Network Security
Firewall

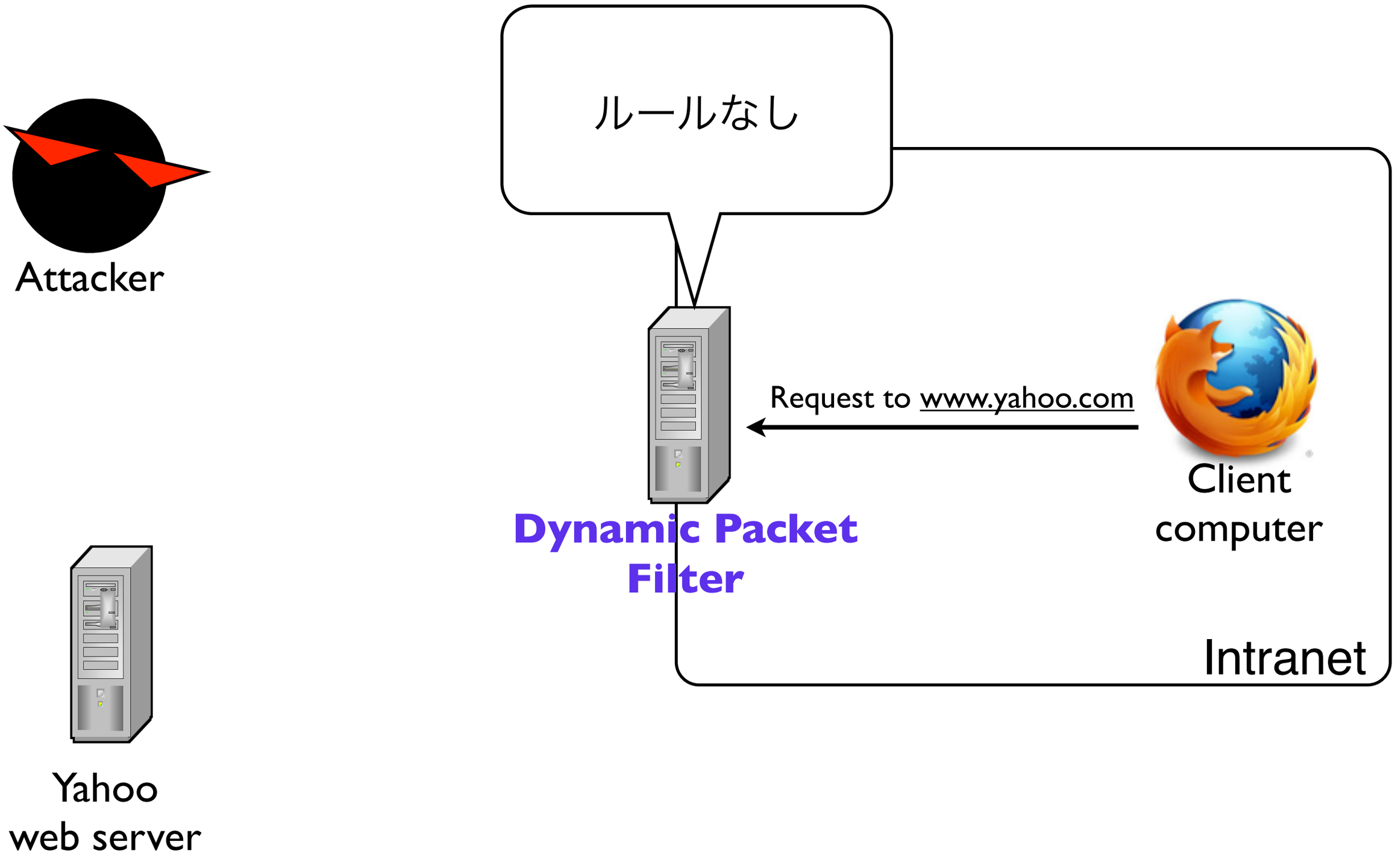
総合情報学科

セキュリティ情報学コース

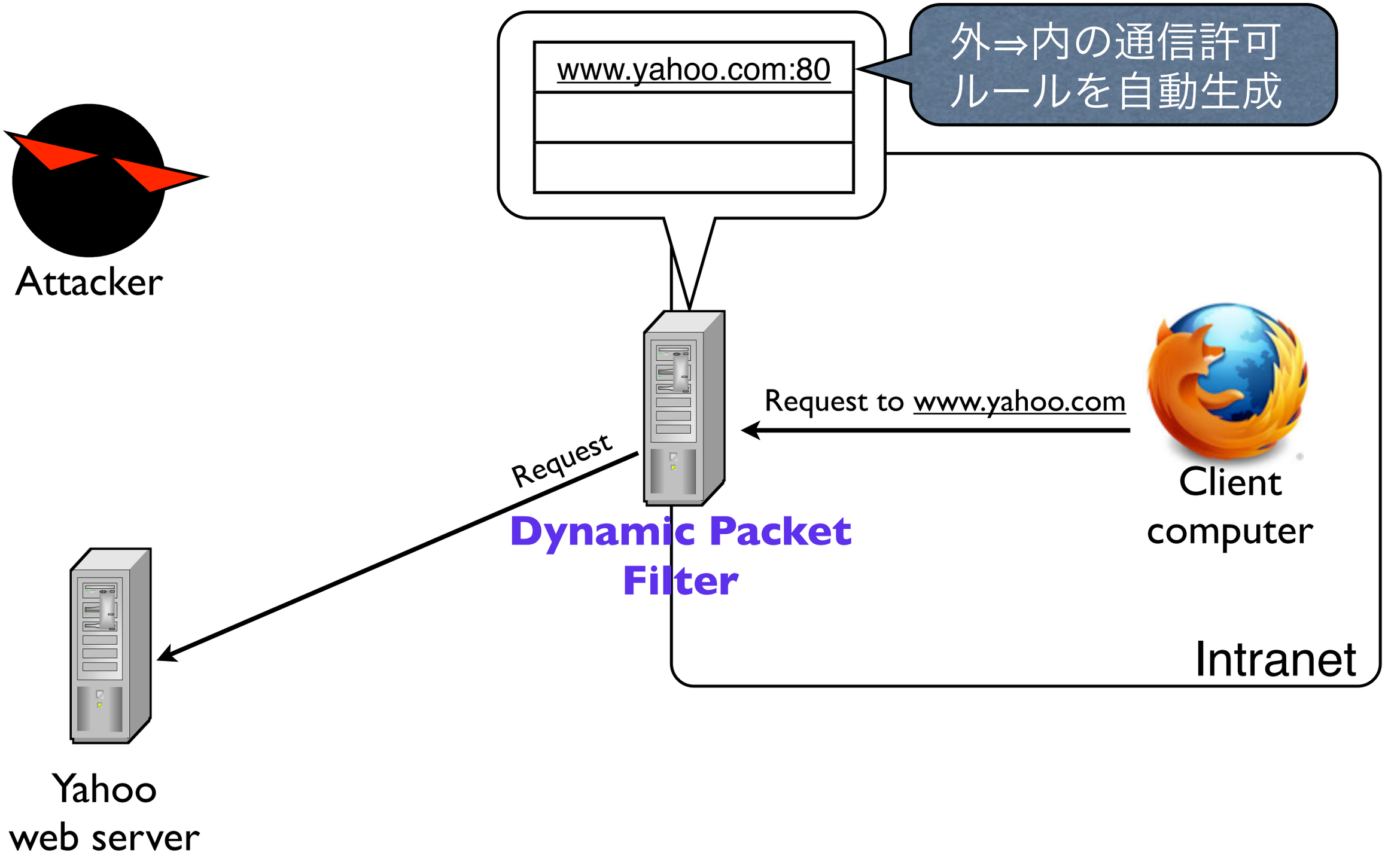
Dynamic packet filtering

- *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

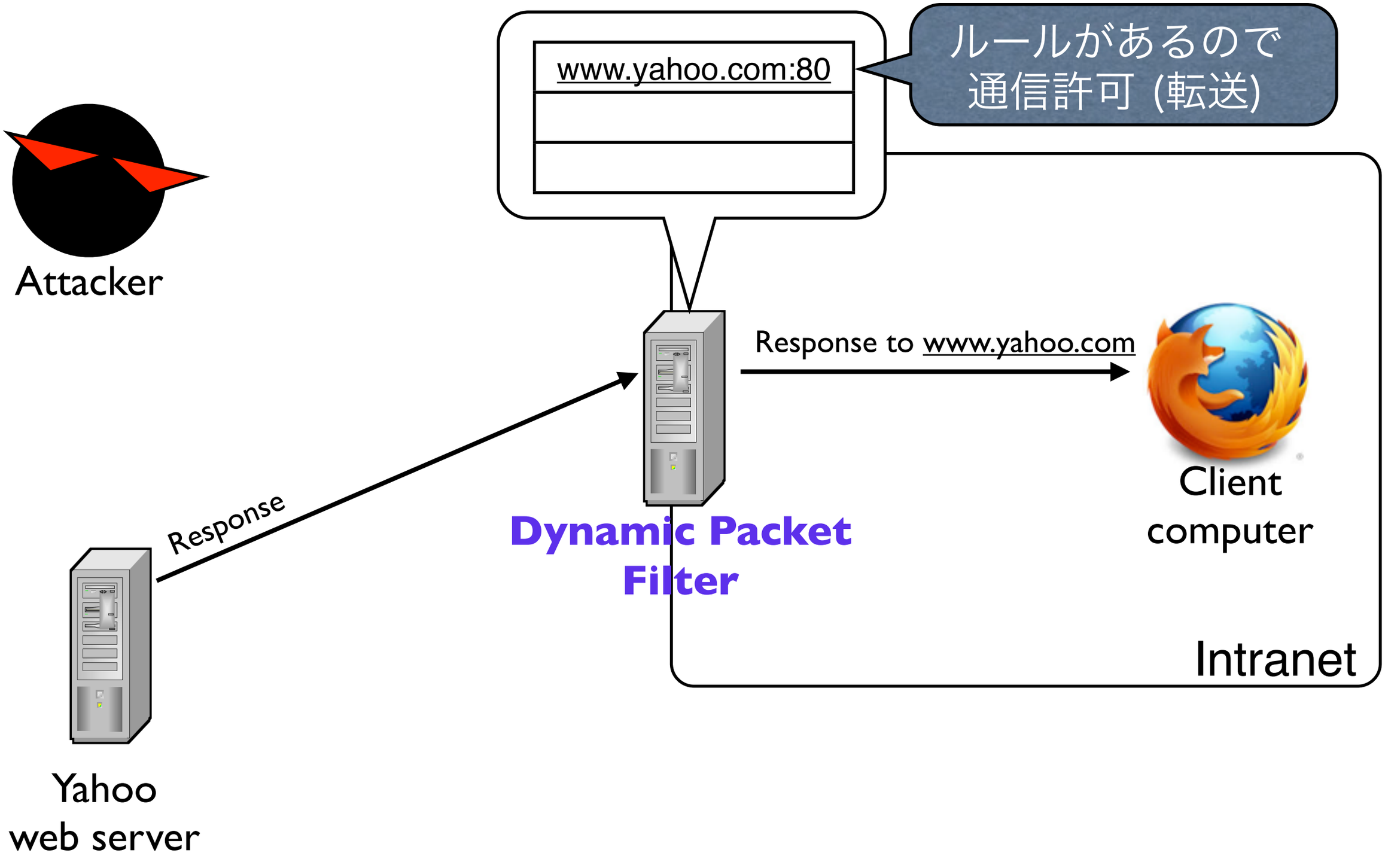
Dynamic packet filtering



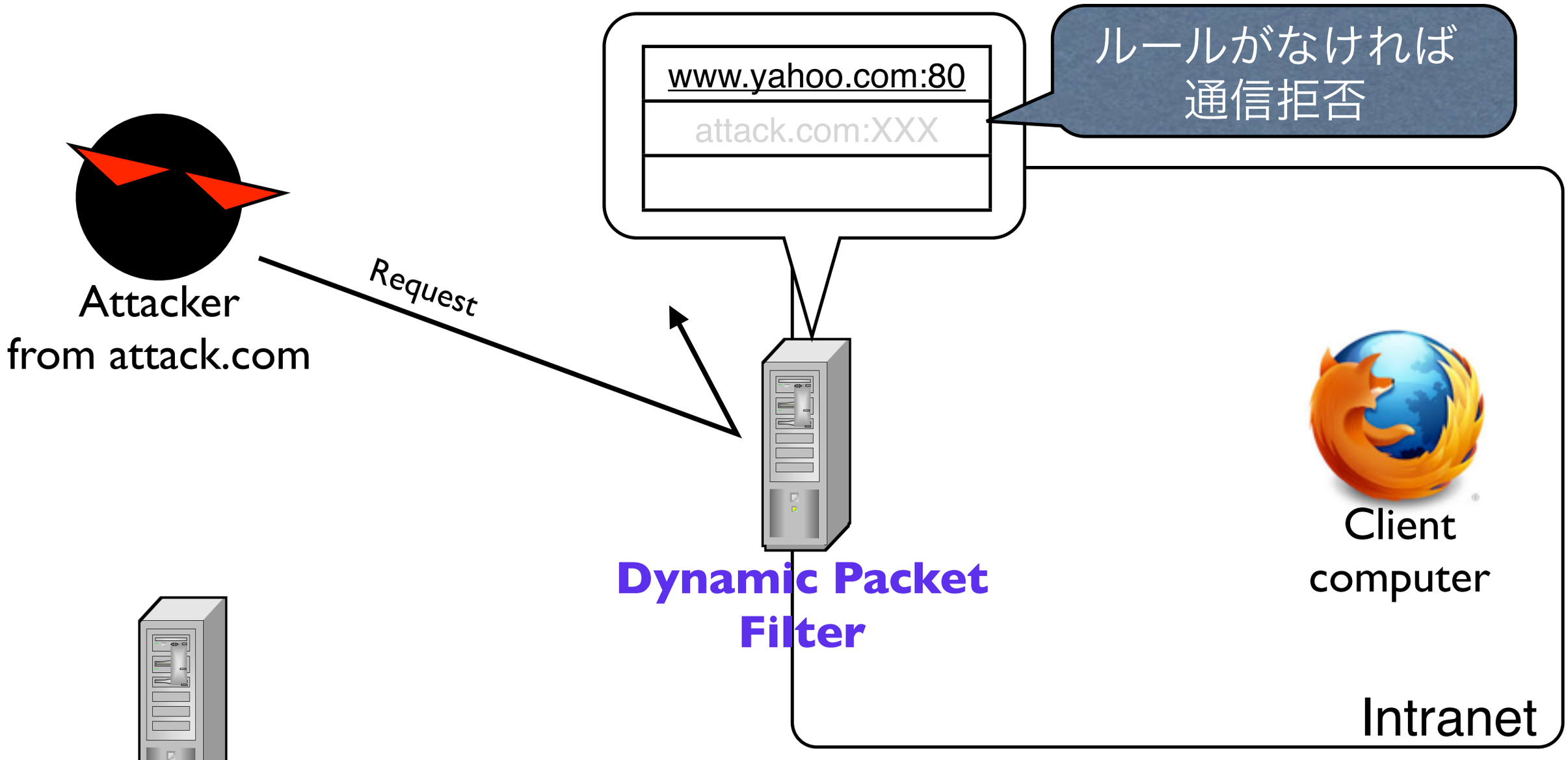
Dynamic packet filtering



Dynamic packet filtering



