ネットワークの仮想化によるハニーポットの集中管理
Centralized Control of Honeypot System by using Virtual Networks

石川 哲[†]　　蓑原 隆[††]
[†] 拓殖大学大学院 工学研究科 電子情報工学専攻
[††] 拓殖大学 工学部 情報工学科

概 要

不正アクセス検知，解析の手法としておとりを用いて攻撃を誘導するハニーポットの技術が注目されている．ハニーポットへのアクセスは不正なものかエラーであると判断できるため，ネットワーク型のIDSなどに比べてfalse positive, false negativeを削減できるという利点があるが，監視対象がハニーポットへのアクセスに限定される点，ハニーポットを不正アクセスに利用されてしまう危険性がある点という欠点もある．しかも，前者の欠点を解消するために複数のネットワークにハニーポットを設置すると，管理コストが増大し，後者の欠点が深刻化するという問題がある．本稿では，仮想ネットワークを用いてハニーポットへのアクセスを調査対象ネットワークから実際にハニーポットを設置する管理ネットワークに転送することで，複数のネットワークの監視と，ハニーポットの集中的な管理を両立させることを目的として，仮想ネットワークの構成方法についての検討とプロトタイプシステムの実現について報告する．

1　はじめに

コンピュータネットワークの普及にともない，システムへの不正アクセスの問題が深刻化している．不正アクセスに対抗するためファイアウォールやIDSなどの対策がとられているが，必ずしも全ての攻撃を防げるわけではない[1]．そこで，対策をくぐり抜けた攻撃を早期に検出，解析することが重要になっている．現在，不正アクセスの検出，解析の手法として注目されている技術にハニーポットがある[2][3]．

ハニーポットとは，攻撃者のアクセスを受けるためにおとりとして設置されるサーバあるいはネットワーク機器を指す．ハニーポットを利用すると攻撃者のアクセスに反応すると同時に，その活動の記録を残すことで，攻撃者の特定や手法の解析に必要な情報を収集することができる．また，正常な利用者は誤操作などを除いてはハニーポットをアクセスしないと考えられることから，正常通信を含む情報から不正アクセスのシグネチャと一致するものを検出する通常のIDSと比較して次のような利点がある．

- 処理するデータ量が少ない．不正アクセスやエラーの量は正常な通信と比較して少ないと考えられる．
- false positiveを削減できる．正常な通信の対象でないことから，正常の通信を誤って不正アクセスと判断しない．
- false negative対策になる．シグネチャが登録されていない未知の攻撃でもハニーポットに対するアクセスは不正であると判断できる．

一方，次のような欠点も指摘されている．

- 監視対象が限定される．ハニーポット以外のサーバに対するアクセスは検知の対象外になる．

- 不正アクセスの経路となる危険性がある．ハニーポットに対するアクセスを許可することで，潜在的な侵入の危険性を持たせることになる．

前者の欠点に対する直感的な解決策として，正常なサービスに使用されていない全てのアドレスを監視対象にするなど，ハニーポットの設置箇所を増やしていくことが考えられる．分散ハニーポットとして，複数のハニーポットで収集した不正アクセスの情報を管理サーバに送って解析するアイデアも示されている[3]．一方，後者の欠点に対しては，ハニーポットが侵入経路にならないように十分な管理下に置く以外の対策は難しい．しかし，ハニーポットの設置箇所が増加すればするほど，十分な管理を行うことは困難になってくる．

Spitznerは，ハニーポットを分散的に設置する代りに攻撃者のアクセスをハニーポットを設置したネットワークに転送するというアイデアを示し，ハニーポット・ファームと名付けている[3][4]．ハニーポット・ファームのアイデアに従えば，不正アクセスにさらされるハニーポットを管理者の手元に置けることから，攻撃者によって利用される危険性を軽減できる可能性がある．また，複数のネットワークの監視をひとつハニーポットのみでおこなうことも可能と考えられる．しかし，転送メカニズムなど，ハニーポット・ファームの技術はまだ確立されているとは言えない．

本研究では，少ない管理者によって効率的にハニーポットを設置，運用することを目的として，ハニーポットを管理者の手元に置いた状態で，遠隔地のネットワークの調査を行うハニーポット・ファーム型のシステムについて，攻撃者からのアクセスを管理ネットワークに転送するための仮想ネットワークの構成方法について検討を行う．また，検討結果として選択された方法の実現についてプロトタイプを作成して評価する．

