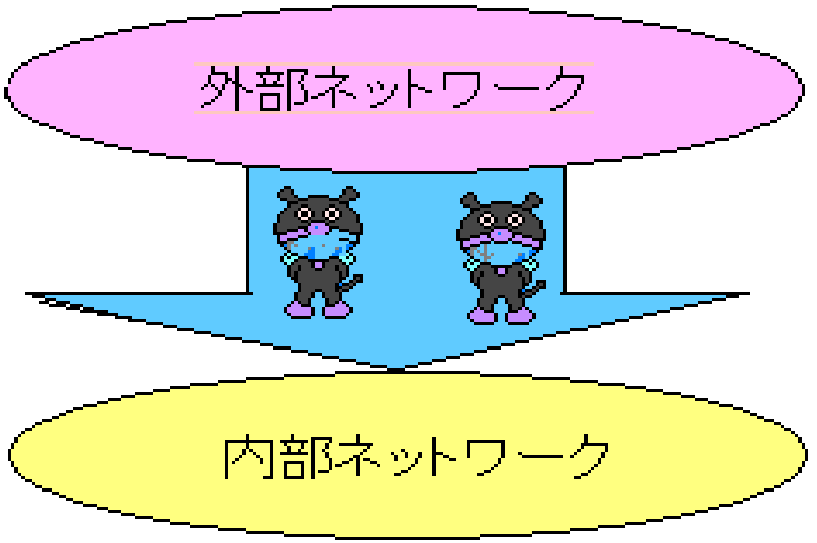
分散ファイアウォールの連携

木下研究室

電気電子情報工学科　　４年B組
学籍番号200502780番　　国崎　大地

研究の背景

- ネットワークの普及
- データやプログラムの盗み見・改ざん・破壊などが行なわれる被害が出ている。

