イントラネットにおける
IPv6 検疫ネットワークシステムの提案

横山　恵一†
† 情報セキュリティ大学院大学
情報セキュリティ研究科修士課程 2 年
221-0835 横浜市神奈川区鶴屋町 2-14-1
mgs042510@iisec.ac.jp

田中　英彦‡
‡ 情報セキュリティ大学院大学
情報セキュリティ研究科長　教授
221-0835 横浜市神奈川区鶴屋町 2-14-1
tanaka@iisec.ac.jp

あらまし　IPv6 の近隣探索プロトコル（NDP）に実装される近隣要請やルータ広告の機能を検疫ネットワークシステムに応用することで、クライアント PC を検査・治療・隔離・再接続するための誘導を効果的に行うことができる。さらに、ABK（Address Based Keys）を実装することで、MAC アドレスや IP アドレスを詐称できない仕組みも実現でき、IPv4 による既存の検疫ネットワークシステムよりもセキュアでコストパフォーマンスの高い検疫ネットワークシステムを実現することができる。本稿ではその実現方式について述べる。

A Proposal of IPv6
Quarantine Network System for Intranet

KEIICHI YOKOYAMA†　　HIDEHIKO TANAKA‡
† INSTITUTE of INFORMATION SECURITY
1-14-1, Tsuruyamachi, Kanagawa-ku, Yokohama-shi 221-0835, Japan
mgs042510@iisec.ac.jp
‡ INSTITUTE of INFORMATION SECURITY
1-14-1, Tsuruyamachi, Kanagawa-ku, Yokohama-shi 221-0835, Japan
tanaka@iisec.ac.jp

Abstract　By applying the function of the Neighbor Solitication and Router Advertisement of the IPv6 Neighbor Discovery Protocol to the Quarantine Network System, we can inspect, treat, isolate, and reconnect client PC effectively. In addition, by using ABK(Address Based Keys) , we can protect a network from MAC address and IP address spoofing. As the result, we can make the Quarantine Network System of IPv6 for Intranet securer than that of IPv4

１．はじめに

検疫ネットワークとは、様々なネットワーク製品やアプリケーションを組合わせ、自己のイントラネットをワームや不正アクセス等の様々な脅威から守るソリューションを指す言葉である。このソリューションは、クライアント PC がイントラネットに接続する際に、認証を行ったうえで、ウイルス定義ファイルや OS のパッチが適切な新しいバージョンであるか等を検査し、既定のセキュリティポリシーに対して不適合の場合はこれを隔離・治療し、既定のセキュリティポリシーに適合させてからイントラネットへの接続を許可するというものである。

現在、企業においてはイントラネットが IPv4 によって構築・運用されていることから検疫ネットワークシステムも IPv4 で実装されている。

２．既存の検疫ネットワークシステム

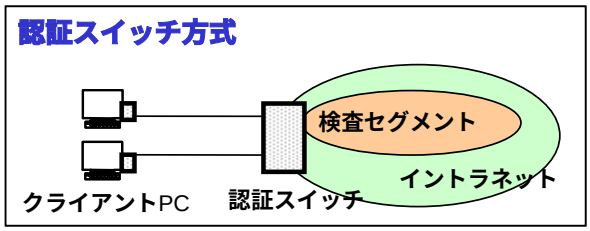
2.1. 検疫ネットワークシステムの動作概要

既存の検疫ネットワークシステムの基本動作

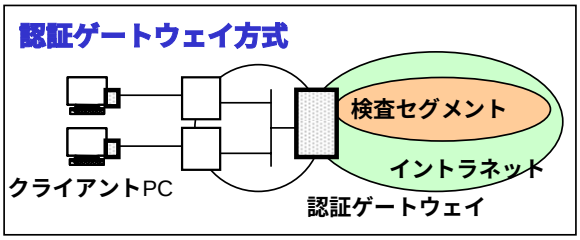
は以下の通りである。
1) クライアント PC をイントラネットに接続
2) 検査を行うセグメントに誘導
3) 検査サーバによる検査
4) 既定のポリシーに反する場合、治療を行うセグメントに誘導
5) パッチあて等、適切な処置を実施
6) 再検査後、再接続

