動的VLAN制御による統合ワーム対策システムの提案

馬場達也[†] 角将高[†]
藤本浩[†] 稲田勉[†]

近年，Blaster や Sasser，Netsky などの，ワームによる被害が大きな問題となっている．これらのワームの被害を防ぐ技術の 1 つに，クライアント PC をイントラネットに接続する際に，ウイルス対策ソフトの動作状況やパッチの適用状況をチェックする「検疫システム」がある．しかし，クライアント PC に，検疫システム側で対応しているウイルス対策ソフトをインストールしておかなければならないという制約や，パッチを適用するとすでにインストールされているアプリケーションが動作しなくなるなどの影響が出てしまうという問題がある．本論文では，クライアント PC にこれらの対策がされていない場合でも，ワーム感染チェック，ワーム駆除，ワーム感染防御，トラフィック監視によるワーム検知，ワーム隔離などの機能をネットワーク側で提供する統合ワーム対策システムを提案する．

A Proposal of an Integrated Worm Countermeasure System Based on Dynamic VLAN Control

Tatsuya Baba,[†] Masataka Kado,[†] Hiroshi Fujimoto[†] and Tsutomu Inada[†]

Recently, infection of Internet worms such as “Blaster”, “Sasser”, and “Netsky” are becoming a serious problem. To prevent damage from these worms, there are “quarantine systems” that check the installed anti-virus software and the applied security patches on the client PCs when they are connected to the enterprise network. They have some problems, however, such that it is necessary to install certain anti-virus software supported by the quarantine system, and some application programs do not work after certain patch is applied. In this paper, we propose an integrated worm countermeasure system which has functionalities such as scan, extermination, protection, detection, and isolation on network side without depending on client software.

1. はじめに

近年，システムに感染するワームの被害が増加している[1)]．ワームは，システムの脆弱性を悪用し，自動的に侵入して感染を広めるもの（本論文では，「脆弱性悪用型ネットワークワーム」と呼ぶ）と，ワームプログラムを添付したメールを送信して感染を広めるもの（本論文では，「マスメーリングワーム」と呼ぶ）の 2 種類に大別される．脆弱性悪用型ネットワークワームの例としては，Blaster，Welchia，Sasser，Zotob などがある．また，マスメーリングワームの例としては，Sobig，Netsky，Beagle，Mydoom などがある．

これらのワームによる被害を防ぐためには，企業のイントラネットにワームが侵入することを防ぐことが重要である．イントラネットへのワームの侵入経路は，**図 1** に示すものがあると考えられる．

インターネット経由で侵入する脆弱性悪用型ネットワークワームに対しては，インターネットとイントラネットの境界にファイアウォールや IPS（Intrusion Prevention System：侵入防止システム）を導入することが効果的である．また，インターネット経由で侵入するマスメーリングワームに対しては，イントラネット上のメールサーバにゲートウェイ型ウイルス対策ソフトを導入することが効果的である．しかし，最近は，外部でワームに感染したノート PC などを，有線 LAN や無線 LAN，リモートアクセス VPN などでイントラネットに接続することによって感染が広まる，いわゆる「持ち込み PC」からの感染が問題となっている．

現在，この持ち込み PC からの感染を防ぐ技術として，「検疫システム」がベンダ各社からリリースされて

† 株式会社 NTT データ
NTT DATA CORPORATION

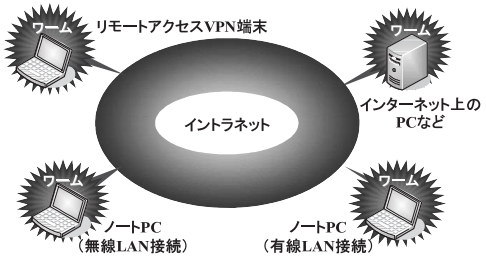

図 1 イントラネットへのワームの侵入経路
Fig. 1 Intrusion path of Internet worms to the Intranet.

いる．現在の多くの検疫システムでは，イントラネットへの接続時にクライアント PC をチェックし，ウイルス対策ソフトのウイルス定義ファイルが最新かどうか，最新のパッチが適用されているかどうかをチェックする．そして，これらのチェックの結果が不十分であった場合には，ネットワークへの接続を許可しないというアプローチをとっている．これにより，ユーザにウイルス定義ファイルのアップデートやパッチの適用を徹底させることができ，ワームの感染の拡大を防止することが可能となる．さらに，このような検疫システムでは，ウイルス定義ファイルに登録されている既知のワームしか対処できないことから，トラフィック監視による未知ワーム検知機能を組み合わせた方式も提案されている[2)]．

しかし，これらの方式では，クライアント PC に，検疫システム側で対応しているウイルス対策ソフトをインストールしておかなければイントラネットに接続できないという制約がある．このため，ゲストが持ち込んだ PC を，一時的にイントラネットへ接続させたい場合などに，検疫システムが対応していないウイルス対策ソフトを使用している場合は接続することができない．また，パッチを適用すると，動作しなくなるアプリケーションが存在するという問題もある．このようなアプリケーションを使用しているクライアント PC には，問題が発生するパッチを適用することができないため，イントラネットへの接続が許可されないことになる．

さらに，市販の IPS 製品をセグメント境界に設置し，脆弱性を狙った攻撃を遮断することによってワーム感染を防ぐという方法も考えられる．しかし，ワームは，同一セグメント内に存在する PC を狙う場合も多く，この場合は，ワームの感染トラフィックがセグメント境界に設置した IPS を通過しないため，検知することができないという問題がある．

2. ネットワーク側での防御アプローチ

そこで，著者らは，従来，クライアント PC 上で行っていた対策と同等の機能をネットワーク側で提供するアプローチを提案する．

2.1 ウイルス対策ソフト非導入 PC への対処

クライアント PC に特定のウイルス対策ソフトが導入されていない場合でも，ワーム感染チェックを行うことができるように，ネットワーク側で用意した機能を使用してワーム感染チェックを行う．具体的には，クライアント PC が ActiveX コントロールをチェック用のサーバからダウンロードすることによって，ネットワーク接続時にワーム感染チェックおよび駆除を行うようにする．

しかし，ネットワーク接続時に通常のウイルス対策ソフトのようなディスクの完全スキャンを行うと非常に時間がかかってしまうため，利用に支障が出るという問題がある．そこで，頻繁に再起動を行うクライアント PC を狙うワームは，OS を再起動した場合でも，ワームプログラムが自動的に起動されるような設定を登録するという性質に着目し，クライアント PC の OS の自動起動設定の内容と，あらかじめ定義したワームの自動起動設定の内容とを比較することで，ワーム感染の有無を判定する．

