


本資料について

本資料は下記論文を基にして作成されたものです。文書の内容の正確さは保障できないため、正確な知識を求める方は原文を参照してください。

- 著者：萱島 信，寺田 真敏，藤山 達也，小泉 稔，加藤 恵理
- 論文名：“多重ファイアウォール環境に適したVPN構築方式の提案”
- 出展：電子情報通信学会論文誌 D-I Vol.J82-D-I No.6 pp.772-228
- 発表日：1999年6月



多重ファイアウォール環境に適した VPN構築方式の提案

萱島 信, 寺田 真敏, 藤山 達也,
小泉 稔, 加藤 恵理

渡邊研究室 00J125 増田 真也

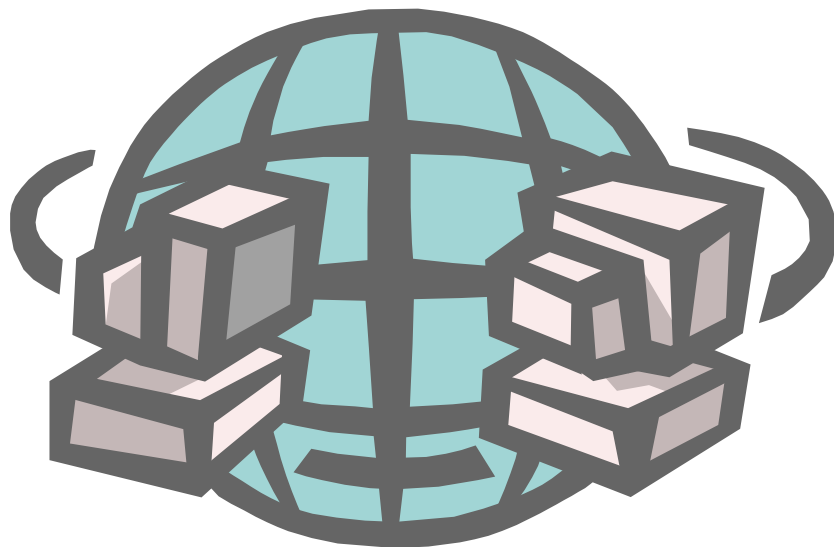
はじめに

■ 全体の流れ

1. 背景
2. 従来のVPN構築方式
3. 部門VPN構築時の問題点
4. 多重ファイアーウォール環境向けのVPN構築方式
5. 提案方式の実装
6. むずび

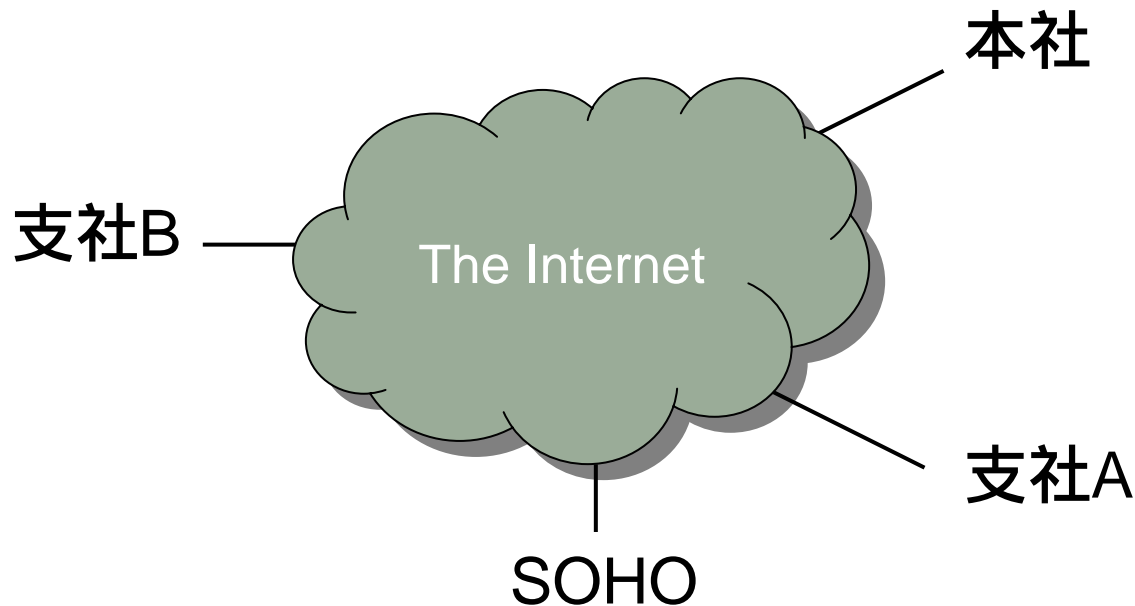


1. 背景



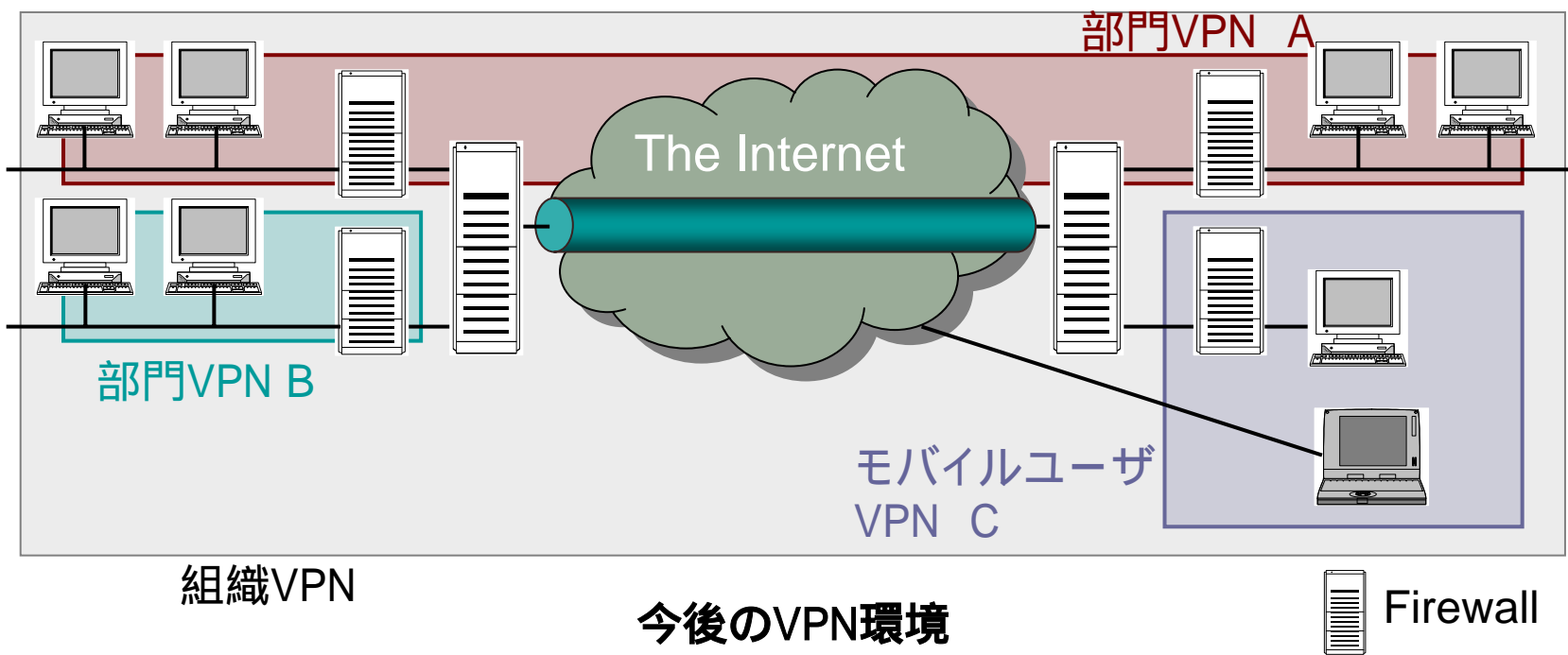
1-1. VPNによる組織ネットワーク

- 組織ネットワークをインターネットに接続する企業の増加
VPNが注目される



1-2. 今後のVPN環境

- 組織内部の不正ユーザによる脅威
 - 他部門からの、権限を越えたアクセスからガードしたいというニーズの増加
- 部門ごとの小規模なVPN



1-2. 今後のVPN環境

■ 部門VPN

- 組織の分散拠点にまたがって構築するもの - A
- 組織の拠点内で構築するもの - B
- 出張者等がインターネット経由で利用するために構築するもの - C

