(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7223022号
(P7223022)

(45)発行日　令和5年2月15日(2023.2.15)

(24)登録日　令和5年2月7日(2023.2.7)

(51)国際特許分類

		FI	
H04W	*12/126 (2021.01)*	H04W	12/126
H04W	*24/00 (2009.01)*	H04W	24/00
H04W	*12/122 (2021.01)*	H04W	12/122
H04W	*92/24 (2009.01)*	H04W	92/24

請求項の数　11　（全27頁）

(21)出願番号　特願2020-552791(P2020-552791)
(86)(22)出願日　平成31年3月27日(2019.3.27)
(65)公表番号　特表2021-517426(P2021-517426A)
(43)公表日　令和3年7月15日(2021.7.15)
(86)国際出願番号　PCT/CN2019/079840
(87)国際公開番号　WO2019/192366
(87)国際公開日　令和1年10月10日(2019.10.10)
審査請求日　令和2年9月29日(2020.9.29)
(31)優先権主張番号　201810299619.5
(32)優先日　平成30年4月4日(2018.4.4)
(33)優先権主張国・地域又は機関
中国(CN)
前置審査

(73)特許権者　510065207
大唐移▲動▼通信▲設▼▲備▼有限公司
ＤＡＴＡＮＧ ＭＯＢＩＬＥ ＣＯＭＭＵＮＩＣＡＴＩＯＮＳ ＥＱＵＩＰＭＥＮＴ ＣＯ．，ＬＴＤ．
中華人民共和国、北京市海淀区上地▲東▼路５号院１号楼１▲層▼１００００８５
１／Ｆ，Ｂｕｉｌｄｉｎｇ １，Ｎｏ．５ Ｓｈａｎｇｄｉ Ｅａｓｔ Ｒｏａｄ，Ｈａｉｄｉａｎ Ｄｉｓｔｒｉｃｔ，Ｂｅｉｊｉｎｇ １００００８５，Ｃｈｉｎａ
(74)代理人　100108453
弁理士　村山 靖彦
(74)代理人　100110364

最終頁に続く

(54)【発明の名称】　端末（ＵＥ）の管理と制御のための方法および装置

(57)【特許請求の範囲】

【請求項１】

ＵＥの動作情報を取得するステップと、

前記動作情報を分析して、前記ＵＥのセキュリティリスクを決定するステップと、

ネットワーク内の少なくとも１つのネットワーク機能エンティティに第１の指示を送信し、前記ＵＥに対するポリシー更新またはパラメーター調整を実行するように、前記少なくとも１つのネットワーク機能エンティティをトリガーするステップを備え、

前記第１の指示は、前記ＵＥの直面するセキュリティリスクのタイプを示し、または、前記ＵＥのセキュリティリスクを解決するためのポリシーまたはパラメーターを示すことを特徴とするネットワークデータ分析機能（ＮＷＤＡＦ）エンティティに適用される、端末（ＵＥ）の管理と制御のための方法。

【請求項２】

前記ＵＥのセキュリティリスクを解決するためのポリシーまたはパラメーターは、前記ＵＥのモビリティ管理パラメーターおよび／またはセッション管理パラメーターを含むことを特徴とする請求項１に記載のネットワークデータ分析機能（ＮＷＤＡＦ）エンティティに適用される、端末（ＵＥ）の管理と制御のための方法。

【請求項３】

前記動作情報は、前記ＵＥの端末タイプ、端末位置、端末モビリティ情報、アプリケーション情報およびＵＥの宛先アドレスのうちの１つまたは複数を含むことを特徴とする請求項１に記載のネットワークデータ分析機能（ＮＷＤＡＦ）エンティティに適用される、

端末（ＵＥ）の管理と制御のための方法。
【請求項４】
前記動作情報を分析して、前記ＵＥのセキュリティリスクを決定することは、
前記端末タイプが、前記ＵＥがモノのインターネット（ＩｏＴ）機器であり、前記ＵＥが事前設定された固定エリアから出たことを示す場合、盗難セキュリティリスクが前記ＵＥに存在すると決定し、または、
前記端末タイプが、前記ＵＥがモノのインターネット（ＩｏＴ）機器であり、前記ＵＥが禁止エリアに位置していることを示す場合、不正使用されるセキュリティリスクが前記ＵＥに存在すると決定し、または、
前記端末タイプが、前記ＵＥがモノのインターネット（ＩｏＴ）機器であり、前記ＵＥがトラフィック使用において異常であることを示す場合、ハッカーによってハイジャックされるセキュリティリスクがＵＥに存在すると決定し、または、
前記端末タイプが、前記ＵＥがモノのインターネット（ＩｏＴ）機器であり、前記ＵＥが不正なターゲットアドレスにアクセスしていることを示す場合、ハッカーによってハイジャックされるセキュリティリスクがＵＥに存在すると決定することを特徴とする請求項３に記載のネットワークデータ分析機能（ＮＷＤＡＦ）エンティティに適用される、端末（ＵＥ）の管理と制御のための方法。
【請求項５】
前記ネットワーク内の少なくとも１つのネットワーク機能エンティティに第１の指示を送信することは、
ポリシー制御機能（ＰＣＦ）にアクセスおよびモビリティ管理ポリシー、および／または、プロトコルデータユニット（ＰＤＵ）セッション管理ポリシーを更新するように、前記ＰＣＦに前記第１の指示を送信することを特徴とする請求項１に記載のネットワークデータ分析機能（ＮＷＤＡＦ）エンティティに適用される、端末（ＵＥ）の管理と制御のための方法。
【請求項６】
前記ＰＣＦが前記第１の指示に従って前記ＵＥのサービス要求を拒否する必要があると決定する場合、前記アクセスおよびモビリティ管理ポリシーで前記ＵＥの禁止エリアとしてすべてのトラッキングエリア（ＴＡ）を構成し、または、
前記ＰＣＦが前記第１の指示に従って前記ＵＥの特定のＰＤＵセッションのデータレートを制限する必要があると決定する場合、前記セッション管理ポリシーでセッションの集約最大ビットレート（ＡＭＢＲ）を調整するように前記ＰＣＦをトリガーし、または、
前記ＰＣＦが前記第１の指示に従って前記ＵＥに対して位置監視または追跡を実行する必要があると決定する場合、位置監視要求を生成するように前記ＰＣＦをトリガーし、または、
前記ＰＣＦが前記第１の指示に従って前記ＵＥの特定のＰＤＵセッションを削除する必要があると決定する必要があると決定する場合、ＰＤＵセッション終了プロセスを開始するように前記ＰＣＦをトリガーすることを特徴とする請求項５に記載のネットワークデータ分析機能（ＮＷＤＡＦ）エンティティに適用される、端末（ＵＥ）の管理と制御のための方法。
【請求項７】
前記ネットワーク内の少なくとも１つのネットワーク機能エンティティに第１の指示を送信することは、
アクセスおよびモビリティ管理機能（ＡＭＦ）に前記第１の指示を送信し、次の操作の１つまたは組み合わせを実行するように前記ＡＭＦをトリガーし、
前記ＵＥの登録を解除し、
前記ＵＥのセキュリティに対する認証を再度実行し、
前記ＵＥに対して位置監視または追跡を実行し、
前記ＵＥにネットワークサービスの取得を制限することを特徴とする請求項１に記載のネットワークデータ分析機能（ＮＷＤＡＦ）エンティティに適用される、端末（ＵＥ）の

管理と制御のための方法。
【請求項８】
前記ネットワーク内の少なくとも１つのネットワーク機能エンティティに第１の指示を送信することは、
セッション管理機能（ＳＭＦ）に前記第１の指示を送信し、次の操作の１つまたは組み合わせを実行するように前記ＳＭＦをトリガーし、
前記ＵＥの特定のＰＤＵセッションのデータレートを制限し、
前記ＵＥの特定のＰＤＵセッションを削除することを特徴とする請求項１に記載のネットワークデータ分析機能（ＮＷＤＡＦ）エンティティに適用される、端末（ＵＥ）の管理と制御のための方法。
【請求項９】
前記モビリティ管理パラメーターは、モビリティ制限パラメーターまたは定期的な更新タイマー値を含み、前記セッション管理パラメーターはサービス品質（ＱｏＳ）パラメーターを含むことを特徴とする請求項２に記載のネットワークデータ分析機能（ＮＷＤＡＦ）エンティティに適用される、端末（ＵＥ）の管理と制御のための方法。
【請求項１０】
前記ＵＥのセキュリティリスクを決定した後、
アプリケーションサーバーに前記ＵＥの前記セキュリティリスクを示す警告情報を送信することを特徴とする請求項１に記載のネットワークデータ分析機能（ＮＷＤＡＦ）エンティティに適用される、端末（ＵＥ）の管理と制御のための方法。
【請求項１１】
ＵＥの動作情報を取得するように構成された取得ユニットと、
前記動作情報を分析して、前記ＵＥのセキュリティリスクを決定するように構成された決定ユニットと、
ネットワーク内の少なくとも１つのネットワーク機能エンティティに第１の指示を送信し、前記ＵＥに対するポリシー更新またはパラメーター調整を実行するように、前記少なくとも１つのネットワーク機能エンティティをトリガーするように構成された処理ユニットと
を備え、
前記第１の指示は、前記ＵＥの直面するセキュリティリスクのタイプを示し、または、前記ＵＥのセキュリティリスクを解決するためのポリシーまたはパラメーターを示すことを特徴とするネットワークデータ分析機能（ＮＷＤＡＦ）エンティティに適用される、端末（ＵＥ）の管理と制御のための装置。
【発明の詳細な説明】
【技術分野】
【０００１】
関連出願の相互参照
本出願は、２０１８年４月４日に中国特許局に提出し、出願番号が２０１８１０２９９６１９．５であり、発明名称が「端末（ＵＥ）の管理と制御のための方法および装置」との中国特許出願を基礎とする優先権を主張し、その開示の総てをここに取り込む。
【０００２】
本発明は、通信技術分野に関し、特に端末（ＵＥ）の管理と制御のための方法および装置に関する。
【背景技術】
【０００３】
第５世代モバイル通信ネットワーク（Ｆｉｆｔｈ Ｇｅｎｅｒａｔｉｏｎ Ｍｏｂｉｌｅ Ｎｅｔｗｏｒｋ，５Ｇ）は、ネットワークデータ分析機能（Ｎｅｔｗｏｒｋ Ｄａｔａ Ａｎａｌｙｔｉｃｓ Ｆｕｎｃｔｉｏｎ，NWDAF）エンティティを導入した。当該機能エンティティは、ネットワークデータを分析し、分析結果を５Ｇネットワークに提供で、そして、ネットワークを最適化する。

【０００４】
従来技術では、ＮＷＤＡＦは静的構成に基づきネットワークスライスの負荷データを収集して分析し、ポリシー制御機能（Ｐｏｌｉｃｙ Ｃｏｎｔｒｏｌ Ｆｕｎｃｔｉｏｎ，ＰＰＣＦ）などのネットワーク機能にスライス負荷に関連するネットワークデータ分析結果を提供し、ＰＣＦなどのネットワーク機能がＮＷＤＡＦの分析結果によれば、当該スライスに属する端末に対して対応するネットワーク制御ポリシーを設定するか、または対応するネットワーク動作を実行する。ただし、ＮＷＤＡＦはネットワークデータをスライスレベルでしか分析できないため、ＮＷＤＡＦは現在スライスを使用しているユーザを認識できない。

【０００５】
つまり、既存の５Ｇネットワークは、端末に対する悪意のある動作を認識できず、悪意のある動作に対する効果的な防御は言うまでもない。

【０００６】
具体的な例を挙げれば、街路灯、共有自転車などの多数のモノのインターネット（ＩｏＴ）装置が悪意を持って使用または乗っ取られると、既存の５Ｇネットワークはそのような端末に対する悪意のある動作を認識できなくなり、セキュリティ上の問題が発生するだけではない、そして深刻な緊急損失を引き起こす。たとえば、２０１６年、「Ｍｉｒａｉ」に感染した８９万台のカメラとルーターがＤＹＮ ＤＮＳサーバにＤＤｏＳ攻撃を仕掛け、米国東海岸を６時間切断し、数十億に及ぶ経済的損失を引き起こした。

