モバイルコードを用いた動的ポートランダマイズド VPN 方式の評価

竹久 達也* 廣友 雅徳** 伊沢 亮一† 森井 昌克** 中尾 康二‡

*ジャパンデータコム株式会社 107-0052 東京都港区赤坂 6-6-28 赤坂カムフィーホームズ 6B
**神戸大学大学院工学研究科 657-8501 神戸市灘区六甲台町 1-1
†株式会社クリプト 105-0014 東京都港区芝 3-2-18-1102
‡独立行政法人情報通信研究機構 184-8759 東京都小金井貫井北町 4-2-1

あらまし 近年，インターネット技術の進歩によりテレワーカーやSOHO事業者などがインターネットを介して各種拠点とリモートアクセスするような広域分散型の社会に移行しつつある．しかし各種サイバー攻撃の数は増え続けており増加の一途であり，サービス提供者および利用者にとって大きな脅威となっている．このような攻撃への対策として着信ポート番号を特定不能にすることが有効である．筆者らはサービスの着信ポート番号を動的に変更するリモートアクセスVPNについて検討し具体的な実装方式を提案した．本稿では筆者らが提案した動的ポートランダマイズドVPN方式の性能を評価することにより有効性を示す．

Evaluation of Dynamic Port Randomized VPN by Mobile Codes

Tatsuya Takehisa*, Masanori Hirotomo**, Ryoichi Isawa†, Masakatu Morii**, Koji Nakao‡

*Security Software R&D Department, Japan Datacom, Co., Ltd.
Akasaka, Comfy Homes 6B 6-6-28 Akasaka, Minato-ku, Tokyo 107-0052, Japan

**Graduate School of Engineering, Kobe University
1-1, Rokkodai, Nada-ku, Kobe-shi, 657-8501 Japan

† Crypto Co., Ltd.,
3-2-18-1101 Shiba, Minato -ku, Tokyo, 105-0014 Japan

‡ National Institute of Information and Communications Technology
4-2-1, Nukui-Kitamachi, Koganei, Tokyo 184-8759, Japan

Abstract Recently, the variety of attacks against servers in the Internet is increased. The survivability of servers serving the remote access VPN is influenced by several cyber attacks. To develop a countermeasure against the attacks, we have proposed a method for the remote access VPN with dynamic port randomization function by mobile codes. In this paper, we evaluate the performance of the dynamic port randomization function embedding the remote access VPN, and show the efficiency of our method.

1 はじめに

近年，インターネット技術の進歩によりテレワークや SOHO 事業者など（利用者）がインターネットを介して各種拠点とリモートアクセスするような広域分散型の社会に移行しつつある．これにより利用者は地理的制約などから解放され，仕事と生活の調和，さまざまな状況に応じた多様で柔軟な働き方が可能となってきている．また，政府が掲げる「テレワーク人口倍増アクションプ

ラン」[1]によりさらなるリモートアクセスを用いた社会環境の実現が行われると予想される.

しかし, インターネット上でサービスを提供するということは各種サイバー攻撃に晒されるということを無視することはできない. 各種サイバー攻撃の数は急速に増加しており, サービスを提供・利用する者にとって脅威となり, 安心・安全な広域分散型社会を実現するための障害となっている. このような安心・安全なリモートアクセスを実現するための技術として Virtual Private Network(VPN)技術がある.

これらの背景を踏まえ, 本研究では各種サイバー攻撃に耐性のあるVPN方式の提案および評価を行い, その有効性を示すことを目標としている. 耐障害性と秘匿性を向上させるためにはサービス拒否(Denial of Service; DoS)攻撃などからサービスを守る必要がある. DoS 攻撃への対策として, サービスの着信ポート番号をランダム化する手法(ポートランダマイゼーション)は攻撃者に対してサービス提供ポート番号を推測しにくくすることが可能であるため, 攻撃者の攻撃確率やモチベーションを低下させることが可能であり, 各種攻撃に対して有効な手法である.

力武らはアプリケーションサービスの着信ポート番号をランダムに変更する方式を与えている[2]. この方式では TCP, UDP 通信のポート番号をパケット毎にランダムに変更することが検討されており, ポート番号のランダム化によってDoS 攻撃への耐性が高められることが示唆され, 概念的な方式の提案が与えられている. 一方, ソフトウエアのみで構成されたポート番号のランダム変更機能を有する方式として, 白石らはモバイルコードを用いた VPN 方式(以下, S-PPVPN と称する)を提案している[3]. S-PPVPN では Java Applet と Java Remote Method Invocation(RMI)で実装されるモバイルコードを用いることで VPN の導入を簡易にしている. さらに白石らは S-PPVPN を VPN サービスの着信ポートをランダム化することによって DoS 攻撃への耐性を付加する方式(以下, S-PRVPN と称する)[4]を提案している. しかし, この方式では通信セッション中でポート番号を変更する機能は実現できておらず, VPN のような長時間セッションが張られるサービスでは各種攻撃への耐性が十分とは言えない. また, IETF Draft ではポートランダマイゼーション方式としてLarsenらの方式が提案されている[5]. しかし, この方式は特定のサービスを対象とした具体的な実装方法を与えているわけではなく, ポート番号をランダム化する概念的な方法が示されているのみである.

