(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2014-197726
(P2014-197726A)
(43)公開日　平成26年10月16日(2014.10.16)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/16	(2006.01)	H04L	9/00	643	5J104
G06F 21/62	(2013.01)	G06F	21/24	166A	
G06Q 50/06	(2012.01)	G06Q	50/06		

審査請求 未請求　請求項の数 13　ＯＬ　（全 22 頁）

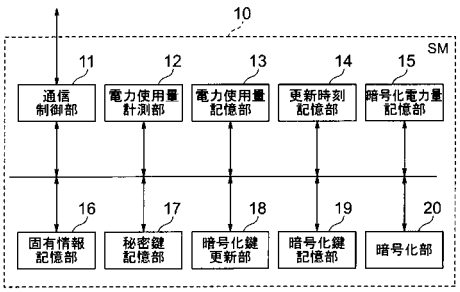
(21)出願番号　特願2013-71529(P2013-71529)
(22)出願日　平成25年3月29日(2013.3.29)

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(74)代理人　100117787
弁理士　勝沼　宏仁
(74)代理人　100082991
弁理士　佐藤　泰和
(74)代理人　100103263
弁理士　川崎　康
(74)代理人　100107582
弁理士　関根　毅
(72)発明者　小　椋　直　樹
東京都港区芝浦一丁目１番１号　株式会社東芝内

最終頁に続く

(54)【発明の名称】計測装置、情報処理装置、鍵管理装置および使用量計算システム

(57)【要約】　（修正有）
【課題】対象物の使用量を隠蔽してプライバシの保護を図る。
【解決手段】計測装置１０は、所定の集計範囲内での対象物の使用量を単位時間ごとに集計する使用量計測部１２と、集計された使用量を記憶する使用量記憶部と、鍵管理装置との間で共有される秘密鍵を記憶する秘密鍵記憶部１７と、所定期間ごとに、秘密鍵と時刻情報とに基づいて暗号化鍵を更新する暗号化鍵更新部１８と、暗号化鍵を記憶する暗号化鍵記憶部１９と、暗号化鍵記憶部に記憶されている暗号化鍵を用いて、使用量を暗号化して暗号データを生成する暗号化部と、生成された暗号データを記憶する暗号データ記憶部１５と、暗号データ記憶部に記憶された暗号データを集計使用量検出装置に送信する制御を行う通信制御部１１と、を備える。
【選択図】図２



SMの機能的構成

【特許請求の範囲】
【請求項１】
所定の集計範囲内での対象物の使用量を単位時間ごとに集計する使用量計測部と、
集計された前記使用量を記憶する使用量記憶部と、
鍵管理装置との間で共有される秘密鍵を記憶する秘密鍵記憶部と、
所定期間ごとに、前記秘密鍵と時刻情報とに基づいて暗号化鍵を更新する暗号化鍵更新部と、
前記暗号化鍵を記憶する暗号化鍵記憶部と、
前記暗号化鍵記憶部に記憶されている前記暗号化鍵を用いて、前記使用量を暗号化して暗号データを生成する暗号化部と、
生成された前記暗号データを記憶する暗号データ記憶部と、
前記暗号データ記憶部に記憶された前記暗号データを集計使用量検出装置に送信する制御を行う通信制御部と、を備える計測装置。
【請求項２】
前記暗号化鍵を更新する頻度である前記所定期間は、前記秘密鍵を更新する頻度より短い請求項１に記載の計測装置。
【請求項３】
前記暗号鍵の更新を行った更新時刻を記憶する更新時刻記憶部と、
前記暗号鍵の更新頻度を表す更新頻度情報を記憶する固有情報記憶部と、を備え、
前記暗号化鍵更新部は、前記更新時刻記憶部に記憶された更新時刻に、前記更新頻度情報により表される更新頻度を加えた時刻に到達する前に前記暗号化鍵を更新することを特徴とする請求項１または２に記載の計測装置。
【請求項４】
前記対象物は、電気、ガスおよび水道の少なくとも一つであることを特徴とする請求項１乃至３のいずれかに記載の計測装置。
【請求項５】
所定の管理対象地域内の複数の計測装置それぞれの単位時間ごとの対象物の使用量を暗号化した暗号データを集計した電力使用総量の暗号データを合計使用量検出装置から受信して記憶する地域暗号データ記憶部と、
鍵管理装置により第１所定期間ごとに更新される復号鍵を記憶する復号鍵記憶部と、
前記電力使用総量の暗号データに含まれる時刻情報と、前記復号鍵記憶部に記憶されている前記復号鍵とを用いて、前記電力使用総量の暗号データを復号して使用総量を取得する復号部と、
前記復号部が取得した前記使用総量に基づいて、前記管理対象地域内の前記対象物の使用量を制御する地域使用量制御部と、
前記鍵管理装置から前記復号鍵を受信する制御を行う通信制御部と、を備える情報処理装置。
【請求項６】
前記復号鍵の更新を行った更新時刻を記憶する更新時刻記憶部と、
前記復号鍵の更新頻度を表す更新頻度情報を記憶する固有情報記憶部と、
前記更新時刻記憶部に記憶された更新時刻に、前記更新頻度情報により表される更新頻度を加えた時刻に到達する前に前記復号鍵を更新する復号鍵更新部と、を備える請求項５に記載の情報処理装置。
【請求項７】
前記通信制御部は、前記鍵管理装置から前記復号鍵を正常に取得できなかった場合は、取得できなかった前記復号鍵の更新時刻を指定して、前記鍵管理装置に対して前記復号鍵の送信を要求する請求項５または６に記載の情報処理装置。
【請求項８】
前記対象物は、電気、ガスおよび水道の少なくとも一つであることを特徴とする請求項５乃至７のいずれかに記載の情報処理装置。

【請求項９】
計測装置との間で共有される秘密鍵を記憶する秘密鍵記憶部と、
所定の管理対象地域内の複数の前記計測装置それぞれの単位時間ごとの対象物の使用量を暗号化した暗号データを集計した電力使用総量の暗号データを情報処理装置が復号するのに用いる復号鍵を更新する時刻を記憶する更新時刻記憶部と、
前記秘密鍵と前記更新時刻記憶部に記憶されている時刻とを用いて、前記復号鍵を更新する復号鍵更新部と、
前記復号鍵更新部が更新した前記復号鍵を記憶する復号鍵記憶部と、
前記情報処理装置に対して前記復号鍵を送信する制御を行う通信制御部と、を備える鍵管理装置。
【請求項１０】
前記復号鍵更新部は、所定時間ごと、または前記情報処理装置から前記復号鍵の送信要求があった場合に、前記復号鍵を更新することを特徴とする請求項９に記載の鍵管理装置。
【請求項１１】
前記復号鍵更新部は、前記情報処理装置が集計使用量検出装置から受信した前記電力使用総量の暗号データに含まれる個々の暗号データに対応する複数の前記計測装置それぞれの識別情報と更新時刻情報とに基づいて前記復号鍵を更新する請求項９または１０に記載の鍵管理装置。
【請求項１２】
前記対象物は、電気、ガスおよび水道の少なくとも一つであることを特徴とする請求項９乃至１１のいずれかに記載の情報処理装置。
【請求項１３】
所定の管理対象地域内に属する複数の計測装置と、
前記管理対象地域内の前記複数の計測装置それぞれが対象物を使用した使用量の暗号データを暗号化されたままで集計した電力使用総量の暗号データを検出する集計使用量検出装置と、
前記電力使用総量の暗号データを復号して、前記管理対象地域内の前記複数の計測装置それぞれの対象物の使用を制御する情報処理装置と、
前記複数の計測装置それぞれとの間で秘密鍵を共有するとともに、前記情報処理装置に提供する復号鍵を更新する鍵管理装置と、を備え、
前記複数の計測装置のそれぞれは、
前記管理対象地域内の所定の集計範囲内での前記対象物の使用量を単位時間ごとに集計する使用量計測部と、
集計された前記使用量を記憶する使用量記憶部と、
鍵管理装置との間で共有される秘密鍵を記憶する第１秘密鍵記憶部と、
所定期間ごとに、前記秘密鍵と時刻情報とに基づいて暗号化鍵を更新する暗号化鍵更新部と、
前記暗号化鍵を記憶する暗号化鍵記憶部と、
前記暗号化鍵記憶部に記憶されている前記暗号化鍵を用いて、前記使用量を暗号化して暗号データを生成する暗号化部と、
生成された前記暗号データを記憶する暗号データ記憶部と、を有し、
前記情報処理装置は、
前記集計使用量検出装置から送信された前記電力使用総量の暗号データを記憶する地域暗号データ記憶部と、
前記鍵管理装置により第１所定期間ごとに更新される復号鍵を記憶する復号鍵記憶部と、
前記電力使用総量の暗号データに含まれる時刻情報と、前記復号鍵記憶部に記憶されている前記復号鍵とを用いて、前記電力使用総量の暗号データを復号して使用総量を取得する復号部と、

