SSHパスワードクラッキング検知システムとその遮断の効果について

小刀稱 知哉[1]　天本 大地[2,†1]　池部 実[2]　吉田 和幸[3]

概要：インターネットの普及に伴い，ネットワークを通して様々な情報がやり取りされている．そのため現在では，ネットワークは社会的基盤の一つとして生活に不可欠な存在になっている．しかし，ネットワークを利用した不正通信も多く存在する．不正通信の中でも，SSH のパスワード認証に対する総当たり攻撃や辞書攻撃への対策は重要である．我々は，22 番ポートの TCP コネクションの接続状態を監視し，各コネクションの確立から，終了までのパケット送受信回数の少ないコネクション数を検出することで，SSH パスワードクラッキング攻撃を検知する「SSH パスワードクラッキング攻撃検知システム」を開発した．また，学内の SSH サーバから，検知した攻撃者 IP アドレスへ送信するパケットを破棄することで SSH サーバと攻撃者との通信を遮断する．
我々は，攻撃者との通信の遮断の有無によりシステムを 2 つの期間運用し，それぞれの期間の 1 つの送信元ホストあたりのパスワードクラッキング攻撃検知回数や遮断中の送信パケット数などを調査した．その結果，攻撃者との通信を遮断する場合では，1 つの送信元ホストあたりのパスワードクラッキング攻撃の検知回数が，遮断をしない場合に比べ約 4 分の 1 に減少していた．しかし，20 件中 10 件の攻撃者が，遮断中も SSH サーバにパケットを送信し，遮断解除後 180 秒以内に再びパスワードクラッキング攻撃を仕掛けてきていた．

Development of a detection system for the SSH password crack attacks and its operational results

Tomoya Kotone[1]　Daichi Amamoto[2,†1]　Minoru Ikebe[2]　Kazuyuki Yoshida[3]

1. はじめに

インターネットの普及に伴い，ネットワークを通して様々な情報がやり取りされている．Web ページの閲覧や電子メールなどのコミュニケーション手段に留まらず，インターネット上での行政手続やクレジットカード番号を利用した電子決済など公共性の高いサービスも提供されている．そのため現在では，ネットワークは社会的基盤の一つとして生活に不可欠な存在になっている．しかし，ネットワークを利用した不正通信も多く存在する．それは，プログラムの脆弱性を利用した攻撃や，ネットワークやホストの存在を探索 (スキャン) する攻撃など様々な脅威が存在する．我々が開発した scan 攻撃や DoS 攻撃を検知する「不正通信検知システム [1]」における運用データから，TCP では，学内ネットワークの 3389 番ポート (RDP)，1433 番ポート (SQL over TCP), 22 番ポート (SSH) に対する scan 攻撃が多いことが判明している．これは，学内に上記のポート番号が利用しているサービスが動作しているホストを探索していると考えられる．攻撃者は scan 攻撃後，反応のあった学内ホストにパスワードクラッキング攻撃や DoS 攻撃などを仕掛ける可能性がある．大分大学では，3389 番，1433 番ポートは学内のファイアウォールにより学外からのアクセスはすべて遮断している．一方，22 番ポートは一部のサ

[1] 大分大学大学院工学研究科知能情報システム工学専攻
Course of Computer Science and Intelligent Systems, Graduate School of Engineering, Oita University
[2] 大分大学工学部知能情報システム工学科
Department of Computer Science and Intelligent Systems, Faculty of Engineering, Oita University
[3] 大分大学学術情報拠点情報基盤センター
Center for Academic Information and Library Services, Oita University
[†1] 現在，株式会社アルファシステムズ

ブネットに対しては、ファイアウォールにより遮断していないため，実際に 22 番ポートへの scan 攻撃やパスワードクラッキング攻撃が観測されている．よって，22 番ポートへの攻撃の監視は重要である．

また，SSH の認証方式にはパスワード認証方式と公開鍵認証方式の 2 種類が存在する．パスワード認証方式は，ログイン時に SSH サーバ側のパスワードを入力する認証方式であり，攻撃者にパスワードを入手されると SSH サーバに不正侵入される．よって，ログイン時に SSH クライアント側の公開鍵と秘密鍵を用いて認証する公開鍵認証方式がより安全であるが，認証方式の設定は SSH サーバの管理者が独自で設定するため，ネットワーク管理者がすべての SSH サーバの認証方式を強制することは困難である．

