エンタープライズ・セキュリティ・アーキテクチャ

Enterprise Security Architecture

遠　藤　英　幸

要　約　一般的に情報セキュリティ活動を継続的に統制することの困難さは，主に情報セキュリティが持つ「多様性と変化」，「運用の負荷（業務効率の低下）」，「投資効果の不透明さ」という三つの特性に起因している．企業が情報セキュリティガバナンスを継続的に維持（すなわちエンタープライズ・セキュリティを確立）するためには，情報セキュリティ活動の全体統制を図るための戦略的な枠組み（エンタープライズ・セキュリティ・アーキテクチャ）の構築が不可欠である．本稿では，エンタープライズ・セキュリティ・アーキテクチャを，四つのレイヤで構成し，さらに個々のレイヤに含まれる構成要素を整理する．また，エンタープライズ・セキュリティを効果的に維持するためのポイントを述べ，今後のエンタープライズ・セキュリティの在り方を論ずる．

Abstract　Generally, the difficulty of the continuous management of the information security activities is attributed to three main factors, namely “diversity and changes”, “load of operation (decrease in operating efficiency)”, and “uncertainness of investment effect”. It is necessary to construct a strategic framework for general control of information security activities (enterprise security architecture), so that the enterprise may maintain the information security governance (enterprise security). This paper gives an outline of the four-layered enterprise security architecture, and organizes components included in individual layers. Additionally, it discusses the point to maintain the enterprise security effectively, and the ideal future for one.

1. は　じ　め　に

2005 年 4 月に施行された個人情報保護法により，企業の情報セキュリティ対策が本格的な動きを見せた．その後も，後を絶たない情報セキュリティ事故を教訓に，様々な対策が実施されてきた．しかし，情報セキュリティ事故は，内部の人間の不注意や，巧妙さを増し高度化するセキュリティ侵害によって，依然として後を絶たない．報道などによって知りえた情報をもとに，適宜，対策を追加しているとは言え，統合的な対策というには及ばず，場当たり的な対策に留まっているのが実状ではないだろうか．

情報セキュリティマネジメントシステムの運用においても，ISMS とプライバシーマーク（個人情報保護）の統合的な運用がなされておらず，それぞれ単体で実施されているという印象が払拭できないのも，企業における実状ではないかと推察される．

また，システムインテグレータとその顧客の間にも，情報セキュリティ対策についての新しい認識が芽生え，実行に移されようとしている段階であることも忘れてはいけない．開発段階において，品質要件としてのセキュリティ対策についての明確化とその実装が求められ，また，運用段階においても，セキュリティ対策レベルを維持するための方策とその実施が求められている．その第一の理由は，情報セキュリティ事故による損害が，企業経営に大きく影響を与え

ることであろう．

こうした背景から，企業が情報セキュリティガバナンスを継続的に維持する，いわゆるエンタープライズ・セキュリティを確立するためには，情報セキュリティ活動の全体統制を図るための戦略的な枠組み，すなわちエンタープライズ・セキュリティ・アーキテクチャの構築が不可欠である．本稿では，このエンタープライズ・セキュリティ・アーキテクチャについて考察する．

2. エンタープライズ・セキュリティ

企業がエンタープライズ・セキュリティに取り組む場合，次のことを要求事項として考えなければならない．

・経営戦略，事業計画
・法令順守（コンプライアンス）
・社会的責任

経営戦略，事業計画については，企業の本質としての活動を定義するものであるが，法令順守，社会的責任についての一定の枠組みの中で許された範囲内での活動でなければならない．情報セキュリティは，主に法令順守，社会的責任に動機付けされた活動と見ることができる．企業にとっては本質的な活動を律する制約と言えるのである．

2.1 情報セキュリティガバナンス

近年，情報セキュリティガバナンスが提唱されている．経済産業省[2]によれば，「社会的責任にも配慮したコーポレートガバナンスと，それを支えるメカニズムである内部統制の仕組みを，情報セキュリティの観点から企業内に構築・運用する」ものと定義されている．この背景として，次のことが述べられている．

