Network Security
Firewall

総合情報学科

セキュリティ情報学コース

iptablesの設定例

```
###
# LOGGING
###
iptables -N LOGGING
iptables -A LOGGING -j LOG --log-prefix “DROP: ” -m limit
iptables -A LOGGING -j DROP
iptables -A INPUT -j LOGGING
iptables -A OUTPUT -j LOGGING
```

新table定義

平時は3回/1 hour
Burst時は5回/1 hour

Output tableにLOGGING tableを追加適用

Logging用に新たにtableを定義
それを既存のtableにchainとして付与

Application level firewall (AF)

通信制御/監視機構という意味でFirewall

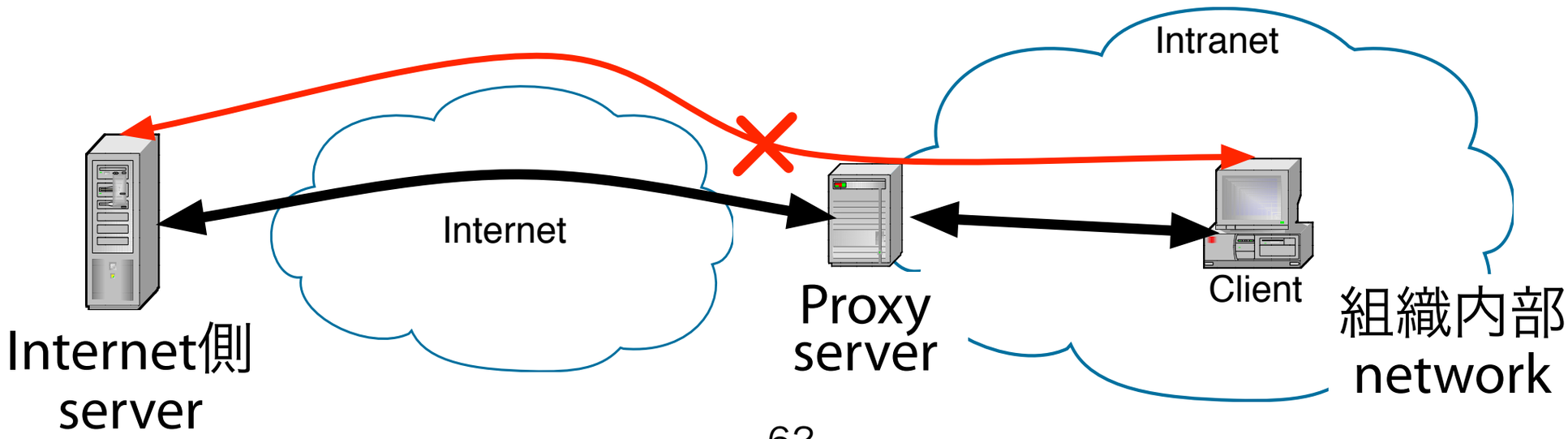
- **Network-based Application Firewall**
  - 例) Proxy server
  - 例) Server-embedded ACL
    (ACL = Access Control List)
- **Host-based Application Firewall**
  - 例) Personal Firewall

Application level firewall (AF)

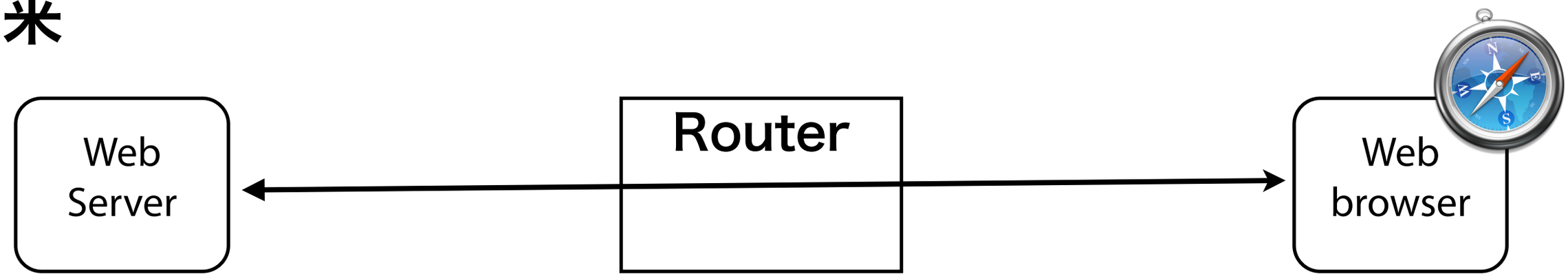
- 利点
  - より詳細な通信制御が可能
    - Applicationレベル(Layer 7)の情報を制御に利用可能
      (= Content filtering: URL, attached file inspection...)
- 欠点:
  - 適用範囲がApp.に限定、App.単位での定義が必要
  - Overheadがかかる

