(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7398685号
(P7398685)

(45)発行日　令和5年12月15日(2023.12.15)

(24)登録日　令和5年12月7日(2023.12.7)

(51)国際特許分類			FI		
Ｅ０５Ｂ	*49/00*	*(2006.01)*	Ｅ０５Ｂ	49/00	Ｋ
Ｅ０５Ｆ	*15/77*	*(2015.01)*	Ｅ０５Ｆ	15/77	
Ｇ０６Ｆ	*21/33*	*(2013.01)*	Ｇ０６Ｆ	21/33	
Ｇ０６Ｆ	*21/35*	*(2013.01)*	Ｇ０６Ｆ	21/35	
Ｈ０４Ｌ	*9/14*	*(2006.01)*	Ｈ０４Ｌ	9/14	

請求項の数　14　（全24頁）　最終頁に続く

(21)出願番号　特願2022-581267(P2022-581267)
(86)(22)出願日　令和4年1月14日(2022.1.14)
(86)国際出願番号　PCT/JP2022/001110
(87)国際公開番号　WO2022/172686
(87)国際公開日　令和4年8月18日(2022.8.18)
審査請求日　令和5年5月29日(2023.5.29)
(31)優先権主張番号　特願2021-20799(P2021-20799)
(32)優先日　令和3年2月12日(2021.2.12)
(33)優先権主張国・地域又は機関
日本国(JP)

(73)特許権者　314012076
パナソニックＩＰマネジメント株式会社
大阪府門真市元町２２番６号
(74)代理人　100109210
弁理士　新居 広守
(74)代理人　100137235
弁理士　寺谷 英作
(74)代理人　100131417
弁理士　道坂 伸一
(72)発明者　藏前 健治
日本国大阪府門真市大字門真１００６番地 パナソニック株式会社内
(72)発明者　秋元 正夫
日本国大阪府門真市大字門真１００６番地 パナソニック株式会社内

最終頁に続く

(54)【発明の名称】　情報処理システム、及び、情報処理方法

(57)【特許請求の範囲】

【請求項１】

空間に対する物品または人の出入りを制限する第一機器の前記制限を解除するために用いられる情報処理システムであって、

情報端末、第一管理装置、及び、制御装置を備え、

前記情報端末は、

第一の秘密鍵及び第一の公開鍵が記憶された端末記憶部と、

前記第一の公開鍵を前記第一管理装置へ送信する端末通信部とを有し、

前記第一管理装置は、

第二の秘密鍵及び第二の公開鍵が記憶された第一記憶部と、

前記情報端末から前記第一の公開鍵を受信する第一通信部と、

受信された前記第一の公開鍵に対する署名を前記第二の秘密鍵を用いて生成し、前記第一の公開鍵、及び、前記署名を含むサーバ証明書を、前記第一通信部に前記情報端末へ送信させる第一情報処理部とを有し、

前記情報端末の前記端末通信部は、前記第一管理装置から前記サーバ証明書を受信し、受信した前記サーバ証明書を前記制御装置へ送信し、

前記制御装置は、

前記第二の公開鍵を含むルート証明書が記憶された記憶部と、

前記情報端末から前記サーバ証明書を受信する通信部と、

受信された前記サーバ証明書に含まれる前記署名を前記記憶部に記憶された前記ルート

証明書に含まれる前記第二の公開鍵を用いて検証し、検証に成功した場合に前記第一機器の前記制限を解除する制御部とを有する
情報処理システム。
【請求項２】
前記記憶部には、他の第一管理装置の第二の公開鍵を含む他のルート証明書が記憶される
請求項１に記載の情報処理システム。
【請求項３】
前記第一情報処理部は、受信された前記第一の公開鍵及び利用条件に対する前記署名を前記第二の秘密鍵を用いて生成し、前記第一の公開鍵、前記利用条件、及び、前記署名を含むサーバ証明書を、前記第一通信部に前記情報端末へ送信させ、
前記制御部は、受信された前記サーバ証明書に含まれる前記署名を、前記記憶部に記憶された前記ルート証明書に含まれる前記第二の公開鍵を用いて検証し、検証に成功した場合に、前記サーバ証明書に含まれている前記利用条件に基づいて、前記第一機器の前記制限を解除する
請求項１または２に記載の情報処理システム。
【請求項４】
第一空間に対する物品または人の出入りを制限する第一機器の前記制限を解除するために用いられる情報処理システムであって、
情報端末、第一管理装置、第二管理装置、及び、制御装置を備え、
前記第二管理装置は、
第三の秘密鍵及び第三の公開鍵が記憶された第二記憶部と、
前記第三の公開鍵を前記第一管理装置へ送信する第二通信部とを有し、
前記第一管理装置は、
第二の秘密鍵及び第二の公開鍵が記憶された第一記憶部と、
前記第二管理装置から前記第三の公開鍵を受信する第一通信部と、
受信された前記第三の公開鍵に対する第一の署名を前記第二の秘密鍵を用いて生成し、前記第三の公開鍵、及び、前記第一の署名を含む中間証明書を、前記第一通信部に前記第二管理装置へ送信させる第一情報処理部とを有し、
前記第二通信部は、前記第一管理装置から前記中間証明書を受信し、
前記情報端末は、
第一の秘密鍵及び第一の公開鍵が記憶された端末記憶部と、
前記第一の公開鍵を前記第二管理装置へ送信する端末通信部とを有し、
前記第二通信部は、前記情報端末から前記第一の公開鍵を受信し、
前記第二管理装置は、受信された前記第一の公開鍵に対する第二の署名を前記第三の秘密鍵を用いて生成し、前記第一の公開鍵、及び、前記第二の署名を含むサーバ証明書と、受信された前記中間証明書とを前記第二通信部に前記情報端末へ送信させる第二情報処理部を有し、
前記端末通信部は、前記サーバ証明書及び前記中間証明書を前記第二管理装置から受信し、受信した前記サーバ証明書及び前記中間証明書を、前記制御装置へ送信し、
前記制御装置は、
前記第二の公開鍵を含むルート証明書が記憶された記憶部と、
前記サーバ証明書及び前記中間証明書を前記情報端末から受信する通信部と、
受信された前記中間証明書に含まれる前記第一の署名を前記ルート証明書に含まれる前記第二の公開鍵を用いて検証し、受信された前記サーバ証明書に含まれる前記第二の署名を前記中間証明書に含まれる前記第三の公開鍵を用いて検証し、それぞれの検証に成功した場合に前記第一機器の前記制限を解除する制御部とを有する
情報処理システム。
【請求項５】
前記第一情報処理部は、受信された前記第三の公開鍵及び第一利用条件に対する前記第一の署名を前記第二の秘密鍵を用いて生成し、前記第三の公開鍵、前記第一利用条件、及

び、前記第一の署名を含む中間証明書を、前記第一通信部に前記第二管理装置へ送信させ、
　前記第二情報処理部は、受信された前記第一の公開鍵及び第二利用条件に対する第二の署名を前記第三の秘密鍵を用いて生成し、前記第一の公開鍵、前記第二利用条件、及び、前記第二の署名を含むサーバ証明書と、受信された前記中間証明書とを前記第二通信部に前記情報端末へ送信させ、
　前記制御部は、前記それぞれの検証に成功した場合に、前記中間証明書に含まれる前記第一利用条件、及び、前記サーバ証明書に含まれる前記第二利用条件に基づいて前記第一機器の前記制限を解除する
　請求項４に記載の情報処理システム。
【請求項６】
　前記第一機器は、ドアに設けられた電気錠であり、
　前記第一機器の前記制限の解除とは、前記電気錠を解錠することである
　請求項１～５のいずれか１項に記載の情報処理システム。
【請求項７】
　前記第一機器は、自動ドアであり、
　前記第一機器の前記制限の解除とは、前記自動ドアを開けることである
　請求項１～５のいずれか１項に記載の情報処理システム。
【請求項８】
　前記第二管理装置は、第二空間に対する物品または人の出入りを制限する第二機器の前記制限を解除する機能を有し、
　前記端末通信部は、受信した前記サーバ証明書を前記第二管理装置へ送信し、
　前記第二通信部は、前記サーバ証明書を受信し、
　前記第二情報処理部は、受信された前記サーバ証明書に含まれる前記第二の署名を前記第二記憶部に記憶された前記第三の公開鍵を用いて検証し、検証に成功した場合に前記第二機器の前記制限を解除する
　請求項４に記載の情報処理システム。
【請求項９】
　前記第一空間は、集合住宅の共用部であり、
　前記第二空間は、前記集合住宅の専有部である
　請求項８に記載の情報処理システム。
【請求項１０】
　前記第一機器は、前記共用部に設けられた自動ドアであり、
　前記第一機器の前記制限の解除とは、前記自動ドアを開けることであり、
　前記第二機器は、前記専有部に設けられたドアの電気錠であり、
　前記第二機器の前記制限の解除とは、前記電気錠を解錠することである
　請求項９に記載の情報処理システム。
【請求項１１】
　前記第一機器は、前記共用部に設けられたドアの電気錠であり、
　前記第一機器の前記制限の解除とは、前記共用部に設けられたドアの前記電気錠を開けることであり、
　前記第二機器は、前記専有部に設けられたドアの電気錠であり、
　前記第二機器の前記制限の解除とは、前記専有部に設けられたドアの前記電気錠を解錠することである
　請求項９に記載の情報処理システム。
【請求項１２】
　空間に対する物品または人の出入りを制限する第一機器の前記制限を解除するために用いられる情報処理システムが実行する情報処理方法であって、
　前記情報処理システムは、
　第一の秘密鍵及び第一の公開鍵が記憶された端末記憶部を有する情報端末と、
　第二の秘密鍵及び第二の公開鍵が記憶された第一記憶部を有する第一管理装置と、

