NTMobileにおけるNTM端末とDC間の認証強化に係わる検討

110425300　三輪 卓也
渡邊研究室

1. はじめに

我々はあらゆるネットワーク環境において移動しながら通信ができる技術として，通信接続性と移動透過性を同時に実現する NTMobile（Network Traversal with Mobility）を提案している．NTMobile におけるモバイル端末の認証方法は，現状ではパスワードを利用しているが，この方法ではパスワードの漏洩などに対処できず，セキュリティ上万全とは言えない．本稿では，その対策として公開鍵証明書をモバイル端末に保持させる方式について提案する．スマートフォンは耐タンパ性が保障されていないため，秘密鍵が漏洩する懸念があるが，秘密鍵をパスワードで暗号化することにより，これを防止する．

2. NTMobile

NTMobile は，NTMobile の機能を実装した端末（以下 NTM 端末）と NTM 端末の管理や通信経路の指示を行う Direction Coordinator（以下 DC），必要に応じて通信を中継する Relay Server（以下 RS）から構成される．NTM 端末はネットワークを切り替えても変化しない仮想 IP アドレスを DC から割り当てられる．仮想 IP アドレスに基づくパケットを実 IP アドレスによりカプセル化し，実 IP アドレスの変化をアプリケーションに対して隠蔽することによって移動透過性を実現している [1]．DC と RS はいずれもサービス提供者が管理する装置であるため，信頼関係があることを前提としている．NTM 端末はアカウント取得時にパスワードを DC に登録することにより DC との信頼関係を構築する．NTM 端末は DC の公開鍵証明書を用いて DC 側を認証するとともに共通鍵を共有する．次にユーザがアカウント取得時に登録したパスワードを DC に送信することにより NTM 端末側を認証する．しかし，この方法ではパスワードが漏れると他の端末からもログインできるため安全性が低い．

3. 提案方式

DC のみに発行していた公開鍵証明書を NTM 端末にも持たせることで双方向の確実な認証を行う．NTM 端末が保持する秘密鍵はユーザが設定するパスワードで暗号化する．ユーザがログインするには所定の NTM 端末を保持し，かつパスワードを知っている必要があり，安全性が高まる．

3.1 端末の登録方法

ユーザは NTMobile のアカウント作成用アプリケーションを起動し，アカウントサーバに接続する．必要事項を入力することにより，秘密鍵/公開鍵ペアの生成とアカウント登録要求を行う．その際生成した秘密鍵はユーザのパスワードで暗号化して端末に保持する．本人確認及び証明書発行審査が完了すると，アカウントサーバから公開鍵証明書が発行される．

3.2 認証方法

図 1 に NTM 端末の認証処理シーケンスを示す．ユーザはログイン画面より Login ID とパスワードを入力する．NTM 端末はまず秘密鍵をパスワードで復号する．次に NTM 端末は通常の SSL 通信により DC を認証するとともに共通鍵を共有する．NTM 端末は秘密鍵を用いて Login ID と FQDN，自身の公開鍵証明書と共に電子署名（$\mathrm{PriKey}_{\mathrm{NTM}}[\mathrm{h[ID]}]$）を DC に送信する．これを受け取った DC は NTM 端末の公開鍵証明書の検証を行う．アカウントサーバによって発行された正規なものであることが確認されると，証明書に含まれる NTM 端末の公開鍵を用いて，電子署名（$\mathrm{PriKey}_{\mathrm{NTM}}[\mathrm{h[ID]}]$）を検証し，NTM 端末を認証する．その後，共通鍵 $\mathrm{CK}_{\mathrm{NTM\text{-}DC}}$ を生成し Login Response により配布する．$\mathrm{CK}_{\mathrm{NTM\text{-}DC}}$ は以後の NTM 端末と DC との間の全ての通信における暗号鍵と認証鍵に利用する．

この手法により，NTM 端末の保有者でかつパスワードを知っているユーザのみが DC との信頼関係を構築できる．パスワードは秘密鍵を復号するためだけに使用されるので，どこにも保管されず送信もされない．ユーザの頭の中に留まるのみという点でセキュリティ性がより向上している．従来の方式との親和性も保たれており，ユーザ目線からは認証の流れに大きな変化がないことも特徴である．そのため，本提案方式を従来の方式に追加することでユーザがどちらの方式を使用するか選択できる方法を採ることができる．

