暗号システムへのリモート端末収容方式

2T－7

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

1．はじめに

インターネットのビジネスユースの普及を背景に、携帯端末やリモートアクセスソフトウェアの普及によって、出張先のモバイル端末あるいは自宅の端末から社内ネットワークにアクセスするリモートワーカが急増している。これらのリモートワーキングをビジネスレベルで考えた場合、セキュリティの確保は必須となる。具体的には、正規ユーザに対してのみサービスを提供するためのアクセス制御や認証機構と、インターネット上を流れるデータを秘匿するための暗号機構が必要になる。

前者は社内への入口にファイアウォールやアクセスサーバを設置し、認証サーバやワンタイムパスワード等と組み合わせて運用するのが一般的である。後者は、メールや WWW のようなアプリケーションレベルの暗号と、アプリケーションに依存しないネットワークレベルの暗号に大別でき、どちらを使うかは組織のセキュリティポリシーによる。最近では、ファイアウォールに暗号機能を付加し、ファイアウォール間あるいは、専用の暗号ドライバやソケットライブラリをインストールしたリモート端末との間で暗号通信を実現する製品が多数発表されている。

これらの製品は、アクセス制御，認証，暗号化を同時に実現できる反面、他社製品との互換性は今のところなく、ファイアウォールの普及度から判断して、既存機器の置き換えに難色を示すユーザも多いと思われる。

筆者らは、既存のアクセス制御や個人認証技術に暗号機能を付加するというアプローチにより、前出の論文 2T-04 で定義される暗号鍵*事前共有型のシステムを考案した。本稿では、同システム上でリモートワーキングを実現する際の方式について、特に暗号化に着目した場合の課題と解決策を述べる。

＊：データの暗号化に用いるセッション鍵のこと。本稿では暗号鍵あるいは単に鍵と表記する。

2．リモートワーキングを実現するための課題

筆者らの考案したシステムは、既存のネットワークに暗号装置をアドオンすることによって LAN を含むネットワーク上を流れるデータを暗号化しており、一般のユーザに暗号装置の存在や暗号化によって守られているという事実を意識させない構造になっている。つまり暗号装置の管理やシステムの運営は、ごく一部の管理者が行うことを前提にしている。暗号鍵の更新なども専用の管理装置によって行っている。

一方、リモートワーカのワーキング形態は公衆網接続されたパソコン（ノート，デスクトップ）によるものが殆どであり、この形態に暗号装置をアドオンするのは現実的ではない。筆者らは暗号ドライバソフトウェアという形で暗号装置の機能を端末に内蔵することでこの問題を解決した。端末への内蔵は問題解決の最適な方法であるが、同時に表１に示す新たな課題を生み出している。

表１．端末内蔵型の課題

比較要素	方式		端末内蔵型の課題
	暗号装置	端末内蔵型	
管理形態	専従管理者	不特定多数のユーザ	暗号鍵の流出等の危険性が増す。
運転形態	２４時間	操作時のみ	管理装置主導の鍵配送ができない。
IP アドレス	固定	ダイアルアップ時に確定	既存の管理通信方式になじまない。
設定	管理者	各ユーザ	予想外のセキュリティホール出現の可能性。

課題を整理すると、端末内蔵型に対する鍵配送手段の確保と、配送された鍵の端末上での安全な管理の２つに集約される。前者に対しては端末側主導の鍵配送方式を確立する、後者は暗号鍵の常駐期間をできるだけ短くし、かつユーザが設定可能なパラメータをある程度限定するという方向でアプローチを行う。

Remote Terminal Support by An Encryption System

Shinobu USHIROZAWA, Yasuhisa TOKINIWA, Toru INADA, Takuya TAGUCHI and Norimitsu NAGASHIMA
Information Technology R&D Center, Mitsubishi Electric Corporation, 5-1-1 Ofuna, Kamakura, 247 JAPAN

3．課題解決のアプローチ

リモートワーキングの殆どは、リモートワーカ側がクライアントとして社内のサーバにアクセスするという形態であると言ってよい。この場合、リモート側は端末内蔵型（暗号ドライバソフトウェア）を使用し、サーバ側には暗号装置を接続するという形態が一般的である。暗号鍵事前共有型のシステムでは、リモート側とサーバ側で同じ暗号鍵を予め持っている必要がある。サーバ側の暗号装置には管理装置から鍵の配送が行われるが、これと同じ鍵をリモート側も入手しなければならない。リモート側は通常は電源が入っておらず、またIPアドレスも確定していないため、管理装置による従来方式の配送の対象とすることはできない。従ってリモート側には、電源投入時等のタイミングで自発的に鍵を取得する機構が必要である。本機構の実施例を図1，2に示す。

