日本ユニシスにおけるエンタープライズ・セキュリティ・アーキテクチャ(ESA)

平岡 昭良
日本ユニシス(株)

これまでのセキュリティ対策は効率性，利便性を犠牲にした過度なセキュリティ対策に陥るケースが多かったが，今後は欧米企業と同様，バリューチェーン全体のビジネスリスクを見定めて，ビジネスプロセスにセキュリティ対策を埋め込んでいく必要がある．本稿では，自社の経営戦略や外部からのセキュリティ要求との整合性を保った上で，管理および技術面のバランスがとれた情報セキュリティ活動を実践していくための体系的な枠組みとして「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，アーキテクチャの構成要素，および構成要素間を効果的に連動させ情報セキュリティ活動を統制する上でのポイントを考察する．また，日本ユニシスグループでの取り組みを踏まえ，適用上の課題，今後の方向性についての見解を紹介する．

企業の情報セキュリティに対する社会的要請の変化とESA

相次ぐ情報漏えい事件と，2005年4月の個人情報保護法の全面施行により，情報セキュリティに対する社会の関心や認識は高まり，それにともなって企業の情報セキュリティへの取り組みに対する社会的要請が強まってきている．

さらに加えて，金融商品取引法（J-SOX法）の施行により，コンプライアンスや内部統制も一層求められるようになり，企業の社会的責任という観点から，企業には適法性と適正性の遵守，透明性や情報開示を求める声が高まり，リスクなどの情報開示，説明責任が求められるようになってきている．社会的責任を考慮した，情報資産の有効活用と管理の高度化，事業継続対応など，ますます多岐にわたる取り組みが必要となってきている．

一方で，情報セキュリティ対策を過剰に優先させるあまり，モバイルPCの使用禁止など，せっかくのICT（情報通信技術）の利便性を犠牲にせざるを得ないケースや，運用負荷の増大や情報共有・交換の制限など，業務の効率性を阻害するケースも増えてきている．情報セキュリティ対策を年々厳しくしてきた結果，企業のICT鎖国，ガラパゴス化といった現象が生じてきた．

グローバル化の波は，閉じた組織，企業から競争力を奪うと言われている．ICTをビジネス基盤として利活用することで，グローバルレベルでの横断的な情報共有・活用を図り，企業が持つバリューチェーンの最適化を図ることが競争力につながることになる．単純に情報セキュリティを強化するだけではなく，企業グループを超えたオープンなサプライチェーンや顧客サービスの強化に，いかにセキュリティ対策を組み込み，競争力を高めていくかが問われている．

また，近年，ワーク・ライフ・バランスが注目を集めるようになってきている．人材を確保するための福利厚生という狭い観点ではなく，働き方や働く環境，いわゆるワークスタイルの変革が企業の競争優位と社員の仕事と生活の調和をもたらすという考え方だ．テレワーク（在宅勤務）やモバイルワークが代表的な手法だが，制度と職場の風土，それを支えるICTの環境，特に十分な情報セキュリティ対策がないと実施できない．

本稿では，企業が戦略的に情報セキュリティに取り組むためのフレームワークとなるエンタープライズ・セキュリティ・アーキテクチャ（ESA）の全体構造，アーキテクチャの構成要素を示し，その構成要素間を効果的に連動させ情報セキュリティ活動を統制するポイントを考察する．また，実際の日本ユニシスグループの取り組み事例と，それを踏まえた運用上の課題，今後の方向性についての見解を紹介する．読者の一助になれば幸いである．

企業における エンタープライズ・セキュリティの課題

前述したような環境変化が加速する中で，企業が情報セキュリティ管理を継続的に維持していく重要性はますます高まっていくであろう．しかしながら，情報セキュリティが持つ特性，特に「多様性と変化」「運用負荷（業務効率の低下）」「投資対効果の不透明さ」が，さらに情

報セキュリティ管理を困難なものにしていく可能性は否定できない．

- 多様性と変化により，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，およ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きわめて広範囲にわたること．また，企業が遵守すべき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，プロセス，情報資産，コンピュータウィルスや不正アクセス手法等のセキュリティリスクとその対策技術の要素が非常に短いサイクルで変化すること．
- 運用負荷により，過剰なセキュリティ対策の実施による，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．
- 効果の不透明さにより，実施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困難であること．

