HMP NX シリーズにおけるセキュリティ機能の実装

Security Enforcement in HMP NX Series

福　家　　裕，武　村　正　彦

要　約　インターネット時代と呼ばれて，世の中の隅々にまでインターネット環境が行き渡った状況の中で，コンピュータの利用形態として業務用，家庭用を問わずインターネットと無関係には成立し得ない時代になっている．同時に，セキュリティへの関心が専門家以外の世界にまで浸透していることは周知の状況である．

このような環境下でコンピュータに求められるセキュリティ対策は多岐に渡り，各種の手法，技術が紹介されている．

本稿では，Unisys の代表的なメインフレームである HMP NX シリーズに実装されているセキュリティ技術を紹介し，インターネット/イントラネット環境での対応状況について記述する．

Abstract　In the circumstances where Internet environment is prevailed overall the world, the use of computers cannot be realized independently of Internet connections regardless in personal or business use. The attention to the computer security has spread out among people not necessarily computer experts simultaneously.

The wide range of security measures is required in the Internet environment, and many technologies and method have been introduced to the field of computer security.

This paper introduces the technological and administrative measures implemented on the HMP NX series, a typical mainframe server of Unisys, and then discusses the status of the security enforcement in the Internet and/or intranet environment.

1. は　じ　め　に

オンラインショップ，ネットバンキング，e マーケットプレイスなどで代表される B to C あるいは B to B による電子商取引（EC）がネットワーク・ビジネスとして急速に成長しつつある．その一方では，企業間の取引情報，顧客のプライバシ情報，個人情報などがインターネットを通して第三者の手に渡ることも考えられるためセキュリティ対策は急務となっている．特に E ビジネスの基幹を成す企業情報システムに於けるセキュリティ確保は必要不可欠である．その基幹サーバとして使用される Unisys e-@ction ClearPath サーバ HMP NX シリーズ（以下，HMP NX シリーズと略す）および ClearPath Plus Server CS 7101 にもいくつかのネットワーク・セキュリティ機能が用意されている．現在，HMP NX シリーズは NX 5600，NX 5800 および NX 6800 が提供されている．本稿では 2000 年 11 月にリリースされた NX 6800 システムに実装されているネットワーク・セキュリティについて述べる．

まず，2 章で HMP NX シリーズのセキュリティ機能を実装する上で必要不可欠な技術要素である Network Services について，3 章では NX 6800 システムに実装されているネットワーク・セキュリティ機能である TCP/IP セキュリティ，Web Enabler

for ClearPath MCP の HTTP トンネリング機能の概要について述べる．4 章では，MCP 環境で SSL（Secure Socket Layer）による暗号化通信を提供する ClearPath Secure Transport についての概要と HMP NX シリーズへの実装について述べる．

2. Network Services

2.1 HMP NX シリーズのネットワーク構成

まず，HMP NX シリーズのネットワーク構成について触れておく．HMP NX シリーズの中でもトップエンドに位置する NX 6800 システムの内部ネットワークは，MCP サーバ，Windows サーバを冗長機能付きの高性能スイッチング・ハブと保守用スイッチング・ハブで接続した構成となっている．また，MCP 環境と Windows 環境を高速に接続するハードウエア機構として，従来よりあるチャネル・サービス・バス（以下，CS-Bus と略す）が採用されている．NX 6800 システムで使用される CS-Bus は 3 世代目である CS-Bus III となり，さらに高速化が図られている．CS-Bus III の最大転送速度は従来の CS-Bus の 3 倍となっている（図 1）．

また，NX 6800 システムでは HMP FastPath-CIA（ClearPath Intraconnect Architecture：以下，CIA と略す）と呼ばれる新しいソフトウェア・アーキテクチャが取り入れられている．CIA は，CS-Bus のハードウエア能力を最大限に発揮できるように設計されている．CIA では，MCP/Windows 環境間の通信データ処理を従来のディスク装置などと同じ入出力管理（IOU : IO Unit）から独立させ，タスク管理（TCU : Task Control Unit）による QUEUE を経由したメッセージ通信へと変更されている．この技術により，数 K バイト程度の比較的小さなメッセージサイズのデータも効率よく取り扱うことが可能となった．