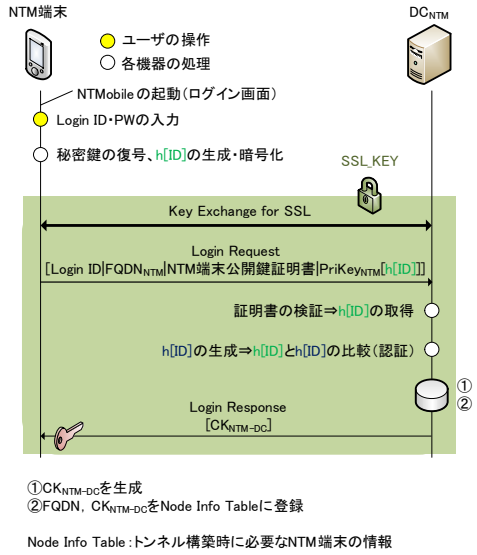


図 1: NTM 端末の認証処理シーケンス

4. まとめ

本稿では，NTMobile における NTM 端末と DC 間のセキュリティをより強化した認証方法について提案した．今後は提案方式の実装を行い，性能評価を行う予定である．

参考文献

[1] 内藤．他：NTMobile における移動透過性の実現と実装，情報処理学会論文誌 Vol.54, No.1, pp.380–393, 2013.

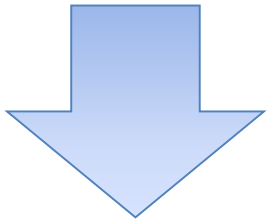
NTMobileにおけるNTM端末とDC間の認証強化に係わる検討

名城大学　理工学部　情報工学科
渡邊研究室
110425300　三輪 卓也

Watanabe Lab.

はじめに

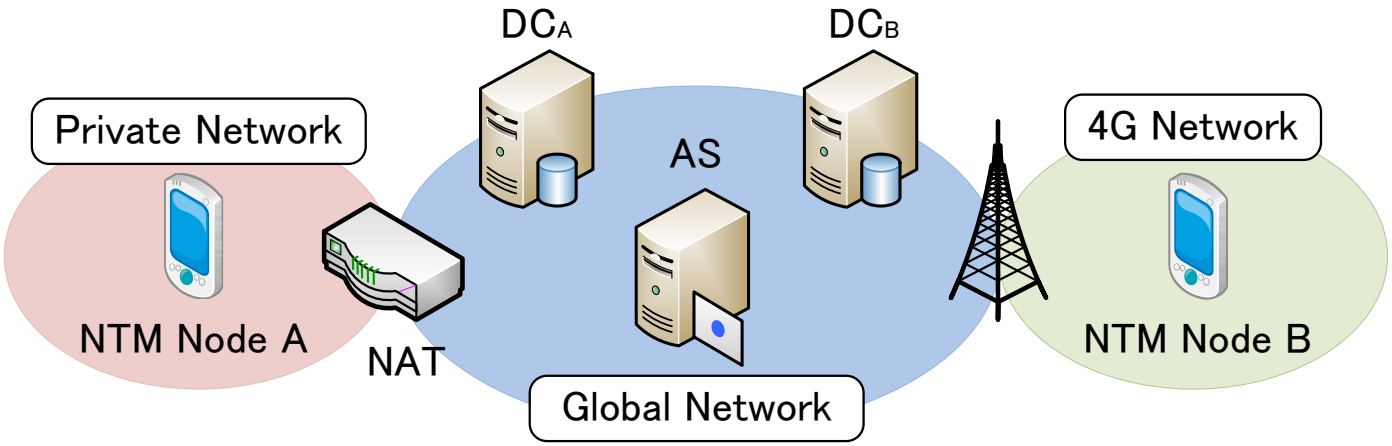
- 通信接続性の確立
  - 相手のネットワーク環境に影響されず通信を開始できる
- 移動透過性の実現
  - 通信中にネットワークを切り替えても通信が継続



NTMobile（Network Traversal with Mobility）

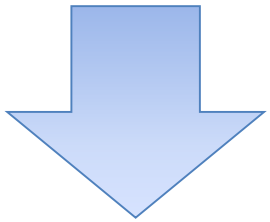
NTMobileの構成

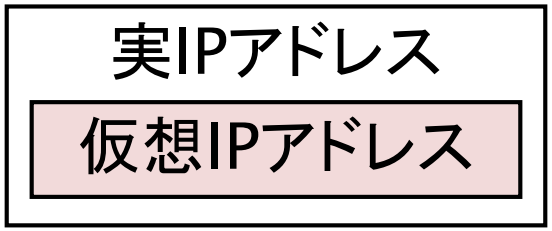
- NTM端末
  - NTMobileを実装した端末
- DC（Direction Coordinator）
  - NTM端末の管理や通信経路の指示
  - 仮想IPアドレスの配布
- AS（Account Server）
  - ユーザのアカウント情報を管理



