

明 細 書

発明の名称： 情報処理装置、制御方法、及び、プログラム

技術分野

[0001] 撮像画像をネットワークを介してクライアント装置に送信する情報処理装置における、セキュリティ機能の設定に関する。

背景技術

[0002] 従来、撮像装置のセキュリティ機能に関する設定を、当該撮像装置にネットワークを介して接続されたクライアント装置から撮像装置に対して行う技術が知られている。

[0003] 例えば、SSL(Secure Sockets Layer)プロトコルを用いた通信処理に用いられる鍵の生成や証明書の設定をクライアント装置から撮像装置に対して指示することができる。

[0004] クライアント装置から撮像装置に対してセキュリティ機能に関する設定を行うためのコマンドとして、ONVIF (Open Network Video Interface Forum) により策定された規格により定義されるコマンド群が知られている。ONVIFでは、セキュリティ機能に関連し、SSL、IEEE802.1X、クライアント認証の設定などが規格化されている。

[0005] 例えば、ONVIFのDevice Managementサービス（非特許文献1）に定義されたコマンドをクライアント装置が撮像装置に送信して、Device Managementサービスに適合した撮像装置に鍵の生成や証明書の設定ができる。

[0006] また例えば、ONVIFのAdvanced Securityサービス（非特許文献2）に定義されたコマンドをクライアント装置が撮像装置に送信して、Advanced Securityサービスに適合した撮像装置に鍵の生成や証明書の設定ができる。

先行技術文献

非特許文献

[0007] 非特許文献1：ONVIF-Core-Specification-v242 (<http://www.onvif.org/specs/core/ONVIF-Core-Specification-v242.pdf>)

非特許文献2：ONVIF-AdvancedSecurity-Service-Spec-v102 (<http://www.onvif.org/specs/srv/security/ONVIF-AdvancedSecurity-Service-Spec-v102.pdf>)

発明の概要

発明が解決しようとする課題

- [0008] クライアント装置から情報処理装置（例えば、撮像装置）に対して同じセキュリティ機能に関する設定を行うための通信手順（プロトコル）が複数存在する場合に、以下の課題が生じる場合があった。すなわち、第1の通信手順により情報処理装置に設定されたセキュリティ機能に関する設定の内容を、第1の通信手順と異なる第2の通信手順を用いるクライアント装置が参照できない場合があるという課題がある。

課題を解決するための手段

- [0009] 上記目的を達成するために、本発明は、第1の通信手順に基づいて行う命令に応じて、暗号化された通信を行うための設定を前記情報処理装置に対して行う第1の処理手段と、第2の通信手順に基づいて行う命令に応じて、暗号化された通信を行うための設定を前記情報処理装置に対して行う第2の処理手段と、前記情報処理装置に対して暗号化された通信を行うための設定を前記第1の処理手段が行った後に受信装置から前記第2の通信手順に基づいて行う命令を受信した場合、暗号化された通信を行うための設定が前記第1の通信手順に基づいて行う命令に応じて行われたことを示す情報を前記受信装置に送信する送信手段とを有する。

発明の効果

- [0010] このような構成によれば、第1の通信手順により情報処理装置に設定されたセキュリティ機能に関する設定の内容を、第1の通信手順と異なる第2の通信手順を用いるクライアント装置が参照することができる。

図面の簡単な説明

- [0011] [図1A]実施形態1に係るセキュリティ通信システムを示したブロック図

[図1B]実施形態1に係るセキュリティ通信システムを示したブロック図

[図2A]証明書等の設定処理を示す図

[図2B]証明書等の設定処理を示す図

[図3]証明書の生成処理を示したフローチャート

[図4]証明書のロード処理を示したフローチャート

[図5]証明書の取得処理を示したフローチャート

[図6]証明書の削除処理を示したフローチャート

[図7]証明書の状態の設定処理を示したフローチャート

[図8]証明書の状態の取得処理を示したフローチャート

[図9]証明書の状態の設定処理を示したフローチャート

[図10]証明書の状態の取得処理を示したフローチャート

[図11]実施形態2に係るセキュリティ通信システムを示したブロック図

[図12]SSLの設定ページのユーザインターフェースの例を示す図

[図13]自己署名証明書を生成する処理を示したフローチャート

[図14]CAが署名した証明書を使用する処理を示したフローチャート

発明を実施するための形態

[0012] 以下に、本発明の実施の形態を、添付の図面に基づいて詳細に説明する。

[0013] (実施形態1)

本実施形態では、第1のクライアント装置及び第2のクライアント装置が、0 NVIFにより規定された手順を用いて、情報処理装置としての撮像装置に対してセキュリティ機能に関する設定を行う例について説明する。

[0014] 本実施形態では、第1のクライアント装置は、ONVIFにより規定されたDevice Managementサービス（以下、「DMサービス」）（第1の手順）を用いて撮像装置に対してセキュリティ機能に関する設定を行う。また第2のクライアント装置は、ONVIFにより規定されたAdvanced Securityサービス（以下、「ASサービス」）（第2の手順）を用いて当該撮像装置に対してセキュリティに機能に関する設定を行う。

[0015] ここで、ONVIFにより規定されたDMサービスと、ASサービスとは独立したサ

ービスである。一方のサービスに基づいて撮像装置に設定された設定内容を、他方のサービスに基づいて当該撮像装置と通信を行うクライアント装置が参照できない場合がある。

[0016] 例えば、第1のクライアント装置がDMサービスに基づいて撮像装置に対してセキュリティ機能に関する設定を行う。次に、第2のクライアント装置がASサービスに規定されたコマンドを用いて、当該撮像装置に対して設定されたセキュリティ機能に関する設定を参照する。このとき、第1のクライアント装置によってDMサービスに基づいて設定したセキュリティの設定の内容を、第2のクライアント装置は参照することができない。

[0017] 従って、第1のクライアント装置によって撮像装置にセキュリティの設定がなされていた場合であっても、第2のクライアント装置からは当該設定が撮像装置に対して既になされていることに気づくことができない。そこで第2のクライアント装置のユーザは、新たなセキュリティ設定を撮像装置に対して行い、既存の設定を上書きしてしまう恐れがある。

[0018] そこで本実施形態にかかる撮像装置は、DMサービスに規定されたコマンドを用いて撮像装置に対する設定がなされたことを示す情報を、ASサービスに規定されているAlias情報として撮像装置内に記録する。このようにして、ASサービスを用いるクライアント装置からであっても、DMサービスによってセキュリティ機能に関する設定がなされていることを確認することができる。このようにして、一方のプロトコルを用いて撮像装置に対する設定を行うクライアント装置は、他方のプロトコルを用いて設定がなされていることを知ることができるようになる。

[0019] また本実施形態にかかる撮像装置は、DMサービスに基づいてセキュリティ設定がなされた場合に、設定された内容を用いて、ASサービスに応じた設定内容を自動的に生成して記録する。そして、Alias情報として、DMサービスによるセキュリティ設定の命令に応じて、ASサービスに応じた設定内容を生成したことを記録する。

[0020] 例えば、暗号化された通信を行うために用いる証明書を撮像装置に生成さ

せるための命令を、DMサービスに基づいて撮像装置が受信する。このとき撮像装置は、DMサービスに基づくセキュリティ設定では規定されていないが、ASサービスに基づくセキュリティ設定では必要とされる証明書パス設定や鍵ペア設定を自動的に行う。そして、証明書パスや鍵ペアの設定をDMサービスの命令の受信に応じて行ったことを示す情報をAlias情報として記録する。

[0021] このようにして、ユーザはDMサービスに基づく命令に応じて、ASサービスに準じたセキュリティ設定がなされたことを知ることができるようになる。

[0022] 実施形態1にかかる撮像システムのハードウェアの構成例について、図1Aを用いて説明する。実施形態1では、撮像装置100がネットワーク108を介して、クライアント装置200及びクライアント装置300に接続された例について説明する。本実施形態において、撮像装置100は撮像した撮像画像を、ネットワークを介してクライアント装置200及びクライアント装置300に送信する。本実施形態では撮像部101を撮像装置100の内部に有する例について説明するがこれに限らない。撮像画像の送信のためのセキュリティに関する設定を管理することができればよく、撮像装置100にかえて、外部の撮像装置から撮像画像を受信して、クライアント装置200及びクライアント装置300に中継する情報処理装置であってもよい。

[0023] 撮像装置100の撮像部101が撮像した画像データは、後述の画像処理部102において処理された後、ネットワーク108を介してクライアント装置200及びクライアント装置300に送信される。

[0024] 撮像部101は、被写体を撮像して画像信号を生成する。撮像部101は、レンズやCMOS (Complementary Metal Oxide Semiconductor) などの撮像素子などによって構成される。撮像素子はレンズによって結像された被写体の像を画像信号に変換する。

[0025] 画像処理部102は、撮像部101が生成した画像信号に対する画像処理を行う。画像処理部102は、例えば、撮像部101が撮像した画像の符号化を行う。画像処理部102は例えば、CPU (Central Processing Unit) などのプロセッサとすることができる。あるいはGPU (Graphics Processing Unit) などの画像処

理のためのプロセッサとすることができる。

[0026] 撮像装置100の制御部103は、図1Aに示した撮像装置100の各構成の制御を行う。制御部103は例えば、CPUなどのプロセッサとすることができる。制御部103がプロセッサとして構成される場合、例えば制御部103は、後述の記録部104に記録されたプログラムを実行することにより、撮像装置100の各構成を制御する。

[0027] 制御部103は、図1Bを用いて後述する撮像装置100の機能を実現するための制御を行う。特に、図1Bを用いて後述するDeviceManagementサービス部112（以下、「DMサービス部112」）の機能を実現するための第1処理部106を有する。また制御部103は、後述のAdvancedSecurityサービス部113（以下、ASサービス部113）を実現するための第2処理部107を有する。また制御部103は、異なる複数の通信手順のうちの一つの通信手順に基づいて行う命令によって撮像装置100に対して設定がなされたことを示す情報を記録部104に記録させる制御を行う。

[0028] 記録部104は、撮像部101が撮像し、画像処理部102が画像処理を行った撮像画像を記録する。さらに、記録部104は制御部103が用いるプログラムや制御パラメータを記録する。また記録部104は、後述のKeystore部114が記録する各種の設定内容を記録する。

[0029] 記録部104は、例えば、RAM（Random Access Memory）やROM（Read Only Memory）等のメモリとすることができる。あるいはHDD（Hard Disk Drive）等の記録媒体であってもよい。また記録部104は、フラッシュメモリやメモリカード等のリムーバブルメディアとしてもよい。

[0030] 通信部105は、撮像部101において撮像され画像処理部102において画像処理して生成された撮像画像を、クライアント装置200及びクライアント装置300に送信する。撮像画像の送信の際には、記録部104に記録された設定情報に基づいて暗号化された通信が用いられる。また通信部105は、第1の通信手順及び第2の通信手順のうち一方の通信手順に基づいて行う命令に応じて撮像装置100に対して設定がなされたことを示す情報を、他方の通信手順に基づいて