2 ハニーポットの集中管理のための仮想ネットワークの構成

複数のネットワークの監視とハニーポットの集中管理の両方を実現するためには，ハニーポットを管理用のネットワークに設置した状態で，あたかも調査対象のネットワークに直接接続したように見せる必要がある．これは2つのネットワークを仮想的に接続し，調査対象のネットワークに到着したパケットを管理ネットワークに転送してハニーポットに受信させ，ハニーポットの応答を逆に転送して，調査対象のネットワークから送り出すことで実現される．このとき調査対象のネットワークには，通常のサービスを提供するサーバも存在すると考えられることから，仮想ネットワークによる転送を行うかどうかをアクセス先によって振り分ける必要がある．

仮想ネットワークの構成は，仮想ネットワークを実現する装置 (VPN 装置) を設置する場所と通信レイヤの組み合せで決定される．VPN 装置の設置場所としては，図1に示すようにネットワークのルータ部に設置する方法と，図2に示すようにネットワークの端末部に設置する方法が考えられる．以下，前者をルータ型VPN，後者をブリッジ型VPNと呼ぶ．

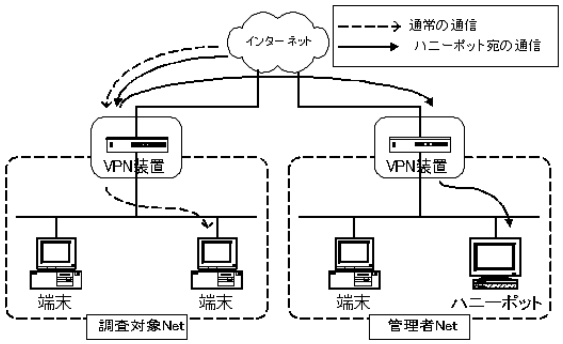

図 1: ルータ型 VPN

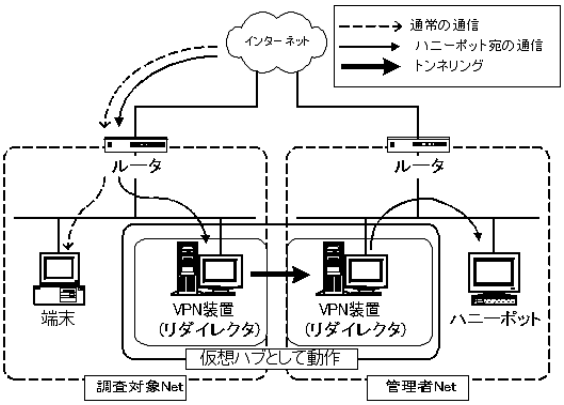

図 2: ブリッジ型 VPN

また，仮想ネットワークの通信レイヤとしては，レイヤ 3(IP 層)，レイヤ 2(リンク層) の 2 通りが考えられる．以下，これらの組み合せについて検討を行う．

2.1 ルータ型 VPN

ルータ型VPNでは，図1に示したように調査対象と管理者の 2 つのネットワーク間で VPN ルータを用いたトンネリングを行い仮想ネットワークを構築する．したがって既存のネットワークを調査対象とするには，ルータ装置を置き換える必要がある．調査対象のネットワークに複数のルータが接続されている場合には，それら全ての置き換えが必要になる場合がある．ただし IP アドレスとしては，VPN のための通信も既存のルータで使われていたアドレスを使って実現できるので，ルータに対して新たにアドレスを割り当てる必要はない．

外部からハニーポットへのアクセスは次の手順で行なわれる．

1. 外部から調査対象ネットワークに送られたパケットをルータが振り分け，ハニーポット宛てのパケットを管理ネットワークに転送する．
2. 管理ネットワークのルータが，転送されたパケットを管理ネットワーク内のハニーポットに対して再送信する．

ハニーポットが生成した応答は，逆のルートをたどり，調査対象ネットワーク側のルータから外部に再送信される．

仮想ネットワークの通信レイヤの違いは，パケットの振り分けに関連する．仮想ネットワークをレイヤ 3 で実現する場合，調査対象ネットワークのルータは，終点 IP アドレスを見て管理ネットワークに転送するかどうかを判断することになる．すなわち，ネットワークの振り分けの判断は調査ネットワーク側で行う必要があり，調査対象ネットワークのルータは，どのアドレスがハニーポット宛てであるのかを情報として保持しなければならない．

