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

2004－ＤＰＳ－117　(20)
2004－CSEC－　24　(20)
2004／3／5

ネットワーク構成の動的な変化に対応したエージェントベースIDSの提案

小手川 祐樹 *　　田端 利宏†　　櫻井 幸一 †

概要　IDS をホスト上に設置する場合，ネットワーク上に設置する場合と比べて多くの情報を侵入検知のために用いることができるが，設置したホスト上の侵入検知しか行えない．そのため，ネットワークに新しく接続したホストを監視するには，そのホストに IDS を新たに導入する必要がある．本論文では，モバイルエージェントを用いることで，ネットワークに新しく接続したホストへ自動的に IDS の機能を導入できるエージェントベース IDS を提案する．提案方式では，モバイルエージェントの移動性によって IDS の導入コストが削減される．またバージョンアップしたエージェントを一斉に配布することにより，効率的な保守管理が可能となる．

キーワード　セキュリティ，モバイルエージェント, IDS，Hotspot

Agent-based IDS for Dynamic Variation of Network Composition

Yuki KOTEGAWA *　Toshihiro TABATA †　Kouichi SAKURAI †

Abstract—　Compared with IDS installed on a network, IDS installed on a host can use more information for intrusion detection. However, IDS installed on a host can detect intrusion into only the host. Therefore, when a host is newly connected to the network, it is necessary to newly install IDS into the connected host. In this paper, Agent-based IDS is proposed. The system can automatically install IDS into the connected host On the proposed system, the mobility of mobile agents can save the time and effort of introduction of IDS. Moreover, by simultaneous distribution of upgraded agents, efficient maintenance management is realized.

1　はじめに

近年，Hotspot[1] において不特定多数のモバイルユーザが無線でのインターネット接続サービスを利用することが可能になっている．非登録制の Hotspot 運用形態では，ユーザは登録としての前準備なしでいつでも手軽にインターネット接続サービスを利用できる．このことはユーザにとって大きな利点であるが，不特定多数のユーザが AP(アクセスポイント) を利用することができるため，悪意を持つ攻撃者が不正行為の踏み台としてその AP を利用する可能性が考えられる．そこで，不特定多数のユーザが AP を利用することを制限するために，登録制の Hotspot 運用形態がある．AP を利用したいユーザはあらかじめ登録作業を行うことでインターネット接続サービスを利用することができる．ユーザが AP を不正行為の踏み台として利用した場合は，ユーザ管理が行われているためその不正ユーザを特定できる．しかしながら，悪意を持つ攻撃者が AP の他のユーザを踏み台として利用する可能性が残る．

Hotspot の管理者がネットワーク上で IDS[2] を用いれば，新たに接続したユーザに対する攻撃やそのユーザからネットワークに対する攻撃もある程度検知することができる．しかしながら，ユーザの数が増加した場合は，解析の負荷はその IDS が稼動しているホストに集中する．その結果，パケットの取り

* 九州大学大学院システム情報科学府 〒 812-8581 福岡市東区箱崎 6-10-1, Graduate School of Information Science and Electrical Engineering, Kyushu University, 6-10-1 Hakozaki, Higashi-ku, Fukuoka City, Japan: kotegawa@itslab.csce.kyushu-u.ac.jp
† 九州大学大学院システム情報科学研究院 〒 812-8581 福岡市東区箱崎 6-10-1, Faculty of Information Science and Electrical Engineering, Kyushu University, 6-10-1 Hakozaki, Higashi-ku, Fukuoka City, Japan: {tabata,sakurai}@csce.kyushu-u.ac.jp

こぼしが生じると侵入検知のリアルタイム性が損なわれる可能性がある．このとき，利用ユーザの各ホストにおいてIDSやFWによる防御を行えば，負荷が集中することを考慮せず踏み台にされる危険性を減少させることができるが，全てのユーザに導入・保守管理を徹底させることは困難である．

