(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3968073号
(P3968073)
(45)発行日　平成19年8月29日(2007.8.29)　(24)登録日　平成19年6月8日(2007.6.8)

(51)Int.Cl.　F I
H04Q 7/38 (2006.01)　H04B 7/26 109R

請求項の数 20　(全 14 頁)

(21)出願番号　特願2003-387318(P2003-387318)
(22)出願日　平成15年11月18日(2003.11.18)
(65)公開番号　特開2004-248253(P2004-248253A)
(43)公開日　平成16年9月2日(2004.9.2)
審査請求日　平成15年11月18日(2003.11.18)
(31)優先権主張番号　10/248731
(32)優先日　平成15年2月13日(2003.2.13)
(33)優先権主張国　米国(US)

(73)特許権者　306045752
イノベイティブ・ソニック・リミテッド
ＩＮＮＯＶＡＴＩＶＥ　ＳＯＮＩＣ　ＬＩＭＩＴＥＤ
英領ヴァージン諸島　トルトラ島　ロード・タウン，オフショア・インコーポレーションズ・センター，ピー．オー．ボックス９５７
(74)代理人　110000028
特許業務法人明成国際特許事務所
(72)発明者　呉　志祥
台湾台北縣新店市二十張路２５巷１８弄３８号５樓

審査官　望月　章俊

最終頁に続く

(54)【発明の名称】ワイヤレス通信機器にセキュリティＳＴＡＲＴ値を記憶させる方法

(57)【特許請求の範囲】
【請求項１】
ワイヤレス機器においてセキュリティＳＴＡＲＴ値を処理するための方法であって、
前記ワイヤレス機器が、ＩｎｔｅｒＲＡＴ引き渡し、ＩｎｔｅｒＲＡＴセル再選択、および、ＵＴＲＡＮからのＩｎｔｅｒＲＡＴセル変更命令よりなる群から選択されたＩｎｔｅｒＲＡＴ手順を正常に完了するステップと、
前記ＩｎｔｅｒＲＡＴ手順の正常な完了に呼応して、前記ワイヤレス機器内にＵＳＩＭが存在するか否かを決定するステップと、
前記ワイヤレス機器内に前記ＵＳＩＭが存在することの決定に呼応して、現行のＲＲＣ接続時にセキュリティキーセットが未使用であったか否かを決定するステップと、
前記現行のＲＲＣ接続時に前記セキュリティキーセットが未使用であった場合に、前記セキュリティキーセットに関連付けられたＣＮドメイン用のセキュリティＳＴＡＲＴ値として、前記ＵＳＩＭに所定の値を記憶させるステップと
を備え、
前記所定の値は、セキュリティキーセットの削除をトリガするＴＨＲＥＳＨＯＬＤ値未満である、方法。
【請求項２】
請求項１に記載の方法であって、
前記所定の値はゼロである、方法。
【請求項３】

請求項１に記載の方法であって、さらに、
前記セキュリティＳＴＡＲＴ値を前記所定の値に設定するステップを備える方法。
【請求項４】
請求項１に記載の方法であって、さらに、
前記ワイヤレス機器内にＳＩＭが存在する場合に、
現行のＲＲＣ接続時にセキュリティキーセットが未使用であったか否かを決定し、
前記現行のＲＲＣ接続時に前記セキュリティキーセットが未使用であった場合に、前記セキュリティキーセットに関連付けられたＣＮドメイン用のセキュリティＳＴＡＲＴ値として、前記ＵＥに所定の値を記憶させるステップを備える方法。
【請求項５】
請求項４に記載の方法であって、さらに、
ＣＮドメインに関連付けられたセキュリティＳＴＡＲＴ値が前記ＴＨＲＥＳＨＯＬＤ値以上である場合に、前記ＣＮドメインに関連付けられたセキュリティキーを前記ＳＩＭから削除するステップを備える方法。
【請求項６】
請求項５に記載の方法であって、さらに、
前記ＣＮドメインに関連付けられたセキュリティキーセットであって、前記ＳＩＭに記憶され前記ＣＮドメインに関連付けられた前記セキュリティキーから得られたセキュリティキーセットを前記ＵＥから削除するステップを備える方法。
【請求項７】
請求項３に記載の方法であって、さらに、
前記ＣＮドメインに関連付けられた前記セキュリティＳＴＡＲＴ値を前記所定の値に設定するステップを備える方法。
【請求項８】
請求項７に記載の方法であって、さらに、
前記ＣＮドメインに関連付けられた前記セキュリティＳＴＡＲＴ値が前記ＴＨＲＥＳＨＯＬＤ値未満である場合に、前記ＣＮドメインに関連付けられた前記セキュリティＳＴＡＲＴ値を前記ＵＥに記憶させるステップを備える方法。
【請求項９】
請求項８に記載の方法であって、さらに、
別のＣＮドメインに関連付けられたセキュリティＳＴＡＲＴ値を前記所定の値に設定するステップと、
前記別のＣＮドメインに関連付けられた前記セキュリティＳＴＡＲＴ値を前記ＵＥに記憶させるステップと
を備える方法。
【請求項１０】
請求項１に記載の方法であって、さらに、
前記セキュリティキーセットに関連付けられた前記ＣＮドメイン用の前記セキュリティＳＴＡＲＴ値が前記ＴＨＲＥＳＨＯＬＤ値を超え、且つ前記ＩｎｔｅｒＲＡＴ手順が前記ＩｎｔｅｒＲＡＴセル再選択手順または前記ＵＴＲＡＮからのＩｎｔｅｒＲＡＴセル変更命令手順である場合に、前記セキュリティキーセットを削除するステップと、
前記セキュリティキーセットに関連付けられた前記ＣＮドメイン用の前記セキュリティＳＴＡＲＴ値が前記ＴＨＲＥＳＨＯＬＤ値未満であり、且つ前記ＩｎｔｅｒＲＡＴ手順が前記ＩｎｔｅｒＲＡＴセル再選択手順または前記ＵＴＲＡＮからのＩｎｔｅｒＲＡＴセル変更命令手順である場合に、前記セキュリティＳＴＡＲＴ値を前記ＵＳＩＭに記憶させるステップと
を備える方法。
【請求項１１】
プロセッサおよびメモリを備えるワイヤレス機器であって、
前記メモリは、

ＩｎｔｅｒＲＡＴ引き渡し、ＩｎｔｅｒＲＡＴセル再選択、およびＵＴＲＡＮからのＩｎｔｅｒＲＡＴセル変更命令よりなる群から選択されたＩｎｔｅｒＲＡＴ手順が正常に完了したことを決定するステップと、