・セキュリティ事故が発生すると企業の存続が脅かされる事態に陥ることがある
・ひとつの会社の事故が社会全体に波及する可能性がある
・顧客情報，製品情報などの企業が保有する情報の価値が高まっている
・個人情報保護法等の施行に伴い法令順守が大きな課題となっている

一旦セキュリティ事故が発生すると，自社のみだけではなく，取引他社，あるいは，社会全体に影響を及ぼしかねないことを意味しており，これらの対策は，全社統制の中で運用されなければならないことを示している．

2.2 情報セキュリティ運用の課題

情報セキュリティ対策を継続的に実施していく上で，最大の課題は，推進力をいかに持続させていくか，ということである．そこには，推進する立場，対策を実施する立場の両面での課題がある．まず，推進する立場としての課題は，いかに効率よく進めるかが最大の関心事になりがちになることである．対策を実施する立場としての課題は，それによって業務の効率が下がることを嫌い，対策導入以前の業務フローに戻す意識が出始めることである．

危機意識の低下も，推進力の持続を妨げる一因となる．一部の ISMS 認証取得企業に限った例だが，認証取得時には経営層を含め従業員の意識も非常に高いものの，取得から数年のうちには意識が低下し，一部の対策は定型作業として継続される一方で，あまり実施されない対策

も出てくる傾向にある.

2.3　困難さの原因

一般的に情報セキュリティ活動を継続的に統制することの困難さは，主に情報セキュリティが持つ「多様性と変化」,「運用の負荷（業務効率の低下)」,「投資効果の不透明さ」という三つの特性に起因している.

2.3.1　多様性と変化

「多様性と変化」の観点からは，情報セキュリティの対象となる事業，業務プロセス，それらに含まれる情報資産等の範囲，情報セキュリティ事故の要因となるセキュリティリスク，及びリスク対応として実践すべきセキュリティ対策の種類と範囲が，極めて広範囲に渡ること，企業が順守すべき情報セキュリティに関わるコンプライアンス要件，経営戦略の変化に伴う事業ドメイン，活動拠点，業務プロセス，情報資産，コンピュータウイルスや不正アクセス手法等に代表されるセキュリティリスク，セキュリティ対策技術等の要素が非常に短いサイクルで変化することが挙げられる.

2.3.2　運用の負荷

「運用の負荷」の観点からは，過剰なセキュリティ対策の実践により，業務やシステム運用の効率が低下し，現場の不満が増大することが挙げられる.

2.3.3　投資効果の不透明さ

「投資効果の不透明さ」の観点からは，実践しなければならないセキュリティ対策の効果を可視化し，経営陣，従業員の理解を得ることが非常に難しいという課題が挙げられる.

2.4　エンタープライズ・セキュリティ・アーキテクチャの必要性

これら課題・特性を踏まえ，企業が自社に合致した情報セキュリティ活動を維持していくためには，情報セキュリティに関わる様々な活動要素を体系化，標準化した枠組みを整備し，企業戦略の一部として実行していくことが必要である．リスク評価から導き出される情報セキュリティポリシーを中心としたセキュリティ教育，監査といった管理的な手法（PDCA サイクル）と，標準化されたセキュリティ技術を自社の情報システムに適用していくための手法をミックスさせ，全体最適の視点で自社のセキュリティ活動を統制するための枠組みを定めなければならない.

これらのことから，エンタープライズ・セキュリティを維持するためには，情報セキュリティ活動の全体統制を図るための戦略的な枠組み（エンタープライズ・セキュリティ・アーキテクチャ）の構築が不可欠となるのである.

3.　エンタープライズ・セキュリティ・アーキテクチャの全体構造

図 1 は，エンタープライズ・セキュリティ・アーキテクチャの全体構造を示したものである．本章では，エンタープライズ・セキュリティ・アーキテクチャの構成要素について概説する.