NTMobileの概要

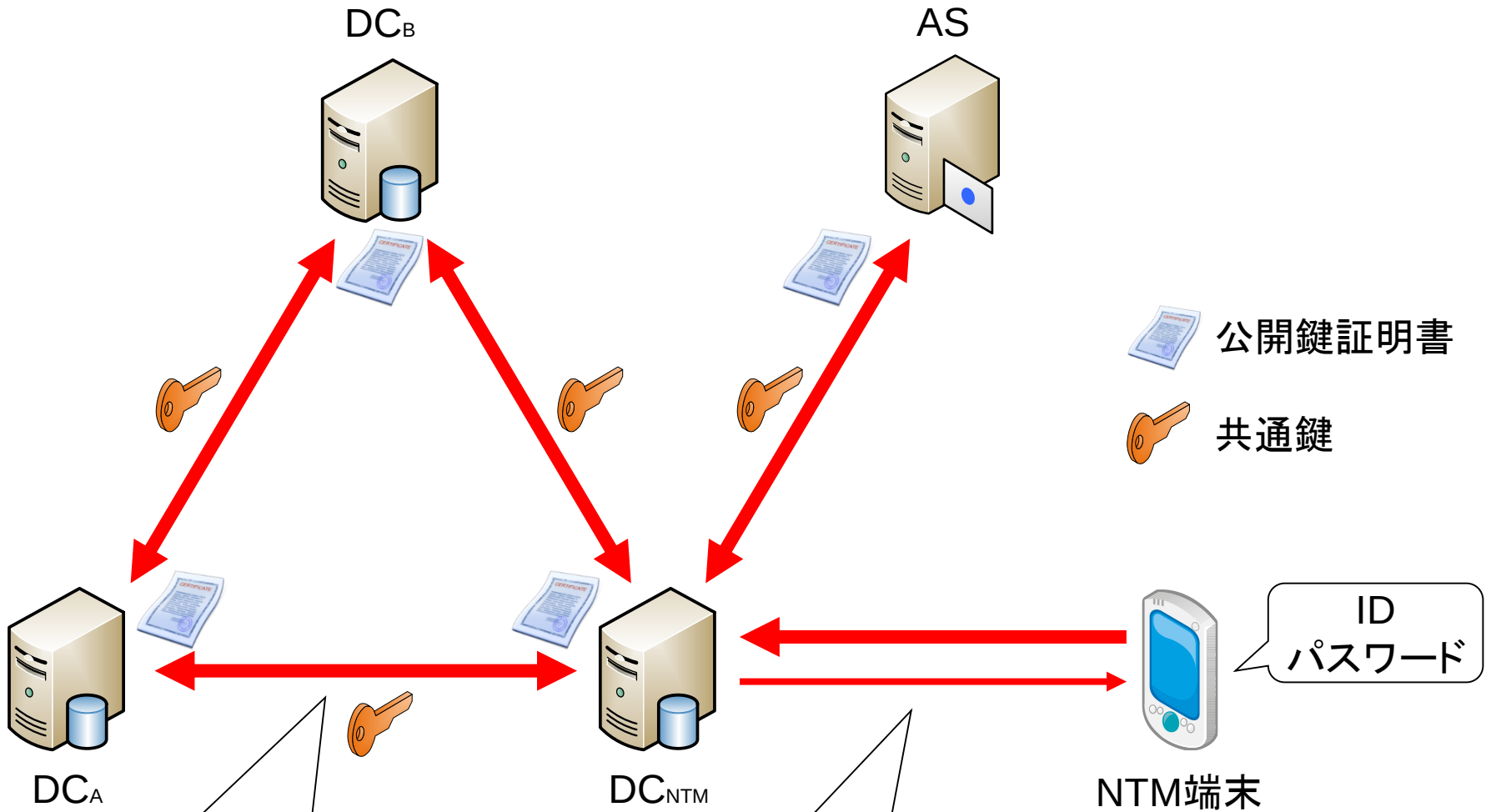
- DCはNTM端末に仮想IPアドレスを割り当てる
  - 仮想IPアドレス：接続先のネットワークを切り替えても変化しない一意なアドレス
- NTM端末は仮想IPアドレスに基づくパケットを実IPアドレスによりカプセル化



