ファイアーウォール

reimei

ファイアーウォールとは

- 複数のネットワークセグメント間で、予め設定されたルール(ACL)に基づいてパケットを中継したり、破棄したりする機能を持つアクセス制御製品
- 火災の時に被害を最小限に食い止める防火壁のような役割を果たすことから、外部のネットワークからの攻撃や不正なアクセスから自分たちのネットワークやコンピュータを制御するためのソフトウェアやハードウェアをファイアーウォール(以後FW)と呼ぶようになった
- IPS, WAFなどの登場によりFWの概念が拡大
  ネットワークFW: 従来のFW
  アプリケーションFW: WAFなどの特定のアプリに対して機能するFW

https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/basic/structure/01.html#:~:text=%E7%81%AB%E7%81%BD%E3%81%AE%E3%81%A8%E3%81%8D%E3%81%AB%E8%A2%AB%E5%AE%B3,%E3%82%88%E3%81%86%E3%81%AB%E3%81%AA%E3%82%8A%E3%81%BE%E3%81%97%E3%81%9F%E3%80%82

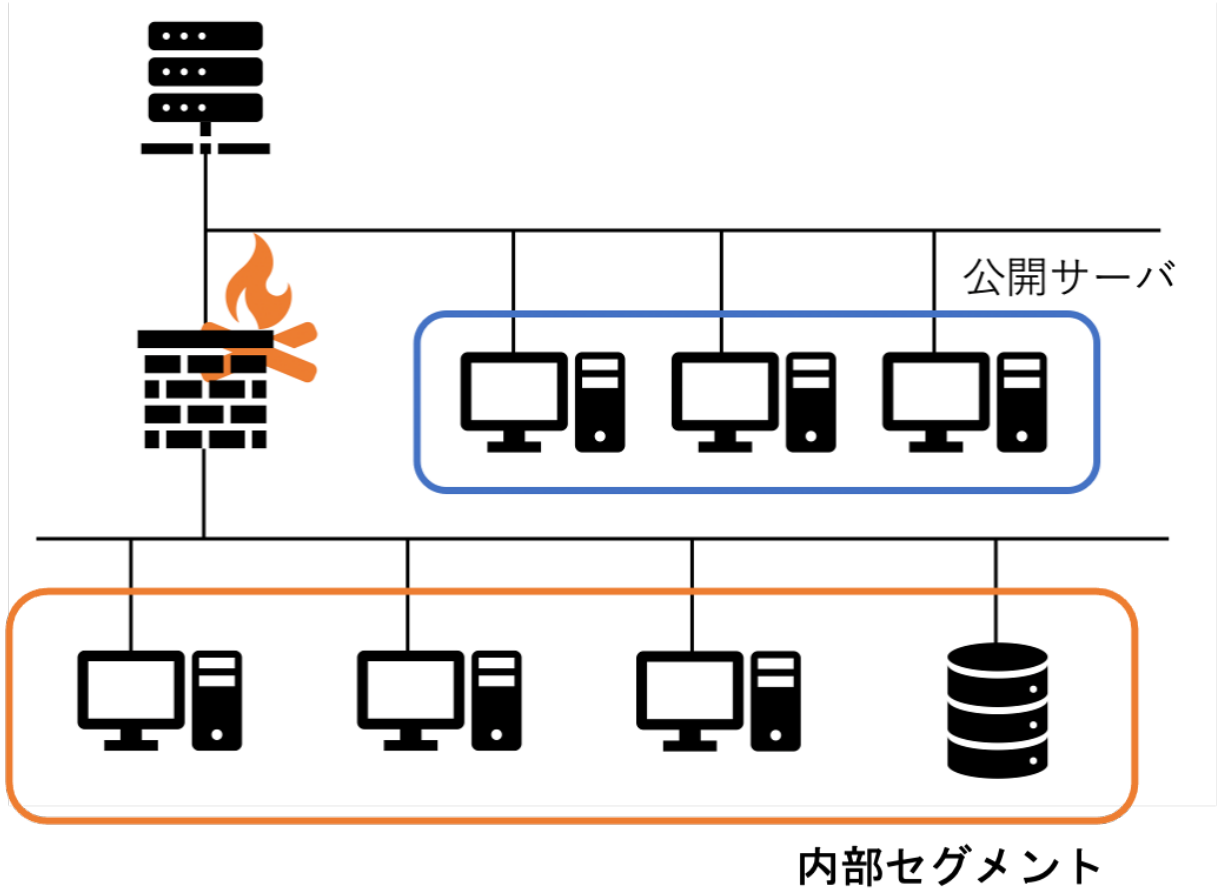
FWの役割

- 元々インターネットからの不正アクセスや攻撃など、インバウンド方向のパケットから組織内のネットワークを守る「盾」
(完全な盾ではなく、HTTPやSMTPなどを通すためにいくつか穴の開いた盾)
- 悪質なマルウェアや不正なプログラムをダウンロードさせるサイトの増加により、インバウンド方向だけでなくアウトバウンド方向のパケットについてもフィルタリングすることが重要な役割
- つまり、現在は「盾」というより「フィルタ」
- 他にも、インターネットから自社のサイトへの快適なアクセスや組織内からの快適なインターネット利用環境を常時提供する可用性の面でも重要な役割

