資料８

関係省庁の取組状況について

【金　融　庁】

資料８－１　金融庁におけるサイバーセキュリティ施策の取組状況について

【総　務　省】

資料８－２　総務省におけるサイバーセキュリティ施策の取組状況について

【厚生労働省】

資料８－３　医療・水道分野におけるサイバーセキュリティに関する取り組み

【経済産業省】

資料８－４　経済産業省におけるサイバーセキュリティ施策の取組状況について

【国土交通省】

資料８－５　国土交通省におけるサイバーセキュリティ施策の取組状況について

資料８－１

金融庁におけるサイバーセキュリティ施策の取組状況について

2022年５月

金融庁総合政策局リスク分析総括課サイバーセキュリティ対策企画調整室

サイバーセキュリティに関する自己評価の促進

課題	地域金融機関（①地域銀行、②信用金庫、③信用組合）が、他の金融機関対比で、自組織の位置付けや改善すべき領域を特定するために適したツールが存在しない。
対応	金融庁、日本銀行、FISCで、地域金融機関向けのサイバーセキュリティに関する自己評価ツールを共同開発する。
活用方法	地域金融機関の自己評価結果を収集・分析し、その結果を還元することで、地域金融機関のサイバーセキュリティ管理の自律的な高度化を促す。

資料８－２

総務省におけるサイバーセキュリティ施策の取組状況について

2022年５月

総務省サイバーセキュリティ統括官室

（１）電気通信事業法の一部を改正する法律案（概要）

➢ 電気通信事業を取り巻く環境変化を踏まえ、電気通信サービスの円滑な提供及びその利用者の利益の保護を図るため、以下の措置を講ずる（令和４年３月４日閣議決定、国会提出）。

情報通信インフラの提供確保

■ ブロードバンドサービスについては、契約数が年々伸び、「整備」に加え、「維持」の重要性も高まっている。

■ 新型コロナウイルス感染症対策を契機とした社会経済活動の変化により、テレワークや遠隔教育などのデジタル活用の場面が増加している。

※ デジタル田園都市国家構想の実現のためにも、ブロードバンドの全国整備・維持が重要。

■ 一定の**ブロードバンドサービスを基礎的電気通信役務（ユニバーサルサービス）に位置付け**、不採算地域におけるブロードバンドサービスの安定した提供を確保するための**交付金制度を創設**する。

■ 基礎的電気通信役務に該当するサービスには、**契約約款の作成・届出義務、業務区域での役務提供義務等**を課す。

②

①

安心・安全で信頼できる通信サービス・ネットワークの確保

■ 情報通信技術を活用したサービスの多様化やグローバル化に伴い、情報の漏えい・不適正な取扱い等のリスク※が高まる中、事業者が保有するデータの適正な取扱いが一層必要不可欠となっている。

※ 国外の委託先から日本の利用者に係るデータにアクセス可能であった事案などが挙げられる。

■ 大規模な事業者※ が取得する**利用者情報について適正な取扱い**を義務付ける。

■ 事業者が利用者に関する情報を第三者に送信させようとする場合、**利用者に確認の機会を付与**する。

※ 大規模な検索サービスまたはSNSを提供する事業についても規律の対象とする。

電気通信市場を巡る動向に応じた公正な競争環境の整備

■ 指定設備（携帯大手３社・NTT東・西の設備）を用いた卸役務が他事業者に広く提供される一方、卸料金に長年高止まりとの指摘がなされている。

■ ＮＴＴ東・西が提供する固定電話について、従来の電話交換機網からＩＰ網への移行を令和３年１月に開始、令和７年１月までの完了を予定している。

■ 携帯大手３社・NTT東・西の指定設備を用いた卸役務に係るMVNO等との協議の適正化を図るため、**卸役務の提供義務**及び**料金算定方法等の提示義務**を課す。

■ 加入者回線の占有率（50%）を算定する区域を都道府県から**各事業者の業務区域（例えばNTT東は東日本、NTT西は西日本）**へ見直す。

上記のほか、認定送信型対電気通信設備サイバー攻撃対処協会（認定協会）の業務の追加、重大事故等のおそれのある事態の報告制度の整備等を行う。

電気通信事業ガバナンス検討会　第18回会合（令和４年４月15日）資料18-２より抜粋・一部編集

（１）① 利用者に関する情報の適正な取扱いに係る制度整備

大量の情報を取得・管理等する電気通信事業者を中心に、諸外国における規制等との整合を図りつつ、利用者に関する情報の適正な取扱いを促進するための新たな規律を整備。

	【 現状・課題 】	【 規律の内容 】
利用者情報の適正な取扱い	➢ **デジタル変革時代のイノベーションを促進**するため**安心・安全な電気通信サービスの確保**が不可欠 ➢ **諸外国の法的環境の変化、サイバー攻撃の複雑化**により、利用者が安心して利用できる電気通信サービスの提供の確保が急務 ➢ 特に、**大量の利用者情報を取り扱う事業者**には一層の高い信頼性の確保が必要	**1. 利用者の利益に及ぼす影響が大きい電気通信事業者（例：利用者数1000万人以上）に対する義務** 利用者情報を守るための必要最小限の規律 ／ 効果 ・利用者情報※の取扱いに関する**社内ルール**（取扱規程）**の策定**、利用者情報の**取扱方針の公表等**（記載事項例：安全管理の方法等） ⇒ **電気通信サービスの高い信頼性を保持**するとともに、**利用者自らが安心して利用できるサービスを選択**することが**可能となる** ・利用者情報の取扱いに関する**自己評価**、取扱規程・取扱方針への反映 ⇒ **自ら PDCAを実施して、各事業者の実態を踏まえた情報の適正な取扱い体制を確保** ・利用者情報の**統括責任者**の選任等 ⇒ **全体的観点からの適切な判断や、情報漏えい時の迅速な対応が可能となる** ※ 利用者に関する情報のうち、通信の秘密に該当する情報、役務契約を締結又はID等により利用登録をした利用者の情報を想定。 **大規模な検索サービス**または**SNS**を提供する事業についても規律の対象とする。
利用者の情報の外部送信	➢ 利用者がアプリやwebサイトを利用する際、タグ等により、**利用者の意思によらず第三者に自身の情報が送信**されている場合がある	**2. 電気通信事業者※に対する義務** ・利用者に電気通信サービスを提供する際に、**情報を外部送信**する指令を与える電気通信を送信する場合、**確認の機会を付与** ⇒ 利用者が意図しない情報の外部送信がなくなり、**利用者が安心して電気通信サービスを利用することが可能となる** ※ 電気通信設備を用いて他人の通信を媒介する電気通信役務以外の電気通信役務を電気通信回線設備を設置することなく提供する電気通信事業（電気通信事業法第164条第1項第3号）を営む者を含む。利用の状況からみて利用者に与える影響が少なくない者に限る。