前記第二の公開鍵を含むルート証明書が記憶された記憶部を有する制御装置とを備え、
前記情報処理方法は、
前記情報端末が前記第一の公開鍵を前記第一管理装置へ送信し、前記第一管理装置が前記情報端末から前記第一の公開鍵を受信する第一通信ステップと、
前記第一管理装置が、受信された前記第一の公開鍵に対する署名を前記第二の秘密鍵を用いて生成する生成ステップと、
前記第一管理装置が前記第一の公開鍵、及び、前記署名を含むサーバ証明書を前記情報端末へ送信し、前記情報端末が前記第一管理装置から前記サーバ証明書を受信する第二通信ステップと、
前記情報端末が、受信した前記サーバ証明書を前記制御装置へ送信し、前記制御装置が前記情報端末から前記サーバ証明書を受信する第三通信ステップと、
前記制御装置が、受信された前記サーバ証明書に含まれる前記署名を前記記憶部に記憶された前記ルート証明書に含まれる前記第二の公開鍵を用いて検証し、検証に成功した場合に前記第一機器の前記制限を解除する制御ステップとを含む
情報処理方法。
【請求項１３】
第一空間に対する物品または人の出入りを制限する第一機器の前記制限を解除するために用いられる情報処理システムが実行する情報処理方法であって、
前記情報処理システムは、
第一の秘密鍵及び第一の公開鍵が記憶された端末記憶部を有する情報端末と、
第二の秘密鍵及び第二の公開鍵が記憶された第一記憶部を有する第一管理装置と、
第三の秘密鍵及び第三の公開鍵が記憶された第二記憶部を有する第二管理装置と、
前記第二の公開鍵を含むルート証明書が記憶された記憶部を有する制御装置とを備え、
前記情報処理方法は、
前記第二管理装置が前記第三の公開鍵を前記第一管理装置へ送信し、前記第一管理装置が前記第二管理装置から前記第三の公開鍵を受信する第一通信ステップと、
前記第一管理装置が、受信された前記第三の公開鍵に対する第一の署名を前記第二の秘密鍵を用いて生成する第一生成ステップと、
前記第一管理装置が、前記第三の公開鍵、及び、前記第一の署名を含む中間証明書を、前記第二管理装置へ送信し、前記第二管理装置が前記第一管理装置から前記中間証明書を受信する第二通信ステップと、
前記情報端末が前記第一の公開鍵を前記第二管理装置へ送信し、前記第二管理装置が前記情報端末から前記第一の公開鍵を受信する第三通信ステップと、
前記第二管理装置が、受信された前記第一の公開鍵に対する第二の署名を前記第三の秘密鍵を用いて生成する第二生成ステップと、
前記第二管理装置が、前記第一の公開鍵、及び、前記第二の署名を含むサーバ証明書と、受信された前記中間証明書とを前記情報端末へ送信し、前記情報端末が前記サーバ証明書及び前記中間証明書を前記第二管理装置から受信する第四通信ステップと、
前記情報端末が、受信した前記サーバ証明書及び前記中間証明書を前記制御装置へ送信し、前記制御装置が前記サーバ証明書及び前記中間証明書を前記情報端末から受信する第五通信ステップと、
前記制御装置が、受信された前記中間証明書に含まれる前記第一の署名を前記ルート証明書に含まれる前記第二の公開鍵を用いて検証し、受信された前記サーバ証明書に含まれる前記第二の署名を前記中間証明書に含まれる前記第三の公開鍵を用いて検証し、それぞれの検証に成功した場合に前記第一機器の前記制限を解除する制御ステップとを含む
情報処理方法。
【請求項１４】
請求項１２または請求項１３に記載の情報処理方法をコンピュータに実行させるためのプログラム。
【発明の詳細な説明】

【技術分野】
【０００１】
本発明は、情報処理システム、及び、情報処理方法に関する。
【背景技術】
【０００２】
従来、施設のドアを施錠または解錠するためのセキュリティシステムが知られている。特許文献１には、指紋認証装置等の他の機器を要さずに住宅の施錠及び解錠を安全に遠隔操作することができるセキュリティシステムが開示されている。
【先行技術文献】
【特許文献】
【０００３】
【文献】特開２０１４－１５９６９２号公報
【発明の概要】
【発明が解決しようとする課題】
【０００４】
施設のドアを施錠または解錠するための機器として電気錠が知られている。電気錠は、物品または人の出入りを制限する機器であるといえる。
【０００５】
本発明は、情報端末に、物品または人の出入りの制限を解除する権限を付与することができる情報処理システム等を提供する。
【課題を解決するための手段】
【０００６】
本発明の一態様に係る情報処理システムは、空間に対する物品または人の出入りを制限する第一機器の前記制限を解除するために用いられる情報処理システムであって、情報端末、第一管理装置、及び、制御装置を備え、前記情報端末は、第一の秘密鍵及び第一の公開鍵が記憶された端末記憶部と、前記第一の公開鍵を前記第一管理装置へ送信する端末通信部とを有し、前記第一管理装置は、第二の秘密鍵及び第二の公開鍵が記憶された第一記憶部と、前記情報端末から前記第一の公開鍵を受信する第一通信部と、受信された前記第一の公開鍵に対する署名を前記第二の秘密鍵を用いて生成し、前記第一の公開鍵、及び、前記署名を含むサーバ証明書を、前記第一通信部に前記情報端末へ送信させる第一情報処理部とを有し、前記情報端末の前記端末通信部は、前記第一管理装置から前記サーバ証明書を受信し、受信した前記サーバ証明書を前記制御装置へ送信し、前記制御装置は、前記第二の公開鍵を含むルート証明書が記憶された記憶部と、前記情報端末から前記サーバ証明書を受信する通信部と、受信された前記サーバ証明書に含まれる前記署名を前記記憶部に記憶された前記ルート証明書に含まれる前記第二の公開鍵を用いて検証し、検証に成功した場合に前記第一機器の前記制限を解除する制御部とを有する。
【０００７】
本発明の一態様に係る情報処理システムは、第一空間に対する物品または人の出入りを制限する第一機器の前記制限を解除するために用いられる情報処理システムであって、情報端末、第一管理装置、第二管理装置、及び、制御装置を備え、前記第二管理装置は、第三の秘密鍵及び第三の公開鍵が記憶された第二記憶部と、前記第三の公開鍵を前記第一管理装置へ送信する第二通信部とを有し、前記第一管理装置は、第二の秘密鍵及び第二の公開鍵が記憶された第一記憶部と、前記第二管理装置から前記第三の公開鍵を受信する第一通信部と、受信された前記第三の公開鍵に対する第一の署名を前記第二の秘密鍵を用いて生成し、前記第三の公開鍵、及び、前記第一の署名を含む中間証明書を、前記第一通信部に前記第二管理装置へ送信させる第一情報処理部とを有し、前記第二通信部は、前記第一管理装置から前記中間証明書を受信し、前記情報端末は、第一の秘密鍵及び第一の公開鍵が記憶された端末記憶部と、前記第一の公開鍵を前記第二管理装置へ送信する端末通信部とを有し、前記第二通信部は、前記情報端末から前記第一の公開鍵を受信し、前記第二管理装置は、受信された前記第一の公開鍵に対する第二の署名を前記第三の秘密鍵を用いて

生成し、前記第一の公開鍵、及び、前記第二の署名を含むサーバ証明書と、受信された前記中間証明書とを前記第二通信部に前記情報端末へ送信させる第二情報処理部を有し、前記端末通信部は、前記サーバ証明書及び前記中間証明書を前記第二管理装置から受信し、受信した前記サーバ証明書及び前記中間証明書を、前記制御装置へ送信し、前記制御装置は、前記第二の公開鍵を含むルート証明書が記憶された記憶部と、前記サーバ証明書及び前記中間証明書を前記情報端末から受信する通信部と、受信された前記中間証明書に含まれる前記第一の署名を前記ルート証明書に含まれる前記第二の公開鍵を用いて検証し、受信された前記サーバ証明書に含まれる前記第二の署名を前記中間証明書に含まれる前記第三の公開鍵を用いて検証し、それぞれの検証に成功した場合に前記第一機器の前記制限を解除する制御部とを有する。

【０００８】

本発明の一態様に係る情報処理方法は、空間に対する物品または人の出入りを制限する第一機器の前記制限を解除するために用いられる情報処理システムが実行する情報処理方法であって、前記情報処理システムは、第一の秘密鍵及び第一の公開鍵が記憶された端末記憶部を有する情報端末と、第二の秘密鍵及び第二の公開鍵が記憶された第一記憶部を有する第一管理装置と、前記第二の公開鍵を含むルート証明書が記憶された記憶部を有する制御装置とを備え、前記情報処理方法は、前記情報端末が前記第一の公開鍵を前記第一管理装置へ送信し、前記第一管理装置が前記情報端末から前記第一の公開鍵を受信する第一通信ステップと、前記第一管理装置が、受信された前記第一の公開鍵に対する署名を前記第二の秘密鍵を用いて生成する生成ステップと、前記第一管理装置が前記第一の公開鍵、及び、前記署名を含むサーバ証明書を前記情報端末へ送信し、前記情報端末が前記第一管理装置から前記サーバ証明書を受信する第二通信ステップと、前記情報端末が、受信した前記サーバ証明書を前記制御装置へ送信し、前記制御装置が前記情報端末から前記サーバ証明書を受信する第三通信ステップと、前記制御装置が、受信された前記サーバ証明書に含まれる前記署名を前記記憶部に記憶された前記ルート証明書に含まれる前記第二の公開鍵を用いて検証し、検証に成功した場合に前記第一機器の前記制限を解除する制御ステップとを含む。

【０００９】

本発明の一態様に係る情報処理方法は、第一空間に対する物品または人の出入りを制限する第一機器の前記制限を解除するために用いられる情報処理システムが実行する情報処理方法であって、前記情報処理システムは、第一の秘密鍵及び第一の公開鍵が記憶された端末記憶部を有する情報端末と、第二の秘密鍵及び第二の公開鍵が記憶された第一記憶部を有する第一管理装置と、第三の秘密鍵及び第三の公開鍵が記憶された第二記憶部を有する第二管理装置と、前記第二の公開鍵を含むルート証明書が記憶された記憶部を有する制御装置とを備え、前記情報処理方法は、前記第二管理装置が前記第三の公開鍵を前記第一管理装置へ送信し、前記第一管理装置が前記第二管理装置から前記第三の公開鍵を受信する第一通信ステップと、前記第一管理装置が、受信された前記第三の公開鍵に対する第一の署名を前記第二の秘密鍵を用いて生成する第一生成ステップと、前記第一管理装置が、前記第三の公開鍵、及び、前記第一の署名を含む中間証明書を、前記第二管理装置へ送信し、前記第二管理装置が前記第一管理装置から前記中間証明書を受信する第二通信ステップと、前記情報端末が前記第一の公開鍵を前記第二管理装置へ送信し、前記第二管理装置が前記情報端末から前記第一の公開鍵を受信する第三通信ステップと、前記第二管理装置が、受信された前記第一の公開鍵に対する第二の署名を前記第三の秘密鍵を用いて生成する第二生成ステップと、前記第二管理装置が、前記第一の公開鍵、及び、前記第二の署名を含むサーバ証明書と、受信された前記中間証明書とを前記情報端末へ送信し、前記情報端末が前記サーバ証明書及び前記中間証明書を前記第二管理装置から受信する第四通信ステップと、前記情報端末が、受信した前記サーバ証明書及び前記中間証明書を前記制御装置へ送信し、前記制御装置が前記サーバ証明書及び前記中間証明書を前記情報端末から受信する第五通信ステップと、前記制御装置が、受信された前記中間証明書に含まれる前記第一の署名を前記ルート証明書に含まれる前記第二の公開鍵を用いて検証し、受信された

