(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6574675号
(P6574675)

(45)発行日　令和1年9月11日(2019.9.11)　(24)登録日　令和1年8月23日(2019.8.23)

| (51)Int.Cl. | | F I | | |
|---|---|---|---|---|
| H04L 9/32 | (2006.01) | H04L | 9/00 | 675A |
| G06F 13/00 | (2006.01) | G06F | 13/00 | 540S |
| G06F 21/62 | (2013.01) | G06F | 13/00 | 540P |
| G06F 21/44 | (2013.01) | G06F | 21/62 | 318 |
| G09C 1/00 | (2006.01) | G06F | 21/44 | |

請求項の数 6　(全 16 頁)　最終頁に続く

(21)出願番号　特願2015-207066(P2015-207066)
(22)出願日　平成27年10月21日(2015.10.21)
(65)公開番号　特開2017-79421(P2017-79421A)
(43)公開日　平成29年4月27日(2017.4.27)
審査請求日　平成30年8月14日(2018.8.14)

(73)特許権者　000102728
株式会社エヌ・ティ・ティ・データ
東京都江東区豊洲三丁目３番３号
(74)代理人　110001634
特許業務法人　志賀国際特許事務所
(72)発明者　栗原　優樹
東京都江東区豊洲三丁目３番３号　株式会社エヌ・ティ・ティ・データ内

審査官　行田　悦資

最終頁に続く

(54)【発明の名称】情報配信システム、情報配信装置、情報配信方法、およびプログラム

(57)【特許請求の範囲】

【請求項１】

情報を配信する第１の装置と前記情報を受信する第２の装置とを有する情報配信システムであって、

前記第１の装置は、

前記第２の装置を認証するために用いられる認証用トークンと前記情報とを対応付けて記憶する記憶部と、

第１の暗号鍵を用いて前記認証用トークンが暗号化された第１の暗号化トークンを前記第２の装置へ送信する第１の通信部と、

前記第２の装置から送信された第２の暗号化トークンと前記記憶部に記憶された前記認証用トークンとに基づいて前記第２の装置を認証し、

前記第２の装置が認証された場合、前記第１の通信部に前記認証用トークンに対応付けられた前記情報を第２の装置へ配信させる認証部と、

を備え、

前記第２の装置は、

前記第１の通信部から送信された前記第１の暗号化トークンを前記第１の暗号鍵で復号し、前記第１の暗号鍵で復号した第１の復号トークンを第２の暗号鍵で再び暗号化する制御部と、

前記第２の暗号鍵で暗号化された前記第２の暗号化トークンを前記第１の装置へ送信する第２の通信部と、を備え、

前記第２の通信部が前記第１の通信部によって配信された前記情報を受信した場合、前記第２の通信部は、前記第２の暗号鍵と前記第１の暗号化トークンの一部分に基づいて前記第１の復号トークンが暗号化された第３の暗号化トークンを前記第１の通信部へ送信し、

前記第１の通信部が前記第３の暗号化トークンを受信した場合、前記認証部は、前記第３の暗号化トークンを前記第２の暗号鍵と前記第１の暗号化トークンの一部分に基づいて復号して得られる第２の復号トークンが前記記憶部に記憶された前記認証用トークンである場合、正常に前記第２の装置が前記情報を受信したものと判定する

ことを特徴とする情報配信システム。

【請求項２】

前記第１の通信部は、

前記情報をプッシュ配信するイベントが発生すると、最初に、前記第１の暗号鍵を用いて前記認証用トークンが暗号化された前記第１の暗号化トークンを前記第２の装置へ送信する

ことを特徴とする請求項１に記載の情報配信システム。

【請求項３】

前記第１の装置が前記情報をプッシュ配信することにより前記第２の装置を遠隔操作する遠隔操作システムである請求項１または２に記載の情報配信システム。

【請求項４】

情報を配信する情報配信装置と前記情報を受信する受信装置とを有する情報配信システムにおける前記情報配信装置であって、

前記受信装置を認証するために用いられる認証用トークンと前記情報とを対応付けて記憶する記憶部と、

第１の暗号鍵を用いて前記認証用トークンが暗号化された第１の暗号化トークンを前記受信装置へ送信する通信部と、

前記受信装置が送信する第２の暗号化トークンであって前記通信部から送信された前記第１の暗号化トークンを前記受信装置が前記第１の暗号鍵で復号し、前記第１の暗号鍵で復号した第１の復号トークンを前記受信装置が第２の暗号鍵で再び暗号化した第２の暗号化トークンと前記記憶部に記憶された前記認証用トークンとに基づいて、前記受信装置を認証し、

前記受信装置が認証された場合、前記通信部に前記認証用トークンに対応付けられた前記情報を前記受信装置へ配信させる認証部と、を備え、

前記受信装置が前記通信部によって配信された前記情報を受信した場合に、前記受信装置が送信する第３の暗号化トークンであって前記第２の暗号鍵と前記第１の暗号化トークンの一部分に基づいて前記受信装置により前記第１の復号トークンが暗号化された第３の暗号化トークンを前記通信部が受信した場合、前記認証部は、前記第３の暗号化トークンを前記第２の暗号鍵と前記第１の暗号化トークンの一部分に基づいて復号して得られる第２の復号トークンが前記記憶部に記憶された前記認証用トークンである場合、正常に前記受信装置が前記情報を受信したものと判定する