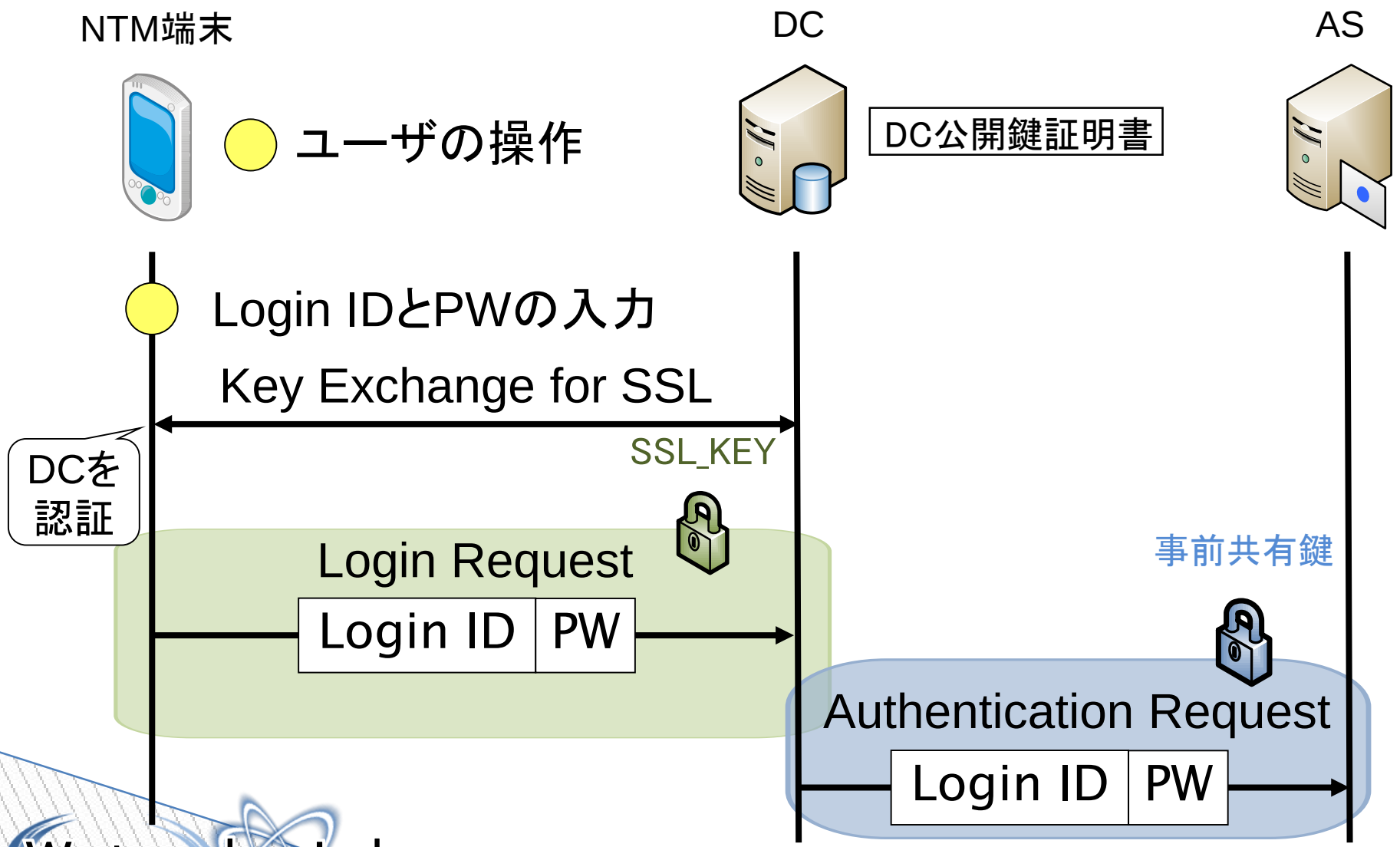


- アプリケーションに対して実IPアドレスの変化を隠蔽することによって移動透過性を実現

