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

特許第5614197号
(P5614197)

(45)発行日　平成26年10月29日(2014.10.29)　(24)登録日　平成26年9月19日(2014.9.19)

(51)Int.Cl.　F I
H04L 9/32 (2006.01)　H04L 9/00 675B
H04L 12/22 (2006.01)　H04L 9/00 675Z
H04L 9/00 675D
H04L 12/22

請求項の数 6　(全 47 頁)

(21)出願番号　特願2010-208614(P2010-208614)
(22)出願日　平成22年9月16日(2010.9.16)
(65)公開番号　特開2012-65207(P2012-65207A)
(43)公開日　平成24年3月29日(2012.3.29)
審査請求日　平成25年8月13日(2013.8.13)

(73)特許権者　000006747
株式会社リコー
東京都大田区中馬込１丁目３番６号
(74)代理人　100123881
弁理士　大澤　豊
(74)代理人　100080931
弁理士　大澤　敬
(72)発明者　千代　直貴
東京都大田区中馬込１丁目３番６号　株式会社リコー内
(72)発明者　佐藤　淳
東京都大田区中馬込１丁目３番６号　株式会社リコー内

審査官　青木　重徳

最終頁に続く

(54)【発明の名称】通信装置及び管理システム

(57)【特許請求の範囲】
【請求項１】
通信装置であって、
端末装置及び、該端末装置を管理する管理装置と通信するための通信手段と、
当該通信装置を一意に特定するための識別情報を記憶する第１の記憶手段と、
通信相手の装置に認証を受けるための当該通信装置の証明書と、通信相手の装置から送信されてくる、特定の発行元が発行した証明書の正当性を確認するための確認用データとを記憶する第２の記憶手段と、
通信先とする管理装置のアドレス情報を記憶する管理装置アドレス記憶手段と、
前記第２の記憶手段が記憶している確認用データが前記端末装置から送信されてくる証明書の発行元と対応しないためにその証明書の正当性が確認できなかった場合に、前記管理装置アドレス記憶手段が記憶するアドレス情報に従い、通信先の管理装置に対して、前記第１の記憶手段が記憶している識別情報と、前記端末装置から送信されてきた証明書の発行元の情報とを送信すると共に、該通信先の管理装置に当該通信装置の更新用の証明書の取得を依頼する証明書更新依頼手段と、
前記証明書更新依頼手段による依頼に応じて前記管理装置から送信されてくるデータのうち、前記管理装置に送信した情報が示す発行元により発行された当該通信装置の証明書及び、該発行元が発行した証明書の正当性を確認するための確認用データを、認証に使用する新たな証明書及び確認用データとして前記第２の記憶手段に記憶させるとともに、該新たな証明書を用いた通信による通信先とする管理装置のアドレス情報を、前記管理装置

アドレス記憶手段に記憶させる証明書設定手段とを設けたことを特徴とする通信装置。
【請求項２】
通信装置であって、
端末装置及び、該端末装置を管理する管理装置と通信するための通信手段と、
当該通信装置を一意に特定するための識別情報を記憶する第１の記憶手段と、
通信相手とする端末装置の識別情報及び該端末装置のアドレス情報を記憶する第２の記憶手段と、
通信相手の装置に認証を受けるための当該通信装置の証明書と、通信相手の装置から送信されてくる、特定の発行元が発行した証明書の正当性を確認するための確認用データとを記憶する第３の記憶手段と、
通信先とする管理装置のアドレス情報を記憶する管理装置アドレス記憶手段と、
前記第３の記憶手段に記憶している証明書を更新する旨の指示を受け付ける受付手段と、
当該通信装置の証明書として、どの発行元が発行した証明書を取得するかを示す情報を、更新可能に記憶する発行元記憶手段と、
前記受付手段が証明書を更新する旨の前記指示を受け付けた場合に、前記管理装置アドレス記憶手段が記憶するアドレス情報に従い、通信先の管理装置に対して、前記第１の記憶手段が記憶している識別情報と、前記発行元記憶手段が記憶する発行元の情報とを送信すると共に、該通信先の管理装置に当該通信装置の更新用の証明書の取得を依頼する証明書更新依頼手段と、
前記証明書更新依頼手段による依頼に応じて前記管理装置から送信されてくるデータのうち、前記管理装置に送信した情報が示す発行元により発行された当該通信装置の証明書及び、該発行元が発行した証明書の正当性を確認するための確認用データを、認証に使用する新たな証明書及び確認用データとして前記第３の記憶手段に記憶させるとともに、該新たな証明書を用いた通信による通信先とする管理装置のアドレス情報を、前記管理装置アドレス記憶手段に記憶させる証明書設定手段と、
少なくとも前記証明書更新依頼手段が前記管理装置へ更新用の証明書の取得を依頼する前に、前記第２の記憶手段に識別情報が登録されている各端末装置から、該端末装置が記憶している該端末装置の証明書の発行元の情報を取得し、該各端末装置のうち該発行元が前記発行元記憶手段が記憶する発行元と異なる各要更新端末装置について、該要更新端末装置の識別情報及び前記発行元記憶手段が記憶する発行元の情報を、前記管理装置アドレス記憶手段が記憶するアドレス情報に従い、通信先の前記管理装置に送信すると共に、該通信先の管理装置に該要更新端末装置の更新用の証明書の取得を依頼し、その依頼に応じて該通信先の管理装置から送信されてくる、前記発行元記憶手段が記憶する発行元が発行した該要更新端末装置の証明書と、前記発行元記憶手段が記憶する発行元が発行した証明書の正当性を確認するための確認用データとを、該要更新端末装置に送信する証明書送信手段とを設けたことを特徴とする通信装置。
【請求項３】
通信装置であって、
端末装置及び、該端末装置を管理する管理装置と通信するための通信手段と、
当該通信装置を一意に特定するための識別情報を記憶する第１の記憶手段と、
通信相手とする端末装置の識別情報及び該端末装置のアドレス情報を記憶する第２の記憶手段と、
通信相手の装置に認証を受けるための当該通信装置の証明書と、通信相手の装置から送信されてくる、特定の発行元が発行した証明書の正当性を確認するための確認用データとを記憶する第３の記憶手段と、
通信先とする管理装置のアドレス情報を記憶する管理装置アドレス記憶手段と、
前記第３の記憶手段に記憶している証明書を更新する旨の指示を受け付ける受付手段と、
当該通信装置の証明書として、どの発行元が発行した証明書を取得するかを示す情報を

、更新可能に記憶する発行元記憶手段と、
前記受付手段が証明書を更新する旨の前記指示を受け付けた場合に、前記管理装置アドレス記憶手段が記憶するアドレス情報に従い、通信先の管理装置に対して、前記第１の記憶手段が記憶している識別情報と、前記発行元記憶手段が記憶する発行元の情報とを送信すると共に、該通信先の管理装置に当該通信装置の更新用の証明書の取得を依頼する証明書更新依頼手段と、
前記証明書更新依頼手段による依頼に応じて前記管理装置から送信されてくるデータのうち、前記管理装置に送信した情報が示す発行元により発行された当該通信装置の証明書及び、該発行元が発行した証明書の正当性を確認するための確認用データを、認証に使用する新たな証明書及び確認用データとして前記第３の記憶手段に記憶させるとともに、該新たな証明書を用いた通信による通信先とする管理装置のアドレス情報を、前記管理装置アドレス記憶手段に記憶させる証明書設定手段と、
少なくとも前記証明書更新依頼手段が前記管理装置へ更新用の証明書の取得を依頼する前に、前記第２の記憶手段に識別情報が登録されている各端末装置から、該端末装置が記憶している該端末装置の証明書の発行元の情報及び、どのアドレスにアクセスされた場合に通信相手の装置に認証を受けるためにその証明書を使用するかを示すアドレス情報を取得し、該各端末装置のうち、前記取得した発行元に前記発行元記憶手段が記憶する発行元が含まれている各更新可能端末装置について、前記第２の記憶手段に記憶している該更新可能端末装置のアドレス情報を、該更新可能端末装置から受信した該発行元記憶手段が記憶する発行元と対応するアドレス情報に更新する端末情報更新手段とを設けたことを特徴とする通信装置。
【請求項４】
端末装置と、該端末装置を管理するための複数の管理装置と、前記端末装置と前記管理装置との間の通信を仲介する仲介装置とを備えた管理システムであって、
前記仲介装置に、
当該仲介装置を一意に特定するための識別情報を記憶する第１の記憶手段と、
通信相手の装置に認証を受けるための当該仲介装置の証明書と、通信相手の装置から送信されてくる、特定の発行元が発行した証明書の正当性を確認するための確認用データとを記憶する第２の記憶手段と、
通信先とする管理装置のアドレス情報を記憶する管理装置アドレス記憶手段と、
前記第２の記憶手段が記憶している確認用データが前記端末装置から送信されてくる証明書の発行元と対応しないためにその証明書の正当性が確認できなかった場合に、前記管理装置アドレス記憶手段が記憶するアドレス情報に従い、通信先の管理装置に対して、前記第１の記憶手段が記憶している識別情報と、前記端末装置から送信されてきた証明書の発行元の情報とを送信すると共に、該通信先の管理装置に当該仲介装置の更新用の証明書の取得を依頼する証明書更新依頼手段と、
前記証明書更新依頼手段による依頼に応じて前記管理装置から送信されてくるデータのうち、前記管理装置に送信した情報が示す発行元により発行された当該仲介装置の証明書及び、該発行元が発行した証明書の正当性を確認するための確認用データを、認証に使用する新たな証明書及び確認用データとして前記第２の記憶手段に記憶させるとともに、該新たな証明書を用いた通信による通信先とする管理装置のアドレス情報を、前記管理装置アドレス記憶手段に記憶させる証明書設定手段とを設け、
前記管理装置の少なくとも１つに、
前記仲介装置から前記更新用の証明書の取得を依頼された場合に、前記仲介装置から受信した識別情報を前記仲介装置から受信した発行元の情報が示す証明書の発行元に送信して、該識別情報を含む新たな証明書の発行を依頼する証明書発行依頼手段と、
前記発行元から、前記証明書発行依頼手段による依頼に基づいて発行された新たな証明書を取得する証明書取得手段と、
前記発行元が発行した証明書の正当性を確認するための確認用データを取得する確認用データ取得手段と、

前記証明書取得手段が取得した新たな証明書と、前記確認用データ取得手段が取得した確認用データと、該新たな証明書を用いた通信による通信先とする管理装置のアドレスとを前記仲介装置に送信する証明書送信手段とを設け、

前記端末装置に、

通信相手の装置に認証を受けるための当該端末装置の証明書と、通信相手の装置から送信されてくる証明書の正当性を確認するための確認用データとを記憶する第３の記憶手段と、

前記第３の記憶手段が記憶する当該端末装置の証明書を、認証を受けるために前記仲介装置に送信する証明書提供手段とを設けたことを特徴とする管理システム。

【請求項５】

端末装置と、該端末装置を管理するための複数の管理装置と、前記端末装置と前記管理装置との間の通信を仲介する仲介装置とを備えた管理システムであって、

前記仲介装置に、

当該仲介装置を一意に特定するための識別情報を記憶する第１の記憶手段と、

通信相手とする端末装置の識別情報及び該端末装置のアドレス情報を記憶する第２の記憶手段と、

通信相手の装置に認証を受けるための当該仲介装置の証明書と、通信相手の装置から送信されてくる、特定の発行元が発行した証明書の正当性を確認するための確認用データとを記憶する第３の記憶手段と、

通信先とする管理装置のアドレス情報を記憶する管理装置アドレス記憶手段と、

前記第３の記憶手段に記憶している証明書を更新する旨の指示を受け付ける受付手段と、

当該仲介装置の証明書として、どの発行元が発行した証明書を取得するかを示す情報を、更新可能に記憶する発行元記憶手段と、

前記受付手段が証明書を更新する旨の前記指示を受け付けた場合に、前記管理装置アドレス記憶手段が記憶するアドレス情報に従い、通信先の管理装置に対して、前記第１の記憶手段が記憶している識別情報と、前記発行元記憶手段が記憶する発行元の情報とを送信すると共に、該通信先の管理装置に当該仲介装置の更新用の証明書の取得を依頼する証明書更新依頼手段と、

前記証明書更新依頼手段による依頼に応じて前記管理装置から送信されてくるデータのうち、前記管理装置に送信した情報が示す発行元により発行された当該仲介装置の証明書及び、該発行元が発行した証明書の正当性を確認するための確認用データを、認証に使用する新たな証明書及び確認用データとして前記第３の記憶手段に記憶させるとともに、該新たな証明書を用いた通信による通信先とする管理装置のアドレス情報を、前記管理装置アドレス記憶手段に記憶させる証明書設定手段と、

少なくとも前記証明書更新依頼手段が前記管理装置へ更新用の証明書の取得を依頼する前に、前記第２の記憶手段に識別情報が登録されている各端末装置から、該端末装置が記憶している該端末装置の証明書の発行元の情報を取得し、該各端末装置のうち該発行元が前記発行元記憶手段が記憶する発行元と異なる各要更新端末装置について、該要更新端末装置の識別情報及び前記発行元記憶手段が記憶する発行元の情報を、前記管理装置アドレス記憶手段が記憶するアドレス情報に従い、通信先の管理装置に送信すると共に、該通信先の管理装置に該要更新端末装置の更新用の証明書の取得を依頼し、その依頼に応じて該通信先の管理装置から送信されてくる、前記発行元記憶手段が記憶する発行元が発行した該要更新端末装置の証明書と、前記発行元記憶手段が記憶する発行元が発行した証明書の正当性を確認するための確認用データとを、該要更新端末装置に送信する証明書送信手段とを設け、

前記管理装置の少なくとも１つに、

前記仲介装置から前記更新用の証明書の取得を依頼された場合に、前記仲介装置から受信した識別情報を前記仲介装置から受信した発行元の情報が示す証明書の発行元に送信して、該識別情報を含む新たな証明書の発行を依頼する証明書発行依頼手段と、

前記発行元から、前記証明書発行依頼手段による依頼に基づいて発行された新たな証明書を取得する証明書取得手段と、
前記発行元が発行した証明書の正当性を確認するための確認用データを取得する確認用データ取得手段と、
前記証明書取得手段が取得した新たな証明書と、前記確認用データ取得手段が取得した確認用データと、該新たな証明書を用いた通信による通信先とする管理装置のアドレスとを前記仲介装置に送信する証明書送信手段とを設け、
前記端末装置に、
通信相手の装置に認証を受けるための当該端末装置の証明書と、通信相手の装置から送信されてくる証明書の正当性を確認するための確認用データとを記憶する第４の記憶手段と、
当該端末装置を一意に特定するための識別情報を記憶する第５の記憶手段と、
前記仲介装置からの要求に応じて、前記第５の記憶手段に記憶している当該端末装置の識別情報を該仲介装置に送信する識別情報送信手段と、
前記仲介装置から送信されてきた当該端末装置の証明書及び確認用データを、通信相手へのアクセスに使用する新たな証明書及び確認用データとして前記第４の記憶手段に記憶させる第２の証明書設定手段とを設けたことを特徴とする管理システム。
【請求項６】
端末装置と、該端末装置を管理するための複数の管理装置と、前記端末装置と前記管理装置との間の通信を仲介する仲介装置とを備えた管理システムであって、
前記仲介装置に、
当該仲介装置を一意に特定するための識別情報を記憶する第１の記憶手段と、
通信相手とする端末装置の識別情報及び該端末装置のアドレス情報を記憶する第２の記憶手段と、
通信相手の装置に認証を受けるための当該仲介装置の証明書と、通信相手の装置から送信されてくる、特定の発行元が発行した証明書の正当性を確認するための確認用データとを記憶する第３の記憶手段と、
通信先とする管理装置のアドレス情報を記憶する管理装置アドレス記憶手段と、
前記第３の記憶手段に記憶している証明書を更新する旨の指示を受け付ける受付手段と、
当該仲介装置の証明書として、どの発行元が発行した証明書を取得するかを示す情報を、更新可能に記憶する発行元記憶手段と、
前記受付手段が証明書を更新する旨の前記指示を受け付けた場合に、前記管理装置アドレス記憶手段が記憶するアドレス情報に従い、通信先の管理装置に対して、前記第１の記憶手段が記憶している識別情報と、前記発行元記憶手段が記憶する発行元の情報とを送信すると共に、該通信先の管理装置に当該仲介装置の更新用の証明書の取得を依頼する証明書更新依頼手段と、
前記証明書更新依頼手段による依頼に応じて前記管理装置から送信されてくるデータのうち、前記管理装置に送信した情報が示す発行元により発行された当該仲介装置の証明書及び、該発行元が発行した証明書の正当性を確認するための確認用データを、認証に使用する新たな証明書及び確認用データとして前記第３の記憶手段に記憶させるとともに、該新たな証明書を用いた通信による通信先とする管理装置のアドレス情報を、前記管理装置アドレス記憶手段に記憶させる証明書設定手段と、
少なくとも前記証明書更新依頼手段が前記管理装置へ更新用の証明書の取得を依頼する前に、前記第２の記憶手段に識別情報が登録されている各端末装置から、該端末装置が記憶している該端末装置の証明書の発行元の情報及び、どのアドレスにアクセスされた場合に通信相手の装置に認証を受けるためにその証明書を使用するかを示すアドレス情報を取得し、該各端末装置のうち、前記取得した発行元に前記発行元記憶手段が記憶する発行元が含まれている各更新可能端末装置について、前記第２の記憶手段に記憶している該更新可能端末装置のアドレス情報を、該更新可能端末装置から受信した該発行元記憶手段が記

憶する発行元と対応するアドレス情報に更新する端末情報更新手段とを設け、
前記管理装置の少なくとも１つに、
前記仲介装置から前記更新用の証明書の取得を依頼された場合に、前記仲介装置から受信した識別情報を前記仲介装置から受信した発行元の情報が示す証明書の発行元に送信して、該識別情報を含む新たな証明書の発行を依頼する証明書発行依頼手段と、
前記発行元から、前記証明書発行依頼手段による依頼に基づいて発行された新たな証明書を取得する証明書取得手段と、
前記発行元が発行した証明書の正当性を確認するための確認用データを取得する確認用データ取得手段と、
前記証明書取得手段が取得した新たな証明書と、前記確認用データ取得手段が取得した確認用データと、該新たな証明書を用いた通信による通信先とする管理装置のアドレスとを前記仲介装置に送信する証明書送信手段とを設け、
前記端末装置に、
当該端末装置の異なる複数のアドレスと対応させて、該アドレスにアクセスされた場合に通信相手の装置に認証を受けるために使用するデータとして、それぞれ異なる発行元が発行した当該端末装置の証明書と、該発行元が発行した証明書の正当性を確認するための確認用データを記憶する第４の記憶手段と、
前記仲介装置からの要求に応じて、前記第４の記憶手段に記憶している情報に基づき、当該端末装置が記憶している当該端末装置の証明書の発行元の情報及び、どのアドレスにアクセスされた場合に通信相手の装置に認証を受けるためにその証明書を使用するかを示すアドレス情報を該仲介装置に送信するアドレス情報送信手段とを設けたことを特徴とする管理システム。

【発明の詳細な説明】
【技術分野】
【０００１】
この発明は、端末装置及びそれを管理する管理装置と通信する通信装置、上記端末装置と上記管理装置と上記通信装置（上記端末装置と上記管理装置との間の通信を仲介する仲介装置）を備えた管理システムに関する。
【背景技術】
【０００２】
従来から、例えば通信機能を有する画像形成装置（例えば複写機，ファクシミリ装置，プリンタ，複合機，又は印刷機）やスキャナ装置等の端末装置（以下「機器」ともいう）を管理する管理システムにおいては、セキュリティを適切に確保することが重要視されている。
そこで、このような管理システムでは、不正な利用者による「改ざん」や、正規の利用者への「なりすまし」を困難にする目的で、例えば、クライアント装置である端末装置（例えば、Ｌｉｎｕｘベース（Ｌｉｎｕｘ：登録商標）のクライアント専用ＯＳを搭載した端末装置）と、サーバ装置である管理装置との間ではセキュア・ソケット・レイヤ（Secure Socket Layer：ＳＳＬ（「エスエスエル」と略称する）による相互認証及び暗号化通信を行っている。
【０００３】
上記ＳＳＬは、インタネット上で情報を暗号化して送受信するプロトコルであり、公開鍵暗号，秘密鍵暗号，デジタル証明書，ハッシュ関数を含むセキュリティ技術を組み合わせてデータの盗聴や「改ざん」や「なりすまし」を防ぐことができる技術である。
そして、上記ＳＳＬによる通信を実施するため、端末装置と管理装置の両方が電子データによる所定フォーマットの証明書を保持する必要がある。
【０００４】
従来、通信端末が、証明書の発行要求と共に、その証明書を設定する端末装置の機種機番情報を証明書管理装置に送信し、その要求に応じて、上記発行要求と共に送信した識別情報を含む証明書を証明書管理装置が発行して送信してくるので、通信端末がこれを受信

し、工場端末を介してその電子証明書に含まれる機種機番情報と同じ機種機番を有する画像機器（端末装置）に設定することにより、複数の画像機器毎に対して一意な証明書を適切に割り当てる管理システム（例えば、特許文献１参照）があった。

【０００５】

近年は、管理システムのセキュリティ機能強度を高めるため、管理システム内の端末装置と管理装置間のＳＳＬ相互認証で利用する証明書の公開鍵の鍵長を長くすることが検討されている。

上述のようにセキュリティ機能強度を高めるには、管理システム上に、公開鍵の鍵長が短い証明書を発行する既存のＣＡとは異なる、公開鍵の鍵長を長くした証明書を発行できる新たな認証機関（「認証局」ともいう、（Certificate Authority：ＣＡ））を運用させる必要がある。

