分散環境におけるセキュリティ証跡解析方式の検討

平田俊明，浦野明裕，藤野修司*，宮崎　聡

日立製作所システム開発研究所

*日立製作所ソフトウエア開発本部

概要

本稿では、多様なアプリケーションやプラットフォームに対して、共通の基盤上で予め指定されたルールに従って監査証跡を自動的に解析する方式を提案する。提案方式は、ログイン/ログアウトに関する監査ログを解析することで通常とは異なる利用状況を検出する。このとき、ログインの連続失敗回数、運用上ありえない場所や時間帯における利用など多様な観点から計算機の利用状況を解析することで不正アクセスの検出の精度を向上させている。さらに、遠隔地の計算機を多段のリモートログインで接続している場合、発信元の計算機を逆路的に探索して特定の条件によって、候補をリストアップする方式を提案している。提案方式では、セキュリティ管理者の負荷を低減できるとともに不正アクセスをより精度高く検出できる。

Security audit method for distributed systems

Toshiaki Hirata, Akihiro Urano, Shuuji Fujino*, Satoshi Miyazaki

Systems Development Laboratory, Hitachi,Ltd.

*Software Development Center, Hitachi,Ltd.

Abstract

A method is proposed for analyzing audit logs automatically by using specified rules on a common database for various applications and platforms. The proposed method monitors login/logout and analyzes the access logs to detect unusual usage. It increases detect precision by analyzing computer usage several points of view (number of login failures or illegal period of time and place, etc.). Moreover, the candidates for source computer are identified if a remote computer is used to execute remote login by way of multiple computers. We propose the method for source computer searching.

This method reduces the security administrator's work load and detects illegal usage more precisely.

1. はじめに

近年のイントラネットの普及に伴い、セキュリティニーズが増大している。セキュリティ管理においては、アクセス制御や暗号化技術の適用ばかりでなく、ネットワークシステムの不正な利用を検出したり事前に対策することを目的としたセキュリティ監査機能も重要である。これに対して、従来はプラットフォームごとに各アプリケーションの有する検出メカニズムを利用しているため、アプリケーションごとに異なる形式のセキュリティ管理情報を参照し、人手でこれらを解析する必要があった。このため、セキュリティ管理者に大きな負担を強いていた。

本稿では、多様なプラットフォーム上の多様なアプリケーションの監査証跡(例えば、アクセスログ)を共通な基盤上で特定のルールで自動的に解析する方法を提案する。提案方式ではセキュリティ管理マネージャがネットワーク上のサーバからアクセスログを収集してこれらを解析する。解析方式としては、ログインの試みを観察して、不信な試みを検出するものである。特に、検出の精度を高めるため、ログインの失敗回数や通常利用しない時間や場所からのアクセスなど多様な観点から計算機の利用状況を解析する。さらに、遠隔地の計算機を複数の計算機を経由して利用しているような場合(例えば、多段の Telnet 等)、発信元の計算機を推定する方法を提案する。

提案方式では、セキュリティ管理者の負荷を低減できるばかりでなく、計算機の不正な利用をより精度高く検出することができる。

2. 背景・目的

2. 1 セキュリティ対策の分類

ネットワークシステムにおいては、図1に示すように計算機室への侵入、クラッカーなどによるネットワークからの攻撃、コンピュータウイルスなどによるソフトウエアを用いた攻撃などがある。これらのリスクに対して不正な利用を防ぐアクセス制御や盗聴や改ざんを防止する暗号化技術など直接的な対策がが有効であることはいうまでもないが、計算機の不正利用の検出や防止のためのリアルタイム監視やオフラインでの監査、ウイルスチェックなど間接的な対策も重要である [1]。ここで、監査とは監査ログのチェックやファイルの改ざんチェック、システムファイルの設定ミスのチェックなどが含まれる。

これらのセキュリティ施策のうち、本稿は上記間接的対策のうち、監査ログのチェックの方式に関し、多様なプラットフォーム上の多様なアプリケーションに対して多様な観点からの解析方式を提案する。

