コンピュータセキュリティ 7－3
（2000．1．21）

分散ネットワークサービス管理のための セキュア通信基盤の開発

中野 喜之‡，寺田 真敏†，萱島 信†，礒川 弘実†，山崎 隆行*
(株) 日立製作所 システム開発研究所†
日立中部ソフトウェア (株)‡
(株) 日立情報ネットワーク*

あらまし: 近年インターネット上では，大規模かつ分散化したネットワークサービスが提供されるようになりつつある．ネットワークサービスを低コストで実現するには，分散した機器に対するネットワークサービス管理システムを実現し，構築，運用コストを下げることが必要である．本稿では，上記のネットワークサービス集中管理システムを実現するために開発した，様々なネットワークサービスに対応可能で，かつセキュリティを考慮したセキュア通信基盤について述べる．本通信基盤を利用することで，管理のためのセキュア通信を容易に実現でき，管理システム全体の構築コストを押さえることができる．

Development of secure communication infrastructure to manage distributed network service

Yoshiyuki Nakano‡, Masato Terada†, Makoto Kayashima†,
Hiromi Isokawa†, Takayuki Yamazaki*
Systems Development Laboratory, Hitachi, Ltd.†
Hitachi Chubu Software, Ltd.‡
Hitachi Information Network,Ltd.*

abstract: Recently on the Internet, the large scale and wide distributed network services become to be provided. To provide a network service with low cost, we need to construct the network service management system for distributed network instrument, then to decrease cost to construct and manage network service. In this paper, we explain a secure communication infrastructure that is developed for realize a network service intensive management system that can manage any various network service intensively. With using this infrastructure, it is easy to construct secure communication environment and to decrease cost to construct whole service management system.

1. はじめに

近年インターネット上では，EC(Electronic Commerce)やEDI(Electronic Data Interchange)等を行うための大規模かつ分散化したネットワークサービスが提供されるようになりつつある．これらのシステムでは，システムを構成する複数サービスが多数のホストに分散して配置されていることが多い．また，組織の大規模なネットワークでは，Web，E-Mail，Netnews サービスなどの様々なネットワークサービスを利用しており，それらのサーバは物理的/論理的にも分散配置されている．

こうした分散ネットワークサービスを低コストで実現するには，各拠点にサービスを管理するための人員を配置するのではなく，ネットワークセンタから分散した機器の管理を集中して行うサービス管理システムが有効である．すなわち，ネットワークサービス集中管理システムは，サービ

ス全体を見通した管理，また個々のサービスの一括した管理を実現することが可能であり，ネットワークサービスシステム全体の管理コストを低減させる．

ネットワークサービス集中管理システムを構築するためには，管理システムにおいて様々なサービスをリモートから統一的に管理できるようにすることが必要である．そのためには，(1) 共通の管理用プロトコルの策定，(2) リモート管理機能に対応していない既存サービスへの対応が必要である．また，管理システムは重要な情報を処理するため，(3) 管理システム全体のセキュリティの確保が必須となる．

本研究では，分散ネットワーク環境において，ネットワーク管理システム構築のためのセキュアな通信基盤を開発した．本通信基盤を使用することによって，上記の(1)～(3)を満たすネットワークサービス集中管理システムの構築が容易になる．

2. 分散ネットワークサービス管理の課題

ネットワークサービス集中管理システムを用いて分散ネットワークサービスに対する管理を実現する場合，大きく分けて以下の 2 つの課題を解決する必要がある．

(1) 集中管理システムの実現方式
(2) 集中管理システムのセキュリティ

本章では，上記の課題について説明する．

2.1. 集中管理システム実現上の課題

ネットワークサービス集中管理システムの実現方式は，管理対象となるサービスと，システムが稼動するネットワーク環境に配慮したものでなければならない．

多様なサービスの集中的な管理

分散ネットワークサービスは，多くの場合既存の複数のサービスを組み合わせ，多数のホストが協調して動作するものであることが多い．ここで利用される既存のサービスは，リモートからの管理手段が提供されていないことが多く，リモートから使用することが可能なサービス管理プログラムを作成する必要がある．

