Secure NICE の運用開始

八 槇 博 史

センターニュース Vol.6 No.2（2007.5）でお知らせしましたとおり，安全なネットワークアクセスの提供をめざした Secure NICE サービスが今年度より開始されております。本稿ではこのシステムの運用状況の報告を含め，前回の記事以降に決まりました利用申請手続きなどに関してお知らせいたします。なお，Secure NICE につきましての詳細は Web ページ http://www.net.itc.nagoya-u.ac.jp/secure-nice/ に載せてあります。

Ⅰ．Secure NICE とは

以下では，簡単に SecureNICE の概要について説明いたします。

従来の NICE で安全性の高いネットワークアクセスを行おうとした場合，インターネットに接続するにあたって各々の研究室等でファイアウォールなどを設置する必要がありましたが，NICE 側で設置するファイアウォールを利用することができるようになります。また，アドレス

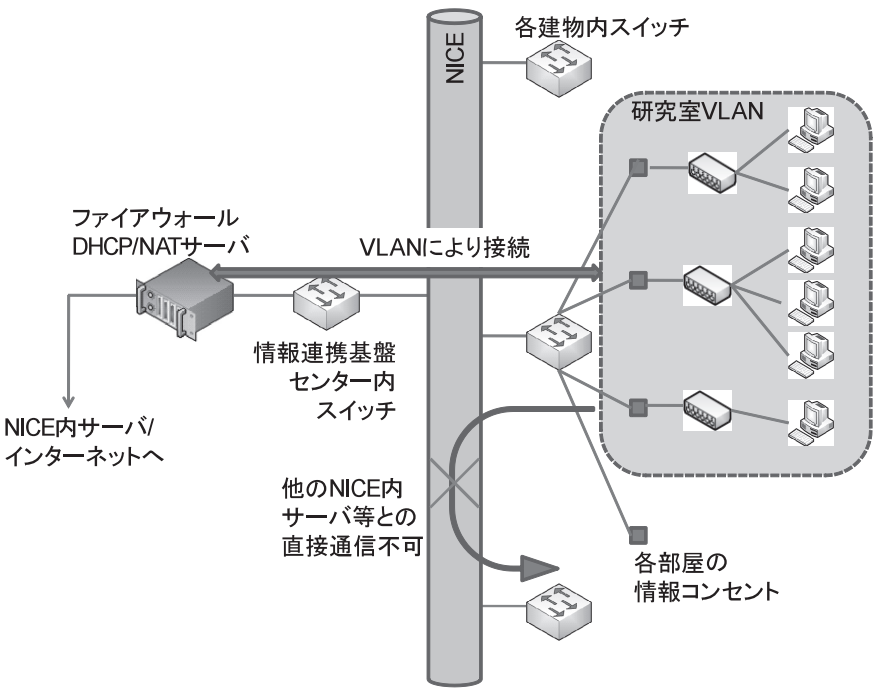

図 1　Secure-NICE システムの概要

の取得や各機器への付与，ルータの設定といった，新規に研究室ネットワークを構築する場合に必要となる各種の作業が必要なくなり，情報コンセントにコンピュータを接続するだけで使用が開始できるメリットがあります。このサービスでは，例えば新任の先生が着任されて研究室のネットワークインフラがまだない場合に，一から機器等をそろえて研究室のネットワークを構築しなくとも，Secure NICE を使えば活動を早期に開始することができる，といった利用シーンを想定しています。あるいは，事務室等から NICE へ接続するための安全な通信経路をつくりたい，といったケースにも適していると考えています。もちろん，すでに研究室ネットワークを構築済みであっても，Secure NICE サービスを利用してネットワークアクセスを安全にするということも可能です。

図 1 が Secure NICE のシステム概要です。

Ⅱ．Secure NICE でつかわれている技術

1．VLAN とは

VLAN（Virtual Local Area Network）とは，ネットワークスイッチなどネットワーク機器の機能によって，物理的な接続形態と異なるネットワークを構成する技術のことです。