【発明の概要】

【発明が解決しようとする課題】

【０００６】

しかしながら、特許文献１に記載の管理システムでは、異なるフォーマットの又は異なる認証処理に対応した証明書を発行する複数のＣＡの運用は考慮されておらず、例えば、鍵長の短い証明書で運用する端末装置と、鍵長の長い証明書で運用する端末装置とが混在する際に、次の原因で、端末装置と管理装置との間の通信のセキュリティについて下位互換を維持しつつセキュリティ強度を容易に上げることができないという問題があった。

【０００７】

上記問題が発生する原因としては、端末装置とそれを管理している仲介装置が保持するそれぞれの証明書の発行元が異なるため、通信相手が送信してきた証明書の正当性を確認できずに、認証を成功させられなくなることが考えられる。

この発明は上記の点に鑑みてなされたものであり、異なるフォーマットの又は異なる認証処理に対応した証明書を発行する複数のＣＡを運用して、端末装置と管理装置との間の通信のセキュリティについて下位互換を維持しつつセキュリティ強度を容易に上げることができるようにすることを目的とする。

【課題を解決するための手段】

【０００８】

この発明は、上記の目的を達成するため、以下の（１）～（３）に示す通信装置及び（４）～（６）に示す管理システムをそれぞれ提供する。

（１）通信装置であって、端末装置及び、その端末装置を管理する管理装置と通信するための通信手段と、当該通信装置を一意に特定するための識別情報を記憶する第１の記憶手段と、通信相手の装置に認証を受けるための当該通信装置の証明書と、通信相手の装置から送信されてくる、特定の発行元が発行した証明書の正当性を確認するための確認用データとを記憶する第２の記憶手段と、通信先とする管理装置のアドレス情報を記憶する管理装置アドレス記憶手段と、上記第２の記憶手段が記憶している確認用データが上記端末装置から送信されてくる証明書の発行元と対応しないためにその証明書の正当性が確認できなかった場合に、上記管理装置アドレス記憶手段が記憶するアドレス情報に従い、通信先の管理装置に対して、上記第１の記憶手段が記憶している識別情報と、上記端末装置から送信されてきた証明書の発行元の情報とを送信すると共に、該通信先の管理装置に当該通信装置の更新用の証明書の取得を依頼する証明書更新依頼手段と、上記証明書更新依頼手段による依頼に応じて上記管理装置から送信されてくるデータのうち、上記管理装置に送信した情報が示す発行元により発行された当該通信装置の証明書及び、その発行元が発行した証明書の正当性を確認するための確認用データを、認証に使用する新たな証明書及び確認用データとして上記第２の記憶手段に記憶させるとともに、該新たな証明書を用いた通信による通信先とする管理装置のアドレス情報を、上記管理装置アドレス記憶手段に記憶させる証明書設定手段とを設けたものである。

【００１１】

（２）通信装置であって、端末装置及び、その端末装置を管理する管理装置と通信するた

めの通信手段と、当該通信装置を一意に特定するための識別情報を記憶する第１の記憶手段と、通信相手とする端末装置の識別情報及びその端末装置のアドレス情報を記憶する第２の記憶手段と、通信相手の装置に認証を受けるための当該通信装置の証明書と、通信相手の装置から送信されてくる、特定の発行元が発行した証明書の正当性を確認するための確認用データとを記憶する第３の記憶手段と、通信先とする管理装置のアドレス情報を記憶する管理装置アドレス記憶手段と、上記第３の記憶手段に記憶している証明書を更新する旨の指示を受け付ける受付手段と、当該通信装置の証明書として、どの発行元が発行した証明書を取得するかを示す情報を、更新可能に記憶する発行元記憶手段と、上記受付手段が証明書を更新する旨の上記指示を受け付けた場合に、上記管理装置アドレス記憶手段が記憶するアドレス情報に従い、通信先の管理装置に対して、上記第１の記憶手段が記憶している識別情報と、上記発行元記憶手段が記憶する発行元の情報とを送信すると共に、該通信先の管理装置に当該通信装置の更新用の証明書の取得を依頼する証明書更新依頼手段と、上記証明書更新依頼手段による依頼に応じて上記管理装置から送信されてくるデータのうち、上記管理装置に送信した情報が示す発行元により発行された当該通信装置の証明書及び、その発行元が発行した証明書の正当性を確認するための確認用データを、認証に使用する新たな証明書及び確認用データとして上記第３の記憶手段に記憶させるとともに、該新たな証明書を用いた通信による通信先とする管理装置のアドレス情報を、上記管理装置アドレス記憶手段に記憶させる証明書設定手段と、少なくとも上記証明書更新依頼手段が上記管理装置へ更新用の証明書の取得を依頼する前に、上記第２の記憶手段に識別情報が登録されている各端末装置から、その端末装置が記憶しているその端末装置の証明書の発行元の情報を取得し、その各端末装置のうちその発行元が上記発行元記憶手段が記憶する発行元と異なる各要更新端末装置について、その要更新端末装置の識別情報及び上記発行元記憶手段が記憶する発行元の情報を、上記管理装置アドレス記憶手段が記憶するアドレス情報に従い、通信先の管理装置に送信すると共に、該通信先の管理装置にその要更新端末装置の更新用の証明書の取得を依頼し、その依頼に応じて該通信先の管理装置から送信されてくる、上記発行元記憶手段が記憶する発行元が発行したその要更新端末装置の証明書と、上記発行元記憶手段が記憶する発行元が発行した証明書の正当性を確認するための確認用データとを、その要更新端末装置に送信する証明書送信手段とを設けたものである。

【００１２】

（３）通信装置であって、端末装置及び、その端末装置を管理する管理装置と通信するための通信手段と、当該通信装置を一意に特定するための識別情報を記憶する第１の記憶手段と、通信相手とする端末装置の識別情報及びその端末装置のアドレス情報を記憶する第２の記憶手段と、通信相手の装置に認証を受けるための当該通信装置の証明書と、通信相手の装置から送信されてくる、特定の発行元が発行した証明書の正当性を確認するための確認用データとを記憶する第３の記憶手段と、通信先とする管理装置のアドレス情報を記憶する管理装置アドレス記憶手段と、上記第３の記憶手段に記憶している証明書を更新する旨の指示を受け付ける受付手段と、当該通信装置の証明書として、どの発行元が発行した証明書を取得するかを示す情報を、更新可能に記憶する発行元記憶手段と、上記受付手段が証明書を更新する旨の上記指示を受け付けた場合に、上記管理装置アドレス記憶手段が記憶するアドレス情報に従い、通信先の管理装置に対して、上記第１の記憶手段が記憶している識別情報と、上記発行元記憶手段が記憶する発行元の情報とを送信すると共に、該通信先の管理装置に当該通信装置の更新用の証明書の取得を依頼する証明書更新依頼手段と、上記証明書更新依頼手段による依頼に応じて上記管理装置から送信されてくるデータのうち、上記管理装置に送信した情報が示す発行元により発行された当該通信装置の証明書及び、その発行元が発行した証明書の正当性を確認するための確認用データを、認証に使用する新たな証明書及び確認用データとして上記第３の記憶手段に記憶させるとともに、該新たな証明書を用いた通信による通信先とする管理装置のアドレス情報を、上記管理装置アドレス記憶手段に記憶させる証明書設定手段と、少なくとも上記証明書更新依頼手段が上記管理装置へ更新用の証明書の取得を依頼する前に、上記第２の記憶手段に識別

情報が登録されている各端末装置から、その端末装置が記憶しているその端末装置の証明書の発行元の情報及び、どのアドレスにアクセスされた場合に通信相手の装置に認証を受けるためにその証明書を使用するかを示すアドレス情報を取得し、その各端末装置のうち、上記取得した発行元に上記発行元記憶手段が記憶する発行元が含まれている各更新可能端末装置について、上記第２の記憶手段に記憶しているその更新可能端末装置のアドレス情報を、その更新可能端末装置から受信したその発行元記憶手段が記憶する発行元と対応するアドレス情報に更新する端末情報更新手段とを設けたものである。

【００１３】

（４）端末装置と、その端末装置を管理するための複数の管理装置と、上記端末装置と上記管理装置との間の通信を仲介する仲介装置とを備えた管理システムであって、上記仲介装置に、当該仲介装置を一意に特定するための識別情報を記憶する第１の記憶手段と、通信相手の装置に認証を受けるための当該仲介装置の証明書と、通信相手の装置から送信されてくる、特定の発行元が発行した証明書の正当性を確認するための確認用データとを記憶する第２の記憶手段と、通信先とする管理装置のアドレス情報を記憶する管理装置アドレス記憶手段と、上記第２の記憶手段が記憶している確認用データが上記端末装置から送信されてくる証明書の発行元と対応しないためにその証明書の正当性が確認できなかった場合に、上記管理装置アドレス記憶手段が記憶するアドレス情報に従い、通信先の管理装置に対して、上記第１の記憶手段が記憶している識別情報と、上記端末装置から送信されてきた証明書の発行元の情報とを送信すると共に、該通信先の管理装置に当該仲介装置の更新用の証明書の取得を依頼する証明書更新依頼手段と、上記証明書更新依頼手段による依頼に応じて上記管理装置から送信されてくるデータのうち、上記管理装置に送信した情報が示す発行元により発行された当該仲介装置の証明書及び、その発行元が発行した証明書の正当性を確認するための確認用データを、認証に使用する新たな証明書及び確認用データとして上記第２の記憶手段に記憶させるとともに、該新たな証明書を用いた通信による通信先とする管理装置のアドレスを、上記管理装置アドレス記憶手段に記憶させる証明書設定手段とを設け、上記管理装置の少なくとも１つに、上記仲介装置から上記更新用の証明書の取得を依頼された場合に、上記仲介装置から受信した識別情報を上記仲介装置から受信した発行元の情報が示す証明書の発行元に送信して、その識別情報を含む新たな証明書の発行を依頼する証明書発行依頼手段と、上記発行元から、上記証明書発行依頼手段による依頼に基づいて発行された新たな証明書を取得する証明書取得手段と、上記発行元が発行した証明書の正当性を確認するための確認用データを取得する確認用データ取得手段と、上記証明書取得手段が取得した新たな証明書と、上記確認用データ取得手段が取得した確認用データと、該新たな証明書を用いた通信による通信先とする管理装置のアドレス情報とを上記仲介装置に送信する証明書送信手段とを設け、上記端末装置に、通信相手の装置に認証を受けるための当該端末装置の証明書と、通信相手の装置から送信されてくる証明書の正当性を確認するための確認用データとを記憶する第３の記憶手段と、上記第３の記憶手段が記憶する当該端末装置の証明書を、認証を受けるために上記仲介装置に送信する証明書提供手段とを設けたものである。

【００１８】

（５）端末装置と、その端末装置を管理するための複数の管理装置と、上記端末装置と上記管理装置との間の通信を仲介する仲介装置とを備えた管理システムであって、上記仲介装置に、当該仲介装置を一意に特定するための識別情報を記憶する第１の記憶手段と、通信相手とする端末装置の識別情報及びその端末装置のアドレス情報を記憶する第２の記憶手段と、通信相手の装置に認証を受けるための当該仲介装置の証明書と、通信相手の装置から送信されてくる、特定の発行元が発行した証明書の正当性を確認するための確認用データとを記憶する第３の記憶手段と、通信先とする管理装置のアドレス情報を記憶する管理装置アドレス記憶手段と、上記第３の記憶手段に記憶している証明書を更新する旨の指示を受け付ける受付手段と、当該仲介装置の証明書として、どの発行元が発行した証明書を取得するかを示す情報を、更新可能に記憶する発行元記憶手段と、上記受付手段が証明書を更新する旨の上記指示を受け付けた場合に、上記管理装置アドレス記憶手段が記憶す

るアドレス情報に従い、通信先の管理装置に対して、上記第１の記憶手段が記憶している識別情報と、上記発行元記憶手段が記憶する発行元の情報とを送信すると共に、該通信先の管理装置に当該仲介装置の更新用の証明書の取得を依頼する証明書更新依頼手段と、上記証明書更新依頼手段による依頼に応じて上記管理装置から送信されてくるデータのうち、上記管理装置に送信した情報が示す発行元により発行された当該仲介装置の証明書及び、その発行元が発行した証明書の正当性を確認するための確認用データを、認証に使用する新たな証明書及び確認用データとして上記第３の記憶手段に記憶させるとともに、該新たな証明書を用いた通信による通信先とする管理装置のアドレスを、上記管理装置アドレス記憶手段に記憶させる証明書設定手段と、少なくとも上記証明書更新依頼手段が上記管理装置へ更新用の証明書の取得を依頼する前に、上記第２の記憶手段に識別情報が登録されている各端末装置から、その端末装置が記憶しているその端末装置の証明書の発行元の情報を取得し、その各端末装置のうちその発行元が上記発行元記憶手段が記憶する発行元と異なる各要更新端末装置について、その要更新端末装置の識別情報及び上記発行元記憶手段が記憶する発行元の情報を、上記管理装置アドレス記憶手段が記憶するアドレス情報に従い、通信先の管理装置に送信すると共に、該通信先の管理装置にその要更新端末装置の更新用の証明書の取得を依頼し、その依頼に応じて該通信先の管理装置から送信されてくる、上記発行元記憶手段が記憶する発行元が発行したその要更新端末装置の証明書と、上記発行元記憶手段が記憶する発行元が発行した証明書の正当性を確認するための確認用データとを、その要更新端末装置に送信する証明書送信手段とを設け、上記管理装置の少なくとも１つに、上記仲介装置から上記更新用の証明書の取得を依頼された場合に、上記仲介装置から受信した識別情報を上記仲介装置から受信した発行元の情報が示す証明書の発行元に送信して、その識別情報を含む新たな証明書の発行を依頼する証明書発行依頼手段と、上記発行元から、上記証明書発行依頼手段による依頼に基づいて発行された新たな証明書を取得する証明書取得手段と、上記発行元が発行した証明書の正当性を確認するための確認用データを取得する確認用データ取得手段と、上記証明書取得手段が取得した新たな証明書と、上記確認用データ取得手段が取得した確認用データと、該新たな証明書を用いた通信による通信先とする管理装置のアドレス情報とを上記仲介装置に送信する証明書送信手段とを設け、上記端末装置に、通信相手の装置に認証を受けるための当該端末装置の証明書と、通信相手の装置から送信されてくる証明書の正当性を確認するための確認用データとを記憶する第４の記憶手段と、当該端末装置を一意に特定するための識別情報を記憶する第５の記憶手段と、上記仲介装置からの要求に応じて、上記第５の記憶手段に記憶している当該端末装置の識別情報をその仲介装置に送信する識別情報送信手段と、上記仲介装置から送信されてきた当該端末装置の証明書及び確認用データを、通信相手へのアクセスに使用する新たな証明書及び確認用データとして上記第４の記憶手段に記憶させる第２の証明書設定手段とを設けたものである。

【００１９】

（６）端末装置と、その端末装置を管理するための複数の管理装置と、上記端末装置と上記管理装置との間の通信を仲介する仲介装置とを備えた管理システムであって、上記仲介装置に、当該仲介装置を一意に特定するための識別情報を記憶する第１の記憶手段と、通信相手とする端末装置の識別情報及びその端末装置のアドレス情報を記憶する第２の記憶手段と、通信相手の装置に認証を受けるための当該仲介装置の証明書と、通信相手の装置から送信されてくる、特定の発行元が発行した証明書の正当性を確認するための確認用データとを記憶する第３の記憶手段と、通信先とする管理装置のアドレス情報を記憶する管理装置アドレス記憶手段と、上記第３の記憶手段に記憶している証明書を更新する旨の指示を受け付ける受付手段と、当該仲介装置の証明書として、どの発行元が発行した証明書を取得するかを示す情報を、更新可能に記憶する発行元記憶手段と、上記受付手段が証明書を更新する旨の上記指示を受け付けた場合に、上記管理装置アドレス記憶手段が記憶するアドレス情報に従い、通信先の管理装置に対して、上記第１の記憶手段が記憶している識別情報と、上記発行元記憶手段が記憶する発行元の情報とを送信すると共に、該通信先の管理装置に当該仲介装置の更新用の証明書の取得を依頼する証明書更新依頼手段と、上

記証明書更新依頼手段による依頼に応じて上記管理装置から送信されてくるデータのうち、上記管理装置に送信した情報が示す発行元により発行された当該仲介装置の証明書及び、その発行元が発行した証明書の正当性を確認するための確認用データを、認証に使用する新たな証明書及び確認用データとして上記第３の記憶手段に記憶させるとともに、該新たな証明書を用いた通信による通信先とする管理装置のアドレスを、上記管理装置アドレス記憶手段に記憶させる証明書設定手段と、少なくとも上記証明書更新依頼手段が上記管理装置へ更新用の証明書の取得を依頼する前に、上記第２の記憶手段に識別情報が登録されている各端末装置から、その端末装置が記憶しているその端末装置の証明書の発行元の情報及び、どのアドレスにアクセスされた場合に通信相手の装置に認証を受けるためにその証明書を使用するかを示すアドレス情報を取得し、その各端末装置のうち、上記取得した発行元に上記発行元記憶手段が記憶する発行元が含まれている各更新可能端末装置について、上記第２の記憶手段に記憶しているその更新可能端末装置のアドレス情報を、その更新可能端末装置から受信したその発行元記憶手段が記憶する発行元と対応するアドレス情報に更新する端末情報更新手段とを設け、上記管理装置の少なくとも１つに、上記仲介装置から、上記更新用の証明書の取得を依頼された場合に、上記仲介装置から受信した識別情報を上記仲介装置から受信した発行元の情報が示す証明書の発行元に送信して、その識別情報を含む新たな証明書の発行を依頼する証明書発行依頼手段と、上記発行元から、上記証明書発行依頼手段による依頼に基づいて発行された新たな証明書を取得する証明書取得手段と、上記発行元が発行した証明書の正当性を確認するための確認用データを取得する確認用データ取得手段と、上記証明書取得手段が取得した新たな証明書と、上記確認用データ取得手段が取得した確認用データと、該新たな証明書を用いた通信による通信先とする管理装置のアドレス情報とを上記仲介装置に送信する証明書送信手段とを設け、上記端末装置に、当該端末装置の異なる複数のアドレスと対応させて、そのアドレスにアクセスされた場合に通信相手の装置に認証を受けるために使用するデータとして、それぞれ異なる発行元が発行した当該端末装置の証明書と、その発行元が発行した証明書の正当性を確認するための確認用データを記憶する第４の記憶手段と、上記仲介装置からの要求に応じて、上記第４の記憶手段に記憶している情報に基づき、当該端末装置が記憶している当該端末装置の証明書の発行元の情報及び、どのアドレスにアクセスされた場合に通信相手の装置に認証を受けるためにその証明書を使用するかを示すアドレス情報をその仲介装置に送信するアドレス情報送信手段とを設けたものである。

【発明の効果】

【００２０】

以上のようなこの発明の通信装置及びそれを備えた管理システムによれば、異なるフォーマットの又は異なる認証処理に対応した証明書を発行する複数のＣＡを運用して、端末装置と管理装置との間の通信のセキュリティについて下位互換を維持しつつセキュリティ強度を容易に上げることができるようにすることができる。

【図面の簡単な説明】

【００２１】

【図１】この発明による仲介装置を含む管理システムの一実施形態である画像形成装置管理システムのネットワーク構成例を示す概念図である。

【図２】図１の画像形成装置２０のハードウェア構成例を示すブロック図である。

【図３】図１の第１管理装置３０，第２管理装置４０の各ハードウェア構成例を示すブロック図である。

【図４】図１の第１ＣＡ５０，第２ＣＡ６０の各ハードウェア構成例を示すブロック図である。

【図５】図１の仲介装置８０のハードウェア構成例を示すブロック図である。

【図６】図２に示した画像形成装置２０の機能構成例を示すブロック図である。

【図７】図６のセキュリティ情報マップ記憶部２５５に記憶保持されているセキュリティ情報マップの詳細例を示す図である。

【図８】図３に示した第１管理装置３０及び第２管理装置４０の機能構成例を示すブロッ

ク図である。
【図９】図８のマップ情報記憶部３５１によって記憶保持するマップ情報の詳細例を示す図である。
【図１０】図４に示した第１ＣＡ５０及び第２ＣＡ６０の機能構成例を示すブロック図である。
【図１１】図５に示した仲介装置８０の機能構成例を示すブロック図である。
【図１２】図１１のマップ情報記憶部８５４に記憶保持されるマップ情報の詳細例を示す図である。
【図１３】図１１のセキュリティ情報マップ記憶部８５６に記憶保持されるセキュリティ情報マップの詳細例を示す図である。
【図１４】図１の画像形成装置２０を含む各画像形成装置が仲介装置８０を含む各仲介装置との間でそれぞれＳＳＬによる認証処理を行う際に使用する個別証明書パッケージの構成例を示す図である。
【図１５】図１の画像形成装置２０と仲介装置８０との間で個別証明書パッケージを用いたＳＳＬによる認証処理を説明するためのシーケンス図である。
【図１６】図１に示した画像形成装置管理システムにおける仲介装置８０のセキュリティ強度情報更新時の仲介装置８０及び第１管理装置３０の動作シーケンス例を示す図である。
【図１７】同じく画像形成装置２０のセキュリティ強度情報更新時の画像形成装置２０，仲介装置８０，及び第１管理装置３０の動作シーケンス例を示す図である。
【図１８】同じく証明書を更新する際の各装置の動作シーケンスの第１実施例を示す図である。
【図１９】同じくその動作シーケンスの第２実施例を示す図である。
【図２０】同じくその動作シーケンスの第３実施例を示す図である。
【図２１】同じくその動作シーケンスの第４実施例を示す図である。
【図２２】同じくその動作シーケンスの第５実施例を示す図である。
【図２３】同じくその動作シーケンスの第６実施例を示す図である。
【図２４】図１の仲介装置８０が画像形成装置２０から取得するセキュリティ情報マップの詳細例を示す図である。
【発明を実施するための形態】
【００２２】
以下、この発明を実施するための形態を図面に基づいて具体的に説明する。
〔管理システムのネットワーク構成〕
まず、この発明による仲介装置を含む管理システムの一実施形態である画像形成装置管理システムの概要について説明する。
【００２３】
図１は、その画像形成装置管理システムのネットワーク構成例を示す概念図である。
この画像形成装置管理システムは、それぞれ１台以上のファイアウォール１０，・・・，仲介装置８０，・・・，及び端末装置２０，・・・と、それぞれ２台以上の管理装置３０，４０，・・・とを備えている。また、管理装置３０，４０，・・・は、ネットワーク７０を介して認証局（Certificate Authority：ＣＡ）５０，６０，・・・へアクセス可能である。
【００２４】
ファイアウォール１０と仲介装置８０との通信可能な接続、及び仲介装置８０と端末装置２０との通信可能な接続は、図示しないＬＡＮ（Local Area Network）等のネットワーク（有線又は無線の別は問わない）を介して行ったり、ＵＳＢ規格に準拠した接続や、ＲＳ－４８５規格等に準拠したシリアル通信又はＳＣＳＩ（Small Computer System Interface）規格等に準拠したパラレル通信等の通信経路を介して行うことができる。ファイアウォール１０，・・・と管理装置３０，４０，・・・と認証局５０，６０，・・・との間の通信可能な接続は、ＬＡＮやインタネット等のネットワーク７０を介して行うことがで

