(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7555962号
(P7555962)

(45)発行日　令和6年9月25日(2024.9.25)

(24)登録日　令和6年9月13日(2024.9.13)

(51)国際特許分類

		FI	
H04W	*12/0433(2021.01)*	H04W	12/0433
G06F	*21/64 (2013.01)*	G06F	21/64
H04W	*12/041 (2021.01)*	H04W	12/041
H04W	*12/06 (2021.01)*	H04W	12/06
H04W	*36/08 (2009.01)*	H04W	36/08

請求項の数　29　（全38頁）　最終頁に続く

(21)出願番号　特願2021-564354(P2021-564354)
(86)(22)出願日　令和2年3月27日(2020.3.27)
(65)公表番号　特表2022-530961(P2022-530961A)
(43)公表日　令和4年7月5日(2022.7.5)
(86)国際出願番号　PCT/CN2020/081779
(87)国際公開番号　WO2020/220888
(87)国際公開日　令和2年11月5日(2020.11.5)
審査請求日　令和3年12月7日(2021.12.7)
審判番号　不服2023-11398(P2023-11398/J1)
審判請求日　令和5年7月6日(2023.7.6)
(31)優先権主張番号　201910356843.8
(32)優先日　平成31年4月29日(2019.4.29)
(33)優先権主張国・地域又は機関
最終頁に続く

(73)特許権者　503433420
華為技術有限公司
HUAWEI TECHNOLOGIES CO.,LTD.
中華人民共和国 518129 広東省深▲チェン▼市龍崗区坂田 華為総部▲ベン▼公楼
Huawei Administration Building, Bantian, Longgang District, Shenzhen, Guangdong 518129, P.R. China
(74)代理人　100110364
弁理士　実広 信哉
最終頁に続く

(54)【発明の名称】　ハンドオーバー処理方法および装置

(57)【特許請求の範囲】

【請求項１】

ハンドオーバー処理方法であって、前記方法は、ハンドオーバー処理装置が第1のアクセス管理ネットワーク要素（AMF）から第2のAMFにハンドオーバーされるシナリオに適用され、前記方法は、

前記ハンドオーバー処理装置により、第1のアクセスネットワークデバイスからハンドオーバーコマンドメッセージを受信するステップであって、前記ハンドオーバーコマンドメッセージが非アクセス層コンテナ（NASC）を搬送する、ステップと、

前記ハンドオーバー処理装置により、前記NASCに対して完全性検証を行うステップと、

前記NASCに対して行われる前記完全性検証が失敗したならば、前記ハンドオーバー処理装置により、第1の非アクセス層（NAS）セキュリティコンテキストを使用し続けるステップであって、前記第1のNASセキュリティコンテキストが前記ハンドオーバー処理装置と前記第1のAMFの間で使用されるセキュリティコンテキストである、ステップと、

を含む方法。

【請求項２】

前記方法は、

前記NASCが鍵導出指示を含み、かつ前記鍵導出指示の値が1であるならば、前記ハンドオーバー処理装置により、前記第1のNASセキュリティコンテキストに基づいて第3のNASセキュリティコンテキストを取得するステップをさらに含む、請求項1に記載の方法。

【請求項３】

前記第1のセキュリティコンテキストは第1の鍵Kamfを含み、前記ハンドオーバー処理装置により、前記第1のセキュリティコンテキストに基づいて第3のセキュリティコンテキストを取得する前記ステップは、
前記ハンドオーバー処理装置により、前記第1のKamfに基づいて第2のKamfを取得するステップを含む、請求項2に記載の方法。
【請求項４】
前記方法は、
前記NASCに対して行われる前記完全性検証が失敗したならば、前記第3のセキュリティコンテキストを削除するステップをさらに含む、請求項2または3に記載の方法。
【請求項５】
前記方法は、
前記NASCに対して行われる前記完全性検証が成功したならば、前記ハンドオーバー処理装置と前記第2のAMFの間で使用される情報に対してセキュリティ保護を行うために、前記第3のセキュリティコンテキストを使用するステップをさらに含む、請求項2または3に記載の方法。
【請求項６】
前記ハンドオーバー処理装置により、第1の非アクセス層（NAS）セキュリティコンテキストを使用し続ける前記ステップは、
前記ハンドオーバー処理装置と前記第1のAMFの間で使用される情報に対してセキュリティ保護を行うために、前記ハンドオーバー処理装置により、前記第1のNASセキュリティコンテキストを使用するステップを含む、請求項1に記載の方法。
【請求項７】
前記方法は、
前記NASCが鍵導出指示を含み、かつ前記鍵導出指示の値が1であるならば、前記ハンドオーバー処理装置により、前記第1のNASセキュリティコンテキストを記憶するステップをさらに含む、請求項1に記載の方法。
【請求項８】
前記方法は、
前記NASCに対して行われる前記完全性検証が失敗したならば、前記ハンドオーバー処理装置により、前記第1のアクセスネットワークデバイスを通じて前記第1のAMFへハンドオーバーキャンセル要求を送信するステップをさらに含む、請求項1に記載の方法。
【請求項９】
第1のアクセスネットワークデバイスからハンドオーバーコマンドメッセージを受信するように構成された受信ユニットであって、前記ハンドオーバーコマンドメッセージが非アクセス層コンテナ（NASC）を搬送する、受信ユニットと、
前記NASCに対して完全性検証を行い、前記NASCに対して行われる前記完全性検証が失敗したならば、第1の非アクセス層（NAS）セキュリティコンテキストを使用し続けるように構成された処理ユニットであって、前記第1のNASセキュリティコンテキストが前記ハンドオーバー処理装置と前記第1のAMFの間で使用されるセキュリティコンテキストである、処理ユニットと、
を備えるハンドオーバー処理装置。
【請求項１０】
前記NASCが鍵導出指示を含み、かつ前記鍵導出指示の値が1であるならば、前記処理ユニットは、前記第1のNASセキュリティコンテキストに基づいて第3のNASセキュリティコンテキストを取得するようにさらに構成された、
請求項9に記載の処理装置。
【請求項１１】
前記第1のセキュリティコンテキストは第1の鍵Kamfを含み、前記処理ユニットは、前記第1のKamfに基づいて第2のKamfを取得するようにさらに構成された、請求項10に記載の処理装置。

【請求項１２】
前記処理ユニットは、前記NASCに対して行われる前記完全性検証が失敗したならば、前記第3のセキュリティコンテキストを削除するようにさらに構成された、請求項10または11に記載の処理装置。
【請求項１３】
前記処理ユニットは、前記NASCに対して行われる前記完全性検証が成功したならば、前記ハンドオーバー処理装置と前記第2のAMFの間で使用される情報に対してセキュリティ保護を行うために、前記第3のセキュリティコンテキストを使用するようにさらに構成された、請求項10または11に記載の処理装置。
【請求項１４】
前記処理ユニットは、具体的には、前記ハンドオーバー処理装置と前記第1のAMFの間で使用される情報に対してセキュリティ保護を行うために、前記第1のNASセキュリティコンテキストを使用するように構成された、請求項9に記載の処理装置。
【請求項１５】
前記処理ユニットは、前記NASCが鍵導出指示を含み、かつ前記鍵導出指示の値が1であるならば、前記第1のNASセキュリティコンテキストを記憶するようにさらに構成された、請求項9に記載の処理装置。
【請求項１６】
前記処理装置は送信ユニットをさらに含み、前記送信ユニットは、前記NASCに対して行われる前記完全性検証が失敗したならば、前記第1のアクセスネットワークデバイスを通じて前記第1のAMFへハンドオーバーキャンセル要求を送信するように構成された、請求項9に記載の処理装置。
【請求項１７】
ハンドオーバー処理装置により、第1のアクセスネットワークデバイスによって送信されるハンドオーバーコマンドメッセージを受信するステップであって、前記ハンドオーバーコマンドメッセージが、第2のアクセスおよびモビリティ管理機能（AMF）によって選択される第2のNASセキュリティアルゴリズム、およびAMF鍵変更指示を搬送する、ステップと、
前記第2のNASセキュリティアルゴリズムが第1のNASセキュリティアルゴリズムと異なり、かつ／または前記AMF鍵変更指示が既定の値であるとき、前記ハンドオーバー処理装置により、第1の非アクセス層（NAS）セキュリティコンテキストを記憶するステップであって、前記第1のNASセキュリティコンテキストが前記ハンドオーバー処理装置と第1のAMFの間のネゴシエーションを通じて生成されるNASセキュリティコンテキストである、ステップと、前記ハンドオーバー処理装置がハンドオーバーされることが失敗したとき、前記ハンドオーバー処理装置と前記第1のAMFの間で非アクセス層NAS保護を行うために、前記記憶された第1のNASセキュリティコンテキストを使用するステップ、または
前記ハンドオーバー処理装置によって非アクセス層コンテナ（NASC）に対して行われる完全性チェックが失敗したとき、前記ハンドオーバー処理装置により、前記第1のNASセキュリティコンテキストを使用し続けるステップであって、前記NASCが前記第1のアクセスネットワークデバイスから前記ハンドオーバーコマンドメッセージによって搬送される、ステップと、
を含むハンドオーバー処理方法。
【請求項１８】
前記第1のNASセキュリティコンテキストは、第1のNASセキュリティアルゴリズム、第1のAMF鍵Kamf1、第1の非アクセス層NAS鍵、および第1の非アクセス層カウントNAS COUNTを含む、請求項17に記載の方法。
【請求項１９】
前記AMF鍵変更指示が既定の値であることは、
前記AMF鍵変更指示が1であることを含む、請求項17または18に記載の方法。
【請求項２０】

ハンドオーバー処理装置であって、
第1のアクセスネットワークデバイスによって送信されるハンドオーバーコマンドメッセージを受信するように構成された受信ユニットであって、前記ハンドオーバーコマンドメッセージが、第2のアクセスおよびモビリティ管理機能（AMF）によって選択される第2のNASセキュリティアルゴリズム、およびAMF鍵変更指示を搬送する、受信ユニットと、
処理ユニットと、を備え、
前記処理ユニットは、前記第2のNASセキュリティアルゴリズムが第1のNASセキュリティアルゴリズムと異なり、かつ／または前記AMF鍵変更指示が既定の値であるとき、第1の非アクセス層（NAS）セキュリティコンテキストを記憶するように構成された処理ユニットであって、前記第1のNASセキュリティコンテキストが前記処理ユニットと第1のAMFの間のネゴシエーションを通じて生成されるNASセキュリティコンテキストである、処理ユニットであって、前記処理ユニットが、ハンドオーバーが失敗したとき、前記装置と前記第1のAMFの間で非アクセス層（NAS）保護を行うために、前記記憶された第1のNASセキュリティコンテキストを使用するようにさらに構成され、または
前記処理ユニットは、非アクセス層コンテナ（NASC）に対して行われる完全性チェックが失敗したとき、前記処理ユニットが前記第1のNASセキュリティコンテキストを使用し続けるように構成され、前記NASCが前記第1のアクセスネットワークデバイスから前記ハンドオーバーコマンドメッセージによって搬送される、装置。
【請求項２１】
前記第1のNASセキュリティコンテキストは、第1のNASセキュリティアルゴリズム、第1のAMF鍵Kamf1、第1の非アクセス層NAS鍵、および第1の非アクセス層カウントNAS COUNTを含む、請求項20に記載の装置。
【請求項２２】
前記AMF鍵変更指示が既定の値であることは、
前記AMF鍵変更指示が1であることを含む、請求項20または21に記載の装置。
【請求項２３】
通信デバイスであって、
メモリーであって、コンピュータプログラムを記憶するように構成されたメモリーと、
トランシーバであって、送信および受信するステップを実行するように構成されたトランシーバと、
プロセッサであって、前記メモリーから前記コンピュータプログラムを呼び出し、前記コンピュータプログラムを実行して、前記通信デバイスが、請求項17から19のいずれか一項に記載の方法を実行することを可能にするように構成されたプロセッサと、
を備える通信デバイス。
【請求項２４】
コンピュータ可読記憶媒体であって、前記コンピュータ可読媒体はコンピュータプログラムを記憶し、前記コンピュータプログラムがコンピュータにおいて実行されるとき、前記コンピュータは請求項17から19のいずれか一項に記載の方法を実行することが可能にされる、コンピュータ可読記憶媒体。
【請求項２５】
コンピュータプログラムを記憶するように構成されたメモリーと、
送信および受信するステップを実行するように構成されたトランシーバと、
プロセッサであって、前記プロセッサが前記メモリーおよび前記トランシーバに結合され、前記メモリー内の前記コンピュータプログラムが前記プロセッサによって実行されるとき、前記プロセッサが請求項1から8のいずれか一項に記載の方法を実行することが可能にされる、プロセッサと、
を備える通信デバイス。
【請求項２６】
コンピュータ可読記憶媒体であって、前記コンピュータ可読媒体はコンピュータプログラムを記憶し、前記コンピュータプログラムがコンピュータにおいて実行されるとき、プ

ロセッサは請求項1から8のいずれか一項に記載の方法を実行することが可能にされる、コンピュータ可読記憶媒体。
【請求項２７】
チップであって、前記チップはプロセッサを備え、前記プロセッサは、メモリーに記憶されたコンピュータプログラムを読み取り、前記コンピュータプログラムを実行して、請求項1から8のいずれか一項に記載の方法を実行するように構成された、チップ。
【請求項２８】
前記チップは前記メモリーをさらに備え、前記メモリーは回路またはケーブルを通じて前記プロセッサに接続され、前記プロセッサは、前記メモリー内の前記コンピュータプログラムを読み取って実行するように構成された、請求項27に記載のチップ。
【請求項２９】
前記チップは通信インターフェイスをさらに備え、前記プロセッサは前記通信インターフェイスに接続され、前記通信インターフェイスは、処理される必要があるデータおよび／または情報を受信するように構成され、前記プロセッサは前記通信インターフェイスから前記データおよび／または情報を取得し、前記データおよび／または情報を処理する、請求項27または28に記載のチップ。
【発明の詳細な説明】
【技術分野】
【０００１】
本出願は、参照により全体が本出願に組み込まれる、2019年4月29日に中国特許庁に提出された「ハンドオーバー処理方法および装置」と題する中国特許出願第201910356843.8号の優先権を主張するものである。
【０００２】
本発明は通信分野に関し、より具体的には、ハンドオーバー処理方法および装置に関する。
【背景技術】
【０００３】
第5世代（5th generation、5G）通信のシナリオでは、ユーザー機器の移動のため、アクセスネットワークデバイスハンドオーバーのシナリオが存在し得る。例えば、ユーザー機器の位置変更は、ユーザー機器にサービス提供するアクセスネットワークデバイスの変更を引き起こす。現在の通信プロトコルでは、2種類のアクセスネットワークデバイスハンドオーバーが、すなわちXnハンドオーバーとN2ハンドオーバーが、規定されている。Xnハンドオーバーは、アクセスネットワークデバイスハンドオーバーが発生する前後にアクセスネットワークデバイス間にXnインターフェイスが存在し、そのインターフェイスに基づいてアクセスネットワークデバイスハンドオーバーが行われることを意味する。N2ハンドオーバーは、アクセスネットワークデバイスとコアネットワーク要素、すなわちアクセスおよびモビリティ管理機能（access and mobility management function、AMF）との間のN2インターフェイスに基づいてアクセスネットワークデバイスハンドオーバーが行われることを意味する。
【０００４】
既存のN2ハンドオーバーシナリオでアクセスネットワークデバイスハンドオーバーが失敗すると、ハンドオーバー手順においてユーザー機器上の鍵が第1のAMF上の鍵と相違する場合がある。このため、アクセスネットワークデバイスハンドオーバーが失敗した後に、ユーザー機器は第1のAMFへの接続を再度確立できない。
【発明の概要】
【課題を解決するための手段】
【０００５】
本出願はハンドオーバー処理方法および装置を開示する。アクセスネットワークデバイスハンドオーバーが失敗したとき、ユーザー機器上のセキュリティコンテキストが第1のAMF上のセキュリティコンテキストと同じになることを保証し、ユーザー機器上の鍵が第1