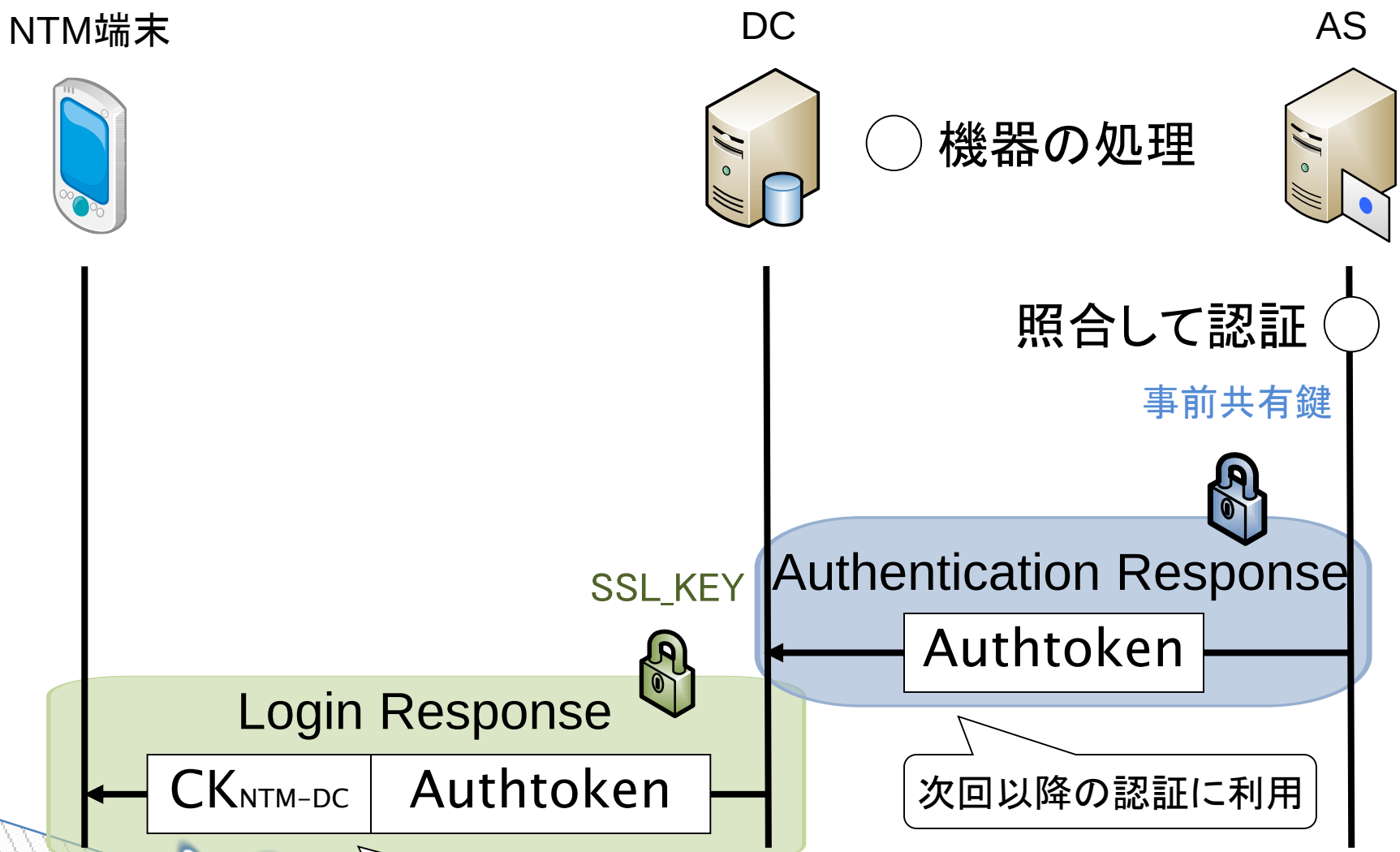
NTMobileのセキュリティ



NTM端末の認証シーケンス(1)

