アクセスセキュリティ　認証　暗号化

Technology Reports

SAE標準化技術特集

SAE/LTEを実現するセキュリティ技術

3Gから4Gへの円滑な移行を進めるために，LTEにおいて新たに導入するセキュリティ機能への要求条件が検討されてきた．中でも，従来の3Gと同等もしくはそれ以上のレベルのセキュリティ機能を有し，かつ，現状のインターネットからの攻撃に対する防御機能を有することが重要な要求条件として挙げられる．このため，LTEにおける主な新しいセキュリティ機能として，鍵階層の導入，アクセス層と非アクセス層セキュリティの分離およびハンドオーバ時におけるフォワードセキュリティの機能拡充を行った．

ドコモ欧州研究所　Alf Zugenmaier
サービス＆ソリューション開発部　青野（あおの）　博（ひろし）

1. まえがき

LTEは，既存のFOMAで採用している標準化方式（3G）と比較しアーキテクチャ設計が大きく変更されている．それに併せてセキュリティ機能の改良も必要となる．その際，最も重要な要求条件は，3Gネットワークと少なくとも同等の安全性をLTEでも保証する必要があることである．この要求条件を満足するために行った主な変更・追加点は，次のとおりである[1][2].

・異なる目的ごとに鍵を変える鍵の階層化の導入
・コアネットワークノードと移動端末（UE）との間の通信を処理する非アクセス層（NAS：Non-Access-Stratum）[*1]のセキュリティ機能の分離
・危殆化[*2]された鍵を使う場合に損害範囲を限定するためのフォワードセキュリティの概念の導入
・3GネットワークとLTEネットワーク間の相互接続におけるセキュリティ機能の追加

本稿では，3GPP SA（Service & Systems Aspects）WG3にてドコモが貢献したLTEにおける主な新しいセキュリティ機能として，鍵階層の導入，NAS層のセキュリティ機能のアクセス層（AS：Access-Stratum）[*3]セキュリティからの分離およびハンドオーバ時におけるフォワードセキュリティの機能拡充について解説する．

2. LTEにおけるセキュリティの要求条件

現在，3Gサービスにおけるセキュリティ機能[3]は，すでに広く使われていて，3Gネットワークには十分に安全なレベルで，ユーザIDの秘匿性，認証，U-Plane（User Plane）[*4]，C-Plane（Control Plane）[*5]の秘匿およびC-Planeの完全性保証[*6]（Integrity Protection）を提供している．LTEにおけるセキュリティ機能の要求条件は主に次の4点であり，従来の認証方法と鍵管理プロトコル（3GPP AKA：Authentication and Key Agreement）[*7]を踏襲することにより実現している．

＊1　**非アクセス層（NAS）**：コアネットワークとUEとの間のUMTS（Universal Mobile Telecommunications System）プロトコルスタックにおける機能レイヤ．
＊2　**危殆化**：セキュリティ上の安全性が脅かされる状態になること．
＊3　**アクセス層（AS）**：eNB（＊10参照）とUEとの間のUMTSプロトコルスタックにおける機能レイヤ．
＊4　**U-Plane**：ユーザデータを転送するためのプロトコル．

①ユーザの使い勝手に影響を与えず，最低でも3Gネットワークと同じレベルもしくはそれ以上のレベルのセキュリティを提供する．

②現状のインターネットからの攻撃に対する防御機能を提供する．

③LTEで提供されるセキュリティ機能は，3GからLTEへの段階的な導入に影響を与えない．

④USIM（Universal Subscriber Identity Module）[*8]の継続利用を可能とする．

LTEでのコアネットワークにおけるセキュリティは，3Gと同様にIPレイヤにおいてTS33.210[4]で標準化されているネットワークドメインセキュリティ（NDS）[*9]を適用することにより，セキュリティ要求条件を満たすことができる．

一方，LTEにおける無線アクセス制御装置（RNC：Radio Network Controller）機能の一部はeNB（evolved NodeB）[*10]に統合されたため，無線アクセスネットワークにおいては，3Gのセキュリティアーキテクチャをそのまま再利用することができない．具体的には，eNBはUEが接続状態にある間のみ，暗号化および完全性保証のための鍵を保持しており，例えば非接続状態などにおいては，3Gと異なり信号メッセージを守るために使う鍵は保持していない．

さらに，LTEにおけるeNBは，オフィスなど屋内のエリアのカバレッジや無線容量を確保するため，身近な場所に設置される傾向にあり，eNBが不正にアクセスされるリスクも増えると予想される．そのため，鍵が不正にeNBから盗み出された場合の被害を最小限に抑えるために，次に述べるような対策が規定されている．

