セキュリティ対策技術はどこまで導入すればいいのか？

葛西 重雄
株式会社トリエス 代表取締役
情報処理推進機構（IPA）CIO 補佐官

概要：高額な情報セキュリティ対策技術を導入しても、情報は十分に守られているのか不安が残る。IPA でも実践している、業務への影響とコストのバランスを意識した、リスクアセスメントに基づく情報セキュリティ対策の計画立案方法を紹介する。

キーワード：情報セキュリティ、ISMS、ISO/IEC27005、リスクアセスメント

1. セキュリティ対策の空白

私は、デザイナー（グラフィックスや社会問題解決のためのデザイン）から監査法人系のコンサルティングファーム（情報システム部門の責任者とコンサルタントを経験）に入り、経済産業省の CIO 補佐官（電子政府政策立案と導入・評価）を経て、現在 IPA[1] の CIO 補佐官の任に就いている。一見、脈絡のない経歴に見えるかもしれないが、問題解決の企画から導入・評価までを経験しており、これが昨今のセキュリティ脅威への対策に非常に役立っている。

情報システム分野にはそれごとに専門家がいる。情報システムを利用する業務の専門家であるコンサルタントや監査法人、企業のシステム部門や運用会社、SI・ベンダーやメーカー、それぞれの立場でセキュリティを論ずる専門家はいても、一気通貫でセキュリティソリューションを検討できる専門家は少ない。手前味噌で恐縮だが、これまでの経歴を生かし、セキュリティ対策について企画から導入までを検討した経験から、本稿をまとめていきたい。

IPA にも、セキュリティ対策はどこまでやるべきかという質問が多く寄せられる。これは、セキュリティ分野とシステム開発分野が分断されている（図 1）ことも一因となっている。

情報セキュリティについて検討するには、サイバーセキュリティ基本法[2]や個人情報保護法[3]などの法律や、業種により法律や規則類、企業ごとのマニュアル、システムの運用手順等があり、これらに準ずる、また参照する必要がある。一方でシステム開発では、利便性向上や効率化といった業務改善の視点や導入する機器の仕様に従って要件定義、設計、開発が行われる。

情報セキュリティに関する法律や規則がありながら、それらを確認しないままに、システム構築が行われることが往々にしてある。また、一連のプロセスをトータルにサポートできる専門性を持った人材が極めて少ないという課題が大きく横たわる。コンサルタントは業務改善の支援まで、ソフトウェア開発業者は顧客の業務をシステムに落とし込み、ベンダーは実装する機能に基づき必要なスペックの機器を供給するものの、セキュリティ対策について相談すると、関連の機器やソリューションの紹介はできても、どういう脅威から守れるかという質問には明確に答えられていないことが多い。

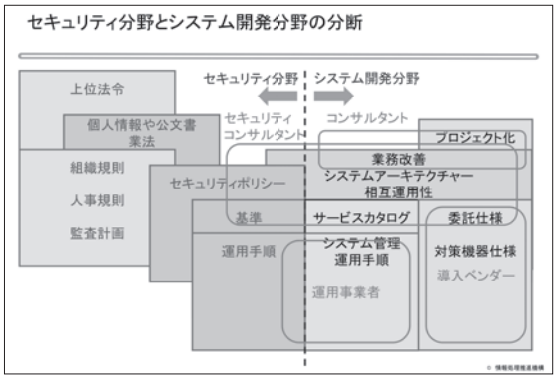

図 1　セキュリティ分野とシステム開発分野の分断

また、システムの運用においてどの程度のサービスレベルを維持すればよいかが十分議論されないまま、カットオーバーを迎えることも多々ある。運用フェーズになりやっとセ

1　独立行政法人情報処理推進機構
http://www.ipa.go.jp/
2　http://www.shugiin.go.jp/internet/itdb_gian.nsf/html/gian/honbun/houan/g18601035.htm
3　http://law.e-gov.go.jp/htmldata/H15/H15HO057.html

キュリティ面を含めて安定的な稼働の維持をしようにも、構築されたシステム環境に対して打てる手だては限られてしまうことも少なからずあり、最良の対応を取ることができない。

