Bull. Natl. Inst. Health Sci.,**122**, 34-36 (2004) **Notes**

国立医薬品食品衛生研究所における基盤ネットワークの現状について

瀬川勝智・中野達也・林譲・中田琴子#

The Status of NIHS Computer Network System (NIHS-NET)

Katsunori Segawa, Tatsuya Nakano, Yuzuru Hayashi and Kotoko Nakata #

We described the development of National Institute of Health Sciences Computer Network System (NIHS-NET), which was named NIHS Information and Computing Infrastructure (NICI) previously. In the system, the main server machines and common machines were replaced and the network lines were upgraded from 100 Mbps to 1Gbps. The connection nodes were changed from Inter Ministry Network (IMnet) to Science Information Network (SINET), and the dedicated lines between NIHS (yoga, osaka, tsukuba) and SINET were constructed. The Internet connection speed from each campus to SINET was upgraded. We also performed security audit in this system.

Keywords: NIHS-NET, SINET, server machines, LAN, security audit

1. はじめに

国立医薬品食品衛生研究所（以下国立衛研）における研究情報基盤環境整備は，平成7, 8年の第1期および第2期[1,2]，平成11, 12年の第3期[3]と進み，平成15, 16年には第4期の整備が行なわれた．今回の変更に伴い，国立衛研における全所的なコンピュータネットワークの基幹部分とヘルプデスクがメンテナンスを行っている大型ソフト（分子計算ソフト，分子グラフィックソフト，遺伝子解析ソフト）やプレゼンテーション機器を総称してNIHS-NET（NIHS-Computer Network System）と呼ぶことにした．

第4期の研究情報基盤環境整備に先立ち，用賀本所，大阪支所，筑波薬用植物栽培試験場（以下筑波試験場），北海道栽培試験場（以下北海道試験場）ではネットワーク接続回線を高速化し，業務の効率化を図った．用賀本所，大阪支所，筑波試験場のネットワークは，それぞれ省際研究情報ネットワーク（IMnet）を経てインターネットに接続していたが，平成15年からは，学術情報ネットワーク（SINET）を経てインターネットに接続するように変更された（IMnetは平成15年9月末にサービスを停止した）．

今回の整備では，平成11年10月に納入した研究情報ネットワークのサーバ機器を，平成15年10月に，平成12年4月に納入したデータベース関連機器を平成16年4月にそれぞれ更新した．新サーバ機器の導入時にソフトウェアをバージョンアップし，一部ソフトウェアの変更も行った．今回の更新により，サーバ機器が高性能化し，ネットワークが高速化され、情報伝達の迅速化が期待される．用賀本所，大阪支所，筑波試験場に加え，北海道試験場も，仮想ネットワーク（Virtual Private Network: VPN）により用賀本所に接続された．またセキュリティを強化するため，ファイアウォール（Fire Wall: FW）を強化し，ウイルス対策用サーバを立ち上げた．

医薬品医療機器審査センター（現独立行政法人医薬品医療機器総合機構）は，平成16年4月に国立衛研から独立し，伊豆栽培試験場は平成14年3月末に，また大阪支所（法円坂）は平成16年3月末で廃止となった．大阪支所（茨木市）は，医薬基盤研究施設（以下基盤研）への移行が完了するまでは，NIHS-NETに暫定的に接続している．

NIHS-NETは所内への情報受信・交換の場だけでなく，所外への情報提供の場であるため，安全性を考慮したネットワークシステムの構築が重要となる．このような点を踏まえ，今回の回線高速化，および機器更新状況について記述する．

2. NIHS-NETの基幹システム

2.1 所外ネットワーク接続環境

当所の研究情報ネットワークは，用賀本所，大阪支所，筑波試験場を，それぞれIMnetの東京ノード，大阪ノード，筑波ノードと繋ぎ，インターネットに接続していた．平成15年には用賀本所（3月），大阪支所（4月），筑波試験場（9月）のネットワーク接続ノードが，IMnetからSINETに変更され，SINETを経由して外部ネットワークに接続する形態となった（IMnetは平成15年9月末にサービスを停止し

To whom correspondence should be addressed:
Kotoko Nakata; Kamiyoga 1-18-1, Setagaya-ku, Tokyo 158-8501, Japan; Tel: 03-3700-9572;Fax: 03-5717-7180;
E-mail: nakata@nihs.go.jp

た)．ノード変更の際に回線も高速化し，用賀本所は100Mbpsに，また大阪支所，筑波試験場は1.5Mbpsへと高速化された（大阪支所法円坂は平成16年5月現在専用回線を停止し，大阪支所茨木市のネットワーク立ち上げまでの期間は，Bフレッツ回線を使用している）．北海道試験場は平成16年5月にADSL回線の8Mbpsに変更され，種子島薬用植物栽培試験場（以下種子島試験場）は平成13年12月にフレッツISDN回線に変更されて64Kbpsになった．一方，和歌山薬用植物栽培試験場（以下和歌山試験場）は現在もISDN回線により接続されている．和歌山試験場を除き回線速度は高速化され，情報収集は以前よりも迅速化した．

