解 説 3

IBM基礎研究部門における サイバー・セキュリティーの取り組み

IT の進化に伴い、人にとっても社会にとっても、サイバー・スペースの重要性が高まっています。商取引、情報伝達、教育、宣伝など、人や企業間のコミュニケーションや活動は、デジタル化されたネットワークとそれにつながったさまざまな種類の機器やセンサー、そしてそこで生成され流通するデータに大きく依存するようになりました。また、電力や都市機能など、人間の暮らしや企業の存続を支える社会的なインフラも、サイバー・スペースとの重なりを深めています。このような社会の変革の中で、従来のセキュリティー技術では守りきれない新しいタイプのリスクや脅威が生まれています。本稿では、著者らが所属する東京基礎研究所を含む、IBM 基礎研究部門が行っているサイバー・セキュリティーに関するイニシアチブや研究開発プロジェクトの一端を紹介します。

❶ はじめに

われわれを取り巻くさまざまな事象がサイバー・スペースへと移行し、人や企業がサイバー・スペースで活動を行うことが当たり前になってきました。この変化は 2 つの要因にけん引されています。1 つは接続され膨張を続ける今日のデジタル社会の発展です。ネットワークによって、コンピューターだけではなく、センサー・デバイス、オフィス機器、医療機器、自動車、そして発電所のような社会インフラに至るまで、あらゆるものがつながりつつあります。そして、それらを用いるユーザー自身も、企業や国の境界を超えて活動する機会が増えてきました。

また、これらの変化に呼応する形で、新しい技術やビジネス・モデルが台頭しています。これが 2 つ目の要因です。市場や労働力のグローバル化、クラウド・コンピューティング、ビジネス・アナリティクス、ビッグデータなどに代表される新しい技術、さらには、ソーシャル・コンピューティングを用いた新しいビジネス・モデルなど、社会の在り方そのものが物理的な空間とサイバー・スペースの相互依存関係によって支えられています。

このような社会と技術の変化によって、新しいタイプのセキュリティーおよびプライバシーに関するリスクや脅威が発生しています。**図1**に、従来の企業を取り巻く状況と今日の変化を示します。

以前は、企業は単一の事業体からなり、外界（インターネット）との接続点は明確に認識され、ファイアウオールなどで強固に防御されていました。ところが、現在では、企業統合や系列・関連会社との協業などにより、異なるポリシーを持つシステムが接続されるケースが出てきました。また、個人や企業に対するサイバー攻撃は、内部的な犯行も含めてより組織的で巧妙なものになっています。さらに、スマートフォンなどのモバイル・デバイスの普及やソーシャル・ネットワーキング・サービス（SNS）などのコミュニティー・ベースのサービスの普及は、情報漏えいのリスクを増大させます。発電所などの社会的なインフラに対する攻撃も報告されています。

IBM 基礎研究部門では、2011 年から、中長期的な視野で技術的なブレークスルーを目指すグランド・チャレンジ・プロジェクトの 1 つとしてサイバー・セキュリティーを取り上げ、著者らが所属する東京基礎研究所を含む世界各国の基礎研究所が参画しています。現在、以下の 5 つのトピックを中心

