ネットワークセキュリティシステムの構築

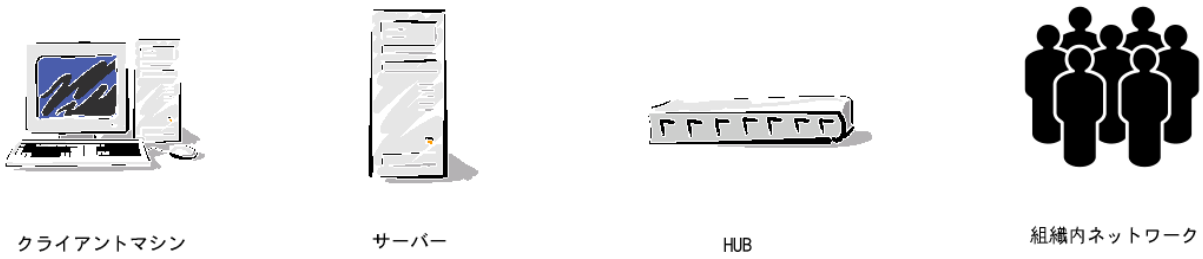
01H029 甲斐望

目次

1　はじめに

近年、インターネットを利用する人口が急増している。知りたい情報を調べたり、好きなアーティストの Web サイトを見るのに便利だからであろう。ところが、インターネットを利用する人口に比例して、マシンのデータ破壊活動などを行うコンピュータウィルスや、他人のマシンを乗っ取るクラッキングなど、ネットワークのセキュリティに悩まされる人々も増えてきた。コンピュータウィルスの被害を防止するために、市販のパソコンにプリインストールされているワクチンソフトウェアを使用したり、新たにワクチンソフトウェアを購入してパソコンへインストールしする家庭も増えている。クラッキング対策として、インターネットに接続しているマシンから自分のマシンへ不正に侵入されるのを防ぐシステムであるファイヤーウォールも使用されるようになった。インターネット上から組織 LAN や個人のマシンへの攻撃から守るこれらの方法が、人々にネットワークセキュリティとして意識されている。ところが、組織 LAN でコンピュータウィルスに感染したマシンを LAN に接続し、LAN 経由で他のマシンへウィルスを感染させたり、他のマシンへ故意に攻撃をしかけたりする者がいる場合がある。これらの攻撃から組織 LAN で身を守る方法はあまり充実していない。そこで、本研究では組織 LAN でのネットワークセキュリティを提案する。

なお、本文中にある図の凡例は以下である。



2　従来のネットワークセキュリティ

ネットワークセキュリティとはネットワーク上でのマシン防衛策。マシンを攻撃から守り、不正アクセスの防止や個人データなどの情報漏洩を阻止し、システムの安全性を保つことである。従来、このネットワークセキュリティはインターネット上から個人のマシンを守る方法であった。まずはその従来のネットワークセキュリティを紹介する。

2.1　ファイヤーウォール

外部ネットワークから内部ネットワークへの侵入を防ぐシステム。社内 LAN などの内部 LAN へ外部から第三者が侵入し、ファイルやプログラムの盗み見、改ざん、破壊などが行われないようにゲートウェイを監視するシステムである。

2.2　コンピュータウィルス対策

コンピュータウィルスとはに許可なく侵入して動くプログラム。その種類はさまざまで、画面の表示をおかしくするものから、コンピュータのファイルを破壊して OS の起動不可にしてしまうものまである。コンピュータウィルスはネットワーク経由で感染するものが多いので、インターネット普及率に比例して感染したパソコンが増えている。これらコンピュータウィルスを駆除するソフトウェアをワクチンソフトウェアという。このソフトウェアをもちいて、コンピュータウィルスに感染したマシンからウィルスを駆除したり、ウィルスに感染するのを未然に防ぐことが可能となる。

