開放型大規模ネットワークのためのIDSログ監視支援システム

沢田篤史[†] 高倉弘喜[†] 岡部寿男[†]

大学などの教育研究機関に展開されるネットワークでは，ネットワーク管理を担う人材の不足とあいまって，セキュリティの維持管理にかかる負担が深刻な問題となっており，IDSなどセキュリティ製品への期待が増大している．しかしながら，このような機関のネットワークには組織の性質上高い開放性が求められる場合があり，IDS製品を導入することが必ずしもセキュリティ監視業務の省力化に直結しないことが多い．本研究では，大規模で開放性の高いネットワークにおいてIDSを実際に運用して得られた経験に基づき，膨大なIDSログからの不正アクセス抽出作業を支援する通報・検索システムを構築した．本システムは現在我々のネットワーク監視業務の中で利用され，不正アクセス検出の省力化に貢献している．

A Support System for Monitoring Log Information of IDS Applied to Large Scaled Open Networks

Atsushi Sawada,[†] Hiroki Takakura[†] and Yasuo Okabe[†]

Recently, large scaled open networks such as university networks are suffering from increasing attacks caused by viruses, worms, and remote attackers. Since it is very hard work to keep such networks in secure, administrators tend to expect that security products such as intrusion detection system (IDS) may reduce the amount of their work. However, an IDS applied to the network actually increases administrator's job with huge amount of log information. This paper summarizes our experiences on managing and maintaining an IDS applied to our large scaled open network. Based on these experiences, we have designed and developed a support system for monitoring log information of IDS. The system has been practically utilized in our network and helps administrators to analyze and detect misuses or intrusions.

1. はじめに

本稿は，2000年8月から2002年11月まで著者らの所属する組織のネットワークにおいて侵入検知システム（IDS）を運用して得られた知見と，それに基づいて開発したIDSログ監視支援システムおよびその運用実績についてまとめたものである．

インターネット上での不正アクセスやウィルス・ワーム被害の増大にともない，IDSの研究開発が活性化し，主に不正検出（misuse detection）型のIDSが商用化され，広く利用されるようになってきた[1)]．これらIDS製品の多くは，監視対象のネットワークがファイアウォールなどにより一定の安全対策が施されていることを前提としており，不正事象（以下，インシデントと呼ぶ）を漏れなく検出するよう設計されている．

一方，大学などの教育研究機関に展開されるネットワークでは，ネットワーク管理を担う人材の不足[2)]とあいまって，セキュリティの維持管理にかかる負担が深刻な問題となっており，IDSなどセキュリティ製品への期待が増大している．しかしながら，このような機関のネットワークには組織の性質上高い開放性が求められる場合があり，IDS製品を導入することが必ずしもセキュリティ監視業務の省力化に直結しないことが多い．

本研究では，大規模で開放性の高いネットワークにおいてIDSを実際に運用して得られた経験に基づき，膨大なIDSログからの不正アクセス抽出作業を支援する通報・検索システムを構築した．本システムは現在我々のネットワーク監視業務の中で運用され，不正アクセス検出の省力化に貢献している．

以下，2章では，IDSの運用実績とそこで得られた知見についてまとめ，3章でログ監視支援システムの開発について述べる．さらに4章では，運用実績に基づいたシステムの評価と問題点の考察を行い，5章で本稿のまとめをする．

† 京都大学
Kyoto University

2. 開放型大規模ネットワークにおける IDS の運用

我々の所属組織のネットワークでは，1999 年 3 月に IDS を導入，1 年余の試用と調整の期間を経て，2000 年 6 月より本格運用を開始した．その後，2001 年 11 月に行われた新バックボーンネットワークの整備とともに IDS 機能の大幅拡充を行い，2002 年 8 月より新しいネットワーク構成において IDS の本格運用を開始した．以下，本章では 2002 年 8 月以前の第 1 期と以降の第 2 期とに分けて IDS の運用形態と実績を説明した後，運用上明らかとなった問題点についてまとめる．

2.1 第 1 期の運用（2000 年 6 月〜2002 年 7 月）

第 1 期に導入した IDS の機種は Cisco 社の NetRanger（現 Cisco Secure IDS[3]）で，シグネチャ（signature）と呼ばれる典型的なパターンに基づきインシデントの検出を行うものである．1 つのインシデントは，タイムスタンプ，シグネチャID，送信 IP アドレス，受信 IP アドレス，送信 TCP ポート番号，受信 TCP ポート番号，ペイロード，メッセージなどの組で記録される．シグネチャには 5 段階の危険レベルが設定されており，レベル 5 が最大の危険度を示すものとされる．第 1 期の運用構成を**図 1** に示す．IDS センサ 1 台が帯域 100 Mbps の対外接続線の監視を行い，検出したインシデントは独自フォーマットのログとして IDS ディレクタへ送られる．ディレクタでは，インシデントのシグネチャあるいはレベルごとに様々な動作を指定することができるが，運用においてはレベル 4 および 5 の事象を管理者メーリングリストへ通報する設定とした．

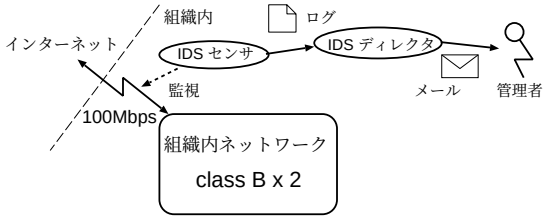

図 1 第 1 期の構成
Fig. 1 IDS deployment at first phase.

