【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成30年11月15日(2018.11.15)

【公表番号】特表2017-534214(P2017-534214A)
【公表日】平成29年11月16日(2017.11.16)
【年通号数】公開・登録公報2017-044
【出願番号】特願2017-524993(P2017-524993)
【国際特許分類】
Ｈ０４Ｌ　9/08　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６０１Ｂ
Ｈ０４Ｌ　9/00　６０１Ｅ

【手続補正書】
【提出日】平成30年10月4日(2018.10.4)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
ワイヤレス通信のための方法であって、
再認証鍵およびシーケンス番号からワイヤレス局において第１の識別子を導出することと、前記再認証鍵は、第１のセッション鍵から少なくとも部分的に導出される、
前記第１の識別子およびドメイン名を認証者に送信することと、前記第１の識別子および前記ドメイン名は、認証サーバとの前記ワイヤレス局の第１の再認証中に送信される、
前記第１の再認証中、前記第１のセッション鍵の名前の送信を差し控えることと、
前記認証サーバとの前記ワイヤレス局の単一の再認証のために前記第１の識別子を使用することと
を備える、ワイヤレス通信のための方法。
【請求項２】
前記シーケンス番号に少なくとも部分的に基づいて次のシーケンス番号を生成することと、
前記再認証鍵および前記次のシーケンス番号に少なくとも部分的に基づいて第２の識別子を導出することと
をさらに備え、
前記方法は、好ましくは、
前記第２の識別子および前記ドメイン名を送信すること、前記第２の識別子および前記ドメイン名は、前記認証サーバとの前記ワイヤレス局の第２の再認証中に送信される、または
再認証失敗メッセージを受信すること、および
前記再認証失敗メッセージを受信することに応答して、前記第２の識別子および前記ドメイン名を送信すること
をさらに備える、請求項１に記載の方法。
【請求項３】
識別子ラベルに少なくとも部分的に基づいて前記第１の識別子を導出すること、または
再認証失敗メッセージを受信すること、および
前記再認証失敗メッセージを受信することに応答して、前記認証サーバとの完全な認証

を遂行すること、ここにおいて、前記第１の再認証は、好ましくは、前記認証サーバとの完全な認証を遂行した後に遂行される、
をさらに備える、請求項１に記載の方法。
【請求項４】
ワイヤレス通信のための装置であって、
プロセッサと、
前記プロセッサと電子通信しているメモリと、
前記メモリに記憶されている命令と
を備え、前記命令は、
再認証鍵およびシーケンス番号からワイヤレス局において第１の識別子を導出することと、前記再認証鍵は、第１のセッション鍵から少なくとも部分的に導出される、
前記第１の識別子およびドメイン名を認証者に送信することと、前記第１の識別子および前記ドメイン名は、認証サーバとの前記ワイヤレス局の第１の再認証中に送信される、
前記第１の再認証中、前記第１のセッション鍵の名前の送信を差し控えることと、
前記認証サーバとの前記ワイヤレス局の単一の再認証のために前記第１の識別子を使用することと
を行うように前記プロセッサによって実行可能である、ワイヤレス通信のための装置。
【請求項５】
前記シーケンス番号に少なくとも部分的に基づいて次のシーケンス番号を生成することと、
前記再認証鍵および前記次のシーケンス番号に少なくとも部分的に基づいて第２の識別子を導出することと
を行うように前記プロセッサによって実行可能な命令をさらに備え、
前記装置は、好ましくは、
前記第２の識別子および前記ドメイン名を送信すること、前記第２の識別子および前記ドメイン名は、前記認証サーバとの前記ワイヤレス局の第２の再認証中に送信される、または
再認証失敗メッセージを受信すること、および
前記再認証失敗メッセージを受信することに応答して、前記第２の識別子および前記ドメイン名を送信すること
を行うように前記プロセッサによって実行可能な命令をさらに備える、請求項４に記載の装置。
【請求項６】
識別子ラベルに少なくとも部分的に基づいて前記第１の識別子を導出すること、または
再認証失敗メッセージを受信すること、および
前記再認証失敗メッセージを受信することに応答して、前記認証サーバとの完全な認証を遂行すること、ここにおいて、前記第１の再認証は、好ましくは、前記認証サーバとの完全な認証を遂行した後に遂行される
を行うように前記プロセッサによって実行可能な命令をさらに備える、請求項４に記載の装置。
【請求項７】
前記第１の再認証は、拡張認証プロトコル（ＥＡＰ）再認証を備え、前記第１のセッション鍵は、拡張マスターセッション鍵（ＥＭＳＫ）を備え、前記再認証鍵は、再認証ルート鍵（ｒＲＫ）を備える、請求項４に記載の装置、または請求項１に記載の方法。
【請求項８】
ワイヤレス通信のための方法であって、
再認証鍵およびシーケンス番号から、認証サーバにおいて、第１の識別子を導出することと、前記再認証鍵は、第１のセッション鍵から少なくとも部分的に導出される、
第２の識別子を前記認証サーバにおいて受信することと、前記第２の識別子は、前記認

