Vol.2010-DPS-142 No.51
Vol.2010-CSEC-48 No.51
2010/3/5

情報セキュリティ施策における有効性評価についての一考察

鈴木宏幸† 内田勝也†

近年、情報セキュリティ問題は過去に例を見ない程クローズアップされ、情報セキュリティに関するインシデントの発生、新たな脅威の警鐘といったものが我々の社会、組織、日常生活へ深く入り込んで来る様になって来た。
それとともに、情報セキュリティに対する技術的な施策も進められて来ている。また、技術的なセキュリティ対策だけではなく、ＩＳＭＳに代表されるマネジメントシステムの導入、情報セキュリティ教育も進められている。しかし、その振り返り、評価というものが進め方を含め重要視されない、行われていないため、施策の実施自体が最終目的化していないだろうか。
本論文では情報セキュリティにおける施策に対する評価に焦点を当て、「比較可能で再現可能な結果を生み出し」、情報資産のセキュリティを担保するために最適な評価を行なうための考察を行なって行く。

A study of measurements of information security policies and controls

Hiroyuki Suzuki† and Katsuya Uchida†

In recent years, information security issues is unprecedented close-up enough in the past, information security incidents occur, and we are warning of new threats to our society, organizations, came in good shape come to life deeply penetrating Ta.
And it also comes ongoing technical measures for information security. Also, not just technical security measures, ISMS management systems that are represented, has been promoting information security education. But looking back it is not something that is important for the proceedings, including evaluation, because it is not done, and what does not in itself the ultimate goal of implementation of the measures.
This paper focuses on the evaluation of measures in information security, "produced comparable and reproducible results," doing a study visit in order to make the best assessment to ensure the security of information assets.

1. はじめに

情報セキュリティに対する脅威に対応する様に情報セキュリティに対する施策が進められ、情報セキュリティに対する技術的対策、マネジメントシステムの導入、教育の実施が進められている。また、プライバシーマーク、ISMS に代表される情報セキュリティ第三者認証では、活動の継続、強化活動に対して一定期間毎に更新の審査があり、情報セキュリティの諸活動における PDCA サイクルが機能しているかが確認される。この PDCA サイクルを回す事が組織の強化に繋がる事ではあるがこれが確実に行われているのであろうか､情報セキュリティ施策の計画と実行を繰り返すのみで、CHECK（監視・レビュー）、ACT（維持・改善）が抜け落ちた PDPD サイクルに陥ってはいないだろうか。目先の情報セキュリティに対して対策を実行し、また次の対策を計画していく事の繰り返しのみに終始していたのでは、情報セキュリティ対策の成熟度は上がらず、全体としての情報セキュリティリスクは減らず、組織の資源を浪費していく事にしかならない。

情報セキュリティに対する施策については、評価をまでを実施範囲とし、有効性を測るべきであると考えられる。

２．情報セキュリティの評価手法の定義付け

情報セキュリティの評価手法を①準拠性評価と②有効性・妥当性評価の２つに分類し、両者の特徴について考察した。

①準拠性評価

準拠性評価の定義

・予め定義された組織活動があり、測定はその定義にしたがって準拠していることを計測する。
・測定は、静的に近い。
・測定は、比較的容易である。

ある時点の状況を、予め定められた評価基準に従い計測し、基準に適合している事を評価する。予め定義された組織活動があるため、チェックシートなどの作成、流用が容易である事が考えられる。

評価実施はその組織の構成員でなくても規格、要求事項を把握している外部の人間

† 情報セキュリティ大学院大学
Institute of Information Security

Vol.2010-DPS-142 No.51
Vol.2010-CSEC-48 No.51
2010/3/5

であれば評価を行う事ができる。
反面、評価を定められた定義に準拠していることの確認を目的に行うため、評価結果は組織の一側面のみを表す静的、表面的なものになりやすい。情報セキュリティ分野においてまず実施されるのはこの準拠性評価である。