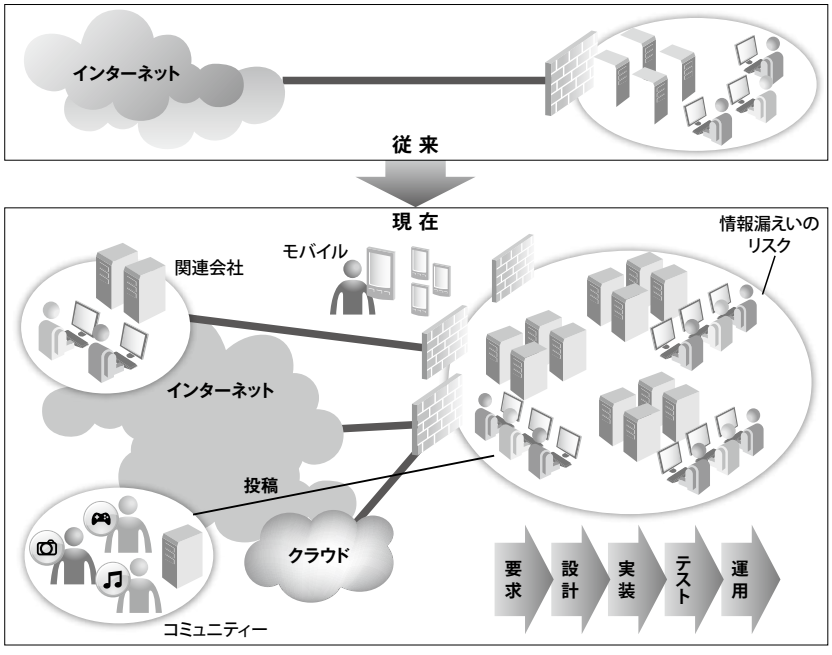

図1. サイバー・セキュリティーを取り巻く状況の変化

にさまざまなプロジェクトが展開されています。

ミッション・クリティカルな企業資産とセンシティブ情報の発見と保護

企業におけるさまざまな情報資産の価値と流出時のリスクを計算し、レベルに応じた保護を行うためのデータ・セキュリティー技術が今後ますます重要になってきます。本稿では、その一例としてIBM 東京基礎研究所とIBM T.J. ワトソン研究所で研究開発を行っている情報漏えい防止プロジェクトを紹介します（第2章1節）。

セキュアでない環境におけるIT資源の保護と管理

インターネットやパブリック・クラウドなどの環境で、セキュアなプラットフォームを構築するための技術です。サーバー、ハイパーバイザー※1、OS、ミドルウェア、アプリケーション、データからなるスタック各層レベルでのセキュリティー技術や、プライベート・クラウドとパブリック・クラウドを統一したセキュリティー・ポリシーによって管理するための技術などが研究開発されています。

エンド・ツー・エンドのセキュリティー

携帯電話やスマートフォンは企業活動や社員のワークスタイルに変革をもたらしました。同時に、モバイル環境におけるセキュリティーという新しい課題も生まれています。さらに、携帯電話に限らず、あらゆるデバイス（エンドポイント）がネットワークでつながり依存し合う環境においては、いかにエンド・ツー・エンドのセキュリティーを守るかが大きな課題となります。本稿では、新しいタイプのエンドポイントとして自動車を取り上げます（第2章2節）。

サイバー・セキュリティーにおける解析技術

サイバー犯罪の巧妙化により、過去に存在するマルウェアを基にして作られるパターン（シグネチャー）を活用した従来の防御手法では、未知の攻撃を防ぐことは困難です。IBMでは、ビジネス・インテリジェンス分野で強みを持つ解析技術、大規模イベント処理技術、ビッグデータ技術を組み合わせることで、リアルタイムでの攻撃検知や、攻撃の予兆を監視するための研究開発（第4章1節）を行っています。

セキュア・バイ・デザイン (Secure by Design)

システムの設計、開発、テスト、運用というライフサイクルにおいて、セキュリティーは、非機能要件の1つとして、ともすれば後回しにされてしまうことがあります。しかし、このことが、最終的に大きな損失を生む危険性があることは昨今の事件が示唆しています。セキュリティーをソフトウェアの設計や開発段階で「作り込む」セキュア・バイ・デザインの考え方が現在注目されています。本稿では、プログラム開発におけるセキュリティー技術（第3章）や、システムの機能としてセキュリティーが組み込まれているという観点で、暗号化に関する先進的な技術（第4章2節）を紹介します。

次章以降では、上記トピックを支える要素技術と関連技術について説明していきます。

❷ データ・セキュリティー

セキュリティー技術がカバーする資源の対象は、ハードウェア、ソフトウェア、データと多岐にわたります。その中でも、ビッグデータと呼ばれる近年のデータ量の爆発的な増大状況から、データに関するセキュリティーおよびプライバシー技術が大きな注目を浴びています。本章では、IBM 基礎研究部門で研究開発されているデータ・セキュリティー技術プロジェクトの一部を紹介します。

2.1 情報漏えい防止（Data Leakage Prevention）

IT環境におけるデータの安全性確保は、企業にとって重要な課題であり続けています。近年採用が増えているデスクトップ・クラウドは、ビジネス文書作成や電子メール処理といった、通常は手元のPCで行う業務を、クラウド上にホスティングされたデスクトップ環境で実行し、手元のPCにはその画面だけを遠隔転送するサービスです。このサービスは「画面だけを転送する」という特性により、手元PCからの情報漏えいの危険性を低減させることができるため、顧客情報を扱う部署など非常に高いセキュリティーが求められる環境や大規模災害発生時などの在宅勤務環境において有益です。一方で、例えば「在宅勤務時に旅費精算用の領収書添付台紙を自宅PCで印刷できない」など、安全性に問題のない操作まで不可能になることに起因する業務効率低下の問題が生じます。このため、安全と思われる操作（ここでは自宅における台紙の印刷操作）だけを選択的に許可する、すなわちコンテキストとデータの内容に応じた許可・不許可の切り替えを行うための技術が求められます。

