社団法人　情報処理学会　研究報告
IPSJ SIG Technical Report

2005－DSM－36（1）
2005／3／18

同報通信を制限した機器を用いる情報コンセント構築法

今泉 貴史
千葉大学 総合メディア基盤センター

佐藤 淳史
千葉大学 自然科学研究科

情報コンセント構築の際には、接続端末を守るための方策、接続端末からの攻撃を防ぐ方策など、さまざまな処理が必要となる。外部と内部の通信であればファイアウォールなどを設けることで対処できるが、情報コンセントにつないだ端末同士の通信は同様の方法では制限できないため、情報コンセントを構成するネットワークセグメントでネットワークワームが蔓延してしまう危険がある。本稿では、同報通信を制限した機器を用いることで、端末間の直接通信を制限するような情報コンセントの構築手法について述べる。提案する機器を用いることで、ワームの蔓延を防ぐことができるだけでなく、許された端末同士が直接通信することも可能となる。

A Construction Method for LAN Sockets using Broadcast-restricted Ethernet Switches

IMAIZUMI Takashi
Institute of Media and Information Technology,
Chiba University

SATO Junji
Graduate School of Science and Technology,
Chiba University

When we construct LAN sockets, we need to consider preventing attacks. There are two types of attacks, attacks from outside of LAN sockets, and those from inside of LAN sockets. Although we can prevent intrusion from outside of LAN sockets using Firewalls or Intrusion Prevention Systems, we need another method to prevent intrusion from inside of LAN sockets. We propose a new method to construct LAN sockets using broadcast-restricted Ethernet switches. Using this method, we can not only prevent spread of network worms, but also permit communication with clients each other.

1　はじめに

インターネットの広がりに加え、ノートパソコンやPDA などのモバイル端末が普及・高性能化したことで、これらの端末をネットワークに接続するための情報コンセントが普及しつつある。情報コンセントを構築するだけであれば難しい技術は必要ない。インターネットとの接続性がある既存のネットワークにスイッチやハブを接続するだけで、基本的な機能は提供できる。しかし実際には、セキュリティの問題などから情報コンセント専用のネットワークを構築している例が多い。

情報コンセントに求められるセキュリティ機能としては、情報コンセントの提供者に対する安全性と、情報コンセントの利用者に対する安全性の 2 つを考えなければならない。提供者に対する安全性としては、情報コンセントを提供する組織が情報コンセントを提供することで不利益を被らないようにすることを考えなければならない。一方利用者に対する安全性としては、情報コンセントを利用するものが情報コンセントに接続したことで不利益を被らないようにすることを考えなければならない。

情報コンセントの利用者は、外部から見れば情報コンセントを提供している組織に属しているように見える。つまり、情報コンセントから外部に対して侵入などの行為が行われた場合、情報コンセントの提供者がその責任を負うことになる。もしこのような事件が発生すれば、その組織は対外的に信用を落とすなど多大な不利益を被ることになる。また、情報コンセントを提供したために、そこから組織内部のネットワークに対する不正侵入を許してしまう可能性もある。このための対策としては、情報コンセントからの通信を厳しく監視するファイアウォールなどを設けて可能な通信を制限する方法や、利用者を特定することで問題発生時の責任の所在を明らかにする、ユーザ認証などによりあらかじめ許された利用者しか利用できないようにするなどの対策が採られている。

情報コンセントに接続することはインターネットに接続することと同義であり、世界中からのさまざまな脅威にさらされることになる。このための対策として

は、やはりファイアウォールを設ける方法が有効である。また、通常は情報コンセントに接続する端末に対して外部から直接接続する必要はないため、NAPT 機器を用いてプライベートアドレスを使う情報コンセントを構築し、外部からの直接の接続を許さないことも多い。さらに、POP や HTTP などの特定のプロトコルに関しては、ウイルスチェックを施す場合もある。

また、情報コンセントを利用する場合には、1 つのネットワークにさまざまな端末が接続することになる。このとき、接続している 1 台がネットワークワームに感染している場合に、情報コンセント用ネットワーク内で活動し、情報コンセントに接続している他の端末に感染してしまう恐れがある。このための対策としては、端末群をそれぞれ異なる VLAN に配置することで端末間の直接通信を制限したり、サーバが提供する DHCP の設定を工夫することで端末を異なるネットワークに配置するなどの技術が研究されている。しかし VLAN を用いる方法は、利用する機器が高価になってしまうという問題がある。また DHCP の設定を工夫する方法では、攻撃者が明示的に DHCP に依らないネットワーク設定を施すことで直接攻撃できてしまう可能性がある。