Dynamic packet filtering



「あるべき返答」のみを通過させる
これらの処理は自動で行われる

Stateful Packet Inspection(SPI)

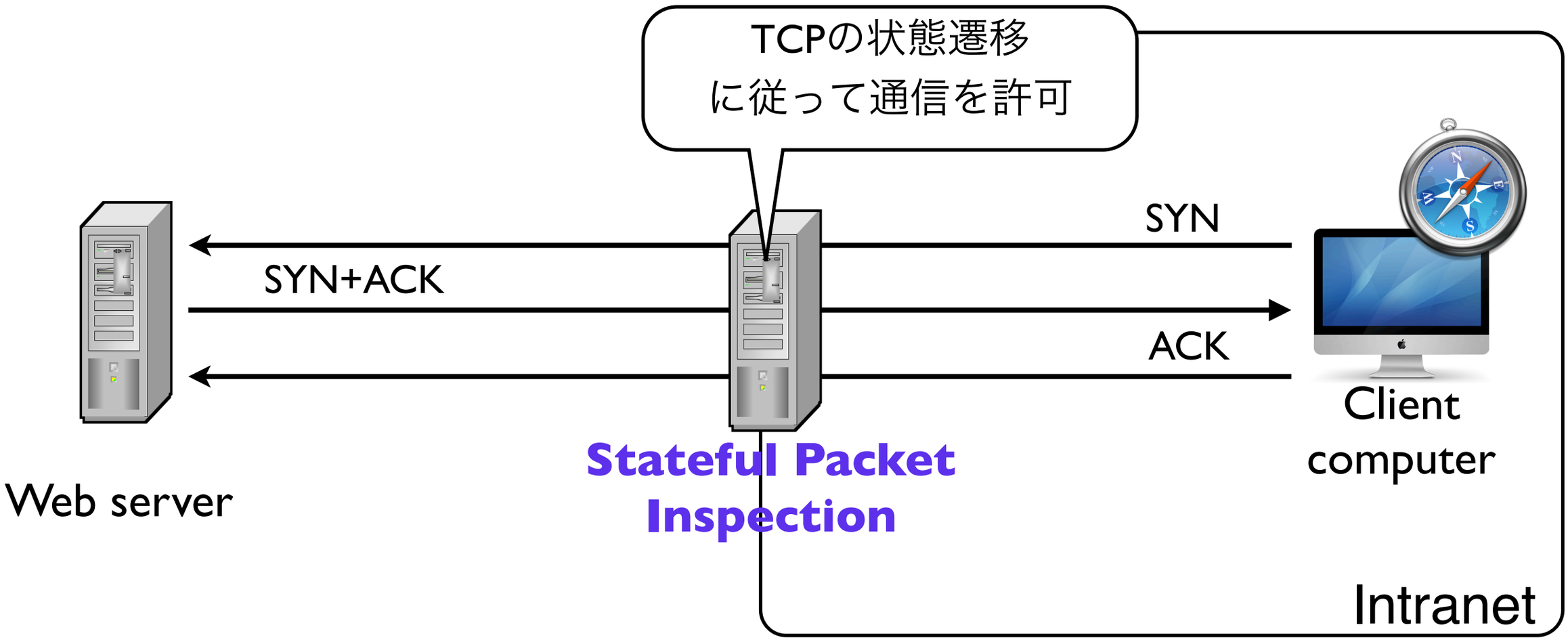
- Dynamic packet filteringの一種
  - 以下の情報を条件設定に利用
    - TCP接続状況 (3 way handshake)
    - アプリケーションプロトコルの既定の振る舞い
  - 状態遷移表に基づき、正常な状態遷移に
    従っているかで通信可否を決定

(2001/7/17), @IT, FTP(File Transfer Protocol)前編,
http://www.atmarkit.co.jp/fnetwork/rensai/netpro10/netpro01.html

