資料１

重要インフラサイバーセキュリティ研究会
これまでの議論（主な意見）

令和８年３月18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（第３回）における主な意見

【重要インフラ統一基準の作成等にあたって】

- CISOの設置が重要。グローバルに見ても、重要インフラ分野においてCISOの設置が推奨を超え義務化されつつある。
- サイバー保険について言及することも一案。近時のランサムウェア攻撃事案でも示されているように、サイバー攻撃により極めて大きな財務的インパクトが発生し得る。ファイナンス部門におけるサイバーリスクに対するソリューション、特に財務的観点からの対策についても、重要インフラ分野において重要視すべきではないか。
- キャッシュフローの確保は、重要インフラ分野において極めて重要な要素であり、政府間の融資といった手段も含め、広く検討すべきではないか。
- ゼロトラストの導入の有無を問わず、レジリエンスの観点から、セグメンテーションによる分離は非常に重要。また、「専用OSだから」「閉域網だから」に加えて、「独自技術仕様だから安全」と認識している例が見受けられるものの、オープンな通信プロトコルではないという理由のみで安全性が担保されるわけではない。
- 閉域網に配置されたネットワーク機器が必ずしも安全ではない理由の一つは、脆弱性に対するパッチ適用が困難である点にある。実際、10年、20年と脆弱性を抱えたままネットワーク機器が稼働し続けているケースも存在する。そこで、ネットワーク機器の更改や、パッチ適用の対策が実効的に進むような記載を取り入れてはどうか。
- リスクマネジメント、あるいはリスクベースの考え方においては、どの文脈で誰を主体として想定するのかについて留意する必要があるのではないか。
- 情報共有については、レイヤーを３段階で考えることが重要。すなわち、同盟国を中心とした国際的な共有、業界内での共有、事業者内部での共有という３つの段階で実施する必要がある。
- 情報共有については、例えば、同一地域内における分野を超えた情報共有といった、地域内の観点も重要。

重要インフラサイバーセキュリティ研究会（第３回）における主な意見

【重要インフラ統一基準の作成等にあたって】

- セキュリティ対策に必要な資源の確保について、重要インフラ事業者等に対しては、投資対効果の観点にとどまらず、社会的使命であり、あるいは最大許容停止時間であるMTPDを達成するために必要な投資であるといったメッセージを発信しなければ、経営層の意思決定には結び付かないのではないか。また、資源の確保の最終的な責任者を誰とするのかという点も重要。
- セキュリティが企業の経営層の課題であることを明記してはどうか。
- 検知の体制について、AIの活用は、攻撃への対処におけるスピード感が高まる中で、深刻化するセキュリティ人材不足の解消につながる取組であると考えている。今後AI、ひいてはAIエージェントを踏まえた対策についても議論していく必要がある。
- 重要インフラ統一基準において対象となる分野・事業者を特定するに当たり、一定の基準を示す必要があるのではないか。例えば、人口カバー率が一定割合以上である事業者や、代替性が低い事業者等といった特定の基準を示すことが考えられる。
- リスクアセスメントの重要性を強調すべき。企業が、従来の手法にとどまってリスクを適切に特定できず、新しい脅威に対応できずに失敗している例がある。また、ネットワーク制御の観点、特に、必要最小限の通信のみを許可するという考え方が重要。さらに、バックアップについては、サイバー攻撃によって破壊されない形式でバックアップを確保することが重要。
- リスクアセスメントについては、確定しているリスクだけを追いかけるのではなく、水平スキャン等を通じて、潜在的・隠れたリスクが存在しないかを発見する行為が重要。
- 人材育成では、担当者レベルのみならず、CISO等のサイバーセキュリティのリーダーとして組織を牽引する人材も育成するという観点も必要ではないか。

重要インフラサイバーセキュリティ研究会（第３回）における主な意見

【重要インフラ統一基準の作成等にあたって】

- 医療分野は特殊であり、小規模な医療機関をはじめ、ほとんどの医療機関では、十分なセキュリティ対策を実施できていない。現場の混乱を避けるためにも、このような医療分野の特殊性、現場の実情等を踏まえた施策を検討いただきたい。また、政府側からの支援も併せて検討いただきたい。他方で、例えば、オンライン資格確認、電子処方箋、電子カルテ共有サービス等を運営する社会保険診療報酬支払基金については、社会的影響が大きいため、対策を徹底する必要がある。
- 重要インフラ統一基準を通じた政府機関における施策のPDCAサイクルにおいては、上位からの指示・下位からのレポートの実効性、あるいはチェックの実効性を確保するため、評価の基準が必要。
- 重要インフラ事業者の実情や、取組と要求事項とのギャップを正確に把握するためには、場合により、国家サイバー統括室が、直接重要インフラ事業者に対して調査やヒアリングを実施し、情報を収集する必要があるのではないか。
- 官民連携においては、政府機関と重要インフラ事業者・業界団体等が方向性を共有し、議論を重ねながら協働して進めていくことが重要。
- 今後の重要インフラ所管省庁等も含めた議論では、方向性がずれないよう、そもそもサイバーセキュリティは誰のためにあり、何を実施すべきかという点について認識を共有する必要がある。大きな方針としては、エンドユーザーへのサービスのクオリティを確保するということから議論をスタートさせるべきではないか。