前記ＩｎｔｅｒＲＡＴ手順の正常な完了に呼応して、前記ワイヤレス機器内にＵＳＩＭが存在するか否かを決定するステップと、

前記ワイヤレス機器内に前記ＵＳＩＭが存在することの決定に呼応して、現行のＲＲＣ接続時にセキュリティキーセットが未使用であったか否かを決定するステップと、

前記現行のＲＲＣ接続時に前記セキュリティキーセットが未使用であった場合に、前記セキュリティキーセットに関連付けられたＣＮドメイン用のセキュリティＳＴＡＲＴ値として、前記ＵＳＩＭに所定の値を記憶させるステップと

を実施するために前記プロセッサによって実行可能なプログラムコードを含み、

前記所定の値は、セキュリティキーセットの削除をトリガするＴＨＲＥＳＨＯＬＤ値未満である、ワイヤレス機器。

【請求項１２】

請求項１１に記載のワイヤレス機器であって、

前記所定の値はゼロである、ワイヤレス機器。

【請求項１３】

請求項１１に記載のワイヤレス機器であって、さらに、

前記セキュリティＳＴＡＲＴ値を前記所定の値に設定するためのプログラムコードを備えるワイヤレス機器。

【請求項１４】

請求項１１に記載のワイヤレス機器であって、さらに、

前記ワイヤレス機器内にＳＩＭが存在する場合に、

現行のＲＲＣ接続時にセキュリティキーセットが未使用であったか否かを決定するステップと、

前記現行のＲＲＣ接続時に前記セキュリティキーセットが未使用であった場合に、前記セキュリティキーセットに関連付けられたＣＮドメイン用のセキュリティＳＴＡＲＴ値として、前記ＵＥに所定の値を記憶させるステップと

を実施するためのプログラムコードを備えるワイヤレス機器。

【請求項１５】

請求項１４に記載のワイヤレス機器であって、さらに、

ＣＮドメインに関連付けられたセキュリティＳＴＡＲＴ値が前記ＴＨＲＥＳＨＯＬＤ値以上である場合に、前記ＣＮドメインに関連付けられたセキュリティキーを前記ＳＩＭから削除するためのプログラムコードを備えるワイヤレス機器。

【請求項１６】

請求項１５に記載のワイヤレス機器であって、さらに、

前記ＣＮドメインに関連付けられたセキュリティキーセットであって、前記ＳＩＭに記憶され前記ＣＮドメインに関連付けられた前記セキュリティキーから得られたセキュリティキーセットを前記ＵＥから削除するためのプログラムコードを備えるワイヤレス機器。

【請求項１７】

請求項１５に記載のワイヤレス機器であって、さらに、

前記ＣＮドメインに関連付けられた前記セキュリティＳＴＡＲＴ値を前記所定の値に設定するためのプログラムコードを備えるワイヤレス機器。

【請求項１８】

請求項１７に記載のワイヤレス機器であって、さらに、

前記ＣＮドメインに関連付けられた前記セキュリティＳＴＡＲＴ値が前記ＴＨＲＥＳＨＯＬＤ値未満である場合に、前記ＣＮドメインに関連付けられた前記セキュリティＳＴＡＲＴ値を前記ＵＥに記憶させるためのプログラムコードを備えるワイヤレス機器。

【請求項１９】

請求項１８に記載のワイヤレス機器であって、さらに、

別のＣＮドメインに関連付けられたセキュリティＳＴＡＲＴ値を前記所定の値に設定し、前記別のＣＮドメインに関連付けられた前記セキュリティＳＴＡＲＴ値を前記ＵＥに記憶させるためのプログラムコードを備えるワイヤレス機器。

【請求項２０】

請求項１１に記載のワイヤレス機器であって、さらに、

前記セキュリティキーセットに関連付けられた前記ＣＮドメイン用の前記セキュリティＳＴＡＲＴ値が前記ＴＨＲＥＳＨＯＬＤ値を超え、且つ前記ＩｎｔｅｒＲＡＴ手順が前記ＩｎｔｅｒＲＡＴセル再選択手順または前記ＵＴＲＡＮからの前記ＩｎｔｅｒＲＡＴセル変更命令手順である場合に、前記セキュリティキーセットを削除するステップと、

前記セキュリティキーセットに関連付けられた前記ＣＮドメイン用の前記セキュリティＳＴＡＲＴ値が前記ＴＨＲＥＳＨＯＬＤ値未満であり、且つ前記ＩｎｔｅｒＲＡＴ手順が前記ＩｎｔｅｒＲＡＴセル再選択手順または前記ＵＴＲＡＮからのＩｎｔｅｒＲＡＴセル変更命令手順である場合に、前記セキュリティＳＴＡＲＴ値を前記ＵＳＩＭに記憶させるステップと

を実施するためのプログラムコードを備えるワイヤレス機器。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、ワイヤレス通信機器に関する。本発明は、特に、ワイヤレス通信機器の不揮発性メモリにセキュリティＳＴＡＲＴ値を記憶させることに関する。

【背景技術】

【０００２】

第３世代モバイル通信システム標準化プロジェクト（３ＧＰＰ）による標準規格である３ＧＰＰ　ＴＳ　２５．３３１　Ｖ３．１２．０（２００２／０９）「無線リソース制御（ＲＲＣ)プロトコル仕様」および３ＧＰＰ　ＴＳ　３３．１０２　Ｖ３．１２．０（２００２／０６）「セキュリティアーキテクチャ」は、ユニバーサルモバイル通信システム（ＵＭＴＳ）およびそれに関連するセキュリティプロトコルを技術的に記述したものである。これらの文献は、いずれも引用として本明細書に組み込まれる。ＵＭＴＳは、１つまたはそれ以上の基地局をともなったワイヤレス通信において使用されるユーザ機器（ＵＥ）と称される機器（通常はモバイル機器である）を開示する。これらの基地局（いわゆるノードＢｓ）は、対応する無線ネットワークコントローラ（ＲＮＣ）と共に、ＵＭＴＳ地上無線アクセスネットワークまたは略してＵＴＲＡＮと総称される。セキュリティの観点からは、ＵＥ側およびＵＴＲＡＮ側にある同位エンティティの無線リソース制御（ＲＲＣ）層が互いに無線アクセスリンクを確立し、ＲＲＣプロトコルデータユニット（ＰＤＵ）を使用してシグナリングおよびユーザデータの交換を行うのが一般的である。以下では、３ＧＰＰプロトコルを熟知していることを前提にして、上記文献３ＧＰＰ　ＴＳ　３３．１０２をもとにした背景技術の簡単な説明を行う。

