

(19) 日本国特許庁(JP)

## (12) 公表特許公報(A)

(11) 特許出願公表番号

特表2014-531165

(P2014-531165A)

(43) 公表日 平成26年11月20日(2014.11.20)

(51) Int.Cl.

HO4W 12/06

(2009.01)

F 1

HO4W 12/06

テーマコード(参考)

5K067

## 審査請求 有 予備審査請求 未請求 (全 32 頁)

(21) 出願番号 特願2014-536422 (P2014-536422)  
 (86) (22) 出願日 平成24年10月29日 (2012.10.29)  
 (85) 翻訳文提出日 平成26年4月22日 (2014.4.22)  
 (86) 國際出願番号 PCT/JP2012/006925  
 (87) 國際公開番号 WO2013/061614  
 (87) 國際公開日 平成25年5月2日 (2013.5.2)  
 (31) 優先権主張番号 特願2011-236699 (P2011-236699)  
 (32) 優先日 平成23年10月28日 (2011.10.28)  
 (33) 優先権主張国 日本国 (JP)

(71) 出願人 000004237  
 日本電気株式会社  
 東京都港区芝五丁目7番1号  
 (74) 代理人 100103894  
 弁理士 家入 健  
 (72) 発明者 張 晓維  
 東京都港区芝五丁目7番1号 日本電気株  
 式会社内  
 (72) 発明者 プラサド アンド ラガワ  
 東京都港区芝五丁目7番1号 日本電気株  
 式会社内  
 F ターム(参考) 5K067 AA33 AA35 BB04 DD17 EE02  
 EE10 EE16 HH21

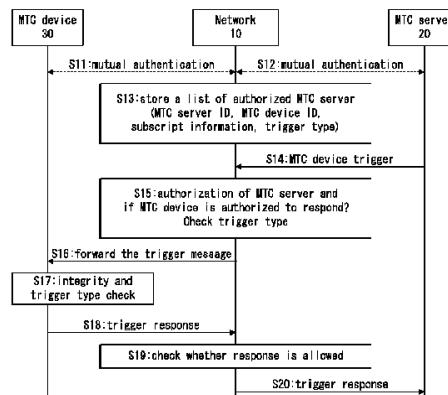
最終頁に続く

(54) 【発明の名称】MTCデバイストリガリングのためのセキュアな方法

## (57) 【要約】

MTCサーバ(20)からのトリガリングメッセージの受信に際して、ネットワーク(10)は、トリガリングメッセージに含まれるMTCデバイスID及びMTCサーバID(オプションとして、加入者に関する情報を承認されているIDと比較することにより、MTCサーバ(20)がターゲットMTCデバイス(30)へのトリガを承認されているか検証し、また、MTCデバイス(30)がトリガリングメッセージへの応答を承認されているか検証する。検証に成功した際、ネットワーク(10)は、トリガリングメッセージに含まれるトリガ種別をチェックして、トリガリングメッセージがMTCデバイス(30)への送信を承認されたものであるか検証する。チェックに成功した際、ネットワーク(10)は、トリガリングメッセージをMTCデバイス(30)へ転送する。また、ネットワーク(10)は、MTCデバイス(30)が宛先のMTCサーバ(20)と通信することを許可されているか否かをチェックすることにより、MTCデバイス(30)からの応答を有効にする。

【選択図】図1



**【特許請求の範囲】****【請求項 1】**

ネットワークと、  
トリガを送信するMTC (Machine-Type-Communication) サーバと、

前記ネットワークにより転送される前記トリガを受信するMTCデバイスと、を備え、  
前記ネットワークは、

前記ネットワークへのアクセスを承認されたMTCサーバの識別子と、各MTCサーバ  
がトリガすることを許可されたMTCデバイスの識別子とが対応付けられたりストを記憶  
し、

前記MTCサーバから前記トリガを受信した場合、前記MTCサーバの識別子を前記リ  
ストに含まれる識別子と照合することによって、前記MTCサーバが前記トリガの送信を  
許可されているか検証する、

システム。

**【請求項 2】**

請求項1において、

前記リストは、前記MTCサーバが送信することを承認されたトリガの種別をさらに含  
み、

前記ネットワークは、前記トリガの種別を前記リストに含まれる種別と照合することに  
よって、前記トリガが承認されているか否かをさらに検証する、

ことを特徴としたシステム。

**【請求項 3】**

請求項1又は2において、

前記リストは、前記トリガへの応答を承認されたMTCデバイスの識別子をさらに含み、

前記ネットワークは、前記MTCデバイスの識別子を前記リストに含まれるMTCデバ  
イズの識別子と照合することによって、前記MTCデバイスが前記トリガへの応答を承認  
されているか否かをさらに検証する、

ことを特徴としたシステム。

**【請求項 4】**

請求項1～3のいずれか一項において、

前記ネットワークは、前記検証に成功した際に、前記トリガを前記MTCデバイスへ転  
送する、

ことを特徴としたシステム。

**【請求項 5】**

請求項3において、

前記ネットワークは、さらに、

前記MTCデバイスから、前記トリガへの応答を受信し、

前記MTCデバイスの識別子を前記リストに含まれるMTCデバイスの識別子と照合す  
ることによって、前記MTCデバイスが前記トリガへの応答を承認されているか否かを検  
証し、

前記MTCデバイスが前記トリガへの応答を承認されていると検証した際に、前記応答  
を前記MTCサーバへ転送する、

ことを特徴としたシステム。

**【請求項 6】**

請求項5において、

前記MTCデバイスは、

前記ネットワークにより転送された前記トリガの完全性及び種別をチェックして、前記  
トリガの正当性を検証し、

前記正当性が検証された場合に、前記応答を前記ネットワークへ送信する、

10

20

30

40

50

ことを特徴としたシステム。

【請求項 7】

トリガをMTC(Machine-Type-Communication)サーバからMTCデバイスへ転送するネットワークを形成するノードであって、

前記ネットワークへのアクセスを承認されたMTCサーバの識別子と、各MTCサーバがトリガすることを許可されたMTCデバイスの識別子とが対応付けられたりストを記憶する記憶手段と、

前記MTCサーバから前記トリガを受信した場合、前記MTCサーバの識別子を前記リストに含まれる識別子と照合することによって、前記MTCサーバが前記トリガの送信を許可されているか検証する検証手段と、

を備えたノード。

【請求項 8】

請求項7において、

前記記憶手段は、前記リストを、前記MTCサーバが送信することを承認されたトリガの種別をさらに含むように記憶し、

前記検証手段は、前記トリガの種別を前記リストに含まれる種別と照合することによって、前記トリガが承認されているか否かをさらに検証する、

ことを特徴としたノード。

【請求項 9】

請求項7又は8において、

前記記憶手段は、前記リストを、前記トリガへの応答を承認されたMTCデバイスの識別子をさらに含むように記憶し、

前記検証手段は、前記MTCデバイスの識別子を前記リストに含まれるMTCデバイスの識別子と照合することによって、前記MTCデバイスが前記トリガへの応答を承認されているか否かをさらに検証する、

ことを特徴としたノード。

【請求項 10】

請求項7～9のいずれか一項において、

前記検証手段は、前記検証に成功した際に、前記トリガを前記MTCデバイスへ転送する、

ことを特徴としたノード。

【請求項 11】

請求項9において、

前記検証手段は、さらに、

前記MTCデバイスから、前記トリガへの応答を受信し、

前記MTCデバイスの識別子を前記リストに含まれるMTCデバイスの識別子と照合することによって、前記MTCデバイスが前記トリガへの応答を承認されているか否かを検証し、

前記MTCデバイスが前記トリガへの応答を承認されていると検証した際に、前記応答を前記MTCサーバへ転送する、

ことを特徴としたノード。

【請求項 12】

請求項7～11のいずれか一項において、

MTC-IWF(Inter Working Function)である、

ことを特徴としたノード。

【請求項 13】

ネットワークを形成するノードによりMTC(Machine-Type-Communication)サーバから転送されるトリガを受信するMTCデバイスであって、

前記トリガの完全性及び種別をチェックして、前記トリガの正当性を検証するチェック手段と、

10

20

30

40

50

前記正当性が検証された場合に、前記トリガへの応答を前記ノードへ送信する送信手段と、

を備えたMTCデバイス。

**【請求項14】**

トリガをMTC(Machine-Type-Communication)サーバからMTCデバイスへ転送するネットワークを形成するノードの動作制御方法であって、

前記ネットワークへのアクセスを承認されたMTCサーバの識別子と、各MTCサーバがトリガすることを許可されたMTCデバイスの識別子とが対応付けられたリストを記憶し、

前記MTCサーバから前記トリガを受信した場合、前記MTCサーバの識別子を前記リストに含まれる識別子と照合することによって、前記MTCサーバが前記トリガの送信を許可されているか検証する、

ことを含む方法。

**【請求項15】**

ネットワークを形成するノードによりMTC(Machine-Type-Communication)サーバから転送されるトリガを受信するMTCデバイスの動作制御方法であって、

前記トリガの完全性及び種別をチェックして、前記トリガの正当性を検証し、

前記正当性が検証された場合に、前記トリガへの応答を前記ノードへ送信する、

ことを含む方法。

**【請求項16】**

ネットワークと、

トリガを送信するMTC(Machine-Type-Communication)サーバと、

前記ネットワークにより転送される前記トリガを受信するMTCデバイスと、を備え、前記トリガは、ライフトайムを有し、

前記ネットワークは、

前記トリガの配送に失敗した際、前記ライフトайムが過ぎているか否かをチェックし、前記ライフトайムが過ぎていない場合、前記トリガを前記MTCデバイスへ再送する、システム。

**【請求項17】**

請求項16において、

前記MTCサーバは、前記トリガに、前記トリガを再送可能な回数を示すカウンタを含め、

前記ネットワークは、前記トリガを再送した回数が前記カウンタにより示される回数に達しておらず且つ前記ライフトайムが過ぎていない場合に、前記トリガを繰り返し再送する、

ことを特徴としたシステム。

**【請求項18】**

請求項17において、

前記MTCデバイスは、前記ライフトайムが過ぎているか又は前記トリガが再送された回数が前記カウンタにより示される回数に達している場合に、前記トリガを破棄する、

ことを特徴としたシステム。

**【請求項19】**

請求項16～18のいずれか一項において、

前記ネットワークは、前記トリガに、前記トリガが再送されたトリガであることを示すステータスを含め、

前記MTCデバイスは、前記ステータスを参照して、前記トリガが前記ネットワークにより再送されたか検証する、

ことを特徴としたシステム。

10

20

30

40

50

**【請求項 2 0】**

ネットワークと、  
トリガを送信するM T C (Machine - Type - Communication) サーバと、

前記ネットワークにより転送される前記トリガを受信するM T C デバイスと、を備え、  
前記トリガは、ライフトайムを有し、

前記M T C サーバは、前記トリガの配送に失敗した際、前記ライフトайムが過ぎているか否かをチェックし、前記ライフトайムが過ぎていない場合、前記トリガを前記ネットワークへ再送し、