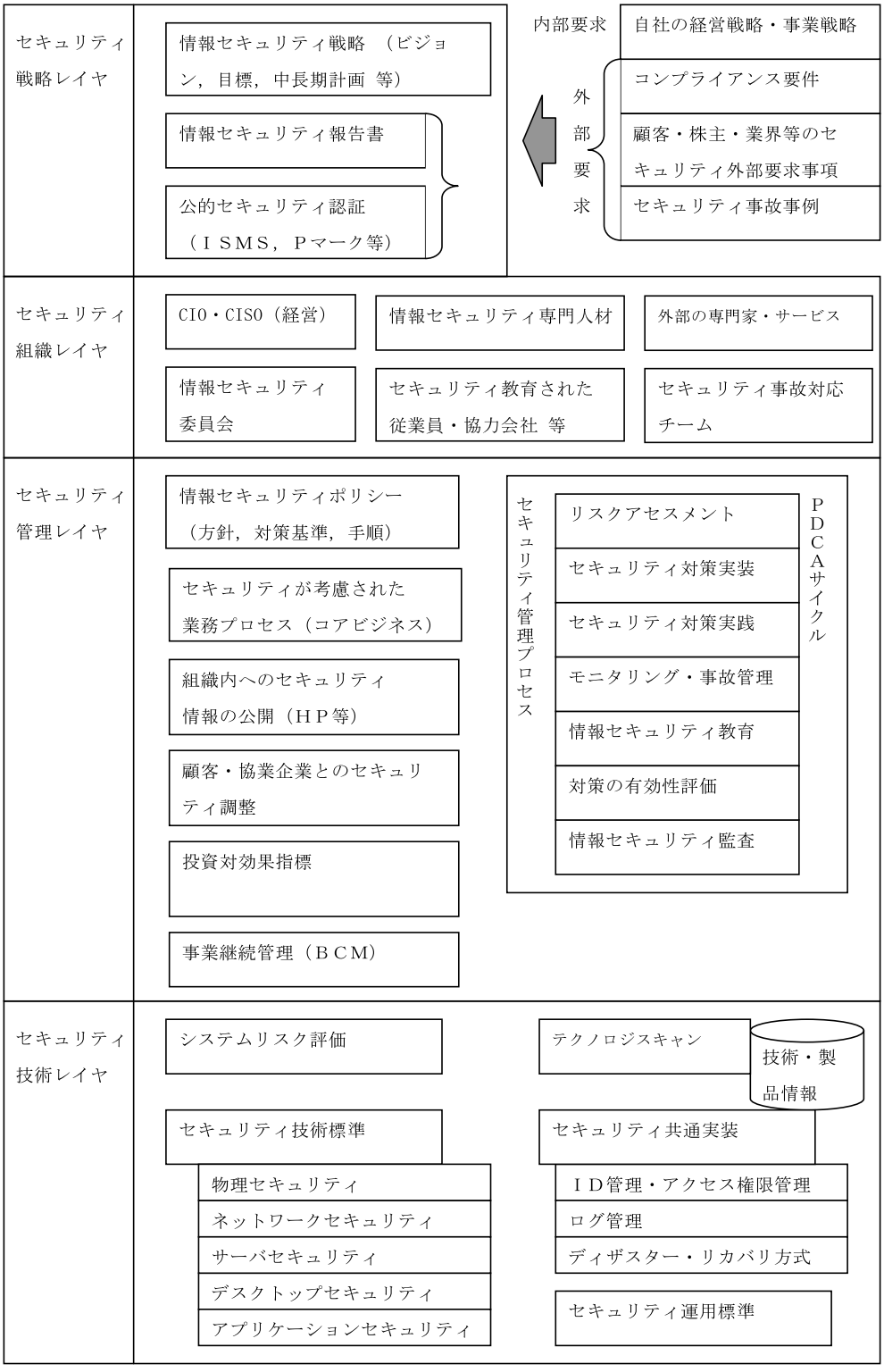

図１　エンタープライズ・セキュリティ・アーキテクチャの全体構造

3.1　セキュリティ戦略レイヤ

セキュリティ戦略レイヤは，情報セキュリティ戦略，情報セキュリティ報告書，公的セキュリティ認証から構成されている．情報セキュリティに対する様々な要求事項を分析し，企業戦略の一部として情報セキュリティ活動を実践していくための中長期戦略，公的認証の取得により企業の情報セキュリティが第三者の評価を受けること，顧客，株主等のステークホルダに対してその活動内容を公開していくことなどの要素が含まれる．