2.2. 検疫ネットワークシステムの様々な方式

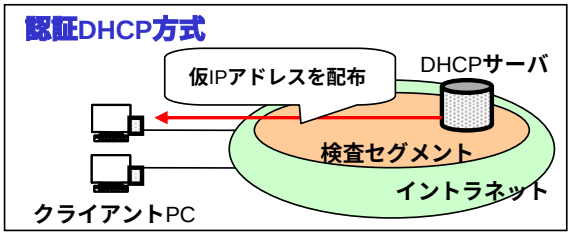
検疫ネットワークシステムは、クライアント PC の検査や治療を行うためのネットワークの切替手法によって以下のように分類される。



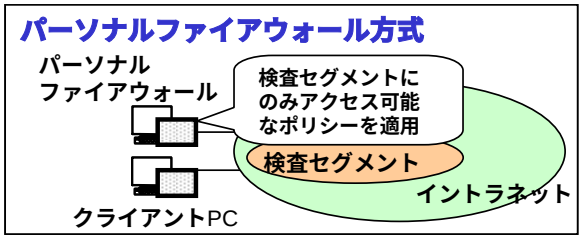
末端のスイッチで IEEE802.1ｘ認証（ユーザまたは機器）と連携して認証・検疫を行うため最も水際での対策が可能となる。末端のスイッチで切替を行うため多くのスイッチの入れ替えが必要となる。



認証ゲートウェイと Web 認証等（ユーザまたは機器）の認証装置を連携させて制御を行う。末端のスイッチに接続されるクライアント間のセキュリティが担保されない。



認証（MAC アドレス）サーバによって許可されたクライアント PC に DHCP サーバからアドレスを割当てて切替を行う方式。MAC アドレスを詐称されたり、IP アドレスを固定で付与された場合、アクセス制御できないという脅威がある。



パーソナルファイアウォールのポリシーを切替えてアクセス制御を行う。パーソナルファイアウォールがインストールされていないクライアント PC は何も処理されず接続されてしまうという脅威がある。

2.3. 既存の検疫ネットワークシステムの課題

2.2. では堅牢な検疫ネットワークシステムを構築するためには、認証スイッチ方式しかないことを述べたが非常にコストが高くつく。認証ゲートウェイ方式やパーソナルファイアウォール方式は根本的に技術的な改善の余地がない。

しかし、認証 DHCP 方式において MAC アドレスの詐称を防止でき、IP アドレスが固定で付与された場合のアクセス制御ができれば、コストパフォーマンスの高い理想的な検疫ネットワークシステムのモデルを実現することができる。

また、認証ゲートウェイ方式と認証 DHCP 方式の場合、検査前のクライアント PC が検査を行うセグメント内で互いにワーム等の感染を広げる脅威が存在する。しかし、認証 DHCP 方式の場合、割当てる IP アドレスのサブネットマスクを（255.255.255.252）で行い、検査時にクライアント PC を 1 台ずつネットワーク的に閉じ込める方法で回避できる。

以上の理由により、既存の認証 DHCP 方式をベースにアドレスマネージメントが洗練されている IPv6 による検疫ネットワークについて検討することとした。

3．IPv6 の特徴とセキュリティ

3.1. IPv6 近隣探索プロトコル（NDP）

IPv6 には、IPv4 におけるアドレスを解決するプロトコル（ARP）の代わりに近隣探索プロトコルが実装されている。近隣探索プロトコルの主な機能は以下の４つである。ここで「ノード」はホストとルータの両方を指す。NDP 通信はリンクローカルアドレスという同一セグメン

ト内でのみ有効なアドレスで通信を行う。

・近隣要請（Neighbor Solitication）
ノードが MAC アドレスの問合わせ、到達可能かどうかの確認、重複アドレス検出のために送信するパケット。

