

卒業論文 2018 年度 (平成 30 年)

低対話型 Honeypot のコマンド拡張による
高対話型 Honeypot への近似

慶應義塾大学 総合政策学部
菅藤 佑太

低対話型 Honeypot のコマンド拡張による
高対話型 Honeypot への近似

PC の普及や IoT デバイスのシステム高度化により、高度な処理系を組むことが可能になった。これによりデバイス上に Linux 系などの OS が搭載された機器が広く人々に使われるようになった。また、Linux 系 OS にリモートログインする手法として SSH がある。これを用いて不正に侵入する攻撃が行われている。侵入された際に侵入者がどのような挙動をしているのかを知る手段として、Honeypot がある。Honeypot は SSH で侵入しやすいような環境を作ることで、侵入者にログイン試行に成功したと検知させ、その際に実行したコマンドのログを収集するものである。また現在では Shell の挙動をエミュレートした Honeypot が広く使用されており、この Honeypot は実行できるコマンドが少ない実装になっている。そのため Honeypot への侵入者に侵入先が Honeypot であると検知されてしまう。そこで事前実験では Honeypot のコマンドを拡張し、拡張をしていない Honeypot とコマンドの拡張をした Honeypot で侵入ログを収集した。収集したログを確率的な算出方法を使用することで比較した結果、より多くの侵入者のコマンド実行ログのパターンを取得できることを示した。本研究ではコマンドを拡張した Honeypot の侵入ログがどれほど実際の OS に不正な SSH の侵入をされた際の侵入ログの近似を試みた。評価として、拡張をしていない Honeypot とコマンドの拡張をした Honeypot と、さらに実際の OS を使用した Honeypot で侵入ログを収集し、比較を行なった。この 3 つの侵入ログを自然言語処理の意味解析を用い、コマンドの一つ一つの意味をベクトル表現することで、拡張した Honeypot で収集した侵入ログが、拡張をしていない Honeypot で収集した侵入ログよりも、実際の OS を使用した Honeypot で侵入ログに意味的に近くなることが明らかとなった。

キーワード:

1. SSH, 2. Honeypot, 3. 機械学習, 4. 自然言語処理

慶應義塾大学 総合政策学部
菅藤 佑太

Approximation of high-interaction honeypots
by Command Extension of low-interaction honeypot

By the spread of PCs and the system advancement of the IoT device, I was able to make high processing system. The apparatus that the OS's such as the Linux system were equipped with on a device came to be in this way used for people widely. In addition, technique to perform a remote login for the Linux system OS includes SSH. An attack to invade using this illegally is carried out. A window includes Honeypot what kind of ways an intruder behaves when it was invaded. Honeypot lets an intruder detect it when I succeeded in a login trial by making the environment where it is easy to invade in SSH and collects the log of the command that I carried out on this occasion. In addition, Honeypot which emulated behavior of Shell is used widely now, and there are few commands that this Honeypot can carry out; is implemented. Therefore it is detected by an intruder to Honeypot when invasion is Honeypot. Therefore I expanded the command of Honeypot by the prior experiment and collected invasion log in Honeypot and Honeypot which I expanded of the command which were not expanded. As a result of having compared the log that I collected by using a probabilistic calculation method, I showed that I could acquire a pattern of the command practice log of more intruders. Invasion log of Honeypot which expanded the command tried an approximation of the invasion log when it was invaded of unjust SSH for the real OS in this study how long. I collected invasion log more in Honeypot using the real OS and compared it with Honeypot and expanded Honeypot of the command which were not expanded as an evaluation. I used semantic analysis of the natural language processing in the invasion log of these three, and a semantically thing nearby became clear in invasion log than the invasion log that I collected in Honeypot which the invasion log that I collected in Honeypot which I expanded because a vector expressed a meaning of none of nothing of the command did not expand in Honeypot using the real OS.

Keywords :

1. SSH, 2. Honeypot, 3. Machine Learning, 4. Natural Language Processing

Keio University, Faculty of Policy Management Studies
Yuta Sugafuji

目 次

图 目 次

表 目 次

第1章 序論

本章では本研究の背景，課題及び手法を提示し，本研究の概要を示す．

1.1 本研究の背景

1.1.1 通信機器の普及

PCの普及やIoTデバイスのシステム高度化により，高度な処理系を組むことが可能になった．これによりデバイス上にLinux系などのOSが搭載された機器が広く人々に使われるようになった．また，Linux系OSにリモートログインする手法としてSSHがある．これを用いて不正に侵入する攻撃が行われている．

1.1.2 honeypot

侵入された際に侵入者がどのような挙動をしているのかを知る手段として，Honeypotがある．これは実際のOSを用いたり，Shellの擬似的な挙動をアプリケーション上で実現し，敢えてSSHで侵入しやすいような環境を作ることで，侵入者にログイン試行に成功したと検知させ，その際に実行したコマンドのログを収集する．

1.2 本研究の問題と仮説

SSHのHoneypotは大きく二種類に分けることができ，一つは低対話型Honeypot，もう一つは高対話型Honeypotである．低対話型Honeypotは実際のShellの挙動をエミュレートしたアプリケーションである．

高対話型Honeypotは実際の機器を設置し，その中に侵入させログを収集する．その設置時には他のホストに攻撃できないようにネットワークの設定や，rootの権限が取られないようにuser権限の設定を適切に行う．高対話型Honeypotは低対話型Honeypotと比較すると，Honeypotへの侵入者が実行できるコマンドが多く，挙動も本物のOSと差異が極めて少なく，侵入先がHoneypotであると極めて検知しきれにくい．そのため，高精度な攻撃ログを取得することができる．しかし，Honeypotとして適切な設定を行なったOSが，設置後に発見された新たなOSの脆弱性を突かれることで，踏み台にされ他のホストに攻撃をしたりウイルスに犯されてしまうなどの危険を孕んでいる．そのため，設置コストが高く普及率も非常に低い．？

一方で低対話型 Honeypot はアプリケーションであるため、root 権限を取られるような危険が極めて少なく、アプリケーション内での脆弱性に限った問題しか存在しない。そのため設置コストが低く、比較的誰でも安全に設置できるため、普及率が高い。しかし、あくまでエミュレーションを行なったアプリケーションであるため、実際の Shell とは異なる挙動や、Honeypot に特有な挙動をすることがある。そのため、設置した Honeypot に侵入した悪意のあるユーザーに侵入先が Honeypot であると検知されてしまう可能性がある。本研究では低対話型 Honeypot に着目する。低対話型で実際の攻撃ログに近いログを収集するには、先述の Honeypot であることの検知を回避する必要がある。そこで本研究では、低対話型に実装されているコマンドの出力を、実際の Shell に近似することで検知を回避できるのではないかと考えた。

1.3 提案手法の実装

先述の Honeypot であることの検知を回避するために、本研究では低対話型 Honeypot を実際の Shell の挙動に近似するために、2 つの実験を行なった。一つは実際の Shell に実装されているが低対話型 Honeypot に実装されていないコマンドの実装した。もう一つは低対話型 Honeypot に特有の異常な挙動を修正を行った。

1.4 予備実験

本研究の予備実験として、SSH の低対話型 Honeypot に実装されていないコマンドで、悪意のある侵入者が使うコマンドを実装することで拡張を行なった低対話型 Honeypot と、素の低対話型 Honeypot でそれぞれ収集したコマンドログの比較を行なった。追加実装を施した SSH の低対話型 Honeypot の方がコマンドパターンとして多く収集できることを示した。

1.5 本研究の評価

提案手法の実装で拡張した低対話型 Honeypot と、素の Honeypot と、高対話型 Honeypot を設置し、それぞれ侵入者が実行したコマンドのログを収集し、比較を行った。収集したコマンドのログはコマンド 1 つ 1 つごとに自然言語処理の手法を用いて意味解析をし、コマンドの意味をベクトル空間上に表現した。本研究では、高対話型のログに近似することで、高度なログが収集できていると考えた。そこで、拡張した低対話型 Honeypot の侵入ログが素の Honeypot と比較して、高対話型 Honeypot の侵入ログにどれほど次元空間上で近似したのかを評価した。