2.3　セキュリティパッチ

ソフトウェアにセキュリティホールが発覚し安全上問題がある時に配布される修正プログラム。通常はインターネットや雑誌の付録 CD-ROM などを通じて無償で配布される。セキュリティパッチは、ソフトウェア内でセキュリティホールの原因となっているファイルを問題のないファイルに置き換える。同時期に複数のセキュリティホールが発覚したり、同じファイルに複数のセキュリティホールが存在していた場合は、1 つのセキュリティパッチが複数のセキュリティホールを修正することもある。

3　新しいネットワークセキュリティ

第 2 節では従来の方法を紹介した。今回新しいネットワークセキュリティとするのは組織内ネットワークにおけるセキュリティを指している。本研究で構築するサーバの名前を Sasna システムと命名した。Strike A SNAg(壁にぶちあたる) という言葉から名前をつけた。このサーバは主に DHCP と IP エイリアスの機能を用いて構築してある。まずはこの DHCP の機能と IP エイリアスについて説明する。

3.1　DHCP

DHCP(Dynamic Host Configuration Protocol) とは、ネットワークに接続するコンピュータに IP アドレスなど必要な情報を割り当てるプロトコル。DHCP サーバには、ゲートウェイサーバや DNS サーバの IP アドレスや、サブネットマスク、クライアントに割り当ててもよい IP アドレスの範囲などが設定されており、LAN などの手段を使ってアクセスしてきたコンピュータにこれらの情報を提供する。クライアントが通信を終えると自動的にアドレスを回収し、他のコンピュータに割り当てる。DHCP を使うとネットワークの設定に詳しくないユーザでも簡単にインターネットに接続することができ、また、ネットワーク管理者は IP アドレスを割り当てる対象を容易に一元管理することができる。

3.2　IP エイリアス

IP エイリアスとは、ひとつのネットワークカードに複数の IP アドレスを割り当てる方法である。この設定により、仮想的に複数のインターフェイス（IP アドレス）を利用可能になる (図 1)。1 台のサーバマシン上で複数の Web サーバを起動して、それぞれ別の IP アドレスを割り当ててサービスを提供する場合などに利用できる。

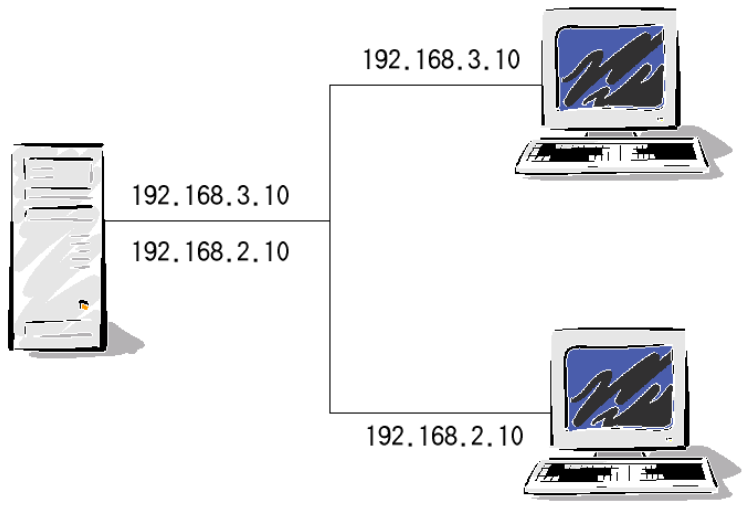


図 1: IPalias

3.3 Sasna システム

Sasna システムとは

本研究では物理的に同一なネットワーク上で、論理的にネットワークを分けることにより他のクライアントへの通信を不可にするものである。他のマシンとの通信をするには、同じサブネット[*1] である必要がある。通常、物理的に同一ネットワークに接続しているマシンには、同じサブネットの IP アドレスを割り当てているのでそれぞれマシン同士での通信が可能となっている。サブネットをマシン別で違うサブネットにわりあてることができれば、マシン同士の通信は不可となる。この違うサブネットの IP アドレスを与えるのに、DHCP のシステムを用いる。しかし、このままマシンに個別のサブネットを割り当てると、サーバとサブネットが違うものになるので、他のマシンはおろか、他の全てのマシンとの通信が不可になってしまう。そこで、IP エイリアスでサーバにマシンの数だけ別々のサブネットである IP アドレスを割り当てて、サーバとマシンとの通信を成り立たせる。これでマシン同士は通信できず、サーバとマシンのみの通信が可能となる。よって、他のマシンへの攻撃が不可となり、攻撃対象となりうるのはサーバだけになる。したがって、サーバのセキュリティだけを考えればよい。

