Secure NICE の概要

八　槙　博　史　　安　藤　八　郎

情報連携基盤センターでは昨年来，安全性の高いインターネットアクセスを提供するためのSecure NICE について企画・検討を行ってまいりました。このたびセンターのサービスとして試験運用を開始するにあたり，サービスの概要について紹介します。

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おのおの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。Secure NICE では以下で説明するような仕組みを用いることで，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。

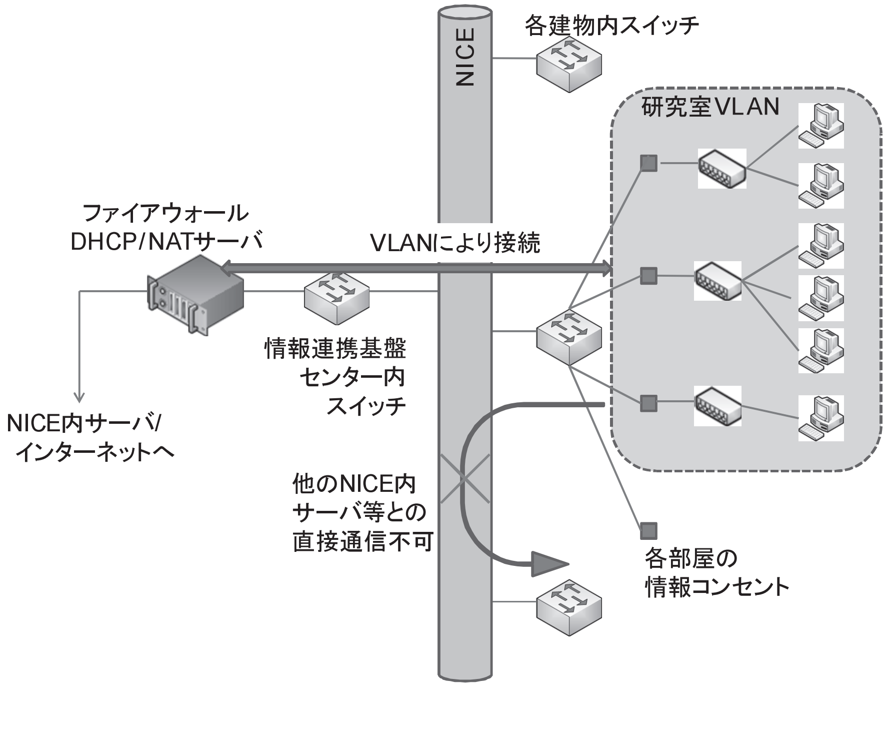

図1　Secure NICE のシステム概要

Secure NICEは新たに物理的なネットワーク配線を引き直すものではありません。すでに研究室等に設置済みの情報コンセントをSecure NICEのコンセントとして設定してプライベートなネットワークとし，通常のNICE内のサーバやインターネットと通信する場合には，NICE側で用意した ファイアウォール +DHCP+NATサーバを経由して行うものです。

Secure NICE用として設定された情報コンセントにPC等を接続すると，情報連携基盤センターに設置されたDHCPサーバからプライベートIPアドレス[1]が自動的に与えられます。このPCからNICE内の他のコンピュータ，あるいは外部のインターネットにアクセスする際には，情報連携基盤センターのNATサーバ及びファイアウォールを経由してアクセスすることになります。

現在NICEで行われているようなグローバルIPアドレスを各コンピュータに直接付与する方式とは異なり，プライベートIPアドレスを持ったコンピュータは外部のネットワークと直接通信することはできません。このようなコンピュータから外部へのアクセス要求が発生すると，NATサーバがプライベートIPアドレスをグローバルIPアドレスに自動的に変換して，通信を成立させます。逆にグローバルIPアドレスを持ったネットワークからプライベートIPアドレスをもったコンピュータへの通信は通常はできません[2]。

このような仕組みであるため，研究室の外に対してWebの閲覧，メールの送受信など，クライアントとしてしか利用しないPCなどの接続に適しています。外部からの接続がファイアウォール及びNATサーバによって遮断されているため，プライベートネットワーク内の各コンピュータが外部からのアクセスをうけることがなくなり，安全性が向上します。その一方，外部から内部へのアクセスができませんので，Webやメールのサーバといった，外部からのアクセスを受けるためのコンピュータの設置には適しません。

Secure NICEを利用する利点をまとめると，以下のようになります。

- 研究室内ではプライベートIPアドレスを使用しているので，外部から直接ワームなどの攻撃を受けることがない[3]
- 個人や研究室でルータやファイアウォールを購入する必要がなく，研究室で購入するものよりパフォーマンスが良い
- DHCPサーバにより，動的にプライベートアドレスが配布されるので，あらかじめグローバルIPアドレスを取得しておく必要がなく，PCなどの設定が簡単

Secure NICEのサービスは平成19年度初頭から実験サービスとして運用を開始します。申請方法や規定などの詳細は情報連携基盤センターのホームページ (http://www.itc.nagoya-u.ac.jp) でご覧になれます。

〈注〉

1　インターネットプロトコルで規定されたアドレスで，インターネットに直接つながない，組織内などプライベートなネットワークで使用するためのものです。規定されたアドレスはいくつかありますが，Secure NICEでは192.168.xxx.xxx（クラスC）という形のアドレスを

用います。

2　厳密にはVPN等を適切に使用することにより可能となりますが，Secure NICEでのサービス提供はいまのところ予定しておりません。

3　同じプライベートネットワーク内のコンピュータ同士の通信は通常どおり行えるため，例えば同じプライベートネットワーク内にあるウィルスに感染したコンピュータからの攻撃などは防げません。また，Secure NICE内のコンピュータであってもウィルス付メールなどを取り込んでしまうことなどはありうるため，個別のコンピュータのセキュリティ対策が不要になることを意味するものではありません。

（やまき　ひろふみ：名古屋大学情報連携基盤センター）
（あんどう　はちろう：名古屋大学情報連携基盤センター）