MHSシステムにおけるセキュリティ機能の設計

2R−1

中尾康二　田中俊昭　加藤聰彦　鈴木健二
国際電信電話株式会社 研究所

1. はじめに

メッセージ通信システム(MHS)の標準化が進むにつれ、MHSに基づく情報通信システムが普及しつつある。それに伴い、このようなシステムのセキュリティ機能の重要性が指摘されている。MHS標準化作業においては、メッセージ秘匿や認証機能などのMHS用セキュリティ機能の拡張[1]が1988年に完了している。そこで、MHSに基づく情報通信システムにおいてセキュリティ機能をどのように実現するかが、解決すべき課題の一つとなっている。

本稿では、先に筆者らが開発したMHS P1/P2/RTボード[2]を用いたMHSシステム(以後、単に"MHSシステム"と呼ぶ)において、セキュリティ機能を実現するための設計手法について述べる。

2. MHSセキュリティ機能の概要

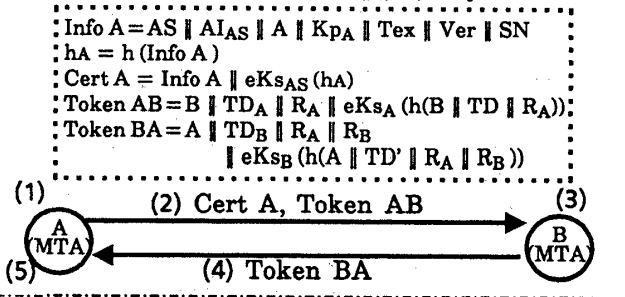
MHSは、メッセージの送/受信者に相当するMTS(Message Transfer System)利用者とメッセージの集配機能を利用者に提供するMTSからなり、MTSはさらにノード間でメッセージを実際に転送する複数のMTA(Message Transfer Agent)からなる。88年版標準には、MHSにおけるセキュリティ機能が導入され、具体的には、以下の機能が標準化された。

- UA(User Agent)とMTA、または隣接のMTA間において、それぞれ互いの認証を行い、不正なアクセスを排除する認証/アクセス管理機能
- UA間でメッセージ内容を秘匿したり、内容の完全性、順序性を保証する内容機密/完全性機能
- 正当な受取人UAに配信されたことを証明する配信証明機能
- MHSで扱う情報の作成元を保証する作成元認証、
- 利用者からのメッセージが正しく、安全に相手に配送されたことを保証する発信証明機能

以上のセキュリティ機能を保証する要素技術としては、対称暗号処理、非対称暗号処理が利用され、主に「アルゴリズム識別子(Algorithm Identifier : AI)」、「保証書(Certificate : Cert)」、および「トークン(Token)」などのセキュリティパラメータの交換によって各セキュリティ機能が実現される。以下に、認証機能の実現方式の例を示す。

MTSbind(アソシエーション確立)サービスにおいては、双方向認証が行われ、認証される側が自分の非対称暗号の秘密鍵を用いて情報を暗号化しているか否かをもって相手の正当性を判断する。図1を用いてAとB(例えば、隣接MTA間)の相互認証手順を示す。

(0):認証サーバ(AS)にアクセスする等の手順によりBの公開鍵Kp_Bを含むCert B(Bの保証書)を得る。
(1)-(2):Token ABを生成し、Aの保有するCert A(Aの保証書)とともにBに転送する。Token ABとは、AがBに対して自分を証明するための認証情報である。Token ABには、作成元を証明する署名情報sgnData、および後の通信で秘匿などに利用する対称暗号鍵encDataを相手の公開鍵で暗号化したeKpB(encData)をオプションとして追加的に保有することができる。
(3)-(4):Cert AよりAの公開鍵Kp_Aを得、Token ABを復号化しAの正当性を検証する。また、Token BAを生成し、Aに対して送る。Token BAには、上記と同様にsgnData、およびeKp_A(encData)をオプションとして追加することができる。
(5):手順(0)で得たBの公開鍵Kp_Bを用いてToken BAを復号し、利用者Bの正当性を検証する。



Info A：利用者Aを識別する情報、AS：認証サーバ名
AI_{AS}：ASで用いる認証アルゴリズム識別子、A：利用者A
Kp_A：利用者Aの公開鍵、Tex：有効期限、Ver:バージョン
SN：通番、h：ハッシュ関数、Ks_A：利用者Aの秘密鍵
eKs_A(X)：利用者Aの秘密鍵Ks_Aで情報Xを暗号化、
‖：連結、TD_A：利用者A発行の日付、R_A：A生成の乱数

図1 MHSにおける認証手順

3. MHSシステムへのセキュリティ機能の設計

(1) 既開発のMHSシステム利用のための考慮点

本稿で対象とする既開発のMHSシステムは、UAとMTAが同一ホスト上に実装され、UA機能は基本的に利用者プログラムが提供し、下位層機能からMTA機能、P2メッセージの符号化/復号化機能までを通信ボード上で実現するもので、上述のMHSセキュリティ機能を搭載する上で、以下のような点を考慮する必要がある。

- 通信ボードは、汎用32ビットCPUを用いているため、非対称暗号の多倍長処理などを実行させるには能力が不足する。従って、非対称暗号処理、

Design of Secure MHS System
Kouji NAKAO, Toshiaki TANAKA, Toshihiko KATO and Kenji SUZUKI
KDD R & D Laboratories

対称暗号処理については、通信ボードの外に専用セキュリティ処理部を設け、そこで実行させる。

- UAとMTAが同一ホスト上にあり、双方のセキュリティ処理は極めて類似しているため、実装効率を考慮し、セキュリティ処理部は、UAとMTAから共通に利用できるようにする。

