❸

ネットワーク社会における セキュリティー・アーキテクチャーの活用

Use of security architecture in network communities

日本アイ・ビー・エム株式会社
ビジネス・イノベーション・サービス
セキュリティ&プライバシー・コンサルティング
エグゼクティブ・コンサルタント
山崎 哲

Satoru Yamasaki
Excutive Consultant
Security & Privacy Consulting
Business Innovation Services
IBM Global Services

ネットワーク社会の発展とともに情報セキュリティーの重要性が増しています。情報セキュリティー確立への要求が高まる中で、日本アイ・ビー・エムのセキュリティー・コンサルティング部門では、技術面および管理面のセキュリティー対策案を策定するためにセキュリティー・アーキテクチャーを活用しています。ISOベースのIBM Security Architectureに基づいて策定していますが、具体的で一貫した展開技法はまだ確立されておらず、今日のネットワーク社会に対応する新しいセキュリティー・アーキテクチャー技法が望まれています。
本論文は、セキュリティー・アーキテクチャー確立の問題点・課題点を洗い出し、ネットワーク社会に対応するセキュリティー・アーキテクチャーを策定する技法を新しく確立しようとするものです。

The development of network communities and the importance of information security are on the increase. As requirements affecting the establishment of network security increase, security consulting at IBM is more and more making use of security architecture for formulating proposals for dealing with security matters from both the technical and administrative angles. Formulation is being carried out in accordance with IBM Security Architecture based on ISO, but concrete, integrated methods of development have yet to be established, and there is a need for new security architecture methods appropriate to today's network communities.
In this paper we take a look at the problems and issues involved in the establishment of security architecture and attempt to establish new methods for formulating security architecture in line with the needs of network communities.

1. はじめに

1.1. セキュリティー・アーキテクチャー確立の背景

ネットワーク社会においては、情報に対する不正アクセスやサービス妨害などのセキュリティーにかかわる諸問題が増加してきており、企業活動に対して、広範囲で多大な影響を及ぼしています。ネットワーク社会において、情報を活用し、変化に対応できる企業活動を推進するには、情報セキュリティーの確立は、避けることのできない最重要課題となっています。

しかし、多くの企業では、セキュリティー対策について明確な手法や答えを持ち合わせていないのが現状です。一般に、セキュリティーについては、情報の価値とそれに対する脅威によってリスク分析を行い、リスクに応じてセキュリティー管理策を選択し、セキュリティー投資を決定するのが本来のやり方です。

多くの企業は、このリスク分析を導入してきた経験をあまり持たず、セキュリティーを実施していたとしても十分にリスク分析を生かしていないのが現状です。企業がネットワーク社会の変化に対応して生き抜くには、お客様や社会から信頼を得られる情報セキュリティーの確立が必須であり、それにはリスク分析に基づき、技術面および管理面の適切なセキュリティー管理策を選択し、セキュリティー投資額を決定する手法の確立が急務となっています。

そのために実施しなければならない主な項目は下記の通りです。これらは、コンサルティングのサービスとして提供されています。

(1) セキュリティー診断

- セキュリティー診断は、プロセス診断・インフラストラクチャー診断・アプリケーション診断の三つの柱から成ります。
- プロセス診断は、グローバル・スタンダードが定める情報セキュリティーの標準フレームワークの10領域ごとに、情報セキュリティー確立のあるべき姿と対比して診断します。各領域にはさらに幾つかの診断項目(コントロール)があり、合計で百数十のコントロールで診断します。
- インフラストラクチャー診断では、情報ネットワークやシステムに対して玄関・ロビー・警備ゲート・社内・勝手口・社内内部などに分類し、玄関と勝手口の両方からハッカーの侵入可能性をテストします。
- アプリケーション診断は、対象アプリケーションをデータ・フローと構成要素の関係に分解し、分解された要素に対して安全性診断の観点であるセキュリティー要件に基づき診断します。

(2) セキュリティー・ポリシー策定

- セキュリティー・ポリシー策定においては、情報資産の分類・機密区分、社員・派遣社員などの人的セキュリティー(責任・教育・報告)などのセキュリティーの考え方や方向性を記述した方針書、それを具現化するための標準書・手続書を策定します。

(3) セキュリティー・アーキテクチャー策定

- セキュリティー・アーキテクチャー策定は、セキュリティーを守るシステム・インフラストラクチャーの設計において、セキュリティー技術の採用の原則を定めた「技術原則」と、セキュリティーを守るシステム・インフラストラクチャーの設計において確立すべき管理の原則を定めた「管理原則」を記述します。

この中で、(1) セキュリティー診断と (2) セキュリティー・ポリシー策定については、基本的な考え方やメソドロジー(技法)が比較的整備されていますが、(3) セキュリティー・アーキテクチャー策定は、システム構築のために重要であるにもかかわらず、進め方やメソドロジー(技法)が十分に完成されておらず、問題点が多くあります。本論文では、このセキュリティー・アーキテクチャー策定を取り上げて、新しいセキュリティー・アーキテクチャー確立の技法を探ります。

