ITセキュリティ要件の抽出手法
―オペレーショナル・モデリングとセキュリティ・メソッドの統合―

大津留 史郎

An Abstract Method for IT Security Requirements
– Integration of Operational Modeling and Security Methods –

Shiroh Ohtsuru

IT基盤アーキテクチャーの設計手法の一つとして, IBMにはオペレーショナル・モデリング（OM：Operational Modeling ）という手法がある. また, IBMには複数のITセキュリティ・アーキテクチャーの設計手法（セキュリティ・メソッド）がある. しかしながら, OMとセキュリティ・メソッドとの関連性は十分に整理されておらず, セキュリティ専門家でないITアーキテクトがITセキュリティ要件を抽出し, IT基盤アーキテクチャーに反映させる事は困難な状況である.

本論文では, この課題を解決するために, ITセキュリティ要件の位置づけを整理し, セキュリティ・メソッドとOMの内容を分析し, これらの手法の統合を提案する. 本論文で提案する手法は, OMの手法を基本とすることで, セキュリティを専門としないITアーキテクトにとっても理解し易い実践的な手法となっている.

There is a design technique at IBM called Operational Modeling (OM) as one of the design technique for IT infrastructure architecture. However, the correlation between OM and security methods is not sufficiently organized, and IT architects who are not security specialists are sampling security requirements, making their reflection in IT infrastructure architecture difficult. In this article, we will straighten out the positioning of IT security requirements, analyze the details of security methods and OM, and propose their integration in order to solve this issue. The proposed method is based on OM, and is therefore a practical method easily understandable by IT architects not specializing in security.

Key Words & Phrases：ITセキュリティ・アーキテクチャー, IT基盤アーキテクチャー, セキュリティ・メソッド, オペレーショナル・モデリング, アーキテクチャー
IT security architecture, IT infrastructure architecture, security method, operational modeling, architecture

1. はじめに

「ITセキュリティのために何をすればよいか？」,「このシステムにおけるITセキュリティ要件は何か？」,「法規制や業界標準に準拠するためにどんな技術を導入すべきか？」. これらの問いは, 提案段階やシステム開発の上流工程においてしばしば議論される課題であるが, これらの課題に対して根拠ある明確な解を提示できる技術者は非常に少ない. これは, IT業界の誰もが感じており, 統計的な根拠を示すまでもない事実であろう. ここで, ITセキュリティとは, 企業・組織が取り組むべき情報セキュリティのうち, ITシステムにより実現する部分であり, ネットワークセキュリティを含む領域である. ITセキュリティを巡る議論と困難の背景には, ITセキュリティが持つ次のような性質があると考えられる.

提出日：2007年3月16日　　再提出日：2007年7月19日

1.1 ITセキュリティは新しいテーマである

ITセキュリティのテーマは, 1990年頃から存在していた[1]が, 日本国内において盛んに議論され始めたのは, 2000年の官庁ホームページ改竄事件以降であり, 総論及び各論においてIT業界における共通理解が確立できていない. これに対して, ITシステムの高可用性やパフォーマンスは1990年代以前から継続的に議論されてきており,「二重障害は発生頻度が低いため, 投資対効果の観点から想定しない」,「ボトル

ネックとなるコンポーネントを見つけて重点的に管理する」といった共通理解が確立されている.

1.2 変化する前提条件1;想定する脅威の変化

2000年以前において, ITセキュリティが想定すべき脅威は, TCP/IPのプロトコルそのもの及びTCP/IPプロトコルの実装上の脆弱性を悪用する攻撃, コンピュータウィルスといったものであったが, 2001年前後においてはソフトウェアやWebアプリケーションの脆弱性を悪用したWebサイトへの侵入(またはホームページの改竄)を考慮する必要性が強まり, 2004年頃からはシステム管理者の内部犯行による情報漏洩も考慮する必要性が強まっている.

1.3 変化する前提条件2;関連する法規制の変化

ITセキュリティが議論され始めた当初, 前提として考慮すべき法律は2000年2月13日に施行された不正アクセス禁止法[2]及び既存の刑法・商法であったが, 現在は2005年4月1日に施行された個人情報保護法[3]及び2008年4月1日以後に開始される事業年度から適用される予定の金融商品取引法(日本版SOX法)[4]を考慮する必要が出てきている.

1.4 断片的な疑問に対する完全な解の要求

実際に発生したセキュリティ事件は, センセーショナルな表現の報道記事として伝えられることが多い. この結果, ITシステムのオーナーや経営者は, 特定の事件の原因となった脅威やリスクについての断片的な知識を持つようになり, 技術者はシステムオーナーや経営者からの断片的な疑問に対して網羅的な説明を行わなければならない立場に立たされている.

