

不正接続PCの検知ソリューション

永野 愛子 稲山 享伸

Solution to Detect Unauthorized Client PCs

Aiko Nagano Kiyonobu Inayama

近年、爆発的に増加するウイルス感染の被害にはインターネット経由だけでなく、外部からの持込などで不正に接続されたPCを起点とした被害も多い。このような被害には不正接続PCのすみやかな検知と対応が必要である。本論文では既存の資産管理ツールとネットワーク監視ツールによる不正接続PCの検知ソリューションを提案し、そのしくみや考慮点を論じる。

In recent years the number of damages by viruses has been increasing explosively. They are not necessarily intruders over the Internet, but many of them originate from PCs brought in from outside and connected to a local network without authorization. To prevent such damages, prompt detections and actions against illegally connected PCs are required. This paper proposes to administer existing assets and to detect unauthorized PCs using Inventory Management and Network Monitoring provided by Tivoli, and discusses its functions and the points to be considered.

Key Words & Phrases : クライアントPC ,不正検知 ,ウイルス ,監視 ,Tivoli®
Client PC, detection of unauthorized PCs, virus, network monitoring, Tivoli®

1. はじめに

続々と新種が登場するコンピュータウイルスによる被害が相次いでいる。特に企業ネットワークにおけるクライアントPCのウイルス感染の被害は甚大で、根本的な対応策が求められている[1]。このウイルス被害への対策として、ウイルス・パターンファイルやセキュリティパッチの配布の必要性が唱えられ[2]、配布ソリューションが注目されている。しかしながらウイルス被害には、外部からの持ち込みなどで不正に接続されたPCを起点とした被害も多く、そのようなケースにはセキュリティパッチなどの配布だけでは十分に対応できない。

このような課題を考慮し、根本的なウイルス対策を行うためには、不正接続されたPCの検知と対応が必要である。そのような不正接続されたPCに対する対策として新しく登場した「自己防衛型ネットワーク・ソリューション」[3]は、一貫性のあるコンプライアンス・チェックと修復の高度な自動化を実現しているが、ネットワーク構成など全面的な刷新が必要である。本論文では、多くのお客様で利用されている既存の資産管理ツールとネットワーク監視ツールを組み合わせ

不正接続PCの検知ソリューションを提案し、その実現および運用に関する考慮点について論じる。

2. ソリューションの概要

提案するソリューションは図1に示すように資産管理ツールとネットワーク監視ツールの組み合わせから成り立っている。具体的には、資産管理ツールで把握した資産管理DBを基本情報として、ネットワーク監視ツールでリアルタイムに検知した「未知のPC」が資産管理DBに登録されている「正規のPC」に該当するかを自動的に検査して対応するというものである。この

