【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成30年11月1日(2018.11.1)

【公表番号】特表2016-527736(P2016-527736A)
【公表日】平成28年9月8日(2016.9.8)
【年通号数】公開・登録公報2016-054
【出願番号】特願2016-503868(P2016-503868)
【国際特許分類】
Ｈ０４Ｌ　9/08　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６０１Ｂ
Ｈ０４Ｌ　9/00　６０１Ｅ

【誤訳訂正書】
【提出日】平成30年9月20日(2018.9.20)
【誤訳訂正１】
【訂正対象書類名】明細書
【訂正対象項目名】０００１
【訂正方法】変更
【訂正の内容】
【０００１】
本発明は、グループベースのMTC（Machine-Type-Communication）のためのセキュリティソリューションに関する。特に、本発明は、グループ鍵を導出するために、および/またはグループ鍵を管理するために、コアネットワーク内およびMTCデバイスにグループ鍵を配布する技術に関する。
【誤訳訂正２】
【訂正対象書類名】明細書
【訂正対象項目名】００１０
【訂正方法】変更
【訂正の内容】
【００１０】
上記目的を達成するために、本発明の第1の態様に係る通信システムは、コアネットワークと通信するMTC（マシンタイプ通信）デバイスのグループと、MTCデバイスの各々に安全にグループ通信を行うための第1の鍵を配布する、グループのコアネットワークへのゲートウェイを備え、前記ゲートウェイは、第1の鍵を配布するときに、ゲートウェイが、予めゲートウェイとMTCデバイスとの間で共有され、グループのメンバーとしてのMTCデバイスの各々を認証するためのゲートウェイ用に使用される第2の鍵、またはコアネットワークを介してグループと通信しSCS（サービス能力サーバ）のためのコアネットワークに進入点を提供するMTC-IWF（MTCインターワーキング機能）とMTCデバイスとの間で共有され、安全にMTC-IWFとMTCデバイスの各々との間の個々の通信を行うための一時的な鍵を導出するために使用される第3の鍵、を使用することにより第1の鍵の機密性と完全性を保護する。
【誤訳訂正３】
【訂正対象書類名】明細書
【訂正対象項目名】００１１
【訂正方法】変更
【訂正の内容】
【００１１】
さらに、本発明の第2の実施態様によれば、ゲートウェイは、コアネットワークと通信

するMTCデバイスのグループのためのコアネットワークへのゲートウェイであって、安全にグループ通信を行うための第1の鍵の機密性と完全性を保護する保護手段と、MTCデバイスの各々に保護された第1の鍵を分配する分配手段と、を備え、保護手段は、予めゲートウェイとMTCデバイスとの間で共有され、グループのメンバーとしてのMTCデバイスの各々を認証するためのゲートウェイ用に使用される第2の鍵、またはコアネットワークを介してグループと通信しSCSのためのコアネットワークに進入点を提供するMTC-IWFとMTCデバイスとの間で共有され、安全にMTC-IWFとMTCデバイスの各々との間の個々の通信を行うための一時的な鍵を導出するために使用される第3の鍵、を使用して保護を行うように構成されている。

【誤訳訂正４】
【訂正対象書類名】明細書
【訂正対象項目名】００１２
【訂正方法】変更
【訂正の内容】
【００１２】
さらに、本発明の第3実施態様に係るMTCデバイスは、コアネットワークと通信するようにグループ化されたMTCデバイスであって、MTCデバイスのグループのためのゲートウェイからコアネットワークへの安全にグループ通信を行うための、第2の鍵または第3の鍵で第1の鍵の秘密性及び完全性が保護された第1の鍵を受信する受信手段を備え、第2の鍵は、予めゲートウェイとMTCデバイスとの間で共有され、グループのメンバーとしてMTCデバイスの各々を認証するためにゲートウェイに使用され、第3の鍵は、コアネットワークを介してグループと通信しSCSのためのコアネットワークに進入点を提供するMTC-IWFとMTCデバイスとの間で共有され、安全にMTC-IWFとMTCデバイスの各々との間の個々の通信を行うための一時的な鍵を導出するために使用される。

【誤訳訂正５】
【訂正対象書類名】明細書
【訂正対象項目名】００１３
【訂正方法】変更
【訂正の内容】
【００１３】
さらに、本発明の第4の実施態様による方法は、コアネットワークと通信するMTCデバイスのグループのためのコアネットワークへのゲートウェイの動作を制御する方法であって、安全にグループ通信を行うための第1の鍵の機密性と完全性を保護し、MTCデバイスの各々に保護された第1の鍵を分配し、予めゲートウェイとMTCデバイスとの間で共有され、グループのメンバーとしてのMTCデバイスの各々を認証するためのゲートウェイ用に使用される第2の鍵、またはコアネットワークを介してグループと通信しSCSのためのコアネットワークに進入点を提供するMTC-IWFとMTCデバイスとの間で共有され、安全にMTC-IWFとMTCデバイスの各々との間の個々の通信を行うための一時的な鍵を導出するために使用される第3の鍵、を使用して、保護を行うように構成されている。

【誤訳訂正６】
【訂正対象書類名】明細書
【訂正対象項目名】００１４
【訂正方法】変更
【訂正の内容】
【００１４】
また、本発明の第5の実施態様による方法は、コアネットワークと通信するようにグループ化されたMTCデバイスの動作を制御するための方法であって、MTCデバイスのグループのためのゲートウェイからコアネットワークへの安全にグループ通信を行うための、第2の鍵または第3の鍵で第1の鍵の秘密性及び完全性が保護された第1の鍵を受信し、第2の鍵は、予めゲートウェイとMTCデバイスとの間で共有され、グループのメンバーとしてMTCデ

