NTMobile における NTM 端末の認証方法の強化

三輪　卓也[†*]，鈴木　秀和[†]，内藤　克浩[‡]，渡邊　晃[†]([†]名城大学，[‡]愛知工業大学)

Reinforcement of Authentication Method of NTM Terminal in NTMobile

Takuya Miwa[†], Hidekazu Suzuki[†], Katsuhiro Naito[‡], Akira Watanabe[†] ([†]Meijo University, [‡]Aichi Institute of Technology)

1　はじめに

なりすましによるシステム等への不正ログインが相次いで問題となっており，より確実性のある認証が求められている．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送信することにより認証をしているが，この方法ではパスワードの漏洩などに対処できず，セキュリティ上安全ではない．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ておく方式について提案する．

2　NTMobile

<2・1>概要　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 端末は接続先の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 より割り当てられる．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．

<2・2>NTM 端末の認証方法とその課題　NTM 端末は DC の公開鍵証明書を用いて DC を認証するとともに共通鍵を共有する．次にユーザが NTM 端末に入力したパスワードと ID（メールアドレス）、FQDN を DC に送信することで NTM 端末を認証する．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

<3・1>概要　セキュリティが重要視される企業向けを想定する．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 端末の耐タンパ性は保障されていないため，NTM 端末が保持する秘密鍵は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・2>端末の登録方法　ユーザは DC の管理者に依頼し，秘密鍵/公開鍵のペアの生成，及び証明書を発行してもらう．生成された秘密鍵をユーザのパスワードで暗号化し，証明書と共に NTM 端末に埋め込む．DC は ID（メールアドレス）を登録する．

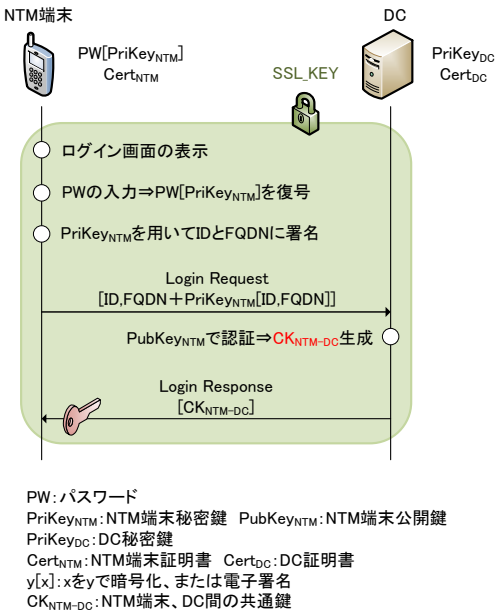


Fig. 1　NTM 端末の認証処理シーケンス

<3・3>認証方法　Fig. 1 に NTM 端末の認証処理シーケンスを示す．ログイン時，NTM 端末は DC の公開鍵証明書を用いて DC を認証するとともに SSL 共通鍵を共有する．ユーザはログイン画面よりパスワードを入力する．NTM 端末は暗号化された秘密鍵をパスワードで復号する．この秘密鍵を用いて NTM 端末は ID と FQDN と共に電子署名を DC に送信する．これを受け取った DC は NTM 端末の公開鍵を用いて ID と FQDN を復号し，NTM 端末を認証する．その後，共通鍵 CK$_{NTM-DC}$ を生成し Login Response により配布する．CK$_{NTM-DC}$ 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ネットワークを流れることがなく，セキュリティ性がより向上している．

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．

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.

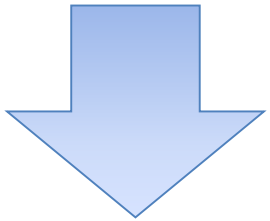
NTMobileにおける NTM端末の認証方法の強化

†名城大学　理工学部　情報工学科
‡愛知工業大学　情報科学部　情報科学科
三輪卓也†　鈴木秀和†　内藤克浩‡　渡邊晃†

Watanabe Lab.