前記ネットワークは、前記M T C サーバから再送された前記トリガを、前記M T C デバイスへ転送する、

システム。

**【請求項 2 1】**

請求項 2 0 において、  
前記M T C サーバは、

前記トリガを再送した回数が予め定めた回数に達しておらず且つ前記ライフトайムが過ぎていない場合に、前記トリガを繰り返し再送し、

前記トリガに、前記予め定めた回数を示すカウンタを含める、  
ことを特徴としたシステム。

**【請求項 2 2】**

請求項 2 1 において、  
前記M T C デバイスは、前記ライフトайムが過ぎているか又は前記トリガが再送された回数が前記カウンタにより示される回数に達している場合に、前記トリガを破棄する、  
ことを特徴としたシステム。

**【請求項 2 3】**

請求項 2 0 ~ 2 2 のいずれか一項において、  
前記M T C サーバは、前記トリガに、前記トリガが再送されたトリガであることを示すステータスを含め、  
前記M T C デバイスは、前記ステータスを参照して、前記トリガが前記M T C サーバにより再送されたか検証する、

ことを特徴としたシステム。

**【請求項 2 4】**

トリガをM T C (Machine - Type - Communication) サーバからM T C デバイスへ転送するネットワークを形成するノードであって、

前記トリガの配送に失敗した際、前記トリガのライフトайムが過ぎているか否かをチェックするチェック手段と、

前記ライフトайムが過ぎていない場合、前記トリガを前記M T C デバイスへ再送する再送手段と、

を備えたノード。

**【請求項 2 5】**

請求項 2 4 において、  
前記トリガは、前記トリガを再送可能な回数を示すカウンタを含み、  
前記再送手段は、前記トリガを再送した回数が前記カウンタにより示される回数に達しておらず且つ前記ライフトайムが過ぎていない場合に、前記トリガを繰り返し再送する、  
ことを特徴としたノード。

**【請求項 2 6】**

請求項 2 4 又は 2 5 において、  
前記再送手段は、前記トリガに、前記トリガが再送されたトリガであることを示すステータスを含める、  
ことを特徴としたノード。

10

20

30

40

50

**【請求項 27】**

請求項 24～26のいずれか一項において、  
MTC - IWF (Inter Working Function) である、  
ことを特徴としたノード。

**【請求項 28】**

トリガを、ネットワークを介して MTC (Machine - Type - Communication) デバイスへ送信する MTC サーバであって、  
前記トリガの配送に失敗した際、前記トリガのライフタイムが過ぎているか否かをチェックするチェック手段と、

前記ライフタイムが過ぎていない場合、前記トリガを前記ネットワークへ再送する再送手段と、  
10

を備えた MTC サーバ。

**【請求項 29】**

請求項 28において、  
前記再送手段は、さらに、  
前記トリガを再送した回数が予め定めた回数に達しておらず且つ前記ライフタイムが過ぎていない場合に、前記トリガを繰り返し再送し、  
前記トリガに、前記予め定めた回数を示すカウンタを含める、  
ことを特徴とした MTC サーバ。

**【請求項 30】**

請求項 28 又は 29において、  
前記再送手段は、前記トリガに、前記トリガが再送されたトリガであることを示すステータスをさらに含める、  
ことを特徴とした MTC サーバ。  
20

**【請求項 31】**

ネットワークを介して MTC (Machine - Type - Communication) サーバから、トリガを受信する MTC デバイスであって、  
前記トリガのライフタイムが過ぎているか、又は前記トリガを繰り返し受信した回数が前記トリガに含まれるカウンタにより示される回数に達している場合に、前記トリガを破棄する破棄手段、  
30

を備えた MTC デバイス。

**【請求項 32】**

請求項 31において、  
前記トリガに含まれるステータスを参照することによって、前記繰り返し受信したトリガが前記ネットワーク又は前記 MTC サーバにより再送されたか検証する検証手段、  
をさらに備えた MTC デバイス。

**【請求項 33】**

トリガを MTC (Machine - Type - Communication) サーバから MTC デバイスへ転送するネットワークを形成するノードの動作制御方法であって、  
前記トリガの配送に失敗した際、前記トリガのライフタイムが過ぎているか否かをチェックし、  
前記ライフタイムが過ぎていない場合、前記トリガを前記 MTC デバイスへ再送する、  
ことを含む方法。  
40

**【請求項 34】**

トリガを、ネットワークを介して MTC (Machine - Type - Communication) デバイスへ送信する MTC サーバの動作制御方法であって、  
前記トリガの配送に失敗した際、前記トリガのライフタイムが過ぎているか否かをチェックし、  
前記ライフタイムが過ぎていない場合、前記トリガを前記ネットワークへ再送する、  
ことを含む方法。  
50

**【請求項 3 5】**

ネットワークを介してMTC(Machine-Type-Communication)サーバから、トリガを受信するMTCデバイスの動作制御方法であって、

前記トリガのライフタイムが過ぎているか、又は前記トリガを繰り返し受信した回数が前記トリガに含まれるカウンタにより示される回数に達している場合に、前記トリガを破棄する、

ことを含む方法。

**【請求項 3 6】**

ネットワークと、

トリガを送信するMTC(Machine-Type-Communication) 10  
サーバと、

前記ネットワークにより転送される前記トリガを受信するMTCデバイスと、を備え、  
前記MTCサーバは、前記トリガに、前記トリガの緊急レベルを含め、

前記ネットワークは、

前記ネットワークからデタッチした前記MTCデバイスのために、前記緊急レベルをチ  
ェックし、

前記チェックの結果に従って、前記トリガを前記MTCへ転送すべきタイミングを判定  
する、

システム。

**【請求項 3 7】**

請求項3 6において、

前記ネットワークは、前記緊急レベルが予め定めたレベルより低いことを確認した場合  
、前記ネットワークへ再アタッチするための再アタッチ要求が前記MTCデバイスから受  
信されるのを予め定めた期間待機し、前記再アタッチ要求が受信されると、前記トリガを  
転送する、

ことを特徴としたシステム。

**【請求項 3 8】**

請求項3 7において、

前記ネットワークは、前記予め定めた期間を、前記MTCデバイスが前記ネットワーク  
からデタッチする場合に前記MTCデバイスへ送信するメッセージに含めることによって  
、前記MTCデバイスへ通知する、

ことを特徴としたシステム。

**【請求項 3 9】**

請求項3 7において、

前記MTCデバイスは、前記ネットワークからデタッチする場合に、前記ネットワーク  
へ前記予め定めた期間を通知する、

ことを特徴としたシステム。

**【請求項 4 0】**

請求項3 6～3 9のいずれか一項において、

前記ネットワークは、前記緊急レベルが予め定めたレベルより高いことを確認した場合  
、前記トリガを即時に転送すると判定する、

ことを特徴としたシステム。

**【請求項 4 1】**

請求項4 0において、

前記ネットワークは、前記MTCデバイスに対して、前記トリガの受信に用いるべきセ  
キュリティコンテキストを、前記セキュリティコンテキストのインジケータを前記MTC  
デバイスが前記ネットワークからデタッチする場合に前記MTCデバイスへ送信するメッ  
セージに含めることによって、指示する、

ことを特徴としたシステム。

**【請求項 4 2】**

10

20

30

40

50

トリガをMTC (Machine-Type-Communication) サーバからMTCデバイスへ転送するネットワークを形成するノードであって、

前記ネットワークからデタッチした前記MTCデバイスのために、前記トリガに含まれる前記トリガの緊急レベルをチェックするチェック手段と、

前記チェックの結果に従って、前記トリガを前記MTCへ転送すべきタイミングを判定する判定手段と、

を備えたノード。

#### 【請求項43】

請求項42において、

前記判定手段は、前記チェック手段により前記緊急レベルが予め定めたレベルより低いことが確認された場合、前記ネットワークへ再アタッチするための再アタッチ要求が前記MTCデバイスから受信されるのを予め定めた期間待機し、前記再アタッチ要求が受信されると、前記トリガを転送する、

ことを特徴としたノード。

#### 【請求項44】

請求項43において、

前記予め定めた期間を、前記MTCデバイスが前記ネットワークからデタッチする場合に前記MTCデバイスへ送信するメッセージに含めることによって、前記MTCデバイスへ通知する通知手段、

をさらに備えたノード。

#### 【請求項45】

請求項42～44のいずれか一項において、

前記判定手段は、前記チェック手段により前記緊急レベルが予め定めたレベルより高いことが確認された場合、前記トリガを即時に転送すると判定する、

ことを特徴としたノード。

#### 【請求項46】

トリガをMTC (Machine-Type-Communication) サーバからMTCデバイスへ転送するネットワークを形成するノードであって、

前記MTCデバイスに対して、前記トリガの受信に際して用いるべきセキュリティコンテキストを、前記セキュリティコンテキストのインジケータを前記MTCデバイスが前記ネットワークからデタッチする場合に前記MTCデバイスへ送信するメッセージに含めることによって、指示する指示手段、

を備えたノード。

#### 【請求項47】

トリガを、ネットワークを介してMTC (Machine-Type-Communication) デバイスへ送信するMTCサーバであって、

前記トリガに、前記トリガの緊急レベルを含める包含手段、

を備えたMTCサーバ。

#### 【請求項48】

ネットワークを介してMTC (Machine-Type-Communication) サーバから、トリガを受信するMTCデバイスであって、

前記MTCデバイスが前記ネットワークからデタッチする場合に、前記ネットワークへ予め定めた期間を通知する通知手段、を備え、

前記ネットワークは、前記ネットワークへ再アタッチするための再アタッチ要求が前記MTCデバイスから受信されるのを前記予め定めた期間待機し、前記再アタッチ要求が受信されると、前記トリガを転送する、

MTCデバイス。

#### 【請求項49】

トリガをMTC (Machine-Type-Communication) サーバからMTCデバイスへ転送するネットワークを形成するノードの制御方法であって、

10

20

30

40

50

前記ネットワークからデタッチした前記MTCデバイスのために、前記トリガに含まれる前記トリガの緊急レベルをチェックし、

前記チェックの結果に従って、前記トリガを前記MTCへ転送すべきタイミングを判定する、

ことを含む方法。

#### 【請求項 5 0】

トリガをMTC (Machine - Type - Communication) サーバからMTCデバイスへ転送するネットワークを形成するノードの制御方法であって、

前記MTCデバイスに対して、前記トリガの受信に際して用いるべきセキュリティコンテキストを、前記セキュリティコンテキストのインジケータを前記MTCデバイスが前記ネットワークからデタッチする場合に前記MTCデバイスへ送信するメッセージに含めることによって、指示する、