【発明の概要】

【発明が解決しようとする課題】

【０００７】
したがって、既存のモバイル通信ネットワークシステムが、端末の直面するリスクまたは潜在的なリスクに対する効果的な検出および防御を欠いていることは明らかである。

【課題を解決するための手段】

【０００８】
本発明の実施形態は、端末（ＵＥ）の管理と制御のための方法および装置を提供して、既存のモバイル通信ネットワークシステムが、端末の直面するリスクまたは潜在的なリスクに対する効果的な検出および防御を欠いているという問題を解決し、モバイル通信ネットワークシステムの端末管理への管理および制御を強化するにより、システムのリスクが軽減させる。

【０００９】
一方では、本発明の実施形態によって提供される端末（ＵＥ）の管理と制御のための方法は、ネットワークデータ分析機能（ＮＷＤＡＦ）エンティティに適用され、前記方法は、
前記ＵＥの動作情報を取得するステップと、
前記動作情報を分析して、前記ＵＥのセキュリティリスクを決定するステップと、
ネットワーク内の少なくとも１つのネットワーク機能エンティティに第１の指示を送信し、前記ＵＥに対するポリシー更新またはパラメーター調整を実行するように、前記少なくとも１つのネットワーク機能エンティティをトリガーし、ここで、前記第１の指示は、前記ＵＥの直面するセキュリティリスクのタイプを示し、または、前記ＵＥのセキュリティリスクを解決するためのポリシーまたはパラメーターを示し、および／または、
前記ＵＥに第２の指示を送信し、警報を発し、および／またはリスク防御を実行するように前記ＵＥをトリガーし、ここで、前記第２の指示は、前記ＵＥの直面するセキュリティリスクのタイプを示すステップとを備える。

【００１０】
任意選択で、前記ＵＥのセキュリティリスクを解決するためのポリシーまたはパラメーターは、前記ＵＥのモビリティ管理パラメーターおよび／またはセッション管理パラメーターを含む。

【００１１】
任意選択で、前記動作情報は、前記ＵＥの端末タイプ、端末位置、端末モビリティ情報

、アプリケーション情報およびＵＥの宛先アドレスのうちの１つまたは複数を含む。
【００１２】
任意選択で、前記動作情報を分析して、前記ＵＥのセキュリティリスクを決定することは、
前記端末タイプが、前記ＵＥがモノのインターネット（ＩｏＴ）機器であり、前記ＵＥが事前設定された固定エリアから出たことを示す場合、盗難セキュリティリスクが前記ＵＥに存在すると決定し、または、
前記端末タイプが、前記ＵＥがモノのインターネット（ＩｏＴ）機器であり、前記ＵＥが禁止エリアに入ったことを示す場合、不正使用されるセキュリティリスクが前記ＵＥに存在すると決定し、または、
前記端末タイプが、前記ＵＥがモノのインターネット（ＩｏＴ）機器であり、前記ＵＥがトラフィック使用において異常であることを示す場合、ハッカーによってハイジャックされるセキュリティリスクがＵＥに存在すると決定し、または、
前記端末タイプが、前記ＵＥがモノのインターネット（ＩｏＴ）機器であり、前記ＵＥが不正なターゲットアドレスにアクセスしていることを示す場合、ハッカーによってハイジャックされるセキュリティリスクがＵＥに存在すると決定する。
【００１３】
任意選択で、前記ネットワーク内の少なくとも１つのネットワーク機能エンティティに第１の指示を送信することは、
前記ＰＣＦにアクセスおよびモビリティ管理ポリシー、および／または、プロトコルデータユニット（ＰＤＵ）セッション管理ポリシーを更新するように、ポリシー制御機能（ＰＣＦ）に前記第１の指示を送信する。
【００１４】
任意選択で、前記方法では、さらに、
前記ＰＣＦが前記第１の指示に従って前記ＵＥのサービス要求を拒否する必要があると決定する場合、前記アクセスおよびモビリティ管理ポリシーで前記ＵＥの禁止エリアとしてすべてのトラッキングエリア（ＴＡ）を構成し、または、
前記ＰＣＦが前記第１の指示に従って前記ＵＥの特定のＰＤＵセッションのデータレートを制限する必要があると決定する場合、前記セッション管理ポリシーでセッションの集約最大ビットレート（ＡＭＢＲ）を調整するように前記ＰＣＦをトリガーし、または、
前記ＰＣＦが前記第１の指示に従って前記ＵＥに対して位置監視または追跡を実行する必要があると決定する場合、位置監視要求を生成するように前記ＰＣＦをトリガーし、または、
前記ＰＣＦが前記第１の指示に従って前記ＵＥの特定のＰＤＵセッションを削除する必要があると決定する必要があると決定する場合、ＰＤＵセッション終了プロセスを開始するように前記ＰＣＦをトリガーする。
【００１５】
任意選択で、前記ネットワーク内の少なくとも１つのネットワーク機能エンティティに第１の指示を送信することは、
アクセスおよびモビリティ管理機能（ＡＭＦ）に前記第１の指示を送信し、次の操作の１つまたは組み合わせを実行するように前記ＡＭＦをトリガーし、
前記ＵＥの登録を解除し、
前記ＵＥのセキュリティに対する認証を再度実行し、
前記ＵＥに対して位置監視または追跡を実行し、
前記ＵＥにネットワークサービスの取得を制限する。
【００１６】
任意選択で、前記ネットワーク内の少なくとも１つのネットワーク機能エンティティに第１の指示を送信することは、
セッション管理機能（ＳＭＦ）に前記第１の指示を送信し、次の操作の１つまたは組み合わせを実行するように前記ＳＭＦをトリガーし、

前記ＵＥの特定のＰＤＵセッションのデータレートを制限し、
前記ＵＥの特定のＰＤＵセッションを削除する。
【００１７】
任意選択で、前記モビリティ管理パラメーターは、モビリティ制限パラメーターまたは定期的な更新タイマー値を含み、前記セッション管理パラメーターはサービス品質（ＱｏＳ）パラメーターを含む。
【００１８】
任意選択で、前記ＵＥのセキュリティリスクを決定した後、前記方法ではさらに、
アプリケーションサーバーに前記ＵＥの前記セキュリティリスクを示す警告情報を送信する。
【００１９】
他方では、本発明の実施形態によって提供される端末（ＵＥ）におけるセキュリティリスクの存在のための処理方法は前記ＵＥに適用され、前記方法は、
ネットワークが前記ＵＥのセキュリティリスクを決定したときにネットワークによって送信された第１の指示を受信し、ここで、前記第１の指示は、前記ＵＥの直面する前記セキュリティリスクのタイプを示すか、または、前記ＵＥの前記セキュリティリスクを解決するためのポリシーやパラメーターを示すステップと、
前記第１の指示に従って、前記セキュリティリスクに対して、前記ＵＥをトリガーして、警報を発し、および／またはリスク防御を実行するステップとを備える。
【００２０】
任意選択で、前記第１の指示は、ネットワークデータ分析機能（ＮＷＤＡＦ）エンティティが前記ＵＥの動作情報を分析して前記ＵＥのセキュリティリスクを決定した後に直接送信され、または、ポリシー制御機能（ＰＣＦ）またはアクセスおよびモビリティ管理機能（ＡＭＦ）またはセッション管理機能（ＳＭＦ）がネットワークデータ分析機能（ＮＷＤＡＦ）エンティティによる前記ＵＥのセキュリティリスクに対する分析結果を受信した後に送信される。
【００２１】
任意選択で、前記第１の指示に従って、前記セキュリティリスクに対して、前記ＵＥをトリガーして、警報を発し、および／またはリスク防御を実行することは、具体的に、
前記第１の指示に従って、前記ＵＥのアプリケーション層に警告情報を送信し、アプリケーションサーバーに警告情報を送信するように前記アプリケーション層をトリガーし、
光学的／音響的／電気的警報を発し、および／または、ＵＥをロックし、および／または、位置を定期的に報告する。
【００２２】
他方では、本発明の実施形態によって提供される端末（ＵＥ）の管理と制御のための装置はネットワークデータ分析機能（ＮＷＤＡＦ）エンティティに適用され、前記装置は、
前記ＵＥの動作情報を取得するように構成された取得ユニットと、
前記動作情報を分析して、前記ＵＥのセキュリティリスクを決定するように構成された決定ユニットと、
ネットワーク内の少なくとも１つのネットワーク機能エンティティに第１の指示を送信し、前記ＵＥに対するポリシー更新またはパラメーター調整を実行するように、前記少なくとも１つのネットワーク機能エンティティをトリガーし、ここで、前記第１の指示は、前記ＵＥの直面するセキュリティリスクのタイプを示し、または、前記ＵＥのセキュリティリスクを解決するためのポリシーまたはパラメーターを示し、および／または、
前記ＵＥに第２の指示を送信し、警報を発し、および／またはリスク防御を実行するように前記ＵＥをトリガーし、ここで、前記第２の指示は、前記ＵＥの直面するセキュリティリスクのタイプを示す処理ユニットとを備える。
【００２３】
任意選択で、前記第１の指示が前記ＵＥのセキュリティリスクを解決するためのポリシーまたはパラメーターを示す場合、前記処理ユニットはさらに、

前記ＵＥのセキュリティリスクを解決するためのポリシーまたはパラメーターが前記ＵＥのモビリティ管理パラメーターおよび／またはセッション管理パラメーターを含むことを決定する。

【００２４】

任意選択で、前記動作情報は、前記ＵＥの端末タイプ、端末位置、端末モビリティ情報、アプリケーション情報およびＵＥの宛先アドレスのうちの１つまたは複数を含む。

【００２５】

本発明の実施形態では、前記決定ユニットは、

前記端末タイプが、前記ＵＥがモノのインターネット（ＩｏＴ）機器であり、前記端末が事前設定された固定エリアから出たことを示す場合、盗難セキュリティリスクが前記ＵＥに存在すると決定し、または、

前記端末タイプが、前記ＵＥがモノのインターネット（ＩｏＴ）機器であり、前記ＵＥが禁止エリアに位置していることを示す場合、不正使用されるセキュリティリスクが前記ＵＥに存在すると決定し、または、

前記端末タイプが、前記ＵＥがモノのインターネット（ＩｏＴ）機器であり、前記ＵＥがトラフィック使用において異常であることを示す場合、ハッカーによってハイジャックされるセキュリティリスクがＵＥに存在すると決定し、または、

前記端末タイプが、前記ＵＥがモノのインターネット（ＩｏＴ）機器であり、前記ＵＥが不正なターゲットアドレスにアクセスしていることを示す場合、ハッカーによってハイジャックされるセキュリティリスクがＵＥに存在すると決定する。

【００２６】

任意選択で、前記処理ユニットはさらに、

前記ＰＣＦにアクセスおよびモビリティ管理ポリシー、および／または、プロトコルデータユニット（ＰＤＵ）セッション管理ポリシーを更新するように、ポリシー制御機能（ＰＣＦ）に前記第１の指示を送信する。

【００２７】

任意選択で、前記処理ユニットはさらに、

前記ＰＣＦが前記第１の指示に従って前記ＵＥのサービス要求を拒否する必要があると決定する場合、前記アクセスおよびモビリティ管理ポリシーで前記ＵＥの禁止エリアとしてすべてのトラッキングエリア（ＴＡ）を構成し、または、

前記ＰＣＦが前記第１の指示に従って前記ＵＥの特定のＰＤＵセッションのデータレートを制限する必要があると決定する場合、前記セッション管理ポリシーでセッションの集約最大ビットレート（ＡＭＢＲ）を調整するように前記ＰＣＦをトリガーし、または、