のAMF上の鍵と同じになることをさらに保証するため、第1のAMFは第1のNASセキュリティコンテキストを記憶し、第1のNASセキュリティコンテキストを使用することを再開する。

【０００６】

第1の態様によると、第1のアクセスおよびモビリティ管理機能AMFにより、第1のアクセスネットワークデバイスによって送信されるハンドオーバー要求メッセージを受信するステップと、鍵導出が行われる必要があると判断するとき、第1のAMFにより、第1の非アクセス層NASセキュリティコンテキストを記憶するステップであって、第1のNASセキュリティコンテキストが第1のAMFとユーザー機器UEの間のネゴシエーションを通じて生成されるNASセキュリティコンテキストである、ステップと、第1のAMFにより、第1のNASセキュリティコンテキストを使用することを再開するステップと、を含むハンドオーバー処理方法が提供される。

【０００７】

本出願の本実施形態で提供されるハンドオーバー処理方法によると、鍵導出が行われる必要がある場合に、第1のAMFは第1のNASセキュリティコンテキストを記憶し、鍵導出の後に第1のNASセキュリティコンテキストを使用することを再開するので、アクセスネットワークデバイスハンドオーバーが失敗したとき、ユーザー機器上の鍵は第1のAMF上の鍵と同じになる。

【０００８】

本出願の本実施形態における第1のNASセキュリティコンテキストが、UEによって現在使用されているNASセキュリティコンテキストと呼ばれることもあることを理解されたい。

【０００９】

第1の態様を参照し、第1の態様のいくつかの実装において、第1のNASセキュリティコンテキストは、第1のNASセキュリティアルゴリズム、第1のAMF鍵Kamf1、第1の非アクセス層NAS鍵、および第1の非アクセス層カウントNAS COUNTを含む。

【００１０】

本出願の本実施形態で提供されるハンドオーバー処理方法によると、第1のNASセキュリティコンテキストは、第1のAMFとユーザー機器UEの間で使用のために取り決められるAMF鍵Kamf1と、第1のAMFとユーザー機器UEの間のネゴシエーションを通じて生成されるNAS鍵と、非アクセス層カウントNAS COUNTとを含む。

【００１１】

第1の態様を参照し、第1の態様のいくつかの実装において、第1のAMFにより、第1のNASセキュリティコンテキストを使用することを再開するステップは、第1のAMFが第2のAMFに対してユーザーコンテキスト作成サービス要求を開始した後に、第1のAMFにより、第1のNASセキュリティコンテキストを使用することを再開するステップを含む。

【００１２】

本出願の本実施形態で提供されるハンドオーバー処理方法によると、第1のAMFは、第1のAMFが第2のAMFに対してユーザーコンテキスト作成サービス要求を開始した後に、開始する前に、または開始するときに、第1のNASセキュリティコンテキストを使用することを再開できる。

【００１３】

第2の態様によると、ユーザー機器UEにより、第1のアクセスネットワークデバイスによって送信されるハンドオーバーコマンドメッセージを受信するステップであって、ハンドオーバーコマンドメッセージが、第2のアクセスおよびモビリティ管理機能AMFによって選択される第2のNASセキュリティアルゴリズム、およびAMF鍵変更指示を搬送する、ステップと、第2のNASセキュリティアルゴリズムがUEによって現在使用されている第1のNASセキュリティアルゴリズムと異なり、かつ／またはAMF鍵変更指示が既定の値であるとき、UEにより、第1の非アクセス層NASセキュリティコンテキストを記憶するステップであって、第1のNASセキュリティコンテキストがUEと第1のAMFの間のネゴシエーシ

ョンを通じて生成されるNASセキュリティコンテキストである、ステップと、UEユーザー機器のハンドオーバーが失敗したとき、UEと第1のAMFの間で非アクセス層NAS保護を行うために、第1のNASセキュリティコンテキストを使用するステップ、またはUEによって非アクセス層コンテナNASCに対して行われる完全性チェックが失敗したとき、UEにより、第1のNASセキュリティコンテキストを使用し続けるステップであって、NASCがハンドオーバーコマンドメッセージ内で搬送される、ステップと、を含むハンドオーバー処理方法が提供される。

【００１４】

本出願の本実施形態で提供されるハンドオーバー処理方法によると、UEによって受信されるハンドオーバーコマンドメッセージが第2のNASセキュリティアルゴリズムを搬送し、かつ／またはAMF鍵変更指示が1であるとき、UEは第1のNASセキュリティコンテキストを記憶し、UEユーザー機器のハンドオーバーが失敗したとき、UEは、UEと第1のAMFの間で非アクセス層NAS保護を行うために、第1のNASセキュリティコンテキストを使用し、または、UEによって行われるNASC完全性チェックが失敗したとき、UEは現在の第1のNASセキュリティコンテキストを使用し続けるので、ユーザー機器上の鍵は第1のAMF上の鍵と同じになる。

【００１５】

第2の態様を参照し、第2の態様のいくつかの実装において、第1のNASセキュリティコンテキストは、第1のNASセキュリティアルゴリズム、第1のAMF鍵Kamf1、第1の非アクセス層NAS鍵、および第1の非アクセス層カウントNAS COUNTを含む。

【００１６】

本出願の本実施形態で提供されるハンドオーバー処理方法によると、第1のNASセキュリティコンテキストは、第1のAMFとユーザー機器UEの間で使用のために取り決められるAMF鍵Kamf1と、第1のAMFとユーザー機器UEの間のネゴシエーションを通じて生成されるNAS鍵と、非アクセス層カウントNAS COUNTとを含む。

【００１７】

第2の態様を参照し、第2の態様のいくつかの実装において、AMF鍵変更指示が既定の値であることは、AMF鍵変更指示が1であることを含む。

【００１８】

本出願の本実施形態で提供されるハンドオーバー処理方法によると、AMF鍵変更指示の値が1である場合、これは鍵導出が行われることを意味する。

【００１９】

第3の態様によると、第1のアクセスおよびモビリティ管理機能AMFにより、第1のアクセスネットワークデバイスによって送信されるハンドオーバー要求メッセージを受信するステップと、第2のAMF鍵を取得するために、第1のAMFにより、ローカルポリシーに従って鍵導出を行うステップと、第1のAMFにより、第2のAMF鍵と第1のNASセキュリティアルゴリズムとに基づいて第2のNASセキュリティコンテキストを生成するステップであって、第1のNASセキュリティアルゴリズムが第1のAMFとユーザー機器UEの間で取り決められるNASセキュリティアルゴリズムである、ステップと、第1のAMFとUEの間で非アクセス層NAS保護を行うために、第1のAMFにより、第2のNASセキュリティコンテキストを使用するステップとを含む、ハンドオーバー処理方法が提供される。

【００２０】

本出願の本実施形態で提供されるハンドオーバー処理方法によると、第1のAMFが鍵導出を行うことによって第2のAMF鍵を生成するときに、第1のAMFは、第2のAMF鍵と、第1のAMFとユーザー機器UEの間で取り決められる第1のNASセキュリティアルゴリズムとに基づいて、第2のNASセキュリティコンテキストを生成できる。

【００２１】

第3の態様を参照し、第3の態様のいくつかの実装において、第2のNASセキュリティコンテキストは、第1のNASセキュリティアルゴリズムと、第2のAMF鍵と、第2の非アクセス層NAS鍵と、第2の非アクセス層カウントNAS COUNTとを含む。

【００２２】
第4の態様によると、ユーザー機器UEにより、第1のアクセスネットワークデバイスによって送信されるハンドオーバーコマンドメッセージを受信するステップであって、ハンドオーバーコマンドメッセージが第2のアクセスおよびモビリティ管理機能AMFによって選択される第2のNASセキュリティアルゴリズム、およびAMF鍵変更指示を搬送する、ステップと、第2のNASセキュリティアルゴリズムが第1のNASセキュリティアルゴリズムと異なり、かつAMF鍵変更指示が既定の値であるとき、UEにより、第1のNASセキュリティアルゴリズムを記憶し、第2のAMF鍵を取得するために鍵導出を行うステップであって、第1のNASセキュリティアルゴリズムがUEと第1のアクセスおよびモビリティ管理機能AMFの間で取り決められるNASセキュリティアルゴリズムである、ステップと、を含むハンドオーバー処理方法が提供される。
【００２３】
本出願の本実施形態で提供されるハンドオーバー処理方法によると、UEによって受信されるハンドオーバーコマンドメッセージが第2のNASセキュリティアルゴリズムを搬送し、かつAMF鍵変更指示が1であるとき、UEは第1のNASセキュリティアルゴリズムを記憶し、第2のAMF鍵を取得するためにAMF鍵変更指示に基づいて鍵導出を行う。第4の態様を参照し、第4の態様のいくつかの実装において、UEは、第2のAMF鍵と第1のNASセキュリティアルゴリズムとに基づいて第2のNASセキュリティコンテキストを生成する。
【００２４】
本出願の本実施形態で提供されるハンドオーバー処理方法によると、UEは、新たに生成される第2のAMF鍵と記憶されている第1のNASセキュリティアルゴリズムとに基づいて、第2のNASセキュリティコンテキストを生成できる。
【００２５】
第4の態様を参照し、第4の態様のいくつかの実装において、UEのハンドオーバーに失敗するとき、UEは、UEと第1のAMFの間で非アクセス層NASセキュリティ保護を行うために、第2のNASセキュリティコンテキストを使用する。
【００２６】
本出願の本実施形態で提供されるハンドオーバー処理方法によると、UEのハンドオーバーに失敗するとき、UEは、UEと第1のAMFの間で非アクセス層NASセキュリティ保護を行うために、第2のNASセキュリティコンテキストを使用する。
【００２７】
第4の態様を参照し、第4の態様のいくつかの実装において、UEのハンドオーバーに失敗するとき、UEは、第2のAMF鍵と第1のNASセキュリティアルゴリズムとに基づいて第2のNASセキュリティコンテキストを生成し、UEと第1のAMFの間で非アクセス層NASセキュリティ保護を行うために、第2のNASセキュリティコンテキストを使用する。
【００２８】
本出願の本実施形態で提供されるハンドオーバー処理方法によると、UEのハンドオーバーに失敗すると、UEはまず、新たに生成される第2のAMF鍵と記憶されている第1のNASセキュリティアルゴリズムとに基づいて、第2のNASセキュリティコンテキストを生成し、次いで、UEと第1のAMFの間で非アクセス層NASセキュリティ保護を行うために、第2のNASセキュリティコンテキストを使用する。
【００２９】
第4の態様を参照し、第4の態様のいくつかの実装において、AMF鍵変更指示が既定の値であることは、AMF鍵変更指示が1であることを含む。
【００３０】
本出願の本実施形態で提供されるハンドオーバー処理方法によると、AMF鍵変更指示の値が1である場合、これは鍵導出が行われることを意味する。
【００３１】
第5の態様によると、ハンドオーバー処理装置が提供される。装置は、第1の態様、または第1の態様の可能な実装のいずれか1つにおけるユーザー機器の動作を、あるいは第3の

態様、または第3の態様の可能な実装のいずれか1つにおけるユーザー機器の動作を、実行するように構成されてよい。具体的に述べると、ハンドオーバー処理装置は、第1の態様、または第1の態様の可能な実装のいずれか1つに記載されたステップまたは機能を、あるいは第3の態様、または第3の態様の可能な実装のいずれか1つに記載されたステップまたは機能を、実現するように構成された対応する手段（means）を含んでよい。対応する手段は、第1の態様または第3の態様におけるユーザー機器であってよく、あるいは第1の態様または第3の態様におけるユーザー機器内のチップもしくは機能モジュールであってもよい。ステップまたは機能は、ソフトウェア、ハードウェア、またはハードウェアとソフトウェアとの組み合わせによって実装されてよい。

【００３２】

第6の態様によると、ハンドオーバー処理装置が提供される。装置は、第2の態様、または第2の態様の可能な実装のいずれか1つにおける第1のAMFの動作を、あるいは第4の態様、または第4の態様の可能な実装のいずれか1つにおける第1のAMFの動作を、実行するように構成されてよい。具体的に述べると、ハンドオーバー処理装置は、第2の態様、または第2の態様の可能な実装のいずれか1つに記載されたステップまたは機能を、あるいは第4の態様、または第4の態様の可能な実装のいずれか1つに記載されたステップまたは機能を、実現するように構成された対応する手段（means）を含んでよい。対応する手段は、第2の態様または第4の態様における第1のAMFであってよく、あるいは第2の態様または第4の態様における第1のAMF内のチップまたは機能モジュールであってもよい。ステップまたは機能は、ソフトウェア、ハードウェア、またはハードウェアとソフトウェアとの組み合わせによって実装されてよい。

【００３３】

第7の態様によると、プロセッサとトランシーバとメモリーとを備える通信デバイスが提供される。メモリーは、コンピュータプログラムを記憶するように構成される。トランシーバは、第1の態様から第4の態様、または第1の態様から第4の態様の可能な実装のいずれか1つのハンドオーバー処理方法において送信および受信するステップを実行するように構成される。プロセッサは、メモリーからコンピュータプログラムを呼び出し、コンピュータプログラムを実行して、通信デバイスが、第1の態様から第4の態様、または第1の態様から第4の態様の可能な実装のいずれか1つのハンドオーバー処理方法を実行することを可能にするように構成される。

【００３４】

任意に選べることとして、1つ以上のプロセッサがあり、1つ以上のメモリーがある。

【００３５】

任意に選べることとして、メモリーはプロセッサと統合されてよく、あるいはメモリーとプロセッサは別々に配置される。

【００３６】

任意に選べることとして、トランシーバは、送信器（送信器）と受信器（受信器）を含んでよい。

【００３７】

第8の態様によると、システムが提供される。システムは、第5の態様および第6の態様で提供されるハンドオーバー処理装置を含む。

【００３８】

第9の態様によると、コンピュータプログラム製品が提供される。コンピュータプログラム製品はコンピュータプログラム（コードまたは命令と呼ばれることもある）を含む。コンピュータプログラムが実行されると、コンピュータは、第1の態様から第4の態様、または第1の態様から第4の態様の可能な実装のいずれか1つの方法を実行することが可能にされる。

【００３９】

第10の態様によると、コンピュータ可読媒体が提供される。コンピュータ可読媒体はコンピュータプログラム（コードまたは命令と呼ばれることもある）を記憶する。コンピュ

ータプログラムがコンピュータで実行されると、コンピュータは、第1の態様から第4の態様、または第1の態様から第4の態様の可能な実装のいずれか1つの方法を実行することが可能にされる。

【００４０】

第11の態様によると、チップシステムが提供され、チップシステムはメモリーとプロセッサとを含む。メモリーは、コンピュータプログラムを記憶するように構成される。プロセッサは、メモリーからコンピュータプログラムを呼び出し、コンピュータプログラムを実行して、チップシステムが取り付けられた通信デバイスが、第1の態様から第4の態様、または第1の態様から第4の態様の可能な実装のいずれか1つの方法を実行することを可能にするように構成される。