②有効性・妥当性評価
有効性・妥当性評価の定義
（以下有効性評価とする）
・評価対象の有効性、妥当性を測定する。
・その為には評価対象の精査が必要である。
・測定は動的であり、多岐に渡る。
本評価を行うための共通的な定義、チェックシート等は存在せず、組織に合わせて評価方法･評価基準を定義し実際に測定を行い評価する評価手法である。組織の形態、実施しているセキュリティ施策が組織ごとに異なるため、他の組織で使用している評価指標をそのまま使用することは難しく、出された結果も不正確なものとなる。
具体的な測定方法、評価方法は定められていない、組織毎に管理策の測定方法も異なるため、規格でも一律に決める事ができず、個々の組織に任せられている。このため測定・評価は“準拠性評価”に比べて、桁違いに難しいものとなる。
両者の適用場面については、情報セキュリティ導入の段階では一般的なセキュリティ基準に対して、現実の対策を確認し、対応していない部分についてギャップを埋めていくアプローチを取ることが主であり、また、継続して施策が行われている段階ではないため準拠性評価が行われる事が多い。
一方、ある程度情報セキュリティ施策が定着した段階において有効性・妥当性評価は行なわれると想定される。セキュリティ施策がある程度浸透し、当面のリスクに対応した上で、予防を含んだセキュリティ施策を選択肢の中から選べる程度に組織が成熟した時点で、その組織に合わせた評価基準、測定方法を導き出す要求が出てくると思われる。

３．情報セキュリティの評価指標

準拠性評価の評価指標としては、既存のものが使用可能であり、P マーク、ISMS 等の第三者認証の規格、IPA が発行している情報セキュリティベンチマーク[1]等既存の評価指標を用いる事が一般的である。
一方、有効性・妥当性評価においては評価指標として定まったものは定義されておらず、組織毎に評価方法、評価基準を設定しなければならない。
考え方の一つとして JIS Q 27001 の解説部分には以下の記述がある。「JIS Q 27001 の附属書 A[2] が掲げる管理目的の多くはその達成の程度を直接に監視・観察・計測できるような内容・表現によっては用意されていない。有効性測定についての要求事項への対処は，管理目的の達成度についての“代理変数”を想定する。」とある、この“代理変数”が評価指標に当たると考えられる。
評価指標となるものについて要件についてここに列挙する。
①測定可能な大きさまで分割されているもの。
②測定可能な単位（回数、割合等）を持つもの。
③プロセスの過程で測定できるもの。
④有効性を判断する基礎となるもの。
⑤属人性を排除し、誰もが測定できるもの。
⑥測定結果が再現可能なもの。

４．有効性の捉え方

有効性とは一般に「計画した結果が達成される程度」と定義される。情報セキュリティにおいてもそれは同様であり、図１に示される手順で測ることができると考えられる。

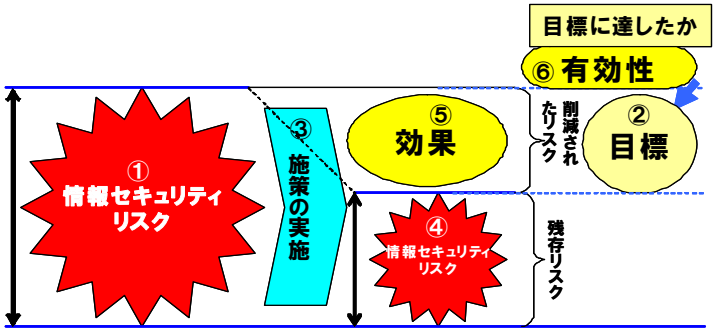

図１　有効性の捉え方

①リスクアセスメントにて情報セキュリティリスクの大きさを測定。
②情報セキュリティリスクの削減度合いを目標として設定。
③情報セキュリティリスクに対して施策の決定、実施。
④施策を実施した後の情報セキュリティ残存リスクの測定。
⑤削減されたリスクの大きさを効果とする。
⑥目標と効果を比較し、施策の有効性を判断する。

Vol.2010-DPS-142 No.51
Vol.2010-CSEC-48 No.51
2010/3/5

５．リスクアセスメント

情報セキュリティの全ての施策は現状のリスク確認から始められる。リスクアセスメントを実施するに当って、組織に合ったリスクアセスメントの手法を選択する事が重要である。