2.2 パッチ未適用 PC への対処

パッチが適用できないクライアント PC をワーム感染から防御するために，クライアント PC に存在する脆弱性を狙ったアクセスをネットワーク側で遮断する機能を提供する．この機能により，パッチが適用できないクライアント PC を保護することが可能となるだけでなく，脆弱性情報が入手できた時点から保護することが可能となるため，脆弱性発見後，早い時期に出現する新種のワームからも防御することが可能となる．

2.3 新種のワームへの対処

ネットワーク接続時のワーム感染チェックでは，前述したように，システムに登録されているワームの情報をもとに感染をチェックし，駆除を行う．このため，システムに登録されていない新種のワームは，ワーム感染チェックでは検知することができない．そこで，トラフィックを監視し，ワームの振舞いをもとに検知するワームセンサをネットワーク上に配置することで，ワーム感染チェックで検知できなかった新種のワームの検知と感染トラフィックの遮断を行う．また，従来では対応することが難しかった，セグメント内の PC を狙った場合にも検知できるようにする．

3. 提案方式

以下に，著者らの提案するネットワーク側での防御方式について述べる．

3.1 処理概要

本方式では，**図 2** のように，「ワーム感染チェック/ワーム駆除」，「脆弱性チェック/ワーム感染防御」，「ワーム検知/隔離」などの対策をネットワーク側で統合的に提供することによって，クライアント PC のセキュリティ対策状態によらずにワーム感染に対する多段防御を実現する．

クライアント PC をイントラネットに接続すると，最初にユーザ認証が行われる（図 2①，②）．ユーザ認証に成功すると，通常の業務ネットワークとは隔離された検疫ネットワークに接続される．

そして，検疫ネットワークに設置されている統合セキュリティマネージャより，ワーム感染チェックを受ける（図 2③）．ワーム感染チェックの結果，ワームに感染していると判断された場合にはワームが駆除される（図 2④）．

次に，クライアント PC の脆弱性がチェックされる（図 2⑤）．脆弱性が存在すると判断された場合には，ネットワーク側で脆弱性を保護しながら，業務ネットワークに接続させることで，業務ネットワークにワームが侵入してしまった場合でも，感染の被害にあわないようにする（図 2⑥，⑦）．脆弱性が存在しないと判断された場合には，ワームの攻撃を受けても感染しないため，直接業務ネットワークに接続される．

業務ネットワークにワームが侵入した場合は，ワームセンサが振舞いをもとにワームを検知し，ワーム感染 PC からのワーム感染トラフィックを遮断することによって，業務ネットワークから隔離する（図 2⑧，⑨）．そして，ネットワーク管理者が，ワームを駆除できたと判断したら，手動でネットワークに接続させる（図 2⑩）．

以上の仕組みを組み合わせることにより，本システムは，既知のワームの感染チェックおよび駆除，既知の脆弱性を狙う新種の脆弱性悪用型ネットワークワームからの防御，未知の脆弱性を狙う新種の脆弱性悪用型ネットワークワームおよび新種のマスメーリングワームの検知・隔離の機能を統合的に提供することができ，既知/未知を含めたワームの感染被害から適切な段階でイントラネットを防御することが可能となる．

3.2 ネットワークエンドでのアクセス制御方式

ネットワーク側でのクライアント PC の脆弱性保護機能は，クライアント PC を接続するエンドスイッチに，レイヤ 4 レベルでのアクセス制御が可能なレイヤ 2 スイッチを使用し，リモートから脆弱性を悪用する際に使用されるポート宛のパケットをそのエンドスイッチで遮断することで実現することが可能である．しかし，Cisco 社の Catalyst 2950 など，一部のレイヤ 2 スイッチではレイヤ 4 レベルでのアクセス制御機能を搭載しているものの，現状では，このようなアクセス制御機能が搭載されているスイッチは非常に少ないという問題がある．

このため，本方式では，レイヤ 4 レベルでのアクセス制御機能が搭載されているスイッチを使用していない場合は，セグメントごとにファイアウォールを設置し，VLAN（Virtual Local Area Network）機能[3] を応用することで，ファイアウォールを強制的に通過させるようにして，レイヤ 4 レベルでのアクセス制御を実現する．

図 3 に本方式の物理構成と論理構成を示す．ブリッジとして動作するファイアウォール（以降，ブリッジファイアウォールと呼ぶ）を，VLAN 対応レイヤ 2 スイッチにトランクモードで接続する．さらに，ブリッジファイアウォール上では，各 VLAN 間をブリッジ

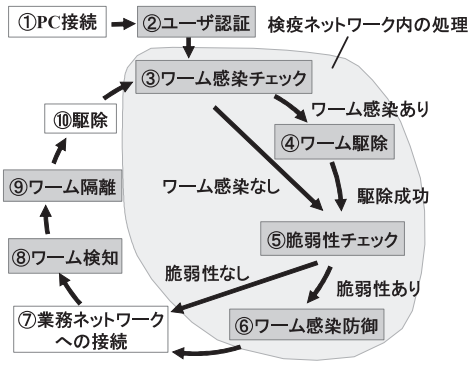

図 2 提案方式の対処サイクル
Fig. 2 Process cycle of the proposed system.

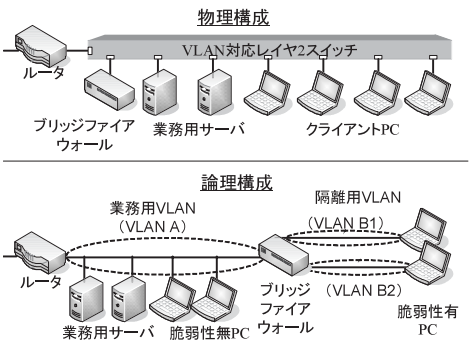

図 3 ブリッジファイアウォールの仕組み
Fig. 3 Mechanism of the bridge firewall.

接続するように設定する．

次に，脆弱性の存在するクライアント PC が接続されているスイッチのポートに対して，それぞれユニークな VLAN ID（VLAN B1, B2...）を設定する（これらを隔離用 VLAN と呼ぶ）．こうすることで，図 3 の論理構成図で示すように，脆弱性が存在するクライアント PC がネットワーク経由でアクセスする場合は，必ずブリッジファイアウォールを経由して行われるようになる．そして，このブリッジファイアウォールにおいて，それぞれのクライアント PC の脆弱性を狙ったアクセスを遮断するフィルタを記述することで，ワームなどの攻撃から脆弱性の存在するクライアント PC を防御することが可能となる．脆弱性が存在しないクライアント PC については，接続されているスイッチのポートの VLAN 設定を，業務ネットワークを構成する業務用 VLAN（VLAN A）に設定することで，ブリッジファイアウォールを経由せずにイントラネットに直接アクセスできるようにする．これにより，脆弱性が存在しないクライアント PC はブリッジファイアウォールを通過せずに通常どおりアクセスするため，ブリッジファイアウォールに余分な負荷がかかることを防ぐことが可能となる．