前記復号部が取得した前記使用総量に基づいて、前記管理対象地域内の対象物の使用量を制御する地域使用量制御部と、を有し、
前記鍵管理装置は、
前記計測装置との間で共有される秘密鍵を記憶する第２秘密鍵記憶部と、
前記電力使用総量の暗号データを前記情報処理装置が復号するのに用いる復号鍵を更新する時刻を記憶する更新時刻記憶部と、
前記秘密鍵と前記更新時刻記憶部に記憶されている時刻とを用いて、前記復号鍵を更新する復号鍵更新部と、
前記復号鍵更新部が更新した前記復号鍵を記憶する復号鍵記憶部と、を有する使用量計算システム。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明の実施の形態は、対象物の使用量を計測等する計測装置、情報処理装置、鍵管理装置および使用量計算システムに関する。
【背景技術】
【０００２】
スマートグリッドと呼ばれる次世代電力網では、各家庭などの電力使用量の集計範囲ごとに、電気機器の電力使用量を集計する電力メータであるスマートメータ（Smart Meter；以下、ＳＭという。）が設置されている。ＳＭは、電力網を介してデータ管理装置であるメータデータ管理システム（Meter Data Management System；以下、ＭＤＭＳという。）と通信する。ＭＤＭＳは、各家庭などに設置されたＳＭから、単位時間あたりの電力使用量を収集する。ＭＤＭＳが収集した単位時間あたりの電力使用量は、例えば、電力網に接続されたエネルギ管理システム（Energy Management System；以下、ＥＭＳという。）で利用される。ＥＭＳは、ＭＤＭＳに集まった複数の家庭などの電力使用量の総量に基づいて、管理対象地域内の各家庭などに対して電力の使用を抑制するよう要求したり、電力網に接続される蓄電池の充放電を制御したりするなどの電力制御を行う。ＭＤＭＳは、ＥＭＳの他にも、ＳＭから収集した電力使用量の総量を利用して処理を行うシステム（以下、総称してアプリケーションサーバという。）に対して、電力使用量を提供することができる。このため、ＭＤＭＳは、ＳＭから収集した電力使用量を保持して、後にアプリケーションサーバで利用する電力使用量の総量を計算できるようにしている。
【０００３】
しかし、ＳＭで集計された電力使用量そのものをＭＤＭＳに保持させる構成にすると、ＭＤＭＳの管理者やＭＤＭＳに侵入した不正なユーザによって電力使用量が盗み見されることで、家庭における活動の様子などを推察することが可能となり、プライバシの侵害に繋がる。そのため、ＳＭで集計した電力使用量そのものを隠蔽した状態でＭＤＭＳに保持させながら、アプリケーションサーバが必要とする電力使用量の総量を計算できるようにすることで、プライバシの保護を図ることが検討されている。電力使用量そのものを隠蔽した状態でＭＤＭＳに保持させるには、ＳＭにおいて電力使用量を暗号化することが有効である。この際、ＳＭやＭＤＭＳに負荷をかけない構成であることが求められる。
【先行技術文献】
【特許文献】
【０００４】
【特許文献１】特開２０１２－５８８５２号公報
【発明の概要】
【発明が解決しようとする課題】
【０００５】
本実施形態が解決しようとする課題は、対象物の使用量そのものを隠蔽してプライバシの保護を図りつつ、情報処理装置にて使用量の総量を計算できるデータ管理装置、鍵管理装置及び電力使用量計算システムを提供するものである。

【課題を解決するための手段】
【０００６】
本実施形態によれば、所定の集計範囲内での対象物の使用量を単位時間ごとに集計する使用量計測部と、
集計された前記使用量を記憶する使用量記憶部と、
鍵管理装置との間で共有される秘密鍵を記憶する秘密鍵記憶部と、
所定期間ごとに、前記秘密鍵と時刻情報とに基づいて暗号化鍵を更新する暗号化鍵更新部と、
前記暗号化鍵を記憶する暗号化鍵記憶部と、
前記暗号化鍵記憶部に記憶されている前記暗号化鍵を用いて、前記使用量を暗号化して暗号データを生成する暗号化部と、
生成された前記暗号データを記憶する暗号データ記憶部と、
前記暗号データ記憶部に記憶された前記暗号データを集計使用量検出装置に送信する制御を行う通信制御部と、を備える計測装置が提供される。
【図面の簡単な説明】
【０００７】
【図１】実施形態に係る電力使用量計算システムの構成例を示すブロック図。
【図２】ＳＭの機能的構成の一例を示すブロック図。
【図３】ＭＤＭＳの機能的構成の一例を示すブロック図。
【図４】ＥＭＳの機能的構成の一例を示すブロック図。
【図５】鍵管理サーバの機能的構成の一例を示すブロック図。
【図６】ＳＭにより実行される処理手順の一例を示すフローチャート。
【図７】ＳＭにより実行される処理手順の一例を示すフローチャート。
【図８】ＳＭにより実行される処理手順の一例を示すフローチャート。
【図９】ＳＭにより実行される処理手順の一例を示すフローチャート。
【図１０】ＭＤＭＳにより実行される処理手順の一例を示すフローチャート。
【図１１】ＭＤＭＳにより実行される処理手順の一例を示すフローチャート。
【図１２】鍵管理サーバにより実行される処理手順の一例を示すフローチャート。
【図１３】鍵管理サーバにより実行される処理手順の一例を示すフローチャート。
【図１４】鍵管理サーバにより実行される処理手順の一例を示すフローチャート。
【図１５】ＥＭＳにより実行される処理手順の一例を示すフローチャート。
【図１６】鍵管理サーバとＥＭＳにより実行される処理手順の一例を示すフローチャート。
【図１７】ＥＭＳにより実行される処理手順の一例を示すフローチャート。
【発明を実施するための形態】
【０００８】
（電力使用量計算システムの概要）
まず、実施形態に係る使用量計算システムの概要について説明する。実施形態に係る使用量計算システムは、複数の集計範囲の各々に設置されたＳＭ（計測装置）と、ＭＤＭＳ（集計使用量検出装置）と、ＥＭＳ（情報処理装置）と、鍵管理サーバ（鍵管理装置）とを備える。以下では、使用量の一例として、主に電力使用量を念頭に置いて、一実施形態に係る使用量計算システムを説明する。
【０００９】
ＳＭは、所定の集計範囲における対象物（例えば電気機器）の単位時間あたりの使用量（例えば電力使用量）を集計し、集計した単位時間あたりの電力使用量を自身の秘密鍵から生成される暗号化鍵を用いて暗号化し、暗号文すなわち暗号データ（第１の値）をＭＤＭＳに送信する。ＳＭが電力使用量の暗号化に用いる秘密鍵は、鍵管理サーバと共有されている。
【００１０】
ＭＤＭＳは、複数のＳＭから各々送信された暗号データを受信して保存する。この際、

ＭＤＭＳに対しては、ＳＭが電力使用量の暗号化に用いる暗号化鍵が秘匿されている。このため、ＳＭが集計した単位時間あたりの電力使用量がＭＤＭＳにおいて復号されることはなく、プライバシの保護が図られる。

【００１１】

また、ＭＤＭＳは、ＥＭＳが集計するＳＭのグループ単位で複数の暗号データを集計して電力使用総量の暗号データ（第２の値）を生成する。そして、ＭＤＭＳは、ＥＭＳに電力使用総量の暗号データをＥＭＳに送信する。

【００１２】

ＥＭＳは、ＭＤＭＳから送信された電力使用総量の暗号データを受信し、この電力使用総量の暗号データを保持する復号鍵を用いて復号し、複数の電力使用量を集計した値である電力使用総量（第３の値）を生成する。このように、ＥＭＳは、グループを構成する所定の管理対象地域内の各ＳＭの電力使用量を集計した電力使用総量の暗号データをＭＤＭＳから取得して、電力使用総量を生成する。そして、ＥＭＳは、生成した電力使用総量を用いて電力使用量抑制要求処理や地域内電力制御処理等のアプリケーションを実行する。ＥＭＳが電力使用総量の暗号データの復号に用いる復号鍵は、鍵管理サーバから一定時刻ごとに受信する。

【００１３】

鍵管理サーバは、一定時刻ごとにＥＭＳが集計するＳＭのグループ単位で復号鍵を更新し、生成した復号鍵をＥＭＳに送信する。この復号鍵は、ＳＭが電力使用量の暗号化に用いる秘密鍵（暗号化鍵）と時刻情報を用いて生成される。上述したように、復号鍵は、ＥＭＳがＭＤＭＳから受信した電力使用総量の暗号データの復号に用いるための鍵である。

【００１４】

以上のように、本実施形態に係る電力使用量計算システムによれば、ＭＤＭＳは電力使用量そのものを保存するのではなく、ＳＭの秘密鍵で電力使用量を暗号化して得られる暗号データを保存する。また、ＭＤＭＳにおいて行われる集計処理は、元の電力使用量を秘匿したままで行われる。したがって、ＭＤＭＳの管理者やＭＤＭＳに侵入した不正なユーザがＭＤＭＳから情報を取り出したとしても、電力使用量そのものが漏洩することはなく、プライバシの保護が図られる。また、ＳＭからＭＤＭＳに対して送信されるのは、ＳＭの秘密鍵で電力使用量を暗号化して得られる暗号データであり、ＭＤＭＳからＥＭＳに対して送信されるのは、鍵管理サーバから受信した復号鍵で電力使用総量を復号可能な電力使用総量の暗号データである。したがって、ＳＭとＭＤＭＳの間の通信やＭＤＭＳとＥＭＳとの間の通信が攻撃の対象となったとしても、電力使用量や電力使用総量が漏洩することはなく、プライバシの保護が図られる。ただし、鍵管理サーバとＥＭＳサーバの間の通信については、別途暗号化処理を行うなどして、復号鍵が流出しないように保護を行う必要がある。

【００１５】

ＳＭで集計した電力使用量そのものを隠蔽した状態でＭＤＭＳに保持させながら、ＥＭＳで利用する電力使用量の総量を算出できるようにする方法として、ＳＭによって暗号化された電力使用量をＭＤＭＳと鍵管理サーバが協調してＥＭＳが復号できる電力使用量に変換する構成が考えられる。しかし、この方法では、ＭＤＭＳが変換処理を行うごとに、ＭＤＭＳと鍵管理サーバの間で通信が発生し、負荷が大きくなる上、鍵管理サーバから送出される情報が大きい。これに対して、本実施形態では、ＳＭから受信した暗号データをＭＤＭＳが集計処理を行う際、鍵管理サーバとの通信を必要としない。そのため、鍵管理サーバと同期を取ることなく、集計処理を進めることが可能となる。また、鍵管理サーバとＥＭＳの間で別途暗号化処理を行うことにより、鍵管理サーバから送出される情報を低減することが可能となる。