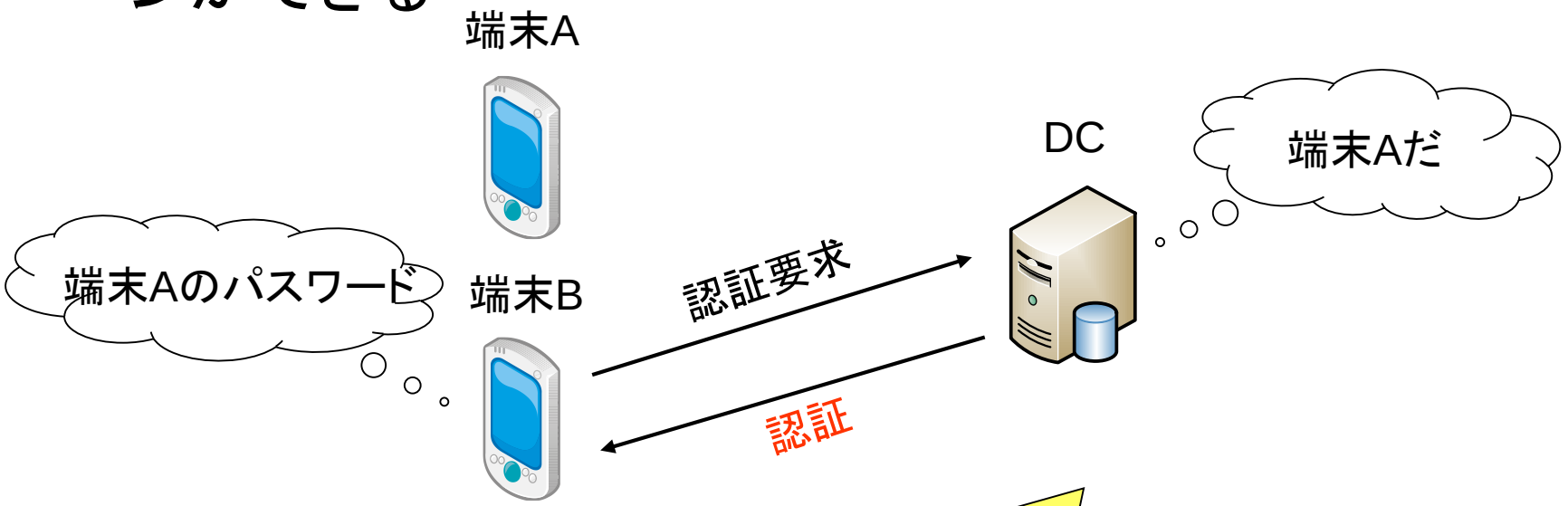


NTM端末の認証シーケンス(2)



NTM端末の認証方法における課題

- なりすましによるログイン
  - パスワードが漏れた場合，他の端末からもログインができる



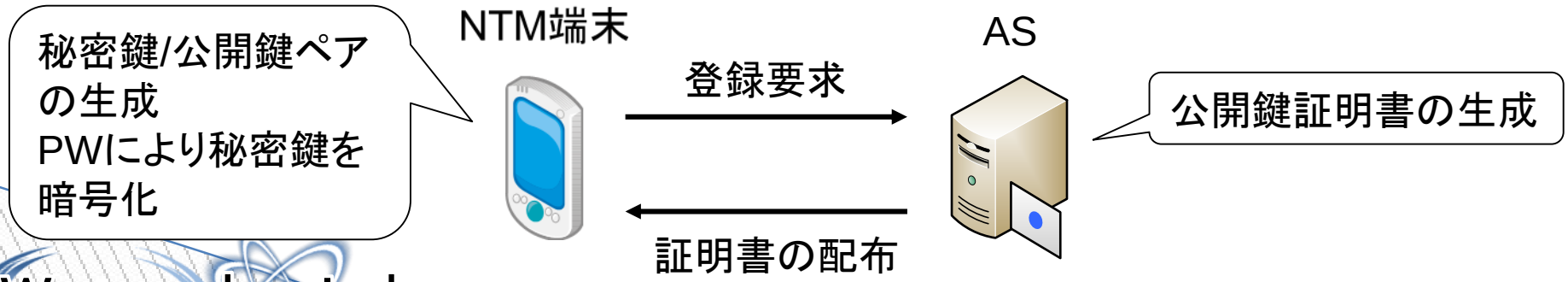
改善の余地がある

認証方式の提案

- NTM端末も公開鍵証明書を保持
  - DCとの双方向の確実な認証
- 秘密鍵をパスワードで暗号化して保持
  - 耐タンパ性が保障されていないことを考慮
  - パスワードはどこにも保管されず，送信もされない

NTM端末の登録方法

- アカウント作成
  - 秘密鍵/公開鍵ペアの生成
  - Login ID・パスワード，個人情報を入力
  - パスワードに基づき秘密鍵を暗号化，Login IDと個人情報をASに送信
- ASの処理
  - 審査をした上で，公開鍵証明書を発行



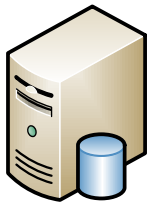
提案方式の認証シーケンス(1)