4. システム構成

提案方式を実現するシステムの構成を**図 4** に示す．本システムでは，業務ネットワークを構成する業務用 VLAN と検疫ネットワークを構成する検疫用 VLAN を用意し，これらの間はレイヤ 2 レベルで通信を制限する．検疫用 VLAN には，クライアント PC のチェックや，VLAN およびフィルタリングの設定を動的に制御する統合セキュリティマネージャと，クライアント PC 接続時の認証を行う RADIUS（Remote Authentication Dial In User Service）サーバ，クライアント PC のチェックで検知できなかった新種のワームが侵入した場合に備えて，トラフィックの振舞いをもとにワームを検知するワームセンサを設置する．また，ワームセンサのもう一方のインタフェースを VLAN 対応レイヤ 2 スイッチのアップリンクを流れるトラフィックをキャプチャできるように接続し，セグメント外との通信を監視できるように設定する．さらに，ブリッジファイアウォールを VLAN 対応レイヤ 2 スイッチにトランクモードで接続する．

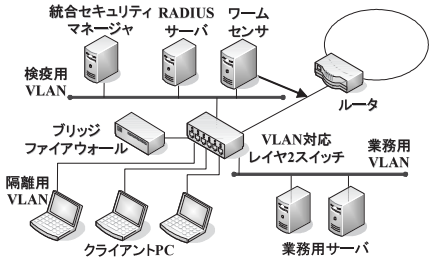

図 4 システム構成
Fig. 4 System configuration.

初期設定では，ネットワークに接続されたクライアント PC を，ブリッジファイアウォールを経由して接続させるために，クライアント PC が接続されるスイッチのポートを隔離用 VLAN に設定しておく．

5. 処理詳細

5.1 ユーザ認証処理（接続検知処理）

統合セキュリティマネージャでは，クライアント PC がネットワークに接続されたことを検知し，接続されたスイッチとそのポートの情報を取得する必要がある．

クライアント PC がネットワークに接続されたことを検知する方法としては，レイヤ 2 スイッチから送信される SNMP（Simple Network Management Protocol）リンクアップトラップメッセージ，クライアント PC からの DHCP（Dynamic Host Configuration Protocol）リクエストメッセージ[4]，IEEE 802.1X 認証[5] 時に送信される RADIUS リクエストメッセージ[6] などを契機とする方法が考えられる．

本システムでは，新たに接続されたクライアント PC からのアクセスを検疫用 VLAN のみに制限するためのフィルタを，クライアント PC がネットワークにアクセス可能となる前に設定しておく必要がある．このため，クライアント PC が実際にネットワークに接続される前に，RADIUS メッセージからフィルタ設定に必要なクライアント PC の情報を取得することが可能な IEEE 802.1X 認証を利用する．

具体的には，統合セキュリティマネージャに RADIUS プロキシ機能を持たせ，IEEE 802.1X 認証時のレイヤ 2 スイッチと RADIUS サーバとの間の RADIUS 認証を，統合セキュリティマネージャを経由して行う．これにより，統合セキュリティマネージャは，RADIUS 認証中に，RADIUS リクエストメッセージの内容をチェックすることができるようになり，クライアント PC の MAC アドレス，接続先スイッチの IP アドレス，接続先スイッチポートの情報を取得することができるようになる．そして，該当クライアント PC が検疫用 VLAN とのみ通信が可能となるように，ブリッジファイアウォールのフィルタ設定を行う．統合セキュリティマネージャは，このフィルタ設定が完了するまでは，RADIUS サーバからの認証完了メッ

セージをレイヤ 2 スイッチへ転送しないように制御することで，認証完了後に業務用 VLAN に接続されることを防ぐ．

ブリッジファイアウォールでのフィルタリングは，MAC アドレスベースで行う．MAC アドレスは詐称することが可能であるが，多くのレイヤ 2 スイッチでは，IEEE 802.1X 認証を行ったポートからのアクセスを，認証を行った MAC アドレス以外は許可しないように設定することが可能であり，MAC アドレスの詐称を防ぐことが可能となる．

5.2 ワーム感染チェック/ワーム駆除処理

認証完了後，ユーザは，統合セキュリティマネージャに対して Internet Explorer を使用してアクセスし，チェック用 ActiveX コントロールをダウンロードして，ワーム感染チェックを行う．

チェック用 ActiveX コントロールは，クライアント PC の自動起動設定の内容を統合セキュリティマネージャに送信し，統合セキュリティマネージャが保持する既知のワームの自動起動設定が記述されたワーム定義ファイルの内容と比較する．もし，ワームに感染していると判断された場合には，自動的に駆除用 ActiveX コントロールをダウンロードさせ，ワームを駆除する．

5.3 脆弱性チェック処理

ワーム感染チェックが完了すると，次に脆弱性チェックを行う．脆弱性チェックの方法としては，Nessus[7] に代表されるような，外部からネットワーク経由でチェックを行うツールによる方法と，チェック用プログラムをクライアント PC にダウンロードさせて，内部から脆弱性をチェックする方法の 2 通りが考えられる．

しかし，著者らが Nessus を用いて行った実験では，1 台のクライアント PC をチェックするために 1 分程度の時間がかかってしまうことが分かった．これに対して，チェック用プログラムをダウンロードさせて内部からチェックする方法では，適用されているパッチを調べればよいだけであるため，チェック時間が非常に短くて済むという利点がある．本システムでは，クライアント PC をイントラネットに接続するたびにチェックを行わなければならないため，チェック時間が短いことが要件となる．このため，チェック用プログラムを使用して内部からチェックする方式を採用することにした．

内部からチェックを行う方法としては，マイクロソフト社の MBSA（Microsoft Baseline Security Analyzer）を使用する方法が提案されている[2]．しかし，この方法では，MBSA をチェック対象のクライアント PC にあらかじめインストールしておかなければならないという問題がある．また，MBSA を利用してリモートからチェックを行うことも可能であるが，この場合は，チェック対象のクライアント PC で MBSA が利用するプロトコルを通すように Windows ファイアウォールやパーソナルファイアウォールの設定を変更しなければならないという問題がある．このため，本システムでは，チェック用 ActiveX コントロールが，クライアント PC に適用されているパッチをチェックし，そのリストを統合セキュリティマネージャに送信する．そして，統合セキュリティマネージャ上に登録されている最新のパッチリストと比較することで脆弱性の有無をチェックする．パッチリストには，パッチが適用されていない場合に，その脆弱性を悪用するために使用されるポート（以降，脆弱ポートと呼ぶ）の情報も記述されている．

5.4 ワーム感染防御処理

クライアント PC に脆弱性が存在した場合には，該当クライアント PC の脆弱ポートへのアクセスをフィルタリングするようにブリッジファイアウォールの設定を行うことで，ワームの感染から防御する．また，脆弱性が存在しないクライアント PC が接続されているスイッチポートには，業務用 VLAN と同じ VLAN ID を設定し，ブリッジファイアウォールを経由せずに業務用 VLAN に接続させる．