こういった困難に対する1つの解として, ITセキュリティ要件を抽出し, ITセキュリティ・アーキテクチャーを設計する手法(セキュリティ・メソッド)が存在している. 一般的に論じられているガイドライン及びセキュリティ・メソッド([5][6])は, 実際のシステム設計への適用という観点からは抽象的であるが, IBMが持つ複数のセキュリティ・メソッド[7][8][9]には, 実際のシステム設計に適用された実績がある. しかしながら, IBMのセキュリティ・メソッドにおいても, 現状ではセキュリティ・メソッドを実践できるのは一部のセキュリティ専門家に限られている.

一方, IBMの一般的なITアーキテクトは, IT基盤アーキテクチャーの設計手法としてIBMのオペレーショナル・モデリング(OM:Operational Modeling[10][11])という手法を使い始めている. OMは, ITシステムに求められる要件が定義されている事を前提として, 物理的なロケーションとセキュリティゾーンに対して, アクター(システムの利用者, 関係する外部システム), データ, 機能, 各アクターに対するインターフェースそれぞれの配置と動的な振る舞いをシステムの運用的側面として定義するものである. しかしながら, OMの実践においてもシステムのITセキュリティ要件の抽出については, やはり一部のセキュリティ専門家に頼らざるを得ない点は同じなのが現状である.

本論文は, 従来の手法が持つこれらの課題を解決する事を目的とし, 一般的なITアーキテクトが理解しやすく, かつ実践可能な, ITセキュリティ要件抽出の手法を提案する.

以下, 2章でITセキュリティ要件の位置づけを明確化し, 3章でOMとセキュリティ・メソッドの手法を分析した後, 4章で2種類の手法の統合を提案する.

2. ITセキュリティ要件の位置づけ

本章では, ITセキュリティ要件の位置づけを明確にすることを目的に, システムに求められる要件と制約全体におけるITセキュリティ要件の位置づけ, 情報セキュリティ全体におけるITセキュリティ要件の位置づけ, 個人情報保護との関係について述べる. なお, SOX法対応及び内部統制から求められるITセキュリティ要件については, ProVISION内部統制特集[12]において取り扱われているため, 本論文の対象からは外しておく.

2.1 要件と制約全体から見たITセキュリティ要件の位置づけ

IBMがITアーキテクチャー設計等に適用している手法の体系であるGS Methodは, 要求工学に基づいてITシステムに求められる要件と制約を分類している. この分類において, ITセキュリティ要件は非機能要件の一部である品質要件の一つとして位置づけられている. ただし, それぞれの要件と制約は必ずしも整合性のあるものではなく, トレードオフの関係になるケースがある. このため, ITセキュリティ要件は必ずしも完全に充たされる訳ではない事に注意する必要がある.

また, しばしば「セキュリティは非機能要件ではなく機能要件ではないか」という疑問を投げかけられることがあるが, 本来機能要件とは, ITシステムに投資をする立場の経営者や, ITシステムのオーナーといったステークホルダーが明確に意識している要件を指す. 例えば, ビジネスプロセス上, 取引の証拠を残す必要性をステークホルダーが明確に意識している場合は, 当該要件は機能要件となる.

2.2 情報セキュリティ全体から見たITセキュリティ要件の位置づけ

「情報セキュリティのために何をすべきか？」, この問いに対する答は, ISO/IEC 17799:2005［13］において, 11の箇条を詳細化した39の管理目的及びそれらを達成するための133の管理策として明確に記述されている. ISO/IEC 17799の記述内容は, 企業・組織が情報セキュリティのために実施すべきセキュリティ対策全体であるが, ISO/IEC 13335（GMITS：Guidelines for the Management for IT Security）［5］ではセキュリティ対策全体を, 物理的セキュリティ対策, 人的セキュリティ対策, 技術的セキュリティ対策の3つに分類している. すなわち, ITセキュリティ要件は, 企業・組織が実施すべき技術的セキュリティ対策に該当する. **図1**に情報セキュリティ対策の分類と具体例を示す.

ITが関与し得る範囲

	防止・低減	検知	回復
技術的(論理的)セキュリティ対策	利用者の識別・認証、アクセス制御、データ暗号化、ゾーニング、コンテンツフィルタリング、ハードニング、検疫ネットワーク アンチウィルス、セキュアコーディング PC操作制限、プリンターセキュリティ	ログ管理、IDS/IPS、データ改竄検知	バックアップ/リストア、システム二重化
人的(組織的)セキュリティ対策	ID・権限管理、資産・構成管理	資産・構成管理、	事業継続計画
	開発・保守プロセスの整備、社員教育、守秘義務契約	報告体制の確立	
物理的(設備的)セキュリティ対策	入退室管理、UPS・自家発電装置、データセンターの立地、塀・壁、	監視カメラ、警報設備	消火設備

図1. 情報セキュリティ対策の分類と具体例

2.3 個人情報保護とセキュリティとの関係

個人情報のセキュリティは, 個人情報保護の一部であり, セキュリティの確保だけでは個人情報保護の要件は満たされない.

