

（３）運用時の工夫

活動の活性化のための取組	・情報提供者に付加価値のあるレポート等の情報を返せるようにしている ・共有する情報の量及び質を高めるための議論を行う WG が設置されている ・特段の活動を行わなくとも他の会合等で信頼関係はできている ・特段の活動はないが、会う機会があれば話すように取り組んでいる
加盟企業の要望を吸い上げるための取組	・他の会議等で、要望があれば受け付ける ・要望等の吸い上げは各分野の集まりで実施。吸い上げた要望は分野団体を通じ、全体の協議会へ反映
運用時の課題	・参加組織が情報提供するモチベーションを保つ方法 ・民間主導の流れの維持 ・事務局の運営や活動内容 / 緊急の連絡対策がない / 加盟事業者に転送すべき情報かの判断 ・IT 分野のサイバーセキュリティの専門家が事務局にいない / 24 時間体制でない

（４）セキュリティ情報共有組織（ISAC 除く）のヒアリング結果まとめ

セキュリティ情報共有組織で共有される情報としては、脆弱性情報やインジケータ等となっている。また、事務局では加盟企業から情報収集を実施していない組織もあった。情報の種類によってはベンダーへの情報展開等、受信者を制限しているものもある。全ての情報共有組織において情報提供の手段としてメールを利用している。また、メールの他に、ポータルサイト（掲示板等）を利用しているセキュリティ情報共有組織もあった。

運用の実態としては、普段の業務で得た情報を会員に流している場合や、外部組織から提供された情報を事務局が会員に提供される場合がある。また、会員から情報から提供される場合もある。情報共有組織を考える上で、国との接点を持つならば、どのような条件にするか検討した方がよい（国からの情報提供を受ける場合は、基本的には徹底が求められることが多い）という意見もあった。

セキュリティ情報共有組織の会員の窓口の多くは IT 部門となっている。ただし、一部の組織では IT 部門の他、安全部門や電気部門が窓口になっている場合もある。事務局人員は事務局を担っている組織と兼任している場合もあり、その場合の人数は数名となっている。

運用時の工夫として、組織活動の活性化のために、付加価値のあるレポート等の情報を返すことや、活性化のための議論を行う WG が設置されている事例がある。加盟企業の要望を吸い上げるための取組としては、要望等の吸い上げを各分野の集まりで実施し、全体の協議会へ反映している事例が挙げられた。運用時の課題としては、参加組織が情報提供するモチベーションを保つ方法や、事務局が IT 分野のサイバーセキュリティの専門家ではないため情報の判断に迷う場合があるといった事務局運営に関する課題も挙げられた。

２．２．３　ISACのヒアリング結果

同一の業界内でのサイバーセキュリティ情報に関する情報を共有する組織である、ISACへのヒアリング結果を以下に示す[11]。

（１）ISACの情報共有の仕組み

共有する情報の種類	**・インシデントの情報** 発生した日時・内容等人に対する情報と、インジケータ[12]等機械に対する情報 **・インジケータと脅威情報** **・WGによって共有する情報が異なる。ただしISAC全体に関わる情報については全体で共有している** 業界に特化した情報は業界内で情報共有した方がよいという考えに基づく
ISACの参加条件	**・正会員は当該分野の事業者のみ[13]** セキュリティベンダーやシステムベンダーは正会員以外の枠で参加する **・情報を提供できる企業** ベンダーも情報提供できるようであれば参加を許可している
情報の受信者の制限（TLP付与）	**・情報発信者が、優先度・TLP・有効期限・匿名化を選択可能** TLPの範囲は基本的に加盟企業内であり、加盟企業のドメインを持っている人に限る **・会員組織内の運用上の問題については展開禁止** インジケータ等機械に対する情報については情報の取扱いに制約を課していない **・会員からの情報提供は、情報提供者がTLPを設定する。外部からの情報は、ISACに提供される際にTLPに準じるものが付加されている**
情報共有のための手法	**・情報共有ポータルを利用** メーリングリストからポータルに移行。理由として、参加企業の中でISACの担当者が変わることなどによる更新が大変であること、双方向の情報共有が容易である等が挙げられる。利用に際して、担当者名の登録、アカウントへの写真の掲載、共有情報のエクスポート機能、インシデント情報とその関連情報やガイドライン等のドキュメント類を共有するためのファイル共有サーバーも搭載といった工夫が施されている **・メールを使用** ポータルもあるがメールの方が利用される / 今後ポータルを整備予定
ISAC設立の理由	**・同じ攻撃者からの攻撃に対し、民間企業で団結し対策をとるため** **・他社の障害が自社の障害となるため、事業者間の相互連携を図り、安定した事業を行うため** **・国外で当該分野に対するサイバー攻撃が増加しており、国内の事業者のセキュリティを高めるため。また、サミットにおいて当該分野でのサイバーセキュリティに関する国際的な協力の議論があったため**

[11] 複数のISACの事例を列挙しているため、記載事項がすべてのISACに共通しているわけではない。
[12] 検知に有効なサイバー攻撃を特徴付ける指標
[13] 正会員とそれに準じる会員を分けていないISACもある。

加盟企業の主な動機	**・同じ攻撃者からの攻撃は、民間企業で団結し対策をとることが有効なため** **・他社の障害が自社の障害となるため、課題解決に向けて情報を共有することに意味があると考えている企業が多い** 会員リストに名前が載っていることや、ガイドラインの検討の場に参加できること、いち早く情報を手に入れることができることにメリットを感じて加盟している事業者が多い **・中小企業は、大企業の取組みを参考にしたいという思いがある。大企業としても他社の障害が自社の障害となるため業界全体のセキュリティレベルの向上を図りたいと考えている**

（２）ISAC の現在の運用実態

共有する情報の収集方法	**・会員からの情報提供** 情報を出しやすい雰囲気を醸成するために業務外のコミュニケーションが重要。また、情報の提供範囲を制限することも重要。ベンダーに情報を流さないように依頼。海外のコンサルティング会社を使った情報収集も検討 **・会員、省庁、国外組織からの情報提供** 省庁等外部から提供された情報は ISAC 内でフィルタリングは行わずそのまま流しており、各社で取扱いを判断してもらう。米国の ISAC と情報共有を行っている。/ 海外の情報に関してはセキュリティ情報の調整機関から連絡されることがある
加盟企業の担当者の所属	**・主に CSIRT・SOC** **・主にシステムのオペレーションを行う部門や情報システム部門** **・主に IT 関係** WG は内容によって別部署の方も出席されている。
ISAC 運営のための人員・資金	**・事務局は 5～10 名 / 会員からの会費収入** 国からの受託事業で補っている / 会費についてはいくつかクラスを設けている / 夜間は営業時間外だが、当該分野に広範囲に重篤な攻撃が発生しているような状況では、夜間も対応する場合がある。また夜間の緊急連絡対応という意味では、情報共有ポータルの投稿は担当者ベースで実施することがある
定期的な刊行物の発行頻度	**・脆弱性情報の配信（毎日）、メールマガジンの配信（２週間ごと）** メルマガの内容として有識者のリレー投稿が主な内容。アナリストのコラムや、外部カンファレンスのまとめ、脆弱性対策のまとめについても流す **・刊行物は出していない** 代わりに年１回総会を行っている。インシデント情報は都度共有を行っている。 / 刊行物について現在検討中。インシデント情報は都度共有を行っている。事務局メンバーが海外の ISAC の総会に行き、得た情報に関してもメールで流している
他情報共有団体とのすみ分け	**・セプターは国が集めた情報を共有する。ISAC は民間企業間で出し合う情報を共有する**

	・ISAC の機能の中にセプター事務局の機能がある。セプター構成員と ISAC 会員とは異なるため、厳密には事務局が得た情報の中でセプター構成員のみに提供するものもあるが、セプターとのすみ分けはあまり意識していない
情報分析	・WG において、各社での対応や影響などににについて報告 インシデント発生から 1 週間程度で実施している WG もある ・分析は行っていない 分析された情報を素早く集めることや、分析の外注を考えている ・事務局の有識者等による分析を適宜実施するとともに外部リソースを利用 分析された情報はインシデント情報の共有に付与する場合がある。外部リソースからの情報については、共有範囲が限定されているものがあるため、その範囲で付与することがある
教育プログラム	・スキルアップ WG の実施、サイバー攻撃対応演習（机上演習）の実施及び会員向けセミナーの実施 ・ISAC を主体として教育プログラムは行っていない

（３）運用時の工夫

ISAC の活動の活性化のための取組	・アニュアルカンファレンスとワークショップの実施（計年 3 回)、WG の開催及び表彰制度 いくつかの WG ではガイドラインを発行している。表彰制度については、人気投票または推薦で、積極的に情報共有を行った方や WG に大きく貢献した方が選ばれる ・WG の開催、各 WG の活動報告会（総会）（年 1 回） 参加者が交流する場を作ることを意識している。設立当初は懇親会費を補助していた ・信頼関係構築のために、昼間の会議・WG だけでなく懇親会での会員同士の交流
加盟企業の要望を吸い上げるための取組	・WG 等でアンケートを実施 ・WG 等で要望を把握 ・WG 等で今後の方針を検討
運用時の課題	・加盟企業間のセキュリティ対策レベルが異なるため、ボトムアップが課題 ・若年層から ISAC の活動への参加が少ないこと、財政基盤の安定化 ・事務局に情報共有の運用を頼られすぎていること、セプター等他ルートとの情報の重複
情報共有を拡充するための計画	・システムによる自動的な情報交換を検討中

（４）ISACのヒアリング結果まとめ

ISACの情報共有の仕組みとして、共有する情報は主に脅威情報やインジケータとなっている。脅威情報等の情報は基本的にはISAC全体で共有されるが、一部のISACでは主にWGの中で情報が共有されている。その理由は、業界に特化した情報は業界内で情報共有した方がよいというものである。

ISACの参加条件として、ベンダーも参加可能なISACもあり、各分野の事業者だけではなくベンダーも巻き込むことが重要と考えられる。情報共有のための手法としてメールを利用するISACが多いが、一部ISACでは情報共有ポータルを利用している。ポータルを利用している理由としては、インシデント情報とその関連情報やガイドライン等のドキュメント類の情報を蓄積することが可能なこと、共有された情報に対する他会員からの質問（双方向）が容易なこと、参加企業の中でISACの担当者が変わることなどによるメーリングリストの更新が大変であることが挙げられた。また、現在メールを利用しているISACでもポータルの整備を検討中の組織もあり、情報共有の促進、情報の蓄積及び運営の負担軽減にはポータルの活用が有効であると考えられる。

また、複数のISACでは情報共有にあたり、TLP分類を行っている。その理由としては、情報共有を促進するためには、把握できない範囲まで情報が流出してしまうことへの情報提供者の不安を取り除くことが重要ということが挙げられる。

各ISACの加盟組織がISACに加盟する理由としては、「同じ攻撃者から攻撃されることが多いため、民間企業で団結し対策をとることが有効であること」、「他社の障害が自社の障害となりうること」、「ISACの会員リストに名前が載っていること」「ガイドラインの検討の場に入り、ガイドラインに自社の実情を反映できること」、「いち早く情報を手に入れることができること」、「他の企業の取組みを参考にすること」、「業界全体の対策レベルが上がること」が挙げられた。

ISACの現在の運用実態として、共有する情報の提供元は、主に会員及び政府機関（NISCや所管省庁、JPCERT/CC等）となっている。海外からの情報については、米国のISACと情報共有を行うことで入手しているISACもある。また、その他のISACでは、国内のセキュリティ情報調整機関経由で海外の情報を入手する場合や、事務局が海外の会議に出席し情報を入手・共有する場合がある。また海外のコンサルティング企業を利用した情報収集を検討しているISACもあった。

加盟企業の窓口担当者の所属はIT部門（CSIRT/SOC含む）が多いが、あるISACではWGの内容に応じて担当部署の方が出席される場合もあり、柔軟な参加が可能となっている。

運営のための事務局の人員は6名～10名で、運営資金として、どのISACも会員クラスに応じた会費を徴収しており、２．１章の調査では、その額は年間数十万～数百万となっている。また、夜間は事務局の営業時間外となっている場合があるが、当該分野に広範囲に重篤な攻撃が発生しているような状況では、夜間も対応されることがある。さらに、夜間の緊急連絡対応として情報共有ポータルの投稿を担当者ベースで実施する体制がとられている。

定期的な刊行物を発行しているISACの一つでは、2週間に1度のメールマガジンを発行している。その内容は、有識者のリレー投稿やアナリストのコラム、外部カンファレンスのまとめ、脆弱性対策のまとめ等となっている。

情報分析を行っているISACもある。WGの場や、事務局の有識者等による分析が実施され

ている。情報の分析が十分にできていない ISAC では分析された情報を素早く集めることや分析の外注を考えている。教育プログラムとしては WG として、演習やスキルアップ講座や勉強会を行っている場合が多い。

いずれの ISAC においても、会員からの情報提供を促進するために大切なことは、情報を出しやすい雰囲気があること、と考えている。情報を出しやすい雰囲気に繋がる信頼関係の醸成には、WG、年次総会及び懇親会といった、会員同士が顔を合わせる機会の開催が有効である。一部の ISAC では懇親会費を補助している場合もある。また、情報共有ポータルを利用している ISAC では、ポータルの登録を会社名ではなく担当者名で行い、本人が同意することで顔写真の掲載も可能となり、顔の見える化による安心感を提供している。また、ある ISAC では、事務局を業界団体が担うことで、これまでの築かれた信頼関係により、スムーズな情報共有を行っている。

その他の運用時の工夫として、ある ISAC では表彰制度を有している。会員の投票により、情報共有や WG に貢献した会員が選ばれる。また、会員の要望を吸い上げるために、各 ISAC ではアンケートの実施や WG 等が開催されている。

ISAC の課題としては、加盟企業全体のセキュリティ対策のボトムアップや、ISAC 担当者が固定化してしまうこと、財政基盤の安定化が必要なこと、情報共有の運用が事務局に依存しており負荷が大きいこと、他のルートからの情報との重複感が挙げられた。

２．３　国内の鉄道・航空関連事業者へのアンケート

２．３．１　調査方針

鉄道分野・航空分野の事業者における情報共有の実態等を把握するために、国内の鉄道・航空関連事業者を対象に、2018 年 2 月にアンケートを実施した。

アンケート調査票は、「運輸部門を対象とした情報共有の実態等に関するアンケート調査票」と「IT 部門を対象とした情報共有の実態等に関するアンケート調査票」の 2 種類を作成した。

表　国内の鉄道・航空関連事業者へのアンケート調査概要

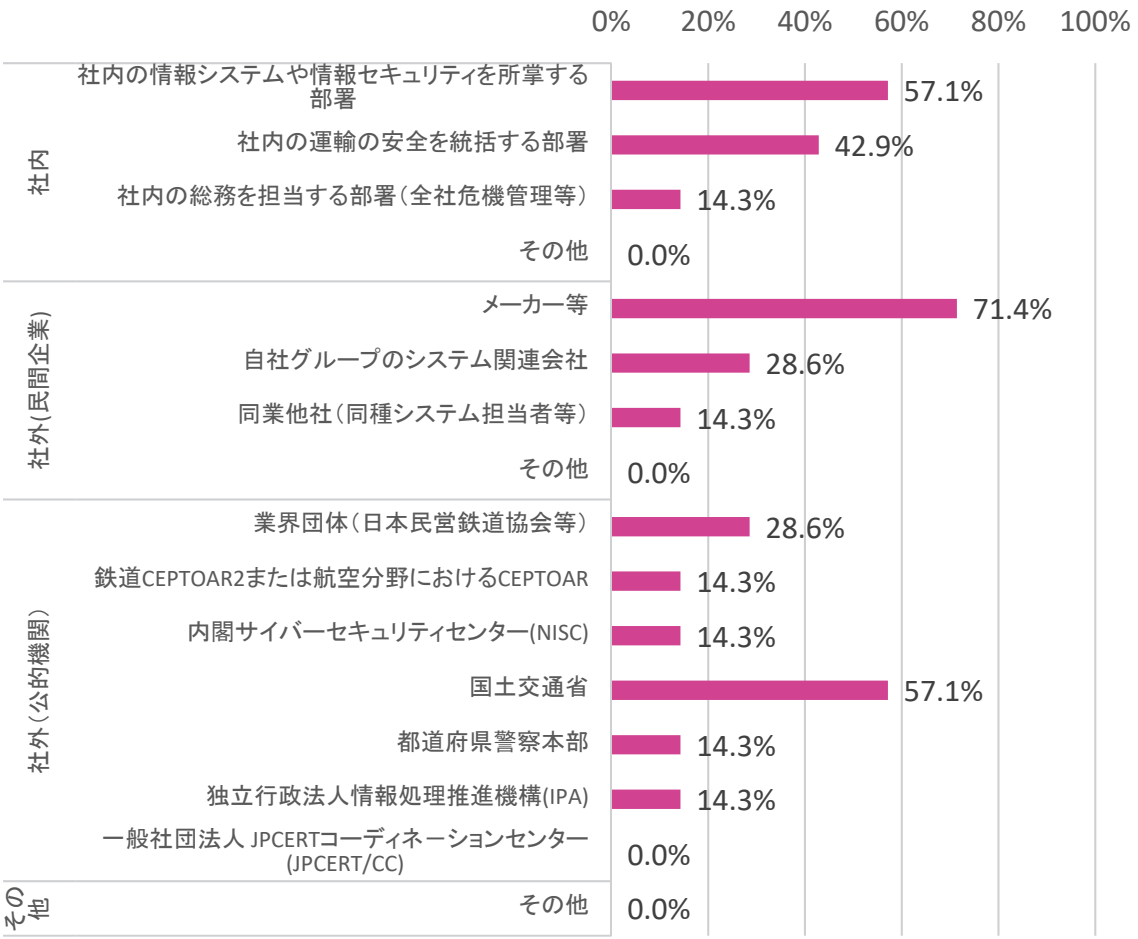
調査対象	■　運輸部門を対象とした情報共有の実態等に関するアンケート調査票 ➢　鉄道事業者の運輸部門：7 社 ➢　航空事業者（空港事業者含む）の運輸部門：2 社 ■　IT 部門を対象とした情報共有の実態等に関するアンケート調査票 ➢　鉄道事業者の情報システム・IT 部門：5 社 ➢　航空事業者（空港事業者含む）の情報システム・IT 部門：6 社
調査項目	■　運輸部門を対象とした情報共有の実態等に関するアンケート調査票 ・　所管するシステム全般の不具合情報の入手状況 ・　所管するシステム全般の不具合情報の提供状況 ■　IT 部門を対象とした情報共有の実態等に関するアンケート調査票 ・　セキュリティ情報の入手・提供の状況 ・　自社の運輸システムがサイバー攻撃を受けた際の情報共有の現状 ・　ISAC について
調査手法	メールで配布
調査期間	2018 年 2 月

２．３．２　鉄道分野における運輸部門を対象とした情報共有の実態等に関する調査結果

（１）所管するシステム全般の不具合情報の入手状況

１）システム全般の不具合情報（サイバー攻撃の恐れを含む）の入手元

鉄道事業者の運輸部門におけるシステム全般の不具合情報の入手元としては、メーカーが最も多く、次いで、社内の情報システムや情報セキュリティを所掌する部署、国土交通省となっている。運輸部門が社内の情報システムを所掌する部署や安全を統括する部門から情報を入手していることがわかる。また、社外からの入手としては、メーカー・国土交通省の他、業界団体からも不具合情報を入手している場合が多い。



n=7

図　システム全般の不具合情報の入手元

２）社外の公的機関から情報を入手した場合の展開先

運輸部門が社外の公的機関から情報を入手した場合の再展開先としては、自部署内若しくは他部署に展開する場合や、システム関連会社、システムの保守を請け負う事業者に転送する場合が多い。

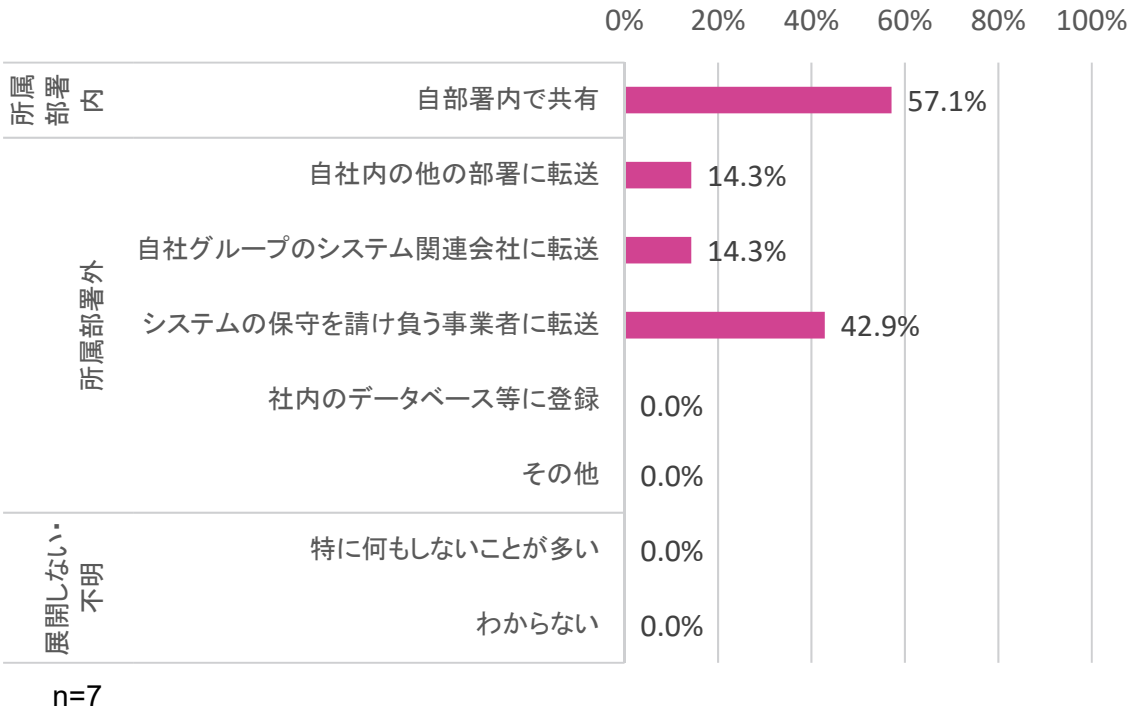


図　社外の公的機関から情報を入手した場合の展開先

（２）所管するシステム全般の不具合情報の提供状況

１）所管するシステムに不具合（サイバー攻撃の恐れを含む）が発生した場合の情報提供の有無

鉄道事業者の運輸部門が所掌するシステムに不具合が発生した場合、運輸部門から他組織に情報は提供されている。

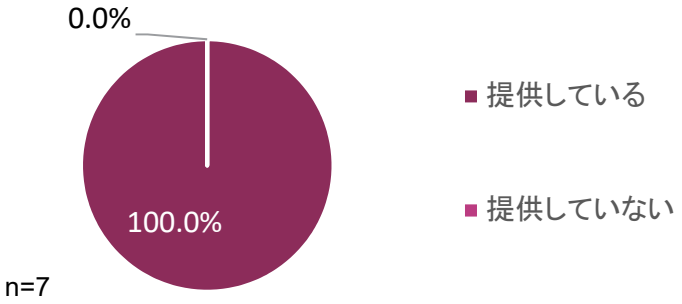


図　所管するシステムに不具合が発生した場合の情報提供の有無

２）所管するシステムに不具合（サイバー攻撃の恐れを含む）が発生した場合の情報提供先

鉄道事業者の運輸部門が所掌するシステムに不具合が発生した場合の、運輸部門からの情報提供先は、社内では、情報システムを所掌する部署や社内の運輸の安全を統括する部署となっている。また、社外ではメーカーが最も多く、次いで国土交通省、システム関連会社となっている。情報入手元として多かった業界団体（日本民営鉄道協会等）にはそれほど情報は提供されておらず、また、同業他社の同種システム担当者も少ない。

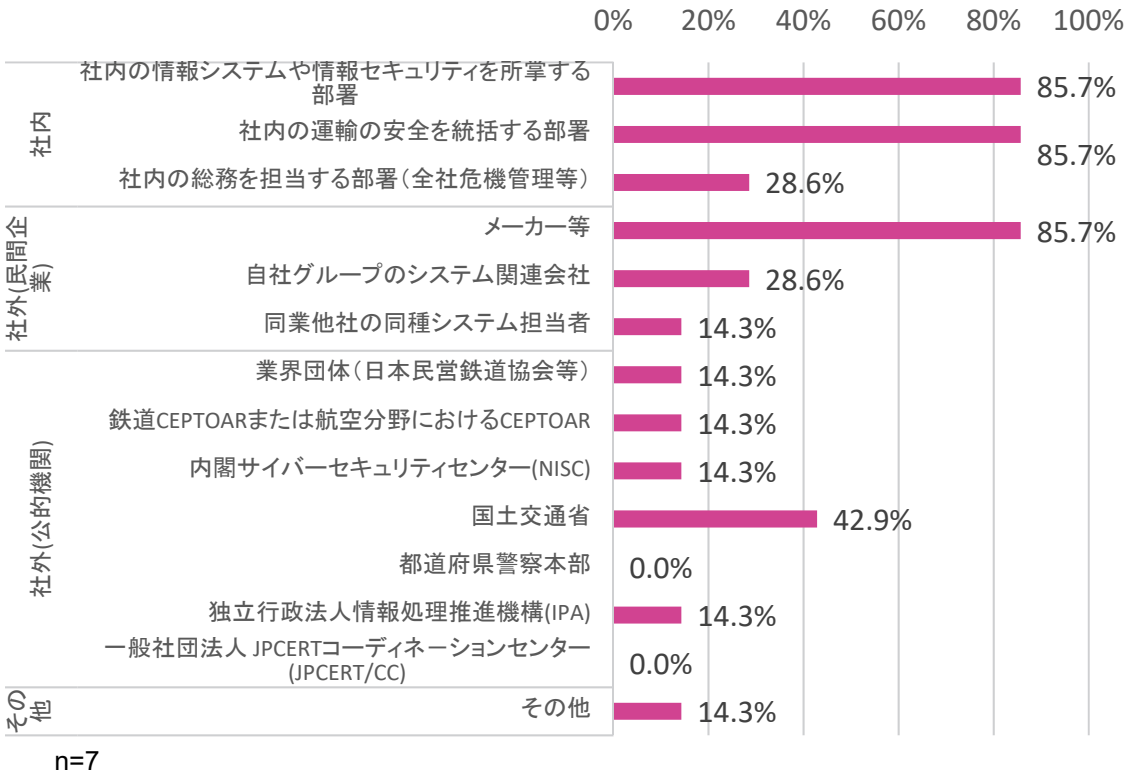


図　所管するシステムに不具合が発生した場合の情報提供先

３）所管するシステムに不具合（サイバー攻撃の恐れを含む）が発生した場合の情報提供のタイミング

鉄道事業者の運輸部門が所掌するシステムに不具合が発生した場合の情報提供のタイミングとしては、不具合が発生した段階ですぐ提供する場合もあれば、仮対応を終えた段階で提供する場合もある。また、提供のタイミングが特に定められていない場合もある。

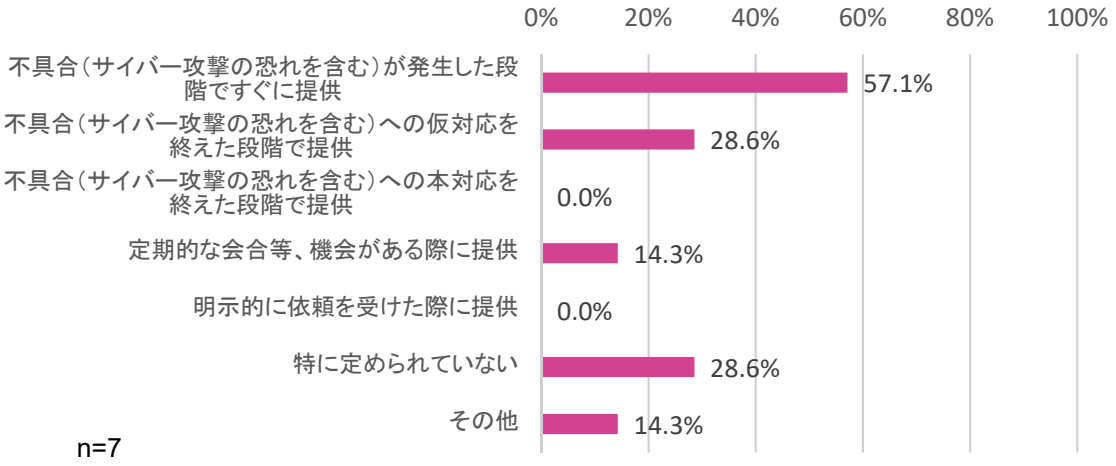


図　所管するシステムに不具合が発生した場合の情報提供のタイミング

２．３．３　鉄道分野における IT 部門を対象とした情報共有の実態等に関するニーズの調査結果

（１）一般的なシステムのセキュリティ情報の入手の状況

１）一般的なシステムのセキュリティ情報の入手頻度

鉄道事業者の IT 部門における一般的なシステムのセキュリティ情報の入手頻度としてはどの企業でも 1 週間に 1 回となっており、頻繁に不具合情報を入手していることがわかる。

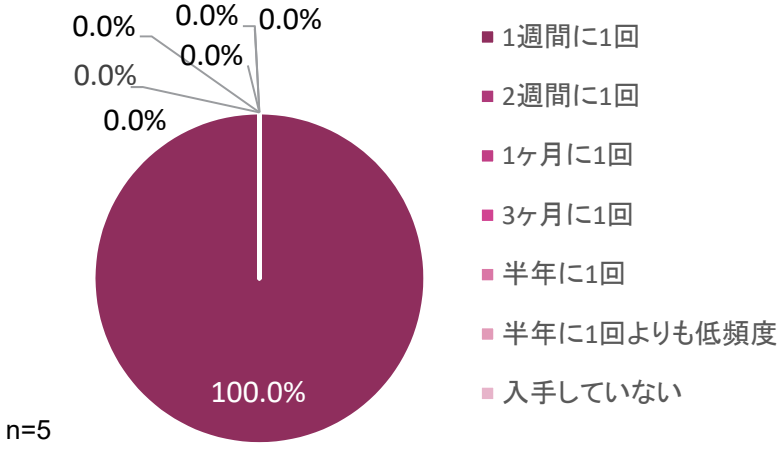


図　一般的なシステムのセキュリティ情報の入手頻度

２）一般的なシステムのセキュリティ情報の種類

鉄道事業者の IT 部門において入手される一般的なシステムのセキュリティ情報の種類としては、インジケータ、サイバー攻撃傾向・手順・攻撃対象、脆弱性情報、侵入検知シグネチャ、具体的対策が挙げられる。ただし、具体的対策は 20%と、他のセキュリティ情報よりも少なくなっている。

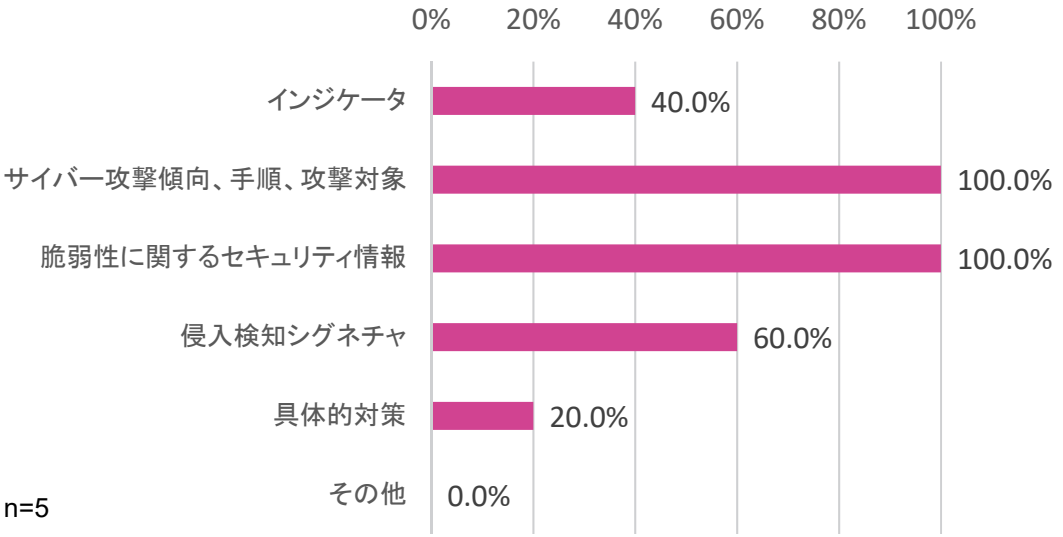


図　一般的なシステムのセキュリティ情報の種類

３）一般的なシステムのセキュリティ情報の入手元

鉄道事業者の IT 部門における、一般的なシステムのセキュリティ情報の入手元としては、日本国内の社外の組織が 100%となっている。その他の意見でも「警視庁及びNISC より入手」となっている。鉄道事業者の IT 部門では、一般的なシステムのセキュリティ情報について社内の他部署や国外の組織から入手されることはない。

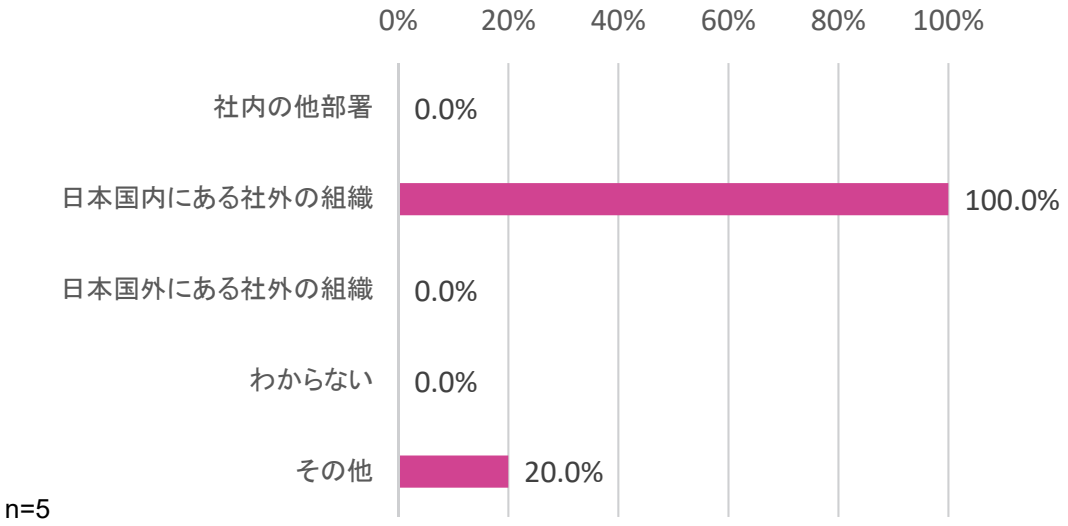


図　一般的なシステムのセキュリティ情報の入手元

４）一般的なシステムのセキュリティ情報の集約部署

鉄道事業者において、一般的なシステムのセキュリティ情報の集約部署はどの企業においても情報システム・IT 部門で行われる。

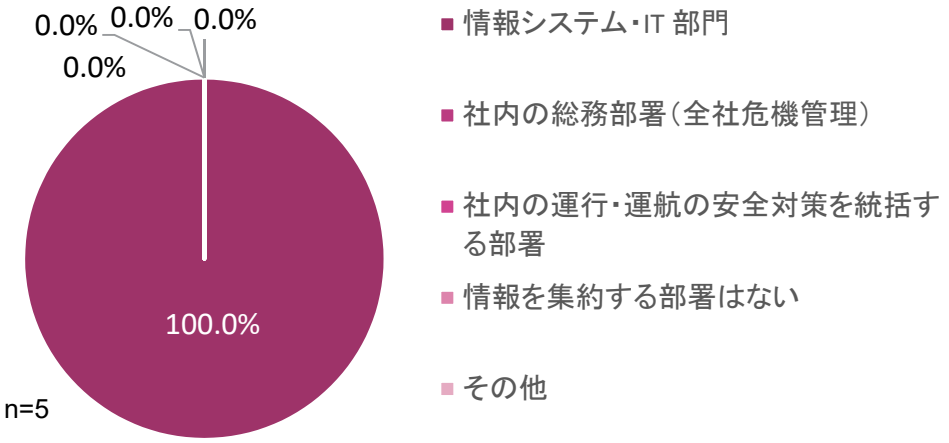
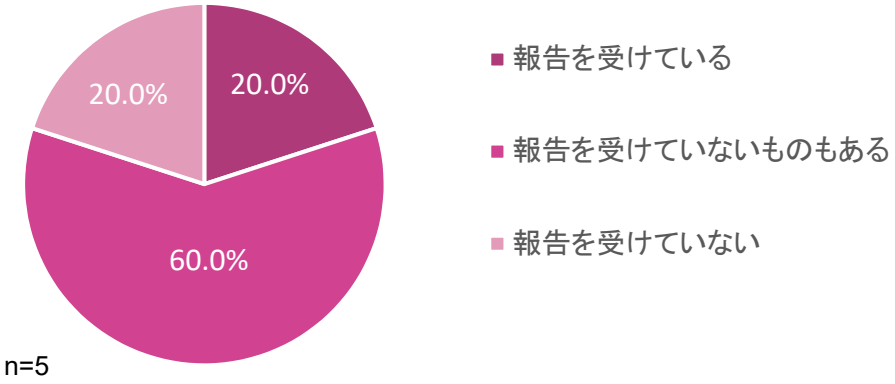


