イントラネット閉域通信グループにおける鍵管理方式の提案

Proposal of the key management method in Closed Communication Group for Intranet

保母　雅敏　Masatoshi Hobo,　渡邊　晃　Akira Watanabe (名城大学)

1. はじめに

イントラネット内でセキュアな通信をするための技術として、閉域通信グループを構築する研究が行われている。この研究の一つとして、グルーピングされた端末が共通鍵（グループ共通鍵）を使用して暗号通信を行うという方法が提案されている。この方法では、共通鍵を鍵管理サーバ（Management Server：MS）と呼ばれる専用の端末が配送するという方法が採られているが、共通鍵を更新する際に全ての端末の通信を一時停止させなければならないという課題がある。

そこで本提案では、グループ共通鍵を更新する際に通信を停止させることなく、鍵を更新することが可能な鍵管理方式を提案する。

2. 提案方式

対象となるシステムでは、セキュリティを確保するため、定期的にMSから共通鍵を配送する事を想定する。この場合、従来は通信中のすべての端末に対して一斉に共通鍵を配布し、切り替えのタイミングで一時的にシステムを停止状態にすることで新旧共通鍵の混在を防止していた。

提案方式では、鍵を配送する対象は常に起動状態にあるサーバのみとする。クライアントは、電源投入時に鍵配送を要求するという方法を採る。クライアント／サーバ間の通信中に、サーバに共通鍵が配送された場合、通信セッションが継続している間は旧鍵のまま通信を継続する。更新前の鍵を使った通信が全て終了した時点で更新前の鍵を破棄する。これにより、鍵更新をする際に通信を停止させることなく鍵を更新することが可能になる。

グループ共通鍵は暗号化処理以外に、グループに属している端末の認証(事前認証)にも使用されるため、同一グループで認証に使用できる鍵は、サーバに配送された最も新しい鍵のみであることが望ましい。これを実現するために、共通鍵にバージョン番号を付加する。事前認証では通信相手のグループ番号の確認と共に共通鍵のバージョンを確認することで、旧鍵を持つクライアントからの通信要求があった場合、クライアントに対して新鍵をMSから取得するように指示を与える。

3．鍵更新シーケンス概要

本提案を用いた通信の概要を図に示す。サーバ、クライアント1、クライアント2は同一のグループに属しているものとする。

① サーバにはMSにより定期的に共通鍵が配送される。
② クライアントは、電源投入時にMSに鍵配送要求を出し、共通鍵を受け取る。
③ クライアント１はサーバに対して通信を要求する。このとき事前認証により、同一のグループでありかつ共通鍵のバージョンが一致するため認証され、暗号通信が開始される。
④ MSによる鍵の定期配送。この時、サーバはクライアント１と旧鍵で暗号通信をしているため、旧鍵を保持したまま新鍵を受け取る。
⑤ クライアント２はサーバに対して通信を要求するが、事前交渉により共通鍵のバージョンが異なることが検出されるため、通信できない。
⑥ 事前交渉の結果を受け、クライアント２はMSに対して新しい鍵の配送を要求。この時、クライアント２は旧鍵を破棄する。
⑦ クライアント２は新鍵を使い、サーバに対して再度通信を要求する。事前認証により共通鍵のバージョンが一致するため認証され、暗号通信が開始される。
⑧ クライアント１とサーバとの通信終了。サーバに旧鍵を使った通信が存在しなくなるため、旧鍵は破棄される。クライアント１は旧鍵を所持したままであるが、次回の通信で新鍵を取得することになる。
⑨ クライアント２とサーバとの通信終了。両者とも新鍵のみを所持している。

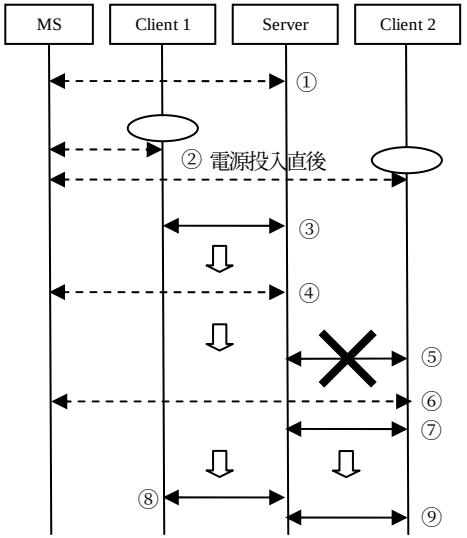


図　通信時の流れ

4．まとめ

イントラネット閉域通信ネットワークにおいて、現在行われている通信を停止させることなく共通鍵を更新させる方式を提案した。今後は提案方式を実装し評価を行う。また鍵を取得するにあたり、安全な鍵配送を行うことの出来るシステムを検討する。

