(19)日本国特許庁(JP)　　(12)公開特許公報(A)　　(11)特許出願公開番号
特開2022-79234
(P2022-79234A)
(43)公開日　令和4年5月26日(2022.5.26)

(51)Int.Cl.			F I			テーマコード（参考）
H04L	*9/32*	*(2006.01)*	H04L	9/00	675B	
G09C	*1/00*	*(2006.01)*	G09C	1/00	640E	

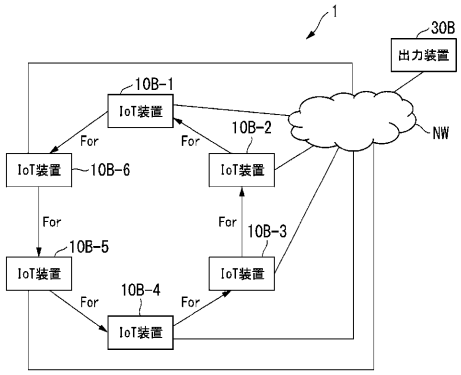
審査請求 未請求　請求項の数 10　ＯＬ　（全 44 頁）

(21)出願番号　特願2020-190308(P2020-190308)
(22)出願日　令和2年11月16日(2020.11.16)

(71)出願人　520449231
株式会社フィールズラボ
東京都渋谷区渋谷３丁目１９番１号
(74)代理人　100141139
弁理士　及川　周
(74)代理人　100145481
弁理士　平野　昌邦
(74)代理人　100181722
弁理士　春田　洋孝
(72)発明者　末神　奏宙
東京都渋谷区渋谷３丁目１９番１号　株式会社フィールズラボ内

(54)【発明の名称】管理システム、装置及び方法

(57)【要約】　（修正有）
【課題】秘密鍵の漏洩を検出する管理システム、装置及び方法を提供する。
【解決手段】管理システム１は、第１の装置１０Ｂ－３と第２の装置１０Ｂ－２を含む。第１の装置は、第１の公開鍵を含む第１メッセージと、第２の秘密鍵を用いて生成された第１の電子署名とを取得する第１取得部と、第１メッセージと第１の電子署名とを出力する通信部と、を備える。第２の装置は、第１メッセージ、第１の電子署名、第２メッセージ及び第２の電子署名を取得する第２取得部と、第１時刻情報と、第１メッセージ又は第２メッセージを取得する際に、第１メッセージ及び第１の電子署名と、第２メッセージ及び第２の電子署名と、の何れかを取得済であることとの少なくともいずれかに基づいて、第２の秘密鍵の漏洩を判定する判定部とを備える。第２メッセージは、第１の公開鍵を少なくとも含む。第２の電子署名は、第２メッセージ及び第２の秘密鍵に基づいて生成される。
【選択図】図９



【特許請求の範囲】
【請求項１】
第１の装置及び第２の装置と、前記第１の装置及び前記第２の装置を接続するネットワークと、を備える管理システムであって、
前記第１の装置は、
時刻に関する第１の時刻情報又は所定の検証プロセスの周期を示す第１のインデックスと、第１の秘密鍵に対応する第１の公開鍵又は前記第１の公開鍵の生成に用いられる値と、を含む第１のメッセージと、前記第１のメッセージについてのハッシュ値に対して第２の秘密鍵を用いることにより生成された第１の電子署名とを取得する第１の取得部と、
前記第１のメッセージと、前記第１の電子署名と、を前記ネットワークと通信を行うことにより出力する通信部と、を備え、
前記第２の装置は、
前記第１のメッセージ、前記第１の電子署名、第２のメッセージ及び第２の電子署名を取得する第２の取得部と、
前記第１の時刻情報又は第１のインデックスと、前記第２の取得部が前記第１のメッセージ又は前記第２のメッセージを取得する際に、前記第１のメッセージ及び前記第１の電子署名と、前記第２のメッセージおよび前記第２の電子署名と、のいずれかを前記第２の取得部が取得済みであることと、の少なくともいずれかに基づいて、前記第２の秘密鍵が不正利用されたことを判定する判定部と、を備え、
前記第２のメッセージは、前記第１の公開鍵又は前記第１の公開鍵の生成に用いられる値を少なくとも含み、
前記第２の電子署名は、前記第２のメッセージ及び前記第２の秘密鍵に基づいて生成され、
前記第１の秘密鍵は前記第２の秘密鍵と異なる
管理システム。
【請求項２】
前記第１の取得部は、
周期ｎにおいて、前記第１のメッセージと、前記第１の電子署名とを取得し、
周期ｎ＋１において、時刻に関する第２の時刻情報又は周期ｎ+1に対応する第２のインデックスと、第３の秘密鍵に対応する第３の公開鍵又は前記第３の公開鍵の生成に用いられる値と、を含む第３のメッセージと、前記第３のメッセージについてのハッシュ値に対して前記第１の秘密鍵を用いることにより生成された第３の電子署名と、を取得し、
ｎは整数であり、前記第３の秘密鍵は前記第１の秘密鍵及び前記第２の秘密鍵と異なる
請求項１に記載の管理システム。
【請求項３】
前記第１のメッセージは、周期ｎ－１におけるメッセージのハッシュ値をさらに含み、
前記第３のメッセージは、前記第１のメッセージのハッシュ値をさらに含む
請求項２に記載の管理システム。
【請求項４】
前記第２の時刻情報が示す第２の時刻が、前記第１の時刻情報が示す第１の時刻と同じもしくは前記第２の時刻が前記第１の時刻より早い場合、又は前記第１のメッセージに前記第１のインデックスが含まれる場合において前記第３のメッセージに含まれるインデックスから前記第１のインデックスを減算した値が１でない場合、前記判定部は前記第１の秘密鍵が不正利用されたと判定する
請求項３に記載の管理システム。
【請求項５】
ネットワークを介して第２の装置と通信する第１の装置であって、
時刻に関する第１の時刻情報又は所定の検証プロセスの周期を示す第１のインデックスと、第１の秘密鍵に対応する第１の公開鍵又は前記第１の公開鍵の生成に用いられる値と、を含む第１のメッセージと、前記第１のメッセージについてのハッシュ値に対して第２

の秘密鍵を用いることにより生成された第１の電子署名と、を取得する取得部と、を備え、
前記第１の時刻情報又は第１のインデックスと、前記取得部が前記第１のメッセージ又は第２のメッセージを取得する際に、前記第１のメッセージ及び前記第１の電子署名と、前記第２のメッセージ及び第２の電子署名と、のいずれかを前記取得部が取得済みであることと、の少なくともいずれかに基づいて、前記第２の秘密鍵が不正利用されたことを判定する判定部と、を備え、
前記第２のメッセージは、前記第１の公開鍵又は前記第１の公開鍵の生成に用いられる値を少なくとも含み、
前記第２の電子署名は、前記第２のメッセージ及び前記第２の秘密鍵に基づいて生成され、
前記第１の秘密鍵は前記第２の秘密鍵と異なる
第１の装置。
【請求項６】
前記取得部は、
周期ｎにおいて、前記第１のメッセージと、前記第１の電子署名とを取得し、
周期ｎ＋１において、時刻に関する第２の時刻情報と、第３の秘密鍵に対応する第３の公開鍵又は前記第３の公開鍵の生成に用いられる値と、を含む第３のメッセージと、前記第３のメッセージについてのハッシュ値に対して前記第１の秘密鍵を用いることにより生成された第３の電子署名とを取得し、
ｎは整数であり、前記第３の秘密鍵は前記第１の秘密鍵及び前記第２の秘密鍵と異なる
請求項５に記載の第１の装置。
【請求項７】
前記第１のメッセージは、周期ｎ－１におけるメッセージのハッシュ値をさらに含み、前記第３のメッセージは、前記第１のメッセージのハッシュ値をさらに含む
請求項６に記載の第１の装置。
【請求項８】
前記第２の時刻情報が示す第２の時刻が前記第１の時刻情報が示す第１の時刻と同じもしくは前記第２の時刻が前記第１の時刻より早い場合、又は前記第１のメッセージに前記第１のインデックスが含まれる場合において、前記第３のメッセージに含まれるインデックスから前記第１のインデックスを減算した値が１でない場合、前記判定部は前記第１の秘密鍵が不正利用されたと判定する
請求項７に記載の第１の装置。
【請求項９】
第１の装置及び第２の装置と、前記第１の装置及び前記第２の装置を接続するネットワークと、を備える管理システムにおいて用いられる方法であって、
前記第１の装置が、
時刻に関する第１の時刻情報又は所定の検証プロセスの周期を示すインデックスと、第１の秘密鍵に対応する第１の公開鍵又は前記第１の公開鍵の生成に用いられる値と、を含む第１のメッセージと、前記第１のメッセージについてのハッシュ値に対して第２の秘密鍵を用いることにより生成された第１の電子署名とを取得するステップと、
前記第１のメッセージと、前記第１の電子署名と、を前記ネットワークと通信を行うことにより出力するステップと、を含み、
前記第２の装置が、
前記第１のメッセージ、前記第１の電子署名、第２のメッセージ及び第２の電子署名を取得するステップと、
前記時刻に関する情報又は前記インデックスと、前記第１のメッセージ又は前記第２のメッセージを取得する際に、前記第１のメッセージ及び前記第１の電子署名と、前記第２のメッセージおよび前記第２の電子署名と、のいずれかを取得済みであることと、の少なくともいずれかに基づいて、前記第２の秘密鍵が不正利用されたことを判定するステップ

と、を含み、
前記第２のメッセージは、前記第１の公開鍵又は前記第１の公開鍵の生成に用いられる値を少なくとも含み、
前記第２の電子署名は、前記第２のメッセージ及び前記第２の秘密鍵に基づいて生成され、
前記第１の秘密鍵は前記第２の秘密鍵と異なる
方法。
【請求項１０】
ネットワークを介して第２の装置と通信する第１の装置に用いられる方法であって、
時刻に関する第１の時刻情報又は所定の検証プロセスの周期を示すインデックスと、第１の秘密鍵に対応する第１の公開鍵又は前記第１の公開鍵の生成に用いられる値と、を含む第１のメッセージと、前記第１のメッセージについてのハッシュ値に対して第２の秘密鍵を用いることにより生成された第１の電子署名と、を取得するステップと、を備え、
前記第１のメッセージ又は第２のメッセージを取得する際に、前記第１のメッセージ及び前記第１の電子署名と、前記第２のメッセージ及び第２の電子署名と、のいずれかを取得済みであることと、前記第１の時刻情報又は前記インデックスと、の少なくともいずれかに基づいて、前記第２の秘密鍵が不正利用されたことを判定するステップと、を含み、
前記第２のメッセージは、前記第１の公開鍵又は前記第１の公開鍵の生成に用いられる値を少なくとも含み、
前記第２の電子署名は、前記第２のメッセージ及び前記第２の秘密鍵に基づいて生成され、
前記第１の秘密鍵は前記第２の秘密鍵と異なる
方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、管理システム、装置及び方法に関する。
【背景技術】
【０００２】
期待するプログラムがデバイスの中で実行されていることを、遠隔の検証者に検証する方法として、リモートアテステーションがある。例えば、非特許文献１には、最小限のハードウェアと認証用ソフトウェア、デバイス埋め込みの秘密鍵で認証できるハイブリッドリモートアテステーションについて記載されている。
【先行技術文献】
【非特許文献】
【０００３】
【非特許文献１】SMART: Secure and Minimal Architecture for (Establishing a Dynamic) Root of Trust, NDSS Symposium 2012.
【発明の概要】
【発明が解決しようとする課題】
【０００４】
しかしながら、従来のリモートアテステーションにおいては、秘密鍵を攻撃者に盗まれ、または装置の電源を遮断するといった攻撃を受けた場合、セキュリティを担保することが困難になる可能性がある。
【０００５】
本発明は、上記した事情に鑑みてなされたもので、秘密鍵の不正利用ないし盗難又は装置の電源を遮断するといった攻撃を容易に検出し、セキュリティの担保を可能にする管理システム、装置及び方法を提供することを目的の一つとする。
【課題を解決するための手段】
【０００６】

（１）本発明は上記の課題を解決するためになされたものであり、本発明の一態様に係る管理システムは、第１の装置 及び第２の装置 と、前記第１の装置及び前記第２の装置を接続するネットワークと、を備える管理システムであって、前記第１の装置は、時刻に関する第１の時刻情報又は所定の検証プロセスの周期を示す第１のインデックスと、第１の秘密鍵に対応する第１の公開鍵又は前記第１の公開鍵の生成に用いられる値と、を含む第１のメッセージと、前記第１のメッセージについてのハッシュ値に対して第２の秘密鍵を用いることにより生成された第１の電子署名とを取得する第１の取得処理部と、前記第１のメッセージと、前記第１の電子署名と、を前記ネットワークと通信を行うことにより出力する通信部と、を備え、前記第２の装置は、前記第１のメッセージ、前記第１の電子署名、第２のメッセージ及び第２の電子署名を取得する第２の取得部と、前記第１の時刻情報又は前記第１のインデックスと、前記第２の取得部が前記第１のメッセージ又は前記第２のメッセージを取得する際に、前記第１のメッセージ及び前記第１の電子署名と、前記第２のメッセージおよび前記第２の電子署名と、のいずれかを前記第２の取得部が取得済みであることと、の少なくともいずれかに基づいて、前記第２の秘密鍵が不正利用されたことを判定する判定部と、を備え、前記第２のメッセージは、前記第１の公開鍵又は前記第１の公開鍵の生成に用いられる値を少なくとも含み、前記第２の電子署名は、前記第２のメッセージ及び前記第２の秘密鍵に基づいて生成され、前記第１の秘密鍵は前記第２の秘密鍵と異なる。

【０００７】

（２）上記（１）の態様において、前記第１の取得部は、周期ｎにおいて、前記第１のメッセージと、前記第１の電子署名とを取得し、周期ｎ＋１において、時刻に関する第２の時刻情報又は周期ｎ+1に対応する第２のインデックスと、第３の秘密鍵に対応する第３の公開鍵又は前記第３の公開鍵の生成に用いられる値と、を含む第３のメッセージと、前記第３のメッセージについてのハッシュ値に対して前記第１の秘密鍵を用いることにより生成された第３の電子署名と、を取得し、ｎは整数であり、前記第３の秘密鍵は前記第１の秘密鍵及び前記第２の秘密鍵と異なる

請求項１に記載の管理システム。

【０００８】

（３）上記（２）の態様において、前記第１のメッセージは、周期ｎ－１におけるメッセージのハッシュ値をさらに含み、前記第３のメッセージは、前記第１のメッセージのハッシュ値をさらに含む。

【０００９】

（４）上記（３）の態様において、前記第２の時刻情報が示す第２の時刻が、前記第１の時刻情報が示す第１の時刻と同じもしくは前記第２の時刻が前記第１の時刻より早い場合、又は前記第１のメッセージに前記第１のインデックスが含まれる場合において前記第3のメッセージに含まれるインデックスから前記第１のインデックスを減算した値が１でない場合、前記判定部は前記第１の秘密鍵が不正利用されたと判定する。

【００１０】

（５）本発明の一態様に係る第１の装置は、ネットワークを介して第２の装置と通信する第１の装置であって、時刻に関する第１の時刻情報又は所定の検証プロセスの周期を示す第１のインデックスと、第１の秘密鍵に対応する第１の公開鍵又は前記第１の公開鍵の生成に用いられる値と、を含む第１のメッセージと、前記第１のメッセージについてのハッシュ値に対して第２の秘密鍵を用いることにより生成された第１の電子署名と、を取得する取得部と、を備え、前記第１の時刻情報又は前記第１のインデックスと、前記取得部が前記第１のメッセージ又は第２のメッセージを取得する際に、前記第１のメッセージ及び前記第１の電子署名と、前記第２のメッセージ及び第２の電子署名と、のいずれかを前記取得部が取得済みであることと、の少なくともいずれかに基づいて、前記第２の秘密鍵が不正利用されたことを判定する判定部と、を備え、前記第２のメッセージは、前記第１の公開鍵又は前記第１の公開鍵の生成に用いられる値を少なくとも含み、前記第２の電子署名は、前記第２のメッセージ及び前記第２の秘密鍵に基づいて生成され、前記第１の秘

密鍵は前記第２の秘密鍵と異なる。
【００１１】
（６）上記（５）において、前記取得部は、周期ｎにおいて、前記第１のメッセージと、前記第１の電子署名とを取得し、周期ｎ＋１において、時刻に関する第２の時刻情報と、第３の秘密鍵に対応する第３の公開鍵又は前記第３の公開鍵の生成に用いられる値と、を含む第３のメッセージと、前記第３のメッセージについてのハッシュ値に対して前記第１の秘密鍵を用いることにより生成された第３の電子署名とを取得し、ｎは整数であり、前記第３の秘密鍵は前記第１の秘密鍵及び前記第２の秘密鍵と異なる。
【００１２】
（７）上記（６）において、
前記第１のメッセージは、周期ｎ－１におけるメッセージのハッシュ値をさらに含み、前記第３のメッセージは、前記第１のメッセージのハッシュ値をさらに含む
請求項６に記載の第１の装置。
【００１３】
（８）上記（７）において、前記第２の時刻情報が示す第２の時刻が前記第１の時刻情報が示す第１の時刻と同じ又もしくは前記第２の時刻が前記第１の時刻より早い場合、又は前記第１のメッセージに前記第１のインデックスが含まれる場合において、前記第３のメッセージに含まれるインデックスから前記第１のインデックスを減算した値が１でない場合、前記判定部は前記第１の秘密鍵が不正利用されたと判定する。
【００１４】
（９）本発明の一態様に係る方法は、第１の装置及び第２の装置と、前記第１の装置及び前記第２の装置を接続するネットワークと、を備える管理システムにおいて用いられる方法であって、前記第１の装置が、時刻に関する第１の時刻情報又は所定の検証プロセスの周期を示すインデックスと、第１の秘密鍵に対応する第１の公開鍵又は前記第１の公開鍵の生成に用いられる値と、を含む第１のメッセージと、前記第１のメッセージについてのハッシュ値に対して第２の秘密鍵を用いることにより生成された第１の電子署名とを取得するステップと、前記第１のメッセージと、前記第１の電子署名と、を前記ネットワークと通信を行うことにより出力するステップと、を含み、前記第２の装置が、前記第１のメッセージ、前記第１の電子署名、第２のメッセージ及び第２の電子署名を取得するステップと、前記時刻に関する情報又は前記第１のインデックスと、前記第１のメッセージ又は前記第２のメッセージを取得する際に、前記第１のメッセージ及び前記第１の電子署名と、前記第２のメッセージおよび前記第２の電子署名 と、のいずれかを取得済みであることと、の少なくともいずれかに基づいて、前記第２の秘密鍵が不正利用されたことを判定するステップと、を含み、前記第２のメッセージは、前記第１の公開鍵又は前記第１の公開鍵の生成に用いられる値を少なくとも含み、前記第２の電子署名は、前記第２のメッセージ及び前記第２の秘密鍵に基づいて生成され、前記第１の秘密鍵は前記第２の秘密鍵と異なる。
【００１５】
（１０）本発明の一態様に係る方法は、ネットワークを介して第２の装置と通信する第１の装置に用いられる方法であって、時刻に関する第１の時刻情報又は所定の検証プロセスの周期を示すインデックスと、第１の秘密鍵に対応する第１の公開鍵又は前記第１の公開鍵の生成に用いられる値と、を含む第１のメッセージと、前記第１のメッセージについてのハッシュ値に対して第２の秘密鍵を用いることにより生成された第１の電子署名と、を取得するステップと、を備え、前記第１のメッセージ又は第２のメッセージを取得する際に、前記第１のメッセージ及び前記第１の電子署名と、前記第２のメッセージ及び第２の電子署名と、のいずれかを取得済みであることと、前記第１の時刻情報又は前記第１のインデックスと、の少なくともいずれかに基づいて、前記第２の秘密鍵が不正利用されたことを判定するステップと、を含み、前記第２のメッセージは、前記第１の公開鍵又は前記第１の公開鍵の生成に用いられる値を少なくとも含み、前記第２の電子署名は、前記第２のメッセージ及び前記第２の秘密鍵に基づいて生成され、前記第１の秘密鍵は前記第２

の秘密鍵と異なる。
【発明の効果】
【００１６】
本発明の上記態様によれば、秘密鍵の不正利用ないし装置に対する攻撃を容易に検出し、セキュリティの担保を可能にすることができる。
【図面の簡単な説明】
【００１７】
【図１】本発明の第１実施形態における管理システム１の構成の一例を示す図である。
【図２】本発明の第１実施形態におけるＩｏＴ装置１０－１の構成図である。
【図３】本発明の第１実施形態における出力装置３０の構成図である。
【図４】本発明の第１実施形態における秘密鍵の不正利用検出を示す概略図である。
【図５】本発明の第１実施形態におけるＩｏＴ装置１０及びスマートコントラクトの動作を示すフローチャートである。
【図６】本発明の第２実施形態における管理システム１の構成の一例を示す図である。
【図７】本発明の第２実施形態におけるサーバ装置４０の構成図である。
【図８】本発明の第２実施形態におけるＩｏＴ装置１０及びサーバ装置４０の動作を示すフローチャートである。
【図９】本発明の第３実施形態における管理システム１の構成の一例を示す図である。
【図１０】本発明の第３実施形態における状態情報の集計方法の一例を示す図である。
【図１１】本発明の第３実施形態における管理システム１の構成の一例を示す図である。
【図１２】本発明の第３実施形態における状態情報の集計方法の一例を示す図である。
【図１３】本発明の第４実施形態における秘密鍵の不正利用検出を示す概略図である。
【図１４】本発明の第４実施形態における管理システム１の構成の一例を示す図である。
【図１５】本発明の第４実施形態におけるＩｏＴ装置１０及びスマートコントラクトの動作を示すフローチャートである。
【図１６】本発明の第４実施形態におけるＩｏＴ装置１０及びスマートコントラクトの動作を示すフローチャートである。
【図１７】本発明の第４実施形態におけるＩｏＴ装置１０及びスマートコントラクトの動作を示すフローチャートである。
【図１８】本発明の第５実施形態における管理システム１の構成の一例を示す図である。
【図１９】本発明の第５実施形態におけるＩｏＴ装置１０及びサーバ装置４０の動作を示すフローチャートである。
【図２０】本発明の第５実施形態におけるＩｏＴ装置１０及びサーバ装置４０の動作を示すフローチャートである。
【図２１】本発明の第５実施形態におけるＩｏＴ装置１０及びサーバ装置４０の動作を示すフローチャートである。
【図２２】本発明の第６実施形態におけるＩｏＴ装置１０の動作を示すフローチャートである。
【図２３】本発明の第６実施形態におけるＩｏＴ装置１０の動作を示すフローチャートである。
【図２４】本発明の第６実施形態におけるＩｏＴ装置１０の動作を示すフローチャートである。
【図２５】本発明の第６実施形態におけるスマートコントラクトの動作を示すフローチャートである。
【図２６】本発明の第６実施形態におけるスマートコントラクトの動作を示すフローチャートである。
【図２７】本発明の第７実施形態におけるＩｏＴ装置１０の動作を示すフローチャートである。
【図２８】本発明の第７実施形態におけるＩｏＴ装置１０の動作を示すフローチャートである。