前記ＰＣＦが前記第１の指示に従って前記ＵＥに対して位置監視または追跡を実行する必要があると決定する場合、位置監視要求を生成するように前記ＰＣＦをトリガーし、または、

前記ＰＣＦが前記第１の指示に従って前記ＵＥの特定のＰＤＵセッションを削除する必要があると決定する必要があると決定する場合、ＰＤＵセッション終了プロセスを開始するように前記ＰＣＦをトリガーする。

【００２８】

任意選択で、前記処理ユニットはさらに、

アクセスおよびモビリティ管理機能（ＡＭＦ）に前記第１の指示を送信し、次の操作の１つまたは組み合わせを実行するように前記ＡＭＦをトリガーし、

前記ＵＥの登録を解除し、

前記ＵＥのセキュリティに対する認証を再度実行し、

前記ＵＥに対して位置監視または追跡を実行し、

前記ＵＥにネットワークサービスの取得を制限する。

【００２９】

任意選択で、前記処理ユニットはさらに、

セッション管理機能（ＳＭＦ）に前記第１の指示を送信し、次の操作の１つまたは組み

合わせを実行するように前記ＳＭＦをトリガーし、
前記ＵＥの特定のＰＤＵセッションのデータレートを制限し、
前記ＵＥの特定のＰＤＵセッションを削除する。
【００３０】
本発明の実施形態では、前記モビリティ管理パラメーターは、モビリティ制限パラメーターまたは定期的な更新タイマー値を含み、前記セッション管理パラメーターはサービス品質（ＱｏＳ）パラメーターを含む。
【００３１】
任意選択で、前記ＵＥのセキュリティリスクを決定した後、前記装置はさらに、
アプリケーションサーバーに前記ＵＥの前記セキュリティリスクを示す警告情報を送信するように構成された送信ユニットを備える。
【００３２】
他方では、本発明の実施形態によって提供される端末（ＵＥ）におけるセキュリティリスクの存在のための処理装置は前記ＵＥに適用され、前記装置は、
ネットワークが前記ＵＥのセキュリティリスクを決定したときにネットワークによって送信された第１の指示を受信するように構成された受信ユニットであって、ここで、前記第１の指示は、前記ＵＥの直面する前記セキュリティリスクのタイプを示すか、または、前記ＵＥの前記セキュリティリスクを解決するためのポリシーやパラメーターを示す前記受信ユニットと、
前記第１の指示に応答して、前記セキュリティリスクに対して、前記ＵＥをトリガーして、警報を発し、および／またはリスク防御を実行するように構成されたトリガーユニットとを備える。
【００３３】
任意選択で、前記受信ユニットは、ネットワークデータ分析機能（ＮＷＤＡＦ）エンティティが前記ＵＥの動作情報を分析して前記ＵＥのセキュリティリスクを決定した後に直接送信された前記第１の指示を受信し、または、ポリシー制御機能（ＰＣＦ）またはアクセスおよびモビリティ管理機能（ＡＭＦ）またはセッション管理機能（ＳＭＦ）がネットワークデータ分析機能（ＮＷＤＡＦ）エンティティによる前記ＵＥのセキュリティリスク分析結果を受信した後に送信した前記第１の指示を、受信する。
【００３４】
任意選択で、前記トリガーユニットは、
前記第１の指示に従って、前記ＵＥのアプリケーション層に警告情報を送信し、アプリケーションサーバーに警告情報を送信するように前記アプリケーション層をトリガーし、
光学的／音響的／電気的警報を発し、および／または、ＵＥをロックし、および／または、位置を定期的に報告する。
【００３５】
他方では、本発明の実施形態によって提供されるコンピュータ装置は、メモリと、プロセッサと、および前記メモリに格納され、前記プロセッサ上で動作するコンピュータプログラムとを備え、前記プロセッサが前記コンピュータプログラムを実行するとき、前記端末（ＵＥ）の管理と制御のための方法のステップが実施される。
【００３６】
他方では、本発明の実施形態は、コンピュータプログラムが格納されたコンピュータ可読前記憶媒体を提供し、コンピュータプログラムがプロセッサによって実行されると、前記端末（ＵＥ）の管理と制御のための方法のステップが実施される。
【発明の効果】
【００３７】
本発明の実施形態における上前記の１つまたは複数の技術的解決策は、以下の技術的効果のうちの少なくとも１つまたは複数を有する。
【００３８】
本発明の実施形態の技術的解決策では、ＵＥの動作情報は、ネットワークデータ分析機

能（ＮＷＤＡＦ）エンティティを通じて取得され、前記動作情報を分析して、前記ＵＥのセキュリティリスクを決定し、ネットワーク内の少なくとも１つのネットワーク機能エンティティに第１の指示を送信し、前記ＵＥに対するポリシー更新またはパラメーター調整を実行するように、前記少なくとも１つのネットワーク機能エンティティをトリガーし、ここで、前記第１の指示は、前記ＵＥの直面するセキュリティリスクのタイプを示し、または、前記ＵＥのセキュリティリスクを解決するためのポリシーまたはパラメーターを示し、および／または、前記ＵＥに第２の指示を送信し、警報を発し、および／またはリスク防御を実行するように前記ＵＥをトリガーし、ここで、前記第２の指示は、前記ＵＥの直面するセキュリティリスクのタイプを示す。言い換えれば、ＮＷＤＡＦエンティティは、端末動作情報を分析して端末のセキュリティリスクを決定し、防御管理を実行することにより、モバイル通信ネットワークシステムの端末管理への管理および制御を強化し、システムのリスクが軽減させる。

【図面の簡単な説明】

【００３９】

本発明に係る実施例や従来の技術方案をより明確に説明するために、以下に実施例を説明するために必要な図面をについて簡単に紹介する。無論、以下の説明における図面は本発明に係る実施例の一部であり、当業者は、創造性作業を行わないことを前提として、これらの図面に基づいて他の図面を得ることができる。

【００４０】

【図１】本発明の実施形態におけるネットワーク機能アーキテクチャの概略構造図である。

【図２】本発明の実施形態１によって提供される端末（ＵＥ）の管理と制御のための方法の一方法のフローチャートである。

【図３】本発明の実施形態１によって提供される端末（ＵＥ）の管理と制御のための方法におけるＰＣＦが前記第１の指示に従って端末に対するネットワークポリシーを調整する概略図である。

【図４】本発明の実施形態１によって提供される端末（ＵＥ）の管理と制御のための方法において、ＮＷＤＡＦがネットワークにおける各ネットワーク機能および／または端末に指示を送信し、対応して、ネットワークにおける各ネットワーク機能および／または端末が直接リスク防止を実行する動作の概略図である。

【図５】本発明の実施形態２によって提供される端末（ＵＥ）におけるセキュリティリスクの存在のための処理方法の方法フローチャートである。

【図６】本発明の実施形態２によって提供される端末（ＵＥ）におけるセキュリティリスクの存在のための処理方法におけるステップＳ３０２の方法の概略的なフローチャートである。

【図７】本発明の実施形態３によって提供される端末（ＵＥ）の管理と制御のための装置の概略構造図である。

【図８】本発明の実施形態４によって提供される端末（ＵＥ）におけるセキュリティリスクの存在のための処理装置の概略構造図である。

【図９】本発明の実施形態５によって提供されるコンピュータ装置の概略構造図である。

【発明を実施するための形態】

【００４１】

以下に本発明に係る実施形態において図面を結合して本発明の実施形態における技術方案について詳細に、完全に説明するが、次に陳述する実施形態は単に本発明のいくつかの実施形態であり、その全てではない。本分野の一般の技術者にとって、創造性的労働をしなくても、これらの実施形態に基づいてその他の実施形態を容易に獲得することができ、全て本発明の保護範囲に属することは明白である。

【００４２】

本発明の技術案は多様な通信システムに応用することができる。例えば、ＧＳＭ（Ｇｌｏｂａｌ Ｓｙｓｔｅｍ ｏｆ Ｍｏｂｉｌｅ ｃｏｍｍｕｎｉｃａｔｉｏｎ）システム、ＣＤＭＡ（Ｃｏｄｅ Ｄｉｖｉｓｉｏｎ Ｍｕｌｔｉｐｌｅ Ａｃｃｅｓｓ）システム、Ｗ

ＣＤＭＡ（登録商標）（Ｗｉｄｅｂａｎｄ Ｃｏｄｅ Ｄｉｖｉｓｉｏｎ Ｍｕｌｔｉｐｌｅ Ａｃｃｅｓｓ）システム、ＧＰＲＳ（Ｇｅｎｅｒａｌ Ｐａｃｋｅｔ Ｒａｄｉｏ Ｓｅｒｖｉｃｅ）、ＬＴＥ（Ｌｏｎｇ Ｔｅｒｍ Ｅｖｏｌｕｔｉｏｎ）システム、ＬＴＥ－Ａ（Ａｄｖａｎｃｅｄ ｌｏｎｇ ｔｅｒｍ ｅｖｏｌｕｔｉｏｎ）システム、ＵＭＴＳ（Ｕｎｉｖｅｒｓａｌ Ｍｏｂｉｌｅ Ｔｅｌｅｃｏｍｍｕｎｉｃａｔｉｏｎ Ｓｙｓｔｅｍ）、ＮＲ（Ｎｅｗ Ｒａｄｉｏ）等に応用できる。

【００４３】

また、本発明に係る実施例において、ＵＥ（Ｕｓｅｒ Ｅｑｕｉｐｍｅｎｔ）は、ＭＳ（Ｍｏｂｉｌｅ Ｓｔａｔｉｏｎ）、移動端末（Ｍｏｂｉｌｅ Ｔｅｒｍｉｎａｌ）、ＭＴ（Ｍｏｂｉｌｅ Ｔｅｌｅｐｈｏｎｅ）、携帯（ｈａｎｄｓｅｔ）及び携帯機器（ｐｏｒｔａｂｌｅ ｅｑｕｉｐｍｅｎｔ）を含むが、それに限られない。当該ユーザ設備は、ＲＡＮ（Ｒａｄｉｏ Ａｃｃｅｓｓ Ｎｅｔｗｏｒｋ，ＲＡＮ）を介して１つまたは複数のコアネットワークと通信することができる。例えば、ユーザ設備は、ＭＴ（Ｃｅｌｌｕｌａｒ ｐｈｏｎｅとも呼ばれる）、無線通信機能を有するコンピュータなどを含むこともできる。ユーザ設備は、携帯式、ポケット式、手持ち式、コンピュータに内蔵されるかまたは、車載の移動装置であることもできる。

【００４４】

本発明に係る実施例において、基地局（例えば、接続点）は、ＡＮ（Ａｃｃｅｓｓ Ｎｅｔｗｏｒｋ）で無線インターフェースにおいて、１つまたは複数のセクターを介して無線端末と通信する設備であることができる。基地局は、受信した無線フレームとＩＰ組み分けを相互に転換して、無線端末とＡＮの他の部分間のルーターとすることができる。ここで、ＡＮの他の部分は、ＩＰネットワークを含むことができる。基地局は、無線インターフェースに対する属性管理を協調することができる。例えば、基地局は、ＧＳＭまたはＣＤＭＡの基地局（Ｂａｓｅ Ｔｒａｎｓｃｅｉｖｅｒ Ｓｔａｔｉｏｎ，ＢＴＳ）であってもよいし、ＷＣＤＭＡ（登録商標）の基地局（ＮｏｄｅＢ）であってもよく、ＬＴＥの進化型基地局（ＮｏｄｅＢまたはｅＮＢまたはｅ－ＮｏｄｅＢ，ｅｖｏｌｕｔｉｏｎａｌ Ｎｏｄｅ Ｂ）、または、５Ｇ ＮＲにおける基地局（ｇＮＢ）であってもよいが、本発明をそれに限定しない。