多重のファイアウォールを越えることを前提とするVPN構築技法は、今まで検討されていなかった

- 従来のVPN構築技法を部門VPNの構築に使用した場合の問題点を検討
- 検討結果を踏まえ、部門VPNの実現に適したVPN構築技法を提案

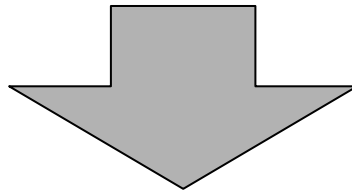


2. 従来のVPN構築方式



2-1. VPNの要件

- アクセス制御処理
- データ暗号化処理
- 認証処理



これらの処理を実現するレイヤによって, VPNを

- ネットワーク層型
- トランスポート/アプリケーション層型

に分類する

2-2. ネットワーク層型VPN

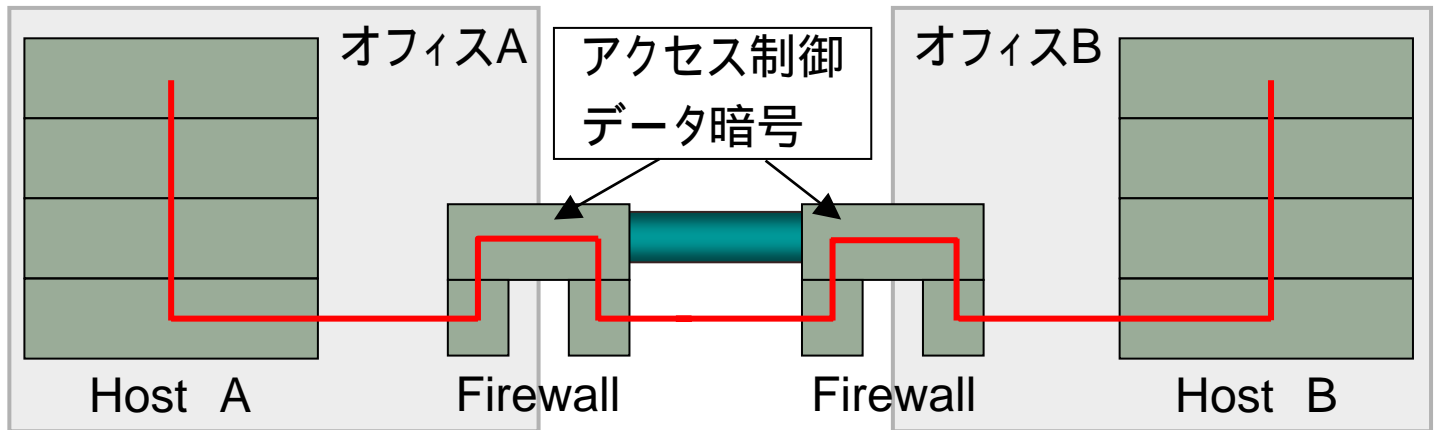
- IPフィルタリングによるアクセス制御
 - 送信元と宛先のアドレスフィールドを検査し, 通過されるパケットを取捨選択
 - ホスト単位, ネットワーク単位でのアクセス制御を実現
- IPトンネリングによるパケット単位のデータ暗号化
 - IPパケットを別のIPパケットでカプセル化した通信
 - カプセル化の際にデータを暗号化
- 代表的な方式
 - IPsec
 - PPTP

2-3. トランスポート/アプリケーション層型VPN

- 代理サーバによるアクセス制御
 - クライアントプロセス単位で実施
 - プロセスとそのユーザは1対1に対応させることで、ユーザ単位でのアクセス制御を実現
- アプリケーションレベルでのデータ暗号化
- 特徴
 - 内部ネットワークへの経路制御情報を隠蔽
 - IPフォワーディングを停止することによる組織内情報の漏洩緩和
- 代表的な方式
 - Socks V5

