参考資料２

# 重要インフラサイバーセキュリティ研究会
# 分野別ヒアリング実施結果

令和８年３月18日
内閣官房国家サイバー統括室

# 分野別ヒアリング一覧



| | 対象分野 | 方式 |
|---|---|---|
| 情報通信 | 電気通信 | 第１回研究会 |
| | ケーブルテレビ | 個別 |
| | 放送 | 個別 |
| 金融 | 銀行等 | 第２回研究会 |
| | 証券 | 個別 |
| | 生命保険 | 個別 |
| | 損害保険 | 個別 |
| | 資金決済 | 個別 |
| 航空 | | 個別 |
| 空港 | | 個別 |
| 鉄道 | | 個別 |
| 電力 | | 第２回研究会 |
| ガス | | 個別 |
| 政府・行政サービス | | 個別 |
| 医療 | | 第２回研究会 |
| 水道 | | 第２回研究会 |
| 物流 | | 個別 |
| 化学 | | 個別 |
| クレジット | | 個別 |
| 石油 | | 個別 |
| 港湾 | | 個別 |

# （参考）分野別ヒアリングの実施方針



■ヒアリングの目的

サイバーセキュリティ対策に関して、各重要インフラ分野における特性・実情、また、国・業界団体等が定めるガイドライン等の普及促進に向けた取組や課題、重要インフラ事業者等の反応・ニーズ等について把握し、重要インフラサイバーセキュリティ対策推進会議における重要インフラ統一基準の検討に当たって、それらを考慮することにより、重要インフラ統一基準によるPDCAサイクルの実効性を高める。

■ヒアリング対象

15重要インフラ分野における上記の特性・実情や現状課題を俯瞰し得る団体・事業者（主にはセプター事務局）。

■ヒアリング実施方法

15重要インフラ分野を対象に質問票を送付、回答をいただくとともに、次の（１）または（２）の方法によりヒアリングを実施。

（１）研究会の場におけるヒアリング

- 研究会の場において、質問票の内容に沿ったヒアリングを実施。
- 各省庁の所管分野の中から１分野程度を選定。

（２）NCOによる個別ヒアリング

- （１）以外の分野を対象に、NCOが質問票の内容に沿って個別ヒアリングを実施。結果をとりまとめ研究会に報告。

# （参考）分野別ヒアリングの実施方針



■ヒアリングの観点

- 重要インフラ統一基準の実効性を高めるためには、現状、各分野において、国・業界団体等によるガイドライン等がどのように効果をもたらしているのか、そのための普及促進の取組や課題、また、受け手となる重要インフラ事業者等の構造や反応・ニーズ等について、背景事情として把握し、それらを踏まえた上で、重要インフラ統一基準の具体化検討を進めることが重要。
- 特に、これまで重要インフラサイバーセキュリティ対策推進会議において、サイバーセキュリティ確保の取組やその水準は分野・事業者によって様々であり、ばらつきが見られるとの複数のご発言があったところ、ヒアリングによってその実情を具体的に把握し、それらを踏まえた上で、重要インフラ統一基準で定める、重要インフラ事業者等において分野・事業者横断的に講ずべきサイバーセキュリティ対策（ベースライン）の適切な水準について検討を進めて行くことが重要。

■質問項目

- 設問１は、上記観点を踏まえ各分野の概要について質問。設問２はさらに、個別トピックを加えて質問。

■設問１：ガイドライン等の現状

（１）情報システムの構成
（２）サービス維持レベルの現状
（３）ガイドライン等の作成及び普及促進に向けた取組
（４）重要インフラ事業者等からの問合せや相談

■設問３：その他課題

■設問２：個別対策に係る課題等

（１）サイバーセキュリティ人材の確保
（２）ランサムウェア等への対策
（３）基盤・制御システム等のサイバーセキュリティ確保
（４）サプライチェーン・リスクへの対応①（取引先、業務委託先等）
（５）サプライチェーン・リスクへの対応②（情報システム等の調達）
（６）先端技術への対応