Proxy Server

- 代理サーバ (中継サーバ)
  - Network境界に設置.　内部⇔外部間の通信をRoutingで転送せず、Proxy サーバが「代理」として中継する
    - Intranet内のClientから見るとProxy はServer
    - Internet側のWeb Serverから見るとProxy はClient

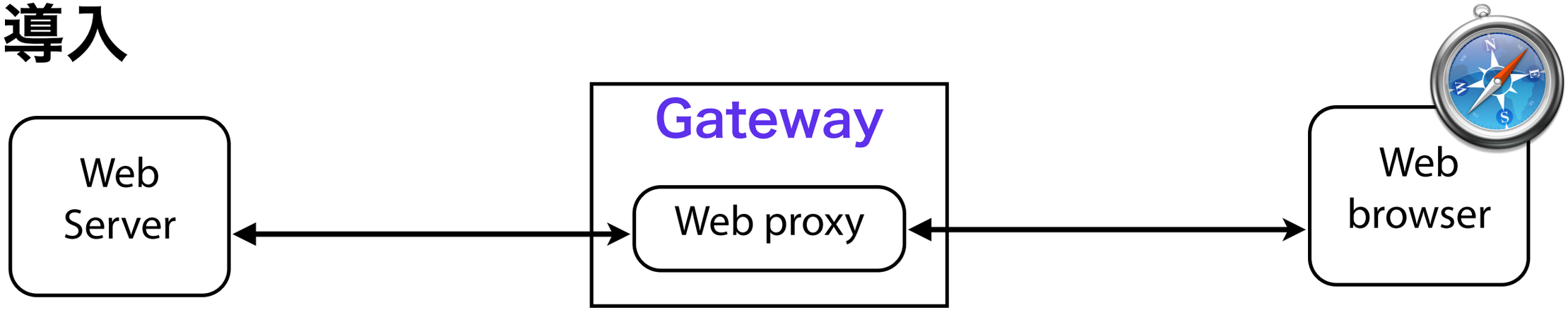


従来



Routerは通信データを**転送**

AF導入



Proxy serverの場合Gatewayは通信データを転送しない
Proxy が 通信データを代理で中継
⇒ 中継処理時に Access Control (アクセス制御)

