多段構成ネットワークにおける鍵配送方式の一検討

11300J120　保母雅敏
渡邊研究室

1. はじめに

イントラネット内で安全な通信を行うための技術として、閉域通信グループを構築する研究が行われている。この研究の一方式として、一定の条件で作られた通信グループと共通鍵(グループ鍵)を一対一に対応させる方式が提案されている。この装置では、暗号装置(EE)が通信経路上に 3 台以上存在するような多段構成ネットワークにおいても柔軟なシステムを構築することが可能である。しかし、グループ鍵は管理装置(MS)から各 EE に配送されるため、MS から対象の EE に配送する際に、第三の暗号装置(中間 EE)を通過しなければならない場合があり、この部分において確実な認証が行っていないという課題があった。

本研究では、中間 EE で確実に認証を行いながら鍵配送が実現できる方法を検討したので報告する。

2. 想定されるシステム

対象となるシステム(図 1)では、クライアントを保護する EES(ソフトウェア型 EE)、配下のネットワークを保護する EEN(ネットワーク型 EE)、直下の端末を保護する EEA(アダプタ型 EE)が存在する。これらの EE は企業内の部署同士などといった一定の条件に基づきグループ化され、同じグループに属している端末とは、グループに割り当てられたグループ鍵を用いて暗号通信を行う。グループ情報やグループ鍵は MS によって管理されているため、暗号通信を行うためには各 EE にこれらのパラメータを配送することが必要となる。この際に、ネットワーク構成によっては MS と終端 EE の経路上に中間 EE が存在する場合がある。

従来システムでは中間 EE の認証を考慮していないため、鍵配送パケットを無条件で通過させているという課題があった。この問題を解決するため、中間 EE の認証を考慮した鍵配送プロトコル SKDP(Secure Key Distribution Protocol)を提案する。

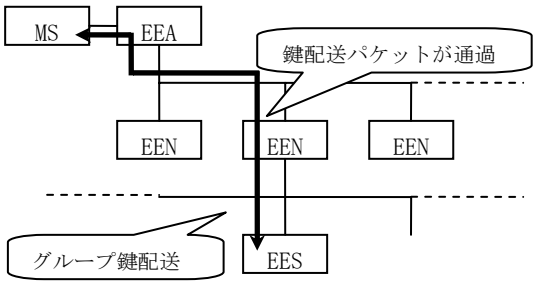


図 1　多段構成ネットワークと従来方式の問題点

3. セキュア鍵配送プロトコル SKDP

SKDP では、鍵配送パケットを受信した中間 EE がディジタル署名による認証を行い、その結果によりパケットの通過を決定する。そのため、MS と EE に表 1 に示すような情報を初期情報として保持させる。

表 1　各端末が所持している情報

EES/EEN/EEA	EE のユーザ ID(IDx) EE の秘密鍵(Prx) MS の公開鍵(PuS) ※暗号化された公開鍵(Eprs[Pux])
MS	MS の秘密鍵(PrS) 各 EE のユーザ ID(IDx) 各 EE の公開鍵(Pux)　(x=1, 2, 3…)

※追加した初期情報

従来の初期情報に加え、各 EE には EE の公開鍵を MS の秘密鍵(PrS)で暗号化した Eprs[Pux]を新たに追加する。

中間 EE は、終端 EE から MS、MS から終端 EE への両方向のパケットを認証する必要がある。

終端 EE からのパケットの中継判定を行うために、追加された初期情報 (Eprs[Pux])をパケットに付加して送信する。このデータは MS の公開鍵で復号できるため、どの EE でも Pux を取得することが可能である。この Pux を用いることで、中間 EE においてもパケットに付加されているディジタル署名の検証を行う事が可能となる。データの正当性が認められた場合は、MS に登録されたユーザが生成したパケットであると判断し、パケットを中継する。

MS からのパケットの転送判定は、初期情報として与えられた PuS を用いて、MS からのパケットに付加されているディジタル署名を検証することによって行う。これにより、データの正当性が認められた場合は、MS が生成したパケットであると判断し、パケットを中継する。

4. まとめ

この SKDP により、終端 EE と MS との間に中間 EE が存在していても、確実な認証によりパケットの中継可否を決定することが可能になる。

今後は提案方式を実装し、処理要求が増加した際の端末に掛かる負荷の計測といった機能評価を行っていく予定である。

参考文献

[1]　渡邊、岡崎、朴、井手口、笹瀬“イントラネット閉域通信グループの構築に適した安全な鍵配送方式とその運用管理方式”電気学会論文誌 C Vol.121-C，No.9 Sep.2001

