(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7549909号
(P7549909)

(45)発行日　令和6年9月12日(2024.9.12)

(24)登録日　令和6年9月4日(2024.9.4)

(51)国際特許分類

Ｇ０６Ｆ　21/60　(2013.01)	Ｇ０６Ｆ	21/60	３２０
Ｈ０４Ｌ　9/14　(2006.01)	Ｈ０４Ｌ	9/14	
Ｇ０６Ｆ　21/62　(2013.01)	Ｇ０６Ｆ	21/62	３０９

ＦＩ

請求項の数　8　（全24頁）

(21)出願番号　特願2022-542563(P2022-542563)
(86)(22)出願日　令和2年8月14日(2020.8.14)
(86)国際出願番号　PCT/JP2020/030888
(87)国際公開番号　WO2022/034684
(87)国際公開日　令和4年2月17日(2022.2.17)
審査請求日　令和4年10月27日(2022.10.27)

(73)特許権者　521205593
株式会社アイルソフト
愛知県名古屋市千種区末盛通一丁目１８番地１
(74)代理人　110001911
弁理士法人アルファ国際特許事務所
(72)発明者　市川 満之
愛知県名古屋市千種区末盛通一丁目１８番地１　株式会社アイルソフト内
審査官　行田 悦資

最終頁に続く

(54)【発明の名称】　端末装置、コンピュータプログラム

(57)【特許請求の範囲】

【請求項１】

外部装置との間で、ブローカを介して、パブリッシュ・サブスクライブ・メッセージ・モデルに基づく通信を行う端末装置であって、

外部データを取得する取得部と、

前記外部データの少なくとも一部を暗号化して、暗号文を含む暗号メッセージデータを生成する暗号化処理部と、

平文のトピック指定データと、前記暗号メッセージデータと、を含む暗号化パブリッシュメッセージを、前記ブローカに配信するデータ配信部と、

暗号化条件が満たされるか否かを判断する暗号化判断部と、

を備え、

前記暗号化判断部によって前記暗号化条件が満たされると判断された場合、前記暗号化処理部は、前記暗号メッセージデータを生成し、前記データ配信部は、前記暗号化パブリッシュメッセージを前記ブローカに配信し、

前記暗号化判断部によって前記暗号化条件が満たされないと判断された場合、前記データ配信部は、平文のトピック指定データと、平文のメッセージデータと、を含む非暗号化パブリッシュメッセージを前記ブローカに配信し、

さらに、前記暗号化パブリッシュメッセージと前記非暗号化パブリッシュメッセージとのそれぞれにおける暗号文の配置パターンを識別するためのパターン識別データを、前記トピック指定データに含めるトピック処理部を備える、端末装置。

【請求項２】
請求項１に記載の端末装置であって、
前記外部データは、第１の外部データと第２の外部データとを含んでおり、
前記暗号化処理部は、前記第１の外部データを平文のままとし、前記第２の外部データを暗号化して、平文と暗号文とを含む前記暗号メッセージデータを生成可能である、
端末装置。
【請求項３】
請求項１または請求項２に記載の端末装置であって、
前記外部データは、第１の外部データと第２の外部データとを含んでおり、
前記暗号化処理部は、前記第１の外部データと前記第２の外部データとを、暗号ルールおよび暗号鍵の少なくとも一方が互いに異なる方法により暗号化して、前記暗号メッセージデータを生成可能である、
端末装置。
【請求項４】
外部装置との間で、ブローカを介して、パブリッシュ・サブスクライブ・メッセージ・モデルに基づく通信を行う端末装置であって、
外部データを取得する取得部と、
前記外部データの少なくとも一部を暗号化して、暗号文を含む暗号メッセージデータを生成する暗号化処理部と、
平文のトピック指定データと、前記暗号メッセージデータと、を含む暗号化パブリッシュメッセージを、前記ブローカに配信するデータ配信部と、
前記暗号メッセージデータを復号化するための復号化ルールと暗号鍵との少なくとも一方を含む暗号ルールデータを生成する暗号ルール生成部と、
を備え、
前記データ配信部は、前記トピック指定データと前記暗号ルールデータとを含む暗号ルールパブリッシュメッセージを前記ブローカに配信し、
前記暗号ルールデータは、前記復号化ルールと、前記暗号鍵と、前記復号化ルールと前記暗号鍵とを区切る区切り文字であって、複数の文字列である区切り文字を含む、
端末装置。
【請求項５】
請求項４に記載の端末装置であって、
さらに、暗号変更条件が満たされるか否かを判断する暗号変更判断部を備え、
前記暗号変更判断部によって前記暗号変更条件が満たされると判断された場合、暗号ルール生成部は、前記復号化ルールと前記暗号鍵と前記区切り文字との少なくとも１つを変更した新たな暗号ルールデータを生成する、
端末装置。
【請求項６】
請求項５に記載の端末装置であって、
前記暗号変更判断部は、第１の暗号変更条件と、前記第１の暗号変更条件よりも満たす頻度が高い第２の暗号変更条件とのそれぞれが満たされるか否かを判断し、
暗号ルール生成部は、前記暗号変更判断部によって前記第１の暗号変更条件が満たされると判断された場合、前記復号化ルールと前記暗号鍵との少なくとも１つを変更した新たな第１の暗号ルールデータを生成し、前記暗号変更判断部によって前記第２の暗号変更条件が満たされると判断された場合、前記区切り文字を変更した新たな第２の暗号ルールデータを生成する、
端末装置。
【請求項７】
外部装置との間で、ブローカを介して、パブリッシュ・サブスクライブ・メッセージ・モデルに基づく通信を行う端末装置が有するコンピュータに、
外部データを取得する取得処理と、

前記外部データの少なくとも一部を暗号化して、暗号文を含む暗号メッセージデータを生成する暗号化処理と、
平文のトピック指定データと、前記暗号メッセージデータと、を含む暗号化パブリッシュメッセージを生成するデータ生成処理と、
前記データ生成処理によって生成された前記暗号化パブリッシュメッセージを、前記ブローカに配信するデータ配信処理と、
暗号化条件が満たされるか否かを判断する暗号化判断処理と、を実行させ、
前記暗号化判断処理で前記暗号化条件が満たされると判断された場合、前記暗号化処理では、前記暗号メッセージデータを生成し、前記データ配信処理では、前記暗号化パブリッシュメッセージを前記ブローカに配信し、
前記暗号化判断処理で前記暗号化条件が満たされないと判断された場合、前記データ配信処理では、平文のトピック指定データと、平文のメッセージデータと、を含む非暗号化パブリッシュメッセージを前記ブローカに配信し、
前記コンピュータに、さらに、前記暗号化パブリッシュメッセージと前記非暗号化パブリッシュメッセージとのそれぞれにおける暗号文の配置パターンを識別するためのパターン識別データを、前記トピック指定データに含めるトピック処理を実行させる、
コンピュータプログラム。
【請求項８】
外部装置との間で、ブローカを介して、パブリッシュ・サブスクライブ・メッセージ・モデルに基づく通信を行う端末装置が有するコンピュータに、
外部データを取得する取得処理と、
前記外部データの少なくとも一部を暗号化して、暗号文を含む暗号メッセージデータを生成する暗号化処理と、
平文のトピック指定データと、前記暗号メッセージデータと、を含む暗号化パブリッシュメッセージを、前記ブローカに配信するデータ配信処理と、
前記暗号メッセージデータを復号化するための復号化ルールと暗号鍵との少なくとも一方を含む暗号ルールデータを生成する暗号ルール生成処理と、
を実行させ、
前記データ配信処理では、前記トピック指定データと前記暗号ルールデータとを含む暗号ルールパブリッシュメッセージを前記ブローカに配信し、
前記暗号ルールデータは、前記復号化ルールと、前記暗号鍵と、前記復号化ルールと前記暗号鍵とを区切る区切り文字であって、複数の文字列である区切り文字を含む、
コンピュータプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本明細書に開示される技術は、パブリッシュ・サブスクライブ・メッセージ・モデルに基づく通信技術に関する。
【背景技術】
【０００２】
端末装置間で通信する方法として、パブリッシュ・サブスクライブ（Ｐｕｂｌｉｓｈ－Ｓｕｂｓｃｒｉｂｅ）・メッセージ・モデル（以下、「パブ・サブ・モデル」という）が知られている（例えば特許文献１参照）。パブ・サブ・モデルでは、パブリッシャとして機能する端末装置（以下、単に「パブリッシャ」という）がトピック指定データとメッセージデータとを含むパブリッシュメッセージを生成し、ブローカに送信する。トピック指定データは、ブローカにおいて管理されるトピックを指定するための情報である。ブローカは、受信したパブリッシュメッセージに含まれるメッセージデータを、そのパブリッシュメッセージに含まれるトピック指定データにより指定されたトピックに登録する。ブローカは、トピックに登録されたメッセージデータを、そのトピックに予め申し込んでいたサブスクライバとして機能する端末装置（以下、「サブスクライバ」という）に送信する

。これにより、サブスクライバは、パブリッシャが配信するメッセージデータのうち、予め申し込んでいたトピックに対応するものを購読することができる。
【先行技術文献】
【特許文献】
【０００３】
【文献】特開２０１８－１３９６０号公報
【発明の概要】
【発明が解決しようとする課題】
【０００４】
ところで、パブ・サブ・モデルにおいて、パブリッシャとサブスクライバとの間でメッセージデータの機密性を確保したい場合がある。ここで、メッセージデータの機密性を確保する方法として、例えば、パブリッシャがパブリッシュメッセージ全体を公知の暗号化方式（例えばＴＬＳ（Ｔｒａｎｓｐｏｒｔ Ｌａｙｅｒ Ｓｅｃｕｒｉｔｙ）による標準の暗号化方式）によって暗号化してブローカに送信する方法が考えられる。しかし、この方法では、ブローカは、トピック指定データを取得するため、暗号化されたパブリッシュメッセージを復号化する必要がある。復号化されると、平文のトピック指定データだけでなく、平文のメッセージデータもブローカに記憶される。このため、この平文のメッセージデータが、例えばブローカにアクセス可能な外部装置から取得可能となり、メッセージデータの機密性を確保できないという問題が生じる。
【０００５】
本明細書では、上述した課題を解決することが可能な技術を開示する。
【課題を解決するための手段】
【０００６】
本明細書に開示される技術は、例えば、以下の形態として実現することが可能である。
【０００７】
（１）本明細書に開示される端末装置は、外部装置との間で、ブローカを介して、パブリッシュ・サブスクライブ・メッセージ・モデルに基づく通信を行う端末装置であって、外部データを取得する取得部と、前記外部データの少なくとも一部を暗号化して、暗号文を含む暗号メッセージデータを生成する暗号化処理部と、平文のトピック指定データと、前記暗号メッセージデータと、を含む暗号化パブリッシュメッセージを、前記ブローカに配信するデータ配信部と、を備える。本端末装置は、平文のトピック指定データと、外部データの少なくとも一部を暗号化した暗号メッセージデータとを含む暗号化パブリッシュメッセージを、ブローカに配信することができる。このため、ブローカでは、暗号メッセージデータの復号化を要することなく、その暗号メッセージデータが指定されたトピックに登録される。これにより、本端末装置によれば、暗号メッセージデータの機密性を確保しつつ外部装置に配信することが可能である。
【０００８】
（２）上記端末装置において、前記外部データは、第１の外部データと第２の外部データとを含んでおり、前記暗号化処理部は、前記第１の外部データを平文のままとし、前記第２の外部データを暗号化して、平文と暗号文とを含む前記暗号メッセージデータを生成可能である構成としてもよい。本端末装置によれば、例えば、公開性を重視した平文の第１の外部データと、機密性を重視した暗号文の第２の外部データとを、暗号化パブリッシュメッセージとしてまとめて外部装置に配信可能である。
【０００９】
（３）上記端末装置において、前記外部データは、第１の外部データと第２の外部データとを含んでおり、前記暗号化処理部は、前記第１の外部データと前記第２の外部データとを、暗号ルールおよび暗号鍵の少なくとも一方が互いに異なる方法により暗号化して、前記暗号メッセージデータを生成可能である構成としてもよい。本端末装置によれば、互いに異なる暗号方法により暗号化された複数の外部データを、暗号化パブリッシュメッセージとしてまとめて外部装置に配信可能である。