ことを含む方法。

#### 【請求項 5 1】

トリガを、ネットワークを介してMTC (Machine - Type - Communication) デバイスへ送信するMTCサーバの制御方法であって、

前記トリガに、前記トリガの緊急レベルを含める、

ことを含む方法。

#### 【請求項 5 2】

ネットワークを介してMTC (Machine - Type - Communication) サーバから、トリガを受信するMTCデバイスの制御方法であって、

前記MTCデバイスが前記ネットワークからデタッチする場合に、前記ネットワークへ予め定めた期間を通知する、ことを含み、

前記ネットワークは、前記ネットワークへ再アタッチするための再アタッチ要求が前記MTCデバイスから受信されるのを前記予め定めた期間待機し、前記再アタッチ要求が受信されると、前記トリガを転送する、

方法。

#### 【発明の詳細な説明】

##### 【技術分野】

##### 【0 0 0 1】

本発明は、承認されたMTC (Machine - Type - Communication) デバイストリガリング(triggering)のセキュアな配送、ネットワーク及びMTCサーバからMTCデバイスへのトリガリングの再送等の障害処理(failure handling)を含むMTCデバイスのためのセキュアな手段、並びにデタッチした(所謂、オンラインな)MTCデバイスをトリガする方法に関する。

##### 【背景技術】

##### 【0 0 0 2】

非特許文献1に記載される如く、MTCデバイストリガリングは、3GPP (Third Generation Partnership Project) のLTE-A (Long Term Evolution - Advanced) で定義される特徴の一つである。MTCデバイストリガリングは、MTCサーバによりネットワークに対して開始され、MTCデバイスで終端される。MTCサーバは、3GPPネットワークドメインの内部又は外部に存在し得る。悪徳なMTCサーバは、多数のMTCデバイストリガリングメッセージを送信して、ネットワークへ過剰な負荷を掛け得る。また、MTCデバイスが非承認のトリガリングへ応答した場合、バッテリ消費、悪徳なMTCサーバへのデータ送信、及びMTCデバイスの潜在的な誤動作 / 誤設定を引き起こすであろう。このため、承認されたMTCサーバからの正当なトリガリングのみがMTCデバイスへ送信されるべきである。よって、MTCサーバは、3GPPネットワーク及びMTCデバイスとのセキュアな接続を確立して、これらの間におけるエンド・ツー・エンドなセキュリティを有することが可能でなければならない。一方、悪徳なUE (User Equipment) 又はMT

10

20

30

40

50

Cデバイスがトリガリングへ応答することも可能であり、このことは、承認されたデバイスのみにトリガリングへの応答を許可するか、或いはデバイス承認をチェックするためのソリューションを開発することによって防止されるべきである。

### 【0003】

また、MTCデバイストリガリングは、ネットワーク障害等の問題に因り、ターゲットとなるMTCデバイスで受信されない虞もある。トラヒックを低減するために、MTCサーバ及びネットワークの両者がトリガリングを再送可能なべきである。

### 【先行技術文献】

### 【非特許文献】

### 【0004】

【非特許文献1】3GPP TR 23.888、“System Improvements for Machine-Type Communications; (Release 11)”, V1.4.0, 2011年8月

10

### 【発明の概要】

### 【発明が解決しようとする課題】

### 【0005】

MTCサーバと3GPPネットワークが相互に認証されるものとすると、上記の背景技術に基づけば、解決すべき課題は以下の1～7である。

1．ネットワークは、MTCサーバからのメッセージを承認し、トリガを検証可能なべきである。これは、MTCサーバの非承認の動作を防止するためである。

20

2．ネットワークは、異なるトリガの種別を識別可能であり、以てトリガが、承認されたMTCデバイスのみへ、これらの契約に基づいて送信されるようにすべきである。

3．トリガからのネットワーク輻輳インパクトが回避されるべきである。

4．MTCデバイスは、非承認のMTCサーバ及びメッセージからのアタック又はMTCデバイスへのインパクトを防止するよう、トリガ及びその送信元を検証可能なべきである。

5．トリガの鮮度及びライフタイムに係るソリューションが、リプレイアタック及びトリガの再送に因るネットワーク負荷を防止するように存在すべきである。

6．トリガのアグリゲーション及びセキュリティが、ネットワークにおけるトラヒックを低減するように検討されるべきである。

30

7．その他の問題を回避するために、ソリューションは、トリガ送信のリトライ及びMTCユーザへの通知を含む障害処理を考慮可能なべきである。

### 【課題を解決するための手段】

### 【0006】

本発明の態様では、MTCサーバにより3GPPネットワークを介して示されるMTCデバイストリガリングを検討する。MTCサーバは3GPPネットワーク外に存在可能であり、特定且つ承認されたMTCサーバからの承認されたトリガリングのみがMTCデバイスへ示されるであろう。同様にして、認証且つ承認されたMTCデバイスのみが、正当なトリガリングへの応答を許可されるであろう。ネットワーク及びMTCデバイスの両者が、MTCサーバ及びこれらのトリガを承認可能であろう。

40

### 【0007】

3GPPネットワードメイン外のMTCサーバは、例えば3GPPネットワークとのセキュアな通信が存在する場合であっても、MTCデバイスとのセキュアな接続を確立することを要求される。トリガリングコンテンツは保護され、MTCデバイスはトリガを検証可能であろう。ここで、検証手段は、メッセージの完全性、トリガの送信元、メッセージがライフタイム内にリプレイされたか否か、及びトリガがMTCデバイスにとってアクションを起こすべき種別のものであるか否かをチェック可能である。MTCデバイスは、承認されたMTCサーバのリストを配備しても良く、トリガリングの受信に際し、リストに応じた検証を行うことが可能である。不当に送信されたトリガの受信を防止するため、ネットワークは、トリガ種別を識別可能であろう。

50

**【0008】**

トリガリングメッセージは、アタッカーによって後に単純にコピーされたり再利用されたりしないよう、ライフタイムを有していても良い。ネットワーク障害又はその他に際して、MTCサーバは、トリガリングメッセージを再送可能である。同様に、ネットワークは、トリガライフタイム内でMTCデバイスへの再送が可能である。MTCサーバ及びネットワークの両者が、トリガのリプレイアタックを防止するソリューションを提供する。

**【0009】**

MTCデバイスは、エネルギー節約のためにデタッチ状態(所謂、オフライン)に在り得る。ネットワークは、MTCデバイスへ、アタッチのためのタイマを、MTCデバイスに対するDetach Accept又はDetach Acceptにおいて送信可能である。よって、ネットワークは、MTCサーバからMTCデバイストリガリングを受信すると、タイマの有効性をチェック可能である。タイマが有効である場合、ネットワークは、トリガリングを保持し、MTCデバイスのアタッチを待機するであろう。タイマが有効で無い場合、ネットワークは、MTCデバイスがアタッチしている(所謂、オンラインの)場合と同様にして、トリガリングを送信可能である。タイマは、契約上で定義されるか、或いはMTCサーバによりネットワークへ伝えることも可能である。

**【発明の効果】****【0010】**

本発明によれば、無効なトリガリングメッセージの送信を防止することにより、不要なネットワークトラヒックを低減し、MTCデバイスのバッテリ浪費を低減することが可能である。

**【0011】**

トリガリングに係るMTCサーバ及びMTCデバイスの承認は、悪徳なMTCサーバ、若しくはMTCデバイスへトリガすることを承認されていないMTCサーバからの無効なトリガリングメッセージがMTCデバイスへ送信されること、又はトリガリングへの応答を承認されていないMTCデバイスへ送信されることを防止するであろう。

**【0012】**

一のソリューションは、MTCデバイスに周期的なAttach Requestを行わせて、MTCデバイスへ送信されるトリガリングが存在するかチェックさせるものであり得る。しかしながら、このソリューションは、不要なバッテリ消費及びトラヒックを招く。MTCサーバは、MTCデバイスへいつトリガするか知っているならば、トリガ頻度に応じて、MTCデバイスにネットワークへアタッチさせるか或いはアイドルに留めさせることが可能である。

**【0013】**

ネットワークからMTCデバイスへのトリガリング送信のセキュアなリトライは、MTCサーバへの干渉及びトリガリングメッセージの悪用を防止するであろう。

**【0014】**

デタッチしている(オフライン)MTCデバイスは、必ずしも、ネットワークがトリガリングメッセージを受信すると直ちにトリガされるべきでは無い。しかしながら、ネットワークは、緊急状態、及びネットワークがMTCデバイスへ割り当てたアタッチ用タイマの有効性に応じて、いつトリガリングメッセージを送信すべきか判定可能である。

**【0015】**

トリガは、MTCサーバ、トリガメッセージの承認、並びにメッセージの完全性及び機密性保護を行うことにより、MTCデバイスへセキュアに配送される。

**【図面の簡単な説明】****【0016】**

【図1】本発明の実施の形態1に係るシステムの構成例を示したブロック図である。

【図2】実施の形態1に係るシステムにおける第1の動作例を示したシーケンス図である。

【図3】実施の形態1に係るシステムにおける第2の動作例を示したシーケンス図である

10

20

30

40

50

。【図4】実施の形態1に係るシステムにおける第3の動作例を示したシーケンス図である。

。【図5】本発明の実施の形態2に係るシステムの構成例を示したブロック図である。

【図6】実施の形態2に係るシステムにおける第1の動作例を示したシーケンス図である。

。【図7】実施の形態2に係るシステムにおける第2の動作例を示したシーケンス図である。

。【図8】実施の形態2に係るシステムにおける第3の動作例を示したシーケンス図である。

。【図9】実施の形態に係るノードの構成例を示したブロック図である。

【図10】実施の形態に係るノードの他の構成例を示したブロック図である。

【図11】実施の形態に係るMTCサーバの構成例を示したブロック図である。

【図12】実施の形態に係るMTCデバイスの構成例を示したブロック図である。

【発明を実施するための形態】

【0017】

以下、本発明の実施の形態1及び2を説明する。

【0018】

[実施の形態1]

図1に示すように、本実施の形態に係るシステムは、3GPPネットワーク10と、MTCサーバ20と、MTCデバイス30とを含む。

【0019】

本願の発明者らは、このようなシステムにおいて、例えば次の脅威がMTCデバイストリガリングに対して特定されることを見出した。

【0020】

<脅威>

ネットワークは、MTCサーバから送信されるトリガインジケーション(以下、このインジケーションを“トリガリングメッセージ”と呼称することがある)に基づき、MTCデバイスをトリガして、MTCサーバとの通信を開始させる。このことは、特にMTCサーバが図1に示す如くオペレータドメインの外部に存在する場合に、アタッカーにとっての機会を広げるであろう。

【0021】

アタッカーは、MTCサーバになりすまして偽りのトリガインジケーションをネットワークへ送信し得て、ネットワークがアタッカーにより対応MTCデバイスをトリガするために利用される。このことは、多数のMTCデバイスがトリガされて同時に認証が要求される程に、MTCデバイスの電力浪費に繋がり得るMTCデバイスの誤判定を引き起こし、ネットワークに対するDOSアタックすら引き起こすであろう。よって、アタッカーは、このことを巧みに操って、そのアタック目標を達成し得る。

【0022】

MTCサーバは、うかつにも例えばソフトウェアアップデータのためにMTCデバイスをトリガしてMTCデバイスへ重大な被害を及ぼし得るから、MTCデバイスに対する完全な制御権を有していないであろう。