【発明を実施するための形態】
【００１８】
以下、図面を参照し、本発明の管理システム、装置及び方法の実施形態について説明する。まず、本発明の第１の実施形態について説明する。
【００１９】
以下、図面を参照し、本発明の管理システム、装置及び方法の実施形態について説明する。まず、本発明の第１の実施形態について説明する。
【００２０】
＜第１の実施形態＞
図１は、本発明の第１の実施形態における管理システム１の構成の一例を示す図である。管理システム１は、ＩｏＴ装置１０－１、ＩｏＴ装置１０－２、ＩｏＴ装置１０－３、ブロックチェーンノード２０－１、ブロックチェーンノード２０－２、ブロックチェーンノード２０－３、ネットワークＮＷ及び出力装置３０を備える。ＩｏＴ装置１０－１～ＩｏＴ装置１０－３、ブロックチェーンノード２０－１～ブロックチェーンノード２０－３及び出力装置３０はネットワークＮＷに接続される。
【００２１】
ＩｏＴ装置１０－１、ＩｏＴ装置１０－２及びＩｏＴ装置１０－３はＩｏＴ（Internet of things）における装置であり、例えばスマートメータである。スマートメータは、電力計であり、測定した電力に関する情報等を他の装置に送信する機能を備える。
【００２２】
ブロックチェーンノード２０－１はＩｏＴ装置１０－１内部の記憶装置にあってもよいし、ネットワークＮＷ内に含まれるいずれかの装置ないしノード内に記憶装置にあってもよい。ブロックチェーンノード２０－２及びブロックチェーンノード２０－３についても同様である。
【００２３】
ネットワークＮＷは、光ファイバ網やメタル線による有線のネットワークでもよいし、ＬＴＥ（Long term evolution、登録商標）、第５世代移動体通信網又はＩＥＥＥ８０２．１１規格に準拠した無線ＬＡＮといった無線ネットワークでもよいし、それらの組み合わせによって構成されていてもよい。ネットワークＮＷは複数の装置ないしノードによって構成される。ネットワークＮＷは、ピア・トゥ・ピア（Ｐ２Ｐ）構成によってブロックチェーンノード２０－１、ブロックチェーンノード２０－２及びブロックチェーンノード２０－３を接続してもよい。
【００２４】
出力装置３０は、ネットワークＮＷ内部又は外部に存在する装置ないしノードに実行させるプログラムを送信する装置である。出力装置３０は、例えばプログラム配信サーバ装置であってもよい。
【００２５】
図２は、本発明の第１実施形態におけるＩｏＴ装置１０－１の構成図である。ＩｏＴ装置１０－１は、機能ブロックとして第１取得部１１－１、第１処理部１２－１、第１表示部１３－１、第１通信部１４－１及び第１記憶部１５－１を備える。ＩｏＴ装置１０－２及びＩｏＴ装置１０－３の構成も同様である。
【００２６】
第１取得部１１－１は、時刻を示す情報及びＩｏＴ装置１０－１の状態を示す状態情報を取得する。第１取得部１１－１は、秘密鍵の生成に用いられる乱数を外部から取得してもよい。
【００２７】
第１処理部１２－１は、メッセージを生成する。また、第１処理部１２－１は、乱数または前のいかなるメッセージからも算出困難な数値を入力として秘密鍵を生成する。もしくは、第１処理部１２－１は、装置を起動した者が予め埋め込んだ秘密鍵をメモリなどから読み取る。第１処理部１２－１は、メッセージに対する電子署名を、秘密鍵を用いて生

成する。

【００２８】

メッセージは、ブロックチェーンに書き込まれてもよいし、何らかの装置に対して送信されてもよい。時刻を示す情報は、例えばタイムスタンプである。「ブロックチェーンに書き込む」とは、データをブロックチェーンのトランザクションプールに登録することをいう。具体的には、「ブロックチェーンに書き込む」とは、複数のブロックチェーンにおけるノードに対してデータを送信し、それら複数のノードがブロックチェーンに書き込むことを指してもよい。ここで、複数のノードとは、ブロックチェーンノード２０－１、ブロックチェーンノード２０－２及びブロックチェーンノード２０－３のいずれでもよい。なお、本実施形態において中継ノードが存在する場合、その中継ノードがブロックチェーンのノードに送信し、そのノードがブロックチェーンにデータを書き込んでもよい。

【００２９】

ブロックチェーンノードは、ブロック生成処理(マイニング処理など)により、トランザクションプールに登録されたデータを保証するブロックを生成する。生成されたブロックはブロックチェーンに取り込まれる。

ここで、メッセージは、ＩｏＴ装置１０－１の状態を示す状態情報、時刻を示す情報、任意の秘密鍵に対応する公開鍵又はその公開鍵の生成に用いられる値、そのメッセージが何個目のものであるかを表すインデックス、前のメッセージのハッシュ値を少なくとも含む。前のメッセージとは、時間的な観点で過去に生成されたメッセージである。

【００３０】

第１表示部１３－１は、情報を表示する。第１表示部１３－１が表示する情報は、例えばスマートメータが設置される住宅における使用電力量であってもよい。第１通信部１４－１は、無線または有線によるネットワークＮＷを介して他の機器と通信可能に接続し、各種のデータの送信および受信を行う。第１通信部１４－１は有線通信インターフェイス又は無線通信インターフェイスである。

【００３１】

有線通信インターフェイスは、電気通信や光通信などが可能なインターフェイスである。有線通信インターフェイスは、例えばイーサネット（登録商標）やＵＳＢ（Ｕｎｉｖｅｒｓａｌ　Ｓｅｒｉａｌ　Ｂｕｓ）（登録商標）に準拠していてもよい。

【００３２】

無線通信インターフェイスは、無線通信が可能なインターフェイスである。無線通信インターフェイスは、例えばＬＴＥでもよいし、第５世代移動体通信網でもよいし、ＩＥＥＥ８０２．１１規格に準拠する無線ＬＡＮインターフェイスでもよいし、Ｂｌｕｅｔｏｏｔｈ（登録商標）に準拠する無線通信インターフェイスでもよい。ＩｏＴ装置１０－２及びＩｏＴ装置１０－３を構成する各機能ブロックの動作についてもＩｏＴ装置１０－１と同様である。本発明において、複数のＩｏＴ装置１０は、ネットワークＮＷ１を介することなく互いに直接通信することが可能である。それぞれのＩｏＴ装置１０は、例えば上記のいずれかの無線通信インターフェイスを用いて互いに直接通信してもよい。

【００３３】

図３は、本発明の第１実施形態における出力装置３０の構成図である。出力装置３０は、入力部３１、処理部３２、記憶部３３及び通信部３４を備える。入力部３１は外部から情報の入力を受け付ける。例えば、入力部３１はマウス、キーボードでもよいし、文字の入力を画面上で受け付けるタッチパネルでもよい。処理部３２は各種処理を実行する。例えば、処理部３２は、記憶部３３に記憶されたプログラムを実行する。又、処理部３２は、通信部３４を介して受信した情報ないしデータを記憶部３３に記憶させる。

【００３４】

記憶部３３は、ＨＤＤ（Ｈａｒｄ　Ｄｉｓｋ　Ｄｒｉｖｅ）、セキュアＮＶＲＡＭ（Ｎｏｎ－Ｖｏｌａｔｉｌｅ　ＲＡＭ）、ＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）などの記憶媒体を含んで構成される。ＨＤＤは、ＯＳ、デバイスドライバ、アプリケーションなどの各種のプログラム、その他、プログラムの動作により取得した各種のデータを記憶

する。

【００３５】

通信部３４は第１通信部１４－１と同様、有線通信インターフェイス又は無線通信インターフェイスである。通信部３４は、ネットワークＮＷに含まれる装置ないしノードに対して、スマートコントラクトによって実行されるプログラムを指定するＩＤおよびプログラムに入力させるデータを送信する。スマートコントラクトとは、ネットワークＮＷに含まれる装置ないしノードに対して、プログラム等を自動的に実行させる機能である。スマートコントラクトに係るプログラムは、予めプログラム毎にユニークなＩＤと共に各ブロックチェーンノードに配布されており、ブロックチェーンノードは、ＩＤの指定を受けることで実行すべきプログラムを一意に特定することができる。

【００３６】

図４は、本発明の第１実施形態における秘密鍵の不正利用検出を示す概略図である。図４における複数の四角形はブロックチェーンを示している。ブロックチェーンは複数のブロックを備える。本発明の第１実施形態において、ＩｏＴ装置１０－１は所定の周期ごとに秘密鍵を更新する。ＩｏＴ装置１０－１は、その秘密鍵に対応する公開鍵又はその公開鍵の生成に用いられる値をメッセージupdateMsg_(x,y)に格納し、当該メッセージupdateMsg_(x,y)を出力する。なお、xはupdateMsg_(x,y) を出力する主体を表し、yはその周期を表す。図４において、デバイスｉが周期ｎにおいて、秘密鍵sk_(i,n) を発行し、メッセージupdateMsg_(i,n)を出力することが示されている。デバイスｉは、周期ｎにおいて、前の秘密鍵sk_(i,n-1) によってメッセージupdateMsg_(i,n) に対する電子署名を作成し、通信部１４を用いてネットワークＮＷ経由でブロックチェーンに書き込む。

【００３７】

図４において、Adversary（攻撃者）はデバイスｉから秘密鍵sk_(i,n) を盗み出している。Adversaryは、周期ｎ終了後に盗み出した秘密鍵sk_(i,n-1) を用いてメッセージupdateMsg'_(i,n) を通信部１４を用いてネットワークＮＷ経由でブロックチェーンに書き込んでいる。上記のように、メッセージupdateMsg’の書き込みが周期ｎの後になるように、公開鍵の更新周期は、物理攻撃によって秘密鍵skを盗み出すのに要する時間より短い時間となるように設計される。この場合、秘密鍵は各周期において１回しか用いられないはずである。つまり、秘密鍵sk_(i,n-1) によって生成された電子署名は１回しかブロックチェーンに書き込まれないのが原則である。しかしながら図４において、秘密鍵sk_(i,n-1) による電子署名は２回ブロックチェーンに書き込まれている。そこで、原則に反するそのような書き込みを検出することにより、秘密鍵sk_(i,n-1)が盗み出されたことを検出することができる。

【００３８】

図５は、本発明の第１実施形態におけるＩｏＴ装置１０及びスマートコントラクトの動作を示すフローチャートである。初期状態において、ｎは1である。ｎは周期を示す整数である。ステップＳ１００において、ＩｏＴ装置１０－１の管理者はコンピュータを用いて乱数を生成する。本実施形態において、乱数の生成方法は特定の方法に限定されるものではない。乱数の生成方法は、その時のある地点での温度の揺らぎなど、物理的な真正乱数を観測するものを含んでいてもよい。第１取得部１１－１は生成された乱数に基づいて秘密鍵の初期値sk_(i,0) 及び対応する公開鍵の初期値pk_(i,0)を、所定のアルゴリズムを用いることにより作成する。ここで所定のアルゴリズムは楕円曲線を利用した暗号方式でもよいし、ＲＳＡ暗号方式でもよい。第１処理部１２－１は、処理をステップＳ１０１に進める。

【００３９】

ステップＳ１０１において、第１取得部１１－１は、タイムスタンプの初期値timestamp_(i,0) ＩｏＴ装置１０－１の状態を示す状態情報の初期値state_(i,0) を取得する。初期状態において前のメッセージupdateMsgは存在しないため、前のupdateMsgのハッシュ値としては予め定めた任意の値を用いる。タイムスタンプは、時刻を示す情報である。状態情報は、プログラムのハッシュ値でもよいし、第１取得部１１－１が取得した特定のセン

サのデータでもよい。この場合、特定のセンサのデータは、特定期間における電力使用量を示す値でもよい。その後、第１取得部１１－１は処理をステップＳ１０２に進める。

【００４０】

ステップＳ１０２において、第１処理部１２－１は、内部に備えるタイマの値をT_attesにセットする。タイマの値が0になったら、第１処理部１２－１は処理をステップＳ１０３に進める。T_attesは、攻撃の有無を周期的に検出する際の各周期の時間である。本実施形態において、攻撃者が秘密鍵を盗むといった攻撃を行う際、2 x T_attes以上の時間を要するものとする。

【００４１】

ステップＳ１０３において、第１処理部１２－１はｎの値を１つインクリメントする。第１処理部１２－１は、処理をステップＳ１０４に進める。

【００４２】

ステップＳ１０４において、第１処理部１２－１は乱数rを生成する。第１処理部１２－１は、生成した乱数rに基づいて周期ｎにおける秘密鍵sk_(i,n) を生成する。ただし、予めsk_(i,n)が生成されておりsk_(i,n)がメモリなどに書き込まれている場合、sk_(i,n) をメモリから読み取る処理に置き換えても良い。第１処理部１２－１は、秘密鍵sk_(i,n) に対応する公開鍵pk_(i,n) を生成する。第１処理部１２－１は、処理をステップＳ１０５に進める。

【００４３】

ステップＳ１０５において、第１取得部１１－１はタイムスタンプ timestamp_(i,n)、状態情報 state_(i,n)及び前の周期で生成されたupdateMsg_(i,n-1)のハッシュ値updateHash_(i,n-1) を取得する。第１取得部１１－１は、処理をステップＳ１０６に進める。

【００４４】

ステップＳ１０６において、第１処理部１２－１は、メッセージ updateMsg_(i,n) 及び電子署名updateSignature_(i,n) を生成する。updateMsg_(i,n) は、ＩｏＴ装置１０－１を識別する識別情報、周期nにおける公開鍵pk_(i,n)、周期nにおける状態情報state_(i,n)、周期nにおけるタイムスタンプtimestamp_(i,n)、updateMsgのインデックスを表すn、前の周期で生成されたupdateMsg_(i,n-1)のハッシュ値updateHash_(i,n-1) を含む。updateMsg_(i,n) は、公開鍵pk_(i,n)の代わりに、公開鍵を特定可能なデータを含んでいてもよいし、公開鍵pk_(i,n) に加えて、公開鍵pk_(i,n)の生成に用いられる乱数値を含んでいてもよい。電子署名updateSignature_(i,n) は、前の周期で生成された秘密鍵sk_(i,n-1) を用いてupdateMsg_(i,n) に対して生成された電子署名である。

【００４５】

なお、電子署名updateSignature_(i,n) は、updateMsg_(i,n) に対して所定のハッシュ関数を用いて得られるハッシュ値に対して、前の周期で生成された秘密鍵sk_(i,n-1) を用いて生成されていてもよい。また、第１取得部１１－１を識別する識別情報は、メッセージupdateMsg_(i,n) に必ずしも含まれていなくてもよい。第１処理部１２－１は、処理をステップＳ１０７に進める。

【００４６】

ステップＳ１０７において、第１処理部１２－１はupdateMsg_(i,n) 及びupdateSignature_(i,n) を通信部１４を用いてネットワークＮＷ経由でブロックチェーンに書き込む。第１処理部１２－１は、処理をステップＳ１０２に進める。

【００４７】

次に、スマートコントラクトの動作を説明する。スマートコントラクトは、ネットワークＮＷ上の装置ないしノードに実装されている。そのような装置ないしノードは、取得部２１、処理部２２、記憶部２３、判定部２４及び通信部２５を備える。処理部２２は、記憶部２３に保存されるスマートコントラクトのプログラムを読み出して実行する。

【００４８】

ステップＳ２００において、処理部２２はタイマの値をT_attesにセットする。処理部２２は、T_attes経過しているか検証し、もしそうであれば処理をステップＳ２０１に進

める。T_attes経過していない場合、処理部２２は以降の処理をキャンセルする。処理部２２はなお、以降の処理ステップにおいて、処理部２２は、プログラムを読み出した時点での所定の時刻に基づいて、各ステップの処理を行ってもよいし、あるいは行わなくてもよい。

【００４９】

ステップＳ２０１において、処理部２２はｎの値を１インクリメントする。その後、処理部２２は処理をステップＳ２０２に進める。

【００５０】

ステップＳ２０２において、取得部２１は、updateMsg_(i,n-1)、updateSignature_(i,n-1)、updateMsg_(i,n) 及びupdateSignature_(i,n) を、通信部１４を用いてネットワークＮＷ経由でブロックチェーンから取得する。updateMsg_(i,n-1) には、第１取得部１１－１を識別する識別情報、周期nにおける公開鍵pk_(i,n-1)、周期n-1における状態情報state_(i,n-1)、周期n-1におけるタイムスタンプtimestamp_(i,n-1) updateMsgのインデックスを表すn-1及び前の周期で生成されたupdateMsg_(i,n-2)のハッシュ値updateHash_(i,n-2)が含まれている。updateMsg_(i,n-1) は、公開鍵pk_(i,n-1)の代わりに、公開鍵を特定可能なデータを含んでいてもよいし、公開鍵pk_(i,n-1) に加えて、公開鍵pk_(i,n-1)の生成に用いられる乱数値を含んでいてもよい。なお、この段階でブロックチェーンから取得したupdatetMsg_(i,n) 及びsignature_(i,n) は真正なものかはわからない。取得部２１は、処理をステップＳ２０３に進める。なお、有効な秘密鍵を所定の周期において取得できなかった場合、取得部２１はその周期における処理を終了し、ステップＳ２００に処理を進める。

【００５１】

ステップＳ２０３において、判定部２４は、演算VerifySignature(pk_(i,n-1), updateMsg_(i,n), updateSignature_(i,n)) を行う。VerifySignature(pk_(i,n-1), updateMsg_(i,n), updateSignature_(i,n)) の値がtrueである場合、判定部２４は処理をステップＳ２０４に進める。VerifySignatureは、updateMsg_(i,n)に対する電子署名updateSignature_(i,n) が、公開鍵pk_(i,n-1)に対応する秘密鍵sk_(i,n-1)によって作成されたものか否かを判定する演算である。VerifySignature(pk_(i,n-1), updateMsg_(i,n), updateSignature_(i,n)) の値がfalseである場合、判定部は処理をステップＳ２０５に進める。

【００５２】

ステップＳ２０４において、判定部２４は、updateMsg_(i,n)に含まれるインデックスから１を減算した値がupdateMsg_(i,n-1) に含まれるインデックスと等しいか否かを判定する。updateMsg_(i,n)に含まれるインデックスから１を減算した値がupdateMsg_(i,n-1) に含まれるインデックスと等しい場合、判定部２４は処理をステップＳ２０６に進め、等しくない場合、判定部２４は処理をステップＳ２１０に進める。

【００５３】

ステップＳ２０５において、判定部２４はメッセージupdateMsg_(i,n)及びupdateSignature_(i,n) を無視し、一切の状態を変更しない。判定部２４は、処理をステップＳ２００に進める。

【００５４】

ステップＳ２０６において、処理部２２は、updateMsg_(i,n-1) のハッシュ値を計算する。判定部２４は、処理部２２が計算したupdateMsg_(i,n-1) のハッシュ値と、updateMsg_(i,n)に含まれるupdateHash_(i,n-1) とが等しいか否かを判定する。その判定結果が等しい場合、判定部２４は処理をステップＳ２０７に進める。その判定結果が等しくない場合、判定部２４は処理をステップＳ２１０に進める。

【００５５】

ステップＳ２０７において、判定部２４はtimestamp_(i,n) がtimestamp_(i,n-1) より大きいか否かを判定する。timestamp_(i,n) がtimestamp_(i,n-1) より大きい場合、判定部２４は処理をステップＳ２０８に進める。timestamp_(i,n) がtimestamp_(i,n-1) と同じかtimestamp_(i,n-1) より小さい場合、判定部２４は処理をステップＳ２１０に進める

。
【００５６】
ステップＳ２０８において、判定部２４は、pk_(i,n-1)を用いた任意のupdateMsg_(i,n) が既にブロックチェーンに書き込まれていないかどうかを判定する。公開鍵pk_(i,n-1)を用いた任意のメッセージupdateMsg_(i,n) がまだブロックチェーンに書き込まれていない場合、判定部２４は処理をステップＳ２０９に進める。公開鍵pk_(i,n-1)を用いた任意のメッセージupdateMsg_(i,n) が既にブロックチェーンに書き込まれていた場合、判定部２４は処理をステップＳ２１０に進める。
【００５７】
ステップＳ２０９において、秘密鍵sk_(i,n-1) が盗まれていないと判定し、判定部２４は変数flag_iに値healthy を代入する。flag_iは、デバイスｉの秘密鍵が盗まれる等不正利用されているか否かを表す変数である。healthyは、デバイスの秘密鍵が不正利用されていないことを表す値である。判定部２４は、その後処理をステップＳ２００に進める。
【００５８】
ステップＳ２１０において、判定部２４は、秘密鍵sk_(i,n-1) が盗まれていると判定し、flag_iに値compromised を代入する。compromisedは、デバイスの秘密鍵が不正利用されている可能性があることを表す値である。判定部２４は、その後処理をステップＳ２００に進める。
【００５９】
なお、ステップＳ２０４からステップＳ２０８の処理は、その順序が変わってもよい。
【００６０】
以上説明した第１実施形態に係る管理システム１は、少なくともＩｏＴ装置１０－１と、スマートコントラクトが実装される装置ないしノードと、ＩｏＴ装置１０－１及びスマートコントラクトが実装される装置ないしノードとを接続するネットワークＮＷを備える。
【００６１】
ＩｏＴ装置１０－１は、時刻に関する情報であるtimestamp_(i,n) 又は検証プロセスの周期を示す第１のインデックスと、第１の秘密鍵sk_(i,n) に対応する第１の公開鍵pk_(i,n)と、を含むメッセージupdateMsg_(i,n) （第１のメッセージの一例）と、メッセージupdateMsg_(i,n)についてのハッシュ値に対して第２の秘密鍵sk_(i,n-1) を用いることにより生成された第１の電子署名updateSignature_(i,n) とを取得する第１処理部と、メッセージupdateMsg_(i,n) と、第１の電子署名updateSignature_(i,n) とを、ネットワークＮＷを介して通信を行うことにより出力する通信部と、を備える。updateMsg_(i,n) は、第1の公開鍵pk_(i,n)の代わりに、第1の公開鍵を特定可能なデータを含んでいてもよいし、第1の公開鍵pk_(i,n) に加えて、第1の公開鍵pk_(i,n)の生成に用いられる乱数値を含んでいてもよい。
【００６２】
ネットワークＮＷにおいてスマートコントラクトが実装された装置は、メッセージupdateMsg_(i,n)、電子署名updateSignature_(i,n)、第２のメッセージ及び第２の電子署名を取得する取得部と、時刻に関する情報timestamp_(i,n) と、前記第２の取得部がupdateMsg_(i,n)又は第２のメッセージを取得する際に、updateMsg_(i,n)及びupdateSignature_(i,n)と、第２のメッセージおよび第２の電子署名と、のいずれかを第２の取得部が取得済みであることと、の少なくともいずれかに基づいて、前記第２の秘密鍵が不正利用されたことを判定する判定部と、を備え、第２のメッセージは、第１の公開鍵pk_(i,n) 又は前記第１の公開鍵pk_(i,n)の生成に用いられる値を少なくとも含み、第２の電子署名は、第２のメッセージ及び第２の秘密鍵sk_(i,n-1)に基づいて生成され、第１の秘密鍵sk_(i,n) は第２の秘密鍵sk_(i,n-1)と異なる。
これにより、秘密鍵の盗難ないし不正利用を検出することが可能になる。
【００６３】