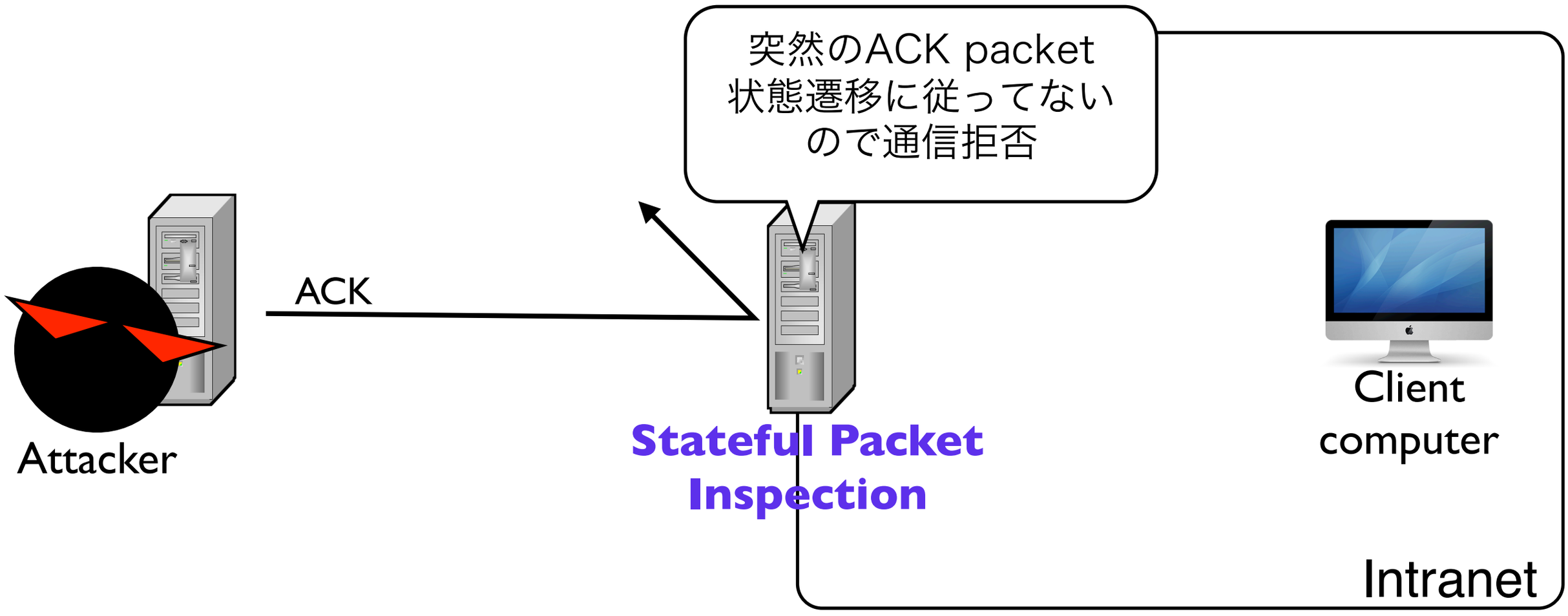
Stateful Packet Inspection 事例1

TCP接続(Web)の場合

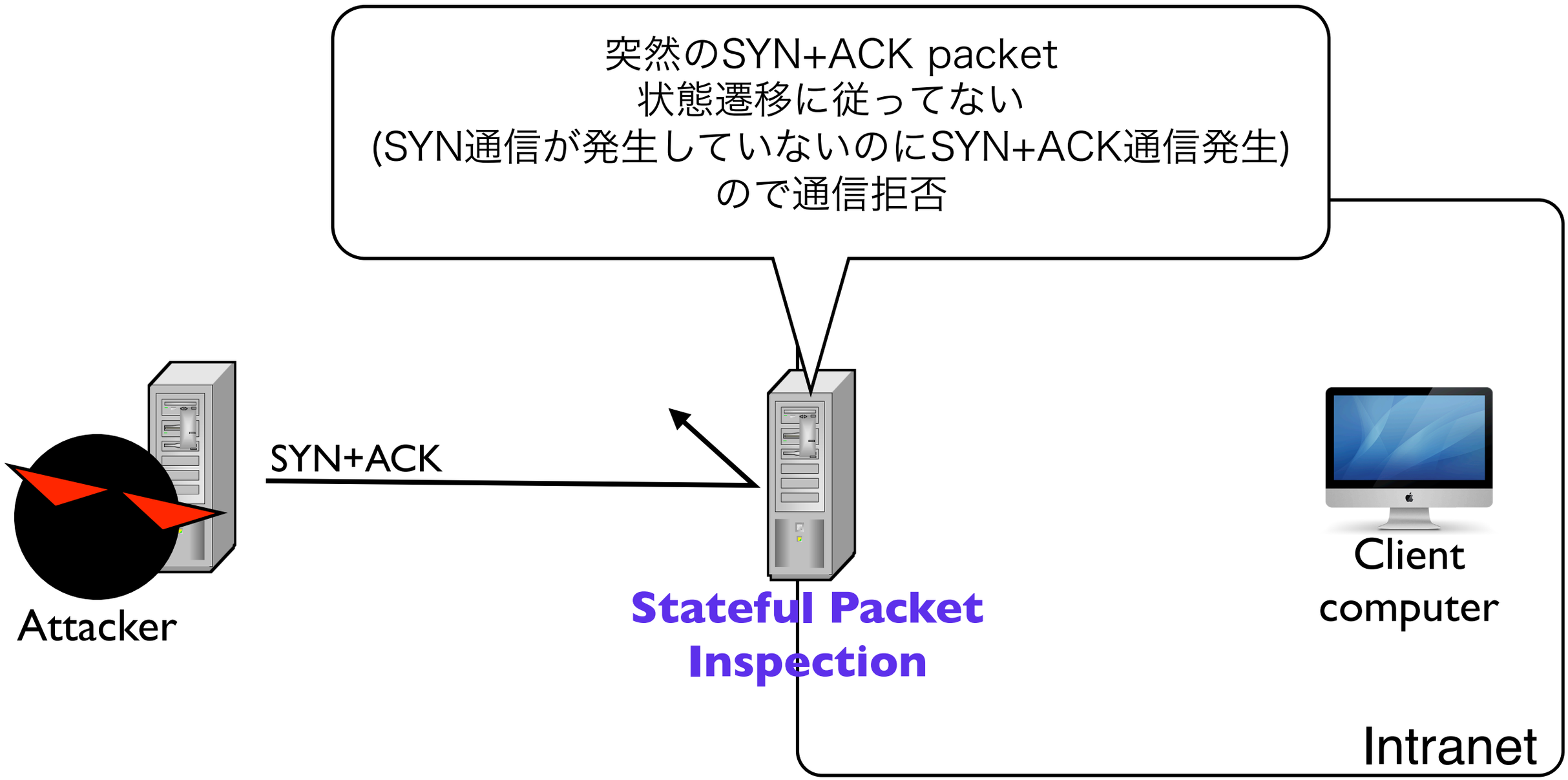
Clientからの接続要求で3 way handshake (状態遷移)



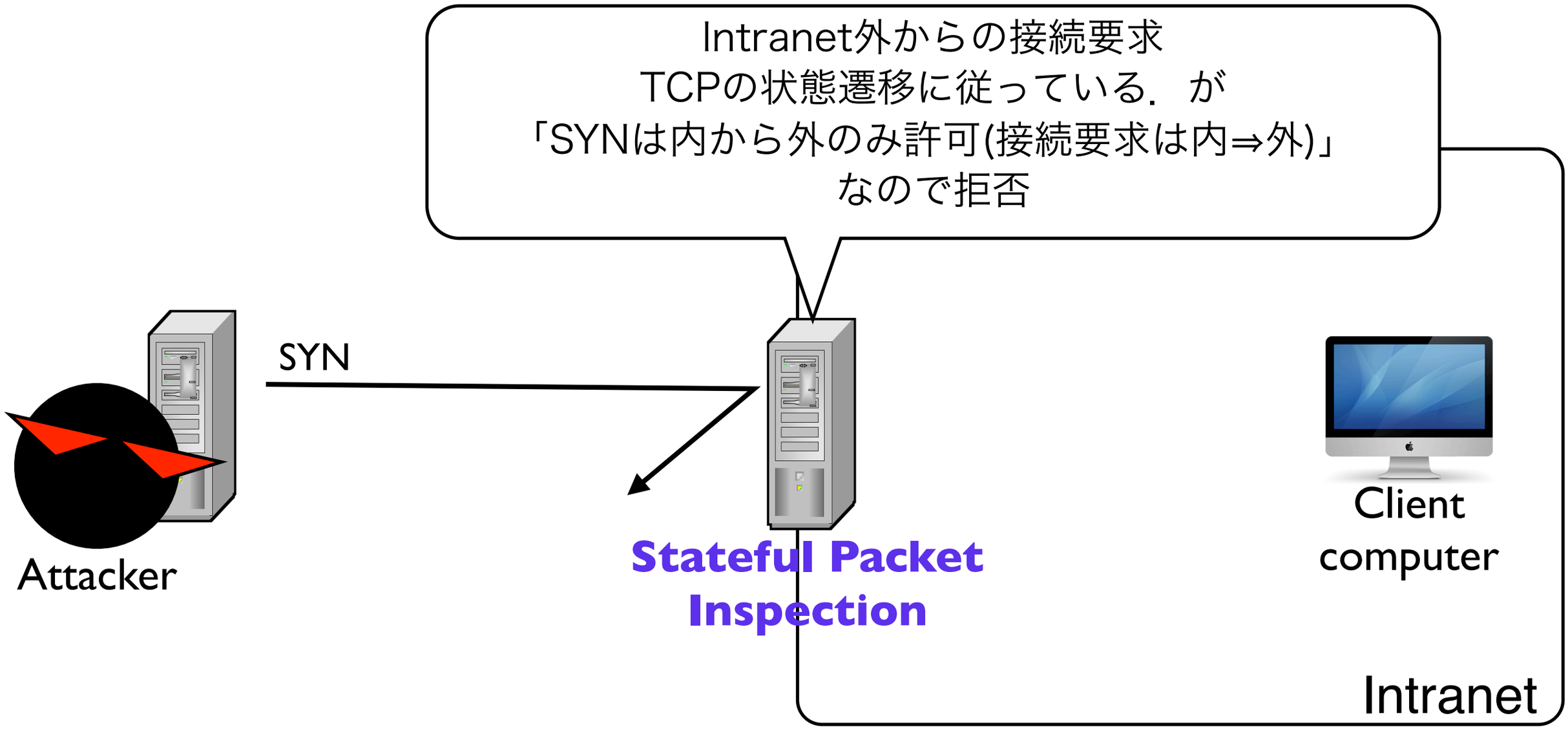
Stateful Packet Inspection 事例1



Stateful Packet Inspection 事例1



Stateful Packet Inspection 事例1



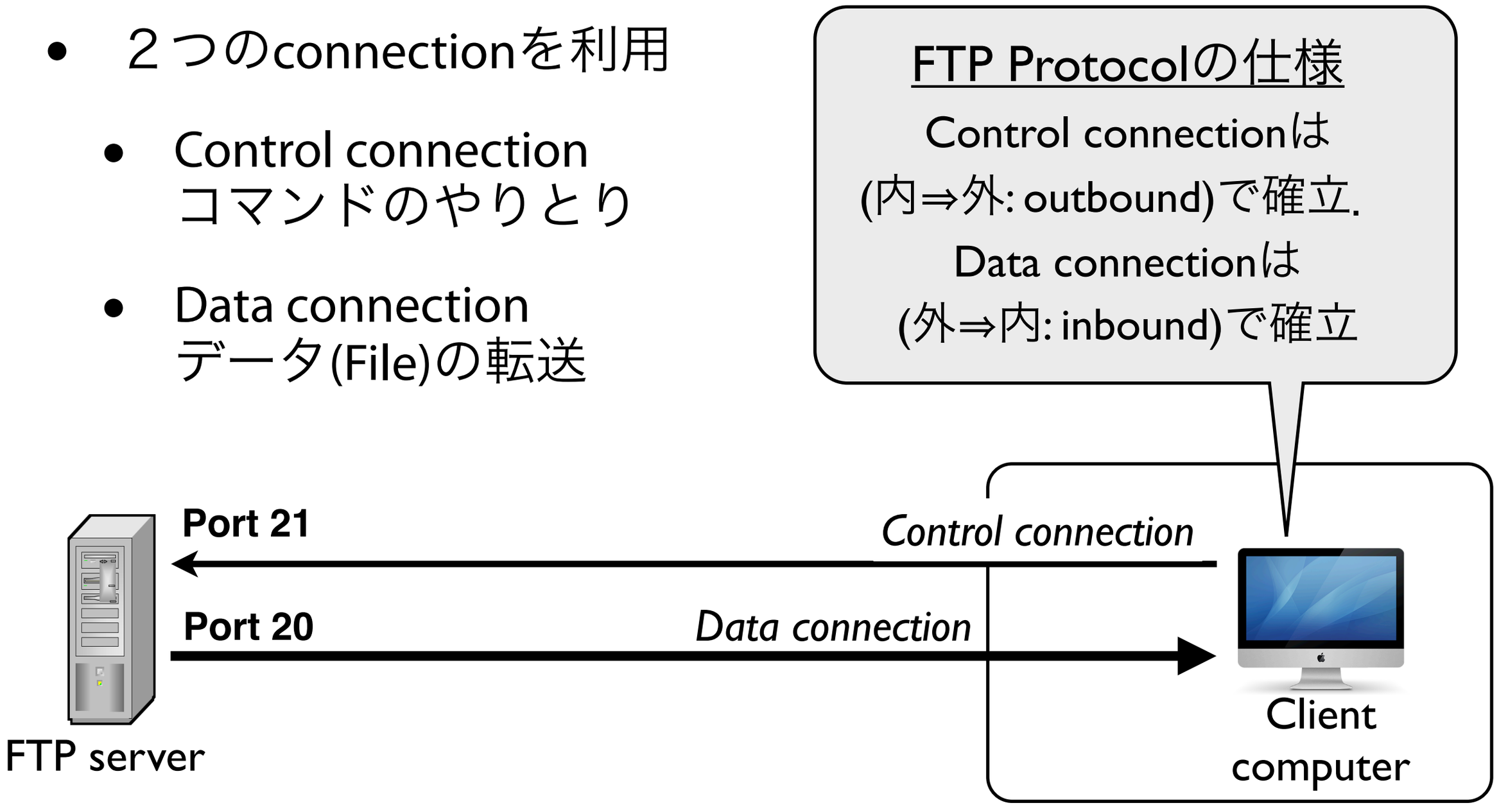
Stateful Packet Inspection 事例2

FTP(File Transfer Protocol)の場合

- ２つのconnectionを利用
  - Control connection
    コマンドのやりとり
  - Data connection
    データ(File)の転送