証サーバとのワイヤレス局の第１の再認証中に受信される、
前記ワイヤレス局の単一の再認証のために前記第１の識別子および前記第２の識別子を使用することと、ここにおいて、前記第１および第２の識別子を使用することは、前記第１の識別子を前記第２の識別子と比較することを備える、
前記比較することに少なくとも部分的に基づいて前記ワイヤレス局の認証者に第２のセッション鍵を送信することと
を備える、ワイヤレス通信のための方法。
【請求項９】
前記シーケンス番号に少なくとも部分的に基づいて次のシーケンス番号を生成することと、
前記再認証鍵および前記次のシーケンス番号に少なくとも部分的に基づいて第３の識別子を導出することと
をさらに備え、
前記方法は、好ましくは、
前記認証サーバとの前記ワイヤレス局の第２の再認証中に第４の識別子を受信することと、
前記第３の識別子を前記第４の識別子と比較することと、
前記比較することに少なくとも部分的に基づいて前記第２のセッション鍵を送信することと
をさらに備える、請求項８に記載の方法。
【請求項１０】
識別子ラベルに少なくとも部分的に基づいて前記第１の識別子を導出すること
をさらに備える、請求項８に記載の方法。
【請求項１１】
前記第１の識別子が前記第２の識別子と一致できないとき、再認証失敗メッセージを送信すること
をさらに備え、
前記再認証失敗メッセージは、好ましくは、前記第１の識別子と前記第２の識別子との間の不一致を示すタイプレングスバリュー（ＴＬＶ）要素を備える、請求項８に記載の方法。
【請求項１２】
前記第１の再認証は、拡張認証プロトコル（ＥＡＰ）再認証を備え、前記第１のセッション鍵は、拡張マスターセッション鍵（ＥＭＳＫ）を備え、前記再認証鍵は、再認証ルート鍵（ｒＲＫ）を備え、前記第２のセッション鍵は、再認証マスターセッション鍵（ｒＭＳＫ）を備える、請求項８に記載の方法。
【請求項１３】
ワイヤレス通信のための装置であって、
プロセッサと、
前記プロセッサと電子通信しているメモリと、
前記メモリに記憶されている命令と
を備え、前記命令は、
再認証鍵およびシーケンス番号から、認証サーバにおいて、第１の識別子を導出することと、前記再認証鍵は、第１のセッション鍵から少なくとも部分的に導出される、
第２の識別子を前記認証サーバにおいて受信することと、前記第２の識別子は、前記認証サーバとのワイヤレス局の第１の再認証中に受信される、
前記ワイヤレス局の単一の再認証のために前記第１の識別子および前記第２の識別子を使用することと、ここにおいて、前記第１および第２の識別子を使用するための前記命令は、前記第１の識別子を前記第２の識別子と比較するための命令を備える、
前記比較することに少なくとも部分的に基づいて前記ワイヤレス局の認証者に第２のセッション鍵を送信することと

