

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第5124621号
(P5124621)

(45) 発行日 平成25年1月23日 (2013. 1. 23)

(24) 登録日 平成24年11月2日 (2012. 11. 2)

(51) Int. Cl.	F I
H04L 9/08 (2006.01)	H04L 9/00 601B
G09C 1/00 (2006.01)	G09C 1/00 660F
	H04L 9/00 601E

請求項の数 15 外国語出願 (全 22 頁)

(21) 出願番号	特願2010-147066 (P2010-147066)	(73) 特許権者	502208205
(22) 出願日	平成22年6月29日 (2010. 6. 29)		アクシス アーバー
(65) 公開番号	特開2011-43798 (P2011-43798A)		スウェーデン国 223 69 ルンド,
(43) 公開日	平成23年3月3日 (2011. 3. 3)		エンダラヴェーイェン 14
審査請求日	平成22年8月27日 (2010. 8. 27)	(74) 代理人	100109726
(31) 優先権主張番号	09164110.0		弁理士 園田 吉隆
(32) 優先日	平成21年6月30日 (2009. 6. 30)	(74) 代理人	100101199
(33) 優先権主張国	欧州特許庁 (EP)		弁理士 小林 義教
(31) 優先権主張番号	61/223, 248	(72) 発明者	ステファン ルンドベリ
(32) 優先日	平成21年7月6日 (2009. 7. 6)		スウェーデン国 エスエー-224 56
(33) 優先権主張国	米国 (US)		ルンド, アストラカンヴェーイェン
			4
		(72) 発明者	ヨアシム テュルベリ
			スウェーデン国 エスエー-222 25
			ルンド, ボフスヴェーイェン 9
			最終頁に続く

(54) 【発明の名称】 カメラによって生成されたメディアデータへのアクセスを制限する方法

(57) 【特許請求の範囲】

【請求項 1】

カメラ (10) によって生成されたメディアデータへのアクセスを制限する方法であって、

非公開の初期ユーザ鍵 (K_{I C U}) を前記カメラ (10) にセットすることと、

ユーザクライアント (16) に前記初期ユーザ鍵 (K_{I C U}) を供給することと、

前記初期ユーザ鍵 (K_{I C U}) に基づく情報を含む認証メッセージを前記ユーザクライアント (16) から前記カメラ (10) に送信することによって、前記ユーザクライアント (16) と前記カメラ (10) との間に認証された関係を確認することと、

動作ユーザ鍵 (K_{O C U}) が前記カメラ (10) にセットされているかどうかをチェックすることと、

前記動作ユーザ鍵 (K_{O C U}) が前記カメラ (10) にセットされているかどうかをチェックする前記行為に応答して、前記動作ユーザ鍵 (K_{O C U}) がセットされていない場合に限って行為 a) ~ d) すなわち、

a) 動作ユーザ鍵 (K_{O C U}) を獲得することと、

b) 前記動作ユーザ鍵 (K_{O C U}) を前記カメラ (10) にセットすることと、

c) 前記動作ユーザ鍵 (K_{O C U}) を前記ユーザクライアント (16) にセットすることと、

d) 前記動作ユーザ鍵 (K_{O C U}) がセットされていることを前記カメラ (10) 内
で示すことと

10

20

を実行することと、

前記カメラ（10）内で、前記動作ユーザ鍵（ K_{OCU} ）に関連するメディアデータ暗号化／復号化鍵をセットすることと、

前記メディアデータ暗号化鍵を使用して、前記カメラ（10）によって登録されるメディアデータを暗号化することと、

前記暗号化されたメディアデータをサービスプロバイダ管理サーバ（17）に送信することと

を含む方法。

【請求項2】

任意のユーザクライアント（16）によって前記サービスプロバイダ管理サーバ（17）を介してメディアデータを取り出し、前記取り出されたメディアデータを前記メディアデータ暗号化／復号化鍵を使用して復号化する行為をさらに含む、請求項1に記載の方法。

10

【請求項3】

前記カメラ（10）、前記ユーザクライアント（16）、およびサービスプロバイダ管理サーバ（17）の間で共有される共通鍵（ K_C ）を獲得することと、

前記共通鍵（ K_C ）を前記カメラ（10）にセットすることと、

前記共通鍵（ K_C ）を前記ユーザクライアント（16）および前記サービスプロバイダ管理サーバ（17）に供給することと、

前記共通鍵（ K_C ）に関連するメタデータ暗号化／復号化鍵を使用して、前記カメラ（10）によって登録されるメタデータを暗号化することと、

20

前記暗号化されたメタデータを前記サービスプロバイダ管理サーバ（17）に送信することと

をさらに含む、請求項1または2に記載の方法。

【請求項4】

サービスプロバイダ鍵（ K_{SP} ）を獲得することと、

前記サービスプロバイダ鍵（ K_{SP} ）を前記サービスプロバイダ管理サーバ（17）に供給することであって、前記サービスプロバイダ鍵（ K_{SP} ）は、前記サービスプロバイダ管理サーバ（17）だけがサービスプロバイダ構成機能にアクセスできることを保証するために使用されることと

30

をさらに含む、請求項1に記載の方法。

【請求項5】

前記動作ユーザ鍵（ K_{OCU} ）がセットされている場合に、前記動作ユーザ鍵（ K_{OCU} ）が既にセットされていることを示すことをさらに含む、請求項1に記載の方法。

【請求項6】

前記動作ユーザ鍵（ K_{OCU} ）がセットされていることを前記カメラ（10）内で示す前記行為が、さらなる使用から前記初期ユーザ鍵（ K_{ICU} ）を削除することを含む、請求項1または5に記載の方法。

【請求項7】

マスタ鍵（ K_M ）を前記カメラ（10）にセットすること

40

をさらに含み、前記非公開の初期ユーザ鍵（ K_{ICU} ）を前記カメラ（10）にセットする前記行為が、前記マスタ鍵（ K_M ）から第1の一方関数（ f_1 ）を使用して前記非公開の初期ユーザ鍵（ K_{ICU} ）を導出すること（すなわち、 $K_{ICU} = f_1(K_M)$ ）によって、前記非公開の初期ユーザ鍵（ K_{ICU} ）を獲得することを含む、請求項1に記載の方法。

【請求項8】

マスタ鍵（ K_M ）を前記カメラ（10）にセットすることをさらに含み、前記非公開の初期ユーザ鍵（ K_{ICU} ）を前記カメラにセットする前記行為が、前記マスタ鍵（ K_M ）から第1の一方関数（ f_1 ）を使用して前記非公開の初期ユーザ鍵（ K_{ICU} ）を導出すること（すなわち、 $K_{ICU} = f_1(K_M)$ ）によって、前記非公開の初期ユーザ鍵（

50

K_{ICU}) を獲得することを含み、前記サービスプロバイダ鍵 (K_{SP}) を獲得する前記ステップが、第2の一方向関数 (f_2) を使用して前記マスタ鍵 (K_M) から前記サービスプロバイダ鍵 (K_{SP}) を導出すること (すなわち、 $K_{SP} = f_2(K_M)$) を含む、請求項4に記載の方法。

【請求項9】

請求項3に記載の特徴をさらに含み、前記共通鍵 (K_C) を獲得する前記ステップが、第3の一方向関数 (f_3) を使用して前記非公開の初期ユーザ鍵 (K_{ICU}) から前記共通鍵 (K_C) を導出すること、または第4の一方向関数 (f_4) を使用して前記サービスプロバイダ鍵 (K_{SP}) から前記共通鍵 (K_C) を導出することを含み、前記第3の一方向関数 (f_3) および前記第4の一方向関数 (f_4) は、前記共通鍵 (K_C) が、前記非公開の初期ユーザ鍵 (K_{ICU}) と前記サービスプロバイダ鍵 (K_{SP}) のうちのどちらから導出されるかは関係なく、同一の共通鍵 (K_C) を作るように構成されている (すなわち、 $K_C = f_3(K_{ICU}) = f_4(K_{SP})$ である)、請求項8に記載の方法。

【請求項10】

前記ユーザクライアント (16) と前記カメラ (10) との間に前記認証された関係を確立する前記行為は、前記初期ユーザ鍵 (K_{ICU}) に基づく情報を含む認証メッセージを前記ユーザクライアント (16) から前記カメラ (10) に送信することによる前記ユーザクライアント (16) の認証が実行された後で、ビデオシーケンスが所期のカメラ (10) によってリアルタイムで取り込まれていることの検証のために前記ビデオシーケンスを前記カメラ (10) から前記ユーザクライアント (16) に送信することと、前記カメラの認証の確認として確認メッセージを前記ユーザクライアント (16) から前記カメラ (10) に送信することとによって、前記カメラ (10) を認証することをさらに含む、請求項1に記載の方法。

【請求項11】

ネットワークカメラによって登録されるメディアデータをエンコードするように構成された前記ネットワークカメラであって、

セキュア鍵生成プロセスを使用して、初期ユーザ鍵 (K_{ICU}) または動作ユーザ鍵 (K_{OCU}) を生成するように構成された鍵生成手段 (50) と、

前記動作ユーザ鍵 (K_{OCU}) が生成されたかどうかを示すように構成された表示手段 (52) と、

前記表示手段 (52) が、前記動作ユーザ鍵 (K_{OCU}) が生成されたことを示しているかどうかをチェックするように構成されたチェック手段 (54) と、

前記動作ユーザ鍵 (K_{OCU}) に関連するメディアデータ暗号化鍵を使用して、前記カメラによって登録されるメディアデータを暗号化するように構成された暗号化手段 (56) と、

