E-17

# ネットワーク境界部における Brute Force 攻撃に対する防御システムの構築

## Design and Implementation of the Border Gateway Defense System against the Brute Force Attack

寺本　達弥†　　川橋　裕‡
Teramoto tatsuya　　Kawahashi Yutaka

## 1．はじめに

インターネットの普及により様々なサービスやアプリケーションが登場した．個人や組織のサーバに自宅や外出先などの遠隔地から手元のコンピュータでアクセスし，様々なサービスを操作する機会が増加した．SSHやPOP，FTPなどが代表的なサービスである．

一方で，インターネットを介して上記のサービスを提供しているサーバやネットワーク機器へのサイバー攻撃による被害も増加している[1][2]．現在のサイバー攻撃に対する一般的な防御システムとしてFirewallによるフィルタリングがあげられる．Firewallによるフィルタリングは通過するパケットのヘッダ情報を検査し，管理者によって設定されたルールを適用することでパケットの通過・遮断を判断する．しかし，Firewallによるフィルタリングには問題がある．まず，多量のパケットを送信することで攻撃対象のサービスを提供不能にするF5リロード攻撃やSYN Flood攻撃などのDoS攻撃では，Firewallが処理するパケットの量が急激に増加しFirewallの過負荷により動作が停止する可能性がある[3]．次に，正規通信を悪用しサーバなどへのユーザ名とパスワードを不正に解読するBrute Force攻撃などを検知することが困難である．正規通信とはFirewallが許可している通信のことである．

既存研究（以下B-DRIP）では，DoS攻撃に対して組織内外の境界で防御する境界型防御システムが提案，実装されている[4][5][6]．B-DRIPでは単位時間ごとのパケット数をカウントし，過剰な数のパケットを送信している送信元IPアドレスを攻撃者と検知している．検知後，攻撃者から送られるパケットをソースアドレスルーティングにより破棄することで，サーバやネットワーク機器への攻撃を回避する．従来のルーティングでは宛先IPアドレスの情報で宛先ホストを決定していた．ソースアドレスルーティングは宛先IPアドレスの情報に加え，送信元IPアドレスも用いることで宛先ホストを決定する手法である．さらにB-DRIPはブリッジとして動作しているため，既存のネットワーク構成を変更せずケーブルの差し替えだけであらゆる場所に導入できる．

しかし，B-DRIPは単位時間のパケット数により攻撃者を検知しているため1セッションで多量のパケットをやり取りするSSHやPOPなどの通信を攻撃と誤検知してしまう問題点がある．さらに，ユーザ名とパスワードを頻数試行するBrute Force攻撃ではパケット数が少ないため検知できないという問題点がある．Brute Force攻撃を検知するために，攻撃を検知するための閾値を下げることでBrute Force攻撃を検知できるが，正規ユーザを攻撃と誤検知してしまう可能性がある．以上のことから，SSHやPOPなどの通信への誤検知を無くし，Brute Force攻撃を検知する別の検知手法が必要である．本研究では，B-DRIPのシステムにBrute Force攻撃を検知し，防御できるシステムの構築を目的とする．Brute Force攻撃はパスワードクラックを効率化するために多量のセッションを張り攻撃をおこなう特徴がある．セッションとは接続を確立してから切断するまでの一連の通信を示す．本研究では，この特徴を利用することでセッション数によりBrute Force攻撃を検知する．提案システムは，組織外から組織内へ流れるパケットをキャプチャし，データベースにセッション情報を格納する．セッション情報は1セッションでのIPアドレスやポート番号，時間などの情報である．提案システムは格納されたセッション情報から，単位時間のセッション数が過剰な送信元IPアドレスを検索することで，Brute Force攻撃を検知する．攻撃者からのパケットは破棄，もしくはICMPメッセージを用いてセッションを長引かせる．提案システムは，以上の動作により攻撃を回避するシステムである．

本論文では，従来の防御手法を説明した後，実装したシステムの構成と動作について説明し，最後に学内ネットワークで実運用した評価をおこなう．

## 2．従来の防御手法

### 2.1　従来の防御手法

サイバー攻撃に対する従来の防御手法としてFirewallとIDS/IPSは代表的なものである．

Firewallは組織内外の境界で，組織外からのサイバー攻撃を防御するために一般的に用いられる境界型防御システムである．Firewallはパケットの宛先IPアドレス，宛先ポート番号，プロトコルなどのヘッダ情報を管理者が設定したルールに適用してパケットのフィルタリングをおこなう．

IDSはネットワーク内のパケットをキャプチャし，シグネチャや管理者が設定したルールを用いて不正アクセスと思われるパケットを検知し管理者に通知するシステムである．シグネチャを用いた攻撃検知では，新しい攻撃に対応するためにシグネチャを頻繁に更新する必要がある．さらに，シグネチャはIDSを設置するネットワークに合わせ管理者が適切なものを使用する必要がある．これによりIDSを導入するには管理者にネットワークやIDSに対する正確な知識と設定が必要になる．IDSは攻撃検知後の対応は管理者がおこなう必要がある．

IPSはIDSに攻撃と検知した通信を自動的に遮断する機能を加えたシステムである．

### 2.2　DoS 攻撃

DoS攻撃とは，サーバやネットワーク機器に対して多量

†和歌山大学，Wakayama University

‡和歌山大学システム情報学センター，Center for Information Science, Wakayama University

のパケットを送りつけ攻撃対象の負荷を高めることによりサービスの提供を不能にする攻撃である．Firewallによるフィルタリングでは処理するパケットの量が急激に増加し，Firewallの負荷が高まり動作が停止する可能性がある．さらに，FirewallとIDS/IPSで共通の問題点として，正規通信を多量発生させるDoS攻撃検知することが難しいという問題点がある．

### 2.3 Brute Force 攻撃

Brute Force攻撃は，正規通信を悪用しパスワード認証を不正に突破する攻撃である．この攻撃はユーザ名とパスワードの組み合わせを頻数試行するクラッキングツールを用いる．効率の悪い攻撃だが，サービスの登録ユーザには単純なパスワードを設定している人もいるため，Brute Force攻撃によりパスワードが解読されてしまう可能性がある．さらに，複雑なパスワードを設定していても時間をかけることで解読されてしまう可能性がある．

