解 説 2

# IBM セキュリティー・フレームワークのご紹介

## ― フレームワーク活用による網羅的なセキュリティー・アプローチの実現 ―

**昨今の事件報道の影響により、セキュリティー対策は企業経営における重要課題の 1 つとして取り組まれるようになりました。しかし多くの企業では単独のテクノロジー／ソリューションによる場当たり的な対策を行うのみで、システム全体を見据えた網羅的な対応ができているとはいえない状況です。IBM では 2008 年にセキュリティー・フレームワークを発表し、ビジネスの観点で IT セキュリティーにアプローチする手法を提供しています。当稿では本年新バージョンとなった IBM セキュリティー・フレームワークをご紹介するとともに、その中で定義された「ひと」「データ」「アプリケーション」「インフラストラクチャー」と「セキュリティー・インテリジェンス&アナリスティクス」の各要素での課題とソリューションを解説します。フレームワークを利用することで、複雑な企業システムにおけるセキュリティー対策を網羅的に検討し、さらにビジネスの観点で投資の優先順位を付けることが可能となります。グローバルで数百のお客様における実績を持つフレームワークをセキュリティー強化にお役立てください。**

### ❶ 企業におけるセキュリティーと IBM セキュリティー・フレームワークの果たす役割

昨今多くのセキュリティー事件が報告され、IT セキュリティーが企業経営における重要課題として認知されています。IBM が実施した CxO Study［1］においても、企業経営層の優先事項として IT セキュリティーにかかわる課題が挙げられており、CEO をはじめ企業幹部がそれぞれの立場で、セキュリティー上のリスク、それによる潜在的なインパクトを重要視していることが読み取れます（**表 1**）。

従来、企業におけるセキュリティー対策は、得てしてテクノロジー主導になりがちでした。しかし多くのシステム／プロセスから構成される企業システムにおいては、特定の機能要素のみ対策を行っても、ほかの部分でセキュリティー強度の低い個所があると、そこから情報漏えいなどの問題が発生します。セキュリティー対策においては、一番低いレベルがその企業のセキュリティー・レベルとなります。このことからも、セキュリティー対策は場当たり的に実施しても効果は期待できず、網羅的なアプローチが必要であるといえます。

では網羅的なアプローチをするにはどうすればいいでしょうか。IBM では、ビジネスの観点で IT セキュリティーにアプローチする手法として、IBM セキュリティー・フレームワーク［2］を提供しています。次章より、IBM セキュリティー・フレームワークについて解説をします。

### ❷ IBM セキュリティー・フレームワークとは

IBM セキュリティー・フレームワークは、情報セキュリ

**表 1. 企業経営層の優先事項とセキュリティー・リスク**

| | CEO | CFO/COO | CIO | CHRO | CMO |
|---|---|---|---|---|---|
| CxO の優先事項 | ・競合他社に対する優位性の確保／維持 | ・各種法令／ガイドラインの遵守 | ・モバイル・デバイスへの対応 | ・各国人材の積極的活用 | ・ブランド・イメージの向上 |
| セキュリティー上のリスク | ・知的資産の不正流出<br>・ビジネス上の重要データの不正流出 | ・法令／ガイドライン上の遵守事項への不適合 | ・重要データの拡散<br>・エンドポイント・セキュリティーの低下<br>・不正アクセス | ・機密データの共有<br>・内部ユーザーの不適切な行動 | ・顧客／社員の個人情報の盗難 |
| 潜在的なインパクト | ・市場シェアのロス<br>・信用失墜<br>・法的措置 | ・監査による指摘<br>・罰金、刑事責任の発生<br>・財務上の損失 | ・データの機密性／完全性／可用性を損なう | ・社員個人情報の流出 | ・顧客からの信用失墜<br>・ブランド・イメージの失墜 |