バイスの各々を認証するためにゲートウェイに使用され、第3の鍵は、コアネットワークを介してグループと通信しSCSのためのコアネットワークに進入点を提供するMTC-IWFとMTCデバイスとの間で共有され、安全にMTC-IWFとMTCデバイスの各々との間の個々の通信を行うための一時的な鍵を導出するために使用される。

【誤訳訂正７】
【訂正対象書類名】明細書
【訂正対象項目名】００１８
【訂正方法】変更
【訂正の内容】
【００１８】
この例示的な実施形態では、コアネットワークにおけるグループ鍵導出の詳細が提案され、適切なネットワークノードとUE、鍵管理方法と、グループ鍵への鍵配布は、通信を保護するために使用される。鍵導出パラメータは、HSS（ホームサブスクリプションサーバ）からMTC-IWFに、またはMTC-IWFからHSSに、送信することができる。導出アルゴリズムは、ネットワークノードで利用可能である。

【誤訳訂正８】
【訂正対象書類名】明細書
【訂正対象項目名】００２５
【訂正方法】変更
【訂正の内容】
【００２５】
グループGW20は、グループ鍵を取得することができ、2つの選択肢がある。選択肢の一つは、グループGW20自体がグループ鍵を導出する場合である。グループ鍵を導出する方法は後述する。選択肢のうちの別の1つは、グループGW20が、他のネットワークノードからグループ鍵を受信する場合である。この例示的な実施形態では、グループGW20は、MTC-IWF50で構成されているかどうかを考慮する。

【誤訳訂正９】
【訂正対象書類名】明細書
【訂正対象項目名】００２６
【訂正方法】変更
【訂正の内容】
【００２６】
（1）MTC-IWF50は、グループGW20ではなく、グループ鍵を共有しないケース
図2に示すように、この場合には、HSS40は、グループ鍵を導出し、サブスクリプション情報応答メッセージでグループIDとともにグループ鍵MTC-IWF50に送信する（ステップS1a～S1c）。

【誤訳訂正１０】
【訂正対象書類名】明細書
【訂正対象項目名】００２７
【訂正方法】変更
【訂正の内容】
【００２７】
また、MTC-IWF50は、サブスクリプション情報応答メッセージで、HSS40からグループIDおよび必要に応じて鍵導出パラメータを受信した場合、グループ鍵を導出する（ステップS2a～S2C）。

【誤訳訂正１１】
【訂正対象書類名】明細書
【訂正対象項目名】００２８
【訂正方法】変更
【訂正の内容】

【００２８】
導出されるグループ鍵は、グループIDとグループ鍵のKSI（鍵セット識別子）と一緒に、MME30を介してグループGW20に、送信される（ステップS3）。
【誤訳訂正１２】
【訂正対象書類名】明細書
【訂正対象項目名】００３４
【訂正方法】変更
【訂正の内容】
【００３４】
もう一つの方法は、ルート鍵K_iwfを使用することである。ルート鍵K_iwfは、MTC-IWF50とMTC　UE10_1～10_nとの間で共有され、MTC-IWF50とMTC　UE10_1～10_nの各々との間の個々の通信を安全に行うための一時的な鍵を導出するために使用される。
【誤訳訂正１３】
【訂正対象書類名】明細書
【訂正対象項目名】００３８
【訂正方法】変更
【訂正の内容】
【００３８】
（2）MTC-IWF50が、グループGW20であるケース
図3に示すように、この場合、HSS40または（グループGWとなる）MTC-IWF50Aは、図2と同様の方法でグループ鍵を導出する（ステップS11a～S12c）。
【誤訳訂正１４】
【訂正対象書類名】明細書
【訂正対象項目名】００４０
【訂正方法】変更
【訂正の内容】
【００４０】
（3）MTC-IWF50が、グループGW20ではなく、グループ鍵を共有する必要がないケース
図4に示すように、この場合には、HSS40は、グループ鍵を導出し、例えば、認証データ応答メッセージにおけるUEの認証手順中にMME30に送信する（ステップS21及びS22）。認証データ応答メッセージ中にグループ鍵を含む場合には、通信プロトコルへの影響を低減することができる。認証データ応答メッセージは、典型的なMMEとHSSとの間で転送される既存のメッセージである。
【誤訳訂正１５】
【訂正対象書類名】明細書
【訂正対象項目名】００４４
【訂正方法】変更
【訂正の内容】
【００４４】
2.鍵導出
グループ鍵を導出するために、3GPP　TS　33.401で定義されたKDF（鍵導出機能）を再利用することができる。
【誤訳訂正１６】
【訂正対象書類名】明細書
【訂正対象項目名】００４６
【訂正方法】変更
【訂正の内容】
【００４６】
他のパラメータは、内部のグループID、グループゲートウェイID、鍵導出アルゴリズム識別子、カウンタとすることができる。