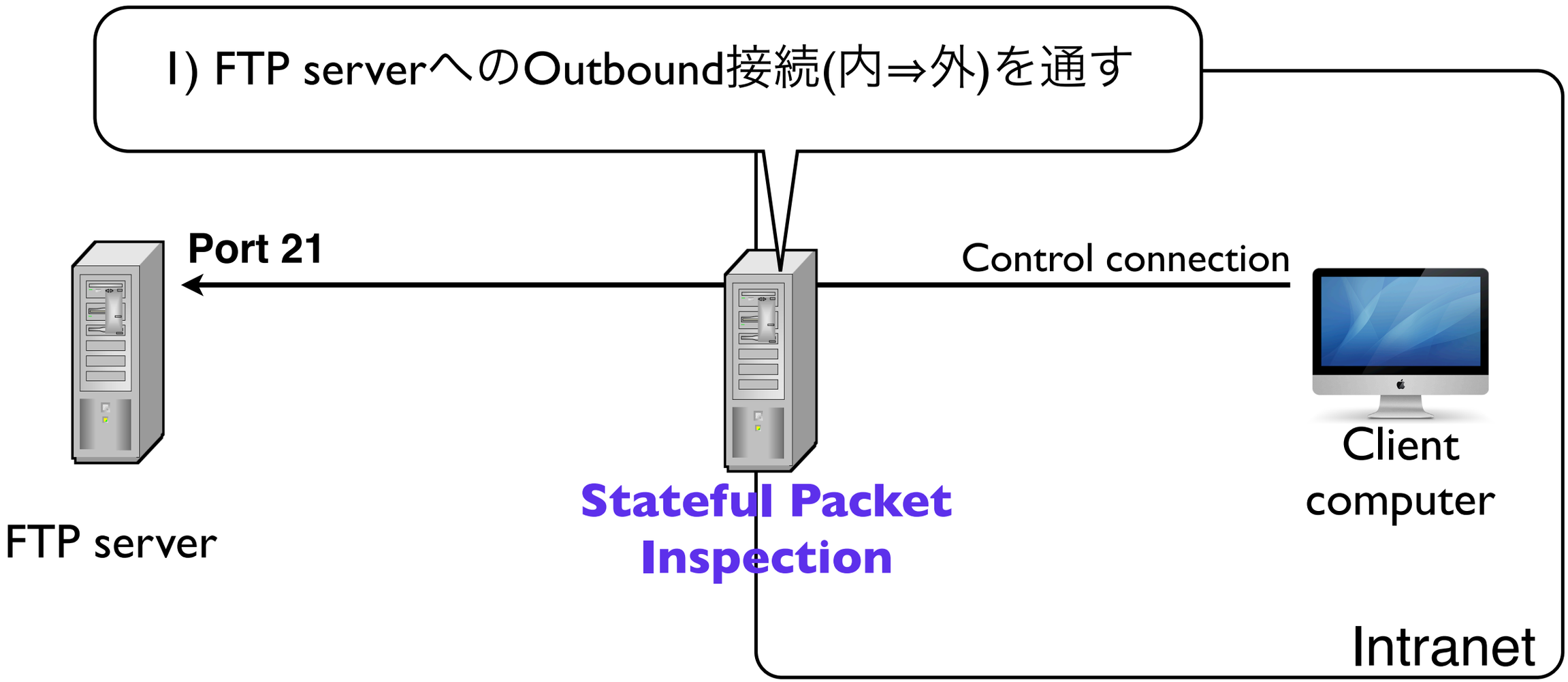
FTP Protocolの仕様

Control connectionは
(内⇒外: outbound)で確立.
Data connectionは
(外⇒内: inbound)で確立

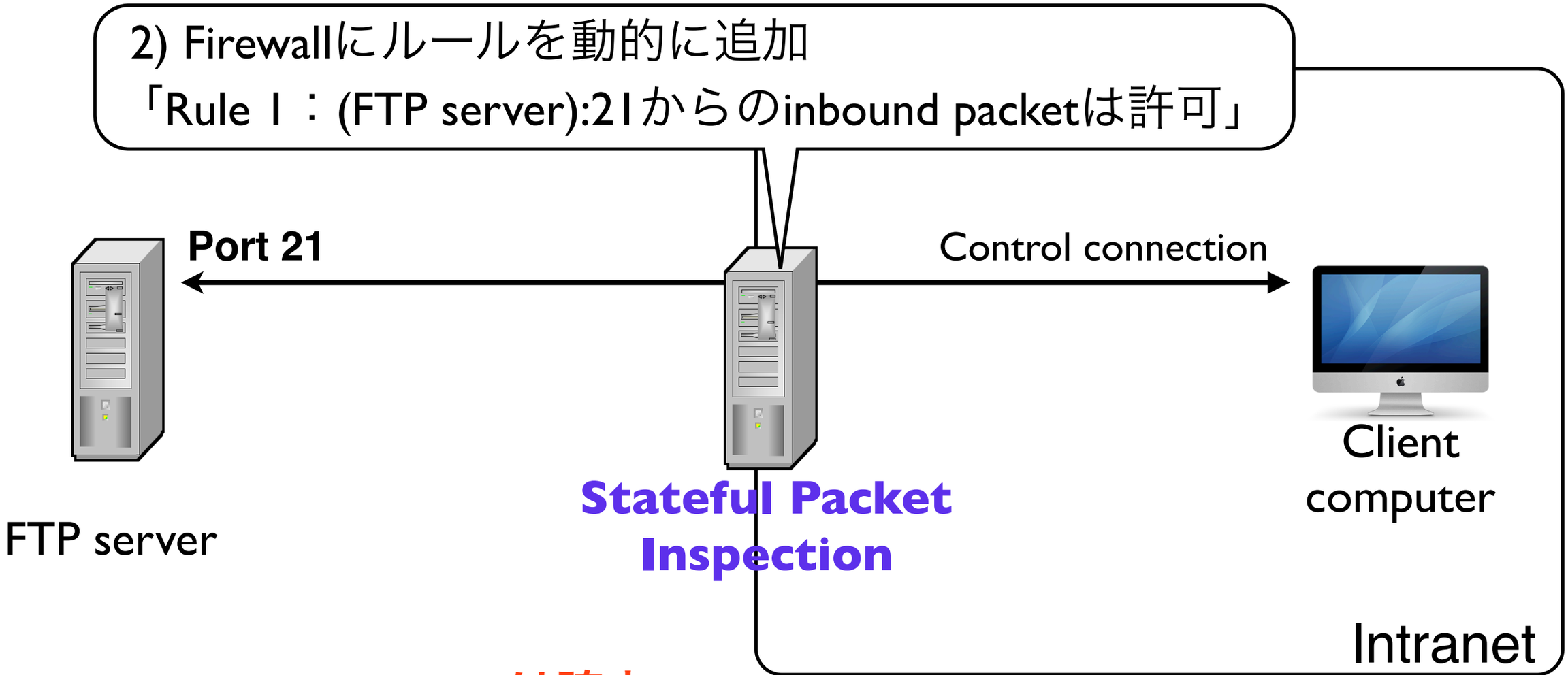


Stateful Packet Inspection 事例2

「SPI 型 Firewall経由ではFTPが使えない」を説明

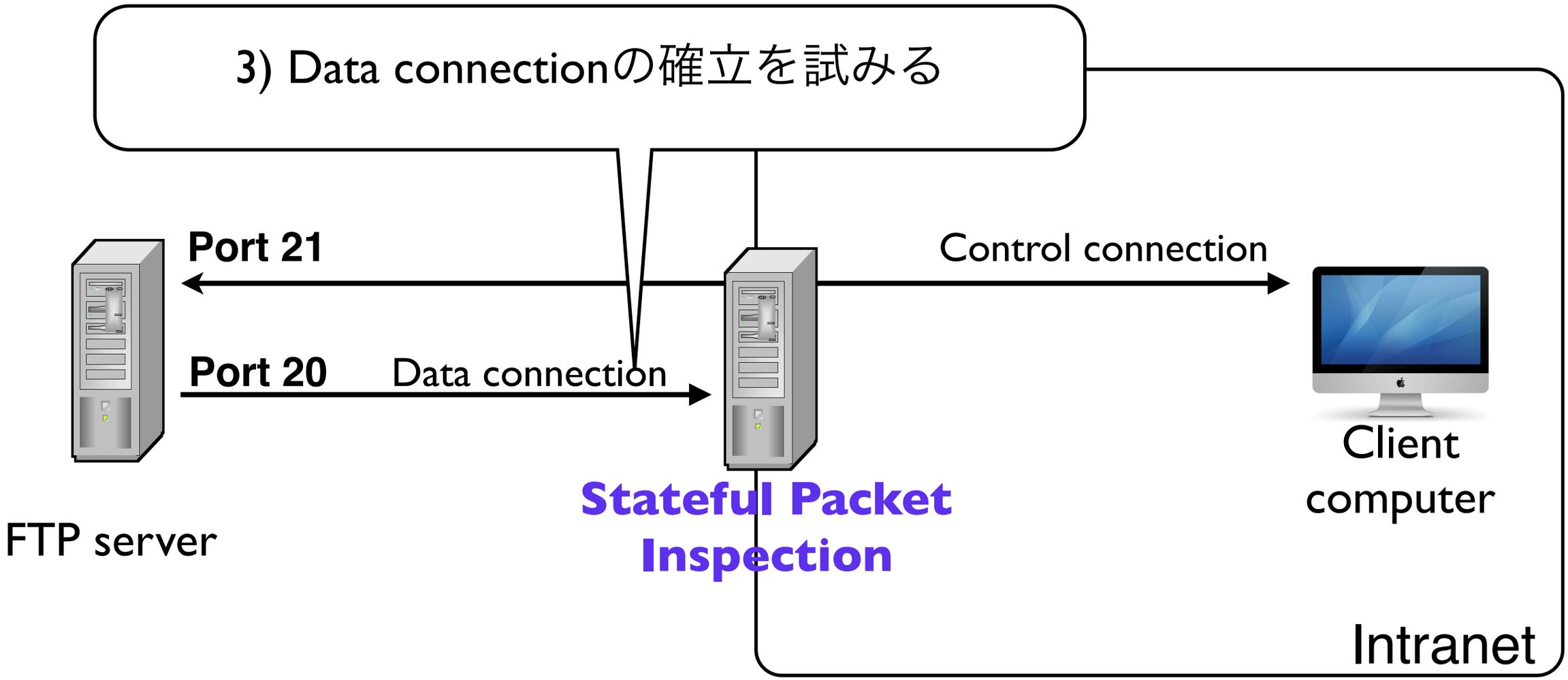


Stateful Packet Inspection 事例2



Control connectionは確立

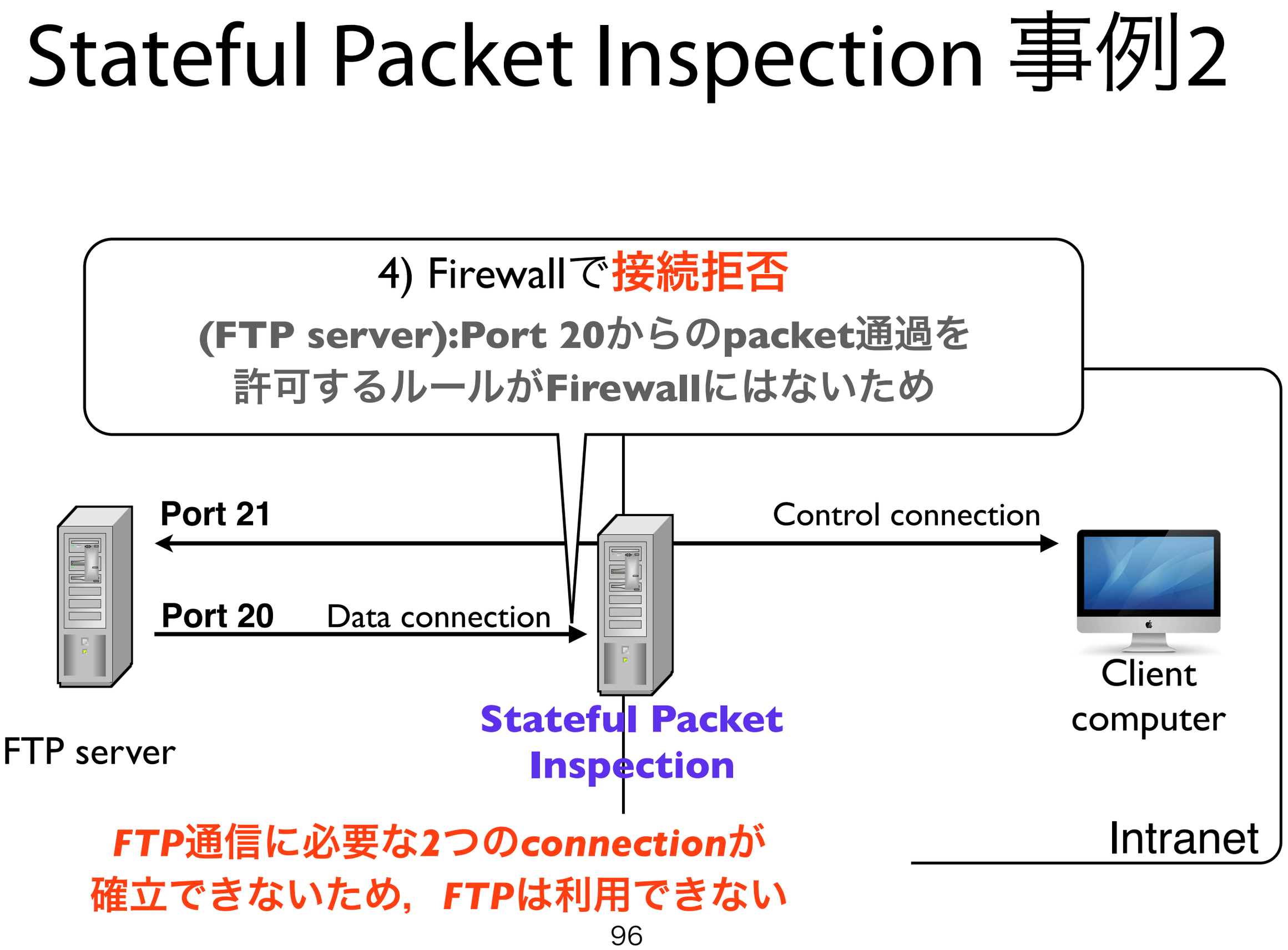
Stateful Packet Inspection 事例2



Stateful Packet Inspection 事例2

4) Firewallで**接続拒否**

(FTP server):Port 20からのpacket通過を許可するルールがFirewallにはないため



***FTP*通信に必要な2つの*connection*が確立できないため，*FTP*は利用できない**

Stateful Packet Inspection 事例2

対応策は２つ

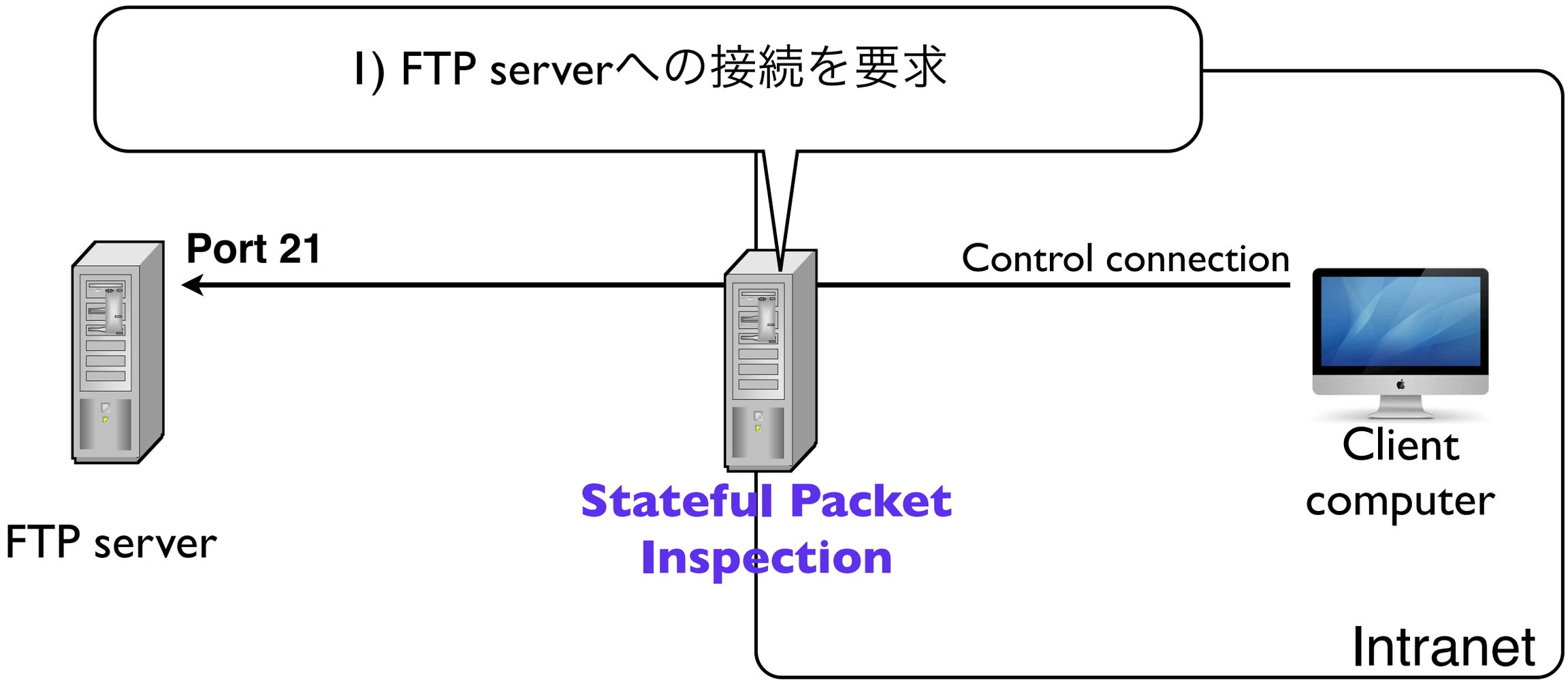
- SPI側での対応
  SPI における動的規則生成に「TCPの接続手順」だけでなく「FTPの振る舞い」を配慮させる