攻撃者ごとに攻撃の間隔，ユーザ名とパスワードの組み合わせは様々であるが，一度のBrute Force攻撃で複数のサーバを同時に攻撃することが多い．さらに，Brute Force攻撃はパスワードクラックを効率化するために，異なる送信元ポート番号を利用し多量のセッションを張る特徴がある．Brute Force攻撃の攻撃対象は，ネットワーク経由で遠隔のコンピュータを操作するSSHなどである．JPCERTの調査によるとtelnetやFTPに対するBrute Force攻撃もあるが，ほとんどのBrute Force攻撃の対象はSSHである[1]．Brute Force攻撃によりパスワードが解読され不正に侵入された場合，情報漏洩やさらなる攻撃への踏み台にされることになる．Brute Force攻撃にはサーバのソケットの最大数まで利用しセッションを張る方法と，ソケットを制限し攻撃を断続的に継続しセッションを張る方法がある．

### 2.4 従来の防御手法の問題点

2.1節で述べたFirewallやIDSは従来の防御手法として代表的なものである．設置するネットワークに合わせて管理者がルールを設定することで，組織外からの様々な攻撃を防ぐことができる．しかし，Firewallでは2.2節で述べたようにDoS攻撃によりFirewallの負荷が高まり，動作が停止する可能性がある．IDS/IPSでは設定やシグネチャが不適切な場合は攻撃者からの攻撃を検知できない，もしくは正規ユーザを攻撃と誤検知してしまう可能性がある．さらに，Brute Force攻撃はFirewallが許可している通信を悪用して攻撃をするため，正規通信とBrute Force攻撃を見分けることが困難である．

## 3 ． 既存研究

### 3.1 既存研究

既存研究では，2.4節で述べたFirewallやIDSの問題点を解消するために，組織内外の境界で防御する境界型防御システムであるB-DRIPの提案と実装がされてきた．B-DRIPでは，攻撃を検知するために単位時間のパケット数を閾値としている．B-DRIPはあらかじめルールファイルに防御対象サーバのIPアドレス，閾値，ポート番号を設定する．パケットをキャプチャし送信元IPアドレスごとのパケット数をカウントすることで，単位時間のパケット数が閾値を超えた送信元IPアドレスをDoS攻撃と検知する．検知した場合，後述するソースアドレスルーティングによりDoS攻撃の防御を可能にしている．さらにB-DRIPはブリッジカーネルオプションを使用してブリッジを実装しているため，OSI参照モデルの第2層で動作しケーブルの差し替えのみであらゆる場所に導入できる．

### 3.2 ソースアドレスルーティング

従来のルーティングでは宛先IPアドレスの情報とルーティングテーブル（経路制御表）によりパケットを宛先ホストまでルーティングしている．従来のルーティングに送信元IPアドレスの情報を付加して，ルーティング先を決定する手法がソースアドレスルーティングである．

送信元IPアドレスの情報を付加することで同じ宛先IPアドレスへのパケットでも送信元IPアドレスによって経路を変更することができる．B-DRIPでは，攻撃と検知した送信元IPアドレスからのパケットの宛先を攻撃回避用IPアドレスへ変更することで，DoS攻撃を防御している．

従来のルーティングでは，攻撃者に関係なくルータは宛先IPアドレスと次ホップの情報によりパケットを宛先ホストまでルーティングする．しかしソースアドレスルーティングでは，宛先IPアドレスと次ホップ，送信元IPアドレスによりパケットを宛先までルーティングする．

### 3.3 既存研究の問題点

既存研究では，B-DRIPを用いてDoS攻撃に対する評価実験を実施し，攻撃を検知，回避できることが示された．しかし，既存研究のB-DRIPは1セッション内で多量のパケットをやり取りするSSHやPOPなどの通信を攻撃だと誤検知してしまう問題点がある．SSHやPOPなどの通信を攻撃と誤検知しないようにするには閾値を上げる必要があるが，閾値を上げてしまうと攻撃を見逃してしまう可能性がある．さらに，ユーザ名とパスワードを頻数試行するBrute Force攻撃では，パケット数が少ないためB-DRIPの閾値を超えず攻撃と検知できない．Brute Force攻撃を検知するため閾値を下げる必要がある．しかし，Brute Force攻撃を検知するために，B-DRIPの閾値を下げてしまうと正規ユーザを攻撃と誤検知してしまう可能性がある．そのため，攻撃を検知する閾値の適切な設定が困難である．

上記の内容より，SSHやPOPなどの通信を攻撃だと誤検知してしまう問題点を無くし，Brute Force攻撃を検知する必要がある．そのためにはパケット数ではなく別の閾値が必要になる．

## 4 ． 研究目的

3.3節で述べたように，B-DRIPではSSHやPOPなどの1セッション内で多量のパケットをやり取りする通信を攻撃と誤検知してしまう．さらに，ユーザ名とパスワードを頻数試行するBrute Force攻撃ではパケット数が少ないため検知することができない．Brute Force攻撃の検知は閾値を下げることで可能になるが，閾値を下げることで正規ユーザを攻撃と誤検知してしまう問題点がある．

本研究では，B-DRIPの問題点を解消しBrute Force攻撃を検知，防御するシステムの構築を目的とする．さらに，ネットマスク単位で防御対象サーバのIPアドレスを指定することでネットワークアドレスに属する全てのサーバを防御し，防御対象サーバへのBrute Force攻撃を迅速に検知し防御する．さらに，防御対象サーバを追加で導入する際，システムに防御対象サーバのIPアドレスを新たに指定せず導入できる．加えて，防御対象サーバには一

切の設定をすることなくBrute Force攻撃を検知し，防御するシステムの構築をする．なお，JPCERTの調査によるとBrute Force攻撃の対象がほとんどSSHであるため，本論文では対象がSSHのBrute Force攻撃を検知，防御するシステムの構築を目的とする．