行う命令に応じて、クライアント装置200又は300に送信する。さらに通信部105は、クライアント装置200及びクライアント装置300から撮像装置100に対する制御命令を受信する。

[0031] 例えば通信部105は、撮像装置100に対して暗号化された通信を行うための設定を第1の処理部が行った後に、クライアント装置300から第2の通信手順に基づいて行う命令を受信した場合、以下の情報を送信する。すなわち通信部105は、暗号化された通信を行うための設定が第1の通信手順に基づいて行う命令に応じて行われたことを示す情報をクライアント装置300に送信する。

[0032] クライアント装置200及びクライアント装置300は、撮像装置100に対し通信セキュリティに関する設定を行う。クライアント装置200は、例えば、撮像装置100と通信を行うための通信部201を有する。また、クライアント装置200はクライアント装置200の各構成を制御するための制御部202を有する。制御部202は例えば、CPUなどのプロセッサとすることができる。制御部202がプロセッサとして構成される場合、例えば制御部202は、後述の記録部203に記録されたプログラムを実行することにより、クライアント装置200の各構成を制御する。さらに、クライアント装置200は、制御部202が用いるプログラムや制御パラメータを記録する記録部203を有する。記録部203は、例えば、RAMやROM等のメモリとすることができる。あるいはHDD等の記録媒体であってもよい。また記録部203は、フラッシュメモリやメモリカード等のリムーバブルメディアとしてもよい。

[0033] クライアント装置200の構成は特に限定せず、上記の例に限られない。上記の構成の一部を他の構成により置き換えたり、或いは、新たな構成を付加することとしてもよい。クライアント装置300の構成についても、クライアント装置200の構成と同様であるため、説明を省略する。

[0034] クライアント装置200及びクライアント装置300は、例えば、PC (Personal Computer) とすることができる。あるいは、タブレット端末、スマートフォン等の携帯用端末とすることができる。

[0035] ネットワーク108は、例えば、インターネットや有線LAN (Local Area Netw

ork)、無線LAN (Wireless LAN)、WAN (Wide Area Network)、又は、アナログケーブル等により構成される。ネットワーク108は、その通信規格、規模、構成を問わない。LANの通信規格として、例えばEthernet (登録商標)等を用いることができる。

[0036] 次に、図1Bの機能ブロック図を用いて、本実施形態にかかる撮像装置100、クライアント装置200、及び、クライアント装置300の機能について説明する。

[0037] 図1Bに示すクライアント装置200は、DMサービスのセキュリティ関係のコマンドを撮像装置100に対して送信する機能を有する。また、クライアント装置300は、ASサービスのコマンドを撮像装置100に対して送信する機能を有する。クライアント装置200とクライアント装置300は、ネットワーク108を介し撮像装置100に対して鍵 (Key) や証明書 (Certificate) の設定を行う機能を有する。証明書は、証明書に記載された鍵が認証局に登録された鍵であることを示し、例えば、認証局に登録された公開鍵を示す情報、公開鍵の持ち主の情報、証明書を発行した認証局の情報、発行元認証局の署名等を含む。

[0038] 撮像装置100は、ONVIFが規定するDMサービス、及び、ASサービスに対応している。すなわち、本実施形態に係る撮像装置100はDMサービスで用いられるコマンドの受信に応じてセキュリティ機能に関する設定を行う。また本実施形態に係る撮像装置100はASサービスで用いられるコマンドの受信に応じてセキュリティ機能に関する設定も行うことができる。

[0039] 撮像装置100のHTTPサーバ部111は、クライアント装置200又はクライアント装置300から送信されたSOAPメッセージを受信する。SOAPメッセージはSOAP (Simple Object Access Protocol)を用いて送受信されるメッセージである。

[0040] HTTPサーバ部111は、クライアント装置200及びクライアント装置300から送信されたSOAPメッセージを受信する。そして、受信したメッセージを、DMサービス部112もしくはASサービス部113に送信する。

クライアント装置200及び300は、撮像装置100のDMサービス部112もしくはASサービス部113を指定するURI (Uniform Resource Identifier) に、SOAPメッ

セージをPOSTする。このようにしてSOAPメッセージを送信することができる。メッセージのPOSTは、HTTP (Hypertext Transfer Protocol) のPOSTメソッドを用いて実行される。本実施形態において、HTTPサーバ部111の機能は、図1 Aに示した通信部105により実現される。

[0041] DMサービス部112とASサービス部113はそれぞれ、受信したSOAPメッセージを解析し、コマンドとその設定内容に応じて撮像装置100のセキュリティ関係の設定もしくは設定されている内容を返答として返す。本実施形態において、DMサービス部112及びASサービス部113の機能は、図1 Aに示した制御部103により実現される。

[0042] 制御部103がDMサービス部112の機能を実現する場合、クライアント装置200が撮像装置100に対してDMサービス（第1の通信手順）を用いて行う命令を実行する第1の処理手段として機能する。また制御部103がASサービス部113の機能を実現する場合、クライアント装置300が撮像装置100に対してASサービス（第1の通信手順と異なる第2の通信手順）を用いて行う命令を実行する第2の処理手段として機能する。

[0043] DMサービス部112は、クライアント装置200が撮像装置100に対してDMサービスをに基づいて行う命令を実行する。DMサービスに基づいて行う命令には、暗号化された通信を行うために用いる公開鍵（第1の公開鍵情報）を撮像装置100に設定するための命令、第1の公開鍵情報に対応する非公開鍵（第1の非公開鍵情報）を撮像装置100に設定するための命令が含まれる。またDMサービスに基づいて行う命令には、公開鍵が正当な鍵情報であることを証明するための証明書（第1の証明書情報）を撮像装置100に設定するための命令が含まれる。DMサービス部112はこれらの全ての命令を必ずしも実行しなくてもよく、少なくともいずれか一つの命令を実行すればよい。

[0044] ASサービス部113は、クライアント装置300が撮像装置100に対してASサービスに基づいて行う命令を実行する。ASサービスに基づいて行う命令には、暗号化された通信を行うために用いる公開鍵（第2の公開鍵情報）と非公開鍵（第2の非公開鍵情報）とが対応することを示す鍵ペア情報を撮像装置100に

設定するための命令が含まれる。また、ASサービスに基づいて行う命令には、公開鍵が正当な鍵情報であることを証明するための証明書（第2の証明書情報）を撮像装置100に設定するための命令が含まれる。さらにASサービスに基づいて行う命令には証明書に関連する他の証明書情報を示す証明書パス（証明書パス情報）を撮像装置100に設定するための命令が含まれる。ASサービス部113はこれらの全ての命令を必ずしも実行しなくてもよく、少なくともいずれか一つの命令を実行すればよい。

[0045] Keystore部114はONVIFのAdvanced Securityに定義されたKeystoreのKeystore情報を保存するデータベースである。本実施形態において、Keystore部114の機能は、図1Aに示した記録部104により実現される。Keystore部114は、以下の記録部を有する。

[0046] Keypair部115：非公開鍵（Privatekey）と、公開鍵（Publickey）と、クライアントが任意の文字列を設定するAliasと、Keypairとを対応付けて一意に示すKeyID（鍵ID）を記録する。

[0047] Certificate部116：証明書（Certificate）と、Aliasと、証明書の公開鍵が保存されたKeypairのKeyIDとを対応付けて一意に示すCertificateID（証明書ID）情報を記録する。

[0048] CertificationPath部117：証明書パスIDと、Aliasと証明書パス（CertificationPath）とを対応付けて一意に示すCertificationPathID（証明書パスID）情報を記録する。証明書パスID（CertificationPathID）は複数の証明書に対応付けられた順序を1つまたは複数のCertificateIDで示す。

[0049] 証明書パスは、撮像装置100が暗号化された通信を行うために証明書を参照する順序、及び、複数の証明書の階層構造を表す。例えばSSL通信等では、第1の証明書を発行した第1の認証局が信頼できる認証局であることを証明するために第2の認証局が第2の証明書を発行する。さらに第2の認証局が信頼できる認証局であることを証明するためにルート認証局が第3の証明書を発行する。この例では、第1の証明書、第2の証明書、及び、第3の証明書が階層構造を成す。証明書パスは、このような証明書の階層構造を示す情報

である。上述の例では証明書の階層構造が3層の場合について説明したが、3層に限られず任意の階層構造を取ることとすればよい。撮像装置100は、証明書を用いて暗号化された通信を行う場合に、第1の証明書を参照する。次に、第1の証明書に含まれる認証局の署名を参照して、第2の証明書を参照する。さらに第2の証明書に含まれる認証局の署名を参照して第3の証明書を参照する。このようにして、撮像装置100は、第1の証明書、第2の証明書、第3の証明書という順序で証明書を参照する。上述の例では3つの証明書の順序について説明したが、証明書数は限られず任意の数とすることができる。

[0050] Keypair部115、Certificate部116、及び、CertificationPath部117のそれぞれには、任意の文字列を記録するための記録領域（Alias）が設けられている。

[0051] クライアント装置200が、DMサービスに基づいて撮像装置100に公開鍵、非公開鍵、及び、証明書を設定する処理について、図2A及び図2Bを用いて説明する。これらの公開鍵、非公開鍵、及び、証明書は、撮像装置100とクライアント装置200との間でHTTPSを用いたセキュリティ通信を開始するために撮像装置100が予め記録している必要がある。

[0052] まず、クライアント装置200が行う処理について、図2Aのフローチャートを用いて説明する。図2Aに示した判定処理は、ユーザの指示に応じてクライアント装置200が実行することができる。あるいは、記録部203に記録されたプログラムを制御部202が読みだして実行することにより、図2Aのフローチャートに示した処理を実行することとしてもよい。

[0053] クライアント装置200は、撮像装置100においてHTTPS（Hypertext Transfer Protocol Secure）サービスが有効であるか否かを示す状態情報を取得する（S201）。

[0054] HTTPSによる設定が有効な状態とは、SSLあるいはTLS（Transport Layer Security）などを用いたHTTPS通信を開始することが可能な状態のことである。すなわちHTTPS通信に用いる公開鍵、非公開鍵、及び、証明書が既に撮像装置100に設定されている状態である。