1.5.1 予備実験

本研究の予備実験として、SSH の低対話型 Honeypot に実装されていないコマンドで、悪意のある侵入者が使うコマンドを実装することで拡張を行なった低対話型 Honeypot と、素の低対話型 Honeypot でそれぞれ収集したコマンドログの比較を行なった。追加実装を施した SSH の低対話型 Honeypot の方がコマンドパターンとして多く収集できることを示した。

1.6 本論文の構成

本論文における以降の構成は次の通りである。

2 章では、本研究の要素技術となる Shell と Honeypot と自然言語処理について整理する。?? 章では、本研究における問題の定義と、解決するための要件、仮説について説明する。?? 章では、本提案手法について解説する。?? 章では、本研究の事前実験や Honeypot の拡張についての実装方法や実装例について述べる。?? 章では、求められた課題に対する評価を行い、考察する。?? 章では、関連研究を紹介し、本研究との比較を行う。?? 章では、本研究のまとめと今後の課題、展望についてまとめる。

第2章 本研究の要素技術

本章では、本研究の要素技術となる Shell と Honeypot と時系列データの扱いについて各々整理する。

2.1 Honeypot

使われているデバイスへの不正な SSH によって侵入された際、実際に攻撃が行えない環境へとフォワードし、その中で攻撃を試行させ、侵入者のログを収集する手段として Honeypot がある。SSH の Honeypot は低対話型 Honeypot と高対話型 Honeypot の大きく二種類に分けることができる。

2.1.1 低対話型 Honeypot

SSH の低対話型 Honeypot は実際の Shell の挙動をエミュレートしたアプリケーションである。実際の Shell の挙動をエミュレートしただけのアプリケーションなので、脆弱性がアプリケーション内に限られる。そのため、root 権限を侵入者に許してしまい、踏み台にされてしまうなどの危険が極めて少ない。しかし、エミュレーションには限界があるため、コマンドやその挙動について、実際の Shell とは異なる挙動をすることがある。そのため、侵入者に侵入先が Honeypot であると検知されてしまう。検知されることで、攻撃者は実際の攻撃を行わず、本来取れるはずの攻撃ログが収集できない可能性を含んでいる。そのため、収集ログの精度に問題がある。

2.1.1.1 Kippo

Kippo は、悪意のある SSH のログイン試行者や侵入者の挙動やログを記録するために使用される Python で実装された SSH の低対話型 Honeypot である。Kippo は前身の Kojoney に大きく影響を受けている。ネットワークは Twisted というフレームワークで組まれている。Kippo のプロジェクトは低対話型 Honeypot として 2009 年に登場し、Raspberry Piなどを筆頭としたシングルボードコンピュータの普及と相まって広く設置された。Kippo の機能の特徴としては収集したコマンドログを時系列データとして保存されており、"playlog" という Kippo 内にあるプログラムを実行することで、過去のコマンドログを実際にタイピングしてるかのように出力できる。また、侵入者によってダウン

ロードされたファイルも実行ができないように保存できる。Kippo は後述の Cowrie の後継実装である。Kippo は IoT デバイスの高度化広く設置された SSH の低対話型 Honeypot のうちのひとつであったが、実装されているコマンドも 17 と少なく、また Kippo 特有の異常な挙動が存在するなど多くの問題があった。

2.1.1.2 Cowrie

Cowrie は Python で実装された SSH の低対話型 Honeypot であり、実装は Kippo のコマンドの拡張や、攻撃者がリダイレクトでマルウェアを送り込む手法をとって送り込んだマルウェアを収集可能にしたりするなど、様々な機能を拡張したものである。Kippo 特有の異常な挙動を改善しており、実装コマンド数は 38 と Kippo より少し多くなっているものの、Cowrie 特有の異常な挙動もまだまだ多い。

2.1.2 高対話型 Honeypot

2.1.2.1 Honeynet Project

2.1.3 SSH の Honeypot の比較

以上をまとめた SSH の低対話型 Honeypot と SSH の高対話型 Honeypot の比較を行った表を図 2.1 に示す。

	設置コスト (リスク)	Honeypotであることの 検知されにくさ
低対話型Honeypot	設置コストが低い	検知されやすい
高対話型Honeypot	設置コストが高い	検知されにくい

図 2.1: SSH の低対話型 Honeypot と SSH の高対話型 Honeypot の比較

2.2 Shell

Shell は OS のユーザーのためにインタフェースで、カーネルのサービスへのアクセスを提供するソフトウェアである。本研究での”Shell”はコマンドラインシェルのことを指す。

2.2.1 Secure Shell

Secure Shell（セキュアシェル、SSH）は、暗号や認証の技術を利用して、安全にリモートコンピュータと通信するためのプロトコルである。パスワードなどの認証部分を含むすべてのネットワーク上の通信が暗号化される。¹SSHにおける問題としては、通信する上での認証方法には鍵認証を推奨されているが、デフォルトではパスワード認証になっている。パスワード認証のままだとパスワードの総当たり攻撃を受けたり、パスワードが標準のままの設定であることで不正なログイン試行によって侵入を許してしまう。

2.2.2 BusyBox

BusyBox は標準 UNIX コマンドで重要な多数のプログラムを単一のバイナリファイルに含むプログラムである。BusyBox に含まれる、多数の標準 UNIX コマンドで必要とするプログラムの実行ファイルは、Linux という OS を BusyBox だけでディストリビューションできるよう、”Linux 上で最小の実行ファイル”として設計されている。一般にインストールされる実行ファイルは一部だけを実装できるように選択することができる。一般的には BusyBox のコマンドは 200 以上も用意されている。¹ BusyBox をインストールして実際に各コマンドを実行するためには、BusyBox 内にある各コマンドにアクセス可能のように path を通すだけで良い。

2.3 自然言語処理

人間が日常的に使っている自然言語をコンピュータに処理させる一連の技術である。本研究において、自然言語処理は意味解析のために使用した。意味解析には様々な手法があり、現在では大きくシソーラス解析とベクトル空間分析がある。

2.3.1 シソーラス解析

シソーラスとは単語を意味レベルで分解し、抽象度の高いものから低いものへと遡っていくことができ、それを体系づけた類語辞書のことである。シソーラスには様々な言語において有名な辞書が存在する。有名なシソーラスとしては Princeton University の WordNet がある。²

¹今回使用した BusyBox に含まれるコマンドの数は 219

2.3.1.1 Wordnet

WordNet は英単語が synset と呼ばれる同義語のグループに分類され、簡単な定義や、他の同義語のグループとの関係が記述されているデータベースである。WordNet のデータベースは約 11 万 5000 の synset に分類された約 15 万語を収録し、全体で 20 万 3000 の単語と意味の組み合わせがある。

2.3.2 ベクトル空間解析

単語の意味を表現するため、単語の文章での出現回数や、その単語の周辺の単語をマトリクス上に表現することで、その単語を数学的に解釈できるようにしている。

2.3.2.1 ベクトル空間モデル

ベクトル空間モデルとは文章を多次元空間上にベクトルとして表現し、それぞれのベクトルの比較を行うことで類似度を算出するためのモデルである。文章の類似度が高いほどベクトルの方向が近いということなので、比較した文章のベクトルのなす角が小さければ文章の類似度が高いということになる。

m 個の単語が使用されている文章 d における各単語の重要度を $w_{d1}, w_{d2}, w_{d3}, \dots, w_{dm}$ とすると、文章 d のベクトルは以下のように表される。

$$\vec{d} = (w_{d1}, w_{d2}, w_{d3}, \dots, w_{dm})$$

また、同様にして n 個の単語が使用されている文章 e をベクトル表現すると、

$$\vec{e} = (w_{e1}, w_{e2}, w_{e3}, \dots, w_{en})$$

と表すことができる。したがって、 \vec{d} と \vec{e} のなす角 θ における $\cos \theta$ は以下のように表される。

$$\cos \theta = \frac{\vec{d} \cdot \vec{e}}{|\vec{d}| |\vec{e}|}$$

ベクトル化した時の単語の重要度は TF-IDF のアルゴリズム (※ 2.3.2.1.1) を用いて算出した重みを用いることで、これを表すことができる。上記の例であれば、文章 d における単語の重要度が $tf(t_1, d) \cdot idf(t_1), tf(t_2, d) \cdot idf(t_2), tf(t_3, d) \cdot idf(t_3), \dots, tf(t_m, d) \cdot idf(t_m)$ であるので、文章 d のベクトルは以下のように表される。

$$\vec{d} = (tf(t_1, d) \cdot idf(t_1), tf(t_2, d) \cdot idf(t_2), tf(t_3, d) \cdot idf(t_3), \dots, tf(t_m, d) \cdot idf(t_m))$$