例えば，Web，E-Mail，Netnews 等のインターネットサービスでは標準的なリモート管理方式が存在しないため，新たにサービス管理プログラムを作成することになる．これらのサービス管理プログラムを効率よく開発するには，集中管理システムと通信するための統一的な通信基盤を利用することが望ましい．

サービス自体への影響

サービスの動作しているホスト上で，そのサービスを管理するためのプログラムが大量のコンピュータリソース(CPU タイム，メモリ，ネットワーク帯域等)を使用してしまうと，本来の目的であるサービス自体の動作に影響を与えてしまうことがある．ネットワークサービス集中管理システムを構築するための通信基盤は，なるべく軽量のものであるべきである．

例えば，管理機能としてサービスの稼動するホストの状況を定期的に管理マネージャに送信するようなことを行う場合，状況調査の頻度や，送信データ量などをサービスに影響しないよう調整する必要がある．

既存ネットワークとの親和性

ネットワークサービス集中管理システムを構築する場合，すでにあるネットワークシステムの構成を考慮しなければならない．

例えば，ファイアウォールやフィルタなどのアクセス制限がある場合，制限に掛らないような一般的なプロトコルを使うか，ファイアウォール自体の設定を変えるなどの選択を行わなければならない．

2.2. 集中管理システムのセキュリティ上の課題

ネットワークサービス集中管理システムは，ネットワークシステム全体に影響を及ぼす操作や情報を扱うため，管理システムやシステムの扱う情報についてのセキュリティを確保することが必要となる．

管理情報の盗聴/改ざん

管理システムとサービス間では，分散ネット

ワークシステムの運用に関する重要な情報が流れる．例えば，設定変更操作，起動/停止制御，ユーザ情報やログデータ等の情報は，悪意を持って使用されると不正侵入やサービス停止攻撃の原因となり，致命的なセキュリティホールを作成してしまう．

盗聴/改ざんされないようにするためには，通信データについて暗号化を行うことによって対処するのが一般的である．

管理システムへの不正アクセス

サービス管理プログラムに対して管理者以外が不正なサービス管理操作を行えないよう，管理者の認証や操作コマンド発信元のネットワークアドレス等によるアクセス制限を行う必要がある．

また，マルチユーザ環境のホスト上でネットワークサービスを管理する場合，ホストにログインしているユーザが管理プログラムやそのデータにアクセスできないように，読取/実行権限を適切に設定する必要がある．

3. セキュア通信基盤

2 章で述べた課題を解決するため，以下に示すセキュア通信基盤を開発した．

3.1. 概要

セキュア通信基盤は，以下に示す 4 つのコンポーネントで構成されるものである．

(1) hsd
　簡易 HTTP サーバで，主に管理対象で取得した稼動状況データの送信と後述する hsc からの要求に応じ CGI プログラムを起動する機能を持つ．

(2) hsc
　簡易 HTTP クライアントで，hsd を介して稼動状況データの収集と，hsd に対する CGI の起動要求を行う機能を持つ．

(3) nhs-lib
　認証／暗号化ライブラリで，クライアントで利用することにより相手認証および通信データの暗号化を実現する．

(4) nhs-gw
　nhs-lib に対応した中継サーバであり，ファイアウォール等を介して通信を行う際に使用する．

本通信基盤の全体構成を図 1に示す．hsd/hsc は，HTTP プロトコルを使用した軽量通信モジュールであり，hsd/hsc 間の通信内容は，nhs-lib によって認証/暗号化される．また，nhs-gw により，複数のファイアウォールを含むネットワーク環境において，ファイアウォールによる保護機能を低下させること無くファイアウォールを越えた hsc/hsd による通信を行うことができる．