本提案方式では，IDSをモバイルエージェント[3]で構成することにより，新しくAPに接続したホストへIDSを自動的に導入することを目的としている．IDSコンポーネントは，情報収集エージェントと解析エージェントから構成され，新たなホストがネットワークに接続したとき，それらのモバイルエージェントはそのホストに送信され実行される．それゆえ，モバイルエージェントの移動性によって，IDSの導入の手間が削減される．またバージョンアップしたエージェントを一斉に配布することにより，効率的な保守管理が可能となる．

2 Hotspot

Hotspotは無線LANやBluetoothなどのAPを設置し，無線でのインターネット接続サービスを不特定多数の利用者に提供している空間である[1]．ISPなどが商用サービスとして提供する場合から，飲食店などが利用客に対して無料サービスとして提供する場合まで，その提供形態は多種多様である．Hotspotの運用形態として以下のように非登録制と登録制をあげ，それらの特徴と問題点について述べる．

(1) 非登録制による運用

APは特別な認証をせずに，接続してきたユーザに対してインターネット接続サービスを提供する．

特徴：APのユーザは，前登録なしでいつでもインターネット接続サービスを利用することができる．

問題点：ユーザ管理を行わないため，不特定多数のユーザがインターネット接続サービスを利用することとなる．そのため，悪意を持つユーザが不正行為の隠れ蓑としてAPを利用する可能性がある．またAPのユーザのセキュリティ意識が低い場合，そのユーザのホストが悪意を持つ攻撃者による不正行為の踏み台にされる可能性もある．どちらの場合も，その不正行為の発信元IPアドレスはAPが配布したものであるため，APの管理者に責任が求められる．

表 1: IDSの分類

		設置場所		
		ネットワーク上	ホスト上	
IDSへの入力	ネットワークトラフィック	ネットワークIDS	ネットワークノードIDS	ハイブリッドIDS
	システムログ	なし	ホストIDS	

(2) 登録制による運用

登録制はAPのユーザを制限するためにユーザの登録を行う運用方法である．ユーザはAPを利用したい場合，事前にアカウント情報を登録することでAPのアカウントを入手する．APは登録されているアカウント情報に基づいて接続ユーザを認証する．そして，認証結果が正しい場合のみ接続ユーザにインターネット接続サービスを提供する．

特徴：認証によるユーザ管理を行うため，APの管理者はアクセスログを参照することでAPのユーザを把握できる．

問題点：ユーザ管理が行われるため，APのユーザが不正行為を行った場合，アクセスログを基に調査を行うことでその不正ユーザは特定される．しかしながら，APのユーザのセキュリティ意識が低い場合は，悪意を持つ攻撃者によって不正行為の踏み台としてそのユーザのホストが利用される可能性がある．このとき，その不正行為の発信元IPアドレスはAPのユーザに配布されたものであるため，そのAPのユーザに責任が求められる．

APの運用を登録制にしたとしても，APのユーザが不正行為の踏み台にされる可能性は残る．しかしながら，次章で扱うIDSを適切に利用できれば，これらのAPのユーザを踏み台とするための侵入行為は検知される．

3 関連研究

3.1 IDS

IDS(Intrusion Detection System)はシステムへの侵入行為を検知するためのシステムである．IDSは導入されたネットワーク上やホスト上で情報を収集し，解析することでターゲットに対する不正な侵入行為の検知を行う．IDSが解析を行う情報や場所は次のように分類される[2]．分類を表1に表す．また，既存のIDSの問題点について述べる．

3.1.1 IDS への入力による分類

何を IDS へ入力するかという点で，以下のように分類できる．

(1) ネットワークトラフィック

ネットワークを流れるパケットを監視対象とする．(ネットワーク IDS，ネットワークノード IDS，ハイブリッド IDS)

(2) システムログ

OS やアプリケーションのログを監視対象とする．(ホスト IDS，ハイブリッド IDS)

3.1.2 設置場所による分類

どこに IDS を設置するかという点で，以下のように分類できる．

(1) ネットワーク上

IDS をネットワーク上に設置する場合，次のような利点がある．(ネットワーク IDS)

・低い監視コスト
・監視対象に対する影響が少ない
・IDS への侵入の可能性が低い

(2) ホスト上

IDS をホスト上に設置する場合，次のような利点がある．(ネットワークノード IDS，ホスト IDS，ハイブリッド IDS)