【００１０】
（４）上記端末装置において、さらに、暗号化条件が満たされるか否かを判断する暗号化判断部を備え、前記暗号化判断部によって前記暗号化条件が満たされると判断された場合、前記暗号化処理部は、前記暗号メッセージデータを生成し、前記データ配信部は、前記暗号化パブリッシュメッセージを前記ブローカに配信し、前記暗号化判断部によって前記暗号化条件が満たされないと判断された場合、前記データ配信部は、平文のトピック指定データと、平文のメッセージデータと、を含む非暗号化パブリッシュメッセージを前記ブローカに配信する構成としてもよい。本端末装置では、所定の暗号化条件が満たされるか否かに基づき、機密性を重視する暗号化パブリッシュメッセージをブローカに配信する機密配信形態と、公開性を重視する非暗号化パブリッシュメッセージをブローカに配信する公開配信形態とを使い分けることができる。これにより、本端末装置によれば、メッセージデータの機密性と公開性とを両立させたパブリッシュ・サブスクライブ・メッセージ・モデルを実現することが可能である。
【００１１】
（５）上記端末装置において、さらに、前記暗号化パブリッシュメッセージと前記非暗号化パブリッシュメッセージとのそれぞれにおける暗号文の配置パターンを識別するためのパターン識別データを、前記トピック指定データに含めるトピック処理部を備える構成としてもよい。端末装置から配信される暗号化パブリッシュメッセージと非暗号化パブリッシュメッセージのトピック指定データには、パターン識別データが含まれている。このため、外部装置では、このパターン識別データに基づき、暗号化パブリッシュメッセージと非暗号化パブリッシュメッセージとのそれぞれにおける暗号文の配置パターンを識別できる。これにより、例えばパターン識別データを外部装置に伝達する手段を別途要することなく、暗号文の配置パターンが随時変わり得るパブリッシュメッセージに対する処理を外部装置に正常に行わせることができる。
【００１２】
（６）上記端末装置において、さらに、前記暗号メッセージデータを復号化するための復号化ルールと暗号鍵との少なくとも一方を含む暗号ルールデータを生成する暗号ルール生成部を備え、前記データ配信部は、前記トピック指定データと前記暗号ルールデータとを含む暗号ルールパブリッシュメッセージを前記ブローカに配信する構成としてもよい。本端末装置によれば、端末装置側で生成した暗号ルールおよび暗号鍵の少なくとも一方が、パブリッシュ・サブスクライブ・メッセージ・モデルに基づく通信によって外部装置に配信される。これにより、端末装置側で暗号ルールや暗号鍵を定めつつ、別の通信手段を要することなく、暗号ルールや暗号鍵を外部装置に配信することができる。
【００１３】
（７）上記端末装置において、前記暗号ルールデータは、前記復号化ルールと、前記暗号鍵と、前記復号化ルールと前記暗号鍵とを区切る区切り文字であって、複数の文字列である区切り文字を含む構成としてもよい。本端末装置によれば、予め共通の区切り文字を把握している外部装置だけが、ブローカから受信した暗号ルールパブリッシュメッセージから暗号ルールデータを取得することができる。これにより、特定の外部装置への暗号ルールデータの配信の機密性を向上させることができる。
【００１４】
（８）上記端末装置において、さらに、暗号変更条件が満たされるか否かを判断する暗号変更判断部を備え、前記暗号変更判断部によって前記暗号変更条件が満たされると判断された場合、暗号ルール生成部は、前記復号化ルールと前記暗号鍵と前記区切り文字との少なくとも１つを変更した新たな暗号ルールデータを生成する構成としてもよい。本端末装置によれば、端末装置側で暗号ルールと暗号鍵と区切り文字との少なくとも１つが変更される。これにより、特定の外部装置への暗号ルールデータの配信の機密性を効果的に向上させることができる。
【００１５】
（９）上記端末装置において、前記暗号変更判断部は、第１の暗号変更条件と、前記第１

の暗号変更条件よりも満たす頻度が高い第２の暗号変更条件とのそれぞれが満たされるか否かを判断し、暗号ルール生成部は、前記暗号変更判断部によって前記第１の暗号変更条件が満たされると判断された場合、前記復号化ルールと前記暗号鍵との少なくとも１つを変更した新たな第１の暗号ルールデータを生成し、前記暗号変更判断部によって前記第２の暗号変更条件が満たされると判断された場合、前記区切り文字を変更した新たな第２の暗号ルールデータを生成する構成としてもよい。本端末装置によれば、変更に伴う処理負担が比較的に小さい区切り文字の変更頻度が、暗号ルールや暗号鍵の変更頻度よりも高いため、暗号ルールデータの変更に伴う処理負担を抑制しつつ、特定の外部装置への暗号ルールデータの配信の機密性を、より効果的に向上させることができる。

【００１６】

（１０）本明細書に開示されるコンピュータプログラムは、外部装置との間で、ブローカを介して、パブリッシュ・サブスクライブ・メッセージ・モデルに基づく通信を行う端末装置が有するコンピュータに、外部データを取得する取得処理と、前記外部データの少なくとも一部を暗号化して、暗号文を含む暗号メッセージデータを生成する暗号化処理と、平文のトピック指定データと、前記暗号メッセージデータと、を含む暗号化パブリッシュメッセージを生成するデータ生成処理と、前記データ生成処理によって生成された前記暗号化パブリッシュメッセージを、前記ブローカに配信するデータ配信処理と、を実行させる。本コンピュータプログラムによれば、暗号メッセージデータの機密性を確保しつつ外部装置に配信することが可能である。

【００１７】

（１１）本明細書に開示される通信システムは、複数の端末装置と、ブローカと、を備え、前記複数の端末装置の間で、ブローカを介して、パブリッシュ・サブスクライブ・メッセージ・モデルに基づく通信を行う通信システムであって、少なくとも一の前記端末装置は、外部データを取得する取得部と、前記外部データの少なくとも一部を暗号化して、暗号文を含む暗号メッセージデータを生成する暗号化処理部と、平文のトピック指定データと、前記暗号メッセージデータと、を含む暗号化パブリッシュメッセージを、前記ブローカに配信するデータ配信部と、を備え、少なくとも、前記一の端末装置とは異なる他の端末装置は、前記ブローカから、前記暗号化パブリッシュメッセージを購読するデータ購読部と、前記暗号化パブリッシュメッセージに含まれる前記暗号メッセージデータを復号化する復号化処理部と、を備える。本通信システムによれば、暗号メッセージデータの機密性を確保しつつ一の端末装置から他の端末装置に配信することが可能である。

【００１８】

（１２）本明細書に開示される通信方法は、複数の端末装置の間で、ブローカを介して、パブリッシュ・サブスクライブ・メッセージ・モデルに基づく通信を行う通信方法であって、少なくとも一の前記端末装置が、外部データを取得する取得し、前記外部データの少なくとも一部を暗号化して、暗号文を含む暗号メッセージデータを生成し、平文のトピック指定データと、前記暗号メッセージデータと、を含む暗号化パブリッシュメッセージを生成し前記暗号化パブリッシュメッセージを、前記ブローカに配信する、パブリッシュ処理と、少なくとも、前記一の端末装置とは異なる他の端末装置が、前記ブローカから、前記暗号化パブリッシュメッセージを購読し、前記暗号化パブリッシュメッセージに含まれる前記暗号メッセージデータを復号化する、サブスクライブ処理と、を備える。本通信方法によれば、暗号メッセージデータの機密性を確保しつつ一の端末装置から他の端末装置に配信することが可能である。

【００１９】

なお、本明細書に開示される技術は、種々の形態で実現することが可能であり、例えば、端末装置（パブリッシャ／サブスクライバ）、ブローカと複数の端末装置とを備える通信システム、通信方法、それらの方法を実現するコンピュータプログラム、そのコンピュータプログラムを記録した一時的でない記録媒体等の形態で実現することができる。

【図面の簡単な説明】

【００２０】

【図１】本実施形態における通信システム１０の概略構成を示す説明図
【図２】ブローカ１００の構成を概略的に示すブロック図
【図３】端末装置２００の構成を概略的に示すブロック図
【図４】パブリッシュ処理の内容を示すフローチャート
【図５】暗号変更処理の内容を示すフローチャート
【図６】サブスクライブ処理の内容を示すフローチャート
【図７】通信システム１０の使用例を示す説明図
【発明を実施するための形態】
【００２１】
Ａ．実施形態：
Ａ－１．通信システム１０の構成：
図１は、本実施形態における通信システム１０の概略構成を示す説明図である。通信システム１０は、パブリッシュ・サブスクライブ（Ｐｕｂｌｉｓｈ－Ｓｕｂｓｃｒｉｂｅ）・メッセージ・モデル（以下、「パブ・サブ・モデル」という）により、複数の端末装置２００の間で通信を行うためのシステムである。通信システム１０は、ブローカ（「サーバ」ということもある）１００と、複数のユーザＰ（Ｐ１，Ｐ２，・・・，Ｐｎ）が使用する端末装置２００とを備える。通信システム１０を構成する各装置は、通信ネットワークＮＥＴを介して互いに通信可能に接続されている。
【００２２】
ブローカ１００は、パブ・サブ・モデルにおいて、複数の端末装置２００の間でメッセージを交換するために、各端末装置２００から、メッセージの出版やメッセージの購読の要求を受け付ける管理装置である。ブローカ１００は、パブ・サブ・モデルに対応するプロトコルとして、例えば、ＭＱＴＴ（ＭＱ Ｔｅｌｅｍｅｔｒｙ Ｔｒａｎｓｐｏｒｔ）、ＡＭＱＰ（Ａｄｖａｎｃｅｄ Ｍｅｓｓａｇｅ Ｑｕｅｕｉｎｇ Ｐｒｏｔｏｃｏｌ）、ＯＰＣ ＵＡ（ＯＰＣ Ｕｎｉｆｉｅｄ Ａｒｃｈｉｔｅｃｔｕｒｅ）、ＸＭＰＰ（ｅＸｔｅｎｓｉｂｌｅ Ｍｅｓｓａｇｉｎｇ ａｎｄ Ｐｒｅｓｅｎｃｅ Ｐｒｏｔｏｃｏｌ）のＰｕｂＳｕｂ拡張（ＸＥＰ－００６０）等を実装してもよい。
【００２３】
図２は、ブローカ１００の構成を概略的に示すブロック図である。ブローカ１００は、制御部１１０と、記憶部１３０と、表示部１５２と、操作入力部１５６と、インターフェース部１５８とを備える。これらの各部は、バス１９０を介して互いに通信可能に接続されている。
【００２４】
ブローカ１００の表示部１５２は、例えば液晶ディスプレイや有機ＥＬディスプレイ等により構成され、各種の画像や情報を表示する。また、操作入力部１５６は、例えばキーボードやマウス、ボタン、マイク等により構成され、管理者の操作や指示を受け付ける。また、インターフェース部１５８は、例えばＬＡＮインターフェースやＵＳＢインターフェース等により構成され、有線または無線により他の装置との通信を行う。
【００２５】
ブローカ１００の記憶部１３０は、例えばＲＯＭやＲＡＭ、ハードディスクドライブ（ＨＤＤ）等により構成され、各種のプログラムやデータを記憶したり、各種のプログラムを実行する際の作業領域やデータの一時的な記憶領域として利用されたりする。例えば、記憶部１３０には、パブ・サブ・モデルに関する各種処理を実行するためのコンピュータプログラムであるブローカプログラムＢＰが格納されている。ブローカプログラムＢＰは、例えば、ＣＤ－ＲＯＭやＤＶＤ－ＲＯＭ、ＵＳＢメモリ等のコンピュータ読み取り可能な記録媒体（不図示）に格納された状態で提供され、あるいは外部装置から通信ネットワークＮＥＴを介してダウンロードされ、ブローカ１００にインストールすることにより記憶部１３０に格納される。
【００２６】
ブローカ１００の記憶部１３０には、トピック管理データＴＤが格納されている。トピ