きる。

【００２５】

ファイアウォール１０，仲介装置８０，及び端末装置２０は、その端末装置２０が設置されているオフィス等のユーザサイトに設置されており、そのようなユーザサイトは複数存在しうる。なお、仲介装置の機能を有する端末装置が設置されているユーザサイトでは、その端末装置とファイアウォール１０とが直接通信可能に接続する。

端末装置２０は、スキャナ，複写機，プリンタ，ファクシミリ装置，又はそれらの機能を有する複合機等の画像形成装置（画像処理装置）であり、この画像形成装置管理システムにおいて監視対象（管理対象）とされるものに相当する。

【００２６】

この端末装置（以下「画像形成装置」又は「機器」ともいう）２０は、監視対象の情報（各種カウンタ値や稼働状況等を示す情報であり、以下「機器情報」という）を自己のプログラムで収集し、第１ＣＡ５０又は第２ＣＡ６０等が発行する証明書を用いた相互認証を経た暗号化通信（例えば、セキュアソケットレイヤ（Secure Socket Layer：ＳＳＬ、登録商標）通信）によって当該機器情報を管理装置３０又は４０等に転送する。なお、管理装置３０，４０をそれぞれ、第１管理装置３０，第２管理装置４０ともいう。また、この実施形態では、画像形成装置２０とネットワーク７０上の外部装置（通信相手の装置）との通信は、仲介装置８０を介して行うことが多いが、説明の都合上、仲介装置８０を省略する場合もある。

【００２７】

仲介装置８０は、第１管理装置３０又は第２管理装置４０等と端末装置２０との間の通信を仲介する装置である。

管理装置３０，４０は、画像形成装置２０の監視サイト（例えば、画像形成装置２０のメーカ等、画像形成装置２０の保守サービスの提供者）に属し、この画像形成装置２０を含む管理システムの通常運用時において、画像形成装置２０から機器情報を受信して蓄積するといった画像機器監視サービスを提供する情報処理装置（コンピュータ）である。

また、管理装置３０，４０は、画像形成装置２０の監視の運用が開始される前に画像形成装置２０から管理装置３０又は４０に対して行われる、通信等の安全性を担保するための処理において、画像形成装置２０とＣＡ５０又は６０との間の仲介を行う。なお、ＣＡ５０，６０をそれぞれ、第１ＣＡ５０，第２ＣＡ６０ともいう。

【００２８】

より具体的には、画像形成装置２０からの要求に応じ、画像形成装置２０毎に固有の秘密鍵（クライアント秘密鍵）や公開鍵証明書（クライアント公開鍵証明書，認証局公開鍵証明書）を含むデータ（以下「個別証明書パッケージ」という）の発行をＣＡ５０又は６０に要求し、ＣＡ５０又はＣＡ６０によって発行される個別証明書パッケージを画像形成装置２０に返信する。その個別証明書パッケージは、画像形成装置２０が機器情報を転送する際に管理装置３０又は４０との間の相互認証や暗号化通信に用いられる。

なお、この実施形態において、個別証明書パッケージは、ＰＫＣＳ（Public Key Cryptography Standards）に基づく電子証明書のパッケージである。

上記ＰＫＣＳとは、ＲＳＡＤＳＩ社が定める、公開鍵暗号技術をベースとした各種の規格群である。一部はＲＦＣ（Request for Comments）に採用され、インタネット標準となっている。

【００２９】

ＣＡ５０，６０は、いわゆる認証機関が管理する認証局であり、画像形成装置２０に対して管理システム内の電子的な身分証明書である電子証明書（一般に「証明書」という）の個別証明書パッケージを発行して管理する情報処理装置（コンピュータ）である。

この実施形態において、ＣＡ５０，６０は、個別証明書パッケージの一意性を担保する。

【００３０】

なお、ＣＡ５０とＣＡ６０とではそれぞれ発行元の異なる証明書を発行する。

また、この実施形態では、第１管理装置３０および第２管理装置４０を含む各管理装置もそれぞれ、第１ＣＡ５０および第２ＣＡ６０を含むＣＡのうち、必要な各ＣＡと通信するための認証に用いる各証明書を予め記憶保持している。

【００３１】

〔画像形成装置のハードウェア構成〕

次に、図１の画像形成装置（端末装置）２０のハードウェア構成について説明する。

図２は、その画像形成装置２０のハードウェア構成例を示すブロック図である。

この画像形成装置２０は、例えば図２に示すように、ＣＰＵ２１，ＲＯＭ２２，ＲＡＭ２３，不揮発性メモリ２４，通信インタフェース（Ｉ／Ｆ）２５，表示パネル２６，及びエンジン部２７を備えており、それらがシステムバス２８により接続されている。

【００３２】

そして、ＣＰＵ２１は、画像形成装置２０全体を統括制御する制御手段であり、ＲＯＭ２２又は不揮発性メモリ２４に記録（記憶）された種々のプログラムを実行することにより、この発明の特徴に関わる機能を含む種々の機能を実現する。

ＲＯＭ２２は、不揮発性の記憶手段であり、ＣＰＵ２１が実行するプログラムや固定的なパラメータを含むデータを記憶する。このＲＯＭ２２を書き換え可能な記憶手段として構成し、上記プログラムや固定的なパラメータを含むデータをアップデートできるようにしてもよい。

【００３３】

ＲＡＭ２３は、一時的に使用するデータを記憶したり、ＣＰＵ２１のワークメモリとして使用したりする記憶手段である。

不揮発性メモリ２４は、フラッシュメモリやＨＤＤ（ハードディスクドライブ）等の書き換え可能な不揮発性記憶手段であり、ＣＰＵ２１が実行するプログラムや、画像形成装置２０の電源がオフ（ＯＦＦ）にされた後でも保持しておく必要があるパラメータの値を含むデータを記憶する。この不揮発性メモリ２４に、画像形成装置２０の個別証明書パッケージである証明書もここに記憶させるとよい。

【００３４】

通信Ｉ／Ｆ２５は、画像形成装置２０をネットワーク等の通信経路に接続するためのインタフェース（通信手段）であり、例えば、イーサネット（登録商標）方式の通信を行うためのネットワークインタフェースとすることができる。

そして、上記通信経路及び仲介装置８０等を介して第１管理装置３０又は第２管理装置４０や第１ＣＡ５０又は第２ＣＡ６０等の他の装置と通信を行う場合、この通信Ｉ／Ｆ２５とＣＰＵ２１とが通信手段として機能する。なお、通信Ｉ／Ｆ２５は、上記通信経路の規格や使用する通信プロトコル等に応じて適切なものを用意する。また、複数の規格に対応させて複数の通信Ｉ／Ｆを設けることも当然可能である。

【００３５】

表示パネル２６は、液晶ディスプレイ（ＬＣＤ）や発光ダイオード（ＬＥＤ）を備え、この画像形成装置２０に対するユーザの操作情報を入力するグラフィカル・ユーザ・インタフェース（Graphical User Interface：ＧＵＩ），各種のメッセージ，画像形成装置２０の動作状態等を表示する入力表示手段である。なお、表示パネル２６に代えて、またはこれに加えて、外部のディスプレイを表示手段として用いてもよい。

【００３６】

エンジン部２７は、画像形成装置２０が外部との間で通信以外の物理的な入出力を行うための手段である。このエンジン部２７は、例えば、画像形成装置２０がデジタル複合機（Multifunction Peripheral：ＭＦＰ）であれば、用紙等の媒体に画像を形成する電子写真方式等のプリントエンジン（画像形成手段）と、原稿の画像を画像データとして読み取るスキャナエンジン（画像読取手段）とを含むものであり、ＣＰＵ２１がこれらの動作を適切に制御することにより、画像形成装置２０に適切な入出力動作を実行させることができる。上記ＭＦＰは、例えば１台でプリンタ，スキャナ，コピー機，ＦＡＸを含む複数種類の機能を兼ねる画像形成装置である。なお、画像形成装置２０が通信以外の入出力を行

わないのであれば、エンジン部２７は不要である。
【００３７】
〔管理装置のハードウェア構成〕
次に、図１の第１管理装置３０，第２管理装置４０の各ハードウェア構成について説明する。
図３は、その第１管理装置３０，第２管理装置４０の各ハードウェア構成例を示すブロック図である。
【００３８】
第１管理装置３０は、例えば図３の（ａ）に示すように、それぞれバス３７で相互に接続されているＣＰＵ３１と、メモリ装置３２と、ＨＤＤ３３と、入力装置３４と、表示装置３５と、インタフェース装置である通信Ｉ／Ｆ３６とを有するように構成される。
また、第２管理装置４０は、例えば図３の（ｂ）に示すように、それぞれバス４７で相互に接続されているＣＰＵ４１と、メモリ装置４２と、ＨＤＤ４３と、入力装置４４と、表示装置４５と、インタフェース装置である通信Ｉ／Ｆ４６とを有するように構成される。
【００３９】
第１管理装置３０のＣＰＵ３１は、メモリ装置３２に格納されたプログラムに従って第１管理装置３０におけるこの発明に関わる機能を含む種々の機能を実現する。
メモリ装置３２は、ＲＡＭ等のメモリを備え、プログラムの起動指示があった場合に、ＨＤＤ３３からプログラムを読み出し、ＣＰＵ３１で実行可能にメモリに格納する。
ＨＤＤ３３は、第１管理装置３０に導入されたプログラムを格納すると共に、必要なファイルやデータ等を格納する記憶装置（記憶手段）であり、第１管理装置３０でのこの発明に関わる機能を実現する処理のプログラムは、例えば、このＨＤＤ３３に導入される。このＨＤＤ３３には、画像形成装置２０へ送る証明書と後述するマップ情報も格納する。
【００４０】
入力装置３４は、キーボード及びマウスを含む入力手段で構成され、ユーザによる様々な操作指示を入力させるために用いられる。
表示装置３５は、プログラムによるＧＵＩを含む各種の情報を表示する。
通信Ｉ／Ｆ３６は、ネットワークに接続するためのインタフェース（通信手段）として用いられる。
なお、ＨＤＤ３３の代わりにフラッシュメモリ等の他の不揮発性記憶手段を使用することもできる。
【００４１】
第２管理装置４０についても第１管理装置３０と同様に、第２管理装置４０のＣＰＵ４１は、メモリ装置４２に格納されたプログラムに従って第２管理装置４０におけるこの発明に関わる機能を含む種々の機能を実現する。
メモリ装置４２は、ＲＡＭ等のメモリを備え、プログラムの起動指示があった場合に、ＨＤＤ４３からプログラムを読み出し、ＣＰＵ４１で実行可能にメモリに格納する。
ＨＤＤ４３は、第２管理装置４０に導入されたプログラムを格納すると共に、必要なファイルやデータ等を格納する記憶装置であり、第２管理装置４０でのこの発明に係る機能を実現する処理のプログラムは、例えば、このＨＤＤ４３に導入される。このＨＤＤ４３には、画像形成装置２０へ送る証明書と後述するマップ情報も格納する。
【００４２】
入力装置４４は、キーボード及びマウスを含む入力手段で構成され、ユーザによる様々な操作指示を入力させるために用いられる。
表示装置４５は、プログラムによるＧＵＩを含む各種の情報を表示する。
通信Ｉ／Ｆ４６は、ネットワークに接続するためのインタフェースとして用いられる。
なお、ＨＤＤ４３の代わりにフラッシュメモリ等の他の不揮発性記憶手段を使用することもできる。
【００４３】

〔ＣＡのハードウェア構成〕
次に、図１の第１ＣＡ５０，第２ＣＡ６０の各ハードウェア構成について説明する。
図４は、その第１ＣＡ５０，第２ＣＡ６０の各ハードウェア構成例を示すブロック図である。
第１ＣＡ５０についても、上述した第１管理装置３０と上記第２管理装置４０と同様のハードウェア構成を有する。
【００４４】
第１ＣＡ５０は、例えば図４の（ａ）に示すように、それぞれバス５７で相互に接続されているＣＰＵ５１と、メモリ装置５２と、ＨＤＤ５３と、入力装置５４と、表示装置５５と、インタフェース装置である通信Ｉ／Ｆ５６とを有するように構成される。
また、第２ＣＡ６０は、例えば図４の（ｂ）に示すように、それぞれバス６７で相互に接続されているＣＰＵ６１と、メモリ装置６２と、ＨＤＤ６３と、入力装置６４と、表示装置６５と、インタフェース装置である通信Ｉ／Ｆ６６とを有するように構成される。
【００４５】
第１ＣＡ５０のＣＰＵ５１は、メモリ装置５２に格納されたプログラムに従って第１ＣＡ５０におけるこの発明に関わる機能を含む種々の機能を実現する。
メモリ装置５２は、プログラムの起動指示があった場合に、ＨＤＤ５３からプログラムを読み出し、ＣＰＵ５１で実行可能に格納する。
ＨＤＤ５３は、第１ＣＡ５０に導入されたプログラムを格納すると共に、必要なファイルやデータ等を格納する記憶装置であり、第１ＣＡ５０でのこの発明に関わる機能を実現する処理のプログラムは、例えば、このＨＤＤ５３に導入される。
【００４６】
入力装置５４は、キーボード及びマウスを含む入力手段で構成され、ユーザによる様々な操作指示を入力させるために用いられる。
表示装置５５は、プログラムによるＧＵＩを含む各種の情報を表示する。
通信Ｉ／Ｆ５６は、ネットワークに接続するためのインタフェースとして用いられる。
なお、ＨＤＤ５３の代わりにフラッシュメモリ等の他の不揮発性記憶手段を使用することもできる。
【００４７】
第２ＣＡ６０についても第１ＣＡ５０と同様に、第２ＣＡ６０のＣＰＵ６１は、メモリ装置６２に格納されたプログラムに従って第２ＣＡ６０におけるこの発明に関わる機能を含む種々の機能を実現する。
メモリ装置６２は、プログラムの起動指示があった場合に、ＨＤＤ６３からプログラムを読み出し、ＣＰＵ６１で実行可能に格納する。
ＨＤＤ６３は、第２ＣＡ６０に導入されたプログラムを格納すると共に、必要なファイルやデータ等を格納する記憶装置であり、第２ＣＡ６０でのこの発明に関わる機能を実現する処理のプログラムは、例えば、このＨＤＤ６３に導入される。
【００４８】
入力装置６４は、キーボード及びマウスを含む入力手段で構成され、ユーザによる様々な操作指示を入力させるために用いられる。
表示装置６５は、プログラムによるＧＵＩを含む各種の情報を表示する。
通信Ｉ／Ｆ６６は、ネットワークに接続するためのインタフェースとして用いられる。
なお、ＨＤＤ６３の代わりにフラッシュメモリ等の他の不揮発性記憶手段を使用することもできる。
【００４９】
さらに、この発明に関わるプログラムを、光ディスクを含むコンピュータ読み取り可能な記録媒体に格納し、その記録媒体を介して上記画像形成装置２０，上記第１管理装置３０，上記第２管理装置４０，上記第１ＣＡ５０，上記第２ＣＡ６０に対してインストールするようにすれば、この発明に関わるプログラムを上記機器及び上記各装置に容易に導入することができる。

また、この発明に関わるプログラムを、ネットワーク７上の端末装置から上記機器及び上記各装置にインストールするようにしても良い。

なお、上記第１管理装置３０，上記第２管理装置４０，上記第１ＣＡ５０，上記第２ＣＡ６０については、必ずしも表示装置及び入力装置は有していなくても（接続されていなくても）よい。また、以上の構成に限らず、公知のコンピュータを用いることができる。

【００５０】

〔仲介装置のハードウェア構成〕

次に、図１の仲介装置８０のハードウェア構成について説明する。

図５は、その仲介装置８０のハードウェア構成例を示すブロック図である。

この仲介装置８０は、例えば図５に示すように、それぞれバス８５で相互に接続されているＣＰＵ８１と、メモリ装置８２と、ＨＤＤ８３と、インタフェース装置である通信Ｉ／Ｆ８４とを有するように構成される。

【００５１】

仲介装置８０のＣＰＵ８１は、メモリ装置８２に格納されたプログラムに従って仲介装置８０におけるこの発明に関わる機能を含む種々の機能を実現する。

メモリ装置８２は、プログラムの起動指示があった場合に、ＨＤＤ８３からプログラムを読み出し、ＣＰＵ８１で実行可能に格納する。

ＨＤＤ８３は、第１管理装置３０に導入されたプログラムを格納すると共に、必要なファイルやデータ等を格納する記憶装置であり、仲介装置８０でのこの発明に関わる機能を実現する処理のプログラムは、例えば、このＨＤＤ８３に導入される。

通信Ｉ／Ｆ８４は、ネットワークに接続するためのインタフェースとして用いられる。

【００５２】

〔画像形成装置の機能構成〕

次に、図２に示した画像形成装置２０の機能構成について説明する。

図６は、その画像形成装置２０の機能構成例を示すブロック図である。

この画像形成装置２０は、図２によって説明したＣＰＵ２１，ＲＯＭ２２，ＲＡＭ２３で構成される制御部６０において、ＣＰＵ２１がＲＯＭ２２又は不揮発性メモリ２４に記録されたプログラムの実行によって実現されるこの発明に関わる機能として、証明書更新依頼部２０１，証明書更新部２０２，管理装置ＵＲＬ情報更新部２０３，マップ情報更新依頼部２０４，及びセキュリティ強度情報更新部２０５の機能を保持する。

また、不揮発性メモリ２４に、管理装置ＵＲＬ情報記憶部２５１，機種機番情報記憶部２５２，証明書記憶部２５３，セキュリティ強度情報記憶部２５４，セキュリティ情報マップ記憶部２５５，仲介装置ＵＲＬ情報記憶部２５６，及び仲介装置通信先情報記憶部２５７を有する。

なお、機種機番情報とは、画像形成装置２０の機種を示す識別情報と、個体を示す識別情報である機番とからなり、画像形成装置２０を一意に特定するための識別情報である。

【００５３】

証明書更新依頼部２０１は、第１管理装置３０又は第２管理装置４０に対して新規の証明書への更新を依頼する。例えば、第１ＣＡ５０が発行した証明書に基づいて第１管理装置３０の監視下にある場合、第１管理装置３０へ、機種機番情報記憶部２５２に記憶された画像形成装置２０の機種機番情報と共に証明書更新依頼を送信する。これにより、第１管理装置３０から、例えば、第２ＣＡ６０が発行した新規の証明書と、その新規の証明書に基づいて新たに画像形成装置２０を監視する新規の管理装置である第２管理装置４０と通信するためにアクセスすべきアドレスを示す管理装置ＵＲＬ（Uniform Resource Locator）情報を受け取ることができる。なお、そのＵＲＬにはポート番号を含む場合もある。

【００５４】

証明書更新部２０２は、証明書記憶部２５３に記憶されている証明書を、上記証明書更新依頼によって取得した新規の証明書に書き換えて更新する。これにより、例えば、証明書記憶部２５３に記憶されている、第１ＣＡ５０が発行した証明書を、第２ＣＡ６０が発行した新規の証明書に更新することができる。

管理装置ＵＲＬ情報更新部２０３は、管理装置ＵＲＬ情報記憶部２５１に記憶されている管理装置ＵＲＬ情報を、上記証明書更新依頼によって新規の証明書と共に取得した新たな管理装置ＵＲＬ情報（新規の証明書に対応する管理装置のＵＲＬを含む）に書き換えて更新する。これにより、例えば、管理装置ＵＲＬ情報記憶部２５１に記憶されている、第１管理装置３０の管理装置ＵＲＬ情報を、第２管理装置４０の管理装置ＵＲＬ情報に更新することができる。

