ソリューション・レポート

ITシステムにおける情報セキュリティの実装と運用
― システムライフサイクルマネジメントモデルに沿った情報セキュリティ管理プロセス ―

アウトソーシングビジネスユニット
ITガバナンスコンサルティングセンター長
井上　広

1．はじめに

2005年4月に個人情報保護法が施行された。しかし、この原稿を書いている同年4月半ば現在、報道される個人情報漏洩事故・事件の数はいっこうに減らない。企業における情報セキュリティ対策の遅れ、というよりは、効果的な情報セキュリティ対策がいかに難しいかを物語るものだ。

法施行までの個人情報保護対策では、PCの暗号化やログ取得ツールの導入、社員の一斉教育など、短期間で実施できかつ効果的なクイックソリューションを中心とした企業も多い。アプリケーションログの見直し、業務フローの見直しなど、既存の情報システムの変更が必要なセキュリティ対策の課題がまだまだ残されている。中期的な視点での情報システムにおけるセキュリティ管理はこれからがスタートともいえよう。

クイックソリューションでは、セキュリティベンダーが中心的役割を果たしてきた。しかしこれからはソフトウェア開発を含めたすべてのSIベンダーが情報セキュリティに対して大きな責任、役割を果たしていかなければならない。このレポートでは、情報システムの大きなライフサイクルの中で、どのような視点で情報セキュリティを構築・運用するのか、またSIベンダーとしてのCACはどのような方針でサービスを提供しなければならないのか、考えてみたい。

2．情報セキュリティのPDCAとシステムライフサイクル

情報セキュリティの管理基準であるISMS認証基準は、PDCAによるライフサイクルモデルをベースに作られている。「ISMSの確立」「ISMSの導入と運用」「ISMSの監視とレビュー」「ISMSの改善」を通じて情報セキュリティリスクを適切にコントロールし、企業活動の継続を担保することを目的としている。また経済産業省の個人情報保護に関するガイドライン（参考文献1）でも、組織的安全管理措置としてPDCAライフサイクルを講じなければならないとしている。

しかしこれら基準は企業全体の情報セキュリティ活動について明記したものであり、情報システムの管理については、詳細に書かれてはいない。企業全体の情報セキュリティライフサイクルに沿った形で、情報システムの管理にもPDCAによる管理モデルが必要であろう。

情報システムの品質管理として、ISO9000やCMMなどを取り入れているSIベンダーは多い。どちらもPDCAをベースとしたライフサイクルモデルである。同様に情報セキュリティ管理にも、PDCAをベースとしたモデルを取り入れるべきである。CACは、ソフトウェアを中心とした情報システムのライフサイクルマネジメントの基準であるSLCP（参考文献2）を利用して、情報セキュリティ管理の枠組みを検討した（次ページ図1）。

