ファイアウォール
～その考え方と今後の動向～

Internet Week 2003

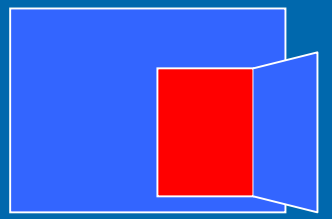
チュートリアル　T2O

担当　二木 真明（SSE）

Agenda

- ファイアウォールとは （復習）
  - 従来型ファイアウォールの概念、機能と形式
  - ファイアウォールに出来なかったこと
- セキュリティホールに対する攻撃の検知と防御
  - IDS（侵入検知システム）の機能と問題点
  - IDPS（侵入検知・防御システム）の特徴
  - ファイアウォールとしてのIDPS
- アプリケーションの脆弱性と保護
  - アプリケーションファイアウォールの考え方

ファイアウォールの概念



- Firewall = 防火壁というよりは防火ドア
  - 何かを通す必要がなければ「壁」でいい
  - あけることが必要だから「ドア」
  - ドアを開ける＝延焼のリスク
- Firewall = 検問所
  - セキュリティポリシーの異なるネットワークを相互接続するためのセキュリティゲートウエイ
  - それぞれのポリシーを維持しながら通信する

ファイアウォールの仕事

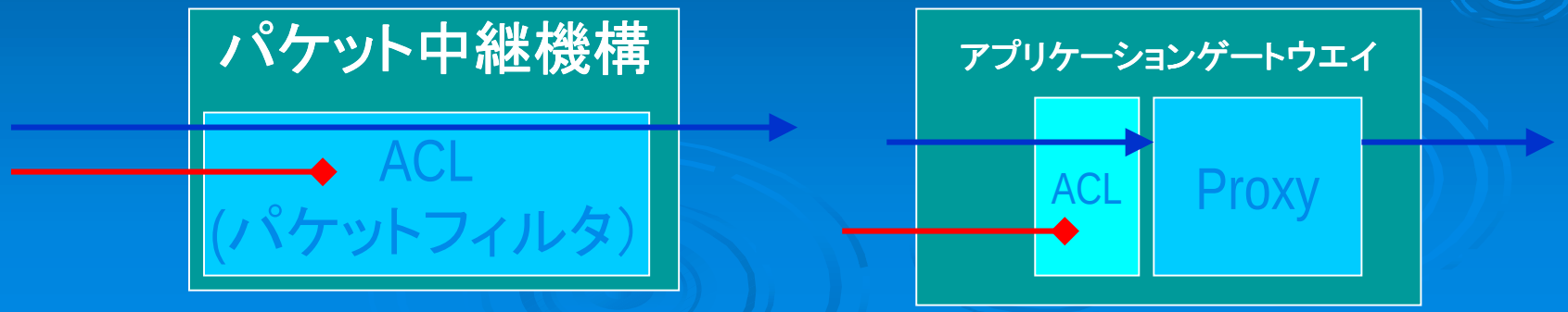
- 基本的な仕事（かならず備えるべき機能）
  - ルータもしくは中継装置としての仕事
  - 通過させていい通信かどうかの判断と通過させてはならない通信の排除
  - 危険な兆候の検出と警告
  - 通信の許可、不許可状況などの記録の保存

通信の中継機能

- 大別して2種類の方式がある
  - パケットフィルタ方式
    - ルータとしてIPパケットを中継することで、通信を行いたい機器同士が直接通信できる方式
  - アプリケーションゲートウエイ方式
    - Proxy（代理）サーバに一旦接続して、接続相手を指示して代理通信させる必要があるため、Proxy方式とも呼ばれる。
    - 直接的なパケット中継は行わず、要求を受けたProxyが相手方と通信して必要な情報を取得してから受け渡す方式。（通信のターミネーション（終端）を行う）

通信の許可、不許可

- 通信の発信元、相手先のIPアドレスやポート番号で許可、不許可を判断
  - ACL（Access Control List) の適用
    - パケットフィルタ方式では、フィルタ定義としてACLを適用する。
    - アプリケーションゲートウエイ方式では、Proxyサーバごとにアクセス許可情報としてACLを適用。