【００４５】

本発明の実施形態によって提供される端末（ＵＥ）の管理と制御のための方法および装置は、既存のモバイル通信ネットワークシステムが、端末の直面するリスクまたは潜在的なリスクに対する効果的な検出および防御を欠いているという問題を解決し、了モバイル通信ネットワークシステムの端末管理への管理および制御を強化するにより、システムのリスクが軽減させる。

【００４６】

本発明の実施形態の技術的解決策が上前記の技術的な問題を解決するための一般的な考え方は次のとおりである。

【００４７】

端末（ＵＥ）の管理と制御のための方法は、ネットワークデータ分析機能（ＮＷＤＡＦ）エンティティに適用され、前記方法では、

前記ＵＥの動作情報を取得し、

前記動作情報を分析して、前記ＵＥのセキュリティリスクを決定し、

ネットワーク内の少なくとも１つのネットワーク機能エンティティに第１の指示を送信し、前記ＵＥに対するポリシー更新またはパラメーター調整を実行するように、前記少なくとも１つのネットワーク機能エンティティをトリガーし、ここで、前記第１の指示は、前記ＵＥの直面するセキュリティリスクのタイプを示し、または、前記ＵＥのセキュリティリスクを解決するためのポリシーまたはパラメーターを示し、および／または、

前記ＵＥに第２の指示を送信し、警報を発し、および／またはリスク防御を実行するように前記ＵＥをトリガーし、ここで、前記第２の指示は、前記ＵＥの直面するセキュリティリスクのタイプを示す。

【００４８】
本発明の実施形態の技術的解決策では、ＵＥの動作情報は、ネットワークデータ分析機能（ＮＷＤＡＦ）エンティティを通じて取得され、前記動作情報を分析して、前記ＵＥのセキュリティリスクを決定し、ネットワーク内の少なくとも１つのネットワーク機能エンティティに第１の指示を送信し、前記ＵＥに対するポリシー更新またはパラメーター調整を実行するように、前記少なくとも１つのネットワーク機能エンティティをトリガーし、ここで、前記第１の指示は、前記ＵＥの直面するセキュリティリスクのタイプを示し、または、前記ＵＥのセキュリティリスクを解決するためのポリシーまたはパラメーターを示し、および／または、前記ＵＥに第２の指示を送信し、警報を発し、および／またはリスク防御を実行するように前記ＵＥをトリガーし、ここで、前記第２の指示は、前記ＵＥの直面するセキュリティリスクのタイプを示す。言い換えれば、ＮＷＤＡＦエンティティは、端末動作情報を分析して端末のセキュリティリスクを決定し、防御管理を実行することにより、モバイル通信ネットワークシステムの端末管理への管理および制御を強化し、システムのリスクが軽減させる。
【００４９】
本明細書で使用される「および／または」という用語は、関連するオブジェクトの関連関係を説明するために単に使用され、３つの関係があり得ることを示し、例えば、Ａおよび／またはＢは、Ａが別個に存在し、ＡとＢは同時に存在し、Ｂは別個に存在する３つのケースを示し得る。さらに、本明細書で使用される文字「／」は、別段の指定がない限り、一般に、前後の関連するオブジェクトが「または」の関係を持つことを示す。
【００５０】
本願の明細書、特許請求の範囲、および図面において、「第１」および「第２」などの用語は、異なるオブジェクトを区別するために使用され、特定の順序を説明するために使用されない。さらに、「含む」または「備える」という用語、およびそれらの任意の変更は、非排他的な包含をカバーすることを意図している。たとえば、プロセス、方法、システム、製品、または機器には、リストされているステップまたはユニットに限定されない一連のステップまたはユニットが含まれるが、オプションとして、リストされていないステップまたはユニットがさらに含まれる。または、これらのプロセス、方法、製品または機器の特定のステップまたはユニットがさらに含まれる。
【００５１】
本明細書における「実施形態」は、実施形態と組み合わせて説明される特定の特徴、構造または特性が、本発明の少なくとも１つの実施形態に含まれ得ることを意味する。本明細書の各位置に現れる「実施形態」という語句は、必ずしも同じ実施形態、または他の実施形態を除いた独立したまたは代替の実施形態を指すとは限らない。当業者は、本明細書に前記載された実施形態が他の実施形態と組み合わせることができることを明示的および暗黙的に理解すべきである。
【００５２】
上前記の技術的解決策をよりよく理解するために、本発明の技術的解決法を添付の図面および特定の実施形態により以下に詳細に説明するが、本発明の実施形態および特定の特徴は、実施形態は、本発明の技術的解決策を詳細に説明するためだけに使用され、本発明の技術的解決策を限定することを意図するものではなく、矛盾がない場合、本発明の実施形態および実施形態における技術的特徴互いに組み合わせることができる。
【００５３】
本明細書で説明される技術的解決策は、例えば５Ｇなどのモバイルネットワークシステムに使用することができる。
【００５４】
図１は、本明細書で使用される技術的解決策に適用されるネットワーク機能アーキテクチャを示している。当該アーキテクチャには、ネットワーク層とユーザプレーン層が含まれる。ネットワーク層は、ＮＷＤＡＦ、統合データ管理（Ｕｎｉｆｉｅｄ　Ｄａｔａ　Ｍａｎａｇｅｍｅｎｔ　，ＵＤＭ）機能、ネットワーク露出機能（Ｎｅｔｗｏｒｋ　Ｅｘｐｏｓ

ｕｒｅ Ｆｕｎｃｔｉｏｎ，ＮＥＦ）、アプリケーション機能（Ａｐｐｌｉｃａｔｉｏｎ Ｆｕｎｃｔｉｏｎ，ＡＦ）、ポリシー制御機能（Ｐｏｌｉｃｙ Ｃｏｎｔｒｏｌ Ｆｕｎｃｔｉｏｎ，ＰＣＦ）などのネットワーク機能を含み得る。ＵＤＭには、ユーザデータリポジトリ（Ｕｎｉｆｉｅｄ Ｄａｔａ Ｍａｎａｇｅｍｅｎｔ，ＵＤＲ）が含まれている。ＵＤＲはユーザサブスクリプションデータストレージサーバーであり、サブスクリプション識別子、セキュリティクレジット、アクセス／モバイル管理設計のユーザサブスクリプション情報およびセッション管理設計のユーザサブスクリプション情報を含むユーザサブスクリプションデータを提供でき、ポリシーデータをＰＣＦに提供することもできる。つまり、ＵＤＲはサブスクリプションデータストレージサービスを提供する。ユーザプレーン層は、ユーザプレーン機能（Ｕｓｅｒ Ｐｌａｎｅ Ｆｕｎｃｔｉｏｎ，ＵＰＦ）、アクセスおよびモビリティ管理機能（Ａｃｃｅｓｓ ａｎｄ Ｍｏｂｉｌｉｔｙ Ｍａｎａｇｅｍｅｎｔ Ｆｕｎｃｔｉｏｎ ，ＡＭＦ）、セッション管理機能（Ｓｅｓｓｉｏｎ Ｍａｎａｇｅｍｅｎｔ Ｆｕｎｃｔｉｏｎ，ＳＭＦ）などを含むことができる。ユーザプレーン層の機能エンティティは、基地局などによりＵＥと接続することができる。モバイルネットワークの機能エンティティは、対応するネットワークインターフェースによって相互に接続される。

【００５５】

実際の用途では、ＵＰＦを使用して、ＵＥと外部データネットワークとの間でデータを相互作用させることができる。ＡＭＦはモビリティ管理を担当するために使用でき、ＡＭＦはＵＥおよびアクセスネットワークに接続されている。また、ＳＭＦはセッション管理を担当するために使用でき、ＳＭＦはＵＰＦと接続される。ＰＣＦはポリシー制御を実行するために使用され、ＮＥＦはサードパーティのアプリケーションとの相互作用とネットワーク機能の公開に使用され、ＵＤＭはユーザデータのストレージと管理を担当するために使用され、ＮＷＤＡＦはネットワーク分析機能で管理されるオペレーターによって、スライス関連のネットワークデータ分析をＰＣＦに提供する。

【００５６】

本発明の実施形態によって提供される技術的解決策を、本明細書の添付図面と組み合わせて以下に説明する。以下の例示的なプロセスでは、本発明の実施形態によって提供される技術的解決策の、図１に示されるネットワーク機能アーキテクチャへの適用が、例として使用される。

【００５７】

実施形態１．

【００５８】

本発明の実施形態１は、ＮＷＤＡＦエンティティに適用される、ＵＥを管理および制御するための方法を提供する。具体的には、この方法は、図１に示すネットワークシステムなどのモバイルネットワークシステムに適用され、この方法は、ネットワークシステム内の対応するネットワーク機能によって実行することができ、方法のステップは以下のように説明される。

【００５９】

Ｓ１０１：ＵＥ動作情報を取得する。

【００６０】

Ｓ１０２：前記動作情報を分析して、前記ＵＥのセキュリティリスクを決定する。

【００６１】

Ｓ１０３：ネットワーク内の少なくとも１つのネットワーク機能エンティティに第１の指示を送信し、前記ＵＥに対するポリシー更新またはパラメーター調整を実行するように、前記少なくとも１つのネットワーク機能エンティティをトリガーし、ここで、前記第１の指示は、前記ＵＥの直面するセキュリティリスクのタイプを示し、または、前記ＵＥのセキュリティリスクを解決するためのポリシーまたはパラメーターを示す。

【００６２】

および／または、

Ｓ１０４：前記ＵＥに第２の指示を送信し、警報を発し、および／またはリスク防御を実行するように前記ＵＥをトリガーし、ここで、前記第２の指示は、前記ＵＥの直面するセキュリティリスクのタイプを示す。

【００６３】

特定の実施プロセスにおいて、それは、ステップＳ１０１、Ｓ１０２およびＳ１０３を順次実行する解決策だけでなく、ステップＳ１０１、Ｓ１０２およびＳ１０４を順次実行する解決策であってもよく、さらにステップＳ１０１、Ｓ１０２、Ｓ１０３、Ｓ１０４を順次実行する解決策であってもよい。もちろん、当業者は、ステップＳ１０３とステップＳ１０４との間の実行シーケンスを、ここでは図示されていない、ユーザの実際の使用習慣に従って設計することもできる。図２は、ステップＳ１０３とステップＳ１０４が同時に実行されるフローチャートを示している。

【００６４】

特定の実施プロセスにおいて、最初に、前記ＮＷＤＡＦ前記ＵＥの動作情報を取得し、ここで、前記動作情報は、前記ＵＥの端末タイプ、端末位置、端末モビリティ情報、アプリケーション情報およびＵＥの宛先アドレスのうちの１つまたは複数を含む。当業者はまた、ＮＷＤＡＦによって取得される、本明細書には示されていない実際の要求に従ってＵＥのＵＥ動作情報を設計することもできる。

【００６５】

次に、前記ＮＷＤＡＦは、前記ＵＥの動作情報を分析し、前記ＵＥのリスクを決定する。例えば、前記ＮＷＤＡＦは、ＵＥタイプおよび／またはアプリケーション情報などを分析することにより、前記ＵＥが固定位置に配置されるべきであると決定し、したがって、前記ＵＥの位置変化が検出された後、前記ＵＥが盗まれたと判断できる。たとえば、ＵＥは街路灯に取り付けられた端末機器、現金自動預け払い機（ＡＴＭ）、および監視機器である。さらなる例として、前記ＮＷＤＡＦは、前記ＵＥの位置と前記ＵＥのモビリティ制限情報を分析することにより、前記ＵＥが許可されていないエリア（または禁止エリア）に長時間留まっていると判断し、その結果、ＵＥが不正に使用されていると判断できる。たとえば、共有自転車が住宅地に入ったと判断できる。さらに別の例として、前記ＮＷＤＡＦは、前記ＵＥがトラフィック使用に異常があると検出すると、例えばビデオ監視のデータストリームに異常があることを検出すると、ＵＥのタイプ、アプリケーション情報などを分析することにより、ＵＥがハッカーに乗っ取られたと判断し、たとえば、データストリームが不正なアドレスに送信されたと判断する。