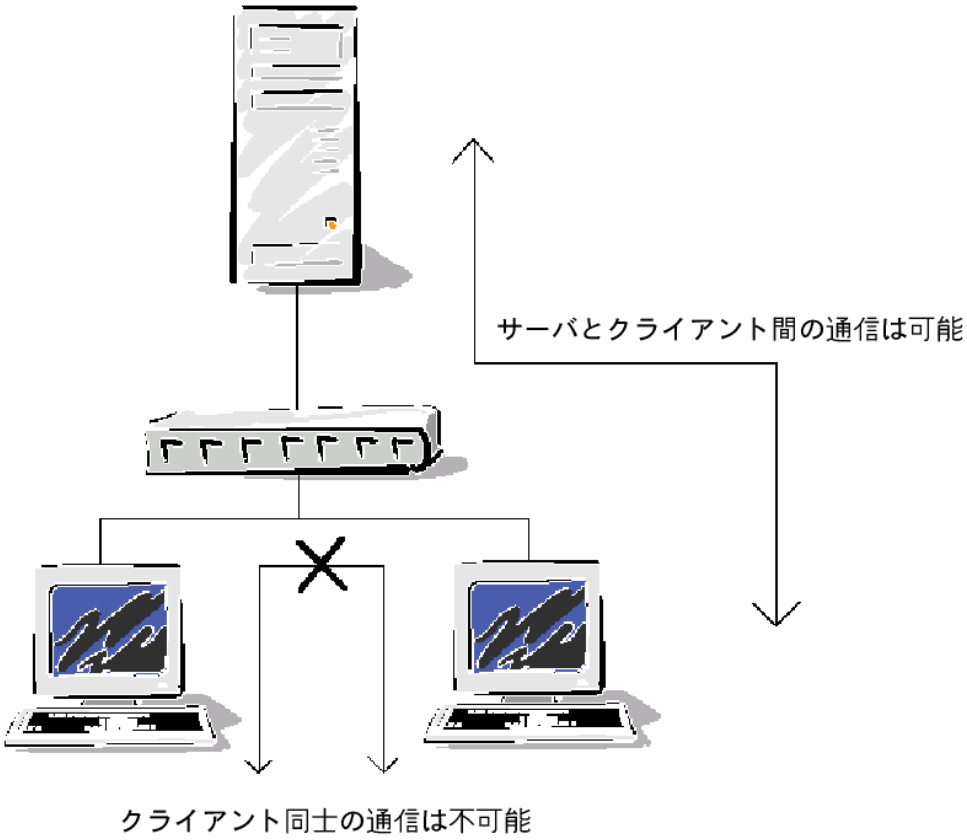


図 2: Sasna システム

[*1] 大きなネットワークを複数の小さなネットワークに分割して管理する際の管理単位となる小さなネットワーク

実装

Sasna システムを実装した手順は以下の通りである。

1. 「/etc/dhcpd.conf[*2] 」の設定を変更する。NIC の MAC アドレスごとに固定 IP アドレスを割り当て、NIC ごとに別々のサブネットとした。
2. 「/etc/rc.d/rc.sysinit[*3]」の設定を変更する。IP エイリアスを割り当てて、その IP アドレスをルーティングに追加するよう変更した。

実装内容の詳細は末尾の付録に記載してある。

[*2] DHCP クライアント設定ファイル
[*3] 起動時の設定をするスクリプト

4　考察

ここで検疫ネットワークとの Sasna システムの比較を行う。検疫ネットワークと比較する理由は、組織内ネットワークでのセキュリティになるからである。まずは検疫ネットワークがどういうものか説明する。