・近隣広告（Neighbor Advertisement）
ノードが近隣要請への応答として返すパケット。

・ルータ要請（Router Solitication）
ホストがリンク内のルータを探索するためにルータへ送信するパケット。

・ルータ広告（Router Advertisement）
ルータがホストに自分の存在を知らせるために送信するパケット。アドレス自動生成、経路設定、通信パラメータ設定に必要な情報が含まれる。

3.2. インタフェースの有効化

IPv6 の IP アドレス設定は、DHCP サーバがなくてもノード自ら自動で設定することができる。これをステートレスアドレス自動設定という[※1]。この場合、ノードは自己にアドレスを付与する前に以下のようなメッセージの形式でマルチキャスト通信を行い、当該アドレスを使用しているノードが他にないか「重複アドレス検出」を行う。重複アドレスが検出されなかった場合、ノードは初めてインタフェースを有効化し当該アドレスが使用できるようになる。

・送信元アドレス
::（未指定アドレス）

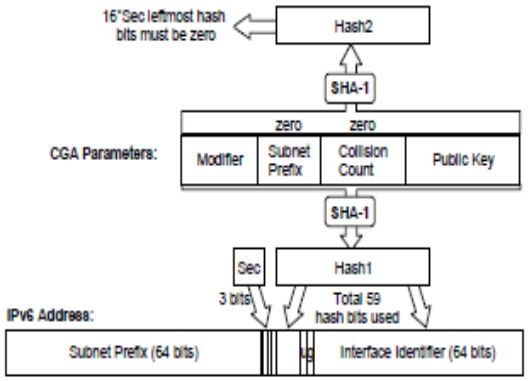
・宛先アドレス
重複アドレス検出したいリンクローカルアドレスに対する要請ノードマルチキャストアドレス

・タイプ=135

・ターゲットアドレス
重複検出したいアドレス

IPv4 の場合、IP アドレスを設定しさえすれば何もチェックを行わずに当該アドレスを利用できる。このことが IPv4 による検疫ネットワークシステムの脆弱点となっている。

3.3. SEND（SEcure Neighbor Discovery）



IPv4 よりも洗練された仕様の IPv6 であるが、近隣探索プロトコル（NDP）において指摘されている脆弱性が存在する[※2]。攻撃者が特定のノードになりすまして近隣広告（NA）を行うことで要求者に対して誤ったアドレス解決を行わせたり、ルータ広告（RA）を偽ってノードの保持する IP アドレスを無効にしたりすることができてしまうのである。これを阻止するために SEND[※3] が提唱されている。

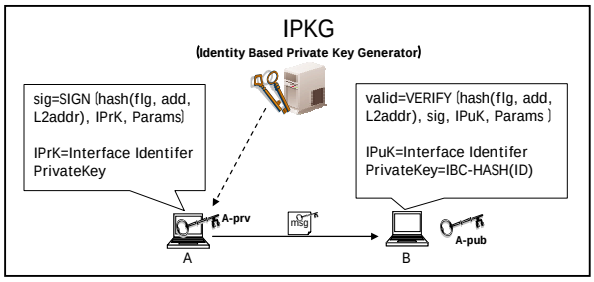
SEND は CGA（Criptgraphically Generated Address）[※4] という公開鍵等のハッシュ値をインタフェース ID として生成した IP アドレスをソースアドレスとし、パケットに署名をつけて送信することで、当該アドレスが生成したパケットであることを受け取ったノードが検証することができる仕組みである。

この方法は、PKI のような認証基盤を必要としないという利点がある。しかし、誰でも公開鍵と秘密鍵のペアを作れることから、あくまでも受け取ったパケットが当該アドレスを持つノードから送られたものであることが検証可能なだけであり、自己の管理するネットワークへ当該ノードが接続することを制御（禁止）できる技術ではない。また、CGA の暗号強度は、IP アドレスに埋め込む関係上、56bit が限界値である。CGA では、ハッシュ拡張の仕組みを提案しているが十分な長さであるとは言えない。

3.4. ABK（Address Based Keys）[※5]

ID ベース暗号方式の考え方において、ID を IP アドレスとし、アルゴリズムに楕円曲線暗号方式を適用する方法である。IPKG（Identity Based Private Key Generator）が、各ノードの