前記サーバ証明書に含まれる前記第二の署名を前記中間証明書に含まれる前記第三の公開鍵を用いて検証し、それぞれの検証に成功した場合に前記第一機器の前記制限を解除する制御ステップとを含む。

【００１０】

本発明の一態様に係るプログラムは、前記情報処理方法をコンピュータに実行させるためのプログラムである。

【発明の効果】

【００１１】

本発明の一態様に係る情報処理システム等は、情報端末に、物品または人の出入りの制限を解除する権限を付与することができる。

【図面の簡単な説明】

【００１２】

【図１】図１は、実施の形態１に係る情報処理システムの外観図である。

【図２】図２は、実施の形態１に係る情報処理システムの機能構成を示すブロック図である。

【図３】図３は、実施の形態１に係る情報処理システムの動作例１の前半のシーケンス図である。

【図４】図４は、実施の形態１に係る情報処理システムの動作例１の後半のシーケンス図である。

【図５】図５は、サーバ証明書のフォーマットの一例を示す図である。

【図６】図６は、実施の形態１に係る情報処理システムの動作例２の前半のシーケンス図である。

【図７】図７は、実施の形態１に係る情報処理システムの動作例２の後半のシーケンス図である。

【図８】図８は、実施の形態２に係る情報処理システムの外観図である。

【図９】図９は、実施の形態２に係る情報処理システムの機能構成を示すブロック図である。

【図１０】図１０は、実施の形態２に係る情報処理システムの動作例のシーケンス図である。

【発明を実施するための形態】

【００１３】

以下、実施の形態について、図面を参照しながら具体的に説明する。なお、以下で説明する実施の形態は、いずれも包括的または具体的な例を示すものである。以下の実施の形態で示される数値、形状、材料、構成要素、構成要素の配置位置及び接続形態、ステップ、ステップの順序などは、一例であり、本発明を限定する主旨ではない。また、以下の実施の形態における構成要素のうち、独立請求項に記載されていない構成要素については、任意の構成要素として説明される。

【００１４】

なお、各図は模式図であり、必ずしも厳密に図示されたものではない。また、各図において、実質的に同一の構成に対しては同一の符号を付し、重複する説明は省略または簡略化される場合がある。

【００１５】

（実施の形態１）

［構成］

まず、実施の形態１に係る情報処理システムの構成について説明する。図１は、実施の形態１に係る情報処理システムの外観図である。図２は、実施の形態１に係る情報処理システムの機能構成を示すブロック図である。

【００１６】

図１に示されるように、実施の形態１に係る情報処理システム１０は、ユーザが電気錠６０を情報端末２０で解錠するために、情報端末２０に電気錠６０の解錠権限（または施

錠権限）を付与するためのシステムである。情報処理システム１０は、情報端末２０と、第一管理装置３０と、第二管理装置４０と、制御装置５０と、電気錠６０とを備える。制御装置５０、及び、電気錠６０は、例えば、施設８０内のドア８１（またはドア枠）に電気錠システムとして設置される。施設８０は、例えば、集合住宅であるが、オフィスビルなどの住宅以外の施設であってもよい。

【００１７】

情報端末２０は、施設８０への訪問者が電気錠６０解錠するために使用する情報端末である。情報端末２０は、例えば、スマートフォンまたはタブレット端末などの携帯型の情報端末である。情報端末２０は、操作受付部２１と、端末通信部２２と、端末制御部２３と、端末記憶部２４とを備える。

【００１８】

操作受付部２１は、ユーザの操作を受け付ける。操作受付部２１は、例えば、タッチパネルによって実現されるが、ハードウェアキーなどによって実現されてもよい。

【００１９】

端末通信部２２は、情報端末２０が第一管理装置３０、第二管理装置４０、及び、制御装置５０のそれぞれと通信を行うための通信回路である。端末通信部２２は、例えば、第一管理装置３０及び第二管理装置４０とは、インターネットなどの広域通信ネットワークを通じた無線通信を行い、制御装置５０とは局所通信ネットワークを通じた無線通信を行う。

【００２０】

端末制御部２３は、電気錠６０を解錠するための情報処理などを行う。端末制御部２３は、例えば、マイクロコンピュータによって実現されるが、プロセッサによって実現されてもよい。端末制御部２３の機能は、例えば、端末制御部２３を構成するマイクロコンピュータまたはプロセッサ等が端末記憶部２４に記憶されたコンピュータプログラムを実行することによって実現される。

【００２１】

端末記憶部２４は、上記情報処理に必要な情報、及び、上記コンピュータプログラムなどが記憶される記憶装置である。端末記憶部２４は、例えば、半導体メモリによって実現される。

【００２２】

第一管理装置３０は、施設８０の管理者等が使用する情報端末である。管理者等とは、施設８０のオーナまたは施設８０の管理事業者の従業員などである。第一管理装置３０は、例えば、パーソナルコンピュータまたはサーバ装置などの据え置き型の情報端末であるが、携帯型の情報端末であってもよい。第一管理装置３０は、第一通信部３１と、第一情報処理部３２と、第一記憶部３３とを備える。

【００２３】

第一通信部３１は、第一管理装置３０が、情報端末２０、第二管理装置４０、及び、制御装置５０のそれぞれと通信を行うための通信回路である。第一通信部３１は、例えば、情報端末２０、第二管理装置４０、及び、制御装置５０のそれぞれと広域通信ネットワークを通じた通信を行う。第一通信部３１は、有線通信を行ってもよいし、無線通信を行ってもよい。

【００２４】

第一情報処理部３２は、情報端末２０に電気錠６０の解錠権限を与えるための情報処理を行う。第一情報処理部３２は、例えば、マイクロコンピュータによって実現されるが、プロセッサによって実現されてもよい。第一情報処理部３２の機能は、例えば、第一情報処理部３２を構成するマイクロコンピュータまたはプロセッサ等が第一記憶部３３に記憶されたコンピュータプログラムを実行することによって実現される。

【００２５】

第一記憶部３３は、上記情報処理に必要な情報、及び、上記コンピュータプログラムなどが記憶される記憶装置である。第一記憶部３３は、例えば、ＨＤＤ（Ｈａｒｄ　Ｄｉｓｋ

Ｄｒｉｖｅ）によって実現されるが、半導体メモリによって実現されてもよい。
【００２６】
第二管理装置４０は、施設８０の入居者等が使用する情報端末である。第二管理装置４０は、例えば、携帯型の情報端末であるが、パーソナルコンピュータまたはサーバ装置などの据え置き型の情報端末であってもよい。第二管理装置４０は、第二通信部４１と、第二情報処理部４２と、第二記憶部４３とを備える。
【００２７】
第二通信部４１は、第二管理装置４０が、情報端末２０、第一管理装置３０、及び、制御装置５０のそれぞれと通信を行うための通信回路である。第二通信部４１は、例えば、情報端末２０、第一管理装置３０、及び、制御装置５０のそれぞれと広域通信ネットワークを通じた通信を行う。第二通信部４１は、有線通信を行ってもよいし、無線通信を行ってもよい。
【００２８】
第二情報処理部４２は、情報端末２０に電気錠６０の解錠権限を与えるための情報処理を行う。第二情報処理部４２は、例えば、マイクロコンピュータによって実現されるが、プロセッサによって実現されてもよい。第二情報処理部４２の機能は、例えば、第二情報処理部４２を構成するマイクロコンピュータまたはプロセッサ等が第二記憶部４３に記憶されたコンピュータプログラムを実行することによって実現される。
【００２９】
第二記憶部４３は、上記情報処理に必要な情報、及び、上記コンピュータプログラムなどが記憶される記憶装置である。第二記憶部４３は、例えば、半導体メモリによって実現される。
【００３０】
制御装置５０は、電気錠６０の施錠及び解錠を制御する制御装置である。制御装置５０は、例えば、ドア８１またはドア枠に内蔵される。ドア８１は、例えば、制御装置５０は、通信部５１と、制御部５２と、記憶部５３とを備える。
【００３１】
通信部５１は、制御装置５０が、情報端末２０、第一管理装置３０、及び、第二管理装置４０のそれぞれと通信を行うための通信回路である。通信部５１は、例えば、情報端末２０とは局所通信ネットワークを通じた無線通信を行い、第一管理装置３０及び第二管理装置４０とは広域通信ネットワークを通じた無線通信を行う。
【００３２】
制御部５２は、電気錠６０を施錠または解錠するための情報処理を行う。制御部５２は、具体的には、電気錠６０に制御信号を出力することにより、電気錠６０を施錠または解錠する。制御部５２は、例えば、マイクロコンピュータによって実現されるが、プロセッサによって実現されてもよい。制御部５２の機能は、例えば、制御部５２を構成するマイクロコンピュータまたはプロセッサ等が記憶部５３に記憶されたコンピュータプログラムを実行することによって実現される。
【００３３】
記憶部５３は、上記情報処理に必要な情報、及び、上記コンピュータプログラムなどが記憶される記憶装置である。記憶部５３は、例えば、半導体メモリによって実現される。
【００３４】
電気錠６０は、制御部５２から出力される制御信号に基づいてドア８１を施錠または解錠する。電気錠６０は、具体的には、電動モータと、電動モータの駆動力をデッドボルトに伝達する伝達機構とを有する。電動モータの駆動力が伝達機構を介してデッドボルトに伝達されることによって、デッドボルトが施錠位置または解錠位置に移動する。
【００３５】
［動作例１］
次に、情報処理システム１０の動作例１について説明する。図３及び図４は、情報処理システム１０の動作例１のシーケンス図である。以下の動作例１においては、情報端末２

０は、施設８０への訪問者によって使用され、第一管理装置３０は、施設８０の管理者等によって使用されるものとして説明が行われる。訪問者は、例えば、家事代行サービスの提供事業者から派遣される者、または、荷物の配達員などである。

【００３６】

まず、図３を参照しながら、情報端末２０の端末記憶部２４にサーバ証明書が記憶されるまでの動作について説明する。サーバ証明書は、電気錠６０の解錠許可証の役割を果たすものである。図３に示されるように、情報端末２０の端末記憶部２４には、第一の公開鍵及び第一の秘密鍵が記憶される。第一の公開鍵及び第一の秘密鍵は、例えば、情報端末２０に情報処理システム１０を利用するためのアプリケーションプログラム（以下、単にアプリとも記載される）をインストールしたときに生成され、端末記憶部２４に記憶される。

【００３７】

また、第一管理装置３０の第一記憶部３３には、第二の公開鍵及び第二の秘密鍵が記憶される。第二の公開鍵及び第二の秘密鍵は、例えば、第一管理装置３０に情報処理システム１０を利用するためのアプリをインストールしたときに第一記憶部３３に記憶される。

【００３８】

まず、訪問者は、上記アプリを実行中の情報端末２０の操作受付部２１へ所定の操作を行う。所定の操作は、サーバ証明書をインストールするための操作である。操作受付部２１は、所定の操作を受け付ける（Ｓ１１）。

