シームレスハンドオーバにおける安全性を考慮した効率的な認証方式の提案

松中隆志[†1] 泉川晴紀[†1] 杉山敬三[†1]

本稿では，シームレスハンドオーバに係る処理時間を短縮するための安全かつ処理が軽量な認証方式を提案する．提案方式では，事前にハンドオーバ元での安全性が保証された通信路を介して，ハンドオーバ先のネットワークと移動端末との間で認証情報を共有することにより，認証処理の簡略化を行う．その際，配布される認証情報の安全性を確保するために，ネットワークブロードキャスト用の認証方式である Timed Efficient Stream Loss-tolerant Authentication（TESLA）の概念を応用し，ネットワークと移動端末で同一の hash-chain を用いて，ユーザとハンドオーバ先ネットワークとの間で認証情報を共有するとともに，ハンドオーバを行うユーザの有効期限にかかわらず認証情報の有効期限を一定に保つ．これにより，通信システムのセキュリティレベルを落とすことなく，認証処理時間の短縮を実現する．さらに，本提案方式の適用例として，無線 LAN における認証フレームワークとして利用されている Extensible Authentication Protocol（EAP）への適用方法を示し，本提案手法の定性的評価および定量的評価を行い，本提案方式の有効性を示すことができた．特に，標準的な EAP 認証プロトコルである EAP-Transport Layer Security（EAP-TLS）と比較して，同等の安全性を満たしながら，約 1/4 に認証処理時間が短縮された．

An Effective Authentication Procedure Considering Security Risks for Seamless Handover

Takashi Matsunaka,[†1] Haruki Izumikawa[†1] and Keizo Sugiyama[†1]

This paper describes an approach of an effective authentication procedure to reduce a handover delay between heterogeneous networks. The two main ideas of this approach are that authentication information is shared between user terminals and the targeted network using two hash-chains and the constant expity time of authentication information regardless of the information possesor's expity time. This approach applies the concept of Timed Efficient Stream Loss-tolerant Authentication (TESLA) which is used in broadcast packets. This approach realizes the efficiency of the authentication procedure during handover without reducing the security level of the system. In addition, this paper proposes "pre-auth" type in the Extensible Authentication Protocol (EAP) authentication process to utilize the authentication information. Finally, this paper describes about the quantative and quantitative analysis of this approach. Especially, compared to EAP-Transport Layer Security (EAP-TLS), this paper confirm that this approach keeps the same security level and reduces an authentication delay to one-forth of EAP-TLS.

1. はじめに

昨今，固定網，移動網を問わず，すべてのアクセス網を IP ネットワークに統合する Next Generation Network（NGN）が注目されている．NGN は，Quality of Service（QoS）制御可能なパケットベースのネットワークであり[1)]，固定通信システム・モバイル通信システムが統合されたサービスを提供可能なネットワークとして，各国で構築が進められている．NGN の環境下では，ユーザの状況に応じて，利用する通信システムを選択し，最適なサービスを提供する必要がある．シームレスハンドオーバはそのようなサービス概念の実現のために重要な技術である．

シームレスハンドオーバ実現のための課題として，ハンドオーバ遅延の削減があり，そのためには移動先のネットワークにハンドオーバした際の認証処理を簡略化し，認証処理に係る時間を短縮することが必要である．これまでに，ハンドオーバ時の認証処理を簡略化するための方法として，事前認証が提案されている．

†1 株式会社 KDDI 研究所
KDDI R&D Laboratories, Inc.

事前認証では，ユーザはハンドオーバ前に，現在アクセスしているネットワーク経由で，移動先のネットワークと認証を行うことで，移動後の認証処理を省略する．その一例として，Mishra ら[2] は，無線 LAN 環境下における Access Point（AP）間ハンドオーバ時の効率的な認証方式として，移動端末のハンドオーバ時に，隣接するすべての AP に事前に Pairwise Master Key（PMK）から派生した認証情報を配布することで，移動後の認証処理を簡略化する手法を考案した．しかしながら，Mishra らのように事前に移動先 AP に鍵材料などの認証情報を配布する手法には，認証情報自身に有効期限を設定する以外に配布した認証情報を失効する方法がなく，当該認証情報が，該当する移動端末のハンドオーバ終了後も，有効期限の終了まで AP 上に残る．よって，たとえば攻撃者が認証情報配布後の AP を盗難するなどして認証情報を取得し，当該認証情報を用いて別の AP に対して認証を試みることにより，攻撃者によるネットワークへの不正アクセスが可能となる．上記課題の解決策として，PMK 生成時に利用した公開鍵証明書の失効情報を Certificate Revocation Lists（CRL）で管理し，当該証明書が失効された場合に認証情報を削除する方法が考えられるが，上記手法では失効情報の管理が煩雑になる．

NGN では，様々なモバイル通信システムが混在するため，ハンドオーバ処理に係る時間が様々である．また，ユーザの用途に応じて，あるユーザはハンドオーバ処理の速さを最優先にする，別のユーザはセキュリティを最優先にするなど，各ユーザのセキュリティポリシも様々である．このような多種多様な環境，ユーザニーズに対応するためには，認証情報ごとに有効期限を設定する必要がある．しかし，個別に認証情報の有効期限を設定すると，ある認証情報が長い期間の有効期限を持つ場合に，その認証情報に，システム全体の安全性が影響されてしまう．そのため，本提案手法では，認証情報に一定の有効期限を与え，移動端末に対しては，その端末のユーザの環境に応じて，適当な個数の認証情報を与えることとした．これにより，ユーザごとに有効期限を柔軟に設定することができ，なおかつシステムの安全性が，各ユーザの有効期限の影響を受けない．