この主張の根拠は, 日本の個人情報保護法制定の基となったOECDのプライバシー8原則［14］にある. 1998年10月, EUは「データ保護指令」［15］を施行し, 1980年9月にOECDが採択したプライバシー8原則を遵守していない他国への個人データの移動を禁じた. この動きを受けて, 米国及び日本はOECDのプライバシー8原則に従って個人情報保護法を制定・施行した. OECDのプライバシー8原則と日本の個人情報保護法との対応づけを**図2**に示す.

図2は, 個人情報のセキュリティ確保を求める安全保護の原則がOECDのプライバシー8原則の1つにすぎないことを示している. 従って, 情報セキュリティ管理の体制・規程と個人情報保護の体制・規程は本来別々に行うべきものであり, ITセキュリティ要件を抽出する際は, 個人情報保護の要件をどこまでとりこむかを明確にする必要がある. 筆者の経験でも, CSO（Chief Security Officer）と CPO（Chief Privacy Officer）に異なる責任者が任命されていたり, 異なる所管部署と規程類による管理が行われていたりするケースがあった. また, このようなケースにおいては, セキュリティの原則以外の7つの原則は, ITシステムの機能ではなく, 業務運用のプロセスとして実装されているケースが多かった.

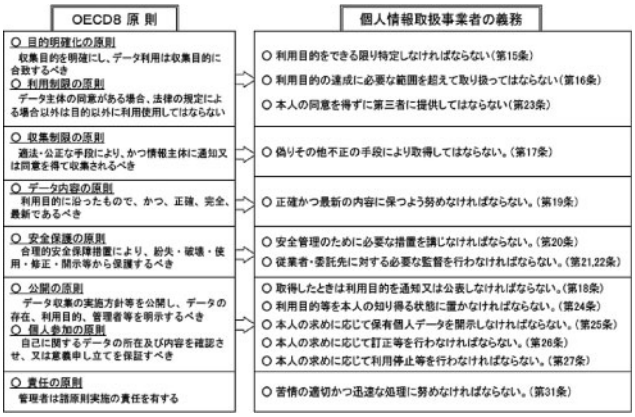

図2. OEECD8原則と日本の個人情報保護法
（首相官邸「個人情報保護法の解説」
（http://www5.cao.go.jp/seikatsu/kojin/kaisetsu/pdf）より転載）

3．IBMのアーキテクチャー設計手法とその課題

本章では, IT基盤アーキテクチャーの設計手法であるOMと, IBMのセキュリティ・メソッドについて概要と課題を述べる.

3.1 OMにおけるITセキュリティ要件の扱い

OMでは, 次の作業手順によりITアーキテクチャーの設計を行う.

(1)業務アプリケーションの機能に対して求められる機能要件を実現するための概念運用モデル（COM：Conceptual Operational Model）の作成
(2)COMに対して機能要件以外の要件である非機能要件を反映した, 仕様運用モデル（SOM: Specified Operational Model）の作成
(3)SOMに基づいて製品選択を行い, 選択した製品をSOMに適用した物理運用モデル（POM: Physical Operational Model）の作成

また, SOM作成作業の品質確保と効率化のために, IBMは実績あるITアーキテクチャーを集めて抽象化した知的資産であるebRA（e-business Reference Architecture）及び ISRA（Infrastructure Solution Reference Architecture）を活用している.

しかしながら, ITセキュリティ要件及びITセキュリティ・アーキテクチャーについては, 一部のセキュリティ技術者に頼っているのが現状であり, セキュリティを専門としないITアーキテクトがITセキュリティ要件を抽出してSOMに反映する事ができるようになるためには, 次の課題を解決する必要がある.

課題1：ITセキュリティ要件を抽出する手法の実践的なガイドが必要である
課題2：COMに追加配置する具体的なセキュリティ対策技術についてのガイドが必要である

3.2　日本IBMにおけるセキュリティ・メソッド

日本IBMにはITセキュリティ・アーキテクチャーを設計するための複数の手法が存在している. いずれの手法も, 次の作業を実施する点で共通している.

(1) ロケーションを含むノード（物理的にはサーバや端末などのコンピュータに該当するが, ここでは, より抽象化して, データ, 機能, ユーザインターフェース, 外部システムインターフェース及びハードウェアの集合体と定義する）, データ, 及びアクターの配置, 通信インターフェース, データフローを洗い出し, システムモデルを描く
(2) システムモデルに対して, リスク（または脅威）の洗い出しと評価（リスク分析）を行う
(3) 重要なリスク（または脅威）に対する対抗策を選定してシステムモデルに追加配置し, セキュリティ・アーキテクチャーを完成させる

筆者の経験から, セキュリティ・メソッドには, 次の課題がある.

課題3：大規模システムに対して, システム全体を鳥瞰するモデルを描く作業が困難である
課題4：セキュリティ標準や規程の策定時に, 抽象度を上げたシステムモデルに対するリスク分析が行われており, システムオーナーからはリスク分析の繰り返しによる無駄が発生しているように見える

4．OMとセキュリティ・メソッドの統合

本章では, OMとセキュリティ・メソッドとを統合し, 3章で述べた課題1～4を解決する新しい手法について述べる.