1.2. セキュリティー・アーキテクチャー確立の問題点

筆者の経験から、セキュリティー・アーキテクチャー確立に必要な要件とその問題点をまとめると次のようになります。

- ISO7498-2やAPKI(Architecture for PKI)などのセキュリティー・アーキテクチャーのフレームワークがありますが、明確にはフレームワークが決まっていません。アーキテクチャー策定には、最適なフレームワークの選択が不可欠です。
- ビジネス要件からセキュリティー要件を求め、それをベースにセキュリティー・アーキテクチャーの技術原則および管理原則を定義する具体的な展開方法が確立していません。
- セキュリティー・アーキテクチャー定義の中で最も複雑で難しい部分は、ビジネス要件から必要なセキュリティー要件を抽出することです。そのための最適な論理的手法の確立が課題となります。

1.3. セキュリティー・アーキテクチャー確立の目標

本論文では、セキュリティー・アーキテクチャーを確立するために次の三つの課題点を解決することを目指します。

- 各種セキュリティー・アーキテクチャーのフレームワークを調査し、ネットワーク社会に対応した新しいセキュリティー・アーキテクチャー策定に使用できる最適なフレームワークを決定します。
- セキュリティー・アーキテクチャーを定義するために、ビジネス要件からセキュリティー要件を抽出し、最終的に技術原則および管理原則を定義するまで、体系的で一貫した展開を確立します。
- ビジネス要件からセキュリティー要件に展開するための最適

な論理的手法を確立します。

2. セキュリティー・アーキテクチャー確立の課題点の分析

2.1. セキュリティー・アーキテクチャーの役割

新しいセキュリティー・アーキテクチャーがなぜ注目されるようになったのかを考えてみます。セキュリティーを取り巻く環境について、次の観点で見ることができます。

(1)ビジネスの観点から…

- 多様なビジネスやサービスに対応して最適なセキュリティーを装備したいが、あまりにも複雑なため困難。
- 手作業や作業の分散化などが増加し、また、スキルの高いスタッフが少ないため高コスト化につながり、セキュリティーのトータル・コストは増えつつある。

(2)セキュリティー・システム構造の観点から…

- 各種の理論(プロトコル、アルゴリズム、APIなど…)に基づいていて複雑。
- 環境(ネットワーク、プラットフォーム、ミドルウェア、アプリケーション)がマルチベンダーで多様。
- 異なったモデル・仕組み(PKI、DCE、独自の仕組み、アプリケーションに組み込まれた仕組み)が組み合わされていて複雑。
- 新技術(技術の発展、アタッカーの技巧の高度化)が絶え間なく変化している。
- ユーザーの増加に応じて、性能の悪化が見られる。

こうした環境に対応するには、セキュリティーの基盤であるネットワークおよびシステムの物理的側面に加えて、分散化によってますます複雑化する機能的側面によるアーキテクチャーの確立が必要です。

2.2. セキュリティー・アーキテクチャーの最適フレームワークの決定の課題点

アーキテクチャー確立の課題点の第1は、「新しいセキュリティー・アーキテクチャー策定に使用できる最適なフレームワークを決定する」ことです。そこで、セキュリティー・アーキテクチャーのフレームワーク標準化の現状を調べてみます。

(1)現在のIBM Security Architectureは、国際標準であるISO7498-2に基づいており(**図1**)、コンサルティングではアーキテクチャー策定のフレームワークとして使用してきましたが、次に挙げる特徴/問題点を持っています。

- ISO7498-2では、ビジネス要件から導き出されるセキュリティー要件を五つのセキュリティー・サービスとしてConfidentiality(機密性)、Integrity(完全性)、Identification & Authentication(識別と認証)、Access Control(アクセス制御)、Non Repudiation(否認防止)で考えています。従来は、C、I、AすなわちConfidentiality(機密性)、Integrity(完全性)、Availability(可用性)で考えるのが一般的でしたが、五つの要件にはAvailability(可用性)が含まれておらず、セキュリティー要件としては不十分です。
- このフレームワークでは、セキュリティー・サービスごとに、適用すべきメカニズム(セキュリティー技術)と管理対象となるオブジェクト(キーなどの実体)を定義していくことで、セキュリティーの確保されたシステム構築の技術的な指針を導き出しています。このアーキテクチャーは、構築するシステムのセキュリティー技術採用の指針をまとめ、セキュリティーの全体の概念をとらえるのに効果的であり、既に多くの実績もあります。
- このフレームワークは、五つのセキュリティー・サービスに基づいており、お客様のビジネス要件の反映が容易ですが、開発に直接結び付けるのは困難です。なぜなら本フレームが示すのはあくまでもコンセプチュアルなアーキテクチャーであり、策定されたアウトプットは技術的な指針を述べるにとどまっているからです。
- ISO7498-2自体が、標準として制定されてから時間がたっており、機能的側面から見た場合に、必ずしもインターネットや分散系システムに代表される最新のネットワーク環境で要求される要件を満たしているとはいえません。

