「信頼できるコンピューター」のための技術

日本アイ・ビー・エム株式会社
東京基礎研究所
IBMディスティングイッシュト・エンジニア
丸山　宏

Hiroshi Maruyama
IBM Distinguished Engineer
Tokyo Research Laboratory
IBM Japan, Ltd.

プラットフォームの信頼は、まず「それが何か（そのプラットフォームを物理的に識別する、すなわちプラットフォームの認証）」の情報に基づく必要があります。これまでも認証には暗号鍵などの技術が使われていました。しかし、鍵といってもデジタル情報ですので、普通に記憶装置に格納したりするだけではコピーされる危険が付いて回ります。そこで、鍵をハードウェア（具体的にはチップ）の中に格納し、絶対にチップの外に出さない仕組みが考え出されました。それがTPM（Trusted Platform Module）と呼ばれるセキュリティー・チップです。次に求められるのが「それが思った通りのものか」の確認です。プラットフォームが物理的に認証されたとしても、そのプラットフォームが信頼できるとは限りません。そのプラットフォームで現在動いているソフトウェアが必ずしも信頼できるわけではないからです。しかし、ソフトウェアの信頼性の検証をソフトウェアだけで行うのには限界があります。そこで、ここでもTPMにソフトウェアの観測を担わせることにしました。このような「信頼できるコンピューター」のためのTPMは、TCG（Trusted Computing Group）の活動の中から開発されたものです。一方、ソフトウェアが複雑になるにつれてセキュリティーの脆弱性が指数関数的に増加していることを背景に、「セキュリティーは品質の問題の一部としてとらえなければならない」という考え方が新しい動きとして起こり、セキュリティー・エンジニアリング、すなわち、セキュアなシステムをつくる手法が注目されています。そのための認証基準が製品単位・組織単位・マネジメント単位で作られ、多くの企業がその取り組みを始めています。

Technologies for "Trusted Computers"

For a platform to be trusted it is first necessary to classify the platform according to its physical type, in other words, conduct a platform authentication. Until now authentication was carried out using encryption keys and similar technologies. However, encryption is also a form of digital information, and carries the risk of allowing information to be copied just by storing it in a memory device such as a memory card. To preclude such risks, it was decided to incorporate the keys into the hardware (i.e. in a chip), which could never be taken out of the system. These are called TPMs (Trusted Platform Modules). Next came the problem of reliable verifications because even if a platform is verified physically, it does not necessarily mean that the platform is reliable since the software working on the platform may not be so. But there are limitations to verifying reliability using only that software. So it was decided to have the TPM also perform observations of the software. TPMs to create "trusted computers" have been developed through the activities of the TCG (Trusted Computing Group).

With software becoming more and more complex, security vulnerability is increasing exponentially. So there is a growing movement to consider security as a criterion to judge the quality of a software product. Security engineering -- employing techniques for building secure systems -- is attracting wide attention and many companies are now making serious efforts to formulate authentication criteria by product, by organization, and by management.

チップがプラットフォームを認証

例えば、あなたが遠隔地にいる知人A氏に機密情報を記載したメールを送り、そのA氏のコメントを付けてB氏に転送してもらうことにします。さて、そのメールをきちんとA氏のコンピューター・プラットフォームに送り、コンピューター・ウィルスなど悪意を持ったプログラムに汚染されていない状態で“正しく”B氏に届けるにはどうしたらいいでしょうか？

ここでいうプラットフォームとは、ハードウェア、OS（Operating System）、アプリケーションを含めたコンピューター・システムのことですが、上記の設問には、「信頼できるコンピューターとは何か」という問題が含まれています。

プラットフォームの信頼は、「それが何か」「それが思った通りのものか」という二つの情報に基づく必要があります。

まず「それが何か」ですが、この解を導くには、そのプラットフォームを物理的に識別し、それが偽物でないことを確認しなければなりません。すなわち、プラットフォームの認証です。これまでも認証については、種々の認証プロトコルが開発され、パスワードを暗号化する、暗号鍵を使うといった工夫がなされてきました。しかし、鍵といってもデジタル情報ですので、ソフトウェアの中に組み込んだり、普通に記憶装置に格納したりするだけではクラッカーなどによって侵入され、コピーされる危険が付いてまわります。そこで、鍵をハードウェア（具体的にはチップ）の中に格納し、絶対にチップの外に出さない仕組みが考え出されました。それがTPM（Trusted Platform Module）と呼ばれるセキュリティー・チップです。このTPMを埋め込んだプラットフォームであれば、安全な鍵を使って相手が間違いなく本物だと識別でき、先の例ではA氏がB氏に確信を持ってメールを送ることができるわけです。

長年の技術的な課題、ソフトウェアの検証

では次に、「それが思った通りのものか」ということの確認です。

プラットフォームが物理的に認証されたとしても、そのプラットフォームが信頼できるとは限りません。そのプラットフォームで現在動いているソフトウェアが必ずしも信頼できるわけではないからです。先の例でも、もしA氏の使っているメール・ソフトウェアがコンピューター・ウィルスなどで汚染されているとしたら、システムが正常に動かなかったり、A氏から転送されたメールを介してB氏のプラットフォームにコンピューター・ウィルスが伝染したりする恐れがあります。