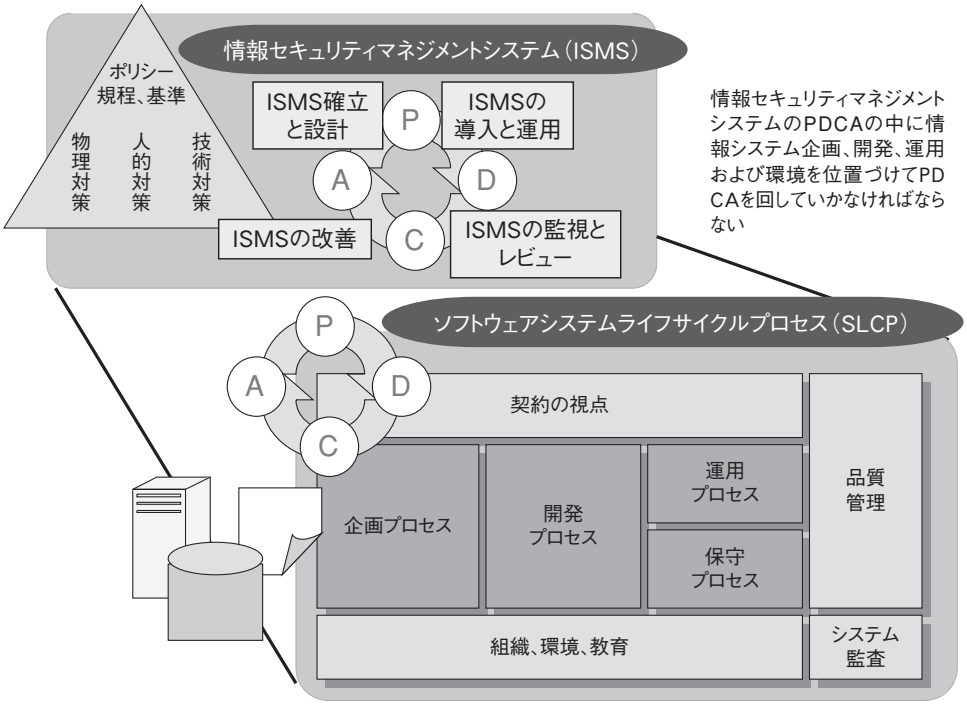

図1　情報セキュリティマネジメントシステムとソフトウェアシステムライフサイクル

2.1　企画プロセス

企画プロセスは、IT戦略の策定、システム計画のフェーズである。情報セキュリティは、独立した単独のシステムではない。業務、運用、インフラ、アプリケーションすべてに総合的に関わる課題である。上位フェーズでは、情報セキュリティの計画は重要な位置を占める（図２）。

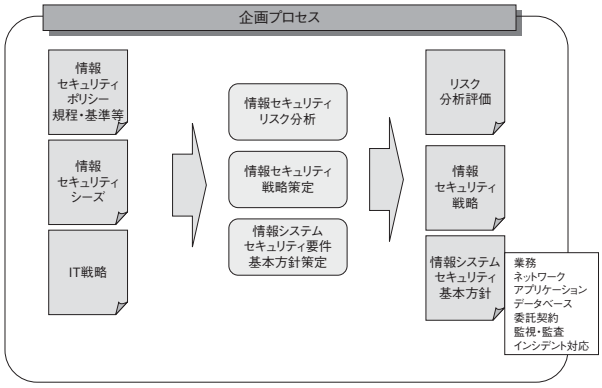

図2　企画プロセス

1）情報セキュリティ戦略

IT戦略策定では、情報セキュリティ戦略を同時に策定すべきである。

情報セキュリティは、ネットワーク、データベース、クライアントPC、アプリケーションなど、レイヤを統合した視点で設計していかなければ効果的な対策は打てない。たとえばアクセス記録の分析では、いつ、誰が、どのデータを、どこから、どのような権限および業務に基づいて、アクセスしたのか記録していかなければならない。クライアントPC、ネットワーク、データベース、アプリケーションなど、関係するすべてのレイヤに、あらかじめ定めた方針、基準に則り記録されていなければ、正確な情報は得られないことになる。

PCやネットワークのリプレイス、アプリケーションシステムのリプレイス、データベースのバージョンアップなど、それぞれの導入時期は異なるだろう。その都度情報セキュリティ対策を考えるのではなく、将来的なセキュリティの実装のゴールを見据えて計画しておく必要がある。図３に中期計画での情報セキュリティ対策ロードマップの例を示す。技術の関連性、優先度を踏まえ、システム相互の関連性を明確にしておく。情報セキュリティにおけるITや環境の変化は激しく、毎年の見直しを必要とする。

2）情報システムにおける情報セキュリティ基本方針

システム計画では、品質の基本方針と同時に情報セキュリティに対する基本方針を併せて検討する。システム開発において情報セキュリティは品質の一部といえるが、スループットや利便性などとのトレードオフの関係になることが多い。

個人情報保護法施行を受けた対応では、PCの持出し禁止やデータ閲覧の制限など、ユーザーの負担が伴う対策を実施した企業も多いと思う。それは、同時に業務効率をかなり犠牲にしたのではないだろうか。業務のきしみ、不満、運用コスト増などの問題が出てくるのはこれからだろう。