ことを特徴とする情報配信装置。

【請求項５】

情報を配信するコンピュータである第１の装置と前記情報を受信するコンピュータである第２の装置とを有する情報配信システムにおける情報配信方法であって、

前記第１の装置において、

記憶部が、前記第２の装置を認証するために用いられる認証用トークンと前記情報とを対応付けて記憶する記憶ステップと、

第１の通信部が、第１の暗号鍵を用いて前記認証用トークンが暗号化された第１の暗号化トークンを前記第２の装置へ送信する第１の通信ステップと、

認証部が、前記第２の装置から送信された第２の暗号化トークンを第２の暗号鍵を用いて復号し、前記第２の暗号鍵を用いて復号されたトークンと前記記憶部に記憶された前記

認証用トークンとが一致するか否かに基づいて前記第２の装置を認証し、
前記第２の装置が認証された場合、前記第１の通信部に前記認証用トークンに対応付けられた前記情報を前記第２の装置へ配信させる認証ステップと、
を有し、
前記第２の装置において、
制御部が、前記第１の通信部から送信された前記第１の暗号化トークンを前記第１の暗号鍵で復号し、前記第１の暗号鍵で復号した第１の復号トークンを前記第２の暗号鍵で再び暗号化する制御ステップと、
第２の通信部が、前記第２の暗号鍵で暗号化された前記第２の暗号化トークンを前記第１の装置へ送信する第２の通信ステップと、
前記第２の通信部が前記認証ステップによって配信された前記情報を受信した場合、前記第２の通信部が前記第２の暗号鍵と前記第１の暗号化トークンの一部分に基づいて前記第１の復号トークンが暗号化された第３の暗号化トークンを前記第１の装置へ送信するステップと、
を有し、
前記第１の装置において、
前記第１の通信部が前記第３の暗号化トークンを受信した場合、前記認証部が前記第３の暗号化トークンを前記第２の暗号鍵と前記第１の暗号化トークンの一部分に基づいて復号して得られる第２の復号トークンが前記記憶ステップにおいて記憶された前記認証用トークンである場合、正常に前記第２の装置が前記情報を受信したものと判定するステップ、
を有する、
ことを特徴とする情報配信方法。
【請求項６】
情報を配信するコンピュータである第１の装置に、
情報を受信するコンピュータである第２の装置を認証するために用いられる認証用トークンと前記情報とを対応付けて記憶する記憶ステップと、
第１の暗号鍵を用いて前記認証用トークンが暗号化された第１の暗号化トークンを前記第２の装置へ送信する第１の通信ステップと、
前記第２の装置から送信された第２の暗号化トークンと前記記憶ステップにおいて記憶された前記認証用トークンとに基づいて前記第２の装置を認証し、
前記第２の装置が認証された場合、前記認証用トークンに対応付けられた前記情報を第２の装置に配信する認証ステップと、
を実行させ、
前記第２の装置に、
前記第１の通信ステップにおいて送信された前記第１の暗号化トークンを前記第１の暗号鍵で復号し、前記第１の暗号鍵で復号した第１の復号トークンを第２の暗号鍵で再び暗号化する制御ステップと、
前記第２の暗号鍵で暗号化された前記第２の暗号化トークンを前記第１の装置へ送信する第２の通信ステップと、
前記認証ステップによって配信された前記情報を受信した場合、前記第２の暗号鍵と前記第１の暗号化トークンの一部分に基づいて前記第１の復号トークンが暗号化された第３の暗号化トークンを前記第１の装置へ送信するステップと、
を実行させ、
前記第１の装置に、
前記第３の暗号化トークンを受信した場合、前記第３の暗号化トークンを前記第２の暗号鍵と前記第１の暗号化トークンの一部分に基づいて復号して得られる第２の復号トークンが前記記憶ステップにおいて記憶された前記認証用トークンである場合、正常に前記第２の装置が前記情報を受信したものと判定するステップ
を実行させるためのプログラム。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、情報配信システム、情報配信装置、情報配信方法、およびプログラムに関する。
【背景技術】
【０００２】
スマートフォンなどの携帯型の情報端末の普及に伴い、サーバから情報端末へ効率的に情報を伝達するためのメッセージ送信方法であるプッシュ配信が広く利用されている。
例えば、特許文献１に記載のシステムは、コンテンツ配信における制御および対話のためにショートメッセージサービス（ＳＭＳ；Ｓｈｏｒｔ Ｍｅｓｓａｇｅ Ｓｅｒｖｉｃｅ）やマルチメディアメッセージサービス（ＭＭＳ；Ｍｕｌｔｉｍｅｄｉａ Ｍｅｓｓａｇｅ Ｓｅｒｖｉｃｅ）を用いる。
また、その他のプッシュ配信サービスとして、ＧＣＭ（Ｇｏｏｇｌｅ Ｃｌｏｕｄ Ｍｅｓｓａｇｉｎｇ）や、ＡＰＮＳ（Ａｐｐｌｅ Ｐｕｓｈ Ｎｏｔｉｆｉｃａｔｉｏｎ Ｓｅｒｖｉｃｅ）が知られている。これらのシステムを利用することによって、情報端末からの配信要求がなくても、情報端末に対する配信条件が成立した場合に、サーバから当該情報端末へプッシュ配信がなされるため、サーバから情報端末への情報伝達が効率化される。プッシュ通知の際に、ある一部の情報のみを情報端末へ送信し、受信した情報端末が、全ての情報をサーバから取得する技術も知られている。
【先行技術文献】
【特許文献】
【０００３】
【特許文献１】特表２０１１－５０９４４１号公報
【発明の概要】
【発明が解決しようとする課題】
【０００４】
しかしながら、従来のプッシュ配信サービスにおいては、情報端末において受信したプッシュ配信が正規のサーバから送信されたプッシュ配信であるかを、情報端末側で確認することができない。そのため、情報端末へ第三者による不正なプッシュ配信がなされた場合であっても、情報端末側ではそのプッシュ配信が不正なプッシュ配信であることを検知することができないという課題がある。
また、情報端末がプッシュ配信を受信して全ての情報をサーバから取得する場合に、サーバは、取得に来た情報端末が正規の情報端末であるか否かを確認することが出来ないという課題がある。
また、従来のプッシュ配信サービスにおいては、一度に送信することができるデータ量が制限（例えば、４キロバイト以内に制限）されていることがあり、データ量が多いコンテンツを送信できないことがあるという課題がある。
【０００５】
本発明は上記の点に鑑みてなされたものであり、安全かつ確実にデータの送受信をすることができる情報配信システム、情報配信装置、情報配信方法、およびプログラムを提供する。
【課題を解決するための手段】
【０００６】
（1）本発明は上記の課題を解決するためになされたものであり、本発明の一態様としては、情報を配信する第１の装置と前記情報を受信する第２の装置とを有する情報配信システムであって、前記第１の装置は、前記第２の装置を認証するために用いられる認証用トークンと前記情報とを対応付けて記憶する記憶部と、第１の暗号鍵を用いて前記認証用トークンが暗号化された第１の暗号化トークンを前記第２の装置へ送信する第１の通信部と、前記第２の装置から送信された第２の暗号化トークンと前記記憶部に記憶された前記認

