

セキュリティシステムのネットワーク管理

1 T-6

伊藤 陽子

(株) 東芝 府中工場

1. はじめに

最近のインターネットの急速な普及に伴い、企業に限らず個人ユーザも気軽に使用できるような環境が調ってきた。一方では、これまであまり重要視されてこなかった不正アクセスやデータの漏洩といったセキュリティ問題が表面化し、もはや後回しにできない状況になりつつある。

そこで東芝では、データの暗号化や認証機能を持つ Network CryptoGate (以降、NCG) を開発した。この中の1つのサブシステムとして、NCG が必要とする各種セキュリティ情報や運用状況の監視など、NCG の運用上なくてはならない NCG 管理サーバの開発を行った。ここでは、セキュリティ製品である NCG を管理する上で重要となる考え方について、いくつか紹介する。

2. Network CryptoGate とは

NCG は、インターネット標準のセキュリティ機能とモバイル機能をサポートした、ネットワークセキュリティ製品である。NCG サーバ、NCG クライアント、NCG 管理サーバの3つのサブシステムから構成される。それぞれの役割は以下の通りである。

●NCG サーバ

IP ネットワーク上で、他の NCG サーバとの間に仮想的な専用線である Virtual Private Network (以降、VPN) を構築する。パケットの暗号化／復号化を行い、公衆回線上での安全な通信を実現する。また NCG クライアントがインストールされた携帯

パソコン宛てに送られたパケットの転送処理を通して、モバイル接続を支援する。

●NCG クライアント

NCG サーバと連携を取り、組織内で使用している PC に、外出先から IP アドレスなどを変更しないままのアクセスを可能とするモバイル接続を可能とする。暗号化機能との組合せにより、通信データの安全性を高めることができる。

●NCG 管理サーバ

通信関係を結ぶ NCG サーバや NCG クライアントに関する環境情報の管理、暗号鍵管理などを行う NCG 情報管理機能と、それらの運用状況の監視を行うネットワーク管理機能を提供する。両機能を組み合わせることにより、同一のサーバから NCG に関する全ての管理作業を行うことができるのが特徴である。

NCG を利用することで、外出先から携帯パソコンを使用して自社のイントラネットにアクセスする際、社内で利用する環境と同一の環境でのアクセスを可能にすると同時に、VPN を構築することで通信データの安全性を高めることができる。

NCG 管理サーバとして動作するマシンには、NCG サーバをもインストールしておく必要がある。NCG 管理サーバが他の NCG サーバや NCG クライアントとの間で行う管理のための通信も、セキュリティの観点から VPN により守られている必要があるからである。NCG 管理サーバを動作させるマシンに NCG サーバ機能を持たせることにより、環境情報や暗号鍵を安全に各 NCG サーバおよび NCG クライアントへ配布することができる上、NCG の運用状況の監視も安全に実施することができるのである。

Network Management in a Security System

Yoko Itoh

Toshiba, Fuchu Works

1 Toshiba-cho, Fuchu-shi, Tokyo, 183, Japan

3. NCG管理サーバの重要性

近年の市場では、認証情報の作成、配布、管理を主に担う製品が出現するなど、セキュリティにおける認証情報の扱いが非常に重要視されてきていることがわかる。NCG においても、実際の運用形態を考えると暗号化および認証の全てを握る鍵を如何に管理するかが最も重要な問題である。特に NCG では、物理的に固定された機器だけでなく移動した携帯パソコンも暗号化／復号化を行うため、鍵は1ヶ所で集中管理する必要がある。

そこで鍵や環境情報の管理機能を VPN および移動 IP 機能から切り離し、一つのサブシステムとして独立させることにした。

また現状では VPN の暗号化機能はソフトウェアで実現しているが、今後はルータやハブといったハードウェアに取り込んでいく方向にある。このとき鍵の管理機能までもハードウェアに持たせてしまうと、一旦運用を開始して野に放ってからの鍵変更や新しい NCG の追加作業が困難になることは間違いない。その点、鍵の管理機能を暗号化機能とは別にソフトウェアで実現しておけば、このような場合にも柔軟に対処できる。

4. 鍵の配布

NCG の運用を開始する前にまず必要な作業は、VPN 構築に必要な公開鍵／秘密鍵や各種環境情報を、これらを一元管理している NCG 管理サーバから何らかの形で入手することである。この際の入手方法としてまず考えられるのが、SNMP による通知方法である。NCG 管理サーバ起動時に、NCG 管理サーバの公開鍵や環境情報を SNMP のプロトコルの一つである set-request を使用して各 NCG サーバおよび NCG クライアントに配布するという方法である。ここで set-request は、マネージャ（管理側）がクライアント（被管理側）内部の管理情報を操作するためのプロトコルである。しかしこの方法では NCG 管理サーバ起動直後、VPN を構築しない段階で公開鍵や環境情報をインターネット上に流すことになり、セキュリティ上危険であることは否

めない。そこで最もセキュリティが高いのはやはりオフライン通信であるという原則に立ち返り、物理的に隔絶された記憶媒体を介して配布するという方法が最も安全、確実であるという判断から、フロッピーディスクを使用する方法を採用することにした。NCG の運用環境構築の基本となる情報を第三者に盗まれることを防ぐため、敢えて人の手に頼った、原始的ではあるが確実な手段を選んだのである。

5. 移動 IP の拡張 MIB

NCG を SNMP で管理するためには、管理情報の集合体である MIB の実装が不可欠である。NCG の機能から実装する MIB は以下のように分類できる。

- ・ NCG 本体の MIB：NCG の稼働状態や鍵情報、各種ヘッダ作成処理に関する統計情報など。
- ・ VPN の MIB：鍵交換方式や各種アルゴリズムなどの、VPN 構築のために使用される環境情報。
- ・ 移動 IP の MIB：移動ノード自身やその代理転送を行うホームネットワーク上の NCG サーバに関する環境情報、移動状態や移動登録結果の統計情報など。

NCG は VPN と移動 IP という2つの技術の融合体であるため、これに適した標準の MIB はもともと存在しなかった。このため NCG を SNMP で管理するための MIB は東芝で独自に開発を行い、これを NCG に実装したのである。

6. 今後の課題とまとめ

暗号化技術、移動 IP 技術を東芝独自方式により融合したセキュリティ製品である NCG を管理するための、鍵管理およびネットワーク管理の考え方について述べた。

今後はディレクトリサービスを利用した分散管理や、NCG 管理サーバ自身が不正アクセスを受けた場合に備えるための、更に強力なセキュリティの実現などについて、検討していく考えである。