従来のアクセス制御手法では、操作の許可・不許可の設定は、人間が手動で行います。しかし、業務で扱うデータは大量であり、人手で設定を行っていては大変な手間が掛かる上に、設定ミスによって機密情報が意図せず流出する危険性があります。このリスクを軽減するための技術が、アクセス制御システムにコンテンツ解析技術を取り込むことでア

※1　仮想化技術により、複数のOSを実行するプログラム

クセスの許可・不許可を自動的に判定する情報漏えい防止（Data Leakage Prevention：以下、DLP）と呼ばれるものです［1］［2］。

通常のアクセス制御システムでは、ある組織が持つセキュリティー・ポリシーと、人間がデータに付与したセキュリティー属性（ラベル）から、ユーザーが行おうとしている特定の操作の許可・不許可を決定し、これを実際のシステムの振る舞いに反映させます。DLP システムでは、人間の代わりにデータの内容を解析するエンジン（コンテンツ解析器）がラベルを付与します。例えばある組織が「公表前の財務情報は『財務機密』という種類のデータに分類し、『財務機密』データは印刷禁止とする」というポリシーを持っているとすると、既存のアクセス制御ではあるデータが「財務機密」であるかどうかを人間が判断して設定に反映させるのに対して、DLP システムではコンテンツ解析器がデータに含まれる数値や特異な表現（例えば「仕掛品」「退職給付引当金」）を抽出し、自動的に「財務機密」というラベルを決定します。DLP システムの性能は、コンテンツ解析器の性能（最初から付属してくるルールの網羅性・正確性や追加ルールの記述しやすさ）や、ポリシーで制御できる操作の広汎性・詳細度、コンテンツ解析などに伴うシステムのパフォーマンス低下の度合いによって評価されます。

図 2 は、IBM 東京基礎研究所と IBM T.J. ワトソン研究所で共同開発したデスクトップ・クラウド向けの DLP の技術実証システムにおいて、印刷を許可されるデータと許可されないデータがどのように処理されるのかを示しています。ユーザーがデスクトップ・クラウド上で開いたファイルは、クラウド上に置かれたコンテンツ解析器によって、内容に即したラベルが与えられます。ラベルは組織の持つポリシー情報と共に手元 PC に導入された制御エンジンに送られ、ユーザーがデータを印刷しようとした時には印刷可のファイルの印刷データだけが実際にプリンターへ送られる仕組みです。異なるユーザーが同一のファイルを印刷しようとした場合は解析結果を再利用することで、パフォーマンスの低下を最小限に抑えています。