ック管理データＴＤは、パブリッシャとして機能する端末装置２００から受信したパブリッシュメッセージに含まれるメッセージデータを、そのパブリッシュメッセージに含まれるトピック指定データにより指定されたトピックに対応付けて登録するための記憶領域である。トピック（「キー」または「ネーム」といわれることもある）は、メッセージを配信（出版）するための論理チャネルを示す名称である。

【００２７】

ブローカ１００の制御部１１０は、例えばＣＰＵ等により構成され、記憶部１３０から読み出したコンピュータプログラムを実行することにより、ブローカ１００の動作を制御する。例えば、制御部１１０は、記憶部１３０からブローカプログラムＢＰを読み出して実行することにより、パブ・サブ・モデルに関する各種処理を実行するメッセージ管理部１１２として機能する。この機能については、後述のメッセージ管理処理の説明に合わせて説明する。

【００２８】

端末装置２００は、例えば、スマートフォンやタブレット型端末、パーソナルコンピュータ（ＰＣ）、ＧＰＳ（Ｇｌｏｂａｌ　Ｐｏｓｉｔｉｏｎｉｎｇ　Ｓｙｓｔｅｍ）端末、ウェアラブル端末、センサ等である。図３は、端末装置２００の構成を概略的に示すブロック図である。端末装置２００は、制御部２１０と、記憶部２３０と、表示部２５２と、取得部２５４と、操作入力部２５６と、インターフェース部２５８とを備える。これらの各部は、バス２９０を介して互いに通信可能に接続されている。

【００２９】

端末装置２００の表示部２５２は、例えば液晶ディスプレイや有機ＥＬディスプレイ等により構成され、各種の画像や情報を表示する。また、操作入力部２５６は、例えばキーボードやマウス、ボタン、マイク等により構成され、ユーザＰの操作や指示を受け付ける。なお、表示部２５２がタッチパネルを備えることにより、操作入力部２５６として機能するとしてもよい。また、インターフェース部２５８は、例えばＬＡＮインターフェースやＵＳＢインターフェース等により構成され、有線または無線により他の装置との通信を行う。

【００３０】

取得部２５４は、例えばカメラ、マイク、各種のセンサ（温度センサ等）、ＧＰＳの受信アンテナ等を備え、外部データを取得する。外部データは、例えば、温度等の気象データ（環境データ）、位置（緯度・経度）データ、センサや計測器等による検知データ（緊急通報データ、異常検知データ、血圧や脈拍等の体内データなど）である。なお、操作入力部２５６が取得部として機能する構成でもよい。この場合、外部データは、操作入力部２５６の操作による入力情報（例えば氏名や年齢等の個人情報など）である。

【００３１】

端末装置２００の記憶部２３０は、例えばＲＯＭやＲＡＭ、ＨＤＤ等により構成され、各種のプログラムやデータを記憶したり、各種のプログラムを実行する際の作業領域やデータの一時的な記憶領域として利用されたりする。例えば、記憶部２３０には、パブ・サブ・モデルに関する各種処理を実行するためのアプリケーションプログラムであるパブリッシュプログラムＰＰとサブスクライブプログラムＳＰとが格納されている。パブリッシュプログラムＰＰとサブスクライブプログラムＳＰとは、例えば、ＣＤ－ＲＯＭやＤＶＤ－ＲＯＭ、ＵＳＢメモリ等のコンピュータ読み取り可能な記録媒体（不図示）に格納された状態で提供され、あるいは外部装置から通信ネットワークＮＥＴを介してダウンロードされ、端末装置２００にインストールすることにより記憶部２３０に格納される。

【００３２】

端末装置２００の制御部２１０は、例えばＣＰＵ等により構成され、記憶部２３０から読み出したコンピュータプログラムを実行することにより、端末装置２００の動作を制御する。例えば、制御部２１０は、記憶部２３０からパブリッシュプログラムＰＰを読み出して実行することにより、パブリッシュ処理を実行するパブリッシュ処理部２１２として機能する。このとき、端末装置２００は、ブローカ１００に対してメッセージの配信（送

信）を要求するパブリッシャとして機能する。以下、パブリッシャとして機能する端末装置２００を、特に「パブリッシャ２００Ｐ」という。なお、パブリッシュ処理部２１２は、配信条件判断部２１３と暗号化判断部２１４と暗号化処理部２１５とトピック処理部２１６とデータ配信部２１７と暗号変更判断部２１８と暗号ルール生成部２１９とを含む。これら各部の機能については、後述のパブリッシュ処理の説明に合わせて説明する。パブリッシャ２００Ｐとして機能する端末装置２００は、特許請求の範囲におけるパブリッシャの一例である。

【００３３】

制御部２１０は、記憶部２３０からサブスクライブプログラムＳＰを読み出して実行することにより、サブスクライブ処理を実行するサブスクライブ処理部２２２として機能する。このとき、端末装置２００は、ブローカ１００に対してメッセージの購読（受信）を要求するサブスクライバとして機能する。以下、サブスクライバとして機能する端末装置２００を、特に「サブスクライバ２００Ｓ」という。なお、サブスクライブ処理部２２２は、購読条件判断部２２３とデータ振り分け部２２４と暗号取得部２２５と復号化処理部２２６とを含む。これら各部の機能については、後述のサブスクライブ処理の説明に合わせて説明する。サブスクライバ２００Ｓとして機能する端末装置２００は、特許請求の範囲におけるサブスクライバ、外部装置の一例である。

【００３４】

Ａ－２．パブ・サブ・モデルに関する各種処理：

Ａ－２－１．ブローカ１００において実行される処理：

ブローカ１００において実行されるメッセージ管理処理について説明する。メッセージ管理処理は、パブリッシャ２００Ｐとサブスクライバ２００Ｓとの間のメッセージの配信および購読を仲介するための処理である。

【００３５】

ブローカ１００のメッセージ管理部１１２（図２）は、トピック指定データとメッセージデータとを含むパブリッシュメッセージをパブリッシャ２００Ｐから受信すると、受信したパブリッシュメッセージに含まれるメッセージデータを、トピック管理データＴＤにおいて、そのパブリッシュメッセージに含まれるトピック指定データにより指定されたトピックに登録する。一方、メッセージ管理部１１２は、トピックに登録されたメッセージデータを、そのトピックに予め申し込んでいたサブスクライバ２００Ｓに送信する。これにより、サブスクライバ２００Ｓは、パブリッシャ２００Ｐが配信するメッセージデータのうち、予め申し込んでいたトピックに対応するものだけを購読することができる。

【００３６】

Ａ－２－２．パブリッシャ２００Ｐにおいて実行される処理：

（パブリッシュ処理）

パブリッシャ２００Ｐにおいて実行されるパブリッシュ処理について説明する。パブリッシュ処理は、ブローカ１００に対して、メッセージの配信要求として、外部データを含むパブリッシュメッセージ（後述の暗号化パブリッシュメッセージＰＤ１，非暗号化パブリッシュメッセージＰＤ２）を配信する処理である。図４は、パブリッシュ処理の内容を示すフローチャートである。パブリッシュ処理は、例えば、端末装置２００の電源がオンされると、端末装置２００とブローカ１００とが通信可能に接続されることにより自動で開始され、端末装置２００の電源オン中、常時実行される。なお、パブリッシュ処理は、特定ユーザＰｘが端末装置２００の表示部２５２に表示されている画面に配置されたパブリッシュ用アイコン（図示しない）をタップすることにより手動で開始されてもよい。

【００３７】

記憶部２３０には、予め、暗号情報ＱＤと区切り文字ＷＤとが記憶されているものとする。暗号情報ＱＤは、復号化ルールと暗号鍵（「秘密鍵」ともいう）とを含む。区切り文字ＷＤは、１または複数の文字列であり、例えばアルファベットと数字と記号との少なくとも２つの組み合わせでもよい。記憶部２３０への暗号情報ＱＤおよび区切り文字ＷＤの初期値の記憶方法は、暗号情報ＱＤが外部機器からメール、ブルートゥース（登録商標）

、ピアツーピア等の通信手段を介して端末装置２００に送信されて記憶部２３０に記憶されてもよいし、暗号情報ＱＤがユーザＰによる入力操作や外部メモリからのデータ移動、ＱＲコード（登録商標）やバーコード読み取りを介して端末装置２００に入力されて記憶部２３０に記憶されてもよい。

【００３８】

図４に示すように、パブリッシャ２００Ｐの配信条件判断部２１３（図３）が、外部データの配信条件が満たされるか否かを判断する（Ｓ１１０）。配信条件は、外部データを配信するための条件であり、例えば、予め定められた周期の繰り返しタイミングや所定の期限が到来することでもよいし、取得部２５４が外部データを取得したときでもよいし、取得部２５４が取得する外部データが変化したときなどでもよい。なお、取得部２５４は、複数種の外部データを、同時または互いに異なる時期に取得可能である。以下、取得部２５４が複数種の外部データを同時期に取得する場合を例に挙げて説明する。取得部２５４が外部データを取得する処理は、特許請求の範囲における取得処理の一例である。

【００３９】

配信条件判断部２１３によって配信条件が満たされると判断された場合（Ｓ１１０：ＹＥＳ）、暗号化判断部２１４（図３）が、取得された複数種の外部データのそれぞれについて、暗号化条件が満たされるか否かを判断する（Ｓ１２０）。暗号化条件は、取得部２５４が取得する外部データの少なくとも一部を暗号化するための条件であり、例えば、予め定められた周期の繰り返しタイミングや所定の期限が到来することでもよいし、取得部２５４が取得する外部データが変化したこと（例えば、異常性や緊急性を有する情報が含まれている、または、含まれていないこと、）でもよいし、外部データが相対的に機密性の高い（例えば個人情報、企業秘密情報）ことなどでもよい。暗号化条件は、複数種の外部データのそれぞれについて個別に設定されているものとする。暗号化判断部２１４は、複数種の外部データのうち、暗号化条件を満たす外部データが少なくとも１種存在する場合、暗号化条件が満たされると判断する。複数種の外部データには、常に暗号化条件が満たされずに暗号化されない外部データ（例えば機密性が低く、公開性が重視される外部データ）が含まれていてもよい。