はじめに

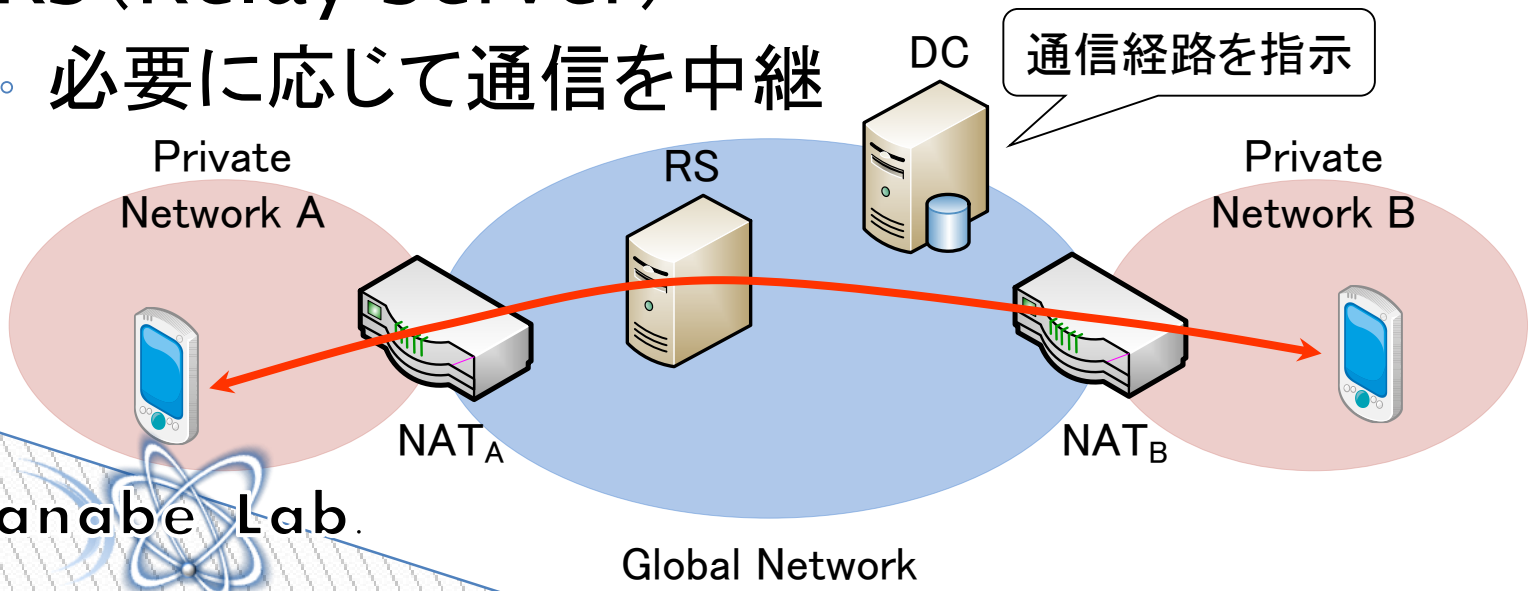
- 通信接続性の確立
  - 相手のネットワーク環境に影響されず通信を開始できる(NAT越え問題)
- 移動透過性の実現
  - 通信中にネットワークを切り替えても通信が継続



NTMobile(Network Traversal with Mobility)

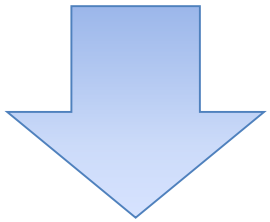
NTMobileの概要(1)

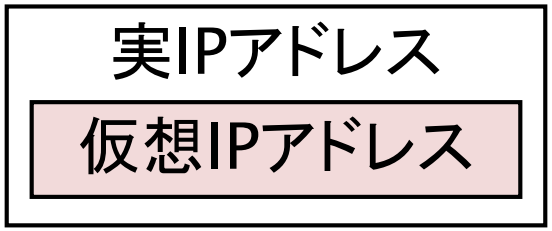
- NTM端末
  - NTMobileを実装した端末
- DC(Direction Coordinator)
  - NTM端末の管理や通信経路の指示，仮想IPアドレスの配布
- RS(Relay Server)
  - 必要に応じて通信を中継



NTMobileの概要(2)