【００６６】

前記ＮＷＤＡＦが前記ＵＥのセキュリティリスクを決定した後、前記方法ではさらに、ネットワーク内の少なくとも１つのネットワーク機能エンティティに第１の指示を送信し、前記ＵＥに対するポリシー更新またはパラメーター調整を実行するように前記少なくとも１つのネットワーク機能エンティティをトリガーし、ここで、前記第１の指示は、前記ＵＥの直面するセキュリティリスクのタイプを示し、または、前記ＵＥのセキュリティリスクを解決するためのポリシーまたはパラメーターを示す。

【００６７】

ここで、前記少なくとも１つのネットワーク機能エンティティは、具体的には、ＰＣＦ、ＡＭＦ、およびＳＭＦのうちの１つまたは複数であり得る。

【００６８】

少なくとも１つのネットワーク機能エンティティがＰＣＦである場合、すなわち、前記ＮＷＤＡＦが第１の指示を前記ＰＣＦに送信する場合、前記ＰＣＦは、第１の指示に従ってＵＥに対するネットワークポリシーを調整する。さらなる例として、まず、前記ＮＷＤＡＦは、前記リスクに応じて、ＵＥの様々なパラメーター、例えば、モビリティ制限パラメーター、ＱｏＳパラメーター、定期的な更新タイマー値などに対する更新を決定する。次に、前記ＮＷＤＡＦはこれらの生成されたパラメーターを対応するネットワーク機能に直接送信する。たとえば、モビリティ制限パラメーターをＡＭＦに送信し、ＱｏＳパラメーターをＳＭＦに送信する。

【００６９】
特定の実施プロセスでは、以下のステップも実行することができる：前記ＮＷＤＡＦは、第２の指示を前記ＵＥに直接送信し、その結果、ＵＥは、警報を発し、および／またはリスク防御を実行するように前記ＵＥをトリガーし、ここで、前記第２の指示は、前記ＵＥの直面するセキュリティリスクのタイプを示す。
【００７０】
すなわち、前記ＵＥが前記第２の指示を受信した場合、前記ＵＥは、リスクのタイプ、例えば「盗難リスクが現在ＵＥに存在している。タイムリーに対処してください。」との警告情報がアプリケーション層によって送信される。当業者は、ユーザの実際の使用習慣に従って、ＵＥが警報を発し、および／またはリスク防御を実行する特定の実施プロセスを設計することができ、ここでは、１つずつ例示しない。
【００７１】
本発明の実施形態では、前記ＮＷＤＡＦは、ネットワーク内の少なくとも１つのネットワーク機能エンティティに第１の指示を送信し、前記ＵＥに対するポリシー更新またはパラメーター調整を実行するように、前記少なくとも１つのネットワーク機能エンティティをトリガーすることができるだけでなく、前記ＵＥに第２の指示を送信し、警報を発し、および／またはリスク防御を実行するように前記ＵＥをトリガーこともできる。具体的な実施プロセスは上前記のプロセスで説明されているため、ここでは１つずつ示さない。
【００７２】
本発明の実施形態では、前記ＵＥのセキュリティリスクを解決するためのポリシーまたはパラメーターは、前記ＵＥのモビリティ管理パラメーターおよび／またはセッション管理パラメーターを含む。
【００７３】
特定の実施プロセスでは、最初に、前記ＮＷＤＡＦは、前記ＵＥのモビリティ管理パラメーターおよび／またはセッション管理パラメーターを決定する。前記モビリティ管理パラメーターは、モビリティ制限パラメーターとすることができ、前記セッション管理パラメーターは、ＱｏＳパラメーターとすることができる。次に、前記ＮＷＤＡＦは、モビリティ管理パラメーターおよび／またはセッション管理パラメーターを少なくとも１つのネットワーク機能エンティティに送信し、その結果、少なくとも１つのネットワーク機能エンティティは、ＵＥのパラメーター調整を実行する。前記モビリティ管理パラメーターは、モビリティ制限パラメーターまたは定期的な更新タイマー値を含み、前記セッション管理パラメーターはサービス品質（ＱｏＳ）パラメーターを含む。
【００７４】
つまり、前記ＮＷＤＡＦは、ＵＥに対して変更されたパラメーターを５Ｇに直接送信できる。
【００７５】
具体的には、第１に、ＮＷＤＡＦは、リスクに従って、ＵＥの様々なパラメーター、例えば、モビリティ制限パラメーター、ＱｏＳパラメーター、定期的更新タイマー値などに対する変更を決定する。次に、ＮＷＤＡＦはこれらの生成されたパラメーターを対応するネットワーク機能に直接送信する。たとえば、ＮＷＤＡＦはモビリティ制限パラメーターをＡＭＦに送信する。さらに、ＡＭＦは、ＵＥに対するパラメーター調整を実行し、例えば、ＵＥの位置を追跡するようにより短い周期的タイマーを構成する。さらなる例では、ＮＷＤＡＦは、ＱｏＳパラメーター、例えば、ＰＤＵセッションを調整するためのＱｏＳパラメーターをＳＭＦに送信する。
【００７６】
本発明の実施形態において、ＮＷＤＡＦは、リスク分析を実行することができ、具体的には、前記ＮＷＤＡＦは、ＵＥの動作情報を分析して、リスクがＵＥに存在するかどうかを判断する。ＵＥのリスクを決定するとき、ＮＷＤＡＦはさらに、ＵＥが持つ可能性のある特定のタイプのリスクを決定することもできる。リスクの種類には、ＵＥが盗まれたタイプ、ＵＥが不正に使用されたタイプ、ハッカーに乗っ取られたタイプなどがある。

【００７７】
特定の実施プロセスでは、ＵＥ動作情報は、ＵＥタイプ、ＵＥ位置、ＵＥモビリティ情報、アプリケーション情報、およびＵＥの宛先アドレスのうちの１つまたは複数を含む。
【００７８】
例えば、ＮＷＤＡＦは、ＵＥタイプおよびＵＥ位置を分析し、ＵＥがＩｏＴ機器であると決定する。具体的には、ＵＥタイプは、一般的なインテリジェント端末であってよく、またはハンドヘルド端末であってよく、またはＩｏＴ端末などであってよい。アプリケーション情報は、監視タイプ、照明タイプ、金融タイプなど、端末上の特定のアプリケーションのアプリケーションタイプを示すことができる。アプリケーション情報は、アプリケーションのデータトラフィックのユースケースを示すこともできるが、ここでは示していない。
【００７９】
本発明の実施形態において、ＵＥの動作情報が分析され、ＵＥにおけるリスクの存在が判定されるステップＳ１０２は、以下の４つの場合を有し得るが、これらに限定されない。
【００８０】
第１のケース
【００８１】
第１のケースは、前記端末タイプが、前記ＵＥがモノのインターネット（ＩｏＴ）機器であり、前記端末が事前設定された固定エリアから出たことを示す場合、盗難セキュリティリスクが前記ＵＥに存在すると決定し、具体的には、前記ＵＥタイプが、前記ＵＥがＩｏＴ機器であることを示し、前記ＮＷＤＡＦが、ＵＥ位置が事前設定された固定エリア内にないことを検出した場合、盗難リスクがＵＥに存在すると決定される。ここで、前記事前設定された固定エリアは、５Ｇから取得してＵＥに設定された許容エリア情報、またはアプリケーションサーバーから取得して端末の移動を許可する地理的範囲情報に従って、ＮＷＤＡＦによって決定できる。たとえば、ＵＥがＩｏＴ機器であり、街灯に取り付けられた端末機器であることがＮＷＤＡＦによって決定される。一般に、このタイプの端末は特定の事前設定された固定エリアに取り付けられる必要があり、端末が事前設定された固定エリアから外れたと検出されると、盗難リスクがＵＥに存在すると判断される。
【００８２】
第２のケース
【００８３】
第２のケースは、前記端末タイプが、前記ＵＥがモノのインターネット（ＩｏＴ）機器であり、前記ＵＥが禁止エリアに位置していることを示す場合、不正使用されるセキュリティリスクが前記ＵＥに存在すると決定し、具体的には、前記ＵＥがＩｏＴ機器であることを前記ＵＥタイプが示しており、前記ＮＷＤＡＦが、ＵＥが禁止エリアに位置していることを検出した場合、不正使用されるリスクがＵＥに存在すると判定される。禁止エリアは、５Ｇから取得してＵＥ用に構成された禁止エリア情報、またはアプリケーションサーバーから取得して端末の進入を禁止するために使用される地理的範囲情報に従って、ＮＷＤＡＦによって決定できる。たとえば、ＵＥがＩｏＴ機器であり、許可されたエリアと禁止されたエリア（共有自転車や共有車など）を持つ輸送手段であることがＮＷＤＡＦによって決定され、ＵＥが住宅地や学校のような禁止エリアに入ると、ＵＥに不正使用されるリスクが存在すると判断される。
【００８４】
第３のケース
【００８５】
第３のケースは、前記端末タイプが、前記ＵＥがモノのインターネット（ＩｏＴ）機器であり、前記ＵＥがトラフィック使用において異常であることを示す場合、ハッカーによってハイジャックされるセキュリティリスクがＵＥに存在すると決定し、例えば、ＮＷＤＡＦが、ＵＥ上の特定のアプリケーションのサービストラフィックが、アプリケーションのトラフィックモデル、ＱｏＳ要求などの面でＮＷＤＡＦによって学習されたものと大き

く異なることを検出すると、ハッカーによってハイジャックされるセキュリティリスクがＵＥに存在すると決定される。さらなる例として、ＵＥがＩｏＴ機器であり、指紋検出機能を備えたアプリケーション端末であることがＮＷＤＡＦによって決定され、ＵＥがトラフィック使用において異常であると決定されると、例えば、検出が定期的に送信されるため、ハッカーによってハイジャックされるセキュリティリスクがＵＥに存在すると決定する。

【００８６】

第４のケース

【００８７】

第４のケースは、前記端末タイプが、前記ＵＥがモノのインターネット（ＩｏＴ）機器であり、前記ＵＥが不正なターゲットアドレスにアクセスしていることを示す場合、ハッカーによってハイジャックされるセキュリティリスクがＵＥに存在すると決定する。例えば、ＮＷＤＡＦは、データ分析と機械学習を通じて、ＵＥによってアクセスされた正当なターゲットアドレス機能を決定することができ、例えば、ターゲットネットワークセグメント情報、ターゲットアドレスホーム情報およびターゲットアドレスの地理的位置属性、アクセス時間、アクセス頻度などを含むことができる。Ｕ前記ＮＷＤＡＦが現在ＵＥによってアクセスされているアドレスが正当なターゲットアドレスの機能に適合していないことを検出すると、ハッカーによってハイジャックされるセキュリティリスクがＵＥに存在すると決定する。さらなる例として、ＵＥがＩｏＴ機器であり、ビデオ監視端末であることがＮＷＤＡＦによって決定され、ビデオ監視端末のデータストリームが不正なターゲットアドレスに送信されたことが検出されると、ハッカーによってハイジャックされるセキュリティリスクがＵＥに存在すると決定する。

【００８８】

確かに、ＵＥのリスクを決定するためにＵＥの前記動作情報が分析される上述の４つのケースに加えて、当業者はまた、実際の要求に応じてＵＥのリスクを決定するための他の方法を設計することができる。ここでは１つずつ例を挙げない。

【００８９】

本発明の実施形態では、本発明の実施形態では、前記ネットワーク内の少なくとも１つのネットワーク機能エンティティに第１の指示を送信することは、具体的に、前記ＰＣＦにアクセスおよびモビリティ管理ポリシー、および／または、プロトコルデータユニット（ＰＤＵ）セッション管理ポリシーを更新するように、ポリシー制御機能（ＰＣＦ）に前記第１の指示を送信する。特定の実施プロセスにおいて、ＰＣＦのみがＮＷＤＡＦからＵＥのＵＥ動作情報の分析結果を受信できる場合、前記ＰＣＦは第１の指示に従って対応するネットワーク防御ポリシーを生成し、コアネットワークと関連するネットワーク機能（ＡＭＦやＳＭＦなど）に対してポリシー更新を実行できる。