証用トークンとに基づいて前記第２の装置を認証し、前記第２の装置が認証された場合、前記第１の通信部に前記認証用トークンに対応付けられた前記情報を第２の装置へ配信させる認証部と、を備え、前記第２の装置は、前記第１の通信部から送信された前記第１の暗号化トークンを前記第１の暗号鍵で復号し、前記第１の暗号鍵で復号した第１の復号トークンを第２の暗号鍵で再び暗号化する制御部と、前記第２の暗号鍵で暗号化された前記第２の暗号化トークンを前記第１の装置へ送信する第２の通信部と、を備え、前記第２の通信部が前記第１の通信部によって配信された前記情報を受信した場合、前記第２の通信部は、前記第２の暗号鍵と前記第１の暗号化トークンの一部分に基づいて前記第１の復号トークンが暗号化された第３の暗号化トークンを前記第１の通信部へ送信し、前記第１の通信部が前記第３の暗号化トークンを受信した場合、前記認証部は、前記第３の暗号化トークンを前記第２の暗号鍵と前記第１の暗号化トークンの一部分に基づいて復号して得られる第２の復号トークンが前記記憶部に記憶された前記認証用トークンである場合、正常に前記第２の装置が前記情報を受信したものと判定することを特徴とする情報配信システムである。

【０００７】

（２）また、本発明の一態様としては、前記第１の通信部は、前記情報をプッシュ配信するイベントが発生すると、最初に、前記第１の暗号鍵を用いて前記認証用トークンが暗号化された前記第１の暗号化トークンを前記第２の装置へ送信することを特徴とする（１）に記載の情報配信システムである。

（３）また、本発明の一態様としては、前記第１の装置が前記情報をプッシュ配信することにより前記第２の装置を遠隔操作する遠隔操作システムである（１）または（２）に記載の情報配信システムである。

【０００８】

（４）また、本発明の一態様としては、情報を配信する情報配信装置と前記情報を受信する受信装置とを有する情報配信システムにおける前記情報配信装置であって、前記受信装置を認証するために用いられる認証用トークンと前記情報とを対応付けて記憶する記憶部と、第１の暗号鍵を用いて前記認証用トークンが暗号化された第１の暗号化トークンを前記受信装置へ送信する通信部と、前記受信装置が送信する第２の暗号化トークンであって前記通信部から送信された前記第１の暗号化トークンを前記受信装置が前記第１の暗号鍵で復号し、前記第１の暗号鍵で復号した第１の復号トークンを前記受信装置が第２の暗号鍵で再び暗号化した第２の暗号化トークンと前記記憶部に記憶された前記認証用トークンとに基づいて、前記受信装置を認証し、前記受信装置が認証された場合、前記通信部に前記認証用トークンに対応付けられた前記情報を前記受信装置へ配信させる認証部と、を備え、前記受信装置が前記通信部によって配信された前記情報を受信した場合に、前記受信装置が送信する第３の暗号化トークンであって前記第２の暗号鍵と前記第１の暗号化トークンの一部分に基づいて前記受信装置により前記第１の復号トークンが暗号化された第３の暗号化トークンを前記通信部が受信した場合、前記認証部は、前記第３の暗号化トークンを前記第２の暗号鍵と前記第１の暗号化トークンの一部分に基づいて復号して得られる第２の復号トークンが前記記憶部に記憶された前記認証用トークンである場合、正常に前記受信装置が前記情報を受信したものと判定することを特徴とする情報配信装置である。

【０００９】

（５）また、本発明の一態様としては、情報を配信するコンピュータである第１の装置と前記情報を受信するコンピュータである第２の装置とを有する情報配信システムにおける情報配信方法であって、前記第１の装置において、記憶部が、前記第２の装置を認証するために用いられる認証用トークンと前記情報とを対応付けて記憶する記憶ステップと、第１の通信部が、第１の暗号鍵を用いて前記認証用トークンが暗号化された第１の暗号化トークンを前記第２の装置へ送信する第１の通信ステップと、認証部が、前記第２の装置から送信された第２の暗号化トークンを第２の暗号鍵を用いて復号し、前記第２の暗号鍵を用いて復号されたトークンと前記記憶部に記憶された前記認証用トークンとが一致するか否かに基づいて前記第２の装置を認証し、前記第２の装置が認証された場合、前記第１の

通信部に前記認証用トークンに対応付けられた前記情報を前記第２の装置へ配信させる認証ステップと、を有し、前記第２の装置において、制御部が、前記第１の通信部から送信された前記第１の暗号化トークンを前記第１の暗号鍵で復号し、前記第１の暗号鍵で復号した第１の復号トークンを前記第２の暗号鍵で再び暗号化する制御ステップと、第２の通信部が、前記第２の暗号鍵で暗号化された前記第２の暗号化トークンを前記第１の装置へ送信する第２の通信ステップと、前記第２の通信部が前記認証ステップによって配信された前記情報を受信した場合、前記第２の通信部が前記第２の暗号鍵と前記第１の暗号化トークンの一部分に基づいて前記第１の復号トークンが暗号化された第３の暗号化トークンを前記第１の装置へ送信するステップと、を有し、前記第１の装置において、前記第１の通信部が前記第３の暗号化トークンを受信した場合、前記認証部が前記第３の暗号化トークンを前記第２の暗号鍵と前記第１の暗号化トークンの一部分に基づいて復号して得られる第２の復号トークンが前記記憶ステップにおいて記憶された前記認証用トークンである場合、正常に前記第２の装置が前記情報を受信したものと判定するステップ、を有する、ことを特徴とする情報配信方法である。

【００１０】

（６）また、本発明の一態様としては、情報を配信するコンピュータである第１の装置に、情報を受信するコンピュータである第２の装置を認証するために用いられる認証用トークンと前記情報とを対応付けて記憶する記憶ステップと、第１の暗号鍵を用いて前記認証用トークンが暗号化された第１の暗号化トークンを前記第２の装置へ送信する第１の通信ステップと、前記第２の装置から送信された第２の暗号化トークンと前記記憶ステップにおいて記憶された前記認証用トークンとに基づいて前記第２の装置を認証し、前記第２の装置が認証された場合、前記認証用トークンに対応付けられた前記情報を第２の装置に配信する認証ステップと、を実行させ、前記第２の装置に、前記第１の通信ステップにおいて送信された前記第１の暗号化トークンを前記第１の暗号鍵で復号し、前記第１の暗号鍵で復号した第１の復号トークンを第２の暗号鍵で再び暗号化する制御ステップと、前記第２の暗号鍵で暗号化された前記第２の暗号化トークンを前記第１の装置へ送信する第２の通信ステップと、前記認証ステップによって配信された前記情報を受信した場合、前記第２の暗号鍵と前記第１の暗号化トークンの一部分に基づいて前記第１の復号トークンが暗号化された第３の暗号化トークンを前記第１の装置へ送信するステップと、を実行させ、前記第１の装置に、前記第３の暗号化トークンを受信した場合、前記第３の暗号化トークンを前記第２の暗号鍵と前記第１の暗号化トークンの一部分に基づいて復号して得られる第２の復号トークンが前記記憶ステップにおいて記憶された前記認証用トークンである場合、正常に前記第２の装置が前記情報を受信したものと判定するステップを実行させるためのプログラムである。