前記暗号化されたメディアデータを送信するように構成されたデジタルネットワークモジュール (58) と

を含む、ネットワークカメラ。

【請求項12】

前記鍵生成手段 (50) が共通鍵 (K_C) を生成するようにさらに構成されており、前記暗号化手段 (56) が、前記共通鍵 (K_C) に関連するメタデータ暗号化／復号化鍵を使用して、前記カメラによって登録されるメタデータを暗号化するようにさらに構成されており、前記デジタルネットワークモジュール (58) が、前記暗号化されたメタデータを送信するようにさらに構成されている、請求項11に記載のネットワークカメラ。

【請求項13】

前記生成された動作ユーザ鍵 (K_{OCU}) をリセットするように構成されたリセット手段 (60) をさらに含む、請求項11に記載のネットワークカメラ。

【請求項14】

前記リセット手段 (60) がリセットボタンを含む、請求項13に記載のネットワークカメラ。

【請求項 15】

前記表示手段（52）が、前記動作ユーザ鍵（K_{OCU}）が生成された場合にさらなる使用から前記初期ユーザ鍵（K_{ICU}）を削除するように構成されている、請求項 11 に記載のネットワークカメラ。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、カメラによって生成されたメディアデータへのアクセスを制限する方法および生成されたメディアデータをエンコードするように構成されたカメラに関する。

【背景技術】

10

【0002】

ビデオサーベイランスシステムの重要な部分は、ビデオおよびオーディオまたはアラームイベントなどの他のメディアコンテンツを記録する可能性である。これらのレコーディングは、ユーザが、後に、たとえば特定のメディアデータを検索し、出来事を追跡するなどを行うことを可能にする。

【0003】

ビデオサーベイランスシステムのもう 1 つの重要な部分は、サーベイランスシステムによってカバーされるエリアをリアルタイムで監視する可能性である。

【0004】

加入者ベースのサーベイランスシステムでは、ユーザは、ユーザがサーベイランスシステムまたはサーベイランスデータのレコーディングを彼自身で構成する必要がなくなるように、サービスプロバイダが、サーベイランスシステムのセットアップならびにメディアストレージおよびストレージサービスを処理することを好む。たとえば、ユーザは、サービスプロバイダに直接に接続でき、そのサービスプロバイダによって提供される検索サービスおよび取出サービスを使用して、サーベイランスデータのレコーディングを検索し、見ることができなければならない。

20

【0005】

しかし、家庭環境でのリアルタイムのまたは記録されたメディアデータは、ユーザがどの状況の下でもサービスプロバイダがアクセスできることを好まない、非常に微妙な情報を含む場合がある。

30

【0006】

したがって、サービスプロバイダサイトにあるリアルタイムのまたは格納されたメディアデータが保護され、メディアデータが財産所有者のみによってアクセス可能であるシステムを提供することが重要である。さらに、サービスプロバイダがアラームおよびレコーディングに関する効率的な検索サービスをエンドユーザに提供できるように、サービスプロバイダが、タイムスタンプ、ビデオトリガリング情報、アラームデータ、または類似物などのメタデータのレコーディングにアクセスすることが、それでも可能でなければならない。

【0007】

データ獲得デバイスによって獲得されたデータの保護されたストレージを提供するシステムが、C. H. Bennett の特許文献 1 に記載されている。特許文献 1 では、データ獲得デバイス、たとえば、マイクロホンと有し、セキュア暗号化プロセッサに接続されたビデオカメラが説明されている。セキュア暗号化プロセッサは、データ獲得デバイスによって獲得されたデータがストレージユニットに転送される前に、そのデータを暗号化する。これは、データが、必ず暗号化された形で格納されることを暗示する。したがって、正しい権利アクセス鍵（right access key）を有する認可された人だけが、データを復号化することができる。

40

【0008】

しかし、データが、特許文献 1 に従って暗号化され、ユーザによってのみアクセス可能である場合には、サービスプロバイダがアラームおよびレコーディングに関する効率的な

50

検索サービスをエンドユーザに提供できるように、サービスプロバイダが、タイムスタンプ、ビデオトリガリング情報、アラームデータ、または類似物などのメタデータのレコーディングにアクセスすることは、不可能である。

【0009】

本発明は、上で述べた問題に対する解決策を説明する。

【先行技術文献】

【特許文献】

【0010】

【特許文献1】 米国特許第7477740号

【発明の概要】

10

【発明が解決しようとする課題】

【0011】

本発明の目的は、サービスプロバイダサイトにあるリアルタイムのまたは格納されたメディアデータを、監視されるサイトの所有者／占有者によって信頼されない人による認可されないアクセスから保護することである。

【課題を解決するための手段】

【0012】

上記の目的は、独立請求項に従う方法およびカメラによって達成される。本発明のさらなる実施形態は、従属請求項で提示される。

【0013】

20

具体的に言うと、カメラによって生成されたメディアデータへのアクセスを制限する方法は、非公開の初期ユーザ鍵をカメラにセットすることと、ユーザクライアントに初期ユーザ鍵を供給することと、初期ユーザ鍵に基づく情報を含む認証メッセージをユーザクライアントからカメラに送信することによって、ユーザクライアントとカメラとの間に認証された関係を確立することと、動作ユーザ鍵 (operational user key) がカメラにセットされているかどうかをチェックすることと、動作ユーザ鍵がカメラにセットされているかどうかをチェックする行為に応答して、動作ユーザ鍵がセットされていない場合に限り行為 a) ～ d) すなわち、a) 動作ユーザ鍵を獲得することと、b) 動作ユーザ鍵をカメラにセットすることと、c) 動作ユーザ鍵をユーザクライアントにセットすることと、d) 動作ユーザ鍵がセットされていることをカメラ内で示すこととを
30 実行することを含む。この方法は、カメラ (10) 内で、動作ユーザ鍵に関連するメディアデータ暗号化／復号化鍵をセットすることと、メディアデータ暗号化／復号化鍵を使用してカメラによって登録されるメディアデータを暗号化することと、暗号化されたメディアデータをサービスプロバイダ管理サーバに送信することとをさらに含む。

【0014】

カメラによって生成されたメディアデータへのアクセスを制限する方法によって、サービスプロバイダサイトにあるリアルタイムのまたは格納されたメディアデータを保護することが可能であり、その結果、メディアデータは、サービスプロバイダによってではなくユーザのみによってアクセスできるようになる。カメラによって登録され、その後にサービスプロバイダ管理サーバに送信されるメディアデータは、動作ユーザ鍵に関連する
40 メディアデータ暗号化／復号化鍵を使用する暗号化によって、サービスプロバイダによるアクセスから保護される。メディアデータ暗号化／復号化鍵を、さまざまな形で動作ユーザ鍵に関連付けることができる。本発明の実施形態によれば、メディアデータ暗号化／復号化鍵の導出は、動作ユーザ鍵に基づく。本発明のもう1つの実施形態によれば、メディアデータ暗号化／復号化鍵を、共有される動作ユーザ鍵を使用して、カメラおよびユーザクライアントにセキュアに配布することができる。その代わりに、本発明のもう1つの実施形態によれば、カメラおよびユーザクライアント内に既にセキュアにセットされている動作ユーザ鍵自体を、メディアデータ暗号化／復号化鍵として使用することができる。したがって、カメラによって登録されたメディアデータへのアクセスを得るためには、動作
50 ユーザ鍵に関連するメディアデータ暗号化／復号化鍵を知らなければならない。本発明に

よれば、動作ユーザ鍵に関する知識を有し、したがって、メディアデータ暗号化／復号化鍵の知識を有するのが、ユーザのみであることが保証される。これは、ユーザが、最初にかメラへのアクセスを得る前に、初期ユーザ鍵を使用して彼／彼女自身を認証する必要があり、動作ユーザ鍵の獲得をトリガできるのが、認証されたユーザのみであり、動作ユーザ鍵が、動作ユーザ鍵がまだカメラにセットされていない場合に限って獲得されるからである。これは、動作ユーザ鍵を獲得する前に、動作ユーザ鍵がカメラに既にセットされているかどうかをチェックすることによって達成される。たとえば、サービスプロバイダが、初期ユーザ鍵をユーザに提供する前に、初期ユーザ鍵を使用して彼／彼女自身をユーザとして登録する場合に、これが、ユーザによって検出される。というのは、ユーザが、カメラによって成功して登録し、それに対する制御を得ることができなくなるからである。したがって、この方法は、たとえば、初期ユーザ鍵がサービスプロバイダによってユーザに提供される場合であっても、サービスプロバイダがカメラの制御を得ることを防ぐ。これによって、この手順は、サービスプロバイダが、動作ユーザ鍵へのアクセスを得るためにユーザの代わりにカメラで登録することを選択する場合に、ユーザが、この手順を繰り返すことを試みる時にそれを発見することを保証する。というのは、動作ユーザ鍵の獲得が失敗し、ユーザが、これによって、誰かが動作ユーザ鍵を既に獲得していることを発見するからである。

10

【0015】

一実施形態によれば、この方法は、任意のユーザクライアントによってサービスプロバイダ管理サーバを介してメディアデータを取り出し、取り出されたメディアデータをメディアデータ暗号化／復号化鍵を使用して復号化することをさらに含むことができる。

20

【0016】

もう1つの実施形態によれば、この方法は、カメラ、ユーザクライアント、およびサービスプロバイダ管理サーバの間で共有される共通鍵を獲得することと、共通鍵をカメラにセットすることと、共通鍵をユーザクライアントおよびサービスプロバイダ管理サーバに供給することと、共通鍵に関連するメタデータ暗号化／復号化鍵を使用してカメラによって登録されるメタデータを暗号化することと、暗号化されたメタデータをサービスプロバイダ管理サーバに送信することとをさらに含むことができる。メタデータ暗号化／復号化鍵を、共通鍵にさまざまな形で関連付けることができる。本発明の実施形態によれば、メタデータ暗号化／復号化鍵の導出は、共通鍵に基づく。本発明のもう1つの実施形態によれば、メタデータ暗号化／復号化鍵を、共有される共通鍵を使用して、カメラ、サービスプロバイダ管理サーバ、およびユーザクライアントにセキュアに配布することができる。その代わりに、本発明のもう1つの実施形態によれば、既にカメラ、サービスプロバイダ管理サーバ、およびユーザクライアントにセキュアにセットされている共通鍵自体を、メディアデータ暗号化／復号化鍵として使用することができる。これは、メタデータが、第三者によるアクセスから保護されることを保証する。さらに、メタデータをサービスプロバイダ管理サーバに送信することによって、サービスプロバイダがアラームおよびレコーディングに関する効率的な検索サービスをエンドユーザに提供できるように、サービスプロバイダが、タイムスタンプ、ビデオトリガリング情報、アラームデータ、または類似物などのメタデータのレコーディングにアクセスすることが可能である。