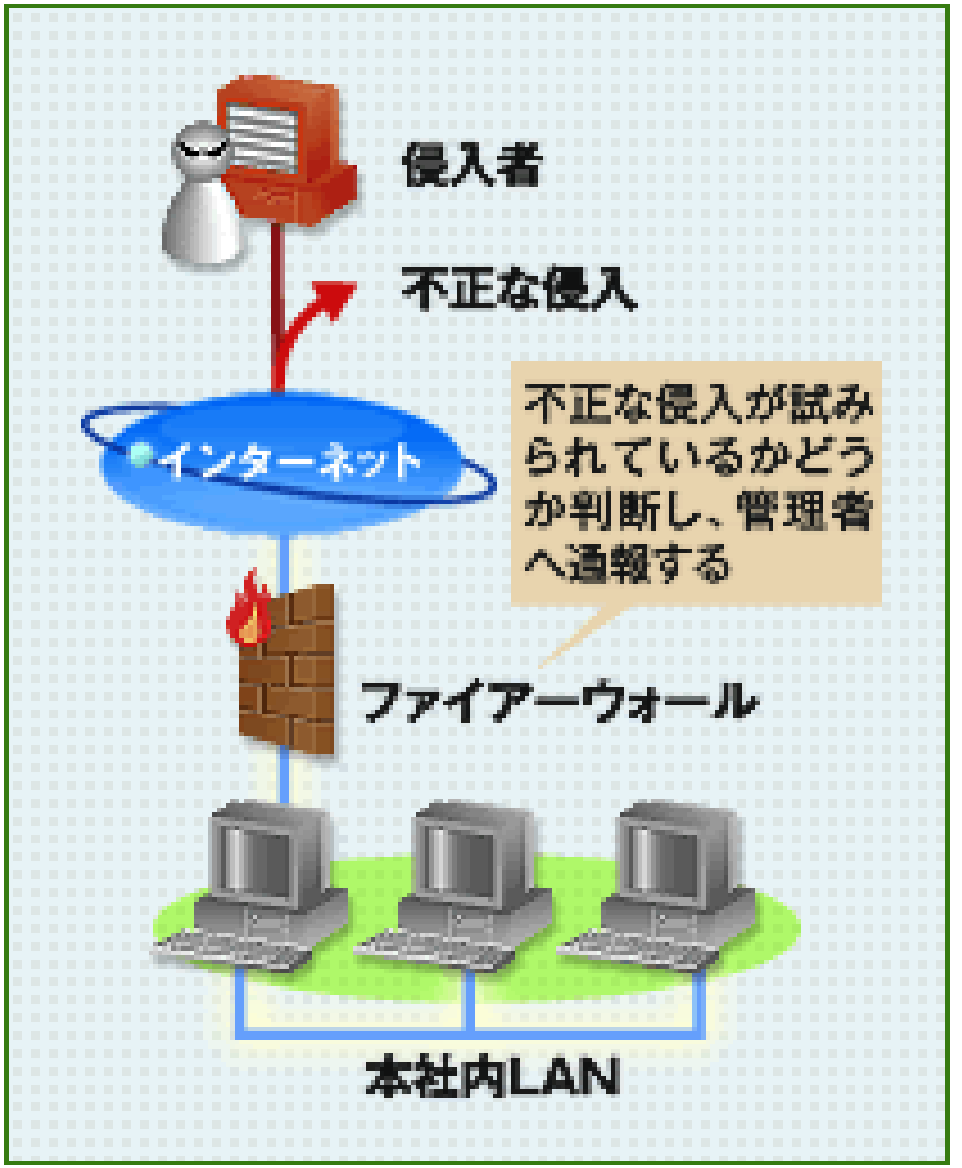


- この様な事のないように、外部との境界を流れるデータを監視し、不正なアクセスを検出・遮断する必要がある。

研究の背景

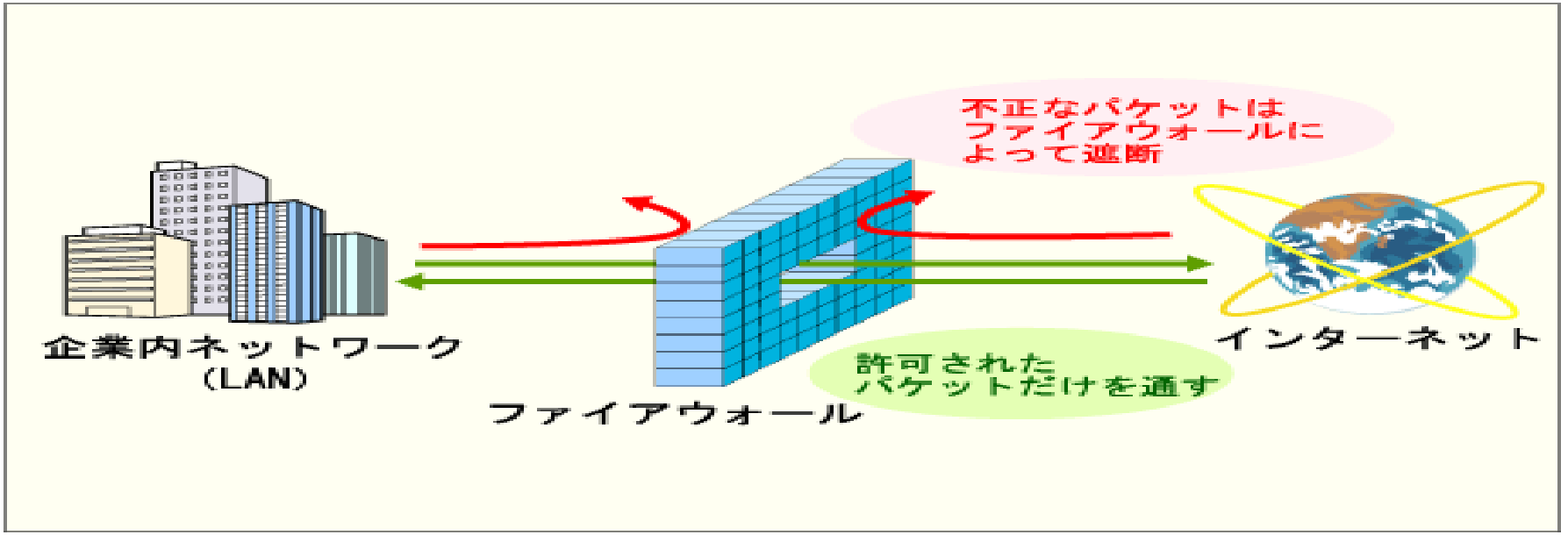
- ネットワークの普及
- データやプログラムの盗み見・改ざん・破壊などが行なわれる被害が出ている。

