おとり誘導装置の試作[1]

2H−03

河内 清人, 藤井 誠司, 木下 洋輔, 芦沢 賢, 勝山 光太郎[2]
三菱電機(株) 情報技術総合研究所[3], 通信機製作所[4]

1. 背景

近年，攻撃をおとりサーバと呼ばれる偽のサーバに誘導することで，本来のサーバを保護しつつ，情報収集を可能とする技術が注目されている．

この誘導技術の実現手法として，Proxyを正規のサーバの前段に配置することで攻撃を動的におとりへと誘導する方式が提案されている[1].

しかし，Proxyを用いた方法は，誘導可能な通信プロトコルが制限されてしまう．また，DNS参照など，おとりサーバから外部ネットワークへのアクセスが行えないという問題点もある．

そこで今回，筆者らはこれらの問題点を解決する誘導技術の検討を行い試作を行った．

本システムの特長は以下の通りである．

- ルータとしてパケットを誘導することで，プロトコル非依存性を実現した．
- 誘導するパケットにアドレス変換を施すことで，おとりサーバから外部へのアクセスを可能にした．

以下，本システムについて説明する．

2. システム構成

図1は，本システムの全体構成を表している．本システムは，おとり誘導装置，侵入検知装置(IDS)，全体制御という3つのコンポーネントで構成されており，外部LAN，正規LAN，おとりLANと呼ばれる3つのLANに接続することで機能する．

- 外部 LAN...ルータを介して外部ネットワークと接続されているLAN
- 正規 LAN...本システムで保護する対象となるサーバ(正規サーバ)群が配置されているLAN
- おとり LAN...攻撃者が誘導されるおとりサーバ群が配置されているLAN．各おとりサーバには，対応する正規サーバと同一のIPアドレスが割り当てられている．

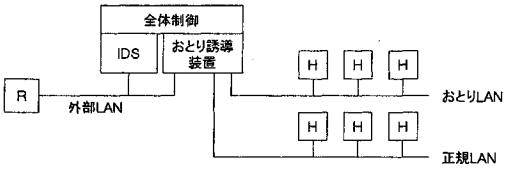

図 1 全体構成図

おとり誘導装置が本システムの核となるコンポーネントである．上記LAN全てに接続され，正規の通信を正規LANへと転送しつつ，攻撃者からの通信をおとりLANへと振り向ける役割を持つ．

おとり誘導装置について，更に詳しく説明する．図2は，同装置の内部構成を示している．

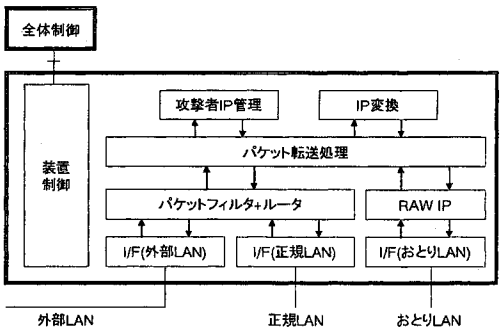

図 2 おとり誘導装置内部構成

パケットフィルタは，外部LANから受信したパケットを，フィルタルールに基づいて正規LANに転送するか，おとりLANに転送するかを決定する．

パケット転送処理ブロックは，外部LANとおとり

---

[1] Prototyping of an intrusion trap
[2] Kiyoto KAWAUCHI, Seiji FUJII, Yosuke KINOSHITA, Satoshi ASHIZAWA, Kotaro KATSUYAMA
[3] Mitsubishi Electric Corporation, Information Technology R&D Center 5-1-1, Ofuna, Kamakura, Kanagawa, 247-8501, JAPAN
[4] Mitsubishi Electric Corporation, Communication Systems Center 8-1-1, Tsukaguchi-Honmachi, Amagasaki, Hyogo, 661-8661, JAPAN

LAN との間のパケット転送処理を行う．このときに IP アドレス変換が行われる場合もある(後述)．

RAW IP ブロックは，おとり LAN とパケットを送受信するための機能ブロックであり，ARP やルーティング処理を行う．

装置制御ブロックは全体制御コンポーネントからの指示に基づいて，装置の初期化，終了及びおとり誘導ルールの更新を行う．

3. システム動作

次に本システムのパケット転送動作について説明する．

3.1. 正規ユーザと正規サーバとの通信

外部 LAN からおとり誘導装置に入力されたパケットは，パケットフィルタ内でその送信元アドレスをチェックされる．攻撃者として登録されたアドレスでなければ，正規 LAN に転送される．

正規 LAN からのパケットは無条件にその送信先アドレスへと転送される．

3.2. 攻撃者とおとりサーバとの通信

IDS によって攻撃が検出されると，通信が遮断され，同時に全体制御がおとり誘導装置に対し，攻撃者として認定されたアドレスを設定する．

以降，同一の送信元アドレスから来たパケットは，パケットフィルタによってパケット転送処理ブロックに渡され，そこから RAW IP ブロックを経由しておとり LAN に送出されるようになる．

一方，おとりサーバからの応答は RAW IP ブロックを経て，パケット転送処理ブロックに渡される．

同ブロックはパケットの送信先アドレスが攻撃者のアドレスと一致することを確認し，パケットフィルタを通じて，パケットを攻撃者へと転送する．

このように，攻撃者とおとりサーバとの間で透過的にパケットを転送することで，プロトコル非依存の誘導機能を実現することができる．

3.3. おとりサーバと外部との通信

おとり LAN 内のホストが攻撃者以外と通信を行う場合，単純にパケットを転送するのみだと，外部ホストからのレスポンスが全て正規サーバに転送されてしまうという問題が生じる．

本システムでは，おとりサーバから攻撃者以外のホストに送信されるパケットに対して IP アドレス変換を行うことでこの問題を解決している．

おとりサーバから送出されたパケットは攻撃者宛でない場合，おとり誘導装置内で，送信元アドレスを変換されてから，外部に転送される．

反対に外部サーバからのレスポンスは，送信先アドレスが本来のアドレスに修正されてから，おとり LAN 上に転送される．

これらのアドレス変換の様子を図 3 に示した．

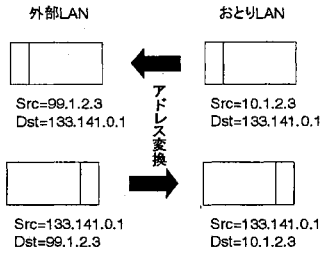

図 3 IP アドレス変換

4. まとめ・今後の課題

パケット転送型のおとり誘導方式を提案した．本方式は，Proxy 型の方式と比較して，次のような特長を持っている．

- プロトコル非依存の誘導機能
- アドレス変換によるおとりと外部との通信の実現

現在，本方式に基づいたおとり誘導装置を Windows 2000 上に試作中である．更に今後の課題として以下を検討中である．

- アドレス変換を高度化(NAT 化)
- 通信状態を管理し，仮想アドレスへの攻撃を防止
- 正規サーバとおとりサーバとの状態同期

5. 参考文献

[1] 竹森, 力武, 田中, 清本, 中尾, “Intrusion Trap System の実装および評価”, 情報処理学会 CSEC pp415-420, 2001 年 10 月