重要インフラサイバーセキュリティ研究会（第３回）における主な意見

【行動計画の改定にあたって】

- 重要インフラに関連する制度や文書が多数存在しており、各事業者等が何を遵守し、あるいは実施すべきなのかが分かりにくくなっているのではないか。今後の行動計画の改定では、各事業者等において内容の理解が進むよう、記載等を工夫いただきたい。

【その他】

- 近時発生したサイバー攻撃の事案も踏まえると、今後の議論では、被害の影響が他分野等に波及するような、単一障害点になっているサービス（例：大手小売業の物流）をどのように位置付けるかについても議論していく必要がある。
- 重要インフラ対策において、クラウドサービス、あるいはデータセンターをどのように位置付けていくかは重要ではないか。

重要インフラサイバーセキュリティ研究会（第２回）における主な意見

【重要インフラ統一基準の作成等にあたって】

- セキュリティ人材の不足は分野共通の課題。
- 小規模な医療機関をはじめ、ほとんどの医療機関では、知識・財源・人材の不足により、十分なセキュリティ対策を実施できておらず、大きな課題。
- 各分野で共通する取組、例えば人材育成、人手の派遣、研修等について、分野を超え、あるいは地域間で連携して実施できるようになると望ましいのではないか。重要インフラ統一基準においては、各分野の連携を促進するといった観点で作成していただきたい。
- 相互依存性の観点を踏まえ、重要インフラサービスに関連する他分野のサービスの防御についても留意する必要がある。
- 安易に専用OSであればセキュリティが確保されると思っているのであれば、危機感を持つべきである。このように、各分野のリスクアセスメントの中で、共通して抜けているものについてより注意すべき。
- 重要インフラ統一基準を策定する際の視点として、「標準化」が１つのポイントになると考えている。TPRM(サードパーティリスク管理)の標準化を行うことができれば、各事業者の負担が軽減され、利便性も高まるのではないか。
- 多要素認証の導入は普及しつつある一方、それを組織内で徹底できているかという点、凡事徹底が重要である。業界として重要なITシステムについては、多要素認証をデフォルト化することも一案。
- いわゆる閉域網神話について、仮に現時点で閉域網だとしても、将来的に外部のネットワークと接続した場合、セキュリティを取り巻く環境が大きく変わっているため、必要な技術的知見等が不足しており対応できないのではないかという懸念がある。このような観点から、最先端の対策に留意しつつも、基本的対策の徹底が最も重要だと考える。

重要インフラサイバーセキュリティ研究会（第２回）における主な意見

【重要インフラ統一基準の作成等にあたって】

- クラウドの利活用の推進についても検討すべきである。公表事例ベースではクラウド環境でデータが暗号化被害を受けたランサムウェア事案は確認しておらず、少ないのではないか。
- クラウド事業者がサイバー攻撃を受けた場合、非常に大きな被害が生じる可能性があるため、クラウドを利用する場合の基準について慎重に検討する必要がある。

重要インフラサイバーセキュリティ研究会（第２回）における主な意見

【その他】

- 現場の人員が不足すればするほどシステムの自動化が必要になり、サイバー攻撃のリスクも高まることを踏まえ、従来のセキュリティ対策の考えをシフトしなければならないという問題に留意する必要がある。
- 安全基準等により実施が求められているセキュリティ対策と、実際に各事業者において実施できているセキュリティ対策とは区別して調査していく必要がある。
- 閉域網は安全ではない。近年、国家を背景とする攻撃者をはじめとして、ネットワーク機器を起点としたサイバー攻撃が発生しているところ、この点について正確な情報が流通していないように思われる。事業者に対し、セキュリティ・クリアランス制度等も活用しつつ、サイバー攻撃に関する情報を正しく伝え、対策を促していくことを検討いただきたい。
- ゼロトラストが重要であるところ、閉域網において専用OSを使用していれば安全といったような安易な考えを戦略的に変えていく必要がある。このような動きは業界間で差が大きく、例えば、グローバルマーケットで勝負している半導体業界は、セキュリティの取組を強固に推進している。このような業界としての意思決定を政府がどのように政策としてドライブしていくかや、業界としてのベストプラクティス等をどのように共有・導入していくかについては、知恵を絞る必要がある。

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等にあたって】

- 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等にあたって】

- 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。