電気通信事業ガバナンス検討会　第18回会合（令和４年４月15日）資料18-２より抜粋・一部編集

（１）② 電気通信サービスの停止に関するリスクの対応に係る制度整備

事業者間連携によるサイバー攻撃対策や事故報告制度について、電気通信役務の安定的な提供の確保を目的とした規律を整備。

	【 現状・課題 】	【規律の内容 】	
事業者間連携によるサイバー攻撃対策	➢ サイバー攻撃では、指令元、攻撃元、攻撃先が複数のISPにまたがる場合が多く、ISP間の連携協力が必要	・これまではサイバー攻撃の発生後に限られていた**ISP間の情報共有や分析をサイバー攻撃の発生前にも実施できるようにするための環境を整備**	ISP間の連携が促進され、**より機動的なサイバー攻撃対策が可能に**
重大事故等のおそれのある事態の報告制度	➢ 電気通信サービスの事故原因が多様化※ ※ 設備の設定（通信経路等）の誤り、他者の提供する設備やサービスの不具合等 ➢ 電気通信サービスの停止が社会に及ぼす影響の増大	・これまでの重大事故等が生じた際の遅滞のない報告に加え、**重大事故等のおそれのある事態に関する報告制度を整備**	より精緻な実態把握や原因分析等が可能となり、**重大な事故等の発生の未然防止や被害軽減に寄与**

電気通信事業ガバナンス検討会　第18回会合（令和４年４月15日）資料18-２より抜粋・一部編集

（２）実践的サイバー防御演習（CYDER）

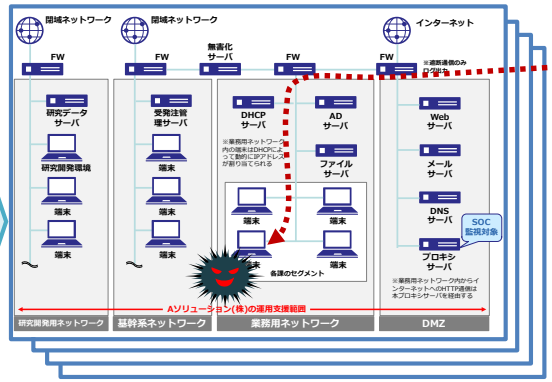
CYDER：CYber Defense Exercise with Recurrence

- 総務省は、情報通信研究機構(NICT)を通じ、**国の機関**、**指定法人**、**独立行政法人**、**地方公共団体**及び**重要インフラ事業者等**の情報システム担当者等を対象とした体験型の**実践的サイバー防御演習(CYDER)**を実施。
- 受講者は、**チーム単位で演習に参加。組織のネットワーク環境を模した大規模仮想LAN環境下で、実機の操作を伴って**サイバー攻撃によるインシデントの検知から対応、報告、回復までの**一連の対処方法を体験。**
- **全都道府県**において、年間**100回・計3,000名規模**で実施。　参加申込 → https://cyder.nict.go.jp

演習のイメージ

我が国唯一の情報通信に関する公的研究機関である**NICTが有する最新のサイバー攻撃情報を活用**し、実際に起こりうるサイバー攻撃事例を再現した**最新の演習シナリオ**を用意。

北陸StarBED技術センターの大規模高性能サーバ群を活用



擬似攻撃者

企業・自治体の**社内LANや端末を再現**した環境で演習を実施

受講チームごとに独立した演習環境を**構築**

演習模様 **専門指導員**による補助

チーム内での議論を通じた相互理解

本番同様のデータを使用した演習

インシデント（事案）対処能力の向上

令和４年度の実施計画（予定）

コース名	演習方法	レベル	受講想定者（習得内容）	受講想定組織	開催地	開催回数	実施時期
A	集合演習	初級	システムに携わり始めた者 (事案発生時の対応の流れ)	全組織共通	４７都道府県	６４回	７月～翌年２月
B-1		中級	システム管理者・運用者 (主体的な事案対応・ｾｷｭﾘﾃｨ管理)	地方公共団体	全国１１地域	２０回	10月～翌年１月
B-2				地方公共団体以外	東京・つくば・大阪・名古屋	１３回	翌年１月～２月
C		準上級	セキュリティ専門担当者 (高度なセキュリティ技術)	全組織共通	東京	３回	10月～翌年２月
オンライン	ｵﾝﾗｲﾝ演習	-	A, Bコースの予習	全組織共通	（受講者職場等）	随時	５月～７月
			Aコースの復習				翌年１月～２月

（2）出前CYDER及びCYDERサテライトの導入

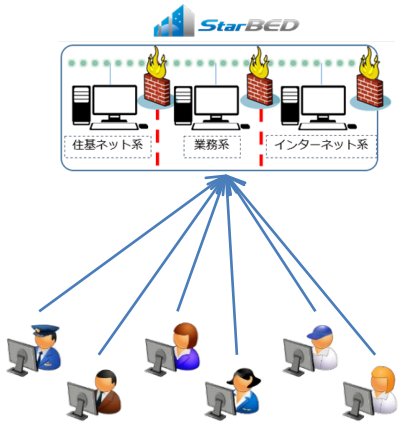
CYDER 集合演習【30人／回】

- 各会場に講師・補助者を手配して、実機演習環境を準備した上で実施

＋

CYDER オンライン演習

- 形態
  - ✓個人単位での遠隔接続による実機演習
  - ✓録画済み教材
  - ✓機材は受講者手配
- R3年度から本格実施



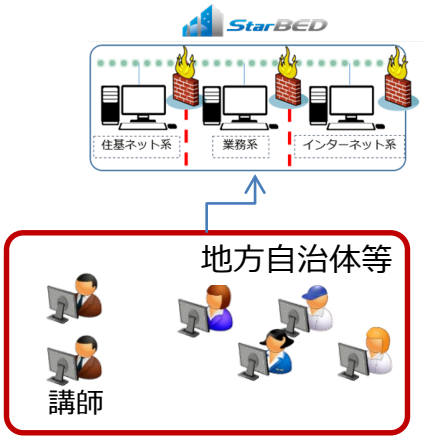
新規実施予定

小規模・柔軟化

2ヶ所

出前CYDER【10 人／カ所】

- ✓**未受講自治体の解消**にフォーカス
- ✓ 地方自治体等での遠隔接続による実機演習
- ✓ 講師が現地指導にてサポート
- ✓ 自治体等の受講者需要に応じて臨機応変に開催
- ✓ 機材貸与も選択可能

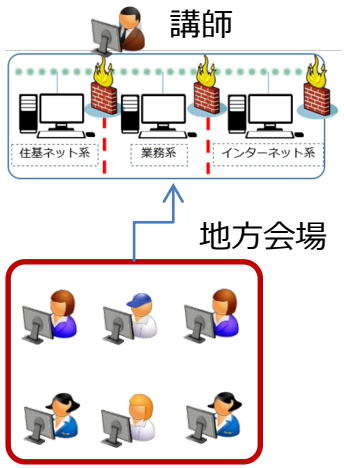


高効率化

1ヶ所

CYDERサテライト

- ✓**集合演習費用の効率化**（実施費用低廉化）にフォーカス
- ✓ サテライト会場からの遠隔接続による実機演習
- ✓ 講師は中央に、遠隔会場には補助者が支援
- ✓ ボトルネックの講師を柔軟に活用
- ✓ 機材貸与も選択可能