これまでのシステム構築がITの利便性を最優先しすぎた反省もあるが、利便性や効率を含めた枠組みの中で、再度

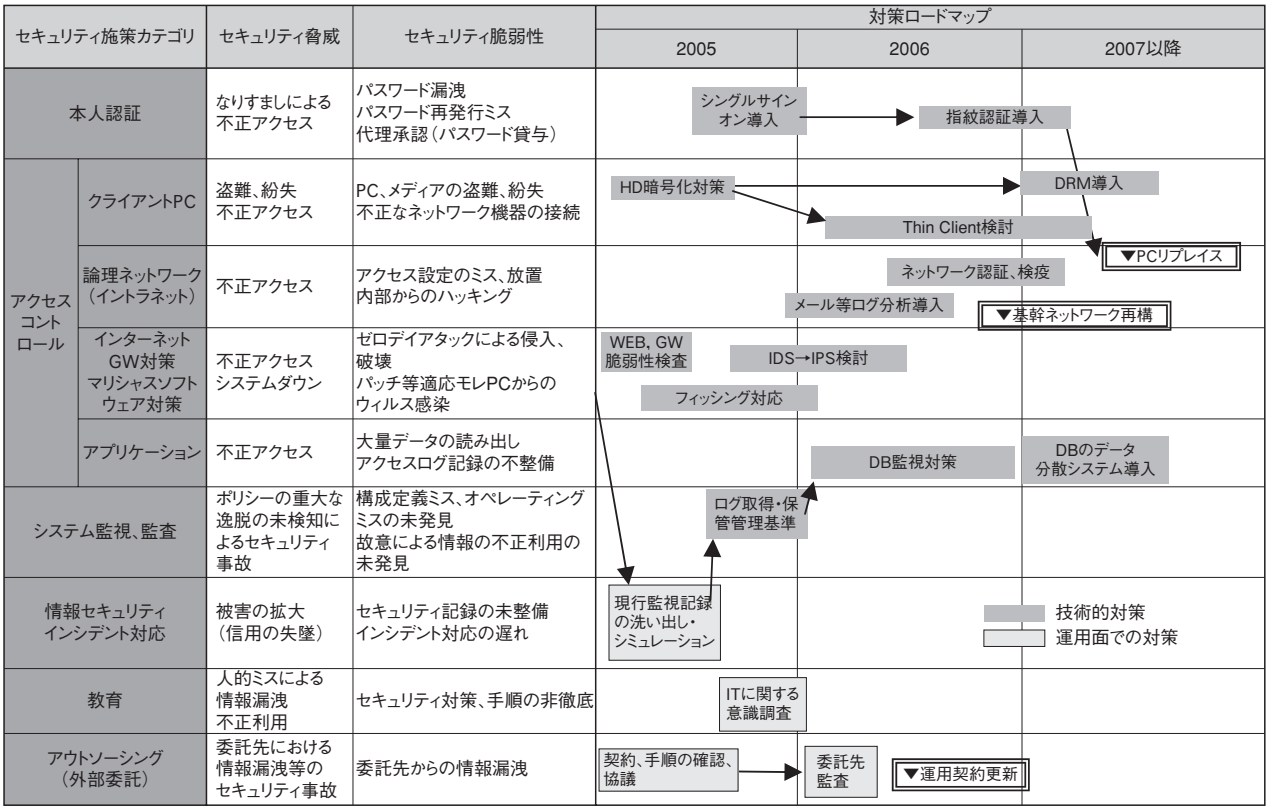

図3　情報システムにおける情報セキュリティ戦略ロードマップ例（情報漏洩対策を中心とした対策）

情報セキュリティの方針を見直す必要がある。

また、企業の情報セキュリティ基本方針は、SIベンダーへ提示するセキュリティ要件のベースになるものでもある。技術的な内容に加えて、監視、監査方針やインシデント対応方針、委託契約方針などを含めて定義しておく。その内容は以下のようなものだ。

・業務設計／運用方針
・ネットワークインフラ設計／運用方針
・アプリケーション設計／運用方針
・データベース設計／運用方針
・SI／SOベンダー委託契約方針
・情報システム監視・監査および記録の方針
・情報セキュリティインシデント対策方針

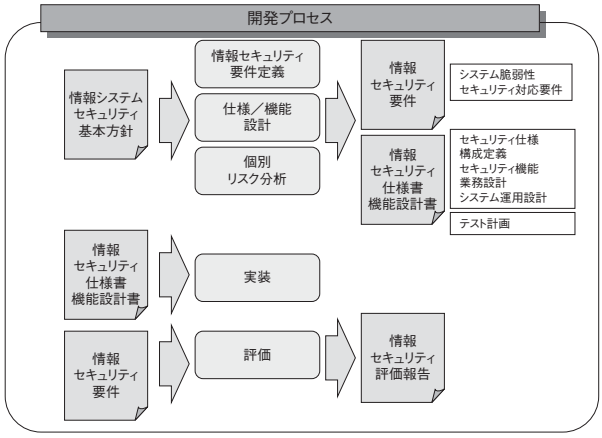

図4　開発プロセス

2.2　開発プロセス

開発プロセスでは、個々の情報システムに対して、実際に情報セキュリティの組込みを行う。その手順は通常のシステム開発と同様である。要件定義、仕様／機能設計、実装、評価(テスト)を通じて適切な情報セキュリティを実装する(図４)。