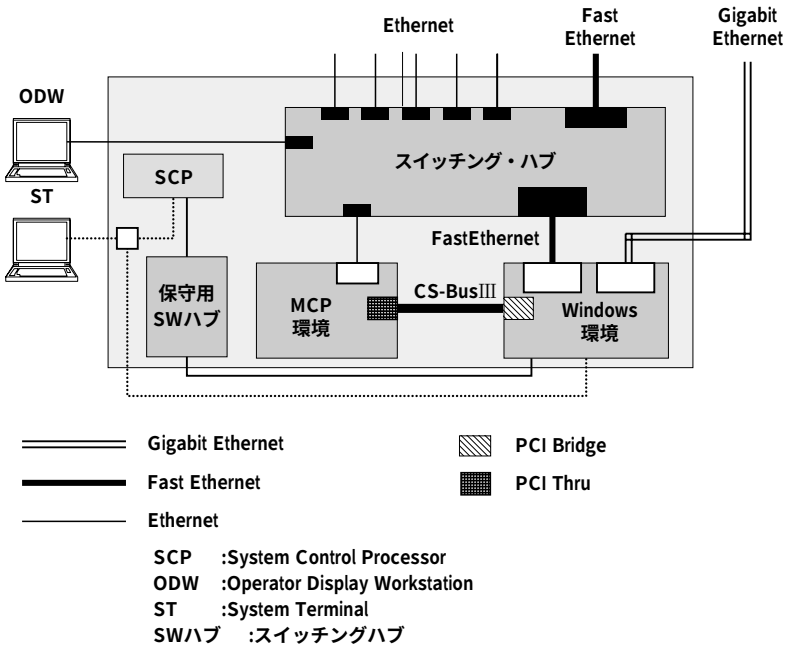


図 1　HMP NX シリーズのネットワーク構成

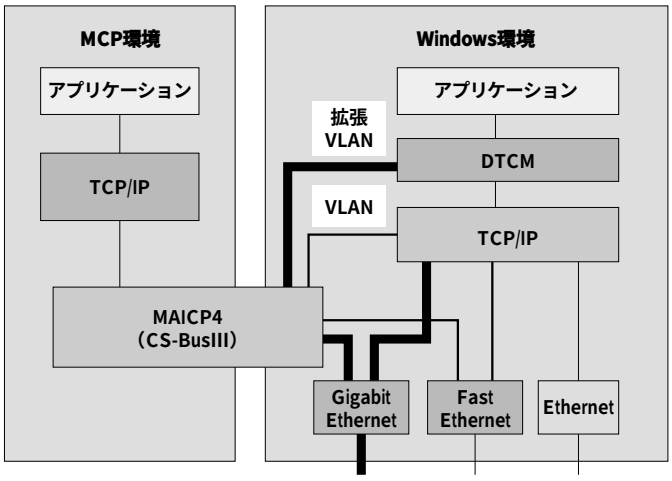
2.2 Network Services の概要

Network Services は，HMP NX システム内の MCP 環境と Windows 環境を密結合させ，両環境間の高速通信を可能にするソフトウェア・サービスであるが，HMP NX シリーズのセキュリティ機能を実装する上で必要不可欠な技術要素の一つでもある．Network Services は，NX 6800 システムでは PCI Thru アダプタ，PCI Bridge アダプタと呼ばれる CS-Bus に接続するためのアダプタ・カード（図 1 参照）と MCP 環境上で稼働する MAICP 4（Micro A Integrated Communications Processor 4）と呼ばれる通信装置エミュレーション・ソフトウェアおよび Windows 環境上で稼働する Network Services ソフトウェアで構成されている．Network Services の実装形態には，仮想 LAN（VLAN : Virtual LAN）およびアダプタ共有（SA : Shared Adapter）の二つがある．

仮想 LAN は，CS-Bus による高速内部バス接続により，MCP 環境と Windows 環境の両プラットフォーム間の高速通信とシームレス環境を提供する．仮想 LAN は，外部に接続されるパブリック LAN とは分離されたプライベート・ネットワークとなっており，外部から仮想 LAN へ直接アクセスすることはできない．

アダプタ共有は，HMP NX システム内の Windows 環境のネットワーク・インタフェース・カード（NIC）を MCP 環境でも使用できるようにする機能である．この機能では，Windows 環境の NIC を MCP 環境から専用のネットワーク・デバイスとしてアクセスすることが可能である．また，Windows 環境と MCP 環境で共有して同時にアクセスすることも可能である．

MCP 環境と Windows 環境の高速なデータパスとして拡張仮想 LAN（拡張 VLAN）と仮想 LAN（VLAN）の二つが用意されている．両環境間のデータ転送効率を上げるため，TCP セグメントの送信には拡張 VLAN のパスが使用される．それ以外の UDP（User Datagram Protocol），IP，ICMP（Internet Control Message Protocol），



MAICP4 : Micro A Integrated Communications Processor 4

DTCM : Distributed TCP/IP Communications Manager

図 2 Network Services の仮想 LAN とアダプタ共有機能

ARP（Address Resolution Protocol）などの送信は VLAN のパスが使用される．また，この例では Windows 環境の FastEthernet NIC と Gigabit Ethernet NIC がアダプタ共有として構成されている（図 2）．