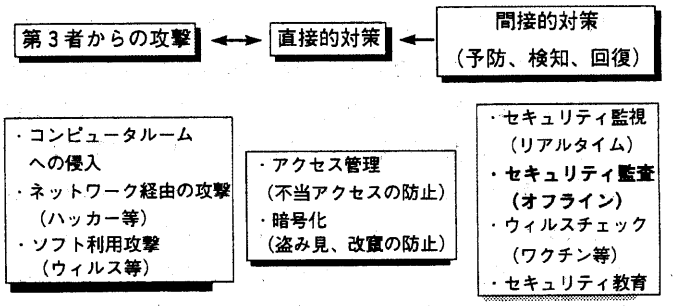

図1 セキュリティ技術における本稿の位置付け

2. 2本稿の対象範囲

侵入者は過去に多様な方法でネットワークシステムへの攻撃を試みている。典型的な方法の1つに finger コマンドで得た利用者名や guest などのよく知られた利用者名を用い、パスワードを推定することによりログインを試みるという手順がある。また、プログラムのセキュリティホールやシステムファイルの設定ミスなどをついた侵入や偽装プログラム(トロイの木馬)の送り込みによるパスワードファイルの流出等も数多く報告されている [2]。これらの侵入を検出するためにはアクセスログのチェックばかりでなく、リアルタイムのパケットモニタリングやファイルの改ざんチェックなどの手法を用いる必要がある [3]。さらに、セキュリティホールのあるプログラムの有無や不用意なシステム設定の有無を

事前にチェックする手法も用いられる[3]。本稿では、アクセスログを解析することによって、不信なログインを検出する手法に関する方法を提案するものである。アクセスログはオペレーティングシステムやアプリケーションプログラムなど幅広く採取し、利用されている。

監査ログ(アクセスログ)を収集し、共通の形式に正規化する。セキュリティ管理マネージャは、正規化されたログを管理対象の計算機から収集し、時系列にデータベースに格納する。収集されたログ情報は、予め指定されたルールで解析され、ルールにヒットしたとき、警告メッセージを管理用コンソールに表示し、セキュリティ管理者に通知する。新しいルールの登録や変更はルール管理部にて実施する。ルールには計算機の不正使用を検出する解析ルールの他に、収集するログを制限するためのフィルタリングルール、収集対象とするログファイルの種類やログファイル(正規化ログ格納ファイル)の容量管理に用いるファイル管理ルールを設ける。

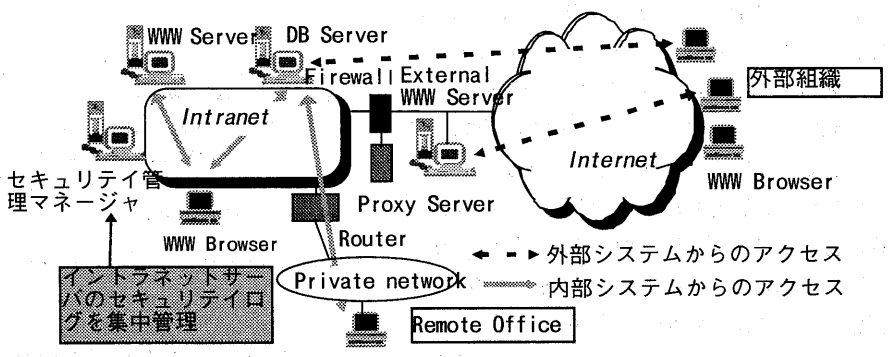

図2対象とするネットワークシステムの構成

3. システム構成

図2は提案方式におけるセキュリティ監査システムが監査対象とするネットワークシステムの構成を示す。企業情報システムにおいては、WWW やデータベースなど多様なサーバが存在する。ファイアウオールはインターネット等の外部のネットワークと分離し、ルータによって遠隔地との接続を行う。利用者はネットワークシステムの内部かまたはファイアウオールの外部から前記サーバにアクセスする。セキュリティ管理マネージャはサーバ、ファイアウオール、ルータなどのセキュリティ監査ログを収集し、自動的に解析する。これにより、セキュリティ管理者の負荷が軽減される。