所外からの接続は，用賀本所に設置されているFWを通り，所内LAN（Local Area Network）に繋がっている．今回の基幹システム構築では，FWを用賀本所にのみ置き，不正アクセスを遮断し，許可された通信のみを所内LANに通す設定にした．

2.2 所内LANの構成

用賀本所内の棟間の基幹幹線が，平成15年9月にこれまでの100Mbpsから1Gbpsに高速化された．新たに研究棟を新築（28号館）したため，内部セグメントを1つ増やし4つのセグメントとした．また，コンピュータやネットワーク対応機器が増加しIPアドレスの枯渇が所内でも問題になってきたため，アドレス体系をCクラスからAクラスに変更しすべてのマシンのIPアドレスを振り直した．IPアドレス変更時に数件のトラブルが発生したが，変更後はIPアドレスの枯渇も解消され，アドレスの割り付けも順調に行われている．

セキュリティ強化の一環として，基幹サーバ更新時にDHCP（Dynamic Host Configuration Protocol）サーバを立ち上げ，平成16年2月からはパソコンやネットワーク機器を所内LANに接続する場合にはMAC（Media Access Control）アドレスの登録を必要とするようにした．

筑波試験場は独自に場内LANシステムを構築しているが，ルータ間で用賀本所とVPN接続しているため，用賀本所と同様のネットワーク環境になっている．北海道試験場では，ルータ間のVPN接続ではなく，各パソコンにVPNクライアントソフトをインストールしVPN接続する形式となっている．VPN接続することにより，通信が暗号化され通信の安全性が強化された．

所内LANはTCP/IPプロトコルによる基幹部分と，Macintoshで使われるApple Talkプロトコルの二つのプロトコルで構築されている．

2.3 基幹システムサーバ機器

平成15年10月に導入した基幹サーバの概要を以下に記す．

a) Fire Wallサーバ（PIX515E）：所内のFW（用賀本所に設置）
b) Mail/外部DNSサーバ（Sun Blade150）：外部向けのDNSサーバ並びに，所内と所外との間のメールを中継するサーバ
c) DBサーバ（Sun Blade150）：Oracle9iにバージョンアップし，データは旧サーバから移設
d) Mail/DNS/Newsサーバ（Sun Fire280R）：メールサーバとして，メール保存用・ウイルスチェック・Webメール・MLサーバの機能を有する
e) Web/DNSサーバ（Sun Blade150）：所内のWebサーバが稼働
f) Proxyサーバ（Sun FireV100）：外部にアクセスするための中継を行うサーバ
g) DHCPサーバ（Sun FireV100）
h) 全文検索サーバ（Sun Fire280R）
i) 認証サーバ（HP ProliantML350）：VPNで接続する際の認証を行うサーバ
j) ウイルス対策用サーバ（HP ProliantL330G3）

2.4 共用プレゼンテーション機器

平成16年3月に更新した共用プレゼンテーション機器および共用ソフトを以下に記す．

共用プレゼンテーション機器

a) 検索用パソコン（HP Desktop d330SF/CT）
b) Macintosh（PowerMacG4）
c) プレゼン用Windowsパソコン（HP Desktop d330SF/CT）
d) プレゼン用Macintoshパソコン（PowerMacG4）
e) スライド作成機（Polaroid PP700U-B（Windows用，Macintosh用各1台）
f) スキャナ（EPSON GT-9400UF）
g) プリンタ（EPSON LP-9500CPS）
h) B0プリンタ（EPSON PX-10000）
i) 計算サーバ（SGI FuelV10）：Accelrys社のInsight Ⅱ実行用機器
j) 計算サーバ（IBM IntelliStation Z Pro 6221）Gaussian社のGaussian 03，GaussView3.0実行用機器
k) 液晶プロジェクタ（EPSON EMP-7800）

共用ソフト

l) Accelrys社のInsight Ⅱ：各モジュールを統合し分子モデリングのための3Dグラフィカル環境を支援し，モデリングおよびシミュレーションを実行するシステム
・継続したモジュールBiopolymer，Sketcher，Homology，MODELER，CHARMm
・新規に追加したモジュールDiscover，Affinity，CFF，Ludi，SeqFold
m) Applied Biosystems社のCELERA DISCOVERY SYSTEM：ヒトゲノム解析によって得られた生物学データ（遺伝子／タンパク質，転写産物，SNPs等）を検索する統合シス

