資料３

内閣サイバーセキュリティセンター
National center of Incident readiness and Strategy for Cybersecurity

サイバーセキュリティ戦略本部 重要インフラ専門調査会（第25回）

重要インフラにおける安全基準等の浸透状況等に関する調査について［2020年度］

令和３年５月31日

内閣サイバーセキュリティセンター
重要インフラグループ

目次

1．概要 …… 3

2．アンケート調査 …… 6

3．往訪調査 …… 20

参考［アンケート調査結果］ …… 26

目次

1．概要 …… 3

2．アンケート調査 …… 6

3．往訪調査 …… 20

参考［アンケート調査結果］ …… 26

安全基準等の浸透状況等に関する調査

- 「重要インフラの情報セキュリティ対策に係る第４次行動計画」（以下「行動計画」という。）では、**各重要インフラ分野に共通して求められる情報セキュリティ対策を「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）」**（以下「指針」という。）**として取りまとめ**、重要インフラサービスの安全かつ持続的な提供の実現を図る観点から**「安全基準等」**（注）**で規定されることが望ましい項目を整理**している。
- 内閣官房は、重要インフラ事業者等における安全基準等の浸透状況等を把握するため、**重要インフラ事業者等に対し、情報セキュリティ対策の実施状況について「アンケート調査」及び「往訪調査」を実施**している。

（注）各重要インフラ事業者等の判断や行為の基準となる基準又は参考となる文書類であり、関係法令に基づき国が定める「強制基準」、関係法令に準じて国が定める「推奨基準」及び「ガイドライン」、関係法令や国民からの期待に応えるべく業界団体等が定める業界横断的な「業界標準」及び「ガイドライン」、関係法令や国民・利用者等からの期待に応えるべく事業者等が自ら定める「内規」等が含まれる。

各調査の目的・内容

調査の流れ（イメージ）

内閣官房 | **重要インフラ事業者等**

アンケート調査

【目的】
- 重要インフラ事業者等における**安全基準等の浸透状況を把握**し、行動計画の検証や指針等の見直しに活用。

【内容】
- 重要インフラ事業者等の**情報セキュリティ対策の実施状況を書面で調査**。

行動計画の検証のための指標
①ベースラインとなる情報セキュリティ対策に取り組んでいる重要インフラ事業者等の割合
②先導的な情報セキュリティ対策に取り組んでいる重要インフラ事業者等の割合

往訪調査

【目的】
- 情報セキュリティ対策の**良好事例の収集**等。

【内容】
- 重要インフラ事業者等に対し、ヒアリング等を実施。

（参考）調査の位置付け

「重要インフラの情報セキュリティ対策に係る第４次行動計画」

（サイバーセキュリティ戦略本部 平成29年４月18日決定、令和２年１月30日最終改定 ）

Ⅲ．計画期間内に取り組む情報セキュリティ対策

１．安全基準等の整備及び浸透

各重要インフラ分野に共通して求められる情報セキュリティ対策を「重要インフラ分野における情報セキュリティ確保に係る安全基準等策定指針」として策定し、必要に応じた改定を行っており、同指針を受けた形で、各重要インフラ分野におけるガイドライン等の見直し、そして重要インフラ事業者等の内規等の見直しが進められ、全体として必要な安全基準等の整備が図られている。

さらに、各重要インフラ事業者等において、安全基準等が情報セキュリティ対策の規範として浸透することにより、重要インフラサービスの安全かつ持続的な提供に必要な取組の推進が図られている。

本行動計画期間においては、**内閣官房は、重要インフラ防護能力の維持・向上を目的に、指針改定及び安全基準等の**継続的改善や**浸透状況の調査**を行う。

また、重要インフラ事業者等は、情報セキュリティ対策の重要性に鑑み、PDCAサイクルに沿った継続的かつ着実な実施に取り組む。

１.３ 安全基準等の浸透

重要インフラ事業者等における安全基準等の浸透状況のより精緻な把握を目的に、内閣官房は、毎年、重要インフラ事業者等の対策状況についてのアンケート調査及び往訪調査を実施する。アンケート調査については、重要インフラ事業者等における安全基準等の浸透及び取組の改善につながるよう、随時調査項目の見直しを行う。

具体的には、対策状況をより詳細かつ精緻に確認するための調査項目を追加するとともに、各施策によって、理想とする将来像へどの程度到達したかを把握するための調査項目を追加する。さらに、調査への回答を通じて、重要インフラ事業者等がセルフチェックを行い、自らの情報セキュリティ対策の充足度や課題点、解決策等を認識可能となるように調査票等を構成する。

また、**アンケート調査結果から得られた仮説の検証及び良好事例の収集を目的に、重要インフラ事業者等へ往訪調査を行う**。

なお、アンケート調査及び往訪調査によって得られた調査結果については、原則、年度ごとに公表するとともに、本行動計画の各施策の改善に活用する。

Ⅴ．評価・検証

２．本行動計画の検証

2.３「政府機関等による施策」の検証

本行動計画の各施策は、いずれも重要インフラ事業者等による情報セキュリティ対策の効果を高めるため政府が支援を行うものである。施策の結果検証は、重要インフラ事業者等による情報セキュリティ対策に対する本行動計画の各施策による寄与の状況を検証することとする。なお、具体的な指標 については、前記「本行動計画の目標」を踏まえ、以下のとおり設定するものとする。

(1) 「安全基準等の整備及び浸透」に係る指標

- ○ **安全基準等の浸透状況等の調査により把握したベースラインとなる情報セキュリティ 対策に取り組んでいる重要インフラ事業者等の割合**
- ○ **安全基準等の浸透状況等の調査により把握した先導的な情報セキュリティ 対策に取り組んでいる重要インフラ事業者等の割合**