また、第１取得部１１－１は、周期nにおいて、第１のメッセージupdateMsg_(i,n)と、第１の電子署名updateSignature_(i,n) とを取得し、周期n+1において、timestamp_(i,n+1) （時刻に関する第２の時刻情報）又は周期ｎ+1に対応する第２のインデックスと、第３の秘密鍵に対応する第３の公開鍵pk_(i,n+1) とを含む第３のメッセージupdateMsg_(i,n+1)と、updateMsg_(i,n+1)についてのハッシュ値に対して第１の秘密鍵sk_(i,n) を用いることにより生成された第３の電子署名updateSignature_(i,n+1) とを取得し、nは整数であり、第３の秘密鍵sk_(i,n+1) は第１の秘密鍵sk_(i,n)及び前記第２の秘密鍵sk_(i,n-1)と異なる。updateMsg_(i,n+1) は、公開鍵pk_(i,n+1)の代わりに、公開鍵pk_(i,n+1)を特定可能なデータを含んでいてもよいし、公開鍵pk_(i,n+1) に加えて、公開鍵pk_(i,n+1)の生成に用いられる乱数値を含んでいてもよい。

これにより、秘密鍵の盗難ないし不正利用を検出することが可能になる。

【００６４】

また、前記第１のメッセージupdateMsg_(i,n)は、周期ｎ－１におけるメッセージのハッシュ値をさらに含んでもよく、前記第３のメッセージupdateMsg_(i,n+1)は、前記第１のメッセージupdateMsg_(i,n)のハッシュ値をさらに含んでもよい。

これにより、秘密鍵の盗難ないし不正利用を検出することが可能になる。

【００６５】

また、timestamp_(i,n)が示す時刻が、timestamp_(i,n-1)が示す時刻と同じもしくはtimestamp_(i,n) が示す時刻が、timestamp_(i,n-1)が示す時刻より早い場合、又はメッセージupdateMsg_(i,n-1)に周期n-1に対応するインデックスが含まれる場合において前記第３のメッセージに含まれるインデックスから周期n-1に対応するインデックスを減算した値が１でない場合、判定部２４は、秘密鍵sk_(i,n-1)が盗難ないし不正利用されたと判定する。

これにより、秘密鍵の盗難ないし不正利用を検出することが可能になる。

【００６６】

＜第２の実施形態＞

本発明の第２の実施形態について説明する。

図６は、本発明の第２実施形態における管理システム１の構成の一例を示す図である。管理システム１は、ＩｏＴ装置１０Ａ－１、ＩｏＴ装置１０Ａ－２、ＩｏＴ装置１０Ａ－３、ネットワークＮＷ及びサーバ装置４０を備える。第１の実施形態と異なり、管理システム１は、サーバ装置４０を備える。

【００６７】

図７は、本発明の第２実施形態におけるサーバ装置４０の構成図である。サーバ装置４０は、取得部４１、処理部４２、判定部４３、表示部４４及び通信部４５を備える。取得部４１は、ＩｏＴ装置１０Ａ－１、ＩｏＴ装置１０Ａ－２及びＩｏＴ装置１０Ａ－３から出力されるメッセージを取得する。処理部４２は、秘密鍵、公開鍵、及びメッセージに対する秘密鍵を用いた電子署名の作成処理を実行する。

【００６８】

判定部４３は、ＩｏＴ装置１０Ａ－１、ＩｏＴ装置１０Ａ－２及びＩｏＴ装置１０Ａ－３の少なくともいずれかが発行する秘密鍵が盗難ないし不正利用されていないかどうかを秘密鍵、公開鍵、電子署名に基づいて判定する。表示部４４は情報を表示する。表示部４４は例えば液晶ディスプレイでもよいし、有機ＥＬディスプレイでもよい。通信部４５は、無線または有線によるネットワークＮＷを介して他の機器と通信可能に接続し、各種のデータの送信および受信を行う。通信部４５のハードウェア構成は第１通信部１４－１及び通信部３４と同様である。通信部４５は、ＩｏＴ装置１０Ａ－１、ＩｏＴ装置１０Ａ－２及びＩｏＴ装置１０Ａ－３からメッセージ及び公開鍵を受信する。

【００６９】

図８は、本発明の第２実施形態におけるＩｏＴ装置１０Ａ－１及びサーバ装置４０の動作を示すフローチャートである。ＩｏＴ装置１０Ａ－１によるステップＳ２１００からステップＳ２１０６までの動作は、図５におけるステップＳ１００からステップＳ１０６ま

での動作と同様である。第２の実施形態において、ＩｏＴ装置１０Ａ－１、ＩｏＴ装置１０Ａ－２及びＩｏＴ装置１０Ａ－３はブロックチェーンを用いない。Ｓ２１０７において、第１通信部１４－１はupdateMsg_(i,n) 及びupdateSignature_(i,n) を、ネットワークＮＷ１を介してサーバ装置４０に対して出力する。

【００７０】

サーバ装置４０による動作は、第１の実施形態におけるスマートコントラクトによる動作と概ね類似する。本実施形態の処理主体について、特に断りのない限り第１実施形態における取得部２１を取得部４１に、処理部２２を処理部４２に、判定部２４を判定部４３に読み替えるものとする。

【００７１】

ステップＳ２４００及びステップＳ２４０１の動作は、スマートコントラクトによるステップＳ２００及びステップＳ２０１の動作と同様である。ステップＳ２４０２において、通信部４５はupdatetMsg_(i,n) 及びupdateSignature_(i,n) をＩｏＴ装置１０Ａ－１から取得する。通信部４５は、処理をステップＳ２４０３に進める。

【００７２】

ステップＳ２４０３からステップＳ２４１０の動作は、スマートコントラクトによるステップＳ２０３及びステップＳ２１０の動作とそれぞれ同様である。なお、本実施形態において、ステップＳ２４０６の処理は省いてもよい。

【００７３】

以上説明した第２の実施形態に係るサーバ装置４０は、ネットワークＮＷを介してＩｏＴ装置１０Ａ－１と通信する。サーバ装置４０は、時刻に関する情報であるtimestamp_(i,n) 又は所定の検証プロセスの周期を示す第１のインデックスと、第１の秘密鍵sk_(i,n) に対応する第１の公開鍵pk_(i,n)と、を含むメッセージupdateMsg_(i,n) と、メッセージupdateMsg_(i,n)についてのハッシュ値に対して第２の秘密鍵sk_(i,n-1) を用いることにより生成された第１の電子署名updateSignature_(i,n) とを取得する取得部４１を備える。updateMsg_(i,n) は、公開鍵pk_(i,n)の代わりに、公開鍵pk_(i,n)を特定可能なデータを含んでいてもよいし、公開鍵pk_(i,n) に加えて、公開鍵pk_(i,n)の生成に用いられる乱数値を含んでいてもよい。

【００７４】

サーバ装置４０は、時刻に関する情報timestamp_(i,n) と、取得部４１がupdateMsg_(i,n)又は第２のメッセージを取得する際に、updateMsg_(i,n)及びupdateSignature_(i,n) と、第２のメッセージおよび第２の電子署名と、のいずれかを第２の取得部が取得済みであることと、の少なくともいずれかに基づいて、前記第２の秘密鍵が不正利用されたことを判定する判定部４３と、を備える。第２のメッセージは、第１の公開鍵pk_(i,n)または又は前記第１の公開鍵pk_(i,n)の生成に用いられる値を少なくとも含み、第２の電子署名は、第２のメッセージ及び第２の秘密鍵sk_(i,n-1)に基づいて生成され、第１の秘密鍵sk_(i,n)は前記第２の秘密鍵sk_(i,n-1)と異なる。

これにより、秘密鍵の盗難ないし不正利用を検出することが可能になる。

【００７５】

また、取得部４１は、周期nにおいて、メッセージupdateMsg_(i,n)と、updateSignature_(i,n) とを取得し、周期n+１において、timestamp_(i,n+１) と、公開鍵pk_(i,n+１) とを含むupdateMsg_(i,n+１)と、updateMsg_(i,n+1)についてのハッシュ値に対して秘密鍵sk_(i,n) を用いることにより生成された第３の電子署名updateSignature_(i,n+1) とを取得し、nは整数であり、秘密鍵sk_(i,n+1) は前記第１の秘密鍵及び前記第２の秘密鍵と異なる。updateMsg_(i,n+1) は、公開鍵pk_(i,n+1)の代わりに、公開鍵pk_(i,n+1)を特定可能なデータを含んでいてもよいし、公開鍵pk_(i,n+1) に加えて、公開鍵pk_(i,n+1)の生成に用いられる乱数値を含んでいてもよい。

これにより、秘密鍵の盗難ないし不正利用を検出することが可能になる。

【００７６】

また、timestamp_(i,n) が示す時刻がtimestamp_(i,n-1) が示す時刻と同じもしくはti

mestamp_(i,n) が示す時刻がtimestamp_(i,n-1)が示す時刻より早い場合、又は前記第１のメッセージに前記インデックスが含まれる場合において前記第３のメッセージに含まれるインデックスから前記インデックスを減算した値が１でない場合、判定部２４は秘密鍵sk_(i,n-1)が盗難ないし不正利用されたと判定する。

これにより、秘密鍵の盗難ないし不正利用を検出することが可能になる。

【００７７】

＜第３の実施形態＞

本発明の第３の実施形態について、図面を参照して説明する。

図９は、本発明の第３実施形態における管理システム１の構成の一例を示す図である。管理システム１は、ＩｏＴ装置１０Ｂ－１、ＩｏＴ装置１０Ｂ－２、ＩｏＴ装置１０Ｂ－３、ＩｏＴ装置１０Ｂ－４、ＩｏＴ装置１０Ｂ－５、ＩｏＴ装置１０Ｂ－６、ネットワークＮＷ及び出力装置３０Ｂを備える。ＩｏＴ装置１０Ｂ－１、ＩｏＴ装置１０Ｂ－２、ＩｏＴ装置１０Ｂ－３、ＩｏＴ装置１０Ｂ－４、ＩｏＴ装置１０Ｂ－５及びＩｏＴ装置１０Ｂ－６はそれぞれ、ネットワークＮＷを介して出力装置３０Ｂに接続される。また、ＩｏＴ装置１０Ｂ－１～ＩｏＴ装置１０Ｂ－６はリング状の網構成を取っている。各ＩｏＴ装置はＮＷ経由でブロックチェーンに接続される。出力装置３０の構成及び機能は第１の実施形態と同様である。なお、ＩｏＴ装置１０Ｂ-１～ＩｏＴ装置１０Ｂ-６の網構成はリング状に限られず、バス型でもよいし、いずれかの装置を起点とするスター型でもよいし、一部又はフルメッシュ構成でもよい。

【００７８】

第３の実施形態において、各ＩｏＴ装置は取得部１１によって他のＩｏＴ装置を観測することにより、そのＩｏＴ装置の状態を示す状態情報を取得する。これにより、他のＩｏＴ装置がオンラインかオフラインかを確認することを、モニタと称してもよい。なお、ＩｏＴ装置の電源が所定の期間において遮断されていない、かつネットワークとの接続を維持している状態をオンラインと称し、また、ＩｏＴ装置の電源が所定の期間において遮断されている、またはネットワークから切断されている状態をオフラインと称する。図９において、各ＩｏＴ装置は、反時計回り方向に接続されているＩｏＴ装置を観測する。例えば、ＩｏＴ装置１０Ｂ－２はＩｏＴ装置１０Ｂ－１を観測し、取得部１１によってＩｏＴ装置１０Ｂ－１の状態情報を取得する。ＩｏＴ装置１０Ｂ－２は、通信部１４を用いてＩｏＴ装置１０Ｂ－１の状態情報を、通信部１４を用いてネットワークＮＷ経由でブロックチェーンに書き込む。

【００７９】

同様に、ＩｏＴ装置１０Ｂ－３はＩｏＴ装置１０Ｂ－２を観測し、取得部１１によってＩｏＴ装置１０Ｂ－２の状態情報を取得する。ＩｏＴ装置１０Ｂ－２は、ＩｏＴ装置１０Ｂ－１の状態情報を、通信部１４を用いてブロックチェーンに書き込む。なお、各ＩｏＴ装置は、隣接する両隣のＩｏＴ装置を観測してもよい。ＩｏＴ装置１０Ｂ－１は、ＩｏＴ装置１０Ｂ－２及びＩｏＴ装置１０Ｂ－６の状態を観測し、取得部１１によってそれぞれの状態情報を取得し、通信部１４を用いてブロックチェーンに書き込んでもよい。他のＩｏＴ装置についても同様である。

【００８０】

スマートコントラクトが実装された装置ないしノードの取得部２１は、出力装置３０Ｂの通信部３４から出力されるプログラムを取得し、記憶部２３に記憶させる。処理部２２は、記憶部２３からプログラムを読み出し、これから述べる各種処理を実行し、また、取得部２１及び判定部２４に実行させる。なお、処理部２２は、ＩＤの指定を伴うコールによってプログラムを実行してもよい。

【００８１】

取得部２１は、ブロックチェーンに書き込まれた各ＩｏＴ装置の状態情報を取得する。処理部２２は、各ＩｏＴ装置自身が観測した状態情報に基づいて、その観測されたＩｏＴ装置の状態に応じた投票値である第１の値又は第２の値を生成する。第１の値は、ＩｏＴ装置の電源が所定の期間内において遮断されていなかった又はＩｏＴ装置の秘密鍵が盗ま

れる等の不正利用されていなかったと判断されたときの投票値である。第１の値は例えばｋでもよい。ｋは自然数でもよい。ｋは１でもよい。第２の値は、ＩｏＴ装置の電源が所定の期間内において遮断されていた又はＩｏＴ装置の秘密鍵が盗まれる等の不正利用がされていたと判断されたときの投票値である。第２の値は例えば－ｋでもよいし、０でもよい。

【００８２】

図１０は、本発明の第３実施形態における状態情報の集計方法の一例を示す図である。図１０において、最も左に記載されているＩｏＴ装置は、観測される対象のＩｏＴ装置を示す。最も左に記載されているＩｏＴ装置の上に記載されている数字は、そのＩｏＴ装置についての投票値の合算値を示している。例えば、図１０の１行目におけるＩｏＴ装置１０Ｂ－１については投票値の合算値が５であることが示されている。

【００８３】

ここで、ＩｏＴ装置１０Ｂ－１～ＩｏＴ装置１０Ｂ－６はリング状の網構成を取っているので、各ＩｏＴ装置は、隣接するＩｏＴ装置の状態情報を取得する。例えばＩｏＴ装置１０Ｂ－１の状態を観測するのは、直接接続されるＩｏＴ装置１０Ｂ－１である。ＩｏＴ装置１０Ｂ－２がＩｏＴ装置１０Ｂ－１を観測した結果、ＩｏＴ装置１０Ｂ－１の状態情報（第１の状態情報）を取得し、スマートコントラクトが実装された装置ないしノードの取得部２１はその状態情報を取得する。

【００８４】

処理部２２は、ＩｏＴ装置１０Ｂ－１の状態情報に基づいて、投票値として第１の値又は第２の値を生成する。図１０において、処理部２２は、ＩｏＴ装置１０Ｂ－１の状態情報に基づいてＩｏＴ装置１０Ｂ－１の電源が所定の期間内において遮断されていなかったと判断し、第１の値として＋１を生成する。

【００８５】

同様にＩｏＴ装置１０Ｂ－３は、ＩｏＴ装置１０Ｂ－２を観測した結果、ＩｏＴ装置１０Ｂ－２の状態情報（第２の状態情報）を取得し、通信部１４を用いてネットワークＮＷ経由でブロックチェーンに書き込む。スマートコントラクトが実装された装置ないしノードの取得部２１はその状態情報を取得する。

【００８６】

処理部２２は、ＩｏＴ装置１０Ｂ－２の状態情報に基づいて、投票値として第１の値又は第２の値を生成する。図１０において、処理部２２は、ＩｏＴ装置１０Ｂ－２の状態情報に基づいてＩｏＴ装置１０Ｂ－２の電源が所定の期間内において遮断されていなかったと判断し、第１の値として＋１を生成する。

【００８７】

ここで、ＩｏＴ装置１０Ｂ－３がＩｏＴ装置１０Ｂ－１の状態を観測する結果、ＩｏＴ装置１０Ｂ－１の状態情報として第３の状態情報を取得するものと仮定する。しかしながら、ＩｏＴ装置１０Ｂ－３はＩｏＴ装置１０Ｂ－１に直接接続されていないため、ＩｏＴ装置１０Ｂ－３はＩｏＴ装置１０Ｂ－１を直接観測できない。一方、ＩｏＴ装置１０Ｂ－２の電源は、所定の期間内において遮断されていなかったと判断されている。

【００８８】

そこで、ＩｏＴ装置１０Ｂ－３がＩｏＴ装置１０Ｂ－１を観測して取得すると想定していた第３の状態情報は、ＩｏＴ装置１０Ｂ－２がＩｏＴ装置１０Ｂ－１を観測して取得した状態情報（第１の状態情報）が示す情報と同一であると、処理部２２は解釈する。つまり、処理部２２は、ＩｏＴ装置１０Ｂ－１の状態について、ＩｏＴ装置１０Ｂ－２が観測した結果を隣接ＩｏＴ装置１０Ｂ－３は引き継ぐと解釈する。その結果、ＩｏＴ装置１０Ｂ－３はＩｏＴ装置１０Ｂ－１を観測した結果、ＩｏＴ装置１０Ｂ－１の電源は所定の期間内において遮断されていなかったと判断し、処理部２２は第１の値として＋１を生成する。

【００８９】

ＩｏＴ装置１０Ｂ－１の状態に関する観測結果について、他の装置の観測によって得ら

れる状態情報についても同様に、ＩｏＴ装置１０Ｂ－１の状態をＩｏＴ装置１０Ｂ－２以外の他のＩｏＴ装置が観測したものとみなす。処理部２２はＩｏＴ装置１０Ｂ－２以外の他のＩｏＴ装置による観測結果についても、第１の値として＋１を生成する。

【００９０】

処理部２２は、ＩｏＴ装置１０Ｂ－１の状態について、他のＩｏＴ装置からの観測結果に基づいて得られた投票値を全て加算した結果、値として＋５を得る。

【００９１】

ＩｏＴ装置１０Ｂ－２も、同様に、ＩｏＴ装置１０Ｂ－３から直接観測される。ＩｏＴ装置１０Ｂ－２の状態について、ＩｏＴ装置１０Ｂ－３以外の他のＩｏＴ装置も、自装置が直接観測したＩｏＴ装置が取得した状態情報を引き継いだものとして、処理部２２は投票値を生成する。処理部２２は、生成した投票値を合算し、値として＋５を得る。ＩｏＴ装置１０Ｂ－３～ＩｏＴ装置１０Ｂ－６が観測される場合も同様である。

【００９２】

このように、電源が遮断されていないＩｏＴ装置が、隣接する他のＩｏＴ装置であって電源が遮断されていないＩｏＴ装置による観測結果を引き継ぐもの解釈することにより、処理部２２は、各ＩｏＴ装置が、他のＩｏＴ装置の状態を直接観測した場合と同一の観測結果を得ることが出来る。したがって、管理システム１におけるＩｏＴ装置の数が膨大になった場合であっても、少ない情報量と状態情報の取得手順とによって効率よく各ＩｏＴ装置の状態を判断することが出来る。

【００９３】

なお、各ＩｏＴ装置は、観測した状態情報を所定期間内にスマートコントラクトが実装された装置ないしノードに出力する。この所定期間を仮に第１の期間とする。処理部２２は、取得部２１により取得された各ＩｏＴ装置の状態情報に基づいて、所定期間内に第１の値又は第２の値の合算値を算出する。処理部２２が第１の値又は第２の値の合算値を算出する期間を仮に第２の期間とする。第１の期間は第２の期間よりも短い。例えば、第１の期間は３分又は５分といった長さでもよい。第１の期間は、悪意を持った者がＩｏＴ装置を乗っ取るのに必要な時間が第１の期間の２倍以上の時間となるように設計される。一方、第２の期間は、数時間ないし１日といった長さでもよい。

【００９４】

処理部２２は、この加算値の合計が大きいほど、各ＩｏＴ装置の電源が遮断されていなかった可能性が高いと判定する。電源が遮断されていないと判断されるＩｏＴ装置のことを、仮にhealthyな装置であると表現する。電源が遮断されていた判断されるＩｏＴ装置のことを、compromisedな装置であると表現する。ここで、compromisedな装置は、何らかの悪意を持った者に攻撃を受けた結果、電源が遮断されていることがある。

【００９５】

healthyな装置は、healthyな装置を観測する際は、その観測される装置がhealthyな装置と判断されるような状態情報を取得する。また、healthyな装置は、compromisedな装置を観測する際は、その観測される装置がcompromisedな装置と判断されるような状態情報を取得する。

【００９６】

一方、compromisedな装置は、healthyな装置を観測する際は、その観測される装置がcompromisedな装置と判断されるような状態情報を取得及び生成する。また、compromisedな装置は、compromisedな装置を観測する際は、投票の信頼性の低下させるためにその観測される装置がhealthyな装置と判断されるような状態情報を取得及び生成する。

【００９７】

ここで、管理システム１におけるＩｏＴ装置の総数がN、compromisedなデバイスの最大数がaの時、healthyなデバイスについての投票値の合算値の最小値は+1*(N-a-1)+0*a = N-a-1、compromisedなデバイスについての投票値の合算値の最大値は+1*(a-1)+0*(N-a) = a-1である。さらに、N-a-1 > a-1すなわちN>2aの時、sum_v1v2_hea>= N-a-1 > a-1 >= sum_v1v2_comという関係が成り立つ。ここで、sum_v1v2_heaは、healthyな装置についての

投票値の合算値である。sum_v1v2_compは、compromisedな装置についての投票値の合算値である。

【００９８】

以上のことから、過半数のデバイスがhealthyという仮定が成り立つ時、投票値の合算値がN-a-1以上かa-1以下かを判定することにより、処理部２２は、各ＩｏＴ装置が、何らかの悪意を持った者に攻撃を受けた結果、装置の電源が遮断されていたか否かを検証することができる。上記のようなN-a-1及び a-1に基づいて装置がhealthyかcompromisedかを判断する手法は、以下の各実施形態においても同様に用いられてもよい。

【００９９】

図１１は、本発明の第３実施形態における管理システム１の構成の一例を示す図である。図１１のシステム構成と図９のシステム構成との差異は、ＩｏＴ装置１０Ｂ－３及びＩｏＴ装置１０Ｂ－４は悪意を持った者に攻撃を受けた結果、装置の電源が遮断されていたという点である。電源が遮断されていないＩｏＴ装置が他のＩｏＴ装置を観測し、状態情報を取得し、取得した状態情報をスマートコントラクトが実装された装置ないしノードに出力する動作について、図９の場合と差異は無い。