資料８－３

厚生労働省 ひと、くらし、みらいのために Ministry of Health, Labour and Welfare

医療・水道分野におけるサイバーセキュリティに関する取り組み

厚生労働省政策統括官（統計・情報政策、労使関係）付
サイバーセキュリティ担当参事官室

Ministry of Health, Labour and Welfare of Japan

医療・水道分野におけるサイバーセキュリティに関する取り組み

課題

重要インフラ事業者のICTへの依存度が高まるにつれ、サイバー攻撃に対するセキュリティを含むサイバーセキュリティへの取組の必要性が増大してきている。また、特に医療分野においては、ランサムウェア等の「外部からの攻撃」が増加傾向にあり、個々の事業者での単独対策には限界がでてきている。

医療分野

これまでの対応

- 病院における医療情報システムのバックアップデータ及びリモートゲートウェイ装置に係る調査の実施
- 上記調査を踏まえ、令和４年３月に医療情報システムの安全管理に関するガイドラインを改定
- 医療分野におけるサイバーセキュリティ対策調査事業を実施し、医療分野におけるISACの設立に向けた検討を実施

水道分野

これまでの対応

- 水道分野における情報セキュリティガイドライン（第４版）を平成31年３月に策定
- 水道施設の技術的基準を定める省令の一部改正し、水道施設の施設基準においても、サイバーセキュリティ対策を強化するために必要な措置を講じる旨を規定

今後の対応

- 重要インフラの情報セキュリティ対策に係る第４次行動計画の改定が予定されており、必要に応じて各種ガイドラインの改訂を検討

病院における医療情報システムのバックアップデータおよびリモートゲートウェイ装置に係る調査（概要）

第28回重要インフラ専門調査会

厚生労働省提出資料より抜粋（一部修正）

目　的

医療機関に対するランサムウェアなどのサイバー攻撃が増加し、長期にわたり診療が停止した事例等が確認されていることから、病院におけるランサムウェアのリスクを把握するとともに、早急に長期に診療が停止することがないよう有効な対策の実施を促すため、病院が保有する医療情報システムの保守等に用いられるリモートゲートウェイ装置の有無とそのアップデート状況及び電子カルテシステムのバックアップ保持の実態についての調査を行う。

調査方法・対象

- G-MISを用いて、リモートゲートウェイ装置及びバックアップ保持の実態に関する調査を実施する。（問数は10～15問程度）
- 調査対象は、G-MIS IDが付与されている、約8300の病院。