目次

1．概要 …… 3

2．アンケート調査 …… 6

3．往訪調査 …… 20

参考［アンケート調査結果］ …… 26

浸透状況調査（アンケート調査）の概要

- 浸透状況調査（アンケート調査）は、重要インフラ事業者等における安全基準等の浸透状況等を把握するため、重要インフラの各分野における情報セキュリティ対策の実施状況について調査するものであり、2019年度に引き続き、**2020年度は、指針が「『安全基準等』において規定が望まれる」として提示している情報セキュリティ（対策項目）（注）の実施状況等について調査**を行った。
- 本調査の結果から得られた知見や課題については、必要に応じて各施策へと展開するとともに、行動計画の検証や評価に活用することとする。

（注）これらの対策項目の実施の有無が当該事業者における情報セキュリティ対策のレベルを直ちに示すものではないことに留意する必要がある。指針においても、対策項目は「重要インフラ事業者等が採否を検討する」ものとされている。

調査の概要

調査内容	**指針が「『安全基準等』において規定が望まれる」として提示している対策項目の実施状況を確認** ［ 調査基準日：2020年３月31日 ］
調査対象	**各重要インフラ分野の事業者等** ※具体的な調査対象は、各重要インフラ分野を所管する重要インフラ所管省庁が選定（ ⇒ 調査対象は7ページに記載）
調査方法	次の方法で書面による調査を実施 **調査方法①：NISC調査** 内閣官房が作成した「調査票」配布し、内閣官房において集計　（金融分野を除く重要インフラ分野） **調査方法②：外部調査** 他の組織が実施した調査結果を、内閣官房が作成した「調査票」の結果に読み替え　（金融分野のみ）

調査結果の活用

【内閣官房】
- 得られた知見や課題は必要に応じて各施策へと展開
- **行動計画の検証や評価に活用**

【重要インフラ事業者等】
- 調査への回答を通じ、**自組織の情報セキュリティ対策の現状を確認**し、**改善・強化すべき方向性を把握**

調査票の構成

- 調査票では、これらの対策項目の実施状況が確認できるよう、指針の構成に沿って調査項目を設けることとした。

指針の構成

調査票の構成

Plan［計画］
- 設問１：組織の状況の観点
- 設問２：セキュリティポリシーの観点
- 設問３：情報セキュリティ対策の観点
- 設問４：支援の観点

Do［実行］
- 設問５：運用の観点

Check［評価］
- 設問６：評価の観点

Act［改善］
- 設問７：改善の観点

その他
- 設問８～設問11：その他の観点

調査票

- 情報セキュリティ対策のPDCAサイクルでは、通常、Planで分析結果を踏まえ対策を導出した上、Doで実行に移し、一定期間経過後、Checkで対策の見直しの必要性を評価し、Actで改善を実施するという流れになる。
- なお、実運用においては、Doでの監視・検知の結果次第では、緊急で対策内容を見直す等の動的な対応が必要となる場合がある。

調査対象及び回答状況

- 2020年度は、**全重要インフラ分野（計14分野）の事業者等を対象に調査を実施し、2,180事業者から回答**（回答率64.8%）を得た。

重要インフラ分野		調査対象事業者	回答数	調査方法
情報通信	電気通信	T-CEPTOAR構成各社、電気通信事業者協会正会員各社	20	NISC調査
	放送	日本放送協会（NHK）、地上系民間基幹放送事業者（多重単営社及びコミュニティ放送事業者を除く。）	97	
	ケーブルテレビ	ケーブルテレビセプターに加盟する全事業者	151	
金融		銀行等、証券会社、生命保険会社、損害保険会社	624	外部調査※1
航空		主たる定期航空運送事業者	7	NISC調査
空港		主要な空港・空港ビル事業者	8	
鉄道		ＪＲ各社及び大手民間鉄道事業者の主要な鉄道事業者	21	
電力		一般送配電事業者、主要な発電事業者	13	
ガス		大手事業者	10	
政府・行政サービス		都道府県及び市区町村	1,047	
医療		医療情報システムを導入している医療機関等の中からランダムで選定した事業者	28	
水道		現在給水人口30万人以上の水道事業者及び水道用水供給事業者	100	
物流		大手物流事業者	13	
化学		石油化学工業協会に加盟する事業者のうち主にエチレンセンターを運営する企業	9	
クレジット		重要インフラ事業者として定めている全事業者	21	
石油		石油連盟に加盟する石油精製・元売の全事業者	11	
全分野合計		―――	**2,180** （1,556）※2	

※1　金融分野については外部調査にて実施したものを、NISC調査の結果に読み替えて集計。
※2　全分野合計の（　）内の数値は、金融分野を除いた合計数。

調査票の構成（設問一覧）

NISC

□ Plan［計画］

- **組織の状況の観点**
  設問1-1. 外部環境・内部環境の整理
  設問1-2. 関係主体からの要求事項の整理
  設問1-3. サプライチェーンの把握
  設問1-4. 自組織で認識しているリスク
  設問1-5. 実施している対策

- **セキュリティポリシーの観点**
  設問2-1. 基本方針の策定・公表
  設問2-2. 安全基準等の把握
  設問2-3. 基本方針策定に当たり参考としている基準等
  設問2-4. 情報セキュリティ対策に関する責任・権限の割当
  設問2-5. 自組織で設置している情報セキュリティに係る役職等

- **情報セキュリティ対策の観点**
  設問3-1. リスクアセスメントの実施
  設問3-2. リスクアセスメントの実施主体
  設問3-3. 実施しているリスクセスメントの方法
  設問3-4. リスクアセスメントの定期実施
  設問3-5. 重要インフラサービスに与える影響の度合いの特定
  設問3-6. 情報セキュリティ対策の実施に当たり参考としている基準等
  設問3-7. 実施している情報セキュリティ対策
  設問3-8. 情報セキュリティ対策の取りまとめ
  設問3-9. 情報セキュリティ対策の導入・実施に関する計画の策定
  設問3-10. 事件・事故が発生した場合の情報開示基準の策定

- **支援の観点**
  設問4-1. 資源（人材・予算）の明確化、適切な配分
  設問4-2. 必要としている情報セキュリティ人材
  設問4-3. 情報セキュリティに係る人材育成や意識啓発に関する取組
  設問4-4. 情報処理安全確保支援士の活用
  設問4-5. 情報共有や意見交換を行っている関係主体
  設問4-6. 情報共有の範囲