本稿では，上述した概念を実現するために，ブロードキャスト，マルチキャストパケット用の認証技術である Timed Efficient Stream Loss-tolerant Authentication（TESLA）[3] の基本概念を，ハンドオーバ時の認証に適用する．TESLA は Perrig らにより考案された認証技術で，一方向関数（ハッシュ関数）を用いて hash-chain と呼ばれる認証用鍵群を生成し，さらに時間をある単位ごとに区切り，その単位時間ごとに認証用鍵を割り当てる．ブロードキャストパケットの送信者は，送信時に現在の時刻に割り当てられた認証用鍵を用いて当該パケットに認証子（MAC: Message Authentication Code）を付加する．**図 1** に TESLA の動作概要を示す．図 1 では，送信者は時刻 T_{j-2} でブロードキャスト用メッセージ M_1 を生成し，時刻 T_{j-2} で有効である鍵 K_{j-2} を用いて MAC を生成する．そして，メッセージ M_1 と MAC を合わせて受信者に送信する．受信者は，メッセージ M_1 と MAC を受信すると，当該 MAC を生成するための鍵 K_{j-2} が公開されるまで当該メッセージおよび MAC を保持する．送信者は，時刻 T_j になると，鍵 K_{j-2} を受信者にブロードキャストする．受信者は，鍵 K_{j-2} を受信すると，保持しておいたメッセージ M_1 から MAC を生成し，これと送信者より送られてきた MAC と一致するか調べる．以上により，受信者は，ブロードキャストメッセージ送信者を認証することができる．この基本概念の導入により，各ユーザの有効期限によらず認証情報の有効期限を一定にすることができ，結果としてシステムの安全性が，各ユーザに与える有効期限の影響を受けないようにすることができる．さらに，ハンドオーバ前の安全性が保証された通信路を用いて，事前に認証情報を認証サーバ，移動端末双方で共有し，当該情報をもとに hash-chain を生成することで，認証処理の簡略化を実現できる．また，提案手法では，ネットワークの各ユーザに与える認証情報の数を制限することにより，ユーザのアクセス権限に制限を与えられるため，セキュリティの低下を招くことなく，認証処理の簡略化を実現できる．

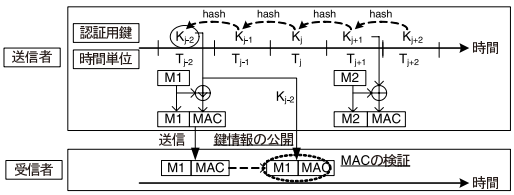

図 1 TESLA 概念図
Fig. 1 Outline of the Timed Efficient Stream Loss-tolerant Authentication (TESLA) protocol.

今回提案した手法に関して，定性的，定量的評価を行った結果，認証処理の簡略化における本提案手法の有効性を示すことができた．特に，本提案手法を Extensible Autheitcation Protocol（EAP）に適用して，提案手法の安全性，認証処理時間の評価を行った結果，標準的な EAP 認証プロトコルである EAP-Transport

Layer Security（EAP-TLS）と比較して，同等の安全性を満たしつつ，認証処理時間を約 1/4 短縮できた．

以下，本稿の構成について述べる．2 章ではハンドオーバ時の認証に関する従来技術を概説する．3 章では本稿で想定するネットワーク構成について，4 章では著者らが考案した認証手法の詳細について，5 章では提案手法の適用方法の一例として，EAP への適用方法について，6 章では提案手法の評価について述べる．最後に，7 章で本稿をまとめる．

2. 従 来 技 術

本章では，ハンドオーバ時の認証処理の簡略化技術に関する従来技術について概説する．IEEE802.11i[4] は，現在世間に広く普及している無線 LAN 規格である IEEE802.11[5] のセキュリティを強化するために制定された標準規格である．IEEE802.11i では，ハンドオーバ時の認証の簡略化に関する機能として pre-authentication が定められている．この機能は，移動端末（STA：STAtion）がアクセスポイント（AP：Access Point）間の移動を行う際に，事前に現在利用している AP を介して，移動先の AP へのアクセス認証を行い，当該 AP との間で Pairwire Master Key Security Association（PMKSA）と呼ばれるセキュリティアソシエーションを確立する．これにより，移動後の認証処理を軽減させる．

IETF の Handover Keying（hokey）ワーキンググループでは，無線 LAN の認証プロトコルフレームワークとして利用されている EAP に関する，ハンドオーバ時の処理を簡略化するためのプロトコル EAP-Efficient Re-authentication（EAP-ER）[6] について検討を行っている．認証サーバおよび移動端末は，通常の EAP 認証後に生成される認証情報 Extended Master Session Key（EMSK）をもとに再認証用の認証情報（rMSK：Re-authentication MSK）を生成する．移動端末がハンドオーバを行う際に，認証サーバは移動先の AP へ rMSK を配布することで，移動端末と AP の間で認証情報が共有され，結果，移動先での認証処理が簡略化される．

Huang ら[7] は，loosely-coupled な異システム間ハンドオーバにおける認証プロトコル Seamless Authentication Protocol（SAP）を提案した．Huang らの提案では，“SAP master key” を事前に各ネットワーク内の認証サーバに配布し，さらに各認証サーバは，SAP master key をさらにネットワーク内の AP および Base Station（BS）に配布する．また，移動端末–AP および BS 間で SAP master key をもとに生成した認証情報を共有する．これにより，ハンドオーバ時にその認証情報の所有を移動端末–AP 間で確認するだけでよく，結果として認証処理が簡略化される．

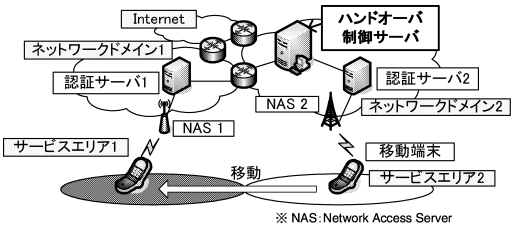

図 2 ネットワーク構成図
Fig. 2 Network assumption.