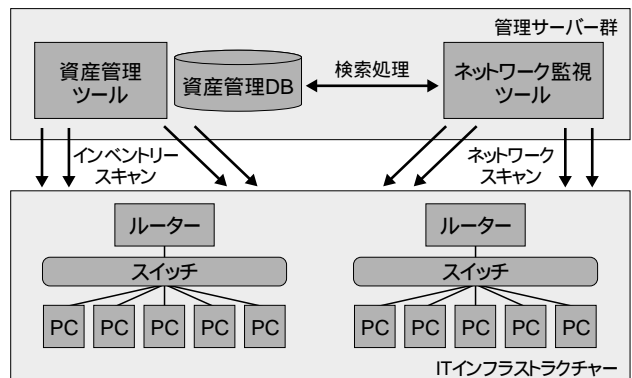


図1. ソリューションの概要図

提出日：2004年08月31日 再提出日：2005年5月14日

ような機能は、既存の単体製品の標準機能としては提供されていないため、本論文では製品の組み合わせとカスタマイズによる実現方法を検討する。

3. ソリューションのしくみ

考案したソリューションのしくみと利用する要素技術について、考察を交えて説明する。

3.1 システム構成

既存のTivoli®製品を使用して不正PCを検知する検証システムを図2のように設計した。

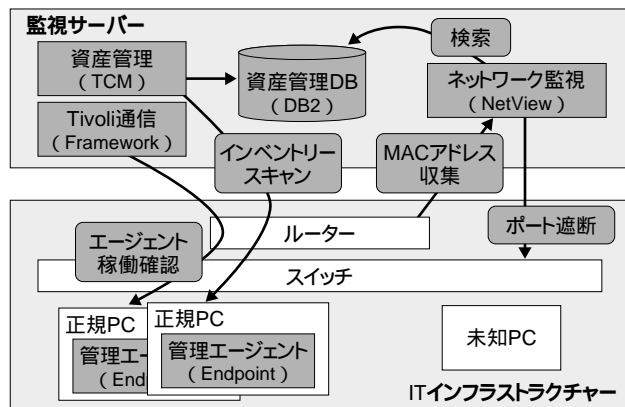


図2. 検証システム構成図

資産管理ツールとしてTivoli製品群のTivoli Configuration Manager(TCM)を利用する。TCMはシステム内のハードウェアやソフトウェア情報を収集し資産管理を実現する製品である。Tivoli FrameworkはTCMの稼働環境となるサーバー機能や管理エージェント(Tivoli Endpoint)を提供する。ネットワーク監視ツールとしてTivoli NetView®(NetView)を利用する。NetViewはSNMPマネージャー機能によるネットワーク監視機能を提供する。使用した製品を下記にまとめる。括弧内の製品略称は図2の表記と一致させており以後の説明でも使用する。

- ・ Tivoli Framework 4.1.1 (Framework)
- ・ Tivoli Configuration Manager 4.2.1 (TCM)
- ・ Tivoli NetView 7.1.4 (NetView)
- ・ DB2 Universal Database® 8.1 (DB2®)

3.2 PCの判定

未知のPCを不正と判定するためには、正規のPCの明確な定義とPCを特定する属性情報が必要になる。拠り所となる資産管理DBの情報を基にPCの判定情報について検討する。

(1) 正規のPC

はじめに正規のPCとは何かを定義する。本論文では、正規のPCの条件を下記とする。

- ・ 管理エージェントを導入済
- ・ 資産管理ツールのインベントリースキャンを受けておりPCの属性情報を登録済

この前提を満たすためには資産管理ツールの全社的な展開が必要である。資産管理ツールの導入により、PC情報の把握にかかる運用負荷の軽減や徹底が期待できる。

(2) PCの判定情報

資産管理DBに登録されるPCの属性情報を調査し、PCが不正かどうかを判定するための情報として下記を検討した。有効性や考慮点に関する考察を交えて整理する。

MACアドレス: PCがNetwork Interface Card(NIC)単位に持つ情報であり、PCの判定に利用可能。考慮点としてNIC引き継ぎやドライバー設定で偽造が可能なことに注意が必要である。

IPアドレス: PCが個別に持つこともあるが、DHCPが普及した昨今のIT環境では判定情報として不適切である。

SMBIOS情報: PCがマザーボードごとに保持するユニークな識別情報であるため、PCの判定に有用である[4]。ただし、取得には資産管理ツールのインベントリースキャンが必要である。

管理エージェント有無: 正規PCの前提条件から、PCにおける管理エージェント有無は有用な判定情報である。

重要なPCの判定情報として、MACアドレス、SMBIOS情報、管理エージェント有無の3つに着目する。

(3) 未知のPC

不正と考えられる未知のPCにはどのような状態が考えられるであろうか。難易度の違いはあるものの、前述のPCの判定情報の一部は偽造が可能である。偽造の可能性を考慮し、表1に未知のPCのパターンを整理した。なお、SMBIOS情報の改ざんは事実上不可能なので偽造を考慮しない。

表1. 未知のPCのパターン

パターン	MACアドレス偽造	管理エージェント偽造
(a)	無	無
(b)	有	無
(c)	有	有

(a)は何も偽造せず不用意に持ち込まれた外部のPCが該当する。未知のPCのもっともポピュラーなパターン

ンである (b)は既存のNIC装備あるいはドライバーの設定変更で ,MACアドレスを改ざんした状態で持ち込まれた外部のPCである (c)は (b)に加えて ,管理エージェントの偽造まで実施したパターンである .ただし ,管理エージェントの偽造には管理製品の特殊なスキルが必要であり ,MACアドレスの偽造に比べて難易度が高い .

