コンピュータセキュリティ　18－7
(2002. 7. 18)

# センター管理型不正アクセス検知システムの提案

大塚　丈司†　　白石　善明††　　森井　昌克†

† 徳島大学工学部知能情報工学科　〒770-8506 徳島県徳島市南常三島町 2-1
†† 近畿大学理工学部情報学科　〒577-8502 東大阪市小若江 3-4-1
E-mail: †{otsuka,morii}@is.tokushima-u.ac.jp, ††zenmei@is.kindai.ac.jp

**あらまし**　ネットワークに対する不正アクセスを検知するシステムとして IDS(侵入検知システム) がある．しかし IDS には設置の困難さやシグネチャの更新といった問題点があり，運用時においても正確な攻撃に関する情報を判別することは困難である．そこで本稿では管理領域毎の IDS の設置やシグネチャの更新が不要になり，さらに管理者は整理された正確なレポートを受け取ることができるセンター管理型不正アクセス検知システムを提案する．
**キーワード**　不正アクセス検知，リモート監視，IDS(侵入検知システム)

# Center Management Type Intrusion Detection System

Takeshi OTSUKA†, Yoshiaki SHIRAISHI††, and Masakatu MORII†

† Department of Information Science and Intelligent Systems, Tokushima University
Minamijosanjima-cho 2-1, Tokushima, 770-8506 Japan
†† Department of Informatics, School of Science and Engineering, Kinki University
Kowakae 3-4-1, Higasi-Osaka, 577-8502 Japan
E-mail: †{otsuka,morii}@is.tokushima-u.ac.jp, ††zenmei@is.kindai.ac.jp

**Abstract**　In this paper, we give an center management model in unlawful access detection. Agents gather the network information in each management domain. When the agent detects abnormal event, it communicates to the center and the center analyzes the network information to specify the unlawful access by using IDS. The advantages of this model are that the administrator of each domain does not need to update signatures of IDS and he can receive an essential information of an unlawful access and the way of its countermeasure.
**Key words**　unlawful access detection, remote surveillance, IDS(Intrusion Detection System)

## 1. まえがき

近年，コンピュータはネットワークに接続することが一般的となり，特にブローバンドと呼ばれる常時接続環境が安価に手に入ることにより，企業や教育機関のみならず一般家庭にも急速に普及しつつある．しかし一方で日本の官公庁の Web の改ざんやコンピュータウイルスの被害の拡大など不正アクセスやハイテク犯罪が増加傾向にある．不正アクセスに対する防御手段として様々なネットワークセキュリティシステムが開発され，特にファイアウォールはそれらの中心技術として開発，利用が一般化している．しかしながら，ファイアウォールは不要なサービスの利用の停止やフィルタリングといった機能しか持たず，それらを迂回する不正アクセスには対応することができない．

そこで近年ファイアウォールでは防ぎきれない不正アクセスに対して有効に働くシステムとして IDS(不正侵入検知システム：Intrusion Detection System) が注目されている．IDS は不正侵入を検知し，それに対するログを生成し，その対策を与える．対策とはシステムの管理者への通知だけでなくネットワークの切断，送信元への逆攻撃まで行うシステムもある．IDS で検知可能な不正アクセスとはネットワークやサーバの設定ミス，プログラムのバグ (セキュリティホール) をついた攻撃や DoS 攻撃など幅広い．

しかしながら，IDS には多種多様な機能の反面，設置や設定，運用に高度なネットワークやセキュリティの管理能力が必要であるという欠点がある．特に問題となるのがアラートと呼ばれる IDS が発する警告情報が整理され

ておらず，大量に発せられるその中から真に必要な情報を管理者自身が選び出さなければならない．したがって，IDS はセキュリティに関する知識を有するネットワーク管理者の支援手段にはなるものの，管理者の能力を補うものではない．

そこで筆者らはこの IDS の設置や管理の問題点を解消するセンター集中管理型不正アクセス検知モデル[1]を与えた．本システムは監視対象のネットワーク内に情報収集エージェントを配置し，インターネットを介してそのエージェントとの通信に基づいて，リモートセンター側で不正アクセスを分析し，リアルタイムに LAN の管理者へ送信するものである．管理者はセンターから送られる整理された解析結果のレポートを受け取ることができる．