【発明の効果】

【００１１】

本発明によれば、安全かつ確実にデータの送受信をすることができる。

【図面の簡単な説明】

【００１２】

【図１】本実施形態に係る情報配信システムの構成を示すブロック図である。

【図２】本実施形態に係る情報配信システムにおける情報配信装置の機能構成を示すブロック図である。

【図３】本実施形態に係る情報配信システムにおける端末装置の機能構成を示すブロック図である。

【図４】本実施形態に係る情報配信システムの初期設定時の動作を示すシーケンス図である。

【図５】本実施形態に係る情報配信システムのプッシュ配信時の認証動作を示すシーケンス図である。

【図６】本実施形態に係る情報配信システムにおけるサービス管理テーブルの構成を示す概略図である。

【図７】本実施形態に係る情報配信システムにおける暗号化処理および復号処理の一例を示す概略図である。
【図８】本実施形態に係る情報配信システムにおける暗号化処理および復号処理の一例を示す概略図である。
【図９】本実施形態に係る情報配信システムにおける端末装置から情報配信装置へ送信される応答メッセージの送受信処理の一例を示す概略図である。
【発明を実施するための形態】
【００１３】
（実施形態）
以下、本発明に係る実施形態について、図面を参照しながら説明する。
図１は、本実施形態に係る情報配信システム１の構成を示すブロック図である。
情報配信システム１は、情報配信装置１０と、端末装置２０と、プッシュ配信サーバ３０と、を含んで構成される。
【００１４】
情報配信装置１０（第１の装置）は、プッシュ配信サーバ３０を介して端末装置２０へ、各種のサービスをプッシュ配信（送信）するサーバ装置である。また、情報配信装置１０は、プッシュ配信サーバ３０を介して端末装置２０の認証処理を行う。情報配信装置１０は、例えば、汎用コンピュータ、またはパーソナルコンピュータなどを含んで構成される。
なお、以下の説明において、プッシュ配信とは、情報配信装置１０から特定の端末装置２０へサービスが送信されることをいう。
【００１５】
なお、情報配信装置１０によって提供されるサービスとは、例えば、プッシュ配信による遠隔操作によって端末装置２０にロックを掛ける「リモートロック」サービス、プッシュ配信による遠隔操作によって端末装置２０に記憶されたデータを消去する「リモートワイプ」サービス、プッシュ配信によって端末装置２０へデータを送信するサービス、情報配信装置１０に記憶されたデータのうち特定のデータを端末装置２０側から取得させるサービス、および緊急時などにおいて端末装置２０のシステムログデータを情報配信装置１０へ送信させるサービスなどである。
【００１６】
情報配信装置１０とプッシュ配信サーバ３０とは、通信ネットワークによって接続される。通信ネットワークとは、例えば、専用線、またはインターネットなどを含んで構成される。また、通信ネットワークは、無線通信ネットワーク、有線通信ネットワーク、または無線と有線の両方が用いられた通信ネットワークのいずれでもよい。また、通信ネットワークには、無線通信基地局などの中継装置が含まれていても構わない。
【００１７】
端末装置２０（第２の装置）は、プッシュ配信サーバ３０を介して情報配信装置１０からのプッシュ配信によってサービスの提供を受ける端末装置である。また、端末装置２０は、プッシュ配信サーバ３０を介して情報配信装置１０の認証処理を行う端末装置である。端末装置２０は、例えば、スマートフォン、またはパーソナルコンピュータなどを含んで構成される。
端末装置２０とプッシュ配信サーバ３０とは、通信ネットワークによって接続される。
【００１８】
プッシュ配信サーバ３０は、情報配信装置１０から指定された端末装置２０へ、情報配信装置から提供されるサービスをプッシュ配信するサーバ装置である。プッシュ配信サーバ３０は、例えば、汎用コンピュータなどを含んで構成される。
なお、プッシュ配信サーバ３０によって提供されるプッシュ配信サービスの一例としてとして、ＧＣＭ（Ｇｏｏｇｌｅ　Ｃｌｏｕｄ　Ｍｅｓｓａｇｉｎｇ）や、ＡＰＮＳ（Ａｐｐｌｅ　Ｐｕｓｈ　Ｎｏｔｉｆｉｃａｔｉｏｎｓ）がある。
【００１９】

なお、本実施形態においては、情報配信装置１０から端末装置２０へプッシュ配信サービスを提供するものとしたが、端末装置２０から情報配信装置１０へプッシュ配信を行うような構成であってもかまわない。または、情報配信装置１０と端末装置２０とにおいて、相互にプッシュ配信が行われるような構成であってもかまわない。

【００２０】

（情報配信装置の構成）

次に、本実施形態に係る情報配信装置１０の機能構成について説明する。

図２は、本実施形態に係る情報配信システム１における情報配信装置１０の機能構成を示すブロック図である。

情報配信装置１０は、制御部１００と、通信部１０１と、認証部１０２と、乱数生成部１０３と、一時記憶部１０４と、記憶部１０５と、を含んで構成される。

【００２１】

制御部１００は、情報配信装置１０の各種の処理を制御する。制御部１００は、例えば、ＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ；中央処理装置）を含んで構成される。通信部１０１（第１の通信部）は、プッシュ配信サーバ３０と通信接続するための通信インターフェースである。

【００２２】

認証部１０２は、自らの情報配信装置１０と端末装置２０との間の認証を行うための各種の処理を行う。なお、情報配信装置１０が通信部１０１を介して外部機器と通信を行う場合において、認証部１０２は、外部機器と、情報配信装置１０の制御部１００、乱数生成部１０３、一時記憶部１０４、および記憶部１０５との間を隔てるＤＭＺ（ｄｅｍｉｌｉｔａｒｉｚｅｄ　ｚｏｎｅ；非武装地帯）としての役割を果たす。これにより、第三者による、制御部１００、乱数生成部１０３、一時記憶部１０４、および記憶部１０５への不正なアクセスを防ぐ。

【００２３】

乱数生成部１０３は、各種の暗号鍵を生成するための乱数を生成する。

一時記憶部１０４は、生成した暗号鍵などを一時的に記憶する。一時記憶部１０４は記憶媒体、例えば、ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　ｒｅａｄ／ｗｒｉｔｅ　Ｍｅｍｏｒｙ；読み書き可能なメモリ）を含んで構成される。

