2G－3

広域不正アクセスに対する侵入検出・状況把握システムに関する検討*

大谷尚通　小迫明徳　桑田喜隆　井上潮　岩田恵一†
(株)NTTデータ§

1 はじめに

不正アクセス技術の高度化や広域で組織的な不正アクセスの出現などによって，ファイアウォールやIDS(Intrusion Detection System)などのセンサ単体では，これらに対応できなくなってきた．これは，CIDF(Common Intrusion Detection Framework)[1]に基づく機械的な不正アクセス検出の限界が原因である．

そこで本稿では，複数のセンサを統合化し，人間による不正アクセスの状況把握を支援する侵入検知・状況把握システムを提案する．

2 現状の問題点

CIDFに基づく不正アクセス検出は，以下のような問題がある．

- 特定センサを回避する不正アクセス手法に対処できない．
- 誤検出か不正アクセスかの判断が難しい．
- 広域な不正アクセスの状況がわからない．
- 不正アクセスの目的や意図がわからず，対応が難しい．

これは，センサによって取得される情報が不正アクセスの断片的な情報の集合でしかなく，機械的な方法では，そこから不正アクセスの全体像を導き出すことが難しいからである．つまり，センサは不正アクセス1つ1つの検出はできるが，それらをまとめたり，不正アクセスの意図を導き出したりすることができない．

3 広域な不正アクセスへの対策方法の提案

センサによる不正アクセスの検出だけではなく，その結果をまとめてより総合的な状況を明らかにする仕組みが必要である．

そこで本稿では，複数のセンサを用いてさまざまな情報を自動的に収集し，その情報を人間が分析することによって，不正アクセスの状況把握を行なうシステムを提案する．これにより，相手の目的や意図を推測し，不正アクセスに対する的確な意思決定と対策が可能になる．

3.1 状況把握のためのアーキテクチャ

状況把握を行なうためには，センシング，情報の統合化，プレゼンテーションの3つの要素が求められる．そしてこれらが有機的に連携して，情報を処理することが必要である．

- センシング
  不正アクセスに関するより多くの情報を取得することが重要である．複数のセンサをネットワーク上に配置し，情報を収集する仕組みが必要である．
- 情報の統合化
  不正アクセスの情報だけでなく，ネットワークの構成情報など，状況を把握するためには，多くの情報が必要である．それらをまとめ，処理できる仕組みが求められる．
- プレゼンテーション
  不正アクセスの現状を迅速に把握しなければならない．状況を直感的に理解させることに重点を置いて，情報をシンプルかつグラフィカルに表示する仕組みが必要である．

4 システムの実装方法について

提案した不正アクセスの対策方法に基づき，システムを試作した．以下に，本システムの全体構成および実装した各項目について述べる．

4.1 全体構成

本システムは，図 1に示すようにセンサ群，統合データベース，情報視覚化システムの3つの部分から構成される．

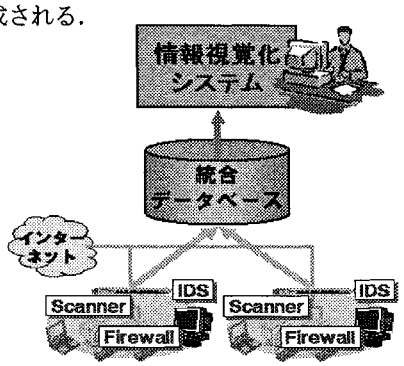

図 1：システムの全体構成

これらは，通信可能なネットワーク上であれば，

---

* Incident Detection and Visualization system against global cyber attacks.
† Hisamichi Ohtani, Akinori Kosako, Yoshitaka Kuwata, Ushio Inoue, and Keiichi Iwata
§ NTTDATA Corporation

分散配置することが可能である．よって，大規模なネットワークや複数の独立したネットワークであっても，それぞれにセンサを配置し，監視センタにおいて統合的に監視・分析することが可能である．

4.2 IDSの複数・マルチベンダ化と情報収集

広域にわたる不正アクセスを監視する場合は，IDSを広域にわたって複数配置する．これにより，不正アクセスの傾向分析や侵入経路の追跡を行なうことができる[2]．重要なシステムなどを重点的に監視したい場合は，検出方式の異なる複数のベンダのIDSを集中的に配置する．これは，特定のIDSやシグネチャを回避する不正アクセスに対して有効であり，検出率を向上させることができる．さらに1つの不正アクセスに対して，複数の検出情報が得られるため，誤検出の比率を下げることも可能になる．監視目的に応じて，この２つの方式をバランスよく組み合わせることが必要である．