## 5 ． 提案手法

### 5.1 Brute Force 攻撃の検知手法

Brute Force攻撃はユーザ名とパスワードを頻数試行する攻撃であるため，攻撃によるパケット数はDoS攻撃のように過剰にならない．さらに，2.3節で述べたようにBrute Force攻撃はパスワードクラックを効率化するために多量のセッションを張り攻撃をする特徴がある．また，Brute Force攻撃はTCPを利用するため，1セッションには1つの送信元ポート番号が必要になる．すなわちBrute Force攻撃はセッションの数だけ異なる送信元ポート番号を使わなければならないと言える．よって，送信元ポート番号が異なる同一送信元IPアドレスのセッション数をカウントすることでBrute Force攻撃を検知できると考えられる．さらに，Brute Force攻撃は一度に複数のサーバを同時に攻撃することが多い特徴がある．防御対象サーバのIPアドレスをネットマスクで指定し，防御対象サーバ群へのセッション数をカウントすることでBrute Force攻撃を効率的に検知できると考えている．なお，ネットマスクでIPアドレスを指定することで防御対象サーバを追加導入する際，システムに防御対象サーバのIPアドレスを新たに指定せず導入できると考えられる．

本研究では，上記の特徴を利用することでBrute Force攻撃を検知する手法を提案する．組織外から組織内の防御対象サーバへ流れるパケットをキャプチャし，パケットのTCP・UDP/IPヘッダの情報をセッション情報に整形しデータベースに格納する．単位時間ごとにデータベースからセッションを検索し，同一送信元IPアドレスからのセッション数をカウントする．同一ネットマスクの宛先IPアドレスと宛先ポート番号が22番（SSH），プロトコルがTCP であり，送信元ポート番号が異なる同一の送信元IPアドレスを検索条件とする．セッション数が閾値以上の送信元IPアドレスをBrute Force攻撃の攻撃者と検知する．図1 はキャプチャしたTCP・UDP/IPのヘッダ情報をセッション情報に整形する概要図である．

受信パケット群のA1とA2とA3，B1とB2はそれぞれ同じ通信のパケットである．受信したパケットのヘッダ情報の送信元IPアドレス，宛先IPアドレス，宛先ポート番号，プロトコルが同じであり，送信元ポート番号が異なるパケットごとにまとめて1つの情報に整形する．図1のA1とA2とA3のパケットはセッションA，B1とB2のパケットはセッションBとまとめることで，それぞれ1つの情報に整形することができる．この情報がセッション情報である．閾値は，1ヶ月以上Brute Force攻撃の対象になっているサーバのログからBrute Force攻撃と正規ユーザを誤認しないよう考慮した値を用いる．さらに，セッション数で攻撃を検知することでB-DRIPの問題点であるSSH やPOPなどへの通常アクセスを攻撃と誤検知することを回避できると考えている．暗号化されていない通信へのBrute Force攻撃はパケットを検査することで検知できる．しかし，SSHなどの暗号化通信へのBrute Force攻撃はパケットを検査するだけでは検知できないため，本研究ではセッション情報によりBrute Force攻撃を検知することで暗号化通信への攻撃を検知できると考えている．

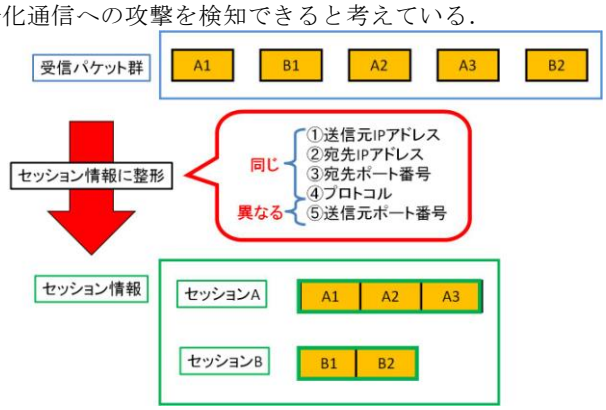

図 1 セッション情報への整形概要図

### 5.2 Brute Force 攻撃の防御手法

Brute Force攻撃を防御するために本研究では2つの防御手法を提案する．本節では，2つの防御手法について述べる．

#### 5.2.1 ルーティングによる防御手法

Brute Force攻撃を防御するには，防御対象サーバに届くまでのネットワーク経路内で防御することが有効であると考えている．そこで，攻撃者からの攻撃パケットを全て破棄することでBrute Force攻撃を防御対象サーバから防御できると考えられる．

ルーティングによる防御手法では，5.1節で述べたBrute Force攻撃検知手法で攻撃と検知した送信元IPアドレスを利用したソースアドレスルーティングにより攻撃パケットを破棄する．ソースアドレスルーティングにより攻撃パケットを/dev/nullに転送することで全て破棄することができる．この手法により，攻撃された防御対象サーバには攻撃パケットが届かなくなり，防御対象サーバを防御することができる．さらに，攻撃者にはACK パケットなどの返信パケットが送られず，防御対象サーバとの通信が切断される．攻撃者は通信が切断されたことにより，それ以降の防御対象サーバへのBrute Force攻撃を中止すると考えられる．

#### 5.2.2 Source Quench による防御手法

5.2.1項で述べたように，Brute Force攻撃を防御するには防御対象サーバに届くまでのネットワークの経路内で防御することが有効であると考えられる．Source Quenchによる防御手法では，攻撃者の攻撃パケットの送信間隔を長くさせることでBrute Force攻撃を防御する．Brute Force攻撃には多量のソケットを利用して多量のセッションを張り攻撃する方法と，ソケットを制限して攻撃を何度も断続的に長時間継続することで多量のセッションを張り攻撃する方法がある．攻撃パケットの送信間隔を長くさせることで，ソケットを制限し攻撃を断続的に継続するBrute Force攻撃には特に効果的だと考えられる．この攻撃方法は1セッション内で複数回パスワードクラックをおこなう処理が断続的に継続する．このため攻撃パケットの送信間隔を長くしセッションを引き伸すことで次の攻撃を止められると考えられる．