IP アドレスから秘密鍵と公開鍵のペアを作成



して配布する。暗号パラメータは公開されているため、上図においてクライアント B はクライアント A の真正性の検証のために IPKG にその都度、問い合わせる必要はない。IPKG が許可するノードのすべての鍵を管理しているため、自己の管理するネットワークへ接続許可するノードのコントロールが可能である。このことから、IPv6 による検疫ネットワークシステムの要素技術として、SEND よりも好ましいと言える。また、楕円曲線暗号を利用するため、SEND に比べて高速な処理が可能であるという利点がある。

4．IPv6 検疫ネットワークシステムの構成法

4.1. 認証 DHCP 方式における IP アドレス固定付与による検査すり抜けに対する対策

3.2.で述べたように、IPv6 では IP アドレスを設定したインタフェースを有効にする前に、ターゲットアドレスに当該アドレスをセットして、要請ノードマルチキャストアドレス宛に重複アドレス検知のための通信を行う。このとき、同じセグメントに認証サーバを設置し、サーバのネットワークカードを Promiscus mode にすることにより、この要請ノードマルチキャストを Listen することができる。

ここで、認証サーバ上にイントラネットに参加することを許可する IPv6 リンクローカルアドレスと MAC アドレスのペアをリストとして登録しておき、リストにないターゲットアドレスがセットされていることを検出したとき、認証サーバを重複アドレス検出に応答させることで、当該不正ノードをイントラネットから排除することができる。登録リストは、MAC アドレスをもとに生成されるステートレスな IP アドレスと MAC アドレスのペアに限定することで、手動で IP アドレスが設定された場合に対する脅威に対してもセキュリティを強化することができる。

4.2. MAC アドレスおよび IP アドレス詐称に対する対策

IPv4 における MAC アドレスの詐称は、Windows の場合、レジストリの編集やツールを使って簡単に行うことができる。これは、IPv6 の場合も同様で、Windows においてレジストリを編集して MAC アドレスを書換え、アドレス自動設定を行うと、編集した MAC アドレスから生成された IP アドレスが設定される。

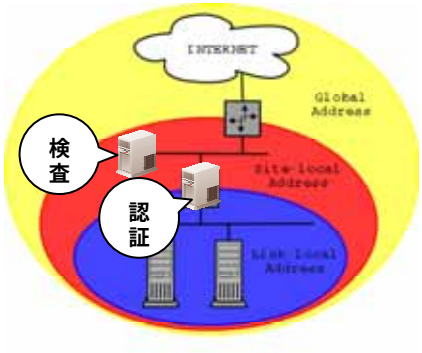
これについての対策は、3.3.SEND または 3.4.ABK という IPv6 独自の技術で対応できることが期待される。

下表は、SEND と ABK の特徴をまとめたものである。SEND は、受け取ったパケットが当該アドレスを持つノードから送られたものであることが検証可能なだけであり、自己の管理するネットワークへ当該ノードが接続することを制御（禁止）できる技術ではない。ABK の方がネットワーク全体として複雑な構成となるが、管理者が認めたクライアント PC のみイントラネットへの接続を許可する検疫ネットワークシステムの考え方に適していると言える。また、SEND は、重複アドレス検知やルータ要請（RS）を行う際、ソースアドレスが未指定アドレス（::）となるため、この場合の送信元の検証ができないという課題がある。

もともと SEND は ABK をもとにして考えられた仕様であり、イントラネットのクライアント同士の認証には PKI 基盤を必要としないが、インターネット上の経路交換を行うルータの信頼性を検証するためには、ABK の IPKG のように PKI 基盤を構築すべきだとしている。インターネットがすべて IPv6 に移行したと仮定した場合、PKI 基盤のクライアント証明書のように鍵を CA から配布する SEND が IPv6 検疫ネットワークシステムの基盤技術になる可能性はあると考えられる。