5.5 ワーム検知/隔離処理

本システムのワームセンサでは，脆弱性悪用型ネットワークワームおよびマスメーリングワームの両方に対して，新種のワームも含めて検知するために，文献 8) および 9) に記述されている手法を用いる．具体的には，セグメント境界で，脆弱性悪用型ネットワークワームが感染先を探すために行う水平ポートスキャンと，マスメーリングワームが送信先メールサーバを探すために行う DNS への MX レコードの問合せを監視することにより，ワーム感染行為を検知する．

しかし，脆弱性悪用型ネットワークワームは，同一セグメント内の PC を感染先候補として選択する場合が多く，この場合は，ポートスキャンのトラフィックがセグメント境界を流れないため，観測することができない．このため，ワームがポートスキャンを行う際に，同一セグメント内のアドレスに対してポートスキャンを多く行った場合には，一連のポートスキャンの一部しか観測することができず，水平ポートスキャンを検知することが難しくなるという問題がある．この問題を解決する方法として，セグメント内でブロードキャストされる，未使用 IP アドレスに対する ARP リク

エストの増加からセグメント内のワーム感染を検知する手法が提案されている[10]．しかし，この手法では，未使用 IP アドレスを事前に学習しておく必要があり，本システムが対象としているような，外部からクライアント PC が持ち込まれ，ネットワーク構成が頻繁に変更される環境には適さない．そこで，本システムでは，DHCP と連携することによって，未使用 IP アドレスをリアルタイムで把握する．さらに，未使用 IP アドレスへの ARP リクエストが発生した場合には，ワームセンサの MAC アドレスを含んだ ARP リプライを送信し，ワームセンサ自身にトラフィックを誘導することで，未使用 IP アドレスに対する水平ポートスキャンをワームセンサ上で観測できるようにする．これにより，セグメント境界で観測される，セグメント外のアドレスに対するポートスキャントラフィックに加えて，同一セグメント内の未使用 IP アドレスに対するポートスキャントラフィックをワームセンサ上で観測することができるようになり，同一セグメント内のアドレスに対してポートスキャンを行うようなワームも検知することが可能となる．

脆弱性悪用型ネットワークワームを検知した場合には，ワーム感染 PC を隔離用 VLAN に移動させ，ブリッジファイアウォールでワーム感染トラフィックを遮断するように設定する．また，マスメーリングワームを検知した場合は，ワームメールの送信を遮断するために，25/TCP をブリッジファイアウォールで遮断するように設定する．

5.6 切断検知処理

統合セキュリティマネージャは，クライアント PC がネットワークから切断されたことを検知し，該当クライアント PC に関するフィルタ設定を解除するようにブリッジファイアウォールに指示する．また，次のクライアント PC の接続に備えて，スイッチの該当ポートを隔離用 VLAN に設定する．切断検知には，レイヤ 2 スイッチから送信される SNMP リンクダウントラップメッセージを用いる．

6. プロトタイプの実装

提案した方式の有効性を検証するため，本方式をプロトタイプとして実装した．

6.1 ブリッジファイアウォール

ブリッジファイアウォールに必要となる次の機能を実装した．

(1) **VLAN 間ブリッジング機能**

VLAN 間ブリッジング機能は，標準の Linux カーネルが持つ VLAN 機能とブリッジ機能を組み合わせることにより実現した．

(2) **フィルタリング機能**

フィルタリング機能には，MAC アドレスベースのフィルタリングが可能な ebtables[11] を使用した．

(3) **フィルタリング変更機能**

統合セキュリティマネージャからの指示を受信して，フィルタ設定を行うための機能を実装した．具体的には，設定する ebtables のコマンドを含んだメッセージを統合セキュリティマネージャから受信し，ebtables に反映した後，その結果を統合セキュリティマネージャに返答するように実装した．統合セキュリティマネージャとブリッジファイアウォールとの間は，UDP 上の独自プロトコルを使用して通信するように実装した．

6.2 統合セキュリティマネージャ

統合セキュリティマネージャに必要な次の機能を実装した．

(1) **フィルタリング変更指示機能**

ユーザ認証処理（端末検知処理），ワーム感染防御処理，ワーム検知/隔離処理，切断検知処理で統合セキュリティマネージャに必要となる，ブリッジファイアウォールに対するフィルタリング変更指示機能を実装した．具体的には，ebtables のコマンドに変換したフィルタの内容を含んだメッセージを，UDP 上の独自プロトコルを使用してブリッジファイアウォールに送信するように実装した．

(2) **VLAN 制御機能**

ワーム感染防御処理，ワーム検知/隔離処理，切断検知処理で統合セキュリティマネージャに必要となる VLAN 制御機能を実装した．

具体的には，SNMP を使用して，標準の Q-Bridge MIB[12] および Cisco 社の Enterprise MIB を用いるスイッチの VLAN 設定を，業務用 VLAN または隔離用 VLAN に動的に変更する機能を実装した．

(3) **端末検知機能**

ユーザ認証処理（端末検知処理）で統合セキュリティマネージャに必要となる機能を実装した．

RADIUS プロキシ機能は，FreeRADIUS[13] の RADIUS プロキシ機能を利用し，IEEE 802.1X 認証時に送信される RADIUS リクエストメッセージ中の Calling-Station-Id，NAS-IP-Address，NAS-Port 属性から，クライアント PC の MAC アドレス，接続先スイッチの IP アドレス，接続先スイッチポートの情報を取得する機能を実装した．そして，検疫用 VLAN 以外とは通信できないようにするために，IEEE 802.1X 認証が完了する前までに，フィルタリング変更機能を使用して，ブリッジファイアウォールに次のフィルタを設

定するようにした（例は，検疫用 VLAN ID を 100，クライアント PC の MAC アドレスを 01:23:45:67:89:ab とした場合の ebtables のコマンド）．

1. 検疫用 VLAN からのアクセスは許可
   例）ebtables -A FORWARD -i eth0.100 -j ACCEPT
2. 検疫用 VLAN へのアクセスは許可
   例）ebtables -A FORWARD -o eth0.100 -j ACCEPT
3. クライアント PC からのアクセスを遮断
   例）ebtables -A FORWARD -s 01:23:45:67:89:ab -j DROP
4. クライアント PC へのアクセスを遮断
   例）ebtables -A FORWARD -d 01:23:45:67:89:ab -j DROP

上記の 1. および 2. のフィルタはあらかじめブリッジファイアウォールに設定されており，3. および 4. のフィルタをクライアント PC 接続時に設定する．