3. HMP NX シリーズのセキュリティ機能

3.1 TCP/IP セキュリティ

3.1.1 TCP/IP セキュリティの概要

TCP/IP セキュリティは，MCP 環境で稼働する TCP/IP 通信のアクセス制御を行うセキュリティ・ソフトウェアである．このセキュリティ・ソフトウェアは，インターネットあるいはイントラネットからの許可されていない利用者による MCP システムへの不正アクセスを防御することを目的としている．

TCP/IP セキュリティは，MCP 環境に TCPIPSECURITY システムライブラリとして実装されており，TCPIPSUPPORT（MCP 環境の TCP/IP プロトコル・スタック）のサブコンポーネントとして機能する．TCPIPSUPPORT にセッション確立の要求があると，その要求はすべて TCPIPSECURITY に渡される．この時，ルール・ファイルと呼ばれる許可条件と禁止条件が定義されたファイル内のルール・テーブルとセッション要求とが照合され，その要求を許可するかどうかが決定される．すなわち，TCP セッション確立要求ごとに現在ロードされているルール内容との照合が行われる．ルール・テーブルには許可ルールと禁止ルールの 2 種類のテーブルがある．当然，複数の許可ルールと禁止ルールを定義することも可能である．もし仮にセッション要求が許可/禁止テーブルのすべてのルール・エントリーに該当しない場合，フェイル・セーフ機能によりその要求は禁止される．

また，TCP/IP 要求による不正アクセス・ログが記録されるため，このシステム・ログを監査することによって不正アクセスを事前に検出し，初期段階で発見することができる．

3.1.2 TCP/IP セキュリティの機能

TCP/IP セキュリティの機能は大きく二つに分けることができる．それはパケット・フィルタリング機能とセキュリティ拡張機能である．パケット・フィルタリング機能は，ファイアウォールの技術要素の一つであるパケットのフィルタリングとほぼ同じ働きをする．セキュリティ拡張機能は，HMP NX システムのセキュリティを強化するために拡張された機能であり，MCP 環境で稼働する TCP アプリケーションのセッション要求の制御，利用者コードによるアクセス制御などを行う．

1） パケット・フィルタリング機能

パケット・フィルタリング機能は，telnet，FTP，HTTP などの TCP/IP アプリケーション・サービスが通信するときに使用する送信元 IP アドレスと送信先 IP アドレス，および送信元ポート番号と送信先ポート番号を検査して許可されたパケットだけを通過させ，アプリケーションへ渡す．この機能は，TCP，UDP，IP および ICMP のヘッダ情報を参照しフィルタリングを行なっている．パケット・フィルタリングの概念図を図 3 に示す．

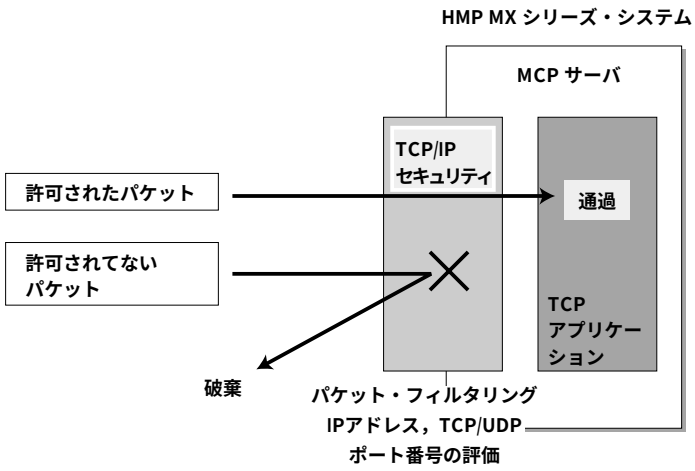


図 3　パケット・フィルタリング機能

① ポート番号

ローカルまたはリモートの TCP/UDP ポート番号を指定してパケットのフィルタリングを行なう．ローカル・ポート番号は，HMP　NX シリーズ上で動作する TCP/IP アプリケーション・サービスのポート番号を指定する．リモート・ポート番号は，MCP サーバと TCP/IP 通信を行なう相手ホストのポート番号を指定する．

② IP アドレス

ローカルおよびリモートの IP アドレスを指定してパケットのフィルタリングを行なう．ローカル・アドレスは，MCP 環境に装備される 802.3 チャネルアダプタ[*1] または Windows 環境に装備される共有アダプタ[*2] の IP アドレスを指定する．リモート・アドレスは，MCP サーバと TCP/IP 通信を行なう相手ホストの IP アドレスを指定する．また，ネットワーク・アドレスを指定することによりサブネットワーク単位に制御することができる．

③ TCP ダイアログ

TCP セッションの能動オープン（Active Open）または受動オープン（Passive Open）のどちらかを指定して制御することができる．例えば，HMP NX システムから宛先ホストに対してオープンした TCP セッション（能動オープン）は許可するが，逆に宛先ホストからオープンされた TCP セッション（受動オープン）は禁止することが可能である（図 4）．

