(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2007-329688
(P2007-329688A)
(43)公開日　平成19年12月20日(2007.12.20)

(51)Int.Cl.			F I			テーマコード（参考）
H04L	9/32	(2006.01)	H04L	9/00	675A	5J104
G09C	1/00	(2006.01)	G09C	1/00	640E	
H04L	9/08	(2006.01)	H04L	9/00	601C	

審査請求 未請求　請求項の数 11　ＯＬ　（全 14 頁）

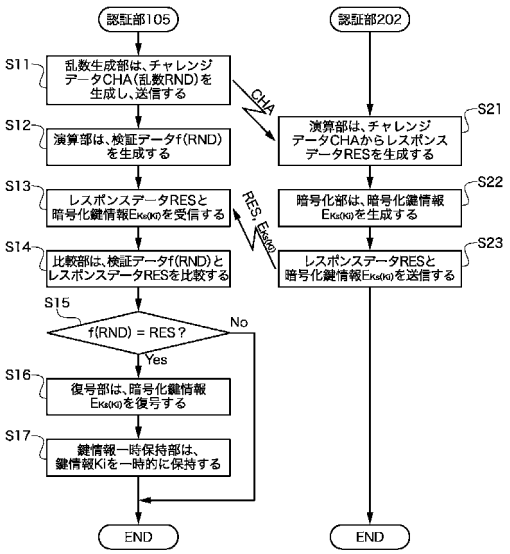
(21)出願番号　特願2006-159144 (P2006-159144)
(22)出願日　平成18年6月7日 (2006.6.7)

(71)出願人　000001007
キヤノン株式会社
東京都大田区下丸子３丁目３０番２号
(74)代理人　100076428
弁理士　大塚　康徳
(74)代理人　100112508
弁理士　高柳　司郎
(74)代理人　100115071
弁理士　大塚　康弘
(74)代理人　100116894
弁理士　木村　秀二
(72)発明者　田頭　信博
東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内

最終頁に続く

(54)【発明の名称】データ処理装置およびその方法

(57)【要約】
【課題】　攻撃に強く、手続が簡単な機器間認証を実現する。
【解決手段】　画像入力装置の認証部105は、情報保持デバイスの認証部202にチャレンジデータを送信し(S11)、チャレンジデータから生成されたレスポンスデータおよび暗号化鍵情報を認証部202から受信する(S13)。認証部105は、チャレンジデータとレスポンスデータに基づき前記相手機器を認証し(S14、S15)、認証が成功した場合、暗号化鍵情報を復号して鍵情報を取得する(S16)。
【選択図】　図3