- この様な事のないように、外部との境界を流れるデータを監視し、不正なアクセスを検出・遮断する必要がある。



研究の目的

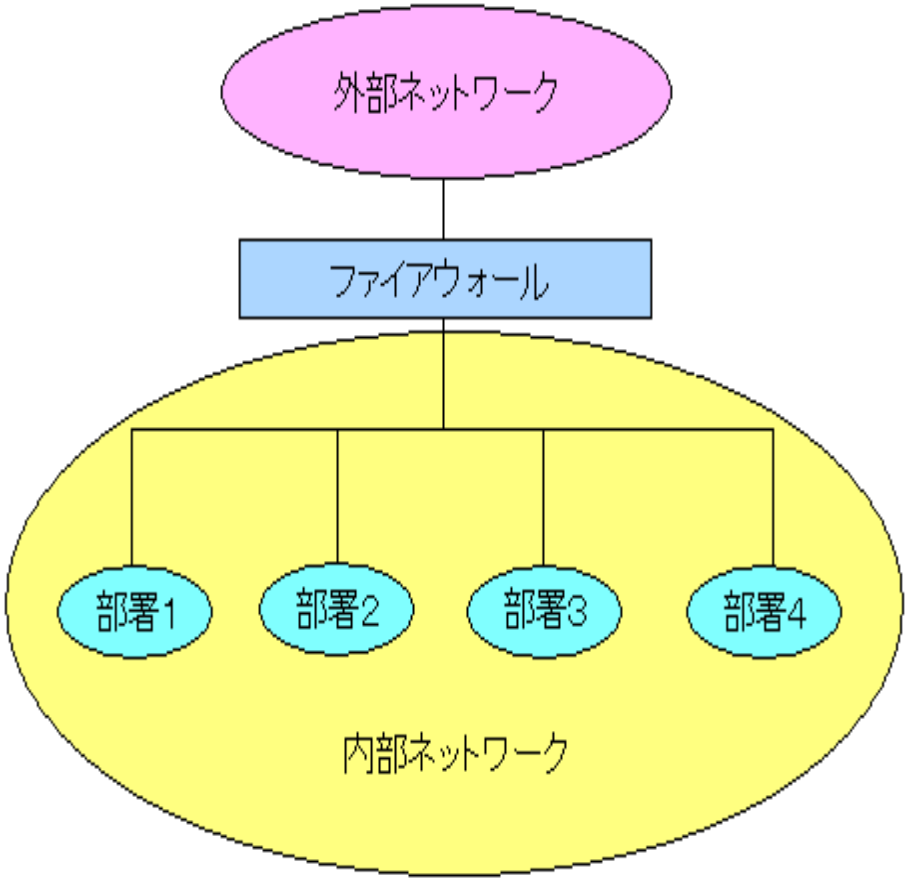
- ファイアウォールを用いた、不正なアクセスの検出、遮断。
- 柔軟で強固なファイアウォールの実現。
- 適切なルールの設定による負荷の軽減。
- 仮想マシンを用いた実装実験により、一般的なネットワークでも使用出来るか検討する。



ファイアウォールの設置方法

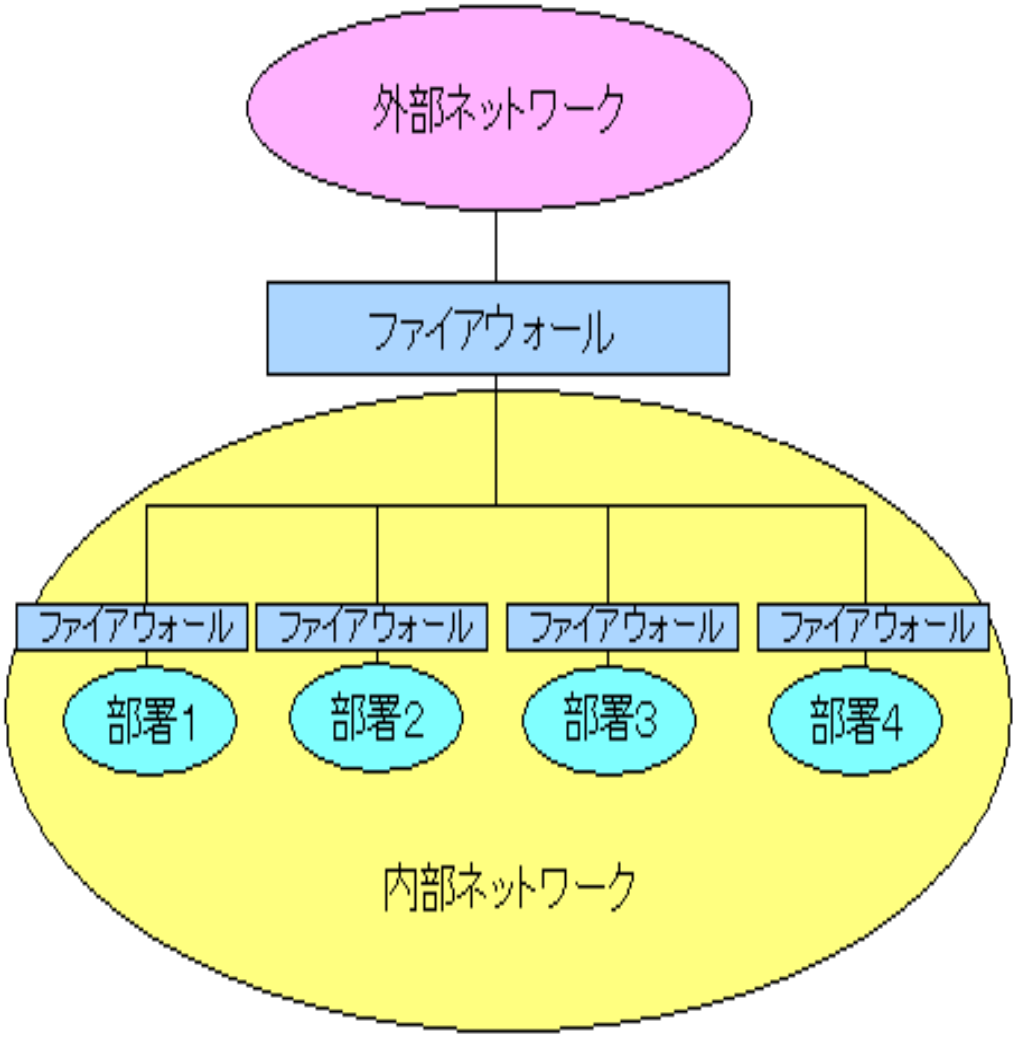
- ファイアウォールの設置方法として、外部ネットワークと内部ネットワークの境界のみに設置する方法（集中型）と、境界のみでなく内部ネットワークの部署単位でも設置する方法（分散型）が考えられる。