ソフトウェアが汚染されていないことを調べる代表的な技術としてはアンチコンピューター・ウィルス（コンピューター・ウィルス対策ソフトウェア）があります。しかし、アンチコンピューター・ウィルスは、既に知られているコンピューター・ウィルスにしか対応できませんし、また、アンチコンピューター・ウィルスそのものが汚染された場合に、そのことを検出することが困難になります。

このように、ソフトウェアの信頼性の検証をソフトウェアだけで行うのには限界があります。完全性を検証するモジュール自身が汚染されていたら、そのソフトウェアから生成される指標は信頼できないからです。

では、遠隔地にあるコンピューターの上で動いているソフトウェアを信頼できる方法で観測するには、どうしたらいいのでしょうか。それは長年の技術的な課題でした。そして、その解への結論は、ハードウェアにサポートさせようということでした。ここでもTPMが登場します。

TPMにはPCR（Platform Configuration Register）と呼ばれる特殊なレジスターがあり、このレジスターにソフトウェアの観測値を格納します。ただし、TPM単独でソフトウェアを観測するのはコストがかかりますので、ソフトウェアの助けを借ります。パソコンにはBIOS（Basic Input Output System）と呼ばれる、コンピューターの基本動作命令を集めたプログラム群の領域がありますが、BIOSの最初の64Kバイトは通常書き換え不能になっています。このため、この部分のソフトウェアは汚染される可能性がないので信頼することができます。このBIOS領域とTPMを組み合わせること

によって、そのプラットフォームで動いているソフトウェアを正しく観測することができるのです。具体的には、観測されたソフトウェアのハッシュ値（一方向関数で得られた160ビットのデータ）をPCRに格納します。そして、あるソフトウェアがコンピューター・ウィルスに感染してその一部が書き換えられた場合などはそのハッシュ値がまったく異なる値となるので、感染を検知し、警告を出します。また、同じ値であれば、「汚染されずに正常に動いている」、すなわち「それが思った通りのものである」ことが確認できるわけです。このようにして、BIOSがOSを、OSがミドルウェアを、ミドルウェアがアプリケーション・プログラムを観測していき、すべてが正常な状態にあることを保証するのです。

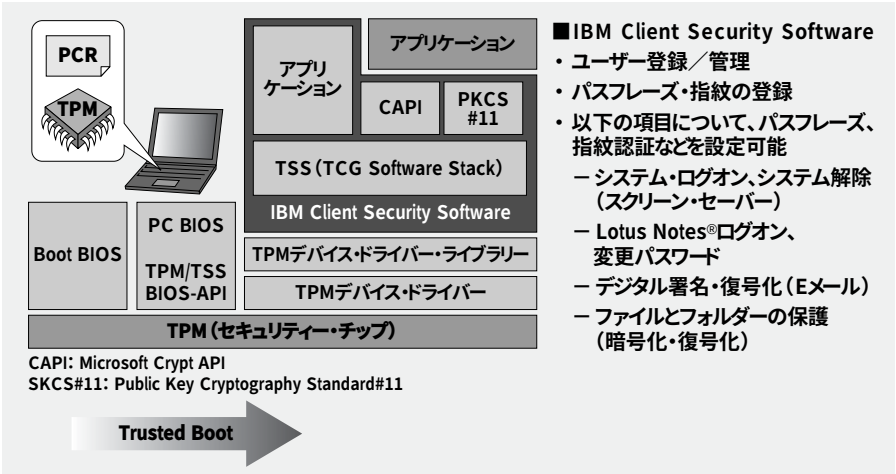

図1. IBMエンデベッド・セキュリティー・サブシステム

広がるTCG技術

以上のような、「信頼できるコンピューター」のためのTPMは、TCG（Trusted Computing Group）の活動の中から開発されたものです。

TCGは、サーバー、PC（Personal Computer）、携帯電話など、さまざまなプラットフォームに適用可能な、信頼できるコンピューター・プラットフォームのためのハードウェア構成要素とソフトウェア・インターフェースの、オープンで非営利な標準仕様の開発・普及をミッションとするフォーラムです。AMD社、Hewlett-Packard社、IBM、Intel®社、Microsoft®社の5社が発足の中心となり、世界を代表するハードウェア／ソフトウェア・ベンダーや半導体メーカーなどが会員企業になっています。

既にTCG仕様であるチップ（TPM）も発表・市販されており、IBMでもノートブックPC ThinkPad®の2002年4月以降のモデルにはTCG準拠のTPMを搭載しています。さらに、TPMの働きをサポートするソフトウェアとしてIBM Client Security Softwareを発表。この製品は、クライアントの鍵管理を安全に行うものであり、Windowsのログイン・パスワードのより強固な保管、ファイルの暗号化などの機能を備えています（**図1**）。