- [0055] 一方、HTTPSによる設定が無効な状態とは、HTTPS通信を行うために用いる公開鍵、非公開鍵、及び、証明書が撮像装置100に設定されていない状態である。例えば、証明書が有効期限切れ、廃棄状態、又は、一時停止状態にあり、その証明書を用いてHTTPS通信を行うことができない状態等を含む。
- [0056] ステップS201において、クライアント装置200は、撮像装置100へGetNetworkProtocolsコマンドを送信する。GetNetworkProtocolsコマンドにより、クライアント装置200は、撮像装置100で提供されているHTTPとHTTPSとRTSP (Real Time Streaming Protocol) のサービスの状態情報の取得を要求する。この状態情報には各サービスが有効であるか無効であることを示す情報が含まれる。またクライアント装置200は、GetNetworkProtocolsコマンドにより、サービスが提供されているポート番号の情報の取得を要求する。撮像装置100は、クライアント装置200に対して、GetNetworkProtocolsレスポンスを応答する。
- [0057] 次にクライアント装置200は、GetNetworkProtocolsレスポンスを確認して、HTTPSによる設定が有効であるか否か判定する (S202)。HTTPSの設定が無効である場合 (S202においてN0の場合)、後述のステップS207の処理に進む。
- [0058] HTTPSによる設定が有効である場合 (S202においてYESの場合)、クライアント装置200は、HTTPSの設定をそのまま使うか、又は、別途HTTPSの設定をするかを判定する (S203)。既に設定されているHTTPSの設定を使う場合 (S203においてYESの場合)、現在撮像装置100に対する、公開鍵、非公開鍵、及び、証明書の設定を終了する。
- [0059] 一方、新たなHTTPSの設定を行う場合 (S203においてN0の場合)、クライアント装置200は撮像装置100が持っている証明書を全て取得する (S204)。
- [0060] ステップS204において、クライアント装置200は、装置100へGetCertificatesコマンドを送信する。撮像装置100は、クライアント装置200に対して、GetCertificatesレスポンスを応答する。GetCertificatesコマンドは、クライアント装置200が、撮像装置100が持っている全ての証明書を示す情報を取得す

ることを要求するためのコマンドである。

- [0061] GetCertificatesレスポンスとして、撮像装置100が有する証明書 (Certificate) を取得する。クライアント装置200は取得した証明書のうちから選択された証明書を使うか、新規に証明書を生成するかを判定する (S205)。ステップS205の判定は、例えば、何れの証明書を用いるかについてのユーザからの指示に応じて判定を行うことができる。
- [0062] クライアント装置200は、撮像装置100から取得した証明書のうちから選択した証明書をHTTPS通信において用いる場合 (S205でYESの場合)、選択した証明書を撮像装置100に設定する (S206)。証明書の設定には、SetCertificatesStatusコマンドを用いることができる。SetCertificatesStatusコマンドは、暗号化された通信を行うために用いる設定情報を記録部104に記録させるための命令である。SetCertificatesStatusコマンドは、クライアント装置200 (第1の受信装置) が撮像装置100に対してDMサービス (第1の通信手順) に基づいて行う命令である。
- [0063] ステップS205において、新規に証明書を生成すると判定した場合 (S205でN0の場合)、クライアント装置200は撮像装置100において新規に公開鍵、非公開鍵、及び、証明書を生成するか判定する (S207)。
- [0064] 撮像装置100において公開鍵、非公開鍵、及び、証明書を生成する場合 (S207でYESの場合)、クライアント装置200は撮像装置100に公開鍵、非公開鍵、及び自己署名証明書の生成を指示する。自己署名証明書は、適宜、SelfSignedCertificateと表記する。
- [0065] クライアント装置200は、CreateCertificateコマンドを用いて、撮像装置100に対して公開鍵と非公開鍵とを生成し、それを用いて自己署名証明書を生成することを要求する。
- [0066] 撮像装置100において新規に公開鍵、非公開鍵、及び、証明書を生成しないと判定した場合 (S207においてN0の場合)、クライアント装置200は自装置内で公開鍵、非公開鍵、及び、証明書を生成する (S210)。そしてクライアント装置200は、生成した非公開鍵、及び、証明書を、LoadCertificateWithPriva

teKeyコマンドを用いて、撮像装置100へロードする（S211）。クライアント装置200から撮像装置100への非公開鍵、及び、証明書のロード処理については、図4を用いて詳細を後述する。

[0067] ステップS209の処理、又は、ステップS211の処理が完了すると、クライアント装置200は、生成した公開鍵、非公開鍵、及び、証明書をHTTPS通信に用いるように、撮像装置100に対して設定する。

[0068] クライアント装置200は、証明書をHTTPS通信に使う状態となっているかどうかを示すステータス情報を、GetCertificatesStatusコマンドを用いて取得する。CreateCertificateコマンドによってCertificateを生成した段階では、生成した証明書をHTTPS通信に使うように設定はされていない。そこで、クライアント装置200は、SetCertificatesStatusコマンドを撮像装置100に送信することによりStatusをTrueに設定する。このようにして、生成した証明書をHTTPS通信に使うように設定することができる。

[0069] SetNetworkProtocolsコマンドはHTTPとHTTPSとRTSPのサービスの有効・無効の状態と、それらのサービスを提供するポート番号を設定するコマンドである。HTTPSを有効（Enable）にすると、撮像装置100はStatusがTrueの証明書をHTTPS通信に使用するようにHTTPサーバ部111を設定する。

[0070] なお、撮像装置100とクライアント装置200との間の、HTTPS通信を行うための設定のシーケンスを図2Bに示す。以上のようにして、クライアント装置200はDMサービスに基づいて、撮像装置100に対して設定を行う。

[0071] 一方、クライアント装置300がASサービスに基づいてHTTPS通信の設定をする場合、鍵ペア（KeyPair）と証明書（Certificate）と証明書パス（CertificationPath）とを撮像装置100に設定する。クライアント装置300は、AddServerCertificateAssignmentコマンドを用いて、HTTPS通信を行うために用いる証明書パスを撮像装置100に設定する。鍵ペア、及び、証明書パスはDMサービスにはないASサービスの概念である。

[0072] ここで、クライアント装置300がASサービスを使用して撮像装置100に対しHTTPS通信の設定をした後、クライアント装置200がDMサービスを使用して撮像

装置100に対してHTTPS通信の設定を開始すると以下が生じ得る。

- [0073] 例えば、クライアント装置300が設定を行った後、クライアント装置200が図2AのステップS201において、GetNetworkProtocolsコマンドを実行し、撮像装置100のHTTPSの設定の有無を確認する。この場合、クライアント装置300によって既にHTTPSの設定が有効化されているので、撮像装置100は、クライアント装置200に対してHTTPS通信の設定が有効（Enable）である旨を応答する。すなわち、HTTPS通信に用いられる公開鍵、非公開鍵、及び、証明書が、撮像装置100に設定されている旨が応答される。
- [0074] しかし、クライアント装置200がステップS204で証明書を要求しても、クライアント装置300が設定した証明書がクライアント装置200に送信されない。これは、ASサービスにではASサービスのコマンドを用いて撮像装置100に設定された証明書を、DMサービスのGetCertificatesコマンドに応答して送信することが規定されていないためである。
- [0075] このように、撮像装置100に証明書が設定されているのに、証明書の要求コマンドに対して証明書が送信されない理由が分からず、クライアント装置200のユーザに混乱を生じさせてしまう場合がある。
- [0076] また、クライアント装置200がステップS212においてGetCertificatesStatusコマンドを実行しても、クライアント装置200には証明書の状態が空で通知される。これは、DMサービスにはASサービスの証明書パスや鍵ペアという概念が無く、GetCertificatesStatusで返答するものが無い状態になるためである。
- [0077] さらに、ASサービスで設定可能なCACertificate（中間証明書またはCA証明書またはクロスルート証明書）の概念もないため、DMサービスでは設定の表現ができない。
- [0078] 加えて、クライアント装置200がDMサービスに基づいてHTTPS通信の設定をした場合、ASには証明書のStatusという概念はなく、DMサービスで設定した内容をASサービスで参照できない。
- [0079] そこで本実施形態にかかる撮像装置100は、ASサービスに規定のKeystoreを

使い、クライアント装置200から参照される撮像装置100の設定の内容とクライアント装置300から参照される撮像装置100の設定との整合性が取れるようにする。クライアント装置200及びクライアント装置300において参照される撮像装置100の設定の整合性が取れるようにするための詳細な構成について、図3のフローチャートを用いて説明する。

[0080] 図3は、撮像装置100により実行される処理である。撮像装置100の制御部103がプロセッサ及びメモリを内蔵する形態では、図3に示した処理は、図3に示される手順を制御部103が記録部104に格納されたプログラムを展開して実行することにより実現される。あるいは、図3に示す処理の一部又は全体をハードウェアが行うこととしてもよい。

[0081] 図3は、図2Aに示したDMサービス部112における、CreateCertificateコマンドの処理を示したフローチャートである。CreateCertificateコマンドは、クライアント装置200が撮像装置100に対して証明書の生成を指示するための命令である。

[0082] 撮像装置100は、クライアント装置200から、証明書の生成を指示するコマンドを受信する（S0301）。本実施形態では、ステップS301において、撮像装置100はクライアント装置200からCreateCertificateコマンドを受信する。

[0083] 本実施形態では、ステップS301において、クライアント装置200が撮像装置100に対して以下内容を設定する場合について説明する。

[0084] CertificateID 123456
Subject CN=sample.com
ValidNotBefore 2015-01-01T01:00:00Z
ValidNotAfter 2020-12-31T23:59:59Z

[0085] DMサービス部112は、HTTPサーバ部111を介して上記のCreateCertificateコマンドを受信すると、公開鍵と非公開鍵を生成する（S302）。ASサービスのCreateRSAKeyPairコマンドによればKeyLengthを指定することでRSAの鍵長を設定できる。しかし、DMサービスのCreateCertificateコマンドにはそのような設定を行うことができないため、例えば2048ビットなど固定の鍵長で生成す

る。

[0086] 次にDMサービス部112は、生成した公開鍵と非公開鍵とを使用して自己署名証明書を生成する（S303）。自己署名証明書は、公開鍵が正当な鍵情報であることを証明するための証明書情報であってDMサービス部112により署名情報が付加された証明書情報である。DMサービスの仕様ではSubjectはstring型で、どのように国名（Country）や一般名（CommonName）を設定すれば良いかは定義がない。本実施形態では、一般名を設定する場合は「CN=」の後に設定するものとする。「CN=」以降の文字列である「sample.com」を自己署名証明書のSubjectとIssuerに設定し、「ValidN0tBefore」を証明書の有効期限の開始日、「ValidN0tAfter」を証明書の有効期限の終了日とする。

[0087] 次にKeystore部114のKeypair部115に設定の内容を記録する（S304）。ステップS304では、公開鍵と非公開鍵と自己書署名証明書とをKeypair部115に保存する。またステップS304において、Keypair部115に記録されていないユニークな文字列をKeyID（鍵ペア情報）として生成しKeypair部115に保存する。このKeyIDは、ステップS304において生成した公開鍵と非公開鍵の両者に関連付けられ、この公開鍵と非公開鍵とが対応することを示す。またステップS304において、Keypair部115のAliasには、DMサービスを用いたコマンドによって、鍵ペア情報が生成されたことを示す情報が記録される。Keypair部115のAliasに記録される情報は例えば、「ONVIF Device Management」等の文字列とすることができる。

[0088] このようにして、DMサービスに概念が無い鍵ペア情報を、DMサービスが提供する証明書を生成させるための命令に応じて自動的に生成することができる。さらに、この鍵ペア情報がDMサービスのコマンドによって生成されたことが分かるように、記録部104に記録を残すことができる。