【０１００】

所定期間内において、ＩｏＴ装置１０Ｂ－４の電源が遮断されていた場合、ＩｏＴ装置１０Ｂ－５はＩｏＴ装置１０Ｂ－４の状態情報を取得することが出来ない。そこで、ＩｏＴ装置１０Ｂ－５は電源が遮断されていない他のＩｏＴ装置を見つけるまで、他のＩｏＴ装置を観測し続ける。その結果、電源が遮断されていないＩｏＴ装置が取得する状態情報を引き継ぐ。例えば、ＩｏＴ装置１０Ｂ－３及びＩｏＴ装置１０Ｂ－４の電源は遮断されている。そこでＩｏＴ装置１０Ｂ－１の観測結果については、ＩｏＴ装置１０Ｂ－５はＩｏＴ装置１０Ｂ－２がＩｏＴ装置１０Ｂ－１を観測した結果取得した状態情報を取得部１１によって取得することにより引き継ぐ。

【０１０１】

ここで、ＩｏＴ装置１０Ｂ－３及びＩｏＴ装置１０Ｂ－４は、悪意を持った者に乗っ取られている可能性がある。例えば、ＩｏＴ装置１０Ｂ－３は、ＩｏＴ装置１０Ｂ－２を観測する場合、ＩｏＴ装置１０Ｂ－２の電源が遮断されていると判断されるような状態情報を生成し、通信部１４によって、スマートコントラクトが実装された装置ないしノードに出力する。ＩｏＴ装置１０Ｂ－４は、ＩｏＴ装置１０Ｂ－３を観測する際、ＩｏＴ装置１０Ｂ－３の電源が遮断されていないと判断されるような状態情報を生成し、スマートコントラクトが実装された装置ないしノードに出力する。

【０１０２】

図１２は、本発明の第３実施形態における状態情報の集計方法の一例を示す図である。図１２において、１行目は、ＩｏＴ装置１０Ｂ－１が観測対象である。ＩｏＴ装置１０Ｂ－２がＩｏＴ装置１０Ｂ－１を観測した結果取得する状態情報に基づいて、処理部２２は、ＩｏＴ装置１０Ｂ－２の観測によるＩｏＴ装置１０Ｂ－１について、第１の値として＋１を生成している。

【０１０３】

電源が所定期間において遮断されているＩｏＴ装置１０Ｂ－３は、ＩｏＴ装置１０Ｂ－２によるＩｏＴ装置１０Ｂ－１の観測結果を引き継がない。ＩｏＴ装置１０Ｂ－３は、ＩｏＴ装置１０Ｂ－１の電源が所定期間において遮断されていたということを示す状態情報を生成及び出力する。電源が所定期間において遮断されているＩｏＴ装置１０Ｂ－３も同様に、ＩｏＴ装置１０Ｂ－１の電源が所定期間において遮断されていたということを示す状態情報を生成し、通信部１４を用いることによって出力する。処理部２２は、ＩｏＴ装置１０Ｂ－３及びＩｏＴ装置１０Ｂ－４の観測によるＩｏＴ装置１０Ｂ－１について、第２の値として０を生成している。

【０１０４】

ＩｏＴ装置１０Ｂ－５は、ＩｏＴ装置１０Ｂ－２に接続されている。ＩｏＴ装置１０Ｂ－６は、ＩｏＴ装置１０Ｂ－５に接続されている。ＩｏＴ装置１０Ｂ－２、ＩｏＴ装置１

０Ｂ－５及びＩｏＴ装置１０Ｂ－６は、いずれもその電源が遮断されていない。そこで、ＩｏＴ装置１０Ｂ－５がＩｏＴ装置１０Ｂ－１を観測して取得すると想定していた状態情報は、ＩｏＴ装置１０Ｂ－２がＩｏＴ装置１０Ｂ－１を観測して取得した状態情報が示す情報と同一であると、処理部２２は解釈する。ＩｏＴ装置１０Ｂ－６によるＩｏＴ装置１０Ｂ－１の観測結果についても同様である。

【０１０５】

以上より、ＩｏＴ装置１０Ｂ－１の状態について、処理部２２は、各投票値を合算することにより、＋１を取得する。ＩｏＴ装置１０Ｂ－１以外の他のＩｏＴ装置を観測する場合についても、処理部２２は同様に投票値を合算する。その結果、処理部２２は、ＩｏＴ装置１０Ｂ－２、ＩｏＴ装置１０Ｂ－５及びＩｏＴ装置１０Ｂ－６については＋３、ＩｏＴ装置１０Ｂ－３及びＩｏＴ装置１０Ｂ－４については＋１を生成する。この結果、処理部２２は、ＩｏＴ装置１０Ｂ－３及びＩｏＴ装置１０Ｂ－４はその電源が遮断されており、悪意を持った者に攻撃を受けたことを判断することが出来る。

【０１０６】

以上説明してきたように、本実施形態に係る出力装置は、ＩｏＴ装置１０Ｂ－２（第２の装置の一例）の状態を示す状態情報（第１の状態情報の一例）及びＩｏＴ装置１０Ｂ－１（第３の装置の一例）の状態を示す状態情報（第２の状態情報の一例）の少なくともいずれかを、ＩｏＴ装置１０Ｂ－３の通信部１４（第１の通信部の一例）から取得する第１取得ステップと、第１の状態情報及び第２の状態情報の少なくともいずれかを出力する第１出力ステップと、前記ＩｏＴ装置１０Ｂ－１の状態を示す状態情報（第３の状態情報の一例）及びＩｏＴ装置１０Ｂ－３（第１の装置の一例）の状態を示す状態情報（第４の状態情報の一例）の少なくともいずれかを、ＩｏＴ装置１０Ｂ－２の通信部１４（第２の通信部の一例）から取得する第２取得ステップと、第３の状態情報及び第４の状態情報の少なくともいずれかを出力する第２出力ステップと、第１の装置の状態を示す状態情報（第５の状態情報の一例）及び第２の装置の状態を示す状態情報（第６の状態情報の一例）の少なくともいずれかを、ＩｏＴ装置１０Ｂ－１の通信部１４（第３の通信部の一例）から取得する第３取得ステップと、第５の状態情報及び第６の状態情報の少なくともいずれかを出力する第３出力ステップと、第１出力ステップにおいて出力された第１の状態情報及び第２の状態情報の少なくともいずれか並びに第２出力ステップにおいて出力された第３の状態情報及び第４の状態情報の少なくともいずれかを取得する第４取得ステップと、第４の状態情報に基づいて、第１の装置が発行する秘密鍵が不正利用されたかを判定し、前記第１の状態情報に基づいて、前記第２の装置が発行する秘密鍵が不正利用されたかを判定し、前記第２の状態情報及び前記第３の状態情報の少なくともいずれかに基づいて、前記第３の装置が発行する秘密鍵が不正利用されたか否かを判定する第１判定ステップと、のいずれかを、ブロックチェーンを構成するコンピュータに実行させるためのプログラムを出力する装置であって、

前記第１判定ステップにおいて、前記第２の状態情報が示す情報は前記第３の状態情報が示す情報と同一であると解釈することにより、前記第３の装置が発行する秘密鍵が不正利用されたか否かを判定する。

【０１０７】

このように、電源が遮断されていないＩｏＴ装置が、隣接する他のＩｏＴ装置であって電源が遮断されていないＩｏＴ装置による観測結果を引き継ぐもの解釈することにより、処理部２２は、各ＩｏＴ装置が、他のＩｏＴ装置の状態を直接観測した場合と同一の観測結果を得ることが出来る。したがって、管理システム１におけるＩｏＴ装置の数が膨大になった場合であっても、少ない情報量と状態情報の取得手順とによって効率よく各ＩｏＴ装置の状態を判断することが出来る。

【０１０８】

また、スマートコントラクトが実装された装置ないしノードによって実行されるプログラムは、ＩｏＴ装置１０Ｂ－２（第２の装置の一例）の状態を示す状態情報（第１の状態情報の一例）、ＩｏＴ装置１０Ｂ－１（第３の装置の一例）の状態を示す状態情報（第２

の状態情報の一例）、ＩｏＴ装置１０Ｂ－１の状態を示す状態情報（第３の状態情報の一例）及びＩｏＴ装置１０Ｂ－３（第１の装置の一例）の状態を示す状態情報（第４の状態情報の一例）の少なくともいずれかに基づいては、第１の値又は第２の値を生成する第１生成ステップと、

前記第２の状態情報に基づく第１の値又は第２の値と、前記第３の状態情報に基づく第１の値又は第２の値と、を用いた演算を行うことにより、前記第３の装置が発行する秘密鍵が不正利用されたか否かを判定する判定ステップと、をさらに備え、

前記第１の値は、前記第１の装置、前記第２の装置又は前記第３の装置の電源が所定の期間において遮断されていないと判断されていることを示し、

前記第２の値は、前記第１の装置、前記第２の装置又は前記第３の装置が前記所定の期間において遮断されていると判断されていることを示す。

【０１０９】

このように、電源が遮断されていないＩｏＴ装置が、隣接する他のＩｏＴ装置であって電源が遮断されていないＩｏＴ装置による観測結果を引き継ぐもの解釈することにより、処理部２２は、各ＩｏＴ装置が、他のＩｏＴ装置の状態を直接観測した場合と同一の観測結果を得ることが出来る。したがって、管理システム１におけるＩｏＴ装置の数が膨大になった場合であっても、少ない情報量と状態情報の取得手順とによって効率よく各ＩｏＴ装置の状態を判断することが出来る。

【０１１０】

また、本実施形態において、図９及び図１１の出力装置３０Ｂをサーバ装置４０Ｂ（第４の装置の一例）に置き換えてもよい。この場合、管理システム１においてブロックチェーン、スマートコントラクト及びスマートコントラクトが実装された装置ないしノードは必ずしもなくてもよい。この場合、ＩｏＴ装置１０Ｂ-１～ＩｏＴ装置１０Ｂ-６の各々が観測する他のＩｏＴ装置に関する状態情報を、各ＩｏＴ装置の通信部１４がネットワークＮＷを介してサーバ装置４０Ｂに対して出力する。

【０１１１】

この場合、サーバ装置４０Ｄの通信部４５は、それらの状態情報を各ＩｏＴ装置からネットワークＮＷ経由で受信、取得部４１はそれらの状態情報を取得する。本実施形態において記載した処理部２２及び判定部２４の動作を、サーバ装置４０Ｄの処理部４２及び判定部４３がそれぞれ実行する。

【０１１２】

このように、電源が遮断されていないＩｏＴ装置が、隣接する他のＩｏＴ装置であって電源が遮断されていないＩｏＴ装置による観測結果を引き継ぐもの解釈することにより、処理部２２は、各ＩｏＴ装置が、他のＩｏＴ装置の状態を直接観測した場合と同一の観測結果を得ることが出来る。したがって、管理システム１におけるＩｏＴ装置の数が膨大になった場合であっても、少ない情報量と状態情報の取得手順とによって効率よく各ＩｏＴ装置の状態を判断することが出来る。

【０１１３】

＜第４の実施形態＞

本発明の第４の実施形態について、図面を参照して説明する。

図１３は、本発明の第４実施形態における秘密鍵の不正利用検出を示す概略図である。第４の実施形態において、デバイスｉ及びｊの２つの装置が互いのデバイスを観測してもよいし、隣接するいずれかの装置のみを観測してもよい。例えば、デバイスｊの隣にデバイスｋが接続されている場合、デバイスｉはデバイスｊを観測し、デバイスｊはデバイスｋを観測してもよい。以下、デバイスｉがデバイスｊを観測し、デバイスｊがデバイスｋを観測する関係にある場合、デバイスｉをデバイスｊの観測デバイスであるといい、デバイスｋをデバイスｊの被観測デバイスであるという。デバイスｉは、デバイスｊを観測した結果、デバイスｊの状態を含むメッセージと、そのメッセージ又はメッセージのハッシュ値を秘密鍵により作成した電子署名と、をブロックチェーンに書き込む。処理部２２は、ブロックチェーンを参照することにより、デバイスが悪意を持った者に攻撃を受け、秘

密鍵が盗まれ又は不正利用されたことを判断する。

【０１１４】

図１４は、本発明の第４実施形態における管理システム１の構成の一例を示す図である。各ＩｏＴ装置は、時計回り方向に隣接する他のＩｏＴ装置の状態を観測する点が図９及び図１１と異なる。すなわち、図１４においては、あるＩｏＴ機器に対して時計回り方向に隣接するＩｏＴ機器が被観測デバイスであり、反時計回り方向に隣接するＩｏＴ機器が観測デバイスである。なお、各ＩｏＴ装置は、隣接する両隣のＩｏＴ装置を観測してもよい。ＩｏＴ装置１０Ｂ－１は、ＩｏＴ装置１０Ｂ－２及びＩｏＴ装置１０Ｂ－６の状態を観測し、それぞれの状態情報を取得し、ブロックチェーンに書き込んでもよい。

【０１１５】

同様に、ＩｏＴ装置１０Ｂ－２は、ＩｏＴ装置１０Ｂ－３及びＩｏＴ装置１０Ｂ－１の状態を観測し、それぞれの状態情報を取得してもよい。ＩｏＴ装置１０Ｂ－３は、ＩｏＴ装置１０Ｂ－２及びＩｏＴ装置１０Ｂ－４の状態を観測し、それぞれの状態情報を取得し、ブロックチェーンに書き込んでもよい。他のＩｏＴ装置についても同様である。

【０１１６】

本実施形態において、ＩｏＴ装置１０Ｂ－２がＩｏＴ装置１０Ｂ－３を観測するものとする。図１３におけるデバイスｉ及びｊは、それぞれＩｏＴ装置１０Ｂ－２及びＩｏＴ装置１０Ｂ－３に対応するものとする。ＩｏＴ装置１０Ｂ－２及びＩｏＴ装置１０Ｂ－３の構成は第１実施形態と同様である。

【０１１７】

図１５、図１６及び図１７は、本発明の第４実施形態におけるＩｏＴ装置１０及びスマートコントラクトの動作を示すフローチャートである。

【０１１８】

ステップＳ４１００～ステップＳ４１０４の動作は、第１実施形態におけるステップＳ１００～ステップＳ１０４における動作と同様である。

【０１１９】

ステップＳ４１０５において、ＩｏＴ装置１０Ｂ－２の第２取得部１１－２は、アップデートメッセージupdateMsg_(i,n)、アップデートメッセージupdateMsg_(i,n) のハッシュ値updateHash(i,n) に対する電子署名updateSignature_(i,n)を取得する。また、第２取得部１１－２は、ＩｏＴ装置１０Ｂ－３から、updateHash_(j,n)、pk_(j,n) 及びupdateSignature_(j,n) を取得する。updateMsg_(i,n) は、ＩｏＴ装置１０Ｂ－２を識別する識別情報、周期nにおける公開鍵pk_(i,n)、周期nにおける状態情報state_(i,n)、周期nにおけるタイムスタンプtimestamp_(i,n)、updateMsgのインデックスを表すn及び前の周期で生成されたupdateMsg_(i,n-1)のハッシュ値updateHash_(i,n-1) を含む。updateMsg_(i,n) は、公開鍵pk_(i,n)の代わりに、公開鍵pk_(i,n)を特定可能なデータを含んでいてもよいし、公開鍵pk_(i,n) に加えて、公開鍵pk_(i,n)の生成に用いられる乱数値を含んでいてもよい。第２取得部１１－２は、処理をステップＳ４１０６に進める。

【０１２０】

ステップＳ４１０６において、第２処理部１２－２は、演算VerifySignature(pk_(j,n-1), updateHash(j,n), updateSignature_(j,n)) を行う。 VerifySignatureの結果がtrueの場合、第２処理部１２－２は処理をステップＳ４１０７に進める。VerifySignatureの結果がfalseの場合、第２処理部１２－２は処理をステップＳ４１０８に進める。

【０１２１】

ステップＳ４１０７において、第２取得部１１－２は、updateHash(j,n) を含む reportMsg_(i,n) を取得する。第２取得部１１－２は、処理をステップＳ４１０８に進める。なお、reportMsgというメッセージは、所定の周期におけるデータ又はメッセージのハッシュ値と、そのハッシュ値に対して所定の周期における秘密鍵を用いて生成された電子署名とを含むものである。

【０１２２】

ステップＳ４１０８において、第２取得部１１－２は、timestamp_(i,n) 及び状態情報

state_(i,n) を取得する。第２取得部１１－２は処理をステップＳ４１０９に進める。

【０１２３】

ステップＳ４１０９において、第２取得部１１－２は、updateMsg_(i,n) 及び reportMsg_(i,n) を含むメッセージmsg_(i,n) を取得し、msg_(i,n)について秘密鍵sk_(i,n-1)による電子署名signature_(i,n) を取得する。第２取得部１１－２は、updateMsg_(i,n)について、秘密鍵sk_(i,n-1) を用いて生成された電子署名updateSignature_(i,n) を取得してもよい。第２取得部１１－２は処理をステップＳ４１１０に進める。

【０１２４】

図１６のステップＳ４１１０において、第２処理部１２－２は、メッセージ (msg_(i,n)) 及び電子署名 (signature_ (i,n)) をブロックチェーンに書き込む。第２処理部１２－２は、updateMsg_(i,n)及びupdateSignature_(i,n) だけをブロックチェーンに書き込んでもよい。なお、このタイミングで装置ｊ（ＩｏＴ装置１０Ｂ－３）の第３処理部１２－３も同様に、メッセージ (msg_(j,n))及び電子署名 (signature_(j,n)) をブロックチェーンに書き込む。メッセージmsg_(j,n) は、updateMsg_(j,n) 及び reportMsg_(j,n) を含む。updateMsg_(j,n) は、ＩｏＴ装置１０Ｂ－３を識別する識別情報と、周期nにおける公開鍵pk_(j,n) と、周期nにおける状態情報state_(j,n) と、周期nにおけるタイムスタンプtimestamp_(j,n)又はupdateMsgのインデックスを表すnとと、前の周期で生成されたupdateMsg_(j,n-1)のハッシュ値updateHash_(j,n-1) とを含む。updateMsg_(j,n) は、公開鍵pk_(j,n)の代わりに、公開鍵pk_(j,n)を特定可能なデータを含んでいてもよいし、公開鍵pk_(j,n) に加えて、公開鍵pk_(j,n)の生成に用いられる乱数値を含んでいてもよい。なお、signature_(j,n) は、第３処理部１２－３がmsg_(j,n)について秘密鍵sk_(j,n-1) によって作成する電子署名である。第３処理部１２－３は、updateMsg_(j,n) 及びupdateSignature_(j,n) のみをブロックチェーンに書き込んでもよい。第２処理部１２－２は、処理をステップＳ４１１１に進める。

【０１２５】

ステップＳ４１１１において、第２処理部１２－２は処理をステップＳ４１０２に進める。

【０１２６】

次に、スマートコントラクトの動作を説明する。スマートコントラクトの概要は第１実施形態と同様である。ｎの初期値は1である。

【０１２７】

ステップＳ４２００～ステップＳ４２０１の動作は、第１実施形態におけるステップＳ２００～ステップＳ２０１の動作と同様である。一方、第１実施形態と比較して、ＩｏＴ装置１０Ｂ－２がブロックチェーンから読み込み、又はブロックチェーンに書き込むメッセージに含まれる情報が一部異なる。具体的には、第１実施形態の処理部２２はupdateMsg_(i,n)をブロックチェーンに書き込むが、本実施形態の処理部２２は、updateMsg_(i,n) とreportMsg_(i,n) を含むmsg_(i,n) をブロックチェーンに書き込んでもよい。

【０１２８】

ステップＳ４２０２において、取得部２１はmsg_(i,n-1)、signature_(i,n-1)、msg_(i,n)及びsignature_(i,n)を取得する。取得部２１は、updateMsg_(i,n-1)、updateSignature_(i,n-1)、updateMsg_(i,n)及びupdateSignature_(i,n)のみを取得してもよい。

【０１２９】

ステップＳ４２０３からステップＳ４２１０までの動作は、第１実施形態におけるステップＳ２０３からステップＳ２１０までの動作と同様である。

【０１３０】

図１７のステップＳ４２１１において、判定部２４は、msg_(i,n) に含まれるreportMsg_(i,n)にupdateHash_(j,n-1)が含まれているかどうかを判定する。reportMsg_(i,n)にupdateHash_(j,n)が含まれている場合、判定部２４は処理をステップＳ４２１２に進める。reportMsg_(i,n)にupdateHash_(j,n)が含まれていない場合、判定部２４は処理をステップＳ４２１４に進める。

【０１３１】
ステップＳ４２１２において、判定部２４は、updateHash_(j,n) と updateMsg_(j,n)のハッシュ値とが同じかどうかを判定する。updateHash_(j,n) と updateMsg_(j,n)のハッシュ値とが同じ場合、判定部２４は処理をステップＳ４２１３に進める。updateHash_(j,n) と updateMsg_(j,n)のハッシュ値とが異なる場合、判定部２４は処理をステップＳ４２１４に進める。
【０１３２】
ステップＳ４２１３において、ＩｏＴ装置１０Ｂ-２（デバイスｉ）がＩｏＴ装置１０Ｂ-３（デバイスｊ）に対して賛成票を投票したと判定部２４は判定し、判定結果の合算値を表す変数result_(i) に１を代入する。つまり、ＩｏＴ装置１０Ｂ－２の観測結果からは、ＩｏＴ装置１０Ｂ-３の電源は遮断されていないかつネットワークとの接続を維持していると判定部２４は判定する。判定部２４は、処理をステップＳ４２１５に進める。
【０１３３】
ステップＳ４２１４において、ＩｏＴ装置１０Ｂ-２（デバイスｉ）がＩｏＴ装置１０Ｂ-３（デバイスｊ）に対して反対票を投票したと判定部２４は判定し、結果を表す変数result_(i) に０を合算する。ｉは観測を行う主体の装置を指す。つまり、ＩｏＴ装置１０Ｂ－２の観測結果からは、ＩｏＴ装置１０Ｂ-３の電源は遮断されているまたはネットワークから切断されていると判定部２４は判定する。判定部２４は、処理をステップＳ４２１５に進める。
【０１３４】
ステップＳ４２１５において、判定部２４は、装置ｉに隣接する装置ｈであって、装置ｊではない方の装置（すなわち装置ｉの観測デバイス）の観測による判定結果result_(h)にresult_(i)を代入する。このことは、図１４の例では、ＩｏＴ装置１０Ｂ－１によるＩｏＴ装置１０Ｂ－３の観測結果が、ＩｏＴ装置１０Ｂ－２によるＩｏＴ装置１０Ｂ－３の観測結果を引き継ぐことと等価である。判定部２４は処理をステップＳ４２１６に進める。
【０１３５】
ステップＳ４２１６において、判定部２４は、装置ｈの観測デバイスである装置ｇが装置ｊ（装置ｉの被観測デバイス）ではないことを判断する。装置ｈの観測デバイスが装置ｊではない場合、処理をステップＳ４２１７に進める。装置ｈの観測デバイスｇが装置ｊの場合、全ての集計が終了したことと判定部２４は判断し、処理をステップＳ４２１８に進める。
【０１３６】
ステップＳ４２１７において、判定部２４は、装置hから離れる方向の隣接装置について、装置jに到達するまでステップＳ４２１３及びステップＳ４２１４と同様の処理を実行する。言い換えると、判定部２４は、装置ｉの被観測デバイスに到達するまで、装置ｉから観測デバイスを再帰的にたどりながらステップＳ４２１３及びステップＳ４２１４と同様の処理を実行する。すなわち、ＩｏＴ装置１０Ｂ－３の状態について、ＩｏＴ装置１０Ｂ－４がＩｏＴ装置１０Ｂ－５による観測結果を引き継ぎまで、ステップＳ４２１５及びステップＳ４２１６の処理を実行する。
【０１３７】
ステップＳ４２１８において、判定部２４は、装置ｊ以外の全ての装置による判定結果を取得する。言い換えると、ＩｏＴ装置１０Ｂ－３の状態について、ＩｏＴ装置１０Ｂ－１、ＩｏＴ装置１０Ｂ－２、及びＩｏＴ装置１０Ｂ－４～ＩｏＴ装置１０Ｂ－６による判定結果を合算する。判定部２４は処理をステップＳ４２１９に進める。
【０１３８】
ステップＳ４２１９において、判定部２４は処理をステップＳ４２００に進める。
【０１３９】
以上説明してきたように、本実施形態に係る出力装置において、スマートコントラクトが実装された装置ないしノードによって実行されるプログラムは、時刻に関する情報であ