(2)IBMやヒューレット・パッカード社を中心に組織化されている「The Open Group」は、今後のネットワーク社会のセキュリティー・アーキテクチャーのフレームワークとしてAPKI(Architecture for Public Key Infrastructure)を定義しています。このフレームワークの特徴や問題点は次の通りです。

- インターネットなどの新しいネットワーク社会を意識し、その環境で安全なコンピューター・ネットワーク・システムを構築できるように考え出されたセキュリティー・アーキテクチャーです。セキュリティーが確保されたシステム構築のための機能を、次の五つの"A"のグループにまとめています(**表1**参照)。

《Authorization》

「アクセス権限」についての機能を表します。「だれが、どの情報を、どのように扱うことが許されているか」を管理する機能が集約されています。

《Accountability》

「責任」についての機能を表します。「だれが、いつ、どんな行為を行ったか」を監査するための機能や、「メッセージ発信および受信の行為に対し、発信者および受信者から否認されない」ための機能が集約されています。

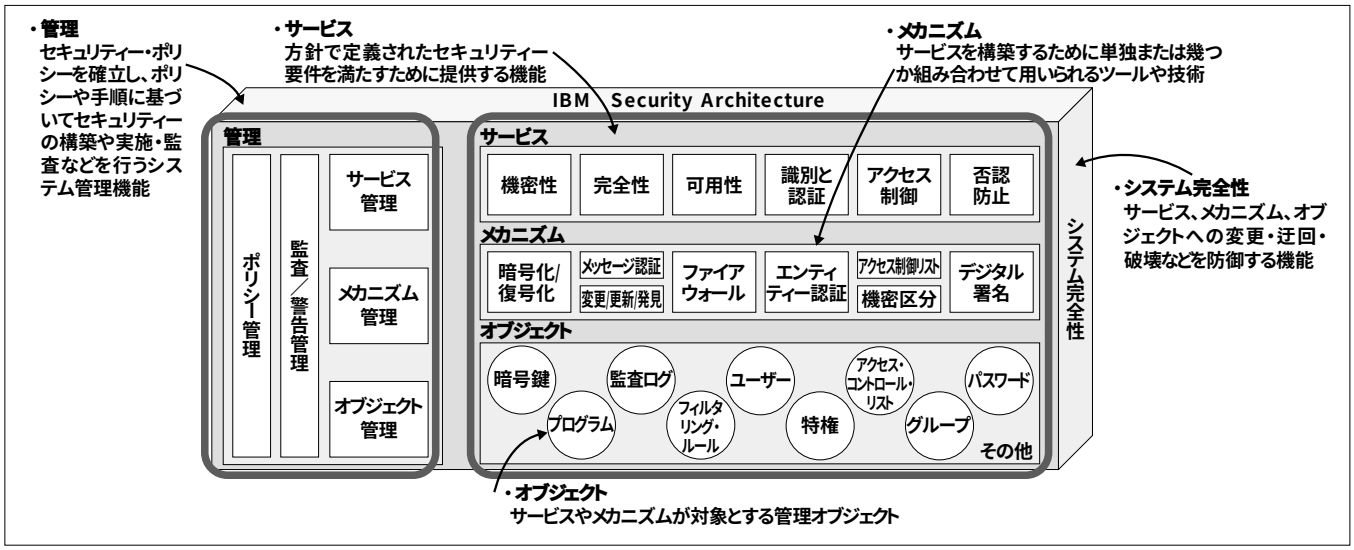


図1．ISO7498-2に基づくIBM Security Architecture

《Availability》

「可用性」についての機能を表します。障害時や災害時におけるサービス継続やバックアップ、リカバリーに関する機能が集約されています。

《Assurance》

「保証」についての機能を表します。構築されたシステムが確実に稼働することを保証するための機能が集約されています。

《Administration》

「管理」についての機能を表します。セキュリティーが確保された状態を維持するための支援機能（例えば、ユーザー管理や構成管理など）が集約されています。

- ネットワーク社会の認証技術であるPKI（Public Key Infrastructure）に基づくアーキテクチャーをフレームワークとしています。このフレームワークは、基本的に開発者を対象としているため、ファンクショナル・アーキテクチャーおよびコンポーネント・アーキテクチャーをカバーしており、セキュリティー機能構造面からのアプローチに適していると考えられます。

2.3. セキュリティー・アーキテクチャー確立のための体系的な展開の課題点

アーキテクチャー確立の第2の課題点は、「全体で体系的に一貫して連続している展開を確立する」ことです。そのための標準化動向は次の通りです。

(1)セキュリティー・アーキテクチャーの基本として、リスク分析に基づいて最適な技術原則および管理原則を定めます。情報セキュリティーの概念とモデルを国際標準として体系化したフレームワークにISO/IEC TR13335：GMITS（Guidelines for the Management of IT Security）があります（図2）。