上述した技術は，前章で述べた Mishra らの手法と同様に，移動先 AP に配布した認証情報の安全性に関する問題が残る．すなわち，認証情報ごとに別の有効期限を設定するような場合，有効期限が長い認証情報にシステムの安全性が影響される．さらに，Huang らの方法においては，ある AP に保持されている認証情報が攻撃者に露呈した場合，すべてのネットワーク間で同じ認証情報を利用しているため，システム全体の安全性に影響を及ぼすという問題がある．

3. 想定ネットワーク構成

本稿では，2 つの異なるモバイル通信システム間のハンドオーバを想定する．本提案方式において，2 つのネットワークは，疎密いずれの結合体系でも問題ないが，本稿では，それぞれのネットワークには認証サーバが設置されているものとし，2 点間は互いに通信可能であるとする．さらに，一方のネットワーク内にハンドオーバ制御サーバを設置する．当該サーバは，移動端末のハンドオーバ動作を支援する役割を担う．移動端末は，各ネットワークが提供するモバイル通信システムを利用して，各ネットワーク内にある Network Access Server（NAS）を介して各ネットワークおよび Internet に接続する．初期接続時には，移動端末は接続対象とするネットワークが指定する認証方式を用いて接続を試みる．接続後，接続ネットワークを介した移動端末–ハンドオーバ制御サーバ間の通信は秘匿性，および完全性が保証されているとする．**図 2** に本稿で想定するネットワークの構成図を示す．図中，ハンドオーバ制御サーバはネットワーク 2 に設置されている．

4. 提 案 手 法

1 章で述べたとおり，本提案手法では，認証処理の簡略化とシステムの安全性確保を同時に満たす．具体

的には，認証情報を事前にハンドオーバ先ネットワークに配布することで認証処理の簡略化を実現し，さらに配布する認証情報の有効期限を一定にすることにより，システムの安全性確保，すなわち 1 章で述べたように，各認証情報の有効期限がシステムの安全性に影響を与えることを防ぐ．

上述した条件を満たす認証方式を実現するために，TESLA の基本概念を二者間の相互認証に適用した．まず第 1 に，ネットワーク上のサーバだけではなく，移動端末でも認証情報の生成を行うことにより，サーバ–移動端末間で認証情報を共有することとした．次に，上記移動端末の認証情報生成に関して制限を設けることにより，認証情報の漏えいによるセキュリティリスクの軽減を図った．具体的には，ユーザの位置情報，速度情報などから移動端末がハンドオーバを行う時間を推測し，その時間を当該移動端末の有効期限として，その値をもとに認証情報の生成可能個数に制限をかけることとした．

提案手法は，(1) 初期フェーズ，(2) 準備フェーズ，(3) ハンドオーバフェーズの 3 つのフェーズから構成される．(1) 初期フェーズは，システムを起動させる際に実行される．ハンドオーバ制御サーバは hash-chain を生成し，各々の認証情報を対応する単位時間に割り当てる．そして，各ネットワークの認証サーバに，一定時間ごとに，すなわち認証情報の有効期限が切れるごとに，現在の時間に対応する認証情報を送信する．(2) 準備フェーズは，移動端末がハンドオーバを行う直前に実行される．移動端末は，ハンドオーバを行うと決定した際，ハンドオーバ制御サーバに対して，ハンドオーバ要求メッセージを送信する．その際，当該メッセージに，自身の位置情報，速度情報などを付加する．ハンドオーバ制御サーバは，当該メッセージ内のこれら属性情報をもとに，当該移動端末のハンドオーバ実行時間を予測し，それをもとに当該移動端末の有効期限を設定する．そして，設定した有効期限分だけ認証情報を生成するためのシードを選定し，ハンドオーバ返信メッセージ内に当該シードを付加して，当該メッセージを送信する．(3) ハンドオーバフェーズは，実際に移動端末が移動し，ハンドオーバ先のネットワークへアクセスした際に実行される．移動端末は，ハンドオーバ先ネットワークのエリアに到達した際に，当該ネットワークと認証を行う．移動端末は，認証を行う際に，現在の時刻に対応した認証情報を選択し，認証を開始する．ネットワーク内の認証サーバ側でも，移動端末からの認証要求を受けた際に，現在の時刻に対応した認証情報を選択し，ユーザ端末の認証を行う．あらかじめ二者間で共有した認証情報を用いることにより，認証処理を簡略化することができる．以下，各フェーズの詳細について述べる．その際に用いる記法を次のとおりとする．

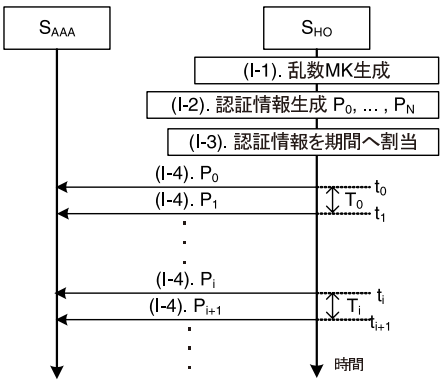

図 3 初期フェーズ
Fig. 3 Message sequence of the Initial phase.

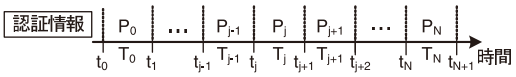

図 4 認証情報の各期間への割当て
Fig. 4 Assignment the authentication materials to each time interval.

- P_i：認証情報（$i = 0, 1, \ldots, N$）．
- T_i：P_i の有効期限（$i = 0, 1, \ldots, N$）．ここで T_i は時間 t_i から時間 t_{i+1} までの区間．
- h：一方向関数．
- MT：移動端末．
- $\mathrm{S_{HO}}$：ハンドオーバ制御サーバ．
- $\mathrm{S_{AAA}}$：移動先ネットワークの認証サーバ．
- $A \to B$：A から B へのメッセージ送信．

4.1 初期フェーズ

初期フェーズのメッセージシーケンスを**図 3** に示す．

(I-1) $\mathrm{S_{HO}}$ は乱数 MK を生成する．

(I-2) $\mathrm{S_{HO}}$ は次式により，認証情報を生成し，格納する．$P_i = h(P_{i+1})$，$P_N = MK$（$i = 0, 1, \ldots, N-1$）

(I-3) $\mathrm{S_{HO}}$ は，時間を各期間 T_i（$i = 0, 1, \ldots, N$）に分割し，各認証情報を対応する期間に割り当てる．**図 4** では，各認証情報 $P_0, \ldots, P_N$ が各期間 $T_0, \ldots, T_N$ に割り当てられている．

(I-4) ($\mathrm{S_{HO}} \to \mathrm{S_{AAA}}$) $\mathrm{S_{HO}}$ は時間が t_i になると，認証情報 P_i を $\mathrm{S_{AAA}}$ に対して送信する．

4.2 準備フェーズ

以下，移動元のネットワークと移動端末との間の通信はセキュアであるとする．すなわち，攻撃者は当該

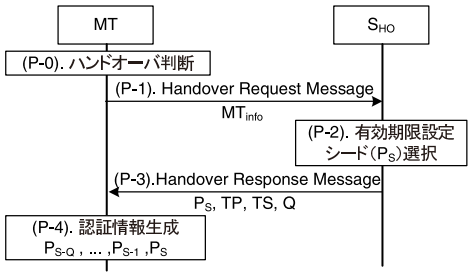

図 5 準備フェーズ
Fig. 5 Message sequence of the Preliminary phase.