また、同様にして文章 e もベクトル表現すると、

$$\vec{d} = (tf(t_1, e) \cdot idf(t_1), tf(t_2, e) \cdot idf(t_2), tf(t_3, e) \cdot idf(t_3), \dots, tf(t_n, e) \cdot idf(t_n))$$

と表すことができ、これを $\cos \theta = \frac{\vec{d} \cdot \vec{e}}{|\vec{d}| |\vec{e}|}$ に代入すると ($\ast m \leq n$),

$$\begin{aligned} \cos \theta &= \frac{\vec{d} \cdot \vec{e}}{|\vec{d}| |\vec{e}|} \\ &= \frac{((tf(t_1, d) \cdot idf(t_1))(tf(t_1, e) \cdot idf(t_1)) + (tf(t_1, d) \cdot idf(t_2))(tf(t_2, e) \cdot idf(t_2)) + \dots \\ &\quad + (tf(t_m, d) \cdot idf(t_m))(tf(t_m, e) \cdot idf(t_m))) \cdot 1}{\sqrt{(tf(t_1, d) \cdot idf(t_1))^2 + (tf(t_2, d) \cdot idf(t_2))^2 + \dots + (tf(t_m, d) \cdot idf(t_m))^2} \cdot \sqrt{(tf(t_1, e) \cdot idf(t_1))^2 + (tf(t_2, e) \cdot idf(t_2))^2 + \dots + (tf(t_n, e) \cdot idf(t_n))^2}} \\ &= \frac{\sum_{i=1}^m ((tf(t_i, d) \cdot idf(t_i))(tf(t_i, e) \cdot idf(t_i)))}{\sum_{i=1}^m \sqrt{(tf(t_i, d) \cdot idf(t_i))^2} \sum_{i=1}^n \sqrt{(tf(t_i, e) \cdot idf(t_i))^2}} \end{aligned}$$

と表すことができる。これがベクトル空間で TF-IDF で抽出した単語の重み付けを行い、二つの文章の類似度を算出するモデルである。

2.3.2.1.1 TF-IDF

TF とは Term Frequency のことで、文章内での単語の出現頻度を表す。数式では以下のように表される。

$$tf(t, d) = \frac{n_{t, d}}{\sum_{s \ni d} n_{s, d}}$$

$tf(t, d)$ は TF の値で、文章 d 内に含まれる単語 t の出現頻度を表す。

$n_{t, d}$ は文章 d における単語 t の出現回数を表す。

$\sum_{s \ni d} n_{s, d}$ は文章 d における全ての単語の出現回数を表す。

以上を踏まえ TF の値とは、

$$\text{文章 } d \text{ 内に含まれる単語 } t \text{ の出現頻度} = \frac{\text{文章 } d \text{ における単語 } t \text{ の出現回数}}{\text{文章 } d \text{ における全ての単語の出現回数}}$$

を数式で表したものである。

IDF とは Inverse Document Frequency のことで、ある単語が様々な文章においてどれほど使われているのかを表す。数式では以下のように表される。

$$idf(t) = \log \frac{N}{df(t)} + 1$$

$idf(t)$ は IDF の値で、単語 t が全文章数 N でどれほど使われているのかを表す。
 N は全文章数を表す。
 $df(t)$ は単語 t が出現する文章の数を表す。
 以上を踏まえ IDF の値とは、

$$\text{単語 } t \text{ が全文章数 } N \text{ でどれほど使われているのか} = \frac{\text{全文章数}}{\text{単語 } t \text{ が出現する文章の数} + 1}$$

を数式で表したものである。
 このような TF の値と IDF の値を重みとすることで、文章を特徴付ける単語の抽出をするものが TF-IDF である。上記の TF と IDF の値より、if-idf の値は

$$ifidf(t, d) = tf(t, d) \cdot idf(t)$$

から算出することができる。

2.3.2.2 word2vec

word2vec は 2 層からなるニューラルネットワークである。word2vec には 2 つのアーキテクチャがあり、一つは *ContinuousSkip-gramModel*、もう一つは *ContinuousBag-of-WordsModel* である。*ContinuousSkip-gramModel* は入力に文章中の任意の単語を用意し、出力に文章においてその任意の単語の前後の周辺語を用意し、ニューラルネットワークに読み込ませることで第一層から第二層への重みを獲得することが目的である。*ContinuousBag-of-WordsModel* では逆に出力に文章中の任意の単語を用意し、入力に文章においてその任意の単語の前後の周辺語を用意し、同様にしてニューラルネットワークに読み込ませることで第一層から第二層への重みを獲得することが目的である。本研究ではより精度の高い *ContinuousSkip-gramModel*（以降、*Skip-gramModel* と呼ぶ。）を使用した。？

2.3.2.3 Continuous Skip-gram Model

Skip-gramModel は先述の通り、与えられた単語に対してその周辺語を予測するためのモデルのことである。このモデルは 2 層からなるニューラルネットで、入力には One-hot ベクトルを用いる。One-hot ベクトルとは $(0, 0, 0, \dots, 1, \dots, 0)$ のように、単語のインデックスから抽出する単語だけを 1 と表記することで表現するベクトルのことである。入力層から隠れ層への重みは $V \times N$ のマトリクス W で表され、 W の各列は単語ベクトルとなっている。隠れ層から出力層への重みはマトリクス W を転置した $N \times V$ のマトリ

クス W' となっている。

このようなモデルを条件付き確率で表現すると、

$$p(w_O|w_I) = \frac{\exp(v'_{W_V}^T \cdot v_{w_I})}{\sum_{w_v \in V} \exp(v'_{W_V}^T \cdot v_{w_I})}$$

と表せる。この w_I は入力する単語、 w_O は w_I の周辺語を表す。 v_{w_I} や $v'_{W_V}^T$ は単語を表すベクトルであり、 v は入力ベクトルで v' は出力ベクトルである。コンテキストサイズとは先述したように、入力単語の周辺語をどこまでとするかのサイズのことである。 $p(w_O|w_I)$ はコンテキストサイズを考慮していない確率であるが、このコンテキストサイズを考慮して先述したモデルの同時確率 $p(w_{O,1}, w_{O,2}, w_{O,3}, \dots, w_{O,C}|w_I)$ は、

$$p(w_{O,1}, w_{O,2}, w_{O,3}, \dots, w_{O,C}|w_I) = \prod_{c=1}^C \frac{\exp(v'_{W_V}^T \cdot v_{w_I})}{\sum_{w_v \in V} \exp(v'_{W_V}^T \cdot v_{w_I})}$$

と表される。

この $p(w_{O,1}, w_{O,2}, w_{O,3}, \dots, w_{O,C}|w_I)$ という確率を表す関数 $\prod_{c=1}^C \frac{\exp(v'_{W_V}^T \cdot v_{w_I})}{\sum_{w_v \in V} \exp(v'_{W_V}^T \cdot v_{w_I})}$ を最大にするベクトル v を求めることで、周辺語が適切に出力されるものとなる。

