オープンソースIDSとハニーポットを組み合わせた不正侵入防止システム構築に関する研究

Illegal Invasion Prevention System Construction using Open Source IDS and Honeypot

088509G　比嘉 哲也　　指導教員:　玉城史朗，長田智和

1　はじめに

インターネットの発達とともに利用者も増え続け，さまざまなサービスがインターネット上で提供されている．サービスの中には，クレジットカード情報などの重要なデータを扱うものもあり，高いセキュリティ性が求められている．

このように，インターネットの重要性が高まるにつれて，セキュリティの重要性も高まってきている．ところが，中小規模事業者やSOHOなどで商用のセキュリティシステムを導入するとなると，高額なコストが問題となる．

そこで，本研究では，オープンソースで開発が行われている侵入検知システムのSnortと，ハニーポットのhoneydを組み合わせた不正侵入防止システムを構築する．オープンソースソフトウェアを利用することで，安価に導入可能なシステムを目指し，Snortとhoneydのログを利用してIPベースのフィルタリングをすることで保守・運用が容易なシステムを構築する．

2　技術概要

2.1　IDS

従来のファイアウォールでは通信内容までは監視しない．そのため，ファイアウォールをすり抜けてサーバの脆弱性に攻撃を行える欠点を持っている．通信内容まで検査し，攻撃や不正侵入の検知を行うのがIDS(Intrusion Detection System)である．設置箇所，検出手法により数種類に分類される．

2.2　ハニーポット

ハニーポットは脆弱性を持ったシステムをネットワーク上に設置することで，攻撃や不正侵入をおびき寄せ，攻撃・不正侵入方法の研究を行うために設置される．また，稼働しているシステムに組み込むことにより，攻撃者の目をハニーポットに向けさせ，サーバへの攻撃を回避する．ハニーポットは実装方法により，低対話型と高対話型に分類される．

3　既存システムの問題点

既存のセキュリティシステムにはいくつかの問題点が挙げられる．ファイアウォール，IDS，ハニーポットが持っている問題点は，大別して次の2つに分類される．

- 商用製品の導入には高額なコストがかかる
- 導入後の保守・運用が煩雑で初心者には敷居が高い

上記のように，ネットワークシステムのセキュリティ対策には，導入費用が高額になる問題や，保守・運用が煩雑になるといった問題が挙げられる．

4　解決手法

既存システムの問題点にあった問題を，提案手法を用い解決する．本システムではSnortとhoneydを利用し，攻撃・不正侵入の検知を行う．Snortだけでは未知の攻撃を検知することができないため，honeydを利用して，Snortが検知漏れを起こした攻撃・不正侵入の検知を行う．

また，Snortとhoneydに記録されたログより，攻撃者のIPアドレスを抽出し，IPアドレスベースのフィルタリングを行う．

このように，オープンソースソフトウェアを利用することで，システム構築にかかる費用を安価にする．Snortとhoneydのログを利用し，IPアドレスベースのフィルタリングを行うことで容易に保守・運用できるシステムの構築を行う．

5　事前実験

システム構築を行う前に，Snortとhoneydの攻撃・不正侵入に対する検知能力の調査を行った．

pingとnmapを用いてホストスキャンを行った結果を表1に示す．pingコマンドはSnort，honeydの両方で検知している．”nmap -sL”コマンドは，ホストの問い合わせにDNS問い合わせを使用している．Snortとhoneydに直接通信を行っていないため，検知できていない．”nmap -sP”コマンドはARP要求を用いてホストスキャンを行う．Snortにはは ARP要求に関するシグネチャが記述されていないため，検知できなかったと考えられる．また，honeydではIPパケットでなかったため，検知できていないと考えられる．

表 1: ホストスキャン結果

調査方法	Snort 検知結果	honeyd 検知結果
ping	検知	検知
nmap -sL	未検知	未検知
nmap -sP	未検知	未検知

次にnmapを使用したポートスキャンの結果を表2に示す．さまざまなオプションを使いポートスキャンを行った．結果はSnortとhoneyの両方で検知することができた．これはSnortにnmapに関する記述があったためである．

最後に汎用パケット作成ツールのhpingによってポートスキャンを行った結果を表3に示す．hpingでポートスキャ

表 2: ホストスキャン結果

調査方法	Snort 検知結果	honeyd 検知結果
nmap -sS	検知	検知
nmap -sT	検知	検知
nmap -sU	検知	検知
nmap -sN	検知	検知
nmap -sF	検知	検知
nmap -sX	検知	検知