FWの基本構成

1. 公開サーバをバリアセグメント(インターネット側セグメント)に接続

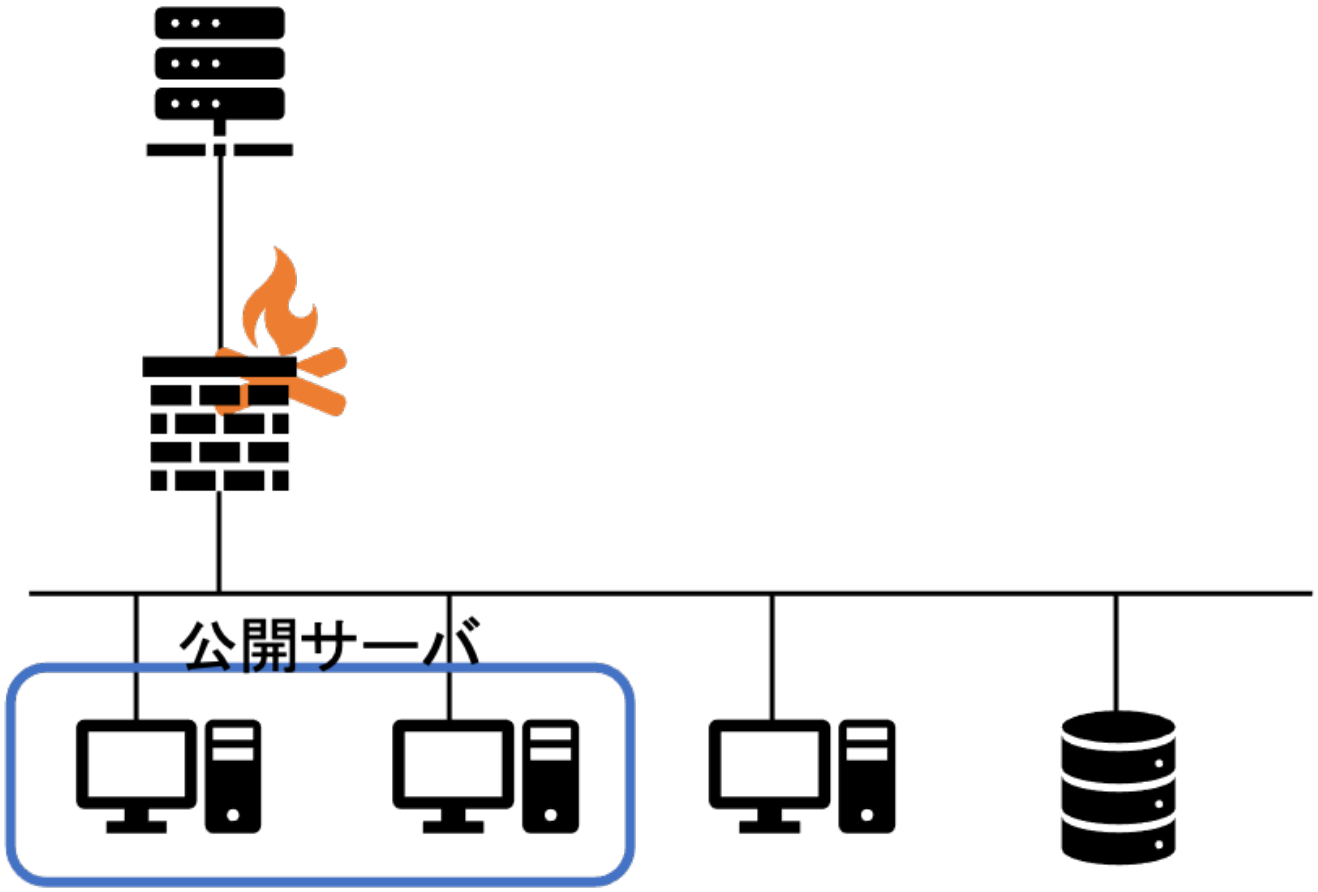
- FWによってインバウンド方向のパケットを全て遮断することが可能
- バリアセグメント上の公開サーバから内部ネットワークへのアクセスについては一部許可(必要最低限)
- FWは公開サーバへの攻撃や不正アクセスについては一切防ぐことは不可
- アウトバウンド方向への各種プロトコルが許可されているため、内部に侵入したマルウェアによってC&Cサーバなどへの不正な通信が行われる可能性あり



