資料５

NISC 内閣サイバーセキュリティセンター
National center of Incident readiness and Strategy for Cybersecurity

2017年度
重要インフラ事業者等
往訪調査　調査報告書

2018年3月20日

内閣官房　内閣サイバーセキュリティセンター(NISC)

往訪調査について

1.本調査の目的

- アンケート調査結果から得られた仮説の検証及び良好事例の収集
- 各分野の状況把握や技術動向等の情報収集に努め、随時施策に反映

※重要インフラの情報セキュリティ対策に係る第4次行動計画（平成29年4月18日サイバーセキュリティ戦略本部決定）

2.調査方法

システム構成図及び安全基準等の浸透状況等調査の結果を基にした現地ヒアリング（2時間程度）

3.主な調査内容

【主な調査項目】

① システム概要
② セキュリティ対策の規程・体制等
③ 平時の対応について
④ 障害発生時の対応について
⑤ 人材育成の考え方
⑥ 経営層の関与状況
⑦ その他

4.調査対象

重要インフラ事業者等8社
（医療・水道・クレジット・鉄道　うち 中小事業者等5社）

※所管省庁や関係セプターと調整の上、対象事業者を選定
※中小事業者とは、従業員数1000名未満を指す

5.調査期間

2017年1月～2017年12月

6.調査結果

往訪先事業者等から得られた検証結果と良好事例を取りまとめた。

※調査対象を公表することにより事業者に不利益が生ずる可能性があるため、個社名は非公表

調査のポイントと良好事例

今年度の主な調査のポイントと往訪調査で得られた良好事例は、以下の通り。

調査のポイント	良好事例
➢ 事業者内で、円滑にセキュリティ対策を実施するには、事業者内部の体制づくりや経営層の役割が重要ではないか。	《CSIRT》 CSIRTを設置し、社外窓口を明確化したことで、関係省庁や関係機関、セプター窓口、NISC等との情報共有が円滑になり、知りえた情報を社内に共有したことで、全社員のセキュリティ意識の向上につながったという良好事例があった。 《経営層》 経営層にシステムに熟知・精通し、セキュリティ意識をもった人材を確保することで、サイバーセキュリティ対策がなされた企業体制の構築ができていた。
➢ 制御系システムを安全かつ持続的に稼働させるためには、人材が重要な要素ではないか。	制御系システムでは、そのシステムを熟知した人材を中心に、セキュリティ対策を実施することで、安全かつ持続的なシステム稼働がなされていた。

課題と取るべき施策の例

今年度の往訪調査で得られた主な課題とNISCが取るべき施策の例は、以下の通り。

課題	NISCが取るべき施策の例
前年度は比較的大規模な事業者等との意見交換が多く、今年度は中小規模（総従業員1,000名未満）の事業者等を中心に意見交換をさせていただいた。 比較的大規模な事業者等と比較して、今年度に意見交換を実施した事業者等の多くは、比較的安価に実行が可能なセキュリティ対策でさえ実施されていない実態がうかがわれた。 以上から、対策が実施されていないのは、予算だけの問題ではなく、セキュリティマインドの低さも原因となっていると考えられる。	事業者等内で**セキュリティマインドを醸成するため**に、2018年上半期に改訂を予定している**「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針」**を普及させるべく、業界団体・関係団体等に働きかける。 また、その傘下の事業者等にNISCが実施している**分野横断的演習**に参加してもらう等、中小事業者向けの普及啓発活動を推進する。
制御系システムは、巨大なシステムになりがちであり、更新費用は巨額で、更新頻度は15年～20年に1度となる場合が多い。 そのため、継続的なメンテナンスが必要であるが、外部媒体の対策が取られていないことが多い。	常に高いセキュリティ状態が保てるように、まずは**構築時から「セキュリティ・バイ・デザイン」の考え方を取り入れておく**必要があるため、「セキュリティ・バイ・デザイン」の考え方の普及を行う。 また、メンテナンスで必要となる外部媒体のセキュリティ対策の在り方についても、普及啓発していく必要がある。