これらの特性を踏まえ，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かかわるさまざま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．

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，そこには，推進する立場と対策を実施する立場の両面での課題がある．危機意識の低下も，推進力を妨げる一因となる．

漸次，セキュリティ対策を追加しているとはいえ，総合的な対策には及ばず，場当たり的な対策にとどまっている企業も多いのではないだろうか．また，ISMS（情報セキュリティマネジメントシステム）☆1とプライバシーマーク（個人情報保護）☆2の運用もそれぞれでなされているというのが実情ではないかと推察される．

全体最適な視点で，情報セキュリティ管理を経営戦略や社会，取引先などからのセキュリティ要求と整合性が保たれた状態で統制していく必要がある．リスク管理，ポリシー，管理の仕組み，技術面の対策，人的対策，BCP（事業継続計画），コンプライアンス，効果測定などを体系的な枠組みとして捉えるESAによる活動が求められる時代になりつつある．

☆1 ISMS：組織が，情報セキュリティリスクを管理し，継続的にリスクの回避や軽減ができるマネジメントシステム．
☆2 プライバシーマーク：個人情報保護に関して一定の要件を満たした事業者について，（財）日本情報処理開発協会により使用を認められる登録商標．
☆3 Security and Privacy Profile for the Federal Enterprise Architecture（FEA SPP）：米国連邦政府の各省庁で共有する情報の保護についてのガイドライン．
☆4 NIST（米国国立標準技術研究所）が公布する情報セキュリティ施策実施のための文書（SP800シリーズ）の1つ．

日本ユニシスが提唱するESA

ESAは，このようなセキュリティに関する多面的な取り組みを対象としている．一般にESAといわれるものには，システムセキュリティ・モデル，コモンクライテリア（ISO 15408）やBS 7799/ISO 17799などの各種標準，FEA SPP☆3など多数のセキュリティガバナンス・モデル，NISTのセキュリティ・サービスモデル☆4などがある．

日本ユニシスのESAは，セキュリティガバナンス・モデルの1つである．セキュリティガバナンス・モデルは，企業組織や企業文化にセキュリティ関連活動を結合させることを目的としている．そのため，このモデルは企業構造や，ビジネス・ニーズと自社のセキュリティ能力の適合度から出発し，情報セキュリティを企業全体にわたって義務付け，実行し，管理するという問題（セキュリティガバナンス）を解決することに注力する．先に述べたように，情報セキュリティ対策を実施していく上での最大の課題は推進力をいかに維持していくかという点であると捉えているため，日本ユニシスのESAはこのモデルを採用している．

セキュリティガバナンス・モデルは多数提唱されているが，ガバナンスモデルであるため共通して，ポリシー策定とセキュリティ施策の実施がそれぞれ，集中して行われるか，分散して行われているかに着目している．そこで，日本ユニシスのESAは，ポリシーを定めて義務付けていくための組織構造と，実行させ管理していく管理の仕組みを2つの柱として考え，その前提となるセキュリティ戦略と，情報システムに埋め込まれる技術と併せ，ESAを4つのレイヤ（セキュリティ戦略レイヤ，セキュリティ組織レイヤ，セキュリティ管理レイヤ，セキュリティ技術レイヤ）で構成し，個々のレイヤに含まれる構成要素を定義している（**図-1**）．

基本的な考え方は，ESAを定めることがすべての出発点であり，そこから企業の情報セキュリティの品質を決定するということである．そして，ESAから導かれる制約条件に基づいてセキュリティ要求レベルを決定し，この要求レベルを企業が自社のセキュリティ品質を具体的に評価するための基準とする．

ESAの起点は，経営のセキュリティへの関与である．どのように企業戦略と情報セキュリティが関連するかを表明したものが「情報セキュリティ戦略」であり，セキュリティ戦略レイヤで定める．