1）情報セキュリティ要件定義、仕様／機能設計

情報セキュリティ基本方針に従い、対象となる情報システムの情報セキュリティ要件を定める。

情報セキュリティ要件は、どのような情報セキュリティの脅威からどの程度に守るのか、を定めるものである。対象となる情報システムが扱う情報資産の価値や利用目的、およびネットワーク環境などの前提条件などによって異なってくる。たとえば不特定多数のユーザーがアクセスできるインターネット上のウェブアプリケーションシステムには、多くの外的脅威が存在する。また個人情報を扱うシステムでは情報漏洩のリスクが非常に大きいため、十分にその脅威から守られなければならない。

必要であれば対象システムに対するリスク分析を行い、セキュリティ要件を定める。

仕様／機能設計では、セキュリティ要件を充足する仕様および機能を決定する。技術的な視点だけではなく、業務プロセス、システム運用プロセス、人的要素、物理的要素を適切に定義しなければ効果を発揮できない。特にシステム運用プロセスは開発時点で十分に設計しなければ、要件の充足を確認することはできない。

セキュリティ要件の高いシステムでは、セキュリティアーキテクトのレビューが必須となる。

要件定義と仕様／機能設計として以下の例が挙げられる。

・情報セキュリティ要件

インターネットを利用した通信データを、第三者に傍受、改ざんされることを防ぐ

・仕様／機能

ウェブへのアクセスにはSSLを利用する

・評価方法

第三者（セキュリティベンダー）による脆弱性検査を実施する

2）情報セキュリティ評価

情報セキュリティの評価では、情報セキュリティ要件を満たした実装が確実に行われていることをテストする。

要件が実装されているかどうかの評価であり、実装した機能の確認だけでなく、ブラックボックステストによって確認することが望ましい。ただし情報セキュリティ評価は時間やコストのかかる作業であり、情報システムが求めるセキュリティ要件レベルに合わせて評価手法を選択する。情報セキュリティ要件では、あらかじめ評価基準を定めておかなければならない。

セキュリティ評価レベルと選択する手法として以下の例が挙げられる。

・レベル１　ソースコード・レビュー
・レベル２　自動ツールによる脆弱性検査
・レベル３　第三者による脆弱性検査（ブラックボックステスト）

2.3　運用プロセス

情報セキュリティの最終評価は、ユーザー、運用担当者を交えて、実際の業務を通じて判断しなければならない（図５）。ユーザーは必ずしも設計していたとおりに業務を遂行するとは限らないからである。

また本番運用後も、情報セキュリティが維持されていることを定期的に評価しなければならない。もちろん運用時に発見された不具合、ミスを通じてセキュリティ対策や手順を見直すプロセスが必要である。

1）運用テスト、移行

ユーザーを含めた運用テストを通じて、定めた運用プロセスが設計通りに実施できるかどうかを確認する。運用テスト時には、しばしば想定しなかった業務手順の変更や運用手順の変更が発生する。加えた変更によってセキュリティ要件を損うことがないよう注意する。最終的な情報セキュリティ運用評価を行ったのちに本番運用の開始となる。

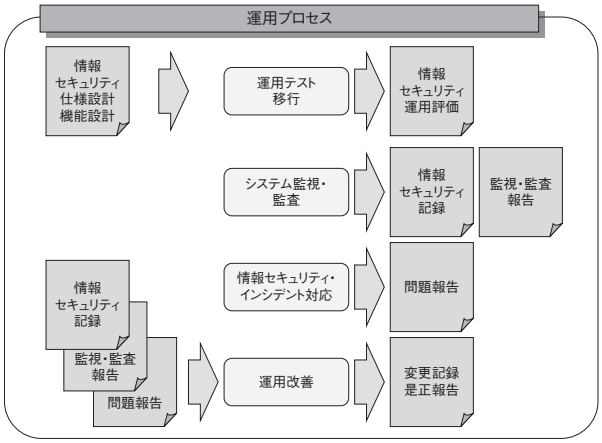

図5　運用プロセス

また移行フェーズでは、開発担当者など多くの一時作業者が関わり、一時的な運用手順が発生する。情報セキュリティ要件の高い情報システムでは、移行時の情報セキュリティリスクも考慮し、作業手順を作成しなければならないだろう。