記憶部１０５は、生成した暗号鍵などを記憶する。記憶部１０５は記憶媒体、例えば、ハードディスクドライブ（ＨＤＤ；Ｈａｒｄ　Ｄｉｓｋ　Ｄｒｉｖｅ）を含んで構成される。

【００２４】

（端末装置の構成）

次に、本実施形態に係る端末装置２０の機能構成について説明する。

図３は、本実施形態に係る情報配信システム１における端末装置２０の機能構成を示すブロック図である。

端末装置２０は、制御部２００と、通信部２０１と、乱数生成部２０３と、一時記憶部２０４と、記憶部２０５と、を含んで構成される。

【００２５】

制御部２００は、端末装置２０の各種の処理を制御する。制御部２００は、例えば、ＣＰＵを含んで構成される。

通信部２０１（第２の通信部）は、プッシュ配信サーバ３０と通信接続するための通信インターフェースである。

乱数生成部２０３は、各種の暗号鍵を生成するための乱数を生成する。

【００２６】

一時記憶部２０４は、生成した暗号鍵などを一時的に記憶する。一時記憶部２０４は記憶媒体、例えば、ＲＡＭを含んで構成される。

記憶部２０５は、生成した暗号鍵などを記憶する。記憶部２０５は記憶媒体、例えば、ＨＤＤを含んで構成される。

【００２７】
（情報配信システムの動作）
まず、本実施形態に係る情報配信システム１の初期設定時（アクティベーション時）の動作について説明する。
図４は、本実施形態に係る情報配信システム１の初期設定時の動作を示すシーケンス図である。
情報配信システム１の初期設定時において、まず、情報配信装置１０の制御部１００は、乱数生成部１０３によって生成される乱数に基づくトークン鍵（第２の暗号鍵）と、乱数生成部１０３によって生成される乱数に基づくメッセージ鍵（第１の暗号鍵）と、を生成する（図４、Ｓ００１）。なお、トークン鍵およびメッセージ鍵とは、いずれもデータを暗号化したり、暗号化されたデータを復号したりする際に用いられる暗号鍵である。
制御部１００は、生成したトークン鍵およびメッセージ鍵を、一時記憶部１０４に記憶させる（図４、Ｓ００２）。
【００２８】
また、制御部１００は、生成したトークン鍵およびメッセージ鍵を示すデータを、通信部１０１およびプッシュ配信サーバ３０を介して、端末装置２０の通信部２０１へ送信する（図４、Ｓ００３）。
端末装置２０の制御部２００は、通信部２０１が受信したトークン鍵およびメッセージ鍵を示すデータを、一時記憶部２０４に記憶させる（図４、Ｓ００４）。
以上の処理により、同一のトークン鍵および同一のメッセージ鍵が、情報配信装置１０と端末装置２０のそれぞれに記憶される。
【００２９】
次に、本実施形態に係る情報配信システム１のプッシュ配信時の認証動作について説明する。
図５は、本実施形態に係る情報配信システム１のプッシュ配信時の認証動作を示すシーケンス図である。
情報配信装置１０がプッシュ配信サーバ３０を介して端末装置２０へプッシュ配信を行う（サービスを提供する）際には、まず情報配信装置１０と端末装置２０の間で相互に認証処理が行われる。認証処理は、以下のように行われる。
【００３０】
情報配信装置１０において、端末装置２０へサービスをプッシュ配信するイベントが発生すると、まず情報配信装置１０の制御部１００は、乱数生成部１０３によって生成される乱数に基づくｎｏｎｃｅ（ｎｕｍｂｅｒ　ｕｓｅｄ　ｏｎｃｅ；ノンス）を生成する。ｎｏｎｃｅとは、ワンタイムトークンとも呼ばれ、１回だけ使われる使い捨てのランダムな値である。
制御部１００は、生成したｎｏｎｃｅ（トークン）を、一時記憶部１０４に記憶されたメッセージ鍵によって暗号化し、暗号化されたｎｏｎｃｅ（第１の暗号化トークン）を生成する（図５、Ｓ１０１）。
制御部１００は、ｎｏｎｃｅを示すデータと、プッシュ配信するサービスを示すデータとを対応付けて、一時記憶部１０４に格納されたサービス管理テーブルに記憶させる（図５、Ｓ１０２）。
【００３１】
上記のサービス管理テーブルについて、図面を参照しながら更に詳細に説明する。
図６は、本実施形態に係る情報配信システム１におけるサービス管理テーブルの構成を示す概略図である。
図示するように、サービス管理テーブルは、「ｎｏｎｃｅ」および「サービス」の２つの項目の列を含む二次元の表形式のデータである。「ｎｏｎｃｅ」の項目の値には、ｎｏｎｃｅの値が格納される。また、「サービス」の項目の値には、プッシュ配信されるサービスの内容を示すデータが格納される。
【００３２】

例えば、図６に例示するサービス管理テーブルにおける１行目のデータ行には、「Ａｇ６４１ｈ２・・・」および「リモートロック」という値が格納されている。これは、「Ａｇ６４１ｈ２・・・」というｎｏｎｃｅの値に対して、「リモートロック」というサービスが対応付けられていることを示す。同様に、図６に例示するサービス管理テーブルにおける２行目のデータ行には、「４Ａ７Ｅ８９４・・・」および「リモートワイプ」という値が格納されている。これは、「４Ａ７Ｅ８９４・・・」というｎｏｎｃｅの値に対して、「リモートワイプ」というサービスが対応付けられていることを示す。

【００３３】

なお、「リモートロック」とは、プッシュ配信による遠隔操作によって端末装置２０にロックを掛けることにより、例えば、盗難された端末装置２０を第三者に使用されることがないようにするためのサービスである。

なお、「リモートワイプ」とは、プッシュ配信による遠隔操作によって端末装置２０に記憶されたデータを消去することにより、例えば、盗難された端末装置２０に記憶されたデータを第三者によって参照されることがないようにするためのサービスである。

【００３４】

再び、図５のシーケンス図に戻って説明する。

制御部１００は、暗号化したｎｏｎｃｅを示すデータを、通信部１０１およびプッシュ配信サーバ３０を介して、端末装置２０の通信部２０１へ送信する（図５、Ｓ１０３）。

端末装置２０の制御部２００は、暗号化されたｎｏｎｃｅを示すデータを、通信部２０１によって受信する。制御部２００は、受信したｎｏｎｃｅを示すデータを、一時記憶部２０４に記憶されたメッセージ鍵によって復号する。