3.3 検知方法

次に3.2節 (3)で挙げた各パターンの未知のPCを見つけ出す検知方法について述べる .下記のように3つの検知方法を検討した .

- | | |
|----------------|-------------|
| 未知のMACアドレス検出 | 未知のPC (a) |
| エージェント未導入の検出 | 未知のPC (b) |
| SMBIOS情報の変化の検出 | 未知のPC (c) |

検証環境ではあるが簡易なプロトタイプを作成し ,各パターンの未知のPCを検知できることを確認した .検証で得た考慮点を交えて ,各方法の技術的な内容をまとめる .

(1)未知のMACアドレス検出

未知のMACアドレス検出は ,NetViewのMIB収集機能を用いて作成することができる .処理の流れを図3に示す .

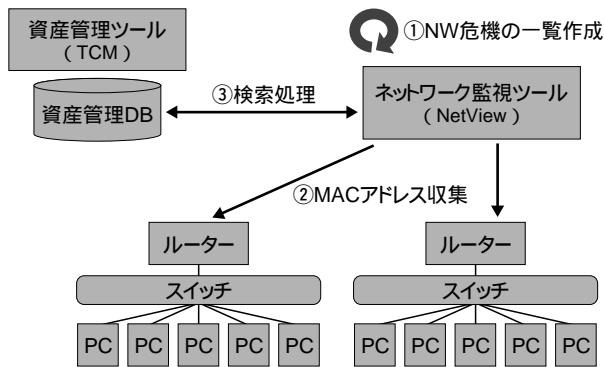


図3. 未知のMACアドレス検出

- ① はじめにNetViewによりPCが接続されるネットワークセグメントのルーターやスイッチの一覧を作成する .具体的にはNetViewのnvdformatコマンドを利用することにより ,特定の条件に基づいたルーターやスイッチの一覧を作成することができる .
- ② 次にルーターやスイッチからMACアドレスとIPアドレスの対応情報であるARPテーブルを収集する .多くのSNMP対応の機器はRFC1213 MIB-IIのAddress Translation group(atグループ)をサポートしている .このatグループはARPテーブルの情報を含む[5] .今回のしくみでは ,NetViewのsnmpwalkコマンドを利用して ,ルーターやスイッチ

からatグループのMIBを取得する .

このとき ,PCが接続される可能性のないWANなどのネットワークアドレスについては除外する配慮が必要である .

- ③ ②の手順で得られた活動中のMACアドレス一覧を ,資産管理DBで検索し ,DBに登録されていない未知のMACアドレスを得る .この方法により未知のMACアドレスを検出でき ,未知のPCパターン (a)の検知に役立つ .

(2)管理エージェント未導入の検出

管理エージェント有無のチェックは ,未知のMACアドレス検出で検査にパスしたPCを検査対象とする .この検出はFrameworkの管理エージェント(Endpoint)稼働状況チェック機能により実現することができる .処理の流れを図4に示す .