システム部門としては、昨今の標的型攻撃の頻発や内部（委託先を含む）からの情報持ち出しによる漏えいといった情報セキュリティの脅威への対策を講じたいと考えても、対応の必要性について、明確な根拠を示せずに予算をうまく取得できないといった課題を抱えることになる。

2. 主観的な評価から合理的な解決へ

私は米国籍の日本法人で、情報システム部門の責任者を経験したが、在籍中に Y2K 問題が起こった。米本社からは、組織全体の利益に対する被害額を算出し、その対策にコストがどれだけかかるのかを出すよう指示があった。しかし日本では、システム部門で利益という経営的なことを考えることがなく、また、多くの場合、システム管理者としての経験や過去の実績など、主観的な判断要素に基づき、システム投資の意思決定を行うことが多かったため、この要求には面食らったことを覚えている。

このような場合、国際的なセキュリティマネジメントの標準（ISO/IEC27001[4]、ISO/IEC 27002 等）を参照することが考えられる。しかし、これら標準は、「これをすることが望ましい」とか、「こうしておくとよい」という表現が多く、標準を読んでその通りに実行すればよいという、「手順書」のようなものではない点に留意が必要である。ただその中でも、セキュリティ対策については、セキュリティの脅威がもたらす被害額を予測し、被害額と被害を予防するための対策費用とのバランスが取れていることと示されており、「望ましい」ではない点に注意が必要だと考える。

セキュリティ分野では、顧客を説得する要素として統計、事例、制約条件の 3 つがあげられる。まず統計を用いて、脅威が前年比何 % 増加の傾向にあり、対策すべき、と勧める。次に、事例を紹介し、どこでもやっているので、対策が必要ですと説得する。そして、このままではシステムが停止しかねないため、入れ替え必須である、というように、要素技術の制約条件で説得するパターンである。しかし、昨今のセキュリティの脅威の前では、統計や事例では、説得力が乏しい。それらに当てはまらない脅威が明日にも起こりかねない状況だからである。私が重要だと思うのは、3 つ目の制約条件であり、これには技術的な制約のみならず、時間軸での制約も該当する。

3. 定量化の必要性

日本でセキュリティ対策を検討すると、PDCA のようなループ状の時間軸で考えてしまいがちで、今発生していない脅威への対策など、来年のことは来年やればいいと考えてしまう。ところが、海外の場合はループではなくシーケンシャルな時間軸での制約条件を設定し、それに準じて対策を展開する。今年、来年、再来年、それぞれ何をやるかを、直線的に示すのである。その際には、社会環境の変化を含めて検討する必要がある。システムやセキュリティの要件定義をする際、お客様のニーズとしてやりたいことは多く出るが、時間という制約条件があり、いつまでに完了させる必要があるという期限は変えられない。

日本の場合、事業化に関して一番重要な間違いは、見積とは費用を算出することだと思う人が多いことである。ところが海外では、バリー・ベーム氏の COCOMO[5] にあるように、プロジェクトはある期間内で行うという原理原則がある（図 2）。つまり、管理するシステムの開発規模によって工数が決まり、工数によって期間が決められるのであって、たとえ何万人もプロジェクトに投入したとしても、期間が決まっていれば、実現できる要求にも限りがある。費用だけに着目すると、この点を見失いがちである。

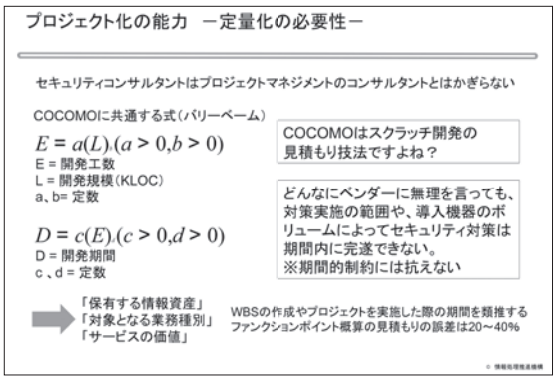

図 2　プロジェクト化の能力

4　http://www.isms.jipdec.or.jp/index.html

5　ソフトウェアの規模を見積もる手法のひとつ
http://sunset.usc.edu/csse/research/COCOMOII/cocomo_main.html