- 集中型ファイアウォール
- 利点：管理しやすい
- 欠点：内部からの攻撃に対処出来ない。
  部署ごとの異なるセキュリティーポリシーに対応できない。



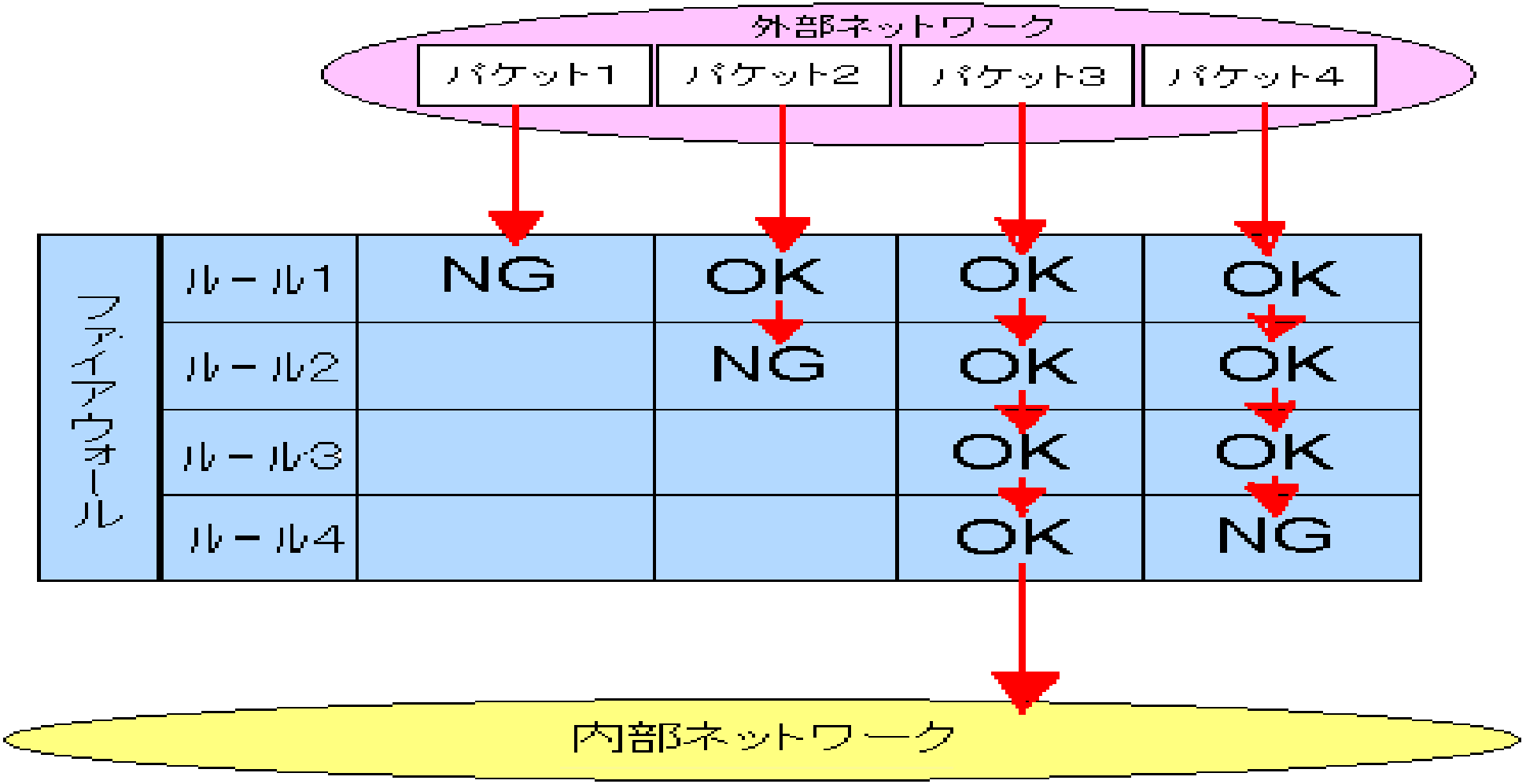
ファイアウォールの設置方法

- 分散型ファイアウォール
- 利点：内部からの攻撃でも対処できる。
  部署ごとに異なるセキュリティーポリシーを設定できるので柔軟で強固なセキュリティーを実現できる。
- 欠点：適切なルールの設置が難しい。



フィルタリングの仕組み

パケットフィルタリングでは送られて来たパケットに対してIPヘッダ情報を元に通信を許可するか、または拒否するかをルールとのマッチングを行い判断する。