リスクアセスメントは大別し以下の二種類のアプローチ方法があり、目的に応じリスクアセスメント手法を使い分けるべきである。

①マネイジィアルアプローチ
経営方針や戦略上の観点からセキュリティ要求事項を明確にしてリスクを把握する経営・管理的アプローチ。

②テクニカルアプローチ
技術要因をベースにして、予測される現象や原因からリスクを把握するアプローチ。

表１に主要なリスクアセスメント手法とアプローチ方法、見込める効果を取りまとめた。

表１　主要なリスクアセスメント手法と見込める効果

リスク分析手法	アプローチ手法	見込める効果
GMITS 詳細分析方式	マネイジィアル アプローチ	・経営面のリスク評価に効果的 ・資産のリスク評価に効果的
DISC　PD3000 方式	マネイジィアル アプローチ	・経営面のリスク評価に効果的 ・資産のリスク評価に効果的
JRAM による リスクアセスメント 方式	マネイジィアル アプローチ	・経営面のリスク評価に効果的
FTA によるリスクア セスメント方式	テクニカルアプローチ	・特定分野に効果的
ALE によるリスク アセスメント方式	テクニカルアプローチ	・経営面のリスク評価に効果的 ・資産のリスク評価に効果的
インシデント発生時 の被害額積み上げ 方式[3]	テクニカルアプローチ	・経営面のリスク評価に効果的 ・資産のリスク評価に効果的

６．組織の成熟度と IT フレームワーク

情報セキュリティの施策を実施するに当っても、組織の成熟度は重要なファクターとなると考えられる。同じ施策を行っても組織の成熟度によって効果、残存リスクは大きく変わってくる。一例を挙げると、「PC のハードディスクを暗号化する」という施策を実施した場合、組織の成熟度が低い場合は、施策が浸透せず、未対応の PC が残存する、暗号化パスワードが PC に貼られているといったリスクが残存する。成熟度が高くなるにつれ施策が徹底して行き、未対応の PC が残存する場合、台数と理由が把握される様になる。さらに成熟度が高まると情報の区分付けが徹底され、重要情報は PC に格納しない様になってくる。組織の成熟度が進むにつれ残存リスクは減り施策は有効性を増していくと考えられる。

この組織の情報セキュリティに関する成熟度を判断するための基準が必要である。組織の成熟度を測る指標を、ゼロベースで定義を行う事なく、IT フレームワークでの考え方を流用可能と考えた。

IT フレームワークは大別すると以下の３つのタイプに分類される。

①方法論：各プロセスを体系化したフレームワークを示してそこで行なうべき事項を示したもの、EA[4]や IT コーディネータガイドライン[5]がこれに当たる。

②チェックリスト：ベストプラクティスをベースにあるべき姿を示し、現在の実現度をチェックし、自組織の成熟度と将来実現目標を考えるもの。代表的なものとして COBIT[6]、CMMI[7]等が挙げられる。

③知識体系：従事者が持つべき知識を網羅的に体系化したもの。PMBOK[8]や ITSS[9]がこれに当たる。この中では②のチェックリスト形式で用いている成熟度が流用可能と想定している。

チェックリストを用いるという事は例えて言うと『実力テスト』を受ける様なものである。その時点の実力を知り、どこが問題に強いのか弱いのかといった傾向を知る事ができる。

一方第三者認証を受けるという事は、『資格試験』に例えられる。定められた条件を満たす事により資格が取れ、相当の事がない限り資格が取り消させる事はない。

７．組織の成熟度の段階表現

情報セキュリティの施策を実施するに当っても、組織の成熟度は重要なファクターとなることを前述した。同じ施策を行っても組織の成熟度によって、効果、残存リスクは大きく変わってくる。成熟度と残存リスクの関係を図２にて表す。

本図では横軸に CMMI で使用されている組織の成熟度段階とそれに対応すると考えた組織の能力段階を配置し、縦軸にリスク値及び管理策の洗練度合いを配置した。管理策の徹底度合いとせず管理策の洗練度合いとしたのは同じ施策を実施しても実施に

Vol.2010-DPS-142 No.51
Vol.2010-CSEC-48 No.51
2010/3/5

対する難易度が変化する事が考えられるためである。

図の左上から右下への点線で表している矢印は組織の保有するリスク値であり、組織の成熟度が上がるにつれ下降する。この矢印線上の楕円は組織の成熟度毎の組織の代表的と思われる対応を配置した。