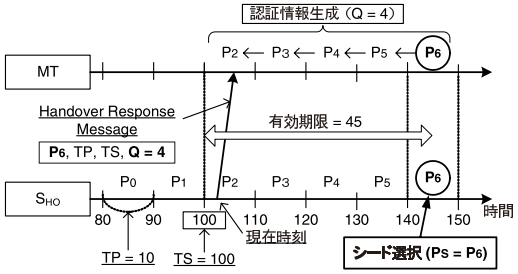

図 6 シード選定と認証情報の生成例
Fig. 6 An example of the selection of the seed and creation of the authentication materials.

通信メッセージを傍受不可能とする．**図 5** に，準備フェーズのメッセージシーケンスを示す．

(P-1) (MT → S_{HO}) MT はハンドオーバ要求メッセージを S_{HO} に対して送信する．その際，MT の属性情報（MT_{info}），たとえば現在位置，速度情報などを，当該メッセージに付加する．

(P-2) S_{HO} は MT_{info} をもとに，MT の有効期限を設定する．

(P-3) (S_{HO} → MT) S_{HO} はハンドオーバ返信メッセージを MT に対して送信する．その際，シード（P_S），認証情報の有効期限（TP），MT の有効期限の開始時刻（TS），MT が生成する認証情報の個数（Q）を当該メッセージに付加する．

(P-4) MT は，シード P_S から Q 個の認証情報を生成する．これにより，MT 内の認証情報は以下となる．$P_S, P_{S-1}, \ldots, P_{S-Q}$．

図 6 は，S_{HO} によるシードの選択と MT による認証情報生成の例である．ここで $TP = 10$，$TS = 100$，$P_S = P_6$，$Q = 4$，MT の有効期限を 45 とする．

4.3 ハンドオーバフェーズ

(H-1) MT は，ハンドオーバを行う際に現在の時刻を調べ，その時刻に対応する認証情報を選択する．

(H-2) (MT ↔ S_{AAA}) MT と S_{AAA} は相互認証を行う．その際，認証情報を利用することにより，認証処理は簡略化される．簡略化の実際の効果に関しては，6 章で評価結果について記載する．

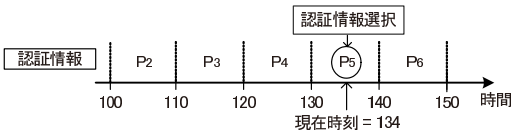

図 7 ハンドオーバフェーズ
Fig. 7 Overview of the Handover phase.

図 7 はハンドオーバフェーズでの MT の動作例を示す．図 7 では，現在の時刻が 134 であるため，MT は P_5 を選択し，認証サーバと認証処理を行う．

5. 提案手法の EAP への適用

Extensible Authentication Protocol（EAP）[8] は，Point-to-Point Protocol（PPP）[9] を拡張したプロトコルであり，認証のための枠組みを提供するプロトコルである．EAP は，ネットワーク接続におけるアクセス認証を行う仕組みを定めた規格である IEEE 802.1X [10] で，認証プロトコル用のフレームワークとして採用され，無線 LAN，セルラなど無線通信や，PPP，Ethernet のスイッチポートにおける認証方式として用いられている．

本章では，提案手法のハンドオーバフェーズ（4.3 節）を EAP に適用した，新しい EAP 認証方式 “pre-auth” を提案する．これにより，EAP 認証における認証処理の簡略化を実現する．本方式は，無線 LAN AP など NAS への改修が不要であり，なおかつ提案手法対応の移動端末と非対応の移動端末が同一環境内に共存できる（backward compatibility）ように設計されている．“pre-auth” の動作手順を以下に示す．

(PA-1) (MT → S_{AAA}) MT は，EAP リクエストメッセージに対して，自身の ID を含めた EAP レスポンスメッセージを送信する．

(PA-2) (S_{AAA} → MT) S_{AAA} は，Remote Authentication Dial In User Service（RADIUS）プロトコルメッセージを用いて，先ほどの EAP リクエストメッセージを送信する．その際，当該メッセージに乱数 *Nonce* を付加し，同時に EAP type が pre-auth であることを示す．

(PA-3) MT は，認証子 $H_{MT} = h(Nonce||P_{MT})$ を算出する．ここで，P_{MT} は現在の時刻に対応する認証情報とする．

(PA-4) (MT → S_{AAA}) MT は，H_{MT} と乱数 $Nonce'$ を付加した EAP レスポンスメッセージを送信する．

(PA-5) S_{AAA} は，認証子 $H_S = h(Nonce||P_{AAA})$

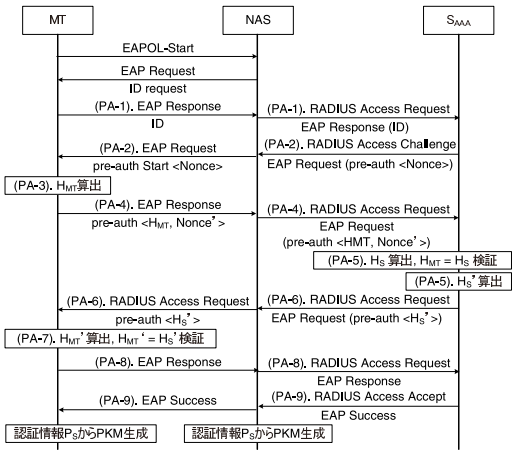

図 8 pre-auth メッセージシーケンス
Fig. 8 Message sequence of "pre-auth" authentication.