【００４０】

暗号化判断部２１４によって暗号化条件が満たされると判断した場合（Ｓ１２０：ＹＥＳ）、トピック処理部２１６（図３）は、暗号化条件に応じたパターン識別データを含むトピック指定データを生成する（Ｓ１３０）。ここで生成されるトピック指定データは、トピック識別データとパターン識別データとを含む。トピック識別データは、ブローカ１００で管理されるトピック名を示すデータである。

【００４１】

パターン識別データは、サブスクライバ２００Ｓにおいて、パブリッシュメッセージ（暗号化パブリッシュメッセージＰＤ１，非暗号化パブリッシュメッセージＰＤ２）における暗号文の配置パターンを識別するためのデータである。配置パターンは、メッセージデータにおける暗号文の有無と、メッセージデータにおける暗号文の位置とに応じたパターンである。例えば、メッセージデータが、複数種の外部データが区切り文字（例えばカンマ）で区切られたデータ列である場合、配置パターンは、複数種の外部データの全てが平文である全平文パターンと、暗号文である外部データを少なくとも１種含む暗号文パターンとを含む。平文とは、復号化せずにコンピュータ（ブローカ１００や端末装置２００）で解読可能なデータである。この暗号文パターンには、メッセージデータにおける暗号文の位置に応じた複数のパターンが含まれる。

【００４２】

例えば、メッセージデータに、第１の外部データと第２の外部データとがこの順で含まれる場合、配置パターンには、次のパターンが含まれる。

「全平文パターン」："第１の外部データ（平文），第２の外部データ（平文）"

「前半暗号文パターン」："第１の外部データ（暗号文），第２の外部データ（平文）"

「後半暗号文パターン」："第１の外部データ（平文），第２の外部データ（暗号文）"

「全暗号文パターン」："第１の外部データ（暗号文），第２の外部データ（暗号文）"
なお、複数種の外部データ（第１の外部データ、第２の外部データ）を暗号化する場合、暗号化処理部２１５は、複数種の外部データのそれぞれを、暗号ルールおよび暗号鍵の少なくとも一方が互いに異なる方法により暗号化して、暗号メッセージデータを生成してもよい。

【００４３】

次に、暗号化処理部２１５（図３）は、複数種の外部データのうち、暗号化すべき外部データを暗号化して、暗号メッセージデータを生成する（Ｓ１４０～Ｓ１７０）。暗号化メッセージデータは、複数種の外部データの少なくとも１種が暗号化された暗号文を含むデータ列である。例えば、複数種の外部データが上述の第１の外部データおよび第２の外部データである場合、暗号化メッセージデータは、上述の前半暗号文パターンと後半暗号文パターンと全暗号文パターンとのいずれかのパターンのメッセージデータである。

【００４４】

具体的には、暗号化処理部２１５は、複数種の外部データのそれぞれについて、次の処理を順次行う。まず、暗号化処理部２１５は、外部データＸの暗号化が必要であるか否かを判断する（Ｓ１４０）。外部データＸは、複数種の外部データのそれぞれを意味するものとする。暗号化処理部２１５は、上記Ｓ１２０での暗号化判断部２１４による暗号化判断の結果に基づき、外部データＸの暗号化の要否を判断する。暗号化処理部２１５は、外部データＸの暗号化が必要であると判断した場合（Ｓ１４０：ＹＥＳ）、その外部データＸに対応する最新の暗号情報ＱＤを記憶部２３０から読みだして、その暗号情報ＱＤに基づき外部データＸを暗号化し、メッセージデータにセットする（Ｓ１５０）。ここで、後述するように、最新の暗号情報ＱＤは、トピックに登録しているサブスクライバ２００Ｓでも把握されている。すなわち、この外部データＸは、上記トピックに登録しているサブスクライバ２００Ｓにて復号化可能な暗号化処理により暗号化されることになる。Ｓ１５０の処理は、特許請求の範囲における暗号化処理の一例である。

【００４５】

暗号化処理部２１５は、外部データＸの暗号化が不要であると判断した場合（Ｓ１４０：ＮＯ）、その外部データＸを暗号化せずに平文のままメッセージデータにセットする（Ｓ１６０）。未処理の外部データＸが残っている場合（Ｓ１７０：ＮＯ）、暗号化処理部２１５は、Ｓ１４０に戻り、次の順位の外部データＸについてＳ１４０以降の処理を実行する。全ての外部データＸの処理が終了した場合（Ｓ１７０：ＹＥＳ）、データ配信部２１７は、暗号化パブリッシュメッセージＰＤ１を生成してブローカ１００に配信する（Ｓ１８０）。暗号化パブリッシュメッセージＰＤ１は、平文の上記トピック指定データと、暗号化メッセージデータとを含む配信用データである。パブリッシャ２００Ｐの制御部２１０は、暗号化パブリッシュメッセージＰＤ１の配信後、Ｓ１１０の処理に戻り待機状態となる。Ｓ１８０の処理は、特許請求の範囲におけるデータ生成処理およびデータ配信処理の一例である。

【００４６】

暗号化判断部２１４によって暗号化条件が満たされないと判断した場合（Ｓ１２０：Ｎ）、非暗号化パブリッシュメッセージＰＤ２を生成してブローカ１００に配信する（Ｓ１９０）。すなわち、複数種の外部データはいずれも暗号化されずに平文のままセットされた上述の全平文パターンのメッセージデータが生成される。すなわち、非暗号化パブリッシュメッセージＰＤ２は、平文のトピック指定データと、平文のメッセージデータとを含む配信用データである。パブリッシャ２００Ｐの制御部２１０は、非暗号化パブリッシュメッセージＰＤ２の配信後、Ｓ１１０の処理に戻り待機状態となる。なお、Ｓ１１０において、配信条件判断部２１３によって配信条件が満たされないと判断された場合（Ｓ１１０：ＮＯ）、Ｓ１１０の処理において待機状態となる。

【００４７】

（暗号変更処理）

パブリッシャ２００Ｐにおいて実行される暗号変更処理について説明する。暗号化変更

処理とは、上記暗号化パブリッシュメッセージＰＤ１の機密性の向上のために、暗号化パブリッシュメッセージＰＤ１に含まれる暗号化メッセージデータをサブスクライバ２００Ｓで復号化するための暗号情報ＱＤを適宜変更するための処理である。図５は、暗号変更処理の内容を示すフローチャートである。

【００４８】

図５に示すように、パブリッシャ２００Ｐの暗号変更判断部２１８（図３）が、外部データＸの暗号変更条件が満たされるか否かを判断する（Ｓ２１０）。暗号変更条件は、複数種の外部データＸのそれぞれについて、外部データを暗号化および復号化する際に用いる暗号情報ＱＤの少なくとも一部を変更するための条件である。暗号変更条件は、例えば、ユーザＰによる所定の操作があったことでもよいし、外部データの暗号化処理の回数が所定回数に達したことでもよいし、予め定められた周期の繰り返しタイミングや所定の期限が到来することでもよい。

【００４９】

暗号変更判断部２１８によって暗号変更条件が満たされると判断された場合（Ｓ２１０：ＹＥＳ）、暗号ルール生成部２１９（図３）が、外部データＸの最新の暗号ルールデータを生成する。暗号ルールデータは、暗号情報ＱＤと区切り文字ＷＤとを含む情報である。暗号ルール生成部２１９は、予め定められたアルゴリズムに従って、外部データＸの新規の暗号情報ＱＤを生成して記憶部２３０の記憶内容を更新する（Ｓ２２０）。新規の暗号情報ＱＤは、すでに記憶部２３０に記憶されている暗号情報ＱＤに対して、復号化ルールと暗号鍵との少なくとも一方が異なる。

【００５０】

ここで、暗号変更判断部２１８は、図５のＳ２１０とは別に、外部データＸの区切り文字変更条件が満たされるか否かを判断し、区切り文字変更条件が満たされると判断した場合に、予め定められたアルゴリズムに従って、外部データＸの新規の区切り文字ＷＤを生成して記憶部２３０の記憶内容を更新する。区切り文字変更条件は、記憶部２３０に記憶されている区切り文字ＷＤを変更するための条件であり、Ｓ２１０における上記暗号変更条件よりも条件を満たす頻度が高い条件である。区切り文字変更条件は、例えば、外部データＸの暗号化処理の回数が、暗号変更条件よりも少ない所定回数に達したことでもよいし、暗号変更条件よりも短い周期の繰り返しタイミングや所定の期限が到来することでもよい。本実施形態では、例えば、ワンタイムパスワード（タイムスタンプ方式でもよいし、チャレンジレスポンス方式でもよい）を用いて所定時間（例えば５分程度）ごとに区切り文字ＷＤを短時間で変更してもよい。

【００５１】

従って、暗号ルール生成部２１９によって生成される暗号ルールデータは、最新の暗号情報ＱＤと最新の区切り文字ＷＤとを含む情報であり、区切り文字ＷＤは、暗号情報ＱＤよりも高い頻度で随時変更される。Ｓ２１０における暗号変更条件は、特許請求の範囲における第１の暗号変更条件の一例であり、区切り文字変更条件は、特許請求の範囲における第２の暗号変更条件の一例である。

【００５２】

次に、データ配信部２１７は、外部データＸの最新の暗号ルールデータから、外部データＸの暗号ルールパブリッシュメッセージＰＤ３を生成し、暗号ルールパブリッシュメッセージＰＤ３をブローカ１００に配信する（Ｓ２３０）。暗号ルールパブリッシュメッセージＰＤ３は、平文のトピック指定データと、平文の暗号ルールデータとを含む配信用のデータ列である。平文のトピック指定データには、トピック識別データに加えて、暗号ルールの通知の有無を示す暗号ルール通知データが含まれる。暗号ルールデータは、平文の復号化ルールと平文の暗号鍵とが、平文の上記区切り文字ＷＤによって区切られつつ、この順序で配列されたデータ列（メッセージデータ）である。なお、復号化ルールと暗号鍵との順序は互いに入れ替えてもよい。パブリッシャ２００Ｐの制御部２１０は、暗号ルールパブリッシュメッセージＰＤ３の配信後、Ｓ２１０の処理に戻り待機状態となる。Ｓ２１０において、暗号変更判断部２１８によって暗号変更条件が満たされないと判断された

