Bull. Natl. Inst. Health Sci., **130**, 75-77（2012）　　**Technical Data**

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更新

瀬川勝智#，中野達也，斎藤嘉朗

Renewal of NIHS computer network system

Katsunori Segawa#, Tatsuya Nakano and Yoshiro Saito

Updated version of National Institute of Health Sciences Computer Network System (NIHS-NET) is described. In order to reduce its electric power consumption, the main server system was newly built using the virtual machine technology. The service that each machine provided in the previous network system should be maintained as much as possible. Thus, the individual server was constructed for each service, because a virtual server often show decrement in its performance as compared with a physical server. As a result, though the number of virtual servers was increased and the network communication became complicated among the servers, the conventional service was able to be maintained, and security level was able to be rather improved, along with saving electrical powers. The updated NIHS-NET bears multiple security countermeasures. To maximal use of these measures, awareness for the network security by all users is expected.

Keywords: NIHS-NET, main server system, virtual machine, network system, security countermeasures

はじめに

平成7年に始まった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23年に第6期の整備が行なわれた（第1期から第4期の整備については，参考文献[1-4]を参照）．平成19年に行った第5期の整備では，第4期で導入した研究情報ネットワークのサーバ機器とデータベース関連機器を一括して刷新し，利用しているサービス内容は極力変更しなかった．今回の「国立衛研における基盤ネットワークNIHS-NET（NIHS-Computer Network System）」更新では，政府方針として地球環境に配慮したグリーンITに対応することが強く求められたことから，これまでのサーバ構築手法を見直すこととした．このため今回の第6期整備（平成23年10月）では，平成19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，省電力なシステムにした．一方，データベース関連機器は予算上の問題から，一部を除き更新できなかった．また必要と思われるサービス内容は，システム更新後も提供を継続している．

NIHS-NETは所内の情報を共有する場だけでなく，所外から有益な情報を収集したり，所外への情報発信の場でもあるため，その出入口においては安全性を考慮したシステムの構築が重要となる．このような点を踏まえ，第6期整備後のNIHS-NETの状況について記述する．

1．NIHS-NETの基幹システム

今回の構築では，前述のようにグリーンIT推進の関係から省電力かつ高性能なシステムが望まれたため，ここ数年の急速な技術革新により，基幹システムへの導入実績も着実に増えている，「仮想化技術」を有するシステムの導入を行うことにした．仮想化技術は様々なサービスを提供していたサーバを仮想化し，高性能サーバ上で稼働させる技術である．これまで専用機器で行っていたサービスについてもできる限り仮想化して構築すること

To whom correspondence should be addressed:
Katsunori Segawa; Division of Medicinal Safety Science, National Institute of Health Sciences, 1-18-1 Kamiyoga, Setagaya-ku, Tokyo 158-8501, Japan; Tel: +81-3-3700-1141 ext. 375; Fax: +81-3-3700-9788; E-mail: k-segawa@nihs.go.jp

にした．

まず，システム構築の基盤となる高性能サーバは，提供するサービスの増加や冗長性を考慮して3台とし，さらに当該高性能サーバの管理用としてサーバ1台を加え，計4台で構成した．その上で稼働させる仮想サーバは，これまで提供してきたサービスを精査し決定した．また，仮想サーバとして稼働する場合，従来の物理サーバと比較して性能の低下が予測されたため，各サービスを提供しているサーバの機能をできる限り分割し，1台のサーバにかかる負荷を分散し，性能低下を極力抑えた．稼働している仮想サーバは，外部DNS（Domain Name System）サーバ，内部DNSサーバ, DHCP（Dynamic Host Configuration Protocol）サーバ，Proxyサーバ，外部Webサーバ，内部Webサーバ，認証サーバ，アンチウイルス対策サーバ，図書管理サーバ等である．特に旧システムのメールサーバは，外部および内部メールサーバの2台で構成していたが，旧システムでメールの大量送受信の際に発生したサーバの性能低下によるトラブルや，仮想サーバへの移行によるサーバの性能低下を考慮し，メールサーバの機能をできるかぎり分割し，個々の機能ごとにサーバ（外部メール中継サーバ，内部メール中継サーバ，メールスプールサーバ，メール送信サーバ，メーリングリストサーバ，迷惑メール隔離サーバ，Webメールサーバ）を構築した．さらに，旧システムでは専用機器を導入していたウイルスゲートウェイや，SSL-VPN（Secure Sockets Layer - Virtual Private Network）についても仮想専用機器として導入した．結果として，今回構築した仮想サーバは，管理運用に使用しているものも含め，23台となった．

仮想サーバによる構築に努めたが，FW（Fire Wall）/IPS（Intrusion Privention System）については構築段階において，今回の更新で必要とする機能を有する仮想サーバが販売されていなかったため，専用機器を導入した．ディスクは，共有ストレージで構築している．データのバックアップは定期的に専用の回線経由で行っているため，所内LAN（Local Area Network）には影響を与えない．また，データベース関連機器の中で利用者が多いB0プラスプリンタについては，ひき続き導入した．

2． ネットワーク接続環境

2.1 所外ネットワーク接続環境

国立衛研大阪支所は，平成17年に独立行政法人医薬基盤研究所（以下基盤研）へ移行したため，国立衛研の研究情報ネットワークへ接続されているのは，用賀本所のみになった．国立衛研から外部への接続は，専用回線を用い学術情報ネットワーク（SINET）を経てインターネットに接続されている．接続スピードは100Mbpsのままとなっている．現在のネットワーク帯域の使用状況は，通常20％以下のため現時点では増速は予定されていない．しかし，取り扱うデータ量が増しネットワーク上を流れる通信量は増加することが予想されるため，今後は，通信回線の増速を検討する必要に迫られる可能性がある．今回のシステム更新では，インターネット接続のルータを更新した．