表1．APKIに基づく5Aセキュリティー・アーキテクチャー

機能グループ	セキュリティー機能	セキュリティー技術
Authorization（アクセス権限）	データ保護	鍵配布
		本人認証
		データ・プライバシー
		データ完全性
	アクセス制御	ポリシー執行
		特権権限管理
		ユーザー認証
Accontability（責任）	監査	
		事象生成／処理
	否認防止	デジタル署名
		信頼時間
Availability（可用性）	サービス継続	複製
		リソース割り当て
		比率限界
	災害対策	データ・バックアップ／リストア
		キー・リカバリー
Assurance（保証）	エンジニアリング	エンジニアリング
	開発プロセス	文書化
	オペレーション管理	完全性保守およびリストア
Administration（管理）	システム構成	導入・構成TCBマネジメント
	メカニズム管理	起動・省略時設定
	ポリシー管理	ユーザー識別・認証・監査・信頼

- ISO/IEC TR13335：GMITSは、脅威、脆弱性、情報資産の価値を基にリスク・レベルを把握し、リスクを下げるためにセキュリティー要件に対応した防御対策を定義します。

2.4. ビジネス要件からセキュリティー要件に展開するための課題点

アーキテクチャー確立の第3の課題点は、アーキテクチャー定義のステップでも重要な「ビジネス要件からセキュリティー要件に展開するための最適な論理的手法の確立」です。

(1)システム単位での情報資産の価値評価に、脅威分析と脆弱性分析とを加味して分析し、リスク・レベルを把握します。

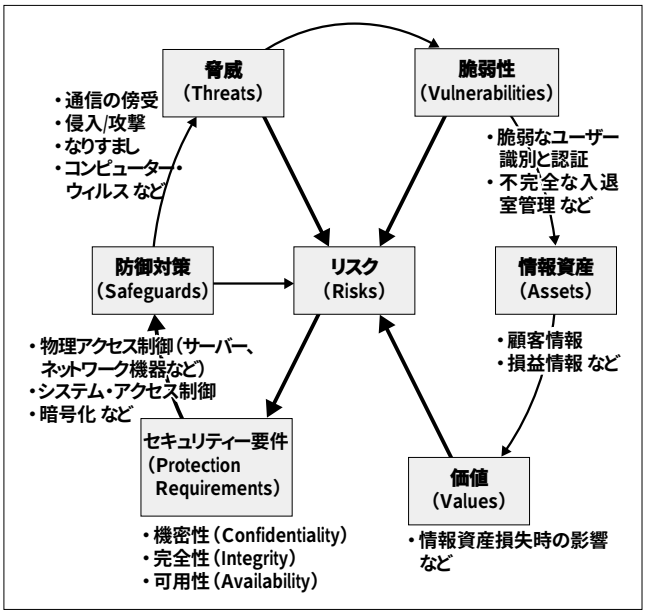


図2. ISO/IEC TR13335-1:GMITS

- 情報資産の価値分析を実施し、情報資産の価値レベルを把握します。セキュリティーが侵されたときの直接金額の損失、信用失墜による損失、法律問題による損失などの結果を反映します。
- 36種類に定義した脅威領域から選択して、情報資産に対する脅威分析により脅威レベルを把握します。
- 脅威に対する情報資産の脆弱性分析を実施し、脆弱性レベルを把握します。
- 情報資産の価値レベル・脅威レベル・脆弱性レベルより、リスク・レベルを把握します。

(2) リスク・レベルから、それに対応した必要な対策を洗い出し、対策を整理してセキュリティー要件を定義します。

3. アーキテクチャー確立のための解決方法

3.1. ネットワーク社会のアーキテクチャーのフレームワーク

前述の通り、ISO7498-2は、ビジネス要件からセキュリティー要件を抽出するのにお客様に理解しやすく、コンサルティングにとっても整理しやすいため、今後ともセキュリティー・アーキテクチャーのフレームワークとして使用することにします。

ISO7498-2では、ビジネス要件から導き出されるセキュリティー要件を、五つのセキュリティー・サービスに分けています。IBMのコンサルティングの手法では、この五つにさらにAvailabilityを追加し、以下の六つのカテゴリーでセキュリティー・サービスを考えています。

- Confidentiality(機密性)
- Integrity(完全性)
- Availability(可用性)
- Identification&Authentication(識別と認証)
- Access Control(アクセス制御)
- Non-Repudiation(否認防止)

この六つのセキュリティー・サービスごとに適用すべきメカニズム(セキュリティー技術)と、管理対象となる管理オブジェクト(暗号キーやパスワード・ファイルなど)を定義していくことで、セキュリティーの確保されたシステム構築の技術的な原則を導き出しています。このアーキテクチャーは、セキュリティーの全体の概念をとらえるのに適しているため、本論文ではこのアーキテクチャーをコンセプチュアル・アーキテクチャーと呼びます。

コンセプチュアル・アーキテクチャーを活用したアーキテクチャー確立手法は、構築するシステムのセキュリティー技術採用の方針をまとめるのに適し、既に多くの実績もあります。しかし、残念ながら以下の二つの課題が残ります。