- 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

現状のNTMobileのセキュリティ

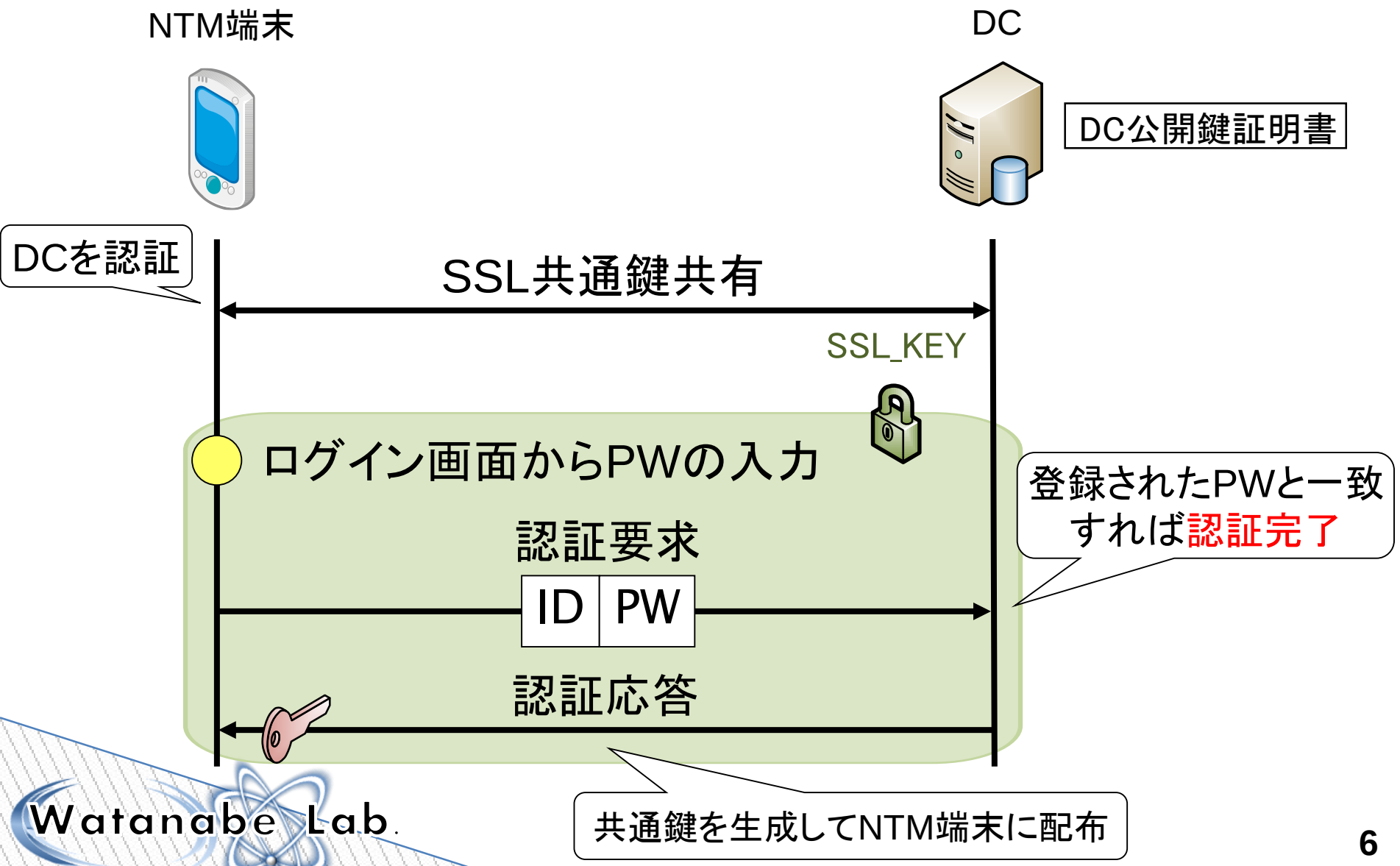
- DC・RS
  - サービス提供者が管理するため相互に信頼関係があることを前提
  - 各装置にはrootDCから公開鍵証明書を発行

rootDC：各DCを管理する最上位DC

- NTM端末
  - 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信頼関係を構築
  - ID・パスワードをDCに送信することで認証
  - 証明書の発行はなし