【図面の簡単な説明】

【００４１】

【図１】本出願の実施形態に適用可能なネットワークアーキテクチャを示す。

【図２】ハンドオーバー失敗手順の概略図である。

【図３】別のハンドオーバー失敗手順の概略図である。

【図４】本出願の一実施形態によるハンドオーバー処理方法の概略フローチャートである。

【図５】本出願の一実施形態による別のハンドオーバー処理方法の概略フローチャートである。

【図６】本出願の一実施形態によるハンドオーバー処理装置10の概略図である。

【図７】本出願の一実施形態に適用可能なユーザー機器20の概略構造図である。

【図８】本出願の一実施形態によるハンドオーバー処理装置30の概略図である。

【図９】本出願の一実施形態に適用可能な第1のAMF 40の概略構造図である。

【発明を実施するための形態】

【００４２】

これ以降は、添付の図面を参照しながら本出願の技術的解決策を説明する。

【００４３】

図1は、本出願の実施形態に適用可能なネットワークアーキテクチャを示す。図1に示されているように、以下では、ネットワークアーキテクチャの構成要素を個別に説明する。

【００４４】

1．ユーザー機器110：ユーザー機器110は、様々な手持ち型デバイス、車載デバイス、ウェアラブルデバイス、または無線通信機能を有する計算デバイス、または無線モデムに接続された他の処理デバイス、ならびに様々な形態の端末、モバイルステーション（mobile station、MS）、端末（terminal）、ユーザー機器（user equipment、UE）、ソフトクライアントなどを含み得る。例えば、ユーザー機器110は、水道メーター、電気メーター、またはセンサであってよい。

【００４５】

2．（無線）アクセスネットワーク（radio access network、（R）AN）ネットワーク要素120：（R）ANネットワーク要素120は、特定のエリア内で認可されたユーザー機器のためにネットワークアクセス機能を提供するように構成され、ユーザー機器タイプおよびサービス要件などに応じて質の異なる伝送トンネルを使用できる。

【００４６】

（R）ANネットワーク要素は無線リソースを管理でき、ユーザー機器とコアネットワークとの間で制御信号やユーザー機器データを転送するため、ユーザー機器のためにアクセスサービスを提供できる。（R）ANネットワーク要素は、従来のネットワークにおける基地局として理解することもできる。

【００４７】

3．ユーザープレーンネットワーク要素130：ユーザープレーンネットワーク要素130は、パケットのルーティングと転送、ユーザープレーンデータに対するクオリティ・オブ・サービス（quality of service、QoS）処理など行うように構成される。

【００４８】

5G通信システムで、ユーザープレーンネットワーク要素はユーザープレーン機能（user plane function、UPF）ネットワーク要素であってもよい。将来の通信システムでは、ユーザープレーンネットワーク要素は依然としてUPFネットワーク要素であってもよく、または別の名前を有してもよい。これは本出願で限定されない。

【００４９】

4．データネットワークネットワーク要素140：データネットワークネットワーク要素140は、データを伝送するためのネットワークを提供するように構成される。

【００５０】

5G通信システムでは、データネットワークネットワーク要素はデータネットワーク（data network、DN）ネットワーク要素であってもよい。将来の通信システムでは、データネットワーク要素は依然としてDNネットワーク要素であってもよく、または別の名前を有してもよい。これは本出願で限定されない。

【００５１】

5．アクセス管理ネットワーク要素150：アクセス管理ネットワーク要素150は主に、モビリティ管理、アクセス管理などを行うように構成され、セッション管理以外のモビリティ管理エンティティ（mobility management entity、MME）の機能の中の機能を、例えば、合法的傍受やアクセス認可／認証を、実行するように構成されてよい。

【００５２】

5G通信システムで、アクセス管理ネットワーク要素はアクセスおよびモビリティ管理機能（access and mobility management function、AMF）ネットワーク要素であってもよい。将来の通信システムでは、アクセス管理ネットワーク要素は依然としてAMFであってもよく、または別の名前を有してもよい。これは本出願で限定されない。

【００５３】

6．セッション管理ネットワーク要素160：セッション管理ネットワーク要素160は、例えば、主に、セッションを管理し、ユーザー機器のインターネットプロトコル（internet protocol、IP）アドレスを割り当てて管理し、ユーザープレーン機能インターフェイスとポリシーコントロールおよび課金機能インターフェイスを管理できるエンドポイントを選択し、ダウンリンクデータ通知を行うように構成される。

【００５４】

5G通信システムで、セッション管理ネットワーク要素はセッション管理機能（session management function、SMF）ネットワーク要素であってもよい。将来の通信システムでは、セッション管理ネットワーク要素は依然としてSMFネットワーク要素であってもよく、または別の名前を有してもよい。これは本出願で限定されない。

【００５５】

7．ポリシーコントロールネットワーク要素170：ポリシーコントロールネットワーク要素170は、例えば、ネットワーク挙動について統一ポリシー機構を案内し、制御プレーン機能ネットワーク要素（AMFまたはSMFなど）のためにポリシールール情報を提供するように構成される。

【００５６】

4G通信システムでは、ポリシーコントロールネットワーク要素はポリシーおよび課金ルール機能（policy and charging rules function、PCRF）ネットワーク要素であってもよい。5G通信システムで、ポリシーコントロールネットワーク要素はポリシーコントロール機能（policy control function、PCF）ネットワーク要素であってもよい。将来の通信システムでは、ポリシーコントロールネットワーク要素は依然としてPCFネットワーク要素であってもよく、または別の名前を有してもよい。これは本出願で限定されない。

【００５７】

8．認証サーバー180：認証サーバー180は、認証サーバー180とユーザー機器との間で相互認証を実施し、統一認証機構をサポートするために、サービスを認証し、鍵を生成するように構成される。

【００５８】

5G通信システムで、認証サーバーは認証サーバー機能（authentication server function、AUSF）ネットワーク要素であってもよい。将来の通信システムでは、認証サーバー機能ネットワーク要素は依然としてAUSFネットワーク要素であってもよく、または別の名前を有してもよい。これは本出願で限定されない。

【００５９】

9．データ管理ネットワーク要素190：データ管理ネットワーク要素190は、例えば、ユーザー機器識別子、アクセス認証を処理し、登録管理およびモビリティ管理を行うように構成される。

【００６０】

5G通信システムで、データ管理ネットワーク要素は統一データ管理（unified data management、UDM）ネットワーク要素であってもよい。4G通信システムでは、データ管理ネットワーク要素は、ホーム加入者サーバー（home subscriber server、HSS）ネットワーク要素であってもよい。将来の通信システムでは、統一データ管理は依然としてUDMネットワーク要素であってもよく、または別の名前を有してもよい。これは本出願で限定されない。

【００６１】

10．アプリケーションネットワーク要素1100：アプリケーションネットワーク要素は、例えば、アプリケーションの影響を受けるトラフィックのルーティングを行い、ネットワーク曝露機能ネットワーク要素にアクセスし、ポリシーコントロールを行うためにポリシー機構とやり取りするように構成される。

【００６２】

5G通信システムで、アプリケーションネットワーク要素はアプリケーション機能（application function、AF）ネットワーク要素であってもよい。将来の通信システムでは、アプリケーションネットワーク要素は依然としてAFネットワーク要素であってもよく、または別の名前を有してもよい。これは本出願で限定されない。

【００６３】

11．ネットワークストレージネットワーク要素：ネットワークストレージネットワーク要素は、ネットワーク上の全てのネットワーク機能サービスのリアルタイム情報を維持するように構成される。

【００６４】

5G通信システムで、ネットワークストレージネットワーク要素はネットワーク登録機能（network repository function、NRF）ネットワーク要素であってもよい。将来の通信システムでは、ネットワークストレージネットワーク要素は依然としてNRFネットワーク要素であってもよく、または別の名前を有してもよい。これは本出願で限定されない。

【００６５】

前述したネットワーク要素や機能が、ハードウェアデバイス上のネットワーク要素、専用のハードウェア上で実行するソフトウェア機能、またはプラットフォーム（例えば、クラウドプラットフォーム）上でインスタンスとして生成される仮想機能であってよいことは理解できるであろう。説明を容易にするため、アクセス管理ネットワーク要素がAMFであり、データ管理ネットワーク要素がUDMネットワーク要素であり、セッション管理ネットワーク要素がSMFネットワーク要素であり、ユーザープレーンネットワーク要素がUPFネットワーク要素であることが、本出願の以降の説明の一例として使用される。

【００６６】

さらに、AMFネットワーク要素は略してAMFと呼ばれ、UDMネットワーク要素は略してUDMと呼ばれ、SMFネットワーク要素は略してSMFと呼ばれ、UPFネットワーク要素は略してUPFと呼ばれる。具体的に述べると、本出願の以降の説明では、AMFはアクセス管理ネットワーク要素に置き換えられてもよく、UDMはデータ管理ネットワーク要素に置き換えられてもよく、SMFはセッション管理ネットワーク要素に置き換えられてもよく、UPFはユーザープレーンネットワーク要素に置き換えられてもよい。

【００６７】

説明を容易にするため、本出願の実施形態では、装置がAMFエンティティおよびUDMエンティティであることが、セッション確立方法を説明するための一例として使用される。装置がAMFエンティティ内のチップおよびUDMエンティティ内のチップである実装方法については、装置がAMFエンティティおよびUDMエンティティである場合の具体的な説明を参照されたい。詳細は繰り返さない。

【００６８】

図1に示されたネットワークアーキテクチャで、ユーザー機器はN1インターフェイスを通じてAMFに接続され、（R）ANはN2インターフェイスを通じてAMFに接続され、（R）ANはN3インターフェイスを通じてUPFに接続され、UPFはN9インターフェイスを通じて互いに接続され、UPFはN6インターフェイスを通じてDNに接続され、SMFはN4インターフェイスを通じてUPFを制御し、AMFはN11インターフェイスを通じてSMFに接続され、AMFはUDMユニットからN8インターフェイスを通じてユーザー機器のサブスクリプションデータを取得し、SMFはUDMユニットからN10インターフェイスを通じてユーザー機器のサブスクリプションデータを取得する。

【００６９】

本出願の実施形態に適用される前述のネットワークアーキテクチャが説明のための一例にすぎず、本出願の実施形態に適用可能なネットワークアーキテクチャがそれに限定されないことを理解されたい。前述したネットワーク要素の機能を実行できるネットワークアーキテクチャはいずれも、本出願の実施形態に適用可能である。

【００７０】

例えば、いくつかのネットワークアーキテクチャにおいて、AMF、SMFネットワーク要素、PCFネットワーク要素、BSFネットワーク要素、およびUDMネットワーク要素などのネットワーク機能ネットワーク要素エンティティはいずれも、ネットワーク機能（network function、NF）ネットワーク要素と呼ばれる。あるいは、いくつかの他のネットワークアーキテクチャにおいて、AMF、SMFネットワーク要素、PCFネットワーク要素、BSFネットワーク要素、およびUDMネットワーク要素などの1セットのネットワーク要素は、制御プレーン機能ネットワーク要素と呼ばれることがある。

【００７１】

本出願の実施形態の技術的解決策は、グローバル・システム・フォー・モバイル・コミュニケーションズ（global system for mobile communications、GSM）システム、符号分割多元接続（code division multiple access、CDMA）システム、広帯域符号分割多元接続（wideband code division multiple access、WCDMA（登録商標））システム、汎用パケット無線サービス（general packet radio service、GPRS）システム、ロングタームエボリューション（long term evolution、LTE）システム、LTE周波数分割二重（frequency division duplex、FDD）システム、LTE時分割二重（time division duplex、TDD）、ユニバーサル・モバイル・テレコミュニケーションズ・システム（universal mobile telecommunication system、UMTS）、ワールドワイド・インターオペラビリティ・フォー・マイクロウェーブ・アクセス（worldwide interoperability for microwave access、WiMAX）通信システム、将来の第5世代（5th generation、5G）システム、または新無線（new radio、NR）システムなどの様々な通信システムに適用され得る。

【００７２】

本出願の実施形態におけるユーザー機器は、ユーザー機器、アクセス端末、加入者ユニット、加入者ステーション、モバイルステーション、モバイルコンソール、リモートステーション、リモート端末、モバイルデバイス、ユーザー端末、端末、無線通信デバイス、ユーザーエージェント、ユーザー装置などと呼ばれることがある。ユーザーデバイスは、携帯電話機、コードレス電話機、セッション開始プロトコル（session initiation protocol、SIP）電話機、ワイヤレスローカルループ（wireless local loop、WLL）ステーション、パーソナルデジタルアシスタント（personal digital assistant、PDA）、無線通信機能を有する手持ち型デバイス、計算デバイス、無線モデムに接続された他の処理デバ

イス、車載デバイス、ウェアラブルデバイス、将来の5Gネットワークにおけるユーザー機器、または将来の発展型公衆陸上移動ネットワーク（public land mobile network、PLMN）におけるユーザー機器であってよい。これは本出願の実施形態で限定されない。

【００７３】

本出願の実施形態におけるネットワークデバイスは、ユーザー機器と通信するように構成されたデバイスであってよい。ネットワークデバイスは、グローバル・システム・フォー・モバイル・コミュニケーションズ（global system for mobile communications、GSM）システムもしくは符号分割多元接続（code division multiple access、CDMA）システムにおけるベーストランシーバステーション（base t（R）ANsceiver station、BTS）であってよく、あるいは広帯域符号分割多元接続（wideband code division multiple access、WCDMA（登録商標））システムにおけるノードB（NodeB、NB）であってよく、あるいはLTEシステムにおけるエボルブドNodeB（evolved NodeB、eNB、またはeNodeB）であってよく、あるいはクラウド無線アクセスネットワーク（cloud radio access network、C（R）AN）シナリオにおける無線コントローラであってよい。代わりに、ネットワークデバイスは、中継局、アクセスポイント、車載デバイス、ウェアラブルデバイス、将来の5Gネットワークにおけるネットワークデバイス、または将来のエボルブドPLMNネットワークにおけるネットワークデバイスなどであってもよい。これは本出願の実施形態で限定されない。

【００７４】

本出願の実施形態において、ユーザー機器またはネットワークデバイスは、ハードウェア層、ハードウェア層上で実行するオペレーティングシステム層、およびオペレーティングシステム層上で実行するアプリケーション層を含む。ハードウェア層は、中央処理装置（central processing unit、CPU）、メモリー管理装置（memory management unit、MMU）、およびメモリー（メインメモリーとも呼ばれる）などのハードウェアを含む。オペレーティングシステムは、プロセス（process）を通じてサービスを処理する任意の1つ以上のコンピュータオペレーティングシステムであってよく、例えば、Linux（登録商標）オペレーティングシステム、Unixオペレーティングシステム、Androidオペレーティングシステム、iOSオペレーティングシステム、またはwindowsオペレーティングシステムであってよい。アプリケーション層は、ブラウザ、連絡先、ワープロソフトウェア、およびインスタントメッセージングソフトウェアなどのアプリケーションを含む。加えて、本出願の実施形態で提供される方法の実行体の具体的な構造は、本出願の実施形態で提供される方法のコードを記録するプログラムが、本出願の実施形態で提供される方法に従って通信を行うために実行されることができる限りにおいて、本出願の実施形態では特に限定されない。例えば、本出願の実施形態で提供される方法の実行体は、ユーザー機器もしくはネットワークデバイスであってよく、またはユーザー機器もしくはネットワークデバイス内にあって、プログラムを呼び出して実行することができる機能モジュールであってよい。