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

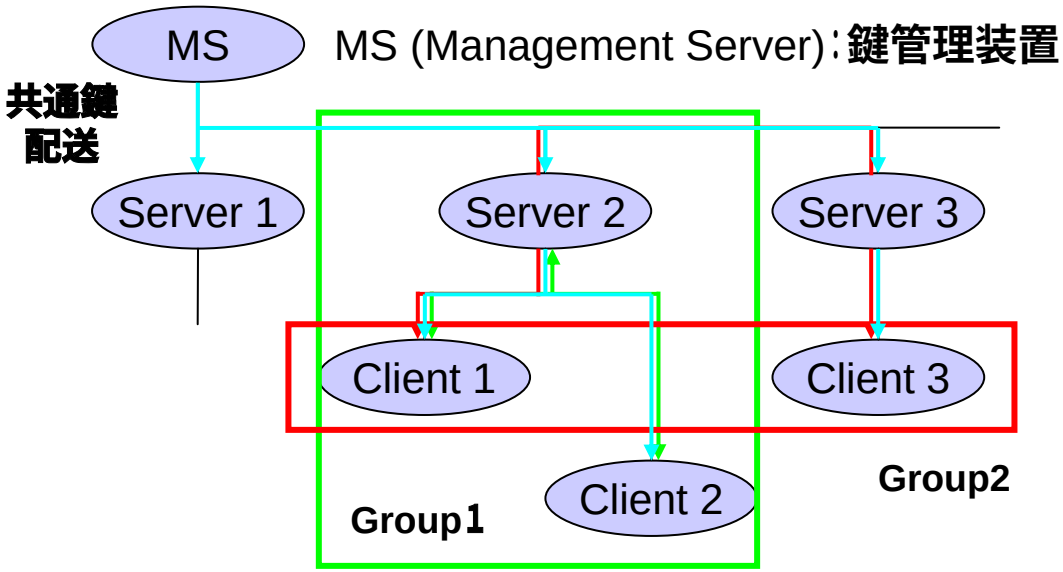
イントラネット閉域通信グループにおける鍵管理方法の提案

Proposal of the key management method in Closed Communication Group for Intranet

名城大学理工学部
保母 雅敏
渡邊 晃

研究の背景

- グルーピングによる暗号通信



グループ化された端末同士では、グループ共通鍵を使用して暗号通信を行う

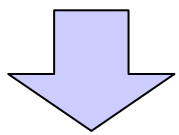
MSは各端末にグループ共通鍵を配送
セキュリティ上、定期的に共通鍵を更新

・Group1では、Server 2・Client 1・Client 2が、割り当てられた共通鍵を使用して暗号通信を行う

・Group2では、Client 1・Client 3が、割り当てられた共通鍵を使用して暗号通信を行う。Client 3は同じグループに属していないServer 2・Server 3とは通信が出来ない