なお、管理対象のサーバ、ファイアウオール、ルータ上には、ログを収集するための専用のエージェントプログラムが必要である。

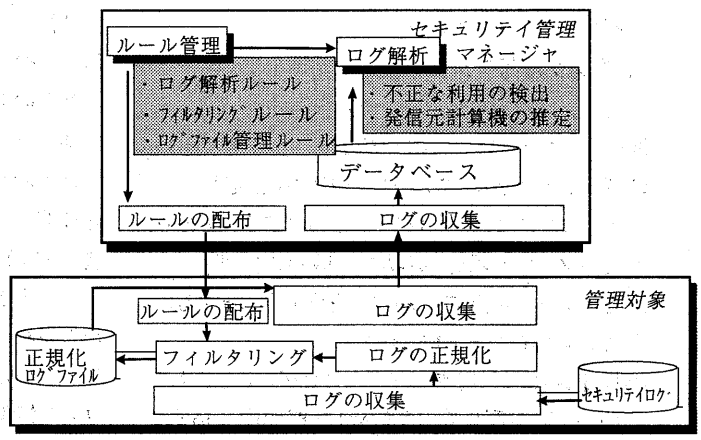

図3セキュリティ監査システムの構成

図3はセキュリティ監査システムの内部構造を示す図である。管理対象の計算機は、

4. ログ解析方法

4. 1 概要

従来の分散環境における計算機システムでは、一般に指定回数連続してログインに失敗した場合や規定時間内にログインに成功しなかった場合、通信路を切断する方法などが多く採用されている。しかしながら、これらの方法では指定された回数または指定された時間内に意図的に通信路を切断した場合には、それ事体は記録に残らないので、アクセスログを参照してログイン失敗が連続して発生していることを確認する必要がある。

これに対して提案方式では、時間や場所など、多様な観点から計算機の利用状況を解析することにより不正利用の検出の精度を向上する。さらに、提案方式では、ログインの試みの結果、ログインが成功したか失敗したかを特定することができるようにしている。主な解析ルールは以下の通りである。

(1)特定の時間内に予め決められた回数の連続したログインの失敗を検出した。

(2)同一の利用者名称で複数の場所から同時にログインしている事象を検出した。

(3)運用上ありえない場所またはありえない時間帯にログインしている事象を検出した。

(4)一定期間以上ログインしていない利用者名でログインしている事象を検出した。

4. 2 ログ解析アルゴリズム

図4に「特定の時間内に予め決められた回数の連続したログインの失敗を検出した」というルールの解析アルゴリズムを示す。一般的な仮定として、アクセスログには、「ログインかログアウトかの区別」、ログインの場合「成功か失敗かの区別」、「利用者名」、「接続元のアドレス」を含むものとする。

以下に解析の手順を示す。

(1)指定された利用者のアクセスログを新しいものから順に参照して、指定された期間内に指定された回数の連続したログイン失敗が検出されたとき、「ログイン失敗カウンタ」をセットする。