なお，組織内のネットワークは，クラス B（16 ビットマスク）2 個分のグローバルアドレス空間を持ち，インターネットとの境界はいくつかの例外を除き，ほぼすべてのトランスポート層プロトコルで通信が可能であった．

図 2 に，2000 年 8 月から 2002 年 8 月までの間，レベル 4 および 5 として検出されたインシデントを 1 週間ごとに合計した数の推移を示す．グラフ中の実線はディレクタが電子メールで管理者に通報したインシデントの数を示す．最大では週あたり 17,460 件（2001

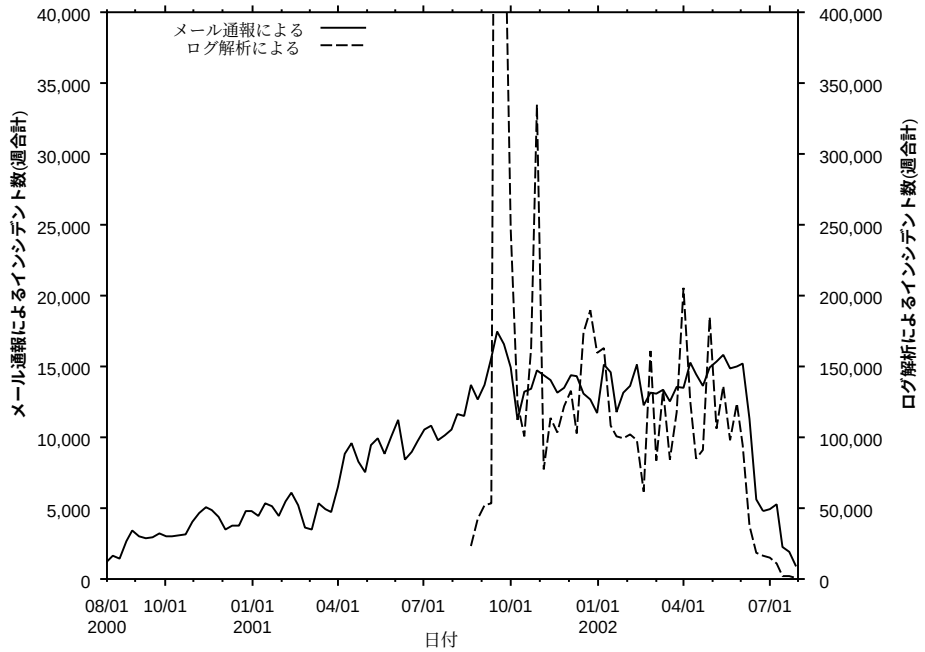

図 2 インシデント数（第 1 期・レベル 4，5・週合計）
Fig. 2 Number of incidents (first phase, level 4 and 5, weekly total).

年 9 月 17 日〜23 日）のインシデントがメールで管理者に通報された．ディレクタのメール通報はセンサが検出したインシデントとほぼ 1 対 1 に対応する設定であることから，平均すると，1 日あたり 2,494 通，1 時間あたり 104 通のメールが丸 1 週間届き続けた計算になる．

一方，破線は IDS センサが IDS ディレクタに送付するログファイルをオフラインで解析し，レベル 4 および 5 のインシデント数を週ごとに合計したものである．縦軸のスケールの違いに注意すると，センサの検出するインシデント数は，ディレクタが管理者に通報するもののほぼ 8 倍から 10 倍程度にのぼっていたことが分かる．なお，ピーク値は，2001 年 9 月 17 日〜23 日の週あたり 1,091,027 件で，1 時間あたりの平均発生件数は 6,494 件となっている．

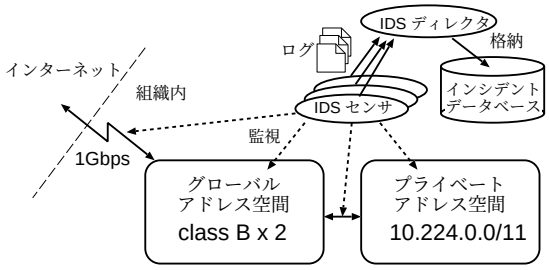

図 3 第 2 期の構成
Fig. 3 IDS deployment at second phase.

2.2 第 2 期の運用（2002 年 8 月〜）

第 2 期では，第 1 期との継続性に配慮し，第 1 期に導入機器の能力を改善した後継機種（Cisco 社の Cisco Secure IDS 4230 および同 Catalyst 6000 Module）を導入した．第 2 期の構成を**図 3** に示す．組織内のネットワークでは，既存のクラス B 2 個分のグローバルアドレス空間に加え，新たに 11 ビットマスク（10.224.0.0/11）のプライベートアドレス空間が構築された．IDS センサは合計 20 台が分散配置され，1 Gbps に増速されたグローバルアドレス空間とインターネットの間のトラフィックだけでなく，グローバル–プライベート間，グローバル内のサブネット間，プライベート内のサブネット間のトラフィック監視も行うようにした．IDS ディレクタは第 1 期同様 1 台で，各センサからのログが集約される構成である．さらに，ディレクタと連携しインシデントを格納することのできるデータベースを新たに導入し，危険レベル 3 以上の事象を格納し，電子メールによる管理者への通報は行わないよう設定した．

図 4 に，2002 年 8 月 6 日から 11 月 25 日の間に検出されたレベル 3〜5 のインシデント数を日ごとに合計したグラフを示す．実線が 1 日ごとのインシデント数の合計の推移，一点鎖線は 1 週間で平均した 1 日