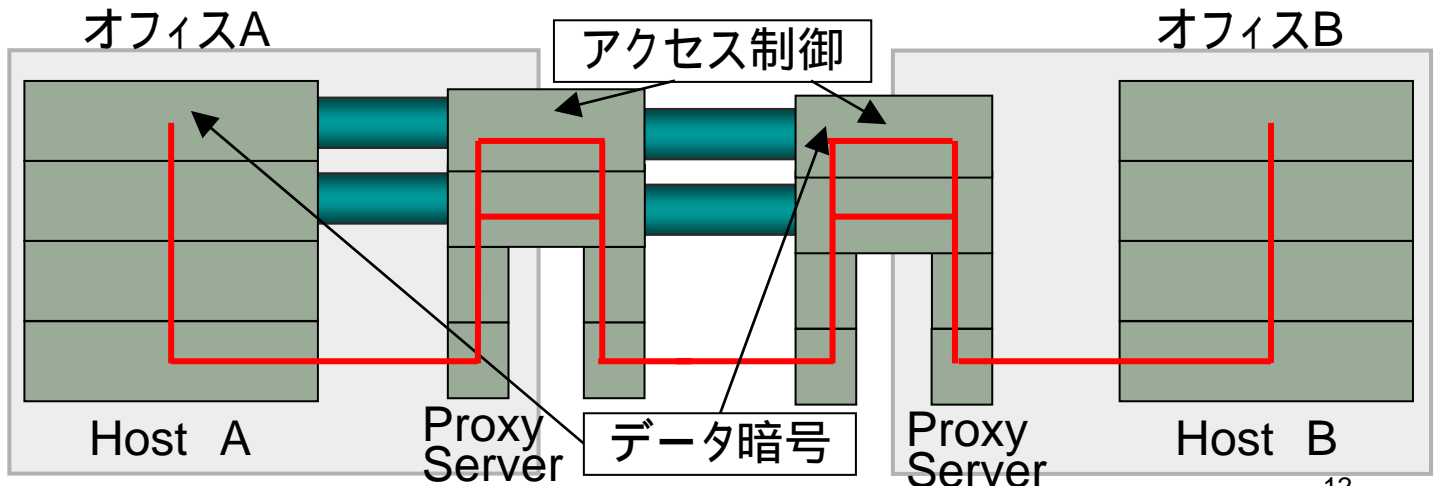
2-4. VPNアーキテクチャと通信レイヤ

Application Level
 Transport Level
 Network Level
 Link Level



ネットワーク層型VPN

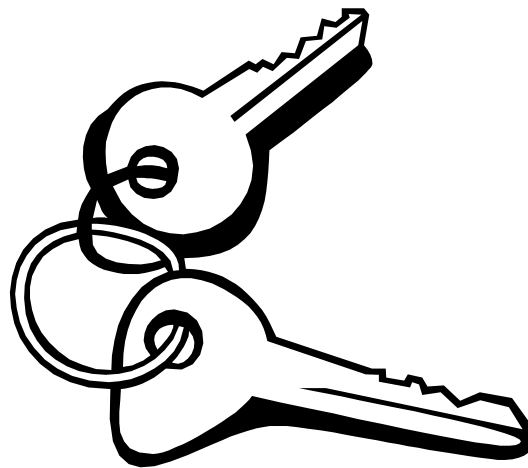
Application Level
 Transport Level
 Network Level
 Link Level