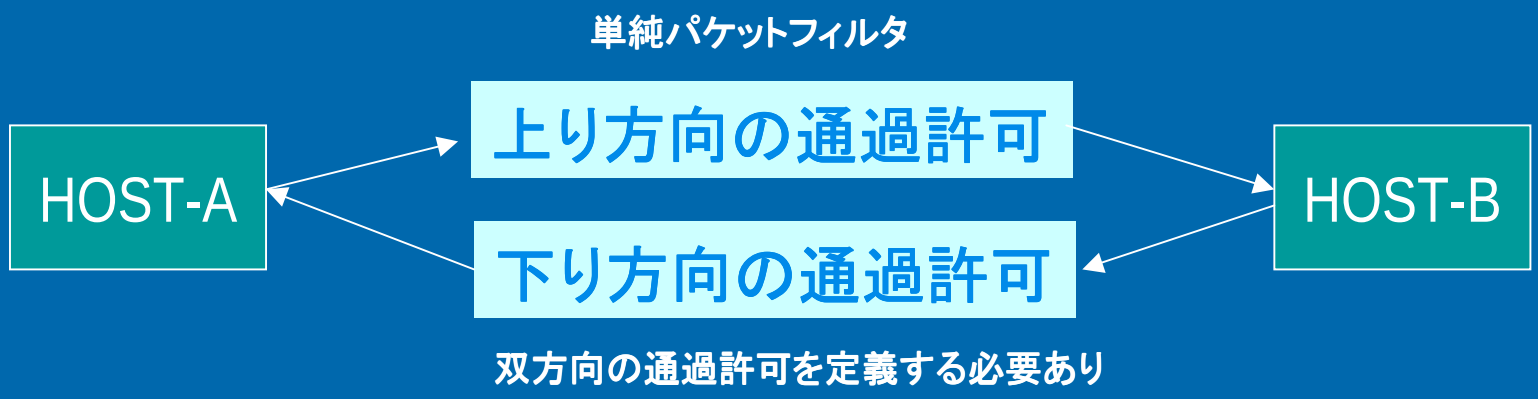
ファイアウォール関連用語・概念

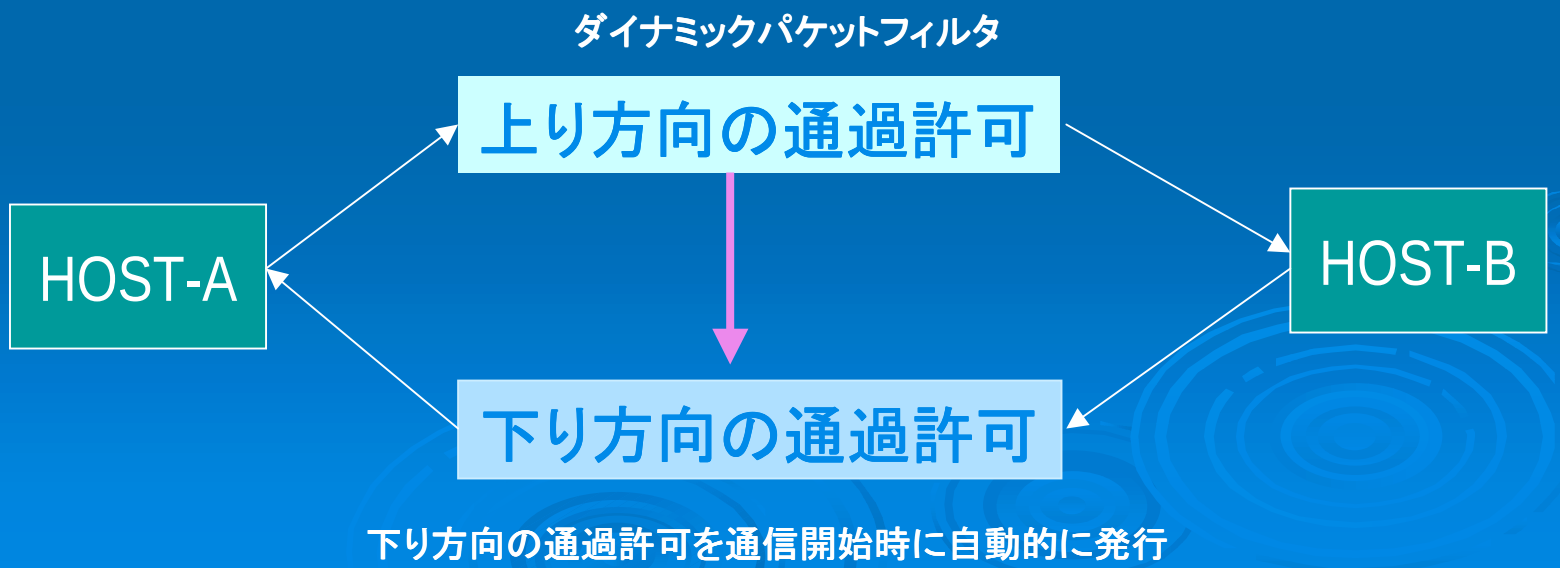
- ダイナミックパケットフィルタ
  - (類)ステートフルインスペクション
- NAT (Network Address Translation)
  - (類) IP Masquerade，NAPT，PAT etc.
- DMZ (De-Militarized Zone)
- VPN (Virtual Private Network)
  - IPSec, L2TP etc.

ダイナミックパケットフィルタ

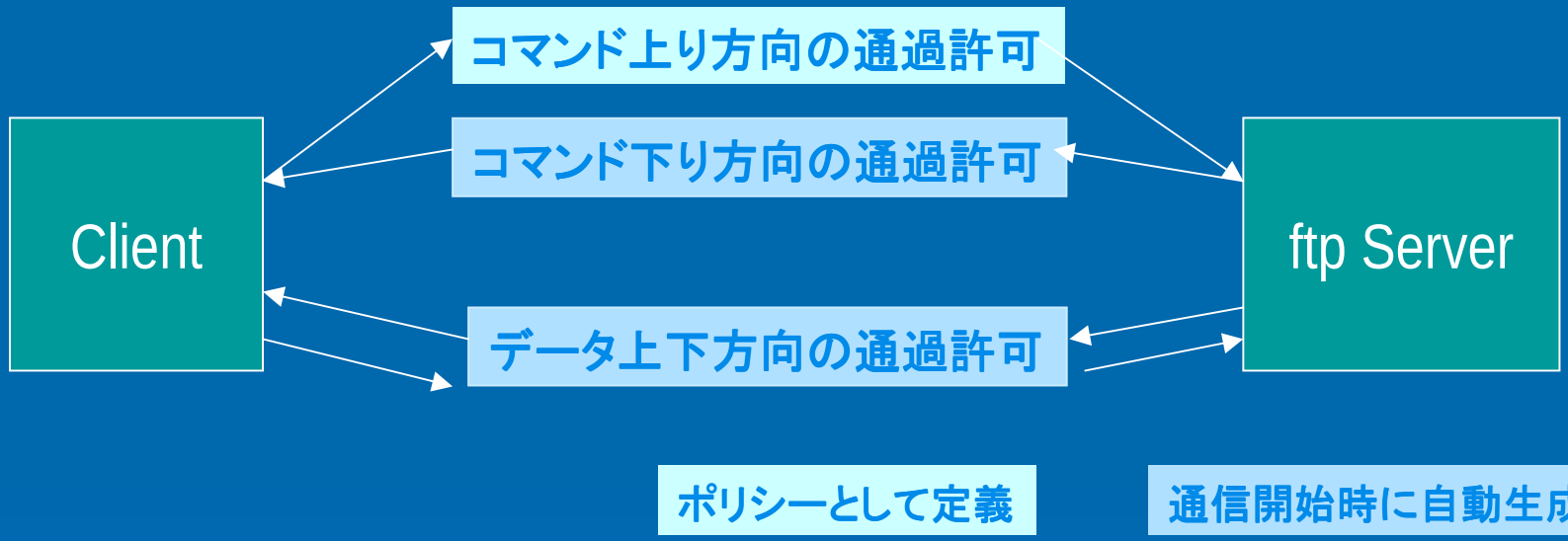
- ファイアウォール製品とルータのフィルタ機能の最大の相違点
  - 通過を許可した通信パケットへの応答や付随する他のセッションなどを総合的に管理、自動処理を行う。
  - ポリシー設定を単純化できる。（許可するセッションの方向のみ定義）

単純パケットフィルタとの比較





FTPの場合のダイナミックフィルタ



FTP の通信は2つのコネクションから構成される。データコネクションの開設や使用するポート番号は、コマンドコネクション内でネゴされる。また、データコネクションはデータ転送のたびに新しいコネクションが生成される。

ダイナミックフィルタの特徴

- 1コネクションのみで構成される通信は確実に対応可能
- 複数コネクション／セッションから構成される通信は対応できないものあり。（ストリーミング系の通信など）

ステートフルインスペクション

- Checkpoint社オリジナルの用語
  - 本来は、単なるパケットヘッダのみのチェックではなく、アプリケーションレイヤまで、プロトコルをデコードして細部の検査ができる方式のこと。
  - 一般にはダイナミックフィルタと同義に使用されることが多い。C社以外のファイアウォールの場合、厳密にはこの言葉に該当しないものが多いが、ステートフルと称することが多い。

NAT, IP Masquerade, Etc.

- 内部アドレスにプライベートアドレスを使用したネットワークとインターネットの境界にファイアウォールを置く場合に必須。（除く、アプリケーションゲートウエイ型F/W）
- プライベートアドレスネットワークを起点とする通信がファイアウォールを通過する時点で、発信元をグローバルアドレスに変換する。