セキュリティについても同様で、限りある時間の中で優先度を決めて対策を講じる必要がある。また、セキュリティは専門分野が細分化されており、要求を取りまとめるにも、多方面での検討が必要となる点に留意することが求められる。

4. リファレンスの活用

セキュリティ対策のもうひとつの留意事項は、開発～運用まで異なるベンダーや開発者が個別部分で作業を行うため、相互運用性が維持できなくなるリスクがあげられる。IPAでは、このようなリスクへの対策のひとつとして、全体的な俯瞰図になる技術参照モデル（TRM）を発行している[6]。この中には、ユーザ（原課）の視点や、運用の作業者、システム部門の責任者からアドミニストレータの視点まで様々な立場の視点から見た情報が表現される。どの立場の人がどの部分の予算の話をしているのか、予算配分やどの機器を見直すべきかも含めて、全体を俯瞰するような図をはじめに作成する（図3）。情報資産の整理を行う場合には、部分的な対応に留まらず、全体像を把握することから始めるべきである。

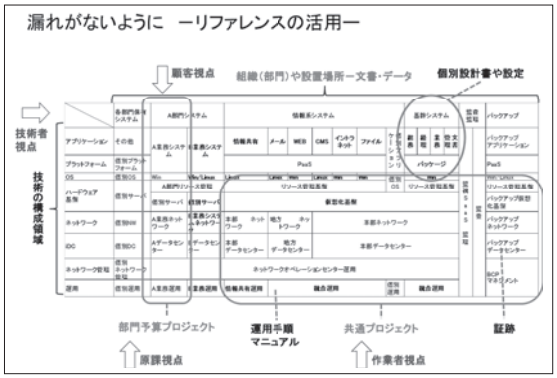

図3　リファレンスの活用

5. リスクアセスメントと対策の基準

セキュリティの専門家でも、セキュリティ対策を検討する際に活用することが少ないものに、ISO/IEC27005[7]がある。（2008年には発行されていたにも関わらず。）これはリスク管理プロセスと情報セキュリティ管理の規格で、組織が保有する情報資産に着目し、それらが内包するリスクに基づき対策を講じるという考え方を示している。

ISO/IEC27005を参照し対策を検討すると、まず組織の情報資産におけるリスクを評価・分析し、優先的に対応すべきセキュリティ課題がどこにあるかを特定する。実際のシステム運用の現場では、メディア等で知り得たセキュリティ脅威に対し、どんな手だてが打てるかを考え、ツールを導入する。昨今の情報資産に対する攻撃は、日々進歩し、新たな手法を用いた攻撃が次々と現れる。このような対策では、限界があることも否めない。このため、守るべき資産に何があり、どのようにリスクを排除または軽減するのかを検討するアプローチが有用であるといえる。そこで活用できるのが、ISO/IEC27005にあるリスクアセスメントのアプローチなのである。

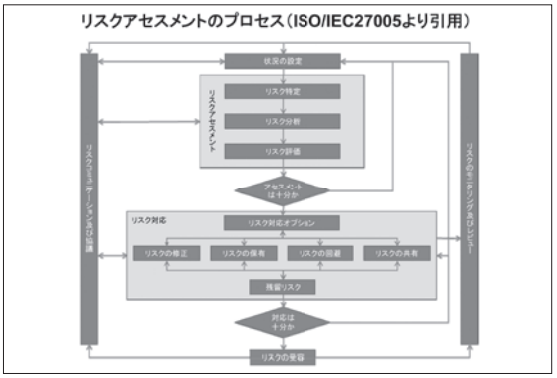

図4　リスクアセスメントのプロセス

ISO/IEC27005では、組織の情報資産を棚卸し、それらが受ける脅威とリスクを特定、分析、評価をして、その結果に基づく対応計画を立てる流れを示している。情報資産の棚卸が出発点であり、ここで漏れがないよう、前出のTRMを用いて情報資産を可視化し整理することが重要になる。また、情報にはIT（情報システムおよび通信機器や格納されたデータ）のみならず、紙の情報もあることに留意することも忘れてはならない。