【０００３】

先ず、図１を参照する。図１は、インテグリティ・アルゴリズムｆ９を使用してシグナリングメッセージのデータ・インテグリティを認証する様子を示している。ｆ９アルゴリズムに入力されるパラメータは、インテグリティ・キー（ＩＫ）、インテグリティ・シーケンス番号（ＣＯＵＮＴ－Ｉ）、ネットワーク側で生成されたランダム値（ＦＲＥＳＨ）、方向ビット（ＤＩＲＥＣＴＩＯＮ）、そしてＲＲＣ　ＰＤＵ内に保持されたシグナリングメッセージデータＭＥＳＳＡＧＥを含む。ワイヤレス機器は、これらの入力パラメータに基づき、インテグリティ・アルゴリズムｆ９を使用して、データ・インテグリティを検証するための認証コードＭＡＣ－Ｉを算出する。次に、ＭＡＣ－Ｉコードは、対応するシグナリングメッセージに付加された状態で、無線アクセスリンクを介して送信される。受信側は、送信側においてシグナリングメッセージをもとにしてＭＡＣ－Ｉを算出したのと同様な方法で、受信したシグナリングメッセージをもとにしてＸＭＡＣ－Ｉを算出し、算出したＸＭＡＣ－Ｉコードを受信したＭＡＣ－Ｉコードと比較することによって、受信し

たシグナリングメッセージのインテグリティを検証する。

【０００４】

次に、図２を参照する。図２は、図１に示されたＣＯＵＮＴ－Ｉ値のデータ構造を示したブロック図である。インテグリティ・シーケンス番号ＣＯＵＮＴ－Ｉは、長さが３２ビットである。ＣＯＵＮＴ－Ｉは、「短い」シーケンス番号と「長い」シーケンス番号の二部構成を採る。「短い」シーケンス番号は、ＣＯＵＮＴ－Ｉの下位ビットを構成し、「長い」シーケンス番号は、ＣＯＵＮＴ－Ｉの上位ビットを構成する。「短い」シーケンス番号は、各ＲＲＣ　ＰＤＵに含まれる４ビットのＲＲＣシーケンス番号ＲＲＣ　ＳＮである。「長い」シーケンス番号は、ＲＲＣ　ＳＮサイクルごとにインクリメントされる２８ビットのＲＲＣハイパーフレーム番号ＲＲＣ　ＨＦＮである。つまり、ＲＲＣ　ＨＦＮは、ＲＲＣ　ＰＤＵに含まれるＲＲＣ　ＳＮのロールオーバーが検出される際に、ＲＲＣ層によってインクリメントされる。ＲＲＣ　ＳＮがＲＲＣ　ＰＤＵと共に伝送されるのに対し、ＲＲＣ　ＨＦＮは伝送されず、その代わりにワイヤレス機器およびＵＴＲＡＮの同位エンティティＲＲＣ層によって維持される。

【０００５】

ＲＲＣ　ＨＦＮは、上記文献３ＧＰＰ　ＴＳ　３３．１０２のセクション６．４．８に記述されたパラメータＳＴＡＲＴによって初期設定される。ＵＥおよびＵＥを割り当てられたＲＮＣは、ＲＲＣ　ＨＦＮのうち２０個の最上位ビットをＳＴＡＲＴ値に初期設定する。ＲＲＣ　ＨＦＮの残りのビットは、ゼロに初期設定される。

【０００６】

次に、図３を参照する。図３は、ユーザおよびシグナリングデータを無線アクセスリンクを通して暗号化する様子を示している。インテグリティ・チェックの場合と同様に、暗号化アルゴリズムｆ８に入力されるパラメータは、暗号化キーＣＫ、時間依存性の入力値ＣＯＵＮＴ－Ｃ、ベアラＩＤであるＢＥＡＲＥＲ、伝送方向ＤＩＲＥＣＴＩＯＮ、そして必要とされるキーストリームの長さ値ＬＥＮＧＴＨを含む。これらの入力パラメータにもとづいて、ｆ８アルゴリズムは、出力キーストリームＫＥＹＳＴＲＥＡＭ　ＢＬＯＣＫを生成する。これは、入力された平文ブロックＰＬＡＩＮＴＥＸＴを暗号化し、出力用の暗号文ブロックＣＩＰＨＥＲＴＥＸＴを生成するために使用される。入力パラメータＬＥＮＧＴＨは、ＫＥＹＳＴＲＥＡＭ　ＢＬＯＣＫの長さのみに影響し、ＫＥＹＳＴＲＥＡＭ　ＢＬＯＣＫの実際のビットには影響しない。

【０００７】

暗号化シーケンス番号ＣＯＵＮＴ－Ｃは、長さが３２ビットである。無線リンク制御（ＲＬＣ）の肯定応答モード（ＡＭ）接続またはＲＬＣ否定応答（ＵＭ）モード接続では、ＣＯＵＮＴ－Ｃ値はアップリンク無線ベアラごとに１つずつのＣＯＵＮＴ－Ｃ値と、ダウンリンク無線ベアラごとに１つずつのＣＯＵＮＴ－Ｃ値とが存在する。ＲＬＣ層はＲＲＣ層の下位層であり、第２層のインターフェースだとみなして良い。ＣＯＵＮＴ－Ｃは、同じコアネットワーク（ＣＮ）ドメインのあらゆる透過モード（ＴＭ）ＲＬＣ無線ベアラに対して同一であり、アップリンクＴＭ接続およびダウンリンクＴＭ接続のいずれに対しても同一である。

【０００８】

次に、図４を参照する。図４は、図３に示されたＣＯＵＮＴ－Ｃ値を各接続モードごとに示したブロック図である。ＣＯＵＮＴ－Ｃは、「短い」シーケンス番号と「長い」シーケンス番号の二部構成を採る。「短い」シーケンス番号は、ＣＯＵＮＴ－Ｃの下位ビットを構成し、「長い」シーケンス番号は、ＣＯＵＮＴ－Ｃの上位ビットを構成する。ＣＯＵＮＴ－Ｃの更新は、以下で述べるように、伝送モードに依存する。

・伝送モードが専用チャネル（ＤＣＨ）上のＲＬＣ　ＴＭであるとき、「短い」シーケンス番号は、ＣＯＵＮＴ－Ｃの８ビットの接続フレーム番号（ＣＦＮ）である。この番号は、ＵＥのＭＡＣ－ｄエンティティおよびサービングＲＮＣ（ＳＲＮＣ）のＭＡＣ－ｄエンティティにおいて、それぞれ別個に維持される。ＳＲＮＣは、ＵＥを割り当てられたＲＮＣであり、ＵＥは、ＳＲＮＣを通してネットワークとの通信を行う。「長い」シーケン