（参考）往訪調査結果　①システム概要（１/７）

（問題点）

- USBポートを物理的に使用不可にする対策は取られていない。
- 保有しているシステムのサイバーセキュリティ対策に対する関心が低い。
- クローズドな環境で利用されているPCはアップデートが行われておらず、古いバージョンで稼働している。

（良好事例）

- USBポートの使用を禁止する等の規程が作成されている。
- 上位事業者等がサイバーセキュリティに関する規程を明確に定め、グループ事業者等に展開している場合、下位事象者等も同様に順守する必要がある。そのため、下位事業者等のサイバーセキュリティ対策が充実している。
- リモート接続が可能なシステムは、常時外部に接続されておらず、必要に応じて接続される規則が徹底されている。
- 重要インフラサービスのシステムは、クローズドな環境で利用されていることが多く、外部接続しているシステムと接続しないように指示が徹底されている。
- システムへのアクセスは、特定の権限・認証システムが必要である。

（考察）

- 制御系システムは、巨大なシステムになりがちであり、更新費用は巨額で、更新頻度は15年～20年に１度となる場合が多い。それゆえ、制御系システムのサイバーセキュリティ対策は、システム構築時から将来を見据えて考慮することが望まれる。
- USBポートを特殊なシールなどで物理的にふさぐ方法は、低コストで実施可能である。このような小さな対策でも、できる対策から実践することが望まれる。

（参考）往訪調査結果　②セキュリティ対策の規程・体制等（２/７）

（問題点）
- 業務委託先からのサイバーセキュリティ対策に関する向上提案が乏しい。
- 事業者内部の報告体制等が内規や基本方針等に明記されていない。
- 制御系システムのサイバーセキュリティ対策に関する規程がない。

（良好事例）
- 所管省庁、セキュリティ関係機関、NISC等が発信するサイバーセキュリティ情報を事業者内部に展開している。
- ステークホルダ全体で、サイバーセキュリティ対策に関するインシデントの訓練を実施している。
- 年に一回以上、サイバーセキュリティ研修を実施している。
- サイバーセキュリティ担当者が、サイバーセキュリティ対策の規程の必要性を感じて、規程の策定を働きかけている。
- 職層ごと（全社員向けやシステム管理者向けなど）にサイバーセキュリティの規程が存在する。

（考察）
- 各事業者の制御系システム構築や保守ができる事業者は限られ、マンネリ化した業務委託となっている可能性がある。早急に現状を把握し、厳格な業務契約により、緊張感を持ったシステム構築や保守ができる体制に改善することが望まれる。
- サイバー攻撃の手段・種類が多様化しており、年々規程の見直しが必要になっている。規程を定期的に見直す仕組み作りを検討し、定着させることが望まれる。

（参考）往訪調査結果　③平時の対応について（３/７）

（問題点）
- 制御系システムへのサイバー攻撃に対する警戒心・危機感が希薄である。
- インシデント発生を考慮した訓練を実施していない。インシデント対応経験がある人材も少ない。
- 分野内でサイバーセキュリティ対策に関する情報交換が行われていない。

（良好事例）
- ICT-BCPを策定しており、毎年外部監査を受け、正当性を担保している。
- 外部からはVPNを利用した接続を徹底している。
- 二要素認証（ID/Password、USBキー等）を利用して、高いセキュリティレベルを維持している。
- USBメモリ等への書出しは、専用のソフトウェアを必要としている。
- 内部ネットワーク上の不正利用端末対策としてMAC認証を実施している。
- 内部ネットワークに接続している全端末にアンチウィルスソフトを導入している。
- 最近発生したサイバーインシデント事例等を題材にしたサイバー訓練を実施している。
- 重要データはクラウドではなく、オンプレミスで運用され、他サービスとは別の専用回線を使用している。
- 物理的なアクセス権の制限等、従業員の出入りを徹底管理している。