また、日本では、セキュリティ対策というとセキュリティ委員会や分科会の設置等、体制整備に注力することが多い。また、セキュリティ対策計画を立てても、実際の現場で運用され、浸透するに至らないケースも見受けられる。体制整備のみならず、リスクアセスメントや対応計画の立案と実行にまで、力を入れるべきである。

6　http://www.ipa.go.jp/osc/trm/

7　http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=56742

6. リスクシナリオの推測と被害額の算定

情報セキュリティリスクへの対策を立てる際に、経営層に対してどのように説明すればよいのか。どの組織でも、どの事業予算を使ってセキュリティ対策を行うのか、部門をまたいだ検討が必要なのはもちろん、どのようなインシデントに対応するために、どの予算を使うのかを明確にしておく必要がある。

情報セキュリティにおけるリスクには、マルウェアを含むメールや不正サイトの閲覧、運用作業のミス等に起因する問題やウイルスの拡散、特権アカウントの奪取、バックドアの組み込みが促進要因となり被害が拡大し、情報漏えいやサービスの停止等の結果につながるという一連の流れを詳細に整理する必要がある（図5）。

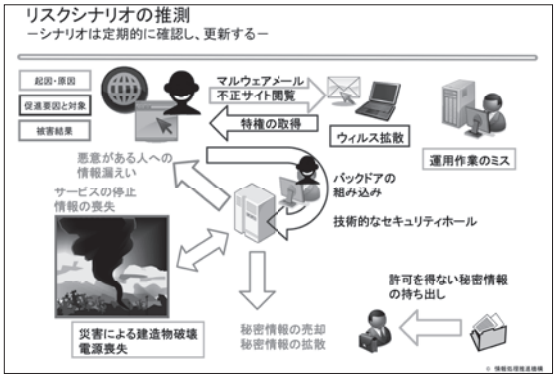

図5　リスクシナリオの推測

一方、リスクを考える際に、直接収入の損失額や倫理的事項に対する被害について説明できる人は非常に少ない（図6）。

IPAの例を挙げると、IPAの事業損害として情報処理試験が行えなくなることがあげられる。情報処理試験に関わるシステムが停止し、試験が開催出来なかった場合、事業の継続を脅かすほど多額の被害が発生するおそれもある。

その他に、個人情報が漏えいした場合を考えることも重要である。個人情報の漏えいには個人に対する罰則規定もあるが、組織においては損害賠償の責務が発生する。近年の平均的な賠償額は、一人あたり1万円から4万円程度である。保持している個人情報の量から賠償額を想定し、損害額を算出する必要がある。

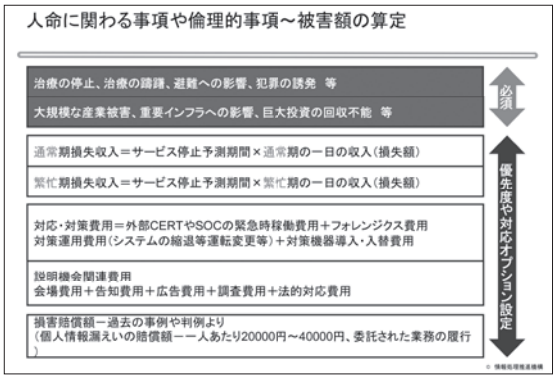

図6　被害額の算定

諸外国と日本で大きく違う点として、情報が漏えいした場合の損失額の検討において、日本では、その算出根拠が妥当かどうかに議論が集中してしまうことがある。その結果、根拠の妥当性が示せないと結論付け、リスクアセスメントやリスク対応計画の信ぴょう性にまで疑いの目を向け、何もしない、またはベンダーが提示するカタログどおりのセキュリティツールを導入する、ということになる。

しかし、損失額算定の目的は、リスク対応の優先度を決めることであり、損失額の研究をしているわけではない。リスク対応においては、その必要性や対応の順序を論理的に整理することが重要である。