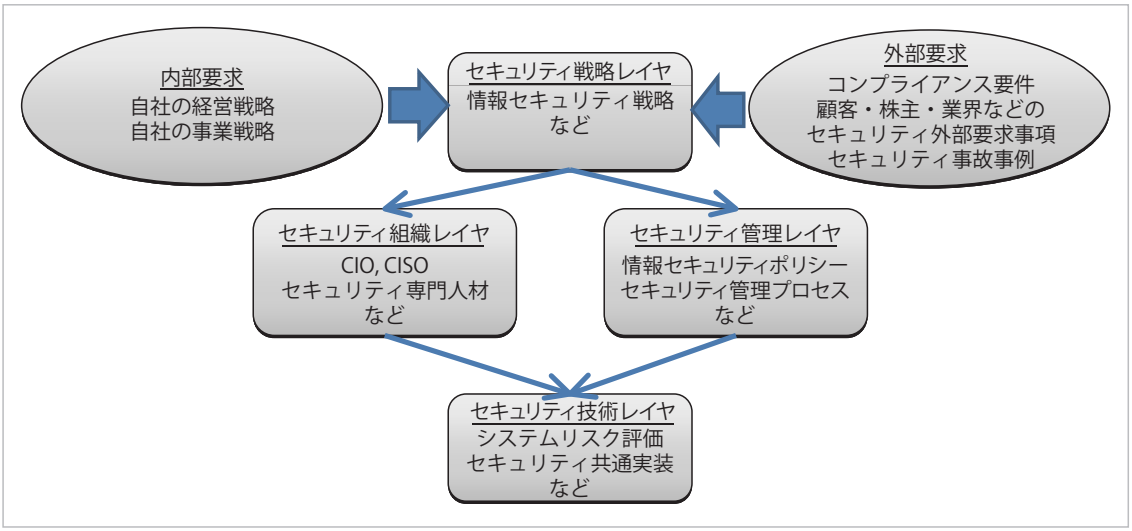

図-1　エンタープライズ・セキュリティ・アーキテクチャの概要

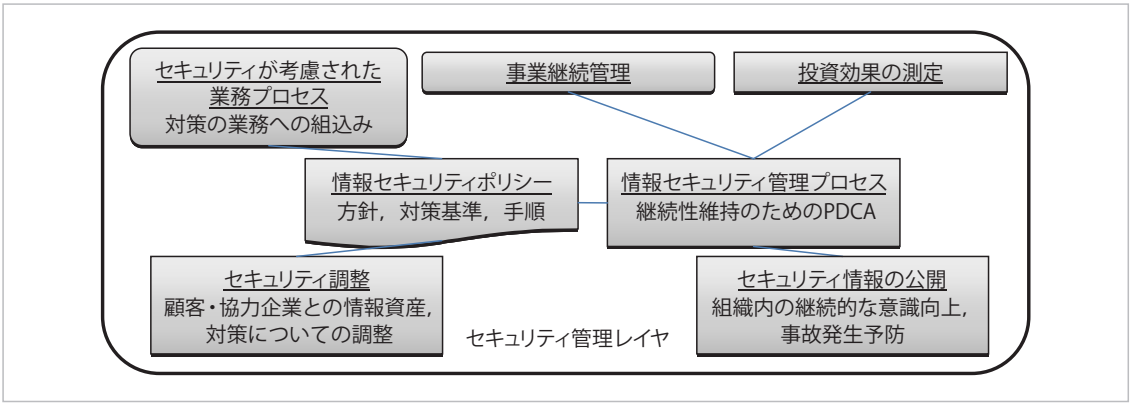

図-2　セキュリティ管理レイヤ

セキュリティ管理レイヤでは，情報セキュリティにかかわる包括的な施策（セキュリティ技術レイヤ）を定めるため，「情報セキュリティ戦略」（セキュリティ戦略レイヤ）の重要な目標を詳細化する（**図-2**）．これがESAから導かれる制約条件の内容となる．

この制約条件は，セキュリティ技術レイヤ（**図-3**）の要件となる．包括的な施策を徹底するには，「セキュリティ共通実装」（セキュリティ技術レイヤ）として要件を定め，共通基盤として提供することが望ましい．しかし，実際には，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，そうでないシステムもある．これらに対して，すべて均一的な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対策や方法を選択できるようにしておくことが求められる．