本稿では、同報通信フレームの転送を制限するスイッチを用いて情報コンセントを構築する方法を提案する。同報通信を制限することで、端末間の直接通信は禁止することが可能である。さらに、情報コンセントの提供者ではなくユーザの設定により特定端末間の通信を許可することも可能である。また、提案する手法を既存のスイッチを用いて実現し、その効果を確認する。

2 情報コンセントの運用

情報コンセントを運用する場合、提供者と利用者の双方の安全性について考慮しなければならない。ここでは、脅威を分類し、そのそれぞれに対してどのような方策が採られるのか、さらには、既存の研究でどのように問題が解決されているのかについて述べる。

2.1 脅威の分類

情報コンセントを運用する場合に注意しなければならない点として、以下のものがある。

1. 情報コンセントの提供者に対する安全性
   (a) 情報コンセントの利用者が攻撃活動をしない
   (b) もし攻撃が行われた場合犯人が特定できる
2. 情報コンセントの利用者に対する安全性
   (a) 情報コンセントの外部から攻撃されない
   (b) 情報コンセントの利用者から攻撃されない

情報コンセントから攻撃活動が行われた場合には、情報コンセントの提供者が責任を取らなければならない。そのため、攻撃が行われないように注意する必要があり、万一、攻撃が行われてしまった場合にもどの端末から行われたのかを特定する必要がある。これが 1 に関する問題である。

また、情報コンセントに接続した端末が脅威にさらされるような状態では、安心してシステムを利用することはできない。そのために、情報コンセントに接続した端末に対する攻撃が不可能なシステムを構築する必要がある。これが 2 に関する問題である。

2.2 脅威に対する一般的な対策

項目 1a に関しては、情報コンセントと外部の接続点においてファイアウォールや侵入遮断システムを運用するなどの方策が採られている。しかしこの方策だけで全ての攻撃を防ぐことはできないので、項目 1b が必要となる。攻撃者を特定するためには、認証機構を設けて情報コンセントを利用可能なユーザを制限したり、認証結果のログを保存しておき、ある時点に情報コンセントを利用していたユーザを特定できるようにするなどの方策が採られることが一般的である。さらに、認証結果のログと異なるユーザが不正に利用することがないように、成りすましが行えないような工夫も採られている。既存の研究ではこの点に着目したものが多く、その成果も多数報告されている。

項目 2a に関しては、項目 1a と同様に情報コンセントと外部の接続点においてファイアウォールや侵入遮断システムを運用するなどの方策が採られている。さらに、情報コンセントに接続する機器に対して外部から直接接続する必要性は低いため、情報コンセントを NAPT の配下に設置することで、外部からの直接通信を許さないという運用も多い。この方法では、情報コンセントを構成するネットワークにプライベートアドレスを利用できるため、グローバルアドレスを消費せ

ずに情報コンセントを構築できるという利点もある。一方、項目 2b に関しては、既存の研究では端末間の直接通信を行えないようにすることで対処している。端末間での通信が必要になる場合にはサーバを介した通信を行い、そこでファイアウォールなどを運用することでワームなどが活動できないようにしている。

2.3 関連研究

丸山らは、VLAN 機能を利用して情報コンセントを構築している [1]。端末に対してはすべて異なる VLAN を割り当て、スイッチの 1 つのポートをサーバ用に固定し、さらにそのポートを Multi VLAN に設定する。これにより、サーバは全ての端末と通信が可能だが、端末はサーバ以外の端末と通信できない。また、端末の認証、MAC アドレスの偽造防止なども考慮されている。石橋らも同様にスイッチの VLAN 機能を用いている [2]。新たにアドレスを配布する際には、MAC アドレスと IP アドレスの組を記録する。さらに、スイッチのポートと MAC アドレスの組を記録することで、スイッチのポート、MAC アドレス、IP アドレスの組が正規のものでない偽装したパケットを破棄できる。また、[3] では、暗号化通信路を用いることで同機構を共有メディアである無線 LAN 環境へと応用している。一方、桝田らは、同じく共有メディア上に利用者認証機能を実現するために、PPPoE を用いる方法を提案している [4]。以上の方式は、VLAN などでネットワークを分離し、利用者間の通信を禁止することで情報コンセント内でのセキュリティを維持しようとするものである。このため、互いに信頼している端末間であっても、通信を行うことはできない。