30

40

【0017】

もう1つの実施形態によれば、この方法は、サービスプロバイダ鍵を獲得することと、サービスプロバイダ鍵をサービスプロバイダ管理サーバに供給することとであって、サービスプロバイダ鍵は、サービスプロバイダ管理サーバだけがサービスプロバイダ構成機能にアクセスできることを保証するのに使用される、供給することとをさらに含むことができる。

【0018】

一実施形態によれば、動作ユーザ鍵がセットされていることをカメラ内で示す行為は、さらなる使用から初期ユーザ鍵を削除することを含むことができる。

【0019】

50

もう1つの実施形態によれば、動作ユーザ鍵がセットされている場合に、動作ユーザ鍵が既にセットされていることを示すことをさらに含むことができる。

【0020】

もう1つの実施形態によれば、この方法は、マスタ鍵をカメラにセットすることをさらに含むことができる。非公開の初期ユーザ鍵をカメラにセットする行為は、その場合に、マスタ鍵から第1の一方関数を使用して非公開の初期ユーザ鍵を導出することによって、非公開の初期ユーザ鍵を獲得することを含むことができる。

【0021】

一実施形態によれば、サービスプロバイダ鍵を獲得するステップは、マスタ鍵から第2の一方関数を使用してサービスプロバイダ鍵を導出することを含むことができる。

10

【0022】

もう1つの実施形態によれば、共通鍵を獲得するステップは、非公開の初期ユーザ鍵から第3の一方関数を使用して共通鍵を導出することまたはサービスプロバイダ鍵から第4の一方関数を使用して共通鍵を導出することを含むことができ、第3の一方関数および第4の一方関数は、共通鍵が非公開の初期ユーザ鍵とサービスプロバイダ鍵のうちのどちらから導出されるかには関係なく、同一の共通鍵を作るように構成される。

【0023】

もう1つの実施形態によれば、ユーザクライアントとカメラとの間に認証された関係を確立する行為は、初期ユーザ鍵に基づく情報を含む認証メッセージをユーザクライアントからカメラに送信することによるユーザクライアントの認証が実行された後に、ビデオシーケンスが所期のカメラによってリアルタイムで取り込まれていることの検証のためにビデオシーケンスをカメラからユーザクライアントに送信することと、カメラの認証の確認として確認メッセージをユーザクライアントからカメラに送信することとによってカメラを認証することをさらに含むことができる。

20

【0024】

さらに、本発明のもう1つの態様によれば、ネットワークカメラによって登録されるメディアデータをエンコードするように構成されたネットワークカメラは、セキュア鍵生成プロセスを使用して、初期ユーザ鍵または動作ユーザ鍵を生成するように構成された鍵生成手段と、動作ユーザ鍵が生成されたかどうかを示すように構成された表示手段と、表示手段が、動作ユーザ鍵が生成されたことを示したかどうかをチェックするように構成されたチェック手段と、動作ユーザ鍵に関連するメディアデータ暗号化鍵を使用してカメラによって登録されるメディアデータを暗号化するように構成された暗号化手段と、暗号化されたメディアデータを送信するように構成されたデジタルネットワークモジュールとを含む。メディアデータ暗号化／復号化鍵を、さまざまな形で動作ユーザ鍵に関連付けることができる。本発明の一実施形態によれば、メディアデータ暗号化／復号化鍵の導出は、動作ユーザ鍵に基づく。本発明のもう1つの実施形態によれば、メディアデータ暗号化／復号化鍵を、共有される動作ユーザ鍵を使用して、カメラおよびユーザクライアントにセキュアに配布することができる。その代わりに、本発明のもう1つの実施形態によれば、既にカメラおよびユーザクライアントにセキュアにセットされている動作ユーザ鍵自体を、メディアデータ暗号化／復号化鍵として使用することができる。

30

40

【0025】

一実施形態によれば、このネットワークカメラは、生成された動作ユーザ鍵をリセットするように構成されたリセット手段をさらに含むことができる。

【0026】

もう1つの実施形態によれば、リセット手段は、リセットボタンを含むことができる。

【0027】

もう1つの実施形態によれば、表示手段は、動作ユーザ鍵が生成された場合にさらなる使用から初期ユーザ鍵を削除するように構成され得る。

【0028】

一実施形態によれば、鍵生成手段は、共通鍵を生成するようにさらに構成され得、暗号

50

化手段は、共通鍵に関連するメタデータ暗号化／復号化鍵を使用して、カメラによって登録されるメタデータを暗号化するようにさらに構成され得、デジタルネットワークモジュールは、暗号化されたメタデータを送信するようにさらに構成され得る。メタデータ暗号化／復号化鍵を、さまざまな形で共通鍵に関連付けることができる。本発明の一実施形態によれば、メタデータ暗号化／復号化鍵の導出は、共通鍵に基づく。本発明のもう1つの実施形態によれば、メタデータ暗号化／復号化鍵を、共有される共通鍵を使用して、カメラ、サービスプロバイダ管理サーバ、およびユーザクライアントにセキュアに配布することができる。その代わりに、本発明のもう1つの実施形態によれば、既にカメラ、サービスプロバイダ管理サーバ、およびユーザクライアントにセキュアにセットされている共通鍵自体を、メディアデータ暗号化／復号化鍵として使用することができる。

10

【0029】

本発明の適用可能性のさらなる範囲は、下で与える詳細な説明から明白になる。しかし、詳細な説明および特定の例は、本発明の好ましい実施形態を示すが、例示のみのために与えられることを理解されたい。というのは、本発明の趣旨および範囲に含まれるさまざまな変更および修正が、この詳細な説明から当業者に明白になるからである。

【0030】

本発明を、本発明の実施形態を示す添付の概略図を参照して、例としてより詳細に説明する。

【図面の簡単な説明】

【0031】

20

【図1】本発明によるサーベイランスシステムの一実施形態を示す概略図である。

【図2】セキュリティ関連付け鍵および暗号化鍵を生成し、カメラによって登録されるメディアデータおよびメタデータを暗号化するプロセスを示す概略流れ図である。

【図3】本発明の一実施形態によるカメラを示す概略図である。

【発明を実施するための形態】

【0032】

ビデオサーベイランスを、加入者ベースのシステムとして実施することができ、ここで、図1に示されているように、ユーザは、ネットワークビデオカメラを監視される位置、たとえばユーザの家庭に設置するが、カメラは、サービスプロバイダによってまたは少なくともサービスプロバイダを介して制御され、管理される。

30

【0033】

図1に示された実施形態によるサーベイランスシステムは、財産を監視するネットワークビデオカメラ10を含む。ネットワークビデオカメラ10は、プライベートネットワーク11に接続され、プライベートネットワーク11は、インターネット12などの公衆ネットワーク、NAT 13および／またはプライベートネットワーク11を外部攻撃から保護するファイアウォール14、プライベートネットワーク11に直接に接続されるかインターネット12に接続されるかのいずれかであるユーザクライアント16、サービスプロバイダネットワーク19に接続された公衆サービスプロバイダ管理サーバ17を介してユーザ財産サーベイランスサービスを提供するサービスプロバイダ、ならびにサービスプロバイダ管理サーバ17に直接に接続されるかサービスプロバイダネットワーク19に接続されるかのいずれかであるサービスプロバイダストレージユニット18に接続される。サービスプロバイダネットワーク19も、インターネット12などの公衆ネットワークに接続される。

40

【0034】

ネットワークビデオカメラ10は、ユーザのローカル財産を監視すると同時に、リモートのサービスプロバイダストレージユニット18にメディアデータ（たとえば、ビデオデータおよびおそらくはオーディオデータなどの他のメディアデータ）を記録する。さらに、メディアデータのほかに、ネットワークビデオカメラ10は、タイムスタンプ、ビデオトリガリング情報、アラームデータ、または類似物などのメタデータも記録する。また、メタデータは、リモートのサービスプロバイダストレージユニット18に記録される。オ

50

プシオンで、メディアデータおよびメタデータを、ローカルストレージユニット15にも記録することができる。

【0035】

ユーザが、ユーザクライアント16によって、格納されたメディアデータを検索し、取り出すことを望む場合に、ユーザは、インターネット12を介してサービスプロバイダ管理サーバ17に接続する。サービスプロバイダ管理サーバ17に接続している時に、ユーザは、記録されたメディアデータを検索し、ダウンロードすることができる。メディアデータは、URLをダウンロードすることによって、またはサービスプロバイダ管理サーバ17からメディアストリームを取り出すことによってダウンロードすることができる。オプションで、メディアデータおよびメタデータがローカルストレージユニット15に配置される場合に、ユーザクライアント16は、ローカルストレージユニット15に直接に記録されたメディアデータにアクセスすることができる。

10

【0036】

同様に、ユーザが、リアルタイムメディアデータにアクセスしたい場合には、ユーザは、ユーザクライアント16を使用してサービスプロバイダ管理サーバ17に接続し、ユーザクライアント16にダウンロードされるかストリーミングされるリアルタイムメディアデータを要求する。オプションで、ユーザクライアント16が、プライベートネットワーク11に接続される場合に、ユーザは、リアルタイムメディアデータにアクセスするためにネットワークビデオカメラ10に直接にアクセスすることができる。