2） セキュリティ拡張機能

アクセス制御の対象となる項目は，MCP 環境における利用者コード名，コードファイル名，時間，曜日，アプリケーションの認可がある．ただし，TCP/IP セキュリティに利用者コードが渡されないアプリケーションでは利用者コードによるアクセス制御はできない．その場合は，パケット・フィルタリング機能などを使って制御するか，MCP システムへのログオン時に使用される LOGONCHECK 手続きによってシステムレベルのアクセス制御を

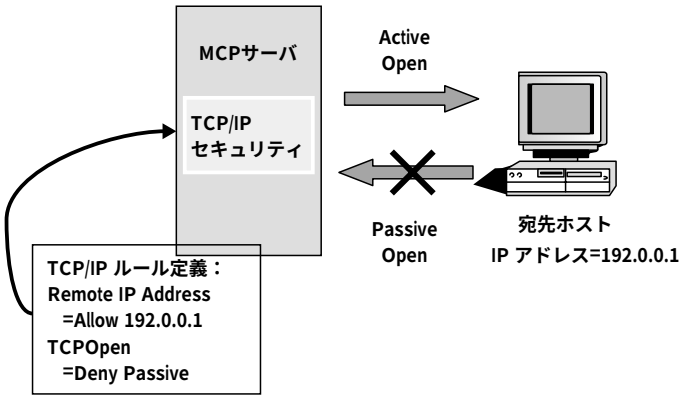


図 4　TCP ダイアログによるアクセス制御

行っている SECURITYSUPPORT を使用する．

① 利用者コード名

タスク属性利用者コードによるアクセス制御を行なう．利用者コード名によるアクセス制御は，TCP/IP アプリケーション・プログラムを実行したときに割り当てられる利用者コード名によってアクセス制御を行なう．

② コードファイル名

MCP 環境上で実行する TCP/IP アプリケーション・プログラムのオブジェクト・コードファイル名の指定によってアクセス制御を行なう．

③ 時間

時間範囲の指定によるアクセス制御を行なう．IP アドレス項目と同時に指定して，サブネットワーク単位にシステムへのアクセス時間帯を指定できる．

④ 曜日

曜日範囲指定による制御を行なう．時間項目と同様に，IP アドレス項目と同時に指定して，サブネットワーク単位にシステムへのアクセスを曜日で指定できる．

⑤ アプリケーションの認可

MCP 環境で動作する TCP/IP アプリケーション・プログラムの TCP セッションの制御を行なう．MCP システムにより認可されていない TCP/IP アプリケーションは，TCP セッションをオープンすることができない．MCP サーバ上に許可なく置かれたトロイの木馬[*3] などの不正プログラムによる TCP セッションのオープンを禁止することができる．

これらフィルタリング機能とセキュリティ拡張機能を組み合わせてセキュリティ・ルールを設定することも可能である．また，ここで紹介した TCP/IP セキュリティ機能とは別に TCPIPSUPPORT に組み込まれている標準セキュリティとして，Well-Known ポート[*4] の制限機能がある．MCP 環境で Well-Known ポートを使用するサーバ・アプリケーション・プログラムは，MCP システムにより認可されていないと TCP セッションをオープンすることができない．この機能は，TCP/IP セキュリティ機能を使用しなくても自動的に有効となる．

3.2 Web Enabler for ClearPath MCP

3.2.1 HTTP トンネリング機能

Web Enabler for ClearPath MCP（以下，Web Enabler と略す）は HMP NX システムに接続するためのホスト端末エミュレーション・ソフトウェアである．このソフトウェアは，Java 技術を取り入れた Web ベースのソフトウェアである．

Web Enabler の HTTP トンネリング機能（図 5）を使用すれば，インターネットから HMP NX システムへの端末接続を容易に実現できる．HTTP トンネリング機能では，Web Enabler アプレットがダウンロードされた Web ブラウザと Web サーバは HTTP または HTTPS プロトコルで通信する．Web サーバとして Internet Information Service/Server（以下，IIS サーバと略す）を使用しており，SSL プロトコルによる暗号化通信と利用者認証が可能である．

3.2.2 HTTP トンネリングの構成

Web Enabler HTTP トンネリング機能は，Windows 環境で稼働する以下のモジュールで構成されている．

① HTTP トンネル・ライブラリ

ダイナミック・リンクライブラリ（DLL）として実装されており，HTTP トンネル・コントロール・プログラムで設定した情報を元に MCP サーバと IIS サーバ間の接続とプロトコル変換を行うソフトウェアである．Web ブラウザ上の Java アプレットと IIS サーバを通して呼ばれたトンネル・モジュールは HTTP または HTTPS プロトコルで通信を行う．また，トンネル・モジュールと MCP サーバ間は TCP ソケット通信を行っている．