事前認証と共通鍵の更新

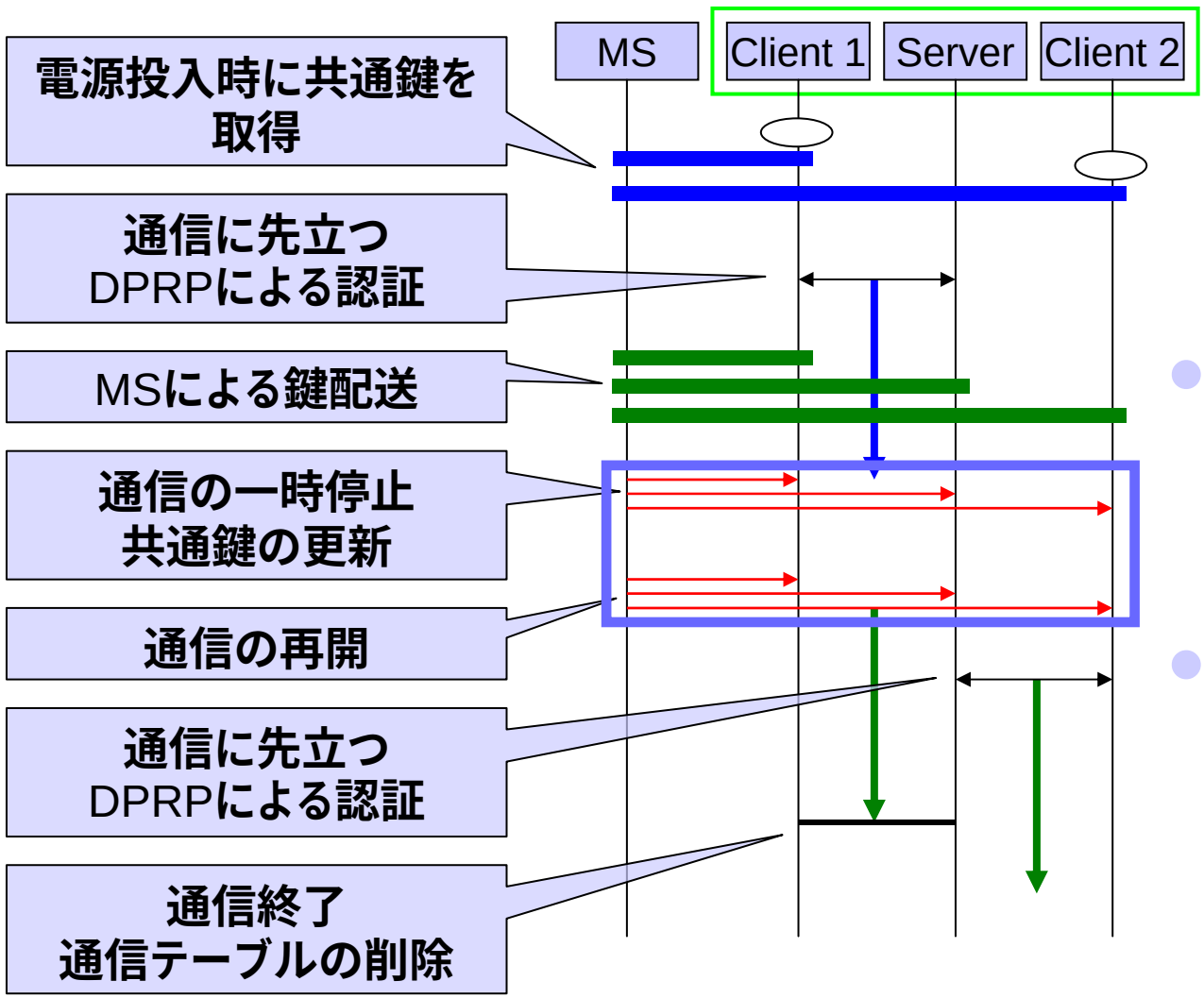
- 通信に先立ち、相手が同じグループに属しているかを確認するための認証(DPRP:動的処理解決プロトコル)を行う
  - DPRPによって通信が許可された端末間には、以後の通信を行うための通信テーブルが作成される
- DPRPの認証要素として、グループ共通鍵を使用
  - セキュリティ確保のための定期的な共通鍵更新の要求