20

【0037】

ユーザがサーベイランスシステムを独力で完全に構成し、管理するシステムと比較した、システム内にサービスプロバイダを含めることの利益は、前者が、ユーザに高度な構成スキルを要求することである。さらに、そのような構成は、追加のソフトウェアおよび機器を必要とするはずである。さらに、ユーザは、ネットワークビデオカメラ10またはローカルストレージユニット15がファイヤウォール14および／またはNAT 13の背後に位置するので、インターネット12からこれらに簡単にはアクセスできないはずである。その一方で、サービスプロバイダを有するシステムは、サービスプロバイダがユーザの財産からのリアルタイムメディアデータまたは記録されたメディアデータへのアクセスを有するので、ユーザがサービスプロバイダを非常に信頼することを要求する。本発明は、この問題に対処する。

30

【0038】

本発明によれば、複数ステップでの鍵導出に基づくメディア保護解決策が提示される。一実施形態によれば、複数ステップでの鍵導出は、次のように実行される。図2を参照されたい。

【0039】

最初のステップとして、一意の秘密マスタ鍵 K_M を生成する(ステップ100)。秘密マスタ鍵 K_M を、カメラ10にセットする(ステップ102)。このマスタ鍵 K_M をセットすることは、たとえば、マスタ鍵 K_M をビデオカメラ10に格納することによって実行することができる。マスタ鍵 K_M の格納は、たとえば、カメラ製造業者によってまたはサービスプロバイダによって実行することができる。マスタ鍵 K_M は、たとえばセキュア擬似乱数ジェネレータと組み合わせられた、熱雑音または無線周波数雑音の測定に基づくセキュア乱数ソース(secure random source)を使用する鍵生成など、セキュア鍵生成プロセスを使用して生成される。マスタ鍵 K_M は、カメラ10自体の中で生成され、または外部で生成され、その後にカメラ10に供給されるのいずれかとすることができる。

40

【0040】

マスタ鍵 K_M を使用して、初期ユーザ鍵 K_{ICU} を導出する(ステップ104)。初期ユーザ鍵 K_{ICU} は、カメラに特有とすることができる。マスタ鍵 K_M を使用して、サービスプロバイダ鍵 K_{SP} も導出する(ステップ106)。サービスプロバイダ鍵 K_{SP} は、カメラに特有とすることができる。初期ユーザ鍵 K_{ICU} またはサービスプロバイダ鍵

50

K_{SP} を今度は使用して、共通鍵 K_C を導出することができる（ステップ108）。共通鍵 K_C も、カメラに特有とすることができる。

【0041】

マスタ鍵 K_M からの初期ユーザ鍵 K_{ICU} の導出を、第1の一方方向関数 f_1 によって実行することができる、すなわち、 $K_{ICU} = f_1(K_M)$ とすることができる。

【0042】

適切な一方方向関数は、すべての入力に対して簡単に計算されるが、ランダム入力のイメージを与えるために逆転が困難な関数である。そのような関数の例は、SHA-1もしくはSHA-256などのハッシュ関数または固定された（既知の）テキスト入力に対するSHA-1ベースのMHAC（未知の入力として鍵値を用いる）またはSHA-256ベースのHMACなどのそのようなハッシュ関数から導出された関数および類似物である。

10

【0043】

同様に、マスタ鍵 K_M からのサービスプロバイダ鍵 K_{SP} の導出を、第2の一方方向関数 f_2 によって実行することができる、すなわち、 $K_{SP} = f_2(K_M)$ とすることができる。

【0044】

共通鍵 K_C を、第3の一方方向関数 f_3 によって初期ユーザ鍵 K_{ICU} から導出することができる、すなわち、 $K_C = f_3(K_{ICU})$ とすることができる。その代わりに、共通鍵 K_C を、第4の一方方向関数 f_4 によってサービスプロバイダ鍵 K_{SP} から導出することができる、すなわち、 $K_C = f_4(K_{SP})$ とすることができる。

20

【0045】

第3の一方方向関数（ f_3 ）および第4の一方方向関数（ f_4 ）は、共通鍵 K_C が非公開（non-public）初期ユーザ鍵 K_{ICU} とサービスプロバイダ鍵 K_{SP} のうちのどちらから導出されるかには関係なく、同一の共通鍵 K_C を作る（すなわち、 $K_C = f_3(K_{ICU}) = f_4(K_{SP})$ ）ように構成される。そのような構成の例は、 K_{ICU} および K_{SP} が、共通の同一の部分を持つように導出され、一方方向関数 f_3 が K_{ICU} をこの共通部分に切り詰め、その切り詰められた部分に適切なハッシュ関数を適用するようになっているときである。同様に、 f_4 は、まず、 K_{SP} を共通部分に切り詰め、次に同一のハッシュ関数のこの部分に適用する。この場合に、 f_1 および f_2 は、この要件に一致するように選択される必要がある。実際に、 f_1 および f_2 を、たとえば $f_1(K)$ を $a(K) + f'_1(K)$ と定義し、 $f_2(K)$ を $a(K) + f'_2(K)$ と定義することによって、そのような形で選択することができ、ここで、 $+$ は連結を表し、 f'_1 および f'_2 は、一意の一方方向ハッシュ関数を表す。

30

【0046】

これらの鍵のすべてすなわち、マスタ鍵 K_M 、初期ユーザ鍵 K_{ICU} 、サービスプロバイダ鍵 K_{SP} 、および共通鍵 K_C は、信頼されるエンティティまたは半信頼される（semi-trusted）エンティティの間の初期セキュリティ関連付けの基礎として使用されるが、必ずしも、メディアデータの実際の保護に使用される鍵ではない。

【0047】

初期ユーザ鍵 K_{ICU} を、カメラ10にセットし（ステップ110）、カメラ10と一緒にユーザクライアント16に供給する（ステップ112）。したがって、初期ユーザ鍵 K_{ICU} は、物理的にユーザクライアント16に配置され、ユーザの制御下にある。カメラ10および初期ユーザ鍵 K_{ICU} を、たとえば、サービスプロバイダによってユーザに供給することができる。

40

【0048】

サービスプロバイダ鍵 K_{SP} をカメラ10にセットし（ステップ113）、サービスプロバイダに供給する（ステップ114）。

【0049】

共通鍵 K_C をカメラ10にセットし（ステップ115）、ユーザとサービスプロバイダとの両方に供給する（ステップ116および118）。これは、たとえば、上で説明した

50

共通鍵 K_C 、初期ユーザ鍵 K_{ICU} 、およびサービスプロバイダ鍵 K_{SP} の間の関係すなわち $K_C = f_3(K_{ICU}) = f_4(K_{SP})$ を使用して実行することができる。

【0050】

マスタ鍵をカメラにセットし、その後、マスタ鍵から初期ユーザ鍵、サービスプロバイダ鍵、および共通鍵を導出することによって、メディアデータ、メタデータ、およびカメラにアクセスするための鍵を効率的に配布する解決策が提供される。

【0051】

カメラ10へのアクセスを得る前に、ユーザは、カメラ10のユーザとしてユーザ自身を認証する必要がある。この認証中に、ユーザクライアント16とカメラ10との間に認証された関係が確立される（ステップ120）。ユーザは、初期ユーザ鍵 K_{ICU} およびユーザアイデンティティに基づく情報を含む認証メッセージをユーザクライアント16からカメラ10に送信することによって認証される。カメラは、ビデオシーケンスが所期のカメラ10によってリアルタイムで取り込まれることの検証のためにビデオシーケンスをカメラ10からユーザクライアント16に送信することと、カメラの認証の確認として確認メッセージをユーザクライアント16からカメラ10に送信することによって認証される。

【0052】

カメラ10とユーザクライアント16との間の認証された関係が確立された時に、動作ユーザ鍵 K_{OCU} が、獲得され（ステップ124）、カメラにセットされ（ステップ126）、ユーザに配布される（ステップ128）。動作ユーザ鍵 K_{OCU} をセットすることは、カメラ10でも示される（ステップ127）。カメラ10およびカメラ10によって作られたメディアデータへのフルアクセス権を有するのは、動作ユーザ鍵 K_{OCU} の所有者だけである。動作ユーザ鍵 K_{OCU} は、たとえば、カメラ10で生成することができる。動作ユーザ鍵 K_{OCU} の配布を、初期ユーザ鍵 K_{ICU} によって保護することができる。動作ユーザ鍵 K_{OCU} を、カメラに特有とすることができる。

【0053】

ステップ124の動作ユーザ鍵 K_{OCU} 獲得を実行する前に、動作ユーザ鍵 K_{OCU} がカメラにセットされているか否かをチェックする（ステップ122）。ステップ124の動作ユーザ鍵 K_{OCU} 獲得、ステップ126のカメラ10での動作ユーザ鍵 K_{OCU} のセット、ステップ127の動作ユーザ鍵 K_{OCU} がセットされていることをカメラ10で示すこと、およびステップ128の動作ユーザ鍵 K_{OCU} をユーザクライアント16に送信することは、ステップ122でのチェックからの結果が、動作ユーザ鍵 K_{OCU} がカメラ10でセットされていないことを示す場合に限って実行される。つまり、初期ユーザ鍵 K_{ICU} は、動作ユーザ鍵 K_{OCU} を作るために1回だけ使用される。したがって、サービスプロバイダが、初期ユーザ鍵 K_{ICU} をユーザに供給する前に、初期ユーザ鍵 K_{ICU} を使用してプロバイダ自身をユーザとして認証する場合、これは、ユーザが、カメラ10によって成功裏に認証されて、それに対する制御を得ることに失敗するとき、ユーザによって検出される。