ス番号は、ＣＦＮサイクルごとにインクリメントされる２４ビットのＭＡＣ－ｄ　ＨＦＮである。

・伝送モードがＲＬＣ　ＵＭモードであるとき、「短い」シーケンス番号は、ＲＬＣ　ＵＭ　ＰＤＵヘッダから得られた７ビットのＲＬＣシーケンス番号（ＲＬＣ　ＳＮ）である。「長い」シーケンス番号は、ＲＬＣ　ＳＮサイクルごとにインクリメントされる２５ビットのＲＬＣ　ＵＭ　ＨＦＮである。ＲＬＣ　ＨＦＮは、この点ではＲＲＣ　ＨＦＮに類似しているが、ワイヤレス機器のＲＬＣ層（ＵＥ側およびＲＮＣ側の両方）によって維持される点が異なる。

・伝送モードがＲＬＣ　ＡＭモードであるとき、「短い」シーケンス番号は、ＲＬＣ　ＡＭ　ＰＤＵヘッダから得られた１２ビットのＲＬＣシーケンス番号（ＲＬＣ　ＳＮ）である。「長い」シーケンス番号は、ＲＬＣ　ＳＮサイクルごとにインクリメントされる２０ビットのＲＬＣ　ＡＭ　ＨＦＮである。

【０００９】

このハイパーフレーム番号（ＨＦＮ）は、上記文献３ＧＰＰ　ＴＳ　３３．１０２のセクション６．４．８に記述されたパラメータＳＴＡＲＴによって初期設定される。ＵＥおよびＲＮＣは、ＲＬＣ　ＡＭ　ＨＦＮ、ＲＬＣ　ＵＭ　ＨＦＮ、ＭＡＣ－ｄ　ＨＦＮの２０個の最上位ビットをＳＴＡＲＴに初期設定する。ＲＬＣ　ＡＭ　ＨＦＮ、ＲＬＣ　ＵＭ　ＨＦＮ、ＭＡＣ－ｄ　ＨＦＮの残りのビットは、ゼロに初期設定される。

【００１０】

暗号化／インテグリティ・キーを生成する認証およびキーに関する同意は、呼び出しセットアップにおいて必須ではないので、欠陥のあるキーが、無制限に且つ悪意的に再利用される可能性がある。したがって、特定の暗号化／インテグリティ・キーの組み合わせが際限なく使用されることを避け、欠陥のあるキーを使用した攻撃を回避するためのメカニズムが必要である。このため、ＵＥの不揮発性メモリであるＵＳＩＭは、アクセスリンクキーセットによって保護されるデータの量を制限するメカニズムを含んでいる。

【００１１】

ＣＮは、回線交換（ＣＳ）ドメインおよびパケット交換（ＰＳ）ドメインという、２つの別個のドメインに分割される。ＲＲＣ接続が解放されるたびに、そのＲＲＣ接続に保護されていたベアラの$START_{CS}$値および$START_{PS}$値は、最大値であるＴＨＲＥＳＨＯＬＤと比較される。$START_{CS}$は、ＣＳドメイン用のＳＴＡＲＴ値である。$START_{PS}$は、ＰＳドメイン用のＳＴＡＲＴ値である。$START_{CS}$および$START_{PS}$の両方または一方が最大値ＴＨＲＥＳＨＯＬＤに達すると、ＵＥは、その$START_{CS}$および$START_{PS}$の両方または一方をＴＨＲＥＳＨＯＬＤに設定することによって、ＵＳＩＭに記憶された対応するＣＮドメイン用のＳＴＡＲＴ値を無効としてマーク付けする。ＵＥは、次に、ＵＳＩＭに記憶された暗号化キーおよびインテグリティ・キーを削除して、キーセット識別子（ＫＳＩ）を無効に設定する（ＳＧＰＰ　ＴＳ　３３．１０２のセクション６．４．４を参照のこと）。それ以外の場合は、$START_{CS}$および$START_{PS}$はＵＳＩＭに記憶される。ＳＴＡＲＴ値の計算は、ＳＧＰＰ　ＴＳ　２５．３３１のセクション８．５．９に記述されており、通常は、該当ドメイン内の最大のＣＯＵＮＴ－Ｃ値またはＣＯＵＮＴ－Ｉ値の最上位ビットをもとにして得られる。最大値ＴＨＲＥＳＨＯＬＤは、オペレータによって設定され、ＵＳＩＭに記憶される。

【００１２】

次のＲＲＣ接続が確立されると、それに適したドメイン用のＳＴＡＲＴ値がＵＳＩＭから読み出される。そして、$START_{CS}$および$START_{PS}$の両方または一方が最大値ＴＨＲＥＳＨＯＬＤに達すると、ＵＥは、対応するコアネットワークドメイン用の新しいアクセスリンクキーセット（暗号化キーおよびインテグリティ・キー）の生成をトリガする。

【００１３】

特定のサービングネットワークドメイン（ＣＳまたはＰＳ）用の無線通信が確立されるとき、ＵＥは、$START_{CS}$および$START_{PS}$の値をＲＲＣ接続セットアップ完了

メッセージに含ませてＲＮＣに送信する。ＵＥは、次に、ＳＴＡＲＴ$_{CS}$およびＳＴＡＲＴ$_{PS}$をＴＨＲＥＳＨＯＬＤに設定することによって、ＵＳＩＭ内のＳＴＡＲＴ値を無効としてマーク付けする。このようなマーク付けが行われるのは、新しいＳＴＡＲＴ値をＵＳＩＭに書き込む前にＵＥの電源が切れた場合またはＵＥが不能になった場合にＳＴＡＲＴ値が不本意に再利用される事態を回避するためである。

【００１４】

また、３ＧＰＰ　ＴＳ　２５．３３１のセクション８．３．７、８．３．９、８．３．１１、８．５．２にも、ＳＴＡＲＴ値をいつＵＳＩＭに記憶させるかに関する記載がある。

【００１５】

３ＧＰＰプロトコルは、ＵＥを別のワイヤレスプロトコルに切り替えることができる。別のワイヤレスプロトコルとしては、例えば、モバイル通信用グローバルシステム（ＧＭＳ）プロトコル等が挙げられ、このような切り替えは、様々な相互無線アクセス技術（ＩｎｔｅｒＲＡＴ）手順の１つによって実施される。次に、図５を参照する。図５は、進行中のＩｎｔｅｒＲＡＴ手順を簡単に示したブロック図である。先ず、ＵＥ２０は、３ＧＰＰ　ＵＴＲＡＮ１０との間にＲＲＣ接続２１を確立された状態にある。ＲＲＣ接続２１は、ＣＳドメイン１２またはＰＳドメイン１４のいずれにあっても良いが、どのＩｎｔｅｒＲＡＴ手順でもＣＳドメイン１２にあるのが通常であるので、以下ではこのような想定のもとで話を進めるものとする。ＵＥ２０が、ＧＳＭネットワーク３０の領域に近づくにつれて、ＵＴＲＡＮ１０では、ＵＥ２０をＧＳＭネットワーク３０に切り替えるか否かに関する決定が下される。ＩｎｔｅｒＲＡＴ手順が正常に完了すると、ＵＥ２０とＧＳＭネットワーク３０との間には、接続２３が確立される。そして、ＵＴＲＡＮとの間の接続２１はドロップされる。したがって、ＵＥ２０のＵＥＩＭに含まれるＳＴＡＲＴ値を更新する必要が生じる。つまり、この実施例では、ＵＳＩＭに含まれるＳＴＡＲＴ$_{CS}$値を更新する必要が生じる。