トランスポート/アプリケーション層型VPN



3 . 部門VPN構築時の 問題点



3-1 . VPN構築技法の組み合わせ

■ ネットワーク層型の組織VPN

○ ネットワーク層型の部門VPN

■ 多重IPトンネリングの問題

- クライアント・サーバ間の暗号化/復号処理の回数増加
- ヘッダ長の増加により実効データ長が低下

■ 組織VPNのファイアウォールにはトラフィックが集中する 大規模な組織VPNの場合は、暗号化/復号処理による パフォーマンスの低下も考慮

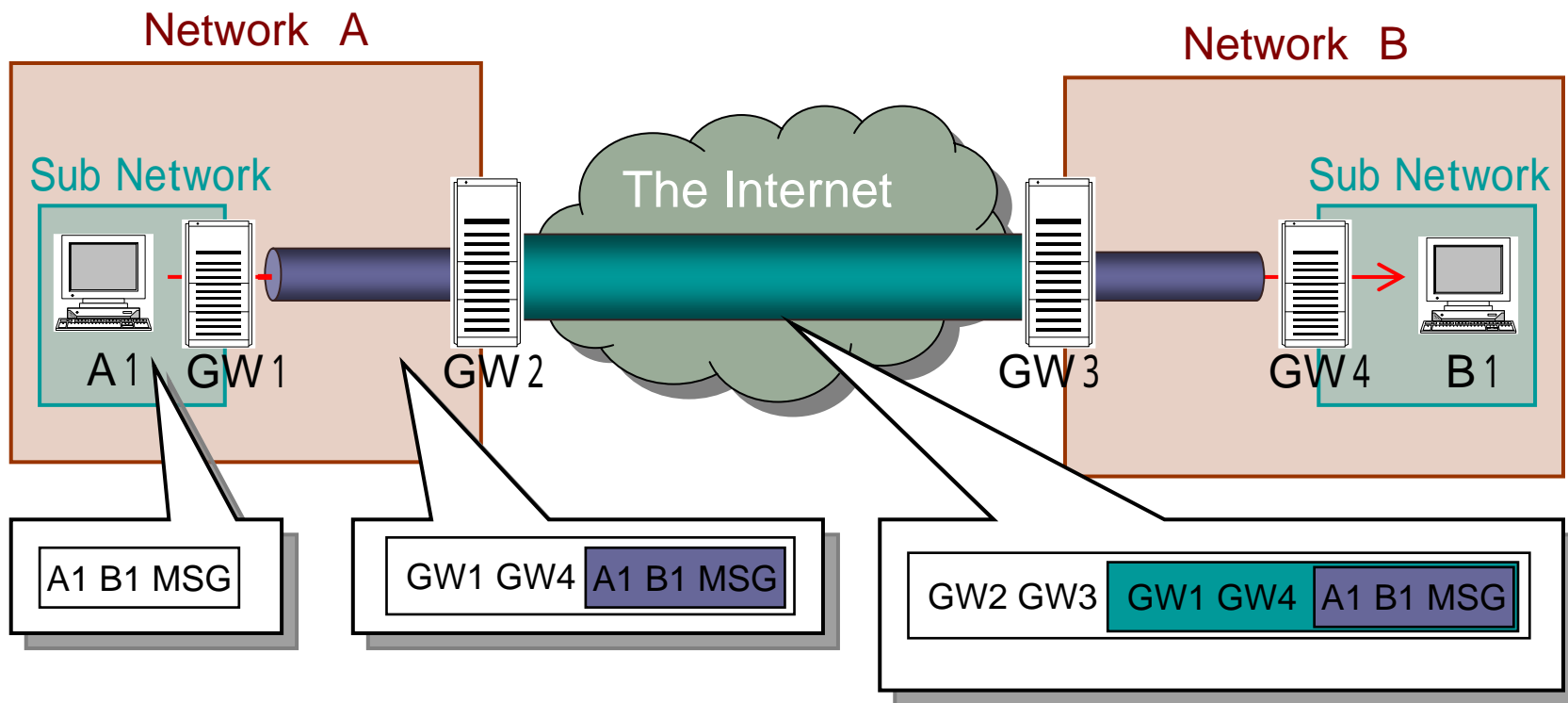
○ トランスポート/アプリケーション層型の部門VPN

■ 組織VPNのファイアウォールにはトラフィックが集中する 大規模な組織VPNの場合は、暗号化/復号処理による パフォーマンスの低下も考慮

パフォーマンスの問題

3-1. VPN構築技法の組み合わせ

■ 多重トンネリングが発生するケース



多重トンネリングが発生するケース

3-1. VPN構築技法の組み合わせ

- **トランスポート/アプリケーション層型の組織VPN**
 - **ネットワーク層型の部門VPN**
 - 組織VPNがトランスポート/アプリケーション層型のため、組織ネットワークは各拠点のファイアウォールによりネットワーク層で遮断される拠点間にまたがった部門VPNはネットワーク層型VPNで構築できない
 - **トランスポート/アプリケーション層型の部門VPN**
 - 組織VPNの代理サーバは、部門ファイアウォールがネットワークの継ぎ目にあるため、保護されたネットワークには直接接続することができない
 - 代理サーバには宛先に応じて適切な部門VPNの代理サーバを選択する仕組みが必要



4 . 多重ファイアーウォール 環境向けVPN構築方式



4-1. パフォーマンスの改善

■ 多重トンネリングの抑制

- VPNの構築にトランスポート/アプリケーション層型を使用

■ 暗号処理集中化の防止

- 部門VPNと組織VPNのトラフィックを区別し, 部門VPNの暗号化はそのまま中継する機能を実現させる
 1. 組織VPNがネットワーク層型の場合
 2. 組織VPNがトランスポート/アプリケーション層型の場合

4-1. パフォーマンスの改善

1. 組織VPNがネットワーク層型の場合

- 送信元と宛先のアドレスより部門VPNのトラフィックを識別
- 組織VPNのファイアウォールで暗号化を行わないように抑制

2. 組織VPNがトランスポート/アプリケーション層型の場合

- コネクティビティの問題により、部門VPNも同じ方式を採用
クライアントからサーバまでの経路上に複数代の代理サーバが存在することになる
 - 代理サーバは、クライアントの認証とデータ中継を実施
 - データの暗号化/復号処理は、代理サーバとクライアントのみで実行する“エンド-エンド暗号化機能”を実装

4-1. パフォーマンスの改善

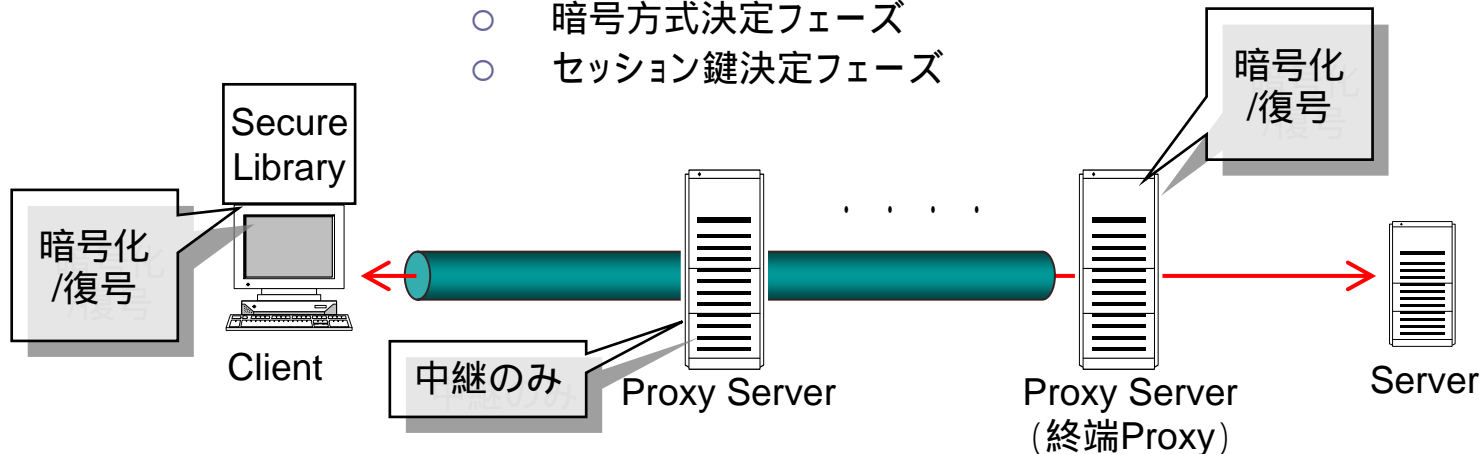
■ エンド-エンド暗号化機能(データ部分)

○ 要件

- 暗号鍵の共有
- 暗号化アルゴリズム, アルゴリズムが使用するパラメタの両者間のネゴシエーション

○ 実現方式

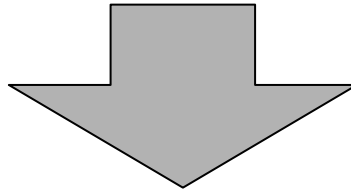
- クライアントと代理サーバ間の相互認証に3パス認証方式を用い, シーケンスの中に以下の2つのフェーズを含ませる
 - 暗号方式決定フェーズ
 - セッション鍵決定フェーズ