□ Do［実行］

設問5-1. 情報セキュリティ対策の導入・運用段階における取組
設問5-2. 外部機関から共有・提供された情報の自組織での活用
設問5-3. コンティンジェンシープランの策定
設問5-4. 事業継続計画の策定
設問5-5. CSIRTの整備
設問5-6. 実施・参加している演習・訓練

□ Check［評価］

設問6-1. 情報セキュリティ対策に関する監査の実施
設問6-2. 実施しているセキュリティ評価

□ Act［改善］

設問7-1. 情報セキュリティ対策の改善に向けた継続的な見直し
設問7-2. 情報セキュリティ対策の見直しの契機

□ その他

- **経営層のコミットメント**
  設問8-1. 経営層の関与
  設問8-2. 経営層とのコミュニケーション
  設問8-3. 経営会議における情報セキュリティリスクの扱い

- **クラウドサービスの利用について**
  設問9-1. クラウドサービスに求める情報セキュリティ対策
  設問9-2. クラウドサービスの利用における責任分界点の把握
  設問9-3. データのバックアップ

- **新型コロナウイルス感染拡大を受けた取組について**
  設問10-1. 円滑な対応
  設問10-2. 重要インフラサービスの継続提供のための対策
  設問10-3. 需要インフラサービスの提供に係るテレワークの実施
  設問10-4. テレワークのセキュリティ対策

- **昨今のインシデント等に関する取組について**
  設問11-1. 記憶媒体の廃棄
  設問11-2. 外部サービス利用の対策
  設問11-3. 制御系システムのセキュリティ対策
  設問11-4. サイバー保険の加入

アンケート調査結果概要（総評）　－　ベースラインとなる情報セキュリティ対策

- 重要インフラの各分野における**情報セキュリティ対策の実施状況は2018年度から大きく向上**し、その傾向が継続していることから、**安全基準等の浸透は着実に進展**していると評価できる。一方で、引き続き項目によって実施状況に差があり、Plan（計画）に係る項目として比較して、Do（実行）、Check（評価）、Act（改善）に係る項目の実施状況は相対的に低いことから、これらを改善していくことが今後の課題である。
- 複雑化・巧妙化する情報セキュリティ上の脅威に対処していくためには、環境の変化にあわせて自主的に対策の見直しと改善を行っていく必要がある。重要インフラ事業者等においては、**PDCAサイクルを構築し、着実に情報セキュリティの確保に向けた取組を進めていくことが期待**される。

各取組の実施状況［過去度の調査との比較］

※ 以下の設問は、2018年度のデータがないため本欄に別記。

設問の中から基礎的な取組と考えられる対策項目を抽出して記載している。これらの対策項目を行動計画でいう「ベースラインとなる情報セキュリティ対策」とみなし、評価に活用することとする。

アンケート調査結果概要（総評）　－　先導的な情報セキュリティ対策（1/2）

NISC

- 行動計画では、**行動計画に基づく取組によって実現が期待される将来像を「理想とする将来像」として提示**している。これらの将来像に関連すると考えられる対策項目を「先導的な情報セキュリティ対策」とみなして本調査結果を整理したところ、**複数の項目で実施状況はおおむね向上**している。
- 「経営層との定期的なレポーティング・対話」「機能保証の考え方を取り入れたリスクアセスメント」等、引き続き実施状況が低い項目も見受けられるため、これらの実施状況も改善しており、**先導的な情報セキュリティ対策に関する取組も着実に進展**しつつあると評価できる。

将来像①：「情報セキュリティガバナンス」に関する次の事項が重要インフラ事業者等の間で十分に浸透している。

※金融分野を除く

情報セキュリティ対策が単に情報システムの構築・運用の観点だけでなく、**企業経営の観点からも検討**されていること。

- **経営層からの関与がある**（設問8-1）（※）

システムの構築・運用及び企業経営の**各責任者が定期的に、適切に相互関与する体制が整備**されていること。

- **経営層と定期的なレポーティング・対話の場が設けられている**（設問8-2）（※）

守るべき重要インフラサービス及びサービス維持レベルを踏まえ、**自らがなすべき必要な対策が理解**されていること。

- **関係主体からの要求事項を整理している**（設問1-2）（※）

- **機能保証の考え方を取り入れたリスクアセスメントを実施している**（設問3-1）（※）

平時における情報セキュリティ対策に対する姿勢やインシデント発生時の対応に関する**情報の開示などが取り組まれている**こと。

- **基本方針を策定し外部に公表している**（設問2-1）（※）

情報セキュリティ対策の水準の向上のためには可能な限り**情報共有を行うという姿勢が積極的に評価される価値観が醸成**されていること。

- **関係主体と情報共有を行っている**（設問4-5）（※）

事業における重要インフラサービス障害の発生について、これを隠すべきものではなく、重要インフラ事業者等内の情報セキュリティ対策に取り組む**関係者間で共有すべきものであるという認識が醸成**されていること。

- **関係主体と情報共有を行っている**（設問4-5）（※）【再掲】

将来像②：「課題抽出」、「リスク評価」及び「対策の改善」に関する次の事項が十分に浸透している。

※金融分野を除く

本行動計画に基づき、関係主体が連携して重要インフラ防護に関する情報セキュリティ対策に取り組むことによって、**自らの情報セキュリティ対策の程度及び残存するリスクが認識**されていること。

● **関係主体からの要求事項を整理している**（設問1-2）（※）【再掲】

● **機能保証の考え方を取り入れたリスクアセスメントを実施している**（設問3-1）（※）【再掲】

各種情報セキュリティ対策の進展や環境変化によるリスク源や重要インフラサービス障害に係る**リスクの変化を適切に察知して、各々自主的に対策を進め、また必要な調整を行うようになっている**こと。