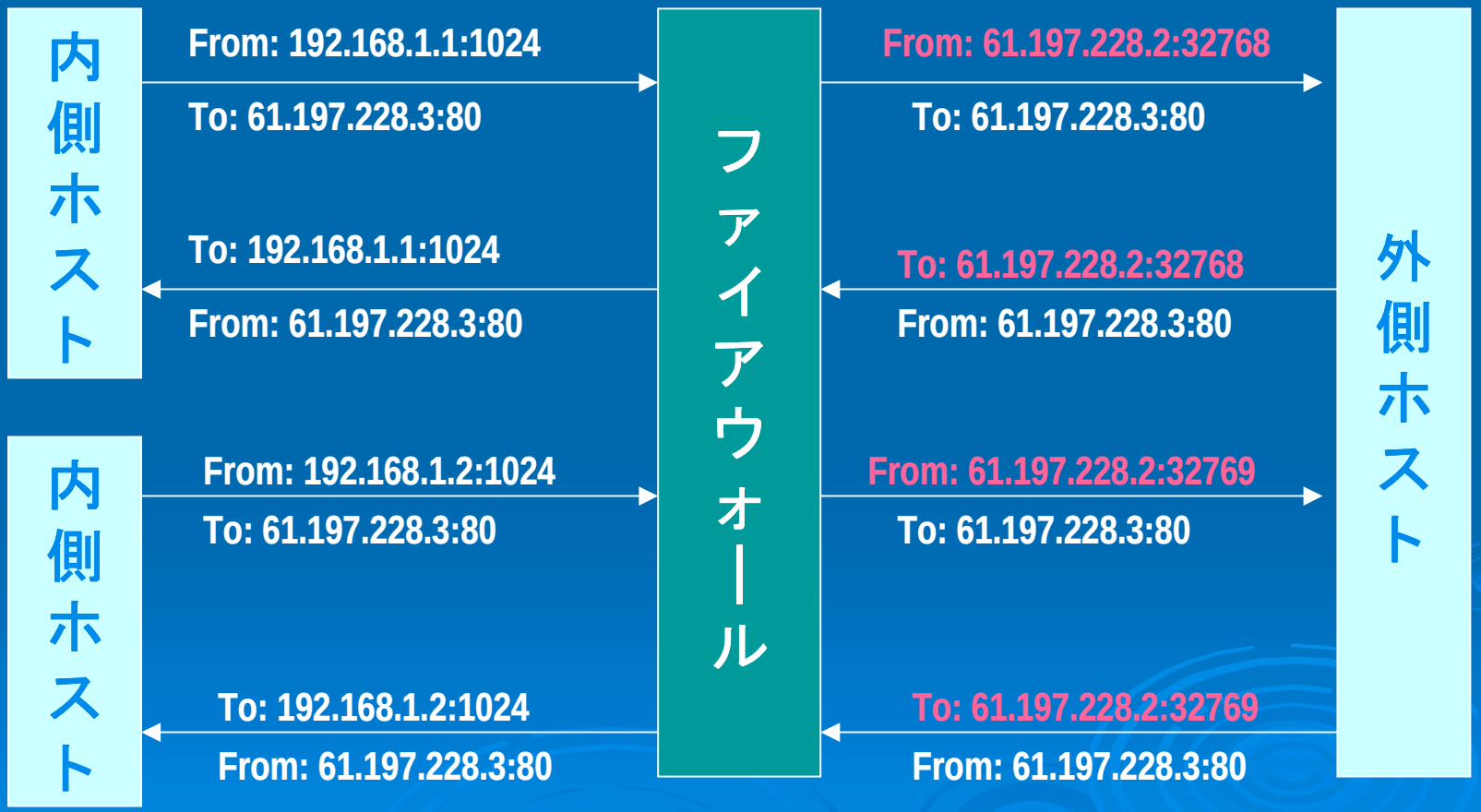
NAT(RFC1631)

- グローバルアドレスプールからアドレスを割り当て。
- 内部側ホストが外部と通信する際にプールからアドレスを一次的に割り当てて、アドレスを変換
- 同時通信数はグローバルアドレスの数に制約される
- 主に双方向通信を行う場合に利用

IP Masquerade, NAPT,PAT

- 1個もしくは少数のグローバルアドレスを多数の内部ホストで共有
- アドレス変換後のセッションが重複しないように発信元のポート番号も含めて変換
- 利用可能なポート番号数×アドレス数分の同時セッションをサポート
- 一部のプロトコルに対応が困難
- 外部からの着信は不可

IP Masquerade



NAT使用上の注意点

- 複数のコネクションを使うプロトコルで対応できない可能性がある。（ダイナミックフィルタと同様の理由）
- データとしてIPアドレスを受け渡すようなアプリケーションの動作を保証できない。（FTPなどは一般に対応されているが、新しいアプリケーションでは未対応のものも多い）
- パケットヘッダの改ざんチェックを行うようなプロトコルに対応できない。（IPSecなど）

サーバ保護とDMZ

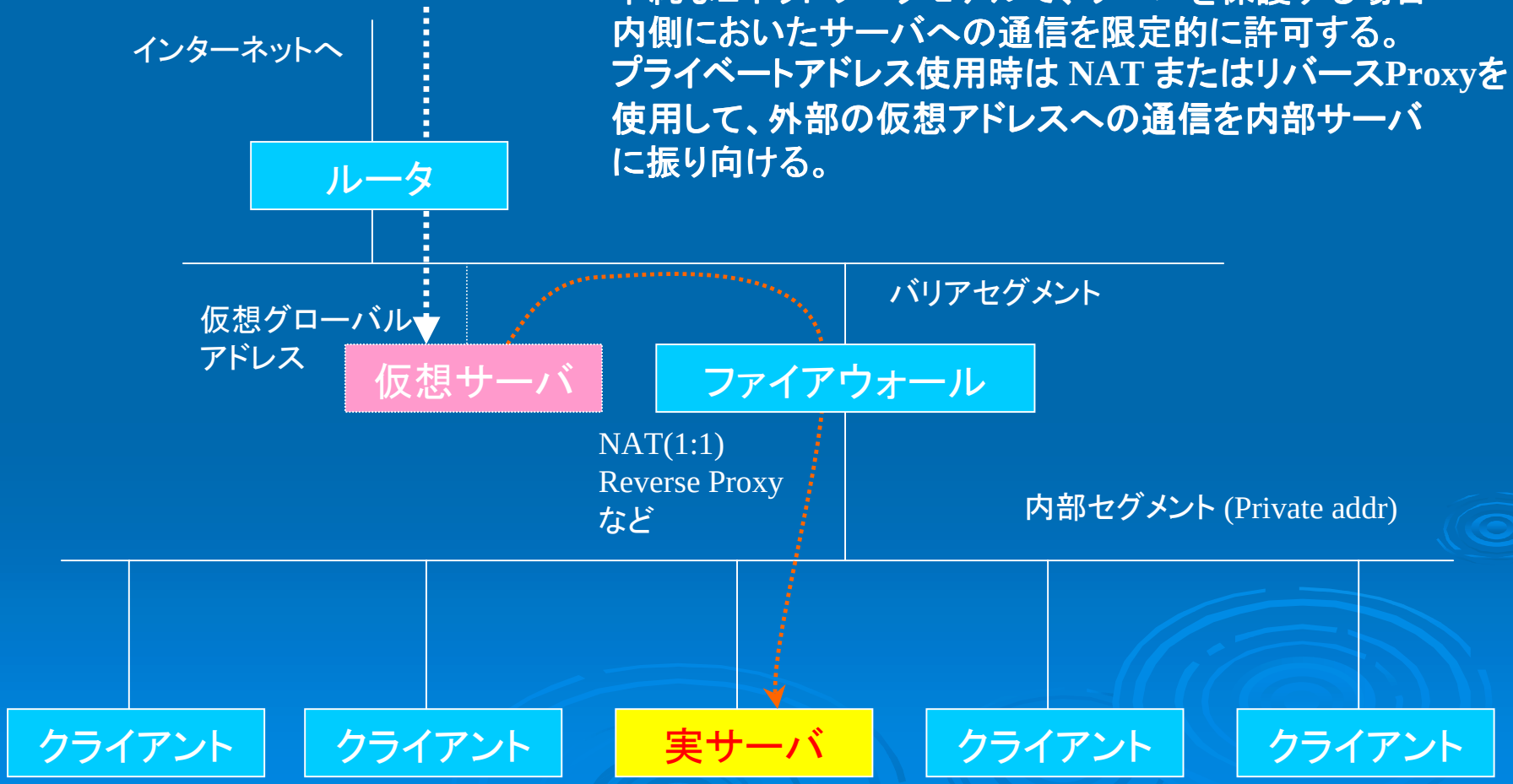
- DMZの意味合い
  - もともとは軍事用語
  - De-Militarized Zone = 非武装地帯（直訳）
  - 直接侵入を防ぐための「緩衝地帯」的意味合いが強い（決して「非武装＝無防備」ではない）
  - ファイアウォールの限界ゆえに・・・・