4.1　OMとセキュリティ・メソドロジーの統合（課題3の解決）

3.2における(1)の作業は, OMにおいてCOMを作成する作業にほぼ一致する. 従ってCOMに必要な情報を追加してリスク分析を行い, その結果であるITセキュリティ要件を満たすためのセキュリティ機能を持つノードを追加してSOMを作成する事で, OMとセキュリティ・メソッドを統合することができる. なお, COMに追加するべき情報は次の2つである.

(1) 各データに対する重要度評価
（セキュリティポリシーにおける情報分類）
(2) データフロー

セキュリティ・メソッドをOMに統合した手法を**図3**に示す.

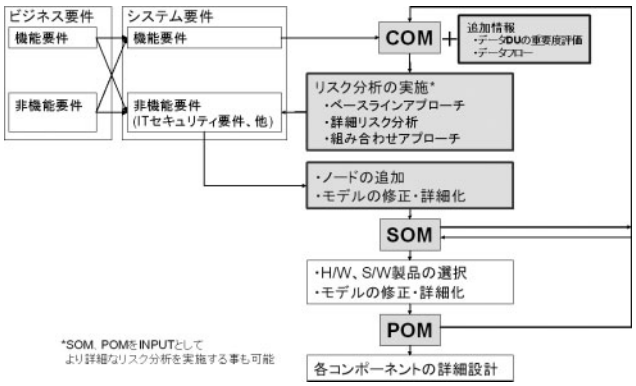

図3.　OMとセキュリティ・メソッドの統合

4.2　リスク分析の実践的手法（課題1及び4の解決）

本節では, 課題1及び課題4の解として, リスク分析の実践的手法について述べる.

4.2.1　詳細リスク分析の実践的手法（課題1の解決）

3.2における(2)の作業は, GMITSにおいて詳細リスク分析として定義されている. 詳細リスク分析の実践において難しいのは, いかにしてリスクの洗い出しと評価を行うか（課題1）である. ここでは, この課題に対する解として, 筆者が実践している手法を紹介する.

リスク洗い出しの考え方の例を**図4**に示す.

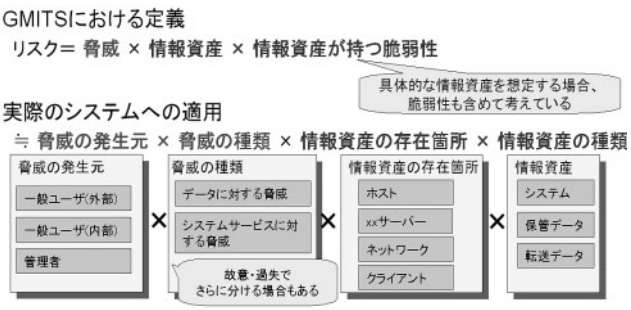

図4.　情報セキュリティ対策の分類と具体例

図4において, 脅威の発生元はCOMにおけるアクターと各ロケーションに存在する第三者であり, 脅威の種類にはGMITSの付録に記述されている脅威の例が適用可能である. 図4の考え方を基にリスク分析を行った例を**表1**に示す.