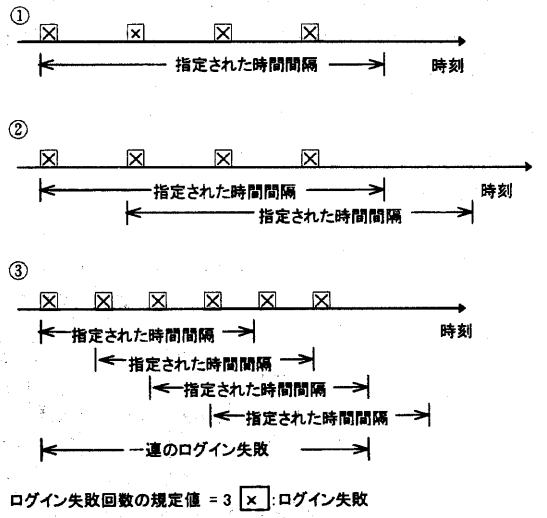

図4 ログ解析アルゴリズム（1）

(2)連続したログイン失敗回数の積算の初期カウント時点を2番目のログイン失敗事象とし、指定された期間内のログイン失敗回数を以下の計算式で求める。

新ログイン失敗回数＝旧ログイン失敗回数－1＋
新規に検出されたログイン失敗回数

新規に検出されたログイン失敗回数は、前回カウントした最後のログイン失敗時点以前に検出したログイン失敗回数である。

(3)以下の条件を満たすまで(2)のステップを繰り返す。

新ログイン失敗回数＜旧ログイン失敗回数

以上の手順により一連のログインの試みを1つの事象として検出する。また、前記アルゴリズムではログレコードの参照は1ログにつき1回でよく、nを参照したログの個数とすると、解析に係る計算量はO(n)(nのオーダ)となる。

次に図5に「同一の利用者名称で複数の場所から同時にログインしている事象を検出した」というルールの解析アルゴリズムを示す。解析対象のログの情報は図4の例と同様とする。アクセスログを最新のものから順に検索し、ログインとログアウトの期間中に同一利用者名でログインしているIPアドレス(TCP/IPネットワークの場合)を検索する。も

し、発見された IP アドレスが元のIPアドレスと異なる場合はカウンタを＋1する。カウンタが既定値に達したときルールにヒットしたとする。

(1)login および logout のログを新しいものから順に検索する。

(2)現在ログイン中の利用者の接続元 IP アドレスと異なるIPアドレスからloginしている同一利用者名の利用者が発見された場合、カウンタを＋1する。

(3)同時にログインしている利用者がログアウトしたという事象を検出した場合、カウンタを－1する。

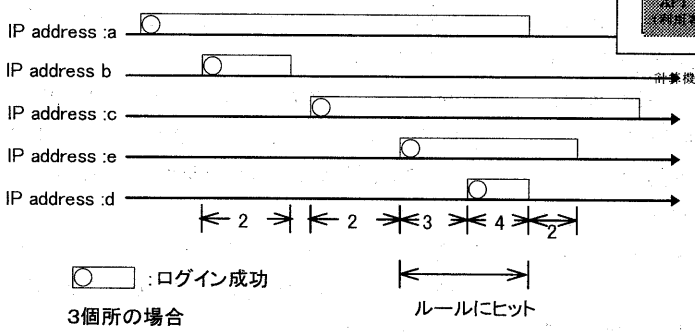

図５ログ解析アルゴリズム（２）

本アルゴリズムでは同一利用者に対してログインおよびログアウトのログを一度のみ読めばよい。よって、 n を参照したログインとログアウトのログの対の個数とすると、解析に係る計算量は O(n)(n のオーダ)となる。

図6に計算機の不正な利用が検出された場合の発信元を推定する方法を示す。分散環境における一般的な計算機システムでは、遠隔地の計算機が複数の計算機を経由してリモートログインで使用されている場合、一般的に採取可能なログ情報では発信元の計算機と利用者名を逆路的に探索して一意に特定することはできない。これに対して、提案方式では特定の条件を設けること