ルータ型 VPN をレイヤ 2 の仮想ネットワークとして構成する場合は，終点 IP アドレスでの振り分けではなく，ARP によってアドレス解決を行うことになる．アドレス解決は，調査対象ネットワーク，管理ネットワークの両方で行う必要があるが，余分な通信を避けるためには，調査対象ネットワークでアドレス解決を行って解決できない場合に管理ネットワークにパケットを転送してアドレス解決を行う方がよい．ハニーポットがパケットを受けとるかどうかは，ハニーポットが ARP リクエストに答えるかどうかで決められるので，レイヤ 3 と異なりネットワークの振り分けは管理ネットワーク側でできるが，アドレス解決を効率よく行うには複雑な制御が必要になる．

2.2 ブリッジ型 VPN

ブリッジ型 VPN は，図 2 に示したように仮想ネットワークで接続する各ネットワークの端末としてトンネリングを行う専用の VPN 装置を設置する．以下この VPN 装置をリダイレクタと呼ぶ．既存のネットワークを調査対象とするには，ネットワークに新たにリダイレクタを接続する必要があるが．調査対象のネットワークに複数のルータが接続されていてもリダイレクタは 1 つだけ設置すればよい．ただし，リダイレクタは新しいホストとなるので，VPN の通信のために，新しい IP アドレスを少なくとも 1 つ割り当てる必要がある．

外部からハニーポットへのアクセスは次の手順で行なわれる．

1. 外部から調査対象ネットワークに送られたパケットのアドレス解決をルータが行いハニーポット宛てのパケットは調査対象ネットワークのリダイレクタに送られる．
2. リダイレクタ間でパケットが転送され，管理ネットワークのリダイレクタが，転送されたパケットを管理ネットワーク内のハニーポットに対して再送信する．

ハニーポットが生成した応答は，逆のルートをたどり，調査対象ネットワーク側のリダイレクタからルータを経由して外部に送信される．

ブリッジ型 VPN のパケットの振り分けは，調査対象ネットワークのリダイレクタが ARP リクエストに応答することで行われる．仮想ネットワークをレイヤ 3 で実現する場合，応答するアドレスを調査ネットワークのリダイレクタが判断することになる．すなわち，ネットワークの振り分けの判断は調査ネットワーク側で行う必要があり，調査対象ネットワークのリダイレクタは，どのアドレスがハニーポット宛てであるのかを情報として保持しなければならない

ブリッジ型 VPN をレイヤ 2 の仮想ネットワークとして構成する場合は，調査対象ネットワーク

の ARP リクエストが管理ネットワークに転送され，ブロードキャストされる．ハニーポットがリクエストに応答すると，それが逆向きに調査ネットワークに転送されて，アドレス解決が行われる．ネットワークの振り分けは管理ネットワーク側でできるが，ブロードキャストパケットを管理ネットワークに転送するというオーバヘッドが生じる．

2.3 VPN 方式の比較

ハニーポットの集中管理を実現するための仮想ネットワークの構成についての比較は次のようにまとめられる．

レイヤ 3 ルータ型 VPN

- 調査対象ネットワークのルータの置き換えが必要
- VPN 通信のための IP アドレスの割り当てが不要
- 調査対象のアドレスの調査ネットワーク側での保持が必要

レイヤ 2 ルータ型 VPN

- 調査対象ネットワークのルータの置き換えが必要
- VPN 通信のための IP アドレスの割り当てが不要
- 調査対象のアドレスの調査ネットワーク側での保持が不要
- アドレス解決の通信が複雑

レイヤ 3 ブリッジ型 VPN

- 調査対象ネットワークにリダイレクタ (端末) を接続
- VPN 通信のための IP アドレスの割り当てが必要
- 調査対象のアドレスの調査ネットワーク側での保持が必要

レイヤ 2 ブリッジ型 VPN

- 調査対象ネットワークにリダイレクタ (端末) を接続
- VPN 通信のための IP アドレスの割り当てが必要
- 調査対象のアドレスの調査ネットワーク側での保持が不要
- アドレス解決のブロードキャスト通信の転送が必要

以上の結果から，ブロードキャスト通信のトラフィックを許容可能であれば，設置および管理のコストの点で，レイヤ 2 ブリッジ型 VPN が有利であると考えられる．

3 ネットワーク仮想化の実現

前節の結果から，ハニーポットの集中化に適していると考えられるレイヤ 2 ブリッジ型 VPN について実装を行った．VPN を構成するリダイレクタはプロトタイプの実験装置として Linux を OS とする PC のプロセスとして実現した．

リダイレクタの処理は図 3 に示すように 1 組の入力処理と出力処理からなる．入力処理はプロミスキャスモードに設定したインターフェースから受信したパケットをカプセル化し対向のリダイレクタに送信する．