本防御手法では，5.1節で述べたBrute Force攻撃検知手法で攻撃と検知した送信元IPアドレスにパケットの送信間隔を長くさせるICMPメッセージの1つであるSource Quench[7] を送ることでサーバを防御する手法を提案す

る．Source Quenchを送ることで攻撃者は攻撃パケットの送信時間の間隔を長くし，Source Quenchを多量に送ることによりパケットの送信間隔時間を長くすることで，セッションが滞りBrute Force攻撃を続けられなくなる．ルーティングによる防御手法とは違い，攻撃者と防御対象サーバとの通信はセッションが滞るため通信は切断されない．なお，正規ユーザが端末エミュレータを用いて攻撃と誤検知された場合は，通信が切断されないため端末エミュレータは強制終了されずパケットも送信できない状態が継続する．誤検知されたユーザが管理者に報告することによりシステムの誤検知がわかると考えられる．

### 5.3　提案手法

本節では，提案システムで用いるハードウェア構成とソフトウェア，5.1節と5.2節で述べた手法を実現した提案システムの機能と動作について述べる．提案システムは和歌山大学のネットワーク内外の境界に設置する．

#### 5.3.1　ハードウェア構成

実装したシステムのハードウェア構成を以下に示す．提案システムはブリッジとして動作するためNICを2枚使用している．

- OS ： FreeBSD
- CPU ： Intel(R) Pentium(R) Dual CPU E2200 @2.20GHz
- Memory ： 4.00GB
- NIC1 ： Intel(R) PRO/1000 Network Connection 7.1.
- NIC2 ： Intel 82559 Pro/100 Ethernet

#### 5.3.2　本研究で用いるソフトウェア

**MySQL**

MySQL[7]はフリーソフトウェアのリレーショナルデータベースマネージメントシステムである．MySQLは多量のデータを高速に検索することが可能である．

**ipfw**

ipfw[8]はFreeBSDに実装されているパケットフィルタリング機能を持つFirewallである．カーネル内で動作するため高速で動作し，負荷が小さい．

**zebra**

zebra[9]はUnix上で動作するルーティングソフトウェアである．様々なルーティングプロトコルに対応しており，経路情報をカーネルのルーティングテーブルに反映させることができる．提案システムでは静的ルーティングにより攻撃パケットを/dev/nullへ転送することで攻撃パケットを破棄している．

**tcpnice**

tcpniceはネット監視ソフトのツールの1つである．tcpniceは指定したIPアドレスに5.2.2節で述べたSource Quenchを送るツールである．指定したIPアドレスにSource Quenchを送りつけることにより，指定したIPアドレスからのパケット送信速度を強制的に下げ通信遅延を起こさせる．

#### 5.3.3　システム構成

本項では，提案システムの構成について述べる．提案システムの構成図を図2に示す．提案システムはパケットキャプチャ部，Brute Force攻撃検知部，Brute Force攻撃防御部で構成される．パケットキャプチャ部では，パケットをキャプチャし，パケットのTCP・UDP/IPヘッダの情報をセッション情報としデータベースに格納する．Brute Force攻撃検知部では，データベースにアクセスしBrute Force攻撃がないか調査する．Brute Force攻撃防御部では，Brute Force攻撃検知部からの攻撃元情報を用いて攻撃を防御する．以下で各部の詳細を述べる．

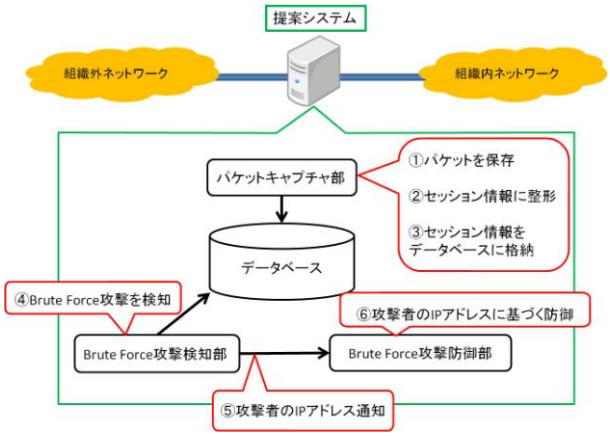


図２　提案システムの構成図

**パケットキャプチャ部**

本システムは組織内外の境界で動作し，組織外から組織内へ流れるパケットをキャプチャし TCP・UDP/IP **ヘッダの情報を保存する．1 分間のパケットの** TCP・UDP/IP **ヘッダの情報をセッション情報へ整形しデータベースに格納する．格納したセッション情報は** Brute Force **攻撃の検知に利用する．格納するデータベースには** MySQL **を使用する．セッション情報を以下に示す．**

- 送信元IPアドレス
- 宛先IPアドレス
- 送信元ポート番号
- 宛先ポート番号
- プロトコル
- キャプチャした時間

**Brute Force 攻撃検知部**

Brute Force攻撃検知部は，5.1節で述べた検知手法を用いてBrute Force攻撃を検知する．実装したBrute Force攻撃の検知プログラムによって，1分ごとにデータベースへアクセスしBrute Force攻撃がされていないかを調べる．検知には，2.3節で述べたBrute Force攻撃の送信元ポート番号が異なる特徴を利用する．1分間にプログラム内で設定した同一ネットマスクの宛先IPアドレスと宛先ポート番号が22番，プロトコルがTCPであり，送信元ポート番号が異なる同一の送信元IPアドレスのセッション数を検索する．検索したセッション数が閾値以上の送信元IPアドレスをBrute Force攻撃の攻撃者と検知する．この閾値は，1ヶ月以上Brute Force攻撃の対象になっていたサーバのログからBrute Force攻撃と正規ユーザを誤認しないよう考慮した値である．表1はBrute Force攻撃されたサーバの1分間の合計セッション数である．10の攻撃者からのBrute Force攻撃で平均セッション数が43.6回，最小セッション数が24回という結果が示された．本研究では，この結果を元に閾値を最小セッション数より少ない20を採用した．本システムでは，宛先ポート番号を22番を指定することで検索している．宛先ポート番号を変更することで，様々なサービスに対するBrute Force攻撃を検知することができる．

| 攻撃者 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 平均 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1分間の合計セッション数 | 41 | 26 | 38 | 46 | 36 | 74 | 42 | 55 | 50 | 28 | 43.6 |