(4) **ワーム感染チェック/ワーム駆除機能**

ワーム感染チェック/ワーム駆除処理で統合セキュリティマネージャに必要となる機能を実装した．

ワーム感染チェック，ワーム駆除を行うためのプログラムは，それぞれ ActiveX コントロールとして実装し，Apache [14] で構築した Web サーバにアクセスすることにより実行できるようにした．ワーム感染チェック用の ActiveX コントロールでは，自動起動設定として，クライアント PC のレジストリの Run/RunOnce エントリおよびスタートアップフォルダの内容を取得して統合セキュリティマネージャに送信するように実装した．そして，統合セキュリティマネージャでは，ワーム定義ファイルの内容と比較し，自動起動設定が一致したものが存在した場合には，ワームに感染していると判断するようにした．そして，ワームが検知された場合には，ワームプロセスを停止し，ワームプログラムを削除する．そして，ワームが設定した自動起動設定を解除することで駆除完了とした．

(5) **脆弱性チェック機能/ワーム感染防御機能**

脆弱性チェック処理およびワーム感染防御処理で統合セキュリティマネージャに必要となる機能を実装した．

クライアント PC に適用されているパッチのリストを取得するプログラムを，ActiveX コントロールとして実装し，パッチのリストは，レジストリの HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Updates キーから取得するようにした．そして，ワーム感染チェック/ワーム駆除処理が完了した後に，脆弱性チェック用の ActiveX コントロールが自動的に実行されるように実装した．そして，統合セキュリティマネージャのパッチリストファイルに，あらかじめ適用されるべきパッチとともに，脆弱ポートを登録しておき，未適用パッチが存在した場合には，該当脆弱ポートへのアクセスを，フィルタリング機能を使用して，ブリッジファイアウォールで遮断するように設定するようにした．また，未適用パッチが存在しなかった場合には，VLAN 変更機能を使用して，クライアント PC が接続されているスイッチポートの VLAN 設定を業務用 VLAN に変更するように実装した．

(6) **ワーム隔離機能**

ワーム検知/隔離処理で統合セキュリティマネージャに必要となる機能を実装した．

具体的には，ワームセンサからワーム感染 PC からのワーム使用ポートの遮断の指示を受信した後，VLAN 変更機能およびフィルタリング変更機能により，該当 PC が接続されているスイッチポートを，端末接続検知機能により得た情報から特定し，その VLAN 設定を VLAN 制御機能により，隔離用 VLAN に変更する．そして，フィルタリング変更機能により，ブリッジファイアウォールで該当トラフィックを遮断するように設定する機能を実装した．統合セキュリティマネージャとワームセンサとの間は，TCP 上の独自プロトコルで通信するように実装した．

(7) **切断検知機能**

切断検知処理で統合セキュリティマネージャに必要となる機能を実装した．

具体的には，スイッチから SNMP リンクダウントラップメッセージを受信した場合に，VLAN 制御機能により，リンクダウンしたポートの VLAN 設定を隔離用 VLAN に設定し，そのポートに接続されていたクライアント PC のフィルタ設定を，フィルタリング変更機能を使用して解除する機能を実装した．

6.3 ワームセンサ

ワーム検知/隔離処理でワームセンサに必要となる機能を実装した．

(1) **ワーム検知機能**

DHCP サーバとして ISC DHCP [15] を使用し，DHCP で割り当てていない IP アドレスに対して ARP 要求が発生した場合に，ワームセンサの MAC アドレスを返答する機能を実装した．そして，スイッチのアップリンクを流れるトラフィックと，ワームセンサ宛のトラフィックを監視してワームの検知を行う機能を実装した．

(2) **ワーム感染 PC 隔離機能**

ワーム検知機能によりワームが検知された場合は，

統合セキュリティマネージャに，ワームが感染に使用しているポート（脆弱性悪用型ネットワークワームの場合は水平ポートスキャンに使用されたポート，マスメーリングワームの場合は 25/TCP）宛のアクセスの遮断を指示する機能を実装した．統合セキュリティマネージャとワームセンサとの間は，TCP 上の独自プロトコルで通信するように実装した．

7. 評　　価

作成したプロトタイプを使用して，検知性能に関する評価を行った．

7.1 評価項目

本システムでは，ワーム感染チェック/ワーム駆除，脆弱性チェック/ワーム感染防御，ワーム検知/隔離といった，一連のワーム対処機能によって，多段防御を実現している．そこで，それぞれの機能によって，次のことを確認することによって，統合システムとしての有効性を評価する．

(1) システムに自動起動設定を登録したワームが，ワーム感染チェック処理において検知でき，さらに，検知したワームをワーム駆除処理において駆除できること

(2) 脆弱性チェック処理において，クライアント PC の脆弱ポートが検出できること．さらに，ワーム感染チェック/ワーム駆除機能で対処できない，既知の脆弱性を悪用する新種のワームが侵入した場合に備えて，検出された脆弱ポートへのアクセスをネットワーク側のブリッジファイアウォールで遮断し，その脆弱性を攻撃するワームの感染から防御できること

(3) ワーム感染チェック/ワーム駆除機能や脆弱性チェック/ワーム感染防御機能でも対処できない，未知の脆弱性を悪用する新種のワームなどが侵入した場合を想定し，ワームセンサで検知できること．さらに，ワーム感染 PC からのワーム感染トラフィックをブリッジファイアウォールで遮断し，ワーム感染被害を広めないようにすること

7.2 評価環境

評価用ネットワークの構成は，図 4 と同様である．VLAN 対応レイヤ 2 スイッチとして，Cisco Catalyst 2950T-24 を使用し，統合セキュリティマネージャ，RADIUS サーバ，ブリッジファイアウォール，ワームセンサを 1 台ずつ設置した．サーバ類はすべて**表 1** のスペックの PC 上で動作させ，統合セキュリティマネージャ，RADIUS サーバ，ワームセンサは 100Base-TX，ブリッジファイアウォールは 1000Base-T で VLAN 対応レイヤ 2 スイッチに接続した．なお，Cisco Catalyst 2950T-24 には，レイヤ 4 レベルでのアクセス制御機能が搭載されているが，今回の評価ではこの機能は使用せず，ブリッジファイアウォールでアクセス制御を行うこととした．

表 1 プロトタイプ実装環境
Table 1 Specification of the prototype system.

OS	Linux（Fedora Core 3）
CPU	Pentium 4 3GHz
メモリ	1GB DDR-SDRAM
ネットワークカード	Intel Pro/1000MT

表 2 登録済み脆弱性情報
Table 2 Registered vulnerability information.