・多様な監視ソースが利用できる
・手法や行為でなく結果に基づいた監視ができる
・監視精度を上げることができる
・高トラフィック下での監視ができる
・暗号化された通信を監視することができる
・直接的な不正アクセスの対処ができる

3.1.3 設置場所に基づく IDS の問題点

ネットワーク上に IDS を設置した場合には，ネットワーク単位で侵入検知を行える．しかしながら，ネットワークのトラフィック量が増大し解析負荷がネットワーク上の IDS に集中した場合，ネットワーク上の IDS は検知すべきパケットを取りこぼし侵入行為を見逃す可能性がある．

一方，ホスト上に IDS を設置した場合，解析負荷を分散できる．また侵入検知のためにホスト上の様々な情報を利用することもできる．ただし，ネットワーク上に設置した場合と比べて，ホスト単位で侵入行為の検知を行うため，ネットワーク単位で行われる侵入行為を検知することができない可能性がある．また管理するホストが増加した場合，その導入と保守管理のためのコストは増加する．

そのため，ネットワーク上に IDS を設置する場合には IDS の分散化が求められ，ホスト上に IDS を設置する場合は IDS 間の協調や導入・保守管理の容易さが求められる．

3.2 モバイルエージェントを利用した IDS

近年，モバイルエージェントを利用した IDS について，様々な研究が行われている [4]．モバイルエージェントは実行を開始したシステムに拘束されず，利用者の代わりに自律的に活動を行うプログラムである [3]．非同期実行，負荷分散，耐故障性の実現や通信量の削減など様々な利点を持つ．提案されている既存のモバイルエージェントミドルウェアの中には，階層構造を用いることで，エージェントに拡張性を持たせることができるものも存在する [5]．

部分的にモバイルエージェントを利用した IDS として，自律エージェントによって情報収集と監視を行う分散型 IDS[6] や，階層型通信機構を用いることで自律エージェント間で協調が行える分散型 IDS[7]，モバイルエージェントを利用して侵入者の追跡を行う IDS[8] および自身を DoS 攻撃から守るためにモバイルエージェントを利用した IDS[9] などが提案されている．一方，全ての IDS コンポーネントがモバイルエージェントで構成されており，情報収集と情報解析機能をもつモバイルエージェントによって，プロセス監視と制御および IDS 間の連携を行う IDS も提案されている [10]．これらの研究では IDS の分散化，IDS 間の協調または機能拡張のためにモバイルエージェントを利用することを目的としている．

しかしながら，Hotspot のようなネットワーク構成が動的に変化する場合において，モバイルエージェントによる IDS を利用するためには，動的に追加されるホストへの導入手段も考慮する必要がある．

4 提案方式

4.1 目標

本提案方式では，不特定多数のモバイルホストがネットワークに接続することで動的にネットワークの構成が変化する Hotspot のような環境において，2 章で取り上げた問題点の一つである AP のユーザのホストが踏み台にされることを防ぐことを目標とする．モバイルホストが AP に接続したときに，AP の DHCP サーバによる IP アドレスの配布と連動して，モバイルエージェントによって IDS の機能をそのホストへ自動的に導入することでこの問題点を解決する．