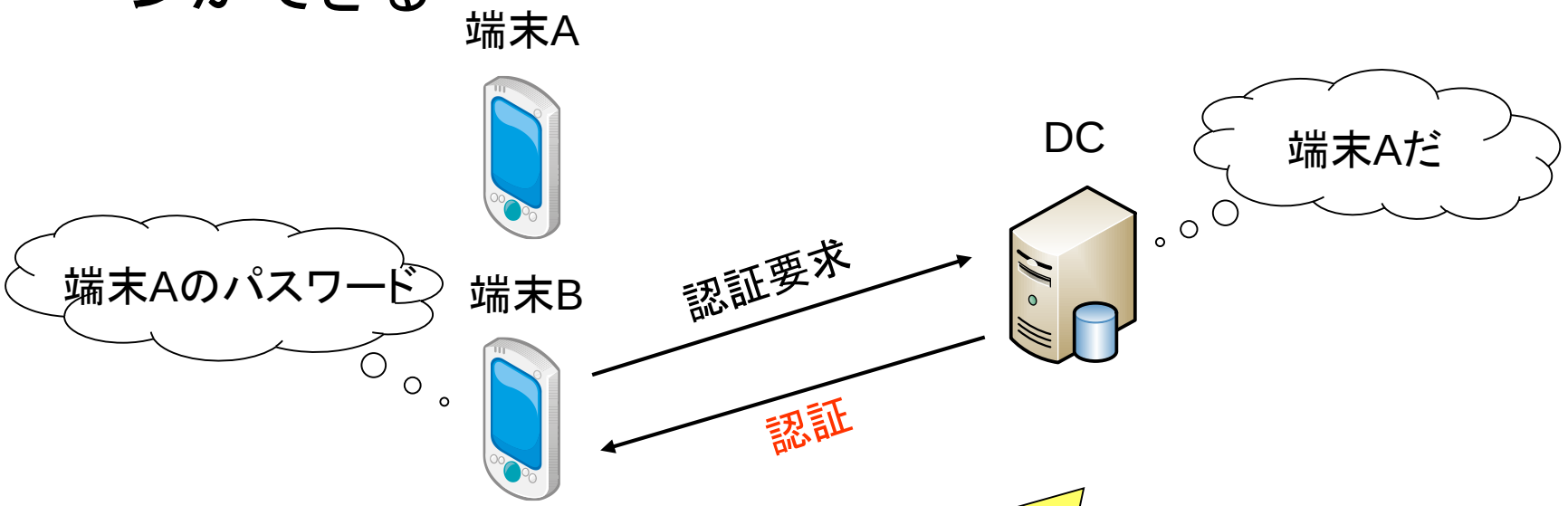
ID：ユーザの登録するメールアドレス

現状のNTM端末の認証シーケンス



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

提案する認証方法について

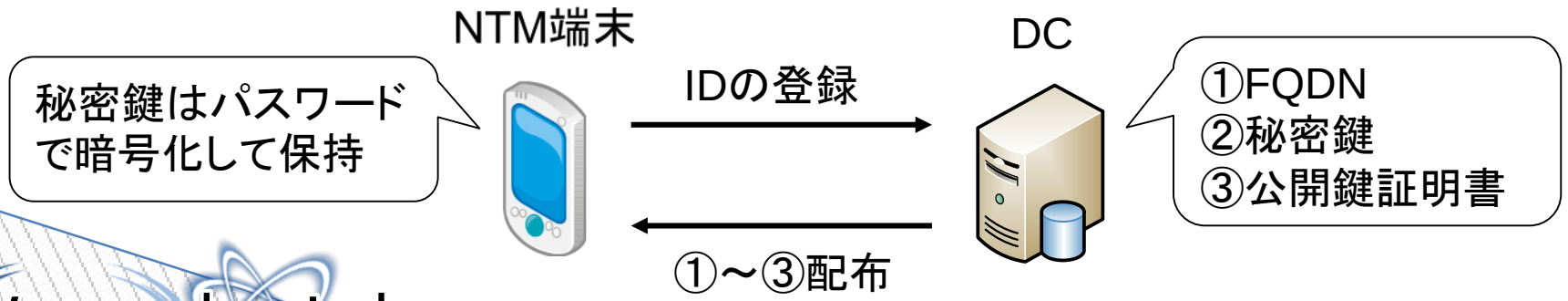
- NTM端末のより確実な認証
  - セキュリティが重要視される企業等に適した方法

- 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

NTM端末の登録

- DCへIDを登録
  - DCの管理者に依頼し，直接登録

- DCの処理
  - IDを基にFQDNを生成
  - NTM端末の公開鍵および公開鍵証明書，秘密鍵の生成



各装置の初期情報

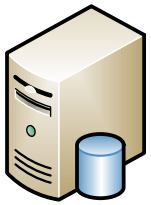
NTM端末	DC
パスワードで暗号化したNTM端末秘密鍵	DC秘密鍵
NTM端末公開鍵証明書	DC公開鍵証明書

- NTM端末もDCと同じように公開鍵・秘密鍵ペアを初期情報として保持

認証処理シーケンス(1)