新旧の共通鍵の混在による問題

- 暗号と復号で異なる共通鍵が使用される危険性

従来の解決方法

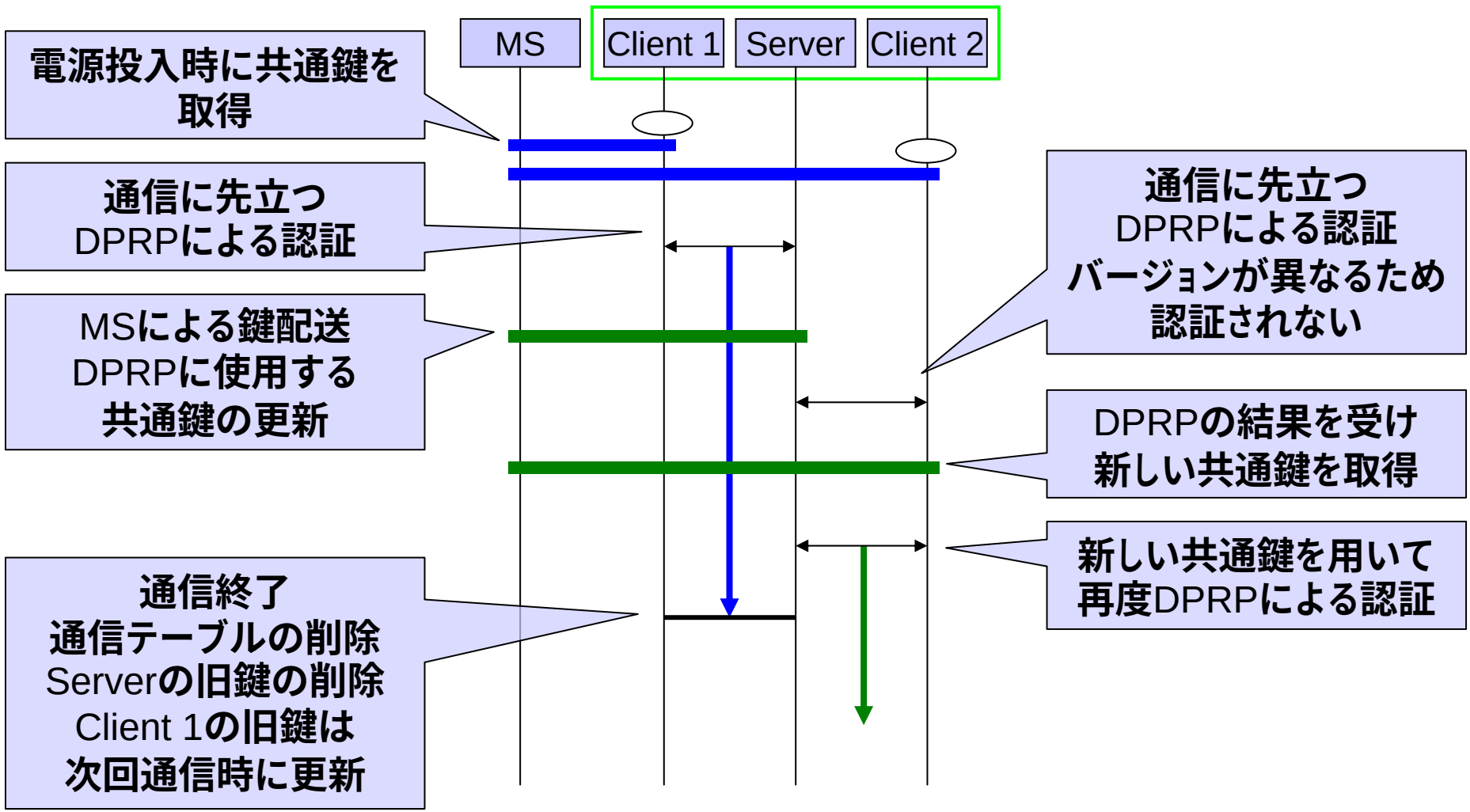


- 共通鍵混在を防ぐため同期を取る
  - 通信の一時停止
  - 端末の増加と共に停止時間も増加
- 更新の前後で暗号通信に使用する共通鍵も変わる

提案方式

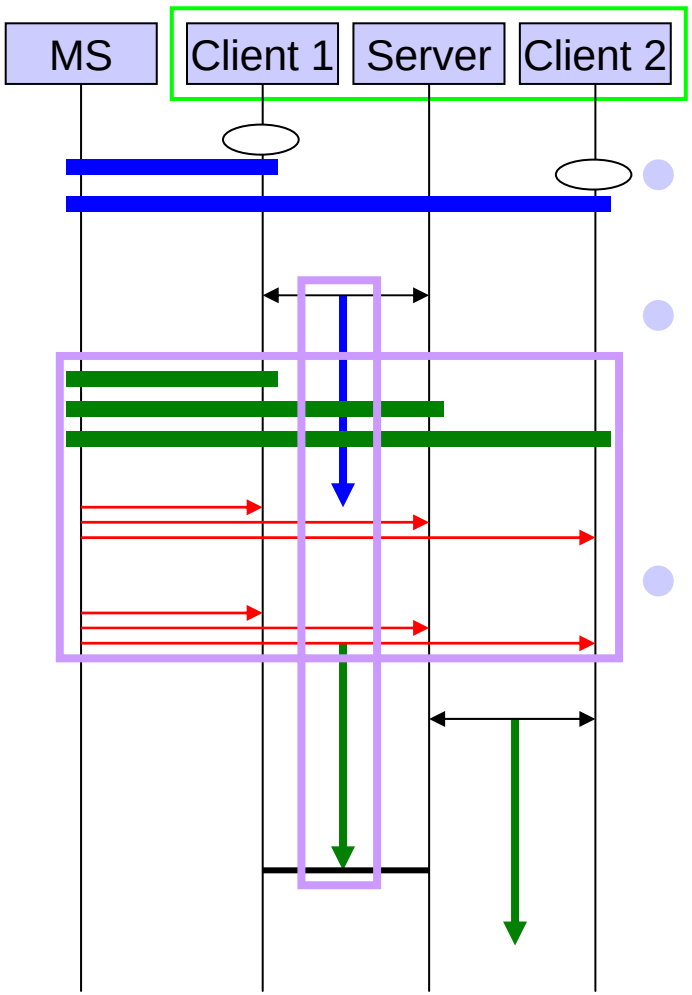
- 自動的に共通鍵を配送する対象はサーバのみ
  - クライアントは常時稼働ではないため、必要時に更新する
- 鍵更新時に通信中の端末とは旧鍵で通信を継続
  - 新旧の共通鍵でDPRPが行える可能性
- 共通鍵にバージョン番号を付加
  - DPRPで使用できる共通鍵を常に新しい鍵に限定する