【００７５】

加えて、本出願の態様または機能は、方法、装置、または標準的なプログラミング技術および／またはエンジニアリング技術を使用する製品として実施されてよい。本出願で使用される「製品」という用語は、何らかのコンピュータ可読コンポーネント、キャリア、または媒体からアクセスされ得るコンピュータプログラムを含む。例えば、コンピュータ可読媒体は、磁気式ストレージコンポーネント（例えば、ハードディスク、フロッピーディスク、または磁気テープ）、光ディスク（例えば、コンパクトディスク（compact disc、CD）、デジタル多用途ディスク（digital versatile disc、DVD）、スマートカード、およびフラッシュメモリーコンポーネント（例えば、消去可能プログラム可能読み取り専用メモリー（erasable programmable read-only memory、EPROM）、カード、スティック、またはキードライブ）を含み得、ただしこれらに限定されない。加えて、本明細書に記載されている様々な記憶媒体は、情報を記憶するように構成された1つ以上のデバイスおよび／または他の機械可読媒体を指す場合がある。「機械可読媒体」という用語

は、無線チャネル、ならびに命令および／またはデータを記憶する、含む、および／または搬送することができる他の様々な媒体を含み得、ただしこれらに限定されない。

【００７６】

本出願の実施形態には主に、図1に示されたネットワークアーキテクチャの中のAMFとUEと（R）ANが関わる。本出願におけるAMFは、第1のAMF（ソースAMF（source AMF）とも呼ばれる）と第2のAMF（ターゲットAMF（target AMF）とも呼ばれる）とを含む。本出願における（R）ANネットワーク要素は、第1の（R）AN（ソース（R）AN（source（R）AN）とも呼ばれる）ネットワーク要素と第2の（R）AN（ターゲット（R）AN（target（R）AN）とも呼ばれる）ネットワーク要素とを含む。

【００７７】

具体的に述べると、本出願における第1のAMFは、ハンドオーバーの前にUEのためにコアネットワークサービスを提供するAMFである。本出願における第2のAMFは、ハンドオーバーの後にUEのためにコアネットワークサービスを提供するために選択されるAMFである。本出願における第1の（R）ANネットワーク要素は、第1のAMFからのハンドオーバーの前にUEのためにアクセスネットワークサービスを提供する（R）ANネットワーク要素である。本出願における第2の（R）ANネットワーク要素は、第2のAMFへのハンドオーバーの後にUEのためにアクセスネットワークサービスを提供するために選択される（R）ANネットワーク要素である。さらに、本出願にはAUSF／UDMが関わることがあり、AUSF／UDMは主に、認証を行うように、例えば、UEとネットワークデバイスとの間で認証を実施するように、構成される。本出願では主にハンドオーバー手順が論述され、認証手順が本出願で限定されず、UEとネットワークデバイスとの認証を以下で説明しないことを理解されたい。

【００７８】

具体的に述べると、本出願の実施形態では、説明を容易にするため、第1の（R）ANネットワーク要素が略して第1の（R）ANと呼ばれることがあり、第2の（R）ANネットワーク要素が略して第2の（R）ANと呼ばれることがある。本出願の実施形態におけるハンドオーバーとは、UEのためにアクセスネットワークサービスを提供する（R）ANネットワーク要素が第1の（R）ANから第2の（R）ANに変わることを意味する。第1の（R）ANは、シグナリング交換のために第2の（R）ANに至る接続を直接的に確立することはできない。第1の（R）ANが第1のAMFによって管理され、第2の（R）ANが第2のAMFによって管理される場合は、UEのためにアクセスネットワークサービスを提供する（R）ANネットワーク要素が第1の（R）ANから第2の（R）ANに変わる過程で、第1のAMFと第2のAMFを通じて関連するシグナリングが転送される必要がある。UEのためにアクセスネットワークサービスを提供する（R）ANネットワーク要素が第1の（R）ANから第2の（R）ANに変わりそこなう場合は、通常は第1の（R）ANがUEのためにアクセスネットワークサービスを提供し続ける。本出願において、UEのためにアクセスネットワークサービスを提供する（R）ANネットワーク要素が第1の（R）ANから第2の（R）ANに変わることは、略してハンドオーバーと呼ばれ、UEのためにアクセスネットワークサービスを提供する（R）ANネットワーク要素が第1の（R）ANから第2の（R）ANに変わりそこなうことは、略してハンドオーバー失敗と呼ばれる。

【００７９】

さらに、ハンドオーバーの前、UEとネットワークデバイスとの認証が完了した後に、UEと第1のAMFは同じAMF鍵を取得する。本出願の実施形態では、説明を容易にするため、UEと第1のAMFによって得られるAMF鍵がKamfと表記され、Kamfは第1のAMF鍵またはKamf 1と呼ばれることもある。その後、UEと第1のAMFは、Kamfと、UEと第1のAMFとの間で取り決められる非アクセス層（non-access stratum、NAS）完全性保護アルゴリズムとに基づいて、NASメッセージ保護に使用される完全性保護鍵を各々生成し、UEと第1のAMFは、Kamfと、UEと第1のAMFとの間で取り決められる非アクセス層（non-access stratum、NAS）機密性保護アルゴリズムとに基づいて、NASメッセージ保護に使用される機密性保護鍵を各々生成し、NASメッセージ保護に使用される完全性保護鍵とNAS

メッセージ保護に使用される機密性保護鍵は、NAS Keyと総称されることがある。本出願の実施形態では、説明を容易にするため、UEと第1のAMFによって生成されてNASメッセージ保護に使用される完全性保護鍵はKnasintと総称され、UEと第1のAMFによって生成されてNASメッセージ保護に使用される機密性保護鍵はKnasencと総称され、Kamfと、UEと第1のAMFとの間で取り決められるNAS完全性保護アルゴリズムとに基づいて、UEと第1のAMFによって生成されて、NASメッセージ保護に使用される、完全性保護鍵と、Kamfと、UEと第1のAMFとの間で取り決められるNAS機密性保護アルゴリズムとに基づいて、UEと第1のAMFによって生成されて、NASメッセージ保護に使用される、機密性保護鍵は、第1のNAS Keyと総称されることがあり、UEと第1のAMFとの間で取り決められるNAS完全性保護アルゴリズムとNAS機密性保護アルゴリズムは、第1のNASセキュリティアルゴリズムと総称されることがある。

【００８０】

NAS完全性保護アルゴリズムとNAS機密性保護アルゴリズムを取り決めるためにUEと第1のAMFによって使用される方式が本出願で限定されず、既存のプロトコルで指定されているネゴシエーション解決策が使用されてよいことを理解されたい。

【００８１】

ハンドオーバーのときにサービスの継続を確実なものにするため、ハンドオーバーが発生するときに、第1のAMFは、第1のAMFとUEとの間で使用されるUEセキュリティコンテキストを第2のAMFへ転送する。UEセキュリティコンテキストは、Kamf、またはKamfに対して鍵導出が行われた後に得られるKamf’（Kamf 2または第2のAMF鍵と呼ばれることもある）、第1のAMFとUEとの間で取り決められる第1のNASセキュリティアルゴリズム、ダウンリンク非アクセス層カウント（downlink non-access stratum count、DL NAS COUNT）、UEによってサポートされるNASセキュリティアルゴリズムリストなどを含む。第1のAMFとUEとの間で使用されるUEセキュリティコンテキストを第1のAMFによって第2のAMFへ転送することが、既存のプロトコルのハンドオーバー手順で規定されているステップであることを理解されたい。本出願ではこのステップに改良が行われない。換言すると、第1のAMFによってUEセキュリティコンテキストを第2のAMFへ送信するステップに含まれる内容については、既存のプロトコルで規定されている内容を参照するべきであり、ここでは簡単な説明だけが提供される。

【００８２】

第2のAMFは、第1のAMFによって転送されるUEセキュリティコンテキストに含まれているAMF鍵と、第2のAMFとUEとの間で取り決められる第2のNASセキュリティアルゴリズムとに基づいて、第3のNASセキュリティコンテキストを生成する。第3のNASセキュリティコンテキストは、Kamf2、Knasint2、Knasenc2、DL NAS COUNT2などを含む。具体的に述べると、第2のAMFがUEと第2のNASセキュリティアルゴリズムを取り決めることは、第2のAMFが、UEによってサポートされ、第1のAMFから受信されるUEセキュリティコンテキストに含まれている、NASセキュリティアルゴリズムリストから、第2のNASセキュリティアルゴリズムを選択し、選択された第2のNASセキュリティアルゴリズムと、受信されたUEセキュリティコンテキストに含まれている鍵KamfまたはKamf’とに基づいて、新しいNASセキュリティコンテキストを生成することを含む。別段の指定がない限り、本出願における第2のNASセキュリティアルゴリズムは第1のNASセキュリティアルゴリズムと異なる。

【００８３】

第1のNASセキュリティアルゴリズムと同様に、第2のNASセキュリティアルゴリズムが、第2のNAS完全性保護アルゴリズムと第2のNAS機密性保護アルゴリズムとを含むことを理解されたい。NAS完全性保護アルゴリズムは、第2の完全性保護鍵を生成するために使用され、NAS機密性保護アルゴリズムは、第2の機密性保護鍵を生成するために使用される。

【００８４】

具体的に述べると、第1のAMFによって第2のAMFへ送信されるUEセキュリティコンテ

キストが以下の2つの可能な形式を含むことは、上記の説明から分かる。

【００８５】

形式1：第1のAMFはKamfに対して導出を行わない。UEセキュリティコンテキストは、Kamf、DL NAS COUNT、第1のAMFとUEとの間で取り決められる第1のNASセキュリティアルゴリズム、およびUEによってサポートされるNASセキュリティアルゴリズムリストを含む。

【００８６】

形式2：第1のAMFはKamfに対して鍵導出を行って第2のAMF鍵Kamf’を生成する。UEセキュリティコンテキストは、Kamf’、DL NAS COUNT、第1のAMFとUEとの間で取り決められる第1のNASセキュリティアルゴリズム、UEによってサポートされるNASセキュリティアルゴリズムリスト、および導出指示情報を含む。導出指示情報は、第1のAMFがAMF鍵に対して水平導出を行うことを指示するために使用される。

【００８７】

形式2では、第1のAMFが第1のAMFとUEとの間で使用されるセキュリティコンテキストを第2のAMFへ転送する前に、第1のAMFが第1のAMFのローカルポリシーに従ってKamfに対して鍵導出を行い、鍵導出後に鍵Kamf’を生成する。本出願の実施形態では、第2の鍵を生成するために鍵に対して鍵導出を行うために使用される鍵導出機構およびパラメータは限定されず、導出が行われる鍵が、生成された第2の鍵に対して鍵導出を行うことによって得られないということだけが限定されることを理解されたい。換言すると、第2の鍵は導出が行われる鍵から分離される。

【００８８】

可能な一実装において、本出願における鍵導出は、既存のプロトコルで規定されている水平鍵導出であってよい。

【００８９】

例えば、Kamf’を生成するためにKamfに対して水平鍵導出を行う方式は以下の通りである。

【００９０】

【数１】

$$
\begin{aligned}
&Kamf' = HMAC\text{-}SHA\text{-}256\ (Key, S);\\
&FC = 0x72;\\
&P0 = 0x01;\\
&L0 = length\ of\ P0\ (i.e.\ 0x00\ 0x01);\\
&P1 = DL\ NAS\ count;\\
&L1 = length\ of\ P1\ (i.e.\ 0x00\ 0x04);\\
&KEY = Kamf;\\
&S = FC||P0||L0||P1||L1.
\end{aligned}
$$

【００９１】

別の可能な一実装において、本出願における鍵導出は、各種ネットワーク要素間で合意される鍵導出方式であってよい。例えば、第1のAMFと第2のAMFは既定の鍵導出方式について合意する。第1のAMFによって第2のAMFへ送信されるUEセキュリティコンテキストが導出指示情報を含むなら、第2のAMFは、受信されたUEセキュリティコンテキスト内の鍵が、既定の鍵導出方式で鍵導出を行うことによって第1のAMFによって得られると判断できる。

【００９２】
具体的に述べると、第1のAMFによって転送されるUEセキュリティコンテキストと、第2のAMFとUEとの間で取り決められる第2のNASセキュリティアルゴリズムとに基づいて、第2のAMFによって生成される新しいNASセキュリティコンテキストが、以下の2つの可能な形式を含むことは、上記の説明から分かる。
【００９３】
形式1：この形式は、第1のAMFがKamfに対して導出を行わない前述の形式1に対応する。新しいNASセキュリティコンテキストは、Kamf2、Knasint2、Knasenc2、およびDL NAS COUNT2を含み、Kamf2はKamfである。
【００９４】
可能な一実装において、第2のAMFとUEとの間で取り決められるNAS完全性保護アルゴリズムおよびNAS機密性保護アルゴリズムが、第1のAMFとUEとの間で取り決められるNAS完全性保護アルゴリズムおよびNAS機密性保護アルゴリズムと同じである場合は、第2のAMFは、Kamfと、UEと第2のAMFとの間で取り決められるNAS完全性保護アルゴリズムおよびNAS機密性保護アルゴリズムとに基づいて、NASメッセージ保護に使用される完全性保護鍵Knasint2と、NASメッセージ保護に使用される機密性保護鍵Knasenc2とを生成し、Knasint2およびKnasenc2は前述のKnasintおよびKnasencである。
【００９５】
別の可能な一実装において、第2のAMFとUEとの間で取り決められるNAS完全性保護アルゴリズムおよびNAS機密性保護アルゴリズムが、第1のAMFとUEとの間で取り決められるNAS完全性保護アルゴリズムおよびNAS機密性保護アルゴリズムと異なる場合は、第2のAMFは、Kamfと、UEと第2のAMFとの間で取り決められるNAS完全性保護アルゴリズムおよびNAS機密性保護アルゴリズムとに基づいて、NASメッセージ保護に使用される完全性保護鍵Knasint2と、NASメッセージ保護に使用される機密性保護鍵Knasenc2とを生成し、Knasint2およびKnasenc2は前述のKnasintおよびKnasencと異なる。
【００９６】
形式2：この形式は、第1のAMFがKamfに対して導出を行う前述の形式2に対応する。新しいNASセキュリティコンテキストは、Kamf’、Knasint2、Knasenc2、DL NASカウント、および導出指示情報を含む。導出指示情報は、Kamf’が導出されたAMF鍵であることを指示するために使用される。
【００９７】
Knasint2とKnasenc2はそれぞれ、Kamf’と、UEと第2のAMFとの間で取り決められるNAS完全性保護アルゴリズムおよびNAS機密性保護アルゴリズムとに基づいて第2のAMFによって生成される、NASメッセージ保護に使用される完全性保護鍵と、NASメッセージ保護に使用される機密性保護鍵である。
【００９８】
形式2では、第2のAMFが導出指示情報を受信し、導出指示情報をUEへさらに送信する。導出指示情報は、Kamfに対して導出を行うことをUEに指示するために使用され、その結果、UE側のKamf’はネットワーク側のものと同じになる。
【００９９】
第2のAMFが、第1のAMFによって送信されるKamfまたはKamf’を受信した後に、第2のAMFによって選択されるNASセキュリティアルゴリズム（完全性保護アルゴリズムと機密性保護アルゴリズムとを含む）と、受信されたKamfまたはKamf’とに基づいて、かつ第2のAMFとUEとの間のアルゴリズムネゴシエーションと組み合わせて、第2のAMFとUEとの間で使用されるNAS鍵（Knasenc2とKnasint）を生成することを理解されたい。UE側も同じ計算を行う。最後に、UE側のAMF鍵とNAS鍵は、第2のAMF側のものと同じになる。
【０１００】
ハンドオーバーが失敗したときに、UE上のAMF鍵およびNAS鍵が第2のAMF上のものと同じであることを保証することはできるが、ハンドオーバーが失敗したときに、UE上のN