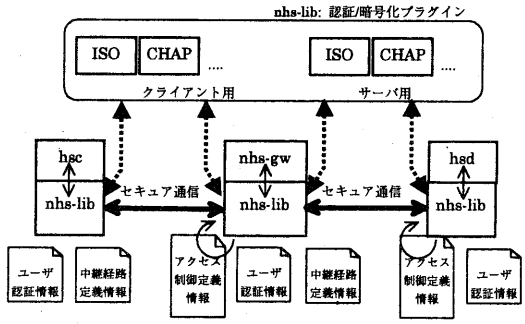

図 1: 全体構成

図 2 に示すように，ネットワークサービス集中管理システム構築において，本通信基盤はサービス集中管理サーバとサービス管理プログラム間の通信基盤として使用される．

2 章で示した通り，ネットワークサービス集中管理システムの構築には，大きく分けて，(1) 集中管理システムの実現方式についての課題，(2) 集中管理システムのセキュリティについての課題が存在する．

(1)管理システムの構築に関する課題については，hsd/hsc を管理システムの共通の通信基盤として使用することによって対応する．また，(2) セキュリティ上の課題については，hsd/hsc に組み込まれた認証/暗号化ライブラリ nhs-lib が，hsd/hsc 間の通信を認証/暗号化することで対応する．

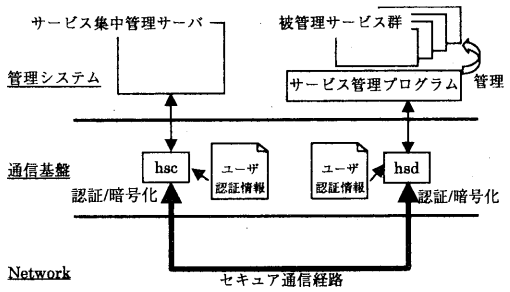

図 2: セキュア通信基盤

以下の節では，各コンポーネントの機能を説明し，管理システムの構築に本通信基盤の各コンポーネントを使用することによって課題がどのように解決されるかを示す．

3.2. HTTP 通信コンポーネント hsd/hsc

セキュア通信基盤では，HTTP 通信コンポーネントである hsd と hsc を用いて対象サービス側のサービス管理プログラムとサービス集中管理システムの間の通信を実現することにした．これは以下の理由による．

(1) ネットワークサービス集中管理システムを構築する際に使用するもっとも典型的なプロトコルは，“何らかのコマンドを送りその結果を得る”ことである．HTTP は，この要件を満たし，かつ単純なプロトコルであるため，プロトコル使用によるトラブルも少ないと考えた．

(2) サービス管理プログラムを作成するために，既に確立されている CGI の技法を使用することができる．

(3) HTTP はもっとも標準的に使用されるプロトコルの一つであり，イントラネット内等でセキュリティ機能を使用しないような場合，ファイアウォール等のネットワークシステム全体の変更も最小限に抑えることができる．

サービス集中管理のための通信基盤として，SNMP[5]を使用する方法も考えられる．しかし，(a)広く使用されている SNMPv1 にはセキュリティ上の問題がある，(b)現時点でネットワークサービスの多くに MIB が存在せず一から作る必要がある，(c)本通信基盤では CGI により管理プログラム(サービス操作や情報収集)を容易に作成できるという点から，ネットワークサービス管理システムの構築には HTTP の使用が有効であると考える．

各ホスト上のサービスは，各ホスト上に記述されたサービス管理プログラムによって管理される．hsd は，サービス集中管理サーバからの管理コマンドを受け取り，サービス管理プログラムを CGI として起動する．また hsd は，サービス集中管理サーバにおいて，管理システムを使用するためのユーザインタフェースを提供するためにも使用される．

hsc は，サービス集中管理サーバにおいて使用される．サービス集中管理サーバは，hsc により hsd を通してサービス管理プログラムにアクセスし，管理コマンド送信や管理情報取得を行う．

hsd/hsc は，ネットワークサービス集中管理システムの構築において，認証/暗号化されたセキュア通信の手段として，また，標準化されたシステム全体での共通プロトコルとして使用することができる．さらに，hsd/hsc を共通の通信基盤として使用することにより，管理システム開発者は本来の目的であるサービス管理の記述に専念できる．

