

# 情報セキュリティソリューション

## Information Security Solutions

あらまし

「日本版SOX法」に代表される動きが活発化し、情報セキュリティガバナンスへの取り組みが求められている。企業・組織は情報セキュリティガバナンスを確立する上で、マネジメントシステムを構築し、顧客・投資家・ビジネスパートナーなどのステークホルダに対して、情報セキュリティ対策の取り組みを継続的に説明することが必要となってきた。

また、政府も企業の情報セキュリティ対策の取り組みを推進するための「情報セキュリティ報告書モデル」を提唱した。

富士通はこのような背景のもと、企業の有効かつ、効率的な情報セキュリティ投資を支援するエンタープライズセキュリティアーキテクチャ（ESA）という概念を提唱するとともに、製品・サービスの体系であるセキュリティソリューションを提供している。

本稿では、情報セキュリティ報告書モデルを紹介し、富士通のESAの概念とそれに基づくセキュリティソリューションを紹介する。

Abstract

In accordance with intensified efforts for enactment of J-SOX, companies are expected to promote various approaches for information security governance. In establishing the governance, companies have been asked to develop management systems and regularly explain their information security measures to stakeholders, for example, customers, investors, and business partners. The Japanese government advocates an information security report model to help companies promote efforts toward security measures. Against this background, Fujitsu has provided the Enterprise Security Architecture (ESA) concept for supporting effective and efficient corporate investment in information security. Fujitsu also separately provides the security solutions that are incorporated into the foundations of its products and services. This paper describes the government's information security report model and Fujitsu's ESA and ESA-based security solutions.



内田清貴（うちだ きよたか）  
セキュリティサービス統括部基盤サービス部 所属  
現在、セキュリティ監査業務に従事。



菅野憲昭（すがの のりあき）  
セキュリティサービス統括部基盤サービス部 所属  
現在、セキュリティアーキテクトとして、セキュリティシステムの設計・構築業務に従事。



安藤彰一（あんどう しょういち）  
セキュリティサービス統括部基盤サービス部 所属  
現在、アウトソーシングセンタ共通インフラの運用に従事。

## まえがき

昨今、外部からのコンピュータウイルス、ワーム、不正アクセスなどの脅威、内部からの機密情報・個人情報への漏えい、システムダウンによる業務停止など、情報システムの事故が相次ぎ発生している。情報漏えいのケースでは、企業・組織の信用問題だけでなく、その顧客への金銭的被害も発生しており、企業経営への影響が顕在化しつつある。

また、業務の情報システム化が加速し、社会全体のネットワークが整備された結果、情報システム事故の影響が個々の企業・組織内の問題にとどまらず、社会全体に波及することも懸念されている。

一方、企業・組織における情報セキュリティ対策の必要性は認識されているが、実態としては、ファイアウォールの設置やコンピュータウイルス対策製品の導入といった技術的な対策が中心であり、マネジメント的な対策（セキュリティポリシー策定、セキュリティ監査、アクセスログの取得・解析など）は、十分に行われていないのが現状である。

このような状況下で、「日本版SOX法」に代表される動きが活発化し、企業・組織には内部統制の強化が求められてきた。企業・組織の業務が情報システムに大きく依存している現状をかんがみると、内部統制の強化には情報システムの対応が必要であり、その中で重要な役割を果たす情報セキュリティガバナンスへの取組みが求められている。

本稿では、まず情報セキュリティに対する企業・組織の果たすべき責任、およびそれを支援する政府が提唱している情報セキュリティ報告書の構成について述べる。

つぎに、情報セキュリティ報告書を作成するために必要な情報と、それを支援する富士通の取組みであるエンタープライズセキュリティアーキテクチャ（ESA）とセキュリティソリューションについて述べる。

## 情報セキュリティ対策の取組み

### 情報システムに求められること

まえがきに述べたように、情報システムの事故は企業・組織の業務継続に多大な影響を与えるとともに、企業・組織内の問題にとどまらず社会全体へ影響を与える場合もある。

そのため企業・組織は、顧客・投資家・ビジネスパートナーなどのステークホルダのみならず社会全体から情報システムの事故が発生しないように対策を行うことが求められている。

### 情報セキュリティ対策の難しさ

企業・組織は、事業継続・法令遵守などの観点から情報セキュリティ対策が必要であるという認識を持っている。

しかし、情報セキュリティ対策の実施にはコストがかかる。企業・組織の情報システム担当者は、経営者へ情報セキュリティ対策の実施に向け予算の確保依頼を要請するが、対策実施によるリスク低減の効果を定量的に示すことが難しいため、経営者の理解が得られず予算が確保できない場合が多い。