るtimestamp_(i,n)（第１の時刻情報の一例）と、第１の秘密鍵sk_(i,n)に対応する第１の公開鍵pk_(i,n)又は前記第１の公開鍵pk_(i,n)の生成に用いられる値と、を含むメッセージmsg_(i,n)（第１のメッセージの一例）と、メッセージmsg_(i,n)についてのハッシュ値に対して第２の秘密鍵sk_(i,n-1)を用いることにより生成された第１の電子署名signature_(i,n)とを取得するステップと、メッセージmsg_(i,n)及び第１の電子署名signature_(i,n)と、を出力するステップと、メッセージmsg_(i,n)、電子署名signature_(i,n)、第２のメッセージ及び第２の電子署名を取得するステップと、時刻に関する情報timestamp_(i,n)（第１の時刻情報の一例）と、msg_(i,n)又は第２のメッセージを取得する際に、msg_(i,n)及びsignature_(i,n)と、第２のメッセージおよび第２の電子署名と、のいずれかを取得済みであることと、の少なくともいずれかに基づいて、前記第２の秘密鍵が不正利用されたことを判定するステップと、を備え、第２のメッセージは、第１の公開鍵pk_(i,n)又は前記第１の公開鍵pk_(i,n)の生成に用いられる値を少なくとも含み、第２の電子署名は、第２のメッセージ及び第２の秘密鍵sk_(i,n-1)に基づいて生成され、第１の秘密鍵sk_(i,n)は前記第２の秘密鍵sk_(i,n-1)と異なる。

これにより、秘密鍵の盗難ないし不正利用を検出することが可能になる。

【０１４０】

また、本実施形態に係る出力装置において、スマートコントラクトが実装された装置ないしノードによって実行されるプログラムは、周期nにおいて、メッセージmsg_(i,n)（第１のメッセージの一例）と、signature_(i,n)（第１の電子署名の一例）とを取得し、周期n+1において、timestamp_(i,n+1)（時刻に関する第２の時刻情報の一例）と、公開鍵pk_(i,n+1)（第３の秘密鍵に対応する第３の公開鍵の一例）又は前記第3の公開鍵の生成に用いられる値とを含むmsg_(i,n+1)（第３のメッセージの一例）と、msg_(i,n+1)についてのハッシュ値に対して秘密鍵sk_(i,n)を用いることにより生成されたsignature_(i,n+1)とを取得し、nは整数であり、秘密鍵sk_(i,n+1)（第３の秘密鍵の一例）は前記第１の秘密鍵sk_(i,n)及び前記第２の秘密鍵sk_(i,n-1)と異なる。

これにより、秘密鍵の盗難ないし不正利用を検出することが可能になる。

【０１４１】

また、本実施形態に係る出力装置において、第１のメッセージ（msg_(i,n)又はupdateMsg_(i,n)）は、周期ｎ－１におけるメッセージのハッシュ値（msg_(i,n-１)のハッシュ値又はupdateMsg_(i,n-1)のハッシュ値）をさらに含み、第３のメッセージ（msg_(i,n+1)又はupdateMsg_(i,n+1)）は、前記第１のメッセージのハッシュ値をさらに含む。これにより、秘密鍵の盗難ないし不正利用を検出することが可能になる。

【０１４２】

また、本実施形態に係る出力装置において、スマートコントラクトが実装された装置ないしノードによって実行されるプログラムは、メッセージmsg_(j,n)（時刻に関する第４の時刻情報と、第４の秘密鍵に対応する第４の公開鍵pk_(j,n)又は前記第4の公開鍵pk_(j,n)の生成に用いられる値と、を含む第４のメッセージの一例）と、電子署名signature_(j,n)（前記第４のメッセージについての第４のハッシュ値に対して第５の秘密鍵を用いることにより生成された第４の電子署名の一例）と、を出力する第５出力ステップと、メッセージmsg_(j,n)及び電子署名signature_(j,n)を取得する第９取得ステップと、ＩｏＴ装置１０Ｂ－３（第３の装置の一例）の電源が遮断されていない場合、前記第４の公開鍵pk_(j,n)、前記第４のハッシュ値（第４のメッセージのハッシュ値の一例）及び前記第４の電子署名を取得する第１０取得ステップと、前記第４の電子署名が秘密鍵sk_(j,n-1)（前記第５の秘密鍵の一例）によって第４のハッシュ値に対して署名されていると判定した場合、第４のハッシュ値を第５のハッシュ値として第１のメッセージに含め、前記第１のメッセージを出力する第６出力ステップと、前記第１のメッセージに前記第５のハッシュ値が含まれない場合又は前記第４のメッセージに含まれる第４のハッシュ値が前記第５のハッシュ値と異なる場合、前記第３の装置の電源が遮断されていると判定する第３判定ステップと、を有し、前記第１のメッセージは少なくとも第４のハッシュ値（第３の状態情報の一例）を含み、前記第４の秘密鍵は前記第５の秘密鍵と異なる。

これにより、秘密鍵の盗難ないし不正利用を検出することが可能になる。

【０１４３】

＜第５の実施形態＞

本発明の第５の実施形態について、図面を参照して説明する。

図１８は、本発明の第５実施形態における管理システム１の構成の一例を示す図である。本実施形態においては第４の実施形態の代わりにサーバ装置４０Ｃを備える。サーバ装置４０Ｃは、通信部４５を用いることによりネットワークＮＷを介してＩｏＴ装置１０Ｃ－１～ＩｏＴ装置１０Ｃ－６と通信する。サーバ装置４０Ｃの構成は第２の実施形態と同様である。本実施形態において、第４の実施形態と異なり、秘密鍵の盗難等の不正利用及びＩｏＴ装置の電源遮断等をサーバ装置４０Ｃが検出する。

【０１４４】

図１９、図２０及び図２１は、本発明の第５実施形態におけるＩｏＴ装置１０及びサーバ装置４０Ｃの動作を示すフローチャートである。図１９において、ステップＳ５１００～ステップＳ５１０９の動作は第４の実施形態におけるステップＳ４１００～ステップＳ４１０９の動作と同様である。

【０１４５】

図２０のステップＳ５１１０において、ＩｏＴ装置１０Ｃ－２の通信部１４は、メッセージ（msg_(i,n)）及び電子署名（signature_(i,n)）を出力する。通信部１４は、updateMsg_(i,n)及びupdateSignature_(i,n)だけを出力してもよい。なお、このタイミングで装置ｊ（ＩｏＴ装置１０Ｂ－３）の第３処理部１２－３も同様に、メッセージ（msg_(j,n))及び電子署名（signature_(j,n)）を出力する。メッセージmsg_(j,n)は、updateMsg_(j,n)及びreportMsg_(j,n)を含む。updateMsg_(j,n)は、ＩｏＴ装置１０Ｂ－３を識別する識別情報と、周期nにおける公開鍵pk_(j,n)と、周期nにおける状態情報state_(j,n)と、周期nにおけるタイムスタンプtimestamp_(j,n)又はupdateMsgのインデックスを表すnと、前の周期で生成されたupdateMsg_(j,n-1)のハッシュ値updateHash_(j,n-1)とを含む。updateMsg_(j,n)は、公開鍵pk_(j,n)の代わりに、公開鍵pk_(j,n)を特定可能なデータを含んでいてもよいし、公開鍵pk_(j,n)に加えて、公開鍵pk_(j,n)の生成に用いられる乱数値を含んでいてもよい。通信部１４は、処理をステップＳ５１１１に進める。

【０１４６】

ステップＳ５１１１において、通信部１４は処理をステップＳ５１０２に進める。次に、サーバ装置４０Ｃの動作について説明する。

【０１４７】

ステップＳ５４００～ステップＳ５４０１０の動作は、第２の実施形態におけるステップＳ２４００～ステップＳ２４１０の動作と概ね同様である。一方、第２実施形態と比較して、ＩｏＴ装置１０Ｃ－２が出力し、サーバ装置４０の取得部４１が取得するするメッセージは、第２実施形態におけるupdateMsg_(i,n)にreportMsg_(i,n)を加えたmsg_(i,n)を含む。なお、取得部４１は、updateMsg_(i,n)、reportMsg_(i,n)を別々に受信してもよく、さらにupdateMsg_(i,n)について秘密鍵sk_(i,n-1)によって作成した電子署名updateSignature_(i,n)を取得してもよい。

【０１４８】

図２１のステップＳ５４１１～ステップＳ５４１９における動作は、第４の実施形態におけるスマートコントラクトが実装されたノードないし装置によるステップＳ４２１１～ステップＳ４２１９における動作と同様であるが、本実施形態においては判定処理を実行する主体が判定部４３である点が第４の実施形態と異なる。

【０１４９】

以上説明した第５の実施形態に係るサーバ装置４０Ｃは、ネットワークＮＷを介してＩｏＴ装置１０Ｃ－１～ＩｏＴ装置１０C-６と通信する。ＩｏＴ装置１０Ｃ－１～ＩｏＴ装置１０C-６の取得部１１は、時刻に関する第１の時刻情報又は所定の検証プロセスの周期を示す第1のインデックスと、第１の秘密鍵に対応する第１の公開鍵又は前記第１の公開鍵の生成に用いられる値と、を含む第１のメッセージと、前記第１のメッセージにつ

いての第１のハッシュ値に対して第２の秘密鍵を用いることにより生成された第１の電子署名とを取得する。ＩｏＴ装置１０Ｃ－１～ＩｏＴ装置１０Ｃ-６の通信部１４は、前記第１のメッセージ、前記第１の電子署名を出力する。

【０１５０】

サーバ装置４０は、時刻に関する情報であるtimestamp_(i,n) と、第１の秘密鍵sk_(i,n) に対応する第１の公開鍵pk_(i,n) 又は前記第１の公開鍵pk_(i,n)の生成に用いられる値と、を含むメッセージmsg_(i,n) と、メッセージmsg_(i,n)についてのハッシュ値（第１のハッシュ値の一例）に対して第２の秘密鍵sk_(i,n-1) を用いることにより生成された第１の電子署名signature_(i,n) とを取得する取得部４１（第４取得部の一例）を備える。

【０１５１】

サーバ装置４０は、時刻に関する情報timestamp_(i,n) と、取得部４１がmsg_(i,n)又は第２のメッセージを取得する際に、msg_(i,n)及びsignature_(i,n)と、第２のメッセージおよび第２の電子署名と、のいずれかを第２の取得部が取得済みであることと、の少なくともいずれかに基づいて、第２の秘密鍵が不正利用されたことを判定する判定部４３（第４判定部の一例）と、を備える。つまり、判定部４３は、以下の何れかの処理によって、第２の秘密鍵の不正利用の判定を行う。

・判定部４３は、timestamp_(i,n)に基づいて第2の秘密鍵が不正利用されたことを判定する。

・判定部４３は、取得部がmsg(i,n)を取得する際に、第2の取得部がmsg(i,n)及びsignature(i,n)を取得済みであることに基づいて第2の秘密鍵が不正利用されたことを判定する。

・判定部４３は、取得部が第2のメッセージを取得する際に、第2の取得部が第2のメッセージ及び第2の電子署名を取得済みであることに基づいて第2の秘密鍵が不正利用されたことを判定する。

【０１５２】

第２のメッセージは、第１の公開鍵pk_(i,n) 又は前記第１の公開鍵pk_(i,n)の生成に用いられる値を少なくとも含み、第２の電子署名は、第２のメッセージ及び第２の秘密鍵sk_(i,n-1)に基づいて生成され、第１の秘密鍵sk_(i,n)は前記第２の秘密鍵sk_(i,n-1)と異なる。

これにより、秘密鍵の盗難ないし不正利用を検出することが可能になる。

【０１５３】

また、取得部４１は、周期nにおいて、メッセージmsg_(i,n)と、signature_(i,n) とを取得し、周期n+1において、timestamp_(i,n+1) と、公開鍵pk_(i,n+1) 又はその公開鍵pk_(i,n+1)の生成に用いられる値 とを含むmsg_(i,n+1)と、msg_(i,n+1)についてのハッシュ値に対して秘密鍵sk_(i,n) を用いることにより生成されたsignature_(i,n+1) とを取得する。nは整数であり、秘密鍵sk_(i,n+1) は第１の秘密鍵sk_(i,n)及び第２の秘密鍵sk_(i,n-1)と異なる。

これにより、秘密鍵の盗難ないし不正利用を検出することが可能になる。

【０１５４】

また、本実施形態において、第１のメッセージは、周期ｎ－1におけるメッセージのハッシュ値をさらに含んでもよく、第３のメッセージは、前記第１のメッセージのハッシュ値をさらに含んでもよい。これにより、秘密鍵の盗難ないし不正利用を検出することが可能になる。

【０１５５】

また、本実施形態に係る管理システム１において、ＩｏＴ装置１０Ｃ－３の通信部１４（第３通信部の一例）は、メッセージmsg_(j,n) （時刻に関する第４の時刻情報と、第４の秘密鍵に対応する第４の公開鍵pk_(j,n) 又は前記第4の公開鍵pk_(j,n)の生成に用いられる値と、を含む第４のメッセージの一例）と、電子署名signature_(j,n)（前記第４のメッセージについての第４のハッシュ値に対して第５の秘密鍵を用いることにより生成さ

れた第４の電子署名の一例）と、を出力する。取得部４１（第４取得部の一例）は、メッセージmsg_(j,n)及び電子署名signature_(j,n)を取得する。ＩｏＴ装置１０Ｃ－３（第３の装置の一例）の電源が遮断されていない場合、ＩｏＴ装置１０Ｃ－２の取得部１１は、第４の公開鍵pk_(j,n) 又は前記第4の公開鍵pk_(j,n)の生成に用いられる値、第４のハッシュ値（第４のメッセージのハッシュ値の一例）及び第４の電子署名を取得する。第４の電子署名が秘密鍵sk_(j,n-1)（第５の秘密鍵の一例）によって第４のハッシュ値に対して署名されている場合、ＩｏＴ装置１０Ｃ－２の通信部１４（第２通信部の一例）は、第４のハッシュ値を第５のハッシュ値として第１のメッセージに含め、第１のメッセージを出力する。第１のメッセージに第５のハッシュ値が含まれない場合又は第４のメッセージに含まれる第４のハッシュ値が第５のハッシュ値と異なる場合、判定部４３（第４判定部の一例）は、第３の装置の電源が遮断されていると判定する。第１のメッセージは少なくとも第４のハッシュ値（第３の状態情報の一例）を含み、第４の秘密鍵は第５の秘密鍵と異なる。

これにより、秘密鍵の盗難ないし不正利用、ＩｏＴ装置の電源が遮断されていたこと又はＩｏＴ装置が乗っ取られたことを検出することが可能になる。

【０１５６】

＜第６の実施形態＞

本発明の第６の実施形態について、図面を参照して説明する。

図２２、２３及び２４は、本発明の第６実施形態におけるＩｏＴ装置１０の動作を示すフローチャートである。図２５及び２６は、本発明の第６実施形態におけるサーバ装置４０の動作を示すフローチャートである。本実施形態において、ＩｏＴ装置１０C-１～ＩｏＴ装置１０C-６は、図１８のように論理的に接続されているものとする。

【０１５７】

本実施形態において、ＩｏＴ装置１０C-１～ＩｏＴ装置１０C-６には、装置各々を識別するための固有の識別子が付与されている。この識別子をデバイスＩＤと称してもよい。デバイスＩＤは、装置の番号に応じて昇順に付される。例えば、ＩｏＴ装置１０C-１の装置ＩＤは１、ＩｏＴ装置１０C-２の装置ＩＤは２で、ＩｏＴ装置１０C-６の装置ＩＤは６であるとする。なお、装置ＩＤの付与方法はこれに限られず、ＩｏＴ装置１０C-１の装置ＩＤは１０１、ＩｏＴ装置１０C-２の装置ＩＤは１０２で、ＩｏＴ装置１０C-６の装置ＩＤは１０６でもよい。

【０１５８】

各ＩｏＴ装置は、自身の装置ＩＤより１つ大きい装置ＩＤのＩｏＴ装置を最初にモニタする。例えば、ＩｏＴ装置１０C-１はＩｏＴ装置１０C-２を最初にモニタし、ＩｏＴ装置１０C-２はＩｏＴ装置１０C-３を最初にモニタし、ＩｏＴ装置１０C-５はＩｏＴ装置１０C-６を最初にモニタする。なお、自身の装置ＩＤよりも大きい装置ＩＤが付与されたＩｏＴ装置が無い場合、最小の装置ＩＤが付されたＩｏＴ装置をモニタしてもよい。例えば、ＩｏＴ装置１０C-６は、ＩｏＴ装置１０C-１をモニタしてもよい。

【０１５９】

例えば、装置ＩＤが２のＩｏＴ装置１０C-２がオフラインであったり通信が検閲されたりした場合、第１処理部１２－１は、その装置を今周期にすでにモニタしたもののオンラインと認められなかった装置であることを示す情報をＩｏＴ装置１０C-１の第１記憶部１５－１に保存する。ここで、検閲とは、装置に対する攻撃者（攻撃主体）が、攻撃対象の装置の通信内容（客体）を傍受し、攻撃対象の装置がブロックチェーンのノードにメッセージを書き込むこと、又はサーバ装置４０にメッセージを送信することを妨害することを意味するものとする。その結果、ノード又はサーバ装置は、攻撃対象の装置からのメッセージを受信することが出来なくなる。

【０１６０】

ステップＳ６１００～ステップＳ６１０４の動作はステップＳ１００～ステップＳ１０４の動作と同様である。なお、ステップＳ６１００の処理を開始する段階で、ＩｏＴ装置１０C-２はＩｏＴ装置１０C-４の公開鍵を取得しているものとする。

【０１６１】
ステップＳ６１０５において、第２取得部１１－２はupdateMsg_(i,n) と、updateMsg_(i,n) のハッシュ値であるupdateHash_(i,n) と、updateSignature_(i,n) とを取得する。updateSignature_(i,n) は、updateHash_(i,n) について秘密鍵sk_(i,n-1) を用いて第２処理部１２－２が作成した電子署名である。
【０１６２】
ステップＳ６１０６において、周期ｎにおいてＩｏＴ装置１０Ｃ-２がまだ直接モニタしていない他のＩｏＴ装置のうち、自身の装置ＩＤより大きく、かつ自身の装置ＩＤとの差の絶対値が最も小さい装置ＩＤが付与されている他のＩｏＴ装置の装置ＩＤを取得する。ただし、そのようなIDが存在しない場合、周期ｎにおいてＩｏＴ装置１０Ｃ-２がまだ直接モニタしていない他のＩｏＴ装置のうち、自身の装置IDより小さく、かつ自身の装置IDとの差の絶対値が最も小さい装置ＩＤが付与されている他のＩｏＴ装置の装置ＩＤを取得する。この場合、ＩｏＴ装置１０Ｃ-３がこの条件を満たせば、ＩｏＴ装置１０Ｃ-３の装置ＩＤを第２取得部１１－２は取得する。なお、ＩｏＴ装置１０Ｃ-３の装置ＩＤは３である。第２取得部１１－２は、処理をステップＳ６１０７に進める。
【０１６３】
ステップＳ６１０７において、モニタ周期ｎで、装置ＩＤが３の装置ｊ（ＩｏＴ装置１０Ｃ-３）の公開鍵pk_(j,n-1) が第２記憶部１５－２に記録されているか否かを第２処理部１２－２は判定する。公開鍵pk_(j,n-1) が第２記憶部１５－２に記録されている場合、第２処理部１２－２は処理をステップＳ６１０８に進める。公開鍵pk_(j,n-1) が第２記憶部１５－２に記録されていない場合、第２処理部１２－２は処理をステップＳ６１０９に進める。
【０１６４】
ステップＳ６１０８において、装置ｉ（ＩｏＴ装置１０Ｃ-２）の第２通信部１４－２は、装置j（ＩｏＴ装置１０Ｃ-３）に対して、モニタ開始フラグ及びＩｏＴ装置１０Ｃ-２装置自身の今周期の公開鍵pk_(i,n-1) を送信する。なお、モニタ開始フラグは、相手の装置のモニタを開始することを示すことを示すフラグである。この場合、デバイスi（ＩｏＴ装置１０Ｃ-２）がデバイスｊ（ＩｏＴ装置１０Ｃ-３）をモニタする。第２通信部１４－２は処理をステップＳ６１１２に進める。
【０１６５】
ステップＳ６１０９において、デバイスi（ＩｏＴ装置１０Ｃ-２）の第２通信部１４－２は、デバイスｊ（ＩｏＴ装置１０Ｃ-３）に対して公開鍵要求リクエストを送付する。公開鍵要求リクエストは、ＩｏＴ装置１０Ｃ-３の公開鍵をＩｏＴ装置１０Ｃ-２に送信することを求めるものである。第２通信部１４－２は、処理をステップＳ６１１０に進める。
【０１６６】
ステップＳ６１１０において、第２処理部１２－２は、デバイスｊ（ＩｏＴ装置１０Ｃ-３）の公開鍵pk_(j,n-1) の取得に成功したか否かを判定する。pk_(j,n-1) の取得に成功した場合、第２処理部１２－２は処理をステップＳ６１０８に進める。pk_(j,n-1) の取得に成功しなかった場合、第２処理部１２－２は処理をステップＳ６１１１に進める。
【０１６７】
ステップＳ６１１１において、第２処理部１２－２は、装置ｊ（ＩｏＴ装置１０Ｃ-３）を、「今周期にモニタした装置」として登録する。そして第２処理部１２－２は、オンライン未確認情報を第２記憶部１５－２に保存してもよい。オンライン未確認情報は、モニタされた装置が、今周期にモニタしたがオンラインではなかった、または検閲されていた装置であることを示す情報である。第２処理部１２－２は、処理をステップＳ６１０６に進める。
【０１６８】
ステップＳ６１１２において、第２処理部１２－２は、自身の今周期の秘密鍵sk_(i,n-1)と、装置_j（ＩｏＴ装置１０Ｃ-３）の今周期の公開鍵pk_(j,n-1) とから、装置i（Ｉ