4.1　検疫ネットワーク

検疫ネットワークとは、コンピュータをすぐに組織内ネットワークに接続せず「検疫ネットワーク」に強制的に接続するシステム。必要なセキュリティ対策のされていないクライアントは隔離、検疫（検査・治療）を行う。組織のセキュリティポリシに合致したのち、組織内のネットワークに接続を切替える。図 3 を用いて説明すると、まずクライアントから HUB へ通信が行われた際、接続してきたクライアントがセキュリティポリシと合致しているかを調べる。もし合致していなかった場合は左上のサーバに隔離し、検疫を行う。検疫が終了したらセキュリティポリシは合致するので、右上の組織 LAN へと接続できるようになる。

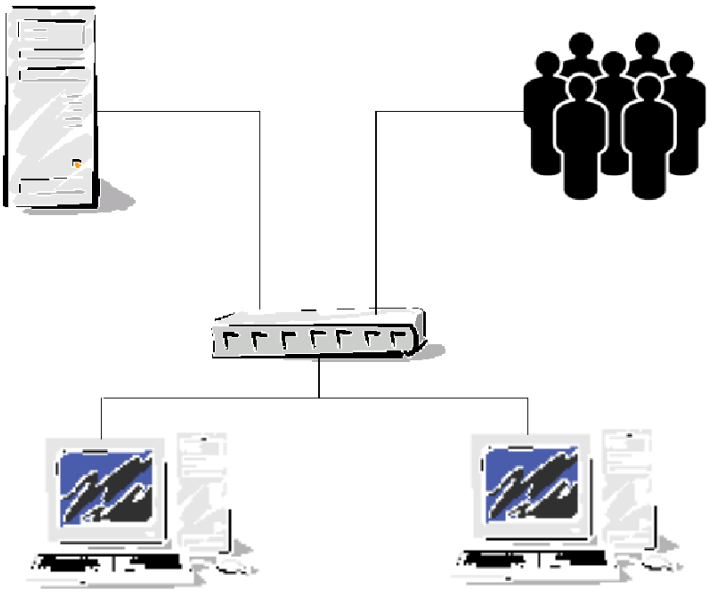


図 3: 検疫ネットワーク

4.2　検疫ネットワークとの比較

持ち込み PC からウィルス感染をふせぐのであれば検疫ネットワークでも可能である。しかし、ネットワークを切替えるスイッチが必要になるので費用が発生する。さらに、クライアント同士は物理的にも論理的にも同一ネットワークなので通信が可能である。したがって、クライアントから他のクライアントへの攻撃があった場合には検疫ネットワークでは対処できない。それにくらべて Sasna システムは費用はサーバの費用のみですむので安価でかつ、

内部での攻撃対策にも使用できる。

4.3 メリット

Sasna システムを構築するにあたっての最大のメリットはサーバの設定のみで成り立つことにある。新しいクライアントが加わった場合や持ち込み PC が接続された場合でも、そのクライアントの設定は変えずに Sansa システムの設定を変えるだけでよいので、クライアントのマシンに入っているデータなどがサーバの管理者にのぞかれる恐れもなくなる。さらに、第 4.2 節にも記述したが、安価であるということもメリットである。

4.4 デメリット

デメリットはクライアント同士での通信が必要になった場合、通信が不可能なので物理的にクライアント同士データを渡す、などの必要があること。あとサーバに負荷がかかるなどしてダウンしてしまった時は、他のマシンとの通信手段がなくなってしまうこと。以上がデメリットである。

5　今後の課題

現状では、サーバの DHCP の設定は、クライアントの NIC の MAC アドレスを個別にあてて実装している。このままでは、新しいマシンを接続しただけでは、ネットワークに接続することが不可能である。今後のとして以下の 2 点があげられる。