② HTTP トンネル・コントロール・プログラム

GUI による構成情報設定用のアプリケーションであり，接続先のホストと使用するポート番号の設定を行う．Windows サーバのコントロールパネルから起動することができる．

ここで紹介した Web Enabler HTTP トンネリング機能でも MCP 環境と Windows 環境の連携が行われており，Network Services 仮想 LAN による高速通信と転送データの秘匿性が確保されている．

3.2.3 HTTP トンネリングでの接続手順

① IIS サーバへのアクセス

Web ブラウザにダウンロードされた Web Enabler アプレットが起動される．起動された Web Enabler アプレットは，IIS サーバ環境で稼働する HTTP トンネル・ライブラリと HTTP あるいは HTTPS プロトコルで接続する．

② MCP 環境へのアクセス

HTTP トンネル・ライブラリは，あらかじめ定義された接続情報をもとに MCP 環境のカスタム接続機構（CCF）プロトコル固有ハンドラ（PSH）（以下，CCF PSH と略す）に接続する．

③ アプリケーションへのアクセス

CCF PSH を介して，IIS サーバと MCP サーバ間の接続が確立され MCP 環境のアプリケーションとの通信が可能となる．

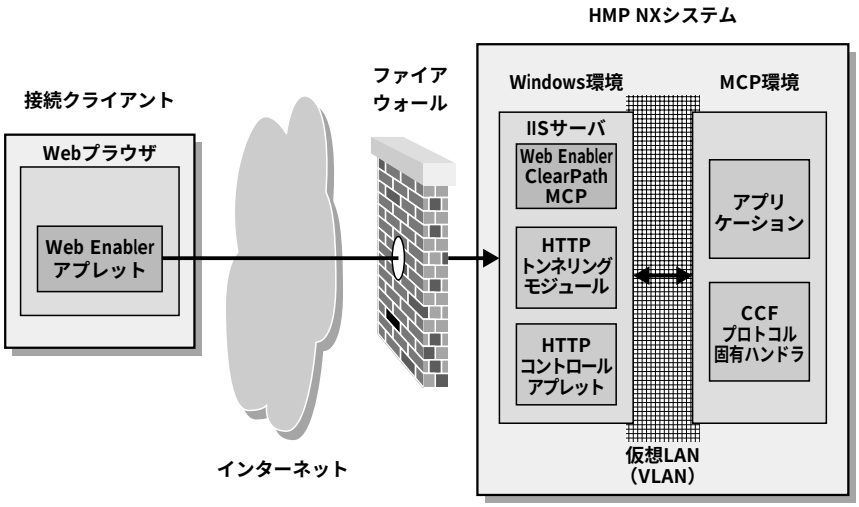


図 5　Web Enabler の HTTP トンネリング機能

4. ClearPath Secure Transport

4.1 ClearPath Secure Transport の概要

ClearPath Secure Transport（以下，Secure Transport と略す）は，MCP 環境で SSL（Secure Sockets Layer）による暗号化通信を実現するためのセキュリティ機能である．Secure Transport の主な機能は，Web ブラウザと Web サーバ間の通信データの暗号化と PKI（Public Key Infrastructure：公開鍵基盤）ベースの電子証明書による認証である．

Secure Transport は HMP NX シリーズの MCP 環境と Windows 環境に実装された複数のモジュールで構成されている．その核となるモジュールが MCP CryptAPI Support ライブラリ（以下，MCAPISUPPORT と略す）である．このモジュールは，MCP 環境と Windows 環境で発生した暗号処理タスクを機能的に結びつけ，効率的に SSL による暗号化通信ができるように働く（図 6）．

4.2 Secure Transport の HMP NX シリーズへの実装

HMP NX シリーズでの SSL 通信の実装に於けるポイントとしては，標準暗号化ライブラリの使用と Windows 環境の利用による暗号処理の負荷分散機能である．Windows 環境とのシームレスな統合により，Windows 環境にあるコンポーネントを有効に利用している．Secure Transport でも同様に，MCP 環境と Windows 環境の高速通信インフラとして Network Services 仮想 LAN が使用されている．

標準暗号化ライブラリは，RSA BSAFE Crypto-C が使用されており，Windows 環境で動作する NX/CryptoProxy を通して暗号化ライブラリが呼び出される（図 7）．

暗号化/復号化処理によるホスト・システムへの負荷増加，スループットの低下は基幹システムとして避けなければならない．HMP NX システムでは，複数台の Windows サーバを構成することにより暗号化/復号化処理に掛かる負荷を各 Windows 環境へ分散させることが可能である．この負荷分散処理を行っているのが MCAPISUPPORT である．また，負荷分散アルゴリズムとしてラウンドロビン[*5] が使用されて