表 3: hping ホストスキャン結果

調査方法	Snort 検知結果	honeyd 検知結果
hping Fin flag	未検知	検知
hping Syn flag	未検知	検知
hping Reset flag	未検知	検知
hping Push flag	未検知	検知
hping Ack flag	未検知	検知
hping Urgent flag	未検知	検知
hping UDPpacket	未検知	検知

ンを行った結果，Snort ではポートスキャンを検知できていない．

表 1，2，3 の結果より，honeyd の検知能力の高さが確認できた．

6　システム構築・動作結果

本提案システムの動作フロー図を図 1 に示す．Snort と honeyd で外部からの攻撃ログを取得する．取得したログから IP アドレスを抽出し，ブラックリストとして，iptables で適用を行い，攻撃のフィルタリングを行うシステムとなっている．

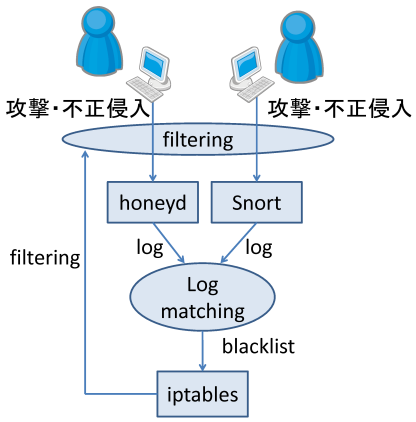

図 1: システムの動作フロー図

本システムの構成図を図 2 に示す．honeyd が偽装している仮想ホストに対しての攻撃は，honeyd 本体と Snort サーバによってログが取得される．ここで，honeyd は 30 台の仮想ホストと，特定のサービスが動作して見えるようにエミュレートした．Snort では，Snort 開発コミュニティより提供されているシグネチャを自動でダウンロードするように設定し，常に最新のシグネチャを適用している．

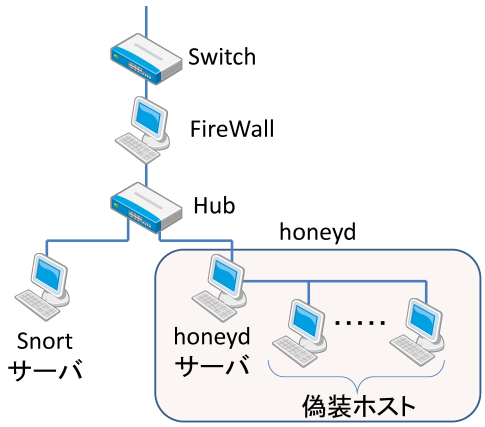

図 2: 提案システム構成図

次に本システムを稼働させ，IP ベースのフィルタリングを行った結果を図 3 と表 4 に示す．

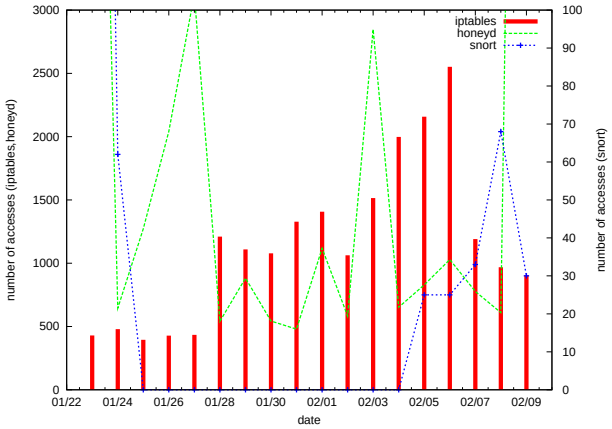

図 3: honeyd・iptables・Snort ログの検知結果比較グラフ

表 4: Snort・honeyd に対するアクセス数の変化

検知システム	平均検知数
Snort フィルタ前	353.8 件
Snort フィルタ後	100 件
honeyd フィルタ前	4752.9 件
honeyd フィルタ後	2186.1 件

図 3 ではフィルタリングを行った期間の Snort，honeyd，iptables で攻撃を検知した回数をグラフ化している．フィルタリングを行ってからは，Snort，honeyd ともにアクセス数は減少している．表 4 では，フィルタ導入前後でのアクセス数の変化を示している．フィルタ導入後では，Snort と honeyd に対するアクセス数は，Snort で約 30%，honeyd で約 45%に減少している．

7　まとめ

本論文では既知のセキュリティシステムの問題点を挙げ，それぞれの解決を図った．オープンソースソフトウェアを使用することで，システムを安価に構築した．また，導入後の保守・運用が容易なソフトウェアを組み合わせることで，初心者でも容易に保守・運用が可能なシステムを構築することができた．