VLAN 非対応のスイッチでは，同じスイッチのポートどうしであれば制限なしに通信するようになっています。この場合，複数の部屋をまたがる LAN を構成するためには，これらの部屋につながる配線を一つのスイッチに収容し，かつ，この LAN に含まれない部屋の配線はこのスイッチにはつながないようにする必要があります。さらに，この LAN を構成する部屋を変更する場合には物理的に配線のつけかえを行う必要があります。

これに対し，VLAN に対応したスイッチでは，スイッチのどのポートとどのポートが通信できるか，また，どのポートとどのポートとの間の通信を遮断するかをソフトウェア的に制御できるようになっています。これによって，例えば，一つのスイッチの 1 番から 4 番までが一つのグループで互いに通信でき，5 番から 10 番までが別のグループ，11 番と 12 番がまた一つのグループ，といったように，一つのスイッチを，あたかも複数のスイッチがあるかのように分割して使うことができます。

名古屋大学の多くの建物では，各部屋の情報コンセントが建物ごとのスイッチにつながれています。このスイッチで VLAN 機能を使うことにより，部屋をまたがった LAN を自由に構成でき，構成変更の際も配線に手をつけることなくソフトウェア的な設定により変更が可能となっています。

Secure NICE はこの VLAN の仕組みを基礎として実現されたサービスです。

2．NAT

Secure NICE のようにプライベート IP アドレスを用いるネットワーク，及びそこにつながれた機器は，インターネット内のグローバル IP アドレスをもった他の機器とは，そのままでは通信することができません。

NAT（Network Address Translator）はこのような場合に使われる技術の一つです。NAT サーバをプライベート IP アドレスをもったネットワークとグローバル IP アドレスをもったネットワークとの間に設置すると，NAT サーバはそこを通過するパケット（データのまとまり）を改変し，あたかもグローバル IP アドレスをもった機器どうしが通信しているかのようにアドレスのつけかえを行います。

このようにすることで，プライベート IP アドレスをもったクライアントから，グローバル IP アドレスをもったサーバに対して，アドレスの種類の違いを気にすることなく，またクライアントやサーバに特別な設定をほどこすことなく，通信を行うことができるようになります。

ただし，どのような通信であっても NAT が利用可能というわけではありません。Web やメールなどといった多くのアプリケーションについては問題なく使用できますが，テレビ会議システムや VoIP など一部のアプリケーションでは NAT 経由では使えなかったり，特別なしかけが必要となったりする場合があります。Secure NICE では，セキュリティ対策なども踏まえた上で，外部との間で通信できるアプリケーションを制限しています。

3．DHCP

DHCP（Dynamic Host Configuration Protocol）とは，ネットワークに接続された機器に，IP アドレスをはじめとした，通信に必要となる諸々の設定情報を付与するしくみのことです。

DHCP に対応したコンピュータ（最近の OS の大半が対応しています）がネットワークに接続されると，このコンピュータからネットワークに対して設定情報の付与が要求されます。DHCP サーバはこの要求を受けて，適切な IP アドレスをはじめとした種々の設定情報をこのコンピュータに対して送信します。コンピュータはその情報を使って，そのネットワーク上での通信を開始することになります。

Secure NICE ではセンター側に DHCP サーバが設置されており，利用者側ではネットワーク設定を特に考えることなく，ただつなぐだけでネットワークの利用が開始できるようになります。

Ⅲ．運用状況

Secure NICE についてですが，本原稿執筆時点でサービスはすでに開始しております。センター内の研究部門や大幸地区などにおいて日常的に使用しながら問題点の抽出や運用状況の監視，及び設定の改良を進めており，安定して使用が可能な状態となってきております。

センターの情報基盤ネットワーク部門での使用例を紹介します。同部門にはセンター所属の教員のほか，教員が兼任しております情報科学研究科及び工学部の学生が所属しています。この学生の居室のアクセスラインを Secure NICE として設定し，利用しています。居室には情報コンセントのポートが二つありますが，片方を Secure NICE 用のラインとして設定し，この下に HUB を設置，各学生の PC とプリンターとを接続しています。他方，外部からのアクセスを受け付ける必要のある Web サーバやメールサーバはこのポートとは別の通信経路に接続されています。この環境で日常的な使用を行いながら，同時に Secure NICE の設定についての細かな検

