SecureNICE について

○石原正也 A)、安藤八郎 A)

A) 共通基盤技術支援室　情報通信技術系

概要

近年，名古屋大学では安全性の高いインターネットアクセスを実現するためにファイアウォール等を設置している研究室が増えてきた。しかし，必ずしも管理者がネットワークに詳しいとは限らない。設定の不備で建物全体のネットワークが停止する事態が起こったことがある。

今回，研究室でファイアウォール等の設置や設定をすることなく，安全性の高いインターネットアクセスを実現できるサービス「SecureNICE」について紹介する。

1　はじめに

名古屋大学では安全性の高いインターネットアクセスを実現するため，研究室や個人でブロードバンドルータを購入しプライベートネットワークを構築しているところがある。しかし，管理者がネットワークに詳しいとは限らない。実際に設定の誤りで，自分の研究室だけでなく建物全体のネットワークが停止したことがあった。また，ブロードバンドルータのみを使って複数の部屋や複数の建物を跨いで同じネットワークにすることもできなかった。

そこで情報連携基盤センターではこれらの問題を解決するために，「SecureNICE」を構築した。

2　SecureNICE について

SecureNICE とは，情報連携基盤センターで用意したファイアウォール/NAT/DHCP サーバを経由してインターネットに接続するサービスである。情報連携基盤センターでファイアウォール/NAT/DHCP サーバの設定を行うため, 研究室や個人でのブロードバンドルータ等の購入と設定, IP アドレスの取得を行う必要がない。また，パフォーマンスも研究室や個人で購入したものよりも高いといえる。

SecureNICE では，VLAN という技術を使ってネットワーク構成を変更するため，物理的な構成変更を行う必要がなく，現在使っている情報コンセントを SecureNICE 用の情報コンセントとして設定する。また，ユーザには DHCP サーバより自動的にプライベート IP アドレスが割り振られるため PC 等の設定も簡単である。プライベート IP アドレスを使っているので直接外部からの攻撃を受けることがない。外部と通信するときは NAT サーバによりプライベート IP アドレスをグローバル IP アドレスに変換することで，インターネットへのアクセスを可能とする。

これらの技術を使うことにより，ユーザは情報コンセントに機器をつなげるだけで安全性の高いインターネットアクセスを実現できる。

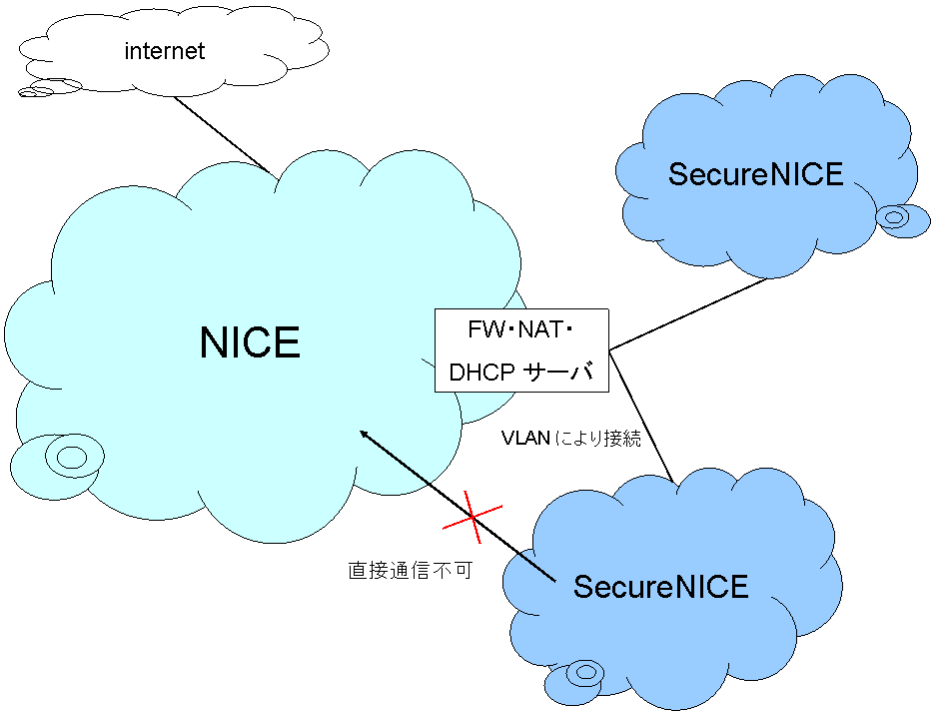

図 1. SecureNICE のイメージ

3 SecureNICE のしくみ

3.1 アドレスの割り当て

SecureNICE ではユーザ毎にクラス C のプライベート IP アドレスを割り当てる。その中でユーザからの申請により DHCP による自動割り当て分とそれ以外に分けられる。

また，SecureNICE 外のネットワークに通信する時には，NAPT により 1 つのグローバル IP アドレスに変換される。

3.2 ポートの制限

SecureNICE では安全性の確保のため，全てのパケットを通過するという設定にはなっていない。デフォルトでは表 1. のように最低限のポートのみの通信を許可している。これらのポートの制限は SecureNICE 内から外へ通信する時のみ行われ，SecureNICE 外から内への通信には原則制限していない。