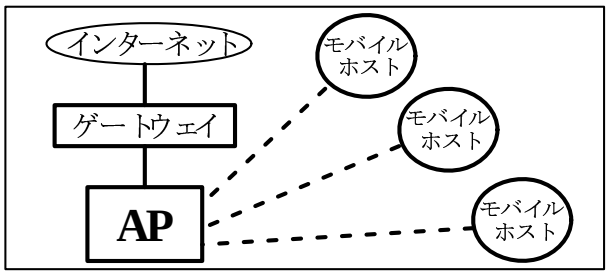

図 1: ネットワーク構成モデル

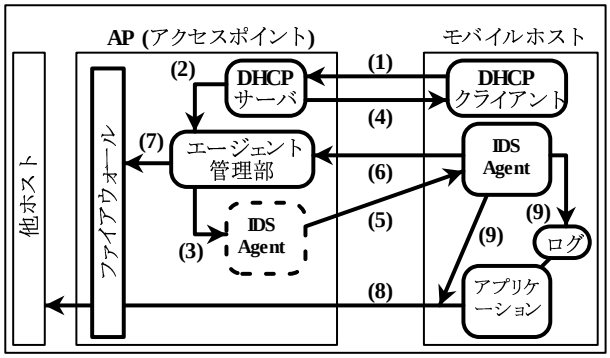

図 2: 提案方式モデル

4.2 前提

4.2.1 ネットワーク構成モデル

ゲートウェイ，AP およびモバイルホストから構成されるネットワークを想定する．ゲートウェイは AP が提供する無線ネットワークとインターネットの境界である．AP には DHCP サーバと FW が導入されており，モバイルホストに無線通信でインターネット接続サービスを提供すると共にパケットフィルタリングが行える．モバイルホストは動的に AP に接続，切断を行うエンドユーザであり，モバイルエージェントミドルウェアが導入されている．ネットワーク構成の概略図を図 1 に表す.

4.2.2 攻撃モデル

モバイルホストが関係する攻撃は以下の 3 つに分類できるが，本論文では，モバイルホストが攻撃を受ける場合，すなわち (1) および (2) を防ぐことを考える．

(1) ゲートウェイの外から内への攻撃
インターネット上の外部者がモバイルホストを攻撃

(2) ゲートウェイの内から内への攻撃
モバイルホストがモバイルホストを攻撃

(3) ゲートウェイの内から外への攻撃
モバイルホストが外部者を攻撃

4.3 提案システム構成

提案システムは，エージェント管理部および IDS エージェント (解析エージェント，収集エージェント) から構成される．以下に各コンポーネントの動作を述べる．また提案方式の概略を図 2 に表す.

(1) **エージェント管理部**
DHCP サーバと連携して，IDS エージェントの生成を行う．DHCP サーバが配布する IP アドレスと生成した IDS エージェントの関連付けなども行い，IDS エージェントの管理を行う．また FW とも連携する．

(2) **IDS エージェント**
IDS エージェントは以下の 2 つのモバイルエージェントから構成される．IDS エージェントはモバイルホスト上のリソースへ自由にアクセスできるとする．

(a) **収集エージェント**
モバイルホスト上でパケットやシステムログの収集を行う．

(b) **解析エージェント**
収集エージェントが収集した情報を解析することで侵入行為を検知する．

4.4 シナリオ

提案方式は以下のように実行される．概略図を図 2 に示す.

(1) モバイルホストが AP に接続する．
(2) DHCP サーバはモバイルホストに IP アドレスの配布を行う前に，エージェント管理部に IDS エージェント (解析エージェントと収集エージェント) の生成を要請する．
(3) エージェント管理部は IDS エージェントを生成する．
(4) DHCP サーバはモバイルホストに IP アドレスを配布する．
(5) エージェント管理部はモバイルホストに IDS エージェントを送信する．
(6) IDS エージェントは実行後，エージェント管理部にハートビートを送信する．
(7) エージェント管理部はハートビートを送信した IDS エージェントに対応する IP アドレスの対外通信を許可するために，FW の設定を変更する．

(8) モバイルホストは他のホストとの通信が可能になる．
(9) IDS エージェントはモバイルホスト上で，パケットやシステムログを監視・解析する．

4.5 侵入行為が検知された場合

IDS エージェントは侵入行為を検知した場合，モバイルホストのユーザにアラートを知らせると同時にエージェント管理部へアラートを送信する．エージェント管理部はアラートのレベルに応じて，そのホストをネットワークから隔離するなどの処置を行う．

4.6 エージェントの終了条件

IDS エージェントには有効期限を持たせる．有効期限は管理サーバからのハートビートによって延長される．有効期限を過ぎたエージェントは自動的に自らを破棄する．

5 考察

5.1 提案方式の特徴

(1) IDS エージェントの導入の自動化

モバイルホストは AP に接続し DHCP サーバから IP アドレスを受け取るとき，IDS エージェントも自動的に受け取る．モバイルホストは AP を利用している間，IDS エージェントによって侵入行為を検知できる．