図の左下より右上への実線で表している矢印は組織の管理策の状況である。組織の成熟度が上がるにつれ上昇する。この矢印上の楕円は管理策を実施する上での基本となる活動を配置した。

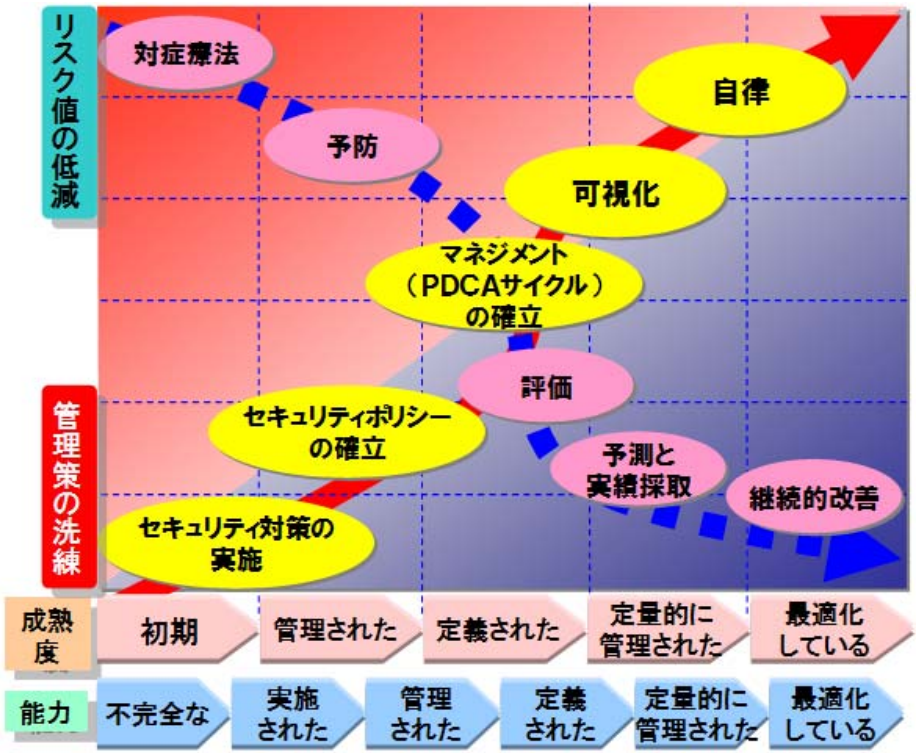

図２組織の成熟度と管理策・リスクの関係

組織の成熟度の各段階の情報セキュリティリスクと施策の状態を CMMI の成熟度レベルを参考に定義したのが表２である。

表２組織の成熟度段階と情報セキュリティ状況

レベル	組織の段階	説　　明
1	初期段階	セキュリティ施策は具現化しているリスクに対症療法的に対応しており、一貫したリスク低減策は確立されていない。
2	管理された段階	リスク・対策が管理され、セキュリティポリシーが確立する。対策は具現化していないリスクに対しても予防として実施される。
3	定義された段階	マネジメントサイクルが定義され、継続的改善のベースとなる、この段階でリスク値、セキュリティ対策の効果の評価の考え方が取り入れられる。
4	定量的に管理された段階	リスク分析、セキュリティ対策は予測される値を算出し、実績を採取しながら行なわれる。測定値は比較・検証可能な形で管理される。
5	最適化された段階	組織の中で PDCA サイクルが定着し、短いサイクルで回り、継続的なプロセス改善が行なわれている。リスク低減の活動は自律して動き、リスクに対しては対策がただちに対策される。

８．組織の情報セキュリティ成熟度の把握

情報セキュリティ施策の有効性評価を実施する前提として、その組織がどういった状態にあるか、把握する必要がある。有効性評価を行なうためにはその組織がある段階まで達し、実績を測定できるようになっていない場合では、評価基準がなく評価が困難である。

評価を行う前提として、組織の状態を基準に基づきモニタリングして、評価結果に対するコンセンサスを行ない、評価する側とされる側で現状に対する認識を合わせておく事が評価の前提と考えた。