【００３５】

上記の、情報配信装置１０の制御部１００による暗号化処理と、端末装置２０の制御部２００による復号処理とについて、図面を参照しながら更に詳細に説明する。

図７は、本実施形態に係る情報配信システム１における暗号化処理および復号処理の一例を示す概略図である。

まず、情報配信装置１０の制御部１００は、乱数生成部１０３によって生成される乱数に基づく初期化ベクトルであるＩＶ１を生成する。

図示するように、情報配信装置１０（制御部１００）は、メッセージ鍵と、ＩＶ１とを用いて、ｎｏｎｃｅを暗号化する。そして情報配信装置１０は、暗号化されたｎｏｎｃｅであるｎｏｎｃｅ１と、ＩＶ１とをプッシュ配信サーバ３０を介して端末装置２０へ送信する。

【００３６】

なお、初期化ベクトル（ＩＶ；Ｉｎｉｔｉａｌｉｚａｔｉｏｎ　Ｖｅｃｔｏｒ）とは、暗号化の処理において毎回異なる初期値を与えるために用いられるランダムな値であり、送信する暗号化データ（例えば、当該初期化ベクトルを用いて暗号化されたｎｏｎｃｅ）とともに初期化ベクトルが送信されたとしても、暗号化データにおける暗号のセキュリティ強度が損なわれることはない。

【００３７】

端末装置２０（制御部２００）は、一時記憶部２０４に記憶されたメッセージ鍵と、受信したＩＶ１とを用いて、受信したｎｏｎｃｅ１を復号する。これにより、端末装置２０は、復号されたｎｏｎｃｅを得る。

【００３８】

再び、図５のシーケンス図に戻って説明する。

端末装置２０の制御部２００は、上記において復号したｎｏｎｃｅを、一時記憶部２０４に記憶されたトークン鍵を用いて暗号化し、暗号化されたｎｏｎｃｅ（第２の暗号化トークン）を生成する（図５、Ｓ１０４）。

すなわち、制御部２００は、情報配信装置１０からプッシュ配信サーバ３０および通信部２０１を介して受信した暗号化されたｎｏｎｃｅをメッセージ鍵によって復号し、次に、制御部２００は、復号したｎｏｎｃｅをトークン鍵によって再び暗号化する。

制御部２００は、暗号化したｎｏｎｃｅを、通信部２０１およびプッシュ配信サーバ３０を介して情報配信装置１０の通信部１０１へ送信する（図５、Ｓ１０５）。

【００３９】

情報配信装置１０の通信部１０１は、暗号化されたｎｏｎｃｅを示すデータを受信する。情報配信装置１０の認証部１０２は、通信部１０１が受信したｎｏｎｃｅを示すデータを、一時記憶部２０４に記憶されたトークン鍵によって復号する（図５、Ｓ１０６）。

【００４０】

上記の、端末装置２０の制御部２００による暗号化処理と、情報配信装置１０の認証部１０２による復号処理とについて、図面を参照しながら更に詳細に説明する。

図８は、本実施形態に係る情報配信システム１における暗号化処理および復号処理の一例を示す概略図である。

まず、端末装置２０の制御部２００は、乱数生成部２０３によって生成される乱数に基づく初期化ベクトルであるＩＶ２を生成する。

図示するように、端末装置２０（制御部２００）は、トークン鍵と、ＩＶ２とを用いて、ｎｏｎｃｅを暗号化する。そして端末装置２０は、暗号化したｎｏｎｃｅであるｎｏｎｃｅ２と、ＩＶ２とをプッシュ配信サーバ３０を介して情報配信装置１０へ送信する。

【００４１】

情報配信装置１０（認証部１０２）は、一時記憶部１０４に記憶されたトークン鍵と、受信したＩＶ２とを用いて、受信したｎｏｎｃｅ２を復号する。これにより、情報配信装置１０は、復号されたｎｏｎｃｅを得る。

【００４２】

再び、図５のシーケンス図に戻って説明する。

情報配信装置１０の認証部１０２は、復号したｎｏｎｃｅの値と、一時記憶部１０４に記憶されたｎｏｎｃｅの値とが一致しているか否かの照合を行う。認証部１０２は、復号したｎｏｎｃｅの値と一時記憶部１０４に記憶されたｎｏｎｃｅの値とが同一であった場合、情報配信装置１０と端末装置２０の間の認証が成功したものと判定する。

【００４３】

すなわち、情報配信装置１０が記憶するメッセージ鍵と同一のメッセージ鍵、および情報配信装置１０が記憶するトークン鍵と同一のトークン鍵を記憶している端末装置２０でなければ、当該メッセージ鍵で暗号化されたｎｏｎｃｅを復号して再び当該トークン鍵で暗号化することはできない。そのため、情報配信装置１０の認証部１０２は、認証が成功したものと判定する。

【００４４】

なお、上記においては、認証部１０２は、復号したｎｏｎｃｅの値と一時記憶部１０４に記憶されたｎｏｎｃｅの値とを照合したが、照合の方法はこれに限られない。例えば、認証部１０２は、一時記憶部１０４に記憶されたトークン鍵と受信したＩＶ２とを用いて一時記憶部１０４に記憶されたｎｏｎｃｅを暗号化し、当該暗号化したｎｏｎｃｅの値と受信したｎｏｎｃｅの値とを照合してもよい。

【００４５】

そして、認証が成功したものと判定された場合、制御部１００は、認証部１０２によって復号されたｎｏｎｃｅに対応するサービスを示すデータを一時記憶部１０４から取得する（図５、Ｓ１０７）。

制御部１００は、通信部１０１およびプッシュ配信サーバ３０を介して、端末装置２０の通信部２０１へ、一時記憶部１０４から取得したサービスを示すデータをプッシュ配信する（図５、Ｓ１０８）。

【００４６】

端末装置２０の制御部２００は、通信部２０１が受信したデータに基づくサービスを実行処理する。サービスとは、上述したように、例えば、システムのロックや、データの消去、およびプッシュ情報の表示などである。

また、制御部２００は、サービスを正常に受信したことを示す応答メッセージを生成す

る（図５、Ｓ１０９）。制御部２００は、通信部２０１およびプッシュ配信サーバ３０を介して、情報配信装置１０の通信部１０１へ、当該応答メッセージを示すデータを送信する（図５、Ｓ１１０）。