【００５５】

マップ情報更新依頼部２０４は、第１管理装置３０又は第２管理装置４０に対してマップ情報の更新を依頼する。例えば、第１ＣＡ５０が発行した証明書に基づいて第１管理装置３０の監視下にある場合、第１管理装置３０へ、機種機番情報記憶部２５２に記憶された画像形成装置２０の機種機番情報とセキュリティ強度情報記憶部２５４に記憶されたセキュリティ強度情報（新たな証明書の発行元である第２ＣＡ６０のＵＲＬを示すＣＡ＿ＵＲＬ情報を含む）と共に、第１管理装置３０のマップ情報の更新依頼を送信する。これにより、第１管理装置３０のマップ情報は、画像形成装置２０の機種機番情報に対応する証明書の発行元である第１ＣＡ５０から、新たに、第２ＣＡ６０のＵＲＬ情報（アクセス先アドレス情報）に書き換えることができる。

セキュリティ強度情報更新部２０５は、例えば、表示パネル２６のユーザインタフェースを介した操作により呼び出され、セキュリティ強度情報記憶部２５４のセキュリティ強度情報を更新する。このセキュリティ強度情報の更新に従い、上記マップ情報更新依頼を管理装置へ送信できる。

【００５６】

なお、上記証明書更新依頼、マップ情報更新依頼、及び前述した機器情報の送信については、ＳＳＬで仲介装置８０及び第１管理装置３０又は第２管理装置４０に対して送信される。この際、画像形成装置２０は、ＳＳＬで用いられるクライアント証明書として自己が保持する証明書を利用する。また、アクセスすべき管理装置の選定として上記管理装置ＵＲＬ情報に基づいてアクセスする。仲介装置８０に管理装置との間の通信を仲介されている場合には、仲介装置ＵＲＬ情報及び仲介装置通信先情報に基づいてアクセスする。

【００５７】

〔画像形成装置のセキュリティ情報マップ〕

次に、図６のセキュリティ情報マップ記憶部２５５に記憶保持されているセキュリティ情報マップの詳細について説明する。

図７は、そのセキュリティ情報マップの詳細例を示す図である。

【００５８】

画像形成装置２０がセキュリティ情報マップ記憶部２５５によって記憶保持するセキュリティ情報マップ２５５０は、例えば図７に示すように、ＣＡ＿ＵＲＬ情報２５５１と通信先ＵＲＬ情報２５５３とが対応付けられ、テーブルとして管理されている。なお、図７に斜線で示す通信先情報２５５２を対応付けた３つの情報とする場合もある。また、それらの対応付けられた２つ又は３つの情報を１レコードとし、図７に破線で示すように複数のレコードとする場合もある。その場合には、仲介装置３０を含む複数の仲介装置又は管理装置等のいずれかと通信する場合に、対応する通信先ＵＲＬ情報に切り替えて使用することになる。

【００５９】

通信先情報２５５２は、例えば発行元が異なる複数の証明書でそれぞれ通信を可能にするサーブレットポート番号に相当するものである。この通信先情報２５５２が複数の場合、ＣＡ発行元ごとに１つ対応付けられている。例えば、第１ＣＡ５０が発行した証明書で通信する場合には、その証明書に対応付けられた通信先へ外部からアクセスしてもらえばよい。

通信先ＵＲＬ情報２５５３は、対応するＣＡが発行した証明書を保持している管理装置と通信する仲介装置のＵＲＬ、あるいはその管理装置のＵＲＬを示す情報である。

【００６０】

セキュリティ情報マップ２５５０は、画像形成装置２０が複数の証明書を保持している場合、利用する証明書を切り替える際にも利用される。

例えば、第１ＣＡ５０が発行した証明書から第２ＣＡ６０が発行した証明書に切り替えるときは、仲介装置８０が第２ＣＡ６０のＵＲＬに対応付けられた通信先へアクセスされればよい。また、通信先ＵＲＬ情報は、仲介装置８０に管理されていた画像形成装置２０が、直接第１管理装置３０又は第２管理装置４０に管理される場合に、仲介装置のＵＲＬ情報から管理装置のＵＲＬ情報に切り替えて用いることになる。

【００６１】

〔管理装置の機能構成〕

次に、図３に示した第１管理装置３０及び第２管理装置４０の機能構成について説明する。

図８は、その第１管理装置３０及び第２管理装置４０の機能構成例を示すブロック図である。

この第１管理装置３０は、例えば図８の（ｂ）に示すように、図３の（ａ）によって説明したＣＰＵ３１，メモリ装置３２で構成される制御部３００において、ＣＰＵ３１がメモリ装置３２に記録されたプログラムの実行によって実現されるこの発明に関わる機能として、証明書発行依頼部３０１およびマップ情報更新部３０２の機能を保持する。

【００６２】

また、ＨＤＤ３３に、マップ情報記憶部３５１，証明書記憶部３５２，及び証明書対応ＵＲＬ情報記憶部３５３を有する。

証明書発行依頼部３０１は、仲介装置８０を含む各仲介装置又は画像形成装置２０を含む各画像形成装置のいずれかから証明書更新依頼を受信すると、その証明書更新依頼と共に受信した機種機番情報と自己のマップ情報に基づいて更新用の証明書を発行する認証局（ここで説明する例では第１ＣＡ５０又は第２ＣＡ６０）へ証明書発行依頼を送信し、その認証局から新規の証明書を受け取ると、それを証明書対応ＵＲＬ情報記憶部３５３に記憶されている新規の証明書を発行した認証局に対応する仲介装置又は管理装置のＵＲＬ情報と共に証明書更新依頼の送信元へ送信する。

【００６３】

マップ情報更新部３０２は、各画像形成装置のいずれかからマップ情報更新依頼をその機種機番情報及びセキュリティ強度情報（証明書を発行させるＣＡのＵＲＬ情報を含む）と共に受信すると、その機種機番情報と、セキュリティ強度情報とに基づいてマップ情報記憶部３５１のマップ情報を書き換えて更新する。また、各仲介装置のいずれかからマップ情報更新依頼をその機種機番情報及びセキュリティ強度情報と共に受信すると、その機種機番情報とセキュリティ強度情報とに基づいてマップ情報記憶部３５１のマップ情報を書き換えて更新する。

【００６４】

証明書記憶部３５２は、第１ＣＡ５０および第２ＣＡ５０を含む必要なＣＡと通信を行うための認証に使用する各証明書を記憶保持する。その各証明書（最初の証明書）は、図３の入力装置３４等を用いた管理者の操作により、ＣＰＵ３１が証明書記憶部３５２に予め記憶しておくことができる。

【００６５】

証明書対応ＵＲＬ情報記憶部３５３は、画像形成装置２０が、各認証局から発行された証明書を用いてＳＳＬ通信を行う際にアクセスすべきアクセス先の仲介装置又は管理装置のアドレスを示すＵＲＬを記憶する。更新により証明書を発行するＣＡが変わると、それまでと同じ通信相手は、更新後の証明書の正当性を確認できなくなるため、認証が行えないので、この情報をもとに、更新後の証明書を用いてアクセスすべき通信先を、証明書の発行先装置に通知する。なお、更新前の証明書では通信相手が仲介装置であるが、更新後の証明書では通信相手が管理装置になるといった場合もある。また、画像形成装置がアクセスすべき通信先は、その通信先が仲介装置である場合は特に、画像形成装置の配置位置によって異なるため、画像形成装置の機種機番情報又は配置位置（アドレスでも、会社や

部署あるいは住所、ビル、部屋番号等の物理的な位置でも可）毎にアクセス先の情報を用意する。

また、証明書対応ＵＲＬ情報記憶部３５３は、仲介装置８０についても、同様に、各認証局から発行された証明書を用いてＳＳＬ通信を行う際にアクセスすべきアクセス先の管理装置のアドレスを示すＵＲＬを記憶する。これらの情報は、管理装置の管理者が適宜設定する。

【００６６】

一方、第２管理装置４０も第１管理装置３０と同様に、例えば図８の（ｂ）に示すように、図３の（ｂ）によって説明したＣＰＵ４１，メモリ装置４２で構成される制御部４００において、ＣＰＵ４１がメモリ装置４２に記録されたプログラムの実行によって実現されるこの発明に関わる機能として、証明書発行依頼部４０１，マップ情報更新部４０２の機能を保持する。

【００６７】

また、ＨＤＤ４３に、マップ情報記憶部４５１，証明書記憶部４５２，及び証明書対応ＵＲＬ情報記憶部４５３を有する。

証明書発行依頼部４０１は、仲介装置８０を含む各仲介装置又は画像形成装置２０を含む各画像形成装置のいずれかから証明書更新依頼を受信すると、その証明書更新依頼と共に受信した機種機番情報と自己のマップ情報に基づいて新規の証明書を発行する認証局（この例では図示しない第３ＣＡ）へ証明書発行依頼を送信し、その認証局から新規の証明書を受け取ると、それを証明書対応ＵＲＬ情報記憶部４５３に記憶されている新規の証明書を発行した認証局に対応する仲介装置又は管理装置のＵＲＬ情報と共に証明書更新依頼の送信元へ送信する。

【００６８】

マップ情報更新部４０２は、各画像形成装置のいずれかからマップ情報更新依頼をその機種機番情報及びセキュリティ強度情報と共に受信すると、その機種機番情報と、セキュリティ強度情報（アクセス先アドレス情報であるＣＡ＿ＵＲＬ情報を含む）、この例では図示しない第３ＣＡのＵＲＬとに基づいてマップ情報記憶部４５１のマップ情報を書き換えて更新する。また、各仲介装置のいずれかからマップ情報更新依頼をその機種機番情報及びセキュリティ強度情報と共に受信すると、その機種機番情報とセキュリティ強度情報とに基づいてマップ情報記憶部４５１のマップ情報を書き換えて更新する。

【００６９】

証明書記憶部４５２は、第１ＣＡ５０および第２ＣＡ５０を含む必要なＣＡと通信を行うための認証に使用する各証明書を記憶保持している。その各証明書は、図３の入力装置４４等を用いた管理者の操作により、ＣＰＵ４１が証明書記憶部４５２に予め記憶しておくことができる。

証明書対応ＵＲＬ情報記憶部４５３は、新規の証明書を発行する認証局から発行された証明書に基づくＳＳＬで画像形成装置及び仲介装置の通信をそれぞれ監視する仲介装置，管理装置のＵＲＬ情報を管理対象の画像形成装置毎に記憶保持している。そのＵＲＬ情報は、図４の入力装置４４等を用いた管理者の操作により、ＣＰＵ４１が証明書対応ＵＲＬ情報記憶部４５３に予め記憶しておくことができる。

【００７０】

なお、上記証明書発行依頼、マップ情報更新依頼、及び前述した管理装置ＵＲＬ情報については、ＳＳＬで送受信される。この際、第１管理装置３０，第２管理装置４０は、ＳＳＬで用いられるサーバ証明書として自己が保持する証明書を利用する。また、第１管理装置３０と第２管理装置４０とは、常に同期して互いに同じマップ情報を持つようにしている。

【００７１】

〔管理装置のマップ情報〕

次に、図８のマップ情報記憶部３５１によって記憶保持するマップ情報の詳細について説明する。なお、マップ情報記憶部４５１によって記憶保持するマップ情報も同様なので

、その詳細説明は省略する。
図９は、図８のマップ情報記憶部３５１によって記憶保持するマップ情報の詳細例を示す図である。
【００７２】
第１管理装置３０がマップ情報記憶部４５１によって記憶保持するマップ情報３５１０は、例えば図９に示すように、画像形成装置２０を含む複数の画像形成装置及び仲介装置８０を含む複数の仲介装置について、その各画像形成装置及び仲介装置の機種機番情報３５１１と、それぞれの画像形成装置及び仲介装置に対する証明書の発行元である第１ＣＡ５０，第２ＣＡ６０を含む複数の認証局のＣＡ＿ＵＲＬ情報３５１２とが対応付けられ、テーブルとして管理されている。
【００７３】
例えば、第１管理装置３０は、画像形成装置２０から証明書更新依頼を受け取ると、それと共に受け取った画像形成装置２０の機種機番情報に基づいてマップ情報を参照し、そのマップ情報より画像形成装置２０の機種機番情報に対応する「ＣＡ＿ＵＲＬ情報」を取得し、その「ＣＡ＿ＵＲＬ情報」（アクセス先アドレス情報）によってアクセス先のＣＡを（例えば第２ＣＡ６０に）選定し、そのＣＡにアクセスして証明書発行依頼をする。
【００７４】
〔ＣＡの機能構成〕
次に、図４に示した第１ＣＡ５０及び第２ＣＡ６０の機能構成について説明する。
図１０は、その第１ＣＡ５０及び第２ＣＡ６０の機能構成例を示すブロック図である。
第１ＣＡ５０は、図１０の（ａ）に示すように、図４の（ａ）によって説明したＣＰＵ５１，メモリ装置５２で構成される制御部５００において、ＣＰＵ５１がメモリ装置５２に記録されたプログラムの実行によって実現されるこの発明に関わる機能として、証明書発行部５０１の機能を保持する。
証明書発行部５０１は、第１管理装置３０から証明書発行依頼を画像形成装置２０の機種機番情報と共に受信すると、その機種機番情報を含む新規の証明書を発行し、第１管理装置３０へ送信する。
【００７５】
一方、第２ＣＡ６０も第１ＣＡ５０と同様に、図１０の（ｂ）に示すように、図４の（ｂ）によって説明したＣＰＵ６１，メモリ装置６２で構成される制御部８３において、ＣＰＵ６１がメモリ装置６２に記録されたプログラムの実行によって実現されるこの発明に関わる機能として、証明書発行部６０１の機能を保持する。
証明書発行部６０１は、第１管理装置３０から証明書発行依頼を画像形成装置２０の機種機番情報と共に受信すると、その機種機番情報を含む新規の証明書を発行し、第２管理装置４０へ送信する。
ここで、セキュリティ強度は発行元のＣＡ毎に決まることから、以降はセキュリティ強度情報をＣＡ＿ＵＲＬ情報として説明する。
【００７６】
〔仲介装置の機能構成〕
次に、図５に示した仲介装置８０の機能構成について説明する。
図１１は、その仲介装置８０の機能構成例を示すブロック図である。
この仲介装置８０は、例えば図１１に示すように、図５によって説明したＣＰＵ８１，メモリ装置８２で構成される制御部８００において、ＣＰＵ８１がメモリ装置８２に記録されたプログラムの実行によって実現されるこの発明に関わる機能として、証明書更新依頼部８０１，証明書更新部８０２，管理装置ＵＲＬ情報更新部８０３，マップ情報更新依頼部８０４，セキュリティ強度情報更新部８０５，通信エラー検知部８０６，証明書送付部８０７，及びセキュリティ情報取得依頼部８０８の機能を保持する。
【００７７】
また、ＨＤＤ８３に、管理装置ＵＲＬ情報記憶部８５１，機種機番情報記憶部８５２，証明書記憶部８５３，マップ情報記憶部８５４，セキュリティ強度情報記憶部８５５，及

びセキュリティ情報マップ記憶部８５６を有する。
証明書更新依頼部８０１は、第１管理装置３０又は第２管理装置４０に対して新規の証明書への更新を依頼する。例えば、第１ＣＡ５０が発行した証明書に基づいて第１管理装置３０の監視下にある場合、第１管理装置３０へ、機種機番情報記憶部８５２に記憶された仲介装置８０を一意に特定するための識別情報である仲介装置８０の機種機番情報と共に証明書更新依頼を送信する。これにより、第１管理装置３０から、例えば、第２ＣＡ６０が発行した新規の証明書と、その新規の証明書に基づいて新たに画像形成装置２０を監視する新規の管理装置である第２管理装置４０の管理装置ＵＲＬ情報を受け取ることができる。

【００７８】
証明書更新部８０２は、証明書記憶部８５３に記憶されている証明書を、上記証明書更新依頼によって取得した新規の証明書に書き換えて更新する。これにより、例えば、証明書記憶部８５３に記憶されている、第１ＣＡ５０が発行した証明書を、第２ＣＡ６０が発行した新規の証明書に更新することができる。
管理装置ＵＲＬ情報更新部８０３は、管理装置ＵＲＬ情報記憶部８５１に記憶されている管理装置ＵＲＬ情報を、上記証明書更新依頼によって新規の証明書と共に取得した新たな管理装置ＵＲＬ情報（新規の証明書に対応する管理装置のＵＲＬを含む）に書き換えて更新する。これにより、例えば、管理装置ＵＲＬ情報記憶部８５１に記憶されている、第１管理装置３０の管理装置ＵＲＬ情報を、第２管理装置４０の管理装置ＵＲＬ情報に更新することができる。

【００７９】
マップ情報更新依頼部８０４は、第１管理装置３０又は第２管理装置４０に対してマップ情報の更新を依頼する。例えば、第１ＣＡ５０が発行した証明書に基づいて第１管理装置３０の監視下にある場合、第１管理装置３０へ、機種機番情報記憶部８５２に記憶された仲介装置８０の機種機番情報とセキュリティ強度情報記憶部８５５に記憶されたセキュリティ強度情報（新たな証明書の発行元である第２ＣＡ６０のＵＲＬを含む）と共に、第１管理装置３０のマップ情報の更新依頼を送信する。これにより、第１管理装置３０のマップ情報は、仲介装置８０の機種機番情報に対応する証明書の発行元である第１ＣＡ５０から、新たに、第２ＣＡ６０のＵＲＬを示すＣＡ＿ＵＲＬ情報に書き換えることができる。

【００８０】
セキュリティ強度情報更新部８０５は、例えば、外部の図示しないパーソナルコンピュータ等の端末装置におけるウェブブラウザに表示させたＧＵＩ等のユーザインタフェースを介したユーザ操作により呼び出され、セキュリティ強度情報記憶部８５５のセキュリティ強度情報を更新する。このセキュリティ強度情報の更新に従い、上記マップ情報更新依頼を管理装置へ送信できる。
通信エラー検知部８０６は、画像形成装置２０との通信が行えず、通信エラーが発生すると、その通信エラーを検知する。

【００８１】
証明書送付部８０７は、第１管理装置３０又は第２管理装置４０から受信する証明書およびその発行元のＣＡを示すＣＡ＿ＵＲＬ情報等を証明書送付として、画像形成装置２０へ送信することができる。
セキュリティ情報取得依頼部８０８は、画像形成装置２０に対して、セキュリティ情報取得依頼を送信することができる。そして、そのレスポンスとして画像形成装置２０から取得するセキュリティ情報を利用して自身のセキュリティ情報マップを更新することができる。

【００８２】
なお、上記証明書更新依頼、マップ情報更新依頼、及び前述した機器情報の送信については、ＳＳＬで第１管理装置３０又は第２管理装置４０に対して送信される。この際、仲介装置８０は、ＳＳＬで用いられるクライアント証明書として自身が保持する証明書を利

用する。また、アクセスすべき管理装置の選定として上記管理装置ＵＲＬ情報に基づいてアクセスする。

【００８３】

〔仲介装置のマップ情報〕

次に、図１１のマップ情報記憶部８５４に記憶保持されるマップ情報の詳細について説明する。

図１２は、そのマップ情報記憶部８５４に記憶保持されるマップ情報の詳細例を示す図である。

【００８４】

仲介装置８０がマップ情報記憶部８５４によって記憶保持するマップ情報８５４０は、例えば図１２に示すように、画像形成装置２０を含む複数の画像形成装置及び仲介装置８０を含む複数の仲介装置について、その各画像形成装置及び仲介装置の機種機番情報８５４１と、それぞれの画像形成装置及び仲介装置に対する証明書の発行元である第１ＣＡ５０，第２ＣＡ６０を含む複数の認証局のＣＡ＿ＵＲＬ情報８５４２とが対応付けられ、テーブルとして管理されている。なお、図１２に斜線で示す通信先情報８５４３を対応付けた３つの情報とする場合もある。

【００８５】

ＣＡ＿ＵＲＬ情報８５４２は、画像形成装置２０のセキュリティ強度を自身のセキュリティ強度と比較するときに利用される。

通信先情報８５４３は、画像形成装置２０にアクセスするときに使用するサーブレットポート番号（画像形成装置２０のアドレス情報）を示す。この通信先情報８５４３は、画像形成装置２０が複数の証明書を記憶保持し、利用する証明書を切り替えるときに更新される。

【００８６】

〔仲介装置のセキュリティ情報マップ〕

次に、図１１のセキュリティ情報マップ記憶部８５６に記憶保持されるセキュリティ情報マップについて説明する。

図１３は、そのセキュリティ情報マップの詳細例を示す図である。

【００８７】

仲介装置８０がセキュリティ情報マップ記憶部８５６によって記憶保持するセキュリティ情報マップ８５６０は、例えば図１３に示すように、ＣＡ＿ＵＲＬ情報８５６１と通信先（管理装置）ＵＲＬ情報８５６３とが対応付けられ、テーブルとして管理されている。なお、図１３に斜線で示す通信先情報８５６２を対応付けた３つの情報とする場合もある。また、それらの対応付けられた２つ又は３つの情報を１レコードとし、図１３に破線で示すように複数のレコードとする場合もある。このセキュリティ情報マップ８５６０は、図７によって説明した画像形成装置２０が記憶保持するセキュリティ情報マップ２５５０と通信先ＵＲＬ情報以外は同じ内容である。また、セキュリティ情報マップ８５６０は、仲介装置８０によって管理される画像形成装置が複数台の場合、その台数分必要となる。

【００８８】

〔ＳＳＬ認証処理〕

次に、この画像形成装置管理システムにおけるＳＳＬ認証処理について説明する。

図１４は、図１の画像形成装置２０を含む各画像形成装置が仲介装置８０を含む各装置との間でそれぞれＳＳＬによる認証処理を行う際に使用する個別証明書パッケージの構成例を示す図である。なお、そのような個別証明書パッケージは、仲介装置８０を含む各仲介装置が第１管理装置３０，第２管理装置４０を含む各管理装置との間でそれぞれＳＳＬによる認証処理を行う際にも使用される。