図　一般的なセキュリティ情報の集約部署

５）情報展開先からの対策実施状況の報告有無（一般的なシステムのセキュリティ情報の集約を情報システム・IT 部門で行う場合）

一般的なシステムのセキュリティ情報を情報システム・IT 部門から関係部署に展開した場合、対策実施状況の報告を受けていない場合もあり、展開された情報を元にどのような対策が講じられているか把握されていない。



n=5

図　対策実施状況の報告有無

（２）運輸に関するシステムのセキュリティ情報の入手の状況

１）運輸に関するシステムのセキュリティ情報の入手頻度

鉄道事業者の IT 部門における、運輸に関するシステムのセキュリティ情報の入手頻度としては１週間に１回～入手していない場合まで多様となっている。

また、その他の意見として「情報の種類によって１週間に１回や、半年に１回の頻度で入手」も挙げられ、情報の種類やシステムに応じて柔軟に対応する様子が見受けられる。

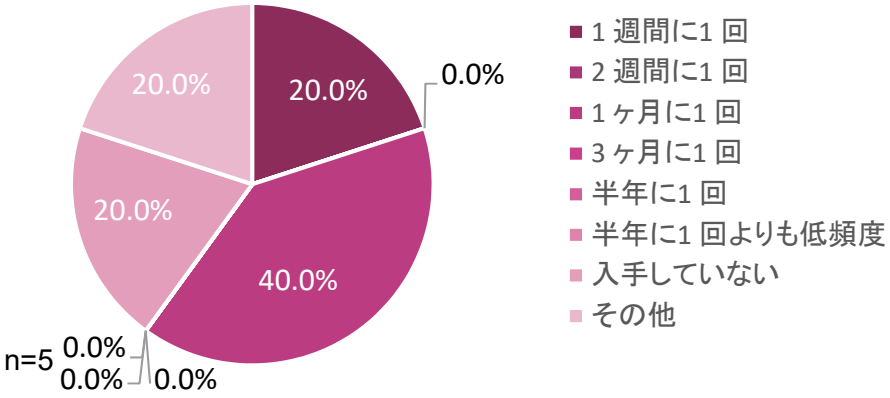


図　運輸に関するシステムのセキュリティ情報の入手頻度

２）運輸に関するシステムのセキュリティ情報の種類

鉄道事業者の IT 部門において入手される運輸に関するシステムのセキュリティ情報の種類としては、インジケータ、サイバー攻撃傾向・手順・攻撃対象、脆弱性情報、侵入検知シグネチャが挙げられた。一般的なシステムで挙げられた「具体的対策」については、運輸に関するシステムの場合、入手されていない。また、その他の意見として、「運輸に関するシステムと一般的なシステムのセキュリティ情報がはっきりと分かれていない」「運輸チャネルからの情報であっても、運輸に関するシステムに特有の情報はほとんどない。」といった意見が挙げられ、運輸に関するシステム特有の情報がそもそもないことがわかる。

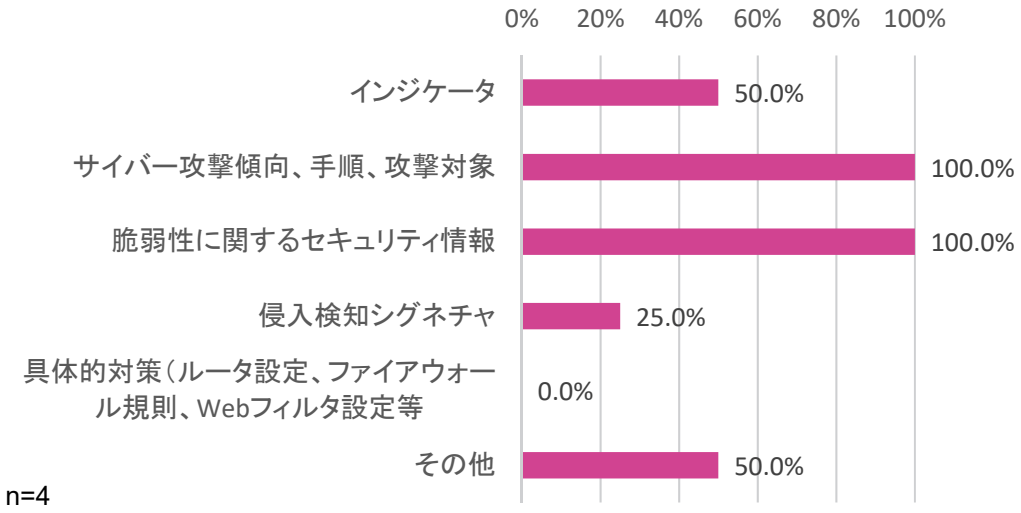


図　運輸に関するシステムのセキュリティ情報の種類

3）運輸に関するシステムのセキュリティ情報の入手元

鉄道事業者の IT 部門における、運輸に関するシステムのセキュリティ情報の入手元としては、日本国内の社外の組織が 100%となっている。鉄道事業者の IT 部門では、運輸に関するシステムのセキュリティ情報について社内の他部署や国外の組織から入手されることはない。

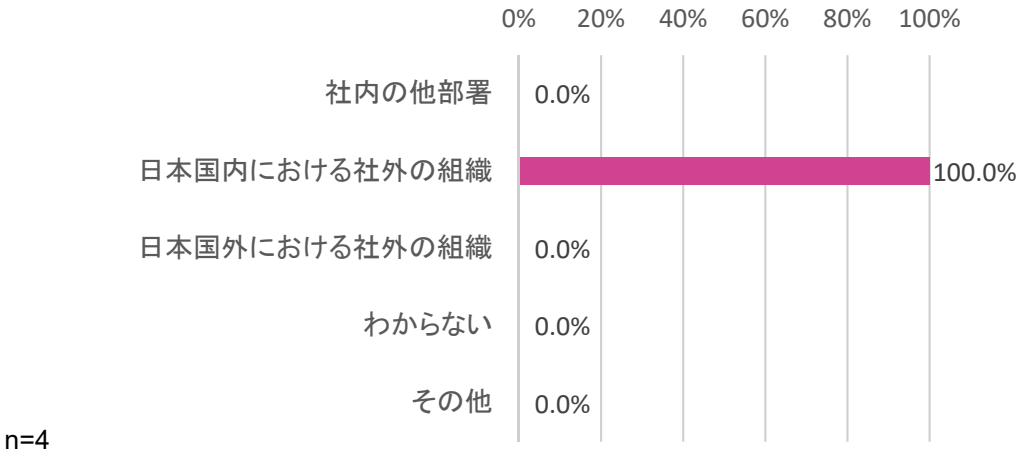


図　運輸に関するシステムのセキュリティ情報の入手元

4）運輸に関するシステムのセキュリティ情報の集約部署

鉄道事業者において、運輸に関するシステムのセキュリティ情報の集約部署は情報システム・IT 部門、安全を統括する部門に分かれる。また、その他の意見として「集約ではなくシステム主管部との相互連携とよって取り扱われる」との意見もあった。

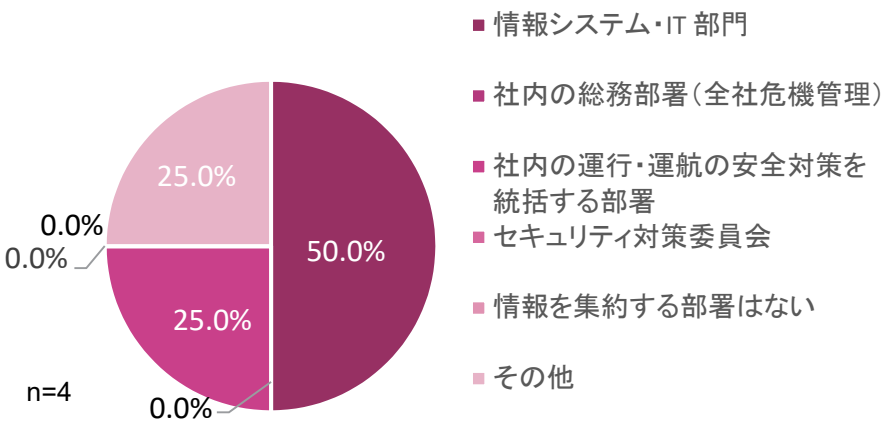


図　運輸に関するシステムのセキュリティ情報の集約部署

５）情報展開先からの対策実施状況の報告有無（運輸に関するシステムのセキュリティ情報の集約を情報システム・IT 部門で行う場合）

運輸に関するシステムのセキュリティ情報の集約を情報システム・IT 部門で行う場合、対策実施状況の報告を受けていない場合もあり、展開された情報を元にどのような対策が講じられているか把握されていない。

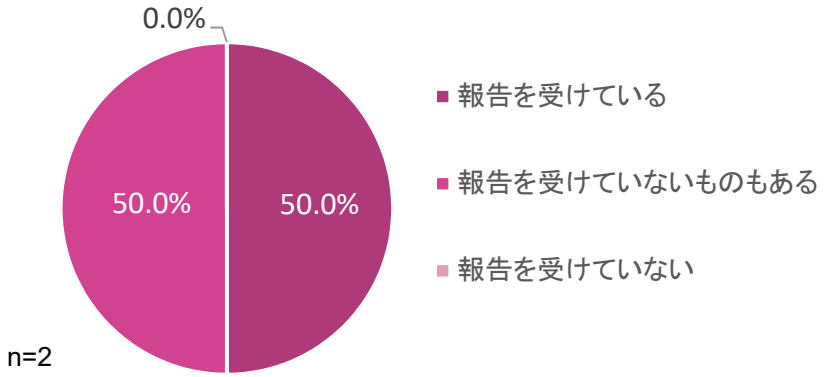


図　情報展開先からの対策実施状況の報告有無

６）情報システム・IT 部門での対応内容（運輸に関するシステムのセキュリティ情報の集約を情報システム・IT 部門以外で行う場合）

運輸に関するシステムのセキュリティ情報の集約を情報システム・IT 部門以外で行う場合の情報システム・IT 部門での対応内容としては、情報システム・IT 部門内で対策を検討場合がある。また、その他の意見として、「当該システム主管部と連携して対応」が挙げられた。

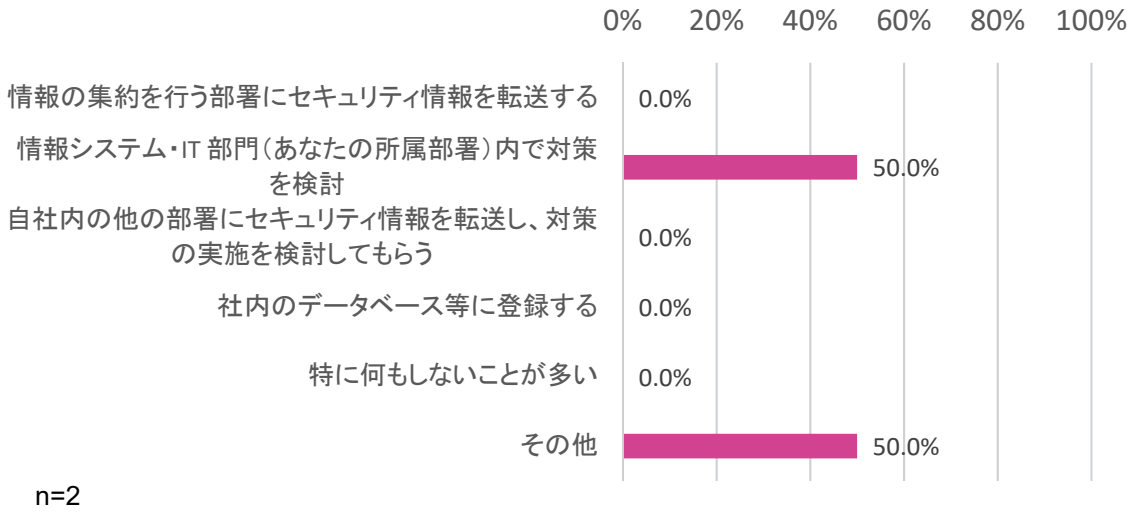


図　情報システム・IT 部門での対応内容

（３）自社の運輸システムがサイバー攻撃を受けた際の情報共有

１）運輸に関するシステムがサイバー攻撃を受けた場合の、情報システム・IT 部門と当該システム担当部門間の情報共有状況

運輸に関するシステムがサイバー攻撃を受けた場合、どの企業でも情報システム・IT 部門と当該システム担当部門間では情報は共有できている。

尚、運輸に関するシステムがサイバー攻撃の被害にあった経験がないため、未回答や想定して回答された場合が含まれる。

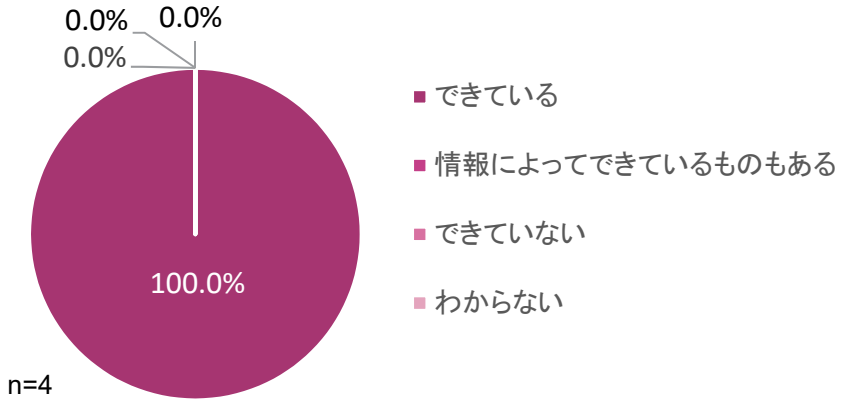


図　運輸に関するシステムがサイバー攻撃を受けた場合の、情報システム・IT 部門と当該システム担当部門間の情報共有状況

２）情報共有で得た情報を元とした、情報システム・IT 部門での対応（情報システム・IT 部門と当該システム担当部門間で情報共有ができている場合）

情報システム・IT 部門と当該システム担当部門間で情報共有ができている場合の情報システム・IT 部門での対応内容として、対策を支援する場合と必要な情報を収集する場合が多い。また、情報システム・IT 部門で直接対策される場合もある。その他の意見として、「現在リスクシナリオを検討しているが、システムによっては初動以降の原因究明まではメーカー等外部協力者との対応になり、また機能復旧を優先させるため、サイバーを原因と特定するまでには一定の時間がかかる。」との意見や「社外組織への報告実施」といった対応がとられる場合もある。

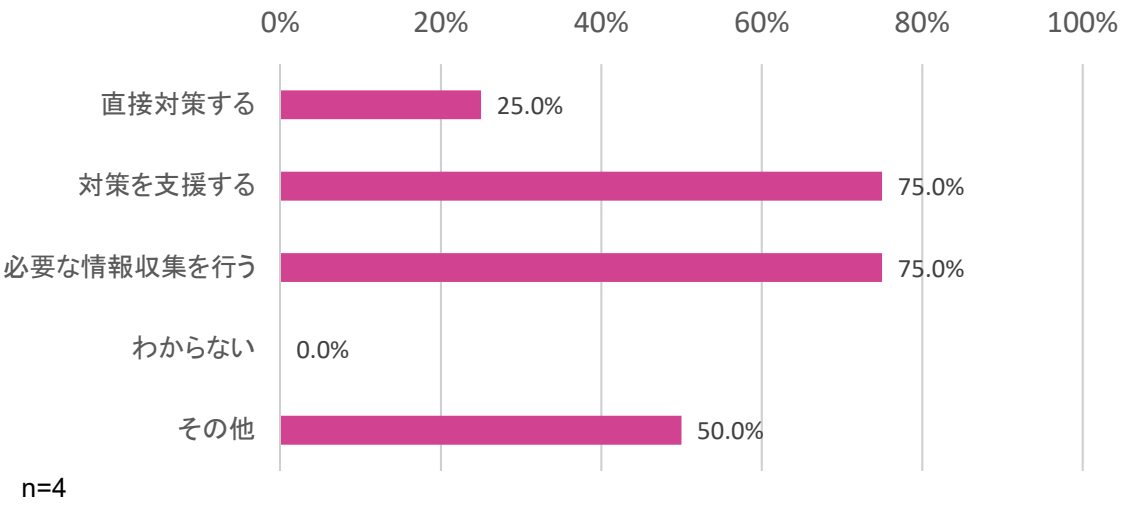


図　情報システム・IT 部門での対応

３）運輸に関するシステムがサイバー攻撃を受けた場合の、情報システム・IT 部門から社外への情報提供経験

運輸に関するシステムがサイバー攻撃を受けた場合、どの企業でも、情報システム・IT 部門から社外への情報提供されたことはない。

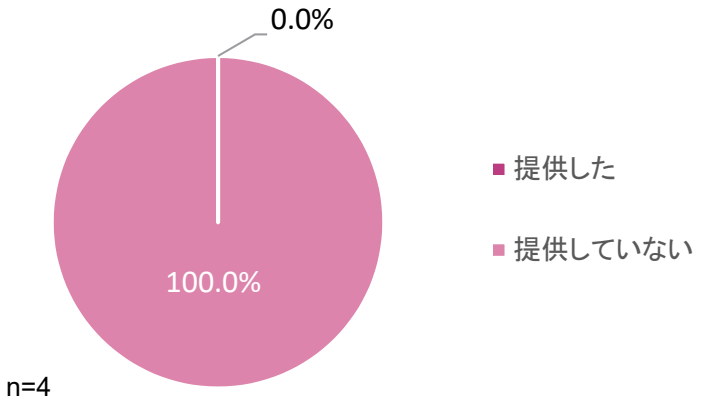


図　運輸に関するシステムがサイバー攻撃を受けた場合の、情報システム・IT 部門から社外への情報提供経験

（４）ISAC について

１）ISAC への期待

どの鉄道事業者も、鉄道分野で ISAC が構築された場合の活動について期待している。

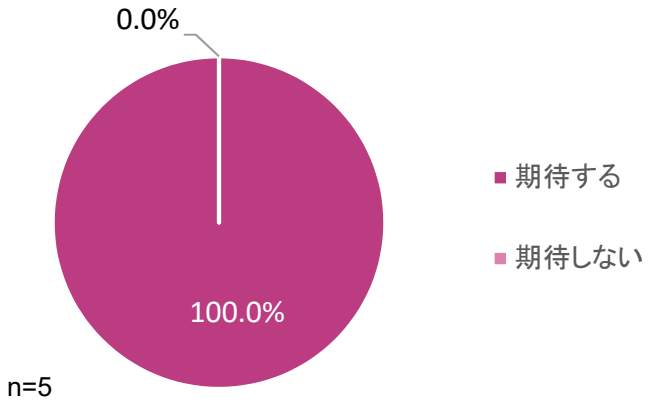


図　ISAC への期待

２）期待する活動

ISAC に期待する活動としては、サイバー攻撃に関する情報を共有することが最も多く、次いでインシデント対応演習等を実施することが高い。

また、その他の意見として、「様々な機関から提供される類似情報の集約窓口としての業務」や「情報共有がＪＲと民鉄、またシステムごとに縦割りとなっていることを踏まえた、全体課題を俯瞰して検討する場」や、「顔の見える人間関係構築の場を期待」という意見が挙げられた。

また、他分野の ISAC 等との連携については特段期待されていない。

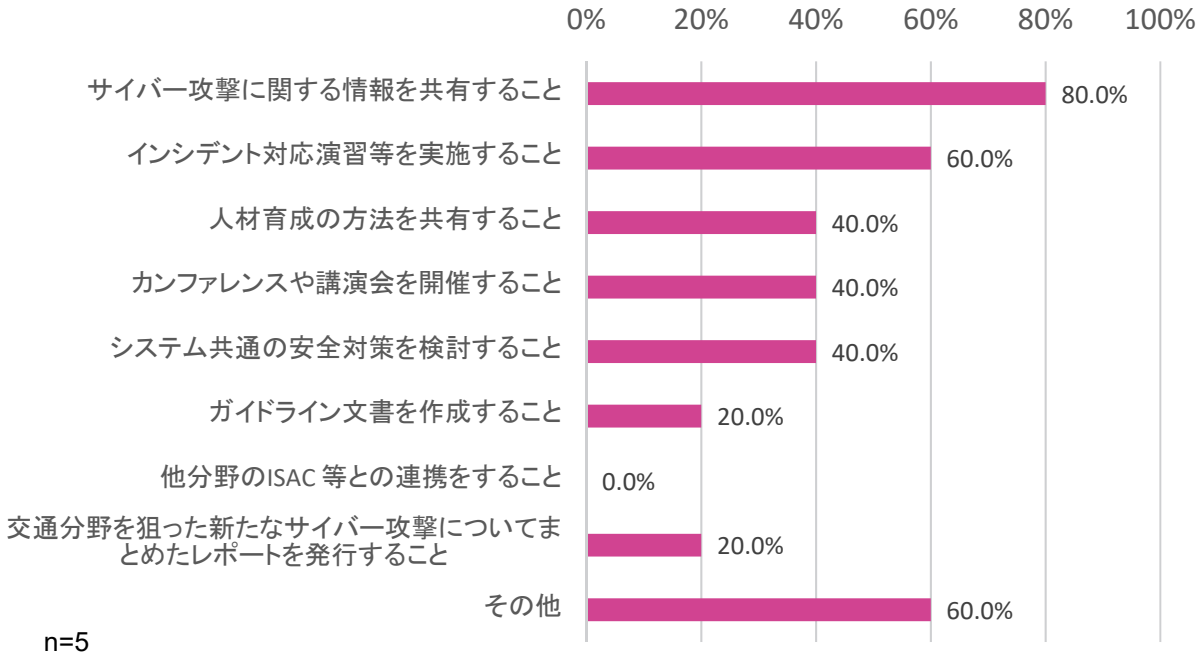


図　ISAC に期待する活動

３）ISAC に加盟すると有効な情報共有ができると考えられる企業

鉄道分野において、ISAC に加盟すると有効な情報共有ができると考えられる企業の種類としては、鉄道事業者が委託しているメーカーが最も多い。またその他の意見でも「日本信号、京三製作所、大同信号、三菱電機、東芝、日立、オムロン」が挙げられており、委託しているメーカーが ISAC に加盟することで、有効な情報共有ができると考えられる。また、「セキュリティベンダー」との意見もあった。

また、鉄道事業者のみが加盟すればよいと考える事業者はいなかった。

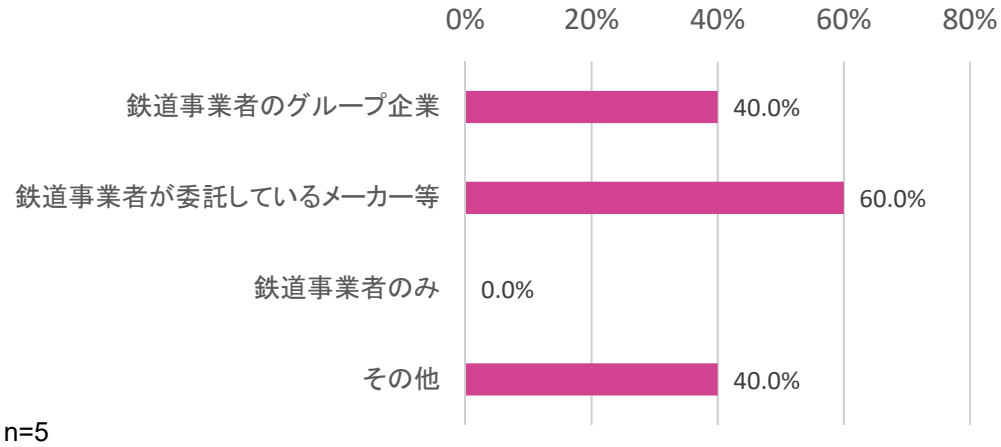


図　ISAC に加盟すると有効な情報共有ができると考えられる企業

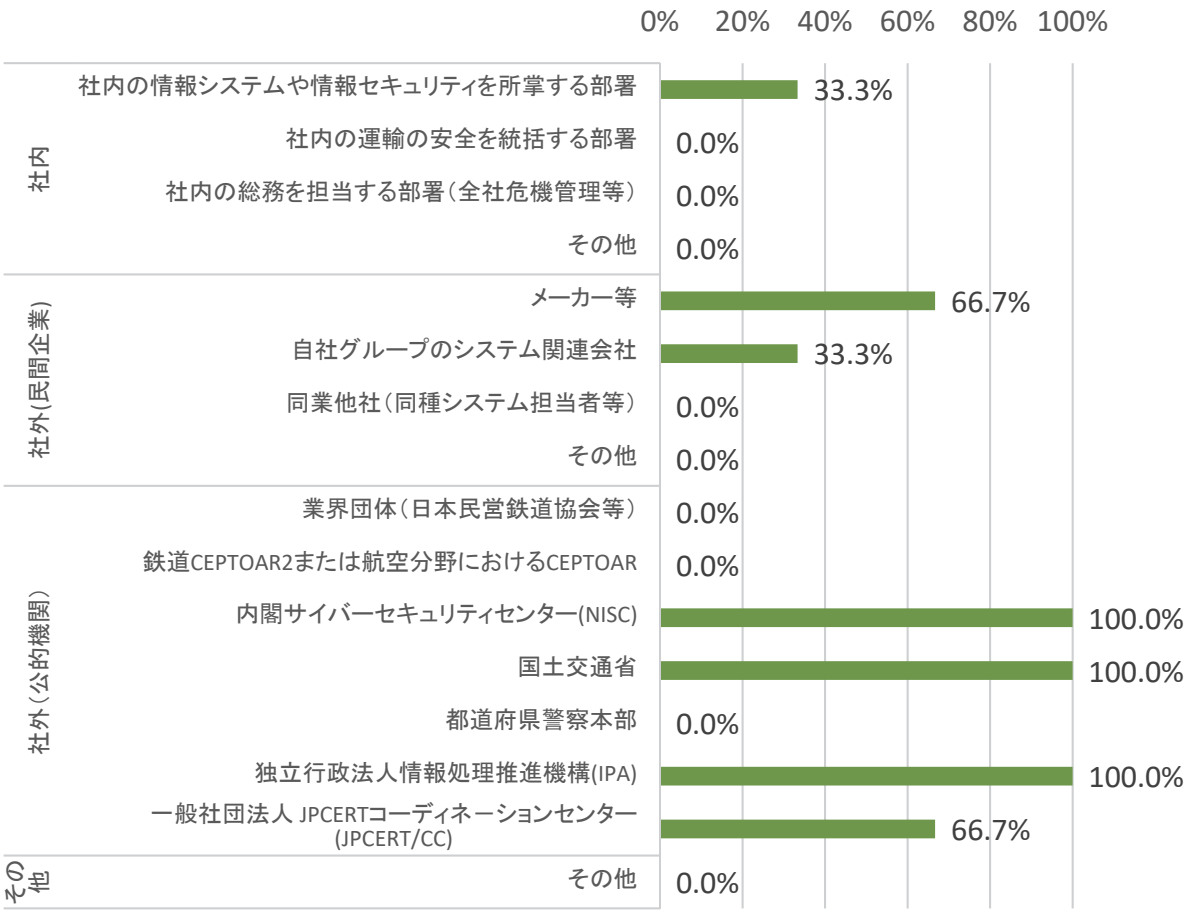
２．３．４　航空分野における運輸部門を対象とした情報共有の実態等に関する調査結果

（１）所管するシステム全般の不具合情報の入手状況

１）システム全般の不具合情報（サイバー攻撃の恐れを含む）の入手元

航空事業者の運輸部門におけるシステム全般の不具合情報の入手元としては、NISC や国土交通省や IPA といった政府機関が最も多く、次いでメーカーとなっている。

また、運輸部門が社内の情報システムを所掌する部署から情報を入手していることがわかる。

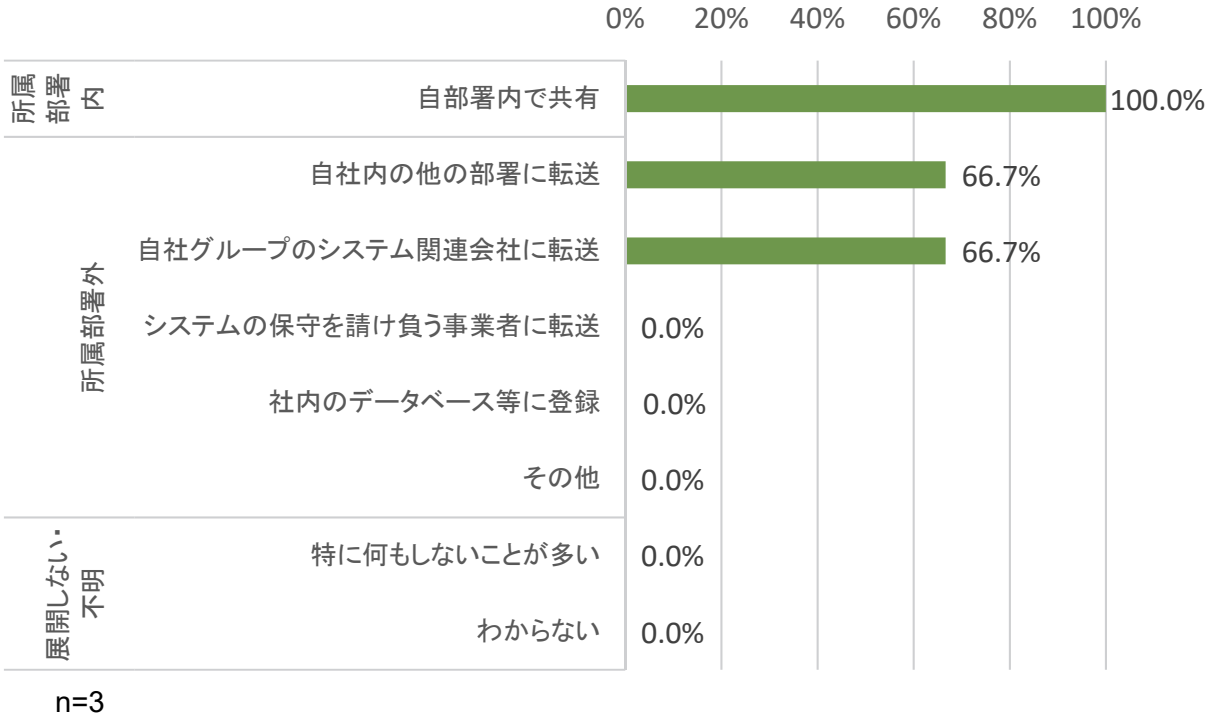


n=3

図　システム全般の不具合情報の入手元

２）社外の公的機関から情報を入手した場合の展開先

運輸部門が社外の公的機関から情報を入手した場合の再展開先としては、自部署内で共有する場合や、自社内の他の部署あるいは自社グループのシステム会社に転送する場合が多い。一方で、システムの保守業者に展開される場合は少ない。



n=3

図　社外の公的機関から情報を入手した場合の展開先

（２）所管するシステム全般の不具合情報の提供状況

１）所管するシステムに不具合（サイバー攻撃の恐れを含む）が発生した場合の情報を提供の有無

航空事業者の運輸部門が所掌するシステムに不具合が発生した場合、運輸部門から他組織に情報は提供されている。

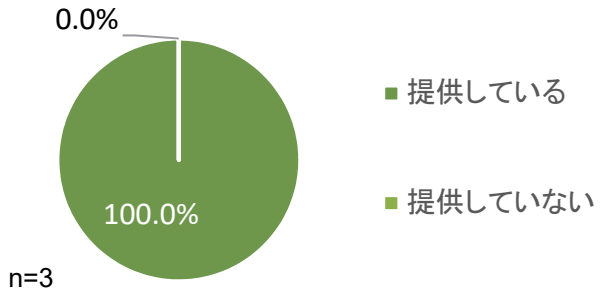


図　所管するシステムに不具合が発生した場合の情報提供の有無

２）所管するシステムに不具合（サイバー攻撃の恐れを含む）が発生した場合の情報提供先

航空事業者の運輸部門が所掌するシステムに不具合が発生した場合における、運輸部門からの情報提供先は、社内では、情報システムや情報セキュリティを所掌する部署や社内の運輸の安全を統括する部署、全社危機管理等となっている。また、社外では NISC や国土交通省が最も多く、次いで警察となっている。