2）本番運用

本番運用では、設計されたセキュリティレベルが常に維持されていることを監視し確認する。また定期的なセキュリティシステム監査によって評価する。監視、監査、あるいは情報セキュリティインシデントによって見つかった不具合は問題報告として記録し、確実に是正を行う。

この本番運用では、情報セキュリティポリシーや基準の見直し、教育・訓練、物理的対策など総合的な視点でセキュリティを監視、改善する。

3）セキュリティ事故・事件の対応（インシデント対応）

万一情報漏洩などの大きな情報セキュリティ事件・事故が発生した際には、速やかに適切で迅速な情報の公開、原因の追求、是正処置を行わなければならない。事後対応の手際は信用面に大きな影響を与える。信用の早期回復こそが企業の最大の課題となるだろう。

情報システムに関しては、運用担当者が事件事故発生時にあらかじめ定められた緊急時行動を適切に取れるかどうかが重要であり、手順の準備と訓練を必要とする。またSIベンダーに対しては緊急時の一時的な作業が要求されるケースも考えられる。契約を含めた整理が必要である。

さらには運用担当者の潔白を証明するためにも、別メンバーによるレビューや監査手順を定めることも検討すべきだろう。

2.4　保守プロセス

情報セキュリティを取り巻く環境、社会、技術は日々変化している。

毎月のようにWindowsの脆弱性が発表されていることは、変更いらずのシステムを作ることの難しさを表わしている。新たに発見されるウィルスの脅威、フィッシングサイトのような巧妙になるウェブ犯罪の手口など、変化の激しい情報セキュリティ環境の中で、保守プロセス(図６)なしに情報セキュリティは保てない。

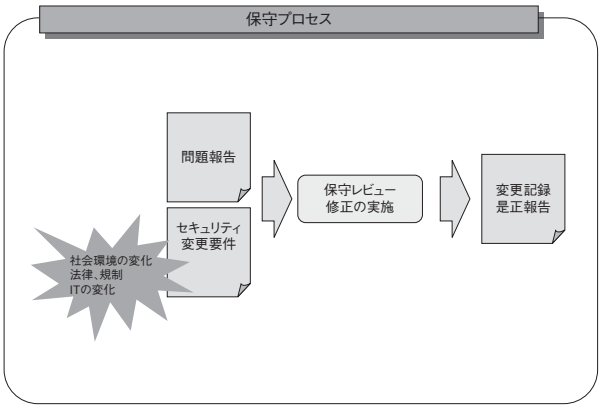

図6　保守プロセス

1）情報セキュリティにおける保守プロセス

システムの改定手順は、開発プロセスと基本的な流れは同一である。要件を定め、機能を設計し評価を行う。しかし、保守案件では部分的な修正ごとに十分な評価（テスト）が実行できない場合が多いだろう。またセキュリティパッチの適用などでは緊急を要する場合もあり、迅速なリリースが必要となる。しかし安易な変更は脆弱性を招き、セキュリティ要件を崩す要因となりかねない。

あらかじめ保守のレビュー手順を定め、情報セキュリティ要件が遵守されていることを確認できる手順を確立しておく。また、セキュリティリスクを防ぐため、パッチなどの評価が終わるまで、一時的にサービスに制約をかけて運用する、などの暫定手順も考えられる。

3．契約、およびSIベンダーに求められる責任と役割

情報システムの開発や運用をSIベンダーにまったく委託していない企業はほとんどないだろう。情報セキュリティでは、発注企業側に、委託先SIベンダーに対する監督責任が伴う。委託先で起きた情報セキュリティ事故・事件について発注側企業の管理責任を全面的に免れることは難しい。また責任の如何によらず、企業ブランドに大きなダメージを受けることになりかねない。

監督責任があるとはいえ、自社の情報セキュリティポリシーや規程・基準をそのまま文化や環境の違う委託先SIベンダーに適用させることは難しい。たとえば従業員に対して行った雇用契約や懲戒懲罰規程は、ベンダー社員に対しては効力を持たない。セキュリティ教育においても文化や情報リテラシーの違うベンダーに対しては相応のプログラムが必要となり、単純には当てはめられない。