本稿ではセンター管理型不正アクセス検知システムの原理，実装手法を述べ，諸考察を行い有効性を述べる．

## 2. 従来手法

### 2.1 IDS の目的・機能

IDS の目的は一般的にネットワークを動的に監視することである．ファイアウォールの通過を許可しているパケットを利用した攻撃に対して管理者に警告を発するため，早期に対処することができる．さらに検知した攻撃に対してネットワークを遮断し，自動的に防ぐものもある．IDS は監視対象を基準としてホストベースとネットワークベースに分類することができる．

### 2.2 ホストベース IDS

図 1 はホストベース IDS の構成例を示したものである．ホストベース IDS は監査対象となるホスト上で動作し，OS や アプリケーションのログを入力情報とする．主に不正ログインや不正行為を検出することを目的とし，ログイン中のユーザの挙動を監視する．しかしながらインストールされたホスト以外の情報は得ることができないことから，図に示したように監査対象となるホストすべてにソフトウェアをインストールする必要がある．

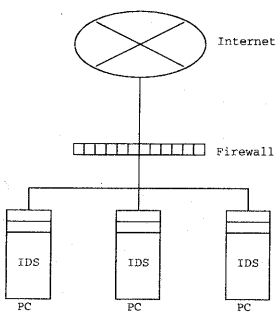


図 1 ホストベース IDS の例

### 2.3 ネットワークベース IDS

図 2 はネットワークベース IDS の構成例を示したものである．ネットワークベース IDS はネットワーク上の専用コンピュータにインストールされ，ネットワークに流れるパケットを入力情報とする．ルータとリピータハブで接続し，ネットワーク内のパケットを取り込むことが可能なように配置する必要がある．不正アクセスの他，ネットワーク資源に対する攻撃も検出できる．ネットワークに流れるすべてのパケットを監視することから，監査対象となるネットワーク全体のホストを監視することができる．しかし，ネットワークをまたぐことなく，ホストに直接ログインしているユーザの不正行為は検出できない．さらにネットワークが輻輳状態にある場合，検出率が低下するという欠点がある．

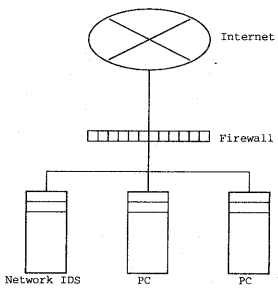


図 2 ネットワークベース IDS の例

### 2.4 IDS の課題

IDS の設置や運用にはセキュリティやネットワークの専門的な知識が必要となる．通常 IDS を初期設定に従って利用すると，図 3 のようにアラートが大量に表示されて真に必要な情報を特定することができない．管理者は真に不正な行為をこのような情報の中から特定する必要がある．また，対処法についても適切に与えられることはないために攻撃を特定した後に対処法を調べて対応する必要がある．

一般的に IDS はシグネチャと呼ばれる定義ファイルによって不正アクセスや疑わしいパケットを検出する．したがってシグネチャの更新を怠れば最新の侵入や攻撃パターンを検出することができない．すなわちシグネチャは常に最新の状態となっている必要がある．

このように IDS を設置・管理するには専門的な知識が必要であり，一般的には有効に活用できない．そこで IDS をリモートから監視し，セキュリティ管理能力のある者が解析して具体的な対策をネットワーク管理者へ報告するシステムとして，IIJ ネットワーク侵入検知サービス[2]，EDSS[3]，Managed Intrusion Detection サービス[4]，bigdog[5]，Hawk-1[6] などが既にサービスを開始している．しかしこれらのサービスは基本的に IDS を監

視対象となるネットワーク内に設置する必要があり，センターへの送信内容もアラートのみである．

本稿で提案するシステムは，セキュリティ管理運用能力を必ずしも必要としない管理者においてさえ，運用可能な方式となっている．IDS の設置を必要とせず，センターへはパケットそのものを送信するので，導入時のコストが低くより詳細に解析できるシステムとなっている．