このモデルを用いてニューラルネットを構築する。先述の通り、入力層 x は One-hot ベクトルを用いる。One-hot ベクトルとは $(0, 0, 0, \dots, 1, \dots, 0)$ のように、単語のインデックスから抽出する単語だけを 1 と表記することで表現するベクトルのことである。

隠れ層 h は、入力層から隠れ層への重み W を入力データ x にかけたものである。したがって隠れ層 h は

$$h = Wx$$

と表すことができる。また、任意の入力 $w_I (= x_i)$ は重み W が掛けられるが、入力が One-hot ベクトルなので、 w_I に対応する単語ベクトルがそのまま出力されることになる。したがって、隠れ層は

$$h = Wx_{w_I} = v_{w_I}$$

と表すことができる。

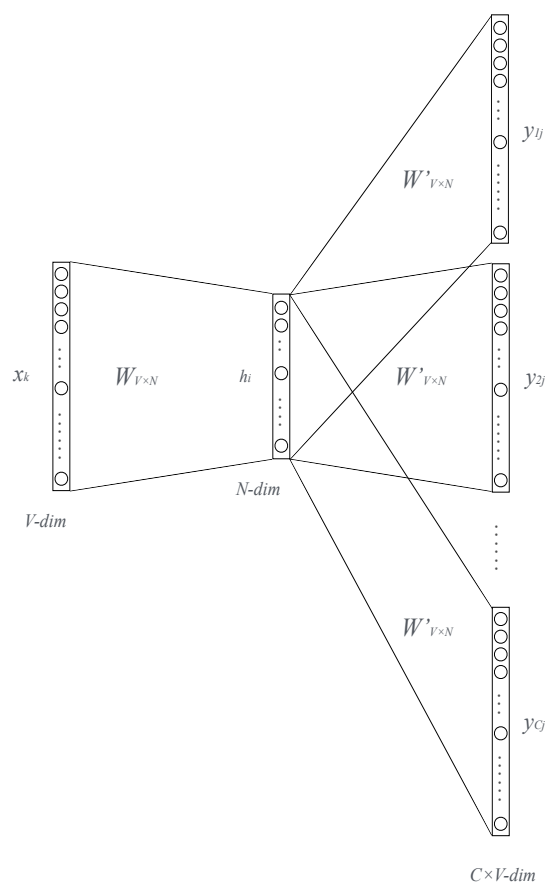
出力層 u_c は、隠れ層 h に隠れ層から出力層への重み W' が掛けられたものであるので、

$$u_c = W'h = W'v_{w_I}$$

と表すことができる。また、出力層はコンテキストサイズに応じて出力のユニット数 c が変動する。したがって、任意のユニット C における最終的な出力 $y_{c,i}$ は softmax 関数を掛けて、

$$\begin{aligned} y_{c,i} &= \frac{\exp(u_{c,i})}{\sum_{v=1}^V \exp(u_{c,v})} \\ &= \frac{\exp(v'_i \cdot v_{w_I})}{\sum_{v=1}^V \exp(v'_v \cdot v_{w_I})} \\ &= p(w_i|w_I) \end{aligned}$$

となる．以上をまとめるとニューラルネットは以下の図のようになる．



第3章 本研究における問題定義と仮説

本章では，1章で述べた背景より，本章では，現状の Honeypot の問題点を整理し，この問題をどのように解決すれば良いのかを定義する．

3.1 本研究における問題定義

現状の Honeypot の問題点を列挙し，整理する．

3.1.1 SSH Honeypot の現状の問題

Honeypot には運用する上で大きな問題が2つある．一つは設置した Honeypot に侵入した悪意のある侵入者が侵入先を Honeypot であると検知してしまう問題である．もう一つは Honeypot に侵入を許した侵入者に Honeypot を設置した機器から他のホストに攻撃を仕掛けられてしまう，所謂踏み台攻撃の踏み台にされる問題である．

以下の図 3.1 は，悪意のある侵入者が不正に機器に侵入してから踏み台にして他の機器に攻撃を仕掛けるまでの一般的なフローである．問題として，2 番目のフローの悪意のある侵入者が侵入した先が Honeypot であると検知してしまうことが考えられる．高対話型 Honeypot で使用した OS 自体の新たな脆弱性を突かれることに限った状況で，3 番目のフローの Honeypot への侵入者に Honeypot を設置した機器から攻撃が仕掛けられてしまう危険があることが問題として挙げられる．

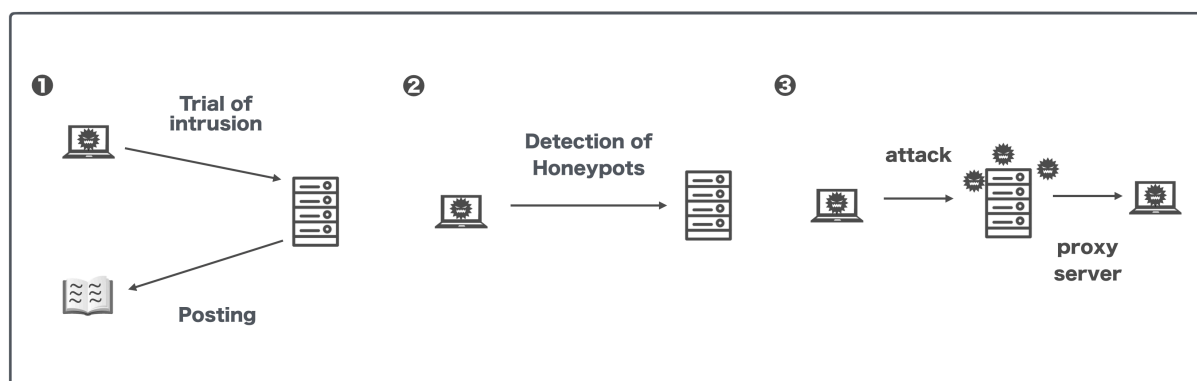


図 3.1: 不正な SSH 侵入者の想定行動フロー

本研究ではこの中でも、2 番目のフローの SSH の低対話型 Honeypot が設置した Honeypot に悪意のある侵入者が侵入先を Honeypot であると検知してしまう問題に着目した。

3.1.1.1 SSH の低対話型 Honeypot における問題

SSH の低対話型 Honeypot は実際の Shell の挙動をエミュレートしたものであるのでコマンドやその挙動についての機能が限定されており、実際の Shell の機能として不足がある。また SSH の低対話型 Honeypot 特有の以上な挙動も存在する。さらに、SSH で Honeypot にセッションを確立する際に、そのレイテンシを計測し、そのレイテンシが Honeypot の場合に通常とは明らかに異なることにより、Honeypot であると検知されてしまう問題がある。また、Honeypot の username が "Richard" がデフォルトのため、username から Honeypot であることを検知されてしまう問題もある。これらの検知手法を用いて、侵入者に侵入先が Honeypot であると検知され、本来取れるはずの攻撃ログが収集できない問題がある。

3.1.1.1.1 SSH でのセッション確立におけるレイテンシの問題

3.1.1.1.2 Honeypot の Username の問題

3.1.1.1.3 Honeypot のコマンドの実装の問題

SSH の低対話型 Honeypot は実際の Shell の挙動をエミュレートしたものであるのでコマンドやその挙動についての機能が限定されており、実際の Shell の機能として不足がある。2.2.2 で述べたように、"Linux 上で最小の実行ファイル" となるよう設計されている BusyBox に含まれるコマンドの数が 200 以上あるのに対し、現状で広く使われている SSH の低対話型 Honeypot である Cowrie に実装されているコマンドは 2.1.1.2 でも述べた通り、38 しか存在しない。また、SSH の低対話型 Honeypot 特有の挙動が存在し、以下にその 1 例であるプログラム 3.1 とプログラム 3.2 を示す。

プログラム 3.1: 正しい Shell の挙動

```
1 nadechin@cpu:~$ echo -n test
2 testnadechin@cpu:~$
```