【００３９】

操作受付部２１によって所定の操作が受け付けられると、端末制御部２３は、サーバ証明書の発行要求を生成し、生成した発行要求を端末通信部２２に第一管理装置３０へ送信させる。発行要求には、第一の公開鍵が含まれる。つまり、端末通信部２２は、第一の公開鍵を第一管理装置３０へ送信する（Ｓ１２）。なお、端末通信部２２は、広域通信ネットワークを通じた無線通信により第一の公開鍵を第一管理装置３０へ送信する。

【００４０】

第一管理装置３０の第一通信部３１は、第一の公開鍵を含む発行要求を受信する。管理者が訪問者の発行要求を確認し、訪問者による電気錠６０の解錠を許可する場合、第一情報処理部３２は、受信した第一の公開鍵及び利用条件に対する署名を第二の秘密鍵を用いて生成する（Ｓ１３）。また、第一情報処理部３２は、第一の公開鍵、利用条件、及び、署名を含むサーバ証明書を、第一通信部３１に情報端末２０へ送信させる（Ｓ１４）。利用条件は、例えば、時期的な条件（言い換えれば、有効期限）を示す情報であり、例えば、第一管理装置３０を使用する管理者などによってあらかじめ定められる。

【００４１】

なお、サーバ証明書のフォーマットとしては、例えば、Ｘ．５０９証明書が用いられる。図５は、サーバ証明書のフォーマットの一例を示す図である。図５における証明書の有効期間は、上記利用条件に相当し、主体者公開鍵情報は、第一の公開鍵に相当し、ｓｉｇｎａｔｕｒｅＶａｌｕｅは、署名に相当する。なお、図５のフォーマットの拡張領域に、有効期限以外の利用条件が格納されてもよい。

【００４２】

情報端末２０の端末通信部２２は、サーバ証明書を受信する。端末制御部２３は、受信されたサーバ証明書を端末記憶部２４に記憶する（Ｓ１５）。

【００４３】

次に、図４を参照しながら、サーバ証明書を用いて電気錠６０が解錠されるまでの動作について説明する。図４に示されるように、制御装置５０の記憶部５３には、ルート証明書が記憶される。ルート証明書には第二の公開鍵が含まれる。ルート証明書は、例えば、第一管理装置３０の第一情報処理部３２によって生成され、第一通信部３１によって制御装置５０に送信されることで記憶部５３に記憶される。ルート証明書は、制御装置５０の製造時に製造設備により記憶部５３に記憶されてもよい。

【００４４】

まず、訪問者は、ドア８１の近くへ移動し、上記アプリを実行中の情報端末２０の操作受付部２１へ電気錠６０を解錠するための所定の解錠操作を行う。操作受付部２１は、解錠操作を受け付ける（Ｓ１６）。なお、ドア８１は、例えば、施設８０の専有部に設けられたドア（図１参照）であるが、施設８０のエントランスに設けられたドアであってもよいし、エントランス以外の共用部に設けられたドアであってもよい。

【００４５】

操作受付部２１によって解錠操作が受け付けられると、端末制御部２３は、サーバ証明書を端末通信部２２に制御装置５０へ送信させる。つまり、端末通信部２２は、サーバ証明書を制御装置５０へ送信する（Ｓ１７）。なお、端末通信部２２は、局所通信ネットワークを通じた無線通信により、サーバ証明書を制御装置５０へ送信する。この無線通信は、例えば、Ｂｌｕｅｔｏｏｔｈ（登録商標）などの通信規格に基づく近距離無線通信である。

【００４６】

制御装置５０の通信部５１は、サーバ証明書を受信する。制御部５２は、受信されたサーバ証明書に含まれる署名を、記憶部５３に記憶されたルート証明書に含まれる第二の公開鍵を用いて検証する（Ｓ１８）。制御部５２は、署名の検証に成功した場合に、サーバ証明書に含まれている利用条件の判定を行う（Ｓ１９）。上述のように利用条件は、例えば、時期的な条件であり、制御部５２は、時期的な条件が満たされるか否かを判定する。制御部５２は、時期的な要件が満たされると判定した場合に、サーバ証明書に含まれる第一の公開鍵を用いてセッション鍵を生成する（Ｓ２０）。制御部５２は、生成したセッション鍵を第一の公開鍵で暗号化し、暗号化されたセッション鍵を通信部５１に情報端末２０へ送信させる（Ｓ２１）。

【００４７】

情報端末２０の端末通信部２２は、暗号化されたセッション鍵を受信する。端末通信部２２は、第一の秘密鍵を用いてセッション鍵を復号し、セッション鍵を用いた暗号化通信により、解錠指令を端末通信部２２に制御装置５０へ送信させる（Ｓ２２）。

【００４８】

制御装置５０の通信部５１は、解錠指令を受信する。制御部５２は、受信された解錠指令に基づいて電気錠を解錠する（Ｓ２３）。制御部５２は、具体的には、電気錠６０に制御信号を送信することにより電気錠６０を解錠する。なお、情報端末２０は、同様の動作シーケンスに基づいて、電気錠６０の施錠を行うこともできる。

【００４９】

このように、情報処理システム１０においては、第一管理装置３０は、サーバ証明書及びルート証明書を用いて、安全に情報端末２０に電気錠６０の解錠権限を付与することができる。

【００５０】

なお、図示されないが、第二管理装置４０も第一管理装置３０と同様に、サーバ証明書及びルート証明書を用いて、安全に情報端末２０に電気錠６０の解錠権限を与えることができる。つまり、図３のシーケンス図において、第一管理装置３０及びその構成要素は、第二管理装置４０及びその構成要素に読み替えられてもよい。例えば、第一管理装置３０が施設８０の管理者によって使用され、第二管理装置４０が施設８０の入居者によって使用される場合、管理者と入居者のそれぞれが訪問者に施設８０への入場権限を付与することができる。

【００５１】

また、制御装置５０の記憶部５３に、第一管理装置３０に対応するルート証明書（第二の公開鍵）、及び、第二管理装置４０に対応するルート証明書（第三の公開鍵）が記憶されていれば、管理者に入場権限を付与された訪問者、及び、入居者に入場権限を付与された訪問者の両方が、自身の情報端末２０を用いて電気錠６０を解錠することができる。

【００５２】

なお、制御装置５０の制御対象は、電気錠６０に限定されない。制御装置５０は、施設

８０内の空間への入場または当該空間への退場を制限する機器を制御すればよい、例えば、制御装置５０は、施設８０のエントランスに設けられた自動ドア７０（後述）の開閉を制御してもよい。

【００５３】

［動作例２］

次に、情報処理システム１０の動作例２について説明する。図６及び図７は、情報処理システム１０の動作例２のシーケンス図である。以下の動作例２においては、第一管理装置３０がルートＣＡ（Ｃｅｒｔｉｆｉｃａｔｉｏｎ Ａｕｔｈｏｒｉｔｙ）として機能し、第二管理装置４０が中間ＣＡとして機能する動作例である。動作例２においては、情報端末２０は、施設８０への訪問者によって使用され、第一管理装置３０は、施設８０の管理者（施設８０のオーナまたは施設８０の管理事業者の従業員など）によって使用されるものとして説明が行われる。第二管理装置４０は、施設８０の入居者などによって使用される者として説明が行われる。なお、動作例２の説明では、動作例１で説明した事項の説明については適宜省略される。

【００５４】

まず、図６を参照しながら、第二管理装置４０の第二記憶部４３に中間証明書が記憶されるまでの動作について説明する。図６に示されるように、第一管理装置３０の第一記憶部３３には、第二の公開鍵及び第二の秘密鍵が記憶される。第二管理装置４０の第二記憶部４３には、第三の公開鍵及び第三の秘密鍵が記憶される。情報端末２０の端末記憶部２４には、第一の公開鍵及び第一の秘密鍵が記憶される。

【００５５】

まず、第二管理装置４０の第二情報処理部４２は、入居者の操作等に基づいて、中間証明書の発行要求を生成し、生成した発行要求を第二通信部４１に第一管理装置３０へ送信させる。発行要求には、第三の公開鍵が含まれる。つまり、第二通信部４１は、第三の公開鍵を第一管理装置３０へ送信する（Ｓ３１）。なお、第二通信部４１は、広域通信ネットワークを通じた通信により第三の公開鍵を第一管理装置３０へ送信する。

【００５６】

第一管理装置３０の第一通信部３１は、第三の公開鍵を含む発行要求を受信する。管理者が入居者の発行要求を確認し、入居者によるサーバ証明書の発行を許可する場合、第一情報処理部３２は、受信した第三の公開鍵及び第一利用条件に対する第一の署名を第二の秘密鍵を用いて生成する（Ｓ３２）。また、第一情報処理部３２は、第三の公開鍵、第一利用条件、及び、第一の署名を含む中間証明書を、第一通信部３１に第二管理装置４０へ送信させる（Ｓ３３）。第一利用条件は、例えば、時期的な条件（言い換えれば、有効期限）を示す情報であり、例えば、第一管理装置３０を使用する管理者などによってあらかじめ定められる。

【００５７】

なお、中間証明書のフォーマットとしては、例えば、上記図５に示されるようなＸ．５０９証明書が用いられる。

【００５８】

第二管理装置４０の第二通信部４１は、中間証明書を受信する。第二情報処理部４２は、受信された中間証明書を第二記憶部４３に記憶する（Ｓ３４）。

【００５９】

その後、訪問者は、上記アプリを実行中の情報端末２０の操作受付部２１へ所定の操作を行う。所定の操作は、サーバ証明書及び中間証明書をインストールするための操作である。操作受付部２１は、所定の操作を受け付ける（Ｓ３５）。

【００６０】

操作受付部２１によって解錠操作が受け付けられると、端末制御部２３は、サーバ証明書及び中間証明書の発行要求を生成し、生成した発行要求を端末通信部２２に第二管理装置４０へ送信させる。発行要求には、第一の公開鍵が含まれる。つまり、端末通信部２２は、第一の公開鍵を第二管理装置４０へ送信する（Ｓ３６）。なお、端末通信部２２は、

広域通信ネットワークを通じた無線通信により第一の公開鍵を第二管理装置４０へ送信する。

【００６１】

第二管理装置４０の第二通信部４１は、第一の公開鍵を含む発行要求を受信する。入居者が訪問者の発行要求を確認し、訪問者による電気錠６０の解錠を許可する場合、第二情報処理部４２は、受信した第一の公開鍵及び第二利用条件に対する第二の署名を第三の秘密鍵を用いて生成する（Ｓ３７）。また、第二情報処理部４２は、第一の公開鍵、第二利用条件、及び、第二の署名を含むサーバ証明書と、ステップＳ３３において受信された（言い換えれば、第二記憶部４３に記憶された）中間証明書とを、第二通信部４１に情報端末２０へ送信させる（Ｓ３８）。第二利用条件は、例えば、時期的な条件（言い換えれば、有効期限）を示す情報であり、例えば、第二管理装置４０を使用する入居者などによってあらかじめ定められる。なお、サーバ証明書のフォーマットとしては、例えば、Ｘ．５０９証明書が用いられる。