齊藤らは、DHCP により配布するネットワーク情報を工夫することで、同一セグメントであっても異なるネットワークに所属している設定を与える方法を提案している [5]。この方法は、DHCP により配布される情報をクライアントが必ず使用するという前提に立っているため、悪意のユーザによる恣意的な設定を排除できない。

3 提案手法

3.1 注目する脅威

既存の研究の多くは、前にあげた項目 1、つまり、提供者の安全性に着目したものが多い。中でも、成りすましの防止を重点的に扱っている。本論文では、情報コンセントの利用者相互の間で行われる攻撃活動に注目する。近年、ウイルスやワームの開発技術も進歩している。潜伏期間が長かったり、発病しても症状が軽いために容易にはウイルスに感染していると気づかないものもある。ファイアウォールや侵入遮断システムでネットワーク全体を守るというネットワーク型のセキュリティモデルを採用している情報コンセントの場合、ひとたび内部でウイルスが発病して感染活動を開始すると、容易にネットワーク内でウイルスが蔓延してしまうためである。

このための対策は、すでに述べたように VLAN を用いて異なるネットワークに配置する方法がある。我々は、[6] においてさまざまな構成要素を用いてネットワークを構築し、その上での IP アドレスの偽造などの脅威に対する頑強度を調べた。そこでは、VLAN を用いる方法が最も優れていると判定している。この方法は端末間の直接通信が不可能であり、ウイルスの蔓延を防ぐ効果は高い。しかし、VLAN 機能が付いたスイッチは安価になっては来たが、いまだ VLAN 機能のないスイッチと比較して 10 倍ほどの価格差がある。情報コンセントを構築する際に VLAN 機能を必須にすることで、情報コンセントの構築コストがかかってしまうという問題がある。また、VLAN を用いてネットワークを分離するため、お互いに相手を信用しているようなユーザ間でも通信を行うことができないという問題もある。もしこれを行おうとすれば、スイッチの VLAN 設定、もしくは、サーバの設定を変更する必要があり、情報コンセント利用者の権限で行うことができない。

そこで本研究では、他の端末との直接通信を防ぎながら、お互いが信用している端末間の通信を利用者の権限で許可できるようなシステムの構築を目指す。

3.2 TCP/IP での通信シナリオ

本研究で注目したのは、TCP/IP での通信の開始方法である。ここでは、ホスト A がホスト B (IP アドレ

スはIP_B) に通信する場合を見る [7]。

1. ホスト A が自身の ARP テーブルからIP_Bを検索する
2. IP_Bが存在する場合 6 へ分岐
3. IP_Bの MAC アドレスを取得するため、IP_Bを問い合わせる ARP パケットを同報通信
4. ホスト B は自身のアドレスに対する ARP パケットを受信すると、自身の MAC アドレスを用いて ARP に応答
5. ホスト A は ARP 応答からIP_Bに対応する MAC アドレスを取得し、ARP テーブルに登録
6. ホスト A はホスト B の MAC アドレスに対してパケットを送信

我々が注目したのは手順 3 である。ここでは同報通信を用いている点である。同報通信を制限することで、通信相手の MAC アドレスが取得できないことになり、直接通信は行えない。しかし、同報通信が必要になるのは ARP を用いて通信相手の MAC アドレスを取得する際のみであるため、あらかじめ ARP テーブルに通信相手の MAC アドレスを登録しておけば、同報通信は必要ない。

3.3 提案する機器

本論文では、同報通信を制限したイーサネットスイッチを用いて情報コンセントを構築する手法を提案する。同報通信を制限したスイッチには、2 通りのポートが存在する。1 つはサーバを接続するためのポートであり、もう 1 つはクライアントを接続するためのポートである。通常、サーバポートは 1 つで、残りのポートはクライアントポートとする。このとき、サーバポートには何の制限もかけないが、クライアントポートからは同報通信フレームの出力を制限する。具体的には、サーバポートから送られた同報通信フレームは出力するが、クライアントポートから送られた同報通信フレームは出力しない。

この制限をかけた状態での動作は、VLAN を用いてクライアント用のポートを別 VLAN に設定し、サーバポートを全ての VLAN と通信できる Multiple VLAN に設定した場合の同報通信フレームを送信した際の動作と同一の動作となる。しかし、本方式では制限するのは同報通信フレームだけであるため、通常のパケットを送信したときの動作は異なる。通常のパケットには何の制限もかけないため、通常のイーサネットスイッチと同様に、対象となる機器が接続されたポートへ転送される。

```
permit host サーバ MAC アドレス any
deny any host ffff.ffff.ffff
permit any any
```