FWの基本構成

2. 公開サーバを内部ネットワークに接続

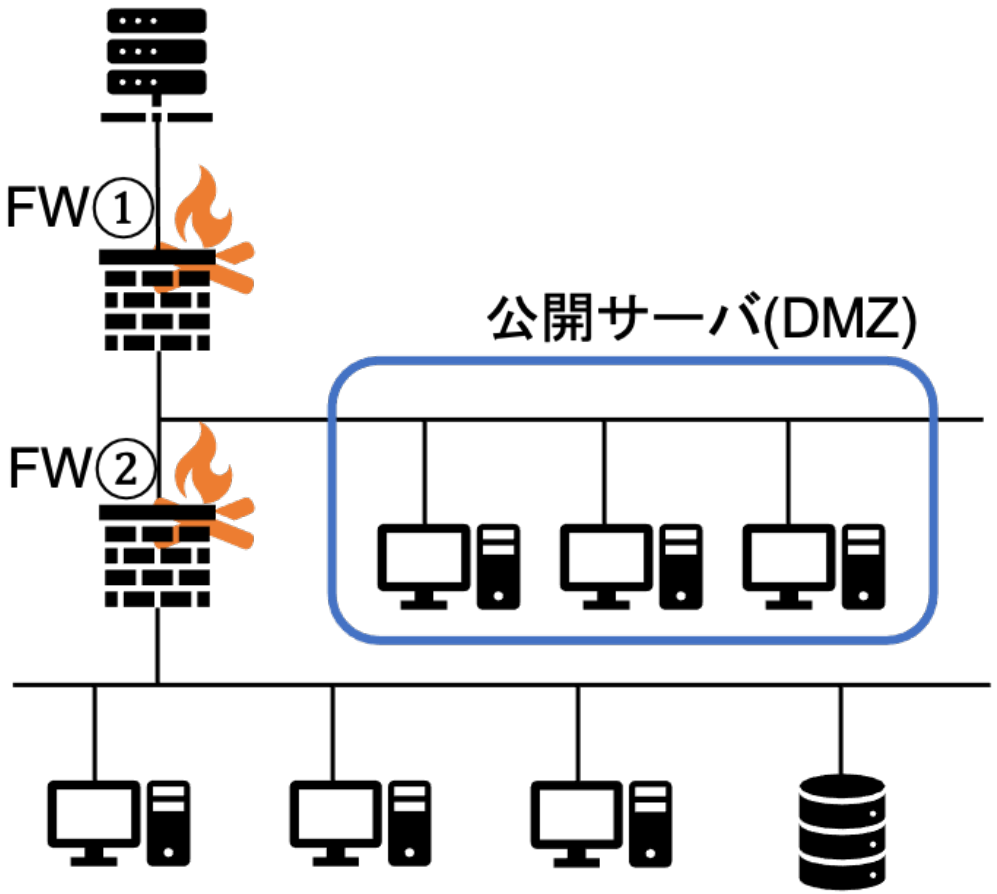
- FWによって公開サーバへのアクセスを最小限のサービスのみに制限可能
- インターネットから内部ネットワークの公開サーバ以外のホストへのアクセスは全て遮断可能
- 公開サーバのOSやアプリケーションの脆弱性により、同サーバへの侵入を許してしまうと、そこを経由して内部ネットワークの他ホストまで被害が及ぶ可能性あり
- 内部からインターネットへの各種プロトコルが許可されているため、内部に侵入したマルウェアによってC&Cサーバなどへの不正な通信が行われる可能性あり



FWの基本構成

3. 2台のFWに挟まれたDMZに公開サーバを接続

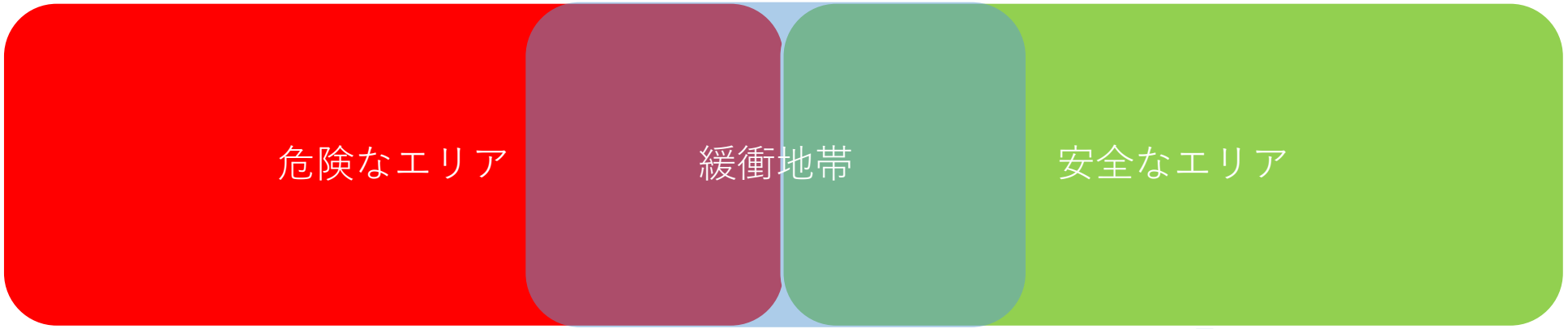
- FW1によって公開サーバへのアクセスを最小限のサービスのみに制限
- FW1, 2によってインターネットから内部ネットワークへのアクセスを全て遮断
- DMZから内部ネットワークへのアクセスは最小限のサービスに制限
  → 公開サーバに侵入されても内部ネットワークまで侵入される可能性を最小限に留めることが可能
- FW1, 2を別ベンダの製品や別のフィルタリング方式にすることでFWのバグなどによって内部ネットワークに侵入される可能性を最小限に留めることが可能
- 内部からインターネットへのHTTP, HTTPSが許可されているため、侵入したマルウェアによってC&Cサーバなどへの不正な通信が行われる可能性あり