情報配信装置１０の認証部１０２は、通信部１０１が受信したデータを、一時記憶部１０４に格納されたトークン鍵を用いて復号する（図５、Ｓ１１１）。

【００４７】

上記の、端末装置２０から情報配信装置１０への応答メッセージの送受信における処理ついて、図面を参照しながら更に詳細に説明する。

図９は、本実施形態に係る情報配信システム１における端末装置２０から情報配信装置１０へ送信される応答メッセージの送受信処理の一例を示す概略図である。

【００４８】

端末装置２０から情報配信装置１０へ応答メッセージを送信するイベントが発生した場合、まず、端末装置２０の制御部２００は、初期化ベクトルであるＩＶ３を生成する。

図示するように、本実施形態においては、ＩＶ３は、上記において情報配信装置１０からプッシュ配信サーバ３０を介して端末装置２０へ送信されたｎｏｎｃｅ１の一部分のデータ（断片）である。ＩＶ３は、例えば、ｎｏｎｃｅ１を構成するビット列の後半半分のビット列である。

端末装置２０（制御部２００）は、トークン鍵と、ＩＶ３とを用いて、ｎｏｎｃｅを暗号化し、暗号化されたｎｏｎｃｅ（第３の暗号化トークン）を生成する。そして端末装置２０は、暗号化されたｎｏｎｃｅであるｎｏｎｃｅ３を、プッシュ配信サーバ３０を介して情報配信装置１０へ送信する。

【００４９】

情報配信装置１０（認証部１０２）は、一時記憶部１０４に記憶されたトークン鍵と、一時記憶部１０４に記憶されたｎｏｎｃｅ１の一部分のデータとを用いて、受信したｎｏｎｃｅ３を復号する。これにより、情報配信装置１０は、復号されたｎｏｎｃｅを得る。なお、ｎｏｎｃｅ１の値からＩＶ３を生成する方法については、予め、情報配信装置１０と端末装置２０との間で共通の認識が図られているものとする。

【００５０】

再び、図５のシーケンス図に戻って説明する。

情報配信装置１０の認証部１０２は、復号したｎｏｎｃｅの値を得ることにより、応答メッセージを受信したものと判定する。すなわち、認証部１０２は、サービスを示すデータが正常に端末装置２０によって受信されたものと判定する。

認証部１０２は、サービスを示すデータが正常に端末装置２０によって受信されたものと判定した場合、応答メッセージを示すデータを制御部１００へ出力する。

【００５１】

制御部１００は、認証部１０２から入力されたデータに基づいて、応答メッセージ（すなわち、サービスを提供した結果）を示すデータを記憶部１０５へ格納する。

また、制御部１００は、応答メッセージを取得した場合、当該応答メッセージに対応するプッシュ配信に用いられたｎｏｎｃｅを示すデータおよびサービスを示すデータを、一時記憶部１０４から削除する。

【００５２】

以上、説明したように、本実施形態に係る情報配信システム１では、端末装置２０が受信したプッシュ配信が、正規の情報配信装置１０から送信されたプッシュ配信であるか否かを、ｎｏｎｃｅを復号できるか否かに基づいて、端末装置２０側で判定をすることができる。

また、本実施形態に係る情報配信システム１では、情報配信装置１０から送信されたプッシュ配信が端末装置２０において正常に受信されたか否かを、応答メッセージを復号できるか否かに基づいて、情報配信装置１０側で判定をすることができる。

また、本実施形態に係る情報配信システム１では、一度に送信することができるデータ量に制限されることがなく、データ量が多いコンテンツも送信することができる。

以上により、本実施形態に係る情報配信システム１は、安全かつ確実にデータの送受信をすることができる。

【００５３】

以上、この発明の実施形態について詳しく説明してきたが、具体的な構成は上述のものに限られることはなく、この発明の要旨を逸脱しない範囲内において様々な設計変更等をすることが可能である。

【００５４】

なお、上述した実施形態における情報配信装置１０および端末装置２０の一部又は全部をコンピュータで実現するようにしてもよい。その場合、この制御機能を実現するためのプログラムをコンピュータ読み取り可能な記録媒体に記録して、この記録媒体に記録されたプログラムをコンピュータシステムに読み込ませ、実行することによって実現してもよい。

【００５５】

なお、ここでいう「コンピュータシステム」とは、情報配信装置１０および端末装置２０に内蔵されたコンピュータシステムであって、ＯＳや周辺機器等のハードウェアを含むものとする。また、「コンピュータ読み取り可能な記録媒体」とは、フレキシブルディスク、光磁気ディスク、ＲＯＭ、ＣＤ－ＲＯＭ等の可搬媒体、コンピュータシステムに内蔵されるハードディスク等の記憶装置のことをいう。

【００５６】

さらに「コンピュータ読み取り可能な記録媒体」とは、インターネット等のネットワークや電話回線等の通信回線を介してプログラムを送信する場合の通信回線のように、短時間、動的にプログラムを保持するもの、その場合のサーバやクライアントとなるコンピュータシステム内部の揮発性メモリのように、一定時間プログラムを保持しているものも含んでもよい。また上記プログラムは、前述した機能の一部を実現するためのものであっても良く、さらに前述した機能をコンピュータシステムにすでに記録されているプログラムとの組み合わせで実現できるものであってもよい。

【００５７】

また、上述した実施形態における情報配信装置１０および端末装置２０を、ＬＳＩ（Ｌａｒｇｅ　Ｓｃａｌｅ　Ｉｎｔｅｇｒａｔｉｏｎ）等の集積回路として実現してもよい。情報配信装置１０および端末装置２０の各機能ブロックは個別にプロセッサ化してもよいし、一部、または全部を集積してプロセッサ化してもよい。また、集積回路化の手法はＬＳＩに限らず専用回路、または汎用プロセッサで実現してもよい。また、半導体技術の進歩によりＬＳＩに代替する集積回路化の技術が出現した場合、当該技術による集積回路を用いてもよい。

【符号の説明】

【００５８】

１・・・情報配信システム、１０・・・情報配信装置、２０・・・端末装置、３０・・・プッシュ配信サーバ、１００・・・制御部、１０１・・・通信部、１０２・・・認証部、１０３・・・乱数生成部、１０４・・・一時記憶部、１０５・・・記憶部、２００・・・制御部、２０１・・・通信部、２０３・・・乱数生成部、２０４・・・一時記憶部、２０５・・・記憶部