【特許請求の範囲】
【請求項１】
相手機器にチャレンジデータを送信する送信手段と、
前記チャレンジデータから生成されたレスポンスデータおよび暗号化鍵情報を前記相手機器から受信する受信手段と、
前記チャレンジデータと前記レスポンスデータに基づき前記相手機器を認証する認証手段と、
前記認証が成功した場合、前記暗号化鍵情報を復号して鍵情報を取得する復号手段とを有することを特徴とするデータ処理装置。
【請求項２】
さらに、前記復号した鍵情報を予め定められた期間保持する保持手段を有することを特徴とする請求項1に記載されたデータ処理装置。
【請求項３】
さらに、前記鍵情報を用いてデータを暗号化し、その暗号化データを前記相手機器に送信する暗号手段を有することを特徴とする請求項1または請求項2に記載されたデータ処理装置。
【請求項４】
前記相手機器は、前記鍵情報または前記暗号化鍵情報を記憶し、前記暗号化データを記憶可能なメモリカードであることを特徴とする請求項3に記載されたデータ処理装置。
【請求項５】
相手機器からチャレンジデータを受信する第一の受信手段と、
前記チャレンジデータからレスポンスデータを生成する生成手段と、
前記レスポンスデータおよび暗号化鍵情報を前記相手機器に送信する送信手段とを有することを特徴とするデータ処理装置。
【請求項６】
さらに、前記暗号化鍵情報を復号して得られる鍵情報により暗号化されたデータを受信する第二の受信手段を有することを特徴とする請求項5に記載されたデータ処理装置。
【請求項７】
さらに、前記鍵情報または前記暗号化鍵情報を記憶し、前記第二の受信手段が受信した暗号化データを記憶可能なメモリを有することを特徴とする請求項6に記載されたデータ処理装置。
【請求項８】
相手機器にチャレンジデータを送信し、
前記チャレンジデータから生成されたレスポンスデータおよび暗号化鍵情報を前記相手機器から受信し、
前記チャレンジデータと前記レスポンスデータに基づき前記相手機器を認証し、
前記認証が成功した場合、前記暗号化鍵情報を復号して鍵情報を取得することを特徴とするデータ処理方法。
【請求項９】
相手機器からチャレンジデータを受信し、
前記チャレンジデータからレスポンスデータを生成し、
前記レスポンスデータおよび暗号化鍵情報を前記相手機器に送信することを特徴とするデータ処理方法。
【請求項１０】
データ処理装置を制御して、請求項8または請求項9に記載されたデータ処理を実現することを特徴とするコンピュータプログラム。
【請求項１１】
請求項10に記載されたコンピュータプログラムが記録されたことを特徴とするコンピュータが読み取り可能な記録媒体。
【発明の詳細な説明】

【技術分野】
【０００１】
本発明は、相互接続された機器間における認証および暗号化に関する。
【背景技術】
【０００２】
近年、ディジタルカメラを利用した写真撮影が普及した。その理由として、ディジタルカメラで撮影した画像は経年劣化がない、保管、検索が容易、遠隔地への伝送が容易などが挙げられる。
【０００３】
そして、半導体プロセスの進歩により画像データを記録するメモリカードの容量が急速に増加し、近年はギガバイトクラスのメモリカードも一般的になり、大量の画像データを一枚のメモリカードに記録できるようになった。その反面、メモリカードの紛失や盗難によって、一度に大量の画像データが流出する懸念がある。一度に大量の画像データが流出すれば、プライバシ保護の観点からも重大な問題である。
【０００４】
画像データの流出を防ぐ対策の一つとして、ディジタルカメラで撮影した画像をディジタルカメラ内で暗号化し、暗号化した画像データをメモリカードに記録する方法が提案されている。暗号化を有効に機能させるには、暗号化に必要な鍵情報を安全に管理しなければならない。ディジタルカメラ内の鍵情報の管理方法として下記が考えられる。
(1) 鍵情報をディジタルカメラ内で管理する方法
(2) 暗号化時に、ディジタルカメラ外から鍵情報を入力する方法
【０００５】
以下では、(1)の方法を「内部鍵方式」、(2)の方法を「外部鍵方式」と呼ぶ。
【０００６】
●内部鍵方式
内部鍵方式は、暗号アルゴリズムの分類に応じて「共通鍵暗号方式型」と「公開鍵暗号方式型」の二つに分類することができる。
【０００７】
共通鍵暗号方式型の内部鍵方式は、共通鍵を暗号側と復号側だけで秘密に保持する方式である。この方式で、PCによる暗号化画像データの利用を想定すると、ディジタルカメラ内に秘密に保持する共通鍵をPCと共有しなければならない。
【０００８】
また、公開鍵暗号方式型の内部鍵方式は、暗号化鍵（公開鍵）と復号鍵（秘密鍵）を異ならせ、暗号化鍵を公開することが可能な方式である。ディジタルカメラは暗号化に必要な公開鍵を管理するが、公開鍵暗号方式の特性からその管理は極めて容易である。しかし、公開鍵暗号方式は、共通鍵暗号方式と比べて処理負荷が非常に大きい。一方、ディジタルカメラの処理能力は小さく、公開鍵暗号方式の処理負荷が問題になる。
【０００９】
●外部鍵方式
外部鍵方式は、鍵情報を管理するエンティティに応じて「人型」と「デバイス型」の二つに分類することができる。
【００１０】
人型の外部鍵方式は、暗号化時に、ユーザがディジタルカメラに鍵情報を入力する方式である。暗号化を有効に機能させるには、一定以上のランダム性をもつ鍵情報（例えば所定長以上のPIN）を利用する。しかし、ディジタルカメラはダイヤルやボタンなど、限られたユーザインタフェイスしかもたない。このため、ディジタルカメラのユーザインタフェイスを介した鍵情報の入力には、実用上の難点がある。
【００１１】
また、デバイス型の外部鍵方式は、鍵情報を保持するデバイスをディジタルカメラに装着し、暗号化時にデバイスから鍵情報を読み込む方式である。この方式は、スマートカー