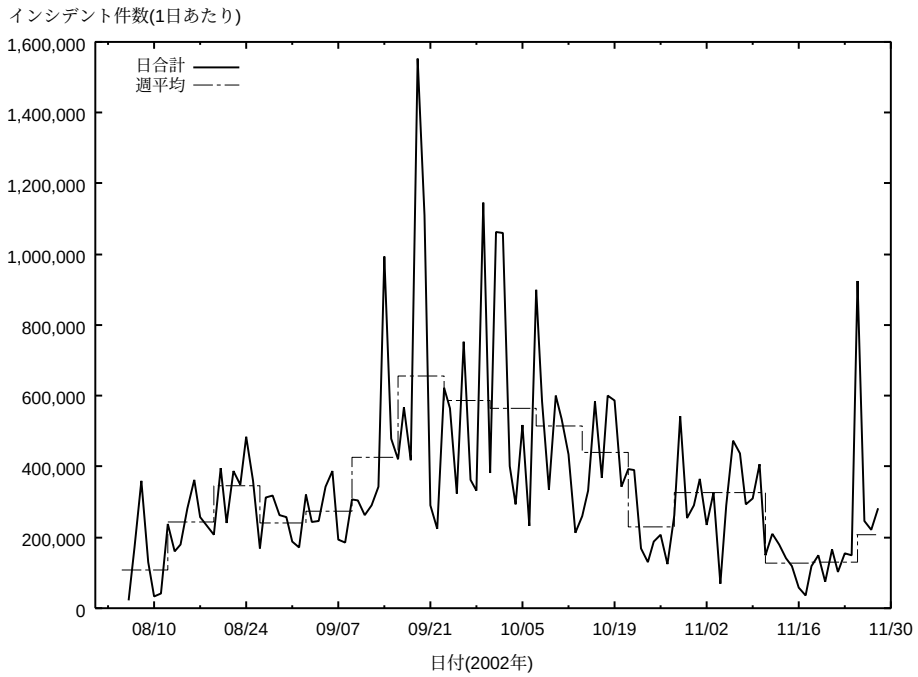

図 4 インシデント数（第 2 期・レベル 3，4，5・日合計）
Fig. 4 Number of incidents (second phase, level 3, 4, and 5, daily total).

あたりの数を示す．ピーク値は 2002 年 9 月 19 日の 1,553,481 件で，1 時間あたりの平均発生件数は 64,728 件となっている．また，1 週間あたりの合計インシデント数のピークは 2002 年 9 月 16 日〜22 日の 4,583,989 件で，第 1 期のピーク値の約 4.2 倍にのぼる．

2.3 メール通報システムのかかえる問題

第 1 期の運用を通じて，IDS ディレクタによるメール通報システムの次の問題点が明らかになった．

- 警報メール数の問題
- 警報メールとインシデントとの対応関係の問題
- 通報の精度の問題

第 1 の問題は，図 2 のグラフに基づいて説明したように，大量の警報メールが管理者に送信される点である．これは，不正検出から通報にいたる処理のリアルタイム性を重視してシステムが設計されていることに起因するものと考えられるが，大量送信の結果，メーリングリスト配送サーバや配送経路が過負荷となり，かえってリアルタイム性を損なうような事態も発生した．

また，警報メールが 1 時間に 100 通にものぼる状況では，管理者がすべてのメールを精査することができなくなり，どこで何が起こっているのかを把握することが困難となってしまう．平時には不正事象がほとんど検出されないネットワークであっても，ウィルスやワームの集団感染により，インシデントが多発するような緊急時においては，同様の状況に陥ることも十分予想される．

第 2 の問題は，1 通の警報メールにより通報されるのが基本的に 1 件のインシデントのみである点である．実際の不正アクセス発見では，複数のシグネチャの組合せや，発生の順序関係，IP アドレスの関係などが有力な手がかりとなるが，別々のメールに細切れにすることで複数のインシデントのつながりが見えにくくなってしまう．

第 3 に，通報の精度の問題がある．図 2 で示したように，IDS センサが検知するインシデント数と，メールにより通報されるインシデント数には大きな開きが生じた．プログラムの仕様が明らかになっていないため，IDS ディレクタがメール通報するインシデントを選ぶアルゴリズムは不明だが，リアルタイム性を高めるため単純な方式を採用しているものと推測される．我々がこの問題を認知したのは，“Code Red” および “Code Red II” ワームが流行した際（2001 年 8 月），特定の感染ホストからの継続的な不正アクセスに対して，それを通報する警報メールが間欠的にしか届かない現象が頻発したことによる．これは，監視対象のトラフィックの増大にともなう IDS の検出性能の低下現象[4] ととらえることもできるため，システム全体の中でボトルネックとなる部分を特定し，高負荷の要因を取り除く対策が必要となる．

通報の精度を改善することは重要であるが，IDS がすべてのインシデントについて残さず通報できるようになると，第 1 点目の問題としてあげた警報メールの数や頻度がさらに増大し，管理者の負荷がかえって増大する結果を招く．このため，シグネチャの種類や送信アドレス，受信アドレスなど，インシデントの内容に対する関心度の高さに応じて，適切なフィルタリングを行ったうえで管理者に通報する機能が重要となるが，このような機能が備わっていない点も問題となる．

2.4 シグネチャによる検出方式のかかえる問題

インシデントをシグネチャに基づいて検出する方式の問題は，シグネチャと不正アクセスとが必ずしも 1 対 1 に対応しない点にある．これは，攻撃ツールやウィルス，ワームなどが複数の脆弱性を利用するようになってきたことに起因し，近年深刻な問題となっている．

たとえば “Nimda” ワームによる不正アクセスは，我々の運用する IDS では 5 種類のシグネチャの組合せで検出することができる．それぞれのシグネチャのインシデントは平常時にも単独で多数検出されるが，5 種類のインシデントが同時に同じ送信アドレスに関して多数観測されたときにはじめて “Nimda” であると判定できる．このように同じアドレスに関するシグネチャの組合せパターンで不正アクセスの発見を支援する仕組みは，通常の IDS 製品には備わっておらず，監視には一定レベルの知識と習熟が必要となる．

2.5 インシデントデータベースのかかえる問題

第 2 期の IDS 運用では，IDS センサが検出したインシデントを格納するインシデントデータベースを導入した．バックエンドには商用の関係データベース管理システムが用いられており，個々のインシデントは検出時に IDS ディレクタから個々のタプルとしてデータベースに登録される．

インシデントデータベースの問題は，データベースに登録されるインシデントの多さと登録の頻度に起因する．第 2 期の運用に関して図 4 で説明したとおり，ピーク時で 1 時間あたり平均で約 65,000 件にのぼる登録クエリが丸 1 日の間継続して発行されることになる．我々の IDS では，バックエンドデータベースの稼働する計算機において，この頻度のトランザクションを滞りなく処理するためのリソースが不足しているため，慢性的な過負荷状態に陥っている．

2.6 インシデント閲覧システムのかかえる問題

IDS ディレクタは，OpenView[5] に基づく GUI でインシデントを閲覧する機能を提供する．GUI による視覚化は直観的に不正アクセス状況を把握するのに有効であるが，この利点もインシデント数が極度に大きくなると無力化する．アイコンでインシデントを表現する方式では，重要なインシデントが多数のアイコンの中に埋没してしまう．OpenView ではズーム機能や階層化機能を利用することで，一定のスケーラビリティを持たせることができるが，階層を深くすればそれだけ個々のインシデントが階層の奥に埋没することになる．