このようにPCの世界ではTCG技術が着々と広がっていますが、今後注目されるのは、サーバーや大型コンピューター用のTPMチップの開発・実装です。それが実現されれば、e-ビジネス・オンデマンドの世界でのセキュリティー性能が確実に高まります。例えば、ネットワーク上のコンピューターを共通資源として巨大な計算を行うグリッド・コンピューティングでは計算資源を提供する計算ノードが信頼できることが前提ですが、TCG技術がそれを保証してくれるでしょう。また、TCG技術をWebサービスに適用することによって、サービスの利用者はそのWebサービスが安全なプラットフォームで提供され、自社のアプリケーションがほかのアプリケーションの影響を受けないことを確認することもできます。

Webサービスと関連して触れておきたい、将来的に注目すべきIT（Information Technology：情報技術）セキュリティー技術の一つに、Federation（連合化）があります。Webサービスに代表されるように、今後は企業ドメインを超えてアプリケーションの相互乗り入れが当たり前のように行われます。そして、このことは、セキュリティー運用システムにおいても相互乗り入れが起こり、お互いの認証システムなどを相互に使

用することを意味しています。そうすると、ゲートウェイが単なるプロトコル・ゲートウェイでは各企業のセキュリティー・ポリシーが実現できなくなってしまいます。そこで、ゲートウェイに統一管理機能を持たせようというのがFederation技術です（**図2**）。現在、パートナー企業担当者を認証する仕組みなどが研究されています。

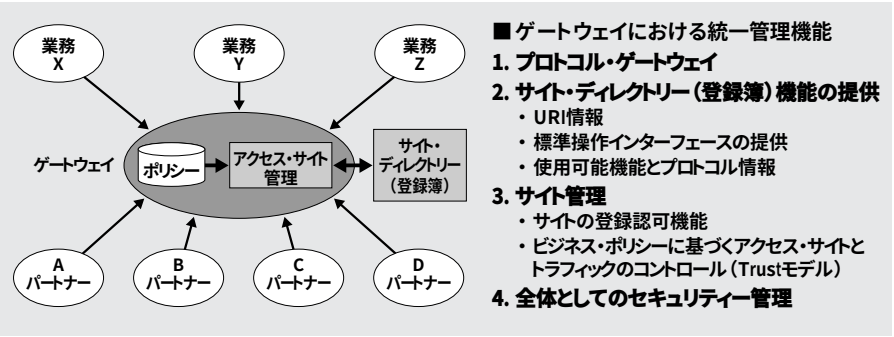

図2. Federation技術

ソフトウェアの「品質」

一方、ソフトウェアが複雑になるにつれてセキュリティーの脆弱（ぜい）性が指数関数的に増加していることを背景に、「セキュリティーは品質の問題の一部としてとらえなければならない」という考え方が新しい動きとして起こり、セキュリティー・エンジニアリング（セキュアなシステムをつくる手法）が注目され、それに沿った基準も生まれています。

ソフトウェア製品については、「製品のセキュリティー要件を明確にし、要件に対するセキュリティー強度の標準化を定めた」セキュリティー品質の基準として、CC（Common Criteria）認証ISO/IEC15408があります。EAL（Evaluation Assurance Levels）を7段階に分けて商用としてはEAL4が目標とされ、いくつかのOS製品、ミドルウェア製品はこの認証を取得しています。

ソフトウェア開発会社など、開発組織の能力アップについてはCMM（Capability Maturity Model：組織成熟度モデル）があり、ソフトウェア開発のプロセス改善のための指標として全世界で採用されています。

また、企業活動における情報セキュリティー確保のための枠組みを提供し、情報リスク管理に有用な活動の規範となるものにはISMS（Information Security Management System：情報セキュリティー・マネジメント・システム）認証基準があるのは広く知られるところで、多くの企業がその取り組みを始めています。

以上のような動向は、セキュリティーのチェックに追われる前に、まずセキュリティー製品の品質向上を図り、組織の開発プロセスやマネジメント・プロセスを改善しようというセキュリティー対策の本質を踏まえたものであり、大いに歓迎されるといえましょう。

今後は「人間系」の研究を

私はTRL（Tokyo Research Laboratory：東京基礎研究所）でWebサービスのセキュリティー技術などを研究していますが、IBMのODIS（On-Demand Innovation Service）プログラムの一環として、2003年9月～2004年4月、アイ・ビー・エム ビジネスコンサルティング サービス株式会社に出向しました。

ODISは、TRLの研究開発者が日本アイ・ビー・エムの営業サービス／コンサルティング担当者と一緒にプロジェクトを組んで、先進のテクノロジーを積極的に提供することにより、お客様のビジネスにお役立ていただくものです。

私が参画したのは半年余の短い期間でしたが、日ごろお客様と接触する機会の少ない研究開発者にとっては貴重な経験でした。情報セキュリティー・マネジメントでは「ポリシー」「プロセス」「人」が重要な要素になりますが、なかでもお客様の切実な関心は従業員のセキュリティー意識にあることを実感しました。

情報技術がセキュリティー・マネジメントにどのように貢献できるかは大きな課題ですが、今後はもっと「人間」に焦点を当て、モラルの高い、協調的な従業員をサポートするIT構築を考えていきたいと思います。