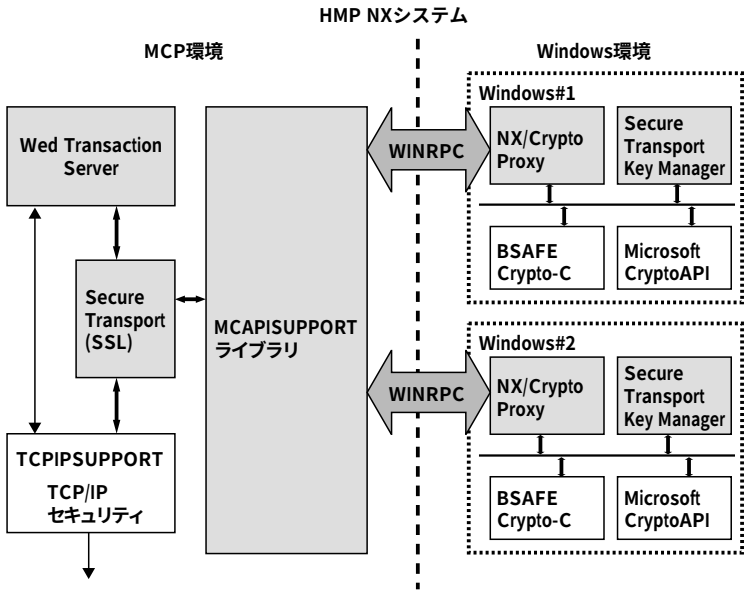


図 6　ClearPath Secure Transport の構成図

おり，MCAPISUPPORT によって各 Windows 環境へ処理の分散化が行なわれている．図 7 では，HMP　NX システムに内蔵された 2 台の Windows サーバで負荷分散処理を行っている例である．

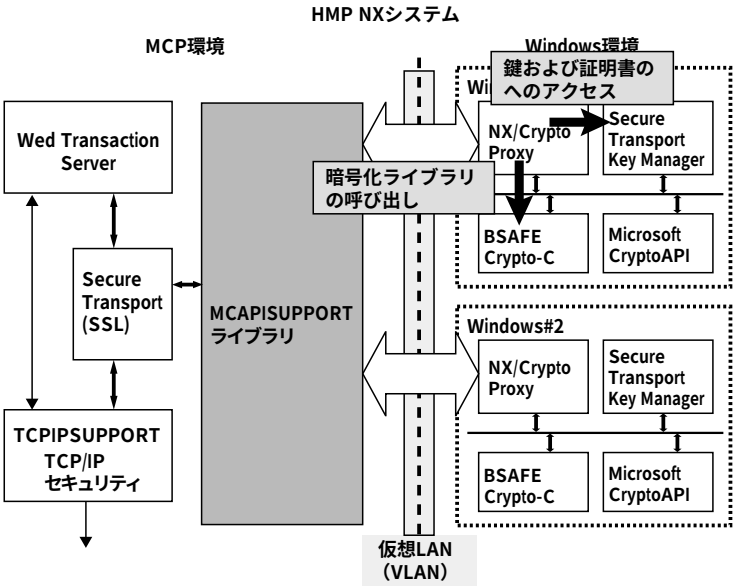


図 7　NX/CryptoProxy による呼び出し

4.2.1　MCP 環境のモジュール

①　MCAPISUPPORT システムライブラリ

MCAPISUPPORT（MCP CryptAPI Support）システムライブラリは MCP 環境で動作し，HMP NX シリーズの TCP/IP アプリケーションに暗号サービスと認証サービスを提供する．MCAPISUPPORT は，各処理モジュールを呼び出して MCP 環境に次の暗号機能を提供する．

・通信データの暗号化と複合化
・公開鍵暗号の公開鍵/秘密鍵の管理
・デジタル署名と電子証明書の管理
・メッセージダイジェスト

② Secure Transport（SSL）

HMP NX シリーズの MCP 環境に実装された SSL プロトコル・モジュールである．SSL プロトコルは TCPIPSUPPORT の上位レイヤに置かれ，Web Transaction サーバあるいは TCPIPSUPPORT からの SSL 要求を処理する．

③ WINRPC システムライブラリ

MCP 環境と Windows 環境間で RPC 通信を行うために実装されているのが WINRPC（Windows RPC）である．WINRPC は MCP 環境にシステムライブラリとして登録され，MCP 環境上に Microsoft 社 RPC と互換性のある RPC 環境を提供する．

④ Web Transaction サーバ

MCP 環境で稼働する大規模トランザクションに対応した高機能，高可用性の Web サーバである．SSL プロトコルに対応したことにより Web データの暗号化通信を実現する．

4.2.2 Windows 環境のモジュール

① NX/CryptoProxy

NX/CryptoProxy は，MCAPISUPPORT システムライブラリからの暗号処理要求あるいは鍵/証明書処理要求を受け取り，Windows 環境に実装されている各モジュールを呼び出す．暗号処理は BSAFE Crypto-C モジュールが，また鍵/証明書処理要求では Secure Transport Key Manager がそれぞれ呼び出される．