IBM C-Suite Study Series［1］より抜粋

注： CEO: Chief Executive Officer　CIO: Chief Information Officer
CFO: Chief Financial Officer　CHRO: Chief Human Resources Officer
COO: Chief Operating Officer　CMO: Chief Marketing Officer

ティーの国際規格として知られるISO 27000シリーズ、COBIT（Control Objectives for Information and related Technology）などを基に、2008年に最初のバージョンがリリースされました。2012年2月には、実際にフレームワークを利用したお客様事例から抽出された新たなニーズや技術革新を受け、新バージョンを発表しています[3]。**図1**に最新のIBMセキュリティー・フレームワークを示します。

多くのセキュリティー・ベンダーは、1つのセキュリティー・エリア、もしくは、部分的なセキュリティー・リスクにフォーカスしているのが特徴です。IBMは、セキュリティーを単独の機能要素ではなく、ビジネス・ストラテジーやビジネス・オペレーションと整合性を持つべきエリアと考えています。

IBMセキュリティー・フレームワークのアプローチは、ビジネスの視点で組織のエンド・ツー・エンドにわたるリスク・マネジメントを戦略的に検討することです。それにより、企業システムに対するリスクや、重要なビジネス・プロセスを混乱させる潜在的な脆弱(ぜいじゃく)性を見つけ出し、施策の優先順位付けを支援します。

IBMセキュリティー・フレームワークでは、オペレーショナル・セキュリティー・ドメインとして、「ガバナンス、リスク、コンプライアンス（GRC）」を以下の4つに分類しています。

**ひと**

企業の保有するリソースに、承認されたユーザーのみがアクセスできるようになっていることの確認と保証

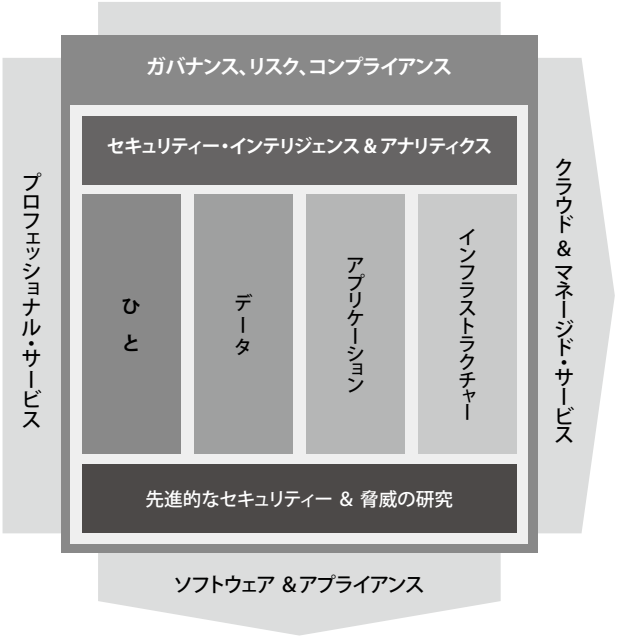



図1. IBMセキュリティー・フレームワーク

**データ**

重要データの移動／保管のライフサイクルにおける保護

**アプリケーション**

アプリケーションとビジネス・サービスのセキュリティー確証

**インフラストラクチャー**

システム・インフラストラクチャーに対する脅威への対策

企業経営において、システム全体のセキュリティー状況を可視化することはとても重要です。この新たなニーズを受けて、今回の更新では、上記4つを効果的かつ補完的に支える仕組みとして、「セキュリティー・インテリジェンス&アナリティクス」と「先進的なセキュリティー&脅威の研究」が追加されました。「セキュリティー・インテリジェンス&アナリティクス」はシステム全体のセキュリティー状況を可視化する一助となり、「先進的なセキュリティー&脅威の研究」は攻撃のパターンや先進リスクを知ることで、予防的な対策の立案を行うものです。