表１　Brute Force 攻撃されたサーバの１分間の合計セッション数

**Brute Force 攻撃防御部**

本研究では，5.2節で述べたように，Brute Force攻撃の防御手法にはルーティングによる防御手法とSource Quenchによる防御手法の2つを使用した．以下に2つの防御手法について述べる．

- **ルーティングによる防御手法**

ルーティングによる防御手法では，Brute Force攻撃検知部で検知した攻撃者からのパケットをソースアドレスルーティングにより破棄し攻撃を防御する手法である．パケットを破棄するためにipfwとzebraを用いる．ipfwは検知した送信元IPアドレスからの攻撃パケットをzebraに転送するipfwルールを作成し，zebraに転送する．さらに，転送されてきたパケットをzebraが/dev/nullへ転送することでパケットを破棄する．攻撃検知後，一定時間はipfwルールが有効化され/dev/nullに転送されるが，一定時間経過後ipfwルールを削除する．攻撃者が検知後の1分間に攻撃を続け閾値を超えた場合，ipfwルールは削除されず再び1分間有効化される．すなわち，攻撃者が攻撃し続け，閾値を超え続ける限り攻撃パケットは破棄され続ける．

- **Source Quenchによる防御手法**

Source Quenchによる防御手法では，Brute Force攻撃検知部で検知した攻撃者のIPアドレスへ5.3.2項で述べたtcpniceを用いてSource Quenchを送り攻撃を防御する手法である．攻撃検知後，一定時間はtcpniceでSource Quenchを攻撃者に送り攻撃を防御する．攻撃者はSource Quenchを受信することで，パケットの送信時間の間隔を遅くする．tcpniceにより多量のSource Quenchを送ることで攻撃者はパケットの送信時間の間隔が抑制され，セッションが長引くことで攻撃ができなくなる．一定時間経過後tcpniceは止まるが，攻撃者が検知後の一定時間内に攻撃を続け閾値を超えた場合，tcpniceは止まらず再び一定時間Source Quenchを送り続ける．

### 5.4　提案システムの動作

本節では，提案システムがBrute Force攻撃を検知してから防御する一連の流れについて述べる．図3に提案システムのフローチャート図を示す．提案手法では組織内外の境界に設置することを前提としている．提案システムの動作について以下に手順を述べる．

1. 組織外ネットワークから組織内ネットワークへ流れるパケットをキャプチャし，TCP・UDP/IPヘッダの情報を保存する
2. パケットキャプチャした1分間のパケットのTCP・UDP/IPヘッダの情報をセッション情報に整形
3. セッション情報をデータベースに格納する
4. Brute Force攻撃検知部がデータベースにアクセスし，セッション情報を検索することでBrute Force攻撃の検知をおこなう．同一ネットマスクの宛先IPアドレスと宛先ポート番号が22番，プロトコルがTCPであり，送信元ポート番号が異なる同一送信元IPアドレスのセッション数を検索する．セッション数が閾値以上の送信元IPアドレスを攻撃者と検知する
5. Brute Force攻撃検知部で検知した攻撃者の送信元IPアドレスをBrute Force攻撃防御部に通知する
6. 通知された攻撃者のIPアドレスを利用した防御手法により防御する

以降は防御手法により動作が異なるため，以下に防御手法ごとの動作を述べる．

**ルーティングによる防御手法**

7. 攻撃者のIPアドレスからのパケットをzebraへ転送するipfwのルールを作成する
8. 攻撃パケットをipfwによりzebraへ転送する
9. zebra によりパケットは/dev/nullへ転送する
10. 一定時間経過後，ipfwのルールを削除する

**Source Quench による防御手法**

7. Brute Force攻撃検知部で検知したIPアドレスへtcpniceによりSorce Qunechを多量に送信する
8. 一定経過後，tcpniceを停止する

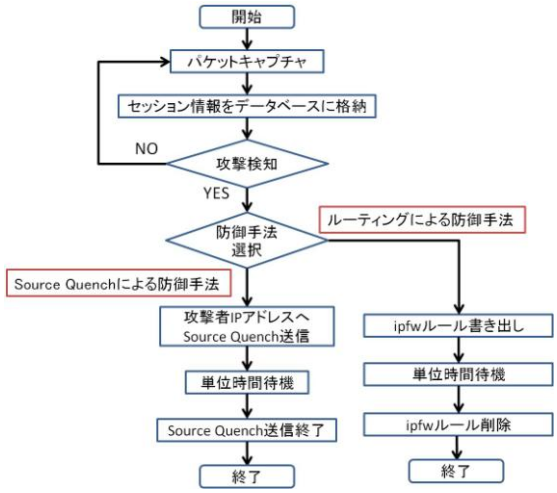


図３　提案システムのフローチャート図

## 6．評価

本章では提案システムの実験の結果を示し，関連システムと提案システムとの比較評価，本研究の今後の課題について述べる．

### 6.1　実験

本節では，5.3節で述べた提案システムを用いた実験について述べる．

#### 6.1.1　実験概要

以前から和歌山大学内の様々なサーバに対してBrute Force攻撃が試行されている．実験では和歌山大学内のBrute Force攻撃が試行されていたサーバの上位に提案システムを設置し，実際に攻撃している攻撃者を対象としBrute Force攻撃を検知し防御できたかの実験をおこなった．実験では攻撃を検知するためのセッション数の閾値を20としている．

パケットキャプチャ部とBrute Force攻撃検知部が正常に動作し，Brute Force攻撃を検知できるかの実験を2013年1月10日から1月25日の2週間おこなった．検知の確認の