● **内部環境や外部環境を整理している**（設問1-1）（※）

● **機能保証の考え方を取り入れたリスクアセスメントを実施している**（設問3-1）（※）【再掲】

● **情報セキュリティ計画を策定している（策定中を含む）**（設問3-9）（※）

重要インフラサービス障害が発生した場合に備えた適切な対策を講じることが可能になっており、その成果として、**重要インフラサービス障害が国民生活や社会経済活動に重大な影響を与えるリスクを可能な限り低減**させることができていること。

● **コンティンジェンシープラン（CP）を策定している**（設問5-3）（※）

● **事業継続計画（BCP）を策定している**（設問5-4）

これらの取組が**対策の継続的な改善の原動力の一つとなっている**こと。

● **基本方針等の継続的な見直しを行っている**（設問7-1）（※）

将来像③：「情報共有」に関する次の事項が十分に浸透している。

※金融分野を除く

重要インフラサービス障害の発生状況等に関する情報の把握ができており、必要に応じて当該情報が各分野のセプターやセプターカウンシルを通じて**外部の関係主体と共有され、公式又は非公式の連携が行われている**こと。

● **関係主体と情報共有を行っている**（設問4-5）（※）【再掲】

アンケート調査結果概要　－　Plan［計画］（1/3）

- 自組織の**重要インフラサービスに影響を与えるおそれがある環境の整理は多くの組織で実施**されており、自組織を取り巻く状況の把握は進んでいる。また、**リスクアセスメントについても着実に進展**してはいるものの、**外部環境を含めた環境の整理や機能保証の考え方の取り入れたリスクアセスメントは一部にとどまっており**、サイバー攻撃の高度化・多様化に伴うリスクの複雑化という観点からも、**今後も引き続きの取組が必要**である。
- なお、自組織のサプライチェーンの把握については重要インフラ事業者等において着実に意識付けされており、それらのリスクに対する対策も実施されている。

組織の状況の観点／情報セキュリティ対策の観点

► 自組織の重要インフラサービスの安定的かつ継続的な提供に影響を与えるおそれがある内部環境・外部環境を整理している（設問1-1）　※金融分野を除く

► リスクアセスメントを実施している（設問3-1）

※金融分野を含む

機能保証：重要インフラサービスを安全かつ持続的に提供するため、関係主体が情報セキュリティ対策に関する必要な努力を適切に払うことを求める考え方

組織の状況の観点

► 自組織のサプライチェーンを把握している（設問1-3）　※金融分野を除く

► サプライチェーンリスクについて実施している対策（設問1-5）　※金融分野を除く

アンケート調査結果概要　－　Plan［計画］（2/3）

- ①情報セキュリティ基本方針、②情報セキュリティ対策基準、③情報セキュリティ対策実施手順等を策定している組織は2018年度から大きく増加しており、**情報セキュリティに係る方針や基準の整備は着実に進展**している。ただし、具体的な基準や計画を規定する②情報セキュリティ対策基準を策定済みの組織は比較的少数にとどまっている。情報セキュリティ対策の実効性を確保するためにも、今後、各組織において策定されることが期待される。
- また、重要インフラ事業者等において、自分野の関係法令及び安全基準等は情報セキュリティポリシを改善していく上で把握、参考とされていることから、策定主体において**今後も適切な見直しを行っていくことが期待**される。

セキュリティポリシの観点／情報セキュリティ対策の観点

情報セキュリティに係る方針や基準の整備

①情報セキュリティ基本方針
情報セキュリティに対する組織としての統一的かつ基本的な考え方や方針

► **情報セキュリティ基本方針を策定している**（設問2-1）

②情報セキュリティ対策基準
情報セキュリティ基本方針を実践し、適切な情報セキュリティレベルを確保・維持するための具体的な遵守事項や基準

► **情報セキュリティ対策基準を策定している**（設問3-9）※金融分野を除く

③情報セキュリティ対策実施手順
情報セキュリティ対策を実施するための詳細な手続・手順（マニュアル等）

► **情報セキュリティ対策実施手順を全て策定している**（設問3-8）
※金融分野を除く

► **自分野に関係する安全基準等を把握している**（設問2-2）※金融分野を除く

- ほぼ全事業者等が自分野の安全基準等を把握している。

► **情報セキュリティに係る方針の策定に当たって参考としている基準等**（設問2-3）※金融分野を除く

- 設問2-2の安全基準等の把握も含めて、国や業界団体が策定する基準は、他の機関が策定する基準にとは比較して多数の組織が参照している。
- 各重要インフラ事業者等に情報セキュリティ対策の改善を促すツールとして非常に効果的である。

アンケート調査結果概要　－　Plan［計画］（3/3）

- 情報セキュリティに係る人材育成や意識啓発については9割以上の組織が何らかの取組を実施しており、**ほぼ全ての組織で研修や訓練を通じた人材育成等が行われている**。また、人材育成や意識啓発の取組の実施割合も2019年度と比較して増加している。
- 一方で、**自組織において人的資産が適切に配分されていると回答した組織はほぼ横ばい**の状況にあり、人材育成・意識啓発に関する取組は積極的に進められているものの、**情報セキュリティに係る人材が引き続き深刻**であることが確認できる。また、自組織で必要としている人材も管理者から現場の従事者まで多岐にわたっており、今後も**人材の育成・確保が多くの組織の課題**であるといえる。

支援の観点

► 情報セキュリティに係る人材育成・意識啓発の取組（設問4-3）※金融分野を除く

► 情報セキュリティに係る人的資産が適切に配分されている（設問4-1）

※金融分野を除く

► 自組織で必要としている情報セキュリティ人材（設問4-2）※金融分野を除く

アンケート調査結果概要　－　Do［実行］

- コンティンジェンシープランや事業継続計画の策定、CSIRTの整備は多くの組織で進められ、その実施状況は2018年度から大きく向上しており、**重要インフラサービスの障害の発生に備えた対処態勢の整備は着実に進展**している。
- また、演習・訓練の実施・参加、外部機関から共有・提供された情報の活用の状況から、重要インフラ事業者等が**自組織の対処能力の向上に努めていることが確認**できる。ただし、一部の組織は演習・訓練に参加していないことから、我が国全体の対処能力を向上させるためにも、それらの組織に対して**政府機関や公的機関が提供する演習等への参加を引き続き促していくことが必要**であると考えられる。