社外の民間企業に提供されることはない点が特徴的である。

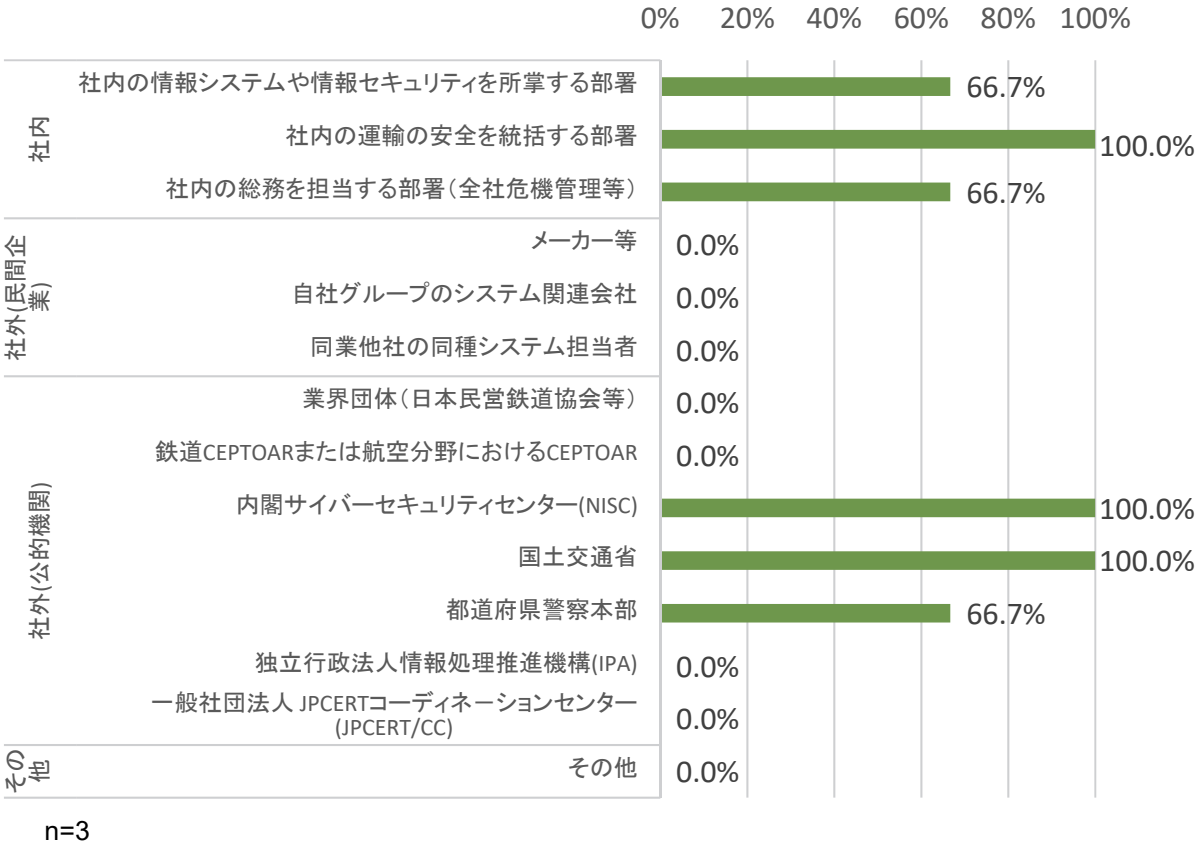


図　所管するシステムに不具合が発生した場合の情報提供先

３）所管するシステムに不具合（サイバー攻撃の恐れを含む）が発生した場合における、情報提供のタイミング

航空事業者の運輸部門が所掌するシステムに不具合が発生した場合の情報提供のタイミングとしては、不具合が発生した段階ですぐに提供されている。

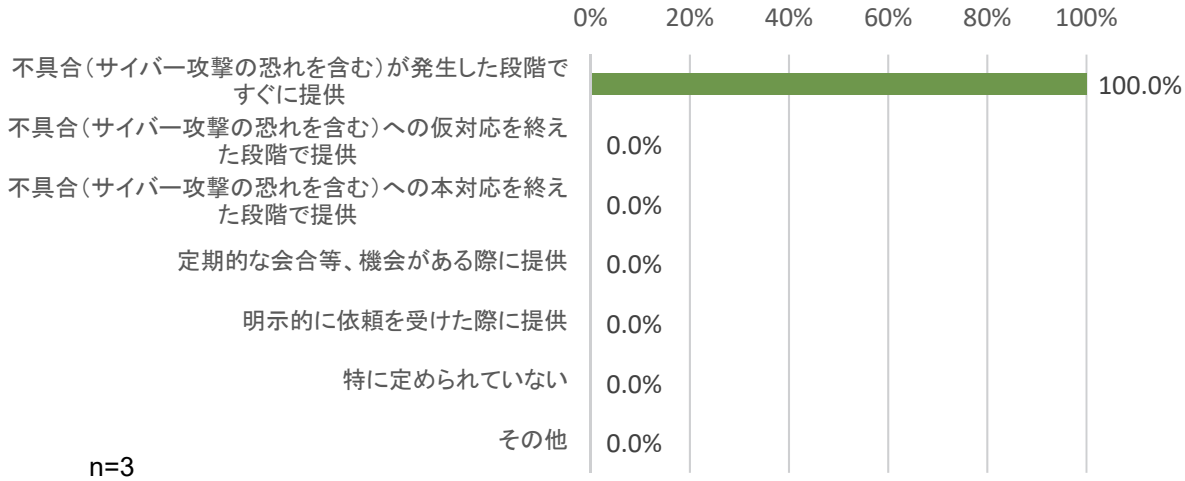


図　所管するシステムに不具合が発生した場合の情報提供のタイミング

２．３．５　航空分野における IT 部門を対象とした情報共有の実態等に関するニーズの調査結果

（１）セキュリティ情報の入手の状況

１）一般的なシステムのセキュリティ情報の入手頻度

航空事業者の IT 部門における一般的なシステムのセキュリティ情報の入手頻度としては多くの企業で 1 週間に 1 回となっており、その他の意見としても「毎営業日」となっており、頻繁に不具合情報を入手していることがわかる。

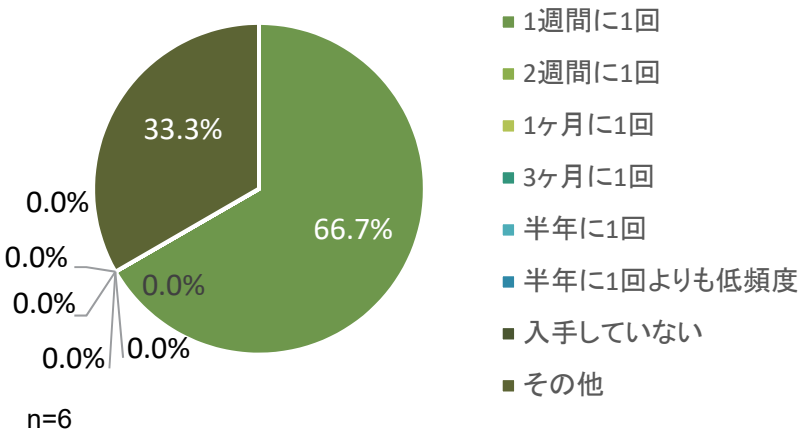


図　一般的なシステムのセキュリティ情報の入手頻度

２）一般的なシステムのセキュリティ情報の種類

航空事業者の IT 部門において入手される一般的なシステムのセキュリティ情報の種類としては、インジケータ、サイバー攻撃傾向・手順・攻撃対象、脆弱性情報、侵入検知シグネチャ、具体的対策が挙げられる。具体的対策は 50%で、攻撃傾向や脆弱性情報等よりも少なくなっている。

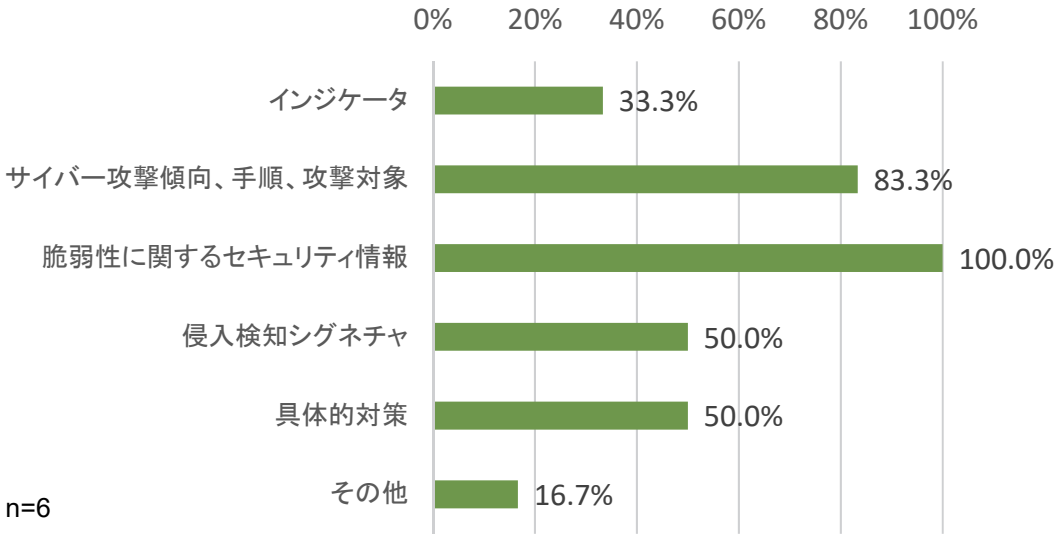


図　一般的なシステムのセキュリティ情報の種類

３）一般的なシステムのセキュリティ情報の入手元

航空事業者の IT 部門における、一般的なシステムのセキュリティ情報の入手元としては、国内外の社外の組織となっている。一方で、航空事業者の IT 部門では、一般的なシステムのセキュリティ情報について社内の他部署から入手されることはない。

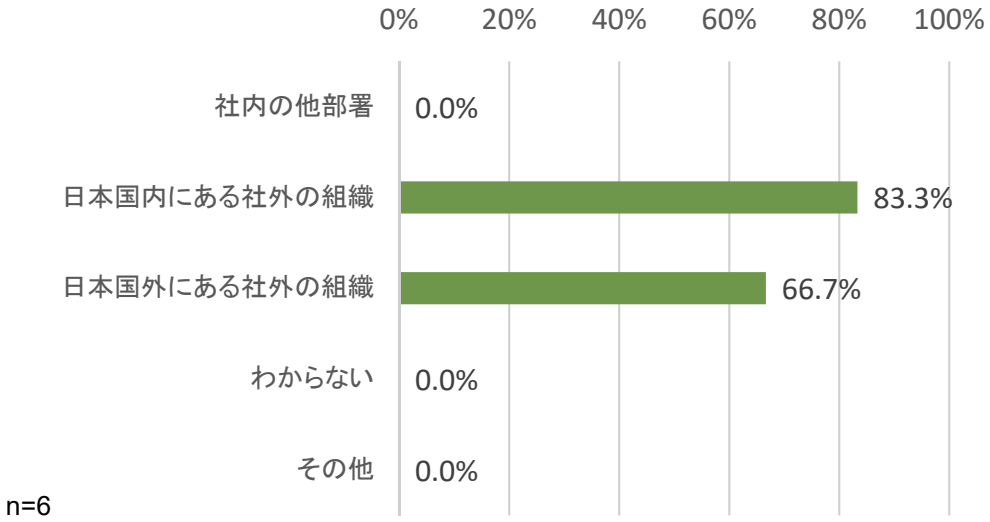


図　一般的なシステムのセキュリティ情報の入手元

４）一般的なシステムのセキュリティ情報の集約部署

航空事業者において、一般的なシステムのセキュリティ情報の集約部署は情報システム・IT 部門で行われる場合が多い。

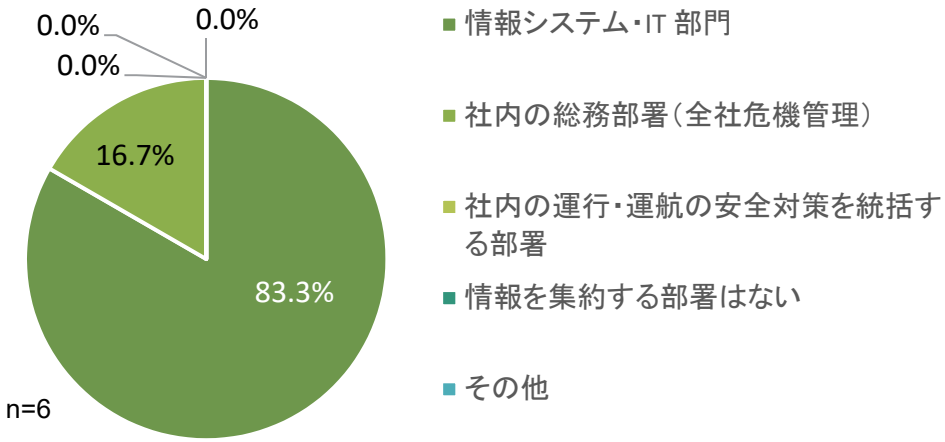


図　一般的なセキュリティ情報の集約部署

５）情報展開先からの対策実施状況の報告有無（一般的なシステムのセキュリティ情報の集約を情報システム・IT 部門で行う場合）

一般的なシステムのセキュリティ情報を情報システム・IT 部門から関係部署に展開した場合、対策実施状況の報告を受けていない場合もあり、展開された情報を元にどのような対策が講じられているか把握されていない。

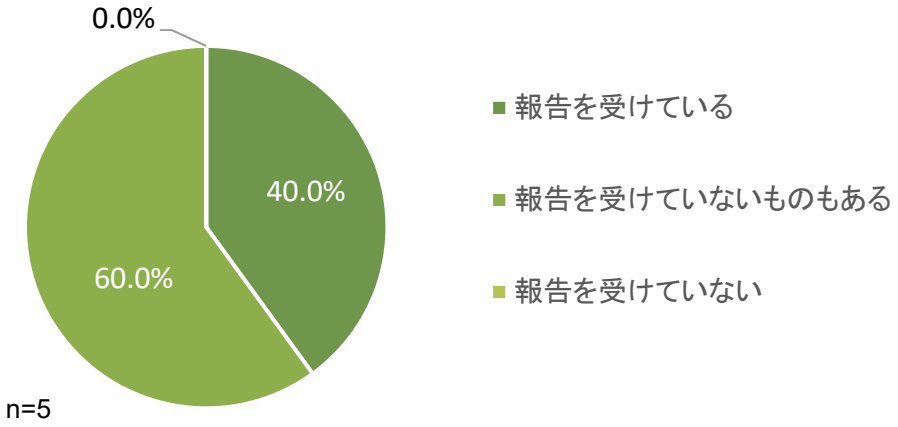


図　対策実施状況の報告有無

６）情報システム・IT 部門での対応内容（一般的なシステムのセキュリティ情報の集約を情報システム・IT 部門以外で行う場合）

一般的なシステムのセキュリティ情報の集約を情報システム・IT 部門以外で行う場合、情報システム・IT 部門での対応内容としては、情報システム・IT 部門で対応される場合がある。またその他としては、「ベンターと共有して対応を行う。」という回答が得られた。

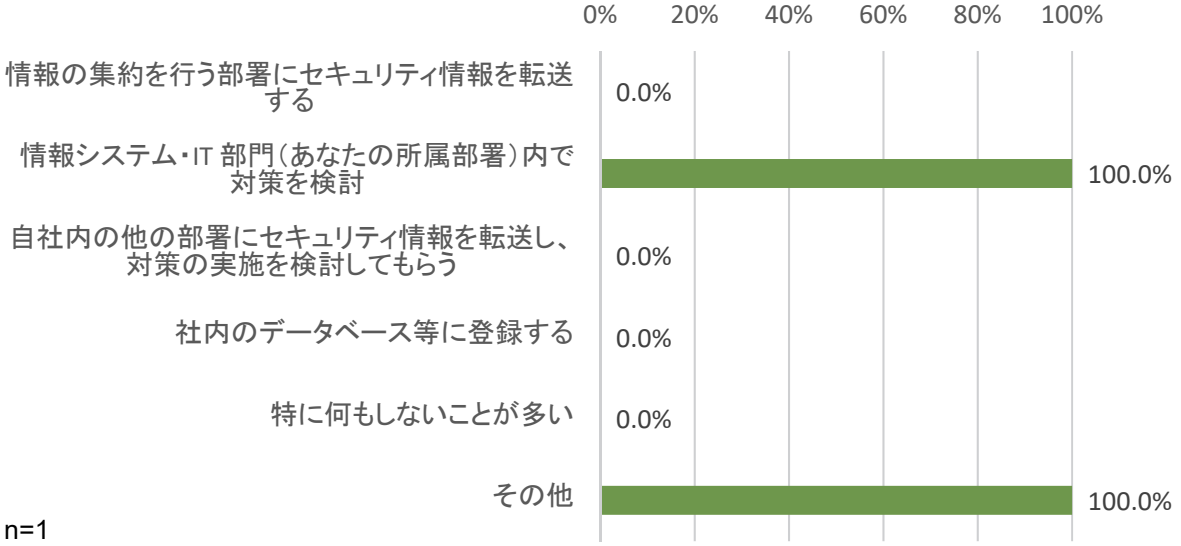


図　一般的なシステムのセキュリティ情報の集約を情報システム・IT 部門以外で行う場合の情報システム・IT 部門での対応内容

（２）運輸に関するシステムのセキュリティ情報の入手の状況

１）運輸に関するシステムのセキュリティ情報の入手頻度

航空事業者の IT 部門における、運輸に関するシステムのセキュリティ情報の入手頻度としては、多くの企業で１週間に１回となっており、その他の意見としても「毎営業日」となっており、頻繁に不具合情報を入手していることがわかる。

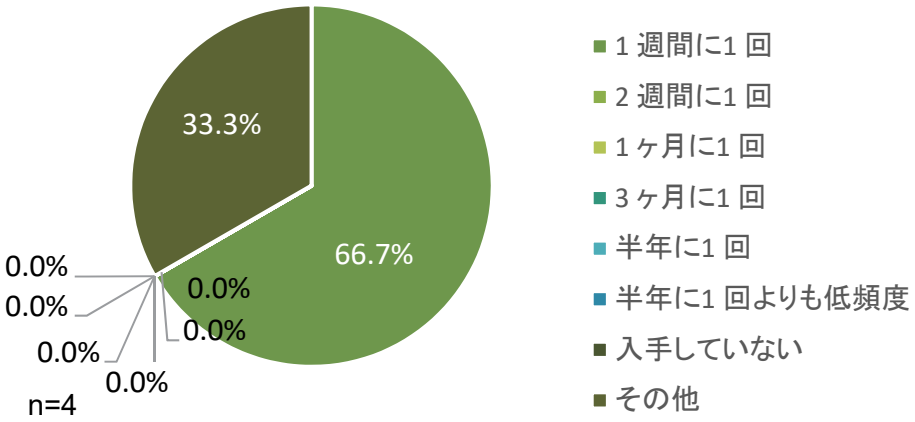


図　運輸に関するシステムのセキュリティ情報の入手頻度

２）運輸に関するシステムのセキュリティ情報の種類

航空事業者の IT 部門において入手される運輸に関するシステムのセキュリティ情報の種類としては、インジケータ、サイバー攻撃傾向・手順・攻撃対象、脆弱性情報、シグネチャ、具体的対策が挙げられる。具体的対策は 50%で、攻撃傾向や脆弱性情報等よりも少なくなっている。

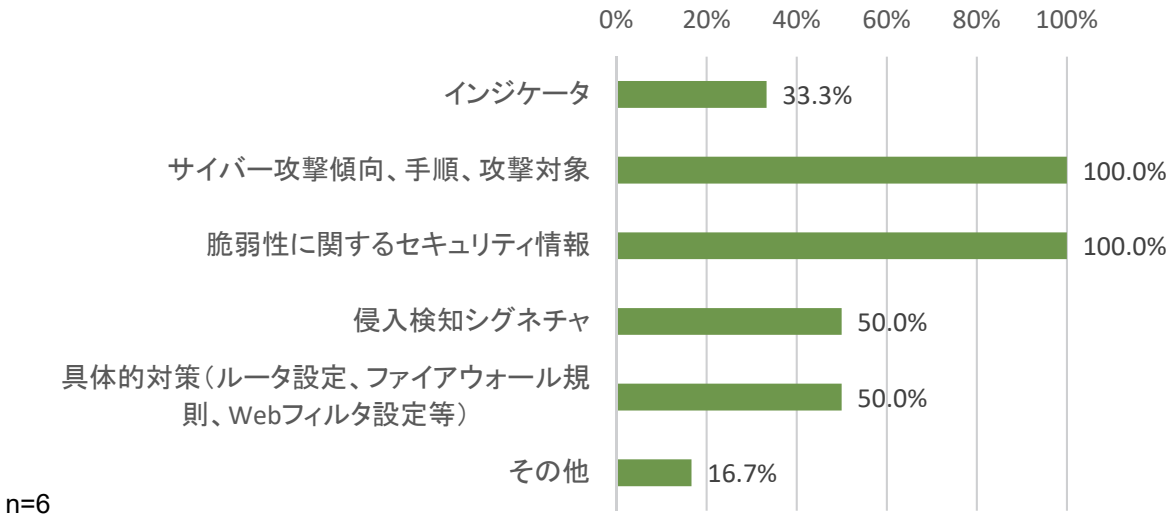


図　運輸に関するシステムのセキュリティ情報の種類

3）運輸に関するシステムのセキュリティ情報の入手元

航空事業者の IT 部門における、運輸に関するシステムのセキュリティ情報の入手元としては、国内外の社外の組織となっている。一方で、航空事業者の IT 部門では、運輸に関するシステムのセキュリティ情報について社内の他部署から入手されることはない。

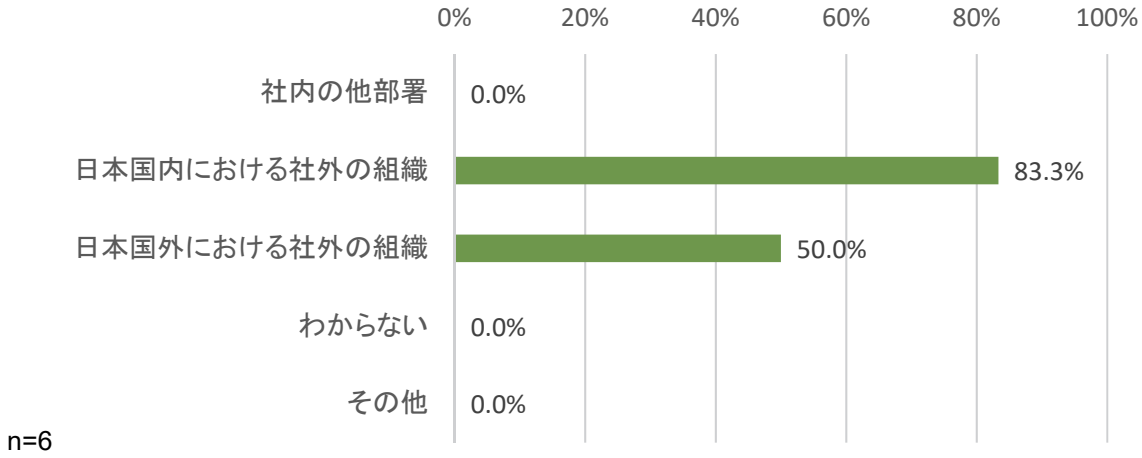


図　運輸に関するシステムのセキュリティ情報の入手元

4）運輸に関するシステムのセキュリティ情報の集約部署

航空事業者において、運輸に関するシステムのセキュリティ情報の集約部署は情報システム・IT 部門で行われる場合が多い。社内の総務部署（全社危機管理）や社内の運行・運航の安全対策を統括する部署で集約されている場合もある。

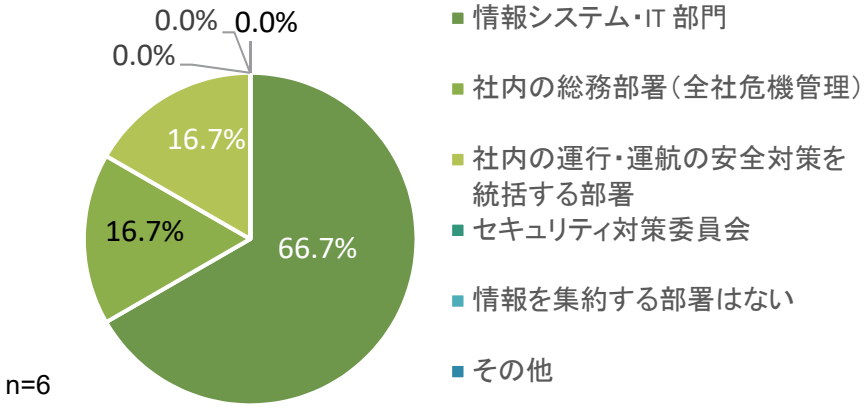


図　運輸に関するシステムのセキュリティ情報の集約部署

５）情報展開先からの対策実施状況の報告有無（運輸に関するシステムのセキュリティ情報の集約を情報システム・IT 部門で行う場合）

運輸に関するシステムのセキュリティ情報を情報システム・IT 部門から関係部署に展開した場合、対策実施状況の報告を受けていない場合もあり、展開された情報を元にどのような対策が講じられているか把握されていない。

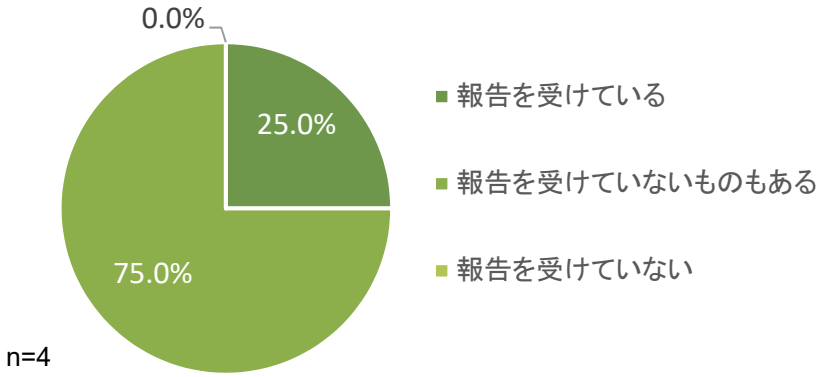


図　情報展開先からの対策実施状況の報告有無

６）情報システム・IT 部門での対応内容（運輸に関するシステムのセキュリティ情報の集約を情報システム・IT 部門以外で行う場合）

運輸に関するシステムのセキュリティ情報の集約を情報システム・IT 部門以外で行う場合、情報システム・IT 部門での対応内容としては、他の部署にセキュリティ情報を転送し、対策の実施を検討してもらう場合がある。またその他としては、「社外へ委託しているため、社外の担当部署に転送し、対策を実施してもらう」という回答が得られた。

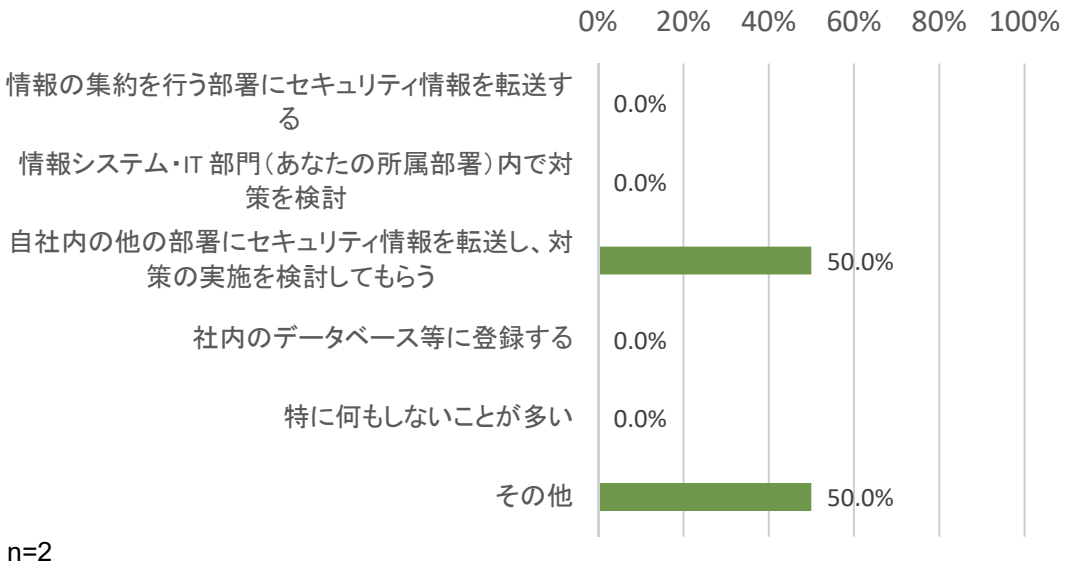


図　運輸に関するシステムのセキュリティ情報の集約を情報システム・IT 部門以外で行う場合の情報システム・IT 部門での対応内容

（３）自社の運輸システムがサイバー攻撃を受けた際の情報共有

１）運輸に関するシステムがサイバー攻撃を受けた場合の、情報システム・IT 部門と当該システム担当部門間の情報共有状況

運輸に関するシステムがサイバー攻撃を受けた場合、どの企業でも情報システム・IT 部門と当該システム担当部門間では情報は共有できている。

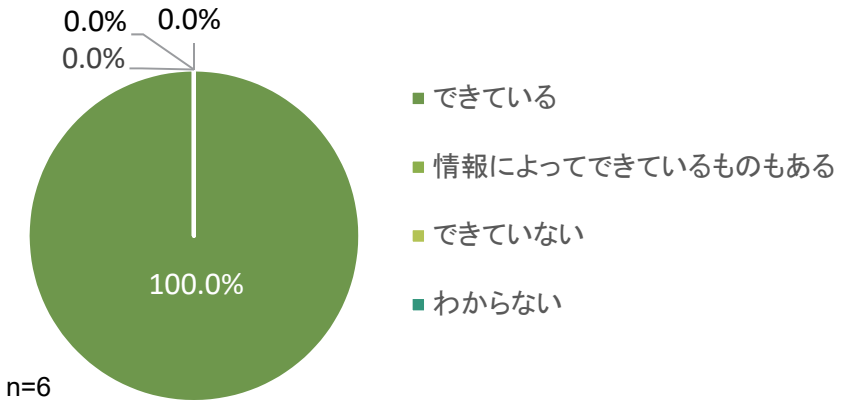


図　運輸に関するシステムがサイバー攻撃を受けた場合の、情報システム・IT 部門と当該システム担当部門間の情報共有状況

２）情報共有で得た情報を元とした、情報システム・IT 部門での対応（情報システム・IT 部門と当該システム担当部門間で情報共有ができている場合）

情報システム・IT 部門と当該システム担当部門間で情報共有ができている場合の情報システム・IT 部門での対応内容は、情報システム・IT 部門で直接対策される場合が多い。

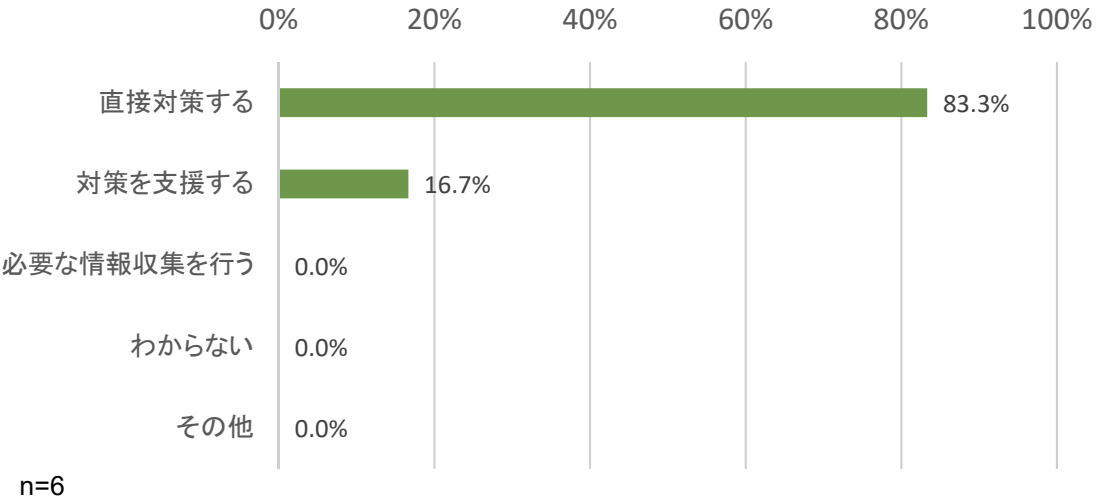


図　情報システム・IT 部門での対応

３）運輸に関するシステムがサイバー攻撃を受けた場合の、情報システム・IT 部門から社外への情報提供経験

運輸に関するシステムがサイバー攻撃を受けた場合、情報システム・IT 部門から社外への情報提供される場合が多い。

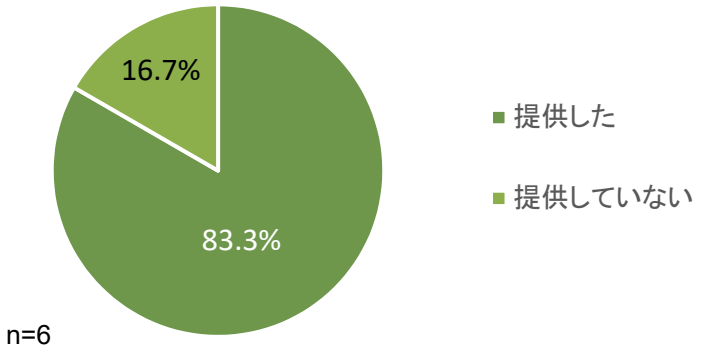
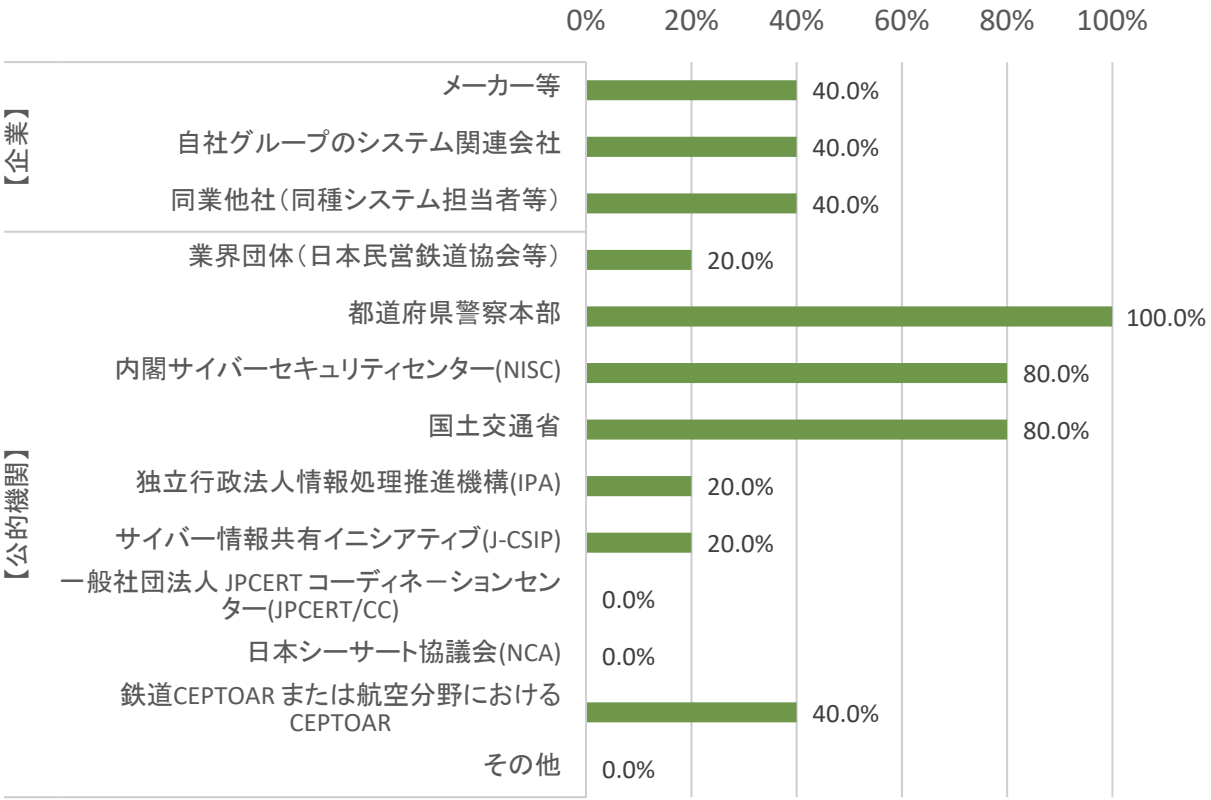


図　運輸に関するシステムがサイバー攻撃を受けた場合の、情報システム・IT 部門から社外への情報提供経験

４）運輸に関するシステムがサイバー攻撃を受けた場合の、情報システム・IT 部門から社外への情報提供先

運輸に関するシステムがサイバー攻撃を受けた場合に、情報システム・IT 部門から社外へ情報提供される先としては警察やNISC、国土交通省等の政府機関が多い。また、メーカーや同業他社に提供する場合もある。さらに、セプターに情報を提供する場合もある。



n=5

図　運輸に関するシステムがサイバー攻撃を受けた場合の、情報システム・IT 部門から社外への情報提供先

５）運輸に関するシステムがサイバー攻撃を受けた場合の、情報システム・IT 部門から社外への情報提供のタイミング

運輸に関するシステムがサイバー攻撃を受けた場合に、情報システム・IT 部門から社外へ情報提供されるタイミングとしては、不具合（サイバー攻撃の恐れを含む）が発生した段階ですぐに提供される場合が多い。