DMZとは？

- DeMilitarized Zone 非武装地帯
- 危険なエリア(インターネット)と安全なエリア(内部ネットワーク)の中間にある「緩衝地帯」
- 危険な場所のそばに大切なものを置くのは危ないから、トラブルが起きても大丈夫なように緩衝地帯を設けて、そこには大切なものは置かない

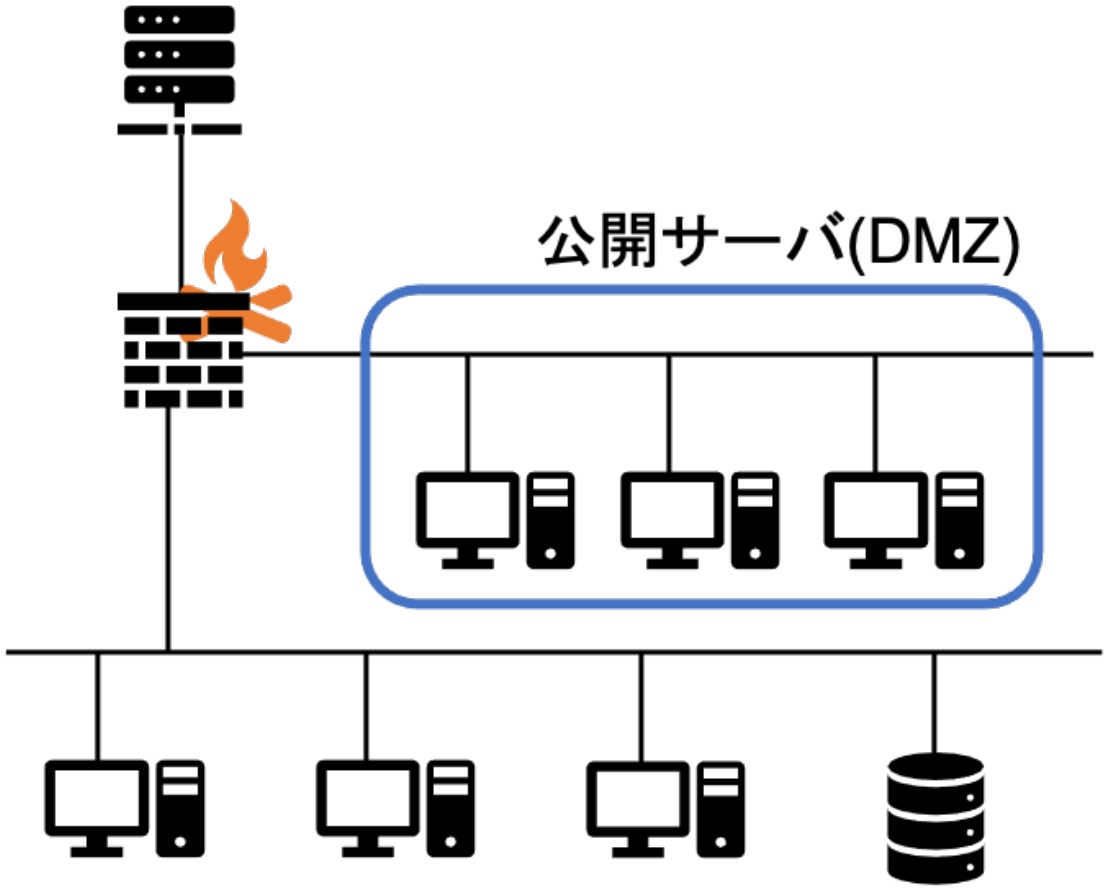
https://www.sbbit.jp/article/cont1/37677