【００８９】

例えば、画像形成装置２０が保持する証明書である個別証明書パッケージ９０は、クライアント公開鍵証明書９１，認証局公開鍵証明書９２，クライアント秘密鍵証明書９３を含む。

そして、クライアント公開鍵証明書９１とクライアント秘密鍵証明書９３は、仲介装置８０をはじめとする他の装置との間の相互認証及び暗号化通信において、画像形成装置２０側の公開鍵証明書，秘密鍵証明書として用いられる。

【００９０】

認証局公開鍵証明書９２は、通信相手から送信されてくる公開鍵証明書に付された認証局の署名を確認し、公開鍵証明書に記載された内容が改竄されていないことを確認するための、認証局の公開鍵証明書であり、確認用データである。なお、認証局公開鍵証明書９２は、クライアント公開鍵証明書９１を発行した、すなわちクライアント公開鍵証明書９１に署名した認証局の公開鍵証明書であり、認証局公開鍵証明書９２を用いて、クライアント公開鍵証明書９１が改竄されていないことも確認できる。

【００９１】

接続先情報９４は、個別証明書パッケージ９０と対応して用意される、個別証明書パッケージ９０を用いて暗号化通信を行う場合にアクセスすべき通信先の識別情報であり、個別証明書パッケージ９０が画像形成装置２０に記憶保持されるものであれば、仲介装置８０，第１管理装置３０，又は第２管理装置４０のＵＲＬが相当する。

【００９２】

図１５は、図１の画像形成装置２０と仲介装置８０との間で個別証明書パッケージを用いたＳＳＬによる認証処理を説明するためのシーケンス図である。なお、以下の図も含め、「Ｓ」は「ステップ」の略である。

この認証処理では、仲介装置８０においても画像形成装置２０が保持するものと同じ認証局が発行した個別証明書パッケージを保持していることが前提となる。つまり、仲介装置８０には、予め固有の個別証明書パッケージを保持されている。この個別証明書パッケージには、仲介装置毎に固有の公開鍵証明書（サーバ公開鍵証明書）、仲介装置毎に固有の秘密鍵（サーバ秘密鍵）、及び認証局公開鍵証明書が含まれている。

【００９３】

通信の開始時に、通信クライアントである画像形成装置２０の制御部２００は、まずステップ３０１において、ＳＳＬバージョン番号，サポートしている暗号セット，及び乱数を含む各種情報を仲介装置８０へ送信する。

一方、仲介装置８０の制御部８００は、その各種情報を受信すると、ステップ３０２において、ＳＳＬバージョン番号，使用する暗号セット，及び乱数を含む各種情報を画像形成装置２０へ送信し、次のステップ３０３においては、サーバ公開鍵証明書を画像形成装置２０へ送信し、更に次のステップ３０４においては、証明書の提示を画像形成装置２０へ要求した後、画像形成装置２０からの応答を待つ。

【００９４】

画像形成装置２０の制御部２００は、仲介装置８０からサーバ公開鍵証明書を受信すると、ステップ３０５において、その受信したサーバ公開鍵証明書の正当性を自装置の認証局公開鍵証明書を用いて検証する。

そして、サーバ公開鍵証明書の正当性を確認できた場合に、ステップ３０６へ進み、クライアント公開鍵証明書を仲介装置８０へ送信する。

【００９５】

画像形成装置２０の制御部２００は、次にステップ３０７へ進み、仲介装置８０とここまでやり取りしたデータのハッシュ値から計算したプリマスタシークレット（乱数）を作成して、それをサーバ公開鍵で暗号化した後、ステップ３０８へ進み、その暗号化したプリマスタシークレットを仲介装置８０へ送信する。

次に、ステップ３０９へ進み、仲介装置８０とここまでやり取りしたデータを使って計算した乱数のデータにクライアント秘密鍵で署名を行い、ステップ３１０でその署名した乱数データ（署名付きデータ）を仲介装置８０へ送信した後、ステップ３１１で２つのシードとプリマスタシークレットとに基づいてセッション鍵を作成する。

【００９６】

仲介装置８０の制御部８００は、画像形成装置２０への証明書の提示の要求に対して、

画像形成装置２０からクライアント公開鍵証明書，プリマスタシークレット，及び署名付きデータを受信すると、ステップ３１２において、その受信したクライアント公開鍵証明書の正当性を自装置が保持する認証局公開鍵証明書を用いて検証する。また、受信した署名付きデータの正当性を先に受信したクライアント公開鍵証明書を用いて検証する。更に、受信したプリマスタシークレットを自装置が保持するサーバ秘密鍵で復号し、その復号したプリマスタシークレットと２つのシードとによってセッション鍵を作成する。

【００９７】

画像形成装置２０の制御部２００は、セッション鍵を作成した後、ステップ３１３において、「今後この共通鍵でデータを送信する旨」のメッセージとＳＳＬ認証終了メッセージとを仲介装置８０へ送信する。

仲介装置８０の制御部８００は、セッション鍵を作成し、それらのメッセージを受信すると、ステップ３１４において、「今後この共通鍵でデータを送信する旨」のメッセージとＳＳＬ認証終了メッセージとを画像形成装置２０へ送信する。

以降は、画像形成装置２０と仲介装置８０との間でセッション鍵による暗号化通信が開始され、画像形成装置２０は、仲介装置８０に対する機器情報等の送信を行う。

したがって、画像形成装置２０及び仲介装置８０に対して適当な個別証明書パッケージが導入されていない場合は、上述した認証を通過することができず、その後の通信を行うことができない。

【００９８】

すなわち、画像形成装置２０から仲介装置８０への機器情報の転送は、個別証明書パッケージが導入されていることが条件となる。

なお、上述した処理は、仲介装置８０が証明書の持ち主以外の偽造サーバであると秘密鍵を持っていないので、画像形成装置２０から送信されたプリマスタシークレットを復号することはできず、また、画像形成装置２０が証明書の持ち主以外の偽造クライアントであるとクライアントからの署名が確認できない、という理論から相互認証を達成している。また、画像形成装置２０と第１管理装置３０又は第２管理装置４０との間でも、同様の認証処理を行うことができる。

【００９９】

〔仲介装置のセキュリティ情報更新時の動作シーケンス〕

次に、図１に示した画像形成装置管理システムにおける仲介装置８０のセキュリティ強度情報更新時の仲介装置８０及び第１管理装置３０の動作シーケンスについて説明する。

図１６は、その動作シーケンス例を示す図である。

【０１００】

仲介装置８０の制御部８００（図１１）は、外部の端末装置におけるウェブブラウザに表示させたＧＵＩ等のユーザインタフェースを介したユーザ操作や、何らかの外部装置からの要求に応じてＨＤＤ８３に記憶保持されているセキュリティ強度情報を更新する（例えば、ＣＡ＿ＵＲＬ情報を、セキュリティ強度を高めるための新たな証明書の発行元であるＣＡのＵＲＬ情報に更新する）と、例えば図１６に示すように、まずステップＳ１において、同じくＨＤＤ８３に記憶保持されている自装置の機種機番情報及び更新後のセキュリティ強度情報と共に、マップ情報更新依頼を第１管理装置３０へ送信する。

【０１０１】

第１管理装置３０の制御部３００（図８）は、仲介装置８０からのマップ情報更新依頼を受信すると、ステップＳ２において、その依頼と共に受け取った仲介装置８０の機種機番情報及びセキュリティ強度情報に基づいて、ＨＤＤ３３に記憶保持されているマップ情報を書き換えて更新する。つまり、マップ情報における仲介装置８０の機種機番情報に対応するセキュリティ強度情報を、ステップＳ１で通知された内容に書き換えて更新する。

なお、同様の動作により、第２管理装置４０のマップ情報を更新することもできる。

〔画像形成装置のセキュリティ情報更新時の動作シーケンス〕

次に、図１に示した画像形成装置管理システムにおける画像形成装置２０のセキュリティ強度情報更新時の画像形成装置２０，仲介装置８０，及び第１管理装置３０の動作シー

ケンスについて説明する。
図１７は、その動作シーケンス例を示す図である。
【０１０２】
画像形成装置２０の制御部２００（図６）は、表示パネル２６を介したユーザ操作等に応じてセキュリティ強度情報記憶部２５４のセキュリティ強度情報を更新する（例えば、ＣＡ＿ＵＲＬ情報を、セキュリティ強度を高めるための新たな証明書の発行元であるＣＡのＵＲＬ情報に更新する）と、例えば図１７に示すように、まずステップＳ１１において、不揮発性メモリ２４に記憶されている自装置の機種機番情報及び更新後のセキュリティ強度情報と共に、マップ情報更新依頼を仲介装置８０へ送信する。
仲介装置８０の制御部８００（図１１）は、画像形成装置２０からのマップ情報更新依頼を画像形成装置２０の機種機番情報及びセキュリティ強度情報と共に受信すると、ステップＳ１２において、そのマップ情報更新依頼に従い、その画像形成装置２０の機種機番情報及びセキュリティ強度情報と共に、マップ情報更新依頼を第１管理装置３０へ送信する。
【０１０３】
第１管理装置３０の制御部３００（図８）は、仲介装置８０からのマップ情報更新依頼を受信すると、ステップＳ１３において、その依頼と共に受け取った画像形成装置２０の機種機番情報及びセキュリティ強度情報（アクセス先アドレス情報であるＣＡのＵＲＬ情報を含む）に基づいて、ＨＤＤ３３に記憶保持されているマップ情報を書き換えて更新する。
なお、同様の動作により、第２管理装置４０のマップ情報を更新することもできる。
【０１０４】
〔証明書更新の動作シーケンスの第１実施例〕
次に、図１に示した画像形成装置管理システムにおける証明書を更新する際の各装置の動作シーケンスの第１実施例について説明する。
図１８は、その第１実施例を示す図である。
【０１０５】
ここで、説明の都合上、証明書の更新先を画像形成装置２０および仲介装置８０、セキュリティ強度を高める前の証明書の発行元を第１ＣＡ５０、セキュリティ強度を高めるための新たな証明書の発行元を第２ＣＡ６０とする。事前条件としては、第１管理装置３０と仲介装置８０、仲介装置８０と画像形成装置２０が、第１ＣＡ５０発行の証明書によるＳＳＬを実施できるものとする。事後条件としては、第２管理装置４０と仲介装置８０、仲介装置８０と画像形成装置２０が、第２ＣＡ６０発行の証明書によるＳＳＬを実施できるものとする。
【０１０６】
そして、証明書更新のシーケンスにより、画像形成装置２０に記憶されている第１ＣＡ５０が発行する証明書を、第２ＣＡ６０が発行する新たな証明書に更新し、管理装置ＵＲＬ情報も第１管理装置３０から第２管理装置４０のＵＲＬへの更新を行い、その処理後は、画像形成装置２０と第２管理装置４０が、第２ＣＡ６０が発行する新たな証明書によるＳＳＬの通信を実施する。
【０１０７】
この第１実施例では、第１ＣＡ５０が発行する証明書は鍵長の短い証明書であり、第２ＣＡ６０が発行する証明書は鍵長の長い証明書にしており、画像形成装置２０の証明書を第１ＣＡ５０の発行のものから第２ＣＡ６０の発行のものへ更新することによって、画像形成装置２０と第１管理装置３０が、第１ＣＡ５０が発行する証明書によるＳＳＬの通信を実施するよりも、画像形成装置２０と第２管理装置４０が、第２ＣＡ６０が発行する新たな証明書によるＳＳＬの通信を実施する方が、セキュリティ強度を高めることができる。
【０１０８】
なお、図１８に示す動作シーケンスを実行する前に、図１７を用いて説明した動作シー

ケンスにより、第１管理装置３０には、図９に示したマップ情報において、画像形成装置２０の機種機番情報と対応するＣＡ＿ＵＲＬ情報として、第２ＣＡ６０のＵＲＬを示す「testCA2.xxx.co.jp」が登録されているとする。

画像形成装置２０の制御部２００（図６）は、表示パネル２６からのユーザ操作等によって証明書更新が要求された場合に、例えば図１８に示すように、まずステップＳ２１において、証明書更新依頼と共に画像形成装置２０の機種機番情報を仲介装置８０へ送信する。

【０１０９】

仲介装置８０の制御部８００（図１１）は、画像形成装置２０からの証明書更新依頼を画像形成装置２０の機種機番情報と共に受信すると、ステップＳ２２において、その証明書更新依頼に従い、その画像形成装置２０の機種機番情報と共に、証明書更新依頼を第１管理装置３０へ送信する。このとき、図８の管理装置ＵＲＬ情報記憶部８５１内の管理装置ＵＲＬ情報を参照することにより、証明書更新依頼先の第１管理装置３０のＵＲＬを認識できる。

【０１１０】

第１管理装置３０の制御部３００（図８）は、仲介装置８０からの証明書更新依頼を受信すると、ステップＳ２３において、その依頼と共に受け取った機種機番情報に基づいて、ＨＤＤ３３に記憶保持されている図９に示したマップ情報を参照し、画像形成装置２０の機種機番情報と対応する「ＣＡ＿ＵＲＬ情報（この例では第２ＣＡ６０のＵＲＬ）」を確認し、その確認した「ＣＡ＿ＵＲＬ情報」に基づいて、第２ＣＡ６０にアクセスして、その第２ＣＡ６０へ画像形成装置２０の機種機番情報と共に証明書発行依頼を送信する。

【０１１１】

第２ＣＡ６０の制御部６００（図１０）は、第１管理装置３０からの証明書発行依頼を受信すると、ステップＳ２４において、その証明書発行依頼と共に受信した機種機番情報を含む新たな証明書を発行し、その新たな証明書を証明書発行依頼元の第１管理装置３０へ送信する。このとき、証明書には、その証明書に含まれる公開鍵と対応する秘密鍵は当然セットにするし、第２ＣＡ６０が発行した証明書の正当性を確認するための確認用データである認証局公開鍵証明書もセットとして、図１４に示した個別証明書パッケージ９０の形で送信する。

【０１１２】

第１管理装置３０の制御部３００は、第２ＣＡ６０からの新たな証明書を受信すると、ステップＳ２５において、その新たな証明書及び上記確認した「ＣＡ＿ＵＲＬ情報（この例では第２ＣＡ６０のＵＲＬを示す情報）」を仲介装置８０へ送信する。

仲介装置８０の制御部８００は、第１管理装置３０からの新たな証明書及びＣＡ＿ＵＲＬ情報を受信すると、ステップＳ２６において、証明書更新依頼元の画像形成装置２０へ受信した新たな証明書及びＣＡ＿ＵＲＬ情報を送信する。

【０１１３】

画像形成装置２０の制御部２００は、仲介装置８０から新たな証明書及びＣＡ＿ＵＲＬ情報を受信すると、ステップＳ２７において、その受信した新たな証明書（第２ＣＡ６０が発行する証明書）を図６の証明書記憶部２５３に、その受信したＣＡ＿ＵＲＬ情報をセキュリティ情報マップ記憶部２５５内の対応する箇所にそれぞれ上書きして、自装置の証明書の更新を行った後、ステップＳ２８において、新たな証明書を受け取った旨の応答を仲介装置８０へ返す。

その後、図示は省略するが、自動で画像形成装置２０を再起動することにより、新たな証明書のセットが完了する。なお、自装置の証明書等を更新した後、画像形成装置２０の再起動を促すメッセージ情報を図２の表示パネル２６に表示させ、ユーザ操作による電源のオフ／オンによって画像形成装置２０に再起動を行わせてもよい。

【０１１４】

そして、画像形成装置２０の再起動によって証明書のセットが完了した時点では、画像形成装置２０の証明書の発行元は第２ＣＡ６０になったが、仲介装置８０の証明書の発行

元は第１ＣＡ５０のままなので、仲介装置８０と画像形成装置２０の証明書の発行元が異なり、両者の間で証明書（クライアント公開鍵）と認証局公開鍵証明書が対応しなくなるので、仲介装置８０と画像形成装置２０は互いに証明書を用いたＳＳＬによる認証処理を行えなくなる。

【０１１５】

そのため、証明書のセットが完了した後、画像形成装置２０の制御部２００が仲介装置８０との通信を試みても、あるいは仲介装置８０の制御部８００が画像形成装置２０との通信を試みても、図１１の証明書記憶部８５３が記憶している仲介装置８０の証明書中の認証局公開鍵証明書（確認用データ）が画像形成装置２０から送信されてくる証明書の発行元と対応しないためにその証明書の正当性が確認できないため、認証がＮＧとなり、通信エラーが発生する。

画像形成装置２０の制御部２００は、証明書記憶部８５３が記憶した証明書を、認証を受けるために仲介装置８０に送信するため、その処理に係る機能が、この発明に関わる証明書提供手段としての機能に該当する。

【０１１６】

仲介装置８０の制御部８００は、証明書のセットが完了した後、画像形成装置２０との通信を行うまでは不具合がないので、上記の通信エラーが発生すると、ステップＳ２９において、その通信エラーを検知し、それをトリガーとして、以下の処理を開始する。

すなわち、まずステップＳ３０において、図１６のステップＳ１と同様に、ＨＤＤ８３に記憶保持されている自装置の機種機番情報及びセキュリティ強度情報（新たな証明書の発行元である第２ＣＡ６０のＵＲＬ情報を含む）と共に、マップ情報更新依頼を第１管理装置３０へ送信する。

【０１１７】

第１管理装置３０の制御部３００（図８）は、仲介装置８０からのマップ情報更新依頼を受信すると、ステップＳ３１において、その依頼と共に受け取った仲介装置８０の機種機番情報及びセキュリティ強度情報に基づいて、ＨＤＤ３３に記憶保持されているマップ情報を書き換えて更新する。

仲介装置８０の制御部８００は、ステップＳ３０の処理を行った後、ステップＳ３２へ進み、証明書更新依頼を自装置の機種機番情報と共に第１管理装置３０へ送信する。

ステップＳ２９，Ｓ３０，Ｓ３２の処理に係る機能が、この発明に関わる証明書更新依頼手段としての機能に該当する。

【０１１８】

第１管理装置３０の制御部３００は、その証明書更新依頼を受信すると、ステップＳ３３において、その依頼と共に受け取った機種機番情報に基づいて、ＨＤＤ３３に記憶保持されている図９に示したマップ情報を参照し、仲介装置８０の機種機番情報と対応する「ＣＡ＿ＵＲＬ情報（この例では第２ＣＡ６０のＵＲＬ）」を確認し、その確認した「ＣＡ＿ＵＲＬ情報」に基づいて、第２ＣＡ６０にアクセスして、その第２ＣＡ６０へ仲介装置８０の機種機番情報と共に証明書発行依頼を送信する。

このステップＳ３３の処理に係る機能が、この発明に関わる証明書発行依頼手段としての機能に該当する。

【０１１９】

第２ＣＡ６０の制御部６００は、第１管理装置３０からの証明書発行依頼を受信すると、ステップＳ３４において、その証明書発行依頼と共に受信した機種機番情報を含む新たな証明書を発行し、その新たな証明書を証明書発行依頼元の第１管理装置３０へ送信する。このとき、証明書には、その証明書に含まれる公開鍵と対応する秘密鍵は当然セットにするし、第２ＣＡ６０が発行した証明書の正当性を確認するための確認用データである認証局公開鍵証明書もセットとして、図１４に示した個別証明書パッケージ９０の形で送信する。この点は、ステップＳ２４で画像形成装置２０の証明書を発行する場合と同様である。

【０１２０】

第１管理装置３０の制御部３００は、第２ＣＡ６０からの新たな証明書を受信（取得）し、ステップＳ３５において、その新たな証明書及び、証明書対応ＵＲＬ情報記憶部３５３に記憶されている、第２ＣＡ６０が発行した証明書を用いて仲介装置８０がアクセスすべきアドレスを示す第２管理装置４０のＵＲＬを示す管理装置ＵＲＬ情報を仲介装置８０へ送信する。

このステップＳ３５の処理に係る機能が、この発明に関わる証明書取得手段，確認用データ取得手段，および証明書送信手段としての機能に該当する。

仲介装置８０の制御部８００は、第１管理装置３０からの新たな証明書及びＣＡ＿ＵＲＬ情報を受信すると、ステップＳ３６において、その受信した新たな証明書（第２ＣＡ６０が発行する証明書）を図１１の証明書記憶部８５３に、その受信した管理装置ＵＲＬ情報を管理装置ＵＲＬ情報記憶部８５１に、自装置のセキュリティ強度情報に含まれているＣＡ＿ＵＲＬ情報をセキュリティ情報マップ記憶部８５５内の対応する箇所にそれぞれ上書きして、自装置の証明書の更新を行う。