ドのように破壊攻撃などに耐性を有し、処理能力も有するデバイスの利用など、鍵情報を管理するための様々な特性をもつデバイスの利用が可能になる。

【００１２】

例えば、MOPASS (mobile passport)カードと呼ばれるデバイスがある。MOPASSカードは、フラッシュメモリとスマートカードを一体化したカードで、フラッシュメモリと同等の物理形状を有する。MOPASSカードを利用することで、ディジタルカメラに新たな物理的なインタフェイスを設けることなく、スマートカードと同等の攻撃耐性を有するデバイスを利用することができる。攻撃耐性を有するデバイスを利用することで、デバイスが保持する鍵情報は安全であると見做すことができる。

【００１３】

●機器間認証

ディジタルカメラとデバイスのセットの観点からすると、ディジタルカメラに装着したデバイスが所望の鍵情報が記録されたデバイスか否かが問題になる。この対策として、ISO/IEC9798シリーズに示される機器間認証（または相手認証）がある。機器間認証によれば、鍵情報を保持するデバイスをディジタルカメラに装着して利用する場合、ディジタルカメラは所望の鍵情報を保持する正しいデバイスか、かつ、デバイスは鍵情報を出力してよいディジタルカメラかを確認する。つまり、相互に認証を行う。

【００１４】

ディジタルカメラの利用形態はネットワークに非接続が多いと考えられる。従って、認証に第三者機関を利用することはできない。ISO/IEC9798シリーズに示される認証方式の中で、第三者機関を利用しない相互認証方式は次のようになる。

共通鍵暗号方式を用いる2パス認証方式 (ISO/IEC9798-2)

【００１５】

エンティティAとBは秘密鍵Kを共有する。Aは、Kで暗号化したメッセージM（$E_K(M)$）をBへ送信する。Bは、暗号化メッセージ$E_K(M)$を復号し、Mの確からしさを検証してAを認証する。同様の手順を逆方向に実行し、AはBを認証する。

共通鍵暗号方式を用いる3パス認証方式 (ISO/IEC9798-2)

【００１６】

エンティティAとBは秘密鍵Kを共有する。Aはチャレンジ/レスポンス方式でBを認証する。なお、Bは、Kと共通鍵暗号方式を用いてレスポンスを生成にする。同様の手順を逆方向に実行し、BはAを認証する。ただし、BがAにレスポンスを返す時は、チャレンジを加えることでパスを一つ削除することができる。特許3526521などにも利用されている方式である。

公開鍵暗号方式を用いる2パス認証方式 (ISO/IEC9798-3)

【００１７】

エンティティAは、ディジタル署名を付加したメッセージMをエンティティBへ送信する。Bは、Aの公開鍵でMのディジタル署名を検証してAを認証する。同様の手順を逆方向に実行し、AはBを認証する。

公開鍵暗号方式を用いる3パス認証方式 (ISO/IEC9798-3)