IBMではこれらの要素に対し、以下に分類される製品／サービスを提供しており、お客様の要件や運用体制に応じ、適切なソリューションを選択いただくことが可能です。

- ソフトウェアとアプライアンス
- プロフェッショナル・サービス
- クラウド & マネージド・サービス

## ❸ お客様の課題とIBMセキュリティー・フレームワーク

**図2**ではIBMセキュリティー・フレームワークを構成するオペレーショナル・セキュリティー・ドメインの4つの要素と「セキュリティー・インテリジェンス&アナリティクス」に対して、代表的な機能をマッピングしています。また、終わりのないセキュリティー対策を支える「先進的なセキュリティー & 脅威の研究」も定義されています。

**ひと**

ここでは最適なコストで企業リソースに対するユーザー・アクセス管理のリスクを軽減することが求められます。具体的な機能要素としては、ユーザーIDと属性情報のライフサイクル管理と、確実な認証が出発点となります。これらの基盤が確保された上で、職掌に応じたアクセス権限

<table>
<tr><td colspan="5">セキュリティー・ガバナンス、リスク、コンプライアンス</td></tr>
<tr><td colspan="5">セキュリティー・インテリジェンス & アナリスティクス</td></tr>
<tr><td>セキュリティー情報と<br>イベント管理</td><td>ログ管理</td><td>リスク管理</td><td colspan="2">監査、コンプライアンスの評価</td></tr>
<tr><td colspan="5">ITインフラストラクチャー・オペレーショナル・セキュリティー・ドメイン</td></tr>
<tr><td>ひと</td><td>データ</td><td>アプリケーション</td><td colspan="2">インフラストラクチャー</td></tr>
<tr><td>ID管理、認証</td><td>データベース・<br>セキュリティー</td><td>Webアプリケーションの脆弱性</td><td>不正侵入防御</td><td>エンドポイント管理</td></tr>
<tr><td>統合認証管理</td><td>テスト・データ・マスキング</td><td>Webセキュリティー・<br>ゲートウェイ</td><td>セキュリティー<br>統合管理</td><td>仮想化環境<br>セキュリティー</td></tr>
<tr><td>シングル・サインオン</td><td>暗号鍵<br>ライフサイクル管理</td><td>セキュリティー・<br>ポリシー</td><td>異常検知</td><td>メインフレーム・<br>セキュリティー</td></tr>
<tr><td rowspan="2">ID管理診断評価サービス、<br>導入サービス、<br>ホスティング・サービス</td><td>データ・セキュリティー<br>評価サービス</td><td rowspan="2">アプリケーション<br>診断評価サービス</td><td rowspan="2">ファイアウオール、<br>IDS/IPS、<br>UTMセキュリティー<br>運用監視</td><td>侵入テスト診断サービス</td></tr>
<tr><td>暗号実装サービス、<br>データ漏えい保護サービス</td><td>モバイル・デバイス<br>管理サービス</td></tr>
<tr><td colspan="5">先進的セキュリティーと脅威の研究</td></tr>
</table>

IDS：Intrusion Detection System　IPS：Intrusion Prevention System　UTM：Unified Threat Management

**図2. IBMセキュリティー・フレームワークと代表的な機能**

の適切な付与が可能となり、リソースへのアクセスの監査およびレポートが実現します。

複雑な企業システムにおいて、このような機能を効率よく、最適なコストで実装／運用するためには、システム単位で個別に構築されたID管理・認証の仕組みでは困難です。ID管理・認証基盤を統合化することで、組織異動などに伴うユーザー情報の変更作業を効率化し、生体認証などの高強度認証をはじめとした新要件の組み込みを容易にできます。

特に監査対象となるシステム、機密データを扱うシステムにおいては、ID管理・認証基盤を統合化し、運用コストを最適化しつつ各サービスでの適切なアクセス制御／IDガバナンスの可視化を行うことが推奨されます。