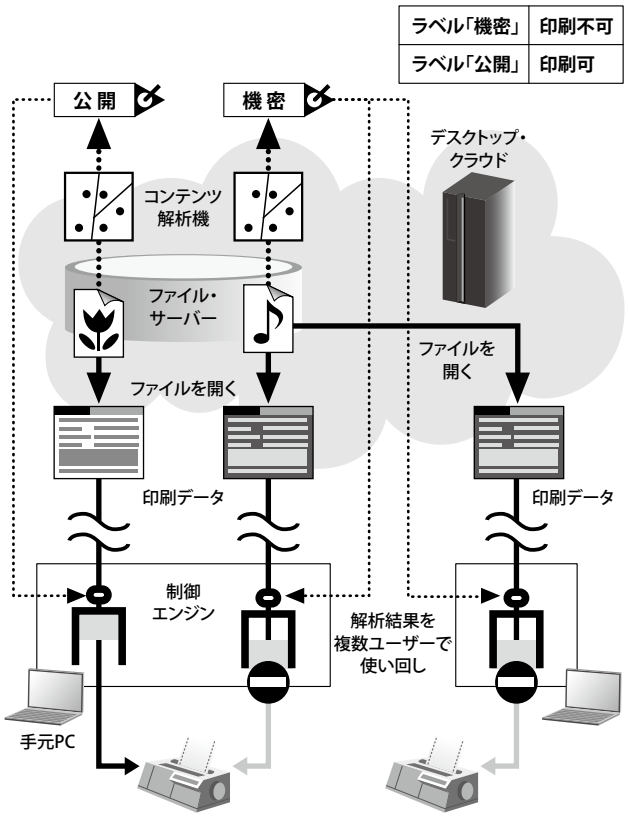

図2. DLPの構成例

2.2 エンドポイントにおけるデータ・セキュリティー

前述した DLP は、主に企業内の情報に対する技術ですが、さまざまな領域で企業が利用可能なデータは増え続けており、安全性を確保した上でそれらを利用することに現在注目が集まっています。いわゆるビッグデータが目指す領域です。エンドポイントも、従来は主にコンピューターや組み込みデバイスなどを示す用語でしたが、現在では、さまざまなセンサーや家電、医療機器、車など、あらゆるものがエンドポイントとしてネットワークに接続されるようになってきました。例えば、車には、ECU（Engine Control Unit）と呼ばれる制御用のコンピューター・ユニットが複数搭載され、ネットワークで接続されています。車からワイヤレスや電話回線などを介して取得されるデータは、車の運転状況や故障に関するさまざまな情報（以下、プローブ・データ）を含むため、今後、車外のさまざまな人・物・サービスと車との間の連携を実現する上で重要となるデータです。一方で、プローブ・データは、車がいつどこを通過したかに関するデータ（経路データ）を含む場合があり、そこには、出発地、目的値、停車・通過地点など、運転者の嗜好（しこう）に関する情報が含まれる可能性があります。そのため、データ管理者は、運転者と合意したデータの利用目的に応じて、データの開示を許可された範囲に限定し、目的以外の情報が「染み出ない」ようにするための対策を行う必要があります。データ処理における技術的な対策としては、必要な情報だけに集約して余分な情報をカットする方法や、元のデータにノイズを載せて、決められた目的以外の処理に利用できないように加工する方法などがあります。経路データは、ほかの経路データを含め、位置と時間に関連する外部の情報と相関が取りやすいことから、さまざまな分析に利用できる反面、特定の人だけが知る情報との相関から意図しない情報が「染み出る」危険性があります。十分な安全性の確保のため、上記のようなデータ処理上の技術的な対策だけでなく、データの隔離・データ利用者の制限など運用上の対策と併せた多重のセキュリティー対策

が必要となります。

❸ セキュア・バイ・デザイン

第 1 章でも述べたように、新しいタイプの脅威は従来の技術では防ぎきれなくなってきています。周到に計画され長い時間をかけて仕掛けられるサイバー攻撃に対処するには、さまざまな観点からセキュリティーを考慮し、対策を作り込んで行くことが必要になります。運用時だけではなく、開発工程全体を通してセキュリティーを考慮するというコンセプトをセキュア・バイ・デザイン［3］［4］と呼びます。

表 1 は、これを実践するための技術や方法をソフトウェア・ライフサイクルに沿って幾つか列挙したものです。この章では、設計から運用において今後重要になるであろう技術として、プロトコル検証、プログラム解析、セキュア・プラットフォームについて取り上げます。

表1. ソフトウェア・ライフサイクルにおけるセキュリティー手法

局面	手法		
要求	セキュリティー上の要求の抽出		
設計	脅威モデル	プロトコル検証	暗号アルゴリズム
実装	プログラム解析	プロトコル検証	セキュア・パターン
テスト	プログラム解析	ファジング	攻撃パターン
運用	暗号化ツール	セキュア・プラットフォーム	

3.1 プログラム解析による脆弱性検査

プログラム解析とは、プログラムの実行状態やソース・コードを解析・検証するための技術です。特に、プログラム・コード（ソース・コード、バイト・コード、バイナリー）を解析し、実行中に起こり得る値や動作を推論・検証を行うものを静的プログラム解析（以下、静的解析）と呼びます。一方で、プログラムを実際に実行することによって行う解析・検証を動的プログラム解析（以下、動的解析）と呼び、ソフトウェアのテスト実行やシミュレーションも動的解析に含まれます。