1)　情報セキュリティ戦略

情報セキュリティ戦略は，エンタープライズ・セキュリティを維持，継続する上で根幹となるものである．内部要求である自社の経営戦略，事業戦略の一部であるとともに，外部要求であるコンプライアンス要件，顧客・株主・業界のセキュリティ外部要求事項や，事故事例に対する対策要求事項に基づくものである．情報セキュリティポリシーの上位に位置し，経営陣の承認のもと経営戦略の一部として全従業員にその内容が周知される．

2)　情報セキュリティ報告書

情報セキュリティ報告書は，自社の情報セキュリティ戦略の取り組みや成果を内外に示すものである．一般的にコスト要因と捉えられることが多い情報セキュリティの活動を顧客，株主等のステークホルダに対して情報公開することにより，企業価値を高める目的も持つ．

3)　公的セキュリティ認証

情報セキュリティ戦略に基づき実施されている対策に対して，客観的評価を得る必要がある場合に利用されるのが，公的セキュリティ認証制度である．ISMS やプライバシーマークの認証を取得する．認証の取得により，ある一定レベルの情報セキュリティが維持されていることを顧客，株主等のステークホルダに対して示す目的も持ち，公的認証の取得がビジネス参入の条件となるケースもある．

3.2　セキュリティ組織レイヤ

セキュリティ組織レイヤは，情報セキュリティ戦略に基づき，セキュリティ対策を実施する組織，人材から構成される．情報セキュリティ戦略の実践に責任を持つ経営陣，全社横断の情報セキュリティ委員会，セキュリティ技術や監査の専門性を備えた情報セキュリティ専門人材，セキュリティ事故発生時の緊急対応チーム等の要素が含まれる．

1)　CIO，CISO

CIO（Chief Information Officer：最高情報責任者），CISO（Chief Information Security Officer：最高情報セキュリティ責任者）は，経営者の立場で，情報セキュリティ戦略の立案，実施に責任を持ち，情報セキュリティ委員会からの報告を承認する．経営陣における情報セキュリティ活動に対する理解，推進力は重要な成功要因である．

2)　情報セキュリティ委員会

情報セキュリティ委員会は，情報セキュリティ戦略に基づく各種施策を立案し，実施する．情報セキュリティ活動は多岐に渡るため，情報セキュリティ委員は情報システム部門だけでなく，人事，総務，営業等の各部門から選任し，横串組織として情報セキュリティを実践するための中心的な役割を担う．

3)　情報セキュリティ専門人材

CIO，CISO，情報セキュリティ委員会に対して，専門家としての助言，支援を行う．情

報セキュリティ専門人材は，システム技術，監査，管理等の特性が異なるスキルが要求される上，コミュニケーション力，折衝力等のヒューマンスキルも必要である．前述の情報セキュリティ委員会のメンバーは情報セキュリティの専門スキルを充分に保有していないケースが多いため，専門家による支援は情報セキュリティ活動を推進する上で重要な成功要因となる．

4） 従業員

情報セキュリティ戦略に基づく教育を受けた従業員であり，実際に各種施策を実施する．派遣要員，協力会社要員を含める場合がある．

5） 外部のセキュリティ専門家やサービス

前述の情報セキュリティ専門人材を設置することが困難である場合，あるいは不足領域がある場合に，外部のセキュリティ専門家やサービスを利用する場合がある．但し，外部の専門家やサービスへの過度な依存は自社の情報セキュリティ活動の自主的推進力を失う要因になる恐れがあるため，利用にあたってはその目的等について充分な検討が必要である．

6） セキュリティ事故対応チーム

企業活動の継続に支障を与えるような重大なセキュリティ事故が発生した場合，事故原因の追究，ステークホルダへの情報公開等の対応，再発防止策の計画と実施等の緊急対応を実施するための特別チームである．これらの対応にはより専門的なスキルを要するため，日頃からの対応訓練やスキルの習得により，迅速な対応を可能とし，セキュリティ事故の影響から企業価値を守る役目を果たす．