NTM端末

DC



ログイン画面の表示

パスワードの入力

パスワードで秘密鍵を復号

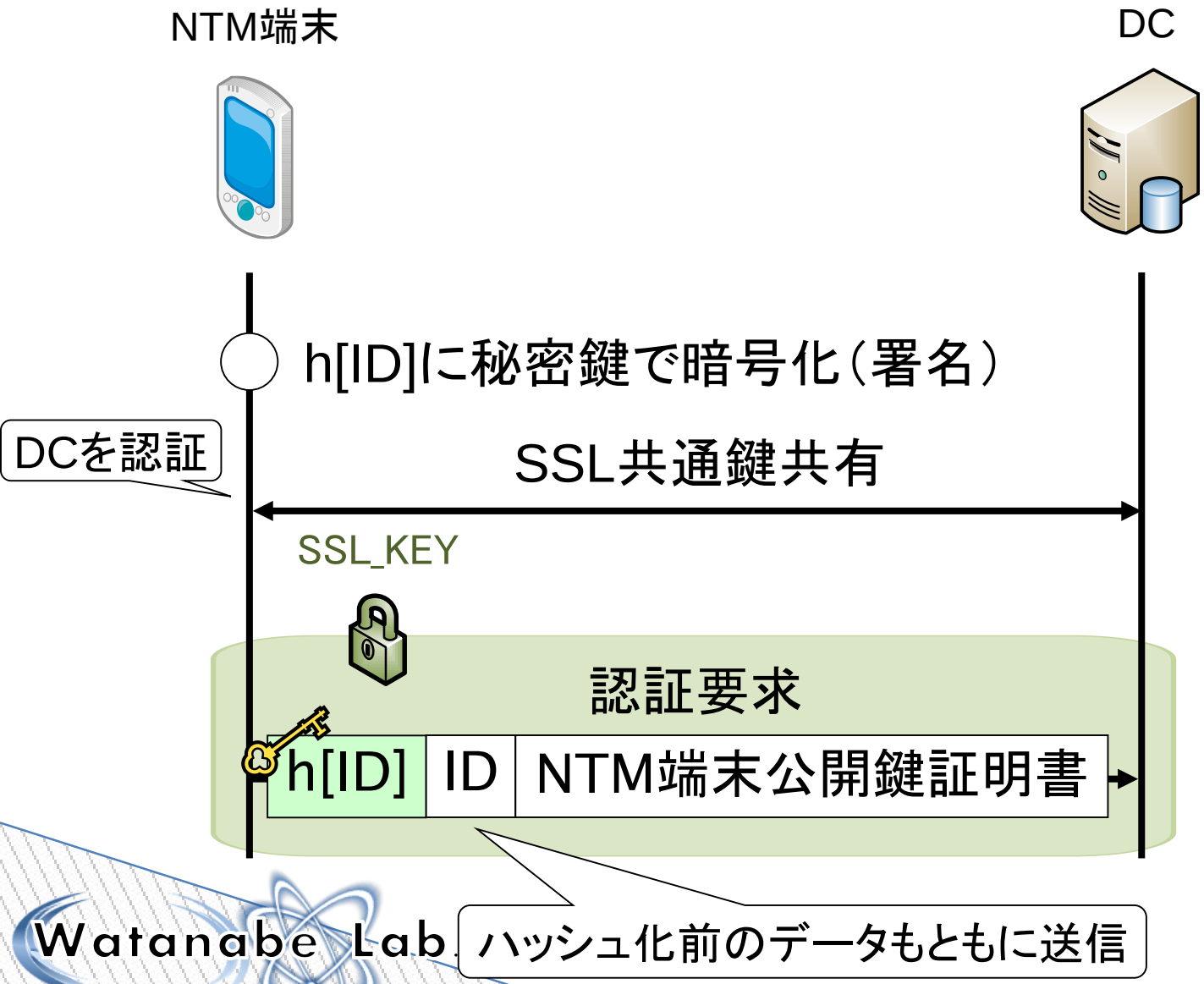
IDのダイジェストを生成

h[ID]