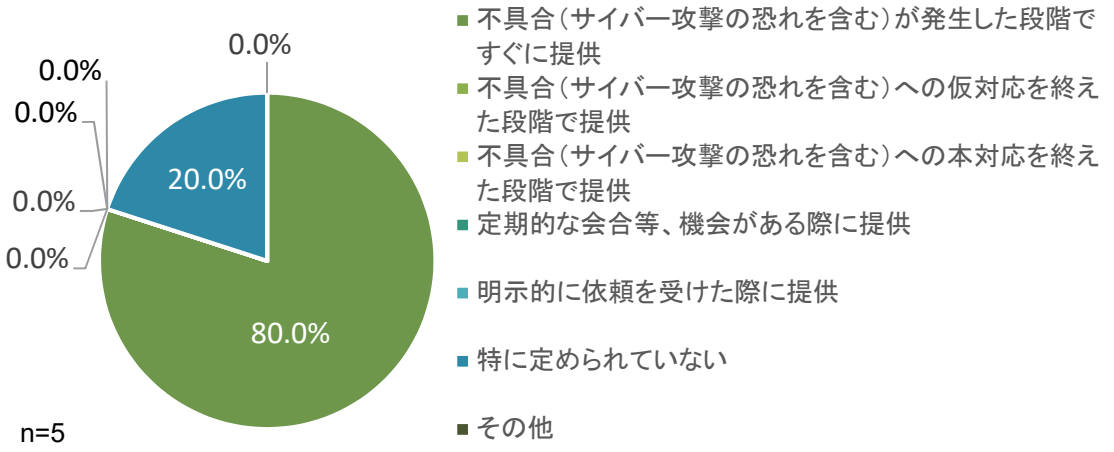


図　運輸に関するシステムがサイバー攻撃を受けた場合の、情報システム・IT 部門から社外への情報提供のタイミング

（４）ISAC について

１）ISAC への期待

多くの航空事業者は、航空分野で ISAC が構築された場合の活動について期待している。

期待しないと回答した事業者の期待しない理由としては、「ISAC の活動（情報共有を目的とした当社へのヒアリング等）が負担になる恐れある」との意見が挙げられた。

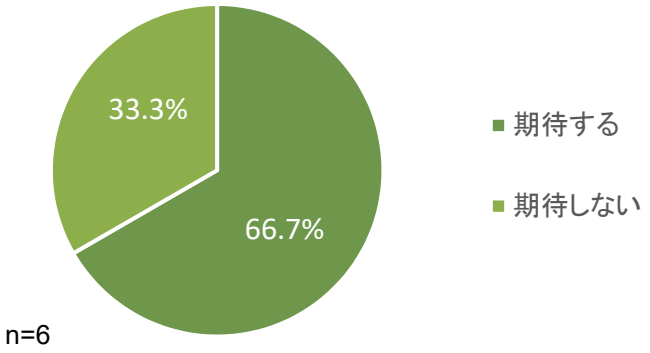


図　ISAC への期待

２）期待する活動

ISAC に期待する活動としては、サイバー攻撃に関する情報を共有すること、インシデント対応演習等を実施することが最も高い。また、人材育成の方法を共有すること、システム共通の安全対策を検討すること、ガイドライン文書を作成すること、交通分野を狙った新たなサイバー攻撃についてまとめたレポートを発行することについてもニーズが高い。

また、鉄道分野では期待されていなかった、他分野の ISAC 等との連携への期待が高くなっている。

一方で、カンファレンスや講演会を開催することについては特段期待されていない。

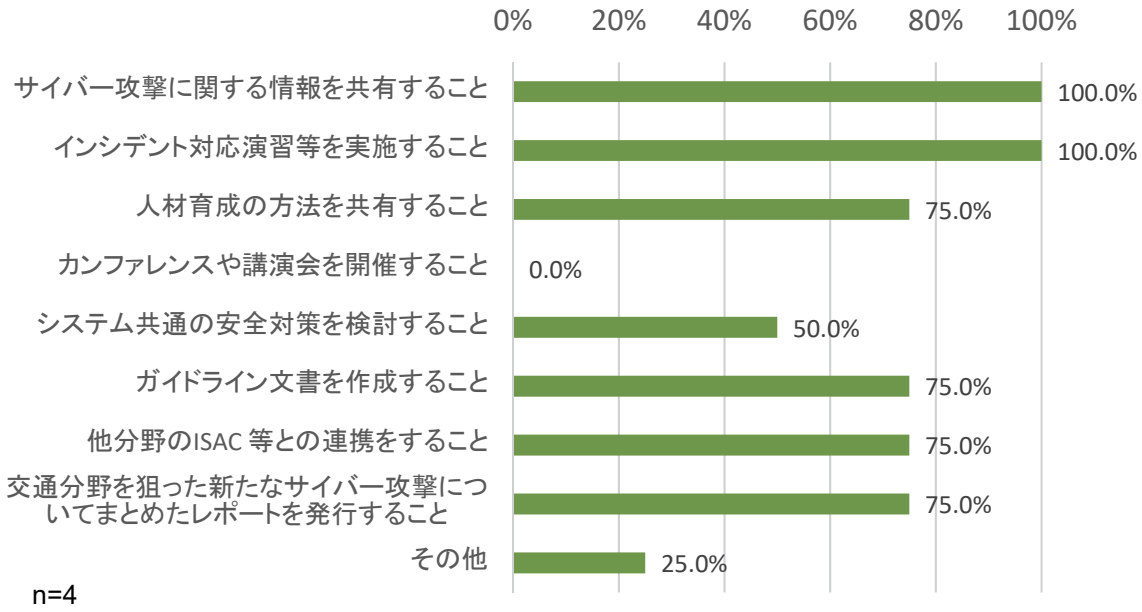


図　ISAC に期待する活動

３）ISAC に加盟すると有効な情報共有ができると考えられる企業

航空分野において、ISAC に加盟すると有効な情報共有ができると考えられる企業の種類としては、航空事業者のグループ企業が最も高い。また、航空事業者が委託しているメーカーも挙げられた。

その他の意見では、「鉄道等の制御系を中心として実施している他重要インフラ事業者」や「外部パートナーとして、空港会社(NAA 他)、日本の空港に乗り入れている外国籍の航空会社、IATA JAPAN,CCS-JAPAN,航空局管制部など航空サービスを支える全インフラ基盤」といった意見が挙げられた。また、「情報の入手先は多いことがよく、特に制限を設けず広くてもいいと思う。」という意見も挙げられた。

航空事業者のみが加盟すればよいと考える事業者はいなかった。

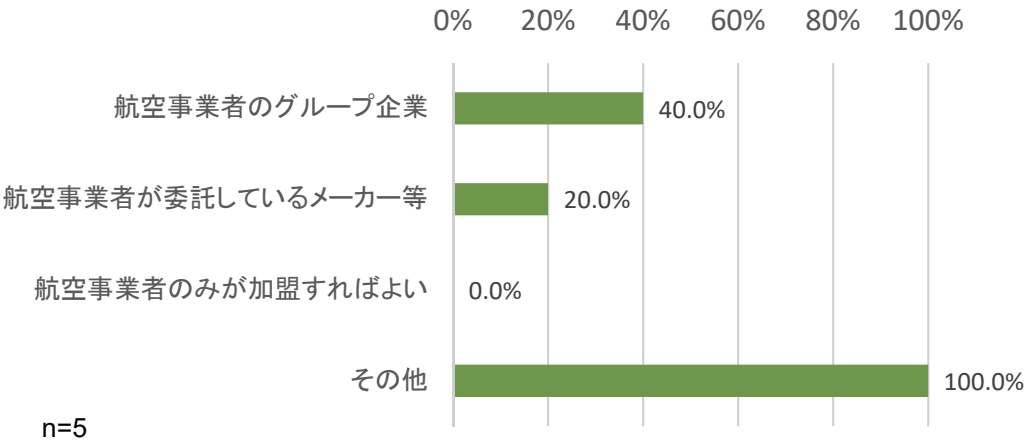


図　ISAC に加盟すると有効な情報共有ができると考えられる企業

２．３．６　アンケートまとめ

（１）鉄道分野における情報共有の実態

鉄道分野の IT 部門では、一般的なシステムのセキュリティ情報については 1 週間に 1 回の頻度で入手しているが、運輸に関するシステムのセキュリティ情報の入手頻度としては 1 週間に 1 回～入手していない場合まで多様となっている。

入手されるセキュリティ情報の種類としては、どちらのシステムについても、インジケータ、サイバー攻撃傾向・手順・攻撃対象、脆弱性情報、侵入検知シグネチャが挙げられる。また、一般的なシステムのセキュリティ情報については具体的対策も入手している場合もあるがその割合は 20%と低くなっており、運輸に関するシステムの場合、入手されていない。

１）一般的なシステムのセキュリティ情報

鉄道事業者の IT 部門における、一般的なシステムのセキュリティ情報の入手元は、国内の社外の組織となっている。一方で、社内の他部署や国外の組織からから入手されることはない。

また、集約部署は、ほぼ情報システム・IT 部門となっている。一般的なシステムのセキュリティ情報を関係部署に展開した場合、対策実施状況の報告を受けていない場合もあり、展開された情報を元にどのような対策が講じられているか把握されていない。

２）運輸に関するシステムのセキュリティ情報

鉄道事業者において、運輸に関するシステムのセキュリティ情報の集約部署は情報システム・IT 部門、安全を統括する部門に分かれる。また、その他の意見として「集約ではなくシステム主管部との相互連携とよって取り扱われる」との意見もある。

社外より鉄道事業者の IT 部門に提供された運輸に関するシステムのセキュリティ情報は自社の運輸を担当する部門に展開されず、IT 部門だけで対策を検討される場合がある。一方で、社外より運輸を担当する部門に直接提供された情報については運輸部門内で共有される他、IT 部門にも共有されている場合がある。

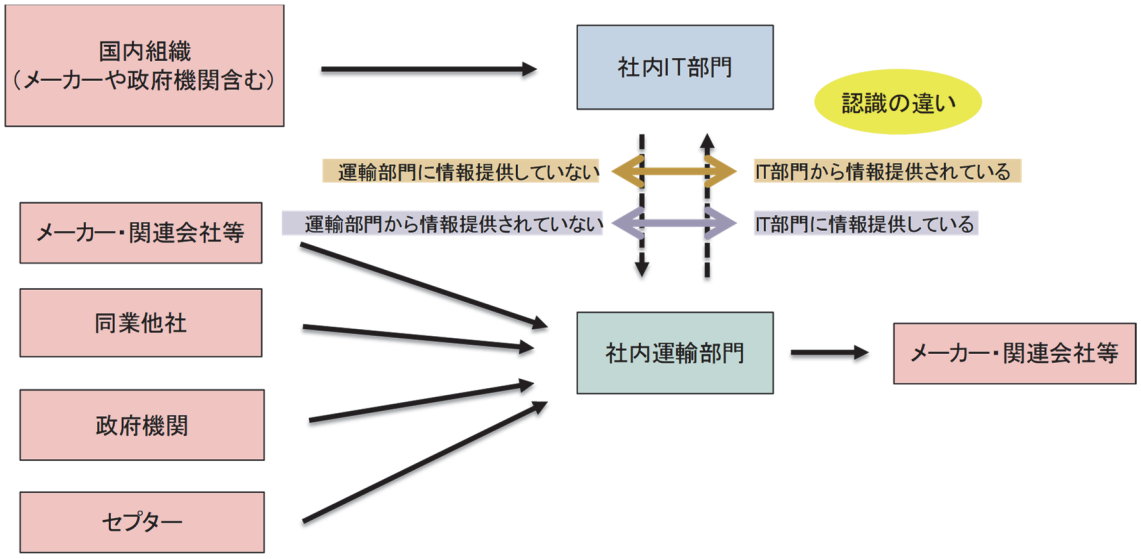


図　社外より提供された運輸に関するシステムのセキュリティ情報の共有の流れ

一方で、自社の運輸に関するシステムがサイバー攻撃を受けた場合は IT 部門と運輸部門で情報共有はされており、IT 部門では直接対策がとられる場合と、他部署の対策を支援する場合、必要な情報を収集する場合がある。この場合、社外への情報提供は運輸部門から行われる。運輸部門からの情報提供先はメーカーが最も多く、次いで国土交通省、システム関連会社となっている。また、事例としては少ないが、同業他社の同種システム担当者や、業界団体（日本民営鉄道協会等)、セプターに提供される場合もある。

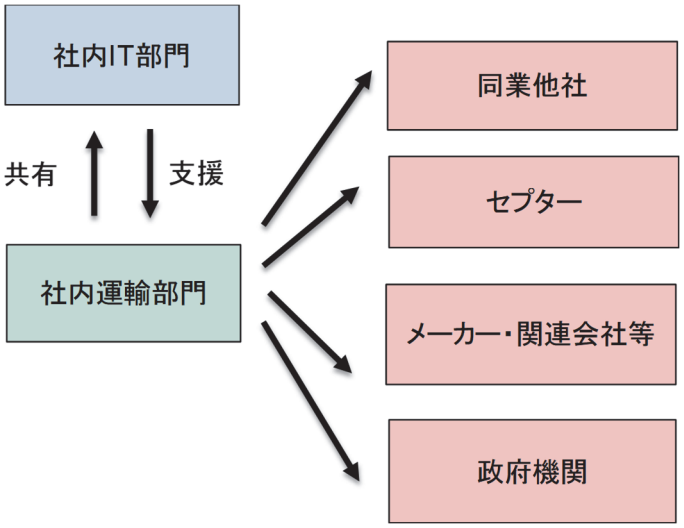


図　自社の運輸に関するシステムがサイバー攻撃を受けた場合の情報共有の流れ

（２）航空分野における情報共有の実態

航空分野の IT 部門では、一般的なシステムのセキュリティ情報も運輸に関するシステムのセキュリティ情報も頻繁に入手されている。入手されるセキュリティ情報の種類としては、どちらのシステムについても、インジケータ、サイバー攻撃傾向・手順・攻撃対象、脆弱性情報、侵入検知シグネチャ、具体的対策が挙げられる。ただし、一般的なシステム及び運輸に関するシステム両方において、具体的対策が入手されている場合は 50%であり、攻撃傾向や脆弱性情報等よりも少なくなっている。

１）一般的なシステムのセキュリティ情報

航空事業者の IT 部門における、一般的なシステムのセキュリティ情報の入手元は、国内外の社外の組織となっている。一方で、社内の他部署から入手されることはない。

また、集約部署は情報システム・IT 部門で行われる場合が多い。情報システム・IT 部門が集約を行う場合、関係部署に展開した場合、対策実施状況の報告を受けていない場合もあり、展開された情報を元にどのように対策が講じられているか把握されていない。情報システム・IT 部門以外の部署で集約される場合でも、実際の対応は情報システム・IT 部門で対応される場合がある。またその他に、ベンターと情報共有して情報システム・IT 部門が対応を行う場合がある。

２）運輸に関するシステムのセキュリティ情報

航空事業者において、運輸に関するシステムのセキュリティ情報の集約部署は情報システム・IT 部門で行われる場合が多い。社内の総務部署（全社危機管理）や社内の運行・運航の安全対策を統括する部署で集約されている場合もある。

航空事業者の運輸を担当する部門における社外からのセキュリティ情報の直接の入手先としては、政府機関やメーカー等となっている。一方で、同業他社や業界団体、航空分野におけるセプターからは、運輸を担当する部門は直接情報を入手していない傾向がある。運輸を担当する部門が入手したセキュリティ情報は IT 部門には共有されており、また、IT 部門に提供された運輸に関するシステムのセキュリティ情報も自社の運輸を担当する部門に展開されていることから、運輸部門と IT 部門の情報共有が行われていると考えられる。

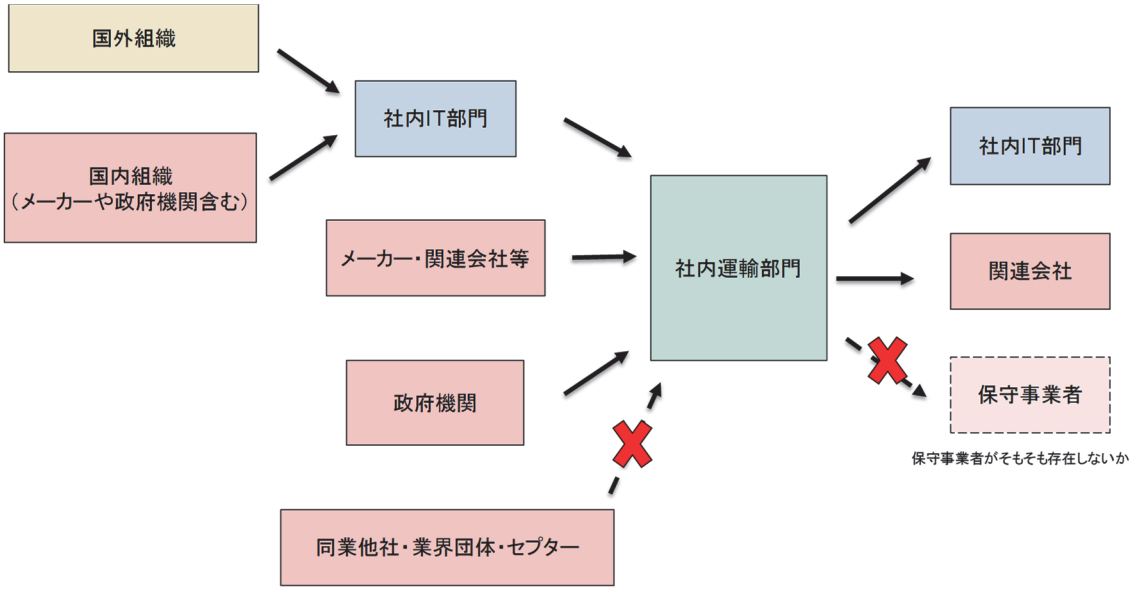


図　社外より提供された運輸に関するシステムのセキュリティ情報の共有の流れ

ただし、自社の運輸に関するシステムがサイバー攻撃を受けた場合は IT 部門と運輸部門で情報共有はされており、IT 部門で直接対策がとられる場合もある。この場合、社外への情報提供は IT 部門と運輸部門のどちらでも行われるが、運輸部門からの報告は公的機関のみに限られ、メーカーや同業他社、セプターへの報告は IT 部門から行われる。

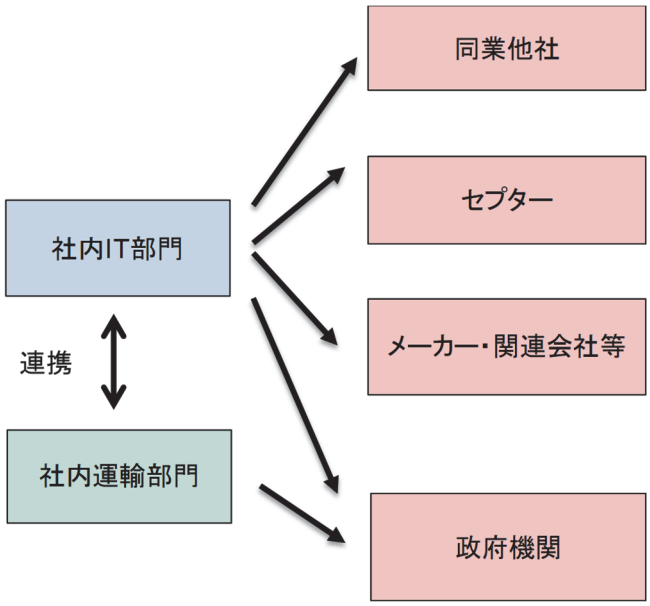


図　自社の運輸に関するシステムがサイバー攻撃を受けた場合の情報共有の流れ

（３）ISAC について

鉄道・航空分野ともに、ISAC への期待は高く、ISAC に期待する活動としては、鉄道・航空分野ともに、「サイバー攻撃に関する情報を共有すること」が最も多くなっている。「インシデント対応演習等を実施すること」や「人材育成の方法を共有すること」、「システム共通の安全対策を検討すること」、「ガイドライン文書を作成すること」、「交通分野を狙った新たなサイバー攻撃についてまとめたレポートを発行すること」についてもニーズが高い。

「他分野の ISAC 等との連携」については鉄道分野では期待されていないが、航空分野では期待が高くなっている。一方で、「カンファレンスや講演会を開催すること」については航空分野では特段期待されていないが、鉄道分野では期待されている。また、その他の意見として、「様々な機関から提供される類似情報の集約窓口としての業務」や「情報共有がシステムごとに縦割りとなっていることを踏まえた、全体課題を俯瞰して検討する場」や、「顔の見える人間関係構築の場を期待」という意見が挙げられた。

ISAC に加盟すると有効な情報共有ができると考えられる企業として、鉄道分野では鉄道事業者が委託しているメーカーが最も多く挙げられた一方、航空分野では事業者のグループ企業が最も高い。また、航空分野からは、「鉄道等の制御系を中心として実施している他重要インフラ事業者」や「外部パートナーとして、空港会社(NAA 他)、日本の空港に乗り入れている外国籍の航空会社、IATA JAPAN, CCS-JAPAN, 航空局管制部など航空サービスを支える全インフラ基盤」、「情報の入手先は多いことがよく、特に制限を設けず広くてもいいと思う。」といった意見が挙げられたことから、航空分野の ISAC では、より多様な関連事業者が加盟すると有効な情報共有ができると考えられる。

尚、鉄道・航空分野ともに、事業者のみが加盟すればよいと考える事業者はいなかった。

２．４　第２章まとめ

鉄道及び航空分野における ISAC 構築に向けた検討を行うため、我が国のセキュリティ情報共有組織におけるセキュリティ情報の収集、分析、提供等の現状、ニーズや課題について把握した。

調査対象としては、国が主導する既存の情報共有組織、国内の既存の ISAC 及び鉄道・航空分野における事業者とした。

国が主導する既存の情報共有組織と先行する ISAC についてはヒアリング調査を実施した。また、鉄道・航空事業者についてはアンケート調査を実施した。

ヒアリング調査の調査項目としては、以下の項目を中心とした。

・情報の収集、分析、提供等の現状、ニーズや課題
・セキュリティ情報共有組織で共有される情報とその入手手段
・情報の受信者の制限
・情報共有の手段と方法
・加盟組織の窓口担当者
・事務局の運営体制
・情報分析
・セキュリティ情報共有組織の提供サービス
・運用時の工夫
・運用時の課題

アンケート調査の調査項目としては、以下の項目を中心とした。

・一般的システムの情報共有の実態
・運輸に関するシステムの情報共有の実態
・ISAC についての考え

本章で明らかにした実情、特に好事例、課題及び事業者の ISAC に対する期待に基づき、鉄道及び航空分野における ISAC 構築に向けた検討（業務・組織の要件）について第 5 章で整理をする。

２．４．１　ヒアリング結果の整理

以下、ヒアリングの各調査項目についての整理を記載する。

（１）セキュリティ情報共有組織で共有される情報とその入手手段

日本国内の代表的なセキュリティ情報共有組織で共有される情報としては、脆弱性情報やインジケータ、脅威情報等が挙げられる。共有される情報は、参加事業者から情報が提供されることもあるが、政府機関が業務で得た情報が共有されている場合が多くを占めている。一方で、ISAC では、政府機関だけではなく、会員からの情報提供も積極的に行われている。政府機関からの情報提供を受ける場合は、受け取った情報の確実な配信を徹底する必要が生じることもあり、国との接点を持つならば、どのような条件にするか検討することが望ましい。

海外からの情報を入手及び共有するための方法として、諸外国の同分野の ISAC との連携や、事務局の国外会議への出席という事例がある。また、海外のコンサルティング会社を利用した情報収集を検討する ISAC もあり、参考事例となりうる。

（２）情報の受信者の制限

各セキュリティ情報共有組織で共有される情報は、情報の種類によってはベンダーへの情報展開等、受信者を制限しているものもあり、TLP が付与されていることも多い。一方で、TLP を付与していない事例もある。TLP によって再提供範囲が定めることで、把握できない範囲まで情報が流出してしまうことへの情報提供者の不安を取り除くことができるため、鉄道及び航空分野における ISAC 構築に向けた検討を行う際には、判断基準を明確にした上で TLP の導入を検討することが望まれる。

（３）情報共有の手段と方法

多くのセキュリティ情報共有組織では、情報共有の手段としてメールを利用している。一部組織ではポータルも利用されている。ポータルを利用している理由としては、インシデント情報とその関連情報やガイドライン等のドキュメント類の情報を蓄積することが可能なこと、共有された情報に対する他会員からの質問（双方向）が容易なこと、メーリングリストの整備が大変であること、参加企業の中で ISAC の担当者が変わることが挙げられている。また、他のセキュリティ情報共有組織でもポータルの整備を検討されている組織があり、情報共有の促進及び情報の蓄積及び運営の負担軽減にはポータルの活用が有効であると考えられる。

また、セキュリティ情報共有組織内における情報共有の方法として、ISAC 全体で脅威情報等の情報を共有する場合と、特定の WG の中で情報が共有される場合がある。特定の WG の中で情報が共有される理由は、業界に特化した情報は業界内で情報共有した方がよいというものである。WG は業界特化型 WG と業界横断型 WG の 2 つに分かれ、それぞれの WG に密接に関わる情報を共有している事例がある。

（４）加盟組織の窓口担当者

各セキュリティ情報共有組織において、参加事業者の窓口の多くは IT 部門所属となっている。ただし、事務局の情報共有以外の主業務と関係した他の部署（安全部門等）が窓口になっている場合もある。また、WG の内容に応じて担当部署の方が出席される場合もあり、柔軟な運営がなされている。鉄道・航空分野（特に鉄道分野）の事業者では、運輸部門と IT 部門で担当範囲が分かれているため、WG に応じて参加者を募集する形になることが望ましい。

（５）セキュリティ情報共有組織の参加条件

セキュリティ情報共有組織によっては、ベンダーの参加を認めている。ベンダーの参加方法としては、ベンダーの枠を設ける場合と、当該分野の事業者とベンダーを区別しない場合がある。鉄道及び航空分野における ISAC 構築に向けた検討を行う際には、WG の種類によっては各分野の事業者だけではなくベンダーも巻き込むことで技術的な詳細を含めた情報を共有することが望ましい。

各 ISAC の加盟組織が ISAC に加盟する理由としては、「同じ攻撃者から攻撃されることが多いため、民間企業で団結し対策をとることが有効であること」、「他社の障害が自社の障害となりうること」、「ISAC の会員リストに名前が載っていること（セキュリティベンダー等）」「ガイドラインの検討の場に入り、ガイドラインに自社の実情を反映できること」、「いち早く情報を手に入れることができること」、「他の企業の取組みを参考にすること」、「業界全体の対策レベルが上がること」が挙げられた。

（６）事務局の運営体制

民間の事業者によるセキュリティ情報共有組織の事務局人員は数名で、事務局を担っている組織に加盟企業が人員を出向させる事例もある。

ISAC では、運営資金として会員クラスに応じた会費を徴収しており、その金額は年間数十万～数百万円程度となっている。また、夜間は事務局の営業時間外となっている場合があるが、当該分野に広範囲に重篤な攻撃が発生しているような状況では、夜間も対応されることがある。さらに、夜間の緊急連絡対応として情報共有ポータルの投稿を担当者ベースで実施する体制がとられている。

また、運営規則において、ISAC で共有された情報に基づく損失については重過失並びに故意の場合を除いて ISAC 及び会員は責任を負わないとしている事例がある。

（７）情報分析

単に情報を共有するだけではなく、攻撃等について各社での対応や影響について報告・分析に力を入れる ISAC や、事務局の有識者等による分析を適宜実施する ISAC がある。分析された情報はインシデント情報の共有に付与される場合がある。一方で、セキュリティ情報の分析には高度な知識と多くの情報が必要となるため、ISAC 内で分析できない場合もある。内部で情報の分析を行うことが難しい ISAC では、日本国外のセキュリティ専門サイトで分析・公開された情報を素早く収集することで対応しており、分析機能の外部委託も検討されている。

（８）セキュリティ情報共有組織の提供サービス

定期的な刊行物を発行している組織や年次総会を実施している組織がある。定期的なメールマガジンを発行し、運営委員のリレー投稿やアナリストのコラム、外部カンファレンスのまとめ、脆弱性対策のまとめ等を記載する事例もある。

また、ISAC では多くの WG を設置しており、教育プログラムとして、演習、スキルアップ講座及び勉強会の開催及びガイドラインの作成等の取組みを行っている。

（９）運用時の工夫

運用時の工夫として、それぞれの組織活動の活性化のために、情報提供者によい情報（その後の流行度合い等の付加情報）を返すことや、活性化のための議論を行う WG が設置されている。また、全ての ISAC では、会員からの情報提供を促進するために大切なことは、情報を出しやすい雰囲気があると考えられている。信頼関係の醸成には WG や年次総会、懇親会等会員同士が顔を合わせる場の提供が有効である。また、ポータルの登録を会社名ではなく担当者名で行い、希望制で顔写真の掲載も可能にすることで、顔の見える化による安心感を提供している。その他の運用時の工夫として、表彰制度がある。会員の投票により、情報共有や WG に貢献した会員が選ばれる。また、会員の要望を吸い上げるために、セキュリティ情報共有組織ではアンケートの実施や WG 等が開催されている場合がある。

（１０）運用時の課題

運用時の課題としては、参加組織が情報提供するモチベーションの維持、配信すべき情報かどうかの判断等、事務局運営に関する課題も挙げられた。ISAC からは、加盟企業全体のセキュリティ対策のボトムアップや、ISAC 担当者が固定化してしまうこと、財政基盤の安定化が必要なこと、情報共有の運用が事務局に依存しており負荷が大きいこと、他のルートからの情報との重複感が挙げられた。

２．４．２　アンケート結果の整理

次に、アンケート調査項目についての整理を記載する。

（１）鉄道分野における一般的なシステムの情報共有の実態

鉄道事業者の IT 部門における、一般的なシステムのセキュリティ情報の入手元は、国内の社外の組織となっている。一方で、社内の他部署や国外の組織からから入手することは少ない。

入手されるセキュリティ情報の種類として、一般的なシステムのセキュリティ情報については具体的対策も入手している場合もあるがその割合は 20%と低くなっており、運輸に関するシステムの場合、入手されていない。

また、集約部署は、情報システム・IT 部門であることが多い。

（２）鉄道分野における運輸に関するシステムの情報共有の実態

鉄道事業者において、運輸に関するシステムのセキュリティ情報の集約部署は情報システム・IT 部門、安全を統括する部門に分かれる。また、その他の意見として「集約ではなくシステム主管部との相互連携とよって取り扱われる」との意見もある。

自社の運輸に関するシステムがサイバー攻撃を受けた場合は IT 部門で直接対策をすることも想定されている。また、IT 部門が他部署の対策を支援する場合、必要な情報の収集を行うことが想定されている。

（３）航空分野における一般的なシステムの情報共有の実態

航空事業者の IT 部門における、一般的なシステムのセキュリティ情報の入手元は、国内外の社外の組織となっている。一方で、社内の他部署から入手されることは少ない。

どちらのシステムについても、インジケータ、サイバー攻撃傾向・手順・攻撃対象、脆弱性情報、侵入検知シグネチャ、具体的対策が入手されているが、具体的対策が入手されている場合は 50%であり、攻撃傾向や脆弱性情報等よりも少なくなっている。

また、集約部署は情報システム・IT 部門である場合が多い。

（４）航空分野における運輸に関するシステムの情報共有の実態

航空事業者において、運輸に関するシステムのセキュリティ情報の集約部署は情報システム・IT 部門である場合が多い。社内の総務部署（全社危機管理）や社内の安全を統括する部署で集約されている場合もある。

自社の運輸に関するシステムがサイバー攻撃を受けた場合は IT 部門で直接対策をすることも想定されている。この場合、社外への情報提供は IT 部門と運輸部門のどちらでも行われるが、運輸部門からの報告は公的機関が中心で、メーカーや同業他社、セプターへの報告は IT 部門から行われる傾向がある。

（５）ISAC についての事業者の考え

鉄道・航空分野ともに、ISAC への期待は高く、以下の活動が期待されている。

・サイバー攻撃に関する情報を共有すること
・インシデント対応演習等を実施すること
・人材育成の方法を共有すること
・システム共通の安全対策を検討すること
・ガイドライン文書を作成すること
・交通分野を狙った新たなサイバー攻撃についてまとめたレポートを発行すること

ISAC に加盟すると有効な情報共有ができると考えられる企業として、鉄道分野では鉄道事業者が委託しているメーカーが最も多く挙げられた。一方で、航空分野では事業者のグループ企業が最も高い。また、航空分野からは、鉄道等他重要インフラ事業者や、空港会社、外国籍の航空会社、IATA JAPAN,CCS-JAPAN,航空局管制部など航空サービスを支える全インフラ基盤といった意見も挙げられたことから、航空分野の ISAC では、より多様な関連事業者が加盟すると有効な情報共有ができると考えられる。

特筆事項として、鉄道・航空分野ともに、事業者のみが加盟すればよいと考える事業者はいなかった。

第３章　サイバー攻撃に関する実態把握

近年起こったサイバー攻撃に関して、国内の情報組織が実施した対応状況を把握し、セキュリティ情報を共有することの重要性を確認するため、近年の起こったサイバー攻撃（特に 2017 年 5 月に世界で流行したランサムウェア WannaCry）に関する事例を整理する。

３．１　サイバー攻撃の事例調査

鉄道・航空分野で発生したサイバー攻撃等、システムに影響が発生ないし可能性があった事例について調査した。

表　航空分野で発生したサイバー攻撃等の事例

事業者名	発生日付	問題分類	概要
LOT polish Airline	2015/6/21[14]	サイバー攻撃	LOT polish Airline の運行計画を行うシステムがサイバー攻撃を受け、ワルシャワ・ショパン空港が混乱に陥った。10 便が欠航になり、15 便が数時間地上待機となり、約 1400 人に影響が出た。
United Airlines	2015/6/2[15]	不正アクセス	システムへの不正アクセスによって不正な運行計画が作成された可能性があり、全てのユナイテッド航空の出発予定便が約 1 時間、地上待機となった。
United Airliness	2015/7/8[16]	システム障害	世界各国で 4900 便に影響が出、米国では全てのユナイテッド航空の出発予定便が約 1 時間、地上待機となった。United Airlines は原因として、ルーターのトラブルによってネットワーク接続が困難になったと発表している。
United Airlines	2015/8/17[17]	脆弱性	United Airlines のアプリケーションに脆弱性が発見され、顧客の個人情報が流出する恐れがあった。

[14] 参考：http://corporate.lot.com/pl/en/press-news?article=772922
[15] 参考：https://www.wired.com/2015/06/united-flights-grounded-mysterious-problem/
[16] 参考：http://money.cnn.com/2015/07/08/news/companies/united-flights-grounded-computer/index.html
https://www.nytimes.com/2015/07/09/business/united-airlines-grounds-flights-citing-computer-glitch.html?_fsi=3fyUhhE9
[17] 参考：https://motherboard.vice.com/en_us/article/8qxy9k/united-airlines-frequent-flyer-app-can-be-hacked-to-reveal-passenger-info

表　鉄道分野で発生したサイバー攻撃等の事例

事業者名	発生日付	問題分類	概要
Trafikverket（スウェーデン産業省交通局）	2017/10/11	サイバー攻撃	サービスプロバイダーTDC と DGC に対する DoS 攻撃の影響により、列車の現在地を示す運行情報システムが表示不能になる等の被害を受けた。
Deutsche Bahn（ドイツ鉄道）	2017/5	ランサムウェア	WannaCry ランサムウェアによる被害。案内表示板にランサムウェアによる攻撃を示す画面が表示された。
San Francisco light rail	2016/11	ランサムウェア	ランサムウェアによる被害。料金を収集せずに運行する措置をとることになった。
Ukraine State Railway	2015	サイバー攻撃	BlackEnergy トロイの木馬による攻撃を受けた[18]。

こうしたサイバー攻撃やシステム障害が発生している中で、最近ではリモートアクセスツールのマルウェアである「Adwind」の感染が、スイスやオーストリア、ウクライナ等の航空業界を標的に拡大している。[19]「Adwind」は Windows、MAC、Linux、Android を含む主要な OS で動作可能で、キー入力情報の収集やスクリーンショットの撮影・収集、標的コンピューターのマイクや Web カメラによる動画、写真、音声の記録・収集、ユーザー情報やシステム情報の収集等、機能が豊富な点に特徴がある。感染の多くは標的型攻撃によるものになっている。

また、2017 年 5 月には世界各地でランサムウェア WannaCry が流行し、日本国内でも鉄道事業者数社が被害を受けた。WannaCry は Windows のファイル共有ネットワークプロトコルの脆弱性「CVE-2017-0144（MS17-010）」を利用しており、コンピューターのファイルを不正に暗号化することで、その解除の見返りに金銭を要求するマルウェアである。その他のランサムウェアとは異なり、WannaCry は一度コンピューターに侵入すると、そのコンピューターからアクセス可能な他のコンピューターに対して自立的に再感染する機能を持っており、この機能によって被害が爆発的に拡大した。WannaCry によってファイルが暗号化され喪失するだけではなく、コンピューター等が使用できなくなることで業務が停止することや、社内外の対応に終われることで社内に混乱が生じるという影響もある。WannaCry によって、ドイツ鉄道では、感染したコンピューターだけではなく駅のディスプレイ画面にも身代金を要求する画面が表示され、ロシア鉄道でも IT システムに影響が発生した。