FWの基本構成

4. FWに設けた第三のセグメントに公開サーバを接続

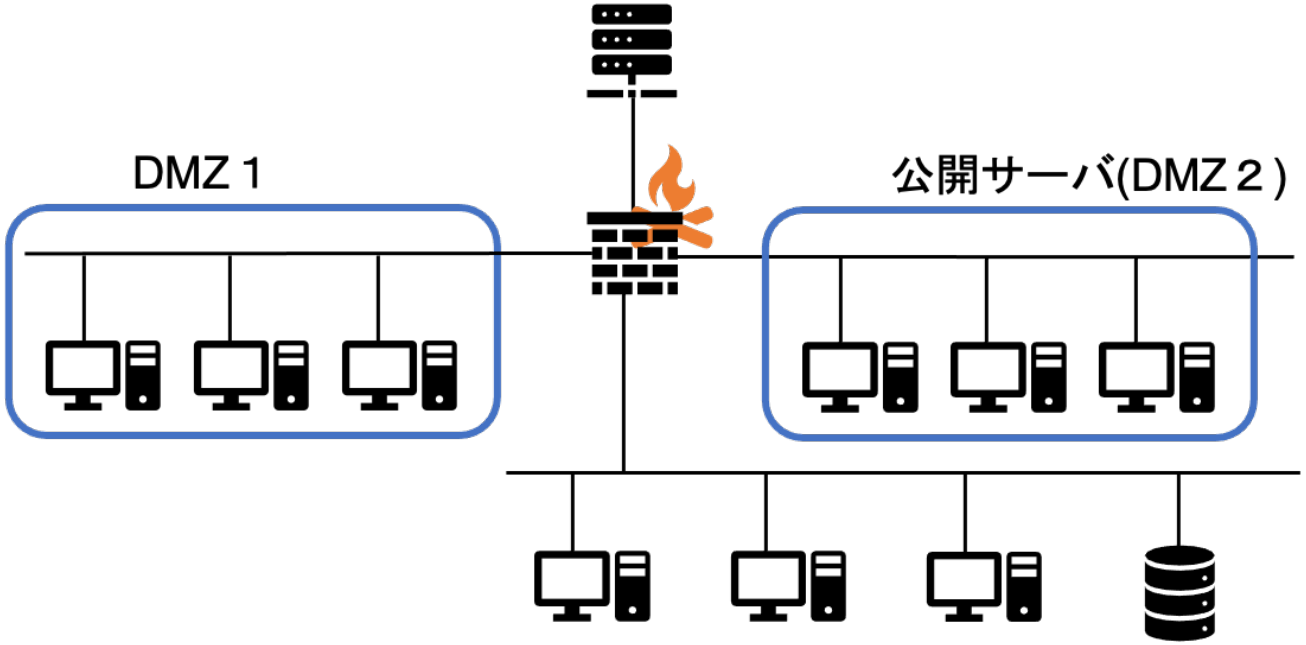
- 公開サーバへのアクセスを最低限のサービスのみに制限
- インターネットから内部ネットワークへのアクセスは全て遮断
- DMZから内部ネットワークへのアクセスは最小限のサービスに制限
  → 公開サーバに侵入されても内部ネットワークまで侵入される可能性を最小限に留めることが可能
- 内部からインターネットへのHTTP, HTTPSが許可されているため、侵入したマルウェアによってC&Cサーバなどへの不正な通信が行われる可能性あり



FWの基本構成

5. セキュリティレベルに応じて複数のDMZを構成

- 各ホストの用途やセキュリティレベルに応じた最適なアクセス制御が可能となる他、特別な用途に用いられるホストなどを別セグメントに切り離すことで、ネットワーク全体のパフォーマンス向上や負荷分散が可能
- 内部からネットワークへの通信を全て遮断し、必ずDMZ1・DMZ2を経由させることで侵入したマルウェアがC&Cサーバなどと通信するリスクを低減することが可能