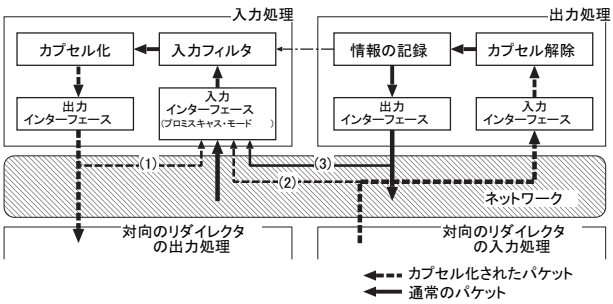

図 3: パケットの流れ

カプセル化されたパケットは出力処理によって受信され，カプセル化を解除した後ネットワークに送信される．このとき入力処理において本来処理すべきパケットの他に次のパケットが受信されてしまう．

1. 自身が出力したカプセル化したパケット
2. 対向のリダイレクタから送られてきたカプセル化されたパケット
3. 自身の出力処理によってカプセル化を解除されて送信されたパケット

これらのパケットを再度カプセル化してしまうことを防ぐため，入力処理においてパケットの破棄を行う．上記の問題のパケットのうち 1，2 についてはイーサネットの始点，終点アドレスのいずれかが自分のアドレスであることで判別できる．3 のパケットはアドレスのみからは判断できないため出力処理でカプセル化を解除したパケットの情報を記録し入力パケットと比較して破棄する．表 1 にパケットを破棄する条件を示す．

表 1: ループバックパケットの破棄

入力	処理
始点アドレスが自分の MAC アドレス	破棄
終点アドレスが自分の MAC アドレス	破棄
カプセル化を解除されたパケット	破棄
上記以外	通過

なお，プロトタイプのトンネリングはパケットをそのまま UDP のペイロードとしてカプセル化することで実現した．

4　実験による遅延時間の評価

ハニーポット・ファーム型のハニーポットの集中管理における問題点は，調査対象のネットワークに直接ハニーポットを接続した場合に比べて応答時間が余分に必要になることにある．オーバヘッドとなる遅延時間は，調査対象ネットワークと管理ネットワーク間の往復通信遅延時間とトンネリング処理に必要な時間からなる．これらを評価するために実験を行った．

4.1　実験装置

実験ネットワークは，図 4 に示すように，調査対象ネットワーク，管理ネットワークおよび，それらを接続するネットワークの 3 つのセグメントをブロードバンドルータで接続した．

2 台の PC をリダイレクタとして構成し，調査対象，管理の両ネットワークに接続し，管理ネットワークにハニーポットの PC を接続した．攻撃者のコンピュータは一般性を失わないと考えて調査対象ネットワークに直接接続した．なお，ネットワークの各セグメントは 100Mbps のスイッチングハブを用いて構成している．リダイレクタを実現する PC の仕様を表 2 に示す．

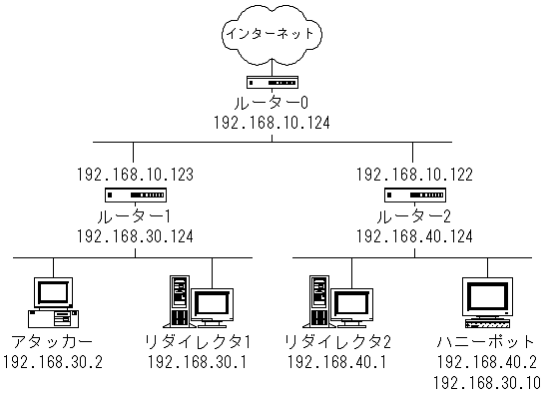

図 4: 実験ネットワークの構成

表 2: リダイレクタ PC の仕様

CPU	Intel Celeron 400MHz
メモリ	128MByte
NIC	Intel Pro/100

4.2　遅延時間実験

仮想ネットワークのオーバヘッド (T_{total}) は管理ネットワークまで往復通信遅延時間 (T_{rtt}) とトンネリング処理時間 (T_{tunnel}) からなる．

$$T_{total} = T_{rtt} + T_{tunnel}$$

このうち T_{rtt} はトンネリングを無効にすれば単独で測定が可能なので，トンネリングを有効にした場合との差でトンネリング処理時間を求める．

測定は，攻撃者コンピュータからハニーポットにペイロードサイズを変えて ping を実行して行った．ペイロードサイズごとに 10 回測定した平均をプロットしたものを図 5 に示す．