場合（Ｓ２１０：ＮＯ）もＳ２１０の処理において待機状態となる。
【００５３】
Ａ－２－３．サブスクライバ２００Ｓにおいて実行される処理：
サブスクライバ２００Ｓにおいて実行されるサブスクライブ処理について説明する。サブスクライブ処理は、ブローカ１００に対して、メッセージの購読要求として、パブリッシュメッセージ（外部データを含むパブリッシュメッセージＰＤ１，ＰＤ２、暗号ルールパブリッシュメッセージＰＤ３）を購読する処理である。図６は、サブスクライブ処理の内容を示すフローチャートである。サブスクライブ処理は、例えば端末装置２００の電源がオンされると、端末装置２００とブローカ１００とが通信可能に接続されることにより自動で開始され、端末装置２００の電源オン中、所定の時間間隔ごとに繰り返し実行される。なお、サブスクライブ処理は、特定ユーザＰｘが端末装置２００の表示部２５２に表示されている画面に配置されたサブスクライブ用アイコン（図示しない）をタップすることにより手動で開始されてもよい。
【００５４】
図６に示すように、サブスクライバ２００Ｓの購読条件判断部２２３（図３）は、ブローカ１００にて登録されたトピックの購読条件が満たされるか否かを判断する（Ｓ３１０）。購読条件は、トピックに対応するパブリッシュメッセージを購読（受信）するための条件であり、例えば、予め定められた周期の繰り返しタイミングや所定の期限が到来することでもよい。
【００５５】
購読条件判断部２２３によって購読条件が満たされると判断された場合（Ｓ３１０：ＹＥＳ）、データ振り分け部２２４（図３）は、トピックに登録されているパブリッシュメッセージ（ＰＤ１からＰＤ３のいずれか）を購読（受信）して、この購読が、暗号情報ＱＤの購読であるか否かを判断する（Ｓ３２０）。このとき、データ振り分け部２２４は、特許請求の範囲におけるデータ購読部の一例である。データ振り分け部２２４は、パブリッシュメッセージに含まれるトピック指定データに上記暗号ルール通知データが含まれていれば、暗号情報ＱＤ（暗号ルールパブリッシュメッセージＰＤ３）の購読であると判断し、トピック指定データに暗号ルール通知データが含まれていなければ、外部データ（暗号化パブリッシュメッセージＰＤ１または非暗号化パブリッシュメッセージＰＤ２）の購読であると判断する。
【００５６】
データ振り分け部２２４によって暗号情報の購読であると判断された場合（Ｓ３２０：ＹＥＳ）、暗号取得部２２５は、現在、記憶部２３０に記憶されている区切り文字ＷＤに一致する区切り文字が、暗号ルールデータに含まれるか否かを判断する（Ｓ３３０）。暗号取得部２２５は、一致する区切り文字が暗号ルールデータに含まれると判断した場合（Ｓ３３０：ＹＥＳ）、その区切り文字ＷＤによって区切られた復号化ルールと暗号鍵とを取り出すことができる。そこで、暗号取得部２２５（図３）は、暗号ルールデータから最新の暗号情報ＱＤを取得して記憶部２３０に記憶して更新し（Ｓ３４０）、Ｓ３１０に戻る。これにより、サブスクライバ２００Ｓは、パブリッシャ２００Ｐにて随時変更される暗号情報ＱＤに基づく暗号化される暗号メッセージデータを復号化することができる。
【００５７】
暗号取得部２２５は、一致する区切り文字が暗号ルールデータに含まれないと判断した場合（Ｓ３３０：ＮＯ）、暗号ルールデータから最新の暗号情報ＱＤを取得できないため、記憶部２３０に記憶している暗号情報ＱＤは更新されずに、Ｓ３１０に戻る。このように、共通のトピックに登録した複数のサブスクライバ２００Ｓについて、それぞれが把握する最新の区切り文字ＷＤを互いに異ならせることにより、互いに異なるタイミングで個別に暗号ルールデータを変更することができる。
【００５８】
データ振り分け部２２４によって暗号情報の購読でないと判断された場合（Ｓ３２０：ＮＯ）、復号化処理部２２６（図３）は、メッセージデータが暗号化されているか、すな

わち暗号化メッセージデータであるか否かを判断する（Ｓ３５０）。復号化処理部２２６は、パブリッシュメッセージのトピック指定データに含まれるパターン識別データが、上記暗号文パターンを示す場合、メッセージデータが暗号化されていると判断し、パターン識別データが、上記全平文パターンを示す場合、メッセージデータが暗号化されていないと判断する。

【００５９】

データ振り分け部２２４によってメッセージデータが暗号化されていると判断された場合（Ｓ３５０：ＹＥＳ）、復号化処理部２２６は、現在、記憶部２３０に記憶されている暗号情報ＱＤを用いて暗号化メッセージデータに含まれる暗号文を復号化できるか否かを判断する（Ｓ３６０）。なお、復号化処理部２２６は、パターン識別データに基づき、暗号化メッセージデータにおける暗号文の配置を把握できる。復号化処理部２２６は、復号化できると判断した場合（Ｓ３６０：ＹＥＳ）、暗号情報ＱＤに従って、暗号化メッセージデータに含まれる暗号文を復号化する（Ｓ３７０）。これにより、暗号化メッセージデータに含まれる複数種の外部データの全てが平文で取得される。次に、サブスクライバ２００Ｓの制御部２１０は、平文のメッセージデータに基づく処理を実行し（Ｓ３８０）、Ｓ３１０に戻る。

【００６０】

復号化処理部２２６によって復号化できないと判断された場合（Ｓ３６０：ＮＯ）、サブスクライバ２００Ｓの制御部２１０は、暗号化メッセージデータに含まれる平文だけを取得し、その平文に基づく処理を実行し（Ｓ３８０）、Ｓ３１０に戻る。

【００６１】

データ振り分け部２２４によってメッセージデータが暗号化メッセージデータでないと判断された場合（Ｓ３５０：ＮＯ）、サブスクライバ２００Ｓの制御部２１０は、メッセージデータに含まれる平文に基づく処理を実行し（Ｓ３８０）、Ｓ３１０に戻る。また、Ｓ３１０において、購読条件判断部２２３によって購読条件が満たされないと判断された場合（Ｓ３１０：ＮＯ）には待機状態になる。

【００６２】

Ａ－３．具体例：

次に上述した通信システム１０の使用例を説明する。図７は、通信システム１０の使用例を示す説明図である。図７に示すように、この説明では、次の点を前提とするものとする。通信システム１０は、１台のパブリッシャ２００Ｐと２台のサブスクライバ２００Ｓとを備える。外部データは、温度データと位置データとの２種である。パブリッシャ２００Ｐと第１のサブスクライバ２００Ｓ１とのそれぞれの記憶部２３０には、共通の暗号情報ＱＤおよび区切り文字ＷＤ（"ｔｅｍｐ＆ｇｐｓ　１"）が記憶されている。一方、第２のサブスクライバ２００Ｓ２の記憶部２３０には、共通の暗号情報ＱＤおよび区切り文字ＷＤが記憶されていない。

【００６３】

Ａ－３－１．暗号化パブリッシュメッセージＰＤ１の配信および購読：

暗号化パブリッシュメッセージＰＤ１の配信および購読について説明する。図７には、次の内容の暗号化パブリッシュメッセージＰＤ１が例示されている。

トピック（トピック指定データ）："温度＆ＧＰＳ／１"

なお、「／１」は、上記後半暗号文パターンを示すパターン識別データである。

メッセージ（メッセージデータ）："東京：２１．３℃，ｎＵｕｍＶ５ＲＵＣＢ３ＥｘｅｔｆＪｇｍＲｚＨＴ３ｖｐｐＦｓｄＵｊｓＱ６ＳｊＲａＴＡＫｆＦｈ／ＪＸＴＯＬｕ８５Ｋ６ｋｇＷ１＋６ｗＫ"

なお、「，」よりも前の文字列が温度データの平文であり、「，」よりも後ろの文字列が位置データ（緯度:３５．６８１２３６　経度:１３９．７６７１２５）を後述の暗号鍵（"Ｅｎｃｒｙｐｔｉｏｎ　ｋｅｙ"）で暗号化した暗号文である。

【００６４】

例えば、パブリッシャ２００Ｐでのパブリッシュ処理（図４）において、温度データの

暗号化条件は満たされず、位置データの暗号化条件が満たされる場合、Ｓ１２０において暗号化条件が満たされると判断される（Ｓ１２０：ＹＥＳ）。ここで、温度データは、公益性が高く、公開性を重視すべきデータであるため、温度データの暗号化条件は、常に満たされないとされている。一方、位置データは、パブリッシャ２００Ｐを所有するユーザＰ１の位置を特定する個人情報であり、機密性を重視すべきデータであるため、位置データの暗号化条件は、例えば取得部２５４が取得する外部データが正常状態を示すデータであることとされている。正常状態とは、例えば温度データが正常範囲内（例えば所定の上限温度以下、所定の下限温度以上）である状態である。また、位置データの暗号化条件は、位置データの位置が所定の禁止領域外であることなどでもよい。

【００６５】

次に、パブリッシャ２００Ｐでは、後半暗号文パターンを示すパターン識別データ「／１」を含むトピック指定データ（"温度＆ＧＰＳ／１"）が作成される（Ｓ１３０）。また、平文の温度データ（"東京：２１．３℃"）と暗号文の位置データ（"ｎＵｕｍＶ５ＲＵＣＢ３Ｅｘｅｔ１００ＪｇｍＲｚＨＴ３ｖｐｐＦｓｄＵｊｓＱ６ＳｊＲａＴＡＫＰＤ１Ｆｈ／ＪＸＴＯＬｕ８５Ｋ６ｋｇＷ１＋６ｗＫ"）がメッセージデータにセットされ（Ｓ１５０，Ｓ１６０）、上記暗号化パブリッシュメッセージＰＤ１が生成され、ブローカ１００に配信される（Ｓ１８０）。

【００６６】

第１のサブスクライバ２００Ｓ１および第２のサブスクライバ２００Ｓ２では、いずれも、サブスクライブ処理（図６）において、購読条件が満たされると（Ｓ３１０：ＹＥＳ）、暗号化パブリッシュメッセージＰＤ１がブローカ１００から購読される。暗号化パブリッシュメッセージＰＤ１のトピック指定データは、後半暗号文パターンを示すパターン識別データ（"／１"）を含んでいるため、暗号情報の購読でないと判断され（Ｓ３２０：ＮＯ）、メッセージデータは暗号化されていると判断される（Ｓ３５０：ＹＥＳ）。

【００６７】

ここで、第１のサブスクライバ２００Ｓ１の記憶部２３０には、パブリッシャ２００Ｐと共通の暗号情報ＱＤが記憶されている。このため、メッセージデータ中の暗号文の位置データが復号化される（Ｓ３６０：ＹＥＳ、Ｓ３７０）。すなわち、第１のサブスクライバ２００Ｓ１では、温度データと位置データとの両方の外部データを平文として取得でき、これらの温度データ及び位置データに基づく処理が実行される（Ｓ３８０）。例えば、第１のサブスクライバ２００Ｓ１の表示部２５２に、パブリッシャ２００Ｐで取得された温度とパブリッシャ２００Ｐの位置とに関する情報が表示される。これにより、第１のサブスクライバ２００Ｓ１を所有するユーザＰ２は、ユーザＰ１の周囲温度と居場所との両方を知ることができる。

【００６８】

一方、第２のサブスクライバ２００Ｓ２の記憶部２３０には、パブリッシャ２００Ｐと共通の暗号情報ＱＤが記憶されていない。メッセージデータ中の暗号文の位置データは復号化されない（Ｓ３６０：ＮＯ）。すなわち、第２のサブスクライバ２００Ｓ２では、温度データだけを平文として取得でき、この温度データに基づく処理が実行される（Ｓ３８０）。例えば、第２のサブスクライバ２００Ｓ２の表示部２５２に、パブリッシャ２００Ｐで取得された温度に関する情報が表示される。これにより、第２のサブスクライバ２００Ｓ２を所有するユーザＰ３は、ユーザＰ１の周囲温度を知ることはできるが居場所を知ることはできない。

【００６９】

以上のように、暗号化パブリッシュメッセージＰＤ１の配信および購読により、公開性を重視すべきデータ（温度データ）を、トピック（"温度＆ＧＰＳ／＃"）に登録している全てのサブスクライバ２００Ｓ（２００Ｓ１，２００Ｓ２）にて取得可能としつつ、機密性を重視すべきデータ（位置データ）を、一部のサブスクライバ２００Ｓ（２００Ｓ１）だけに取得可能とすることができる。