【0054】

したがって、この方法は、たとえば、初期ユーザ鍵 K_{ICU} がサービスプロバイダによってユーザに供給される場合であっても、サービスプロバイダがカメラの制御を得ることを防ぐ。これによって、この手順は、サービスプロバイダが動作ユーザ鍵 K_{OCU} へのアクセスを得るためにユーザの代わりにカメラ10で登録することを選択する場合に、ユーザが、この手順を繰り返すことを試みる時にそれを発見することを保証する。というのは、動作ユーザ鍵 K_{OCU} の獲得が失敗し、ユーザが、これによって、誰かが既に動作ユーザ鍵 K_{OCU} を獲得していることを発見するからである。

【0055】

カメラ10へのユーザの登録中に問題が発生する場合には、ユーザは、新規の初期ユーザ鍵 K_{ICU} または新規の動作ユーザ鍵 K_{OCU} を生成することができる。たとえば、カメラ10への物理的アクセスを有するか、他のアクセス制限ルールに従うユーザは、カメ

10

20

30

40

50

ラ内のセキュリティセッティングをリセットし、カメラでの新規の初期ユーザ鍵 K_{ICU} の生成をトリガできるものとすることができる（ステップ130）。その代わりに、カメラへの物理的アクセスを有するか、他のアクセス制限ルールに従うユーザは、現在使用されている動作ユーザ鍵 K_{OCU} を削除し、初期ユーザ鍵 K_{ICU} を使用して新しい登録を要求し、したがって、新しい動作ユーザ鍵 K_{OCU} を獲得できるものとすることができる（ステップ132）。リセットするプロセス（ステップ130）、または削除するプロセス（ステップ132）は、カメラ10のハウジングに配置されたリセットボタンを押すことによって開始することができる。他のアクセス制限ルールの例は、たとえば、ユーザによってまたは保護されたトリガに基づいてネットワークを介してリモートコントロールによって提供されるトリガ信号の無線送信または光送信に基づくリモートローカルコントロールとすることができる。トリガを、後者の場合に、たとえば、共通鍵 K_C またはサービスプロバイダ鍵 K_{SP} によって保護することができる。

10

【0056】

本発明は、カメラ10から送信されたすべてのメディアデータを動作ユーザ鍵 K_{OCU} に基づいて保護することを可能にし、カメラによって監視されるサイトの所有者／占有者がカメラ10によって生成されるメディアデータの排他的制御を有することを可能にする。

【0057】

本発明の実施形態によれば、メディアデータは、メディアデータ暗号化／復号化鍵を使用する対称暗号化によって暗号化される。このメディアデータ暗号化／復号化鍵は、一実施形態によれば、時間セグメント鍵（time segment key）である。セキュリティを高めるために、本発明は、通信を、それぞれを異なる時間セグメント鍵を使用して暗号化できる異なる時間セグメントに分割することを提供する。使用される時間セグメント鍵は、たとえば、時間、送信されるデータの量、または送信されるメッセージの個数に基づいて変更することができる。たとえば、時間セグメント鍵を、 x 分後に、 y メガバイトのデータの後に、または送信される z 個のメッセージの後に、変更することができる。本発明によれば、それぞれの時間セグメントについて使用される時間セグメント鍵は、破棄されるのではなく、暗号化され、復号化および／または認証のために各時間セグメントの暗号化された情報に関連して格納される、すなわち、現在の時間セグメント鍵を使用して、以前の時間セグメント鍵を含むデータを復号化することができ、この以前の時間セグメント鍵によって暗号化されたメディアデータの復号化が可能になる。当技術分野で既知のように、対称暗号化技法は、暗号化と復号化との両方に同一の鍵を使用する。対称暗号化および復号化は、高速であるが、送信側（この場合にはカメラ10）および受信側（この場合にはユーザクライアント16）が事前に鍵を共有することを必要とする。本発明によれば、事前に共有される鍵を、動作ユーザ鍵 K_{OCU} とすることができる。メディアデータ自体は、時間セグメント鍵の形のメディアデータ暗号化／復号化鍵を使用して暗号化され、復号化される。

20

30

【0058】

本発明の実施形態によれば、時間セグメント鍵の形のメディアデータ暗号化／復号化鍵の導出を、動作ユーザ鍵 K_{OCU} に基づくものとすることができる。

40

【0059】

さらに、もう1つの実施形態によれば、時間セグメント鍵の形のメディアデータ暗号化／復号化鍵を、事前に共有される動作ユーザ鍵 K_{OCU} を使用して送信側（カメラ10）および受信側（ユーザクライアント16）にセキュアに配布することができる。

【0060】

その代わりに、本発明の実施形態によれば、既にカメラ10およびユーザクライアント16にセキュアに配布されている動作ユーザ鍵 K_{OCU} 自体を、メディアデータ暗号化／復号化鍵として使用することができる。

【0061】

したがって、カメラ10によって生成されたメディアデータは、動作ユーザ鍵 K_{OCU}

50

に関連するメディアデータ暗号化／復号化鍵を使用して暗号化され、復号化される（ステップ134）。メディアデータ暗号化／復号化鍵は、動作ユーザ鍵 K_{OCU} から導出されるか、動作ユーザ鍵 K_{OCU} によって保護されてセキュアに配布されるか、実際に動作ユーザ鍵 K_{OCU} であるかのいずれかなので、カメラによって監視されるサイトの所有者／占有者は、カメラ10によって生成されるメディアデータの排他的制御を有している。

【0062】

暗号化された時に、メディアデータは、格納のためにサービスプロバイダ管理サーバ17に送信される（ステップ136）。

【0063】

メディアデータ暗号化／復号化鍵を所有しているのはユーザだけなので、カメラ10によって生成されたメディアデータを復号化し、実際に見ることは、ユーザだけである。さらに、すべてのメタデータを、その代わりに共通鍵 K_C に基づいて保護することができる。

10

【0064】

やはり本発明の実施形態によれば、メタデータは、メタデータ暗号化／復号化鍵を使用する対称暗号化によって暗号化される。メタデータ暗号化／復号化鍵は、時間セグメント鍵とすることができ、時間セグメント鍵に関しては上を参照されたい。本発明によれば、事前に共有される鍵を、共通鍵 K_C とすることができる。メタデータ自体は、時間セグメント鍵の形のメタデータ暗号化／復号化鍵を使用して暗号化され、復号化される。

【0065】

20

本発明の実施形態によれば、時間セグメント鍵の形のメタデータ暗号化／復号化鍵の導出を、共通鍵 K_C に基づくものとすることができる。

【0066】

さらに、もう1つの実施形態によれば、時間セグメント鍵の形のメタデータ暗号化／復号化鍵を、事前に共有される共通鍵 K_C を使用して送信側（カメラ10）および受信側（サービスプロバイダ管理サーバ17および／またはユーザクライアント16）にセキュアに配布することができる。

【0067】

その代わりに、本発明の実施形態によれば、既にカメラ10、サービスプロバイダ管理サーバ17、および／またはユーザクライアント16にセキュアに配布されている共通鍵 K_C 自体を、メタデータ暗号化／復号化鍵として使用することができる。

30

【0068】

したがって、カメラ10によって生成されたメタデータは、メタデータ暗号化／復号化鍵を使用して暗号化され、復号化される（ステップ138）。したがって、カメラ10によって登録されるメタデータを、共通鍵 K_C に関連するメタデータ暗号化鍵を使用して暗号化し、復号化することができ（ステップ138）、サービスプロバイダ管理サーバ17に送信することができる（ステップ140）。したがって、ユーザとサービスプロバイダとの両方が、カメラ10によって生成されたメタデータにアクセスすることができ、これは、ユーザとサービスプロバイダとの両方が、共通鍵 K_C へのアクセスを有しているからである。

40

【0069】

代替案では、カメラ10を、メタデータとメディアデータとの両方に、ユーザとサービスプロバイダとの両方によってアクセスできるように、すべてのデータ（メディアデータとメタデータとの両方）を、共通鍵 K_C を使用して保護する形で構成することができる。これは、ユーザが、サービスプロバイダがカメラのサイトを監視することを望む時に有用である。これは、たとえば、ユーザが長期にわたって出かける時に有用である可能性がある。

【0070】

したがって、正当なユーザは、必ず、構成に応じて、動作ユーザ鍵 K_{OCU} または共通鍵 K_C の助けを得てメディアデータにアクセスし、これを復号化することができる。

50

【0071】

さらに、カメラ10を、リモート構成用に構成することができる。リモート構成用のインターフェースは、少なくとも2つのサブセット（潜在的に部分的にオーバーラップする）すなわち、サービスプロバイダによってアクセスされ得るセットと、ユーザによってアクセスされ得るもう1つのセットとに分割される。サービスプロバイダ鍵 K_{SP} は、サービスプロバイダだけがサービスプロバイダ構成機能、たとえばサービスプロバイダアドレスネットワーク構成、無線セッティング、ファームウェアアップグレードなどにアクセスできることを保証するのに使用される。同様に、動作ユーザ鍵 K_{OCU} は、ユーザだけがユーザ構成機能にアクセスできることを保証するのに使用され、たとえば、カメラアクセス保護機構は、動作ユーザ鍵 K_{OCU} を保持する者だけが暗号化ポリシ、すなわち、メディアデータが動作ユーザ鍵 K_{OCU} または共通鍵 K_C のどちらに基づいて保護されなければならないのかをセットできるように実施される。ユーザについてのみ使用可能とすることができる他の機能の例は、メディアストリーミング構成（フレームレート、解像度など）またはパンチルトズーム制御である。