プログラム 3.2: Kippo 特有の異常な挙動の例

```
1 s15445ys@s15445ys-neco:~$ echo -n hello
2 -n hello
3 s15445ys@s15445ys-neco:~$
```

プログラム 3.1 が通常の挙動でプログラム 3.2 が SSH の低対話型 Honeypot の挙動である。echo コマンドの -n オプションは改行出力末尾にしないようにするものである。しかし、実際の Shell の出力は改行がされない一方、Honeypot の挙動ではオプション部分も出力されてしまい、末尾も改行されてしまう。これは SSH の低対話型 Honeypot 特有の

挙動であるため、この挙動を観測することによって侵入者に侵入先が Honeypot であると検知されてしまう可能性がある。

3.1.2 本研究の問題

??で列挙した SSH の低対話型 Honeypot の問題の中で、実際の Shell に実装されているコマンドの不足がある。また SSH の低対話型 Honeypot に特有の異常な挙動も存在するため、設置した Honeypot が悪意のある侵入者に侵入先を Honeypot であると検知されてしまい、実際の OS に悪意のある侵入者が侵入した時の侵入ログとの違いが大きく出てしまう問題に着目した。

3.2 問題解決のための要点

??で着目した問題を解決するためには、以下 2 つの手法を取る必要がある。

コマンドの追加実装: 実際の Shell に実装されているコマンドで、SSH の低対話型 Honeypot に実装されていないコマンドを実装する

既実装コマンドの修正: SSH の低対話型 Honeypot に特有の異常な挙動をする既実装コマンドを修正する

3.3 仮説

??と ??で示す問題解決のための要点を踏まえると、SSH の低対話型 Honeypot に侵入した悪意のある侵入者に侵入先を Honeypot であると検知させず、SSH の低対話型 Honeypot に悪意のある侵入者が侵入した時の侵入ログを、実際の OS に悪意のある侵入者が侵入した時の侵入ログに近似できるのでないかと考えた。

3.3.1 コマンドの追加実装

実際の Shell に実装されているコマンドで、SSH の低対話型 Honeypot に実装されていないコマンドを実装することで、Honeypot への侵入者が実行できるコマンドの少なさによる、Honeypot であることの検知を回避することができる。

3.3.2 既実装コマンドの修正

SSH の低対話型 Honeypot に特有の異常な挙動をする既実装コマンドを修正することで、Honeypot について認知している侵入者が、侵入先を Honeypot であると検知することを回避することができる。

第4章 本研究の手法

本章では， ??節で述べた仮説を検証するために， 本研究の手法について概説する．

4.1 問題解決の為のアプローチ

??で述べた問題解決のための2つの要件を満たすために， 本研究では低対話型 Honeypot に実装されていないコマンドを実装し， さらに低対話型 Honeypot の既実装コマンドで， 低対話型 Honeypot に特有の異常な挙動をするコマンドの修正を行う．

第5章 実装

本章では， ??節で述べた手法を用いて純正の Honeypot にどのようなコマンドを実装し， Honeypot 特有の異常な挙動を修正したのかを説明する．

5.1 実装環境

TBD

5.1.1 純正の Honeypot で未実装のコマンドの実装

本研究において純正の Honeypot は Cowrie?を使用し，実際の Shell には実装されているが，純正の Honeypot で未実装のコマンドについては BusyBox?に含まれるコマンドの実装を行なった．2.1.1.2 や 2.2.2 で紹介した通り，BusyBox に含まれるコマンドの種類が 219 ある中で，Cowrie の実装コマンド数は 38 しか存在しない．この差分を Python で実装する．

また実装したコマンド一覧を表 hoge に示す．(付録にて例で紹介できなかったコマンドを掲載する)

第6章 評価と考察

本章では，予備実験と??章で実装した本研究での提案手法の評価とその考察を述べる．

6.1 予備実験

SSH の低対話型 Honeypot である Cowrie はコマンドの実装数が少なく，Cowrie 特有の異常な挙動が多い．そのため，侵入者に Honeypot であると検知されることで，本来実際の OS への攻撃であれば取れるはずであった侵入ログが取れない問題がある．また，収集ログを分析する際に，これまで用いられてきた”危険なコマンド”としてインデックスを作り，それらを危険なコマンドとしてパターンマッチングする手法では，今後出現してくる様々なコマンドパターンなどに対応できない．

予備実験では，Cowrie はコマンドの実装数が少なく，Cowrie 特有の異常な挙動が多いため，コマンドの追加実装を行い，Cowrie 特有の異常な挙動を修正した．実装を施していない純正の Cowrie と Cowrie に BusyBox に含まれるコマンドを実装した修正済みの Cowrie の両方でコマンドログの収集を行い，比較することで，収集ログのパターンの変化を観測できるのではないかと考えた．評価として収集した二つのログを Skip-gram モデルを用いてスコアリングし，どちらがより多くのコマンドログのパターンを収集できているのかを検証した．

その結果，より多くのコマンドパターンを取れたのが Cowrie に BusyBox に含まれるコマンドを実装した修正済みの Cowrie であるということが明らかとなった．

6.1.1 予備実験の手法

実装を施していない純正の Cowrie に対して，これには実装されていないが Shell には実装されているコマンドを実装したものを設置し，ログを収集した．

6.1.2 侵入ログの収集環境

6.1.3 実装

純正の Cowrie に BusyBox に含まれるコマンドを実装し，また Honeypot 特有の異常な挙動を修正した．ここでの実装を紹介する．

6.1.4 評価

実装を施していない純正の Cowrie と Cowrie に BusyBox に含まれるコマンドを実装した修正済みの Cowrie の両方で侵入ログの収集を行い，Word2vec の Skip-Gram Model により次のコマンドの予測，スコアリングを行い比較を行うことで，差異を評価した．スコアリングでは，あるコマンドが実行された時に次のコマンドの出やすさを予測したため，次に実行されるコマンドがスコアとして高い数値を出せばそのコマンドパターンがパターンとして存在しやすいものであることを示す．予備実験の評価に関しては第 7 章の評価で一部説明している．本研究の評価と評価手法の違いは，モデル化を純正の Honeypot に BusyBox に含まれるコマンドを実装したものしか行っていないため，実際の OS に近いログが取れたことが証明できておらず，比較する対象が少なかった．

6.1.5 結果

SSH の低対話型 Honeypot の稼働期間は 12/10 から 2/1(54 日間) で，収集できたものとしてコネクション数，パターン数，コマンド数を以下の図 6.1 に記す．

	純正のHoneypot	修正済みのHoneypot
コネクション数	19829	27914
パターン数	53	91
コマンド数	470	841

図 6.1: 収集した SSH の低対話型 Honeypot のデータ

また，モデル化を行い純正の Cowrie と Cowrie に BusyBox に含まれるコマンドを実装した修正済みの Cowrie のスコアリングを行なった結果を以下の図 6.2 に記す．横軸はコマンド拡張を行なった Honeypot か素の Honeypot であるかを示している．縦軸は予備実験の評価手法によって算出されたコマンドの表れやすさを数値化したものであり，数値が高くなればのコマンドパターンがパターンとして存在しやすいものであることを示して