図 1: クライアントポートに登録すべきアクセスリスト

4 実験

提案する手法が有効に働くことを確認するために実験を行った。しかし、新たなハードウェアを提案しているため、実際に作成して実験することはできなかった。そのため、既存のスイッチに対してアクセスリストを設定することで同様な動作をする機器を作成し、実験を行った。

4.1 実験機器

実験に用いた機器は、Cisco 社製 Catalyst2950T である。この機器では MAC アドレスベースのアクセスリストを登録できる。そのため、クライアントポートの出力フィルタとして、図 1 のようなフィルタを設定すれば、提案するスイッチとほぼ同様な動作をさせることができる。

しかし、ここで問題が 2 つ発生した。1 つは、Catalyst が 1 のような複雑なアクセスリストを許さない点である。これは、ホスト指定の host キーワードと、特に指定しない any キーワードの組み合わせ方に問題があったため、図 2 ようなアクセスリストに変更することで対応した。

もう 1 つの問題は、Catalyst が入力フィルタリングにしか対応していない点である。想定する機能を実現するためには、出力フィルタリング機能が必須となるため、このままでは正しく設定できない。そこで、サーバポートからクライアントポートに到達するためにス

```
permit host サーバ MAC アドレス host ffff.ffff.ffff
deny host クライアント MAC アドレス 1 host ffff.ffff.ffff
deny host クライアント MAC アドレス 2 host ffff.ffff.ffff
    ⋮
permit any any
```

図 2: クライアントポートに登録したアクセスリスト

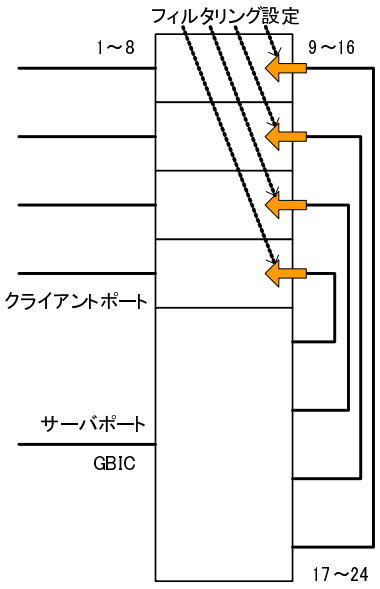

図 3: スイッチの VLAN 構成

イッチを 2 度通る構成とし、2 度目にスイッチに入る段階でフィルタリングを行うことで、出力フィルタリングと同等のフィルタリングを行うようにした (図 3)。

図で 9～16 番ポートの入力フィルタとしてフィルタを設定したため、クライアントを 1～8 番ポートに接続すると、フィルタを経由してパケットが到達することになる。VLAN の設定としては、1 番と 9 番ポート、2 番と 10 番ポート、...8 番と 16 番ポートをそれぞれ 1 つの VLAN に設定し、残った 17 番～24 番ポートとギガビットに対応した 2 ポートを 1 つの VLAN とする。このギガビットに対応したポートがサーバポートとなる。さらに、クロスケーブルを用いて 9 番と 17 番ポート、10 番と 18 番ポート、...16 番と 24 番ポートを直結する。

4.2 実験結果

まず最初に、情報コンセントとして利用可能であることを確認する。このため、サーバポートに DHCP サーバを、クライアントポートに Windows を搭載した PC を接続し、アドレスの取得が可能であることを確認した。DHCP の処理は正しく終了し、クライアントは IP アドレスを取得できた。

端末間でウイルス感染が起こらないことを確認する。このため、2 つのクライアントポートに 2 台の端末を接続し、IP アドレスを指定した通信ができないことを確認した。端末を接続した直後の状態では、ARP テーブルにはサーバのアドレスしか追加されておらず、ARP による MAC アドレスの取得も行えないため、通信は行えなかった。

互いに許可したユーザ同士の通信が可能となることを確認する。このため、2 つのクライアントポートに接続した 2 台の端末に、互いに相手端末の MAC アドレスを登録した状態で、通信が行えることを確認した。ARP テーブルにアドレスを登録することで、ARP による MAC アドレスの取得が不要になり、端末間での直接通信が可能となった。