(1)本フレームが示すものはあくまでコンセプチュアルなアーキテクチャーであり、策定されたアウトプットは技術的な方針を述べるにとどまっています。この方針をどのように実装していくかについては現在のところ展開できていません。

(2)ISO7498-2自体が、標準として制定されてから時間がたっており、特に機能的側面から見た場合、必ずしもインターネットや分散系システムに代表される最新のネットワーク環境での要件を満たしているとはいえません。

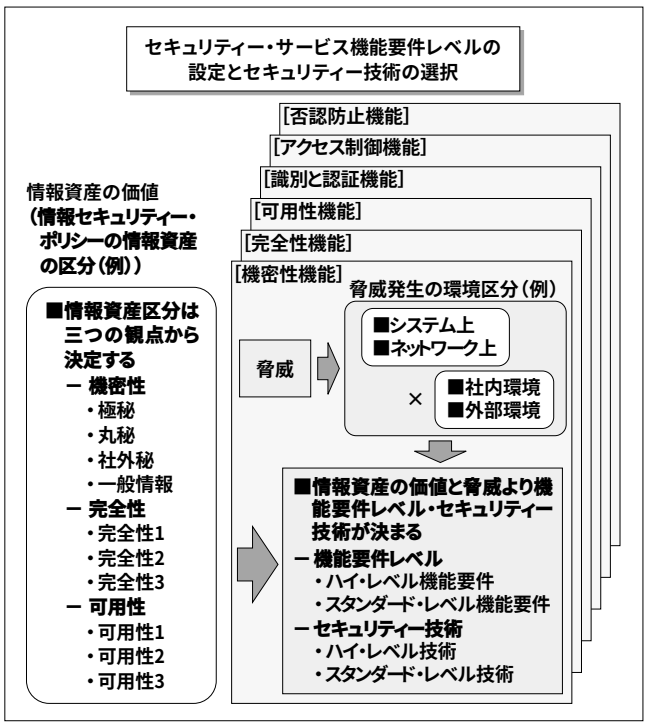


図3. セキュリティー・サービス機能要件レベルの設定

3.2. 全体で一貫した体系的アーキテクチャーの確立

セキュリティー・アーキテクチャー策定は、ISO7498-2をフレームワークとして、セキュリティー技術／管理原則を定義するセキュリティー・コンサルティングのサービス・メニューとして提供されています。しかし、メソドロジー（技法）は、セキュリティー・コンサルティングの手法として基本的に活用しているものの、全体を通して一貫した体系的なアーキテクチャーの確立の手法としては完成の域には達せず、幾つかの試みを実施している段階です。

現在のアーキテクチャー策定のステップは次の通りです。

(1) ビジネス要件からセキュリティー要件を定義するためにリスク分析を実施します（図3。3. 3節で詳述）。

- 業務システムとそこで使用されている情報を定義します。
- 情報の価値を定義し、価値レベルを把握します。
- 情報に与える脅威を設定し、脅威レベルを把握します。
- 脅威に対する情報の脆弱性（ぜいじゃく）レベルを把握します。
- 情報資産の価値レベル・脅威レベル・脆弱性（ぜいじゃく）レベルより、リスク・レベルを把握します。
- リスク・レベルの脅威ごとに必要な対策を洗い出し、対策を整理してセキュリティー要件ごとにまとめます。これが、業務システムの情報ごとのセキュリティー要件となります。

(2) セキュリティー要件ごとにリスク・レベルに対応した対策をまとめ、メカニズムを定義します。

- リスク・レベルに対応して、標準的な対策（スタンダード・レベル）と、より高度な対策（ハイ・レベル）に分類します。
- 対策に応じた技術標準情報を参照して、標準的な対策（スタンダード・レベル）が求めるメカニズムと、高度な対策（ハイ・レベル）が求めるメカニズムを定義します。
- メカニズムに対応して、管理オブジェクトを定義します。

(3) リスク分析により、技術原則を支援する必要な管理機能を抽出し、管理原則のフレームワークに分類し定義します。

- (1) のリスク分析を通じて、技術原則を支援する必要な管理機能を洗い出します。
- 管理機能をフレームワークをベースに分類します。フレームワークとしては、ポリシー管理・監査／警告管理・サービス管理・メカニズム管理・オブジェクト管理があります。

(4) 結果として、技術／管理原則を定義します。

- 技術原則は、セキュリティーを守るシステム・インフラストラクチャーの設計においてセキュリティー技術の採用の原則を定めたものを定義します。
- 管理原則は、セキュリティーを守るシステム・インフラストラクチャーの設計において、確立すべき管理の原則を定義します。

3.3. ビジネス要件からセキュリティー要件に展開するための最適な論理的手法

セキュリティー・アーキテクチャー策定において、ビジネス要件からセキュリティー要件を抽出することは、非常に複雑で難しい課題です。これまでもさまざまな試みが行われましたが、最近ではISO/IEC TR13335：GMITSが提唱しているリスク分析を中心とした手法を採用しています（図4）。手法は次の通りです。