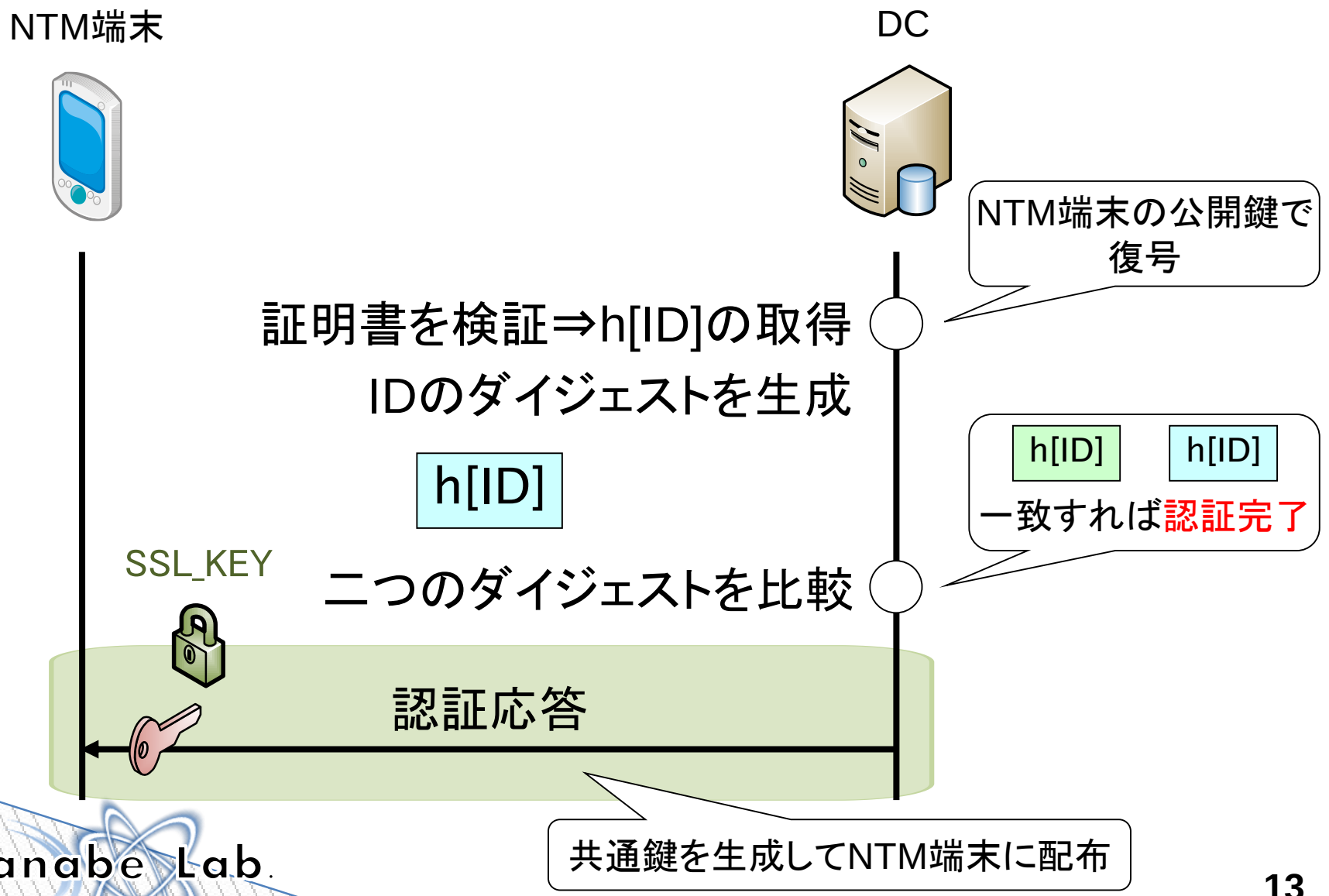
黄丸はユーザのアクション
白丸は各機器の処理
を示す

Watanabe Lab.

認証処理シーケンス(2)


NTM端末
DC
h[ID]に秘密鍵で暗号化(署名)
DCを認証
SSL共通鍵共有
SSL_KEY
認証要求
h[ID]
ID
NTM端末公開鍵証明書
ハッシュ化前のデータもともに送信

認証処理シーケンス(3)


NTM端末
DC
NTM端末の公開鍵で復号
証明書を検証⇒h[ID]の取得
IDのダイジェストを生成
h[ID]
h[ID]
h[ID]
一致すれば認証完了
SSL_KEY
二つのダイジェストを比較
認証応答
共通鍵を生成してNTM端末に配布

提案する認証方法の利点

- 認証が完了する条件
  - 所定のNTM端末を保持
  - パスワードを知っている

二つの条件による認証で安全性が向上

なりすましによるログインの防止

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
  - パスワードは秘密鍵の復号にのみ使用
- 今後について
  - 提案方式の実装を行い，性能評価を行う