公開サーバの保護

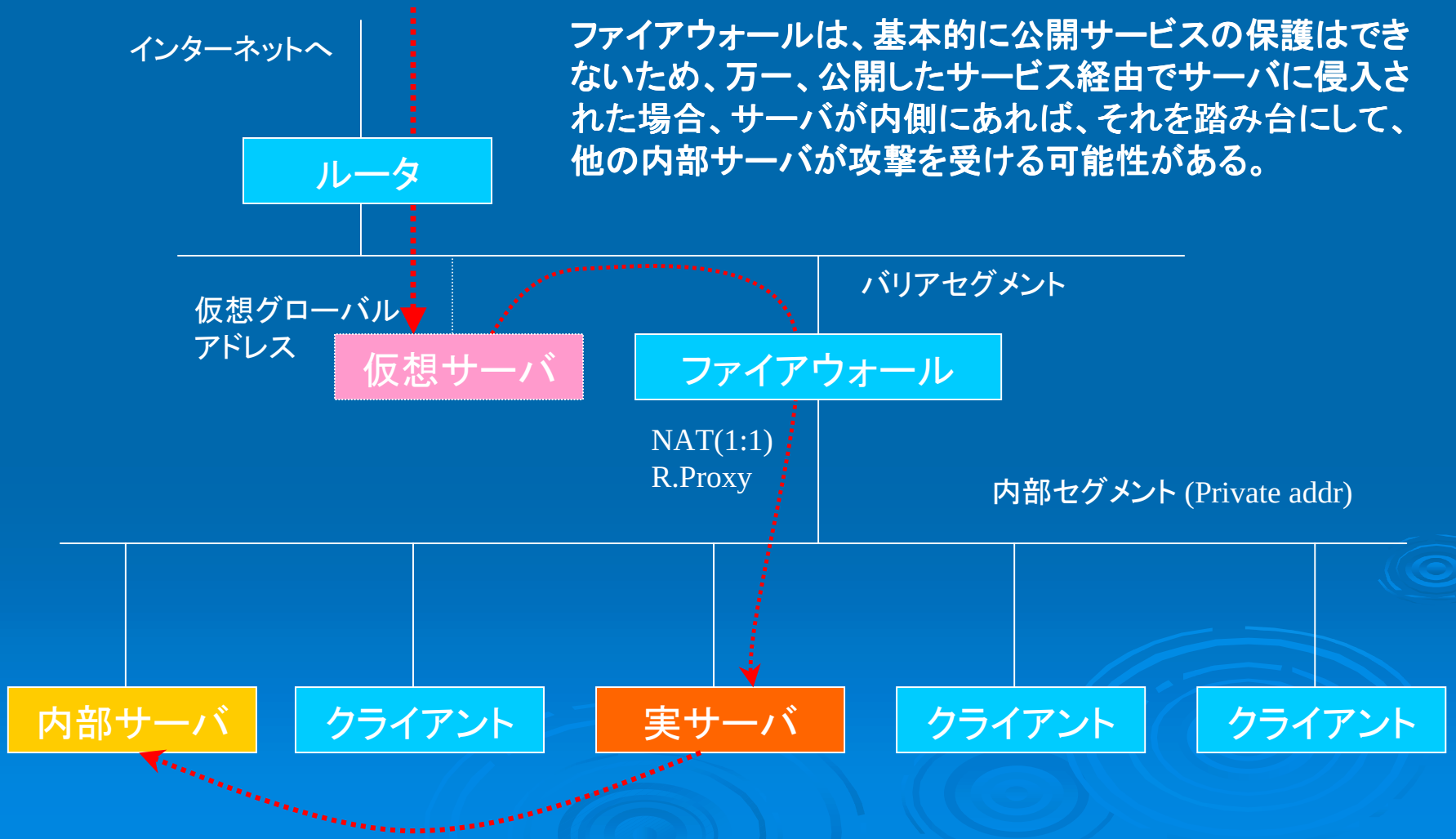
- サーバをファイアウォール下に配置
- 外部からサーバに対して、公開するサービス以外へのアクセスを禁止
- しかし、公開サービスは通さねばならない
  - サーバの公開サービスに脆弱性があると、攻撃、侵入の可能性がある。
  - これをファイアウォールで防ぐことは難しい

単純な保護モデルの場合

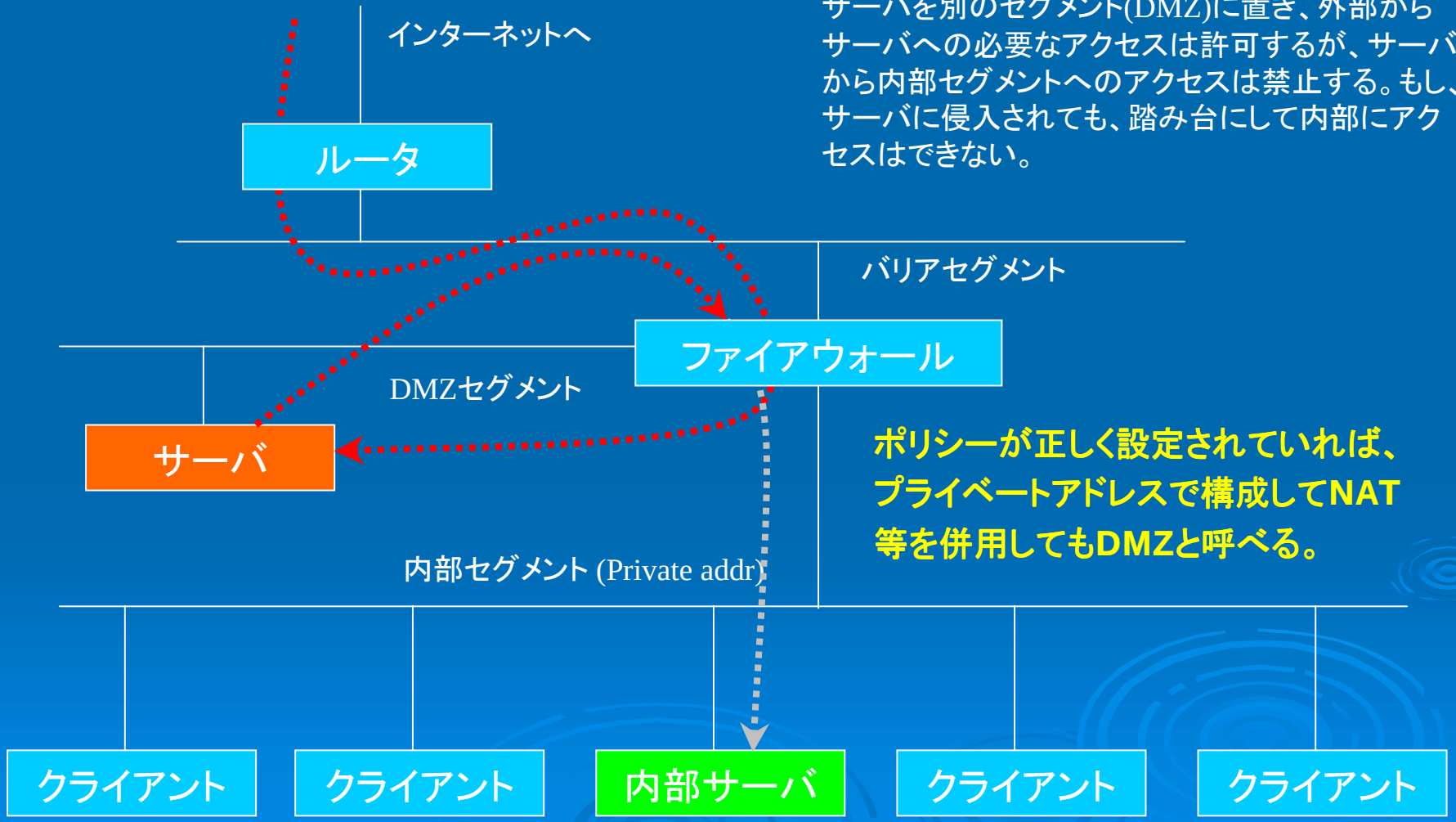
単純な2ネットワークモデルで、サーバを保護する場合
内側においたサーバへの通信を限定的に許可する。
プライベートアドレス使用時は NAT またはリバースProxyを
使用して、外部の仮想アドレスへの通信を内部サーバ
に振り向ける。