スケジュール

調査期間：令和４年１月28日～令和４年２月14日、令和４年３月８日～令和４年３月24日（予備）

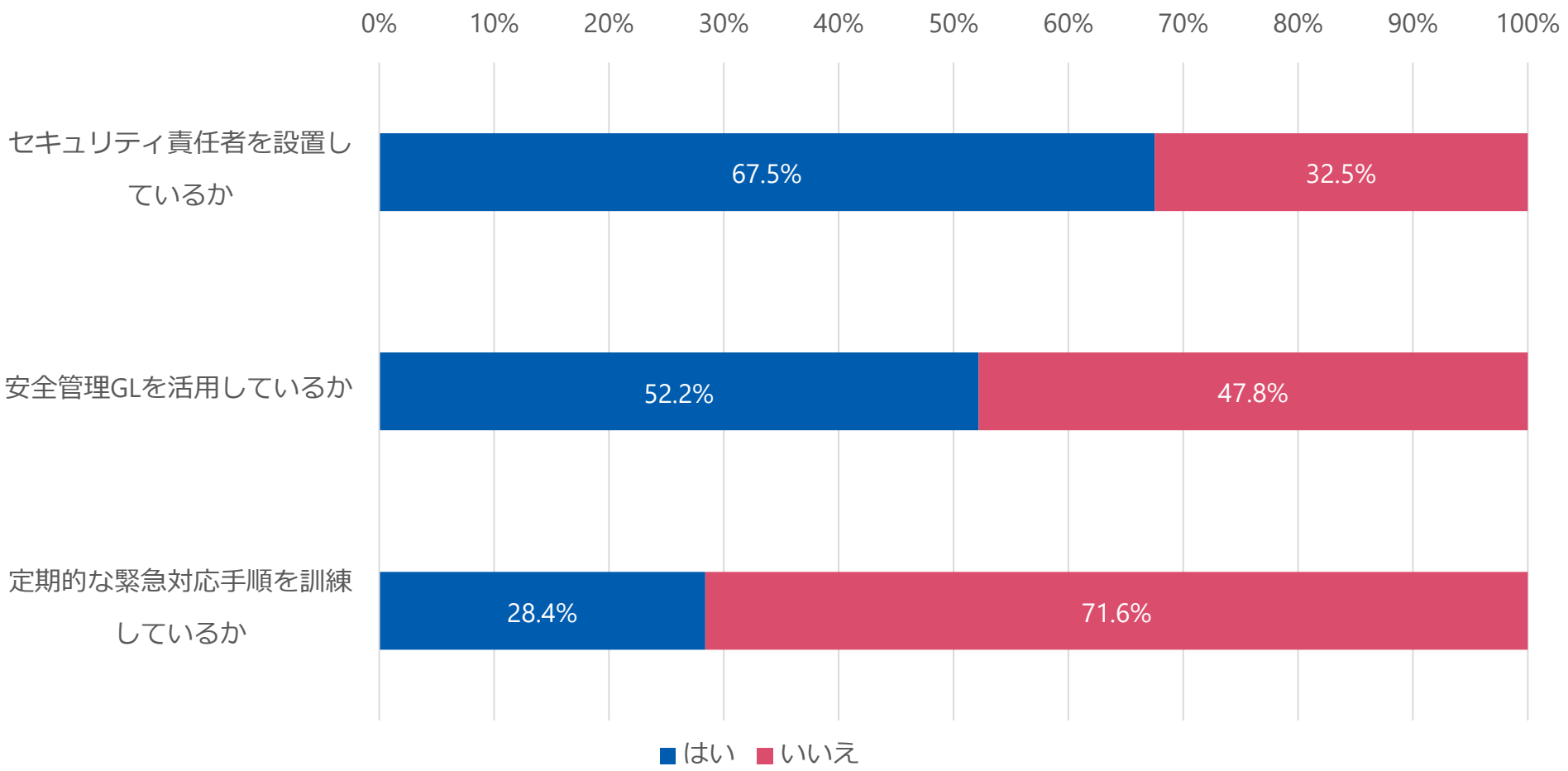
第10回医療等情報利活用
ワーキンググループ

資料2より抜粋

調査結果について

調査対象医療機関数：8,252施設

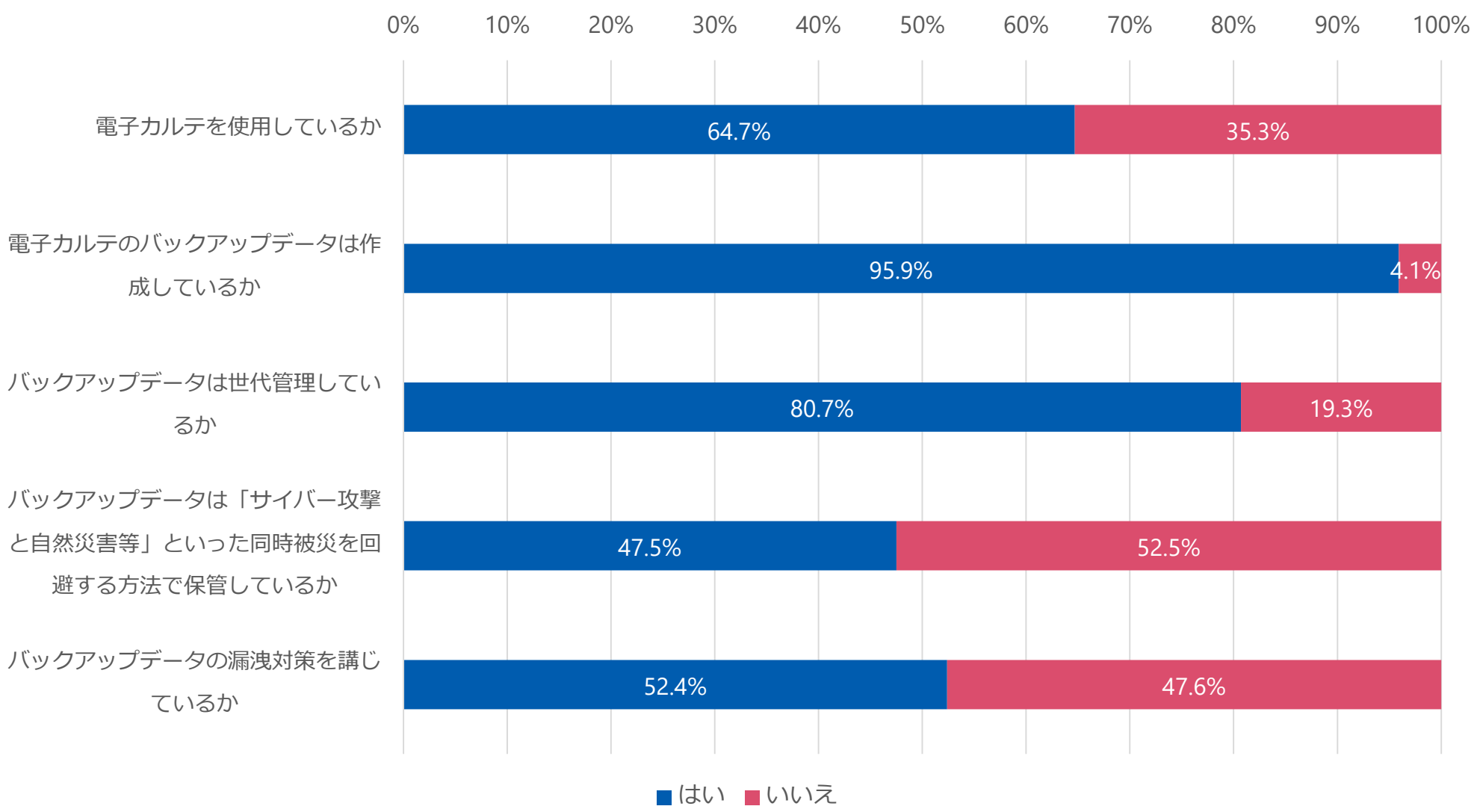
有効回答数　　：6,216施設（回答率：75.3%）



調査結果について（電子カルテシステムのバックアップについて）

第10回医療等情報利活用ワーキンググループ

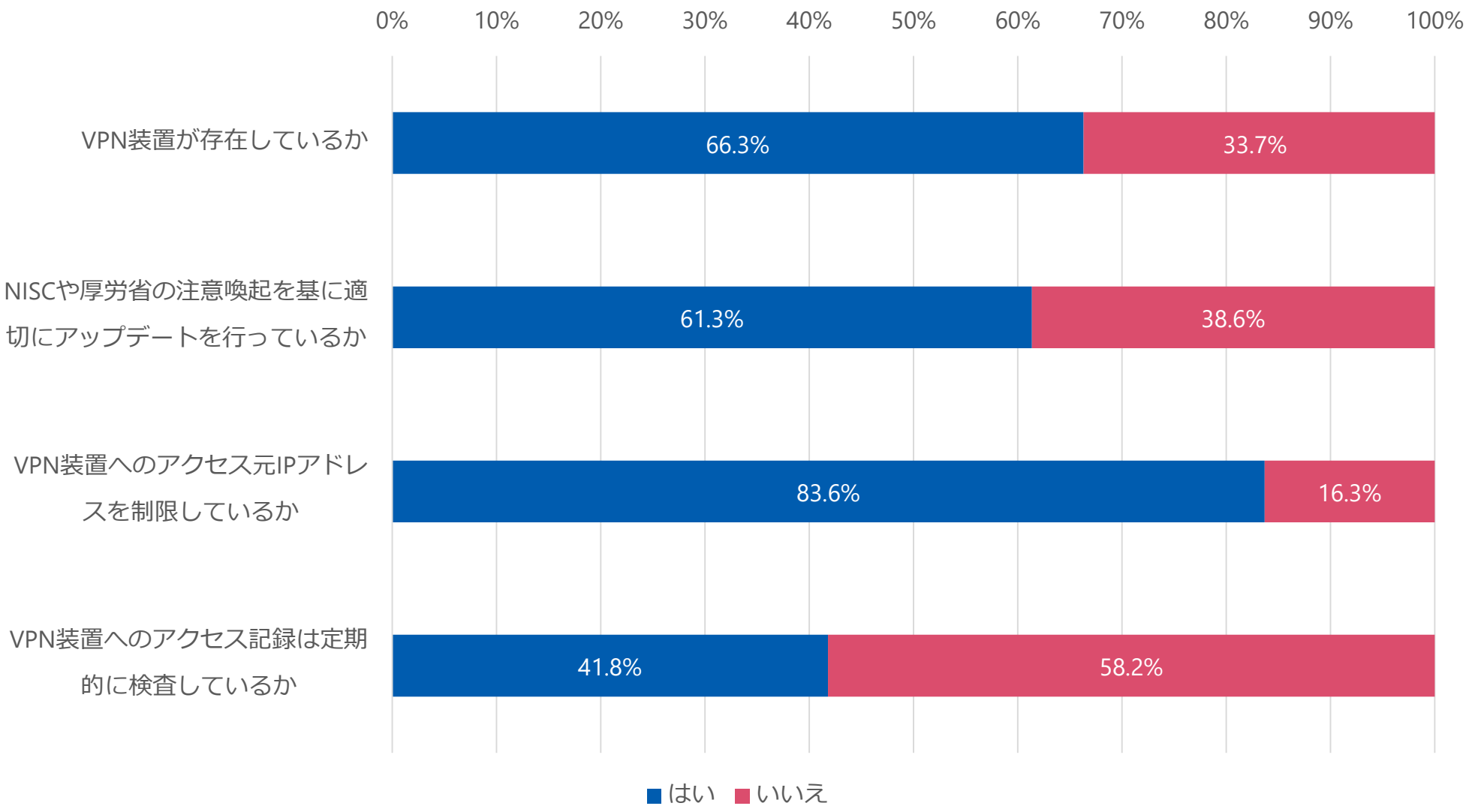
資料2より抜粋



※バックアップデータ作成に関する質問（2項目）以降ついては、電子カルテを導入している64.7%（4,020施設）が母数となっている。

調査結果について（リモートゲートウェイ装置について）

第10回医療等情報利活用ワーキンググループ
資料2より抜粋



※VPN装置のアップデートに関する質問（2項目）以降については、VPN装置が存在する66.3%（4,120施設）が母数となっている。

医療における情報セキュリティ インシデント事例（一部）

【参考】

第28回重要インフラ専門調査会

第3回健康・医療・介護情報利活用検討会医療情報ネットワークの基盤に関するワーキンググループ

参考資料５より抜粋。

2015.11.27　菰野厚生病院（三重県）：医事システムの端末がウイルス感染。インターネット利用中に感染し、ウイルスが院内ネットワークを通じてサーバーに侵入。サポート終了したOS(Windows XP)を使用していたことも原因の一つ。

2017

2016.01.14　鳥取県立中央病院（鳥取県）：庁内LANパソコン１台が、外部からのウイルスメールによりコンピュータウイルスに感染し、保存されていた3,152個の電子ファイルがコンピュータウイルスにより、開くことができなくなった。

2017.08～2018.01　福島医大病院（福島県）：コンピューターウイルス感染により検査装置が不具合を起こし、患者へのコンピューター断層撮影(CT)などをやり直すトラブルが起きた。

2018

2018.10.16　宇陀市立病院（奈良県）：電子カルテを含む医療情報システムがコンピュータウイルスに感染し、一部のデータが暗号化され、患者カルテが参照できなくなった。外部と接続されていないはずの医療情報システムが外部と接続された状況になり、ウイルスの侵入・感染に至った可能性が高いとの指摘。

2019

2019.05.20　多摩北部医療センター（東京都）：職務用パソコン端末へ送信された不正アクセスを意図したメールの添付ファイルを開封した結果、マルウェアに感染し、メールボックス内に不正アクセスされ、メールボックス内の情報の一部が流出した。

2019.11.01　徳島大学病院（徳島県）：海外出張の際にパソコン及び業務用携帯電話の収められたカバンの盗難被害が発生した。当該パソコンに患者の症例情報（3,201件）等、業務用携帯電話に職員氏名・業務用電話番号（約1,000件）が保管されていた。

2020

2021.04.30　千葉大学医学部附属病院（千葉県）：患者586名の個人情報を個人用パソコンに保存し、大学で許可されていないクラウドサービスを利用していたところ、宅配業者を装ったフィッシングメールによりクラウドサービス用ID・パスワードを盗み取られ、個人情報を閲覧できる状態になっていた。

2021

2021.05.31　市立東大阪医療センター（大阪府）：医用画像参照システムに不正アクセスがあり、システムが利用できなくなった。

2021.10.31　つるぎ町立半田病院（徳島県）：電子カルテがランサムウェアに感染し、システムが利用できなくなった。