### データ

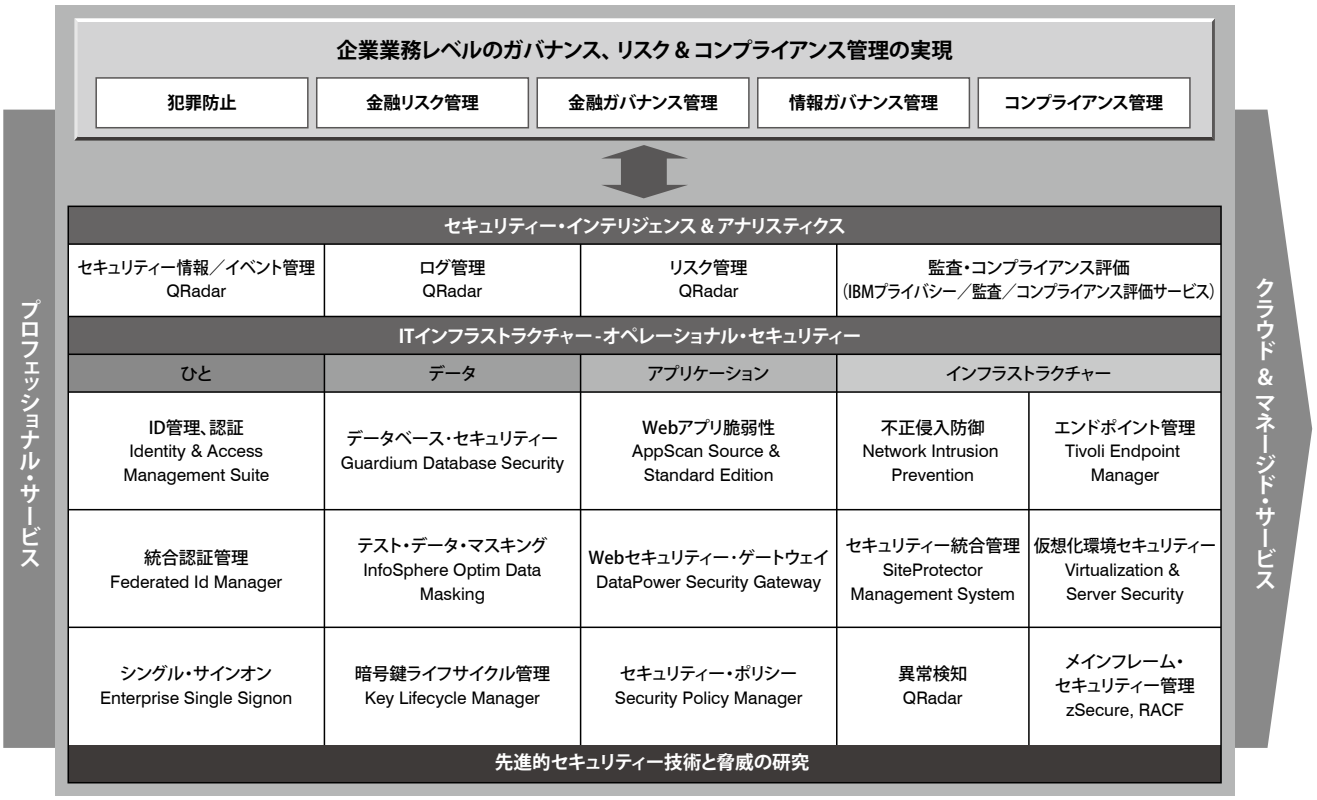
機密データへのアクセスと利用の制御は、ITセキュリティーにおける重要な関心事の1つです。顧客の個人情報、知的資産などを確実に管理するためには、機密あるいは規制対象となっている情報の棚卸しを行い、識別・分離することが重要です。その上でデータの管理基準に応じた、暗号化、アクセス制御、アクティビティー・モニタリングなどのセキュリティー機能を実装することになります。

