行き先表示機能をつけたアクセス制御システム

1S-07　　林 昌樹　　中村 康弘

防衛大学校 情報工学科

1. はじめに

近年，ネットワークを介したコンピュータの不正アクセスが社会問題化しており，ファイアウォールや侵入検知システム (IDS) などに関する研究が盛んに行われている [1]．さまざまな不正アクセスの中でもとくに，許可されていない者による不正侵入は情報の盗用や改ざんなどの原因となり，その被害も大きい．しかしながら一般にこのような不正侵入は，あらかじめ許可された利用者のアカウントの盗用などにより発生するため，不正であるか否かの判断が難しい．すなわち，ネットワーク上の通信を静的に監視して不正侵入を自動検出するためには，その兆候や頻度などの統計量を用いる必要があり，完全な自動検出は難しいと考えられる [2]．

そこで我々は，インタラクティブな TCP セッションに関しては，そのクライアント側に必ず当該利用者が居るはずであるという原則 [3] を仮定し，利用者個人の実世界上での所在地を管理することによりアクセス管理を行うオンライン行き先表示板を提案する．利用者は帰宅や出張などにより自身の所在地が変る際にその行き先を登録し，接続依頼を受けたサーバは通常のユーザ名・パスワードとともに接続元の正当性を確認することにより，アカウントの盗用などによる「本人が居ないはずの場所」からの接続を拒否することができる．ここではシステムの概要と実験システムによる検証結果について報告する．

2. システムの概要

通常のアクセス管理においては利用者のユーザ名とパスワードの組を認証情報としており，登録済みの情報と一致しさえすればシステムの使用が許可される．このため利用者名の盗用などの問題が起こる．我々はここで，許可された使用者自身は実世界上の唯一個所にのみ所在しているはずであるという原則に注目し，利用者が物理的に所在しているドメインあるいはマシンからの接続のみを許可するようにアクセス管理方式を拡張する．この方式により，たとえユーザ名・パスワードが一致しようとも，当該利用者が今居るはずの場所（以下，所在地という）以外からの接続を拒否することができる．**(図1(a))**

また，利用者は実世界上で移動する（すなわち所在地が変わる）可能性があるため，その日時と行き先をリアルタイムに管理する必要がある．そこで利用者の所在地管理のための行き先管理サーバを設置し，利用者の所在地が変更になる際はこのサーバに登録手続きを行う．接続要求を受けたマシンは，ユーザ名・パスワードの確認とともに，クライアントのドメイン情報をもとに行き先管理サーバに問い合わせを行い，登録済みの行き先ドメインからの接続であることを確認する．登録日時を過ぎると登録ドメインからの接続のみが許可され，現在接続しているドメインからの接続さえも拒否される．**(図1(b))**

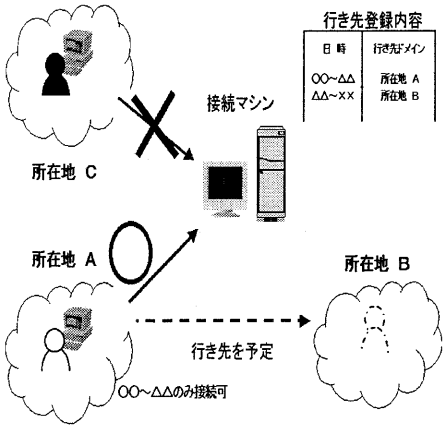
3. 実装方法

本方式はインタラクティブなセッションの特性を利用しているため，アプリケーション層でのみの実装に限って検証を行った．具体的には telnet や rlogin をクライアントとして，対応する daemon のユーザ認証部分に，行き先に基づくクライアント認証機能を追加することにより実装した．

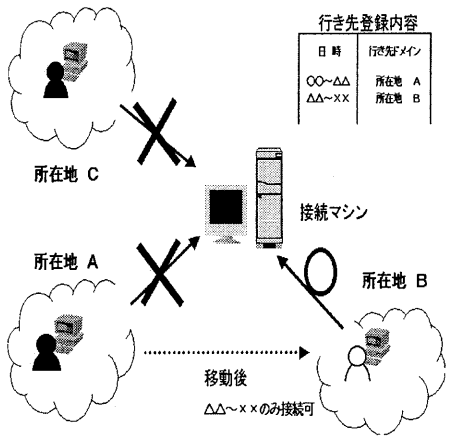
3.1 行き先登録手続き

利用者は所在地の変更に際して，行き先管理サーバに以下の形式の情報を登録する．この登録手続きは現在の所在地からのみ可能である．

An access control method using user location management system
Masaki Hayashi, Yasuhiro Nakamura
Department of Computer Science,
National Defense Academy



(a) 移動前の状態



(b) 移動後の状態

図 1: システム概要

日時	YYYY/MM/DD HH:MM:SS
行き先ドメイン	domain.jp

3.2 クライアント認証手続き

接続要求を受けたマシンはクライアントのドメイン情報を元に，行き先管理サーバに問い合わせを行う．問い合わせメッセージ形式は以下の通りである．

ユーザ名	ドメイン名

これに対し行き先管理サーバは，現在時刻と当該利用者の行き先ドメイン情報を元に問い合わせ内容の正当性を確認し，登録済みの正しい行き先からの接続であるか否かを返答する．

4. システムの評価

本システムを用いることにより，登録されていない日時・場所からのアクセスを拒否することができるため，アカウントの盗用などによる不正侵入を防止することができる．また，サーバ側のみで実装することができ，クライアントに対しては従来通りのユーザ名・パスワードのみを要求するため，特別なクライアントプログラムを用意する必要がなく，本システムの存在を秘匿することができる．

一方，行き先管理サーバへの行き先登録手続き時においても同様の認証を行うため，行き先管理情報と利用者の実際の所在地は常に一致していなければならない．実運用上の利便性との兼ね合いについてはさらに検討を加える必要がある．

5. まとめ

利用者の物理的な所在地を管理する行き先管理サーバを用いたアクセス制御システムを提案し，実験システムを構築してその評価を行った．本システムによりアカウントの盗用などによる利用者の所在地外からの不正侵入を防止することができる．行き先の登録方法などのユーザインターフェースについて改良していく必要がある．

参考文献

[1] 小林信博，勝山光太郎，“環境適応型侵入検知システム，”2000 年暗号と情報セキュリティ・シンポジウム講演論文集，SCIS2000-D20，January，2000.

[2] 高田哲司，小池秀樹，”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，pp2216-2227，2000.

[3] 飯田恭弘，佐藤直之，鈴木英明，”バイオメトリクスを用いたユーザを識別しない認証方式の実装，”情報処理学会第 61 回全国大会論文集，3F-03，2000.