[18] 参考：https://www.its-mobility.de/download/Test4Rail/171018_Cherfia_fortiss_Test4Rail_Presentation.pdf
[19] 参考：https://amp.thehackernews.com/thn/2017/07/adwind-rat-malware.html

３．２　国内の情報共有組織へのヒアリング

３．２．１　調査方針

近年の起こったサイバー攻撃(特に 2017 年 5 月に世界で流行したランサムウェア WannaCry)に関して、国内の情報組織が実施した対応についてヒアリングを行った。

表　国内のセキュリティ情報共有組織へのヒアリング調査概要

調査対象	国内のセキュリティ情報共有組織 7 団体
調査項目	■　近年の起こったサイバー攻撃に関する加盟企業の被害状況の共有の形 ■　セキュリティ情報共有組織としての対応 ■　情報共有により被害が防止されたなどの成功事例
調査期間	2017 年 11 月～12 月

３．２．２　調査結果

近年の起こったサイバー攻撃(特に2017年5月に世界で流行したランサムウェアWannaCry)に関して、国内の情報組織が実施した対応について下表に示す。

表　近年の起こったサイバー攻撃に対する国内の情報共有組織の対応

WannaCryに関する情報共有の有無	**・WannaCryの情報は共有された** WannaCry の発生当初は各社の被害状況について共有した。攻撃が落ちついた頃にはWannaCryの特徴・脅威について共有した。/ 各事業者から政府機関へ情報提供され、その情報は所管省庁経由で各事業者に情報提供された **・WannaCry についてはネットワークの脅威ではないため情報共有をしていない。Mirai（機器を乗っ取り、サイバー攻撃を可能にするマルウェア）については情報共有された** 攻撃対象のポートや、踏み台と推測される機械、対策の検証結果等について共有した
サイバー攻撃が発生した場合のセキュリティ情報共有組織としての対応	**・身代金を要求してDDoS攻撃を仕掛ける事例が増加した際にはレポートをまとめ、配信を行った** インシデントが発生した際には、会員が集まり、意見交換を行う **・サイバー攻撃が発生した場合は、該当するWGで議論される。該当するWGがない場合は事務局として会合の開催を提案する** **・WannaCry の発生時には、欧州に出張している事務局メンバーがいたため、日本国内でWannaCryの被害について大きく報道されるよりも前に情報展開を行った** **・WannaCry の発生時には、事務局として情報を取りまとめることはしなかった** **・サイバー攻撃が発生した場合は、所管省庁から各事業者に展開する。NISCからの情報はセプターに提供される** **・WannaCry の発生時には、事務局を運営している組織として情報を公表した** **・サイバー攻撃が発生した場合は、関連するWGにおいて、専門機関から事後的に解説される場合がある**
情報共有により被害が防止されたなどの成功事例	**・当該のセキュリティ情報共有組織が対象とする分野において最も発生件数が多い攻撃が、対前年で半数以下に減少した** **・攻撃の踏み台となる機器を探すWGでDNSのリフレクション攻撃[20]の踏み台になる機器を探しだし､所有者に修正を依頼し､対応してもらった。修正を始めるタイミングで攻撃が始まったので､完全ではないが､迅速に抑制できた** **・特に具体的な事例はない** 展開した情報によって被害が防げたか、紐付けが難しい **・定量的な検証はしていないが、防御できたという報告は上がっている** 想定される失敗として、共有されるインジケータが間違っている可能性がある。正規のサイトをブロックすることで業務が遂行できなくなる事例も考えられる **・対策を実行し防げたという報告がある**

[20] 攻撃対象のIPアドレスに偽装して踏み台となるDNSサーバーにDNSリクエストを送ることによって、問合せを受けたDNSサーバーは偽の送信元である攻撃対象に大量のDNSパケットを送り付ける。

WannaCry による被害状況については、他情報機関からもたらされた情報や独自に収集した情報が加盟企業間で共有されている場合が多い。WannaCry の発生直後から被害の収束後まで、継続的に被害状況や対応策、問題点等について共有・議論されていたセキュリティ情報共有組織もある。一方で、WannaCry は通信等のネットワークの脅威ではないという理由から情報は取り扱われていないセキュリティ情報共有組織もあり、各分野への影響度に合わせて情報共有されていることが伺える。

サイバー攻撃が発生した場合の情報共有組織としての対応方法は、発生直後はメール等を用い情報共有され、ある程度被害が収束した後に WG 等集まる機会が設置され、議論される場合がある。また、事務局からレポートを配信する場合もある。

情報共有よって被害が防止された事例もある。例えば、DNS のリフレクション攻撃の踏み台になる機器を探しだし、修正を依頼したことによって急速に攻撃を封じ込めることができたという事例がある。また、継続的な情報共有によって、当該のセキュリティ情報共有組織が対象とする分野において最も発生件数が多い攻撃が、対前年で半数以下に減少したという効果もあった。

３．３　国内の鉄道・航空事業者へのアンケート

３．３．１　調査方針

2017 年 5 月に世界で流行したランサムウェアに関して、国内の鉄道・航空事業者の情報入手状況及び対応について把握し、実際に発生した事例に基づく情報共有の課題を明らかにするため、アンケート調査を行った。

表　国内の鉄道・航空関連事業者へのアンケート調査概要

調査対象	➢ 鉄道事業者の情報システム・IT 部門：5 社 ➢ 航空事業者（空港事業者含む）の情報システム・IT 部門：6 社
調査項目	・ ランサムウェア WannaCry による被害状況・要因・対策等に関する、社外から情報入手状況 ・ ランサムウェア WannaCry による被害状況・要因・対策等に関する情報を入手した場合の対策の実施状況
調査手法	メールで配布
調査期間	2018 年 2 月

３．３．２　調査結果

（１）2017 年 5 月に発生したランサムウェア WannaCry に関連する情報共有状況

１）ランサムウェア WannaCry による被害状況・要因・対策等に関する、社外から情報入手状況

ランサムウェア WannaCry による被害状況・要因・対策等に関する情報は、鉄道・航空分野ともに社外から情報入手されている。社外からの入手経路は鉄道・航空分野ともに公的機関が最も多く、他業界から入手されるケースは少なくなっている。また、同業他社から入手するよりも、自社システムベンダーから情報を入手する場合が多く、ベンダーとの結びつきが強いことが推測される。

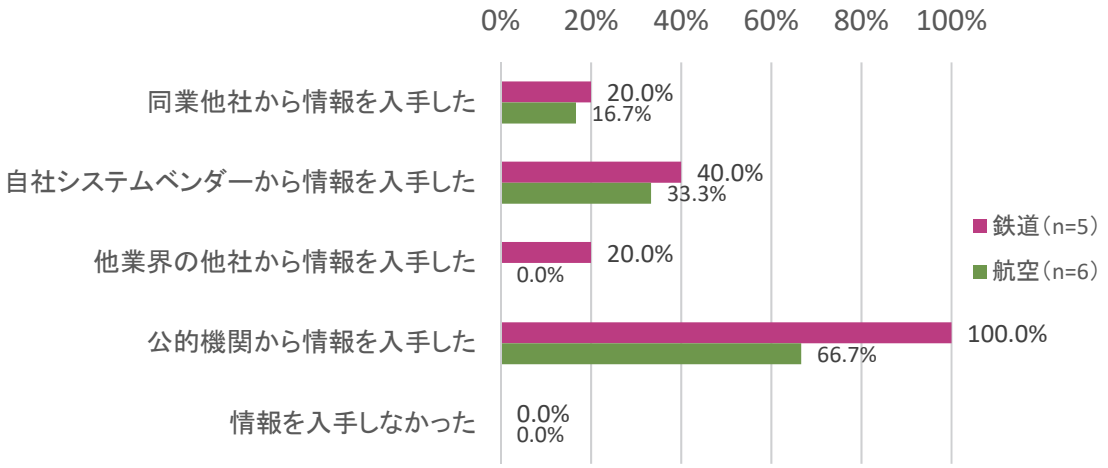


図　WannaCry に関する情報の入手状況

２）ランサムウェア WannaCry による被害状況・要因・対策等に関する情報を入手した場合の対策の実施状況

ランサムウェア WannaCry に関する情報を入手した企業の多くでは、情報を元に対策が実施されている。

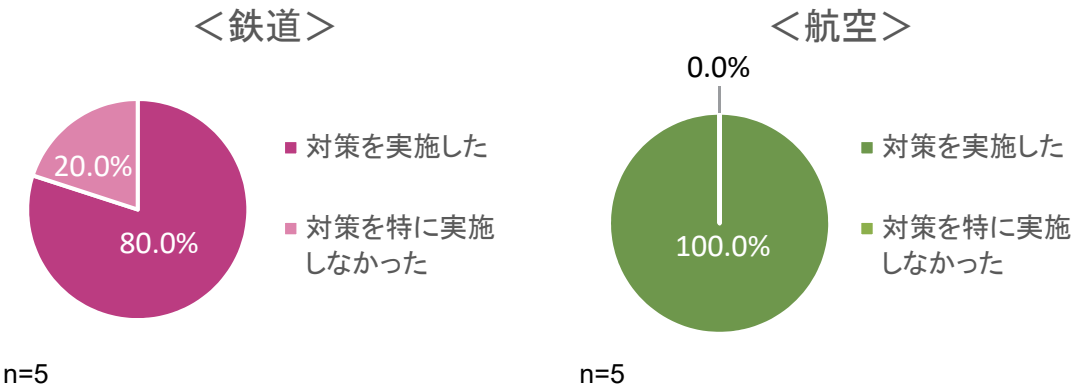


図　WannaCry に関する情報を入手した場合の対策の実施状況

（２）アンケートまとめ

鉄道・航空分野では、ランサムウェア WannaCry が発生した際、被害状況や要因、対策等について、社外と情報共有されているが、その多くは公的機関からの情報入手であり、民間企業の中での情報共有はまだまだである。また、公的機関の次に多い情報の入手先は自社ベンダーで、次いで同業他社、他業界の他社となっている。鉄道・航空分野のベンダーとの結びつきの強さが伺える。

また、ランサムウェア WannaCry の被害状況や要因、対策等についての情報を入手した企業の多くでは対策が実施されており、対策の実施には、まず、情報を入手することが大切と考えられる。

３．４　第３章まとめ

本章では、サイバー攻撃の実態に関する調査を行い、共有すべき情報の発生状況、及び情報共有組織としての対応について実態を把握した。

調査対象としては、国が主導する既存の情報共有組織、国内の既存の ISAC 及び鉄道・航空分野における事業者とした。

調査項目としては、以下の項目を中心とした。

・近年に起こったサイバー攻撃に関する加盟企業の被害状況の共有の形
・セキュリティ情報共有組織としての対応
・情報共有により被害が防止されたなどの成功事例

近年では、鉄道・航空分野でもサイバー攻撃等のシステムに影響する可能性のある事例が発生しており、特に 2017 年 5 月に世界で流行したランサムウェア WannaCry は、鉄道・航空分野に限らず多くの分野で広範な被害をもたらした。

国内の情報組織の多くでは、WannaCry に関する他情報機関からもたらされた情報や独自に収集した情報が加盟企業間で共有されていた。WannaCry の発生直後から被害の収束後まで、継続的に被害状況や対応策、問題点等について共有・議論されていたセキュリティ情報共有組織もある。一方で、WannaCry は通信等のネットワークの脅威ではないという理由から情報は取り扱われていないセキュリティ情報共有組織もあり、各分野への影響度に合わせて情報共有されていることが伺える。

鉄道・航空事業者では、WannaCry に関する情報の入手先のトップは公的機関となっており、事業者間の情報共有は局所的なものにとどまっている。一方で、WannaCry の情報を入手した鉄道・航空事業者の多くでは対策が実施されており、情報を入手することの重要性が認識され、適宜活用されていることも確認できた。

サイバー攻撃が発生した場合の情報共有組織としての対応方法は、発生直後にはメール等を用い情報共有され、ある程度被害が収束した後に WG 等集まる機会が設置され、議論される場合が多い。また、事務局からレポートを配信する場合もある。

こうした情報共有よって被害が防止された事例もある。例えば、DNS のリフレクション攻撃の踏み台になる機器を探しだし、修正を依頼したことによって急速に攻撃を封じ込めることができたという事例がある。また、継続的な情報共有によって、当該のセキュリティ情報共有組織が対象とする分野において最も発生件数が多い攻撃が、対前年で半数以下に減少したことに寄与していると考えられる。

国内において、鉄道・航空分野の運輸に関わるシステムを直接的に狙うサイバー攻撃については、共有対象となる情報に乏しいが、影響範囲の広いインシデントが発生したとき等は、事業者は情報共有と対策を確認している。また、既存の情報共有組織としても適切な情報提供を加盟企業に実施するために対応を実施している。

鉄道・航空分野における情報共有組織としては、特定の運輸に関わるシステムを狙った攻撃に関する情報ではなく、汎用的なソフトウェアの情報や他分野の情報について会員に提供することになると推測される。

第４章　諸外国のセキュリティ情報共有組織の実態調査

第５章において今後の我が国のセキュリティ情報共有組織の在り方を検討するために、セキュリティ情報の共有体制が進んでいる諸外国のセキュリティ情報組織の実態を調査する。合わせて、ロンドン五輪、リオデジャネイロ五輪でのサイバー攻撃の実態や取組みについて調査し、2020東京五輪に向けて情報共有組織のベストプラクティスを把握する。

４．１　諸外国のセキュリティ情報共有組織に関する調査

４．１．１　米国のセキュリティ情報共有組織

米国の主なセキュリティ情報共有組織としては、ISAC（Information Sharing and Analysis Center)、ISAO（Information Sharing and Analysis Organization)、CISCP（Cyber Information Sharing and Collaboration Program）が挙げられる。

ISACは分野ごとにセキュリティ情報を収集し、分析し、共有する組織のことで、1998年の大統領命令による要請を受け、重要インフラの分野ごとにセキュリティに関する情報を共有する目的で形成された。ISACは、セキュリティ情報共有コミュニティとして一定の成果を上げており、米国におけるISAC間の連携を図るための組織であるNCI（National Council of ISACs）には、2018年2月現在、20のISACが登録されている。

しかしながら、ISACが蓄積する情報は、内部では共有されるが、外部組織に共有されることは少ないことから、分野に所属しないセキュリティ関連組織や研究者、他分野の企業など、情報に関心のある者がISACから脅威や脆弱性の情報を得ることは難しくなっており、大局的な視点からのセキュリティ対策を行うことができないという課題がある。

こうしたISACの課題を受けて、重要インフラの分野にとらわれない自由な枠組みで情報収集・共有・分析を行うために、2015年の大統領令にて提唱されたものがISAOであり、ISAO SO（ISAO Standards Organization）により標準化された。ISAOでは、地域やイベント、特定の脆弱性など様々な要素を目的とした情報共有が行われる。

CISCPはNCCIC（National Cybersecurity and Communications Integration Center：米国国土安全保障省の内部組織)がハブとなり、参加組織から提供されたセキュリティ情報を分析し、参加組織間で共有する。対象分野などは絞っておらず、最新の情報を対象としている。

こうした組織を中心に、米国では積極的なサイバーセキュリティに関する情報共有が行われている。

（１）Aviation ISAC

Aviation ISACはボーイング社が中心となって航空業界を対象に2014年に設立された。設立時の参加組織数は7団体で、2016年5月には22団体が参加している。その内訳としては、旅客・貨物の航空事業者、空港、グループ企業含む関連事業者、メーカー、業界団体、サービスプロバイダー等が含まれる。事務局は2018年2月現在8名で運営されている。

活動としては、①音声通話やSMSテキスト、ツイッター、電子メール、及び情報共有プラットフォームを介した、航空機等のインシデントの兆候に関する緊急通知、②関連レポート、

ISAC に提供された脅威情報、メンバー及び政府から報告された早期警戒情報のリアルタイムの投稿・共有、③様々な情報機関の最新の脅威情報、指標、及び分析レポートを週 1 回発行、④インシデント中・後の緩和策[21]の確立、及び普及、⑤他分野の ISAC、民間セクター、ベンダー、政府と協力し分析を実施、となっている。特に①については、2014 年第 4 四半期には 106 の情報が共有されており、内訳は 2 つの TLP Red の情報、48 の TLP Amber の情報、43 の TLP Green の情報、13 の TLP White の情報となっている。また、STIX / TAXII と呼ばれる標準に基づく脅威情報が掲載される MITRE CRITS については、常に閲覧可能になっている。

会員は会費によって 3 つにランク分けされており、Aviation ISAC がランクを決定する。一番上の Platinum クラスは、年間売上が$20 億以上の企業を対象にしており、会費は年間$5 万となっている。Platinum クラスに加盟すると、ポータルへのアクセスアカウントが 20 個付与され、会合の参加は 7 名まで可能となり、その他の机上演習や訓練、WG など、Aviation ISAC が提供しているサービスを制限なく受けることができる。中間の Gold クラスは、年間売上が$20 億未満の企業を対象にしており、会費は年間$2.5 万となっている。ポータルへのアクセスアカウントは 5 個付与され、会合の参加は 5 名まで可能となり、その他の Aviation ISAC が提供しているサービスについては、NIAB と呼ばれるネットワークスキャンツールの利用やインシデント対応の補助に制限がある。一番下の Silver クラスは、サイバーセキュリティレベルが発展途上にある企業や業界団体を対象にしており、会費は年間$1 万で、ポータルへのアクセスアカウントは 1 個であり、演習など多くサービスへの参加が制限されている。

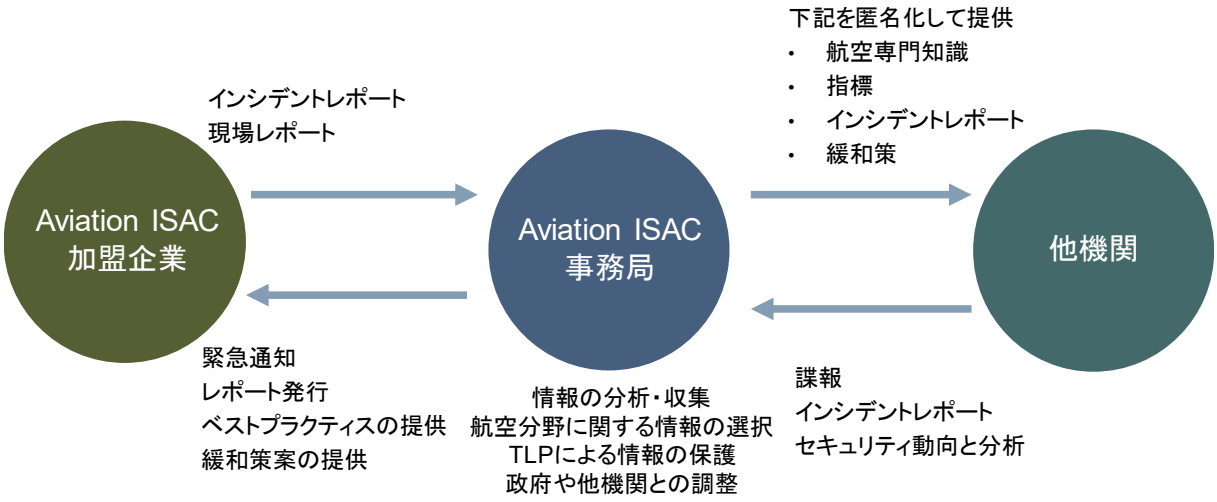


図　Aviation ISAC の情報共有内容

1）Aviation ISAC 秋総会

2017 年 11 月 8 日～10 日に Aviation ISAC の秋総会である、”2017 FALL SUMMIT “GLOBAL RESILIENCY ACROSS THE AVIATION COMMUNITY”が開催された。この秋総会は、Aviation ISAC がセキュリティベンダー、航空機メーカー、航空会社、空港関係等航空関連産業に関わるグローバルの関係者と密に関係を築くためのイベントであり、参加申込のプロモーションも積極的である。スピーカーの多くはイベントのスポンサー企業となっており、サイバーセキュ

[21] 脆弱性悪用の深刻度(悪用のされやすさ)を下げる可能性のある対策

リティに関する最新情報や解決策に関するプレゼンが中心となっている。自社製品の宣伝は禁止となっているが、航空関係者が一堂に会し、セキュリティに対する航空業界のニーズを具体的に把握できるとともに、セキュリティ動向及び一般的な対策方法に関して提示できるため、セキュリティベンダーにとって魅力的な総会となっている。次年度の会議のスポンサー申込が既に3件もある。

また、元ブルーエンジェル・パイロットによる自己啓発系のプレゼンや、ハッカー組織と実際に対峙しているエンジニアによるプレゼン等､聴衆受けするスピーカーも招待している。さらに、参加者の懇親を深めるために、長めのブレイクやクルーズ、プールサイドハッピーアワーなどネットワーク作りのための様々な工夫がされている。

表　Aviation ISAC 年次総会の概要

正式名称	2017 FALL SUMMIT “GLOBAL RESILIENCY ACROSS THE AVIATION COMMUNITY
日時	2017年11月8日～10日（8日はメンバー関係者のみによる机上演習等）
場所	ヒルトンホテル　マイアミ　ダウンタウン
主催	Aviation ISAC、IATA
スポンサー	プラチナ: IBM、ForeScout, Deloitte ゴールド: Anomali, SHAPE, CROWDSTRIKE, GOOD HARBOR シルバー: FLASHOINT, hackerone, pwc, Symantec

表　Aviation ISAC 年次総会のプログラム

開催日	題	概要
11月8日	What Does a Decade of Intelligence Lessons Learned Mean for Business Execution in 2020?	・IBM社Steve Stone氏によるプレゼン。Stone氏は米国空軍に勤務した経歴を持つ。IBMに勤め始めて7か月 ・IBMの今後3年間の計画を立てるにあたり、これまでの経緯、教訓、すべきこと、将来像について概観 ・911以降、軍ではテロリズムの専門だったが、そのときの経験がサイバーセキュリティ現場に有効 ・IBMは2020年までに1000億ドル規模の企業に急成長するが、その大部分はサイバーセキュリティ業務
	Featured Speaker: Amit Serper “Everything is Terrible and We Should All go Home and Think About It”	・ウクライナを中心として広がったランサムウェアNotPetyaに対するアンチウイルスを開発したセキュリティの研究者Amit Serper氏によるプレゼン。 ・イスラエル出身だが現在はボストンのサイバーセキュリティ会社に所属。以前は

		イスラエル政府のサイバー攻撃防衛を担当 ・Bug bounties、Bug bunnies, Bug cloud などハッカーに報酬を払って脆弱性を探させる業者は多数ある ・システムは常に最新状態に保ち、パッチは後回しにせず出たらすぐにインストールしておくことが重要
	Cyber Reconnaissance: Using Big Data to Reveal Hidden Cyber Exposures and Attackers within Your Network	・Anomali 社 Travis Farral 氏のプレゼン ・Threat Hunting とは、既にあるセキュリティツールや対策をすり抜ける侵入や感染、その他悪意のあるアクティビティの兆候を探索すること ・検知や予防のツールは未だに十分ではなく、アーチファクトをうまくとらえて検知に繋げるため、ハンターのスキルも重要である
11 月 9 日	The Good, the Bad and the Downright Dangerous: Connecting the Internet of Things to Aviation Networks and Infrastructure	・Fore Scout Technologies, Inc.の主席エンジニア Bob Reny 氏によるプレゼン ・デバイス全般に対するベースレベルのセキュリティ強化、プロセスの自動化、社内及び社外顧客との情報共有はどの組織にとっても課題 ・航空産業は、運輸と IT の大きなネットワークの融合という危険に直面している
	Are UAS the Ultimate Disruptive Technology? Mitigating Threats and Disruptive Technologies for a Globally Resilient Aviation Ecosystem	・National Aviation Intelligence Integration Office の局長補佐 Kenneth E. O’Neal 氏と航空サイバー分析官の Scott Simon 氏によるプレゼン ・無人航空機による新たなセキュリティの課題であるプライバシー侵害、テロ攻撃、空港における衝突の危険性等について解説 ・新たな脅威に対する対策と将来的な展望を提示
	KEYNOTE SPEAKER: JOHN FOLEY “The High Performance Climb”	・ブルーエンジェルスの元主席ソロパイロットによるプレゼン ・自己啓発的内容で観衆を喚起 ➢ プレッシャーの対処の仕方

		➢明確な目標設定、ビジョンとは何か ➢ハイパフォーマンスを達成するチームの作り方 ・サイバーセキュリティの情報共有も同じ側面
	PANEL: SOC It to ME! Creating an Effective SOC, Successful SOC Strategies, and How to Get the Most Out of Your Detection Capabilities	・モデレータは Acviation ISAC の Terrance Kirk オペレーションディレクター、パネリストは FedEX の Matthew House 主任テクニカル分析官、GE Aviation の Greg Seipelt インテリジェンス分析官、ボーイングの Philip Potts サイバー脅威インテリジェンス分析官 ・Aviation ISAC の主要メンバーによる高機能 SOC 構築のためのベストプラクティスと具体的な導入システムや製品に関するパネルディスカッション
	Using Threat Intelligence to Hunt for Hidden Threats	・Anomali 社の Travis Farral セキュリティ戦略ディレクターによるプレゼン ・Threat Hunting とは既にあるセキュリティツールや対策をすり抜ける侵入や感染、その他悪意のあるアクティビティの兆候を探索すること ・Threat Hunting には 43%もの誤検出が出るという難点もあり、30%は効果がない ・Threat Hunting に重要なのは、適切なデータ、ツール、スキル
	Combining Physical Security and Cyber Security to Build Resiliency	・ISTA の主席セキュリティアナリスト Necmiye Genc 女史によるプレゼン ・IP ベースのネットワーク技術により物理的セキュリティとサイバーセキュリティは統合的に取扱う必要性がある ・統合的システムは同時に単一過失点を生み出す可能性もあり、脅威やリスクを修正し、物理システムとサイバーシステムの所有の分け方に関する課題がある
11 月 10 日	Lessons Learned from Protecting 50% of America’s Passengers	・Shape Security の攻撃フォレンジクスのディレクターである Dan Woods 氏によるプレゼン ・航空チケット予約システムを対象とした

		攻撃に関して紹介 ➢ マイルサービスアカウントの乗っ取りと盗んだマイルの換金化 ➢ 料金のスクレイピング方法と検知にかかる時間 ➢ Web アプリケーションからモバイル API への標的の進化
	PANEL: IATA: Putting the Elation in Regulation!	・IATA の ITO ディレクター兼チーフインフォメーションオフィサーの Pascal Bucher 氏がモデレータとなり、エアバスの CSO である Pascal Andrei 氏、Aviage Systems のアプリケーションセキュリティリーダーである Mohammed Waheed 氏、GE Aviation の CISO 補佐兼テクノロジーリスク・セキュリティの VP である Laurie Seims 氏によるパネルディスカッション ・規制機関の現状の活動状況と今後の協力方法に関して議論
	Collaboration Between Government and Industry on Securing the ADS-B A/G Link	・Federal Aviation Administration NAS 情報セキュリティ・アドミニストレイターの Luci Holemans 女史、及び国防省の主任テクニカル・アドバイザーの Steven Hoffmann 氏、国防省 航空サイバーイニシアティブのプロジェクトマネージャーである W. Baird McNaught 氏によるプレゼン ・2020 年 1 月から導入される ADS-B 技術について紹介 ・航空業界が ADS-B を取扱うためのガイドラインや官民連携による情報共有プラットフォームの紹介

２）Aviation ISAC 事務局へのヒアリング

Aviation ISAC における情報共有の仕組みや運用時の工夫等を把握するために、Aviation ISAC 事務局の Jeff Troy, Executive Director、及び Aviation ISAC の理事である John A. Craig, P.E, Chief Engineer (ボーイング社) にヒアリングを行った。ヒアリングは Aviation ISAC 秋総会に合わせ、2017 年 11 月 9 日に実施した。ヒアリングで得られた結果は以下の通り。

①A-ISAC 立ち上げについて

Aviation ISAC は航空業界の 7 人の信頼できる仲間が中心となり設立された。ISAC の活動を行っていく中で信頼できる仲間が徐々に加わり、設立から 4 年経て、2017 年には 35 の会員が加盟している。航空業界自体が国際的な業界のため、Aviation ISAC では国際連携を非常に重視しており、カナダ、ヨーロッパ、オーストラリア、アジアから参加している会員がいる。また、IATA も主要な会員として参加している。航空機メーカーであるボーイング社は Aviation ISAC 設立当初から参加している。

政府機関は加盟しておらず、政府機関に対する報告義務も特にないが、パートナーとしてよい協力関係を築くことができている。また、セキュリティベンダーもメンバーではないが、会議やイベントを開催する際のスポンサーとして関与している。

各社が Aviation ISAC に加盟する動機としては、1 社だけの投資では得られないサイバーセキュリティに関する情報・対策方法・リスクを共有でいることや、リアルタイムでお互いの情報をやり取りできる結束の固さを理由として挙げている。

②情報共有の仕組み

Aviation ISAC 内の情報共有にあたっては関係者以外には情報が漏れないように配慮されている。また、発信者の情報も匿名化することができる。

情報共有プラットフォームには Anomali のシステムを導入し、メンバー各社の環境（セキュリティソフト、OS、ネットワーク機器等）に応じてログやインシデント情報、分析結果(インテリジェンス)、対応と対策情報を共有している。Anomali は Aviation ISAC が契約しているため、加盟企業は 2 アカウントが無料で使用可能となっている。

③運用実態

Aviation ISAC の運営費用は会費によって賄われており、会社の規模に応じて年間$5 万、$2.5 万、$1 万の 3 つのランクを設けている。会員から徴収した会費は運営費用の他に、会議の会場費用や、食事代、グッズ、イベント費用に充当している。

また、会費以外に GE やボーイングのように人員を無料で出向させてサポートしている企業もおり、2017 年現在、事務局は 7 人の専任スタッフから構成されている。

④運用時の工夫

ISAC の活動で一番大切なことは、信頼である。メンバー間の信頼関係を醸成するため懇親会やパーティを開催して親交を深める努力をしている。また、加盟企業の分析担当は年に 4 回集まり、机上演習を定期的に実施している。

Aviation ISAC 秋総会のように年に 1 回開催する大きな会議を開催し、航空業界に興味のあるベンダーに対してスポンサーとなるチャンスを与え、参加費用では賄えないようなコストを負担していただく仕組みを作っている。

インシデント情報の共有にあたり、セキュリティの専門家ではない担当者に対しては、物語形式にし、解説する工夫を行っている。

コアなメンバーによる解決策やベストプラクティスの情報共有により、1 社では解決が困難の問題に対する共有も積極的に展開されている。

一方で、こうした工夫や配慮にもかかわらず、会員が実際にインシデント被害にあっていたにも関わらず、情報を共有されないケースが5件あり、事務局が個別に問合せを行った。

⑤インシデントの情報共有例

WannaCryも含め、実際に被害にあったインシデントは机上演習で詳細な状況を共有している。机上演習には加盟企業の分析担当が出席するが、内容は非公開となっている。

（2）Surface Transportation, Public Transportation and Over-the-road Bus ISACS

Surface Transportation, Public Transportation and Over-the-road Bus ISACSは鉄道・バス・その他地上交通業界を対象に、2003年に設立された。ISAC内で鉄道分野とその他の地上交通分野に分かれ、それぞれAAR（Association of American Railroads)、APTA（American Public Transportation Association）の支援を受け、Information and Infrastructure Technologies,Inc.が運営を行っている。そのため、入会申込にはAPTAまたはABAの審査を受ける必要がある。

Surface Transportation, Public Transportation and Over-the-road Bus ISACSの主な活動は、鉄道・バス・その他地上交通に関するサイバー・物理セキュリティ情報の収集・分析・共有と、専門家によるインシデント対応コンサルティングとなっている。また、会員はTRIADと呼ばれるAPTA、AAR、TSAと共同で運用されている交通機関のセキュリティ情報ライブラリや、TRAIN と呼ばれる鉄道・バス・その他地上交通業界に関連するニュース及びインシデント情報を共有するサービスを利用できる。TRIAD では、テロ等の疑わしい活動や一般的なセキュリティ情報などが蓄積される。TRAIN では、Surface Transportation, Public Transportation and Over-the-road Bus ISACSを通じて、会員がインシデント情報を他の会員に共有することが可能となっている。

（3）その他のセキュリティ情報共有組織

代表的な米国のISAOとしては、以下が挙げられる。

表　代表的な米国のISAO[22]

名称	概要
Advanced Cyber Security Center	米国New Englandの大学・企業・政府機関等21団体が参加する非営利ISAO（Facebook, RSA, Harvard University, MITなど） 情報共有により、最先端のセキュリティ研究や教育プログラムの作成、セキュリティ政策の作成を遂行する
The National Cybersecurity Society	社員数499人以下の中小企業を対象とした非営利ISAO これまでISACの枠組みに入れなかった中小企業に対し、セキュリティ情報の提供や教育を実施している
The Trustworthy	デジタル広告のセキュリティ向上を目的としたISAO

[22] 参考：https://www.isao.org/information-sharing-groups/

Accountability Group	広告代理店の他、広告主や出版社、セキュリティベンダー、政府機関などが業種を超えてデジタル広告の不正排除、マルウェア防止などに取組む
Global Resilience Federation	FS-ISAC（金融）、Energy Analytic Security Exchange（エネルギー）、Legal services ISAO（法務）の3組織を運営するISAC・ISAOを束ねるISAOであるという点で特徴的
CyberUSA	各州に作られた官民パートナーシップ体制の集合体 2016年10月に7組織で結成され、オバマ政権下でサイバーセキュリティ顧問を務めたHoward A.Schmidt氏らが設立した財団により運営している
Information Association of Certified ISAOs	情報共有組織の立ち上げ・活動支援を行っている団体 国土安全保障省でISAOの枠組み作成に携わった者が設立した

ISAO SOより、ISAOの設立に関するガイドライン「ISAO 100-2: Guidelines for Establishing an Information Sharing and Analysis Organization (ISAO)」や、情報共有機能に関するガイドライン「ISAO 300-1: Introduction to Information Sharing」も発行されている。

「ISAO 100-2: Guidelines for Establishing an Information Sharing and Analysis Organization (ISAO)」では、ISAOの設立戦略に関する要素として、①ISAOの定義、②共有する情報の決定、③ISAOエコシステムでの役割の特定、④パートナー及び協力、⑤サービス及び機能の定義、⑥メンバーシップ基準の定義及び対象メンバーの特定、⑦有効性の評価、について検討事項が挙げられている。また、ISAOの運用計画に関する要素として、①ガバナンスモデルの確立、②ビジネスモデルの作成、に関する検討事項が挙げられている。また、信用できるコミュニティの構築に関する検討事項も記載されている。

「ISAO 300-1: Introduction to Information Sharing」では、ISAOにおける情報共有の基礎的事項として、情報共有の概念、共有する情報、情報の分析、アーキテクチャの検討事項運用上の検討事項、情報セキュリティとプライバシーについて説明されている。

４．１．２　欧州のセキュリティ情報共有組織

欧州の主なセキュリティ情報共有組織としては、ENISA（European Network and Information Security Agency：欧州ネットワーク情報セキュリティ庁)、EPCIP（European Programme for European Critical Infrastructure Protection）がある。また、一部の分野ではISACも存在しており(European FI-ISAC(金融分野)、EE-ISAC(電力分野))、航空分野においてはEU-Aviation ISAC(EA-ISAC)[23]が、また鉄道分野においてはEURail ISAC[24]の検討が進められている。

航空分野のサイバーセキュリティに関係する機関としては、EASA(European Aviation Safety Agency：欧州航空安全局）や、EUROCONTROL（European Organisation for the Safety of Air Navigation：欧州航空航法安全機構）がある。

（１）EA-ISAC

欧州版の航空分野におけるISACであるEA-ISACはENISAの発行するInformation Sharing and Analysis Center（ISACs）- Cooperative modelsの記載によると、設立済みとなっている。EUの規制の中で、事業者間での情報共有を実施する必要があり、その実現方式としてのISACという位置づけとなる。活動の実態等は、今後注目される。