【００１６】

ＳＴＡＲＴ値は、特定の暗号化／インテグリティ・キーがＵＥ２０とＵＴＲＡＮ１０との間でどれだけ長く使用されているかを反映することが望ましい。しかしながら、現行の３ＧＰＰプロトコルは、ＩｎｔｅｒＲＡＴ引き渡し、ＩｎｔｅｒＲＡＴセル再選択、そしてＵＴＲＡＮからのＩｎｔｅｒＲＡＴセル変更命令等のＩｎｔｅｒＲＡＴ手順時におけるＳＴＡＲＴ値の処理が正確でない。例として、３ＧＰＰ　ＴＳ　２５．３３１のセクション８．３．７．４に明記されるように、ＩｎｔｅｒＲＡＴ引き渡しが正常に完了した際にＵＥによって実施されるステップを考える。ＵＥは、ＩｎｔｅｒＲＡＴ引き渡しが正常に完了した際に、これらのステップを経てＳＴＡＲＴ値を処理することが望ましい。

１＞　ＵＳＩＭが存在する場合は、

２＞　各ＣＮドメイン用の現行のＳＴＡＲＴ値をＵＳＩＭ［５０］に記憶させ、

２＞　あるＣＮドメイン用にＵＳＩＭ［５０］に記憶された「ＳＴＡＲＴ」が可変値ＳＴＡＲＴ＿ＴＨＲＥＳＨＯＬＤの値「ＴＨＲＥＳＨＯＬＤ」以上である場合は、

３＞　そのＣＮドメイン用にＵＳＩＭに記憶された暗号化キーおよびインテグリティ・キーを削除し、

３＞　これらのキーを削除した旨を上層に通知する。

１＞　ＳＩＭが存在する場合は、

２＞　各ドメイン用の現行のＳＴＡＲＴ値をＵＥに記憶させ、

２＞　あるＣＮドメイン用にＵＥに記憶された「ＳＴＡＲＴ」が可変値ＳＴＡＲＴ＿ＴＨＲＥＳＨＯＬＤの値「ＴＨＲＥＳＨＯＬＤ」以上である場合は、

３＞　そのＣＮドメイン用にＳＩＭに記憶された暗号化キーおよびインテグリティ・キーを削除し、

３＞　これらのキーを削除した旨を上層に通知する。

【００１７】

前述したように、ＳＴＡＲＴ値がＵＳＩＭから読み出されるごとに、ＵＥは、そのＳＴ

ＡＲＴ値をＴＨＲＥＳＨＯＬＤと等しい値に設定することによって、そのＵＳＩＭ内のＳＴＡＲＴ値を無効としてマーク付けし、同じセキュリティ構成が意図に反して再利用される事態を回避する。特定のサービングネットワークドメイン（ＣＳまたはＰＳ）用に無線接続が確立されると、ＵＥは、ＳＴＡＲＴ値（ＣＳまたはＰＳ）をＲＲＣ接続セットアップ完了メッセージに含ませてＲＮＣに送信する。ＳＴＡＲＴ値がＴＨＲＥＳＨＯＬＤに等しい場合は、ネットワークは、新しいキーセット（ＣＳまたはＰＳ）を割り当てる。セキュリティプロトコルによるキー同期化の処理方法によれば、ＵＥは、そのＲＲＣ接続用に古いキーセットを使用しつつ新しいキーセットを取得することができる。このような状況下では、新しいキーセットが使用可能であるにもかかわらず、現行のＳＴＡＲＴ値はＴＨＲＥＳＨＯＬＤ値を超える極めて大きい値をとる。ＩｎｔｅｒＲＡＴ引き渡し、ＩｎｔｅｒＲＡＴセル再選択、またはＵＴＲＡＮからのＩｎｔｅｒＲＡＴセル変更命令手順では、この点が考慮されていない。これら３種類の手順において、割り当てられた新しいキーセットが使用されていない場合は、ＵＥは以下のステップを経る。

１）　ＵＳＩＭが存在することを決定し、
２）　ＳＴＡＲＴ値をＵＳＩＭに記憶させ、
３）　記憶されたＳＴＡＲＴ値がＴＨＲＥＳＨＯＬＤ値を超えることを決定し、
４）　暗号化キーおよびインテグリティ・キーを削除し、
５）　削除した旨を上層に通知する。

【００１８】

上記の手順では新しいキーセットが除去されるが、これは全く不要である。キーセットは無線リソースであり、可能な限り効率良く使用して節約することが望まれる。さらに、上記の手順では、新しいキーセットの構築が強制される。キーセットは無線インターフェースを通じて伝送されるので、キーセットの不要な割り当ては無線リソースの無駄遣いでもある。

【発明の開示】

【００１９】

したがって、本発明の目的は、ＩｎｔｅｒＲＡＴ引き渡し、ＩｎｔｅｒＲＡＴセル再選択、またはＵＴＲＡＮからのＩｎｔｅｒＲＡＴセル変更命令におけるＵＥによるＳＴＡＲＴ値の処理を正し、新しいキーセットが不要に削除される事態を回避することにある。

【００２０】

本発明の好ましい実施形態は、簡単に言えば、ＩｎｔｅｒＲＡＴ手順における新しいキーセットの削除を回避できるようにＳＴＡＲＴ値を処理する方法およびそれに関連するワイヤレス機器を提供する。ワイヤレス機器は、先ず、ＩｎｔｅｒＲＡＴ引き渡し、ＩｎｔｅｒＲＡＴセル再選択、またはＵＴＲＡＮからのＩｎｔｅｒＲＡＴセル変更命令のいずれかを正常に完了させる。ワイヤレス機器は、次に、ＵＳＩＭが存在するか否かを決定する。ＵＳＩＭが存在する場合は、ワイヤレス機器は、新しいキーセットが受信されたか否か、そしてそのキーセットが現行のＲＲＣ接続時に暗号化機能およびインテグリティ機能のために使用されたか否かを決定する。新しいキーセットが存在し且つ未使用である場合は、ワイヤレス機器は、そのＲＲＣ接続に関連付けられたＣＮドメイン用のセキュリティＳＴＡＲＴ値として、ゼロの値をＵＳＩＭに記憶させる。