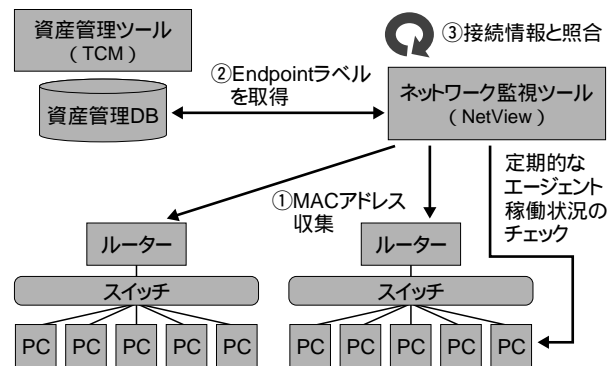


図4. 管理エージェント未導入の検出

- ① “ 未知のMACアドレス検出 ”で得られたMACアドレス一覧から ,検査にパスした活動中のMACアドレス一覧(正規)を作成する .
- ② ①で得られた活動中のMACアドレス一覧(正規)のEndpointラベルを資産管理DBから取得する .得られた一覧は ,活動中であるべきEndpointラベル一覧である .
- ③ ②のEndpointラベル一覧を入力にして ,Frameworkのwepstatusコマンドで各Endpointの稼働状況を照会する .ステータスが異常の場合 ,MACアドレスが活動中であるにもかかわらず管理エージェント(Endpoint)が稼働していない状況と判断でき ,MACアドレスを偽造した未知のPCパターン(b)の検出が可能になる .

wepstatusコマンドはFrameworkのゲートウェイによるEndpointの稼働状況チェック結果を表示する機能である[6] .ゲートウェイによるチェックは定期的であるため ,タイムラグによる誤報の可能性も懸念される .対策として ,異常検知後にwepコマンドでピンポイント

トに即時の再確認をすれば、誤報を削減できる。

(3) SMBIOS情報変化の検出

SMBIOS情報のチェックは、資産管理ツール(TCM)のインベントリースキャンにより可能である。この処理は管理エージェントが活動中のPCを対象とする。処理の流れを図5に示す。

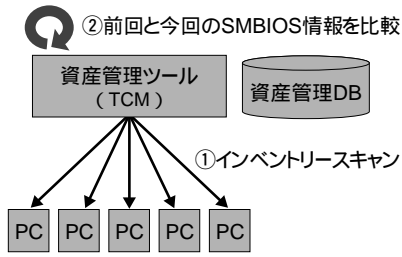


図5. SMBIOS情報変化の検出

- ① 資産管理ツールでインベントリースキャンを実行し、SMBIOS情報を収集する。
- ② 前回と今回のSMBIOS情報をチェックし、変化した場合に不正と判断する。この方法により未知のPCパターン(c)を検出できる。

(4) 検知方法のサマリー

それぞれの検知方法とその検知対象を図6にまとめる。各検知方法はお互いを補完して、想定したすべてのパターンの未知のPCを検知する。

この中で、「管理エージェント未導入の検出」は「未知のMACアドレス検出」の出力を利用するため、二つの方法を連続して実行することが望ましい。一方で、「SMBIOS情報変化の検出」は他の二つの方法とは処理が独立しているため、個別に実行できる。

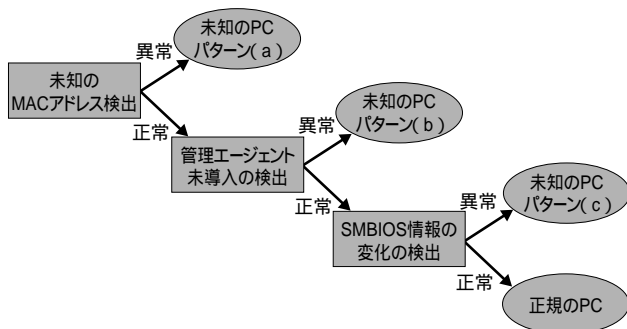


図6. 検知方法のサマリー

3.4 アクション

不正なPCと判断した場合の対応方法として、不正検出後のアクションについてまとめる。不正検出後の対応として、通知と強制排除の二通りが考えられる。通知は管理者へ不正なPCの存在を連絡する。通知

の方法としては、ポップアップの表示や統合監視サーバーへの転送など、運用形態にあわせてさまざまな方法を選択することが可能である。通知は必ず組み込むべきアクションである。

強制排除は不正なPCをネットワークから強制的に排除する。強制排除は通知よりも自動化の効果は高いが、接続断のリスクを伴う。強制排除の方法として、スイッチにおけるポート遮断が効果的と考える。自動的なポート遮断の処理の流れを図7に示す。

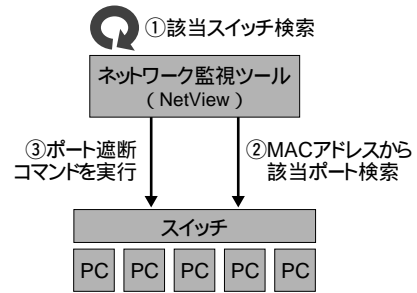


図7. 強制排出

- ① 不正なPCの属性情報からPCが接続されているスイッチを検索する。NetViewが持つトポロジー情報からIPアドレスをキーにして該当のスイッチを割り出すことができる。
- ② 該当のスイッチに対して、不正なPCのMACアドレスが接続されているポートを検索する。スイッチのポートとPCのMACアドレスの対応情報はatグループなどの標準MIBで知ることができない。この情報を得るためには、スイッチの拡張MIBを使用するか、市販のtelnetエミュレーション機能などを使用してスイッチのコマンドを実行する必要がある。Cisco Catalystシリーズであれば、「show mac address table」コマンドが該当する。
- ③ 該当のスイッチに対して、対象のMACアドレスが接続されているポートの遮断コマンドを実行する。②と同様にポート遮断の操作は汎用的な標準MIBで行うことができないため、スイッチの拡張MIBを使用するか、市販のtelnetエミュレーション機能などを使用してスイッチ独自のコマンドを実行するしくみが必要である。Cisco Catalystシリーズであれば、「shut」コマンドが該当する。

これらの検知方法やアクションについて、4章の考察をへて、5章のソリューションの活用で効果的な実行方法や組み合わせをまとめる。

4. 考察

検知方法やアクションの最適な活用方法を模索するため、いくつかの考察を以下に述べる。

(1) 負荷

3章で検討した検知方法の負荷をデータ量とPC負荷の二つの観点で表2にまとめる。

表2. 検知方法の負荷

検出方法	データ量(PC 1台あたり)	PC負荷
未知のMACアドレス検出 (MACアドレス収集)	送信データ量 50byte 受信データ量 50byte	小
管理エージェント未導入の検出 (ゲートウェイのチェック)	送信データ量 75byte 受信データ量 75byte	小
SMBIOS情報変化の検出 (インベントリースキャン)	送信データ量 15000byte 受信データ量 4500byte	大

下記にそれぞれの計測結果と考察をまとめる。

① データ量

管理サーバーが送受信するデータ量をトレースで計測しネットワークに与える負荷を調べた。

“未知のMACアドレス検出”では、ルーターに対するARPテーブル収集のデータ量を計測し、PC1台のエントリーあたり約50byteであることがわかった。ただし、照会先はルーターでありPCへの直接の通信は発生しない。やり取りするデータ量は変動しないため、PCによる差異はほとんどない。

“管理エージェント未導入の検出”では、ゲートウェイのチェックのデータ量を計測し、PC1台あたり約75byteであることがわかった。この処理も、やり取りするデータ量はあまり変動しないため、PCによる差異はほとんどない。

“SMBIOS情報変化の検出”では、インベントリースキャン処理を計測した。送受信データは他の方法よりも多いが、スキャン項目を絞ることにより、データ量は少なくできる。

どの処理も1台あたりのトラフィック量はそれほど大きくないが、低速回線の先に多数のPCが設置されるネットワーク環境ではこのようなデータにも注意すべきである。

② PC負荷

“未知のMACアドレス検出”および“管理エージェント未導入の検出”は、検証によりPCにほとんど負荷を与えないことを確認した。

“SMBIOS情報変化の検出”のインベントリースキャン実行中はPCのCPU使用率が非常に高くなることが、検証で確認された。スキャンの実行時間は対象項目

を絞ることで短くすることは可能であるが、あまり頻繁に実施することは現実的ではないと考える。

(2) MACアドレス収集の精度

ルーターのARPテーブルにPCのMAC/IPアドレスが登録されるのは、PCがルーター経由で通信したタイミングである[7]。また、ARPにはキャッシュの制限時間が設定されている。このため、未知のPCが頻繁に通信しない場合、タイミングによってはルーターのARPテーブルから未知のPCを発見できない可能性がある。ひとつの対策としてはNetViewから能動的にPCに対して実施する状況ポーリング(PING相当の通信)の活用が考えられる。状況ポーリングの間隔をARPのキャッシュの制限時間より短くすることによりARPテーブルが最新に保たれるため、収集するMACアドレスの網羅性を上げることができる。

(3) 誤報への対策

それぞれの検知方法では、想定している未知のPCの他に、表3のように必ずしも不正と決め付けられない事象を検知する可能性がある。

表3. 誤報の例

検知方法	誤報の例
未知のMACアドレス検出	NICの交換 / 追加
管理エージェント未導入の検出	エージェントの障害・停止 チェックのタイムラグ
SMBIOS情報の変化の検出	マザーボードの交換

対策について考察する。NICの交換/追加やマザーボードの交換などのハードウェアレベルの交換については、ユーザーから管理部門への連絡と資産管理DBの更新を徹底させることにより、ある程度防ぐことができる。エージェント稼働確認のタイムラグによる誤報は、チェックのリトライによる再確認で削減できる。エージェントの障害はそれ自身が対応の必要なエラーである。不正なPCの可能性とエージェント障害の両方の可能性を考慮して、管理部門が対応することが望ましい。

(4) 大規模ネットワークへの対応

PC数十万台という規模の環境も少なくはない。管理サーバー群やネットワークの負荷は管理対象の数に依存するところが多いので、対象数が多い場合には、実行タイミングや頻度、同時に実施する対象数などを考慮する必要がある。具体的には複数の管理サーバーや複数のゲートウェイによる担当範囲の分散が、大規模環境の対策として効果的だ。また、MACアドレスな

どの情報を資産管理DBで検索する作りこみの処理の負荷も懸念される。この部分はRDBMSのチューニングやSQLコーディングの工夫などにより、効率的な検索処理を心がける必要がある。

(5) 強制排除の考慮点

ポート遮断による強制排除のしくみはスイッチの機種に依存するため、機種によっては実装できない場合もある。このため、ネットワーク環境の整備・標準化と共に実装を進める必要がある。さらに、スイッチの先に子ハブを接続した環境では、ひとつのスイッチ・ポートに複数のMACアドレスが接続された状態となり、スイッチのポート遮断が他の正規のPCに影響を与えるリスクがある。また、(3) 誤報で考察したように、必ずしも不正と決め付けられないIPCを検知した場合の強制排除の是非も考慮すべきである。

疑わしき事象が発生した場合に、通知のみとするか、あるいはひとまず強制排除した後で確認するかを方針として決定する必要がある。

5. ソリューションの活用

不正PC検知ソリューションを活用するには、はじめに正規のPCの定義と検知する不正PCのレベルを明確にするべきである。

3.2節で整理した未知のPCのパターンのうち、管理エージェントの偽造のある(c)は、ユーザーに特殊なスキルを要するため存在する可能性が少ない。パターン(a)および(b)を対象としてMACアドレスの偽造がある状態までを想定すれば、ほとんどの不正なPCはカバーできるであろう。つまり、それらを検知する“未知のMACアドレス検出”と“管理エージェント未導入の検出”を組み合わせることで実行すれば、不正PCの大半を検知できると考える。また4章 考察(1)負荷にあるように、“未知のMACアドレス検出”と“管理エージェント未導入の検出”には、ネットワークおよびPCの観点で大きな負荷はかからないので、頻繁に実行しても問題ないと考えられる。

一方で、“SMBIOS情報の変化の検出”については、あまり頻繁に実行するとPCへの負荷が懸念される。通常の資産管理のインベントリースキャンの際に、相乗りして検査する運用が妥当と考える。アクションに関しては、強制排除の考慮点を重視し、まずは通知で実績を重ねて、強制排除へ段階的にレベルアップすることが妥当である。

上記の考え方をベースにして、考案した検知方法を活用する設計例を実行タイミングとアクションの観点で表4にまとめる。

新規PCに対しては、インベントリースキャンをユー

表4. 検知方法の活用例

処 理	実行タイミング	アクション
①インベントリースキャン	月2回および申請時	-
②未知のMACアドレス検出	毎15分	通知
③管理エージェント未導入の検出	毎15分(②と同じ)	通知
④SMBIOS情報の変化の検出	月2回(①と同じ)	通知

ザーの申請時に実行し、資産管理DBを確立する。PC利用中にも長いインターバルで実行して資産管理DBを更新する。そして、“未知のMACアドレス検出”と“管理エージェント未導入の検出”を組み合わせることで短いインターバルで定期実行し、おかたの不正PCの発見を目指す。“SMBIOS情報の変化の検出”は、定期的なインベントリースキャンに付加して行う。このような活用方法は、検知方法の守備範囲と負荷の観点でバランスのとれた例と考える。

6. おわりに

本論文ではMACアドレス偽造などのさまざまな不正PCのパターンを考慮し、既存の製品にない不正PC検知の方法を考案・検証した。

今回のソリューションは、多くのお客様で既に利用されている製品群の組み合わせを使用している[8]。また、ネットワークに大きな変更を加えることなく不正PC検知を実現できることも特長である。よって、実際のお客様の環境においても、技術者が本論文のしくみを応用することは容易である。

さらに、今回選択したTCMはセキュリティパッチ配布にも利用でき、TCMを利用したセキュリティパッチ配布ソリューションも紹介されている[9]。本論文の不正PC検知機能とセキュリティパッチ配布機能を組み合わせることで、より強力なウイルス対策を実現できる。

本論文の基本的な手法は広く展開できる可能性がある。本論文の内容が、増大するウイルス被害を食い止めるための一助となれば幸いである。

参考文献

- [1] JIPA, 国内・海外におけるコンピュータウイルス被害状況調査, 2004年4月
- [2] @IT, ネットワーク管理者のためのBlasterワーム対策, <http://www.atmarkit.co.jp/fwin2k/hotfix/ms03-blaster/blaster01.html>, 2003/08/16
- [3] IBM Japan, 自己防衛型ネットワーク・ソリューション, <http://www-6.ibm.com/jp/software/tivoli/solution/nss/>, 2005年5月
- [4] DMTF, SMBIOS Specification, 2004年1月

- [5] IETF, RFC 1213 - Management Information Base for Network Management of TCP/IP-based internets: MIB-II, 1991年3月
- [6] IBM, Tivoli Management Framework Release Notes Version 4.1.1, 2003年11月
- [7] オライリー・ジャパン ,TCP/IPネットワーク管理 , 1999年12月
- [8] IBM ,Tivoli 事例 ,
<http://www-6.ibm.com/jp/software/tivoli/>
 「Tivoli事例一覧」,2005年5月
- [9] IBM Japan ,統合ウイルス管理ソリューション ,
<http://www-6.ibm.com/jp/software/tivoli/solution/virus/> ,2005年5月



日本アイ・ピー・エム株式会社
ITスペシャリスト

永野 愛子 Aiko Nagano

[プロフィール]

1998年 ,日本IBM入社 .1999年からシステム管理系プロジェクトを経験 ,技術支援を実施 .現在 ,今までの経験を生かしシステム管理分野をベースのスキルとして ,金融のお客様へのソリューションの提案活動に携わっている .

aikon@jp.ibm.com



日本アイ・ピー・エム
システムズ・エンジニアリング株式会社
ITスペシャリスト

稲山 享伸 Kiyonobu Inayama

[プロフィール]

1995年 ,日本IBM入社 .同年 ,日本アイ・ピー・エム システムズ・エンジニアリング出向 .

入社以来一貫して ,システム管理製品やプロジェクトを担当 .主に ,金融や製造業のお客様のプロジェクトを経験し ,その経験をベースにしてシステム管理分野の技術支援を実施中 .

inayama@jp.ibm.com