脆弱性 ID	パッチ ID	パッチリリース日
MS01-059	315000	2001/12/21
MS02-006	314147	2002/02/13
MS03-001	810833	2003/01/23
MS03-043	828035	2004/09/06
MS04-011	835732	2004/04/14
MS04-012	828741	2004/04/14
MS04-031	841533	2004/10/13

統合セキュリティマネージャには，ワーム感染チェック用に，1,500 種類のワーム（亜種を含む）の情報と，2005 年 2 月 1 日時点で公開されている，外部からの攻撃に悪用される可能性のある Windows 2000 および Windows XP の脆弱性情報（**表 2**）を脆弱ポートとともに登録しておいた．

クライアント PC の OS には Windows XP を使用し，2002 年 4 月 10 日までのパッチのみを適用した「パッチ未適用 PC」と，2005 年 2 月 1 日時点での最新のパッチを適用した「パッチ適用済み PC」の 2 種類を用意した．クライアント PC では，IEEE 802.1X サプリカントとして Funk Software 社の Odyssey Client を使用し，認証方式として EAP/MD5-Challenge を選択した．なお，クライアント PC のレジストリの Run/RunOnce エントリおよびスタートアップフォルダには，計 12 の自動起動設定がすでに記述されていた．

ワームセンサでは，5 秒以内に同じクライアント PC から 30 以上の宛先に対して水平ポートスキャンが行われた場合に，脆弱性悪用型ネットワークワームに感染しているとして検知するように設定した．また，DNS サーバに対して，5 秒以内に同じクライアント PC から 3 ドメイン以上の MX レコードを問い合わせた場合に，マスメーリングワームに感染しているとして検知するように設定した．

7.3 評価方法

脆弱性悪用型ネットワークワームである Blaster.C, Sasser.C，マスメーリングワームである Sobig.F, Beagle.X，Netsky.Z のそれぞれをクライアント PC に感染させ，本システムのワーム感染チェック/ワーム駆除，脆弱性チェック/ワーム感染防御，ワーム検知/隔離において適切に対処できるかどうかを確認した．

また，Blaster.C に感染したパッチ未適用 PC と，ワームに感染していないパッチ適用済み PC を本システムに接続した場合の処理時間を測定した．さらに，接続後のクライアント PC を Blaster.C に感染させた場合に，ワームセンサがワーム感染を検知してから，実際にワームトラフィックが遮断されるまでの時間についても測定した．処理時間は 10 回ずつ測定し，その平均を求めた．なお，チェック用 ActiveX コントロールおよび駆除用 ActiveX コントロールは，すでにダウンロードが完了している状態で測定を行った．

7.4 評価結果

7.4.1 ワームへの対処機能

(1) **ワーム感染チェックおよび駆除結果**

本システムのワーム感染チェックおよび駆除処理における対処結果は，**表 3** のようになった．これらのワームに関する情報は，ワーム定義ファイルにあらかじめ登録されていたため，すべてのワームが検知され，正常に駆除された．

(2) **脆弱性チェックおよびワーム感染防御結果**

Blaster.C が悪用する脆弱性を修正するパッチ（MS03-026）や Sasser.C が悪用する脆弱性を修正するパッチ（MS04-011）などが適用されていないパッチ未適用 PC では，これらのワームが感染に使用するポートを含む計 8 つの脆弱ポートが発見された．そして，該当クライアント PC のこれらの脆弱ポートへのアクセスが，ブリッジファイアウォールで遮断されるように設定され，他のクライアント PC からの該当脆弱ポートに対するアクセスが遮断されることを確認した．

(3) **ワームセンサによる検知および隔離結果**

表 4 に示すように，接続後のクライアント PC を Blaster.C および Sasser.C に感染させた場合に，ワームセンサによって，該当クライアント PC が脆弱性悪用型ネットワークワームに感染していることが検知された．そして，ワーム感染に使用されるポートがブリッジファイアウォールで遮断されるように設定され，ワーム感染 PC からの感染トラフィックが遮断されることを確認した．また，Sobig.F，Beagle.X，Netsky.Z に感染させた場合には，ワームセンサによって，該当クライアント PC がマスメーリングワームに感染していることが検知された．そして，25/TCP がブリッジファイアウォールで遮断されるように適切に設定され，ワーム感染 PC からのメールトラフィックが遮断されることを確認した．

表 3 ワーム感染チェックおよび駆除結果
Table 3 Results of worm infection check and worm extermination.

ワーム	ワーム感染チェック	ワーム駆除
Blaster.C	○	○
Sasser.C	○	○
Sobig.F	○	○
Beagle.X	○	○
Netsky.Z	○	○

7.4.2 処理性能

Blaster.C に感染したパッチ未適用 PC およびワームに感染していないパッチ適用済み PC をスイッチに接続してから業務用 VLAN に接続されるまでの各処理における平均処理時間は，それぞれ**表 5** のとおりであった．パッチ未適用 PC の場合の業務用 VLAN 接続処理時間は，検疫用 VLAN 接続処理で追加した 2 つのフィルタの解除と 8 つの脆弱ポートを保護するためのフィルタ設定にかかった時間である．また，パッチ適用済み PC の場合の業務用 VLAN 接続処理時間は，業務用 VLAN に直接接続するための VLAN 設定変更，および，変更後の再認証にかかった時間である．業務用 VLAN に接続されるまでの時間は長くても 3 秒以内であり，十分許容できる範囲であると考えられる．

また，ワームセンサで Blaster.C の感染活動を検知した後に，ワームトラフィックが遮断されるまでの時

表 4 ワームセンサにおける検知結果
Table 4 Detection results of worm sensor.

ワーム	検知結果	遮断ポート
Blaster.C	○	135/TCP
Sasser.C	○	445/TCP
Sobig.F	○	25/TCP
Beagle.X	○	25/TCP
Netsky.Z	○	25/TCP

表 5 平均処理時間
Table 5 Average processing time.

処理	パッチ未適用 ワーム感染有	パッチ適用済 ワーム感染無
接続認証/検疫用 VLAN 接続処理	0.33 秒	0.28 秒
ワーム感染チェック	0.96 秒	0.55 秒
ワーム駆除処理	0.88 秒	
脆弱性チェック	0.46 秒	0.37 秒
業務用 VLAN 接続処理	0.24 秒	0.41 秒
計	2.87 秒	1.61 秒

間は，平均で 0.18 秒であった．これは，ワームトラフィックを遮断するためのフィルタを設定する時間と，隔離 VLAN への設定変更にかかった時間である．これにより，ワームが感染活動を始めてからわずかな時間でワームトラフィックが遮断されることが確認できた．

7.5 誤検知に関する評価

実際のワームを使用した評価とは別に，通常利用時の誤検知の評価を実施した．

(1) **ワーム感染チェックおよび脆弱性チェック**

2005 年 7 月 4 日から 2005 年 10 月 7 日の約 3 カ月間，業務で使用している Windows 2000 マシン 4 台，Windows XP マシン 56 台により，それぞれ 294 回，1,738 回のワーム感染チェックおよび脆弱性チェックを行った．なお，検証期間中にリリースされた MS05-036，MS05-039，MS05-045 の 3 つの脆弱性情報については，表 2 の脆弱性情報に加えて，パッチリリース日にシステムに追加登録して検証を実施した．