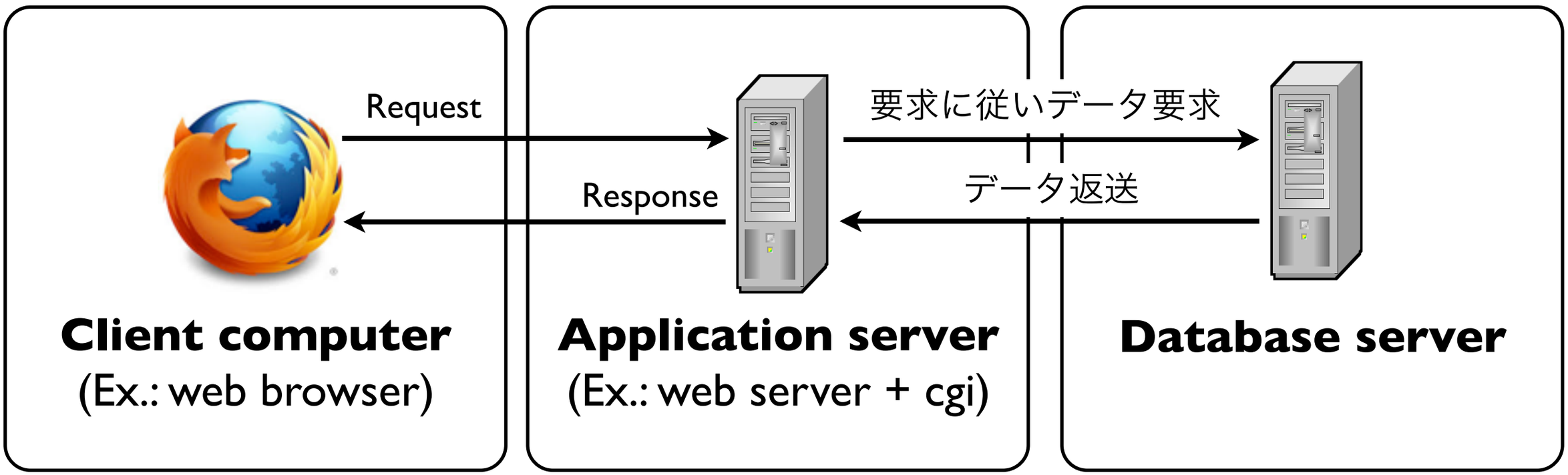
Network-based AFとしての Proxy Server

- 利点: Content Filterが可能
  - Application Layerでの解釈
    ⇒ Application protocolにおける情報を利用可能
    - Web proxyの例：
      http request および http response情報が利用可能
      - domain名, URL, file拡張子, mime_type, protocol, http method(get, post, head), http_status, web browserなど
- 例) SquidAcl, squid-cache wiki, http://wiki.squid-cache.org/SquidFaq/SquidAcl

Acl.= Access Control List

Web application firewall (WAF)

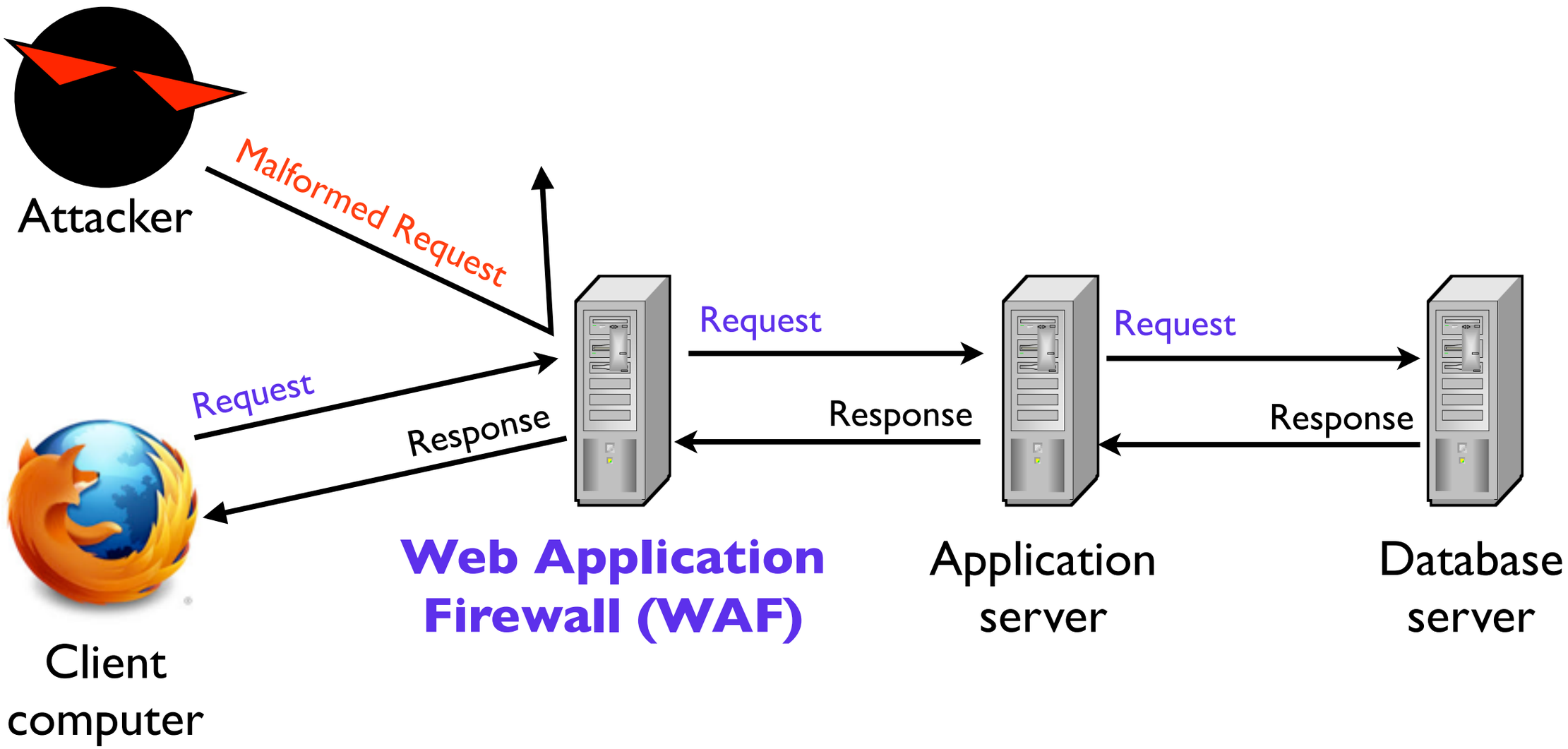
- Webアプリケーションを対象としたApplication Firewall
  - Webアプリの脆弱性を悪用する攻撃からWebアプリを保護
- Webアプリ = 基本は三層構造