情報セキュリティ対策は，このようにして定められた包括的な方策と個別の選択肢を合わせたものになる．セキュリティ要求レベルは，この対策を「システムリスク評価」（セキュリティ技術レイヤ）で評価した結果として定められる．このリスク評価は，セキュリティと業務プロセス効率とのバランスをモニタリングする「リスクアセスメント」（セキュリティ管理レイヤ）の作業と連動して行われる．

そして，このような関連する活動を継続的に実行するには，役割に応じた教育や人材育成（セキュリティ組織レイヤ）が重要である（**図-4**）．1つは，専門家の育成である．情報セキュリティ人材にはさまざまなスキルが必要とされるため，すべてのスキルを持つスーパー人材を育成することはきわめて難しい．ESAの構成要素に必要なスキル定義に基づいて，自社に必要なセキュリティ人材を定義し，人材育成計画に組み込んで育成を図ることが重要である．もう1つは，非専門家への教育である．他のガバナンス施策と同様に，情報セキュリティは，経営者の立場で情報セキュリティの立案，実施に責任を持つCIO（最高情報責任者）やCISO（最高情報セキュリティ責任者）の熱意と，情報セキュリティの各種施策を業務の一部として実行する従業員の高い意識に支えられることが望ましい．経営者や従業員の多くはセキュリティの専門家ではないので，意識づけを中心とした教育が重要となる．

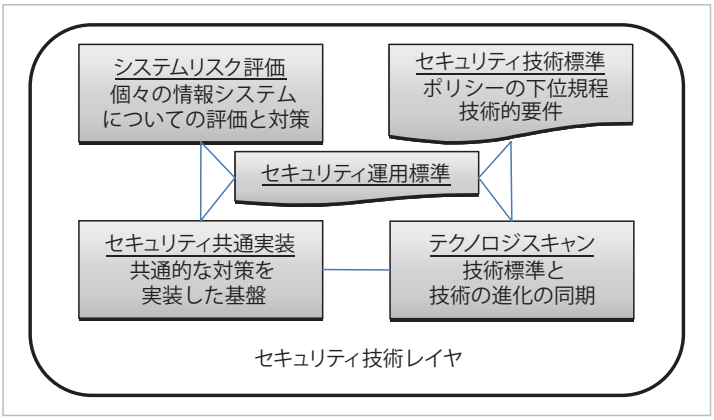

図-3　セキュリティ技術レイヤ

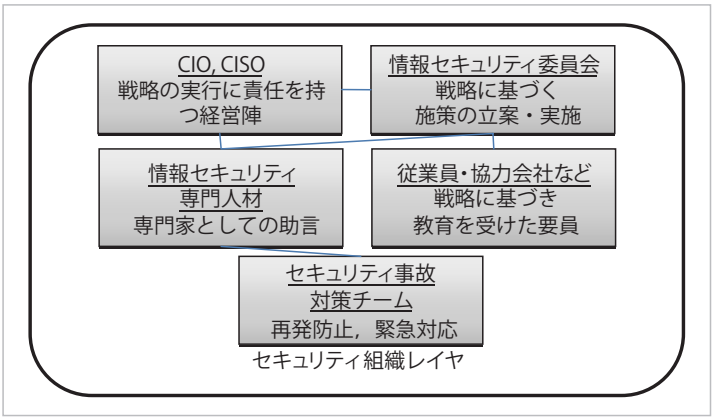

図-4　セキュリティ組織レイヤ

以下では，この日本ユニシスのESAモデルを適用した実例として，日本ユニシスグループ（以下，当社）における情報セキュリティへの取り組みを紹介する．当社のセキュリティガバナンスの型は，ポリシーの策定も，施策の実行・管理も，CIO/CISOに集中した一体型である．

ESAの適用事例

当社のESAの適用事例について，前章で紹介した4つのレイヤ（セキュリティ戦略レイヤ，セキュリティ組織レイヤ，セキュリティ管理レイヤ，セキュリティ技術レイヤ）の構成要素に従って，その取り組みを以下に紹介する．