また、経営者としても情報セキュリティ対策に取り組む企業・組織がステークホルダから相応に評価される仕組みがないため、積極的に情報セキュリティ対策に取り組みにくい環境にある。

これらにより、企業・組織においては、情報セキュリティ対策の必要性は認識しているが、実施困難という課題を抱えている。

### 情報セキュリティ対策への取組みの推進

企業・組織の情報システムは、日々脅威にさらされており、事故発生時にその都度対策を実施したとしても、新たな脅威により情報セキュリティ事故は発生する可能性がある。このため、企業・組織はその場しのぎの個別対処療法で済ませるのではなく、情報セキュリティガバナンスを確立し自律的・継続的に改善・向上する仕組みを導入することが必要となる。

それには、情報セキュリティ対策を企業・組織が自主的に行っていることを顧客・投資家・ビジネスパートナーなどのステークホルダから評価される必要がある。

政府は企業による自主的な情報セキュリティ対策の取組みを促す環境の整備を支援することを掲げており、その一環として「情報セキュリティ報告書」モデル<sup>(1)</sup>を提唱した。

## 情報セキュリティ報告書の作成について

### 「情報セキュリティ報告書」モデル

企業はIR（Investor Relations）を通して、顧客・投資家・ビジネスパートナーなどのステークホル

ダに対して、投資判断に必要な情報を提供する活動を実施している。

「情報セキュリティ報告書」は、企業・組織が同報告書を通して、情報セキュリティに関する取り組み状況を提供することにより、ステークホルダが当該企業・組織の情報セキュリティ対策の実施状況を適正に把握できることを目指すものである。

「情報セキュリティ報告書」の位置付けとしては、記載項目・内容のレベルは企業・組織の状況に応じて選択可能とし、開示方法としてはCSR (Corporate Social Responsibility) 報告書の一部として組み込むことも、単体の報告書として公表することも可能としている。

また、「情報セキュリティ報告書」に記載する内容の雛形として経済産業省は「情報セキュリティ報告書」モデルを提示し、情報セキュリティポリシーやそれを実現する内部統制の仕組み、第三者評価など、ステークホルダから適正に評価されるために報告すべき事項を提示している。

## 情報セキュリティ報告書

情報セキュリティ報告書には、セキュリティに関する取り組み方針と対象範囲、およびマネジメント体制を記載する。さらに、中長期的な情報セキュリティ戦略と情報セキュリティに関するリスクをまとめなければならない。

そのためには、アクションプランや数値目標を定め、企業・組織自らによる、計画に対する実績・評価・分析を行い、さらに第三者による評価・認証も必要となる。

情報セキュリティ報告書には、以下に示す七つの項目から必要なものを選択し、記載することとなる。

### (1) 基礎情報

発行目的、利用上の注意、対象期間、責任部署など。

### (2) 経営者の情報セキュリティに関する考え方

方針、対象範囲、ステークホルダの位置付け、メッセージなど。

### (3) 情報セキュリティガバナンス

マネジメント体制、リスク、情報セキュリティ戦略など。

### (4) 情報セキュリティ対策の計画、目標

アクションプラン、数値目標など。

(5) 情報セキュリティ対策の実績、評価  
実績、評価、事故報告など。

(6) 情報セキュリティにかかわる主要注力テーマ  
アピールしたいテーマなど。

(7) 第三者評価・認証

客観的な評価など。

情報セキュリティ報告書作成に必要な情報

前節で示した項目の記載には、それを裏付ける証拠が必要になる。大きく以下の3点に分類することができる。

### (1) マネジメント体制の確立

マネジメント体制を確立し、セキュリティポリシー（方針）を定め、数値目標や情報戦略を決定する。対象となる情報資産個々にCIA分析（機密性、完全性、可用性）を行い、その対応策を検討し、活動実績と評価を行う必要がある。つまり組織全体での取り組みが要求される。

### (2) ログの記録と管理

情報セキュリティに関する活動の証拠として、そのログ情報の取得と管理、そして分析を行う必要がある（表-1）。

### (3) 第三者評価・認証

情報セキュリティの取り組みについて、客観的な評価として情報セキュリティマネジメントシステム（ISMS：Information Security Management System）適合性評価制度、情報セキュリティ監査制度、プライバシーマーク制度などの活動が必要となる。