そこで我々は，SSH サーバへのパスワードクラッキング攻撃の検知を目的として「SSH パスワードクラッキング攻撃検知システム」を開発した．本システムは，22 番ポートの TCP コネクションの接続状態を監視し，各コネクションの確立から，終了までのパケット送受信回数の少ないコネクション数を検出することで，SSH パスワードクラッキング攻撃を検知する．また，学内の SSH サーバから，検知した攻撃者 IP アドレスへ送信するパケットを破棄することで SSH サーバと攻撃者との通信を遮断する．

第 2 章では，SSH パスワードクラッキング攻撃の検知に関する関連研究について述べる．第 3 章では，我々が開発している SSH パスワードクラッキング攻撃検知システムのシステム構成，攻撃者検知アルゴリズム，及び検知基準を述べる．第 4 章では，パスワードクラッキング攻撃検知回数や遮断中のパケット数などを調査し，その結果をもとに，遮断の効果について述べる．第 5 章では，まとめと今後の課題について述べる．

2. 関連研究

SSH サーバへのパスワードクラッキング攻撃を検知するにはアクセスログを監視する手法や，トラフィックを解析する手法がある．

アクセスログを監視する手法として，大隅ら [2] はホスト間連携による攻撃対策手法を提案した．これは，組織内で 1 つの syslog サーバを運用し，組織内に存在する各 SSH サーバのアクセスログを収集して監視する．アクセスログには sshd のアクセスログファイルである/var/log/secure を利用し，パスワード認証に失敗したログを抽出する．syslog サーバでは，各 SSH サーバから収集したアクセスログをもとに，単位時間あたりのパスワード認証エラーとなった回数がしきい値を越えた送信元ホストを攻撃者として検知する．攻撃者を検知すると，syslog サーバが攻撃者 IP アドレスを組織内の各 SSH サーバに通知し，それぞれで攻撃者 IP アドレスとの接続を拒否するなどの対策を講じる．また，syslog サーバは，組織内の各 SSH サーバからのアクセスログを集めて監視し，攻撃者を検知するため，まだ攻撃を受けていない SSH サーバも未然に攻撃を防ぐことが可能になる．しかし，上記の手法は組織内の全 SSH サーバを把握し，そのアクセスログを監視する必要がある．また，上記のシステムでは組織内の各 SSH サーバからのアクセスログを監視し，検知する．よって，組織内でボットに感染したホストが，組織内からインターネットへパスワードクラッキング攻撃を仕掛けている場合，そのホストを発見することは困難である．

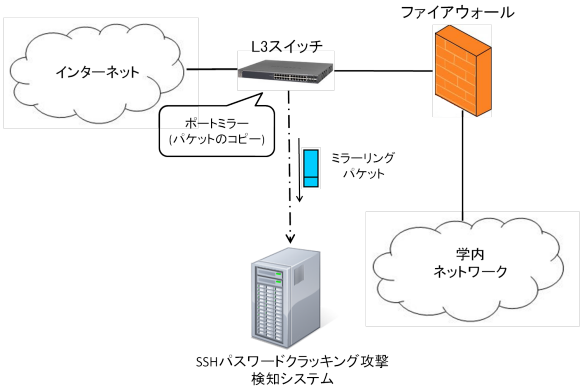


図 1 システムの構成図

また，トラフィックを解析して SSH パスワードクラッキング攻撃を検知するには Laurens ら [3] が提案した手法が挙げられる．scan 攻撃の場合は 1 コネクションあたりのパケット数が少ないが，単位時間あたりのコネクション数は多い．一方，パスワードクラッキングの場合は 1 コネクションあたりのパケット数が，scan 攻撃時に比べ多くなるが，単位時間あたりのコネクション数は少なくなる．以上から，SSH サーバと送信元との間の 1 コネクションあたりのパケット数や単位時間あたりのコネクション数を監視することで scan 攻撃やパスワードクラッキング攻撃をリアルタイムに検知する．しかし，上記の手法は単位時間ごとのコネクション数を計測しているため，単位時間以上の間隔でパスワードクラッキング攻撃が仕掛けれた場合は検知が困難である．

3. SSH パスワードクラッキング検知検知システム

3.1 システム構成

我々が開発している SSH パスワードクラッキング攻撃検知システムは，インターネットから学内ネットワークへ送信されるインバウンドパケット，または学内ネットワークからインターネットへ送信されるアウトバウンドパケットの中から，22 番ポート (SSH) に関する TCP コネクションの接続状態を監視する (図 1)．そして，各コネクションの確立から，終了までのパケット送受信回数の少ないコネクション数を検出することで，リアルタイムに SSH パス