NTM端末

暗号化したNTM端末秘密鍵

NTM端末公開鍵証明書

DC



DC公開鍵証明書

AS公開鍵証明書

NTMobileの起動(ログイン画面)

Login IDとPWの入力

PWで秘密鍵を復号

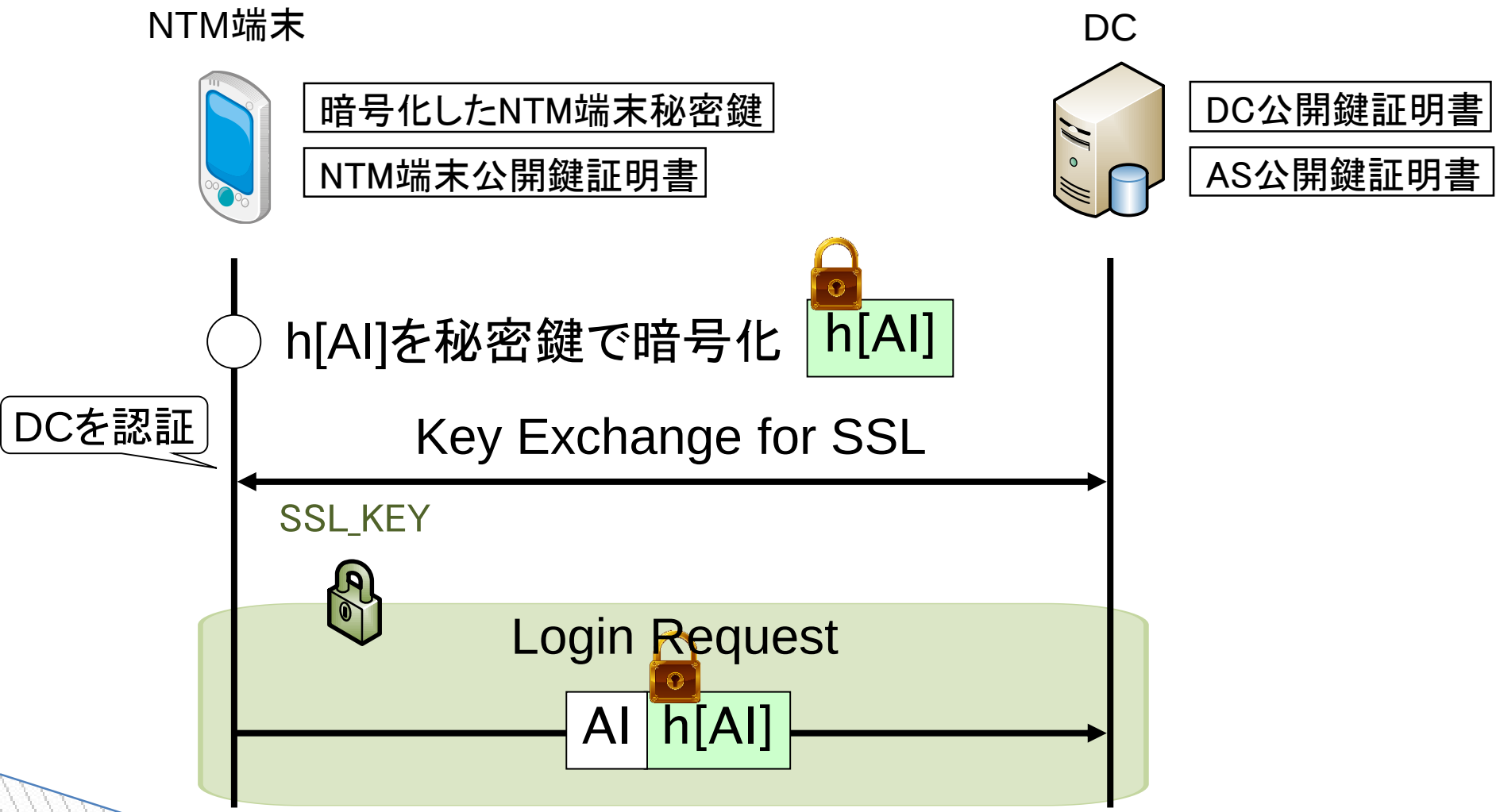
認証情報のダイジェストを生成

h[AI]