このステップＳ３６の処理に係る機能が、この発明に関わる証明書設定手段としての機能に該当する。

以上により、第２管理装置４０と仲介装置８０が、仲介装置８０と画像形成装置２０が、それぞれ第２ＣＡ６０が発行した証明書によるＳＳＬを実施できるようになる。

【０１２１】

この第１実施例によれば、仲介装置８０が、当該仲介装置８０を一意に特定するための識別情報（機種機番情報）を記憶する記憶部（第１の記憶部）と、通信相手の装置に認証を受けるための当該仲介装置８０の証明書と、通信相手の装置から送信されてくる証明書の正当性を確認するための確認用データとを記憶する記憶部（第２の記憶部）とを備え、第２の記憶部に記憶している確認用データ（認証局公開鍵証明書）が画像形成装置２０から送信されてくる証明書の発行元である第２ＣＡ６０と対応しないためにその証明書の正当性が確認できなかった場合に、第１管理装置３０に対して、第１の記憶部が記憶している識別情報と、画像形成装置２０から送信されてきた証明書の発行元である第２ＣＡ６０の情報とを送信すると共に、第１管理装置３０に当該仲介装置８０の更新用の証明書（新しい証明書）の取得を依頼し、その依頼に応じて第１管理装置３０から送信されてくる、その第１管理装置３０に送信した情報が示す発行元である第２ＣＡ６０により発行された当該仲介装置８０の証明書（サーバ公開鍵証明書，サーバ秘密鍵証明書）及び、その発行元が発行した証明書の正当性を確認するための確認用データを、認証に使用する新たな証明書及び確認用データとして第２の記憶部に記憶させることにより、仲介装置８０と画像形成装置２０とが第２ＣＡ６０が発行した証明書を用いて認証を行うことができるため、第２ＣＡ６０が発行した証明書をそれぞれ保持している第２管理装置４０と画像形成装置２０とが仲介装置８０を介して通信を行うことができる。

【０１２２】

なお、仲介装置８０は、自己が管理する画像形成装置として画像形成装置２０を含む複数台数の画像形成装置が設置されている場合には、第１管理装置３０に対して自身の証明書更新を依頼する前に、各画像形成装置の機種機番情報にそれぞれ対応付けられているセキュリティ情報マップから、更新が必要な画像形成装置を割り出し、更新な必要な画像形成装置に対応する証明書更新依頼を第１管理装置３０に対して行うことにより、更新な必要な画像形成装置の証明書更新を実施した後、自己の証明書更新を実施することもできる。それについては、第２実施例以降の各実施例でも同様とする。

また、仲介装置８０以外の仲介装置も仲介装置８０と同様の処理を、第２管理装置４０以外の管理装置も第２管理装置４０と同様の処理を、画像形成装置２０以外の画像形成装置も画像形成装置２０と同様の処理をそれぞれ行うことができる。それについても、第２実施例以降の各実施例でも同様とする。

【０１２３】

〔証明書更新の動作シーケンスの第２実施例〕

次に、図１に示した画像形成装置管理システムにおける証明書を更新する際の各装置の

動作シーケンスの第２実施例について説明する。この第２実施例は、複数の仲介装置を使用する場合に対応するものである。

図１９は、その第２実施例を示す図である。

【０１２４】

ここで、説明の都合上、画像形成装置２０を直接管理する仲介装置として、仲介装置８０（第２実施例では「第１仲介装置８０ａ」という）の他に、第２仲介装置８０ｂが設置されているものとする。そして、第１仲介装置８０ａは発行元が第１ＣＡ５０の、第２仲介装置８０ｂは発行元が第２ＣＡ６０の証明書をそれぞれ保持しているものとする。また、証明書の更新先を画像形成装置２０、セキュリティ強度を高める前の証明書の発行元を第１ＣＡ５０、セキュリティ強度を高めるための新たな証明書の発行元を第２ＣＡ６０とする。事前条件としては、第１管理装置３０と第１仲介装置８０、仲介装置８０と画像形成装置２０が、第１ＣＡ５０発行の証明書によるＳＳＬを実施できるものとする。事後条件としては、第２管理装置４０と第２仲介装置８０ｂ、第２仲介装置８０ｂと画像形成装置２０が、第２ＣＡ６０発行の証明書によるＳＳＬを実施できるものとする。

【０１２５】

この第２実施例は、発行元が異なる証明書を記憶した仲介装置である第１仲介装置８０ａと第２仲介装置８０ｂを用意した例であり、画像形成装置２０の証明書を更新する（第１ＣＡ５０から第２ＣＡ６０の証明書に更新する）際に、その更新後の証明書と発行元が同一の証明書を持つ第２仲介装置８０ｂが画像形成装置２０を管理するように切り替える。つまり、第１仲介装置８０ａが、画像形成装置２０の証明書を更新させる際に、第２ＣＡ６０のが発行した証明書と共に、第２仲介装置８０ｂのアドレスを示す通信先情報（ＵＲＬ情報）を送信することにより、画像形成装置２０のアクセス先を第２仲介装置８０ｂに切り替える。具体的には、以下に示す通りである。

【０１２６】

なお、この例においても、図１９に示す動作シーケンスを実行する前に、図１７を用いて説明した動作シーケンスにより、第１管理装置３０には、図９に示したマップ情報において、画像形成装置２０の機種機番情報と対応するＣＡ＿ＵＲＬ情報として、第２ＣＡ６０のＵＲＬを示す「testCA2.xxx.co.jp」が登録されているとする。

【０１２７】

画像形成装置２０の制御部２００（図６）は、表示パネル２６からのユーザ操作等によって証明書更新が要求された場合に、例えば図１９に示すように、まずステップＳ４１において、証明書更新依頼と共に画像形成装置２０の機種機番情報を第１仲介装置８０ａへ送信する。

このステップＳ４１の処理に係る機能が、この発明に関わる第１の仲介要求手段としての機能に該当する。

第１仲介装置８０ａの制御部８００（図１１）は、画像形成装置２０からの証明書更新依頼を画像形成装置２０の機種機番情報と共に受信すると、ステップＳ４２において、その証明書更新依頼に従い、その画像形成装置２０の機種機番情報と共に、証明書更新依頼を第１管理装置３０へ送信する。

【０１２８】

第１管理装置３０の制御部３００（図８）は、仲介装置８０からの証明書更新依頼を受信すると、ステップＳ４３において、その依頼と共に受け取った機種機番情報に基づいて、ＨＤＤ３３に記憶保持されている図９に示したマップ情報を参照し、画像形成装置２０の機種機番情報と対応する「ＣＡ＿ＵＲＬ情報（この例では第２ＣＡ６０のＵＲＬ）」を確認し、その確認した「ＣＡ＿ＵＲＬ情報」に基づいて、第２ＣＡ６０にアクセスして、その第２ＣＡ６０へ画像形成装置２０の機種機番情報と共に証明書発行依頼を送信する。

【０１２９】

第２ＣＡ６０の制御部６００（図１０）は、第１管理装置３０からの証明書発行依頼を受信すると、ステップＳ４４において、その証明書発行依頼と共に受信した機種機番情報を含む新たな証明書を発行し、その新たな証明書を証明書発行依頼元の第１管理装置３０

へ送信する。
第１管理装置３０の制御部３００は、第２ＣＡ６０からの新たな証明書を受信すると、ステップＳ４５において、その新たな証明書及び、証明書対応ＵＲＬ情報記憶部３５３に記憶されている、第２ＣＡ６０が発行した証明書を用いてステップＳ４２で送信された機種機番情報の画像形成装置２０がアクセスすべきアドレスを示す仲介装置ＵＲＬ（この例では第２ＣＡ６０が発行した証明書を保持している第２仲介装置８０ｂのＵＲＬを示す情報）を第１仲介装置８０ａへ送信する。
【０１３０】
第１仲介装置８０ａの制御部８００は、第１管理装置３０からの新たな証明書及び仲介装置ＵＲＬ情報を受信すると、ステップＳ４６において、証明書更新依頼元の画像形成装置２０へ受信した新たな証明書及び仲介装置ＵＲＬ情報を画像形成装置２０へ送信する。
画像形成装置２０の制御部２００は、第１仲介装置８０ａから新たな証明書及び仲介装置ＵＲＬ情報を受信すると、ステップＳ４７において、その受信した新たな証明書（第２ＣＡ６０が発行する証明書）を図６の証明書記憶部２５３に、その受信した仲介装置ＵＲＬ情報を仲介装置ＵＲＬ情報記憶部２５６とセキュリティ情報マップ記憶部２５５内の対応する箇所にそれぞれ上書きして、自装置の証明書の更新を行った後、ステップＳ４８において、新たな証明書を受け取った旨の応答を第１仲介装置８０ａへ返す。
【０１３１】
第１仲介装置８０ａの制御部８００は、その応答を受け取ると、新たな証明書及び仲介装置ＵＲＬ情報を画像形成装置２０が受け取ったことを確認でき、ステップＳ４９において、自装置のマップ情報記憶部８５４に記憶されているマップ情報のテーブルから、画像形成装置２０の機種機番情報を含むマップ情報のレコードを削除して、マップ情報のレコードを更新する。画像形成装置２０はもはや第１仲介装置８０ａとは通信できないため、この処理により、画像形成装置２０を第１仲介装置８０ａによる仲介の対象から外すのである。
画像形成装置２０の制御部２００は、ステップＳ４８の処理を行った後、図示は省略するが、第１実施例と同様に画像形成装置２０を再起動する。
そして、証明書のセットが完了した後、ステップＳ５０へ進んで、ステップＳ４７で設定した仲介装置ＵＲＬに従い、第２仲介装置８０ｂにアクセスする。第２仲介装置８０ｂは、第２ＣＡ６０が発行した証明書を記憶しているため画像形成装置２０との間の認証は成功するはずである。そして、認証が成功すると、管理開始要求を自装置の機種機番情報と共に送信する。
【０１３２】
第２仲介装置８０ｂの制御部は、図１１の証明書記憶部８５３に記憶している自装置の証明書中の認証局公開鍵証明書が画像形成装置２０から送信されてくる証明書の発行元と対応するためにその証明書の正当性が確認でき、画像形成装置２０からの管理開始要求を受信すると、ステップＳ５１において、自装置のマップ情報記憶部８５４に記憶されているマップ情報のテーブルに、管理開始要求と共に受信した画像形成装置２０の機種機番情報と自装置が記憶保持している証明書の発行元である第２ＣＡ６０のＣＡ＿ＵＲＬ情報とを対応付けたマップ情報のレコードを追加して、マップ情報のレコードを更新する。このことにより、画像形成装置２０が新たに第２の仲介装置８０ｂによる仲介の対象となったことを示す。
【０１３３】
その後、ステップＳ５２において、自装置の管理装置ＵＲＬ情報記憶部に記憶されている管理装置ＵＲＬ情報が示すＵＲＬの第２管理装置４０へ管理開始要求を送信する。
以上により、第２管理装置４０と第２仲介装置８０ｂが、第２仲介装置８０ｂと画像形成装置２０が、それぞれ第２ＣＡ６０が発行した証明書によるＳＳＬを実施できるようになる。
【０１３４】
この第２実施例によれば、第１仲介装置８０ａが、通信相手とする画像形成装置２０の

識別情報（機種機番情報）を記憶する記憶部を備え、その識別情報が登録されている画像形成装置２０からの要求に応じて、その画像形成装置２０から送信されたその識別情報及び証明書の発行元である第２ＣＡ６０の情報を第１管理装置３０に送信する第１の仲介処理を行い、当該第１仲介装置８０ａに識別情報が登録されている画像形成装置２０からの要求に応じて、その画像形成装置２０から送信されたその識別情報を第１管理装置３０に送信すると共に、第１管理装置３０にその画像形成装置２０の更新用の証明書の取得を依頼する第２の仲介処理を行い、その依頼に応じて第１管理装置３０から送信されてくる、第１の仲介処理によって第１管理装置３０に送信した情報が示す発行元である第２ＣＡ６０により発行された画像形成装置２０の証明書と、その画像形成装置２０がその証明書を用いてアクセスすべきアクセス先である第２仲介装置８０ｂのアドレス情報と、その発行元が発行した証明書の正当性を確認するための確認用データとを、第２の仲介処理によって受けた要求の送信元である画像形成装置２０に送信する第３の仲介処理を行い、その処理によって送信した証明書、アドレス情報及び確認用データを画像形成装置２０が受信したことを確認した場合に、その画像形成装置２０の識別情報を記憶部から消去することにより、第１ＣＡ５０が発行した証明書を保持する第１仲介装置８０ａと第２ＣＡ６０が発行した証明書を保持する画像形成装置２０とが証明書を用いた認証を行えなくなるが、第２ＣＡ６０が発行した証明書をそれぞれ保持する第２仲介装置８０ｂと画像形成装置２０とが証明書を用いた認証を行うことが可能になる。

【０１３５】

また、第２仲介装置８０ｂが、当該第２仲介装置８０ｂに識別情報が登録されていない画像形成装置２０からアクセスを受け、その画像形成装置２０をその画像形成装置２０の証明書により認証した場合に、その画像形成装置２０からその識別情報を受信して記憶保持することにより、第２管理装置４０と画像形成装置２０とが第２仲介装置８０ｂを介して通信を行うことができる。

【０１３６】

〔証明書更新の動作シーケンスの第３実施例〕

次に、図１に示した画像形成装置管理システムにおける証明書を更新する際の各装置の動作シーケンスの第３実施例について説明する。この第３実施例は、仲介装置が複数の証明書を保持する場合に対応するものである。

図２０は、その第３実施例を示す図である。

【０１３７】

ここで、説明の都合上、証明書の更新先を画像形成装置２０および仲介装置８０、セキュリティ強度を高める前の証明書の発行元を第１ＣＡ５０、セキュリティ強度を高めるための新たな証明書の発行元を第２ＣＡ６０とする。また、第１管理装置３０および仲介装置８０がそれぞれ発行元の異なる複数の証明書である第１ＣＡ５０と第２ＣＡ６０の各証明書を記憶保持しているものとする。そのため、仲介装置８０がセキュリティ情報マップ記憶部８５６によって記憶保持するセキュリティ情報マップは、図１３に示した第１ＣＡ５０と第２ＣＡ６０に対応する２レコード分のＣＡ＿ＵＲＬ情報８５６１と通信先ＵＲＬ情報８５６３とが対応付けられたテーブルとなる。但し、第１ＣＡ５０に対応するレコードを使用可能に設定している。

【０１３８】

この第３実施例では、仲介装置８０が発行元の異なる複数の証明書を持っている場合、画像形成装置２０の証明書を更新する際に、その画像形成装置２０の仲介装置８０への通信先情報も更新することで、仲介装置８０と画像形成装置２０との通信を可能にできる。例えば、仲介装置８０が、発行元がそれぞれ第１ＣＡ５０、第２ＣＡ６０である２枚の証明書を保持していて、自装置が管理している画像形成装置２０の証明書を発行元の第１ＣＡ５０から第２ＣＡ６０の証明書に更新させる際に、発行元が第２ＣＡ６０の証明書と共に、当該仲介装置８０の通信先情報（第２ＣＡ６０が発行した証明書で通信を可能にするサーブレットポート番号）を送信することにより、画像形成装置２０は第２ＣＡ６０が発行した証明書を用いて仲介装置８０と通信可能にできる。具体的には、以下に示す通りで

ある。
なお、この例においても、図２０に示す動作シーケンスを実行する前に、図１７を用いて説明した動作シーケンスにより、管理装置３０には、図９に示したマップ情報において、画像形成装置２０の機種機番情報と対応するＣＡ＿ＵＲＬ情報として、第２ＣＡ６０のＵＲＬを示す「testCA2.xxx.co.jp」が登録されているとする。
【０１３９】
画像形成装置２０の制御部２００（図６）は、ステップＳ６１で、表示パネル２６からのユーザ操作等によって証明書更新が要求された場合に、例えば図２０に示すように、まずステップＳ６１において、証明書更新依頼と共に画像形成装置２０の機種機番情報を仲介装置８０へ送信する。
以降、画像形成装置２０の制御部２００，第１管理装置３０の制御部３００、および第２ＣＡ６０の制御部６００が、ステップＳ６２～Ｓ６５において、図１８のステップＳ２２～Ｓ２５と同様の処理を行う。
【０１４０】
仲介装置８０の制御部８００は、第１管理装置３０からの新たな証明書及び第２ＣＡ６０を示すＣＡ＿ＵＲＬ情報を受信すると、ステップＳ６６において、図１３に示したセキュリティ情報マップのテーブルを参照し、受信したＣＡ＿ＵＲＬ情報に対応する第２ＣＡ６０が発行した証明書で通信を可能にする仲介装置通信先情報（サーブレットポート番号）を抽出する。そして、ステップＳ６６で、ステップＳ６５で受信した更新用の証明書と共にその抽出した仲介装置通信先情報を画像形成装置２０へ送信する。
【０１４１】
画像形成装置２０の制御部２００は、仲介装置８０から新たな証明書及び仲介装置通信先情報を受信すると、ステップＳ６７において、その受信した新たな証明書（第２ＣＡ６０が発行する証明書）を図６の証明書記憶部２５３に、その受信した仲介装置通信先情報を管理装置通信先情報記憶部２５７とセキュリティ情報マップ記憶部２５５内の対応する箇所にそれぞれ上書きして、自装置の証明書の更新を行った後、ステップＳ６８において、新たな証明書を受け取った旨の応答を仲介装置８０へ返す。
【０１４２】
第１仲介装置８０の制御部８００は、その応答を受け取ると、新たな証明書及び通信先情報を画像形成装置２０が受け取ったことを確認でき、ステップＳ６９において、自装置のマップ情報記憶部８５４に記憶されているマップ情報のテーブルのうち、画像形成装置２０の機種機番情報を含むレコードのＣＡ＿ＵＲＬ情報および通信先情報をそれぞれ、先に受信したＣＡ＿ＵＲＬ情報，先に抽出した通信先情報に変更して、マップ情報のテーブルを更新する。このことにより、画像形成装置２０とは、以後第２ＣＡ６０が発行した証明書を用いて通信を行うことを示す。
【０１４３】
画像形成装置２０の制御部２００は、ステップＳ６８の処理を行った後、図示は省略するが、第１実施例と同様に画像形成装置２０を再起動することにより、証明書のセットが完了した後、ステップＳ７０へ進み、第２ＣＡ６０が発行した証明書を保持している仲介装置８０の通信先（サーブレットポート）へアクセスする。
仲介装置８０の制御部８００は、そのアクセスされる通信先（サーブレットポート）に対応する第２ＣＡ６０が発行した証明書を画像形成装置２０との認証に使用し、また図示は省略しているが、第２管理装置４０へ管理開始要求を送信することにより、第２管理装置４０との認証にも第２ＣＡ６０が発行した証明書を使用することができる。
【０１４４】
以上により、第１管理装置３０と仲介装置８０との間と、仲介装置８０と画像形成装置２０との間とで、それぞれ第２ＣＡ６０が発行した証明書によるＳＳＬを実施できるようになる。
なお、この第３実施例では、第１管理装置３０が発行元の異なる複数の証明書である第１ＣＡ５０と第２ＣＡ６０の各証明書を記憶保持するようにしたが、第１，第２実施例の

ように、第１管理装置３０が第１ＣＡ５０を、第２管理装置４０が第２ＣＡ６０の証明書を保持するようにしても良い。

【０１４５】

この第３実施例によれば、仲介装置８０が、当該仲介装置８０の異なる複数のアドレス（通信先情報）と対応させて、それぞれそのアドレスにアクセスを受け付けて通信相手とする画像形成装置２０の識別情報（機種機番情報）を記憶する記憶部（第１の記憶部）と、当該仲介装置８０の異なる複数のアドレスと対応させて、そのアドレスにアクセスされた場合に通信相手の装置の認証に使用するデータとして、それぞれ異なる発行元について、その発行元が発行した証明書の正当性を確認するための確認用データを記憶する記憶部（第２の記憶部）とを備え、第１の記憶部に識別情報が登録されている画像形成装置２０からの要求に応じて、その画像形成装置２０から送信されたその画像形成装置２０の識別情報及び証明書の発行元である第２ＣＡ６０の情報を第１管理装置３０に送信する第１の仲介処理を行い、第１の記憶部に識別情報が登録されている画像形成装置２０からの要求に応じて、その画像形成装置２０から送信されたその識別情報を第１管理装置３０に送信すると共に、その第１管理装置３０に画像形成装置２０の更新用の証明書の取得を依頼する第２の仲介処理を行い、その依頼に応じて第１管理装置３０から送信されてくる、第１の仲介処理によって第１管理装置３０に送信した情報が示す発行元である第２ＣＡ６０により発行された画像形成装置２０の証明書と、その発行元が発行した証明書の正当性を確認するための確認用データとを、その発行元と対応する仲介装置８０のアドレスを示すアドレス情報と共に第２の仲介処理によって受けた要求の送信元である画像形成装置２０に送信する第３の仲介処理を行い、第３の仲介処理によって送信した証明書、アドレス情報及び確認用データを画像形成装置２０が受信したことを確認した場合に、第１の記憶部におけるその画像形成装置２０の識別情報の登録を、その送信した証明書の発行元である第２ＣＡ６０と対応するアドレスと対応付けた登録に変更することにより、仲介装置８０と画像形成装置２０とが第２ＣＡ６０が発行した証明書を用いて認証を行うことができるため、第１管理装置３０と画像形成装置２０とが仲介装置８０を介して再び通信を行うことができる。

【０１４６】

〔証明書更新の動作シーケンスの第４実施例〕

次に、図１に示した画像形成装置管理システムにおける証明書を更新する際の各装置の動作シーケンスの第４実施例について説明する。この第４実施例は、画像形成装置が管理装置に管理される場合に対応するものである。

図２１は、その第４実施例を示す図である。

【０１４７】

ここで、説明の都合上、証明書の更新先を画像形成装置２０および仲介装置８０、セキュリティ強度を高める前の証明書の発行元を第１ＣＡ５０、セキュリティ強度を高めるための新たな証明書の発行元を第２ＣＡ６０とする。事前条件としては、第１管理装置３０と仲介装置８０、仲介装置８０と画像形成装置２０が、第１ＣＡ５０発行の証明書によるＳＳＬを実施できるものとする。事後条件としては、第２管理装置４０と画像形成装置２０が、第２ＣＡ６０発行の証明書によるＳＳＬを実施できるものとする。