エンド-エンド暗号化機能

4-2. コネクティビティの確保

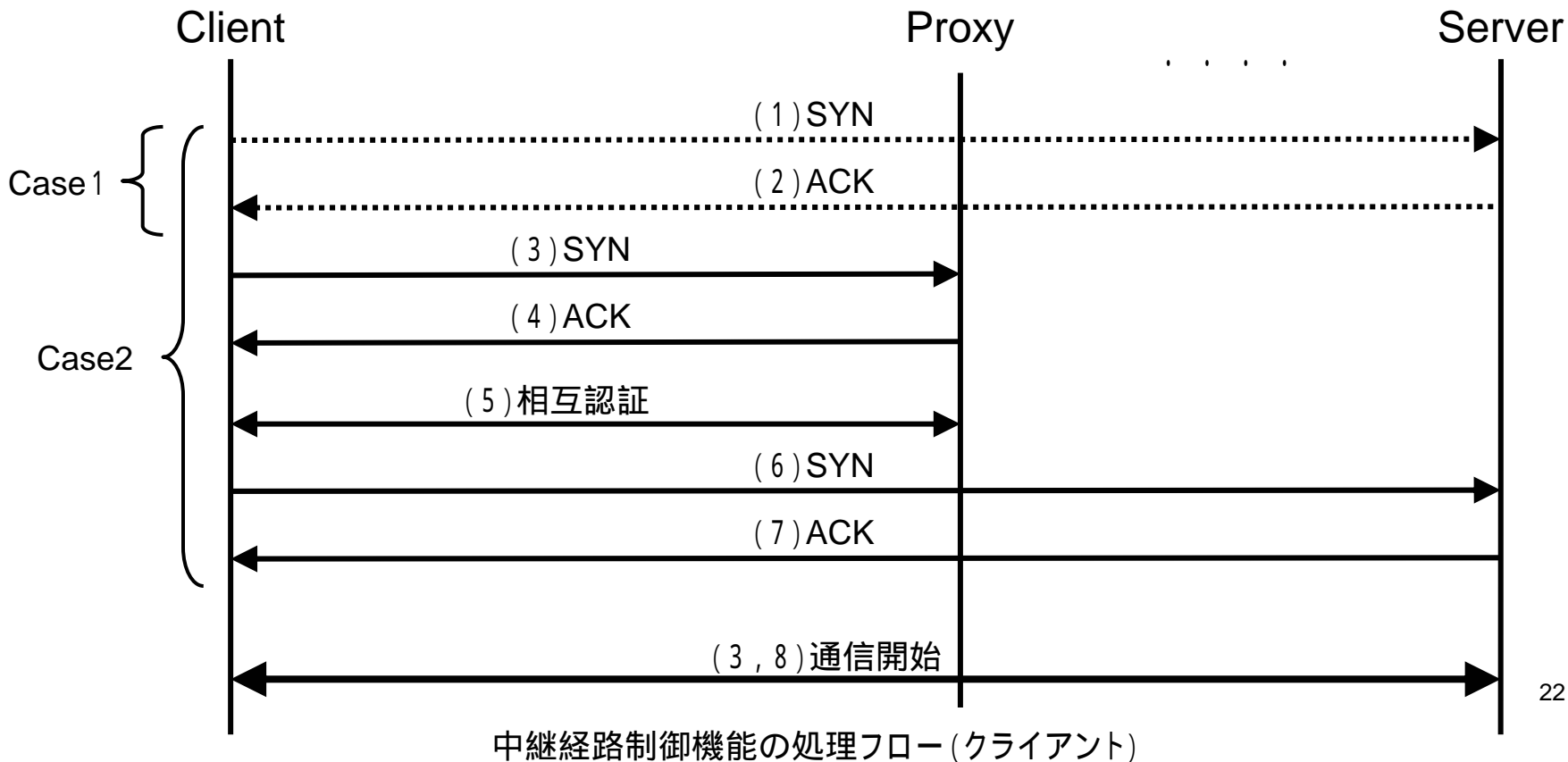
- トランスポート/アプリケーション層型VPNでは、組織情報が隠蔽され、かつIPフォワーディングが停止される
部門VPNの通信で代理サーバを多段に経由する場合、ネットワーク層における経路情報を利用できない