3.3 セキュリティ管理レイヤ

セキュリティ管理レイヤは，情報セキュリティ委員会で決定された各種施策の実体である．セキュリティ管理レイヤの中心は，セキュリティマネジメントシステムにおける情報セキュリティポリシーと継続性維持のためのセキュリティ管理プロセス（PDCA サイクル）であり，セキュリティ関連の規定により文書化された管理の仕組みが全従業員に公開，教育される．また，セキュリティ管理は独立したプロセスであるとともに，自社の重要なビジネス領域の業務を規定したプロセスの中に埋め込まれた形態で実践する方式がある．

1） 情報セキュリティポリシー（方針，対策基準，手順）

情報セキュリティ戦略を実現するための方針や，普遍性の高い対策基準，実施手順を定めた文書群である．セキュリティ管理プロセスにおけるリスクアセスメントの結果により定期的な見直しを実施し，陳腐化を防止することが必要である．

2） セキュリティ管理プロセス

情報セキュリティポリシーによって定められた方法で，自社のリスクアセスメントを行い，セキュリティ対策の実行，監査，見直しを行う．一般的に PDCA サイクルの各工程に沿った実運用を定義し，一定期間で継続的に実施する．前述の公的認証の取得にあたっては，認証制度により実践の枠組みが規定されており，最も重要視されている部分である．

3） セキュリティが考慮された業務プロセス

実践する情報セキュリティ対策を業務プロセスの中に組み込むことで，セキュリティ対策の実施を確実にする．特に企業の重要業務に合わせて適切なプロセスを策定すれば，情報セキュリティ対策の実施とその有効性をより確実なものにすることができる．

4)　組織内へのセキュリティ情報の公開

セキュリティに関する情報を企業内へ公開するための仕組みを構築する．従業員に継続的な意識向上を促し，事故発生を予防する．一般的にセキュリティポータルサイト等の情報公開サイトを社内イントラネット上に構築し，情報セキュリティ戦略や情報セキュリティポリシーの公開，E ラーニングによるセキュリティ教育の実施等に活用する．

5)　顧客・協業企業とのセキュリティ調整

企業を跨る他社とのビジネス協業や，顧客へのアウトソーシング型サービスの提供にあたり，情報セキュリティに関する調整を実施する機能が必要である．保有する情報資産の価値に関する見解の違いや，セキュリティ対策レベルに相違が発生した場合に，自社および他社のセキュリティ対策に関する調整と合意を行うことにより，ビジネス協業や顧客サービスの安全性を確保する．

6)　投資効果の測定

情報セキュリティに関する投資に対する効果を定量的に測定し，最適な投資を継続的に行うことを目的とする．情報セキュリティの大きな課題である「投資効果の不透明さ」に対する回答として，投資効果を定量化し，経営陣への説明や従業員への公開に活用することは，情報セキュリティの継続性を保つために重要な意味を持つ．

7)　事業継続管理

事業継続に関する監視と管理を行う．情報資産に対するリスク管理である情報セキュリティを超えたリスクを扱う部分が含まれているが，実践する管理プロセス等で情報セキュリティとの共通点も多いため，情報セキュリティ戦略の一部として扱うことが有効である．

3.4　セキュリティ技術レイヤ

セキュリティ技術レイヤは，自社で使用する情報システムが保持すべき技術的セキュリティ対策に関する統制を行うレイヤである．情報セキュリティポリシーの下流の対策として実装，運用されるものであるが，適用するセキュリティ対策の選択肢が多く，利用技術の変化も非常に早いため，適用にあたっては情報システムのセキュリティ対策に特化した統制の仕組みを考慮しなければならない．

1)　システムリスク評価

セキュリティ管理プロセスにおけるリスクアセスメントでは情報セキュリティの網羅的なリスクの評価を行うことに主眼が置かれるため，個別の情報システムに対して必要とされる技術的セキュリティ対策のレベルを導出することは難しい．個々の情報システムの重要度や保有する情報資産の価値に応じて，各情報システムのリスクを個別に評価することにより，適用する技術的セキュリティ対策の検討，選定を行う．