表1. リスク洗い出しの実践例

情報資産(脆弱性を含む)			脅威			リスク例
箇所(イントラネット)			発生元	脅威の種類		
種別	コンポーネント	種類(※1)	発生元	大項目	小項目	
端末・プリンタ	運用員用端末	機密度Ｉの情報(転送データ	運用員	システム停止	DoS攻撃	運用員が運用員用端末に対してDoS攻撃を行い、運用員用端末を停止させ
端末・プリンタ	運用員用端末	機密度Ｉの情報(転送データ	運用員	システム停止	不正操作	運用員が運用員用端末に対して不正操作を行い、運用員用端末を停止させ
端末・プリンタ	運用員用端末	機密度Ｉの情報(転送データ	運用員	不正アクセス	なりすまし	運用員が運用員用端末に対してなりすましによる不正アクセスを行う
端末・プリンタ	運用員用端末	機密度Ｉの情報(転送データ	運用員	不正アクセス	脆弱性の悪用	運用員が運用員用端末に対して脆弱性を悪用して不正アクセスを行う
端末・プリンタ	運用員用端末	機密度Ｉの情報(転送データ	運用員	不正コード	ウィルス	運用員が(故意または過失で)運用員用端末に対してウィルスを送信する
端末・プリンタ	運用員用端末	機密度Ｉの情報(転送データ	運用員	不正コード	スパイウェア	運用員が(故意または過失で)運用員用端末に対してウィルスを送信する
端末・プリンタ	運用員用端末	機密度Ｉの情報(転送データ	運用員	改竄	アクセス制御の不備	運用員が本来アクセスできないはずの運用員用端末のデータを改竄する
端末・プリンタ	運用員用端末	機密度Ｉの情報(転送データ	運用員	漏洩	アクセス制御の不備	運用員が本来アクセスできないはずの運用員用端末のデータを閲覧する
端末・プリンタ	運用員用端末	機密度Ｉの情報(転送データ	運用員	漏洩	記憶媒体による漏洩	運用員が記憶媒体により運用員用端末のデータを持ち出す
端末・プリンタ	運用員用端末	機密度Ｉの情報(転送データ	運用員	漏洩	帳票による漏洩	運用員が帳票により運用員用端末のデータを持ち出す
端末・プリンタ	運用員用端末	機密度Ｉの情報(転送データ	運用員	漏洩	(正規の)通信による漏洩	運用員が通信により運用員用端末のデータを外部に送信する
端末・プリンタ	運用員用端末	機密度Ｉの情報(転送データ	運用員	漏洩	盗聴による漏洩	運用員が盗聴により運用員用端末のデータを外部に送信する
端末・プリンタ	運用員用端末	機密度Ｉの情報(転送データ	運用員	消去	アクセス制御の不備	運用員が本来アクセスできないはずの運用員用端末のデータを消去する
ネットワーク	オフィスLAN	機密度Ｉの情報(転送データ	運用員	システム停止	DoS攻撃	運用員がオフィスLANに対してDoS攻撃を行い、オフィスLANを停止させる
ネットワーク	オフィスLAN	機密度Ｉの情報(転送データ	運用員	システム停止	不正操作	運用員がオフィスLANに対して不正操作を行い、オフィスLANを停止させる
ネットワーク	オフィスLAN	機密度Ｉの情報(転送データ	運用員	不正アクセス	なりすまし	運用員がオフィスLANに対してなりすましによる不正アクセスを行う
ネットワーク	オフィスLAN	機密度Ｉの情報(転送データ	運用員	不正アクセス	脆弱性の悪用	運用員がオフィスLANに対して脆弱性を悪用して不正アクセスを行う
ネットワーク	オフィスLAN	機密度Ｉの情報(転送データ	運用員	不正コード	ウィルス	運用員が(故意または過失で)オフィスLANに対してウィルスを送信する
ネットワーク	オフィスLAN	機密度Ｉの情報(転送データ	運用員	不正コード	スパイウェア	運用員が(故意または過失で)オフィスLANに対してウィルスを送信する

洗い出されたリスクの評価手法として, 筆者はGMITSに記述されているリスク評価手法ではなく, リスクマネジメント論における, 発生頻度と影響度に基づく定性評価の手法を適用している. **図5**にリスク評価の考え方の例を, また, この考え方に基づいて表1で洗い出したリスクを評価した例を**表2**に示す.

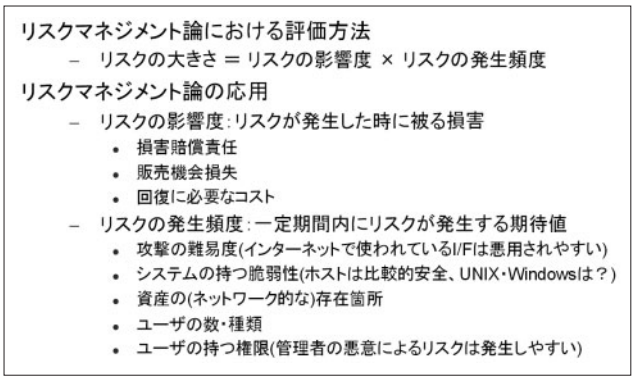

図5. リスク評価の考え方の例

表2. リスク評価の実践例

				脅威			リスク評価					
機密度最大のデータ		発生元		脅威の種類						発生頻度		
機密度	種別	発生元	対象	大項目	小項目	影響度評価	アクセス容易性	背反性	ITスキル必要性	発生元スキル	発生頻度評価	総合評価
2	保管データ	運用員	A	システム停止	DoS攻撃	2	5	5	Y	3	60%	1
2	保管データ	運用員	A	システム停止	不正操作	2	5	5	N	3	100%	2
2	保管データ	運用員	C	不正アクセス	なりすまし	5	5	5	N	3	100%	5
2	保管データ	運用員	C	不正アクセス	脆弱性の悪用	5	5	5	Y	3	60%	3
2	保管データ	運用員	A	不正コード	ウィルス	5	5	5	N	3	100%	5
2	保管データ	運用員	C	不正コード	スパイウェア	5	5	5	N	3	100%	5
2	保管データ	運用員	I	改竄	アクセス制御の不備	5	5	5	N	3	100%	5
2	保管データ	運用員	C	漏洩	アクセス制御の不備	5	5	5	N	3	100%	5
2	保管データ	運用員	C	漏洩	記憶媒体による漏洩	5	5	5	N	3	100%	5

4.2.2 GMITSに基づく補完：ベースラインアプローチの追加（課題1及び課題4の解決）

3.2で述べたセキュリティ・メソッドは, GMITSで定義されている詳細リスク分析を実施する手法であるが, GMITSには詳細リスク分析の他に, ベースラインアプローチというもう一つのリスク分析手法が定義されている. 従って, これまで述べてきた手法にベースラインアプローチを追加する事で, セキュリティの観点からより網羅性が高く実践的な手法とする事ができる.