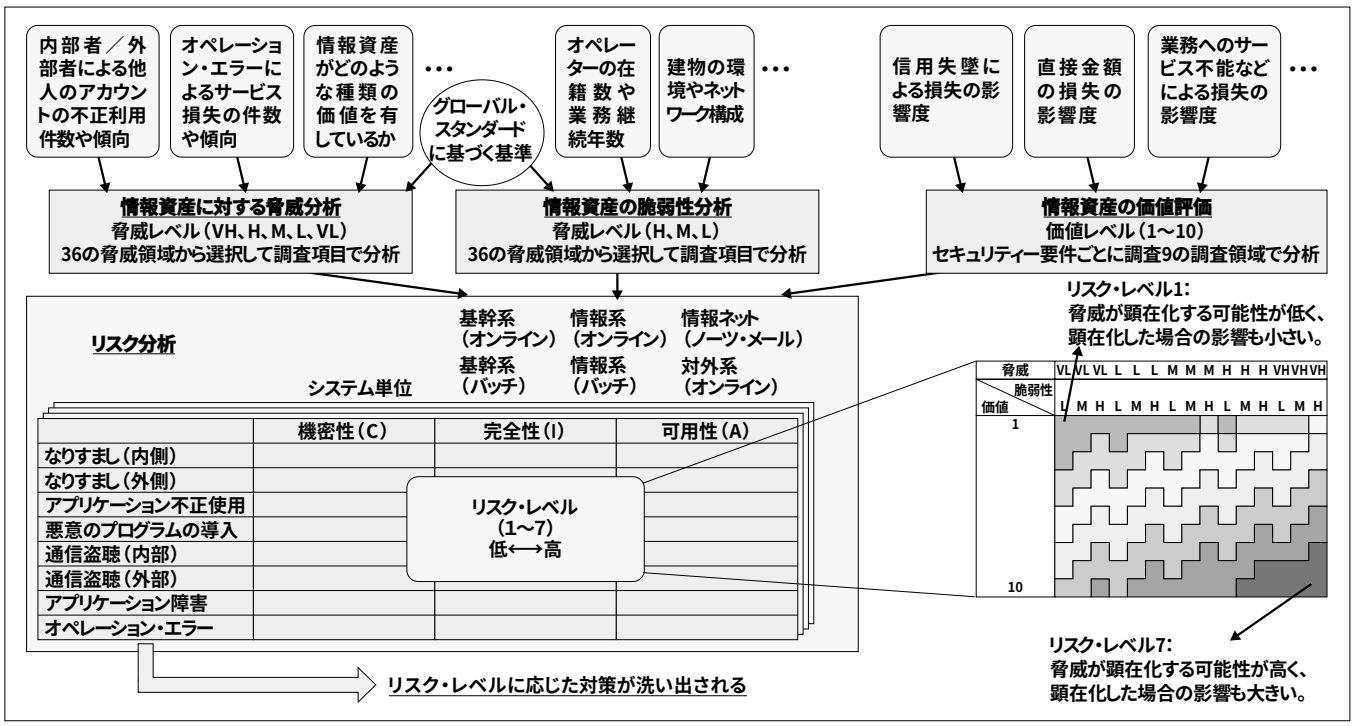
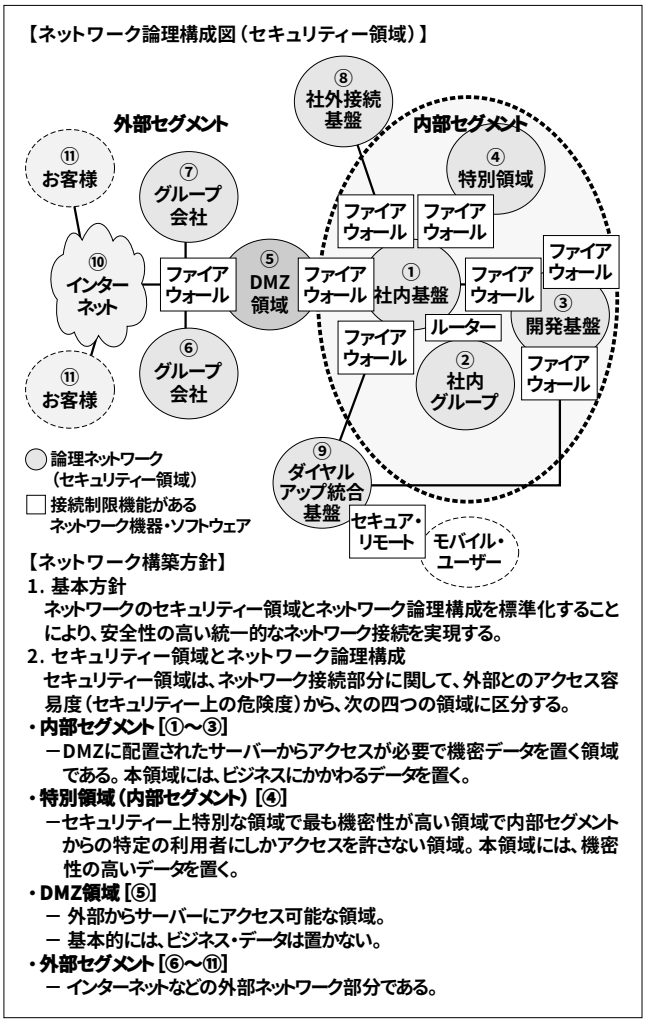