【００９０】

図３に示されるように、前記ＰＣＦは、前記第１の指示に従って、ＵＥに対するネットワークポリシーを調整する。具体的には、前記ＰＣＦはＮＷＤＡＦから前記第１の指示（たとえば、リスクプロンプトまたは警告表示）を受信し、５Ｇの応答動作を決定できる。具体的には以下とおりである。

【００９１】

前記ＵＥが盗まれたことをリスクプロンプトまたは警告表示が示している場合、位置監視または追跡はＵＥに対して実行され、ＵＥのサービス要求は拒否される。

【００９２】

前記ＵＥが不正に使用されていることをリスクプロンプトまたは警告表示が示す場合、前記ＵＥに対して位置監視または追跡が実行され、前記ＵＥはネットワークサービスを取得できないように制限される。

【００９３】

リスクプロンプトまたは警告の表示が、ＵＥがハッカーに乗っ取られたことを示している場合、ＵＥの登録が解除され、ＵＥがトリガーされて再登録と再認証が実行され、ＵＥ

の新しいセキュリティ認証プロセスが開始され、前記ＵＥの特定のＰＤＵセッションのデータレートを制限し、および／または、指定されたＰＤＵセッションが削除される。

【００９４】

特定の実施プロセスでは、ＰＣＦは、Ｒｘインターフェースメッセージを介してＡＦからリスクプロンプトまたは警告表示を受け取ることもでき、これは、具体的には、ＡＦがＮＷＤＡＦからリスクプロンプトまたは警告表示を受信した後に端末動作をさらに分析して、確認することによって得られる。また、前記ＡＦがリスクが前記ＵＥに存在しないと判断した場合、現時点では、前記ＰＣＦはＲｘインターフェースメッセージからリスクなしのプロンプトを受信する。

【００９５】

特定の実施プロセスにおいて、前記ＰＣＦは、第１の指示を受信した後、対応する命令またはポリシー更新要求を前記ＡＭＦおよび／またはＳＭＦに送信し、これは、以下の４つのケースを含むが、これらに限定されない。

【００９６】

第１のケース

【００９７】

第１のケースは、前記ＰＣＦが前記第１の指示に従って前記ＵＥのサービス要求を拒否する必要があると決定する場合、前記アクセスおよびモビリティ管理ポリシーで前記ＵＥの禁止エリアとしてすべてのトラッキングエリア（ＴＡ）を構成し、言い換えれば、前記ＰＣＦが前記第１の指示に従って前記ＵＥのサービス要求を拒否する必要があると決定する場合、すべてのＴＡは、アクセスおよびモビリティ管理ポリシーにおいて、前記ＵＥの禁止エリアまたは不許可エリアとして構成される。

【００９８】

第２のケース

【００９９】

第２のケースは、前記ＰＣＦが前記第１の指示に従って前記ＵＥの特定のＰＤＵセッションのデータレートを制限する必要があると決定する場合、前記セッション管理ポリシーでセッションの集約最大ビットレート（ＡＭＢＲ）を調整するように前記ＰＣＦをトリガーし、言い換えれば、前記ＰＤＵセッション

【０１００】

第３のケース

【０１０１】

第３のケースは、前記ＰＣＦが前記第１の指示に従って前記ＵＥに対して位置監視または追跡を実行する必要があると決定する場合、位置監視要求を生成するように前記ＰＣＦをトリガーし、言い換えれば、前記第１の指示に従って前記ＵＥに対して位置監視または追跡を実行する必要があると前記ＰＣＦが決定した場合、位置監視要求が生成され、その結果、ＵＥは定期的な位置報告を実行する。

【０１０２】

第４のケース

【０１０３】

第４のケースは、前記ＰＣＦが前記第１の指示に従って前記ＵＥの特定のＰＤＵセッションを削除する必要があると決定する必要があると決定する場合、ＰＤＵセッション終了プロセスを開始するように前記ＰＣＦをトリガーする。具体的には、指定されたＰＤＵセッションが第１の指示に従って削除される必要があるとＰＣＦが決定した場合、ＰＤＵセッション終了プロセスが開始される。

【０１０４】

確かに、当業者にとって、前記ＰＣＦは前記第１の指示を受信した後、対応する命令またはポリシー更新要求をＡＭＦおよび／またはＳＭＦに送信し、上前記の４つのケースに加えて、当業者はまた、本明細書では例示されていない、ユーザの実際の使用習慣に従って、ＰＣＦによってＡＭＦおよび／またはＳＭＦに送信される他の指示またはポリシー更

新要求を設計することもできる。

【０１０５】

特定の実施プロセスにおいて、前記ＡＭＦがアクセスおよびモビリティ管理ポリシーを受信した場合、対応するモビリティ管理プロセスがトリガーされ、対応する動作が実行される。例えば、モビリティ制限の更新が実行される。さらなる例として、前記ＡＭＦが前記ＰＣＦの要求命令、例えば位置監視要求を受信した場合、ＰＣＦの要求命令が実行される。

【０１０６】

特定の実施プロセスでは、前記ＳＭＦがＰＤＵセッションの関連するポリシーを受信した場合、ＰＤＵセッションの操作がトリガーされ、対応する動作が実行され、例えば、ＰＤＵセッションのセッション集約最大ビットレート（ＡＭＢＲ）が調整される。また、前記ＳＭＦが前記ＰＣＦの要求命令を受信すると、前記ＰＣＦの要求命令が実行され、たとえば、ＰＤＵセッションが削除される。

【０１０７】

さらに、前期ＵＥの管理および制御効率をさらに改善するために、前記ＮＷＤＡＦが前期ＵＥのリスクを決定した後、セキュリティリスクのタイプに従って前記第１の指示が、対応するネットワーク機能に送信されることがさらに決定される。たとえば、前記第１の指示がＵＥの盗難を示している場合、第１の指示は前期ＡＭＦおよび／または前記ＰＣＦに送信される。さらなる例では、前記第１の指示が前記ＵＥが不正に使用されていることを示している場合、前記第１の指示が前記ＡＭＦに送信される。さらに別の例として、前記ＵＥがハッカーに乗っ取られたことを前記第１の指示が示している場合、前記第１の指示は前記ＡＭＦ、前記ＳＭＦ、前記ＰＣＦのいずれか１つ以上に送信される。

【０１０８】

特定の実施プロセスにおいて、前記ＮＷＤＡＦが前記第１の指示を５ＧのＡＭＦに直接送信すると、前記ＡＭＦはリスク防御操作を直接実行し、以下の操作の１つまたは組み合わせを実行することができる：

前記ＵＥの登録を解除し、

前記ＵＥのセキュリティに対する認証を再度実行し、

前記ＵＥに対して位置監視または追跡を実行し、

前記ＵＥにネットワークサービスの取得を制限する。

【０１０９】

特定の実施プロセスでは、前記ＡＭＦが前記ＵＥの前記第１の指示をサブスクライブする場合、前記ＡＭＦは、リスクのタイプに従って対応するモビリティ管理動作を決定し、例えば、より短い定期的なタイマーを構成して、端末位置を追跡する。

【０１１０】

特定の実施プロセスでは、前記ＮＷＤＡＦが５Ｇネットワークの前記ＳＭＦに前記第１の指示を直接送信すると、前記ＳＭＦはリスク防御操作を直接実行し、以下の操作の１つまたは組み合わせを実行することができる：

前記ＵＥの特定のＰＤＵセッションのデータレートを制限し、

前記ＵＥの特定のＰＤＵセッションを削除する。

【０１１１】

特定の実施プロセスでは、前記ＳＭＦが特定のＰＤＵセッションの指示をサブスクライブする場合、前記ＳＭＦは、リスクタイプに従って対応するセッション管理操作を決定し、例えば、ＰＤＵセッションを削除する。

【０１１２】

本発明の実施形態では、前記ＮＷＤＡＦが前記ＵＥに第２の指示を送信する場合、警報を発し、および／またはリスク防御を実行するように前記ＵＥをトリガーし、ここで、前記第２の指示は、前記ＵＥの直面するセキュリティリスクのタイプを示す。具体的には、前記ＵＥが前記第２の指示を受信した場合、アプリケーションサーバーに前記ＵＥの前記セキュリティリスクを示す警告情報を送信する。特定の実施プロセスにおいて、前記第２

の指示は、前記第１の指示と同じであってもよく、または前記第１の指示とは異なっていてもよく、具体的には、当業者は、実際の要求に従って動作を設計することができ、ここで繰り返される。

【０１１３】

本発明の実施形態では、前記ＮＷＤＡＦは、５Ｇネットワークにおける各ネットワーク機能および／または前記ＵＥに指示を直接送信し、対応して、５Ｇネットワークにおける各ネットワーク機能および／または前記ＵＥは、関連するリスク防御を直接実行することができる。全体的な処理プロセスの概略図は図４に示すとおりであり、特定の処理プロセスは上で詳細に説明されているため、本明細書では図示されていない。

【０１１４】

実施形態２

【０１１５】

本発明の実施形態１と同じ発明思想に基づいて、図５を参照すると、本発明の実施形態２は、前記ＵＥに適用される、ＵＥにおけるセキュリティリスクの存在のための処理方法を提供する。この方法には以下のステップが含まれる。

【０１１６】

Ｓ２０１：ネットワークが前記ＵＥのセキュリティリスクを決定したときにネットワークによって送信された第１の指示を受信し、ここで、前記第１の指示は、前記ＵＥの直面する前記セキュリティリスクのタイプを示すか、または、前記ＵＥの前記セキュリティリスクを解決するためのポリシーやパラメーターを示す。

【０１１７】

Ｓ２０２：前記第１の指示に従って、前記セキュリティリスクに対して警報を発し、および／またはリスク防御を実行するように、前記ＵＥをトリガーする。

【０１１８】

本発明の実施形態では、Ｓ２０１～Ｓ２０２の特定の実施プロセスは、実施形態１で詳細に説明されており、したがって、本明細書では繰り返されない。

【０１１９】

本発明の実施形態では、前記第１の指示は、ネットワークデータ分析機能（ＮＷＤＡＦ）エンティティが前記ＵＥの動作情報を分析して前記ＵＥのセキュリティリスクを決定した後に直接送信され、または、ポリシー制御機能（ＰＣＦ）またはアクセスおよびモビリティ管理機能（ＡＭＦ）またはセッション管理機能（ＳＭＦ）がネットワークデータ分析機能（ＮＷＤＡＦ）エンティティによる前記ＵＥのセキュリティリスクに対する分析結果を受信した後に送信される。

【０１２０】

本発明の実施形態では、図６に示すように、ステップＳ２０２において、前記第１の指示に従って、前記セキュリティリスクに対して警報を発し、および／またはリスク防御を実行するように、前記ＵＥをトリガーすることは、具体的に、

Ｓ３０１：前記第１の指示に従って、前記ＵＥのアプリケーション層に警告情報を送信し、アプリケーションサーバーに警告情報を送信するように前記アプリケーション層をトリガーする。

【０１２１】

Ｓ３０２：光学的／音響的／電気的警報を発し、および／または、ＵＥをロックし、および／または、位置を定期的に報告する。

【０１２２】

特定の実施プロセスにおいて、Ｓ３０１～Ｓ３０２の特定の実施プロセスは、以下のように示される。

【０１２３】

最初に、前記第１の指示に従って、前記ＵＥのアプリケーション層に警告情報を送信し、アプリケーションサーバーに警告情報を送信するように前記アプリケーション層をトリガーする。