を行うように前記プロセッサによって実行可能である、ワイヤレス通信のための装置。
【請求項１４】
前記シーケンス番号に少なくとも部分的に基づいて次のシーケンス番号を生成することと、
前記再認証鍵および前記次のシーケンス番号に少なくとも部分的に基づいて第３の識別子を導出することと
を行うように前記プロセッサによって実行可能な命令をさらに備える、請求項１３に記載の装置。
【請求項１５】
実行されたとき、プロセッサに、請求項１乃至３、または請求項８乃至１２のいずれかに記載の方法を行わせる命令を備える、コンピュータプログラム。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】０１３２
【補正方法】変更
【補正の内容】
【０１３２】
[0147] 本開示の前の説明は、当業者が本開示を製造または使用することを可能にするために提供される。本開示への様々な修正は、当業者にとって容易に明らかであり、本明細書に定義された一般的な原理は、本開示の範囲から逸脱することなく、他の変形形態に適用され得る。本開示全体にわたって、「例」または「例示的」という用語は、例または事例を示すものであり、言及された例についてのいかなる選好を暗に示すものでも必要とするものでもない。したがって、本開示は、本明細書に説明された例および設計に限定されるべきではなく、本明細書に開示された原理および新規な特徴と一致する最も広い範囲を与えられるべきである。
以下に本願の出願当初の特許請求の範囲に記載された発明を付記する。
［Ｃ１］
ワイヤレス通信のための方法であって、
再認証鍵およびシーケンス番号からワイヤレス局において第１の識別子を導出することと、前記再認証鍵は、第１のセッション鍵から少なくとも部分的に導出される、
前記第１の識別子およびドメイン名を認証者に送信することと、前記第１の識別子および前記ドメイン名は、認証サーバとの前記ワイヤレス局の第１の再認証中に送信される、
前記第１の再認証中、前記第１のセッション鍵の名前の送信を差し控えることと
を備える、ワイヤレス通信のための方法。
［Ｃ２］
前記シーケンス番号に少なくとも部分的に基づいて次のシーケンス番号を生成することと、
前記再認証鍵および前記次のシーケンス番号に少なくとも部分的に基づいて第２の識別子を導出することと
をさらに備える、Ｃ１に記載の方法。
［Ｃ３］
前記第２の識別子および前記ドメイン名を送信すること、前記第２の識別子および前記ドメイン名は、前記認証サーバとの前記ワイヤレス局の第２の再認証中に送信される、
をさらに備える、Ｃ２に記載の方法。
［Ｃ４］
再認証失敗メッセージを受信することと、
前記再認証失敗メッセージを受信することに応答して、前記第２の識別子および前記ドメイン名を送信することと
をさらに備える、Ｃ２に記載の方法。
［Ｃ５］

前記認証サーバとの前記ワイヤレス局の単一の再認証のために前記第１の識別子を使用すること
をさらに備える、Ｃ１に記載の方法。
［Ｃ６］
識別子ラベルに少なくとも部分的に基づいて前記第１の識別子を導出すること
をさらに備える、Ｃ１に記載の方法。
［Ｃ７］
前記第１の再認証は、拡張認証プロトコル（ＥＡＰ）再認証を備え、前記第１のセッション鍵は、拡張マスターセッション鍵（ＥＭＳＫ）を備え、前記再認証鍵は、再認証ルート鍵（ｒＲＫ）を備える、Ｃ１に記載の方法。
［Ｃ８］
前記第１の再認証は、前記認証サーバとの完全な認証を遂行した後に遂行される、Ｃ１に記載の方法。
［Ｃ９］
再認証失敗メッセージを受信することと、
前記再認証失敗メッセージを受信することに応答して、前記認証サーバとの完全な認証を遂行することと
をさらに備える、Ｃ１に記載の方法。
［Ｃ１０］
ワイヤレス通信のための装置であって、
プロセッサと、
前記プロセッサと電子通信しているメモリと、
前記メモリに記憶されている命令と
を備え、前記命令は、
再認証鍵およびシーケンス番号からワイヤレス局において第１の識別子を導出することと、前記再認証鍵は、第１のセッション鍵から少なくとも部分的に導出される、
前記第１の識別子およびドメイン名を認証者に送信することと、前記第１の識別子および前記ドメイン名は、認証サーバとの前記ワイヤレス局の第１の再認証中に送信される、
前記第１の再認証中、前記第１のセッション鍵の名前の送信を差し控えることと
を行うように前記プロセッサによって実行可能である、ワイヤレス通信のための装置。
［Ｃ１１］
前記シーケンス番号に少なくとも部分的に基づいて次のシーケンス番号を生成することと、
前記再認証鍵および前記次のシーケンス番号に少なくとも部分的に基づいて第２の識別子を導出することと
を行うように前記プロセッサによって実行可能な命令をさらに備える、Ｃ１０に記載の装置。
［Ｃ１２］
前記第２の識別子および前記ドメイン名を送信することと、前記第２の識別子および前記ドメイン名は、前記認証サーバとの前記ワイヤレス局の第２の再認証中に送信される、
を行うように前記プロセッサによって実行可能な命令をさらに備える、Ｃ１１に記載の装置。
［Ｃ１３］
再認証失敗メッセージを受信することと、前記再認証失敗メッセージを受信することに応答して、前記第２の識別子および前記ドメイン名を送信することと
を行うように前記プロセッサによって実行可能な命令をさらに備える、Ｃ１１に記載の装置。
［Ｃ１４］
前記認証サーバとの前記ワイヤレス局の単一の再認証のために前記第１の識別子を使用