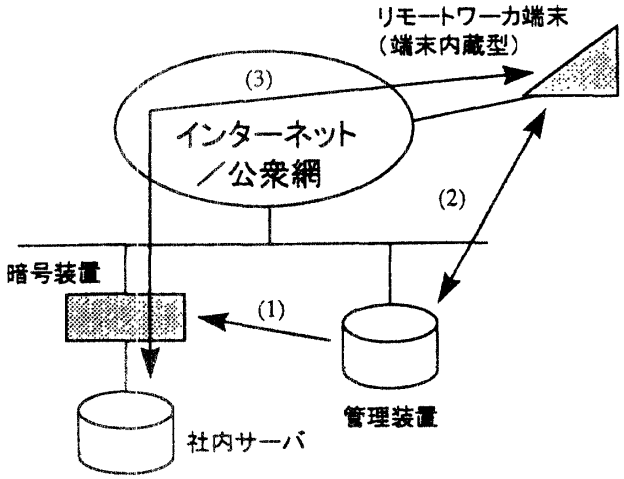

図1．暗号通信成立までの手順

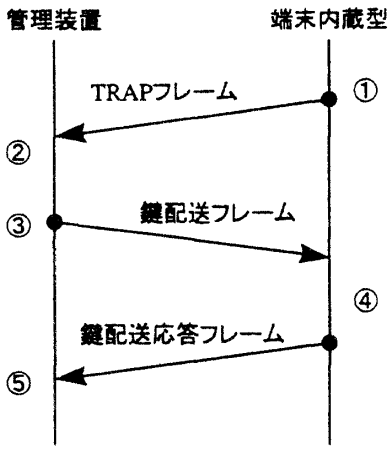

図2．端末内蔵型への鍵配送シーケンス

図1の手順について説明する。 (1)管理者は任意のタイミングで管理装置を操作し、暗号装置に対する鍵配送を実施する。 (2)リモートワーカは端末起動等のタイミングで、管理装置に対して図2に示す鍵配送シーケンスを起動して、鍵を入手する。入手した鍵は端末の不揮発性メモリには保存されない。 (3)社内サーバへのアクセス時、(2)で入手した鍵によりネットワークを流れるデータは暗号化される。これを受信した暗号装置は(1)で配送された鍵を使って復号し、社内サーバに渡す。サーバからの応答は逆の手順によりネットワーク上で暗号化される。

次に図2の手順を説明する。図は管理装置と端末内蔵型との通信シーケンスを示すものであるが、各通信フレームは前出の論文2T-06同様、公開鍵暗号を用いて暗号化されており、相手認証と情報秘匿が実現されている。 ①端末内蔵型はTRAPフレームを管理装置に送信する。TRAPには端末を識別する情報等が格納されており、これらの情報は予め設定しておいた管理装置の公開鍵で暗号化されている。 ②管理装置はTRAPを自己の秘密鍵で復号して端末識別情報等を得る。この情報を基に端末に許可された鍵のみを格納した鍵配送フレームを作成する。同フレームは端末側の公開鍵で暗号化されている。 ③暗号装置への鍵配送と同じ手順により、鍵配送フレームを送信する。この時の宛先IPアドレスは、TRAPフレーム内の送信元アドレスを用いる。 ④端末内蔵型は自己の秘密鍵で復号して暗号鍵を得ると共に、鍵配送応答フレームを送信する。尚、端末側で使用する公開鍵／秘密鍵はユーザのパスワード等で暗号化された状態で端末内に保存されている。 ⑤配送結果を保存すると共に、イベントログを残す。

4．まとめと今後の課題

リモートワーカを暗号システムに収容する方式について述べた。本方式によれば、リモートワーカは必要な時に認証と暗号を兼ねた安全な手順により暗号鍵を入手することができる。また入手した鍵にはユーザの権限等が反映されており、かつ端末内には残らないので、エンドユーザの不注意による暗号鍵の流出やセキュリティホール出現の危険性を抑えることができる。今後はセキュリティ産業の国際的な流れや、次世代のインターネットワーキング技術への対応に備えて、IPSECやMobile-IP等の技術の取り込みが不可欠であると考える。

参考文献

妹尾他“ネットワークセキュリティのためのパケット暗号化方式に関する一考察”，情報処理学会第51回全国大会，1995
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