医療における情報セキュリティに関する脅威やインシデント

【参考】

第28回重要インフラ専門調査会

第3回健康・医療・介護情報利活用検討会医療情報ネットワークの基盤に関するワーキンググループ

参考資料５より抜粋。

近年、「外的要因」かつ「意図的な事象」に脅威・インシデントの傾向が変化しつつある

外的要因

外部事業者等によるミス

・外部事業者の情報紛失
・外部事業者の設定ミス

等

(事例)
・外部事業者の設定ミスにより、患者70人分の個人情報が含まれたファイルがインターネットを経由しアクセス可能な状態となり、個人情報が漏洩する恐れがあった。

外部からの攻撃

・Webサイト、保守回線等を経由した攻撃
・ランサムウエアやマルウエアなど、システムの様々な脆弱性を利用した攻撃

等

近年、「外部からの攻撃」が増加傾向にあり、医療機関個々での単独対策には限界がある。

偶発的

意図的

職員によるミス

・USBメモリやPCの紛失・盗難
・FAXやメールの誤送信
・誤操作によるファイルのアップロード

等

(事例)
・医師が患者約330人分の手術記録を保存したUSBメモリを紛失した。
・薬剤師が、糖尿病・内分泌代謝内科を受診した患者3,835人の氏名や生年月日などの個人情報を保存したUSBメモリを紛失した。

内部不正

・職員による、機密情報、個人情報等の持ち出し
・委託事業者による機密情報、個人情報等の持ち出し

等

(事例)
・元職員が、在職中に患者の個人情報を持ち出し、新しく開設する介護事業所の案内状送付に利用した。

内的要因

参照：https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/iryou/johoka/cyber-security.html

【参考】③
海外のヘルスケア分野における情報セキュリティ インシデント事例 等

【参考】

2016.02.15　アメリカ・ハリウッドにあるHollywood Presbyterian医療センターで、サイバー犯罪者による攻撃を受け、
病院のデータを人質にして、9000枚のビットコイン（約340万ドル相当）を要求された。
急を要する患者については救急車で移送が行われ、病院の職員は紙とペンで患者のカルテを記録し、各部門はファックスでやりとりをせざるを得なくなっており、病院のメールサーバーがダウンしたため、患者は検査結果を確認するために、病院に出向くことにもなった。

2020.09　ドイツ・デュッセルドルフ大学病院でランサムウェアによりシステムが停止が発生した。
同病院で救命処置を受ける予定だった患者を受け入れることができず、別の病院に搬送された。

2021.05　アイルランドの公的医療サービスを提供するHealth Service Executive（HSE）のシステムの一部が、
ランサムウェアグループContiによる攻撃で、停止した。これにより、一部の外来患者の予約がキャンセルされた。
なお、Contiは「Apache Log4j」の脆弱性を利用していた。

第28回重要インフラ専門調査会

第3回健康・医療・介護情報利活用検討会医療情報ネットワークの基盤に関するワーキンググループ

参考資料５より抜粋。

The health sector and in particular the vaccine rollout was a major focus for the NCSC, with the organisation's world-leading services protecting NHS, healthcare, and vaccine supplier IT systems from malicious domains billions of times.