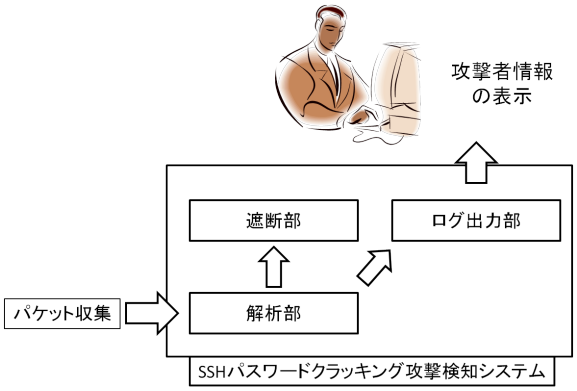


図 2　システムの内部構成図

ワードクラッキング攻撃を検知することを目的としている．また，学内・インターネット間に流れるパケットを取得するため，パスワードクラッキング攻撃を仕掛けた攻撃者が学外に存在する場合と学内に存在する場合のどちらも検知可能である．

本システムは図 2 に示す 3 つのコンポーネント「解析部」「遮断部」「ログ出力部」から構成されている．

以下では，パケット収集とそれぞれのコンポーネント，さらにパスワード攻撃検知アルゴリズムと検知基準について述べる．

3.2　パケット収集

本システムはインターネットから学内ネットワークへ流れるパケット，または学内ネットワークからインターネットへ流れるパケットのうち，22 番ポート (SSH) に関するパケットを tcpdump[4] を用いて収集する．

本システムは，インターネットと学内ネットワークの間に存在するファイアウォールの外側に位置する L3 スイッチからポートミラーしたパケットを収集している (図 1)．

3.3　解析部

解析部では収集されたパケットの IP ヘッダ，TCP ヘッダ情報から送信元 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，TCP フラグの 5 つのデータを抽出し，パスワードクラッキング攻撃かどうか判定する．パスワードクラッキング攻撃の検知アルゴリズムについては以下で述べる．

3.4　パスワードクラッキング攻撃検知アルゴリズム

本システムは，SSH の 1 コネクションあたりのパケット送受信回数から攻撃者を判定する．SSH の通信において，一般ユーザはユーザ認証プロセス後にデータの送受信などを開始するため，1 コネクションあたりのパケット送受信回数が多くなりやすい．一方，攻撃者はブルートフォース攻撃や辞書攻撃によって何度もユーザ認証のプロセスを繰り返すことになる．しかし，SSH サーバでは一定回数以上

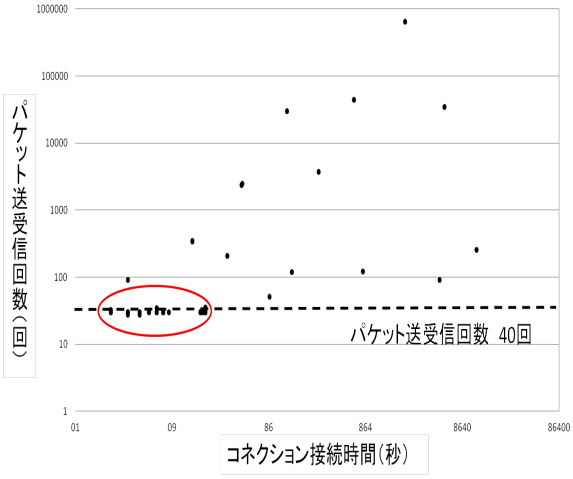


図 3　1 コネクションあたりのパケット送受信回数

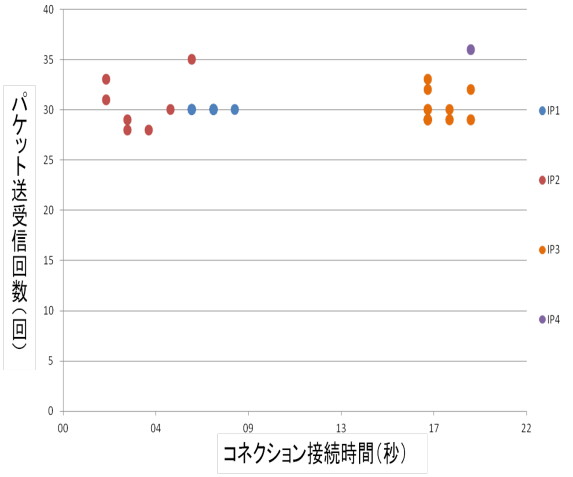


図 4　パケット送受信回数が 40 回以下の SSH コネクション

(通常は 3 回程度) パスワード認証に失敗した場合，クライアントとの TCP コネクションを切断する．このため，攻撃者の 1 コネクションあたりのパケット送受信回数は少なく，また SSH サーバと TCP コネクションを確立する回数が非常に多くなると考えられる．