【００２１】

本発明による利点は、対象となるＲＲＣ接続用に新しく且つ未使用なキーセットが存在するか否かをチェックすることによって、過度に大きいＳＴＡＲＴ値がＵＳＩＭに書き込まれる事態を回避できることにある。したがって、新しいキーセットが削除されるのを阻止し、無線リソースを節約することが可能である。

【００２２】

当業者ならば、各種の図面に例示された好ましい実施形態に関する以下の詳細な説明を読むことによって、本発明の上記の目的およびその他の目的を明白に理解することができる。

【発明を実施するための最良の形態】

【００２３】
先ず、図６を参照する。図６は、本発明の好ましい一実施形態にしたがったワイヤレス機器１００を簡単に示したブロック図である。ワイヤレス機器１００は、入出力（Ｉ／Ｏ）ハードウェア１１０と、当該分野において周知の形で共に中央処理装置（ＣＰＵ）１３０に接続され且つその制御下にあるワイヤレストランシーバ１２０およびメモリ１４０と、を備える。Ｉ／Ｏハードウェア１１０は、例えば、出力用のディスプレイおよびスピーカと、入力用のキーパッドおよびマイクロフォンと、を備えても良い。ワイヤレストランシーバ１２０は、ワイヤレス機器１００によるワイヤレス信号の送受信を可能にする。ＣＰＵ１３０は、メモリ１４０に含まれ且つＣＰＵ１３０によって実行可能であるプログラムコード１４２にしたがって、ワイヤレス機器１００の機能性を制御する。ワイヤレス機器１００は、大部分が従来技術と同一であるが、本発明による方法を実現するために、プログラムコード１４２に変更が加えられている。このような変更を、どのようにしてプログラムコード１４２に加えるかに関しては、当業者ならば、以下の詳細な説明を読むことによって明らかである。

【００２４】
従来技術と同様に、本発明によるワイヤレス機器１００は、ＩｎｔｅｒＲＡＴ手順を実施して３ＧＰＰプロトコルをＧＳＭ等の別のプロトコルに切り替えることができる。このためには、ワイヤレス機器１００は、先ず、ＵＴＲＡＮとの間に無線リソース制御（ＲＲＣ）接続を確立する必要がある。このＲＲＣ接続は、ＰＳドメインまたはＣＳドメインのいずれかにあって良い。ワイヤレス機器は、次に、ＩｎｔｅｒＲＡＴ手順を実施する。ＩｎｔｅｒＲＡＴ手順は、ＩｎｔｅｒＲＡＴ引き渡し手順、ＩｎｔｅｒＲＡＴセル再選択手順、またはＵＴＲＡＮからのＩｎｔｅｒＲＡＴセル変更命令手順のいずれかであって良い。ＲＲＣ接続手順およびＩｎｔｅｒＲＡＴ手順は、従来技術のそれらと同一であるので、ここでは詳細な説明を省くものとする。ＩｎｔｅｒＲＡＴ手順が正常に完了すると、ワイヤレス機器１００は、次に、本発明による方法のステップを実施する。ワイヤレス機器１００は、ＩｎｔｅｒＲＡＴ手順が正常に完了した後に、以下のステップを経ることが望ましい。

１＞　ＵＳＩＭが存在する場合は、各ＣＮドメインに対し、
２＞　このＣＮドメイン用に新しいセキュリティキーセットが受信されたが、この新しいキーセットがこのＲＲＣ接続時にインテグリティ保護または暗号化のために使用されなかった場合は、
３＞　このドメイン用のＳＴＡＲＴ値をゼロに設定し、
３＞　このドメイン用のこのＳＴＡＲＴ値をＵＳＩＭに記憶させる。
２＞　さもなければ、
３＞　あるＣＮドメイン用の所定の式によって決定された現行の「ＳＴＡＲＴ」値が可変値ＳＴＡＲＴ＿ＴＨＲＥＳＨＯＬＤの値「ＴＨＲＥＳＨＯＬＤ」以上である場合は、
４＞　そのＣＮドメイン用にＵＳＩＭに記憶された暗号化キーおよびインテグリティ・キーを削除し、
４＞　これらのキーを削除した旨を上層に通知する。
３＞　さもなければ、
４＞　このＣＮドメイン用の現行の「ＳＴＡＲＴ」値をＵＳＩＭに記憶させ、
１＞　さもなければ、
２＞　ＳＩＭが存在する場合は、各ＣＮドメインに対し、
３＞　このＣＮドメイン用に新しいセキュリティキーセットが受信されたが、この新しいキーセットがこのＲＲＣ接続時にインテグリティ保護または暗号化のために使用されなかった場合は、
４＞　そのドメイン用のＳＴＡＲＴ値をゼロに設定し、
４＞　そのドメイン用のこのＳＴＡＲＴ値をＵＥに記憶させる。
３＞　さもなければ、

４＞　あるＣＮドメイン用の所定の式によって決定された現行の「ＳＴＡＲＴ」値が可変値ＳＴＡＲＴ＿ＴＨＲＥＳＨＯＬＤの値「ＴＨＲＥＳＨＯＬＤ」以上である場合は、

５＞　ＳＩＭに記憶されたＫｃキーを削除し、

５＞　そのＣＮドメイン用にＵＥに記憶された暗号化キーおよびインテグリティ・キーを削除し、

５＞　両ＣＮドメイン用の「ＳＴＡＲＴ」値をゼロに設定し、それらの値をＵＥに記憶させ、

５＞　これらのキーを削除した旨を上層に通知する。

４＞　さもなければ、

５＞　各ＣＮドメイン用の現行の「ＳＴＡＲＴ」値をＵＥに記憶させる。

【００２５】

図７Ａおよび図７Ｂは、本発明による方法の上記ステップを示したフローチャートである。本発明によるステップが完了したら、ＵＥは、当然ながら、その先に進んで他の多くの手順を実施しなければならない。ただし、これらの手順は従来技術と同一であるので、本発明の範囲外である。なお、本発明は、従来技術による所定の方法を利用してドメイン内のＳＴＡＲＴ値を計算するとともに、従来技術によるＴＨＲＥＳＨＯＬＤ関連の構造、ＵＳＩＭ関連の構造、そしてＳＩＭ関連の構造をも利用する。