【００７０】

Ａ－３－２．非暗号化パブリッシュメッセージＰＤ２の配信および購読：
非暗号化パブリッシュメッセージＰＤ２の配信および購読について説明する。図７には、次の内容の非暗号化パブリッシュメッセージＰＤ２が例示されている。
トピック（トピック指定データ）："温度＆ＧＰＳ／ｅｍｇ"
なお、「／ｅｍｇ」は、「緊急」を意味するとともに、上記全平文パターンを示すパターン識別データである。
メッセージ（メッセージデータ）："緊急：緯度:３５．６８１２３６　経度:１３９．７６７１２５　東京：３８．１℃"
なお、メッセージデータは全て平文である。

【００７１】
例えば、パブリッシャ２００Ｐにおいて、取得部２５４が正常温度範囲を超える３８．１℃を示す温度データを取得した場合、温度データの暗号化条件だけでなく位置データの暗号化条件も満たされなくなる。すると、パブリッシュ処理（図４）において、暗号化条件が満たされないと判断される（Ｓ１２０：ＮＯ）。

【００７２】
次に、パブリッシャ２００Ｐでは、全平文パターンを示すパターン識別データ「／ｅｍｇ」を含むトピック指定データ（"温度＆ＧＰＳ／ｅｍｇ"）が作成され、上記非暗号化パブリッシュメッセージＰＤ２が生成され、ブローカ１００に配信される（Ｓ１９０）。

【００７３】
第１のサブスクライバ２００Ｓ１および第２のサブスクライバ２００Ｓ２では、いずれも、サブスクライブ処理（図６）において、購読条件が満たされると（Ｓ３１０：ＹＥＳ）、非暗号化パブリッシュメッセージＰＤ２がブローカ１００から購読される。非暗号化パブリッシュメッセージＰＤ２のトピック指定データは、全平文パターンを示すパターン識別データ（"／ｅｍｇ"）を含んでいるため、暗号情報の購読でないと判断され（Ｓ３２０：ＮＯ）、メッセージデータは暗号化されていないと判断される（Ｓ３５０：ＮＯ）。

【００７４】
この結果、第１のサブスクライバ２００Ｓ１および第２のサブスクライバ２００Ｓ２のいずれにおいても、温度データと位置データとの両方の外部データを平文として取得でき、これらの温度データ及び位置データに基づく処理が実行される（Ｓ３８０）。例えば、第１のサブスクライバ２００Ｓ１および第２のサブスクライバ２００Ｓ２の表示部２５２に、緊急とパブリッシャ２００Ｐで取得された温度とパブリッシャ２００Ｐの位置とに関する情報が表示される。これにより、第１のサブスクライバ２００Ｓ１を所有するユーザＰ２だけでなく、第２のサブスクライバ２００Ｓ２を所有するユーザＰ３も、ユーザＰ１の周囲温度と居場所との両方を知ることができる。

【００７５】
以上のように、暗号化パブリッシュメッセージＰＤ１および非暗号化パブリッシュメッセージＰＤ２の配信および購読により、暗号化条件に基づいて、機密性を重視すべきデータ（位置データ）を、トピック（"温度＆ＧＰＳ／＃"）に登録している全てのサブスクライバ２００Ｓ（２００Ｓ１，２００Ｓ２）に配信する公開配信形態と、一部のサブスクライバ２００Ｓ（２００Ｓ１）だけに配信する機密配信形態とを切り替えることができる。

【００７６】
Ａ－３－３．暗号ルールパブリッシュメッセージＰＤ３の配信および購読：
暗号ルールパブリッシュメッセージＰＤ３の配信および購読について説明する。図７には、次の内容の暗号ルールパブリッシュメッセージＰＤ３が例示されている。
トピック（トピック指定データ）："温度＆ＧＰＳ／ｋｅｙ"
なお、「／ｋｅｙ」は、暗号ルールの通知を意味する暗号ルール通知データである。
メッセージ（メッセージデータ）："ＣＳＶ－２Ｃｏｌｕｍｎｔｅｍｐ＆ｇｐｓ　１Ｅｎｃｒｙｐｔｉｏｎ　ｋｅｙ"
なお、区切り文字（"ｔｅｍｐ＆ｇｐｓ　１"）よりも前の文字列が復号化（暗号化）ルールの平文であり、区切り文字（"ｔｅｍｐ＆ｇｐｓ　１"）よりも後ろの文字列が暗

号鍵の平文である。「ＣＳＶ－２Ｃｏｌｕｍｎ」は、メッセージデータの２カラム目を復号化するというルールを意味する。

【００７７】

例えば、パブリッシャ２００Ｐでの暗号変更処理（図５）において、位置データの暗号変更条件が満たされると判断された場合（Ｓ２１０：ＹＥＳ）、新規の暗号情報ＱＤが生成されて記憶部２３０が記憶される（Ｓ２２０）。また、その新規の暗号情報ＱＤが区切り文字（"ｔｅｍｐ＆ｇｐｓ　１"）によって区切られた上記暗号ルールパブリッシュメッセージＰＤ３がブローカ１００に配信される（Ｓ２３０）。

【００７８】

トピック（"温度＆ＧＰＳ／＃"）に登録している第１のサブスクライバ２００Ｓ１には、共通の区切り文字ＷＤ（"ｔｅｍｐ＆ｇｐｓ　１"）が記憶されているため、購読した暗号ルールパブリッシュメッセージＰＤ３の暗号ルールデータにおける上記共通の区切り文字ＷＤを特定し、最新の暗号情報ＱＤ（復号化ルールと暗号鍵）を取得することができる。一方、トピック（"温度＆ＧＰＳ／＃"）に登録している第２のサブスクライバ２００Ｓ２には、共通の区切り文字ＷＤが記憶されていないため、購読した暗号ルールパブリッシュメッセージＰＤ３の暗号ルールデータから暗号情報ＱＤを取得することができない。すなわち、パブリッシャ２００Ｐ側で随時変更される暗号情報ＱＤを、機密性を確保しつつ、パブ・サブ・モデルにより特定のサブスクライバ２００Ｓ（２００Ｓ１）だけに購読させることができる。しかも、パブリッシャ２００Ｐと第１のサブスクライバ２００Ｓ１とでは、例えばワンタイムパスワードによって時刻に同期して共通の区切り文字が逐次変更されていく。このため、暗号情報ＱＤの機密性をより向上させることができる。

【００７９】

Ａ－４．使用例：

本実施形態の通信システム１０を例えば以下の形態で使用することができる。

（条件付きオープン形態）

条件付きオープン形態は、所定のオープン条件が満たされない場合、パブリッシャ２００Ｐが、機密性を重視する暗号化パブリッシュメッセージＰＤ１を配信し、所定のオープン条件が満たされる場合、パブリッシャ２００Ｐが、公開性を重視する非暗号化パブリッシュメッセージＰＤ２を配信する形態である。

【００８０】

条件付きオープン形態は、例えば次のような用途で使用可能である。

パブリッシャ２００Ｐのユーザ Ｐ１：被保護者（子ども老人、要介護者等）

第１のサブスクライバ２００Ｓ１のユーザＰ２：保護者（被保護者の家族や親族等）

第２のサブスクライバ２００Ｓ２のユーザＰ３：非保護者（トピックに登録している契約者、周辺住民等）

所定のオープン条件：緊急を要する事態が発生したこと

暗号化パブリッシュメッセージＰＤ１：機密性を重視すべき外部データ（例えば、体温、脈拍や発汗等の身体データなどの個人データや位置データ）の暗号文と、公開性を重視すべき外部データ（温度等の気象データなどの公共性の高いデータ）の平文とを含む。

なお、緊急事態の例としては、パブリッシャ２００Ｐの緊急ボタンが押下されたこと、パブリッシャ２００Ｐで所定の正常範囲外の値を示す外部データ（気象データ、身体データや位置データなど）が取得されたことなどが挙げられる。

【００８１】

オープン条件が満たされない場合、パブリッシャ２００Ｐから、機密性を重視する暗号化パブリッシュメッセージＰＤ１が配信される。その結果、機密性を重視すべき外部データは、保護者（Ｐ２）に取得されるが、非保護者（Ｐ３）には取得されず、機密性を重視すべき外部データの機密性が確保される。一方、公開性を重視すべき外部データは、保護者（Ｐ２）だけでなく非保護者（Ｐ３）にも取得される。このように公開性を重視すべき外部データを広く配信することにより、条件付きオープン形態の契約者へのサービスの向上や、ビックデータの取得と活用に繋げることができる。

【００８２】
オープン条件が満たされる場合、パブリッシャ２００Ｐから、非暗号化パブリッシュメッセージＰＤ２が配信される。その結果、機密性を重視すべき外部データは、保護者（Ｐ２）だけでなく非保護者（Ｐ３）にも取得される。これにより、例えば、被保護者（Ｐ１）を見つけた非保護者（Ｐ３）は、機密性を重視すべき外部データに基づき適切な対応を行うことができる。
【００８３】
（位置発信形態）
位置発信形態は、パブリッシャ２００Ｐが、個人の位置データの平文を含む暗号化パブリッシュメッセージＰＤ１を配信する形態である。
【００８４】
位置発信形態は、例えば次のような用途で使用可能である。
パブリッシャ２００Ｐのユーザ Ｐ１：注意対象者（子ども老人、要介護者、ウイルス感染者等）
第１のサブスクライバ２００Ｓ１のユーザＰ２：関係者（注意対象者の家族や親族等）
第２のサブスクライバ２００Ｓ２のユーザＰ３：非関係者（トピックに登録している契約者、車両、自転車やバイク等のドライバ、周辺住民等）
暗号化パブリッシュメッセージＰＤ１：特に機密性を重視すべき外部データ（例えば注意対象者（Ｐ１）を特定可能な個人データ）の暗号文と、その注意対象者（Ｐ１）の位置を特定するための位置データの平文とを含む。
【００８５】
パブリッシャ２００Ｐから、位置データの平文を含む暗号化パブリッシュメッセージＰＤ１が配信される。この結果、注意対象者（Ｐ１）の位置データは、関係者（Ｐ２）だけでなく非関係者（Ｐ３）にも取得される。但し、注意対象者（Ｐ１）の個人データは、関係者（Ｐ２）に取得されるが、非関係者（Ｐ３）には取得されない。すなわち、関係者（Ｐ２）は、自分の保護対象の注意対象者（Ｐ１）がどこにいるかを常に把握することができる。一方、非関係者（Ｐ３）は、注意対象者（Ｐ１）が誰であるかは知らないが注意すべき注意対象者（Ｐ１）の位置を第２のサブスクライバ２００Ｓ２の表示部２５２等を介して把握できる。これにより、例えば車両等に搭載されたカーナビゲーションシステムや所有の携帯電話等に表示される地図上に、注意対象者（Ｐ１）の位置を表示させることにより、注意対象者（Ｐ１）の近くを通るため、特に運転等に注意する必要があることを知ることができ、交通事故の抑制を期待することができる。
【００８６】
Ａ－５．本実施形態の効果：
以上説明したように、本実施形態のパブリッシャ２００Ｐは、平文のトピック指定データと、外部データの少なくとも一部を暗号化した暗号メッセージデータとを含む暗号化パブリッシュメッセージＰＤ１を、ブローカ１００に配信することができる（図４参照）。このため、ブローカ１００では、暗号メッセージデータの復号化を要することなく、その暗号メッセージデータが指定されたトピックに登録される。これにより、本実施形態によれば、暗号メッセージデータの機密性を確保しつつ外部装置（サブスクライバ２００Ｓ）に配信することが可能である。すなわち、トピックを暗号化しないことにより、メッセージデータの暗号化を実現しつつ、ブローカ１００でのトピックによる振り分けが可能になる。
【００８７】
本実施形態では、外部データは、第１の外部データと第２の外部データとを含んでおり、暗号化処理部２１５は、第１の外部データを平文のままとし、第２の外部データを暗号化して、平文と暗号文とを含む暗号メッセージデータを生成可能である（図４参照）。これにより、本実施形態によれば、例えば、公開性を重視した平文の第１の外部データと、機密性を重視した暗号文の第２の外部データとを、暗号化パブリッシュメッセージＰＤ１としてまとめて外部装置に配信可能である。