多段構成ネットワークにおける鍵配送方式の一検討

情報科学科　渡邊研究室
11300J120
保母雅敏

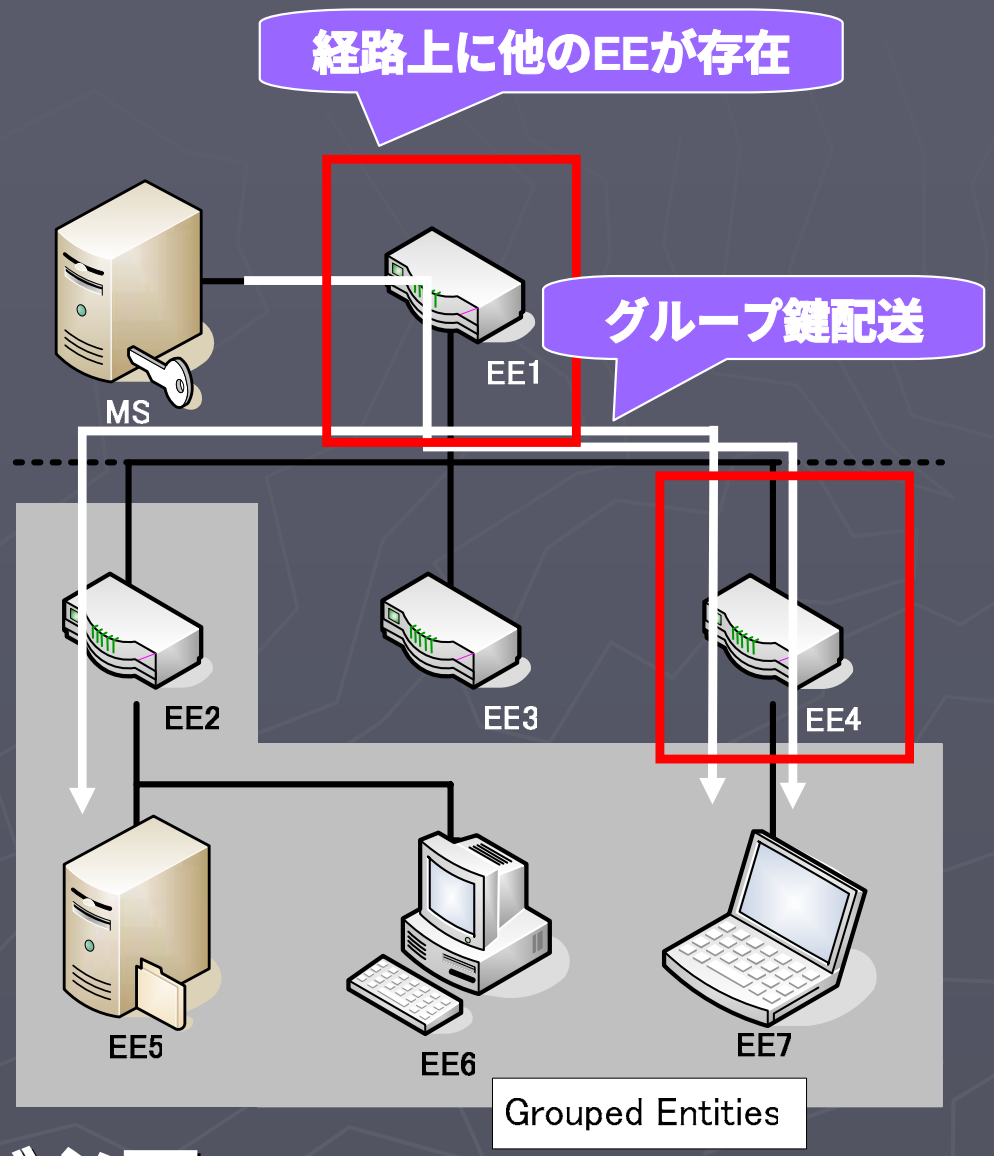
はじめに

- インターネット技術の発展
  - インターネット技術を利用したイントラネットの構築
- セキュリティに関する問題
  - イントラネット内での不正アクセス問題の深刻化

- イントラネット内で安全な通信を行う研究

Flexible Private Network (FPN)

- FPNでは・・・
  - 端末の移動や構成の変更に柔軟に対応できるシステム
  - 部署単位といった条件で複数の端末を一つのグループして扱う
  - グループ内の端末とは同じ暗号鍵(グループ鍵)で通信を行う
- 暗号装置(EE)
  - グループ情報に基づく暗号通信
  - 不正なパケットの通過を防止
- 管理装置(MS)
  - ユーザ作成、グループ情報、グループ鍵の管理
  - EEからの要求に応じてグループ鍵を配送