2)　セキュリティ共通実装

自社の情報システムで，共通に使用する技術的セキュリティ対策を実装したものである．共通実装基盤を利用することにより，情報システムに対して特に重要な部分のセキュリティ対策の実装や運用の負担を軽減するとともに，統制の取れた情報システムの実現を図る．ID 管理，アクセス権限管理，ログ管理，ディザスタリカバリ対策などがこれに該当する．重要なセキュリティ対策を複数の情報システムで共通利用することにより，実装，運用コストの低減化を図ることができる．

3） セキュリティ技術標準

セキュリティ管理レイヤの情報セキュリティポリシーの下位規定として，情報システムが保持しなければならない情報セキュリティに関する技術的要件を，あらかじめ定めたものである．入退管理やセキュリティ区画等を定めた物理セキュリティ，ファイアーウォールの実装や配置等を定めたネットワークセキュリティ，オペレーティングシステムのセキュリティ設定等サーバ上に実装するサーバセキュリティ，コンピュータウイルス対策やモバイルPCの暗号化，セキュリティパッチの適用等クライアントPCに実装するデスクトップセキュリティ，稼働するアプリケーションプログラムにセキュリティホールを作らないためのセキュアプログラミング技法等のアプリケーションセキュリティといった分類が挙げられる．

前述のシステムリスク評価の結果により，これらセキュリティ技術標準で規定されたセキュリティ対策を情報システムに対して確実に適用する．

4） セキュリティ運用標準

実装した技術的セキュリティ対策の多くは，適切な運用を実施しないとセキュリティ対策の効果が半減してしまうケースが多い．実装した技術的セキュリティ対策を有効に機能させるためには，セキュリティ運用標準を定めることが必要である．セキュリティ対策が発する事故通知に基づく監視やセキュリティログの定期チェックといった運用が挙げられる．但し，過剰なセキュリティ運用の実施はシステム部門の運用負荷を著しく増加させる恐れがあるため，運用項目の取捨選択が必要である．

5） テクノロジスキャン（技術・製品情報）

情報システムに適用できる技術的セキュリティ対策の選択肢は非常に多く，技術の進化等による変化が激しい．従って，セキュリティ技術標準で規定した技術的セキュリティ対策を陳腐化させないために，定期的な情報収集と自社で適用する可能性があるセキュリティ技術についての評価（テクノロジスキャン）が必要となる．また，技術的セキュリティ対策としてセキュリティ製品を使用している場合，当該製品の販売停止やサポート停止といった製品リスクについても，早期の情報収集により製品の変更，ソフトウエアのバージョンアップ等の対応を検討する必要がある．

4. 実践のためのポイント

エンタープライズ・セキュリティを効果的に持続するのは容易なことではない．まず，3章で述べたエンタープライズ・セキュリティ・アーキテクチャの構成要素の中から自社に必要とされる要素を選択し，その実装内容を充分に検討する必要がある．すべての構成要素がそろっていない場合は，その構築，あるいは，代替措置を講ずる必要がある．その上で，効果的に運用するためには，個々の構成要素間の依存関係に着目し，構成要素間の関連に留意する必要がある．本章では，各レイヤにおける施策実践のためのポイントを述べる．

4.1 セキュリティ戦略レイヤ

エンタープライズ・セキュリティを実践する上で，最も重要となるのは，情報セキュリティ戦略である．前述のとおり，情報セキュリティ戦略は，自社の経営戦略，事業計画の一部である必要がある．これは，経営の意思として社内外に対して明確に示されなければならない．実際の各種施策を実施するのは従業員である．従業員に高い意識を持たせ，継続的に実施させる

ためには，情報セキュリティの実践が業務の一部であるという意識付けを行う必要がある．

戦略の立案にあたり，長期的戦略はある程度普遍的なものにする必要があるが，短期的な戦略については，その見直しをできるだけ頻繁に行うべきであり，見直しを躊躇すべきではない．経営戦略や事業戦略に影響されるのはもちろんだが，情報セキュリティに関するさまざまな事象を観察し，戦略の見直しが必要な局面では即座に対応すべきである．