（２）EURail ISAC

欧州における鉄道分野の ISAC は構想が打ち立てられているというのが現状である。“CyberSecurity4Rail” Railway Industry Conference (2017.10, ブリュッセル)という会議のクロージングのキーノートで “Achieving an EURail-ISAC, without replication or over-regulation...” という説明が、EUの研究プロジェクトであるShift2Railのエグゼクティブディレクターからなされた[25]。ST-ISACとの違い等、今後具体化される場合にはその詳細が注目される。

（３）その他のセキュリティ情報共有組織

ENISAはEUの機関であり、ヨーロッパにおけるセキュリティ情報収集・注意喚起、CSIRTの支援、教育活動、各国の政策立案支援などを行う。EU各国のセキュリティ政策の現状を調査し、公開しており、欧州の情報共有組織に関する調査も報告されている。

EPCIPはエネルギー、交通・運輸、金融の保護を目的として、2006年に欧州委員会で策定された重要インフラ保護プログラムである。エネルギー分野では TNCEIP を介した情報共有が開始されている。

EASAは EUの民間航空機産業の安全に関する規制機関で2002年7月に設立された。2016年11月には”High level meeting Cybersecurity in civil aviation”がブカレストで行

[23] https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models/at_download/fullReport

[24] https://www.hitrail.com/events/cyber-security-for-railways-conference-2017/conference-report-17

[25] 参考：https://www.hitrail.com/events/cyber-security-for-railways-conference-2017/conference-report-17

われ、今後の EU の民間航空機産業におけるサイバーセキュリティに関して、以下の目標が示された。

・連携機関の設立・・・・・・European Strategic Coordination Platform の設立・整備
・情報共有と報告の促進・・・航空業界（EA-ISAC）と EASA（ECCSA）の両方での取組が必要
・規制の整備・・・・・・・・競争とリスク管理のバランスをとる規制が必要
・リスク評価方法の確立・・・共通の用語及びリスク評価手法の開発が必要
・サイバーセキュリティの推進・・・全ての関係者がサイバーセキュリティの概念を共有していることが必要
・研究活動の継続・・・・・・安全性と迅速性のジレンマに対する解決策等のサイバーセキュリティに関する研究活動の継続
・コミットメント・・・・・・規制当局・事業者・サービスプロバイダー・メーカー間のパートナーシップ憲章の調印、及び航空分野におけるサイバーセキュリティ戦略の採択が必要

2017 年 2 月には、EASA と CERT-EU が ECCSA （European Centre for Cyber Security in Aviation)の設置に関する相互協力覚書に調印している。このセンターは、欧州の航空製造業者、エアライン、整備業者、ナビゲーションサービス等に対して、重要システムを保護するための情報提供や支援を行うことを目的とする。また、2017 年 5 月には、ブリュッセルにおいて”Workshop on Cybersecurity in Aviation” が開催され、将来の規制や標準化について産業界、航空企業、加盟国、EU 機関、学術機関等を集めて議論が行われた。

EUROCONTROL は 41 か国による国際機関で、EU における安全、効率的、環境に配慮した航法を支援する。2017 年 3 月には“SWIM cybersecurity Hints & Tips”という、次世代 ATM を実現するための情報共有システムである「SWIM[26]」の実施にあたって、考慮すべきサイバーセキュリティ事項を整理したパンフレットを発行している。このパンフレットでは各シチュエーションにおいて、サイバーセキュリティのガイダンスと参照すべき NIST、ISO の標準が示されている。

また、SITA（Société International de Télécommunications Aéronautiques：国際航空通信共同体）という、世界の航空会社や旅行代理店、その他の関連業界のための業界団体もあり、SITA と Airbus が共同で CyberSecurity Aviation Security Operations Center（SOC）を設立している。2017 年には Community Cyber Threat Center（CCTC)も設立し、インシデント情報のコントロールだけではなく、状況に即した脅威関連情報のメンバー間によるタイムリーな交換を促進することにより、コミュニティ全体の対応を支援することを目的とする。CCTC では以下を提供する。

・情報交換及び連携を目的とした非公開のフォーラムの開催
・個々のメンバーにカスタマイズしたアラートの提供
・セキュリティに関する週報の発行

[26] System Wide Information Management。空港内における航空機及び空港サービスに関連する全ての事業者が相互に情報交換できるシステム。ICAO が提唱する「統一的な運用を目指した世界規模の ATM システム」を構築するための 4 つの改善分野のうちのひとつ、「全世界レベルで統一されたシステム及び情報交換」において必要とされている。

・定期的な会合の実施
・支援若しくは連携を目的としたメンバー登録簿の利用

SITA の 2016 年航空業界 IT 動向調査[27]によると、今後 3 年間に 9%の航空会社がサイバーセキュリティに投資する予定であり、調査対象の 200 社のうち 72%が既にサイバーセキュリティプロジェクトに投資している。

[27] 2016 Airline IT Trends Survey

４．２　リオデジャネイロ・ロンドン五輪での取組みに関する調査

４．２．１　リオデジャネイロ五輪

リオデジャネイロ五輪におけるサイバー攻撃の実態や取組みを把握するために、リオデジャネイロ五輪のオフィシャルサプライヤーである ISDS 社(International Security & Defence Systems Ltd.)にヒアリングを行った。ヒアリングは 2017 年 12 月 10 日に実施した。ヒアリングで得られた結果は以下の通り。

（１）サイバー攻撃の実態

実際に問題があった件数については具体的な数字はない。コンピューターシステムに直接攻撃された事例は少なく、チケット詐欺など偽サイトを作るサイバー攻撃が多かった。また、そのような攻撃については、地元自治体と協力して住民にアラートを流したため、被害を防ぐことができた。

（２）情報共有に関する取決め

情報共有に関する取決めはされていなかったが、セキュリティ情報を提供する際に、具体的な対策についても提供することで、対策の実施が迅速に進んだ。

（３）情報公開

インテリジェンスによって得た全ての情報を公開しているわけではない。オリンピックの数か月前から情報収集活動し、政府に対し調査報告した後に、政府とともに情報の公開・非公開を決定した。公開は政府側が主体となって行った。

（４）教育プログラム

リオデジャネイロ五輪に向けて数万人を対象に、ミッションごとにグループ分けしトレーニングを行った。例えば、制御システムのオペレーターに対してはサイバーセキュリティの注意喚起をするとともに、USB が機能しない理由を特定する必要がある状況や、IP カメラを更改する際には、MAC アドレス認証の設定を管理者に変更してもらう必要がある状況等を体験させた。それぞれのレベルに合わせたトレーニングが重要である。時間もかかり、大変ではあったが、効果はあった。

４．２．２　ロンドン五輪

ロンドンオリンピック(2012)の際には、英国の官民情報共有機能である The Cyber Information Sharing Partnership (CISP)の前身による情報共有が行われた。オリンピックの際の輸送対策に奏功したとされる当時は、160 の官民組織による情報共有がなされた[28]。

[28] 参考：https://www.gov.uk/government/speeches/cyber-security-information-sharing-programme

４．３　第４章まとめ

本章では、今後の我が国のセキュリティ情報共有組織の在り方を検討するために、セキュリティ情報の共有体制が進んでいる諸外国のセキュリティ情報組織の実態を調査した。

調査対象としては、米国、欧州の鉄道・航空分野における情報共有組織を中心とした。特に米国を中心とした航空分野における Aviation-ISAC についてはヒアリング調査を実施した。

調査項目としては、情報共有組織の活動の事例、及び運用上の課題を中心とした。

鉄道・航空分野における情報共有は、米国では Aviation ISAC や Surface Transportation, Public Transportation and Over-the-road Bus ISACS による活動が先行事例として挙げられる。

Aviation ISAC は航空業界の信頼できる数人の仲間が中心となり設立され、2017 年現在では 35 の会員が所属している。Aviation ISAC の会員は、旅客・貨物の航空事業者、空港、グループ企業含む関連事業者、メーカー、業界団体、サービスプロバイダー等、多様な関連業界からなり、情報共有及び、対策の確立・普及、ISAC 外の組織とも協力した情報の分析を行っている点で特徴的である。

また、Aviation ISAC では信頼関係の醸成を重要視しており、年次のイベントや定期的な WG の開催等によって会員間の親交を深める努力をしている。そのような取組みの結果、航空関連事業者の目には、1 社だけの投資では得られないサイバーセキュリティに関する情報・対策方法・リスクを共有でいることや、リアルタイムでお互いの情報をやり取りできる結束の固さが魅力的に映り、Aviation ISAC の加盟が進む好循環が生まれている。

Aviation ISAC のイベントのスピーカーの多くはイベントのスポンサー企業（セキュリティベンダー等）である。航空関係者が一堂に会し、セキュリティに対する航空業界のニーズを具体的に把握できるとともに、セキュリティ動向及び一般的な対策方法に関して提示できるため、セキュリティベンダーにとって魅力的な総会となっている。今後の我が国のセキュリティ情報共有組織におけるスポンサー収入の確保方法として参考となると考えられる。

Surface Transportation, Public Transportation and Over-the-road Bus ISACS では、情報共有の他、専門家によるインシデント対応コンサルティングも行っている点で特徴的である。また会員は APTA、AAR、TSA と共同で運用されている交通機関のセキュリティ情報ライブラリを利用することができる。

Aviation ISAC と Surface Transportation, Public Transportation and Over-the-road Bus ISACS ともに、情報共有には、情報共有プラットフォームが利用されている。Aviation ISAC では、メンバー各社の環境（セキュリティソフト、OS、ネットワーク機器等）に応じてログやインシデント情報、分析結果(インテリジェンス)、対応と対策情報を共有している。

一方、欧州でも鉄道・航空分野における ISAC が EU の規制の流れの中で構築されつつある。鉄道・航空事業者が国の規制を受ける点で日本国内の鉄道・航空分野に近い面もあり、今後の動きや活動内容については参考にすべきといえる。

また、リオデジャネイロ五輪でのサイバー攻撃の実態や取組みについて調査し、2020 東京五輪に向けて情報共有組織のベストプラクティスを把握した。

リオデジャネイロ五輪のオフィシャルサプライヤーである ISDS 社(International Security & Defence Systems Ltd.)にヒアリングを行ったところ、リオデジャネイロ五輪を契機としたサイバー攻撃では、コンピューターシステムに直接攻撃された事例は少なく、偽サイトを作るサイバー攻撃が多かったとの回答を得た。また、そのような攻撃については、地元自治体と協力して住民にアラートを流すことで、被害を防ぐことができた。また、リオデジャネイロ五輪に向けて数万人を対象にトレーニングを行い、効果があった。2020 東京五輪に向けて、参考になる取組みと考える。

第５章　鉄道、航空 ISAC の実現に向けた検討

日本国内の鉄道分野・航空分野における ISAC 構築に向けて、ISAC の機能や運用方法について調査し、第２章～第４章で調査した結果と合わせ、ISAC の検討を行う。

５．１　ISAC のあるべき姿に関する調査

５．１．１　NIST 発行　SP800-150　“Guide to Cyber Threat Information Sharing”

NIST（National Institute of Standards and Technology：米国国立基準技術研究所）は科学技術分野における計測と標準に関する研究を行う米国商務省に属する政府機関で、NIST が発行する SP800 シリーズではコンピューターセキュリティに関する調査及びガイドを提供している。

SP800-150 “Guide to Cyber Threat Information Sharing”は脅威情報の共有関係を確立するためのガイドラインである。SP800-150 では、情報共有の利点として、①1 組織での検出が、情報共有組織のセキュリティ向上に繋がる、②各組織のセキュリティ対策を情報共有により強化することができ、枠組み全体のセキュリティ向上に繋がる、③一見無関係な情報を組み合わせることで新たな知見を得られる、④攻撃者の TTP（戦術（tactics）、技術（techniques）、手順（procedures））の進化に、より早く対応することができ、攻撃成功確率を下げることができる、⑤同タイプのシステムや情報を対象とした組織的な攻撃に対抗することができる、としている。

情報共有を行う場合の取組要件と内容として、以下が挙げられている。

表　情報共有にあたっての取組要件と内容

取組要件	内容
信頼関係の確立	定期的な会議、SNS 等で関係を維持する必要がある
情報の相互運用性と自動化の確立	共有する情報の形式の標準化と自動化により、共有を高速化する
機密情報の保護	各組織において、損失や契約違反に繋がる情報（個人情報等）の取扱手順を定め、不正な情報開示を避ける
政府機関からの情報の保護	政府機関からの機密情報を継続的に入手するには認定を受け、外国籍職員のアクセスを禁止する
情報の受信・提供方法の選択	ツール・人員の処理能力及び情報量の観点からどのように情報共有を行うかについて、慎重に検討する
外部情報へのアクセス	外部情報を取得するためのツールと、取得した情報を意思決定に利用するプロセスを用意する
情報の品質評価	情報の質、関連性、適用時を評価する

法的・組織的要件の遵守	法律上あるいはプライバシー上、あるいはビジネス上の要件に従って提供する情報の種類や技術詳細レベルを制限する。ただし過度な情報制限は情報共有に悪影響を与える
発信者帰属の制限	発信者を匿名化する。ただし匿名化することでリスクは低下するが、信頼性も低下する

５．１．２ ENISA 発行 “Information Sharing and Analysis Centres (ISACs) Cooperative models”

ENISAが発行する“Information Sharing and Analysis Centres(ISACs)Cooperative models”は、①EU 内にある各 ISAC の状況を調査し、ISAC をすること、②ISAC の設立と運営の過程で、官民が直面している課題を洗い出すこと、③EU における更なる ISAC 発展のための方策を提案すること、④EU 全体の ISAC 設立に関する ENISA の潜在的役割を調査すること、を目的としたレポートである。

“Information Sharing and Analysis Centres (ISACs) Cooperative models”では、ISAC が抱えている課題として、以下が挙げられている。

表　ISAC の課題

人員の不足
分析機能の弱さ
資金の不足
ISAC 活動の定量評価の難しさ
情報の重複
ISAC 間での協力
監督官庁とセキュリティ専業会社の役割
共有のための IT ツール

これらの課題を受けて、以下の ISAC の役割を引き出すための推奨事項が提示されている。

① ISAC 参加者

・適切なレベルでの情報共有を行うための、信頼関係を築くための努力する

・委任規約と行動規範へ同意する

② 事務局

・ISAC 参加者がある程度同じレベルの視点・知識から議論できるよう、対象とする役職を適切に設定する（技術者、経営者、弁護士を同じ会議に出席させない）

③ ISAC の機能

・ISAC は民間分野からの参加を促す仕組みを持つ

・ISAC は公的機関も、事務局または ISAC 活動のパートナーとして関与できる仕組みを持つ

・情報共有には TLP を利用するとよい

・国家の安全や公安に関係する情報等、強制的な情報共有が必要とされるような特定の状況を認める

・設立当初から資金調達メカニズムを確保する

・分野を跨いだ ISAC の協力関係に注力する

・定期的な成果報告を実施する
・定期的な評価を実施する
・メンバーのニーズに基づく新しいサービスを開発する
・法執行機関と連携することでサイバー犯罪に対抗する機会が可能になり、新しい脅威に関する情報を入手できる可能性がある。

５．２　ISAC のあるべき姿の提言

第２章～第４章で調査した国内外のセキュリティ情報共有組織での情報共有の現状･ニーズ･課題と、５．１章で調査した NIST と ENISA から発行されている情報共有組織に関する文献で提言されている情報共有にあたっての課題を踏まえ、鉄道及び航空分野における ISAC の要件を整理する。

５．２．１　ISAC 構築時に予め協議すべき事項

（１）情報共有の目的の定義

ISAC の構築を検討するにあたり、限られたリソース[29]の中でより重要かつ有用な情報共有を行うために、情報共有の目的を定める。情報共有の目的や ISAC の機能を検討する際は、事業者が ISAC に参加する利点についても考慮する必要がある。

金融 ISAC は日本の金融機関の間でサイバーセキュリティに関する情報の共有・分析、及び安全性の向上のための協働活動を行い、金融サービス利用者の安心・安全を継続的に確保すること、ICT-ISAC はネットワークのセキュリティ確保のために幅広い分野の事業者と協力すること、電力 ISAC は事業者間で脅威情報等を共有し、適切かつ迅速に対応できるような仕組みを構築することを目的として設立されている。

また、国内の既存の ISAC に事業者が加盟する理由としては、「同じ攻撃者から攻撃されることが多いため、民間企業で団結し対策をとることが有効であること」、「他社の障害が自社の障害となりうること」、「ISAC の会員リストに自社名が載っていることのステータス（セキュリティベンダー等)」「ガイドラインの検討の場に入ることで、自社の実情をガイドラインに反映できること」、「いち早く情報を手に入れることができること」、「他の企業の取組みを参考にできること」、「業界全体の対策レベルが上がること」が挙げられている。

鉄道分野では、IT 分野・運輸分野の横断的な情報共有の促進や加盟企業の相互協力による効率的な対策の構築を目的とすることで、各事業者におけるセキュリティ対策強化という利点を提供することが可能と考えられる。

航空分野では、1 社が攻撃を受け営業が困難になった場合、管制や空港運営に影響を及ぼし、他の事業者まで影響が拡大する可能性がある。そのため、ISAC を構築する際は、業界全体のセキュリティレベルの向上を目的とすることで、自社の障害に繋がるような他社の障害を防ぐという利点を提供することが可能と考えられる。

（２）共有する情報と情報源を決定

情報共有を行うためには共有する情報と、その情報の入手先（情報源）を特定することが重要となる。

セキュリティ情報共有組織で共有される情報としては、脆弱性情報やインジケータ、脅威情報等となっている場合が多い。また、情報の入手先は、主に政府機関や会員となっている場合が多い。

[29] 人・物・金銭・時間等の経営資源

会員から得られない情報については、外部情報源を利用することも検討するとよい。例えば、海外からの情報を入手し共有するための方法として、同じ分野の諸外国の ISAC との連携、事務局による国際会議への参加、海外のコンサルティング会社を利用した情報収集等が挙げられる。

２．３章で行ったアンケート調査結果によると、鉄道・航空事業者では、導入されている機器等に対する情報（インジケータや侵入検知シグネチャ等）、人的対応に対する情報（脅威情報等）、ルーター設定・ファイアウォール規則・Web フィルタ設定等の具体的対策について、事業者内や取引関係にあるベンダーで情報が共有されていることがわかった。一方で、具体的対策は機器等に対する情報や人的対応に対する情報に比べ、それほど共有されていないこともわかった。

鉄道及び航空分野で ISAC を構築する場合は、上記の情報を中心に共有を始め、事業者のニーズに応じて共有する情報の種類を追加することがよいと考えられる。特に、具体的対策を共有することで、会員が容易に対策を実行可能となることから、具体的な対策を共有することが望ましい。

また、今回のアンケート調査結果から、鉄道・航空事業者は ISAC に対し、サイバー攻撃に関する情報を共有することだけではなく、インシデント対応演習や人材育成の方法を共有すること、システム共通の安全対策を検討すること等も期待していることがわかった。後述の「５．２．２章（２）ISAC を活性化するための活動」と併せ、社内でのインシデント対応方法と訓練、人材育成、安全対策等のマネジメントにかかる情報についても共有することで、鉄道及び航空分野における ISAC の活動が、鉄道・航空事業者にとってより有用なものになると考えられる。

（３）情報共有規則の確立

情報共有を始める前に、情報共有規則を確立することが必要である。情報共有規則を定める場合、情報の受信者の信頼性、情報の機密性、共有することによる潜在的影響等を考慮する必要がある。

１）共有可能な情報のリストアップ

共有可能な情報をポータルサイト等でリストアップすることにより、会員から必要な情報を特定しやすいようにする。

２）情報共有の手段と方法の決定

情報共有の手段についても検討する必要がある。

日本国内におけるセキュリティ情報共有組織では、情報共有の手段として基本的にメールを利用しているが、金融 ISAC や米国の Aviation ISAC、Surface Transportation, Public Transportation and Over-the-road Bus ISACS では情報共有ポータルが利用されている。ポータルを利用することで、インシデント情報とその関連情報やガイドライン等のドキュメント類の情報を蓄積することが可能となる。また、共有された情報に対する他会員からの質問（双方向）が容易となるなどのメリットあるため、情報共有ポータルを利用することが望ましい。

情報共有ポータルでは、会員の登録を会社名ではなく担当者名で行い、本人の希望により顔写真の掲載も可能にすることで、顔の見える化による安心感を提供することが可能となる。また、共有フォーマットは加盟企業内のツールと互換性があるとよい。尚、情報提供の際の匿名化については、「３)情報提供者の匿名化するか否かのオプション付与」を参照されたい。

また、セキュリティ情報共有組織内における情報共有の方法として、ISAC 全体に脅威情報を共有するのか、関係する組織で WG 等を組み、その中で情報を展開するかについて検討する必要がある。また、鉄道及び航空分野で ISAC を構築する場合は業界が異なるため、鉄道分野・航空分野それぞれにおいて、業界特有の情報について共有する WG の立ち上げを検討する必要がある。

３）情報提供者の匿名化するか否かのオプション付与

情報提供者の保護のため、情報提供の際には本人の希望により匿名化を可能とすることが望ましい。

また、情報提供者の匿名化を行うことで、情報提供への心理的障壁を軽減する効果が見込まれる。

金融 ISAC では、情報共有にポータルを利用しており、情報提供者が TLP 等と併せて、提供者名を匿名化するか否かを選択することが可能となっている。

４）情報共有が許可される条件の明文化

情報共有の範囲（展開先）とその条件（情報の共有が許可される情報の種類、状況）を TLP 分類として明文化する必要がある。

情報共有の範囲とその条件を定める場合は、会員が持っていない情報が適切に共有され、必要な情報が適切な範囲に提供されるように考慮することが必要である。情報提供範囲を過度に制限することにより、共有された情報に基づく対策の実行が不可能となる場合がある。また一方で、情報提供範囲が適切に定められていない場合、把握できない範囲まで情報が流出してしまうことに対し、情報提供者が不安を抱くことになり、情報共有が進まないことになる。

実際に情報共有する場合は、共有する情報に TLP を付与し、機密性の高い情報については情報の公開・配布を制御することで、不適切な情報開示を抑制することができる。これにより、組織・顧客等へ悪影響を及ぼす可能性のある情報の拡散を防ぐことが可能となる。TLP によって会員外へ情報展開が可能な場合であっても NDA を締結することが望ましい。

また、一方で機密性が低い情報については、外部への公開を可能にすることで、他分野の ISAC、民間セクター、ベンダー、政府と協力し分析を実施することができ、分野にとらわれない大局的な視点や、外部の組織における知識や経験からのセキュリティ対策を行うことが可能となる。

金融 ISAC、Aviation ISAC 等では共有する情報に TLP を付与している。

鉄道及び航空分野における ISAC 構築を検討する場合は、以下のような TLP を付与することが望まれる。

表　望ましいTLP分類[30]

TLP区分	会員活動上の情報の取扱い	会員各社における情報の取扱い
Red/赤	特定のグループ（会議参加者等）の受信者のみとし、当該グループ外への転送を禁ずる	必要最小限の範囲内で共有することができる
Amber/黄	ISAC会員限りで共有する	発信者情報を適切に削除等した上で、必要に応じて、会員個社及びグループ子会社内で共有することができる
Green/緑	ISAC 会員及び予め定める業界団体等の外部組織との共有を行うことが可能	発信者情報を適切に削除等した上で、必要に応じて、Amber/黄で定められた共有範囲に加え、情報セキュリティ、物理セキュリティ対応に関連する外部委託先を含めた範囲で共有することができる
White/白	公知の情報として扱う ※著作権法その他の法令を遵守する	常識的な範囲で共有することができる

５）情報の修正・消去のための要件の明文化

共有される情報の信頼性確保のために、情報提供者の同意なしに情報の修正・消去ができないようにする必要がある。

ただし、誤った情報を提供された場合に事務局による情報の修正・消去が可能となる規則を定める必要がある。

６）免責

ISACで共有された情報に基づく損失については重過失並びに故意の場合を除いてISAC及び会員は責任を負わないと定める必要がある。

また、加盟企業の法務担当者、情報管理者等は、情報共有規則がそれぞれの会員組織の内部規則と合致するか確認する必要がある。

共有規則は、法令の改正、それぞれの組織の内部規則の改正、新規情報源の導入、リスク許容度の変化、情報の所有権の変更、脅威環境の変化、ISACの合併等の実施に合わせて、定期的に再評価する必要がある。

（４）会員制度の制定

セキュリティ情報を共有するために、会員制度を制定する必要がある。会員制度として検討すべき要件は以下の通りとなる。

[30] 参考：Traffic Light Protocol (TLP) https://www.first.org/tlp/ 及びヒアリングに基づき作成

１）資格要件

ISAC の会員の資格要件を定める。資格要件を定めるにあたり、以下を考慮するとよい。

① 対象事業分野（鉄道及び航空サービスを支える事業を含む）
② 各事業者のグループ企業、ベンダーやセキュリティベンダー、サービスプロバイダー、業界団体の参加可否
③ 外国資本の事業者や業界団体等の参加可否

国内の既存の ISAC の参加条件としては、金融 ISAC、ICT-ISAC ともにベンダーも参加可能となっている。

また、Aviation ISAC では旅客・貨物の航空事業者、空港、グループ企業含む関連事業者、メーカー、業界団体、サービスプロバイダー等も会員に含まれる。

アンケート調査結果から、鉄道・航空事業者はシステムの不具合情報等について、ベンダーと密接に情報共有をしていることが判明しているため、鉄道・航空分野における ISAC 構築に向けた検討を行う際には、各分野の事業者だけではなくベンダーも巻き込むことが重要と考えられる。ベンダーの参加にあたっては、正会員とするのか、ベンダー会員枠（共有される情報や提供されるサービスを制限）を設けるのか検討が必要である。また、対象となるベンダーの参加資格（事業者と取引関係のあるベンダーに限定するのか、あるいは特段の制限を設けない等）についても検討が必要である。

２）担当者に求められる能力

加盟企業の窓口となる担当者の要件を定める必要がある。ISAC 内で共有される情報が事業者の内部で適切な部署に提供され、対策が実施されるために、窓口となる担当者は IT・運輸両方のシステムをある程度理解していることが望ましい。

IT・運輸両方のシステムを理解している人材が不足している場合は、WG の内容に応じて関連部署の担当が出席可能とするなど、柔軟な参加を可能とするとよい。

３）会費

ISAC の財政基盤の安定化、ISAC の活動内容や会員特典とそれに対する会員のコスト意識などを考慮し会費を設定する必要がある。

国内の既存の ISAC では、サービス内容や事業者の規模別に会員クラスを設定し、会員クラスに応じた会費を徴収している。その額は年間数十万～数百万となっている。鉄道及び航空分野で ISAC を構築する際も、この金額が参考になると考えられる。

４）スポンサー制度

ISAC の財政基盤の安定化のために、スポンサー制度の導入を検討するとよい。

会費だけで運営資金を賄うことができていない ISAC もあり、鉄道及び航空分野で ISAC を構築する場合も同様の課題が顕在化する可能性がある。スポンサー制度を導入し、会費だけではなく、スポンサー収入も得ることで、ISAC の財政基盤が安定すると考えられる。スポンサーの候補であるセキュリティベンダー等にとっても、ISAC は事業者等関係者が一堂に会し、ベンダーの技術力、商品の魅力を示す絶好の機会である。

スポンサーの参加方法としては、スポンサー会員の枠を設け、参加してもらう方法、若しくは会議やイベントを開催する際のスポンサーとして関与する方法がある。Aviation IAC では後者の方法を選択している。一方で金融 ISAC では、アフィリエイト会員として、セキュリティベンダーに参加してもらい、WS 等での講演を可能にしている。

スポンサーが参加することによる影響が不透明であること、スポンサー会員の枠を ISAC 構築時から設けることは検討のハードルが高いこともあるため、まずは、会議やイベントを開催する際のスポンサーとして関与する形式にすることが望ましい。

（５）事務局の決定

（１）～（４）で検討した情報共有組織のスムーズな運営のために事務局の体制を検討する。

鉄道及び航空分野で ISAC を構築する際に、事務局に必要とされる能力として、鉄道及び航空分野のシステムのセキュリティ情報を扱い、共有される情報の取捨選択や重要度、ISAC としての対応方法を判断するための、IT・運輸両方の知識を持っていることが望ましい。また、セキュリティ情報には機微な情報も含まれるため、会員から信頼されることが必要となる。

上記の必要な能力を踏まえ、事務局の設置方法を検討する。事務局の設置方法としては、各社から出向者を募り事務局を新たに設立する場合と、既存の業界団体が事務局を担う場合が考えられる。事務局を新たに設立した事例としては、Aviation ISAC ではボーイング社が中心となって数人の仲間が集まり、事務局兼会員として立ち上げた。既存の業界団体が事務局を担っている事例としては、航空分野における CEPTOAR と鉄道 CEPTOAR が挙げられる。ただし、この場合、事務局が IT の専門家ではないため情報の判断に迷う場合があるという課題が挙げられている。また、電力 ISAC では、事務局を業界団体である電気事業連合会が担うことで、同連合会の各社とのハブ機能によって培われてきた信頼関係により、スムーズな情報共有を行っている。また、電気事業連合会には各社から IT 部門の担当者が出向しており、IT 分野の知識も十分にあるため、システムのセキュリティ情報の取扱いがスムーズとなっている。

鉄道及び航空分野で ISAC を構築する際には、事務局を新たに設立する場合と、既存の業界団体が事務局を担う場合の双方の長所と短所を考慮し、決定することが望ましい。また、事務局は鉄道及び航空分野のシステムのセキュリティ情報を扱うことになるため、事務局を担う業界団体は、事業者の IT・運輸部門からの出向者、若しくは過去に事業者の IT・運輸部門に在籍していた経験者など、鉄道及び航空分野のシステムのセキュリティ情報に詳しい人物が含まれることが望ましい。さらに、事務局の技術力を向上させるため、ベンダー企業からの出向者を配することも考えられる。

事務局の人数としては、多くのセキュリティ情報共有組織で数名程度であり、鉄道及び航空分野で ISAC を構築する際も、この数字が参考となる。また、広範囲に重篤な攻撃が発生している場合を除き、事務局の運営は 24 時間体制である必要はないが、夜間の緊急連絡対応として、情報共有ポータルの投稿を担当者ベースで実施することが望まれる。

事務局では、法務担当者や情報の収集、保管、公開、保護等に関わるプライバシー情報担当者を任命し、主要利害関係者（理事会、監事、顧問、事務局等）を開示し、加盟企業からの承認を受ける必要がある。

５．２．２　ISACの機能として検討すべき事項

（１）情報分析の実施

情報分析について、具体的に誰が、どのような分析を担うかについて検討する必要がある。

Surface Transportation, Public Transportation and Over-the-road Bus ISACSでは、APTA、AAR、TSAが分析したテロ等の疑わしい活動や一般的なセキュリティ情報を会員が利用できるようになっている。また、攻撃等について各社での対応や影響について報告・分析に力を入れるISACや、事務局の有識者等による分析を適宜実施するISACもある。情報の分析が十分にできていないISACでは、分析された情報を迅速に収集する例や、分析機能の外部委託が検討されている例もある。

さらに、ISDS社へのヒアリングでは、セキュリティ情報を提供する際に、具体的な対策についても提供することの必要性が指摘された。

鉄道及び航空分野で ISAC を構築する場合も事務局の分析能力が懸念される。そのため、JPCERT/CC等の脆弱性関連情報の調整機関や国外のISACで分析された情報の収集やセキュリティベンダーに情報分析を委ねることなどが考えられる。セキュリティベンダーに情報分析を委ねる場合、業界に対するベンダーの理解向上が必要となると考えられる。

（２）ISACを活性化するための活動

ISACの情報共有を活性化するための活動を実施する必要がある。

会員同士の情報共有の場を構築するだけでは、活発な情報共有は行われない可能性がある。その理由の一つに、情報共有のサイクルが醸成されていない状態で情報を提供することに対し、会員がメリットを感じられないことが挙げられる。ある会員が情報提供を行ったのにも関わらず、それに対する他の会員からのレスポンスや新たな知見が得られない場合、情報提供を行った会員の立場としては、情報を吸い取られるのみで、得るものがない形になる。情報共有のサイクルを始めるためには、最初に情報提供を行う会員が必要であり、会員に対し協力を呼びかけることが必要となる。また、継続的に会員が情報提供を行うモチベーションを保つためにも、提供された情報に対して受信者との双方向の議論を可能にする等、フィードバックの質を高めることが重要である。

また、情報共有以外の活動を実施し、ISACへの参加意識を高めることも重要である。活動にあたっては、適宜アンケートやWG等で事業者のニーズを把握し、適切な活動を検討・提供することが望まれる。

ISACの活動例としては、以下が挙げられる。

・年次総会やWG等の会合開催

会合を開催し、情報を交換する機会を提供することで会員間の信頼関係を醸成することができる。親睦を促進するために、ISAC 事務局より懇親の場の提供をすることも有効である。

また、年次総会など大きな会合において、スポンサー枠などを設けることにより、スポンサー収入を得ることで財政基盤の強化に繋がる。スポンサー企業にとってISACの会合は、ユーザーとなる事業者等が一堂に会すことから、セキュリティベンダーの技術力、商品の魅力を示す絶好の機会となるだけでなく、事業者のセキュリティニーズを具体的に把握できるな

どのメリットがある。

・ガイドラインの作成

加盟企業が業界のガイドラインを作成する際に、検討の経緯から参画できる他、各社の要望などを反映させることができる点で、ISAC に加盟へのインセンティブとなる。作成するガイドラインの例としてはマルウェア等の対策集や脆弱性評価方法、グッドプラクティスガイドなどが挙げられる。

・インシデント・脆弱性情報以外の情報を提供

インシデント・脆弱性情報以外の情報提供としてメールマガジンによる情報提供も有効である。その内容としては、有識者のリレー投稿やアナリストのコラム、国内外のカンファレンスのまとめなどが考えられる。

・教育プログラム

演習やスキルアップ講座を開催することも ISAC の活動として考えられる。国内の既存の ISAC では、情報共有の更なる推進のために加盟企業全体のセキュリティ対策のボトムアップが課題となっている例もあることから、鉄道及び航空分野で ISAC を構築する場合も同様の課題が顕在化する可能性がある。演習やスキルアップ講座を開催することで、会員のセキュリティレベルを向上させることが重要である。また、今回のアンケート調査結果から、鉄道・航空事業者は ISAC に対してインシデント対応演習、人材育成に期待していることが把握されている。

・コンサルティング

事務局やセキュリティレベルの高い会員が、セキュリティについて困っている加盟企業に対してコンサルティングすることも ISAC の活動として考えられる。Surface Transportation, Public Transportation and Over-the-road Bus ISACS では、専門家によるインシデント対応コンサルティングが行われている。

・表彰制度

情報共有に関する表彰制度を設けることで、情報共有が促進される。表彰者は有益な情報共有や WG へ貢献した会員を投票形式により、選出することで参加意識が生まれる。

（３）情報共有の状況の評価

定期的に情報共有の状況について評価することが望ましい。

情報共有の状況を評価する場合は、以下の点を考慮する必要がある。

- 共有される情報が適時性や信頼性を持ち、品質がよいか
- 共有される情報は会員に関連性があり、会員組織が持つ既存の情報を補完できているか。
- 共有された情報を元に、会員が対策を実行可能か
- 共有される情報の頻度や数が、会員組織の処理能力に見合っているか

・情報発信者の匿名化の仕組みが適切であるか
・情報交換フォーマットが会員組織内のツールと互換性があるか
また、共有される情報の他にも、ISAC の運営と活動状況についても考慮する必要がある。
・ISAC の規模や構成（参加者数、情報供給者、情報消費者）
・ISAC の活動実績（1 日当たりの共有情報数など）
・会員の審査方法
・会員の技術スキルや熟練度
・ISAC の共有規則（加盟企業の目標、目的、ビジネスルールに一致するか等）
・ISAC のデータ保管・廃棄ポリシー
評価にあたっては、総会、WG でのヒアリング等による意見収集を行うとよい。