ベースラインアプローチは, 想定するシステム, すなわちCOMに対して, 既存の規程や標準をチェックリストとして適用することで, リスク分析を簡易に実施する手法である. これにより追加すべきセキュリティ機能がITセキュリティ要件として導き出される. 一般的に, ベースラインアプローチは詳細リスク分析と比較して作業工数が少なくて済むという長所を持っており, 遵守すべきセキュリティ標準や規程が明確になっているケースにおいては, ITセキュリティ要件抽出の有効な手法となる. **表3**にベースラインアプローチの実践例を示す.

表3.　ベースラインアプローチの実践例

項目		記述内容	システム対応要否	対応評価	評価理由	対応方法(案)
1.1情報の格付け	(1)情報の格付け	(a) 情報の格付け及び取扱制限の基準並びに格付け及び取扱制限を明示する手順は別紙のとおりとする。	○	△	・格付け、取扱制限は明示されていない	・格付け、取扱制限の明示機能の実装
2.1 情報の作成と入手	(1)業務以外の情報の作成又は入手の禁止	(a) 事務従事者は、事務の遂行以外の目的で、情報システムに係る情報を作成又は入手しないこと。	×	N/A	N/A	N/A
2.1 情報の作成と入手	(2)情報の作成又は入手時における格付けの決定と取扱制限の検討	(a) 事務従事者は、情報の作成時に当該情報の属性に応じて格付けを行い、あわせて取扱制限の必要性の有無を検討すること。	×	N/A	N/A	N/A
2.1 情報の作成と入手	(2)情報の作成又は入手時における格付けの決定と取扱制限の検討	(b) 事務従事者は、省外の者が作成した情報を入手し、管理を開始する時に当該情報の属性に応じて格付けを行い、あわせて取扱制限の必要性の有無を検討	×	N/A	N/A	N/A
2.1 情報の作成と入手	(3)格付けと取扱制限の明示	(a) 事務従事者は、情報の格付けを、当該情報の参照が許されている者が認識できる方法を用いて明示し、必要に応じて取扱制限についても明示すること。	○	△	・格付け、取扱制限は明示されていない	・格付け、取扱制限の明示機能の実装
2.1 情報の作成と入手	(4)格付けと取扱制限の継承	(a) 事務従事者は、情報を作成する際に、既に格付けされた情報を引用する場合には、当該情報の格付け及び取扱制限を継承すること。	×	N/A	N/A	N/A
2.1 情報の作成と入手	(5)格付けと取扱制限の変更	(a) 事務従事者は、情報の格付けを変更する必要性があると思料する場合には、当該情報の作成者又は入手者に相談すること。相談された者は、格付けの見直しを行う必要があると認めた場合には、当該情報に対して妥当な格付けを行う	×	N/A	N/A	N/A

ベースラインアプローチの実践に際しては次の点に注意する必要がある.

(1)基準となる標準・規程の解釈

ベースラインアプローチの基準となる標準・規程は, 様々なシステムに適用する事を想定しているため, 抽象的な表現で記述されている. 従って, ベースラインアプローチを実施する際には, 標準・規程に記述されている要求項目の解釈について, システムオーナーと合意する必要がある.

(2)規程遵守と実質的なセキュリティの違い

ベースラインアプローチの基準となる標準・規程の要求項目の中には, 技術的に見ると必ずしも有効なセキュリティ対策ではないものがある. このような場合, ベースラインアプローチの目的が, 標準・規程の遵守のみであるか, 技術的に有効なITセキュリティ要件を導き出す事を含むものであるかによって, (1)で述べた基準の解釈やITセキュリティ要件に違いが出てくる.

(3)運用対処とシステム対処の切り分け

ベースラインアプローチの基準とする標準・規程の要求項目は, 必ずしも特定のセキュリティ対策を求めているものではない. このため, 項目によっては人的セキュリティ対策(運用)でも技術的セキュリティ対策(システム)でも対応可能であり, どちらで対処するのか判断しなければならないケースがある. このような場合は, まず技術的対策が可能なものは全てITセキュリティ要件としておき, コストの制約を考慮する際に運用対処とシステム対処のどちらを選択するのか判断するとよい.

(4)ITセキュリティ要件の優先順位づけ

詳細リスク分析では, リスク評価結果に基づいてITセキュリティ要件を優先順位づけすることが可能である. 一方, ベースラインアプローチを実施する場合は, ITセキュリティ要件を優先順位づけする基準がないため, 何らかの基準を設けてITセキュリティ要件の優先順位づけを行う必要がある. 筆者がベースラインを実践した際に行ったITセキュリティ要件の優先順位づけの例を**図6**に示す.