以上のように, 力武らの方式, 白石らの S-PRVPN, Larsen らの方式を含めて着信ポート番号をランダムに変更する方式が検討されているが, 攻撃を受けた際にもスループットの低下を抑えられるVPNを実装することは容易ではない. この課題を解決するため, 筆者らはモバイルコードを用いたポート動的変更機能を有する VPN 方式を提案した[6]. この方式は耐障害性, 秘匿性, 利便性を備えたポートランダマイズド VPN 方式であり, その実装方法を具体的に与えている.

本稿ではモバイルコードを用いたポートランダマイズドVPN方式の評価を与える. 本稿で示す評価においてDoS攻撃環境下での通過可能な攻撃パケット数を詳細に評価することにより, 提案方式が耐障害性に関して有効であることを示す.

2 モバイルコード

モバイルコードはクライアントからダウンロードされ実行することを目的として作成された実行ファイルである. 通常はユーザが意識することなく, オンデマンドにダウンロードされ実行される. モバイルコードはその特徴としてモバイルコードのバージョンアップがサーバに登録してあるモバイルコードを更新することでユーザに負荷を与えることなくバージョンアップが行える. よって, モバイルコードにセキュリティ上の脆弱性などが発見された場合, 即座にサーバのモバイルコードを更新することで, 以後クライアントへのサービスを更新することができる. これにより, 新しい

機能をクライアントへ配布する手法としては有用なメカニズムである.

モバイルコードの実装としてはActiveXコントロールによる方式やJava Appletを用いた方式などが存在する.

3 S-PPVPN

現在, VPN 方式として多数の方式が提案されている. これらはVPN装置を利用する方式とソフトウエアによる VPN 方式に分類できる. VPN 装置にて VPNトンネルを提供する場合, 装置の導入など構成する際にいろいろ障害が発生する. また, ソフトウエアによるVPN方式においてもサービス利用者側へのソフトウエアのインストール作業などが必要であり, サービス利用者が簡単に利用できるような方式が少ない. その中でも, SSL-VPN のようにアプレットベースのクライアントソフトウエアをオンデマンドでダウンロードし, VPN トンネルを構成することができる方式も提案されている. SSL-VPN は通常スループット向上などのために VPN 装置にて構成することが多く, 装置購入などサービス提供する上においてサービス利用者側には容易ではあるが, 設備投資や導入時の設定作業などサービス提供者側は簡単にサービス提供することができるとは言えない.

S-PPVPN は, ソフトウエアのみで構成できるVPNとして提案されておりJava AppletとJava Remote Method Invocation(RMI), iptablesなどにより構成し VPN を提供する. SSL-VPNと大きく違うのはJava RMIを用いたinvoke機能を有していることであり, この機能は VPN を提供するサーバ側からサービスを利用するクライアントへ任意の指示を行うことができる. これは, 障害や攻撃などを受けた際に情報を伝達し, それに対応する行動(モバイルコードの切り替えや認証, 通信プロトコルの切り替えなど)が行えるようになる素地となっており, これはモバイルコードの作り込みにおいて自由に行うことができる.

4 S-PRVPN

SSL-VPN や S-PPVPN では, サービスの着信ポート番号が固定されており, 攻撃者がサービスの着信ポート番号を知ると, 容易にターゲット型 DoS 攻撃を行うことができる. そのため S-PRVPN は, 攻撃者から着信ポート番号を推測されないようにするための手法として, サービスの着信ポート番号を乱数化するポートランダマイズド手法を採用している. しかし S-PRVPN は長期間セッションが張られるアプリケーションを実行するようなサービスでは通信セッション中のポートランダマイズは検討されておらず, 通信パケットの傍受やポートスキャンなどを行うことにより着信ポート番号が推測され攻撃される恐れがある.