3. 鍵の階層化

データの暗号化については，LTEも3Gと同様に，データとキーストリーム[*11]を排他的論理和（XOR）[*12]することにより暗号化するストリーム暗号方式が採用されている．この方式では，キーストリームが決して再利用されないことが重要である．3GおよびLTEで使われたアルゴリズム[5][6]は，有限長のキーストリームを生成するだけである．そこで，キーストリーム再利用を避けるためには，キーストリームを生成するのに使われる鍵を，例えば網接続やハンドオーバ時など，任意のタイミングで変えられなければならない．3Gネットワークにおいては，この鍵を生成するためにAKA実行を必要とする．AKAの実行には，USIM上での計算とHSS（Home Subscriber Service）[*13]との接続に数百ミリ秒かかる可能性があるため，LTEのように，より高いデータレートを実現するには，AKAを実行せずに鍵の更新を可能にする機能の追加が必要になる．

加えて，暗号化または完全性保証に使われる鍵の1つが危険にさらされた場合の被害を最小にするために，ネットワーク上の複数の箇所に同じ鍵を保存しないことが望まれる．LTEでは，それらを解決する方法として，鍵の階層化が導入された（**図1**）．

3Gネットワーク同様に，USIMとAuC（Authentication Center）[*14]は，あらかじめ秘密情報（鍵K）を

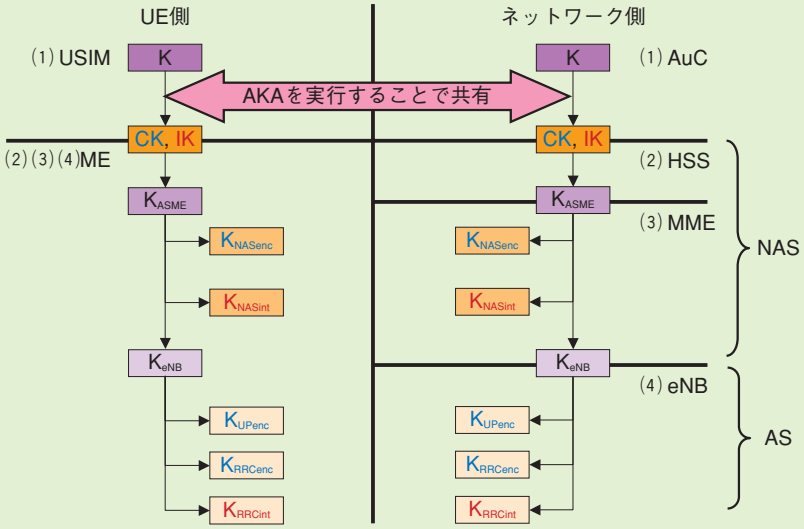

図1　LTEにおける鍵階層化とエンティティ間の鍵生成方法

＊5 **C-Plane**：制御信号を転送するためのプロトコル．

＊6 **完全性保証**：通信データの改ざんがないことを保証する暗号技術．

＊7 **鍵管理プロトコル（3GPP AKA）**：USIM（＊8参照）と通信事業者の網間相互認証を行い，一時的な秘密情報（暗号化，完全性保証のための鍵）を共有するためのプロトコル．

＊8 **USIM**：携帯電話会社と契約した電話番号などを記録しているICカード．3GPPでのW-CDMA/LTE用途の移動通信用加入者識別モジュールをUSIMと呼ぶ．

＊9 **ネットワークドメインセキュリティ（NDS）**：ネットワークドメイン内のノード間のセキュリティ．

＊10 **eNB**：LTEにおける無線基地局．

共有している．

(1) ネットワークとユーザの相互認証のためにAKAが実行されるたびに，暗号化および完全性保証に使われる鍵CK，IKが生成され，USIMからME（Mobile Equipment），AuCからHSSへ渡される．

(2) 在圏ネットワークの識別子に基づいた鍵生成機能を利用し，MEおよびHSSはこの鍵ペアCK，IKからK_{ASME}を生成する．この鍵の関連付けを実行することにより，HSSはこのK_{ASME}が在圏ネットワークによってのみ使うことができることを保証する．K_{ASME}はHSSによって在圏ネットワークのMME（Mobility Management Entity）[*15]に移され，鍵階層化の基の情報となる．

(3) UEとMME間のNASプロトコルの暗号化のための鍵K_{NASenc}および完全性保護のためのK_{NASint}は，K_{ASME}から生成される．

(4) UEがネットワークに接続するときは，MMEは鍵K_{eNB}を生成し，eNBに渡す．このK_{eNB}から，U-Planeの暗号化の鍵であるK_{UPenc}と，RRC（Radio Resource Control）のための暗号化と完全性保証の鍵であるK_{RRCenc}とK_{RRCint}が生成される．