【誤訳訂正１７】
【訂正対象書類名】明細書
【訂正対象項目名】００４７
【訂正方法】変更
【訂正の内容】
【００４７】
新しいグループ鍵が導出されたときに有効期間も生成することができる。
【誤訳訂正１８】
【訂正対象書類名】明細書
【訂正対象項目名】００４８
【訂正方法】変更
【訂正の内容】
【００４８】
鍵導出パラメータは、HSS40からMTC-IWF50（または50A）に、またはMTC-IWF50（または50A）からHSS40に、送信することができる。導出アルゴリズムは、グループ鍵を導出するネットワークノードで設定されている。
【誤訳訂正１９】
【訂正対象書類名】明細書
【訂正対象項目名】００４９
【訂正方法】変更
【訂正の内容】
【００４９】
3.鍵管理
グループ鍵は、
グループ鍵の有効期間が切れている、
グループメンバーがグループから削除される、
導出パラメータ（例えば、ルート鍵K_iwf）を更新した、または
非アクティブ状態に遷移する前に、新しいグループ鍵を導出し、保存する、
ときに更新することができる。
【誤訳訂正２０】
【訂正対象書類名】明細書
【訂正対象項目名】００５２
【訂正方法】変更
【訂正の内容】
【００５２】
また、MTC-IWF50は、グループ鍵を更新し、必要に応じてHSS40から鍵導出パラメータを取得する（ステップS32a及びS32B）。
【誤訳訂正２１】
【訂正対象書類名】明細書
【訂正対象項目名】００６２
【訂正方法】変更
【訂正の内容】
【００６２】
図9で示したように、グループGW20は、少なくとも保護ユニット21と分配ユニット22を含む。保護ユニット21は、鍵KgrまたはK_iwfを使用して、グループ鍵を保護する。分配ユニット22は、MTC端末10に保護されたグループ鍵を配布する。HSS40または（グループGW20ではない）MTC-IWF50がグループ鍵を導出する場合には、グループGW20は、HSS40またはMTC-IWF50からグループ鍵を受信する受信ユニット23を備える。受信ユニット23はまた、更新されたグループ鍵を受信する。グループGW20は、受信ユニット23の代わりに、鍵導出パラメータとして、鍵Kgr、鍵K_iwf、Kasmeまたは乱数を使用してグループ鍵を導出する導

出ユニット24を含むことができる。導出ユニット24は、グループ鍵を更新する。いずれの場合においても、保護ユニット21は、鍵KgrまたはK_iwfを使用して、更新されたグループ鍵を保護し、分配ユニット22は、保護され更新されたグループ鍵を再分配する。これらユニット21～24は、相互にバスなどを介して互いに接続されていることに留意されたい。これらユニット21～24は、コアネットワーク内の他のノードと通信を行う、例えば、通信器、およびそのようなこれらの通信器を制御するCPU等の制御装置によって構成することができる。

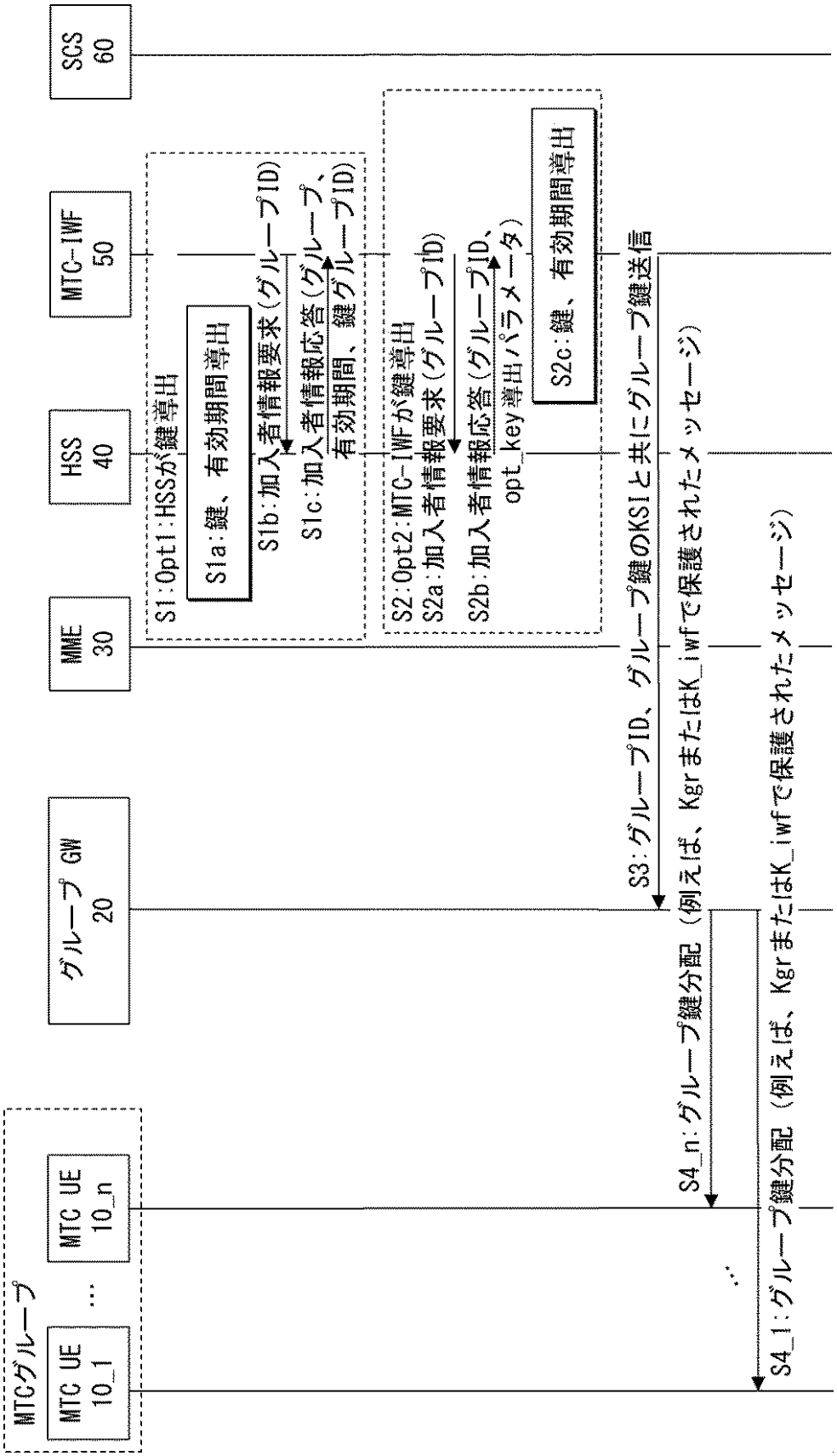
【誤訳訂正２２】
【訂正対象書類名】明細書
【訂正対象項目名】００６３
【訂正方法】変更
【訂正の内容】
【００６３】
図10で示すように、HSS40は、HSSの典型的な要素に加えて、導出ユニット42と、送信ユニット42を含むことができる。導出ユニット42は、鍵導出パラメータとして、鍵Kgr、鍵K_iwf、Kasmeまたは乱数を使用して、グループ鍵を導出する。送信ユニット42は、グループGW20および/またはMTC-IWF50にグループ鍵を送信する。導出ユニット42は、グループ鍵を更新することができ、送信ユニット42は、グループGW20および/またはMTC-IWF50に更新されたグループ鍵を送信する。これらのユニット41および42は、相互にバスなどを介して互いに接続されていることに留意されたい。これらのユニット41及び42は、例えば、他のコアネットワーク内のノード、及びコントローラと通信を行う通信器、及びこれらの通信器を制御するCPU等で構成することができる。