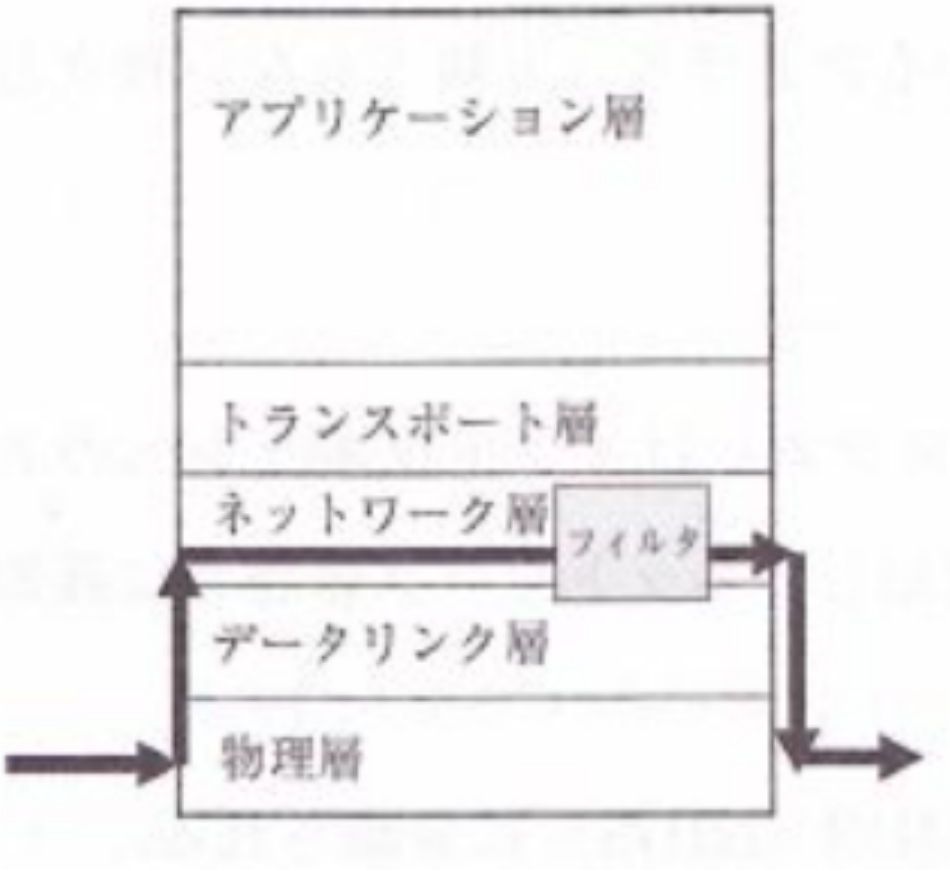


パケットフィルタ型

- 通信を細分化したパケットを監視するファイアウォール
- 通信をパケット単位で解析し、決められたルールに基づいて通過の許否を判断
- スタティックパケットフィルタ型・ダイナミックパケットフィルタ型・(ステートフルパケットインスペクション型)の三種類

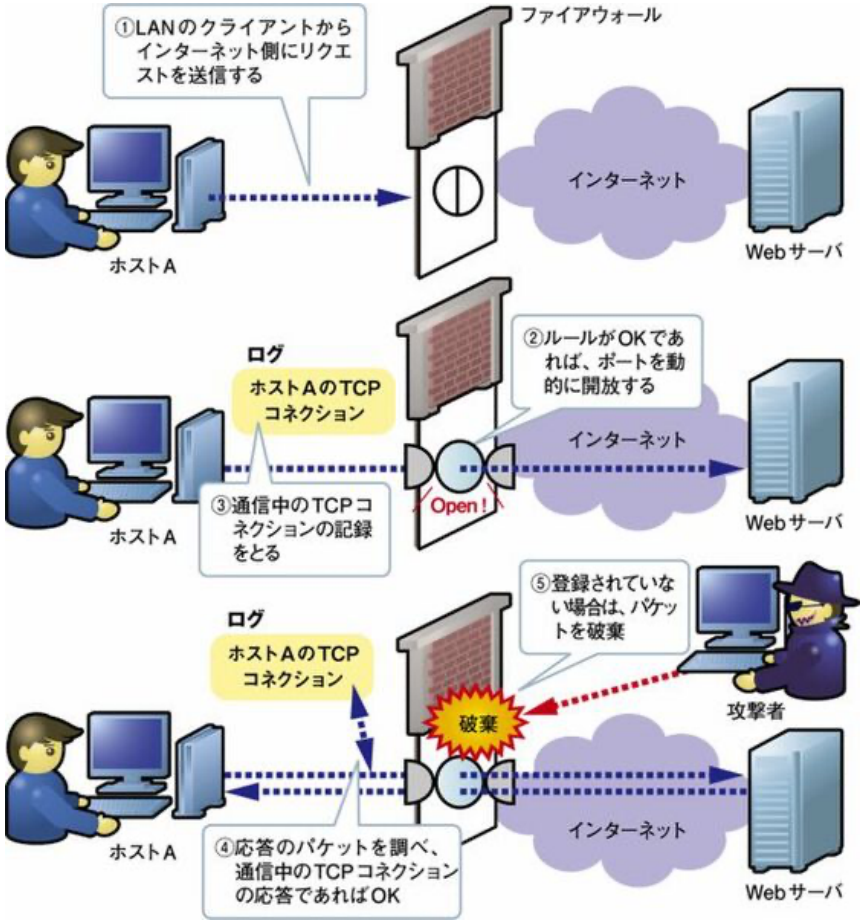
スタティックパケットフィルタ型

- ルータがベース
- パケットのヘッダ情報に含まれるIPアドレス、ポート番号などによって中継の可否を判断
- 発信元・送信先IPアドレス、プロトコル、パケットの方向、発信元・送信先ポートなどがフィルタリングの設定に利用可能



ダイナミックパケットフィルタ型

- クライアントとサーバのやりとりをファイアウォールが記憶し、動的にポートを開け閉めする
- コネクションを確立する方向のみを意識した基本的なACLを事前に登録しておき、接続要求があると、個々の通信をセッション管理テーブルに登録するとともに必要なルールが生成される方式