図 3　IDS のアラート例

## 3. センター管理型不正アクセス検知システム

### 3.1 原　　理

IDS の管理・運用の困難さを解決するためにリモート監視による不正アクセス検知システムを提案する．図 4 は提案システムの全体図を示したものである．本システムはファイル改ざん検出部，パケット収集部，不正アクセス解析部からなる．ファイル改ざん検出部では重要なファイルが改ざんされていないかを定期的にチェックする．改ざんを検出すればパケット収集部に通知する．パケット収集部では改ざん通知によりそれ以前に収集したパケットを不正アクセス解析部に暗号化して送信する．不正アクセス解析部では受信したパケットを復号し，IDS により解析する．不正アクセス解析部ではセンター側でのエキスパートシステムが，解析結果を基に具体的な対処方法を与える．そのレポートをネットワーク管理者にメールと Web で通知する．

本方式では監査したいネットワークにパケットを収集するエージェントを設置しセンターからのレポートを受け取り，そのレポートの指示に基づいて対策を与える方式である．

表 1　提案システムと従来の IDS の比較表

| | 提案システム | 従来の IDS |
|---|---|---|
| シグネチャの更新 | 不要 | 必要 |
| 解析結果 | 整理されたレポート | 大量のアラート |
| 設定 | 不要 | 必要 |
| セキュリティに関する知識 | 不要 | 必要 |
| 初期の異常判定の確実性 | あり | なし |

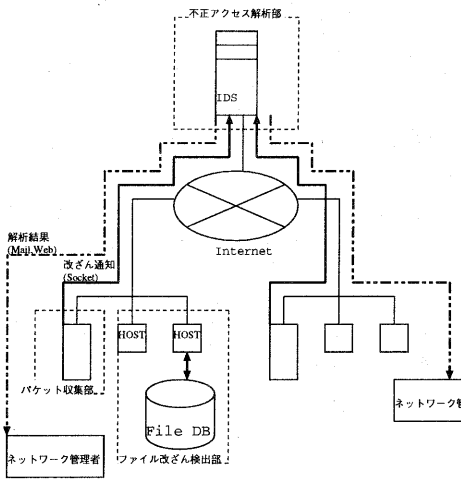


図 4　システムの全体図

### 3.2 ファイル改ざん検知部

ファイル改ざん検出部は，監査対象となるネットワーク内のサーバ上で動作し，ファイルが不正に改ざんされていないかどうかを検査する．不正アクセスによる重大な被害が生じた場合，通常侵入者はファイルを書き換えることになる．このファイル改ざんを検出することにより侵入を検知することが可能となる．しかしながらすべてのファイルに対する改ざんの有無の検査には多大な時間を必要とし，リアルタイムでの検知には適当でない．またシステムに対しても多大な負荷が掛かるため，他のプロセスの実行に影響を及ぼしてしまう．したがって重大な影響を与えるファイル改ざんの検査のみを対象とすることが考えられる．ファイルの改ざんを検出すると，ファイル改ざん検出部はパケット収集部に対して改ざんの有無とその特定を通知する．

### 3.3 パケット収集部

パケット収集部は監査対象となるネットワーク内に常駐し，不正アクセス解析のためにすべてのパケットを収集して保存する．パケットの保存においては時間等をインデックスとしてデータベース化する．ファイル改ざん検出部からの改ざん検出の通知により不正アクセス解析部にパケットを送信する．パケットはファイル改ざんが検出された時点のパケットファイルを送信し，必要であれば不正アクセス解析部との通信によりそれ以前のパケットも送信する．通信量低減のため，送出するパケットには圧縮が施され，また通信路上の盗聴，改ざんを防ぐためディジタル署名を含む暗号化を行う．

### 3.4 不正アクセス解析部

不正アクセス解析部と監査対象となるネットワークとはインターネットで接続されており，パケット収集部か

ら受信したファイルを基に一括して不正アクセスを検出・解析する．不正アクセスの検出・解析には，通常の IDS を利用し，IDS から出力される情報を更に分析・解析し，監視対象となるネットワークに対して本質的に重要となる情報のみ，管理者に送出する．なお，パケット収集部との通信は逐次的に行うものとして，必要であれば解析時点のパケット以前にさかのぼってパケットの取得を行う．センターからの解析結果は，その重要度，および対策方法を含めて通知される．通知はメールや Web を利用する．