図4. リスク分析によるビジネス要件からセキュリティー要件の抽出



【ネットワーク構築方針】

1. 基本方針

ネットワークのセキュリティー領域とネットワーク論理構成を標準化することにより、安全性の高い統一的なネットワーク接続を実現する。

2. セキュリティー領域とネットワーク論理構成

セキュリティー領域は、ネットワーク接続部分に関して、外部とのアクセス容易度（セキュリティー上の危険度）から、次の四つの領域に区分する。

・**内部セグメント**［①～③］
－DMZに配置されたサーバーからアクセスが必要で機密データを置く領域である。本領域には、ビジネスにかかわるデータを置く。

・**特別領域（内部セグメント）**［④］
－セキュリティー上特別な領域で最も機密性が高い領域で内部セグメントからの特定の利用者にしかアクセスを許さない領域。本領域には、機密性の高いデータを置く。

・**DMZ領域**［⑤］
－ 外部からサーバーにアクセス可能な領域。
－ 基本的には、ビジネス・データは置かない。

・**外部セグメント**［⑥～⑪］
－ インターネットなどの外部ネットワーク部分である。

図5. ネットワーク論理構成図（例）

(1)業務システムと、そこで使用されている情報の定義

- **情報の価値は、機密区分などが目安となります。**

(2)情報の価値を定義し、価値レベルを把握

- **セキュリティー要件ごと（機密性・完全性・可用性）に情報の価値レベル（1～10レベル）を把握します。**
- **信用失墜による損失、訴訟による損失、直接金額の損失などによる損失を把握することで、資産の価値を分析します。**

(3)情報に与えられる脅威を設定し、脅威レベルを把握

- **36の脅威領域から情報に与えられる脅威を選択します。**
- **脅威レベルをVH、H、M、L、VLで設定します。**
- **内部者／外部者による他人のアカウントの不正利用件数と傾向、オペレーション・エラーによるサービス損失と傾向、情報資産の価値などの調査結果により判断します。**

(4)脅威に対する情報の脆弱性（ぜいじゃく）レベルを把握

- **脅威に対する脆弱性（ぜいじゃく）レベルをH、M、Lで設定します。**
- **オペレーターの在籍数や業務継続年数、建物、環境やネットワーク構成などの調査結果により判断します。**