【０１４８】

仲介装置８０の証明書の更新が何らかの理由で行えない場合には、画像形成装置２０の証明書を更新しても、その証明書を用いた通信を行うことができない。それは、仲介装置８０が画像形成装置２０と同じ発行元の証明書を保持できないためである。

そこで、第４実施例では、証明書更新の際に、画像形成装置２０に管理装置ＵＲＬ情報を送ることにより、画像形成装置２０は管理装置８０が管理することが可能になる。具体的には、以下に示す通りである。

なお、この例においても、図２１に示す動作シーケンスを実行する前に、図１７を用いて説明した動作シーケンスにより、第１管理装置３０には、図９に示したマップ情報において、画像形成装置２０の機種機番情報と対応するＣＡ＿ＵＲＬ情報として、第２ＣＡ６

０のＵＲＬを示す「testCA2.xxx.co.jp」が登録されているとする。

【０１４９】

画像形成装置２０の制御部２００（図６）は、表示パネル２６からのユーザ操作等によって証明書更新が要求された場合に、例えば図２１に示すように、まずステップＳ７１において、証明書更新依頼と共に画像形成装置２０の機種機番情報を仲介装置８０へ送信する。

以降、画像形成装置２０の制御部２００，第１管理装置３０の制御部３００、および第２ＣＡ６０の制御部６００が、ステップＳ７２～Ｓ７４において、図１８のステップＳ２２～Ｓ２４と同様の処理を行う。

【０１５０】

第１管理装置３０の制御部３００は、第２ＣＡ６０からの新たな証明書を受信すると、ステップＳ７５において、その新たな証明書及び、証明書対応ＵＲＬ情報記憶部３５３に記憶されている、第２ＣＡ６０が発行した証明書を用いてステップＳ７２で送信された機種機番情報の画像形成装置２０がアクセスすべきアドレスを示す管理装置ＵＲＬ（この例では第２ＣＡ６０が発行した証明書を保持している第２管理装置４０のＵＲＬを示す情報）を第１仲介装置８０ａへ送信する。

仲介装置８０の制御部８００は、第１管理装置３０からの新たな証明書及び管理装置ＵＲＬ情報を受信すると、ステップＳ７６において、証明書更新依頼元の画像形成装置２０へ受信した新たな証明書及び管理装置ＵＲＬ情報を画像形成装置２０へ送信する。

【０１５１】

画像形成装置２０の制御部２００は、仲介装置８０から新たな証明書及び管理装置ＵＲＬ情報を受信すると、ステップＳ７７において、その受信した新たな証明書（第２ＣＡ６０が発行する証明書）を図６の証明書記憶部２５３に、その受信した管理装置ＵＲＬ情報を管理装置ＵＲＬ情報記憶部２５１とセキュリティ情報マップ記憶部２５５内の対応する箇所にそれぞれ上書きして、自装置の証明書の更新を行った後、ステップＳ７８において、新たな証明書を受け取った旨の応答を仲介装置８０へ返す。

仲介装置８０の制御部８００は、その応答を受け取ると、新たな証明書及び管理装置ＵＲＬ情報を画像形成装置２０が受け取ったことを確認でき、ステップＳ７９において、自装置のマップ情報記憶部８５４に記憶されているマップ情報のテーブルから画像形成装置２０の機種機番情報を含むレコードを削除（消去）して、マップ情報のテーブルを更新する。画像形成装置２０はもはや第１仲介装置８０ａとは通信できないため、この処理により、画像形成装置２０を第１仲介装置８０ａによる仲介の対象から外すのである。

【０１５２】

画像形成装置２０の制御部２００は、ステップＳ７８の処理を行った後、図示は省略するが、第１実施例と同様に画像形成装置２０を再起動することにより、証明書のセットが完了した後、ステップＳ８０へ進んで、ステップＳ７７で設定した管理装置ＵＲＬに従い、第２管理装置４０にアクセスする。第２管理装置４０は、第２ＣＡ６０が発行した証明書を記憶しているため画像形成装置２０との間の認証は成功するはずである。そして、認証が成功すると、管理開始要求を自装置の機種機番情報と共に送信する。

【０１５３】

第２管理装置４０の制御部４００は、図８の証明書記憶部３５２に記憶している自装置の証明書中の認証局公開鍵証明書が画像形成装置２０から送信されてくる証明書の発行元と対応するためにその証明書の正当性が確認でき、画像形成装置２０からの管理開始要求を受信すると、自装置のマップ情報記憶部４５１に記憶保持されているマップ情報のテーブルに、管理開始要求と共に受信した画像形成装置２０の機種機番情報と自装置に保持している証明書の発行元である第２ＣＡ６０のＣＡ＿ＵＲＬ情報とを対応付けたマップ情報のレコードを追加して、マップ情報のレコードを更新する。このことにより、画像形成装置２０が新たに第２管理装置４０による管理の対象となったことを示す。

以上により、第２管理装置４０と画像形成装置２０が、第２ＣＡ６０が発行した証明書によるＳＳＬを実施できるようになる。

【０１５４】
この第４実施例によれば、仲介装置８０が、通信相手とする画像形成装置２０の識別情報（機種機番情報）を記憶する記憶部を備え、その記憶部に識別情報が登録されている画像形成装置２０からの要求に応じて、その画像形成装置２０から送信されたその識別情報及び証明書の発行元である第２ＣＡ６０の情報を第１管理装置３０に送信する第１の仲介処理を行い、記憶部に識別情報が登録されている画像形成装置２０からの要求に応じて、その画像形成装置２０から送信されたその識別情報を第１管理装置３０に送信すると共に、第１管理装置３０にその画像形成装置２０の更新用の証明書の取得を依頼する第２の仲介処理を行い、その依頼に応じて第１管理装置３０から送信されてくる、第１の仲介処理によって第１管理装置３０に送信した情報が示す発行元である第２ＣＡ６０により発行された画像形成装置２０の証明書と、その画像形成装置２０がその証明書を用いてアクセスすべきアクセス先である第２管理装置４０のアドレス情報と、その発行元が発行した証明書の正当性を確認するための確認用データとを、第２の仲介処理によって受けた要求の送信元である画像形成装置２０に送信する第３の仲介処理を行い、その処理によって送信した証明書、アドレス情報及び確認用データを画像形成装置２０が受信したことを確認した場合に、その画像形成装置２０の識別情報を記憶部から消去することにより、第１ＣＡ５０が発行した証明書を保持する仲介装置８０と第２ＣＡ６０が発行した証明書を保持する画像形成装置２０とが証明書を用いた認証を行えなくなるが、第２ＣＡ６０が発行した証明書をそれぞれ保持する第２管理装置４０と画像形成装置２０とが証明書を用いた認証を行うことが可能になる。
【０１５５】
〔証明書更新の動作シーケンスの第５実施例〕
次に、図１に示した画像形成装置管理システムにおける証明書を更新する際の各装置の動作シーケンスの第５実施例について説明する。この第５実施例は、仲介装置の証明書を先に更新しようとした（仲介装置がトリガーとなる）場合に対応するものである。
図２２は、その第５実施例を示す図である。
【０１５６】
ここで、説明の都合上、証明書の更新先を画像形成装置２０および仲介装置８０、セキュリティ強度を高める前の証明書の発行元を第１ＣＡ５０、セキュリティ強度を高めるための新たな証明書の発行元を第２ＣＡ６０とする。また、仲介装置８０がマップ情報記憶部８５４に記憶保持しているマップ情報は、図１２に示した画像形成装置２０の機種機番情報８５４１と、画像形成装置２０に対する証明書の発行元である第１ＣＡ５０，第２ＣＡ６０のＣＡ＿ＵＲＬ情報８５４２と、通信先情報（画像形成装置２０のアドレス情報）８５４３とが対応付けられたテーブルとなる。事前条件としては、第１管理装置３０と仲介装置８０、仲介装置８０と画像形成装置２０が、第１ＣＡ５０発行の証明書によるＳＳＬを実施できるものとする。事後条件としては、第２管理装置４０と仲介装置８０、仲介装置８０と画像形成装置２０が、第２ＣＡ６０発行の証明書によるＳＳＬを実施できるものとする。
【０１５７】
仲介装置８０の制御部８００は、ユーザ操作による外部の図示しないパーソナルコンピュータ等の端末装置におけるウェブブラウザに表示させたＧＵＩ等のユーザインタフェースあるいは管理者の操作等による第１管理装置３０からの証明書更新依頼を受けた場合（証明書期限切れ間際を検知した場合でもよい）に、自身の証明書を更新するが、実際には、例えば図２２に示すように、まずステップＳ９１において、証明書更新依頼を受けると、自身の証明書を更新する前に、ステップＳ９２へ進み、ＨＤＤ８３に記憶保持されている自装置の機種機番情報及びセキュリティ強度情報（この例では第２ＣＡ６０のＵＲＬを示すＣＡ＿ＵＲＬ情報）と共に、マップ情報更新依頼を第１管理装置３０へ送信する。
【０１５８】
第１管理装置３０の制御部３００は、仲介装置８０からのマップ情報更新依頼を受信すると、ステップＳ９３において、その依頼と共に受け取った仲介装置８０の機種機番情報

及びセキュリティ強度情報に基づいて、ＨＤＤ３３に記憶保持されているマップ情報を書き換えて更新する。

仲介装置８０の制御部８００は、ステップＳ９２の処理を行った後、ステップＳ９４において、自装置が管理している画像形成装置２０に対してセキュリティ情報取得を要求する。

【０１５９】

画像形成装置２０の制御部２００は、その要求を受信すると、ステップＳ９５において、図６のセキュリティ情報マップ記憶部２５５に記憶保持されている自装置のセキュリティ情報マップ（セキュリティ強度情報としてのＣＡ＿ＵＲＬ情報を含む）を要求元の仲介装置８０へ送信する。

仲介装置８０の制御部８００は、画像形成装置２０からそのセキュリティ情報マップを受信すると、ステップＳ９６において、そのセキュリティ情報マップ中のセキュリティ強度情報（ＣＡ＿ＵＲＬ情報）を抽出し、自装置のセキュリティ強度情報と抽出した画像形成装置２０のセキュリティ強度情報とを比較し、両セキュリティ強度情報が一致する場合には、自装置が更新する予定のセキュリティ強度に画像形成装置２０が対応しているため、ステップＳ９７以降の処理を行わない。

【０１６０】

もし、上記両セキュリティ強度情報が一致しない場合には、自装置が更新する予定のセキュリティ強度に画像形成装置２０が対応していないため、ステップＳ９７へ進み、画像形成装置２０の機種機番情報及び自装置のセキュリティ強度情報と共に、マップ情報更新依頼を第１管理装置３０へ送信する。

【０１６１】

第１管理装置３０の制御部３００は、仲介装置８０からのマップ情報更新依頼を受信すると、ステップＳ９８において、その依頼と共に受け取った画像形成装置２０の機種機番情報及びセキュリティ強度情報に基づいて、ＨＤＤ３３に記憶保持されているマップ情報を書き換えて更新する。

仲介装置８０の制御部８００は、ステップＳ９７の処理を行った後、ステップＳ９９へ進む。

そして、仲介装置８０，第１管理装置３０，第２ＣＡ６０，および画像形成装置２０の各制御部がステップＳ９９～Ｓ１０６で図１８のステップＳ２２～Ｓ２９と同様の処理を行って画像形成装置２０の証明書を更新させた後、仲介装置８０，第１管理装置３０，および第２ＣＡ６０の各制御部がステップＳ１０７～Ｓ１１１で図１８のステップＳ３２～Ｓ３６と同様の処理を行って仲介装置８０の証明書を更新させる。

【０１６２】

なお、この第５実施例では、仲介装置８０が管理している画像形成装置を画像形成装置２０のみとしているが、画像形成装置２０を含む複数の画像形成装置を管理する場合には、仲介装置８０の制御部８００がステップＳ９４でその管理対象全ての各画像形成装置に対してセキュリティ情報取得を要求し、その各画像形成装置の制御部がそれぞれステップＳ９５で対応する処理を行う。また、仲介装置８０の制御部８００がステップＳ１０３で管理対象全ての各画像形成装置に対して第１管理装置３０からの新たな証明書等を画像形成装置２０へ送信し、その各画像形成装置の制御部がそれぞれステップＳ１０４で対応する処理を行う。

【０１６３】

この第５実施例によれば、仲介装置８０が、当該仲介装置８０を一意に特定するための識別情報を記憶する記憶部（第１の記憶部）と、通信相手とする画像形成装置２０等の画像形成装置の識別情報（機種機番情報）及びその画像形成装置のアドレス情報（通信先情報）を記憶する記憶部（第２の記憶部）と、通信相手の装置に認証を受けるための当該仲介装置８０の証明書と、通信相手の装置から送信されてくる証明書の正当性を確認するための確認用データとを記憶する記憶部（第３の記憶部）とを備え、証明書更新依頼（第３の記憶部に記憶している証明書をそれまでと異なる新たな発行元である第２ＣＡ６０が発

行した証明書に更新する旨の指示）を受け付けた場合に、第１管理装置３０に対して、第１の記憶部が記憶している識別情報と、上記新たな発行元の情報とを送信すると共に、第１管理装置３０に当該仲介装置８０の更新用の証明書の取得を依頼し、その依頼に応じて第１管理装置３０から送信されてくる、その第１管理装置３０に送信した情報が示す発行元である第２ＣＡ６０により発行された当該仲介装置８０の証明書及び、その発行元が発行した証明書の正当性を確認するための確認用データを、認証に使用する新たな証明書及び確認用データとして第３の記憶部に記憶させるが、少なくとも第１管理装置３０へ更新用の証明書の取得を依頼する前に、第２の記憶部に識別情報が登録されている各画像形成装置から、その画像形成装置が記憶しているその画像形成装置の証明書の発行元の情報を取得し、その各画像形成装置のうちその発行元が上記新たな発行元と異なる各要更新画像形成装置について、その要更新画像形成装置の識別情報及び上記新たな発行元の情報を第１管理装置３０に送信すると共に、第１管理装置３０にその要更新画像形成装置の更新用の証明書の取得を依頼し、その依頼に応じて第１管理装置３０から送信されてくる、上記新たな発行元が発行したその要更新画像形成装置の証明書と、上記新たな発行元が発行した証明書の正当性を確認するための確認用データとを、その要更新画像形成装置に送信することにより、仲介装置８０の証明書を先に更新しようとした場合でも、仲介装置８０と各画像形成装置とが新たな証明書を用いた認証を行えなくなる事態を回避することができる。

【０１６４】

〔証明書更新の動作シーケンスの第６実施例〕

次に、図１に示した画像形成装置管理システムにおける証明書を更新する際の各装置の動作シーケンスの第６実施例について説明する。この第６実施例は、画像形成装置が複数の証明書を保持している場合に対応するものである。

図２３は、その第６実施例を示す図である。

【０１６５】

ここで、説明の都合上、証明書の更新先を仲介装置８０、セキュリティ強度を高める前の証明書の発行元を第１ＣＡ５０、セキュリティ強度を高めるための新たな証明書の発行元を第２ＣＡ６０とする。また、仲介装置８０がマップ情報記憶部８５４に記憶保持しているマップ情報は、図１２に示した画像形成装置２０の機種機番情報８５４１と、画像形成装置２０に対する証明書の発行元である第１ＣＡ５０，第２ＣＡ６０のＣＡ＿ＵＲＬ情報８５４２と、通信先情報（画像形成装置２０のアドレス情報）８５４３とが対応付けられたテーブルとなる。更に、仲介装置８０がセキュリティ情報マップ記憶部８５６に記憶保持しているセキュリティ情報マップは、第１ＣＡ５０，第２ＣＡ６０の各ＣＡ＿ＵＲＬ情報をそれぞれ含む複数の２つのレコードからなるものとする。事前条件としては、第１管理装置３０と仲介装置８０、仲介装置８０と画像形成装置２０が、第１ＣＡ５０発行の証明書によるＳＳＬを実施できるものとする。事後条件としては、第２管理装置４０と画像形成装置２０が、第２ＣＡ６０発行の証明書によるＳＳＬを実施できるものとする。

【０１６６】

仲介装置８０の制御部８００は、第５実施例と同様のタイミングで、例えば図２３に示す動作シーケンスを開始し、まずステップＳ１１１で証明書更新依頼を受けると、自身の証明書を更新する前に、ステップＳ１１２へ進み、自装置が管理している画像形成装置２０に対してセキュリティ情報取得を要求する。

画像形成装置２０の制御部２００は、その要求を受信すると、ステップＳ１１２において、図６のセキュリティ情報マップ記憶部２５５に記憶保持されている自装置のセキュリティ情報マップ（セキュリティ強度情報としてのＣＡ＿ＵＲＬ情報を含む）を要求元の仲介装置８０へ送信する。

【０１６７】

仲介装置８０の制御部８００は、ステップＳ１１３で画像形成装置２０から送信されるセキュリティ情報マップを取得（受信）するが、そのセキュリティ情報マップにはセキュリティ強度情報としてのＣＡ＿ＵＲＬ情報が含まれている。ここで、画像形成装置２０に

２つの証明書が記憶保持されているため、取得したセキュリティ情報マップは図２４に示すようなものとなる。

【０１６８】

そのため、ステップＳ１１４においては、その取得したセキュリティ情報マップ中のセキュリティ強度情報（第１ＣＡ５０と第２ＣＡ５０の各ＣＡ＿ＵＲＬ情報）を抽出して、自装置のセキュリティ強度情報（第２ＣＡ５０のＣＡ＿ＵＲＬ情報）と比較し、抽出したセキュリティ強度情報の中に、自装置のセキュリティ強度情報（第２ＣＡ５０のＣＡ＿ＵＲＬ情報）と一致するものがあれば、つまり自装置が更新する予定のセキュリティ強度に画像形成装置２０が対応していれば、画像形成装置２０の証明書更新は不要と判断する。

【０１６９】

この場合、画像形成装置２０にアクセスするときの通信先情報を更新して通信を行うことで、新たに更新する証明書での通信が可能になる。

そこで、ステップＳ１１５では、マップ情報記憶部８５４に記憶保持している自装置のマップ情報のテーブルのうち、画像形成装置２０の機種機番情報を含むレコードにおけるＣＡ＿ＵＲＬ情報および通信先情報（画像形成装置２０にアクセスするときに使用する情報）をそれぞれ次のように更新する。つまり、ＣＡ＿ＵＲＬ情報を第１ＣＡ５０から第２ＣＡ６０のＣＡ＿ＵＲＬ情報に、通信先情報を「ポート７４４３」から「ポート８４４３」にそれぞれ更新する。すなわち、通信先情報を、画像形成装置２０から通知された、第２ＣＡ６０が発行した証明書を認証に使用するアドレス（ポート）の情報に更新する。

【０１７０】

その後、仲介装置８０，第１管理装置３０，および第２ＣＡ６０の各制御部がステップＳ１１６～Ｓ１２２で図１８のステップＳ３０～Ｓ３６と同様の処理を行って仲介装置８０の証明書を更新させる。

その後、仲介装置８０の制御部８００は、自装置の証明書更新を完了した後、画像形成装置２０と通信する際には、自装置のマップ情報に含まれている通信先情報を参照して、画像形成装置２０にアクセスする（Ｓ１２５）。このアドレスにアクセスすれば、画像形成装置２０との間で、第２ＣＡ６０が発行した証明書を用いて認証を行うことができる。

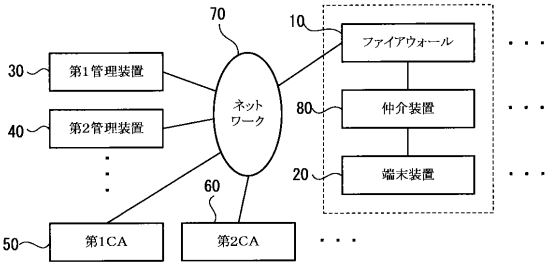
【０１７１】

この第６実施例によれば、仲介装置８０が、当該仲介装置８０を一意に特定するための識別情報を記憶する記憶部（第１の記憶部）と、通信相手とする画像形成装置２０等の画像形成装置の識別情報（機種機番情報）及びその画像形成装置のアドレス情報（通信先情報）を記憶する記憶部（第２の記憶部）と、通信相手の装置に認証を受けるための当該仲介装置８０の証明書と、通信相手の装置から送信されてくる証明書の正当性を確認するための確認用データとを記憶する記憶部（第３の記憶部）とを備え、証明書更新依頼（第３の記憶部に記憶している証明書をそれまでと異なる新たな発行元である第２ＣＡ６０が発行した証明書に更新する旨の指示）を受け付けた場合に、第１管理装置３０に対して、第１の記憶部が記憶している識別情報と、上記新たな発行元の情報とを送信すると共に、第１管理装置３０に当該仲介装置８０の更新用の証明書の取得を依頼し、その依頼に応じて第１管理装置３０から送信されてくる、その第１管理装置３０に送信した情報が示す発行元である第２ＣＡ６０により発行された当該仲介装置８０の証明書及び、その発行元が発行した証明書の正当性を確認するための確認用データを、認証に使用する新たな証明書及び確認用データとして第３の記憶部に記憶させるが、少なくとも第１管理装置３０へ更新用の証明書の取得を依頼する前に、第２の記憶部に識別情報が登録されている各画像形成装置から、その画像形成装置が記憶しているその画像形成装置の証明書の発行元の情報及び、どのアドレスにアクセスされた場合に通信相手の装置に認証を受けるためにその証明書を使用するかを示すアドレス情報を取得し、その各画像形成装置のうち、上記取得した発行元に上記新たな発行元が含まれている各更新可能画像形成装置について、第２の記憶部に記憶しているその更新可能画像形成装置のアドレス情報を、その更新可能画像形成装置から受信したその新たな発行元と対応するアドレス情報に更新することにより、画像形成装置が複数の証明書を保持している場合でも、仲介装置８０と画像形成装置とが新たな

