DoS 攻撃に対する柔軟なセキュリティ施策に関する考察

2016SE093 山田悟士
指導教員：沢田篤史

1 はじめに

近年，インターネットの発展に伴い，企業や組織のインターネット上でのウェブサイト等の運営や情報の発信，サービスの提供などが増加している．これらのサービスにはインターネット上での行政的な手続きやクレジットカードなどを利用した電子決済など機密性や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，これらのネットワークサービスは社会的基盤の一つとして生活に必要不可欠な存在となっている．

一方で，それらのサービスを提供するための企業や組織のサーバに対して，意図的に大量のアクセスを仕掛け，インターネットサービスの提供を妨害する Denial of Service(DoS) 攻撃や Distributed DoS(DDoS) 攻撃が問題になっている [6]．ネットワークサービスの発展に伴い，DoS や DDoS 攻撃を利用したサイバー攻撃やサイバーテロが今後ますます脅威になってくると予想される．

本研究では，DoS や DDoS 攻撃に対して，攻撃情報に応じて適切な対策を動的に選択するシステムのアーキテクチャを設計することが目的である．

2 DoS 攻撃対策の課題

2.1 現状の対策

一般に DoS や DDoS 攻撃に対する対策方法として 3 つの手法がある [5]．それらについて以下に述べる．

2.1.1 AC(Access Control)

攻撃元の IP アドレスを特定し，ルータなどの通信機器がその IP アドレスからのアクセスを遮断する．

2.1.2 代理応答

攻撃ツールの多くが通信プロトコルに従わないという特徴を利用して，DoS 対策装置などの通信機器が攻撃通信か否か見分け，正当通信のみを保護対象にする．

2.1.3 攻撃対象の避難，隔離

攻撃を受けたサーバやコンピュータをネットワーク管理者がネットワーク構成を変更して，別のネットワークへ避難させ，攻撃の被害をなくす．

2.2 柔軟な対策の必要性

現在，DoS や DDoS 攻撃に対する防御として，AC，代理応答，攻撃対象の避難，隔離の三つの対策が行われている．しかし，それぞれ三つの対策の関係に連動性はなく，個々の機能が独立して動作している．

そこで，提供サービスの重要性や攻撃状況に応じて適切な対策を選択できる必要性がある．近年，攻撃ツールや通信技術の発展により，攻撃がより複雑になってきている．複雑化する攻撃に対して，状況に応じて柔軟に対応する必要がある．

3 DoS 攻撃に対する柔軟な対策切り替え手法

3.1 対策方針

攻撃状況の条件ごとに選択する対策をあらかじめ決めておき，条件にあてはまったとき自動的に対策を切り替える機能を設計する．そのために攻撃状況の条件と対応する対策方法をまとめた攻撃対策表を作成する．攻撃状況の条件を分類する基準は攻撃の強さなどの攻撃情報をもとに設定する．守るべきサーバとして，そのサーバが提供するサービスの種類や可用性が重要か重要ではないかの二つのパターンを想定し，その二つのパターンそれぞれの攻撃対策表を作成する．

3.2 攻撃情報による対策分類

3.3 攻撃条件の基準

攻撃状況の条件を分類する基準として，攻撃のプロトコルの種類，攻撃の強さ，攻撃継続時間，攻撃のソース数，攻撃の時間帯の五つを設定した．これは IDS のログ情報をもとに設定した [3]．攻撃情報から適切な対策を判断する五つの基準をまとめたものを表 1 に示す．

表 1 攻撃条件の分類基準

	変数名	しきい値
プロトコルの種類	p	-
攻撃の強さ (Mbps)	s	s1
攻撃継続時間 (min)	t	t1
攻撃のソース数	n	n1,n2 (n1 < n2)
攻撃時間帯	T	深夜時刻：T1，早朝時刻：T2

3.4 攻撃対策表

表 1 をもとに攻撃状況の条件と対応する対策方法をまとめた攻撃対策表を以下に示す．サーバの種類や可用性が重要である攻撃対策表は表 2, 重要でない攻撃対策表は表 3 である．

4 提案システムのアーキテクチャ

アーキテクチャの設計には Interpreter パターン [1] と PBR パターン [4] を適用した．設計したアーキテクチャを以下図 1，図 2 に示す．図中の各要素について以下に記述する．

- イベントリスト
  攻撃情報を取得し，攻撃状況の変化を検知する．
- Client，判定器
  攻撃情報をもとに対策方法を判定する．

表 2 攻撃対策表：重要な場合

重要	条件 1-1	条件 1-2	条件 2	条件 3	条件 4-1	条件 4-2	条件 5	条件 6	条件 7
プロトコルの種類 p	低レイアプロトコル	高レイアプロトコル	-	-	-	-	-	-	-
強さ s	-	-	s < s1	s > s1	s < s1	s < s1	s > s1	-	s = 0
継続時間 t	-	-	t < t1	t < t1	t > t1	t > t1	t > t1	-	-
ソース数 n	n < n1	n < n1	n1 < n < n2	n1 < n < n2	n1 < n < n2	n1 < n < n2	n1 < n < n2	n > n2	-
攻撃を受けた時間帯 T	-	-	-	-	not T1 < T < T2	T1 < T < T2	-	-	-
選択する対策	代理応答	AC	AC	隔離，避難	隔離，避難	AC	避難，隔離	避難，隔離	無対策