- 新しい NIC が LAN につながれたら、自動で新しいサブネットの IP アドレスを割り当てること
- クライアントからクライアントへの通信が必要な際は、データの種類などを調べて、送れるようにすること

これらを実装することが課題である。

6　まとめ

高速な通信が可能なネットワークが世の中にどんどん普及している。ところが、その環境にふさわしいセキュリティシステムは整っていない。本研究のシステムもすべての環境で適切とは限らないが、今度さらに加工を加え、使い勝手を良くし、システムを適用すべきふさわしい環境において使用すると、より良いネットワーク環境になるだろう。

謝辞

Sasna システムを構築したサーバに PlatHome 社の OpenBlockS を使用した。手軽さ持ち運びのしやすさから、家庭でも学校でもサーバの構築が進めることができ、非常に研究向きだったと思われる。OpenBlockS を開発した研究者たちに深く敬意を表すとともに、研究するにあたって助言をいただいた大垣斉講師・藤井教授・中村講師ならびに fken.a4w メーリングリストの方々に感謝の意をのべます

参考文献

[1] PLAT'ONLINE 『http://www.plathome.co.jp/』
[2] OpenBlockS Users room 『http://his.luky.org/OBU/』
[3] IT 用語辞典 e-Words 『http://e-words.jp/』
[4] @IT -アットマーク・アイティ- 『http://www.atmarkit.co.jp/index.html』

(上記 URL は 2004/12/16 現在のものである)

付録A　設定ファイル

A.1　/etc/dhcpd.conf

```
subnet 192.168.2.0 netmask 255.255.255.0
{
        range 192.168.2.10 192.168.2.132;
}
```

以上が変更する前の dhcpd.conf(一部分) である。これは 192.168.2.0 のサブネット (ネットマスク 255.255.255.0) で、クライアントに与える IP アドレスが 192.168.2.10 から 192.168.2.132 のうち使用されていない IP アドレスを与えることをさしている。

```
subnet 192.168.2.0 netmask 255.255.255.0
{
        option broadcast-address        192.168.2.255;
        host haru
        {
                hardware ethernet       00:00:00:XX:XX:XX;
                fixed-address           192.168.2.10;
        }
}

subnet 192.168.3.0 netmask 255.255.255.0
{
        option broadcast-address        192.168.3.255;
        host natu
        {
                hardware ethernet       00:00:00:XX:XX:0X;
                fixed-address           192.168.3.10;
        }
}
```

以上が dhcpd.conf の変更点である。この設定では、個別にサブネットを与えるため、サブネットごとに MAC アドレスを指定している。サブネット 192.168.2.0 では MAC アドレス 00:00:00:XX:XX:XX を持つホスト haru に 192.168.2.10 という固定 IP アドレスを与えている。同様に 192.168.3.0 のサブネットではホスト natu に固定 IP アドレス 192.168.3.10 を与えている。

A.2 /etc/rc.d/rc.sysinit

```
if [ -f /usr/sbin/dhcpd ]; then
        echo "starting dhcpd..."
        /usr/sbin/dhcpd eth0
        touch /var/lock/subsys/dhcpd
fi
```

以上が/etc/rc.d/rc.sysinit 変更する前の設定である。dhcpd に関する記述のみ抜粋してある。ここでは dhcp を起動するコマンドがかかれている。

```
if [ -f /usr/sbin/dhcpd ]; then
        echo "starting dhcpd..."
        /usr/sbin/dhcpd eth0
        touch /var/lock/subsys/dhcpd
        ALIAS1="192.168.3.1"
        ifconfig eth0:0 ${ALIAS1}
        /sbin/route add -host ${ALIAS1} dev eth0:0
fi
```

以上のうち if から fi 間の 6 行のうち下 3 行が/etc/rc.d/rc.sysinit の加筆点である。ALIAS1 という変数に IP アドレス（この場合、IP エイリアスで設定したい値）192.168.3.1 を代入し、ifconfig eth0:0 で eth0 に IP エイリアスを設定。/sbin/route add で eth0:0 のルーティングを行っている。