異なるベンダのセンサを運用する場合，その出力情報の形式が異なるため，それらを統一的に扱うことが難しい．そこで本システムでは，それらを統一した形式に基づいて正規化し，データベースへ蓄積することとした．これにより，表現形式の違いが解消され，分析等に利用しやすくなる．図 2のように，IDSの検知情報とファイアウォールの出力情報は，IDMEF(Intrusion Detection Message Exchange Format)[3]を独自に拡張したフォーマットを利用して正規化を行ない，統合データベースへ収集・蓄積する．

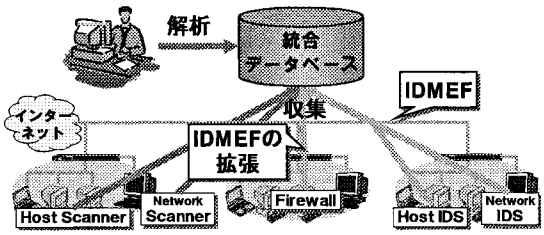

図 2：センサ情報のデータベースへの統合化

4.3 総合的な情報統合化

センサのもたらす侵入検知情報と，稼動中のシステムの情報やそれを利用する組織情報など，監視対象のネットワーク環境情報等，システム全体の情報も含めた統合データベース(図 2)を作成する．これにより，例えば，検知情報と脆弱性情報を照合することにより，不正アクセスの成功の成否を推測し，調整が必要なファイアウォールを特定したり，対象組織へ連絡したりすることができる．このように，統合化したデータベースは，全体的な状況分析と意思決定，具体的な対応方針作成のための情報源として利用する．

4.4 状況把握の支援

迅速で的確な意思決定を行なうためには，「何が起こっているか」を把握することが第一ステップであり，かつ重要なステップである．そこで，上記の総合データベースから必要な情報を取り出し，情報視覚化システム上にて，直感的にわかりやすく表示する．以下に，不正アクセスの状況把握を行なうための2つの表現形式をあげる．

- **ネットワーク情報(地図)に基づく表示方法**
  実際のネットワークやコンピュータの接続情報を記述したネットワーク地図をベースに，被害情報等を表示する方法．ネットワーク構成を表すことが可能なため，侵入経路の分析等に有効である．
- **分析したい情報に注目した表示方法(図 3)**
  端末の脆弱性と重要度の関係や，不正アクセスとOSの関係など，オブジェクトの関係表現を中心とした方法．分析したい項目を縦軸や横軸などに自由に設定できるため，多角的な分析ができ，侵入相関分析(Intrusion Correlation Analysis)に有効である．

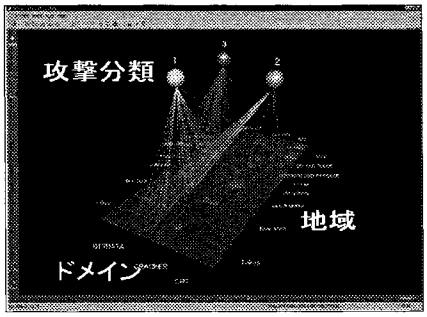

図 3：多角的分析が可能な表現

5 まとめ

本稿では，侵入検出システムに人間の判断を加えた広域不正アクセスに対する侵入検出・状況把握システムを提案し，このシステムのプロトタイプ構築における実現方法を説明した．今後は，実ネットワークへ接続して実証実験を行ない，不正アクセスに対する本システムの有効性や，本システムを利用したコンティンジェンシプラン[¶]の検討等を行ないたい．

参考文献

[1] P.Porras, The Common Intrusion Detection Framework Architecture, 1999.
[2] Tim Bass, Intrusion Detection Systems Multisensor Data Fusion: Creating Cyberspace, Situational Communications of the ACM. Forthcoming, 1999.
[3] IDWG (IETF), draft-ietf-idwg-data-model-03.txt, http://www.ietf.org/ID.html, 2000.

[¶]不慮の出来事により情報システムが影響を受けた場合の対処計画。