【００１６】

以下では、アプリケーションサーバとしてＥＭＳを備えた電力使用量計算システムについて、さらに詳しく説明する。

【００１７】

ＥＭＳは、管理対象地域内の複数のＳＭから収集した第１単位時間における複数の電力使用量の総量（以下、第１電力使用総量という。）に基づいて、管理対象地域に対する電力制御を行う。ここで、第１単位時間とは、ＥＭＳが電力制御を実行する時間間隔を表し、例えば３０分などの時間間隔である。ＳＭが集計する電力使用量は、この第１単位時間あたりの電力使用量であるものとする。

【００１８】

なお、以下では、ＳＭは家庭における電力使用量を集計するものとして説明するが、ＳＭがオフィスビルなどの建物の電力使用量を集計する場合や、工場の電力使用量を集計する場合、地域における電力使用量を集計する場合であっても、同様の電力使用量計算システムを構築できる。また、アプリケーションサーバはＥＭＳに限定されるものではなく、電力使用量の総量を用いて所定のアプリケーションを実行する他のアプリケーションサーバを備えていてもよい。また、後述する電力使用量の暗号化処理は、ＳＭ以外の機器、例えばＳＭの集約器であるコンセントレータや、電力使用量を一時的に蓄積するＨＥＳ（Head End System）などで実施してもよい。

【００１９】

なお、本実施形態に係る使用量計算システムが扱う対象物は、電気機器に限らず、水道機器やガス機器など、使用量を定期的に計算する必要のある種々の機器に適用可能である。

【００２０】

図１は、一実施形態に係る電力使用量計算システム１の構成例を示すブロック図である。本実施形態に係る電力使用量計算システム１は、図１に示すように、ＳＭ１０と、ＭＤＭＳ３０と、ＥＭＳ５０と、鍵管理サーバ７０とを備え、これらがネットワーク９０を介して接続される構成である。なお、図面の簡略化のため、ＳＭ１０は１つしか図示していないが、電力使用量計算システムには、複数のＳＭ１０が接続されている。ネットワーク９０とは、例えば、ＬＡＮ（Local Area Network）、イントラネット、イーサネット（登録商標）またはインターネットなどである。

【００２１】

ＳＭ１０は、各家庭に設置され、各家庭で使用される電気機器の電力使用量を集計する設備である。なお、各ＳＭ１０に対しては、これを識別するための識別情報（以下、ＳＭ＿ＩＤという。）が付与されており、各ＳＭ１０は当該ＳＭ１０に対して付与されたＳＭ＿ＩＤを記憶しているものとする。

【００２２】

ＭＤＭＳ３０は、ネットワーク９０を介して各家庭のＳＭ１０から電力使用量を収集して管理するシステムである。ＭＤＭＳ３０は、複数の装置で構成されていてもよいし、単体の装置として構成されていてもよい。以下では、ＭＤＭＳ３０は単体の装置として構成されているものとして説明する。なお、各ＭＤＭＳ３０は複数のＳＭ１０を纏めたグループ単位ごとに処理を行う。各ＭＤＭＳ３０はＳＭ１０のグループ単位各々に付与されたＳＭ＿ＧＲ＿ＩＤを記憶しているものとする。以下では、簡略化のため、扱うグループは１つとし、ＳＭ＿ＩＤは１からｉｄ＿ｅｎｄまで連番で付いているものとする。

【００２３】

ＥＭＳ５０は、管理対象地域における複数の家庭の第１単位時間における電力使用量の総量（第１電力使用総量）を把握し、第１電力使用総量と供給可能な電力量とのバランスを考慮して、管理対象地域内の各家庭に対して、電力の使用を抑制するよう要求したり、電力網に接続される蓄電池の充放電を制御したりするなどの電力制御を行う。ＥＭＳ５０は、複数の装置で構成されていてもよいし、単体の装置として構成されていてもよい。以下では、ＥＭＳ５０は単体の装置として構成されているものとして説明する。

【００２４】

鍵管理サーバ７０は、ＳＭ１０と秘密鍵を共有し、一定時刻ごとに後述する復号鍵を生成してＥＭＳ５０に送信する。また、ＥＭＳ５０からの復号鍵の要求に対し、復号鍵を生成してＥＭＳ５０に送信する。

【００２５】
なお、ＭＤＭＳ３０、ＥＭＳ５０、および鍵管理サーバ７０は各々、電力使用量計算システム１に接続される各ＳＭ１０のＳＭ＿ＩＤをすべて記憶しているものとする。また、ＳＭ１０が集計した第１単位時間における電力使用量に対しては、少なくともＳＭ＿ＩＤと、集計された時間帯を表す時刻情報とが対応付けられる。電力使用量の暗号データは、電力使用量に対応付けられた時刻情報も利用して生成される。ただし、電力使用量に対してＳＭ＿ＩＤや時刻情報に加えて他の情報をさらに対応付けて、他の情報をさらに用いて暗号データを生成するようにしてもよい。
【００２６】
ＳＭ１０は独自の秘密鍵を保持しており、同じ秘密鍵を鍵管理サーバ７０も保持している。ＳＭ１０の秘密鍵は工場出荷時にＳＭ１０に埋め込まれていてもよいし、家庭に設置した際にＳＭ１０内部で生成されて、それがネットワーク９０を通じて鍵管理サーバ７０に送信されてもよいし、家庭に設置した後にネットワーク９０を通じて鍵管理サーバ７０から配信されてもよい。また、ＳＭ１０は電力使用量の暗号化に用いるための暗号化鍵を保持している。暗号化鍵は秘密鍵からＳＭ１０が生成する。また、ＥＭＳ５０は電力使用総量の復号に用いるための復号鍵を保持しており、同じ復号鍵を鍵管理サーバ７０も保持している。復号鍵は複数の秘密鍵から鍵管理サーバ７０が生成・更新を行い、ＥＭＳ５０に配信する。
【００２７】
このような構成の電力使用量計算システムにおいて、ＳＭ１０は、自身の暗号化鍵を用いて第１単位時間における電力使用量を暗号化して暗号データを生成する。ＳＭ１０が生成した暗号データは、ネットワーク９０を介してＭＤＭＳ３０に送信される。
【００２８】
ＭＤＭＳ３０は、ＳＭ１０から送信された暗号データを受信して保持する。そして、ＭＤＭＳ３０は、ＥＭＳ５０からの要求に応じて、まず、ＥＭＳ５０の管理対象地域に含まれる家庭のＳＭ１０から収集した複数の暗号データを集計した電力使用総量の暗号データを生成する。そして、ＭＤＭＳ３０は、得られた電力使用総量の暗号データを、ネットワーク９０を介してＥＭＳ５０に送信する。
【００２９】
ＥＭＳ５０は、要求に対する応答としてＭＤＭＳ３０からネットワーク９０を介して送信された電力使用総量の暗号データを受信し、復号鍵を用いてこの電力使用総量の暗号データを復号することにより、電力使用総量を生成する。そして、ＥＭＳ５０は、得られた電力使用総量に基づいて、管理対象地域に対する電力制御を行う。
【００３０】
次に、ＳＭ１０、ＭＤＭＳ３０、ＥＭＳ５０、鍵管理サーバ７０のハードウェア構成について説明する。
【００３１】
ＳＭ１０は、装置全体を制御するＣＰＵなどの制御部と、ＣＰＵのワークエリアとなるＲＡＭなどの主記憶部と、各種データや各種プログラムを記憶するＲＯＭや不揮発性メモリなどの補助記憶部と、これらを接続するバスとを備えており、専用ハードウェアあるいは組み込み機器と同様の構成となっている。また、ＳＭ１０は、ネットワーク９０を介して通信を行うための通信Ｉ／Ｆを備える。さらに、ＳＭ１０には、電力使用量などの各種情報を表示する表示部と、ユーザの操作が入力される操作ボタンやキーボードなどの操作入力部とが接続される。
【００３２】
ＭＤＭＳ３０、ＥＭＳ５０、鍵管理サーバ７０は、装置全体の制御や基本演算を実行するＣＰＵ（Central Processing Unit）などの制御部と、ＣＰＵのワークエリアとなるＲＡＭ（Random Access Memory）などの主記憶部と、各種データや各種プログラムを記憶するＲＯＭ（Read Only Memory）、ＨＤＤ（Hard Disk Drive）、ＣＤ（Compact Disk）ドライブ装置などの補助記憶部と、これらを接続するバスとを備えており、通常の

コンピュータを利用したハードウェア構成となっている。また、ＭＤＭＳ３０、ＥＭＳ５０、鍵管理サーバ７０は、ネットワーク９０を介して通信を行うための通信Ｉ／Ｆ（Interface）を備える。

【００３３】

次に、このようなハードウェア構成において、ＳＭ１０、ＭＤＭＳ３０、ＥＭＳ５０および鍵管理サーバ７０のそれぞれにおいて実現される各種機能について説明する。

【００３４】

まず、ＳＭ１０において実現される各種機能について説明する。図２は、ＳＭ１０の機能的構成の一例を示すブロック図である。ＳＭ１０は、例えば図２に示すように、通信制御部１１と、電力使用量計測部１２と、電力使用量記憶部１３と、更新時刻記憶部１４と、暗号化電力量記憶部１５と、固有情報記憶部１６と、秘密鍵記憶部１７と、暗号化鍵更新部１８と、暗号化鍵記憶部１９と、暗号化部２０を備える。通信制御部１１の機能は、通信Ｉ／Ｆと、ＣＰＵが実行する各種プログラムにより実現される。電力使用量計測部１２と、暗号化鍵更新部１８と、暗号化部２０の各機能は、ＣＰＵが実行する各種プログラムにより実現される。電力使用量記憶部１３と、更新時刻記憶部１４と、暗号化電力量記憶部１５と、固有情報記憶部１６と、秘密鍵記憶部１７および暗号化鍵記憶部１９はそれぞれ、例えば補助記憶部に確保される記憶領域である。