IBM Rational AppScan は、静的解析と動的解析の両方を用いた Web アプリケーションの脆弱（ぜいじゃく）性検査ツールであり、著者らが所属する東京基礎研究所も製品開発に貢献しています。動的解析では、Web サイトをクロールしながら攻撃用の HTTP リクエストを送り、その HTTP レスポンスを解析して脆弱性の有無を判定します。静的解析では、汚染解析［5］と文字列解析［6］と呼ぶ静的解析技術が用いられており、ユーザー入力によって引き起こされる SQL インジェクションや XSS（クロス・サイト・スクリプティング）と呼ばれる脆弱性の検出に有効です。

汚染解析とは、セキュリティー上重要な操作（例：データベースへの問い合わせ）が外部からの入力データ（汚染データ）を扱う場合に、その入力データが必ず無害化（サニタイズ）されていることを確認するための静的解析です。ここで、無害化とは、汚染された文字列中から危険な部分の文字列（例：実行可能なスクリプト・コード）を取り除くことであり、そのような変換を行う関数をサニタイザーと呼びます。文字列解析は、そのような独自に定義されたサニタイザーの正しさ（生成される可能性のある文字列に危険な文字列が含まれないこと）を確認できます。

一般的に、静的解析では、プログラムの動作や実行状態、あるいはプログラム中の変数間の制約関係を抽象化や近似を用いて形式的な（数学的な）モデルとして表現します。例えば、前述の文字列解析では、実行時に起こり得る文字列の集合（あるいは性質）や、文字列操作前後の関係をモデル化しています。このため、動的解析よりも網羅性を確保しやすく、また、実行情報だけでは得られないプログラムの性質を明らかにすることができます。

一方で、動的解析では、検出過誤をなくすことができますが、その検出結果の網羅性は、ソフトウェア・テストと同様に、入力データに依存します。近年では、静的解析と動的解析を組み合わせた検出手法も存在します。例えば、文献［7］では静的プログラム解析を用いて脆弱性を起こす可能性のある入力データを推論し、その入力データを用いて実際にプログラムの実行を行っています。

3.2 プロトコル検証

プロトコル検証とは、複数のコンポーネント間で用いられる通信手続き（プロトコル）の正しさを検証することです。ここで、正しさとは、仕様またはより一般的な要求、例えば、データの秘匿性が守られることから定義されます。また、ハードウェア、ソフトウェア、サービスなどがコンポーネントとなり、さまざまな開発工程において作成されたモデルの正しさを検証するために利用されています。

このような検証手法は、検証対象となるコンポーネントの動作や、それにかかわるポリシーを形式的にモデル化することが必要です。形式モデルとしては、プロセス代数 [8] や有限状態オートマトン［9］、論理［10］、あるいはそれらから派生したモデルが利用され、定理証明器やモデル検査器などのツールを用いて検証を行います。

例えば、文献［11］では、ウェブ・サービスにおけるポリシーなどを形式的にモデル化し、TulaFale というツールを用いてその安全性の検証を行っています。

3.3 セキュアな通信プラットフォーム:ZTIC

インターネットを介して、商取引を行うことが一般的になっ

てきた今日、信頼できない端末（ブラウザー）やネットワークを使う場合でもいかにセキュアな取引を行うかが、大きな課題となっています。ZTIC（Zone Trusted Information Channel）は、IBM チューリッヒ研究所で開発された、SSL/TLS により安全にインターネットに接続するための USB デバイスです［12］。ZTIC はサーバーと安全な通信路を確立した際、PC に表示されている内容を確認するための情報を USB デバイス上に設置された小型ディスプレーに表示します。PC に侵入したマルウェアが PC の画面上の情報を操作した場合、PC のユーザーは ZTIC の画面とのずれを目視確認して侵入を検出し、ZTIC 上のボタンを押して通信を遮断できます。ZTIC は PC とは独立の計算実行メカニズムを持つため、PC に侵入したマルウェアであっても ZTIC を不正に操作することはできません。また、2012 年 3 月に発表されたエンタープライズ版の ZTIC（eZTIC）は、ZTIC 技術に基づいてサーバーと ZTIC の間に安全な iSCSI 接続を確立し、それを通じてサーバー上の（マルウェアの入っていない）仮想マシンのイメージを ZTIC にダウンロードし、それを TPM（Trusted Platform Module）技術に基づいて安全に起動することにより、PC 上のマルウェアの干渉を不可能にする技術で、現在、スイスの銀行での試験運用中です［13］。