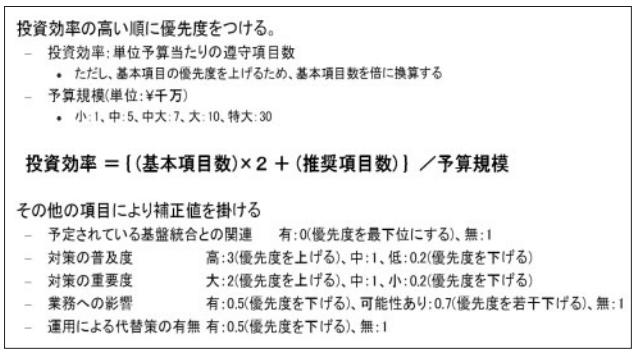

図6.　ITセキュリティ要件の優先順位づけの例

ただし, ベースラインアプローチは, 既存のセキュリティ標準や規程を基準とするため, セキュリティ標準や規程が想定している標準的なシステムに対するリスク分析手法としては有効であるが, 検討対象のシステム固有の箇所についてはリスク分析の精度が低くなるという欠点がある. そこで, 2つのリスク分析手法の応用として, 検討対象のシステムの標準的な箇所に対してはベースラインアプローチを適用し, 固有の箇所に対しては詳細リスク分析を適用する手法がある. この手法はGMITSで組み合わせアプローチとして定義されているもう一つのリスク分析手法であり, 組み合わせアプローチを使うことでリスク分析の精度を確保しつつ作業工数を少なくする事が可能である. (GMITSは, ベースラインアプローチ, 詳細リスク分析, 組み合わせアプローチの3つのリスク分析手法を定義している)

また, リスク分析のその他の実践的手法として, 複数の基準を適用したベースラインアプローチを行う手法や, ベースラインアプローチと詳細リスク分析の両方を行う手法もある.

表4. セキュリティ対策技術の分類

セキュリティ対策技術	対象箇所	セキュリティ対策技術の具体例
利用者識別	業務ユーザ、システムユーザ	ユーザ個人にIDを割り当てる、特権IDの貸し出し管理
ID管理	業務ユーザ、システムユーザ	ディレクトリによる統合ID管理、人事DBとの連携
利用者認証	業務ユーザ、システムユーザ	Tivoli Access Managerによる認証、OSによるユーザ認証
アクセス制御	業務ユーザ、システムユーザ	Tivoli Access Managerによるアクセス制御、 OSによるアクセス制御(セキュアOS)
権限管理	業務ユーザ、システムユーザ	権限管理アプリケーション
ゾーニング	ネットワーク・サーバ構成	ゾーニングルールの定義、 ゾーニングルールに従ったネットワーク・サーバ配置
Webアプリケーションセキュリティ	Webアプリケーション	コーディングルール、Web Application Firewall、 コードチェックツール
コンテンツフィルタリング	Web、メール通信	ウィルスフィルタリング、URLフィルタリング、 スパムフィルタリング、メール容量制限
PCデータ操作制限	クライアントPC	秘文、Alliss
否認防止	業務アプリケーション	デジタル署名
ウィルス対策	Windows PC、サーバ	アンチウィルス
ハードニング	PC、ネットワーク機器、サーバ	不要なサービス・アプリケーション・ファイルの削除、 デフォルト設定の見直し、最新パッチ適用
検疫ネットワーク	構内LAN	検疫ネットワーク、認証LAN、 MACアドレスフィルタリング、ポートセキュリティ
構成・資産管理	PC、ネットワーク機器、サーバ	H/W・S/W構成管理
ディスク・メモリー管理	サーバ	ディスク・メモリー使用率の監視
保管データ暗号化	重要度の高い保管データ	外部媒体暗号化、ファイル暗号化、DB暗号化、暗号化API
転送データ暗号化	重要度の高い転送データ	VPN、IPSec、ネットワーク暗号化装置、 暗号化通信機能(SSLなど)
冗長化	ネットワーク機器、サーバ	ネットワーク・サーバの冗長構成、RAID、 バックアップ機器の確保(コールドスタンバイ)
ログ管理	PC、ネットワーク機器、サーバ	ログ取得・保管・分析
データ改竄検知	重要度の高い静的データ	デジタル署名、Tripwire
侵入検知・遮断	攻撃のリスクが高いネットワーク	IDS/IPS
異常検知	PC、ネットワーク機器、サーバ	ノード・プロセス稼動監視、アラート検知
バックアップリストア	重要度の高いデータ、システムイメージ	データ、システムの定期バックアップ、リストア手順確立
セキュアプリント	プリンター	プリンターセキュリティソリューション、認証プリント

4.3 セキュリティ対策技術の分類(課題2の解決)

図3において, リスク分析の後に行うノード追加の作業は, リスク分析の結果から抽出されたITセキュリティ要件を満たす機能を, COMに追加配置する作業である. しかしながら, 現状ではセキュリティの専門家でない技術者が具体的な製品や技術を想定してTechnical NodeをCOMに追加配置することは困難である(課題2). この困難に対する解として, 筆者が複数の実プロジェクトで適用してきた, 現在実装可能なセキュリティ対策技術の分類を**表4**に示す.