（NCSC英国家サイバーセキュリティセンター 年次レビュー）

参照： https://www.ncsc.gov.uk/news/record-number-mitigated-incidents
https://japan.zdnet.com/article/35179996/

医療機関におけるサイバー攻撃の現状

第28回重要インフラ専門調査会
厚生労働省提出資料より抜粋

【参考】

医療機関からの報告について

○ 平成19年3月から、「医療情報システムの安全管理に関するガイドライン」に基づき、医療機関等においてサイバー攻撃等のインシデント事案が発生した場合は、当該医療機関等から厚生労働省等の所管官庁へ報告することを求めている。

○ また、都道府県等に対しては、平成30年10月に通知（「医療機関等におけるサイバーセキュリティ対策の強化について」（医政総発1029 第1号　医政地発1029 第3号　医政研発1029 第1号　平成30年10月29日））を発出し、必要に応じて管内の医療機関等における被害状況、対応状況等に係る調査及び指導を行うとともに、厚生労働省へ報告することを求めている。

診療に及ぼす影響について

1. 一般に、ランサムウェアによるサイバー攻撃は**情報の暗号化**と**情報の詐取**と**金銭の要求**がセットとなっていることが多いが、**情報の詐取が確認された場合には個人情報漏洩事案となる**。

   ※ 令和2年改正個人情報保護法において、不正アクセス等による個人情報の漏えい（疑いを含む）については、件数に関わりなく個人情報保護委員会への報告を義務付け（令和4年4月施行）。また、法人に対する罰金を最大1億円に引き上げ。

2. 保存すべき診療録等が滅失・毀損する。また、患者の病歴等について再度の聴取等が必要となることによる**患者側も負担増加**。

   ※ ランサムウェアによって、診療録をはじめとする診療に関する諸記録が暗号化され、バックアップファイルも含めて、完全には復号化できないことが判明した場合には、医療法第21 条等に抵触する恐れがある。

3. 過去の患者カルテと、来院した患者の氏名等といった基礎情報が電子的に突合できず、対面での指差し確認等の手作業で本人確認が必要。医療従事者が慣れない紙カルテでの運用に追われることになる**医療者側の負担増加**。

4. 被害の状況により、診療報酬の請求事務に影響を及ぼすことがあるほか、診療データの継続的な提出を評価する「データ提出加算」の算定や、「データ提出加算」を前提とする入院料の届出に影響が生じる場合がある。

医療機関における情報セキュリティについて

【参考】

現在の取組

○ 厚生労働省においては、「医療情報システムの安全管理に関するガイドライン」を定め、医療機関等に対し、技術的・運用管理上の観点から必要な対策を求めている。

第28回重要インフラ専門調査会

厚生労働省提出資料より抜粋（一部修正）

【ガイドラインに基づく対策】

（情報漏えい対策）

- ネットワーク接続に当たっては、送信元と送信先を限定する方式等で接続を行うこと
- セキュリティ対策（ウイルス対策ソフトやセキュリティ・パッチなど）を適切に実施すること
- システムの保守に当たっては、保守会社と守秘契約を締結するとともに、作業者、作業内容及び作業結果を確認すること　等

（医療情報を外部に保存する際の基準）

- 受託事業者が情報セキュリティに関する国際認証を取得していること等を確認すること
- 医療情報を格納する機器等が国内法（医療法に基づく立入検査等）の適用を受けることを確認すること　等

（非常時も含めた重大なシステム障害への備え）

- 災害・サイバー攻撃等の非常時における事業継続計画を策定すること
- システム障害の発生時にもシステム全体の機能を維持するため、平常時からサーバやネットワーク機器等の予備設備を準備・運用すること
- データの適切なバックアップを行うこと

サイバー攻撃を踏まえた対応

○ 今般、病院へのサイバー攻撃により、診療が長期にわたって制限された事例（※）があったことから、令和3年11月、全国の医療機関に対し脆弱性が指摘されている機器の点検、バックアップの作成等について注意喚起を行った。

○ また、厚生労働省では、令和4年1月21日に各都道府県・関係団体宛に通知し、全国の病院における、ランサムウェアを想定したリスクを把握するための実態調査を実施済。

○ 許可病床400床以上の保険医療機関について、医療情報システムのバックアップ体制の確保状況を届け出ることを診療録体制加算の要件として追加した。

※ 徳島県つるぎ町立半田病院におけるマルウェア感染事案（R3.10）

- バックアップがオンラインで保持されていたことから、電子カルテシステムがランサムウェアに感染した際にバックアップも感染し、長期にわたり過去の診療情報を閲覧できなくなったため一部診療が縮小されたが、近隣の医療機関との連携等を図ることで、必要な医療を提供した。

今後、都道府県等と連携しながら、各医療機関のバックアップ状況等に関する所要の対応を行うとともに、医療情報システムの安全管理に関するガイドラインを見直すなど、電子カルテの適切なバックアップの徹底を図っていく。

医療分野におけるサイバーセキュリティ対策調査事業（厚生労働省委託事業）

【参考】

第28回重要インフラ専門調査会

厚生労働省提出資料より抜粋（一部修正）

背　景

医療分野のサイバーセキュリティについては、その脅威がますます高まるとともに、日本の医療機関における人材育成の必要性や医療分野におけるＩＳＡＣの在り方の検討等が求められている。

○自民党サイバーセキュリティ対策本部第一次提言（2018年4月24日）　→　医療分野におけるＩＳＡＣの創設

○「サイバーセキュリティ2019」（令和元年（2019年）５月23日サイバーセキュリティ戦略本部決定）

→　厚生労働省において、医療分野及び水道分野におけるISAC 等のサイバーセキュリティ対策に関する情報共有のあり方について引き続き検討を行う。

令和３年度事業内容

令和２年度までの調査研究事業を実施して把握した、日本や海外におけるサイバーセキュリティ人材の実態、海外における医療分野におけるＩＳＡＣや日本の他分野におけるＩＳＡＣの実態を踏まえ、サイバーセキュリティ研修の実施や日本における医療分野におけるＩＳＡＣの設立に向けた基盤整備を行った。

1. 医療関係者向け、サイバーセキュリティ研修の実施
2. 継続的な医療関係者による意見交換会の開催、情報共有・掲示板ツール（ＳＩＧＮＡＬ等）を用いた相談体制の構築

※なお、上記意見交換会においては、内閣サイバーセキュリティセンター（NISC）にもオブザーバーとしてご参画いただいた。

水道分野における情報セキュリティガイドライン（第４版）の概要

【参考】

○　サイバーセキュリティ戦略本部による「重要インフラの情報セキュリティ対策に係る第４次行動計画（平成29年６月）」や「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第５版）（平成30年４月）」等を踏まえ、**「水道分野における情報セキュリティガイドライン（第４版）」**を平成31年３月に策定。

○　安全基準等策定指針では、重要インフラ事業者が、分野の特性に応じた必要な、又は望まれる情報セキュリティ対策を着実に実施するとともに、対策を継続的に改善していくことの重要性を指摘。

○　ガイドラインでは、水道事業者において実施することが必要な、又は望まれる情報セキュリティ対策の項目及び水準を示した。

改訂のポイント

① PDCAサイクルによる情報セキュリティ対策の実施と見直しの考え方の充実。
② 情報セキュリティの取組における経営層の役割の追加、最高情報セキュリティ責任者の役割の充実。
③ インシデント発生時における対応の追加。(対応計画の事前策定の必要性等)
④ 平時及びインシデント発生時における関係機関との連携体制の追加。
⑤ 制御系システムにおける対応として、多層的な防御の実施の必要性を強調するとともに、古いバージョンのOSのアップデート等の具体的対策を追記。

水道施設の技術的基準を定める省令改正の概要

【参考】

○　サイバーセキュリティ基本法に基づく施策の一環として、「重要インフラの情報セキュリティ対策に係る第４次行動計画」において、必要に応じて情報セキュリティ対策を関係法令等の保安規制に位置づけることが求められている。
○　これを踏まえ、水道施設の技術的基準を定める**省令を改正**し、水道施設の施設基準においても、サイバーセキュリティ対策を強化するために必要な措置を講じる旨を規定。

■水道施設の技術的基準を定める省令　第１条第１１の２項（新設）

（施行期日：令和２年４月１日）

施設の**運転を管理する**電子計算機が水の供給に著しい支障を及ぼすおそれがないように、サイバーセキュリティ（サイバーセキュリティ基本法（平成26年法律第104号）第２条に規定するサイバーセキュリティをいう。）を確保するために必要な措置が講じられていること。

■「水道施設の技術的基準を定める省令の一部改正について」

（令和元年9月30日付け薬生水発0930第7号）

○ 対象とするシステムは、水の供給に影響を与える**制御系システム**（浄水場の監視制御、ポンプ場の運転、水運用等）**に使用されている電子計算機**※。
○ サイバーセキュリティを確保するために必要な措置とは、以下をいう。
- 電子計算機へアクセスする者について**主体認証を行うことができる機能を有する**こと。
- 不正プログラム対策として、**アンチウイルスソフトウェアが導入**され、常に最新の状態が保たれていること。
- セキュリティ更新プログラムの提供等の**サポートが終了したオペレーティングシステムが使用されていない**こと。
  （外部ネットワークからの分離、USBメモリ等の外部記憶媒体からの感染防止対策等、**不正プログラムの侵入を防ぐ措置が講じられている場合はこの限りではない**）
- 電子計算機は、部外者がみだりに立ち入ることができないよう、障壁、施錠等により他の区域から隔離され、**人の入退室を制限することができる場所に設置**されること。

※電子計算機とは、コンピューター全般を指し、情報システムを構成するサーバ、端末、周辺機器等の装置全般。

資料８－４

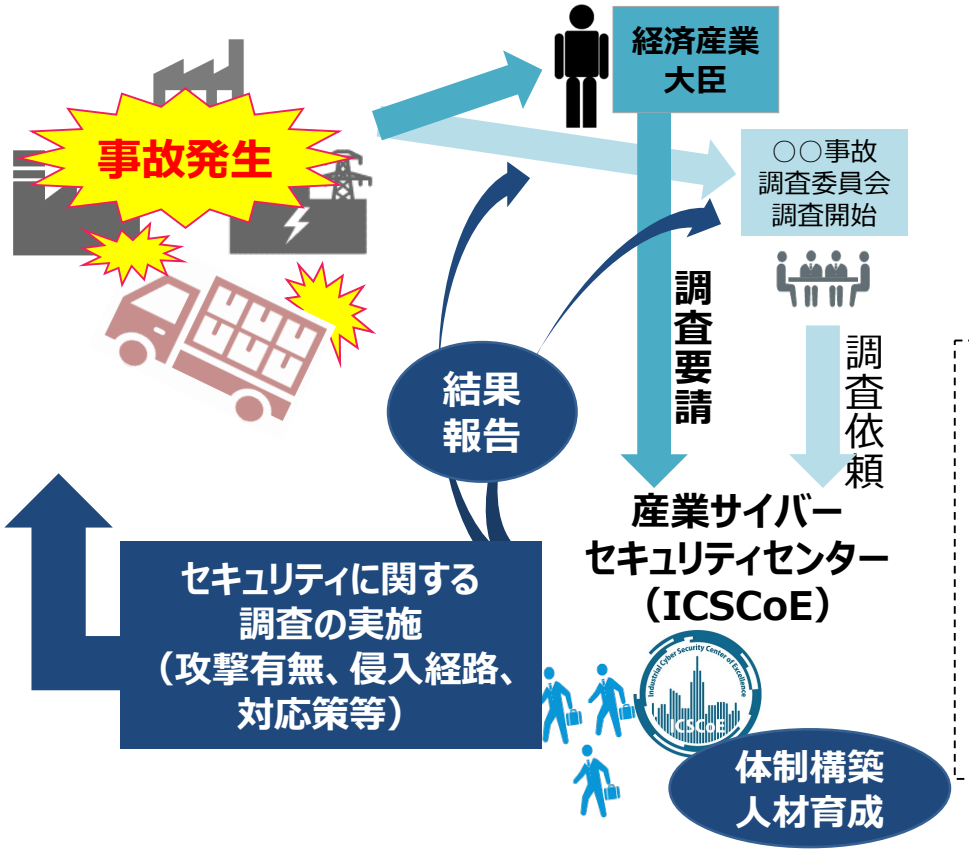
経済産業省における
サイバーセキュリティ施策の取組状況について

令和４年５月
経済産業省サイバーセキュリティ課

国としての対処能力の強化～サイバーインシデントに係る事故調査の体制整備

- サイバー攻撃の起点が拡散し、サイバー攻撃がフィジカル領域に大きな影響を及ぼすようになることから、プラント等の事故が発生した場合に、**サイバーインシデントの観点からの原因究明可能な機能を有することが必要に（いわゆる「サイバー事故調」）**。
- IPA産業サイバーセキュリティセンター（ICSCoE）は、「サイバー事故調」機能を整備するため、**2022年度に、重要インフラ２分野においてパイロット・実証事業を実施。経済産業大臣からの調査要請**が規定される**高圧ガス保安法等の一部を改正する法律案の施行（2023年12月頃を想定）にあわせて、機能整備**の準備を推進。

サイバーインシデントに係る事故調査のイメージ



取組の概要

＜令和４年度＞パイロット・実証

- **サイバー事故調機能のあり方は産業分野により様々**であるとの仮説を基に、令和4年度は、令和３年度の成果を活用しつつ、**２分野でパイロット・実証事業を実施**。
- 具体的には、重要インフラである**電力等産業保安分野**から事業者の協力を得て、現在行われている**通常の事故調査と将来的なサイバーインシデントに係る事故調査の円滑な連携に向けた課題の洗い出しや連携方策**に係る検討を実施する。

＜参考＞高圧ガス保安法改正案　（※3月4日閣議決定）

（調査の要請）

第60条の2　経済産業大臣は、認定高度保安実施者その他の保安の確保上特に重要な者として経済産業省令で定める者において保安に係るサイバーセキュリティ（サイバーセキュリティ基本法（平成二十六年法律第百四号）第二条に規定するサイバーセキュリティをいう。）に関する重大な事態が生じ、又は生じた疑いがある場合において、必要があると認めるときは、独立行政法人情報処理推進機構に対し、その原因究明のための調査を要請することができる。

（ガス事業法、電気事業法の改正案にも同趣旨の記載。）

資料８－５

国土交通分野におけるサイバーセキュリティ施策の取組状況について

令和４年５月

国土交通省総合政策局情報政策課

サイバーセキュリティ対策室

一般社団法人交通ISACについて

国土交通省

平成29年度から令和元年度までの３年間、航空・空港・鉄道及び物流分野の重要インフラ事業者等が中心となり、**サイバーセキュリティに関する情報共有・分析及び対策を連携して行う体制「交通ISAC」**の創設に向けた検討・取組みが行われ、令和２年４月、**「一般社団法人交通ISAC」が設立**された。

■一般社団法人交通ISACの概要

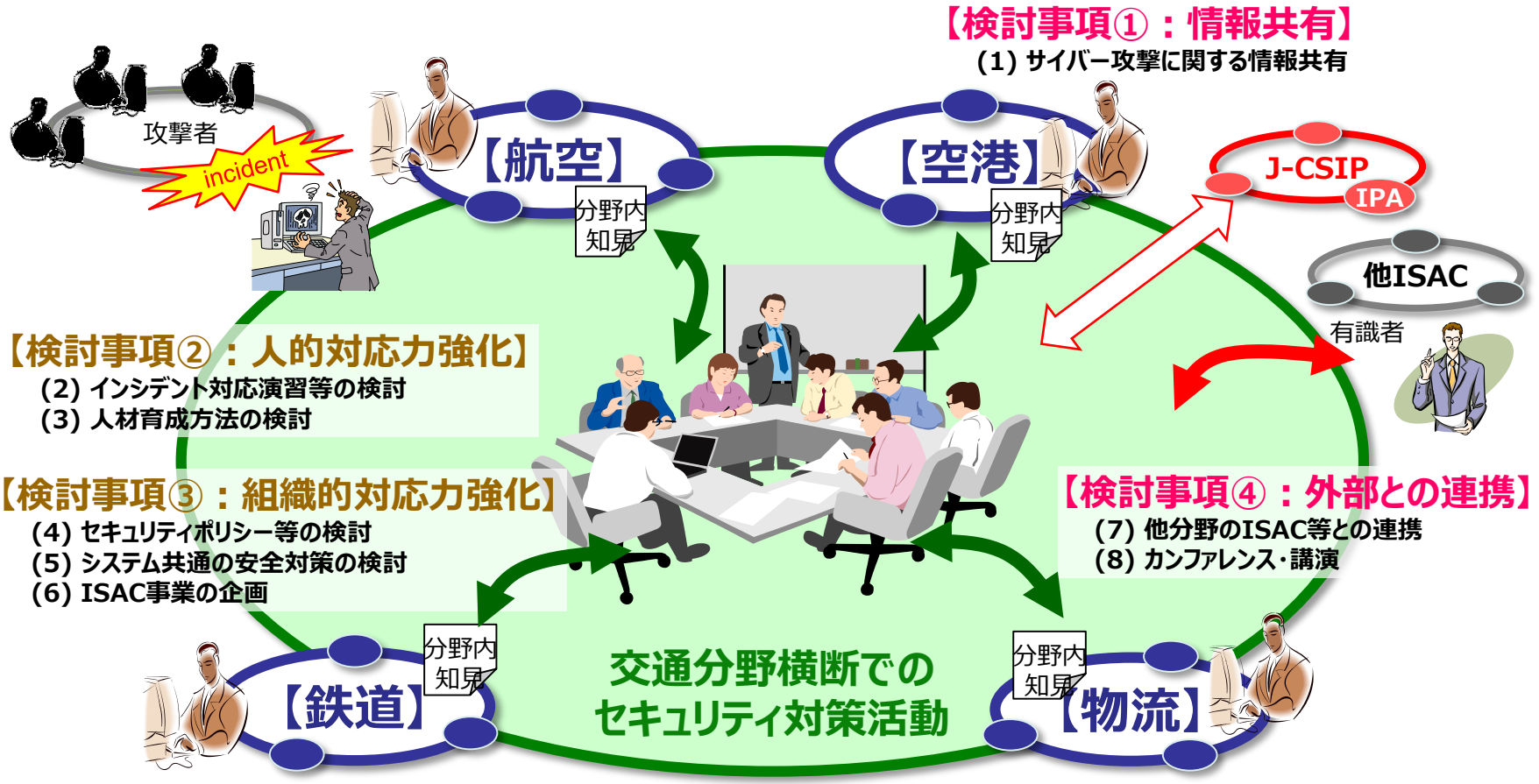
法人の名称	一般社団法人交通ISAC （英文表示：Transportation ISAC JAPAN）
所在地	東京都港区
設立日	令和２年４月１日
会員数	89団体【令和３年６月１日現在】 （うち、正会員68団体、賛助会員11団体、オブザーバー会員10団体）
設立の目的	交通・運輸分野の事業者等が組織や業界の枠を超えたコミュニティ活動を通じて共に助け合う体制を確立し、サイバー攻撃等に対する交通・運輸分野全体の集団防御力の向上に資する活動を推進することで、我が国における交通・運輸サービス全体の安全・安心の向上に寄与する。
事業の内容	①　サイバーセキュリティに関する情報の収集及び共有 ②　サイバーセキュリティに関する課題に対する共通認識の醸成及び共同対処 ③　その他当法人の目的を達成するために必要な事業

一般社団法人交通ISACについて

国土交通省

活動内容

- 参画事業者間で共通の課題に対し、協同で解決策を検討する活動　⇒ ②、③
- インシデント等の情報を参画事業者間で展開し、対策を共有する活動　⇒ ①、④



一般社団法人交通ISACの活動について

国土交通省

■一般社団法人交通ISACの活動（設立から令和3年度末まで）

	航空・空港分野	鉄道分野	物流分野
分野横断系WG	**①セキュリティマネジメント共有WG（8回開催）** ✓ インテリジェンス情報（攻撃情報、インシデント情報等）の共有 ✓ 他社の対策・取組み（先進事例、ベストプラクティス等）の共有 ✓ 情報システムの外部ネットワーク接続におけるセキュリティ対策の検討等		
分野特化系WG	**②航空・空港分野における脅威情報分析WG（17回開催）** ✓ 航空・空港分野におけるインシデント情報等の共有 ✓ セキュリティ人材の育成のため、業界共通のCSIRTの構築についての検討	**③IT-OT連携WG（5回開催）** ✓ 鉄道分野におけるインシデント情報等の共有 ✓ 社内のIT・OT部門における情報連絡体制の構築についての検討	**④事例共有WG（5回開催）** ✓ 物流分野におけるインシデント対応に関する対策取組事例の共有 ✓ 社内のセキュリティ対策を容易にするための対策ベンチマーク指標の検討・作成 **⑤海事分野WG（3回開催）** ✓ 船舶サイバーセキュリティ対策の充実・強化のため、現状の課題及び今後取り組むべき方策の検討

上記の他に、国内ISAC間での連携会議（令和３年度に５回開催）、
東京オリンピック中の国内ISAC間での情報連携（オリンピック期間中）を実施。