いる。予備実験ではコマンドの拡張実装をしたものの方がコマンドパターンとして存在しにくいものを観測できたという結果になった。

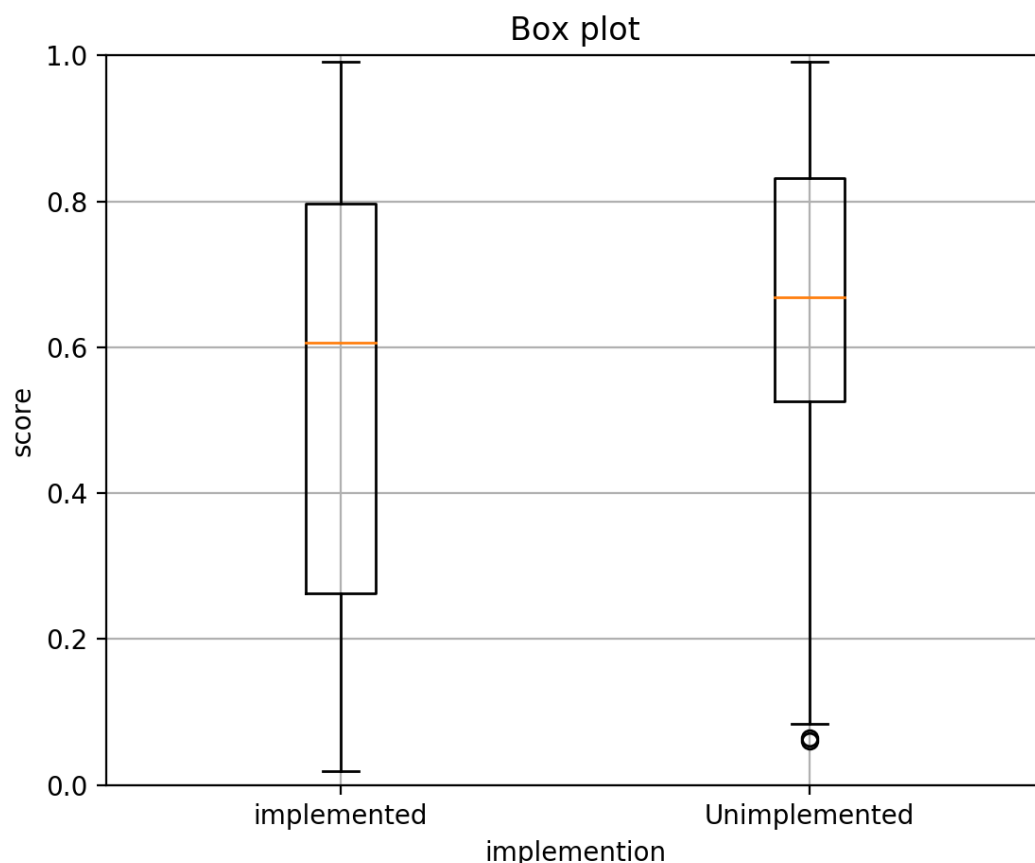


図 6.2: 純正の Cowrie と修正済みの Cowrie のスコアリングによる比較

本研究の予備実験では、Cowrie に実装されていないコマンドで悪意のある侵入者が使うようなコマンドを実装し、何の追加実装も施していない Cowrie で取れた侵入者の実行コマンドログと、追加実装を施した Cowrie の侵入者の実行コマンドログを比較することで、追加実装を施した SSH の Cowrie の方がコマンドパターンとして多く収集できることを示した。

6.2 評価手法

本研究の仮説の検証手法としての評価として、??節で述べた要件に対して評価を行う。予備実験では、素の低対話型 Honeypot よりも、コマンドを拡張した Honeypot の方がコマンドパターンが多く収集できることを示した。本研究では拡張した Honeypot で収集したコマンドログが、どれほど高対話型 Honeypot で収集したコマンドログに近似したのかを評価した。

本研究では、以下の三種類の Honeypot を設置する。

1. 広く利用されている SSH の低対話型 Honeypot
2. 実際の Shell には実装されているが、1. の Honeypot で未実装のコマンドを実装した Honeypot
3. 広く利用されている高対話型 Honeypot

これ以降、1. の広く利用されている SSH の低対話型 Honeypot のことを ”純正の低対話型 Honeypot”、2. の実際の Shell には実装されているが、1. の Honeypot で未実装のコマンドを実装した Honeypot のことを ”修正済みの低対話型 Honeypot”、3. の広く利用されている高対話型 Honeypot のことを ”高対話型 Honeypot” と呼ぶこととする。

また予備実験では、純正の Honeypot に実装されていないコマンドで悪意のある侵入者が使うようなコマンドを実装し、純正の Honeypot で取れた侵入者の実行コマンドログと、修正済みの Honeypot の侵入者の実行コマンドログを比較することで、修正済みの Honeypot の方がコマンドパターンとして多く収集できることを示した。予備実験における収集ログの比較の概念図を図 6.3 に示す。

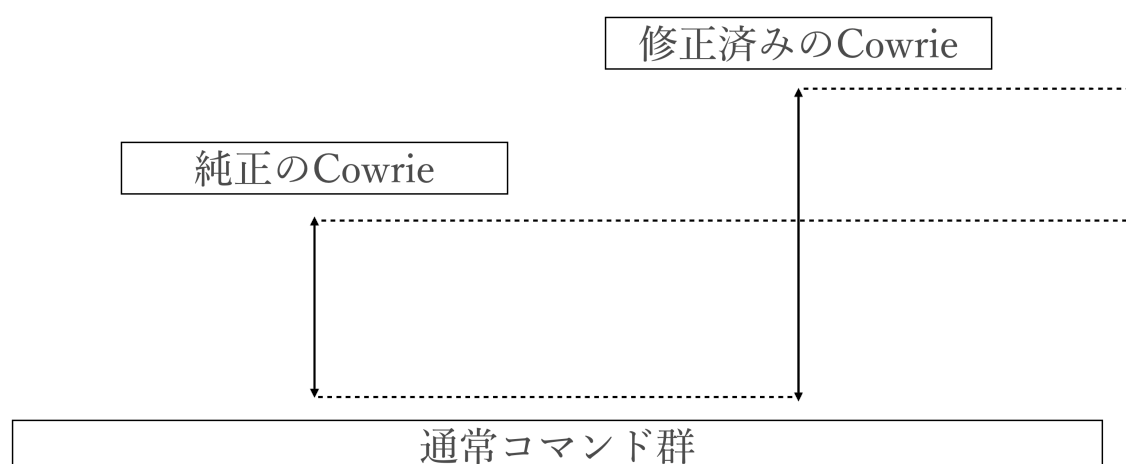


図 6.3: 予備実験の評価の概念図

この予備実験では評価として何の追加実装も施していない SSH の低対話型 Honeypot で取れた侵入者の実行コマンドログと追加実装を施した SSH の低対話型 Honeypot の侵入者の実行コマンドログとを比較したのに対して、本件研究の評価手法では、純正の Honeypot で取れた侵入者の実行コマンドログと修正済みの Honeypot の侵入者の実行コマンドログをと高対話型 Honeypot の侵入者の実行コマンドログを比較することで、修正済みの Honeypot の侵入者の実行コマンドログが実際の Shell の挙動にどれほど近似したのかを評価した。予備実験における収集ログの比較の概念図を図 6.4 に示す。