ステートフルパケットインスペクション型

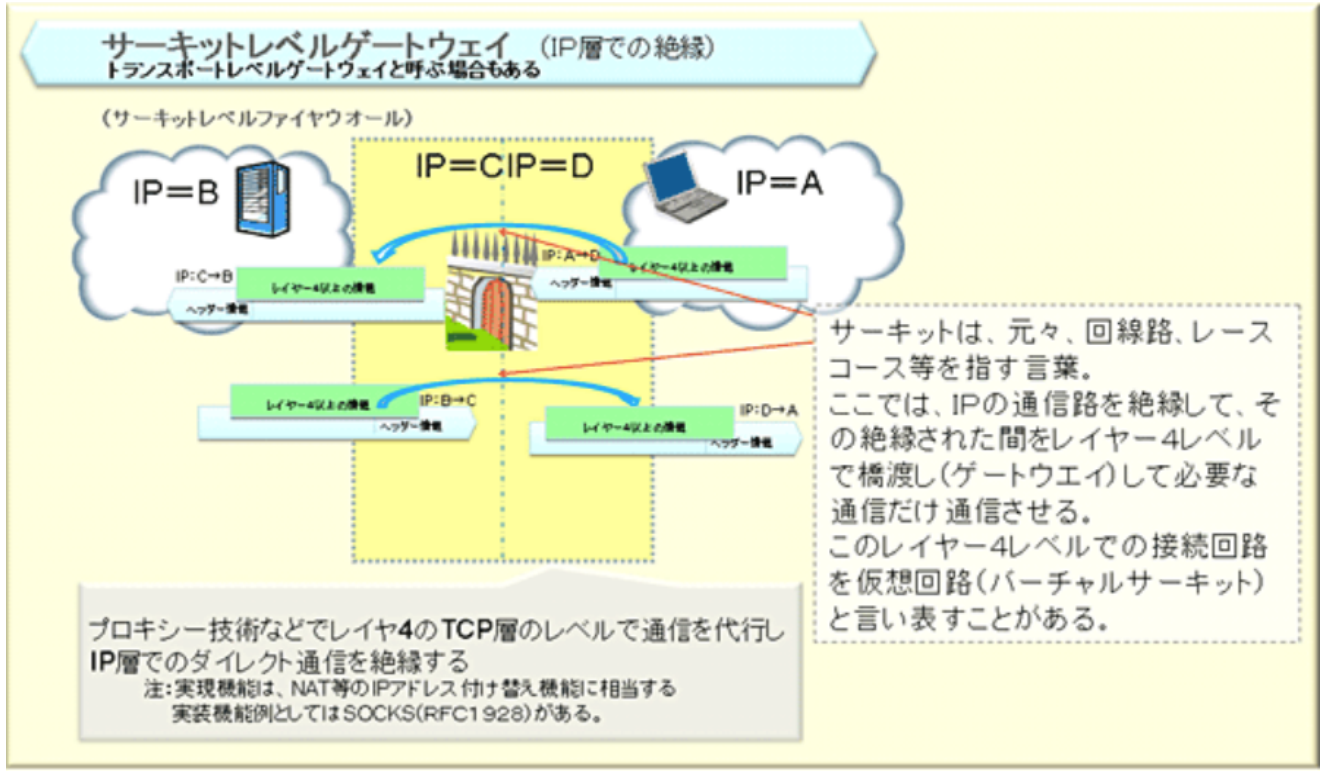
- ダイナミックパケットフィルタ型ファイアウォールとほぼ同じと考えて良い
- ダイナミックパケットフィルタ型ファイアウォールの方が広い意味

アプリケーションゲートウェイ型

- 通信の中身まで確認することができ、精度が高い検査が可能
- 読み込む通信量が多くなり、通信速度が遅くなるため注意が必要
- FWが内部ネットワークのコンピュータに代わり、外部サーバと接続しその通信内容を内部へと送る。
  → 内部ネットワークのコンピュータは直接外部と接触することはないため外部の不正攻撃から保護可能
- アプリケーション層のプロトコルごとに別々のプロキシを持つ
- プロキシ型とも呼ばれる

サーキットレベルゲートウェイ型

- アプリケーションゲートウェイ型と同様にクライアントからの接続要求をいったん受け取る
- アプリケーションゲートウェイ型とは異なり、目的のサーバに対してトランスポート層レベルでコネクションを確立してクライアントとサーバを結ぶ仮想的な通信路(バーチャルサーキット)を確立



FWで防御できない攻撃

- OS、プロトコル、ミドルウェアの脆弱性をついた攻撃
- Webアプリケーションプログラムの脆弱性をついた攻撃
- DoS系の攻撃
- マルウェアの侵入

OS、プロトコル、ミドルウェアの脆弱性をついた攻撃

[攻撃手法例]

- ポートスキャン
- BOF攻撃
- パスワードクラック
- プロトコルベースのセッションハイジャック

[対策]

- ホストの要塞化(堅牢な状態にすること)
- 脆弱性検査及び対策の実施
- IPSによる攻撃の遮断

Webアプリケーションプログラムの脆弱性をついた攻撃

[攻撃手法例]

- XSS
- SQLインジェクション
- OSコマンドインジェクション
- アプリケーションベースのセッションハイジャック

[対策]