- 鍵配送には中間EEの通過が必要

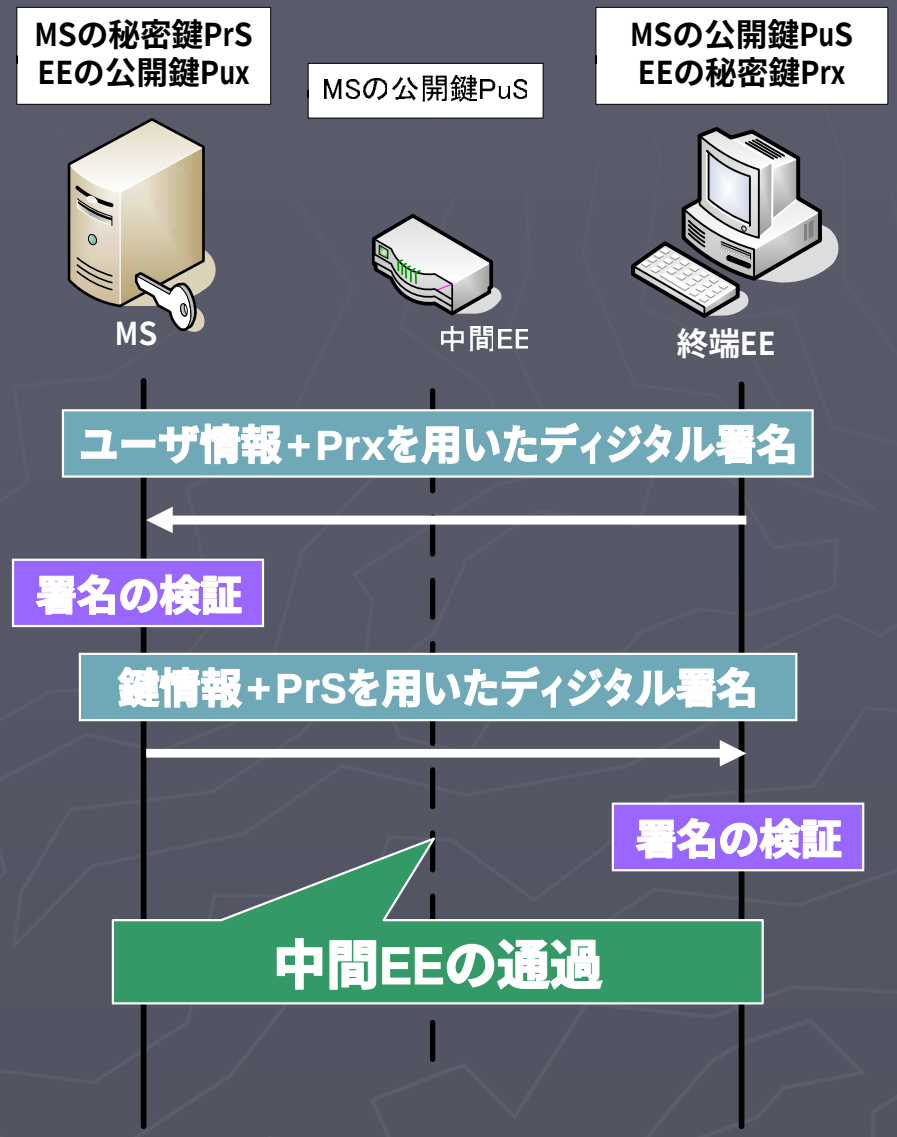
従来の鍵配送方式

公開鍵暗号によるディジタル署名の検証

- 公開鍵暗号
  - 暗号と復号に公開鍵、秘密鍵のペアを用いる暗号方式
  - 一方の鍵で暗号化したデータは、もう一方の鍵でないと復号出来ない
- ディジタル署名
  - 公開鍵暗号を利用し、メッセージの改竄をチェックする仕組み
  - 送信者の秘密鍵で暗号化
  - 受信者は送信者の公開鍵でメッセージを検証
  - メッセージが改竄されていないことを証明
  - 公開鍵と対になった秘密鍵の持ち主が作成したことを証明