【００６２】

情報端末２０の端末通信部２２は、サーバ証明書及び中間証明書を受信する。端末制御部２３は、受信されたサーバ証明書及び中間証明書を端末記憶部２４に記憶する（Ｓ３９）。

【００６３】

次に、図７を参照しながらサーバ証明書及び中間証明書を用いて電気錠６０が解錠されるまでの動作について説明する。図７に示されるように、制御装置５０の記憶部５３には、ルート証明書が記憶される。動作例２では、ルート証明書には第二の公開鍵が含まれる。ルート証明書は、例えば、第一管理装置３０の第一情報処理部３２によって生成され、第一通信部３１によって制御装置５０に送信されることで記憶部５３に記憶される。ルート証明書は、制御装置５０の製造時に製造設備により記憶部５３に記憶されてもよい。

【００６４】

訪問者は、ドア８１の近くへ移動し、上記アプリを実行中の情報端末２０の操作受付部２１へ電気錠６０を解錠するための所定の解錠操作を行う。操作受付部２１は、解錠操作を受け付ける（Ｓ４０）。端末制御部２３は、操作受付部２１によって解錠操作が受け付けられると、サーバ証明書及び中間証明書を端末通信部２２に制御装置５０へ送信させる。つまり、端末通信部２２は、サーバ証明書及び中間証明書を制御装置５０へ送信する（Ｓ４１）。なお、端末通信部２２は、局所通信ネットワークを通じた無線通信により、サーバ証明書及び中間証明書を制御装置５０へ送信する。

【００６５】

制御装置５０の通信部５１は、サーバ証明書及び中間証明書を受信する。制御部５２は、受信された中間証明書に含まれる第一の署名を、記憶部５３に記憶されたルート証明書に含まれる第二の公開鍵を用いて検証する（Ｓ４２）。制御部５２は、第一の署名の検証に成功した場合に、中間証明書に含まれている第一利用条件の判定を行う（Ｓ４３）。

【００６６】

制御部５２は、第一利用条件の判定に成功した場合に、受信されたサーバ証明書に含まれる第二の署名を、中間証明書に含まれる第三の公開鍵を用いて検証する（Ｓ４４）。制御部５２は、第二の署名の検証に成功した場合に、サーバ証明書に含まれている第二利用条件の判定を行う（Ｓ４５）。以降のステップＳ４６～ステップＳ４９の処理は、動作例１のステップＳ２０～Ｓ２３と同様であり、最終的に電気錠６０が解錠される。なお、情報端末２０は、同様の動作シーケンスに基づいて、電気錠６０の施錠を行うこともできる。

【００６７】

このように、情報処理システム１０においては、第二管理装置４０は、情報端末２０に電気錠６０の解錠権限を付与することができる。なお、図示されないが、動作例２において第一管理装置３０が第二管理装置４０に対してサーバ証明書を発行してもよい。この場合、第二管理装置４０は、第一管理装置３０によって発行されたサーバ証明書を取得し、制御装置５０へ送信することで、電気錠６０を解錠することができる。つまり、動作例２

においては、第一管理装置３０は、第二管理装置４０に、電気錠６０の解錠権限と、サーバ証明書の発行権限（情報端末２０への電気錠の解錠権限を付与する権限）とを付与することができる。

【００６８】

上述のように、第二管理装置４０の使用者が入居者である場合、入居者は、施設８０に入居している間、自身が契約している専有部の電気錠６０の解錠でき、また、施設８０に入居している間、訪問者に当該専有部の電気錠６０の解錠を許可することができる。なお、第二管理装置４０が発行したサーバ証明書は、第一管理装置３０によって無効化することが可能である。

【００６９】

（実施の形態２）

［構成］

次に、実施の形態２に係る情報処理システムの構成について説明する。図８は、実施の形態２に係る情報処理システムの外観図である。図９は、実施の形態２に係る情報処理システムの機能構成を示すブロック図である。以下、実施の形態２に係る情報処理システム１０ａの情報処理システム１０との相違点について説明する。

【００７０】

情報端末２０は、訪問者ではなく入居者によって使用される。第二管理装置４０は、当該入居者が契約した専有部８３（具体的には、専有部８３のドア８１またはドア枠など）に設けられ、電気錠６０の施錠及び解錠をする機能を有する。つまり、実施の形態２における第二管理装置４０は、電気錠６０の制御装置としても機能し、第二情報処理部４２は、電気錠６０へ制御信号を送信することにより、電気錠６０を施錠及び解錠することができる。

【００７１】

制御装置５０は、施設８０の共用部８４に設けられる。共用部８４は、具体的には、施設８０のエントランスである。制御装置５０は、当該エントランスに設けられた自動ドア７０（オートロックドア）を開閉する。なお、エントランスに設けられたドアが手動で開閉されるドアである場合、制御装置５０は、自動ドア７０ではなく電気錠を施錠及び解錠してもよい。

【００７２】

［動作例］

施設８０の入居者は、専有部８３への入居開始時に情報端末２０の端末記憶部２４に中間証明書及びサーバ証明書をインストールする。このときの動作は、実施の形態１の動作例２の図６を用いて説明した通りである。

【００７３】

このように情報端末２０の端末記憶部２４に中間証明書及びサーバ証明書が記憶されれば、入居者は、情報端末２０を用いて専有部８３に設けられた電気錠６０を施錠及び解錠することができる。図１０は、情報処理システム１０ａの動作例のシーケンス図である。

【００７４】

訪問者は、ドア８１の近くへ移動し、情報処理システム１０ａに対応するアプリを実行中の情報端末２０の操作受付部２１へ電気錠６０を解錠するための所定の解錠操作を行う。操作受付部２１は、解錠操作を受け付ける（Ｓ５０）。端末制御部２３は、操作受付部２１によって解錠操作が受け付けられると、サーバ証明書を端末通信部２２に第二管理装置４０へ送信させる。つまり、端末通信部２２は、サーバ証明書を第二管理装置４０へ送信する（Ｓ５１）。なお、端末通信部２２は、局所通信ネットワークを通じた無線通信により、サーバ証明書を第二管理装置４０へ送信する。この無線通信は、例えば、Ｂｌｕｅｔｏｏｔｈ（登録商標）などの通信規格に基づく近距離無線通信である。

【００７５】

第二管理装置４０の第二通信部４１は、サーバ証明書を受信する。第二情報処理部４２は、受信されたサーバ証明書に含まれる第二の署名を、第二記憶部４３に記憶された第三

の公開鍵を用いて検証する（Ｓ５２）。制御部５２は、第二の署名の検証に成功した場合に、サーバ証明書に含まれている第二利用条件の判定を行う（Ｓ５３）。以降のステップＳ５４～ステップＳ５７の処理は、動作例１のステップＳ２０～Ｓ２３と同様であり、最終的に電気錠６０が解錠される。なお、情報端末２０は、同様の動作シーケンスに基づいて、電気錠６０の施錠を行うこともできる。

【００７６】

また、情報端末２０の端末記憶部２４に中間証明書及びサーバ証明書が記憶されれば、入居者は、情報端末２０を用いて共用部８４に設けられた自動ドア７０を開けることができる。この場合のシーケンス図は、図７と同様であるため説明が省略される。

【００７７】

以上説明したように、情報処理システム１０ａにおいては、入居者は、専有部８３の第二管理装置４０へ情報端末２０を登録する際（つまり、電気錠６０の解錠権限を得る際）に、共用部８４の自動ドア７０の開放権限を得ることができる。情報処理システム１０ａにおいては、第一管理装置３０及び第二管理装置４０が通信接続していなくても情報端末２０に権限を付与することができるので、利便性が高いといえる。

【００７８】

（変形例）

上記実施の形態では、利用条件がサーバ証明書に含まれたが、利用条件は、サーバ証明書とは別に安全な方法で情報端末２０から制御装置５０へ送信されてもよい。例えば、図４でステップＳ２１よりも後にセッション鍵を用いた暗号化通信によって利用条件が第一管理装置３０の署名と共に情報端末２０から制御装置５０へ送信されてもよい。サーバ証明書と利用条件を分けることにより、サーバ証明書の再発行をしなくても利用条件を柔軟に追加または変更することが可能となる。

【００７９】

また、上記実施の形態では、制御装置５０（情報処理システム１０ａにおいては、第二管理装置４０及び制御装置５０）は、電気錠６０または自動ドア７０などの施設８０内の空間への人の出入りを制限する機器を制御したが、物品の出入りを制限する機器を制御してもよい。例えば、制御装置５０は、宅配ボックス、コインロッカー、または、貸金庫などの扉を施錠及び解錠する電気錠を制御してもよい。つまり、制御装置５０は、空間に対する物品または人の出入りを制限する機器を制御すればよい。

【００８０】

また、情報処理システム１０及び情報処理システム１０ａは、空間に対する物品または人の出入りを制限する機器だけでなく、照明機器及び空調機器などの家電機器の制御を特定の人にのみ許可する場合にも適用できる。

【００８１】

また、上記実施例では図示しないが、ステップＳ１７、ステップＳ４１、およびステップＳ５１のサーバ証明書の送信後に、制御装置５０は、乱数を含めた疑似情報を情報端末２０に送信し、情報端末２０は、受信した疑似情報に対する第一の秘密鍵による署名を行い制御装置５０に送信してもよい。制御装置５０は、ステップＳ１８、ステップＳ４２、及び、ステップＳ５１の後でステップＳ５２よりも前の第一ステップにおいて、情報端末２０から受信した署名をサーバ証明書に含まれる第一の公開鍵を用いて検証することにより、証明書の盗用を防ぐことが可能である。

【００８２】

また、ステップＳ１９、ステップＳ４３、及び、上記第一ステップの後でステップＳ５２よりも前の第二ステップにおいて、サーバ証明書に含まれる制御装置５０のＩＤを検証することで、別の制御装置用の証明書の流用を防ぐことが可能である。