【００１８】

上記の共通鍵暗号方式を用いる3パス認証方式 (ISO/IEC9798-2)と同様のチャレンジ/レスポンス方式であるが、レスポンスの生成にディジタル署名を用いる。

MACを用いる2パス認証方式 (ISO/IEC9798-4)

【００１９】

上記の共通鍵暗号方式を用いる2パス認証方式 (ISO/IEC9798-2)と同様の認証方式であるが、暗号化メッセージ$E_K(M)$の代わりに、MAC (message authentication code)を生成する。

MACを用いる3パス認証方式 (ISO/IEC9798-4)

【００２０】

上記の共通鍵暗号方式を用いる3パス認証方式 (ISO/IEC9798-2)と同様のチャレンジ/レ

スポンス方式であるが、レスポンスの生成にMACを用いる。
【００２１】
●ディジタルカメラにおける問題
デバイス型の外部鍵方式に機器間認証を単純に組み合わせて、ディジタルカメラ内で画像を暗号化する方法は、以下の問題が残る。
【００２２】
第一に、機器間認証が問題になる。つまり、ディジタルカメラが鍵を保持するデバイスを認証し、かつ、デバイスがディジタルカメラを認証する、二度の認証（相互認証）を実施しなければならない。加えて、ディジタルカメラとデバイスの双方に認証機能をもたせる必要がある。つまり、処理手続および機能実装の観点で冗長になる問題がある。
【００２３】
第二に、ディジタルカメラに外部から鍵情報を受信する機能が必要になる。第一の問題と同様に、処理手続および機能実装の観点で複雑になる問題がある。
【００２４】
●機器間認証の問題
機器間認証に関して、単純に従来方式を組み合わせた場合、以下の問題がある。
【００２５】
2パス認証方式は本質的に再送攻撃に対抗できない。例えば、共通鍵暗号方式を用いる2パス認証方式 (ISO/IEC9798-2)の場合、攻撃者はエンティティAとBの間の通信路を盗聴し、暗号化メッセージ$E_K(M)$を取得し、$E_K(M)$をBに再送する。これによって、攻撃者はAになりすますことが可能である。
【００２６】
また、3パス認証方式は、機器間認証を完了するまでに、3パスのメッセージ交換（手続）が必要になり、時間がかかる。
【００２７】
【特許文献１】特許3526521公報
【発明の開示】
【発明が解決しようとする課題】
【００２８】
本発明は、攻撃に強く、手続が簡単な機器間認証の実現を目的とする。
【課題を解決するための手段】
【００２９】
本発明は、前記の目的を達成する一手段として、以下の構成を備える。
【００３０】
本発明にかかるデータ処理は、相手機器にチャレンジデータを送信し、前記チャレンジデータから生成されたレスポンスデータおよび暗号化鍵情報を前記相手機器から受信し、前記チャレンジデータと前記レスポンスデータに基づき前記相手機器を認証し、前記認証が成功した場合、前記暗号化鍵情報を復号して鍵情報を取得することを特徴とする。
【００３１】
また、相手機器からチャレンジデータを受信し、前記チャレンジデータからレスポンスデータを生成し、前記レスポンスデータおよび暗号化鍵情報を前記相手機器に送信することを特徴とする。
【発明の効果】
【００３２】
本発明によれば、攻撃に強く、手続が簡単な機器間認証の実現することができる。
【発明を実施するための最良の形態】
【００３３】
以下、本発明にかかる実施例の情報処理を図面を参照して詳細に説明する。
【実施例１】
【００３４】