(2) セキュアMHSシステムの構成要素

以上の考察に基づき、通信ボードを用いたMHSシステムにセキュリティ機能を搭載したシステム(セキュアMHSシステム)の設計を行う。以下に構成要素を示す。(図2参照)

- セキュリティ処理部：暗号/署名処理などを実現するもので、通信ボード、および利用者プログラムから利用可能な共通セキュリティ処理モジュールである。
- セキュリティインタフェース機能部(SIF)：通信ボード、および利用者プログラムからセキュリティ処理部を共通に呼び出すためのインタフェース機能部である。
- 利用者プログラム部：UAにおけるセキュリティ機能を実現するために、セキュリティパラメータの設定、および解析を実行し、暗号/署名などは、セキュリティ処理部にSIFを介して依頼計算する。
- MHS/P1/P2/RT通信ボード：MTAにおけるセキュリティ機能を実現するために、セキュリティパラメータの設定、および解釈を実行し、具体的な暗号/署名などは、セキュリティ処理部にSIFを介して依頼計算する。

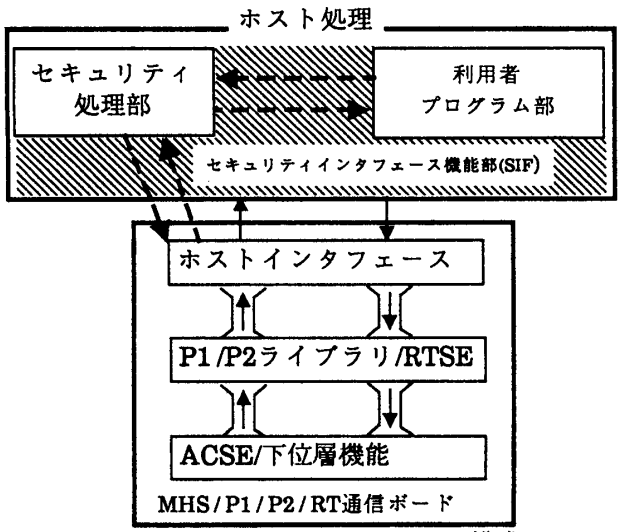


図2 セキュアMHSシステムの構成

(3) セキュリティ処理部の機能

セキュアMHSシステムにおけるセキュリティ処理部は、以下のセキュリティ関数ライブラリの提供を利用者プログラム、および通信ボードに対して共通的に行う。

- 非対称暗号化/復号化処理：保証書、トークン、および署名情報の生成、検証を実行するために使用する。
- ハッシュ処理：非対称暗号処理の前処理として暗号化対象の情報を圧縮するために使用する。
- 対称暗号化/復号化処理：対称暗号鍵encDataを用いた内容機密や完全性機能を用いる場合に使用する。なお、暗号利用モードとしては、ECB/CBCモードなどの国際標準をすべてサポートする。
- 非対称暗号鍵生成処理：非対称暗号処理を行うための公開鍵/秘密鍵のペアの生成を行う。

なお、以下の点をセキュリティ処理部の利用においては考慮する必要がある。

①証明書(Certificate)の発行：証明書の生成のために、信頼できる第3者に相当する認証サーバ(AS)が必要である。また、ASの公開鍵は、保証書の検証時に利用するため、すべてのセキュリティ利用者が保持する必要がある。

②非対称暗号秘密鍵の管理：セキュリティ利用者の非対称暗号の秘密鍵は、セキュアにその利用者によって管理される必要がある。

以下に、セキュリティ処理部が提供する具体的なメカニズムを、図1で示した認証手順で必要となる「Cert Aの正当性の検証」を例にとり示す。保証書Cert Aは信頼できる第3者(認証サーバ:AS)によって署名がなされていることが想定される。セキュリティ処理部の利用者は、署名検証の前処理としてCert Aに含まれるInfo Aのハッシュ処理を行い、$h_A = X$を取得する。さらに、検証のための非対称暗号化依頼をASの公開鍵Kp_{AS}を付けて行い、その結果$h_A = Y$を得る。その後、利用者はXとYを比較することにより、保証書Cert Aの正当性を確認する。

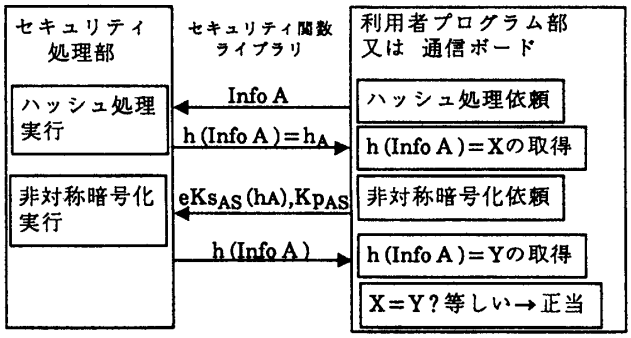


図3 Cert Aの正当性の検証メカニズム

4. おわりに

本稿では、MHS P1/P2/RTボードを用いたMHSシステムに、MHSセキュリティ機能の導入するための設計手法について述べた。今後は、その実装評価を行うこととしたい。最後に日頃御指導頂くKDD研究所小野所長、浦野次長に感謝します。

参考文献

[1] 中尾,田中,鈴木 "OSI通信環境下におけるセキュリティ技術",信学,情報伝書と信号処理ワークショップ,1992 11月
[2] 加藤,井戸上,鈴木 "MHS P1/P2/RTボードの開発",信学1993春季全国大会