高額医療対策を例に、リスクアセスメントの方法について説明する。病気の薬代で月40万円かかる場合、一般的なサラリーマンの収入では払いきれず、高額医療対策等の補助を受ける。もし、この制度がなくなったら、薬を飲むことを諦めてしまう人が大半だろう。その結果、病気の悪化、また長期の治療が必要になるなどすれば、保険料負担が高まり、補助金を出すより行政の負担が高まることが懸念される。このような生命に関わること、また犯罪を誘発するような、倫理的な問題に関わることは、損害額の算定は不要で、即時優先的に対応を行うこととする。

インシデントは、身近な話で考えるとわかりやすい。漠然とした「運用作業ミス」や「災害」という言葉ではなく、日常で発生しているようなインシデントを具体的に想定して確認をする必要がある。

IPAでは、My JVN[8]という脆弱性情報を提供している。この提供情報が止まってしまった場合、重要インフラの維持を目的に脆弱性情報を取得している利用者への情報提供

8　http://jvndb.jvn.jp/apis/myjvn/

が止まり、重要インフラに関わる損害が発生するかもしれない。リスクシナリオを書くことは、より詳細にリスクを想定し、自分が持っているリスクの恐ろしさを認識してもらうことも目的である。「許可を得ていない情報の持ち出し」という言い方ではなく、重要な研究データを持ち出した結果、それが漏れた場合、どんな事件になるかというように具体的に考え、それに対して、責任を持てるかどうか判断を問うのが、リスクアセスメントである。

IPA のシステムを例に挙げると、まず、止まっても人命や倫理的な問題に関わらないものであれば、投資の優先度は低くする。次に、情報処理試験に関するシステムが止まり、試験が中止になれば損失額が大きいので、これも優先的に対応すべき、ということになる。

リスクが発生した際に、対策チームの稼働費用やフォレンジクス費用、システムの対策費用や説明や広告を打つための費用も必要になる。明日その問題が発生しても対応できるよう、シナリオを事前に組んでおくべきである。

7. 必須対策以外の対策優先度

必須対策以外の対策優先度を決めるために、細かく確認をすべきところをまとめたのが図 7 である。システムの分類からインシデントや想定被害額、対象の情報資産等があるが、対応策と費用をどこに割り振るかを細かく分けて考える必要がある。このような詳細化にあたっては、必須対策のものも、そうでないものも、調達仕様の作成を意識することとなる。仕様の検討においては、製品に関する理解だけでなく、一連のリスクアセスメントの作業や考え方を理解しているメーカーやベンダーの協力も必要となる。ただし、自社の手法しか説明できない担当者だった場合は、注意が必要だ。

最も重要なのは、制約条件である。これは金額だけでなく、いつまでにやるのかという時間的制約のことである。

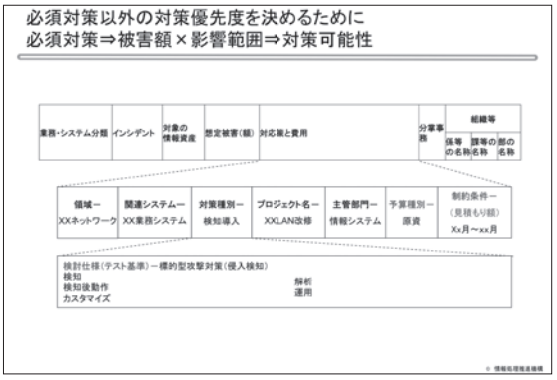

図 7　必須対策以外の対策優先度

ISO/IEC27005 のリスク対応プロセスに、残留リスクがある（図 4 参照）。これはリスクの全てに対し一度に対応するのは難しいことから、未対応である点を記録し、次の担当者に引き継いだり、次の年に対応したりすることである。残留リスクとするにあたっては、対応ができていない事をリスクとして識別し、説明責任を負えるかが重要になる（図 8）。単なる先延ばしは間違いで、いつまでにやりきるかという明確な計画は、立てるべきである。