[0089] 同様に、S304において、Keypair部115のAliasには、DMサービスを用いたコマンドによって、自己署名証明書が生成されたことを示す文字列が記録される。

[0090] 次に、Keystore部114のCertificate部116に設定の内容を記録する（S305）

。ステップS305では、生成した自己署名証明書をCertificate部116に保存する。またステップS305において、Certificate部116に存在しないユニークな文字列をCertificateIDとして生成しCertificate部116に記録する。またステップS305において、Certificate部116のAliasにはDMサービスを用いたコマンドによって、HTTPSに関する設定が撮像装置100に対してなされたことを示す文字列が記録される。また、ステップS305において、Certificate部116に記録された情報とKeypair部115に記録された情報とを関連付けるため、Keypair部115に記録したKeyIDをCertificate部116にも保存する。

[0091] 次に、Keystore部114のCertificationPath部117に設定の内容を記録する（S306）。CreateCertificateコマンドに応じて証明書を生成する場合、自己署名証明書を使うので、証明書の階層は1のみである。そのためステップS306において、CertificationPath部117には、CertificationPathIDとして、ステップS305で生成したCertificateIDのみを設定する。また、CertificationPath部117のAliasにはDMサービスを用いたコマンドによって証明書パス情報を生成したことを示す情報を記録部104に記録する。

[0092] このようにして、ASサービスには概念が無い証明書パス情報を、DMサービスが提供する証明書を生成させるための命令に応じて自動的に生成することができる。さらに、証明書パス情報がDMサービスの命令によって生成されたことが分かるように、記録部104に記録を残すことができる。

[0093] 最後に、CreateCertificateの返答のCertificateIDとCertificateに、ステップS305で生成したCertificateIDと自己署名証明書をそれぞれ代入する。そして、クライアント装置200へ送信する（S307）。

[0094] このようにして、クライアント装置300は、クライアント装置200が撮像装置100に対して設定した公開鍵と非公開鍵とをKeypairとして参照できる。本実施形態では、Keypairを参照するためにクライアント装置300はGetAllKeysコマンドを撮像装置100に送信する。Keypair部115のAliasには、DMサービスを用いたコマンドによって公開鍵及び非公開鍵が既に設定されていることを示す文字列が記述されている。このAliasの内容は、GetAllKeysコマンドに対

する応答として、撮像装置100からクライアント装置300に送信される。したがって、クライアント装置300のユーザは、DMサービスを用いるクライアント装置200によって公開鍵及び非公開鍵が撮像装置100に設定されていることを知ることができる。

[0095] また、Certificate部116のAliasには、DMサービスを用いたコマンドによって証明書及び証明書パスが設定されていることを示す文字列が記述されている。このAliasの内容は、撮像装置100からクライアント装置300に送信される。

[0096] したがって、クライアント装置300のユーザは、DMサービスを用いるクライアント装置200によって証明書及び証明書パスが設定されていることを知ることができる。クライアント装置300はAddServerCertificateAssignmentコマンドによりCertificationPathIDを指定して、クライアント装置200が生成した自己署名証明書をHTTPS通信で使うよう設定できる。

[0097] 次に、図2AのステップS211の処理によって非公開鍵、及び、証明書をクライアント装置200から撮像装置100へロードした場合の撮像装置100における処理について、図4を用いて説明する。図4に示した処理は、撮像装置100により実行される処理である。撮像装置100の制御部103がプロセッサ及びメモリを内蔵する形態では、図4に示した処理は、図4に示される手順を制御部103が記録部104に格納されたプログラムを展開して実行することにより実現される。あるいは、図4に示す処理の一部又は全体をハードウェアが行うこととしてもよい。

[0098] 撮像装置100は、クライアント装置200から、証明書をロードするためのコマンド（LoadCertificates）を受信する（S401）。LoadCertificatesコマンドには以下の内容が含まれる。

CertificateID : GetPkcs10RequestでCSR（Certificate Signing Request : 証明書署名要求）を生成した時に指定したCertificateID

証明書 : 認証局（Certification Authority: CA）が署名（Sign）した証明書

DMサービス部112がLoadCertificatesコマンドを受信すると、Keystore部11

4からKeypair部115に格納された情報（Keypair情報）を取得する（S402）。

次にCertificate部116から公開鍵を取得する（S403）。

[0099] CreateCertificateコマンドに応答して撮像装置100が生成した自己署名証明書について、公開鍵と非公開鍵は、Keystore部114のKeypair部115に記録されている。その自己証明書のCertificateIDを元に生成したCSR（Certificate Signing Request：証明書署名要求）に署名した証明書も同様に関連した鍵ペアがある。撮像装置100は、Keypair部115に記録されている公開鍵と、ステップS403において取得した公開鍵とが一致するか判定する（S404）。

[0100] Keystore部114のKeypair部115にCertificate部116の公開鍵に一致するものが無い場合（S404においてN0の場合）、証明書として使えないため、エラー処理する（S410）。

[0101] 一方、Keystore部114のKeypair部115にCertificate部116の公開鍵に一致するものがある場合（S404においてYESの場合）、指定されたCertificateIDを含んだ証明書パスを削除する（S405）。このようにして、自己署名証明書のために設定された証明書パスを削除することができる。

[0102] 次に、Keystore部114のCertificate部116が記録する情報が示すCertificateIDを有する証明書を削除する（S406）。次に、クライアント装置200からロードされた証明書を含んだ証明書パスを設定する。ロードされた証明書に加え、DMサービスを用いたコマンドによって設定されたことを示すAliasをKeystore部114のCertificationPath部117に保存する（S407）。次に、CertificateIDを設定した証明書パスを生成する。そして、ユニークなCertificationPathIDと、DMサービスによって設定がなされたことを示すAliasをKeystore部114のCertificationPath部117に保存する。

[0103] LoadCertificatesコマンドは複数の証明書のロードを指定できるので、さらに他にロードすべき証明書があるか否かを判定する（S409）。さらにロードすべき証明書がある場合（409でYESの場合）、ステップS403に戻る。全ての証明書の処理が終われば（409でN0の場合）、LoadCertificatesコマンドに対する返答をクライアント装置200に送信する（S411）。

- [0104] この時点で、クライアント装置200がロードした証明書は、以下の手順によりクライアント装置300が撮像装置100に対して暗号化通信を行う時に用いる証明書として設定を行うことができるようになる。すなわち、クライアント装置300がAddServerCertificateAssignmentコマンドによりCertificationPathIDを指定すればHTTPS通信（例えば、SSL）で使うよう設定できる。
- [0105] DMサービス部112においてLoadCACertificatesコマンドを処理する場合、CACertificateの非公開鍵はKeystore部114のKeypair部115に無い。そこで、Keystore部114から鍵ペアを取得する。そして、ロードされた証明書の公開鍵と、Keypair部115に保存された非公開鍵の組み合わせが一致するものをエラーとすることができる。一致するものが無ければ、Certificate部116から取得した公開鍵とユニークなKeyIDをKeystore部114のKeypair部115に保存し、そのAliasにはDMサービスのコマンドに応じて設定したことを示す情報を設定する。さらに、証明書とユニークなCertificateIDをKeystore部114のCertificate部116に保存し、さらにそのAliasにはDMサービスのコマンドに応じて設定したことを示す情報を設定する。
- [0106] 次に、撮像装置100がクライアント装置200からGetCertificatesを受信した場合の処理について、図5を用いて説明する。図5の処理は、図2BのDMサービス部112において実現される。
- [0107] クライアント装置200からGetCertificatesを受信すると（S501）、DMサービス部112はKeystore部114から鍵ペアと証明書を取得する（S502）。
- [0108] 次に、取得した証明書に関連付けられたKeypair部115を参照し、Keypair部115に非公開鍵があるか判定する（S503）。非公開鍵がある場合（S503でYESの場合）、返答のNVTCertificateに証明書を追加する（S504）。
- [0109] Keypair部115に非公開鍵が無ければ（S503でNO）、返答に含めない。これは非公開鍵が無い場合はCACertificateと判断できるからである。
- [0110] ステップS502において複数の証明書が取得できた場合はそれぞれの証明書を返答に含めるかの判定を行う（S505）。次の証明書がある場合には、ステップS503以降の処理を繰り返す。全てのCertificateの判定が終われば（S505

でN0の場合)、クライアント装置200に返答を送信する(S506)。

[0111] DMサービス部112においてGetCACertificatesコマンドを処理する場合、CACertificateは非公開鍵を持っていないはずなので、図5のステップS503でN0と判定した証明書をレスポンスに返せばよい。

[0112] 図6はDMサービス部112における、証明書の削除の処理を示したフローチャートである。DMサービスのセキュリティ関係のコマンドは証明書パス(CertificationPath)や鍵ペア(Keypair)の概念がない。本実施形態では、DMサービスに基づくDeleteCertificatesコマンドで証明書を削除する場合に、一緒にAMサービスに基づく証明書パスと鍵ペアも削除する。

[0113] DeleteCertificatesコマンドは、DMサービスに基づいて行われる命令であって、記録部104に記録された証明書情報を削除することを要求する命令である。本実施形態では証明書の削除処理について説明するが、証明書を無効にすればよく、古い証明書を新たな証明書で上書きすることにより、古い証明書を無効にすることとしてもよい。

[0114] DMサービス部112がDeleteCertificatesコマンドを受信すると(S601)、Keystore部114から鍵ペアと証明書と証明書パスを取得する(S602)。

[0115] 次に、DeleteCertificatesコマンドで指定されたCertificateIDが含まれた証明書パスが有るかを判定する(S603)。無い場合は(S603でN0の場合)、CertificateIDで指定された証明書について証明書パスを削除する必要がない。Keystore部114のCertificate部116に同じCertificateIDの証明書が有るかを判定する(S604)。無い場合は指定された証明書が無い場合、ASサービス部113はクライアント装置200への返答としてエラーを送信する(S611)。有る場合は指定されたCertificateIDのCertificateを削除する(S607)。

[0116] ステップS603で指定されたCertificateIDが含まれた証明書パスがあると判定した場合(S603でYES)、その証明書パスがSSLなどに使用されているかを判定する。使用している場合(S605でYES)は証明書を削除できないため、ASサービス部113はクライアント装置200への返答としてエラーを送信する(S611)。