2.2 所内ネットワーク接続環境

NIHS-NETのサーバ室と，各棟に設置したスイッチは光ケーブルで，また各棟の各階間，および各階のスイッチから各居室間はLANケーブルで接続されている（一部設置されていないところがある）．今回，各棟のスイッチも更新し，所内LANは基幹システム内および各棟各階の各居室まで1Gbpsに対応した．従って，1Gbpsに対応したパーツ・機器を接続することにより，所内間では高速の通信が可能となっている．

2.3 VPN接続環境

所外から所内LANにアクセスするための環境も整っている．所外からパソコンをインターネット経由でSSL-VPN仮想専用機器に接続し，許可されれば接続が可能となる．VPN接続するには，アカウントの登録が必要である．

3． 所内LAN環境

NIHS-NET基幹サーバのIPアドレスを一部変更した．旧システムまではほとんどの基幹サーバにグローバルIPを割り当ててきた．しかし，外部に周知する必要がないサーバは，ローカルIPアドレスに変更した．内部セグメントや内部アドレス体系の変更は行わなかった（管理用に使うセグメント等の新設は行った）．以前導入したMAC（Media Access Control）アドレス認証は現在も有効になっており，MACアドレスが登録されていないネットワーク機器は接続できない．

セキュリティ対策として，アンチウイルス対策サーバを導入している．旧システムではWindows機器のみが対象だったがMacintoshにも対応できるようになり，このサーバから提供されたアンチウイルスソフトをインストールした端末に関しては，セキュリティ対策状況を常に管理している．また，ウイルスゲートウェイを設置し，メールの送信やWeb閲覧の際に使っているプロトコルについてセキュリティ検査を行っている．これらのサーバや専用機器から緊急性のあるトラブル報告があった時は，迅速に対応することにしている．

考　察

サーバを仮想化してシステムを構築したため，物理サーバ数が激減し，かなりの節電効果（旧システムと比較し約40%削減）が得られた．これまでサーバ室では，2台のエアコンをフル稼働していたが，システム更新後は1台でまかなえるようになった．一方で，仮想サーバ数はかなり増加したため，各サーバの管理および機能分割したサーバ内の通信経路が複雑になった．そのため，管理すべき箇所が増えて，トラブルの発生場所の特定も難しくなっている．今回の整備では管理機器の充実も図り，迅速な対応を行える体制を整えている．

NIHS-NETのセキュリティ対策は，以前にもまして重要である．先ずは，MACアドレスを登録制にしていて，必要でない機器は所内LANに接続させないようにし，不要な通信を排除している．現在も認証サーバに接続できなかった機器のMACアドレスの情報があがってくることがある．所内LANに接続した端末機器（パソコン等）には，使用しているOSやソフトの最新のセキュリティパッチを適用するよう，注意喚起を行っている．またアンチウイルス対策サーバが提供しているウイルス対策ソフトをインストールした端末機器の場合には，パターンアップを最新にして，定期的にウイルススキャンを行うことになっている．しかし，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，アンチ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管理できる体制作りを進めている（現行の情報セキュリティポリシー上，アンチウイルス対策サーバが提供しているウイルス対策ソフトを，必ず使用しなければならないというわけではない．他のウイルス対策ソフトを使用しても，同様の対策をとっていれば良いことになっている．しかし，管理対象にならないので，各種トラブル発生時には，利用者自身で対処することになるので，今後の検討課題である.）.

所外へのアクセスは，proxyサーバやウイルスゲートウェイを経由している．ウイルスゲートウェイを経由するときにウイルス等のチェックを行い，また外部への不正なサイトへのアクセスを遮断している．そこで利用している不正サイト情報は，刻々と変化するため更新作業を速やかに行い，できる限り最新の状態を保つようにしている．

最近では，外部からの不正アクセスがセキュリティ上の脅威として挙げられることが多くなった．不正アクセス対策については，NIHS-NETのFWで許可された通信やポートのみを所内LANに通し，IPSで不正アクセス元からの通信を遮断している．不正なアクセスやパケット等の発生源を調査（発信元を詐称したり，通信経路を複雑にした場合には調査は困難だが）することが可能となった．さらに，FW/IPSシステムによる監視をすり抜けたものについては，ウイルスゲートウェイで遮断している．不要な通信をできる限り遮断することで所内LANの帯域が確保され，利用者が効率的に使えるよう対処していくことが重要である．

このように，NIHS-NETのセキュリティ対策は多段階になっている．どれか選択して行うのではなく，それらを組合せて実行することにより，高度なセキュリティ対策がとれるのである．これらの監視はヘルプデスクで行っている．

さらに，毎年NIHS-NETの基幹システムについてネットワーク監査を実施して，セキュリティホールを定期的に見つけ速やかに対処して，セキュリティホールの解消に努めている．

今回の更新したNIHS-NETは，サーバ数が増加しネットワーク通信経路が複雑になったが，従来のサービス内容を維持し，さらにセキュリティが向上し省電力なネットワークシステムとして構築することができた．ただ，ネットワーク技術は刷新が早く，放置すればセキュリティホールを生む．NIHS-NETに最新の様々な技術を投入する必要がある時には，充分に検討し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ている．またNIHS-NETの保守，維持および障害時の対応にはヘルプデスク（日立電線ネットワークス株式会社）の協力を得ており，ここに深く感謝する．

引用文献

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）
4）Segawa, K., Nakano, T., Hayashi, Y. and Nakata, K.: *Bull. Natl. Inst. Health Sci.*, **122**, 34-36（2004）