(2) 既存のエージェントベース IDS の特徴

(a) 導入の容易さ

IDS のコンポーネントはモバイルエージェントで構成されているため，モバイルエージェントミドルウェアが導入されているホスト上に容易に導入できる．

(b) 一括した保守管理

解析部はモバイルエージェントで構成されており，全てのホストへ一括して送信し実行できる．そのため，ホスト毎にシグネチャの追加や更新のようなセキュリティを保守するための作業を行う必要はなく，保守管理に必要なコストを削減できる．

(c) 負荷分散

不正侵入の解析は AP に接続しているモバイルホスト自身が行うため，解析の負荷は特定のマシンに集中せずに各モバイルホストに分散される．ホスト自身の解析だけを行うので，ネットワークが高トラフィック状態の場合でも解析が可能である．

5.2 他 IDS と提案方式との比較

ホスト IDS(HIDS)，ネットワーク IDS(NIDS) および提案方式を，導入コスト，保守管理コストならびに負荷分散の点で比較する．

(1) 導入コスト

HIDS を用いる場合では，既存のネットワークに新しいホストが接続されるとき，そのホスト毎に手動で HIDS を導入する必要がある．NIDS を用いる場合では，ネットワーク上でパケットを監視するため，新しいホストがネットワークに接続しても新たに IDS の導入を行う必要はない．提案方式では，新しいモバイルホストが接続すると IDS エージェントが自動的に移動・実行されるため，新しいモバイルホストに対して導入作業を特別に意識する必要はない．

(2) 保守管理コスト

HIDS を用いる場合は，解析部のバージョンアップなどを行うとき全ての HIDS 毎に作業を行う必要がある．そのため，管理ホスト数が多数の場合には多量の保守管理コストが求められる．NIDS を用いる場合は，ネットワーク監視ポイントは一つ (またはホストより少数) であるため保守管理コストは削減される．提案方式では収集・解析部はモバイルエージェントとして各ホストに自動的に配布される．それらのエージェントはエージェント管理部で一括して保守管理が行われる．保守管理が行われたエージェントを全てのホストに一括して配布することで，保守管理コストが削減できる．

(3) 負荷分散

HIDS を用いる場合は，パケット解析の負荷は各ホストに分散される．そのため，ネットワークが高トラフィック状態になっても各ホストでは侵入検知が行える．NIDS を用いる場合は，高トラフィック状態のとき NIDS を設置したマシンに解析の負荷が集中するため，パケットの取りこぼしなどが生じる可能性がある．提案方式では，パケット解析の負荷は HIDS を用いた場合と同様に各ホストに分散されるため，高トラフィック状態でも問題は生じない．

5.3 提案方式の課題

(1) エージェントミドルウェアの普及

現在，エージェントミドルウェアが導入されているマシンは皆無に近い．しかしながら，セキュリティ要件が満たされれば，モバイルエージェントによって多くの恩恵を受けることができる．将来，多くのマシンにエージェントミドルウェアが導入される可能性はあると考える．

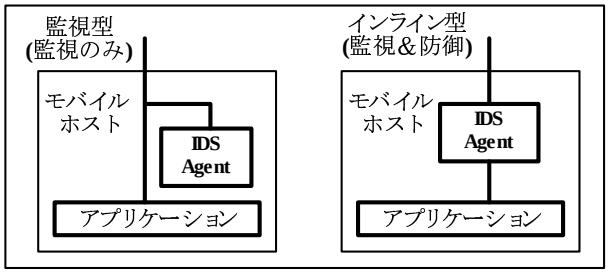

図 3: IDS エージェントのインライン化

(2) エージェントに対する改竄

攻撃者は，まずモバイルホストを踏み台にする前に，IDS エージェントを直接攻撃し，不正行為を検知できなくしてしまう可能性がある．エージェントはこのような直接攻撃に対して耐性を持つ必要がある．

(3) モバイルユーザのプライバシの問題

提案方式では，IDS エージェントはモバイルホスト上のリソースへ自由にアクセス可能であると仮定している．そのため，IDS エージェントを配布する AP は，IDS エージェントが実行する際，IDS としての機能以外の活動，例えばトロイのような活動を行わないという証拠をユーザに提示できることが必要である．

