インターネットにおけるセキュリティ対策方式の検討

1Ｔ－6

今井　功　　中川路　哲男
三菱電機（株）情報技術総合研究所

1. はじめに

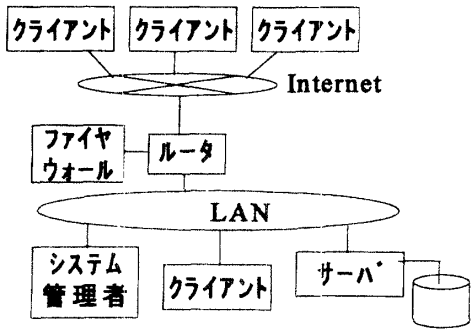
インターネットなどの外部ネットワークに接続したコンピュータシステムは、外部との情報交換が可能となる反面、悪質な侵入者によるシステム破壊やデータの盗聴及び改ざんなどの危険性が増加する。本稿では、インターネット接続システムに求められるセキュリティ要件を整理し、オープンな技術を使ってそれを満足するセキュリティ対策方式について述べる。

2. 必要なセキュリティ機能

図１に示す様なインターネット接続システムを想定する。このシステムにおいては、セキュリティ・サーバに登録されたユーザだけが、ローカルもしくはインターネット経由でクライアントからアクセスすることが出来る必要がある。その場合に求められるセキュリティ機能を以下に示す。

(1) ユーザ認証機能

サーバに接続を試みたユーザが正しいユーザであることを確認する機能。ユーザ認証機能は通常サーバで実現される。



【図１】 システム構成

(2) アクセス制御機能

ユーザのレベルに応じて実行可能な機能を制限する機能。ユーザは、登録時にクラス分けされ、属するクラスによって利用可能なサービスが異なる。

(3) データ完全性の保証

ネットワーク上を流れるデータの盗聴及び改ざんを防ぐために行うデータ暗号化。

3. 実現検討

実現方式検討に当たって採用したオープンな技術は以下の２つである。

(1) 暗号ライブラリ

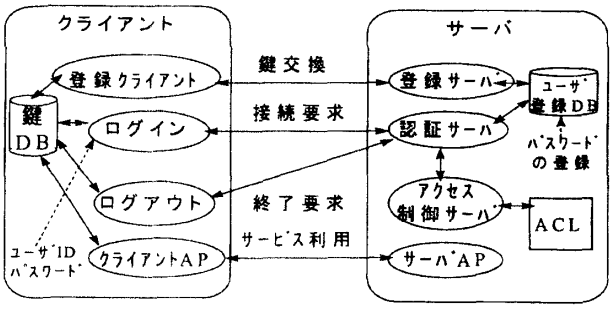
RSA, DES(Data Encryption Standard)等の各種暗号化方式をサポートし、暗号化やディジタル署名などの情報セキュリティを持つアプリケーションを開発するためのAPIを提供する。

(2) DCE(Distribute Computing Environment)

DCE[1]は、大規模な分散システムを作成および保守するために必要な基本的機能を提供するミドルウェアである。DCEは、非DCEアプリケーションに、DCEの認証機能をGSS-API(Generic Security Services Application Interface)というインタフェースによって提供している。

3.1 暗号ライブラリを用いた方式(1)

図２に本方式の概略を示す。



【図２】 暗号ライブラリを用いた方式(1)

Study on Security Countermeasure for Internet

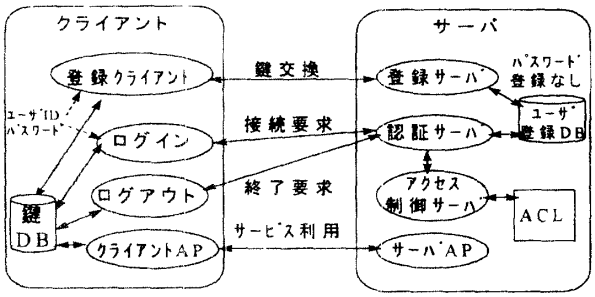
• Isao IMAI and Tetsuo NAKAKAWAJI
MITSUBISHI ELECTORIC CORPORATION

本方式では、(1)ユーザ情報データベースに登録されたデータによって認証を行い、(2)暗号ライブラリを用いてクライアント／サーバ間の通信データを暗号化する。

3.2 暗号ライブラリを用いた方式(2)

図３に本方式の概略を示す。本方式では、(1)サーバの認証機能を暗号ライブラリによって構築し、(2) 暗号ライブラリを使用してクライアント／サーバ間の通信データを暗号化する。

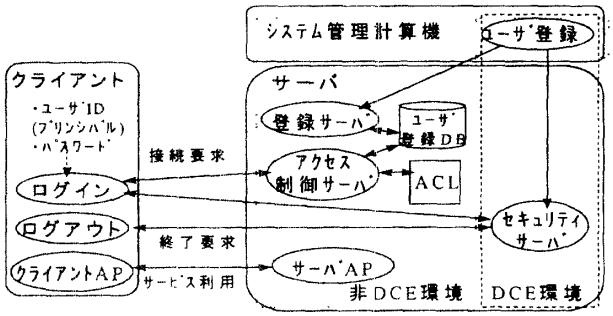
方式(1)では、パスワードは平文のまま管理されるため、データの盗聴や改ざんの危険がある。本方式では、パスワードデータを暗号化処理して保護する。



【図３】 暗号ライブラリを用いた方式(2)

3.3 DCEを用いた方式

本方式は、認証処理にDCEセキュリティ・サービスの認証機能を使用する。そのためには、サーバにDCEセルを構築し、クライアントにDCEソフトウェアを実装する必要がある。図４に、本方式の概略を示す。



【図４】 DCEを用いた実現方式

3.4 各方式の評価

各実現方式におけるセキュリティ要件の比較を表１に示す。DCEを用いた方式は、必要なセキュリティ要件を全て満足しており、特に追加する機能はない。一方、暗号ライブラリを用いた方式は、セキュリティ機能の実現は実装方法に依存し、認証機能、アクセス制御リストやパスワード管理等の管理ツールを開発する必要がある。

【表１】実現方式の比較

要件	暗号ﾗｲﾌﾞﾗﾘ(1)	暗号ﾗｲﾌﾞﾗﾘ(2)	DCE
認証機能	暗号化処理が施されていないため、パスワードが盗まれる危険がある。	パスワード情報が暗号化処理によって保護される。	DCEの認証機能を利用することで実装が不要
ア制ク御セ機ス能	実装するための機能は提供されていない。独自に実装する必要あり。	左に同じ	DCEアプリケーションであればアクセス制御機能が利用できるが、非DCEアプリケーションの場合はDCE APIを用いて独自に実装する。
デ安｜全タ性	ライブラリの組み合わせにより実装。通信データの安全性は保証される。	左に同じ	GSS-APIによる実装を行うことによってセキュアな通信が保証される。

4. おわりに

本稿では、インターネットを通じてサービスを利用するシステムのセキュリティ対策方式の検討結果について述べた。今後の課題としては、GSS-APIによる実装などを通じて詳細な検討を行っていく予定である。

参考文献

[1]Introduction to OSF DCE Version1.1 : TR ANSARC CORPORATION (1995)