我々は先行研究 [5] により，学内ネットワークの SSH サーバと外部ホストとの通信を調査し，1 コネクションあたりのパケット送受信回数を集計した．また，本システムで定義している 1 コネクションあたりのパケット数とは，送信元が SYN パケットを送信後，送信元と SSH サーバとの間で最初の FIN パケットまたは，RST パケットが観測されるまでのパケット数である．調査結果を図 3 に示す．図 3 の中で各コネクションの挙動について調査した結果，攻撃者と推測される挙動の通信は，パケット送受信回数が全て 40 回以下の通信であった．図 4 にパケット送受信回数が 40 回以下の通信を抜き出して示す．図 4 では，IP1 が 74 回，IP2 が 7 回，IP3 が 38 回，IP4 が 1 回の通信をしていた．IP1，IP2，IP3 の通信に関しては短期間の間に何度もユーザ認証を試みていると推測される挙動であったた

```
#configure terminal
#ip route 192.0.2.30 255.255.255.255 133.37.A.B
#ip route 192.168.51.100.1 255.255.255.255 133.37.A.B
#ip route 203.0.113.3 255.255.255.255 133.37.A.B
#exit
```

図 5　静的経路の登録例

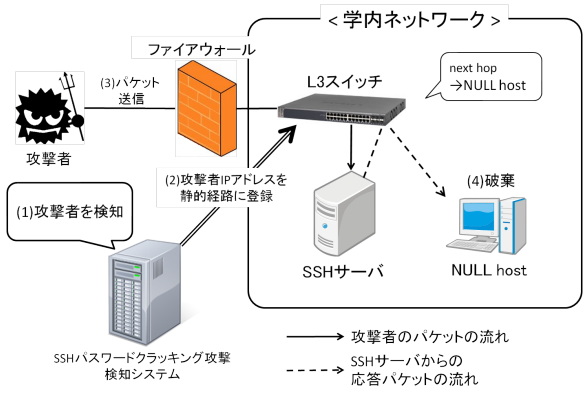


図 6　攻撃パケット遮断の流れ

め，パスワードクラッキング攻撃による通信と判断した．しかし，IP4 の通信はパケット送受信回数が 40 回以下であったのは 1 回だけであり，以降の通信ではパケット送受信回数が 40 回を大きく超える通信が何度も確認された．そのため，この IP4 の通信は一般ユーザによるパスワードの入力ミスであると考えられる．

以上から，パスワードクラッキング攻撃を検知するためのしきい値を，1 コネクションあたりのパケット送受信回数が 45 回以下の場合と定めた．また，一般ユーザによるパスワードの入力ミスがパスワードクラッキング攻撃として検知され，送信元ホストが攻撃者と誤検知することを防ぐため，パケット送受信回数が 45 回以下のコネクションを 10 回連続して観測した時点で，送信元ホストを攻撃者として検知する．

3.5　遮断部

遮断部では，SSH サーバから攻撃者 IP アドレスへ送信される戻りのパケットを学内の特定ホスト (以下 NULL ホスト) 宛への静的経路を登録することで攻撃者との通信を遮断する．図 5 に静的経路の登録例を，図 6 に攻撃パケット遮断の流れを示す．

(1) 本システムが攻撃者を検知すると，
(2) 学内ネットワークの L3 スイッチへ攻撃者 IP アドレスの next hop を NULL ホスト (図 5 の 133.37.A.B) とする静的経路を登録する．登録した経路情報は OSPF により学内の各ルータへ配布する．
(3) 次に，攻撃者からパケットが送信されると
(4) SSH サーバからの応答パケットはすべて NULL ホストへ転送される．

以上の手順により，攻撃者と SSH サーバとの通信を遮断する．

表 1　コネクションの判定結果

判定結果	説明
SUCCESS-CLOSE	1 コネクションのパケット送受信回数がしきい値以上 (FIN パケットによりコネクションが終了した)
SUCCESS-ILLEGAL	1 コネクションのパケット送受信回数がしきい値以上 (RST パケットによりコネクションが終了した)
FALSE-CLOSE	1 コネクションのパケット送受信回数がしきい値未満 (FIN パケットによりコネクションが終了した)
FALSE-ILLEGAL	1 コネクションのパケット送受信回数がしきい値未満 (RST パケットによりコネクションが終了した)