## 4. 提案システムの実装

### 4.1 実験環境

図 5 に実験環境のネットワーク構成図を示す．

- ファイル改ざん検出部，パケット収集部
  - CPU：PentiumIII 1GHz
  - Memory:256MByte
  - OS:FreeBSD4.5-RELEASE
  - HDD:ATA100
  - Network:Fast Ethernet
- 不正アクセス解析部
  - CPU：PentiumIII 1GHz
  - Memory:256MByte
  - OS:FreeBSD4.5-RELEASE
  - Network:Fast Ethernet
  - Web Server:Apache

今回の実験ではファイル改ざん検出部とパケット収集部は同一マシンを使用している．

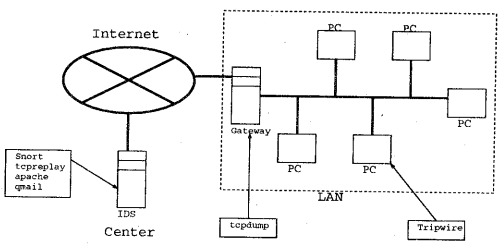


図 5 ネットワーク図

### 4.2 ファイル改ざん検出部

ファイル改ざん検出部は監査対象となるサーバ上で動作し，Tripwire [7] を用いて定期的にファイル改ざんを検出する．ファイル改ざんを検出すれば，パケット収集部へ通知する．

Tripwire は指定したファイルやディレクトリ中のファイル群の MD5 値や最終アクセス時間，最終更新時間などの変更を検査・通知するプログラムである．Tripwire を実行すると設定ファイルに指定されたファイルやディレクトリ中のファイル群をスキャンして得られた情報をデータベースファイルに格納する．ファイルの整合性を調べるオプションを付けて実行すると指定されたファイルの情報とデータベースとの情報を比較し，更新されていたり，追加・削除があればその旨を通知する．今回の実験環境では Tripwire の初期設定での検査時間は約 90 秒で検査対象ファイル数は 34770 個であった．

今回のシステムでは不正アクセスの発見をファイルの改ざんを検出することにより行う．ここですべてのファイルに対して改ざんの検出を行うと多大な時間を要しシステムにも多大な負荷を掛けるため，ファイルを選定する必要がある．以下に改ざん検出対象となるファイルの選択方法を挙げる．

- ネットワーク管理者が選択

この方法では OS 毎に検出対象となるファイルのひな型を作成しておき，ネットワーク管理者がその中から選択する方法である．

- 外部からのアクセスにより改ざんされたファイル

この方法ではネットワークを使った外部からのアクセスでファイルを変更された場合に改ざんとみなす方法である．

- 過去との相関関係を見る

この方法ではファイルが変更された時間を記録しておき，更新頻度の低いファイルが変更された場合に改ざんとみなす方法である．

- ユーザプロファイルを用いる

この方法ではユーザ毎にプロファイルを作成しユーザ毎の更新履歴を記録しておき，更新頻度の低いファイルが変更された場合に改ざんとみなす方法である．

提案システムでは Perl [13] 言語を用いて，各コマンドの呼び出しやネットワーク通信を行う．

ファイル改ざん検出部では Perl のシステムコールを用いて Tripwire を定期的に起動し，ファイルの改ざんや追加・削除がないかチェックする．Perl は子プロセスとして任意のコマンドを起動でき，標準出力を文字列として取り出すことが可能である．この機能を用いて，Tripwire の結果を Perl 上で文字列として取得する．その文字列をシステムのソケットを通して，パケット収集部に送信する．図 6 はファイル改ざん検出部とパケット収集部の間の通信のイメージ図である．

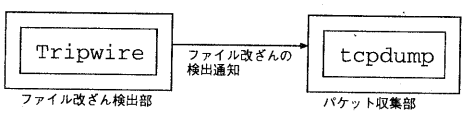


図 6 ファイル改ざん検出部・パケット収集部間の通信

### 4.3 パケット収集部

パケット収集部では Perl のシステムコールを用いて tcpdump を実行し，一定時間 (今回は 120 秒) 毎に保存ファイル名を変更してパケットを収集する．パケットのファイル名には保存された日時が分かるように，2002 年 6 月 7 日 12 時 34 分ならば 200206071234.p というファイル名が付けられる．tcpdump は指定したネットワークインタフェース上で取得可能なすべてのパケットを表示，保存することが可能である．取得したパケットは保存する際にディスク容量の節約や後の通信量の低減のために bzip2 [9] 形式で圧縮を施しておく．不正アクセスを検知するためにはネットワーク内に外部から流れてくるパケットを全て取得しなければならないため，インタフェースをプロミスカス・モードで動作させる必要がある．