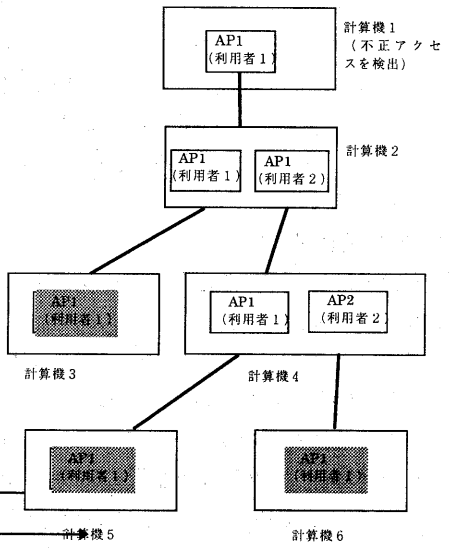

図６発信元の推定方法

で発信元の計算機と利用者名の候補を絞り込む方法を提案する。ログの解析アルゴリズムを以下に示す。

(1)不正な計算機の利用に関するアクセスログをピックアップする。

(2)(1)のログを参照して接続元(当該計算機に直接接続している計算機)計算機を選択する。

(3)(2)で特定した計算機上で、(1)の利用者が利用中の期間に利用している利用者をリストアップする。

(4)(3)の利用者について利用者名と計算機名を記録し、当該ログから(2)と同様の方法で接続元(当該計算機に直接接続している計算機)計算機を選択する。

(5)(3),(4)の手順を当該利用者の接続元計算機がローカル計算機になるまで繰り返す。

上記手順において、ネットワーク上の計算機数や利用者数が多い場合は、探索空間が大きく絞り込みの方法が必要となる。提案方式で上記手順の(3)において以下の絞り込みの条件を適用する方法を提案する。

(1)不正な利用が検出された計算機上の利用者と同一の利用者名を探索する。
(2)運用上ありえない場所からまたは時間帯における接続を行っている利用者を探索する。
(3)初めてもしくは一定期間利用がなかった利用者を探索する。

4.3 ログ管理方式

本節では以下のログ管理方式を提案する。

(1)ログの正規化

アクセスログはプラットフォームやアプリケーションによって多様な形式を持っている。このため、プラットフォームやアプリケーションに依存しない共通のログ解析プログラムを適用するための共通のログ形式を定義する方式が有効である。ログの共通の項目としては、「イベントやその結果の種別」、「利用者名」、ログを収集した「計算機名」、「ログの収集時刻」がある。「ログの収集時刻」は計算機によって時計が一致している保証がないため、標準の時刻(例えば、セキュリティ監査マネージャの時刻)にあわせる必要がある。

OSやアプリケーションが出力したログは、一定時間間隔で収集、正規化して共通形式に変換する。変換ルールは、固定的に持つ方式の他、変換ルールを定義する方式が考えられる。

(2)データベースへの格納

正規化済みのデータはセキュリティ管理マネージャが収集し、データベースに格納する。ログデータは時系列に、イベントの識別や利用者で検索可能なキーを設定してデータベース化する。

(3)ログ管理ルール

収集すべきログファイルの指定をするためのファイル管理ルール、収集すべきログの種別(ログの種類、収集期間、特定の文字列を含むログ、等)を指定するフィルタリングルールを設ける。これらのログ情報はセキュリティ管理マネージャに登録して、特定の管理対象の計算機に送信、適用される。

5. おわりに

本稿では、多様なプラットフォームやアプリケーションに対して共通の基盤上で予め指定されたルールを用いてアクセスログを自動的に解析し、セキュリティ管理者の負荷を低減する方式を提案した。提案方式の特徴は以下の通りである。

(1)提案方式は計算機に対するログインの試みをモニタし、計算機の不正な利用を検出するための解析方法に関するものであり、ログイン失敗回数や運用上ありえない場所からもしくは時間帯での使用等多様な観点からの利用状況の解析によって、検出の精度を向上した。
(2)提案アルゴリズムではログレコードの参照は1ログにつき1回でよく、n を参照したログの個数とすると、解析に係る計算量は O(n)(n のオーダ)となる。
(3)遠隔地の計算機を多段のリモートログインで利用している場合の発信元計算機の探索、推定方法を提案した。

本提案方式は、監査ログの解析による計算機の不正利用の検出方法に関するものであるが、実際のフィールドでの不正利用の検出には2. で述べたような多様な手法を組み合わせて利用する必要がある。

[参考文献]

(1)Thomas E. Tahan, "SECURITY MANAGEMENT", IM'97 TUTORIAL May 1997.
(2)CERT Advisary, ftp://info.cert.org/pub/cert_advisories
(3)UNIX Security Tools: Use and Comparison, SANS'96 COURSE BOOK May 1996.
(4)K. Christian, S. Richter: The UNIX(R) Operating System Third Edition, John Wiley & Sons, INC. 1994