トランスポート層において、サーバへの中継経路を確立する機能“中継経路制御機能”を備える

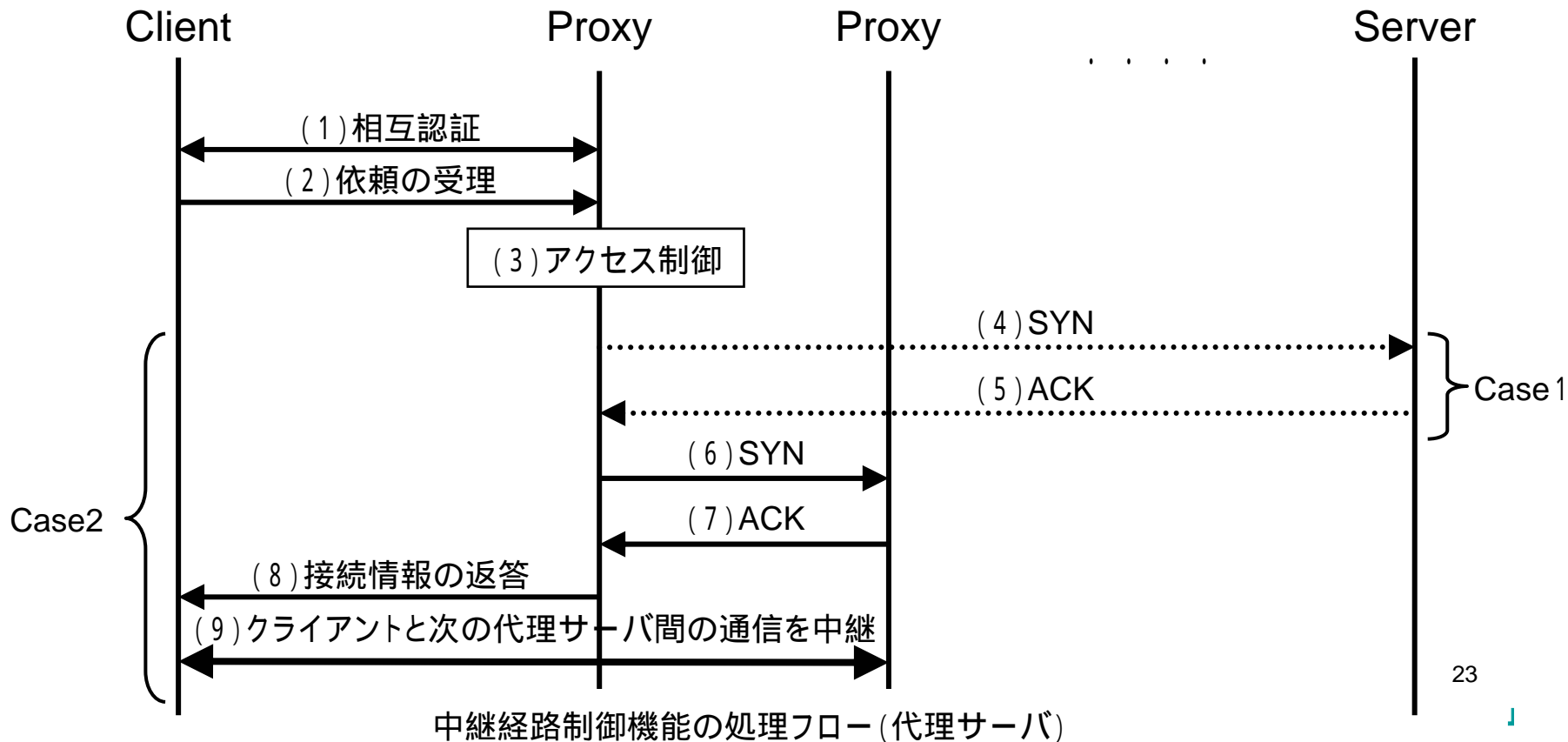
4-2. コネクティビティの確保

- クライアントと代理サーバ間の中継経路制御機能の処理フロー(クライアント)



4-2. コネクティビティの確保

- クライアントと代理サーバ間の中継経路制御機能の処理フロー(代理サーバ)





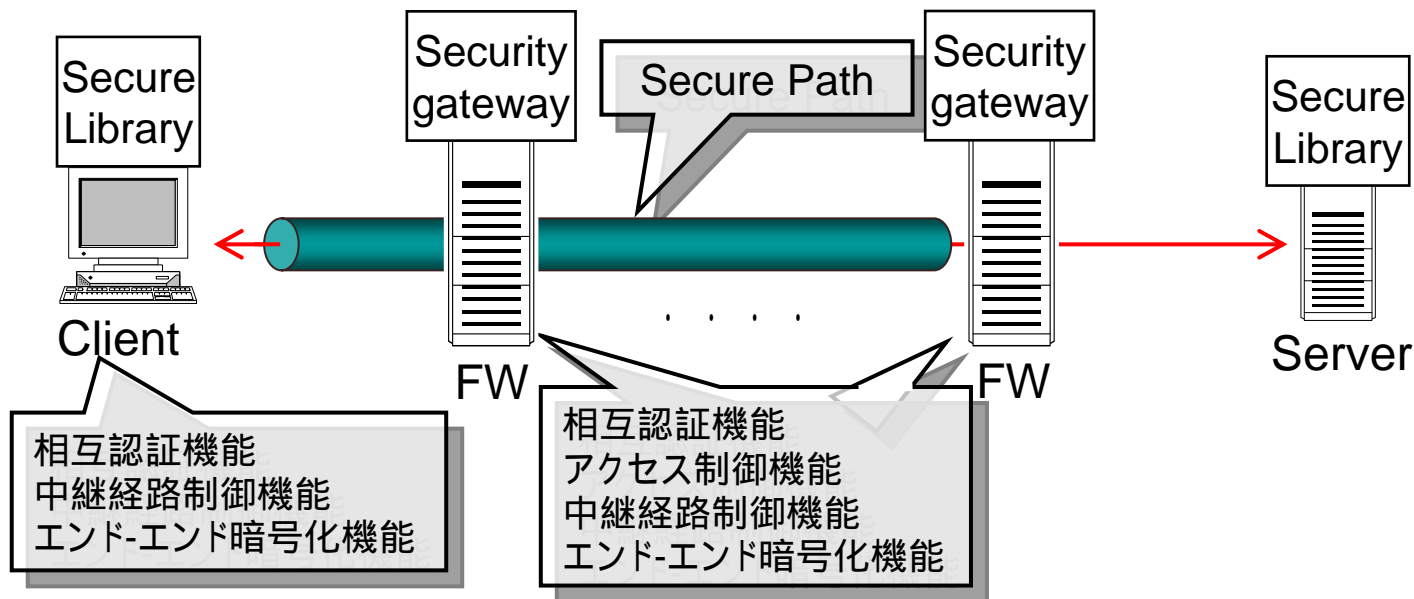
5 . 提案方式の実装



5-1. システム構成

■ 部門VPN構築技法を実装した“シームレスVPN”

- トランスポート/アプリケーション層型をベース
多重トンネリングを抑制することに主眼をおいたVPN構築技法



システム構成

5-1. システム構成

■ クライアント

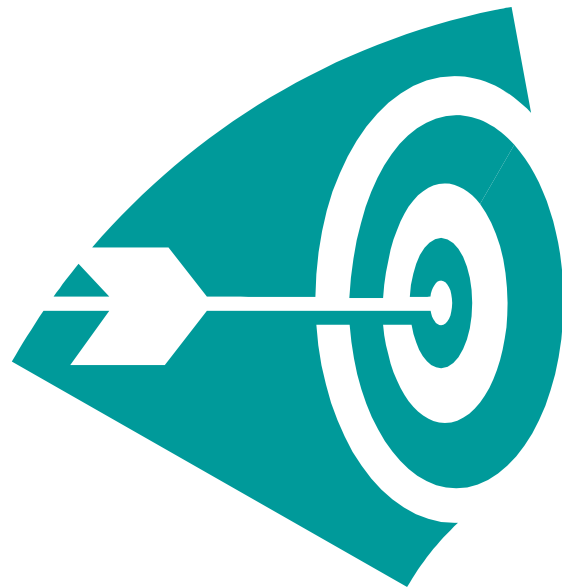
- ソケットライブラリとしてセキュリティゲートウェイとの通信を可能にする“セキュアライブラリ”を実装
- セキュアライブラリに実装した機能
 - 相互認証機能
 - 中継経路制御機能
 - エンド-エンド暗号化機能

■ ファイアウォール

- ファイアウォール上にトランスポート層に実装した代理サーバである“セキュリティゲートウェイ”を設置
- セキュリティゲートウェイに実装した機能
 - 相互認証機能
 - アクセス制御機能
 - 中継経路制御機能
 - エンド-エンド暗号化機能