（４）その他検討すべき事項

その他に検討すべき事項として以下が挙げられる。

１）加盟企業の ISAC の窓口担当者が固定化しないための工夫

加盟企業の ISAC の窓口担当者が固定化してしまうと、知識・経験が窓口担当者に依存してしまうことになり、持続的な ISAC の活動が困難となる。

２）情報共有の運用が事務局に依存しないための工夫

ISAC の構築当初は、情報共有のサイクルが醸成されていないため、他の会員からの新たな知見が得られないと見込まれる状態で情報を提供することにメリットを感じられないことや、会員外への情報漏えいへの不安等により、会員からの積極的な情報共有が行われない可能性もある。そのため、事務局からの情報提供が主となることや、その他の活動を事務局主導で行わなければならないことも考えられる。会員による積極的な活動のために、会合や懇親の場を提供する等、粘り強い呼びかけが重要である。

３）他のセキュリティ情報共有組織で取り扱われる情報との重複感の回避

他のセキュリティ情報共有組織と取扱う情報が重複する場合、加盟企業において情報の取扱いの負担が増加する。国内の既存の ISAC では、セプターを兼ねる場合もあり、既報か否かを明示した配信等を検討するとよい。

５．３　第５章まとめ

本章では、鉄道及び航空分野の ISAC の実現に向けた検討を実施した。検討にあたっては、ヒアリング調査などにより把握された国内外の情報共有組織の活動の好事例や課題、アンケート調査により把握された鉄道・航空事業者の情報共有に関する実情を踏まえるとともに、脅威情報の共有関係を確立するためのガイドラインである NIST SP 800-151 や、EU 内にある各 ISAC の状況を調査し、EU における更なる ISAC 発展のための方策を提案するレポートである ENISA ISACs Cooperative models において提示された実施すべき活動や課題を参考に、鉄道及び航空分野の ISAC あるべき姿を整理した。

鉄道分野・航空分野は、我が国のサイバーセキュリティ戦略において重要インフラ分野に特定されており、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。最近では、鉄道分野・航空分野でも制御システムの IoT（Internet of Things）化の波が進む中、新しい脅威が生まれている。国内では、現時点においては大規模なサイバー攻撃は報告されていないが、海外では鉄道分野・航空分野においても被害が報告されるようになってきていることからも、対策は急務となっている。こうしたことから、情報共有組織の機能を涵養し、ISAC に期待される活動を実施していくことが今後重要となる。

参考１．SP800-150 “Guide to Cyber Threat Information Sharing” 抄訳

Abstract

サイバー脅威情報は、組織が脅威を特定し、評価し、監視し、対応するために役立つあらゆる情報を指す。サイバー脅威情報は妥協策（compromise）の指標（攻撃者の戦術、技術、手順）や、攻撃を検出し抑制し防止する推奨策、インシデントの分析により得られた知見を含む。サイバー脅威情報を共有する組織は、自身のセキュリティ姿勢だけでなく他の組織も向上させることができる。

この文書はサイバー脅威情報共有体制を確立し参加するためのガイドラインを提供する。この文書は、情報共有のゴール設定、サイバー脅威情報の情報源の特定、情報共有活動のチェック、脅威情報の開示と拡散に関するルール策定、既存の情報共有コミュニティとの関わり方、そして、組織のサイバーセキュリティ対策全体における脅威情報の効果的な利用方法について組織を支援する。

Executive Summary

サイバー攻撃はますます増加し、その手法も高度化しているため、データまたはシステムを攻撃者から保護する必要がある組織にとって、大きな課題となっている。攻撃者は個人から犯罪組織や国家的な組織まで及ぶ。攻撃者は常に存在しており、意欲的で、機敏である。また、彼らは様々な「戦術（tactics)、技術（techniques)、手順（procedures)」（TTPs）を使用し、システムへの不正アクセス、サービスの中断、詐欺、知的財産・機密情報の奪取を行う。これらの脅威がもたらすリスクを考慮して、組織がサイバー脅威の情報を共有し、セキュリティ体制を向上することがますます重要になっている。

サイバー脅威情報とは、組織が脅威を測定、評価、監視、及び対応からするために役立つ情報のことを指す。サイバー脅威情報の例としては、インジケータや、TTPs、セキュリティアラート、脅威情報レポート、推奨されるセキュリティツールの設定等がある。多くの組織では、情報システムやセキュリティ運用の一環として、社内で共有可能な複数種類のサイバー脅威情報を作成している。

共有コミュニティの中でサイバー脅威情報を共有することにより、組織は共有コミュニティの知識・経験・能力を活用し、直面する脅威をより詳しく理解することが可能となる。この知識を利用して、組織は、脅威に対する防御、検知、緩和にあたり、適切な判断を下すことができる。また、組織は、複数の情報源からのサイバー脅威情報を相互に関連付けて分析することで、既存の情報をより深淵化し有効なものにすることができる。深淵化は、コミュニティの他のメンバーの報告を確認し、曖昧さや間違いを減らして、脅威情報の全体的な品質を向上させることによって可能となる。組織が脅威情報を受け取り、その情報を利用して修正を行うことで、脅威の広がりを妨げることができ、それによって他組織に対して、ある程度の保護を与える。さらに、サイバー脅威情報を共有することで、特定の業種、事業体、機関を対象とした攻撃がより適切に検出可能となる。

本文書は組織がサイバー脅威情報共有関係を確立し、参加することを支援する。本文書では、共有の利点と課題を説明し、信頼の重要性を明確にし、情報の取扱いにおける考慮事項を紹介する。また、本文書の目的は、安全かつ効果的な情報共有の取組みを通じた、サイバーセキュリティの運用とリスク管理活動を改善するためのガイドラインを提供して、組織が情報共有の計画、実施、維持を行うこと支援する。

NIST は、他組織からのサイバー脅威情報の取得と、自組織で生じた脅威情報の他組織への提供の、両面に関する情報共有の強化を促進する。組織が情報共有を効率的かつ効果的に行うための推奨事項を以下に示す。

・業務及びセキュリティポリシーをサポートするような情報共有の目的と目標を確立する

組織の情報共有の目標と目的は、全体のサイバーセキュリティ戦略を推進し、組織がサイバー関連のリスク管理をより効果的に行うことに役立つ。セキュリティやプライバシー、規制、法令遵守の要件に従いながら脅威情報を共有するために、サイバー脅威情報共有組織のメンバー等、他社と自組織の知識と経験を照らし合わせて利用する必要がある。

・組織内でのサイバー脅威情報の出所を整理する

現在のセキュリティ対応能力がわかり、外部などから追加で必要な情報を検討することができる上、外部へ共有可能な情報を決めることができる

組織は、サイバー脅威情報を収集・生成・保存するツール、センサー、及びリポジトリと、サイバー脅威情報の交換をサポートする脅威分析プラットフォーム、さらに配信方法を特定する必要がある。組織内部のサイバー脅威情報源と能力が特定された後、これらの情報源からの情報がどのようにサイバーセキュリティとリスクの管理をサポートしているかを判断する必要がある。組織はまた、判明した知識のギャップを文書化し、外部の情報源や、他のツールやセンサーを配備することで追加の脅威情報の取得を検討する必要がある。さらに、外部組織との共有に適した脅威情報を特定する必要がある。

・情報共有を行う範囲を指定する

組織の情報共有活動の範囲は、そのリソース、能力、目的と一貫している必要がある。情報共有にあたっては、組織とその共有相手に最大の価値を提供することに焦点をあてることが望ましい。焦点をあてる際は、主要な利害関係者が共有可能な情報の種類、状況、及び人を特定する必要がある。

・情報共有のルールを確立する

情報共有のルールは、脅威情報の公開と配布を制限することを目的としており、組織、顧客、またはビジネスパートナーに悪影響を及ぼす可能性のある情報の流出を防止するのに役立つ。情報共有ルールは、受信者の信頼性、共有する情報の機密性、及び情報を共有する（または共有しない）ことによる影響を考慮する必要がある。

・情報共有活動に参加する

組織は、既存の脅威情報機能を補完する活動を判別し、参加する必要がある。また、運用上

のニーズを満たすために、複数の情報共有コミュニティに参加する必要がある。公的及び私的共有コミュニティ、政府リポジトリ、商業的なサイバー脅威情報フィード、及びオープンソースを考慮する必要がある。

・情報の意図や解釈、関連性についても提供することで情報（インジケータ）の質を積極的に高めるよう努める

可能であれば、組織はインジケータごとにメタデータを生成することによって、脅威情報の有用性と有効性を高めるべきである。メタデータは、解釈の方法や他のインジケータとの関連といったインジケータの意図を付け加えることによってインジケータに関する文脈を提供することができる。さらに、共有プロセスには、インジケータの公開や、インジケータと関連メタデータの更新、誤って共有された情報の取消しなどの仕組みが含まれている必要がある。このようなフィードバックは、コミュニティ内で共有されるインジケータの詳細度や質に重要な役割を果たす。

・サイバー脅威情報の共有・分析・処理のために、自動化された仕組みを利用する

サイバー脅威情報を共有するにあたって、標準化されたデータ形式とトランスポートプロトコルを使用することより、脅威情報の処理をより簡単に自動化できる。自動化することで、サイバー脅威情報を迅速に共有、変換、分析、処理することが可能となる。

・情報共有に関する協定を確立する

サイバーインシデントが発生している間に情報共有に関する協定を確立するのではなく、インシデントが発生する前に計画し、協定を結んでおく必要がある。このような高度な計画は、参加組織同士が信頼できる関係を確立し、互いの役割、責任、及び情報の取扱いポリシーを理解することに役立つ。

・機密情報のセキュリティとプライバシーを保護する

サイバー脅威情報を取扱う場合、制限情報（CUI）や個人識別情報（PII）などの機密情報を取扱う可能性がある。そのような機密情報を不適切に開示してしまうと、財政的損失や法律・規制・契約の違反、訴訟の原因、または組織や個人の評判を損なう可能性がある。したがって、不正な開示や改ざんから機密情報を保護するために、組織は必要なセキュリティとプライバシーの管理と取扱い手順を実装する必要がある。

・情報共有活動の継続的なサポートを行う

各組織は、継続的なインフラの整備とユーザーへのサポートの提供に関する情報共有計画を策定する必要がある。情報共有計画は、内外の情報源からの脅威情報の収集と分析を行い、防護措置の開発と展開に収集・分析した情報を使用することに言及する必要がある。持続可能なアプローチは、サイバー脅威情報の継続的な収集、保存、分析、及び普及を行うためのリソースを保証するために重要である。

1. Introduction

1.1 目的及び対象

本文書は、組織がサイバー脅威情報を交換するにあたっての指針を提供する。本文書は、組織内でのサイバー脅威情報の共有や、外部情報源から受け取ったサイバー脅威情報の利用、及び他の組織と共有できるサイバー脅威情報の作成について言及する。本文書はまた、情報共有コミュニティへの参加のための具体的な考慮事項を提示している。

本文書はNIST SP800-61の第4章“Coordination and Information Sharing”で紹介された情報共有の概念を拡張したものである。

1.2 対象読者

本文書は、CSIRTs、及びシステムやネットワークのアドミニストレーター、サイバーセキュリティスペシャリスト、個人情報監督者、技術サポートスタッフ、CISOs、CIOs、コンピューターセキュリティプログラムマネージャー、及びその他のサイバー脅威情報の共有活動を行う上での主要な関係者を対象としている。

本文書は主に連邦政府機関向けに記載されているが、様々な政府機関及び非政府機関に適用されることを想定している。

1.3 文章構成

本文書は以下の章と付録で構成される。

第2章では、基本的なサイバー脅威情報共有の概念を紹介し、情報共有の利点について説明し、組織が共有機能を実装する際に組織が直面する課題について説明する。

第3章では、他の組織との関係を確立するためのガイドラインを示す。

第4章では、関係を効果的に共有するための考慮事項について説明する。

・付録Aでは、サイバー脅威情報を共有し、パートナーのサイバーの経験と能力を活用して、組織がネットワーク防御を強化する方法に関するシナリオが掲載されている。

・付録Bでは、本文書で使用されている用語のリスト、及び関連する定義が掲載されている。

・付録Cでは、本文書で使用されている略語リストが掲載されている。

・付録Dは、本文書のリファレンスが掲載されている。

2. Basics of Cyber Threat Information Sharing

本章では、サイバー脅威情報の種類や専門用語と併せて、サイバー脅威情報の共有に関する基本的な概念を紹介する。また、共有されたサイバー脅威情報の利用方法について説明し、脅威情報の共有に関する利点と課題いついても明らかにする。

2.1 脅威情報の種類

「サイバー脅威」とは、組織の業務、組織の資産、個人、その他の組織、国家に対し悪影響を与える可能性のあるあらゆる状況または事象であり、情報システムを介して不正アクセス、破壊、情報の暴露や改ざん、サービスの停止などが行われる。本文書では完結にするために、「サイバー脅威」を「脅威」と呼ぶ。また、脅威をもたらす者を攻撃者と呼ぶ。

「脅威情報」とは、組織が脅威から自身を保護し、攻撃者の活動を検出するのに役立つ情報のことを指す。主な脅威情報は以下のようになっている。

・**インジケータ（Indicator）**は、攻撃が差し迫っているか、あるいは現在進行中であるか、あるいは既に不正にアクセスされているかについて示唆する技術的指標のことで、潜在的な脅威を検出し防御するために使用することができる。インジケータの例には、疑わしいコマンド及び制御サーバーの IP アドレスや、疑わしい DNS のドメイン名、悪意のあるコンテンツを参照する URL、悪質な実行ファイルのハッシュ、悪意のある電子メールの件名のテキストがある。

・**戦術（tactics）、技術（techniques）、手順（procedures）（TTPs）**は攻撃者の行動に関する情報を意味する。「戦術」は上位レベルの振る舞いに関する情報を指し、「技術」は戦術上の詳細な振る舞いに関する情報を指し、「手順」は技術上の具体的な振る舞いを指す。TTPs は特定のマルウェアの亜種、操作の順序、攻撃ツール、フィッシング等の配信メカニズム、搾取など、攻撃者の傾向。について記述される。

・**セキュリティアラート**は、アドバイザリ、掲示板、脆弱性メモとも呼ばれる、脆弱性やその悪用等についての技術的なセキュリティ情報のことを指す。セキュリティアラートは US-CERT や ISAC、国家脆弱性データベース（NVD）、PSIRT、セキュリティサービス企業、研究者等から発信される。

・**脅威インテリジェンスレポート**は、TTP や攻撃者、対象システム、情報の種類、その他脅威関連情報が記述された文書を指す。インテリジェンスとは意思決定プロセスで必要な情報を提供するために、集約、変換、分析、解釈、または強化された脅威情報を意味する。

・**ツール構成**は、脅威情報の自動収集・分析・共有・利用のためのツールの設定及び使用法方に関する推奨事項を指す。ツール構成情報の例として、ルートキット検出・削除ツールのインストール方法と使用方法、侵入検知シグネチャの作成と構成方法、ルーターアクセス制御リスト（ACLs）、ファイアウォール規則、Web フィルタ設定などがある。

多くの組織は、既に内部で脅威情報を共有している。例えば、組織のセキュリティチームは、インシデントに応答する際に、侵害されたシステム上の悪質なファイルを特定し、関連する一連のインジケータ（ファイル名、サイズ、ハッシュ値等）を生成する。これらのインジケータは、他のシステム上の有無を検出するために、侵入検知システムなどのセキュリティツールのシステム管理者と共有される可能性がある。同様に、セキュリティチームは、組織内におけるフィッシング攻撃の増加に対応して、電子メールについてのセキュリティ意識向上を喚起する可能性がある。

本文書の第一の目的は、他の組織から脅威情報を取得し、内部で生成された脅威情報を他の組織に提供することなど、組織の境界を越えた脅威情報共有を促進することである。

2.2 情報共有の利点

脅威情報の共有により、組織が本来であれば利用できない脅威情報へのアクセスが可能となる。組織は共有されたリソースを利用し、パートナーの知識、経験、能力を積極的に活用することで、セキュリティ体制を強化することができる。「一つの組織の検出が他者の予防になる」ことは、情報を共有する組織の全体的なセキュリティを向上させる強力な枠組みである。

組織は、様々な方法で共有された脅威情報を利用できる。運用上の例としては、攻撃や不正アクセスを検出するための新しいインジケータとコンフィグレーションを用いた継続的監視のためのエンタープライズセキュリティコントロールの更新がある。また、組織のセキュリティシステムの更新時に、共有された脅威情報を考慮するなど、脅威情報を戦略的に使用することもできる。

同業他社は、同じ種類のシステム及び情報を対象とした共通の TTP を使用する攻撃者から攻撃されるため、特定の業界を中心に組織されたコミュニティ内で交換される脅威情報は特に有益である。サイバー防衛は、集団の攻撃者から組織を防衛するために組織同士が協力する場合に最も効果的となる。このような連携は、リスクを軽減し、組織のセキュリティの体制を向上することに役立つ。

情報共有に関する利点として以下が挙げられる。

・状況に関する認識の共有

情報を共有することで、組織は、パートナーの総合的な知識、経験、及び分析機能を活用することが可能となり、その結果として、複数の組織の防御能力を高めることができる。攻撃者に関する新たなインジゲータや観察を共有するだけでも、コミュニティ全体のセキュリティ向上に貢献することができる。

・セキュリティ体制の改善

脅威情報を共有することで、組織は脅威に関して理解を深め、リスク管理の実施に関する通知に脅威情報を利用することができる。また、共有された情報を使用して、影響を受けるプラットフォームやシステムを特定し、対策を実施、検出機能を強化、脅威環境の変化に基づいたインシデントへの効果的な対応・回復が可能となる。組織同士が情報を共有し、脅威を緩和するにつれ、攻撃者が実行可能な攻撃経路の数を減らすことになり、コミュニティ全体のサイバ

ーセキュリティの体制を改善できる。

・知識の成熟

一見無関係と思われる情報を組織同士で共有し、分析することで、他社が収集した情報と連携させることが可能となる。これにより、既存のインジケータを強化し、攻撃者の TTPs に関する知識を深めることで、情報の価値を高めることになる。また、情報を連携させることで、インジケータ間の貴重な示唆を与えることも可能となる。

・防御の機敏性の向上

攻撃者は検出やセキュリティ対策を回避し、新しい脆弱性を悪用しようと、常に TTPs を変化させる。情報を共有する組織は、TTPs の変化や、脅威に関する素早い検知と対応の必要性について通知されることがある。これにより運用スピードを高め、攻撃者の攻撃を失敗させることが可能となる。素早い対応によって、攻撃者は新たな TTPs を練る必要が発生する。

2.3 情報共有の課題

脅威情報の共有には利点があるが課題もある。脅威情報の利用と生成に関する課題としては以下が挙げられる。

・信頼関係の確立

信頼関係は情報共有の基盤であり、定期的な対面会議、電話会議、ソーシャルメディアなどを活用して信頼関係を構築する。

・相互運用性と自動化の実現

共有する情報のデータ形式の標準化とプロトコルが相互運用性に重要である。一般化された形式とプロトコルを使用することで、自動化でき、また情報交換が高速化できる。フォーマットとプロトコルを適用する場合、時間とリソースが必要になる可能性があるが、共有するパートナーが異なるフォーマットとプロトコルを要求してくる手間を減らすことができる。標準化にあたって、フォーマットとプロトコルの変更時にはツールの変更が必要となる場合がある。

・機密情報の保護

個人情報（PII）や取扱注意情報（CUI）等の機密情報の開示によって、金銭的損失や契約違反、訴訟、評判の低下に繋がる。セキュリティログやスキャン結果などのセキュリティ情報やインシデント情報を共有すると、組織の保護機能や偵察機能が公開されることになり、攻撃者による脅威の変化を招く可能性がある。組織は、機密情報のリスクを管理するために、共有情報を扱う際のポリシー、手順、コントロール技術を実装し、不正な開示を回避する必要がある。

・分類された（政府機関から提供された）情報の保護

政府筋から受信した情報は分類され印がつけられており、組織が利用することが難しくなる。また、そうした情報を継続的にアクセスするための認定を取得し、維持するためには費用や時間がかかる。さらに、多くの組織では機密情報へのアクセスが許可されていない米国国外のス

タッフを雇用している。

・情報の受信・提供方法の確立

脅威情報を共有しようと考えている組織は、まず始めにツールや人員の訓練を行う必要がある。大量の情報を受け取った場合、組織の処理能力を上回る可能性があることから、どのように情報共有を行うかについて、慎重に検討する必要がある。インジケータ等を自動的に交換できない場合は、ベストプラクティスや脅威情報のまとめのみを受け取ることを検討する。

以下の課題は、脅威情報を利用する場合に発生する。

・外部情報へのアクセス

組織は、外部ソースから情報を得るためのツール及び外部情報を意思決定に使用するためのプロセスが必要である。組織が情報に基づき行動できてこそ、外部情報に価値がある。

・情報の品質評価

脅威情報に基づいて行動する前に、受信情報が正しいことや、対象とする脅威に関連すること、情報を利用した場合（あるいは利用しなかった場合）の影響について確認する必要がある。

以下の課題は、組織が他組織に対して、独自の情報を提供する場合に発生する。

・法的・組織的要件の遵守

組織の執行チームや法務部が、他社に提供する情報の種類や技術詳細レベルを制限する場合がある。これらの制限が、法律上あるいはプライバシー上、あるいはビジネス上で、適切に設定されていればよいが、不当な制限によって、情報の有用性、可用性、品質、適時性を低下させる可能性がある。

・発信者帰属の制限

組織は情報共有コミュニティに自由に参加できるが、発信は匿名でなければならない。匿名の情報共有は、組織のリスクが少なく、より多くの情報を共有できる可能性がある。しかし、匿名情報の信頼性は低く、有用性が制限される可能性がある。また、元の情報源が特定できない場合、組織は複数の情報源から情報の情報を識別することができないため、受信した情報の信頼性を高めることができない可能性がある。

3. Establishing Sharing Relationships

情報共有機能を確立するにあたり、以下の計画と準備が推奨される。

・情報共有の目的と目標の定義（3.1 章）
・脅威情報の情報源を特定（3.2 章）
・情報共有活動の範囲を定義（3.3 章）
・情報共有規則の確立（3.4 章）
・情報共有コミュニティへの参加（3.5 章）
・情報共有活動への継続的なサポートを計画（3.6 章）

この過程で、組織内外の専門家と相談することが推奨される。専門家としては以下のような例が挙げられる。

・経験豊富なサイバーセキュリティ担当者
・既存の脅威情報共有組織の運営者とメンバー
・信頼できるビジネスパートナー、サプライチェーン、同業他社
・法律、内部業務プロセス、手順、システムに関する専門家

組織は、これらの専門家の知識と経験を利用し、脅威情報の共有機能を形成する必要がある。絶えず変化するリスクや要件、優先順位、技術、規制等により、このプロセスは繰り返されることになる。組織は、状況の変化に応じて、情報共有機能を再評価し、変更する必要がある。変更にあたっては、上記の計画及び準備の一部または全部を再度行う必要がある。

3.1 情報共有の目標と目的の定義

まず始めに、ビジネスとセキュリティポリシーの観点から情報共有の成果目標と目的を定める。目標及び目的は、情報共有活動のスコープの設定、共有するコミュニティの選択、情報共有活動を行う上で、組織を導くものになる。限られたリソースの中で重要な情報共有が確実に行われるために、最適な目標及び目的を定めることが必要である。

3.2 サイバー脅威情報の情報源の特定

情報共有を行うにあたり、組織内の脅威情報の情報源を特定することが重要なステップとなる。組織内部の脅威情報源を一覧化することで、足りないものを特定することができる。組織内部に存在しない情報源については、追加のツールやセンサー、あるいは外部情報源を使用することで対処できる。大規模な組織では、脅威情報源を一覧化することで、これまで共有されていなかった情報源を特定することができる。

脅威情報源を特定するプロセスには以下が含まれる。

・脅威情報を生成するセンサーやツール、リポジトリ等を特定し、それらの情報が、サイバーセキュリティに関する意思決定を行うために適切な頻度及び精度で生成されていることを確認する
・これまでに継続的に収集・分析されてきた脅威情報を特定する
・これまでに収集・保存されてきた脅威情報を特定する。活用されていない脅威情報があった場合、リスク管理に活用する方法を検討する
・外部との共有に適した、脅威への対応に役立つ情報を特定する

脅威情報源の所有者と運営者は、脅威情報の一覧化にあたって重要であり、両者に話を聞く必要がある。彼らは、利用可能な情報と、その保存形式（エクスポート形式、データ検索用のクエリ言語・プロトコル・サービス）を理解している。オープンかつ機械可読なフォーマットで構造化されたデータであれば、ツールで容易にアクセス・検索・分析することが可能となる。したがって、情報のフォーマットは情報交換・分析の容易さと効率を決定する上で重要な要素となる。

脅威情報の一覧化にあたって、目標の実現に必要な情報が抜け落ちていないか注意する必要がある。足りていない情報を特定することで、組織は新しい機能に関する投資の優先順位をつけやすくなり、また、外部情報源や、追加導入したツールやセンサーから脅威情報を取得することで足りていない情報を保管することを検討できるようになる。

表 3-1 は、サイバーセキュリティ関連情報の一般的な情報源とデータ要素の例を示している。

表3-1　内部情報源の選択

情報源	例
ネットワークデータ情報源	
ルーター、ファイアウォール、リモートサービス、DHCP サーバーのログ	タイムスタンプ、IP アドレス、ドメイン名、ポート番号、MAC アドレス、ホスト名、サービス挙動、ステータスコード、その他のプロトコル情報
診断・監視ツール（ネットワーク侵入検知・防止システム、パケットキャプチャ・プロトコル解析）	タイムスタンプ、IP アドレス、ポート番号、ネットワークフロー、パケットペイロード、アプリケーション固有の情報、受けた攻撃の種類、ターゲットとなった脆弱性、攻撃の成否
ホストデータ情報源	
OS やアプリケーションの構成設定、状態、ログ	結合され確立されたネットワーク接続とポート、プロセスとスレッド、レジストリ設定、設定ファイルのエントリ、ソフトウェアバージョンとパッチレベル、ハードウェア情報、ユーザーとグループ、ファイル属性、ファイルアクセス、システムイベント、コマンド履歴
アンチウイルス製品	ホスト名、IP アドレス、MAC アドレス、マルウェア名、マルウェアの種類、ファイル名、ファイルパス、ファイルのハッシュ値、実行アクション
Web ブラウザ	ブラウザ履歴とキャッシュ（閲覧したサイト、ダウンロードオブジェクト、アップロードオブジェクト、ブラウザ拡張機能、クッキー）
その他の情報源	
セキュリティ情報とイベント管理（SIEM）	様々なデータソースが合わさったサマリーレポート

メールシステム	メールメッセージ（メールヘッダー・メールアドレス・県名・経路情報、添付ファイル、URL、組み込み画像）
ヘルプデスク、インシデント管理システム	インシデント観測・分析レポート ユーザー画面キャプチャ
科学捜査ツールや動的・仮想実行環境	マルウェアのサンプル システム構成

新たなセンサーやリポジトリや機能等を導入する場合や、システム構成や設定、所有者が変わった場合などには、使用可能な IT 資産のデータ一覧を更新する必要がある。

3.3 情報共有活動範囲の定義

共有可能な情報の種類、情報の共有が許可される状況・人を特定し、情報共有活動の範囲を指定する必要がある。情報共有活動の範囲を定めた上で、情報共有の目標を見直し、優先順位が処理されるようにする。情報共有活動の範囲を定める場合は、組織にとって必要な情報源と処理能力がきちんと機能することを考慮する必要がある。また、組織は自組織が持っていない情報を得るための共有活動を検討するべきである。例えば、組織内に分析機能がなくとも、共有コミュニティに参加することで、インジケータを得られる可能性がある。

情報共有活動の範囲は組織のリソースと能力によって異なる。リソースが限られる組織は、活動範囲を狭めることで、一つの活動を集中して行うことができる。リソースが潤沢で、高度な機能を持つ組織は、目標を実現するために、最初から広範な活動を行うとよい。

また、情報共有活動の範囲を定める際には、情報共有の自動化の程度についても考慮する必要がある。手動で情報共有を行った場合、人件費が増加し、処理可能な情報量が制限される。自動化を進めることで、人件費を削減し、より多くの情報を共有することが可能になる。情報共有の自動化の概念については第 4 章で詳しく解説する。

3.4 情報共有規則の確立

情報共有を始める前に、以下を行うべきである。

・共有可能な情報種類のリストアップ
・情報共有が許可される条件と状況の明文化
・脅威情報の受信者の明確化
・情報の修正・消去のための要件の明文化
・情報の帰属の指定
・情報保護のため、情報受信者の義務を記述した情報管理規定を定める

情報共有規則は、情報の公開・配布を制御し、不適切な開示が行われた場合に、組織・顧客等へ悪影響を及ぼす可能性のある情報が拡散されることを防ぐ。情報共有規則は、受信者の信頼性、情報の機密性、共有することによる潜在的影響について考慮する必要がある。例えば、非常に機密性の高い情報については個人間またはグループ内での情報交換を制限し、機密性の高い情報については、特定の信頼できるパートナーとのみ共有を許可し、機密性の低い情報については共有コミュニティ内の共有を許可し、重要ではない情報についてはコミュニティ外に

公開可能、といったルールを確立する。

情報共有規則は、大規模企業において、部署間で脅威情報の共有を行う際にも確立されるべきである。共有を行う部署間で、どのような種類の脅威情報を共有するのか、どのように情報共有を行うのかについて議論する必要がある。多国籍企業では、各国での法令の違いや、外国人と共有不可能な情報の取扱いについても検討する必要がある。

情報共有規則を確立する際には、法務担当者、情報管理者、利害関係者等による、共有規則が組織の内部規則と合致するかの確認が必要である。情報共有規則は、MOUs や NDA やその他の共有枠組み協定など、様々な形で適用可能である。また、情報共有規則はインシデント発生時にのみ適用するのではなく、平時から適用することが望ましい。

情報共有規則は、規制・法令の変化、組織のポリシーの更新、新規情報源の導入、リスク許容度の変更、情報の所有権の変更、脅威環境の変化、組織の合併や買収といったイベント等に合わせて、定期的に再評価する必要がある。

3.4.1 情報の機密性とプライバシー

組織は、個人情報（PII）や取扱注意情報（CUI）、その他米国の各法律で保護された機密情報を取扱う。機密情報を特定し、適切に保護する必要がある。機密情報を特定し保護するための手順を定める際には、組織の法務担当者、プライバシー担当者、監査人、各規制・枠組みの専門家に相談する必要がある。

プライバシーの観点からの脅威情報の共有における重要な課題の一つとして、PII の開示可能性がある。脅威情報を取扱う担当者が PII を判断し保護できるようにするために、教育と啓蒙活動が必要である。

脅威情報を組織内部で共有した際に、通常業務ではアクセス権がない人に PII が開示される可能性がある。例えば、フォレンジックアナリストやインシデントレスポンダがマルウェア、電子メール、パケットキャプチャを確認する際に、それらの中に PII が含まれる場合がある。分析結果が他の職員に共有される場合は PII の機密性を保護する措置を講じる必要がある。

組織は、PII の取扱いに関する情報共有ポリシーと手順を定めるべきである。ポリシーと手順には、PII を含む可能性が高いインシデント・データ型を識別する手順も含む。ポリシーには、そのようなデータを共有する際のプライバシーリスクを管理するための適切な保護手段が記述されている必要がある。一般的にはインジケータの交換をメインとする場合が多い。ハッシュやネットワークポート番号、レジストリキー値、その他のデータ要素などのインジケータは PII をほとんど含まない。ただし、PII が特定されている場合、組織は、情報共有を行う前に、関係のない PII を含む情報を修正する必要がある。

実際には、PII の識別と保護にあたっては、エラーを防ぐために自動化することが推奨される。PII を手動で識別することは、エラーが発生しやすく、リソースを大量に消費する。自動的な PII の識別・保護の方法として、ホワイトリストを使用したフィールドのデータ検証、正規表現等のパターンマッチングによる検索、PII を含む情報の共有解除、マスク、匿名化などが挙げられる。

また、組織は知的財産、営業秘密、その他の専有情報の不適切な開示からの保護を実施すべきである。不適切に開示された場合、金銭的損失や NDA 等共有協定違反、法的罰則または組織の評判を損なう可能性がある。組織は CUI の不正または意図しない開示に対処するための計画

を立てるべきである。この計画には、不適切な開示の抑制、管理、復旧の手順が含まれ、違反を通知する要件、及び再発防止策の検討も含まれる。

表 3-2 は、各脅威情報に存在する可能性のある機密データと、その処理のための推奨事項が示されている。

表3-2 機密情報の種別ごとの取扱い推奨事項

脅威情報の種類	機密データの例	推奨事項
ネットワークインジゲータ	単体のインジゲータには機密性があるが、複数のインジゲータの情報を集約することで、ネットワーク内の構成やデバイスに関する情報、組織が採用しているセキュリティ保護策とツールを推測することができる	攻撃者が実行したコマンドや宛先 IP アドレス、悪意のある URL・ドメイン名、ステージングサーバーなどのインジゲータを使用する。 共有前に、組織内の IP アドレス、MAC アドレス、また内部ネットワークの構造や製品が特定可能なポート、プロトコルの匿名化・消去を行う。
パケットキャプチャ（PCAP）	暗号化されていないパケットや復号したパケットには機密情報が含まれる場合がある	ネットワークインジゲータがパケットヘッダーとペイロードの両方に存在する可能性がある。PCAP ファイルは DHCP や FRP、FTP、DNS 及びアプリケーション等の情報を含んでいるため、機密情報の黒塗りや匿名化が必要な場合がある。 共有前に特定のインシデントやイベントに関連したパケットのみを抽出する。 機密情報が含まれ、かつ対象のイベントに関係ないペイロードは編集する。
ネットワークフローデータ	ネットワークフローデータには、IP アドレスやポート、プロトコル、バイト数、タイムスタンプが含まれる。 匿名化されていない場合、ユーザーの識別と挙動に関する情報がわかってしまう。	共有前には暗号化、プレフィックス保存、IP アドレス匿名化手法を使用し、データの一部の修正を検討するべきである。参照整合性を損なわないように変換しなければならない。
フィッシングメールのサンプル	メールヘッダーには、IP アドレス、ホスト・ドメイン名、メールアドレスが含まれる。また、本文には PII や CUI、その他の機密情報が含まれる場合がある。	インシデントの調査に必要ない範囲でメールの匿名化や機密情報の削除を実施すべきである。

システム、ネットワーク、アプリケーションのログ	ログファイルには、PII、CUI、その他の機密情報が含まれる場合がある。また、IP アドレス、ポート番号、プロトコル、サービス、URL、接続文字列、ログオン資格情報、金融取引情報、URL パラメータなどが含まれる。	IP アドレス、タイムスタンプ、ポート番号、プロトコルの匿名化を実行し、インシデントの調査に必要でない機密情報の削除を実施するべきである。 共有前にセッション ID やユーザーID 等の識別情報を含むURL の消去が必要な場合もある。 特定のアプリケーションログ形式に固有の修正や匿名化が必要な場合がある。
マルウェアインジゲータとサンプル	マルウェアのターゲットや収集方法によっては、機密情報が含まれてしまう可能性がある。	インシデントやイベントの調査に必要ない範囲で PII や CUI、その他の機密情報の削除を実施すべきである。

3.4.2 共有の指定

脅威情報の処理要件を指定することで、未公開で取扱いに注意すべき情報を特定することが可能となる。組織は、共有された脅威情報に対する明確な取扱いガイドラインを提供することが推奨される。また、共有情報の受信者は、ガイドラインに定められた取扱い・帰属・展開・保管要件を遵守する必要がある。

表 3-3 は Traffic Light Protocol (TLP) を示す。共有の指定を表現するフレームワークである。

表3-3 Traffic Light Protocol

色	分類条件	共有方法
TLP：赤 関係者以外への公開禁止	外部に情報を展開することによる効果的が見込まれない場合、かつ、情報が誤用された場合、プライバシーや評判、経営に悪影響を及ぼす場合	受信者は、最初に情報が公開された特定の関係者以外への共有が禁止される。会議で共有された場合は、会議の出席者に限定される。多くの場合、口頭または直接共有される。
TLP:橙 関係者が所属する組織のみの公開	情報を効果的に使用するためには外部の協力が必要だが、情報を外部に共有した場合、プライバシーや評判、経営にリスクが存在する場合	受信者は自組織のメンバー及び更なる被害を防ぐために情報を知る必要のある顧客とのみ共有することができる。また、制限を追加することもできる。
TLP:緑 コミュニティ内のみの公開	全ての参加組織やコミュニティのメンバーにとって情報が有用である場合	コミュニティ内のメンバーと情報共有することは可能だが、一般に公開することはできない。コミュニティ内でのみ公開される。
TLP:白 公開制限なし	一般公開用ルールと手順に則り公開されることで、誤った利用のリスクが最小限に抑えられている場合	制限なく公開される。