また別プロセスでファイル改ざん検出部からの通信を待つ必要がある．このプロセスはファイル改ざん検出部から Tripwire の出力結果の文字列を受信するとそれを解析し，どのような改ざんが行われたか知る必要がある．例えば以下のような文字列を受信したとする．

```
added: -rwxr-xr-x root 3132 (null) /usr/local/bin/ruby16
changed: -rw-r--r-- root 140453 (null) /usr/share/man/whatis
```

この警告は /usr/local/bin/ruby16 というファイルが追加され/usr/share/man/whatis というファイルが変更されたということを示している．つまり “added:” や “changed:” といった最初の文字列によってどのようなことが行われたか分かり，最後の文字列で追加・変更されたファイルが分かる．このようにファイル改ざん検出部から送られてきた文字列を解析することにより，ファイル改ざんを知ることができる．

ファイル改ざんが通知されると，パケット収集部ではアクセス解析部にコネクションを確立する．コネクション確立後は保存しておいた送信すべきパケットを PGP(Pretty Good Privacy) [10] により暗号化し，ソケットを通して不正アクセス解析部に送信する．PGP は主に電子メールで利用されている公開鍵暗号を使った暗号方式である．PGP では送信すべきデータに対して受信側が公開している公開鍵を使って暗号化する．暗号化されたデータは受信側が保有している秘密鍵でのみ復号可能なため，盗聴を防ぐことが可能であり，ディジタル署名を施せるため改ざんも防ぐことが可能である．このようにして暗号化されたファイルを不正アクセス解析部に送信する．図 7 にパケット収集部と不正アクセス解析部の間の通信のイメージ図を示す．

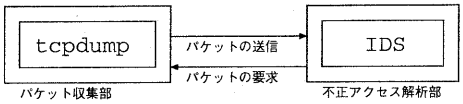


図 7 パケット収集部・不正アクセス解析部間の通信

### 4.4 不正アクセス解析部

不正アクセス解析部ではパケット収集部からの通信をソケットを用いて待ち受ける．受信した暗号化・圧縮されたパケットを Perl から PGP と bzip2 を呼び出すことによって復号する．復号されたファイルは tcpdump によって保存されたデータであるので，tcpreplay [11] というツールを用いると再生することができる．tcpreplay はオプションを付けずに実行すると，現在使用しているネットワークカードが出すことが可能な最高速度でパケットを再生することができるため，高速に不正アクセスを解析することが可能である．

tcpreplay により 再生されたトラヒックは，IDS を使って解析される．本稿では Snort [12] を利用する．Snort は GPL のもと Freeware として公開されているホストベースとネットワークベースの両方の機能を持つ IDS である．Snort はシグネチャマッチングを用いて不正アクセスを検知する．この Snort を用いたセキュリティに関するエキスパートシステムが，不正アクセスを解析する．

解析結果を通知するにはメールと Web を用いるが，今回はそれぞれ qmail と Apache を用いた．

### 4.5 提案システムに対する諸考察

実装する上で考察すべき点を以下に挙げる．

#### 4.5.1 ファイル改ざんのチェック間隔

現在の実験環境の場合，重要なファイルのチェックに約 90 秒かかるが，この時間は環境によって変化すると思われる．また改ざんチェックによるシステムへの負荷も考えられ，常にチェックしていると他のプロセスの妨げとなってしまう．現在は 1 時間毎にチェックするようにしているが，最適なチェック間隔ついては運用実験で評価したい．

#### 4.5.2 Tripwire の データベースファイルの管理

Tripwire は検査対象となるファイルの情報をデータベースファイルに保存しておくが，このファイルを改ざんされると正常に検出できない．読み出し専用のメディアに保存しておくなどし，データベースファイルの管理は厳重にする必要がある．

#### 4.5.3 ネットワークの高負荷状態および通信不能時

DoS 攻撃などを受けてネットワークが使用不能になった場合，不正アクセス解析部にパケットを送信できないため解析が不能となってしまう．そのために，緊急時に備えて別ネットワークを用意しておく必要がある．