【図１】

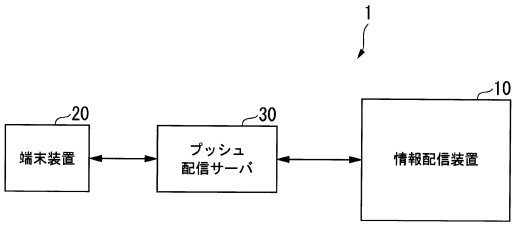


図1

【図２】

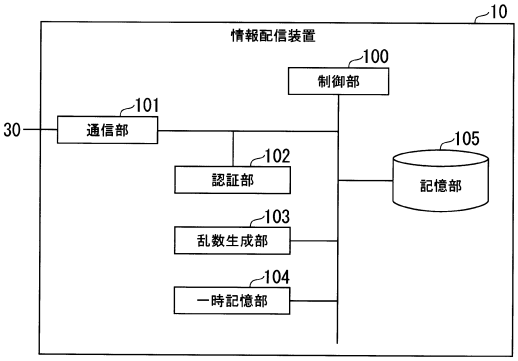


図2

【図３】

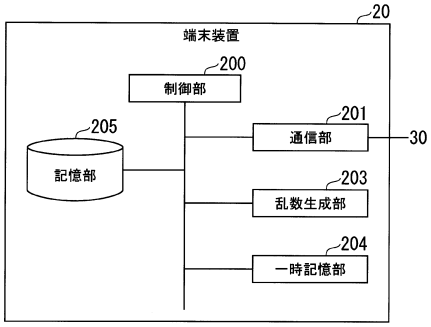


図3

【図４】

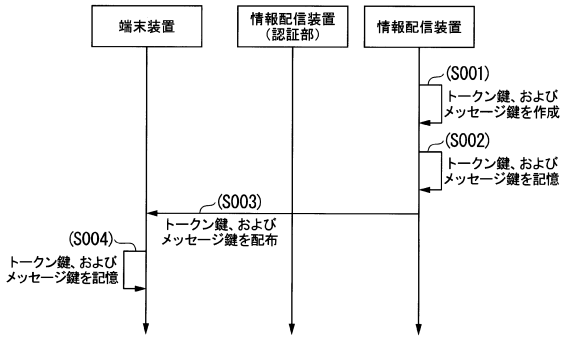


図4

【図５】

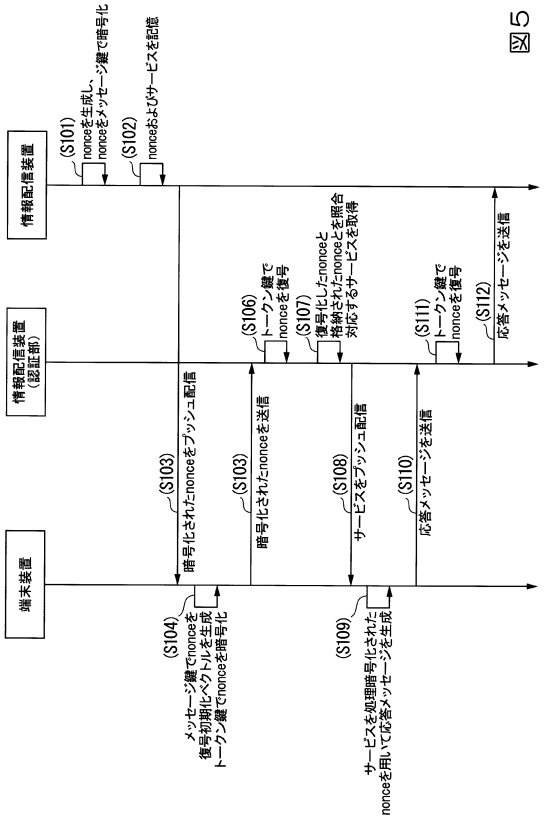


図5

【図６】

| nonce | サービス |
|---|---|
| Ag641h2… | リモートロック |
| 4A7E894… | リモートワイプ |
| ・・・ | ・・・ |

図6

【図７】

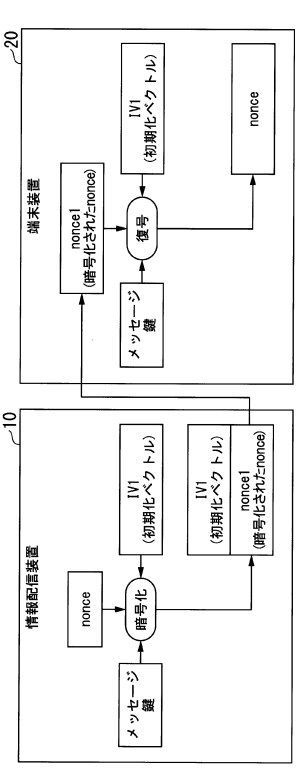


図７

【図８】

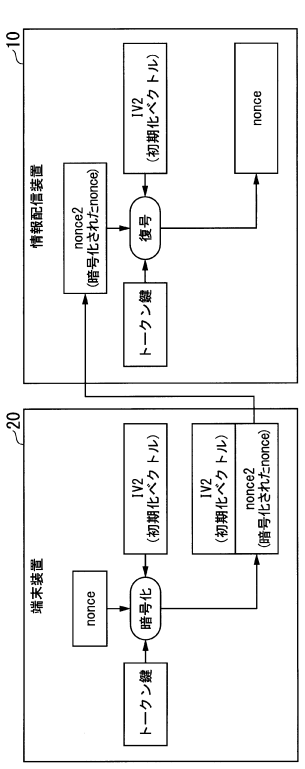


図８

【図９】

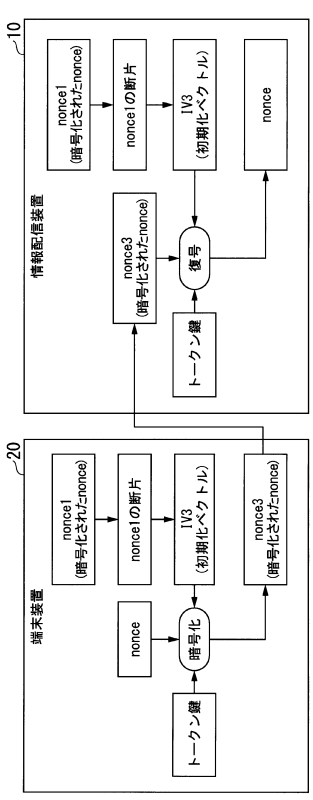


図９

フロントページの続き

(51)Int.Cl. F I

| | | | | |
|---|---|---|---|---|
| *H04L 9/14 (2006.01)* | | G09C | 1/00 | 640E |
| | | H04L | 9/00 | 641 |

(56)参考文献 特開２００６－２６８４１２（ＪＰ，Ａ）
特開平０９－１０７３５０（ＪＰ，Ａ）
特開２００４－２７４１３４（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)

| | |
|---|---|
| H04L | ９／３２ |
| G06F | １３／００ |
| G06F | ２１／４４ |
| G06F | ２１／６２ |
| G09C | １／００ |
| H04L | ９／１４ |