組織の情報セキュリティの成熟度を測ることのできるツールを作成し、評価を実施した。

本ツールは ISMS（JIS Q27001)の付属書 A の管理目的及び管理策 133 項目の管理策に対して、適用・非適用の選択と表１のレベルを１～５の間で選択すると、11 のドメイン毎に平均レベルを算出し、評価レポートとしてグラフを出力し、有効性の実施可能性の判断材料とするものである。このツールをある組織（構成員約 100 名、ISMS 認

Vol.2010-DPS-142 No.51
Vol.2010-CSEC-48 No.51
2010/3/5

証取得済み）で実践を試みた。その結果グラフを図３に示す。

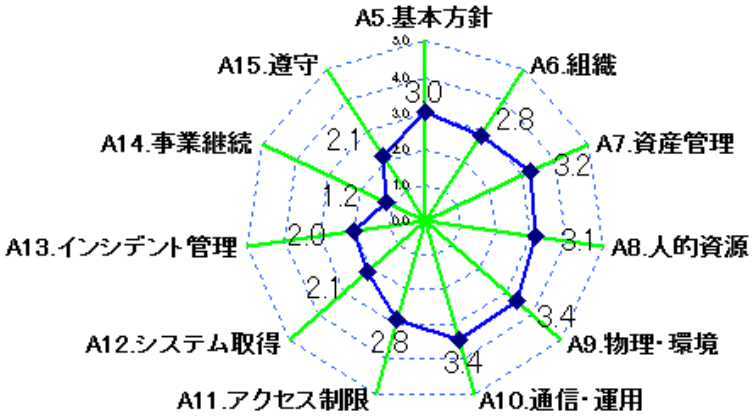

図３　組織の成熟度把握グラフ

実践の結果以下の事が判明した。

①評点付けは管理策毎に行ない、結果は管理ドメイン毎に出力されるため、ドメイン中の管理策に１つでも低い評点のものがあれば、ドメイン全体の点数が下がるため、ドメイン毎の評点＝ドメイン毎のレベルとはならない。

②ドメインによりレベルの判断に難易度がある。A9、A10、A11 等技術的対策の部分の判断はやり易いが、A5、A13、A15 などマネジメントの部分の判断は難しい。

③入力自体の手間はそれ程かからない。入力シートを見ながら複数人でレベル判定を行うと、施策の振り返りになり、入力結果が視覚化されるので組織内のコンセンサスを得易い結果となった。

９．有効性評価のアプローチ

有効性評価を行なうに当っては以下の２通りの方法が考えられる。基本的にはリスクアセスメントのアプローチ方法であるが、有効性の評価に適用できると考えた。

①ベースラインアプローチ

組織の現状のリスクと望ましいリスクとの比較を行なう。管理ドメインの成熟度レベルが低い部分において実施を行なう。望ましいリスクとのギャップを埋めるため、どのような施策を行なえば良いかを評価していく。既存施策の実施については目的を達成した/未達成というゼロイチでの評価となり、準拠性評価に近いものとなる。本アプローチはリスク対応計画のベースとして活用する事を考えている。

②詳細アプローチ

成熟度レベルである程度高いレベルと評価した管理ドメイン、または大きなリスクが存在し、詳細な評価が必要と思われるドメインの中の情報セキュリティ施策に関しては、施策の実施前のリスク、残存リスクの評価とともに、施策の適用度合いも評価の指標とする事を考慮する。施策の適用度合いについてはメトリクス（尺度）の利用を行なう事が考えられる。メトリクスについては NIST(米国商務省標準技術局)から SP800-55（情報技術システムのためのセキュリティメトリクスガイド）[10]が発行されておりかなり、技術的対策の部分において詳細な達成指標が定義されている。これを ISMS（JISQ 27001)の付属書 A の管理目的及び管理策と突きあわせて使用する事とした。

10. 有効性評価テンプレートの作成

実際に有効性評価の詳細アプローチを行なうツールとしてのテンプレート作成を行なった。テンプレートを用いる事により同一の評価基準の下でリスク値、施策の実行度、残存リスクを測定、評価できると考えたためである。

テンプレートの項目は大きく 4 つに分けて考えた。分類、目標指標等の基本項目、施策の実施前に測定する項目、施策の実施後に測定する項目、入力された値から自動算出を行なう項目となる。