AS鍵が第1のAMF上のものと同じであることを保証することはできない。以下、ハンドオーバー失敗プロセスにおいて第1のAMFがKamfに対して導出を行うとき、ならびに第1のAMFによってサポートされるNASセキュリティアルゴリズムが第2のAMFによってサポートされるNASセキュリティアルゴリズムと異なるときに、UE上のAMF鍵およびNAS鍵が第1のAMF上のものと異なる場合と、ハンドオーバー失敗プロセスにおいて第1のAMFがKamfに対して導出を行わないとき、ならびに第1のAMFによってサポートされるNASセキュリティアルゴリズムが第2のAMFによってサポートされるNASセキュリティアルゴリズムと異なるときに、UE上のAMF鍵およびNAS鍵が第1のAMF上のものと異なる場合とを、図2および図3を参照しながら別々に手短に説明する。

【０１０１】

図2は、ハンドオーバー失敗手順の概略図である。UE、第1のAMF、第2のAMF、第1の（R）AN、第2の（R）AN、およびS1～S11が含まれている。以下、図2に示された方法手順を詳しく説明する。

【０１０２】

ハンドオーバーが発生する前に、UEおよび第1のAMF上のAMF鍵およびNAS鍵はKamf、Knasenc、およびKnasintであり、DL NAS COUNT＝Xである。

【０１０３】

S1：第1の（R）ANは第1のAMFへハンドオーバー要求メッセージを送信する。

【０１０４】

ハンドオーバー要求メッセージは、アクセスネットワークデバイスハンドオーバーが必要であることを指示するために使用される。ハンドオーバー要求メッセージはhandover requiredと呼ばれることがある。本出願で、第1の（R）ANによって第1のAMFへ送信されるハンドオーバー要求メッセージに改良が行われないことを理解されたい。詳細については、既存のプロトコルで規定されているハンドオーバー要求メッセージを参照されたい。

【０１０５】

S2：第1のAMFは鍵導出を行う。

【０１０６】

図2に示されたハンドオーバー失敗手順において、第1のAMFは、第1の（R）ANによって送信されるハンドオーバー要求メッセージを受信した後に、アクセスネットワークデバイスハンドオーバーが必要であると判断する。第1のAMFは、第2のAMF鍵Kamf’を取得するために、ローカルの第1のAMF鍵Kamfに対して鍵導出を行う。

【０１０７】

第1のAMFがS2を実行した後に、第1のAMF上のAMF鍵およびNAS鍵が、Kamf’、Knasenc、およびKnasintであることを理解されたい。

【０１０８】

S3：第1のAMFは第2のAMFへUEセキュリティコンテキストを送信する。

【０１０９】

UEセキュリティコンテキストは、Kamf’、Knasenc、Knasint、およびDL NAS COUNT（DL NAS COUNT＝X＋1）を含む。第1のAMFによって第2のAMFへUEセキュリティコンテキストを送信するステップは、第1のAMFによって、第2のAMFに対してUEコンテキスト作成サービス要求を開始するステップであってもよく、UEコンテキスト作成サービス要求はcreate UE context requestと呼ばれることがある。本出願で、第1のAMFによって第2のAMFへUEセキュリティコンテキストを送信するステップに改良が行われないことを理解されたい。詳細については、既存のプロトコルで規定されている、第1のAMFによって第2のAMFへUEセキュリティコンテキストを送信するステップを参照されたい。

【０１１０】

S4：第2のAMFは新しいNASセキュリティコンテキストを生成する。

【０１１１】

新しいNASセキュリティコンテキストは、第2のAMFによって受信されるKamf’と、第2のAMFとUEとの間で取り決められる第2のNASセキュリティアルゴリズムに基づいて第2

のAMFによって生成され、第2のAMFとUEとの間で使用される、NAS鍵（Knasenc2とKnasint2）と、DL NAS COUNT（DL NAS COUNT＝0）とを含み、Knasenc2およびKnasint2はKnasencおよびKnasintと異なる。

【０１１２】

S5：第2のAMFは第2の（R）ANへハンドオーバー要求を送信する。

【０１１３】

ハンドオーバー要求は、第2の（R）ANの関連情報を取得するために使用される。ハンドオーバー要求はhandover requestと呼ばれることがある。本出願で、第2のAMFによって第2の（R）ANへハンドオーバー要求を送信するステップに改良が行われないことを理解されたい。詳細については、既存のプロトコルで規定されている、第2のAMFによって第2の（R）ANへハンドオーバー要求を送信するステップを参照されたい。

【０１１４】

S6：第2の（R）ANは第2のAMFへハンドオーバー要求応答を送信する。

【０１１５】

ハンドオーバー要求応答は、第2の（R）ANの関連情報を第2のAMFに通知するために使用される。ハンドオーバー要求応答はhandover request acknowledgeと呼ばれることがある。本出願で、第2の（R）ANによって第2のAMFへハンドオーバー要求応答を送信するステップに改良が行われないことを理解されたい。詳細については、既存のプロトコルで規定されている、第2の（R）ANによって第2のAMFへハンドオーバー要求応答を送信するステップを参照されたい。

【０１１６】

S7：第2のAMFは第1のAMFへUEコンテキスト作成サービス要求応答を送信する。

【０１１７】

UEコンテキスト作成サービス要求応答は、第2の（R）ANの関連情報を第1のAMFに通知するために使用される。UEコンテキスト作成サービス要求応答は、create UE context responseと呼ばれることがある。本出願で、第2のAMFによって第1のAMFへUEコンテキスト作成サービス要求応答を送信するステップに改良が行われないことを理解されたい。詳細については、既存のプロトコルで規定されている、第2のAMFによって第1のAMFへUEコンテキスト作成サービス要求応答を送信するステップを参照されたい。

【０１１８】

S8：第1のAMFは第1の（R）ANへハンドオーバーコマンドメッセージを送信する。

【０１１９】

ハンドオーバーコマンドメッセージは、第2の（R）ANの関連情報を第1の（R）ANに通知するために使用される。ハンドオーバーコマンドメッセージはhandover commandと呼ばれることがある。本出願で、第1のAMFによって第1の（R）ANへハンドオーバーコマンドメッセージを送信するステップに改良が行われないことを理解されたい。詳細については、既存のプロトコルで規定されている、第1のAMFによって第1の（R）ANへハンドオーバーコマンドメッセージを送信するステップを参照されたい。

【０１２０】

S9：第1の（R）ANはUEへハンドオーバーコマンドメッセージを送信する。

【０１２１】

ハンドオーバーコマンドメッセージは、第2の（R）ANの関連情報をUEに通知するために使用される。ハンドオーバーコマンドメッセージはhandover commandと呼ばれることがある。本出願で、第1の（R）ANによってUEへハンドオーバーコマンドメッセージを送信するステップに改良が行われないことを理解されたい。詳細については、既存のプロトコルで規定されている、第1の（R）ANによってUEへハンドオーバーコマンドメッセージを送信するステップを参照されたい。

【０１２２】

S10：UEは新しいNASセキュリティコンテキストを生成する。

【０１２３】

新しいNASセキュリティコンテキストは、Kamf’と、第2のAMFとUEとの間で取り決められる第2のNASセキュリティアルゴリズムに基づいてUEによって生成され、第2のAMFとUEとの間で使用される、NAS鍵（Knasenc2とKnasint2）と、DL NAS COUNT（DL NAS COUNT＝0）とを含む。

【０１２４】

UEがS10を実行した後に、UE上のAMF鍵およびNAS鍵は、Kamf’、Knasenc2、およびKnasint2である。

【０１２５】

UEが何らかの理由で（例えば、第2の（R）ANの信号が劣化したため、または受信されたNASCに対してUEによって行われる完全性チェックが失敗したため）ハンドオーバーに失敗する場合は、S11が発生する、すなわち、ハンドオーバーが失敗する。この場合、UEは引き続き第1のAMFによってサービスされる。しかし、ハンドオーバー中に第1のAMFがKamfに対して導出を行うときに、UE上のNAS Keyは第1のAMF上のNAS Keyと異なるため、UEと第1のAMFは後ほどNASメッセージセキュリティ保護を行うことができない。

【０１２６】

図3は、別のハンドオーバー失敗手順の概略図である。UE、第1のAMF、第2のAMF、第1の（R）AN、第2の（R）AN、およびS20～S29が含まれている。以下、図3に示されている方法手順を詳しく説明する。

【０１２７】

ハンドオーバーが発生する前に、UEおよび第1のAMF上のAMF鍵およびNAS鍵はKamf、Knasenc、およびKnasintであり、DL NAS COUNT＝Xである。

【０１２８】

S20：第1の（R）ANは第1のAMFへハンドオーバー要求メッセージを送信する。

【０１２９】

ハンドオーバー要求メッセージは、ハンドオーバーが必要であることを指示するために使用される。このステップは、図2に示されている、第1の（R）ANによって第1のAMFへハンドオーバー要求メッセージを送信するステップと同様である。したがって、ここでは詳細を再度説明しない。

【０１３０】

S21：第1のAMFは第2のAMFへUEセキュリティコンテキストを送信する。

【０１３１】

UEセキュリティコンテキストは、Kamf、Knasenc、Knasint、およびDL NAS COUNT（DL NAS COUNT＝X＋1）を含む。

【０１３２】

S22：第2のAMFは新しいNASセキュリティコンテキストを決定する。

【０１３３】

新しいNASセキュリティコンテキストは、第2のAMFによって受信されるKamfと、第2のAMFとUEとの間で取り決められる第2のNASセキュリティアルゴリズムに基づいて第2のAMFによって生成され、第2のAMFとUEとの間で使用される、NAS Key（Knasenc2とKnasint2）と、DL NAS COUNT（DL NAS COUNT＝X＋1）とを含み、Knasenc2およびKnasint2はKnasencおよびKnasintと異なる。

【０１３４】

S23：第2のAMFは第2の（R）ANへハンドオーバー要求を送信する。

【０１３５】

ハンドオーバー要求は、第2の（R）ANの関連情報を取得するために使用される。

【０１３６】

S24：第2の（R）ANは第2のAMFへハンドオーバー要求応答を送信する。

【０１３７】

ハンドオーバー要求応答は、第2の（R）ANの関連情報を第2のAMFに通知するために使用される。

【０１３８】
S25：第2のAMFは第1のAMFへUEコンテキスト作成サービス要求応答を送信する。
【０１３９】
UEコンテキスト作成サービス要求応答は、第2の（R）ANの関連情報を第1のAMFに通知するために使用される。
【０１４０】
S26：第1のAMFは第1の（R）ANへハンドオーバーコマンドメッセージを送信する。
【０１４１】
ハンドオーバーコマンドメッセージは、第2の（R）ANの関連情報を第1の（R）ANに通知するために使用される。
【０１４２】
S27：第1の（R）ANはUEへハンドオーバーコマンドメッセージを送信する。
【０１４３】
ハンドオーバーコマンドメッセージは、第2の（R）ANの関連情報をUEに通知するために使用される。
【０１４４】
S28：UEは新しいNASセキュリティコンテキストを生成する。
【０１４５】
新しいNASセキュリティコンテキストは、Kamfと、第2のAMFとUEとの間で取り決められる第2のNASセキュリティアルゴリズムに基づいてUEによって生成され、第2のAMFとUEとの間で使用される、NAS Key（Knasenc2とKnasint2）と、DL NAS COUNT（DL NAS COUNT＝X＋1）とを含む。
【０１４６】
UEがS28を実行した後、UE上のAMF鍵およびNAS Keyは、Kamf、Knasenc2、およびKnasint2である。
【０１４７】
UEが何らかの理由で（例えば、第2の（R）ANの信号が劣化したため）ハンドオーバーに失敗した場合は、S29が発生する、すなわち、ハンドオーバーが失敗する。この場合、UEは引き続き第1のAMFによってサービスされる。しかし、第2の（R）ANがハンドオーバー中に前述の第1のNASセキュリティアルゴリズムとは異なる第2のNASセキュリティアルゴリズムを選択する場合は、Kamfと第2のNASセキュリティアルゴリズムとに基づいてUEによって生成されるKnasenc2およびKnasint2は、KnasencおよびKnasintと異なる。この場合、UE上のNAS Keyは第1のAMF上のNAS Keyと異なるため、UEと第1のAMFは後ほどNASメッセージセキュリティ保護を行うことができない。
【０１４８】
図2および図3に示された方法手順において、UE上のNAS Keyが第1のAMF上のNAS Keyと異なる事態を回避するため、本出願は、UEによって使用されるNASセキュリティコンテキストが第1のAMFによって使用されるNASセキュリティコンテキストと確実に同じになるようにして、UE上のNAS Keyが第1のAMF上のNAS Keyと同じになるようにする、ハンドオーバー処理方法を提案する。以下、図4および図5を参照しながら、本出願の実施形態で提供されるハンドオーバー処理方法を詳しく説明する。
【０１４９】
図4は、本出願の一実施形態によるハンドオーバー処理方法の概略フローチャートである。概略フローチャートは、UE、第1のAMF、第2のAMF、第1の（R）AN、第2の（R）AN、およびS110～S140を含む。以下、図4に示された方法手順を詳しく説明する。
【０１５０】
ハンドオーバーの前に、UE上のNASセキュリティコンテキストと第1のAMF上のNASセキュリティコンテキストは、Kamf（第1のAMF鍵Kamf1）、Knasenc、Knasint（KnasencとKnasintは第1の非アクセス層NAS鍵と総称される）、DL NAS COUNT（第1の非アクセス層カウントNASカウントであって、DL NAS COUNT＝X）、UEと第1のAMFと

の間で取り決められるNASセキュリティアルゴリズム（第1のNASセキュリティアルゴリズム）などをそれぞれ含む。図4に示されている実施形態では、ハンドオーバー前のUEおよび第1のAMF上のNASセキュリティコンテキストが、第1のNASセキュリティコンテキストと総称される。

【０１５１】

S110：第1のAMFは鍵導出が行われる必要があると判断し、第1のNASセキュリティコンテキストを記憶する。

【０１５２】

可能な一実装において、第1のAMFは、鍵導出を行う前に、第1のNASセキュリティコンテキストを記憶する。

【０１５３】

可能な一実装において、第1のAMFは、鍵導出を行った後に、第1のNASセキュリティコンテキストを記憶する。

【０１５４】

本出願で、第1のAMFによって鍵導出を行い、第1のAMFによって第1のNASセキュリティコンテキストを記憶する順序は厳密に限定されない。具体的に述べると、第1のAMFがS110を実行する前に、図4に示された実施形態は、S111を、すなわち、第1の（R）ANが第1のAMFへハンドオーバー要求メッセージを送信するステップを、さらに含む。図4に示された実施形態で、第1の（R）ANによって、第1のAMFへハンドオーバー要求メッセージを送信するステップは、図2のS1と同様である。したがって、ここでは詳細を再度説明しない。

【０１５５】

具体的に述べると、図4に示された実施形態で、第1のAMFが、ハンドオーバー要求メッセージを受信した後に、第1のNASセキュリティコンテキストを記憶することは、以下の2つの可能なケースを含む。

【０１５６】

可能なケース1では、第1のAMFが、第1のNASセキュリティコンテキストに含まれている鍵Kamfに対して鍵導出を行わない場合に、第1のNASセキュリティコンテキストを記憶することを決定する。これは、図2に示された既存の手順と一致する。

【０１５７】

可能なケース2では、第1のAMFが、ローカルポリシーに従って、第1のNASセキュリティコンテキストに含まれている鍵Kamfに対して鍵導出が実行される必要があると判断する。図4に示された実施形態は、S112を、すなわち、第1のAMFが鍵導出を行うステップを、さらに含む。

