3V-05

VpnService 型 NTMobile システムへのユーザ認証機能の導入

山田 貴之 [†1]　上野 泰輔 [†2]　鈴木 秀和 [†1]　内藤 克浩 [†3]　渡邊 晃 [†1]
[†1] 名城大学大学院理工学研究科　[†2] 名城大学理工学部　[†3] 愛知工業大学情報科学部

1 はじめに

筆者らは，複雑化したインターネット環境において，通信接続性と移動透過性を実現する技術として NTMobile（Network Traversal with Mobility）[1] を提案しており，これまでに複数の実装モデルを設計，実装を行ってきた．NTMobile では，今後の実用化を見据え，ID 連携プロトコルである OpenID Connect の仕組みを用いることで，NTMobile ユーザの認証に関わるユーザ情報の管理を NTMobile の枠組みから切り離すことを検討している [2]．本稿では，Android 端末において root 権限を必要としない実装モデルである VpnService 利用型 [3] へ OpenID Connect を用いたユーザ認証方式の基礎的実装を行い，その実現性および有用性を確認する．

2 NTMobile

2.1 概要

NTMobile では，NTMobile の通信を行う端末（以後，NTM 端末）に不変の仮想的な IP アドレスを割り当てる．NTM 端末上で動作するアプリケーションは，仮想 IP アドレスを用いてコネクションを確立することで，ネットワークの移動に伴う実 IP アドレスの変化や経路上のネットワークの影響を受けない．また，アプリケーションが送信した仮想 IP アドレスに基づくパケットは，NTM 端末間で交換した共通鍵を用いて暗号化トンネルを構築し，UDP によるカプセル化を行う．暗号化トンネルは特定の状況下を除いてエンドツーエンドで構築されるため，常に最適な経路でセキュアな通信を実現できる．これまでに様々な利用環境に応じた実装モデルを複数提案しており，今後は NTMobile による移動透過性やセキュアな直接通信を利用したいアプリ開発者やサービス事業者に，NTMobile の枠組みを提供することを検討している．

2.2 ユーザ認証方法

図 1 にパスワードを用いた従来型認証方式を示す．従来の NTMobile では，予めに AS（Account Server）に対してアカウント登録を行い，ログインを行う際にはアカウント登録時に AS のデータベース（DB）に登録したパスワードを用いて NTMobile ユーザの認証を行っていた．そのため，アプリ開発者やサービス事業者はユーザのパスワードなどを自身が運用する AS で安全に保管する必要があり，セキュリティ対策が不十分である場合，ユーザの認証情報が漏えいする危険性がある．一方，近年

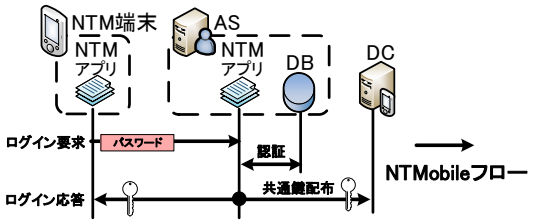

図 1　パスワードを用いた従来型認証方式

OpenID に対応したサービスも増加しており，NTMobile の実用化を見据えると，ユーザの認証情報は可能な限り NTMobile の枠組みから切り離すことが望ましい．

そこで筆者らは，ID 連携の仕組みである OpenID Connect を利用することで，NTMobile で管理するユーザの認証情報を分離する方式を提案している [2]．これにより，ユーザは NTMobile のアカウントを作成する手間が軽減されるほか，運用側はパスワードなどの認証に関わるユーザ情報を管理する必要がない．

3 OpenID Connect を用いた認証方式

OpenID Connect を用いた NTMobile 認証方式を図 2 に示す．本認証方式では，従来のような永続的なパスワードではなく，OpenID Connect による一過性のあるユーザの認可情報を基に NTMobile ユーザの認証を行う．以降は，図 2 に従い認証の手順を述べる．

- 認証開始
  NTM 端末は認証を開始すると外部ブラウザを起動し，AS の Web ページにアクセスする．ユーザが Web ページ上にある OP（OpenID Provider）のログインボタンを押すと，OP へリダイレクトが実行され OpenID Connect による認可フローを開始する．
- 認可処理
  OP と NTM 端末間でユーザ認証を行い，ユーザは AS に対して OP が持つ自身のユーザ情報へのアクセスを認可する．
- 認可コード発行
  ユーザ情報へのアクセスが認可されると，OP は応答として AS の Web ページにリダイレクトを実行し，認可コードを AS に送信する．
- ID トークン取得
  AS は取得した認可コードを OP に送信し，ユーザに認可された情報を示す ID トークンを取得する．
- ID トークン登録・送信
  AS は取得した ID トークンをユーザ認証用，ID トークン内に含まれるクレーム情報をユーザ識別用として DB に登録する．この時，AS は各ユーザ毎に FQDN やアドレス情報を管理する DC（Direction Coordinator）のアドレス情報など，NTM 端末の初期情報も設定して同時に DB に登録する．その後，AS は取得した ID トークンを NTM 端末に送信する．

Implementation of User Authentication Function for VpnService-based NTMobile System

Takayuki Yamada[†1], Taisuke Ueno[†2], Hidekazu Suzuki[†1], Katsuhiro Naito[†3] and Akira Watanabe[†1]
[†1] Graduate School of Meijo University
[†2] Meijo University
[†3] Aichi Institute of Technology

