資料１

重要インフラサイバーセキュリティ研究会における議論

令和７年11月27日
内閣官房国家サイバー統括室

重要インフラサイバーセキュリティ研究会の開催について

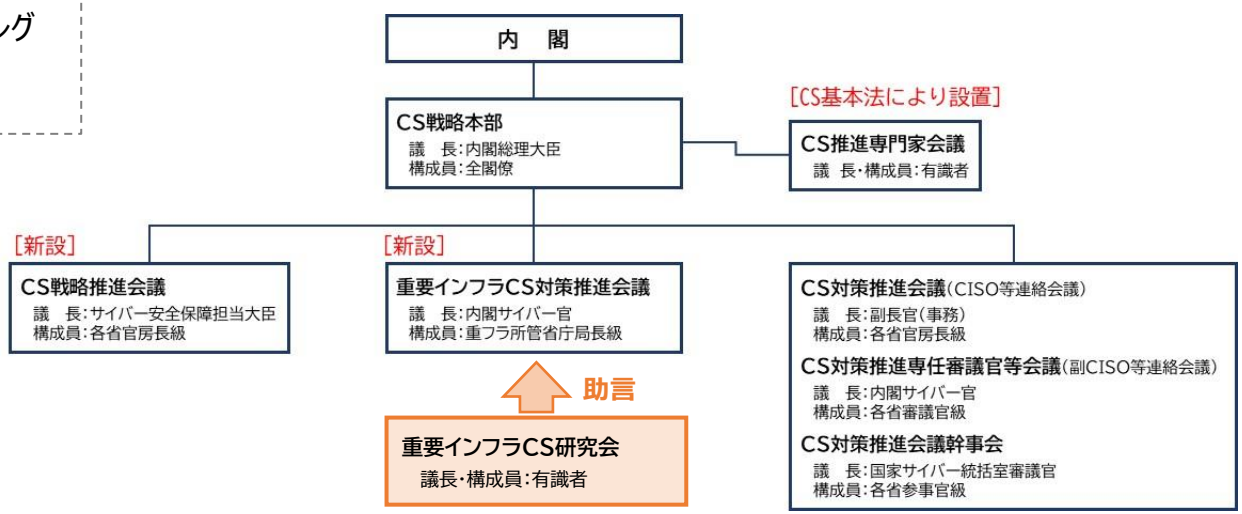
- 我が国全体の重要インフラ防護に資するサイバーセキュリティ対策の推進に向けて、重要インフラサイバーセキュリティ対策推進会議における検討に資するため、内閣サイバー官の私的懇談会として、重要インフラサイバーセキュリティ研究会を開催。

➢ 開催趣旨
- 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検討に当たり、各重要インフラ分野における特性・実情の把握や現状課題の整理、それらを踏まえた議論等を通じて、民間有識者の知見・示唆を得るため開催。

➢ 検討内容
- 各重要インフラ分野における特性・実情の把握及び現状課題の整理
- 重要インフラ統一基準（ガイドライン含む）の検討に資する助言
- 重要インフラのサイバーセキュリティに係る行動計画の検討に資する助言
- その他

➢ 開催頻度
- 今年度は３回程度。

今後のスケジュール案
- ➢ 第１回（11/5）　：キックオフ、分野別ヒアリング
- ➢ 第２回（12月頃）　：分野別ヒアリング
- ➢ 第３回（２月頃）　：基準案への助言



重要インフラサイバーセキュリティ研究会　構成員名簿

令和７年11月５日時点（五十音順、敬称略）

構成員	江崎　浩	東京大学大学院情報理工学系研究科　教授
	大日向　隆之	一般社団法人金融ISAC　理事 株式会社三菱総合研究所　エグゼクティブフェロー
	柿崎　淑郎	東海大学情報通信学部　准教授
	北尾　辰也	国土交通省　最高情報セキュリティアドバイザー
	小松　文子	ノートルダム清心女子大学情報デザイン学部　教授
	小山　覚	NTTドコモビジネス株式会社情報セキュリティ部　部長
	神保　謙	慶應義塾大学総合政策学部　教授
	長島　公之	公益社団法人日本医師会　常任理事
	西本　逸郎	株式会社ラック　技術顧問
	山岡　裕明	八雲法律事務所　弁護士
	渡辺　研司	名古屋工業大学大学院工学研究科社会工学専攻　教授
オブザーバ	高見　穣	独立行政法人情報処理推進機構　セキュリティセンター グループリーダー

分野別ヒアリングの実施について

■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。

分野別ヒアリングの実施について

■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ではないか。
- 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ではないか。

■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

重要インフラサイバーセキュリティ研究会（第１回）における主な意見

【重要インフラ統一基準の作成にあたって】

- 演習・訓練、あるいはその後のアフター・アクション・レビュー、すなわち振り返りを行って改善につなげるという観点からの検討も重要。
- 平時における対策だけでなく、緊急時のインシデント対処を念頭においた対策も示すことが重要。
- NIST CSFを参照してはどうか。
- As Is、すなわち現在用いられているシステムに対してどのようなセキュリティ対策を講ずるべきかに加え、To Be、すなわち30,40年後のシステムに対するセキュリティ対策はどうあるべきかの議論が必要。
- 国際標準等との整合性を確保することが重要。その観点から、いわゆるゼロトラストを基本にすべき。
- 共助の概念も取り入れるべきではないか。
- ボトムアップのアプローチにより共通的なセキュリティ対策を抽出するのではなく、あるべき姿を見据え、トップダウンでベースラインを検討すべき。
- リスクとの兼ね合いによって必要な対策が決まる。また、丁寧なスコア評価が重要。例えば、「不正プログラム対策ソフトを導入し定義ファイルが常に最新の状態となるように構成する」といった対策について、クローズドネットワークでは、この対策のためにネットワークにインターネットとの接続口をつけると、かえってリスクを高める。
- 基準で定める対策項目の水準設定については現実的・最適化の視点が重要。一般的に、企業のセキュリティ・ポリシーの水準を厳しくしすぎると負担が大きく形骸化しやすい。また一度、厳しく設定すると緩くするのがなかなか難しい傾向にある。
- 行動計画で例示されている「対象となる重要システム」に限らずネットワーク全体の評価を行うべき。

重要インフラサイバーセキュリティ研究会（第１回）における主な意見

【重要インフラ統一基準の作成にあたって】

- 所管省庁と業界団体の棲み分けや役割分担についても整理すべき。
- 浸透状況調査における事業者の回答率が100%ではないところ、その理由として、セキュリティ担当者が通常業務により逼迫し、調査回答の余力がない可能性があるのではないか。
- ベースラインの要求事項と、リスク評価は区別して議論すべき。
- CS戦略との整合も重要。新たなCS戦略は、強化法をはじめアクティブな内容となっている。分野等によっても条件は異なると思うが、（強化法における）基幹インフラ事業者を対象とした制度との連動の考慮が重要。
- 新たな基準によるブレイクスルーを目指すにあたっては、「官民連携」等の要素も含め検討すべき。
- 新たな基準の活用によるメリット・デメリットを今後分かりやすく説明いただきたい。
- 重要インフラ企業の取締役のスキル・マトリックスとして、サイバーセキュリティのスキルを求めてはどうか。
- 固定的な対策事項の一方で、その時々でタイムリーな対策事項もある。２層に分けて、それら対策事項を扱えるようにしてはどうか。