# 卒業研究審査登録書の書式

G984822019 吉村　直将

指導教員　教授　蓑原　隆
助手　田島　信行

## 1　はじめに

### 1.1　研究背景

近年, サイバー攻撃の発生件数が年々増加してきており, その攻撃手法も多様化している．対策として, 攻撃者を誘き寄せ, 不正アクセスを受けるハニーポットを運用し, 攻撃者の情報を収集してきた. 過去の研究では, ハニーポットを利用して, ログイン試行時に使われる ID やパスワード, ログイン後に攻撃者から送られるシェルコマンド等の情報を収集し, 研究を行ってきた. 得られる情報の中でログイン後に送られるコマンドを解析することは、攻撃者がログイン成功後にどうゆう意図で, 何を目的をとして攻撃を行なってくるかの予測が立てらる．又, コマンドから攻撃者がダウンロードさせようとしてくる不正なソフトウェアの情報を知り、調査できる為, より最新の攻撃に対して具体的なセキュリティ対策につながると思われる．

### 1.2　攻撃ホストからハニーポットへの攻撃の流れ

攻撃者ホストからハニーポットへの攻撃の流れとして図 1 に示してある．攻撃ホストはハニーポットにログイン試行として ID/パスワードを送信してくる．ハニーポットはそれに対して, ログイン許可をしている風に見せる, 攻撃者はログイン後操作する為に, コマンドを送信する．この攻撃の中でハニーポットはログイン試行時に使われる ID やパスワード, ログイン後に攻撃者から送られるシェルコマンド等の情報を収集し, 収集した情報から攻撃手法の研究してきた.

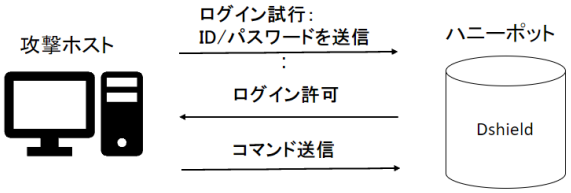


図 1　攻撃の流れ

### 1.3　目的

本研究では, より具体的な攻撃者の攻撃手法の情報を得る為、攻撃者がログイン成功後に行う攻撃に着目し, ハニーポットを用いることで, 攻撃者から送信されるコマンドやそのコマンドから入手できるファイルの情報を収集し, 解析するシステムを構築する. そして, 攻撃の分析を行い, 最新の攻撃内容について警告を発することを目的とする。

## 2　研究方法

本研究では, ハニーポット Dshield を用いる.DShield (Distributed Intrusion Detection System) は, グローバルなセキュリティコミュニティによって構築された分散型侵入検知システムである．世界中のネットワーク上で発生するセキュリティイベントのデータを収集し, 分析することでセキュリティの脅威情報を提供する.Dshield は研究室で以前から運用していたが, ログイン試行時の Id やパスワードを収集することを目的としたハニーポットであった．本研究では, ログイン後のコマンドを収集することが目的としている為, 新しくハニーポットを構築することとする.

本研究の目的である攻撃者がダウンロードさせようとしてくる不正なソフトウェアの解析を実現する為のシステムを図 2 に示す．ハニーポットはインターネットから攻撃受け, 攻撃者からのコマンドを収集する．コマンドから, 不正なサイトで攻撃者がダウンロードさせてくるソフトウェアのデータを集めるプログラムを構築し, 不正なソフトウェアを解析するものを作る.

研究計画として,

1. Dshield を運用できる環境を構築をする.
2. コマンドを収集するために、Dshield のプログラム内で、攻撃者からのコマンドに対してどのような動作をしているかを確認する.
3. 実際に Dshield を運用してみる.
4. 取集したコマンドの内容について調べる.
5. コマンドからファイル又は,URL などを取集するプログラムを作成する.
6. ファイルがどのようなものなのか調べる.

という手順で進めていき, 攻撃ファイルがどの様なものなのか把握し, どのような対策が有効的なのか等の警告を発することで, セキュリティの向上に貢献していきたい.

## 3　今まで行ってきたこと

### 3.1　Dhield の運用できる環境の構築

Raspberry Pi に Dshield をインストールし, パスワードや接続する無線 LAN の設定を行なった．設定の更新には, 少しの時間が掛かっった. 又,RassberryPi の設定からインターフェースの SSH を有効にする事で, SSH を通って外部 PC から接続を可能にした. 研究室内のネットワークからの接続は攻撃と見さないように設定した.

### 3.2　Dshield が行う攻撃者のログイン試行への対処方法

Dshield は研究室で以前から運用されていたが id やパスワードの収集を目的として使われていた. 本研究

では、コマンドを収集したいので, Dshield のプログラム内容からコマンドを収集できているのか, 又出来る様に設定していきたい. 調査の結果, Dshield はコマンドを取集していることが分かった. 収集したコマンドは,/srv/cowrie/var/log/cowrie の場所に保存されていることが分かった. 又,

### 3.3 収集したコマンド内容と攻撃者の意図

## 4 今後やる事

## 参考文献