【００３５】

通信制御部１１は、ＭＤＭＳ３０との間のネットワーク９０を介した通信を制御する。具体的には、通信制御部１１は、ＭＤＭＳ３０から送信された制御コマンドを受信したり、後述の暗号化部２０が電力使用量記憶部１３に記憶された電力使用量を暗号化して得られる暗号データをＭＤＭＳ３０に送信したり、外部の時刻サーバから時刻情報を受信して同期を取ったりする。

【００３６】

電力使用量計測部１２は、家庭における電気機器の電力使用量を第１単位時間ごとに集計する。そして、電力使用量計測部１２は、集計した電力使用量を電力使用量記憶部１３に記憶させる。また、電力使用量計測部１２は、通信制御部１１が受信した制御コマンドに応じて、電力使用量の集計を開始したり、その集計を中止したりする。

【００３７】

電力使用量記憶部１３は、電力使用量計測部１２が集計した第１単位時間ごとの電力使用量を記憶する。電力使用量記憶部１３に記憶された電力使用量は第１所定時間後に削除される。ここで第１所定時間とは、ＳＭ１０の記憶領域のサイズなどに依存する時間であり、例えば２週間であったり３０日であったりする。

【００３８】

更新時刻記憶部１４は、暗号化鍵更新部で必要とされる、過去に暗号化鍵の更新を行った時刻を記憶する。更新時刻記憶部１４に記憶された時刻（更新時刻）は暗号化鍵更新部１８を実行する際に、書き換えが行われる。

【００３９】

暗号化電力量記憶部１５は、暗号化部２０で計算された、暗号化処理が施された電力使用量を記憶する。電力使用量記憶部１３に記憶された電力使用量は第１所定時間後に削除される。

【００４０】

固有情報記憶部１６は、電力使用量記憶部１３と、更新時刻記憶部１４と、暗号化電力量記憶部１５と、秘密鍵記憶部１７と、暗号化鍵記憶部１９とに記憶されない情報で、ＳＭ１０が必要とする情報を記憶する。具体的には、固有情報記憶部１６には、ＳＭ１０が固有に保持するＳＭ＿ＩＤ、および更新時刻記憶部１４に記憶される更新時刻を更新する頻度を表すｔ＿δが記憶される。

【００４１】

秘密鍵記憶部１７は、暗号化鍵を更新するために用いる秘密鍵を記憶する。

【００４２】

暗号化鍵更新部１８は、第二所定時間後に、暗号化鍵を計算し直し新しい暗号鍵を生成する。そして、生成した暗号化鍵を暗号化鍵記憶部１９に記憶させる。ここで、第二所定時間とは、固有情報記憶部１６に記憶されている、更新時刻の頻度を表すｔδより短い時間であり、例えば、６時間であったり、１日であったりする。暗号化鍵の生成の詳細は後述する。

【００４３】

暗号化鍵記憶部１９は、電力使用量を暗号化して暗号データを生成するための暗号化鍵を記憶する。

【００４４】

暗号化部２０は、電力使用量記憶部１３が記憶する第１単位時間ごとの電力使用量を、暗号化鍵記憶部１９に記憶された暗号化鍵を用いて暗号化して暗号データを生成する。本実施形態においては、電力使用量の暗号化には、鍵管理サーバ７０と共有した秘密鍵を利用した暗号方式を用いる。電力使用量の暗号化の詳細は後述する。

【００４５】

ここで、秘密鍵について説明する。秘密鍵は、ＳＭ１０と鍵管理サーバ７０との間のみで共有される秘密鍵Ｋｓｍが存在する。秘密鍵Ｋｓｍは、ＳＭ１０の秘密鍵記憶部１７に記憶される。秘密鍵の更新頻度は、ＳＭの管理者が設定したポリシに依存しており、例えば、半年や数年など比較的長い期間となることが一般的である。したがって、一般には、秘密鍵Ksmの更新周期は、暗号化鍵の更新周期よりも長い。

【００４６】

次に、暗号化鍵について説明する。暗号化鍵は電力使用量の暗号化に用いるための鍵であり、秘密鍵Ｋｓｍと時刻情報とを用いて生成される。時刻情報の例としては、「２０１２年１月１日」や「１４：３５：４６，１／１／２０１２」やＵＮＩＸ（登録商標）時刻（１９７０年１月１日０時０分０秒（ＧＭＴ）を起点とし、それから経過した秒数）などが挙げられる。秘密鍵をｋ＿ＳＭ、更新時刻をｔ＿ｕｐ＿ＳＭとしたときに、暗号化鍵Ｋｅｎｃは、下記式（１）により計算される。

Ｋｅｎｃ＝Ｈ１（ｋ＿ＳＭ，ｔ＿ｕｐ＿ＳＭ）　・・・（１）

ここで、Ｈ１（ｘ，ｙ）はｘとｙを入力とする一方向性関数あるいは鍵付きハッシュ関数であり、一方向性関数の例としてはｓｈａ－１やｍｄ５、ｓｈａ２５６など、また鍵付きハッシュ関数としてはｈｍａｃ、ｏｍａｃなどが挙げられる。

【００４７】

暗号化鍵は、現在時刻ｔ＿１が更新時刻記憶部１４に記憶されている更新時刻ｔ＿ｕｐ＿ＳＭを越えた時刻において更新が行われる。ｔ＿ｕｐ＿ＳＭは一定の頻度ｔδごとに更新を行う。ｔδは固有情報記憶部１６に記憶されている。ＳＭ１０を起動する際、ｔ＿ｕｐ＿ＳＭは現在時刻ｔ＿１から下記式（２）により計算される。

ｔ＿ｕｐ＿ＳＭ＝ｔδ　＊　ＩＮＴ（ｔ＿１／ｔ＿δ）　・・・（２）

ここで、ＩＮＴ（ｘ）はｘを入力とし、ｘの整数部分を出力する関数である。

【００４８】

前回の更新時刻ｔ＿ｕｐ＿ＳＭからｔδを過ぎた時刻において、式（１）を用いて暗号化鍵Ｋｅｎｃを更新する。更新した暗号化鍵は暗号化鍵記憶部１９に記憶される。同時に、前回の更新時刻ｔ＿ｕｐ＿ＳＭにｔδを加算することにより、更新時刻ｔ＿ｕｐ＿ＳＭを更新する。更新した更新時刻は更新時刻記憶部１４に記憶される。

【００４９】

次に、暗号化部２０が行う暗号化の方法の具体例について説明する。本実施形態において使用する暗号化の方法は、準同型性を有する。データｄを暗号化鍵ｅｋ＿Ｐで暗号化する暗号化Ｅｎｃ＿Ｐ（ｅｋ＿Ｐ，ｄ）が準同型であるとは、データｄとｄ’について、Ｅｎｃ＿Ｐ（ｅｋ＿Ｐ，ｄ）＊Ｅｎｃ＿Ｐ（ｅｋ＿Ｐ，ｄ’）＝Ｅｎｃ＿Ｐ（ｅｋ＿Ｐ，ｄ＋ｄ’）を満たすことをいう。ここで、＋は算術加算を表し、＊は適切な演算子を表す。このような暗号化の方法としては、例えば、十分に大きな基数を用いるシーザー暗号や、以下の参考文献１に記載された暗号化などがあり、＊はそれぞれ、剰余環での加算および

剰余乗算を表す。
（参考文献１）Pascal Paillier, Public-Key Cryptosystems Based on Composite Degree Residuosity Classes, EUROCRYPT 1999, pp223-238
【００５０】
ここで、電力使用量を暗号化して暗号データを生成する手順の具体的な一例について説明する。時刻情報ｔで示される第１単位時間において電力使用量計測部１２で集計された電力使用量をｄｔとする。暗号化部１７は、まず下記式（２）に従って、ｃｔを計算する。
ｃｔ＝ｄｔ＋Ｋｅｎｃ＊Ｈ２（ｔ）　・・・（２）
ここで、Ｋｅｎｃは、更新時刻ｔｕｐを用いて得られる暗号化鍵で、Ｈ２（ｘ）はｘを入力とする一方向性関数あるいは鍵付きハッシュ関数である。
【００５１】
なお、時刻情報ｔは、以降の処理において必要な情報となるため、暗号データに付随してＭＤＭＳ３０に送信する必要がある。このため、ＳＭ１０がＭＤＭＳ３０に送信するデータＣｓｍ＿ｔは、下記式（５）で示されるように、暗号データ（ｃｔ）と時刻情報ｔとを対応付けたデータとなる。
Ｃｓｍ＿ｔ＝（ｃｔ，ｔ）　・・・（５）
以下では、暗号データｃｔと時刻情報ｔとを対応付けたデータＣｓｍ＿ｔ＝（ｃｔ，ｔ）を、電力使用量の暗号データとして扱うものとする。
【００５２】
次に、ＭＤＭＳ３０において実現される各種機能について説明する。図３は、ＭＤＭＳ３０の機能的構成の一例を示すブロック図である。ＭＤＭＳ３０は、例えば図３に示すように、通信制御部３１と、暗号化電力量記憶部３２と、集計暗号化電力量記憶部３３と、集計部３４と、固有情報記憶部３５とを備える。通信制御部３１の機能は、通信Ｉ／Ｆと、ＣＰＵが実行する各種プログラムにより実現される。集計部３４の機能は、ＣＰＵが実行する各種プログラムにより実現される。暗号化電力量記憶部３２と、集計暗号化電力量記憶部３３と、固有情報記憶部３５とは、例えば補助記憶部に確保される記憶領域である。
【００５３】
通信制御部３１は、ＳＭ１０やＥＭＳ５０などの他の機器との間のネットワーク９０を介した通信を制御する。具体的には、通信制御部３１は、第１単位時間ごとにＳＭ１０から電力使用量の暗号データを受信したり、ＳＭ１０に制御コマンドを送信したり、集計部３４により生成された電力使用総量の暗号データをＥＭＳ５０に送信したりする。なお、ＳＭ１０に送信する制御コマンドとは、例えば、電力使用量の計測の中止やその開始、電力使用量の送信などを指示するコマンドである。
【００５４】
暗号化電力量記憶部３２は、通信制御部３１がＳＭ１０から受信した第１単位時間ごとの電力使用量の暗号データを記憶する。
【００５５】
集計暗号化電力量記憶部３３は、集計部３４が生成した電力使用総量の暗号データを記憶する。電力使用総量の暗号データは複数の第１単位時間の電力使用量を集計した電力使用総量の暗号データに対応する。
【００５６】
集計部３４は、ＥＭＳ５０からの要求に応じて、ＥＭＳ５０が定める管理グループに含まれるすべての家庭のＳＭ１０から収集して電力使用量記憶部２２に記憶された複数の第１単位時間の電力使用量の暗号データを集計し、電力使用総量の暗号データを生成する。集計部３４が生成した電力使用総量の暗号データは、通信制御部３１からネットワーク９０を介してＥＭＳサーバ３０に送信される。
【００５７】
ここで、複数の暗号データを集計して電力使用総量の暗号データを生成する手順の具体

