巧妙化し続ける
サイバー攻撃への対策の研究
－CSR モデルを活用したセキュリティ体制の構築－

アブストラクト

1. 研究の背景

近年、サイバー攻撃によるウェブサイトの改ざんや不正アクセスによる情報漏えいが後を絶たない。サイバー攻撃による被害は企業にとって大きな脅威であり、対策を強化している企業も多い。

しかし、一方のサイバー攻撃は、企業側の対策を回避するために日々巧妙化が進んでおり、それらを完全に防ぐことがもはや困難となっている。「完全に防ぐことが困難」という理由で対策を疎かにすることはできない。なぜならば、それはサイバー攻撃によるセキュリティ事故発生時の被害拡大、収束の長期化を招くことになり、最終的には顧客や取引先からの信用の喪失、競争力の低下、金銭的な損失を招くことになるからである。

つまり、現在の我々は、サイバー攻撃について「完全に防ぐことが困難であるとしても、それらに対応するための何らかの対策を講じなければならない」という非常に難しい課題に直面しているのである。

では、一体我々はこのような課題をどのように乗り越えればよいのであろうか。

そこで、当分科会ではテーマである「巧妙化し続けるサイバー攻撃」を「防御が困難で、防ぎようのないサイバー攻撃」と定義し、このようなサイバー攻撃に対する最も効果的かつ効率的な対策を検討することとした。

2. 研究のアプローチ

当分科会は巧妙化し続けるサイバー攻撃の定義をふまえ、セキュリティ事故発生を前提とした観点から、セキュリティ事故発生時の「早期収束、被害最小化」に重点を置いて研究を進めることとした。

また、このような観点からの対策としてセキュリティ事故発生に対応する専門チーム CSIRT(Computer Security Incident Response Team、シーサート)を組織内に設置することを推奨する意見が多い。しかし、当分科会では CSIRT のような新たな専門チームを設置するのではなく、既存の体制を極力活用して短期間ですばやく効果的に対応可能な対策を検討した。

3. 研究の内容、成果

巧妙化し続けるサイバー攻撃に対する最も効果的かつ効率的な対策を検討するため、以下の内容で研究を行った。

(1) 巧妙化し続けるサイバー攻撃への対策(サイバー攻撃対策製品の導入など)の現状と課題の把握

まず、巧妙化し続けるサイバー攻撃の代表例として「標的型攻撃」についてその手法と技術的な対策方法について調査を行った。

調査の結果、現在講じられている対策は有効であることがわかった。しかし、絶えず発生する新しい攻撃に対応するためには、それに追従して新たな対策を検討する必要があるが、追いついていないのが現状である。対策が導入できていないと対処に時間がかかってしまい、被害がより拡大してしまう。「早期収束、被害最小化」を実現するためには、あらかじめ意思決定のルートや担当などを決めておく必要がある。

(2) セキュリティ事故発生を前提とした対策の検討と対策案の提示

次に、(1)の検討結果をふまえ、セキュリティ事故発生を前提とした「早期収束、被害最小化」を目的とする対策が最も有効かつ効率的ではないかとの仮説に至った。そこで、セキュリティ事故発生を前提とした対策について検討した。

検討にあたっては、最初にセキュリティ事故発生時に早期収束させ、被害を最小化するために必要な機能(役割分担、報告ルートの確立など)を検討した。そして、それらを円滑に機能させるための体制のモデルとして CSR(Cyber Security Relations)モデルを定めた。

(3) 提示した対策案の有効性の検証

最後に、当分科会が提示した対策案の検証を行った。

検証にあたっては、当分科会メンバーに折よくセキュリティ体制の強化推進を行っていた企業があったため、当分科会の対策案として提示した CSR モデルを実際に活用してもらい、その有効性(提言によって改善・強化された点)の検証と改善点(改善・強化できなかった点)の洗い出しを行った。

4. 研究の成果

当分科会が提示した CSR モデルの活用により、セキュリティ事故発生時の役割分担や責任の所在、対応の手順が明確化され、迅速な対応が可能となったことで、早期収束、被害の最小化に効果があることを確認することができた。

また、副次的な効果として、CSR モデルに基づく対応体制構築(とくに訓練の実施による体制や手順の見直し)がセキュリティ事故対応の PDCA サイクルの確立にも貢献することがわかった。PDCA サイクルの対応の確立は、構築した対応体制をサイバー攻撃の巧妙化に合わせて変化させていくために欠かすことのできないものである。

5. 提言

当分科会では、巧妙化し続けるサイバー攻撃に対する有効かつ効率的な対策として、以下の 2 つを提言として結論付けた。

(1) 当分科会が提示した CSR モデルを参考に、セキュリティ事故発生時の対応体制を構築すること。

CSR モデルは CSR-C(Cyber Security Relations-Controller)という部署間の連携を調整することを目的とした担当者を中心に、セキュリティリスクをコントロールできる人材を育成し、組織として体制を構築すること。

(2) 体制を構築したうえで、定期的な訓練実施を通じて体制・対応の手順について見直す PDCA サイクルを確立すること。

CSR モデルに基づく体制を設置し、巧妙化し続けるサイバー攻撃により有効に対処するためには、定期的な訓練や体制の見直しを行う PDCA サイクルを構築し運用することが重要となる。

これらの提言を活用することで、図 1 に示すような CSR モデルを活用し、図 2 の巧妙化し続けるサイバー攻撃への対応サイクルを確立することが、セキュリティ事故発生時の早期収束と被害最小化および予防までを視野に入れた確実な対策となる。

図 1 CSR モデルの活用

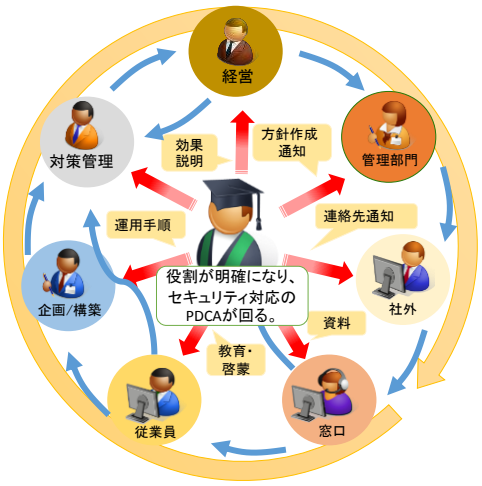

図 2 対応サイクル