4. ASとNAS間のセキュリティ機能の分離

UEは，接続状態でのみ大量のデータを転送することが想定されるため，LTEのネットワークは，接続状態のUEのためにのみ，UEとeNBの間にセキュリティアソシエーション[*16]を確立する．したがって，eNBはアイドルモードのUEに対しては，状態を保持する必要はない．NASメッセージはアイドルモードのUEとやりとりをするため，UEとコアネットワークのノードすなわちMME間でNASセキュリティアソシエーションを確立する．

UEの認証後は，MMEが在圏ネットワークにおける鍵階層化の基となる情報であるK_{ASME}を保持している．NASセキュリティモードコマンドは，暗号化と完全性保証のアルゴリズムをネゴシエートにより決定するのと同時に，K_{NASenc}とK_{NASint}を使ったNAS通信を始めることを許可する．MMEはここで，復号と完全性を検証するために使う正しい鍵を探すために，どのUEから認証要求のメッセージが届いたかを判別する必要がある．しかしながら，UEの識別子（IMSI：International Mobile Subscriber Identity）は無線区間では保護されるべきである．そのためLTEでは，IMSIでUEを識別するのではなく，GUTI（Global Unique Temporary Identity）[*17]と呼ばれる一時的な識別子が導入された．このGUTIは定期的に変えられるため，どのUEがどのGUTIを使っているかをトレースすることはできない．

UEが接続状態になるとすぐに，eNBは分離したASセキュリティモードコマンドでASの保護機能に切り替わる．ASセキュリティは，UEとeNBとの間のすべての通信に適用され，ASのために使われるアルゴリズムは，NASのために使われるアルゴリズムとは独立してネゴシエートされる．暗号化を認めていない国においては，セキュリティを提供しない暗号化なしのモードをネゴシエートにより決定することも可能である．

LTEでは，Snow 3G[*18]ベースとAES（Advanced Encryption Standard）[*19]ベースの暗号化および完全性保証アルゴリズムを標準化している．これら2つのアルゴリズムはそれぞれ，十分なセキュリティを提供するが，3GPPにおいて2つの基本的な構造が異なるアルゴリズムを標準として用意している理由は，たとえ1つのアルゴリズムが破られても，もう一方のアルゴリズムを使用することにより，LTEシステムをそれまでどおり安全に使い続けることができるからである．

5. ハンドオーバにおけるセキュリティ

eNBは，身近な場所に設置される傾向にあり，不正アクセスのリスクも高いため十分な安全性が要求される．そこで，LTEにおけるセキュリティすなわちフォワードセキュリティという概念を導入する．ここで，K_{eNB}鍵配送におけるフォワードセキュリティとは，UEとeNBで共有するK_{eNB}に関して，UEと接続するeNBとの間で使われる将来のK_{eNB}を推測することが計算量的に不可能であり，鍵が破られないことをいう．

LTEにおけるハンドオーバ時の鍵

＊11 **キーストリーム**：ストリーム暗号では平文のデータをビット単位で擬似乱数と排他的論理和（＊12参照）を行うことで暗号化を行う．そのストリーム暗号が発生させる擬似乱数をキーストリームという．

＊12 **排他的論理和（XOR）**：与えられた入力のうち真が奇数個であるときに真となり，偶数個のとき偽となる，論理演算における1つの演算．

＊13 **HSS**：3GPP移動通信網における加入者情報データベースであり，認証情報および在圏情報の管理を行う．

＊14 **AuC**：ユーザの認証などセキュリティにかかわるデータを保持する3GPPにおける論理ノード．

＊15 **MME**：移動管理制御をする論理ノード．

配送のモデルを**図2**に示す.初期ASセキュリティコンテキストをUEとeNBとの間で共有する場合，MMEとUEは同じK_{eNB}とNext Hopパラメータ[*20]（以下，NH）をそれぞれで生成する必要がある．K_{eNB}とNHはK_{ASME}から生成され，NCC（NH Chaining Counter）[*21]ごとにK_{eNB}とNHがある．それぞれのK_{eNB}は，NCCごとにNHの値から生成される．初期設定において，K_{eNB}は直接K_{ASME}とNAS uplink COUNTから生成され，NCC＝0の鍵連鎖とされる．初期設定において導き出されるNHの値は，NCC＝1以降の鍵連鎖にも使われる．