的な一例について説明する。ここでは、集計の対象となるＳＭ１０が３つであるものとして説明する。３つのＳＭ１０をそれぞれＳＭ１０－１，ＳＭ１０－２，ＳＭ１０－３とし、それぞれのＳＭ　ｉｄをそれぞれ１，２，３とする。ＳＭ１０－１，ＳＭ１０－２，ＳＭ１０－３それぞれの時刻情報ｔで示される第１単位時間における電力使用量の暗号データをＣｓｍ＿１＿ｔ，Ｃｓｍ＿２＿ｔ，Ｃｓｍ＿３＿ｔとすると、これらは下記式（６）～（８）のように表すことができる。

Ｃｓｍ＿１＿ｔ＝（ｃｔ＿１，ｔ）　・・・（６）

Ｃｓｍ＿２＿ｔ＝（ｃｔ＿２，ｔ）　・・・（７）

Ｃｓｍ＿３＿ｔ＝（ｃｔ＿３，ｔ）　・・・（８）

このとき、電力使用総量の暗号データをＣｓｍ＿Ａ（１２３）＿（ｔ）とすると、集計部３４は、下記式（９）を用いて電力使用総量の暗号データを求めることができる。

Ｃｓｍ＿Ａ（１２３）＿（ｔ）＝（ＣＡ＿ｃ，ｔ）　・・・（９）

ただし、ＣＡ＿ｃ＝ｃｔ＿１＋ｃｔ＿２＋ｃｔ＿３、である。

【００５８】

次に、ＥＭＳ５０において実現される各種機能について説明する。図４は、ＥＭＳ５０の機能的構成の一例を示すブロック図である。ＥＭＳ５０は、例えば図４に示すように、通信制御部５１と、地域暗号化電力量記憶部５２と、地域電力量記憶部５２と、地域電力量制御部５３と、更新時刻記憶部５５と、復号鍵記憶部５６と、復号鍵更新部５７と、復号部５８と、固有情報記憶部５９とを備える。通信制御部５１の機能は、通信Ｉ／Ｆと、ＣＰＵが実行する各種プログラムにより実現される。復号部５８、復号鍵更新部５７および地域電力量制御部５４の各機能は、ＣＰＵが実行する各種プログラムにより実現される。地域暗号化電力量記憶部５２、更新時刻記憶部５５、復号鍵記憶部５６および固有情報記憶部５９は、例えば補助記憶部に確保される記憶領域である。

【００５９】

通信制御部５１は、ＭＤＭＳ３０や鍵管理サーバ７０との間のネットワーク９０を介した通信を制御する。具体的には、通信制御部５１は、ＭＤＭＳ３０から送信された電力使用総量の暗号データを受信したり、鍵管理サーバから送信された復号鍵を受信したりする。

【００６０】

地域暗号化電力量記憶部５２は、通信制御部５１で受信された電力使用総量の暗号データを記憶する。

【００６１】

地域電力量記憶部５３は、復号部５８によって、地域暗号化電力量記憶部５２に記憶された電力使用総量の暗号データを復号することによって得られる、第１電力使用総量を記憶する。

【００６２】

復号鍵記憶部５６は鍵管理サーバ７０から受信した復号鍵ｓを記憶する。復号鍵ｓは鍵管理サーバ７０がＳＭの秘密鍵と更新時刻を用いて生成する。復号鍵の生成手順は後に詳細を述べる。

【００６３】

ここで、復号部５８が復号鍵ｓを用いて電力使用総量の暗号データを復号して第１電力使用総量を生成する手順の具体的な一例について説明する。ここでは、通信制御部５１が、ＭＤＭＳ３０から第１変換電力使用総量の暗号データＣｓｍ＿Ａ（１２３）＿（ｔ）＝（ＣＡ＿ｃ，ｔ）を受信した場合を例示する。

【００６４】

復号部５８は、まずＭＤＭＳ３０から受信した電力使用総量の暗号データに含まれる時刻情報ｔと更新時刻ｔｕｐを用いて、下記条件式（１５）を満たすか判断を行う。

ｔｕｐ＜＝ｔ＜ｔｕｐ＋ｔδ　・・・（１５）

条件式を満たさない場合には、復号鍵が有効でないと判断して、復号処理を中止する。復号処理を中止した場合には、鍵管理サーバ７０に対して時刻情報ｔに対応する復号鍵を送

るようにリクエストを送信する。

【００６５】

次に、ＭＤＭＳ３０から受信した電力使用総量の暗号データに含まれる時刻情報ｔと復号鍵記憶部５６に保持してある復号鍵ｓを用いて下記（１６）で示す計算を行い、第１電力使用総量ｄ＿ＥＭＳを得る。

ｄ＿ＥＭＳ＝ＣＡ＿ｃ－ｓ＊Ｈ２（ｔ）　・・・（１６）

ここで、Ｈ２（ｘ）は、上述したようにｘを入力とする一方向性関数あるいは鍵付きハッシュ関数である。

【００６６】

地域電力量制御部５４は、復号部５８が生成した第１電力使用総量に基づいて、管理対象地域に対する電力制御を行う。電力制御とは、例えば、第１電力使用総量が上限値を超えている場合に、管理対象地域内の各家庭に対して電力の使用を抑制するよう要求したり、電力網に接続される蓄電池の放電を促したり、第１電力使用総量が下限値を下回っている場合に、電力網に接続される蓄電池に余剰の供給電力を蓄電したりする制御である。

【００６７】

復号鍵更新部５７は鍵管理サーバから受信した復号鍵ｓ＿ＫＭとｔ＿ｕｐ＿ＫＭを用いて復号鍵ｓ＿ＥＭＳとｔ＿ｕｐ＿ＥＭＳを更新する。鍵管理サーバ７０は復号鍵を更新する度にＥＭＳ７０に復号鍵と更新時刻を送信し、ＥＭＳは受信した復号鍵と更新時刻をそのまま記憶する。

【００６８】

万一、適切な復号鍵を取得できず、復号部５８において復号が中止された場合、鍵管理サーバに対して、復号で用いる時刻情報に対応する復号鍵を要求する。ＥＭＳ７０は、鍵管理サーバ７０から要求に対する応答として送信される復号鍵と更新時刻を記憶する。

【００６９】

固有情報記憶部５９は、地域暗号化電力量記憶部５２、更新時刻記憶部５５、復号鍵記憶部５６に記憶されない情報で、ＥＭＳ５０が必要とする情報が記憶される。具体的には、更新時刻記憶部５５に記憶される更新時刻を更新する頻度を表すｔδが記憶される。

【００７０】

次に、鍵管理サーバ７０において実現される各種機能について説明する。図５は、鍵管理サーバ７０の機能的構成の一例を示すブロック図である。鍵管理サーバ７０は、例えば図５に示すように、通信制御部７１と、更新時刻記憶部７２と、秘密鍵記憶部７３と、復号鍵更新部７４と、復号鍵記憶部７５と、固有情報記憶部７６とを備える。通信制御部７１の機能は、通信Ｉ／Ｆと、ＣＰＵが実行する各種プログラムにより実現される。復号鍵更新部７４の機能は、ＣＰＵが実行する各種プログラムにより実現される。更新時刻記憶部７２と、秘密鍵記憶部７３と、復号鍵記憶部７５は、例えば補助記憶部に確保される記憶領域である。

【００７１】

通信制御部７１は、ＥＭＳ５０との間のネットワーク９０を介した通信を制御する。具体的には、通信制御部５１は、後述の復号鍵更新部４３で生成された復号鍵をＥＭＳ５０に送信する。

【００７２】

更新時刻記憶部７２は、復号鍵更新部７４で用いられる復号鍵を更新する時刻ｔ＿ｕｐ＿ＫＭを記憶する。

【００７３】

秘密鍵記憶部７３は、ＳＭ１０と共有する上述した秘密鍵Ｋｓｍを記憶する。

【００７４】

復号鍵更新部７４は、第二所定時間ごと、あるいは、ＥＭＳから復号鍵の要求を受信した際に、秘密鍵記憶部７３に記憶されているＳＭ１０のすべての秘密鍵Ｋｓｍと更新時刻記憶部７２に記憶されている更新時刻情報ｔ＿ｕｐ＿ＫＭを用いて復号鍵を生成する。

【００７５】

ここで、復号鍵更新部７４が処理対象に含まれるＳＭ１０のグループに対する復号鍵を生成する手順の具体的な一例について説明する。ここでは、処理対象となるＳＭ１０が３つであるものとして説明する。３つのＳＭ１０をそれぞれＳＭ１０－１，ＳＭ１０－２，ＳＭ１０－３とし、それぞれのＳＭ　ｉｄをそれぞれ１，２，３とする。ＳＭ１０－１，ＳＭ１０－２，ＳＭ１０－３それぞれが保持する秘密鍵をｋ＿ＳＭ＿１，ｋ＿ＳＭ＿２，ｋ＿ＳＭ＿３とする。これらに対して、まず下記式（１７）～（１９）で表される部分暗号化鍵ｓ＿１，ｓ＿２，ｓ＿３を計算する。

ｓ＿１＝Ｈ１（ｋ＿ＳＭ＿１，ｔｕｐ）　　・・・（１７）

ｓ＿２＝Ｈ１（ｋ＿ＳＭ＿２，ｔｕｐ）　　・・・（１８）

ｓ＿３＝Ｈ１（ｋ＿ＳＭ＿３，ｔｕｐ）　　・・・（１９）

ただし、Ｈ１（ｘ，ｙ）は、上述したようにｘとｙを入力とする一方向性関数あるいは鍵付きハッシュ関数である。

【００７６】

式（１７）～（１９）を用いて，ＳＭ１０のグループＳＭ１０－１，ＳＭ１０－２，ＳＭ１０－３に対する復号鍵を、下記式（２０）を用いて生成する。

ｓ＝ｓ＿１＋ｓ＿２＋ｓ＿３　　・・・（２０）

【００７７】

復号鍵記憶部７５は、復号鍵更新部７４が生成した復号鍵を記憶する。

【００７８】

固有情報記憶部７６は、秘密鍵記憶部７３、復号鍵記憶部７５に記憶していない情報で、鍵管理サーバ７０が必要とする情報が記憶される。具体的には、更新時刻記憶部７２に記憶される更新時刻を更新する頻度を表すｔδが記憶される。

【００７９】

次に、本実施形態に係る電力使用量計算システムにおいて実行される各種の処理の手順について、図６から図１６のフローチャートを参照しながら説明する。

【００８０】

まず、ＳＭ１０が更新時刻ｔ＿ｕｐ＿ＳＭを初期起動時に生成する処理の手順について、図６を用いて説明する。図６はＳＭ１０により実行される処理手順の一例を示すフローチャートである。

【００８１】

ＳＭ１０はまず時刻ｔ＿１を取得する（ステップＳ１０１）。固有情報記憶部に保存されているｔδと時刻ｔ＿１を用いて更新時刻ｔ＿ｕｐ＿ＳＭを生成する（ステップＳ１０３，Ｓ１０４）。生成されたｔ＿ｕｐ＿ＳＭは更新時刻として更新時刻記憶部１４に記憶される（ステップＳ１０４）。

【００８２】

次に、ＳＭ１０が一定時刻ごとに暗号化鍵を更新する処理の手順について、図７を用いて説明する。図７は、ＳＭ１０により実行される処理手順の一例を示すフローチャートである。

【００８３】

ＳＭ１０は、まず更新時刻ｔｕｐと時刻ｔ＿１を取得し（ステップＳ２０１，Ｓ２０２）、ｔ＿１とｔｕｐの値を比較する（ステップＳ２０３）。ｔ＿１がｔｕｐ以上である場合のみ、その後の処理を実行する。ｔ＿１がｔｕｐ未満の場合は、復号鍵の更新を中止する。

【００８４】

次に、ＳＭ１０は、秘密鍵ｋ＿ＳＭを取得し（ステップＳ２０４）、暗号化鍵ｋ＿ｅｎｃを計算する（ステップＳ２０５）。ｋ＿ｅｎｃは暗号化鍵記憶部１６に記憶する（ステップＳ２０６）。更新時刻ｔ＿ｕｐを更新し（ステップＳ２０７）、暗号化鍵の更新時刻としてｔ＿ｕｐを保存する（ステップＳ２０８）。

【００８５】

ＳＭ１０が電力使用量の暗号データを生成するまでの処理の手順について、図８を用い

て説明する。図８は、ＳＭ１０により実行される処理手順の一例を示すフローチャートである。

【００８６】

ＳＭ１０は、第１単位時間ごとに電気機器の電力使用量ｄｔを集計すると（ステップＳ３０１）、時刻ｔ＿１を取得する（ステップＳ３０２）。また、暗号化鍵記憶部１６から暗号化鍵ｋ＿ｅｎｃを取得する（ステップＳ３０３）。

【００８７】

ステップＳ３０３で取得した暗号化鍵ｋ＿ｅｎｃと時刻情報ｔ＿１を用いて集計した電力使用量ｄ＿ｔを暗号化し、暗号データｃｔを生成する（ステップＳ３０４）。ＳＭ１０は、ステップＳ２０４で生成した暗号データｃｔを時刻情報ｔ＿１と対応付けてＭＤＭＳ３０に送信する（ステップＳ３０５）。このとき、ＳＭ１０は、ＳＭ１０に付与された識別コードＳＭ＿ＩＤも送信する。

【００８８】

次に、暗号化された電力データをＭＤＭＳ３０に送信する処理の手順について、図９を用いて説明する。図９はＳＭ１０により実行される処理手順の一例を示すフローチャートである。

【００８９】

まず、識別コードＳＭ＿ＩＤと、暗号化電力量ｃｔを取得する（ステップＳ４０１，Ｓ４０２）。次に、各暗号データｃｔに対応づけてある時刻情報ｔ＿２を取得する（ステップＳ４０３）。取得したＳＭ＿ＩＤと、ｃｔと、ｔ＿２を組にして、ＭＤＭＳ３０に送信する（ステップＳ４０４）。

【００９０】

送信する情報は、ｉｄ、ｃｔ、ｔ＿２のみに限るものではない。例えば、ＳＭ１０を特定する情報を含めてもよい。

【００９１】

次に、ＭＤＭＳ３０がＳＭ１０から受信した暗号化された電力使用量を集計する処理の手順について、図１０を用いて説明する。図１０はＭＤＭＳ３０により実行される処理手順の一例を示すフローチャートである。

【００９２】

まず、集計値の値を格納する変数ｇｒ＿ｃｔに０を設定して集計値の計算の準備を行う（ステップＳ５０１）。また、ｉｄに１を設定し、ループ変数を準備する（ステップＳ５０２）。

【００９３】

次に、ｉｄに対応する電力データｃｔ＿ｉｄを取得し（ステップＳ５０３）、ｇｒ＿ｃｔに加算する（ステップＳ５０４）。次に、ｉｄを１増やし（ステップＳ５０５）、ｉｄの値がｉｄ＿ｅｎｄと等しくなるか調べ（ステップＳ５０６）、等しくなるまでこれらの処理を繰り返す（ステップＳ５０５，Ｓ５０６）。ステップＳ５０１からＳ５０６の処理を行うことにより、ｉｄが１からｉｄ＿ｅｎｄの各電力データｃｔ＿ｉｄの総和がｇｒ＿ｃｔに得られる。ｇｒ＿ｃｔを集計値として集計暗号化電力量記憶部３３に記憶する（ステップＳ５０７）。

【００９４】

次に、ＭＤＭＳ３０がＥＭＳ５０に集計暗号化電力量を送信する処理の手順について、図１１を用いて説明する。図１１はＭＤＭＳ３０により実行される処理手順の一例を示すフローチャートである。

【００９５】

まず、電力使用量の集計を計算するグループの識別コード（ＳＭグループＩＤ）ｇｒ＿ｉｄを取得するとともに（ステップＳ６０１）、集計暗号化電力量記憶部３３に記憶されている集計暗号化電力量ｇｒ＿ｃｔと、対応する時刻情報ｔ＿２を取得する（ステップＳ６０２，Ｓ６０３）。取得したｇｒ＿ｉｄ、ｇｒ＿ｃｔ、ｔ＿２を組にしてＥＭＳ５０に送信する（ステップＳ６０４）。

【００９６】
なお、送信する情報はｇｒ＿ｉｄ、ｇｒ＿ｃｔ、ｔ＿２のみに限るものではない。例えば、ＭＤＭＳ３０を特定する情報を含めてもよい。
【００９７】
次に、初期起動時あるいはＥＭＳ５０による復号鍵要求の受信時に鍵管理サーバ７０が更新時刻を生成する処理の手順について図１２を用いて説明する。図１２は鍵管理サーバ７０により実行される処理手順の一例を示すフローチャートである。
【００９８】
鍵管理サーバ７０はまず時刻ｔ＿１を取得する（ステップＳ７０１）。固有情報記憶部に保存されている更新頻度ｔδと時刻ｔ＿１を用いて更新時刻ｔ＿ｕｐ＿ＫＭを生成する（ステップＳ７０２，Ｓ７０３）。生成されたｔ＿ｕｐ＿ＫＭは更新時刻として更新時刻記憶部７２に記憶される（ステップＳ７０４）。
【００９９】
次に、鍵管理サーバ７０が復号鍵を更新する処理の手順について図１３を用いて説明する。図１３は鍵管理サーバ７０により実行される処理手順の一例を示すフローチャートである。
【０１００】
まず、更新時刻記憶部３５に記憶されている更新時刻ｔ＿ｕｐ＿ＫＭと時刻情報ｔ＿１を取得し（ステップＳ８０１，Ｓ８０２）、ｔ＿１とｔ＿ｕｐ＿ＫＭの値の比較を行う（ステップＳ８０３）。ｔ＿１がｔ＿ｕｐ＿ＫＭより小さい場合には、更新が不要と判断し、更新処理を終了する。そうでない場合は処理を続行する。
【０１０１】
復号鍵の値を保持する変数ｓ＿ＫＭを０に設定し、復号鍵計算の準備を行う（ステップＳ８０４）。また、また、ｉｄに１を設定し、ループ変数を準備する（ステップＳ８０５）。
【０１０２】
次に、ｉｄに対応する秘密鍵ｋ＿ＳＭを取得する（ステップＳ８０６）。ｋ＿ＳＭとｔ＿ｕｐ＿ＫＭを用いてＨ１（ｋ＿ＳＭ，ｔ＿ｕｐ＿ＫＭ）を計算し、ｓ＿ＫＭに加算する（ステップＳ８０７）。Ｈ１（ｘ，ｙ）は、上述したようにｘとｙを入力とする一方向性関数あるいは鍵付きハッシュ関数である。ｉｄを１増やし、ｉｄの値がｉｄ＿ｅｎｄと等しくなるか調べ、等しくなるまでこれらの処理を繰り返す（ステップＳ８０８，Ｓ８０９）。ステップＳ８０１からＳ８０９の処理を行うことにより、ｉｄが１からｉｄ＿ｅｎｄのＳＭ１０を総合した復号鍵がｓ＿ＫＭに得られる。ｓ＿ＫＭを復号鍵として復号鍵記憶部７５に記憶する（ステップＳ８１０）。復号鍵ｓ＿ＫＭは更新時刻ｔ＿ｕｐ＿ＫＭに対応付けて記憶される（ステップＳ８１１）。
【０１０３】
次に、鍵管理サーバ７０が復号鍵をＥＭＳ５０に送信する手順について図１４を用いて説明する。図１４は鍵管理サーバ７０により実行される処理手順の一例を示すフローチャートである。
【０１０４】
まず、復号鍵ｓ＿ＫＭを復号鍵記憶部７５から取得する（ステップＳ９０１）。次に、ｓ＿ＫＭに対応する更新時刻ｔ＿ｕｐ＿ＫＭを取得する（ステップＳ９０２）。取得したｓ＿ＫＭ、ｔ＿ｕｐ＿ＫＭを組にしてＥＭＳ５０に送信する（ステップＳ９０３）。
【０１０５】
なお、送信する情報は復号鍵ｓ＿ＫＭと更新時刻ｔ＿ｕｐ＿ＫＭのみに限るものではない。例えば、鍵管理サーバ７０を特定する情報を含める。
【０１０６】
次に、ＥＭＳ５０が復号鍵と更新時刻を保存する処理手順について図１５を用いて説明する。図１５はＥＭＳ５０により実行される処理手順の一例を示すフローチャートである。

【０１０７】
まず、通信制御部５１で受信が行われた復号鍵ｓ＿ＫＭを取得する（ステップＳ１００１）。また、復号鍵ｓ＿ＫＭに対応する、通信制御部５１で受信が行われた更新時刻ｔ＿ｕｐ＿ＫＭを取得する（ステップＳ１００２）。次に、ｓ＿ＥＭＳにｓ＿ＫＭを代入し、復号鍵として復号鍵記憶部３７に記憶する（ステップＳ１００３，Ｓ１００４）。また、ｔ＿ｕｐ＿ＥＭＳにｔ＿ｕｐ＿ＫＭを代入し、更新時刻として更新時刻記憶部４５に記憶する（ステップＳ１００５，Ｓ１００６）。
【０１０８】
次に、ＥＭＳ５０が鍵管理サーバ７０に復号鍵を要求した際、鍵管理サーバ７０が返答する復号鍵をＥＭＳ５０が保存するまでの処理手順について図１６を用いて説明する。図１６は鍵管理サーバ７０とＥＭＳ５０により実行される処理手順の一例を示すフローチャートである。
【０１０９】
まず、ＥＭＳ５０は時刻情報ｔを取得する（ステップＳ１１０１）。ここで取得する時刻情報は現在時刻に限定するものではない。例えば、地域暗号化電力量記憶部に記憶されている暗号化電力量に対応付けられた時刻でもよい。
【０１１０】
次に、ＥＭＳ５０は、時刻情報ｔに対応する復号鍵を鍵管理サーバ７０に要求する（ステップＳ１１０２）。具体的には、通信制御部５１から時刻情報ｔと復号鍵を要求する旨のコマンドが鍵管理サーバ７０に送信される。
【０１１１】
鍵管理サーバ７０は受信した時刻情報ｔから更新時刻ｔ＿ｕｐ＿ＫＭを生成する（ステップＳ１１０３）。実際には、時刻ｔ＿１としてｔが用いられて、図１２に示されたフローチャートの処理が実行される。
【０１１２】
次に、鍵管理サーバ７０は更新時刻ｔ＿ｕｐ＿ＫＭに対応する復号鍵を生成する（ステップＳ１１０４）。実際には、時刻ｔ＿１としてｔが用いられて、図１３に示されたフローチャートの処理が実行される。
【０１１３】
次に、鍵管理サーバ７０はＥＭＳ５０に対し、更新時刻ｔ＿ｕｐ＿ＫＭと復号鍵ｓ＿ＫＭを送信する（ステップＳ１１０５）。ＥＭＳ５０は受信した復号鍵ｓ＿ＫＭと更新時刻ｔ＿ｕｐ＿ＫＭから得られる復号鍵と更新時刻をそれぞれ復号鍵記憶部５６と更新時刻記憶部５５に記憶する（ステップＳ１１０６）。実際には、図１１に示されたフローチャートの処理が実行される。
【０１１４】
次に、ＥＭＳ５０が暗号化された集計電力データを復号する処理手順について図１７を用いて説明する。図１７はＥＭＳ５０により実行される処理手順の一例を示すフローチャートである。
【０１１５】
まず、地域暗号化電力量記憶部５２から電力データｇｒ＿ｃｔを取得する（ステップＳ１２０１）。次に、ｇｒ＿ｃｔに対応付けられた時刻ｔ＿２を取得する（ステップＳ１２０２）。また、更新時刻記憶部５５から更新時刻ｔ＿ｕｐ＿ＥＭＳを取得する（ステップＳ１２０３）。
【０１１６】
取得したｔ＿２とｔ＿ｕｐ＿ＥＭＳの値を比較し、ｔ＿２がｔ＿ｕｐ＿ＥＭＳより小さい、または、ｔ＿２がｔ＿ｕｐ＿ＥＭＳ＋ｔδ以上の場合には、適切な復号鍵を保持していないと判断し、復号処理を終了する。終了した場合は、鍵管理サーバ７０に復号鍵を要求する処理を行い、再度復号処理を行う。
【０１１７】
次に、復号鍵記憶部５６から復号鍵ｓ＿ＥＭＳを取得する（ステップＳ１２０５）。ｇ

ｒ＿ｃｔからｓ＿ＥＭＳとＨ２（ｔ＿２）の積を減算した値をｇｒ＿ｄｔとする（ステップＳ１２０６）。ここで、Ｈ２（ｘ）は、上述したようにｘを入力とする一方向性関数あるいは鍵付きハッシュ関数である。地域電力データｇｒ＿ｄｔを地域電力量記憶部５３に記憶する（ステップＳ１２０７）。

【０１１８】

上述したように、本実施形態では、ＳＭ１０と鍵管理サーバ７０で秘密鍵を共有し、ＳＭ１０は秘密鍵を用いて暗号化鍵を定期的に更新して、暗号化鍵を用いて電力使用量の暗号データを生成して、ＭＤＭＳ３０に送信する。ＭＤＭＳ３０は、各ＳＭ１０からの暗号データを復号することなく、暗号データのままで集計する。これにより、ＭＤＭＳ３０に、各ＳＭの電力使用量が把握されるおそれがなくなり、ＭＤＭＳ３０を介した電力使用量の漏洩を防止できる。

また、ＭＤＭＳ３０が生成した電力使用総量の暗号データは、ＥＭＳ５０に送信され、ＥＭＳ５０は鍵管理サーバ７０から送られた復号鍵を用いて電力使用総量の暗号データを復号して、電力使用総量を検出する。このように、鍵管理サーバ７０が復号鍵を生成してＥＭＳ５０に送信するため、ＭＤＭＳ３０に鍵情報を送信しなくて済み、ＭＤＭＳ３０とＥＭＳ５０の間の通信が攻撃の対象になっても、電力使用量や電力使用総量が漏洩するおそれはなくなる。

【０１１９】

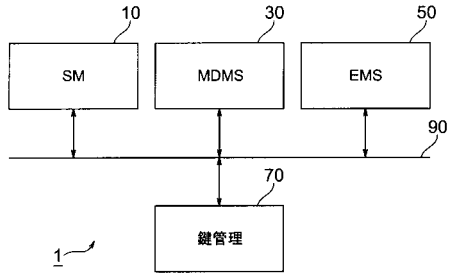
なお、以上説明した実施形態は、例として提示したものであり、発明の範囲を限定することは意図していない。上記の新規な実施形態は、その他の様々な形態で実施されることが可能であり、発明の要旨を逸脱しない範囲で、種々の省略、置き換え、変更を行うことができる。上記の実施形態やその変形は、発明の範囲や要旨に含まれるとともに、請求の範囲に記載された発明とその均などの範囲に含まれる。

【符号の説明】

【０１２０】

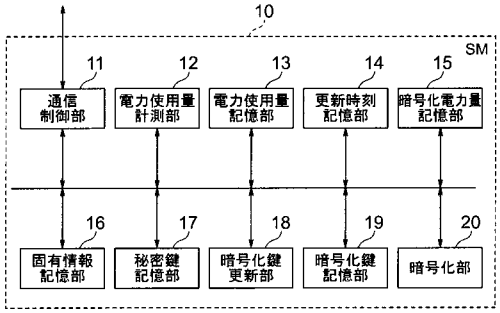
１０　ＳＭ、１１　通信制御部、１２　電力使用量計測部、１３　電力使用量記憶部、１４　更新時刻記憶部、１５　暗号化電力量記憶部、１６　固有情報記憶部、１７　秘密鍵記憶部、１８　暗号化鍵更新部、１９　暗号化鍵記憶部、２０　暗号化部、３０　ＭＤＭＳ、３１　通信制御部、３２　暗号化電力量記憶部、３３　集計暗号化電力量記憶部、３４　集計部、３５　固有情報記憶部、５０　ＥＭＳ、５１　通信制御部、５２　地域暗号化電力量記憶部、５３　地域電力量記憶部、５４　地域電力量制御部、５５　更新時刻記憶部、５６　復号鍵記憶部、５７　復号鍵更新部、５８　復号部、５９　固有情報記憶部、７０　鍵管理、７１　通信制御部、７２　更新時刻記憶部、７３　秘密鍵記憶部、７４　復号鍵更新部、７５　復号鍵記憶部、７６　固有情報記憶部、９０　ネットワーク

【図１】



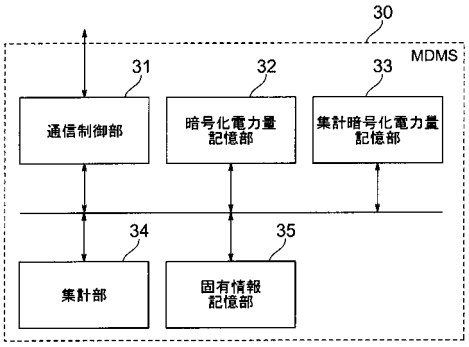
電力使用量計算システムの構成例

【図２】



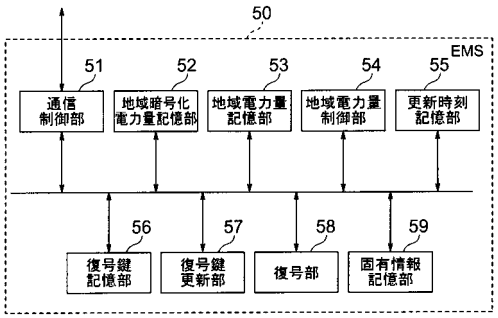
SMの機能的構成

【図３】



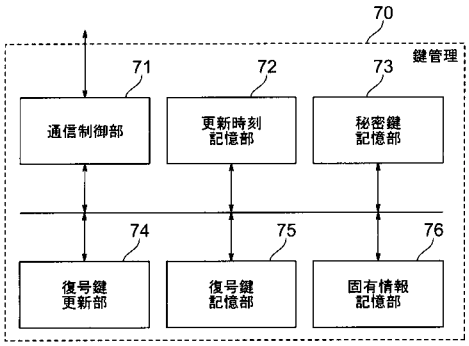
MDMSの機能的構成

【図４】



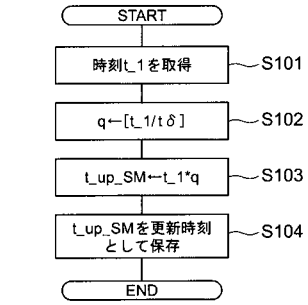
EMSの機能的構成

【図５】



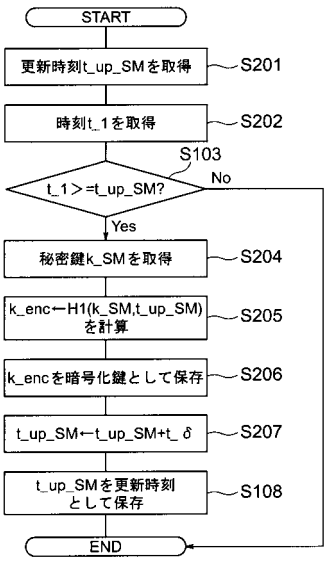
鍵管理サーバの機能的構成

【図６】



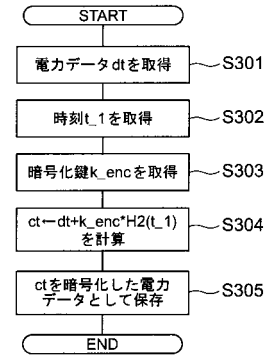
SM内における初期更新時刻生成処理

【図７】



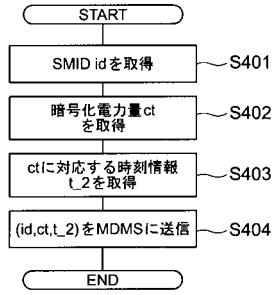
SMの暗号化鍵更新処理

【図８】



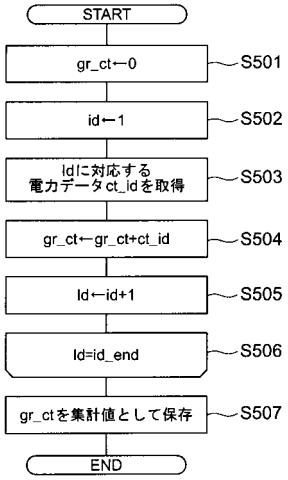
SMの暗号データ生成処理

【図９】



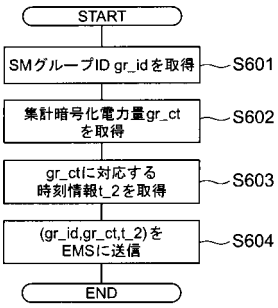
SM内の暗号化電力データ送信処理

【図１０】



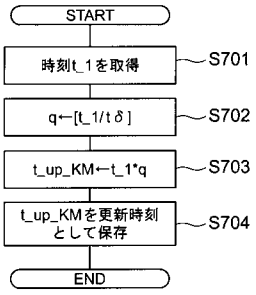
MDMSの暗号化電力データ集計処理

【図１１】



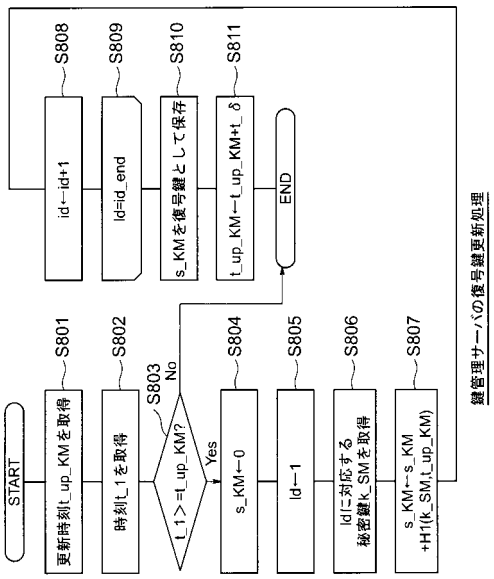
MDMSの暗号化電力データ送信処理

【図１２】

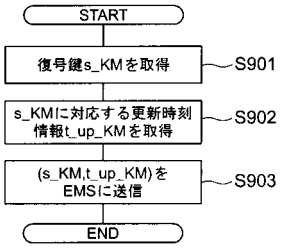


鍵管理サーバの初期更新時刻生成処理

【図１３】

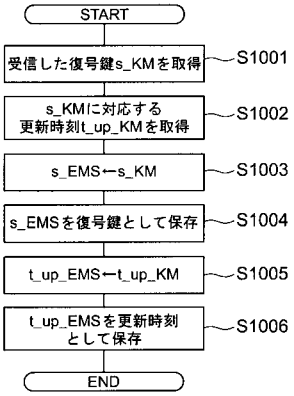


【図１４】



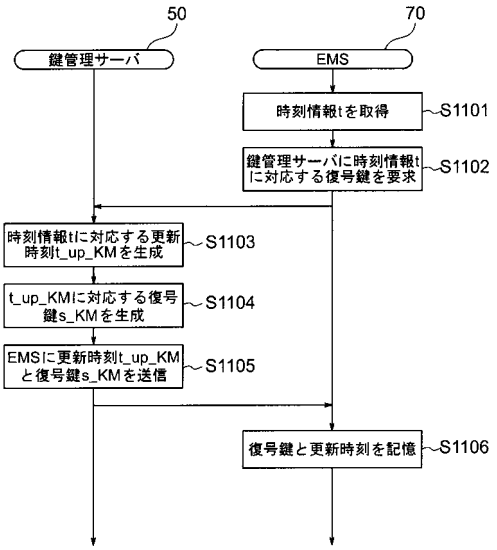
鍵管理サーバの復号鍵送信処理

【図１５】



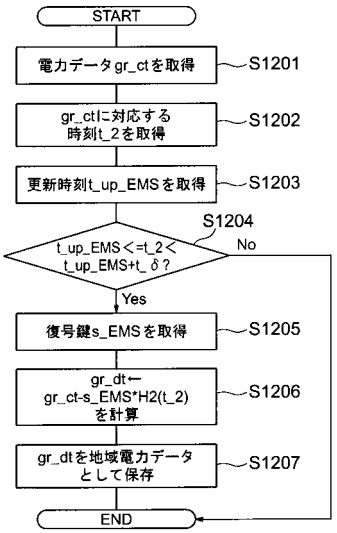
EMSの復号鍵と更新時刻の保存処理

【図１６】



復号鍵送信要求処理

【図１７】



EMSの集計電力データ復号処理

フロントページの続き

(72)発明者 山 中 晋 爾
東京都港区芝浦一丁目１番１号 株式会社東芝内
(72)発明者 花 谷 嘉 一
東京都港区芝浦一丁目１番１号 株式会社東芝内
(72)発明者 高 橋 俊 成
東京都港区芝浦一丁目１番１号 株式会社東芝内
(72)発明者 駒 野 雄 一
東京都港区芝浦一丁目１番１号 株式会社東芝内

Ｆターム(参考) 5J104 AA34 EA23 NA02 NA37