討（どの通信ポートを開放すべきか，利用上の問題が生じないかなど）を行うとともに，システムの動作状況の監視も同時に行っています。

Ⅳ．通信ポートの許可・遮断について

図 1 にも示しましたとおり，Secure NICE では VLAN 内部からのアクセスをいったんセンターのファイアウォール /DHCP/NAT サーバで受け，そこから NICE 内外への通信を行う仕組みになっておりますが，その性質上，どんな通信でも通過するという設定にはしておりません。どのような通信が許可されるべきかは利用者のニーズにも依存しますので，原則としては利用申請時に通過させる通信の種類を指定していただき，それに応じて通信ポートの開け閉めを行うという体制をとっています。現在の利用者の使い方をもとに検討して，今のところ標準では表 1 に示す通信が許可されるようにしております。

表 1　Secure NICE で標準で通信が許可されるポート

DNS（53/udp, 53/tcp），
NTP（123/udp）
HTTP（80/tcp）
HTTPS（443/tcp）
FTP（20-21/tcp）　（FTP は Active, Passive 両モードが使用できます）
SMTP（25/tcp）
SMTPS（465/tcp）
POP3（110/tcp）
POP3S（995/tcp）
IMAP4（143/tcp）
IMAP4S（993/tcp）
SSH（22/tcp）
TELNET（23/tcp）

実際の利用については，例えば，NICE 内の HTTP プロクシを使いたいがそのポート番号が 3128 だ，TELNET は不要なので止めておきたい，など個別のニーズがあると考えられますので，申請に応じてこれら以外の設定も可能です。適宜ご相談いただければと思います。なお，最近ではメールの送信のために Submission ポート（587/tcp）を使われるケースも増えてきておりますので，このポートも上記の標準許可ポートに入れる方向で検討中です。ただし，上記のポートの開放・遮断はあくまでも Secure NICE 内から外への通信に関してで，外から内への通信については原則として対応しておりませんのでご注意ください。

Ⅴ．利用申請について

上述の Web ページに申請書等のデータがあり，これに記入してセンターまで提出いただくことになります。

申請フローは以下のようになります。最初の申請については紙ベースで行っていただくことになりますが，設定の変更等はメールにより申請いただくことといたしました。

1 利用資格の確認
2 申請書の作成（新規・追加の場合）
3 申請書の提出（新規・追加の場合）
4 承認（新規・追加の場合）
5 メールによる申請（継続・変更・取消しの場合）

費用についてですが，規定では申請者に費用負担をおねがいいただくこととなっておりますが，現時点では Secure NICE サービスは試行期間という位置づけになっています。サービス試行期間中は無料となっております。

また利用の資格は下記のとおりです。これは NICE の利用資格と同様となっております。

1 本学の教職員
2 本学の学部学生
3 本学の大学院学生
4 本学の研究生及び客員研究員
5 その他センター長が適当と認めた者

Ⅵ．Secure NICE の増強について

Secure NICE は学内の複数の LAN を一か所でまとめ，ファイアウォール等のサービスを行う仕組みであるため，利用者数が増加しますとサーバに負荷がかかって性能が低下する恐れがあります。現在はサービス開始直後ということもあり，そのような問題が起きるような状況にありますが，将来にわたってのサービスを考えた場合には増強が必要となってまいります。

その費用に関しまして，将来的には課金による収入でまわしていくということなどまで含めて考えていかなければなりませんが，当面の対応としまして，本年度の総長裁量経費におきましてシステムの改善費用をお認めいただきました。今後，利用状況をにらみ，かつサービス内容の検討を行いながら，適宜増強作業を進めてまいります。

（やまき　ひろふみ：名古屋大学情報連携基盤センター）