運用の観点

重要インフラサービス障害の発生に備えた対処態勢の整備

► **コンティンジェンシープラン（CP）を策定している**（設問5-3）→

► **事業継続計画（BCP）を策定している**（設問5-4）

► **CSIRTを整備**（注）**している**（設問5-5）（注）同等の機能を持つ組織を含む。

► **情報セキュリティ対策担当部署に対する責任・権限の割当て**（設問2-4）

演習・訓練及び情報活用による対処能力の向上

► **実施・参加している演習・訓練**（設問5-6）※金融分野を除く

► **外部機関から共有・提供された情報の活用**（設問5-2）※金融分野を除く

アンケート調査結果概要　－　Check［評価］／ Act［改善］

- 約2/3の組織で**内部監査を中心に情報セキュリティ対策に関する監査が実施**されており、**「評価」の枠組みは一定程度構築**されていると考えられるが、監査結果を基にした見直しの実施は少数にとどまっている。環境が変化していく中で適切に情報セキュリティを確保していくためには、現状を評価し、適時に改善していくことが必要不可欠であることから、**「評価」を「改善」につなげていく体制を構築していくことが引き続きの課題**であるといえる。
- また、**経営層の情報セキュリティ対策に対する関心の度合は徐々に高まっていることは望ましい変化**であり、今後に向けては定期的なレポーティング・対話の場や経営会議等への案件の付議等を通じて、**経営層との密なコミュニケーションを図っていくことが重要**であると考えられる。

評価の観点

► 情報セキュリティ対策に関する監査を実施している（設問6-1）※金融分野を除く

► 情報セキュリティ対策に経営層が関与している（設問8-1, 8-2, 8-3）

※金融分野を除く

※設問内容が2019年度と2020年度で異なる（2019年度は「積極的な関与」と「ある程度の関与」）為、参考

改善の観点

► 継続的に見直しを行っている（設問7-1）※金融分野を除く

► 情報セキュリティ対策の見直しの契機（設問7-2）※金融分野を除く

アンケート調査結果概要　－　その他（クラウドサービスの利用）

- 現在、**多くの重要インフラ事業者等においてクラウドサービスが利用**されており、クラウドサービス提供者側の情報セキュリティ対策として、不正アクセス対策や認証の方法の整備、アクセスログの管理、通信の暗号化等をはじめとするセキュリティ対策が実施されている。
- その一方で、**クラウドサービス提供事業者と自組織の責任分解点の把握した上で必要な情報セキュリティ対策を行っているのは約４割にとどまっており**、また、バックアップをとっていない事業者も一定数存在することから、**クラウドの特性を把握して適切に利用していく必要**がある。

クラウドサービスの利用について

► 自組織がクラウドサービスを利用する際に確認しているクラウドサービス提供事業者側の情報セキュリティ対策（設問9-1）

※金融分野を除く
（複数回答）

► クラウドサービス利用時における責任分界点の把握（設問9-2）

※金融分野を除く

► データのバックアップ（設問9-3）

※金融分野を除く

アンケート調査結果概要　－　その他（テレワーク等）

- 新型コロナウイルス感染症の拡大を契機に多くの組織でもテレワークが実施されたが、**重要インフラ事業者等においても半数以上の組織でテレワークが実施**されている。テレワークにおいては、一般にセキュリティ上の脅威が高まるため、適切にセキュリティ対策を実施していく必要がある。
- 外部サービスについても多くの組織で利用されているが、サービス提供者とのSLA（Service Level Agreement）の締結等の対策をとっていない組織が一定数存在するため、重要インフラサービスの安全かつ継続的な提供という観点から今後改善していくことが望まれる。

新型コロナウイルスの取組について

► テレワーク（在宅勤務）の実施（設問10-3）※金融分野を除く

► テレワークのセキュリティ対策（設問10-4）※金融分野を除く

その他

► 外部サービス利用時のセキュリティ対策（設問11-2）※金融分野を除く

► ハードディスクの廃棄（設問11-1）※金融分野を除く

目次

1．概要 …… 3

2．アンケート調査 …… 6

3．往訪調査 …… 20

参考［アンケート調査結果］ …… 26

浸透状況調査（往訪調査）の概要

- 内閣官房では、重要インフラ分野における情報セキュリティ対策の良好事例を収集するため、書面による安全基準等の浸透状況の調査に加えて、**重要インフラ事業者等に対して個別に調査（往訪調査）を実施**している。
- 2020年度の往訪調査においては、サイバー攻撃が複雑化・巧妙化し、その適切な対応が課題となっている昨今の状況を踏まえ、**情報セキュリティ対策の実施体制や監査体制、重要インフラサービスの持続的な提供、制御系システムのセキュリティ対策等の調査を実施**した。