単純モデルで攻撃を受けたら



DMZモデルの場合



サーバを別のセグメント(DMZ)に置き、外部からサーバへの必要なアクセスは許可するが、サーバから内部セグメントへのアクセスは禁止する。もし、サーバに侵入されても、踏み台にして内部にアクセスはできない。

ポリシーが正しく設定されていれば、プライベートアドレスで構成してNAT等を併用してもDMZと呼べる。

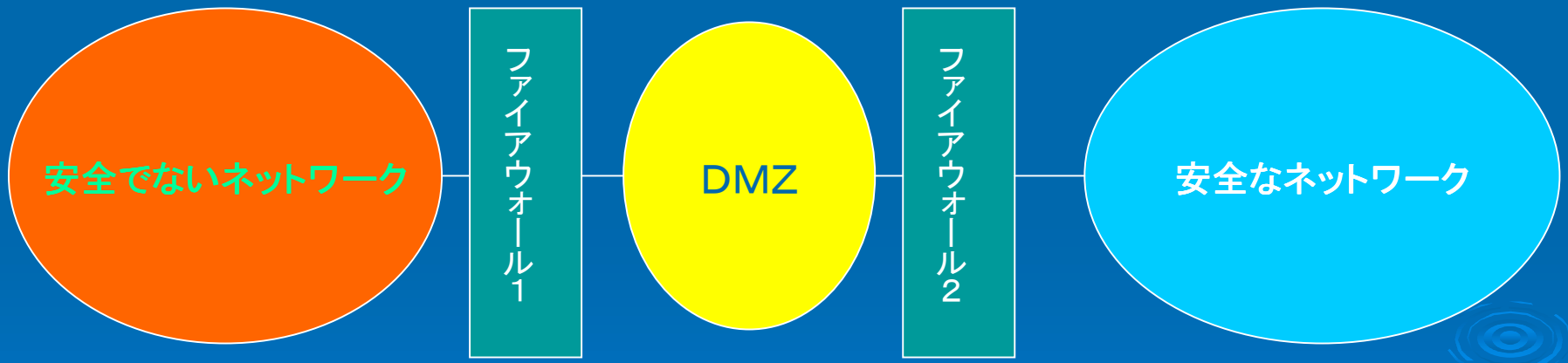
DMZを構成する意味

- **DMZは中間的な保護層**
  - 公開サーバ群をファイアウォールで保護し、必要以外のアクセスを排除する。
  - 万一、公開サーバが不正アクセスにより侵入されるなどの事態が生じても、そこから内部に直接入れないようにすることで、安全性の向上をはかる。（不正アクセスに対応する時間をかせぐ）
  - さらに、外部へのアクセスも制限することで、侵入されたサーバを踏み台にして外部を攻撃することも困難にする。（かごの鳥作戦）
  - 不正アクセスによって深刻な事態に陥るような重要なホストは置かない。

DMZ本来の形

外部→DMZ
必要なサービスへの
アクセスのみ通過

DMZ→内部
基本的に通過できな
いように設定。



外部←DMZ
基本的に通過できな
いように設定。どうし
ても必要なもののみ
通過。

DMZ←内部
必要なサービスへの
アクセスのみ通過

DMZを正しく理解するために

- DMZは「非武装=無防備」ではない
- 正しくポリシー設定しなければDMZではない
  - 外部からDMZへのアクセスは必要なものに限定
  - DMZから内部へのアクセスは原則不許可
  - DMZから外部へのアクセスも必要最小限に限定

VPNとファイアウォール

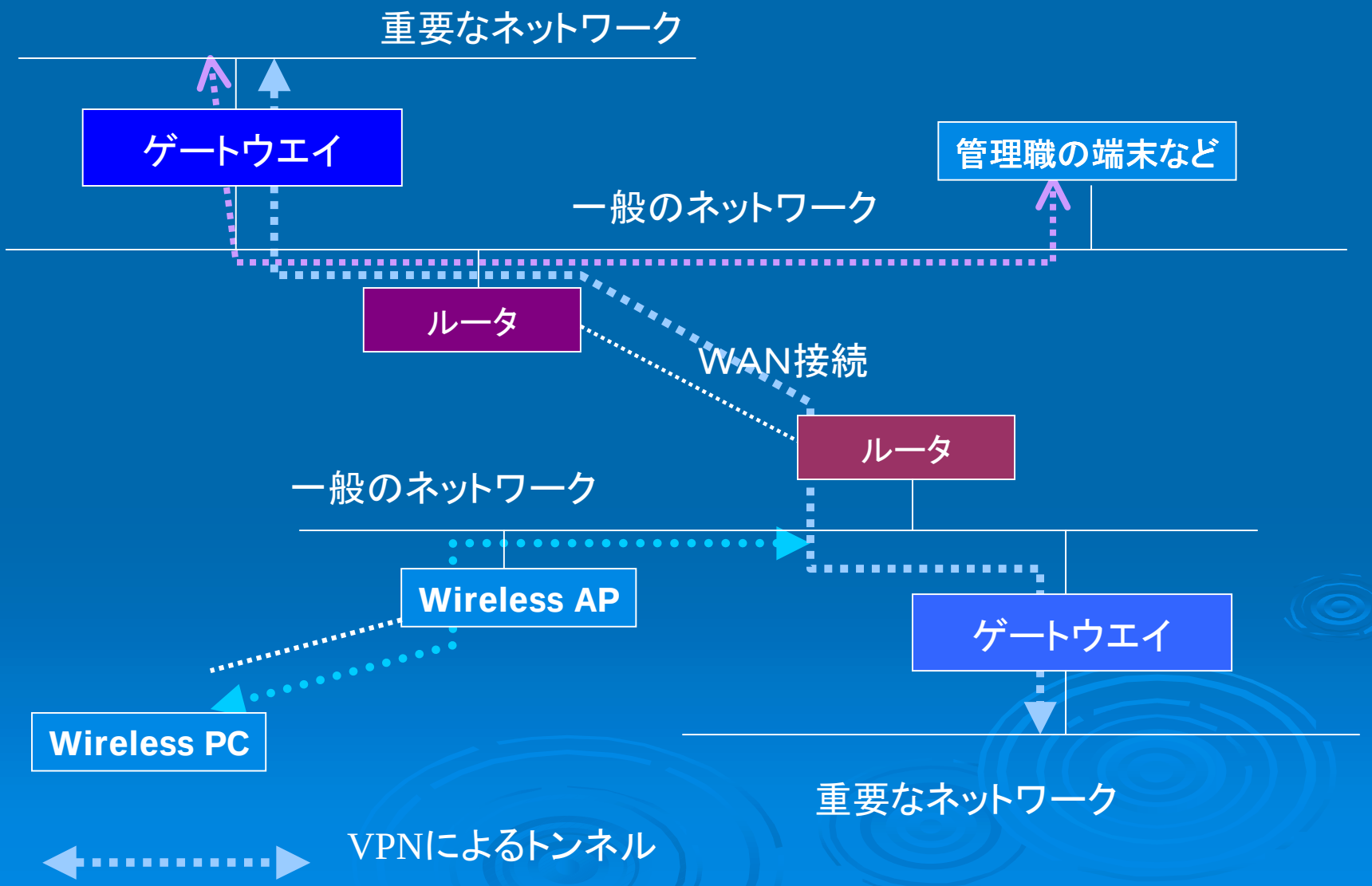
- VPNゲートウエイ機能
  - インターネットなどの安全でない（セキュリティポリシーの異なる）ネットワークを介して、安全にネットワーク間接続を行う。
  - VPNゲートウエイは相手側のネットワークに対するルータの役割をする。
  - ゲートウエイ間は暗号通信によって、通信の内容が保護される。
- セキュリティの観点から見ればファイアウォールに別のネットワークを追加接続したのと同じ意味合い。
  - 接続先ネットワークのセキュリティが破られれば、当然、リスクにさらされることに注意