3.3. セキュアソケットライブラリ nhs-lib

nhs-lib は，hsc に組み込むことにより hsd との間の相互認証と通信路暗号化を実現するモジュールである．nhs-lib は，SocksV5[4]に準拠したトランスポート層認証/暗号化ライブラリで，既存の socket ライブラリを使用したアプリケーションで，socket 関数を nhs-lib が提供するセキュアソケットライブラリ関数に置き換えることで，そのアプリケーションに認証／暗号化機能を組み込むことができる．

また，セキュアソケットライブラリは SocksV5

を独自に拡張し，多段接続ゲートウェイ nhs-gw による多段ファイアウォール接続を行う機能を持つ(3.4節).

セキュアソケットライブラリでの認証/暗号化手段はプラグイン化されており，図 1の上部で示されているように必要に応じて追加，拡張できる．現在の本通信基盤でサポートされている認証/暗号化アルゴリズムを，表 1に示す．

表 1: nhs-lib 認証/暗号化方法

	認証アルゴリズム	暗号化アルゴリズム
1	user name/password	なし
2	CHAP	なし
3	ISO/IEC9798-2[3]	MULTI2

hsd/hsc は，nhs-lib を使用することによって認証/暗号化機能を実現している．つまり，hsd/hsc を管理システムの通信基盤として使用することで，サービス集中管理サーバとサービス管理プログラム間の通信を認証/暗号化し，管理情報の盗聴/改ざんや管理システムへの不正アクセスを防止する．

3.4. 多段ファイアウォール接続機能 nhs-gw

nhs-gw は，中継経路制御機能により，多段ファイアウォール環境下においてユーザが途中のファイアウォールを意識すること無く通信するためのゲートウェイサーバである．

Internet 経由や部門をまたいだサービス管理を行う場合，ファイアウォールを通して被管理サービスマシンに接続する必要がある．またその場合，間に多重にファイアウォールが存在する場合もある．例えば，図 3で，kiwi から carrot にアクセスする場合，lemon，potato と 2 つのファイアウォールが存在し，それぞれユーザ認証しなければならない．

セキュアソケットライブラリを使用して通信を行う場合，基本的に通信の両端(管理サーバと個々のサービス管理プログラム)で認証/暗号化が行われるが，間にファイアウォールが存在する場合は，そこで通信が止められてしまう．しかし，ここで特別にセキュアソケットライブラリの通信を素通りするようファイアウォールを設定することは，ファイアウォールに抜け穴を作ることになり，ネットワーク全体のセキュリティレベルを落とすことにも繋がる．

多段ファイアウォール接続サーバ nhs-gw は，通信経路上のファイアウォールで動作し，一つ以上のファイアウォールを通して通信が行われるとき，セキュアソケットライブラリの通信を認証を行いつつ中継する．nhs-gw を使用した多段ファイアウォール接続は，図 4のように中継する各 nhs-gw が自動的に認証を行い，それにより確立した暗号化経路を使用して，次の nhs-gw または終端の hsd と認証を行い最終的な暗号化経路を確立する．

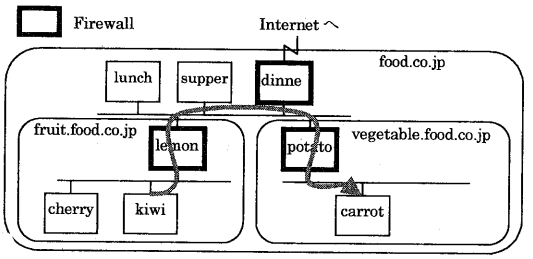

図 3: 多段ファイアウォール環境

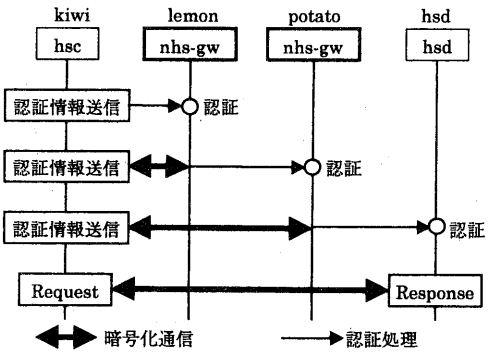

図 4: 多段接続手順

nhs-gw を使用することにより，ファイアウォールを使用している既存ネットワークのセキュリティレベルを落とすこと無くファイアウォールを超えたセキュア通信環境を構築できる．また，セキュアソケットライブラリを使用するプログラム