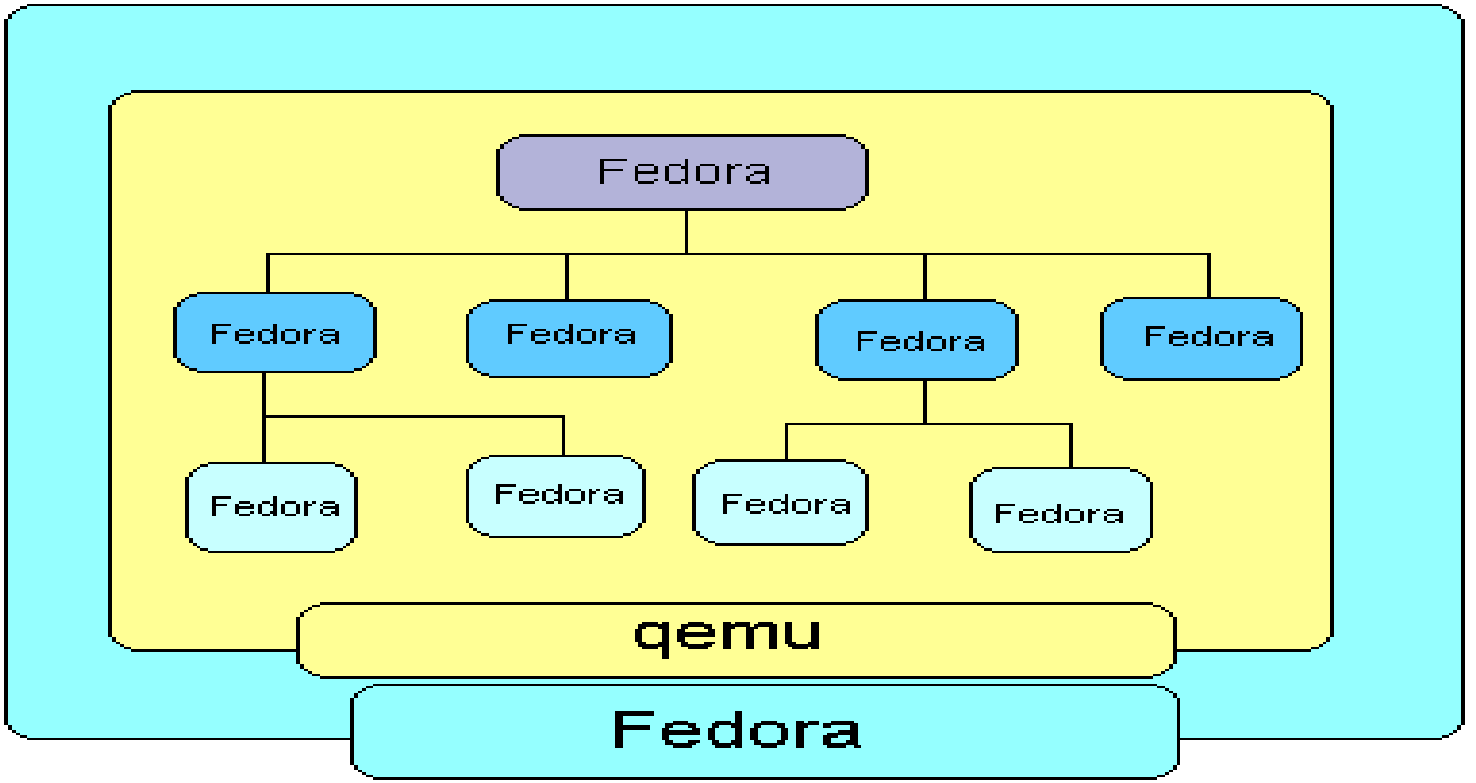


ルールの設定

- 操作
  - add：ルールを追加する。
  - delete：ルールを削除する。
- 処置方法
  - Pass:パケットを通過させる。
  - deny:パケットを破棄する。
- プロトコル　tcp,udp,icmp,ipが指定可能。
- ルール設定の例
- ①add pass tcp from any to 133.72.88.10 22
- ②add deny udp from any to any