これらを実施するためには、セキュリティに対する技術、労力が求められ、一筋縄では、実施することが困難である。

表-1 情報セキュリティ対策と実施例

機密 情報 保護	アクセス制御	・ファイアウォールの導入 ・侵入検知システム（IDS）の導入 など
	ユーザ認証	個人認証 など
	情報漏えい 対策	暗号化 など
	ウイルス対策	ウイルス対策ソフトウェアの導入 など
法令 対策	ログ管理/分析	取得した様々なログの一元管理 （証拠管理） など
その他		・セキュリティ脆弱性診断 ・侵入検知システム運用 ・情報漏えい対策 などの外部委託（アウトソーシング） など

富士通のセキュリティソリューション

適切な情報セキュリティ投資

情報セキュリティ対策を実施するに当たり、投資効果の高い最適な対策の実施と、残存リスクを経営者が認識することが重要だと考える。

富士通は、有効かつ効率的なセキュリティ投資を実現するためのセキュリティ機能のあり方として、以下に述べるエンタープライズセキュリティアーキテクチャ（ESA）を提唱した（図-1）。

エンタープライズセキュリティアーキテクチャ

従来のセキュリティ対策では、情報セキュリティポリシーからシステムへの実装に当たって検討が必要な、実現テクノロジー（例えば認証方式における、パスワード認証、生体認証）の選択、セキュリティ機能実現方式（例えばパスワード認証方式における、パスワード長・有効期限）の決定に際し、セキュリティ標準が規定されておらず、業務・投資の有効性・効率性が著しく阻害されていた。

ESAでは、認証・アイデンティティマネジメント、アクセスコントロールや証跡管理、集中管理などを明確に規定しており、例えば、認証・アイデンティティマネジメントの一意識別としては、パスワードと生体を利用した認証方式を規定している（図-2）。

前述のように、富士通ではセキュリティの基本概念をESAとしてまとめ、IT基盤のインフラモデルパターンをTRIOLEテンプレートとして定義し、個々の製品・サービスをカテゴリごとに整理した

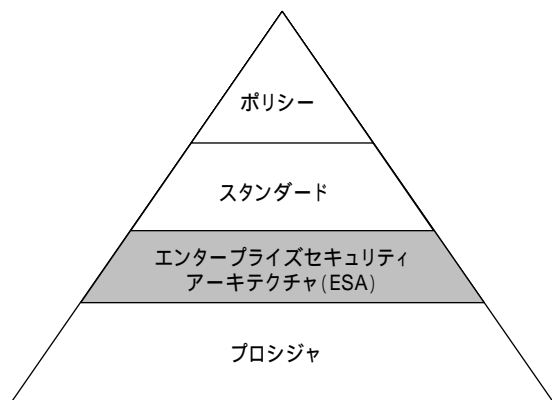


図-1 エンタープライズセキュリティアーキテクチャの位置付け  
Fig.1-Positioning of Enterprise Security Architecture.

ものをセキュリティソリューションとして提供している。

セキュリティ統制ソリューション

ESAに基づき、セキュリティ統制に必要な4機能について製品・サービスをセキュリティ統制ソリューションとして体系付けた（図-3）。

主なセキュリティ製品・サービスを以下に示す。

(1) 認証・アイデンティティマネジメント

- ・SMARTACCESS/Premium
- ・バイオ認証装置
- ・手のひら静脈認証装置
- ・Secure Login Box
- ・Sun Java System Identity Manager

(2) アクセスコントロール

- ・Systemwalker Desktop Rights Master
- ・eTrust Access Control
- ・エンドポイントセキュリティソリューション

(3) 証跡管理

- ・Systemwalker Centric Manager
- ・Systemwalker Desktop Keeper
- ・Systemwalker Desktop Log Analyzer

・PISO

・ETERNUS3000

・NR1000

・個人情報保護/情報漏洩対策運用サービス

(4) 集中管理

- ・Systemwalker Desktop Patrol
- ・Systemwalker Centric Manager

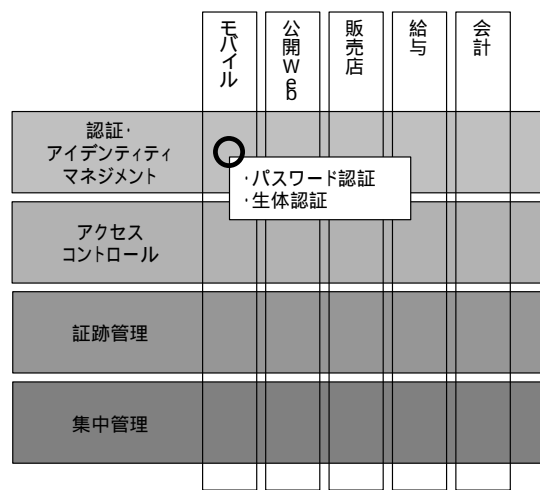


図-2 基本機能と実現方式  
Fig.2-Basic functionality and implementation method.