を算出し，MT より送付された認証子 H_{MT} が，式 $H_{\mathrm{MT}} = H_{\mathrm{S}}$ を満たすかどうか検証する．ここで P_{AAA} は現在の時刻に対応する認証情報とする．検証が成功した場合，$\mathrm{S_{AAA}}$ は認証子 $H_{\mathrm{S}}' = h(Nonce'||P_{\mathrm{AAA}})$ を算出する．

(PA-6) ($\mathrm{S_{AAA}} \rightarrow$ MT) $\mathrm{S_{AAA}}$ は，H_{S}' を付加した EAP リクエストメッセージを送信する．

(PA-7) MT は，認証子 $H_{\mathrm{MT}}' = h(Nonce'||P_{\mathrm{MT}})$ を算出し，$\mathrm{S_{AAA}}$ より送付された認証子 H_{S}' が，式 $H_{\mathrm{S}}' = H_{\mathrm{MT}}'$ を満たすかどうか検証する．

(PA-8) (MT $\rightarrow \mathrm{S_{AAA}}$) 検証 $H_{\mathrm{S}}' = H_{\mathrm{MT}}'$ が成功した場合，MT は EAP レスポンスメッセージを送信する．

(PA-9) ($\mathrm{S_{AAA}} \rightarrow$ MT) $\mathrm{S_{AAA}}$ は EAP 成功メッセージ（EAP Success）を送信する．

図 8 に，pre-auth 方式のメッセージシーケンス図を示す．図 8 より，NAS は EAP メッセージおよび RADIUS メッセージを，それぞれ認証サーバ，移動端末に転送しているだけであり，EAP pre-auth を導入するにあたり，特に NAS に改修を加える必要はない．また，本提案手法に非対応な移動端末の場合は，図 8 の手順 (2) において，認証サーバは EAP type として当該端末がサポートしている認証方式を指定し，以後，指定された認証方式を利用して認証処理を行えばよく，非対応の移動端末も同じ環境下に共存できる．

6. 提案手法の評価

6.1 定性的評価

本節では，提案手法の定性的評価として，5 章で述べた EAP pre-auth に対して，(1) 安全性，(2) 認証処理コスト，(3) 時間同期，(4) 複数端末環境への拡張の 4 点に関して考察を行う．(1)，(2) では提案の目的である，安全性の維持および認証処理の簡略化に関して評価するとともに，既存の EAP 認証方式である EAP-Transport Layer Security (EAP-TLS)[11] および Microsoft EAP CHAP Extensions Protocol Version 2 (EAP-MS-CHAPv2)[12] との比較評価を行う．EAP-TLS は，Windows XP に標準でサポートされており，電子証明書を用いて，認証クライアント–サーバ間で相互認証を行う認証プロトコルである．EAP-MS-CHAPv2 は，二者間であらかじめ共有された情報をもとに相互認証を行う認証プロトコルである．**図 9** に EAP-TLS，**図 10** に EAP-MS-CHAPv2 のメッセージシーケンスをそれぞれ記載する．(3)，(4) では本提案手法の実現性の評価として，時間同期および複数端末環境への本提案の拡張に関して評価する．

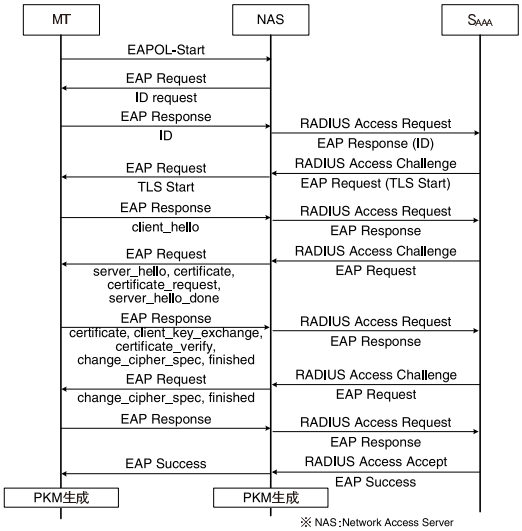

図 9 EAP-TLS メッセージシーケンス
Fig. 9 Message sequence of EAP-TLS.

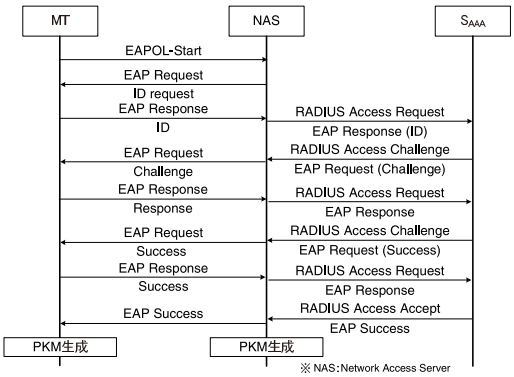

図 10 EAP-MS-CHAPv2 メッセージシーケンス
Fig. 10 Message sequence of EAP-MS-CHAPv2.

表 1 各 EAP 認証方式のコスト比較（H：ハッシュ関数処理，P：公開鍵暗号処理，S：秘密鍵暗号処理）
Table 1 Comparison of each cost of authentication process.

	EAP-TLS	EAP-MS-CHAPv2	EAP pre-auth
総メッセージサイズ (バイト)	5021	121	96
総メッセージ数	9	7	7
MT の計算量	8H 2P 2S	2H 1S	2H

(1) 安全性

提案方式では，認証情報の有効期限を設定することで，認証情報漏えい時のセキュリティリスクを，漏えいした認証情報によらず一定に保つことができる．この有効期限は，システムの要求するセキュリティレベル，認証情報の生成コスト，および時間同期ずれの場合の再認証コストを考慮して設定すべきである．提案方式で利用している一方向関数の安全性は，たとえば SHA-1 [13] であれば，文献 14) より，鍵長 80 ビットの総当り攻撃に対する安全性と同等の安全性を持つ．よって，ハンドオーバ時に利用することを考えると，ハンドオーバに係る処理時間は数十秒程度であることから，暗号解読による認証情報漏えいの危険性よりも機器からの認証情報漏えいの危険性の方が高いと考えられる．したがって，上述したセキュリティレベルは後者の危険性を考慮して決定することとなると考えられる．