- FTP側での対応
  FTPを改良し，SPI 経由でも問題なくFTPを利用できるようにする
  ⇒ PASVモード

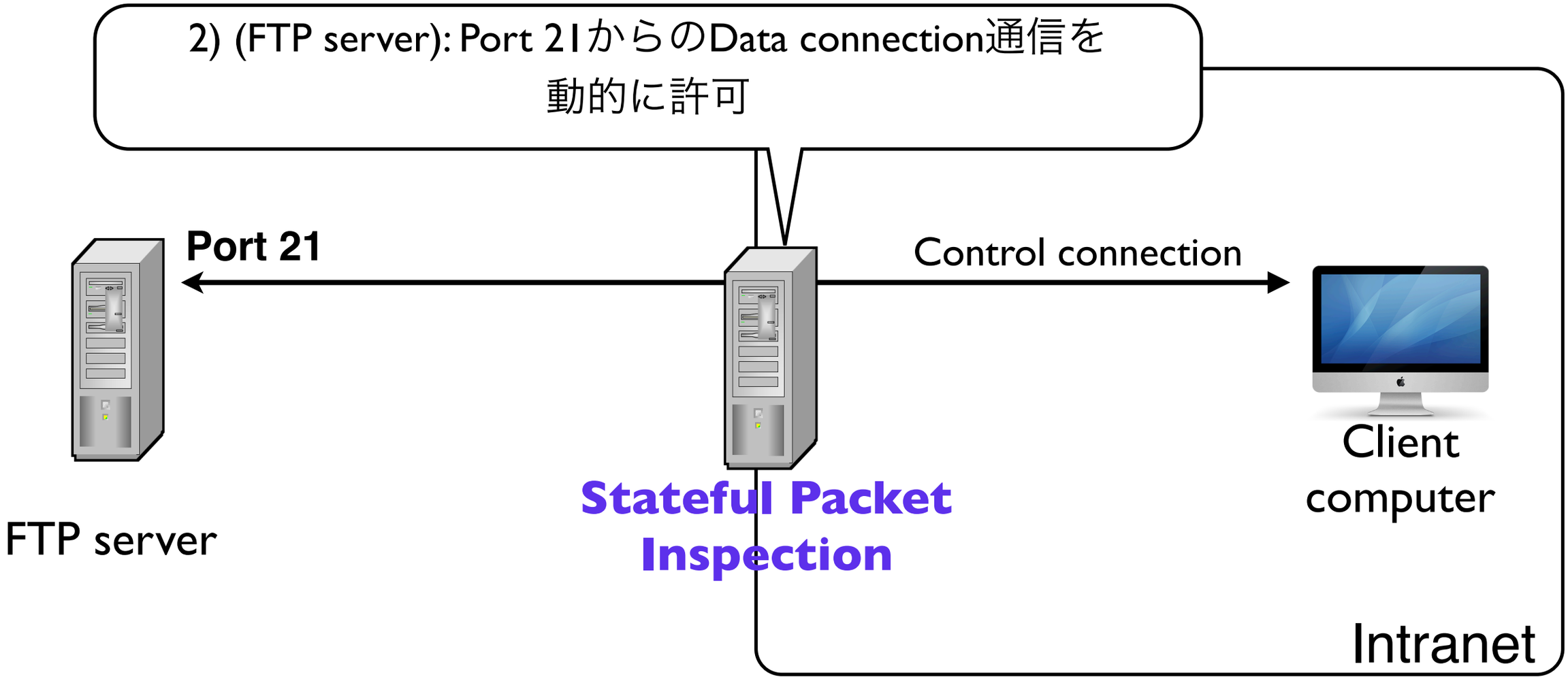
今回は「SPI側での対応」を説明

Stateful Packet Inspection 事例2

SPI 型 Firewallでの対応

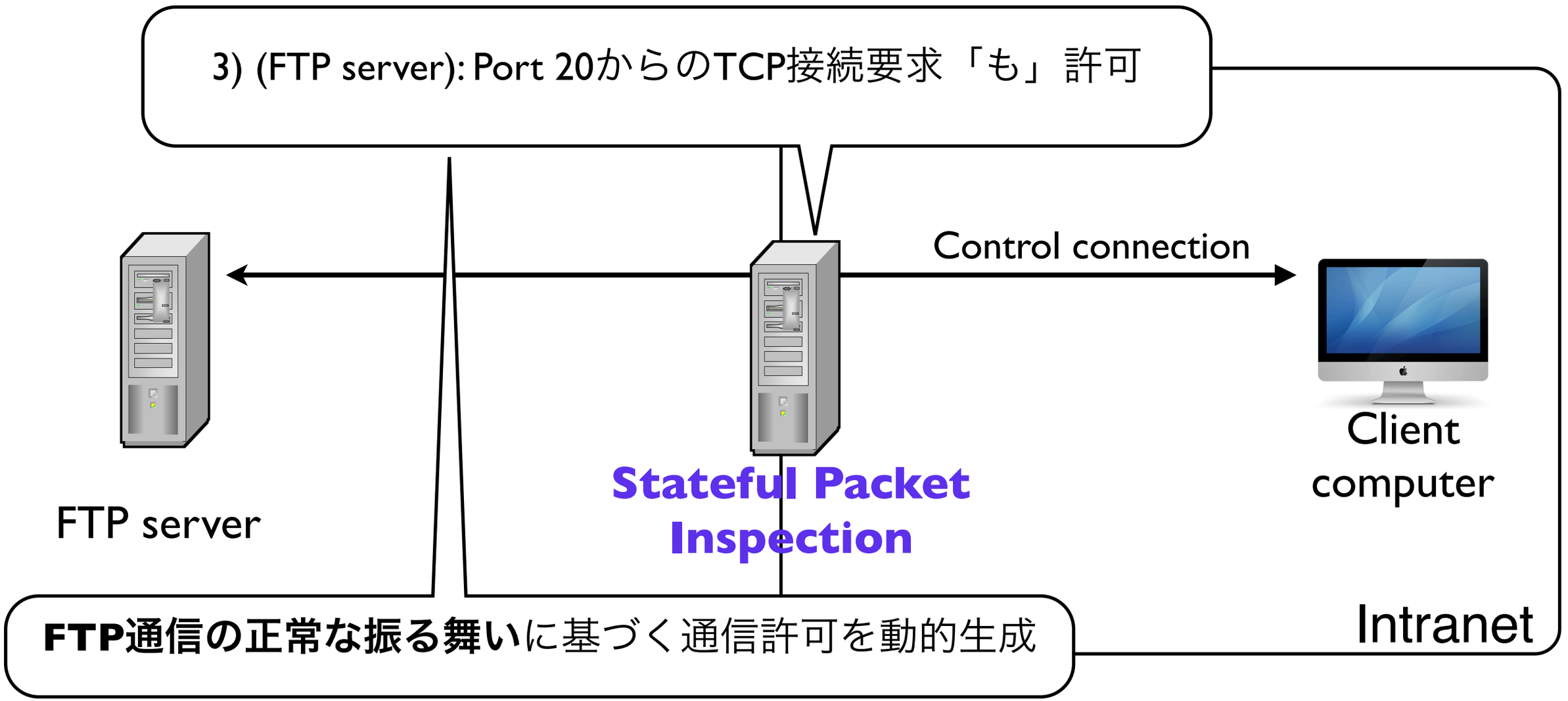


Stateful Packet Inspection 事例2

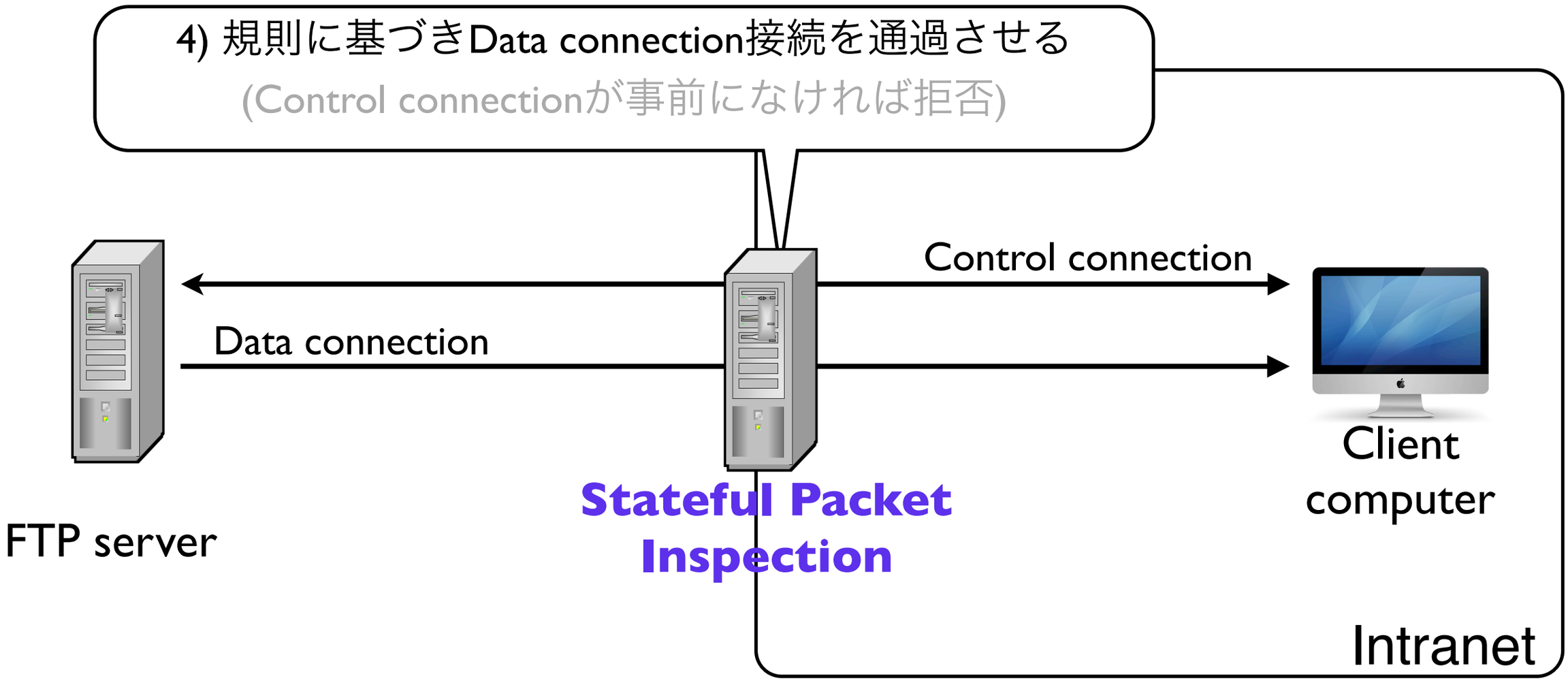


Stateful Packet Inspection 事例2

FTPの正常な振る舞いを想定した
動的な規則生成



Stateful Packet Inspection 事例2



dynamic packet filtering
参考資料

- (2009/08/12) 不正アクセスを防ぐFirewallの仕組み
- http://ascii.jp/elem/000/000/447/447615/
- 第2回: SPIと動的パケットフィルタリングの違い
- http://plusd.itmedia.co.jp/broadband/0305/16/lp13.html
- ITPro, Security用語辞典, ダイナミック・パケット・フィルタリング
- http://itpro.nikkeibp.co.jp/word/page/10006000/