4.3　考察

グラフからトンネリング処理時間はパケットサイズの変化に対して比較的ゆるやかに変化していることがわかる．トンネリング処理時間の平均は 1Kbyte 時に 2.69ms で，管理ネットワークまでの距離には影響されない．実験ネットワークでは管理ネットワークと調査対象ネットワークが近いが，

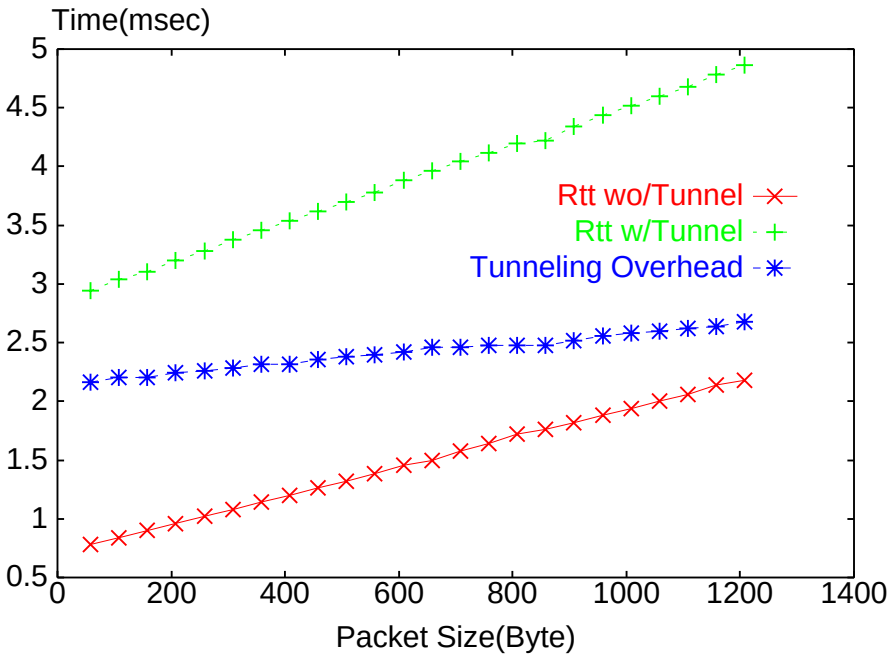

図 5: オーバヘッド測定結果

距離が離れるにつれて仮想ネットワークのオーバヘッドは，ネットワーク間の通信遅延時間が支配的になることが予想される．このことから，ハニーポット・ファーム型のハニーポットの集中運用は，攻撃者からの調査対象ネットワークまでの通信遅延時間に比べて，調査対象ネットワークから管理ネットワークまでの通信遅延時間が十分に小さい場合に有効だと考えられる．転送オーバヘッドが小さい場合にも，正規のサービスと比較することで攻撃者によってハニーポットを識別される可能性はあるが，スクリプトを使った自動攻撃など攻撃者が十分な識別能力を持たない場合にも有効であると考えられる．

5　まとめ

本研究では調査対象のネットワークと管理者のネットワークを仮想的に結合することにより管理者の手元にハニーポットを設置し，遠隔地のネットワークの調査，監視を行うハニーポットファーム型のシステムについて，仮想ネットワークの構成方法について検討を行い，設置，設定コストの点で，レイヤ 2 のブリッジ構成が適しているという結論を得た．

さらにブリッジ構成の VPN 機能を 2 台の Linux PC にプロセスとして実装し動作を確認した．

ハニーポット・ファームによるネットワーク監視では，監視対象のアドレスとしてどのアドレスを設定するかが重要だと考えられる．レイヤ 2 ブリッジ構成により，監視対象アドレスは管理ネットワーク側で設定可能だが，監視アドレス決定などハニーポット設置，設定を支援するシステムが必要であり，これらを開発することが今後の課題である．

参考文献

[1] 武田圭史:“侵入検知システムに関する研究の現状”, 情報処理学会誌 Vol.42 No.12-005 pp.1169-1174 2001.

[2] Lance Spitzner:“Honeypts ハニーポット-ネットワーク・セキュリティのおとりシステム-”, 小池 他訳, 慶應義塾大学出版会 pp.55-103 2004.

[3] The Honeynet Project 著 : “Know Your Enemy –Learning about Security Threats–”, Addison Wesley 2004.

[4] Lance Spizner : “Haneypot Farms”, http://www.securityfocus.com/printable/infocus/1720, Aug. 2003.