

# 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 4 日  
内閣官房国家サイバー統括室



## 【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と。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と。
- 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。

## 【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いるかどうか。
- 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。