◆セキュリティ戦略レイヤ

セキュリティ戦略レイヤは，情報セキュリティに対するさまざまな要求事項を分析し，企業の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を策定するとともに，公的認証取得により情報セキュリティが第三者評価を受けること，顧客，株主等のステークホルダに対してその活動を公開することが必要とされる．

当社では，自社の経営戦略，事業戦略を踏まえた上で，「情報セキュリティ総合戦略」として戦略策定し実践中である．2004年に策定した「第一次情報セキュリティ総合戦略」は，情報セキュリティに関して単に「守り」の視点からの対応のみならず，技術・ノウハウを活かし企業の情報セキュリティの高度化を実現し，生産性向上およびコスト削減等「攻め」の視点を定めた．その後，2年ごとに，経営戦略の変化，セキュリティ外部要求事項の変化，セキュリティインシデントの変化等を的確に捉え，見直しを実施している．昨年，「情報セキュリティ総合戦略2008」を策定，キーワードを「攻め」と設定し，企業グループの枠組みを超え，オープンなサプライチェーンや顧客サービスのさらなる強化を行い企業競争力を高めるための活動を2年計画で推進中である．

これら情報セキュリティへの取り組みを，顧客，株主等のステークホルダへ公開するために，毎年発行される当社「CSR報告書」にて公開している．

公的認証取得については，ISMS（ISO 27001）やプライバシーマークの認証取得を「総合セキュリティ戦略」で取得計画を定め，グループ全社が認証取得すべく推進中である．すでにISO 27001は全グループ企業で取得済みであり，プライバシーマークについても年内に全企業取得予定である．

◆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を実践する組織から構成される．セキュリティの実践に責任を持つ経営陣であるCISO，CPO（最高個人情報保護責任者），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必要とされる．

当社では，CISOのもとに「総合セキュリティ委員会」が組織されている．同委員会は当社の最高意思決定機関と位置付けられ，情報セキュリティ戦略に基づく各種施策の承認を行う．実施する情報セキュリティ活動は多岐にわたるため，情報システム部門のみならず，営業，システム，経営企画，人事，法務等の各部門長で構成され，迅速な意思決定と情報セキュリティを実践するための中心的な役割を担っている．

情報セキュリティの各種施策の立案および推進を実施する情報セキュリティ専門部隊は，2004年の「第一次情報セキュリティ総合戦略」を開始した時点で，50名の専門部員で新たな組織として構成された．ISMSの構築や，内部監査等の実施を同部門が特化して実施して

いる．

セキュリティ事故対応については，企業内にセキュリティ事故対策チームを設置し，事故原因の究明，再発防止のための緊急対応を実施する．これらの対応は，専門的な知識を要するため，このチームはバーチャルな組織として，事故状況に対応して専門家集団による最適な布陣で対応できるように考慮している．

◆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情報セキュリティ管理プロセスであり，セキュリティ規程により文書化された管理の仕組みが全従業員に公開されるとともに教育される必要がある．

当社の情報セキュリティポリシーは，グループ企業共通であり，セキュリティの対策基準や，実施手順を定めた規程類で構成される．毎年実施する情報資産の棚卸や，セキュリティ事故等に基づくリスクアセスメント結果により定期的な見直しを実施し陳腐化を防止している．

「情報セキュリティ総合戦略」の一施策としてISMS日本ユニシスグループ全社統一認証を掲げている．ISMSの管理策やセキュリティマネジメントシステムのフレームを活用することにより，リスクアセスメントを行い，セキュリティ施策を実施し，内部監査，対策の見直しを行うこれらの工程（PDCAサイクル）を，継続的に廻している．

セキュリティにかかわる各種情報は，イントラネット上にセキュリティポータルサイトを構築し全従業員への情報共有を図っている．また，セキュリティ教育については，役員，従業員のみならず，派遣社員，委託先社員に対しても集合教育やe-ラーニングにより定期的な目的別の教育を実施している．

各種セキュリティ施策で技術的な対応を要し投資を伴うものについては，最適な投資であるか第三者の判断を行うためのボードを設置して，定性効果および定量効果の両面で費用対効果が審議され投資費用の最適化を図っている．

