アプリケーション不正利用の発見・防止技術の一考察

6F－4

中山隆二　冨士仁　伊集院正

NTT ソフトウェア研究所

1. はじめに

近年、情報処理システムを不正に利用する事件が発生しており、エレクトロニックコマース(EC)や企業の業務処理システム等にとっては重大な脅威になっている。このような不正利用を防止するために、利用者が本人であることを確認する認証の技術や、外部からの危険性の高い通信を制限するファイアウォールの技術等の開発が活発である。

これらの技術の不正利用防止効果は高いが、パスワード等を盗み出して正規利用者になりすます、システムの欠陥を利用する等の手段による不正利用を防止することは難しい。これらに対抗するには、利用者の行動等から不正利用を発見する必要がある。

UNIX 等の OS については従来から不正利用発見技術の研究があるが[1], [2]、EC や業務処理システム等のアプリケーションについてはほとんど研究事例がない(図 1)。今後の EC 等の発展を考えると、この技術の研究開発が重要である。本論文では、利用者の行動モデルと実際の行動を比較して不正利用を発見する手法について述べる。

2. EC における不正利用発見上の課題

本論文では、販売者が商品や情報の目録を Web ページ上に示し、利用者はそれらを閲覧して購入する商品や情報を決めて注文を出し、クレジットカードや電子現金等で代金の決済を行うような、WWW をベースとした EC システムを対象とする。

この場合、アプリケーション不正利用とは、正規の利用者認証情報を何らかの方法で窃用、または EC システムの欠陥を利用する等して、正規ユーザになりすまし、不正に商品やサービスを購入する事によって、販売者や正規利用者等に何らかの金銭的被害をもたらすものを言う。

OS の不正利用においては、多くの不正利用者は特権ユーザの権限を手に入れることを目標にしている。このため、不正利用者は、普通の利用者が行わないような特定の行動をとる。

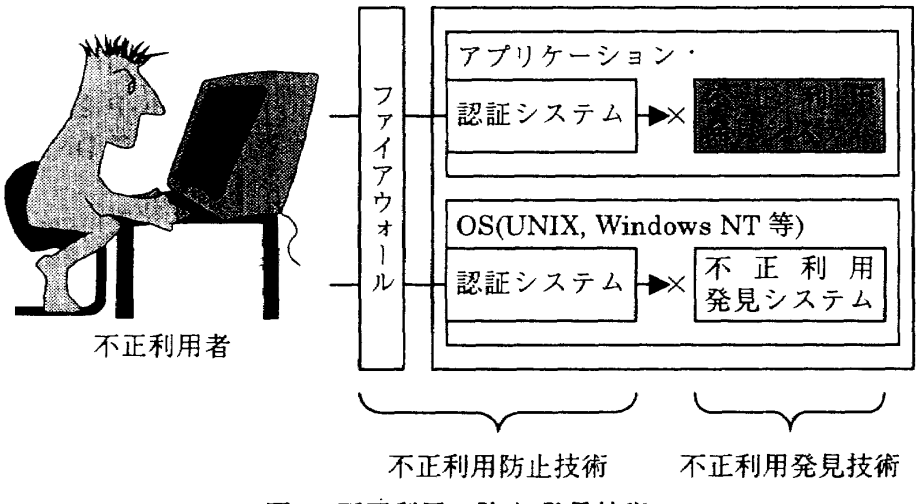

図 1: 不正利用の防止/発見技術

それに対して、EC システムにおいては、一般に特権ユーザは存在せず、不正利用者と正規利用者のとる行動はほとんど同じである。したがって、多くの OS 用不正利用発見システムで用いられている利用者の特定の行動(特権ユーザになろうとする試み)をトラップして警告を出す類の手法は適用できない。