そこで、委託するSIベンダーとの契約では、セキュリティに関する要求を適切に記述しなければならない。当該SIベンダーが契約をきちんと遵守できるかどうか、信用の評価も行なわなければならない。SIベンダーに依存する度合いが高いほど、この契約プロセスの重要度は非常に高い。

3.1　顧客がSIベンダーに求めるもの

では、顧客企業はSIベンダーに情報セキュリティに関して何を望むべきか。それは以下の３点である（図７）。

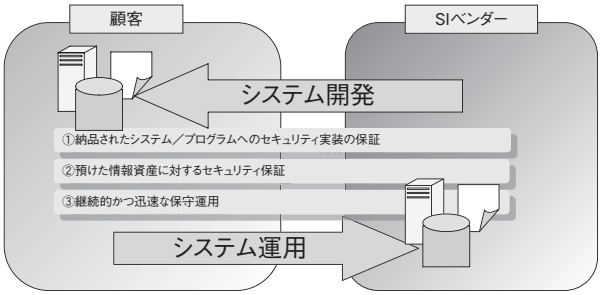

図7　セキュリティに関して顧客がSIベンダーに望むこと

1）納品されたシステム/プログラムへのセキュリティ実装の保証

設計、開発した情報システムが十分にセキュアであること。SIベンダーからこの保証を取付ける必要がある。開発したウェブアプリケーションが情報セキュリティ要件を満たしておらず、コードの脆弱な部分をアタックされて情報が盗まれた場合、設計・実装を行ったSIベンダーに責任があるだろう。この場合のセキュリティ保証とは、品質保証の一部として重要な要素となる。

プログラムのバグによる事故は明らかにSIベンダーのミスと考えられるが、ではセキュリティ要件上の洗い出しの漏れはどちらの責任だろうか。要件定義まではコンサルティング契約、設計からSI契約であれば、要件定義を策定した発注側の責任も否めない。専門性の高いセキュリティ要件を十分に策定、検収できる能力がなければ、発注側の企業の大きなリスクとなってしまう。

こうしたSI開発における品質責任の問題は従来からあり、情報セキュリティ要件に限ったことではない。しかし、運用テストでは脆弱性の発見が難しいこと、ひとたび事件が起これば莫大な損害が発生することなどを考えあわせる

と、情報セキュリティでは契約および検収の枠組みをしっかり検討すべきである。

2）預けた情報資産に対するセキュリティ保証

本番運用では、情報資産そのものをSIベンダーに預けることになるため、資産およびサービスの情報セキュリティについて保証を求めることになる。

運用のアウトソーシングを行う際は、運用の実態がブラックボックスになるため、契約の定義は慎重になるべきである。フルアウトソーシング契約では、年度ごとのコストダウンを条件にすることがしばしばあるが、セキュリティ要件を下げないことを前提としなければならない。

開発と運用が異なるベンダーである場合は、設計が運用に確実に移行されているかどうかを互いに確認し、設計上の責任と運用上の責任を明確にする必要がある。

情報セキュリティの評価を定期的に行うために、SIベンダーに対する監査は重要である。監査についての条件を契約に盛り込んでおく。さらにSIベンダー自身による内部監査の実施を契約に含めることで、保証が担保されていることの報告義務を持たせるのがよい。

運用だけでなく開発を委託するベンダーに対しても、開発環境の安全性の確保を契約に明記すべきだろう。同時に「本番データを開発時には使わない」など、事前にリスクを十分に下げておくべきである。

3）継続的かつ迅速な保守、運用

情報セキュリティに関しては、社会環境の変化、技術の変化が非常に速い。システム納品時には想定されなかった新たな脆弱性が次々に発見される。

また、情報セキュリティに対する脅威には早急に対応しないと、企業にとって致命的な損害を招く恐れがある点が大きな特徴だ。新型のウィルス、OS等の脆弱性、あるいはウェブフィッシングなどの新たな情報セキュリティ事件など、次々に起きる情報セキュリティイベントに対して迅速で適切な対応が求められる。

システム開発を委託する際には、継続的で迅速な保守が可能であるSIベンダーを選択しなければならない。保守契約では、対応スピードや専門性についての体制の見直しが必要だろう。