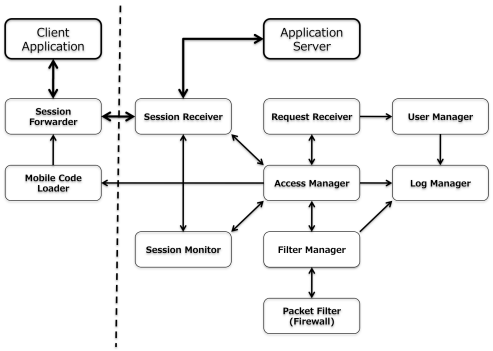

図 1 アーキテクチャ

S-PRVPN のアーキテクチャは 図 1で与えられる. 以降では, その概要を記述する. S-PRVPNでの中核となるモジュールがAccess Manager(AM)であり, 通信セッション, フィルタリング, 認証, ログ機能を AM は集中的に管理する. クライアントとの通信は, モバイルコード側の Session Forwarder(SF)とサーバ側の Session Receiver(SR)間で行われ Session Monitor(SM)により監視される.

S-PRVPN では, Filter Manager(FM)とFirewall(Packet Filter)が密接に連携し, AMからの指示により Firewall のフィルタリングポリシーを動的にその変更することで, ポートランダマイズ手法を付加させている.

5　提案方式

筆者らは各種攻撃に耐性のある VPN 手法として，モバイルコードを用いたポート動的変更機能を有する VPN 方式を提案した[6]．提案方式では長期間セッションを張ったままにするようなアプリケーションを利用する VPN を構築する際，ランダムに着信ポート番号を決定づけることができる．これにより，セッションを動的に別の着信ポート番号のセッションへ切り替え可能となり，長期間の運用時においても各種攻撃への耐性を確保することができる．提案方式ではサービス提供者・利用者双方の負荷が少ないように特別なハードウエア装置を要求することなくソフトウエアのみで実装できるようにしている．

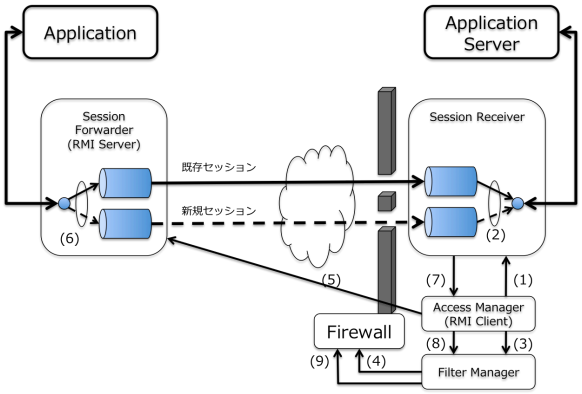

図 2　セッションの切り替え

5.1　セッション切り替え方法

本節では SF, SR のセッション切り替え方法について述べる．図 2は切り替える際に発生するシーケンスを示している．以下で各シーケンスを順に説明する．

(1)後述するポート動的変更アルゴリズムを用いて新規セッションの着信ポートを決定する．(2)指定された着信ポート番号のセッションを生成し，セッションをリッスン状態にする．(3)新規セッションの着信ポートを開く．(4)要求されたポート番号の着信を開始する．(5)RMI を用いて新規セッションの開始を行う．(6)ポート動的変更マイズアルゴリズムを用いて新規セッションのポート番号を決定し，新規セッションを有効にする．既存セッションは破棄する．(7)新規セッションをコネクション完了にする．(8)既存セッションのポートを閉じる．(9)既存セッションのポート番号を遮断する．新規セッションのポート番号に対する TCP の接続要求(SYN フラグ)を無視する．

5.2　ポート動的変更アルゴリズム

本節では各算出方法と必要な事前準備について説明する．

5.2.1　事前準備

サービスを利用するための登録情報のユーザ ID (*ID*)，パスワード (*PW*)，サーバ ID (*SrvIP*)，乱数 SEED (*S*)をセキュアチャネル利用して入手し，時刻は NTP(Network Time Protocol)により同期させておく．

5.2.2　初期接続ポート番号算出

新規セッションの着信ポート番号を算出する方法を説明する．

NTP にて同期した時刻を利用して着信ポート番号を決定する．互いの許容時刻誤差を±30秒とし，双方の時刻のずれを吸収する．

以下の計算を行うことで接続フェーズでの着信ポート番号 P を求め，クライアント側は同様の計算方法で初期接続先のポート番号を得る．

$$TM = HHMMDDhhmmss \geq 30 \rightarrow mm + 1$$
$$RNDSEED(S)$$
$$R_0 = RND()$$
$$P = h(ID \| PW \| TM \| R_0) \bmod (P_{\max} - P_{\min}) + P_{\min}$$