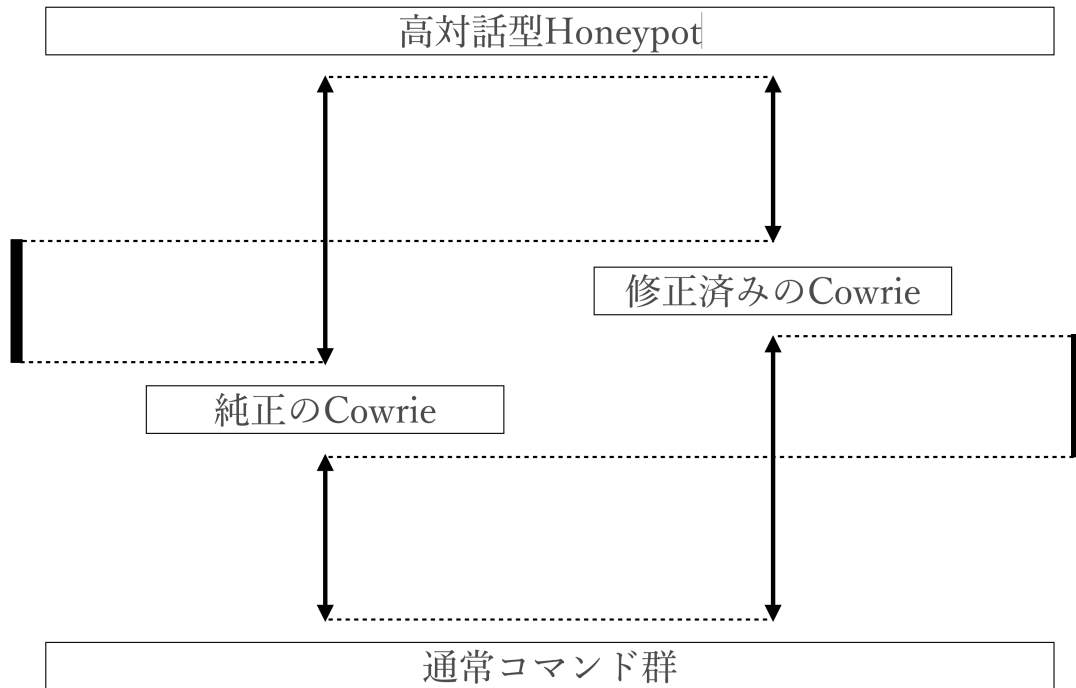


図 6.4: 本研究の評価の概念図

6.2.1 コマンドログのスコアリング手法の実装の提案

コマンドログの比較を行う手法は多く存在する．例えば評価基準として，あるコマンドが実行された時に，そのコマンドは危険であるとしたブラックリストを作成するパターンマッチングの手法がある．また，攻撃であるとされたコマンドを ?? で説明したマルコフモデルで学習させることで，攻撃性を表現する手法がある．しかしパターンマッチングであれば静的解析であるので未知の攻撃に対応ができず，マルコフモデルであれば現在の状態だけに依存して次の状態への推移確率が決まるので，未知の特徴量を無視してしまうので，いずれも未知の攻撃に対応できない．しかし， ?? で説明した意味解析をコマンドログに導入することで，コマンド名が別でも同じような内容のコマンドを実行しようとした時に，それが同じような内容であることを検知できる自然言語処理における意味解析のニューラルネットワークのモデルを評価基準とすることで未知の攻撃にも対応できる．そのため，本研究では自然言語処理における意味解析のニューラルネットワークのモデルを評価基準とした．

6.2.2 機械学習を用いたコマンドログのスコアリング

本研究では，評価基準となる，自然言語処理における意味解析のニューラルネットワークのモデルとして Word2vec の skip-gram モデルを採用した．純正の低対話型 Honeypot で収集した侵入ログで skip-gram モデルの隠れ層の重みを学習させ (これをモデル 1 とす

る), 同様にして高対話型 Honeypot で収集した侵入ログも skip-gram モデルの隠れ層の重みを学習させる (これをモデル 2 とする). 次に修正済みの Honeypot で収集したログをセッション開始からセッション終了までに打たれたコマンドごとに (以降これを 1 セッションごとと呼ぶ) モデル 1 とモデル 2 のそれぞれに入力していき, 出力された数値 a を活性化関数としてソフトマックス関数をかけることで, $0 \leq a \leq 1$ の範囲を取るようし確率的な数値として出力することでスコアリングを行う. このため入力に対して多数存在する出力を全てを合計すると 1 になる. 純正の低対話型 Honeypot や高対話型 Honeypot の収集ログをモデル化する際、入力層として収集ログのコマンドの入力に対してそのコマンドの周辺のコマンドを出力として与えることでこれを学習させる.

例えば 3 つのコマンドが打たれたとしたものを以下のプログラム 6.1 に示す.

プログラム 6.1: 3 つの実行コマンドの例

```
1  $  uname
2  $  free
3  $  ps  x
```

モデルを構築する際には”free”コマンドを入力にした時に, 出力として”uname”コマンド”ps”コマンドを用意しておくことで, free が入力として与えられた時に他 2 つの出力される周辺のコマンドが出力する確率が高くなるようにする. また, 実装としては周辺語をどこまで広げるのかはパラメータとして window size で与えることができ, 上記の例の周辺語は”1”であり, window size を”2”にすればモデル化する際に出力層に与えられる数は 4 つとなる.

以下の図 6.5 にモデル化のフローを示す.

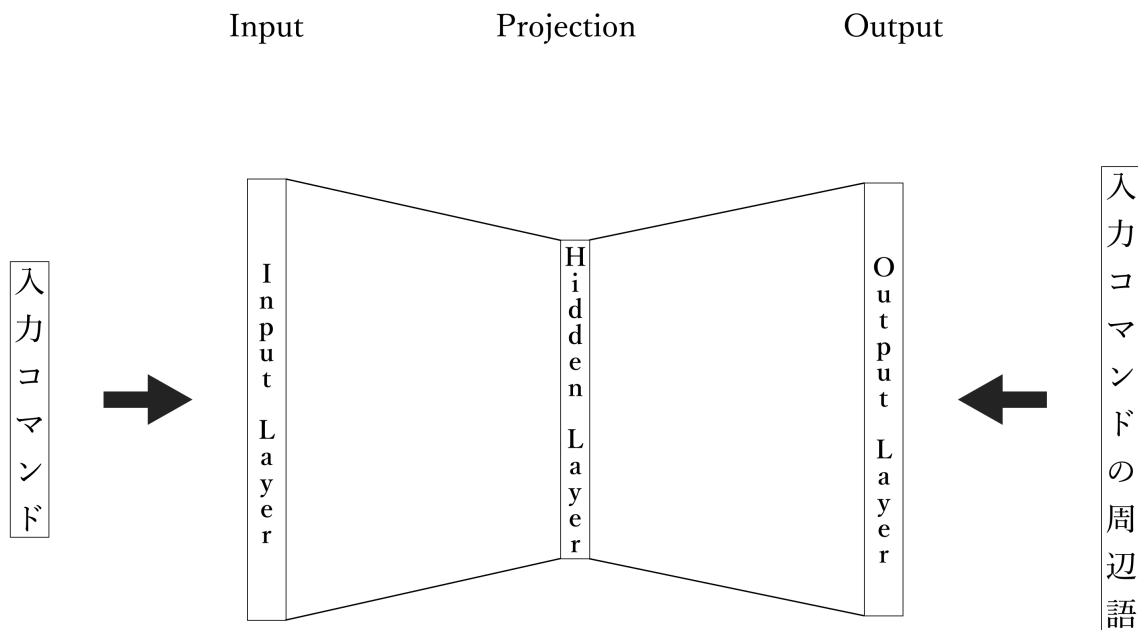


図 6.5: 評価のフロー??

また，このようにして純正の低対話型 Honeypot の収集ログと高対話型 Honeypot の収集ログに対して各々のモデルを構築する．次にこのモデルに対して，修正済みの Honeypot で収集したログを入力して，確率的にスコアリングしていくことで数値を出力する．

