携帯端末に対応した侵入対策環境の構築

2G－2

田中俊久　坂上仁志　高橋豊
姫路工業大学工学部

1．はじめに

近年，web siteの改竄やDDoS攻撃によるサーバのダウンなど，クラッカーによる攻撃が増加しており，セキュリティへの関心が高まっている．また，個人の常時接続も普及してきており，個人でサーバを持つ機会が増加している．クラッカーにとっては個人サーバも攻撃対象であり，個人レベルで攻撃から身を守る事が必要となっている．現在，攻撃から身を守る手段として，さまざまな侵入検知システムが商用製品やフリーウェアとして存在する．これらのシステムは侵入を検知した際に，管理者にメールで通知したり，自動的にスクリプトを起動するなどの対策を施せる．更に，携帯端末の急速な普及により，侵入検知システムからの通知を携帯端末にメールとして送信することで，時間や場所を選ばずに管理者に侵入事象を知らせることが可能になった．しかし，侵入を通知しても，管理者がすぐに侵入対策を実施できる環境にいるとは限らない．そこで，本研究では，最も身近なwebへの接続手段である携帯端末を用いてweb siteを介して現状を把握し，侵入対策を施す環境を提供する侵入対策管理システムを開発する．

2．システム構成

本研究では侵入対策管理システムとして，IPパケットを常時監視し侵入検知を行う侵入検知システム(IDS)，侵入対策を一元的に行う集中侵入対策システム(CIS)，携帯端末を用いてネットワーク内の情報収集や侵入対策要求を行うための機能を提供する携帯端末ゲートウェイシステム(PGS)を開発した．これら3システムのシステム構成を図1に示す．図1において，Rはルータ，FWはファイアウォールである．

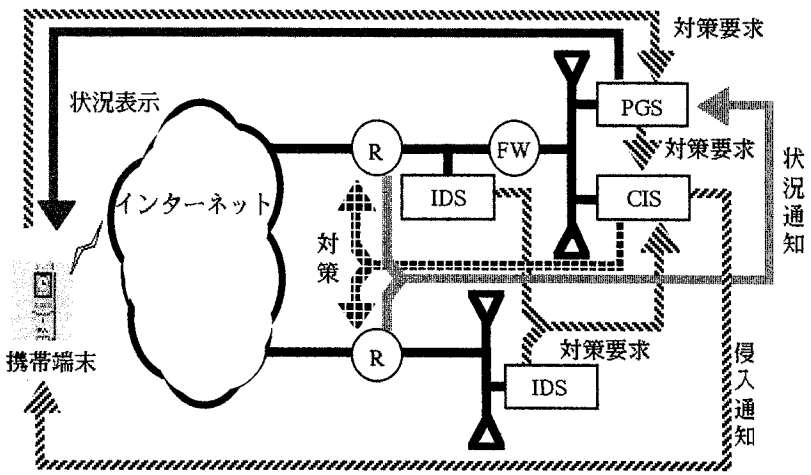

図1　システム構成

The construction of intrusion countermeasure environment with portable terminals

Toshihisa Tanaka , Hitoshi Sakagami , Yutaka Takahashi
Faculty of Technology, Himeji Institute of Technology

本研究で開発した侵入検知システムは，プローブとして侵入検知専用にディスクレスの超小型サーバを使用することを考慮し，プログラムサイズや消費メモリを少なくした．また，対策要求送信等の通信が必要なとき以外はインターフェイスにIPアドレスを割り当てないことで，プローブが外部からの攻撃対象にならないようにした．本システムでは，同一ホストの複数ポートに対するポートスキャン，複数ホストの同一ポートに対するアドレススキャン，許可IP以外からのftp，telnet等の特定のポートに対する接続要求，自ネットワーク内のマシンのIPスプーフィングなどを検出できる．従来のポートスキャン検出ツールは，一定時間以内に同一IPから，管理者が設定した閾値以上の接続要求が来た場合に検出し，HTTP，DNSなど誤検知が発生しやすいポートに対する接続要求を監視対象から除外する設定を行うものが多い．しかし，除外すると本当の攻撃を見逃す可能性がある．本システムはポート毎に閾値を設定することで，誤検知や未検知に対応している．ルールにはTCPフラグ，送信元・受信先ポート，通信を許可する送信元・受信先IPの範囲，侵入とみなす閾値を指定する．本システムはIPパケットを常時監視し，ヘッダから送信元・受信先ポート，TCPフラグを解析して該当するルールを検索し，許可されたIP以外の通信であれば，送信元・受信先IP毎に不許可パケット数を加算し，不許可パケット数が閾値以上になると侵入とみなし，集中侵入対策システムに対して対策要求を行う．

集中侵入対策システムは，侵入検知システムや携帯端末ゲートウェイシステムからの対策要求を受け取ると，要求の内容をactionテーブルと呼ばれる，管理者が任意に付けたアクション名と，実際に実行するコマンドの対応を表にしたものを用いて実際のコマンドを実行する．実行可能なコマンドはactionテーブルに記述されたもののみであり，対策要求時にはアクション名を用いるため，アクション名に推測の困難な文字列を使用することで，悪意あるユーザによるコマンドの実行を防止する．現在，侵入検知システムから対策要求を受け取った際に，管理者の携帯端末に侵入を通知するメールを送信したり，CISCO-4000とLINUXに対して，トラフィックログの取得，攻撃元へのルートの破棄，インターフェイスの一定時間shutdown等を指示することができる．

携帯端末ゲートウェイシステムは，携帯端末から対策要求やルータ等の情報表示を行うためのユーザインターフェイスを提供する．管理者は集中侵入対策システムから侵入通知を受け取ると，携帯端末を用いて携帯端末ゲートウェイシステムに接続し対策要求を行う．管理者が対策要求を行うと，携帯端末ゲートウェイシステムは集中侵入対策システムに対策要求を転送する．また，携帯端末ゲートウェイシステムから，ルータや侵入検知システムを実装したプローブ等に接続し，現在の状況を取得して，携帯端末上に表示することもできる．現在，携帯端末上で，ルータのトラフィック量のグラフ表示，プローブが監視する各セグメント上を現在流れるトラフィック情報の表示，CISCO-4000やLINUX上で侵入調査のために必要な各種コマンドの実行と結果の表示を行える．これらのルータの状況表示を要求する際，ルータのIPやドメイン名とは関係ない，管理者が設定したニックネームを用いてルータを指定する事で，管理者以外が情報を取得する事を防止する．集中侵入対策システムはルータのニックネームから，IP，パスワードなどのルータの情報を引き出し，それを用いてルータに接続する．

3．まとめ

本研究では，携帯端末を用いてweb siteやメールを介して現状を把握し，侵入対策を施す環境を提供する侵入対策システムを開発した．本システムは，IPパケットを常時監視し侵入検知を行う侵入検知システム，侵入対策を一元的に実行する集中侵入対策システム，および，携帯端末上でネットワーク内の情報収集や侵入対策要求を行う機能を提供する携帯端末ゲートウェイシステムから構成される．このシステムにより，管理者は侵入通知を受け，携帯端末を用いてその場で即時対策を施す事が可能となった．