Web application firewall (WAF)

- 攻撃者: 不正な要求を作り込み、Databaseを不正に操作
- 本来：正常な要求は想定通りに処理.
  異常な要求はエラーを返すべき.
  が、**そうなっていないアプリ多数**
- **WAF**はこれに対する対策の１つ
  - Client(攻撃者、利用者)から処理要求を検査.
  - 正常な要求のみをWeb アプリケーションサーバに渡す

Web application firewall (WAF)



Webアプリへの要求

Webアプリへの要求 (これで1 request)

http://search.yahoo.co.jp/search?p=%E9%AB%98%E7%94%B0%E7%A0%94%E7%A9%B6%E5%AE%A4%E3%80%80%E9%9B%BB%E6%B0%97%E9%80%9A%E4%BF%A1&aq=-1&oq=&ei=UTF-8&fr=top_lt2_sa&x=wrt

Webアプリへの要求

Webアプリへの要求 (これで1 request)

http://search.yahoo.co.jp/search?p=%E9%AB%98%E7%94%B0%E7%A0%94%E7%A9%B6%E5%AE%A4%E3%80%80%E9%9B%BB%E6%B0%97%E9%80%9A%E4%BF%A1&aq=-1&oq=&ei=UTF-8&fr=top_lt2_sa&x=wrt

Webアプリへのデータ数：？個

Webアプリへの要求

http://search.yahoo.co.jp/search?p=%E9%AB%98%E7%94%B0%E7%A0%94%E7%A9%B6%E5%AE%A4%E3%80%80%E9%9B%BB%E6%B0%97%E9%80%9A%E4%BF%A1&aq=-1&oq=&ei=UTF-8&fr=top_lt2_sa&x=wrt

URL部
　http://search.yahoo.co.jp/search

データ部
　p=%E9%AB%98%E7%94%B0%E7%A0%94%E7%A9%B6%E5%AE%A4%E3%80%80%E9%9B%BB%E6%B0%97%E9%80%9A%E4%BF%A1&aq=-1&oq=&ei=UTF-8&fr=top_lt2_sa&x=wrt

“？”で分割

Webアプリへの要求

データ部

p=%E9%AB%98%E7%94%B0%E7%A0%94%E7%A9%B6%E5%AE%A4%E3%80%80%E9%9B%BB%E6%B0%97%E9%80%9A%E4%BF%A1&aq=-1&oq=&ei=UTF-8&fr=top_lt2_sa&x=wrt