【調査対象（2020年度）】 情報通信分野、電力分野、ガス分野、医療分野、化学分野、石油分野等の重要インフラ事業者等

往訪調査結果概要

事例① 情報セキュリティ対策の実施体制について

- CISOに直結する**情報セキュリティ責任者を各所に配置**
- 製品・サービスの情報セキュリティ対策を行うPSIRTを設置

✓ **CISOの指示の円滑な実施**
✓ 事案発生等の**迅速な対応の実現**

● 情報セキュリティ対策の権限の分担

事例② 情報セキュリティ監査について

- 監査者は、**自組織に必要な情報セキュリティが確保されているかの観点から監査**

✓ **監査を通じた情報セキュリティの確保**
✓ 監査の実効性の向上

● リスクベースの情報セキュリティ監査

事例③ 重要インフラサービスの安全かつ持続的な提供について

- **障害の内容や規模に応じた事業継続計画を整備**
- 人による運営ができるよう必要な紙媒体を準備

✓ 全ての情報システムが停止した場合でも、**サービスの継続的な提供**を実現

● 障害の内容や規模に応じた態勢を整備

事例④ 制御系システムのセキュリティ対策について

- 情報システム部門と生産製造部門の**連携体制の構築**。
- 情報系システムと制御系システムの**一元的な管理**

✓ **制御系システムも含めた一体的なセキュリティ**の実現

● 制御系システムを含めたセキュリティ対策

事例①　－　情報セキュリティ対策の実施体制について

NISC

事例の概要

- 情報セキュリティ対策の実施体制を強化するため、**最高情報セキュリティ責任者（CISO）に直結する情報セキュリティ責任者を各部署に配置**し、**CISOの指示を円滑に実施する体制を構築**している。また、組織内の情報セキュリティ対策を統制するCISRTに加えて、**自組織が提供する製品・サービスの情報セキュリティ対策を推進するPSIRT（※）を設置**し、情報セキュリティ上の脅威への対処能力の向上を図っている。
- さらに、情報セキュリティに関する組織横断的な委員会等を設置し、自組織の情報セキュリティ対策の検討・評価を行っている。
- これらの取組により、**組織内へのCISOの指示の徹底、情報セキュリティに関する事故への迅速な対処等を実現**するとともに、組織内外の意見も踏まえて**情報セキュリティ対策を評価・改善**することで、自組織の情報セキュリティの確保につなげている。

※Product Security Incident Response Team

情報セキュリティ対策の実施

- 各部署の情報セキュリティ責任者は、CISOの指示等を踏まえ、情報セキュリティ対策を着実に実施するとともに、情報セキュリティに関する事故が発生した際には事業責任者と協力して即応（サービス停止等）、事後対策（再発防止策の策定等）等を実施。
- CISOの下、情報セキュリティ部門に組織内の情報セキュリティ対策を統制するCISRTを設置。また、各部署にはPSIRTを設置し、自組織で提供している製品・サービスの情報セキュリティに関する監視を実施。

情報セキュリティ対策の検討・評価

情報セキュリティ委員会

CISOと各部署の情報セキュリティ責任者で構成

- 情報セキュリティに関する基本方針、具体的な対策等の検討

助言

アドバイザリーボード

外部から有識者や専門家を招へい

- 情報セキュリティ対策の助言
- 実施状況の評価

本事例のポイント

- ✓ 各部署に**CISOに直結する情報セキュリティ責任者を配置**。
- ✓ CISRTに加えて、**自組織が提供する製品・サービスの情報セキュリティ対策を推進するPSIRTを設置**。
- ✓ **外部有識者・専門家からの助言による情報セキュリティ対策の評価・改善**の実施。

本事例の利点

- ✓ 組織全体において、**CISOからの指示を迅速かつ円滑に実施**。
- ✓ 情報セキュリティに関する事故等に対し、**各部署の責任者が対応を迅速に判断**（サービスの停止等）。
- ✓ **組織全体で情報セキュリティ対策等の検討及び情報連携の実現**。

事例②　－　情報セキュリティ監査について

NISC

事例の概要

- 複雑化・巧妙化する情報セキュリティ上の脅威に対応するため、情報セキュリティに関する内部監査において、情報セキュリティ対策が規定どおり実施されているかをチェックリスト等に基づき確認するだけではなく、**国内外の事故事例や情報セキュリティに関する最新動向動向を踏まえて自組織のリスクを確認**（高リスク領域を中心としたリスクアセスメントの実施）**し、監査者と被監査者の対話を通じて情報セキュリティの確保を図るリスクベースの監査**を行っている。
- また、**監査部門と情報セキュリティ部門が連携して監査を実施**することにより、**情報セキュリティ監査の実効性の向上**を図っている。

ルールベースの情報セキュリティ監査
（チェックリスト等による定型的な監査）

実施目的・手法

目的
- 情報セキュリティ対策が規定どおり実施されているかを確認
- 情報セキュリティ対策の不備の是正

手法
- チェックリスト等を用いて、情報セキュリティ対策の実施状況の確認

実施主体

- ✓ 監査部門が、監査項目の一つとして情報セキュリティ監査を実施
- ✓ 情報セキュリティ部門は監査を受ける立場

リスクベースの情報セキュリティ監査
（リスクに応じた非定型的な監査）

目的
- 自組織に必要な情報セキュリティの確保
- 情報セキュリティに関するリスクの洗い出し
- 情報セキュリティ対策の不備の是正

手法
- 国内外の事故事例や情報セキュリティに関する最新動向を踏まえ、新たなリスクの確認（高リスク領域を中心としたリスクアセスメント等の実施）
- 国内外の最新のガイドラインへの対応状況の確認

- ✓ 監査部門が、情報セキュリティ部門と連携して情報セキュリティ監査を実施
- ✓ 情報セキュリティ監査に際し、情報セキュリティ部門の専門的知識を活用し、監査の実効性の向上

本事例のポイント

- ✓ 監査者は被監査者と協力し、**自組織に必要な情報セキュリティが確保されているかの観点から監査**を実施。
- ✓ **監査を通じ、自組織の情報セキュリティ関するリスクの洗い出し**を実施。
- ✓ 監査部門と情報セキュリティ部門の連携による監査の実施。

本事例の利点

- ✓ 国内外の事故事例や情報セキュリティに関する最新動向を踏まえ、自組織におけるリスクの確認を行うことにより、**監査を通じた情報セキュリティの確保を実現**
- ✓ 監査部門と情報セキュリティ部門が連携することで、監査部門の権限の下で、情報セキュリティ部門の専門的知識を活用した監査が可能となり、**情報セキュリティ監査の実効性の向上**