その結果，検証期間中に，ワーム感染チェックにおいて，正常なアプリケーションがワームであるとして誤検知されることはなかった．また，脆弱性チェックの結果，30 台のクライアント PC による延べ 75 回のチェックにおいてパッチ未適用と判断されたが，実際にパッチを適用しているクライアント PC が未適用と判断されることはなかった．

(2) **ワームセンサ**

実際のワームを用いて行った評価と同じ閾値を使用して，Windows XP マシンで，Web アクセスやメールの送受信，Microsoft Outlook による予定表の閲覧，Windows ファイル共有，リモートプリンタへの印刷などの通常の業務を 3 日間（操作時間は 8 時間/日）行った．その結果，ワームセンサによる誤検知は発生しなかった．

8. 考　　察

8.1 本システムの適用範囲

今回の評価によって，ネットワーク接続時のワーム感染チェック，ワーム駆除，脆弱性チェック，ワーム感染防御，そして，トラフィック監視によるワーム検知およびワーム隔離の各処理が，高速に，そして，正確に行われることを確認することができた．本システムの各機能によって，対処可能なワームの種類を**表 6** に示す．

本システムのワーム感染チェックおよびワーム駆除機能では，自動起動設定を行うワームであれば検知および駆除を行うことが可能であるが，システムに登録された既知のワームしか検知することができない．このため，新種のワームはワーム感染チェックで検知されずにイントラネット内に侵入してしまう可能性がある．ただし，今回の評価によって，新種のワームであっても，それがシステムに登録された脆弱性を狙う脆弱性悪用型ネットワークワームであれば，本システムのワーム感染防御機能によって，感染の拡大を防ぐことが可能であることが確認できた．

表 6 本システムにおいて対処可能なワーム
Table 6 Internet worms that can be handled by the proposed system.

ワームの種類＼機能		ワーム感染チェック/駆除	ワーム感染防御	ワーム検知/隔離
脆弱性悪用型ネットワークワーム	既知	○（注 1）	○	○
	未知	×	△（注 2）	○
マスメーリングワーム	既知	○（注 1）	×	○
	未知	×	×	○
その他のワーム	既知	○（注 1）	×	×
	未知	×	×	×

注 1）自動起動設定を行うもの
注 2）既知の脆弱性を悪用するものであれば可

そして，システムに登録されていない脆弱性を狙う新種の脆弱性悪用型ネットワークワームや，新種のマスメーリングワームであった場合は，ワーム感染チェック/ワーム駆除機能や，脆弱性チェック/ワーム感染防御機能では防ぐことができないが，水平ポートスキャンや DNS への MX レコードの問合せを行うものであれば，ワームセンサによって検知され，ワームトラフィックを遮断することができることが確認できた．以上のことから，提案方式によって，既知/未知の脆弱性悪用型ネットワークワームおよびマスメーリングワームを早期の段階で対応できることが示された．

また，本方式では，P2P ファイル交換ソフトウェアの機能などを利用して感染を広めるようなワームについても，既知のものであればワーム感染チェック/ワーム駆除機能により対処することが可能である．しかし，このようなワームは，P2P ファイル交換ソフトウェアの機能を利用して感染を広めるため，ワーム感染チェックで検知できなかった場合に，ワーム感染防御機能やワームセンサのようなトラフィック監視機能によって対処することは難しい．このようなワームの感染を防ぐには，企業のイントラネット内では P2P ファイル交換ソフトウェアの利用を禁止し，接続時のチェックで P2P ファイル交換ソフトがインストールされている場合には接続させないなどの対策を行う必

要がある．

8.2 ワーム感染チェックの妥当性

OS 起動時に自動起動するように設定を行うワームであれば，ウイルス対策ソフトがインストールされていない状態でも，本システムのワーム感染チェックによって，高速に検知および駆除を行うことが可能であることを示すことができた．ワームには CodeRed や SQLSlammer などのように，自動起動設定を行わないものも存在するが，これらは再起動を頻繁に行わないサーバをターゲットとしたものである．しかし，OS の再起動を頻繁に行うクライアント PC をターゲットとしているワームは，自動起動設定が不可欠である．本システムでは，クライアント PC をチェック対象としており，今後出現するワームに対しても十分対応できると考えられる．

ただし，ワームの中には，レジストリの HKEY_LOCAL_MACHINE/System/CurrentControlSet/Services キーにエントリを追加することにより，Windows のサービスとして自動起動するものが存在することも判明した．今回作成したプロトタイプでは，クライアント PC のレジストリの Run/RunOnce エントリおよびスタートアップフォルダの内容のみを自動起動設定としてチェックしていたため，検知することができないが，チェック対象のレジストリエントリを追加することで対処することが可能となる．

また，今回の評価では誤検知は存在しなかったが，もし，ワームと同じ自動起動設定を行う正常なアプリケーションが存在した場合には，ワームとして誤検知してしまうことが予想される．これを回避するためには，自動起動設定のチェックに加えて，起動されるプログラムを従来のウイルス対策ソフトと同様にウイルス定義ファイルを使用する方式などでチェックすることにより，そのプログラムがワームであるのか，正常なアプリケーションであるのかの判別をすることで対応できると考えられる．

8.3 ワームセンサの検知方式の妥当性

今回の評価では，ワームセンサにおいて，5 秒以内に同じクライアント PC から 30 以上の宛先に対して水平ポートスキャンが行われた場合に，脆弱性悪用型ネットワークワームに感染しているとして検知するように設定した．また，同様に，DNS サーバに対して，5 秒以内に同じクライアント PC から 3 ドメイン以上の MX レコードを問い合わせた場合に，マスメーリングワームに感染しているとして検知するように設定した．評価の結果，Blaster.C がスキャン開始から 2 秒で 40 アドレス，Sasser.C がスキャン開始から 2 秒で 309 アドレスに対してポートスキャンを行い，ともに設定した閾値を超えていたため，脆弱性悪用型ネットワークワームとして検知することができた．また，Sobig.F がスキャン開始から 2 秒で 10 アドレス，Beagle.X がスキャン開始から 2 秒で 15 アドレス，Netsky.Z がスキャン開始から 2 秒で 4 アドレスに対して MX スキャンを行い，こちらもすべて設定した閾値を超えていたため，マスメーリングワームとして検知することができた．今後出現する脆弱性悪用型ネットワークワームやマスメーリングワームについても，適切な閾値を設定することで，同様に検知することが可能であると期待できる．

また，今回の 3 日間にわたる誤検知の評価では，同じ閾値を設定しても誤検知は発生しなかった．文献 16) では，タブブラウザを使用した場合に水平ポートスキャンが発生したとして誤検知される問題が指摘されているが，今回の評価環境では，プロキシサーバ経由で Web アクセスを行っていたため，すべての Web アクセスがプロキシ宛となり，水平ポートスキャンとして検知されなかった．しかし，誤検知の有無は閾値の高低や適用先のネットワークの状態で変わるものであり，今後，適切な閾値に関する評価を行う必要があると考える．