【００８８】
本実施形態において、暗号化処理部２１５は、第１の外部データと第２の外部データとを、暗号ルールおよび暗号鍵の少なくとも一方が互いに異なる方法により暗号化して、暗号メッセージデータを生成してもよい。これにより、本実施形態によれば、互いに異なる暗号方法により暗号化された複数の外部データを、暗号化パブリッシュメッセージＰＤ１としてまとめて外部装置に配信可能である。
【００８９】
本実施形態では、暗号化判断部２１４によって暗号化条件が満たされると判断された場合（Ｓ１２０：ＹＥＳ）、暗号化処理部２１５は、暗号メッセージデータを生成し、データ配信部２１７は、暗号化パブリッシュメッセージＰＤ１をブローカ１００に配信し、暗号化条件が満たされないと判断された場合（Ｓ１２０：ＮＯ）、データ配信部２１７は、平文のトピック指定データと、平文のメッセージデータと、を含む非暗号化パブリッシュメッセージＰＤ２をブローカ１００に配信する。すなわち、本実施形態では、所定の暗号化条件が満たされるか否かに基づき、機密性を重視する暗号化パブリッシュメッセージをブローカに配信する機密配信形態（Ｓ１８０）と、公開性を重視する非暗号化パブリッシュメッセージをブローカに配信する公開配信形態（Ｓ１９０）とを使い分けることができる。これにより、本実施形態によれば、メッセージデータの機密性と公開性とを両立させたパブ・サブ・モデルを実現することが可能である。
【００９０】
パブリッシャ２００Ｐから配信される暗号化パブリッシュメッセージＰＤ１と非暗号化パブリッシュメッセージＰＤ２のトピック指定データには、パターン識別データが含まれている。このため、サブスクライバ２００Ｓでは、このパターン識別データに基づき、暗号化パブリッシュメッセージＰＤ１と非暗号化パブリッシュメッセージＰＤ２とのそれぞれにおける暗号文の配置パターンを識別できる（図６参照）。これにより、例えばパターン識別データをサブスクライバ２００Ｓに伝達する手段を別途要することなく、暗号文の配置パターンが随時変わり得るパブリッシュメッセージに対する処理をサブスクライバ２００Ｓに正常に行わせることができる。
【００９１】
本実施形態では、パブリッシャ２００Ｐ側で生成した暗号ルールおよび暗号鍵の少なくとも一方が、パブ・サブ・モデルに基づく通信によってサブスクライバ２００Ｓに配信される。これにより、ブローカ１００に制約されることなく、パブリッシャ２００Ｐ側で暗号ルールや暗号鍵を定めつつ、別の通信手段を要することなく、暗号ルールや暗号鍵をサブスクライバ２００Ｓに配信することができる。また、暗号化に関してブローカ１００の処理負担が増大することを抑制することができる。
【００９２】
本実施形態では、予め共通の区切り文字を把握している第１のサブスクライバ２００Ｓ１だけが、ブローカ１００から受信した暗号ルールパブリッシュメッセージＰＤ３から暗号ルールデータを取得することができる（図６参照）。これにより、特定のサブスクライバ２００Ｓへの暗号ルールデータの配信の機密性を向上させることができる。パブ・サブ・モデルに基づく通信は、トピックに登録した全てのサブスクライバ２００Ｓが、そのトピックのパブリッシュメッセージを購読可能なオープンな通信であるため、特に特定のサブスクライバ２００Ｓへの暗号ルールデータの配信の機密性は重要である。
【００９３】
本実施形態では、パブリッシャ２００Ｐ側で暗号ルールと暗号鍵と区切り文字との少なくとも１つが変更される（図５参照）。これにより、特定の外部装置への暗号ルールデータの配信の機密性を効果的に向上させることができる。
【００９４】
本実施形態では、変更に伴う処理負担が比較的に小さい区切り文字の変更頻度が、暗号ルールや暗号鍵の変更頻度よりも高い。このため、暗号ルールデータの変更に伴う処理負担を抑制しつつ、特定の外部装置への暗号ルールデータの配信の機密性を、より効果的に

向上させることができる。
【００９５】
Ｂ．変形例：
本明細書で開示される技術は、上述の実施形態に限られるものではなく、その要旨を逸脱しない範囲において種々の形態に変形することができ、例えば次のような変形も可能である。
【００９６】
上記実施形態における通信システム１０、ブローカ１００および端末装置２００の構成は、あくまで一例であり、種々変更可能である。例えば、上記実施形態では、通信システム１０は、複数のサブスクライバ２００Ｓを備える構成であったが、パブリッシャ２００Ｐとサブスクライバ２００Ｓとを１つずつを備える構成でもよい。端末装置２００は、表示部２５２と操作入力部２５６との少なくとも１つを備えない構成でもよい。また、ブローカ１００は、複数の情報処理装置を備え、これらの複数の情報処理装置が協働して上記メッセージ管理処理を実行する構成でもよい。
【００９７】
上記実施形態では、取得部２５４が複数種の外部データを同時期に取得可能な構成を例示したが、取得部２５４は、複数種の外部データを互いに異なる時期に取得可能な構成でもよいし、１種の外部データだけを取得可能な構成でもよいし、同種の複数の外部データ（例えば互いに検出位置が異なる複数の温度データなど）を取得可能な構成でもよい。
【００９８】
上記実施形態における各処理の内容は、あくまで一例であり、種々変形可能である。例えば、上記実施形態では、端末装置２００は、パブリッシャ２００Ｐとサブスクライバ２００Ｓとの両方として機能する汎用の装置であったが、パブリッシャ２００Ｐとサブスクライバ２００Ｓとのいずれか一方だけとして機能する専用の装置でもよい。
【００９９】
上記実施形態において、暗号化パブリッシュメッセージＰＤ１の暗号メッセージデータに含まれる１または複数の外部データの全てが暗号文であってもよい。また、パブリッシャ２００Ｐにて、パブリッシュメッセージの全体を公知の暗号化方式（例えばＴＬＳ（Ｔｒａｎｓｐｏｒｔ　Ｌａｙｅｒ　Ｓｅｃｕｒｉｔｙ）による標準の暗号化方式）によって暗号化してブローカ１００に配信してもよい。また、ブローカ１００にて、パブリッシュメッセージの全体を公知の暗号化方式によって暗号化してサブスクライバ２００Ｓに購読させてもよい。
【０１００】
暗号情報ＱＤは、復号化ルールと暗号鍵とのいずれか一方だけを含んでもよい。区切り文字ＷＤは、１文字の記号（例えばカンマや特殊記号）でもよいし、アルファベットと数字と記号との少なくとも２つの組み合わせを含む複数の文字からなる文字列でもよい。
【０１０１】
上記実施形態では、暗号変更処理（図５）において、復号化ルールと暗号鍵との両方を変更する例を説明したが、復号化ルールと暗号鍵とのいずれか一方だけを変更してもよい。また、上記実施形態では、暗号情報ＱＤと区切り文字ＷＤとの両方を変更する例を説明したが、暗号情報ＱＤと区切り文字ＷＤとのいずれか一方だけを変更してもよい。
【０１０２】
上記実施形態では、１つのトピックに対する処理を説明したが、複数のトピックのそれぞれについて、上記各処理を実行してもよい。例えば、パブリッシャ２００Ｐは、互いに異なる複数のトピックのそれぞれについて、ブローカ１００に対してメッセージの送信要求を行うとともに図４および図５の処理を個別に実行する構成でもよい。サブスクライバ２００Ｓは、互いに異なる複数のトピックのそれぞれについて、ブローカ１００に対してメッセージの購読要求を行うとともに図６の処理を個別に実行する構成でもよい。
【０１０３】
図４のパブリッシュ処理において、Ｓ１２０の処理を実行せずに、常にＳ１３０の処理

を実行してもよい。また、パブリッシュメッセージにおける暗号文の配置パターンが不変である場合、Ｓ１３０の処理はなくてもよい。また、図５の暗号変更処理を実行しなくてもよい。この場合、図６のサブスクライブ処理において、Ｓ３２０の処理を実行せずに、Ｓ３５０の処理を実行してもよい。

【０１０４】

また、上記各実施形態において、ハードウェアによって実現されている構成の一部をソフトウェアに置き換えるようにしてもよく、反対に、ソフトウェアによって実現されている構成の一部をハードウェアに置き換えるようにしてもよい。

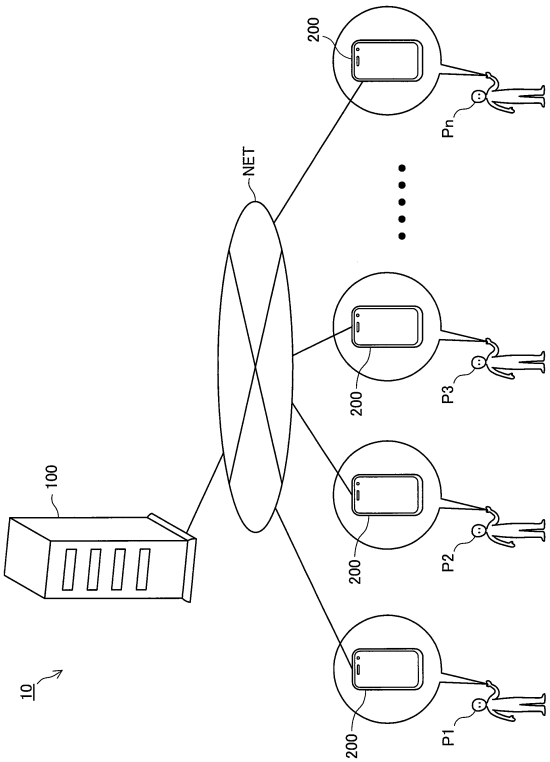
【符号の説明】

【０１０５】

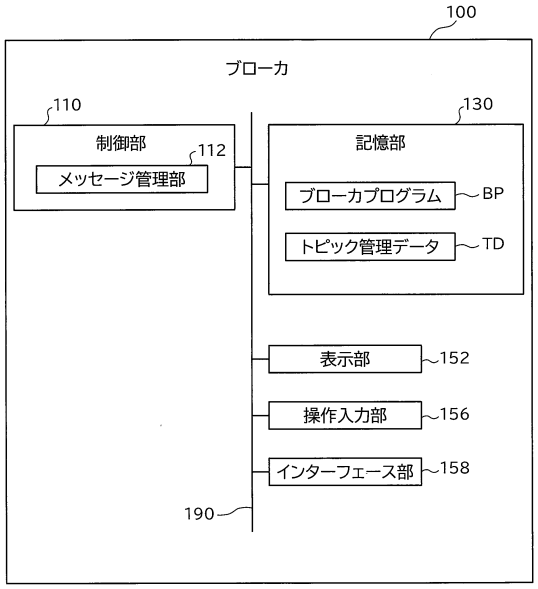
１０：通信システム　３５：緯度:　１００：ブローカ　１１０，２１０：制御部　１１２：メッセージ管理部　１３０，２３０：記憶部　１３９：６８１２３６　経度:　１５２，２５２：表示部　１５６，２５６：操作入力部　１５８，２５８：インターフェース部　１９０，２９０：バス　２００：端末装置　２００Ｐ：パブリッシャ　２００Ｓ１：第１のサブスクライバ　２００Ｓ２：第２のサブスクライバ　２００Ｓ：サブスクライバ　２１２：パブリッシュ処理部　２１３：配信条件判断部　２１４：暗号化判断部　２１５：暗号化処理部　２１６：トピック処理部　２１７：データ配信部　２１８：暗号変更判断部　２１９：暗号ルール生成部　２２２：サブスクライブ処理部　２２３：購読条件判断部　２２４：データ振り分け部　２２５：暗号取得部　２２６：復号化処理部　２５４：取得部　ＮＥＴ：通信ネットワーク　ＰＤ１：暗号化パブリッシュメッセージ　ＰＤ２：非暗号化パブリッシュメッセージ　ＰＤ３：暗号ルールパブリッシュメッセージ