3.2　情報セキュリティ保証の枠組み

では、SIベンダーは前述の顧客の要求に応え信頼を得るにはどうしたらよいか。CACはどのようなサービスをすべきか、その枠組みについて考えてみる。

1）損害補償

保証というとまず損害補償が思い浮かぶ。SIベンダー側の過失によるセキュリティ事件・事故によって発生した顧客の営業損失、利益損失について補償することである。

しかしこれはあくまでも事後の対策だ。顧客にとってはセキュリティ事件による信用の失墜は深刻で、信用回復までを十分に保証できる可能性は低い。また、個人情報漏洩事件による賠償金額も数十億～百億円以上といった莫大な数字となりえる。SIベンダーの体力を大きく消耗させることは発注側にとってもデメリットである。

損害補償としての情報セキュリティ保険の活用はこれからの重要な対策の１つであるが、これだけで保証の担保を行うのには無理がある。

2）品質管理体制

情報セキュリティ事故を未然に防ぐための保証の枠組みが必要である。情報セキュリティも品質システム同様、プロセスや環境によって保証することができると考えられる（図８）。

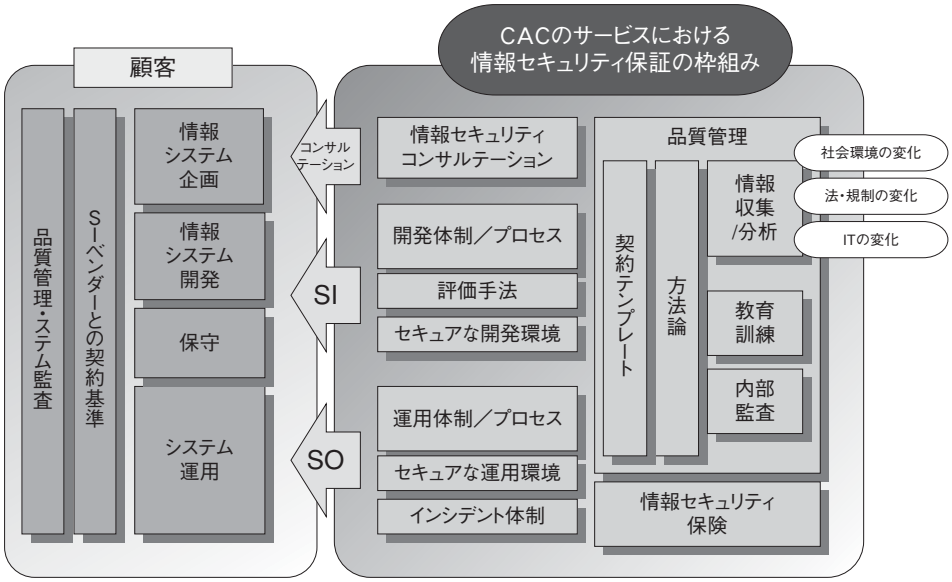

図8　CACのサービスにおける情報セキュリティ保証の枠組み

SIベンダーは、情報セキュリティの構築/運用方法論を準備し、標準プロセス、テンプレートを用意する。開発、運用を行うのに必要な教育を実施し、必要なスキルを持つエンジニアを育成する。定期的な内部監査を行い、改善を行う。情報セキュリティに関する社会環境の変化、法や規制の変化、IT技術の変化に伴い、見直しをかけていく定常的なプロセスを実施する。

このプロセスを実施するには、従来以上にSIベンダー企業としての組織、枠組み、プロジェクト支援体制が必要となるだろう。またその枠組みを示すことで顧客の信用を得ることができる。

4．終わりに

システム開発、システム運用は顧客とSIベンダーの共同作業であり、互いに共通のフレームを理解し、互いに改善していかなければならないものであろう。今後は政府や業界を通じた規制やガイドラインが整備されていくものと思われる。

しかし情報セキュリティは専門性の高い分野である。システム設計にあたっては「顧客の言葉で仕様を定義する」とよく言われるが、情報セキュリティの設計や評価においても、わかりやすく正確に顧客に伝えること、これもまた重要な品質の一部と考えられるだろう。

現在、CACでは、生産品質強化本部が主管となり、ITガバナンスコンサルティングセンターのITセキュリティチームと共同で、当社のSI／SOサービスにおける情報セキュリティのフレームワークを整備、改訂しているところである。その中でも、当社のサービスにおいて情報セキュリティに対する方針をお客様に提示する文書が最も重要であると考えている。

〈参考文献〉

1. 経済産業省：『個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン』（2004年）
2. 経済産業省：『SLCP-JCF98　ソフトウェアを中心としたシステム開発および取引のための共通フレームワーク1998年版』（1998年）