また，専従の管理者が存在せず，複数の管理者で分散してログ監視を行うような組織においては，インシデント閲覧システムから情報を引き出すプル型の情報提供手段のみでは監視が疎かになりがちであるという問題も存在する．

さらに，既存の GUI によるインシデント閲覧システムは，一般に多くの計算機リソースを必要とする．このため，同時に閲覧システムを起動する管理者数が増えると閲覧の性能が極端に低下したり，遠隔から低速のネットワーク回線を介した監視業務には適さなかったりするという問題がある．また，IDS ディレクタの提供する閲覧システムは，専用の GUI ライブラリを前提としているため，そのライブラリがインストールされた計算機上でしか動作しない，あるいは監視に使用する計算機ごとにライセンス料が必要となるなど，地理的に分散した管理者が共同で監視する形態をとる組織には向かない点も問題であると考えられる．

2.7 IDS 運用上の問題点のまとめ

これまでに説明した運用経験をまとめると，開放型大規模ネットワークにおいて IDS を運用する上での問題点は次の 3 つの項目に大別することができる．

(1) 大量インシデントとその取扱いの問題
(2) インシデント情報のフィルタリングの問題
(3) 分散監視体制への対応の問題

大量のインシデントが検出され，それを IDS が適切に扱えないことに起因して，

- 警報メールの頻度や量が過剰となり監視の負荷が増大する，
- 通報の精度が低下する，
- データベースが過負荷となる，
- GUI による閲覧が困難となる，

といった問題が生じ，大量のインシデント情報に対するフィルタリング機能が貧弱であることに起因して，

- インシデントの内容に対する関心度に応じた情報抽出が困難となる，
- 複数のシグネチャの組合せなどによるインシデント間の関係把握が困難となる，

という問題が生じている．また，IDS が専従の管理者を設けない分散監視体制を前提として設計されていないために，システムの運用には専用の GUI ライブラリや商用のデータベースシステムを用いた閉鎖的な環境が必要で，これに起因して，

- 複数人による同時監視により GUI 性能が低下する，
- 分散監視体制での運用に追加のライセンス料が必要となる，
- 遠隔から低速ネットワークを介した監視に適さない，

という問題が生じている．

3. IDS ログ監視支援システムの構築

前章で説明した運用経験と問題意識に基づいて，我々は IDS の実運用と並行してログ監視を支援するシステムの構築と改善を行っている．システムの設計と構築は次の方針に従ってすすめた．

(1) 管理者へのプッシュ型の通報手段を重視する．
専従の監視者が存在しない場合，プル型の監視は成り立たない．メールによる通報を主な手段とした設計を行う．

(2) 管理者への通報頻度を極端に大きくしない．
通報のリアルタイム性にはこだわらず，適切な間隔でその間に起きたインシデントのとりまとめを行う．

(3) 1 回の通報サイズを極端に大きくしないようフィルタリングを行う．
インシデントとりまとめに際して，監視対象のネットワークに対する関心度の高さなどに応じたフィルタリングを行い，内容の一覧性を高める．

(4) 複数インシデント間の関係が把握できる形で情報を提供する．
危険度の高いインシデントのアドレスに注目したとりまとめや，異なるシグネチャにまたがる検索を行えるようにする．

(5) フィルタした情報を補う手段を提供する．
定期的なレポート作成機能やオンデマンドの検索手段を提供する．

(6) 高性能のデータベースサーバを必要としない．
インシデント登録のリアルタイム性にはこだわらず，適切な間隔でインシデントをとりまとめてデータベースに登録することで，過負荷状態

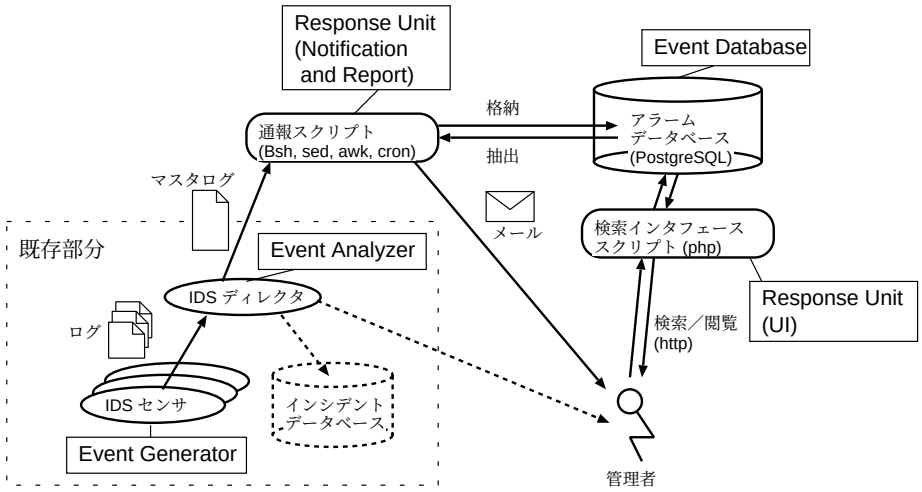

図 5 IDS ログ監視支援システムの構成
Fig. 5 Architecture of the support system for monitoring IDS log information.

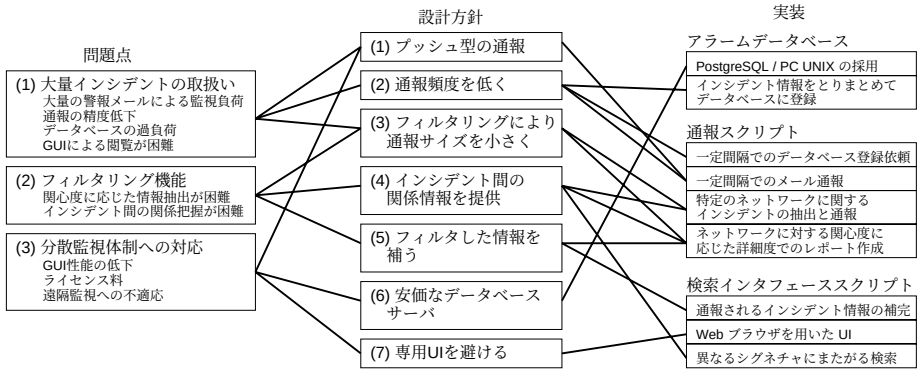

図 6 IDS 運用上の問題点とシステムの設計方針
Fig. 6 IDS management problems and the system design policies.