【００２６】

本発明において特に重要なのは、図７Ａに示したステップ２００である。現行では、ＰＳドメインとＣＳドメインの２つのドメインのみが存在するので、ステップ２００は、ＰＳドメイン用に一度、ＣＳドメイン用に一度の二度実行される。ＣＳドメインは、自己の構造、すなわちＣＳ領域１４１をメモリ１４０内に有する。同様に、ＰＳドメインは、ＰＳ領域１４３をメモリ１４０内に有する。これらの領域１４１，１４３は、メモリ１４０内において連続している必要はない。すなわち、これらの領域１４１，１４３は、メモリ１４０内において分散していて良い。ステップ２００は、現行のＲＲＣ接続時においてまだセキュリティ目的で未使用である新しいキーセット１４１ｎ，１４３ｎを、当該ドメインが既に受信しているか否かをチェックする。現行のＲＲＣ接続とは、ＵＥ１００とＵＴＲＡＮとの間で開始された接続であって、ＵＥによって現在処理中であるＩｎｔｅｒＲＡＴ手順の１つが正常に完了することによって終結される接続のことである。新しく受信されたキーセット１４１ｎ，１４３ｎがセキュリティ目的で使用されたか否かを決定する方法は、当該技術分野において既知であるので、ここでは詳細な説明を省くものとする。ただし、新しいキーセット１４１ｎ，１４３ｎは、一般に、データの暗号化に使用されておらず、また、データ・インテグリティのチェック値を提供するためにも使用されていない場合に未使用であるとみなされる。また、新しく受信されたキーセット１４１ｎ，１４３ｎは、現行のＲＲＣ接続時に受信されたキーセット、または現行のＲＲＣ接続に呼応して受信されたキーセットであると考えられる。前述したように、ＵＥ１００は、古いキーセット１４１ｏ，１４３ｏを使用しつつ新しいキーセット１４１ｎ，１４３ｎを取得することが可能である。なお、これらのキーセット１４１ｎ，１４１ｏ，１４３ｎ，１４３ｏは、（図１に示すような）インテグリティ・キーＩＫおよび（図３に示すような）暗号化キーＣＫの両方を含む。新しく受信されたキーセット１４１ｎ，１４３ｎが未使用である場合は、対応するＳＴＡＲＴ値１４１ｓ，１４３ｓがゼロに設定される。そして、ゼロ設定されたこのＳＴＡＲＴ値１４１ｓ，１４３ｓは、ＵＳＩＭ１４４メモリに記憶される。ゼロという値が好まれるのは、ＳＴＡＲＴ値を最大限に活用するためである。ゼロの代わりに他の非ゼロ値を使用することも可能である。ただし、この場合はＳＴＡＲＴ値および関連のキーセットの寿命が短くなる。ＵＳＩＭ１４４は、単に、３ＧＰＰプロトコル用に特別に設計された不揮発性メモリ構造であって良い。なお、$START_{CS}$値１４１ｓおよび$START_{PS}$値１４３ｓは、実装例によってはＵＳＩＭ１４４内に含まれて良い場合もある。つまり、ドメインＳＴＡＲＴ値を複製しなくて良い場合もある。図６は、最も一般的な実装例を簡単に示している。

【００２７】
従来技術と異なり、本発明は、ＩｎｔｅｒＲＡＴ手順が正常に完了した後、且つドメインＳＴＡＲＴ値がチェックされる前に、新しいキーセットが未使用であるか否かを決定する検証ステップを設けている。新しいキーセットが未使用である場合は、ドメインＳＴＡＲＴ値はゼロに設定される。本発明は、このようにして、ＩｎｔｅｒＲＡＴ手順による新しいキーセットの削除を回避し、無線リソースの節約を図っている。
【００２８】
当業者ならば、本発明の教示内容から逸脱することなく、上記方法からの多数の変更形態および代替形態を容易に見いだせると考えられる。したがって、上記の開示内容は、添付した特許請求の範囲の境界によってのみ限定されることが望ましい。
【図面の簡単な説明】
【００２９】
【図１】インテグリティ・アルゴリズムｆ９を使用してシグナリングメッセージのデータ・インテグリティを認証する様子を示した図である。
【図２】図１に示されたＣＯＵＮＴ－Ｉ値のデータ構造を示したブロック図である。
【図３】ユーザおよびシグナリングデータを無線アクセスリンクを介して暗号化する様子を示した図である。
【図４】図３に示されたＣＯＵＮＴ－Ｃ値を各接続モードごとに示したブロック図である。
【図５】ＩｎｔｅｒＲＡＴ手順を簡単に示したブロック図である。
【図６】本発明の好ましい一実施形態にしたがったワイヤレス機器１００を簡単に示したブロック図である。
【図７Ａ】本発明による方法のステップを示したフローチャートである。
【図７Ｂ】本発明による方法のステップを示したフローチャートである。
【符号の説明】
【００３０】
１０...３ＧＰＰ　ＵＴＲＡＮ
１２...ＣＳドメイン
１４...ＰＳドメイン
２０...ＵＥ
２１...ＲＲＣ接続
２３...接続
３０...ＧＳＭネットワーク
１００...ワイヤレス機器
１１０...Ｉ／Ｏハードウェア
１２０...ワイヤレストランシーバ
１３０...ＣＰＵ
１４０...メモリ
１４１...ＣＳ領域
１４２...プログラムコード
１４３...ＰＳ領域
１４１ｎ，１４３ｎ...新しいキーセット
１４１ｏ，１４３ｏ...古いキーセット
１４１ｓ，１４３ｓ...ＳＴＡＲＴ値
１４４...ＵＳＩＭ