ために，Brute Force攻撃を検知した場合アラートを通知する設定をおこないデータベースと照らし合わせる．

Brute Force攻撃防御部が正常に動作し攻撃を防御できるかの実験を異なる期間でおこなった．期間としてルーティングによる防御手法は2013年1月10日から1月17日，Source Quenchによる防御手法は2013年1月18日から1月25日の1週間ずつおこなった．攻撃を回避できたことは，攻撃者のアクセスが検知後の防御対象サーバのアクセスログに出力されていないことで確認する．実際に組織外から攻撃している攻撃者を対象としているため，実験結果の攻撃間隔，攻撃時間などは攻撃者により異なる．

### 6.1.2 実験結果

本項では，実験により得られた結果をBrute Force攻撃検知手法とBrute Force攻撃の防御手法2つについてそれぞれ述べる．Brute Force検知手法は実験期間の2週間の結果である．Brute Force攻撃の防御手法はそれぞれ実験期間の1週間ずつの結果である．

#### Brute Force 攻撃検知部

実験結果を表2に示す．閾値を超えたBrute Force攻撃は全て検知することに成功し，さらに正規ユーザを誤検知しなかった．しかし，閾値を超えなかったBrute Force攻撃が1件存在し，検知することができなかった．

| 攻撃者 | 攻撃検知 | 攻撃者 | 攻撃検知 | 攻撃者 | 攻撃検知 |
|---|---|---|---|---|---|
| 攻撃者1 | ○ | 攻撃者12 | ○ | 攻撃者23 | ○ |
| 攻撃者2 | ○ | 攻撃者13 | ○ | 攻撃者24 | ○ |
| 攻撃者3 | ○ | 攻撃者14 | ○ | 攻撃者25 | ○ |
| 攻撃者4 | ○ | 攻撃者15 | ○ | 攻撃者26 | ○ |
| 攻撃者5 | ○ | 攻撃者16 | × | 攻撃者27 | ○ |
| 攻撃者6 | ○ | 攻撃者17 | ○ | 攻撃者28 | ○ |
| 攻撃者7 | ○ | 攻撃者18 | ○ | 攻撃者29 | ○ |
| 攻撃者8 | ○ | 攻撃者19 | ○ | 攻撃者30 | ○ |
| 攻撃者9 | ○ | 攻撃者20 | ○ | 攻撃者31 | ○ |
| 攻撃者10 | ○ | 攻撃者21 | ○ | 攻撃者32 | ○ |
| 攻撃者11 | ○ | 攻撃者22 | ○ | | |

表 2　Brute Force 攻撃検知部実験結果

#### ルーティングによる防御手法

実験結果を表3に示す．表3は攻撃検知時のセッション数と防御手法では回避できなかった攻撃回数の表である．この実験中に合計14の攻撃者から合計900回以上のBrute Force攻撃がされていた．表3の防げなかった攻撃回数が全て0回であったため，攻撃検知後のBrute Force攻撃は全て回避に成功したことがわかった．

#### Source Quench による防御手法

実験結果を表4に示す．表4は表3と同様の項目である．この実験中に合計17人の攻撃者から合計7200回以上のBrute Force攻撃がされていた．本手法では表4の攻撃者4以外のBrute Force攻撃を全て回避できたことがわかった．攻撃者4は約120分間で5234回の攻撃を続けていたが本防御手法では防御ができなかった．

### 6.1.2 実験結果

#### Brute Force 攻撃検知部

6.1.2項の実験結果より，提案システムのBrute Force攻撃の検知システムはセッション数の閾値を超えたBrute Force攻撃は全て検知することができた．しかし，1件だけ閾値を超えずにBrute Force攻撃と検知できなかった攻撃者がいた．この攻撃者は1分間に16回のBrute Force攻撃を続けていた．今回の実験では，閾値を20としていたためこの攻撃者を検知できなかった．検知時間を調整することで検知できなかった．Brute Force攻撃に対応できると考えられる．もしくは，閾値を調整することでBrute Force攻撃の見逃しを限りなく少なくすることができると考えられる．閾値を調整する場合，正規ユーザを攻撃と誤検知しない値にする必要があるため検証と評価が必要である．

| 攻撃者 | 攻撃検知時のセッション数 | 防げなかった攻撃回数 |
|---|---|---|
| 攻撃者1 | 50 | 0 |
| 攻撃者2 | 41 | 0 |
| 攻撃者3 | 75 | 0 |
| 攻撃者4 | 54 | 0 |
| 攻撃者5 | 92 | 0 |
| 攻撃者6 | 60 | 0 |
| 攻撃者7 | 43 | 0 |
| 攻撃者8 | 30 | 0 |
| 攻撃者9 | 55 | 0 |
| 攻撃者10 | 67 | 0 |
| 攻撃者11 | 84 | 0 |
| 攻撃者12 | 31 | 0 |
| 攻撃者13 | 21 | 0 |
| 攻撃者14 | 87 | 0 |

表 3　ルーティングによる防御手法実験結果

| 攻撃者 | 攻撃検知時のセッション数 | 防げなかった攻撃回数 |
|---|---|---|
| 攻撃者1 | 31 | 0 |
| 攻撃者2 | 32 | 0 |
| 攻撃者3 | 30 | 0 |
| 攻撃者4 | 41 | 5234 |
| 攻撃者5 | 50 | 0 |
| 攻撃者6 | 130 | 0 |
| 攻撃者7 | 89 | 0 |
| 攻撃者8 | 60 | 0 |
| 攻撃者9 | 65 | 0 |
| 攻撃者10 | 22 | 0 |
| 攻撃者11 | 29 | 0 |
| 攻撃者12 | 32 | 0 |
| 攻撃者13 | 30 | 0 |
| 攻撃者14 | 26 | 0 |
| 攻撃者15 | 42 | 0 |
| 攻撃者16 | 43 | 0 |
| 攻撃者17 | 28 | 0 |

表 4　Source Quench による防御手法実験結果

#### ルーティングによる防御手法

6.1.2項の実験結果より，攻撃検知後の攻撃者からの全ての攻撃を回避することに成功した．本手法の実験中に攻撃してきたほとんどの攻撃者にはある共通の特徴が見られた．それは検知後のルーティングによりパケットが破棄されると，ほとんどの攻撃者はすぐに攻