- [0117] 証明書パスが使用されていない場合（S605でN0）、証明書パスを削除し（S606）、CertificateIDで指定された証明書を削除する（S607）。次に証明書に関連付けられた鍵ペアを削除する。DMサービスのセキュリティ関連コマンドには鍵ペアを削除するものは無いため、DeleteCertificatesコマンドで削除する必要がある。
- [0118] しかし鍵ペアは他の証明書に関連付けられているかもしれないので、ステップS610で判定する。他の証明書に鍵ペアが関連付けられていなければ（S608でYES）、削除の対象となる証明書に関連付けられた鍵ペアを削除する（S609）。他の証明書に鍵ペアが関連付けられていれば（S608でN0）は削除しない。DeleteCertificatesコマンドは複数のCertificateIDを指定できるため、次のCertificateIDがあれば（S610でYES）、そのCertificateIDの削除処理をする（S603に戻る）。全てのCertificateIDを処理し終わると（S610でN0）、DMサービス部112はクライアント装置200への返答に成功を送信する。
- [0119] このようにして、DMサービス部112は、DeleteCertificatesコマンド（第1の命令）によって指定された証明書情報に対応する鍵ペア情報を記録部104から削除する。またDMサービス部112は、DeleteCertificatesコマンドによって指定された証明書に対応する証明書パス情報を記録部104から削除する。上述のように、証明書を無効にすればよく、証明書を上書きしたり、証明書に無効の情報を付加したりすることにより証明書を無効としてもよい。
- [0120] つぎに、証明書のステータスを設定する処理について説明する。SetCertificatesStatusコマンドはDMサービスに基づいて行う命令であって、証明書をSSLなどのHTTPS通信を行うために用いる証明書を指定する命令である。以下の実施形態ではSSLを用いた暗号化通信を行う例について説明する。本実施形態では、証明書の状態情報（Status）を有効（enable）にすることにより、その証明書をSSLに用いることを設定でき、Statusを無効（disable）にすることによりその証明書はSSLに用いないことを設定することができる。
- [0121] しかしDMサービスにおいて、Statusを変更できる証明書は1つのみで、DMサービスにはASサービスの証明書パスの概念がないため、多段の証明書を指定

できない。そこで、本実施形態では、SetCertificatesStatusコマンドでCertificateIDを指定された場合は以下の2つの処理を行うことができる。

- [0122] 第1にSetCertificatesStatusコマンドによって指定された証明書の識別情報が、証明書パスが示す証明書の順序における先頭の証明書の識別情報と一致する場合、その証明書パスをSSLの設定に使用する。証明書の識別情報は、ONVIFにおいてCertificateIDとして表現される。
- [0123] 第2にSetCertificatesStatusコマンドによって指定された証明書の識別情報と一致する証明書の識別情報を証明書の順序における先頭とする証明書パスが記録部104に記録されていない場合の処理である。この場合、SetCertificatesStatusコマンドによって指定されたCertificateIDの証明書を使用した1段の証明書パスを生成し、SSLに用いる証明書パスとして記録部104に記録させて設定する。以降でそれぞれの実施方法について詳細を説明する。
- [0124] 次にDMサービス部112における、SetCertificatesStatusコマンドの実行処理について図7を用いて説明する。図7に示した処理では、証明書パスの先頭のCertificateIDに一致したものがあればその証明書パスをSSLの設定に使用する処理を示したフローチャートである。DMサービス部112がSetCertificatesStatusを受信すると（S701）、Keystore部114から鍵ペアと証明書と証明書パスを取得する（S702）。次に、CertificatePath部117から、最初のCertificateIDが指定されたCertificateIDと一致するものを検索する（S703）。一致するものが無ければ（S703でN0）、DMサービス部112はクライアント装置200へエラーを送信する（S704）。一致するものがあれば（S703でYES）、StatusがTrueの場合はその証明書パスをSSLに使用するように設定し、Falseの場合はSSLに使用しないように設定する（S705）。SetCertificatesStatusコマンドは複数のCertificateIDを指定することができるため、次のCertificateIDがあれば（S706でYES）、ステップS703に戻り処理を繰り返す。全てのCertificateIDの処理が終われば（S706でN0）、DMサービス部112はクライアント装置200への返答で成功を送信する。
- [0125] このようにして、予めクライアント装置300が複数のCertificateIDを含ん

だ証明書パスを設定していた場合、クライアント装置200でも複数のCertificateIDを含んだ証明書パスをSSLとして設定できる。

[0126] 次に、撮像装置100がクライアント装置200からGetCertificatesStatusコマンドを受信した場合の、DMサービス部112における処理について図8を用いて説明する。GetCertificatesStatusコマンドは、DMサービスに基づいて行う命令である。GetCertificatesStatusコマンドは、記録部104が記録している証明書の状態（例えば、暗号化した通信に用いることが設定された証明書であるか否か）を示す情報の送信を要求するための命令である。

[0127] 図8の例はSetCertificatesStatusコマンドによって指定されたCertificateIDに対応する証明書を先頭とする証明書パスが、SSLの設定に使用する証明書パスとして記録部104に記録されている場合について説明する。

[0128] DMサービスによって提供されるGetCertificatesStatusコマンドは証明書単体についてそのStatusを返すため、ASサービスの証明書パスを表わすことができない。ASサービスに基づく証明書パス情報には複数の証明書の識別情報（CertificateID）が示される。そこで、DMサービスによるGetCertificatesStatusコマンドを受信した場合に、それら複数の証明書のうち何れの証明書についてのStatusを応答すべきかが問題となる。そこで本実施例では、証明書パスが示す複数の証明書のうち、暗号化された通信を行うために撮像装置100が参照する順序において先頭であることを示す証明書についての情報（例えば、Status情報）を応答として送信する。

[0129] DMサービス部112がGetCertificatesStatusコマンドを受信すると（S801）、Keystore部114から証明書と証明書パスを取得する（S802）。Keystore部114の証明書のCertificateIDの中で、証明書パスの先頭のCertificateIDが一致するものが無ければ（S803でN0）、SSLの設定には使えない。そこで、GetCertificatesStatusコマンドの返答に含めずステップS807へ進む。有る場合はその証明書パスがSSLに使われているかどうかを判定する（S804）。使われている場合は（S804でYES）返答にそのCertificateIDと、StatusにTrueを設定したものを追加する。使われていない場合は（S804でN0）返答にそのCertifica

teIDと、StatusにFalseを設定したものを追加する。そして、その他に証明書があればその返答処理のためステップS803に戻る（S807でYES）。全ての証明書の処理が終わると（S807でNO）、ASサービス部113はクライアント装置200に対して返答を送信する（S808）。

[0130] 図9はDMサービス部112における、SetCertificatesStatusコマンドの処理を示したフローチャートである。図9に示した処理では、証明書パスの先頭のCertificateIDに一致したものがあればその証明書パスをSSLの設定に使用する。一方、証明書パスの設定が無い場合は指定されたCertificateIDの証明書を使用した1段の証明書パスを生成し、それをSSLの設定に使用する。

[0131] DMサービス部112がSetCertificatesStatusコマンドを受信すると（S901）、Keystore部114から鍵ペアと証明書と証明書パスを取得する（S902）。

[0132] 次に、指定されたCertificateIDが、証明書パスの先頭のCertificateIDに一致するものが有るかを判定する（S903）。有る場合は（S903でYES）、指定されたStatusの値に応じてTrueなら証明書パスをSSLに使うように設定し、FalseならSSLに使わないように設定する。

[0133] ステップS903で指定されたCertificateIDと一致した証明書パスが無いと判定された場合（S903でNO）、Keystore部114の証明書に指定されたCertificateIDの証明書があるかを判定する（S904）。無い場合は返答にエラーを送信する（S905）。

[0134] 一致するものがある場合、そのCertificateIDで1段の証明書パスを生成し（S906）、指定されたStatusを反映する（S907）。SetCertificatesStatusコマンドは複数のCertificateIDを指定できるため、次のCertificateIDがあれば（S908でYES）ステップS903に戻り、次のCertificateIDの処理を続ける。全てのCertificateIDの処理が終われば（S908でNO）、DMサービス部112はクライアント装置200に対する返答として成功を送信する。

[0135] 本実施形態に係るDMサービス部112は、SetCertificatesStatusコマンドによって、証明書パスの先頭でないCertificateIDを指定されても証明書パスを生成するために、以下の処理を行う。すなわち、GetCertificatesStatusコマ

ンドに対して、証明書パスの先頭に無いCertificateIDも返答する。

[0136] 次に、DMサービス部112における、GetCertificatesStatusコマンドに対する処理について図10を用いて説明する。図10の例では、図9に示した処理に応じて、証明書及び証明書パスが設定されている場合について説明する。

[0137] DMサービス部112がGetCertificatesStatusコマンドを受信すると（S1001）、Keystore部114から証明書パスと証明書と鍵ペアを取得する（S1001）。次に、GetCertificatesStatus コマンドによって指定されたCertificateIDが証明書パスが示す順序の先頭のCertificateIDと一致する証明書を検索する。一致する証明書が有る場合は（S1003でYESの場合）、その証明書パスがSSLに使われているかどうかを判定する（S1004）。

[0138] 使われている場合（S1004でYESの場合）はそのCertificateIDを返答に追加し、そのStatusはTrueに設定する（S1005）。使われていない場合（S1004でN0）は、CertificateIDを返答に追加し、そのStatusはFalseに設定する（S1007）。

[0139] このようにして、DMサービス部112は、記録部104に記録された証明書情報が暗号化された通信を行うために用いる証明書情報として設定されているかを示す情報の取得を要求する第3の命令を処理する。そして、第3の命令に応じて、証明書パス情報が前記順序の先頭であることを示す第4の証明書情報が、暗号化された通信を行うために用いる証明書情報として設定されていることを示す情報（例えば、StatusがTrue）を記録部104に記録させる。またDMサービス部112は、第4の証明書情報と異なる第5の証明書情報が、暗号化された通信を行うために用いることが設定されていないことを示す情報（例えば、StatusがFalse）を記録部104に記録させる。

[0140] 次に、CertificatePath部117にはCertificateIDが含まれない場合（S1003でN0）、自己署名証明書として使用可能な証明書の返答を生成する。自己署名証明書として使用可能な証明書は、その証明書に関連付けられる鍵ペアに非公開鍵が設定されたものである。Keypair部115に非公開鍵が有る場合（S1006でYES）、その証明書のCertificateIDを返答に追加し、そのStatusはFalse

に設定する。Keypair部115に非公開鍵が無い場合は（S1006でN0）、そのCertificateIDを返答に含めない。

[0141] このようにして、DMサービス部112がGetCertificatesStatus（第3の命令）を実行した場合、証明書パスが示す複数の証明書のうち、鍵ペア情報に関連付けられていない証明書情報を送信しないようにすることができる。

[0142] SetCertificatesStatusコマンドは複数のCertificateIDを指定できるため、次のCertificateIDがあれば（S1008でYES）ステップS1003に戻り、次のCertificateIDの処理を続ける。全てのCertificateIDの処理が終われば（S1008でN0）、DMサービス部112はクライアント装置200に返答を送信する。

[0143] LoadCertificatesWithPrivatekeyコマンドは、証明書と非公開鍵とそれに付随する公開鍵を撮像装置100にロードするコマンドである。このコマンドをDMサービス部112が受信すると、証明書と非公開鍵からそれぞれ公開鍵を取得し、一致しなければエラー処理とする。一致した場合、非公開鍵と公開鍵とユニークなKeyIDをKeystore部114に保存し、そのAliasはDMサービスのコマンドで設定されたことを示す情報を設定する。さらに、証明書とCertificateIDをKeystore部114のCertificate部116に保存し、そのAliasにはDMサービスのコマンドで設定されたことを示す情報を記述する。