を避ける．

(7) UI に専用コンソールや専用ソフトウェアを必要としない．
Web ブラウザを用いたデータベース検索/閲覧手段を提供する．

図 5 に，Common Intrusion Detection Framework（CIDF）アーキテクチャ[6] との対比に基づいたシステムの全体構成を示す．IDS ログ監視支援システムでは，IDS ディレクタが担っていたレスポンスユニット☆の機能と，インシデントデータベースが担っていたイベントデータベースの機能を既存のものとは別に新たに構築し，全体への統合を行う．結果として，本システムでは，図中には破線で示した IDS ディレクタの GUI 機能やメール通報機能，インシデントデータベースの利用を行わない構成となっている☆☆．

図 6 には，前章にあげた IDS 運用上の問題点と本支援システムとの関係を示す．図左部には 2.7 節でまとめた問題点が列挙され，それを解決するために立案したシステムの設計方針（中央）と，それに基づいて実装したシステムの機能・特徴（右部）との関係が示されている．本章では以下，システム各部の機能についてより詳細に説明する．

3.1 アラームデータベース

アラームデータベース部は，CIDF アーキテクチャにおけるイベントデータベースの機能を担当する．データベーススキーマの設計は，IDS センサが持つ独自のログ形式にあわせた形で行っている．次節で述べるよ

☆ CIDF アーキテクチャでは侵入検知の報告を受け，管理者への通知や自動遮断措置などの対応を行う部分と規定されている．

☆☆ ただし，これら機能の利用を妨げるものではない．

```
[   suspicious   ]
 sid  | l |     srcaddr     |    dstaddr     |   description    | count
[ 192.168.12.231  ]
 3216 | 4 | 192.216.123.244 | 192.168.12.231 | IIS DOT DOT DENI |    10
 5081 | 4 | 192.216.123.244 | 192.168.12.231 | WWW WinNT cmd.ex |    10
 5124 | 4 | 192.216.123.244 | 192.168.12.231 | WWW IIS Double D |     8
 3215 | 4 | 192.216.123.244 | 192.168.12.231 | IIS DOT DOT EXEC |     1
 3214 | 3 | 192.216.123.244 | 192.168.12.231 | IIS DOT DOT VIEW |     8
[ 192.168.59.159  ]
 2150 | 4 | 68.100.187.5    | 192.168.59.159 | Fragmented ICMP  |     2
 2150 | 4 | 192.168.59.159  | 68.100.187.5   | Fragmented ICMP  |     2
 2151 | 3 | 68.100.187.5    | 192.168.59.159 | Large ICMP       |    21
 2151 | 3 | 192.168.59.159  | 68.100.187.5   | Large ICMP       |    20
....
```

図 7 詳細レポートスクリプトの出力例
Fig. 7 An example of detailed summary report from the system.

表 1 アラームデータベースサーバの仕様
Table 1 Specification of the alarm database server.

CPU	Intel XEON 1.7 GHz × 2
メモリ容量	900 MB
ハードディスク容量	480 GB
OS	Debian/GNU Linux 3.0

うに，通報スクリプト部は，インシデント情報を一定時間間隔でアラームデータベースに登録依頼する機能を有し，アラームデータベースではそれらをとりまとめてデータベースに登録することで，サーバの負荷軽減を図っている（方針 2）．アラームデータベースの DBMS としてはオープンソースの PostgreSQL[7] を採用し，現在は**表 1** に示す仕様の IBM PC/AT 互換機上で動作させているが，過負荷による監視活動への支障などは特に発生していない（方針 6）．

3.2 通報スクリプト

通報スクリプト部は，CIDF アーキテクチャにおけるレスポンスユニットの「通報とレポート」の機能を担当する．管理者への通報機能のほかに，センサが検出したインシデントをアラームデータベースに登録依頼する機能を備える．この機能では，IDS ディレクタのマスタログに蓄えられるインシデント情報を一定時間ごとに取り出すことでデータベースへ依頼する頻度を下げ，負荷軽減を図る（方針 2）．なお，現運用ではデータベース登録の間隔を 3 分に設定している．

また，3 分ごとのデータベースへの登録依頼の際には，新たに登録を行うインシデントのうち，管理者によりあらかじめ指定されるネットワークセグメントに関するもののみを抽出し，同一時刻に検出された同一のシグネチャ，発信アドレス，送信アドレスの組については 1 行にまとめ，その件数とともにメールで通報する機能を備える．これにより一定時間間隔でのプッシュ型の通報を実現（方針 1）し，警報メールの数を抑制する（方針 2）とともに，警報メールのサイズを削減することができる（方針 3）．

さらに，通報スクリプト部には，あるネットワークセグメントに対する関心の高さに応じて 3 種類の詳細度で定期レポートを行うスクリプトが用意されている．管理者があらかじめ関心度別に「大」「中」「小」のネットワークセグメントを指定することで，それぞれの詳細度でレポートを作成することができる．最も詳細なレポートでは，**図 7** に示す形で，危険度の高いインシデントに関わる IP アドレス（`suspicious`）に関して，シグネチャ（`sid, description`），危険レベル（`l`），送信アドレス（`srcaddr`），受信アドレス（`dstaddr`）の組合せでインシデントの発生件数（`count`）を報告する．このような形態でレポートを行うことで，特定の IP アドレスにからんで検出された複数のインシデント間の関係把握が容易になる（方針 4）．我々は，このスクリプトを cron デーモンを用いて 30 分間隔で動作させている．より関心の低いネットワークセグメントに関する情報は，詳細度のより低いレポートスクリプトを低い頻度で動作させることで補完する（方針 5）．なお，現在の運用では，1 時間ごとのレポートで，関心度「中」のネットワークセグメントに関して検出されたインシデントが，シグネチャ，送信アドレス，受信アドレスの組合せで件数の多い順に報告され，3 時間ごとのレポートで，関心度「低」のセグメントに関して，同様の組合せが件数の多い順に 100 件報告されるよう設定している．