実装実験方法

- 仮想マシン内にネットワーク環境を構築する。
- 分散型ファイアウォールの図に示したようにルーターとホスト間の通信経路を確立する。
- 各ファイアウォールのセキュリティポリシーに基づいたルールの設定。



ファイアウォールの負荷

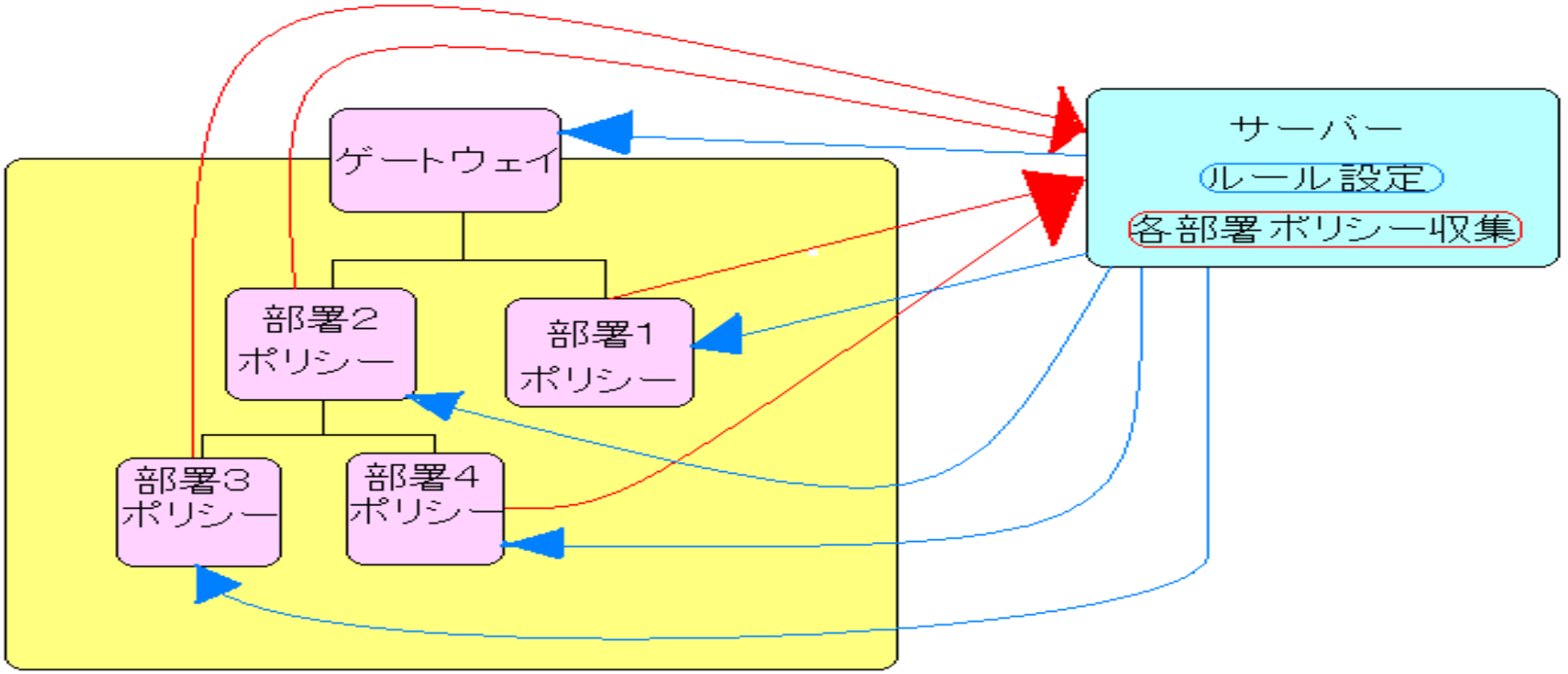
- パケットとルールにマッチング処理に注目した。
- 「ルール数を減らす」＝「負荷の軽減」