3.6　ログ出力部

ログ出力部では，解析部によりパスワードクラッキング攻撃と判定されたホストに関する情報を「攻撃者ログ」として出力し，管理者に提示する．その他にも，1 コネクションあたりのパケット送受信回数がしきい値以上の場合のコネクション情報を格納する「正規通信ログ」，しきい値未満の場合のコネクション情報を格納する「非正規通信ログ」もそれぞれ保持している．非正規通信ログには攻撃者がパスワードクラッキング攻撃を仕掛けた場合と正規ユーザがパスワード入力ミスをした場合の 2 種類が含まれる．攻撃ログの書式と実際の攻撃ログをそれぞれ図 7 と図 8 に示す．コネクションの判定結果の一覧を表 1 に示す．1 コネクションのパケット送受信回数がしきい値以上の場合は SUCCESS，しきい値未満の場合は FALSE と定義する．また，コネクション終了時のパケットが FIN の場合は CLOSE，RST の場合は ILLEGAL と定義する．

4.　システム運用結果

4.1　設置環境

以下に SSH パスワードクラッキング検知システムが動作している環境を示す．

- OS : Red Hat Enterprise Linux Server release 5.5
- CPU : Intel(R) Xeon(TM) CPU E5620 2.40GHz (4 cores, 8 threads) × 2
- メモリ : DDR3 1066MHz 12GByte

今回遮断は，Alaxala AX3640S-24T2XW にて実施した．また，登録する静的経路の上限数は 7,500 件に設定した．これは学内 LAN の L3 スイッチの最大経路数を考慮したためである．

また，今回の実験では攻撃者が検知されると，本システムが攻撃者と SSH サーバとの通信を遮断する．その後，180 秒経過経過すると，通信の遮断を解除する．しかし，攻撃者検知後の経過時間を判定するハンドラが 60 秒毎に起動するため，実際には 180 秒から 240 秒の間に遮断が解除される．

[検知時刻] [パケット数] [src IP addr] [src port] -> [dst IP addr] [ISN] [コネクション状態] [対象コネクション中の最終パケット到着時刻]

図 7 攻撃者ログの書式

```
2013 04/18 18:10:14 43 188.190.X.Y 63507 -> 133.37.C.D 1895279705 FALSE 2013 04/18 18:08:20
2013 04/18 18:10:14 44 188.190.X.Y 63561 -> 133.37.C.D 1196371905 FALSE 2013 04/18 18:08:20
2013 04/18 18:10:14 43 188.190.X.Y 65149 -> 133.37.C.D 4978768343 FALSE 2013 04/18 18:08:47
2013 04/18 18:10:14 42 188.190.X.Y 65202 -> 133.37.C.D 3441215005 FALSE 2013 04/18 18:08:48
2013 04/18 18:10:14 41 188.190.X.Y 10910 -> 133.37.C.D 2395673895 FALSE 2013 04/18 18:09:15
2013 04/18 18:10:14 42 188.190.X.Y 10934 -> 133.37.C.D 2510168308 FALSE 2013 04/18 18:09:16
2013 04/18 18:10:14 42 188.190.X.Y 12359 -> 133.37.C.D 3084294630 FALSE 2013 04/18 18:09:44
2013 04/18 18:10:14 41 188.190.X.Y 12400 -> 133.37.C.D 2503339015 FALSE 2013 04/18 18:09:46
2013 04/18 18:10:14 41 188.190.X.Y 13734 -> 133.37.C.D 1615811561 FALSE 2013 04/18 18:10:12
2013 04/18 18:10:14 39 188.190.X.Y 13856 -> 133.37.C.D 1513560304 FALSE 2013 04/18 18:10:14
```

図 8 攻撃者ログ

表 2 総攻撃記者検知数 (約 8 日間)

	検知件数 (件)	
	遮断無	遮断有
総攻撃検知数	139	81

表 3 SSH クライアント検知数 (約 8 日間)

	検知件数 (件)	
	遮断無	遮断有
検知攻撃者数	28	20
一般ユーザ検知数	37	33
重複検知数	3	5

表 4 SSH サーバに対する通信件数 (約 8 日間)