【誤訳訂正２３】
【訂正対象書類名】明細書
【訂正対象項目名】００６４
【訂正方法】変更
【訂正の内容】
【００６４】
図11で示したように、MTC-IWF50（50A）は、典型的なMTC-IWFの要素に加えて、導出ユニット51、送信ユニット52を含むことができる。導出ユニット51は、鍵導出パラメータとして、鍵Kgr、鍵K_iwf、Kasmeまたは乱数を使用して、グループ鍵を導出する。送信ユニット52は、グループGW20またはMTC　UE10にグループ鍵を送信する。導出ユニット51は、グループ鍵を更新することができ、送信ユニット52は、グループGW20またはMTC　UE10に更新されたグループ鍵を送信することができる。これらのユニット51および52は、相互にバスなどを介して互いに接続されていることに留意されたい。これらのユニット51および52は、コアネットワーク内の他のノードと通信を行う、例えば、通信器、およびそのようなこれらの通信器を制御するCPU等の制御装置によって構成することができる。

【誤訳訂正２４】
【訂正対象書類名】明細書
【訂正対象項目名】００６７
【訂正方法】変更
【訂正の内容】
【００６７】
10、10_1-10_n　MTC　UE
11、23　受信ユニット
20　グループGW
21　保護ユニット
22　分配ユニット
24、41、51　導出ユニット
30　MME

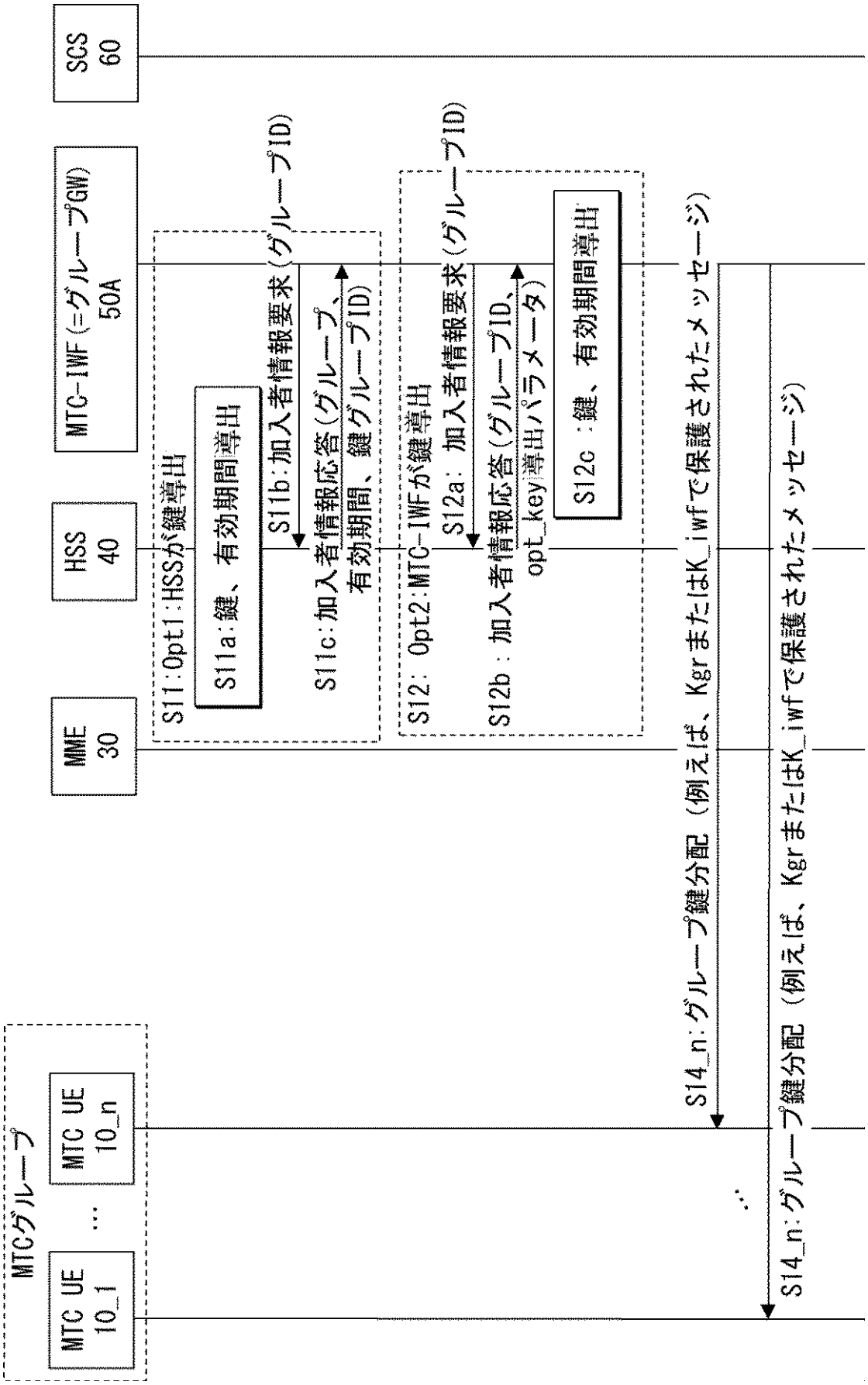
40　HSS
42、52　送信ユニット
50、50A　MTC-IWF
60　SCS
【誤訳訂正２５】
【訂正対象書類名】図面
【訂正対象項目名】図２
【訂正方法】変更
【訂正の内容】