【０１２４】
例えば、第１の表示が盗難リスクが「００１００」と番号付けされたインテリジェント機器に存在することを示す場合、警告情報は当該インテリジェント機器のアプリケーション層に送信され、「盗難リスクは、「００１００」という番号が付けられたインテリジェント機器に存在し、アプリケーションサーバーに存在する」との警報情報をアプリケーションサーバーに送信するように前記アプリケーション層はトリガーされる。次に、警報が相応に発せられ、および／またはリスク防御が相応に実行される。たとえば、「００１００」という番号のインテリジェント機器の懐中電灯は、ユーザに警告するために特定の周波数で発光する。さらなる例として、「００１００」と番号付けされたインテリジェント機器は、ユーザに警告するために特定の周波数で振動する。さらに別の例として、「００１００」の番号が付けられたインテリジェント機器は直接ロックされており、たとえば、共有自転車はロックされており、ユーザはそれを使用できなくなる。また、定期的な位置報告を行うようにＵＥを制御することもできるため、リアルタイムでモニターがＵＥの位置を特定することで、ＵＥが盗難される事態を最大限で回避することができる。
【０１２５】
実施形態３
【０１２６】
実施形態１と同じ発明思想に基づいて、図７を参照すると、本発明の実施形態は、ネットワークデータ分析機能（ＮＷＤＡＦ）エンティティに適用される、ＵＥを管理および制御するための装置をさらに提供する。この装置は、取得ユニット１０、決定ユニット２０および処理ユニット３０を含む。
【０１２７】
前記取得ユニット１０は、前記ＵＥ動作情報を取得するように構成される。
【０１２８】
決定ユニット２０は、前記ＵＥ動作情報を分析し、前記ＵＥのリスクを決定するように構成される。
【０１２９】
前記処理ユニット３０は、ネットワーク内の少なくとも１つのネットワーク機能エンティティに第１の指示を送信し、前記ＵＥに対するポリシー更新またはパラメーター調整を実行するように、前記少なくとも１つのネットワーク機能エンティティをトリガーし、ここで、前記第１の指示は、前記ＵＥの直面するセキュリティリスクのタイプを示し、または、前記ＵＥのセキュリティリスクを解決するためのポリシーまたはパラメーターを示し、および／または、
前記ＵＥに第２の指示を送信し、警報を発し、および／またはリスク防御を実行するように前記ＵＥをトリガーし、ここで、前記第２の指示は、前記ＵＥの直面するセキュリティリスクのタイプを示す。
【０１３０】
本発明の実施形態では、前記第１の指示が前記ＵＥのセキュリティリスクを解決するためのポリシーまたはパラメーターを示す場合、処理ユニット３０はさらに、
前記ＵＥのセキュリティリスクを解決するためのポリシーまたはパラメーターが前記ＵＥのモビリティ管理パラメーターおよび／またはセッション管理パラメーターを含むことを決定する。
【０１３１】
本発明の実施形態では、前記動作情報は、前記ＵＥの端末タイプ、端末位置、端末モビリティ情報、アプリケーション情報およびＵＥの宛先アドレスのうちの１つまたは複数を含む。
【０１３２】
本発明の実施形態では、決定ユニット２０は、
前記端末タイプが、前記ＵＥがモノのインターネット（ＩｏＴ）機器であり、前記ＵＥが事前設定された固定エリアから出たことを示す場合、盗難セキュリティリスクが前記Ｕ

Ｅに存在すると決定し、または、
前記端末タイプが、前記ＵＥがモノのインターネット（ＩｏＴ）機器であり、前記ＵＥが禁止エリアに位置していることを示す場合、不正使用されるセキュリティリスクが前記ＵＥに存在すると決定し、または、
前記端末タイプが、前記ＵＥがモノのインターネット（ＩｏＴ）機器であり、前記ＵＥがトラフィック使用において異常であることを示す場合、ハッカーによってハイジャックされるセキュリティリスクがＵＥに存在すると決定し、または、
前記端末タイプが、前記ＵＥがモノのインターネット（ＩｏＴ）機器であり、前記ＵＥが不正なアドレスにアクセスすることを示す場合、ハッカーによってハイジャックされるセキュリティリスクがＵＥに存在すると決定する。

【０１３３】
本発明の実施形態では、処理ユニット３０は、
前記ＰＣＦにアクセスおよびモビリティ管理ポリシー、および／または、プロトコルデータユニット（ＰＤＵ）セッション管理ポリシーを更新するように、ポリシー制御機能（ＰＣＦ）に前記第１の指示を送信する。

【０１３４】
本発明の実施形態では、処理ユニット３０はさらに、
前記ＰＣＦが前記第１の指示に従って前記ＵＥのサービス要求を拒否する必要があると決定する場合、前記アクセスおよびモビリティ管理ポリシーで前記ＵＥの禁止エリアとしてすべてのトラッキングエリア（ＴＡ）を構成し、または、
前記ＰＣＦが前記第１の指示に従って前記ＵＥの特定のＰＤＵセッションのデータレートを制限する必要があると決定する場合、前記セッション管理ポリシーでセッションの集約最大ビットレート（ＡＭＢＲ）を調整するように前記ＰＣＦをトリガーし、または、
前記ＰＣＦが前記第１の指示に従って前記ＵＥに対して位置監視または追跡を実行する必要があると決定する場合、位置監視要求を生成するように前記ＰＣＦをトリガーし、または、
前記ＰＣＦが前記第１の指示に従って前記ＵＥの特定のＰＤＵセッションを削除する必要があると決定する必要があると決定する場合、ＰＤＵセッション終了プロセスを開始するように前記ＰＣＦをトリガーする。

【０１３５】
本発明の実施形態では、前記処理ユニット３０はさらに、
アクセスおよびモビリティ管理機能（ＡＭＦ）に前記第１の指示を送信し、次の操作の１つまたは組み合わせを実行するように前記ＡＭＦをトリガーし、
前記ＵＥの登録を解除し、
前記ＵＥのセキュリティに対する認証を再度実行し、
前記ＵＥに対して位置監視または追跡を実行し、
前記ＵＥにネットワークサービスの取得を制限する。

【０１３６】
本発明の実施形態では、前記処理ユニット３０はさらに、
セッション管理機能（ＳＭＦ）に前記第１の指示を送信し、次の操作の１つまたは組み合わせを実行するように前記ＳＭＦをトリガーし、
前記ＵＥの特定のＰＤＵセッションのデータレートを制限し、
前記ＵＥの特定のＰＤＵセッションを削除する。

【０１３７】
本発明の実施形態では、前記モビリティ管理パラメーターは、モビリティ制限パラメーターまたは定期的な更新タイマー値を含み、前記セッション管理パラメーターはサービス品質（ＱｏＳ）パラメーターを含む。

【０１３８】
本発明の実施形態では、前記ＵＥのセキュリティリスクを決定した後、前記装置は、
アプリケーションサーバーに前記ＵＥの前記セキュリティリスクを示す警告情報を送信

するように構成された送信ユニットをさらに備える。
【０１３９】
実施形態４
【０１４０】
実施形態１と同じ発明思想に基づいて、図８を参照すると、本発明の実施形態は、前記ＵＥに適用される、端末（ＵＥ）におけるセキュリティリスクの存在のための処理装置をさらに提供する。この装置は、受信ユニット４０およびトリガーユニット４０を含む。
【０１４１】
前記受信ユニット４０は、ネットワークが前記ＵＥのセキュリティリスクを決定したときにネットワークによって送信された第１の指示を受信するように構成され、ここで、前記第１の指示は、前記ＵＥの直面する前記セキュリティリスクのタイプを示すか、または、前記ＵＥの前記セキュリティリスクを解決するためのポリシーやパラメーターを示す。
【０１４２】
前記トリガーユニット５０は、前記第１の指示に従って、前記セキュリティリスクに対して、前記ＵＥをトリガーして、警報を発し、および／またはリスク防御を実行するように構成される。
【０１４３】
本発明の実施形態では、前記受信ユニット４０は、ネットワークデータ分析機能（ＮＷＤＡＦ）エンティティが前記ＵＥの動作情報を分析して前記ＵＥのセキュリティリスクを決定した後に直接送信された前記第１の指示を受信し、または、ポリシー制御機能（ＰＣＦ）またはアクセスおよびモビリティ管理機能（ＡＭＦ）またはセッション管理機能（ＳＭＦ）がネットワークデータ分析機能（ＮＷＤＡＦ）エンティティによる前記ＵＥのセキュリティリスク分析結果を受信した後に送信した前記第１の指示を、受信する。
【０１４４】
本発明の実施形態では、前記トリガーユニット５０は、
前記第１の指示に従って、前記ＵＥのアプリケーション層に警告情報を送信し、アプリケーションサーバーに警告情報を送信するように前記アプリケーション層をトリガーし、
光学的／音響的／電気的警報を発し、および／または、ＵＥをロックし、および／または、位置を定期的に報告する。
【０１４５】
実施形態５
【０１４６】
本発明の実施形態は、コンピュータ装置を提供する。コンピュータ装置の構造は図９に示されるとおりである。特定の実施プロセスにおいて、前記コンピュータ装置は、メモリ６０、プロセッサ７０、およびメモリ６０に格納され、プロセッサ７０上で動作可能なコンピュータプログラムを含む。本発明の実施形態１によって提供される方法のステップは、プロセッサ７０が前記コンピュータプログラムを実行するときに実施され、本発明の実施形態２によって提供される方法のステップは、プロセッサ７０が前記コンピュータプログラムを実行するときに実施される。
【０１４７】
本発明の実施形態では、プロセッサ７０は、具体的には中央処理装置または特定用途向け集積回路（Ａｐｐｌｉｃａｔｉｏｎ Ｓｐｅｃｉｆｉｃ Ｉｎｔｅｇｒａｔｅｄ Ｃｉｒｃｕｉｔ，ＡＳＩＣ）であり得、プログラム実行を制御するための１つまたは複数の集積回路であり得、フィールドプログラマブルゲートアレイ（Ｆｉｅｌｄ Ｐｒｏｇｒａｍｍａｂｌｅ Ｇａｔｅ Ａｒｒａｙ，ＦＰＧＡ）によって開発されたハードウェア回路であり得る。ベースバンドプロセッサの場合もある。
【０１４８】
本発明の実施形態では、プロセッサ７０は、少なくとも１つの処理コアを含むことができる。
【０１４９】

本発明の実施形態では、電子機器はメモリ６０をさらに含み、メモリ６０は、読み取り専用メモリ（Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ，ＲＯＭ）、ランダムアクセスメモリ（Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ，ＲＡＭ）、および磁気ディスクメモリを含むことができる。メモリ６０は、プロセッサ７０が動作するときに必要なデータを格納するように構成される。１つまたは複数のメモリ６０が提供される。

【０１５０】

実施形態６

【０１５１】

本発明の実施形態は、コンピュータプログラムを前記憶するコンピュータ可読前記憶媒体をさらに提供する。前記コンピュータプログラムがプロセッサによって実行されるとき、本発明の実施形態１によって提供される方法のステップが実施される。そして、前記コンピュータプログラムがプロセッサによって実行されるとき、本発明の実施形態２によって提供される方法のステップが実施される。

【０１５２】

本発明の実施形態では、開示された方法および装置は他の方法で実施できることを理解されたい。たとえば、上前記の機器の実施形態は単に概略的なものであり、たとえば、ユニットの分割は単なる論理機能の分割であり、実際の実施プロセスには他の分割モードがあり、たとえば、複数のユニットまたはコンポーネントを組み合わせたり、別のシステムに統合することもできる。または、一部の機能を無視したり、実行しないこともできる。さらに、表示または議論された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ース、機器またはユニットによる間接結合または通信接続であり得、電気モードまたは他のモードであり得る。