撃を中止したという結果が得られたことである．実験前は数分～数十分間Brute Force攻撃を試行されていたが，この手法の実験中は攻撃時間が最長3分間だったことが確認できた．さらに，この手法の実験中に対処された攻撃者からのBrute Force攻撃の頻度が減ってきているのが確認できた．これはパケットが破棄され攻撃者へACKパケットなどの返答パケットが送られないことにより，攻撃者が攻撃を中止もしくは攻撃対象を変更したと考えられる．以上より，本防御手法はBrute Force攻撃を防御する手法として適切であると考えられる．

#### Source Quench による防御手法

6.1.2項の実験結果より，攻撃検知後の攻撃者からの攻撃は1件を除き回避することに成功した．回避できなかった攻撃者は実際の攻撃時に発見することができた．Source Quenchを送る回数を変更したが，攻撃者の挙動が変更前と何も変化せずBrute Force攻撃を続けていた．この原因と考えられるのが，攻撃者のFirewallがSource Quenchを遮断していたのではないかと考えられる．しかし，1週間実験しこの攻撃者以外の攻撃は全て回避することに成功したため，Source Quenchによる防御手法はBrute Force攻撃を防御する手法として利用できると考えられる．

### 6.1.4　防御手法の比較

6.1.3項でそれぞれの防御手法の考察をおこなった．Source Quenchによる防御手法では，1件の攻撃者を除く攻撃は全て回避することができた．一方で，ルーティングによる防御手法は全ての攻撃を回避することができた．さらに，対処された攻撃者からのBrute Force攻撃頻度が減ってきているのが確認された．以上より，Brute Force攻撃を防御する手法としてルーティングによる防御手法が最も適切であると考えられる．

## 6.2　評価

本節では，Brute Force攻撃を検知，防御する関連システムを説明し，提案システムと関連システムとの比較評価を述べる．

### 6.2.1　関連システム

#### ソニックウォール社の IPS

ソニックウォール社のIPSでは，Brute Force攻撃の検知が可能である[10]．このIPSでのBrute Force攻撃検知手法は一定時間内に防御対象サーバへ設定した回数以上のパスワード認証をおこなったIPアドレスを攻撃者と検知する．このIPSを導入するには導入するネットワーク環境にあわせた様々な設定が必要になる．設定によりブリッジとして導入が可能である．

しかし，ソニックウォール社のIPSはパケットのペイロードをシグネチャからBrute Force攻撃や他の攻撃と検知している．すなわち，ソニックウォール社のIPSが検知できるBrute Force攻撃はFTPなどの暗号化していない通信に限られる．SSHやPOPなどの暗号化されている通信へのBrute Force攻撃は検知することができない．

#### syslog サーバを用いた防御システム

syslogサーバを運用してあらかじめ設定しておいた組織内サーバのSSHDのアクセスログを集めて監視することにより，組織内で発生した総当たり攻撃を検知し，ホスト間で連携して対策をする手法である[11]．

syslogサーバで検知した攻撃者のIPアドレスを各ホストに通知し接続を拒否などの対策が取れるため，まだ攻撃を受けていないサーバに対して事前に攻撃を防止することができる．攻撃検知には一定時間内に閾値以上の認証エラーをしたIPアドレスを攻撃者と検知する．以下のいずれかの条件を超えた場合攻撃と検知する．

- 条件1:2分以内に11回（繰り返しの接続試行1）
- 条件2:10分以内に20回（繰り返しの接続試行2）
- 条件3:10分以内に30回（比較的信頼できる相手）

各ホストに固有の検知条件が必要な場合は各ホストで例外ルールを設定する必要がある．接続の拒否にはアクセス制御ファイルやiptablesに書き出して接続を拒否する． syslogサーバとホストの連携には各ホストでsyslogサーバにSSHDのアクセスログを送るための設定をおこないsyslogdを動作させておくことでsyslogサーバと連携できる．

### 6.2.2　関連システムと本研究の比較評価

本節では，Brute Force攻撃の検知，Brute Force攻撃の防御，ネットマスクによる防御対象サーバ指定，防御対象サーバの設定変更不要の項目から本研究と関連システムの比較評価をおこなう．

#### Brute Force 攻撃の検知

ほとんどのBrute Force攻撃がSSHを対象としているため，比較項目のBrute Force攻撃の検知するしくみとはSSHへのBrute Force攻撃を検知できる手法が実装されていることと定義する．

ソニックウォール社のIPSでは，Brute Force攻撃を検知する手法が実装されているが検知できるBrute Force攻撃はtelnetやFTPなどの暗号化されていない通信だけである．SSHやPOPなどの暗号化された通信に対するBrute Force攻撃は検知できない．syslogサーバを用いた防御システムでは，防御対象サーバからのSSHDアクセスログを収集することでBrute Force攻撃を検知する手法を実装している．この手法では，SSHへのBrute Force攻撃を検知することが可能である．

本研究では，防御対象サーバの上位に設置し，防御対象サーバへのセッション数が閾値を超えたBrute Fource攻撃を検知する手法を実装している．さらに，本研究ではSSHに対するBrute Force攻撃を検知が可能である．よって，本研究とsyslogサーバを用いた防御手法はSSHに対するBrute Force攻撃を検知するしくみがあるといえる．

#### Brute Force 攻撃の防御

ソニックウォール社のIPSでは，攻撃者のIPアドレスをアクセス拒否にすることでBrute Force攻撃を防御している．syslogサーバを用いた防御システムでは，攻撃者のIPアドレスを防御対象サーバに通知し各サーバでアクセス拒否することでBrute Force攻撃を防御している．本研究のルーティングによる防御手法では，攻撃者からのパケットを全て/dev/nullへ転送しパケットを破棄することでBrute Force攻撃を防御している．本研究のSource Quenchによる防御手法では，攻撃者のIPアドレスにSource Quenchを送ることでBrute Force攻

撃を防御しているが，実験でこの防御手法で防御できない攻撃者もいたが他の全てのBrute Force攻撃を防御できた．よって，ソニックウォール社のIPSとsyslogサーバを用いた防御システム，本研究のルーティングによる防御手法は本研究のSource Quenchによる防御手法よりBrute Force攻撃を防御できるといえる．