ｏＴ装置１０Ｃ-２）と装置ｊ（ＩｏＴ装置１０Ｃ-３）との共通鍵sharedKey_(i,j,n-1)を計算する。第２処理部１２－２は、処理をステップＳ６１１３に進める。共通鍵の計算にあたっては、例えばディフィー・ヘルマン鍵共有等を用いてもよい。

【０１６９】

ステップＳ６１１３において、updateHash_(j,n) 及びmac_(j,i,n) を所定時間以内に装置ｊ（ＩｏＴ装置１０－３）から直接受信したか否かを第２処理部１２－２は判断する。updateHash_(j,n) は、周期ｎにおけるupdateMsg_(j,n) のハッシュ値である。mac_(j,i,n) は、updateHash_(j,n) 及びsharedKey_(j,i,n-1) から計算されるメッセージ認証符号である。sharedKey_(j,i,n-1)は、装置ｊ（ＩｏＴ装置１０Ｃ-３）自身の今周期の秘密鍵sk_(j,n-1)と、装置_ｉ（ＩｏＴ装置１０Ｃ-２）の今周期の公開鍵pk_(i,n-1)とから計算される共通鍵である。

【０１７０】

updateHash_(j,n) 及びmac_(j,i,n) を所定時間以内に装置ｊ（ＩｏＴ装置１０－３）から直接受信していた場合、第２処理部１２－２は処理をステップＳ６１１４に進める。updateHash_(j,n) 及びmac_(j,i,n) を所定時間以内に装置ｊ（ＩｏＴ装置１０－３）から直接受信しなかった場合、第２処理部１２－２は処理をステップＳ６１１５に進める。

【０１７１】

ステップＳ６１１４において、第２処理部１２－２は、updateHash_(j,n) 及びsharedKey_(i,j,n-1) からmac'_(i,j,n)を計算する。第２処理部１２－２は処理をステップＳ６１１６に進める。

【０１７２】

ステップＳ６１１５の処理はステップＳ６１１１の処理と同様である。

【０１７３】

ステップＳ６１１６において、第２処理部１２－２はmac_(j,i,n) が mac'_(i,j,n) と等しいか否かを判定する。mac_(j,i,n) が mac'_(i,j,n) と等しい場合、第２処理部１２－２はは処理をステップＳ６１１７に進める。mac_(j,i,n) が mac'_(i,j,n) と等しくない場合、第２処理部１２－２は処理をステップＳ６１１８に進める。

【０１７４】

ステップＳ６１１７において、第２通信部１４－２はupdateMsg_(j,n) 及びupdateSignature_(j,n) をサーバ装置４０からダウンロードする。第２通信部１４－２は処理をステップＳ６１１９に進める。

【０１７５】

ステップＳ６１１８における処理はステップＳ６１１１の処理と同様である。

【０１７６】

ステップＳ６１１９において、第２処理部１２－２は、updateMsg_(j,n) 及びupdateSignature_(j,n) をサーバ装置４０からダウンロードすることに成功したか否かを判定する。updateMsg_(j,n) 及びupdateSignature_(j,n) をサーバ装置４０からダウンロードすることに成功した場合、第２処理部１２－２は処理をステップＳ６１２０に進める。updateMsg_(j,n) 及びupdateSignature_(j,n) のいずれか又は双方をサーバ装置４０からダウンロードすることに成功しなかった場合、第２処理部１２－２は処理をステップＳ６１２１に進める。

【０１７７】

ステップＳ６１２０において、updateHash_(j,n) が updateMsg(j,n) のハッシュ値と等しく、かつVerifySignature (pk_(j,n-1),updateHash_(j,n),updateSignature_(j,n)) がtrueか否かを第２処理部１２－２は判定する。updateHash_(j,n) が updateMsg(j,n)のハッシュ値 と等しく、かつVerifySignature (pk_(j,n-1),updateHash_(j,n),updateSignature_(j,n)) がtrueであることの双方が満たされた場合、第２処理部１２－２は処理をステップＳ６１２２に進める。updateHash_(j,n) が updateMsg(j,n)のハッシュ値 と等しく、かつVerifySignature (pk_(j,n-1),updateHash_(j,n),updateSignature_(j,n)) がtrueであることとのいずれか又は双方が満たされなかった場合、第２処理部１２－２は処

理をステップＳ６１２３に進める。
【０１７８】
ステップＳ６１２２において、第２処理部１２－２はmonitoredSignature_(i,j,n) を計算する。monitoredSignature_(i,j,n) は、updateHash_(j,n) に対して秘密鍵sk_(i,n) を用いて第２処理部１２－２が生成する電子署名である。第２処理部１２－２は処理をステップＳ６１２４に進める。
【０１７９】
ステップＳ６１２３における処理はステップＳ６１１１の処理と同様である。
【０１８０】
ステップＳ６１２４において、第２処理部１２－２はモニタ開始フラグを他のデバイスから受信していたかどうかを判定する。モニタ開始フラグを他のデバイスから受信していた場合、第２処理部１２－２は処理をステップＳ６１２５に進める。モニタ開始フラグを他のデバイスから受信していなかった場合、第２処理部１２－２は処理をステップＳ６１２６に進める。
【０１８１】
ステップＳ６１２５において、第２通信部１５－２は、updateMsg_(i,n) 及びupdateSignature_(i,n) をブロードキャストする。なお、ブロードキャストとは、ブロックチェーンノード又はサーバ装置４０に対してＩｏＴ装置が生成する様々な情報を送信することであるとする。ブロードキャストされる情報は、メッセージ、メッセージのハッシュ値、ハッシュ値の電子署名等であり、例えばupdateMsg_(i,n)、updateHash_(i,n) 及びupdateSignature_(i,n) を含む。なお、updateMsg_(i,n) 及びupdateSignature_(i,n) のブロードキャストは、ステップＳ６１０５より後であって、ステップＳ６１２８においてステップＳ６１０２に遷移する前であればどのタイミングでもよい。
【０１８２】
ステップＳ６１２６において、第２通信部１５－２はmonitoredSignature_(i,j,n) をブロードキャストする。第２通信部１５－２は処理をステップＳ６１２７に進める。
【０１８３】
ステップＳ６１２７において、第２処理部１２－２は、装置ｊ（ＩｏＴ装置１０Ｃ-３）を、「今周期にモニタした装置」として登録する。第２処理部１２－２は、オンライン確認情報を第２記憶部１５－２に保存してもよい。オンライン確認情報は、モニタされた装置が、今周期にモニタし、オンラインだった装置であることを示す情報である。第２処理部１２－２は処理をステップＳ６１２８に進める。
【０１８４】
ステップＳ６１２８において、第２処理部１２－２は処理をステップＳ６１０２に進める。
【０１８５】
なお、本実施形態において、ＩｏＴ装置１０Ｃ-２がモニタ主体である装置iで、ＩｏＴ装置１０Ｃ－３がモニタされる装置ｊの場合を主に説明したが、他のＩｏＴ装置も同様にモニタ主体として他の装置をモニタし、同様の処理を実行する。
【０１８６】
続いて、図２５及び２６を用いて、サーバ装置４０の動作について説明する。
【０１８７】
ステップＳ６２００からステップＳ６２０３及びｓ６２０５の動作は、ステップＳ２００からステップＳ２０３及びステップＳ２０５の動作と同様である。
【０１８８】
ステップＳ６２０４において、判定部４３はtimestamp_(i,n) がtimestamp_(i,n-1) より大きいか否かを判定する。timestamp_(i,n) がtimestamp_(i,n-1) より大きい場合、判定部４３は処理をステップＳ６４０６に進める。timestamp_(i,n) がtimestamp_(i,n-1) と同じかtimestamp_(i,n-1) より小さい場合、判定部４３は処理をステップＳ６２０７に進める。

【０１８９】
ステップＳ６２０６において、判定部４３は、pk_(i,n-1)を用いた任意のupdateMsg_(i,n) が生成されていないかどうかを判定する。pk_(i,n-1)を用いた任意のupdateMsg_(i,n) が生成されていた場合、判定部４３は処理をステップＳ６２０７に進める。pk_(i,n-1)を用いた任意のupdateMsg_(i,n) が生成されていない場合、判定部４３は処理をステップＳ６２０８に進める。
【０１９０】
ステップＳ６２０７において、判定部４３は、秘密鍵sk_(i,n-1) が盗まれたと判定し、flag_i に値 compromisedを入力する。判定部４３は、処理をステップＳ６２０８に進める。
【０１９１】
ステップＳ６２０８において、取得部４１はmonitoredSignature(i,j,n) を取得する。取得部４１は、処理をステップＳ６２０９に進める。
【０１９２】
ステップＳ６２０９において、判定部４３は、VerifySignature(pk_(i,n), updateHash_(j,n), monitoredSignature_(i,j,n)) が trueか否かを判定する。判定結果がtrueの場合、判定部４３は処理をステップＳ６２１０に進める。判定結果がfalseの場合、判定部４３は処理をステップＳ６２１１に進める。
【０１９３】
ステップＳ６２１０において、装置i（ＩｏＴ装置１０Ｃ－２）がモニタ対象の装置j（例えばＩｏＴ装置１０Ｃ－３）に賛成票を投票したと判定部４３は判定し、result (i,j) に+1を入力する。判定部４３は処理をステップＳ６２１２に進める。なお、賛成票を投票したとは、モニタ対象の装置がオンラインであったことを示す。
【０１９４】
ステップＳ６２１１において、装置i（ＩｏＴ装置１０Ｃ－２）がモニタ対象の装置j（例えばＩｏＴ装置１０Ｃ－３）に反対票を投票したと判定部４３は判定し、result (i,j) に0を入力する。判定部４３は処理をステップＳ６２１２に進める。なお、反対票を投票したとは、モニタ対象の装置がオフライン又は検閲されていたことを示す。判定部４３は処理をステップＳ６２１２に進める。
【０１９５】
なお、ステップＳ６２０８からステップＳ６２１１までの処理は、モニタ主体の装置ｉ（例えばＩｏＴ装置１０Ｃ－２）が、装置ｊ（例えばＩｏＴ装置１０Ｃ－３）をモニタした際の結果に関する動作だが、ＩｏＴ装置１０Ｃ－３以外の他の装置がモニタ対象の装置ｊである場合についても同様の処理をＩｏＴ装置１０Ｃ－２は行い、result (i,j) を計算する。
【０１９６】
また、ステップＳ６２００からステップＳ６２１１までの処理は、モニタ主体の装置i（例えばＩｏＴ装置１０Ｃ－２）が他の装置をモニタした際の結果に関する動作だが、サーバ装置４０は、装置i以外の他の全ての装置がモニタ主体であった場合についてもステップＳ６２００からステップＳ６２１１までの処理を実行する。
【０１９７】
ステップＳ６１００からステップＳ６１２８及びステップＳ６２００からステップＳ６２１１までの処理の結果、モニタ主体としての各装置（例えば、装置ｉ）が他の装置（例えば装置ｊ）をモニタする際、少なくとも直接モニタすることが出来た装置についてはステップＳ６２０９の結果がtrueならばresult (i,j) として１が得られる。他の装置のうち、直接モニタされなかった装置又は直接モニタしたとしてもステップＳ６２０９の結果がfalseの装置については、result (i,j) として０が得られる。モニタ主体の装置ｉについて、全てのＩｏＴ装置の各々がモニタ主体として、他ののＩｏＴ装置をモニタした場合についても同様に、result (i,j) として１又は０が得られる。
【０１９８】

ステップＳ６２１２において、処理部４２は、result (i,j)=1の時、装置kについてresult(i,k) = result(i,k) or result(j,k) という論理演算により論理和を求める。装置ｋは、装置ｉ（例えばＩｏＴ装置１０Ｃ－２）及び装置ｊ（ＩｏＴ装置１０Ｃ－３）以外の他のＩｏＴ装置（例えば、ＩｏＴ装置１０Ｃ－４～ＩｏＴ装置１０Ｃ－６のいずれか）である。例えば、装置ｉが装置ｊを直接モニタした結果得られたresult (i,j) が１で、装置ｊが装置ｋを直接モニタした結果得られたresult (j,k) が１の場合、result (i,k) = result(i,k) or result(j,k) の結果は１となる。つまり、装置ｉは装置ｋを直接モニタしていないものの、装置ｊが装置ｋを直接モニタした結果を、装置ｉは引き継ぐことが出来る。

【０１９９】

ステップＳ６２１０及びステップＳ６２１１の結果に基づき、ステップＳ６２１２において、処理部４２は装置ｉ及びｊ以外の他のＩｏＴ装置ｋについて、result(i,k) = result(i,k) or result(j,k)の演算により論理和を求める。また、同様に、全装置の各々がモニタ主体であった場合についても同様に、処理部４２はresult (i,k) = result(i,k) or result(j,k) の演算により論理和を求める。処理部４２は、処理をステップＳ６２１３に進める。

【０２００】

ステップＳ６２１３において、処理部４２は、sum(i) = result(0,i) + result(1,i) + … + result(X,i) の演算を行う。ここで、Xは、全装置のうち最大の装置ＩＤである。この場合、各装置に対して付与される装置ＩＤは0、1から始まり、Ｘで終わる。ステップＳ６２１３における演算は、モニタ対象としての装置ｉがhealthyかcompromisedか否かを判定するためのものである。処理部４２は、処理をステップＳ６２１４に進める。

【０２０１】

ステップＳ６２１４において、処理部４２はsum(i)>=N-a-1>a-1がtrueか否かを判定する。判定結果がtrueの場合かつflag_iがhealthyの場合、処理部４２は処理をステップＳ６２１５に進める。判定結果がfalseまたはflag_iがcompromisedの場合、処理部４２は処理をステップＳ６２１６に進める。

【０２０２】

ステップＳ６２１５において、秘密鍵sk_(i,n-1) が盗まれていないと処理部４２は判断し、flag_i に値 healthyを入力する。

【０２０３】

ステップＳ６２１６において、sk_(i,n-1)が盗まれたと処理部４２は判断し、flag_i に値 compromisedを入力する。

【０２０４】

ステップＳ６２１２からステップＳ６２１５までの処理により、処理部４２は、モニタ対象としての装置ｉがhealthyかcompromisedかを推定することができる。

【０２０５】

ステップＳ６２１２からステップＳ６２１５までの処理は、モニタ対象が装置ｉ以外の他の全てのＩｏＴ装置に対しても同様に行われる。

【０２０６】

これにより、管理システム１を構成する各ＩｏＴ装置がhealthyかcompromisedか、すなわち各ＩｏＴ装置の電源が遮断されていないかどうかを確定的に判断することが出来る。

【０２０７】

以上説明した本発明の第６の実施形態に係る管理システム１において、前記第２通信部は、第3の装置のモニタの開始を示すことを示す情報及び前記第2の公開鍵（pk_(i,n-1)）を前記第3の装置に出力する。前記第３処理部は、時刻に関する第６の時刻情報又は所定の検証プロセスの周期を示す第６のインデックスと、第７のメッセージ（updateMsg_(j,n-1)）に含まれる第７の公開鍵（pk_(j,n-1)）又は第７の公開鍵（pk_(j,n-1)の生成に用いられる値と、前記第７のメッセージのハッシュ値（updateHash_(j,n-1)）とを含む第６のメッセージ（updateMsg_(j,n)）を生成する。また、前記第３処理部は、前記第７の公

開鍵（pk_(j,n-1)）に対応する第7の秘密鍵（sk_(j,n-1)）を用いて前記第６のメッセージ（updateMsg_(j,n)）に対する第6の電子署名（updateSignature_(j,n)）を生成する。
さらに、前記第３処理部は、前記第７の秘密鍵sk_(j,n-1)及び第2の公開鍵pk_(i,n-1)を用いて前記第2の装置及び前記第3の装置の共通鍵である第1の共通鍵sharedKey_(j,i,n-1)を生成し、前記第６のメッセージ（updateMsg_(j,n)）に対する第６のハッシュ値（updateHash_(j,n)）及び第1の共通鍵sharedKey_(j,i,n-1) を用いて第１のメッセージ認証符号（mac_(j,i,n)）を生成する。前記第３通信部は、前記第６のメッセージ（updateMsg_(j,n)）及び前記第6の電子署名（updateSignature_(j,n)）を前記第1の装置、前記第2の装置、前記第3の装置及び前記第4の装置以外の他の装置と、前記第4の装置とのいずれかに出力する。前記第２取得部が第６のハッシュ値（updateHash_(j,n)）及び第1のメッセージ認証符号（mac_(j,i,n)）のいずれかを前記第3の装置から取得しなかった場合、前記第２処理部は、前記第３の装置をモニタした装置であることを示す第1の情報を生成し、前記第２通信部は、前記第1の情報を出力する。

これにより、モニタされた装置が今周期にモニタされたもののオンラインではなかった否かを効率よく判定することができ、モニタされた装置の電源が遮断されていたか否かを精度よく推定することが出来る。

【０２０８】

また、本発明の第６の実施形態に係る管理システム１において、前記第２取得部は、前記第６のハッシュ値（updateHash_(j,n)）及び第1のメッセージ認証符号（mac_(j,i,n)）前記第3の装置からを取得し、前記第7の公開鍵（pk_(j,n-1)）、を取得する。前記第２処理部は、前記第2の秘密鍵（sk_(i,n-1)）及び前記第7の公開鍵（pk_(j,n-1)）を用いて第2の共通鍵（sharedKey_(i,j,n-1)）を生成する。また、前記第２処理部は、前記第６のハッシュ値（updateHash_(j,n)）及び前記第2の共通鍵（sharedKey_(i,j,n-1)）を用いて第2のメッセージ認証符号（mac’_(i,j,n)）を生成する。さらに前記第２処理部は、前記第1のメッセージ認証符号（mac_(j,i,n)）が前記第2のメッセージ認証符号（mac’_(i,j,n)）と等しい場合、前記第６のハッシュ値（updateHash_(j,n)）が前記第3の装置から送信されたことを示す第2の情報を生成する。前記第２処理部は、前記第1のメッセージ認証符号（mac_(j,i,n)）が前記第2のメッセージ認証符号（mac’_(i,j,n)）と等しくない場合、前記第３の装置をモニタした装置であることを示す第1の情報を生成する。第２通信部は、前記第1の情報又は前記第2の情報を出力する。

これにより、モニタされた装置が今周期にモニタされたもののオンラインではなかった否かを効率よく判定することができ、モニタされた装置の電源が遮断されていたか否かを精度よく推定することが出来る。

【０２０９】

また、本発明の第６の実施形態に係る管理システム１において、前記第２取得部が前記第６のメッセージ（updateMsg_(j,n)）及び前記第6の電子署名（updateSignature_(j,n)）を所定数以上の前記他の装置と、前記第4の装置とのいずれかから取得しなかった場合、前記第２処理部は前記第1の情報を生成する。

これにより、モニタされた装置が今周期にモニタされたもののオンラインではなかった否かを効率よく判定することができ、モニタされた装置の電源が遮断されていたか否かを精度よく推定することが出来る。

【０２１０】

また、本発明の第６の実施形態に係る管理システム１において、第２取得部が所定数以上の他の装置と、前記第4の装置とのいずれかから取得した前記第６のメッセージ（updateMsg_(j,n)）を基に生成したハッシュ値と、前記第3の装置から取得した第6のハッシュ値（updateHash_(j,n)）とが等しいことと、前記第6の電子署名（updateSignature_(j,n)）が、前記第6のハッシュ値（updateHash_(j,n)）に対して前記第7の秘密鍵（sk_(j,n-1)）を用いて生成されていたこととがいずれも満たされた場合、前記第２処理部は、前記第6のハッシュ値（updateHash_(j,n)）に対して前記第1の秘密鍵（sk_i,n））を用いてモニタに関する第１の電子署名（monitoredSignature_(i,j,n)）を生成し、前記第２通信部は

前記モニタに関する第１の電子署名（monitoredSignature_(i,j,n)）を前記他の装置又は前記第4の装置に出力する。第２取得部が所定数以上の他の装置と、前記第4の装置とのいずれかから取得した前記第６のメッセージ（updateMsg_(j,n)）を基に生成したハッシュ値と、前記第3の装置から取得した第6のハッシュ値（updateHash_(j,n)）とが等しいことと、前記第6の電子署名（updateSignature_(j,n)）が、前記第6のハッシュ値（updateHash_(j,n)）に対して前記第7の秘密鍵（sk_(j,n-1)）を用いて生成されていたこととのいずれかが満たされなかった場合、前記第２処理部は、前記第1の情報を生成し、前記第２通信部は前記第1の情報を出力する。

これにより、モニタされた装置が今周期にモニタされたもののオンラインではなかった否かを効率よく判定することができ、モニタされた装置の電源が遮断されていたか否かを精度よく推定することが出来る。

【０２１１】

また、本発明の第６の実施形態に係る管理システム１において、前記第4取得部は、前記モニタに関する第１の電子署名（monitoredSignature_(i,j,n)）を取得し、前記モニタに関する第１の電子署名（monitoredSignature_(i,j,n)）が、前記第1の秘密鍵（sk_(i,n)）を用いて前記第6のハッシュ値（updateHash_(j,n)）に対して作成された署名であることを前記第４判定部が確認した場合、前記第4処理部は、前記第1の値を生成する。前記モニタに関する第１の電子署名（monitoredSignature_(i,j,n)）が、前記第1の秘密鍵（sk_(i,n)）を用いて前記第6のハッシュ値（updateHash_(j,n)）に対して作成された署名であることを前記第４判定部が確認できなかった場合、前記第4処理部は、前記第2の値を生成し、前記第4通信部は、前記第１の値又は前記第２の値を出力する。

これにより、モニタされた装置の電源が遮断されていたか否かを精度よく推定することが出来る。

【０２１２】

また、本発明の第６実施形態において、サーバ装置の代わりにブロックチェーンに基づくスマートコントラクトが用いられてもよい。すなわち、管理システム１の構成は図１４であってもよい。

【０２１３】

この場合、ＩｏＴ装置側の動作はステップＳ６１００からステップＳ６１２８と同様である。スマートコントラクト側の動作は、原則としてステップＳ６２００からステップＳ６２１６の動作と同様である。この場合、各処理の動作主体を、取得部２１から取得部４１に、処理部２２から処理部４２に、判定部２４から判定部４３にそれぞれ置き換える。

これにより、モニタされた装置の電源が遮断されていたか否かを精度よく推定することが出来る。

【０２１４】

＜第７の実施形態＞

本発明の第７の実施形態について、図面を参照して説明する。

図２７及び２８は、本発明の第７実施形態において管理システム１を構成するＩｏＴ装置１０の動作を示すフローチャートである。本実施形態において、管理システム１の構成は第６の実施形態と同様とする。また、本実施形態においてＩｏＴ装置によって実行される処理はステップＳ７１００からステップＳ７１１２を有する。なお、ステップＳ７１００の処理を開始する段階で、装置ｉ（例えばＩｏＴ装置１０Ｃ-２）は、装置ｊ（例えばＩｏＴ装置１０Ｃ-４）の公開鍵を取得していないものとする。