5 考察

実験の結果は、当初の想定どおり、端末間の通信は拒否しながらも、特定の端末間の通信が可能になった。これは、MAC アドレスの取得が ARP によってのみ可能であるためである。しかし実験としては、非常に簡単な構成においてのみ検査を行っているため、より複雑な構成を用いた大規模な実験や、多種のシステムを接続した際の挙動、さらには、攻撃者の活動を想定し、さまざまな実験を試みる必要がある。

注意しなければならないのは、場合によっては ARP

によらずに別な端末の MAC アドレスを取得できる可能性についてである。たとえば、DHCP サーバがパケットを返答する際に、要求を発した端末の MAC アドレスではなく、ブロードキャストアドレスを用いて返答する可能性がある [8]。この場合、DHCP パケットの中には MAC アドレスが含まれるため、この情報を元に別な端末の MAC アドレスを取得できる可能性がある。さらにこの場合には、IP アドレスも同じパケットに格納されているため、次の攻撃はさらに容易になる。いくつかの DHCP サーバを用いて実験したところ、このような返答を行う DHCP サーバは見つからなかったが、実際に情報コンセントを運用する際には DHCP サーバの返答を確認する必要がある。

一般に、情報コンセントを構築する場合、多数のコンセントを設ける必要がある。その場合に有効なのは、スイッチを多段接続して末端のポート数を増やす方法である。この場合、今回提案しているスイッチでは、下段スイッチのサーバポートを上段スイッチのクライアントポートと接続することで、全体として単一のスイッチを用いた場合と同様な効果が得られる。VLAN を用いてネットワークを分離した場合には、上段スイッチと下段スイッチとでは異なる設定を施す必要がある。しかし本論文で提案するスイッチの場合には、接続するポートさえ間違わなければ良く、特別な設定は不要である。

6 おわりに

本論文では、新たな情報コンセントの構築方法として、同報通信のみを一部制限するイーサネットスイッチを用いて情報コンセント用のセグメントを構築する手法について述べた。本手法では、サーバポートからの同報通信フレームはすべてのポートに中継するが、クライアントポートからの同報通信フレームはサーバポートにのみ中継する。これにより、クライアントが ARP を用いて他のクライアントの MAC アドレスを取得することが困難になり、結果として、クライアント間の直接通信を阻止できる。これは、情報コンセントに限らず、単一セグメント内でのワームの感染が問題となるようなネットワークでも有効である。

今回、いくつかの実験は行ったものの必ずしも十分ではないため、他のさまざまな状況に関して実験を行う必要がある。また、実際にハードウェアとして作成する際に安価に作成できなければ、本システムの価値は半減してしまう。そこで、実際にハードウェアを作成し、作成にかかる費用を見積もったり、実際に作成したハードウェアを用いて実験を行う必要もある。

参考文献

[1] 丸山伸, 浅野善男, 辻斉, 藤井康雄, 中村順一: 既存の DHCP 端末で利用できる利用者にも管理者にも安全な情報コンセントシステムの構築, 情報処理学会分散システム/インターネット運用技術研究会, pp. 131–136 (1999). DSM14-24.

[2] 石橋勇人, 阪本晃, 山井成良, 安倍広多, 大西克実, 松浦敏雄: 情報コンセントにおける認証とアドレス偽造防止を VLAN 機能により実現するシステム LANA2, 情報処理学会分散システム/インターネット運用技術研究会, pp. 137–142 (1999). DSM14-25.

[3] 石橋勇人, 山井成良, 森下英夫, 森俊明, 安倍広多, 松浦敏雄: 無線 LAN における利用者認証機構, 情報処理学会分散システム/インターネット運用技術研究会, pp. 13–18 (2001). DSM21-3.

[4] 桝田秀夫, 鈴木未央, 中西通雄: PPPoE を利用した認証付き情報コンセントの実装と評価, 情報処理学会分散システム/インターネット運用技術研究会, pp. 19–24 (2001). DSM21-4.

[5] 齊藤明紀, 桝田秀夫: DHCP を用いた情報コンセントにおけるウィルス感染を防止する一手法, 情報処理学会分散システム/インターネット運用技術研究会, pp. 19–24 (2004). DSM34-4.

[6] 佐藤淳史, 今泉貴史: 公衆ネットワークにおける利用者保護機構に関する研究, 日本ソフトウェア科学会第 20 回大会講演論文集, ISSN 1348-0901, 日本ソフトウェア科学会 (2003).

[7] Plummer, D. C.: An Ethernet Address Resolution Protocol — or — Converting Network Protocol Addresses (1982). RFC826.

[8] Droms, R.: Dynamic Host Configuration Protocol (1997). RFC2131.