【0023】

アタッカーは、外部インターフェース上で、MTCデバイス識別子等のプライバシーな機密情報を盗聴し得る。

【0024】

これらの脅威に対処するため、特にMTCサーバが3GPPオペレータドメインの外部に設定される場合には、次のセキュリティ要件を適用する。

【0025】

<セキュリティ要件>

10

20

30

40

50

3 GPP ネットワークは、(1) MTC サーバが MTC デバイスと通信することを承認されているか否か、及び(2) MTC サーバが特定の MTC デバイスへ特定のトリガを送信することを承認されているか否かを判定可能なべきである。

#### 【0026】

これらのセキュリティ要件を満たすソリューションを、主要論点として説明する。

#### 【0027】

##### <ソリューション>

3 GPP ネットワークは、特定の MTC デバイスへのトリガ送信を承認された MTC サーバ、及び当該 MTC サーバが送信を承認されたトリガの種別のリストを維持すべきである。このリストは、MTC デバイスの識別子、MTC サーバの識別子、及び関連する許可されたトリガリングを含むべきである。このように、トリガ毎に、3 GPP ネットワークは、MTC サーバがトリガ送信を許可されているか否か及びトリガが承認されているか否かを検証する。

10

#### 【0028】

次に、本実施の形態の詳細を説明する。

#### 【0029】

本実施の形態は、3つの主たる課題を考慮に入れる。

I . 承認された MTC デバイストリガリングのセキュアな配送

II . 障害処理：ネットワーク及び MTC サーバから MTC デバイスへのトリガリング送信のリトライ

20

III . デタッチした(オフライン) MTC デバイスをトリガすること

#### 【0030】

次の通り、幾つかの前提を立てる。

1 . MTC サーバは 3 GPP ドメインネットワークの内 / 外に存在する。

2 . MTC デバイス及びネットワークは相互認証を有する。

3 . MTC サーバ及びネットワークは相互認証を有する。

30

#### 【0031】

I (MTC デバイストリガリングのセキュアな配送)を達成するため、トリガメッセージは、完全性を有するべきであり、機密性が保護され得る。ネットワークは、トリガの完全性及び機密性チェックを行う。

30

#### 【0032】

そして、ネットワークは、MTC サーバの承認を行う。ネットワークは、MTC デバイス ID (identity)、MTC サーバ ID 及び関連する加入者(契約)情報を含むリストを伴って配備される。MTC サーバは、ターゲット MTC デバイス ID、MTC サーバ ID、及びオプションとして加入者 ID を含むトリガリングを送信するであろう。ネットワークは、トリガリングを受信すると、リストに応じて MTC サーバの承認を行って、MTC サーバがターゲット MTC デバイスをトリガすることを承認されているか、及び MTC デバイスがトリガリングへの応答を承認されているかを検証するであろう。MTC サーバ、MTC デバイス及び(このケースでは登場する)契約に対する承認に成功した場合のみ、ネットワークは、MTC デバイストリガリングを続行するであろう。

40

#### 【0033】

そして、ネットワークは、トリガメッセージの承認を行う。トリガメッセージは、トリガ種別とトリガ本文とを含む。トリガ種別は、緊急レベル、加入者情報、及びアグリゲーション / ブロードキャストトリガ / グループトリガの可用性等から成る。トリガ本文は、期待される MTC デバイスの動作、例えば、データを返信すること、ソフトウェアをアップデートすること、ネットワークへアタッチすること、ネットワークからデタッチすること等を含む。ネットワークは、トリガ種別をチェックして、トリガメッセージが MTC デバイスへの送信が承認されているか検証する。トリガ種別チェックの成功の後、ネットワークは、トリガメッセージを MTC デバイスへ転送するであろう。

50

#### 【0034】

また、トリガインジケーション(メッセージ)を受信したMTCデバイスは、完全性チェック及びトリガ種別チェックを行って、トリガの正当性を検証するであろう。正当性が検証された後にのみ、MTCデバイスは、ネットワークを介してMTCサーバへ応答するであろう。

#### 【0035】

また、ネットワークは、MTCデバイスからMTCサーバへの応答も検証するであろう。ここで、検証とは、特定のMTCデバイスが宛先のMTCサーバとの通信を許可されているか否かチェックすることである。非認証又は誤った通信は、ユーザへ通知されるであろう。

#### 【0036】

I I (障害処理：ネットワーク及びMTCサーバからMTCデバイスへのトリガリング送信のリトライ)を達成するため、トリガのMTCデバイスへの配送に失敗し且つこのことがMTCサーバへ通知されると、MTCサーバは、トリガ送信をリトライすることが可能である。また、ネットワークがMTCデバイスへのトリガ送信をリトライすることも要求される。トリガは、ライフタイムを有しており、このライフタイムが過ぎている場合には、MTCサーバ又はネットワークから送出されるべきでは無い。また、ライフタイムの過ぎたトリガを受信したMTCデバイスは、トリガを破棄すべきである。頻度、及び何回に亘ってトリガを再送可能であるかの上限は、MTCサーバとネットワークとの間で定義且つ同期される。

#### 【0037】

ネットワークは、それをMTCサーバから受信した後に、リトライを開始するであろう。或いは、MTCサーバは、ネットワークへ、MTCデバイスへのトリガリングメッセージ送信のリトライが必要かどうかを指示する。

#### 【0038】

通常、ネットワークは、トリガのライフタイム迄はトリガをMTCデバイスへ再送でき、MTCサーバは、トリガのライフタイムが終了した後にトリガをネットワークへ再送するであろう。

#### 【0039】

リプレイアタックを防止するため、トリガリングメッセージのレシーバは、トリガリングメッセージがリトライメッセージであるか或いはオリジナルメッセージであるかを識別可能なべきである。トリガリングメッセージは、その状態(オリジナル又はリトライ)を示すパラメータを含むべきであり、何回リトライされたかのカウンタが、リトライメッセージ中に定義される。

#### 【0040】

ネットワークは、非承認のトリガリングメッセージが承認されたMTCサーバから受信された場合、MTCユーザへの通知を送信する。この通知は、SMS、Eメール又はログへの記録等の何らかの手段によって送信可能である。更なる非承認のトリガは、破棄されるべきであり、MTCサーバが非承認のトリガを送信し続けるならば、ネットワークは、当該MTCサーバとの通信を一時停止すべきである。

#### 【0041】

I I I (デタッチした(オンライン)MTCデバイスをトリガすること)を達成するため、オフラインMTCデバイスは、所定のインターバルの間、通信を必要とせず且つ通信すべきものも有していないから、スタンバイ又はスリープモードへ移行してバッテリ電力を節約する。このインターバルは、MTCデバイスがインターバルの後に周期的に起床するという意味では固定であり、或いは可変である。オフラインMTCデバイスにとって、MTCサーバからのトリガリングがあると直ちに起床する必要が無いかも知れないし、或いはMTCサーバの要求に応じて即時に起床すべきであるかも知れない。

#### 【0042】

いつトリガをMTCデバイスへ送信すべきか判定するため、まずネットワークは、トリガ種別フィールド中の緊急レベルをチェックするであろう。高い緊急レベルを有するトリ

10

20

30

40

50

ガは、即時にMTCデバイスへ送信されるであろう。緊急レベルが低い場合、ネットワークは、オフラインタイマ(又はアタッチのための時間)が有効かチェックするであろう。有効で無い場合、ネットワークは、即時にトリガを送信するであろう。オフラインタイマが有効な場合、ネットワークは、トリガを送信するに先立って、タイマが満了した後に送信されるMTCデバイスからのアタッチ要求を待機するであろう。

#### 【0043】

アタッチのための時間は、ネットワークからMTCデバイスへ送信され、この時間は、Detach Request又はDetach Accept(他のメッセージも存在し得る)のいずれかに含まれ得る。このタイマは、MTCサーバからネットワークへ通知され得るか、或いは契約時に合意され得る。なお、MTCデバイスが、タイマをネットワーク及びMTCサーバへ通知しても良い。

10

#### 【0044】

既存の仕様とは異なり、MTCデバイスがデタッチしている場合であっても、トリガをMTCデバイスへ送信できる。よって、緊急メッセージのために(或いはオフラインタイマが満了した後に)使用すべきセキュリティコンテキストは、MTCデバイスがデタッチ状態へ遷移する前に合意されるべきである。セキュリティコンテキストは、デタッチ手順(例えば、Detach Acceptメッセージ又はDetach Requestメッセージ)の間に指示若しくはネゴシエートされ得て、MTCデバイスは、トリガリングメッセージを解読でき、また将来のメッセージを保護できる。

20

#### 【0045】

次に、本実施の形態の動作例を、図2～図4を参照してより詳細に説明する。

#### 【0046】

図2は、承認されたMTCデバイストリガのセキュアな配送という第1の課題のための動作例を示している。

#### 【0047】

MTCデバイス30及びネットワーク10は相互認証を有するものとする(ステップS11)。また、ネットワーク10及びMTCサーバ20は相互認証を有するものとする(ステップS12)。

30

#### 【0048】

ネットワーク10は、承認されたMTCサーバのリストを記憶する。このリストは、MTCサーバID、許可されたターゲットMTCデバイスID、加入者情報、MTCデバイスへの許可されたトリガ種別を含む(ステップS13)。

#### 【0049】

MTCサーバ20は、MTCデバイストリガをネットワーク10へ送信する(ステップS14)。

30

#### 【0050】

ネットワーク10は、リストと照合して、MTCサーバ20が特定のMTCデバイス30へのトリガ送信を承認されていか否か、及びMTCデバイス30が特定のトリガ種別への応答を許可されているかをチェックする(ステップS15)。例えば、ネットワーク10は、受信したトリガに含まれるMTCサーバ20のIDがリストに含まれるMTCサーバIDと一致し、且つトリガに含まれるトリガ種別がリストに含まれる許可されたトリガ種別と一致する場合に、MTCサーバ20が特定のトリガ種別を送信することを許可されていると検証しても良い。また、ネットワーク10は、トリガに含まれるMTCデバイス30のIDがリストに含まれるMTCデバイスIDと一致する場合に、MTCデバイス30がトリガへの応答を許可されていると検証しても良い。

40

#### 【0051】

ネットワーク10は、ステップS15でのチェックに通過した場合、トリガメッセージをMTCデバイス30へ転送する(ステップS16)。

#### 【0052】

MTCデバイス30は、トリガメッセージを受信すると、完全性チェックを行うと共に

50

、トリガ種別をチェックする(ステップS17)。

【0053】

MTCデバイス30は、適切な応答をネットワーク10へ送信する(ステップS18)。

【0054】

ネットワーク10は、リストとの照合により、ステップS15と同様にして、MTCデバイス30が応答を許可されているか否かをチェックする(ステップS19)。

【0055】

ネットワーク10は、トリガ応答をMTCサーバ20へ転送する(ステップS20)。

【0056】

図3は、障害処理という第2の課題のための動作例を示している。

10

【0057】

MTCデバイス30及びネットワーク10は相互認証を有するものとする(ステップS21)。また、ネットワーク10及びMTCサーバ20は相互認証を有するものとする(ステップS22)。