- Webアプリケーションの脆弱性検査及び対策の実施
- Webサーバ、DBサーバの設定による対策
- WAFによる攻撃の遮断

DoS系の攻撃

[攻撃手法の例]

- Connection Flood攻撃
- 反射・増幅型DDoS攻撃

[対策]

- 十分な帯域を持つネットワークと処理能力を持つFWやサーバを用いる
- CDNのサービスを利用

マルウェアの侵入

[攻撃手法例]

- コンピュータウイルス
- ワーム
- スパイウェア
- ランサムウェア
- ボット

[対策]

- ホストの要塞化
- サンドボックスによって侵入を防ぐ

参考文献

- うかる！情報処理安全確保支援士2021
- ファイアーウォールの仕組み｜総務省 安心してインターネットを使うために国民のための情報セキュリティサイト
https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/basic/structure/01.html#:~:text=%E7%81%AB%E7%81%BD%E3%81%AE%E3%81%A8%E3%81%8D%E3%81%AB%E8%A2%AB%E5%AE%B3,%E3%82%88%E3%81%86%E3%81%AB%E3%81%AA%E3%82%8A%E3%81%BE%E3%81%97%E3%81%9F%E3%80%82
- 5分でざっくりわかる「DMZ」、役割や構築方法をやさしく解説｜ビジネス+IT
https://www.sbbit.jp/article/cont1/37677
- ファイアウォールの種類とは？違いや特徴をわかりやすく解説！| ITトレンド
https://it-trend.jp/firewall/article/60-0020
- パケットフィルタリング型ファイアーウォールは、ネットワーク層でパケットのヘッダ情報でアクセス制御を行うファイアウォールです。| ponsuke_tarou's blog
https://ponsuke-tarou.hatenablog.com/entry/2019/10/14/085238#%E3%83%80%E3%82%A4%E3%83%8A%E3%83%9F%E3%83%83%E3%82%AF%E3%83%91%E3%82%B1%E3%83%83%E3%83%88%E3%83%95%E3%82%A3%E3%83%AB%E3%82%BF%E3%83%AA%E3%83%B3%E3%82%B0%E3%81%AF%E9%80%9A%E4%BF%A1%E3%81%AE%E3%82%84%E3%82%8A%E5%8F%96%E3%82%8A%E3%82%92%E5%88%A4%E6%96%AD%E3%81%97%E3%81%A6%E5%8B%95%E7%9A%84%E3%81%AB%E3%83%95%E3%82%A3%E3%83%AB%E3%82%BF%E3%83%AA%E3%83%B3%E3%82%B0%E3%83%86%E3%83%BC%E3%83%96%E3%83%AB%E3%81%8C%E6%9B%B4%E6%96%B0%E3%81%99%E3%82%8B%E3%83%95%E3%82%A1%E3%82%A4%E3%82%A2%E3%82%A6%E3%82%A9%E3%83%BC%E3%83%AB%E3%81%A7%E3%81%99
- ステートフルインスペクションとは？ファイアウォールの仕組みを理解しよう！| ITトレンド
https://it-trend.jp/firewall/article/60-0009

参考文献

- 覚えておくべき４種のファイアウォール｜インターネット・アカデミー
https://www.internetacademy.jp/it/management/security/four-types-of-firewalls.html#:~:text=%E8%A8%B1%E5%8F%AF%E3%81%95%E3%82%8C%E3%81%BE%E3%81%99%E3%80%82-,%E3%82%B9%E3%83%86%E3%83%BC%E3%83%88%E3%83%95%E3%83%AB%E3%83%91%E3%82%B1%E3%83%83%E3%83%88%E3%82%A4%E3%83%B3%E3%82%B9%E3%83%9A%E3%82%AF%E3%82%B7%E3%83%A7%E3%83%B3,%E3%83%91%E3%82%B1%E3%83%83%E3%83%88%E3%82%92%E5%88%A4%E6%96%AD%E3%81%97%E3%81%BE%E3%81%99%E3%80%82&text=%E3%82%B9%E3%83%86%E3%83%BC%E3%83%88%E3%83%95%E3%83%AB%E3%83%91%E3%82%B1%E3%83%83%E3%83%88%E3%82%A4%E3%83%B3%E3%82%B9%E3%83%9A%E3%82%AF%E3%82%B7%E3%83%A7%E3%83%B3%E3%81%AF%E3%80%81%20%E3%82%B3%E3%83%B3%E3%83%86%E3%82%AD%E3%82%B9%E3%83%88,%E3%81%99%E3%82%8B%E3%81%93%E3%81%A8%E3%81%8C%E5%8F%AF%E8%83%BD%E3%81%A7%E3%81%99%E3%80%82
- 通信の中身までチェックできる！アプリケーション型ファイアウォールとは｜インターネット・アカデミー
https://www.internetacademy.jp/it/management/security/what-is-application-firewall.html
- NGN時代の必須技術 ファイアウォール｜ビジネスコミュニケーション東京ジャーナル
http://www.ric.co.jp/expo/bctj/column/kobayashi01/kobayashi_10.html