このため、正規利用と不正利用のわずかな違いを手がかりとして不正利用を発見する必要がある。

3. EC における不正利用発見の方法

わずかな違いを発見する方法として、各利用者が行う一連の購買行動全体を、追跡して分析対象とし、それに対して統計的数量化を行い、その結果を平均

A study of abuse detection and prevention technology for applications

Ryûji Nakayama, Hitoshi Fuji and Sei Ijuuin

NTT Software Laboratories

3-9-11, Midori-cho Musashino-shi Tokyo 180 Japan

的な購買行動モデルの統計量と比較することによって、不正利用の疑いが濃い行動を見つける手法を考案した。

3.1 購買行動モデル

ここで、比較対象とする平均的な購買行動のモデルとしては、

- それぞれの利用者の購買行動を表す、個人別モデル
- 問屋的行動をする等の特異な利用者を除いた、一般的な利用者の購買行動を表す、一般モデル

を考える。

上記二つのモデルを利用する理由は、非常にバラエティに富むであろうECシステムの利用者を追跡するにあたって、一般的な行動モデルだけでは分散が大きくなって不十分であり、「個人の行動」を参照することが、異常、すなわち不正利用の発見に寄与する率が高いと考えられるからである。

3.2 数量化手法

上記の購買行動モデルにおいて、利用者の行動を代表する数値として、

- 利用時刻、一回の利用時間
- 一つのページを読むのに要する時間
- 購入を決意するまでに眺める目録ページの枚数
- 購入商品の傾向

等の値が有効ではないかと思われる。

これらの数値を得る手法として、WWWをベースとするシステムからデータを得る事を考慮し、

- Webサーバに残される単独のイベント記録から直接データが得られるもの
- 複数のイベント記録から必要なデータを導き出す必要があるもの

の二つのデータ導出手法に分け、この両者が利用できる事が、購買行動モデルを有効に機能させるために必要であると考えている。

4. 不正利用発見システムの環境

以上のような手法を効率よく実現・運用するためには、それを支援するシステム環境が必要になる。

4.1 データ収集とモデル適用の連携

このモデル化と数量化の手法は、実際の利用者が残す運用データによって、検証・精密化される。また、運用データを分析することで、新たなモデル・数量化手法の追加や更新なども可能になる。

例えば、利用者がシステムに慣れるにしたがって、ページの購読時間や、購入用件の記入などに要する時間が変化すると考えられる。また、新たな販売者が加わるなどして、利用者層が大きく変化した場合など、一般モデルの尺度が変換すると考えられる。

それらに対応するために、データを分析し、モデルに反映させるための環境を整備する必要がある。

4.2 データの収集方法

今回考案した手法においては、記録の中から個々の利用者の購買行動が得られていることを前提としている。しかし、現状のWWWをベースとするシステムでは、Webサーバには個々のやり取りが分断された状態で記録されてしまう。また、proxyを使っている場合など、利用者クライアントのアドレスもグローバルなものしか残らないため、利用者の特定も不十分なままのデータしか収集できない。

そこで、Webサーバの記録から、同一の利用者が残したデータを導き出すためには、CGIを活用して利用者情報を記録するなどの改造を、ベースとなるシステムに施す必要がある。

5. まとめ

本論文では、WWW上のECシステムに対する不正利用に対して、利用者の行動モデルと統計的手法を用いて検出する方法の概要について述べるとともに、実現に際して必要なモデルや数量化に関する考察を行い、システムとして構築する際に必要な技術に関しても述べた。

今後は、試験的なシステムを構築し、試験利用を通じてあらかじめ想定した購買行動を検証し、周辺ツールの充実やモデルの構築・修正を行いつつ、実システムとしての運用を目指す予定である。

参考文献

[1] D. E. Denning, "An intrusion-detection model", IEEE Trans. on Software Engineering., Vol. SE-13, No. 2, pp. 222-232, Feb 1987.

[2] B. Mukherjee, L. T. Heberlein, and K. N. Levitt, "Network Intrusion Detection," IEEE Network., pp. 26-41, May/June 1994.