情報セキュリティ対策の効果測定方法

ータテ・ヨコサイクルが生み出すベストプラクティスー

アブストラクト

1. 情報セキュリティ対策の現状

IT 技術の進化と発展の速度はめざましく、同時に情報セキュリティの脅威となる様々な要素は従来の愉快犯的なものから組織化、ビジネス化され、その場限りの付け焼き刃的な対策を行っても、対策し損ねた箇所を新たに攻撃されるという様相を見せている。企業はステークホルダーから強度な情報管理を求められており、増大する情報セキュリティコストと、必要と思われる情報セキュリティ水準の維持・確保との板挟みにより苦心している。

しかし、何をどこまで実施すれば情報セキュリティは担保されるのか、施している情報セキュリティ対策が適正であり、本当に情報セキュリティ事件・事故を抑止しているのか判断できる基準および測定方法は存在しない。一般的な情報セキュリティ規格である ISO/IEC27001(以下「ISMS」という)においても具体的な基準や有効性の測定方法は明示されていないのが現状である。

当論文は、この情報セキュリティ対策分野で適用可能な効果測定手法につき提案を行うものである。

2. 当分科会で取り組む課題

当分科会では、各企業での情報セキュリティ対策実施状況と現状の洗い出し、情報セキュリティ対策の測定基準を記した参考文献の調査を実施した。その結果、当分科会で扱う課題を以下の 3 つに絞った。

①ISMS に代表されるセキュリティマネジメントシステムに問題はないのか。効果を出すためにはどんなことをするべきなのか。

②情報セキュリティ事件・事故はなぜ発生し続けるのか。

③定量的かつ客観的な情報セキュリティ対策指標を作成する必要があるのではないか。

3. 課題解決へのアプローチ

「2」で挙げた課題を解決するために、3 つの切り口（手法）で課題解決のためのアプローチを行った。

①「セキュリティ対策指標」の具体化とセキュリティ強度レベルの見直し

②実際の情報セキュリティ事件・事故の根本分析

③セキュリティマネジメントシステムが円滑に機能しない原因の分析

3 つの切り口から導き出された結果（原因に対する対応策）をもとに、管理策の「網羅性」、セキュリティ対策の強度レベルの「十分性」についてフォーカスをあてた当分科会オリジナルの「セキュリティ対策指標」を策定することとした。そして「セキュリティ対策指標」を組み込んだ「セキュリティ対策シート」にまとめた。

作成した「セキュリティ対策シート」を実際の企業に適用を行い、「セキュリティ対策指標」として有効であるか、「2」で挙げた課題について解決できたのかを検証することとした。

4. 「セキュリティ対策シート」の作成

4.1 「セキュリティ対策指標」の具体化とセキュリティ強度レベルの見直し

「セキュリティ対策指標」について、一般的に高度なセキュリティ要件が求められる金融業界での活用を想定し、各詳細管理策のセキュリティ強度を高水準とした。また、定性的ではなく定量的に測定できるように各管理策に具体性を持たせた。

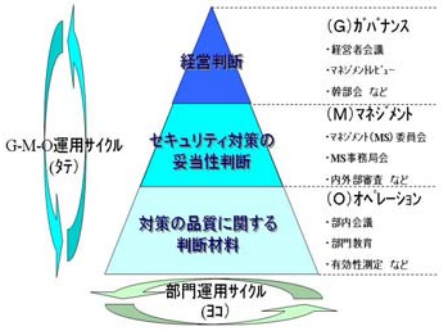
4.2 実際の情報セキュリティ事件・事故の根本分析

近年発生した情報セキュリティ事件・事故について FTA（Fault Tree Analysis）分析方法を使用して、根本原因を特定した。各根本原因についてそれぞれ対応策を検討し、その対応策が「セキュリティ対策シート」で網羅されているか比較検証した。その結果、不足している管理策として「情報セキュリティに関する事業計画」が導き出された。また、「セキュリティ対策指標」についても複数の管理策に対して「十分性」が不足していたので、見直しおよび指標の追加を行った。

4.3 セキュリティマネジメントシステムが円滑に機能しない原因の分析

ISMS 等セキュリティマネジメントシステムを導入している企業は多数存在するが、それでもセキュリティ事件・事故は発生する。セキュリティマネジメントシステムが円滑に機能していない原因について連関図法を使用して分析した。企業活動をフレームワークに仕立て「ガバナンス」「マネジメント」「オペレーション」の側面から分析を実施したところ、「ガバナンス」「マネジメント」「オペレーション」の三者（以下、頭文字をとって「GMO」という）の一貫した情報セキュリティに対する共通認識、共通理解が欠如していることが判明し、ISO27002 における 133 の詳細管理策への追加項目とそれに対する対策指標を設定した。

図表１　PDCA サイクル相関図



4.4 分析のまとめ

「4.2」、「4.3」の分析結果を集約し、情報セキュリティマネジメントシステムを円滑に機能させ、情報セキュリティ事件・事故を発生させないために何が必要であるのかを検討した結果、以下のキーワードが導き出された。

・「GMO 三者の、企業をフレームワークとした PDCA サイクルの機能」つまり「タテの PDCA サイクルの円滑な機能」の欠如

「タテの PDCA サイクル」が企業に意識されていなかったことが、セキュリティマネジメントシステムの機能していなかった原因である。そこで、「セキュリティ対策シート」にも「タテの PDCA サイクル」を円滑に機能させるために、対応するセキュリティ対策の何に該当するか分類できるセキュリティ管理アイテム欄を追加した。

5. 企業の適用および検証

当分科会のメンバー企業（金融機関、ISMS 認証済み）に「セキュリティ対策シート」を適用し、検証を行った。その結果、現在実施されている指標測定よりも具体的かつ定量的な有効な指標であり、また、今まで把握できなかったセキュリティ対策の実態にまで踏み込むことができた、との評価を得た。同時に「セキュリティ対策シート」のレビューも行い、実適用における留意点としてまとめた。当分科会で作成した指標はどの企業でも使用できる汎用的な指標であるため、使用する際は各企業の現状に合わせてどの部分を使用するのかを検討し、語句の読み替え等の作業（カスタマイズ）の必要がある場合も想定される。

6. まとめ

当分科会で作成した「セキュリティ対策シート」は企業のセキュリティの実態に対して測定できる有効な指標である。ただし、冒頭でも述べたとおり、セキュリティの進化速度は速く、それと同時に新たなる脅威も発生し続けているため、この「セキュリティ対策シート」は有効な指標であるが、企業の PDCA サイクルに落とし込み、ブラッシュアップさせていく必要がある。

また、昨今情報セキュリティガバナンスが注目されているが、この「セキュリティ対策シート」は企業におけるセキュリティ対策の根幹となるものである。「セキュリティ対策シート」の適用結果をもとに、「ガバナンス」やステークホルダーに説明できる情報セキュリティレポートの作成が可能である。