従来の鍵配送方式

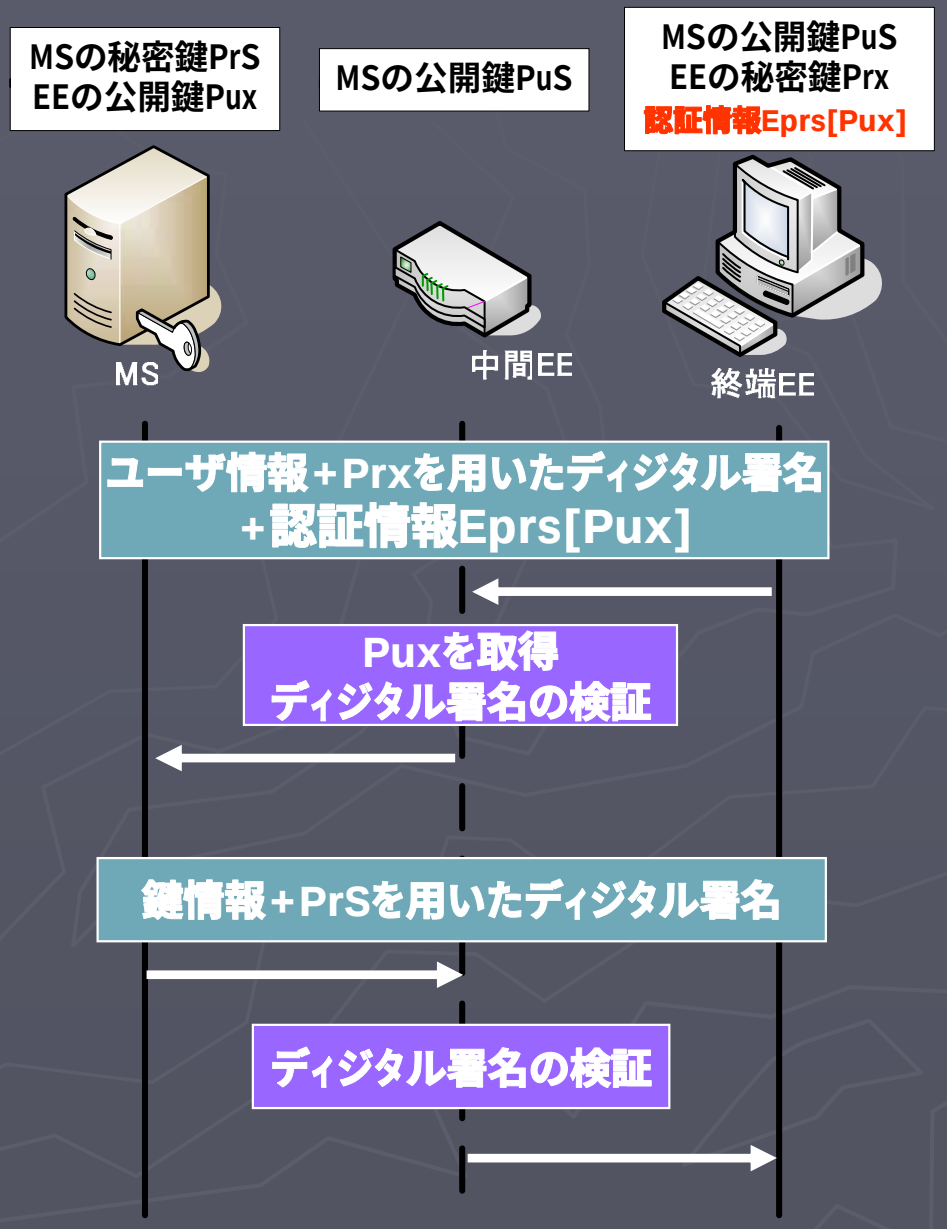
- 初期情報
  - EE・・・EE自身の秘密鍵Prx
    MSの公開鍵PuS
  - MS・・・MSの秘密鍵PrS
    各EEの公開鍵Pux
- ユーザ情報・・・ユーザIDなど
- 鍵情報・・・グループ鍵など
- End-to-Endでの認証
  - 中間EEの認証は考慮されていない
- 鍵配送パケットならば中継
  - 不正パケット通過の危険性



- 中間EEで認証によってパケットの通過を決定できる仕組み

セキュア鍵配送方式の提案

- 中間EEでのパケットの認証
  - 正規の端末が作成した鍵配送パケットのみを通過させる
- EEの初期情報に認証情報Eprs[Pux]を追加
  - MSが認証したEEの公開鍵であることを示す
  - PuSによりどのEEでも復号可能
- 終端EE-MS
  - 認証情報を付加して送信
  - MSが認証したEEが作成したパケットかどうかを検証
- MS-終端EE
  - 従来のパケットで送信
  - 初期情報PuSで認証



提案方式の利点

- 中間EEで鍵配送パケットの確実な認証が可能
  - 不正パケットの通過防止
- 認証情報をパケットに付加
  - 各EEが全EEの認証情報を保持しなくても良い
  - EEが移動しても認証が可能
  - ユーザの追加、グループ変更の影響を受けない

まとめ

- 通信経路上に中間EEが存在しても認証によって鍵配送パケットが通過できる方式を提案
  - 認証情報PrS[Pux]の追加による中間EEでのディジタル署名の検証
- システムの実装による機能評価
  - 中間EEの負荷の測定

おわり