IT連サイバーセキュリティ委員会設立について

2019年11月

事務局

日本IT団体連盟

目的

昨今の情報通信技術の発展とともに、社会・経済活動のクラウド化、モバイル化、IoT化が進み、様々な産業でのデータの収集・分析・活用が行われるようになり、国民生活のあらゆる活動がデジタルに依存している。一方で、情報セキュリティの脅威は巧妙化・複雑化し、サイバー空間上での脅威は質量ともに拡大している。従来、サイバーセキュリティ対策はネットワーク事業者を中心に行われてきたが、本格的なデジタルトランスフォーメーションが到来しており、社会経済活動確保等の観点から、さらに広い範囲での企業間協力が求められる。

そこで、現代社会の安心・安全を確保する上で、サイバーセキュリティが最も基本的な構成要素であることを多様な事業者の中で共有し、その講ずべき対策や既存の取組の改善など幅広い観点から検討を行い、必要な方策を推進することを目的として、「サイバーセキュリティ委員会」を設立する。

委員会活動内容

（１）サイバーセキュリティ対策の促進方策の検討
- 積極的に対策を進めている企業に対する評価
- 実践的なサイバーセキュリティ演習の推進

（２）サイバーセキュリティを支える制度・基盤の構築
- サイバーセキュリティ投資に関わる税制優遇措置要望等の取りまとめ

（３）サイバーセキュリティ確保に向けた国際情勢等の共有
（今後予定）

企業評価の考え方①

●IoTセキュリティ総合対策プログレスレポート2019（抜粋）
「サイバーセキュリティ対策を積極的に取り進めている企業が、市場を含む第三者から適切に評価されることが必要である。」

総務省において、「サイバーセキュリティ対策情報開示の手引き」を公表。
実施しているサイバーセキュリティ対策の開示項目の例を示すとともに、既に公開されている開示書類の事例集を掲載することで、各企業が情報開示の在り方を検討する際のガイドラインとなる。

企業評価の考え方②

同ガイドラインを参考に企業が行うサイバーセキュリティ対策の情報開示（オープンソース）から、IT連が評価する仕組みを構築。

IT連が評価することで、企業のステークホルダーに対する、信頼性の確保に向けた取組に貢献。

一方で、こうした評価が新たな攻撃を誘発しないよう十分配慮するとともに、評価の在り方を今後検討する。

企業評価の考え方③

- 各企業におけるオープンソースの情報から、サイバーセキュリティに関する記載を抜き出し、評価・公表する。

第1段階：評価・公表

評価・公表することで、各企業のサイバーセキュリティへの対策を世の中に可視化することで、同対策の全体のボトムアップを図り、また、投資家等からの信頼性の確保に貢献。

第2段階：実践

有価証券報告書やコーポレート・ガバナンス報告書等、企業で開示が義務付けられているレポートへ、CS対策が記載されるよう促し、また、当該制度につき、関係省庁に働きかけを行う。

ご参考

企業におけるサイバーセキュリティ対策の情報開示に活用されている主な開示書類例

①有価証券報告書【制度開示】

②コーポレート・ガバナンス報告書【制度開示】

③CSR報告書／サステナビリティ報告書【任意開示】

④年次報告書【任意開示】

⑤情報セキュリティ報告書【任意開示】

サイバーセキュリティ演習の考え方①

経済産業省 サイバーセキュリティ経営ガイドラインVer2.0

「3.3 インシデント発生に備えた体制構築」（抜粋）

- 「インシデント発生時の対応について、適宜実践的な演習を実施させる。」
- 対策を怠った場合のシナリオ

  「演習を実施していないと、不測の事態が起こった際に、担当者が緊急時に適切に行動することが出来ない。」

「3.2 サイバーセキュリティリスクの特定と対策の実装」（抜粋）

- (サイバーセキュリティリスク管理に関する) KPIとしては、リスク分析での指摘事項数、組織内のセキュリティ教育の受講率、インシデントの発生数等が考えられる。

サイバーセキュリティ演習の考え方②

「サイバーセキュリティ経営チェックシート 」（抜粋）

□　インシデント収束後の再発防止策の策定も含めて、定期的に対応訓練や演習を行っている

□　定期的に復旧対応訓練や演習を行っている

セキュリティ人材の育成や組織のセキュリティ的能力の向上において、知識・技能の習得に加え、実際のインシデント対応の経験も重要である。

他のセキュリティベンダーと連携をして、インシデント対応を体験できる実践演習の定期的受講が、人材教育や組織能力の向上をする上で原則となることを目的として、サイバーセキュリティ演習の普及と演習の在り方を検討する。

サイバーセキュリティ演習の考え方③

様々な企業がセキュリティやレジリエンスの机上・機能演習を提供している中、サービスの選択方法がわかりづらい状況。

演習プロバイダーのプログラムから、適したものを選別できる仕組みを構築

1. 各プロバイダーの演習プログラムを、カバーされている業種・職種、スキル項目・レベル別に分類（マッピング）
   （将来、IT連として紹介する演習プロバイダーを選別。演習を検討する企業は、自社の業界や規模、IT依存度、職種などから、一番適したプログラムを選べる仕組み構築。）

2. 経営者層向けに演習の重要性を啓発するセミナーや体験イベントなどを実施。

活動の段階的拡張

今後のサイバーセキュリティ委員会の活動については、設立から、以下の段階を踏みながら拡張していく。

サイバーセキュリティサミット（仮）

短期

（目的）
サイバー分野に係るあらゆるステークホルダーの参画により、技術に関する知見、各国法規制の動向等につき情報共有を図る。
※他の団体・企業等との共催も考えられる。

サイバーセキュリティ演習の推進

中期

（目的）
企業に具体的な経験値の蓄積等を実践演習を促すため、各プロバイダーの演習プログラムをマッピングし、また、演習の重要性を啓発するセミナーや体験イベントなどを実施。

企業評価

中長期

（目的）
企業への評価により、日本においてサイバーセキュリティが最も基本的な構成要素であることのボトムアップを図る。

体制