以下にこのモデルを使用した時の入力から出力のフローを図 6.6 を示す．

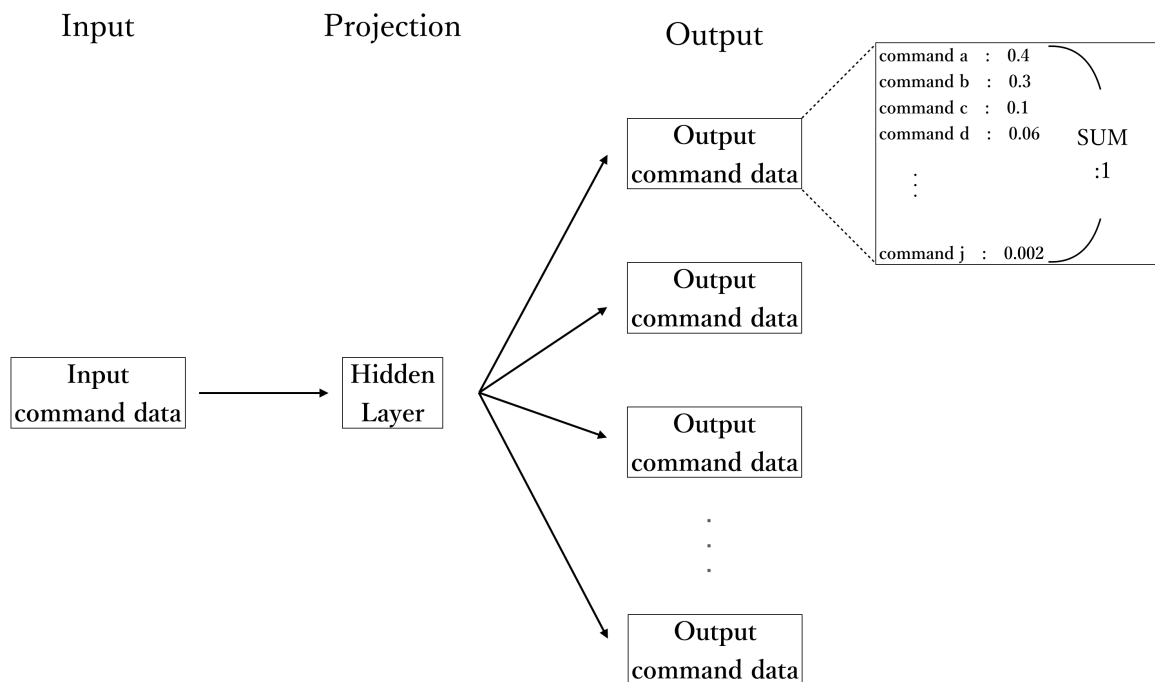


図 6.6: 評価のフロー??

このようにして出力された数値を 1 セッションごとに平均化し、また全てのセッションにおいてもセッションごとに平均化し、全てのセッションの平均化を行うことで、純正の低対話型 Honeypot の収集ログと高対話型 Honeypot の収集ログとの各々で構築したモデルごとに平均値を算出する。

6.2.2.1 コマンド群データのベクトル表現

6.2.2.2 SSH の低対話型 Honeypot の攻撃ログの比較

6.3 考察

第7章 関連研究

7.1 関連研究

本章では，SSH の Honeypot と時系列データの処理に関連する先行研究について紹介する．

7.1.1 SSH の Honeypot

7.1.2 自然言語処理

7.1.2.1 単語の意味のベクタ表現

第8章 結論

本章では、本研究のまとめと今後の課題を示す。

8.1 本研究のまとめ

本研究では、低対話型 Honeypot において、高対話型 Honeypot の侵入ログに近似するためには、侵入者から Honeypot であることの検知を回避する必要がある。そのために、低対話型 Honeypot の実行コマンドの挙動を本物の Shell の実行コマンドの挙動に近づけることを提案した。侵入者から Honeypot であることの検知を回避するためには、本物の Shell に実装されているコマンドの実装と、低対話型 Honeypot 特有の異常な挙動をするコマンドの修正を行う必要がある。そこで、本物の Shell に実装されているコマンドを低対話型 Honeypot に全て実装し、低対話型 Honeypot 特有の異常な挙動をするコマンドの修正を行った。低対話型 Honeypot の実行コマンドの挙動を本物の Shell の実行コマンドも挙動に近づけたかを検証するために、追加実装を施していない低対話型 Honeypot とコマンド拡張を行なった低対話型 Honeypot、高対話型 Honeypot を設置してコマンドログを収集し、比較した。コマンドログの自然言語処理による意味解析を行ない、個々のコマンドの意味を多次元のベクトル空間上で表現することで、コマンド拡張を行なった低対話型 Honeypot のコマンドログが高対話型 Honeypot のコマンドログの空間的距離が近いということが明らかにした。このことから、素の Honeypot にコマンド拡張を行い、低対話型 Honeypot の実行コマンドの挙動を本物の Shell の実行コマンドの挙動に近づけることで、拡張した低対話型 Honeypot で取れたコマンドログが高対話型 Honeypot のコマンドログに近似することを確認した。

8.2 本研究の課題と展望

本節では、提案手法の課題とその展望を述べる。SSH の低対話型 Honeypot に実装するコマンドについて、ディストリビューションごとに実装コマンドが異なるが、今回は BusyBox をそのまま Python で実装した。したがって、低対話型 Honeypot がエミュレーションしているディストリビューションで実装されているコマンドは必要条件しか満たしていない。また、??で述べた通り、低対話型 Honeypot には本研究と着目した問題以外にも、SSH でのセッション確立におけるレイテンシの問題や、Honeypot の Username の問題も存在する。しかし本研究ではこれらを扱わず、本物の Shell の挙動を完全にエミュ

レートできていないため，侵入者から Honeypot であることを検知されてしまう可能性はまだ残されている．

8.2.1 ディストリビューションごとの実装コマンド

ディストリビューションごとの実装コマンドについてはバージョンの問題にも依存する．しかし，OS のリリースには LTS(Long Term Support) があり，広く使われている OS での実装コマンドの検証は十分に可能である．

8.2.2 様々な Honeypot のコマンドログの精度評価への応用

現在様々な種類の SSH の低対話型 Honeypot が普及しているおり，それらの Honeypot ごとに実装コマンドが異なる．そのため，Honeypot の種類ごとに攻撃ログを収集し，本研究の評価手法を用いることで，自然言語処理による意味解析において使用した Honeypot で取れたコマンドログが，高対話型 Honeypot のコマンドログにどれほど空間的距離が近いのかを検証することができる．

8.2.3 コマンド系ごとの評価への応用

SSH の低対話型 Honeypot を設置し，自然言語処理による意味解析を行なったコマンドログにおいて，個々のコマンドごとに持つ意味が異なる，あるコマンドが使用できないような実装を施すと高対話型 Honeypot のコマンドログにどれほど空間的距離が遠くなるかを検証できる．

謝辞

俺と俺に関わった全てに感謝

参考文献

- Greg Corrado Jeffrey Dean Tomas Mikolov, Kai Chen. Efficient estimation of word representations in vector space. *ACM Transactions on Graphics (TOG)*, 32(4):138, 2013.
- Xin Rong. Word2vec parameter learning explained. *ACM Transactions on Graphics (TOG)*, 32(4):138, 2013.
- Kippo. Kippo. <https://github.com/desaster/kippo>, 2014.
- Ken Fujiyoshi, Chihiro Fukai, Hiroya Tanaka, Jin Mitsugi, and Jun Murai. Honeypot. *NIP & Digital Fabrication Conference 2014 1*, pages 316–319, 2014.
- Kippo. <https://github.com/desaster/kippo/>.
- Satoshi Nakamoto. kojoney: Kojoney. <http://kojoney.sourceforge.net/>, 2008.
- Vitalik Buterin. Twisted. <https://twistedmatrix.com/trac/>, 2014.
- Raspberry pi. <http://www.idc.com/getdoc.jsp?containerId=prUS40960716>, 2016.
- Single board computer. <http://fablabjapan.org/>.
- Kippo のプロジェクトの現在. <http://www.thingiverse.com/>.
- Number of kippo'commands. <https://github.com/desaster/kippo/tree/master/txtcmds>.
- Number of cowrie'commands. <https://github.com/cowrie/cowrie/tree/master/src/cowrie/commands>.
- 消費者庁. Kippo と cowrie の実装コマンドの違い. http://www.caa.go.jp/seikatsu/shingikai2/kako/spc13/houkoku_g/spc13-houkoku_g-4-1.html, 1992.
- Karl DD Willis and Andrew D Wilson. Secure shell. *ACM Transactions on Graphics (TOG)*, 32(4):138, 2013.
- Busybox. <https://proofofexistence.com/>.
- Wordnet. <https://wordnet.princeton.edu/>.

Wordnet wikipedia. <https://ja.wikipedia.org/wiki/WordNet>.

出口 利憲. ベクトル空間法による文書の類似度の算出. <http://www.gifu-nct.ac.jp/elec/deguchi/sotsuron/hayashi/node20.html>, 2010.

Cowrie. <https://github.com/cowrie/cowrie/>.