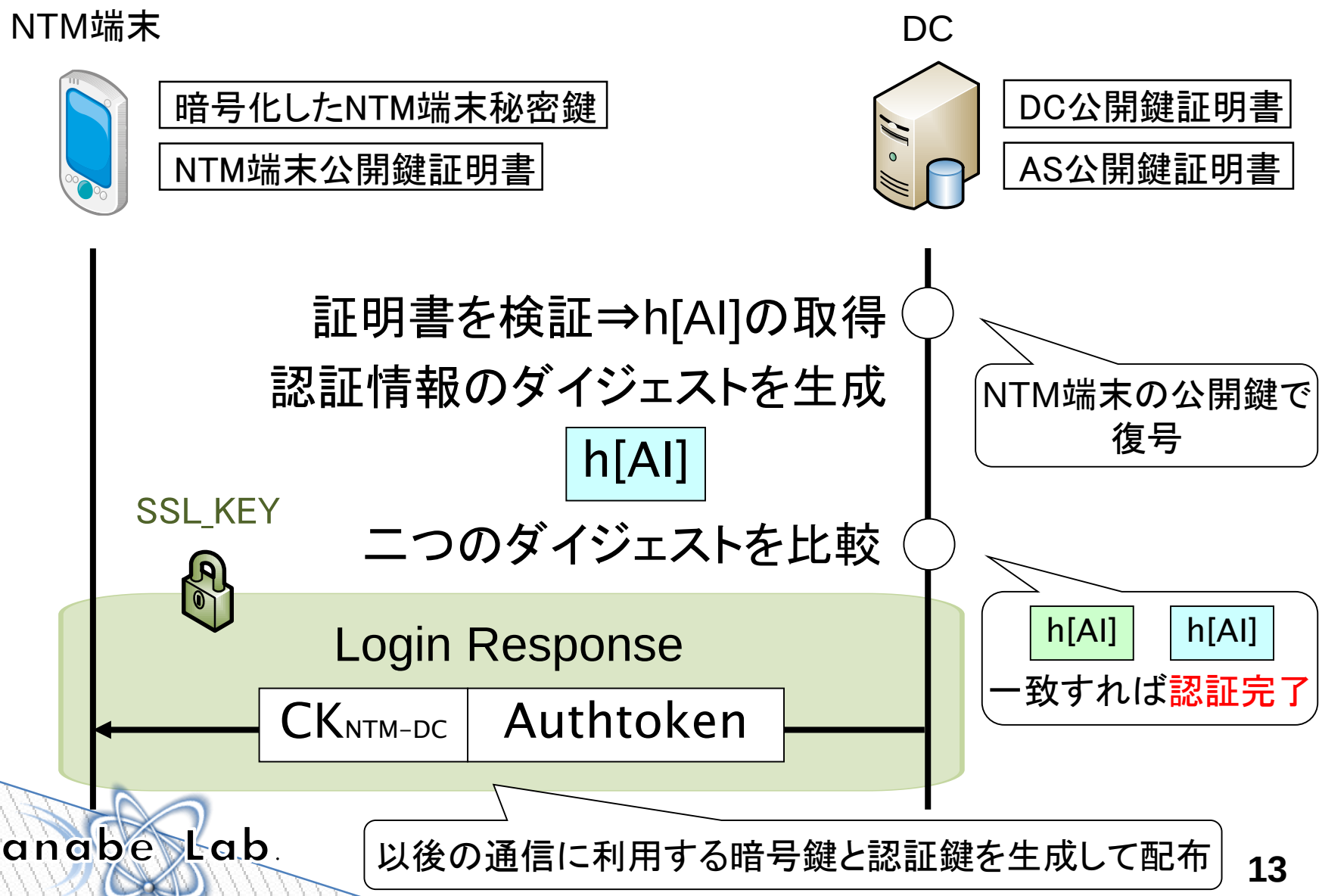
AI:Login ID, FQDN, 公開鍵証明書

黄丸はユーザのアクション
白丸は各機器の処理
を示す

提案方式の認証シーケンス(2)



提案方式の認証シーケンス(3)



評価

	現状の方式	提案方式
不正ログイン	△	○
辞書攻撃	△	○
利便性	○	△

辞書攻撃：辞書（ファイル）に載っている単語を試行し，パスワードを解析する手法
利便性：ユーザ側，管理者側から総合的に評価

まとめ

- NTM端末の認証方法の改善
  - なりすましによるログインを防止する必要性
- 提案する認証方法
  - 所定のNTM端末とパスワードによる認証
  - 秘密鍵の暗号化・復号にパスワードを利用
- 今後について
  - 提案方式の実装を行い，性能評価を行う