Need to Knowの原則に従い、データへのアクセス権を最小限にすべきであることは言うまでもありませんが、データベース管理者など、正規の権限を有するユーザーによる機密データへのアクセスを完全に止めることは不可能です。アクセス権を有するユーザーによる不正行為を抑制するには、運用ルールに合わせたきめ細かなアクセス制限の見直しとアクティビティー・モニタリングが効果的です。具体的には運用端末以外からの特権IDのアクセスを許可しない、一定の操作については操作ログを取得するなどの対策が挙げられます。ここで取得されるログは、データベース管理者であったとしても削除できない場所に格納するなどの運用を行うことで、ログ・データの完全性を担保する必要があります。

### アプリケーション

ここでは、アプリケーションを堅牢（けんろう）に保ち、悪意ある攻撃、または不正な利用から保護することが求められます。そのためには、まずアプリケーション開発プロセスにおけるセキュリティー確保が重要です。

すでにオフショア開発に取り組んでいる企業も多いと思われますが、そこでの重要課題の1つは品質管理とされています［4］。当然のことながら、アプリケーションの脆弱性も管理すべき品質の1項目です。国内外のリソースを活用し一定の品質を確保するには、企業のポリシーに合致したセキュアなアプリケーション開発プロセスの確立が必要です。開発の段階で脆弱性をチェックするツールを




RACF: Resource Access Control Facility

図3. IBM セキュリティー製品ポートフォリオ

活用することで、開発要員のスキルに依存せずアプリケーション・コードのセキュリティー強度を一定に保ち、安全なシステム開発が可能となります。脆弱性は日々新たに発見され、一方で攻撃手法も進化しています。リリース前だけでなく、定期的な脆弱性診断の実施、および発見された脆弱性が修正されるまでのトレース管理のプロセス化はとても重要なポイントです。業種によっては社内外の情報システムだけでなく、組み込みソフトウェアも品質管理の対象となるでしょう。そのソフトウェアの重要性、予測されるリスクに応じた管理基準の定義が必要となります。

次に大切なのが、アプリケーションの利用者の制御や実行権限の見直しなどのアクセス制御ポリシーの管理です。企業システムにおいては、ビジネス要件、コンプライアンス上の要求に応じて、一旦定義したポリシーが変更されることも予想されます。このような変更に柔軟に対応し、適切なアクセス制御の導入展開と検証ができる仕組みが必要です。残念ながらマルチベンダー環境においてアクセス制御処理自体の統合は現時点では困難ですが、アクセス制御ポリシーを集中管理し、業界標準のフォーマットで実行点に配布する仕組みはすでに実装可能となっています。

### インフラストラクチャー

インフラストラクチャーは、ネットワークとエンドポイントに大別されます。ここでいうエンドポイントはクライアントPCだけでなく、メインフレーム、分散サーバー、スマートフォンなどのモバイル機器も含みます。インフラ・セキュリティーの強化には、これらのエンドポイントの特性に合わせたセキュリティー対策の適用と運用が必要となります。

従来、インフラ・セキュリティーでは、ファイアウオールやIPS/IDSによる外部接続セキュリティーの強化、Windowsプラットフォームに対するアンチウイルス機能が代表的な対策とされてきました。しかし、昨今の標的型サイバー攻撃においては、これらの対策だけでは不十分であることが指摘されています［5］。これからのエンドポイント管理では、確実なパッチ適用や、管理基準に従ったOS上のセキュリティー設定の徹底が要求されます。システムを構成する全エンドポイントからこれらの情報を確実に収集することで、企業システム全体の脆弱性を可視化し、新たな脅威に対し適切な対応を行うことが可能となります。

ITインフラストラクチャーをクラウド環境に移行されるお客様も増えています。クラウド環境においては、従来の対

策に加え、マルチテナンシーや仮想化技術への対応が求められます。マルチテナント環境では隣接テナントへデータやトランザクションの漏えいが発生しない仕組みを構築する、仮想環境ではハイパーバイザーなどの新しい構成要素に対する脅威を定義するといった対応を検討する必要があります。このような新たな課題に対しても、各ベンダーから対策技術が開発されており、セキュリティーを考慮した仮想化インフラの構築が進められています。