Firewallの限界

- Network Securityにおける基本防御システム
  - ⇒ ルールに基づいて通信制御
  - ⇒ ルールが適切に定義されている必要性あり
- 適切に運用(ルールを適用)すれば、外部からの不正なアクセスに対し効果発揮
  - ⇒ 逆も真なり (例) http://blog.ohgaki.net/waf
  - 逸話：「穴だらけFirewall」⇒ 設置はしたが、ルールゼロ
- 検証は必ず必要：意図した通りの制御動作か？

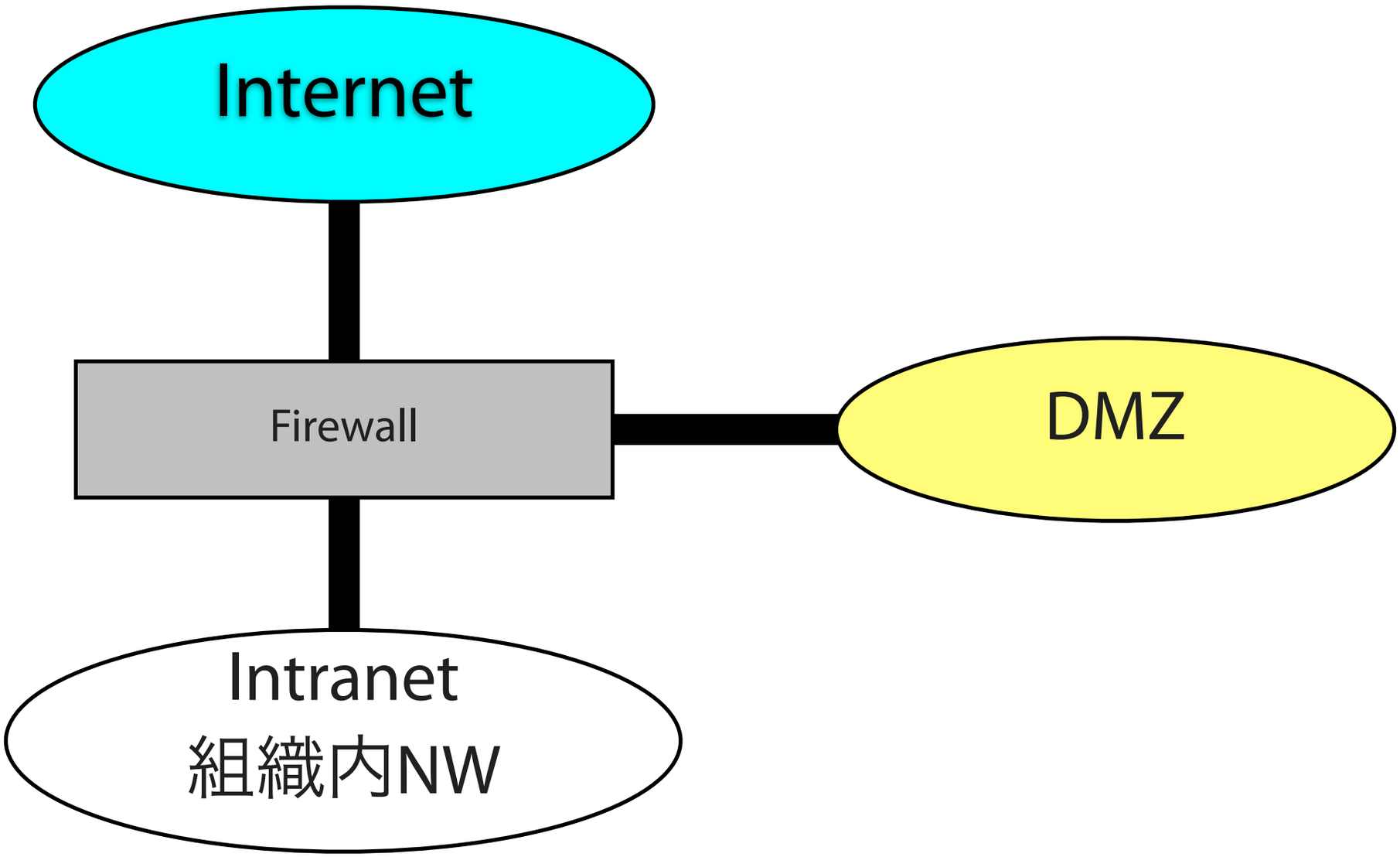
Firewallの限界

- 許可している通信を利用した攻撃は防御不能
  - 電子メール(smtp), Web(http)経由の攻撃は別の対策が必要
    - DoS攻撃、AFにおける暗号化通信(VPN, SSL)
- Backdoorを誘因
  - DMZやIntranet内に無線LANや通信Modemを設置 Firewallを迂回可能に ⇔ 組織内調整を密に

Backdoorとは

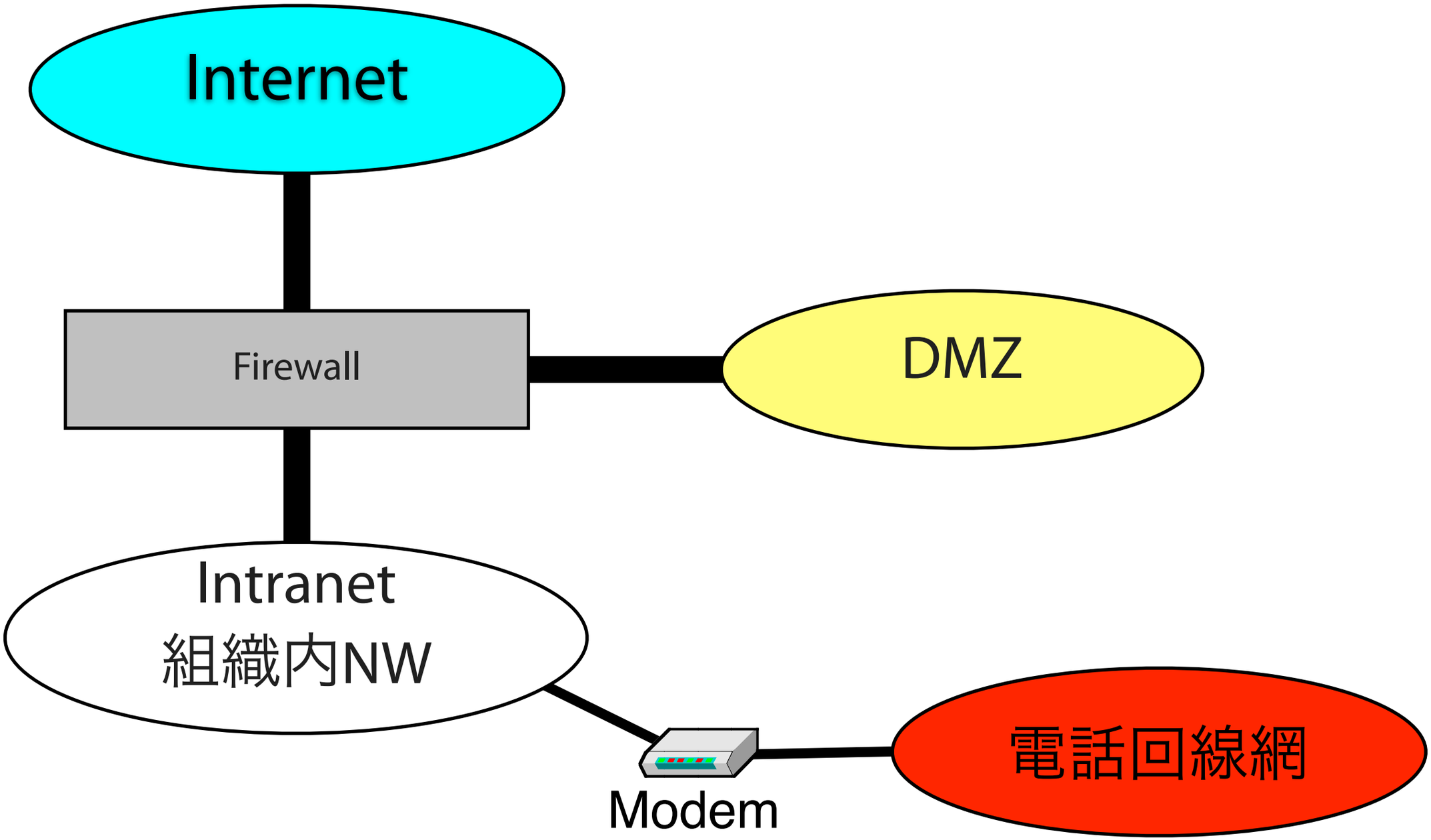
- 不正侵入に成功した侵入者が行う行為の1つ
- 以降の侵入のために、今回の侵入方法とは別の侵入口を新たに設置する行為
  - 別の侵入口 ⇒ Backdoor (裏口)
- なぜ設置？
  - 侵入が発覚すると、その侵入口は塞がれる
  - 別の入り口(裏口)を用意しておけば、そうなってもまた侵入できる