各認証情報は，秘匿性，完全性が保証された通信を介して配布されたシードをもとに，一方向関数を用いて生成されるため，一方向関数が一方向性（一方向関数 h において，任意の x に対して $h(x) = h(x')$ を満たす x' を見つけることが困難），衝突発見困難性（$h(x) = h(x')$ を満たす (x, x') の組を発見することが困難）を満たす場合，提案方式は Perfect Forward Secrecy（PFS）を満たす．すなわち，ある認証情報が攻撃者に漏えいしても，その認証情報が有効となる期間以降に有効となる認証情報は漏えいしない（P_i が漏えいしても，P_j（$i < j$）は漏えいしない）．なお，移動端末–ハンドオーバ制御サーバ間の通信の安全性に関しては，初期接続後に当該接続ネットワークを介して移動端末–ハンドオーバ制御サーバ間で鍵を共有し，以降の移動端末–ハンドオーバ制御サーバ間のメッセージは，当該鍵を利用して秘匿化するような方法が考えられる．鍵共有方法に関しては，事前に両者間で共通されたマスタ鍵をもとに鍵情報を交換する方式，公開鍵暗号を用いる方式，Diffie-Hellman 鍵共有方式[15] などがあげられる．

pre-auth の認証シーケンスの安全性に関しては，EAP-TLS に比べ，公開鍵暗号技術による認証メッセージの妥当性検証機能がないため，EAP-MS-CHAPv2 と同程度の安全性レベルとなっている．しかし，EAP-TLS は公開鍵暗号を用いて情報共有を行うため，man-in-the-middle 攻撃を防ぐために認証メッセージの完全性を保証する必要があるのに対し，pre-auth はすでに二者間で情報が共有されているため，認証メッセージ内に鍵材料を含める必要がなく，上記機能は必須ではない．また，NIST は文献 14) の中で，たとえば一方向関数 SHA-1 と鍵長 1,024 ビットの RSA 暗号[16] は同等の安全性を持つとしている．このことより，認証メッセージを解読されることで，二者間で共有する認証情報が漏えいする危険性に対しては，EAP-TLS で用いる公開鍵暗号の鍵長，および pre-auth で用いる一方向関数の出力ビット数を適切に設定することで，ほぼ同等の安全性となる．以上より，pre-auth の安全性は，EAP-TLS と同等の安全性を持つといえる．

(2) 認証処理のコスト

表 1 に，pre-auth と EAP-TLS および EAP-MS-CHAPv2 のコストを比較した結果を示す．ここで，総メッセージサイズは EAP ヘッダ長を除いた EAP メッセージ長の加算結果とした．また，ID 長は 10 バイトとして計算した．EAP-TLS は，暗号のセキュリティレベルを他の認証方式と合わせるため，Cipher Spec を `TLS_DHE_RSA_WITH_AES_256_CBC_SHA` として，コストを算出した．なお，公開鍵暗号の鍵長を 128 バイト，公開鍵証明書のサイズを 1,024 バイト，pre-auth で用いる一方向関数の出力値を 20 バイトとした．表 1 より，EAP-TLS は公開鍵暗号を用いて情報共有を行うため，電子署名により認証メッセージの完全性を保証する必要があり，処理負荷が高く，移動端末で多くの処理時間を要することが分かる．対して pre-auth は，事前に共有された認証情報を元に相互認証を行うため，認証方式のセキュリティレベルとしては，EAP-MS-CHAPv2 と同等のレベルを満たせばよく，そのため EAP-TLS などの公開鍵暗号を用いた認証方式よりも軽微な認証処理で，安全に認証を行うことができる．なお，表 1 の EAP pre-auth のコストには，4 章で説明したハンドオーバ要求メッセージ，ハンドオーバ返信メッセージのコストは含まれていない．移動端末の属性情報（MT_{info}）を 16 バイト，認証情報のサイズを 16 バイト，各時間データ（TS，TP）を

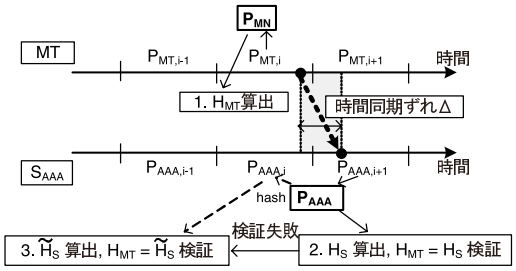

図 11 時間同期ずれ補正
Fig. 11 Correction of time lag.

4 バイトとすると，ヘッダ長を除くと，ハンドオーバ要求メッセージ，返信メッセージはそれぞれ 16 バイト，28 バイトと見積もることができる．さらに移動端末では，準備フェーズで Q 個の認証情報を一方向関数を用いて算出する必要がある．本稿では，移動端末の有効期限は認証情報の有効期限の 10 倍程度，すなわち $Q \leq 10$ と想定している．この想定においては，準備フェーズにおける認証情報の算出処理の計算負荷は問題とならない．

(3) 時間同期

提案手法は，二者間での時間同期を必要とする．Global Positioning System（GPS）機能を搭載した携帯端末では，GPS 機能により，定期的に時刻取得が可能であるため，端末内の時刻の正確さを保つことができる．また，Network Time Protocol（NTP）[17] を用いることでも，時刻の正確さを保つことができる．しかし提案方式では，TESLA と同様に，二者間で緩い時間同期（loosely synchronization）がとれている環境下でも動作可能である．以降，二者間の時間同期のずれを Δ とする．以下，時間同期のずれに対する対策方法を示す．この対策方法では，$\Delta \leq T_i$（T_i：認証情報の有効期限）を満たす範囲の時間同期のずれを許容する．具体的には，5 章の手順 (PA-5) および (PA-7) の後に，以下の手順を追加する．

(PA-5)'. $H_{\mathrm{MT}} = H_{\mathrm{S}}$ を満たさない場合，$\mathrm{S_{AAA}}$ は $\widetilde{H}_{\mathrm{S}} = h(Nonce||h(P_{\mathrm{AAA}}))$ を計算し，認証子 H_{MT} が $\widetilde{H}_{\mathrm{S}} = H_{\mathrm{MT}}$ を満たすかどうか検証する．