6 . むすび



6-1. 結論

- 部門VPNの構築時の問題

- パフォーマンスの問題
- コネクティビティの問題

- 解決策

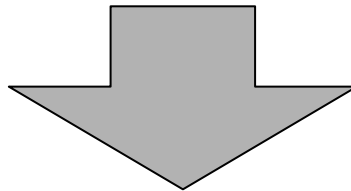
- トランスポート/アプリケーション層をベースとすることで、多重トンネリングによるパフォーマンスの問題を回避
- 暗号化通信路の途中ではデータ中継のみを実施する“エンド-エンド暗号化機能”をVPNに導入
- 多重のファイアウォールにより隠蔽されたネットワークに対する経路情報を確保するために、トランスポート層で中継経路の情報交換を行う“中継経路制御機能”をVPNに導入

6-2. 課題

- “中継経路制御機能”における課題

- 本機能は、トランスポート層において各代理サーバが静的な中継経路テーブルを参照

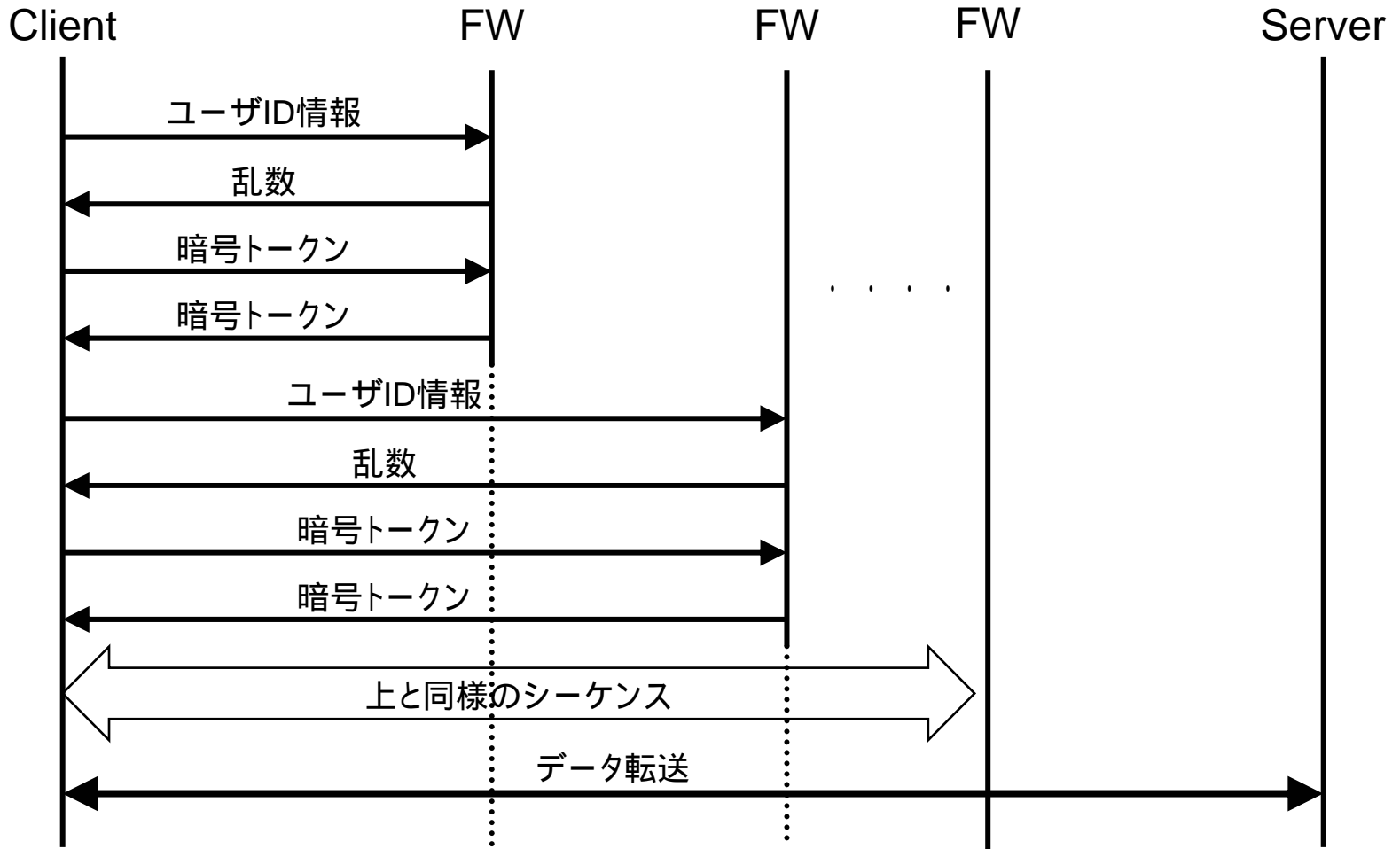
インターネットの世界は変化が激しく、中継経路の情報も時と場合により柔軟に変化させる仕組みが必要



