暗号システムの管理方式

2Ｔ－6

田口　卓哉　　後沢　忍　　時庭　康久　　稲田　徹　　永島規充
三菱電機（株）情報技術総合研究所

1. はじめに

近年のインターネットの拡大により、専用線に変わってインターネットを利用して例えば本社／支社間の通信を行う、イントラネットという形態が注目されてきている。しかし、反面、インターネットは誰にでもアクセス可能であるゆえ、ネットワーク利用者は、クラッカーによる盗聴、なりすましといった攻撃を受けやすく、そのため、セキュリティ面が注目されるようになってきている。

我々は、これらの問題に対し、通信データの盗聴防止を目的としたネットワークセキュリティシステムＭＥＬＷＡＬＬを開発した。本システムは、２Ｔ－０４で定義される、暗号鍵事前共有型のシステムである。本稿では、本システムにおける暗号装置の管理方式について述べ、暗号装置の一元管理を行う管理装置（ＭＥＬＷＡＬＬ Ｍｇｒ）を紹介する。

2. ＭＥＬＷＡＬＬの管理形態

本システムの暗号装置は、端末とネットワークの間等に設置され、中継する通信データの暗号化／復号を行う。暗号装置内では、複数のセッション鍵をメモリ上に保持しており、システム管理者はこの中から、暗号通信に利用するセッション鍵を選択する。デフォルトで利用するセッション鍵、及びある特定のホストに対して利用するセッション鍵が選択可能である。以降、前者を基本パス、後者を特例パスと呼ぶことにする。

暗号システムを運用するにあたり、暗号側／復号側で、セッション鍵が一致している必要があり、また、基本パス／特例パスの設定も同様につじつまが合っていなければならない。これらの設定作業をシステム管理者が指揮して行うことになるが、管理者自身が、暗号装置の置いてあるサイトへ行って、逐一設定を行うか、又はサイトの利用者に通知して設定してもらうなど、管理に膨大な作業量が発生する。また、利用者に通知する場合、管理情報を第三者に対して秘匿する必要もある。

こういった問題に対して、本システムでは、管理者のみ実行権限のある管理装置を設け、暗号装置を一元管理することによって対応することにした。

管理装置の主要機能をまとめると、次のようになる。

1）管理情報の編集（追加／変更／削除）。
2）セッション鍵の生成／一括配送。
3）基本パス／特例パス情報の収集／編集／設定。

図１は、本システムの構成例である。暗号装置には、外部ネットワークの境界点に設置し、内部のＬＡＮ全体を収容するアダプタ型と、端末を収容するＨＵＢ型、及び端末内蔵型がある。

管理装置は、管理対象の暗号装置とＩＰ接続されていれば、ネットワークのどこにでも設置できる。

尚、本稿では、アダプタ型及びＨＵＢ型の管理方式について述べ、端末内蔵型については触れない。端末内蔵型の管理方式については２Ｔ－０７で説明する。

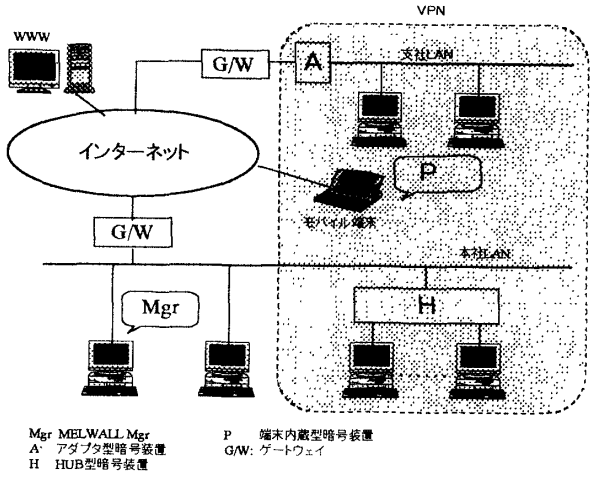

図１．ＭＥＬＷＡＬＬ概略図

3. 管理通信方式

管理通信は、ＵＤＰ上に独自構築したプロトコルによって行っている。

管理装置が、各暗号装置に対して管理通信を行う際、お互いのなりすましや、管理通信データの盗聴を防止するため、管理通信に対してセキュリティを考慮しなければならない。そのためには、認証及び暗号化の必要があるが、管理通信に対してＲＳＡ公開鍵暗号を適用することによって、セキュリティを確保することにした。

ＲＳＡ公開鍵暗号に用いる暗号鍵は、暗号装置導

Management Method for a Encryption System

Takuya TAGUCHI, Shinobu USHIROZAWA, Yasuhisa TOKINIWA,
Toru INADA, Norimitsu NAGASHIMA
Information Technology R&D Center, Mitsubishi Electric Corporation