負荷を軽減させる方法

- 各ファイアウォール間でのルールの受け渡し、受け取ったルールの並び替え。
- システム全体としてセキュリティポリシーを変えずにルールの統合を行う。

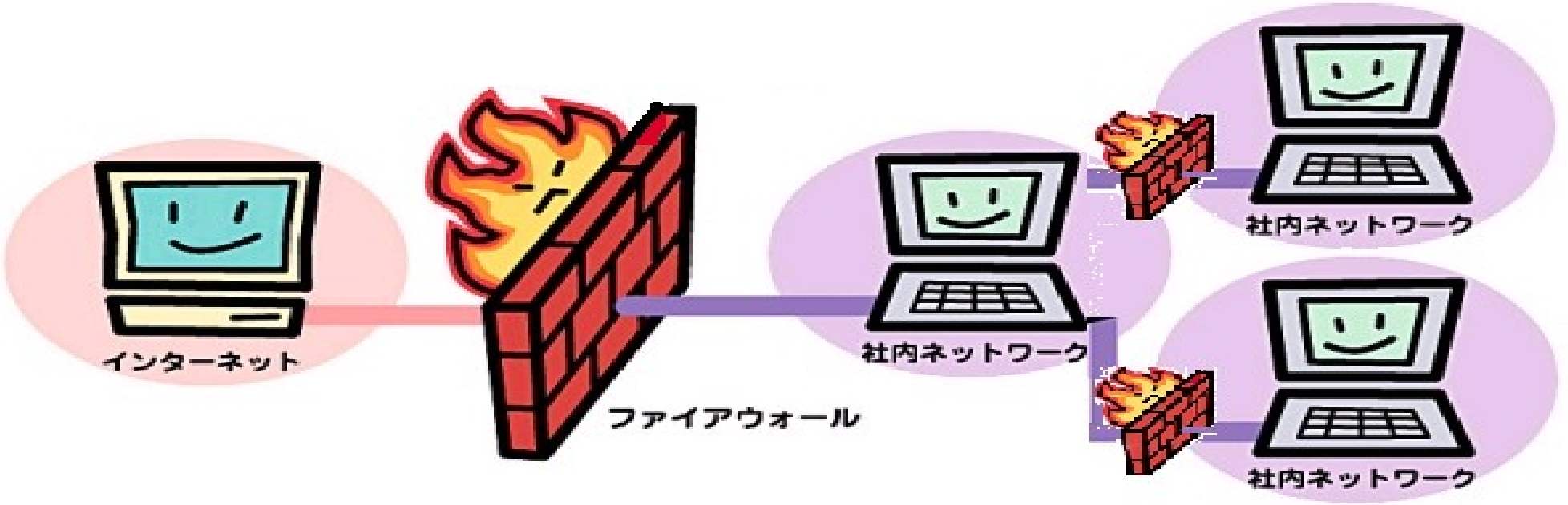
システムの概要

- 部署ごとのセキュリティポリシーを集める。
- 集めたセキュリティポリシーに基づいてルールの統合し最適化を行う。
- 最適化の論理式に基づいて各ファイアウォールにルールを返し、設定する。