3.3 検索インタフェーススクリプト

検索インタフェーススクリプト部では，アラームデータベースを検索するための Web インタフェースを提供する．管理者は，メールで通報されたインシデント情報を補完するためにデータベース検索を行うことができる（方針 5）．データベース検索のスクリプト

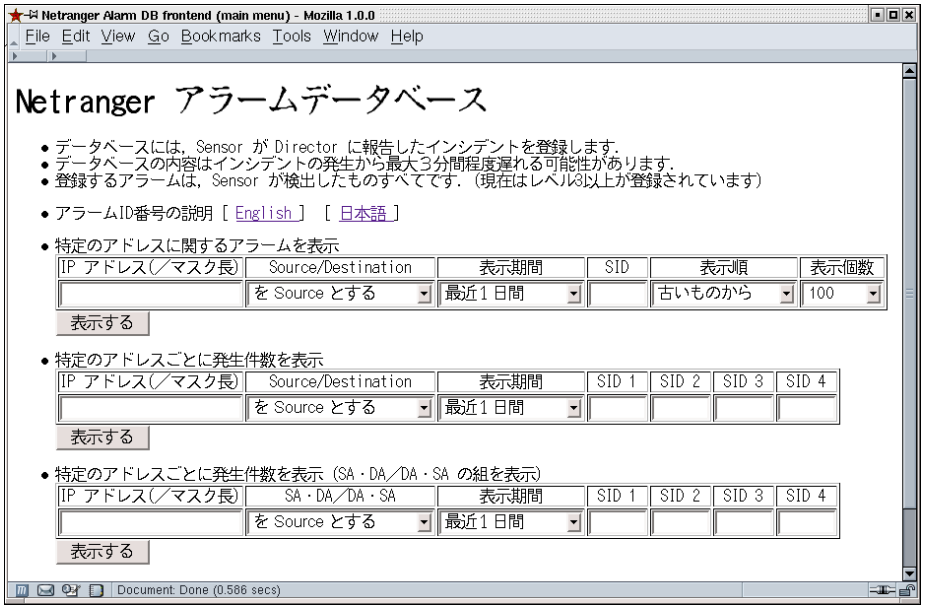

図 8 検索インタフェース
Fig. 8 Browser based user interface for incident information retrieval.

は PHP[8] を用いて作成されているため，Web ブラウザ側には特別な機能を備える必要はなく，データベースに格納されているすべてのインシデントの検索が可能となる（方針 7）．

図 8 に検索入力画面を示す．図下部のインタフェースでは，特定のアドレスまたはアドレス範囲に関して，異なるシグネチャ（SID1〜4 の欄に指定する）にまたがる検索機能を提供し，複数インシデント間の関係について把握が容易になるよう構成されている（方針 4）．

4. 評価と考察

前章で説明した IDS ログ監視支援システムは，2001 年 8 月に初期プロトタイプの運用を開始し，現在も運用を続けながら評価・改善を行っている．本章では，不正アクセスの検出効果と管理者によるログ監視業務の負荷軽減について実例に基づく評価を行った後，システムの一般性に関して考察し，既存の IDS 製品や関連研究との比較を行う．

4.1 不正アクセスの検出効果

表 2 には，システムの初期運用開始から 2002 年 10 月末日までに，組織内部を発信源とする外部への不正アクセスと強く疑われる事象が報告され，ネットワークやホスト管理者に対する初動調査，修復依頼などが行われたのべ回数を示す．組織内部から外部に向けた不正アクセスと疑われる事象が期間中にのべ 76 回発生し，そのうち 84%にあたる 64 回が本システムの通報および閲覧機能により発見された．一方，管理者が本システムによって発見できず，海外，組織内，国内（組織外）からの苦情メールなどにより発覚した事象がそれぞれ 7 回，3 回，2 回となっており，外部に向けた不正アクセス事象を発見するのに本システムが実際に効果を上げていることが分かる．また，本システムを用いて検出された事象に対する初動対策を行った後に，組織外から苦情が寄せられたケースが 3 件記録されている．組織内部からの不正アクセスに対して外部からの苦情や反応が届くまでには一般的に一定の時間を要することから，このケースはシステムを用いた監視が被害の拡大を未然に防いでいることの表れであると考えることもできる．

表 2 不正アクセスが疑われる事象とその報告元
Table 2 Number of exploitation reports grouped by types of reporters.

報告・検出元	回数
本システムによる検出	**64**
海外からの報告	7
組織内からの報告	3
国内からの報告	2
合計	76

※期間 2001 年 8 月 1 日〜2002 年 10 月 31 日

本システムの運用開始までは IDS ログ監視は体系的に行われて来なかったため不正アクセスの検出記録が存在せず，運用前後の定量的な比較は行えないが，運用開始前は外部からの苦情をトリガとして調査対策

表 3 システムから通報されたメールの行数
Table 3 Size of alarm mails from the system.

種別	合計行数	平均行数	メール数
定期通報（3 分間隔）	76,567	160	480
詳細度別レポート（30 分間隔）	13,282	277	48
詳細度別レポート（1 時間間隔）	1,880	78	24
詳細度別レポート（3 時間間隔）	800	100	8

※期間 2002 年 10 月 1 日 0 時〜24 時

を開始したケースがほとんどであったことから，不正アクセスの早期発見と対策にシステムはかなりの効果をあげているといえる．

なお，3.2 節で説明した IDS ログの詳細度別レポート機能は，監視業務担当者の意見を汲み上げる形で追加され，2002 年 10 月より運用を行っている．この機能追加によって，現在では “Nimda” などシグネチャの組合せで攻撃するタイプの不正アクセスを含め，既知のものに関しては発生後 30 分ないしは 1 時間での検出と初動を可能とする支援体制が整っている．