◆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をセキュリティ要求に変換し，技術上の対策として実装し，運用する．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．

当社では早くから種々のセキュリティ技術的対策を講じてきていたが，これらはIT分野に限られた対症療法的な対応であった．2004年の情報セキュリティ戦略策定後は，情報セキュリティガバナンスを継続的に維持すべく，戦略に基づく各種対策の策定に際してセキュリティ事故や外部・内部の変動要因を分類整理の上，リスクアセスメントを実施し，その結果に基づいてセキュリティの要求レベルを定め，情報セキュリティポリシーの見直しと改定，その下位規程類である各種管理策の改定，および技術的対応策の決定を統括的に行っている．

具体的には，システムのリスク評価に際しては，全社内システムの重要度や保持する情報資産の価値に応じて，社内システムを層別し，そのレベルに応じた基本的なセキュリティ技術的対策を決定して，個別システムへの適用を実施している．セキュリティ共通実装は，特に重要課題であると認識している．この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や運用負荷を軽減するとともに，統制のとれた情報システム構築を図るべく対応を行っている．具体的には，「情報セキュリティ総合戦略」に着手するまでは，システムの利用者パスワードやアクセス制御・権限情報の保持やパスワード変更，アクセス権付与・剥奪等は，すべて個別業務システムごとに運用されていたため，運用負荷の増大や，セキュリティ統制面でも問題をはらんでいた．これらの問題を解決すべく，個人認証，権限管理，アクセス制御，監査ログ管理等を，セキュリティ共通実装要件として定め，社内システムを一元的に管理するための共通認証基盤（Usagi：Unisys Secure Authentication Global Infrastructure）の構築を実施した．Usagiの導入によりグループ全従業員のユーザID･パスワードを一元管理することで，アカウント統合，ロール管理，シングルサインオン，ログ監視等を実現することが可能となった．結果，新システムへの実装，運用コストの低減化が図れた．

セキュリティ技術標準に関しても，入退室管理やセキュリティ区画を定めた物理セキュリティ，ファイアウォールの実装や配置を定めたネットワークセキュリティ，モバイルPCの暗号化等々，セキュリティに関する技術要件を定め，情報システムに適用している．

また，利便性と安全担保の追求においては，技術的な情報漏えい対策のみならず，グループ各社・各部門が情報共有を安全に行えるための，「シェアードITサービス」を構築し，オンラインストレージ，グループウェア機能を充実させ，USB型認証基盤キーデバイス（SASTIK；**図-5**）の提供により，業務の効率性を阻害しないよう

図 -5　USB 型認証基盤キーデバイス（SASTIK）

対応を実施している．SASTIK は当社の全社員に配布され，ワークスタイル変革に対応すべく，セキュアな環境で「AnyPlace AnyTime」を実現するとともに災害・緊急時の連絡手段，事業継続手段としても有効に機能すると考えている．

ESA の適用に向けて

本稿では当社においての実践を素材として，ESA に基づいて要求を定め，実現していく過程を紹介した．この事例は一体型のセキュリティガバナンスの事例であるが，いくつかの大企業で見られるように企業グループで守るべき共通セキュリティポリシーと，グループ企業各社が個別に定めるポリシーを分けて，施策を進める分散型であっても，この ESA のモデルは適用できる．このモデルの詳細は，ユニシス技報 [2] の特集をご覧いただきたい．

参考文献
1)「第一次情報セキュリティ基本計画」，情報セキュリティ政策会議(Feb. 2006)．
2）ユニシス技報「特集：エンタープライズ・セキュリティ」，日本ユニシス（2008 年 11 月），http://www.unisys.co.jp/tec_info/home.html?num=tr98

（平成 21 年 2 月 2 日受付）

平岡 昭良　▶Akiyoshi.Hiraoka@unisys.co.jp
日本ユニシスにて，営業部門，マーケティング部門などの統括を経て，平成 14 年より日本ユニシス（株）執行役員．現在，同社上席常務執行役員，日本ユニシスグループの CIO（最高情報責任者），CISO（最高情報セキュリティ責任者），CPO（最高個人情報保護責任者）．