テム

n) SGI 社の FAMSBASE：高性能タンパク質立体構造予測アルゴリズムによるモデル構造のデータベース

o) Gaussian 社の Gaussian 03［アップグレード］，GaussView3.0［新規］：分子軌道計算および軌道可視化プログラム

今回の更新には，SRS-EMBOSS（ライフサイエンス系データベースおよびツールの統合環境支援システム）を実行する Sun Fire880 の保守（2.5 年分）およびネットワーク監視機器に使用する OS（RedHat LINUX （4 本））が含まれている．また，Active mail のユーザ数を 500 に増やした．

2.5 VPN 接続環境

用賀本所と筑波試験場の VPN 接続は，2 拠点に設置されたルータ間で行っている．そのため，筑波試験場内の LAN は，用賀本所とほぼ同様の環境となる．また，北海道試験場では，回線移行時にブロードバンドルータを用いており，ルータによる VPN 接続ができない．そのため，各パソコンにクライアントソフトをインストールし，用賀本所に設置されているルータを通り認証サーバに接続することにより VPN 接続を可能とした．他の試験場でも回線の高速化が進み，ソフトをインストールすることにより用賀本所へ VPN 接続が可能である．

所外から所内にパソコンを繋ぐときにも，パソコンにソフトをインストールすることにより VPN 接続でき，非常に便利になった．またパソコンを VPN 接続する際には，アカウント登録が必要である．

3. 結果と考察

用賀本所を始め，各拠点での回線の高速化が進み，今回の整備によりサーバ機器も高機能のものに変更された．ネットワーク回線は高速化したものの，パソコン一人一台から一人数台となり，かつプリンタ等のネットワーク対応機器が所内 LAN に接続されている．したがって以前では考えられなかった大容量のファイルがネット上を流れており，これまで以上にネットワークに負荷がかかる状況になっている．また，接続機器の増加に伴いスイッチのポートが足りなくなり，カスケードして接続しているため，ネットワーク通信のボトルネックになっている．現行システムではネットワークのセキュリティを向上するため，接続する際に MAC アドレスを登録制にした．この MAC アドレスを基に接続マシンを監視することで，不正なアクセスやパケット等の発生源を調査することが可能となり，以前のように容易に所内 LAN に接続できなくした．不要な通信をできる限り遮断し，所内 LAN を全所員が有効に使えるよう対処していくことが重要である．

最近では，所外から所内 LAN への不正アクセスやウイルス対策が極めて重要な課題となっている．不正アクセスについては，用賀本所の FW により許可された通信のみを所内 LAN に通している． VPN 接続を利用して所内 LAN にアクセスすれば，通信の暗号化により安全性も確保される．しかし，所内のパソコンが不正アクセスされた場合には対処が難しくなるため，所内 LAN に接続しているパソコンの使用者がセキュリティ対策を講じる必要がある．

現行システムのウイルス対策については，基幹サーバ上でのウイルススキャンおよびウイルス対策サーバ（Windows マシンのみが対象）上でのウイルス対策ソフト稼働状況の確認の 2 段階で行っている（Macintosh については，スタンドアロン版のウイルス対策ソフトを配布）．どちらの監視もヘルプデスクで行っているが，各パソコンにウイルス対策ソフトのインストールが行われていなければ，ウイルス対策サーバでの監視はできない．このため，ウイルス対策ソフトのインストールを所内に徹底し，ウイルス感染状況を集中的に監視できる体制作りを進めている．ネットワーク監査については平成13年度から小規模に実施していたが、平成15年度より外部業者に委託して本格的に実施し、セキュリティホールの解消に務めた。

現在の NIHS-NET には，単にネットワークサービスの提供ができるだけでなく，コンピュータウイルス等へのセキュリティ対策の高い，安定したネットワークシステムであることが強く要求されている．ネットワーク技術は，秒進分歩であり，できる限り最新の技術を投入して（もちろん検証は必要であるが）さらなるセキュリティ向上に繋げていきたい．

謝辞

NIHS-NETの運用，維持および更新には所内の多くの方々にご協力いただいた．ネットワークの保守，維持および障害時の対応にはヘルプデスク（CTC-LS（株））の協力を得ており，ここに感謝する．

参考文献

1) Nakata, K., Nakano, T. and Kaminuma, T.: *Bull. Natl. Inst. Health Sci.*, **114**, 53-61 (1996)

2) Nakata, K., Nakano, T., Takai, T. and Kaminuma, T.: *Bull. Natl. Inst. Health Sci.*, **116**, 92-100 (1998)

3) Nakata, K., Nakano, T., Takai, T., Komine, K. and Kaminuma, T.: *Bull. Natl. Inst. Health Sci.*, **118**, 107-116 (2000)