【0058】

MTCサーバ20は、MTCデバイストリガメッセージを送信する(ステップS23)。但し、トリガメッセージの配送に失敗した際(ステップS24)、ネットワーク10(ステップS24)又はMTCサーバ20(ステップS25)の一方が、トリガライフタイムが過ぎているか否か、及び/又はリトライカウンタを超過しているか否かをチェックすることが可能である。

20

【0059】

具体的には、ネットワーク10は、トリガライフタイムが過ぎているか、及び/又はリトライカウンタが制限に達しているかをチェックする(ステップS24a)。ステップS24aのいずれも生じていなければ、ネットワーク10は、トリガのリトライメッセージをMTCデバイス30へ転送するであろう(ステップS24b)。

【0060】

或いは、MTCサーバ20が、ネットワーク10と同様のチェックを行う(ステップS25a)。チェックに通過した場合、MTCサーバ20は、ネットワーク10へのトリガメッセージ送信をリトライする(ステップS25b)。ネットワーク10は、リトライトリガメッセージを転送する(ステップS25c)。

30

【0061】

MTCデバイス30は、トリガがリトライメッセージであるか検証する(ステップS26)。

【0062】

MTCデバイス30は、そのライフタイムが過ぎているか或いはリトライカウンタを超過しているリトライトリガメッセージを受信した場合、トリガを破棄するであろう(ステップS27)。

【0063】

図4は、オフラインMTCデバイスをトリガするとの第3の課題のための動作例を示している。

40

【0064】

MTCデバイス30及びネットワーク10は相互認証を有するものとする(ステップS31)。また、ネットワーク10及びMTCサーバ20は相互認証を有するものとする(ステップS32)。

【0065】

MTCデバイス30がオフラインへ移行した(例えば、Detach Request又はDetach Acceptがネットワーク10からMTCデバイス30へ送信された)デタッチ手順の間、ネットワーク10は、MTCデバイス30へ、再アタッチタイマ及びセキュリティコンテキストインジケータを送信する(ステップS33a)。或いは、MTCデバイス30が、ネットワーク10へ再アタッチタイマを送信して、次回にいつネットワ

50

ーク 1 0 ヘアタッチするかを知らせることもできる(ステップ S 3 3 b)。

【 0 0 6 6 】

M T C デバイス 3 0 は、オフラインである(ステップ S 3 4)。

【 0 0 6 7 】

M T C サーバ 2 0 は、M T C デバイストリガメッセージをオフライン M T C デバイス 3 0 へ送信する。このメッセージは、トリガ種別を含む(ステップ S 3 5)。

【 0 0 6 8 】

ネットワーク 1 0 は、トリガの緊急レベルをチェックするであろう(ステップ S 3 6)。トリガが高い緊急レベルを有している場合(ステップ S 3 7)、ネットワーク 1 0 は、トリガメッセージを即時に転送する(ステップ S 3 8)。

10

【 0 0 6 9 】

トリガが低い緊急レベルを有している場合には(ステップ S 3 9)、ネットワーク 1 0 は、再アタッチタイマをチェックする(ステップ S 3 9 a)。ネットワーク 1 0 は、再アタッチタイマが満了する迄、M T C デバイス 3 0 からの `re-Attach request` を待機する(ステップ S 3 9 b)。その後、ネットワーク 1 0 は、トリガメッセージを転送するであろう(ステップ S 3 9 c)。

【 0 0 7 0 】

[実施の形態 2]

図 5 に示すように、本実施の形態に係るシステムにおいて、ネットワーク 1 0 は、M T C - I W F (I n t e r - W o r k i n g F u n c t i o n) 4 0 を含む。M T C - I W F 4 0 は、M T C デバイス 3 0 と S C S (S e r v i c e C a p a b i l i t y S e r v e r) 6 0 との間でメッセージを中継するノードとして機能する。S C S 6 0 は、図 1 に示した M T C サーバ 2 0 として機能する。ネットワーク 1 0 は、他のノードとして、H S S (H o m e S u b s c r i b e r S e r v e r)、M M E (M o b i l i t y M a n a g e m e n t E n t i t y)、S G S N (S e r v i n g G P R S (G e n e r a l P a c k e t R a d i o S e r v i c e) S u p p o r t N o d e)、M S C (M o b i l e S w i t c h i n g C e n t r e) 等を含む。以降の説明においては、M M E、S G S N 及び M S C を “M M E / S G S N / M S C” と呼称し、符号 5 0 で総称することがある。M T C デバイス 3 0 と M T C - I W F 4 0 の間の通信は、M M E / S G S N / M S C 5 0 及び R A N (R a d i o A c c e s s N e t w o r k) を介して行われる。なお、M T C デバイス 3 0 は、M T C 用に装備された U E (U s e r E q u i p m e n t)。

20

30

【 0 0 7 1 】

次に、本実施の形態の動作例を、図 6 ~ 図 8 を参照して詳細に説明する。

【 0 0 7 2 】

図 6 は、承認された M T C デバイストリガのセキュアな配達という第 1 の課題のための動作例を示している。

【 0 0 7 3 】

M T C デバイス 3 0 、及び M M E / S G S N / M S C 5 0 、M T C - I W F 4 0 は相互認証を有しているものとする(ステップ S 4 1)。また、M T C - I W F 4 0 及び S C S 6 0 は相互認証を有しているものとする(ステップ S 4 2)。

40

【 0 0 7 4 】

M T C - I W F 4 0 は、承認された M T C サーバ(この例では S C S )のリストを記憶する。このリストは、M T C サーバ I D (この例では S C S I D)、許可されたターゲット M T C デバイスの I D、加入者情報、M T C デバイスへの許可されたトリガ種別を含む(ステップ S 4 3)。

【 0 0 7 5 】

S C S 6 0 は、M T C デバイストリガを M T C - I W F 4 0 へ送信する(ステップ S 4 4)。

【 0 0 7 6 】

50

MTC-IWF\_40は、リストとの照合により、SCS\_60がターゲットMTCデバイス30への特定のトリガ種別の送信を承認されていか否か、及びMTCデバイス30がSCS\_60からの特定のトリガ種別への応答を許可されているかをチェックする(ステップS45)。

【0077】

MTC-IWF\_40は、ステップS45でのチェックに通過した場合、トリガメッセージをMTCデバイス30へ転送する(ステップS46)。

【0078】

MTCデバイス30は、トリガメッセージを受信すると、完全性チェックを行うと共に、トリガ種別をチェックする(ステップS47)。  
10

【0079】

MTCデバイス30は、適切な応答をMTC-IWF\_40へ送信する(ステップS48)。

【0080】

MTC-IWF\_40は、MTCデバイス30が応答を許可されているか否かをチェックする(ステップS49)。

【0081】

MTC-IWF\_40は、トリガ応答をSCS\_60へ転送する(ステップS50)。

【0082】

図7は、障害処理という第2の課題のための動作例を示している。

20  
【0083】

MTCデバイス30、及びMME/SGSN/MSC\_50、MTC-IWF\_40は相互認証を有しているものとする(ステップS51)。また、MTC-IWF\_40及びSCS\_60は相互認証を有しているものとする(ステップS52)。

【0084】

SCS\_60は、MTCデバイストリガメッセージをMTC-IWF\_40へ送信する(ステップS53)。そして、MTC-IWF\_40は、MTCデバイストリガメッセージを転送する(ステップS54)。但し、トリガメッセージの配送に失敗した際(ステップS24)、MTC-IWF\_40(ステップS55)又はSCS\_60(ステップS56)の一方が、トリガライフタイムが過ぎているか否か、及び/又はリトライカウンタを超過しているか否かをチェックすることが可能である。  
30

【0085】

具体的には、MTC-IWF\_40は、トリガライフタイムが過ぎているか、及び/又はリトライカウンタが制限に達しているかをチェックする(ステップS55a)。ステップS55aのいずれも生じていなければ、MTC-IWF\_40は、トリガのリトライメッセージをMTCデバイス30へ転送するであろう(ステップS55b)。

【0086】

或いは、SCS\_60が、MTC-IWF\_40と同様のチェックを行う(ステップS56a)。チェックに通過した場合、SCS\_60は、MTC-IWF\_40へのトリガメッセージ送信をリトライする(ステップS56b)。MTC-IWF\_40は、リトライトリガメッセージを転送する(ステップS56c)。  
40

【0087】

MTCデバイス30は、トリガがリトライメッセージであるか検証する(ステップS57)。

【0088】

MTCデバイス30は、そのライフタイムが過ぎているか或いはリトライカウンタを超過しているリトライトリガメッセージを受信した場合、トリガを破棄するであろう(ステップS58)。

【0089】

図8は、オフラインMTCデバイスをトリガするとの第3の課題のための動作例を示し

50

ている。

【0090】

MTCデバイス30、及びMME/SGSN/MSC50、MTC-IWF40は相互認証を有しているものとする(ステップS61)。また、MTC-IWF40及びSCS60は相互認証を有しているものとする(ステップS62)。

【0091】

MTCデバイス30がオフラインへ移行した(例えば、Detach Request又はDetach Acceptがネットワーク10からMTCデバイス30へ送信された)デタッチ手順の間、MME/SGSN/MSC50は、MTCデバイス30へ、再アタッチタイマ及びセキュリティコンテキストインジケータを送信する(ステップS63a)。或いは、MTCデバイス30が、MME/SGSN/MSC50へ再アタッチタイマを送信して、次回にいつネットワーク10へアタッチするかを知らせることもできる(ステップS63b)。

【0092】

MTCデバイス30は、オフラインである(ステップS64)。

【0093】

MME/SGSN/MSC50は、再アタッチタイマをMTC-IWF40へ送信する(ステップS65)。

【0094】

SCS60は、MTCデバイストリガメッセージをオフラインMTCデバイス30へ送信する。このメッセージは、トリガ種別を含む(ステップS66)。

【0095】

MTC-IWF40は、トリガの緊急レベルをチェックするであろう(ステップS67)。トリガが高い緊急レベルを有している場合(ステップS68)、MTC-IWF40は、トリガメッセージを即時に転送する(ステップS68a)。

【0096】

トリガが低い緊急レベルを有している場合には(ステップS69)、MTC-IWF40は、再アタッチタイマをチェックする(ステップS69a)。再アタッチタイマが満了するより前にMTCデバイス30からのreattach requestがあったならば、MTC-IWF40は、トリガメッセージを転送するであろう(ステップS69c)。

【0097】

次に、上述した実施の形態に係る、MTC-IWF40、MME/SGSN/MSC50、MTCサーバ20(SCS60)及びMTCデバイス30の構成例を、図9～図12を参照して順に説明する。