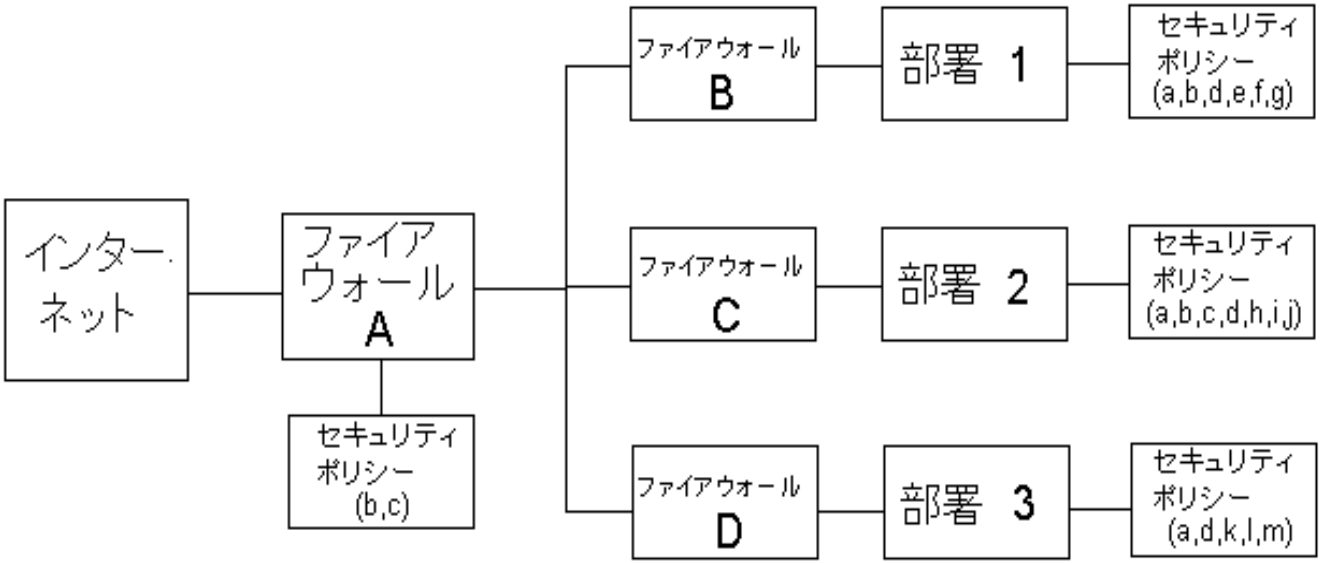
今後の課題

- ファイアウォールにかかる負荷の軽減が見込めるようなルールの設定、システムの提案。
- 提案したシステムの論理的解析。
- 提案したシステムの実装実験。



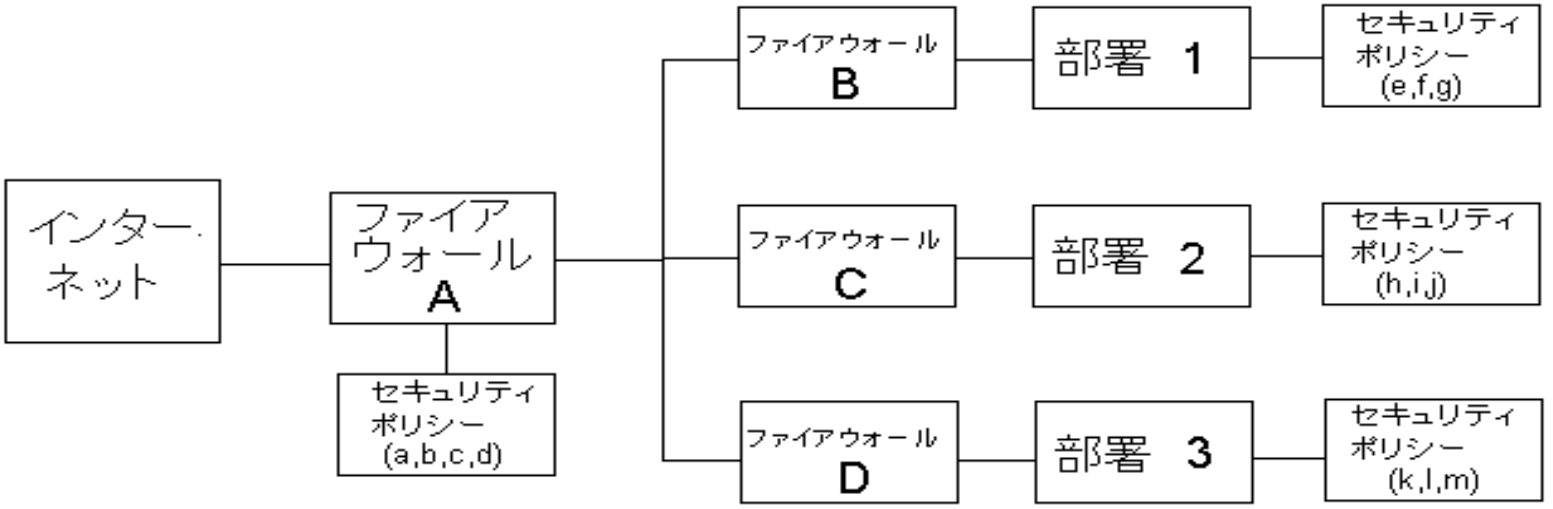
実装実験例

- ４台のファイアウォールを図のように配置する。
- 各ファイアウォールにa～mというルールを設定する。
- インターネットからのパケットは最大で9回マッチング処理される。
- 図の状態では重複されていたり、統一されていないルールが多いので各ファイアウォールに負荷がかかる。



実装実験例

- ルールの最適化を行うことにより、インターネットからのパケットは最大で7回マッチング処理に軽減された。
- 各ファイアウォールでのマッチング処理回数を減らすことで、システム全体としての負荷を軽減。



結論

- 仮想マシンを用いた実装実験により、分散型ファイアウォールにおいて、各ファイアウォール間での連携を持たせることでルールの最適化による負荷の軽減を実現した。
- 今回は特定のセキュリティポリシーに対してのルール最適化を行うプログラムだったので、様々なルールに対しても最適化出来るプログラムの検討が必要。
- 実際のネットワークでも対応できるような、柔軟で強固な分散型ファイアウォールの開発が、今後の課題。