評価を行なうに当っては、管理策が対象とするセキュリティリスクのリスク値を管理策の実施前に明確にしておく。リスク値は選択するリスクアセスメント手法により金額の場合、リスクポイントになる場合等があるが、

数値と単位を別に登録する事によっていずれも登録可能とした。

管理策を実施するに当ってはその管理策に該当するメトリクスの目的、目標値、計算式を考慮する。評価に当っては、メトリクスにて推奨される実施率と実際の実施率とを比較し、管理策自体の適用度合いのギャップの分析を行なう。次にリスク値削減に対して管理策がどの程度効果的であったかの評価を行なう。

有効性評価テンプレートを組織に適用する場合の前提条件、課題を以下の様に考えた。

①有効性評価実施のコンセンサス
②リスクの算定手法の決定
③測定に必要なプロセスの確認
④施策の影響項目の数値化

Vol.2010-DPS-142 No.51
Vol.2010-CSEC-48 No.51
2010/3/5

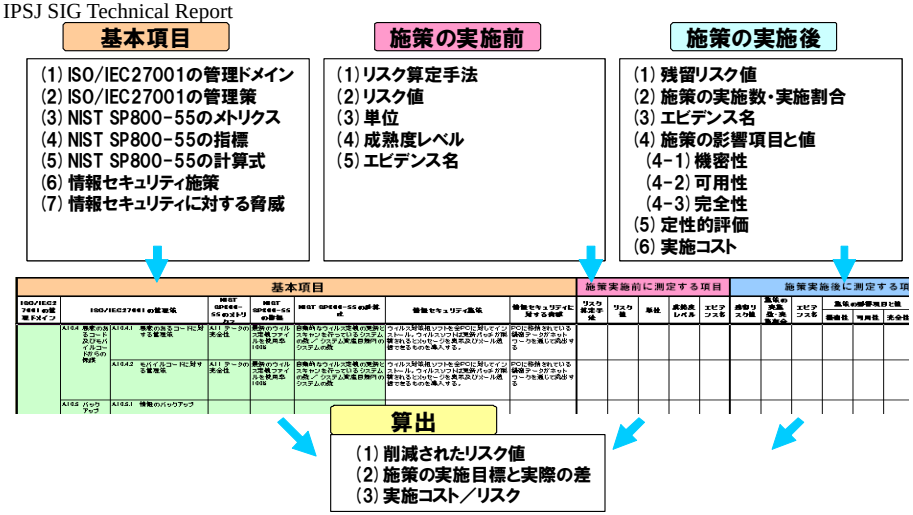

図４有効性評価テンプレートの主要項目

11. 有効性評価テンプレートの組織への適用シミュレーション

有効性評価テンプレートを架空の組織に対し適用し、情報セキュリティ施策の評価シュミレーションを実施した。その概要は以下の通り。

①評価対象の施策
・ウィルス対策ソフトの導入
・PC のハードディスクの暗号化
・入出力デバイスの接続制御
・外部からネットワーク接続する利用者の認証
・情報交換に関する合意
・情報のバックアップ
・物理的セキュリティ境界

②リスクアセスメント手法
・想定被害額の積み上げ方式とし、リスク値はインシデント一回当りの想定被害額とした。

個々の施策に対し、施策の達成度、リスクの削減度合いの観点から評価を行なうとともに、このシミュレーションにて、施策実施結果から特徴的な事項を洗い出した。
・組織内で関心の高い情報セキュリティ施策は、実施率が高い。
・ルールが定着している情報セキュリティ施策に対して、新たなツールを適用する場合実施率は高まる。
・逆にツールだけ導入して、ルールが曖昧な場合は施策は定着しにくい。
・新しいツールを導入する場合、フィージビリティスタディは充分行う事、もし、ツール導入による弊害が大きい場合、情報セキュリティ活動全体が停滞する。
・ルールを作り管理強化を行う場合は、何をもって実施率とするかを良く検討する必要がある。これを誤ると実施率は上がってもリスクは減らない。
・目に見えるハードウェア、ソフトウェアの導入は組織内のセキュリティの関心を引くため、目玉として用いる。