ネットワーク層における動的経路制御機能に適用することを含め、より高度な中継経路制御のあり方を検討

おわり

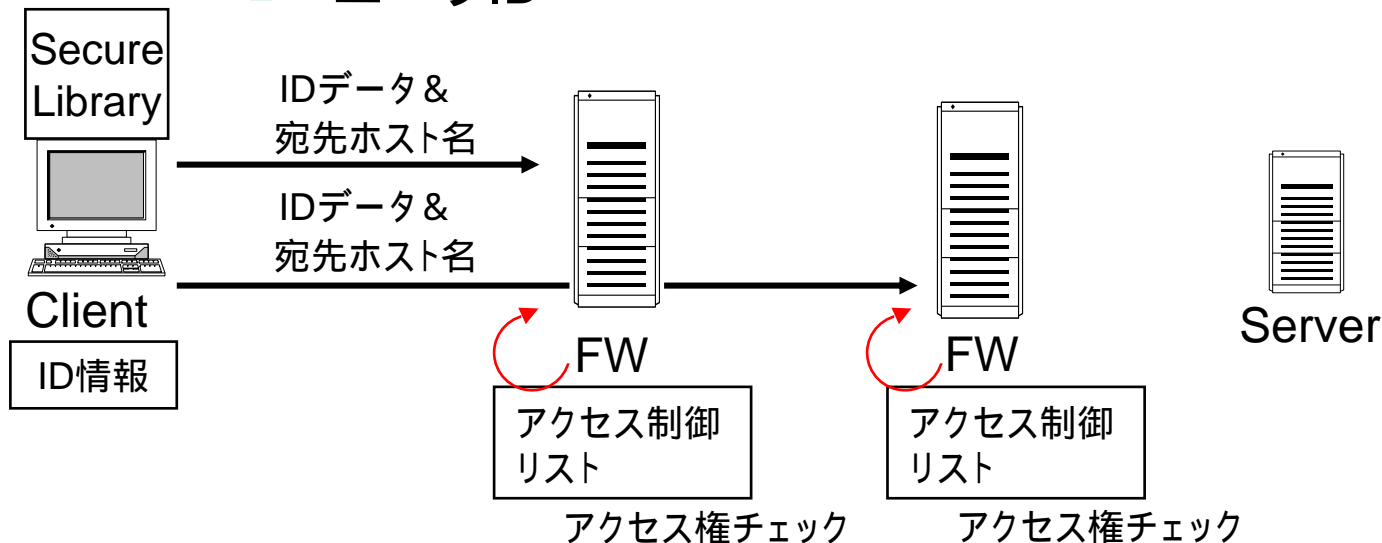
相互認証機能



相互認証機能

アクセス制御機能

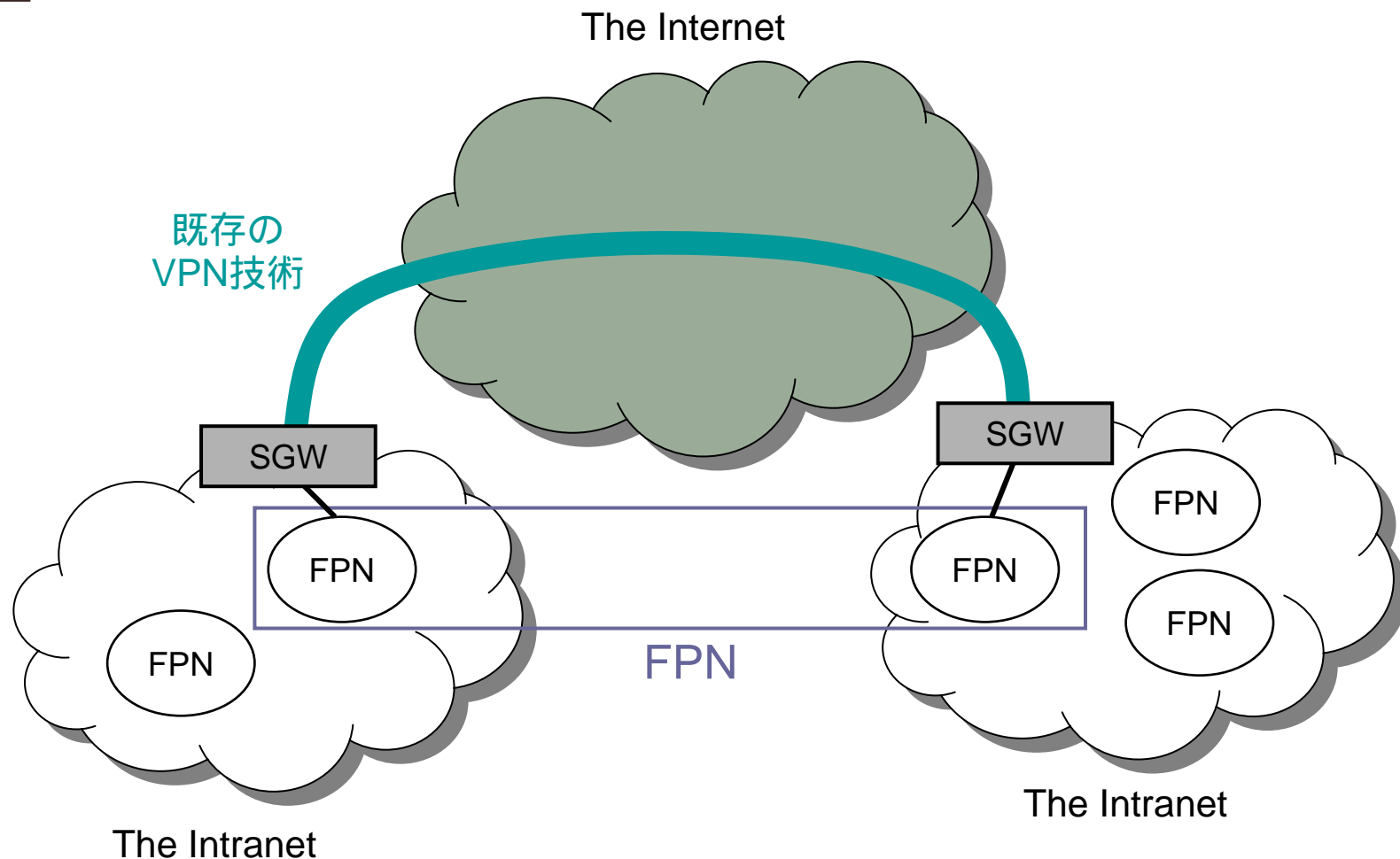
- クライアントとサーバの間に複数のFW
 - FWはアクセス制御リストを用いて制御する
 - アクセス制御リストのパラメタ
 - 送信元と宛先のアドレス
 - サービス名とポート番号
 - ユーザID



エンド-エンド暗号化機能 補足説明

- エンド-エンド暗号化機能 (データ部分)
 - 暗号方式決定フェーズ
 - 暗号メカニズムとパラメタを決定するフェーズ
 - データ暗号化に使用するメカニズム
 1. クライアントから使用可能な暗号メカニズムのリストを代理サーバに送信
 2. 代理サーバに実装した戦略に基づき,暗号メカニズム及びパラメタを決定し,その結果をクライアントに返信
 - セッション鍵決定フェーズ
 - 暗号方式決定フェーズの暗号メカニズム及びパラメタに適用可能なセッション鍵を生成する

FPNにおける考察1



インターネットを通したFPN

FPNにおける考察2

- 既存VPNの構築手段
 - IPsec, PPTP, SOCKS, SSL, VLAN...
- 既存VPNとの相性
 - パフォーマンス
 - 暗号処理の多重化
既存VPNでの暗号化を抑制
 - コネクティビティ
 - 提案方式では既存システムに影響を与えない暗号通信なので、問題は少ないと思われる
- 鍵管理の方法

参考文献

- 萱島, 寺田, 藤山, 小泉, 加藤 “多重ファイアウォール環境に適したVPN構築方式の提案”
電子情報通信学会論文誌 D-1 Vol.J82-D-1
No.6
- Kayashima, Koizumi, Fujiyama, Terada,
Hirayama “Seamless VPN” INET 97
Proceedings