❹ 新しい流れ

最近注目されているビジネス・アナリティクスやクラウド・コンピューティングに呼応する形で、新しいセキュリティー技術が注目されています。この章では、セキュリティー分析プラットフォームと準同型暗号を取り上げます。

4.1 セキュリティー分析プラットフォーム

最近のサイバー攻撃は、あらかじめマルウェアのパターンを登録しておき、それに合致するものを排除するという従来の方式では防げなくなってきています。そこで、大量のデータを分析して、攻撃者の行動パターンの検出や攻撃の予兆の検知を行うための分析プラットフォームが重要になってきます。IBM では、ビジネス・インテリジェンスの観点から分析技術に注力しており、その成果をセキュリティー分野に応用する試みが始まっています。例えば、ネットワーク、ハイパーバイザー、アプリケーションのログ・データをリアルタイムに収集・分析することで、ボットネットやマルウェアの検出を行うことが考えられます。データ処理のために、イベント・ストリームの高速な処理を行う IBM InfoSphere Streams や IBM InfoSphere BigInsights などの並列処理エンジンが活用されています。この分野での研究成果は、例えば米国空軍との防衛施策およびインテリジェントなネットワーク構築を支援する高度にセキュアなクラウド・コンピューティング環境の設計と実証プロジェクトなどに生かされています。

4.2 完全準同型暗号

クラウド・コンピューティングにおけるセキュリティーの課題の 1 つは、ユーザーによるデータのコントロールが難しくなることです。ユーザーの機密データをクラウド上の計算リソースを用いて処理するケースを考えましょう。パブリック・クラウド上にデータを置く場合、暗号化しておくことで情報が流出した際のリスクを軽減することができます。暗号鍵をユーザー側で管理することによりクラウド提供者に対してもデータを非開示とすることが可能です。ところが、暗号化を行うことで、逆にクラウド上でデータの検索や処理を行うことが困難になってしまいます。この問題を解くために、データを暗号化したまま計算処理できるようにするための新しい技術として注目されているのが、完全準同型暗号です。

準同型暗号は、準同型性を有する暗号方式です。準同型暗号とは、メッセージ「M1,M2」に対する暗号文を「E(M1),E(M2)」とするとき、「E(M1)」と「E(M2)」から「E(M1+M2)」または「E(M1M2)」が計算できる暗号のことをいいます。前者は、暗号化されたままで暗号文に隠されたメッセージの和を計算できることから、加法準同型性と呼ばれ、後者は同様に乗法準同型性と呼ばれています。これまで加法準同型性を有する暗号としては、岡本－内山暗号［14］や Paillier 暗号［15］が知られています。また、RSA 暗号や ElGamal 暗号は乗法準同型性を備えています。

加法と乗法の両方の準同型性を同時に満足する暗号は、「完全準同型暗号」と呼ばれます。整数上の加法と乗法が暗号化したまま計算できれば、それに基づいて排他的論理和、論理積、否定といったビット演算を暗号化したまま計算できます。これらのビット演算を組み合わせることによって、入出力を暗号化したまま任意のロジックの計算処理回路を構成できます。すなわち、あらゆるプログラムは計算処理回路として表現できます。つまり、完全準同型暗号があれば、クラウド上のどのようなプログラムに対しても、入力を暗号化したまま処理できるような仕組みを作り出せるのです。長い間、完全準同型暗号を安全に実現する方法は未解決の問題でしたが、2009 年に IBM T.J. ワトソン研究所に在籍する Craig Gentry によって、初めて完全準同型暗号の安全な構成方法が提案されました［16］。それ以降、この分野では暗号化・復号の効率性を上げるなど活発な研究が進展中です。原理的には、データを秘匿したまま外部で代理処理するシナリオに有効であるため、クラウド上での機密データの処理などへの応用が期待されています。

❺ おわりに

本稿では、IBM 基礎研究部門におけるサイバー・セキュリティー関連の研究開発プロジェクトを中心に、最新の技術動向を紹介しました。サイバー・セキュリティーの問題を解決するために必要な技術領域は幅広く、複数の技術の組み合わせによって対策を行うことが必要です。IBM は、研究および製品開発、セキュリティー・サービスやコンサルティングなど、広範囲のサポート力が強みです。今後もこれらのチームが団結し、社会や技術の変化に対応しながらお客様の問題を解決して行きたいと考えています。