【0098】

図9に示すように、MTC-IWF40は、承認されたMTCデバイストリガのセキュアな配送という第1の課題のために、記憶部41と、検証部42とを含む。記憶部41は、上記のリストを記憶する。検証部42は、リストを照合することによって、MTCサーバ20(SCS60)、MTCデバイス30及びトリガメッセージの種別が承認されたものであるか否かを検証する。これらのユニット41及び42に代えて或いは加えて、MTC-IWF40は、障害処理という第2の課題のために、チェック部43と、再送部44とを含む。チェック部43は、上記のトリガライフタイム及びノアリトライカウンタをチェックする。再送部44は、トリガライフタイムが過ぎていない場合、及びノアリトライカウンタを超過していない場合に、トリガメッセージを再送する。これらのユニット41、42及び44に代えて或いは加えて、MTC-IWF40は、オフラインMTCデバイスをトリガするとの第3の課題のために、チェック部43と、判定部45とを含む。この場合、チェック部43は、上記の緊急レベルをチェックする。判定部45は、緊急レベルに従って、トリガメッセージを転送すべきタイミングを判定する。また、MTC-IWF40は、通知部46を含んでも良い。通知部46は、MTCデバイス30へ

10

20

30

40

50

上記の再アタッチタイマを通知する。なお、これらのユニット41～46は、バス等を介して相互接続される。これらのユニット41～46は、例えば、MTCサーバ20及びMTCデバイス30とそれぞれ通信するトランシーバと、これらのトランシーバを制御して、図2のステップS11～S16、S19及びS20に示した処理、図3のステップS21～S25に示した処理、図4のステップS31～S39に示した処理、図6のステップS41～S46及びS48～S50に示した処理、図7のステップS51～S56に示した処理、図8のステップS61、S62及びS62～S69に示した処理、或いはこれらと同等の処理を実行するコントローラと、で構成可能である。

#### 【0099】

図10に示すように、MME/SGSN/MSC50は、指示部51を含む。指示部51は、MTCデバイス30に対して、上記のセキュリティコンテキストを指示する。このユニット51は、例えば、MTCデバイス30及びMTC-IWF40とそれぞれ通信するトランシーバと、これらのトランシーバを制御して、図8のステップS63～S65に示した処理或いはこれと同等の処理を実行するコントローラと、で構成可能である。10

#### 【0100】

また、図11に示すように、MTCサーバ20(SCS60)は、障害処理という第2の課題のために、チェック部21と、再送部22とを含む。チェック部21は、トリガライフタイム及び/又はリトライカウントをチェックする。再送部22は、トリガライフタイムが過ぎていない場合、及び/又はリトライカウンタを超過していない場合に、トリガメッセージを再送する。これらのユニット21及び22に代えて或いは加えて、MTCサーバ20は、オフラインMTCデバイスをトリガすると第3の課題のために、包含部23を含む。包含部23は、トリガメッセージに緊急レベルを含める。なお、これらのユニット21～23は、バス等を介して相互接続される。これらのユニット21～23は、例えば、MTC-IWF40と通信するトランシーバと、このトランシーバを制御して、図3のステップS22、S23及びS25に示した処理、図4のステップS32、S33及びS35に示した処理、図7のステップS52、S53及びS56に示した処理、図8のステップS62及びS66に示した処理、或いはこれらと同等の処理を実行するコントローラと、で構成可能である。20

#### 【0101】

さらに、図12に示すように、MTCデバイス30は、承認されたMTCデバイストリガのセキュアな配送という第1の課題のために、チェック部31と、送信部32とを含む。チェック部31は、上記の完全性及びトリガ種別チェックを行う。送信部32は、チェックに通過した場合、MTC-IWF40への応答を送信する。これらのユニット31及び32に代えて或いは加えて、MTCデバイス30は、障害処理という第2の課題のために、破棄部33を含む。破棄部33は、トリガライフタイムが過ぎた場合又はリトライカウンタを超過した場合に、トリガメッセージを破棄する。MTCデバイス30は、検証部34を含んでも良い。検証部34は、上述したステータス(オリジナル又はリトライ)を参照することによって、トリガメッセージがリトライメッセージか検証する。これらのユニット31～34に代えて或いは加えて、MTCデバイス30は、オフラインMTCデバイスをトリガると第3の課題のために、通知部35を含む。通知部35は、MTC-IWF40へ再アタッチタイマを通知する。なお、これらのユニット31～35は、バス等を介して相互接続される。これらのユニット31～35は、例えば、MTC-IWF40と通信するトランシーバと、このトランシーバを制御して、図2のステップS11及びS16～S18に示した処理、図3のステップS21及びS23～S27に示した処理、図4のステップS31、S33、S34及びS37～S39に示した処理、図6のステップS41及びS46～S48に示した処理、図7のステップS51及びS54～S58に示した処理、図8のステップS61、S63、S64、S68及びS69に示した処理、或いはこれらと同等の処理を実行するコントローラと、で構成可能である。40

#### 【0102】

なお、本発明は、上記の実施の形態によって限定されるものではなく、特許請求の範囲50

の記載に基づき、当業者によって種々の変更が可能なことは明らかである。

**【0103】**

この出願は、2011年10月28日に出願された日本出願特願2011-236699を基礎とする優先権を主張し、その開示の全てをここに取り込む。

**【0104】**

上記の実施の形態の一部又は全部は、以下の付記のようにも記載され得るが、以下には限られない。

**【0105】**

(付記1)

ネットワークでのトリガの検証

ネットワークは、MTCサーバ及びトリガの両者に対する承認を行って、トリガが承認されたMTCサーバからのものであるか及び正当なものであるか検証する。

**【0106】**

(付記2)

MTCデバイスでのトリガの検証

MTCデバイスは、トリガが承認されたMTCサーバからのものであるか、及びその契約に応じたトリガの正当性の両者を検証する。

**【0107】**

(付記3)

ネットワークでの、MTCデバイスからMTCサーバへのメッセージの検証。

**【0108】**

(付記4)

MTCサーバ及びネットワークは、トリガの鮮度を維持しつつ、例えばネットワーク障害に際して、MTCデバイストリガリングメッセージの送信をリトライする。

**【0109】**

(付記5)

ネットワークは、MTCユーザへ非承認のトリガ受信について通知すると共に、トリガを送信するMTCサーバとの更なる通信を一時停止することが可能である。通知には、SMS、Eメールを介して、或いはログに記録すること等、手段を選ばない。

**【0110】**

(付記6)

ネットワークは、緊急レベル及びアタッチ用タイマに応じて、トリガをデタッチした(オフラインの)MTCデバイスへ送信する。

**【0111】**

(付記7)

ネットワークは、次の通信において用いるべきメッセージのセキュリティコンテキストを指示する。

**【符号の説明】**

**【0112】**

10 ネットワーク

20 MTCサーバ

21, 31, 43 チェック部

22 再送部

23 包含部

30 MTCデバイス

32 送信部

33 破棄部

34, 42 検証部

35, 46 通知部

40 MTC - IWF

10

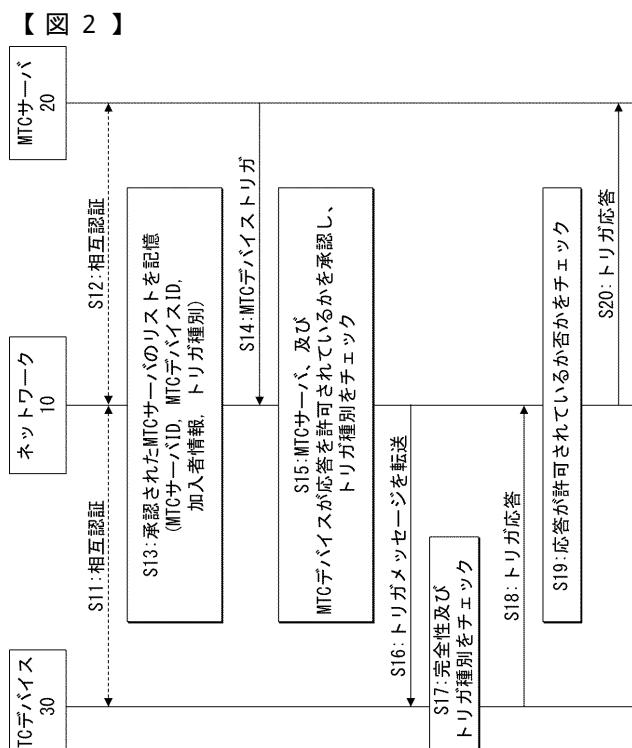
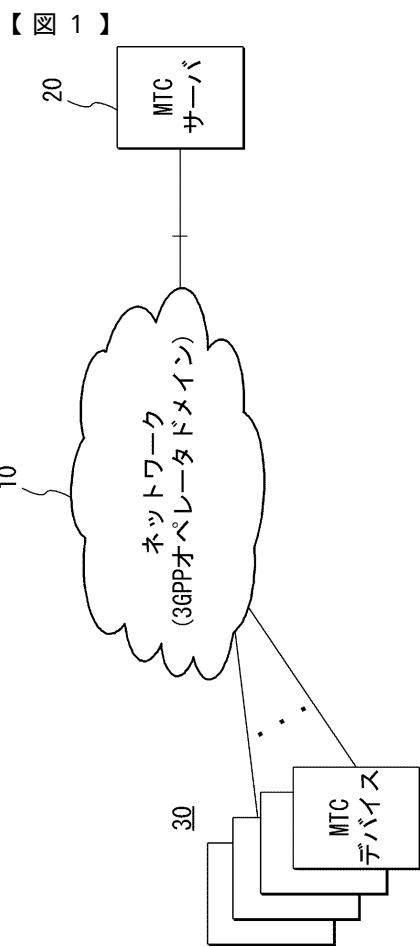
20