【図２】



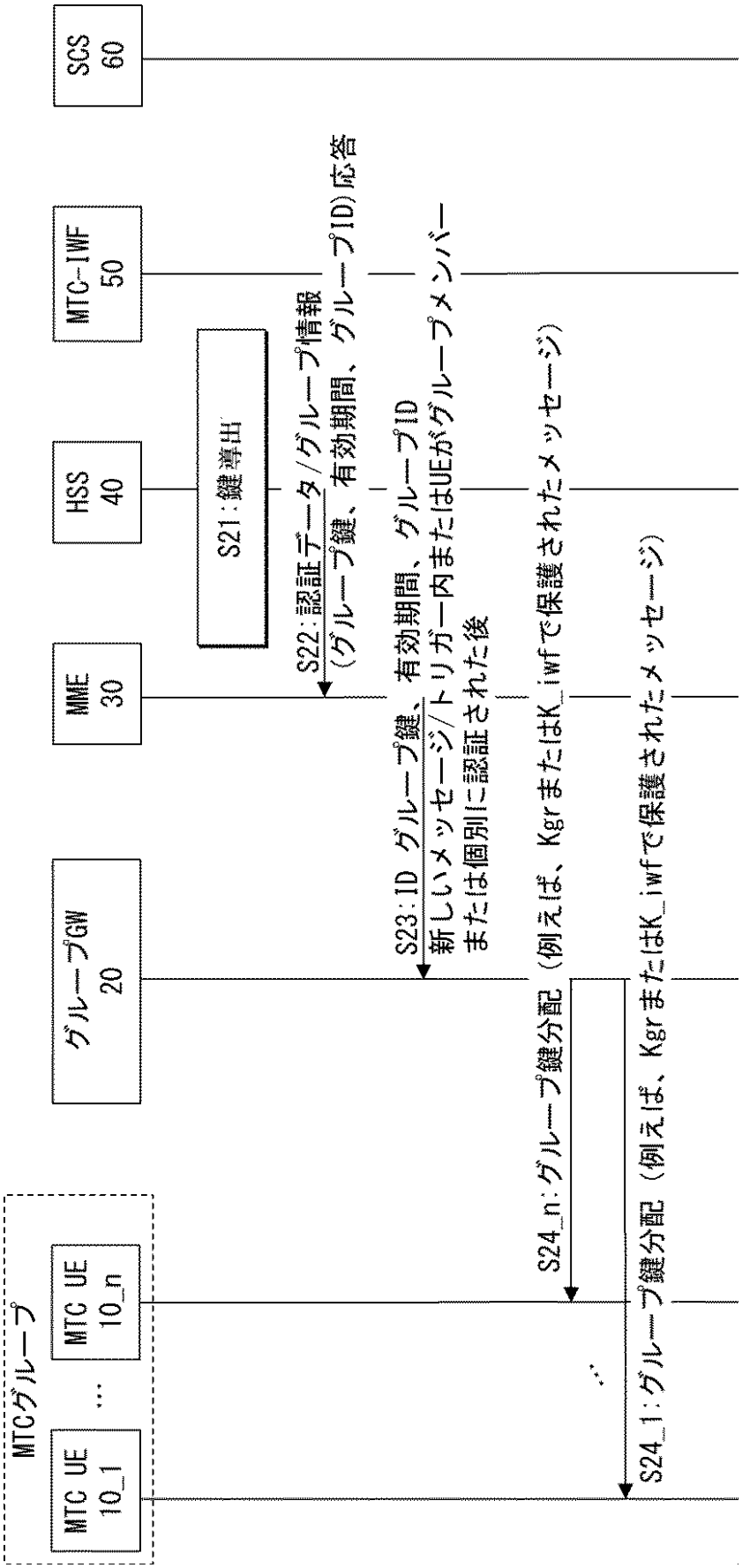
【誤訳訂正２６】
【訂正対象書類名】図面
【訂正対象項目名】図３
【訂正方法】変更
【訂正の内容】