Firewall回避のBackdoor



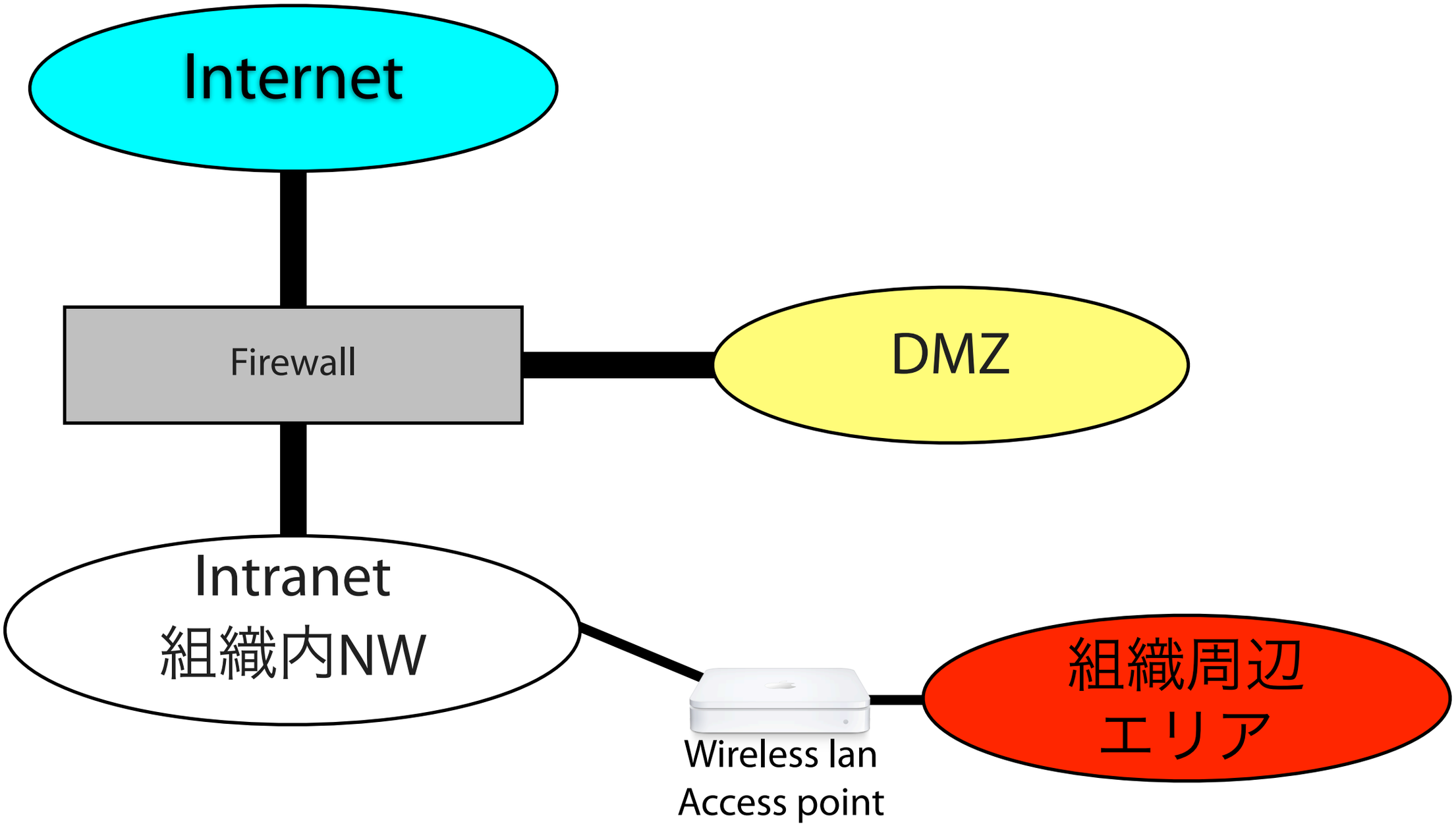
NW=Network

Backdoorの方が容易



NW=Network

Backdoorの方が容易



NW=Network

Firewallの限界 (cont.)

- 内部⇒外部へのアクセス制御
  - ルール定義なし/ゆるくなりがち。そこをついて受動的攻撃が発生する可能性 (Spyware/Bot)
- Firewall自体の脆弱性
  - Firewallはsecurity対策機器 = 脆弱性はない。ではない
  - 脆弱性管理 / アップデートは必要
  - (2007/07/11), Microsoft, Windows Vista firewallの脆弱性により、情報漏えいが起こる, http://www.microsoft.com/japan/technet/security/bulletin/ms07-038.mspx
  - (2005/09/01) ITPro, Windows firewallに不具合、設定画面に表示されない「例外」を作成できる, http://itpro.nikkeibp.co.jp/article/NEWS/20050901/220450/
  - Brothersoft, “Leopard”のfirewallに早くも問題が発覚、http://jp.brothersoft.com/show-news/1028.html

Firewallの今後(1)

- 現状の問題
  - 通信許可しているプロトコルを利用した攻撃への対策
    - Web(http), E-mail(SMTP), SSHなど
  - 通信許可しているプロトコルを使用した通信制御迂回への対策
    - HTTP-ProxyやVPN, ssh port forwardingなど
- 従来: Packet header(荷札)で通信制御
- 今後: DPI (Deep Packet Inspection)へ
  - 通信トラフィックからアプリケーションを識別、制御
  - アプリケーション、利用者、コンテンツでの通信制御
  - Not only in-bound traffic, But also out-bound traffic

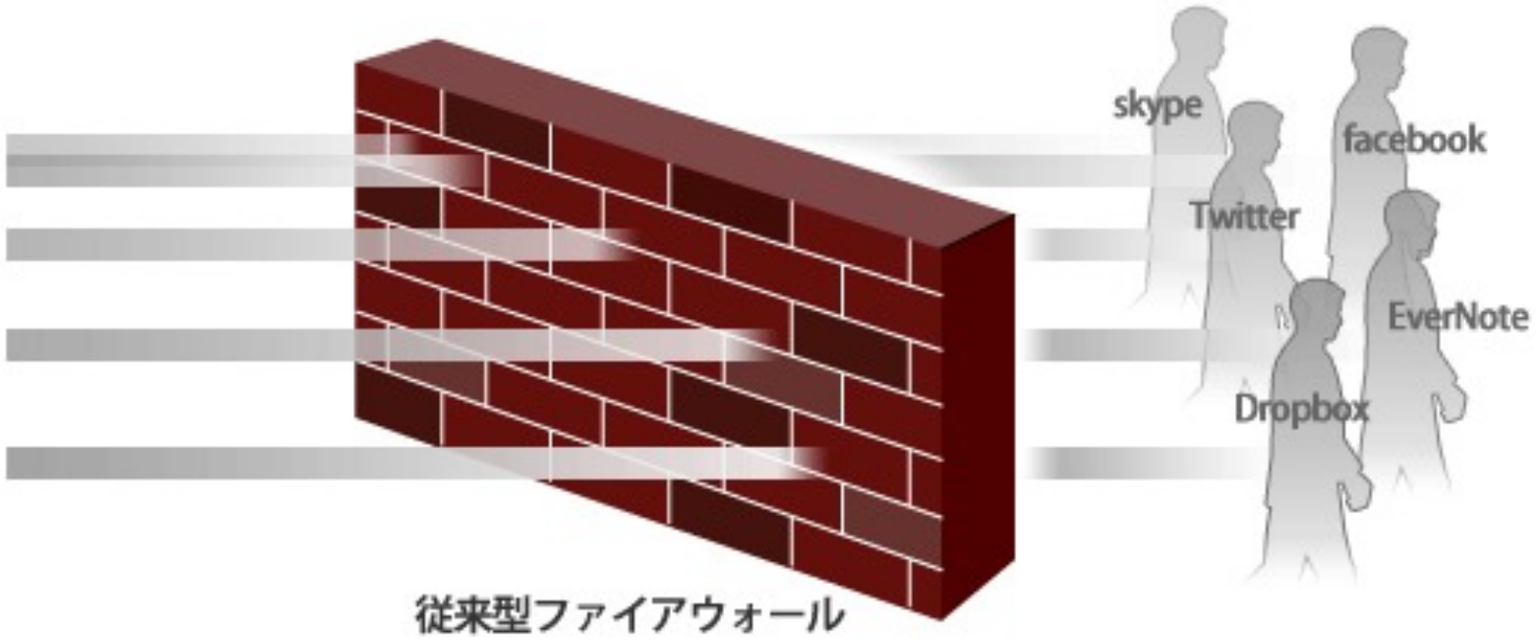
最近の問題

従来

1つのポートに１つの
アプリケーション

最近

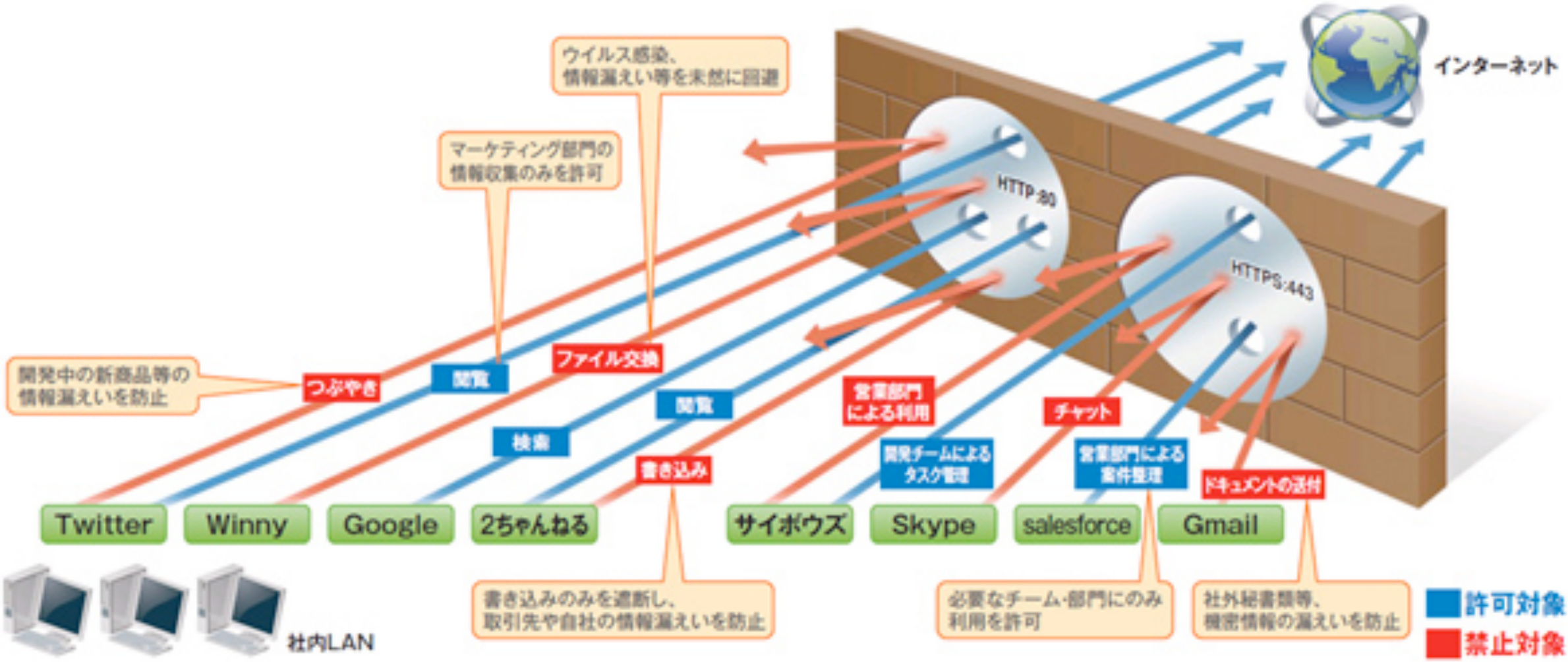
1つのポートに複数の
アプリケーション



ポート番号で
アプリケーションの
通信制御が困難
特にHTTP(80)