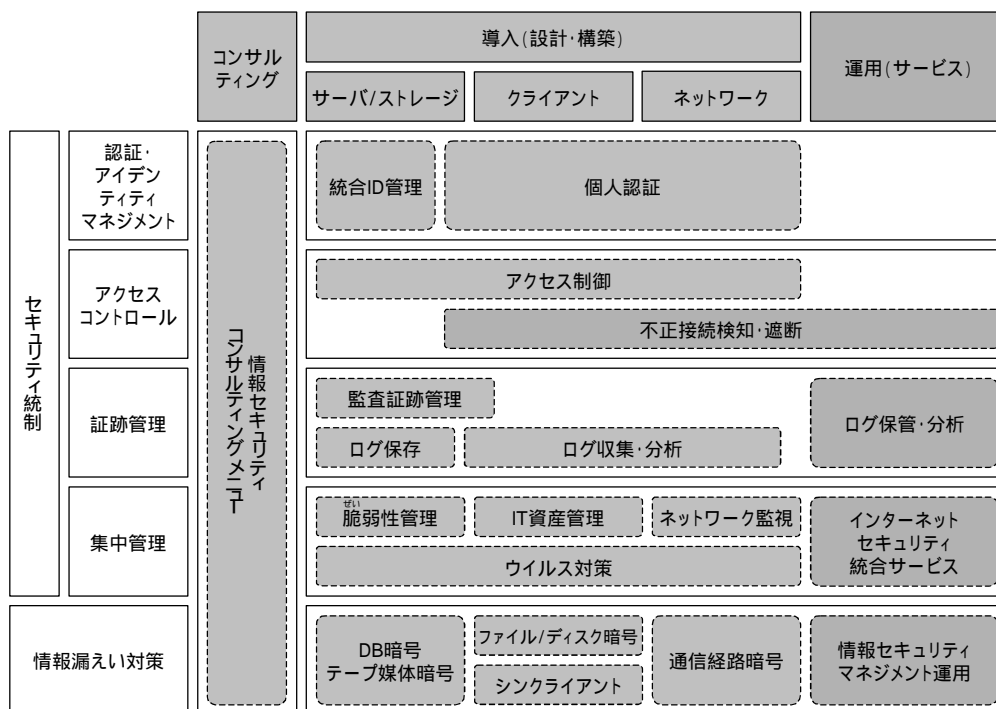


図-3 セキュリティ統制ソリューション  
Fig.3-Security control solution.

- ・ Systemwalker Process管理 (仮称)
- ・ インターネットセキュリティ統合サービス
- ・ アタックテストサービス エクスプレス
- ・ Webアプリケーションセキュリティ診断サービス
- ・ セキュリティ監視サービス
- ・ 入退出および動態監視
- ・ 画像監視

以上のように、富士通ではコンサルティングから導入、運用までお客様をトータルでサポートするための製品・サービスを用意し、強力なセキュリティ対策を実現する。

## む す び

富士通の提唱する、エンタープライズセキュリティアーキテクチャを活用することにより、企業・組織にとって適切な情報セキュリティ報告書を作成

することが可能となる。

これにより、情報セキュリティガバナンスの確立や向上を確実に行うことが可能となるため、企業・組織が顧客・投資家・ビジネスパートナーなどのステークホルダから評価され、健全なビジネス環境を構築することができる。

今後も富士通では、企業・組織の情報セキュリティガバナンスの確立や向上を図る製品・サービスを提供していく。

## 参 考 文 献

- (1) 経済産業省 商務情報政策局 情報セキュリティ政策室 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：情報セキュリティ報告書モデル．平成17年3月31日．

[http://www.meti.go.jp/policy/netsecurity/downloadfiles/5\\_sec\\_report.pdf](http://www.meti.go.jp/policy/netsecurity/downloadfiles/5_sec_report.pdf)