**ネットマスクによる防御対象サーバの IP アドレス指定**

ソニックウォール社のIPSとsyslogサーバを用いた防御システムでは，防御対象サーバを1つずつIPアドレスで指定しなくてはならないためネットマスクによる防御対象サーバのIPアドレス指定することはできない．さらに，ネットマスクで防御対象サーバのIPアドレスを指定できないということは，新しく防御対象サーバを導入する際にシステムの設定を変更しなければならない．本研究では，防御対象サーバのIPアドレスをネットマスク単位で指定できるため防御対象サーバを追加で導入する際，システムに防御対象サーバのIPアドレスを新たに指定せず導入できる．

よって，本研究はソニックウォール社のIPSとsyslogサーバより防御対象サーバを柔軟に指定することができ，新しくサーバを導入するのが容易であるといえる．

**防御対象サーバの設定変更不要**

ソニックウォール社のIPSでは，防御対象サーバへのパケットを監視し不正アクセスや攻撃を検知するため防御対象サーバへの設定変更は不要である．syslogサーバを用いた防御システムでは，防御対象サーバにSSHのアクセスログをsyslogサーバに転送するなどの設定変更が必要である．本研究では，防御対象サーバへのセッション情報を監視し，Brute Force攻撃を検知するため防御対象サーバへの設定変更は不要である．

よって，本研究とソニックウォール社のIPSは防御対象サーバの設定を変更せず導入が可能であるといえる．

**関連システムと本研究の比較評価のまとめ**

関連システムと本研究の比較評価のまとめをおこなう．Brute Force攻撃の検知するしくみ，Brute Force攻撃を防御，ネットマスクによる防御対象サーバのIPアドレス指定，防御対象サーバの設定変更不要の項目で関連システムと本研究の比較評価を表5に示す．提案システムはネットマスクにより防御対象サーバのIPアドレスを指定できる点と防御対象サーバの設定を変更せず導入できる点で有用性があるといえる．Source Quenchによる防御手法は実験中1件の攻撃者からの攻撃を防御できなかったため，全ての攻撃を防御できたルーティングによる防御手法の方が有用性があるといえる．

| | Brute Force攻撃の検知 | Brute Force攻撃の防御 | ネットマスクによる防御サーバのIPアドレス指定 | 防御サーバの設定変更不要 |
|---|---|---|---|---|
| IPS(ソニックウォール社) | × | ○ | × | ○ |
| syslogサーバによる防御システム | ○ | ○ | × | × |
| ルーティングによる防御手法 | ○ | ○ | ○ | ○ |
| Source Quenchによる防御手法 | ○ | △ | ○ | ○ |

表５　関連システムと本研究の比較評価のまとめ

### 6.3　今後の課題

#### 6.3.1　検知できなかった事例に対応

実験中に提案システムの1分間での閾値を超えずBrute Force攻撃を続けていた攻撃者がいた．提案システムではセッション数が20以上の送信元を攻撃者として検知している．そのため間隔をあけて攻撃するBrute Force攻撃は検知できないという問題点が明らかになった．さらに，攻撃を検知する前の1分間で200回以上のBrute Force攻撃をしてきた攻撃者もいることが確認できた．よって，Brute Force攻撃の検知する時間を短縮し，または延長することで検知できなかったBrute Force攻撃を検知できるようにする必要がある．

#### 6.3.2　ネットワーク内の設置場所による評価

和歌山大学のあるサーバの上位に提案システムを設置し実験をおこなった．今後和歌山大学の外部ネットワークとの境界に設置することで，学内ネットワークを全て防御対象にすることができる．境界に設置することで，実験時より多くのパケットをキャプチャ，セッション情報を格納し攻撃者を検知するので，様々な検証を実施する必要がある．

## 7．おわりに

本研究では，既存研究にBrute Force攻撃を検知，防御する手法を提案した．本研究を用いて実際に攻撃されている環境での実験によりBrute Force攻撃を検知し防御できることが確認できた．今後はBrute Force攻撃を検知する時間を短縮，または延長することで検知できなかった攻撃を検知できるようにする予定である．

## 参考文献


[1] 有限責任中間法人JPCERTコーディネーションセンター”インターネットセキュリティに対するJPCERT/CC 2005 年第3 四半期活動報告”
www.jpcert.or.jp/press/2005/1107.pdf
[2] 独立行政法人情報処理推進機構（IPA）“ サービス妨害攻撃の対策等調査- 報告書- ”
http://www.ipa.go.jp/security/fy22/reports/isec-dos/2010_isec_dos.pdf
[3] 警視庁，“ DoS/DDoS対策について”
http://www.npa.go.jp/cyberpolice/server/rd_env/pdf/DDoS_Inspection.pdf
[4] 金森励起，元木伸宏，川橋裕，塚田晃司，“ ソースアドレスルーティングによるトラフィック管理システム”電子情報通信学会技術研究報告，IN，情報ネットワーク108(342)，25-30，2008-12-04
[5] 澤和晃，“ トラフィック監視によるホスト・サービス単位の境界型ネットワーク防御システムの構築”2010年度和歌山大学卒業論文
[6] 羽場　賢，”DoS攻撃に対する透過型防御システムの構築とステートレスなTCP 代理応答の評価”2011 年度和歌山大学卒業論文
[7] ” INTERNET CONTROL MESSAGE PROTOCOL ”
ftp://ftp.rfc-editor.org/in-notes/rfc792.txt
[8] FreeBSD System Manager’s Manual，” IPFW ”
http://www.freebsd.org/cgi/man.cgi?query=ipfw%20
[9] 石黒邦弘，“ GNU Zebra ” http://www.zebra.org/
[10] ソニックウォール社
http://www.sonicwall.com/japan/
[11] 大隅淑弘，山井成良，”ホスト間連携を可能にするパスワード総当り攻撃対策手法”情報処理学会研究報告. DSM，[分散システム/インターネット運用技術]2007(93)，49-54，2007-09-21