セキュリティAPIに関する技術調査

富士ゼロックス株式会社
稲田　龍

JNSAでは、独立行政法人情報処理推進機構（略称: IPA Information Technology Promotion Agency）の「2003年度 情報セキュリティ関連の調査に関する公募」のテーマ4の「セキュリティAPIに関する技術調査」に応募し、採択された。
「セキュリティAPIに関する技術調査」の目的は、IPAのホームページにある公募要領に述べられている（http://www.ipa.go.jp/security/kobo/15fy/isec2/index.html）。

> セキュリティ機能の実装に関しては、開発者によるプログラムの作成負担を軽減し、入出力や設定等を統一するための汎用APIが整備されている。ソフトウェアベンダーにおけるセキュリティ機能の実装を促進するにあたっては、セキュリティAPIを用いた設計・実装のための最新の技術情報を提供する必要がある。（公募要領P.5より抜粋）

この公募要領を受け、JNSAでは、セコム株式会社IS研究所、大日本印刷株式会社、オレンジソフト株式会社および富士ゼロックス株式会社と共同で調査を行い、2003年11月末に報告書の納品をした。
納品物はすでにhttp://www.ipa.go.jp/security/fy15/reports/sec_api/index.htmlで公開されている（サンプルプログラムは現時点2004/3/4では未公開であるが、追って公開が予定されている）。
また、同時にIPA公募のテーマ3「タイムスタンプ・プロトコルに関する技術調査」の採択も受けた。「タイムスタンプ・プロトコルに関する技術調査」に関しては、次回に報告する。
「タイムスタンプ・プロトコルに関する技術調査」の納品物もhttp://www.ipa.go.jp/security/fy15/reports/tsp/index.htmlにて公開済みである。

「セキュリティAPIに関する技術調査」を行うにあたり、開発者が実際にAPIを利用する局面において具体的に有用となる情報の提供を目的とし、個別のAPIという観点ではなく、API群を横断する技術や機能という観点からAPI関数の利用に役立つ情報に焦点を絞って報告を行うことを目標とした。
具体的には、以下の四点に重点を当て、調査を行った。

1. セキュリティAPIのアーキテクチャ
2. セキュリティAPIが共通に提供する重要な機能
3. 普及しているプラットフォーム上で提供されているセキュリティAPIの利用法
4. 近年の技術動向の中で重要性が増している新しいセキュリティAPI

報告書は全部の6つのパートよりなる。各々のパートの表題は以下のとおりである。

Part 0. 報告書の構成、セキュリティAPIの利用に関する提言
Part 1. セキュリティ API の概要、アーキテクチャ、機能、暗号技術とアルゴリズム
Part 2. Java JCE（Java Cryptographic Extensions）：機能と利用法
Part 3. .NET Crypto API：機能と利用法
Part 4. ICカードなどのハードウェアトークンAPI
Part 5. バイオメトリック認証のAPI

Part 0では、報告書のサマリと電子政府に対しての提言を行っている。

Part 1では、セキュリティAPIが共通に前提とする階層アーキテクチャについて報告し、次いで、セキュリティAPIが提供する主要な機能について概説している。また、暗号技術とアルゴリズムに関して、セキュリティAPIの機能を理解する上で最低限必要となる知識の整理が行われている。

Part 2およびPart 3では、主要なプラットフォームであるJavaとWindowsの上で提供されるセキュリティAPIである、Java Cryptography Extension（JCE）とMicrosoft Windows .NET CryptoAPIにつ

いて報告した。それぞれのAPIについて、APIの基本的な構造を述べた後、API上を利用した上位のアプリケーションの開発方法およびプリミティブの暗号機能を提供する下位のプロバイダモジュールの開発方法に関して、サンプルプログラムを例示しながら解説を行った。特に、サンプルプログラムは、JCEとCryptoAPIとで同じ機能を実装しており、比較することでより具体的な理解が得られる様に考慮して作成した。

Part 4では、クレジットカード、交通機関、住民基本台帳などの利用で注目を集めているICカードなどのハードウェアトークン上でのセキュリティAPIを報告した。まず、ICカードなどのハードウェアトークンを利用するアプリケーション開発のための主要なセキュリティAPIとして、PKCS #11とCSP(CryptoAPI)を取り上げ、基本的な構造やサポートされている関数を整理し、開発上の留意するべき点を述べた。PKCS #11とCSPを相互に運用する場合の留意点についても述べた。また、ICカード内のファイル構造の標準としてPKCS #15を、ICカードのハードウェアの差違を隠蔽し共通の開発環境を提供するための標準化動向としてGSC-ISを報告した。

Part 5では、人間の生態的な特徴・特性に基づく本人認証(バイオメトリクス認証)のためのセキュリティAPIとして策定中のBioAPIを取り上げ、基本的な構造やサポートされている関数を整理し、開発上の留意するべき点を述べた。また、近年その重要性の認識が進みつつある、バイオメトリクス認証とスマートカード・PKIとの連携について述べるとともに、GSC-ISのバイオメトリクス認証への対応状況を解説を行った。

これらの調査の元に、以下にあげる電子政府に対してセキュリティAPIの利用に関する提言を行っている。

1. アプリケーション実装者が、どのセキュリティAPIを使うべきなのか、どのようにセキュリティAPIを利用するべきなのかを明確にした資料の作成とその更新、教育が必要である。
2. セキュリティ業界に対して、必要とされるセキュリティAPIの作成支援をすべきである。そのために必要となる、技術の供与、人材の育成を行なうべきである。
3. また、3に述べるように標準化に対して積極的に関与し、独自のものとしないようにしなければならない。
4. セキュリティ関連技術は、多くの標準が定められており、それらをベースに複数のセキュリティAPIが定義されつつある。
5. セキュリティに関する標準／セキュリティAPIは、複数の学会、業界団体、標準化団体において議論され策定されている。今後、アプリケーションが必要とするセキュリティプロトコル、セキュリティ技術に関して米国政府がICカードに対してGSC-ISを定義したように、わが国においてもこれらの学会、業界団体、標準化団体に対して標準化の状況の情報入手、標準化への関与を行なうべきである。
6. セキュリティAPIが正しく実装されている事、相互運用性に問題がない事を確認するための手法、手続きの策定とこれらの確認を行なうための仕組み、運用を考えるべきである。

以上、今後PKIを利用したアプリケーションを開発する際に一番大きな問題となるセキュリティAPIの標準化を見据え、関係者が共有してほしい情報を整理してまとめてある。ぜひ本文をご参照していただけると幸いである。