【図面】

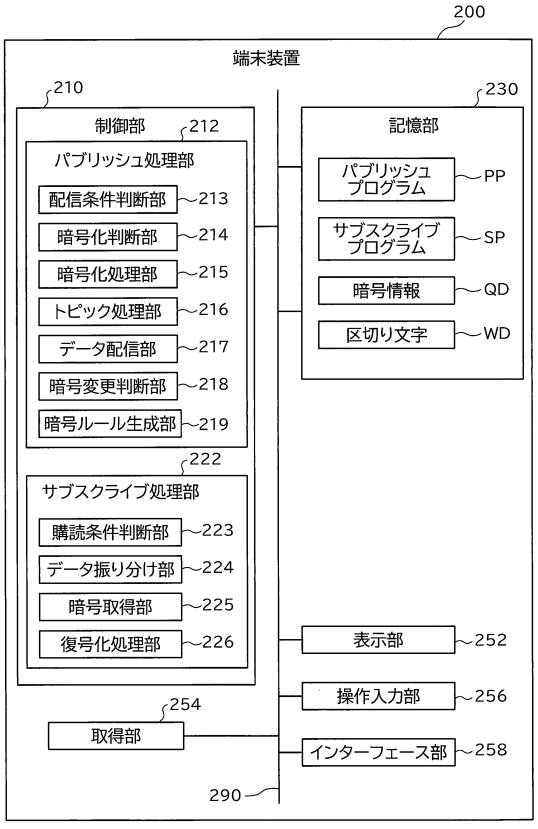
【図１】


200
Pn
NET
200
P3
100
200
P2
200
P1
10

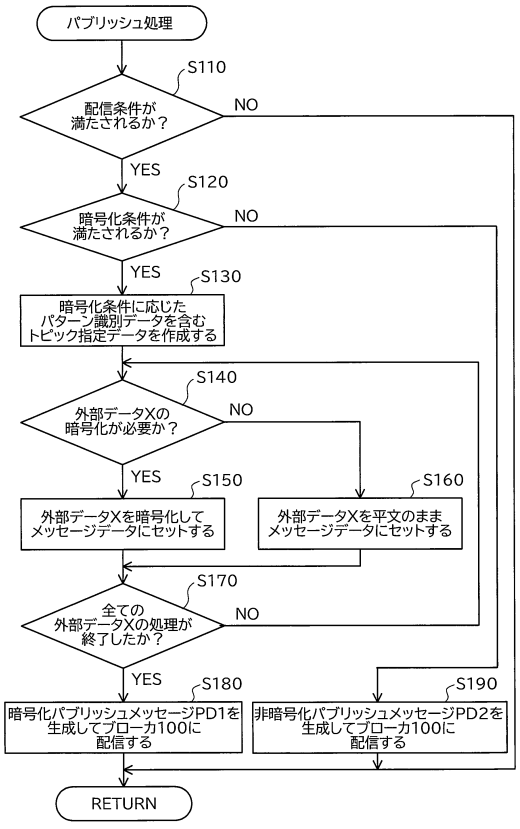
【図２】


100
ブローカ
110
制御部
112
メッセージ管理部
130
記憶部
ブローカプログラム
BP
トピック管理データ
TD
表示部
152
操作入力部
156
インターフェース部
158
190

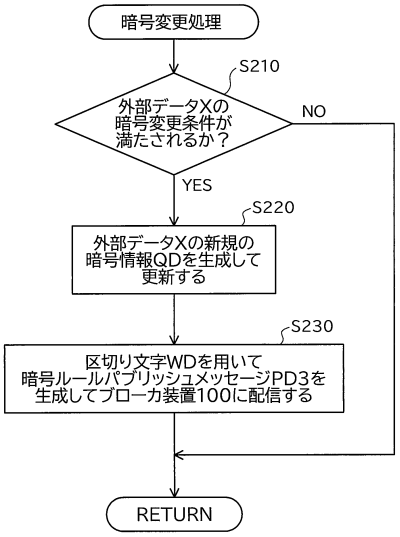
【図３】


200
端末装置
210
制御部
212
パブリッシュ処理部
配信条件判断部
213
暗号化判断部
214
暗号化処理部
215
トピック処理部
216
データ配信部
217
暗号変更判断部
218
暗号ルール生成部
219
222
サブスクライブ処理部
購読条件判断部
223
データ振り分け部
224
暗号取得部
225
復号化処理部
226
254
取得部
230
記憶部
パブリッシュプログラム
PP
サブスクライブプログラム
SP
暗号情報
QD
区切り文字
WD
表示部
252
操作入力部
256
インターフェース部
258
290

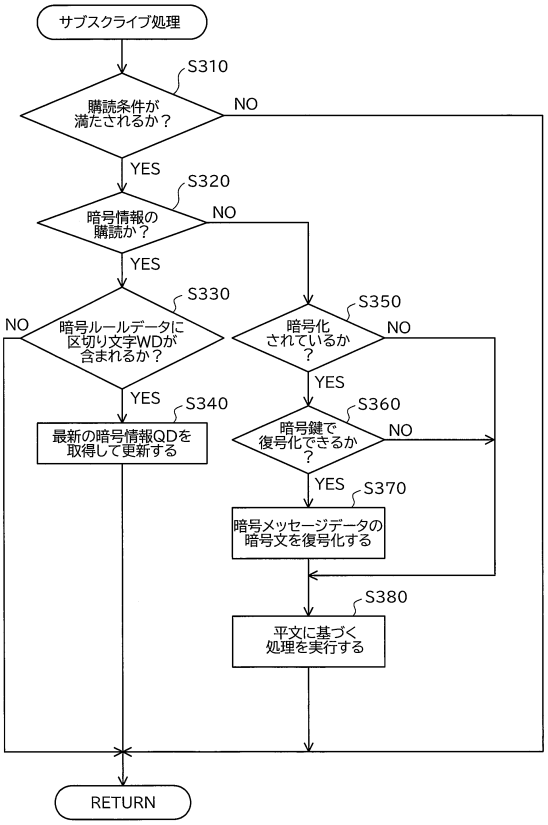
【図４】


パブリッシュ処理
S110
配信条件が満たされるか？
NO
YES
S120
暗号化条件が満たされるか？
NO
YES
S130
暗号化条件に応じたパターン識別データを含むトピック指定データを作成する
S140
外部データXの暗号化が必要か？
NO
YES
S150
外部データXを暗号化してメッセージデータにセットする
S160
外部データXを平文のままメッセージデータにセットする
S170
全ての外部データXの処理が終了したか？
NO
YES
S180
暗号化パブリッシュメッセージPD1を生成してブローカ100に配信する
S190
非暗号化パブリッシュメッセージPD2を生成してブローカ100に配信する
RETURN

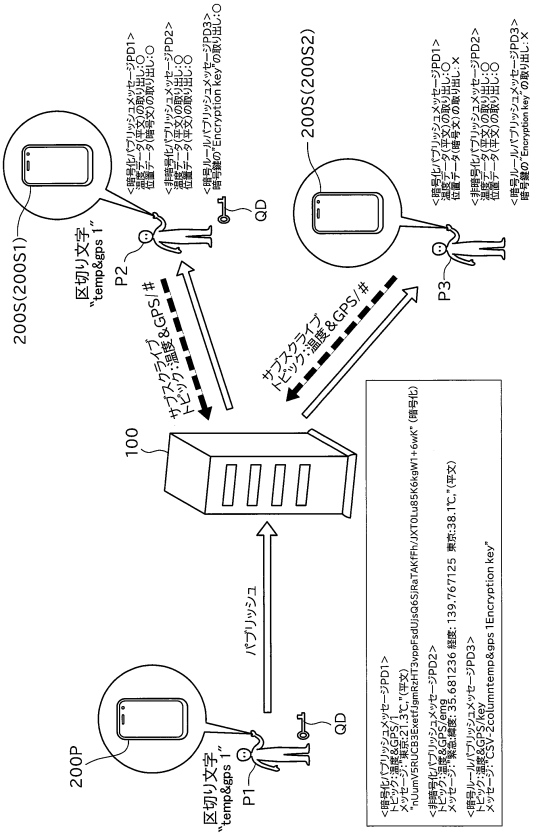
【図５】


暗号変更処理
S210
外部データXの
暗号変更条件が
満たされるか？
NO
YES
S220
外部データXの新規の
暗号情報QDを生成して
更新する
S230
区切り文字WDを用いて
暗号ルールパブリッシュメッセージPD3を
生成してブローカ装置100に配信する
RETURN

【図６】


サブスクライブ処理
S310
購読条件が
満たされるか？
NO
YES
S320
暗号情報の
購読か？
NO
YES
S330
暗号ルールデータに
区切り文字WDが
含まれるか？
NO
YES
S340
最新の暗号情報QDを
取得して更新する
S350
暗号化
されているか
？
NO
YES
S360
暗号鍵で
復号化できるか
？
NO
YES
S370
暗号メッセージデータの
暗号文を復号化する
S380
平文に基づく
処理を実行する
RETURN

【図７】


200S(200S1)
区切り文字
"temp&gps 1"
P2
QD
200S(200S2)
P3
サブスクライブ
トピック:温度&GPS/#
サブスクライブ
トピック:温度&GPS/#
100
パブリッシュ
200P
区切り文字
"temp&gps 1"
P1
QD

フロントページの続き

(56)参考文献　欧州特許出願公開第０３４２８８６５（ＥＰ，Ａ１）
特開２０１５－０４１３１９（ＪＰ，Ａ）
特開２００８－１６３６１２（ＪＰ，Ａ）
国際公開第２０１８／０９６６４１（WO，Ａ１）
特表２００８－５０３９５０（ＪＰ，Ａ）
米国特許出願公開第２００２／０１９９１２１（ＵＳ，Ａ１）

(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／６０
Ｈ０４Ｌ　　９／１４
Ｇ０６Ｆ　２１／６２