ただし，*HHMMDDhhmmss* は現在の年月日時分秒を表し，*RND* は疑似乱数発生関数を，*RNDSEED* は *RND*()の SEED 値を S として設定することを表す． h は一方向性ハッシュ関数である．$P_{\min}$, $P_{\max}$ はランダマイズするポート範囲を与える． *TM* は接続中保持する．

5.2.3　切り替えポート番号算出

セッション中に動的に切り替えるポート番号を算出する方法は，以下の式にて得る．

$$R_i = RND()$$
$$P = h(ID \| PW \| TM \| R_i) \bmod (P_{\max} - P_{\min}) + P_{\min}$$

iは，切り替える毎に+1 する．

6　評価

本章では提案方式においてDoS攻撃を受けた際の攻撃パケットがサーバへ流入する通過パケット数を計算し，DoS 攻撃に対する耐性を評価する．本評価では，図 3で示す評価モデルを用いて評価する．

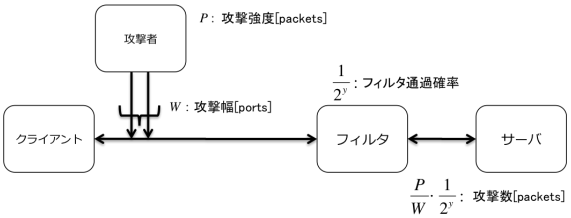

図 3　評価モデル

提案方式は通信セッション中のサーバ側の着信ポート番号をランダムに変更する方式であるため，攻撃者が単一ポートに対して攻撃をおこなった際，ポートランダマイズをしていないサーバと比べDoS攻撃の成功確率が低くなる．

通常，DoS 攻撃を行う攻撃者側の単位時間あたりの攻撃強度（パケット数）はその攻撃者が接続しているインターネット接続回線帯域に左右される．そのため攻撃者の攻撃強度は一定と考えられ，攻撃成功率を高めるために攻撃ポートを分散して攻撃する方式が考えられる．

本評価では，ポートランダマイズを行っているサーバに対して，（1）特定のポート（HTTP:80など）に対しての攻撃，（2）特定のポート範囲をランダムに攻撃した場合の2種類の攻撃に対して評価をおこなった．

ポートランダマイズ方式を用いたサーバのフィルタを通過する事ができるDoS攻撃の成功パケット数は次式で与えられる．

$$\frac{P}{W} \cdot \frac{1}{2^y} \qquad (1)$$

式（1）での P は攻撃者が送信する単位時間あたりの攻撃強度（パケット数），Wは攻撃ポート幅である．P を W で除した値に，$1/2^y$で与えられる確率（y=ランダマイズ範囲）を乗じた値がフィルタを通過する事ができるパケットの数となる．

表 1は式（1）に，Wを1から100に広げた場合，Pを1万から10万パケットにしたときにフィルタを通過することができる攻撃者のパケット数をポートランダマイズ範囲y=4,8,16 で計算した結果である．また図 4～図 6 は上記パラメータで計算した結果をグラフ化したものである．

本評価から，攻撃者の攻撃強度が一定の状態で攻撃ポート範囲を広げる方式は結果として攻撃成功率を$1/W$と減衰させることになり，効果的ではないといえる． またサーバのポートランダマイズ範囲を 2^{16} にすると，攻撃ポート範囲が1で単位時間あたりの攻撃強度が 10 万パケットであっても，4パケットほどしかフィルタを通過することができず，さらに攻撃ポート範囲を 10～100 と広げた場合にはフィルタを攻撃パケットが通過できず DoS 攻撃の影響を受けないといえる．

ポートランダマイズ範囲	攻撃範囲(W)	フィルタを通過する攻撃数 P= 10,000	P= 20,000	P= 100,000
2^4	1	1250.0	3125.0	6250.0
	10	125.0	312.5	625.0
	100	12.5	31.3	62.5
2^8	1	78.1	195.3	390.6
	10	7.8	19.5	39.0
	100	0.8	2.0	3.9
2^{16}	1	0.3	0.8	1.5
	10	0.0	0.1	0.2
	100	0.0	0.0	0.0