入時に、管理装置で各暗号装置毎のＲＳＡ鍵を自動生成し、秘密鍵の方を暗号装置にあらかじめ設定しておく。公開鍵は管理装置側で保持しておく。

実際には、このＲＳＡ暗号に加え、演算処理の高速化をはかるため、当社の共通鍵暗号アルゴリズムである、ＭＩＳＴＹを併用している。

3.1. シーケンス

管理通信のシーケンスは、管理装置から要求を発行し、暗号装置が応答を返すというシンプルなものである。情報の収集を例にとって以下に説明する。

1)管理装置は、ＭＩＳＴＹ鍵等をＲＳＡ公開鍵で暗号化して収集要求フレームを作成し、暗号装置へ送信する。

2)暗号装置は、受信した収集要求フレームをＲＳＡ秘密鍵で復号してＭＩＳＴＹ鍵を取得し、自身のもつ管理情報をそのＭＩＳＴＹ鍵で暗号化して管理装置へ送信する。

3.2. 暗号化及び認証について

管理フレームの管理情報を全て暗号化しているので、第三者による盗聴を防止できる。

また、要求フレームのＲＳＡ暗号部分に固定情報を含め、暗号装置においてそれを確認することにより、要求フレームが正規の管理装置発行のものであることを認証している。

更に、ＲＳＡの公開鍵及び秘密鍵を非公開とすることによって、セキュリティを強化している。

4. 管理装置の実現方式

管理装置の実現方式について簡単に述べる。

動作環境は、ユーザ管理、ファイルへのアクセス権限等、セキュリティが考慮されていることから、WindowsNT を選んだ。

図２に、管理装置のモジュール構成、表１に管理装置の機能一覧を示す。暗号装置管理モジュールは、諸機能を、暗号制御処理、通信制御処理、ログ制御処理を使って実現する。通信制御処理は Winsock によって管理通信を行い、セッションを管理するものであり、暗号制御処理は当社製暗号エンジンによって、管理フレームの暗号化を行う。ログ制御処理は、管理通信やファイルアクセスの履歴を、WindowsNT 付属のログ機能によって保存する。

管理装置のＧＵＩは、管理対象とする暗号装置についての、以下の情報をリストで表示したものである。

- ホスト名
- 装置タイプ(HUB 型／アダプタ型)
- コメント
- セッション鍵配送実行結果
- その他の管理通信の実行結果

ユーザは、このリスト上で暗号装置を選択し、セッション鍵配送等の各種操作をメニュー実行する。

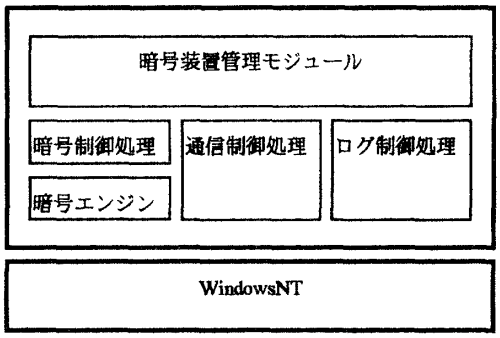

図２．管理装置のモジュール構成

表１．管理装置の機能一覧

機能	内容
暗号装置編集機能	管理情報の編集（暗号装置の登録／変更／削除，最大５００台）。
	管理情報の保存／読み込み／印刷。
	管理通信用 RSA 鍵の生成／保存。
	暗号装置検索／表示ソート。
ｾｯｼｮﾝ鍵管理機能	ｾｯｼｮﾝ鍵の生成／配送／保存。
ﾊﾟﾗﾒｰﾀ管理機能	基本パス、特例パス、ＳＮＭＰ情報、ポート認証情報の編集／収集／設定／保存／読み込み。
その他の機能	セッション鍵チェック。
	暗号装置リブート。
	暗号装置タイプ情報取得。

5. まとめ

今回、ネットワークセキュリティシステムＭＥＬＷＡＬＬにおける管理方式について検討し、管理装置ＭＥＬＷＡＬＬ Ｍｇｒを開発した。

今後の課題としては、ネットワーク構成が把握できるユーザインタフェースへの改良、といったものがある。

参考文献

[1] 馬場他：“ネットワークセキュリティ（盗聴防止）とセキュリティドメインに関する一考察”，情報処理学会第５１回全国大会，１９９５

[2] 横山他：“LAN 暗号装置の実現方式”，電子情報通信学会総合大会，１９９７