実施率の観点からでの特徴を以下の５つに分類した。実施率の高い施策の傾向順に以下に記載する
・一つの施策を実施する事により、従来からの方法が行えなくなり全てが新しい方法に移行する施策
・組織内で脅威が広く認識されているものに対しての対策
・予めルールが決まっているものに対しての強化策
・施策を実施する事により可用性を損ねる施策
・実施率の指標が曖昧な施策
これらの特徴を踏まえた施策実施計画を立てないと達成率が上がらない事が確認できた。

リスク削減面での評価としては、被害額の積み上げ方式でリスク算定を行ない、リスク値を金額で示すことによって、リスク値以外の要素と直接比較が可能となった事が大きい。
リスク値を求めるために各種数値を収集するが、この作業がリスクの費用構造を理解する事となった。また、以外な事に残留リスクの大小は、もとのリスクの大小に起因しないという結果が今回のシュミレーションでは
だされた。

組織の成熟度については原則を”レベル 3”としてマネジメントサイクルが確立された組織での適用とし、施策毎に組織の情報セキュリティ成熟度レベルを見直し、施策によって成熟度レベルを変更した。その上で組織の成熟度レベルの相違に応じてリスク値、インシデントの発生確率に乗数を設定しリスク算定を行なった。成熟度レベルによってリスク値は当然変化するが、その変化は成熟度レベルによる乗数を使用する前のリスク値が覆る程の変化では無かった。

成熟度毎の乗数については一定の基準が作れず、その妥当性については組織内で決定していくしかないと考えられる。

Vol.2010-DPS-142 No.51
Vol.2010-CSEC-48 No.51
2010/3/5

12. 問題点・課題

実際に有効性評価のシミュレーションを実施し出てきた問題点は以下の通り。

①時系列のリスクの推移の取り込み
シミュレーションでは情報セキュリティ施策の実施前、実施完了時点の数値を計算しているのみで時系列で推移して行くリスクを取り込むにはケーススタディが必要であると考えている。
②セキュリティ施策の対象
施策の側からのシミュレーションを行うため、施策対象の情報資産が異なる。同一の情報資産に対する異なる施策のシミュレーションは今回未実施。
③組織の成熟度レベルの判定
あくまでも「自己判定」であり、組織がそのレベルに達しているという基準、保証を行うものではない。
また、今後の課題としては、有効性評価テンプレートにに対してシミュレーションで発生した問題点の反映、及び、ツールを含めた有効性評価の拡大が考えられる。

13. まとめ

本論文では情報セキュリティ施策に対する評価方法を調査し、ツールを作成しシミュレートを実施してきたが、有効性評価を行うに当たっては数々の前提条件を満たさねばならない。情報セキュリティ活動を行って行く上で有効性評価、特に数値による評価は「比較可能、再現可能」な結果を生み出す強い原動力となることを実感した。

参考文献

1 独立行政法人　情報処理推進機構
情報セキュリティ対策ベンチマーク
(http://www.ipa.go.jp/security/benchmark/) 2009 年 9 月 14 日アクセス
2 日本規格協会
「情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－要求事項
JISQ27001：2006」、2006 年
3 高津　岳志(情報セキュリティ大学院大学)
情報セキュリティインシデントにおける定量的費用分析に関する一考察 2006 年
4 EA 入門（EA 概要）－EA ポータル（経済産業省）
(http://www.meti.go.jp/policy/it_policy/ea/nyumon/meaning/index.html)
2009 年 12 月 25 日アクセス
5 IT コーディネーターとは（IT コーディネーター協会）
(http://www.itc.or.jp/about/index.html) 2009 年 12 月 25 日アクセス
6 情報システムコントロール協会
COBIT4.1 日本語訳　2007 年
7 独立行政法人情報処理推進機構
開発のための CMMI®1.2 版　2007 年
8 広兼 修
プロジェクトマネジメント標準 PMBOK 入門 2005 年
9 独立行政法人情報処理推進機構
IT スキル標準センター
(http://www.ipa.go.jp/jinzai/itss/)2009 年 12 月 19 日アクセス
10 独立行政法人情報処理推進機構
「情報技術システムのためのセキュリティメトリクスガイド（NIST SP 800-55)」、2003 年