事例③　－　重要インフラサービスの安全かつ持続的な提供について

NISC

事例の概要

- 重要インフラサービスの安全かつ持続的な提供のため、CSIRTをはじめとする対処体制の整備に加え、自然災害、システム・ネットワーク障害、サイバー攻撃等を想定し、**非常時の事業継続計画（BCP）として障害の内容や規模に応じた対応手順を整理**している。
- また、必要なデータを紙で保管するなど**情報システムに依存せずにサービスが提供できるよう規程の整備、訓練等を実施**している。
- これらの取組により、自然災害、システム障害、サイバー攻撃等によって全ての情報システムが停止した場合でも、**必要最低限の重要インフラサービスの継続的な提供を実現**している。

重要インフラサービス障害を引き起こす事態

自然災害

障害等発生

システム障害

障害等発生

サイバー攻撃

障害等発生

・
・
・

重要インフラサービスの安全かつ持続的な提供が可能な態勢の構築

運営面の対策

- **障害の内容や規模に応じた対応手順の整備**
- **対処態勢の維持・運営**（関係者の招集、対策本部の設置、関係先への連絡等）
- 情報システムが使用できない緊急時対策として**情報システムに依存しない業務体制の確立**

設備面の対策

情報システムの故障等の対応

- **情報システム等の冗長化**（単一機器の障害等による影響を最小化）
- **無停電電源装置、非常用発電機等の設置**（停電による業務への影響を回避）
- **市場で十分な使用実績がある信頼性の高い機器の利用**（稼働率の向上、故障発生時の早期対応（代替品の入手等））

情報システム全体が停止した場合の対応

- **業務の継続に必要不可欠なデータのバックアップ、紙での保管**

演習・訓練等を通じて対処能力の向上

重要インフラサービス安全かつ持続的な提供の実現

本事例のポイント

- ✓ 障害の内容や規模に応じた**事業継続計画を整備**。
- ✓ 様々な障害に円滑に対応できるよう体制の運用面・設備面で必要な対策を実施。
- ✓ 情報システムが完全に停止した場合でも、**人による運営に切り替えられるよう必要な紙媒体を準備**。

本事例の利点

- ✓ 自然災害、システム障害、サイバー攻撃等によって全てのシステムが停止した場合でも、紙をベースとした人による運営に切り替えることにより、**必要最低限の重要インフラサービスの継続的な提供**を実現。

事例④　－　制御系システムのセキュリティ対策について

NISC

事例の概要

- 制御系システムに対するセキュリティを確保するため、**情報システム部門（情報系システムを管理）と生産製造部門（制御系システムを管理）が相互に連携して実施する体制を構築**している。
- 両部門の連携により**情報系システムと制御系システムを一元的に管理**することで、**制御系システムも含めた一体的なセキュリティを実現**している。
- また、制御系システムは原則として外部システム・ネットワークから遮断するとともに、**制御系システムを構成する機器ごとに個別に監視・制御を行うことで制御系システムを分割し、セキュリティ上の事故が発生しても影響を最小化**している。

本事例のポイント

- ✓ **情報システム部門と生産製造部門の相互理解による連携体制の構築**。
- ✓ **情報系システムと制御系システムの一元的な管理**。
- ✓ 制御系システムの**情報系システムからの遮断**。
- ✓ 制御系システムを構成する機器ごとに個別設計したUTMの設置。

本事例の利点

- ✓ **制御系システムも含めた一体的なセキュリティを実現**。
- ✓ 機器ごとに設定が異なる**制御系システムの統一的な監視の実現**。
- ✓ 制御系システムをUTMによって分割し、**セキュリティ上の事故が発生しても影響を最小化**。

※1. Unified Threat Management：　ファイアウォール、不正侵入検知防御システム等の複数のセキュリティ機能を統合した機器。
※2. DeMilitarized Zone：　情報系システムから制御系システムへの通信を遮断するため、情報系システムと制御系システムとの境界に設けられる領域。

目次

1．概要 ・・・・・・・・・・・・・・・・・・・・・・ 3

2．アンケート調査 ・・・・・・・・・・・・・・・・・・・・・・ 6

3．往訪調査 ・・・・・・・・・・・・・・・・・・・・・・ 20

参考［アンケート調査結果］ ・・・・・・・・・・・・・・・・・・・・・・ 26

設問１－１．【単一回答】
自組織の重要インフラサービスの安定的かつ継続的な提供に影響を与えるおそれがある外部環境（政治・経済・社会等）や内部環境（組織体制・業務内容等）について、近い将来の状況を含めて整理していますか。

設問１－２．【単一回答】
関係省庁、顧客、サプライヤー、委託先等からの、情報セキュリティに関する自組織への要求事項（各事業分野の関係法令や契約等に規定された義務、サプライヤーや委託先が提示する制限事項等）を把握して整理していますか。

設問１－３．【単一回答】
自組織のサプライチェーン（サプライヤー、委託先等）を把握していますか。

設問１－４．【複数回答】
サプライチェーンについて、自組織で認識しているリスクを全て選択してください。

設問１－５．【複数回答】
自組織のサプライチェーンに関するリスクについて、実施している対策を全て選択してください。

設問２－１．【単一回答】
自組織が情報セキュリティ対策に取り組む目的、方向性等を示した情報セキュリティ対策に関する基本方針を策定・公表していますか。

（内訳）金融分野を除く結果のため、上段の図の結果とは一致しない。

設問２－２．【単一回答】
自組織に関係する安全基準等を把握していますか。

設問２－３．【複数回答】
情報セキュリティに関する方針の策定に当たって参考としているものを全て選択してください。

設問２－４．【単一回答】
自組織の情報セキュリティ対策を担当する部署及び従業員を決定するとともに、それらの責任及び権限が明確になっていますか。

設問２－５．【複数回答】
自組織で設置しているものを全て選択ください。

設問３－１．【単一回答】
情報セキュリティ対策の実施に当たって、自組織でリスクアセスメント（リスクの特定・分析・評価）を実施していますか。また、機能保証の考え方を取り入れていますか。