【図３】



【誤訳訂正２７】
【訂正対象書類名】図面
【訂正対象項目名】図４

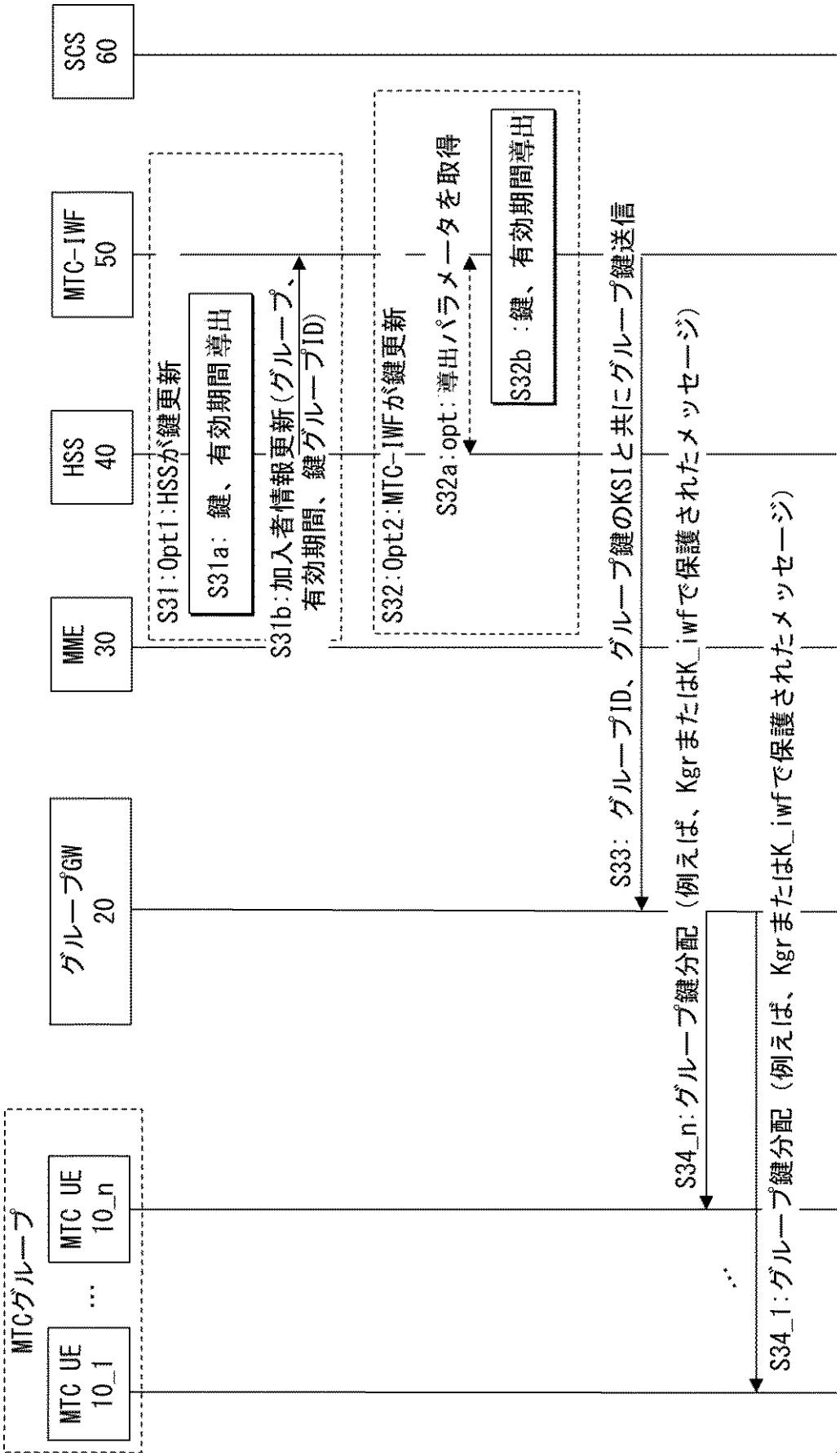
【訂正方法】変更
【訂正の内容】
【図４】



【誤訳訂正２８】

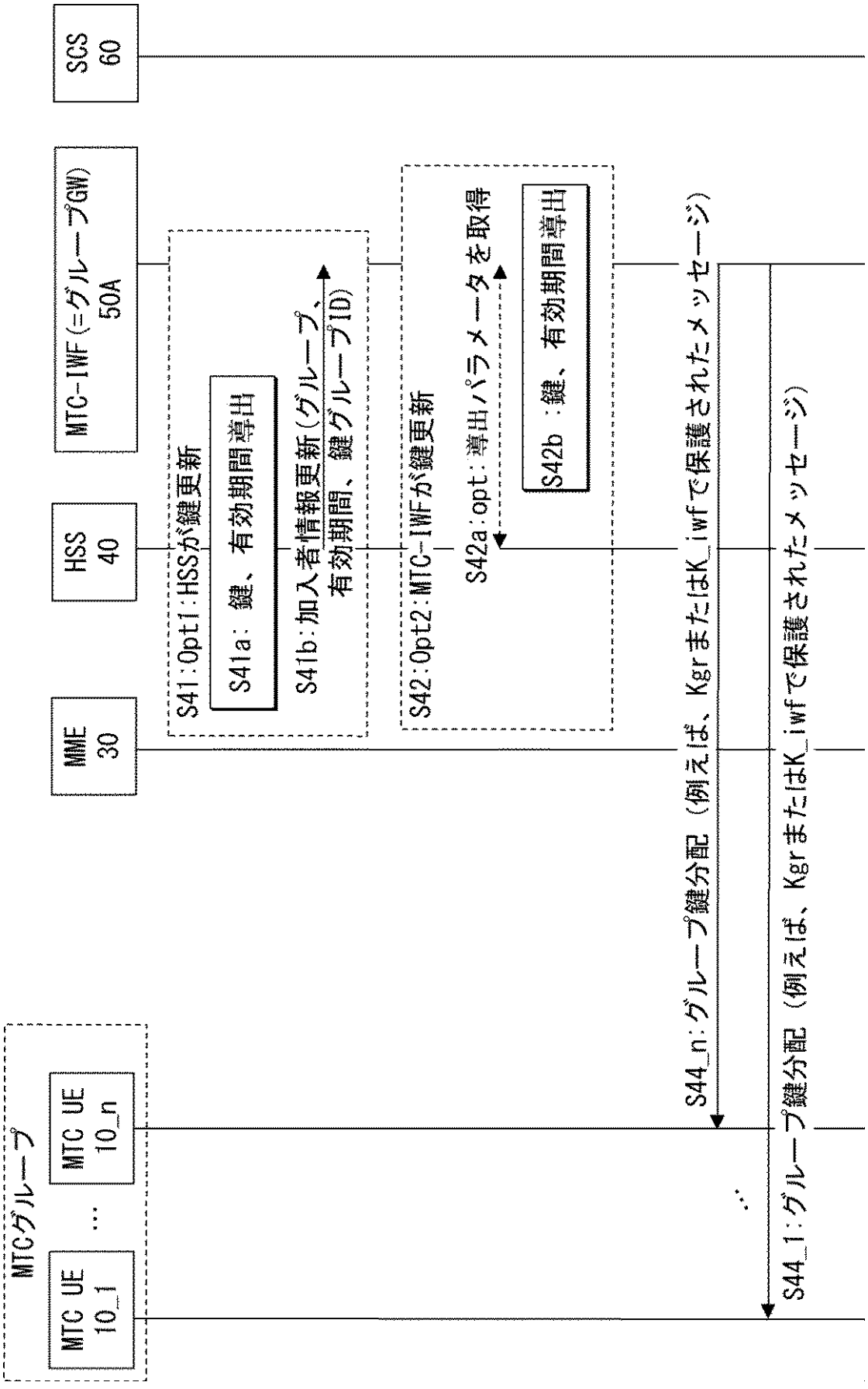
【訂正対象書類名】図面
【訂正対象項目名】図５
【訂正方法】変更
【訂正の内容】