#### 4.5.4 解析結果の通知方法

これも上記と同じ理由で，ネットワークが使えない場合，メールとWebを管理者は見ることができないため解析結果を知ることができない．これについてはインターネット以外の媒体を使った，例えば電話やFAXなどを用いた連絡方法を用意しておくことで対処できる．

#### 4.5.5 パケットファイルの保存

本システムでは不正アクセスを完全に検知するために，ネットワーク上を流れるパケットをすべてキャプチャする必要がある．またセンター側からの要求に応じるために，パケットは保存しておく必要もある．そのためパケットに圧縮を施すとしても保存容量には限界があるので，一定期間経ったファイルまたは一定容量に達した場合に削除しなければならない．

#### 4.5.6 既存のサービスとの比較

既存のネットワーク遠隔監視システムは一般的にリモートにある監視センターで管理対象となるネットワーク内にあるFirewallやIDSのアラート情報を受け取り，セキュリティ管理能力のある者が解析する．攻撃元や攻撃手法を特定すると，それらに対する対策手法をネットワーク管理者に通知したり遠隔からポートを遮断したりする．

表2は提案システムと既存のシステムについて比較を行ったものである．

表2 既存のシステムとの比較表

| | 提案システム | 既存のシステム |
|---|---|---|
| IDSの設置位置 | センター側 | 管理ネットワーク内 |
| センターへの送信内容 | パケット | アラート情報 |

本システムは表2で示したように，IDSの設置位置とセンターへの送信内容が既存のシステムと異なる．IDSの設置位置では管理領域毎にIDSを設置しないので，IDSの設定やシグネチャの更新などのメンテナンス作業の必要がない．またIDSの導入自体の必要がないので，コストの削減にもつながる．センターへの送信内容であるが，アラートの場合は現在のIDSは完全に不正アクセスを検知することができないので，取りこぼしが発生してしまう．それに対しパケット自体を送信する場合は通信内容がすべて分かるため，より詳細な解析が可能である．センター側に複数の種類のIDSを用意することにより，IDSが1台しかない場合に比べ検出もれを防ぐことも可能である．またセンター側で被害判定予測システムのようなエキスパートシステムを用いることにより，不正アクセスの解析を自動化することができる．

## 5. むすび

本稿ではリモートで不正アクセスを検知するシステムの提案をし，その有効性や既存のシステムとの比較により優位性について述べた．またそのシステムの実装概要を述べた．そこで，今後の課題として本稿ではTripwireやSnort等のツールを用いる方法を一例として述べたが，これらと同等以上の機能を持つ他のツールを利用しセンター集中管理モデルを実現することも可能と考えられる．またIDSは複数提案，さらに製品化されており，それぞれが特徴を有している．そこで，センター側のIDSに多機能，多機種かつ高性能なIDSを複数並列分散的に稼働させることによって検知率の向上を確認することである．

## 謝　辞

有益な御討論を頂いた中尾康二氏を始めとするKDDI研究所ネットワークセキュリティグループの各位に感謝する．

## 文　献

[1] 大塚丈司, 白石善明, 森井昌克, “リモート監視による不正アクセス検知について,” 信学技報, Technical Report of IEICE, OIS2002-5 (2002-5).
[2] IIJ ネットワーク侵入検知サービス, “http://www.iij.ad.jp/service/index-IIJ-NID.html”
[3] EDSS(Enterprise Datacenter Support Service), “http://www.hucom.co.jp/service/service.html”
[4] Managed Intrusion Detection サービス, “http://www.networld.co.jp/service/security.htm”
[5] bigdog, “http://www.nttdata-sec.co.jp/service/kanshi.html”
[6] Hawk-1, “http://www.gtisec.net/service/hawk_1.html”
[7] Tripwire, Inc., “http://www.tripwire.com/”
[8] TCPDUMP public repository, “http://www.tcpdump.org/”
[9] The bzip2 and libbzip2 official home page, “http://sources.redhat.com/bzip2/”
[10] Network Associates, “http://www.pgp.com/”
[11] SourceForge Project Info - tcpreplay -, “http://sourceforge.net/projects/tcpreplay/”
[12] Snort, “http://www.snort.org”
[13] Larry Wall and Randal L.Schwarts, 近藤嘉雪 “Perl プログラミング,” ソフトバンク株式会社, 東京, 1993.