エンタープライズ・セキュリティ・アーキテクチャーの策定
ー情報システム部門の立場からのアプローチー

アブストラクト

1. エンタープライズ・セキュリティ・アーキテクチャー出現の背景と研究のアプローチ

昨今、IT 技術の進歩と利用状況の多様化に伴い、個人情報や機密情報の漏洩事故が新聞や雑誌の一面を賑わせており、その事故・事件の手口も巧妙かつ複雑化している。このため、情報セキュリティ対策の必要性が浸透し、ISMS やプライバシーマークの取得を目指す企業も年々増えてきている。一方、IT 技術を駆使した情報セキュリティ対策の進化も目覚しく、情報システムベンダ・セキュリティベンダの製品を組み合わせ、統一されたシステムの構築と運用を行うことが必要となってきている。

しかしながら、ベンダのソフト・ハードの組み合わせにより、安全性が大きく変化するため、最適な情報セキュリティ対策を行うためには、非常に多岐にわたる専門知識やスキルが必要とされる。また、構築するシステムに対しても有効な効果があったかを評価する基準が無いのが現状である。

このような企業における情報セキュリティに対する問題・課題を解決するために、富士通では「エンタープライズ・セキュリティ・アーキテクチャー(以下 ESA)」を提唱しており、この概念に基づき製品・サービスを提供している。

分科会開始当初、ESA に対する参加メンバーの認識はそれぞれ異なっており、研究テーマに対するアプローチが定まらなかったが、富士通 ESA や他社素材を参考に以下の 3 点について研究を行うこととした。

(1) ESA の理解
(2) 企業における ESA 策定手順の確立
(3) ESA の有効性の検証

2. 研究内容･成果

ESA は、企業内における情報セキュリティ対策の技術的な基本方針を明確にする「情報セキュリティのあるべき姿を体系化する」文書である。富士通 ESA は、情報セキュリティ技術を体系的に整理され、それぞれの技術について選定ポイントが詳しく説明されており､非常に理解しやすいものとなっている。

しかしながら、各企業においては、セキュリティポリシーが異なり、またシステム環境が様々であることから、富士通 ESA からは、どの技術をどの機器にどのレベルまで施せばよいのかといった具体的な手順・手法を導き出すことができない。

そこで、本分科会ではユーザ企業の情報セキュリティ対策の指針となる ESA を容易に作成する手法について、研究を進めた｡その結果、分科会メンバーのノウハウを結集し、対象となる情報システムを 18 の要素モデルに分解し、それぞれの情報システムに要求される機密レベルから必要とされる情報セキュリティ対策の基準を明示する「セキュリティ対策ベースライン」を作成するツールを開発した。

さらに､「セキュリティ対策ベースライン作成ツール」と合わせて利用する「ESA ひな型」および「ESA 作成ガイドブック」を作成した。また、分科会参加各社のシステムに対して「セキュリティ対策ベースライン」を使用して、有効性について検証を行った。詳細について、以下に述べる。

(1)「セキュリティ対策ベースライン作成ツール」

ユーザ企業の現状および今後導入される予定の情報システムを 18 の要素モデル(社内利用クライアント／内部用 DB サーバ／内部用 AP サーバ／外部用 DB サーバ／外部用 AP サーバ／内部用ネットワーク機器／内部用通信経路など)に分解する。

それぞれに要求される機密レベル(4 段階)を設定することで、必要とされる情報セキュリティ対策技術(6 分類 28 種)が選定できる。対策基準は、分科会メンバー(ユーザとベンダメンバー参加)のノウハウを結集し、検討している。

これらの成果は、Excel を使用した「セキュリティ対策ベースライン作成ツール」として開発した。

(2) 「ESA ひな型」

ESA は、企業の情報システム開発時や監査時に適合性をチェックする際、適用される。そのため、情報システムの開発、運用に携わる人に容易に理解されるよう文書化される必要がある。

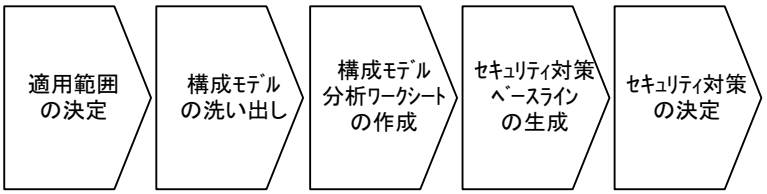
本分科会では、情報セキュリティ担当者が短期かつ品質の良い ESA 文書を作成できるようにするため、「セキュリティ対策ベースライン作成ツール」の結果を利用する「ESA ひな型」を作成した。

「ESA ひな型」では、本書の目的／基本的セキュリティ要求事項／セキュリティ対策ベースライン／ESA の管理／ESA の運用について記述している。

(3) 「ESA 作成ガイドブック」

本分科会では、「セキュリティ対策ベースライン作成ツール」の使用方法や「ESA ひな型」を利用した作成手順（図表 1）や留意点を記述した「ESA 作成ガイドブック」を作成し、本分科会に参加されていない方でも容易に ESA 作成ができるように考慮した。

図表 1 ESA 作成における情報セキュリティ対策決定プロセス



(4) 分科会成果の有効性の検証

企業向け ESA 作成のための各種ツールや文書を作成してきたが、今回の研究の最大の成果である「セキュリティ対策ベースライン」の有効性について検証を行った。

検証方法としては、「セキュリティ対策ベースライン」を分科会参加各社のシステムに適用し、使い勝手とベースラインの妥当性を確認している。検証結果は以下の通りであり、本分科会で作成したツールは十分実用に耐えられるものであった。

- 情報システムの要素モデル分解や機密レベルの選定は、すべての情報システムを網羅でき選択のあやふやさは、ほとんどなかった。
- セキュリティ対策ベースラインで導き出せる情報セキュリティ対策内容と実際の情報セキュリティレベルには差が発生したものの、本来情報セキュリティ強化が必要と考えている内容であり、基準として容認できるレベルであった。また、業種による差についても、要求される機密レベルが異なっていることから、妥当な情報セキュリティ対策が導き出された。

3. 研究成果の評価と提言

バランスがとれた ESA を作成するためには、幅広い情報セキュリティに関する知識が必要である。また、ESA の妥当性を検討するために膨大な労力を必要とする。そのために、一般企業で ESA を作成することが容易ではなかった。

本分科会では、この課題の克服のためにメンバーのノウハウを結集し、情報セキュリティ対策の基準値を検討し、ESA 作成の型決めを行うことができた。これにより、一般企業で短期間に適正な ESA 作成が可能になったと言える。

しかしながら、全社全システムに適用するためには、関連システム部門への説明と理解が必要となる。

また、実際に ESA を理解して、導入システム毎の具体的な製品を選択する手法が確立されていないため、全面的な適用を徹底させるには、さらに労力を要することとなる。そこで、今回の ESA は、以下の用途で限定して使用することを特に推奨する。

(1) ESA ギャップ分析への利用

作成された ESA と現状の情報セキュリティ対策状況の差異を明確化し、弱点を明らかにすることで改善点を明示することに利用する。

(2) 情報セキュリティ対策ロードマップへの適用

情報セキュリティ対策はロードマップを作成し、適正な導入が必要であり、ESA はロードマップ作成時の根拠に利用することが有効的である。