【００８３】

（まとめ）

以上説明したように、情報処理システム１０は、空間に対する物品または人の出入りを制限する第一機器の制限を解除するために用いられる。情報処理システム１０は、情報端

末２０、第一管理装置３０、及び、制御装置５０を備える。情報端末２０は、第一の秘密鍵及び第一の公開鍵が記憶された端末記憶部２４と、第一の公開鍵を第一管理装置３０へ送信する端末通信部２２とを有する。第一管理装置３０は、第二の秘密鍵及び第二の公開鍵が記憶された第一記憶部３３と、情報端末２０から第一の公開鍵を受信する第一通信部３１と、受信された第一の公開鍵に対する署名を第二の秘密鍵を用いて生成し、第一の公開鍵、及び、署名を含むサーバ証明書を、第一通信部３１に情報端末２０へ送信させる第一情報処理部３２とを有する。情報端末２０の端末通信部２２は、第一管理装置３０からサーバ証明書を受信し、受信したサーバ証明書を制御装置５０へ送信する。制御装置５０は、第二の公開鍵を含むルート証明書が記憶された記憶部５３と、情報端末２０から前記サーバ証明書を受信する通信部５１と、受信されたサーバ証明書に含まれる署名を記憶部５３に記憶されたルート証明書に含まれる第二の公開鍵を用いて検証し、検証に成功した場合に第一機器の制限を解除する制御部５２とを有する。なお、空間は、例えば、施設８０内の任意の閉空間である。

【００８４】

このような情報処理システム１０は、情報端末２０に、物品または人の出入りの制限を解除する権限を付与することができる。

【００８５】

また、例えば、記憶部５３には、他の第一管理装置３０の第二の公開鍵を含む他のルート証明書が記憶される。他の第一管理装置３０は、例えば、第二管理装置４０である。

【００８６】

このような情報処理システム１０においては、複数の第一管理装置３０のそれぞれが、情報端末２０に、物品または人の出入りの制限を解除する権限を付与することができる。

【００８７】

また、例えば、第一情報処理部３２は、受信された第一の公開鍵及び利用条件に対する署名を第二の秘密鍵を用いて生成し、第一の公開鍵、利用条件、及び、署名を含むサーバ証明書を、第一通信部３１に情報端末２０へ送信させる。制御部５２は、受信されたサーバ証明書に含まれる署名を、記憶部５３に記憶された前記ルート証明書に含まれる第二の公開鍵を用いて検証し、検証に成功した場合に、サーバ証明書に含まれている利用条件に基づいて、第一機器の制限を解除する。

【００８８】

このような情報処理システム１０においては、制御装置５０は、利用条件を考慮して第一機器の制限を解除することができる。

【００８９】

また、情報処理システム１０は、第一空間に対する物品または人の出入りを制限する第一機器の制限を解除するために用いられる。情報処理システム１０は、情報端末２０、第一管理装置３０、第二管理装置４０、及び、制御装置５０を備える。第二管理装置４０は、第三の秘密鍵及び第三の公開鍵が記憶された第二記憶部４３と、第三の公開鍵を第一管理装置３０へ送信する第二通信部４１とを有する。第一管理装置３０は、第二の秘密鍵及び第二の公開鍵が記憶された第一記憶部３３と、第二管理装置４０から第三の公開鍵を受信する第一通信部３１と、受信された第三の公開鍵に対する第一の署名を第二の秘密鍵を用いて生成し、第三の公開鍵、及び、第一の署名を含む中間証明書を、第一通信部３１に第二管理装置４０へ送信させる第一情報処理部３２とを有する。第二通信部４１は、第一管理装置３０から中間証明書を受信する。情報端末２０は、第一の秘密鍵及び第一の公開鍵が記憶された端末記憶部２４と、第一の公開鍵を第二管理装置４０へ送信する端末通信部２２とを有する。第二通信部４１は、情報端末２０から第一の公開鍵を受信する。第二管理装置４０は、受信された第一の公開鍵に対する第二の署名を第三の秘密鍵を用いて生成し、第一の公開鍵、及び、第二の署名を含むサーバ証明書と、受信された中間証明書とを第二通信部４１に情報端末２０へ送信させる第二情報処理部４２を有する。端末通信部２２は、サーバ証明書及び中間証明書を第二管理装置４０から受信し、受信したサーバ証明書及び中間証明書を、制御装置５０へ送信し、制御装置５０は、第二の公開鍵を含むル

ート証明書が記憶された記憶部５３と、サーバ証明書及び中間証明書を情報端末２０から受信する通信部５１と、受信された中間証明書に含まれる第一の署名をルート証明書に含まれる第二の公開鍵を用いて検証し、受信されたサーバ証明書に含まれる第二の署名を中間証明書に含まれる第三の公開鍵を用いて検証し、それぞれの検証に成功した場合に第一機器の制限を解除する制御部５２とを有する。なお、第一空間は、例えば、施設８０内の任意の閉空間である。

【００９０】

このような情報処理システム１０は、第二管理装置４０を中間ＣＡとして、情報端末２０に、物品または人の出入りの制限を解除する権限を付与することができる。

【００９１】

また、例えば、第一情報処理部３２は、受信された第三の公開鍵及び第一利用条件に対する第一の署名を第二の秘密鍵を用いて生成し、第三の公開鍵、第一利用条件、及び、第一の署名を含む中間証明書を、第一通信部３１に第二管理装置４０へ送信させる。第二情報処理部４２は、受信された第一の公開鍵及び第二利用条件に対する第二の署名を第三の秘密鍵を用いて生成し、第一の公開鍵、第二利用条件、及び、第二の署名を含むサーバ証明書と、受信された中間証明書とを第二通信部４１に情報端末２０へ送信させる。制御部５２は、それぞれの検証に成功した場合に、中間証明書に含まれる第一利用条件、及び、サーバ証明書に含まれる第二利用条件に基づいて第一機器の制限を解除する。

【００９２】

このような情報処理システム１０においては、制御装置５０は、第一利用条件及び第二利用条件を考慮して第一機器の制限を解除することができる。

【００９３】

また、例えば、第一機器は、ドア８１に設けられた電気錠６０であり、第一機器の制限の解除とは、電気錠６０を解錠することである。

【００９４】

このような情報処理システム１０は、情報端末２０に、電気錠６０を解錠する権限を付与することができる。

【００９５】

また、例えば、第一機器は、自動ドア７０であり、第一機器の制限の解除とは、自動ドア７０を開けることである。

【００９６】

このような情報処理システム１０は、情報端末２０に、自動ドア７０（オートロック式の自動ドア７０）を開ける権限を付与することができる。

【００９７】

また、情報処理システム１０ａにおいては、第二管理装置４０は、第二空間に対する物品または人の出入りを制限する第二機器の制限を解除する機能を有する。端末通信部２２は、受信したサーバ証明書を、第二管理装置４０へ送信する。第二通信部４１は、サーバ証明書を受信する。第二情報処理部４２は、受信されたサーバ証明書に含まれる第二の署名を第二記憶部４３に記憶された第三の公開鍵を用いて検証し、検証に成功した場合に第二機器の制限を解除する。なお、第二空間は、例えば、施設８０内の任意の閉空間である。

【００９８】

このような情報処理システム１０は、情報端末２０に、第一空間及び第二空間のそれぞれに対する物品または人の出入りの制限を解除する権限を付与することができる。

【００９９】

また、第一空間は、集合住宅の共用部８４であり、第二空間は、集合住宅の専有部８３である。

【０１００】

このような情報処理システム１０は、情報端末２０に、共用部８４及び専有部８３のそれぞれに対する物品または人の出入りの制限を解除する権限を付与することができる。

【０１０１】

また、第一機器は、共用部８４に設けられた自動ドア７０であり、第一機器の制限の解除とは、自動ドア７０を開けることである。第二機器は、専有部８３に設けられたドア８１の電気錠６０であり、第二機器の制限の解除とは、電気錠６０を解錠することである。

【０１０２】

このような情報処理システム１０は、情報端末２０に、共用部８４の自動ドアを開ける権限と、専有部８３の電気錠６０を解錠する権限とを付与することができる。

【０１０３】

また、第一機器は、共用部８４に設けられたドアの電気錠であり、第一機器の制限の解除とは、共用部８４に設けられたドアの電気錠を開けることである。第二機器は、専有部８３に設けられたドア８１の電気錠６０であり、第二機器の制限の解除とは、専有部８３に設けられたドア８１の電気錠６０を解錠することである。

【０１０４】

このような情報処理システム１０は、情報端末２０に、共用部８４及び専有部８３のそれぞれに設けられた電気錠を解錠する権限を付与することができる。

【０１０５】

また、情報処理方法は、空間に対する物品または人の出入りを制限する第一機器の制限を解除するために用いられる情報処理システムが実行する情報処理方法である。情報処理方法は、情報端末２０が第一の公開鍵を第一管理装置３０へ送信し、第一管理装置３０が情報端末２０から第一の公開鍵を受信する第一通信ステップＳ１２と、第一管理装置３０が、受信された第一の公開鍵に対する署名を第二の秘密鍵を用いて生成する生成ステップＳ１３と、第一管理装置３０が第一の公開鍵、及び、署名を含むサーバ証明書を情報端末２０へ送信し、情報端末２０が第一管理装置３０からサーバ証明書を受信する第二通信ステップＳ１４と、情報端末２０が、受信したサーバ証明書を制御装置５０へ送信し、制御装置５０が情報端末２０からサーバ証明書を受信する第三通信ステップＳ１７と、制御装置５０が、受信されたサーバ証明書に含まれる署名を記憶部５３に記憶されたルート証明書に含まれる第二の公開鍵を用いて検証し、検証に成功した場合に第一機器の制限を解除する制御ステップＳ１８～Ｓ２３とを含む。

【０１０６】

このような情報処理方法は、情報端末２０に、物品または人の出入りの制限を解除する権限を付与することができる。

【０１０７】

また、情報処理方法は、第一空間に対する物品または人の出入りを制限する第一機器の制限を解除するために用いられる情報処理システム１０が実行する情報処理方法である。情報処理方法は、第二管理装置４０が第三の公開鍵を第一管理装置３０へ送信し、第一管理装置３０が第二管理装置４０から第三の公開鍵を受信する第一通信ステップＳ３１と、第一管理装置３０が、受信された第三の公開鍵に対する第一の署名を第二の秘密鍵を用いて生成する第一生成ステップＳ３２と、第一管理装置３０が第三の公開鍵、及び、第一の署名を含む中間証明書を、第二管理装置４０へ送信し、第二管理装置４０が第一管理装置３０から中間証明書を受信する第二通信ステップＳ３３と、情報端末２０が第一の公開鍵を第二管理装置４０へ送信し、第二管理装置４０が情報端末２０から第一の公開鍵を受信する第三通信ステップＳ３６と、第二管理装置４０が、受信された第一の公開鍵に対する第二の署名を第三の秘密鍵を用いて生成する第二生成ステップＳ３７と、第二管理装置４０が、第一の公開鍵、及び、第二の署名を含むサーバ証明書と、受信された中間証明書とを情報端末２０へ送信し、情報端末２０がサーバ証明書及び中間証明書を第二管理装置４０から受信する第四通信ステップＳ３８と、情報端末２０が、受信したサーバ証明書及び中間証明書を制御装置５０へ送信し、制御装置５０が前記サーバ証明書及び中間証明書を情報端末２０から受信する第五通信ステップＳ４１と、制御装置５０が、受信された中間証明書に含まれる第一の署名をルート証明書に含まれる第二の公開鍵を用いて検証し、受信されたサーバ証明書に含まれる第二の署名を中間証明書に含まれる第三の公開鍵を用いて検証し、それぞれの検証に成功した場合に第一機器の前記制限を解除する制御ステップ