	SEND (Secure Neighbor Discovery)	ABK (Address Based Keys)
IPアドレスと鍵の関係	公開鍵のHashをインタフェースIDとして使う	公開鍵を生成するためにインタフェースIDまたはPrefixを使う
鍵の生成	ノード自身に公開鍵と秘密鍵のペアを生成させる	IPKG(Identity Based Key Generator)によって公開鍵と秘密鍵のペアを提供される
各ノードの設定	何も設定する必要がない	暗号パラメータを事前に共有しておく必要あり
認証基盤	ABKのような認証基盤が全く必要ない	IPKGが必要 IPKGは各ノードの秘密鍵を生成するMaster秘密鍵を持つ

4.3. 検査セグメント内におけるクライアント PC 間の感染防止策



IPv6 のアドレス種類と有効範囲

2.3.で述べたが、既存の検疫ネットワークシステムでは、クライアント PC がイントラネットに接続された場合、検査が行われる前に同一セグメントに同時に複数台、接続されるため、クライアント PC 間のワーム等の感染が発生する脅威がある。IPv6 の同一セグメント内の通信のみ可能なリンクローカルアドレスの場合、（/64）でステートレスに割当てられるが、既存の方式と同様の脅威が存在する。

サイトローカルアドレスや今後明確に定義されるであろうユニークローカルアドレス、またはグローバルアドレスの場合、サブネットを自由に変更することができる。そこで、本検疫ネットワークモデルでは、リンクローカルアドレスは、近隣探索プロトコル通信にのみ使用することとし、通常の通信では他のアドレス体系を利用するフィルタをクライアント PC に設定することを提案する。これによりワーム等に感染したクライアント PC がイントラネットに接続されたとしても蔓延することを防ぐことができる。

4.4. IPv6 による検疫用アドレスの割当て

IPv6 では 3.1.で述べたルータ広告の機能によって、クライアント PC に対するアドレス割当てを柔軟に行うことができる。

例えば、検査後一定時間経過すれば再接続して再検査しなければならないよう IP アドレスの LifeTime を予め設定したり、特定のクライアントがワーム等に感染した場合、他の仕組みでこれを検知し、LifeTime をゼロにセットした当該ノードのリンクローカルアドレス以外のアドレスを無効にするルータ広告パケットを投げてコントロールすることもできる。

IPv4 の場合、一度割当てた IP アドレスをサーバ側から無効にすることは不可能であったが、IPv6 の場合はこれが可能となる。検疫ネットワークシステムにおいては、このような柔軟なアドレスのマネージメントが必要であることから、IPv6 は IPv4 よりも検疫ネットワークシステムに適しているということが言える。

4.5. IPv6 検疫ネットワークシステムの動作

以下の前提条件でクライアント PC がイントラネットに接続されるまでの流れを説明する。

前提条件

・ネットワークは IPv6 のみで構成される

・認証サーバ（IPKG）

1 次認証；クライアント MAC アドレスおよびその MAC アドレスから生成された Interface-ID をもつリンクローカルアドレスを認証する機能を持つ。

2 次認証；Interface-ID から生成したクライアントの秘密鍵と公開鍵のペア。

・クライアント

IPv6 を実装しステートレス（自動）でリンクローカルアドレスを構成され、認証サーバ（IPKG）から配布される秘密鍵と公開鍵のペアを持つ。NDP（近隣広告）通信のみリンクローカルアドレスで通信するフィルタを設定する。

1. クライアント PC をイントラネットに接続
2. 認証サーバにて MAC アドレスおよび MAC アドレスから自動生成されたリンクローカルアドレスであることを確認

3-1.(OK)リンクローカルアドレスを有効化
近隣探索プロトコルのみ通信可

3-2.(NG)重複アドレス検知の応答パケットを認証サーバから受取りイントラネットから排除される

4.クライアント PC は認証サーバに通信用のアドレスを付与してもらうためルータ要請（RS）を行う

5. 認証サーバはクライアント PC の署名されたパケットを検証する

6-1.(OK)認証サーバはルータ広告（RA）を行い個々のクライアントを切り離すため(/127)でアドレスをアサインする

6-2.(NG) イントラネットから排除される

7. 認証サーバ経由で検査サーバへアクセス

8-1.(OK)認証サーバからルータ広告（RA）を受取り（/127）を (/64) に変更し通常の通信

を行う
8-2.(NG)治療サーバへアクセス後、再接続
ここで、5.（2 次認証）で署名検証するのであれば、2.（1 次認証）は不要であると考えられるかもしれないが、鍵を持っていない複数のノードがイントラネットに接続された場合、それらノード間でワーム等が広がりイントラネットのリソースを消費する脅威があることを考えると 1 次認証は必要である。