② Secure Transport Key Manager

Secure Transport Key Manager（以下，Key Manager と略す）は，鍵の管理と電子証明書の管理を行う GUI ソフトウェアである．公開鍵と秘密鍵の鍵ペアの作成, 証明書要求ファイルの作成, 証明書の管理を行うために NX/CryptoProxy から Microsoft CryptoAPI を通して呼び出される．

Key Manager の機能：

●鍵の管理
・公開鍵/秘密鍵の鍵ペアの作成
・鍵の削除
・鍵情報の表示
・MCP 環境への鍵の複製と削除
●電子証明書の管理

・電子証明書要求ファイルの作成
・電子証明書の更新要求
・アプリケーションへの電子証明書の導入

③ BSAFE Crypto-C

BSAFE Crypto-C は標準暗号化ライブラリであり，暗号化/複合化の暗号化エンジンとして機能する．Windows 環境で動作する NX/CryptoProxy を通して暗号化ライブラリが呼び出される．

④ NSProcurator

Windows 環境に導入される NSProcurator コンポーネント（Name Service Procurator）は，MCP 環境で動作する WINRPC ライブラリと Windows 環境で動作する Microsoft 名前サービス間のインタフェースを提供する．

4.3 電子証明書を用いた Web サイトの構築

HMP NX シリーズで SSL による暗号化通信と電子証明書を使用したサーバ認証機能を提供する Web サイトの構築について述べる．具体的には，Web Transaction サーバに電子証明書を導入し，SSL による暗号化通信とサーバ認証が行える Web サイトの設定手順を示している．

1） サーバ証明書の発行依頼

SSL ネゴシエーション時に Web ブラウザに送られる Web Transaction サーバのサーバ証明書を発行してもらうための準備をする．まず，Key Manager により，Web サーバの公開鍵/秘密鍵の鍵ペアと証明書要求ファイルを作成する．鍵ペア作成時，作成された鍵ペアを一意に識別するためのセキュリティ・サービス名を指定する必要がある．このサービス名によって鍵ペアと後に導入されるサーバ証明書の管理が行われる．

サーバ証明書の発行は認証局（CA）に依頼する必要がある．Web サーバを特定するための識別名（DN：Distinguished Name），公開鍵（Key Manager が作成した公開鍵）などの情報を含んだ証明書要求ファイルを作成し認証局に依頼する．証明書要求ファイルは PKCS#10（Public Key Cryptography Standards #10）形式で作成される．図 8 に作成された証明書要求ファイルの例を示す．

2） サーバ証明書の発行

証明書の発行は認証局で行われる．証明書の発行依頼を受けた認証局は自分の署名（発行した認証局の署名）を証明書に追加し，サーバ証明書を発行する．認証局の利用形態としては，VeriSign Onsite などの第三者による認証サービスを利用して証明書を発行してもらう方法と UniCERT などの認証局サーバを自営して自社内で証明書の発行・管理を行う方法の 2 通りがある．

3） サーバ証明書の導入

Key Manager を使用しサーバ証明書を導入する．このとき，証明書要求ファイル作成時に生成された鍵ペアとサーバ証明書の関連付けが行われる．

4） 負荷分散環境の構成

負荷分散環境を構成するために，HMP NX シリーズ内のすべての Windows 環境へ既に生成された鍵ペアを導入する．同じ鍵を共有することにより関連付け

```
Certificate Requestor:  Taro.Toyosu@toyosukk.co.jp
Telephone:  03-1234-5678
Generated by:  Unisys NX/Secure Transport Key Manager
Commonname:  HMPNXSVR
Organization:  ToyosuKK
Keyname:  MCAPI_S_NXATLAS_HMPNXSVR
Locality:  KOTOKU
State:  TOKYO
Country:  JP
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBSjCB+QIBADCBkzGBkDAJBgNVBAYTAkpQMAoGA1UEChMDTIVMMAwGA1UECBMF
VE9LWU8wDQYDVQQHEwZLT1RPS1UwDgYDVQQDEwdOVUxUEMB4GA1UECxMXTUNB
            （途中省略）
QrXm3lhJxBYzAgMBAAGgADAJBgUrDgMCHQUAA0EAS+ZrdrUhN5eDej3vGCacyWsK
/H8dMynZ+gN9yB/jTEKgnwUREhwb12z0p+EO5JCMV5cKBk7X64PpY9KQMXNgLQ==
-----END NEW CERTIFICATE REQUEST-----
```

図 8　証明書要求ファイル

られ，Windows 環境による負荷分散環境が構成される．

5）Web サイトの設定

Web サイトの SSL 設定は，Web Transaction サーバ Site Manager(以下，Site Manager）で行う．SSL による暗号化通信と電子証明書によるサーバ認証を実施する Web サイトを選択し，SSL の使用を有効にする．この時，鍵ペアの作成時に指定したセキュリティ・サービス名と同じものを使用する．