【０２１５】

ステップＳ７１００からステップＳ７１０４までの処理はステップＳ６１００からステップＳ６１０４迄の動作と同様である。

【０２１６】

ステップＳ７１０５において、装置ｉ（例えばＩｏＴ装置１０Ｃ－２）の第２通信部１４－２は、装置ｋ（例えばＩｏＴ装置１０Ｃ－４）に対して公開鍵要求を送信する。この公開鍵要求は、装置ｋの周期ｎにおける公開鍵pk_(k,n) を装置ｉに対して求めるもので

ある。第２通信部１４－２は処理をステップＳ７１０６に進める。

【０２１７】

ステップＳ７１０６において、第２取得部１１－２は、第２通信部１４－２を用いてupdateMsg_(k,n) 及びmonitoredSignature_(j,k,n) をデバイスkから取得する。第２取得部１１－２は処理をステップＳ７１０７に進める。

【０２１８】

ステップＳ７１０７において、第２処理部１２－２は、updateMsg_(k,n) 及びmonitoredSignature_(j,k,n) をデバイスjから取得したか否かを判定する。updateMsg_(k,n) 及びmonitoredSignature_(j,k,n) をデバイスjから取得した場合、第２処理部１２－２は処理をステップＳ７１０８に進める。updateMsg_(k,n) 及びmonitoredSignature_(j,k,n) をデバイスjから取得していない場合、第２処理部１２－２は処理をステップＳ７１０９に進める。

【０２１９】

ステップＳ７１０８において、第２処理部１２－２はupdateMsg_(k,n)からupdateHash_(k,n) を計算する。第２処理部１２－２は処理をステップＳ７１１０に進める。

【０２２０】

ステップＳ７１０９において、第２処理部１２－２はデバイスｊ（例えばＩｏＴ装置１０Ｃ－３）がオフラインであると判定する。

【０２２１】

ステップＳ７１１０において、第２処理部１２－２は、VerifySignature(pk_(j,n), updateHash_(k,n), monitoredSignature_(j,k,n)) = trueか否かを判定する。判定結果がtrueの場合、第２処理部１２－２は処理をステップＳ７１１１に進める。判定結果がfalseの場合、第２処理部１２－２は処理をステップＳ７１１２に進める。

【０２２２】

ステップＳ７１１１において、updateMsg_(k,n)に含まれるpk_(k,n) がn+1回目の装置認証プロセスにおいて、装置ｋが用いる公開鍵であると第２処理部１２－２は判定する。

【０２２３】

ステップＳ７１１２において、第２処理部１２－２は処理をステップＳ７１０５に進める。

【０２２４】

なお、第7実施形態における管理システム１の構成は、図１４に示す構成でもよい。すなわち、サーバ装置４０の代わりにブロックチェーンが用いられ、管理システム１は出力装置３０を備えていてもよい。

【０２２５】

以上説明した本発明の第７の実施形態に係る管理システム１において、前記第２通信部は、第８の公開鍵（pk_(k,n)）を求める公開鍵要求リクエストを第5の装置に出力する。また、前記第２通信部は、前記第８の公開鍵（pk_(k,n)）又は前記第8の公開鍵(pk_(k,n))の生成に用いられる値 を含む第８のメッセージ（updateMsg_(k,n)）と、モニタに関する第2の電子署名（monitoredSignature_(j,k,n)）とを前記第5の装置から受信する。前記モニタに関する第2の電子署名（monitoredSignature_(j,k,n)）は、前記第８のメッセージのハッシュ値（updateHash_(k,n)）に対して第6の秘密鍵（sk_(j,n)）によって生成され、前記第6の秘密鍵（sk_(j,n)）に対応する第6の公開鍵（pk_(j,n)）又は前記第6の公開鍵pk_(j,n)の生成に用いられる値 は前記第6のメッセージ（updateMsg_(j,n)）に含まれる。前記第8のメッセージ（updateMsg_(k,n)）と、前記モニタに関する第2の電子署名（monitoredSignature_(j,k,n)）とのいずれかを前記第２通信部が受信しなかった場合、前記第２処理部は、前記第3の装置の電源が遮断されている遮断され又はネットワークから切断されていると判断し、前記第8のメッセージ（updateMsg_(k,n)）と、前記モニタに関する第2の電子署名（monitoredSignature_(j,k,n)）とを前記第２通信部が受信し、前記モニタに関する第2の電子署名（monitoredSignature_(j,k,n)）が、前記第6の公開鍵（pk_(j,n)）に対応する第6の秘密鍵（sk_(j,n)）を用いて前記第８のメッセージのハッシ

ュ値（updateHash_(k,n)）に対して生成されたものである場合、前記第2の処理部は、前記第8の公開鍵（pk_(k,n)）が真正であると判断する。

これにより、モニタされた装置の電源が遮断されていたか否かを精度よく推定することに加えて、公開鍵の盗難ないし漏洩があったことを精度よく推定することが出来る。

【０２２６】

以上、この発明の実施形態について図面を参照して詳述してきたが、具体的な構成は上述の実施形態に限られるものではなく、この発明の要旨を逸脱しない範囲の設計等も含まれる。上述の実施形態において説明した各構成は、任意に組み合わせることができる。

【０２２７】

なお、上述したＩｏＴ装置１０は、内部にコンピュータシステムを有していてもよい。そして、上述したＩｏＴ装置１０が備える各構成の機能を実現するためのプログラムをコンピュータ読み取り可能な記録媒体に記録して、この記録媒体に記録されたプログラムをコンピュータシステムに読み込ませ、実行することにより上述したＩｏＴ装置１０が備える各構成における処理を行ってもよい。ここで、「記録媒体に記録されたプログラムをコンピュータシステムに読み込ませ、実行する」とは、コンピュータシステムにプログラムをインストールすることを含む。ここでいう「コンピュータシステム」とは、ＯＳや周辺機器等のハードウェアを含むものとする。また、「コンピュータシステム」は、インターネットやＷＡＮ、ＬＡＮ、専用回線等の通信回線を含むネットワークを介して接続された複数のコンピュータ装置を含んでもよい。また、「コンピュータ読み取り可能な記録媒体」とは、フレキシブルディスク、光磁気ディスク、ＲＯＭ、ＣＤ－ＲＯＭ等の可搬媒体、コンピュータシステムに内蔵されるハードディスク等の記憶装置のことをいう。このように、プログラムを記憶した記録媒体は、ＣＤ－ＲＯＭ等の非一過性の記録媒体であってもよい。

【０２２８】

また、記録媒体には、当該プログラムを配信するために配信サーバからアクセス可能な内部又は外部に設けられた記録媒体も含まれる。なお、プログラムを複数に分割し、それぞれ異なるタイミングでダウンロードした後に電子機器１が備える各構成で合体される構成や、分割されたプログラムのそれぞれを配信する配信サーバが異なっていてもよい。さらに「コンピュータ読み取り可能な記録媒体」とは、ネットワークを介してプログラムが送信された場合のサーバやクライアントとなるコンピュータシステム内部の揮発性メモリ（ＲＡＭ）のように、一定時間プログラムを保持しているものも含むものとする。また、上記プログラムは、上述した機能の一部を実現するためのものであってもよい。さらに、上述した機能をコンピュータシステムに既に記録されているプログラムとの組み合わせで実現できるもの、いわゆる差分ファイル（差分プログラム）であってもよい。

【０２２９】

また、上述した実施形態におけるＩｏＴ装置１０が備える各機能の一部、または全部を、ＬＳＩ（Ｌａｒｇｅ　Ｓｃａｌｅ　Ｉｎｔｅｇｒａｔｉｏｎ）等の集積回路として実現してもよい。各機能は個別にプロセッサ化してもよいし、一部、又は全部を集積してプロセッサ化してもよい。また、集積回路化の手法はＬＳＩに限らず専用回路、または汎用プロセッサで実現してもよい。また、半導体技術の進歩によりＬＳＩに代替する集積回路化の技術が出現した場合、当該技術による集積回路を用いてもよい。

【０２３０】

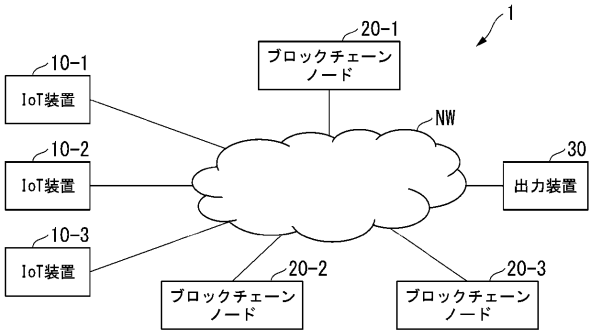
また、上記実施形態のＩｏＴ装置は、スマートメータに限られるものではなく、ネットワークで他の装置と互いに通信可能な組み込み型装置であってもよいし、家庭用電気製品や業務用電気製品にも適用できる。組み込み型装置としては、Micro control unit（MCU）等の小型の演算装置とセンサーなどを搭載したものでもよい。家庭用電気製品としては、テレビや、表示部が備えられた冷蔵庫、電子レンジ等を含むＩｏＴ装置に適用できる。また、上記実施形態のＩｏＴ装置は、任意のコンピュータであってもよく、例えば、携帯電話、スマートフォン、パーソナルコンピュータ、サーバ又はワークステーションでもよい。

【符号の説明】

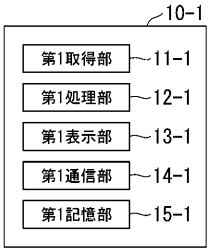
【０２３１】

ＮＷ　ネットワーク、１　管理システム、１０　ＩｏＴ装置、２０　スマートコントラクトが実装された装置ないしノード、３０　出力装置、４０　サーバ装置、１１　取得部、１２　処理部、１３　表示部、１４　通信部、３１　入力部、３２　処理部、３３　記憶部、３４　通信部、４１　取得部、４２　処理部、４３　判定部、４４　表示部、４５　通信部

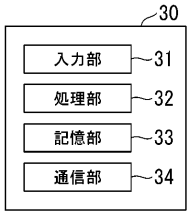
【図１】



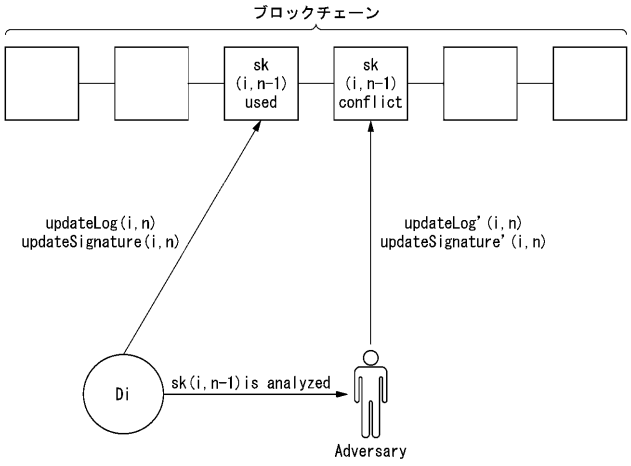
【図２】



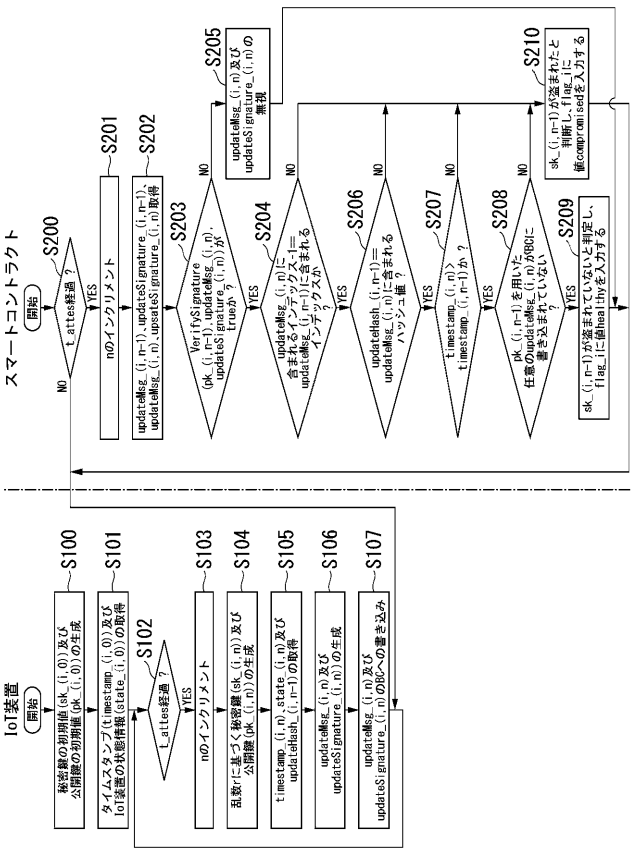
【図３】



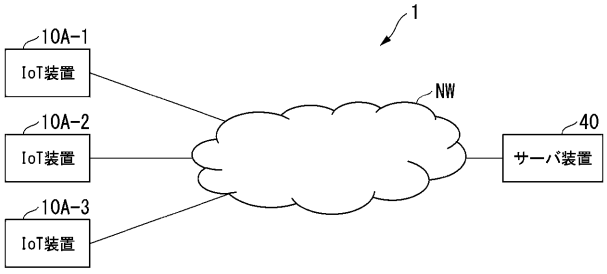
【図４】



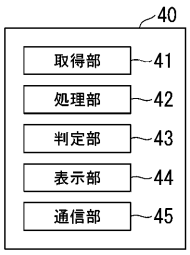
【図５】


スマートコントラクト
開始
t_attes経過？
YES
NO
S200
nのインクリメント
S201
updateMsg_(i,n-1)、updateSignature_(i,n-1)、updateMsg_(i,n)、updateSignature_(i,n)取得
S202
VerifySignature (pk_(i,n-1)、updateMsg_(i,n)、updateSignature_(i,n))がtrueか？
S203
updateMsg_(i,n)及びupdateSignature_(i,n)の無視
S205
updateMsg_(i,n)に含まれるインデックスはupdateMsg_(i,n-1)に含まれるインデックスより大きい？
S204
updateHash_(i,n-1)=updateMsg_(i,n)に含まれるハッシュ値？
S206
timestamp_(i,n)>timestamp_(i,n-1)か？
S207
pk_(i,n-1)を用いたupdateMsg_(i,n)が改ざんされていない
S208
sk_(i,n-1)が盗まれたと判断し、flag_iにcompromisedを入力する
S210
sk_(i,n-1)が盗まれていないと判定し、flag_iに値healthyを入力する
S209
IoT装置
開始
秘密鍵の初期値(sk_(i,0))及び公開鍵の初期値(pk_(i,0))の生成
S100
タイムスタンプ(timestamp_(i,0))及びIoT装置の状態情報(state_(i,0))の取得
S101
t_attes経過？
S102
nのインクリメント
S103
乱数rに基づく秘密鍵(sk_(i,n))及び公開鍵(pk_(i,n))の生成
S104
timestamp_(i,n)、state_(i,n)及びupdateHash_(i,n-1)の取得
S105
updateMsg_(i,n)及びupdateSignature_(i,n)の生成
S106
updateMsg_(i,n)及びupdateSignature_(i,n)の記への書き込み
S107

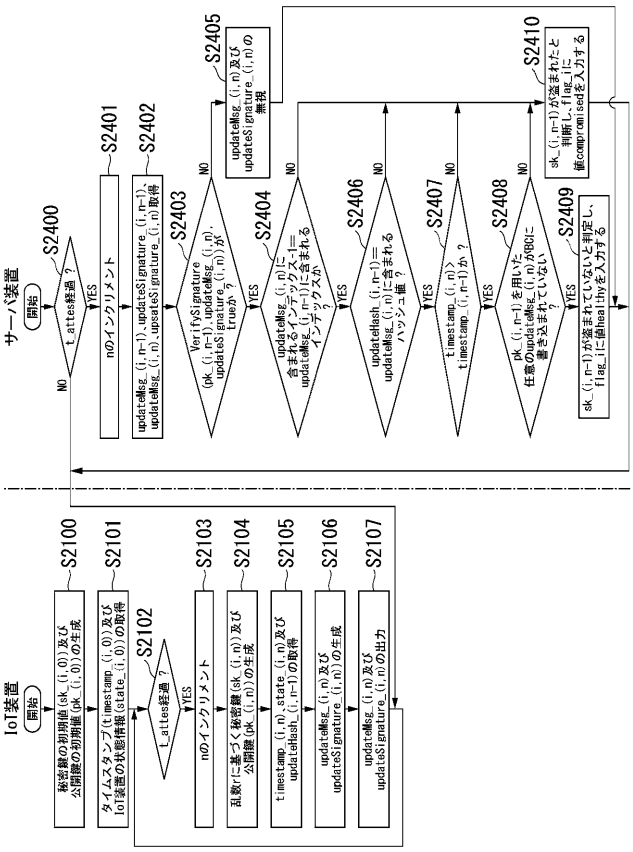
【図６】


1
10A-1
IoT装置
10A-2
IoT装置
10A-3
IoT装置
NW
40
サーバ装置

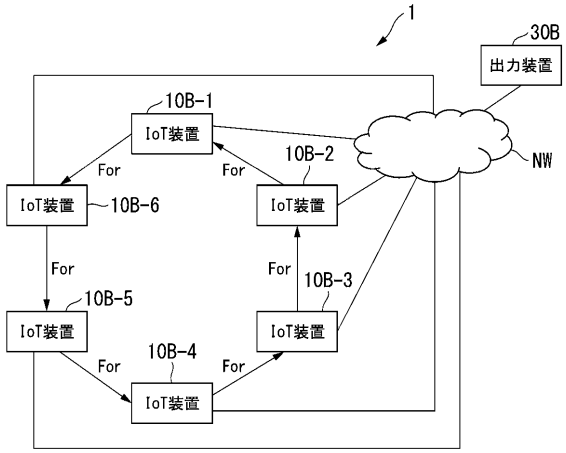
【図７】


40
取得部
41
処理部
42
判定部
43
表示部
44
通信部
45

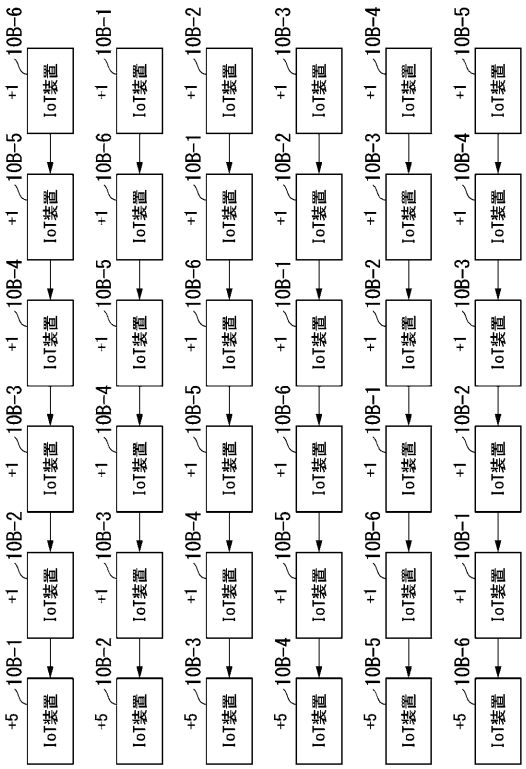
【図８】


サーバ装置
開始
t_attes経過？
YES
NO
S2400
nのインクリメント
S2401
updateMsg_(i,n-1)、updateSignature_(i,n-1)、updateMsg_(i,n)、updateSignature_(i,n)取得
S2402
VerifySignature (pk_(i,n-1)、updateMsg_(i,n)、updateSignature_(i,n))がtrueか？
S2403
updateMsg_(i,n)及びupdateSignature_(i,n)の無視
S2405
updateMsg_(i,n)に含まれるインデックスはupdateMsg_(i,n-1)に含まれるインデックスより大きい？
S2404
updateHash_(i,n-1)=updateMsg_(i,n)に含まれるハッシュ値？
S2406
timestamp_(i,n)>timestamp_(i,n-1)か？
S2407
pk_(i,n-1)を用いたupdateMsg_(i,n)が改ざんされていない
S2408
sk_(i,n-1)が盗まれたと判断し、flag_iにcompromisedを入力する
S2410
sk_(i,n-1)が盗まれていないと判定し、flag_iに値healthyを入力する
S2409
IoT装置
開始
秘密鍵の初期値(sk_(i,0))及び公開鍵の初期値(pk_(i,0))の生成
S2100
タイムスタンプ(timestamp_(i,0))及びIoT装置の状態情報(state_(i,0))の取得
S2101
t_attes経過？
S2102
nのインクリメント
S2103
乱数に基づく秘密鍵(sk_(i,n))及び公開鍵(pk_(i,n))の生成
S2104
timestamp_(i,n)、state_(i,n-1)の取得
S2105
updateMsg_(i,n)及びupdateSignature_(i,n)の生成
S2106
updateMsg_(i,n)及びupdateSignature_(i,n)の出力
S2107

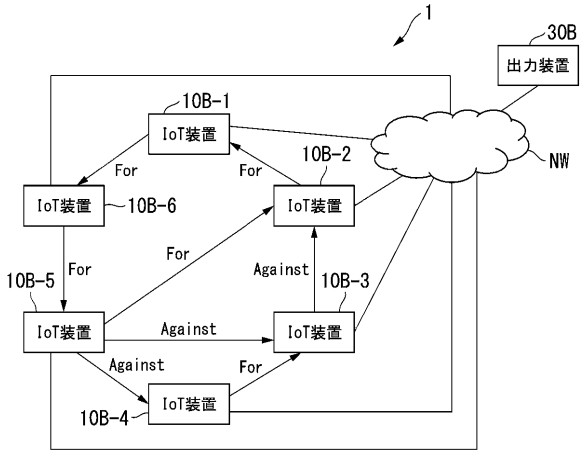
【図９】


1
30B
出力装置
10B-1
IoT装置
10B-2
IoT装置
NW
For
IoT装置
10B-6
IoT装置
For
For
10B-3
For
10B-5
IoT装置
IoT装置
For
10B-4
For
IoT装置