表 3 攻撃対策表：重要でない場合

重要でない	条件 1-1	条件 1-2	条件 2	条件 3-1	条件 3-2	条件 4-1	条件 4-2	条件 5-1	条件 5-2	条件 6	条件 7
プロトコル p	低レイアプロトコル	高レイアプロトコル	-	-	-	-	-	-	-	-	-
強さ s	-	-	s < s1	s > s1	s > s1	s < s1	s < s1	s > s1	s > s1	-	s = 0
継続時間 t	-	-	t < t1	t < t1	t < t1	t > t1	t > t1	t > t1	t > t1	-	-
ソース数 n	n < n1	n < n1	n1 < n < n2	n1 < n < n2	n1 < n < n2	n1 < n < n2	n1 < n < n2	n1 < n < n2	n1 < n < n2	n > n2	-
攻撃を受けた時間帯 T	-	-	-	not T1 < T < T2	T1 < T < T2	not T1 < T < T2	T1 < T < T2	not T1 < T < T2	T1 < T < T2	-	-
選択する対策	代理応答	AC	AC	避難，隔離	AC	避難，隔離	AC	避難，隔離	AC	避難，隔離	無対策

- 対策構成器
  選択した対策方法を構成する．

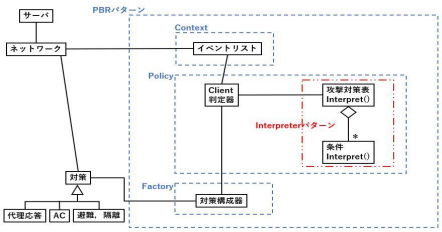

図 1 静的構造

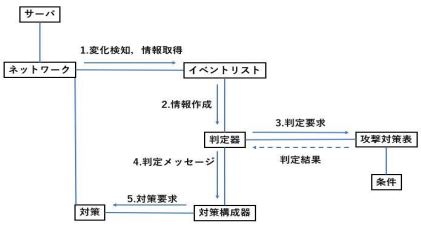

図 2 動的振舞い

5 考察

5.1 提案手法による有用性

本研究で提案した手法を用いることによって，従来攻撃に対して独立的だったそれぞれの対策方法から，サーバの特性や攻撃状況に応じて動的に柔軟に対策する方法へと変更することができる．これにより，従来の対策における柔軟性やリアルタイム性の問題に対処できると考えられる．

5.2 柔軟な対策を可能とするシステムの実現に向けて

5.2.1 SDN(Software Defined Network)

SDN とは，単一のソフトウェアによりネットワーク機器を集中的に制御して，ネットワーク構成や設定などを柔軟に動的に変更することができる技術のことである．

5.2.2 OpenFlow

OpenFlow[2] とは，SDN を実現する技術の 1 つであり，ネットワーク機器を 1 つの制御装置で集中管理して複雑な転送制御を行ったり，柔軟にネットワーク構成を変更できる技術である．この OpenFlow の技術を用いて，柔軟な対策切り替え部分の機能を実現できると考えられる．

6 おわりに

インターネットの発展に伴い，企業や組織のインターネット上でのサービスが増加し，これらは社会的基盤の一つとなっている．一方で，サービスを提供するサーバやネットワークに対して妨害攻撃をする DoS や DDoS 攻撃が問題となっている．攻撃に対する対策としていくつか存在するが，それぞれの対策は独立的で防御としては不十分である．

本研究では，DoS や DDoS 攻撃に対して，提供サービスの重要性や攻撃状況に応じて適切な対策を動的に選択するシステムのアーキテクチャを設計した．

今後の課題としては，設計したアーキテクチャに基づいて実装し，実験を行うことが挙げられる．また，判断基準それぞれのしきい値に具体的な数値の設定をする必要がある．

参考文献

[1] E. Gamma, R. Helm, R. Johnson, and J. M. Vlissides, *Design Patterns: Elements of Reusable Object-Oriented Software*, Addison-Wesley, 1995.

[2] Open Networking Foundation, “ ONF, ” `https://www.opennetworking.org`, 2019.

[3] IPA, “ 侵入検知および侵入防止システム (IDPS) に関するガイド, ” `https://www.ipa.go.jp/files/000025364.pdf`, 2007.

[4] 江坂篤侍, 野呂昌満, 沢田篤史, “ インタラクティブシステムのための共通アーキテクチャの設計, ” コンピュータソフトウェア, vol.35, no.4, pp.3-15, 2018.

[5] 齋藤衛, “ DoS 攻撃：3.1DoS/DDoS 攻撃対策 (1)ISP における DDoS 対策の現状と課題, ”情報処理, vol.54, no.5, pp.468-474, 2013.

[6] 寺田真敏, “ DoS 攻撃：1.DoS/DDoS 攻撃とは, ” 情報処理, vol.54, no.5, pp.428-435, 2013.