【０１５８】

具体的に述べると、第1のAMFは、第1のNASセキュリティコンテキストを記憶した後に、第2の鍵Kamf’を取得するために、第1の鍵Kamfに対して鍵導出を行う。第1のAMFによって鍵導出を行うプロセスが本出願の本実施形態で限定されず、既存のプロトコルで規定されている、第1のAMFによって鍵導出を行うプロセスであってもよいことを理解されたい。第1のAMFは鍵導出を行って導出されたKamf’を生成し、これは図4に示された実施形態で第1の鍵と呼ばれる。図4に示された実施形態では、手順が既存の手順と一致しない可能なケース2が主に説明され、手順が既存の手順と一致する可能なケース1は手短に説明される。

【０１５９】

S113：第1のAMFは第2のAMFへUEセキュリティコンテキストを送信する。

【０１６０】

具体的に述べると、第1のAMFによって第2のAMFへUEセキュリティコンテキストを送信するステップは、第1のAMFによって、第2のAMFに対してUEコンテキスト作成サービス要求を開始するステップであってもよい。S110の可能なケース1と可能なケース2とに基づいて、第1のAMFが第2のAMFへUEセキュリティコンテキストを送信することは、以

下の2つの可能なケースも含む。

【０１６１】

可能なケース1では、第1のAMFが第1のNASセキュリティコンテキストに含まれている第1の鍵Kamfに対して鍵導出を行わない場合に、第1のAMFによって第2のAMFへ送信されるUEセキュリティコンテキストは、Kamfと、DL NAS COUNT（DL NAS COUNT＝X＋1）と、UEと第1のAMFとの間で取り決められるNASセキュリティアルゴリズムと、UEによってサポートされるNASセキュリティアルゴリズムリストとを含む。

【０１６２】

可能なケース2では、第1のAMFが第1のNASセキュリティコンテキストに含まれている第1の鍵Kamfに対して鍵導出を行う場合に、第1のAMFによって第2のAMFへ送信されるUEセキュリティコンテキストは、Kamf’と、DL NAS COUNT（DL NAS COUNT＝X＋1）と、UEと第1のAMFとの間で取り決められるNASセキュリティアルゴリズムと、UEによってサポートされるNASセキュリティアルゴリズムリストと、鍵導出指示とを含む。鍵導出指示は、第1のAMFによって第2のAMFへ送信されるUEセキュリティコンテキスト内の鍵が、第1のAMFによる鍵導出によって得られることを指示するために使用される。鍵導出指示は、K_AMF_change_flagと呼ばれることがある。具体的に述べると、K_AMF_change_flagの値が1であるなら、これは、第1のAMFによって第2のAMFへ送信されるUEセキュリティコンテキスト内の鍵が、第1のAMFによる鍵導出によって得られることを意味する。

【０１６３】

図4に示された実施形態で、第2のAMFは、第1のAMFによって送信されたUEセキュリティコンテキストを受信した後に、S114を実行する、すなわち、第2のAMFは第3のNASセキュリティコンテキストを生成する。S113の可能なケース1と可能なケース2とに基づいて、第2のAMFが第3のNASセキュリティコンテキストを生成することは、以下の2つの可能なケースも含む。

【０１６４】

可能なケース1では、第1のAMFによって第2のAMFへ送信されるUEセキュリティコンテキストに含まれる鍵がKamfである。

【０１６５】

第2のAMFは、第1のAMFによって送信されるUEセキュリティコンテキスト内の鍵Kamfと、UEによってサポートされるNASセキュリティアルゴリズムリストから選択されるNASセキュリティアルゴリズムとに基づいて、NASメッセージ保護に使用される完全性保護鍵Knasint2と機密性保護鍵Knasenc2とを生成する。第2のAMFによって生成される第3のNASセキュリティコンテキストは、Kamfと、Knasint2と、Knasenc2と、DL NAS COUNT（DL NAS COUNT＝X＋1）と、UEと第2のAMFとの間で取り決められるNASセキュリティアルゴリズムとを含む。

【０１６６】

可能な一実装において、UEによってサポートされるNASセキュリティアルゴリズムリストから第2のAMFによって選択されるNASセキュリティアルゴリズムが、UEと第1のAMFとの間で取り決められるNASセキュリティアルゴリズムと同じであるなら、Knasint2およびKnasenc2は、KnasintおよびKnasencと同じである。この実装で、ハンドオーバーが失敗したときにUE上のAMF鍵およびNAS Keyが第1のAMF上のものと異なる事態は発生しない。

【０１６７】

別の可能な一実装において、UEによってサポートされるNASセキュリティアルゴリズムリストから第2のAMFによって選択されるNASセキュリティアルゴリズムが、UEと第1のAMFとの間で取り決められるNASセキュリティアルゴリズムと異なるなら、Knasint2およびKnasenc2は、KnasintおよびKnasencと異なる。この実装では、図3に示された、UE上のNAS鍵が第1のAMF上のNAS Keyと異なる事態が発生する。

【０１６８】

可能なケース2では、第1のAMFによって第2のAMFへ送信されるUEセキュリティコンテキストに含まれる鍵がKamf’である。

【０１６９】

第2のAMFは、第1のAMFによって送信されるUEセキュリティコンテキスト内の鍵Kamf’と、UEによってサポートされるNASセキュリティアルゴリズムリストから選択されるNASセキュリティアルゴリズムとに基づいて、NASメッセージ保護に使用される完全性保護鍵Knasint2と機密性保護鍵Knasenc2とを生成する。第2のAMFによって生成される第3のNASセキュリティコンテキストは、Kamf’、Knasint2、Knasenc2、DL NAS COUNT（DL NAS COUNT＝X＋1）またはDL NAS COUNT（DL NAS COUNT＝0）、UEと第2のAMFとの間で取り決められるNASセキュリティアルゴリズム、および鍵導出指示を含む。

【０１７０】

可能な一実装において、UEによってサポートされるNASセキュリティアルゴリズムリストから第2のAMFによって選択されるNASセキュリティアルゴリズムがUEと第1のAMFとの間で取り決められるNASセキュリティアルゴリズムと同じである場合は、鍵が異なるため、Knasint2およびKnasenc2はKnasintおよびKnasencと異なる。この実装では、図2に示された、UE上のAMF鍵およびNAS Keyが第1のAMF上のものと異なる事態が発生する。

【０１７１】

別の可能な一実装において、UEによってサポートされるNASセキュリティアルゴリズムリストから第2のAMFによって選択されるNASセキュリティアルゴリズムが、UEと第1のAMFとの間で取り決められるNASセキュリティアルゴリズムと異なる場合は、鍵とNASセキュリティアルゴリズムの両方が異なるため、Knasint2およびKnasenc2はKnasintおよびKnasencと異なる。この実装では、図2に示された、UE上のAMF鍵およびNAS Keyが第1のAMF上のものと異なる事態が発生する。

【０１７２】

さらに、第2のAMFは、第3のNASセキュリティコンテキストを生成した後に、第3のNASセキュリティコンテキストに基づいて非アクセス層コンテナNASC（non-access stratum container、NASC）を決定する。換言すると、図4に示された実施形態はS115をさらに含む、すなわち、第2のAMFはNASCを決定する。S114の可能なケース1と可能なケース2とに基づいて、第2のAMFがNASCを決定することは、以下の2つの可能なケースも含む。

【０１７３】

可能なケース1では、第3のNASセキュリティコンテキストは、Kamf’と、Knasint2と、Knasenc2と、DL NAS COUNT（DL NAS COUNT＝X＋1）と、UEと第2のAMFとの間で取り決められるNASセキュリティアルゴリズムとを含む。この場合、NASCは、COUNT（COUNT＝X＋1）と、UEと第2のAMFとの間で取り決められるNASセキュリティアルゴリズムとを含む。

【０１７４】

可能なケース2では、第3のNASセキュリティコンテキストは、Kamf’、Knasint2、Knasenc2、DL NAS COUNT（DL NAS COUNT＝X＋1）またはDL NAS COUNT（DL NAS COUNT＝0）、UEと第2のAMFとの間で取り決められるNASセキュリティアルゴリズム、および鍵導出指示を含む。この場合、NASCは、DL NAS COUNT（DL NAS COUNT＝X＋1）またはDL NAS COUNT（DL NAS COUNT＝0）、UEと第2のAMFとの間で取り決められるNASセキュリティアルゴリズム、および鍵導出指示を含む。

【０１７５】

第2のAMFがUEへNASCを送信する必要があることを理解されたい。具体的に述べると、NASCは、第2の（R）AN、第1のAMF、および第1の（R）ANによる転送によってUEへ送信される必要がある。UEへNASCを送信する方式は本出願の本実施形態で限定されない。詳細については、既存のプロトコルで規定されている方式を参照されたい。例えば、図

4に示された実施形態は以下のステップをさらに含む。

【０１７６】

S116：第2のAMFは第2の（R）ANへハンドオーバー要求を送信する。

【０１７７】

ハンドオーバー要求は、第2の（R）ANの関連情報を取得するために使用される。

【０１７８】

S117：第2の（R）ANは第2のAMFへハンドオーバー要求応答を送信する。

【０１７９】

ハンドオーバー要求応答は、第2の（R）ANの関連情報を第2のAMFに通知するために使用される。

【０１８０】

S118：第2のAMFは第1のAMFへUEコンテキスト作成サービス要求応答を送信する。

【０１８１】

UEコンテキスト作成サービス要求応答はNASCを搬送する。

【０１８２】

S119：第1のAMFは第1の（R）ANへハンドオーバーコマンドメッセージを送信する。

【０１８３】

ハンドオーバーコマンドメッセージはNASCを搬送する。

【０１８４】

S1191：第1の（R）ANはUEへハンドオーバーコマンドメッセージを送信する。

【０１８５】

ハンドオーバーコマンドメッセージはNASCを搬送する。

【０１８６】

任意に選べることとして、図4に示された実施形態はS120をさらに含む、すなわち、第1のAMFは第1のNASセキュリティコンテキストを使用することを再開する。

【０１８７】

可能な一実装において、第1のAMFは、S110に示されたハンドオーバー要求メッセージを受信した後に、S110の可能なケース2に基づいて、鍵導出を行う。第1のAMFは、水平方向に導出されたKamf’を含むUEコンテキストを第1のAMFが第2のAMFへ送信した後に、第2のKamf’を随時削除し、第1のNASセキュリティコンテキストを使用することを再開する。

【０１８８】

別の可能な一実装において、第1のAMFは、S110を実行した後に、すなわち、第1のNASセキュリティコンテキストを記憶し、第4のNASセキュリティコンテキストを生成するために鍵導出を行った後に、第4のNASセキュリティコンテキストから第1のNASセキュリティコンテキストを区別するためにフラグビットを設定する。換言すると、第1のAMFは、第2のAMFへUEコンテキストを送信する前に、または送信するときに、第1のNASセキュリティコンテキストを使用することを再開できる。

【０１８９】

S130：UEは第1のNASセキュリティコンテキストを記憶する。

【０１９０】

UEが第1の（R）ANによって送信されるハンドオーバーコマンドメッセージを受信してNASCを取得した後、UEは、NASCに対して完全性検証を行う。NASCに対して行われる完全性検証が成功した後に、UEと第2のAMFとの間で取り決められ、NASCに含まれる、NASセキュリティアルゴリズムが、UEと第1のAMFとの間で取り決められるNASセキュリティアルゴリズムと異なり、および／またはNASCが値1を有するK_AMF_change_flagを搬送する場合、UEは第1のNASセキュリティコンテキストを記憶する。K_AMF_change_flagは、AMF鍵変更指示または鍵導出指示と呼ばれることがある。

【０１９１】

UEは、第1のNASセキュリティコンテキストを記憶した後に、NASC内の情報に基づい

て第1のNASセキュリティコンテキストを更新することで第3のNASセキュリティコンテキストを取得する、すなわち、S131を実行する。

【０１９２】

S140：UEは第1のNASセキュリティコンテキストを使用することを再開する。

【０１９３】

UEがハンドオーバーが失敗したことを発見すると、UEは、S130で記憶された第1のNASセキュリティコンテキストを使用することを再開する。

【０１９４】

任意に選べることとして、UEは第3のNASセキュリティコンテキストを削除する。

【０１９５】

別の可能な一実装において、UEは、S130、S131、およびS140を実行しない。代わりに、UEはS132を実行する、すなわち、UEは第1のNASセキュリティコンテキストを使用し続ける。

【０１９６】

UEが第1の（R）ANによって送信されるハンドオーバーコマンドメッセージを受信してNASCを取得した後、UEは、NASCに対して完全性検証を行う。NASCに対して行われる完全性検証が失敗した後に、UEは、現在使用されている第1のNASセキュリティコンテキストを使用し続ける。

【０１９７】

本出願の本実施形態におけるNASセキュリティコンテキストは主に、鍵識別子ngKSI、AMF鍵、NAS Key、DL NAS count、UL NAS count、NASセキュリティアルゴリズムなどを含む。鍵識別子はAMF鍵を指示するために使用され、DL NAS countおよびUL NAS countはそれぞれ、ダウンリンクNASカウントおよびアップリンクNASカウントである。上述したNASセキュリティコンテキストに含まれる内容は手短に説明されているにすぎず、本出願の保護範囲を制限するものではない。

【０１９８】

要するに、図4に示された実施形態では、ハンドオーバーが失敗したときに、UEと第1のAMFの両方は、NASセキュリティ保護を行うために第1のNASセキュリティコンテキストを使用することを再開し、これにより、UEによって使用されるAMF鍵およびNAS鍵は、第1のAMFによって使用されるAMF鍵およびNAS鍵と同じになる。

【０１９９】

図5は、本出願の一実施形態による別のハンドオーバー処理方法の概略フローチャートである。概略フローチャートは、UE、第1のAMF、第2のAMF、第1の（R）AN、第2の（R）AN、およびS210～S240を含む。以下、図5に示された方法手順を詳しく説明する。

【０２００】

ハンドオーバーの前に、UE上のNASセキュリティコンテキストと第1のAMF上のNASセキュリティコンテキストは、Kamf、Knasenc、Knasint、DL NAS COUNT（DL NAS COUNT＝X）、UEと第1のAMFとの間で取り決められるNASセキュリティアルゴリズムなどをそれぞれ含む。図4に示されている実施形態では、ハンドオーバー前のUEおよび第1のAMF上のNASセキュリティコンテキストが、第1のNASセキュリティコンテキストと総称される。

【０２０１】

S211：第1の（R）ANは第1のAMFへハンドオーバー要求メッセージを送信する。

【０２０２】

図5に示された実施形態で、第1の（R）ANによって第1のAMFへハンドオーバー要求メッセージを送信するステップは、図2のS1と同様である。したがって、ここでは詳細を再度説明しない。

【０２０３】

S212：第1のAMFは第2のAMFへUEセキュリティコンテキストを送信する。

【０２０４】

具体的に述べると、第1のAMFによって第2のAMFへUEセキュリティコンテキストを送信するステップは、第1のAMFによって、第2のAMFに対してUEコンテキスト作成サービス要求を開始するステップであってもよい。以下の2つの可能なケースが含まれる。

【０２０５】

可能なケース1では、第1のAMFが第1のNASセキュリティコンテキストに含まれている鍵Kamfに対して鍵導出を行わない場合に、第1のAMFによって第2のAMFへ送信されるUEセキュリティコンテキストは、Kamfと、DL NAS COUNT（DL NAS COUNT＝X＋1）と、UEと第1のAMFとの間で取り決められるNASセキュリティアルゴリズムと、UEによってサポートされるNASセキュリティアルゴリズムリストとを含む。