UEとeNBとの間のセキュア通信にはK_{eNB}が使われる．ハンドオーバにおいて，UEとターゲットeNBの間で使われるK_{eNB}の構成要素K_{eNB}^*は，アクティブなK_{eNB}もしくはNHから生成される．K_{eNB}^*が現在のK_{eNB}から生成されるなら，これは図中の水平方向の鍵配送を使用し，NHから生成されるなら，図中の縦の鍵配送を使用する．縦の鍵配送を使ったハンドオーバにおいては，NHとターゲットPCI（Physical Cell Identity）と周期的なEARFCN-DL（E-UTRAN Absolute Radio Frequency Channel Number-Down Link）を使ってK_{eNB}^*を生成する．水平方向の鍵配送を使ったハンドオーバにおいては，現在のK_{eNB}はターゲットPCIとその周期的なEARFCN-DLを使って生成される．

NHがUEとMMEによってのみ計算可能なとき，NHはフォワードセキュリティが達成される方法でMMEから複数のeNBに提供される．ここで，縦の鍵配送時におけるセキュリティであるnホップフォワードセキュリティとは，UEがn回（nは1または2）もしくはそれ以上のハンドオーバの後に接続する他のeNBとの間で使われる将来のK_{eNB}を，推測されることが計算量的に不可能であり鍵が破られないことをいう．本機能により，たとえ鍵が破られた場合でも，縦の鍵配送により現在のK_{eNB}を用いることなく鍵が生成されるため，損害範囲を限定することが可能になる．

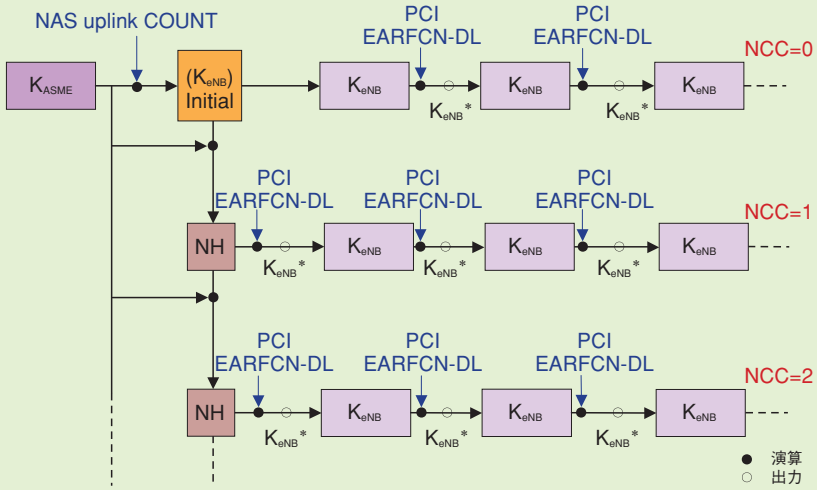

図2　ハンドオーバにおける鍵連鎖のモデル

6. あとがき

LTEのセキュリティ機能は，3Gによって提供されたセキュリティ機能以上のものが望まれる一方で，従来のアーキテクチャへの影響を最小限に抑える必要があった．今回制定された3GPP Release 8においては，それらの要求条件を満たしたセキュリティ機能の標準化を行うことができた．今後も，Release 9の標準化を目指し，Home eNBのセキュリティ，M2M（Machine to Machine）セキュリティなどの新たなセキュリティ機能開発を進めていく．

文　献

[1] 3GPP TS33.401 V8.4.0：“3GPP System Architecture Evolution (SAE); Security architecture,” 2009.
[2] 3GPP TR33.821 V8.0.0 “Rationale and track of security decisions in Long Term Evolution (LTE) RAN / 3GPP System Architecture Evolution (SAE),” 2009.
[3] 3GPP TS33.102 V8.3.0 “3G security; Security architecture,” 2009.
[4] 3GPP TS33.210 V8.3.0：“3G Security; Network Domain Security; IP network layer security,” 2009.
[5] 3GPP TS35.201 V8.0.0：“Specification of the 3GPP confidentiality and integrity algorithm; Document 1:f8 and f9 specification,” 2008.
[6] 3GPP TS35.216 V8.0.0：“Specification of the 3GPP confidentiality and integrity algorithm; Document1: UEA2 and UIA2 specification,” 2008.

＊16 **セキュリティアソシエーション**：通信を始める前に暗号化方式や暗号鍵などの情報を交換・共有し，安全な通信路を確立すること．
＊17 **GUTI**：SAE/LTEで採用された，ユーザを識別する一時的なID．
＊18 **Snow 3G**：LTEで使われるストリーム暗号方式の1つ．
＊19 **AES**：アメリカ合衆国の新暗号規格として規格化された共通鍵暗号方式であり，3GPPでも利用される暗号方式の1つ．
＊20 **Next Hopパラメータ**：フォワードセキュリティを実現するためにUEとMMEで生成される鍵の1つで，NCC（＊21参照）が加算されるたびに変化する値．
＊21 **NCC**：垂直方向のハンドオーバが実行されるときに加算されるNext Hopのカウンタ．