10

【0072】

このシステムを使い易くするために、ユーザに、暗号化鍵／復号化鍵対を生成し、鍵ストレージを助けるツール（セキュリティトークン／セキュリティデバイス）を与えることができる。たとえば、メディアデータ暗号化／復号化鍵が、動作ユーザ鍵 K_{OCU} に基づく場合に、動作ユーザ鍵 K_{OCU} を、ハードウェアセキュリティトークンの内部に格納することができ、メディアデータ暗号化／復号化鍵が、必ず、動作ユーザ鍵 K_{OCU} をセキュアトークンの外部で露出せずにトークンおよびカメラの内部で生成されるようにするために、鍵管理方式が、トークンとカメラとの間で使用される。

20

【0073】

実際のメディア保護（認証、暗号化など）を、たとえばBennettによる特許文献1に記載の方法など、適切な技術的現状のメディア保護機構を使用して実行することができる。

【0074】

次に、異なる鍵の導出と、ユーザがネットワークビデオカメラ10を彼の家庭に設置するが、カメラ10がサービスプロバイダによって制御され、管理される、加入者ベースのシステムによって達成される家庭環境内のビデオサーベイランスの設置に含まれるインストールステップとのより詳細な説明を与える。

30

【0075】

カメラ10は、カメラ製造業者によって製造される。マスタ鍵 K_M を、セキュア鍵生成プロセスを使用してカメラ10の製造業者で生成し、その後、カメラ10にセットすることができる。マスタ鍵 K_M をカメラ10にセットすることは、たとえば、マスタ鍵 K_M を、セキュアプロセスを使用してカメラ10に格納することによって行うことができる。そのようなセキュアプロセスの1つの例が、いわゆる保護されたカメラハードウェアの内部でのオンボード鍵生成（onboard key generation）である。もう1つの例は、鍵が、セキュア鍵生成プロセスを使用してカメラの外部で生成され、その後、カメラの内部の保護されたストレージ位置に転送される時である。後者の場合に、鍵は、カメラ10に成功してインストールされた後に、外部環境内でセキュアに破壊される。

40

【0076】

マスタ鍵 K_M は、その後、3つの異なるサブ鍵すなわち、サービスプロバイダ鍵 K_{SP} 、初期ユーザ鍵 K_{ICU} 、および共通鍵 K_C を生成するのに使用される。これらのサブ鍵も、カメラ10にセットされる。鍵は、たとえば、これらの鍵をカメラ10内にセキュアに格納することによってカメラ10にセットされる。

【0077】

初期ユーザ鍵 K_{ICU} を与えられて、マスタ鍵 K_M を導出することが計算的に実現不能になるように、初期ユーザ鍵 K_{ICU} を、適切な第1の一方関数 f_1 を使用してマスタ鍵 K_M から導出することができる、すなわち、 $K_{ICU} = f_1(K_M)$ とすることができ

50

る。同様に、サービスプロバイダ鍵 K_{SP} を与えられて、マスタ鍵 K_M を導出することが計算的に実現不能になるように、サービスプロバイダ鍵 K_{SP} を、適切な第2の一方方向関数 f_2 を使用してマスタ鍵 K_M から導出することができる、すなわち、 $K_{SP} = f_2(K_M)$ とすることができる。さらに、前記適切な第1および第2の一方方向関数 f_1 、 f_2 は、追加の第3および第4の一方方向関数 f_3 、 f_4 を使用することによって、共通鍵 K_C を、 $K_C = f_3(K_{ICU}) = f_4(K_{SP})$ に従って導出できるように構成される。したがって、共通鍵 K_C を、第3の一方方向関数 f_3 によって初期ユーザ鍵 K_{ICU} から導出することができる、すなわち、 $K_C = f_3(K_{ICU})$ とすることができ、あるいはその代わりに、共通鍵 K_C を、第4の一方方向関数 f_4 によってサービスプロバイダ鍵 K_{SP} から導出することができる、すなわち、 $K_C = f_4(K_{SP})$ とすることができる。第3の一方方向関数 (f_3) および第4の一方方向関数 (f_4) は、共通鍵 K_C が非公開の初期ユーザ鍵 K_{ICU} とサービスプロバイダ鍵 K_{SP} のうちのどちらから導出されるかには関係なく、同一の共通鍵 K_C を作る (すなわち、 $K_C = f_3(K_{ICU}) = f_4(K_{SP})$) ように構成される。

【0078】

サービスプロバイダ鍵 K_{SP} は、サービスプロバイダに供給される。カメラ10を、おそらくは、ユーザに引き渡される前にサービスプロバイダに引き渡すことができる。この場合に、サービスプロバイダ鍵 K_{SP} を、カメラ10と一緒に引き渡すことが可能である。その代わりに、サービスプロバイダ鍵 K_{SP} を、カメラ10がサービスプロバイダサーバ17に接続される時にサービスプロバイダに供給することができる。サービスプロバイダ鍵 K_{SP} が、サービスプロバイダに引き渡されるか供給された後に、サービスプロバイダは、関数 f_4 を使用し、共通鍵 K_C すなわち $K_C = f_4(K_{SP})$ を計算し、サービスプロバイダ鍵 K_{SP} および共通鍵 K_C を適切なデータベースにセキュアに格納する。ユーザデータ、たとえば名前、住所などが、サービスプロバイダ鍵 K_{SP} および共通鍵 K_C に関連付けられてデータベースに格納される。サービスプロバイダ鍵 K_{SP} を使用して、サービスプロバイダ管理サーバ17だけが、サービスプロバイダ構成機能、たとえばサービスプロバイダアドレスおよび類似物にアクセスできることを保証することもできる。

【0079】

カメラ10は、ユーザに引き渡され、ユーザ住居ネットワーク11に設置される。ユーザは、カメラ10と一緒に、カメラに特有の初期ユーザ鍵 K_{ICU} を受け取る (おそらくはサービスプロバイダを介してまたは他の手段によって)。カメラ10は、インターネット12アクセスを有する任意の位置からサービスプロバイダによってアクセス可能であり、インターネット12アクセスを有する任意の位置からユーザクライアント16によってアクセス可能になるように、住居ネットワーク11に設置される。

【0080】

初期ユーザ鍵 K_{ICU} は、ユーザクライアント16に供給される。たとえば、ユーザは、初期ユーザ鍵 K_{ICU} をユーザクライアント16にセキュアにインストールすることができる。初期ユーザ鍵 K_{ICU} のインストールは、USBスティックまたは類似物を介して実行することができる。次に、第3の一方方向関数 f_3 が、やはりユーザクライアント16にセキュアに格納される共通鍵 K_C を計算するのに使用される、すなわち、 $K_C = f_3(K_{ICU})$ である。

【0081】

ユーザは、潜在的にサービスプロバイダシステムを介して、カメラ10に接続し、カメラ10によるユーザクライアント16の登録を要求する。

【0082】

ユーザクライアント16は、たとえば、サービスプロバイダネットワーク内のプロキシサーバに接続し、このプロキシサーバは、セキュアデータ伝送トンネルをユーザクライアント16とカメラ10との間で確立することを可能にする。

【0083】

データ伝送トンネルを使用する伝送を、機密性および保全性を達成するために保護する

10

20

30

40

50

ことができる。これは、T L S、S S H、またはI K E / I P s e cなどのプロトコルを介して達成することができる。トンネルを確立する時に、カメラ10は、公開鍵証明書を使用して認証される。公開鍵証明書は、信頼される第三者証明権限当事者によって署名されなければならない、この権限者の署名は、セキュアトンネル確立を受け入れる前にクライアントによって検証されなければならない、そのすべてが、使用される選択されたプロトコル(T L S、S S H、またはI K E / I P s e c)に従う。

【0084】

次に、相互認証が、ユーザクライアント16とカメラ10との間で実行される。ユーザクライアント16は、初期ユーザ鍵 K_{ICU} に基づく情報を含む認証メッセージをユーザクライアント16からカメラ10に送信することによって認証される。これに対して、カメラ10は、ビデオシーケンスが所期のカメラ10によってリアルタイムで取り込まれていることの検証のためにビデオシーケンスをカメラ10からユーザクライアント16に送信することと、カメラ10の認証の確認として確認メッセージをユーザクライアント16からカメラ10に送信することによって認証される。相互認証が失敗する場合には、カメラ10および／またはユーザクライアント16は、認証プロセスを中断する。

【0085】

次に、カメラ10の認証のより詳細な説明を与える。セキュアトンネルが確立された後に、カメラ10は、カメラ10によって記録された1つまたは複数のビデオシーケンス、たとえばJ P E Gイメージのシーケンスをユーザクライアント16に送信する。これらのビデオシーケンスは、トンネル確立時にカメラ認証で使用されたものと同一の公開鍵を用いて署名される。

【0086】

ユーザクライアント16は、署名された1つまたは複数のビデオシーケンスをカメラ10から受信し、それらがセキュアトンネル確立に使用されたものと同一の公開鍵によって署名されていることを検証する。次に、ユーザは、登録ソフトウェアユーザインターフェースによって、1つまたは複数のビデオシーケンスが実際にカメラ10によってリアルタイムで撮影されていることを検証するように求められる。ユーザがこれを確認する場合には、ユーザクライアント16は、セキュアトンネルによって保護された確認メッセージを、カメラ10の認証の確認として送信する。

【0087】

カメラ10とユーザクライアント16との間の認証された関係が確立された時に、動作ユーザ鍵 K_{OCU} が、獲得され、カメラにセットされ、ユーザに配布される。動作ユーザ鍵 K_{OCU} をセットしたことは、カメラ10内でも示される。カメラ10によって作られるメディアデータへのフルアクセス権を有するのは、動作ユーザ鍵 K_{OCU} の所有者だけである。動作ユーザ鍵 K_{OCU} は、カメラ10でこれを生成することによって獲得することができる。動作ユーザ鍵 K_{OCU} の配布を、初期ユーザ鍵 K_{ICU} によって保護することができる。動作ユーザ鍵 K_{OCU} を、カメラに特有とすることができる。