【０１５３】

本発明の実施形態における機能ユニットは、１つの処理ユニットに統合することができ、または各ユニットは、独立した物理モジュールであることもできる。

【０１５４】

統合されたユニットがソフトウェア機能ユニットの形で実施され、独立した製品として販売および使用されるとき、統合されたユニットは、１つのコンピュータ可読前記憶媒体に格納することができる。そのような理解に基づいて、本発明の実施形態の技術的解決策のすべてまたは一部をソフトウェア製品の形で示すことができ、コンピュータソフトウェア製品は１つの前記憶媒体に格納される。例えばパーソナルコンピュータ、サーバまたはネットワーク機器など、またはプロセッサであり得るコンピュータ機器に、本発明の各実施形態によって提供される方法のステップの全部または一部を実行させるための、複数の命令が含まれる。上前記の前記憶媒体は、ユニバーサルシリアルバスフラッシュドライブ（Ｕｎｉｖｅｒｓａｌ Ｓｅｒｉａｌ Ｂｕｓ ｆｌａｓｈ ｄｒｉｖｅ，ＵＳＢ）、モバイルハードディスク、ＲＯＭ（Ｒｅａｄ－Ｏｎｌｙ Ｍｅｍｏｒｙ）、ＲＡＭ（Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）、磁気ディスクまたはコンパクトディスクなどのプログラムコードを前記憶することができる様々な媒体を含む。

【０１５５】

本発明の実施形態における上前記の１つまたは複数の技術的解決策は、少なくとも以下のような１つまたは複数の技術的効果を有する。

【０１５６】

本発明の実施形態の技術的解決策では、ＵＥの動作情報は、ネットワークデータ分析機能（ＮＷＤＡＦ）エンティティを通じて取得され、前記動作情報を分析して、前記ＵＥのセキュリティリスクを決定し、ネットワーク内の少なくとも１つのネットワーク機能エンティティに第１の指示を送信し、前記ＵＥに対するポリシー更新またはパラメーター調整を実行するように、前記少なくとも１つのネットワーク機能エンティティをトリガーし、ここで、前記第１の指示は、前記ＵＥの直面するセキュリティリスクのタイプを示し、または、前記ＵＥのセキュリティリスクを解決するためのポリシーまたはパラメーターを示し、および／または、前記ＵＥに第２の指示を送信し、警報を発し、および／またはリス

ク防御を実行するように前記ＵＥをトリガーし、ここで、前記第２の指示は、前記ＵＥの直面するセキュリティリスクのタイプを示す。言い換えれば、ＮＷＤＡＦエンティティは、端末動作情報を分析して端末のセキュリティリスクを決定し、防御管理を実行することにより、モバイル通信ネットワークシステムの端末管理への管理および制御を強化し、システムのリスクが軽減させる。

【０１５７】

本分野の技術者として、本発明の実施形態が、方法、システム或いはコンピュータプログラム製品を提供できるため、本発明は完全なハードウェア実施形態、完全なソフトウェア実施形態、またはソフトウェアとハードウェアの両方を結合した実施形態を採用できることがわかるはずである。さらに、本発明は、一つ或いは複数のコンピュータプログラム製品の形式を採用できる。当該製品はコンピュータ使用可能なプログラムコードを含むコンピュータ使用可能な前記憶媒体（ディスク前記憶装置、ＣＤ－ＲＯＭ、光学前記憶装置等を含むがそれとは限らない）において実施する。

【０１５８】

以上は本発明の実施形態の方法、装置（システム）、およびコンピュータプログラム製品のフロー図および／またはブロック図によって、本発明を前記述した。理解すべきことは、コンピュータプログラム指令によって、フロー図および／またはブロック図における各フローおよび／またはブロックと、フロー図および／またはブロック図におけるフローおよび／またはブロックの結合を実現できる。プロセッサはこれらのコンピュータプログラム指令を、汎用コンピュータ、専用コンピュータ、組込み式処理装置、或いは他のプログラム可能なデータ処理装置設備の処理装置器に提供でき、コンピュータ或いは他のプログラム可能なデータ処理装置のプロセッサは、これらのコンピュータプログラム指令を実行し、フロー図における一つ或いは複数のフローおよび／またはブロック図における一つ或いは複数のブロックに指定する機能を実現する。

【０１５９】

これらのコンピュータプログラム指令は又、また、コンピュータ或いは他のプログラム可能なデータ処理装置を特定方式で動作させるコンピュータ読取前記憶装置に前記憶できる。これによって、指令を含む装置は当該コンピュータ読取前記憶装置内の指令を実行でき、フロー図における一つ或いは複数のフローおよび／またはブロック図における一つ或いは複数のブロックに指定する機能を実現する。

【０１６０】

これらコンピュータプログラム指令はさらに、コンピュータ或いは他のプログラム可能なデータ処理装置設備に実施もできる。コンピュータプログラム指令が実施されたコンピュータ或いは他のプログラム可能設備は、一連の操作ステップを実行することによって、関連の処理を実現し、コンピュータ或いは他のプログラム可能な設備において実行される指令によって、フロー図における一つ或いは複数のフローおよび／またはブロック図における一つ或いは複数のブロックに指定する機能を実現する。

【０１６１】

上述した実施形態に前記述された技術的な解決手段を改造し、或いはその中の一部の技術要素を置換することもできる。そのような、改造と置換は本発明の各実施形態の技術の範囲から逸脱するとは見なされない。

【０１６２】

無論、当業者によって、上述した実施形態に前記述された技術的な解決手段を改造し、或いはその中の一部の技術要素を置換することもできる。そのような、改造と置換は本発明の各実施形態の技術の範囲から逸脱するとは見なされない。そのような改造と置換は、すべて本発明の請求の範囲に属する。

【符号の説明】

【０１６３】

10　取得ユニット

20　決定ユニット

30 処理ユニット
40 受信ユニット
50 トリガーユニット
60 メモリ
70 プロセッサ

【図面】

【図１】

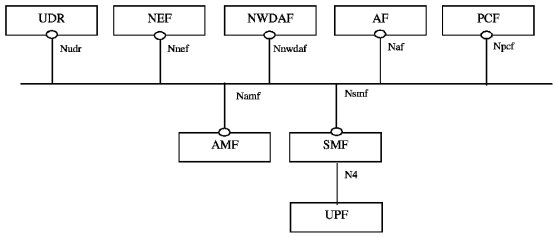
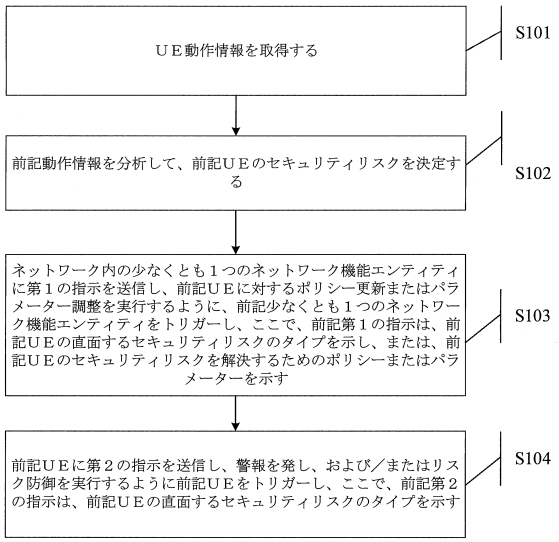
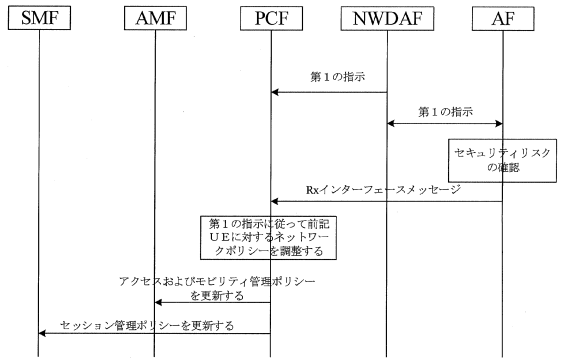


図１

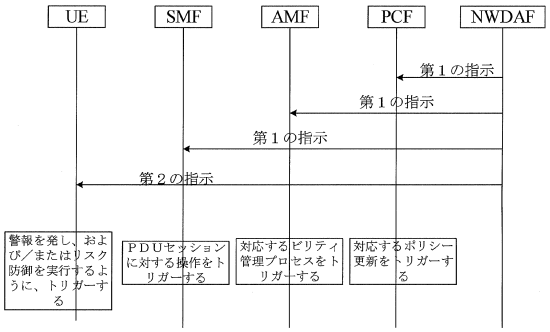
【図２】



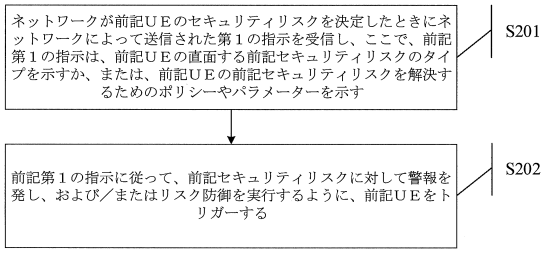
【図３】



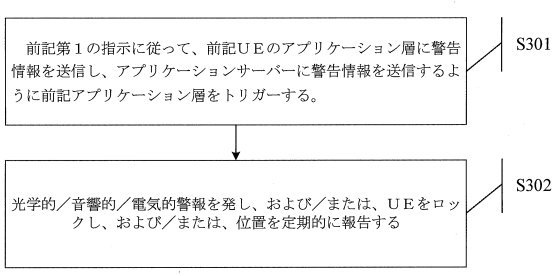
【図４】



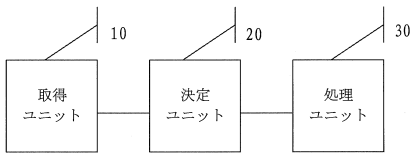
【図５】


ネットワークが前記ＵＥのセキュリティリスクを決定したときにネットワークによって送信された第１の指示を受信し、ここで、前記第１の指示は、前記ＵＥの直面する前記セキュリティリスクのタイプを示すか、または、前記ＵＥの前記セキュリティリスクを解決するためのポリシーやパラメーターを示す
S201
前記第１の指示に従って、前記セキュリティリスクに対して警報を発し、および／またはリスク防御を実行するように、前記ＵＥをトリガーする
S202

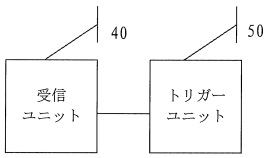
【図６】


前記第１の指示に従って、前記ＵＥのアプリケーション層に警告情報を送信し、アプリケーションサーバーに警告情報を送信するように前記アプリケーション層をトリガーする。
S301
光学的／音響的／電気的警報を発し、および／または、ＵＥをロックし、および／または、位置を定期的に報告する
S302

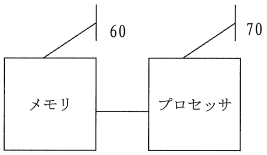
【図７】


10
20
30
取得ユニット
決定ユニット
処理ユニット

【図８】


40
50
受信ユニット
トリガーユニット

【図９】


60
70
メモリ
プロセッサ

フロントページの続き

弁理士　実広 信哉
(74)代理人　100133400
弁理士　阿部 達彦
(72)発明者　王 胡成
中華人民共和国１００１９１北京市▲海▼淀区学院路４０号
審査官　伊東 和重
(56)参考文献　韓国公開特許第１０－２０１４－００１８０９３（ＫＲ，Ａ）
CATT, Lenovo, Motorola Mobility，Update to the use case on customized mobility management[online]，3GPP TSG SA WG2 #126，3GPP，2018年03月02日，S2-182346，検索日[2022.12.22],Internet〈URL:https://www.3gpp.org/ftp/tsg_sa/WG2_Arch/TSGS2_126_Montreal/Docs/S2-182346.zip〉
(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｈ０４Ｂ　７／２４－７／２６
Ｈ０４Ｗ　４／００－９９／００
３ＧＰＰ ＴＳＧ ＲＡＮ ＷＧ１－４
ＳＡ　ＷＧ１－４
ＣＴ　ＷＧ１，４