	通信件数 (件)	
	遮断無	遮断有
攻撃件数	6,511	1,072
正規通信件数	965	429

4.2 運用期間

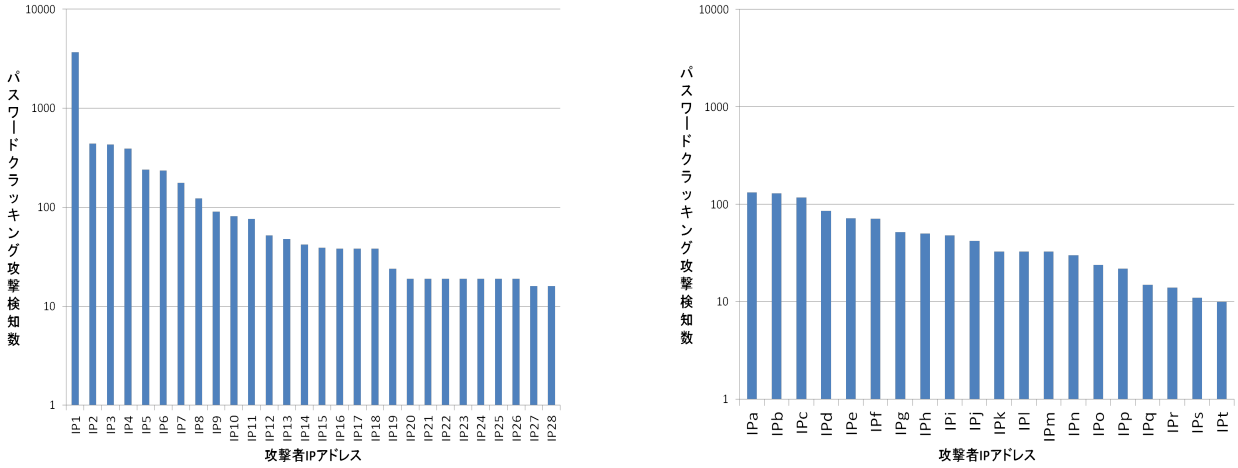
今回，遮断の効果を検証するため，攻撃者を検知した後，攻撃者と SSH サーバ間の通信を遮断しない場合とする場合の 2 つの期間，システムを運用した．遮断なし場合の運用期間は 2013 年 4 月 1 日 7 時 45 分から 2013 年 4 月 7 日 22 時 9 分の約 7 日間である．一方，遮断あり場合運用期間は 2013 年 4 月 18 日 8 時 29 分から 2013 年 4 月 25 日 14 時 15 分の約 7 日間である．また，攻撃者が送信したパケットを詳細に調査するため，同期間のシステムの入力となっているパケットデータを tcpdump により保存した．

4.3 運用結果

2 つの運用期間中に本システムが検知した総攻撃者検知数を表 2 に，SSH クライアント数の総計を表 3 に示す．遮断なし，ありの場合のそれぞれの運用期間中の総攻撃検知数は 139 件，81 件であった．同一送信元ホストが複数回攻撃者として検知することがあるため，本システムが検知した異なる攻撃者 (IP アドレス) 数はそれぞれ 28 件，20 件であった．また，表 3 内の重複検知した送信元ホストとは，攻撃者ログと正規通信ログの双方のログで共に検知されたユーザである．これは現在のしきい値は，SSH サーバが 1 コネクション中に 3 回パスワード認証を要求する場合を想定した値であるが，SSH サーバの設定により，1 コネクションあたり 3 回以上のパスワード認証を行う場合が存在する．この場合，1 コネクションあたりのパケット数が現在のしきい値を超過することがある．よって，送信元ホストが複数の SSH サーバにパスワードクラッキング攻撃を仕掛けた際，SSH サーバの設定により，1 コネクションあたりのパケット送受信回数が検知基準以下の通信と検知基準をわずかに超過した通信の 2 種類の通信が観測され，重複検知が発生したと考えられる．

4.4 遮断の効果

図 9 に 2 つの運用期間中に，本システムが検知した，各送信元ごとのパスワードクラッキング攻撃の回数を，検知数が少ない送信元から示す．遮断無しの場合，1 つの送信元から最大で 3,681 回のパスワードクラッキング攻撃を検知した．一方，遮断有りの場合，1 つの送信元から観測されたパスワードクラッキング攻撃の検知数は最大で 132 件である．また，1 つの送信元からのパスワードクラッキング攻撃検知回数の平均は遮断無しの場合は 230 件，遮断有りの場合は 51 件であり，遮断有りの場合は無しの場合と比較して，パスワードクラッキング攻撃の検知回数が約 4 分の 1 に減少している．