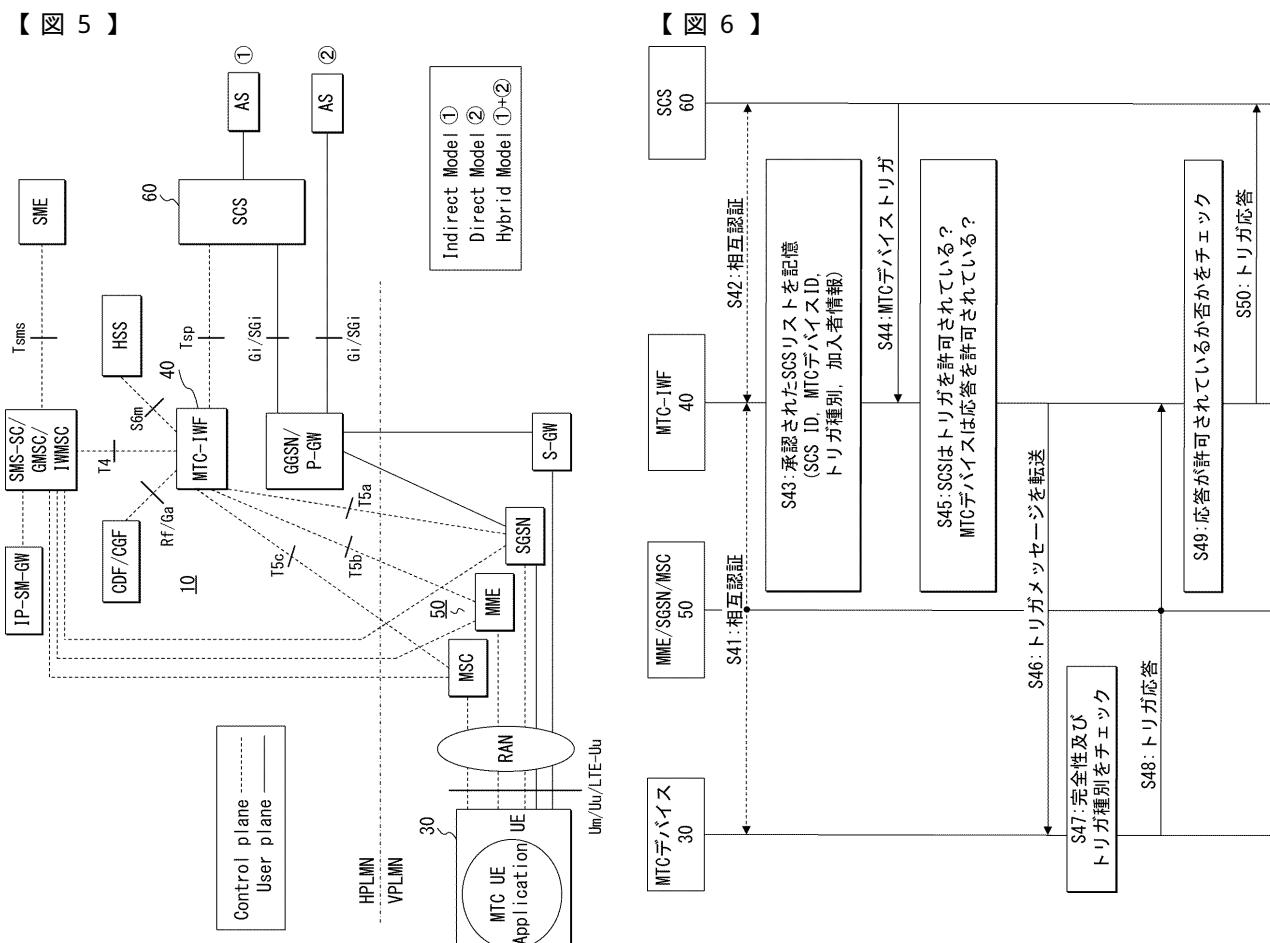
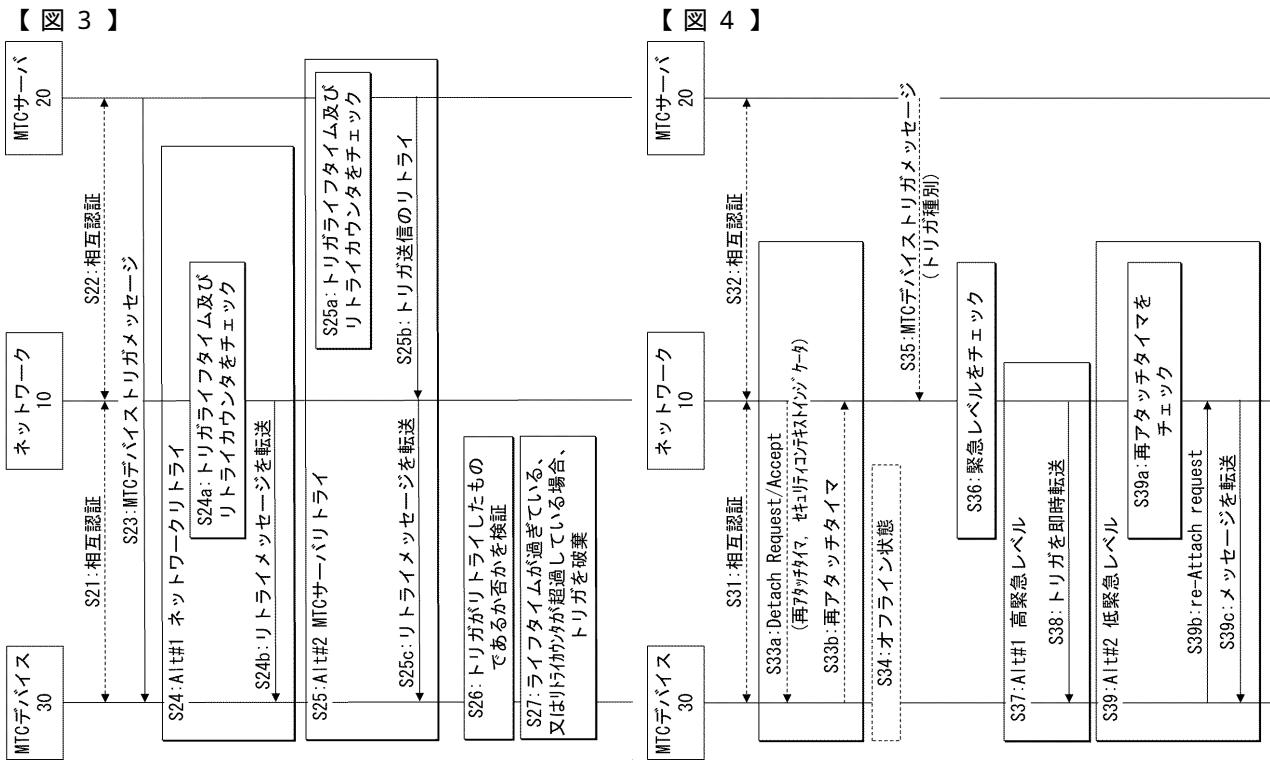
30

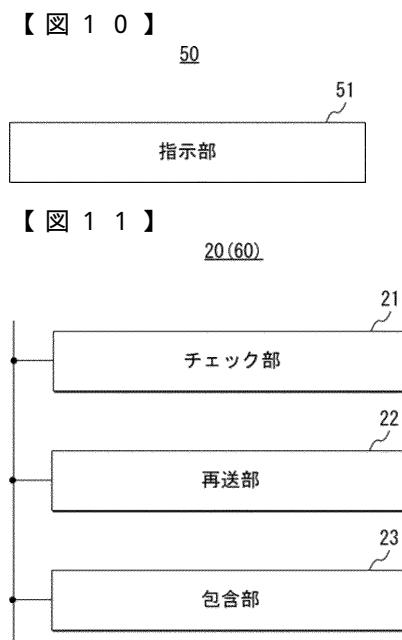
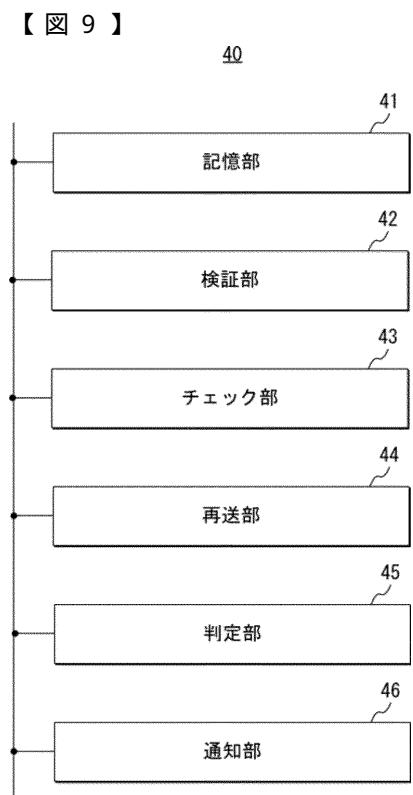
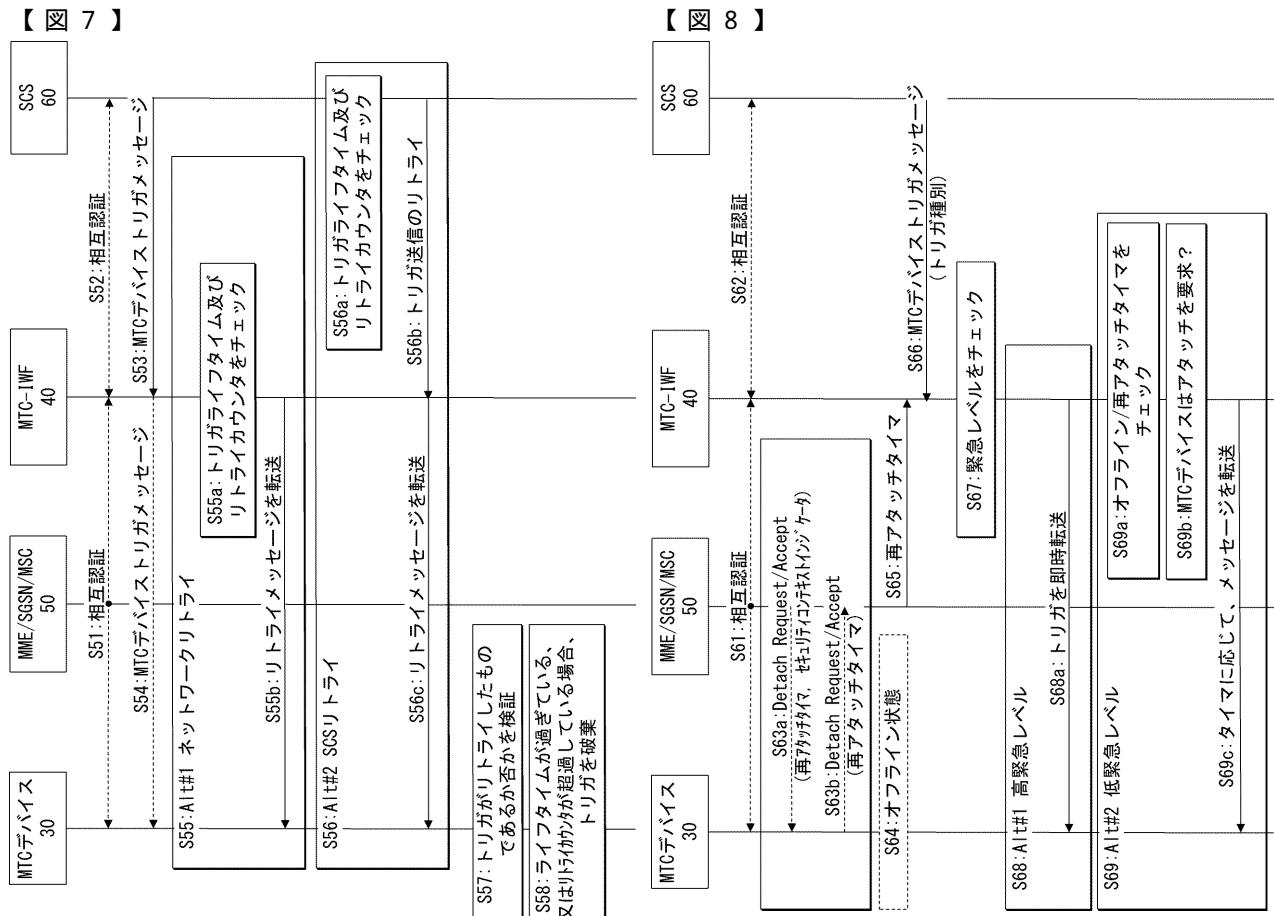
40

