重要インフラサイバーセキュリティ研究会（第１回）議事概要

１　日時

令和７年 11 月５日(水)16:00～18:00

２　場所

赤坂グリーンクロス４階　会議室

３　出席者

【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

４　議事概要

【議事】

（１）重要インフラサイバーセキュリティ研究会について

・事務局（国家サイバー統括室）から、資料１、資料２及び資料３に基づき、本研究会の開催や運営について説明。

・飯田陽一内閣サイバー官の指名により、渡辺構成員が主査に選任された。

・資料３の本研究会の運営要領（案）について、特段の異議等なく決定された。

（2）重要インフラにおける現状課題等について

・事務局から、資料４及び資料５に基づき、検討の背景及び重要インフラのサイバーセキュリティに係る施策の基準等に関する今後の取組方向性の骨子について説明。

【主な発言】

〇構成員

・重要インフラ統一基準の検討に当たり、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。

〇構成員

・重要インフラ統一基準の検討に当たり、純粋な平時の観点だけではなく、例えば国家を背景とする攻撃者による重要インフラ等への事前侵入等、有事の観点からの検討も行っていただきたい。

〇構成員

・サイバーセキュリティ確保の取組やその水準は分野・事業者によってばらつきが見られるところ、動的な観点を視野に入れつつ重要インフラ統一基準を策定するべきではないか。

〇構成員

・例えば米国 NIST サイバーセキュリティフレームワークは、平時だけでなく、有事における復旧対応まで視野に入れて策定されている。NIST サイバーセキュリティフレームワークをボトムラインとし、その上に乗る部分で分野ごとの特徴等について対応していくことが自然な形だと思う。

・今回のベースラインの策定は正しい方向性であると考える。その際、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、ToBe、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である。あるいは両者の中間部分、現状からどのように移行していくかも重要なポイントである。

・重要インフラ統一基準の検討に当たり、国内仕様に閉じたものではなく、国際標準等との整合性を確保した上でのサイバーセキュリティを確立することが重要と考える。その観点から、いわゆるゼロトラストを基本にすべきである。

〇構成員

・インシデント対応においては、自助共助公助の共助の観点が重要である

ため、重要インフラ統一基準には、共助の概念も取り入れるべきではないか。例えば欧米ではインシデント・コマンド・システムが普及しつつある。制度関係の調整を要するため、策定段階では難しいかもしれないが、将来的に共助の基本的な考え方を整理いただきたい。

○構成員

・重要インフラ統一基準の策定に当たり、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いただきたい。低いレベルに合わせた場合、脅威への対応が不十分となりサイバー攻撃を受けるリスクがある。

○構成員

・重要システムへのサイバー攻撃対策は、重要システムに対するサイバー攻撃が重要インフラサービスに与えるリスクとの兼ね合いによって必要な対策が決まってくる。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。

○構成員

・重要インフラ統一基準の視点として、ベースラインに賛成であるが、ベースラインの厳格化は形骸化を招き、かえってリスクを高める面もある。大規模な重要インフラほど、一度厳格化すると緩めるのは困難であることからも、現実的・最適化されたベースラインという視点が重要。例えばヒアリングに加えて、データに基づいてもベースラインを設定すべき。例えば、警察庁の公表データ（「サイバー空間をめぐる脅威の情勢等について」）によれば、不正アクセスの原因として、ID・パスワードからの侵入が最も多い。また、近時の証券口座の不正アクセス事案では、証券会社が多要素認証を導入してから被害が減少している。一例を挙げると、このようなデータを踏まえ、ベースラインとして多要素認証やパスキーの導入について検討することが考えられる。

（3）分野別ヒアリングについて

・事務局から、資料６及び資料７に基づき、分野別ヒアリングの実施及びヒアリング質問票について説明。

・情報通信分野のヒアリング対象の担当者から、資料８に基づき、ヒアリング質問票に対する回答について説明。

（ヒアリング質問票に対する回答及びそれに関する質疑応答は非公開）

【主な発言】

○構成員

・ヒアリング質問票について、対策のみについて質問しており、背景状況を質問していない。重要インフラサービスと重要システムの関係、重要システムが異常な動きや停止するとどうなるのか（サービス維持レベルへの影響）、代替策でどのぐらい耐えられるのか、重要システムのプラットフォーム（IT・制御システム（汎用 OS）・制御システム（専用 OS））、ネットワーク（閉域・オープン）、重要システムの使われ方（制御システムでは立ち上げっぱなしのケースも少なくない）、サプライチェーンや調達の状況と想定されるリスクといった観点も加えるべき。

・ランサムウェア攻撃や破壊型のサイバー攻撃は、ネットワーク全体に被害が発生する。重要システムが他の多くのシステムと同じネットワークに属しており、ネットワーク全体に影響が及ぶようなサイバー攻撃が発生した場合、たとえ重要システムが無事であっても簡単には動かすことはできない。重要システムが他の多くのシステムと同じネットワークに属している場合、ネットワーク全体に被害が発生するケースを想定し、早期復旧のための仕組みやプランが必要であり、重要インフラ統一基準にはこの観点が必要と考える。

・態勢、対策に対する評価、人材育成、演習・訓練、情報収集・情報共有が重要。例えばリスクベースで考えて状況を踏まえて判断できる人を育てていかないといけない。

・実施状況の把握、評価について、重要システムに対するサイバー攻撃が重要インフラサービスに与える影響の大小が、対策の出来不出来の点数と相関関係を持つと想定される。しかしながら、点数が低いから十分な対策ができていない、点数が高いから十分な対策ができているということには単純に結びつかないことを認識していただきたい。

○構成員

・資料７・３頁の「（３）制御システム（OT）のサイバーセキュリティ確保」について、プラントの製造設備等の典型的な制御システム（OT）だけではなく、例えば情報通信を司るシステム等も、その重要性を踏まえると質問対象に加える必要があるのではないか。

○構成員

・ヒアリングを実施するに当たり、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である。例えば医療分野では、厚労省が主体

となってセキュリティ対策を推進しているため、事業者側だけではなく厚労省にもヒアリングを行い、全体像を把握すべきである。

〇構成員

・参考資料１によれば、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。組織の余力がなければサイバーセキュリティ対策を実施することは不可能であることから、未回答の理由の把握及び解決を行わなければ、策定した重要インフラ統一基準が十分に機能しないことが想定される。

〇構成員

・ヒアリング質問票について、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ではないか。例えば、あるベースラインの要求事項が、分野によってはリスクベースでは不要という場合もある。また、例えばインシデントにより自社業務に対してどのようなインパクトが発生するかは、プロファイルによって異なるはずである。このように、これらの議論は区別すべきと考える。

（４）その他

【主な発言】

〇構成員

・本年末を目処に策定予定のサイバーセキュリティ戦略と重要インフラ統一基準を連携させ、同基準を同戦略の実装の最前線として位置付けることが望ましい姿だと考える。

・現在公表されている同戦略の案は、基幹インフラ事業者における報告制度の基盤整備、脅威ハンティング、アクセス・無害化措置等について記載されるなど、官民連携の強化が図られていることが特徴。これらを踏まえると、重要インフラ統一基準におけるベースラインの取組についても、新たなフェーズの考えが必要なのではないか。業種により対応の仕方やベースラインの考え方が異なる中、新しい能動的サイバー防御の考えをどのように重要インフラ統一基準に実装していくことができるかについても今後議論させていただきたい。

〇構成員

・重要インフラ統一基準について、重要インフラ事業者等が遵守すべきことのみを対象に策定するのであれば大きなブレイクスルーは起きないように思う。例えば官民連携もスコープに含めることで、重要インフラ

全体のセキュリティ対策の底上げを図ることができるのではないか。

〇構成員

・重要インフラ統一基準の位置付けと具体的な活用方法が明確ではない。同基準の活用による、重要インフラ分野のメリット・デメリットを今後分かりやすく説明いただきたい。

〇構成員

・過去の重要インフラ対策関連文書の改定について、「重要インフラのサイバーセキュリティに係る行動計画」では、「経営層の内部統制システム構築義務には、適切なサイバーセキュリティを講じる義務が含まれ得る」と明記された。また、安全基準等策定指針では、CISO の設置が明記された。いずれも重要インフラの経営層においてサイバーセキュリティの関心が高まる要因となったと考えられる。このようにコーポレートガバナンスの視点を加えるのは重要と思われる。新たなアイディアとして、例えばコーポレートガバナンスコード 4－11 で取締役のスキル・マトリックスの開示が補充原則として記載されている。そこで、重要インフラ企業においては、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。安全基準等策定指針 3.7「情報開示」にサイバーセキュリティのスキル・マトリックスを加えるイメージである。

〇構成員

・米国 NIST サイバーセキュリティフレームワークは、旧バージョンでは重要インフラ事業者向けであったが、現行の 2.0 では重要インフラ事業者に限らず一般向けにチューンナップされており、重要インフラ統一基準を策定する上でも参考になるものと考える。

・資料４・21 頁には、分野横断的に全体として対策の水準を上げるための仕組みとして、複数レベルに分けた提示も想定されている。各重要インフラ分野における特性や実情といった観点を踏まえると、例えば、重要インフラ統一基準を２階建ての構成とし、１階部分にはベースラインとなる対策を記載し、２階部分には各重要インフラ分野の特性や実情に合った対策を記載することも一案ではないか。その際、１階部分と２階部分を併せて策定するというよりは、２階部分については、タイムリーなサイバー攻撃にも対応できるような柔軟な設計とすることも一案ではないか。

【今後の予定】

・事務局から、次回の研究会の開催予定について説明。