また，情報セキュリティ戦略に織り込む内容が外部からのセキュリティ要求にいかに対応しているかを明確にし，情報セキュリティ活動の目に見えるアウトプットである公的セキュリティ認証や情報セキュリティ報告書が自社のビジネスに与える効果や影響についても，情報セキュリティ戦略の中で記述するべきである．更に，エンタープライズ・セキュリティ・アーキテクチャにおける組織レイヤ，管理レイヤ，技術レイヤの実施状況を評価した上で短期，中期，長期の戦略として策定することが望ましい．

4.2　セキュリティ組織レイヤ

情報セキュリティ戦略を実行に移すためには，社内のすべての従業員が，それを理解して行動する必要がある．そのためには，施策を推進する責任者を明らかにし，施策推進を担う情報セキュリティ委員会の役割と責任を明確にするべきである．また，情報セキュリティの施策を有効なものにするためには，次のような，役割に応じた教育や人材の育成が必要である．

・全従業員向けセキュリティ教育（経営者，一般職員）
・運用スペシャリスト教育（定常対応，インシデント対応）
・業務に特化したセキュリティ教育（セキュアプログラミング，個人情報取扱者など）

また，エンタープライズ・セキュリティでは，情報セキュリティ事故に対する対応を怠ってはならない．情報セキュリティ事故が発生することを前提にした対策が必要である．一般的に，情報セキュリティ事故が発生した場合，なんらかの業務停止は避けられない．事故原因の調査，対策に時間がかかればかかるほど，経営に及ぼす影響は大きくなる．当事者企業だけに留まらず，顧客，取引先企業，さらに社会全体に影響を与えることもある．事故原因の調査，対策にかかる時間を最小限にするためには，事故発生時の対応組織と対応手順を明確にしておくことが必要である．事故の程度，種類によっては，外部の専門家やサービスを利用することが効果的な場合もあるので，そういった調査を行っておくことも重要である．

情報セキュリティ専門人材の育成は，継続的な情報セキュリティ活動を行う上で重要な成功要因であり，自社の人材育成計画の一環として組み込まれるべきである．情報セキュリティ専門人材には様々な種類のスキルが必要とされるため，全てのスキルを保有するスーパー人材を育成することは極めて難しい．エンタープライズ・セキュリティ・アーキテクチャの構成要素の遂行に必要とされるスキル定義に基づき，自社に必要な情報セキュリティ専門人材を定義し計画的な育成を図ることが必要である．また，情報セキュリティ組織についても，エンタープライズ・セキュリティ・アーキテクチャの構成要素に基づき，その役割と配置を定めることが必要である．

4.3　セキュリティ管理レイヤ

セキュリティ管理レイヤでは，情報セキュリティポリシーに基づき，実際に対策を実行する部分が含まれる．通常，情報セキュリティ対策の実行は，業務プロセスの中に組み込まれた状

態で実施されるのが一般的である．業務プロセスは，経営戦略，事業戦略を実行するために効果的でなければならないが，情報セキュリティポリシーによる対策の実施により，業務効率が下がることがある．このことは，経営戦略，事業戦略に影響を与えるばかりでなく，情報セキュリティ対策の実行にも悪影響を及ぼす可能性がある．従業員の意識によっては，業務効率を優先する傾向になりがちだからである．そのため，セキュリティ管理レイヤでは，業務プロセスと情報セキュリティ対策のバランスを，常にモニタリングしておく必要がある．本レイヤで最も重要な構成要素は，情報セキュリティポリシーとセキュリティ管理プロセスであり，完全な文書化と教育により，情報セキュリティの PDCA サイクルを確実に実践することに尽きる．特に，公的セキュリティ認証を取得している企業であれば，認証基準に準拠したセキュリティ管理プロセスの実践は，当然の義務である．