VPNは「セキュリティ」ではなく「ネットワーキング」である

VPNの利用目的

- 同一組織のブランチ間のインターネット経由接続
  - 専用回線の代替えまたはバックアップ、回線費用の節約
- モバイルアクセスのコスト削減と安全性の確保
- 複数組織の協同ネットワーク（エクストラネット）構築
  - 回線費用の節約
  - インターネットの利用による柔軟性の確保
- 組織内のネットワークセキュリティーの階層的強化
  - 組織内 LAN のセキュリティー階層化
  - セキュリティーの低いネットワークを使って重要なネットワークを接続
  - ワイアレスLANのセキュリティ強化策

組織内でのVPN利用例



VPN利用時の注意点

- VPNは安全か？
  - 通信方式は安全でも、接続先によっては問題が生じることに注意（ポリシー設定や認証はきちんと行う必要あり）
- パケットサイズ（MTUまたはMSS）に注意
  - カプセリングを行うことで最大パケットサイズ(MTU）が実質的に減少するため、フラグメントが発生する可能性あり。
- NAT越えの場合、通信できない場合あり
  - IPSec の場合、特殊な方法（NAT Traversal）を使用する必要がある。

ファイアウォールの運用・管理

- ログは宝の山
  - 定期的な解析を・・・・
    - 異常ログの検査
    - 通信傾向の掌握（各プロトコルの利用状況など）
  - ファイアウォールのログだけでも・・・・・
    - 特定プロトコルセッションの異常増加→ワーム侵入？
    - 拒否ログの増加→ポートスキャンなどの偵察活動？
    - DMZ から外部への接続→サーバ上での不正行為？
    - などなど・・・・
  - 悪い人たちにとっても宝の山
    - データマイニングを行えば様々な情報が得られる可能性
    - 個人情報保護の観点からは？（今後の課題）

従来型の

ファイアウォールがもたらす安全とは

- 基本的にはIPアドレスやサービスをベースにした通信の到達性の制御
- つながるか、つないでいいかの制御
- つないだことの記録、つながなかったことの記録
- アクセスされる必要のないホスト、サービスに到達できなくなること。

従来型の

ファイアウォールが苦手なこと

- 通信内容の厳密なチェックと内容による通信制限
  - 特にパケットフィルタ系はこれが苦手（複雑な処理は負担が大きいため）
  - アプリケーションゲートウエイ系はこうしたことも可能だが、スピードはそれなり。
  - オール・イン・ワン型もあるにはあるが・・・・
  - 基本的に通過させたサービスに関する保護はサーバ側で行うのが基本となる

☺ちょっと休憩 ☺

セキュリティホール

- セキュリティ上の脆弱性（Vulnerability）
  - OSやサーバソフトウエアのバグによるもの
  - システムのミスコンフィグレーションによるもの
  - アプリケーションのバグによるもの
  - これらの設計ミス

セキュリティホールの影響

- システムへの侵入・乗っ取り
  - コマンド実行権、システム管理権限の奪取
  - 任意のコードの実行
- 情報窃取や改ざん、破壊
  - アカウント、パスワード情報の盗用
  - データベース上の顧客情報、業務情報の窃取
  - サイトの詐称やなりすまし、詐欺的行為
- サービス妨害行為
  - システムダウンを引き起こしたり過負荷を発生
  - ワーム、ウイルスの拡散

従来型の

ファイアウォールとセキュリティホール

- Web サーバの脆弱性への攻撃
  - ファイアウォールは TCP 80/443 を通過
  - 攻撃は許可されたポートを使って行われる
- たとえば以下のようなHTTPリクエストの中身まではほとんどの従来型ファイアウォールではチェック不可
  - GET /scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
  - GET /default.ida ? NNNNN…N %u9090…..%u00=a HTTP/1.0

侵入検知（Intrusion Detection）

- 攻撃を検出する手法
  - 攻撃コード（Exploit）の特徴（signature）を利用する方法
  - 脆弱性（vulnerability）自体の特徴（signature）を利用する方法
  - 不正な挙動（behavior)を検出する方法
    - 利用ポリシーへの違反など
  - 統計的な異常（anomaly）を検出する方法
    - 日常とかけはなれたトラフィックの検出など

IDS（侵入検知システム）と問題点

- アラームの信頼度が低い
  - 特定の脆弱性や攻撃コードの特徴検出
    - Signature の構成やチェックの深さによっては「誤認」「見落とし」が生じる
    - 攻撃であっても「有効」なものかどうかの判断ができない。（ノイズ的アラームが多い）
  - 統計的異常の検出
    - 確率的（非確定的）である
- アラームを受けたら行動を起こすのは人間
  - 誤報排除や緊急対応

ガートナーレポートの衝撃

Information Security Hype Cycle (2003/06)

- （ネットワーク型）IDS に将来はない
  - 多くのユーザはノイズ的アラームに辟易している
  - プロテクション機能が貧弱
  - もう誰も買わないだろう（投資に見合う効果なし）
- これからはファイアウォールの時代

「言い過ぎ」、ではあるが重要なポイントを含んでいるのは確か。

ファイアウォールという言葉自体の再定義が必要になる。

IDSの反省

- 誤認>=False Positives>=ノイズ・・・・
  - Stateful Signature の普及で「誤認」は減少
  - ノイズは、他のシステムとの連携で解消
    - 脆弱性検査ツールのデータを元に有効な攻撃のみを警告する
    - 統合的な監視システムを使い、他の機器（ファイアウォール、サーバ等）のイベント、ログとの関連づけによって有効な攻撃を判断
- 手間がかかる、後手にまわる・・・・
  - 自動プロテクション（Intrusion Prevention）機能

侵入検知・防御システム(IDPS)

- 検出したら止めてしまおう、という発想
  - 「誤認」の減少によって可能に
  - ノイズチューニングは不要（止めても問題なし）
- インライン型（ファイアウォール的）導入モデル
  - 従来のIDSのTCPリセットやFW連携機能では不十分
    - 単発パケットやTCP以外での攻撃を防御困難
    - インライン型ならば検査完了までパケットを保留しておける
  - ネットワークモニタはパケットロスを発生
    - インライン（ゲートウエイ）型は、全パケットをモニタ可能
    - 遅延やボトルネックの危険性とのトレードオフではあるが・・・・

これってファイアウォールじゃ・・？

- IDPSは一種のファイアウォール
  - 従来よりも、より深い検査が可能なファイアウォールと言える
  - 将来的にはファイアウォールに取り込まれるべき機能とみるべき？
    - ガートナーが言う「ファイアウォール」の形
    - 性能とのトレード・オフ問題は？（MPU高速化やASIC処理によるH/W化で克服可能？）
    - 障害耐性問題は冗長化による対応で充分か？
    - 基幹部分は従来型、内部サブネットやDMZ保護はIDPS機能付きという使い分けも