設問３－２．【単一回答】
情報セキュリティに関するリスクアセスメントの実施主体を選択してください。

設問３－３．【複数回答】
自組織で実施しているリスクアセスメントの方法を全て選択してください。

注１　既存の標準や基準をもとにベースライン（自組織の対策基準）を策定し、チェックしていく方法
注２　コンサルタント又は組織や担当者の経験、判断により行う方法
注３　保護すべき資産を明確にし、資産に対する脅威を定義、脆弱性を評価して行う方法
注４　回避すべき事業被害を明確にし、被害を引き起こす攻撃シナリオの定義、発生可能性を評価して行う方法

設問３－４．【単一回答】
情報セキュリティに関するリスクアセスメントを定期的に実施していますか。

設問３－５．【単一回答】
自組織が重要インフラサービスを提供するために必要な情報システム（＝重要システム）を、重要インフラサービスに与える影響の度合いを踏まえて特定していますか。

設問３－６．【複数回答】
情報セキュリティ対策の実施に当たって、参考としているものを全て選択してください。

設問３－７．【複数回答】
自組織で実施している情報セキュリティ対策を全て選択してください。

人的資源のセキュリティ

物理的及び環境的セキュリティ

設問３－７．【複数回答】（続き）
自組織で実施している情報セキュリティ対策を全て選択してください。

設問３－８．【単一回答】
設問３－７で実施しているとした情報セキュリティ対策を内規（実施手順・マニュアル等）として取りまとめていますか。

設問３－９．【単一回答】
情報セキュリティ対策の導入や実施に向けた計画（目標・達成度・スケジュール等）を策定していますか。

設問３－10．【単一回答】
情報セキュリティに関する事件・事故（サービス停止、情報漏えい、改ざん等）が発生した場合の情報開示の基準を策定していますか。

設問４－１．【単一回答】
情報セキュリティ対策の実施に必要となる人材や予算が明確化され、組織内に適切に配分されていますか。

設問４－２．【複数回答】
自組織において、必要としている情報セキュリティ人材を全て選択してください。

設問４－３．【複数回答】
情報セキュリティ人材の育成や従業員の情報セキュリティに関する意識啓発について、自組織で取り組んでいるものを全て選択してください。

設問４－４．【単一回答】
自組織において、情報処理安全確保支援士資格取得者を活用していますか。

設問４－５．【複数回答】
重要インフラサービスの安全かつ持続的な提供を実現するという観点から、情報共有や意見交換を行っている関係主体を全て選択してください。

設問４－６．【単一回答】
自組織の情報システムの不具合について、重要インフラ所管省庁等との情報共有の対象範囲を選択してください。

アンケート調査結果　－　Do［実行］（1/3）

設問５－１．【複数回答】
情報システムの導入・運用時の情報セキュリティ対策を全て選択してください。

設問５－２．【複数回答】
外部機関から共有・提供された情報について、自組織で活用しているものを全て選択してください。

設問５－３．【単一回答】
重要インフラサービス障害の発生に備えたコンティンジェンシープランを策定していますか。また、機能保証の考え方を取り入れていますか。

（内訳）金融分野を除く結果のため、上段の図の結果とは一致しない。

設問５－４．【単一回答】
重要インフラサービス障害の発生に備えた事業継続計画を策定していますか。また、機能保証の考え方を取り入れていますか。

設問５－５．【単一回答】
自組織にCSIRT（又は同等機能を持つ組織）を整備していますか。

設問５－６．【複数回答】
情報セキュリティ対策に関する演習・訓練について、自組織で実施・参加しているものを全て選択してください。

設問６－１．【単一回答】
自組織の情報セキュリティ対策に関する目標の達成状況、計画の進捗状況等について、監査を実施していますか。

設問６－２．【複数回答】
自組織にて実施しているセキュリティ評価を全て選択してください。

設問７－１．【複数回答】
情報セキュリティ対策の改善に向け、継続的な見直しを行っていますか。

（内訳）金融分野を除く結果のため、上段の図の結果とは一致しない。

設問７－２．【複数回答】
情報セキュリティ対策の見直しの契機となったものを全て選択してください。

設問８－１．【単一回答】
情報セキュリティリスクが経営のリスクと認識され、その対応方針の策定に経営層が関与していますか。

設問８－２．【単一回答】
情報セキュリティリスクの対処に当たり、経営層とのレポーティング・対話の場が設けられていますか。

設問８－３．【単一回答】
情報セキュリティリスクが経営会議（経営層が一同に参加する会議）等に付議されていますか。

設問９－１．【複数回答】
自組織がクラウドサービスを利用する際に、確認しているクラウドサービス提供事業者側の情報セキュリティ対策等を全て選択してください。

設問９－２．【単一回答】
クラウドサービスを利用するに当たり、サービス提供者側とサービス利用者側の責任分界点を確認し、自組織において必要な情報セキュリティ対策を行っていますか。

設問９－３．【単一回答】
クラウドに保管しているデータについて、クラウド上のデータが消失する等の事態に備えて、自組織でデータのバックアップを定期的に取っていますか。

設問10－1．【単一回答】
新型コロナウイルス感染症の感染拡大防止のため、政府や自治体から外出の自粛等が要請されましたが、コンティンジェンシープランや事業継続計画に基づき円滑な対応が行うことができましたか。

設問10－3．【単一回答】
重要インフラサービスの提供に関する業務でテレワーク（在宅勤務）を実施していますか。

設問10－2．【複数回答】
新型コロナウイルス感染症の感染拡大が懸念される中で、重要インフラサービスの継続的な提供のため、自組織で実施している（実施した）対策を全て選択してください。

設問10－4．【複数回答】
テレワークの際に実施している情報セキュリティ対策を全て選択してください。

設問11－1．【単一回答】
ハードディスク等の記憶媒体を廃棄する際に、どのような対策を取っていますか。

設問11－3．【単一回答】
制御系システムも情報系システムと同等のセキュリティ対策を実施していますか。

設問11－2．【複数回答】
他組織が提供するサービス（外部サービス）が何らかの事由によって利用不可能となった場合に備えて行っている対策を全て選択してください。

設問11－4．【単一回答】
自組織でサイバー保険に加入していますか。