- ログイン要求
  NTM 端末は AS から受信した ID トークンをそのままログイン要求として送信し，AS は受け取った ID トークンと DB に登録した ID トークンを比較する．ID トークンが一致すればログインを完了したとみなし，以後の NTM 端末と DC 間の通信の暗号化に用いる共通鍵を生成する．
- 共通鍵配布・ログイン応答
  AS は DC に生成した共通鍵を配布し，NTM 端末にはログイン応答として共通鍵と NTM 端末の初期情報を送信する．その後，認証に使用した ID トークンを AS の DB および NTM 端末から削除する．なお，一度ログインして共通鍵が配布されると，共通鍵の有効期間内には AS へのログインは不要である．そのため，ユーザが OpenID Connect による認可処理を頻繁に行うことはない．
- 2 回目以降のログイン
  共通鍵の有効期限が切れた後，再度ログインを行う場合は，OpenID Connect による認証処理を行い，新たに ID トークンを取得する．ID トークンの情報を DB に登録する際には，ID トークン内のクレーム情報を確認し，同一ユーザのエントリを更新する．

以上のようにして，OpenID Connect を用いた NTMobile のユーザ認証を実現し，NTMobile システムからユーザ認証情報を分離する．

4 動作検証・定性評価

Android 端末において root 権限を必要としない実装モデルである VpnService 利用型の NTMobile[3] に本認証方式の基礎的実装を行い，動作検証を行った．

VpnService 型では NTM 端末の機能を Android アプリ（以後，NTMobile トンネルサービス）として実装しており，NTMobile トンネルサービスと AS に本認証方式の実現に必要な機能を実装した．動作検証を行うにあたり，NTMobile トンネルサービスには Android の Intent クラスを利用し，外部のブラウザアプリと連携するように Web ブラウジング機能を実装した．また，AS に対して ID トークンを送信する単純なクライアントプログラムを実装した．AS には，JavaScript と PHP を用いた Web アプリケーションを実装し，Google アカウントによる OpenID Connect の認証機能および AS の DB にアクセス機能を追加した．また，NTMobile トンネルサービスから ID トークンを受け取り，DB を参照して認証結果を返す単純なサーバプログラムを実装した．

動作検証の結果，NTMobile トンネルサービスから AS にアクセスし，OpenID Connect による認証を行った後，AS 側で取得した ID トークンを用いてユーザを認証するといった基本的な認証動作を確認することができた．

表 1 にユーザ側と運用側から見た各認証方式の比較表を示す．本認証方式の導入に際し，運用側は OP に対して OpenID の利用登録を行うなど，外部システムとの連携が必要となる．しかし，OP によってサンプルコードやガイドラインが整備されていることが多く，難易度はそれほど高くない．また，ユーザからすれば，新たにアカウントを作成する必要がないため，導入の敷居は低い．

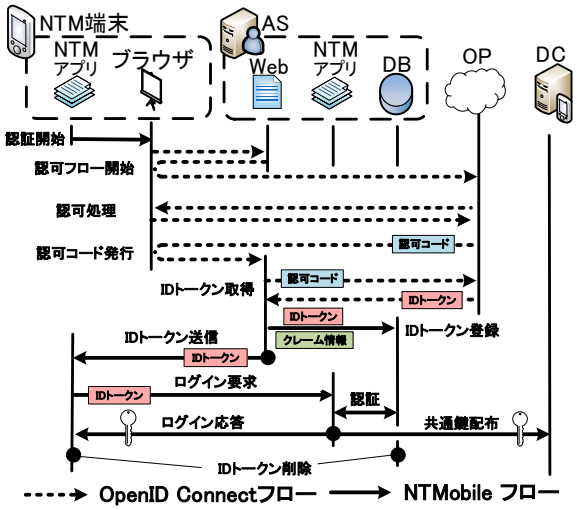

図 2　OpenID Connect を用いた NTMobile 認証方式

表 1　各認証方式の比較

	Password 認証		OpenID 認証	
	ユーザ側	運用側	ユーザ側	運用側
導入の容易さ	×	○	○	△
認証情報の管理	×	×	○	○
認証処理時間	○		△	

認証情報の管理について，本認証方式では，認証に使用した ID トークンは認証終了後に削除するため，運用側はパスワードなどの認証に関わるユーザ情報を保管する必要がない．また，OpenID を用いるため，従来のようにユーザが NTMobile アカウント用のパスワードを記憶する必要はない．一方で，本認証方式では従来のログイン要求を送信する前に OpenID Connect による認可処理を行うため，認証にかかる時間は従来より増加する．しかし，AS へのログイン処理は共通鍵が無い，または有効期限が切れた場合にしか発生しないため，ユーザへの影響は小さいと考えられる．

以上のことから，本認証方式の実現性と NTMobile を利用するユーザ側，運用側の両方で有用性を確認できた．

5 まとめ

本稿では，OpenID Connect を用いた NTMobile の認証方式について，VpnService 型 NTMobile への基礎的実装と動作検証を行った．また，従来の認証方式と比較し，ユーザ側，運用側ともに有用であることを確認した．

謝辞

本研究は JSPS 科研費 15K00140 および日本私立学校振興・共済事業団平成 27 年度学術研究振興資金（若手研究者奨励金）の助成を受けたものである．

参考文献

[1] 上醉尾一真ほか:情報処理学会論文誌, Vol. 54, No.10, pp. 2288-2299 (2013).
[2] 上野泰輔ほか : 第 13 回 情報学ワークショップ WiNF 2015 論文集，pp.153–158（2015）.
[3] 山田貴之ほか : DICOMO2015 シンポジウム論文集，Vol.2015，pp.1874–1791（2015）.