“&”で分割

p　=%E9%AB(以降省略)
aq =-1
oq =
ei　=UTF-8
fr　=top_lt2_sa
x　=wrt

変数名：ei

値：UTF-8

Webアプリへのデータ数：６個

Webアプリへの攻撃

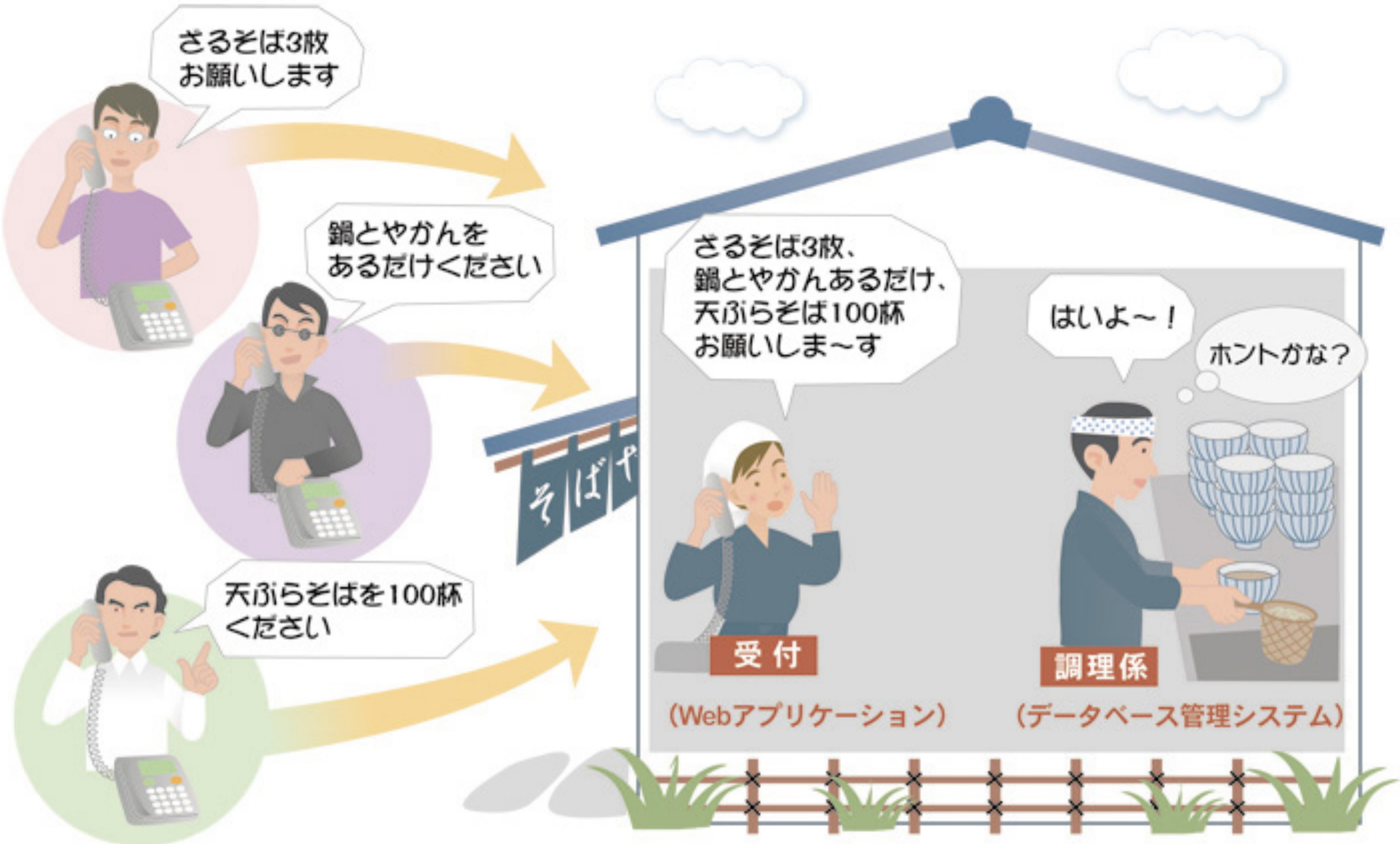
攻撃者はこの変数値に細工を施し
想定外の動作を起こそうと画策する

p　=%E9%AB(以降省略)
aq =-1
oq =
ei　=UTF-8
fr　=top_lt2_sa
x　=wrt

以下の値を試行したら
どういう返答が来るか？

bottom_lt2_sa
top_lt1_sa
top_lt2_sb...