【図５】



【誤訳訂正２９】
【訂正対象書類名】図面
【訂正対象項目名】図６

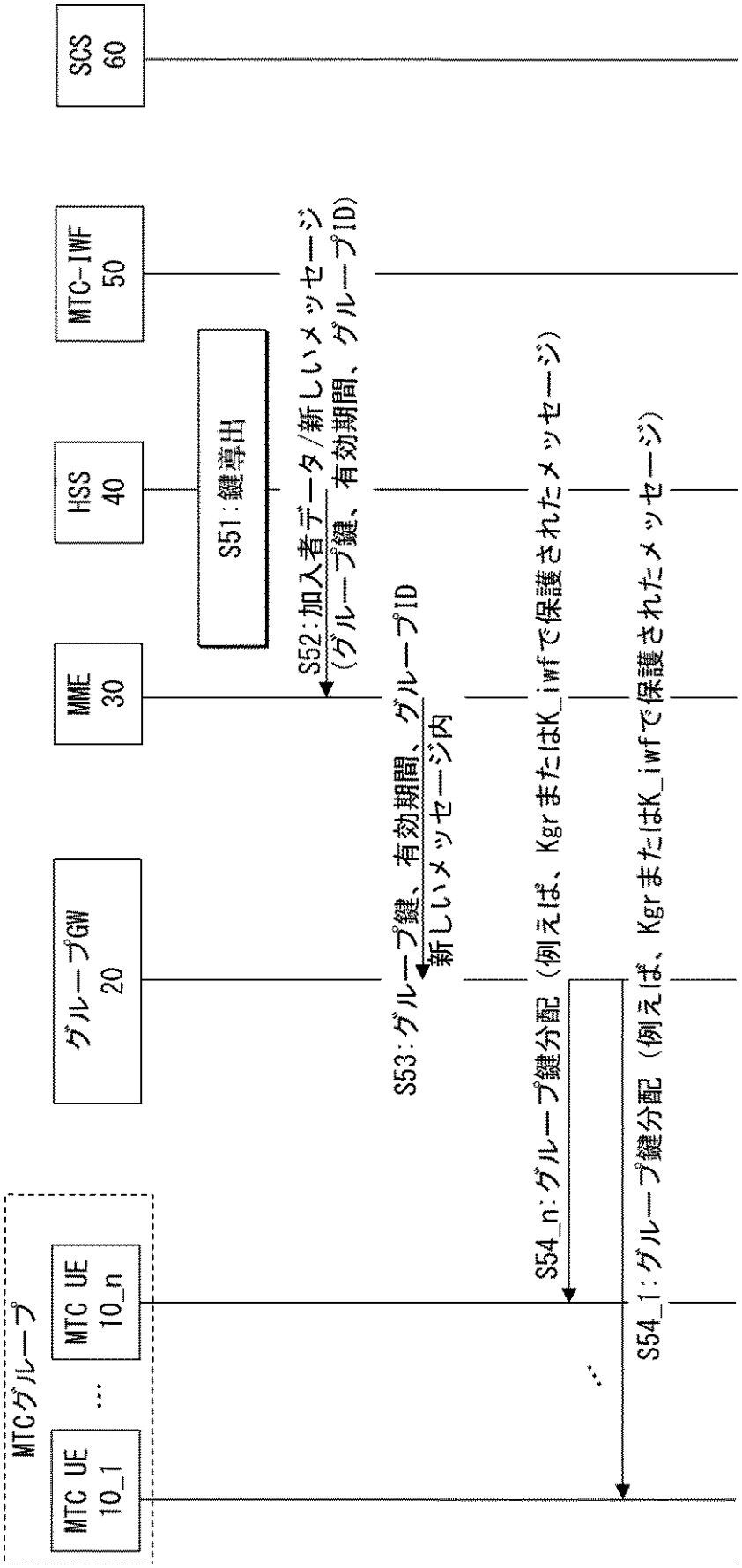
【訂正方法】変更
【訂正の内容】
【図６】



【誤訳訂正３０】

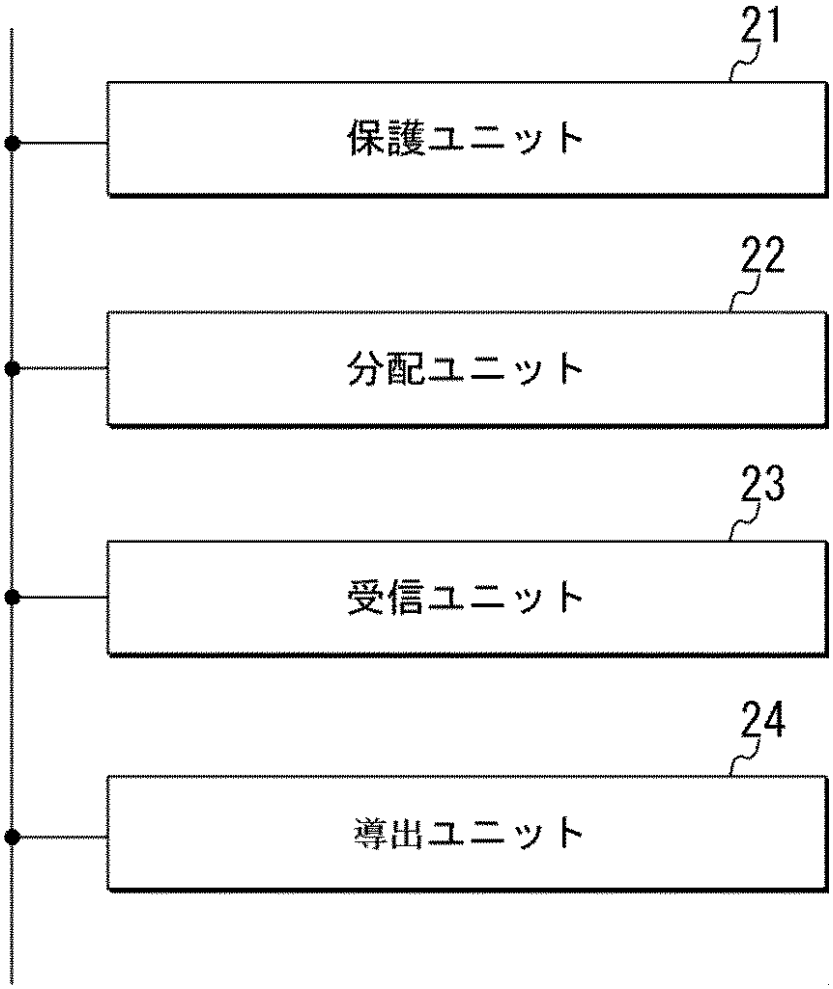
【訂正対象書類名】図面
【訂正対象項目名】図７
【訂正方法】変更
【訂正の内容】

【図７】