表 1 ポートランダマイズ特性

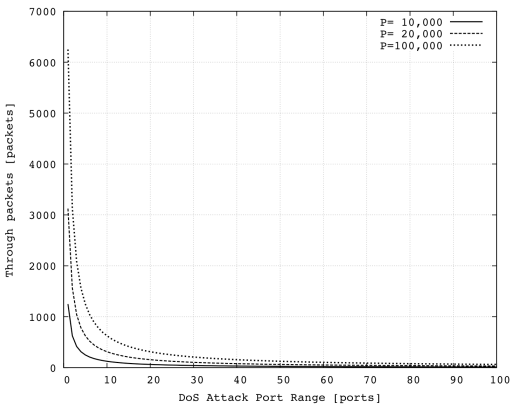

図 4　ポートランダマイズ範囲 2^4 の場合のフィルタを通過する攻撃パケット数

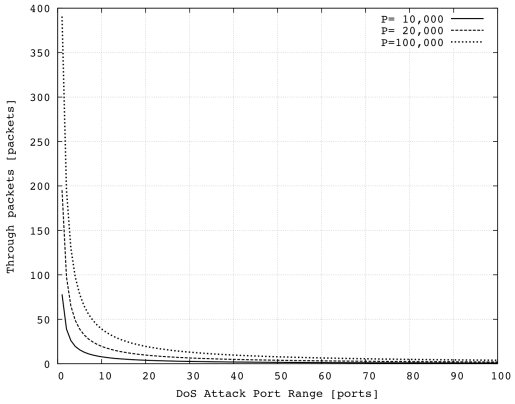

図 5　ポートランダマイズ範囲 2^8 の場合のフィルタを通過する攻撃パケット数

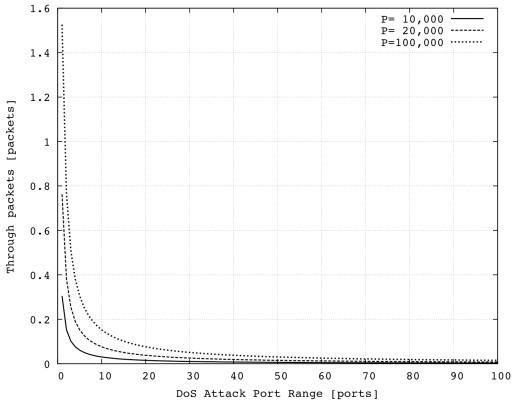

図 6　ポートランダマイズ範囲 2^{16} の場合のフィルタを通過する攻撃パケット数

7　まとめ

本稿では着信ポート番号のランダマイズ化手法の耐障害性に対して評価を行った．その結果，ポートランダマイズ方式を採用しているサーバに対し，攻撃者が攻撃するポートを分散させる方式は効率的ではない．また，ポートランダマイズ範囲を 2^{16} 個にした場合，単位時間あたり 1 万パケットほどの攻撃ではほぼ攻撃パケットからの影響を排除することが可能であることを示した．この結果からも着信ポート番号のランダマイズ化手法の有効性が示される．また，我々が提案している手法を用いることで耐障害性を有する利用者側の事前ソフトウエアインストールなどが不要なソフトウエアのみで構成された VPN システムが構築でき，攻撃手法が進化した場合でもモバイルコードの入れ替えを行うことで対応できる動的に認証・秘匿化手法を更新可能なシステムとして有効であると考える．今後は提案手法を実装し，その性能評価実験を行う予定である．

謝辞

本研究は，独立行政法人 情報通信研究機構の委託研究「インシデント分析の広域化・高速化技術に関する研究開発」の一課題として実施されました．本研究において多くのご意見や助力を頂いた関連・共同プロジェクトの方々に心から謝意を表します．

参考文献

[1] テレワーク推進に関する関係省庁連絡会議,"テレワーク人口倍増アクションプラン",2009.05.29,http://www.kantei.go.jp/jp/singi/it2/dai41/41siryou5.pdf.

[2] 力武健次，菊地高広，永田宏，濱井龍明，浅見徹，“着信ポート番号のランダム化によるサーバー防衛”，情報処理学会研究報告，CSEC，no.124，pp.7-12，Dec. 2001.

[3] Y. Shiraishi, Y. Fukuta, and M. Morii, “Remote Access VPN with Port Protection Function by Mobile Codes,” Proc. the 4th International Workshop on Information Security Applications (WISA2003), LNCS2908, pp.16–26, Jeju island, Korea, Aug. 2003.

[4] Y. Shiraishi, Y. Fukuta, and M. Morii, “Port Randomized VPN by Mobile Codes”,Proc. 2004 IEEE Consumer Communications and Networking Conference (CCNC2004), Las Vegas, Nevada, USA, Jan. 2004.

[5] M. Larsen, F. Gont, "Port Randomization", draft-ietf-tsvwg-port-randomization-04,July 2009, http://tools.ietf.org/html/draft-ietf-tsvwg-port-randomization-04.

[6] 竹久 達也，伊沢 亮一，廣友 雅徳，森井 昌克，中尾 康二，“モバイルコードを用いたポート動的変更機能を有するリモートアクセス VPN 方式，” 信学技報，IA2009-8，pp. 43-48，2009 年 6 月．