(5)情報資産の価値レベル・脅威レベル・脆弱性（ぜいじゃく）レベルにより、リスク・レベルを把握

3.4. 構築方針

(1)ネットワーク論理構成の考え方

システムおよびネットワーク環境における脅威を想定するために、セキュリティー領域とネットワーク論理構成の標準を定義し、

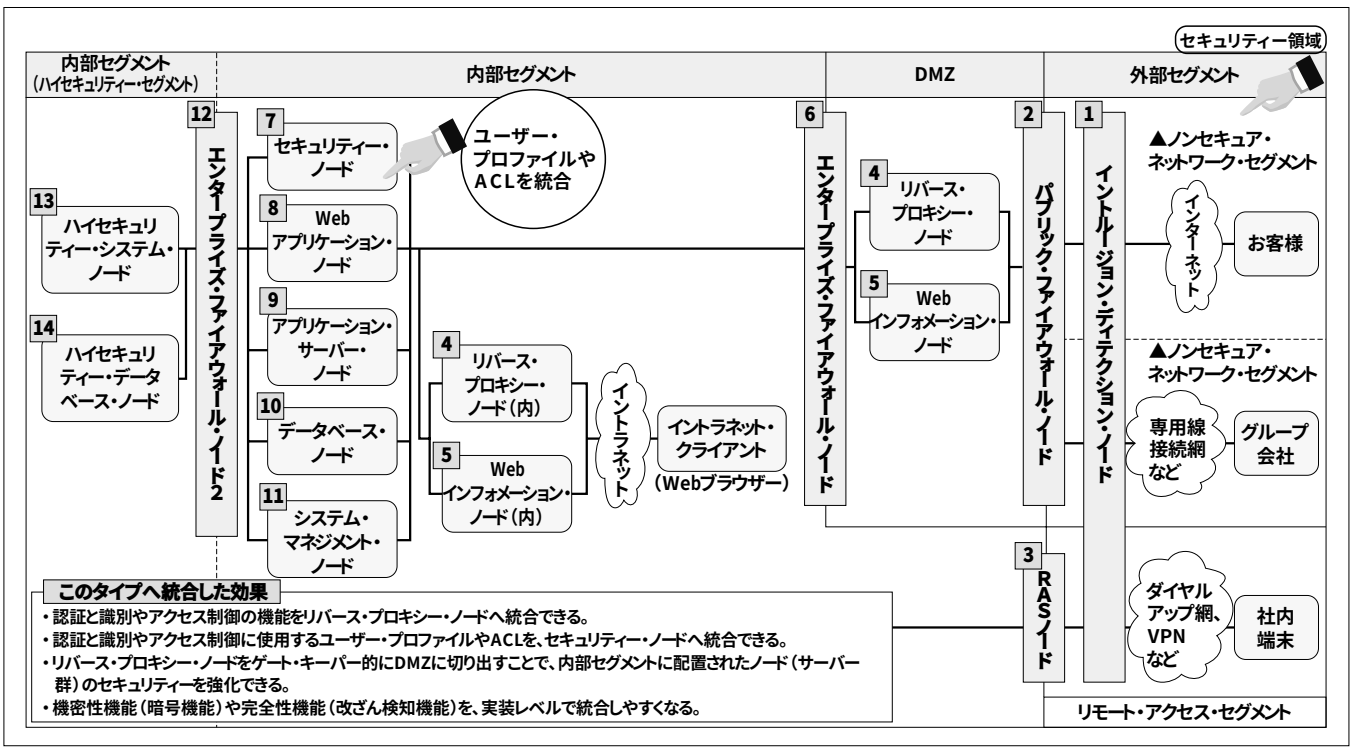


図6. システム論理構成図（例）

安全性の高い統一的なネットワーク接続を実現します(図5)。

(2)システム論理構成の考え方

セキュリティー領域やネットワーク論理構成に基づき、アプリケーション・システムを通した全体のシステム論理構成を考えることで、セキュリティー・サービス機能要件を満足するセキュアなセキュリティー・システム基盤を構築できます(図6)。

4. 提案したアーキテクチャー技法の効果と今後の計画

4.1. 今回の方法の評価および効果

今回の方法は、セキュリティー・アーキテクチャー策定にリスク分析の手法を取り入れたものです。それにより、ビジネス要件からセキュリティー要件を効果的に抽出できました。セキュリティー・アーキテクチャーにおいて、セキュリティー要件の抽出は最も重要なテーマです。

リスク分析の導入により、次のような効果が期待できます(図7)。

- ビジネス要件やセキュリティー・ポリシーの方針といった企業の意向を、セキュリティーの技術方針や管理方針まで一貫性を持って反映させることが可能となります。
- フレームワークとして体系的なアーキテクチャーにのっとっているため、機能的に見ても漏れのない技術標準の設定が可能となります。
- セキュリティー確保のための技術標準を策定できます。こうして出来上がった企業独自のセキュリティー・アーキテクチャーは一回限りのものではなく、更新していくことで普遍的に活用できます。
- 新規のアプリケーション開発やシステム開発において、セキュリティーの状態維持のために何をしなければならないかが明確になります。

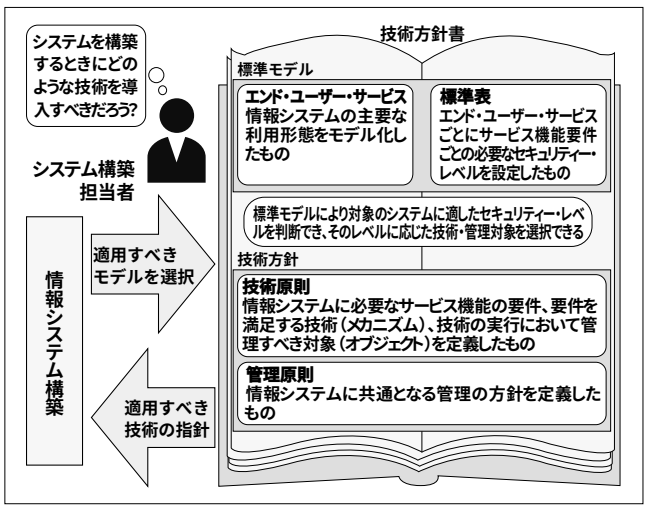


図7. セキュリティー・アーキテクチャー(技術方針書)策定の効果

4.2. 今後の計画

セキュリティーの重要性が一段と増している中で、セキュリティー・ポリシーをシステムにより実現するためにセキュリティー・アーキテクチャーの策定の要求が増してきています。従来、ビジネス要件からセキュリティー・サービス要件へ展開するコンセプチュアル・アーキテクチャーが中心に実施される傾向にありましたが、今後は、早急にシステム化を図るために、システムの構築に近いコンポーネント・アーキテクチャーまでを実施する必要が生じています。

主にコンサルティングで実施するコンセプチュアル・アーキテクチャーにおいて、お客様のビジネス要件から技術方針の策定まで、一貫したアーキテクチャーの確立を必要とする方々に、本論文が真に有効であることを心から願っています。

(ページ数および表記上の観点から、著者の了解を得て編集部にて手を入れてあります)

[参考文献]

[1] IBM Security Architecture (SC28-8135)

[2] ISO/IEC TR13335-1:GMITS(Guidelines for the management of IT Security)

[3] ISO 7498-2:Security Architecture