５．評価

5.1. 脆弱性の評価
1) MAC アドレスを詐称された場合
クライアント PC の MAC アドレスを認証サーバに登録されたものに詐称しイントラネットに接続された場合、IP アドレスを自動生成していれば、1 次認証をすり抜けることができる。しかしながら、2 次認証では鍵をもっていないと許可されないため、2 次認証で排除される。
2) IP アドレスを詐称された場合
1) と同様、認証サーバに登録された MAC アドレスとそれから自動生成される IP アドレスに詐称された場合、1 次認証は抜けられるが 2 次認証で排除される。
3) 秘密鍵が漏洩した場合
秘密鍵が第３者に漏洩し、その秘密鍵を使ってイントラネットに接続が行われた場合、1 次認証で必要な IP アドレスと MAC アドレスが正しければ 2 次認証までクリアされ接続されてしまう。ただし、正規のクライアント PC が既に接続されている場合は、IPv6 の重複アドレス検知機能により第３者はインタフェースを有効化することができない。本攻撃に対する根本的な解決は、定期的な鍵交換の仕組みと秘密鍵が漏洩した場合の鍵の無効化であるが、その仕組みについては本稿の範囲外とし今後検討を行うこととする。

5.2. 本検疫システム実現性の評価
以上のように検疫ネットワークシステムを IPv6 で構成することは、不正なクライアントをイントラネットに接続させないだけでなく、接続させた後に感染した場合にイントラネットから切り離すという柔軟なアドレスマネージメントが可能になるという利点がある。
本検疫ネットワークモデルは、IPv6 の基礎技術や RFC、インターネットドラフトの仕様を組合わせることで、IPv6 でしか実現できないモデルである。企業のイントラネットにおける IPv6 の導入はまだ進んでいないが、NAT-PT※6 に代表されるように IPv4/v6 アドレス変換技術を用いれば、IPv6 検疫ネットワークシステムの構築は現段階で実現可能である。この場合、クライアント PC が接続される末端のセグメントは IPv6 で制御し、基幹ネットワークやサーバに関しては、IPv4 または IPv4/v6 デユアルで構成することになる。

６.結論

本稿では、イントラネットの検疫システムを IPv6 で構成することにより IPv4 で構成するよりもより安全なシステムが実現できることを示した。

《参考文献》

※1 RFC2461 Neighbor Discovery for IP Version 6 (IPv6)
T.Narten(IBM), E.Nordmark(SunMicrosystems)
W. Simpson(Daydreamer), December 1998
RFC2462 IPv6 Stateless Address Autoconfiguration
S. Thomson(Bellcore), T. Narten(IBM), December 1998

※2 RFC3756 IPv6 Neighbor Discovery (ND) Trust Models and Threats P. Nikander, Ed.(Ericsson Research Nomadic Lab), J. Kempf(DoCoMo USA Labs), E. Nordmark(Sun Microsystems Laboratories), May 2004

※3 RFC3971 SEcure Neighbor Discovery (SEND)
J.Arkko, Ed.(Ericsson), B.Zill(Microsoft).
J.Kempf (DoCoMo Communications Labs USA),
P. Nikander(Ericsson), March 2005

※4 RFC3972 Cryptographically Generated Addresses (CGA)
T. Aura(Microsoft Research), March 2005

※5 Internet Draft draft-kempf-abk-nd-00
Securing IPv6 Neighbor Discovery Using Address Based Keys (ABKs)
James Kempf, Craig Gentry, Alice, Silverberg
May 2003

※6 RFC:2766 Network Address Translation - Protocol Translation (NAT-PT) G.Tsirtsis(BT)
P.Srisuresh(Campio Communications), February 2000