Ｓ４２～Ｓ４９とを含む。
【０１０８】
このような情報処理方法は、第二管理装置４０を中間ＣＡとして、情報端末２０に、物品または人の出入りの制限を解除する権限を付与することができる。
【０１０９】
（その他の実施の形態）
以上、実施の形態について説明したが、本発明は、上記実施の形態に限定されるものではない。
【０１１０】
例えば、上記実施の形態において、情報処理システムは、複数の装置によって実現されたが、単一の装置として実現されてもよい。例えば、情報処理システムは、情報端末、第一管理装置、第二管理装置、及び、制御装置のいずれかに相当する単一の装置として実現されてもよい。情報処理システムが複数の装置によって実現される場合、情報処理システムが備える構成要素（特に、機能的な構成要素）は、複数の装置にどのように振り分けられてもよい。
【０１１１】
また、上記実施の形態において、特定の処理部が実行する処理を別の処理部が実行してもよい。また、複数の処理の順序が変更されてもよいし、複数の処理が並行して実行されてもよい。
【０１１２】
また、上記実施の形態において、各構成要素は、各構成要素に適したソフトウェアプログラムを実行することによって実現されてもよい。各構成要素は、ＣＰＵまたはプロセッサなどのプログラム実行部が、ハードディスクまたは半導体メモリなどの記録媒体に記録されたソフトウェアプログラムを読み出して実行することによって実現されてもよい。
【０１１３】
また、各構成要素は、ハードウェアによって実現されてもよい。例えば、各構成要素は、回路（または集積回路）でもよい。これらの回路は、全体として１つの回路を構成してもよいし、それぞれ別々の回路でもよい。また、これらの回路は、それぞれ、汎用的な回路でもよいし、専用の回路でもよい。
【０１１４】
また、本発明の全般的または具体的な態様は、システム、装置、方法、集積回路、コンピュータプログラムまたはコンピュータ読み取り可能なＣＤ－ＲＯＭなどの記録媒体で実現されてもよい。また、本発明の全般的または具体的な態様は、システム、装置、方法、集積回路、コンピュータプログラム及び記録媒体の任意な組み合わせで実現されてもよい。
【０１１５】
例えば、本発明は、上記実施の形態の情報端末、第一管理装置、第二管理装置、制御装置、または、電気錠システム（制御装置及び電気錠）として実現されてもよい。
【０１１６】
また、本発明は、上記実施の形態の情報処理システムなどのコンピュータが実行する情報処理方法として実現されてもよい。また、本発明は、情報処理方法をコンピュータに実行させるためのプログラムとして実現されてもよい。本発明は、このようなプログラムが記録されたコンピュータ読み取り可能な非一時的な記録媒体として実現されてもよい。
【０１１７】
また、本発明は、汎用の情報端末を、上記実施の形態の情報端末として機能させるためのアプリケーションプログラムとして実現されてもよい。本発明は、このようなアプリケーションプログラムが記録されたコンピュータ読み取り可能な非一時的な記録媒体として実現されてもよい。
【０１１８】
その他、各実施の形態に対して当業者が思いつく各種変形を施して得られる形態、または、本発明の趣旨を逸脱しない範囲で各実施の形態における構成要素及び機能を任意に組

み合わせることで実現される形態も本発明に含まれる。

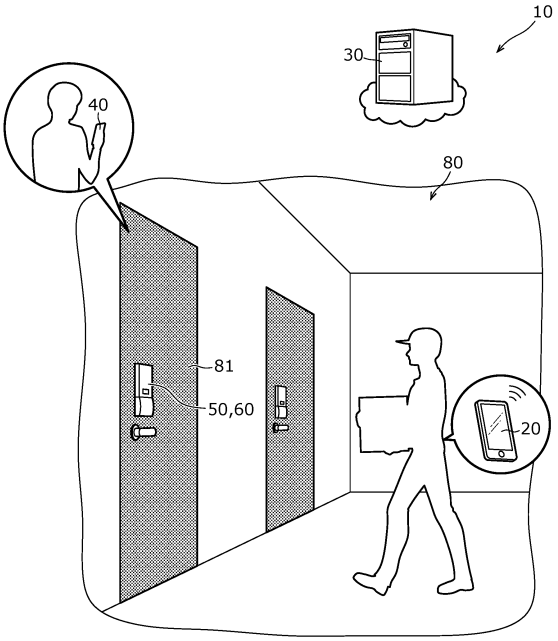
【符号の説明】

【０１１９】

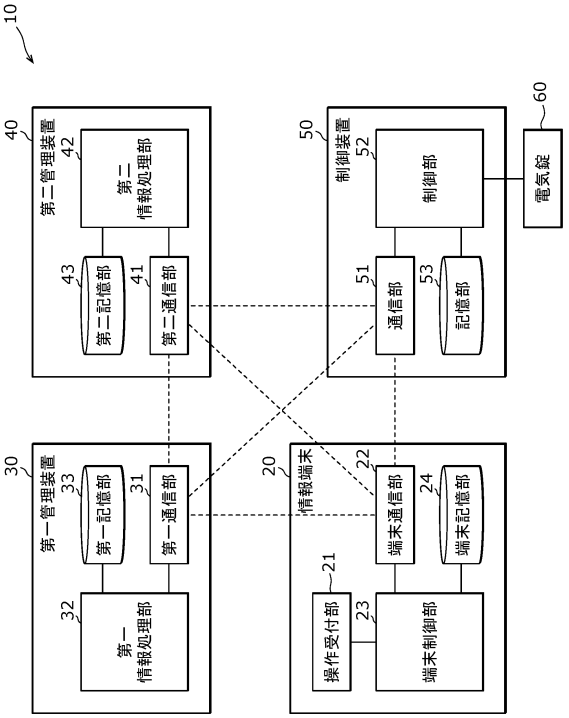
１０、１０ａ　情報処理システム
２０　情報端末
２１　操作受付部
２２　端末通信部
２３　端末制御部
２４　端末記憶部
３０　第一管理装置
３１　第一通信部
３２　第一情報処理部
３３　第一記憶部
４０　第二管理装置
４１　第二通信部
４２　第二情報処理部
４３　第二記憶部
５０　制御装置
５１　通信部
５２　制御部
５３　記憶部
６０　電気錠
７０　自動ドア
８０　施設
８１　ドア
８３　専有部
８４　共用部

【図面】

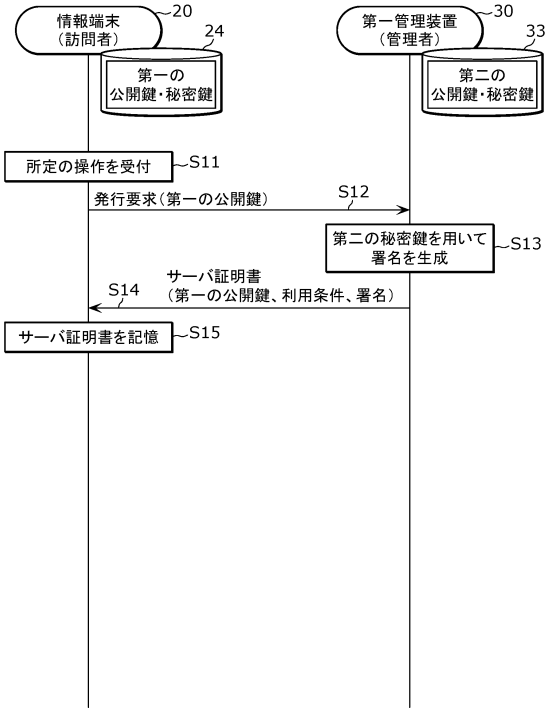
【図１】


10
30
40
80
81
50,60
20

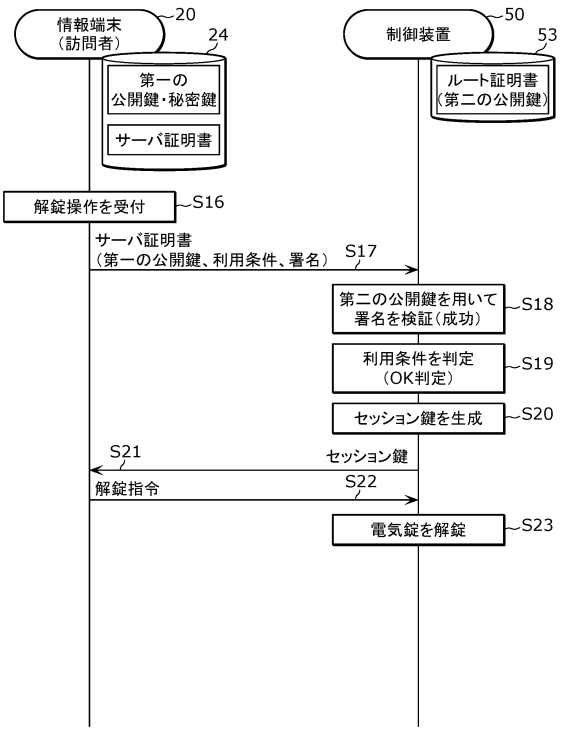
【図２】


10
40
第二管理装置
42
第二
情報処理部
43
第二記憶部
41
第二通信部
50
制御装置
52
制御部
60
電気錠
51
通信部
53
記憶部
30
第一管理装置
33
第一記憶部
31
第一通信部
32
第一
情報処理部
20
情報端末
22
端末通信部
24
端末記憶部
21
操作受付部
23
端末制御部

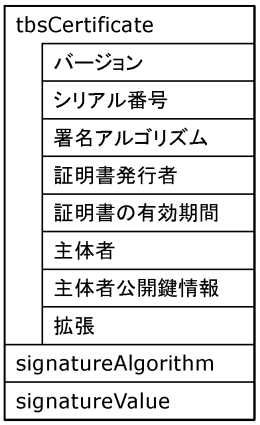
【図３】


情報端末
（訪問者）
20
24
第一の
公開鍵・秘密鍵
第一管理装置
（管理者）
30
33
第二の
公開鍵・秘密鍵
所定の操作を受付
S11
発行要求（第一の公開鍵）
S12
第二の秘密鍵を用いて
署名を生成
S13
サーバ証明書
（第一の公開鍵、利用条件、署名）
S14
サーバ証明書を記憶
S15