50

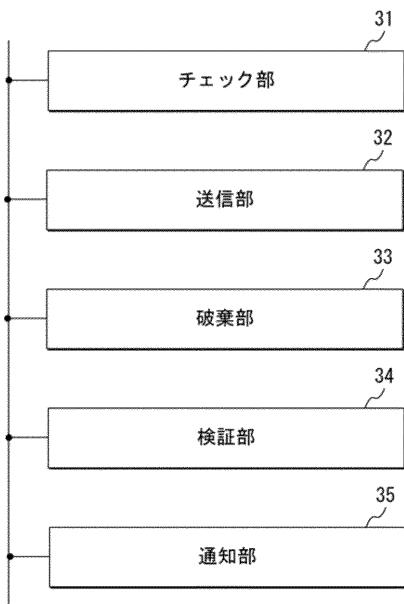
4 1 記憶部  
 4 4 再送部  
 4 5 判定部  
 5 0 M M E / S G S N / M S C  
 5 1 指示部  
 6 0 S C S







## 【図12】

30

## 【手続補正書】

【提出日】平成26年4月22日(2014.4.22)

## 【手続補正1】

【補正対象書類名】特許請求の範囲

【補正対象項目名】全文

【補正方法】変更

## 【補正の内容】

【特許請求の範囲】

## 【請求項1】

ネットワークと、

複数のMTC(M a c h i n e - T y p e - C o m m u n i c a t i o n )サーバと、MTCデバイスと、を備え、前記ネットワークは、前記MTCデバイスへトリガを送信することを承認されたMTCサーバ、及び前記MTCサーバが送信することを承認されたトリガの種別のリストを保持し、前記リストに応じて、前記MTCサーバが前記MTCデバイスへトリガを送信することを許可されているか否かと、当該トリガの送信が承認されているか否かと、を検証する、  
システム。

## 【請求項2】

請求項1において、

前記ネットワークは、前記MTCサーバが前記MTCデバイスへ前記トリガを送信する  
ことを承認されていると判定した場合、前記MTCデバイスが前記承認されたMTCサー  
バと通信することを有効にする、ことを特徴としたシステム。

## 【請求項3】

請求項 1 において、

前記ネットワークは、前記トリガの完全性をチェックする、  
ことを特徴としたシステム。

**【請求項 4】**

請求項 1 において、

前記トリガの種別は、緊急レベル、加入者情報、アグリゲーションの可用性、ブロードキャストトリガの可用性、及びグループトリガの可用性の少なくとも一つを含む、  
ことを特徴としたシステム。

**【請求項 5】**

請求項 1 において、

前記リストは、前記トリガへの応答を承認されたMTCデバイスの識別子をさらに含み

前記ネットワークは、前記リストに応じて、前記MTCデバイスが前記トリガへの応答を承認されているか否かをさらに検証する、  
ことを特徴としたシステム。

**【請求項 6】**

請求項 5 において、

前記ネットワークは、

前記MTCデバイスから、前記トリガへの応答を受信し、

前記リストに応じて、前記MTCデバイスが前記トリガへの応答を承認されているか否かを検証し、

前記MTCデバイスが前記トリガへの応答を承認されていると検証した際に、前記応答を前記MTCサーバへ転送する、

ことを特徴としたシステム。

**【請求項 7】**

請求項 6 において、

前記MTCデバイスは、

前記ネットワークにより転送された前記トリガの完全性及び種別をチェックして、前記トリガの正当性を検証し、

前記正当性が検証された場合に、前記応答を前記ネットワークへ送信する、  
ことを特徴としたシステム。

**【請求項 8】**

請求項 1 において、

前記ネットワークは、前記検証に成功した際に、前記トリガを前記MTCデバイスへ転送する、

ことを特徴としたシステム。

**【請求項 9】**

ネットワークと、複数のMTC(Machine-Type-Communication)サーバと、MTCデバイスとを含むシステムの制御方法であって、

前記ネットワークが、前記MTCデバイスへトリガを送信することを承認されたMTCサーバ、及び前記MTCサーバが送信することを承認されたトリガの種別のリストを、保持し、

前記ネットワークが、前記リストに応じて、前記MTCサーバが前記MTCデバイスへトリガを送信することを許可されているか否かと、当該トリガの送信が承認されているか否かと、を検証する、

ことを含む方法。

**【請求項 10】**

請求項 9 において、

前記ネットワークは、前記MTCサーバが前記MTCデバイスへ前記トリガを送信することを承認されていると判定した場合、前記MTCデバイスが前記承認されたMTCサー

バと通信することを有効にする、  
ことを特徴とした方法。

**【請求項 1 1】**

請求項 9において、

前記ネットワークは、前記トリガの完全性をチェックする、  
ことを特徴とした方法。

**【請求項 1 2】**

請求項 9において、

前記トリガの種別は、緊急レベル、加入者情報、アグリゲーションの可用性、ブロードキャストトリガの可用性、及びグループトリガの可用性の少なくとも一つを含む、  
ことを特徴とした方法。

**【請求項 1 3】**

請求項 9において、

前記リストは、前記トリガへの応答を承認されたMTCデバイスの識別子をさらに含み

前記ネットワークは、前記リストに応じて、前記MTCデバイスが前記トリガへの応答を承認されているか否かをさらに検証する、  
ことを特徴とした方法。

**【請求項 1 4】**

請求項 1 3において、

前記ネットワークが、前記MTCデバイスから、前記トリガへの応答を受信し、  
前記ネットワークが前記リストに応じて、前記MTCデバイスが前記トリガへの応答を承認されているか否かを検証し、

前記ネットワークが、前記MTCデバイスが前記トリガへの応答を承認されていると検証した際に、前記応答を前記MTCサーバへ転送する、  
ことをさらに含む方法。

**【請求項 1 5】**

請求項 1 4において、

前記MTCデバイスが、前記ネットワークにより転送された前記トリガの完全性及び種別をチェックして、前記トリガの正当性を検証し、

前記MTCデバイスが、前記正当性を検証した場合に、前記応答を前記ネットワークへ送信する、  
ことをさらに含む方法。

**【請求項 1 6】**

請求項 9において、

前記ネットワークは、前記検証に成功した際に、前記トリガを前記MTCデバイスへ転送する、

ことを特徴とした方法。

## 【国際調査報告】

INTERNATIONAL SEARCH REPORT				
				International application No PCT/JP2012/006925
<b>A. CLASSIFICATION OF SUBJECT MATTER</b> INV. H04W12/08 H04W12/10 H04W4/00 H04W68/00 H04L29/06 ADD.				
According to International Patent Classification (IPC) or to both national classification and IPC				
<b>B. FIELDS SEARCHED</b> Minimum documentation searched (classification system followed by classification symbols) H04W				
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched				
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) EPO-Internal, COMPENDEX, INSPEC, WPI Data				
<b>C. DOCUMENTS CONSIDERED TO BE RELEVANT</b>				
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.		
X	"3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; System Improvements for Machine-Type Communications; (Release 11)", 3GPP STANDARD; 3GPP TR 23.888, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE, vol. SA WG2, no. V1.5.0, 19 October 2011 (2011-10-19), pages 1-155, XP050554391, [retrieved on 2011-10-19] page 7, line 21 - page 8, line 17 page 12, line 13 - page 13, line 32 page 18, lines 22-23 page 25, line 9 - page 26, line 34 page 112, line 14 - page 115, line 14 -/--	1-12, 14		
<input checked="" type="checkbox"/> Further documents are listed in the continuation of Box C.		<input type="checkbox"/> See patent family annex.		
* Special categories of cited documents : "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed				
*T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family				
Date of the actual completion of the international search		Date of mailing of the international search report		
17 June 2013		24/06/2013		
Name and mailing address of the ISA/ European Patent Office, P.O. 5818 Patentlaan 2 NL-2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016		Authorized officer  Ghomrasseni, Z		

**INTERNATIONAL SEARCH REPORT**

International application No.  
PCT/JP2012/006925

**Box No. II Observations where certain claims were found unsearchable (Continuation of Item 2 of first sheet)**

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1.  Claims Nos.: because they relate to subject matter not required to be searched by this Authority, namely:
  
  
  
  
2.  Claims Nos.: because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:
  
  
  
  
3.  Claims Nos.: because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

**Box No. III Observations where unity of invention is lacking (Continuation of Item 3 of first sheet)**

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1.  As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2.  As all searchable claims could be searched without effort justifying an additional fees, this Authority did not invite payment of additional fees.
3.  As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

1-15

4.  No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

**Remark on Protest**

- The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.
- The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.
- No protest accompanied the payment of additional search fees.

## INTERNATIONAL SEARCH REPORT

International application No PCT/JP2012/006925
---

## C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	----- SIERRA WIRELESS: "Update to MTC Device Trigger Gateway solution", 3GPP DRAFT; S2-111440 UPDATE DEVICE TRIGGER GATEWAY, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE, vol. SA WG2, no. Bratislava; 20110411, 6 April 2011 (2011-04-06), XP050524397, [retrieved on 2011-04-06] page 1, paragraph 6.40 - page 5, paragraph 6.45.4 ----- 3GPP: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security aspects of Machine-Type Communications; (Release 11)", 3GPP DRAFT; S3-110839_TR33868, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE, vol. SA WG3, no. Mainz; 20110711, 15 July 2011 (2011-07-15), XP050550215, [retrieved on 2011-07-15] page 17, line 18 - page 18, line 35 ----- ZTE CORPORATION: "SIMTC - Discussion of secure MTC device triggering", 3GPP DRAFT; SIMTC - DISCUSSION OF SECURE MTC DEVICE TRIGGERING, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE, vol. SA WG3, no. Mainz; 20110711, 4 July 2011 (2011-07-04), XP050550155, [retrieved on 2011-07-04] pages 1-2 -----	1-12,14  13,15  13,15
3		

International Application No. PCT/JP2012/006925

**FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210**

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. claims: 1-12, 14

A system and an apparatus for checking an MTC server's authorization.

---

2. claims: 13, 15

A method and an apparatus for verifying the validity of an MTC trigger message.

---

3. claims: 16-35

Methods, systems and apparatuses for handling an MTC trigger delivery failure.

---

4. claims: 36-45, 47, 51

Methods, systems and apparatuses for determining the forwarding timing of an MTC trigger.

---

5. claims: 46, 50

A method and an apparatus for agreeing on a security context with an MTC device.

---

6. claims: 48, 52

A methods and an apparatus for triggering a detached MTC device.

---

---

## フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,MK,MT,NL,NO,PL,PT,RO,R,S,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CZ,DE,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,H,U,ID,IL,IN,IS,JP,KE,KG,KM,KN,KP,KR,KZ,LA,LK,LR,LS,LT,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SC,SD,SE,SG,SK,SL,SM,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC