

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第5446922号
(P5446922)

(45) 発行日 平成26年3月19日(2014.3.19)

(24) 登録日 平成26年1月10日(2014.1.10)

(51) Int.Cl.		F I			
HO2J	13/00	(2006.01)	HO2J	13/00	301A
GO6Q	50/00	(2012.01)	GO6Q	50/00	
HO4L	9/32	(2006.01)	HO4L	9/00	675B
HO4Q	9/00	(2006.01)	HO4Q	9/00	301A
HO4M	11/00	(2006.01)	HO4M	11/00	301

請求項の数 7 (全 123 頁)

(21) 出願番号 特願2010-13672 (P2010-13672)
 (22) 出願日 平成22年1月25日(2010.1.25)
 (65) 公開番号 特開2011-155709 (P2011-155709A)
 (43) 公開日 平成23年8月11日(2011.8.11)
 審査請求日 平成25年1月10日(2013.1.10)

(73) 特許権者 000002185
 ソニー株式会社
 東京都港区港南1丁目7番1号
 (74) 代理人 100095957
 弁理士 亀谷 美明
 (74) 代理人 100096389
 弁理士 金本 哲男
 (74) 代理人 100101557
 弁理士 萩原 康司
 (74) 代理人 100128587
 弁理士 松本 一騎
 (72) 発明者 松田 誠一
 東京都港区港南1丁目7番1号 ソニー株式会社内

最終頁に続く

(54) 【発明の名称】 電力管理装置、電子機器及び電子機器登録方法

(57) 【特許請求の範囲】

【請求項1】

電力網に接続された電子機器を認証し、認証に成功した機器を管理機器として登録する管理機器登録部と、

前記管理機器の動作及び前記管理機器への電力供給を制御する制御部と、
 を備え、

前記管理機器登録部は、

他の電力管理装置に登録されている電子機器が電力網に接続されると、当該電子機器から、前記他の電力管理装置によって前記電子機器に固有の識別情報に対して付与されたデジタル署名と、前記他の電力管理装置に固有の識別情報とを取得し、

前記他の電力管理装置によって付与されたデジタル署名の検証に成功した場合に、前記他の電力管理装置に登録されている電子機器を、一時的に登録する、電力管理装置。

【請求項2】

前記電力管理装置は、前記他の電力管理装置に登録されている電子機器が生成する、一時的に登録された電力管理装置から電力供給を受けた旨を証明する電力使用証明書を管理する電力使用証明書管理部を更に備え、

前記電力使用証明書管理部は、

前記制御部が一時的に登録された電子機器に対して電力供給を行った場合に、当該一時的に登録された電子機器から前記電力使用証明書を取得し、

取得した前記電力使用証明書に対してデジタル署名を付与した後に、電力使用の課金を

行う外部サーバに対して、デジタル署名を付与した前記電力使用証明書を送信する、請求項 1 に記載の電力管理装置。

【請求項 3】

前記電力管理装置が前記電子機器から電力供給を受けた場合、前記電力使用証明書管理部は、電力供給を受けた前記電子機器に対して、電子機器から電力供給を受けた旨を照明する電力使用証明書を生成する、請求項 2 に記載の電力管理装置。

【請求項 4】

自装置に固有の識別情報、及び、所定の認証局により認証されたデジタル署名を保持する記憶部と、

前記記憶部に格納された前記デジタル署名を利用して自装置への給電を管理する電力管理装置との間で認証処理を行い、自装置を前記電力管理装置に登録する認証処理部と、を備え、

前記認証処理部は、自装置が前記電力管理装置に登録された場合に、登録された前記電力管理装置から、当該電力管理装置に固有の識別情報と、自装置に固有の識別情報に対して前記電力管理装置が付与したデジタル署名と、を取得する、電子機器。

【請求項 5】

前記認証処理部は、自装置が登録されている前記電力管理装置以外の電力管理装置に対して一時的な登録を要請する場合に、前記自装置が登録されている電力管理装置から取得した前記デジタル署名を、一時的な登録を要請する電力管理装置に対して送信する、請求項 4 に記載の電子機器。

【請求項 6】

前記電子機器は、一時的に登録された前記電力管理装置から電力供給を受けた場合に、一時的に登録された電力管理装置から電力供給を受けた旨を証明する電力使用証明書を生成する制御部を更に備える、請求項 5 に記載の電子機器。

【請求項 7】

電力網に接続された電子機器を認証し、認証に成功した機器を管理機器として電力管理装置に登録するステップを含み、

前記電子機器を登録するステップでは、

前記電子機器が保持する所定の認証局により認証されたデジタル署名を利用して認証処理が行われ、

前記電子機器が前記電力管理装置に登録された場合に、前記電力管理装置から前記電子機器へ、当該電力管理装置に固有の識別情報と、電子機器に固有の識別情報に対して前記電力管理装置が付与したデジタル署名とが送信され、

他の電力管理装置に登録されている電子機器が電力網に接続されると、当該電子機器から、前記他の電力管理装置によって前記電子機器に固有の識別情報に対して付与されたデジタル署名と、前記他の電力管理装置に固有の識別情報とを取得し、

前記他の電力管理装置によって付与されたデジタル署名の検証に成功した場合に、前記他の電力管理装置に登録されている電子機器を、一時的に登録する、電子機器登録方法。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、電力管理装置、電子機器及び電子機器登録方法に関する。

【背景技術】

【0002】

近年、スマートグリッドと呼ばれる技術に注目が集まっている。このスマートグリッドとは、送電網に通信路を併せ持つ新たな送電網を構築し、このインテリジェントな送電網を利用して効率的な電力利用を実現するための技術的な枠組みのことを言う。スマートグリッド構想の背景には、電力使用量の効率的な管理、事故発生時の迅速対応、使用電力量の遠隔制御、電力会社の管理外にある発電設備を用いた分散発電、電動移動体の充電管理

10

20

30

40

50

等を実現したいという要望がある。特に、一般家庭や電力会社以外の事業者による再生可能エネルギーを用いた自家発電設備の有効利用、及び電気自動車に代表される種々の電動移動体の充電管理には大きな注目が集まっている。なお、再生可能エネルギーとは、化石燃料を用いずに生成されるエネルギーのことである。

【0003】

一般家庭や電力以外の事業者により発電された電力は、発電者自身が利用する。また、発電者自身が利用した後で余った電力は、現在、電力会社を買電している。しかし、電力会社にとって、管理外の発電設備から供給される電力を買電することは大きな負担となっている。例えば、太陽光発電設備から供給される電力量は天候に左右される。また、一般家庭の自家発電設備から供給される電力量は日毎に大きく変化する一般家庭の電力使用量に左右される。そのため、電力会社が管理外の発電設備から安定した電力供給を受けることは難しい。こうした理由から、将来、電力会社による買電が難しくなる可能性がある。

10

【0004】

そこで、最近では、電力会社の管理外にある発電設備で発電された電力を一旦バッテリーに蓄電して利用するホームバッテリー構想に注目が集まっている。例えば、太陽光発電設備で発電した電力をバッテリーに蓄電しておき、夜間や天候不良の際に不足分をバッテリーから補うといった利用方法が考案されている。さらに、バッテリーの蓄電量に応じて電力会社から給電を受ける電力量を制限したり、価格の安い夜間に電力会社から電力供給を受けてバッテリーに蓄電し、価格の高い昼間にバッテリーに蓄電した電力を利用したりする方法等が考案されている。また、バッテリーは直流のまま電力を蓄えることができるため、送電の際に行われるDC/AC変換、AC/DC変換が不要になり、変換時のロス削減できる。

20

【0005】

このように、スマートグリッド構想の中で電力管理に関する様々な思惑が交錯している。こうした電力管理を実現するため、スマートグリッド構想の中では送電網に通信路を併せ持つことが前提とされている。つまり、このインテリジェントな送電網を利用して電力管理に関する情報をやり取りすることが想定されているのである(例えば、以下の特許文献1を参照)。但し、通信インフラが既に整備されている地域においては、送電網を通信路として用いず、既に敷設されている通信インフラで構築されたネットワークを利用して電力管理に関する情報のやり取りが行われてもよい。つまり、スマートグリッド構想において重要なのは、一元管理されていない発電設備及び蓄電設備を如何にして効率よく管理するかということである。

30

【先行技術文献】

【特許文献】

【0006】

【特許文献1】特開2002-354560号公報

【非特許文献】

【0007】

【非特許文献1】D. Naccache et al., "Can D.S.A be improved? Complexity trade-offs with the digital signature standard," Proceedings of Eurocrypt 94, Lecture Notes in Computer Science Vol. 950, Springer-Verlag, 1994.

40

【非特許文献2】M. Bellare et al., "Fast Batch Verification for Modular Exponentiation and Digital Signatures," Proceedings of Eurocrypt 98, Lecture Notes in Computer Science Vol. 1403, Springer-Verlag, 1998.

【非特許文献3】D. Boneh et al., "Aggregate and Verifiably Encrypted Signatures from Bili

50

near Maps , " Proceedings Eurocrypt 2003 , Lecture Notes in Computer Science Vol . 2656 , Springer - Verlag , 2003 .

【非特許文献4】D. Boneh et al . , " A Survey of Two Signature Aggregation Techniques , " Crypt oBytes Vol . 6 , No . 2 , 2003 .

【発明の概要】

【発明が解決しようとする課題】

【0008】

ところで、実際の生活において、ある電子機器を例えば自宅から自宅外へと持ち出して利用するといったように、ある電子機器がユーザの移動とともにあらゆる場所へと移動する場合も生じうる。したがって、先に説明したようなスマートグリッド構想の中で、ある装置によって電力管理が行われている電子機器を、一時的に、電力管理を行う別の装置に接続したいという場合も生じうるであろう。

10

【0009】

しかしながら、上述のような、ある装置に電力管理されている電子機器を、一時的に他の装置に登録するような仕組みは、未だ提案されていない。

【0010】

そこで、本発明は、上記問題に鑑みてなされたものであり、本発明の目的とするところは、ある装置に電力管理されている電子機器を、一時的に他の装置に登録することが可能な、電力管理装置、電子機器及び電子機器登録方法を提供することにある。

20

【課題を解決するための手段】

【0011】

上記課題を解決するために、本発明のある観点によれば、電力網に接続された電子機器を認証し、認証に成功した機器を管理機器として登録する管理機器登録部と、前記管理機器の動作及び前記管理機器への電力供給を制御する制御部と、を備え、前記管理機器登録部は、他の電力管理装置に登録されている電子機器が電力網に接続されると、当該電子機器から、前記他の電力管理装置によって前記電子機器に固有の識別情報に対して付与されたデジタル署名と、前記他の電力管理装置に固有の識別情報とを取得し、前記他の電力管理装置によって付与されたデジタル署名の検証に成功した場合に、前記他の電力管理装置に登録されている電子機器を、一時的に登録する、電力管理装置が提供される。

30

【0012】

前記電力管理装置は、前記他の電力管理装置に登録されている電子機器が生成する、一時的に登録された電力管理装置から電力供給を受けた旨を証明する電力使用証明書を管理する電力使用証明書管理部を更に備え、前記電力使用証明書管理部は、前記制御部が一時的に登録された電子機器に対して電力供給を行った場合に、当該一時的に登録された電子機器から前記電力使用証明書を取得し、取得した前記電力使用証明書に対してデジタル署名を付与した後に、電力使用の課金を行う外部サーバに対して、デジタル署名を付与した前記電力使用証明書を送信してもよい。

【0013】

前記電力管理装置が前記電子機器から電力供給を受けた場合、前記電力使用証明書管理部は、電力供給を受けた前記電子機器に対して、電子機器から電力供給を受けた旨を照明する電力使用証明書を生成してもよい。

40

【0014】

上記課題を解決するために、本発明の別の観点によれば、自装置に固有の識別情報、及び、所定の認証局により認証されたデジタル署名を保持する記憶部と、前記記憶部に格納された前記デジタル署名を利用して自装置への給電を管理する電力管理装置との間で認証処理を行い、自装置を前記電力管理装置に登録する認証処理部と、を備え、前記認証処理部は、自装置が前記電力管理装置に登録された場合に、登録された前記電力管理装置から、当該電力管理装置に固有の識別情報と、自装置に固有の識別情報に対して前記電力管理

50

装置が付与したデジタル署名と、を取得する、電子機器が提供される。

【0015】

前記認証処理部は、自装置が登録されている前記電力管理装置以外の電力管理装置に対して一時的な登録を要請する場合に、前記自装置が登録されている電力管理装置から取得した前記デジタル署名を、一時的な登録を要請する電力管理装置に対して送信してもよい。

【0016】

前記電子機器は、一時的に登録された前記電力管理装置から電力供給を受けた場合に、一時的に登録された電力管理装置から電力供給を受けた旨を証明する電力使用証明書を生成する制御部を更に備えてもよい。

10

【0017】

上記課題を解決するために、本発明の更に別の観点によれば、電力網に接続された電子機器を認証し、認証に成功した機器を管理機器として電力管理装置に登録するステップを含み、前記電子機器に登録するステップでは、前記電子機器が保持する所定の認証局により認証されたデジタル署名を利用して認証処理が行われ、前記電子機器が前記電力管理装置に登録された場合に、前記電力管理装置から前記電子機器へ、当該電力管理装置に固有の識別情報と、電子機器に固有の識別情報に対して前記電力管理装置が付与したデジタル署名とが送信され、他の電力管理装置に登録されている電子機器が電力網に接続されると、当該電子機器から、前記他の電力管理装置によって前記電子機器に固有の識別情報に対して付与されたデジタル署名と、前記他の電力管理装置に固有の識別情報とを取得し、前記他の電力管理装置によって付与されたデジタル署名の検証に成功した場合に、前記他の電力管理装置に登録されている電子機器を、一時的に登録する、電子機器登録方法が提供される。

20

【発明の効果】

【0018】

以上説明したように本発明によれば、ある電力管理装置に電力管理されている電子機器を、一時的に他の電力管理装置に登録することが可能となる。

【図面の簡単な説明】

【0019】

【図1】本発明の実施形態に係る電力管理システムの全体像を説明するための説明図である。

30

【図2】管理対象ブロックの全体構成を説明するための説明図である。

【図3】局所電力管理システム内の通信網について説明するための説明図である。

【図4】電力管理装置を中心としたシステム構成を説明するための説明図である。

【図5】外部サーバの具体例について説明するための説明図である。

【図6】システム管理サーバの一機能について説明するための説明図である。

【図7】本発明の実施形態に係る電力管理装置の機能構成について説明するための説明図である。

【図8】情報管理部の詳細な機能構成について説明するための説明図である。

【図9】情報管理部の詳細な機能構成について説明するための説明図である。

40

【図10】表示部に表示される内容について説明するための説明図である。

【図11】表示部に表示される内容について説明するための説明図である。

【図12】表示部に表示される内容について説明するための説明図である。

【図13】表示部に表示される内容について説明するための説明図である。

【図14】電力消費量の時系列パターンについて説明するための説明図である。

【図15】電力消費量の時系列パターンについて説明するための説明図である。

【図16】電力消費パターンの秘匿方法について説明するための説明図である。

【図17】電力消費パターンの秘匿方法について説明するための説明図である。

【図18】電力消費パターンの秘匿方法について説明するための説明図である。

【図19】電力管理装置が実施する各種制御について説明するための説明図である。

50

- 【図20】電力管理装置が管理している各種情報を説明するための説明図である。
- 【図21】端子の形態及び接続機器の形態に応じた通信手段、認証手段、給電制御の組み合わせを示した説明図である。
- 【図22】機器管理部の構成を説明するためのブロック図である。
- 【図23】管理機器登録部の構成を説明するためのブロック図である。
- 【図24】情報改ざん検知部の構成を説明するためのブロック図である。
- 【図25】情報分析部の構成を説明するためのブロック図である。
- 【図26】制御化機器の構成を説明するためのブロック図である。
- 【図27】制御化機器の制御部の構成を説明するためのブロック図である。
- 【図28】制御化機器の制御部の構成を説明するためのブロック図である。 10
- 【図29】改ざん検知情報生成部の構成を説明するためのブロック図である。
- 【図30】蓄電装置の構成を説明するためのブロック図である。
- 【図31】蓄電装置の制御部の構成を説明するためのブロック図である。
- 【図32】蓄電装置の制御部の構成を説明するためのブロック図である。
- 【図33】改ざん検知情報生成部の構成を説明するためのブロック図である。
- 【図34】電力管理装置の登録方法について説明するための流れ図である。
- 【図35】電力管理装置の登録方法の具体例を説明するための流れ図である。
- 【図36】制御化機器の登録方法について説明するための流れ図である。
- 【図37】制御化機器の登録方法の具体例を説明するための流れ図である。
- 【図38】制御化機器の登録方法の具体例を説明するための流れ図である。 20
- 【図39】制御化端子の登録方法について説明するための流れ図である。
- 【図40】一時的に登録された制御化機器の課金処理について説明するための説明図である。
- 【図41】一時的に登録された制御化機器の課金処理を説明するための流れ図である。
- 【図42】制御化機器の登録方法の変形例を説明するための説明図である。
- 【図43】制御化機器の登録方法の変形例を説明するための説明図である。
- 【図44】制御化機器の登録方法の変形例を説明するための説明図である。
- 【図45】制御化機器の登録方法の変形例を説明するための説明図である。
- 【図46】制御化機器の登録方法の変形例を説明するための説明図である。
- 【図47】制御化機器の登録方法の変形例を説明するための説明図である。 30
- 【図48】制御化機器の登録方法の変形例を説明するための流れ図である。
- 【図49】異常の発生した管理機器に対する電力管理装置の動作を説明するための流れ図である。
- 【図50】異常の発生した管理機器に対する電力管理装置の動作を説明するための流れ図である。
- 【図51】異常の発生した管理機器に対する電力管理装置の動作を説明するための流れ図である。
- 【図52】異常の発生した管理機器に対する電力管理装置の動作を説明するための流れ図である。
- 【図53】電力状態に異常が発生した場合における電力管理装置の動作を説明するための流れ図である。 40
- 【図54】電力状態に異常が発生した場合における電力管理装置の動作を説明するための流れ図である。
- 【図55】電子透かし情報の埋め込み方法を説明するための流れ図である。
- 【図56】電子透かし情報の検証方法を説明するための流れ図である。
- 【図57】電子透かし情報の埋め込み方法を説明するための流れ図である。
- 【図58】電子透かし情報の検証方法を説明するための流れ図である。
- 【図59】解析サーバの構成を説明するためのブロック図である。
- 【図60】解析サーバが有する情報改ざん検知部の構成を説明するためのブロック図である。 50

- 【図 6 1】解析サーバが有する第 1 検証部の構成を説明するためのブロック図である。
- 【図 6 2】解析サーバが有する第 2 検証部の構成を説明するためのブロック図である。
- 【図 6 3】排除すべきバッテリーについて説明するための説明図である。
- 【図 6 4】電力管理装置への不正攻撃に対する防御方法を説明するための流れ図である。
- 【図 6 5】バッテリーの排除方法について説明するための流れ図である。
- 【図 6 6 A】解析サーバの取得データ検証部における検証処理を説明するための流れ図である。
- 【図 6 6 B】解析サーバの取得データ検証部における検証処理を説明するための流れ図である。
- 【図 6 7】第 1 検証部による検証処理を説明するための流れ図である。 10
- 【図 6 8】データベース管理部における検査処理を説明するための流れ図である。
- 【図 6 9】データベース管理部におけるデータベースの更新及び判定辞書の生成について説明するための説明図である。
- 【図 7 0】ウィルス定義ファイル管理部によるウィルス定義ファイルの管理方法を説明するための流れ図である。
- 【図 7 1 A】取得データ検証部が実施する排除すべきバッテリーの特定方法を説明するための流れ図である。
- 【図 7 1 B】取得データ検証部が実施する排除すべきバッテリーの特定方法を説明するための流れ図である。
- 【図 7 1 C】取得データ検証部が実施する排除すべきバッテリーの特定方法を説明するための流れ図である。 20
- 【図 7 2】取得データ検証部が実施する排除すべきバッテリーの特定方法を説明するための流れ図である。
- 【図 7 3】多重化された電力管理装置の動作フローを説明するための説明図である。
- 【図 7 4】多重化された電力管理装置の動作フローを説明するための説明図である。
- 【図 7 5】多重化された電力管理装置の動作フローを説明するための説明図である。
- 【図 7 6】電力管理装置が有するサービス提供部の構成を説明するためのブロック図である。
- 【図 7 7】電力管理装置が有するサービス提供部の構成を説明するためのブロック図である。 30
- 【図 7 8】電力管理装置が有するデータベースとの連携について説明するための説明図である。
- 【図 7 9】システム連動エンタテインメントのセキュリティについて説明するための説明図である。
- 【図 8 0】システム連動エンタテインメントの流れを説明するための流れ図である。
- 【図 8 1 A】システム連動エンタテインメントの流れを説明するための流れ図である。
- 【図 8 1 B】システム連動エンタテインメントの流れを説明するための流れ図である。
- 【図 8 2】本発明の実施形態に係る電力管理装置のハードウェア構成を説明するためのブロック図である。
- 【発明を実施するための形態】 40
- 【0020】
- 以下に添付図面を参照しながら、本発明の好適な実施の形態について詳細に説明する。なお、本明細書及び図面において、実質的に同一の機能構成を有する構成要素については、同一の符号を付することにより重複説明を省略する。
- 【0021】
- なお、説明は、以下の順序で行うものとする。
- (1) 第 1 の実施形態
- (1-1) 電力管理システムの全体像について
- (1-2) 電力管理装置の構成について
- (1-3) 表示部に表示される内容について 50

- (1 - 4) 消費電力パターンの秘匿について
- (1 - 5) 電力管理装置が行う各種制御について
- (1 - 6) 機器管理部の構成について
- (1 - 7) 情報分析部の構成について
- (1 - 8) 制御化機器の構成について
- (1 - 9) 蓄電装置の構成について
- (1 - 10) 電子透かし情報の埋め込み方法及び検証方法の具体例
- (1 - 11) 電力管理装置の登録方法について
- (1 - 12) 制御化機器の登録方法について
- (1 - 13) 制御化端子の登録方法について 10
- (1 - 14) 一時的に登録された制御化機器の課金処理について
- (1 - 15) 制御化機器の登録方法の変形例について
- (1 - 16) 異常の発生した管理機器に対する電力管理装置の動作について
- (1 - 17) 電力状態に異常が発生した場合における電力管理装置の動作
- (1 - 18) 電子透かし情報の埋め込み方法及び検証方法の流れについて
- (1 - 19) 解析サーバが果たす役割について
- (1 - 20) 解析サーバの構成について
- (1 - 21) 排除すべきバッテリーの特定処理について
- (1 - 22) 電力管理装置への不正攻撃に対する防御方法について
- (1 - 23) バッテリーの排除方法について 20
- (1 - 24) 取得データ検証部における検証処理について
- (1 - 25) 第 1 検証部による検証処理の流れについて
- (1 - 26) データベース管理部における検査処理について
- (1 - 27) データベースの更新と判定辞書の生成について
- (1 - 28) ウィルス定義ファイルの管理方法について
- (1 - 29) 排除すべきバッテリーの特定方法の流れについて
- (1 - 30) 複数の電力管理装置が存在する場合の処理について
- (2) 第 2 の実施形態
 - (2 - 1) 第 2 実施形態の概要について
 - (2 - 2) サービス提供部の構成について 30
 - (2 - 3) データベースとの連携について
 - (2 - 4) システム連動エンタテインメントのセキュリティについて
 - (2 - 5) システム連動エンタテインメントの流れについて
- (3) 本発明の各実施形態に係る電力管理装置のハードウェア構成について
- 【 0 0 2 2 】
- (第 1 の実施形態)
- < 電力管理システムの全体像について >
- まず、本発明の第 1 の実施形態に係る電力管理システムの全体像について説明する。
- 【 0 0 2 3 】
- 図 1 は、本実施形態に係る電力管理システムの全体像を示している。 40
- 図 1 に示すように、本実施形態に係る電力管理システムは、局所電力管理システム 1、広域ネットワーク 2、外部サーバ 3、電力情報収集装置 4、電力供給者システム 5、端末装置 6、電力取引システム 7 を含む。また、局所電力管理システム 1、外部サーバ 3、電力情報収集装置 4、電力供給者システム 5、端末装置 6、電力取引システム 7 は、広域ネットワーク 2 に接続されているため、相互に情報をやり取りすることができる。
- 【 0 0 2 4 】
- なお、本稿において「局所」「広域」という表現を用いるが、「局所」とは、広域ネットワーク 2 を介さずに通信可能な要素で構成された小規模なグループを意味する。一方、「広域」とは、広域ネットワーク 2 を介して通信する要素を含んだ大規模なグループを意味する。また、局所電力管理システム 1 の内部に配置された要素で構成される小規模なグ 50

ループのことを特に「局所」という表現で表すことがある。一方、図1に示した電力管理システムの全体を「広域」という表現で表すことがある。

【0025】

さて、上記の電力管理システムは、先に述べたスマートグリッド構想と同様に電力利用の効率化を企図し、電力を利用して動作する様々な機器、電力を蓄える蓄電手段、電力を発生させる発電手段、電源から電力を供給する給電手段等を適切に管理するものである。この電力管理システムにおける電力の管理対象は、局所電力管理システム1の内部に設けられた機器、蓄電手段、発電手段、給電手段等である。なお、スマートグリッド構想においてHEMS(Home Energy Management System)、或いは、BEMS(Building Energy Management System)と呼ばれるシステムは、局所電力管理システム1の一例である。

10

【0026】

図1に示すように、局所電力管理システム1は、電力管理装置11、及び管理対象ブロック12を含む。電力管理装置11は、局所電力管理システム1の内部に設けられた機器、蓄電手段、発電手段、給電手段等を管理する役割を担う。例えば、電力管理装置11は、各機器に対する電力の供給を許可したり、禁止したりする。また、電力管理装置11は、各機器を特定したり、各機器の正当性を確認したりするために各機器に対する認証を実施する。そして、電力管理装置11は、各機器から消費電力量等の情報を収集する。

【0027】

また、電力管理装置11は、蓄電手段から蓄電量等の情報を取得する。そして、電力管理装置11は、蓄電手段に対する充放電の制御を実施する。さらに、電力管理装置11は、発電手段から発電量等の情報を取得する。また、電力管理装置11は、外部から供給された電力量の情報を給電手段から取得する。このように、電力管理装置11は、局所電力管理システム1の内部に設けられた機器、蓄電手段、発電手段、給電手段から情報を取得したり、電力の入出力を制御したりする。もちろん、電力管理装置11は、機器、蓄電手段、発電手段、給電手段以外の構成要素に対しても必要に応じて同様の管理を実施する。また、電力管理装置11は、電力だけでなく、CO₂、水資源等といった削減値の情報化が可能なエコ全般について、管理を行うことも可能である。すなわち、電力管理装置11は、エコ管理装置として機能することも可能である。なお、以下では、削減値の情報化が可能な資源の例として電力を例にとって説明する。

20

30

【0028】

図1に示した局所電力管理システム1において、電力管理の対象となる機器、蓄電手段、発電手段、給電手段等の構成要素は、管理対象ブロック12に含まれる。管理対象ブロック12に含まれる構成要素と電力管理装置11は、直接的又は間接的に情報をやり取りできる。また、電力管理装置11は、電力情報収集装置4と情報をやり取りできるように構成されていてもよい。電力情報収集装置4は、電力供給者が管理する電力供給者システム5から供給される電力の情報を管理するものである。なお、スマートグリッド構想においてスマートメータと呼ばれる装置は、電力情報収集装置4の一例である。

【0029】

電力供給者システム5は、個々の局所電力管理システム1に対して電力を供給する。そして、電力供給者システム5から供給された電力は、電力情報収集装置4を介して局所電力管理システム1内の管理対象ブロック12に供給される。このとき、電力情報収集装置4は、管理対象ブロック12に供給した電力量等の情報を取得する。そして、電力情報収集装置4は、取得した電力量等の情報を電力供給者システム5に送信する。このような仕組みを利用して、電力供給者システム5は、個々の局所電力管理システム1にある管理対象ブロック12の消費電力量等に関する情報を収集する。

40

【0030】

また、電力供給者システム5は、収集した消費電力量等の情報を参照し、電力情報収集装置4を制御して、個々の管理対象ブロック12、或いは、電力管理システム全体における電力利用が効率化されるように電力の供給量を制御する。このとき、電力情報収集装置

50

4 は、管理対象ブロック 1 2 に対して電力供給者システム 5 から供給される電力量を抑制したり、管理対象ブロック 1 2 の電力消費量に応じて電力量の抑制を解除したりする。なお、電力供給者としては、例えば、電力会社や、個人又は法人で発電施設を所有する発電管理者、或いは、個人又は法人で蓄電施設を所有する蓄電管理者等が考えられる。

【 0 0 3 1 】

ただし、現状では電力会社が電力供給者となる場合が多いため、本稿においては電力会社が電力供給者となる場合を想定して説明を進める。また、外部から供給される電力は、現状、電力供給者である電力会社から購入する 경우가圧倒的に多い。しかし、今後、電力取引市場が活性化し、電力取引市場において購入した電力が、外部から供給される電力の主流を占めることになるかもしれない。このような場合、局所電力管理システム 1 は、図 1 に示すように、電力取引システム 7 から電力の供給を受けることになると考えられる。

【 0 0 3 2 】

電力取引システム 7 は、電力取引市場における売り注文 / 買い注文の受付、注文確定後の価格算定、決済処理、給電の発注等、電力取引に関わる処理を実施するものである。また、図 1 の例では、電力取引市場において注文が確定した電力の受給も、電力取引システム 7 が実施する。そのため、図 1 の例では、確定した注文の種類に応じて、局所電力管理システム 1 に対して電力取引システム 7 から電力が供給されたり、局所電力管理システム 1 から電力取引システム 7 へと電力が供給されたりする。また、電力取引システム 7 に対する注文の申し入れは、電力管理装置 1 1 を利用して自動又は手動で行われる。

【 0 0 3 3 】

また、図 1 に示した電力管理システムは、複数の局所電力管理システム 1 を含む。上記の通り、個々の局所電力管理システム 1 は、電力管理装置 1 1 を有する。そして、複数の電力管理装置 1 1 は、広域ネットワーク 2、或いは、セキュアな通信路（非図示）を介して相互に情報をやり取りすることができる。また、一方の局所電力管理システム 1 から他方の局所電力管理システム 1 へと電力を供給する仕組みが設けられていてもよい。この場合、両システムの電力管理装置 1 1 は、互いに電力の受給に関する情報交換を実施し、この情報交換の中で適宜決定された電力量を一方から他方へと送信するように制御する。

【 0 0 3 4 】

ところで、電力管理装置 1 1 は、広域ネットワーク 2 を介して接続された外部の端末装置 6 から操作できるように構成されていてもよい。例えば、ユーザは、端末装置 6 を利用して、自身が管理する局所電力管理システム 1 の電力状況を確認したい場合があるかもしれない。このような場合、電力管理装置 1 1 を端末装置 6 から操作できるように構成しておく、ユーザは、端末装置 6 に自身が管理する局所電力管理システム 1 の電力状況を表示させ、その電力状況を確認することが可能になる。また、ユーザは、端末装置 6 を利用して電力管理装置 1 1 による電力取引を行うことができるようになる。

【 0 0 3 5 】

なお、端末装置 6 は、局所電力管理システム 1 の内部に設けられていてもよい。この場合、端末装置 6 は、広域ネットワーク 2 を介さず、局所電力管理システム 1 の内部にある通信路を利用して電力管理装置 1 1 に接続する。端末装置 6 を利用する利点の 1 つは、電力管理装置 1 1 が設置された場所にユーザが足を運ばずに済む点にある。つまり、端末装置 6 が利用できれば、任意の場所から電力管理装置 1 1 を操作できるようになる。なお、端末装置 6 の具体的な形態としては、例えば、携帯電話、携帯情報端末、ノート型コンピュータ、携帯型ゲーム機、情報家電、ファクシミリ、固定電話機、音声・映像機器、カーナビゲーションシステム、電動移動体等が考えられる。

【 0 0 3 6 】

ここまで、図 1 に示した電力管理システムにおける電力管理について、各構成要素の動作や機能を交えながら簡単に説明してきた。しかし、上記の電力管理装置 1 1 は、電力管理に関する機能の他、管理対象ブロック 1 2 等から収集される様々な情報を活用し、ユーザに様々なサービスを提供する機能を有している。

【 0 0 3 7 】

電力管理装置 1 1 により収集可能な情報には、例えば、各機器の型番や機器 ID（以下、機器情報）、ユーザのプロフィールに関する情報（以下、ユーザ情報）、ユーザの課金口座やクレジットカード等に関する情報（以下、課金情報）、利用するサービスに関する登録情報（以下、サービス情報）等がある。上記の機器情報は、各機器に予め設定されているか、或いは、ユーザにより手入力される。また、上記のユーザ情報、課金情報、サービス情報は、多くの場合、ユーザにより電力管理装置 1 1 に手入力される。なお、情報の入力方法はこれらの例に限定されず、任意の入力方法に変更可能である。また、以下の説明において、機器情報、ユーザ情報、課金情報、サービス情報を「初期情報」と呼ぶ。

【 0 0 3 8 】

また、電力管理装置 1 1 により収集可能な情報には、初期情報の他にも、例えば、各機器に接続されたバッテリーの仕様に関する情報（以下、機器バッテリー情報）、各機器等（蓄電手段、発電手段、給電手段等を含む。）の状態に関する情報（以下、機器状態情報）、広域ネットワーク 2 に接続された外部のシステムやサーバから取得可能な情報（以下、外部情報）等がある。上記の機器状態情報としては、例えば、情報の収集時点における蓄電手段の蓄電容量や放電電圧、発電手段の発電容量や発電電圧、各機器の消費電流量等がある。また、上記の外部情報としては、電力取引システム 7 から取得される電力の市場単価や、外部サーバ 3 から取得される利用可能なサービス一覧等がある。なお、以下の説明において、機器バッテリー情報、機器状態情報、外部情報を「一次情報」と呼ぶ。

【 0 0 3 9 】

また、電力管理装置 1 1 は、自身で、或いは、外部サーバ 3 の機能を利用して、初期情報、一次情報を利用して二次的な情報（以下、「二次情報」）を算出することができる。例えば、電力管理装置 1 1 は、上記の一次情報を解析して、電力供給者システム 5 から供給される電力、発電手段により発電された電力、蓄電手段にて充放電される電力、管理対象ブロック 1 2 にて消費される電力のバランスを示す指標値（以下、バランス指標）を算出する。また、電力管理装置 1 1 は、消費電力量に基づく CO₂ の削減状況、課金状況を算出する。さらに、電力管理装置 1 1 は、初期情報に基づいて各機器の消耗度（耐用年数に対する使用期間の割合等）を算出したり、消費電力の時系列変化に基づいてユーザの生活パターンを解析したりする。

【 0 0 4 0 】

また、電力管理装置 1 1 は、二次情報を利用して算出したり、広域ネットワーク 2 に接続されたシステムやサーバ、或いは、他の電力管理装置 1 1 と情報交換したりして様々な情報（以下、「三次情報」）を得る。例えば、電力管理装置 1 1 は、電力取引市場における売買注文の状況や価格に関する情報（以下、市場データ）、近隣地域における余剰電力量や不足電力量の情報（以下、地域電力情報）、効率的な電力利用を促進する上でユーザの生活パターンに適合した機器の情報（以下、機器推薦情報）、コンピュータウイルス等に関するセキュリティ情報、機器の不具合等に関する機器リスク情報等を得る。

【 0 0 4 1 】

上記の初期情報、一次情報、二次情報、三次情報を適宜利用することにより、電力管理装置 1 1 は、ユーザに対して様々なサービスを提供することができる。一方で、電力管理装置 1 1 は、ユーザのプライバシーや局所電力管理システム 1 のセキュリティに関わる重要な情報を保持することになる。また、電力管理装置 1 1 は、管理対象ブロック 1 2 に対する電力供給の許可や禁止を司る立場にある。そのため、局所電力管理システム 1 の外部から受ける攻撃、或いは、局所電力管理システム 1 の内部で行われる不正行為に対抗できるよう、電力管理装置 1 1 には高いレベルのセキュリティが求められる。

【 0 0 4 2 】

局所電力管理システム 1 の外部から電力管理装置 1 1 が受ける攻撃としては、例えば、DoS 攻撃（Denial of Service attack）やコンピュータウイルス等が考えられる。もちろん、局所電力管理システム 1 と広域ネットワーク 2 の間にはファイアウォールが設けられるが、上記の理由から、より強固なセキュリティ対策が求められる。また、局所電力管理システム 1 の内部で行われる不正行為としては、例えば、機

10

20

30

40

50

器や蓄電手段等の不正改造、情報の改竄、不正機器の接続等が考えられる。さらに、ユーザの生活パターンを反映した消費電力の情報が悪意ある第三者に利用されないようにする対策や、各機器及び電力管理装置 11 の故障（場合によっては発火等）を検出・回復できるようにすることも、セキュリティレベルを高める上で必要になると考えられる。

【 0 0 4 3 】

後述するように、電力管理装置 11 は、上記のような高度なセキュリティレベルを実現する機能を有している。そして、電力管理装置 11 は、このセキュリティレベルを保持しつつ、管理対象ブロック 12 を対象とする電力管理、及び、管理対象ブロック 12 から収集した初期情報、一次情報、二次情報、三次情報に基づくサービスの提供等を実現する。なお、電力管理装置 11 による高度なセキュリティレベルの確保は、必ずしも電力管理装置 11 が単独で実現できるものではない。そのため、管理対象ブロック 12 に含まれる機器、蓄電手段、発電手段、給電手段等が電力管理装置 11 と協同でセキュリティレベルの確保に努めることになる。なお、そのような管理対象ブロック 12 の構成要素についても、後段において詳述する。

【 0 0 4 4 】

[管理対象ブロックの構成]

ここで、図 2 ~ 図 4 を参照しながら、管理対象ブロック 12 の構成について、より詳細に説明する。図 2 は、管理対象ブロック 12 の構成を示している。また、図 3 は、管理対象ブロック 12 の内部における通信網の構成を示している。そして、図 4 は、電力管理装置 11 と情報をやり取りする主な構成要素の具体的な構成を示している。

【 0 0 4 5 】

まず、図 2 を参照する。図 2 に示すように、管理対象ブロック 12 は、分電装置 121、AC/DC 変換器 122、制御化端子 123、電動移動体 124、制御化機器 125、非制御化機器 126、端子拡張装置 127、蓄電装置 128、第 1 発電装置 129、第 2 発電装置 130、環境センサ 131 を含む。

【 0 0 4 6 】

なお、制御化端子 123、電動移動体 124、制御化機器 125、端子拡張装置 127 は、上記機器の一例である。また、蓄電装置 128 は、上記蓄電手段の一例である。さらに、第 1 発電装置 129、第 2 発電装置 130 は、上記発電手段の一例である。ただし、制御化端子 123、端子拡張装置 127 は、上記給電手段の一例でもある。また、非制御化機器 126 は、直接的に電力管理装置 11 の電力管理を受けられないため、単独では上記機器の一例に含まれない。しかし、後述するように、端子拡張装置 127 と組み合わせることで、電力管理装置 11 の管理を受けられるようになり、上記機器の一例となる。

【 0 0 4 7 】

電力の流れについて

分電装置 121 には、電力供給者システム 5、電力取引システム 7、或いは、他の局所電力管理システム 1 から供給された電力（以下、外部電力）が入力される。図 2 の例では、分電装置 121 に AC の外部電力を入力することが想定されているが、DC の外部電力が入力されるような構成にしてもよい。但し、説明の都合上、以下では AC の外部電力が分電装置 121 に入力されるものとする。分電装置 121 に入力された外部電力は、AC/DC 変換器 122 により AC から DC へと変換され、制御化端子 123、又は蓄電装置 128 に入力される。

【 0 0 4 8 】

また、分電装置 121 には、蓄電装置 128 から出力された電力（以下、放電電力）も入力される。蓄電装置 128 から出力された放電電力は、AC/DC 変換器 122 により DC から AC へと変換され、分電装置 121 に入力される。そして、分電装置 121 に入力された AC の放電電力は、AC/DC 変換器 122 により AC から DC へと変換され、制御化端子 123 に入力される。但し、AC/DC 変換器 122 における放電電力の口スを避けるため、蓄電装置 128 から制御化端子 123 へと AC/DC 変換器 122 を介さずに放電電力が供給されるような構成にしてもよい。

【0049】

蓄電装置128には、分電装置121を介して入力される外部電力の他に、第1発電装置129、第2発電装置130により発電された電力（以下、発電電力）が入力される。なお、図2の例では、第1発電装置129、第2発電装置130により発電された発電電力は、一旦、蓄電装置128に蓄えられる。しかし、第1発電装置129、第2発電装置130により発電された発電電力が、蓄電装置128を介さずにAC/DC変換器122や制御化端子123に入力されるような構成にしてもよい。ただし、第1発電装置129から出力される発電電力は、天候や環境に左右されて供給が不安定になることが多い。そのため、第1発電装置129から出力される発電電力を利用する場合には、その発電電力を蓄電装置128に一旦蓄えてから利用の方が好ましい。

10

【0050】

なお、第1発電装置129は、再生可能エネルギーを利用して発電する発電手段である。第1発電装置129は、例えば、太陽光発電装置、風力発電装置、地熱発電装置、水力発電装置等である。一方、第2発電装置130は、ガソリンや石炭等を燃焼させ、その燃焼を利用して発電する火力発電等に比べて環境負荷の低い再生不可能エネルギーを利用して発電する発電手段である。第2発電装置130は、例えば、燃料電池、天然ガス発電装置、バイオマス発電装置等である。但し、燃料電池の発電用燃料である水素が再生可能エネルギー由来の電力を利用して生成された場合、燃料電池は、再生不可能エネルギーを利用しないで発電する発電手段となる。

20

【0051】

第1発電装置129、第2発電装置130により発電された発電電力、及び蓄電装置128に蓄えられた電力は、分電装置121、AC/DC変換器122を介して制御化端子123に入力される一方、電力供給者システム5や電力取引システム7等にも買電されることもある。この場合、第1発電装置129、第2発電装置130により発電された発電電力、及び蓄電装置128から出力された放電電力は、AC/DC変換器122によりDCからACへと変換され、分電装置121を介して電力供給者システム5や電力取引システム7等へと送られる。

【0052】

以上、管理対象ブロック12における大まかな電力の流れについて説明した。特に、ここでは分電装置121を介して流れる電力の流通経路について説明した。上記の通り、分電装置121は、管理対象ブロック12の内部における電力の流通経路を分岐する役割を担っている。そのため、分電装置121が停止すると、管理対象ブロック12の内部における電力の流通が滞ってしまう。そこで、分電装置121は、無停電電源装置（UPS；Uninterruptible Power Supply）を搭載している。なお、図2の例では分電装置121を電力管理装置11と別体に行しているが、分電装置121と電力管理装置11を同じ筐体内に設置してもよい。

30

【0053】

電力供給時の認証について

管理対象ブロック12において、分電装置121を介して制御化端子123や蓄電装置128に流れる電力は、電力管理装置11により管理される。例えば、電力管理装置11は、分電装置121を制御して制御化端子123へと電力を供給したり、制御化端子123に対する電力の供給を停止したりする。

40

【0054】

また、電力管理装置11は、制御化端子123に対する認証を実施する。そして、電力管理装置11は、認証が成功した制御化端子123に対して電力を供給し、認証が失敗した制御化端子123に対する電力の供給を停止する。このように、管理対象ブロック12における電力の供給可否は、電力管理装置11による認証の成否により決められる。電力管理装置11による認証は、制御化端子123だけでなく、電動移動体124、制御化機器125、端子拡張装置127に対しても実施される。ただし、電力管理装置11との通信機能や認証に必要な演算機能を有しない非制御化機器126は、電力管理装置11によ

50

る認証を受けることができない。

【 0 0 5 5 】

そのため、認証を通った制御化端子 1 2 3、電動移動体 1 2 4、制御化機器 1 2 5、端子拡張装置 1 2 7 は、電力管理装置 1 1 による制御に基づく電力の供給を受けることができる。しかし、単独では認証を受けられない非制御化機器 1 2 6 は、電力管理装置 1 1 による制御に基づく電力の供給を受けることができない。従って、非制御化機器 1 2 6 には、電力管理装置 1 1 による制御とは無関係に電力が供給され続けるか、一切電力が供給されなくなる。ただし、端子拡張装置 1 2 7 に認証を代行させることで、非制御化機器 1 2 6 は、電力管理装置 1 1 の制御に基づく電力の供給を受けることができるようになる。

【 0 0 5 6 】

[機器機能の整理]

ここで、制御化端子 1 2 3、電動移動体 1 2 4、制御化機器 1 2 5、非制御化機器 1 2 6、端子拡張装置 1 2 7 の機能について簡単に整理する。

【 0 0 5 7 】

制御化端子 1 2 3

まず、制御化端子 1 2 3 の機能について整理する。制御化端子 1 2 3 は、電動移動体 1 2 4、制御化機器 1 2 5、非制御化機器 1 2 6、端子拡張装置 1 2 7 の電源プラグを接続するための端子を有する。そして、制御化端子 1 2 3 は、分電装置 1 2 1 を介して供給された電力を端子に接続された電動移動体 1 2 4、制御化機器 1 2 5、非制御化機器 1 2 6、端子拡張装置 1 2 7 に供給する機能を有する。つまり、制御化端子 1 2 3 は、給電端子としての機能を有する。

【 0 0 5 8 】

また、制御化端子 1 2 3 は、電力管理装置 1 1 による認証を受けるために必要な各種の機能を有する。例えば、制御化端子 1 2 3 は、電力管理装置 1 1 と情報をやり取りするための通信機能を有する。この通信機能は、電力線や信号線による有線通信、或いは、無線通信の通信モジュールを制御化端子 1 2 3 に設けることにより実現される。また、制御化端子 1 2 3 は、認証の際に必要な演算を実行するための演算機能を有する。さらに、制御化端子 1 2 3 は、認証に必要な鍵情報や機器 ID 等の識別情報を保持している。これらの機能及び情報を利用し、制御化端子 1 2 3 は、電力管理装置 1 1 による認証を受けることができる。なお、認証の種類は、乱数を利用した相互認証でもよいし、秘密鍵と公開鍵のペアを利用した公開鍵認証でもよい。

【 0 0 5 9 】

また、制御化端子 1 2 3 は、電力管理装置 1 1 に対する認証の成否、認証中の状態（以下、認証状態）を表示するための状態表示手段を有していてもよい。この場合、制御化端子 1 2 3 に設けられた状態表示手段は、制御化端子 1 2 3 に接続された電動移動体 1 2 4、制御化機器 1 2 5、端子拡張装置 1 2 7 の認証状態を表示してもよい。さらに、この状態表示手段は、制御化端子 1 2 3 に接続された機器が非制御化機器 1 2 6 であるか否かを表示してもよい。なお、この状態表示手段は、例えば、LED や小型電球等の表示ランプ、或いは、LCD や ELD 等の表示デバイスにより構成される。

【 0 0 6 0 】

先に述べた通り、電力管理装置 1 1 による認証が成功した制御化端子 1 2 3 には、電力管理装置 1 1 の制御により分電装置 1 2 1 を介して電力が供給される。一方、認証が失敗した制御化端子 1 2 3 には、電力管理装置 1 1 の制御により電力の供給が停止される。このように、認証の成否に応じた給電制御が行われることにより、分電装置 1 2 1 に対して不正な給電端子が接続されるのを防止できる。さらに、分電装置 1 2 1 に対して不正に接続された給電端子を容易に検出することが可能になる。また、制御化端子 1 2 3 に状態表示手段を設けた場合、制御化端子 1 2 3 の認証状態が容易に把握できるようになり、認証失敗と制御化端子 1 2 3 の故障を容易に見分けることができるようになる。

【 0 0 6 1 】

さて、制御化端子 1 2 3 の形状は、電源プラグを接続するためのコンセント形状に限ら

10

20

30

40

50

ない。例えば、非接触ICカード用リーダー/ライタのように電磁誘導を利用して電力を供給するコイルを内蔵し、コンセント形状のない表面形状を持った制御化端子123を実現することも可能である。この場合、非接触ICカードと同様に、電動移動体124、制御化端子125、端子拡張装置127には、制御化端子123が発生する磁場から誘導起電力を発生させるためのコイルが搭載される。このような構成にすることで、電源プラグを利用せずに電力の授受が可能になる。なお、電磁誘導を利用する構成の場合、制御化端子123と、電動移動体124、制御化機器125又は端子拡張装置127との間で磁場の変調を利用した情報のやり取りができる。

【0062】

また、制御化端子123は、端子に接続された電動移動体124、制御化端子125、端子拡張装置127に供給した電力量を測定する機能を有する。さらに、制御化端子123は、測定した電力量を電力管理装置11に送信する機能を有する。そして、制御化端子123は、端子に接続された電動移動体124、制御化端子125、端子拡張装置127から一次情報を取得し、取得した一次情報を電力管理装置11に送信する機能を有している。このように、制御化端子123により測定又は取得された情報が電力管理装置11に送られることで、電力管理装置11は、個々の制御化端子11を単位として電力状況を把握したり、電力の給電制御を行ったりすることが可能になる。

【0063】

電動移動体124

次に、電動移動体124の機能について整理する。電動移動体124は、電力を蓄えるバッテリーを有する。また、電動移動体124は、バッテリーから放電される電力を利用して駆動する駆動機構を有する。電動移動体124が電気自動車又はプラグインハイブリッド車両の場合、この駆動機構には、例えば、モータ、ギア、シャフト、ホイール、タイヤ等が含まれる。その他の電動移動体124の駆動機構には、少なくともモータが含まれる。また、電動移動体124は、バッテリーを充電する際に利用する電源プラグを有する。この電源プラグを制御化端子123に接続することにより電力の供給を受けることができる。ただし、制御化端子123が電磁誘導を利用して電力を供給する方式の場合、電動移動体124には、磁場を受けて誘導起電力を発生させるためのコイルが搭載される。

【0064】

また、電動移動体124は、電力管理装置11による認証を受けるために必要な各種の機能を有する。例えば、電動移動体124は、電力管理装置11と情報をやり取りするための通信機能を有する。この通信機能は、電力線や信号線による有線通信、或いは、無線通信の通信モジュールを電動移動体124に設けることにより実現される。また、電動移動体124は、認証の際に必要な演算を実行するための演算機能を有する。さらに、電動移動体124は、認証に必要な鍵情報や機器ID等の識別情報を保持している。これらの機能及び情報を利用し、電動移動体124は、電力管理装置11による認証を受けることができる。なお、認証の種類は、乱数を利用した相互認証でもよいし、秘密鍵と公開鍵のペアを利用した公開鍵認証でもよい。

【0065】

また、電動移動体124は、バッテリー残量、充電量、放電量等、搭載されたバッテリーに関する機器バッテリー情報を電力管理装置11に送信する機能を有する。さらに、電動移動体124を所有するユーザに関するユーザ情報、電動移動体124の燃費や性能等に関する機器情報が電力管理装置11に送信される。このような情報が電動移動体124から電力管理装置11に送信されることにより、ユーザ情報を利用した課金、ユーザ情報と機器情報に基づく課税等の処理を電力管理装置11において実施することが可能になる。例えば、CO₂排出量に基づいて算出される環境税の課税処理や、バッテリー残量に基づく走行可能距離の表示処理等を電力管理装置11において実施できるようになる。

【0066】

なお、電動移動体11のバッテリーを蓄電装置128の代わりに利用する構想もある。例えば、蓄電装置128の故障時や交換時等、一時的に蓄電装置128が利用できない場

10

20

30

40

50

合に、蓄電装置 1 2 8 に代えて電動移動体 1 2 4 のバッテリーを利用してよい。また、電動移動体 1 2 4 は、それ自体が移動可能であるため、外部の電力を物理的に運搬することができる。つまり、移動可能な蓄電装置 1 2 8 として利用することができる。このような利点があるため、災害時や緊急時のバックアップ電源として電動移動体 1 2 4 を利用する使い方も有用であるかもしれない。もちろん、こうした使い方も、本実施形態に係る局所電力管理システム 1 の枠組みの中で実現可能である。

【 0 0 6 7 】

制御化機器 1 2 5

次に、制御化機器 1 2 5 の機能について整理する。制御化機器 1 2 5 は、電力管理装置 1 1 による認証を受けるために必要な各種の機能を有する。例えば、制御化機器 1 2 5 は、電力管理装置 1 1 と情報をやり取りするための通信機能を有する。この通信機能は、電力線や信号線による有線通信、或いは、無線通信の通信モジュールを制御化機器 1 2 5 に設けることにより実現される。また、制御化機器 1 2 5 は、認証の際に必要な演算を実行するための演算機能を有する。さらに、制御化機器 1 2 5 は、認証に必要な鍵情報や機器 ID 等の識別情報を保持している。これらの機能及び情報を利用し、制御化機器 1 2 5 は、電力管理装置 1 1 による認証を受けることができる。なお、認証の種類は、乱数を利用した相互認証でもよいし、秘密鍵と公開鍵のペアを利用した公開鍵認証でもよい。

10

【 0 0 6 8 】

また、制御化機器 1 2 5 は、バッテリー残量、充電量、放電量等、搭載されたバッテリーに関する機器バッテリー情報を電力管理装置 1 1 に送信する機能を有する。さらに、制御化機器 1 2 5 を所有するユーザに関するユーザ情報、制御化機器 1 2 5 の種類や性能等に関する機器情報が電力管理装置 1 1 に送信される。このような情報が制御化機器 1 2 5 から電力管理装置 1 1 に送信されることにより、ユーザ情報を利用した課金、ユーザ情報と機器情報に基づく課税等の処理を電力管理装置 1 1 において実施することが可能になる。例えば、CO₂ 排出量に基づいて算出される環境税の課税処理や、より環境性能の高い機器を推薦するための表示処理等を電力管理装置 1 1 において実施できるようになる。

20

【 0 0 6 9 】

非制御化機器 1 2 6、端子拡張装置 1 2 7

次に、非制御化機器 1 2 6 及び端子拡張装置 1 2 7 の機能について整理する。非制御化機器 1 2 6 は、上記の制御化端子 1 2 3、電動移動体 1 2 4、制御化機器 1 2 5 とは異なり、電力管理装置 1 1 による認証を受けるために必要な機能を有していない。つまり、非制御化機器 1 2 6 は、現行の家電製品や映像機器等である。このように認証を通らない非制御化機器 1 2 6 は、電力管理装置 1 1 による電力管理を受けることができず、場合によっては電力の供給を受けることができない。そのため、局所電力管理システム 1 において非制御化機器 1 2 6 を利用できるようにするには、認証を代行する手段が必要になる。

30

【 0 0 7 0 】

端子拡張装置 1 2 7 は、2 つの役割を担う。1 つの役割は、局所電力管理システム 1 において非制御化機器 1 2 6 を利用できるようにするために認証を代行する機能である。もう 1 つの役割は、制御化端子 1 2 3 に接続する機器の数を増加させる機能である。端子拡張装置 1 2 7 には、電動移動体 1 2 4、制御化機器 1 2 5、非制御化機器 1 2 6 の電源プラグを接続するための端子が 1 つ又は複数設けられている。複数の端子が設けられた端子拡張装置 1 2 7 を利用すれば、制御化端子 1 2 3 に接続可能な電動移動体 1 2 4、制御化機器 1 2 5、非制御化機器 1 2 6 の台数を増加させることができる。つまり、端子拡張装置 1 2 7 は、高度な機能を有する電源タップとして機能する。

40

【 0 0 7 1 】

以上、制御化端子 1 2 3、電動移動体 1 2 4、制御化機器 1 2 5、非制御化機器 1 2 6、端子拡張装置 1 2 7 の機能について簡単に整理した。但し、ここで述べた機能は、制御化端子 1 2 3、電動移動体 1 2 4、制御化機器 1 2 5、非制御化機器 1 2 6、端子拡張装置 1 2 7 が有する機能の全てではない。これらの機能を基本とし、さらに後述する電力管理装置 1 1 による電力管理の動作に必要な機能が追加される。

50

【 0 0 7 2 】

[通信機能について]

ここで、図 3 を参照しながら、局所電力管理システム 1 の内部における電力管理装置 1 1、制御化端子 1 2 3、電動移動体 1 2 4、制御化機器 1 2 5、端子拡張装置 1 2 7 等の通信機能について説明する。図 3 に示すように、局所電力管理システム 1 においては、例えば、近距離無線通信、無線 LAN、電力線通信等が利用される。例えば、Z i g B e e は、近距離無線通信の一例である。また、P L C は、電力線通信の一例である。

【 0 0 7 3 】

図 2 に示したように、局所電力管理システム 1 においては、電力線により分電装置 1 2 1 と、制御化端子 1 2 3 及び制御化端子 1 2 3 に接続された機器が接続される。そのため、この電力線を利用して電力線通信による通信網が容易に構築できる。一方、近距離無線通信を利用する場合、図 3 に示すように、アドホックに個々の機器を接続する形で通信網を構築できる。また、無線 LAN を利用する場合、個々の機器が電力管理装置 1 1 に直接接続できるようになる。そのため、いずれの通信方法を利用しても、局所管理システム 1 の内部に、必要な通信網を構築することができる。

【 0 0 7 4 】

ただし、図 3 に示すように、非制御化機器 1 2 6 は、通信網を利用して電力管理装置 1 1 に接続できない場合がある。そのため、非制御化機器 1 2 6 を利用する場合、非制御化端子 1 2 6 を端子拡張装置 1 2 7 に接続する必要がある。なお、通信機能や認証機能を有しない非制御化端子を利用する場合でも、その非制御化端子に電動移動体 1 2 4、制御化機器 1 2 5、端子拡張装置 1 2 7 が接続されれば、電動移動体 1 2 4、制御化機器 1 2 5、端子拡張装置 1 2 7 の機能を利用して通信網を介した電力管理装置 1 1 への接続ができる。もちろん、非制御化端子に非制御化機器 1 2 6 を接続した場合には、通信網への接続ができないため、電力管理装置 1 1 による制御を受けられない。

【 0 0 7 5 】

なお、図 3 に示すように、局所電力管理システム 1 の内部に構築された通信網には、電力情報収集装置 4 が接続先として含まれていてもよい。さらに、この通信網を利用して、電動移動体 1 2 4 や制御化機器 1 2 5 と電力情報収集装置 4 が情報をやり取りしてもよい。もちろん、この通信網を利用して電力管理装置 1 1 と電力情報収集装置 4 が情報をやり取りしてもよい。このように、局所電力管理システム 1 の内部に構築される通信網の構成は、実施の態様に応じて適宜設定されるべきものである。但し、この通信網は、十分にセキュアな通信路により構築されるべきである。そして、この通信路を流れる情報の安全性が確保されるような仕組みが設けられるべきである。

【 0 0 7 6 】

[機器及び各種装置の具体例について]

ここで、図 4 を参照しながら、局所電力管理システム 1 の一部構成要素について、その具体例を紹介する。図 4 に示すように、電力管理装置 1 1 と情報をやり取りする可能性のある構成要素としては、例えば、電動移動体 1 2 4、制御化機器 1 2 5 (スマート機器)、非制御化機器 1 2 6 (レガシー機器)、蓄電装置 1 2 8、第 1 発電装置 1 2 9、第 2 発電装置 1 3 0 等がある。

【 0 0 7 7 】

電動移動体 1 2 4 としては、例えば、電気自動車やプラグインハイブリッド車等が具体例として挙げられる。また、制御化機器 1 2 5、非制御化機器 1 2 6 としては、例えば、家電、パーソナルコンピュータ、携帯電話、映像機器等が具体例として挙げられる。蓄電装置 1 2 8 としては、例えば、L i - I o n 蓄電池、N A S 蓄電池、キャパシタ等が具体例として挙げられる。さらに、第 1 発電装置 1 2 9 としては、例えば、太陽光発電装置、風力発電装置、地熱発電装置等が具体例として挙げられる。そして、第 2 発電装置 1 3 0 としては、例えば、燃料電池、天然ガス発電装置、バイオマス発電装置等が具体例として挙げられる。このように、局所電力管理システム 1 の構成要素として、様々な装置や機器が用いられる。

10

20

30

40

50

【 0 0 7 8 】

以上、管理対象ブロック 1 2 の構成について説明した。ただし、管理対象ブロック 1 2 に含まれる各構成要素の機能は、ここで説明したものに限定されない。電力管理装置 1 1 による電力管理の中で、必要に応じて各構成要素の機能が追加される。なお、各構成要素に対する追加的な機能については、後段において説明する電力管理装置 1 1 の構成及びその他の構成要素に関する説明の中で詳細に説明する。

【 0 0 7 9 】

[外部サーバの構成]

次に、図 5 を参照しながら、外部サーバ 3 の構成について説明する。図 5 に示すように、外部サーバ 3 としては、例えば、サービス提供サーバ 3 1、課金サーバ 3 2、システム管理サーバ 3 3、解析サーバ 3 4、認証局サーバ 3 5、製造者サーバ 3 6、地図 DB サーバ 3 7 等が利用される。

10

【 0 0 8 0 】

サービス提供サーバ 3 1 は、電力管理装置 1 1 等の機能を利用したサービスを提供する機能を有する。課金サーバ 3 2 は、電力管理装置 1 1 が管理する電力量の情報に基づき、局所電力管理システム 1 において消費された電力に応じて電力管理装置 1 1 に課金情報を提供したり、ユーザに対して利用料金の決済を求めたりする機能を有する。また、課金サーバ 3 2 は、サービス提供サーバ 3 1 と連携し、ユーザが利用したサービスに対する課金処理を実施する。なお、課金処理は、電力を消費した電動移動体 1 2 4 や制御化機器 1 2 5 等の所有ユーザに対して実施してもよいし、消費された電力の情報を管理する電力管理装置 1 1 のユーザに対して実施してもよい。

20

【 0 0 8 1 】

システム管理サーバ 3 3 は、図 1 に示した電力管理システム全体、又は、地域単位で電力管理システムを管理する機能を有する。例えば、図 6 に示すように、システム管理サーバ 3 3 は、ユーザ # 1 の局所電力管理システム 1 における利用状況、ユーザ # 2 の局所電力管理システム 1 における利用状況、ユーザ # 3 の局所電力管理システム 1 における利用状況を把握し、必要な情報を課金サーバ 3 2 等に提供する。

【 0 0 8 2 】

図 6 の例では、ユーザ # 1 が、ユーザ # 1 自身、ユーザ # 2、ユーザ # 3 の局所電力管理システム 1 において電力を利用したケースが想定されている。この場合、電力を消費したユーザ # 1 の機器 ID、利用情報（消費電力量等）がシステム管理サーバ 3 3 により収集され、システム管理サーバ 3 3 から課金サーバ 3 2 へとユーザ # 1 のユーザ情報及び利用情報が送信される。また、システム管理サーバ 3 3 は、収集した利用情報に基づいて課金情報（課金額等）を算出してユーザ # 1 に提供する。一方、課金サーバ 3 2 は、ユーザ # 1 に対して課金情報に対応する料金の請求を実施する。

30

【 0 0 8 3 】

このように、システム管理サーバ 3 3 が複数の局所電力管理システム 1 を統括することにより、他ユーザの局所電力管理システム 1 において電力を利用しても、利用したユーザに課金する仕組みが実現される。特に、電動移動体 1 2 4 に対する充電は、自身の管理する局所電力管理システム 1 の外部で行われることが多い。このような場合、システム管理サーバ 3 3 の上記機能を利用すると、電動移動体 1 2 4 のユーザに対して確実に課金が行えるようになる。

40

【 0 0 8 4 】

解析サーバ 3 4 は、電力管理装置 1 1 が集取した情報、或いは、広域ネットワーク 2 に接続された他のサーバが保持する情報を解析する機能を有する。例えば、地域を単位とする給電制御の最適化を行う場合、個々の局所電力管理システム 1 から収集される情報は膨大であり、その情報を解析して個々の局所電力管理システム 1 に対する最適な制御方法を算出するには膨大な量の演算を処理する必要がある。このような演算は、電力管理装置 1 1 にとって負担が大きいため、解析サーバ 3 4 を利用して実施される。なお、解析サーバ 3 4 は、その他様々な演算処理に利用することも可能である。また、認証局サーバ 3 5 は

50

、公開鍵に認証を与え、公開鍵証明書を発行するものである。

【0085】

製造者サーバ36は、機器の製造者が管理するものである。例えば、電動移動体124の製造者サーバ36には、その電動移動体124の設計に関する情報が保持されている。同様に、制御化機器125の製造者サーバ36には、その制御化機器125の設計に関する情報が保持されている。さらに、製造者サーバ36は、個々の電動移動体124や制御化機器125等、製造した機器を個々に特定するための情報を保持している。そして、製造者サーバ36は、これらの情報を利用し、電力管理装置11と協力して、個々の局所電力管理システム1の内部に設置された電動移動体124や制御化機器125を特定する機能を有する。この機能を利用して電力管理装置11は、電動移動体124や制御化機器125の認証を実施したり、不正な機器の接続を検知したりすることができる。

10

【0086】

地図DBサーバ37は、地図データベースを保持している。そのため、広域ネットワーク2に接続されたサーバや電力管理装置11は、地図DBサーバ37にアクセスして地図データベースを利用することができる。例えば、システム管理サーバ33は、ユーザが自身の局所電力管理システム1外で電力を利用した場合、その利用場所を地図データベースから検索し、課金情報と共に利用場所の情報をユーザに提供することができる。このように、外部サーバ3には様々な種類があり、ここに例示したサーバ構成以外にも、必要に応じて異なる種類の外部サーバ3を追加してもよい。

【0087】

<電力管理装置の構成について>

ここまで、本実施形態に係る電力管理システムの全体像について説明してきた。以下では、図7～図9を参照しながら、この電力管理システムにおける電力管理を主に担う電力管理装置11の構成について説明する。

20

【0088】

[機能の概要]

まず、図7を参照しながら、電力管理装置11の全体的な機能構成について説明する。図7に示すように、電力管理装置11は、局所通信部111、情報管理部112、記憶部113、広域通信部114、制御部115、表示部116、入力部117及びサービス提供部118を有する。

30

【0089】

局所通信部111は、局所電力管理システム1の内部に構築された通信網を介して通信するための通信手段である。情報管理部112は、局所電力管理システム1に含まれる各構成要素の機器情報や電力に関する情報を管理する手段である。また、制御化端子123、電動移動体124、制御化機器125、端子拡張装置127等に対する認証処理は、情報管理部112により実施される。記憶部113は、認証に利用する情報や電力管理に利用する情報を保持するための記憶手段である。この記憶部113には、電力管理装置11が有する公開鍵及び秘密鍵からなる鍵ペアや共通鍵等に関する鍵情報や、各種のデジタル署名又は証明書や、各種のデータベースや履歴情報が格納されている。広域通信部114は、広域ネットワーク2を介して外部のシステムやサーバと情報をやり取りするための通信手段である。

40

【0090】

制御部115は、局所電力管理システム1に含まれる各構成要素の動作を制御するための制御手段である。表示部116は、局所電力管理システム1内における消費電力に関する情報、ユーザ情報、課金情報、その他電力管理に関する情報、局所電力管理システム1外における電力管理に関する情報、電力取引に関する情報等を表示するための表示手段である。なお、表示手段としては、例えば、LCDやELD等が用いられる。入力部117は、ユーザが情報を入力するための入力手段である。なお、入力部117としては、例えば、キーボードやボタン等が用いられる。また、表示部116、入力部117を組み合わせるとタッチパネルを構成することも可能である。サービス提供部118は、外部のシステ

50

ムやサーバ等と連携しながら、電力管理装置 1 1 に各種のサービスや機能を実現し、ユーザに提供する手段である。

【 0 0 9 1 】

このように、電力管理装置 1 1 は、局所電力管理システム 1 の内外にある機器、装置、システム、サーバ等と情報をやり取りするための通信手段（局所通信部 1 1 1、広域通信部 1 1 4）を有する。さらに、電力管理装置 1 1 は、局所電力管理システム 1 内の機器や装置を制御するための制御手段（制御部 1 1 5）を有する。そして、電力管理装置 1 1 は、局所電力管理システム 1 の内外にある機器、装置、システム、サーバ等から情報を収集したり、その情報を利用してサービスを提供したり、局所電力管理システム 1 内の機器や装置を認証したりする情報管理手段（情報管理部 1 1 2）を有する。また、電力管理装置 1 1 は、局所電力管理システム 1 内外の電力に関する情報を表示するための表示手段（表示部 1 1 6）を有する。

10

【 0 0 9 2 】

局所電力管理システム 1 内における安全で効率的な電力管理を行うためには、まず、局所電力管理システム 1 内の機器や装置等を正しく特定できるようにすることが求められる。また、局所電力管理システム 1 内における安全で効率的な電力管理を行うためには、局所電力管理システム 1 内外の電力に関する情報を解析して適切な電力制御を行うことも求められる。このような要求に応えるために行われる情報の管理には、情報管理部 1 1 2 の機能が利用される。そこで、情報管理部 1 1 2 の機能について、より詳細に説明する。なお、具体的な機器や装置等の制御には、制御部 1 1 5 の機能が利用される。

20

【 0 0 9 3 】

[機能の詳細]

以下、図 8、図 9 を参照しながら、情報管理部 1 1 2 の機能構成について、より詳細に説明する。図 8 は、情報管理部 1 1 2 の詳細な機能構成を示している。図 9 は、情報管理部 1 1 2 の各構成要素が持つ主な機能を示している。

【 0 0 9 4 】

図 8 に示すように、情報管理部 1 1 2 は、機器管理部 1 1 2 1、電力取引部 1 1 2 2、情報分析部 1 1 2 3、表示情報生成部 1 1 2 4、及びシステム管理部 1 1 2 5 を有する。

【 0 0 9 5 】

機器管理部 1 1 2 1

図 9 に示すように、機器管理部 1 1 2 1 は、局所電力管理システム 1 内にある機器や装置等を管理する手段である。例えば、機器管理部 1 1 2 1 は、制御化端子 1 2 3、電動移動体 1 2 4、制御化機器 1 2 5、端子拡張装置 1 2 7 等について、登録、認証、機器 ID の管理、動作設定やサービス設定の管理、動作状況や使用状況の把握、環境情報の収集等を行う。なお、環境情報の収集は、管理対象ブロック 1 2 内に設置された環境センサ 1 3 1 を利用して実施する。但し、環境情報とは、温度、湿度、天候、風向き、風速、地形、地域、天気予報等に関する情報及びその解析により得られる情報である。

30

【 0 0 9 6 】

電力取引部 1 1 2 2

図 9 に示すように、電力取引部 1 1 2 2 は、電力市場における市場取引データや個別取引データの取得、取引を実行するタイミングの制御、取引の実行、売買ログの管理等を行う。なお、市場取引データとは、電力取引市場における取引価格や取引条件に関する情報である。また、個別取引データとは、電力供給者や近隣の電力需要者等との間で個別に電力取引を行う際に決められた取引価格や取引条件に関する情報である。そして、取引を実行するタイミングの制御とは、例えば、買電価格が所定値より低くなったタイミングで所定数量の買い注文を出したり、売電価格が所定値より高くなったタイミングで所定数量売り注文を出したりする自動制御のことである。

40

【 0 0 9 7 】

情報分析部 1 1 2 3

50

図9に示すように、情報分析部1123は、発電データの分析、蓄電データの分析、生活パターンの学習、電力消費データの分析を行う。さらに、情報分析部1123は、これらの分析に基づいて電力消費パターンの予測、蓄電パターンの予測、放電パターンの予測、発電パターンの予測を行う。なお、情報分析部1123による分析や学習は、例えば、局所電力管理システム1内にある第1発電装置129、第2発電装置130における発電量の時系列データ、蓄電装置128における充放電量又は蓄電量の時系列データ、電力供給者システム5から供給される電力量の時系列データを利用して行われる。

【0098】

また、情報分析部1123による予測は、これらの時系列データ又は時系列データを分析して得られる分析結果を学習用のデータとして利用し、所定の機械学習アルゴリズムに基づいて得られる予測式を用いて行われる。例えば、遺伝的学習アルゴリズム（例えば、特開2009-48266号公報を参照）を利用することにより、予測式を自動構築することができる。そして、この予測式に過去の時系列データ又は分析結果を入力することで予測結果を得ることができる。また、算出された予測結果を逐次的に予測式へ入力することで時系列データを予測することもできる。

【0099】

また、情報分析部1123は、現在又は将来におけるCO₂排出量の算出、電力消費量を低減するための電力供給パターン（省電力パターン）の算出、CO₂の排出量を低減するための電力供給パターン（低CO₂排出パターン）の算出、局所電力管理システム1における電力消費量及びCO₂排出量を低減することが可能な機器構成や機器配置等の算出及び推薦を行う。CO₂排出量は、全消費電力量、又は、発電方法毎に区別された消費電力量に基づいて算出される。

【0100】

全消費電力量を利用する場合、おおよその平均的なCO₂排出量が算出される。一方、発電方法毎に区別された消費電力量を利用する場合、比較的正確なCO₂排出量が算出される。なお、少なくとも外部から供給された電力、第1発電装置129により発電された電力、第2発電装置130により発電された電力を区別することで、全消費電力量を利用する場合に比べ、より正確なCO₂排出量を算出することができる。炭素税等の税金や課金は、多くの場合、CO₂排出量に応じて決められる。そのため、CO₂排出量を正確に算出できるようにすることは、ユーザの公平感を高め、再生可能エネルギー由来の発電手段を普及させることに寄与するものと考えられる。

【0101】

表示情報生成部1124

図9に示すように、表示情報生成部1124は、局所電力管理システム1内にある機器や装置等に関する情報、電力に関する情報、環境に関する情報、電力取引に関する情報、情報分析部1123による分析結果や予測結果に関する情報等について、形式を整えて表示部116に表示するための表示情報を生成する。例えば、表示情報生成部1124は、電力量を示す情報をグラフ形式で表示するための表示情報を生成したり、市場データを表形式で表示するための表示情報を生成したりする。また、表示情報生成部1124は、各種情報の表示や情報の入力に用いるグラフィカルユーザインターフェース（GUI）を生成する。これら表示情報生成部1124により生成された表示情報は、表示部116に表示される。

【0102】

システム管理部1125

図9に示すように、システム管理部1125は、電力管理装置11の基本的な動作を制御するためのプログラムであるファームウェアのバージョン管理、アップデート、アクセス制限、ウィルス対策等を行う。また、局所電力管理システム1内に電力管理装置11が複数設置される場合、システム管理部1125は、他の電力管理装置11と情報のやり取りを行い、複数の電力管理装置11が協調動作するための制御を行う。例えば、システム管理部1125は、各電力管理装置11の属性（機器や装置等に対する制御処理の優先度

10

20

30

40

50

等)を管理する。また、システム管理部1125は、協調動作への参加や協調動作からの脱退に関する各電力管理装置11の状態制御を行う。

【0103】

以上、電力管理装置11の機能構成について説明した。なお、ここで示した電力管理装置11の機能構成は一例であり、上記以外にも必要に応じて機能を追加できる。

【0104】

<表示部に表示される内容について>

次に、図10～図13を参照しながら、表示部に表示される内容について、具体的に説明する。図10～図13は、表示部に表示される内容について説明するための説明図である。

10

【0105】

電力管理装置11の表示部116には、先に述べたように各種の情報が表示される。例えば、図10に示したように、電力管理装置11の表示部には、電力管理装置11に登録されている機器の一覧が、その消費電力とともに表示される。ここで、消費電力は、数値で表示されていてもよく、図10に示したように、例えば棒グラフの形状で表示されていてもよい。また、端子拡張装置などのように複数の機器を接続可能な装置については、端子拡張装置という表示部分を選択することで、端子拡張装置に接続されている個々の機器の消費電力を把握することも可能となる。

【0106】

また、表示部116には、図11に示したように、電力管理装置11に接続されている機器の認証状態があわせて表示されるようにしてもよい。このような表示を行うことで、電力管理装置11のユーザは、機器が認証されているのか否かを容易に判別することが可能となって、ユーザによるメンテナンスの効率化を図ることが可能となる。

20

【0107】

更に、表示部116には、図12に示したように、各利用場所における消費電力と課金額とが、一覧表のように表示されてもよい。このような表示がなされることで、ユーザは、不要な待機電力の有無等を容易に把握することが可能となる。

【0108】

また、表示部116に表示される消費電力は、図13に示したように、利用した電力の種類別(すなわち、システム外で利用した電力か、システム内で利用した電力か)を区別して表示することも可能である。

30

【0109】

<消費電力パターンの秘匿について>

ここで、図14～図18を参照しながら、消費電力パターンの秘匿方法について説明する。

【0110】

管理対象ブロック12の消費電力パターンは、ユーザの生活パターンを反映してしまう。例えば、図14に例示した消費電力パターンは、一日を通して満遍なくピークが現れている。そのため、この消費電力パターンからユーザが一日中在宅していたことが分かる。また、午前0時前後に消費電力のピークがほぼ消滅していることから、ユーザが午前0時前後に就寝したことが分かる。一方、図15に例示した消費電力パターンは、午前7時前後、午後21時前後に大きなピークが現れているものの、その他の時間帯はほとんどピークが立っていない。この消費電力パターンは、ユーザが午前7時前後に家を出た後、午後21時近くまで家を不在にすることを示唆している。

40

【0111】

このように、消費電力パターンは、ユーザの生活パターンを反映したものになる。そのため、この消費電力パターンが悪意ある第三者に知られると、その第三者により消費電力パターンが悪用されてしまう。例えば、ユーザが不在にする時間帯を狙って空き巣に入られたり、ユーザが在宅している時間を狙って押し売りが訪問してきたり、就寝時を狙って強盗が入る可能性がある。

50

【0112】

こうした理由から、消費電力量の情報を厳重に管理するか、消費電力パターンを秘匿する仕組みを設ける必要がある。先に述べたように、電力供給者システム5から供給される電力量の情報は、電力供給者が管理する電力情報収集装置4によって収集されてしまう。そのため、少なくとも電力供給者には、管理対象ブロック12における電力消費量の時系列パターンが露呈してしまう。

【0113】

こうした理由から、ユーザの生活パターンが第三者に知られないようにすべく消費電力パターンを秘匿する仕組みを設ける方が望ましい。消費電力パターンを秘匿するには、電力供給者システム5から供給される電力量の時系列パターンと生活パターンを乖離させればよい。例えば、ユーザが不在のときに電力供給者システム5から電力が供給されるようにしたり、ユーザが在宅のときに電力供給者システム5から電力の供給を受けないようにしたりすればよい。

【0114】

このような対策は、蓄電装置128を利用することにより実現される。例えば、ユーザが不在のときに電力供給者システム5から供給を受けた電力を蓄電装置128に蓄え、ユーザが在宅のときに蓄電装置128に蓄えた電力を利用し、電力供給者システム5から供給される電力量を抑制すればよい。さらに安全性を高めるには、消費電力パターンが所定のパターンになるように蓄電装置128の充放電制御を行い、生活パターンに起因して消費電力パターンに現れる特徴がほぼ無くなるようにする方が好ましい。

【0115】

[平均化]

例えば、図16に示すように、消費電力量が一定値となるように、蓄電装置128の充放電制御を行う方法が考えられる。消費電力量を一定値にする場合、消費電力量が一定値よりも少ない場合に蓄電装置128の蓄電量を増やし、消費電力量が一定値よりも多い場合に蓄電装置128の放電量を増やせばよい。このような制御は、電力管理装置11により行われる。また、蓄電装置128の充放電制御だけでなく、電力需要者間における電力のやり取りや電動移動体124等のバッテリーを利用した充放電制御を利用してもよい。このように、消費電力量が一定値になることで、生活パターンに起因して消費電力パターンに現れる特徴を無くすることができる。その結果、消費電力パターンを悪用した不法行為にユーザが巻き込まれる危険性を無くすることができる。

【0116】

[複雑化]

なお、消費電力パターンと生活パターンを乖離させるだけであれば、必ずしも消費電力量を一定値にせずともよい。消費電力量を一定値にするには、電力の消費ピークを吸収できるだけの十分な容量を持った蓄電装置128が必要になる。しかしながら、このような大容量の蓄電装置128は高価であり、消費電力パターンを秘匿化する目的で一般家庭に配置するのは現実的ではない。そのため、より少ない容量の蓄電装置128を利用して消費電力パターンと生活パターンを乖離させる方法が望ましい。そうした方法の一例として、図17に示すように、消費電力パターンを複雑化する方法が考えられる。

【0117】

例えば、比較的小さなピークや窪みが満遍なく出来るように消費電力パターンを複雑化する方法が考えられる。大きなピークを平均値付近まで抑制するには容量の大きな蓄電装置128が必要になるが、比較的小さなピークを発生させたり、移動させたりする分には、それほど大きな蓄電容量を必要としない。また、1日を単位として消費電力パターンの複雑化を行ってもよいが、日毎に異なる消費電力パターンになるようにしたり、曜日や月毎の周期性が無くなるように、消費電力パターンの複雑化を行ったりすることも効果的である。また、外出、帰宅、就寝、起床等、悪用されやすいタイミングだけを複雑化するような仕組みにすれば、蓄電装置128の充放電制御を必要以上に煩雑化させずに、十分な不正行為の抑制効果を得ることができる。

【 0 1 1 8 】

〔パターン化〕

また、図 1 8 に示すように、近隣地域の平均パターンにほぼ一致するように、消費電力パターンを制御する方法も考えられる。近隣地域の平均パターンは、人間の生活パターンを基準に得られるものである。そのため、特定ユーザの消費電力パターンを近隣地域の平均パターンに一致させるために行うべき電力の制御量はそれほど大きくならず済む。そのため、消費電力量を一定値に制御する場合に比べ、少ない容量の蓄電装置 1 2 8 を利用して特定ユーザの生活パターンを秘匿することが可能になる。このような消費電力量の制御を行う場合、近隣地域の電力管理装置 1 1 間で互いに電力情報のやり取りが行われる。また、情報分析部 1 1 2 3 の機能又は解析サーバ 3 4 の機能を利用して近隣地位の平均パターンが算出される。その上で、充電装置 1 2 8 の充放電制御が実施される。

10

【 0 1 1 9 】

< 電力管理装置が行う各種制御について >

以上説明したような局所電力管理システム 1 における電力管理装置 1 1 について、電力管理装置 1 1 が実施する各種制御を、図 1 9 を参照しながら簡単に説明する。図 1 9 は、電力管理装置における各種制御の概要を説明する説明図である。

【 0 1 2 0 】

電力管理装置 1 1 は、管理すべき分電装置 1 2 1、制御化端子 1 2 3、電動移動体 1 2 4、制御化機器 1 2 5 及び端子拡張装置 1 2 7 等に対して、図 1 9 に示したような制御を行う。すなわち、電力管理装置 1 1 は、これら管理すべき機器に対して、蓄電制御、平均化制御、売買制御、電力源切替制御、異常時切替制御、復帰制御、認証・登録制御、情報収集・情報加工制御、外部アクセス制御、サービス連携制御等の各種の制御を行う。これらの制御のうち、例えば蓄電制御は、昼間は管理ブロック内の各種発電装置により発電された電力を使用し、夜間は外部電力を使用するなどといった、電力使用・蓄電に関する制御である。

20

【 0 1 2 1 】

図 1 9 に例示したように、電力管理装置 1 1 は、これらの制御を、電力源に関する情報、優先順位に関する情報、制御条件（パラメータ）に関する情報等を参照しながら実施していく。

【 0 1 2 2 】

電力源に関する情報は、例えば図 1 9 に示したように、電力管理装置 1 1 が属している局所電力管理システム 1 が利用可能な電力源に関する情報である。この電力源は、図 1 9 に例示したように、外部電力と、家庭内電力（システム内電力）とに大別できる。外部電力は、局所電力管理システム 1 の外部から供給される電力であり、例えば、電力供給会社等から供給される、一般の電力である。また、家庭内電力は、局所電力管理システム 1 内で管理されている電力であり、例えば、蓄電装置内に蓄電されている電力、発電装置により発電された電力、電動移動体に蓄電されている電力、バッテリーモジュール内に蓄電されている電力等を挙げることができる。なお、蓄電装置内に蓄電されている電力は、いわゆる専用の蓄電装置に蓄電されている電力にとどまらず、コンピュータ、家庭電化製品、携帯端末等、電力管理装置 1 1 が制御可能な装置が備えるバッテリー等に蓄電されている電力を含む。また、電力管理装置 1 1 は、かかる情報を利用して、蓄電装置に蓄電されている電力が、どの電力源から供給された電力なのか、という情報を保持することも可能となる。

30

40

【 0 1 2 3 】

また、優先順位に関する情報は、例えば図 1 9 に示したように、給電の優先順位を規定する情報である。飲食物の鮮度を維持する機能を有する冷蔵庫や、システム内のセキュリティを担保するセキュリティ関連機器や、照明、機器制御用の電力といったものは、給電が停止すると、その機能の実現に困難をきたし、ひいては、ユーザにも影響を及ぼしかねない装置である。したがって、電力管理装置 1 1 は、これらの機器に対しては、完全給電を行い、その機能の維持を担保することが可能である。また、電力管理装置 1 1 は、省電

50

力給電という優先順位を有する機器（例えば、テレビや冷暖房機器等）については、電力供給を適宜制御して使用電力を抑制することもできる。また、電力管理装置 10 は、電源 OFF という優先順位も設定することが可能であり、例えば、蓄電器は通常は電源 OFF としておく等といった制御も実施可能である。なお、図 19 に示した優先順位は、あくまでも一例であって、電力管理装置 11 に設けられた優先順位は、図 19 に示したものに限定されるわけではない。

【0124】

制御条件に関する情報は、例えば図 19 に示したように、電力管理装置 11 の制御条件を規定した情報である。これらの制御条件は、例えば、電力の使用環境に関する条件、電力の使用時間に関する条件、電力使用モードに関する条件、異常時に関する条件等に大別される。また、各条件には、図 19 に示したような、更に細かな条件項目が設定可能である。なお、図 19 に示した制御条件は、あくまでも一例であって、電力管理装置 11 に設けられた制御条件は、図 19 に示したものに限定されるわけではない。

10

【0125】

電力管理装置 11 は、これらの情報に基づいて、システム 1 内の各種機器に対して、図 19 に示したような制御を実施する。これにより、電力管理装置 11 は、管理している各種機器の充電制御を行ったり、機器の動作そのものを制御したり、デバイスのファームウェアをアップデートしたりすることが可能となる。例えば、電力管理装置 11 は、「時に炊飯器の機能をスタートさせる」といった制御を行うことができる。この制御に関しても、電力管理装置 11 が備える機能の一つである電力予測機能と連動させて、電力の安い時間帯に機能をスタートさせることもできる。また、電力管理装置 11 は、システム 1 外に設けられたサーバと連携して、各種のサービスを利用者に提供することも可能である。例えば、外部に設けられたサーバは、電力管理装置 11 が出力する電力情報を利用して、離れて暮らす家族が普段どおりの電力使用状況となっている（すなわち、健康上の問題なく生活している）ことを容易に確認可能なサービス等を提供することもできる。

20

【0126】

また、かかる制御は、電力管理装置 11 だけでなく、例えば、システム 1 内に設けられた制御化端子 123 や端子拡張装置 127 等が実施することも可能である。

【0127】

このような各種制御を行うために、電力管理装置 11 は、図 20 に示したような情報を保持しており、電力管理装置 11 は、この情報を、システム 1 の外部に設けられたシステム管理サーバ 33 に更に登録する。図 20 は、電力管理装置 11 が管理している各種情報を説明するための説明図である。

30

【0128】

図 20 に例示したように、電力管理装置 11 は、自装置に割り当てられている識別番号（ID）、製造メーカーや型番に関する情報、システムへの登録日、ステータス等といった情報を保持している。更に、電力管理装置 11 は、電力管理装置 11 を所有しているユーザのユーザ名、住所、電話番号、課金情報（銀行口座に関する情報等）、緊急連絡先等といった情報も保持している。また、電力管理装置 11 は、システム 1 内に存在する分電装置 121 に付与されている ID、メーカー名、型番、登録日、ステータス等に関する情報を保持している。更に、電力管理装置 11 は、システム 1 内に存在する各種の制御化機器 125 に付与されている ID、メーカー名、型番、登録日、ステータス等に関する情報も保持している。

40

【0129】

電力管理装置 11 は、これらの情報を保持することにより、例えば、システム 1 の外部に設けられたサーバに対して、各種の情報の取得要請を行ったり、各種のサービスの提供を要請したりすることが可能となる。例えば、電力管理装置 11 は、ある制御化機器 125 についてメーカー情報を参照し、このメーカーが運営するサーバにアクセスして、アクセスしたサーバから、制御化機器に関する各種の情報を取得することができる。

【0130】

50

なお、局所電力管理システム 1 内には、電力管理装置 1 1 により制御が可能な制御化機器 1 2 5 (分電装置 1 2 1、制御化端子 1 2 3、電動移動体 1 2 4、端子拡張装置 1 2 7、蓄電装置 1 2 8、発電装置 1 2 9, 1 3 0) 以外に、制御が不可能な装置である非制御化機器や非制御化端子が混在する場合もある。そのため、電力管理装置 1 1 は、どのような装置 (制御化機器又は非制御化機器) が、どのような端子 (制御化端子又は非制御化端子) に接続されているかに応じて、情報のやり取りを行う手段や、電力供給の制御方法等を選択する。なお、以下の説明において、制御化機器 1 2 5 という場合には、断りの無い限り、制御化端子 1 2 3、電動移動体 1 2 4、端子拡張装置 1 2 7、蓄電装置 1 2 8 等の制御化された機器類を含むものとする。

【 0 1 3 1 】

図 2 1 は、端子の形態及び接続機器の形態に応じた通信手段、認証手段、給電制御の組み合わせを示した説明図である。図 2 1 から明らかなように、端子の形態及び端子に接続された接続機器の形態の組み合わせは、4 通りに大別される。

【 0 1 3 2 】

制御化端子 1 2 3 に制御化機器 1 2 5 が接続されている場合、電力管理装置 1 1 は、制御化端子 1 2 3 と制御化機器 1 2 5 と通信が可能であり、制御も可能である。したがって、接続機器が電力情報を電力管理装置 1 1 に送信する際には、接続機器 (すなわち、制御化機器 1 2 5) が、例えば Zig B e e を利用して、電力情報を電力管理装置 1 1 に送信してもよい。また、制御化端子 1 2 3 が、例えば Zig B e e 又は P L C を利用して、電力情報を電力管理装置 1 1 に送信してもよい。さらに、接続機器の認証に際しては、接続機器 (制御化機器 1 2 5) が、例えば Zig B e e を利用して、電力管理装置 1 1 との認証を行うことが可能である。また、接続機器への給電制御に関しては、電力管理装置 1 1 が分電装置 1 2 1 に制御命令を送信することで行うことが可能である。また、場合によっては、接続機器に対して、制御化端子 1 2 3 から限定的な給電制御を行うことも可能である。

【 0 1 3 3 】

制御化端子 1 2 3 に非制御化機器 1 2 6 が接続されている場合には、接続機器は電力管理装置 1 1 との認証処理を行うことはできない。そのため、かかる場合には、接続機器と電力管理装置 1 1 との間の機器認証手段は存在しない。また、かかる場合における電力情報の通信は、非制御化機器 1 2 6 が接続されている制御化端子 1 2 3 から、例えば Zig B e e 又は P L C を介して行われることとなる。また、接続機器への給電制御に関しては、電力管理装置 1 1 が分電装置 1 2 1 に制御命令を送信することで行うことが可能である。また、場合によっては、接続機器に対して、制御化端子 1 2 3 から限定的な給電制御を行うことも可能である。

【 0 1 3 4 】

非制御化端子に制御化機器 1 2 5 が接続されている場合には、接続機器は、例えば Zig B e e を利用して、電力管理装置 1 1 と機器認証処理を行ったり、電力情報を電力管理装置 1 1 に送信したりすることが可能である。また、接続機器への給電制御に関しては、電力管理装置 1 1 が分電装置 1 2 1 に制御命令を送信することで行うことが可能である。

【 0 1 3 5 】

非制御化端子に非制御化機器 1 2 6 が接続されている場合には、接続機器は、電力管理装置 1 1 と機器認証処理を行ったり、電力情報を電力管理装置 1 1 に送信したりすることはできない。また、接続機器への給電制御を行うこともできないため、電力管理装置 1 1 は、接続機器に対して常時給電を行うこととなる。

【 0 1 3 6 】

< 機器管理部の構成について >

以上説明したような機器制御は、電力管理装置 1 1 が備える情報管理部 1 1 2 が取得する各種の情報に基づいて行われる。以下では、電力管理装置 1 1 の情報管理部 1 1 2 が有する機器管理部 1 1 2 1 の詳細な構成について、図 2 2 を参照しながら、詳細に説明する。図 2 2 は、本実施形態に係る機器管理部 1 1 2 1 の構成を説明するためのブロック図で

10

20

30

40

50

ある。

【0137】

機器管理部1121は、鍵生成部1501、システム登録部1503、管理機器登録部1505、管理機器情報取得部1507、管理機器情報出力部1509、排除機器特定部1511、情報改ざん検知部1513及び電力使用証明書管理部1515を主に備える。

【0138】

鍵生成部1501は、例えば、CPU(Central Processing Unit)、ROM(Read Only Memory)、RAM(Random Access Memory)等により実現される。鍵生成部1501は、局所電力管理システム1内で使用される公開鍵、秘密鍵、共通鍵等の各種の鍵、及び、局所電力管理システム1とシステム1の外部に設けられた装置との間で使用される公開鍵、秘密鍵、共通鍵等の各種の鍵を生成する。鍵生成部1501は、例えばシステム管理サーバ33又は認証局サーバ35等で公開されている公開パラメータを利用して、これらの鍵の生成のために利用する各種のパラメータや、鍵そのものを生成する。鍵生成部1501は、生成した各種のパラメータや鍵そのものを、記憶部113等にセキュアに格納する。

10

【0139】

鍵生成部1501による鍵生成処理は、後述するシステム登録部1503又は管理機器登録部1505からの要請に応じて実施される。鍵生成部1501は、鍵生成処理が終了すると、生成した鍵等を、要請のあった処理部(システム登録部1503又は管理機器登録部1505)等に出力してもよい。また、鍵生成部1501は、要請のあった処理部(システム登録部1503又は管理機器登録部1505)等に鍵生成処理が終了した旨を通知して、これらの処理部が所定の箇所(例えば記憶部113)から生成された鍵等を取得してもよい。

20

【0140】

鍵生成部1501が鍵生成処理を実施する際のプロトコルは、特定のプロトコルに限定されるわけではなく、局所電力管理システム1内、又は、各種サーバとの間の取り決め等によって規定されているプロトコルを利用することが可能である。

【0141】

システム登録部1503は、例えば、CPU、ROM、RAM等により実現される。システム登録部1503は、広域通信部114を介して、電力管理装置11自身を、局所電力管理システム1を管理しているシステム管理サーバ33に登録する処理を行う処理部である。

30

【0142】

システム登録部1503は、まず、広域通信部114を介して、システム管理サーバ33に接続し、システム管理サーバ33との間で所定の認証処理を実施する。次に、システム登録部1503は、所定の登録情報をシステム管理サーバ33に送信して、電力管理装置11自身をシステム管理サーバ33に登録する。

【0143】

システム登録部1503がシステム管理サーバ33に送信する登録情報として、例えば、図20に示したような情報を挙げる事が可能である。

40

【0144】

システム登録部1503が実施する登録処理の具体例については、以下で改めて詳細に説明する。

【0145】

管理機器登録部1505は、例えば、CPU、ROM、RAM等により実現される。管理機器登録部1505は、局所通信部111を介して通信可能な制御化端子123、電動移動体124、制御化機器125、端子拡張装置127、蓄電装置128、発電装置129、130等と通信を行い、通信の確立できた機器を管理機器として登録する。これらの制御化された装置がコンセント(制御化端子123、端子拡張装置127、非制御化端子)に接続されたり、電源がONになったりすると、管理機器登録部1505は、これらの

50

装置との間で所定の認証処理を行い、認証後に所定の登録処理を行う。

【0146】

管理機器登録部1505は、制御化された装置から、装置に固有の識別番号(機器ID)、製造メーカー名、型番、電力使用量、接続されている端子のID等の情報を登録情報として取得する。管理機器登録部1505は、取得したこれらの登録情報を、記憶部113等に格納されているデータベースに登録する。また、管理機器登録部1505は、取得したこれらの登録情報を、広域通信部114を介してシステム管理サーバ33に送信し、システム管理サーバ33に登録する。

【0147】

管理機器登録部1505の詳細な構成については、以下で改めて詳細に説明する。また、管理機器登録部1505が実施する登録処理の具体例については、以下で改めて詳細に説明する。

10

【0148】

管理機器情報取得部1507は、例えば、CPU、ROM、RAM等により実現される。管理機器情報取得部1507は、局所通信部111を介して、電力管理装置11に登録されている管理機器から、各種の情報を取得する。管理機器から取得する情報としては、例えば図8に記載されているように、機器の動作状況を表す情報、機器の使用状況を表す情報、環境情報、電力情報等を挙げることができる。また、管理機器情報取得部1507は、上述の情報以外にも、各種の情報を管理機器から取得することが可能である。

【0149】

20

また、管理機器情報取得部1507は、管理機器から取得した各種情報を、後述する管理機器情報出力部1509および排除機器特定部1511に伝送することが可能である。また、機器管理部1121が情報改ざん検知部1513を有している場合には、管理機器情報取得部1507は、管理機器から取得した各種情報を、情報改ざん検知部1513に伝送してもよい。

【0150】

管理機器情報出力部1509は、例えば、CPU、ROM、RAM等により実現される。管理機器情報出力部1509は、管理機器情報取得部1507が管理機器から取得した各種の情報を、電力管理装置11の所定の処理部に出力したり、広域通信部114を介して電力管理装置11の外部に設けられた装置へと出力したりする。また、管理機器が、後述するような、情報の改ざんの有無を検知するためのデータを情報に埋め込んでいる場合には、管理機器情報出力部1509は、このデータが埋め込まれた情報を解析サーバ34に伝送する際の仲介となる。

30

【0151】

排除機器特定部1511は、例えば、CPU、ROM、RAM等により実現される。排除機器特定部1511は、管理機器情報取得部1507が管理機器から取得した各種の情報に基づいて、局所電力管理システム1内から排除すべき管理機器を特定する。この排除機器は、取得した各種の情報に基づいて決定されてもよく、本来取得可能な情報が取得できなかったという状況に基づいて決定されてもよい。この排除機器の特定方法は、特定の方法に限定されるわけではなく、任意の方法を用いることが可能である。

40

【0152】

情報改ざん検知部1513は、例えば、CPU、ROM、RAM等により実現される。情報改ざん検知部1513は、管理機器情報取得部1507が管理機器から取得した情報に、情報の改ざんの有無を検知するためのデータが埋め込まれている場合に、かかるデータを検証して、情報の改ざんが行われたか否かを検知する。このような情報に埋め込まれたデータの一例として、例えば、電子透かしを挙げることができる。

【0153】

情報改ざん検知部1513は、情報に改ざんが行われていることを検知した場合には、その結果を、排除機器特定部1511に通知してもよい。これにより、排除機器特定部1511は、情報の改ざんが行われている機器を、システム1内から排除することが可能と

50

なる。

【 0 1 5 4 】

情報改ざん検知部 1 5 1 3 によって実施される改ざん検知処理については、以下で改めて詳細に説明する。

【 0 1 5 5 】

電力使用証明書管理部 1 5 1 5 は、例えば、CPU、ROM、RAM等により実現される。電力管理装置 1 1 を含む局所電力管理システム 1 では、システム 1 に属していない制御化機器 1 2 5 等に対しても、電力の供給を行う場合が生じうる。そのため、以下で説明するように、かかる場合においては、電力の供給を受けたシステム 1 外の制御化機器 1 2 5 等は、電力の供給を受けたシステムを管理する電力管理装置 1 1 に対して、電力使用証明書 10 を発行する。電力使用証明書は、電力の供給を受けたことを示す、所定の形式を有する証明書である。電力使用証明書管理部 1 5 1 5 は、発行された電力使用証明書の管理を行い、発行された電力使用証明書が正式な証明書であるか否かを検証する。また、発行された電力使用証明書が正式な証明書である場合には、電力使用証明書管理部 1 5 1 5 は、電力使用証明書を利用して、供給した電力に対する課金制御を行うことができる。

【 0 1 5 6 】

電力使用証明書管理部 1 5 1 5 によって実施される処理については、以下で改めて詳細に説明する。

【 0 1 5 7 】

[管理機器登録部の構成について]

続いて、図 2 3 を参照しながら、管理機器登録部 1 5 0 5 の構成について、より詳細に説明する。図 2 3 は、管理機器登録部の構成について説明するためのブロック図である。

【 0 1 5 8 】

管理機器登録部 1 5 0 5 は、図 2 3 に示したように、管理機器認証部 1 5 5 1 と、署名生成部 1 5 5 3 および署名検証部 1 5 5 5 を更に有する。

【 0 1 5 9 】

管理機器認証部 1 5 5 1 は、例えば、CPU、ROM、RAM等により実現される。管理機器認証部 1 5 5 1 は、電力管理装置 1 1 が管理している局所電力管理システム 1 に登録されていない制御化機器 1 2 5 等が接続された場合に、鍵生成部 1 5 0 1 が生成した鍵等を利用して、登録されていない制御化機器 1 2 5 等を認証する。この認証処理は、公開鍵を利用した公開鍵認証処理であってもよいし、共通鍵を利用した共通鍵認証処理であってもよい。管理機器認証部 1 5 5 1 は、後述する署名生成部 1 5 5 3 及び署名検証部 1 5 5 5 と連携しながら、管理機器の認証処理及び登録処理を行う。

【 0 1 6 0 】

署名生成部 1 5 5 3 は、例えば、CPU、ROM、RAM等により実現される。署名生成部 1 5 5 3 は、鍵生成部 1 5 0 1 が生成した鍵等を利用して、認証処理を行う制御化機器 1 2 5 等に対して、所定の署名（デジタル署名）や証明書を生成する。署名生成部 1 5 5 3 は、生成した署名や証明書に関する情報を、記憶部 1 1 3 等に格納されているデータベースに登録するとともに、生成した署名や証明書を、局所通信部 1 1 1 を介して、認証処理を行う制御化機器 1 2 5 等に対して送信する。

【 0 1 6 1 】

署名検証部 1 5 5 5 は、例えば、CPU、ROM、RAM等により実現される。署名検証部 1 5 5 5 は、鍵生成部 1 5 0 1 が生成した鍵等を利用して、認証処理を行う制御化機器 1 2 5 等が電力管理装置 1 1 に送信した署名（デジタル署名）や証明書の検証を行う。署名検証部 1 5 5 5 は、署名や証明書の検証に成功した場合には、検証に成功した署名や証明書に関する情報を、記憶部 1 1 3 等に格納されているデータベースに登録する。また、署名検証部 1 5 5 5 は、署名や証明書の検証に失敗した場合には、認証処理を中止してもよい。

【 0 1 6 2 】

管理機器登録部 1 5 0 5、管理機器認証部 1 5 5 1、署名生成部 1 5 5 3 及び署名検証

10

20

30

40

50

部 1 5 5 5 が、互いに連携しながら実施する管理機器の認証処理および登録処理の具体例については、以下で改めて詳細に説明する。

【 0 1 6 3 】

[情報改ざん検知部の構成について]

続いて、図 2 4 を参照しながら、情報改ざん検知部 1 5 1 3 の構成について、より詳細に説明する。図 2 4 は、情報改ざん検知部の構成について説明するためのブロック図である。

【 0 1 6 4 】

情報改ざん検知部 1 5 1 3 は、図 2 4 に示したように、埋め込み位置特定部 1 5 6 1 と、電子透かし抽出部 1 5 6 3 と、電子透かし検証部 1 5 6 5 とを更に有する。

10

【 0 1 6 5 】

本実施形態に係る局所電力管理システム 1 では、電流値、電圧値、温度、湿度といった物理データそのものや物理データを利用して算出された各種情報に、これらの情報に適した電子透かしデータを埋め込むことが可能である。局所電力管理システム 1 内の装置および局所電力管理システム 1 と相互に通信可能な各種サーバは、かかる電子透かしデータの検証を行うことで、物理データ（物理データを利用して算出された各種情報を含む。以下同じ。）に改ざんが行われたか否かを検知することができる。

【 0 1 6 6 】

埋め込み位置特定部 1 5 6 1 は、例えば、CPU、ROM、RAM 等により実現される。埋め込み位置特定部 1 5 6 1 は、所定の信号処理回路により、電子透かしの埋め込まれた物理データを解析することで、データに対応する信号の特徴に応じて、電子透かし情報の埋め込み位置を特定する。埋め込み位置特定部 1 5 6 1 は、電子透かし情報の埋め込み位置を特定すると、特定した埋め込み位置に関する情報を、電子透かし抽出部 1 5 6 3 に通知する。なお、電子透かしの埋め込み位置が、制御化装置 1 2 5 等と電力管理装置 1 1 との間で予め決まっている場合には、かかる埋め込み位置の特定処理は、実行しなくともよい。

20

【 0 1 6 7 】

電子透かし抽出部 1 5 6 3 は、例えば、CPU、ROM、RAM 等により実現される。電子透かし抽出部 1 5 6 3 は、埋め込み位置特定部 1 5 6 1 から通知された埋め込み位置に関する情報に基づいて、物理データの中から電子透かし情報を抽出する。電子透かし抽出部 1 5 6 3 は、物理データの中から抽出した電子透かし情報を、後述する電子透かし検証部 1 5 6 5 に伝送する。

30

【 0 1 6 8 】

電子透かし検証部 1 5 6 5 は、例えば、CPU、ROM、RAM 等により実現される。電子透かし検証部 1 5 6 5 は、まず、制御化装置 1 2 5 等との間で共有している共有情報と、電子透かし抽出部 1 5 6 3 によって抽出された物理データとに基づいて、電子透かし情報を生成する。この電子透かし情報の生成には、ハッシュ関数、疑似乱数発生器、公開鍵暗号、共通鍵暗号、他の暗号プリミティブ（例えば、メッセージ認証符号 Message Authentication Code : MAC）等が用いられる。続いて、電子透かし検証部 1 5 6 5 は、生成した電子透かし情報と、電子透かし抽出部 1 5 6 3 が抽出した電子透かし情報とを比較する。

40

【 0 1 6 9 】

電子透かし検証部 1 5 6 5 は、生成した電子透かし情報と抽出された電子透かし情報とが同一である場合には、制御化装置 1 2 5 等によって生成された物理データ等に改ざんがなされていないと判断する。また、電子透かし検証部 1 5 6 5 は、生成した電子透かし情報と抽出された電子透かし情報とが同一ではない場合には、物理データに改ざんがなされたと判断する。

【 0 1 7 0 】

電子透かし検証部 1 5 6 5 は、物理データに改ざんがなされていた場合には、その旨を排除機器特定部 1 5 1 1 に通知する。これにより、排除機器特定部 1 5 1 1 は、改ざんを

50

加えうる操作がなされている制御化機器 1 2 5 等を、局所電力管理システム 1 内から排除することが可能となる。

【 0 1 7 1 】

以上、機器管理部 1 1 2 1 の構成について、詳細に説明した。

【 0 1 7 2 】

< 情報分析部の構成について >

続いて、情報分析部 1 1 2 3 の構成について、詳細に説明する。図 2 5 は、情報分析部の構成を説明するためのブロック図である。

【 0 1 7 3 】

情報分析部 1 1 2 3 は、機器管理部 1 1 2 1 が取得したり生成したりした情報に基づいて、図 8 に示したような、各種データの解析結果である二次情報を生成する処理部である。この情報分析部 1 1 2 3 は、例えば図 2 5 に示したように、機器状態判定部 1 6 0 1 と、電力状態判定部 1 6 0 3 と、を更に有する。

10

【 0 1 7 4 】

機器状態判定部 1 6 0 1 は、例えば、CPU、ROM、RAM 等により実現される。機器状態判定部 1 6 0 1 は、機器管理部 1 1 2 1 が取得した各種の管理機器情報に基づいて、管理機器それぞれについて、その機器の状態を判定する。機器状態判定部 1 6 0 1 は、判定の結果、ある管理機器の状態が異常であると判断した場合には、表示部 1 1 6 を介して異常をユーザに通知するとともに、制御部 1 1 5 に対して、異常な状態にあると判断される管理機器の制御を要請する。

20

【 0 1 7 5 】

電力状態判定部 1 6 0 3 は、例えば、CPU、ROM、RAM 等により実現される。電力状態判定部 1 6 0 3 は、機器管理部 1 1 2 1 が各装置から取得した電力情報に基づいて、電力管理システム 1 1 が電力状態を管理している局所電力管理システム 1 内の電力状態を判定する。電力状態判定部 1 6 0 3 は、判定の結果、ある管理機器の状態が異常であると判断した場合には、表示部 1 1 6 を介して異常をユーザに通知するとともに、制御部 1 1 5 に対して、異常な状態にあると判断される管理機器の電力状態の制御を要請する。

【 0 1 7 6 】

以上、本実施形態に係る電力管理装置 1 1 の機能の一例を示した。上記の各構成要素は、汎用的な部材や回路を用いて構成されていてもよいし、各構成要素の機能に特化したハードウェアにより構成されていてもよい。また、各構成要素の機能を、CPU 等が全て行ってもよい。従って、本実施形態を実施する時々の技術レベルに応じて、適宜、利用する構成を変更することが可能である。

30

【 0 1 7 7 】

なお、上述のような本実施形態に係る電力管理装置の各機能を実現するためのコンピュータプログラムを作製し、パーソナルコンピュータ等を実装することが可能である。また、このようなコンピュータプログラムが格納された、コンピュータで読み取り可能な記録媒体も提供することができる。記録媒体は、例えば、磁気ディスク、光ディスク、光磁気ディスク、フラッシュメモリなどである。また、上記のコンピュータプログラムは、記録媒体を用いずに、例えばネットワークを介して配信してもよい。

40

【 0 1 7 8 】

< 制御化機器の構成について >

続いて、図 2 6 を参照しながら、本実施形態に係る制御化機器の構成について、詳細に説明する。図 2 6 は、本実施形態に係る制御化機器の構成を説明するためのブロック図である。

【 0 1 7 9 】

制御化機器 1 2 5 は、図 2 6 に例示したように、制御部 2 0 0 1、センサ 2 0 0 3、バッテリー 2 0 0 5、機能提供部 2 0 0 7、局所通信部 2 0 0 9、入力部 2 0 1 1、表示部 2 0 1 3 及び記憶部 2 0 1 5 等を主に備える。

【 0 1 8 0 】

50

制御部 2001 は、例えば、CPU、ROM、RAM 等により実現される。制御部 2001 は、制御化機器 125 が備える処理部の実行制御を行う処理部である。また、この制御部 2001 は、電力管理装置 11 に対して、先に説明したような、自身に関する一次情報等を送信する。更に、制御部 2001 は、一時的に登録された電力管理機器から電力供給を受けた場合に、後述するような電力使用証明書を作成する。なお、この制御部 2001 の構成については、以下で改めて詳細に説明する。

【0181】

センサ 2003 は、バッテリーの状態を監視する電流センサもしくは電圧センサ、又は、制御化機器 125 の設置箇所の周囲環境を監視する温度センサ、湿度センサもしくは気圧計等のような、各種の物理データを取得可能なセンサからなる。センサ 2003 は、制御部 2001 の制御に基づいて、所定の時間間隔毎、又は、任意のタイミングで、各種の物理データの測定を行って、得られた物理データを、センサ情報として制御部 2001 に出力する。

10

【0182】

バッテリー 2005 は、制御化機器 125 が備える蓄電装置であり、1 または複数のセルから構成されて、制御化機器 125 が動作するために要する電力を供給する。このバッテリー 2005 には、外部電力又はシステム 1 内に存在する発電装置 129, 130 から電力が供給され、蓄電される。このバッテリー 2005 は、制御部 2001 によって制御され、所定の時間間隔毎、又は、任意のタイミングで、各種の物理データを、バッテリー情報として制御部 2001 に出力する。

20

【0183】

なお、図 26 では、制御化機器 125 がバッテリー 2005 を備えている場合について図示したが、制御化機器 125 の種別によっては、バッテリー 2005 を備えずに、電力が直接制御化機器 125 に給電されるような構成となってもよい。

【0184】

機能提供部 2007 は、例えば、CPU、ROM、RAM、各種のデバイス等により実現される。機能提供部 2007 は、制御化機器 125 がユーザに提供する特定の機能（例えば、炊飯機能、冷蔵機能、各種コンテンツを記録したり実行したりする機能等）を実現する処理部である。この機能提供部 2007 は、制御部 2001 の制御に基づいて、これらの機能をユーザに提供する。

30

【0185】

局所通信部 2009 は、例えば、CPU、ROM、RAM、通信装置等により実現される。局所電力管理システム 1 の内部に構築された通信網を介して通信するための通信手段である。局所通信部 2009 は、局所電力管理システム 1 の内部に構築された通信網を介して、本実施形態に係る電力管理装置 11 と相互に通信を行うことが可能である。

【0186】

入力部 2011 は、例えば、CPU、ROM、RAM、入力装置等により実現される。この入力部 2011 は、ユーザが情報を入力するための入力手段である。なお、入力部 2011 としては、例えば、キーボードやボタン等が用いられる。また、後述する表示部 2013 を入力部 2011 と組み合わせて、タッチパネルを構成することも可能である。

40

【0187】

表示部 2013 は、例えば、CPU、ROM、RAM、出力装置等により実現される。表示部 2013 は、制御化機器 125 における消費電力に関する情報、ユーザ情報、課金情報、その他電力管理に関する情報、局所電力管理システム 1 外における電力管理に関する情報、電力取引に関する情報等を表示するための表示手段である。なお、表示手段としては、例えば、LCD や ELD 等が用いられる。

【0188】

記憶部 2015 は、制御化機器 125 が有するストレージ装置の一例である。記憶部 2015 には、制御化機器 125 に固有の識別情報、制御化機器 125 が保持する各種の鍵に関する情報、制御化機器 125 が保持する各種のデジタル署名や証明書等が格納される

50

。また、記憶部 2015 には、各種の履歴情報が記録されていてもよい。さらに、記憶部 2015 には、本実施形態に係る制御化機器 125 が、何らかの処理を行う際に保存する必要が生じた様々なパラメータや処理の途中経過等、または、各種のデータベース等が、適宜記録される。この記憶部 2015 には、制御化機器 125 の有する各処理部が、自由に読み書きを行うことが可能である。

【0189】

[制御部の構成について - その 1]

以上、本実施形態に係る制御化機器 125 の全体構成について説明した。以下では、図 27 を参照しながら、制御化機器 125 の有する制御部 2001 の構成について、より詳細に説明する。

【0190】

制御化機器 125 の有する制御部 2001 は、図 27 に例示したように、認証処理部 2021 と、センサ制御部 2023 と、センサ情報出力部 2025 と、バッテリー制御部 2027 と、バッテリー情報出力部 2029 と、を更に有する。

【0191】

認証処理部 2021 は、例えば、CPU、ROM、RAM 等により実現される。認証処理部 2021 は、電力管理装置 11 との間で所定のプロトコルに則して認証処理を行うとともに、制御化機器 125 を電力管理装置 11 に登録する処理を行う。認証処理部 2021 は、電力管理装置 11 との間で処理を行うにあたって、記憶部 2015 等に格納されている各種の鍵や、制御化装置 125 の製造時に製造元によって提供されたデジタル署名又は証明書類や、各種のパラメータ等を利用することが可能である。認証処理部 2021 が実施する認証処理は、特定のものに限定されるわけではなく、システム 1 の内容や構成に応じて任意のものを利用することが可能である。

【0192】

センサ制御部 2023 は、例えば、CPU、ROM、RAM 等により実現される。センサ制御部 2023 は、制御化機器 125 が備えるセンサ 2003 を制御する処理部である。センサ制御部 2023 は、所定の方法によりセンサ 2003 の制御を行うとともに、所定の時間間隔毎、又は、任意のタイミングで、センサ 2003 により測定される物理データを取得し、後述するセンサ情報出力部 2025 に出力する。

【0193】

センサ情報出力部 2025 は、例えば、CPU、ROM、RAM 等により実現される。センサ情報出力部 2025 は、センサ制御部 2023 から出力されたセンサ情報を、局所通信部 2009 を介して、電力管理装置 11 に出力する。また、センサ情報出力部 2025 は、センサ情報を出力するに際して、ノイズ除去処理やデジタル化処理等の前処理を実施してもよい。また、センサ情報出力部 2025 は、センサ制御部 2023 から取得した情報を利用して各種の二次情報を生成し、センサ情報として出力してもよい。

【0194】

バッテリー制御部 2027 は、例えば、CPU、ROM、RAM 等により実現される。バッテリー制御部 2027 は、制御化機器 125 が備えるバッテリー 2005 を制御する処理部である。バッテリー制御部 2027 は、バッテリー 2005 内に蓄電されている電力を利用して、制御化機器 125 を機能させるとともに、状況によっては、バッテリー 2005 内に格納されている電力を、制御化機器 125 の外部に供給する。このバッテリー制御部 2023 は、所定の方法によりバッテリー 2005 の制御を行うとともに、所定の時間間隔毎、又は、任意のタイミングで、バッテリー 2005 により測定される物理データを取得し、後述するバッテリー情報出力部 2029 に出力する。

【0195】

バッテリー情報出力部 2029 は、例えば、CPU、ROM、RAM 等により実現される。バッテリー情報出力部 2029 は、バッテリー制御部 2027 から出力されたバッテリー情報を、局所通信部 2009 を介して、電力管理装置 11 に出力する。また、バッテリー情報出力部 2029 は、バッテリー情報を出力するに際して、ノイズ除去処理やデジ

10

20

30

40

50

タル化処理等の前処理を実施してもよい。また、バッテリー情報出力部 2029 は、バッテリー制御部 2027 から取得した情報を利用して各種の二次情報を生成し、バッテリー情報として出力してもよい。

【0196】

[制御部の構成について - その2]

また、制御化機器 125 の有する制御部 2001 は、図 27 に示したような構成ではなく、以下で説明するような構成を有していても良い。以下では、図 28 を参照しながら、制御化機器 125 の有する制御部 2001 の構成について、より詳細に説明する。

【0197】

制御化機器 125 の有する制御部 2001 は、図 28 に例示したように、認証処理部 2021 と、センサ制御部 2023 と、バッテリー制御部 2027 と、改ざん検知情報生成部 2031 と、を更に有していてもよい。

10

【0198】

図 28 に示した認証処理部 2021 は、図 27 に示した認証処理部 2021 と同様の構成を有し、同様の効果を奏するものであるため、詳細な説明は省略する。また、図 28 に示したセンサ制御部 2023 及びバッテリー制御部 2027 は、センサ制御情報及びバッテリー情報を改ざん検知情報生成部 2031 に出力する以外は、図 27 に示した各処理部と同様の構成を有し、同様の効果を奏する。従って、以下では、詳細な説明を省略する。

【0199】

改ざん検知情報生成部 2031 は、例えば、CPU、ROM、RAM 等により実現される。改ざん検知情報生成部 2031 は、センサ制御部 2023 から出力されたセンサ情報、及び、バッテリー制御部 2027 から出力されたバッテリー情報に基づいて、情報に改ざんが加えられたか否かの検知に利用される改ざん検知情報を生成する。改ざん検知情報生成部 2031 は、生成した改ざん検知情報を、局所通信部 2009 を介して、電力管理装置 11 に送信する。また、電力管理装置 11 は、改ざん検知情報生成部 2031 が生成した改ざん検知情報を、局所電力管理システム 1 の外部に設けられた解析サーバ 34 等の各種サーバに伝送してもよい。

20

【0200】

[改ざん検知情報生成部の構成について]

以下では、図 29 を参照しながら、改ざん検知情報生成部の詳細な構成について改めて説明する。図 29 は、改ざん検知情報生成部の構成を説明するためのブロック図である。

30

【0201】

改ざん検知情報生成部 2031 は、図 29 に例示したように、機器特徴情報生成部 2033 と、電子透かし生成部 2035 と、埋め込み位置決定部 2037 と、電子透かし埋め込み部 2039 と、を更に有する。

【0202】

機器特徴情報生成部 2033 は、例えば、CPU、ROM、RAM 等により実現される。機器特徴情報生成部 2033 は、センサ制御部 2023 及びバッテリー制御部 2027 から出力されたセンサ情報及びバッテリー情報に基づいて、制御化機器 125 を特徴付ける特徴量情報である機器特徴情報を生成する。機器特徴情報生成部 2033 は、センサ情報及びバッテリー情報そのものを機器特徴情報として使用してもよいし、センサ情報及びバッテリー情報を利用して新たに生成される情報を機器特徴情報として使用してもよい。機器特徴情報生成部 2033 は、生成した機器特徴情報を、後述する埋め込み位置決定部 2037 及び電子透かし埋め込み部 2039 に出力する。

40

【0203】

なお、機器特徴情報生成部 2033 は、機器特徴情報の生成に先立ち、入力されたセンサ情報及びバッテリー情報の検証を行ってもよい。この場合、機器特徴情報生成部 2033 は、記憶部 2013 等に格納されているデータベース等を参照して、センサ情報及びバッテリー情報等の物理データが取り得る値の範囲を取得し、得られた物理データがこの範囲内に存在しているかを判断してもよい。また、機器特徴情報生成部 2033 は、得られ

50

た物理データを解析して、制御化機器 1 2 5 が異常な挙動を示していないかを確認してもよい。機器特徴情報生成部 2 0 3 3 は、これらの検証によって、物理データの正当性が確認できない状況や異常な挙動を検知した場合には、表示部 2 0 1 3 を介して、このような状況をユーザに通知してもよい。

【 0 2 0 4 】

電子透かし生成部 2 0 3 5 は、例えば、CPU、ROM、RAM等により実現される。電子透かし生成部 2 0 3 5 は、制御化機器 1 2 5 と、電力管理装置 1 1 又は解析サーバ 3 4 等の外部サーバとの間で共有される、鍵情報や識別番号に関する情報などの共有情報を利用して、改ざん検知情報として利用される電子透かし情報を生成する。

【 0 2 0 5 】

電子透かし生成部 2 0 3 5 によって生成される電子透かし情報は、例えば、共有情報そのもの、共有情報を基に生成した疑似乱数列、制御化機器 1 2 5 に固有なID情報等の固有値を利用して生成した情報等を利用して生成可能である。電子透かし情報の生成・埋め込み方法や、電子透かし情報の埋め込みそのものを明らかにしない場合には、かかる情報を利用した電子透かし情報を用いることで、情報の改ざんを検知することが可能となる。

【 0 2 0 6 】

また、以下で説明するような方法で生成される電子透かし情報が埋め込まれた物理データは、電力管理装置 1 1 を介して、解析サーバ 3 4 等の外部サーバにも転送されうる。他方、悪意のある第三者等によって、仲介装置である電力管理装置 1 1 が乗っ取られる場合が生じる可能性がある。この場合には、電力管理装置 1 1 を乗っ取った第三者は、乗っ取りを正規のユーザや外部サーバの管理者等に気づかせないようにするために、乗っ取る以前に利用された改ざん検知情報を再利用する等といった、不正行為を行う場合が考えられる。そこで、電子透かし生成部 2 0 3 5 は、上述のような情報だけでなく、時刻情報をも利用した電子透かし情報を定期的に生成することで、上述のような電力管理装置 1 1 の乗っ取り等も検知することが可能となる。

【 0 2 0 7 】

電子透かし生成部 2 0 3 5 は、電子透かし情報を生成するために、ハッシュ関数、公開鍵暗号、疑似乱数発生器、共通鍵暗号、他の暗号プリミティブ(MAC)など、各種の技術を利用することが可能である。この場合、出力された電子透かし情報のデータサイズは、mビットであるとする。

【 0 2 0 8 】

このように、本実施形態に係る電子透かし生成部 2 0 3 5 は、物理データを利用して電子透かし情報を生成し、物理データそのものは電子透かし情報としない。

【 0 2 0 9 】

電子透かし生成部 2 0 3 5 は、生成した電子透かし情報を、後述する電子透かし埋め込み部 2 0 3 9 に出力する。

【 0 2 1 0 】

埋め込み位置決定部 2 0 3 7 は、例えば、CPU、ROM、RAM等により実現される。埋め込み位置決定部 2 0 3 7 は、機器特徴情報生成部 2 0 3 3 から伝送された機器特徴情報を解析して、改ざん検知情報を機器特徴情報に埋め込む位置を決定する。具体的には、埋め込み位置決定部 2 0 3 7 は、機器特徴情報のうち、所定の閾値以上の大きな値を有している領域、分散の大きな領域、雑音領域に対応する領域、また、周波数領域のデータを扱う場合には高周波領域などを、埋め込み位置として決定する。このようなデータ中の雑音が大きい領域、SN比が大きい領域等は、かかる領域に電子透かし情報を埋め込んだとしても、機器特徴情報の全体的な傾向(例えば統計的な性質)に与える影響は少ない。そのため、かかる領域を、電子透かし情報の埋め込み位置として用いることで、電子透かし情報を、機器特徴情報とは別に送信する必要がなくなり、機器特徴情報の受信機能のみしか有さない電力管理装置 1 1 であっても、改ざんを検知することが可能となる。

【 0 2 1 1 】

埋め込み位置決定部 2 0 3 7 は、決定した埋め込み位置に関する位置情報を、後述する

10

20

30

40

50

電子透かし埋め込み部 2039 に出力する。なお、電子透かし情報の埋め込み位置が予め取り決められている場合には、かかる処理は行わなくとも良い。

【0212】

電子透かし埋め込み部 2039 は、例えば、CPU、ROM、RAM 等により実現される。電子透かし埋め込み部 2039 は、埋め込み位置決定部 2037 から通知された埋め込み位置に関する位置情報に基づいて、電子透かし生成部 2035 が生成した電子透かし情報を、機器特徴情報生成部 2033 が生成した機器特徴情報に埋め込む。これにより、電子透かし情報が埋め込まれた機器特徴情報が生成されることとなる。

【0213】

また、電子透かし埋め込み部 2039 は、電子透かし情報が埋め込まれた機器特徴情報を、再度検証してもよい。再度の検証により、この情報が機器特徴情報の取り得る値の範囲を超える値を有している場合や、明らかに異常な挙動を示す場合には、改ざん検知情報生成部 2031 は、再度、電子透かし情報の埋め込み処理を実行する。また、再試行回数が所定の閾値以上継続する場合には、電子透かし埋め込み部 2039 は、表示部 2013 を介して、このような状況をユーザに通知してもよい。

10

【0214】

なお、時刻情報を利用して、情報の改ざんの有無に加えて電力管理装置 11 の乗っ取りをも検証する場合には、時刻情報を上述のように電子透かし情報の一部として取り込んでも良く、時刻情報を電子透かし情報とは別に機器特徴情報に埋め込んでもよい。

【0215】

以上、本実施形態に係る制御化機器 125 の機能の一例を示した。上記の各構成要素は、汎用的な部材や回路を用いて構成されていてもよいし、各構成要素の機能に特化したハードウェアにより構成されていてもよい。また、各構成要素の機能を、CPU 等が全て行ってもよい。従って、本実施形態を実施する時々の技術レベルに応じて、適宜、利用する構成を変更することが可能である。

20

【0216】

例えば、図 26 では、バッテリー 2005 が制御化機器 125 と一体になっている場合について図示しているが、バッテリー 2005 は、制御化機器 125 と別体になっ

【0217】

また、制御化装置 125 は、図 26 に示した処理部に加えて、広域通信部のような通信機能を更に有していてもよい。

30

【0218】

なお、上述のような本実施形態に係る制御化機器の各機能を実現するためのコンピュータプログラムを作製し、パーソナルコンピュータ等に実装することが可能である。また、このようなコンピュータプログラムが格納された、コンピュータで読み取り可能な記録媒体も提供することができる。記録媒体は、例えば、磁気ディスク、光ディスク、光磁気ディスク、フラッシュメモリなどである。また、上記のコンピュータプログラムは、記録媒体を用いずに、例えばネットワークを介して配信してもよい。

【0219】

<蓄電装置の構成について>

続いて、図 30 を参照しながら、本実施形態に係る蓄電装置 128 の構成について、詳細に説明する。図 30 は、本実施形態に係る蓄電装置の構成を説明するためのブロック図である。

40

【0220】

蓄電装置 128 は、図 30 に例示したように、制御部 2501、センサ 2503、セル 2505、局所通信部 2507、表示部 2509 及び記憶部 2511 等を主に備える。

【0221】

制御部 2501 は、例えば、CPU、ROM、RAM 等により実現される。制御部 2501 は、蓄電装置 128 が備える処理部の実行制御を行う処理部である。また、この制御

50

部 2 5 0 1 は、電力管理装置 1 1 に対して、先に説明したような、自身に関する一次情報等を送信する。更に、制御部 2 5 0 1 は、後述するセル 2 5 0 5 に故障等の問題が発生した場合には、セルの再構成（セル構成の組み換え）を実施する。この制御部 2 5 0 1 の構成については、以下で改めて詳細に説明する。

【 0 2 2 2 】

センサ 2 5 0 3 は、セル 2 5 0 5 の状態を監視する電流センサもしくは電圧センサ、又は、蓄電装置 1 2 8 の設置箇所の周囲環境を監視する温度センサ、湿度センサもしくは気圧計等のような、各種の物理データを取得可能なセンサからなる。センサ 2 5 0 3 は、制御部 2 5 0 1 の制御に基づいて、所定の時間間隔毎、又は、任意のタイミングで、各種の物理データの測定を行って、得られた物理データを、センサ情報として制御部 2 5 0 1 に出力する。

10

【 0 2 2 3 】

セル 2 5 0 5 は、蓄電装置 1 2 8 が備える蓄電デバイスであり、1 または複数のセルから構成されて、電力を蓄電装置 1 2 8 及び蓄電装置 1 2 8 の外部に設けられた装置へと供給する。このセル 2 5 0 5 には、外部電力又はシステム 1 内に存在する発電装置 1 2 9 , 1 3 0 から電力が供給され、蓄電される。このセル 2 5 0 5 は、制御部 2 5 0 1 によって制御され、所定の時間間隔毎、又は、任意のタイミングで、各種の物理データを、セル情報として制御部 2 5 0 1 に出力する。

【 0 2 2 4 】

局所通信部 2 5 0 7 は、例えば、CPU、ROM、RAM、通信装置等によって実現される。局所電力管理システム 1 の内部に構築された通信網を介して通信するための通信手段である。局所通信部 2 5 0 7 は、局所電力管理システム 1 の内部に構築された通信網を介して、本実施形態に係る電力管理装置 1 1 と相互に通信を行うことが可能である。

20

【 0 2 2 5 】

表示部 2 5 0 9 は、例えば、CPU、ROM、RAM、出力装置等によって実現される。表示部 2 5 0 9 は、蓄電装置 1 2 8 における消費電力に関する情報、ユーザ情報、課金情報、その他電力管理に関する情報、局所電力管理システム 1 外における電力管理に関する情報、電力取引に関する情報等を表示するための表示手段である。なお、表示手段としては、例えば、LCD や ELD 等が用いられる。

【 0 2 2 6 】

記憶部 2 5 1 1 は、蓄電装置 1 2 8 が備えるストレージ装置の一例である。記憶部 2 5 1 1 には、蓄電装置 1 2 8 に固有の識別情報、蓄電装置 1 2 8 が保持する各種の鍵に関する情報、蓄電装置 1 2 8 が保持する各種のデジタル署名や証明書等が格納される。また、記憶部 2 5 1 1 には、各種の履歴情報が記録されていてもよい。さらに、記憶部 2 5 1 1 には、本実施形態に係る蓄電装置 1 2 8 が、何らかの処理を行う際に保存する必要が生じた様々なパラメータや処理の途中経過等、または、各種のデータベース等が、適宜記録される。この記憶部 2 5 1 1 には、蓄電装置 1 2 8 の有する各処理部が、自由に読み書きを行うことが可能である。

30

【 0 2 2 7 】

[制御部の構成について - その 1]

以上、本実施形態に係る蓄電装置 1 2 8 の全体構成について説明した。以下では、図 3 1 を参照しながら、蓄電装置 1 2 8 の有する制御部 2 5 0 1 の構成について、より詳細に説明する。

40

【 0 2 2 8 】

蓄電装置 1 2 8 の有する制御部 2 5 0 1 は、図 3 1 に例示したように、認証処理部 2 5 2 1 と、センサ制御部 2 5 2 3 と、センサ情報出力部 2 5 2 5 と、セル制御部 2 5 2 7 と、セル情報出力部 2 5 2 9 と、を更に有する。

【 0 2 2 9 】

認証処理部 2 5 2 1 は、例えば、CPU、ROM、RAM 等により実現される。認証処理部 2 5 2 1 は、電力管理装置 1 1 との間で所定のプロトコルに則して認証処理を行うと

50

ともに、蓄電装置 1 2 8 を電力管理装置 1 1 に登録する処理を行う。認証処理部 2 5 2 1 は、電力管理装置 1 1 との間で処理を行うにあたって、記憶部 2 5 1 5 等に格納されている各種の鍵や、蓄電装置 1 2 8 の製造時に製造元によって提供されたデジタル署名又は証明書類や、各種のパラメータ等を利用することが可能である。認証処理部 2 5 2 1 が実施する認証処理は、特定のものに限定されるわけではなく、システム 1 の内容や構成に応じて任意のものを利用することが可能である。

【 0 2 3 0 】

センサ制御部 2 5 2 3 は、例えば、CPU、ROM、RAM 等により実現される。センサ制御部 2 5 2 3 は、蓄電装置 1 2 8 が備えるセンサ 2 5 0 3 を制御する処理部である。センサ制御部 2 5 2 3 は、所定の方法によりセンサ 2 5 0 3 の制御を行うとともに、所定の時間間隔毎、又は、任意のタイミングで、センサ 2 5 0 3 により測定される物理データを取得し、後述するセンサ情報出力部 2 5 2 5 に出力する。

10

【 0 2 3 1 】

センサ情報出力部 2 5 2 5 は、例えば、CPU、ROM、RAM 等により実現される。センサ情報出力部 2 5 2 5 は、センサ制御部 2 5 2 3 から出力されたセンサ情報を、局所通信部 2 5 0 9 を介して、電力管理装置 1 1 に出力する。また、センサ情報出力部 2 5 2 5 は、センサ情報を出力するに際して、ノイズ除去処理やデジタル化処理等の前処理を実施してもよい。また、センサ情報出力部 2 5 2 5 は、センサ制御部 2 5 2 3 から取得した情報を利用して各種の二次情報を生成し、センサ情報として出力してもよい。

【 0 2 3 2 】

20

セル制御部 2 5 2 7 は、例えば、CPU、ROM、RAM 等により実現される。セル制御部 2 5 2 7 は、蓄電装置 1 2 8 が備えるセル 2 5 2 7 を制御する処理部である。セル制御部 2 5 2 7 は、セル 2 5 0 5 内に蓄電されている電力を利用して、蓄電装置 1 2 8 を機能させるとともに、状況によっては、セル 2 5 0 5 内に格納されている電力を、蓄電装置 1 2 8 の外部に供給する。このセル制御部 2 5 2 3 は、所定の方法によりセル 2 5 0 5 の制御を行うとともに、所定の時間間隔毎、又は、任意のタイミングで、セル 2 5 0 5 により測定される物理データを取得し、後述するセル情報出力部 2 5 2 9 に出力する。

【 0 2 3 3 】

セル情報出力部 2 5 2 9 は、例えば、CPU、ROM、RAM 等により実現される。セル情報出力部 2 5 2 9 は、セル制御部 2 5 2 7 から出力されたセル情報を、局所通信部 2 5 0 9 を介して、電力管理装置 1 1 に出力する。また、セル情報出力部 2 5 2 9 は、セル情報を出力するに際して、ノイズ除去処理やデジタル化処理等の前処理を実施してもよい。また、セル情報出力部 2 5 2 9 は、セル制御部 2 5 2 7 から取得した情報を利用して各種の二次情報を生成し、セル情報として出力してもよい。

30

【 0 2 3 4 】

[制御部の構成について - その 2]

また、蓄電装置 1 2 8 の有する制御部 2 5 0 1 は、図 3 1 に示したような構成ではなく、以下で説明するような構成を有していても良い。以下では、図 3 2 を参照しながら、蓄電装置 1 2 8 の有する制御部 2 5 0 1 の構成について、より詳細に説明する。

【 0 2 3 5 】

40

蓄電装置 1 2 8 の有する制御部 2 5 0 1 は、図 3 2 に例示したように、認証処理部 2 5 2 1 と、センサ制御部 2 5 2 3 と、セル制御部 2 5 2 7 と、改ざん検知情報生成部 2 5 3 1 と、を更に有していてもよい。

【 0 2 3 6 】

図 3 2 に示した認証処理部 2 5 2 1 は、図 3 1 に示した認証処理部 2 5 2 1 と同様の構成を有し、同様の効果を奏するものであるため、詳細な説明は省略する。また、図 3 2 に示したセンサ制御部 2 5 2 3 及びセル制御部 2 5 2 7 は、センサ制御情報及びセル情報を改ざん検知情報生成部 2 5 3 1 に出力する以外は、図 3 1 に示した各処理部と同様の構成を有し、同様の効果を奏する。従って、以下では、詳細な説明を省略する。

【 0 2 3 7 】

50

改ざん検知情報生成部 2 5 3 1 は、例えば、CPU、ROM、RAM等により実現される。改ざん検知情報生成部 2 5 3 1 は、センサ制御部 2 5 2 3 から出力されたセンサ情報、及び、セル制御部 2 5 2 7 から出力されたバッテリー情報に基づいて、情報に改ざんが加えられたか否かの検知に利用される改ざん検知情報を生成する。改ざん検知情報生成部 2 5 3 1 は、生成した改ざん検知情報を、局所通信部 2 5 0 9 を介して、電力管理装置 1 1 に送信する。また、電力管理装置 1 1 は、改ざん検知情報生成部 2 5 3 1 が生成した改ざん検知情報を、局所電力管理システム 1 の外部に設けられた解析サーバ 3 4 等の各種サーバに伝送してもよい。

【 0 2 3 8 】

[改ざん検知情報生成部の構成について]

以下では、図 3 3 を参照しながら、改ざん検知情報生成部の詳細な構成について改めて説明する。図 3 3 は、改ざん検知情報生成部の構成を説明するためのブロック図である。

【 0 2 3 9 】

改ざん検知情報生成部 2 5 3 1 は、図 3 3 に例示したように、機器特徴情報生成部 2 5 3 3 と、電子透かし生成部 2 5 3 5 と、埋め込み位置決定部 2 5 3 7 と、電子透かし埋め込み部 2 5 3 9 と、を更に有する。

【 0 2 4 0 】

機器特徴情報生成部 2 5 3 3 は、センサ制御部 2 5 2 3 から出力されたセンサ情報及びセル制御部 2 5 2 7 から出力されたセル情報に基づいて機器特徴情報を生成する以外は、図 2 9 に示した機器特徴情報生成部 2 0 3 3 と同様の機能を有し、同様の効果を奏する。従って、以下では、詳細な説明は省略する。

【 0 2 4 1 】

また、電子透かし生成部 2 5 3 5、埋め込み位置決定部 2 5 3 7 及び電子透かし埋め込み部 2 5 3 9 は、図 2 9 に示した各処理部と同様の構成を有し、同様の効果を奏するものであるため、以下では、詳細な説明は省略する。

【 0 2 4 2 】

以上、本実施形態に係る蓄電装置 1 2 8 の機能の一例を示した。上記の各構成要素は、汎用的な部材や回路を用いて構成されていてもよいし、各構成要素の機能に特化したハードウェアにより構成されていてもよい。また、各構成要素の機能を、CPU等が全て行ってもよい。従って、本実施形態を実施する時々の技術レベルに応じて、適宜、利用する構成を変更することが可能である。

【 0 2 4 3 】

例えば、蓄電装置 1 2 8 は、図 3 0 に示した処理部に加えて、広域通信部のような通信機能を更に有していてもよい。

【 0 2 4 4 】

なお、上述のような本実施形態に係る蓄電装置の各機能を実現するためのコンピュータプログラムを作製し、蓄電機能を有するパーソナルコンピュータ等に実装することが可能である。また、このようなコンピュータプログラムが格納された、コンピュータで読み取り可能な記録媒体も提供することができる。記録媒体は、例えば、磁気ディスク、光ディスク、光磁気ディスク、フラッシュメモリなどである。また、上記のコンピュータプログラムは、記録媒体を用いずに、例えばネットワークを介して配信してもよい。

【 0 2 4 5 】

< 電子透かし情報の埋め込み方法及び検証方法の具体例 >

以下では、電子透かし情報の埋め込み方法及び検証方法の具体例について、詳細に説明する。

【 0 2 4 6 】

情報化・ネットワーク化・インテリジェント化された局所電力管理システム 1 では、システム内の各種機器の電力使用について、システム全体の電力利用が最適化されるように、電力管理装置 1 1 が各種機器 / バッテリーなどと通信を行う。これにより、電力管理装置 1 1 は、各機器 / バッテリーからのセンサ情報や日時、電力価格、気温、住人が在宅・

10

20

30

40

50

在室か否かなどの状況をモニターし、その状況に合わせて、各機器の動作モードや上限電流値を設定するなどの制御を行う。また、電力管理装置 11 を介した家庭外からの制御、セキュリティチェックサーバの支援による高度なセキュリティ対策、最適化など、様々なサービスの享受が可能となる。

【0247】

この際、外部から機器/バッテリーへのアクセスが可能となるため、機器/バッテリーへの異常動作指令、電力管理装置を踏み台にした他の家庭の電力管理装置/機器/バッテリーへの攻撃、DoS 攻撃、情報漏洩など、セキュリティ上の脅威が高まる。これらの対策として、電力管理装置 11 でのトラフィック管理、ウィルス対策、ファイアウォール設置が考えられる。また、未知の攻撃に対しては、機器/バッテリーのセンサ情報や実行命令情報を、解析サーバ 34 等のセキュリティチェックサーバへ送付し、物理シミュレーションや学習理論を利用して危険度予測、不正利用検知を行うことも想定される。

10

【0248】

しかしながら、これらの対策では、電力管理装置の正常動作が前提であるため、外部攻撃者により電力管理装置の制御機能が奪われた場合は、これらの防御は役に立たない。また、製造・管理コストの観点から機器/バッテリーの防御性は比較的低下すると予想されるため、電力管理装置が制御機能を奪われた状況下では、想定された機器/バッテリーは無力である。更に、不正な電力管理装置が正規の電力管理装置になりすまし、物理データを改ざんしてセキュリティチェックサーバへ送信する攻撃が考えられるが、サービス側での不正な電力管理装置と正当な電力管理装置の区別は困難なため、攻撃の検知が困難となる。従来コンピュータへの攻撃と比較し、機器/バッテリーへの攻撃は甚大な被害をもたらす危険性が高いため、電力管理装置だけでなく、機器/バッテリー側でもある程度のセキュリティ機能を持つ必要がある。

20

【0249】

そこで、本実施形態では、先に説明したように、機器/バッテリーのセンサ等により得られる物理データに対して、不正改ざん防止用の電子透かしを挿入することが可能である。この手法を用いれば、通信路上で攻撃者により物理データが改ざんされた場合であっても、攻撃の検知が可能である。また、電力管理装置の制御機能が奪われた場合も、時間情報が入った電子透かし情報を定期的にセキュリティチェックサーバへ送信することで、サービスとの協調によって制御機能が奪われたことを検知できる。更に、電子透かし情報を用いることで、例えば MAC などの認証情報を物理データとは別に送信する必要がないため、物理データの受信のみに対応した電力管理装置でも使用できる。

30

【0250】

以下では、電子透かし情報の埋め込み方法及び検証方法について、例を挙げながら具体的に説明する。なお、以下の説明では、電子透かし情報は、ある一定時間に得た物理データ(機器特徴情報)に埋め込まれるものとする。また、物理データは、 n 個のデータからなる時系列データであり、時刻 k ($0 \leq k < n$) における物理データの値を、 X_k と表記することとする。また、各時刻の物理データ値は、センサ等から取得された後は離散化され、 r ビットのデータとなるものとする。また、電子透かし情報のデータサイズを m ビットとする。

40

【0251】

[共有情報を利用した電子透かし情報の埋め込み方法及び検証方法]

以下では、共有情報を利用した電子透かし情報の埋め込み方法及び検証方法について、具体例を挙げながら説明する。

【0252】

具体例 1

まず、制御化装置 125 等で実施される、電子透かし情報の埋め込み方法について説明する。

まず、改ざん検知情報生成部 2031 の埋め込み位置決定部 2037 は、所定の信号処理回路等を利用して、物理データ等の機器特徴情報の中から値の大きいデータを p 個選択

50

する。続いて、電子透かし埋め込み部 2039 は、所定の埋め込み処理回路等を利用して、時系列順に、選択された p 個の機器特徴情報の最下位ビット (Least Significant Bit: LSB) から数えて q(k) ビット分に、共有情報をもとに生成した電子透かし情報を順次挿入する。ここで、q(k) は、以下に示す条件 a を満たす値である。

【0253】

【数 1】

$$1 \leq q(k) \leq r-1, 0 \leq k \leq p-1, \sum_{k=0}^{p-1} q(k) = m \quad \dots (\text{条件 a})$$

10

【0254】

電子透かし情報埋め込み後の p 個の選択された機器特徴情報の値が p + 1 番目以降の値以下になる場合も生じうる。この場合、改ざん検知情報生成部 2031 の機器特徴情報生成部 2033 は、p + 1 番目以降の値が p 個の電子透かし情報埋め込み後の機器特徴情報の最小値未満になるように、電子透かし情報の埋め込み位置以外のデータを補正する。改ざん検知情報生成部 2031 は、補正後の値をもとに、電子透かし情報を更新し、条件を満たすまで、埋め込み処理を繰り返す。

【0255】

次に、電力管理装置 11 及び解析サーバ 34 等のセキュリティチェックサーバの情報改ざん検知部で実施される電子透かし情報の検証方法について説明する。

20

情報改ざん検知部の埋め込み位置特定部は、所定の信号処理回路等を利用して、物理データ等の機器特徴情報の中から値の大きいデータの位置を p 個特定する。続いて、電子透かし抽出部は、特定されたデータの位置を表す位置情報を利用し、所定の埋め込み抽出回路等を利用して、時系列順に、選択された p 個の機器特徴情報の最下位ビットから数えて q(k) ビット分の値を、順次抽出する。その後、電子透かし検証部は、記憶部等に格納された鍵情報などの共有情報を基に電子透かし情報を生成し、電子透かし抽出部が抽出した電子透かし情報と比較する。

【0256】

具体例 2

30

まず、制御化装置 125 等で実施される、電子透かし情報の埋め込み方法について説明する。

まず、改ざん検知情報生成部 2031 の埋め込み位置決定部 2037 は、所定の信号処理回路等を利用して、以下の式 101 で表される離散フーリエ変換、又は、以下の式 102 で表される離散コサイン変換により、時間領域の機器特徴情報 (物理データ) (X₀, X₁, ..., X_{n-1}) を、周波数領域のデータ列 (Y₀, Y₁, ..., Y_{n-1}) に変換する。

【0257】

【数 2】

$$y_j = \sum_{k=0}^{n-1} x_k e^{-\frac{2\pi}{n}jk}, j = 0, \dots, n-1 \quad \dots (\text{式 101})$$

40

$$y_j = \begin{cases} \frac{\sqrt{2}}{n} \sum_{k=0}^{n-1} x_k & (j=0) \\ \frac{2}{n} \sum_{k=0}^{n-1} x_k \cos \frac{(2k+1)j\pi}{2n} & (j \neq 0) \end{cases} \quad \dots (\text{式 102})$$

50

【 0 2 5 8 】

その後、埋め込み位置決定部 2 0 3 7 は、高周波成分（式 1 0 1 及び式 1 0 2 において、j が大きい成分）を、高い周波数から順に p 個選択する。続いて、電子透かし埋め込み部 2 0 3 9 は、所定の埋め込み処理回路等を利用して、選択された p 個の周波数領域データの最下位ビット（LSB）から数えて q（k）ビット分に、共有情報をもとに生成した電子透かし情報を順次挿入する。ここで、q（k）は、上記条件 a を満たす値である。

【 0 2 5 9 】

ここで、離散フーリエ変換を用いた場合の埋め込み方法としては、実数及び複素数両方に均等に割り振る、数値の大きい方に優先的に割り振る、など、任意の方法を用いることが可能である。

10

【 0 2 6 0 】

次に、電子透かし埋め込み部 2 0 3 9 は、所定の信号処理回路等を利用して、電子透かし情報埋め込み後の周波数領域のデータを、式 1 0 3 で表される逆離散フーリエ変換、又は、式 1 0 4 で表される逆離散コサイン変換により逆変換し、時間領域のデータ列に戻す。

【 0 2 6 1 】

【 数 3 】

$$x_k = \frac{1}{n} \sum_{j=0}^{n-1} y_j e^{2\pi j k / n}, \quad k=0, \dots, n-1 \quad \dots (式 1 0 3)$$

20

$$x_k = \frac{1}{\sqrt{2}} y_0 + \sum_{j=1}^{n-1} y_j \cos \frac{(2k+1)j\pi}{2n}, \quad k=0, \dots, n-1 \quad \dots (式 1 0 4)$$

【 0 2 6 2 】

次に、電力管理装置 1 1 及び解析サーバ 3 4 等のセキュリティチェックサーバの情報改ざん検知部で実施される電子透かし情報の検証方法について説明する。

情報改ざん検知部の埋め込み位置特定部は、まず、所定の信号処理回路等を利用して、上記式 1 0 1 で表される離散フーリエ変換、又は、上記式 1 0 2 で表される離散コサイン変換により、時間領域の機器特徴情報（物理データ）（ X_0, X_1, \dots, X_{n-1} ）を、周波数領域のデータ列（ Y_0, Y_1, \dots, Y_{n-1} ）に変換する。次に、埋め込み位置特定部は、高周波成分（式 1 0 1 及び式 1 0 2 において、j が大きい成分）を、高い周波数から順に p 個選択する。これにより、電子透かし情報の埋め込まれた位置を特定することができる。続いて、電子透かし抽出部は、特定されたデータの位置を表す位置情報を利用して、所定の埋め込み抽出回路等を利用して、選択された p 個の機器特徴情報の最下位ビットから数えて q（k）ビット分の値を、順次抽出する。その後、電子透かし検証部は、記憶部等に格納された鍵情報などの共有情報を基に電子透かし情報を生成し、電子透かし抽出部が抽出した電子透かし情報と比較する。

30

40

【 0 2 6 3 】

具体例 3

まず、制御化装置 1 2 5 等で実施される、電子透かし情報の埋め込み方法について説明する。

まず、改ざん検知情報生成部 2 0 3 1 の機器特徴情報生成部 2 0 3 3 は、機器特徴情報 X_k について、差分データ $S_k = X_k - X_{k-1}$ （ $1 \leq k \leq n-1$ ）を生成する。続いて、埋め込み位置決定部 2 0 3 7 は、連続する p - 1 個の差分データの和が所定の閾値未満であり、かつ、その条件を満たす連続データ列の中で二乗和が最大となる p - 1 の連続データ列 S_k （ $t \leq k \leq t + p - 2, 1 \leq t \leq n - p + 1$ ）を選択する。

【 0 2 6 4 】

50

続いて、電子透かし埋め込み部 2039 は、所定の埋め込み処理回路等を利用して、時系列順に、選択された p 個の機器特徴情報 $X_k (t-1 \leq k \leq t+p-2)$ の最下位ビット (LSB) から数えて $q(k)$ ビット分に、共有情報をもとに生成した電子透かし情報を順次挿入する。ここで、 $q(k)$ は、上記条件 a を満たす値である。

【0265】

電子透かし情報埋め込み後の p 個の選択された機器特徴情報の連続する差分データについて、和が閾値 未満であり、かつ、その条件を満たす連続データ列の中で二乗和が最大になる、という条件を満たさない場合も生じうる。この場合、改ざん検知情報生成部 2031 の機器特徴情報生成部 2033 は、条件が満たされるように、電子透かし情報の埋め込み位置以外のデータを補正する。改ざん検知情報生成部 2031 は、補正後の値をもとに、電子透かし情報を更新し、条件を満たすまで、埋め込み処理を繰り返す。

10

【0266】

次に、電力管理装置 11 及び解析サーバ 34 等のセキュリティチェックサーバの情報改ざん検知部で実施される電子透かし情報の検証方法について説明する。

情報改ざん検知部の埋め込み位置特定部は、まず、機器特徴情報 X_k について、差分データ $S_k = X_k - X_{k-1} (1 \leq k \leq n-1)$ を生成する。続いて、埋め込み位置特定部は、連続する $p-1$ 個の差分データの和が所定の閾値 未満であり、かつ、その条件を満たす連続データ列の中で二乗和が最大となる $p-1$ の連続データ列 $S_k (t-k \leq t+p-2, 1 \leq t \leq n-p+1)$ を選択する。これにより、電子透かし情報の埋め込まれた位置を特定することができる。

20

【0267】

続いて、電子透かし抽出部は、特定されたデータの位置を表す位置情報を利用して、所定の埋め込み抽出回路等を利用して、時系列順に、選択された p 個の機器特徴情報 $t-1 \leq k \leq t+p-2$ の最下位ビット (LSB) から数えて $q(k)$ ビット分の値を、順次抽出する。その後、電子透かし検証部は、記憶部等に格納された鍵情報などの共有情報を基に電子透かし情報を生成し、電子透かし抽出部が抽出した電子透かし情報と比較する。

【0268】

[共有情報及び時刻情報を利用した電子透かし情報の埋め込み方法及び検証方法]

以上、共有情報を利用した電子透かし情報の埋め込み方法及び検証方法を具体的に説明した。続いて、以下では、共有情報及び時刻情報を利用した電子透かし情報の埋め込み方法及び検証方法について、具体例を挙げながら説明する。

30

【0269】

なお、共有情報及び時刻情報を利用した電子透かし情報は、電力管理装置 11 の乗っ取り検知等に利用することも可能であるため、その検証は、通常、解析サーバ 34 等のセキュリティチェックサーバにより実施される。

【0270】

なお、時刻情報を利用した電子透かし情報の検証を行う場合、解析サーバ 34 等のセキュリティチェックサーバは、時刻情報の埋め込まれ方に応じて、検証方法を変更する。すなわち、時刻情報が電子透かし情報と共に埋め込まれている場合には、埋め込まれている時刻情報を抽出して、検証時におけるデータの生成処理に利用する。また、時刻情報が埋め込まれていない場合には、予め決められた時刻情報や、機器特徴情報の推定取得時刻に基づいて選択した 1 又は複数の時刻情報を用いて、電子透かし情報を生成する。

40

【0271】

具体例 1

まず、制御化装置 125 等で実施される、電子透かし情報の埋め込み方法について説明する。

改ざん検知情報生成部 2031 の電子透かし生成部 2035 は、所定の回路等を利用して、 n 個の機器特徴情報 (物理データ) の最上位ビット (Most Significant Bit: MSB) から数えて $r-m$ ビット ($1 \leq m \leq r-1$) のビット列と、鍵情報等の共有情報と、時刻情報と、場合によってはその他の情報とに基づき、 m ビットの電

50

子透かし情報を各機器特徴情報について生成する。

【0272】

続いて、埋め込み位置決定部2037は、所定の埋め込み回路等を利用し、各機器特徴情報について、最下位ビットから m ビット分に生成された電子透かし情報を埋め込む。この場合、電子透かし情報全体のデータサイズは、 nm ビットとなる。

【0273】

次に、解析サーバ34等のセキュリティチェックサーバの情報改ざん検知部で実施される電子透かし情報の検証方法について説明する。

まず、情報改ざん検知部の電子透かし抽出部は、所定の埋め込み抽出回路を利用して、 n 個の機器特徴情報の最下位ビットから数えて m ビット分のデータを、電子透かし情報として抽出する。続いて、電子透かし検証部は、 n 個の機器特徴情報の最上位ビットから数えて $r - m$ ビット($1 \leq m \leq r - 1$)のビット列と、鍵情報等の共有情報と、時刻情報と、埋め込み側で使用されたデータとに基づき、 m ビットの電子透かし情報を各機器特徴情報について生成する。その後、電子透かし検証部は、記憶部等に格納された鍵情報などの共有情報を基に電子透かし情報を生成し、電子透かし抽出部が抽出した電子透かし情報と比較する。

10

【0274】

なお、以上の説明では、時間領域のデータについて説明を行ったが、物理データ等の機器特徴情報を、離散フーリエ変換又は離散コサイン変換により変換した後の周波数領域のデータについても、同様の方式を利用することが可能である。

20

【0275】

具体例2

まず、制御化装置125等で実施される、電子透かし情報の埋め込み方法について説明する。

改ざん検知情報生成部2031の埋め込み位置決定部2037は、所定の信号処理回路等を利用して、物理データ等の機器特徴情報の中から値の大きいデータを p 個選択する。

【0276】

続いて、電子透かし生成部2035は、選択された p 個の機器特徴情報の最下位ビットから数えて q (k)ビット分を除く全ビット($nr - m$ ビット)と、鍵情報等の共有情報と、時刻情報と、場合によってはその他の情報とに基づき、 m ビットの電子透かし情報を生成する。ここで、 q (k)は、上記条件aを満たす値である。

30

【0277】

続いて、電子透かし埋め込み部2039は、所定の埋め込み処理回路等を利用して、時系列順に、選択された p 個の機器特徴情報の最下位ビットから数えて q (k)ビット分に、生成した電子透かし情報を順次挿入する。

【0278】

電子透かし情報埋め込み後の p 個の選択された機器特徴情報の値が $p + 1$ 番目以降の値以下になる場合も生じうる。この場合、改ざん検知情報生成部2031の機器特徴情報生成部2033は、 $p + 1$ 番目以降の値が p 個の電子透かし情報埋め込み後の機器特徴情報の最小値未満になるように、電子透かし情報の埋め込み位置以外のデータを補正する。改ざん検知情報生成部2031は、補正後の値をもとに、電子透かし情報を更新し、条件を満たすまで、埋め込み処理を繰り返す。

40

【0279】

次に、解析サーバ34等のセキュリティチェックサーバの情報改ざん検知部で実施される電子透かし情報の検証方法について説明する。

情報改ざん検知部の埋め込み位置特定部は、所定の信号処理回路等を利用して、物理データ等の機器特徴情報の中から値の大きいデータの位置を p 個特定する。続いて、電子透かし抽出部は、特定されたデータの位置を表す位置情報を利用して、所定の埋め込み抽出回路等を利用して、時系列順に、選択された p 個の機器特徴情報の最下位ビットから数えて q (k)ビット分の値を、順次抽出する。

50

【0280】

次に、電子透かし検証部は、電子透かし情報が埋め込まれていない部分の全ビット（ $n_r - m$ ビット）と、鍵情報等の共有情報と、時刻情報と、埋め込み側で使用されたデータとに基づき、 m ビットの電子透かし情報を生成する。その後、電子透かし検証部は、電子透かし抽出部が抽出した電子透かし情報と生成した電子透かし情報とを比較する。

【0281】

具体例3

まず、制御化装置125等で実施される、電子透かし情報の埋め込み方法について説明する。

まず、改ざん検知情報生成部2031の埋め込み位置決定部2037は、所定の信号処理回路等を利用して、上記式101で表される離散フーリエ変換、又は、上記式102で表される離散コサイン変換により、時間領域の機器特徴情報（物理データ）（ X_0, X_1, \dots, X_{n-1} ）を、周波数領域のデータ列（ Y_0, Y_1, \dots, Y_{n-1} ）に変換する。

10

【0282】

その後、埋め込み位置決定部2037は、高周波成分（式101及び式102において、 j が大きい成分）を、高い周波数から順に p 個選択する。

【0283】

続いて、電子透かし生成部2035は、選択された p 個の機器特徴情報の最下位ビットから数えて $q(k)$ ビット分を除く全ビット（ $n_r - m$ ビット）と、鍵情報等の共有情報と、時刻情報と、場合によってはその他の情報とに基づき、 m ビットの電子透かし情報を生成する。ここで、 $q(k)$ は、上記条件aを満たす値である。

20

【0284】

続いて、電子透かし埋め込み部2039は、所定の埋め込み処理回路等を利用して、選択された p 個の周波数領域データの最下位ビット（LSB）から数えて $q(k)$ ビット分に、共有情報をもとに生成した電子透かし情報を順次挿入する。

【0285】

ここで、離散フーリエ変換を用いた場合の埋め込み方法としては、実数及び複素数両方に均等に割り振る、数値の大きい方に優先的に割り振る、など、任意の方法を用いることが可能である。

30

【0286】

次に、電子透かし埋め込み部2039は、所定の信号処理回路等を利用して、電子透かし情報埋め込み後の周波数領域のデータを、式103で表される逆離散フーリエ変換、又は、式104で表される逆離散コサイン変換により逆変換し、時間領域のデータ列に戻す。

【0287】

次に、解析サーバ34等のセキュリティチェックサーバの情報改ざん検知部で実施される電子透かし情報の検証方法について説明する。

情報改ざん検知部の埋め込み位置特定部は、まず、所定の信号処理回路等を利用して、上記式101で表される離散フーリエ変換、又は、上記式102で表される離散コサイン変換により、時間領域の機器特徴情報（物理データ）（ X_0, X_1, \dots, X_{n-1} ）を、周波数領域のデータ列（ Y_0, Y_1, \dots, Y_{n-1} ）に変換する。次に、埋め込み位置特定部は、高周波成分（式101及び式102において、 j が大きい成分）を、高い周波数から順に p 個選択する。これにより、電子透かし情報の埋め込まれた位置を特定することができる。続いて、電子透かし抽出部は、特定されたデータの位置を表す位置情報を利用し、所定の埋め込み抽出回路等を利用して、選択された p 個の機器特徴情報の最下位ビットから数えて $q(k)$ ビット分の値を、順次抽出する。

40

【0288】

次に、電子透かし検証部は、電子透かし情報が埋め込まれていない部分の全ビット（ $n_r - m$ ビット）と、鍵情報等の共有情報と、時刻情報と、埋め込み側で使用されたデータ

50

とに基づき、 m ビットの電子透かし情報を生成する。その後、電子透かし検証部は、電子透かし抽出部が抽出した電子透かし情報と生成した電子透かし情報とを比較する。

【0289】

具体例4

まず、制御化装置125等で実施される、電子透かし情報の埋め込み方法について説明する。

まず、改ざん検知情報生成部2031の機器特徴情報生成部2033は、機器特徴情報 X_k について、差分データ $S_k = X_k - X_{k-1}$ ($1 \leq k \leq n-1$)を生成する。続いて、埋め込み位置決定部2037は、連続する $p-1$ 個の差分データの和が所定の閾値未満であり、かつ、その条件を満たす連続データ列の中で二乗和が最大となる $p-1$ の連続データ列 S_k ($t \leq k \leq t+p-2$, $1 \leq t \leq n-p+1$)を選択する。

10

【0290】

続いて、電子透かし生成部2035は、選択された p 個の機器特徴情報の最下位ビットから数えて $q(k)$ ビット分を除く全ビット($n_r - m$ ビット)と、鍵情報等の共有情報と、時刻情報と、場合によってはその他の情報とに基づき、 m ビットの電子透かし情報を生成する。ここで、 $q(k)$ は、上記条件aを満たす値である。

【0291】

続いて、電子透かし埋め込み部2039は、所定の埋め込み処理回路等を利用して、選択された p 個の周波数領域データの最下位ビット(LSB)から数えて $q(k)$ ビット分に、共有情報をもとに生成した電子透かし情報を順次挿入する。

20

【0292】

電子透かし情報埋め込み後の p 個の選択された機器特徴情報の連続する差分データについて、和が閾値未満であり、かつ、その条件を満たす連続データ列の中で二乗和が最大になる、という条件を満たさない場合も生じうる。この場合、改ざん検知情報生成部2031の機器特徴情報生成部2033は、条件が満たされるように、電子透かし情報の埋め込み位置以外のデータを補正する。改ざん検知情報生成部2031は、補正後の値をもとに、電子透かし情報を更新し、条件を満たすまで、埋め込み処理を繰り返す。

【0293】

次に、電力管理装置11及び解析サーバ34等のセキュリティチェックサーバの情報改ざん検知部で実施される電子透かし情報の検証方法について説明する。

30

情報改ざん検知部の埋め込み位置特定部は、まず、機器特徴情報 X_k について、差分データ $S_k = X_k - X_{k-1}$ ($1 \leq k \leq n-1$)を生成する。続いて、埋め込み位置特定部は、連続する $p-1$ 個の差分データの和が所定の閾値未満であり、かつ、その条件を満たす連続データ列の中で二乗和が最大となる $p-1$ の連続データ列 S_k ($t \leq k \leq t+p-2$, $1 \leq t \leq n-p+1$)を選択する。これにより、電子透かし情報の埋め込まれた位置を特定することができる。

【0294】

続いて、電子透かし抽出部は、特定されたデータの位置を表す位置情報を利用して、所定の埋め込み抽出回路等を利用して、時系列順に、選択された p 個の機器特徴情報 $t-1 \leq k \leq t+p-2$ の最下位ビット(LSB)から数えて $q(k)$ ビット分の値を、順次抽出する。

40

【0295】

次に、電子透かし検証部は、電子透かし情報が埋め込まれていない部分の全ビット($n_r - m$ ビット)と、鍵情報等の共有情報と、時刻情報と、埋め込み側で使用されたデータとに基づき、 m ビットの電子透かし情報を生成する。その後、電子透かし検証部は、電子透かし抽出部が抽出した電子透かし情報と生成した電子透かし情報とを比較する。

【0296】

以上、共有情報を利用した電子透かし情報の埋め込み方法及び検証方法、並びに、共有情報及び時刻情報を利用した電子透かし情報の埋め込み方法及び検証方法について、具体例を挙げながら説明した。本実施形態に係る局所電力管理システム1では、かかる方法を

50

用いることで、情報に加えられた改ざんの有無や、電力管理装置の乗っ取り等を、検知することが可能となる。

【0297】

なお、以上の説明においては、電子透かし情報が値の大きい領域に埋め込まれる場合について具体的な説明を行ったが、分散が大きい領域や、雑音領域等に電子透かし情報を埋め込む場合についても、同様に実施することが可能である。

【0298】

<電力管理装置の登録方法について>

続いて、図34及び図35を参照しながら、本実施形態に係る電力管理装置11で実施される、電力管理装置の登録方法について、順を追って流れを説明する。図34は、本実施形態に係る電力管理装置の登録方法について説明するための流れ図である。図35は、本実施形態に係る電力管理装置の登録方法の具体例を説明するための流れ図である。

10

【0299】

まず、図34を参照しながら、電力管理装置11の登録方法の全体的な流れについて、説明する。

電力管理装置11の機器管理部1121は、まず、局所電力管理システム1内に設置された分電装置121の接続を行う(ステップS1001)。より具体的には、機器管理部1121は、分電装置121の製造時に分電装置121に格納されたデジタル署名や証明書等を分電装置121から取得し、分電装置121を自動的に認識したり、オンライン認識したりする。分電装置121の認識処理及び登録処理は、後述する制御化機器125等の認識処理及び登録処理の流れに準じて行われる。

20

【0300】

続いて、機器管理部1121は、電力管理装置11が備える表示部116に、登録すべき情報(登録情報)の内容をユーザに問い合わせるメッセージを表示する。ユーザは、電力管理装置11が備えるタッチパネルやキーボード等の入力部117を操作して、図20に示したような登録情報の内容を、電力管理装置11に入力する。これにより、機器管理部1121は、登録情報を取得することができる(ステップS1003)。

【0301】

次に、機器管理部1121は、広域通信部114を介して、システム管理サーバ33との接続及びシステム管理サーバ33による認証が行われる(ステップS1005)。このシステム管理サーバ33との接続及び認証処理は、任意の技術を用いて行うことが可能であるが、例えば、公開鍵暗号技術を利用する。

30

【0302】

このシステム管理サーバ33による認証処理により、システム管理サーバ33から電力管理装置11へと認証結果が通知される。機器管理部1121は、通知された認証結果を参照して、認証に成功したか否かを判断する(ステップS1007)。

【0303】

システム管理サーバ33による認証処理が失敗していた場合には、機器管理部1121は、認証結果に記載されているエラー内容を判定する(ステップS1009)。登録情報に不備がある場合(a)には、機器管理部1121は、ステップS1003に戻って、不備のある登録情報の内容を問い合わせ、正しい内容を取得する。登録情報に不備がなく、認証に失敗していた場合(b)には、機器管理部1121は、再度システム管理サーバ33と接続し、再度認証処理を行う。また、所定の回数以上連続して認証に失敗した場合(c)には、機器管理部1121は、電力管理装置11の登録を中止する。

40

【0304】

他方、システム管理サーバ33による認証処理が成功していた場合には、機器管理部1121は、取得した登録情報をシステム管理サーバ33に正式に送信して(ステップS1011)、システム管理サーバ33のデータベースに、電力管理装置11を登録してもらう。

【0305】

50

電力管理装置 1 1 の機器管理部 1 1 2 1 は、かかる流れで処理を行うことで、電力管理装置 1 1 自体を、システム管理サーバ 3 3 に登録することができる。なお、電力管理装置 1 1 の登録が成功した場合、電力管理装置 1 1 はシステム管理サーバ 3 3 と定期的に通信し、状況の確認を行う。

【 0 3 0 6 】

[電力管理装置の登録方法の具体例について]

続いて、図 3 5 を参照しながら、電力管理装置の登録方法の具体例を説明する。図 3 5 は、公開鍵暗号技術を用いた電力管理装置の登録方法の一例である。

【 0 3 0 7 】

なお、以下の説明に先立ち、電力管理装置 1 1 は、公開されているシステムパラメータ（公開パラメータ）を何らかの方法で取得しているものとする。また、電力管理装置に固有の識別情報（ID）と、システム管理サーバ 3 3 による識別情報のデジタル署名とが、例えば製造メーカー等により装置内に格納されているものとする。更に、システム管理サーバ 3 3 は、システム管理サーバ 3 3 に固有の公開鍵及び秘密鍵を保持しているものとする。

10

【 0 3 0 8 】

電力管理装置 1 1 のユーザが電力管理装置の登録処理を開始する操作を行うと、機器管理部 1 1 2 1 の鍵生成部 1 5 0 1 は、公開パラメータを利用して、公開鍵及び秘密鍵からなる鍵ペアを生成する（ステップ S 1 0 2 1）。鍵生成部 1 5 0 1 は、生成した鍵ペアを、記憶部 1 1 3 等に格納する。

20

【 0 3 0 9 】

次に、システム登録部 1 5 0 3 は、広域通信部 1 1 4 を介して、電力管理装置の識別情報と、識別情報のデジタル署名と、生成した公開鍵とを、システム管理サーバ 3 3 の公開鍵を用いて暗号化する。次に、システム登録部 1 5 0 3 は、生成した暗号文を、証明書発行依頼としてシステム管理サーバ 3 3 に送信する（ステップ S 1 0 2 3）。

【 0 3 1 0 】

システム管理サーバ 3 3 は、電力管理装置 1 1 から送信された証明書発行依頼を取得すると、まず、デジタル署名に付加されている署名の正当性を検証する（ステップ S 1 0 2 5）。具体的には、システム管理サーバ 3 3 は、サーバが秘匿している秘密鍵を利用して、電力管理装置の識別情報に付加されているデジタル署名が正当なものであるかを検証する。

30

【 0 3 1 1 】

検証に失敗した場合には、システム管理サーバ 3 3 は、認証に失敗した旨を示す認証結果を、電力管理装置 1 1 に送信する。他方、検証に成功した場合、システム管理サーバ 3 3 は、電力管理装置 1 1 の識別情報を、システム管理サーバ 3 3 が保持しているデータベース中の管理リストに追加する（ステップ S 1 0 2 7）。

【 0 3 1 2 】

続いて、システム管理サーバ 3 3 は、電力管理装置 1 1 が生成した公開鍵に対して、公開鍵証明書を発行し（ステップ S 1 0 2 9）、発行した公開鍵証明書を、電力管理装置 1 1 に送信する。

40

【 0 3 1 3 】

電力管理装置 1 1 のシステム登録部 1 5 0 3 は、システム管理サーバ 3 3 から送信された公開鍵証明書を受信すると、この公開鍵証明書の検証を行う（ステップ S 1 0 3 1）。公開鍵証明書の検証に成功すると、システム登録部 1 5 0 3 は、登録情報をシステム管理サーバ 3 3 に送信する（ステップ S 1 0 3 3）。なお、この登録情報の送信は、暗号化通信を用いて行われる。

【 0 3 1 4 】

システム管理サーバ 3 3 は、電力管理装置 1 1 から送信された登録情報を受信すると、受信した登録情報を管理リストに登録する（ステップ S 1 0 3 5）。これにより、電力管理装置 1 1 - システム管理サーバ 3 3 間で行われる電力管理装置 1 1 の登録処理が成功し

50

たことになる（ステップS1037）。

【0315】

以上、電力管理装置11の登録処理の具体例について、その一例を説明した。なお、上述の登録方法の具体例は、あくまでも一例であって、本実施形態に係る登録処理が上述の例に限定されるわけではない。

【0316】

<制御化機器の登録方法について>

続いて、図36～図38を参照しながら、制御化機器125の電力管理装置11への登録方法について説明する。図36は、本実施形態に係る制御化機器の登録方法について説明するための流れ図である。図37及び図38は、本実施形態に係る制御化機器の登録方法の具体例を説明するための流れ図である。

10

【0317】

なお、以下の説明では、電力管理装置11が管理する管理機器として制御化機器125を例にとって、その登録方法について説明する。以下で説明する登録方法は、電動移動体124、蓄電装置128、第1発電装置129及び第2発電装置130を電力管理装置11に登録する場合にも、同様に行われる。

【0318】

まず、図36を参照しながら、制御化機器125の登録方法の全体的な流れについて、説明する。

電力管理装置11の機器管理部1121は、電力管理装置11が管理する局所電力管理システム1に未登録の制御化装置125が接続されると、制御化装置125がシステムに接続された旨を検知する（ステップS1041）。具体的には、電力管理装置11自体が、制御化装置125の接続を検知してもよく、分電装置121やコンセント（制御化端子123又は端子拡張装置127）が制御化装置125の接続を検知して、電力管理装置11にその旨を通知してもよい。この処理によって、電力管理装置11は、制御化装置125が接続されている端子に関する情報（位置情報）を把握することができる。

20

【0319】

続いて、機器管理部1121は、新たに接続された制御化機器125の認証処理を実施する。この認証処理は、任意の技術を用いて行うことが可能であるが、例えば、公開鍵暗号技術を利用する。この認証処理により、機器管理部1121は、図20に示したような情報を、制御化機器125から取得する。

30

【0320】

制御化機器125の認証に失敗した場合、機器管理部1121は、制御化機器125の登録処理を終了する。なお、機器管理部1121は、制御化機器125の認証にした場合に、いきなり登録処理を終了するのではなく、ステップS1043に戻って再度認証処理を行うようにしてもよい。

【0321】

他方、制御化機器125の認証に成功した場合、機器管理部1121は、広域通信部114を介して、システム管理サーバ33に制御化機器125を登録する（ステップS1047）。続いて、機器管理部1121は、認証に成功した制御化機器125に対して、署名（デジタル署名）や証明書等を発行する（ステップS1049）。その後、機器管理部1121は、制御化機器125を記憶部113等に格納されている管理用のデータベースに登録する（ステップS1051）。

40

【0322】

[制御化機器の登録方法の具体例について]

続いて、図37及び図38を参照しながら、制御化機器の登録方法の具体例を説明する。図37及び図38は、公開鍵暗号技術を用いた制御化機器の登録方法の一例である。

【0323】

なお、以下の説明に先立ち、電力管理装置11は、公開されているシステムパラメータ（公開パラメータ）を何らかの方法で取得しているものとする。また、電力管理装置に固

50

有の識別情報（ID）と、システム管理サーバ33による識別情報のデジタル署名とが、例えば製造メーカー等により装置内に格納されており、公開鍵及び秘密鍵からなる鍵ペアも装置内に格納されているものとする。更に、システム管理サーバ33は、システム管理サーバ33に固有の公開鍵及び秘密鍵を保持しているものとする。また、制御化機器125には、例えば製造メーカー等により、機器に固有の識別情報（ID）と、システム管理サーバ33によるデジタル署名とが、装置内に格納されているものとする。

【0324】

まず、図37を参照しながら、制御化機器の初期登録方法の具体例について説明する。

制御化機器125がシステム1に接続される（具体的には、制御化端子123等に接続される）（ステップS1061）と、先に説明したような手順で、電力管理装置11の管理機器登録部1505は、制御化機器125が接続された旨を検知する（ステップS1063）。

10

【0325】

続いて、管理機器登録部1505は、図19に示した優先順位等の登録条件を取得する（ステップS1065）。具体的には、管理機器登録部1505は、電力管理装置11が備える表示部116に、登録条件をユーザに問い合わせるメッセージを表示する。ユーザは、電力管理装置11が備えるタッチパネルやキーボード等の入力部117を操作して、図19に示したような登録条件を、電力管理装置11に入力する。

【0326】

次に、管理機器登録部1505は、登録開始信号を、局所通信部111を介して制御化機器125に送信する（ステップS1067）。

20

【0327】

登録開始信号を受信した制御化機器125の認証処理部2021は、機器に固有の識別情報（ID）及びシステム管理サーバ33によるデジタル署名を電力管理装置11に送信し、機器登録依頼とする（ステップS1069）。

【0328】

機器登録依頼を受信した管理機器登録部1505は、システム管理サーバ33の公開鍵を利用して、受信したデジタル署名の正当性を検証する（ステップS1071）。検証に失敗した場合には、管理機器登録部1505は、認証に失敗した旨を示す認証結果を、制御化機器125に送信する。他方、検証に成功した場合、管理機器登録部1505は、制御化機器125の識別情報や、制御化機器125の製造メーカー名や型番等を含む機器情報の登録を、システム管理サーバ33に要請する（ステップS1073）。

30

【0329】

システム管理サーバ33は、登録要請を受信すると、登録要請のあった制御化機器125が正規の機器であるか（すなわち、既に登録されている機器か否か）を確認する（ステップS1075）。正規の機器である場合、システム管理サーバ33は、受信した機器情報を、システム管理サーバ33が保持しているデータベース中の管理リストに追加する（ステップS1077）。

【0330】

その後、システム管理サーバ33は、自己が保持している各種のデータベースや、製造メーカーに属するサーバ等から、登録した制御化機器125の仕様に関する情報（機器仕様情報）を取得して、電力管理装置11に送信する（ステップS1079）。

40

【0331】

電力管理装置11の管理機器登録部1505は、続いて、制御化機器の識別情報（ID）に対して、自己が保持している鍵を利用して署名（証明書）を発行する（ステップS1081）。続いて、管理機器登録部1505は、発行した署名を、電力管理装置11の識別情報（ID）とともに、制御化機器125に送信する（ステップS1083）。

【0332】

制御化装置125の認証処理部2021は、受信した署名および電力管理装置11の識別情報（ID）を、記憶部2015等の所定の箇所に保存する（ステップS1085）。

50

また、電力管理装置 1 1 の管理機器登録部 1 5 0 5 は、制御化機器 1 2 5 の機器情報を記憶部 1 1 3 等に格納されている管理用のデータベースに登録する（ステップ S 1 0 8 7）。これにより、制御化機器 1 2 5 の初期登録処理が成功したことになる（ステップ S 1 0 8 9）。

【 0 3 3 3 】

図 3 7 は、制御化機器 1 2 5 を電力管理装置 1 1 に正式に登録する（初期登録する）際の処理であった。しかし、例えば知人の家に設けられた電力管理装置 1 1 に、自分の家の電力管理装置 1 1 に既に登録されている制御化機器 1 2 5 を一時的に登録したい、等といった場合も生じうる。そこで、本実施形態に係る電力管理装置 1 1 は、既に別の電力管理装置 1 1 に初期登録済みである制御化機器 1 2 5 を、一時的に登録するための登録処理が準備されている。以下では、図 3 8 を参照しながら、制御化機器 1 2 5 の一時的な登録処理について、説明する。

10

【 0 3 3 4 】

なお、以下の説明に先立ち、電力管理装置 1 1 は、公開されているシステムパラメータ（公開パラメータ）を何らかの方法で取得しているものとする。また、電力管理装置に固有の識別情報（ID）と、システム管理サーバ 3 3 による識別情報のデジタル署名とが、例えば製造メーカー等により装置内に格納されており、公開鍵及び秘密鍵からなる鍵ペアも装置内に格納されているものとする。更に、システム管理サーバ 3 3 は、システム管理サーバ 3 3 に固有の公開鍵及び秘密鍵を保持しているものとする。また、制御化機器 1 2 5 には、例えば製造メーカー等により、機器に固有の識別情報（ID）と、システム管理サーバ 3 3 によるデジタル署名とが、装置内に格納されており、登録済みの電力管理装置の識別情報（ID）及び署名も格納されているものとする。

20

【 0 3 3 5 】

制御化機器 1 2 5 がシステム 1 に接続される（具体的には、制御化端子 1 2 3 等に接続される）（ステップ S 1 0 9 1）と、先に説明したような手順で、電力管理装置 1 1 の管理機器登録部 1 5 0 5 は、制御化機器 1 2 5 が接続された旨を検知する（ステップ S 1 0 9 3）。

【 0 3 3 6 】

続いて、管理機器登録部 1 5 0 5 は、図 1 9 に示した優先順位等の登録条件を取得する（ステップ S 1 0 9 5）。具体的には、管理機器登録部 1 5 0 5 は、電力管理装置 1 1 が備える表示部 1 1 6 に、登録条件をユーザに問い合わせるメッセージを表示する。ユーザは、電力管理装置 1 1 が備えるタッチパネルやキーボード等の入力部 1 1 7 を操作して、図 1 9 に示したような登録条件を、電力管理装置 1 1 に入力する。

30

【 0 3 3 7 】

次に、管理機器登録部 1 5 0 5 は、登録開始信号を、局所通信部 1 1 1 を介して制御化機器 1 2 5 に送信する（ステップ S 1 0 9 7）。

【 0 3 3 8 】

登録開始信号を受信した制御化機器 1 2 5 の認証処理部 2 0 2 1 は、登録済みの電力管理装置 1 1 の識別情報（ID）及び提供された署名、並びに、制御化機器に固有の識別情報（ID）を電力管理装置 1 1 に送信し、機器登録依頼とする（ステップ S 1 0 9 9）。

40

【 0 3 3 9 】

機器登録依頼を受信した管理機器登録部 1 5 0 5 は、機器登録依頼に含まれる、制御化機器に固有の識別情報（ID）を確認する（ステップ S 1 1 0 1）。その後、管理機器登録部 1 5 0 5 は、制御化機器に固有の識別情報（ID）に基づいて、システム管理サーバ 3 3 に、制御化機器 1 2 5 の証明書を要請する（ステップ S 1 1 0 3）。

【 0 3 4 0 】

システム管理サーバ 3 3 は、証明書を要請された制御化機器 1 2 5 が、失効リストに記載されている機器ではないことを確認した上で（ステップ S 1 1 0 5）、要請のあった証明書を、電力管理装置 1 1 に送信する（ステップ S 1 1 0 7）。

【 0 3 4 1 】

50

電力管理装置 1 1 の管理機器登録部 1 5 0 5 は、制御化機器 1 2 5 が有している署名（登録されている電力管理装置 1 1 から取得した署名）を検証する（ステップ S 1 1 0 9）。管理機器登録部 1 5 0 5 は、署名の検証に成功すると、制御化機器 1 2 5 を一時的に電力管理装置 1 1 に登録する（ステップ S 1 1 1 1）。これにより、電力管理装置 1 1 は、別の電力管理装置 1 1 に既に登録されている制御化機器 1 2 5 を、一時的に登録することができる。

【 0 3 4 2 】

< 制御化端子の登録方法について >

続いて、図 3 9 を参照しながら、制御化端子 1 2 3 の電力管理装置 1 1 への登録方法について説明する。図 3 9 は、本実施形態に係る制御化端子の登録方法について説明するための流れ図である。

10

【 0 3 4 3 】

なお、以下では、制御化端子 1 2 3 を例に挙げて説明を行うが、端子拡張装置 1 2 7 についても、同様に登録処理を行うことが可能である。

【 0 3 4 4 】

電力管理装置 1 1 が有する機器管理部 1 1 2 1 は、まず、分電装置 1 2 1 に接続して（ステップ S 1 1 2 1）、分電装置 1 2 1 から、システム 1 内に存在する端子に関する情報を取得する（ステップ S 1 1 2 3）。端子に関する情報とは、制御化端子・非制御化端子の区別、制御化端子の識別情報（ID）、製造メーカー名や型番、電力供給量・供給限界等のスペック、端子のシステム内における位置情報などである。

20

【 0 3 4 5 】

次に、機器管理部 1 1 2 1 の管理機器登録部 1 5 0 5 は、システム内に存在する制御化端子と接続を確立する（ステップ S 1 1 2 5）。その後、管理機器登録部 1 5 0 5 は、接続を確立した制御化端子を、記憶部 1 1 3 等に格納されている管理用のデータベースに登録する（ステップ S 1 1 2 7）。

【 0 3 4 6 】

続いて、管理機器登録部 1 5 0 5 は、図 2 1 に示したような給電制御方法や機器認証手段を確認し、管理用データベースに設定する。これにより、この制御化端子 1 2 3 に制御化機器 1 2 5 や非制御化機器 1 2 6 が接続された場合に、電力管理装置 1 1 は、適切な給電制御や機器認証処理を実行することが可能となる。

30

【 0 3 4 7 】

次に、管理機器登録部 1 5 0 5 は、全ての端子（制御化端子）について処理を実施したか否かを判断する（ステップ S 1 1 3 1）。処理を実施していない制御化端子が存在している場合には、管理機器登録部 1 5 0 5 は、ステップ S 1 1 2 5 に戻って処理を継続する。また、全ての制御化端子に対して処理を実施した場合には、管理機器登録部 1 5 0 5 は、処理を正常終了する。

【 0 3 4 8 】

以上、本実施形態に係る局所電力管理システム 1 における各装置の登録処理について説明した。

【 0 3 4 9 】

< 一時的に登録された制御化機器の課金処理について >

以下では、図 4 0 及び図 4 1 を参照しながら、一時的に登録された制御化機器の課金処理について説明する。図 4 0 は、一時的に登録された制御化機器の課金処理を説明するための説明図である。図 4 1 は、一時的に登録された制御化機器の課金処理を説明するための流れ図である。

40

【 0 3 5 0 】

先に説明したように、ある電力管理装置 1 1 に既に登録されている制御化機器 1 2 5 を、他の局所電力管理システム 1 を管理している別の電力管理装置 1 1 に一次的に登録するという状況が考えうる。この際、一時的に登録された制御化機器 1 2 5 は、別の電力管理装置 1 1 の制御下において、他の局所電力管理システム 1 から電力の供給を受ける状況が

50

生じうる。

【0351】

このような状況を図示したものが、図40である。図40に示したように、局所電力管理システム#1に属する制御化機器#1は、電力管理装置#1に既に登録されている。また、制御化機器#1は、電力管理装置#1から、電力管理装置#1の識別情報(ID_{p1})と、制御化機器#1の識別情報に対する電力管理装置#1のデジタル署名(sig(ID_{p1}))を受け取っている。この制御化機器#1を、一時的に、電力管理装置#2が管理を行っている局所電力管理システム#2(例えば、公共電力供給ステーション等)に登録して、制御化機器#1が局所電力管理システム#2から電力の供給を受ける場合を考える。ここで、システム管理サーバ33は、電力管理装置#1の識別情報(ID_{p1})と、電力管理装置#2の識別情報(ID_{p2})とを把握しているものとする。

10

【0352】

このときの電力料金は、制御化機器#1を登録している電力管理装置#1へ請求され、電力管理装置#1が課金サーバ32と所定の課金処理を実施することが望ましい。この仕組み自体は、機器が公開鍵・秘密鍵を保持する場合のみ可能であり、保持していない場合は、電力管理装置#2は、無償で制御化機器#1に電力を供給することになる。なお、公開鍵及び秘密鍵からなる鍵ペアを持っている場合であっても、無償で電力供給を許可することを許容するかについては、設定次第である。

【0353】

ここで問題となるのは、仮に電力管理装置#1が不正な装置であった場合には、電力管理装置#2が電力を制御化機器#1に供給しても、電力料請求自体が無効となることである。そのため、本実施形態では、電力管理装置#2は、制御化機器#1に電力供給を許可するに先立って、電力管理装置#1の正当性、及び、制御化機器#1が電力管理装置#1に正式に登録されていること、を確認する。これらの確認作業は、安全のため、電力を無償で供給する場合にも行うことが望ましい。つまり、電力管理装置#2は、電力管理装置#1の署名や証明書等を利用して、その都度電力管理装置#1と制御化機器#1との関係を検証し、更に、システム管理サーバ33に問い合わせを行うことで、電力管理装置#1及び制御化機器#1の正当性を確認する。

20

【0354】

また、本実施形態では、電力料の請求に関して、以下で図41を参照しながら説明するように、電力供給と、電力を使用したことを正式に証明する電力使用証明書との交換方式を取り入れることにより、安全な課金処理を実現することが可能となる。

30

【0355】

以下、図41を参照しながら、一時的に登録された制御化機器の課金処理について、その流れを説明する。なお、以下の処理は、主に、制御化機器125の制御部2001及び電力管理装置の機器管理部1121が実行する処理である。

【0356】

まず、制御化機器#1は、電力管理装置#2に対して、認証処理を依頼する(ステップS1141)。この認証依頼に際して、制御化機器#1は、電力管理装置#2に対して、制御化機器#1が保持している、電力管理装置#1の識別情報(ID_{p1})と、制御化機器#1の識別情報(ID_{d1})と、ID_{p1}及びID_{d1}に対するデジタル署名と、を送信する。

40

【0357】

電力管理装置#2は、自身が管理する管理リストに、通知された制御化機器の識別情報(ID_{d1})が存在するかを確認する。また、電力管理装置#2は、自身が保持している証明書リストの中に、電力管理装置#1の識別情報(ID_{p1})が存在するかを確認する。これにより、電力管理装置#2は、電力管理装置#1の確認を行うこととなる(ステップS1143)。

【0358】

電力管理装置#2は、自身が保持している証明書リストに電力管理装置#1の識別情報

50

が存在しなければ、システム管理サーバ33に電力管理装置#1の証明書を要求する(ステップS1145)。また、電力管理装置#1は、この証明書の要求にあわせて、システム管理サーバ33に制御化機器#1の識別情報を通知してもよい。

【0359】

システム管理サーバ33は、電力管理装置#1が失効リストにないことを確認することで、電力管理装置#1の正当性を確認する(ステップS1147)。電力管理装置#1の識別情報が失効リストに記載されている場合には、システム管理サーバ33は、その旨を電力管理装置#2に通知して、電力管理装置#2は、処理をエラー終了する。

【0360】

一方で、電力管理装置#2は、制御化機器#1に電力管理装置#1が発行した証明書又は電力管理装置#1によるデジタル署名を要求する(ステップS1149)。この要求を受けて、制御化装置#1は、電力管理装置#1から提供されたデジタル署名($sig(ID_{p1})$)を電力管理装置#2に送付する(ステップS1151)。

【0361】

また、システム管理サーバ33は、電力管理装置#1の正当性が確認できた場合には、自身が保持している電力管理装置#1の証明書を、電力管理装置#2に送付する(ステップS1153)。

【0362】

電力管理装置#2は、制御化機器#1から送信されたデジタル署名及び/又は証明書を検証し(ステップS1155)、検証に成功すれば、制御化機器#1に対して電力供給を許可する。このとき、電力管理装置#2は、制御化機器#1に対して、電力の有料・無料を通知する。このとき、電力が無料である場合には、以降のステップは実行しない。

【0363】

検証に成功することで、電力管理装置#2は、制御化機器#1に対して、所定時間、電力を供給する(ステップS1157)。

【0364】

電力の供給を受けた制御化機器#1は、所定時間電力を消費したことを証明する証拠として、電力使用に関するメッセージを生成し、署名を添付して電力管理装置#2に送付する(ステップS1159)。この署名が添付された電力使用に関するメッセージが、電力使用証明書である。なお、ステップS1157及びステップS1159の処理は、電力管理装置#2が電力供給を停止する、又は、制御化機器#1が電力網(局所電力管理システム)から接続解除されるまで、一定時間ごとに繰り返し行うことが好ましい。

【0365】

電力管理装置#2は、制御化機器#1から取得した電力使用証明書に、自身の識別情報(ID_{p2})及び機器の証明書を追加して、システム管理サーバ33に送付する(ステップS1161)。

【0366】

システム管理サーバ33は、「制御化機器#1が電力管理装置#2から電力を購入した」という事実の検証を行う。この検証は、電力使用証明書を、機器の証明書をを用いて検証することで行われる(ステップS1163)。

【0367】

電力使用証明書の検証に成功すると、システム管理サーバ33は、課金サーバ32に対して、課金処理を依頼する(ステップS1165)。その後、課金サーバ32は、システム管理サーバ33の依頼内容に従って、課金処理を実行する(ステップS1167)。

【0368】

このような処理を行うことで、公共ステーションにも拡張可能な、安全な課金処理機能を実現することが可能となる。

【0369】

なお、電力管理装置11が管理する制御化機器等の中でも、大容量のバッテリーを搭載する電気自動車等の電動移動体124等については、バッテリー電力を他の電力網(局所

10

20

30

40

50

電力管理システム)に販売する機会も考えられる。この場合においても、図4-1に示した手順で対応が可能である。この際には、電力管理装置1-1が電動移動体1-2-4等から電力の供給を受け、電力管理装置1-1が電動移動体1-2-4等に対して電力使用証明書を発行することとなる。ここで、システム管理サーバ3-3への電力使用証明書の送付は、電力を購入した電力管理装置1-1が基本的に担当することが好ましい。

【0370】

また、供給を受けた電力管理装置1-1が、電力使用証明書をシステム管理サーバ3-3に送付しないなどの不正を行う場合も考えられる。かかる場合には、電動移動体1-2-4等を登録している電力管理装置1-1が、電動移動体1-2-4等に格納された電力使用証明書をシステム管理サーバ3-3に送付することにより、不正を検出することができる。

10

【0371】

<制御化機器の登録方法の変形例について>

ここで、図4-2～図4-8を参照しながら、先に説明した制御化機器の登録方法の変形例について、詳細に説明する。図4-2～図4-7は、制御化機器の登録方法の変形例を説明するための説明図であり、図4-8は、制御化機器の登録方法の変形例を説明するための流れ図である。

【0372】

先に説明したように、局所電力管理システム1においては、不正機器や不正バッテリーに電力を供給しない、不正機器や不正バッテリーがシステムに接続されることを防止する等の目的で、機器やバッテリーの認証が行われる。以下で説明する本実施形態に係る制御化機器の登録方法の変形例の目的は、制御化機器や複数のバッテリーを有する蓄電装置の認証を効率的に行うことが可能な登録方法を提供することにある。

20

【0373】

以下の説明では、図4-2に例示したように、電力管理装置1-1が、A～Hの8台の制御化機器1-2-5を認証及び登録する場合を考える。

【0374】

先に説明したような方式では、電力管理装置1-1と1台の制御化機器1-2-5との間で行われる1対1の認証処理を、全ての制御化機器1-2-5に対して計8回繰り返すこととなる。この場合において、ある制御化機器1-2-5を認証する場合には、以下のようなプロセスが実施されることとなる。すなわち、まず、電力管理装置1-1が制御化機器1-2-5に乱数を含むチャレンジメッセージを送信する。次に、このチャレンジメッセージに対して、制御化機器1-2-5は、自身の保持する鍵を作用させてレスポンスメッセージを作成して返送する。その後、電力管理装置1-1は、受信したレスポンスメッセージの正しさを検証する。

30

【0375】

ここで、認証方法としては、(i)チャレンジメッセージからレスポンスメッセージを作成する際に作用させる鍵として公開鍵暗号系の秘密鍵を用い、レスポンスメッセージがデジタル署名となるものと、(ii)電力管理装置1-1と制御化機器1-2-5とで共有した鍵を使用する共通鍵暗号系を用いるもの、の2種類に大別できる。

【0376】

ここで、本変形例では、(i)に示したデジタル署名を用いる認証方法に着目する。なぜならば、かかる認証方法の中には、バッチ検証およびアグリゲート署名という技術を利用可能であるものが存在するからである。

40

【0377】

ここで、バッチ検証とは、複数のデジタル署名を検証する際に、一括して検証を行うことが可能な検証技術のことであり、全てのデジタル署名が正しい場合のみ、検証アルゴリズムは「検証成功」を出力する。かかる技術を利用することで、個々のデジタル署名をひとつひとつ検証していくよりも、計算量の効率化を図ることが可能となる。

【0378】

かかるバッチ検証処理の具体例として、上記非特許文献1及び上記非特許文献2に記載

50

された方法がある。本変形例では、かかるバッチ検証処理を利用することで、計算量の効率化を実現できる。また、これらの技術の中には、複数の署名者がそれぞれ異なるメッセージに対して生成した署名を、一括して検証することが可能な技術も含まれている。

【0379】

また、アグリゲート署名は、複数の署名をひとつの署名にまとめることが可能な技術であり、まとめられた署名を検証処理にかけると、検証アルゴリズムは、すべての署名が正しいときにのみ、「検証成功」を出力する。ここで、複数の署名は、複数の署名者がそれぞれ異なるメッセージに対して作成したものであってもよい。

【0380】

かかるアグリゲート署名の具体例として、上記非特許文献3及び上記非特許文献4に記載された方法がある。本変形例では、かかるアグリゲート署名を利用することで、計算量の効率化を実現できる。

【0381】

ここで、図42に示したように、電力管理装置11が8台の制御化機器125を認証する場合を考える。通常の1対1認証を繰り返す方法では、計8回の認証処理が実施されることとなるが、バッチ検証処理又はアグリゲート署名を利用することで、図42下段に示したように、計算の効率化を図ることが可能となる。

【0382】

なお、以下で説明する認証処理は、主に、電力管理装置11の機器管理部1121及び制御化機器125の制御部2001が実行する処理である。

【0383】

まず、電力管理装置11は、制御化機器A～Hに対して、チャレンジメッセージCを送信する(ステップS1171)。この送信では、各制御化機器に対して個別のメッセージを送る必要はないため、通信路が同報送信のできる環境であれば、同報送信であってもよい。

【0384】

このチャレンジメッセージCに対し、各制御化機器A～Hは、自身が持つ公開鍵暗号系の秘密鍵を用いて、チャレンジメッセージCに対するレスポンスメッセージを生成して、生成したレスポンスメッセージを電力管理装置11に返送する。

【0385】

例えば、制御化機器Aは、チャレンジメッセージCを受信すると、制御化機器Aが保持している秘密鍵を利用して、チャレンジメッセージCに対するレスポンスメッセージ R_A を生成する(ステップS1173)。続いて、制御化機器Aは、生成したレスポンスメッセージ R_A を、電力管理装置11に対して送信する(ステップS1175)。

【0386】

また、制御化機器Hは、チャレンジメッセージCを受信すると、制御化機器Hが保持している秘密鍵を利用して、チャレンジメッセージCに対するレスポンスメッセージ R_H を生成する(ステップS1177)。続いて、制御化機器Hは、生成したレスポンスメッセージ R_H を、電力管理装置11に対して送信する(ステップS1179)。

【0387】

具体的には、これらのレスポンスメッセージ R_A ～ R_H は、チャレンジメッセージCに対する、各制御化機器A～Hのデジタル署名となる。

【0388】

この間、電力管理装置11は、認証処理を実施する制御化機器A～Hからのレスポンスメッセージを待ち受ける。電力管理装置11は、8台の制御化機器からのレスポンスメッセージが集まったら、全てのレスポンスメッセージ R_A ～ R_H をまとめて認証して(ステップS1181)、全てのレスポンスメッセージが正しいか否かを検証する。この検証は、バッチ検証処理によって行っても良いし、8つのレスポンスメッセージをアグリゲート署名技術によって1つのデジタル署名にまとめ、この1つのデジタル署名を検証することで行っても良い。

10

20

30

40

50

【0389】

なお、以上の説明では、簡単のために、電力管理装置11は各制御化機器の公開鍵を予め知っているものとしているが、各制御化機器A～Hは、それぞれのレスポンスメッセージとあわせて、各自の公開鍵証明書を電力管理装置11に送信してもよい。

【0390】

ここで、公開鍵証明書は、機器の識別情報(ID)や公開鍵に対する、Certificate Authorityである認証局サーバ35のデジタル署名である。そのため、この際にも、バッチ検証やアグリゲート署名の技術を利用して、効率的に検証を行うことが可能となる。

【0391】

電力管理装置11のチャレンジメッセージに対して各制御化機器からレスポンスメッセージが集まってきて、これらのレスポンスメッセージを一括検証すると、多くの場合では全てのレスポンスメッセージが正しく、検証結果が「成功」となるはずである。この場合には、電力管理装置11が全ての制御化機器A～Hの正当性を確認できたとして、通常処理を行えばよい。

【0392】

しかしながら、n台に対する一括検証処理において、「検証失敗」が出力されることが生じうる。この場合には、n台の制御化機器の中に1台以上、正常でない機器があることを意味する。したがって、電力管理装置11は、正常ではない機器を特定して、正常ではない機器に対して別の処理を行うとともに、正常である機器に対しては新たに一括検証処理を行うことが重要となる。

【0393】

正常ではない機器を特定するためには、一括検証の対象とする制御化機器のグループを、小さなグループへと分割することを繰り返せばよい。具体的な方法を、図43及び図44を示しながら以下に説明するが、これには2種類の方法がある。

【0394】

第1のストラテジーは、正常ではない機器を最低1台特定する方法であり、このために要する試行回数(計算量)は、 $O(\log 2n)$ となる。

【0395】

他方、第2のストラテジーは、正常ではない機器を全て特定する方法であり、このために要する試行回数は、 $O(n)$ となる。

【0396】

以下、それぞれの戦略に基づいた手法を、詳しく説明する。

【0397】

ストラテジー1は、一括検証の結果が「失敗」となったグループのうちの1つ(例えば、構成要素数が最も小さいもの)を選択し、グループが1台の制御化機器のみを含むまで繰り返す手法である。図43にその例を示す。図43では、A～Hの制御化機器のうち、制御化機器C, E, Fの3台が正常ではないとする。

【0398】

電力管理装置11は、ステップ1として、8台全ての制御化機器に対してチャレンジメッセージを送信し、8台の制御化機器を一括検証する。この検証結果が「失敗」に終わると、電力管理装置11は、ステップ2に進み、8台の制御化機器からなる1つのグループを、2つのグループに分割する。

【0399】

図43に示した例では、電力管理装置11は、グループを、制御化機器A～Dからなるグループと、制御化機器E～Hからなるグループとに分割し、各グループにチャレンジメッセージを送信する。その後、電力管理装置11は、得られたレスポンスメッセージを、各グループで一括検証する。図43に示した例では、両方のグループにおいて、一括検証の結果が「検証失敗」となる。

【0400】

次に、ステップ3として、電力管理装置11は、現在のグループ(図43では、制御化機器A B C Dのグループと制御化機器E F G Hのグループ)で検証結果が「失敗」になったもの(両方)から、次に分割するグループを選択する。図43に示した例では、電力管理装置11は、制御化機器A B C Dからなるグループを選択し、このグループを更に分割する。図43に示した例では、制御化機器A B C Dからなるグループが、制御化機器A Bからなるグループと、制御化機器C Dからなるグループの2台ずつの2つのグループに分割される。

【0401】

電力管理装置11は、この2台ずつのグループに対してチャレンジメッセージを送信し、受信したレスポンスメッセージを一括検証する。図43に示した例の場合、制御化機器A Bからなるグループの検証結果は「成功」となるため、制御化機器A, Bは、いずれも正常であることが確認できる。他方、制御化機器C Dからなるグループの検証結果は「失敗」となるため、制御化機器C, Dの少なくとも一方が正常ではないことがわかる。

10

【0402】

次に、ステップ4として、電力管理装置11は、制御化機器C Dからなるグループを1台ずつのグループに分け、両方のグループについて認証処理を行う。これにより、電力管理装置11は、制御化機器Cが正常ではないことを特定することができる。

【0403】

図43に示した例では、8台の制御化機器に対して、4段階のステップにより正常ではない制御化機器を1台特定することができた。一般的にn台の制御化機器を考えたとき、リーフノードの数がnである2分木を考えるとわかりやすいが、グループの分割を構成要素数が約半分になるように行っていくと、2分木の高さである $\log_2(n+1)$ 回のステップで、処理を終えることができる。また、1つのステップでは、最大2つのグループに対して検証処理を行うため、検証処理の計算回数は、 $O(\log_2 n)$ となる。

20

【0404】

次に、ストラテジー2について説明する。

ストラテジー2は、正常ではない機器を全て検出する方法である。図44にその例を示す。図44では、A~Hの制御化機器のうち、制御化機器C, E, Fの3台が正常ではないとする。

【0405】

ステップ1では、電力管理装置11は、ステップ1として、8台全ての制御化機器に対してチャレンジメッセージを送信し、8台の制御化機器を一括検証する。この検証結果が「失敗」に終わると、電力管理装置11は、ステップ2に進み、8台の制御化機器からなる1つのグループを、2つのグループに分割する。

30

【0406】

図44に示した例では、電力管理装置11は、グループを、制御化機器A~Dからなるグループと、制御化機器E~Hからなるグループとに分割し、各グループにチャレンジメッセージを送信する。その後、電力管理装置11は、得られたレスポンスメッセージを、各グループで一括検証する。図44に示した例では、両方のグループにおいて、一括検証の結果が「検証失敗」となる。

40

【0407】

ストラテジー2では、ステップ3として、前のステップで検証が「失敗」であった全てのグループについて、再度認証処理を行う。図44に示した例では、電力管理装置11は、制御化機器A B C Dからなるグループを、制御化機器A Bからなるグループと、制御化機器C Dからなるグループとに分割する。また、電力管理装置11は、制御化機器E F G Hからなるグループを、制御化機器E Fからなるグループと、制御化機器G Hからなるグループとに分割する。その後、電力管理装置11は、この4つのグループそれぞれに対して、認証処理を実施する。

【0408】

図44に示した例では、制御化機器A Bからなるグループと、制御化機器G Hからなる

50

グループは検証に「成功」し、制御化機器 C D からなるグループと制御化機器 E F からなるグループは検証に「失敗」することとなる。

【 0 4 0 9 】

続くステップ 4 において、電力管理装置 1 1 は、検証に失敗した制御化機器 C D からなるグループを、制御化機器 C からなるグループと制御化機器 D からなるグループに分割する。同様に、電力管理装置 1 1 は、検証に失敗した制御化機器 E F からなるグループを、制御化機器 E からなるグループと、制御化機器 F からなるグループに分割する。その後、電力管理装置 1 1 は、新たな 4 つのグループそれぞれに対して、認証処理を実施する。

【 0 4 1 0 】

この結果、図 4 4 に示したように、制御化機器 D は、認証に「成功」し、他の 3 台の制御化機器は、認証に「失敗」することとなる。これにより、電力管理装置 1 1 は、制御化機器 C , E , F という正常ではない機器を、全て特定することが可能となる。

10

【 0 4 1 1 】

ストラテジー 2 は、ステップ数はストラテジー 1 と同様の 4 ステップであるが、I 番目のステップでは、 $2I - 1$ 個のグループの検証処理を行うこととなる。この方法では、正常ではない機器と正常な機器が交互に並んでいた場合など、あるケースにおいては、すべての機器に対して検証処理を行うこととなり、検証回数は $2n$ となる。このため、ストラテジー 2 での計算量は、 $O(n)$ となる。

【 0 4 1 2 】

ところで、電力管理装置 1 1 は、局所電力管理システム 1 に接続される制御化機器等がどのようなものであるかを把握しているものである。そうでないと、どの機器に電力を供給してよいかのコントロールができないからである。すなわち、ユーザが、例えば家庭内の局所電力管理システム 1 に機器を導入する際、その機器を電力管理装置 1 1 に登録する処理が行われる。したがって、先に説明したように、電力管理装置 1 1 は、登録された機器のリストを管理している。

20

【 0 4 1 3 】

ここで、局所電力管理システム 1 において、制御化機器 A ~ 制御化機器 H の 8 台の機器が電力管理装置 1 1 に登録されていたが、認証の結果として、制御化機器 C が正常ではないことがわかったとする。

【 0 4 1 4 】

この場合、電力管理装置 1 1 は、管理リストから制御化機器 C を削除するか、一時的に使用不可とマークしておく。これにより、電力管理装置 1 1 は、次回の認証時には制御化機器 C を認証の対象から予め外すことが可能になり、その分だけ認証処理の軽減を図ることが可能となる。例えば、制御化機器 C 以外の 7 台の制御化機器が正常であれば、7 台の制御化機器に対する認証一回で、その旨を確認可能である。

30

【 0 4 1 5 】

また、機器が修理を経て正常になった旨がユーザの指示で電力管理装置 1 1 に通知された場合、又は、電力管理装置 1 1 が正常でない機器それぞれに対して定期的・不定期的に認証を試みて「成功」の結果が得られた場合には、電力管理装置 1 1 は、認証の対象からはずされた機器を正常のものとして扱うように、自身が管理している管理リストを修正してもよい。

40

【 0 4 1 6 】

[バッテリーの認証について]

一般に、バッテリーの筐体中には、複数のバッテリーセルが装備されていることが多い。また、バッテリーは、これら複数のセルの組み合わせによって、様々な出力に対応することが可能となる。

【 0 4 1 7 】

例えば、図 4 5 では、1 V のバッテリーセルを 6 個備えた蓄電装置 1 2 8 が図示されている。これらのセル A ~ F は、図 4 5 に示すように、様々な電圧を出力するように組み合わせることが可能である。また、すべてのセルを利用しない場合や、蓄電装置 1 2 8 に一

50

組ではなく複数組の出力端子対が備わっている場合などを考慮すると、更に多くのバリエーションを持った出力を得ることが可能になる。

【0418】

バッテリー中に、故障したセルや、もともと不正に製造されたセル等が含まれていると、所望の出力が得られないばかりでなく、充電時などに発火などの事故を起こす確率も高くなる。そのため、バッテリーセルそれぞれの認証を行って、各セル（ひいては、バッテリー）が正常であることを確認することは重要である。

【0419】

ここで、電力管理装置11またはバッテリーの制御部が、各セルを認証することを考える。この際に、図46に示したように、6個のセルを3つずつ組み合わせて使用し、3Vの出力を得ようとするのを考える。この場合、通常は、電力管理装置11またはバッテリーの制御部がひとつのセルを認証する処理を6回繰り返すことで、すべてのセルのチェックについて、バッテリーの制御部は、予め把握しているものとする。また、電力管理装置11は、バッテリーのセル構成について、電力管理装置11に登録されている型番等に基づいて、外部のサーバ等から取得することが可能である。

10

【0420】

また、電流容量は小さくても、3Vの電圧を取り出したい場合には、AとBとC（またはDとEとF）の3つのセルの認証を行えば、バッテリーとして使用することができる。この場合には、3回の検証処理が行われることとなる。

【0421】

20

ところが、先に述べたパッチ検証或いはアグリゲート署名の技術を用い、ABC（またはDEF）をまとめて検証することで、1回の検証処理によって3Vのバッテリーとして使用できるか否かを把握することが可能となり、認証処理の効率化を図ることができる。更に、ABCからなるグループ、又は、DEFからなるグループのいずれか一方でも認証に「成功」すれば、バッテリーとして利用できることを容易に把握することができる。

【0422】

更に、認証に「失敗」したグループがあった場合には、前述の方法でグループを分割していけば、正常ではないセルを特定することも可能である。

【0423】

また、図46に示したように、2Vの電圧を得たい場合には、AB、CD、EFと直列に並んだ2つのセルのグループに対して、一括の認証を行えばよい。

30

【0424】

このように、バッテリーセルの組み合わせ方に応じて、認証するセルのグループ分けを行うことで、認証処理の効率化を図ることが可能となる。

【0425】

いま、6個のバッテリーセルを、図47の（初期状態）に示すように、2Vの電圧で使用していたものとする。ここで、初期状態では6個のセルが全て正常であったが、ある時点における認証の結果、認証に「失敗」することがあったとする。

【0426】

この場合、電力管理装置11やバッテリーの制御部は、前述のストラテジー2を利用して、正常ではない全てのセルを特定することができる。その結果、図47の中央に示したように、セルD及びセルEが正常ではないことが特定できたものとする。

40

【0427】

この場合、バッテリーの制御部又は電力管理装置11は、バッテリーセルを接続する配線を切り替えて、図47右図に示すように、セルの再構成を行うことができる。これにより、正常なセルのみを用いてバッテリーとして使用することができる組み合わせを構成することが可能となる。再構成を行わない場合には、正常なセルC及びセルFが無駄になるしかなかったが、かかる再構成を実行することにより、資源を無駄なく利用することが可能となる。このようなセルの再構成は、バッテリーの制御部や電力管理装置11が各セルの状態を的確に把握し、認証結果に応じてセルの接続を再構成することにより達成するこ

50

とが可能である。

【0428】

以上説明したような、制御化機器のバッチ認証の大まかな流れを図示すると、図48に示したようになる。

【0429】

まず、電力管理装置11の機器管理部1121は、チャレンジメッセージを生成して、認証すべき制御化機器125の全てに対して同報送信する(ステップS1191)。これにより、各制御化機器125の制御部2001は、チャレンジメッセージに対してレスポンスメッセージを生成し、電力管理装置11に生成したレスポンスメッセージを返信する。

10

【0430】

電力管理装置11では、制御化機器125から送信されるレスポンスメッセージを待ち受けており、制御化機器125からレスポンスメッセージが送信されると、送信されたレスポンスメッセージを取得する(ステップS1193)。

【0431】

ここで、電力管理装置11の機器管理部1121は、全てのレスポンスメッセージを取得したか否かを判断する(ステップS1195)。全てのレスポンスメッセージを取得していない場合には、機器管理部1121は、ステップS1193に戻って、レスポンスメッセージを待ち受ける。

【0432】

他方、全ての制御化機器125からレスポンスメッセージを取得した場合には、機器管理部1121は、バッチ認証処理を実施する(ステップS1197)。全ての制御化機器についてバッチ認証処理が成功した場合には、機器管理部1121は、認証に成功したと判断し、バッチ認証処理を正常終了する。

20

【0433】

また、全ての制御化機器125についてバッチ認証処理が成功しなかった場合には、機器管理部1121は、先に説明したストラテジー1又はストラテジー2に則して、認証に失敗した制御化機器を特定する(ステップS1201)。その後、機器管理部1121は、認証に失敗した機器を除いて再度認証処理を実行し(ステップS1203)、ステップS1199に戻って、バッチ認証処理が成功したか否かを判断する。

30

【0434】

以上のような流れで処理を行うことにより、本変形例では、制御化機器を効率よく認証することが可能となる。

【0435】

ここまで、公開鍵暗号系のデジタル署名技術のうち、バッチ検証やアグリゲート署名技術を用いて、制御化機器や蓄電装置をグループ化し、効率的に認証を行う方法を説明してきた。しかしながら、公開鍵暗号技術は、共通鍵暗号技術に比べて、個々の秘密鍵を用いたデジタル署名等が利用可能であるというメリットがあるものの、一般に計算量が非常に大きいというデメリットが存在する。

【0436】

そこで、このデメリットを解決するために、公開鍵暗号技術と共通鍵暗号技術との併用を考える。具体的には、電力管理装置11は、制御化機器等の認証を公開鍵暗号技術に基づいて行う。また、公開鍵暗号技術に基づく認証に成功した制御化機器や蓄電装置に対して、電力管理装置(又は、バッテリーの制御部等)と制御化機器との間で利用される1:1の共通鍵を、電力管理装置(又は、バッテリーの制御部等)が提供するものとする。

40

【0437】

この共通鍵は、1日や1時間などの有効期間があり、この有効期間中は、電力管理装置11による制御化機器の認証処理に対して、この共通鍵を使用する。また、共通鍵の有効期間の終了後には、再度公開鍵暗号を用いて認証処理を行い、新たな共通鍵を電力管理装置-制御化機器間に確立する。

50

【0438】

このような方法を用いることで、計算負荷が大きな公開鍵暗号を用いた処理を、1日や1時間に1回のみで済むようにし、頻繁に行う認証には処理の負荷の軽い共通鍵暗号を用いることが可能となる。

【0439】

なお、電力管理装置11とある制御化機器125との間の1:1の共通鍵ではなく、電力管理装置とその認証対象である複数の制御化機器とでひとつのグループ鍵を共有し、このグループ鍵を共通鍵としてその後の認証処理に用いることも可能である。

【0440】

以上、本変形例に係る制御化機器の登録方法について説明した。

10

以下では、異常の発生した管理機器に対して電力管理装置が行う処理について、具体的な例を挙げながら詳細に説明する。

【0441】

<異常の発生した管理機器に対する電力管理装置の動作について>

以下では、図49～図52を参照しながら、異常の発生した管理機器に対する電力管理装置の動作について、具体例を挙げながら詳細に説明する。図49～図52は、異常の発生した管理機器に対する電力管理装置の動作を説明するための流れ図である。

【0442】

まず、図49を参照しながら、異常の発生した管理機器に対する電力管理装置の動作の大きな流れについて説明する。

20

【0443】

電力管理装置11の機器管理部1121は、現在時刻に関する時刻情報、又は、前回動作確認処理を行ってからの経過時間に関する情報を参照して、管理機器の動作確認処理を実施する時刻(チェック時刻)が到来したか否かを判断する(ステップS1211)。チェック時刻が到来していない場合には、機器管理部1121は、ステップS1211に戻って、チェック時刻の到来を待ち受ける。

【0444】

また、チェック時刻が到来した場合には、機器管理部1121の管理機器情報取得部1507は、各制御化機器125から、異常の発生を報告するセンサ情報を受信しているか否かを判断する(ステップS1213)。異常の発生を報告するセンサ情報を受信している場合には、機器管理部1121は、後述するステップS1225を実施する。

30

【0445】

また、異常の発生を報告するセンサ情報を受信していない場合には、管理機器情報取得部1507は、分電装置121から、異常の発生を報告する機器情報を受信しているか否かを判断する(ステップS1215)。異常の発生を報告する機器情報を受信している場合には、機器管理部1121は、後述するステップS1225を実施する。

【0446】

また、分電装置における異常の発生を報告する機器情報を受信していない場合には、管理機器情報取得部1507は、制御化端子123(端子拡張装置127も含む。以下同じ。)から、異常の発生を報告する機器情報を受信しているか否かを判断する(ステップS1217)。異常が発生していると判断される場合には、機器管理部1121は、後述するステップS1225を実施する。

40

【0447】

なお、ステップS1215及びステップS1217における処理によって、電力管理装置11は、電力管理装置11と直接通信を行うことができない非制御化機器126に異常が発生していないかを判断することが可能となる。

【0448】

次に、管理機器情報取得部1507は、各制御化機器等から、センサ情報、バッテリー情報、セル情報といった機器情報を収集して、情報分析部1123の機器状態判定部1601及び電力状態判定部1603に伝送する。機器状態判定部1601及び電力状態判定

50

部 1 6 0 3 は、伝送された情報の履歴や典型例との比較を行う（ステップ S 1 2 1 9）。これにより、電力管理装置 1 1 は、制御化機器等に発生している異常を検知することが可能である。また、管理機器情報取得部 1 5 0 7 及び / 又は機器状態判定部 1 6 0 1 は、本来受信するはずの情報が受信していない、という事実からも、制御化機器等に発生した異常を検知することが可能である。

【 0 4 4 9 】

機器管理部 1 1 2 1 は、機器情報の収集・比較処理結果を参照して、問題が発生しているか否かを判断する（ステップ S 1 2 2 1）。問題が発生している場合には、機器管理部 1 1 2 1 は、後述するステップ S 1 2 2 5 を実施する。

【 0 4 5 0 】

また、機器情報の収集・比較処理の結果、問題が発生していないと判断される場合には、機器状態判定部 1 6 0 1 は、全ての機器について問題が発生していないかを判断する（ステップ S 1 2 2 3）。判断の結果、一部の装置について検証が終了していない場合には、機器管理部 1 1 2 1 及び情報分析部 1 1 2 3 は、ステップ S 1 2 1 9 に戻って、検証処理を継続する。また、全ての機器について検証が終了した場合には、機器管理部 1 1 2 1 は、管理機器の動作の検証処理を終了する。

【 0 4 5 1 】

ここで、上述のような検証処理によって何らかの異常が検出された場合には、情報分析部 1 1 2 3 は、表示部 1 1 6 に警告を表示する（ステップ S 1 2 2 5）。また、電力管理装置 1 1 は、異常が検出された場合の動作モード（異常モード）へと移行する（ステップ S 1 2 2 7）。

【 0 4 5 2 】

続いて、機器管理部 1 1 2 1 は、ユーザの登録電話番号や登録メールアドレスに対して、警告メッセージを発信して、異常が発生した旨をユーザに通知する（ステップ S 1 2 2 9）。その後、機器管理部 1 1 2 1 は、規定時間内に、電力管理装置 1 1 に対してユーザアクセスがあったかどうかを判断する（ステップ S 1 2 3 1）。規定時間内にユーザアクセスが存在した場合には、電力管理装置 1 1 の制御部 1 1 5 は、ユーザ指示に基づいた制御化機器の動作制御を開始する（ステップ S 1 2 3 3）。他方、規定時間内にユーザアクセスが無かった場合には、電力管理装置 1 1 の制御部 1 1 5 は、自動制御を開始する（ステップ S 1 2 3 5）。その後、電力管理装置 1 1 の制御部 1 1 5 は、制御化端子による制御に動作モードを切り替えて（ステップ S 1 2 3 7）、異常動作検出時の処理を終了する。

【 0 4 5 3 】

以下では、異常が発生した装置の種別に応じて、実施される具体的な処理について、簡単に説明する。

【 0 4 5 4 】

[電力管理装置に異常が発生した場合]

まず、図 5 0 を参照しながら、電力管理装置 1 1 自体に異常が発生した場合の動作について、簡単に説明する。

【 0 4 5 5 】

なお、以下の説明に先立ち、ユーザは、電力管理装置 1 1 に異常が発生した場合にどのような制御を行うか（例えば、制御化端子による制御、電力供給を定常維持する制御など）を、予め設定してあるものとする。また、電力管理装置 1 1 は、局所電力管理システム 1 外に設けられたサービス管理サーバ 3 3 に対して、履歴情報、管理機器の識別情報（ID）、設定条件等の各種情報を、定期的にバックアップしているものとする。

【 0 4 5 6 】

電力管理装置 1 1 自体に何らかの異常が発生し（ステップ S 1 2 4 1）、電力管理装置 1 1 自体がダウンすると、システム管理サーバ 3 3 は、電力管理装置 1 1 からの定期的な通信が途絶することとなるため、電力管理装置 1 1 に異常が発生したことを検知することができる（ステップ S 1 2 4 3）。

10

20

30

40

50

【 0 4 5 7 】

その後、システム管理サーバ 3 3 は、登録されている緊急連絡先等を参照して、ユーザに異常が発生した旨を通知する（ステップ S 1 2 4 5）。

【 0 4 5 8 】

また、制御化端子 1 2 3 及び制御化機器 1 2 5 は、電力管理装置 1 1 との間で行われる定期的な通信が不能となるため（ステップ S 1 2 4 7）、電力管理装置 1 1 に異常が発生した可能性があることを検知する。その後、制御化端子 1 2 3 及び制御化機器 1 2 5 は、電力管理装置 1 1 の状態を確認し（ステップ S 1 2 4 9）、電力管理装置 1 1 に異常が発生したことを把握すると、制御化端子 1 2 3 及び制御化機器 1 2 5 が移行すべきモードがどのモードであるかを確認する（ステップ S 1 2 5 1）。その後、制御化端子 1 2 3 及び
10 制御化機器 1 2 5 は、制御化端子制御モードへと移行する（ステップ S 1 2 5 3）。

【 0 4 5 9 】

具体的には、制御化端子 1 2 3 は、制御化機器 1 2 5 及び非制御化機器 1 2 6 の制御を開始し（ステップ S 1 2 5 5）、制御化機器 1 2 5 は、制御化端子 1 2 3 に対して電力情報の出力を開始する（ステップ S 1 2 5 7）。また、制御化端子 1 2 3 は、制御化機器 1 2 5 から取得した電力情報に異常を検出した場合には、給電停止等の制御を実施することが可能である。

【 0 4 6 0 】

ここで、システム管理サーバ 3 3 からの連絡を受けたユーザが、電力管理装置 1 1 を再起動したり、電力管理装置 1 1 に対して手動で何らかの操作を行ったりすることにより、
20 電力管理装置 1 1 が復帰したとする（ステップ S 1 2 5 9）。

【 0 4 6 1 】

この際、復帰した電力管理装置 1 1 の機器管理部 1 1 2 1 は、システム管理サーバ 3 3 に対して、認証処理を実施するように要請する（ステップ S 1 2 6 1）。システム管理サーバ 3 3 は、電力管理装置 1 1 の認証に成功すると、バックアップしてある設定情報を取得して、電力管理装置 1 1 に送付する（ステップ S 1 2 6 3）。

【 0 4 6 2 】

設定情報を受信した電力管理装置 1 1 は、受信した設定情報に従って、管理装置である制御化端子 1 2 3 及び制御化機器 1 2 5 に自動接続し（ステップ S 1 2 6 5）、復帰した旨をこれらの機器に通知する。
30

【 0 4 6 3 】

その後、制御化端子 1 2 3 及び制御化機器 1 2 5 は、電力管理装置制御モードへとモードを移行し（ステップ S 1 2 6 7）、通常の電力管理装置 1 1 による制御が実行されることとなる。

【 0 4 6 4 】

[制御化端子に異常が発生した場合]

次に、図 5 1 を参照しながら、制御化端子 1 2 3 に異常が発生した場合の動作について、簡単に説明する。

【 0 4 6 5 】

まず、制御化端子 1 2 3 のセンサ又は通信部の少なくともいずれかに、異常が発生した
40 （ステップ S 1 2 7 1）ものとする。この場合、制御化端子 1 2 3 から接続されている制御化機器 1 2 5 への電力供給は維持されている（ステップ S 1 2 7 3）ため、電力管理装置 1 1 は、直接的には異常検知することは困難である。しかしながら、定期的受信するはずの制御化端子 1 2 3 からの機器情報を受信しない、などの判定により、電力管理装置 1 1 は、制御化端子 1 2 3 に異常が発生したことを検知することができる（ステップ S 1 2 7 5）。

【 0 4 6 6 】

異常を検知した電力管理装置 1 1 の情報分析部 1 1 2 3 は、制御化端子 1 2 3 に異常が発生した旨を、ユーザに通知する（ステップ S 1 2 7 7）。具体的には、電力管理装置 1 1 は、表示部 1 1 6 に異常が発生した旨を表示したり、警告音を鳴らしたり、ユーザが登
50

録している電話番号やメールアドレスにメッセージを送信することで、ユーザに異常が発生したことを通知する。

【0467】

通知を受けたユーザが、問題の発生している制御化端子123に対して手動で何らかの操作を行うことで、制御化端子123の機能は、復帰することとなる(ステップS1279)。

【0468】

また、制御化端子123の給電制御に異常が発生した(ステップS1281)ものとする。この場合には、制御化機器125は、制御化端子123に異常が発生したことを検知することが可能であり、場合によっては、制御化機器125は、電力供給が受けられなくなつて、動作停止する可能性もある(ステップS1283)。その結果、制御化機器125が電力管理装置11に対して制御化端子123に異常が発生した旨を通知したり、制御化機器125の動作停止に伴う定期的な通信が停止したりすることによって、電力管理装置11は、制御化端子123での異常発生を検知する(ステップS1285)。

【0469】

異常を検知した電力管理装置11の情報分析部1123は、制御化端子123に異常が発生した旨を、ユーザに通知する(ステップS1287)。具体的には、電力管理装置11は、表示部116に異常が発生した旨を表示したり、警告音を鳴らしたり、ユーザが登録している電話番号やメールアドレスにメッセージを送信することで、ユーザに異常が発生したことを通知する。

【0470】

通知を受けたユーザが、問題の発生している制御化端子123に対して手動で何らかの操作を行うことで、制御化端子123の機能は、復帰することとなる(ステップS1289)。

【0471】

[分電装置に異常が発生した場合]

次に、図52を参照しながら、分電装置121に異常が発生した場合の動作について、簡単に説明する。

【0472】

分電装置121に異常が発生すると(ステップS1301)、分電装置121が電力管理装置11に対して異常が発生した旨を通知したり、分電装置121からの定期的な通信が停止したりする。また、分電装置121に異常が発生した場合には、制御化機器125への電力供給にも問題が発生する可能性がある。そのため、制御化機器125が定期的送信する電力情報(ステップS1303)にも異常が発生する可能性がある。これらの情報により、電力管理装置11の情報分析部1123は、分電装置121に異常が発生した旨を検知することができる(ステップS1305)。

【0473】

異常を検知した電力管理装置11の情報分析部1123は、分電装置121に異常が発生した旨を、ユーザに通知する(ステップS1307)。具体的には、電力管理装置11は、表示部116に異常が発生した旨を表示したり、警告音を鳴らしたり、ユーザが登録している電話番号やメールアドレスにメッセージを送信することで、ユーザに異常が発生したことを通知する。

【0474】

通知を受けたユーザが、問題の発生している分電装置121に対して手動で何らかの操作を行うことで、分電装置121の機能は、復帰することとなる(ステップS1309)。

【0475】

また、分電装置121に異常が発生し(ステップS1311)、分電装置121が電力管理装置11に対して異常が発生した旨を通知したり、分電装置121からの定期的な通信が停止したりする。また、分電装置121に異常が発生した場合には、制御化機器12

10

20

30

40

50

5への電力供給にも問題が発生する可能性がある。そのため、制御化機器125が定期的に送信する電力情報(ステップS1313)にも異常が発生する可能性がある。これらの情報により、電力管理装置11自体にも異常が発生した(ステップS1317)ものとする。

【0476】

この場合、システム管理サーバ33は、電力管理装置11からの定期的な通信が途絶することとなるため、電力管理装置11に異常が発生したことを検知することができる(ステップS1319)。

【0477】

その後、システム管理サーバ33は、登録されている緊急連絡先等を参照して、ユーザに異常が発生した旨を通知する(ステップS1321)。

10

【0478】

この場合、電力管理装置11では、先に説明した、電力管理装置に異常が発生した際の処理が実施される(ステップS1323)。また、制御化機器125は、電力管理装置11の異常発生に伴い、制御化端子制御モードへと移行する(ステップS1325)。

【0479】

ここで、通知を受けたユーザが、問題の発生している分電装置121に対して手動で何らかの操作を行うことで、分電装置121の機能は、復帰することとなる(ステップS1327)。また、電力管理装置11についても、電力管理装置に異常が発生した場合の動作が実施されることにより、電力管理装置11の機能は復帰することとなる(ステップS1327)。

20

【0480】

以上、制御化端子123、制御化機器125等の管理装置に異常が発生した場合の電力管理装置11の動作について説明した。

【0481】

<電力状態に異常が発生した場合における電力管理装置の動作>

続いて、停電や漏電といった、局所電力管理システム1における電力状態に異常が発生した場合における電量管理装置11の動作について、図53及び図54を参照しながら説明する。図53及び図54は、電力状態に異常が発生した場合における電力管理装置の動作を説明するための流れ図である。

30

【0482】

[停電が発生した場合の電力管理装置の動作]

まず、図53を参照しながら、停電が発生した場合における電力管理装置の動作について、簡単に説明する。

【0483】

外部電力に異常が発生して停電が発生すると、分電装置121への外部電力の供給が停止することとなる。その結果、分電装置121が停電の発生した旨を電力管理装置11に通知したり、分電装置121から異常を含む機器情報が送信されたりすることで、電力管理装置11は、分電装置121の異常を検知することができる(ステップS1331)。

【0484】

40

情報分析部1123の電力状態判定部1603は、停電発生を検知すると、発電装置129、130及び蓄電装置128による電力供給モード(蓄電供給モード)へとモードを移行する(ステップS1333)。具体的には、電力管理装置11の制御部115は、分電装置121に対して、外部電力から、システム1内で供給可能な電力への切り替えを実施する制御命令を発信する。また、機器管理部1121は、予め設定されている情報に基づいて、電力供給の優先度を確定したり、電力配分量を確定したりする処理を開始する。また、情報分析部1123は、停電が発生した旨を、表示部116等を介してユーザに通知する。

【0485】

機器管理部1121は、まず、電力供給対象機器が制御化機器125であるか否かを判

50

断する（ステップS 1 3 3 5）。電力供給対象機器が制御化機器 1 2 5 である場合には、機器管理部 1 1 2 1 は、制御部 1 1 5 を介して、対象機器に制御命令を発信する（ステップS 1 3 3 7）。具体的には、制御部 1 1 5 は、対象機器である制御化機器 1 2 5 に対して、省電力モード又は電源OFFを要請する制御命令を発信する。

【0 4 8 6】

また、電力供給対象機器が制御化機器 1 2 5 ではない場合（すなわち、非制御化機器 1 2 6 である場合）には、機器管理部 1 1 2 1 は、電力供給対象機器が制御化端子 1 2 3（端子拡張装置 1 2 7 も含む。）に接続されているかを判断する（ステップS 1 3 3 9）。電力供給対象機器が制御化端子 1 2 3 に接続されている場合には、機器管理部 1 1 2 1 は、制御部 1 1 5 を介して、制御化端子 1 2 3 に制御命令を発信する（ステップS 1 3 4 1）。

10

【0 4 8 7】

また、電力供給対象機器が制御化端子 1 2 3 に接続されていない場合には、電力管理装置 1 1 が電力供給対象機器に対して電力供給制御を行うことができないため、電力管理装置 1 1 は、現状のまま放置するか、現状の電力供給を継続する（ステップS 1 3 4 3）。

【0 4 8 8】

かかる判定が終了すると、機器管理部 1 1 2 1 は、全ての機器に対して設定が完了したかを判断する（ステップS 1 3 4 5）。全ての機器に対して設定が完了していない場合には、電力管理装置 1 1 は、ステップS 1 3 3 5 に戻って処理を継続する。また、全ての機器に対して設定が完了した場合には、電力管理装置 1 1 は、停電時における処理を終了する。

20

【0 4 8 9】

[漏電が発生した場合の電力管理装置の動作]

次に、図 5 4 を参照しながら、漏電が発生した場合における電力管理装置の動作について、簡単に説明する。

【0 4 9 0】

漏電が発生すると、漏電発生前よりも電力使用量の傾向が変化することが予測される。したがって、電力管理装置 1 1 が有する情報分析部 1 1 2 3 の電力状態判定部 1 6 0 3 は、過去の電力使用量等の履歴と、現状の電力使用量とを比較することで、漏電が発生していることを検知することができる（ステップS 1 3 5 1）。また、電力状態判定部 1 6 0 3 は、システム 1 内に存在する機器について、制御化機器 1 2 5 の電力使用量の理論値と、非制御化機器 1 2 6 の予測電力使用量とに基づいて、電力使用理論値を算出し、実際の電力使用量と電力使用理論値とを比較することでも、漏電を検知することができる。なお、非制御化機器 1 2 6 の予測電力使用量は、過去の使用状況から推定することが可能である。

30

【0 4 9 1】

また、この漏電発生の検知は、電力管理装置 1 1 だけでなく、局所電力管理システム 1 の外部に存在する、セキュリティチェックサーバ等の解析サーバ 3 4 が検知することが可能である。そのため、漏電が発生した場合、解析サーバ 3 4 から電力管理装置 1 1 へとその旨が通知される場合もある。

40

【0 4 9 2】

漏電の発生が検知されると、電力管理装置 1 1 は、任意の方法で漏電箇所を特定し（ステップS 1 3 5 3）、制御部 1 1 5 は、漏電箇所への電力供給停止命令を発信する（ステップS 1 3 5 5）。また、情報分析部 1 1 2 3 は、表示部 1 1 6 に、漏電が発生している事実、及び、漏電箇所に関する情報を表示する（ステップS 1 3 5 7）。

【0 4 9 3】

このような処理を行うことで、電力管理装置 1 1 は、停電や漏電といった電力状態の異常時であっても、局所電力管理システム 1 内の様々なセキュリティを維持することができ

50

る。

【 0 4 9 4 】

< 電子透かし情報の埋め込み方法及び検証方法の流れについて >

続いて、図 5 5 ~ 図 5 8 を参照しながら、本実施形態に係る局所電力管理システム 1 内で実施される電子透かし情報の埋め込み方法及び検証方法について、その流れを説明する。図 5 5 及び図 5 7 は、本実施形態に係る電子透かし情報の埋め込み方法を説明するための流れ図である。図 5 6 及び図 5 8 は、本実施形態に係る電子透かし情報の検証方法を説明するための流れ図である。

【 0 4 9 5 】

[共有情報を利用した電子透かし情報の埋め込み方法及び検証方法]

10

まず、図 5 5 及び図 5 6 を参照しながら、共有情報を利用した電子透かし情報の埋め込み方法及び検証方法の流れについて、説明する。なお、以下では、機器特徴情報として、物理データそのものを利用する場合について説明する。

【 0 4 9 6 】

埋め込み方法の流れ

まず、図 5 5 を参照しながら、制御化機器 1 2 5 の改ざん検知情報生成部 2 0 3 1 により実施される埋め込み方法について説明する。

【 0 4 9 7 】

制御化機器 1 2 5 が有する改ざん検知情報生成部 2 0 3 1 の機器特徴情報生成部 2 0 3 3 は、まず、センサ制御部 2 0 2 3 及びバッテリー制御部 2 0 2 7 から、物理データを取得する（ステップ S 2 0 0 1）。その後、機器特徴情報生成部 2 0 3 3 は、取得した物理データの検証を行う（ステップ S 2 0 0 3）。続いて、機器特徴情報生成部 2 0 3 3 は、取得した物理データが正常であるか否かを判断する（ステップ S 2 0 0 5）。

20

【 0 4 9 8 】

検証により、物理データの値が、物理データの取り得る値の範囲を超える場合や、明らかに異常な挙動を示すものである場合には、機器特徴情報生成部 2 0 3 3 は、異常を通知する（ステップ S 2 0 1 9）。

【 0 4 9 9 】

また、検証によって物理データが正常である旨が確認されると、電子透かし生成部 2 0 3 5 は、物理データ及び共有情報に基づいて電子透かし情報を生成し（ステップ S 2 0 0 7）、電子透かし埋め込み部 2 0 3 9 に生成した電子透かし情報を出力する。また、埋め込み位置決定部 2 0 3 7 は、物理データを解析して、物理データに適した電子透かし情報の埋め込み位置を決定し、電子透かし埋め込み部 2 0 3 9 に決定した埋め込み位置に関する情報を通知する。

30

【 0 5 0 0 】

その後、電子透かし埋め込み部 2 0 3 9 は、埋め込み位置に関する情報に基づいて、物理データの中に電子透かし情報を埋め込む（ステップ S 2 0 0 9）。続いて、電子透かし埋め込み部 2 0 3 9 は、電子透かし情報が埋め込まれた物理データ（以下、埋め込みデータと称する。）の検証を行う（ステップ S 2 0 1 1）。続いて、電子透かし埋め込み部 2 0 3 9 は、検証結果の検討を行う（ステップ S 2 0 1 3）。

40

【 0 5 0 1 】

埋め込みデータが正常である場合には、電子透かし埋め込み部 2 0 3 9 は、埋め込みデータを電力管理装置 1 1 に送信する（ステップ S 2 0 1 5）。電力管理装置 1 1 は、受信した埋め込みデータを、局所電力管理システム 1 外の解析サーバ 3 4 に送信する。

【 0 5 0 2 】

他方、埋め込みデータに異常が見つかった場合には、電子透かし埋め込み部 2 0 3 9 は、発生した異常の回数が所定の閾値未満であるか否かを判断する（ステップ S 2 0 1 7）。異常の回数が所定の閾値未満である場合には、改ざん検知情報生成部 2 0 3 1 は、ステップ S 2 0 0 7 に戻って処理を継続する。また、異常の回数が所定の閾値以上である場合には、改ざん検知情報生成部 2 0 3 1 は、異常を通知する（ステップ S 2 0 1 9）。

50

【 0 5 0 3 】

なお、電子透かし情報の埋め込み位置が予め決まっている場合には、埋め込み位置の決定処理、ステップ S 2 0 0 3 ~ ステップ S 2 0 0 5 の物理データの検証処理、及び、ステップ S 2 0 1 1 ~ ステップ S 2 0 1 9 の埋め込みデータの検証処理は、省略可能である。

【 0 5 0 4 】

検証方法の流れ

続いて、図 5 6 を参照しながら、セキュリティチェックサーバ等の解析サーバ 3 4 が有する情報改ざん検知部で実施される、電子透かし情報の検証方法について説明する。なお、以下では、解析サーバ 3 4 において実施される検証方法について説明するが、同様の方法は、電力管理装置の情報改ざん検知部でも実施される。

10

【 0 5 0 5 】

解析サーバ 3 4 の情報改ざん検知部が有する埋め込み位置特定部は、電子透かし情報の埋め込まれた物理データを取得する（ステップ S 2 0 2 1）。その後、埋め込み位置特定部は、取得した物理データの検証を行う（ステップ S 2 0 2 3）。続いて、埋め込み位置特定部は、取得した物理データが正常であるか否かを判断する（ステップ S 2 0 2 5）。

【 0 5 0 6 】

検証により、物理データの値が、物理データの取り得る値の範囲を超える場合や、明らかに異常な挙動を示すものである場合には、埋め込み位置特定部は、異常を通知する（ステップ S 2 0 2 7）。

【 0 5 0 7 】

また、検証によって物理データが正常である旨が確認されると、埋め込み位置特定部は、物理データを解析して、電子透かし情報が埋め込まれた位置を特定し（ステップ S 2 0 2 9）、埋め込み位置に関する位置情報を、電子透かし抽出部に通知する。

20

【 0 5 0 8 】

次に、電子透かし抽出部は、通知された埋め込み位置に関する位置情報に基づいて、物理データの中から電子透かし情報を抽出し（ステップ S 2 0 3 1）、抽出した電子透かし情報を、電子透かし検証部に出力する。

【 0 5 0 9 】

続いて、電子透かし検証部は、物理データ及び共有情報に基づいて電子透かし情報を生成し（ステップ S 2 0 3 3）、抽出された電子透かし情報を、生成した電子透かし情報と比較することで、電子透かし情報の検証を行う（ステップ S 2 0 3 5）。電子透かし検証部は、比較による電子透かし情報の検証に失敗した場合には、電力管理装置 1 1 に異常を通知する（ステップ S 2 0 2 7）。また、比較による電子透かし情報の検証に成功した場合には、電子透かし検証部は、検証に成功したことを通知して、処理を正常終了する。

30

【 0 5 1 0 】

なお、電子透かし情報の埋め込み位置が予め決まっている場合には、ステップ S 2 0 2 3 ~ ステップ S 2 0 2 5 の物理データの検証処理、及び、埋め込み位置の特定処理（ステップ S 2 0 2 9）は、省略可能である。

【 0 5 1 1 】

[時刻情報及び共有情報を利用した電子透かし情報の埋め込み方法及び検証方法]

40

次に、図 5 7 及び図 5 8 を参照しながら、時刻情報及び共有情報を利用した電子透かし情報の埋め込み方法及び検証方法の流れについて、説明する。なお、以下では、機器特徴情報として、物理データそのものを利用する場合について説明する。

【 0 5 1 2 】

埋め込み方法の流れ

まず、図 5 7 を参照しながら、制御化機器 1 2 5 の改ざん検知情報生成部 2 0 3 1 により実施される埋め込み方法について説明する。

【 0 5 1 3 】

なお、制御化機器 1 2 5 は、電力管理装置 1 1 を介して定期的に、解析サーバ 3 4 へ電子透かし情報の埋め込まれた物理データを送信しており、制御化機器 1 2 5 - 解析サーバ

50

3 4 間では、予めデータ送信時刻が決定されているものとする。

【0514】

制御化機器125の改ざん検知情報生成部2031は、予定されたデータの送信時刻が到来したか否かを判断する(ステップS2041)。予定送信時刻が到来していない場合には、改ざん検知情報生成部2031は、予定時刻の到来を待ち受ける。また、予定送信時刻が到来している場合には、機器特徴情報生成部2033は、センサ制御部2023及びバッテリー制御部2027から、物理データを取得する(ステップS2043)。その後、機器特徴情報生成部2033は、取得した物理データの検証を行う(ステップS2045)。続いて、機器特徴情報生成部2033は、取得した物理データが正常であるか否かを判断する(ステップS2047)。

10

【0515】

検証により、物理データの値が、物理データの取り得る値の範囲を超える場合や、明らかに異常な挙動を示すものである場合には、機器特徴情報生成部2033は、異常を通知する(ステップS2065)。

【0516】

また、検証によって物理データが正常である旨が確認されると、埋め込み位置決定部2037は、物理データを解析して、物理データに適した電子透かし情報の埋め込み位置を決定し(ステップS2049)、電子透かし埋め込み部2039に決定した埋め込み位置に関する情報を通知する。

【0517】

20

続いて、電子透かし生成部2035は、現在時刻又は送信予定時刻を表す時刻情報を取得する(ステップS2051)。その後、電子透かし生成部2035は、物理データ、時刻情報及び共有情報に基づいて電子透かし情報を生成し(ステップS2053)、電子透かし埋め込み部2039に生成した電子透かし情報を出力する。

【0518】

その後、電子透かし埋め込み部2039は、埋め込み位置に関する情報に基づいて、物理データの中に電子透かし情報を埋め込む(ステップS2055)。続いて、電子透かし埋め込み部2039は、電子透かし情報が埋め込まれた物理データ(以下、埋め込みデータと称する。)の検証を行う(ステップS2057)。続いて、電子透かし埋め込み部2039は、検証結果の検討を行う(ステップS2059)。

30

【0519】

埋め込みデータが正常である場合には、電子透かし埋め込み部2039は、埋め込みデータを電力管理装置11に送信する(ステップS2061)。電力管理装置11は、受信した埋め込みデータを、局所電力管理システム1外の解析サーバ34に送信する。

【0520】

他方、埋め込みデータに異常が見つかった場合には、電子透かし埋め込み部2039は、発生した異常の回数が所定の閾値未満であるか否かを判断する(ステップS2063)。異常の回数が所定の閾値未満である場合には、改ざん検知情報生成部2031は、ステップS2053に戻って処理を継続する。また、異常の回数が所定の閾値以上である場合には、改ざん検知情報生成部2031は、異常を通知する(ステップS2065)。

40

【0521】

なお、電子透かし情報の埋め込み位置が予め決まっている場合には、埋め込み位置の決定処理、ステップS2045～ステップS2047の物理データの検証処理、及び、ステップS2057～ステップS2063の埋め込みデータの検証処理は、省略可能である。

【0522】

検証方法の流れ

続いて、図58を参照しながら、セキュリティチェックサーバ等の解析サーバ34が有する情報改ざん検知部で実施される、電子透かし情報の検証方法について説明する。

【0523】

なお、制御化機器125は、電力管理装置11を介して定期的に、解析サーバ34へ電

50

子透かし情報の埋め込まれた物理データを送信しており、制御化機器 1 2 5 - 解析サーバ 3 4 間では、予めデータ送信時刻が決定されているものとする。

【 0 5 2 4 】

解析サーバの情報改ざん検知部は、予定されたデータの送信時刻が到来したか否かを判断する（ステップ S 2 0 7 1）。予定送信時刻が到来していない場合には、情報改ざん検知部は、予定時刻の到来を待ち受ける。また、予定送信時刻が到来している場合には、情報改ざん検知部は、電力管理装置 1 1 を介して、制御化機器 1 2 5 より送信された物理データの取得を試みる。ここで、情報改ざん検知部は、所定の時間範囲内に物理データを受信できたか否かを判断する（ステップ S 2 0 7 3）。

【 0 5 2 5 】

所定の時間範囲内に物理データを受信しなかった場合には、情報改ざん検知部は、電力管理装置 1 1 のユーザに、異常を通知する（ステップ S 2 0 8 9）。また、所定の時間範囲内に物理データを受信した場合には、埋め込み位置特定部は、取得した物理データの検証を行う（ステップ S 2 0 7 5）。続いて、埋め込み位置特定部は、取得した物理データが正常であるか否かを判断する（ステップ S 2 0 7 7）。

【 0 5 2 6 】

検証により、物理データの値が、物理データの取り得る値の範囲を超える場合や、明らかに異常な挙動を示すものである場合には、埋め込み位置特定部は、異常を通知する（ステップ S 2 0 8 9）。

【 0 5 2 7 】

また、検証によって物理データが正常である旨が確認されると、埋め込み位置特定部は、物理データを解析して、電子透かし情報が埋め込まれた位置を特定し（ステップ S 2 0 7 9）、埋め込み位置に関する位置情報を、電子透かし抽出部に通知する。また、電子透かし抽出部は、埋め込み位置に関する位置情報に基づいて、物理データの中から電子透かし情報を抽出し、抽出した電子透かし情報を、電子透かし検証部へ出力する。

【 0 5 2 8 】

続いて、電子透かし検証部は、現在時刻又は送信予定時刻を表す時刻情報を取得する（ステップ S 2 0 8 1）。

【 0 5 2 9 】

続いて、電子透かし検証部は、物理データ、時刻情報及び共有情報に基づいて電子透かし情報を生成し（ステップ S 2 0 8 3）、抽出された電子透かし情報を、生成した電子透かし情報と比較することで、電子透かし情報の検証を行う（ステップ S 2 0 8 5）。電子透かし検証部は、比較による電子透かし情報の検証に失敗した場合には、異常を通知する（ステップ S 2 0 8 9）。また、比較による電子透かし情報の検証に成功した場合には、電子透かし検証部は、検証に成功したことを通知して、処理を正常終了する。

【 0 5 3 0 】

なお、電子透かし情報の埋め込み位置が予め決まっている場合には、ステップ S 2 0 7 5 ~ ステップ S 2 0 7 7 の物理データの検証処理、及び、埋め込み位置の特定処理（ステップ S 2 0 7 9）は、省略可能である。

【 0 5 3 1 】

以上説明したような処理を行うことにより、解析サーバ 3 4 - 制御化機器 1 2 5 間の中間に位置する電力管理装置 1 1 の制御機能が奪われた場合に、その異常を検知することができる。また、かかる電子透かし情報を利用することで、通信路上で攻撃者により行われる物理データへの改ざんを検知することができる。また、電力管理装置 1 1 は、物理データを仲介するだけで、改ざん防止用の特別なデータを送受信する必要がなく、解析サーバ 3 4 - 制御化機器 1 2 5 間で物理データの改ざん検知が可能となる。

【 0 5 3 2 】

また、電力管理装置 1 1 の制御機能が奪われた場合であっても、攻撃者が物理データを改ざんする攻撃を防止することができる。更に、かかる方法を利用することで、物理データの統計的性質を失うことなく、物理データに改ざん検知機能を付加することができる。

10

20

30

40

50

【0533】

<解析サーバが果たす役割について>

局所電力管理システム1においてセンター的機能を負う電力管理装置11には、バッテリーが搭載された様々な制御化機器等が接続される。電力管理装置11は、各機器から得られた電力情報をもとに分電装置121をコントロールすることで、配電制御を行う。電力管理装置11は、システム1に接続されている機器の電力消費をリアルタイムで把握し、太陽光発電等の自然エネルギーによる自家発電による電力も含めて、システム1内の電力使用状況を一元管理することができる。また、電力管理装置11は、消費電力の可視化を実現することが可能であり、これにより、無駄なエネルギー消費の抑制につながる事が期待されている。

10

【0534】

しかしながら、局所電力管理システム1は、局所的な電力網を制御するネットワークシステムであるため、システム構成やサービスにおいて、セキュリティ技術の利用は不可欠である。また、昨今、バッテリーを搭載した機器においては、バッテリーセルの粗悪品への差し替えや、本体機器との認証をパスするチップ偽造も横行しており、品質の低下が発火事故を起こすなどの問題を引き起こしている。本実施形態に係る局所電力管理システム1で扱うバッテリーは、システム内に存在する蓄電装置や電動移動体等を含め様々あり、その安全性を確保する事は重要な課題である。

【0535】

局所電力管理システム1の外部とシステム1の内部とのインターフェースとなる電力管理装置11に対して実施されうる外部攻撃としては、例えば以下のようなものが考えられる。

20

機器やバッテリーが異常動作するよう不正な命令(ウィルス)を忍び込ませる

- 電力管理装置の制御の乗っ取り
- トロイの木馬攻撃
- 電力管理装置を介した他の機器やシステムへの攻撃
- DoS攻撃

【0536】

これらの外部攻撃に対して防御を行うために、従来では、以下のような方策が採られてきた。

30

- 予め想定される不正な操作を防止
- 予め定義されたウィルスパターンファイルを用いてウィルスを検知する
- 未知の攻撃については実行ファイルの挙動監視により不正ファイルを検知する

【0537】

しかしながら、これらの対策は、コンピュータ上での挙動を対象としているため、例えばバッテリー等のような物理デバイスでの監視には適用が困難であり、防御対策として十分であるとは言いがたい。また、電力管理装置に接続可能なバッテリーや機器は頻繁に更新されると考えられるため、攻撃の対策は非常に複雑になる可能性が高く、攻撃の内容を予め想定することは困難である。

【0538】

40

また、偽造バッテリーについては、バッテリーモジュールに認証チップを組み込む事で、品質が保証されたバッテリーしか接続されないような対策が施されている。しかしながら、近年、認証チップの機能を無効化する技術が進み、偽造チップでも認証がパスするケースが横行している。粗悪なバッテリーセルに搭載された偽造チップから、本体機器を通して伝達されるバッテリー状態(電圧、電流、残量等)が正確なものでない(デジタル情報が誤っている)場合、電力管理装置が電力網を正しく制御することができず、事故に繋がる危険性が高い。このような場合には、機器の動作を停止させる等、問題のあるバッテリーを排除しなくてはならないが、そのような機構は既存技術としては存在しない。

【0539】

そこで、電力管理装置・システムに接続された機器・バッテリー等への攻撃(ウィルス

50

混入等)や、バッテリーの劣化や偽造品に伴うリスクを回避することが可能な技術が必要となる。そこで、以下では、バッテリーやシステムに接続された機器から出力されるセンサ情報や各種の履歴情報を用いて、システムに対する上述のような攻撃の有無やバッテリーの劣化等を検出可能な手法について説明する。

【0540】

以下で説明する攻撃の有無やバッテリーの劣化等を検出する方法は、各機器から出力されるセンサ情報等の物理データと履歴情報とを主に利用して、物理予測計算による判断及びヒューリスティックな統計手法を用いて迅速に判断する方法である。これにより、未知の攻撃の検出が可能となり、リスクを事前に回避することが可能となる。

【0541】

本実施形態では、かかる攻撃検出及びリスク回避を実現するための装置として、局所電力管理システム1の外部に設けられた解析サーバ34を利用する。この解析サーバ34は、その機能の一部として、局所電力管理システムのセキュリティチェックを行う機能を有しているものとする。したがって、以下で説明する解析サーバ34は、セキュリティチェックサーバとして機能するサーバである。

【0542】

かかる解析サーバ34は、電力管理装置から送信された各種機器やバッテリーのセンサ情報、実行命令情報、予め解析サーバ34に登録された機器/バッテリー情報、使用環境情報、使用履歴情報をもとに、以下のような機能を実現する。

【0543】

- 認証をパスしたコピー品や劣化して動作が危ういバッテリーの排除
- ヒューリスティックな外部攻撃防御
- 現在の状態、入力、外部環境の情報に基づく予測により妥当性を検証
- 電力管理装置内のアンチウィルスシステムで用いるウィルス定義ファイルの作成・更新

【0544】

また、先に説明したように、かかる解析サーバ34は、各種機器/バッテリーから送信された機器特徴情報に埋め込まれている改ざん検知情報(電子透かし情報)の検証を行う機能を更に備えることも可能である。かかる改ざん検知情報を利用することでも、電力管理装置の乗っ取りの有無を確認することが可能である。

【0545】

ここで、上述のセンサ情報として、例えば、電圧値、電流値、温度、湿度、時刻、使用機器情報、使用者等を挙げることができ、実行命令情報として、命令コマンド、実行ファイル、機器/バッテリー使用パラメータ等を挙げることができる。また、予め解析サーバ34に登録された機器/バッテリー情報として、例えば、メーカー、型番、製造番号等を挙げることができる。また、使用環境情報として、例えば、家族情報、場所、所有機器情報等を挙げることができる。また、上述の使用履歴情報として、例えば、過去の機器/バッテリーのセンサ情報、実行命令情報、使用時間、使用頻度等を挙げることができる。

【0546】

<解析サーバの構成について>

続いて、図59～図62を参照しながら、本実施形態に係るセキュリティチェックサーバである解析サーバ34の構成について、詳細に説明する。図59は、本実施形態に係る解析サーバの構成を説明するためのブロック図である。図60は、本実施形態に係る解析サーバが有する情報改ざん検知部の構成を説明するためのブロック図である。図61は、本実施形態に係る解析サーバが有する第1検証部の構成を説明するためのブロック図である。図62は、本実施形態に係る解析サーバが有する第2検証部の構成を説明するためのブロック図である。

【0547】

[解析サーバの全体構成について]

まず、図59を参照しながら、本実施形態に係る解析サーバ34の全体的な構成を説明する。

10

20

30

40

50

【 0 5 4 8 】

本実施形態に係る解析サーバ34は、図59に例示したように、広域通信部3001と、情報改ざん検知部3003と、取得データ検証部3005と、記憶部3013と、を主に備える。

【 0 5 4 9 】

広域通信部3001は、広域ネットワーク2を介して局所電力管理システム1や他のサーバ等と情報をやり取りするための通信手段である。

【 0 5 5 0 】

情報改ざん検知部3003は、例えば、CPU、ROM、RAM等により実現される。情報改ざん検知部3003は、解析サーバ34が電力管理装置11から取得した情報に、情報の改ざんの有無を検知するためのデータが埋め込まれている場合に、かかるデータを検証して、情報の改ざんが行われたか否かを検知する。このような情報に埋め込まれたデータの一例として、例えば、電子透かしを挙げることができる。

10

【 0 5 5 1 】

情報改ざん検知部3003は、情報に改ざんが行われていることを検知した場合には、その結果を、電力管理装置11やユーザ本人に通知する。これにより、電力管理装置11やこの電力管理装置11を保持しているユーザは、情報の改ざんが行われている機器を、システム1内から排除することが可能となる。

【 0 5 5 2 】

取得データ検証部3005は、例えば、CPU、ROM、RAM等により実現される。取得データ検証部3005は、電力管理装置11から取得した各種の情報を検証して、先に説明したような、電力管理装置11を外部攻撃から防御するための各種機能を提供する処理部である。

20

【 0 5 5 3 】

この取得データ検証部3005は、図59に示したように、取得データ検証制御部3007と、第1検証部3009と、第2検証部3011と、を更に備える。

【 0 5 5 4 】

取得データ検証制御部3007は、解析サーバ34が電力管理装置11から取得した各種のデータを解析及び検証する際の制御を行う。具体的には、取得データ検証制御部3007は、後述する第1検証部3009による検証と第2検証部3011による検証とを、どのように組み合わせて取得データの解析及び検証を実施するかを判断する。したがって、後述する第1検証部3009及び第2検証部3011は、この取得データ検証制御部3007による制御下で、各検証部における検証処理を実施する。

30

【 0 5 5 5 】

第1検証部3009は、例えば、CPU、ROM、RAM等により実現される。第1検証部3009は、解析サーバ34が取得した各種の情報を、統計処理に基づくヒューリスティックな方法を利用して解析及び検証する。

【 0 5 5 6 】

この第1検証部3009は、主に、以下の2つの機能を有する。
 (i) ある電力管理装置から取得したデータを、類似する電力使用環境を持つ他の電力管理装置から取得したデータと比較することで、電力管理装置への攻撃の有無、バッテリーや各種機器又はセンサの異常を検知する機能
 (ii) ある電力管理装置から取得したデータについて、これまでの使用履歴データとの比較から、電力管理装置への攻撃の有無、バッテリーや各種機器又はセンサの異常を検知する機能

40

【 0 5 5 7 】

上記(i)の機能を実現するために、第1検証部3009は、検証対象である電力管理装置11から取得した「バッテリーの型番・ID情報及び電力ステータス情報、履歴」や「各種機器の型番・ID情報及び温度等のセンサ情報、履歴」又は「電力管理装置の実行ファイル」を利用する。また、第1検証部3009は、検証対象である電力管理装置から

50

取得した上述の情報だけでなく、検証対象ではない他の電力管理装置 11 から取得した上述の情報を利用する。第 1 検証部 3009 は、これらのデータを比較及び検証することで、検証対象である電力管理装置への攻撃の有無、バッテリーや各種機器又はセンサの異常を判定する。

【0558】

上記 (ii) の機能を実現するために、第 1 検証部 3009 は、検証対象である電力管理装置 11 から、「バッテリーの型番・ID 情報及び電力ステータス情報」や「各種機器の型番・ID 情報及び温度等のセンサ情報」又は「電力管理装置の実行ファイル」を取得する。また、第 1 検証部 3009 は、検証対象である電力管理装置 11 の「バッテリーの電力ステータス情報履歴」、「各種機器のセンサ情報履歴」、「電力管理装置の実行ファイル履歴」を利用する。第 1 検証部 3009 は、これらのデータを比較及び検証することで、検証対象である電力管理装置への攻撃の有無、バッテリーや各種機器又はセンサの異常を判定する。

10

【0559】

また、第 1 検証部 3009 は、「電力管理装置の実行ファイル」における命令情報を検証し、命令情報が異常だと判定される場合に、異常だと判定された命令情報の中からウィルスパターンを抽出する機能を更に有する。第 1 検証部 3009 は、抽出したウィルスパターンを利用して、当該ウィルスに関するウィルス定義ファイルを生成する。

【0560】

また、各種機器のセンサ情報や実行ファイル、命令情報等が異常だと判定されたとき、第 1 検証部 3009 は、これらの情報を、第 2 検証部 3011 と共有したり、第 2 検証部 3011 に伝達したりしてもよい。このような情報の共有や伝達を行うことで、第 2 検証部でのシミュレーションに用いるパラメータの更新が可能となり、シミュレーション精度を更に向上させることが可能となる。

20

【0561】

第 2 検証部 3011 は、例えば、CPU、ROM、RAM 等により実現される。第 2 検証部 3011 は、解析サーバ 34 が取得した各種の情報を、取得データを利用したシミュレーション（物理予測計算）により解析及び検証する。

【0562】

この第 2 検証部 3011 は、主に、物理量の予測計算による精度の高い判定により、バッテリーや各種機器又はセンサの異常を検知する機能を有する。

30

【0563】

第 2 検証部 3011 は、検証対象である電力管理装置 11 から、システム 1 内の「バッテリーの型番・ID 情報及び電力ステータス情報、履歴」や「各種機器の型番・ID 情報及び温度等のセンサー情報、履歴」を取得する。更に、第 2 検証部 3011 は、検証対象である電力管理装置 11 から、バッテリーや各種機器の電気仕様や特性情報を取得する。第 2 検証部 3011 は、取得した機器情報、電気仕様及び特性情報、並びに、使用履歴情報に基づいてシミュレーションを行い、これら機器が適切に稼働していることを示す指標（以下、正常稼働範囲）を算出する。第 2 検証部 3011 は、算出した正常稼働範囲と、取得した上述の各種データとを比較・検証することで、検証対象である電力管理装置への攻撃の有無、バッテリーや各種機器又はセンサの異常を判定する。

40

【0564】

記憶部 3013 は、本実施形態に係る解析サーバ 34 が備えるストレージ装置の一例である。記憶部 3013 には、解析サーバ 34 が保持する各種の鍵に関する情報、解析サーバ 34 が保持する各種のデジタル署名や証明書等が格納される。また、記憶部 3013 には、各種の履歴情報が記録されていてもよい。さらに、記憶部 3013 には、本実施形態に係る解析サーバ 34 が、何らかの処理を行う際に保存する必要が生じた様々なパラメータや処理の途中経過等、または、各種のデータベース等が、適宜記録されてもよい。この記憶部 3013 には、解析サーバ 34 の有する各処理部が、自由に読み書きを行うことが可能である。

50

【0565】

[情報改ざん検知部の構成について]

続いて、図60を参照しながら、情報改ざん検知部3003の構成について説明する。

【0566】

情報改ざん検知部3003は、図60に示したように、埋め込み位置特定部3021と、電子透かし抽出部3023と、電子透かし検証部3025とを更に有する。

【0567】

本実施形態に係る局所電力管理システム1では、電流値、電圧値、温度、湿度といった物理データそのものや物理データを利用して算出された各種情報に、これらの情報に適した電子透かしデータを埋め込むことが可能である。局所電力管理システム1と相互に通信可能な解析サーバ34は、かかる電子透かしデータの検証を行うことで、物理データ(物理データを利用して算出された各種情報を含む。以下同じ。)に改ざんが行われたか否かを検知することができる。

10

【0568】

埋め込み位置特定部3021は、例えば、CPU、ROM、RAM等により実現される。埋め込み位置特定部3021は、所定の信号処理回路により、電子透かしの埋め込まれた物理データを解析することで、データに対応する信号の特徴に応じて、電子透かし情報の埋め込み位置を特定する。埋め込み位置特定部3021は、電子透かし情報の埋め込み位置を特定すると、特定した埋め込み位置に関する情報を、電子透かし抽出部3023に通知する。なお、電子透かしの埋め込み位置が、制御化装置125等と解析サーバ34との間で予め決まっている場合には、かかる埋め込み位置の特定処理は、実行しなくともよい。

20

【0569】

電子透かし抽出部3023は、例えば、CPU、ROM、RAM等により実現される。電子透かし抽出部3023は、埋め込み位置特定部3021から通知された埋め込み位置に関する情報に基づいて、物理データの中から電子透かし情報を抽出する。電子透かし抽出部3023は、物理データの中から抽出した電子透かし情報を、後述する電子透かし検証部3025に伝送する。

【0570】

電子透かし検証部3025は、例えば、CPU、ROM、RAM等により実現される。電子透かし検証部3025は、まず、制御化装置125等との間で共有している共有情報と、電子透かし抽出部3023によって抽出された物理データとに基づいて、電子透かし情報を生成する。この電子透かし情報の生成には、ハッシュ関数、疑似乱数発生器、共通鍵暗号、共有鍵暗号(例えば、メッセージ認証符号 Message Authentication Code: MAC)等が用いられる。続いて、電子透かし検証部3025は、生成した電子透かし情報と、電子透かし抽出部3023が抽出した電子透かし情報とを比較する。

30

【0571】

電子透かし検証部3025は、生成した電子透かし情報と抽出された電子透かし情報とが同一である場合には、制御化装置125等によって生成された物理データ等に改ざんがなされていないと判断する。また、電子透かし検証部3025は、生成した電子透かし情報と抽出された電子透かし情報とが同一ではない場合には、物理データに改ざんがなされたと判断する。

40

【0572】

電子透かし検証部3025は、物理データに改ざんがなされていた場合には、その旨を電力管理装置11やユーザ本人に通知する。これにより、電力管理装置11やユーザ本人は、改ざんを加えうる操作がなされている制御化機器125等を、局所電力管理システム1内から排除することが可能となる。

【0573】

また、電子透かし情報が、物理データ及び共有情報だけでなく、時刻情報をも利用して

50

生成されたものである場合には、先に説明したように、局所電力管理システム 1 を管理している電力管理装置が乗っ取られているか否かについても検証することが可能となる。

【0574】

[第1検証部の構成について]

次に、図61を参照しながら、第1検証部3009の構成について、詳細に説明する。

【0575】

上述のように、第1検証部3009は、電力管理装置11から送信されたバッテリーや各種機器のセンサ情報や実行命令情報と、予め解析サーバ34に登録されているバッテリーや各種機器の情報、使用環境情報、使用履歴情報を基に、特徴量を抽出する。その後、第1検証部3009は、抽出した特徴量に基づいて、違いや異常を迅速に検出する。

10

【0576】

第1検証部3009は、図61に示したように、検証制御部3031、動作判定部3033、データベース管理部3035、ウィルス定義ファイル管理部3037及び共有情報生成部3039を有する。また、第1検証部3009は、電力管理装置データベース3041、判定辞書3043及びウィルス定義ファイルデータベース3045を更に有する。

【0577】

検証制御部3031は、例えば、CPU、ROM、RAM等により実現される。検証制御部3031は、第1検証部3009で行われる統計処理を利用したヒューリスティックな検証処理の制御を行い、第1検証部3009の有する各処理部を連携して機能させることができる。

20

【0578】

動作判定部3033は、例えば、CPU、ROM、RAM等により実現される。動作判定部3033は、検証対象である電力管理装置11から取得したセンサ情報や実行命令情報等の各種情報を入力とし、当該電力管理装置11や他の電力管理装置11の履歴情報等をもとに、検証対象である電力管理装置の動作の正常/異常を判定する。動作判定部3033で実施される判定処理については、以下で改めて説明する。

【0579】

データベース管理部3035は、例えば、CPU、ROM、RAM等により実現される。データベース管理部3035は、電力管理装置11から送信された、新たなバッテリーや各種機器のセンサ情報、実行命令情報、履歴情報等の各種情報をデータベース3041に保存するとともに、判定辞書3043の更新を行う。また、データベース管理部3035は、特定の電力管理装置11の統計量と、他の電力管理装置11のデータの統計量とを定期的に比較し、故意に生成されたデータであるか否かを検査する。

30

【0580】

ウィルス定義ファイル管理部3037は、例えば、CPU、ROM、RAM等により実現される。ウィルス定義ファイル管理部3037は、動作判定部3033で異常と判定された実行命令情報をウィルスパターンとして定義し、ウィルス定義ファイルを作成する。また、ウィルス定義ファイル管理部3037は、生成したウィルス定義ファイルをウィルス定義ファイルデータベース3045に格納してデータベースを更新するとともに、生成したウィルス定義ファイルを、検証制御部3031を介して外部に送信する。

40

【0581】

共有情報生成部3039は、動作判定部3033で異常だと検知された電力管理装置11の情報(例えば、バッテリー/各種機器のセンサ情報、実行命令情報、バッテリー/各種機器の機器情報、使用履歴情報等)を、共有情報として取りまとめる。その後、共有情報生成部3039は、生成された共有情報を、検証制御部3031及び取得データ検証制御部3007を介して、第2検証部3011に出力する。

【0582】

第2検証部3011は、かかる共有情報を利用して、シミュレーションの各種設定情報(パラメータ等)を更新することで、シミュレーション精度を更に向上させることが可能となる。

50

【0583】

電力管理装置データベース3041は、第1検証部3009の有するデータベースの一つである。このデータベースには、各電力管理装置11のバッテリーや各種機器に関する機器情報、使用環境情報、使用履歴情報等の各種の情報が格納されている。

【0584】

判定辞書3043は、第1検証部3009の有するデータベースの一つであって、動作判定部3033がヒューリスティックに動作判定を行う際の特徴量に関する情報が格納されている。この特徴量は、ある条件（機器情報、使用環境情報等）が与えられたときの典型的なセンサ情報の統計量であり、電力管理装置データベース3041に基づいて生成される。

【0585】

ウィルス定義ファイルデータベース3045は、第1検証部3009の有するデータベースの一つである。ウィルス定義ファイルデータベースには、ウィルス定義ファイル管理部3037で生成されるウィルス定義ファイルが格納されている。

【0586】

以上、第1検証部3009の構成について、詳細に説明した。

【0587】

[第2検証部の構成について]

次に、図62を参照しながら、第2検証部3011の構成について、詳細に説明する。

【0588】

上述のように、第2検証部3011は、バッテリーの経年変化や使用環境、使用履歴、使用状況、特性情報に基づいてシミュレーションを行うことで正常稼働範囲を算出し、違いや異常を迅速に検出する。第1検証部3009における検証は、擬似環境等からの統計情報を用いた迅速な判定手法であるが、第2検証部3011による検証は、検証時間は要するものの、正規品の品質劣化状況を精度高く算出することが可能となる。

【0589】

また、第2検証部3011は、第1検証部3009から出力された共有情報を利用して、シミュレーションを実行する際に利用される各種の設定情報（パラメータ）を適切な値に更新する機能を有する。

【0590】

第2検証部3011は、図62に示したように、特性予測値算出部3051と、データベース3053と、データ判定部3055と、を更に備える。

【0591】

特性予測値算出部3051は、例えば、CPU、ROM、RAM等により実現される。特性予測値算出部3051は、検証対象である電力管理装置11から取得した機器情報、電気仕様及び特性情報、並びに、使用履歴情報に基づいてシミュレーションを行い、特性予測値を算出する。この特性予測値が、機器が適切に稼働していることを示す指標（すなわち、正常稼働範囲）となる。特性予測値算出部3051は、シミュレーションを実行するにあたって、データベース3053に登録されているシミュレーションの各種パラメータを取得する。

【0592】

データベース3053は、第2検証部3011が有するデータベースの一つであり、特性予測値算出部3051がシミュレーションを行う場合に利用する各種設定情報（パラメータ）が格納されている。データベース3053に格納されているパラメータは、先に説明したように、第1検証部3011から出力された共有情報を利用して、第2検証部3011により更新される。

【0593】

データ判定部3055は、例えば、CPU、ROM、RAM等により実現される。データ判定部3055は、検証対象である電力管理装置11から取得した各種データと、特性予測値算出部3051が算出した特性予測値とを比較して、検証対象である電力管理装置

10

20

30

40

50

11から取得した各種データの判定を行う。データ判定部3055は、任意のロジックを利用することで、バッテリーや各種機器又はセンサの異常を検知することが可能であるが、例えば、実際の値と特性予測値との乖離が所定の閾値以上となっている場合、又は、乖離が所定の閾値以下となっている場合等に、各種機器に異常が発生していると判断することが可能である。

【0594】

第2検証部3011では、物理シミュレーションで用いるパラメータを、より実際の値に補正することが可能である。また、これらの情報をバッテリー/機器メーカーへ送信し、事前に想定されなかった故障を知らせることも可能である。

【0595】

以上、第2検証部3011の構成について、詳細に説明した。

【0596】

以上、本実施形態に係る解析サーバ34の機能の一例を示した。上記の各構成要素は、汎用的な部材や回路を用いて構成されていてもよいし、各構成要素の機能に特化したハードウェアにより構成されていてもよい。また、各構成要素の機能を、CPU等が全て行ってもよい。従って、本実施形態を実施する時々の技術レベルに応じて、適宜、利用する構成を変更することが可能である。

【0597】

なお、上述のような本実施形態に係る解析サーバの各機能を実現するためのコンピュータプログラムを作製し、パーソナルコンピュータ等に実装することが可能である。また、このようなコンピュータプログラムが格納された、コンピュータで読み取り可能な記録媒体も提供することができる。記録媒体は、例えば、磁気ディスク、光ディスク、光磁気ディスク、フラッシュメモリなどである。また、上記のコンピュータプログラムは、記録媒体を用いずに、例えばネットワークを介して配信してもよい。

【0598】

<排除すべきバッテリーの特定処理について>

続いて、上述のような機能を有する解析サーバ34によって行われる、排除すべきバッテリーの特定処理について、図63を参照しながら簡単に説明する。図63は、排除すべきバッテリーについて説明するための説明図である。

【0599】

図63に示した表は、局所電力管理システム1に用いられるバッテリーについて、考えられる状況を列挙したものである。局所電力管理システム1に用いられるバッテリーは、図63の上側に示したように、電力が蓄えられている1または複数のセルと、セルを制御するための基板と、基板上に設けられている認証用のチップと、を備える。セル及び認証チップを含む基板が取りうる状況は、表に示した7通りに大別されると考えられる。

【0600】

ケース1~ケース3は、正規品のセルと正規品の基板とからなるバッテリーに生じうる状況を示したものである。また、ケース4~ケース7は、非正規品のセルが用いられたバッテリーに生じうる状況を示したものである。

【0601】

これらの7つのケースのうち、ケース1、ケース2及びケース4については、セル特性に問題は無く、正しい機器状況を出力している場合である。かかるケースに区分されるバッテリーについては、予測の範囲にある劣化や、コピー品であるものの特性や情報に問題がないものであるため、局所電力管理システム内に存在したとしても大きな問題はない。

【0602】

しかしながら、ケース3及びケース5~7に区分されるバッテリーについては、セルの特性又は機器情報が正規品で正常な使用をした場合と比べて乖離があるものであって、ある種のリスクを伴うものであるため、局所電力管理システムからの排除が必要である。

【0603】

そこで、本実施形態に係る解析サーバ34は、上述のような各種の検証処理を利用する

10

20

30

40

50

ことで、上述のような排除すべきバッテリーを特定することが可能となる。

【0604】

解析サーバ34による排除すべきバッテリーの特定処理については、以下で改めて詳細に説明する。

【0605】

<電力管理装置への不正攻撃に対する防御方法について>

次に、図64を参照しながら、電力管理装置への不正攻撃に対する防御方法の全体的な流れを説明する。図64は、電力管理装置への不正攻撃に対する防御方法を説明するための流れ図である。

【0606】

なお、以下の説明に先立ち、電力管理装置11には、不正攻撃を防止するサービス(すなわち、解析サーバ34によるサービス)に加入する設定がなされ、サービスの実行頻度やタイミング等が予め設定されているものとする。

【0607】

電力管理装置11のシステム管理部1125は、まず、不正攻撃の有無をチェックする時刻が到来したか否かを判断する(ステップS3001)。チェック時刻が到来していない場合には、電力管理装置11のシステム管理部1125は、チェック時刻の到来を待ち受ける。また、チェック時刻が到来していた場合には、電力管理装置11のシステム管理部1125は、これまでに電力管理装置11に蓄えられている攻撃パターンファイル(ウィルス定義ファイル)を利用して、システム内を検索する(ステップS3003)。

【0608】

パターンチェックに問題があった場合には、電力管理装置11のシステム管理部1125は、電力管理装置11が保持している機器排除リストに問題のあった機器を登録し、制御部115が問題のあった機器をシステムから離脱させる(ステップS3005)。

【0609】

また、パターンチェックに問題がなければ、電力管理装置11の機器管理部1121は、システムに接続されているバッテリーを含む各種機器からセンサ情報、実行命令情報の各種情報を収集する(ステップS3007)。続いて、電力管理装置11の機器管理部1121は、解析サーバ34に相互認証を経てアクセスする(ステップS3009)。コネクションが確立されると、電力管理装置11は、電力管理装置のID、機器毎のバッテリーID、バッテリーの電力情報、センサ情報及び電力管理装置の実行命令情報を暗号化して、解析サーバ34に送信する(ステップS3011)。

【0610】

解析サーバ34の取得データ検証部3005は、電力管理装置11から送信された各種データに異常がないかを判定する(ステップS3013)。異常がない場合は、取得データ検証部3005は、取得した電力管理装置11のデータをデータベースに追加した上で(ステップS3015)、解析結果を電力管理装置11へ通知する(ステップS3017)。

【0611】

他方、ステップS3013において異常が認められた場合、解析サーバ34の取得データ検証部3005は、ウィルス定義ファイルを生成する(ステップS3019)。また、解析サーバ34の取得データ検証部3005は、異常が認められた電力管理装置11に異常が多発しているかを確認する(ステップS3021)。異常が多発しており、電力管理装置11が攻撃の踏み台になっている等と判断される場合、解析サーバ34は、システム管理サーバ33に異常を通報する(ステップS3023)。通報を受けたシステム管理サーバ33は、該当する装置をブラックリストに掲載するなどして除外する(ステップS3025)。また、解析サーバ34は、解析結果と、ステップS3019で生成したウィルス定義ファイルを、電力管理装置11に対して送信する(ステップS3027)。電力管理装置11のシステム管理部1125は、結果を受けて、ウィルス定義ファイルがある場合はこれを更新するなどの対応を行う(ステップS3029)。

10

20

30

40

50

【0612】

以上、電力管理装置への不正攻撃に対する防御方法の全体的な流れを説明した。

【0613】

<バッテリーの排除方法について>

続いて、図65を参照しながら、解析サーバ34で行われる排除すべきバッテリーの特定処理及び電力管理装置11で行われるバッテリーの排除処理について、その流れを説明する。図65は、バッテリーの排除方法について説明するための流れ図である。

【0614】

本実施形態に係る解析サーバ34は、電力管理装置11から発信された情報をもとに、バッテリーに異常がないかを検知し、異常時には電力管理装置11にその旨を通知する。通知を受けた電力管理装置11は、異常なバッテリーへの給電を中止するなどといった一連の動作を実施する。

10

【0615】

なお、以下の説明に先立ち、電力管理装置11には、バッテリーリスクを排除するサービス(すなわち、解析サーバ34によるサービス)に加入する設定がなされ、サービスの実行頻度やタイミング等が予め設定されているものとする。

【0616】

電力管理装置11のシステム管理部1125は、まず、バッテリーリスクをチェックする時刻が到来したか否かを判断する(ステップS3031)。チェック時刻が到来していない場合には、電力管理装置11のシステム管理部1125は、チェック時刻の到来を待ち受ける。また、チェック時刻が到来していた場合には、電力管理装置11の機器管理部1121は、バッテリーを有する制御化機器125等にバッテリー情報(バッテリー一次情報)を送信するように要請する。これにより、バッテリーを有する各制御化機器125は、バッテリー情報を、電力管理装置11に送信することとなる(ステップS3033)。電力管理装置11は、全ての機器からバッテリー情報を取得できたかを確認する(ステップS3035)。なお、必ずしも全ての機器からバッテリー情報を取得するようにしなくとも良いが、好ましくは、全ての機器をチェックすることが好ましい。

20

【0617】

電力管理装置11の機器管理部1121は、解析サーバ34に相互認証を経てアクセスする(ステップS3037)。コネクションが確立されると、電力管理装置11は、電力管理装置のID、機器毎のバッテリーID、バッテリーの一次情報を、解析サーバ34に送信する(ステップS3039)。

30

【0618】

解析サーバ34の取得データ検証部3005は、電力管理装置11から送信された各種データを利用して特性予測値を算出し、取得したデータと算出した特性予測値との比較を行う。その上で、解析サーバ34の取得データ検証部3005は、得られた結果を電力管理装置11に通知する(ステップS3041)。

【0619】

電力管理装置11のシステム管理部1125は、得られた結果を判断する(ステップS3043)。異常なしという結果である場合、電力管理装置11の機器管理部1121は、収集したセンサからの物理情報を確認して(ステップS3045)、問題が無ければ処理を終了する。

40

【0620】

また、ステップS3043において異常がある場合、電力管理装置11の制御部115は、異常を持つバッテリーの本体機器への給電停止命令を、分電装置121に出令する(ステップS3047)。分電装置121は、電量管理装置11の命令に従い、該当機器への給電を停止する(ステップS3049)。電力管理装置11のシステム管理部1125は、異常のあった機器のIDをリポークリストに掲載し、機器管理部1121は、該当機器の情報ネットワークを切断する(ステップS3051)。

【0621】

50

以上のような処理が行われることで、解析サーバ34は、排除すべきバッテリーを特定することが可能となり、電力管理装置11は、排除すべきバッテリーをシステム内から除外することができる。

【0622】

<取得データ検証部における検証処理について>

続いて、図66A及び図66Bを参照しながら、解析サーバ34の取得データ検証部3005における検証処理の全体的な流れを説明する。図66A及び図66Bは、取得データ検証部における検証処理を説明するための流れ図である。

【0623】

解析サーバ34の取得データ検証部3005が有する取得データ検証制御部3007は、まず、電力管理装置11から送信された各種のデータを取得する(ステップS3061)。続いて、取得データ検証制御部3007は、取得したデータに対して、所定のフィルタを用いた検査を行う(ステップS3063)。このフィルタは、例えば、特定の電力管理装置11から大量の情報が送信されるDOS攻撃に対する防御、ファイアウォールの機能、及び/又は、規格外の通信の除去を行うためのものである。

【0624】

取得データ検証制御部3007は、取得データに対するフィルタ処理で異常を検出した場合、異常判定を出力して(ステップS3083)、所定の警告処理を実施し(ステップS3085)、このフローを終了する。この警告処理は、例えば、システム管理サーバ33や、該当する電力管理装置と関係のある他のサーバに対して行われるものである。

【0625】

また、取得データ検証制御部3007は、フィルタ処理で異常を検出しなかった場合、取得データに対して、簡易判定処理を実施する(ステップS3065)。簡易判定では、予め解析サーバ34側で把握しているウィルスパターンの検出や、第1検証部3009による簡易的な判定や、典型的な使用法とのマッチングが行われ、通常は高速に行うことが想定される。この段階で明らかに正常な動作であると確認できる場合は、正常判定を出力して(ステップS3081)、フローを終了する。

【0626】

他方、取得データ検証制御部3007は、この簡易判定において、異常ありと判断された場合又は判断ができない場合に、以下で説明するパターン1~パターン3の3つの判定処理のいずれを利用するかを判断を行う(ステップS3067)。

【0627】

パターン1は、第1検証部3009と第2検証部3011とを組み合わせて利用する、連携型判別処理を選択するパターンである。

【0628】

例えば、取得データ検証部3007は、はじめに、第1検証部3009による統計処理(ステップS3069)により判定を行うとともに、送信された情報からバッテリー/機器の物理的な特性を把握する。ここで、取得データ検証制御部3007は、処理経路の判定を行って(ステップS3071)、最終的な結果を出力するか(ステップS3075)、第2検証部3009による検証(ステップS3073)を行うかを判断する。第2検証部3009による検証が更に行われる場合、第2検証部3009は、第1検証部3009から通知される共有情報(すなわち、物理的特性)に基づいて、シミュレーションで用いる物理パラメータを更新し、送信された情報をもとにシミュレーションを行う。更に、第1検証部3009は、第2検証部3009による検証で得られた知見をもとに判定辞書の更新を行って、再度統計処理により判定を行う。

【0629】

また、一方での判定により、より詳しく調査する点を明確化し、他方の判定法にフィードバックを与える判定処理も選択可能である。このように、第1検証部3009と、第2検証部3011とを相補的に用いることで判定精度を向上させるのが、パターン1の手法である。

10

20

30

40

50

【0630】

パターン2は、第1検証部3009による検証と、第2検証部3011による検証を順番に実行する直列型判別処理を選択するパターンである。

【0631】

具体的には、取得データ検証制御部3007は、比較的処理時間を短く判定できる第1検証部3009による検証をまず実施し(ステップS3077)、正常と判断されない場合に長い処理時間を要する第2検証部3011による検証(ステップS3079)へ移行する方式である。ここでの第1検証部3009による検証は、簡易判定における検証よりも詳細に調査されることを想定している。

【0632】

このパターン2の場合、第1検証部3009による検証で正常と判断されれば、取得データ検証制御部3007は、正常判定を出力して(ステップS3081)、このフローを終了する。

【0633】

図66Aでは、比較的高速な第1検証部3009による検証を先に実施することを想定しているが、第2検証部3011による検証を先に実施してもよい。

【0634】

パターン3は、第1検証部3009による検証と、第2検証部3011による検証とを同時に用いる並列型判別処理を選択するパターンである。

【0635】

取得データ検証制御部3007により、第1検証部3009及び第2検証部3011の双方による検証を行うか、どちらか一方による検証のみを行うか、更に、どの属性について検査するかが決定される(ステップS3087)。第1検証部3009(ステップS3089)及び第2検証部3011(ステップS3091)は、各々検査を行い、取得データ検証制御部3007は、両処理部からの調査結果をもとに最終的な判断を行う(ステップS3093)。

【0636】

なお、これら3つの手法は、いずれかが行われる使用法もあるが、並列して行われる場合もありえる。また、調査する属性情報やセンサ情報の範囲などにより、適応的に配分する可能性もある。更に、パターン1～パターン3が各々1つだけでなく、複数用いて並列化することで、高速性を期待するモデルも可能である。

【0637】

<第1検証部による検証処理の流れについて>

続いて、図67を参照しながら、第1検証部による検証処理の流れを説明する。図67は、第1検証部による検証処理を説明するための流れ図である。

【0638】

第1検証部3009の検証制御部3009は、まず、検証対象の電力管理装置11について、バッテリー/センサ情報及び実行命令情報の少なくとも何れか一方を、検証データとして取得する(ステップS3101)。続いて、動作判定部3033は、取得した情報(例えば、バッテリーや各種機器のセンサ情報)に対して、データ形式を整形する前処理を実施する(ステップS3103)。

【0639】

その後、第1の動作判定部3033は、特定の属性情報(例えば、機器情報、使用環境情報)が指定され、その属性に応じて、前処理により整形したデータ(バッテリーや各機器のセンサ情報、実行命令情報)から特徴量が抽出される(ステップS3105)。特徴量の抽出の際に指定された属性情報について、典型的な特徴量が、他の電力管理装置や検証対象である電力管理装置の使用履歴から予め算出されているので、判定辞書には、指定された属性情報の場合の典型的な特徴量が格納されている。

【0640】

なお、特徴量は、以下のいずれかのものとなる。

10

20

30

40

50

- 検証対象ではない電力管理装置におけるバッテリー / センサ情報や使用履歴による特徴
- 検証対象である電力管理装置のバッテリー / センサ情報・履歴による特徴
- 検証対象ではない電力管理装置における実行命令の特徴
- 検証対象である電力管理装置の実行命令の特徴

【0641】

続いて、第1の動作判定部3033は、指定された属性情報の場合の典型的な特徴量と、算出した特徴量とを比較し(ステップS3107)、判定結果を出力する(ステップS3109)。動作判定部3033は、例えば、2つの特徴量の相関度が低い場合は異常と判定し、高い場合は正常と判定することが可能である。

【0642】

また、他の動作判定部3033においても、同一の特徴量又は異なる特徴量について、同様の処理が実施され(ステップS3111~ステップS3115)、判定結果が出力される。

【0643】

その後、検証制御部3031は、各動作判定部3033からの判定結果をもとに、最終的な正常 / 異常の判定を行う(ステップS3117)。例えば、各動作判定部3033から正常 / 異常の判定がなされる場合は、検証制御部3031は、多数決をとる。または、検証制御部3031は、正常を1、異常を0として、重みをかけた上で足し合わせ、閾値以上の値の場合を正常とするなどの手法を行う。また、相関度や関数値が算出される場合は、検証制御部3031は、同様に重みをかけて和をとった上での閾値判定や、何らかの関数を用いる手法がありえる。

【0644】

検証制御部3031は、以上のようにして得られた総合判定結果を取得データ検証制御部3007に出力し(ステップS3119)、検証処理を終了する。また、取得データ検証制御部3007は、得られた検証結果を、電力管理装置、ユーザ自身、他のサービスを提供するサーバ等へ出力する。

【0645】

なお、動作判定部3033は、判定関数として、例えば、Nearest neighbor rule、パーセプトロン、ニューラルネットワーク、サポートベクタマシン、多変量解析、Boostingなどの手法を用いることが可能である。また、判定関数の各パラメータは、他の電力管理装置11のデータや物理データをもとに、予め学習により決定することが可能である。

【0646】

なお、上述の処理によって最終的に異常が認められた場合は、ウィルス定義ファイル管理部3037によって、異常が認められた実行命令情報からパターンが抽出され、ウィルス定義ファイルが生成される。

【0647】

<データベース管理部における検査処理について>

続いて、図68を参照しながら、第1検証部3009が有するデータベース管理部3037における検査処理について、説明する。図68は、データベース管理部における検査処理を説明するための流れ図である。

【0648】

データベース管理部3037では、特定の電力管理装置11から取得したデータの統計量と、他の電力管理装置から取得したデータの統計量とを定期的に比較し、故意に生成されたデータであるか否かの検査を行う。

【0649】

データベース管理部3037は、動作判定部3033における異常動作の検知のために、通常は、多くの電力管理装置から収集した各種情報(例えば、バッテリーや各機器のセンサ情報)から、比較用の特徴量を予め抽出しておく。

【0650】

10

20

30

40

50

この場合に、悪意のある電力管理装置 1 1 が、改ざんを施したバッテリーや各機器のセンサ情報等を送信し、特徴量を操作する可能性がある。そのため、データベース管理部 3 0 3 7 は、特定の属性情報（例えば、機器情報や使用環境情報等）を有する特定の電力管理装置の使用履歴情報から抽出した特徴量と、同じ属性情報を有する他の複数の電力管理装置の使用履歴から抽出した特徴量を比較することで、この攻撃を検出する。

【 0 6 5 1 】

データベース管理部 3 0 3 7 は、まず、特定の属性情報に関して、悪意のある電力管理装置が否かを判定したい電力管理装置のセンサ情報又は実行命令情報を取得して（ステップ S 3 1 2 1）、取得した情報から特徴量を抽出する（ステップ S 3 1 2 3）。また、データベース管理部 3 0 3 7 は、同じ属性情報を持つ他の複数の電力管理装置から同様の情報を取得して（ステップ S 3 1 2 5）、同様の方法で特徴量を抽出する（ステップ S 3 1 2 7）。

10

【 0 6 5 2 】

次に、データベース管理部 3 0 3 7 は、算出した 2 つの特徴量を比較し、着目している特定の電力管理装置が、特徴量に対して不正な操作をしているか否かを判定して（ステップ S 3 1 2 9）、最終的な結果を出力する（ステップ S 3 1 3 1）。または、データベース管理部 3 0 3 7 は、他の属性についても同様の比較・判定を行い、最終的な結果を決定する。なお、特徴量の比較・判定には、先に列挙した判定関数を用い、そのパラメータは、予め学習により算出しておく。

【 0 6 5 3 】

判定の結果、悪意がある電力管理装置であると判断される場合、解析サーバ 3 4 は、その旨を、電力管理装置 1 1 を保持するユーザや、電力会社等のサービス提供サーバへと通知する。

20

【 0 6 5 4 】

< データベースの更新と判定辞書の生成について >

続いて、図 6 9 を参照しながら、データベース管理部 3 0 3 5 におけるデータベースの更新と、判定辞書の生成について、簡単に説明する。図 6 9 は、データベース管理部におけるデータベースの更新及び判定辞書の生成について説明するための説明図である。

【 0 6 5 5 】

データベース管理部 3 0 3 5 は、電力管理装置 1 1 からの新たなセンサ情報や実行命令情報等をデータベース 3 0 4 1 に格納するとともに、動作判定部 3 0 3 3 が用いる判定辞書 3 0 4 3 の生成も行う。

30

【 0 6 5 6 】

電力管理装置 1 1 から定期的に送信されるセンサ情報、実行命令情報、電力管理装置 1 1 から登録時に送信される機器情報、使用環境情報等は、検証制御部 3 0 3 1 を介して、電力管理装置データベース 3 0 4 1 に格納される。また、特定の電力管理装置 1 1 の使用時間、使用頻度等についても、センサ情報に基づいて算出され、電力管理装置データベース 3 0 4 1 に格納される。

【 0 6 5 7 】

動作判定部 3 0 3 3 が用いる判定辞書 3 0 4 3 には、特定の属性情報それぞれについて、複数の電力管理装置 1 1 のセンサ情報、実行命令情報等をもとに抽出された特徴量が格納されている。この判定辞書 3 0 4 3 は、初期段階ではサンプル数が少ないと想定されるため、電力管理装置 1 1 から各機器に関する物理データが送信され、特徴量が推定される。また、特定の属性情報の場合にはサンプル数も少ないことが予想されるので、その物理データからの特徴量を抽出し、特徴量の補正に用いる使用方法もありえる。

40

【 0 6 5 8 】

< ウィルス定義ファイルの管理方法について >

次に、図 7 0 を参照しながら、ウィルス定義ファイル管理部 3 0 3 7 によるウィルス定義ファイルの管理方法について、簡単に説明する。図 7 0 は、ウィルス定義ファイル管理部によるウィルス定義ファイルの管理方法を説明するための流れ図である。

50

【0659】

ウイルス定義ファイル管理部3037は、動作判定部3033による判定で異常と判定された実行命令情報をウイルスパターンとして定義し、ウイルス定義ファイルを作成する。その後、ウイルス定義ファイル管理部3037は、生成したウイルス定義ファイルを、ウイルス定義ファイルデータベース3045に格納する。

【0660】

ウイルス定義ファイルの生成に先立ち、まず、動作判定部3033によって、ある電力管理装置11の動作が異常であると判断される(ステップS3141)。すると、ウイルス定義ファイル管理部3037は、動作判定部3033で異常であると判断された実行命令情報を解析し、パターンを抽出する(ステップS3143)。

10

【0661】

続いて、ウイルス定義ファイル管理部3037は、抽出したパターンをもとにファイル(ウイルス定義ファイル)を生成し(ステップS3145)、生成した定義ファイルをウイルス定義ファイルデータベース3145に格納する。また、ウイルス定義ファイル管理部3037は、取得データ検証制御部3007を介して、生成した定義ファイルを、電力管理装置11に送信する(ステップS3149)。各電力管理装置11や解析サーバ34は、この定義ファイルをウイルス検出のためのフィルタとして利用することが可能である。

【0662】

また、ウイルス定義ファイル管理部3037は、パターンが抽出された実行命令情報を有する電力管理装置11の使用履歴情報を解析する。その結果、この電力管理装置11から頻繁に異常が発せられているならば、場合によってはこの電力管理装置を悪意ある攻撃者とみなし、ブラックリストへ登録する(ステップS3151)。また、ウイルス定義ファイル管理部3037は、かかる電力管理装置11の存在を電力会社へ報告してもよい。

20

【0663】

なお、電力管理装置がブラックリストに登録されると、登録された電力管理装置からの通信の受信拒否や他の電力管理装置への注意の喚起が行われる。

【0664】

<排除すべきバッテリーの特定方法の流れについて>

続いて、図71A～図72を参照しながら、取得データ検証部3005が実施する排除すべきバッテリーの特定方法の流れを説明する。図71A～図72は、取得データ検証部が実施する排除すべきバッテリーの特定方法を説明するための流れ図である。

30

【0665】

まず、図71A～図71Cを参照しながら、図63におけるケース3、ケース5及びケース6に該当するバッテリーを特定する処理について説明する。

【0666】

なお、説明に先立ち、電力管理装置11には、バッテリーリスクを排除するサービス(すなわち、解析サーバ34によるサービス)に加入する設定がなされ、サービスの実行頻度やタイミング等が予め設定されているものとする(ステップS3161)。

【0667】

電量管理装置11のシステム管理部1125は、バッテリーリスクをチェックする時刻が到来すると、電力管理装置11が管理している管理機器である制御化機器125に対して、性能チェックを要求する(ステップS3163)。

40

【0668】

制御化機器125の本体は、接続されているバッテリーに対して、バッテリーに関する電圧/電流/残量/インピーダンス/負荷等に関する一時情報(すなわち、セル特性)D1と、機器情報D2と、を取得するように要請する(ステップS3165)。

【0669】

制御化機器125に接続されているバッテリーは、これらの情報D1及びD2を取得して(ステップS3167)、制御化機器125の本体を介して、これらの情報およびバッテリーのID情報を、電力管理装置11に送信する(ステップS3169)。

50

【 0 6 7 0 】

電力管理装置 1 1 の機器管理部 1 1 2 1 は、取得した情報を電力管理装置 1 1 が保持しているデータベースに保存する（ステップ S 3 1 7 1）。また、電力管理装置 1 1 は、解析サーバ 3 4 に対して、特性の問い合わせを行う（ステップ S 3 1 7 3）。その後、電力管理装置 1 1 は、解析サーバ 3 4 との間で認証を行い（ステップ S 3 1 7 5）、両者の間の通信路を確立する。

【 0 6 7 1 】

続いて、電力管理装置 1 1 のシステム管理部 1 1 2 5 は、解析サーバ 3 4 に、取得した情報（D 1、D 2 及びバッテリーの ID 情報）を送信する（ステップ S 3 1 7 7）。

【 0 6 7 2 】

解析サーバ 3 4 の取得データ検証部 3 0 0 5 が有する第 2 検証部 3 0 1 1 は、取得したデータを利用して、特性予測計算を行って（ステップ S 3 1 7 9）、情報 D 1 及び情報 D 2 に関する特性予測値を算出する。その後、第 2 検証部 3 0 1 1 は、実測値と予測値との乖離の具合を算出して、結果を判定する（ステップ S 3 1 8 1）。その後、解析サーバ 3 4 は、得られた判定結果を、電力管理装置 1 1 に送信する（ステップ S 3 1 8 3）。

【 0 6 7 3 】

ここで、ステップ S 3 1 8 1 において得られる判定結果は、各ケースについて、以下のようになると考えられる。

【 0 6 7 4 】

（ケース 3）D 1 に関する乖離具合：所定範囲外、D 2 に関する乖離具合：所定範囲外

（ケース 5）D 1 に関する乖離具合：所定範囲外、D 2 に関する乖離具合：所定範囲外

（ケース 6）D 1 に関する乖離具合：所定範囲外、D 2 に関する乖離具合：所定範囲外

【 0 6 7 5 】

上述のような判定結果を取得した電力管理装置 1 1 は、異常に対応するための処理を行う（ステップ S 3 1 8 5）。具体的には、電力管理装置 1 1 の機器管理部 1 1 2 1 は、分電装置 1 2 1 に対して、異常が発生している制御化機器 1 2 5 に対して給電を停止するように命令する（ステップ S 3 1 8 7）。分電装置 1 2 1 は、かかる命令を受けて、制御化機器 1 2 5 に対する給電を停止する（ステップ S 3 1 8 9）。

【 0 6 7 6 】

その一方で、電力管理装置 1 1 のシステム管理部 1 1 2 5 は、ユーザに対して警告を発するとともに（ステップ S 3 1 9 1）、リポークリストの更新を行う（ステップ S 3 1 9 3）。その後、電力管理装置 1 1 は、該当する制御化機器 1 2 5 とのネットワークを切断する（ステップ S 3 1 9 5）。

【 0 6 7 7 】

なお、図 7 1 A では、解析サーバ 3 4 が排除すべきバッテリーを特定する処理を行う場合について図示しているが、電力管理装置 1 1 が特性予測値の算出機能を有している場合には、図 7 1 A のステップ S 3 1 7 7 ~ ステップ S 3 1 8 3 に換えて、図 7 1 C に示す処理を行っても良い。具体的には、電力管理装置 1 1 は、解析サーバ 3 4 に対して、特性値などの、特性予測値の算出に必要な情報を要求する（ステップ S 3 2 0 1）。解析サーバ 3 4 は、要請を受けると、特性予測値の算出に必要な情報を、電力管理装置 1 1 に送信する（ステップ S 3 2 0 3）。その後、電力管理装置 1 1 は、取得した情報を利用して、特性予測値を計算し（ステップ S 3 2 0 5）、結果を判定する（ステップ S 3 2 0 7）。このような処理を行うことで、電力管理装置 1 1 であっても排除すべきバッテリーを特定することができる。

【 0 6 7 8 】

続いて、図 7 2 を参照しながら、ケース 7 に該当するバッテリーを特定し、排除するための流れを説明する。ケース 7 に該当するバッテリーを特定するまでの処理は、図 7 1 A に示したステップ S 3 1 6 1 ~ ステップ S 3 1 8 3 までと同様である。ただし、ケース 7 に該当するバッテリーの場合には、判定結果は、以下のようになる。

【 0 6 7 9 】

10

20

30

40

50

(ケース7) D1に関する乖離具合：所定範囲外、D2に関する乖離具合：所定範囲内
【0680】

上述のような判定結果を取得した電力管理装置11は、異常に対応するための処理を行う(ステップS3211)。具体的には、電力管理装置11の機器管理部1121は、制御化機器125に対して、センサ確認命令及び確認頻度を増加させる命令を送信する(ステップS3213)。制御化機器125は、かかる命令を受けると、受けた命令を実施して、センサに計測を行うように要請する(ステップS3215)。その結果、センサは、警告に関するセンサ情報を出力することとなる(ステップS3217)。

【0681】

警告に関するセンサ情報を取得した電力管理装置11は、分電装置121に対して、異常が発生している制御化機器125への給電を停止するように命令する(ステップS3219)。分電装置121は、かかる命令を受けて、制御化機器125に対する給電を停止する(ステップS3221)。

【0682】

その一方で、電力管理装置11のシステム管理部1125は、ユーザに対して警告を発するとともに(ステップS3223)、リポークリストの更新を行う(ステップS3225)。その後、電力管理装置11は、該当する制御化機器125とのネットワークを切断する(ステップS3227)。

【0683】

以上、排除すべきバッテリーの特定方法及びバッテリーの排除方法の流れについて説明した。

【0684】

以上説明したような解析サーバ34の存在により、電力管理装置11への既存攻撃はもちろんのこと、未知の攻撃に対しても、防御を行うことが可能となる。本実施形態に係る解析サーバ34の取得データ検証部3005は、ヒューリスティック又は物理解析的な判定が可能な機能を有しており、問題が生じていない場合には、迅速な判断を実施可能である。

【0685】

また、取得データ検証部3005による検証結果を利用することで、正規のバッテリー、コピー品などの不正なバッテリー何れの場合にしても、これらから得られる物理情報又はデジタル情報と乖離が認められる機器を特定することができる。これにより、問題のあるバッテリーを、局所電力管理システム1から離脱させたり給電停止させたりすることが可能となる。バッテリーには各種安全対策が施されているが、それ自体でのコントロールが不可能な場合でも、本方法を介して安全を確保することが可能となる。

【0686】

<複数の電力管理装置が存在する場合の処理について>

続いて、図73～図75を参照しながら、局所電力管理システム1内に複数の電力管理装置11が存在している場合の処理を説明する。

【0687】

ここで、図73～図75を参照しながら、電力管理装置11の多重化について説明する。これまで述べてきた通り、電力管理装置11は、局所電力管理システム1の内部にある機器等の電力供給を統括的に管理している。そのため、電力管理装置11が故障したり、ソフトウェアをアップデートする際に停止したりすると、局所電力管理システム1の内部にある機器等が利用できなくなってしまう。こうした事態に備え、電力管理装置11を多重化の方が好ましい。しかしながら、電力管理装置11は、電力に関する情報を統括的に管理し、局所電力管理システム1内の各種機器等を制御している。そのため、複雑な管理及び制御を複数の電力管理装置11で安全かつ効率的に行うには工夫が求められる。そこで考案されたのが図73～図75に示す方法である。

【0688】

[制御動作]

まず、図73を参照しながら、多重化された電力管理装置11による機器等の制御方法について説明する。なお、複数の電力管理装置11による協調動作は、情報管理部112に含まれるシステム管理部1125の機能により実現される。

【0689】

図73に示すように、まず、システム管理部1125は、2台以上の電力管理装置11が動作しているか否かを確認する(S4001)。このとき、システム管理部1125は、局所通信部111の機能を利用し、他の電力管理装置11のシステム管理部1125に問い合わせた動作を確認する。2台以上の電力管理装置11が動作している場合、システム管理部1125は、処理をステップS4003に進める。一方、他の電力管理装置11が動作していない場合、システム管理部1125は、処理をステップS4009に進める。

10

【0690】

ステップS4001においてステップS4003に処理を進めた場合、システム管理部1125は、所定の電力管理装置11を親機に設定し、残りの電力管理装置11を子機に設定する(S4003)。例えば、優先的に親機に設定される順番が予め決められており、最も優先順位の高い電力管理装置11が親機に設定される。なお、ここで言う「親機」「子機」は、電力管理装置11の属性を意味する。属性が設定されると、子機の属性を持つ電力管理装置11は、機器等を制御する場合に、親機の属性を持つ電力管理装置11に制御信号を送信する(S4005)。

【0691】

複数の子機から親機へと制御信号が送信された場合、親機のシステム管理部1125は、多数決、又は親機の判断(所定の条件又はランダム)で、機器等に送信する制御信号を決定する(S4007)。制御信号を決定すると、制御部115は、システム管理部1125により決定された制御信号を機器等に送信し、その機器等に制御信号の処理を実行させ(S4011)、一連の処理を終了する。一方、ステップS4001においてステップS4009に処理を進めた場合、自身の制御信号を機器等に送信し、その機器等に制御信号の処理を実行させ(S4009)、一連の処理を終了する。

20

【0692】

このように、システム管理部1125は、各電力管理装置11の属性を設定する機能、及び制御信号を選択する機能を有する。システム管理部1125がこのような機能を有することによって効率的な機器等の制御が可能になる。また、一部の電力管理装置11が故障やアップデートで停止しても、他の電力管理装置11により電力管理が継続され、機器等が利用不能になってしまう事態を回避することができる。

30

【0693】

[アップデート時の動作]

次に、図74、図75を参照しながら、電力管理装置11の基本的な動作を規定するソフトウェア(ファームウェア)のアップデート方法について説明する。なお、ファームウェアのアップデート処理は、システム管理部1125の機能により実現される。また、局所電力管理システム1内でN台の電力管理装置11が動作しているものとする。

【0694】

図74に示すように、まず、システム管理部1125は、2台以上の電力管理装置11が動作しているか否かを確認する(S4021)。2台以上の電力管理装置11が動作している場合、システム管理部1125は、処理をステップS4023に進める。一方、他の電力管理装置11が動作していない場合、システム管理部1125は、アップデートに係る一連の処理を終了する。

40

【0695】

ステップS4023に処理を進めた場合、システム管理部1125は、第1番目にアップデートする電力管理装置11を協調動作から切り離し、アップデートを実行する(S4023)。このとき、協調動作から切り離された電力管理装置11のシステム管理部1125は、システム管理サーバ33から最新のファームウェアを取得し、古いファームウェア

50

アを最新のファームウェアに更新する。ファームウェアの更新が完了した後、協調動作している残りの電力管理装置 11 は、アップデートが完了した電力管理装置 11 の動作を確認する (S 4 0 2 5、S 4 0 2 7)。

【 0 6 9 6 】

アップデートした電力管理装置 11 が正常に動作している場合、処理は、ステップ S 4 0 2 9 に進行する。一方、アップデートした電力管理装置 11 が正常に動作していない場合、処理は、ステップ S 4 0 3 1 に進行する。処理がステップ S 4 0 2 9 に進行した場合、アップデートした電力管理装置 11 を含む複数の電力管理装置 11 のシステム管理部 11 2 5 は、アップデートした電力管理装置 11 を協調動作に復帰させ (S 4 0 2 9)、アップデートの対象とする電力管理装置 11 を変更する。このとき、N 台全ての電力管理装置 11 に対するアップデートが完了しているか確認し (S 4 0 3 3)、N 台のアップデートが完了している場合にはアップデートの処理を終了する。

10

【 0 6 9 7 】

一方、N 台全ての電力管理装置 11 に対するアップデートが完了していない場合には、処理がステップ S 4 0 2 3 に戻り、第 2 番目にアップデートする電力管理装置 11 に対してアップデートの処理が実行される。このように、N 台全ての電力管理装置 11 のアップデートが完了するまで、ステップ S 4 0 2 3 ~ S 4 0 2 9 の処理が繰り返し実行される。ただし、ステップ S 4 0 2 7 において処理がステップ S 4 0 3 1 に進行した場合、アップデートの中止処理が実行され (S 4 0 3 1)、アップデートに係る一連の処理が終了する。

20

【 0 6 9 8 】

ここで、図 7 5 を参照しながら、アップデートの中止処理について説明する。

図 7 5 に示すように、アップデートの中止処理が開始されると、アップデートした電力管理装置 11 のシステム管理部 11 2 5 は、アップデートした電力管理装置 11 のファームウェアをアップデート前の状態に戻す (S 4 0 4 1)。次いで、協調動作している残りの電力管理装置 11 のシステム管理部 11 2 5 は、アップデート前に戻した電力管理装置 11 が正常に動作しているか否かを確認する (S 4 0 4 3、S 4 0 4 5)。

【 0 6 9 9 】

アップデート前の状態に戻した電力管理装置 11 が正常に動作している場合、処理は、ステップ S 4 0 4 7 に進む。一方、アップデート前の状態に戻した電力管理装置 11 が正常に動作していない場合、そのままアップデートの中止処理は終了する。処理がステップ S 4 0 4 7 に進んだ場合、アップデート前に戻した電力管理装置 11 を含む複数の電力管理装置 11 のシステム管理部 11 2 5 は、アップデート前に戻した電力管理装置 11 を協調動作に復帰させ (S 4 0 4 7)、アップデートの中止処理を終了する。

30

【 0 7 0 0 】

このように、アップデートする際には、アップデート対象の電力管理装置 11 を協調動作から切り離し、アップデート後の正常動作が確認された場合に協調動作に戻す処理が行われる。また、アップデートが失敗した場合にも、アップデート前の状態に戻した後で正常動作を確認し、正常動作が確認された場合に協調動作に戻す処理が行われる。このような構成にすることにより、協調動作をしている電力管理装置 11 にアップデートの影響が及ばずに済み、安全な電力管理装置 11 の運用が担保される。

40

【 0 7 0 1 】

(第 2 実施形態)

< 第 2 実施形態の概要について >

局所電力管理システムは、エコ社会への移行の一つの現れであるが、現在のところ、導入には手間がかかるため、広く普及しているとは言い難い状況である。このような中、システム導入と使用に魅力的な要素を付加することは、システムを積極的に導入させ、エコ社会を実現するうえで重要である。かかる魅力的な要素の一つとして、局所電力管理システムに連動するエンタテインメント (例えば、ゲーム等) を挙げることができる。

【 0 7 0 2 】

50

現在流通しているゲームの多くは、フィクションである。歴史に関するものやスポーツ等のゲームの一部には、実在の人名・地名などの要素を取り入れたり、実際の動きをゲーム映像に描写したりしたものもあるが、ゲームそのものが実社会や実生活とリンクしているわけではない。そこで、以下で説明する本発明の第2の実施形態では、ゲームの内容そのものが、個別の局所電力管理システム（例えば、家庭内のシステム）のエコ化に繋がるようストーリー化された、実社会リンク型ゲームを提案する。

【0703】

また、従来ของเกมによりもたらされるものは、得点、入手したアイテム、ステージクリアによる満足感・達成感、話題といった無形のものであった。しかしながら、以下で説明するシステム連動エンタテインメントは、ゲームによる効果的な対応が、実際の局所電力管理システムに連動可能である。これにより、本実施形態に係るシステム連動エンタテインメントは、実際の電力制御、電気量低下、CO₂削減値への寄与、売電等といった実利に繋がる要素を含み、同時に、実際の知識を得ることができるという有形の結果を得ることができる。

【0704】

以上からもわかる通り、以下で説明するシステム連動エンタテインメントにより、ユーザは、楽しみながら電力削減等のエコ活動を行うことができる。

なお、本実施形態は、局所電力管理システムへの適用を示したものであるが、有形結果を有する実社会リンク型のゲームに展開することが可能である。

【0705】

このシステム連動エンタテインメントは、電力管理装置11のサービス提供部118が、電力管理装置11の各処理部及び局所電力管理システム1の外部に存在するサービス提供サーバ31（ゲームサービス提供サーバ）と連携しながら動作することで実現される。また、ユーザは、電力管理装置11に接続可能な制御化機器125を操作することで、ゲームに代表されるシステム連動エンタテインメントを楽しむことができる。

【0706】

<サービス提供部の構成について>

まず、図76及び図77を参照しながら、電力管理装置11のサービス提供部118の構成について説明する。図76及び図77は、電力管理装置のサービス提供部の構成を説明するためのブロック図である。

【0707】

なお、本実施形態に係る電力管理装置11は、本発明の第1の実施形態に係る電力管理装置11が有する処理部を備えており、第1の実施形態に係る電力管理装置11が実現可能な機能を同様に実現できるものとする。

【0708】

サービス提供部118は、例えば、CPU、ROM、RAM等により実現される。サービス提供部118は、図76に示したように、ゲームサービス提供部1181と、他のサービスの提供部1182と、を更に備える。

【0709】

ゲームサービス提供部1181は、例えば、CPU、ROM、RAM等により実現される。ゲームサービス提供部1181は、ゲーム制御部1701と、パーツライブラリ1707と、コンテンツライブラリ1709と、を更に備える。

【0710】

ゲーム制御部1701は、例えば、CPU、ROM、RAM等により実現される。ゲーム制御部1701は、パーツライブラリ1707やゲームサービス提供サーバ31と連携しながら、ゲームの物語背景及びステージなどのゲームの基本設定を行う処理部である。また、コンテンツライブラリ1709やゲームサービス提供サーバ31に格納されているゲームプログラムの実行中は、ゲームプログラムの実行制御を行って、ゲームの進行を制御する。このゲーム制御部1701は、更に、現実世界構築部1703と、仮想世界構築部1705とを更に備える。

【 0 7 1 1 】

現実世界構築部 1 7 0 3 は、例えば、CPU、ROM、RAM等により実現される。現実世界構築部 1 7 0 3 は、電力管理装置 1 1 の記憶部 1 1 3 等に格納されているデータベースを参照しながら、実際の局所電力管理システム 1 の情報を取り入れた、現実世界を構築する。

【 0 7 1 2 】

仮想世界構築部 1 7 0 5 は、例えば、CPU、ROM、RAM等により実現される。仮想世界構築部 1 7 0 5 は、コンテンツプログラムに予め用意された仮想世界を構築する。

【 0 7 1 3 】

ゲーム制御部 1 7 0 1 は、この現実世界構築部 1 7 0 3 及び仮想世界構築部 1 7 0 7 と互いに連携しながら、システム連動エンタテインメントを実現する。

10

【 0 7 1 4 】

また、ゲーム制御部 1 7 0 1 は、電力管理装置 1 1 が有するデータベースにアクセス可能であり、また、電力管理装置 1 1 の制御実行パスを有している。

【 0 7 1 5 】

また、ゲーム制御部 1 7 0 1 が制御するゲームは、他の局所電力管理システム 1 のメンバーをキャラクターに含め、対戦を行ったり、ロールプレイングゲームのメンバーとしてゲームを遠隔操作したりすることで楽しむ事ができる。なお、他のシステムのメンバーの参加を許容する場合には、かかる他のシステムのメンバーが、本システム 1 における現実世界にはアクセスできないようにすることが好ましい。

20

【 0 7 1 6 】

パーツライブラリ 1 7 0 7 は、ゲームサービス提供部 1 1 8 1 が備えるデータベースの一つである。パーツライブラリ 1 7 0 7 には、ゲームコンテンツに登場する仮想家具、仮想機器、登場人物などのパーツや、ゲーム中に登場するアイテム等に関する情報が記録されている。なお、このパーツライブラリ 1 7 0 7 は、ゲームサービス提供サーバ 3 1 に存在していてもよい。

【 0 7 1 7 】

コンテンツライブラリ 1 7 0 9 は、ゲームサービス提供部 1 1 8 1 が備えるデータベースの一つである。コンテンツライブラリ 1 7 0 9 には、電力管理装置 1 1 が実行可能なゲームコンテンツの実体プログラムが各種格納されている。

30

【 0 7 1 8 】

図 7 7 には、コンテンツライブラリ 1 7 0 9 に格納されているゲームコンテンツの一例が図示されている。以下に、具体的なゲームコンテンツの一例を、簡単に説明する。

【 0 7 1 9 】

お部屋の模様替え（現実世界のゲーム）

現在の部屋の配置状態から、家具や家電などの配置替え、カーテン・絨毯のコーディネート、新しい家具や家電の購入を行い、色彩・バランス感覚などのコーディネート技術を競うなどのコンセプトを有するゲームである。配置換えの結果、家電の総電力量がどう変化するか、又は、新たな家電製品を買って配置した場合に、どのような電力量になるかを把握することができる。この場合、メーカー、デザイン、消費電力量など、現実属性をもつアイテムの表示が可能なライブラリが準備されている。これらのライブラリは、ゲームサービス提供サーバ 3 1 に格納されているものであってもよい。また、現実世界にリンクした改善ができたものについては、結果適用モード（ゲーム結果を現実のシステムに適用するモード）の実施が可能となる。

40

【 0 7 2 0 】

電気食い虫を撃退せよ（現実世界 + 仮想世界のゲーム）

現在の部屋での電力使用状況を表示し、不必要な電気を切る。また、ライトや音量などを調整する事で、いかに電力が削減されるかを競ったり、売電で利益を得たりする。また、電気をつけて回る”虫”が出てくる仮想世界で、いかに有効にそれを撃退するかを競うコンセプトを有するゲームである。前者については、結果適用モードの実施が可能となる

50

。

【0721】

究極生活冒険隊（現実世界＋仮想世界のゲーム）

現在の家庭にある家電を用いて、究極の低消費生活を目指すステージと、仮想家庭にある家電を用いて究極の生活を目指すステージからなる。

【0722】

地球を救え！緑増大計画（仮想世界のゲーム）

地球のCO₂排出による温暖化危機をどう乗り切るかをコンセプトとするゲームである。ある国の環境大臣になったことを仮定し、国内の世論をまとめ、諸外国と交渉しながらステージを進んでいく。現実的な数字や状況を使って、環境に関する高度な学習も可能な知能ゲームである。

10

【0723】

ロールプレイングゲーム（現実世界＋仮想世界のゲーム）

1Fのみを現実世界とリンクしたステージとし、他のステージはそれに合う形で仮想的な環境（例えば、庭、倉庫、開かずの間等）が提供され、この物語を進んでいくというゲームである。現実世界のステージにおいて、電力状況に反映可能な結果は、結果適用モードの実施が可能である。

【0724】

<データベースとの連携について>

続いて、図78を参照しながら、現実の局所電力管理システム1の状況を表す各種情報が格納された、電力管理装置11が有するデータベースとの連携について説明する。図78は、電力管理装置が有するデータベースとの連携について説明するための説明図である。

20

。

【0725】

電力管理装置11が保持するデータベースには、例えば以下のようなデータが格納されている。

【0726】

- 制御化機器、電動移動体、発電装置、蓄電装置、各機器のバッテリー、制御化端子、端子拡張装置等の機器情報
- 上記装置に関する電力情報（使用／蓄電状況）、位置情報
- 登録ユーザ及びアクセス権限
- 電力課金情報及び口座情報
- 時間、天気、気温

30

【0727】

これらのデータを利用して、ゲーム制御部1701は、現実世界をゲームの中に実現させる。

【0728】

現実世界構築部1703は、これらの機器を配置することにより、ゲームステージの大体の間取りを想定可能である。例えば、冷蔵庫などがあればダイニングエリア、パソコンやスタンドがあれば個人部屋エリア、洗濯機があれば風呂場／洗面所エリア、電動移動体があれば車庫エリア、ライトがあれば廊下など、適宜間取りを想定することができる。現実世界構築部1703は、このような想定を基に間取りを決定し、パーツライブラリ1707から、機器を表すアイテムや家具などを配置する。

40

【0729】

また、現実世界構築部1703は、登録ユーザ情報に基づいて、ゲームの登場人物（キャラクター）を決定する。現実世界では、実際の機器とアイテムの属性はリンクされており、それを表示したり、結果適用モードにおいて電源をOFFにしたりするなどのことが可能となる。したがって、ユーザによって、表示画面等に配置されている各種機器のアイコン等のオブジェクトが選択された場合には、選択された機器の機器情報や電力情報など、データベースに記載されている各種の情報が表示される。

50

【0730】

また、現実世界のみである場合には、ゲームステージが限定的となってしまうため、仮想世界構築部1703は、現実世界に基づいて設定されたゲームステージに、予めゲームコンテンツ上に設定された仮想世界を付加し、ゲームステージ（物語背景）を構成する。

【0731】

図78では、現実世界をディスプレイの表示領域に表示した際の状態を示している。ユーザはメインキャラクターを操作しながら、ステージでゲームを楽しむことが可能である。

【0732】

<システム連動エンタテインメントのセキュリティについて>

続いて、図79を参照しながら、システム連動エンタテインメントのセキュリティについて説明する。図79は、システム連動エンタテインメントのセキュリティについて説明するための説明図である。

10

【0733】

本ゲームを実行するシステムにおいて、セキュリティとしては大きく以下の三点に気をつけることが好ましい。

【0734】

(1) 電力管理装置上のゲームが受け入れた匿名の第三者の参加又はその接続を利用した悪意ある第三者からの攻撃で、電力管理装置がダウンする、結果適用モードの制御権を奪われる、電力管理装置上の機密情報が漏洩するなどのリスクがある。

(2) 電力管理装置上のゲームが、悪意ある第三者の機器から実行されて、有害な実行が実施される。

20

(3) 電力管理装置と売電に関するサービス提供サーバ（売電管理サーバ）との間の機密情報（口座・課金情報等）が漏洩する。

【0735】

[セキュリティリスク1について]

まず、電力管理装置上のゲームが受け入れた匿名の第三者の参加については、このような第三者が参加する場合には、本ゲームは仮想世界のみで構成されたものに限定するよう作り込み、電力管理装置上の機密情報のゲーム上からの漏洩を防ぐ。

【0736】

次に、悪意ある第三者からの攻撃に関しては、電力管理装置の制御を自由にさせないようにする必要がある。そのため、電力管理装置にウイルス排除ソフトを入れるなどで、第三者からの攻撃を検知したり排除したりする。また、電力管理装置の乗っ取りを防ぐ電子透かしを利用したり、解析サーバ34を利用して、実行履歴から不審な繰り返し攻撃等を検知して実行を阻止したり接続を切ったりする攻撃を防御する。

30

【0737】

[セキュリティリスク2について]

機器とプレイヤーが、本ゲームをプレイすることが可能な正当なメンバーかを確認する。また、たとえ正規メンバーであったとしても、売電などの行為を子供が行うことは好ましくないため、ゲーム自体のアクセスをレベル分けして、そのアクセス権があるか、結果適用モードを実施できるかを設定する。また、他人のプレイを許可した場合は、現実世界情報を用いた物語にしないよう制御する。

40

【0738】

従って、電力管理装置には予め機器と利用者を設定し、アクセスレベルを付与して、機器とユーザの2つの認証を実施する。認証は、第1の実施形態に示した公開鍵もしくは共通鍵又はその両方を用いた方法と同じスキームを利用することができる。また、ゲーム中は、所定の間隔で認証を実施するような仕組みを導入することが好ましい。また、データベースは、アクセス権のない利用者の使用中はアクセスできないようにすることが好ましい。

【0739】

[セキュリティリスク3について]

50

本ゲーム関わらず、売電時に守るべきセキュリティとして構築されていることが好ましい。この点については、局所電力管理システム1のインターネットを介したサービスの認証が機能していれば問題ないとする。

【0740】

<システム連動エンタテインメントの流れについて>

続いて、図80～図81Bを参照しながら、本実施形態に係る電力管理装置が提供するシステム連動エンタテインメントの流れを説明する。図80～図81Bは、システム連動エンタテインメントの流れを説明するための流れ図である。なお、図80～図81Bでは、システム連動エンタテインメントの一例としてゲームを取り上げ、説明を行っている。

【0741】

なお、以下の説明に先立ち、局所電力管理システム1と連動したゲームをプレイしようとするユーザは、電力管理装置11に接続可能であり、表示画面を有するディスプレイ端末（例えば、テレビなどの各種ディスプレイ機器又は携帯電話、携帯ゲーム機等のポータブル機器）を操作して、ゲームをプレイするものとする。また、ゲームをプレイするためにユーザが使用する機器は、電力管理装置11そのものであってもよい。

【0742】

まず、図80を参照しながら、大まかな流れについて説明する。

【0743】

まず、ユーザは、ディスプレイ端末125の電源を投入して、端末そのものを起動させる（ステップS5001）。また、ユーザは、端末が起動すると、ゲームを起動するためのアイコン等のオブジェクトを選択して、ゲームの起動を電力管理装置11に要請する。

【0744】

要請を受けた電力管理装置11は、ゲームの起動を要請したディスプレイ端末が、自身が管理している管理機器であるか否かを判断するために、ディスプレイ端末を認証する処理を実施する（ステップS5003）。また、図81A及び図81Bにて詳細に説明するように、ディスプレイ端末が管理機器であるか否かに応じて、ユーザに提供するゲームの機能が異なってくるため、電力管理装置11は、設定情報を確認して（ステップS5005）、提供可能な機能を確認する。その後、電力管理装置11は、ゲームプログラムを起動して（ステップS5007）、ディスプレイ端末に必要なデータ類を送信する。

【0745】

ディスプレイ端末125は、電力管理装置11から送信されたデータ類を受信して、自身の表示画面にゲームの初期画面を表示する（ステップS5009）。ユーザは、初期画面に表示されている、ゲームを表すアイコン等のオブジェクトを選択して（ステップS5011）、プレイを希望するゲームコンテンツを特定する。ここで、表示画面に表示されるゲームは、コンテンツライブラリ1709等に格納されているゲームのうち、ユーザに実行が許可されているものである。

【0746】

ユーザは、ディスプレイ端末125の入力装置（マウス、キーボード、タッチパネル等）を操作して、ゲームを開始する（ステップS5013）。また、電力管理装置11は、ディスプレイ端末でのゲームの進行とあわせて、個別データをロードしたり、データの準備をしたり、ゲーム内容の保存を行ったりする（ステップS5015）。

【0747】

また、ユーザは、ゲーム中の任意の時点で、ゲーム結果を実際のシステムに適用する結果適用モードの開始を要請する場合がある（ステップS5017）。要請を受けた電力管理装置11は、結果適用モードの開始要請を行ったユーザによる結果適用モードの実行が可能か否かを、確認する（ステップS5019）。電力管理装置11は、設定情報等を確認して、ユーザのアクセス権や実行権を確認して、実行リスクを確認した（ステップS5020）後、結果適用モードのうち実行可能な範囲を、ディスプレイ端末に提示する（ステップS5021）。

【0748】

10

20

30

40

50

ディスプレイ端末では、電力管理装置 1 1 から提示された内容を表示画面に表示し、実行内容の選択をユーザにしてもらう(ステップ S 5 0 2 3)。ディスプレイ端末は、ユーザの選択内容を、電力管理装置 1 1 に通知する。

【 0 7 4 9 】

電力管理装置 1 1 は、ユーザによる選択結果に応じて、分電装置に選択結果に応じた実行指示を発令する(ステップ S 5 0 2 5)。また、電力管理装置 1 1 は、ログ情報の更新を行って(ステップ S 5 0 2 7)、結果適用モードの実行が終了した旨を通知する(ステップ S 5 0 2 9)。

【 0 7 5 0 】

続いて、図 8 1 A 及び図 8 1 B を参照しながら、システム連動エンタテインメントの詳細な流れを説明する。

10

【 0 7 5 1 】

先に説明したように、ユーザは、ゲームを実行する機器を操作して、ゲームを起動させるが、電力管理装置 1 1 のゲームサービス提供部 1 1 8 1 は、ゲームの開始要請がディスプレイ端末から送信されたか否かを、待ち受けている(ステップ S 5 0 3 1)。

【 0 7 5 2 】

ゲーム開始要請がディスプレイ端末から送信されると、電力管理装置 1 1 は、ゲームの開始要請のあったディスプレイ端末の機器認証を実施する(ステップ S 5 0 3 3)。これにより、電力管理装置 1 1 は、ゲーム開始を要請したディスプレイ端末が、自身の管理している管理機器であるか否かを確認することができる(ステップ S 5 0 3 5)。

20

【 0 7 5 3 】

電力管理装置 1 1 のゲームサービス提供部 1 1 8 1 は、ディスプレイ端末が管理機器ではない場合には、電力管理装置 1 1 のユーザに、ゲーム開始を許可するか否かを確認し(ステップ S 5 0 3 7)、電力管理装置 1 1 のユーザが実行を許可しないのであれば、処理を終了する。また、電力管理装置 1 1 のユーザが実行を許可した場合には、電力管理装置 1 1 のゲームサービス提供部 1 1 8 1 は、後述するステップ S 5 0 3 9 を実施する。

【 0 7 5 4 】

他方、ディスプレイ端末が管理機器であった場合、又は、管理機器ではないものの電力管理装置 1 1 のユーザから実行許可が得られた場合には、電力管理装置 1 1 のゲームサービス提供部 1 1 8 1 は、ユーザ認証を実施する(ステップ S 5 0 3 9)。

30

【 0 7 5 5 】

電力管理装置 1 1 のゲームサービス提供部 1 1 8 1 は、ユーザが、電力管理装置 1 1 に登録されたメンバーであることが確認できたら、その制御権のレベルから、ゲームのアクセスレベルと、結果適用モード時の制御レベルを設定する(ステップ S 5 0 4 1)。

【 0 7 5 6 】

続いて、電力管理装置 1 1 のゲームサービス提供部 1 1 8 1 は、ゲームのメインプログラムを起動し(ステップ S 5 0 4 3)、ユーザの使用するディスプレイ端末に、ゲームの初期画面を表示させる。

【 0 7 5 7 】

ディスプレイ端末のユーザは、遊びたいゲームコンテンツを選択すると、その選択結果が電力管理装置 1 1 に送信され、電力管理装置 1 1 のゲームサービス提供部 1 1 8 1 は、選択されたゲームコンテンツを特定することができる(ステップ S 5 0 4 5)。

40

【 0 7 5 8 】

電力管理装置 1 1 のゲームサービス提供部 1 1 8 1 は、特定したコンテンツが、ディスプレイ端末のユーザにアクセス可能か及び結果適用モードを実施できるかを確認する(ステップ S 5 0 4 7)。

【 0 7 5 9 】

ゲームユーザにアクセス権がない場合又は結果適用モードを実施する権限がない場合、電力管理装置 1 1 のゲームサービス提供部 1 1 8 1 は、ゲームの起動中、データベースへのアクセス及び結果適用モードが行えないように設定する(ステップ S 5 0 4 9)。

50

【0760】

また、ゲームユーザにアクセス権があり結果適用モードが実施できる場合、電力管理装置11は、データベースにアクセスして、管理機器の機器情報及び電力情報を収集する(ステップS5051)。

【0761】

ゲームサービス提供部1181のゲーム制御部1701は、ステップS5051にて収集した各種情報を用いて、ゲームの物語の背景などの基本設定を構築する(ステップS5053)。基本設定の構築が終了すると、ゲーム制御部1701は、設定された物語背景をもとに、選択されたゲームコンテンツの実行制御を行う(ステップS5055)。この間、電力管理装置11とディスプレイ端末とはインタラクティブに通信し、電力管理装置11は、ゲーム画面を端末のディスプレイに表示させ、ディスプレイ端末からはユーザの入力情報が送信される。また、この間、電力管理装置11のゲーム制御部1701は、ゲームの終了/中断等を要請する処理がなされたか否かを判断している(ステップS5057)。

10

【0762】

ユーザにより、ゲーム終了/中断などのステータスが選択されると、電力管理装置10のゲームサービス提供部1181は、結果適用モードの起動が可能なコンテンツであれば、ユーザに結果提要モードに移行するかを確認する(ステップS5059)。

【0763】

結果適用モードに移行しない旨の選択がなされた場合には、電力管理装置11のゲームサービス提供部1181は、ゲーム内容を保存するかどうかを確認した後に、ゲームプログラムを終了する。

20

【0764】

また、結果適用モードに移行する場合には、電力管理装置11のゲームサービス提供部1181は、ユーザに結果適用モードの実施権があるかを確認する(ステップS5061)。ユーザに結果適用モードの実施権がない場合には、電力管理装置11のゲームサービス提供部1181は、ゲームプログラムを終了する。

【0765】

また、ユーザに結果適用モードの実施権がある場合、電力管理装置11のゲームサービス提供部1181は、起動後からこれまでにプレイした内容に基づいて、実際に機器に実施できる制御を抽出し(ステップS5063)、リストをユーザに表示する。

30

【0766】

また、電力管理装置11のゲームサービス提供部1181は、リストを表示する前に、リスク確認を実施することが好ましい。具体的には、解析サーバ34に問い合わせを行い、制御可能内容とその履歴から不審な制御でないかを確認し、不審な制御に関しては、上記抽出リストより制御内容を削除する。これにより、サイバー攻撃等に関するリスクのほか、常時接続が望ましい機器(例えば、冷蔵庫などの家電製品)等の電源を切るような命令については、そのリスクを確認することが可能となる。

【0767】

ゲームのユーザは、ディスプレイ端末の表示画面に表示されたリストから、「機器Aのswitch off」などといった実施したい項目を選択する。この選択結果は、電力管理装置11に送信され、電力管理装置11は、事項内容を特定することができる(ステップS5065)。

40

【0768】

その後、電力管理装置11は、ユーザによる選択結果に応じて、分電装置121、制御化端子123、制御化機器125等に選択結果に応じた実行指示を発令する(ステップS5067)。また、電力管理装置11は、ログ情報の更新を行って(ステップS5069)、全ての制御を実施したかを確認する(ステップS5071)。

【0769】

電力管理装置11は、命令対象機器から実行終了を受け、全ての制御が実施されたら、

50

ユーザに終了表示を行う(ステップS5073)。電力管理装置11は、ゲームを終了するか継続するかを確認し(ステップS5075)、継続する場合は、ステップS5055に戻る。また、終了の場合、電力管理装置11は、ゲームを終了させる。

【0770】

このような流れで処理を行うことにより、電力管理装置は、局所電力管理システムに連動したゲーム等のエンタテインメントをユーザに提供することが可能となる。その結果、システム連動エンタテインメントは、局所電力管理システムの魅力あるアプリケーションとして、電力量やCO₂削減に実際に寄与することが可能となる。

【0771】

(ハードウェア構成について)

次に、図82を参照しながら、本発明の実施形態に係る電力管理装置11のハードウェア構成について、詳細に説明する。図82は、本発明の実施形態に係る電力管理装置11のハードウェア構成を説明するためのブロック図である。

【0772】

電力管理装置11は、主に、CPU901と、ROM903と、RAM905と、を備える。また、電力管理装置11は、更に、ホストバス907と、ブリッジ909と、外部バス911と、インターフェース913と、入力装置915と、出力装置917と、ストレージ装置919と、ドライブ921と、接続ポート923と、通信装置925とを備える。

【0773】

CPU901は、演算処理装置および制御装置として機能し、ROM903、RAM905、ストレージ装置919、またはリムーバブル記録媒体927に記録された各種プログラムに従って、電力管理装置11内の動作全般またはその一部を制御する。ROM903は、CPU901が使用するプログラムや演算パラメータ等を記憶する。RAM905は、CPU901の実行において使用するプログラムや、その実行において適宜変化するパラメータ等を一次記憶する。これらはCPUバス等の内部バスにより構成されるホストバス907により相互に接続されている。

【0774】

ホストバス907は、ブリッジ909を介して、PCI(Peripheral Component Interconnect/Interface)バスなどの外部バス911に接続されている。

【0775】

入力装置915は、例えば、マウス、キーボード、タッチパネル、ボタン、スイッチおよびレバーなどユーザが操作する操作手段である。また、入力装置915は、例えば、赤外線やその他の電波を利用したリモートコントロール手段(いわゆる、リモコン)であってもよいし、電力管理装置11の操作に対応した携帯電話やPDA等の外部接続機器929であってもよい。さらに、入力装置915は、例えば、上記の操作手段を用いてユーザにより入力された情報に基づいて入力信号を生成し、CPU901に出力する入力制御回路などから構成されている。電力管理装置11のユーザは、この入力装置915を操作することにより、電力管理装置11に対して各種のデータを入力したり処理動作を指示したりすることができる。

【0776】

出力装置917は、取得した情報をユーザに対して視覚的または聴覚的に通知することが可能な装置で構成される。このような装置として、CRTディスプレイ装置、液晶ディスプレイ装置、プラズマディスプレイ装置、ELディスプレイ装置およびランプなどの表示装置や、スピーカおよびヘッドホンなどの音声出力装置や、プリンタ装置、携帯電話、ファクシミリなどがある。出力装置917は、例えば、電力管理装置11が行った各種処理により得られた結果を出力する。具体的には、表示装置は、電力管理装置11が行った各種処理により得られた結果を、テキストまたはイメージで表示する。他方、音声出力装置は、再生された音声データや音響データ等からなるオーディオ信号をアナログ信号に変

10

20

30

40

50

換して出力する。

【0777】

ストレージ装置919は、電力管理装置11の記憶部の一例として構成されたデータ格納用の装置である。ストレージ装置919は、例えば、HDD(Hard Disk Drive)等の磁気記憶部デバイス、半導体記憶デバイス、光記憶デバイス、または光磁気記憶デバイス等により構成される。このストレージ装置919は、CPU901が実行するプログラムや各種データ、および外部から取得した各種のデータなどを格納する。

【0778】

ドライブ921は、記録媒体用リーダライタであり、電力管理装置11に内蔵、或いは外付けされる。ドライブ921は、装着されている磁気ディスク、光ディスク、光磁気ディスク、または半導体メモリ等のリムーバブル記録媒体927に記録されている情報を読み出して、RAM905に出力する。また、ドライブ921は、装着されている磁気ディスク、光ディスク、光磁気ディスク、または半導体メモリ等のリムーバブル記録媒体927に記録を書き込むことも可能である。リムーバブル記録媒体927は、例えば、DVDメディア、HD-DVDメディア、Blu-rayメディア等である。また、リムーバブル記録媒体927は、コンパクトフラッシュ(登録商標)(CompactFlash:CF)、フラッシュメモリ、または、SDメモ리카ード(Secure Digital memory card)等であってもよい。また、リムーバブル記録媒体927は、例えば、非接触型ICチップを搭載したICカード(Integrated Circuit card)または電子機器等であってもよい。

【0779】

接続ポート923は、機器を電力管理装置11に直接接続するためのポートである。接続ポート923の一例として、USB(Universal Serial Bus)ポート、IEEE1394ポート、SCSI(Small Computer System Interface)ポート等がある。接続ポート923の別の例として、RS-232Cポート、光オーディオ端子、HDMI(High-Definition Multimedia Interface)ポート等がある。この接続ポート923に外部接続機器929を接続することで、電力管理装置11は、外部接続機器929から直接各種のデータを取得したり、外部接続機器929に各種のデータを提供したりする。

【0780】

通信装置925は、例えば、通信網931に接続するための通信デバイス等で構成された通信インターフェースである。通信装置925は、例えば、有線または無線LAN(Local Area Network)、Bluetooth(登録商標)、またはWUSB(Wireless USB)用の通信カード等である。また、通信装置925は、光通信用のルータ、ADSL(Asymmetric Digital Subscriber Line)用のルータ、または、各種通信用のモデム等であってもよい。この通信装置925は、例えば、インターネットや他の通信機器との間で、例えばTCP/IP等の所定のプロトコルに則して信号等を送受信することができる。また、通信装置925に接続される通信網931は、有線または無線によって接続されたネットワーク等により構成され、例えば、インターネット、家庭内LAN、赤外線通信、ラジオ波通信または衛星通信等であってもよい。

【0781】

以上、本発明の実施形態に係る電力管理装置11の機能を実現可能なハードウェア構成の一例を示した。上記の各構成要素は、汎用的な部材を用いて構成されていてもよいし、各構成要素の機能に特化したハードウェアにより構成されていてもよい。従って、本実施形態を実施する時々の技術レベルに応じて、適宜、利用するハードウェア構成を変更することが可能である。

【0782】

また、本発明の実施形態に係る制御化機器125及び解析サーバ34のハードウェア構成は、本発明の実施形態に係る電力管理装置11の構成と同様であるため、詳細な説明は

10

20

30

40

50

省略する。

【 0 7 8 3 】

以上、添付図面を参照しながら本発明の好適な実施形態について詳細に説明したが、本発明はかかる例に限定されない。本発明の属する技術の分野における通常の知識を有する者であれば、特許請求の範囲に記載された技術的思想の範疇内において、各種の変更例または修正例に想到し得ることは明らかであり、これらについても、当然に本発明の技術的範囲に属するものと了解される。

【符号の説明】

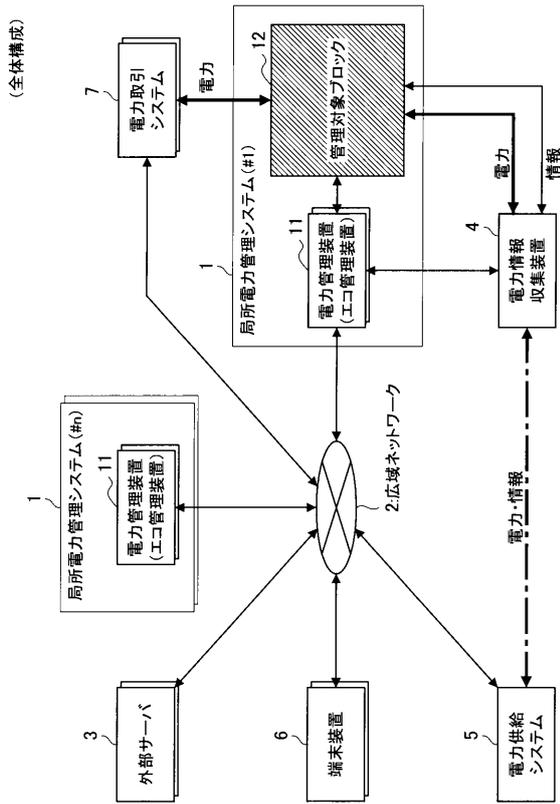
【 0 7 8 4 】

1	局所電力管理システム	10
1 1	電力管理装置	
1 1 1	局所通信部	
1 1 2	情報管理部	
1 1 2 1	機器管理部	
1 1 2 2	電力取引部	
1 1 2 3	情報分析部	
1 1 2 4	表示情報生成部	
1 1 2 5	システム管理部	
1 1 3	記憶部	
1 1 4	広域通信部	20
1 1 5	制御部	
1 1 6	表示部	
1 1 7	入力部	
1 1 8	サービス提供部	
1 1 8 1	ゲームサービス提供部	
1 2	管理対象ブロック	
1 2 1	分電装置	
1 2 2	A C / D C 変換器	
1 2 3	制御化端子	
1 2 4	電動移動体	30
1 2 5	制御化機器	
1 2 6	非制御化機器	
1 2 7	端子拡張装置	
1 2 8	蓄電装置	
1 2 9	第 1 発電装置	
1 3 0	第 2 発電装置	
1 3 1	環境センサ	
2	広域ネットワーク	
3	外部サーバ	
3 1	サービス提供サーバ	40
3 2	課金サーバ	
3 3	システム管理サーバ	
3 4	解析サーバ	
3 5	認証局サーバ	
3 6	製造者サーバ	
3 7	地図 D B サーバ	
4	電力情報収集装置	
5	電力供給者システム	
6	端末装置	
7	電力取引システム	50

1 5 0 1	鍵生成部	
1 5 0 3	システム登録部	
1 5 0 5	管理機器登録部	
1 5 0 7	管理機器情報取得部	
1 5 0 9	管理機器情報出力部	
1 5 1 1	排除機器特定部	
1 5 1 3	情報改ざん検知部	
1 5 5 1	管理機器認証部	
1 5 5 3	署名生成部	
1 5 5 5	署名検証部	10
1 5 6 1	埋め込み位置特定部	
1 5 6 3	電子透かし抽出部	
1 5 6 5	電子透かし検証部	
1 6 0 1	機器状態判定部	
1 6 0 3	電力状態判定部	
1 7 0 1	ゲーム制御部	
1 7 0 3	現実世界構築部	
1 7 0 5	仮想世界構築部	
1 7 0 7	パーツライブラリ	
1 7 0 9	コンテンツライブラリ	20
2 0 0 1	制御部	
2 0 0 3	センサ	
2 0 0 5	バッテリー	
2 0 0 7	機能提供部	
2 0 0 9	局所通信部	
2 0 1 1	入力部	
2 0 1 3	表示部	
2 0 1 5	記憶部	
2 0 2 1	認証処理部	
2 0 2 3	センサ制御部	30
2 0 2 5	センサ情報出力部	
2 0 2 7	バッテリー制御部	
2 0 2 9	バッテリー情報出力部	
2 0 3 1	改ざん検知情報生成部	
2 0 3 3	機器特徴情報生成部	
2 0 3 5	電子透かし生成部	
2 0 3 7	埋め込み位置決定部	
2 0 3 9	電子透かし埋め込み部	
3 0 0 1	広域通信部	
3 0 0 3	情報改ざん検知部	40
3 0 0 5	取得データ検証部	
3 0 0 7	取得データ検証制御部	
3 0 0 9	第1検証部	
3 0 1 1	第2検証部	
3 0 3 1	検証制御部	
3 0 3 3	動作判定部	
3 0 3 5	データベース管理部	
3 0 3 7	ウイルス定義ファイル管理部	
3 0 3 9	共有情報生成部	
3 0 4 1	電力管理装置データベース	50

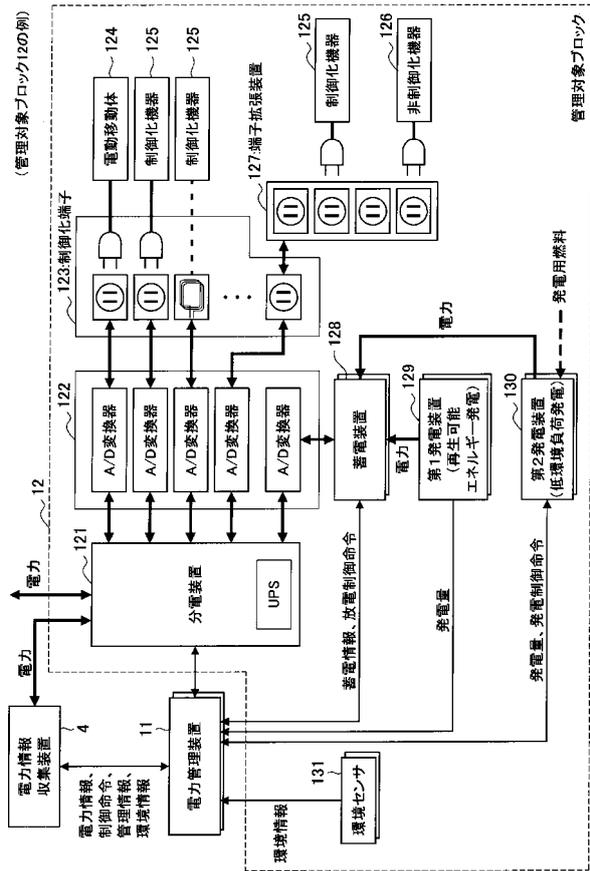
- 3 0 4 3 判定辞書
- 3 0 4 5 ウィルス定義ファイルデータベース
- 3 0 5 1 特性予測値算出部
- 3 0 5 3 データベース
- 3 0 5 5 データ判定部

【図1】



(全体構成)

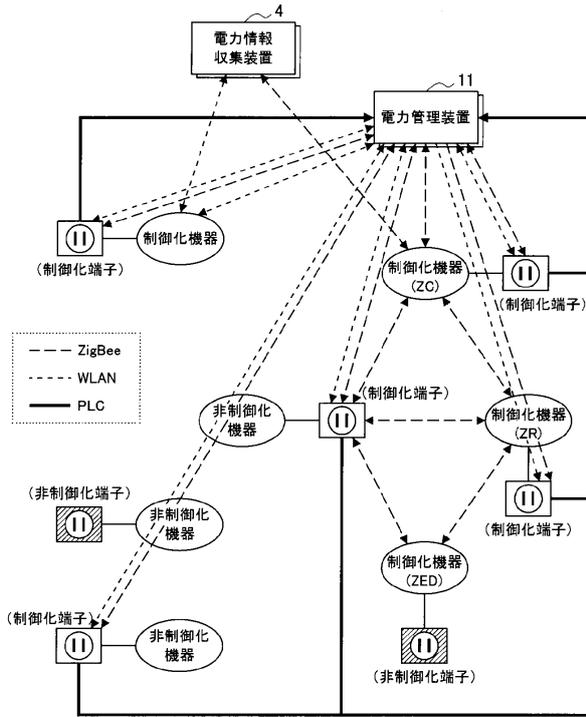
【図2】



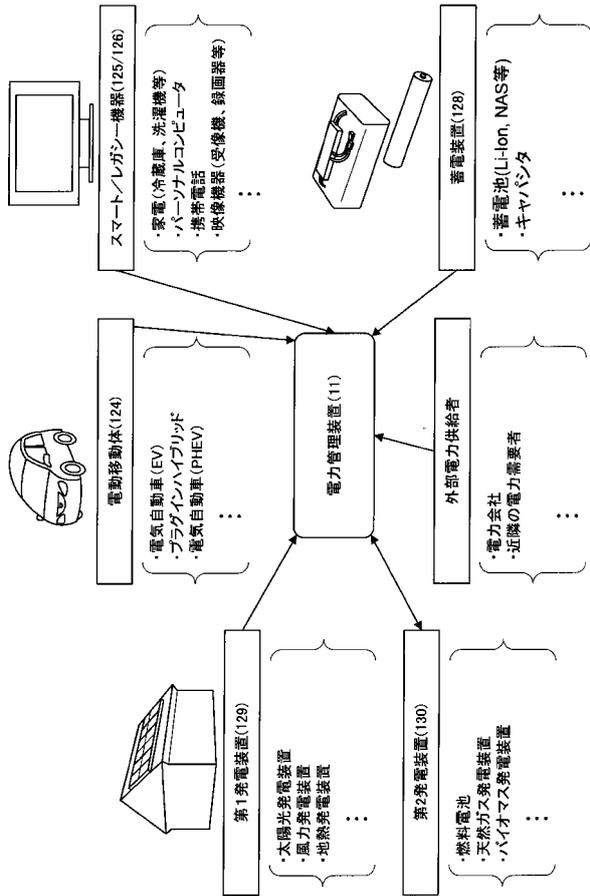
(管理対象ブロック12の例)

【図3】

(局所情報網の構成例)

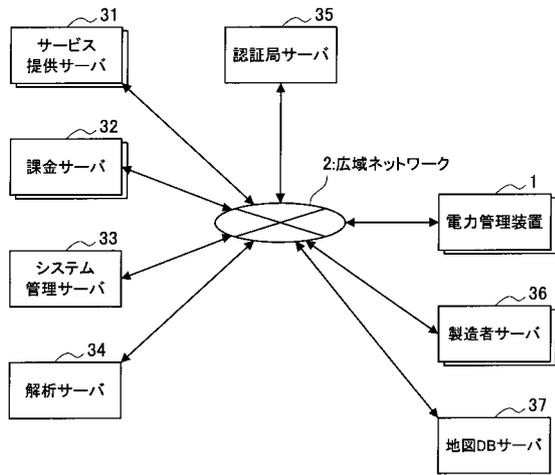


【図4】

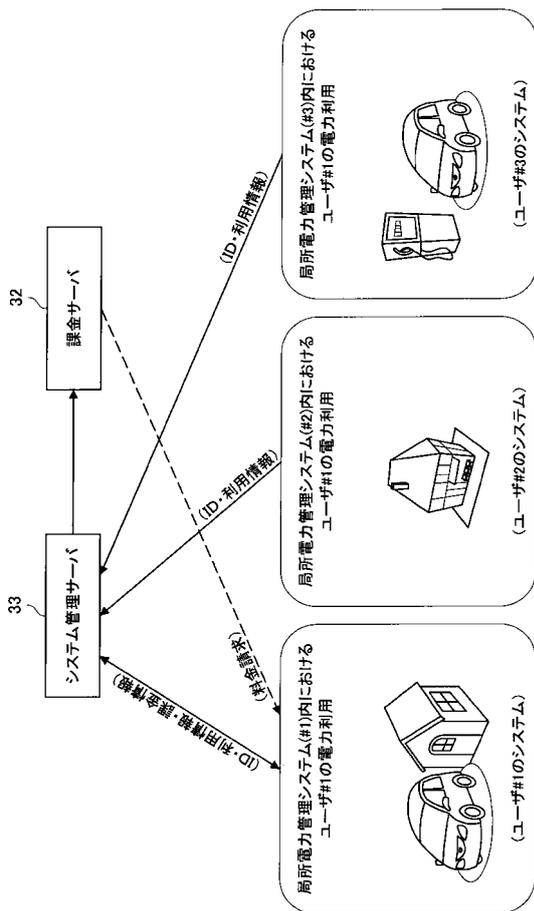


【図5】

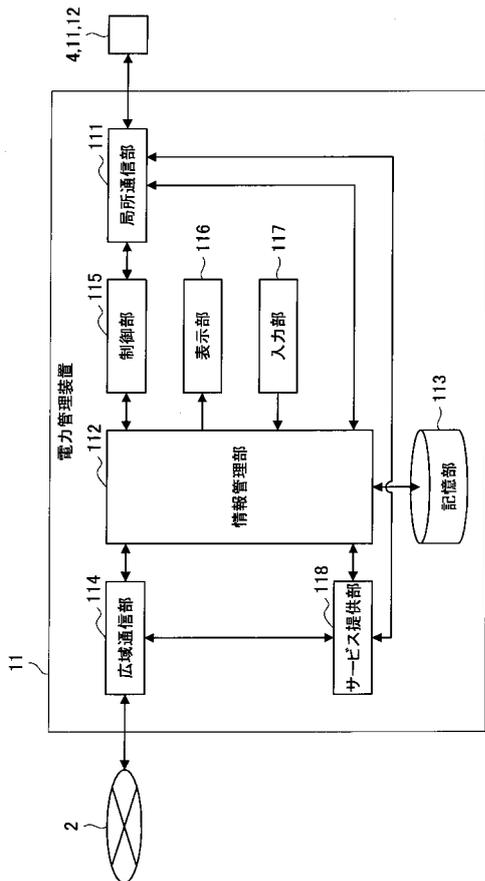
(外部サーバ3の例)



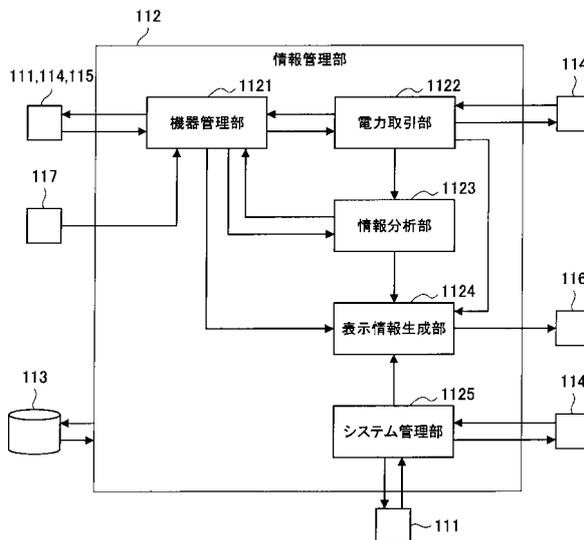
【図6】



【図7】



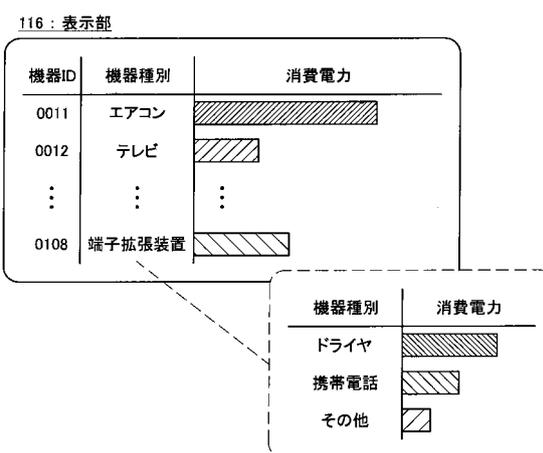
【図8】



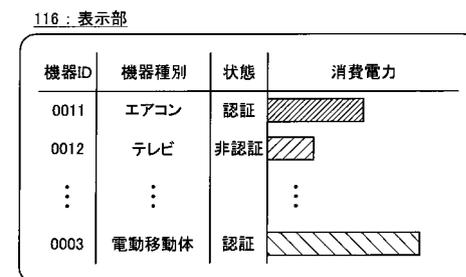
【図9】

構成要素	主な機能の概要
機器管理部 1121	機器登録、機器認証、各機器のID管理、各機器の動作設定・サービス設定の管理、各機器の動作状況・使用状況の把握、環境情報の収集、使用状況の把握(機器毎、全体、所定ブロック単位)等
電力取引部 1122	市場取引データ/個別取引データの取得、売り注文/買い注文のタイミング制御、売り注文/買い注文の実行、売買ログの管理等
情報分析部 1123	発電データの分析、蓄電データの分析、ライフパターンの学習、電力消費データの分析(機器毎、全体、所定ブロック単位)、電力消費パターンの予測、蓄電パターンの予測、放電パターンの予測、発電パターンの予測、現在のCO2排出量の算出、将来のCO2排出量の予測、省電力パターンの算出、低CO2排出パターンの算出、省電力・低CO2排出となる機器構成・機器配置の算出等
表示情報生成部 1124	機器に関する情報、電力に関する情報、環境に関する情報、取引データに関する情報、分析結果に関する情報等の生成
システム管理部 1125	ファームウェアのバージョン管理、アップデート、アクセス制限、ウイルス対策等

【図10】



【図11】



【図12】

116:表示部

利用場所	消費電力	課金額
場所#1	*** kW	*** 円
場所#2	*** kW	*** 円
場所#3	*** kW	*** 円

【図13】

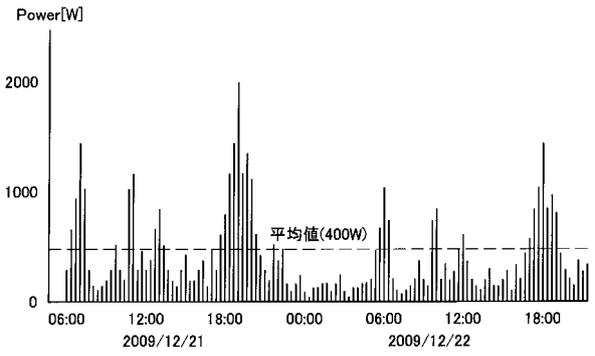
116:表示部

機器ID	機器種別	消費電力
0011	エアコン	
0012	テレビ	
⋮	⋮	⋮
0003	電動移動体	

自身のシステム外で利用した電力
 自身のシステム内で利用した電力

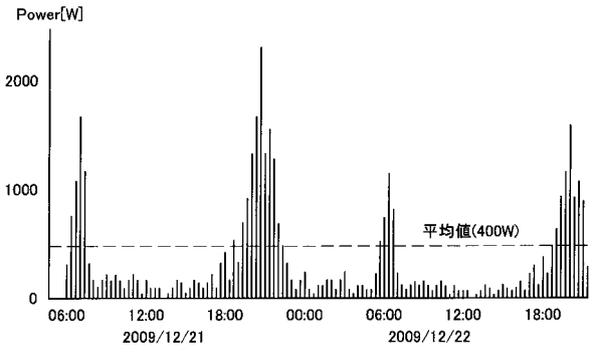
【図14】

(A) 電力消費パターンの例

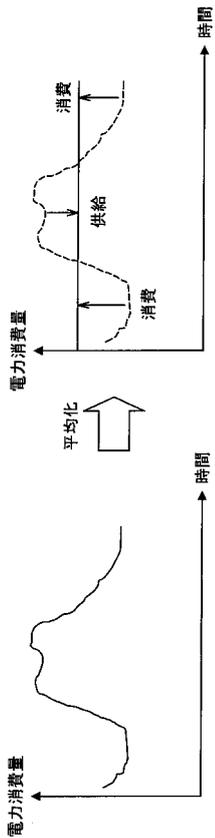


【図15】

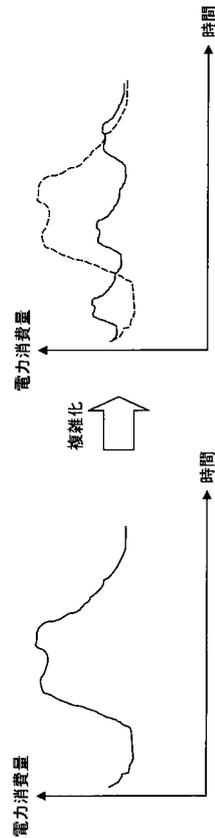
(B) 電力消費パターンの例



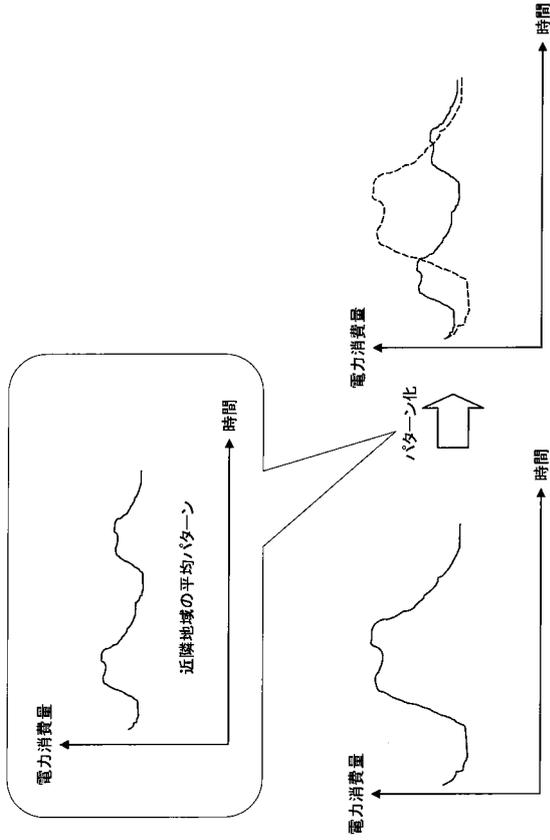
【図16】



【図17】



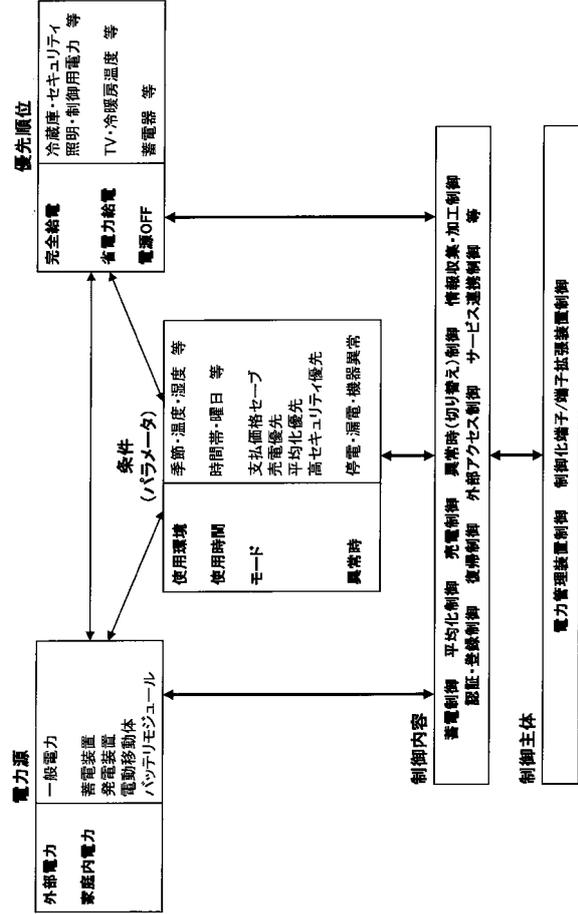
【図18】



【図20】

管理シリアルNo.	電力管理装置ID	メーカー・型番	登録日/失効日	ステータス
	電力管理装置公開鍵	証明書	証明書発行日	ステータス
	ユーザ名	ユーザ住所・TEL	課金情報	ステータス
	電力管理装置内の設定条件	メーカー・型番	登録日	ステータス
	異常時の緊急連絡先	メーカー・型番	登録日/失効日	ステータス
	分電装置ID	...		
	制御化機器-ID1			
	制御化機器-ID2			
	...			
管理シリアルNo.	電力管理装置ID	...		

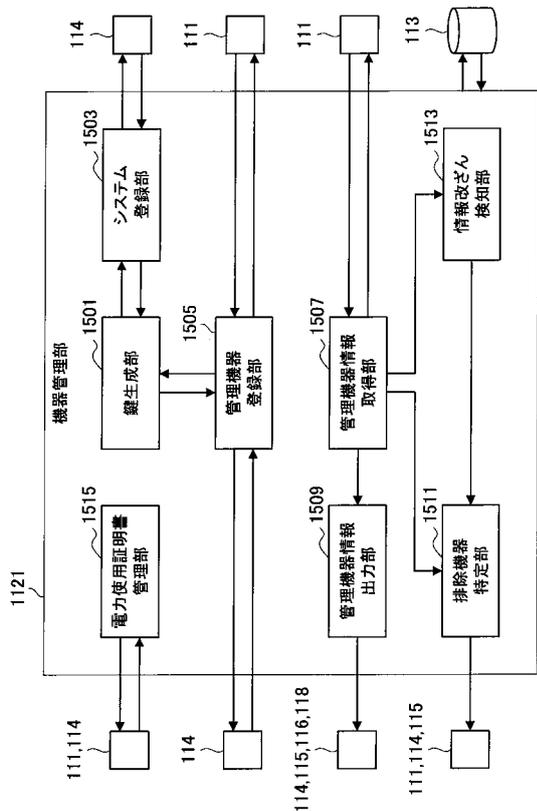
【図19】



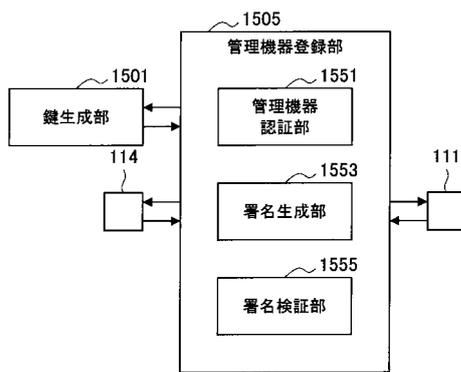
【図21】

端子の形態	接続機器の形態	電力情報通信手段	機器認証手段	給電制御
制御化端子	制御化機器	接続機器から ZigBeeで 制御化端子から ZigBeeまたはPLCで	接続機器から ZigBeeで	電力管理装置から分電装置に制御命令 制御化端子から限定的な制御が可能
制御化端子	非制御化機器	制御化端子から ZigBeeまたはPLCで	なし	電力管理装置から分電装置に制御命令 制御化端子から限定的な制御が可能
非制御化端子	制御化機器	接続機器から ZigBeeで	接続機器から ZigBeeで	電力管理装置から分電装置に制御命令
非制御化端子	非制御化機器	なし	なし	常時給電

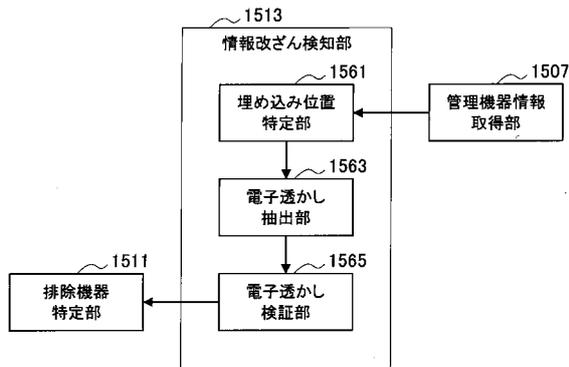
【図22】



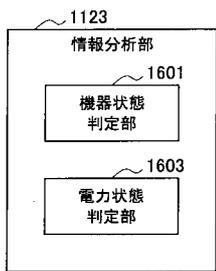
【図23】



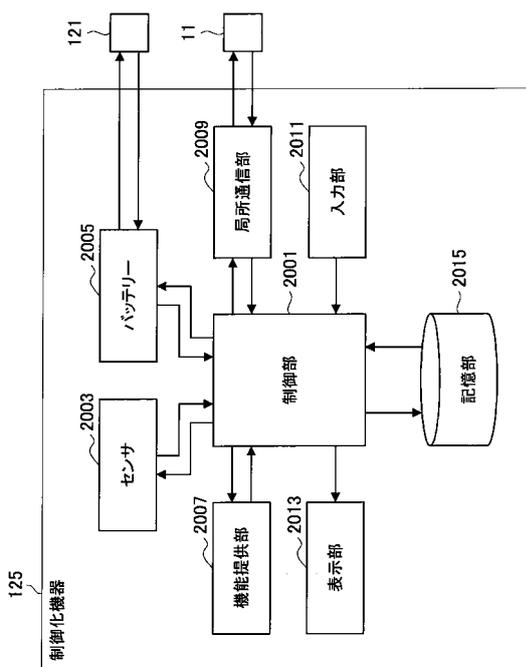
【図24】



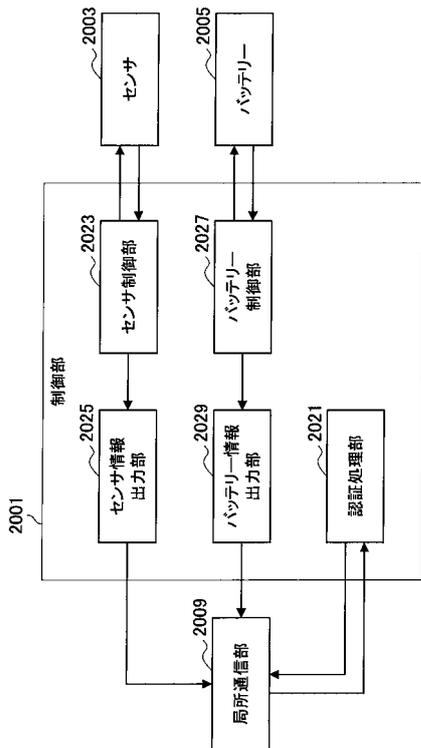
【図25】



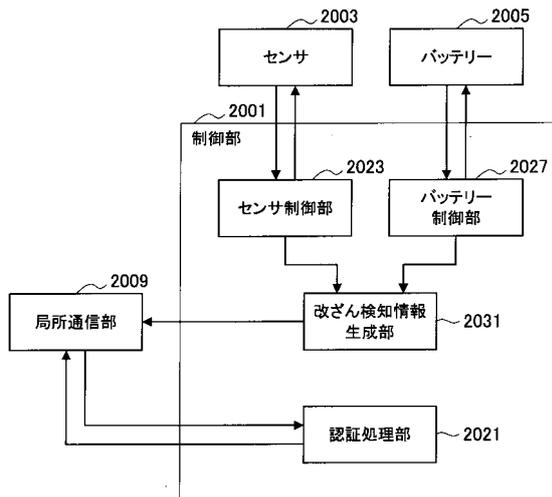
【図26】



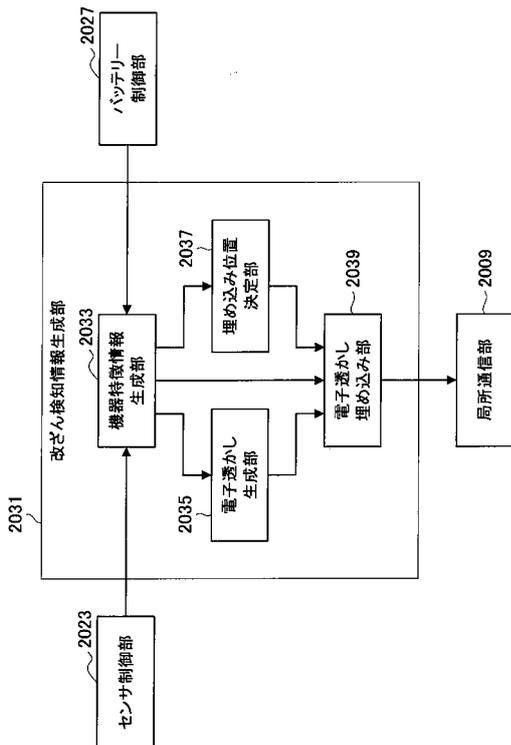
【図 27】



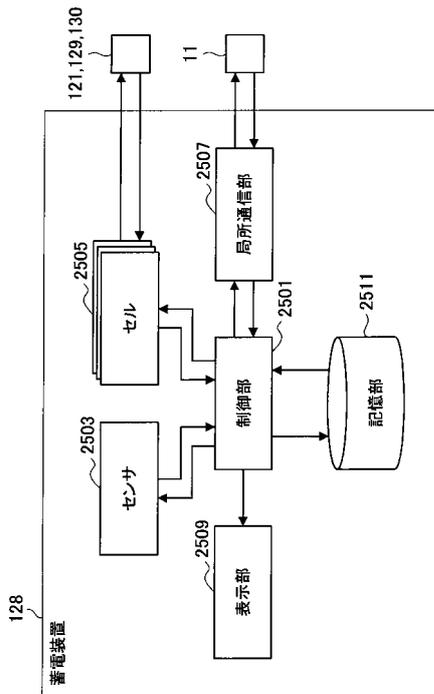
【図 28】



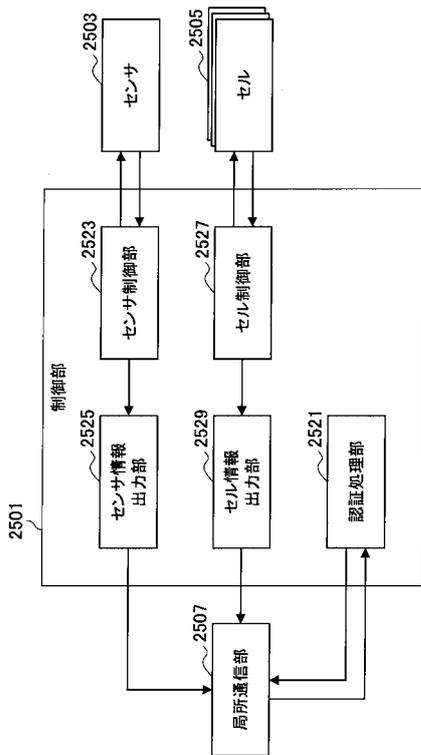
【図 29】



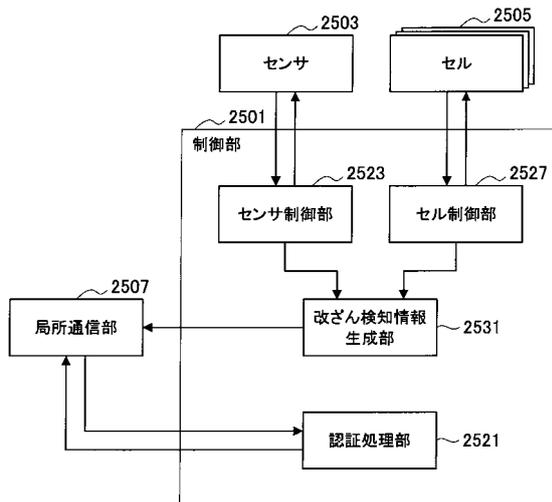
【図 30】



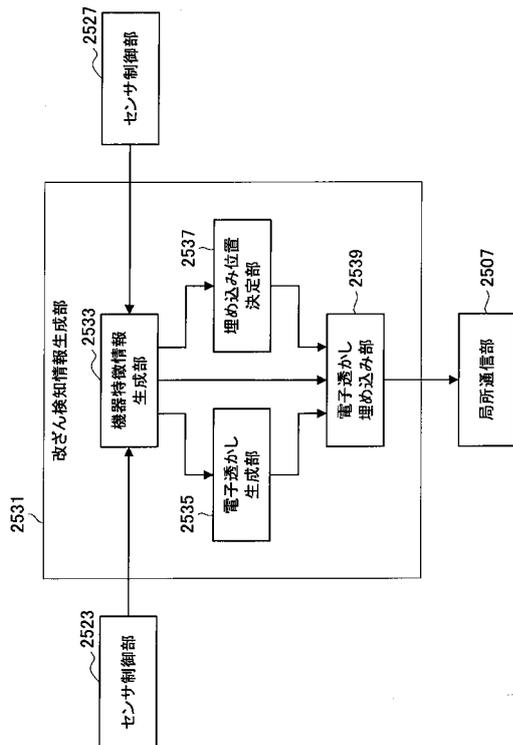
【図 3 1】



【図 3 2】

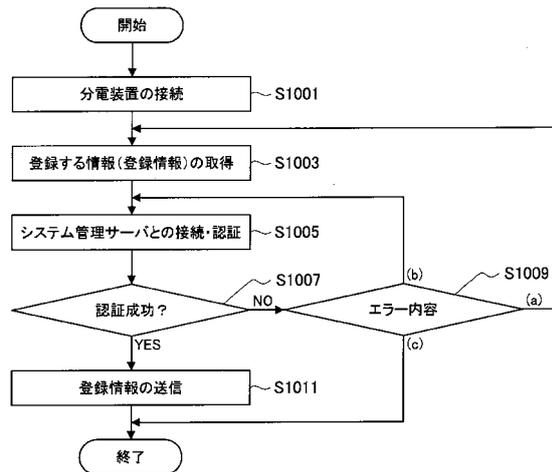


【図 3 3】



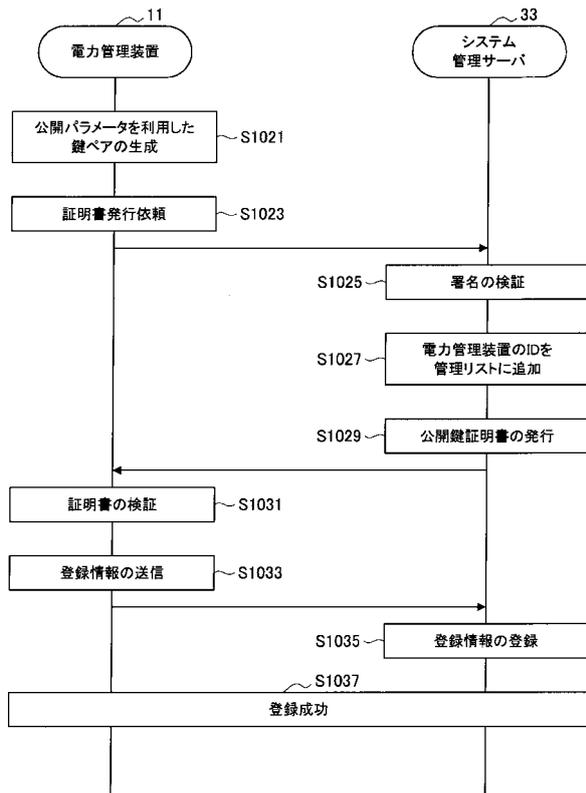
【図 3 4】

(電力管理装置の登録)



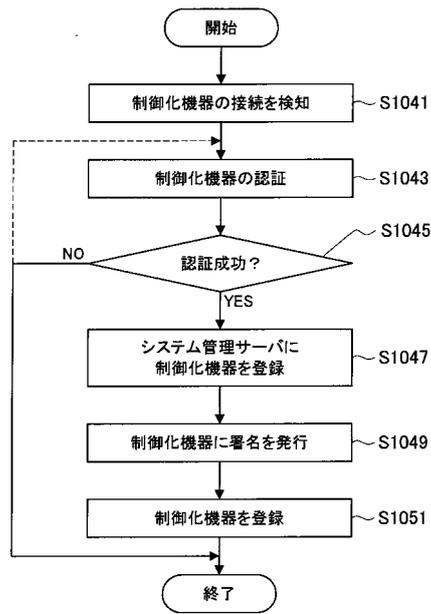
【図35】

(システム管理サーバの間で行われる処理の例)



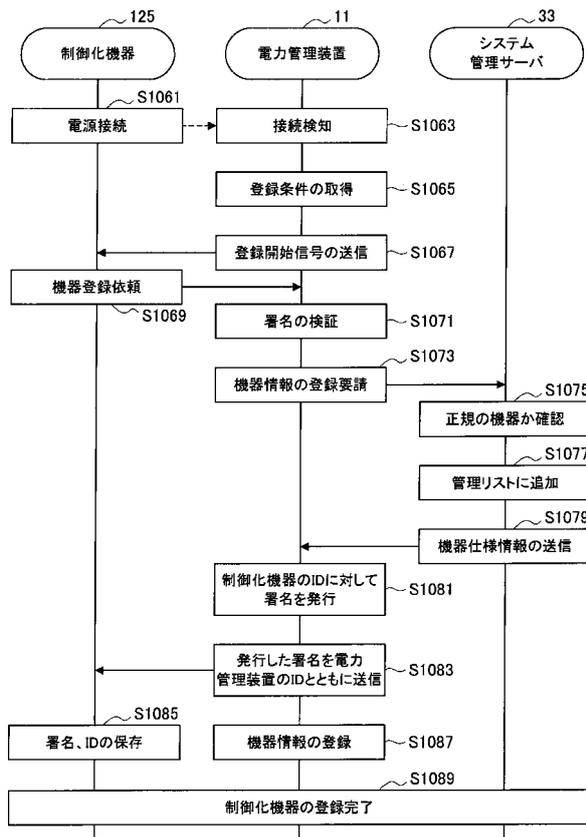
【図36】

(制御化機器の登録)



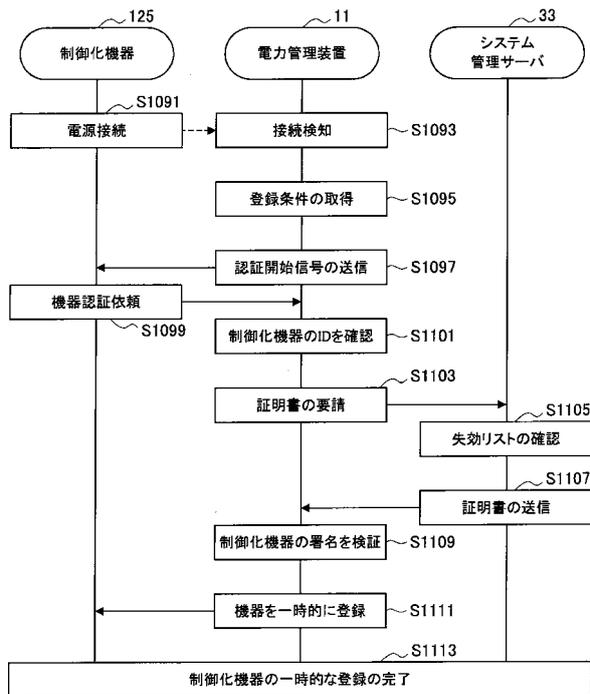
【図37】

(制御化機器の初期登録)

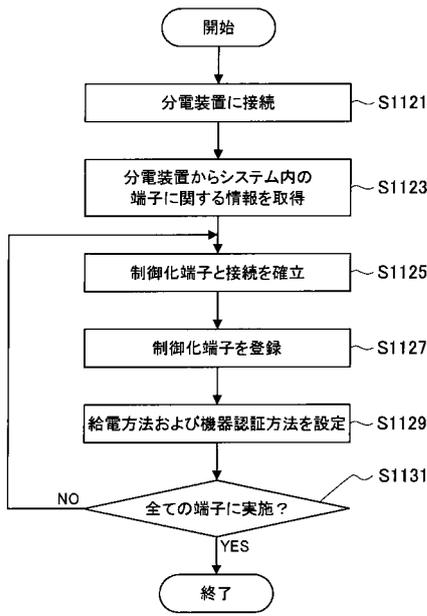


【図38】

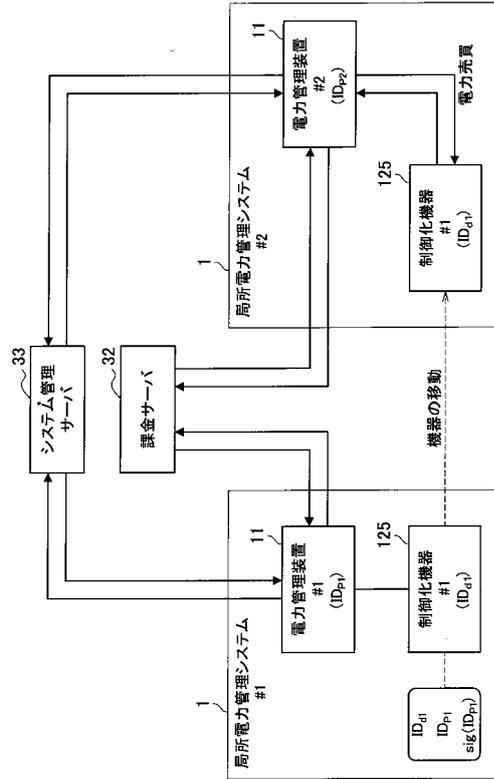
(制御化機器の一時的な登録)



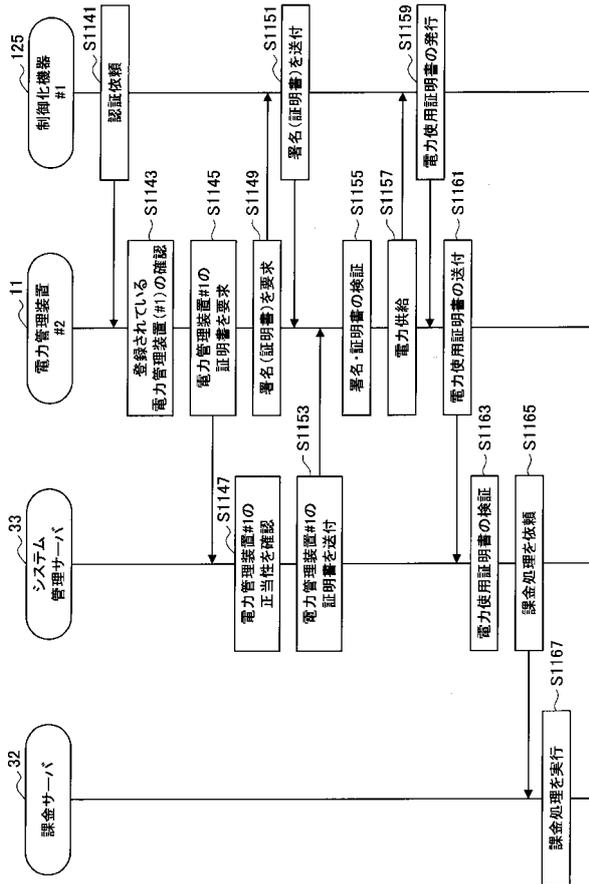
【図39】



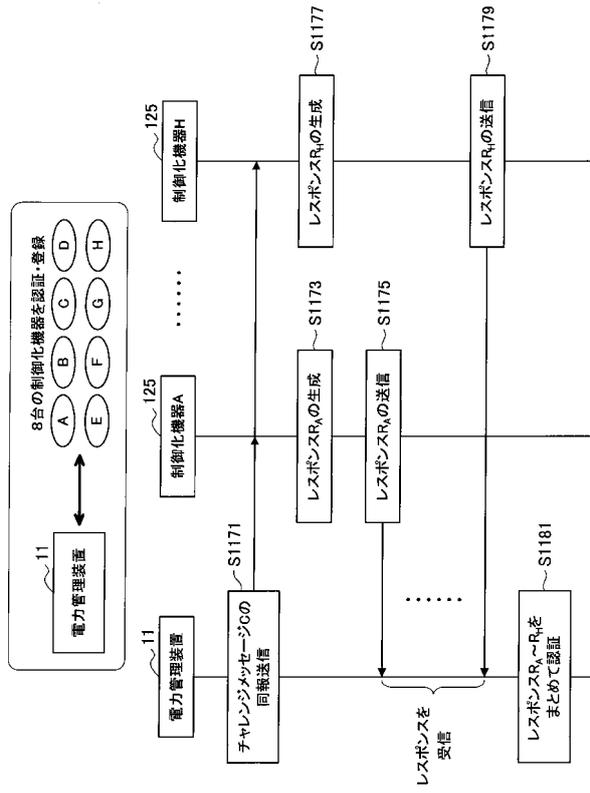
【図40】



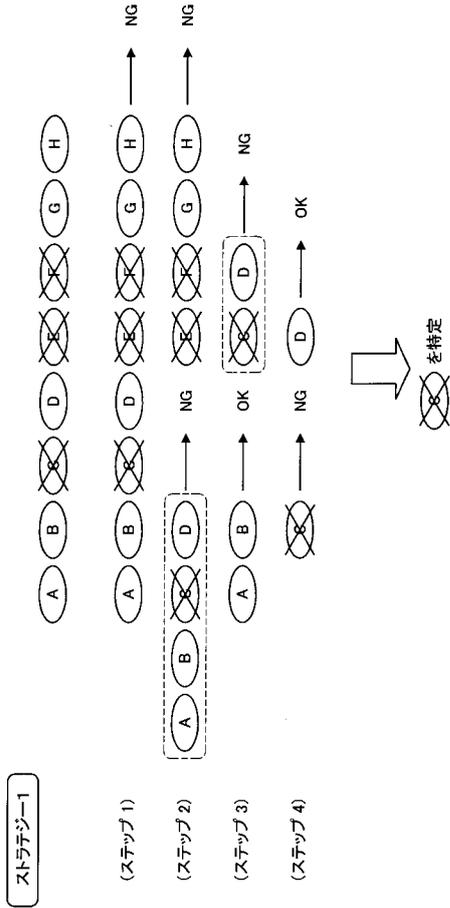
【図41】



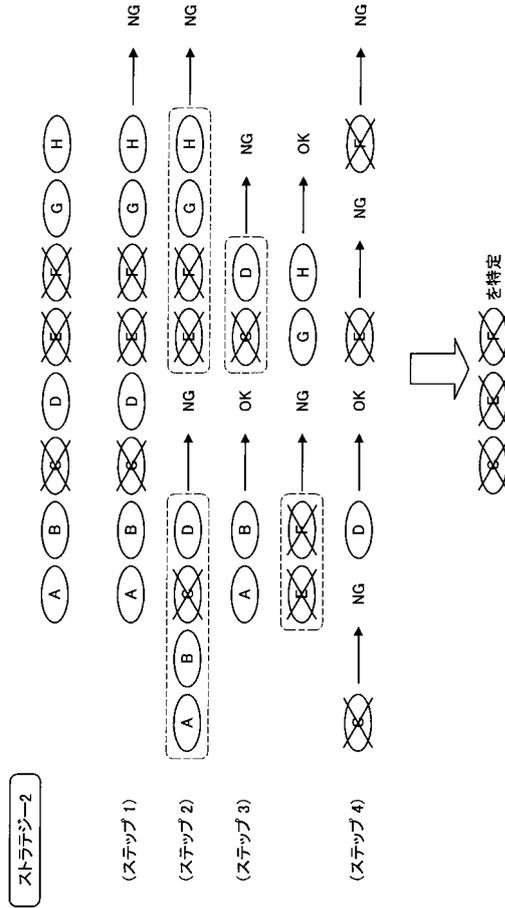
【図42】



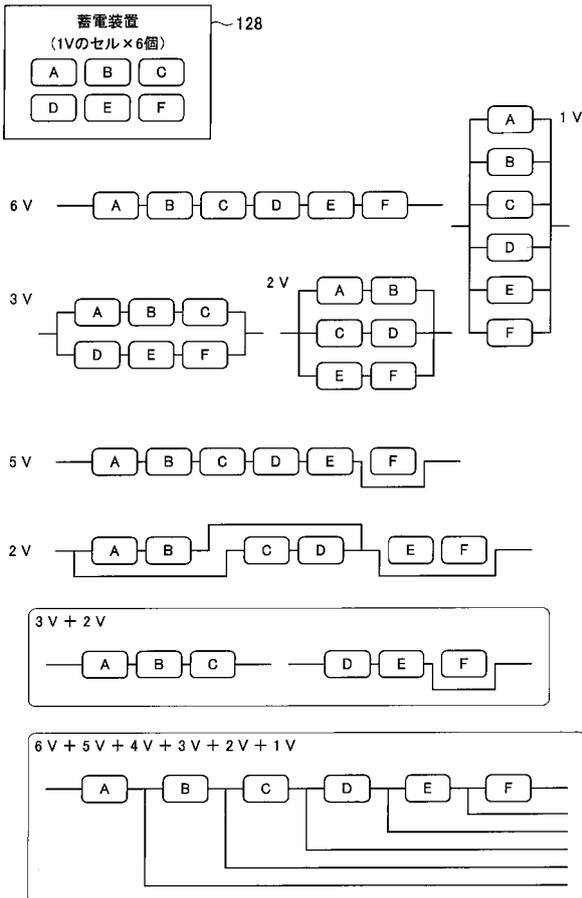
【 図 4 3 】



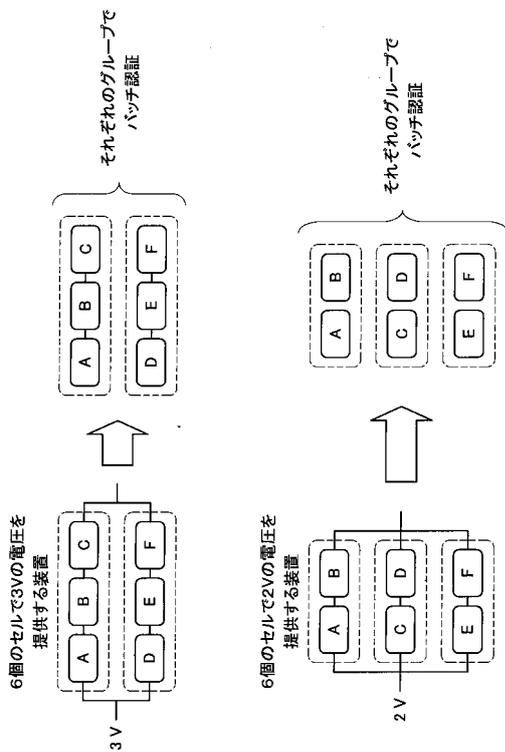
【 図 4 4 】



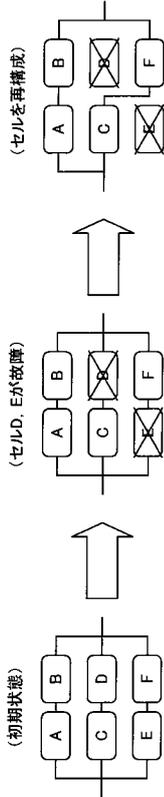
【 図 4 5 】



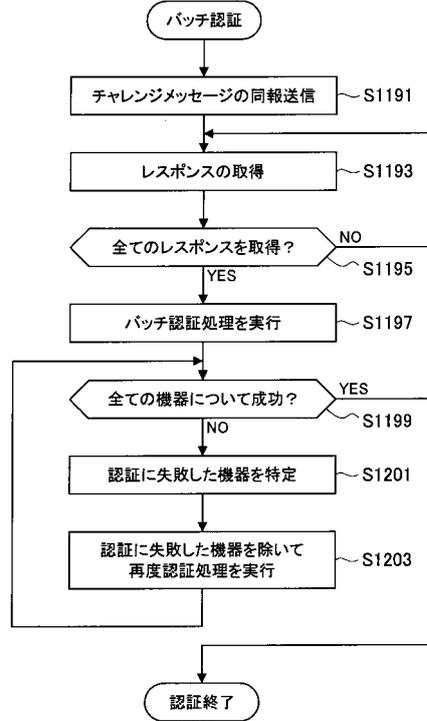
【 図 4 6 】



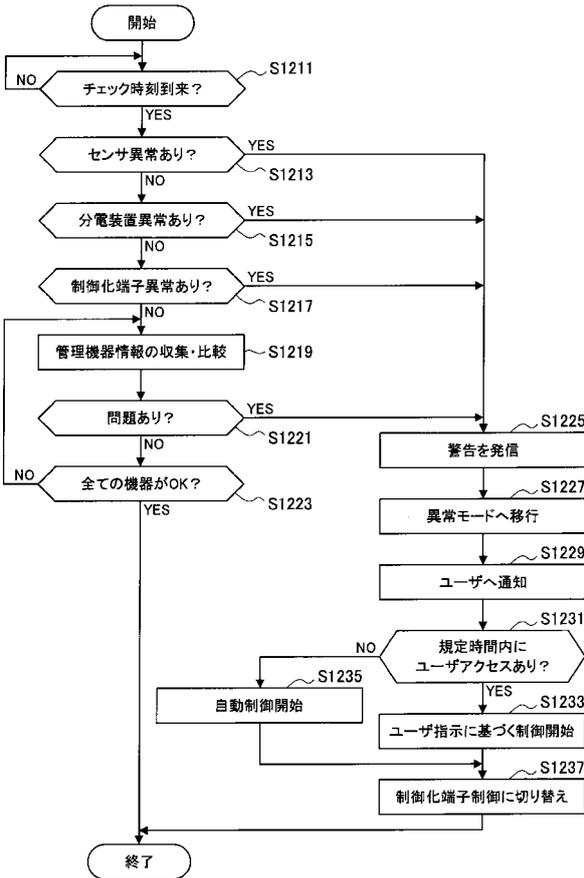
【図47】



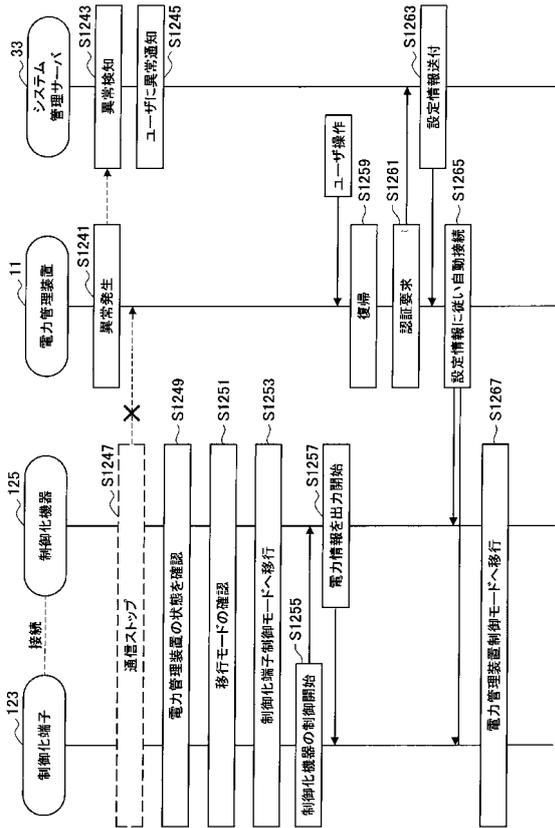
【図48】



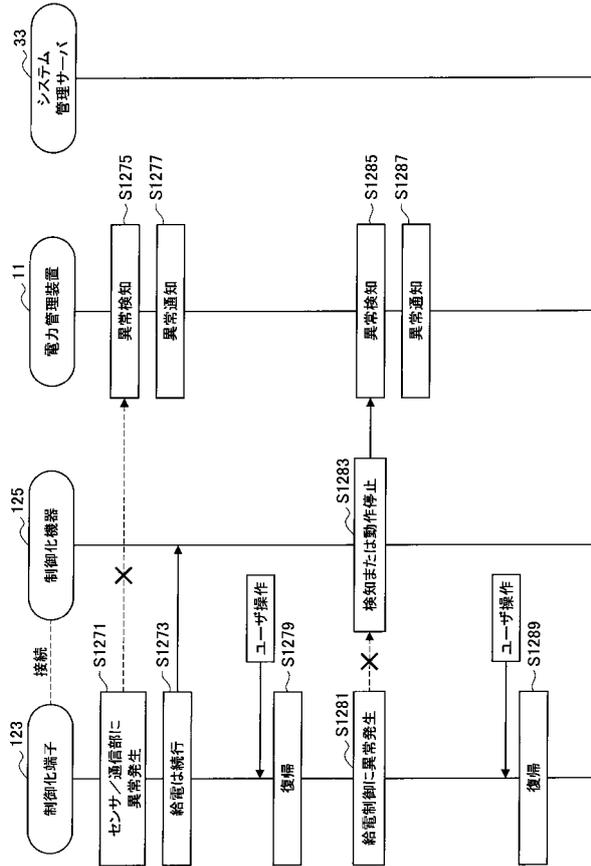
【図49】



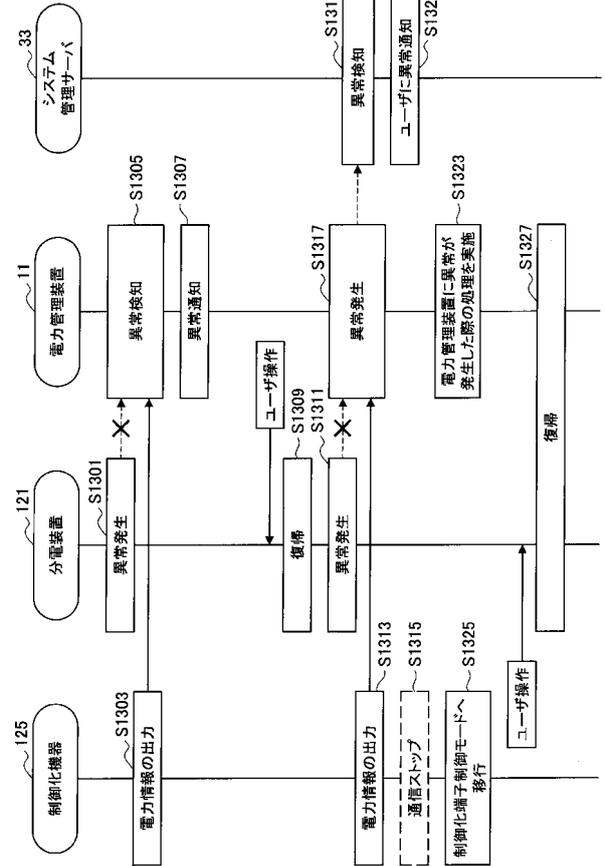
【図50】



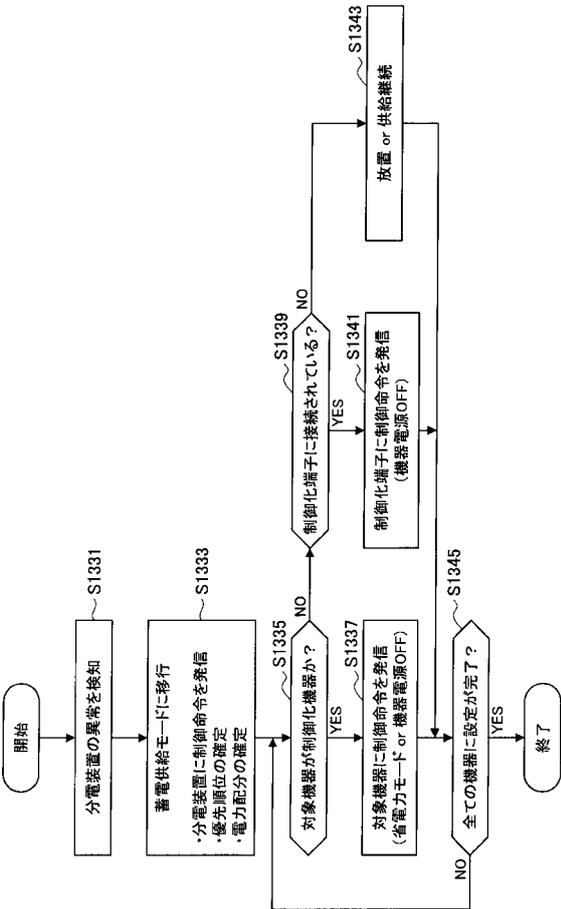
【図 5 1】



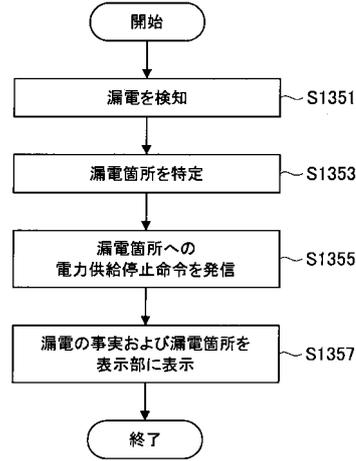
【図 5 2】



【図 5 3】

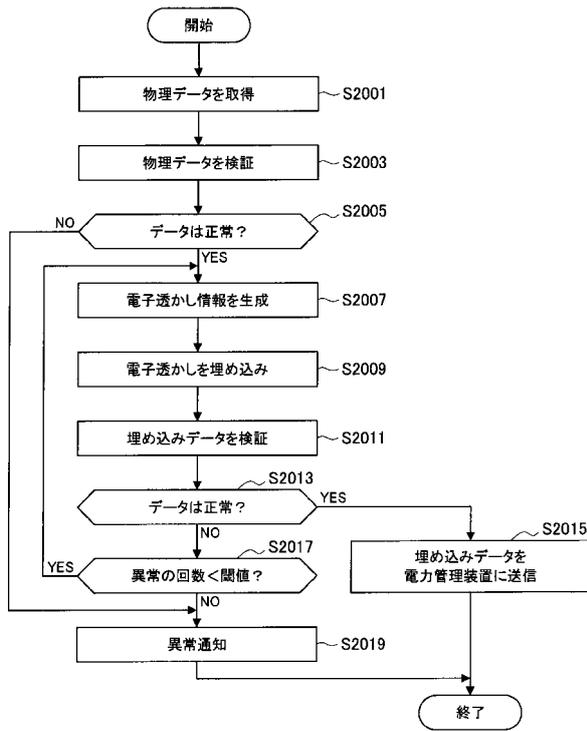


【図 5 4】



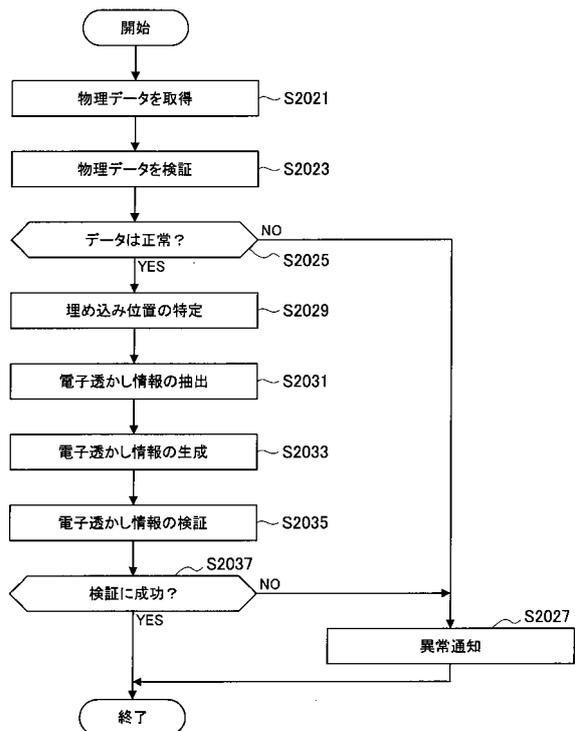
【図55】

(制御化機器における処理)



【図56】

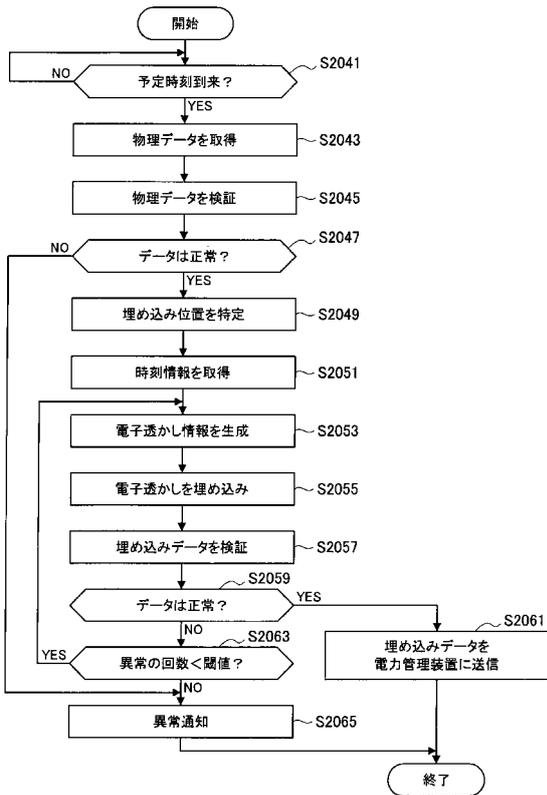
(解析サーバ(*)における処理)



(*)電力管理装置においても同様の検証を実行可能

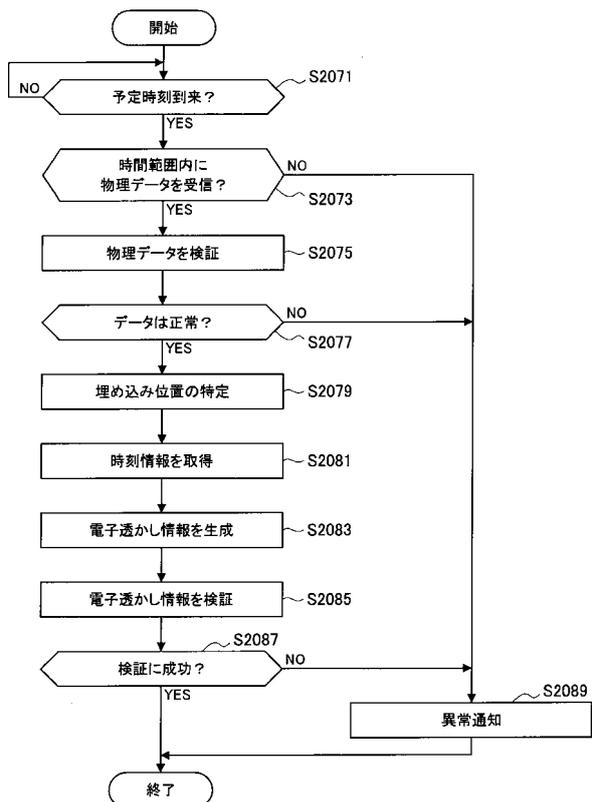
【図57】

(制御化機器における処理)

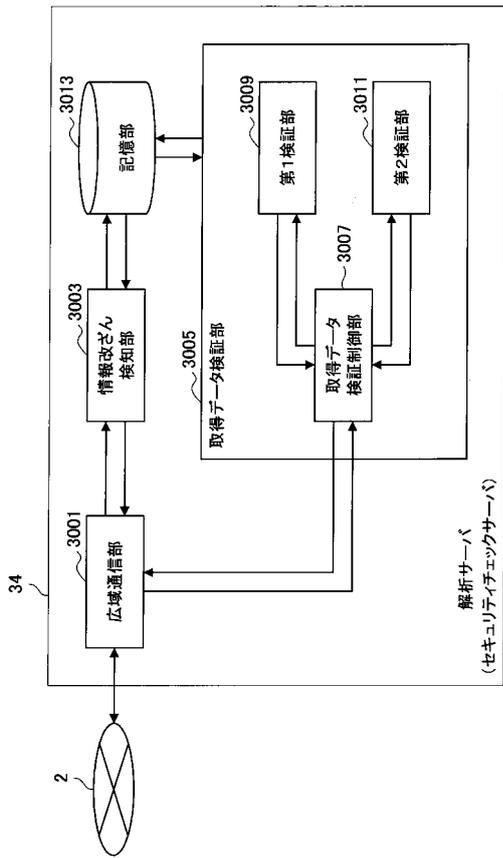


【図58】

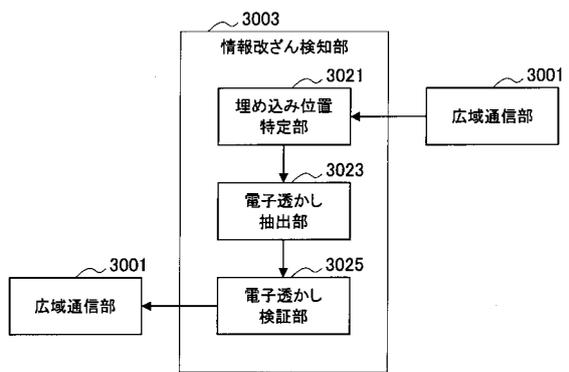
(解析サーバにおける処理)



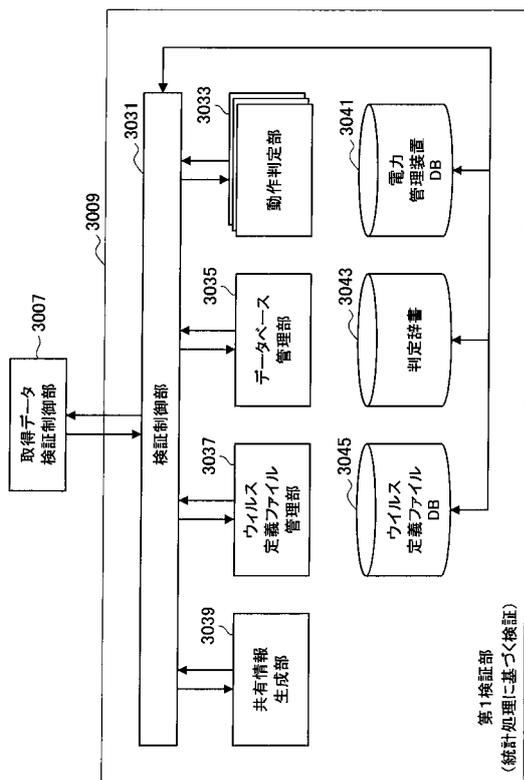
【図 59】



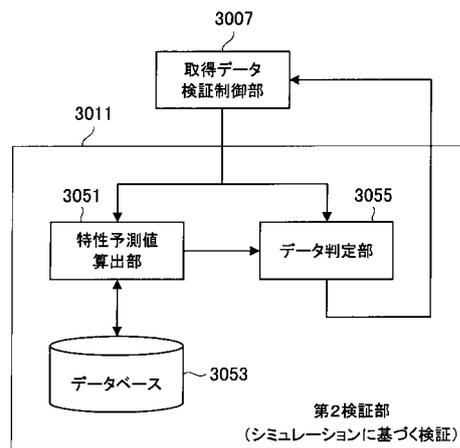
【図 60】



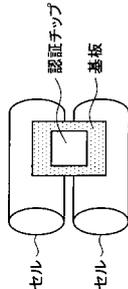
【図 61】



【図 62】



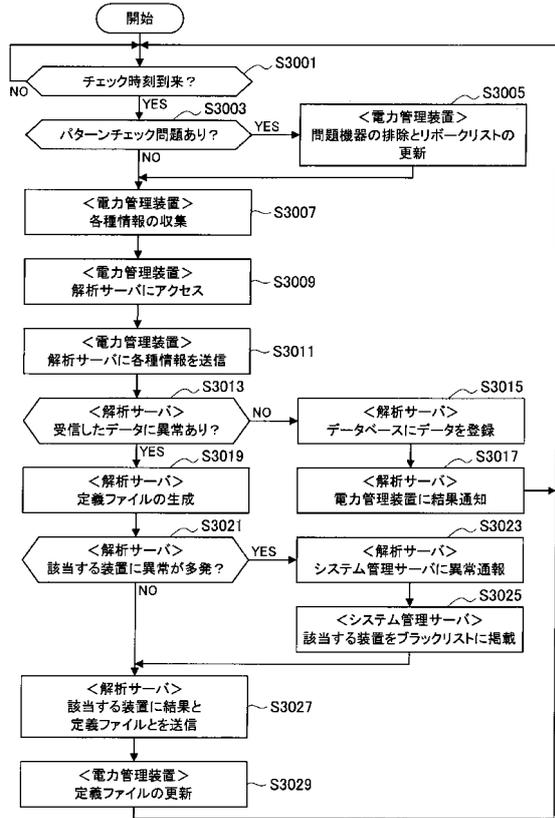
【図63】



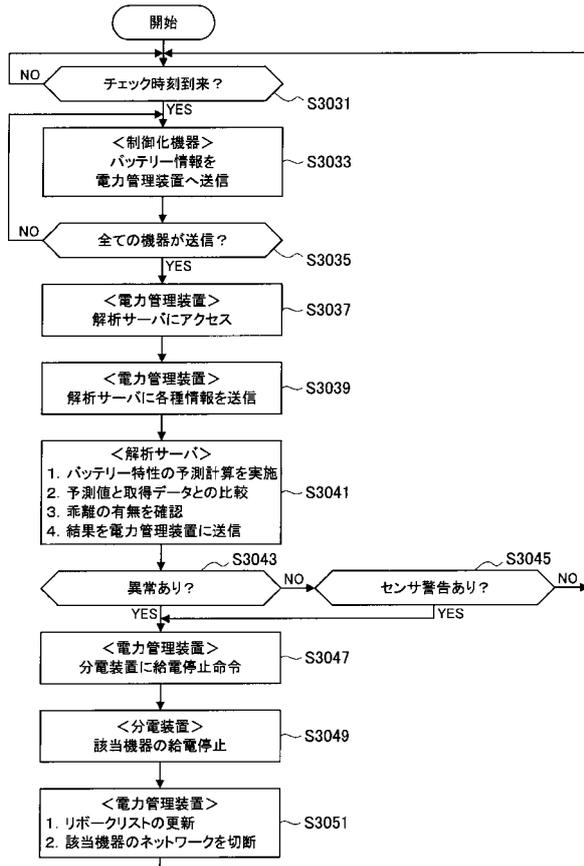
セル	セル	セル	セル特性・機器情報
セル	セル	セル	セル特性に問題はなく正しい機器情報(*)を出力
セル	セル	セル	セル特性に問題はなく正しい機器情報を出力
セル	セル	セル	セル特性または機器情報に予測との乖離がある
セル	セル	セル	セル特性に問題はなく正しい機器情報を出力
セル	セル	セル	セル特性に予測との乖離があるが正しい機器情報を出力
セル	セル	セル	セル特性に予測との乖離があるが正しい機器情報を出力
セル	セル	セル	セル特性に予測との乖離がある機器情報にも乖離がある

(*)バッテリーの電圧に関する情報、残量に関する情報等

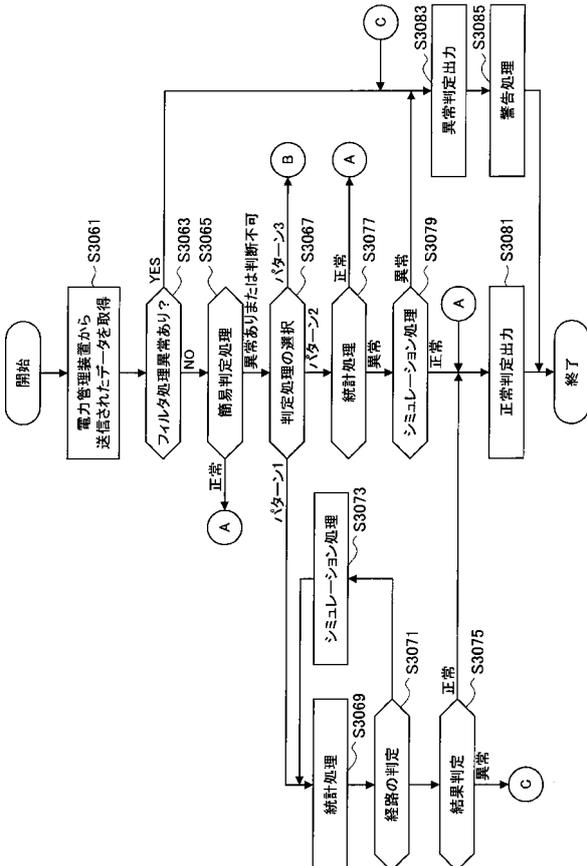
【図64】



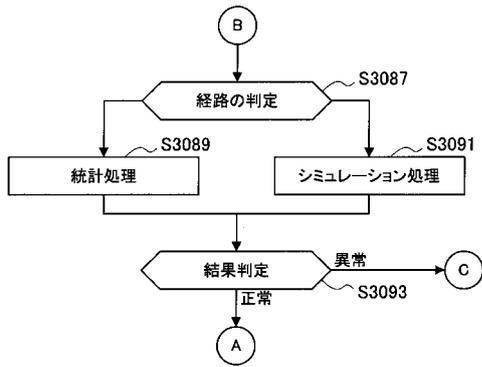
【図65】



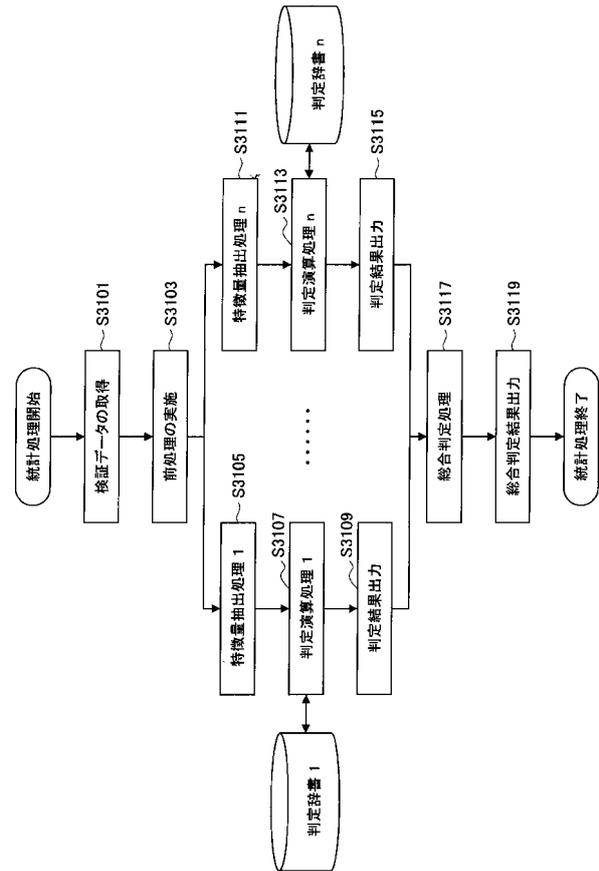
【図66A】



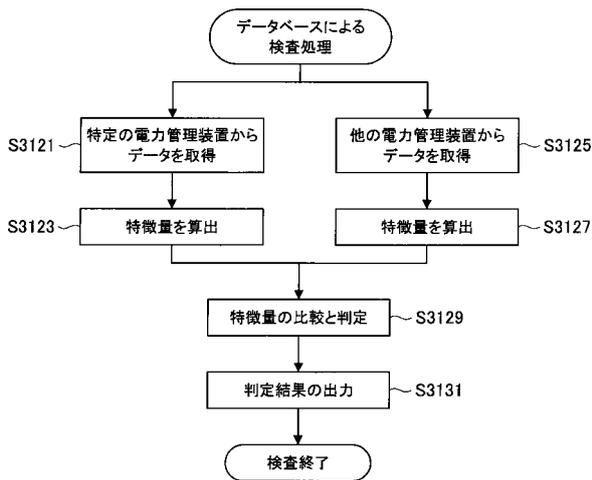
【図66B】



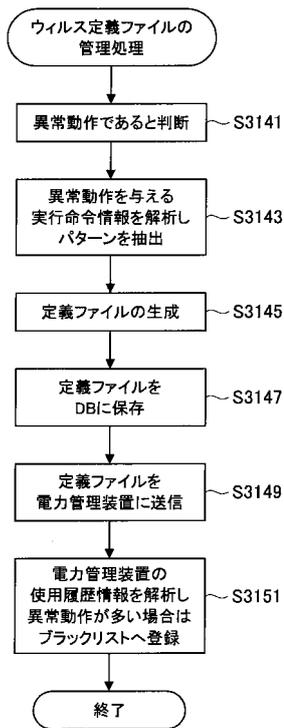
【図67】



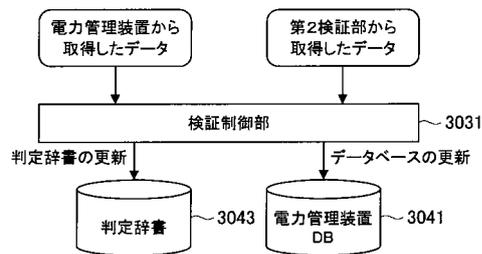
【図68】



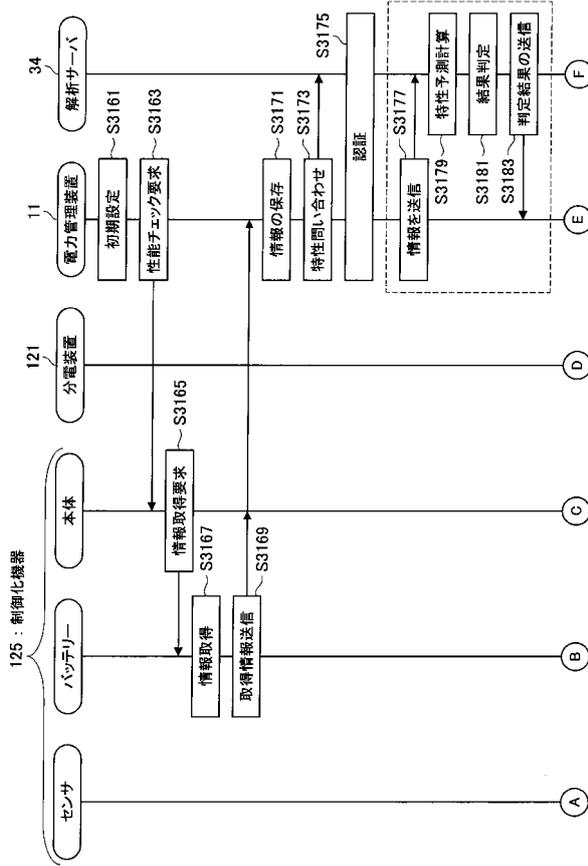
【図70】



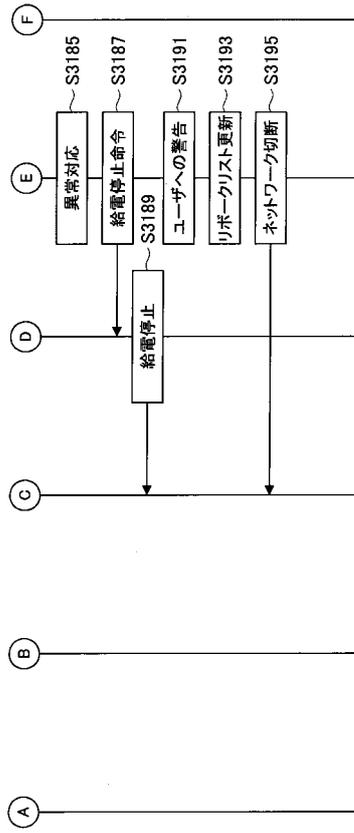
【図69】



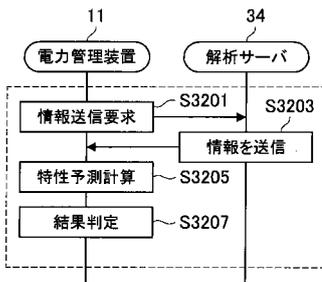
【図71A】



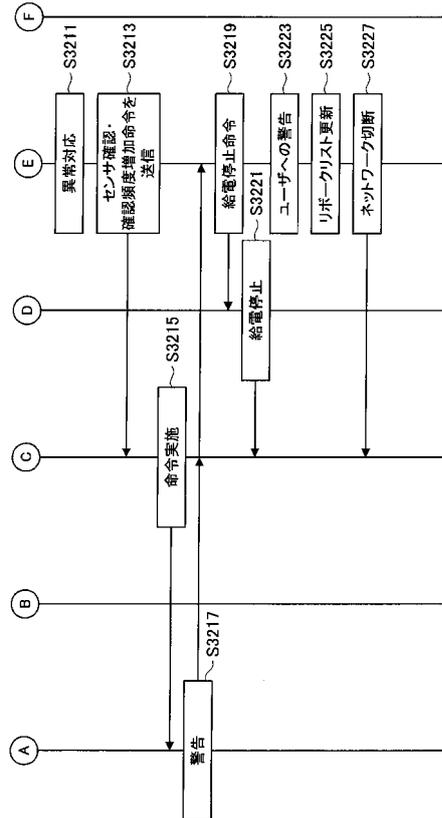
【図71B】



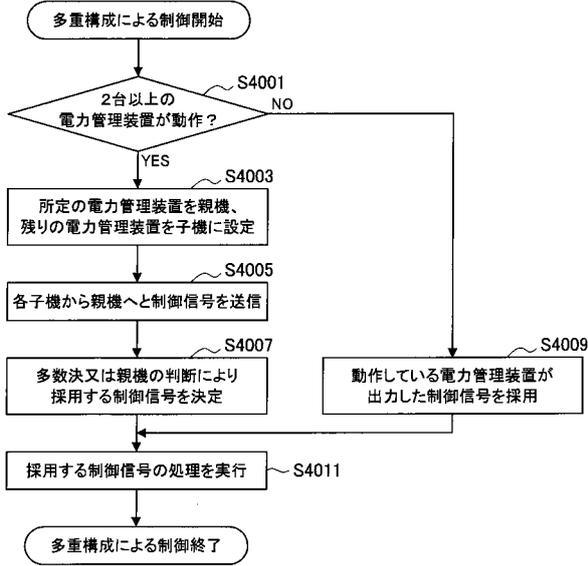
【図71C】



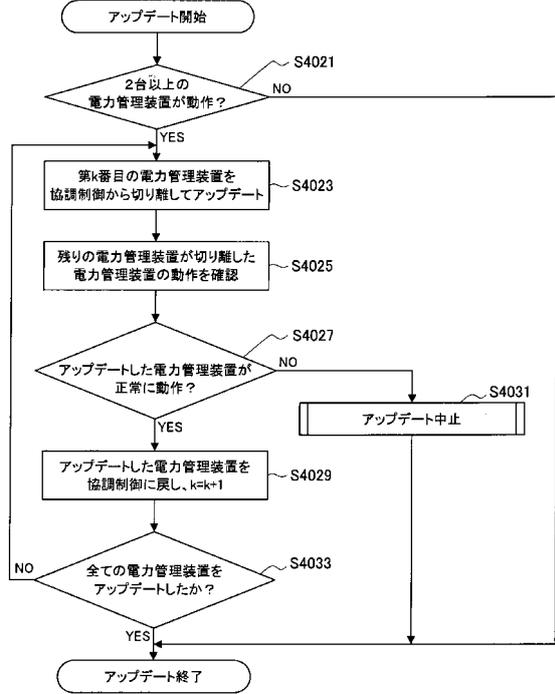
【図72】



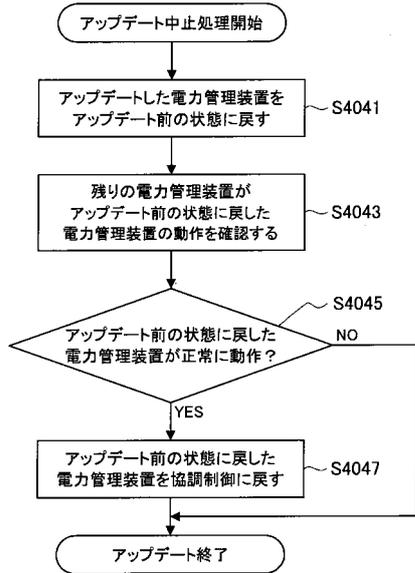
【図73】



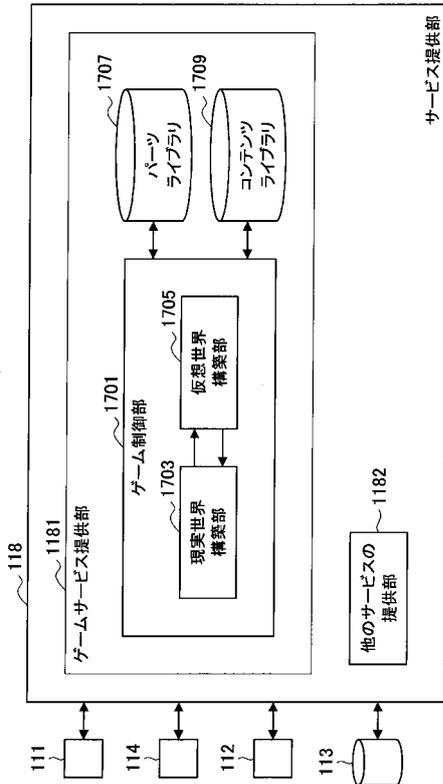
【図74】



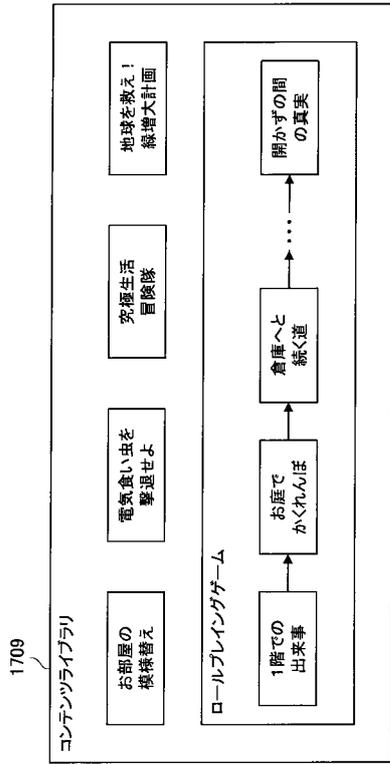
【図75】



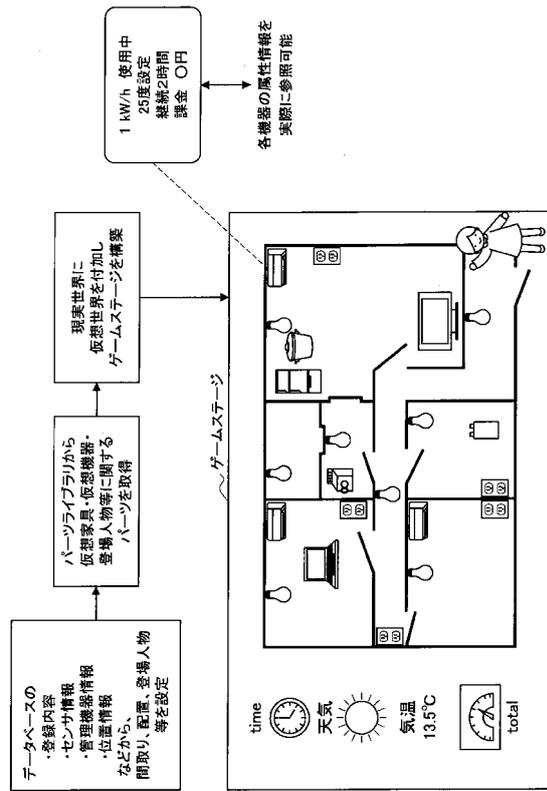
【図76】



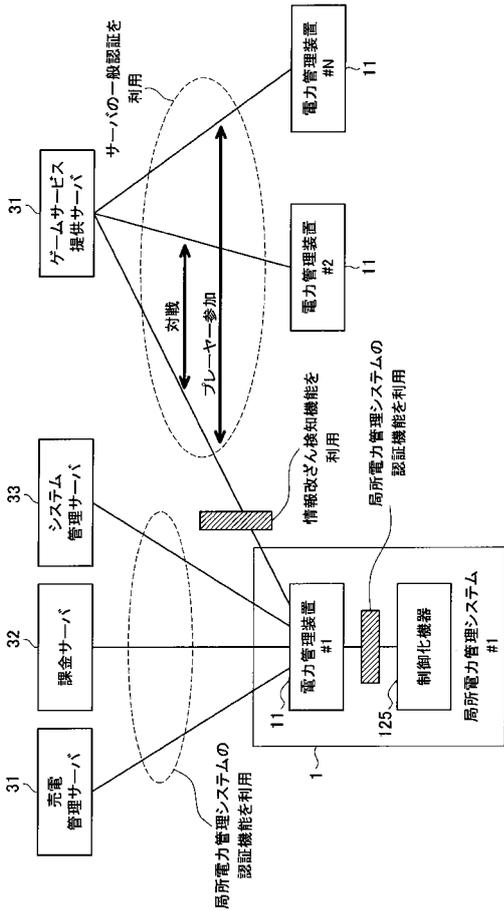
【図77】



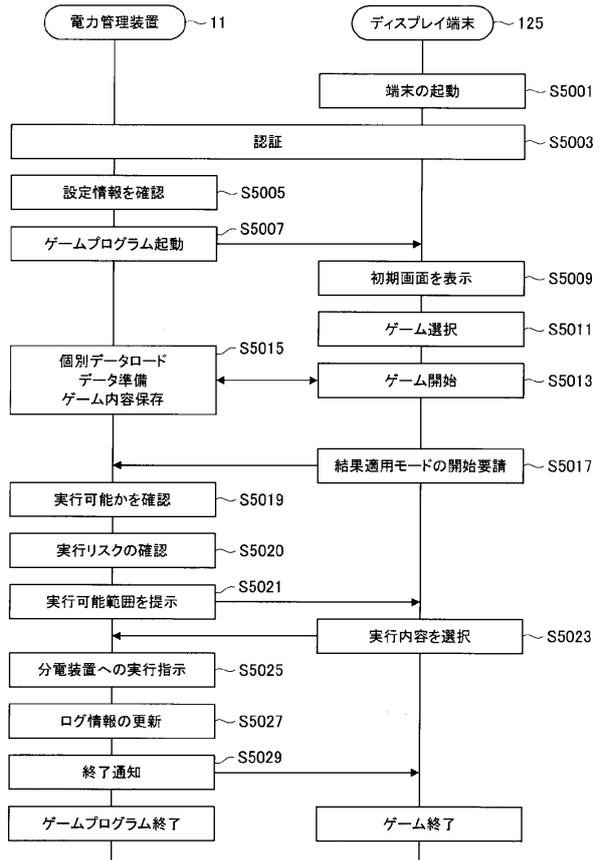
【図78】



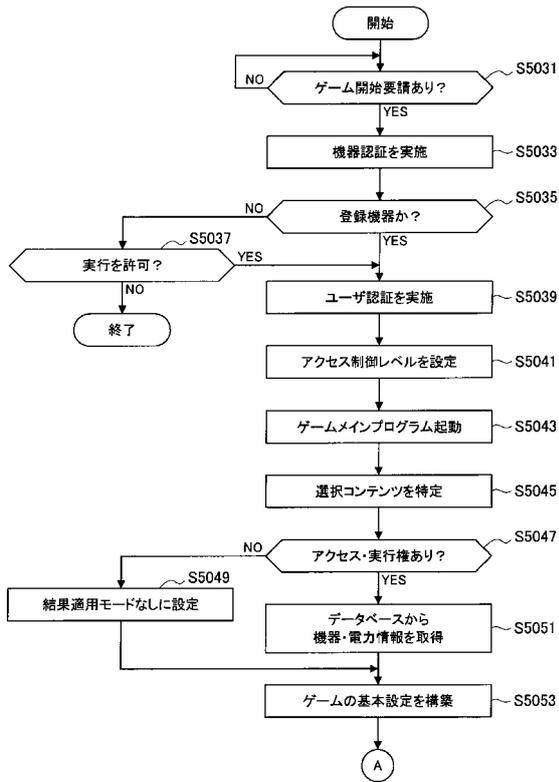
【図79】



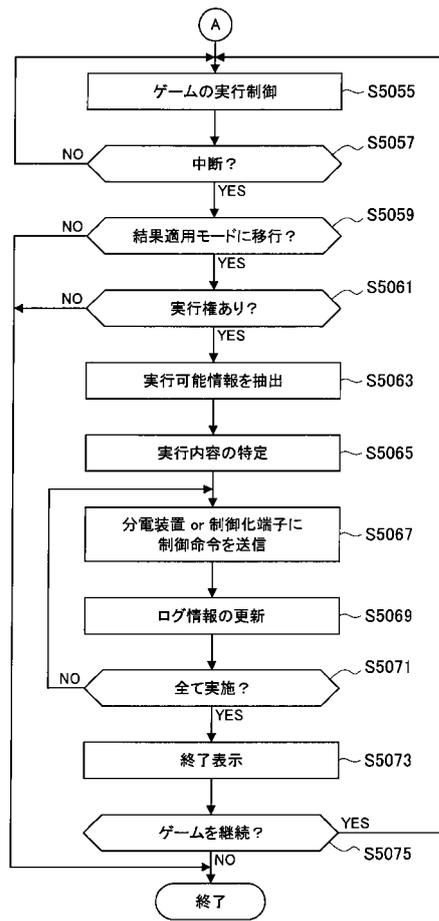
【図80】



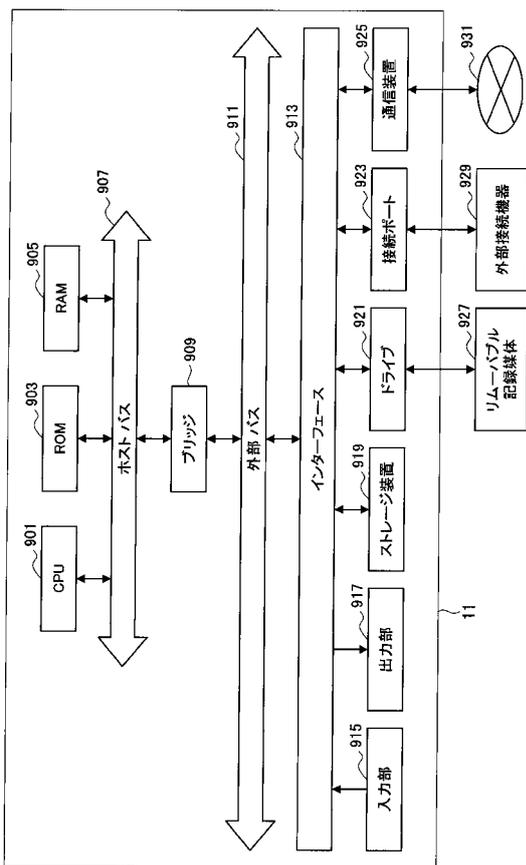
【図81A】



【図81B】



【図82】



フロントページの続き

- (72)発明者 堅木 雅宣
東京都港区港南1丁目7番1号 ソニー株式会社内
- (72)発明者 吉田 亜左実
東京都港区港南1丁目7番1号 ソニー株式会社内
- (72)発明者 浅野 智之
東京都港区港南1丁目7番1号 ソニー株式会社内
- (72)発明者 盛合 志帆
東京都港区港南1丁目7番1号 ソニー株式会社内
- (72)発明者 浮田 昌一
東京都港区港南1丁目7番1号 ソニー株式会社内
- (72)発明者 川元 洋平
東京都港区港南1丁目7番1号 ソニー株式会社内
- (72)発明者 田中 雄
東京都港区港南1丁目7番1号 ソニー株式会社内

審査官 高野 誠治

- (56)参考文献 特開2006-094655(JP,A)
特開2006-262570(JP,A)
特開2004-038292(JP,A)
特開2007-081493(JP,A)
特開2004-023497(JP,A)
特開2009-282718(JP,A)

(58)調査した分野(Int.Cl., DB名)

H02J 13/00
G06Q 50/00
H04L 9/32
H04M 11/00
H04Q 9/00