これらのオペレーショナル・セキュリティー・ドメインからの情報を基に、企業システム全体のセキュリティーを可視化するのが、セキュリティー・インテリジェンス&アナリスティクスです。

**セキュリティー・インテリジェンス&アナリスティクス**

個別のシステムからさまざまなフォーマットで出力されるセキュリティー・イベント／ログを統合的に管理することで、システム全体のセキュリティー状況を可視化します。さらに、高度な相関分析を施すことにより、インシデントの前兆を予見するプロアクティブなセキュリティー対策を実装することが可能となります。すでに米国国防系組織など一部の先進事例では、高度なリアルタイム分析技術によるサイバー攻撃への対応が実装され始めています。

**先進的なセキュリティー&脅威の研究**

巧妙化する攻撃手法に対抗するには、一時的な対策の適用だけでなくセキュリティー専門家による監視、脆弱性や脅威の対策についての定期的なレビューが推奨されます。

IBM は、X-Force と呼ばれるセキュリティー専門の研究機関を有しており、その規模は民間最大級といわれています。地球全体をカバーする 9 カ所のセキュリティー・オペレーション・センターで、一日 130 億件以上のイベントを監視・分析することで得た最新の知見を新たな製品・サービスへとフィードバックしています［6］。

## ❹ IBM のセキュリティー・ソリューション

IBM では、セキュリティー・フレームワークに対応した包括的なセキュリティー・ソリューションを提供しています。個別の製品提供・構築だけにとどまらず、上流のコンサルティングから運用サービスまで、企業システムの全ライフサイクルを通じてセキュリティー強化を支援します。

**図 3** に IBM セキュリティー・フレームワークの各要素に代表的な IBM ソリューションをマッピングしたものを示します。ここではソフトウェア、アプライアンスのみを記述していますが、2 章で述べたように、プロフェッショナル・サービス、クラウド & マネージド・サービスとして提供している要素もあります。

**ひと**

ユーザー ID 管理からフェデレーションを含む統合的なシングル・サインオン・ソリューションを Identity and Access Management Suite として提供しています。「ひと」の管理は、**表 1** で CHRO の優先事項となっている「各国人材の積極的活用」に直結します。単純なデータ連携だけでなく、職掌に合わせたロール定義や、ユーザー情報を正確に維持するためのプロセス設計が必須です。IBM は国内外の多くの事例で得た知見を基に ID 管理・認証基盤構築を支援します。

**データ**

重要データを格納するデータベースのセキュリティー強化が必要となっても、現行システム構成や負荷状況に大きな影響を及ぼすような機能追加はできないケースも多いのではないでしょうか。IBM では、データベースへの負荷を最小化しつつ、確実なアクセス制御／ログ取得を実現するデータベース・セキュリティー強化アプライアンス製品を提供しています。また、テスト環境でのデータ・マスキング・ツール、暗号鍵のライフサイクル管理ツールなど多彩なソリューションの提供が可能です。

**アプリケーション**

IBM の開発ツールである Rational のラインアップに加え、アプリケーション脆弱性のテスト・ツールを提供しています。これにより、セキュリティー対策も品質管理の 1 項目として、開発プロセスに組み込むことが可能です。

また、SOA 環境のセキュリティー実装を容易にするソフトウェアやアプライアンス製品を利用し設計段階からセキュリティー機能を組み込むことで、セキュアなシステム構築を支援します。

**インフラストラクチャー**

緊急度の高い脆弱性に対するパッチ適用が必須とはいえ、サービス継続性の観点から適用のタイミングが限定されるシステムもあるでしょう。IBM の IPS/IDS に組み込ま

れたバーチャル・パッチ・テクノロジーでは、あたかもサーバーに最新のパッチを適用したかのように、高いレベルでOSやミドルウェアの脆弱性に対する攻撃を無効にすることが可能です。また、UNIXサーバーからPCクライアント、モバイル機器の構成／設定情報をリアルタイムで収集し、システム内の脆弱性を可視化するツールを用いることで、継続的なセキュリティー対策立案を支援します。