また，マスメーリングワームには，送信先メールサーバを探索するために，DNS の MX レコードではなく，A レコードを問い合わせるものや，レジストリに記述されたメールサーバ経由で送信するものも存在する．この場合には，現在のワームセンサでは検知することができない．今後，アルゴリズムを追加して，このようなワームにも対応できるようにする必要がある．

8.4 アプリケーションの利用への影響

今回の評価では，パッチ未適用 PC において，135/tcp，135/udp，137/udp，138/udp，139/tcp，445/tcp，445/udp，593/tcp の 8 つの脆弱ポートが発見され，脆弱ポートへの外部からのアクセスが遮断されるように設定された．この場合，Web アクセスやメールの送受信は通常どおり行うことが可能であることが確認できたが，利用環境によっては，Windows のファイル共有やプリンタ共有などが利用できない可能性がある．このような場合には，ブリッジファイアウォールにおいて，WINS サーバやドメインコントローラからの必要なプロトコルをあらかじめ許可するように設定しておく必要がある．

8.5 無線 LAN 接続への適用

これまでは，有線 LAN 接続の場合を例に説明して

きたが，本システムは，無線 LAN 接続の場合にも適用することが可能である．

ただし，有線 LAN 接続の場合と異なり，いくつかの制約がある．1 つは，現状の無線 LAN のアクセスポイントでは，有線 LAN スイッチと異なり，クライアント PC ごとに異なる VLAN ID を設定することが難しいということがある．このため，無線 LAN 接続されたすべてのクライアント PC を，脆弱性の有無にかかわらず，必ずブリッジファイアウォールを経由してアクセスするように設定する必要がある．

また，無線 LAN 接続の場合は，電波状況の悪化などにより頻繁に瞬断が発生することがある．この場合，再接続後に再びチェックを行う必要があり，利用者に大きな負担がかかってしまうという問題がある．また，利用者がネットワーク経由でファイルを修正していた場合などにファイルが壊れるなどの問題も発生する可能性がある．このため，クライアント PC 接続時に，該当するクライアント PC の MAC アドレスが無線 LAN アクセスポイントの ARP テーブルに残っていた場合は瞬断が発生したと判断し，接続時のチェックをバイパスするなどの対処を行う必要がある．

9. むすびに

イントラネットに接続したクライアント PC のワーム感染チェック，脆弱性チェック，トラフィック監視によるワーム検知の結果から，ネットワーク機器の VLAN およびファイアウォールのフィルタ設定を動的に制御することによって，ワーム感染による被害から防御する統合対策システムを提案した．そして，プロトタイプを作成し，実際のワームを使用したワーム対処機能や，処理性能，誤検知の評価を行い，本システムの有効性を示した．

参考文献

1) コンピュータウイルスの届出状況［2005 年 10 月分］について，独立行政法人情報処理推進機構セキュリティセンター (2005). http://www.ipa.go.jp/security/txt/2005/documents/virus-full0511.pdf
2) 武仲正彦，面　和成，東角芳樹，鳥居　悟：ワーム検知隔離と連携したエンドポイントセキュリティシステムの試作，2005 年暗号と情報セキュリティシンポジウム予稿集，Vol.IV of IV, pp.1723–1728 (2005).
3) IEEE Standards for Local and Metropolitan Area Networks—Virtual Bridged Local Area Networks, IEEE Std 802.1Q, 2003 Edition, Institute of Electrical and Electronics Engineers, Inc. (2003).
4) Dynamic Host Configuration Protocol, RFC 2131, Internet Engineering Task Force (1997).
5) IEEE Standards for Local and Metropolitan Area Networks—Port-Based Network Access Control, IEEE Std 802.1X-2004, Institute of Electrical and Electronics Engineers, Inc. (2004).
6) Remote Authentication Dial In User Service (RADIUS), RFC 2138, Internet Engineering Task Force (1997).
7) The Nessus Project. http://www.nessus.org/
8) 日本国特許庁：不正アクセス阻止方法，装置及びシステム並びにプログラム，公開特許公報，特開 2005-252808 (2005).
9) Whyte, D., van Oorschot, P.C. and Kranakis, E.: Addressing Malicious SMTP-based Mass-Mailing Activity Within an Enterprise Network, Carleton University, School of Computer Science, Technical Report TR-05-06 (2005).
10) Whyte, D., van Oorschot, P.C. and Kranakis, E.: Detecting Intra-Enterprise Scanning Worms Based on Address Resolution, *Proc. 21st Annual Computer Security Applications Conference* (*ACSAC 2005*), pp.371–380 (2005).
11) ebtables. http://ebtables.sourceforge.net/
12) Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions, RFC 2674, Internet Engineering Task Force (1999).
13) The FreeRADIUS Project. http://www.freeradius.org/
14) The Apache Software Foundation. http://www.apache.org/
15) Internet Systems Consortium, Inc. http://www.isc.org/
16) 東角芳樹，面　和成，鳥居　悟：ワームのランダムスキャンによる検知の改良方式の提案，コンピュータセキュリティシンポジウム 2005 (CSS2005) 論文集，Vol.I of II, 情報処理学会シンポジウムシリーズ，Vol.2005, No.13, pp.175–181 (2005).

(平成 17 年 11 月 25 日受付)
(平成 18 年 6 月 1 日採録)

馬場 達也（正会員）

平成 7 年慶應義塾大学理工学部電気工学科卒業．同年 NTT データ通信株式会社（現，株式会社 NTT データ）入社．以来，同社技術開発本部にてネットワークセキュリティに関する研究に従事．著書に『マスタリング IPsec』（オライリー・ジャパン）がある．IEEE 会員．

角 将高

平成 15 年日本大学大学院工学研究科情報工学専攻博士前期課程修了．同年株式会社 NTT データ入社．以来，同社技術開発本部にてネットワークセキュリティに関する研究に従事．電子情報通信学会会員．

藤本 浩

平成 3 年東北工業大学通信工学科卒業．同年 NTT データ通信株式会社（現，株式会社 NTT データ）入社．同社技術開発本部にてネットワークセキュリティに関する研究に従事．現在，同社ビジネスソリューション事業本部勤務．

稲田 勉（正会員）

昭和 59 年東北大学大学院工学研究科電気通信工学専攻博士前期課程修了．同年日本電信電話公社（現 NTT）入社．音声応答認識装置，OCR，通信処理装置の開発に従事．昭和 63 年より NTT データ通信株式会社（現，株式会社 NTT データ）．同社技術開発本部にてネットワークセキュリティに関する研究に従事．現在，同社第二公共システム事業本部勤務．