4.2 IDS ログ監視業務の負荷軽減効果

本システムの主な目的は，IDS のログを監視する業務にかかる管理者の負荷を軽減することである．そのための具体的な設計方針として，メールによるプッシュ型の通報形態を保ちつつ（方針 1），メール通報の頻度を低く（方針 2），1 通のメールのサイズを小さくする（方針 3）ことをあげている．本節では監視負荷の軽減効果について，メール数，メール行数の点から評価を行う．

表 3 には，詳細度別レポート機能を現在の設定で運用を開始した 2002 年 10 月以来，1 日あたりの検出インシデント数が最大の 1,062,400 件を記録した 2002 年 10 月 1 日について，3 分ごとのメール通報，および 30 分・1 時間・3 時間ごとの詳細度別レポートとして管理者に送付された警報の行数（ヘッダ部分，表の見出し部分，空行は除く）の合計と平均を示す．

上記 4 種類の通報に含まれなかったインシデントは，検出数上位 100 位までの組合せのインシデントのみを通報する 3 時間間隔の詳細度別レポートにおいて，101 位以下の組合せで，関心度「小」のネットワークに関して検出されたものであり，その総数は 8,879 件となっている．

これらの結果から本システムを利用することで，総数 1,062,400 件のインシデントに対し，99%にあたる 1,053,521 件（1,062,400 件 − 8,879 件）をいずれかの手段で管理者に通報し，しかも通報の総行数が 92,529 行（1,053,521 件の 9%）に抑られていることが分かる．また，警報メールの数の面でも 1 日あたり 560 通で，2.1 節で示した第 1 期の運用時のピーク数である 2,494 通の 22%に抑えられており，管理者の監視負荷が軽減されていることが分かる．

4.3 一般性に関する考察

本システムの一般性に関しては次の 3 点が主に問題となるだろう．

- 組織への依存度
- ネットワーク利用形態への依存度
- IDS 製品への依存度

組織への依存度について，本システムはもともと我々の組織内での運用に向けて構築されてきたものであり，現システムをそのまま他組織に移植することは難しい．組織固有の定数や処理方式のパラメータ化，通報システムのレポート機能や Web UI の部品化をすすめ，ポータビリティを高めることは今後の重要な課題である．

また，ネットワーク利用形態への依存度について，インターネットと高い開放度で接続される大規模ネットワークを管理する組織では，本システムを適用して監視業務を行うメリットが大きいと考える．そのような組織は我々に限らず，研究教育機関，インターネットプロバイダなど，相当数にのぼると考えている．

IDS 製品の依存度について，現システムでは，アラームデータベースのスキーマが Cisco Secure IDS のログ形式に依存している点がポータビリティのネックとなる．しかしながら，IDS センサからのインシデント情報の取得，データベース登録，通報，検索については，SQL，メール，Web という一般的な枠組みを用いており，機種ごとのインシデント情報を本システムのものへ翻訳し，スキーマ変換を行うツールを整備すれば，他機種の IDS への適用も可能である．我々は現在，オープンソースの IDS ソフトウェア Snort [9] への適用を検討している．また，IDS データの交換フォーマットを定める IDMEF [10] の標準化動向にも注目しなければならないと考えている．

4.4 IDS 製品との比較および関連研究の動向

本システムと既存の IDS 製品との機能比較を**表 4** に示す☆．

Cisco Secure IDS は，本システムの前提となっているシステムであり，データベース連携，メール通報，検索インタフェースを備えるが，それぞれに不足する

☆ 表 4 は，IDS の周辺機能（データベース連携，メール通報，検索・閲覧インタフェース）に関する比較であり，IDS の主機能である不正検出に関する優劣を示すものではない．

表 4 IDS 製品との比較
Table 4 Comparison with IDS products.

	本システム	Secure IDS	Man Hunt	Snort
データベース連携	○	○	○	○
とりまとめ登録	○	×	×	×
メール通報	○	○	○	×
定期通報	○	×	○	−
インシデント間関係の通報	○	×	○	−
詳細度別通報	○	×	×	−
検索・閲覧インタフェース	○	○	○	×
Web ブラウザ利用	○	×	×	−
インシデント間関係の検索	○	×	△	−

機能を補う形で本システムが開発されている．

Symantec 社の ManHunt [11] は，Cisco Secure IDS などで採用されている不正検出型の検出機能と，トラフィック全体から特定のプロトコルやアドレスに対する通信量の増大などの特異現象を検出する異常検出（anormaly detection）型の検出機能を組み合わせたハイブリッド型の IDS として知られる．ManHunt もデータベースへの出力機能を備えるが，一定期間のインシデントをとりまとめて登録することはできず，データベースに格納されたインシデントに対する検索インタフェースも提供されない．ManHunt の特徴として，特定の IP アドレスに関連して指定したシグネチャのインシデントをとりまとめ，管理者に通報できる点があげられる．また，このようにとりまとめた情報を定期的にメール通報する機能や，専用の Java クライアントによる閲覧インタフェースが提供されている．ただし，複数の異なるシグネチャにわたる関係情報の提示や，ネットワークセグメントに対する検索はできない．また，本システムで提供するような詳細度別のとりまとめやレポートを行うことはできない．

Snort は，インシデントの検出機能を中心として設計されており，IDS センサにあたる部分のみが提供される．開放性を重視した設計となっており，センサの検出ルールやログの出力フォーマットなどを柔軟に設定することができ，様々なアプリケーションとの組合せが容易となるよう配慮されている．データベース連携機能に関しては，各種 SQL データベースにログを出力するためのフォーマットが用意されている．ただしデータベースの検索機能やユーザインタフェースは用意されておらず，別途開発が必要となる．また，メールによる通報機能は直接的には備えないが，ログの出力先やフォーマットをメール用に定義すれば可能となる．インシデントの検索・閲覧インタフェース機能も備えないが，XML 形式での出力が可能であるなど，作り込みが容易となるよう設計されている．

また，本システムの機能を拡張・高機能化するために参考となる研究の動向として次のような成果があげられる．

大谷ら [12] は，各種の IDS が検出するインシデントを統合して管理するデータベースにより，インシデントの分析支援を行うシステムを提案している．インシデント分析のためにデータベースが備えるべき情報やツールの分類が行われている．