図引用: 日立ソリューションズ, 次世代firewallとは？
http://www.hitachi-solutions.co.jp/paloalto/sp/firewall/firewall.html

次世代firewall



通信トラフィック内のアプリケーションを識別、制御
(アプリ x ユーザ x 読み書きで制御)

図引用: http://www.hitachi-solutions.co.jp/paloalto/sp/firewall/firewall.html

参考文献

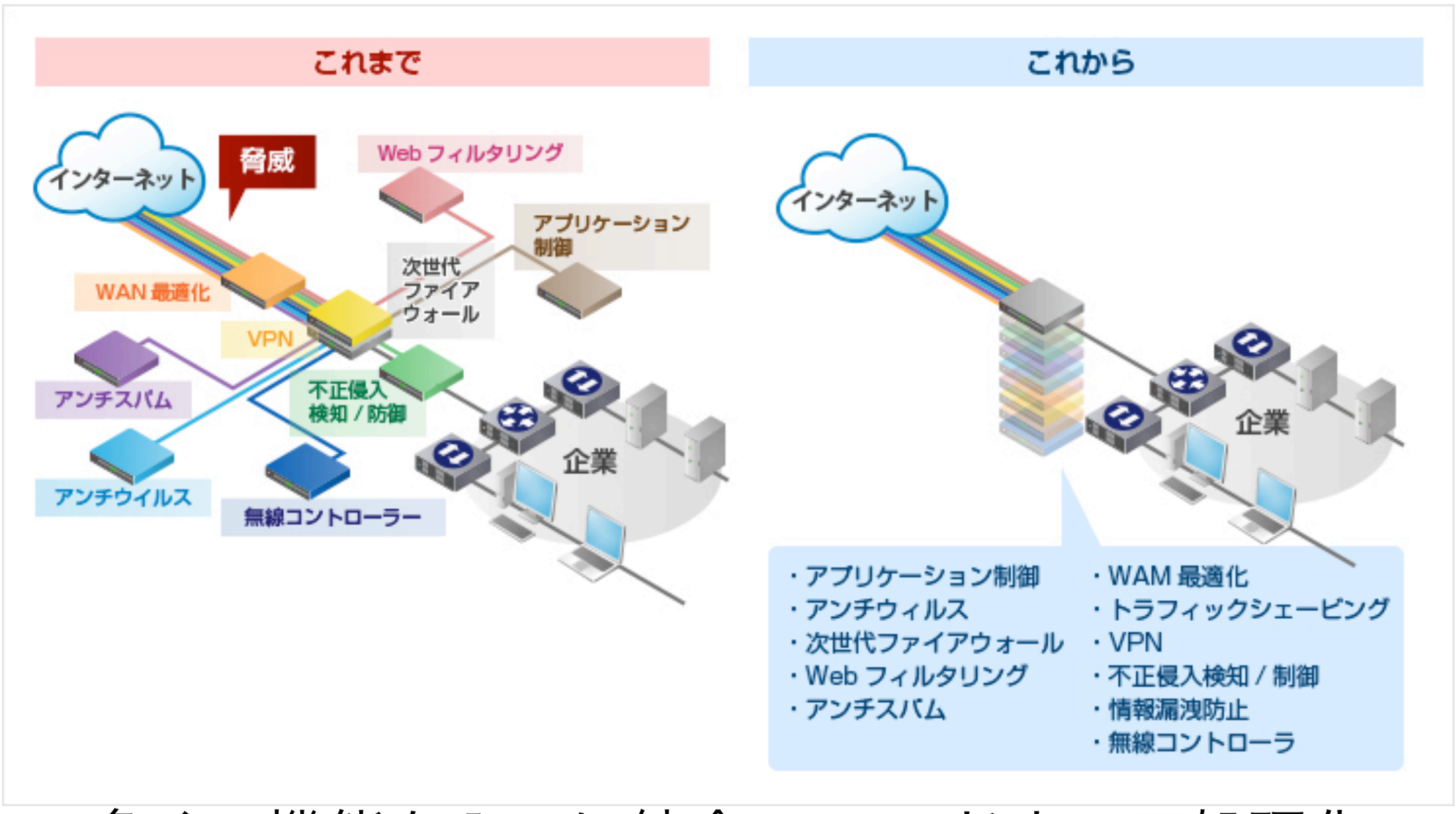
- Defining the Next-Generation Firewall
  - John Pescatore, Greg Young, Gartner, Oct. 2009.

Firewallの今後(2): UTM

- 統合脅威管理 (Unified Threat Management)
  - ⇒ 通信制御だけから包括的な対策の実施へ
    - Firewall + Anti-SPAM + Anti-Virus + 不正侵入検知/防止 + Content filtering
  - Firewall単体機能から、一台の専用機器で上記すべての処理を実施
    - Defense in Depthの多くの層を担う機器へ
  - Security対策が一極化、人材、管理コスト的にメリット
    - 中堅、中小企業には効果あり

(2009/01/30), ZDNet, 次世代firewallとは何か? - 第3回: firewallの停滞と進化、
http://japan.zdnet.com/security/sp_next-firewall-2009/20387398/2/

UTM イメージ



多くの機能を１つに統合 + ハードウェア処理化

図引用: http://cas.softbank.jp/services/vappliance/products/category/utm.html

侵入検知・防止システム

情報理工学部 総合情報学科

先端工学基礎課程

2016/07/25

侵入検知システム

- 英語名: **I**ntrusion **D**etection **S**ystem（略称 IDS ）
- 不正行為を迅速に「**検**出」し、

  セキュリティ管理者に「通**知**」するシステム

FirewallとIDSの違い

- Firewall
  - アクセス制御：既定の通信のみを通過. それ以外の不要な通信を遮断. 管理者が設定
- IDS
  - 通過する情報を精査し、不正行為を積極的に発見. 管理者に通知

補完性 (Firewall と IDS)

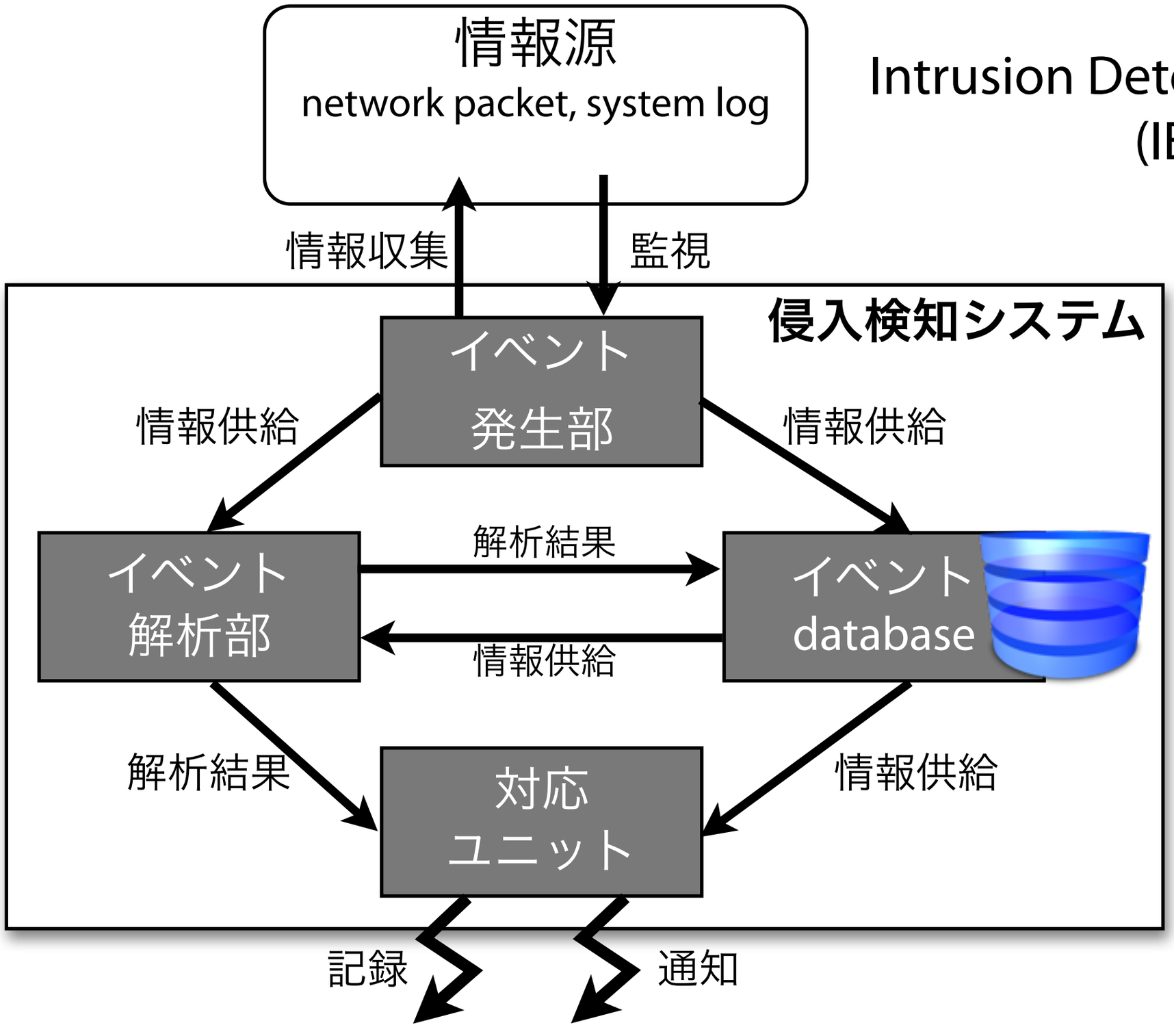
- Firewall ⇒ アクセス制御
  - 事前に決定された規則に基づく制御
    - 例：空港でのパスポートコントロール
- IDS ⇒ 不正の検出
  - 与えられるデータから不正を見つける
  - 例：空港での手荷物検査

Anti Virus softwareとの違い

- Anti-Virus Software
  - Malwareの検知、駆除
    - 電子メールの添付file、計算機内fileから Malwareを発見、通知、駆除
- IDS
  - fileの有無に限定せず、またマルウェアだけに限定せず、不正行為を検出、通知する

Malware = Malicious software（悪意あるソフトウェア）の省略形

IDSの概念モデル



Intrusion Detection Working Group (IETF-IDWG)

- イベント発生部
  - Event generators: **E-box**
- イベント解析部
  - Event analyzers: **A-box**
- イベントDB
  - Event databases: **D-box**
- 対応ユニット
  - Response Units: **R-box**

IDSにおける３つの特徴軸

- 監視対象 (入力情報)
- 検知手法
- 設置場所 (配置方法)

監視対象

- 監視対象 = IDSへの入力情報
  - Network を対象
    - 入力: Network packet
      - Network-based IDS = **NIDS**と呼ばれる
  - Host (計算機内の情報) を対象
    - 入力: files、 system logs、 resource usage
    - Host-based IDS = **HIDS**と呼ばれる