[0144] このように、DMサービス部112でセキュリティ関係のコマンドを処理する場合、DMのセキュリティ関連コマンドでは、鍵ペアや証明書パスの設定を行うことができない。そこで本実施形態では、Keystore部114に鍵ペアと証明書と証明書パスに相当する設定を記録する。このようにしてDMのセキュリティ関連コマンドを用いるクライアント装置200とASサービスのコマンドで設定を行うクライアント装置300との間で設定状況を共有できる。

[0145] また、Keystore部114に鍵ペアと証明書と証明書パスを保存する際に、それぞれのAliasにDMサービスに基づいて設定したことを示す情報を記録する。そして通信部105はDMサービスに基づいて行う命令に応じて撮像装置100に対して設定がなされたことを示す情報を、ASサービスに基づいて行う命令（設定を参照するための命令）に応じて送信することができる。このようにして、

クライアント装置200で設定したセキュリティ関係の設定であっても、クライアント装置300で知ることができる。

- [0146] 以上、本発明の第1の実施形態について説明したが、本発明この実施形態に限定されず、その要旨の範囲内で種々の変形及び変更が可能である。通信部105はASサービスに基づいて行う命令に応じて撮像装置100に対して設定がなされたことを示す情報を記録し、その情報をDMサービスに基づいて行う命令（設定を参照するための命令）に応じて送信してもよい。このようにして、クライアント装置300で設定したセキュリティ関係の設定であっても、クライアント装置200で知ることができる。

- [0147] （実施形態2）

以下、図11から15を参照して、本発明の第2の実施形態による、セキュリティ機能の設定機能を備えた撮像装置について説明する。

- [0148] 本実施形態にかかる撮像装置100は、ONVIFの通信手順以外の手段でも撮像装置100に対する設定を可能とする。本実施形態において、情報処理装置としての撮像装置100は、クライアント装置1100が撮像装置100を設定するためのWEBページを起動する。ユーザはクライアント装置1100においてWEBブラウザを通してカメラにアクセスし、設定を変更することができる。
- [0149] また、例えばSSLの設定であると、撮像装置100はSSLの設定用のWEBページを用意しておき、そこで証明書の設定やSSLサービスの開始・終了の制御を行う。以降、設定用のWEBページを設定ページと呼ぶ。
- [0150] 本実施形態では、設定ページで設定したセキュリティ関係の機能は、ONVIFのDMサービスのセキュリティに関するコマンドや、ASサービスのセキュリティコマンドでも参照できるようにする撮像装置100について説明する。すなわち、設定ページを用いてクライアント装置1100が撮像装置100に対して行った設定の内容を、実施形態1のクライアント装置200や300においても確認できるようにする。
- [0151] ONVIFでは非公開鍵や公開鍵、証明書を設定するコマンド群と、それをSSLやIEEE802.1Xに使うように設定するコマンド群、さらにサービスの開始・終

了を設定するコマンドが規定されている。

[0152] 例えば、証明書を作成またはロードするとCertificateIDが得られるが、その時点でその証明書の用途は決定されない。証明書の用途を決定するのは、SSLに使用する場合、DMサービスにおいて用いられるセキュリティ関係コマンドであればSetCertificatesStatusコマンドである。また、ASサービスにおいて用いられるコマンドであればAdd/ReplaceServerCertificateAssignmentコマンドである。

[0153] ONVIFのセキュリティの設定関係のコマンドに合わせた設定ページを用意する場合、証明書の設定と、その証明書をSSLなどのサービスに適用するページを分けることが想定される。この場合、証明書の設定をし、別のページでその証明書を指定することになる。しかし、SSLの設定ページで証明書の設定とサービスの開始及び停止を完了することにより、ユーザが操作しやすい設定ページとすることができる。

[0154] また、Keystore部114では複数の証明書を設定できるのが一般的であるが、SSLの設定ページの場合は通常はSSLサーバ用の証明書を1つ、もしくはそれに加えて中間層の証明書を1組設定できれば十分である。

[0155] 本実施形態では、設定ページを用いた設定を可能とする撮像装置100にSSL設定をする例について説明する。特に、Keystore部114のAliasを使い、設定ページと、DMサービスのセキュリティ関係コマンドと、ASサービスのコマンドの設定を相互に反映する方法について説明する。

[0156] 本実施形態に係る撮像装置100の制御部103は、DMサービス部112、ASサービス部113の機能に加え、後述の設定ページ制御部118の機能を実行する。例えば第1の処理部106が設定ページ制御部118の機能を実行することができる。その他の構成については図2Aを用いて説明した内容と同様であるため説明を省略する。図11は撮像装置100と撮像装置100に対して設定ページを用いてセキュリティの設定を行うクライアント装置1100を示した図である。

[0157] また、本実施形態にかかる撮像装置100の機能構成について図11を用いて説明する。本実施形態にかかる撮像装置100は、実施形態1と同様にHTTPサーバ

部111、DMサービス部112、ASサービス部113、Keystore部114を有する。本実施形態2にかかる撮像装置100は、設定ページ制御部118からKeystore部114を操作可能とする点で、実施形態1に示した構成と異なる。

[0158] 設定ページ部118は、設定ページを用いるクライアント装置1100（第1の受信装置）が撮像装置100に対してHTTP（第1の通信手順）に基づいて行う命令を実行する。HTTPに基づいて行う命令には、暗号化された通信を行うために用いる公開鍵（第1の公開鍵情報）と暗号化された通信を行うために用いる非公開鍵（第1の非公開鍵情報）とが対応することを示す第1の鍵ペア情報を記録部104に記録させる命令が含まれる。またHTTPに基づいて行う命令には、公開鍵と非公開鍵との対応関係を示す鍵ペア情報（第1の鍵ペア情報）を通信部105から送信させる命令が含まれる。またHTTPに基づいて行う命令には、記録部104に記録された鍵ペア情報を無効にする（例えば、削除する）命令が含まれる。さらにHTTPに基づいて行う命令には、公開鍵情報が正当な鍵情報であることを証明するための証明書情報であって設定ページ制御部118により署名情報が付加された自己署名証明書を生成させる命令が含まれる。設定ページ制御部118はこれらの全ての命令を必ずしも実行しなくてもよく、少なくともいずれか一つの命令を実行すればよい。

[0159] 本実施形態にかかる撮像装置100は、クライアント装置1100からSSLの設定ページの要求があると、図12に示すような設定ページを返答する。

[0160] ラジオボタン（1201、1202、1203）はそれぞれ、SSLを無効の状態にするか、自己署名証明書を使用するか、CAが署名した証明書を使用するかを選択するための表示である。

[0161] サブジェクト1204は自己署名証明書に使うサブジェクトを設定するための入力欄である。入力した内容は自己署名書のSubjectとIssuerに設定される。例えばサブジェクト1204に「CN=example.com」と設定すると、CommonNameに「example.com」が設定される。

[0162] また、入力欄1205と入力欄1206は、自己署名証明書の有効期間の開始日と終了日を設定するための入力欄である。サブジェクト1204と入力欄1205と入

力欄1206を設定した後、生成ボタン1207を押すと、自己署名証明書が生成される。表示ボタン1208は生成した自己署名証明書を別ウィンドウにポップアップして表示させるためのボタンである。削除ボタン1209は自己署名証明書を削除するためのボタンである。

[0163] サブジェクト1210は証明書署名要求のサブジェクトを設定するもので、設定方法はサブジェクト1204と同様である。生成ボタン1211はサブジェクト1210に設定されたサブジェクトに従い証明書署名要求を生成し、表示ボタン1212は証明書署名要求を別ウィンドウにポップアップして表示する。

[0164] インストールボタン1213は、証明書署名要求を元にCAが署名した証明書をインストールすることを指示するボタンである。クライアント装置1100を実行している機器のファイルシステムを参照して証明書ファイルを選択する。表示ボタン1214は別ウィンドウに証明書を表示させることを指示するためのボタンである。削除ボタン1215は証明書を削除することを指示するためのボタンである。

[0165] インストールボタン1216は、CAが提供するCA証明書（中間層の証明書またはクロスルート証明書）をインストールすることを指示するためのボタンである。インストールボタン1216を選択すると、クライアント装置1100を実行している機器のファイルシステムを参照して証明書ファイルを選択する。表示ボタン1217は別ウィンドウに証明書を表示させるためのボタンである。削除ボタン1218は証明書を削除するためのボタンである。適用ボタン1219は設定を反映するためのボタンである。キャンセルボタン1220は設定をキャンセルするためのボタンである。

[0166] ラジオボタン1202を選択し、サブジェクト1204と入力欄1205と入力欄1206を設定し、生成ボタン1207を押した場合の処理について、図13を用いて説明する。このように設定することにより、撮像装置100において、自己署名証明書を生成し、それをSSLに使うように設定される。撮像装置100は、設定の内容をKeystore部114に反映する。

[0167] 撮像装置100は、最初に公開鍵と非公開鍵を生成する（S1302）。暗号・署

名のアルゴリズムや鍵長を設定できるようにしても良いが、ここではsha-2WithRSAEncryption、2048ビットを固定の設定とする。公開鍵、非公開鍵、及び、自己署名証明書の作成は、制御部103が行うこととすることができる。図11の機能構成図ではHTTPサーバ部111において生成することができる。

[0168] 次に自己署名証明書を、設定された値に応じて生成する（S1302）。次に、DMのセキュリティ関係コマンドとASのコマンドで、設定ページで設定した証明書等が参照できるように、Keystore部114に保存する。

[0169] まず、公開鍵と非公開鍵に加えてユニークなKeyIDを生成し、Keystore部114のKeypairに保存する。さらに、そのAliasには設定ページの自己署名証明書で設定されたことを意味する情報を記録させる（S1303）。そして、自己署名証明書に加えてユニークなCertificateIDを生成してKeystore部114のCertificate部116に保存する。そしてそのAliasには設定ページの自己署名証明書で設定されたことを意味する情報を設定する（S1304）。

[0170] 次に、CertificateIDが1つだけ含まれた証明書パスとユニークなCertificationPathIDを生成し、Keystore部114のCertificationPath部117に保存する。そして、そのAliasには設定ページの自己署名証明書で設定されたことを意味する情報を設定する（S1303）。さらに、SSLの設定ページで生成した自己署名証明書なのでSSLに使われることが決まっているため、生成した証明書パスをSSLに使うように設定する（S1306）。

[0171] この時点で、クライアント装置300はGetAllKeysコマンドを用いて設定ページで生成した自己署名証明書の非公開鍵と公開鍵を参照できる。また、GetAllCertificatesコマンドを用いて自己署名証明書を参照できる。さらにGetCertificationPathコマンドを用いて自己署名証明書が1段で設定されていることが分かる。また、GetAssignedServerCertificatesコマンドを用いて証明書パスがSSLに使用されることが分かる。さらに、各Aliasには設定ページの自己署名証明書で生成したことを意味する情報が設定されているため、クライアント装置300で設定を参照または上書きなどする際には参考となる。