表 1. 通信が許可されているポート

ポート	tcp/udp	サービス
20-21	tcp	FTP
22	tcp	SSH
23	tcp	TELNET
25	tcp	SMTP
53	udp	DNS
67-68	udp	DHCP
80	tcp	HTTP
110	tcp	POP3

123	udp	NTP
143	tcp	IMAP4
443	tcp	HTTPS
465	tcp	SMTPS
587	tcp	Submission
993	tcp	IMAP4S
995	tcp	POP3S
8001	tcp	教員プロフィール
8900, 8989	Tcp	メディア WebCT

デフォルトのポートのみだと不都合があると考えられるので, ユーザからの申請により表 1. 以外のポートの通信を許可し，逆に表 1. にあるポートを遮断することもできる。

4 SecureNICE の特徴

SecureNICE を使うメリットは以下の通りである。

- 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等の攻撃を受けない。
- 研究室や個人でブロードバンドルータを購入する必要がなく，パフォーマンスも良い。
- DHCP サーバより自動的に IP アドレスが付与されるので，あらかじめグローバル IP アドレスを取得する必要がない。

また，SecureNICE を使う時に注意することは以下の通りである。

- 外部からの接続がファイアウォールと NAT サーバに遮断されるため, Web や Mail サーバといった外部からのアクセスを受けるためのサーバ等の設置には適さない。
- 一般的な TCP/IP ポートは通信が許可されているが，特別なポートを使用する場合，申請する必要がある。
- NAT 変換されたグローバル IP アドレスは情報連携基盤センターのアドレスを使用しているため，IP アドレスで制限してある部局内専用ページ等にアクセスできない。その場合，部局管理者に SecureNICE の IP アドレスを追加してもらう必要がある

5 補足

ここでは，SecureNICE で使用している技術について補足する。

5.1 VLAN

VLAN とはルータやスイッチに附属している機能で，物理的な接続形態とは独立したネットワークを構築できる技術である。通常，同じスイッチに接続しているホストは同じネットワークに属する。ネットワークを分割するにはルータが必要であった。

VLAN を使うことにより，ルータを使うことなくネットワークを分割することができる。これにより今までは物理的に構成を変更しなければいけなかったのが，論理的にネットワークを変更することができる。

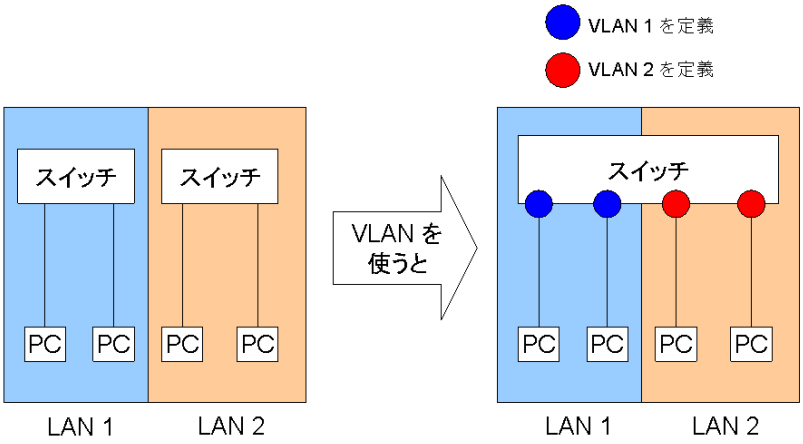

図 2. VLAN のイメージ

5.2 DHCP

DHCP とはネットワークに接続された機器に，IP アドレス等の通信に必要な情報を自動的に割り当てる技術である。DHCP サーバにはクライアントに割り当てる IP アドレス，サブネットマスク，ゲートウェイサーバや DNS サーバの IP アドレスなどが設定されている。

5.3 NAT（NAPT）

NAT とはある IP アドレスを別の IP アドレスに変換する技術で，パケットのヘッタ部を変換する。NAT では 1 つの IP アドレスを 1 つの IP アドレスに変換することができる。NAT に対し，NAPT とは IP アドレスに加えて TCP/UDP のポート番号も変換する。これにより，複数の IP アドレスを 1 つの IP アドレスに変換することができる。

なお SecureNICE では NAPT をしている。

5.4 ファイアウォール

ファイアウォールとは外部からの不正な通信を遮断するハードウェアやソフトウェアのことである。

6 おわりに

SecureNICE は情報連携基盤センターにある機器を使って運用しており，グローバル IP アドレスも情報連携基盤センターのアドレスを使っている。このため，部局専用ページにアクセスするとき等に不便を感じることと思われるため，将来的には部局のグローバル IP アドレスでアドレス変換できるようになればと思う。

また，SecureNICE は広く広報しなかったため，ユーザ数も多くない。IPv4 アドレスの枯渇の問題，管理者の負担減やセキュリティの面でも SecureNICE を使うことのメリットがあると思う。本稿にて SecureNICE に興味を持っていただけたらと思う。

参考文献

[1] “SecureNICE ホームページ “(http://www.net.itc.nagoya-u.ac.jp/secure-nice/)

[2] “SecureNICE の概要”，名古屋大学情報連携基盤センターニュース，Vol.6，No.2，pp146-148

[3] “SecureNICE 運用開始”，名古屋大学情報連携基盤センターニュース，Vol.6，No.4，pp349-354