# 分野別ヒアリングから得られた考察ポイント



| 項目 | 考察ポイント |
|---|---|
| サイバーセキュリティ人材の確保・育成 | ✓ 人材確保の問題は、中規模以下の事業者において顕著だが、大手事業者を含め全体的に不足。<br>✓ 制御システムやインシデントレスポンスに精通した人材確保・育成は特に課題。<br><br>⇒ 分野内、分野・地域間の連携による人材確保・育成を促進しつつ、必要な人材の知識・スキルに応じたアプローチ選択が重要ではないか（例 分野・業界内でのトレーニー派遣、人材プール等）。<br>また、人材マッチングやキャリア形成など、効率的・効果的な人材の確保・育成のため、必要な知識・スキル等を体系的に整理したサイバーセキュリティ人材フレームワークの活用が有効ではないか。 |
| ランサムウェア等への対策 | ✓ ランサムウェア対策を重要視しつつも、会社規模によって、また、同社内でも担当部局によって対応の違いが見られる場合あり。<br>✓ 脆弱性対応は、対処すべき脆弱性が多く、大きな負荷となっている。<br>✓ EDR・MDR・XDR 等は、ランサムウェア対策として導入との意見が多数あるが、対策コストや専門性の要求等について要考慮。<br>✓ 多要素認証は凡事徹底が重要であり、重要なITシステムについてデフォルト化するのも一案。<br><br>⇒ IT・OTや分野によって脆弱性対応等の要求水準が異なることを踏まえ、重要インフラ統一基準においては、リスクベースの取組やサイバー・フィジカル・セキュリティ対策としての基本的な考え方を記載することが適当ではないか。<br>他方で、リスクマネジメント及び危機管理の両面から、体制や取組の有効性検証を進めることが重要であり、各分野・事業者における実践的な演習・訓練の実施の他、政府等が実施する最新の脅威動向を踏まえたな演習等への参加も有効ではないか。 |

# 分野別ヒアリングから得られた考察ポイント



| 項目 | 考察ポイント |
|---|---|
| 基盤・制御システム等のサイバーセキュリティ確保 | ✓制御システムにおいてソフト・ハードの汎用機採用、IT技術の浸透が進んでいる一方、OT技術者のIT知識が不足している場合あり。<br>✓OTの維持管理を別会社が行っている場合等があり、連携のための工夫が必要。<br>✓そもそも基盤・制御システムのサイバーリスクがあまり想定されていないと思われる分野がある等、分野によって相当の温度差あり。<br><br>⇒ 「閉域網は安全ではない」※との認識を前提として、基本的対策の徹底を促進することが重要ではないか（例えば、重要システムと他システムのネットワーク原則分離等）。<br>また、閉域網において専用OSを使用していれば安全といった考えを各分野で変えていくための戦略的なアプローチが必要ではないか（例えば、業界のWG活動、業界ベストプラクティスの共有等）。<br>※ メンテナンス等のための外部接続点を標的とした攻撃リスク、内部の役職員の不正行為リスク等 |
| サプライチェーン・リスクへの対応 | ✓契約条項でのセキュリティ要件や役割・責任分担の明確化等により対応。<br>✓事業者規模等による委託先のセキュリティレベルの差、国内外に分散する取引先等への個別対応、委託先とのリスク管理等の確認に係る負担等が課題。<br>✓クラウド利用で高いセキュリティレベルが求められる場合等において、さらなるクラウド事業者側のリスク把握や、利用開始以降に顕在化したリスクへの対応は課題あり。<br><br>⇒ 委託先とのリスク管理等の確認に係る負担軽減や利便性向上のため、TPRM標準化等の仕組みが有効ではないか（例えば「サプライチェーン強化に向けたセキュリティ対策評価制度」の活用等）。<br>また、クラウドサービス利用を含む情報システム等の調達に当たっては、第三者認証や評価制度の活用の他、クラウド事業者がサイバー攻撃を受けるリスクや、利用開始以降に顕在化したリスクへの対応への備えとして、役割分担を明確にしサイバーセキュリティ対策の実効性を確保するために参考となる考え方の参照が有効ではないか（例えば「サイバーインフラ事業者に求められる役割等に関するガイドライン」等）。 |