- 通信終了時に旧鍵での通信が存在しなければ、旧鍵を破棄する
  - クライアントは、同じグループの共通鍵を1つしか所持していなければ、次回通信時に鍵を更新する

提案方式による鍵配送方式



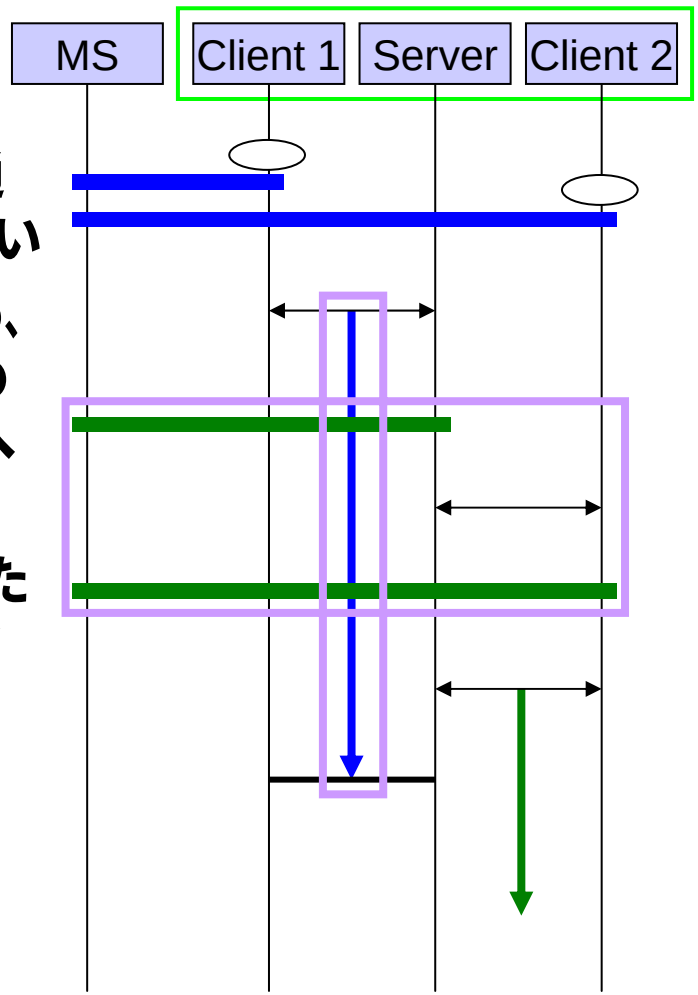
従来方式との比較

従来方式



- 鍵更新の前後で通信が一時停止しない
- 非同期更新のため、鍵更新時の動作の簡略化及び、MSへの負荷の分散
- DPRPで使用された共通鍵で通信終了まで暗号通信可能

提案方式



むすび

- まとめ
  - 通信を一時停止させない鍵更新方法の提案
    - 鍵更新の非同期化
    - 共通鍵へのバージョン番号の付加
- 今後の課題
  - 提案方式の実装と評価
  - 安全な鍵配送システムの検討

おわり