（考察）
- サイバーセキュリティ対策関係は、優先順位が低く、対策検討の段階で落されがちである。サイバーセキュリティ対策の重要性を認識していただき、重要インフラサービスを堅守することが望まれる。
- 事業者間で活発な情報交換を実施し、重要インフラ全体の防護能力を向上することが望まれる。

（参考）往訪調査結果　④障害発生時の対応について（４/７）

（問題点）
- コンティンジェンシープランが策定されていない。
- コンティンジェンシープランを策定している事業においても、コンティンジェンシープランを発動する訓練は実施されていない。

（良好事例）
- 初動対応マニュアルが存在している。
- 小規模のサイバー攻撃に対しても、関連グループ内で情報共有し、連携を深めている。
- 全従業員向けの連絡手段を構築している。
- サイバーセキュリティ対策の訓練は、全国拠点で実施し、実機にて行っている。

（考察）
- システムに関わるインシデント発生時には、システムを総括する責任者に報告し、対応することになる。普段から障害発生時を想定した訓練を行い、その連絡系統が実際に機能するのか、責任者から有効な指示が出せるのか、等を検証することが望まれる。

（参考）往訪調査結果　⑤人材育成の考え方（５/７）

（問題点）
- サイバーセキュリティ人材が不足している。

（良好事例）
- サイバーセキュリティ知識向上のため、外部研修等の機会を設けている。
- サイバーセキュリティの専門講師を招聘し、全社員のセキュリティ意識向上に役立てている。
- セキュリティポリシーに基づき、セルフチェックを実施している。
- 全従業員が複数年に一度は参加できるよう、サイバーセキュリティの訓練を実施している。
- サイバーセキュリティ人材育成に特化した取り組みとして、資格取得を奨励している。
- サイバーセキュリティ対策向けの業者に委託し、全従業員向けの訓練を実施している。
- セキュリティ関係団体が貸与しているDVD等を利用した視聴教材で人材育成を実施している。

（考察）
- 各事業者等には、サイバーセキュリティの専門人材がいないことが多く、担当者は他業務（主にシステム関係）と併任になっている体制が主立っている。今後サイバーセキュリティ対策の重要度はますます増加することが予想されるため、セキュリティ対応体制の強化を検討することが望まれる。

（参考）往訪調査結果　⑥経営層の関与状況（６/７）

（問題点）
- 一部の経営層は、サイバーセキュリティ対策を軽視している

（良好事例）
- 経営層がITに関する講演を外部で行うなど、IT全般に知見がある。
- 経営層とシステム関係者が直接意見交換できる場を設けている。
- 経営層が、サイバーセキュリティ意識の醸成が必要であると強く感じている。

（考察）
- サイバーセキュリティ対策の強化は、年々重要度が増し、意識の醸成が必要不可欠である。経営層の方々には、従業員に対して、サイバーセキュリティの重要性を気付かせる機会を提供するなど、積極的な働きかけを行っていくことが望まれる。また、サイバーセキュリティ対策の専門人材の配置や内規・基本方針等の整備等、インシデント発生時に早急に的確な対応ができる仕組みを作り上げていくことが望まれる。

（参考）往訪調査結果　⑦その他（７/７）

（問題点）
- 制御系システムのある事業者等では、内部でコンセンサスを取る部署が明確になっていない。
- CSIRTを十分に理解していない従業員が多い。
- データの開示範囲やアクセス権などの分類が出来ておらず、全てのデータを守っている状態である。

（良好事例）
- 情報系の人材と制御系の人材間の情報交換が活性化され、分野横断的演習などの訓練に部署間を跨いで参加するようになり、相互協力体制が強化されている。
- セキュリティ対策の観点から、外部委託は一切実施していない。
- CSIRTの設置により、事業者内部でのセキュリティ意識が向上した。
- 新規システム構築時には、セキュリティ審査を行う委員会に稟議を掛けてから実施している。
- リスクアセスメントを実施している。

（考察）
- Miraiのように、IoT機器を利用したマルウェアも存在する。各組織のIoTについても管理体制を強化することが望まれる。