WAF 概念図 (1/2)



図引用: Networkキーワード: WAFとは (2007/06/13)
http://itpro.nikkeibp.co.jp/article/Keyword/20070612/274428/

WAF 概念図 (1/2)

図引用: Networkキーワード: WAFとは (2007/06/13)
http://itpro.nikkeibp.co.jp/article/Keyword/20070612/274428/

本来は...

- 脆弱性のあるWebアプリケーションを修正すべき
- しかし、以下のような状況では修正困難
  - 開発者がメンテナンスを放棄
  - 保守契約が切れて、Web app.の改修依頼ができない
- WAF＝「根本解決が困難な場合」の対応策
- 平時からの脅威監視 / 要求内容の監査

課題

- Ruleの作成が手間
  - Webアプリケーションの仕様を知る必要性
    ⇒ 各変数値の値域を知らないとRule設定不可能
- 基本的なもの/共通化できるRuleを共有
  - OWASP ModSecurity Core Rule Set Project
    - https://www.owasp.org/index.php/Category:OWASP_ModSecurity_Core_Rule_Set_Project
    - OWASP = The Open Web Application Security Project

ModSecurity = Apache(Web server)用WAF module

WAF 参考資料

- (2011/02/28), IPA, Web Application Firewall読本, http://www.ipa.go.jp/security/vuln/waf.html
- オープンソースWAF「ModSecurity」導入事例〜IPAはこう考えた〜: http://www.ipa.go.jp/security/vuln/documents/201012_websecurity_05.pdf
- (2007/06/13) ITPro, Networkキーワード WAFとは, http://itpro.nikkeibp.co.jp/article/Keyword/20070612/274428/
- (2005/08/17), @IT, Web application firewallの必要性 第1回, http://www.atmarkit.co.jp/fsecurity/rensai/waf01/waf01.html
- ModSecurity, http://www.modsecurity.org/
- (2005/05), SofTek Security TOPIC, mod_securityでWebサーバを守る, http://www.softek.co.jp/Sec/mod_security1.html

Personal firewall (PFW)

- Client PCに設置するFirewallのこと
  - 保護対象は個々の計算機 (not Network)
  - 通信制御単位
    - アプリケーション単位
    - 通信 Protocol 単位
- 実装方法
  - 3rd party 製品をinstall
  - AV(Anti Virus)製品の一機能
  - Operating SystemのSecurity機能の一つ

Mac OS X(10.6)の場合

Personal firewall (PFW)

- なぜPFWが必要なのか?
  - 利用形態の多様化 (Note pcを所持、組織外で利用)
    - 利用者が常に保護環境内にいるとは限らない
      ⇒ ”End point security”が重要に
  - Malware、不正アクセス手段の多様化
    - DarkHotel攻撃
- 多層防御の一つ

DarkHotel

標的型攻撃(APT)の1つ

- スパイ(諜報)活動の１種
- 対象人物の宿泊ホテルでそのNetworkを使って偵察活動
  - 攻撃者の活動の場は１位が日本

Kasperskyの報告(2014/11/19) (FBIの報告は2012年)

Dynamic packet filtering

- *Static packet filtering*
  - ⇒ *Rule*を管理者が定義
- *Dynamic packet filtering*
  - ⇒ *Rule(Access control list(ACL))*を動的に生成
    - *Firewall*の運用負担低減
  - 内⇒外の通信要求を監視、そこから外⇒内のあるべき応答*packet*を決定し、該当返答のみを通信許可するよう規則を自動生成