4.4 HTTPS（SSL）による Web Transaction サーバへのアクセス

図 9 は，HMP NX システムで Secure Transport を使用した HTTPS（SSL）通信を行った時の Web Transaction サーバまでの通信データの経路を示したものである．

まず，クライアントからの HTTPS 接続要求は Secure Transport（SSL）によりネゴシエーションが行われる．この時，クライアントによるサーバ認証，使用する暗号方式の決定，通信データの暗号に使用される共通鍵の受け渡しなどが行われる．

暗号化通信が開始されると，クライアントからの暗号化されたデータは MCAPISUPPORT により NX/CryptoProxy へデータの複合化要求が送られる．復号化されたデータは MCAPISUPPORT に戻され，Web Transaction サーバへ渡される．また，暗号化されたデータをクライアントへ送る場合は NX/CryptoProxy へデータの暗号化要求が送られ，暗号化されたデータは MCAPISUPPORT により TCPIPSUPPORT に渡されてクライアントへ送信される（図 9）．

5. おわりに

本稿では，HMP NX シリーズのセキュリティに関して，主としてネットワーク関連の機能について概説した．HMP NX シリーズの開発姿勢には，時々刻々進化するオープン環境のテクノロジーをタイムリーに搭載することがある．そのため，HMP NX シリーズは登場以来，MCP 環境と内蔵 Windows 環境を如何に高速かつ効率よく相互接続するかを主眼に Network Services の機能拡張を続けている．そして，この構造を基盤として，Windows 環境の機能を積極的に利用することで HMP システムという MCP と Windows からなる仮想的な単一システムを形成してきた．本稿で解

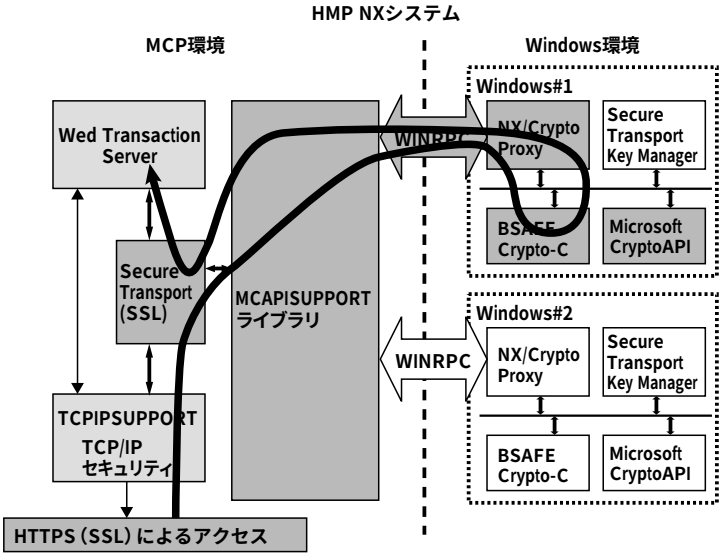


図 9　HTTPS（SSL）による Web Transaction Server へのアクセス

説した HTTP トンネリング機能や，SSL の実装等はこの構造故に実現した典型的な事例である．

今後も HMP　NX シリーズや後継シリーズもこのアーキテクチャに沿って，オープン環境への親和性の向上や膨大なアプリケーション資産を近代化する為に HMP システムの拡張計画が進められている．

＊ 1　802.3 チャネルアダプタ：ICP（Integrated Communication Processor）と呼ばれている Ethernet ネットワークに接続するための通信アダプタ．
＊ 2　共有アダプタ：Windows 環境の NIC を MCP 環境でも使用するアダプタ共有機能が設定されたネットワーク・アダプタのこと．
＊ 3　トロイの木馬：不正にシステムへ侵入し，データ消去やファイルの外部流出，他のコンピュータの攻撃などの破壊活動を行うプログラムのこと．
＊ 4　Well-Known ポート：ポート番号 0〜1023 までの既に割り当てられているポート．
＊ 5　処理を順番に割り当てるためのアルゴリズム．DNS サーバの負荷分散などにも使用されている．

執筆者紹介　福　家　　裕（Yutaka Fuke）
1973 年電気通信大学電波通信学科卒業．同年日本ユニシス(株)入社．NX シリーズの通信関連プロダクトの受入評価，日本化，保守に従事．現在，プロダクトサービス部 NX ソフトウェア室に所属．

武　村　正　彦（Masahiko Takemura）
1985 年大阪工業大学電気工学科卒業．同年日本ユニシス(株)入社．NX シリーズの金融端末，日本語印書装置の開発を経て，1997 年から同シリーズの通信関連プロダクトの受入評価，保守に従事．現在，プロダクトサービス部 NX ソフトウェア室に所属．