IDPSの製品例

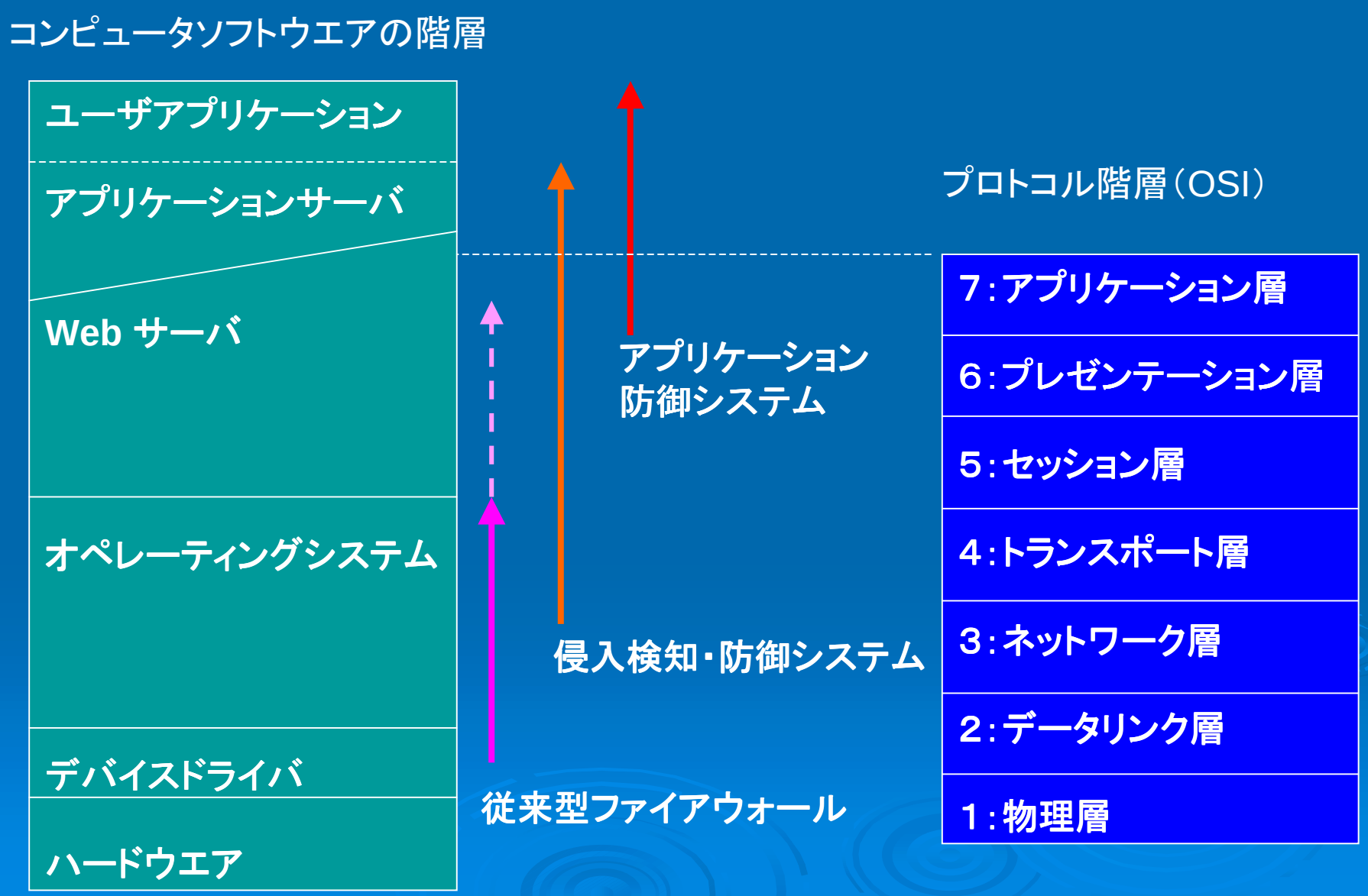
- NetScreen IDP (旧 One Secure）
- Intruvert (Network Associates) IntruShield
- TippingPoint Unity One
- Intrusion Inc. SecureNet