(a) 遮断無　　(b) 遮断有

図 9　送信元 IP アドレスごとのパスワードクラッキング攻撃検知回数

また，今回 2 つの運用期間中に，同一送信元ホストからパスワードクラッキング攻撃が観測された．この送信元ホストの 2 つの期間において，最初のパスワードクラッキング攻撃を検知した後の経過時間と検知回数を図 10 に示す．遮断無しの場合は 720 秒間で合計 69 回のパスワードクラッキング攻撃を仕掛け，攻撃が終了していた．一方，遮断有りの場合は 10 回パスワードクラッキング攻撃を検知した後，本システムにより SSH サーバとの通信を遮断されたため，約 180 秒間パスワードクラッキング攻撃が観測されなかった．しかし，遮断解除後，再びパスワードクラッキング攻撃が 10 回観測したため，再度攻撃者として検知され，通信を遮断した．2 度目の遮断解除後はパスワードクラッキング攻撃は観測されなかった．この間のパスワードクラッキング攻撃の回数は合計で 20 回であり，遮断無しの場合と比較すると，3 分の 1 程度に減少していた．よって，攻撃を検知した時点で SSH サーバと送信元ホストとの通信を遮断することにより，パスワードクラッキングを仕掛ける回数が減少しており，遮断の効果はあったと判断する．

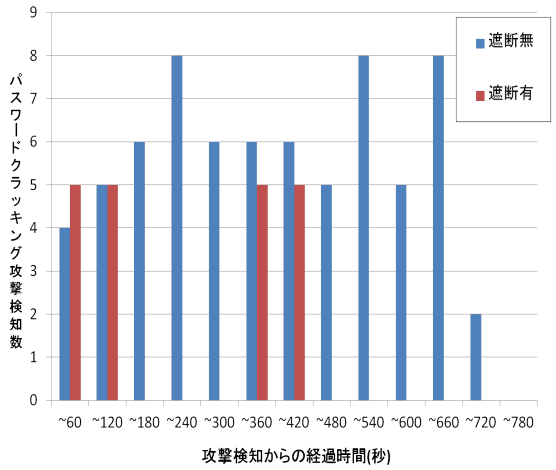


図 10　同一送信元ホストのパスワードクラッキング攻撃検知回数

4.5　遮断中の送信パケット

図 11 にすべての攻撃者が遮断中に送信したパケット数とその割合を示す．攻撃者の遮断中に本システムが観測した全体のパケット数は 11,822 パケットであった．また，全体の約 61%のパケット (7,364 パケット) が攻撃者を検知してから 5 秒以内に観測された．その後，検知後 60 秒以内では，1 秒間に 50〜60 パケット程度観測された．検知後 60 秒以降は，1 秒間に 10〜20 パケット程度観測された．

また，同一攻撃者が短期間に複数回攻撃者として再検知されていた．調査したところ，20 件中 10 件の攻撃者が遮断解除後，180 秒以内に再びパスワードクラッキング攻撃を再検知していた．図 12 に遮断解除後，180 秒以内に再

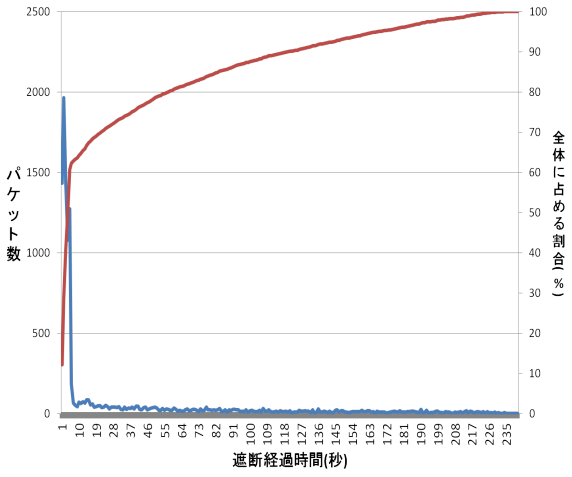


図 11　全体の攻撃者の遮断中の送信パケット数とその割合

びパスワードクラッキング攻撃を再検知した攻撃者 A と，解除後 7 日間以内には再検知しなかった攻撃者 B の，遮断中の送信パケット数を示す．攻撃者 A は遮断中も，一定間隔で SSH サーバへパケットを送信していた．一方，攻

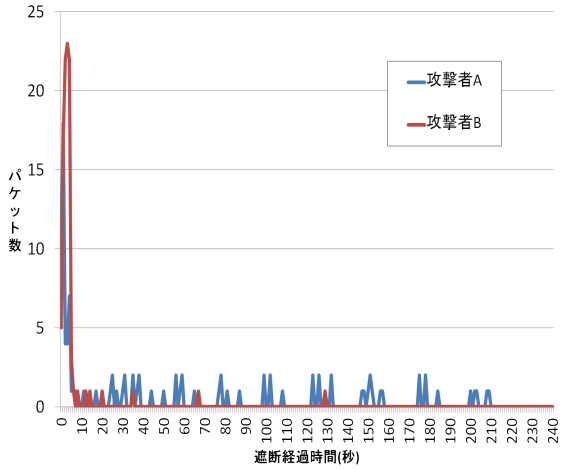


図 12 2 つの攻撃者の遮断中のパケット数

撃者 B は遮断後，8 秒間に 94 パケット送信していた．その後，12 秒，14 秒，20 秒，35 秒，67 秒，129 秒に 1 パケットずつパケットを送信していた．遮断開始後から 129 秒経過後，攻撃者 B からのパケットは観測されていない．tcpdump により攻撃者 A の挙動を調査したところ，遮断後に SSH サーバからの応答がなくなっても，SYN パケットを送信していた．その後，遮断が解除され，SSH サーバからの応答が返ってくると，再びパスワードクラッキング攻撃を仕掛けており，攻撃者として再検知していた．よって，現在の通信遮断時間は，攻撃者を検知してから一定時間と設定したが，今回の実験から，通信の遮断中も一定間隔で SYN パケットを送信する攻撃者は，通信の遮断を解除した後，短期間で再びパスワードクラッキング攻撃を仕掛ける可能性があると判明した．そのため，通信の遮断を解除するタイミングを，攻撃者からの送信パケットが観測されなくなってから一定時間経過後と設定することで，より効果的にパスワードクラッキング攻撃を抑制することができるのではないかと考えられる．

5. おわりに

5.1 まとめ

本論文では，攻撃者との通信の遮断の有無により，システムを 2 つの期間運用し，それぞれの期間の 1 つの送信元ホストあたりのパスワードクラッキング攻撃検知回数や遮断中のパケット数などを調査した．その結果，攻撃者との通信を遮断する場合では，1 つの送信元ホストあたりのパスワードクラッキング攻撃の検知回数が，遮断をしない場合に比べ約 4 分の 1 に減少していた．しかし，20 件中 10 件の攻撃者が，遮断中も SSH サーバにパケットを送信し，遮断解除後 180 秒以内にパスワードクラッキング攻撃を仕掛けてきていた．よって，通信の遮断を解除するタイミングを，攻撃者からの送信パケットが観測されなくなってから一定時間経過後と設定することで，より効果的にパスワードクラッキング攻撃を抑制することができるのではないかと考えられる．

5.2 今後の課題

今回の実験で用いた攻撃検知基準は，SSH サーバが 1 コネクション中に 3 回パスワード認証を要求する場合を想定した値である．しかし，SSH サーバの設定により，1 コネクションあたり 3 回以上のパスワード認証を行う場合が存在する．この場合，1 コネクションあたりのパケット数が現在のしきい値を超過し，検知漏れが発生する．よって，今後はしきい値の検討をしていく必要がある．

参考文献

[1] 有馬竜昭, 小埜勇貴, 永山聖希, 吉田和幸：scan 攻撃検知システムの誤検知の調査，インターネットと運用技術シンポジウム 2011 論文集，pp. 45–50 (2011).
[2] 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たり攻撃対策手法，情報処理学会研究報告 2007-DSM-47(9)，pp. 49–54 (2007).
[3] Laurens, H. Luuk, H. Rick, H. Anna, S. Ramin, S. and Aiko, P.: SSHCure: A Flow-Based SSH Intrusion Detection Sytem, *International Conference on Autonomous Infrastructure, Management, and Security, AIMS 2012*, pp. 86–97 (2012).
[4] tcpdump. 入手先 `http://www.tcpdump.org/`.
[5] 天本大地, 小刀祢知哉, 小埜勇貴, 有馬竜昭, 池部実, 吉田和幸：scan 攻撃検知システムを用いた SSH ポートに対する攻撃についての調査，電気関係学会九州支部第 65 回連合大会，pp. 279–279 (2012).