[0172] クライアント装置1100において、ユーザが表示ボタン1208を押した場合の

処理について説明する。Keystore部114のCertificate部116にはAliasに設定ページの自己署名証明書で設定されたことを意味する情報が設定されている。そこで、証明書の一覧を取得し、Aliasが一致する証明書を検索し、それをクライアント装置1100において表示させる。

[0173] 表示ボタン1208の操作に応じて、SSLの設定ページから自己署名証明書の設定がされていない場合、以下のようにすることができる。すなわち、CertificationPath部117に自己署名証明書を使うものが設定されていれば、クライアント装置200や300で設定した自己署名証明書を表示しても良い。その場合、CertificationPath部117でSSLに使われているものを検索する。存在すればCertificationPath部117に設定されているCertificateIDから証明書を参照し、それが自己署名証明書であればクライアント装置1100に表示させる。

[0174] 次に、ユーザが削除ボタン1209を押した場合の処理について説明する。Keystore部114のKeypair部115とCertificate部116とCertificationPath部117にはAliasに設定ページの自己署名証明書で設定されたことを意味する情報が設定されている。削除ボタン1209の選択に応じて、それらを削除する。まずは証明書パスをSSLに使用しないように設定する。そしてAliasに一致する証明書パスを削除し、同じく証明書と鍵ペアの順に削除する。

[0175] 削除ボタン1209は、SSLの設定ページから自己署名証明書の設定がされていなくても、CertificationPath部117で自己署名証明書を使うものが設定されていればよい。例えば、クライアント装置200や300で設定した自己署名証明書を削除しても良い。その場合、CertificationPath部117でSSLに使われているものを検索し、存在すればCertificationPath部117に設定されているCertificateIDから証明書を参照する。証明書が自己署名証明書であれば、証明書パスをSSLに使わないように設定し、証明書パス、証明書、鍵ペアの順に削除する。

[0176] 次にCAが署名した証明書を使用する場合の処理について説明する。サブジェクト1210にサブジェクトが設定され、生成ボタン1211が押された場合、最初に公開鍵と非公開鍵を生成する。そして、公開鍵と非公開鍵とユニークなK

eyIDをKeystore部114のKeypair部115に保存し、そのAliasにはCAが署名した証明書を使用する設定を意味する情報を設定する。さらにサブジェクト1210に設定された値を用いて証明書署名要求を生成する。

表示ボタン1212が押された場合、生成ボタン1211で生成した証明書署名要求をクライアント装置1100に別ウィンドウを生成して表示する。

[0177] 図14は、CAが署名した証明書を使用する場合において、インストールボタン1213とインストールボタン1216で証明書とCA証明書が設定された時の処理のフローチャートである。ここでは、インストールされた証明書が証明書署名要求を元に生成されたものか、またASのCertificationPathを正しく設定するために、証明書のIssuerとCA証明書のCommonNameの確認を行う。

[0178] まずKeystore部114のKeypair部115の中から、CAが署名した証明書を使用することを意味するAliasの鍵ペアを取得する（S1401）。次にインストールボタン1213でインストールされた証明書から公開鍵を取得する（S1402）。取得したKeypairのPublickeyと証明書の公開鍵を比較し、一致していなければ（S1403でN0）、公開鍵と非公開鍵の組み合わせが合わないためエラー処理を行う（S1412）。一致していれば（S1403でYES）、証明書のパスを確認するために証明書からIssuerを取得し（S1404）、CA証明書からはSubjectを取得する（S1405）。

[0179] そして取得したIssuerとSubjectを比較し、一致していなければ（S1406でN0）証明書のパスが合わないため、エラー処理を行う（S1402）。一致する場合（S1406でYES）はステップS1407へ進む。本実施形態ではCA証明書は1つの前提で扱っているが、複数ある場合には同様に証明書のパスを確認する必要がある。

[0180] 次に、インストールボタン1213で設定した証明書をKeystore部114のCertificateに設定する。証明書とユニークなCertificateIDとステップS1401で取得したKeypairのKeyIDをKeystore部114のCertificateに保存する。そして、そのAliasにはCA証明書が署名した証明書を使用することを意味する情報を設定する（S1407）。

- [0181] 次に、インストールボタン1216で設定されたCA証明書をKeystore部114のKeypair部115とCertificate部116に設定する。CA証明書の公開鍵とユニークなKeyIDをKeystore部114のKeypair部115に保存し、そのAliasにはCA証明書が署名した証明書を使用することを意味する情報を設定する（S1408）。さらに、CA証明書とユニークなCertificateIDとステップS1408で設定したKeyIDを関連付けてKeystore部114のCertificateに保存する。そして、そのAliasにはCA証明書が署名した証明書を使用することを意味する情報を設定する（S1409）。
- [0182] 次に、ステップS1407で設定した証明書のCertificateIDを先頭とし、次にCA証明書のCertificateIDを設定した証明書パスをKeystore部114のCertificationPath部117に保存する。そしてそのAliasにはCA証明書が署名した証明書を使用することを意味する情報を設定する（S1410）。最後に、生成したCertificationPathをSSLで使用するよう設定する（S1411）。
- [0183] 表示ボタン1214が押された場合、Keystore部114のCertificate部116に記録された情報の一覧を取得し、AliasがCA証明書が署名した証明書を使用することを意味する情報のものを検索する。次に、各Certificateに関連付けられているKeyIDにPrivatekeyが存在するかを調べ、存在すれば表示する。
- [0184] 表示ボタン1217が押された場合、Keystore部114のCertificateの一覧を取得し、AliasがCA証明書が署名した証明書を使用することを意味する情報のものを検索する。次に、各Certificateに関連付けられているKeyIDにPrivatekeyが存在するかを調べ、存在しなければ表示する。
- [0185] 削除ボタン1215が押された場合、Keystore部114からAliasがCA証明書が署名した証明書を使用することを意味する情報をもった証明書パスを検索する。存在すればSSLに使用しないように設定し、さらに証明書パスを削除する。次に、AliasがCA証明書が署名した証明書を使用することを意味する情報のものを検索し、証明書に関連付けられているKeyIDに非公開鍵があれば削除する。
- [0186] 削除ボタン1218が押された場合、AliasにCA証明書が署名した証明書を使用することを意味する情報が記録されている証明書パスをKeystore部114におい

て検索する。存在すればSSLに使用しないように設定し、さらに証明書パス削除する。次に、AliasがCA証明書が署名した証明書を使用することを意味する情報のものを検索し、証明書に関連付けられているKeyIDに非公開鍵が無ければ削除する。

[0187] 適用ボタン1219はラジオボタン（1201、1202、1203）選択肢に従い、SSLサービスを開始または停止する処理を行う。また、キャンセルボタン1220が押された場合は設定途中のサブジェクトや証明書の設定をキャンセルする。

[0188] ここではCAが署名した証明書を使用する設定の場合、証明書とCA証明書は同じAliasを設定したが、異なるものを用いても良い。証明書やCA証明書の削除、それに伴う証明書パスと証明書と鍵ペアの削除にはAliasを用いて検索しても良い。

[0189] このように、設定ページからSSLの設定がされた場合でもKeystore部114に鍵ペアと証明書と証明書パスを設定することで、ASサービスのコマンドでも設定を参照できるようになる。また、実施形態1で示したDMサービスのセキュリティ関連のコマンドの処理を行うことで、DMのセキュリティ関連のコマンドでも設定ページで設定したSSLの設定を参照できるようになる。

[0190] このようにして、通信部105は、設定ページを用いたHTTPに基づいて行う命令に応じて撮像装置100に対して設定がなされたことを示す情報を、ASサービスに基づいて行う命令（設定を参照するための命令）に応じて送信することができる。また、通信部105は、設定ページを用いたHTTPに基づいて行う命令に応じて撮像装置100に対して設定がなされたことを示す情報を、DMサービスに基づいて行う命令（設定を参照するための命令）に応じて送信することができる。

[0191] 本実施形態ではSSLの設定に関して記載したが、その他の証明書を扱う機能においてもAliasを設定することで設定を反映することができる。

[0192] 以上、本発明の第2の実施形態について説明したが、本発明はこれらの実施形態に限定されず、その要旨の範囲内で種々の変形及び変更が可能である。

[0193] (その他の実施形態)

本発明は、上述の実施形態の1以上の機能を実現するプログラムを、ネットワーク又は記録媒体を介してシステム又は装置に供給し、そのシステム又は装置のコンピュータにおける1つ以上のプロセッサがプログラムを読み出し実行する処理でも実現可能である。また、1以上の機能を実現する回路（例えば、ASIC）によっても実現可能である。

[0194] 本発明は上記実施の形態に制限されるものではなく、本発明の精神及び範囲から離脱することなく、様々な変更及び変形が可能である。従って、本発明の範囲を公にするために以下の請求項を添付する。

符号の説明

- [0195] 100 撮像装置
103 制御部
104 記録部
105 通信部
106 第1処理部
107 第2処理部
200 第1のクライアント装置
300 第2のクライアント装置

請求の範囲

[請求項1]

情報処理装置であって、

第1の通信手順に基づいて行う命令に応じて、暗号化された通信を行うための設定を前記情報処理装置に対して行う第1の処理手段と、

第2の通信手順に基づいて行う命令に応じて、暗号化された通信を行うための設定を前記情報処理装置に対して行う第2の処理手段と、

前記情報処理装置に対して暗号化された通信を行うための設定を前記第1の通信手順に基づいて行う命令に応じて前記第1の処理手段が行った後に受信装置から前記第2の通信手順に基づいて行う命令を受信した場合、暗号化された通信を行うための設定が前記第1の通信手順に基づいて行う命令に応じて行われたことを示す情報を前記受信装置に送信する送信手段と

を有することを特徴とする情報処理装置。

[請求項2]

前記第1の通信手順に基づいて行う命令によって前記情報処理装置に対して設定がなされたことを示す情報を記録手段に記録させる制御を行う制御手段を有することを特徴とする請求項1に記載の情報処理装置。

[請求項3]

前記第1の処理手段は、暗号化された通信を行うために用いる第1の公開鍵情報、前記第1の公開鍵情報に対応し暗号化された通信を行うために用いる第1の非公開鍵情報、又は、前記公開鍵情報が正当な鍵情報であることを証明するための第1の証明書情報の少なくともいずれか一つを前記情報処理装置に設定するための命令であって、第1の受信装置が前記情報処理装置に対して前記第1の通信手順に基づいて行う命令を実行し、

前記第2の処理手段は、暗号化された通信を行うために用いる第2の公開鍵情報と暗号化された通信を行うために用いる第2の非公開鍵情報とが対応することを示す鍵ペア情報、前記第2の公開鍵情報が正当な鍵情報であることを証明するための第2の証明書情報、又は、前