【０２０６】

可能なケース2では、第1のAMFが第1のNASセキュリティコンテキストに含まれている鍵Kamfに対して鍵導出を行う場合に、第1のAMFによって第2のAMFへ送信されるUEセキュリティコンテキストは、Kamf’と、DL NAS COUNT（DL NAS COUNT＝X＋1）と、UEと第1のAMFとの間で取り決められるNASセキュリティアルゴリズムと、UEによってサポートされるNASセキュリティアルゴリズムリストと、鍵導出指示とを含む。鍵導出指示は、第1のAMFによって第2のAMFへ送信されるUEセキュリティコンテキスト内の鍵が、第1のAMFによる鍵導出によって得られることを指示するために使用される。鍵導出指示は、K_AMF_change_flagと呼ばれることがある。具体的に述べると、K_AMF_change_flagの値が1であるなら、これは、第1のAMFによって第2のAMFへ送信されるUEセキュリティコンテキスト内の鍵が、第1のAMFによる鍵導出によって得られることを意味する。

【０２０７】

図5に示された実施形態で、第2のAMFは、第1のAMFによって送信されるUEセキュリティコンテキストを受信した後に、S213を実行する、すなわち、第2のAMFは第3のNASセキュリティコンテキストを生成する。具体的に述べると、図5に示された実施形態で、第2のAMFによって第3のNASセキュリティコンテキストを生成するステップは、図4に示された実施形態で第2のAMFによって第3のNASセキュリティコンテキストを生成するステップと同様である。したがって、ここでは詳細を再度説明しない。

【０２０８】

さらに、第2のAMFは、第3のNASセキュリティコンテキストを生成した後に、新しいNASセキュリティコンテキストに基づいてNASCを決定する。換言すると、図5に示された実施形態はS214をさらに含む、すなわち、第2のAMFはNASCを決定する。具体的に述べると、図5に示された実施形態で、第2のAMFによってNASCを決定するステップは、図4に示された実施形態で第2のAMFによってNASCを決定するステップと同様である。したがって、ここでは詳細を再度説明しない。

【０２０９】

第2のAMFがUEへNASCを送信する必要があることを理解されたい。具体的に述べると、NASCは、第2の（R）AN、第1のAMF、および第1の（R）ANによる転送によってUEへ送信される必要がある。UEへNASCを送信する方式は本出願の本実施形態で限定されない。詳細については、既存のプロトコルで規定されている方式を参照されたい。この方式は、図4に示された実施形態で第2のAMFによってUEへNASCを送信する方式と同様である。したがって、ここでは詳細を再度説明しない。

【０２１０】

S210：UEは第1のNASセキュリティコンテキストを記憶する。

【０２１１】

UEが第1の（R）ANによって送信されるハンドオーバーコマンドメッセージを受信してNASCを取得した後に、UEは、最初に第1のNASセキュリティコンテキストを記憶し、次いで、NASC内の情報に基づいて第1のNASセキュリティコンテキストを更新することで第3のNASセキュリティコンテキストを取得する、すなわち、S211を実行する。

【０２１２】

S220：UEは第2のNASセキュリティコンテキストを生成する。

【０２１３】

ハンドオーバーが失敗したことをUEが発見した場合に、UEが第3のNASセキュリティコンテキストを生成することは、以下のいくつかの可能なケースを含む。

【０２１４】

可能なケース1では、UEと第2のAMFとの間で取り決められ、NASCに含まれる、NASセキュリティアルゴリズムが、UEと第1のAMFとの間で取り決められるNASセキュリティアルゴリズムと異なり、NASCは、値1を有するK_AMF_change_flagを搬送する。NASC内で搬送された値1を有するK_AMF_change_flagは、UEがKamf’を取得するために鍵導出を行う必要があることを意味する。

【０２１５】

UEは、Kamf’を取得するためにKamfに対して鍵導出を行う。さらに、UEは、第2の鍵Kamf’と、UEと第1のAMFとの間で取り決められ、記憶された第1のNASセキュリティコンテキストに含まれる、NASセキュリティアルゴリズムとに基づいて、第2のNASセキュリティコンテキストを生成する。次いで、UEは、第1のNASセキュリティコンテキストとS211で生成された第3のNASセキュリティコンテキストを削除し、UEと第1のAMFとの間でNAS保護を行うためにUEは第2のNASセキュリティコンテキストの使用を開始する。

【０２１６】

可能なケース2では、UEと第2のAMFとの間で取り決められ、NASCに含まれる、NASセキュリティアルゴリズムが、UEと第1のAMFとの間で取り決められるNASセキュリティアルゴリズムと異なる。

【０２１７】

UEは第1のNASセキュリティコンテキストを使用して、UEと第1のAMFとの間でNAS保護を行う。これは、図4に示された実施形態のステップと同様である。

【０２１８】

可能なケース3では、NASCが値1を有するK_AMF_change_flagを搬送する。

【０２１９】

UEは、Kamf’を取得するためにKamfに対して鍵導出を行う。さらに、UEは、第2の鍵Kamf’と、UEと第1のAMFとの間で取り決められ、記憶された第1のNASセキュリティコンテキストに含まれる、NASセキュリティアルゴリズムとに基づいて、第2のNASセキュリティコンテキストを生成する。次いで、UEは、第1のNASセキュリティコンテキストとS211で生成された第3のNASセキュリティコンテキストを削除し、UEと第1のAMFとの間でNAS保護を行うためにUEは第2のNASセキュリティコンテキストの使用を開始する。

【０２２０】

さらに、UEは、ハンドオーバーが失敗したことを発見した後に、ハンドオーバーをキャンセルすることを、第1の（R）ANを通じて第1のAMFに通知する必要がある。この場合、図5に示された方法手順はS221をさらに含む、すなわち、第1の（R）ANは第1のAMFへハンドオーバーキャンセル要求を送信する。

【０２２１】

S230：第1のAMFは第2のNASセキュリティコンテキストを生成する。

【０２２２】

ハンドオーバーキャンセル要求を受信した後に第1のAMF側が第2のNASセキュリティコンテキストを生成することは、以下の2つの可能なケースを含む。

【０２２３】

可能なケース1では、第1のAMFが、第2の鍵Kamf’を取得するために、S212を実行する前に、Kamfに対して鍵導出を行う。この場合、第1のAMF側は、ハンドオーバーキャンセル要求を受信した後に、Kamf’と、UEと第1のAMFとの間で取り決められ、第1のNASセキュリティコンテキストに含まれる、NASセキュリティアルゴリズムとに基づいて、第2のNASセキュリティコンテキストを生成する。次いで、第1のAMF側は、第2のNASセキュリティコンテキストを使用して、第1のAMFとUEとの間でNASセキュリティ保護を行う

。図5に示された実施形態では、第1のAMFが第2のNASセキュリティコンテキストを生成する可能なケース1が主に考慮される。

【０２２４】

可能なケース2では、第1のAMFが、S212を実行する前に、Kamfに対して鍵導出を行わない。この場合、第1のAMF側は、ハンドオーバーキャンセル要求を受信した後に、第1のNASセキュリティコンテキストを使用して、UEと第1のAMFとの間でNAS保護を行う。これは、図4に示された実施形態のステップと同様である。

【０２２５】

要するに、図5に示された実施形態では、ハンドオーバーが失敗したときに、UEと第1のAMFの両方が第2のNASセキュリティコンテキストを使用してNASセキュリティ保護を行い、これにより、UEによって使用されるNAS鍵は第1のAMFによって使用されるNAS鍵と同じになる。

【０２２６】

前述したプロセスの順序番号は、前述した方法の実施形態における実行順序を意味しないことを理解されたい。プロセスの実行順序は、プロセスの機能および内部ロジックに基づいて決定されるべきであり、本出願の実施形態の実施過程に対する制限として解釈されるべきではない。

【０２２７】

本出願における「第1」および「第2」が区別のために使用されているにすぎず、本出願に対する制限として解釈されるべきではないことをさらに理解されたい。第1のNASセキュリティコンテキストと第2のNASセキュリティコンテキストは、異なるNASセキュリティコンテキストを区別するために使用されているにすぎない。

【０２２８】

上記では、図4および図5を参照しながら本出願の実施形態で提供されるハンドオーバー処理方法を詳しく説明している。以下では、図6から図9を参照しながら本出願の実施形態で提供されるハンドオーバー処理装置を詳しく説明する。

【０２２９】

図6は、本出願によるハンドオーバー処理装置10の概略図である。図6に示されているように、装置10は受信ユニット110と処理ユニット120とを備える。

【０２３０】

受信ユニット110は、第1のアクセスネットワークデバイスによって送信されるハンドオーバーコマンドメッセージを受信し、ハンドオーバーコマンドメッセージが、第2のアクセスおよびモビリティ管理機能AMFによって選択される第2のNASセキュリティアルゴリズム、およびAMF鍵変更指示を搬送するように構成される。

【０２３１】

処理ユニット120は、第2のNASセキュリティアルゴリズムがUEによって現在使用されている第1のNASセキュリティアルゴリズムと異なり、かつ／またはAMF鍵変更指示が1であるとき、第1の非アクセス層NASセキュリティコンテキストを記憶するように構成され、第1のNASセキュリティコンテキストがUEと第1のAMFの間のネゴシエーションを通じて生成されるNASセキュリティコンテキストである。

【０２３２】

処理ユニット120は、ハンドオーバーが失敗したとき、UEと第1のAMFとの間で非アクセス層NAS保護を行うために、第1のNASセキュリティコンテキストを使用するようにさらに構成される。

【０２３３】

装置10は方法の実施形態におけるユーザー機器に正確に一致する。装置10は方法の実施形態におけるユーザー機器であってよく、あるいは方法の実施形態におけるユーザー機器内のチップまたは機能モジュールであってもよい。装置10内の対応するユニットは、図4および図5に示されている方法の実施形態においてユーザー機器によって実行される対応するステップを実行するように構成される。

【０２３４】
装置10内の受信ユニット110は、方法の実施形態においてユーザー機器によって実行される受信ステップを実行する。例えば、受信ユニット110は、図4で第1の（R）ANによって送信されるハンドオーバーコマンドメッセージを受信するステップ1191と、図5で第1の（R）ANによって送信されるハンドオーバーコマンドメッセージを受信するステップ219とを実行する。
【０２３５】
処理ユニット120は、方法の実施形態においてユーザー機器によって実行される内部実行または処理ステップを実行する。例えば、処理ユニット120は、図4で第1のNASセキュリティコンテキストを記憶するステップ130、図4で第3のNASセキュリティコンテキストを生成するステップ131、図4で第1のNASセキュリティコンテキストを使用することを再開するステップ140、または図4で第1のNASセキュリティコンテキストを使用し続けるステップ132、図5で第1のNASセキュリティコンテキストを記憶するステップ210、図5で第3のNASセキュリティコンテキストを生成するステップ211、および図5で第2のNASセキュリティコンテキストを生成するステップ220を実行する。
【０２３６】
図6に示されているハンドオーバー処理装置10は、送信ユニット（図6に図示せず）をさらに備えてもよい。送信ユニットは、別のデバイスへメッセージを送信する機能を実行するように構成される。受信ユニット110と送信ユニットはトランシーバユニットを形成してもよく、受信器能と送信器能の両方を有してもよい。処理ユニット120はプロセッサであってもよく、送信ユニットは受信器であってもよく、受信ユニット110は送信器であってもよく、受信器と送信器は統合されてトランシーバを形成してもよい。
【０２３７】
図7は、本出願の一実施形態に適用可能なユーザー機器20の概略構造図である。ユーザー機器20は図1に示されたシステムに適用できる。説明を容易にするため、図7はユーザー機器内の主要なコンポーネントのみを示している。図7に示されているように、ユーザー機器20は、プロセッサと、メモリーと、制御回路と、アンテナと、入出力装置とを備える。プロセッサは、信号を送受信するようにアンテナおよび入出力装置を制御するように構成される。メモリーは、コンピュータプログラムを記憶するように構成される。プロセッサは、本出願で提供されるハンドオーバー処理方法でユーザー機器によって実行される対応する手順および／または動作を実行するために、メモリーからコンピュータプログラムを呼び出し、かつコンピュータプログラムを実行するように構成される。ここでは詳細を説明しない。
【０２３８】
当業者なら、説明を容易にするために、図7がただ1つのメモリーとただ1つのプロセッサを示していることを理解できるであろう。実際には、ユーザー機器は複数のプロセッサおよびメモリーを備えてよい。メモリーは、記憶媒体やストレージデバイスなどと呼ばれることもある。これは本出願の実施形態で限定されない。
【０２３９】
図8は、本出願によるハンドオーバー処理装置30の概略図である。図8に示されているように、装置30は、受信ユニット310と、処理ユニット320と、送信ユニット330とを備える。
【０２４０】
受信ユニット310は、第1のアクセスネットワークデバイスによって送信されるハンドオーバー要求メッセージを受信するように構成される。
【０２４１】
処理ユニット320は、ローカルポリシーに従って、鍵導出が行われる必要があると判断するように構成される。
【０２４２】
処理ユニット320は、第1の非アクセス層NASセキュリティコンテキストを記憶するよ

うにさらに構成され、第1のNASセキュリティコンテキストが、第1のAMFとユーザー機器UEの間のネゴシエーションを通じて生成されるNASセキュリティコンテキストである。

【０２４３】

送信ユニット330は、第2のAMFへユーザー機器UEセキュリティコンテキストを送信するように構成される。

【０２４４】

処理ユニット320は、第1のNASセキュリティコンテキストを使用することを再開するようにさらに構成される。

【０２４５】

装置30は方法の実施形態における第1のAMFに正確に一致する。装置30は方法の実施形態における第1のAMFであってよく、あるいは方法の実施形態における第1のAMF内のチップまたは機能モジュールであってもよい。装置30内の対応するユニットは、図4および図5に示されている方法の実施形態において第1のAMFによって実行される対応するステップを実行するように構成される。

【０２４６】

装置30内の受信ユニット310は、方法の実施形態において第1のAMFによって実行される受信ステップを実行する。例えば、受信ユニット310は、図4で第1の（R）ANによって送信されるハンドオーバー要求メッセージを受信するステップ111、図4で第2のAMFによって送信されるUEコンテキスト作成サービス要求応答を受信するステップ118、図5で第1の（R）ANによって送信されるハンドオーバー要求メッセージを受信するステップ211、および図5で第2のAMFによって送信されるUEコンテキスト作成サービス要求応答を受信するステップ217を実行する。

【０２４７】

処理ユニット320は、方法の実施形態において第1のAMFによって実行される内部実行または処理ステップを実行する。例えば、処理ユニット320は、図4で第1のNASセキュリティコンテキストを記憶するステップ110、図4で鍵導出を行うステップ112、図4で第1のNASセキュリティコンテキストを使用することを再開するステップ120、および図5で第2のNASセキュリティコンテキストを生成するステップ230を実行する。

【０２４８】

送信ユニット330は、方法の実施形態において第1のAMFによって実行される送信ステップを実行する。例えば、送信ユニット330は、図4で第2のAMFへUEセキュリティコンテキストを送信するステップ113、図4で第1の（R）ANへハンドオーバーコマンドメッセージを送信するステップ119、図5で第2のAMFへUEセキュリティコンテキストを送信するステップ212、および図5で第1の（R）ANへハンドオーバーコマンドメッセージを送信するステップ218を実行する。

【０２４９】

受信ユニット310と送信ユニット330はトランシーバユニットを形成してもよく、受信器能と送信器能の両方を有してもよい。処理ユニット320はプロセッサであってもよく、送信ユニット330は受信器であってもよく、受信ユニット310は送信器であってもよく、受信器と送信器は統合されてトランシーバを形成してもよい。