(hsd/hsc や独自プログラム)は，ファイアウォールを通さず直接接続した時と同様，認証/暗号化を意識することなく通信できる．

4. 適用事例

本基盤環境を，セキュリティ管理支援のためのインタネットサービス管理システム[6]の開発に適用した．この管理システムは，インタネットサービス(Mail, Web, Netnews 等)やサービスが動作しているホスト自身に対し，動作状況の監視，サービス/ホストの設定変更を行い，複数のホストを統合的，多面的に管理する機能を提供する．

インタネットサービス管理システムは，監視対象となるホスト上で動作する「エージェントモジュール」と，管理サーバ上で動作する「マネージャモジュール」により構成される．この管理システムの構成の概略を図 5に示す．

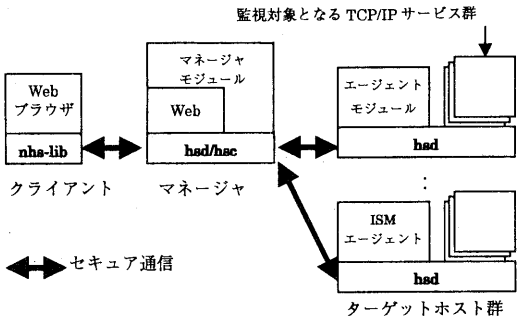

図 5:管理システム構成概略

本通信基盤は，エージェントモジュールとマネージャモジュール間，また，管理クライアントとマネージャモジュール間のセキュア通信基盤として利用されている．

エージェントモジュールは，hsd から起動される CGI として記述され，またエージェントモジュールが稼動することによりターゲットホストの提供サービスに支障が発生することがないよう最小限の機能の記述がされている．

インタネットサービス管理システムは本通信基盤を利用することによって，(1)各モジュール間の通信認証/暗号化，(2)通信環境を意識すること無く管理システム本来の機能のみの記述を達成することができた．

5. 今後の課題

本通信基盤の認証/暗号化手段を利用する場合は，使用する各ホストにユーザ情報の登録や使用する認証/暗号化手段の設定が必要になる．管理対象ホストの数が増大すれば，この登録/設定コストも無視できないものになるため，登録/設定を集中的に管理するための手段が必要となる．

このような設定の管理方式は，ポリシーベース管理システム[1]として提案されているが，将来的に，本通信基盤もこの方式に対応することが重要だと考える．

また，本通信基盤は，標準的なプロトコルである HTTP，SocksV5 に対応することによってファイアウォール等のネットワーク全体設定の変更の手間を最小限にしている．今後は，SSL/TLS やファイアウォール，VPN などと連携することによって，よりネットワーク透過な通信基盤としたい．

6. おわりに

本稿では，分散ネットワークサービスを管理するための基盤を開発した．

本通信基盤を利用することで，標準化された通信手段によるセキュア通信を実現でき，また，管理システムに必要な機能の構築に専念することができる．

参考文献

[1] 藤山達也 他, 多段ファイアウォール環境における VPN 管理方式の提案, コンピュータセキュリティシンポジウム'98, 1998

[2] 磯川弘実 他, 多面的ビューを持つインターネットセキュリティ管理支援システムの提案, 第 7 回 CSEC 研究発表会, 1999

[3] OSP/IEC9798-2, Information technology-Security technique-Entity authentication

[4] SocksV5, IETF RFC1928

[5] SNMP: RFC 1157 他, SNMPv3: RFC2571 他