記第2の証明書情報に関連する第3の証明書情報を示す証明書パス情報のうち少なくともいずれか一つを前記情報処理装置に設定するための命令であって、第2の受信装置が前記情報処理装置に対して前記第2の通信手順に基づいて行う命令を実行することを特徴とする請求項2に記載の情報処理装置。

[請求項4]

前記第1の処理手段は、暗号化された通信を行うために用いる第1の公開鍵情報と暗号化された通信を行うために用いる第1の非公開鍵情報とが対応することを示す第1の鍵ペア情報を前記記録手段に記録させる命令、前記第1の鍵ペア情報を前記送信手段から送信させる命令、前記記録手段に記録された前記第1の鍵ペア情報を無効にする命令、又は、前記第1の公開鍵情報が正当な鍵情報であることを証明するための証明書情報であって前記第1の処理手段により署名情報が付加された証明書情報を生成させる命令の少なくともいずれか一つの命令であって、第1の受信装置が前記情報処理装置に対して前記第1の通信手順に基づいて行う命令を実行し、

前記第2の処理手段は、暗号化された通信を行うために用いる第2の公開鍵情報と暗号化された通信を行うために用いる第2の非公開鍵情報とが対応することを示す鍵ペア情報、前記第2の公開鍵情報が正当な鍵情報であることを証明するための第2の証明書情報、又は、前記第2の証明書情報に関連する第3の証明書情報を示す証明書パス情報のうち少なくともいずれか一つを前記記録手段に記録させるための命令であって、第2の受信装置が前記情報処理装置に対して前記第2の通信手順に基づいて行う命令を実行し、

前記送信手段は、前記第1の通信手順に基づいて行う命令に応じて前記情報処理装置に対して設定がなされたことを示す情報を、前記第2の通信手順に基づいて行う命令に応じて送信することを特徴とする請求項2に記載の情報処理装置。

[請求項5]

前記第1の処理手段は、前記第1の通信手順に基づいて行う命令で

あって前記第 1 の証明書情報の生成を指示する命令に応じて、前記公開鍵情報が正当な鍵情報であることを証明するための証明書情報であって前記第 1 の処理手段により署名情報が付加された証明書情報と、前記鍵ペア情報と、前記証明書パス情報とを生成して前記記録手段に記録させ、

前記制御手段は、前記第 1 の通信手順に基づいて行った命令に応じて、前記証明書情報と、前記鍵ペア情報と、前記証明書パス情報とを生成したことを示す情報を前記記録手段に記録させる制御を行うことを特徴とする請求項 3 に記載の情報処理装置。

[請求項 6] 前記第 1 の処理手段は、前記第 1 の通信手順に基づいて行う命令であって前記記録手段に記録された証明書情報を無効にすることを要求する第 1 の命令を実行し、前記第 1 の命令によって指定された証明書情報に対応する前記鍵ペア情報、又は、前記第 1 の命令によって指定された証明書情報に対応する前記証明書パス情報を無効にすることを特徴とする請求項 3 に記載の情報処理装置。

[請求項 7] 前記証明書パス情報は、暗号化された通信を行うために前記情報処理装置が前記記録手段に記録された複数の証明書情報を参照する順序を示す情報であり、

前記第 1 の処理手段は、暗号化された通信を行うために用いる証明書情報を指定する命令であって前記第 1 の通信手順に基づいて行う第 2 の命令に応じて、前記第 2 の命令によって指定された識別情報に対応する証明書情報が前記順序における先頭であることを示す前記証明書パス情報を、前記暗号化された通信を行うために用いる証明書パス情報として前記記録手段に記録させることを特徴とする請求項 3 に記載の情報処理装置。

[請求項 8] 前記証明書パス情報は、暗号化された通信を行うために前記情報処理装置が前記記録手段に記録された複数の証明書情報を参照する順序を示す情報であり、

前記送信手段は、前記第1の通信手順に基づいて行う命令であって前記記録手段に記録された証明書情報についての情報の送信を要求する命令に応じて、前記記録手段に記録された複数の証明書情報のうち前記証明書パス情報が前記順序における先頭であることを示す証明書情報を示す情報を送信することを特徴とする請求項3に記載の情報処理装置。

[請求項9]

前記証明書パス情報は、暗号化された通信を行うために前記情報処理装置が前記記録手段に記録された複数の証明書情報を参照する順序を示す情報であり、

前記第1の処理手段は、前記記録手段に記録された証明書情報が暗号化された通信を行うために用いる証明書情報として設定されているかを示す情報の取得を要求する第3の命令に応じて、前記複数の証明書情報のうち前記証明書パス情報が前記順序の先頭であることを示す第4の証明書情報が暗号化された通信を行うために用いる証明書情報として設定されていることを示す情報を前記記録手段に記録させ、前記複数の証明書情報のうち前記第4の証明書情報と異なる第5の証明書情報が暗号化された通信を行うために用いることが設定されていないことを示す情報を前記記録手段に記録させることを特徴とする請求項3に記載の情報処理装置。

[請求項10]

前記送信手段は、前記第1の処理手段が前記第3の命令を実行した場合、前記複数の証明書情報のうち、前記鍵ペア情報に関連付けられていない証明書情報を送信しないことを特徴とする請求項9に記載の情報処理装置。

[請求項11]

前記第1の通信手順は、ONVIFにより規定されるDeviceManagementサービスが提供する通信手順であり、前記第2の通信手順はONVIFにより規定されるAdvancedSecurityサービスが提供する通信手順であり、

前記制御手段は、前記第2の通信手順に基づくKeystore情報及びAl

ias情報を前記記録手段に記録させ、前記第1の通信手順に基づいて行う命令によって前記情報処理装置に対して設定がなされたことを示す情報を、前記Alias情報として前記記録手段に記録させることを特徴とする請求項3に記載の情報処理装置。

[請求項12] 前記第1の処理手段は、前記第1の通信手順に基づく命令であって前記第1の証明書情報を前記情報処理装置にロードするための命令であるLoadCertificatesコマンド、LoadCACertificatesコマンド、LoadCertificateWithPrivateKeyコマンド、又は、LoadCertificateWithPrivateKeyコマンドのうち少なくとも一つの命令を実行し、

前記制御手段は、前記第1の通信手順によって前記LoadCertificatesコマンド、前記LoadCACertificatesコマンド、前記LoadCertificateWithPrivateKeyコマンド、又は、前記LoadCertificateWithPrivateKeyコマンドのうち少なくとも一つの命令を前記第1の処理手段が実行した場合、前記第1の通信手順によって証明書のロードが行われたことを示す情報を前記Alias情報として前記記録手段に記録させることを特徴とする請求項11に記載の情報処理装置。

[請求項13] 前記制御手段は、前記鍵ペア情報に前記第2の証明書情報を関連付けて前記記録手段に記録させ、

前記第1の処理手段は、前記第1の通信手順に基づく命令であって証明書情報の送信を前記情報処理装置に要求する命令であるGetCertificatesコマンド、及び、前記第1の通信手順によって提供される命令であって認証局により発行された証明書情報の送信を前記情報処理装置に要求する命令であるGetCACertificatesコマンドを実行し、

前記送信手段は、前記第1の処理手段が前記GetCertificatesコマンドの実行した場合には前記鍵ペア情報に関連付けられている前記第2の証明書情報を送信し、前記第1の処理手段が前記GetCACertificatesコマンドを実行する場合には前記鍵ペア情報に関連付けられていない第3の証明書情報を送信することを特徴とする請求項11に記載

の情報処理装置。

[請求項14] 前記第1の処理手段は、前記第1の通信手順に基づく命令であって前記記録手段に記録された証明書情報の削除を要求する命令であるDeleteCertificatesコマンドを実行し、前記DeleteCertificatesコマンドによって指定された証明書情報に対応する前記鍵ペア情報、又は、前記DeleteCertificatesコマンドによって指定された証明書情報に対応する前記証明書パス情報を前記記録手段から削除することを特徴とする請求項11に記載の情報処理装置。

[請求項15] 撮像手段を有し、
前記送信手段は、前記撮像手段が撮像した撮像画像を、前記記録手段に記録された情報に基づいて暗号化された通信によって送信することを特徴とする請求項2に記載の情報処理装置。

[請求項16] 情報処理装置の制御方法であって、
第1の通信手順に基づいて行う命令に応じて、暗号化された通信を行うための設定を前記情報処理装置に対して行う第1の処理ステップと、
第2の通信手順に基づいて行う命令に応じて、暗号化された通信を行うための設定を前記情報処理装置に対して行う第2の処理ステップと、
前記情報処理装置に対して暗号化された通信を行うための設定を前記第1の通信手順に基づいて行う命令に応じて前記第1の処理ステップにおいて行った後に受信装置から前記第2の通信手順に基づいて行う命令を受信した場合、暗号化された通信を行うための設定が前記第1の通信手順に基づいて行う命令に応じて行われたことを示す情報を前記受信装置に送信する送信ステップと
を有することを特徴とする制御方法。

[請求項17] 前記第1の通信手順に基づいて行う命令によって前記情報処理装置に対して設定がなされたことを示す情報を記録手段に記録させる制御

を行う制御ステップを有することを特徴とする請求項 16 に記載の制御方法。

[請求項18]

前記第 1 の処理ステップにおいて、暗号化された通信を行うために用いる第 1 の公開鍵情報、前記第 1 の公開鍵情報に対応し暗号化された通信を行うために用いる第 1 の非公開鍵情報、又は、前記公開鍵情報が正当な鍵情報であることを証明するための第 1 の証明書情報の少なくともいずれか一つを前記情報処理装置に設定するための命令であって、第 1 の受信装置が前記情報処理装置に対して前記第 1 の通信手順に基づいて行う命令を実行し、

前記第 2 の処理ステップにおいて、暗号化された通信を行うために用いる第 2 の公開鍵情報と暗号化された通信を行うために用いる第 2 の非公開鍵情報とが対応することを示す鍵ペア情報、前記第 2 の公開鍵情報が正当な鍵情報であることを証明するための第 2 の証明書情報、又は、前記第 2 の証明書情報に関連する第 3 の証明書情報を示す証明書パス情報のうち少なくともいずれか一つを前記情報処理装置に設定するための命令であって、第 2 の受信装置が前記情報処理装置に対して前記第 2 の通信手順に基づいて行う命令を実行することを特徴とする請求項 17 に記載の制御方法。

[請求項19]

コンピュータに、

第 1 の通信手順に基づいて行う命令に応じて、暗号化された通信を行うための設定を前記コンピュータに対して行う第 1 の処理工程と、

第 2 の通信手順に基づいて行う命令に応じて、暗号化された通信を行うための設定を前記コンピュータに対して行う第 2 の処理工程と、

前記コンピュータに対して暗号化された通信を行うための設定を前記第 1 の通信手順に基づいて行う命令に応じて前記第 1 の処理工程において行った後に受信装置から前記第 2 の通信手順に基づいて行う命令を受信した場合、暗号化された通信を行うための設定が前記第 1 の通信手順に基づいて行う命令に応じて行われたことを示す情報を前記

受信装置に送信する送信工程と
を実行させるためのプログラム。