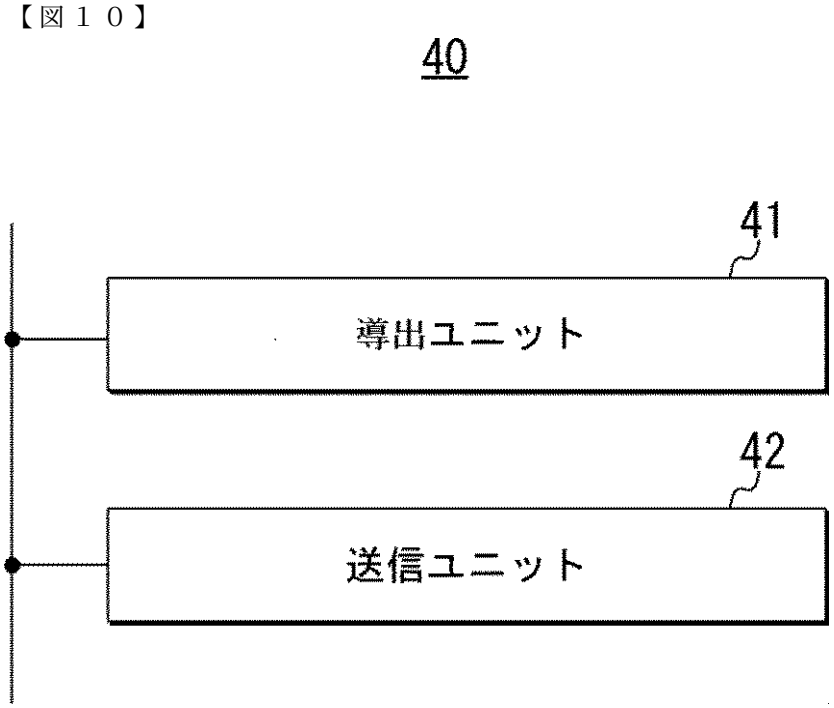
【誤訳訂正３１】
【訂正対象書類名】図面
【訂正対象項目名】図９

【訂正方法】変更
【訂正の内容】
【図９】



【誤訳訂正３２】
【訂正対象書類名】図面
【訂正対象項目名】図１０
【訂正方法】変更
【訂正の内容】

【図１０】



【誤訳訂正３３】
【訂正対象書類名】図面
【訂正対象項目名】図１１
【訂正方法】変更
【訂正の内容】
【図１１】