資料３

関係省庁の取組状況について

【金　融　庁】

資料３－１　金融分野のサイバーセキュリティレポート（令和２年６月）の概要について

【総　務　省】

資料３－２　放送設備のサイバーセキュリティ確保に関する検討について

資料３－３　大規模なインターネット障害に関して電気通信事業者等に推奨する対策の制定について

【経済産業省】

資料３－４　IoT セキュリティ・セーフティ・フレームワーク（IoT-SSF）の案の策定について

【国土交通省】

資料３－５　一般社団法人交通 ISAC の設立について

金融分野のサイバーセキュリティレポート（令和2年6月）の概要

資料３－１

背　景

○「金融分野におけるサイバーセキュリティ強化に向けた取組方針」（2018年10月アップデート）に基づき、これまで官民が一体となって、金融分野のサイバーセキュリティ強化に向けた取組みを実施

○ 同取組方針に基づく令和元事務年度の取組みにおいて、把握した実態や共通する課題等を取りまとめレポートとして公表

1．金融分野を巡るサイバーセキュリティの現状について

（1）近年の脅威動向等

- 国内金融機関においては、これまでに大規模なサイバーインシデントは発生していないものの、**攻撃者が金融機関などを装った偽のウェブサイトに利用者を誘導**し、**不正送金やクレジットカード情報が窃取される**等の被害が発生。
- 海外金融機関においては、**個人情報の漏えいやサービスの停止につながる大規模なサイバーインシデント**が発生。

（2）国内金融機関のサイバーインシデントについて

- **リスト型攻撃による不正ログインやDDoS攻撃に関する報告**が多く、他金融機関においても同様のインシデントが発生する恐れがあることから、2019年10月、**金融機関に注意喚起を発出**し、所要の対応を求めた。
- 今後も**新たな脅威や脆弱性をタイムリーに把握・分析**し、金融分野のサイバーセキュリティ管理態勢の強化を図る必要。

（3）新型コロナウイルス感染症等によるサイバーセキュリティへの影響

- **新型コロナウイルス感染症に便乗したサイバー攻撃**や**テレワーク環境を狙ったサイバー攻撃**などが数多く発生。
- 国内金融機関では、重大な問題は発生していないものの、**テレワークを活用した新しい働き方や金融サービスの電子化が一層進展することが想定**されるため、**セキュリティ対策にも留意していく必要**。

金融分野のサイバーセキュリティレポート（令和2年6月）の概要

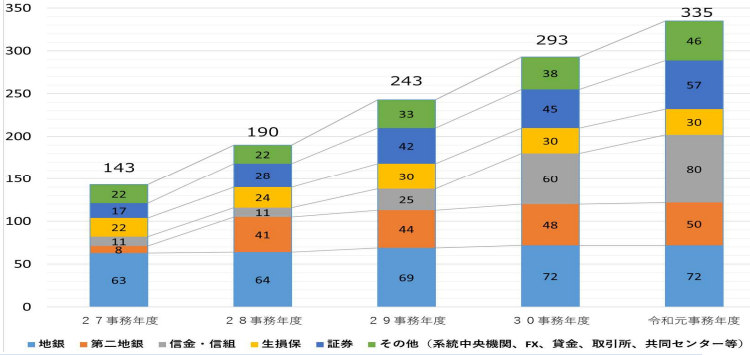
2. 金融分野のサイバーセキュリティ強化に向けた取組み状況 （1/3）

（1）①平時のサイバー対策

ア. 中小金融機関等

- ✓ これまで、中小金融機関については、実態把握（対話によるモニタリング）を通じて、基礎的なサイバーセキュリティ管理態勢の整備状況を検証
- ✓ 令和元事務年度は、業界全体の底上げの観点から、基礎的なサイバーセキュリティ管理態勢の整備の遅れが懸念される先を中心に、実態把握を実施

【業態別実態把握先の推移（実態把握先の累計（2巡目含む））】



業態名	取組結果等の概要
地域銀行・信金・信組	・一部の先では、自主的に強化を図っている状況。他方、**依然として基礎的な態勢整備に課題**がある先もみられた ・課題がみられた先については、**経営陣が主体となった取組みの推進態勢の整備**を促進
証券会社等	・取組みが進展している金融機関が増えている一方、**依然として取組みの進展が停滞状態**の先もみられた ・課題がみられた先については、**経営陣が主体となった取組みの推進態勢の整備**を促進

イ. 大手金融機関等

- ✓ これまで、大手金融機関については、グローバルな動向等を念頭に、定期的な対話を通じて議論
- ✓ 令和元事務年度は、高度化が期待されるグループ・グローバルの管理態勢の高度化、TLPTの活用状況を中心に確認
- ✓ また、信託銀行やネット銀行等については、アンケートを通じたオフサイトモニタリングを実施

業態名	取組結果等の概要
3メガグループ等	・**グループ・グローバルベースの一元的な管理態勢の高度化**に取り組んでいる。**アクセスコントロールの強化、サイバーレジリエンスの高度化**等を通じて、管理態勢の強化を図っていくことを期待 ・TLPTをより実効性のあるものとするため、**各種ガイドラインへの準拠**に加え、**国際的なフレームワーク を活用したインシデント対応能力の評価等の高度化、高度な専門人材の育成**を継続することを期待
信託・ネット銀行等	・サイバーセキュリティの高度化に向けた取組みを推進している先がみられた。他方、一部銀行では、**経営陣が主体となった取組推進やリスク認識に改善の余地**がみられ、意見交換を通じて課題を共有し自主的な改善活動を促進

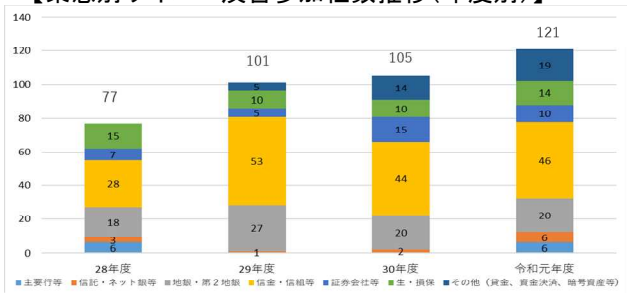
金融分野のサイバーセキュリティレポート（令和2年6月）の概要

2. 金融分野のサイバーセキュリティ強化に向けた取組み状況 （2/3）

（1）②有事のサイバー対策

- 金融庁では、毎年、金融機関の対応能力強化を図るため、「金融業界横断的なサイバーセキュリティ演習（Delta Wall）」を実施
- 令和元事務年度は、東京2020大会に向け、業界全体の底上げの観点から中小・大手金融機関に加え、資金移動業者等が参加（121社（約2,000名））
- 金融庁のほか、様々な団体が多様な演習を実施しており、こうした演習への参加を通じて**インシデント対応能力の更なる向上を図っていくことが重要**

【業態別サイバー演習参加社数推移（年度別）】



業態名	金融業界横断的なサイバーセキュリティ演習結果の概要
大手銀行、地域銀行	・全般として対応が概ねできていたものの、**復旧対応や顧客対応に課題**が一部みられた ・**金融機関内での深度ある議論が求められるような形式**とするなど、更なる高度化を図っていく
その他	・**トリアージや顧客対応、再発防止策の検討など、全体的に改善の余地**がみられた ・引き続きインシデント対応能力の向上を図っていく必要

（1）③東京2020オリンピック・パラリンピック競技大会の開催を見据えた管理態勢の強化

- 東京2020大会の開催を見据え、金融機関のサイバーセキュリティ管理態勢の強化に向けた取組みを実施

ア. 基礎的なサイバーセキュリティ管理態勢の実効性向上

業態名	取組結果等の概要
地域銀行、信金・信組	・2020年3月末までに、**①脆弱性診断、②演習・訓練、③監視・分析状況の整理等、を実施するよう要請** ・多くの金融機関は上記①～③の**実施を完了**。一部は対応に遅れがみられ、**協会と連携しフォロー**を実施
その他 （都市銀行、資金決済事業者、証券、生損保、貸金業等）	・上記①～③の各事項について確認 ・特段の課題はみられなかったが、今後も必要に応じて取組み状況の把握やフォローを実施

イ. 要請対応やアンケートを通じて把握した事例や実効性向上への課題

要請事項	良好・課題事例
脆弱性診断	・リスクを踏まえ計画的に診断を実施する先がある一方、リスク認識不足で対策実施が停滞している先がみられた
演習・訓練	・演習・訓練によりコンチプランを見直している先がある一方、参加後の振返り等を実施していない先がみられた
監視・分析	・インシデントの早期検知・分析態勢を整備している先がある一方、ログの確認・分析には至っていない先がみられた

金融分野のサイバーセキュリティレポート（令和2年6月）の概要

2. 金融分野のサイバーセキュリティ強化に向けた取組み状況 （3/3）

（1）④デジタライゼーションの加速的な進展を踏まえた対応

- 国内外の金融機関やITベンダー等にヒアリングを行い、デジタライゼーションの進展状況等の把握・分析を実施

ア. クラウドサービス全般
- ✓ 大手金融機関では、**研修の受講、認定資格保有者数の目標設定、新サービスの説明会やイベントへの参加**等を通して、新サービスの早期活用、継続的なスキルアップを図っている

イ. 新たなセキュリティモデルへの転換
- ✓ 大手金融機関では、**ゼロトラストを意識したセキュリティ対策に本格的に取り組む**動きがみられる

（2）①情報共有の枠組みの実効性向上

- これまで、「共助」の意義について、機会を捉えて、金融機関に周知してきたところ、**金融ISAC の加盟金融機関数は着実に増加**
- 今後、さらなるサイバーセキュリティ強化を図るためには、**業界団体との連携等を一層充実**させていくことにより、サイバーセキュリティ対策の提供を含めた「共助」を深化していくことが期待され、引き続きこうした活動を積極的に支援

（2）②大規模インシデント発生時の連携

- サイバーセキュリティ対策関係者連携会議（2019年6月立上げ）を活用し、東京2020大会の開催を見据えた大規模インシデント発生時の連携態勢について、**連携手順の整備やサイバー演習等を通じて業界全体の連携態勢**を強化
- 今後は、**情報共有システムを利用したメンバー間での情報連携**について、**演習により有効性・実効性**等を確認

（2）③国際的な連携

- 2019年6月、大規模なサイバーインシデントの発生を想定した合同演習を実施し、G7諸国の当局を中心とした**クロスボーダーの連携を確認**
- 最近の国際的な議論においては、クラウドサービスなどの**サードパーティやサイバーインシデントからの復旧・回復といったレジリエンス**の考え方が取り上げられ、こうした議論を含め**国際的な動向を的確に把握・対応**していくことが重要

3. 当局の今後の取組み

○ 新型コロナウイルス感染症の拡大に伴う外部環境の変化や2021年に延期された東京2020大会など、金融機関を取り巻くサイバーリスクは一層高まっている状況

○ 今後当局としても、金融分野における更なるサイバーセキュリティ対策の強化を図っていくために、以下の取組みを重点的に推進

金融分野の環境変化への対応

- 金融分野では、デジタライゼーションが進展する中、新型コロナウイルス感染症への対応としてオンライン化・リモート化が加速しており、金融機関を取り巻く環境は大きく変化。こうした新たな金融サービス・インフラの前提として、サイバーセキュリティの確保はますます重要な課題
- 金融庁としては、こうした環境の変化を踏まえた新たなセキュリティに関する脅威の動向について、**デジタライゼーションの進展を踏まえたサイバーセキュリティへの取組みとあわせて、積極的に情報収集**を行い、**必要な対応を促進**

金融機関のサイバーセキュリティ強化に向けた対応

- 中小金融機関に対しては、**業界団体等との連携を通じた基礎的なサイバーセキュリティ管理態勢の実効性の維持・向上**を促すとともに、**サイバー演習によりインシデント対応能力の底上げ**を図る。また、**各業態の取組みに進展がみられる先との意見交換**を通じてプラクティスを収集し、好事例を積極的に還元
- 大手金融機関に対しては、国際的な議論の動向を念頭に、**グループ・グローバルベースでのサイバーセキュリティに関するリスク管理の高度化、TLPTの実効性向上**を通じたサイバーセキュリティ対策のより一層の高度化を促進。また、検知の遅れにより長期間ネットワーク内で活動するリスク等を踏まえ、**サイバーレジリエンスへの取組み**についても対話を行う

放送設備のサイバーセキュリティ確保に関する検討

資料３－２

■ 総務省において、放送設備のサイバーセキュリティ確保に関する検討を実施。

- 「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30年7月25日 サイバーセキュリティ戦略本部決定）において、重要インフラ分野おけるセキュリティ対策について、安全等を維持する観点から情報セキュリティ対策を関係法令等における保安規制として位置付けることなど、制度的枠組みを適切に改善する取組の継続的な実施が明記されている。

- サイバー攻撃の多様化、2020年東京オリンピック・パラリンピック競技大会への対応等を見据え、令和元年6月に情報通信審議会に放送設備のサイバーセキュリティ確保に関する技術的条件について諮問し、７月より情報通信審議会放送システム委員会（※）で検討を開始。同年12月、情報通信審議会より答申。

（※）放送システム委員会の下に、放送事業者、電気通信事業者、放送関係団体、メーカ、研究機関等の関係者で構成する作業班を設置し検討。

放送システム委員会

放送設備安全信頼性検討作業班

（作業班１）地上放送・衛星放送関係

主　任　甲藤二郎 早稲田大学基幹理工学部 教授

構成員　放送事業者（地上放送(テレビ・ラジオ)、衛星放送）、電気通信事業者、メーカ、放送関係団体関係者、研究機関関係者、学識経験者（21名）

（作業班２）有線放送関係

主　任　上園一知 一般社団法人日本ケーブルラボ主任研究員

構成員　放送事業者、電気通信事業者、メーカ、放送関係団体関係者（14名）

総務省令の改正

■ 総務省において、放送設備のサイバーセキュリティ確保に関する省令改正を令和2年３月に実施。

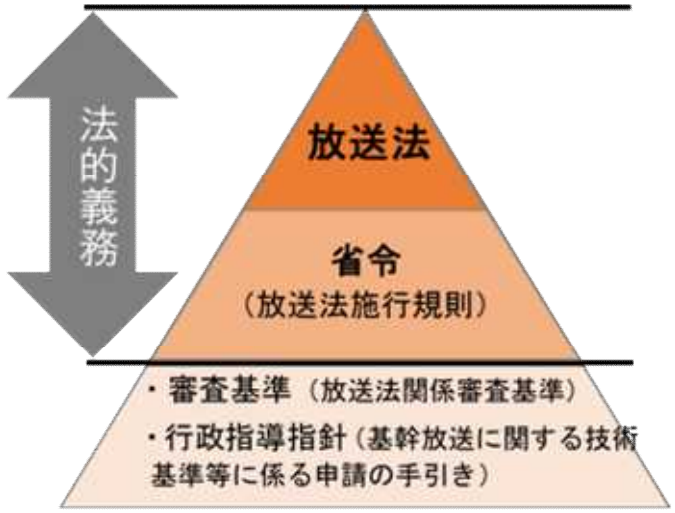
- 放送法第121条等において、放送設備の技術基準への適合維持を義務付け。
- 技術基準は、従来より、放送停止事故を未然に防ぐ又は即座に復旧させるための措置として、予備機器等、耐震対策、停電対策その他12項目の措置事項を省令（放送法施行規則）で規定。

・予備機器等
・故障検出
・試験機器及び応急復旧機材の配備
・耐震対策
・機能確認
・停電対策
・誘導対策（アンテナからの電磁誘導影響への対策）
・防火対策
・屋外設備
・収容する建築物
・耐雷対策
・宇宙線対策
・サイバーセキュリティの確保【追加】

- 今般、この技術基準にサイバーセキュリティの確保の規定を追加

放送法施行規則
第115条の2　放送設備及び当該放送設備を維持又は運用するために必要な設備は、当該放送設備によって行われる放送の業務に著しい支障を及ぼすおそれがないよう、サイバーセキュリティ（サイバーセキュリティ基本法第２条に規定するサイバーセキュリティをいう。）の確保のために必要な措置が講じられていなければならない。

※ 措置の具体的な内容については、放送法関係審査基準にその具体的措置を例示し、事業者ごとの対策内容を確認。



放送設備の現状とサイバーセキュリティの確保のための措置項目

- 放送設備及び有線放送設備の構成は、①放送番組を視聴者に届ける放送ネットワーク系統（放送本線系）と②各放送設備の故障検出や設備切替等を行う監視・制御ネットワーク系統（監視・制御系）に大別。
- 放送本線系は、映像や音声伝送のための専用方式による片方向の中継伝送と、直接受信のための放送方式による一対多の片方向の送信で構成されており、外部のネットワークと直接接続されていない。したがって、送信の起点となる箇所について対策を行うことで、効率的・効果的に他のネットワークから分離することが可能。
- 放送本線系の予備回線や監視・制御及び保守等のために電気通信事業者回線を使用する場合は、専用回線の使用、VPN化、ポート制限、ID・パスワードによる使用者の権限・アクセスの管理に加え、その管理に係る規程・マニュアルの整備など、セキュリティの確保のための措置が重要。

（サイバーセキュリティ確保のための具体的措置項目）

1　放送本線系入力となる番組送出設備について、外部ネットワークから隔離するための次の措置又はこれと同等と認められる措置

- 原則として、第三者が接続可能な外部ネットワークとの接続を行わない措置
- やむを得ず接続を行う場合には、ファイアーウォールの設置又は不正接続対策等の措置

2　放送設備に接続される監視・制御及び保守に使用される回線について、外部ネットワークからの不正接続対策を行うための次の措置又はこれと同等と認められる措置

- 専用回線又はＶＰＮ回線の使用、ポート番号若しくはＩＰアドレスによる接続制限又はＩＤ及びパスワードにより権限を有する者だけが接続できるようにする措置
- 未使用時は回線を通じた接続を遮断する等の措置

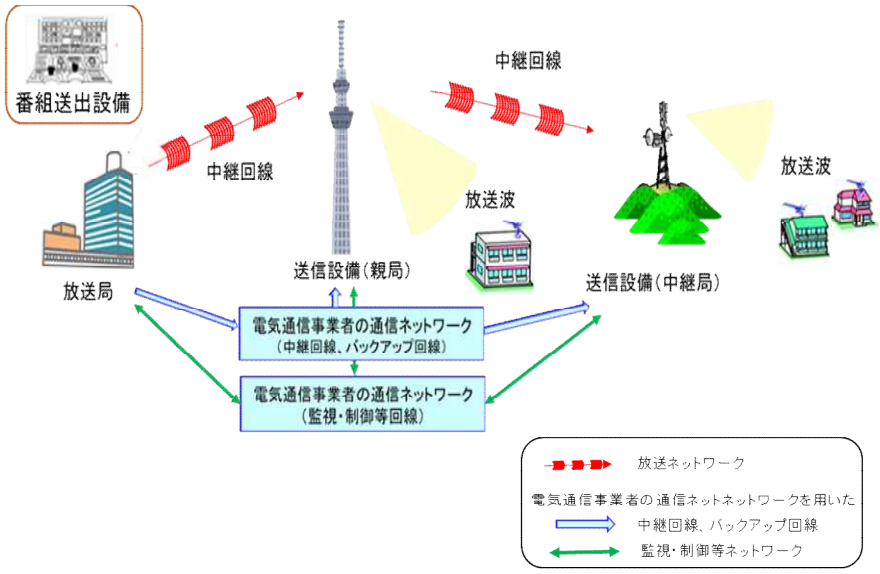
3　設備の導入時及び運用・保守時におけるソフトウェアの点検について、不正プログラムによる被害を防止するため、放送設備のネットワークからの分離・遮断の措置及び不正プログラムの感染防止の措置

4　放送設備に対する物理的なアクセス管理について、機密性が適切に配慮されるための次の措置又はこれと同等と認められる措置

- 番組送出設備に対しＩＤカード、テンキー錠又は有人による入退室の管理等を行う措置及び監視・制御回線、保守回線に係る機器の設置場所に対し公衆が容易に立ち入ることができないよう施錠その他の必要な措置
- 外部記録メディア等を介した不正プログラムへの感染防止の措置

5　放送設備の運用・保守に際して、業務を確実に実施するための組織体制の構築及び業務の実施に係る規程若しくは手順書の整備に関する次の措置又はこれと同等と認められる措置

- 事故報告を含む事後対応を、迅速かつ確実に実施するための規程を整備する措置
- 放送設備のソフトウェアの更新等設備の運用・保守等について、実施方法を定める規程を整備する措置



放送設備の構成のイメージ（地上デジタル放送の例）

放送分野における設備に関する報告様式の変更

放送法令において、各放送事業者は設備の状況を定期的（※）に総務大臣に報告することとされている。

当該報告に関し、放送事故の発生区分に『サイバー事案』を追加し、『サイバー事案』に起因する事故報告を明記するよう、報告様式を変更。

（※）認定基幹放送事業者、特定地上基幹放送事業者及び基幹放送局提供事業者は半年ごと、登録一般放送事業者は１年ごと

別表第二十九号（第127条関係）

特定地上基幹放送局等設備の状況報告書

年　月　日

総務大臣　殿

郵　便　番　号
住　　　　　所
（ふりがな）
氏　　　　　名　（法人又は団体にあつては、名称及び代表者の氏名。記名押印又は署名）
電　話　番　号
免　許　番　号　（親局の免許番号を記載すること。）

放送法施行規則第127条の規定により、　年　月　日から　年　月　日までの特定地上基幹放送局等設備の状況を、次のとおり報告します。

発生年月日（発生時刻）	復旧年月日（復旧時間）	発生区分	発生原因	故障設備	措置模様	影響があつた下位の放送局	備考
		□設備故障　□回線障害 □自然災害　□停電 □ｻｲﾊﾞｰ事案　□その他					
		□設備故障　□回線障害 □自然災害　□停電 □ｻｲﾊﾞｰ事案　□その他					
		□設備故障　□回線障害 □自然災害　□停電 □ｻｲﾊﾞｰ事案　□その他					
		□設備故障　□回線障害 □自然災害　□停電 □ｻｲﾊﾞｰ事案　□その他					
		□設備故障　□回線障害 □自然災害　□停電 □ｻｲﾊﾞｰ事案　□その他					

大規模なインターネット障害に関して電気通信事業者等に推奨する対策の制定

資料３－３

■　大規模インターネット障害の防止又は被害の最小化のため、平成30年８月にGoogleの人為的ミスを起因として発生したインターネット障害から得られた教訓を踏まえ、各電気通信事業者等に推奨すべき対策について、情報通信ネットワーク安全・信頼性基準に規定（平成31年３月）。

インターネットの経路設定時の人為的ミスの防止に係る対策

＊未然防止を前提とした手法と、事後措置を前提とした手法があり、少なくともいずれかの実施を推奨。

（未然防止を前提とした手法）

・経路情報の設定作業において、容易に誤りが混入しないよう措置を講ずること（新）

・経路情報の設定に係る教育・訓練を実施すること（既）

（事後措置を前提とした手法）

・経路情報の設定後のトラヒックの疎通状況を監視し、異常等をアラートで知らせる機能を設けること（既）

・経路情報の設定に伴い、トラヒックの疎通に係る異常等が発生した場合を想定し、復旧対応手順を作成すること（既）

・経路情報の設定後に、トラヒックの疎通に係る異常等が発生した場合の対応について、教育・訓練を実施すること（既）

誤送信された経路情報の受信防止及び不要な経路情報の送信防止に係る対策

・不要又は不正な経路情報の送受信を防ぐために有効な機能を設けること（新）

・経路情報の瞬間的かつ急激な増加を考慮した設計とすること（改）

・将来の経路情報の増加を考慮した設計とすること（改）

経路設定誤り又はサイバー攻撃による障害に関する情報の事業者間での共有に係る対策

・事故又は障害発生時に迅速な原因分析や状況把握等のため、電気通信事業者間での情報共有を含め、複数のルートを活用し幅広く情報収集に努めること（新）

・契約関係等がある事業者（海外の事業者を含む。）との障害対応時の連絡先を把握しておくこと（既）

ネットワーク構成に係る対策

・重要な回線については、異なる2者以上の電気通信事業者から提供を受けること等により、信頼性の向上を図ること（新）

利用者周知に係る対策

・インターネットにつながりにくい障害が発生した場合に、速やかに利用者に対して公開すること（改）

（凡例）　（新） 規定を新たに追加。（既） 既存の規定が存在。（改） 既存の規定に趣旨を追加する改正を行うもの。

IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF）の案の策定

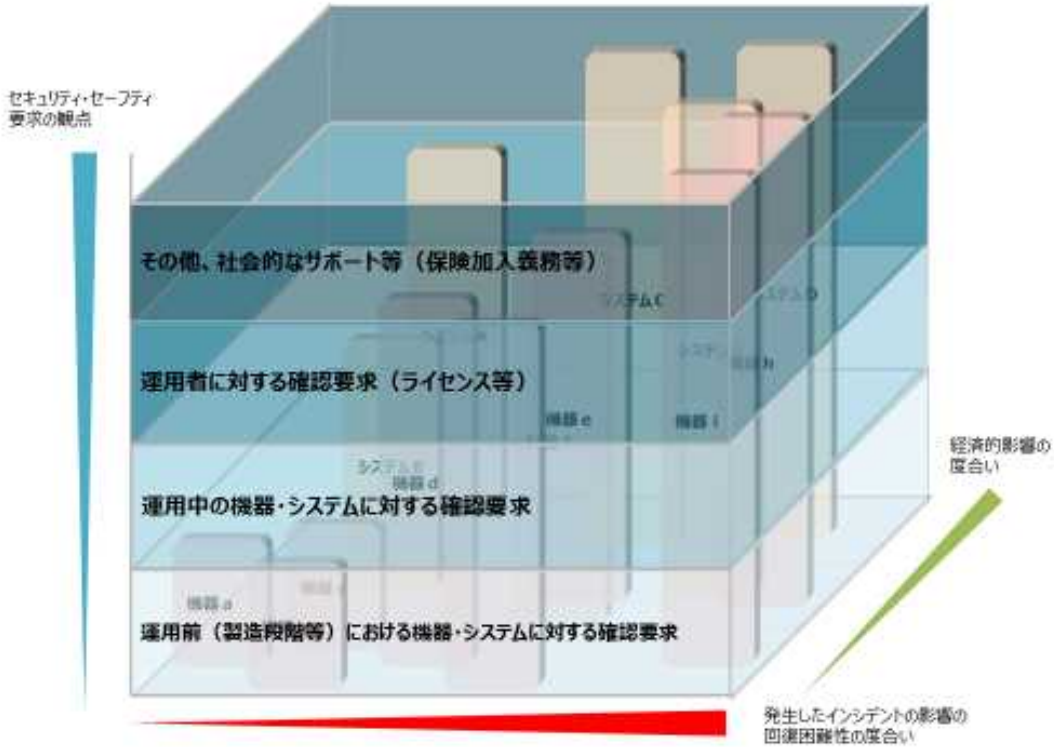
資料３－４

- IoT機器・システムの性質や利用環境によって課題が一様ではないことに着目し、IoT機器・システムをリスクに応じてカテゴライズした上で、それぞれに対するセキュリティ・セーフティ要求を検討することが重要。
- 経済産業省産業サイバーセキュリティ研究会WG１において、IoT機器・システムのカテゴライズやセキュリティ・セーフティ要求の検討に資するフレームワーク「IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF)」の案を策定。世界中から幅広く意見を収集するため、日本語版・英語版のパブコメを実施（2020年3月31日～6月24日）。

フィジカル・サイバー間をつなげる
機器・システムのカテゴライズのイメージ

※　同じ機器でも使用形態などによってマッピング先が異なり得る。
例えば、機器gと機器hが同じ機器で異なる使用形態である場合などがあり得る。）

カテゴリに応じて求められる
セキュリティ・セーフティ要求の観点のイメージ



一般社団法人交通ISACの設立について

資料３－５　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・取組みが行われてきたところ、今般、**「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	78団体 【令和２年７月１日現在】 （うち、正会員66団体、賛助会員２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