ログ解析にデータマイニングやテキストマイニング手法を用いるアプローチ [13] もさかんに行われている．見えログ [14] では，テキストマイニングによりログ情報の特徴抽出を行い，情報視覚化による異常事象発見の省力化を支援する．また，宮本ら [15] の研究では，サーバのログ監視にテキストマイニングと周期性解析を組み合わせた方法を提案している．いずれも大量のデータにリアルタイムで適用するためには処理時間の点で問題があるが，より精度の高い不正アクセス監視の一手法としてマイニング技術の導入も今後の検討課題である．

ユーザ参加型の共同管理の視点からログ監視業務の効率化を試みるモデルの提案が，高田らによって行われている [16]．このような管理モデルの施行には，組織構成員の技術レベルやセキュリティ意識がある程度揃っていることを前提とすべきであるが，今後，本システムにおいても，ユーザへのインシデント情報の提供について検討するさいの参考としたい．

5. おわりに

本稿では，不正アクセス監視業務を支援するシステムの構築経緯と運用経験についてまとめた．筆者らが所属する組織における，2000 年 8 月から現在にいたる IDS の運用経験から，大規模ネットワークに監視現場で IDS 製品のかかえる諸問題を明らかにし，その問題点を解決するための支援システムを構築した．また，システムの評価では，不正侵入の検出作業の省力化に有効であることを実例により示した．

今後の課題は，4.3 節でも述べたとおり，システムの汎用性を高めることが第 1 にあげられる．また，IDS を含む監視支援システム自身の保護についても，必須アクセス制御 [17] などの方法を用いた対策について検討の必要があると考えている．

謝辞 本システムの開発と運用にあたり，京都大学学術情報メディアセンター学術情報ネットワーク（KUINS）担当スタッフ各位の助言と協力を得た．ここに記して謝意を表す．

参 考 文 献

1) 山口 英：ネットワークセキュリティに係る動向，情報処理，Vol.42, No.12, pp.1153–1158 (2001).
2) 警察庁：ハイテク犯罪に関するアンケート (1998). http://www.npa.go.jp/hightech/enquete/index.htm
3) Cisco Secure IDS. http://www.cisco.com/japanese/warp/public/3/jp/product/product/security/ids/index.html
4) 武田圭史：侵入検知システムに関する研究の現状，情報処理，Vol.42, No.12, pp.1169–1174 (2001).
5) Hewlett-Packard: HP OpenView. http://www.openview.hp.com/
6) Porres, P., Schnakenberg, D., Staniford-Chen, S., Stillman, M. and Wu, F.: The Common Intrusion Framework Architecture (1998). http://www.isi.edu/gost/cidf/drafts/architecture.txt
7) PostgreSQL. http://www.postgresql.org/
8) PHP: Hypertext Preprocessor. http://www.php.net/
9) Snort: The Open Source Network Intrusion Detection System. http://www.snort.org/
10) Curry, D. and Debar, H.: Intrusion Detection Message Exchange Format Data Model and Extensible Markup Language (XML) Document Type Definition, IETF Internet Draft: draft-ietf-idwg-idmef-xml-08.txt (2002).
11) Symantec ManHunt. http://www.symantec.co.jp/region/jp/products/manhunt/index.html
12) 大谷尚通，桑田喜隆，小迫明徳，井上 潮：統合データベースを用いた不正アクセス検出情報の分析および意思決定支援システム，第 13 回データ工学ワークショップ（DEWS2002）予稿集，A1-6 (2002).
13) Lee, W., Stolfo, S.J. and Mok, K.W.: Adaptive Intrusion Detection: A Data Mining Approach, *Artificial Intelligence Review*, Vol.13, No.6, pp.533–567 (2000).
14) 高田哲司，小池英樹：見えログ：情報可視化とテキストマイニングを用いたログ情報ブラウザ，情報処理学会論文誌，Vol.41, No.12, pp.3265–3275 (2000).
15) 宮本貴朗，泉 正夫，田村武志，福永邦雄：ネットワーク・サーバ運用監視支援システム，システム制御情報学会論文誌，Vol.15, No.6, pp.279–287 (2002).
16) 高田哲司，小池英樹：ログ情報視覚化システムを用いた集団監視による不正侵入対策手法の提案，情報処理学会論文誌，Vol.41, No.8, pp.2216–2227 (2000).
17) 女部田武史，井上 直，浅香 緑：必須アクセス制御方式を用いた侵入検出システム保護機能，情報処理学会論文誌，Vol.42, No.8, pp.2057–2066 (2001).

(平成 14 年 12 月 2 日受付)
(平成 15 年 6 月 3 日採録)

沢田 篤史（正会員）

1995 年京都大学大学院工学研究科情報工学専攻博士後期課程研究指導認定退学．同年奈良先端科学技術大学院大学情報科学研究科助手．京都大学大学院工学研究科助手，同大学大型計算機センター助教授を経て，現在同大学学術情報メディアセンター助教授．博士（工学）．ソフトウェア工学，ソフトウェア生産環境等の研究に従事．電子情報通信学会，システム制御情報学会，日本ソフトウェア科学会各会員．

高倉 弘喜（正会員）

1995 年京都大学大学院工学研究科情報工学専攻博士後期課程修了．同年イリノイ大学訪問研究員，奈良先端科学技術大学院大学情報科学研究科助手．京都大学大学院工学研究科講師，同大学大型計算機センター助教授を経て，現在同大学学術情報メディアセンター助教授．博士（工学）．大規模ネットワークにおけるセキュリティの研究，地理情報システム等の研究に従事．ACM 会員．

岡部 寿男（正会員）

1988 年京都大学大学院工学研究科情報工学専攻修士課程修了．同年同大学工学部助手．同大学大型計算機センター助教授，同大学大学院情報学研究科助教授を経て，現在同大学学術情報メディアセンター教授．博士（工学）．並列・分散アルゴリズム，新世代インターネット等の研究に従事．電子情報通信学会，システム制御情報学会，日本ソフトウェア科学会，IEEE，ACM，EATCS 各会員．