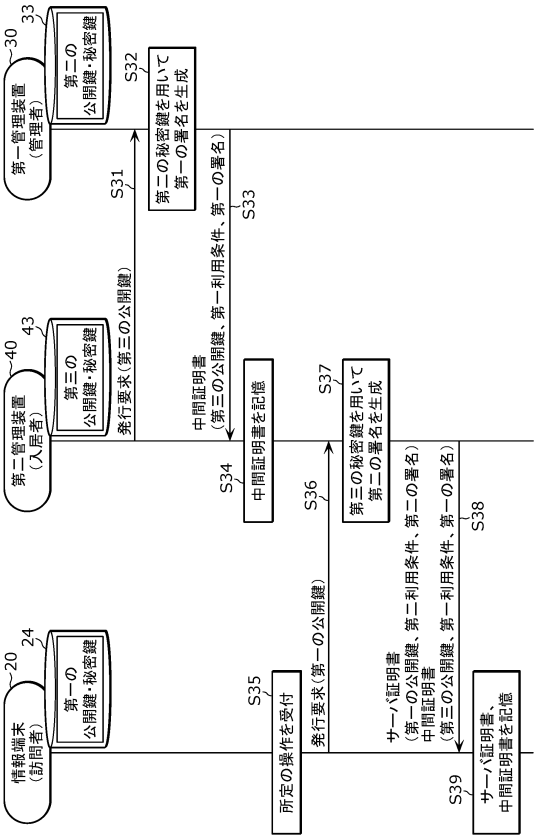
【図４】


情報端末
（訪問者）
20
24
第一の
公開鍵・秘密鍵
サーバ証明書
制御装置
50
53
ルート証明書
（第二の公開鍵）
解錠操作を受付
S16
サーバ証明書
（第一の公開鍵、利用条件、署名）
S17
第二の公開鍵を用いて
署名を検証（成功）
S18
利用条件を判定
（OK判定）
S19
セッション鍵を生成
S20
S21
セッション鍵
解錠指令
S22
電気錠を解錠
S23

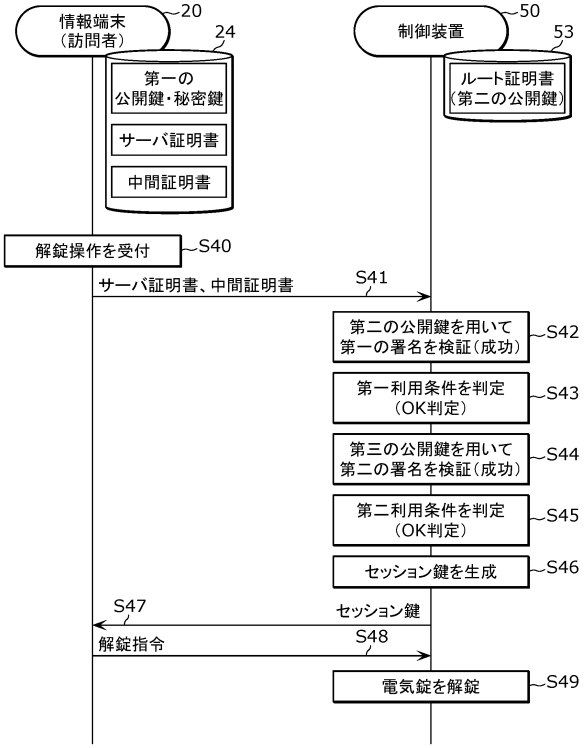
【図５】


tbsCertificate
バージョン
シリアル番号
署名アルゴリズム
証明書発行者
証明書の有効期間
主体者
主体者公開鍵情報
拡張
signatureAlgorithm
signatureValue

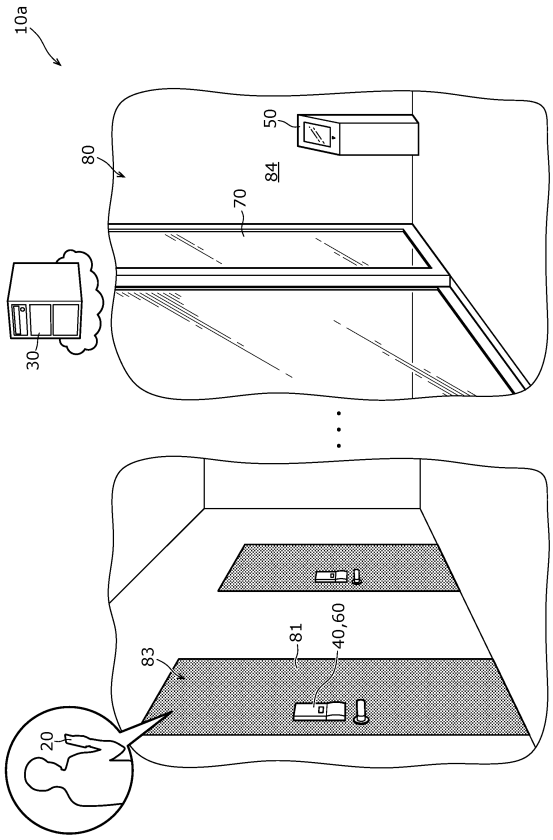
【図６】


第一管理装置（管理者）
30
第二の公開鍵・秘密鍵
33
S32
第二の秘密鍵を用いて第一の署名を生成
S31
発行要求（第三の公開鍵）
S33
中間証明書（第三の公開鍵、第一利用条件、第一の署名）
第二管理装置（入居者）
40
第三の公開鍵・秘密鍵
43
S34
中間証明書を記憶
S37
第三の秘密鍵を用いて第二の署名を生成
S36
発行要求（第一の公開鍵）
S38
サーバ証明書（第一の公開鍵、第一利用条件、第二の署名）中間証明書（第三の公開鍵、第一利用条件、第一の署名）
情報端末（訪問者）
20
第一の公開鍵・秘密鍵
24
S35
所定の操作を受付
S39
サーバ証明書、中間証明書を記憶

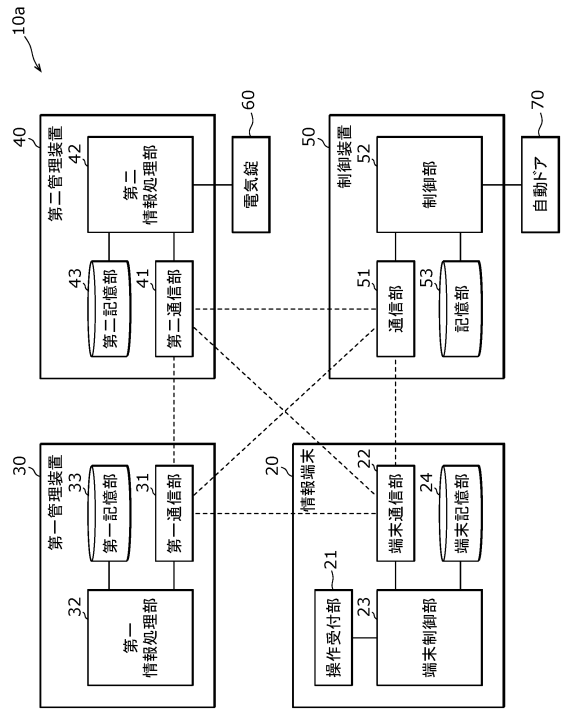
【図７】


情報端末（訪問者）
20
24
第一の公開鍵・秘密鍵
サーバ証明書
中間証明書
制御装置
50
53
ルート証明書（第二の公開鍵）
解錠操作を受付
S40
サーバ証明書、中間証明書
S41
第二の公開鍵を用いて第一の署名を検証（成功）
S42
第一利用条件を判定（OK判定）
S43
第三の公開鍵を用いて第二の署名を検証（成功）
S44
第二利用条件を判定（OK判定）
S45
セッション鍵を生成
S46
S47
セッション鍵
解錠指令
S48
電気錠を解錠
S49

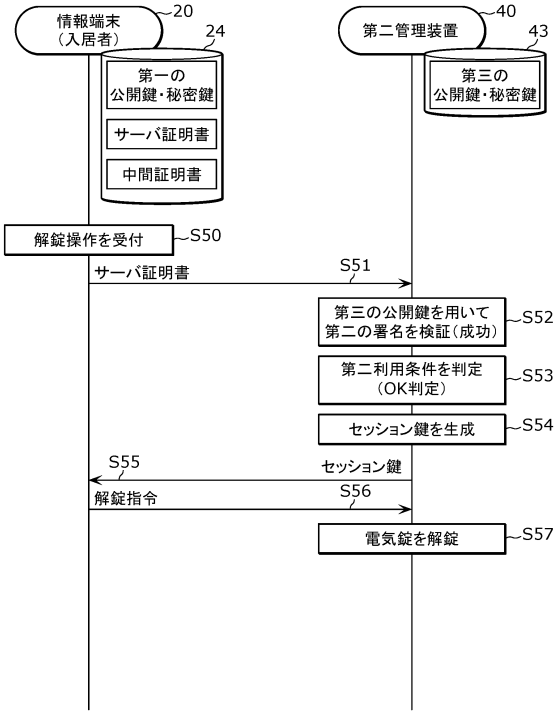
【図８】


10a
80
50
84
70
30
81
40,60
83
20

【図９】


10a
40
第二管理装置
42
第二
情報処理部
60
電気錠
50
制御装置
52
制御部
70
自動ドア
43
第二記憶部
41
第二通信部
51
通信部
53
記憶部
30
第一管理装置
33
第一記憶部
31
第一通信部
20
情報端末
22
端末通信部
24
端末記憶部
32
第一
情報処理部
21
操作受付部
23
端末制御部

【図１０】


情報端末
（入居者）
20
24
第一の
公開鍵・秘密鍵
サーバ証明書
中間証明書
第二管理装置
40
43
第三の
公開鍵・秘密鍵
解錠操作を受付
S50
サーバ証明書
S51
第三の公開鍵を用いて
第二の署名を検証（成功）
S52
第二利用条件を判定
（OK判定）
S53
セッション鍵を生成
S54
S55
セッション鍵
S56
解錠指令
電気錠を解錠
S57

フロントページの続き

(51)国際特許分類
H04L 9/32 (2006.01)

FI
H04L 9/32 200B
H04L 9/32 200F

審査官 砂川 充

(56)参考文献
特開２０１９－１７３５２３（ＪＰ，Ａ）
特開２０１９－１７６４４１（ＪＰ，Ａ）
特開２００３－３４３１３３（ＪＰ，Ａ）
特開２０１４－１５９６９２（ＪＰ，Ａ）
特開２０１６－２２３２１２（ＪＰ，Ａ）
米国特許出願公開第２０１９／０３２７０９８（ＵＳ，Ａ１）

(58)調査した分野 (Int.Cl.，ＤＢ名)
Ｅ０５Ｂ １／００－８５／２８
Ｅ０５Ｆ １／００－１７／００
Ｇ０６Ｆ ２１／３１－２１／４３
Ｇ０７Ｃ ９／００－ ９／３８
Ｈ０４Ｌ ９／００－ ９／４０