**セキュリティー・インテリジェンス&アナリスティクス**

システム内に点在する多様なフォーマットの監査ログを収集し正規化の上分析することで、不正の兆候を可視化することができます。蓄積されたログから不正の証跡を後追いで調査するだけでなく、あらかじめ決められたポリシーに基づいた、リアルタイムでのセキュリティー・イベントの生成、監査レポートの出力も可能です。

## ❺ まとめ

IBMセキュリティー・フレームワークのアプローチは、クラウド・コンピューティング、モバイル・セキュリティーなど最新の機能領域に適用することができます。

以下にIBMセキュリティー・フレームワークのもたらす価値を列挙します。

- ひと、データ、アプリケーション、インフラストラクチャーの4要素において、企業が持つ既存のセキュリティー対策の中から不足している部分を明確化します。
- 最適な効果を実現するために、ビジネスの観点でセキュリティー対策と投資の優先付けを支援します。
- 企業全体に対するセキュリティー対策プログラムの計画と実行の簡素化、迅速化を進めます。
- 企業の競争力と成長をサポートする観点でセキュリティー管理を支援するために、再現性、測定可能性、プロセス計画、そしてロードマップとソリューションを提供します。
- ガバナンス、リスク、コンプライアンスの要件に対応できる、あるべきセキュリティーの体制作りを支援します。
- 全社的なコスト削減のためのスマートなセキュリティー・ソリューションの強化を支援します。

2012年、IBMのソフトウェア事業では、これまで各ブランドで個別に提供していたセキュリティー・ソリューションを統括して提供するセキュリティー・システムズ事業部を新設しました。全世界のIBMでは6,000名以上のセキュリティー・エキスパートがアサインされ、18億ドルの技術投資が計画されています。また、各エリアのリーダー企業の買収を含め、継続的な投資を行っています。

今後も高度に複雑化するITセキュリティーの脅威からお客様を守るために、グローバルIBMの重点エリアとして当分野に取り組んでいきます。

**［参考文献］**


[1] The IBM C-suite Studies, http://www.ibm.com/services/c-suite/series-download.html
[2] Axel Buecker, Martin Borrett, Carsten Lorenz, Calvin Powers: Introducing the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security, IBM, http://www.redbooks.ibm.com/redpapers/pdfs/redp4528.pdf（2009）.
[3] Marc van Zadelhoff: The IBM Institute for Advanced Security Expert Blog, http://instituteforadvancedsecurity.com/ias-blogs/community-blogs/b/marc_van_zadelhoff/archive/2012/02/01/introducing-the-updated-ibm-security-framework.aspx（2012）.
[4] 天野武彦："特集テーマ：グローバル・リーダーシップ ― 日本の競争力の再構築", PROVISION No.68, http://www.ibm.com/ibm/jp/provision/no68/pdf/68_article2.pdf（2011）.
[5] 標的型サイバー攻撃の事例分析と対策レポート，独立行政法人情報処理推進機構，http://www.ipa.go.jp/security/fy23/reports/measures/documents/report20120120.pdf（2012）.
[6] 東京セキュリティー・オペレーション・センター：東京SOCレポート，https://www.ibm.com/connections/blogs/tokyo-soc/?lang=ja（2012）.



**日本アイ・ビー・エム株式会社**
**ソフトウェア事業**
**セキュリティー・システムズ事業部**
**シニア アーキテクト**

丹羽 奈津子 **Natsuko Niwa**


**［プロフィール］**
1990年、日本IBM入社。クライアント／サーバー・システム、ネットワーク、システム運用管理ソリューションの技術支援を経て、2002年よりIBMセキュリティー・ソリューションを担当。2011年よりグローバルIBMのSecurity Tiger Teamにてアーキテクトを務める。