(PA-7)'. $H_{\mathrm{S}}{}' = H_{\mathrm{MT}}{}'$ を満たさない場合，MT は $\widetilde{H}'_{\mathrm{MT}} = h(Nonce'||h(P_{\mathrm{MT}}))$ を算出し，認証子 $H_{\mathrm{S}}{}'$ が $\widetilde{H}'_{\mathrm{MT}} = H_{\mathrm{S}}{}'$ を満たすかどうか検証する．

図 11 に対策法の概観を示す．本対策法は，たとえば，認証情報の有効期限に対して，二者間の時間同期のずれおよび通信の遅延がさほど大きくない場合，上記の手法でも問題なく動作するものと考えられる．ただ，上記の方法により，移動端末に対して，当該端末の有効期限に認証情報の有効期限を加えた時間までのアクセスを許すこととなる．

(4) 複数端末環境への拡張

提案手法の拡張に関して，まず複数端末が同時にハンドオーバを行う際に，各端末間で互いに認証情報が漏えいしないための，提案手法の拡張方法について述べ，その後，認証コストに関して見積もる．

(a) 提案手法の拡張

準備フェーズ（4.2 節）において，ハンドオーバ制御サーバは移動端末にシードを送信する際に，当該移動端末の ID（ID_{MT1}）と認証情報（P_S）とのハッシュ値（$P_{\mathrm{MT1},S} = h(ID_{\mathrm{MT1}}||P_S)$）を生成し，これをシードとして移動端末に送付する．また，ハンドオーバ制御サーバは，ハンドオーバ先ネットワークの認証サーバに対して，移動端末の ID，さらに現在時刻 t_{MT1} を送信する．認証サーバは，受け取った情報を移動端末の ID と関連付けて，自身のメモリ内に格納する．シードを受け取った移動端末は，受け取ったシードから認証情報群（$P_{\mathrm{MT1},S-Q}, \ldots, P_{\mathrm{MT1},S}$）を生成する．移動端末から EAP Request メッセージの ID リクエストがでると，認証サーバは，準備フェーズ時に作成した表を参照し，移動端末のエントリからシード（$P_{\mathrm{MT1},S}$）を参照し，現在時刻に有効となる認証情報を生成する．そして生成された認証情報を用いて認証処理を行う．これにより，各移動端末には，各 ID をもとに生成されたシードのみ生成されるため，ある移動端末の認証情報は他の移動端末に対して秘匿される．

(b) 認証コスト評価

移動端末の ID のサイズを 10 バイト，認証情報のサイズを 16 バイト，時刻情報のサイズを 4 バイトとすると，認証サーバでは移動端末 1 台あたり 30 バイトのメモリ領域が消費される．一方，移動端末と認証を行う際の計算量は，最大で一方向関数演算 $(2+Q)$ 回である．(2) と同様に $Q \leq 10$ と想定し，さらに 6.2 節の測定結果より，一方向関数 1 回にかかる演算時間を 1 ミリ秒とすると，移動端末と認証を行う際の，認証サーバの計算時間は，最大で 12 ミリ秒程度と見積もることができる．このように，複数端末を考慮した場合においても移動端末 1 台あたりの認証サーバ側の処理は軽いため，実環境下においても，問題なく動作すると推定される．

6.2 定量的評価

5 章で提案した pre-auth 方式を実装し，認証処理時間に関して評価を行った．評価にあたり，認証クライアント用 PC として，CPU が Pentium M 1.5 GHz，メモリが 768 M バイトのノート PC，認証サーバ用 PC として，CPU が Pentium III 750 MHz，メモリ

表 2 認証処理時間の比較
Table 2 Comparison of each of the authentication processing time.

	EAP-TLS	EAP-MS-CHAPv2	EAP pre-auth
全処理時間 [ms]	226.3	54.7	56.7
移動端末側演算処理時間 [ms]	44.7	1.8	0.3
認証サーバ側演算処理時間 [ms]	35.7	3.4	1.5
通信時間 [ms]	145.8	49.3	54.9

が 256 M バイトのデスクトップ PC を利用した．OS はそれぞれ Linux を利用した．また，pre-auth の実装に関して，認証クライアント用ソフトウェアである Xsupplicant [18]（ver. 1.2.8），認証サーバ用ソフトウェアである freeRADIUS [19]（ver. 1.1.3）に pre-auth の機能を追加して実現した．測定に用いたシステム構成は，認証サーバと無線 LAN AP を Ethernet を用いて接続し，認証クライアントと無線 LAN の間の無線規格として，IEEE802.11g [20] を用いた．

評価結果を**表 2** に示す．ここで演算処理時間とは，ハッシュ関数演算，秘密鍵暗号処理，公開鍵暗号処理，そして乱数処理といった暗号処理に係る処理を含む．表 2 より，EAP-TLS と比較して pre-auth の認証処理時間が約 1/4 になっており，明らかに認証処理時間が短縮されていることが確認できる．また，pre-auth では，暗号処理としてハッシュ関数演算しか用いておらず，測定結果においても，暗号処理の占める割合は全処理時間の約 3%程度である．これにより，たとえば携帯電話のような，PC に比べて計算能力が非力な端末においても問題なく動作する．EAP-MS-CHAPv2 と比較すると，pre-auth の処理時間は EAP-MS-CHAPv2 とほぼ同じ処理時間になっている．これより，pre-auth では，EAP-MS-CHAPv2 とほぼ同じ処理時間で，認証情報の安全性に関する付加価値を実現していることが確認できる．また，端末–サーバ間の通信時間においても，pre-auth の処理時間は，EAP-TLS の約 38%になっている．今回 pre-auth において，相互認証を保証するため，また，無線 LAN AP に対して pre-auth に関する機能を追加する必要がない形で実現するために，5 章で示したようなメッセージ数が 7（3 ラウンド）となるプロトコルを提案した．しかし，2 章で紹介した EAP-ER のように無線 LAN AP に対して改修を許すのであれば，メッセージ数を 3（1 ラウンド）まで削減できるため，さらなる認証処理の削減が見込まれる．