また，このレイヤでは，自社以外の組織との接点がある場合の，対策レベルを調整する機能が含まれる．言い換えれば，エンタープライズ・セキュリティ間のゲートウェイ機能である．組織が異なれば，情報資産の価値感や，対策方法などが異なることが予想される．この場合，お互いのエンタープライズ・セキュリティを尊重した上で，自社エンタープライズ・セキュリティを維持しなければならない．情報システムで実現することもあれば，その業務に携わる人の運用で実現することもある．適切な方式で実現されているか，適切な運用がされているかをモニタリングする必要がある．他社との協業をベースとしたビジネスの拡大はもはや一般的なことであり，情報セキュリティについても企業間の調整を実施する機能を持つことが必要とされる．具体的には，相手企業と情報セキュリティの調整を図るためのプロセスを定義し，必要なテンプレート類を用意することになるが，自社の情報セキュリティポリシーを押し付けることではなく，企業間での取引や情報システムの連携におけるリスクの評価に基づき，お互いに合意できるレベルに調整することが重要である．

4.4　セキュリティ技術レイヤ

セキュリティ技術レイヤは，情報システムに関わる包括的な対策と，個別システムの種類により選択される対策を合わせたものである．包括的な施策は，情報セキュリティ戦略の重要な目標をブレークダウンしたものであり，セキュリティ共通実装としてあらかじめ実装しておくことで対策の徹底が図られる．しかし，情報システムは多種多様であり，機密性の高い情報資産を扱うシステムや，そうではないシステムもある．これらに対して，すべて均一の対策を実施することは，コストや運用負荷の面で望ましくない．そのため，個別システムの種類によって，可能な対策方法を選択できるようにしておくことが望ましい．セキュリティ管理レイヤのセキュリティ管理プロセスに含まれる包括的なリスクアセスメントと連動し，保有する情報システムを対象に定期的なシステムリスク評価を行い，適用されている技術的セキュリティ対策の妥当性を確認するとともに，新規で情報システムが追加される場合にもシステム開発の一環としてシステムリスク評価を実施し，技術的セキュリティ対策の実装を確実にする必要がある．適用する技術的セキュリティ対策は，システムリスク評価の結果として導出されるセキュリティ要求レベルに応じてあらかじめ選択，評価を行っておき，セキュリティ技術や製品の定期的なテクノロジスキャンによりその陳腐化を防止する必要がある．また，適用する技術的セキュリティ対策に対応するセキュリティ運用標準を定め，セキュリティ対策の効果を持続させるために必要な運用機能を実装する．

5. おわりに

本稿では，エンタープライズ・セキュリティを効果的に維持するための方法として，その構成要素をエンタープライズ・セキュリティ・アーキテクチャとして整理し，実践のためのポイントを述べた．多くの企業が情報セキュリティに関する何らかの戦略を策定し，実践していることは，まぎれもない事実ではあるが，維持・継続する難しさを実感しているのもまた事実であろう．その多くは，断片化された施策がうまく統合できずに，運用の負荷が増大していることに起因しているとの仮説を立て，本稿を著するに至った．同じような問題を抱えている方の参考になれば幸いである．

日本ユニシスグループにおいても，経営戦略の一環として情報セキュリティ戦略が組み込まれて数年経過し，従業員の意識もはっきりと変わってきているが，ひとりひとりの意識の方向が，同じ一点に向いているとは言いがたい．今後も，変化し続ける情報セキュリティを取り巻く情勢に敏感に反応し，効果的なエンタープライズ・セキュリティを実践していく所存である．

参考文献
［1］ 情報技術と経営戦略会議〈提言〉，経済産業省，2003 年 10 月
［2］ 企業における情報セキュリティガバナンスのあり方に関する研究会報告書，経済産業省，2005 年 3 月
［3］「JIS Q 27001：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」，日本規格協会，2006 年 5 月
［4］「JIS Q 27002：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の実践のための規範」，日本規格協会，2006 年 5 月
［5］「情報セキュリティ管理基準」，経済産業省，2003 年 4 月
［6］「政府機関の情報セキュリティ対策のための統一基準（第 3 版）」，内閣官房情報セキュリティセンター，2008 年 2 月

執筆者紹介
遠　藤　英　幸（Hideyuki Endo）
1987 年日本ユニシス(株)入社．オブジェクト指向言語および実行環境の開発，アウトソーシング基盤構築，セキュリティ監視などを担当．現在，共通利用技術部システム管理技術室セキュリティグループマネージャ．CISSP．情報処理技術者試験委員．