表4は, SOMや既存システムに対して, セキュリティ対策に漏れがないかを点検するための簡易チェックリストとしても活用できる. また, ベースラインアプローチにおいて基準とすべき標準・規程が複数存在する場合, 技術的セキュリティ対策に関する項目をこのセキュリティ対策技術の分類に基づいて分類・整理する事で, 要求項目をまとめることが可能である.

5. おわりに

本論文は, OM及びセキュリティ・メソッドを実践する際の課題を解決する事を目的とした, OMとセキュリティ・メソッドの統合の提案である. 本論文が解決を目指した課題とは, ITセキュリティ・アーキテクチャーの設計を一部のセキュリティ専門家に頼っている現状であり, 本来であれば, ITアーキテクトであれば誰でもが, ITセキュリティ要件を包含したITアーキテクチャーを設計できるべきである.

本論文で提案した手法は, 基本としてのOMの手法に, 既存のセキュリティ・メソッド及びベースラインアプローチの実践的手法を組み合わせたものであり, セキュリティを専門としないITアーキテクトにとっても理解し易い実践的な手法となっている. 特に, 本論文の2章及び4章は, 筆者が実プロジェクトで実践してきたノウハウを集約した内容であり, 是非参考にして頂きたい内容である.

謝辞

本論文の執筆にあたり, 多数のアドバイスを頂いた, 日本アイ・ビー・エムの大西克美ICP, 大嶽隆児ICP, そして渡辺芳明技術理事に感謝致します.

参考文献

[1] ISO 7948-2, Information processing systems- Open Systems Interconnection- Basic reference model- Part2: Security architecture（1989）
[2] 不正アクセス行為の禁止等に関する法律, http://www.ipa.go.jp/security/ciadr/law199908.html（2007.7.19）
[3] 個人情報の保護に関する法律, http://www5.cao.go.jp/seikatsu/kojin/houritsu/index.html（2007.7.19）
[4] 貸金業の規制等に関する法律等の一部を改正する法律, http://www5.cao.go.jp/seikatsu/kojin/houritsu/ index.html（2007.3.16）
[5] ISO/IEC 13335, Guidelines for the Management for IT Security（2004.11.19）
[6] Trustworthy Refinement Through Intrusion-Aware Design, http://www.sei.cmu.edu/publications/documents/ 03.reports/03tr002.html（2007.7.19）
[7] J.J Whitmore; "A method for designing secure solutions," IBM System Journal Vol.40（2001）
[8] 渡辺芳明: "セキュリティを確保したシステムを構築するための方法論, " ProVISION No.29（2001.4）
[9] 大西克美; "上流工程におけるセキュリティ・メソドロジーの実践," ProVISION No.42（2004.7）
[10] 長井浩; "情報システムの設計思想　第5回運用基盤的側面のモデル化（オペレーショナル・モデリング）," 日経ITプロフェッショナル, pp.145-153（2004.7）
[11] 山本久好, 榊原彰; "オペレーショナル・モデリングにおける非機能要件の効果的検証方法," ProVISION No.35, pp.85-92（2004）
[12] ProVISION Spring 2006 No.49, http://www-06.ibm.com/jp/provision/no49/index.html
[13] ISO/IEC 17799, Information technology –Security techniques– Code of practice for information security management（2005）
[14] プライバシー保護と個人データの国際流通についてのガイドラインに関するOECD理事会勧告, http://www.mofa.go.jp/mofaj/gaiko/oecd/privacy.html（2007.7.19）
[15] 個人データ処理に係る個人の保護及び当該データの自由な移動に関する欧州議会及び理事会の指令, http://www.isc.meiji.ac.jp/~sumwel_h/doc/intnl/ Direct-1995-EU.htm（2007.7.19）

**日本アイ・ビー・エム
　システムズ・エンジニアリング株式会社
ビジネス・アーキテクチャー
ICPシニアITアーキテクト**

大津留 史郎 Shiroh Ohtsuru

［プロフィール］

1989年日本IBM入社，OSIネットワークのスペシャリストおよびプロジェクト・マネージャーとして公共・通信分野におけるSIプロジェクトを担当．1998年より日本アイ・ビー・エム システムズ・エンジニアリングに出向し，OSI，SNA，TCP/IPのネットワーク技術支援を担当．2002年よりITアーキテクトとしてセキュリティ，システム基盤のアーキテクチャー設計を担当し，2007年より現職．

ohtsuru@jp.ibm.com