＊ Network IDPS で、私自身が興味をひかれたもので、有名、無名、実績の有無は関係ありませんので念のため・・・・

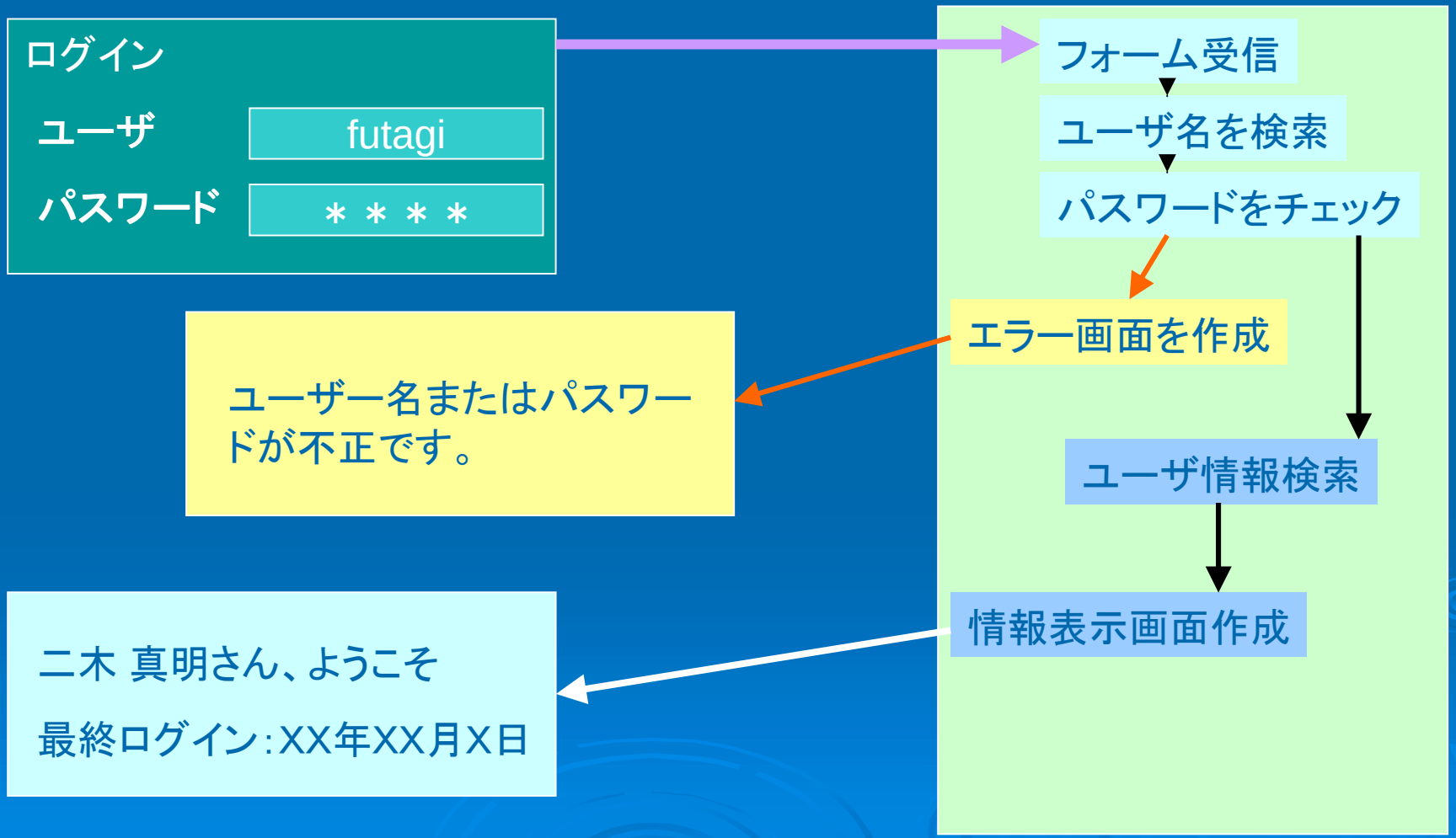
Beyond the IDPS

- それでもまだ、攻撃対象は残る・・・・・・
  - たとえば、Web アプリケーションには・・・・・
    - ソフトウエアだから、バグはある・・・・・・
    - 設計ミスだってある・・・・・・
    - コンフィグレーションミスだってある・・・・・・
    - 思わぬ裏口だってある・・・・かも・・・・
  - つまり攻撃可能なセキュリティホールはまだ存在する
    - IDPS では、ユーザアプリの脆弱性までは面倒みきれない
- 「Layer 7対応プロテクション」では不十分？
  - Layer 7の意味は？（プロトコル？、アプリケーション？）

プロトコル階層とソフトウエア階層



Webアプリケーションの仕組み



Webアプリケーションの処理

- 処理すべきデータの受信
  - フォームの受信（GET/POST）
  - URL 引数による受け渡し
  - アプレット、スクリプト処理による受け渡し
- 応答ページの作成
  - 入力データに対する処理（検索、その他のデータ処理の実行）
  - 入力データもしくは処理結果を使って応答ページ（HTMLデータ）を作成、クライアントに送信

危険が生じるポイント

- 入力データの利用方法に注意
  - 入力データの一部を応答ページになんらかの形で転記する場合。
  - 入力データを検索条件にしてデータベース等を検索する場合（SQLの構成）
  - 入力データを引数にして他の処理やコマンドを実行する場合
  - 入力データを使って、行う処理を選択する場合

たとえば・・・・

- 入力データを応答ページに転記
  - もし、入力データに<script …>….</script> などのHTMLタグが含まれていたら・・・・
- 入力データをSQL分の検索条件に使う場合
  - たとえば、”futagi’; -- “ というような値を入力データに与えたら、どんな動作をするだろうか。
- 入力データをコマンドの引数に使う場合
  - たとえば、”; rm –f /usr” などというデータを与えられても大丈夫だろうか・・・・

たとえば・・・・

- 隠し（hidden）パラメータを処理に使っている
  - フォームを保存し、パラメータを書き換えられて送信されても大丈夫？
- Cookie を認証に使っている
  - Cookie の内容を見られても大丈夫？
  - Cookie の内容を改ざんして送られても大丈夫？
- 古いページやデバッグ用ページが残っている
  - リンクされていなくても直接アクセス可能では？
  - 思わぬトラブルや不正アクセスの元凶に

手口のおさらい

- URL パラメータやフォーム
  - Hidden パラメータ、URLパラメータ改ざん
  - フィールドオーバーフロー
  - SQL インジェクション（フィールドへのSQLコマンドや記号の入力）
  - コマンドインジェクション（システムコマンドや記号の入力）
  - クロスサイトスクリプティング（HTMLタグやスクリプトの挿入）
- Cookie
  - 内容の窃取、改ざん
- 隠し（消し忘れ）ページ
  - ありがちな名前（debug, admin …..)で検索・・・・・など

アプリケーション攻撃対策

- 第一義的に、「修正する」こと・・・だが
  - バグはなくならないし、発見は難しい
  - 修正→テスト→リリースには時間がかかる
- 攻撃を食い止める方法は・・・
  - 対策は個々のアプリケーションに依存する
  - 通信の内容の細部までをチェックする必要

アプリケーションファイアウォール

- アプリケーション保護に特化したF/W
  - URLやフォームのようなアプリケーションに与えられるデータ、パラメータを監視
  - Cookie の監視、保護
  - SOAP/XMLなどの通信の監視
  - データベースへのリクエストの監視
- アプリケーションに対するIDPSとして機能。

アプリケーションファイアウォールの技術的困難さ

- 多種多様なアプリケーションへの対応
  - ページ、フィールドごとに監視・保護ポリシーが異なる
  - 設定が煩雑化しがち（サイトに依存して設定項目が多い）
- 性能面での問題
  - プロトコルの7階層の処理に加えて、さらに深いチェックが必要。ボトルネックになる危険性

問題点へのチャレンジ

- ポリシー、設定の煩雑化
  - アプリケーションの自動学習機能
    - 一定期間の通信監視によるもの（受動型）
    - アプリケーションスキャナによる調査（能動型）
- 性能面の問題
  - PCサーバH/Wの高性能化 （消極策）
  - ASIC等の専用H/W化 （積極策）

アプリケーションF／W製品例

- Sanctum AppShield
- KavaDo InterDo
- Teros Application Gateway
- NetContinuum NC1000

＊ アプリケーションFW で、私自身が興味をひかれたもので、有名、無名、実績の有無は特に関係ありませんので念のため・・・

ファイアウォーリングの意味

- セキュリティ境界（perimeter）を構成する
  - ネットワークレベルでの境界
  - サービスレベルでの境界
  - ユーザレベルでの境界
  - 機能レベルの境界
- ネットワークの検問所的な意味合い
- ネットワークごとの異なるポリシーを保証
  - 「必要な通信」を維持しながら、「不要、不正な通信」を排除する　→物理的な接続の維持と論理的な分離

繋ぐことの危険性

- 物理的に繋がっていることが「危険」なのか
  - 「危険」かどうかは「繋がり方」による！！
  - でも、なにがしかの「リスク」は増える
- 物理的に繋ぐことのリスク
  - ファイアウォーリングに関するリスク
    - ポリシー設定に不具合がある可能性
    - 通過させた通信に不正な内容が含まれる可能性
    - ファイアウォールに対する不正操作、攻撃の可能性
- 適切な管理を行うことでリスクは減らせる！

繋げないことの安全性への疑問

- 「思いこみの」危険
  - 繋がっていないから「安全」「大丈夫」と思っていないか？？
    - 不正なPCが接続されていたりしないか？
    - ワーム持ち込みなどの危険はないか？
    - 不正なブリッジが存在したりしないか？
      - LAN に接続中にダイヤルアップを起動したためBlasterを内部に入れてしまった例も・・・・・
    - 接続されているPC,サーバ、機器は物理的に保護されているか？

要は管理！！！

- 「~~繋いだから危険~~」、「~~繋がないから安全~~」
  - きちんと管理すれば繋ぐリスクはかなり軽減できる。
  - 繋いでなくても管理が杜撰ならば「危険！」
  - 最終的には繋ぐメリット／必要性とリスクのバランスで判断

まとめ

- ファイアウォール（概念）は進化する
  - ネットワークファイアウォール
  - IDPS
  - アプリケーションファイアウォール
- ファイアウォールは「繋ぐ」道具
  - 安全に繋ぐには、きちんとした管理を
- しかし、なお・・・
  - ファイアウォールは万能の盾にあらず！！

お疲れ様でした

- 参考資料・文献
  - ファイアウォール構築（オライリー・ジャパン）
  - Web Hacking（Addison　Wesley）
  - Hacking Exposed（Osborne / McGraw-Hill)
  - 過去のIWチュートリアル資料など
    - http://www.kazamidori.jp/SECURITY/index.html

    - futagi@kazamidori.jp