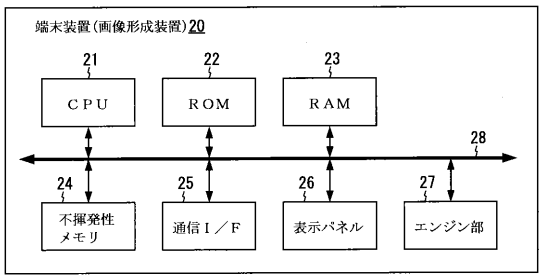
証明書を用いた認証を行えなくなる事態を回避することができる。
したがって、第１～第６実施例のいずれにおいても、異なる証明書を発行する複数のＣＡを運用する際に、画像形成装置と管理装置との間の通信のセキュリティについて下位互換を維持しつつセキュリティ強度を容易に上げることができる。
【０１７２】
なお、第１～第６実施例においては、仲介処理８０が、画像形成装置から管理装置に宛てた依頼（コマンド）を解釈した上で、その依頼と同じ内容の依頼を管理装置へ送信するようにしているが、管理装置に宛てた依頼を一旦受け取ってプールしてから管理装置へ送信することもできる。
また、第１，第５，第６実施例においては、マップ情報更新依頼と証明書更新依頼を別々に行っているが、その各依頼を別々に行う必要はない。すなわち、証明書更新依頼にどのＣＡが発行した証明書に更新したいかを示す情報を含めて送るようにし、この情報に基づいて、更新用証明書の発行を依頼するＣＡを選択すると共にマップ情報を更新するようにしても構わない。
【０１７３】
以上で実施形態の説明を終了するが、システムを構成する装置の組み合わせ、個々の装置の構成、データの構成、具体的な処理内容等が上述の実施形態で説明したものに限られないことはもちろんである。
以上の実施形態では、この発明を通信機能を有する仲介装置（通信装置）および画像形成装置を含む画像形成装置管理システムに適用した例について説明したが、この発明はこれに限られるものではなく、ネットワーク家電，自動販売機，医療機器，電源装置，空調システム，ガス・水道・電気等の計量システム，ＡＶ機器，遊戯機器等の組み込み機器や、ネットワークに接続可能なコンピュータなど、各種端末装置を含む管理システムにも適用可能である。
【産業上の利用可能性】
【０１７４】
以上の説明から明らかなように、この発明によれば、通信装置及び管理システムが、異なるフォーマットの又は異なる認証処理に対応した証明書を発行する複数のＣＡを運用して、端末装置と管理装置との間の通信のセキュリティについて下位互換を維持しつつセキュリティ強度を容易に上げることができるようにすることができる。したがって、異なるフォーマットの又は異なる認証処理に対応した証明書を発行する複数のＣＡを運用する際に、画像形成装置と管理装置との間の通信のセキュリティについて下位互換を維持しつつセキュリティ強度を容易に上げることができる通信装置及び管理システムを提供することができる。
【符号の説明】
【０１７５】
１０：ファイアウォール　２０：端末装置　３０：第１管理装置
４０：第２管理装置　５０：第１ＣＡ　６０：第２ＣＡ　７０：ネットワーク
８０：仲介装置　２１，３１，４１，５１，６１，８１：ＣＰＵ
２２：ＲＯＭ　２３：ＲＡＭ　２４：不揮発性メモリ
２５，３６，４６，５６，６６，８４：通信Ｉ／Ｆ　２６：表示パネル
２７：エンジン部　２８，３７，４７，５７，６７，８５：バス
３２，４２，５２，６２，８２：メモリ装置　３３，４３，５３，６３，８３：ＨＤＤ
３４，４４，５４，６４：入力装置　３５，４５，５５，６５：表示装置
２００，３００，４００，５００，６００，８００：制御部
２０１，８０１：証明書更新依頼部　２０２，８０２：証明書更新部
２０３，８０３：管理装置ＵＲＬ情報更新部　２０４，８０４：マップ情報更新依頼部
２０５，８０５：セキュリティ強度情報更新部
２５１，８５１：管理装置ＵＲＬ情報記憶部　２５２，８５２：機種機番情報記憶部
２５３，３５２，８５３：証明書記憶部

２５４，８５５：セキュリティ強度情報記憶部
２５５，８５６：セキュリティ情報マップ記憶部　２５６：仲介装置ＵＲＬ情報記憶部
２５７：仲介装置通信先情報記憶部　３０１，４０１：証明書発行依頼部
３０２，４０２：マップ情報更新部　３５１，４５１，８５４：マップ情報記憶部
３５２，４５２，８５３：証明書記憶部
３５３，４５３：証明書対応ＵＲＬ情報記憶部　５０１，６０１：：証明書発行部
【先行技術文献】
【特許文献】
【０１７６】
【特許文献１】特開２００４－３２０７１５号公報

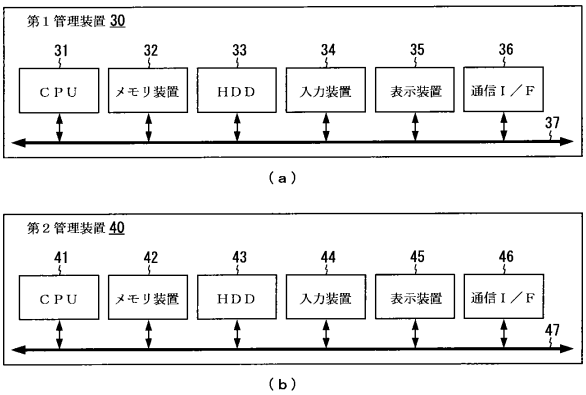
【図１】



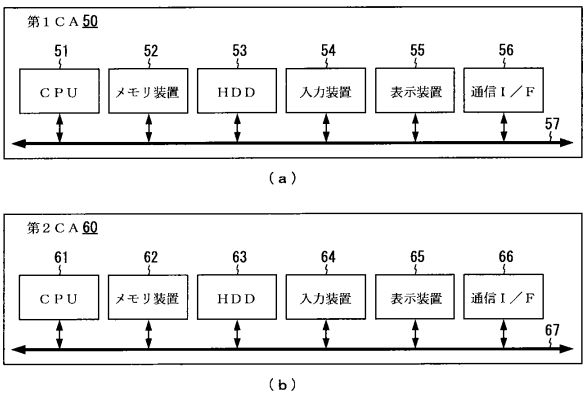
【図２】



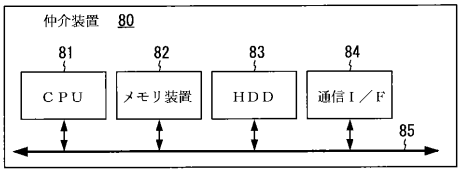
【図３】



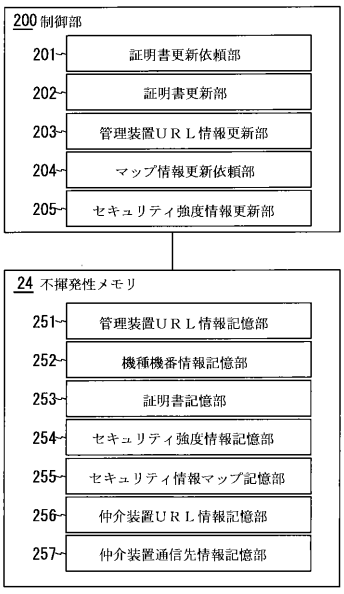
【図４】



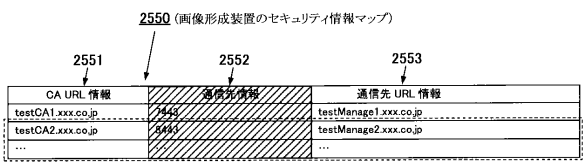
【図５】



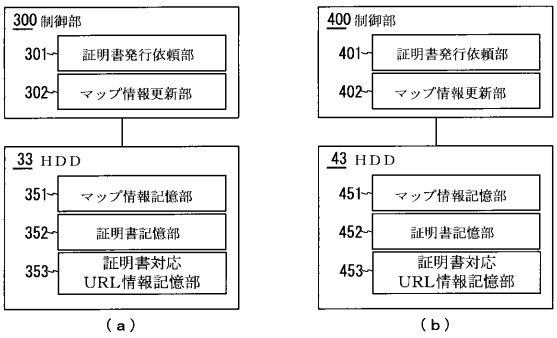
【図６】



【図７】



【図８】

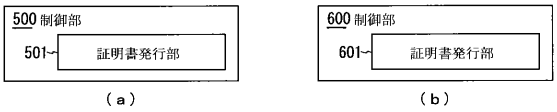


【図９】

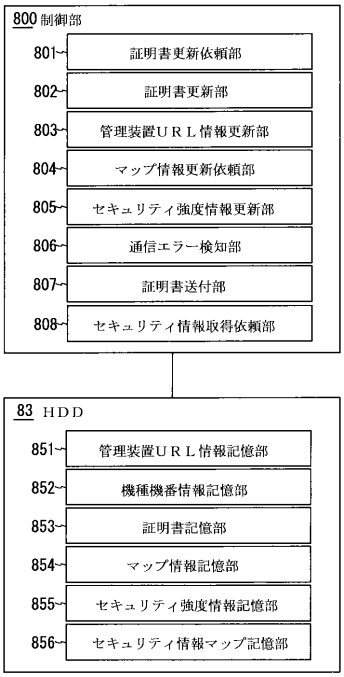
3510 (管理装置のマップ情報)

3511 機種機番情報	3512 CA URL 情報
3A88-123001	testCA1.xxx.co.jp
3A88-123002	testCA1.xxx.co.jp
3A88-123003	testCA1.xxx.co.jp
3A88-123004	testCA1.xxx.co.jp
…	…
4D56-012001	testCA2.xxx.co.jp
4D56-012002	testCA2.xxx.co.jp
4D56-012003	testCA2.xxx.co.jp
…	…

【図１０】



【図１１】



【図１２】

8540（仲介装置のマップ情報）

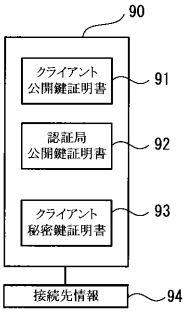
8541 機種機番情報	8542 CA URL 情報	8543 通信先情報
3A88-123001	testCA1.xxx.co.jp	7443
3A88-123002	testCA1.xxx.co.jp	7443
3A88-123003	testCA1.xxx.co.jp	7443
3A88-123004	testCA1.xxx.co.jp	7443
…	…	
4D56-012001	testCA2.xxx.co.jp	8443
4D56-012002	testCA2.xxx.co.jp	8443
4D56-012003	testCA2.xxx.co.jp	8443
…	…	

【図１３】

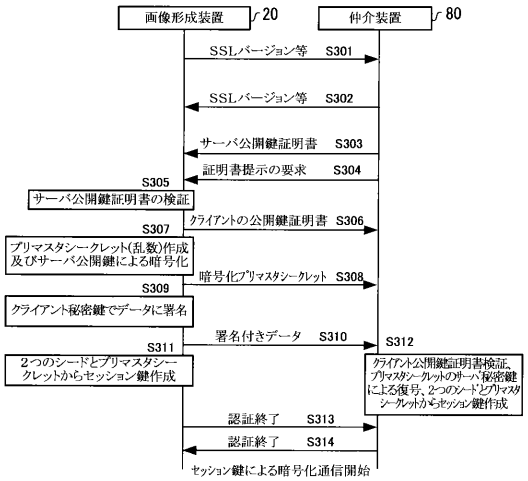
8560（仲介装置のセキュリティ情報マップ）

8561 CA URL 情報	8562 通信先情報	8563 通信先 URL 情報
testCA1.xxx.co.jp	7443	testManage1.xxx.co.jp
testCA2.xxx.co.jp	8443	testManage2.xxx.co.jp
…	…	…

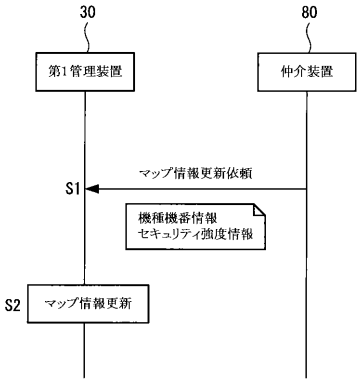
【図１４】



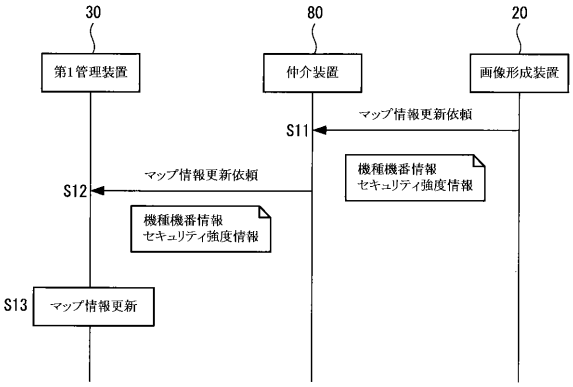
【図１５】



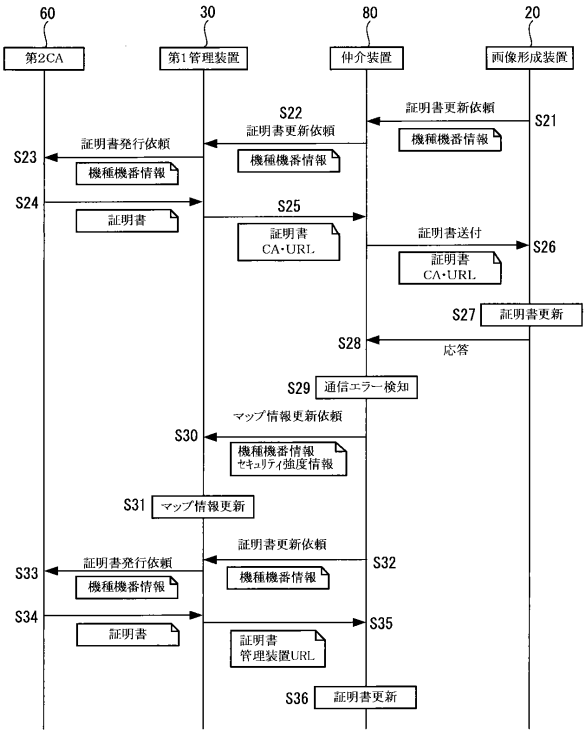
【図１６】



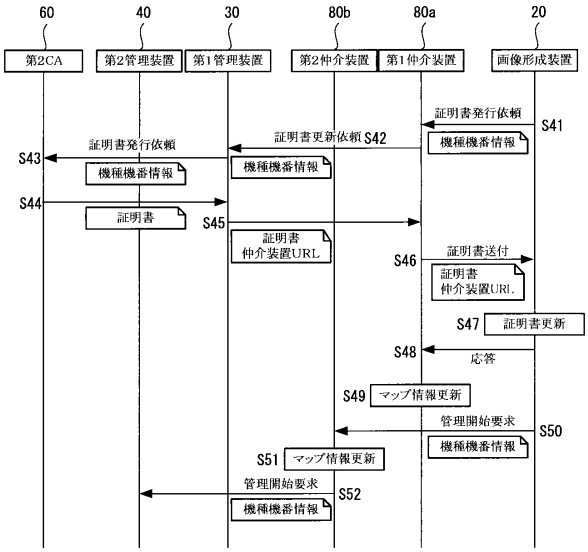
【図１７】



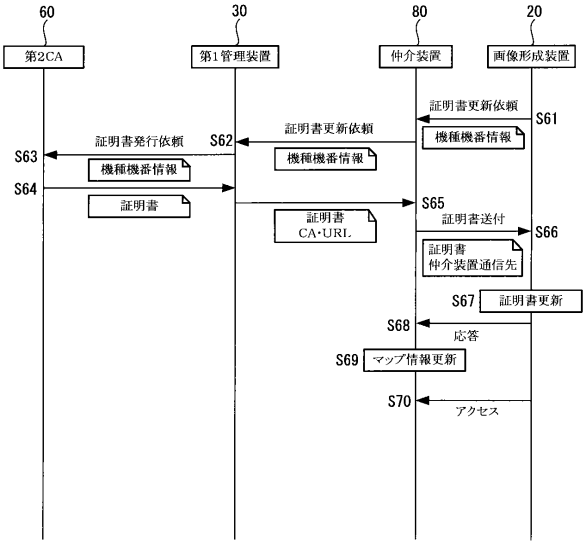
【図１８】



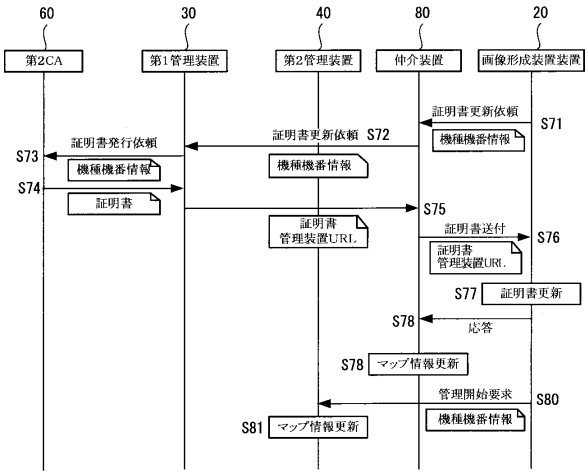
【図１９】



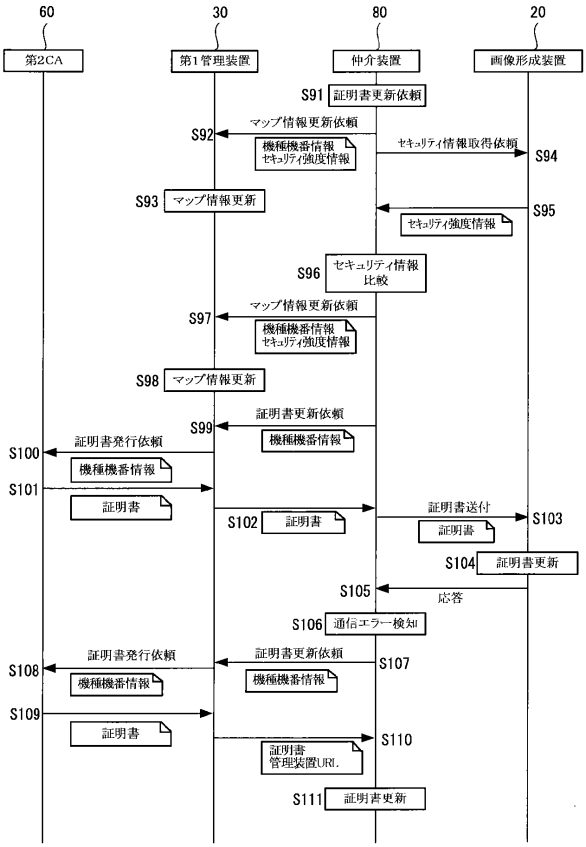
【図２０】



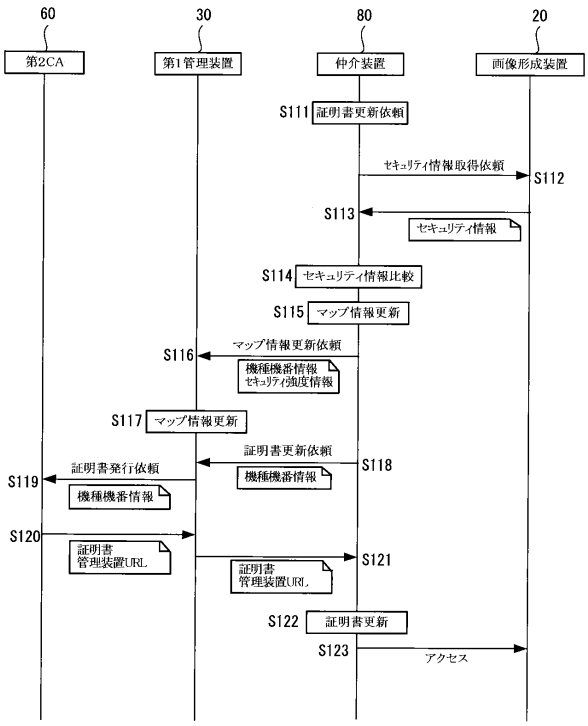
【図２１】



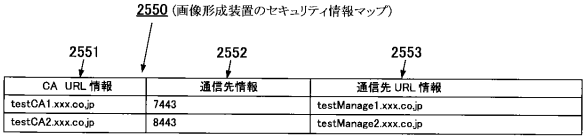
【図２２】



【図２３】



【図２４】



CA URL情報	通信先情報	通信先URL情報
testCA1.xxx.co.jp	7443	testManage1.xxx.co.jp
testCA2.xxx.co.jp	8443	testManage2.xxx.co.jp

フロントページの続き

(56)参考文献 特開２００８－００５０９０（ＪＰ，Ａ）
特開２００４－２５９１７６（ＪＰ，Ａ）
特開２０００－３３８８６８（ＪＰ，Ａ）
特開２０１１－０６６８３４（ＪＰ，Ａ）
山崎 重一郎，荒木 啓二郎，“信用情報と利用ポリシーの管理が可能な相互認証を実現する認証基盤の提案”，情報処理学会論文誌，日本，社団法人情報処理学会，１９９９年 1月１５日，第４０巻，第1号，ｐ．２９６－３０９

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ 9／３２
Ｈ０４Ｌ １２／２２