TLP は適用される制限を色で示している。赤色は、参加者自身の組織内であっても共有が制限される、厳しいルールである。橙色、緑色、白色の順に制限が緩やかになる。

アンチフィッシングワーキンググループ（APWG）は、共有の指定を表現するスキームを提案している。このスキームでは、拡張可能な階層的タグを使用し、共有情報に関する制限（共有者等）を表現できる。

脅威情報の中には、収集方法については機密だが、情報自体は共有可能なものがある。この場合には、異なる制限レベルの情報が混ざらないように章分けしたレポートを利用できる。レポートを制限レベルで章ごとに分けることで、受信者が許可されている情報だけを含むレポートを作成することができる。

組織は、共有の指定を定めるための基準を慎重に検討する必要がある。また、その基準を文書化し、担当者の訓練を行わなければならない。

3.4.3 サイバー脅威情報の共有と追跡手順

情報共有を行っていく中で、組織には内外の情報源からの脅威情報が大量に蓄積される可能性がある。情報源を追跡することは、困難ではあるが、情報所有者を守ること及び情報受信側の組織がデータ保護に関する規制を遵守するために、重要である。また、組織は情報の提供元・収集方法・変換方法・処理方法等、共有された情報から結論を導く上で重要な情報を追跡する必要がある。

組織は、機密性の高いデータを保護するための義務を果たすと同時に、情報の迅速な共有を可能にする手順を策定する必要がある。手順の策定にあたっては、情報を共有して効果がないリスクと、共有せずに保護されないリスクのバランスを考慮する必要がある。情報共有と追跡の手順は以下の通りである。

- 信頼できる人物・組織とすぐに共有可能な情報を識別する
- 機密情報が含まれると思われる脅威情報を見直し、サニタイズし、保護するプロセスを定める
- 機密データの漏えいに対処するための計画を定める
- 可能であれば脅威情報の取扱いと交換を自動化する
- 情報管理に関する指定の適用・監視・実行について文書化する
- 必要に応じ、非帰属情報交換を受け入れる
- 内外の脅威情報源を追跡する

情報取扱い手順には、全てのステークホルダーの役割、責任、権限が記載されている必要がある。また、手順では、意志決定者に情報が共有される流れと効果的な権限の委譲を可能とし、必要に応じて、外部コミュニティとの共同作業を可能とする必要がある。

3.5 共有コミュニティへの加入

組織は、既存の脅威情報を補完する情報源や、不足している情報を補完する情報源を検討し、共有パートナーを評価しなければならない。特定のタイプの情報のみを共有するコミュニティもあるため、複数の共有コミュニティに参加する必要がある可能性がある。

脅威情報は、公的・私的コミュニティ、政府データベース、自組織内部、有料情報源、オープンソースから取得できる。共有コミュニティは、共有する特性や関心を中心に構成されるこ

とがある。一方、地理・政治・産業分野、対象脅威等を目的にコミュニティを構成してもよい。また、多くのコミュニティは、様々な国から参加者が集まり、国際的に活動している。情報共有パートナーの例としては、ISAC、CERT・CSIRT、ISAO、DHS の AIS イニシアティブ、脆弱性収集機関、法執行機関、ISP、セキュリティサービスプロバイダー、サプライチェーン、業界セクターの同業者、ビジネスパートナー、顧客などが挙げられる。

コミュニティの中には、有志が運営する非公式なグループがある。この場合、正式な会員制度はなく、基本的な行動規範の下でのみ運営されている。また、共有される情報の質と正確性については保証されない。信頼度は提出者の評判に依存する。

一方で、公式の共有コミュニティは、以下のような会員制度を定めている。

・会費
・組織の資格要件
・個人の資格要件
・スポンサーシップの要件
・試用会員期間の要件
・コミュニティで受け付け、配信する情報の種類
・コミュニティでサポートする配信方式、フォーマット、プロトコル
・求められる組織のサイバーセキュリティ能力

公式のコミュニティでは、招待やスポンサーシップにより会員を募集しており、また会員は審査されている。このため、非公式のコミュニティよりも会員が安定している。公式のコミュニティでは、SLA、NDA、その他の合意により情報交換を規定する。いくつかのコミュニティでは会費を集めて運営を行っている。料金体系が階層化され、サービス内容が異なる場合がある。

組織は情報共有協定に参加する前に、以下の承認を受ける必要がある。

・情報共有活動を監視し、必要なリソースを管理するリーダーシップチーム
・法務チーム、または加入にあたっての権限を持つもの
・脅威情報の収集、保管、分析、公開、保護に関わるプライバシー担当者や主要な利害関係者

加入する共有コミュニティを選択する際には、共有される情報の種類やコミュニティの構造、影響力、会員になるためのコストを考慮するべきである。情報共有方法を評価する場合には、以下の点を考慮すべきである。

・コミュニティで共有される情報は組織に関連性があり、組織が持つ既存の情報を補完できるか
・コミュニティで共有される脅威情報は実行可能であるか
・非帰属情報を受け入れる仕組みと、提供者を保護する仕組みを持っているか
・脅威情報が適時性、信頼性を持ち、良質であるか
・コミュニティで使用される情報交換フォーマットが自組織内のシステムやツールと互換

性があるか
・コミュニティで共有される情報の頻度や量が、組織の処理能力に合致しているか

コミュニティで共有される情報の他にも、コミュニティと参加者の影響力についても考慮する必要がある。

・コミュニティの規模や構成（参加者数、情報供給者、情報消費者）
・コミュニティの活動実績（1 日当たりの情報共有数など）
・会員の審査方法
・会員の技術スキルや熟練度
・コミュニティのガバナンスモデル
・会員になるための初期費用及び継続費用
・コミュニティが使用する共有契約の種類
・共有契約が組織の目標、目的、ビジネスルールに一致するか
・コミュニティのデータ保持・廃棄ポリシー

コミュニティを調査する際には、現在や過去の会員に状況を聞き取り、コミュニティの信頼性を評価することが推奨される。

3.6 情報共有活動の継続的サポート計画

組織は、情報共有インフラのメンテナンスとユーザーサポートに対応したサポート計画を構築するべきである。この計画では、以下を実行するために必要な人員、資金調達、インフラ、プロセスを特定する必要がある。

・社内外の情報源からの情報を収集・分析する
・保護措置を実施し、展開する
・監視や脅威検出のシステムを構築し、展開する

組織は、情報の収集・保管・分析・普及のための継続的な運用サポートや、更新や、コミュニティに参加する上で、必要な人員、情報インフラ、及びトレーニングに資金を提供する必要がある。情報共有活動には継続的に資金を提供する必要があるが、脅威情報を効果的に使用すれば潜在的な攻撃に対するコストを大幅に削減することができる。

4. Participating in Sharing Relationships

情報共有コミュニティに参加した際の活動には、通常は以下の活動が含まれる。

・継続中のコミュニケーションへの関与（4.1 章）
・セキュリティ警告の消費と対応（4.2 章）
・インジゲータの消費と使用（4.3 章）
・インジゲータの整理と保存（4.4 章）
・インジゲータの作成と公表（4.5 章）

情報共有に参加し始めて間もない組織は、まず 1～2 個の活動に参加し、活動が成熟したら追加していくことを推奨する。組織は、情報共有活動が自身の基礎的なサイバーセキュリティ能力を代替するものではなく、拡充するものであるということを理解しなければならない。

4.1 継続中のコミュニケーションへの関与

情報共有コミュニティは、様々な方法で情報共有を行う。電子メール、Web ポータル等で情報共有を行う場合はインフラ投資を伴わないが、処理を手作業で行う必要がある。標準データフォーマットをサポートするツールを利用した場合は、半自動的に情報の収集・処理・利用が可能となるデータフィードを使用できる。会議やワークショップ等で情報共有を行う場合は、スタッフの出張が必要である。また、脅威情報を積極的に共有する場合、コミュニケーションコストが高くなる可能性がある。コミュニケーションは、インシデント発生時のみでも、隔週のレビュー・電話会議・年次会議等の定期的なものでもよい。

人間が判読可能な形式で配信されるメッセージの頻度や分量については、各コミュニティで異なる。最新の情報をできるだけ早く配信するよう求めるコミュニティもある。また、リアルタイムではなくある程度まとまったデータを求める場合もある。受信するメッセージを減らすために、個々のメッセージを受信するのではなく、一定間隔のダイジェストを受信するオプションを設けているコミュニティもある。

新たにコミュニティに加入した組織は、新しい情報源を既存のセキュリティ対策に統合してツールを設定するため、また、脅威情報をどのように解釈し行動する必要があるかについて意思決定者へ訓練を行うために時間が必要である。立ち上げ期間中は、組織はコミュニティが提供するガイダンスを参照し、既存会員の行動の観察し学び、コミュニティのサポートを利用するべきである。コミュニティが主催するトレーニングイベントでは、成熟度の低い組織や経験の浅い職員に対して、熟練者から実践的な訓練を受ける機会が提供される。

組織は、担当者がコミュニティ内で信頼関係をより高めるために、担当者の異動を減らすべきである。信頼関係を強固にするために、コミュニティへの継続的な参加が不可欠である。コミュニティが主催する電話会議や対面会議に積極的に参加することで信頼関係をより強固にし、共有の効果を高めることが可能となる。

4.2 セキュリティアラートの受信と対応

コミュニティは、新規脆弱性や悪用等のセキュリティ問題を通知するセキュリティアラートを公開することがある。US-CERT アラートや NVD 脆弱性アドバイザリ・ベンダーのセキュリティ情報等のセキュリティアラートに表示されるフィールドは次の通りである。

・簡単な概要とインジゲータを含む技術詳細

・影響を受けるプラットフォーム
・予測される影響
・深刻度（CVSS など）
・修正や暫定回避策等のオプション
・詳細を知るための参考文献
・アラートメタデータ（作成・変更日時、謝辞）

組織がセキュリティアラートを受信した場合、そのアラートの発信元が信頼できるか判断する必要がある。アラートの発信元が不明、または信頼できない場合、まず詳細な調査や確認を行う必要がある。アラートが信頼でき、組織のシステムやハードに適用される場合には適切な行動をする必要がある。

適切な対応を決める際には、アラートの重要度や影響を受けるシステムの数、攻撃が組織のミッションクリティカル機能に与える影響、軽減策を展開した場合の運用上の影響などを評価する必要がある。対応方法には、アラートからのインジゲータの特定と抽出、インジゲータを使用した検出シグネチャの開発と展開、構成の変更、パッチの適用、職員への通知、セキュリティ管理の実装や強化などが含まれる。インジゲータの抽出は主に手作業で行われている場合が多いが、自動化することで、データ操作よりも情報の解釈に集中することができる。

4.3 インジゲータの受信と利用

外部情報源からインジゲータを受信し、使用するには、以下の複数プロセスがある。

- **検証：**デジタル署名、暗号化ハッシュなどを用いてインジゲータの内容と出所の完全性を検証する
- **復号化：**暗号化されたインジゲータファイルやデータストリームを復号化する。
- **解凍：**圧縮されたファイルやデータストリームを解凍する
- **コンテンツ抽出:**インジゲータファイルを解析して、組織が関心を持つものを抽出する。
- **優先順位づけ：**相対的重要度、データの全体的な信頼度、特定の処理順序、データを実行可能な情報に変換する労力、その他の要因を踏まえた優先的なインジゲータの処理
- **分類：**インジゲータのメタデータを確認し、求められるセキュリティ要件と処理を決定する。機密情報には暗号化ストレージ、厳格なアクセス制御、情報配布の制限が必要な場合がある。

以上の活動は上記の順序で行われるが、運用要件やセキュリティ要件により異なる場合がある。可能なら、処理を自動化することで手作業を削減することが推奨される。インジゲータが電子メール等で非公式に共有されている場合、インジゲータの優先順位分けと分類分けは受信者が実行する必要がある。

理想的には、インジゲータは以下であるべきである。

- **即時的：**インジゲータはできるだけ早くで伝達されるべきであり、それにより対応を準備するための時間が生まれる。インジゲータの時間臨界性は、脅威の重大性、速度、普及の容易さ、対象のインフラ、使用された TTP、攻撃者の能力などの脅威特性に依存する。
- **関連的：**インジゲータは受信者の環境に適用可能なもので、組織が直面する可能性のある脅威に対処するものである必要がある。無関係な処理を行うことにより、優先順位づ

けや分類で余分な時間を使ってしまう。

- **正確：**インジゲータは正確で、完全で、明確でなければならない。不正確または不完全な情報は不確実性をもたらし、クリティカルな行動を妨げ、不必要な行動を起こし、無効な対応をもたらし、誤った安心感を喚起する可能性がある。インジゲータの精度に関する不確実性や注意事項について認識する必要がある。
- **特定：**インジゲータは、観察可能なイベントを明確に説明する必要がある。
- **行動可能：**インジゲータは、受信者が適切に対応策を作成できるように十分な情報と文脈を提供する必要がある。

独立した一つのインジゲータでは曖昧かもしれないが、他の情報源からの情報を集約するとインジゲータが豊富になり追加の情報が生まれる。複数の情報源からの情報は正確さや精度が異なる場合があるため、ユーザーが情報を評価し、品質や信頼性を表すタグを割り当てることが重要である。タグは、情報源の間の不一致を解決する際に特に重要である。組織がインジゲータを充実させると同時に、コミュニティ全体が利益を得られるよう、新たな知見を共有する必要がある。組織は、内外部で生成されたインジゲータを使用して、以下を行うことできる。

- ファイアウォール、侵入検知システム、データ損失防止システム、その他のセキュリティ管理で使用されるルールやシグネチャを追加または変更し、インジゲータ（ブラックリストの IP アドレスを含む接続等）に一致するアクティビティをブロックまたは警告する
- セキュリティ情報とイベント管理、ログ管理システムを設定し、セキュリティログデータの分析を支援する
- インジゲータを検索キーとして使用し、セキュリティログ、システム、その他のソースをスキャンして、既に侵害されている可能性のあるシステムを特定する
- 脅威の詳細を把握し、対応と復旧を早めるために、インシデントを調査する際に一致する記録を検索する
- セキュリティオペレーションセンターの分析官に追加の情報を提供する
- 脅威の特徴について担当者に教育する
- セキュリティ管理の変更が必要となるかもしれない脅威の傾向を特定する

一般に、外部情報源からのインジゲータを使用する際のモチベーションは、情報源の信頼性に強く影響される。信頼できる情報源からの情報はすぐに利用される可能性がある。一方で、信頼されない情報源からの情報は使用前に検証や追加分析、テストを必要とする場合がある。インジゲータの仕様は、サービス中断への組織の耐性などにも影響される。セキュリティを重視し、通常活動に影響が出ることを許容する組織や、サービスの可用性を重要視して、悪意のあるアクティビティが出て初めて監視を行う組織がある。

組織は、受信したインジゲータの特徴を慎重に検討して、インジゲータを最も効果的に使用する方法を決定するためのリスクベースのアプローチをとるべきである。あるインジゲータが、特定の状況には有用であるが、その他では有用でない場合がある。各組織がインジゲータを最大限に活用する方法を決めなければならない。

4.4 インジゲータの整理と保存

組織は、様々なソースよりインジゲータを収集することができる。使用方法により、インジゲータを知識ベースで整理する必要がある。Wiki などの自由方式は柔軟で、作業メモやインジゲータメタデータの開発に適している。構造化されたデータベースは、インジゲータを格納、整理、追跡、紹介、分析するのに有用である。

データベースに記録される情報には、一般に以下の情報が含まれる。

・インジゲータのソース
・インジゲータの仕様、共有ルール
・収集日時
・有効期間
・インジゲータに関連する攻撃が特定の組織や部門を対象としているかどうか
・CVE、CPE、CWE、CCE レコード
・インジゲータに関連付けられたグループや攻撃者
・関連する攻撃者のエイリアス
・攻撃者の TTP
・関連する攻撃の対象となる個人やそのタイプ
・攻撃対象のシステム

インジゲータのデータベース自体も攻撃対象となりうるため、アクセスコントロール、定期的なバックアップ、OS やアプリケーションの更新、セキュアな構成の検証、データベースに使用されるソフトウェアの生産に関するソフトウェア開発のベストプラクティスの参考、を行うべきである。

組織は、インジゲータや脅威情報の処分方針や手順を確立するべきである。この際、短期・長期の可用性に関してデータ保持要件を定義する必要がある。情報の取扱い・保存要件は、情報が証拠として採用されることで変わる場合がある。インシデントの調査中に求められる証拠は、証拠の提出に関する保管要件とその他の法令に従い、データの保存に関する最適な方法を使用して収集・保存する必要がある。情報の完全性を維持するための取扱いについては、NIST SP 800-86 や NIST SP 800-61 を参照するとよい。

証拠として必要とされないインジゲータについては、適切な保持方針を定める必要がある。情報の保持にはコストがかかる一方、歴史的価値や新規会員・パートナーが攻撃の進化を知ることができる。財務、契約、法律、規制上の問題等により、データの保存期間が数か月や数年に制限される可能性がある。計画に従い、組織はインジゲータをアーカイブや破棄する必要がある。

4.5 インジゲータの提供と公開

多くの組織はインジゲータを受信するだけだが、高度なセキュリティ機能を持つ組織では独自のインジゲータを作成し公開する場合がある。組織が脅威情報を生成することで、組織はより専門知識を得ることができ、他の組織と脅威に対応することで信頼関係を築くことができる。脅威情報の作成者は、情報に付属するメタデータの有無、使用するデータ形式、機密データの取扱い方法、情報共有ルールの更新方法を定める必要がある。

4.5.1 インジゲータの強化

インジゲータにはメタデータが含まれていなければならない。メタデータには情報の機密性や起源に関する情報が含まれる。インジゲータが作成、集約、強化されるにつれ、その機密性と分類は再評価されるべきである。

インジゲータの作成プロセスでは、公開、更新、消去の動作を提供する必要がある。自動化された仕組みでは、攻撃者の攻撃対象とならないように強化され、テストされるべきである。インジゲータを共有する組織では、フィードバックメカニズムを提供する必要がある。フィードバックをすることで、パートナーのレポート提出、改善提案、追加情報の要求が可能になる。

コミュニティ内で共有される情報の中には「現在調査中」とマークされるものがあり、収集後に共有をしないよう求めている。こうしたマークはまた、潜在的な攻撃者へ情報漏えいや、調査活動を妥協させる可能性のあるアクティブな情報収集活動をメンバーに禁止させている。一定期間後に共有や調査の制限が緩和される場合があり、マークを変更する仕組みがあると望ましい。

4.5.2 標準データ形式

インジゲータの交換に標準データ形式を使用することで、相互運用性が向上し、情報をより高速に交換できるようになる。より高速にインジゲータを交換する必要がある場合、標準データ形式の仕様が望ましい。

組織は、ユースケースを共有し、必要な機能を特定し、標準化開発機関にフィードバックを提供することにより、情報共有の標準化活動に参加することが推奨されている。組織は、使用状況を共有する重要な脅威情報を効果的にサポートし、高度な成熟度を示し、適用手法を広げ、幅広い製品や組織間の相互運用性を可能にするため、データフォーマットと交換プロトコルの改良を模索するべきである。

4.5.3 機密データの保護

組織が公表するインジゲータには機密性があるため、不正開示や改ざんを防ぐための適切な保護手段を使用する必要がある。インジゲータは、通信の暗号化、認証メカニズム、リポジトリの強化などの手法で保護できる。リポジトリが使用されている場合には、リポジトリ用の SLA を作成し、予想される可用性、セキュリティ姿勢の要件、許容されるポリシーを指定する必要がある。機密情報が含まれている可能性のあるインジゲータを作成する場合には適切な共有ルールに従う必要があり、共有ルールに従うことを同意し信頼されたコミュニティメンバーとのみ情報を共有する必要がある。

参考２．【運輸部門対象】情報共有の実態等に関するアンケート調査票

以下、あなたがご所属されている部署のシステムについてお聞きします。

１．所管するシステム全般の不具合情報の入手状況について

問1．あなたの所属部署が所管するシステムは、システム全般の不具合情報（サイバー攻撃の恐れを含む）を**どの組織から入手**していますか。（複数回答可）

【社内】　→　問３へ

□　社内の情報システムや情報セキュリティを所掌する部署

□　社内の運輸の安全を統括する部署

□　社内の総務を担当する部署（全社危機管理等）

□　その他（　　）

【社外（民間企業）】　→　問３へ

□　メーカー等[31]

□　自社グループのシステム関連会社

□　同業他社（同種システム担当者等）

□　その他（　　）

【社外（公的機関）】　→　**問２へ**

□　業界団体（日本民営鉄道協会等）

□　鉄道 CEPTOAR[32]または航空分野における CEPTOAR

□　内閣サイバーセキュリティセンター(NISC)

□　国土交通省

□　都道府県警察本部

□　独立行政法人情報処理推進機構(IPA)

□　一般社団法人 JPCERT コーディネーションセンター(JPCERT/CC)

【その他】　→　問３へ

□　その他（下の欄にご記入ください。）

[31] 鉄道分野：株式会社 京三製作所、日本信号株式会社等 / 航空分野：株式会社アマデウス・ジャパン、日本ユニシス株式会社等

[32] 重要インフラ事業者等の情報共有・分析機能及び当該機能を担う組織を、英語名称（Capability for Engineering of Protection, Technical Operation, Analysis and Response）の略称として、セプター（CEPTOAR）と呼んでいます(出典: www.nisc.go.jp)。

【該当なし】　　→　問 3 へ

□　特に入手していない

問2.（問 1 で**社外(公的機関)**のいずれかの選択肢を選択した方にお伺いします。）

社外の公的機関から入手したシステム全般の不具合情報（サイバー攻撃の恐れを含む）を**どこに展開**しますか。（複数回答可）

【所属部署内】

□　自部署内で共有

【所属部署外】

□　自社内の他の部署に転送

□　自社グループのシステム関連会社に転送

□　システムの保守を請け負う事業者に転送

□　社内のデータベース等に登録

□　その他（　　）

【展開しない・不明】

□　特に何もしないことが多い

□　わからない

２．所管するシステム全般の不具合情報の提供状況について

問3. あなたの所属部署が所管するシステムに不具合（サイバー攻撃の恐れを含む）が発生した後に、**自部署以外の組織へ情報を提供**していますか。

□　提供している　　□　提供していない

→　**問 3-1、問 3-2 へ**

問3-1.（問 3 で【提供している】を選択した方にお伺いします。）

所管するシステムで発生した不具合情報（サイバー攻撃の恐れを含む）を、**どの組織へ提供していますか**。（複数回答可）

【社内】

□　社内の情報システムや情報セキュリティを所掌する部署

□　社内の運輸の安全を統括する部署

□　社内の総務を担当する部署（全社危機管理等）

【社外（民間企業）】

□　メーカー等

□　自社グループのシステム関連会社

□　同業他社の同種システム担当者

【社外（公的機関）】

□　業界団体（日本民営鉄道協会等）

□　鉄道 CEPTOAR または航空分野における CEPTOAR

□　内閣サイバーセキュリティセンター(NISC)

□　国土交通省

□　都道府県警察本部

□　独立行政法人情報処理推進機構(IPA)

□　一般社団法人 JPCERT コーディネーションセンター(JPCERT/CC)

【その他（下の欄にご記入ください。】

問3-2.　(問 3 で【提供している】を選択した方にお伺いします。)

所管するシステムで発生した不具合情報（サイバー攻撃の恐れを含む）を、**どのようなタイミング**で**提供していますか**。

□　不具合（サイバー攻撃の恐れを含む）が発生した段階ですぐに提供

□　不具合（サイバー攻撃の恐れを含む）への仮対応を終えた段階で提供

□　不具合（サイバー攻撃の恐れを含む）への本対応を終えた段階で提供

□　定期的な会合等、機会がある際に提供

□　明示的に依頼を受けた際に提供

□　特に定められていない

□　その他（下の欄にご記入ください。）

（提供のきっかけ等）

ご協力ありがとうございました。

以上

参考３．【IT 部門対象】情報共有の実態等に関するアンケート調査票

１．セキュリティ情報の入手・提供の状況

[ここでは、一般的なシステム[33]のセキュリティ情報についてお聞きします。]

問1．現在、**あなたの所属する部署**は**一般的なシステム**のセキュリティ情報（インシデント情報、脆弱性情報、対策情報等）を、どの程度の**頻度**で**入手**していますか。

- □ １週間に１回 ⟶ 問２へ
- □ ２週間に１回 ⟶ 問２へ
- □ １か月に１回 ⟶ 問２へ
- □ ３か月に１回 ⟶ 問２へ
- □ 半年に１回 ⟶ 問２へ
- □ 半年に１回よりも低頻度 ⟶ 問２へ
- □ 入手していない ⟶ 問５へ

問2．現在、**あなたの所属する部署**は**一般的なシステム**のセキュリティ情報（インシデント情報、脆弱性情報、対策情報等）は、どのような**内容**の情報を**入手**していますか。（複数回答可）

- □ インジケータ
- □ サイバー攻撃傾向、手順、攻撃対象
- □ 脆弱性に関するセキュリティ情報
- □ 侵入検知シグネチャ
- □ 具体的対策（ルーター設定、ファイアウォール規則、Web フィルタ設定等
- □ その他（下の欄にご記入ください。）

問3．現在、**あなたの所属する部署**は**一般的なシステム**のセキュリティ情報（インシデント情報、脆弱性情報、対策情報等）を、どのような**組織**から**入手**していますか。（複数回答可）

- □ 社内の他部署
- □ 日本国内にある社外の組織
- □ 日本国外にある社外の組織
- □ わからない
- □ その他（下の欄にご記入ください。）

[33] 基幹システム（会計、販売、人事・給与等）、業務系システム（営業支援、個別原価管理等）、業務支援系システム（グループウェア、ナレッジ管理、情報共有、申請ワークフロー等）等

問4．**一般的なシステム**のセキュリティ情報（インシデント情報、脆弱性情報、対策情報等）の**情報の集約は、**どの**部署**が行っていますか。

- □ 情報システム・IT 部門 ⟶ 問 4-1 へ
- □ 社内の総務部署（全社危機管理） ⟶ 問 4-2 へ
- □ 社内の運行・運航の安全対策を統括する部署 ⟶ 問 4-2 へ
- □ セキュリティ対策委員会 ⟶ 問 4-2 へ
- □ 情報を集約する部署はない ⟶ 問 4-2 へ
- □ その他（下の欄にご記入ください。） ⟶ 問 4-2 へ

問4-1．（問 4 で【情報システム・IT 部門】を選択した方にお伺いします。）

一般的なシステムのセキュリティ情報（インシデント情報、脆弱性情報、対策情報等）をあなたの所属する組織以外に**転送した場合**、**対策の実施状況**について**報告**を受けていますか。

- □ 報告を受けている
- □ 報告を受けていないものもある
- □ 報告を受けていない

問4-2．（問 4 で【情報システム・IT 部門】**以外の選択肢**を選択した方にお伺いします。）

あなたの所属する部署で入手した**一般的なシステム**のセキュリティ情報に対してどのように**対応**しますか。（複数回答可）

- □ 情報の集約を行う部署にセキュリティ情報を転送する
- □ 情報システム・IT 部門（あなたの所属部署）内で対策を検討
- □ 自社内の他の部署にセキュリティ情報を転送し、対策の実施を検討してもらう
- □ 社内のデータベース等に登録する
- □ 特に何もしないことが多い
- □ その他（下の欄にご記入ください。）

⟶ 問 5 へ

[ここからは、運輸に関するシステムのセキュリティ情報についてお聞きします。]

問5. 現在、**あなたの所属する部署**は**運輸に関するシステム**のセキュリティ情報（インシデント情報、脆弱性情報、対策情報等）を、どの程度の**頻度**で**入手**していますか。

□ 1週間に1回 ⟶ 問6へ　□ 2週間に1回 ⟶ 問6へ
□ 1か月に1回 ⟶ 問6へ　□ 3か月に1回 ⟶ 問6へ
□ 半年に1回 ⟶ 問6へ　□ 半年に1回よりも低頻度 ⟶ 問6へ
□ 入手していない ⟶ 問9へ

問6. 現在、**あなたの所属する部署**は**運輸に関するシステム**のセキュリティ情報（インシデント情報、脆弱性情報、対策情報等）について、どのような**内容**の情報を**入手**していますか。（複数回答可）

□ インジケータ
□ サイバー攻撃傾向、手順、攻撃対象
□ 脆弱性に関するセキュリティ情報
□ 侵入検知シグネチャ
□ 具体的対策（ルーター設定、ファイアウォール規則、Web フィルタ設定等
□ その他（下の欄にご記入ください。）

問7. 現在、**あなたの所属する部署**は**運輸に関するシステム**のセキュリティ情報（インシデント情報、脆弱性情報、対策情報等）を、どの**組織**から**入手**していますか。（複数回答可）

□ 社内の他部署
□ 日本国内における社外の組織
□ 日本国外における社外の組織
□ わからない
□ その他（下の欄にご記入ください。）

問8. **運輸に関するシステム**のセキュリティ情報（インシデント情報、脆弱性情報、対策情報等）**の集約は、どの部署**が行っていますか。

- □ 情報システム・IT 部門 ⟶ 問 8-1 へ
- □ 社内の総務部署（全社危機管理） ⟶ 問 8-2 へ
- □ 社内の運行・運航の安全対策を統括する部署 ⟶ 問 8-2 へ
- □ セキュリティ対策委員会 ⟶ 問 8-2 へ
- □ 情報を集約する部署はない ⟶ 問 8-2 へ
- □ その他（下の欄にご記入ください。） ⟶ 問 8-2 へ

問8-1. （問 8 で【情報システム・IT 部門】を選択した方にお伺いします。）

運輸に関するシステムのセキュリティ情報（インシデント情報、脆弱性情報、対策情報等）をあなたの所属する組織以外に**転送した場合**、**対策の実施状況について報告**を受けていますか。

- □ 報告を受けている
- □ 報告を受けていないものもある
- □ 報告を受けていない

問8-2. （問 8 で【情報システム・IT 部門】**以外の選択肢**を選択した方にお伺いします。）

あなたの所属する部署で入手した**運輸に関するシステム**のセキュリティ情報に対してどのように**対応**しますか。（複数回答可）

- □ 情報の集約を行う部署にセキュリティ情報を転送する
- □ 情報システム・IT 部門（あなたの所属部署）内で対策を検討
- □ 自社内の他の部署にセキュリティ情報を転送し、対策の実施を検討してもらう
- □ 社内のデータベース等に登録する
- □ 特に何もしないことが多い
- □ その他（下の欄にご記入ください。）

⟶ 問 9 へ

２．自社の運輸システムがサイバー攻撃を受けた際の情報共有について

[ここでは、社内での情報共有についてお聞きします。]

問9. 自社の運輸に関するシステムが、**サイバー攻撃を受けた場合**（サイバー攻撃の恐れを含む）、**情報システム・IT 部門**と**当該システム担当部門間**で**情報共有**はできていますか。

□ できている ⟶ 問 9-1 へ　□ 情報によってできているものもある ⟶ 問 9-1 へ

□ できていない ⟶ 問 11 へ　□ わからない ⟶ 問 11 へ

問9-1. （問 9 で【できている】【情報によってできているものもある】のいずれかの選択肢を選択した方にお伺いします。）

情報共有で得た情報を元に、**情報システム・IT 部門**ではどのような**立場**で対応していますか。（複数回答可）

□ 直接対策する　□ 対策を支援する

□ 必要な情報収集を行う　□ わからない

□ その他（下の欄にご記入ください。）

[ここからは、社外との情報共有についてお聞きします。]

問10. 自社の運輸に関するシステムが、**サイバー攻撃を受けた場合**（サイバー攻撃の恐れを含む）、**あなたの所属する組織から社外**に情報を**提供**したことがありますか。

□ 提供した ⟶ 問 10-1 へ　□ 提供していない ⟶ 問 11 へ

問10-1. (問 10 で【提供した】を選択した方にお伺いします。)

自社の運輸に関するシステムが、**サイバー攻撃を受けた場合**（サイバー攻撃の恐れを含む）、**業法に定められた報告以外で、**どのような**社外の組織**にセキュリティ情報を**提供**していますか。（複数回答可）

【企業】

□ メーカー等

□ 自社グループのシステム関連会社

□ 同業他社（同種システム担当者等）

【公的機関】

□ 業界団体（日本民営鉄道協会等）　□ 都道府県警察本部

□ 内閣サイバーセキュリティセンター(NISC)　□ 国土交通省

□ 独立行政法人情報処理推進機構(IPA)　□ サイバー情報共有イニシアティブ(J-CSIP)

□　一般社団法人 JPCERT コーディネーションセンター(JPCERT/CC)

□　日本シーサート協議会(NCA)

□　鉄道 CEPTOAR または航空分野における CEPTOAR

□　その他（下の欄にご記入ください。）

問10-2. (問 10 で【提供した】を選択した方にお伺いします。)

自社の運輸に関するシステムが、**サイバー攻撃を受け不具合が発生した際**、どのような**タイミング**で社外に情報を**提供**していますか。

□　不具合（サイバー攻撃の恐れを含む）が発生した段階ですぐに提供

□　不具合（サイバー攻撃の恐れを含む）への仮対応を終えた段階で提供

□　不具合（サイバー攻撃の恐れを含む）への本対応を終えた段階で提供

□　定期的な会合等、機会がある際に提供

□　明示的に依頼を受けた際に提供

□　特に定められていない

□　その他（下の欄にご記入ください。）

（提供のきっかけ等）

３．ISAC について

金融、ICT 及び電力分野では、民間企業主導でサイバーセキュリティに関する情報を共有・分析するISAC[34]と呼ばれる組織が立ち上がり、当該分野の事業者が参加し、様々な活動を実施しています。

問11．ISAC の活動に期待しますか。

□ 期待する ⟶ 問 11-1 へ　□ 期待しない ⟶ 問 11-2 へ

問11-1．**ISAC** に**期待する**活動をお答えください。（複数回答可）

□ サイバー攻撃に関する情報を共有すること
□ 人材育成の方法を共有すること
□ システム共通の安全対策を検討すること
□ 他分野の ISAC 等との連携をすること
□ インシデント対応演習等を実施すること
□ カンファレンスや講演会を開催すること
□ ガイドライン文書を作成すること
□ 交通分野を狙った新たなサイバー攻撃についてまとめたレポートを発行すること
□ その他（下記にご記入ください。）

問11-2．**ISAC の活動**に**期待しない**理由を下記にご記入ください。

問12．ISAC ができた場合、ISAC 加盟メンバーとして、鉄道・航空事業者の他に**どのような企業**が加盟すると有効な**情報共有ができる**と考えられますか。加盟するとよいと考えられる企業を全てお答えください。（複数回答可）

□ 鉄道・航空事業者のグループ企業
□ 鉄道・航空事業者が委託しているメーカー等
□ 鉄道・航空事業者のみが加盟すればよい
□ その他（下記にご記入ください。）

[34] 分野内における情報共有・連携を促進するための組織(ISAC: Information Sharing and Analysis Center) (出典: www.nisc.go.jp)

４．ランサムウェア「WannaCry」に関連する情報共有状況

ランサムウェアによって影響を受けたドイツ鉄道のディスプレイ出典: @ZEICHENTATEN/TWITTER

問13. ランサムウェア「WannaCry」による被害状況・要因・対策等について、**社外から情報を得ました**か。
（複数回答可）

- □ 同業他社から情報を入手した ⟶ 問 13-1 へ
- □ 自社システムベンダーから情報を入手した ⟶ 問 13-1 へ
- □ 他業界の他社から情報を入手した ⟶ 問 13-1 へ
- □ 公的機関から情報を入手した ⟶ 問 13-1 へ
- □ 情報を入手しなかった ⟶ 設問は以上です。

問13-1. （問 13 で【情報を入手しなかった】**以外の選択肢**を選択した方にお伺いします。）
入手した情報を元に、貴社では**対策を実施**しましたか。

□ 対策を実施した　　□ 対策を特に実施しなかった

ご協力ありがとうございました。

以上