(4) インライン化

IDS の基本機能は不正侵入を検知し，アラートを発生することである．しかしながら，検知するだけでは，その侵入行為を防ぐことはできない．リアルタイムに侵入行為からホストを保護するためには，IDS をインライン化する必要がある．インライン化するためには IDS エージェントをプロキシサーバのように利用できる必要がある．概略図を図 3 に示す．

(5) AP を直接踏み台にする攻撃者への対策

本論文では，4.2.1(3) で取り上げた AP を利用するユーザが，AP を直接踏み台として利用する攻撃については扱っていない．しかしながら，非登録制の AP では悪意を持つユーザが存在する場合を考える方が現実的である．そのため，IDS エージェントによって AP のユーザを保護するだけでなく，AP のユーザによる AP を直接踏み台にする行為を制御可能な方式も必要である．

6 まとめ

本論文では，Hotspot のような動的にネットワーク構成が変化する場合において，ネットワークに接続するモバイルホストへ自動的に IDS を導入できるエージェントベース IDS を提案した．提案方式では，AP の DHCP サーバによる IP アドレスの配布と連動して，モバイルエージェント化した IDS をモバイルホストへ移動させる．このことにより，新しく接続したモバイルホストも IDS の機能を自動的に利用することが可能となる．さらには，解析部の一括したバージョンアップなども可能になり運用管理面での効果が期待できる．今後の課題として，利用者が IDS エージェントを信頼するための仕組み，IDS エージェントのインライン化およびモバイルホストの不正行為に対する制御方式の解決をあげる．

参考文献

[1] IT 用語辞典 e-Words, http://e-words.jp/

[2] Japan Network Security Association Dynamic Defense Working Group, “ホストベースの IDS の概要と適用について”, 2002.
http://www.jnsa.org/active/houkoku/IDSBasic.pdf

[3] OMG, “Mobile Agent Facility Specification”, 2000.
http://www.omg.org/cgi-bin/apps/doc?formal/00-01-02.pdf

[4] Wayne A. Jansen, “Intrusion detection with mobile agents”, ELSEVIER, Computer communications, p. 1392-1401 Volume 25, Issue 15, 2002.
http://csrc.nist.gov/mobilesecurity/Publications/IDwMA.pdf

[5] I. Sato, “MobileSpaces: A Framework for Building Adaptive Distributed Applications using a Hierarchical Mobile Agent System”, In Proceedings of IEEE International Conference onDistributed Computing Systems, 2000.
http://research.nii.ac.jp/~ichiro/papers/satoh-icdcs2000.pdf

[6] Jai Sundar Balasubramaniyan, Jose Omar Garcia-Fernandez, David Isacoff, Eugene Spafford, Diego Zamboni, “An Architecture for Intrusion Detection using Autonomous Agents”, Department of Computer Sciences, Purdue University; Coast TR 98-05, 1998.
ftp://ftp.cerias.purdue.edu/pub/papers/diego-zamboni/zamboni9805.pdf

[7] Rajeev Gopalakrishna, Eugene H. Spafford,“A framework for distributed intrusion detection using interest driven cooperating agents”, Paper for Qualifier II examination, Department of Computer Sciences, Purdue University, 2001.
http://citeseer.nj.nec.com/gopalakrishna01framework.html

[8] Midori Asaka, Shunji Okazawa, Atsushi Taguchi, and Shigeki Goto, “A Method of Tracing Intruders by Use of Mobile Agents, ” INET ’99 Conference, June 1999.
http://www.ipa.go.jp/STC/IDA/paper/inet99.pdf

[9] Peter Mell, Donald Marks, and Mark McLarnon, “A Denial of Service Resistant Intrusion Detection Architecture”, Computer Networks Journal, 2000.
http://csrc.nist.gov/mobilesecurity/Publications/ComputerNetworkIDS.pdf

[10] Serge Fenet and Salima Hassas, “A Distributed Intrusion Detection and Response System Based on Mobile Autonomous Agents Using Social Insects Communication Paradigm”, First International Workshop on Security of Mobile Multiagent Systems, Autonomous Agents Conference, 2001.
http://citeseer.nj.nec.com/465543.html