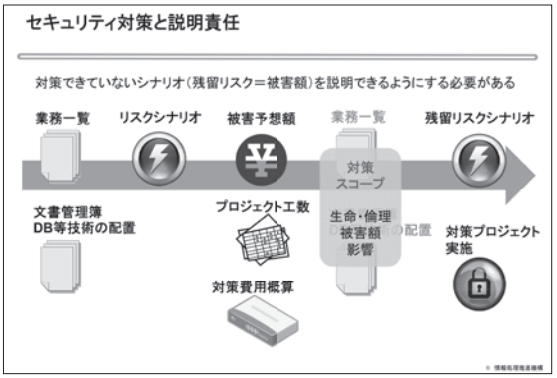

図 8　セキュリティ対策と説明責任

8. 対策機器導入の盲点

対応策において具体的なツールを特定する場合、そのツールを導入することが目的ではないことに注意しなければならない。高度標的型攻撃の対策のために、APT（高度な脅威保護）と言われるツールを入れればすべて解決するわけではない（図 9）。高度標的型攻撃には様々な種類があり、SOC と言われるセキュリティオペレーションセンターや

SIEM[9] との連携が不可欠である。また、対策機器を選定する際にポイントとなるのは、検知性能である。検知するスピードが速いのか、検知可能な媒体が多いのか、対象物が膨大でも解析できるのか等、細かく仕様を確認する必要がある。これは、それ単独でトータルなセキュリティ対策が可能なツールはないからである。侵入検知に優れていても、どんな動作をしたかを検知できないものもあるので、偵察検知能力が高いか、レポートが分かりやすいものか等、総合的に判断する必要がある。判断の基準となるのは、やはりリスクアセスメントの結果である。どの情報資産がどのような危機にさらされているかを整理し、検知能力が高い機器を選択するか、偵察検知能力が高い機器を導入するかを判断する。リスクシナリオが明確でないと、的確な機器の選定はできないのである。

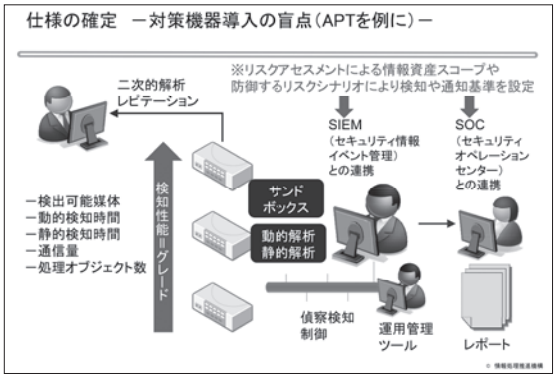

図 9　対策機器導入の盲点

9.　セキュリティ対策と説明責任

次々に発生する情報セキュリティの新たな脅威、これは外部からの攻撃に留まらず、内部（委託先、再委託先を含む）からの情報漏えいも内包し、一口に対策を講じるといってもどこまでやるべきか、何からやるべきか、悩ましい問題である。特に、クラウドの利用増など、組織の情報システムが様々なものと連携したことで、リスクシナリオを想定するにも、範囲も広がりアセスメントのスコープを設定するのも一苦労といったところだ。

国立大学法人においては、リスクアセスメントにかかわるガイドライン[10]が、内閣セキュリティセンターから公表されている。ここでは、情報セキュリティのリスクアセスメントを行い、セキュリティセンターや災害セキュリティ本部でリスクを把握し、定期的にチェックする流れが説明されている。これまで述べてきたリスクシナリオを決め、組織としての被害額を把握し、それに基づき対策することが重要であるという認識は、本ガイドラインでも示されたとおりである。ともすると、起きている脅威やそれを防ぐ個々の情報技術の視点だけで対策を検討しがちだが、組織の情報資産は経営資源であり、経営視点で検討することにより、網羅性を確保しつつ優先度をつけた対応計画の立案が可能である。

経営視点で対応計画を立てるためには、IT の知識のみならず、予算取得のための会計知識や資産保護の優先度に影響する法律に関する知識も必要となる。国立大学法人として、なぜそのような対策を講じたのか、現状の環境に対し説明責任を果たすためには、リスクアセスメントに立脚した対策を行える力をつけるべきである。

9　セキュリティ情報イベント管理

10　高度サイバー攻撃対処のためのリスク評価等のガイドライン
http://www.nisc.go.jp/active/general/risk.html