【図１】

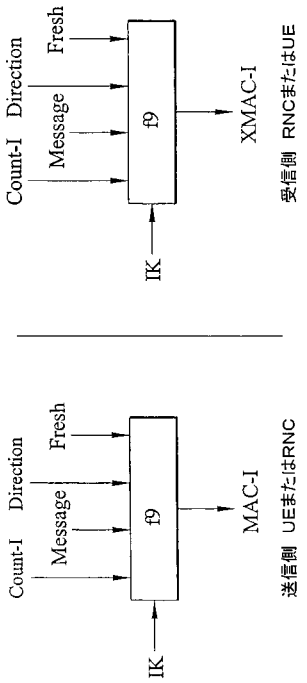

FIG. 1

【図２】

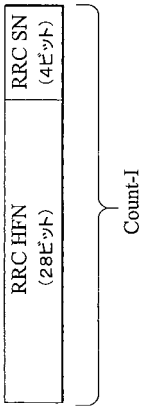

FIG. 2

【図３】

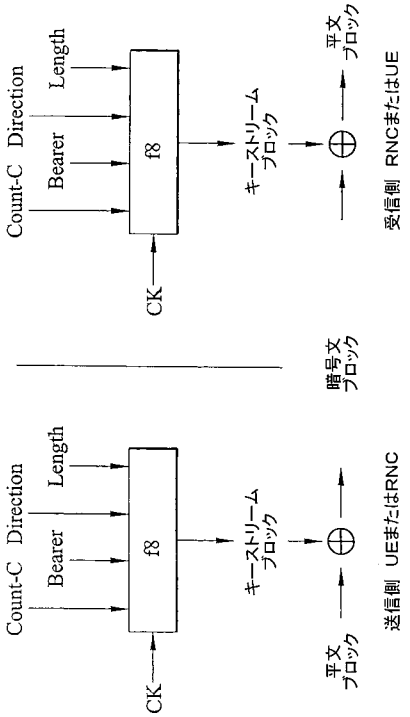

FIG. 3

【図４】

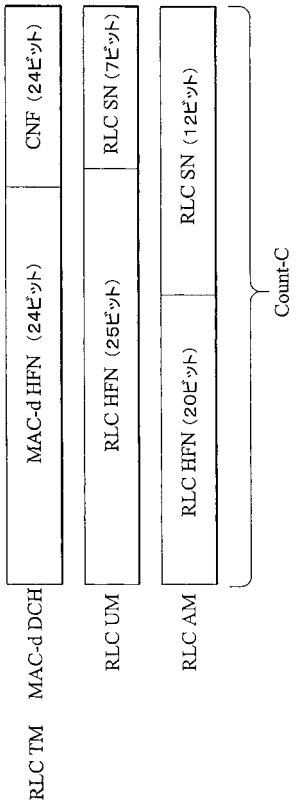

FIG. 4

【図５】

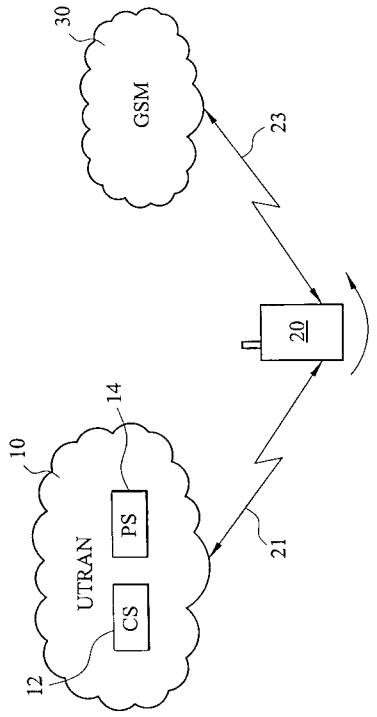

FIG. 5

【図６】

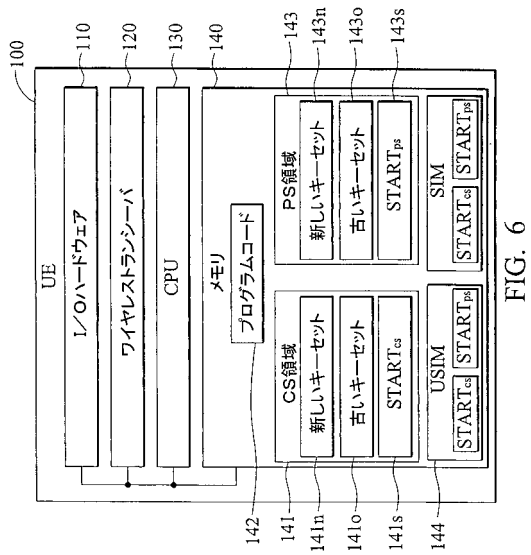

FIG. 6

【図７Ａ】

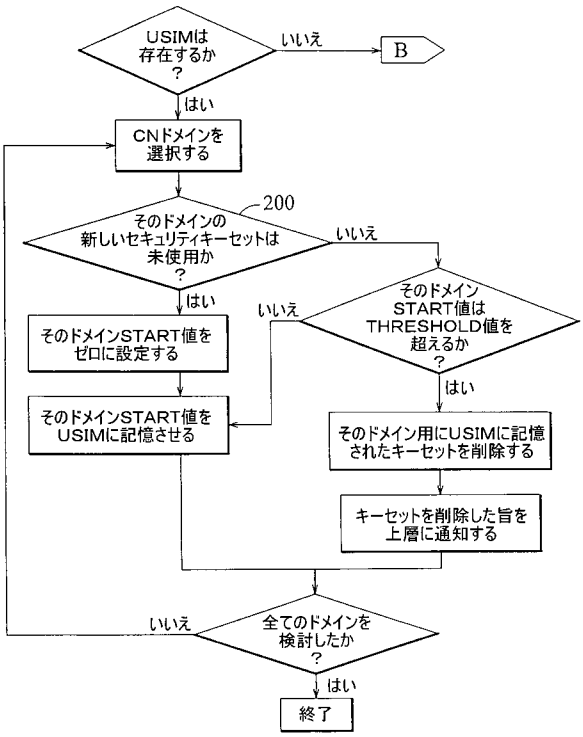

FIG. 7A

【図７Ｂ】

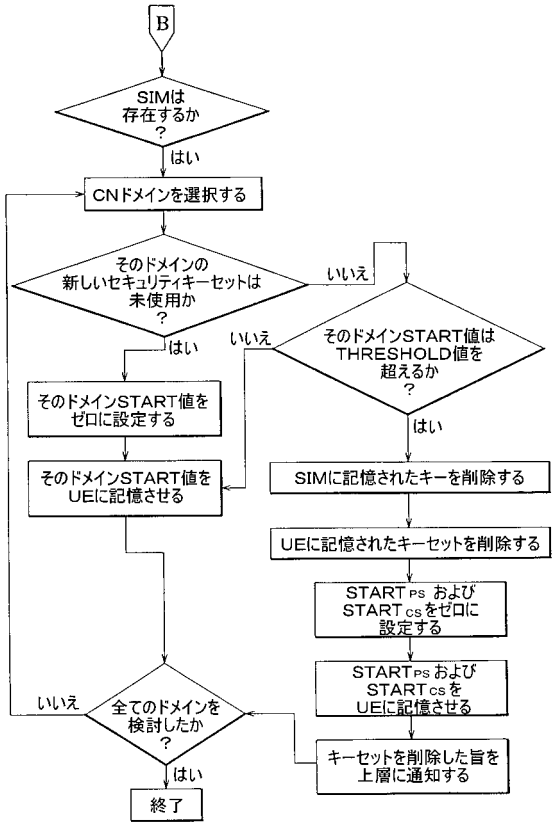

FIG. 7B

フロントページの続き

(58)調査した分野(Int.Cl., ＤＢ名)
Ｈ０４Ｂ７／２４－７／２６
Ｈ０４Ｑ７／００－７／３８