【0088】

相互認証が実行される時に、動作ユーザ鍵 K_{OCU} が、たとえばカメラ10内でのセキュア生成によって、獲得される。動作ユーザ鍵 K_{OCU} を獲得する前に、動作ユーザ鍵 K_{OCU} が既にカメラ10にセットされているか否かをチェックするチェックが実行される。動作ユーザ鍵 K_{OCU} は、動作ユーザ鍵 K_{OCU} がカメラ10にセットされていない場合に限って獲得される。動作ユーザ鍵 K_{OCU} を獲得した後に、動作ユーザ鍵 K_{OCU} は、カメラ10にセットされ、セキュアトンネルによって保護されてユーザクライアント16に送信される。したがって、初期ユーザ鍵 K_{ICU} は、動作ユーザ鍵 K_{OCU} を作るために1回だけ使用される。これは、たとえば、初期ユーザ鍵 K_{ICU} がサービスプロバイダによってユーザに供給される場合であっても、サービスプロバイダがメディアデータの制御を得ることを防ぐ。たとえば、サービスプロバイダが、初期ユーザ鍵 K_{ICU} をユーザに供給する前に、初期ユーザ鍵 K_{ICU} を使用して彼／彼女自身をユーザとして登録する場合に、これは、ユーザによって検出される。というのは、ユーザが、カメラ10によ

って成功して登録することができず、カメラ10に対する制御を得ることができないからである。動作ユーザ鍵 K_{OCU} は、カメラ10内およびユーザクライアント16内にセキュアに格納される。

【0089】

次に、カメラ10は、将来の使用から初期ユーザ鍵 K_{ICU} を非アクティブ化する。したがって、カメラ10は、この初期ユーザ鍵 K_{ICU} をすべての新規の動作ユーザ鍵 K_{OCU} 確立の基礎として受け入れなくなる。これは、たとえば、動作ユーザ鍵 K_{OCU} がセットされていることをカメラ内で示すことによって、または初期ユーザ鍵 K_{ICU} を削除することによって、初期ユーザ鍵 K_{ICU} が使用されたことをカメラ内で示すことによって実行することができる。

10

【0090】

上で説明した手順は、サービスプロバイダが動作ユーザ鍵 K_{OCU} へのアクセスを得るためにユーザの代わりにカメラ10で登録することを選択する場合に、ユーザが通知されることを保証する。一旦真のユーザがこの手順を繰り返すことを試みたならば、その試みは失敗し、ユーザは、サービスプロバイダによって行われた偽装を検出する。

【0091】

本発明の第2の実施形態によれば、動作ユーザ鍵 K_{OCU} を、ユーザクライアント16と複数のカメラ10との間で共有することができる。これは、複数の異なる形で達成することができる。

【0092】

20

1つの代替案によれば、動作ユーザ鍵 K_{OCU} は、カメラ10で生成されるのではなく、ユーザクライアント16で生成され、その後、カメラ10にセキュアに転送される。したがって、ユーザクライアント16は、まさに同一の動作ユーザ鍵 K_{OCU} を複数の異なるカメラ10に転送することができる。

【0093】

第2の代替案によれば、動作ユーザ鍵 K_{OCU} は、やはりカメラ10で生成される。しかし、動作ユーザ鍵 K_{OCU} の生成は、ユーザが彼／彼女のシステムで制御することを望む各カメラを識別する、カメラに特有の識別子、たとえばカメラの通し番号と一緒に、すべてのカメラの間で共有される共通秘密鍵に基づく。各カメラ10で動作ユーザ鍵 K_{OCU} を生成するステップ中に、ユーザは、ユーザが彼／彼女のシステムで制御することを望む各カメラを識別する、カメラに特有の識別子をカメラ10に与え、その結果、同一の一意の秘密鍵がすべてのカメラで生成されることを保証する。ユーザクライアントが、生成プロセス中にカメラに特有の識別子をカメラに与えない場合には、カメラは、登録を拒否する。

30

【0094】

第3の代替案によれば、代替案1と2との組合せが使用される。

【0095】

図3に、本発明の一実施形態によるネットワーク対応デジタルビデオカメラ10を示す。ネットワーク対応デジタルビデオカメラは、デジタルネットワークに接続されるように構成される。デジタルネットワークは、たとえば、サービスプロバイダによって管理されるサーベイランスシステムの一部とすることができる。ネットワークカメラ10は、鍵生成手段50、表示手段52、チェック手段54、暗号化手段56、デジタルネットワークモジュール58、リセット手段60、鍵格納手段62、入出力ポート64、イメージセンサ66、およびイメージプロセッサ68を含む。

40

【0096】

ネットワーク対応デジタルビデオカメラ10でのメディアデータ、たとえばデジタルビデオイメージの生成および入出力ポート64へのメディアデータの供給は、下のよう

50

されたデジタルビデオイメージを、圧縮ユニット（図示せず）に転送することができ、ここで、デジタルビデオイメージが、H. 264、JPEG、M-JPEG、またはMPEGなどの事前定義の標準規格に従って圧縮される。その後、（おそらくは圧縮された）デジタルビデオまたはイメージ信号が、デジタル信号を送信し、受信するように構成されたデジタルネットワークモジュール58に転送される前に、暗号化手段56によって暗号化され、ここで、暗号化されたデジタルビデオまたはイメージ信号（すなわち、暗号化されたメディアデータ）が、処理され、入出力ポート64を介しデジタルネットワークを介する伝送のために準備される。

【0097】

ネットワーク対応デジタルビデオカメラを、オーディオデータを記録するように適合させることもできることに留意されたい。オーディオデータを、デジタルネットワークモジュール58を介して伝送される前に、暗号化手段56によって暗号化することもできる。

【0098】

メディアデータ（すなわち、オーディオデータおよびビデオまたはイメージデータ）は、暗号化手段56によって、動作ユーザ鍵 K_{OCU} に関連するメディア暗号化／復号化鍵によって暗号化される。上で説明したものに従って、メディアデータを動作ユーザ鍵 K_{OCU} に関連するメディア暗号化／復号化鍵によって暗号化することによって、ユーザだけが、メディアデータへのアクセスを有することができる。というのは、サービスプロバイダが、動作ユーザ鍵 K_{OCU} の知識を有しないからである。やはり上記に従って、代替案では、メディアデータ（すなわち、オーディオデータおよびビデオまたはイメージデータ）を、共通鍵 K_C を使用して保護することができる。共通鍵 K_C を使用してメディアデータを保護することによって、ユーザとサービスプロバイダとの両方が、メディアデータへのアクセスを有する。というのは、ユーザとサービスプロバイダとの両方が、共通鍵 K_C の知識を有するからである。

【0099】

さらに、カメラ10によって登録されたか生成されたメタデータ（タイムスタンプ、ビデオトリガリング情報、アラームデータ、または類似物など）を、暗号化手段56によって暗号化することができる。したがって、デジタルネットワークモジュール58は、暗号化されたメタデータを送信するように構成される。上で説明したものに従って、メタデータを、たとえば、共通鍵 K_C に関連するメタデータ暗号化／復号化鍵によって暗号化することができる。メタデータをメタデータ暗号化／復号化鍵によって暗号化することによって、ユーザとサービスプロバイダとの両方が、メタデータへのアクセスを有する。というのは、ユーザとサービスプロバイダとの両方が、共通鍵 K_C の知識を有するからである。したがって、サービスプロバイダは、メタデータへのアクセスを得、したがって、たとえば、アラームおよびレコーディングに関する効率的な検索サービスをユーザに提供することができる。

【0100】

動作ユーザ鍵 K_{OCU} および共通鍵 K_C は、鍵生成手段50によって生成される。鍵生成手段50を、さらに、初期ユーザ鍵 K_{ICU} および／またはサービスプロバイダ鍵 K_{SP} を生成するように構成することができる。初期ユーザ鍵 K_{ICU} 、動作ユーザ鍵 K_{OCU} 、共通鍵 K_C 、およびサービスプロバイダ鍵 K_{SP} は、セキュア鍵生成プロセスを使用して生成される。セキュア鍵生成プロセスは、同一プラットフォーム上で実行される非セキュアソフトウェアにまたはデバイスの直接の物理的タンパリングを介して秘密情報が漏らされるのを防ぐ、保護された実行環境（ハードウェアおよび／またはソフトウェア）内で実行される。

【0101】

生成された鍵は、鍵格納手段62に格納される。たとえばカメラ10の製造業者によって生成された（上を参照されたい）マスタ鍵 K_M も、鍵格納手段62に格納される。

【0102】

上記に従って、初期ユーザ鍵 K_{ICU} を与えられて、マスタ鍵 K_M を導出することが計算的に実現不能になるように、初期ユーザ鍵 K_{ICU} を、適切な第1の一方向関数 f_1 を使用してマスタ鍵 K_M から導出することができる、すなわち、 $K_{ICU} = f_1(K_M)$ とすることができる。同様に、サービスプロバイダ鍵 K_{SP} を与えられて、マスタ鍵 K_M を導出することが計算的に実現不能になるように、サービスプロバイダ鍵 K_{SP} を、適切な第2の一方向関数 f_2 を使用してマスタ鍵 K_M から導出する、すなわち、 $K_{SP} = f_2(K_M)$ とする。さらに、前記適切な第1および第2の一方向関数 f_1 、 f_2 は、追加の第3および第4の一方向関数 f_3 、 f_4 について、共通鍵 K_C を、 $K_C = f_3(K_{ICU}) = f_4(K_{SP})$ に従って導出できるように構成される。したがって、共通鍵 K_C を、第3の一方向関数 f_4 によって初期ユーザ鍵 K_{ICU} から導出することができ、すなわち、 $K_C = f_3(K_{ICU})$ とすることができ、あるいはその代わりに、共通鍵 K_C を、第4の一方向関数 f_3 によってサービスプロバイダ鍵 K_{SP} から導出することができる、すなわち、 $K_C = f_4(K_{SP})$ とすることができる。第3の一方向関数 (f_3) および第4の一方向関数 (f_4) は、共通鍵 K_C が非公開の初期ユーザ鍵 K_{ICU} とサービスプロバイダ鍵 K_{SP} のうちのどちらから導出されるには関係なく、同一の共通鍵 K_C を作る (すなわち、 $K_C = f_3(K_{ICU}) = f_4(K_{SP})$) ように構成される。