【０２５０】

図9に示されているように、本出願の一実施形態は第1のAMF 40をさらに提供する。第1のAMF 40は、プロセッサ410と、メモリー420と、トランシーバ430とを含む。メモリー420は命令またはプログラムを記憶する。プロセッサ430は、メモリー420に記憶された命令またはプログラムを実行するように構成される。メモリー420に記憶された命令またはプログラムが実行されると、トランシーバ430は、図8に示された装置30内の受信ユニット310と送信ユニット330とによって実行される動作を実行するように構成される。

【０２５１】

本出願の一実施形態はコンピュータ可読記憶媒体をさらに提供する。コンピュータ可読

記憶媒体は命令を記憶する。命令がコンピュータで実行されると、コンピュータは、図4および図5に示されている方法で第1のAMFによって実行されるステップを実行できるようになる。

【０２５２】

本出願の一実施形態はコンピュータ可読記憶媒体をさらに提供する。コンピュータ可読記憶媒体は命令を記憶する。命令がコンピュータで実行されると、コンピュータは、図4および図5に示されている方法でユーザー機器によって実行されるステップを実行できるようになる。

【０２５３】

本出願の一実施形態は、命令を含むコンピュータプログラム製品をさらに提供する。コンピュータプログラム製品がコンピュータで実行すると、コンピュータは、図4および図5に示されている方法で第1のAMFによって実行されるステップを実行できるようになる。

【０２５４】

本出願の一実施形態は、命令を含むコンピュータプログラム製品をさらに提供する。コンピュータプログラム製品がコンピュータで実行すると、コンピュータは、図4および図5に示されている方法でユーザー機器によって実行されるステップを実行できるようになる。

【０２５５】

本出願の一実施形態は、プロセッサを含むチップをさらに提供する。プロセッサは、本出願で提供されるハンドオーバー処理方法においてユーザー機器によって実行される対応する動作および／または手順を実行するために、メモリーに記憶されたコンピュータプログラムを読み取り、かつコンピュータプログラムを実行するように構成される。任意に選べることとして、チップはメモリーをさらに含む。メモリーは、回路またはケーブルを通じてプロセッサに接続される。プロセッサは、メモリー内のコンピュータプログラムを読み取って実行するように構成される。任意に選べることとして、チップは通信インターフェイスをさらに含み、プロセッサは通信インターフェイスに接続される。通信インターフェイスは、処理される必要があるデータおよび／または情報を受信するように構成される。プロセッサは、通信インターフェイスからデータおよび／または情報を取得し、データおよび／または情報を処理する。通信インターフェイスは入出力インターフェイスであってもよい。

【０２５６】

本出願は、プロセッサを含むチップをさらに提供する。プロセッサは、本出願で提供されるハンドオーバー処理方法において第1のAMFによって実行される対応する動作および／または手順を実行するために、メモリーに記憶されたコンピュータプログラムを呼び出し、かつコンピュータプログラムを実行するように構成される。任意に選べることとして、チップはメモリーをさらに含む。メモリーは、回路またはケーブルを通じてプロセッサに接続される。プロセッサは、メモリー内のコンピュータプログラムを読み取って実行するように構成される。任意に選べることとして、チップは通信インターフェイスをさらに含み、プロセッサは通信インターフェイスに接続される。通信インターフェイスは、処理される必要があるデータおよび／または情報を受信するように構成される。プロセッサは、通信インターフェイスからデータおよび／または情報を取得し、データおよび／または情報を処理する。通信インターフェイスは入出力インターフェイスであってもよい。

【０２５７】

当業者なら、本明細書で開示されている実施形態で説明されている例と組み合わせて、ユニットとアルゴリズムステップが、電子ハードウェアによって、またはコンピュータソフトウェアと電子ハードウェアとの組み合わせによって、実装され得ることに気づくであろう。機能がハードウェアによって実装されるのかソフトウェアによって実装されるのかは、技術的解決策の具体的な用途と設計上の制約条件とに左右される。当業者なら、様々な方法を用いて具体的な用途ごとに説明されている機能を実装できるが、その実装が本出願の範囲を超えるとみなされるべきではない。

【０２５８】

当業者なら、簡便で簡潔な説明のために、前述のシステム、装置、およびユニットの詳しい動作プロセスについては、前述の方法の実施形態における対応するプロセスを参照でき、ここで詳細が再度説明されないことを明確に理解できるであろう。

【０２５９】

本出願で提供されるいくつかの実施形態において、開示されているシステム、装置、および方法が別の方式で実装され得ることを理解されたい。例えば、説明されている装置の実施形態は一例にすぎない。例えば、ユニットへの分割は論理的な機能の分割にすぎず、実際の実装では別の分割であってもよい。例えば、複数のユニットまたはコンポーネントが別のシステムに組み合わされてもよく、あるいは統合されてもよく、またはいくつかの機能は無視されてもよく、あるいは実行されなくてもよい。加えて、提示または論述されている相互結合または直接結合または通信接続は、いくつかのインターフェイスを使用して実装されてよい。装置またはユニット間の間接結合または通信接続は、電子的形態、機械的形態、またはその他の形態で実装されてよい。

【０２６０】

別個の部分として説明されているユニットは物理的に分離されていてもいなくてもよく、ユニットとして表示されている部分は物理的なユニットであってもなくてもよく、一箇所に置かれてもよく、あるいは複数のネットワークユニットに分散されてもよい。実施形態の解決策の目的を達成するために、実際の要件に基づいてユニットの一部または全部が選択されてよい。

【０２６１】

加えて、本出願の実施形態の機能ユニットは1つの処理ユニットに統合されてもよく、あるいはユニットの各々が物理的に単独で存在してもよく、あるいは2つ以上のユニットが1つのユニットに統合される。

【０２６２】

機能がソフトウェア機能ユニットの形態で実装され、独立した製品として販売または使用される場合は、機能がコンピュータ可読記憶媒体に記憶されてよい。そのような理解に基づき、本出願の技術的解決策は本質的に、または先行技術に寄与する部分は、または技術的解決策のうちのいくつかは、ソフトウェア製品の形態で実装されてもよい。コンピュータソフトウェア製品は記憶媒体に記憶され、本出願の実施形態で説明されている方法のステップの全部または一部を実行することをコンピュータデバイス（パーソナルコンピュータ、サーバー、またはネットワークデバイスであってよい）に命令するいくつかの命令を含む。前述の記憶媒体は、USBフラッシュドライブ、リムーバブルハードディスク、読み取り専用メモリー（Read-Only Memory、ROM）、ランダムアクセスメモリー（（R）ANdom Access Memory、RAM）、磁気ディスク、または光ディスクなど、プログラムコードを記憶できる何らかの媒体を含む。

【０２６３】

以上の説明は本出願の特定の実装にすぎず、本出願の保護範囲を制限することを意図していない。本出願で開示されている技術的な範囲内で当業者によって容易に考え出される変形や置換は、本出願の保護範囲内に入るものとする。したがって、本出願の保護範囲は特許請求の範囲の保護範囲に従うものとする。

【符号の説明】

【０２６４】

10　ハンドオーバー処理装置
20　ユーザー機器
30　ハンドオーバー処理装置
40　第1のAMF
110　受信ユニット
120　処理ユニット
310　受信ユニット
320　処理ユニット

330 送信ユニット
410 プロセッサ
420 メモリー
430 トランシーバ

【図面】

【図１】

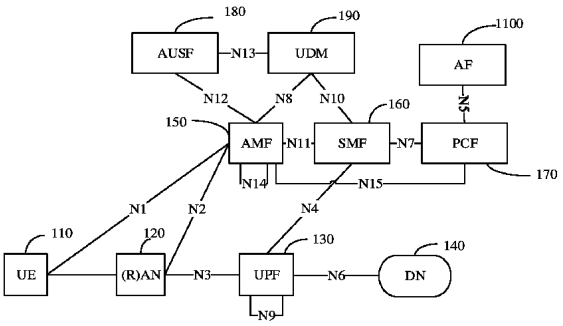
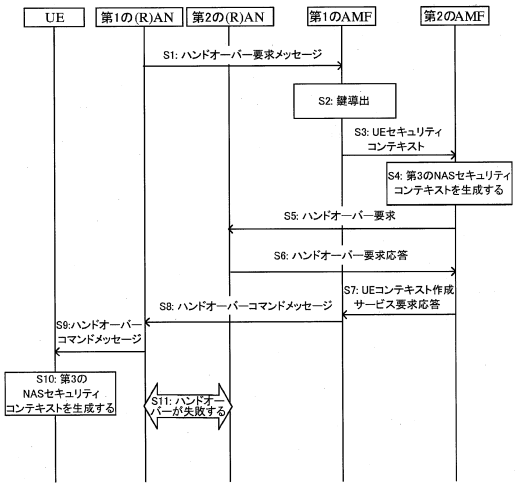
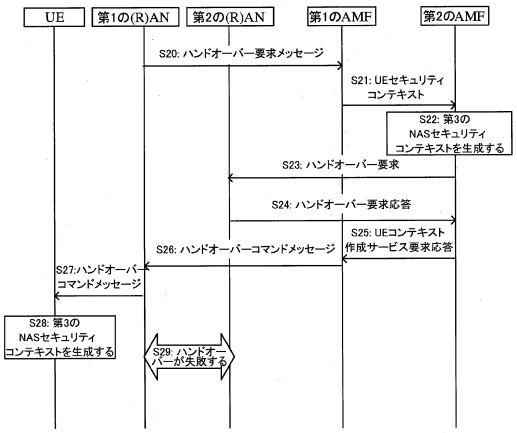


図 1

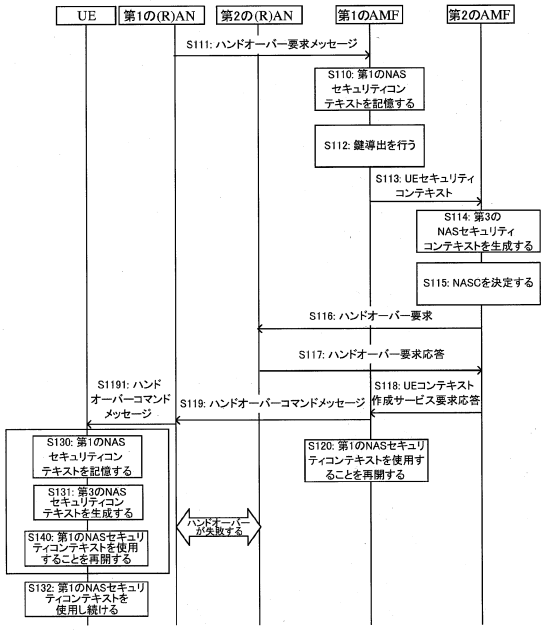
【図２】



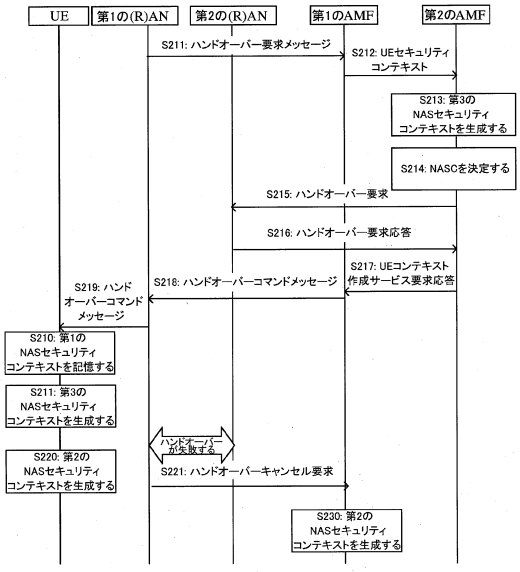
【図３】



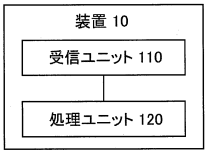
【図４】



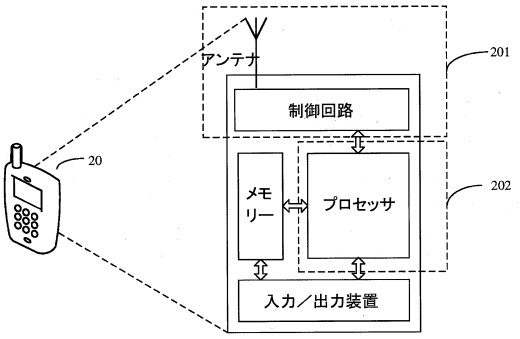
【図５】


UE
第1の(R)AN
第2の(R)AN
第1のAMF
第2のAMF
S211: ハンドオーバー要求メッセージ
S212: UEセキュリティコンテキスト
S213: 第3のNASセキュリティコンテキストを生成する
S214: NASCを決定する
S215: ハンドオーバー要求
S216: ハンドオーバー要求応答
S217: UEコンテキスト作成サービス要求応答
S218: ハンドオーバーコマンドメッセージ
S219: ハンドオーバーコマンドメッセージ
S210: 第1のNASセキュリティコンテキストを記憶する
S211: 第3のNASセキュリティコンテキストを生成する
ハンドオーバーが失敗する
S220: 第2のNASセキュリティコンテキストを生成する
S221: ハンドオーバーキャンセル要求
S230: 第2のNASセキュリティコンテキストを生成する

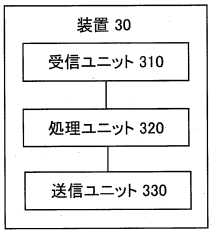
【図６】


装置 10
受信ユニット 110
処理ユニット 120

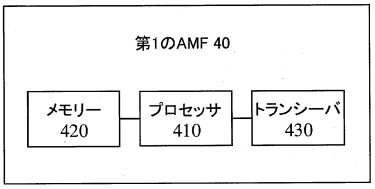
【図７】


アンテナ
201
制御回路
20
メモリー
プロセッサ
202
入力／出力装置

【図８】


装置 30
受信ユニット 310
処理ユニット 320
送信ユニット 330

【図９】



フロントページの続き

(51)国際特許分類　　FI
H04W 36/12 (2009.01)　　H04W 36/12

中国(CN)

(74)代理人　100133569
弁理士　野村 進
(72)発明者　李 ▲飛▼
中華人民共和国 518129 広東省深▲チェン▼市龍崗区坂田 華為総部▲ベン▼公楼
(72)発明者　▲楊▼ 林平
中華人民共和国 518129 広東省深▲チェン▼市龍崗区坂田 華為総部▲ベン▼公楼

合議体
審判長　廣川 浩
審判官　本郷 彰
審判官　河合 弘明

(56)参考文献
米国特許出願公開第2010／0002883（US，A1）
国際公開第2019／053185（WO，A1）
1．3rd Generation Partnership Project；technical Specification Group Services and System Aspects；Security archtecture and procedures for 5G system（Release15），3GPP TS33．501 V15．4．1．0，2019年03月28日，6．4．3．2 NASintegrity activation－6．9．3 Key handling in mobility registration update
Huawei，HiSilicon，Clarification on UE behavior after handover failure，3GPP TSG RAN WG2 #104 R2－1818096，2018年11月02日，<URL：https：／／www．3gpp．org／ftp／tsg_ran／WG2_RL2／TSGR2_104／Docs／R2－1818096．zip>
Huawei，HiSilicon，Discussion on error and key handling on UE for Reestablishment Procedure in case of N2 handover failure [online]，3GPP TSG RAN WG2 #104 R2－1817842，2018年11月01日，<URL：https：／／www．3gpp．org／ftp／tsg_ran／WG2_RL2／TSGR2_104／Docs／R2－1817842．zip>

(58)調査した分野　(Int.Cl.，DB名)
H04B7/24-7/26
H04W4/00-99/00
3GPP TSG RAN WG1-4
3GPP TSG SA WG1-4
3GPP TSG CT WG1,4