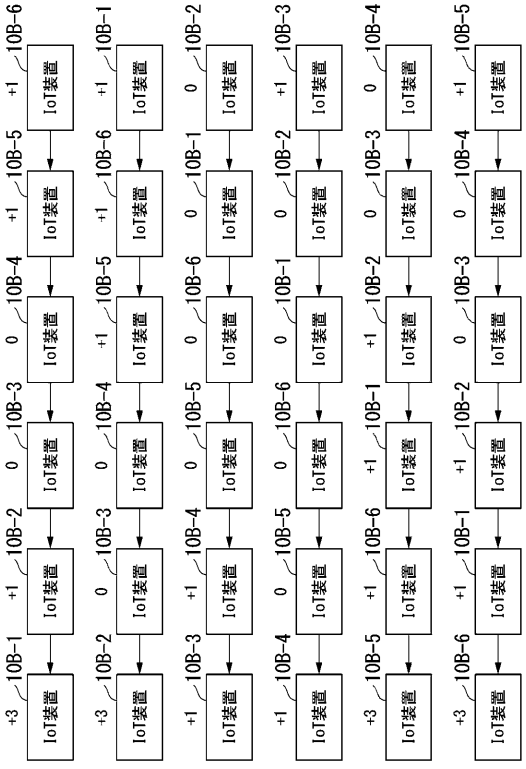
【図１０】



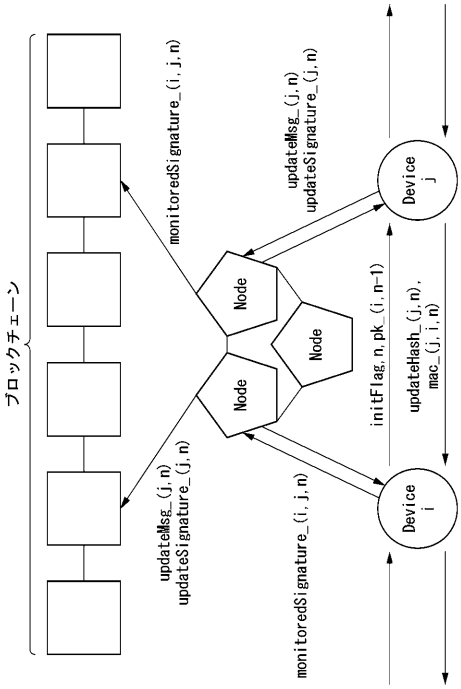
【図１１】



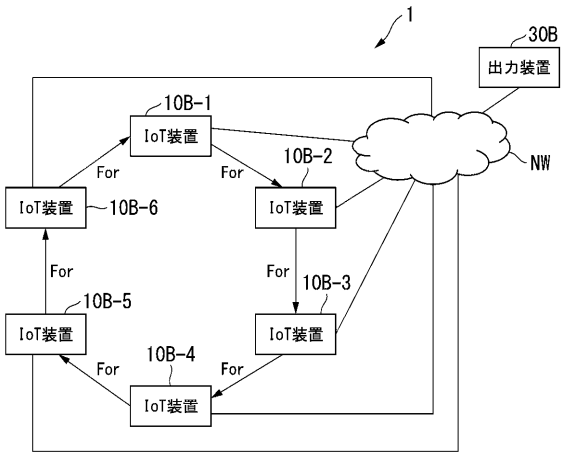
【図１２】



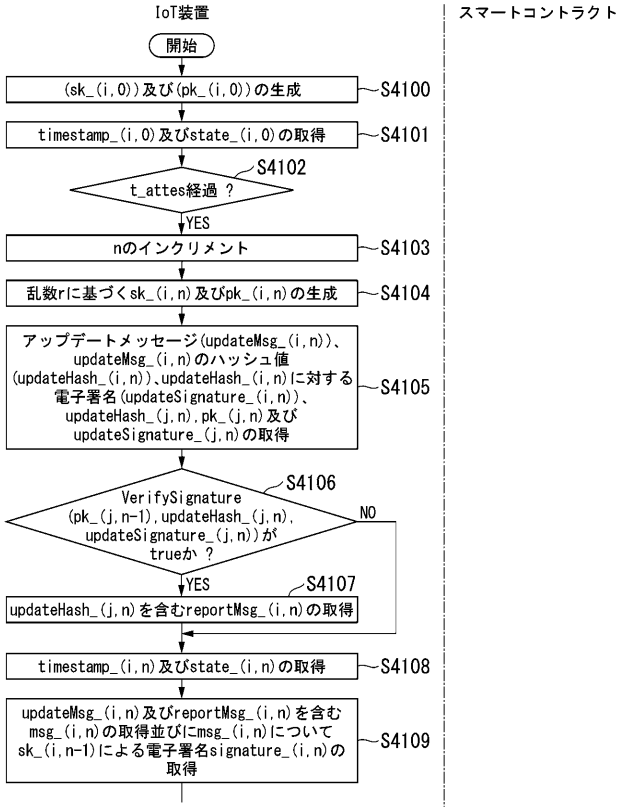
【図１３】



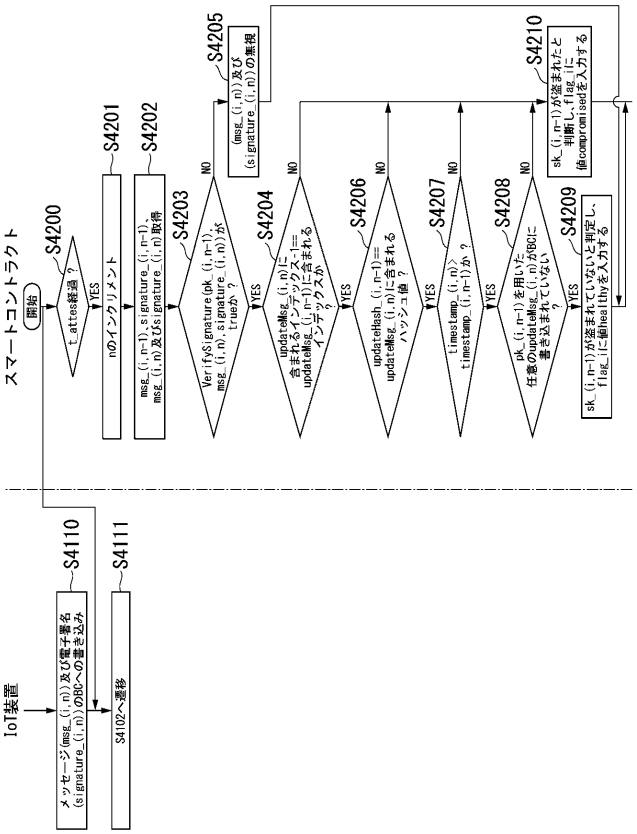
【図１４】



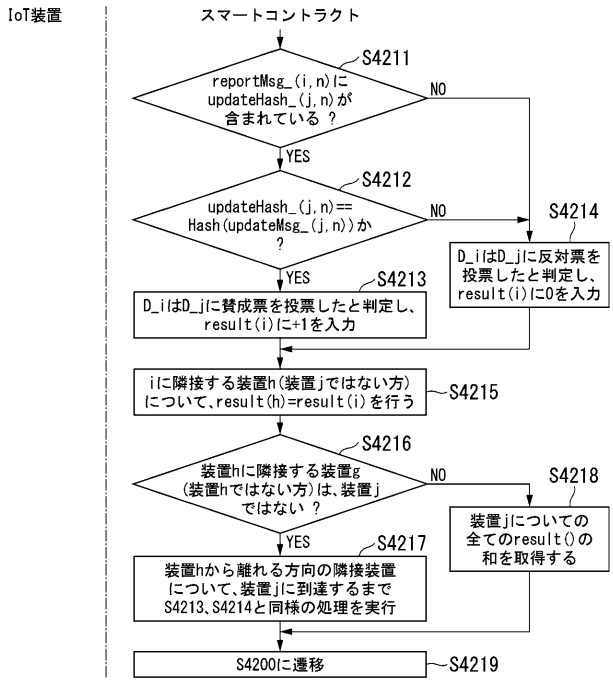
【図１５】



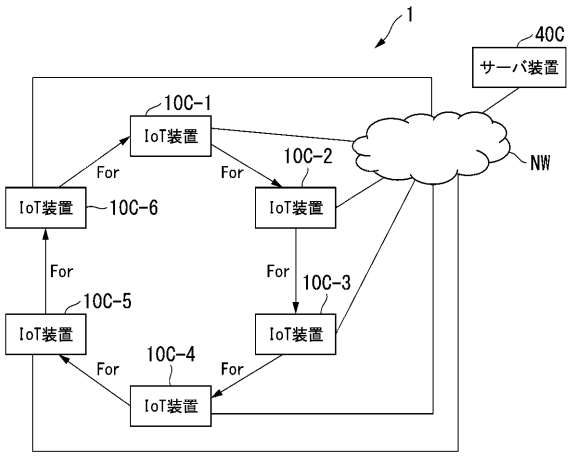
【図１６】



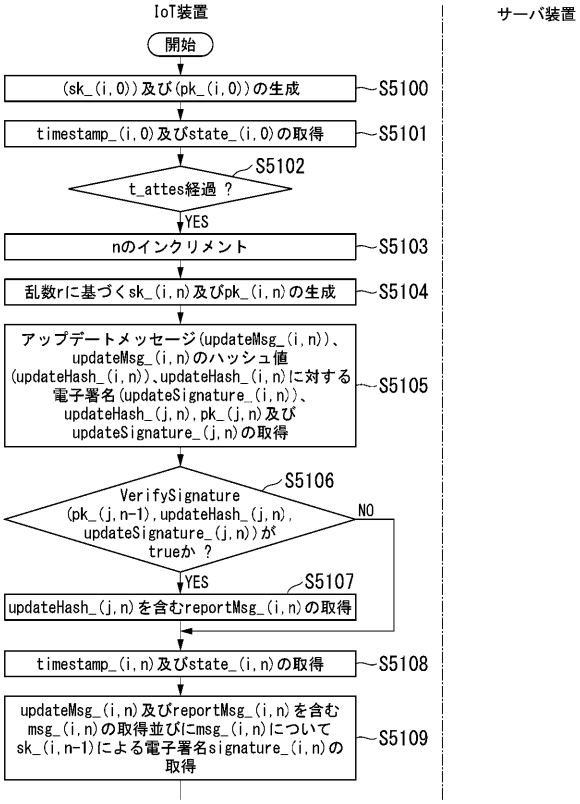
【図１７】



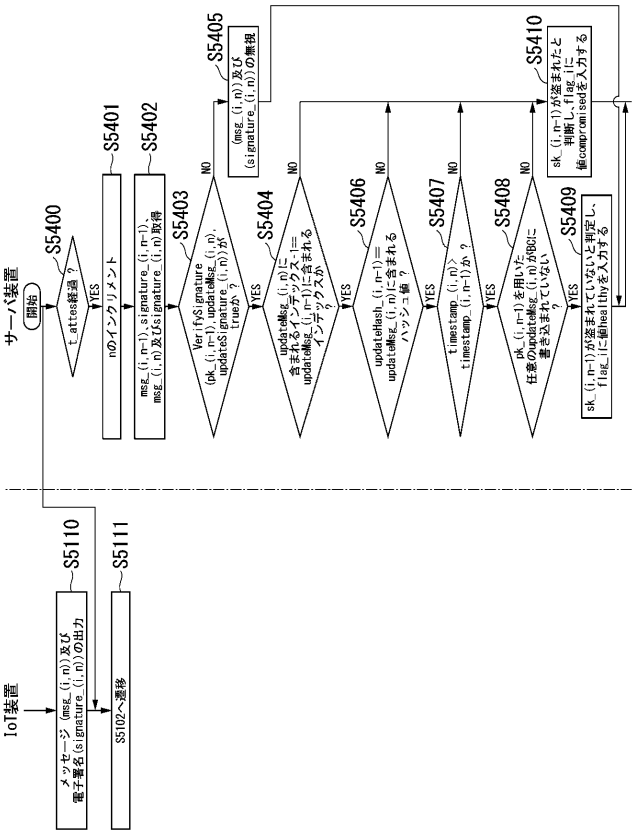
【図１８】



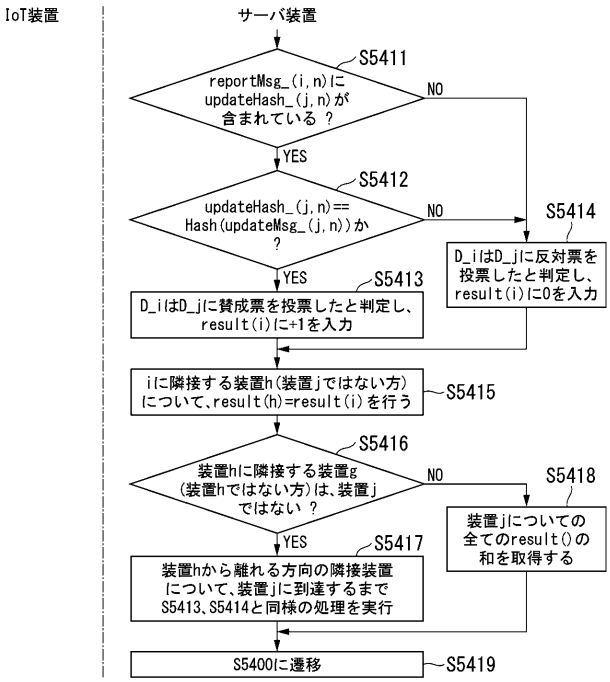
【図１９】



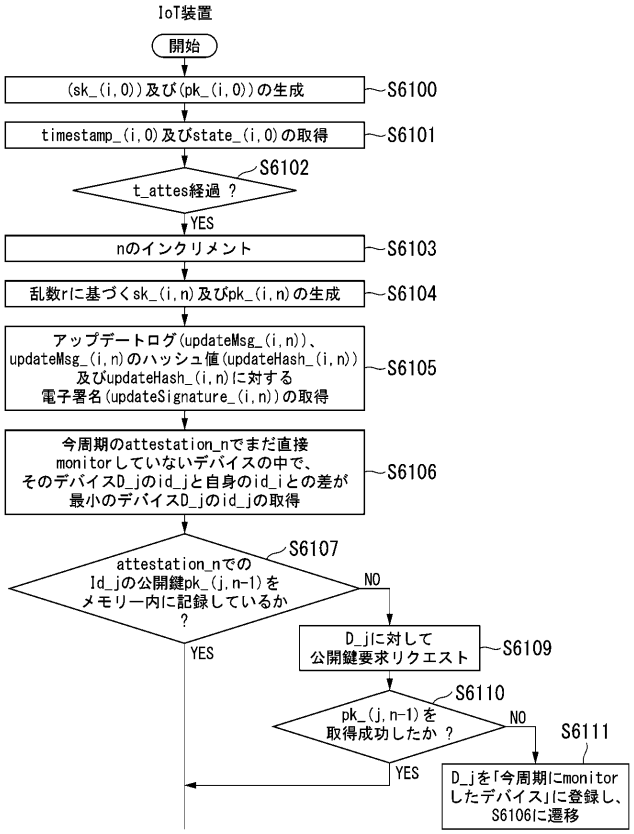
【図２０】



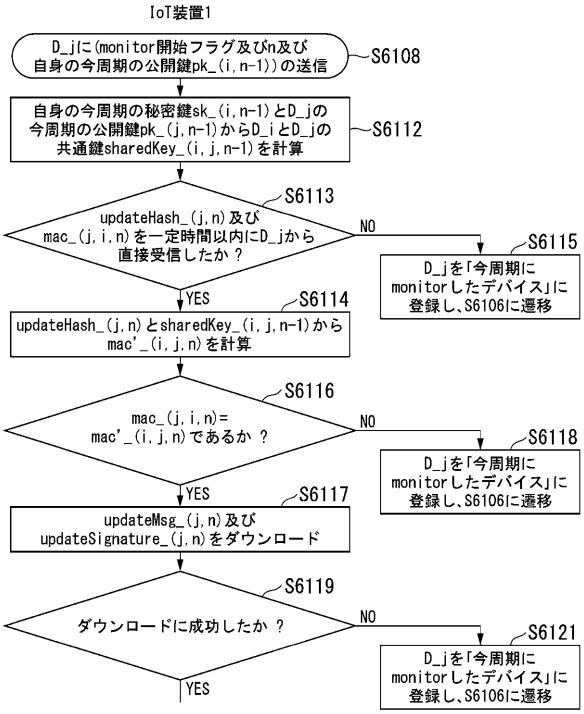
【図２１】



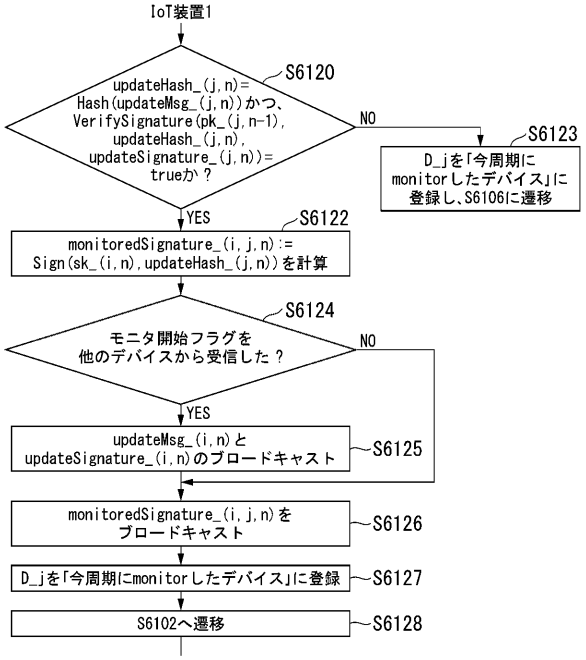
【図２２】



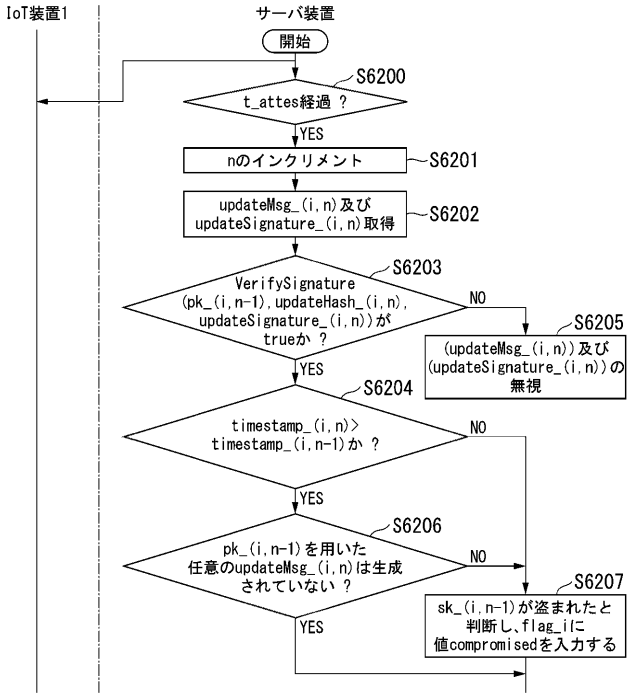
【図２３】



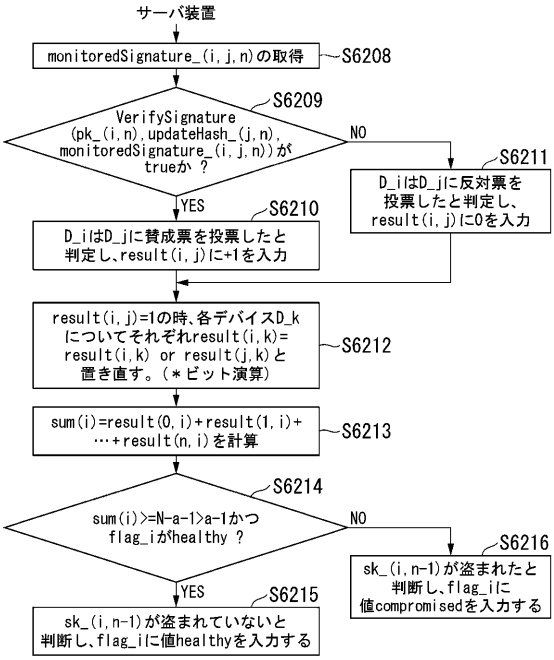
【図２４】



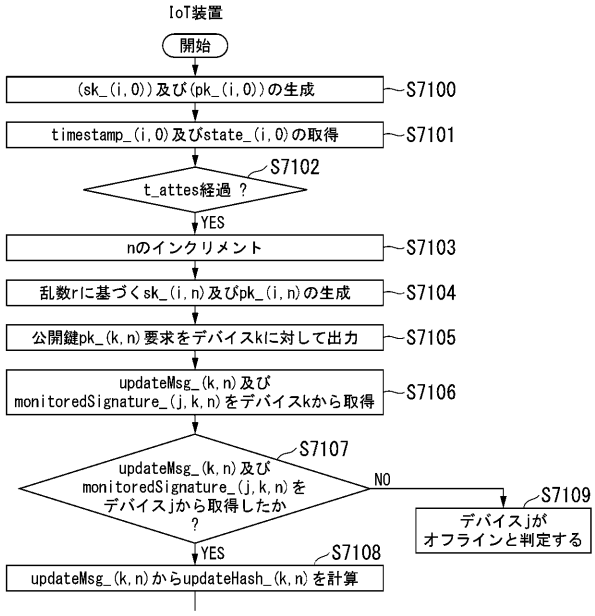
【図２５】



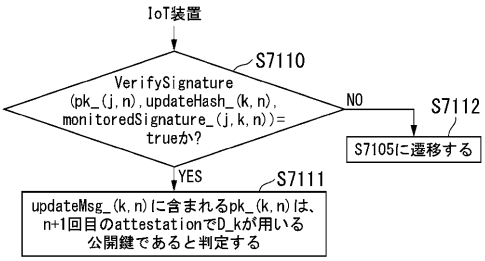
【図２６】


サーバ装置
monitoredSignature_(i,j,n)の取得
S6208
VerifySignature (pk_(i,n),updateHash_(j,n), monitoredSignature_(i,j,n))がtrueか ?
S6209
NO
YES
S6211
D_iはD_jに反対票を投票したと判定し、result(i,j)に0を入力
S6210
D_iはD_jに賛成票を投票したと判定し、result(i,j)に+1を入力
result(i,j)=1の時、各デバイスD_kについてそれぞれresult(i,k)= result(i,k) or result(j,k)と置き直す。(＊ビット演算)
S6212
sum(i)=result(0,i)+result(1,i)+…+result(n,i)を計算
S6213
sum(i)>=N-a-1>a-1かつflag_iがhealthy ?
S6214
NO
YES
S6216
sk_(i,n-1)が盗まれたと判断し、flag_iに値compromisedを入力する
S6215
sk_(i,n-1)が盗まれていないと判断し、flag_iに値healthyを入力する

【図２７】


IoT装置
開始
(sk_(i,0))及び(pk_(i,0))の生成
S7100
timestamp_(i,0)及びstate_(i,0)の取得
S7101
t_attes経過 ?
S7102
YES
nのインクリメント
S7103
乱数rに基づくsk_(i,n)及びpk_(i,n)の生成
S7104
公開鍵pk_(k,n)要求をデバイスkに対して出力
S7105
updateMsg_(k,n)及びmonitoredSignature_(j,k,n)をデバイスkから取得
S7106
updateMsg_(k,n)及びmonitoredSignature_(j,k,n)をデバイスjから取得したか ?
S7107
NO
YES
S7109
デバイスjがオフラインと判定する
S7108
updateMsg_(k,n)からupdateHash_(k,n)を計算

【図２８】


IoT装置
VerifySignature (pk_(j,n),updateHash_(k,n), monitoredSignature_(j,k,n))= trueか?
S7110
NO
YES
S7112
S7105に遷移する
S7111
updateMsg_(k,n)に含まれるpk_(k,n)は、n+1回目のattestationでD_kが用いる公開鍵であると判定する