［参考文献］

[1] George Lawton: New Technology Prevents Data Leakage, Computer 41(9), IEEE Computer Society (2008).
[2] Understanding and Selecting a Data Loss Prevention Solution, http://securosis.com/publications/DLP-Whitepaper.pdf
[3] Secure by Design, http://www.ibm.com/security/
[4] The Trustworthy Computing Security Development Lifecycle, http://msdn.microsoft.com/library/ms995349.aspx
[5] O. Tripp, M. Pistoia, S. Fink, M. Sridharan and O. Weisman: TAJ: Effective Taint Analysis of Web Applications, PLDI'09 (2009-9).
[6] Takaaki Tateishi, Marco Pistoia and Omer Tripp: Path- and Index-sensitive String Analysis based on Monadic Second-order Logic. ISSTA'11 (2011).
[7] Adam Kieyzun, Philip J. Guo, Karthick Jayaraman and Michael D. Ernst: Automatic creation of SQL Injection and cross-site scripting attacks. ICSE'09, http://dspace.mit.edu/bitstream/handle/1721.1/42836/MIT-CSAIL-TR-2008-054.pdf (2009).
[8] R. Milner：プロセス代数, Communication and concurrency, Prentice-Hall, Inc., ISBN:0-13-115007-3, (1989).
[9] J. E. Hopcroft, R. Motwani, J. D. Ullman：有限状態オートマトン, Introduction to Automata Theory, Languages, and Computation,Addison Wesley,ISBN: 0201441241, (2000).
[10] E. M. Clarke, O. Grumberg, D. A. Peled：論理, Model Checking, MIT Press, ISBN 0-262-03270-8, (1999).
[11] Karthikeyan Bhargavan, C´edric Fournet and Andrew D. Gordon: Verifying Policy-Based Security for Web Services. CCS'04. ACM, http://research.microsoft.com/en-us/um/people/fournet/papers/verifying-policy-based-security-for-web-services-ccs.pdf (2005).
[12] ZTIC, http://www.zurich.ibm.com/ztic/
[13] IBM Secure Enterprise Desktop, http://www.zurich.ibm.com/secure-ed/
[14] T. Okamoto and S. Uchiyama: "A New Public-key Cryptosystems Secure as Factoring," Eurocrypt '98, pp. 308-318, Springer-Verlag (1998).
[15] P. Paillier: Public-Key Cryptosystems Based on Composite Degree Residuosity Classes, Eurocrtpt '99, pp. 223-238, Springer-Verlag (1999).
[16] C. Gentry: Fully Homomorphic Encryption Using Ideal Lattices, STOC, ACM (2009).

日本アイ・ビー・エム株式会社
東京基礎研究所 サービス・イノベーション・ラボ
シニア・テクニカル・スタッフ・メンバー

浦本 直彦 **Naohiko Uramoto**

［プロフィール］
1990 年日本 IBM 入社。以来同東京基礎研究所にて、自然言語処理、XML/Web セキュリティーなどのプロジェクトに従事。現在は、2011 年に設立されたサービス・イノベーション・ラボを担当しクラウドおよびセキュリティーに関するプロジェクトをリードしている。博士（工学）。2010 年より情報セキュリティ大学院大学連携教授を兼務。

日本アイ・ビー・エム株式会社
東京基礎研究所 サービス・イノベーション・ラボ
スタッフ・リサーチャー

立石 孝彰 **Takaaki Tateishi**

［プロフィール］
2003 年日本 IBM 入社。以来主にプログラム解析・検証にかかわるプロジェクトに従事。IPSJ SIGSE 運営委員、JSSST 理事などを務める。博士（工学）。

日本アイ・ビー・エム株式会社
東京基礎研究所 サービス・イノベーション・ラボ
スタッフ・リサーチャー

三品 拓也 **Takuya Mishina**

［プロフィール］
2004 年日本 IBM 入社。以来同社東京基礎研究所にてセキュリティー・コンプライアンス関係、特にドキュメント・セキュリティーの研究に従事。情報処理学会会員。

日本アイ・ビー・エム株式会社
東京基礎研究所 サービス・イノベーション・ラボ
スタッフ・リサーチャー

渡邊 裕治 **Yuji Watanabe**

［プロフィール］
2001 年日本 IBM 入社。以来同東京基礎研究所にて、P2P 技術、プライバシー保護、RFID、トレーサビリティー技術、トラステッド・コンピューティングに関する研究開発に従事。東京工業大学大学院非常勤講師。博士（工学）。