すること
を行うように前記プロセッサによって実行可能な命令をさらに備える、Ｃ１０に記載の装置。
［Ｃ１５］
識別子ラベルに少なくとも部分的に基づいて前記第１の識別子を導出すること
を行うように前記プロセッサによって実行可能な命令をさらに備える、Ｃ１０に記載の装置。
［Ｃ１６］
前記第１の再認証は、拡張認証プロトコル（ＥＡＰ）再認証を備え、前記第１のセッション鍵は、拡張マスターセッション鍵（ＥＭＳＫ）を備え、前記再認証鍵は、再認証ルート鍵（ｒＲＫ）を備える、Ｃ１０に記載の装置。
［Ｃ１７］
前記第１の再認証は、前記認証サーバとの完全な認証を遂行した後に遂行される、Ｃ１０に記載の装置。
［Ｃ１８］
再認証失敗メッセージを受信することと、
前記再認証失敗メッセージを受信することに応答して、前記認証サーバとの完全な認証を遂行することと
を行うことを前記プロセッサによって実行可能な命令をさらに備える、Ｃ１０に記載の装置。
［Ｃ１９］
ワイヤレス通信のための方法であって、
再認証鍵およびシーケンス番号から、認証サーバにおいて、第１の識別子を導出することと、前記再認証鍵は、第１のセッション鍵から少なくとも部分的に導出される、
第２の識別子を前記認証サーバにおいて受信することと、前記第２の識別子は、前記認証サーバとのワイヤレス局の第１の再認証中に受信される、
前記第１の識別子を前記第２の識別子と比較することと、
前記比較することに少なくとも部分的に基づいて前記ワイヤレス局の認証者に第２のセッション鍵を送信することと
を備える、ワイヤレス通信のための方法。
［Ｃ２０］
前記第１の識別子は、前記第２の識別子と一致する、Ｃ１９に記載の方法。
［Ｃ２１］
前記シーケンス番号に少なくとも部分的に基づいて次のシーケンス番号を生成することと、
前記再認証鍵および前記次のシーケンス番号に少なくとも部分的に基づいて第３の識別子を導出することと
をさらに備える、Ｃ１９に記載の方法。
［Ｃ２２］
前記認証サーバとの前記ワイヤレス局の第２の再認証中に第４の識別子を受信することと、
前記第３の識別子を前記第４の識別子と比較することと、
前記比較することに少なくとも部分的に基づいて前記第２のセッション鍵を送信することと
をさらに備える、Ｃ２１に記載の方法。
［Ｃ２３］
前記第３の識別子は、前記第４の識別子と一致する、Ｃ２２に記載の方法。
［Ｃ２４］
識別子ラベルに少なくとも部分的に基づいて前記第１の識別子を導出すること、をさらに備える、Ｃ１９に記載の方法。

［Ｃ２５］
前記第１の識別子が前記第２の識別子と一致できないとき、再認証失敗メッセージを送信すること、をさらに備える、Ｃ１９に記載の方法。
［Ｃ２６］
前記再認証失敗メッセージは、前記第１の識別子と前記第２の識別子との間の不一致を示すタイプレングスバリュー（ＴＬＶ）要素を備える、Ｃ２５に記載の方法。
［Ｃ２７］
前記第１の再認証は、拡張認証プロトコル（ＥＡＰ）再認証を備え、前記第１のセッション鍵は、拡張マスターセッション鍵（ＥＭＳＫ）を備え、前記再認証鍵は、再認証ルート鍵（ｒＲＫ）を備え、前記第２のセッション鍵は、再認証マスターセッション鍵（ｒＭＳＫ）を備える、Ｃ１９に記載の方法。
［Ｃ２８］
ワイヤレス通信のための装置であって、
プロセッサと、
前記プロセッサと電子通信しているメモリと、
前記メモリに記憶されている命令と
を備え、前記命令は、
再認証鍵およびシーケンス番号から、認証サーバにおいて、第１の識別子を導出することと、前記再認証鍵は、第１のセッション鍵から少なくとも部分的に導出される、
第２の識別子を前記認証サーバにおいて受信することと、前記第２の識別子は、前記認証サーバとのワイヤレス局の第１の再認証中に受信される、
前記第１の識別子を前記第２の識別子と比較することと、
前記比較することに少なくとも部分的に基づいて前記ワイヤレス局の認証者に第２のセッション鍵を送信することと
を行うように前記プロセッサによって実行可能である、ワイヤレス通信のための装置。
［Ｃ２９］
前記第１の識別子は、前記第２の識別子と一致する、Ｃ２８に記載の装置。
［Ｃ３０］
前記シーケンス番号に少なくとも部分的に基づいて次のシーケンス番号を生成することと、
前記再認証鍵および前記次のシーケンス番号に少なくとも部分的に基づいて第３の識別子を導出することと
を行うように前記プロセッサによって実行可能な命令をさらに備える、Ｃ２８に記載の装置。