10

【0103】

さらに、上記に従って、サービスプロバイダ (サービスプロバイダ管理サーバ17の形の) は、サービスプロバイダ鍵 K_{SP} を与えられ、ユーザ (たとえば、ユーザクライアント16の形の) は、初期ユーザ鍵 K_{ICU} を与えられる。

20

【0104】

カメラ10へのアクセスを得る前に、ユーザは、カメラ10で、ユーザであるものとして彼自身を認証する必要がある。認証中に、ユーザクライアント16とカメラ10との間の認証された関係が、確立される。ユーザは、初期ユーザ鍵 K_{ICU} に基づく情報を含む認証メッセージをユーザクライアント16からカメラ10に送信することによって認証される。カメラは、ビデオシーケンスが所期のカメラ10によってリアルタイムで取り込まれていることの検証のためにビデオシーケンスをカメラ10からユーザクライアント16に送信することと、カメラの認証の確認として確認メッセージをユーザクライアント16からカメラ10に送信することとによって認証される。

30

【0105】

カメラ10とユーザクライアント16との間の認証された関係が確立された時に、チェック手段54は、動作ユーザ鍵 K_{OCU} がカメラ10にセットされているかどうかをチェックするように構成される。これは、たとえば、表示手段52が、動作ユーザ鍵 K_{OCU} がセットされていることを示したかどうかをチェックすることによって実行することができる。

【0106】

さらに、チェック手段54によって実行されるチェックからの結果が、動作ユーザ鍵 K_{OCU} がカメラ10にセットされていることである場合には、動作ユーザ鍵 K_{OCU} が既にカメラ10にセットされていることを示すメッセージが、ユーザクライアントに送信される。ユーザは、その場合に、カメラ10にセットされた動作ユーザ鍵 K_{OCU} を削除することによってカメラ10のセキュリティセッティングをリセットし、認証プロセスからやり直すことができる。代替案では、ユーザは、その場合に、カメラ10にセットされた動作ユーザ鍵 K_{OCU} を削除することによってカメラ10のセキュリティセッティングをリセットし、生成される新しい動作ユーザ鍵 K_{OCU} を獲得し、カメラ10にセットすることができる、上を参照されたい。リセットは、リセット手段60によって実行することができる。リセット手段60は、セットされている動作ユーザ鍵 K_{OCU} をリセットするように構成される。リセット手段60は、リセットボタンを含むことができる。

40

【0107】

その代わりに、チェック手段54によって実行されるチェックからの結果が、動作ユーザ鍵 K_{OCU} がカメラ10にセットされていないことである場合には、動作ユーザ鍵 K_{OCU}

50

K_{OCU} が、鍵生成手段 50 によって生成される。さらに、動作ユーザ鍵 K_{OCU} が生成される時に、その動作ユーザ鍵 K_{OCU} は、鍵格納手段 62 によってカメラにセットされると同時に、表示手段 52 によって、動作ユーザ鍵 K_{OCU} がカメラにセットされていることが示される。したがって、表示手段 52 は、動作ユーザ鍵 K_{OCU} が生成されたかどうかを示すように構成される。表示手段 52 を、一実施形態に従って、動作ユーザ鍵 K_{OCU} が生成済みである場合に初期ユーザ鍵 K_{ICU} をさらなる使用から削除するように構成することができる。その代わりに、表示手段 52 を、動作ユーザ鍵 K_{OCU} が生成されたかどうかを示すフラグをセットするように構成することができる。

【0108】

生成され、カメラにセットされた後に、動作ユーザ鍵 K_{OCU} は、ユーザクライアント 16 に、したがってユーザに送信される。カメラ 10 への、したがってカメラ 10 によって作られるメディアデータへのフルアクセス権を有するのは、動作ユーザ鍵 K_{OCU} の所有者だけである。

【符号の説明】

【0109】

- 10 ネットワークビデオカメラ
- 11 プライベートネットワーク
- 12 インターネット
- 13 NAT
- 14 ファイアウォール
- 15 ローカルストレージユニット
- 16 ユーザクライアント
- 17 サービスプロバイダ管理サーバ
- 18 サービスプロバイダストレージユニット
- 19 サービスプロバイダネットワーク
- 50 鍵生成手段
- 52 表示手段
- 54 チェック手段
- 56 暗号化手段
- 58 デジタルネットワークモジュール
- 60 リセット手段
- 62 鍵格納手段
- 64 入出力ポート
- 66 イメージセンサ
- 68 イメージプロセッサ
- K_C 共通鍵
- K_{ICU} 初期ユーザ鍵
- K_M マスタ鍵
- K_{OCU} 動作ユーザ鍵
- K_{SP} サービスプロバイダ鍵

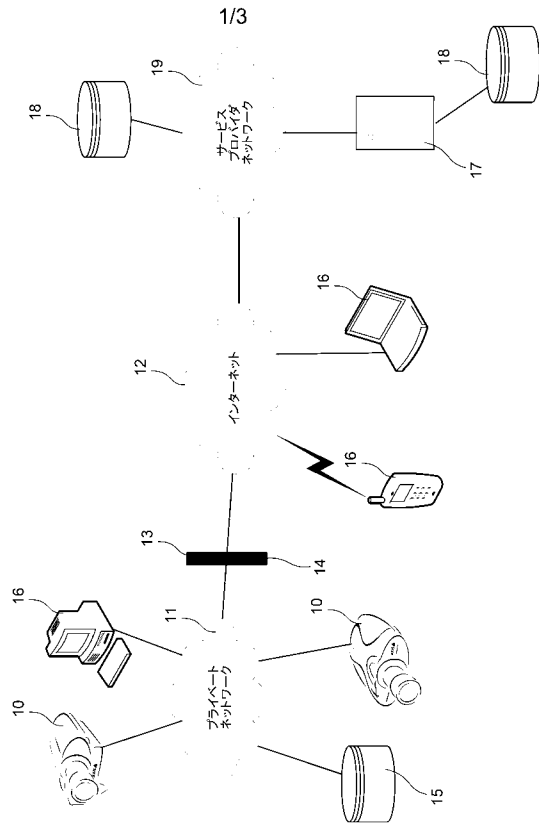
10

20

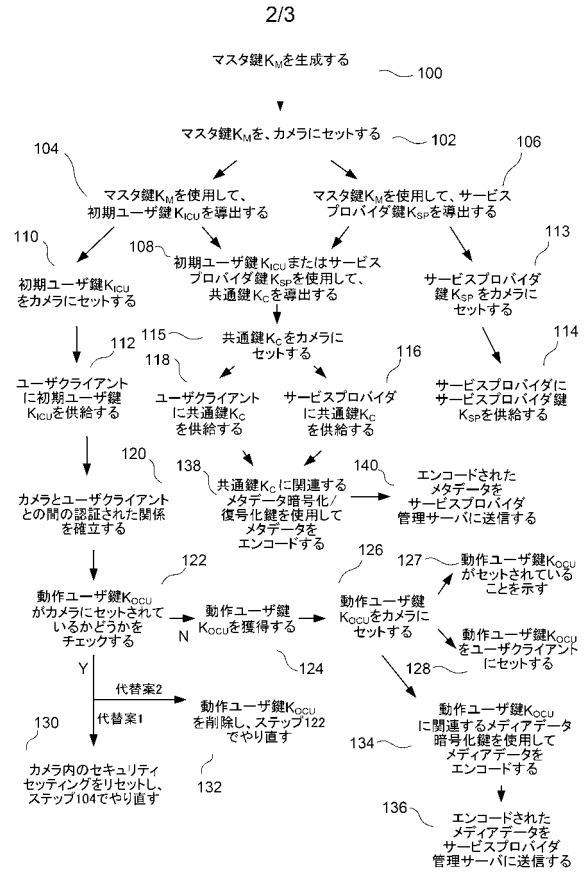
30

40

【図 1】

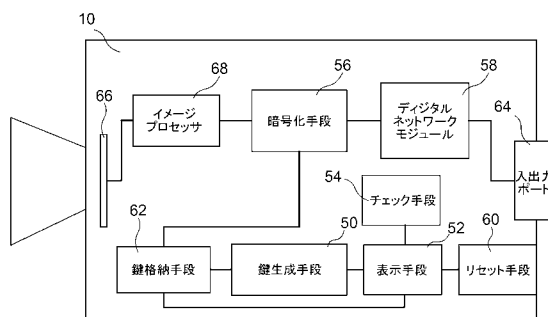


【図 2】



【図 3】

3/3



フロントページの続き

- (72)発明者 クリスチャン ゲールマン
スウェーデン国 エスエー 227 38 ルンド, スケルデヴェーイェン 2 セー
- (72)発明者 フレドリック ターネロット
スウェーデン国 エスエー 223 53 ルンド, リラ トヴェルガタン 19

審査官 松平 英

- (56)参考文献 特開2007-156812 (JP, A)
特開2008-59561 (JP, A)
特開2008-5095 (JP, A)

- (58)調査した分野(Int.Cl., DB名)
- | | |
|------|-------|
| G09C | 1/00 |
| H04L | 9/00 |
| G06F | 21/24 |
| H04N | 5/78 |
| H04N | 5/91 |
| H04N | 5/225 |
| H04N | 7/167 |
| H04N | 7/18 |