7. ま と め

本稿では，シームレスハンドオーバを実現するために，ハンドオーバに係る処理時間を短縮するための安全かつ処理が軽量な認証方式を考案した．提案方式では，事前にハンドオーバ元での安全性が保証された通信路を介して，ハンドオーバ先のネットワークと移動端末との間で認証情報を共有することにより，認証処理の簡略化を行っている．その際に配布される認証情報の安全性を確保するために，ネットワークブロードキャスト用の認証方式である TESLA の概念を応用し，ネットワークと移動端末で同一の hash-chain を用いて，ユーザとハンドオーバ先ネットワークとの間で認証情報を共有するとともに，ハンドオーバを行うユーザの有効期限にかかわらず認証情報の有効期限を一定に保つ．これにより，通信システムのセキュリティレベルを落とすことなく，認証処理時間を短縮することができる．

さらに，本提案方式の適用例として，無線 LAN における認証フレームワークとして利用されている EAP への適用案 EAP pre-auth を提案した．EAP pre-auth は無線 LAN AP など NAS への改修を行う必要がなく，なおかつ提案手法に非対応な移動端末も収容できるといった特徴を持つ．

最後に，EAP pre-auth に対して，計算コスト，安全性などの定性的評価，および認証処理時間の定量的評価を行い，本提案方式の有効性を確認した．特に EAP-TLS と比較し，同等の安全性を満たしながら認証処理時間を約 1/4 に削減できることを確認した．

謝辞 日頃よりご指導いただく KDDI 研究所秋葉所長，松本副所長，野本執行役員に感謝いたします．

参 考 文 献

1) ITU-T: General Overview of NGN, Y.2001 ITU-T Recommendation (2004).
2) Mishra, A., Shin, M.H., Petroni, N.L., Jr., Clancy, T.C. and Arbaugh, W.A.: Proactive Key Distribution Using Neighbor Graphs, *IEEE Wireless Communications*, pp.26–36 (2004).
3) Perrig, A., Song, D., Canetti, R., Tygar, J.D. and Briscoe, B.: Timed Efficient Stream Loss-Tolerant Authentication (TESLA): Multicast Source Authentication Transform Intro-

duction, RFC 4082 (2005).
4) IEEE Standard 802.11i–2004, Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Medium Access Control (MAC) Security Enhancements, IEEE (2004).
5) IEEE Std 802.11-1997: Part 11, Wireless LAN Medium Access Control (MAC) And Physical Layer (PHY) Specifications (1997).
6) Narayanan, V. and Dondeti, L.: EAP Extensions for Efficient Re-authentication, IETF Internet draft draft-vidya-eap-er-02 (2007).
7) Huang, S.C.-H., Zhu, H. and Zhang, W.: SAP: Seamless Authentication Protocol for Vertical Handoff in Heterogeneous Wireless Networks, *The 3rd International Conference on Quality of Service in Heterogeneous Wired/Wireless Networks* (*QShine 2006*) (2006).
8) Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J. and Levkowetz, H.E.: Extensible Authentication Protocol (EAP), RFC 3748 (2004).
9) Simpson, W.: The Point-to-Point Protocol (PPP), STD 5, RFC 1661 (1994).
10) IEEE Std 802.1X-2001, IEEE standard for local and metropolitan area networks – Port-based network access control (2001).
11) Aboba, B. and Simon, D.: PPP EAP TLS Authentication Protocol, RFC 2716 (1999).
12) Hurst, R. and Palekar, A.: Microsoft EAP CHAP Extensions, Internet draft: draft-kamath-pppext-eap-mschapv2-02.txt (2007).
13) Federal Information Processing Standard 180-2, Secure Hash Standard, Available at http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf (2002).
14) Barker, E., Barker, W., Burr, W., Polk, W. and Smid, M.: Recommendation on Key Management, NIST Special Publications 800 Series: SP 800-57 (2007).
15) Diffie, W. and Hellman, M.: New directions in cryptography, *IEEE Trans. Information Theory*, Vol.22, pp.644–654 (1976).
16) Rivest, R.L., Shamir, A. and Adleman, L.: A Method for Obtaining Digital Signatures and Public Key Cryptosystems, *Comm. ACM*, Vol.21, No.2, pp.294–299 (1978).
17) Mills, D.L.: Network Time Protocol (Version 3) Specification, Implementation and Analysis, RFC 1305 (1992).
18) the Open 1x Project: Open Source Implementation of IEEE 802.1X/WPA/WPA2/IEEE802.11i. Available at http://open1x.sourceforge.net/
19) The FreeRADIUS Server Project: freeRADIUS: The world's most popular RADIUS Server. Available at http://www.freeradius.org/
20) IEEE Std 802.11g-2003: Part II: Wireless LAN Medium Access Control (MAC) And Physical Layer (PHY) Specifications (2003).

(平成 19 年 4 月 2 日受付)
(平成 19 年 10 月 2 日採録)

松中 隆志（正会員）

平成 14 年電気通信大学電気通信学部情報工学科卒業．平成 16 年北陸先端技術大学院大学情報科学研究科博士前期課程修了．同年 KDDI（株）入社．現在，（株）KDDI 研究所無線ネットワークアーキテクチャーグループ研究員．主に無線通信におけるセキュリティの研究に従事．

泉川 晴紀

平成 13 年早稲田大学理工学部電子・情報通信学科卒業．平成 15 年同大学大学院修士課程修了．同年 KDDI（株）入社．現在，（株）KDDI 研究所無線ネットワークアーキテクチャーグループ研究員．主にシームレス通信，マルチホップネットワークの研究に従事．電子情報通信学会員．

杉山 敬三（正会員）

昭和 60 年京都大学工学部情報学科卒業．昭和 62 年同大学大学院修士課程修了．同年国際電信電話（株）入社．以来，同社研究所にて主に OSI 応用プロトコル，EDI，ネットワーク管理，ITS，無線 LAN の研究に従事．現在，（株）KDDI 研究所開発センター企画調査グループ・グループリーダー．情報学博士．平成 6 年電子情報通信学会学術奨励賞受賞．