［認証システムの構成］
図1は機器間認証機能を有する画像処理装置の構成例を示すブロック図である。
【００３５】
画像処理装置は、ディジタルカメラなどの画像入力装置10およびスマートカードなどの攻撃耐性のある情報保持デバイス20から構成される。なお、画像処理装置の実現に当り、図1に示す全構成要素の使用は必須ではない。また、画像入力装置10で撮影する画像は静止画像に限らず、動画像も含む。
【００３６】
●画像入力装置
画像入力装置10において、撮像素子101は、CCDやCMOSセンサなど、レンズ102を介して入力される光を電気信号に変換する。表示部103は、液晶モニタや複数の表示パネルに画像データ、画像入力装置10の各種設定値および状態を表示する。操作部104は、各種ボタンや設定ダイヤルなどを備え、画像入力装置10の利用者の各種指示を入力する。
【００３７】
制御演算部108は、RAM 109をワークメモリとして、ROM 110に格納されたプログラムを実行して、画像入力装置10の各部を制御する。また、撮像素子101が出力する電気信号のディジタル変換、ディジタル信号の符号化や圧縮処理などの画像処理を実行し、撮影画像の画像データを生成する。
【００３８】
暗号処理部107は、認証部105が保持する鍵情報を暗号鍵として制御演算部108が生成した画像データを暗号化する。なお、暗号化アルゴリズムは、AES (advanced encryption standard)などの様々な共通鍵暗号方式を利用することができる。
【００３９】
認証部105は、情報保持デバイス20の正当性を認証する。そして、詳細は後述するが、情報保持デバイス20を認証した場合、情報保持デバイス20から受信した暗号化鍵情報を復号して、復号した鍵情報を一時的に保持する。
【００４０】
鍵情報の保持期間は、認証の正当性の維持期間と一致させることができる。例えば、暗号処理部107の処理ごとに認証を行い、鍵情報を保持し、鍵情報が利用された後、鍵情報を消去してもよい。また、画像入力装置10に情報保持デバイス20が接続（または装着）される度に認証を行い、鍵情報を保持する。そして、画像入力装置10と情報保持デバイス20の接続（または装着）が解除されるまで鍵情報を保持し続けてもよい。さらに、鍵情報にチェックサムやハッシュ値などの完全性を検証する情報が付加されている場合、鍵情報の完全性を検証し、情報保持デバイス20の正当性を認証し、かつ、復号した鍵情報の完全性を検証した場合に鍵情報を一時的に保持することもできる。
【００４１】
インタフェイス(I/F) 106は、情報保持デバイス20とのインタフェイスを提供する。情報保持デバイス20に応じた物理形状、コネクタなどを有する。また、画像入力装置10に情報保持デバイス20を直接装着するのでなければ、例えばUSBやIEEE1394等のシリアルバスインタフェイス、有線、無線または赤外線の通信インタフェイスでも構わない。
【００４２】
●情報保持デバイス
情報保持デバイス20の制御部204は、記録部203、I/F 201を制御する。記録部203は、画像データなどを保持する不揮発性メモリである。認証部202は、詳細は後述するが、画像入力装置10に対して情報保持デバイス20の正当性を証明するとともに、保持する鍵情報を暗号化して画像入力装置10に送信する。I/F 201は、画像入力装置10のI/F 106と対応するインタフェイスである。
【００４３】
［機器間認証用の構成］
図2は、図1に示す認証部105と202の構成例を示すブロック図である。

【００４４】
認証部105の乱数生成部111は、乱数RNDを発生し、これを内部に一時的に保持するとともに、チャレンジデータCHAとしてI/F 106を介して認証部202へ送信する。
【００４５】
演算部112は、乱数生成部111に一時的に保持された乱数RNDから検証データf(RND)を生成する。検証データを生成する関数f()は、演算部211と秘密に共有する関数で、入力データから特定の出力データを生成することで、相手の認証が可能な関数である。例えば、関数f()は、画像入力装置10と情報保持デバイス20の間で共有するシステム鍵Ksを鍵とした暗号化関数やMAC (message authentication code)によって実現することができる。
【００４６】
比較部113は、情報保持デバイス20の正当性を検証する。つまり、認証部202から受信したレスポンスデータRESと、演算部112が生成した検証データf(RND)を比較し、これらデータが一致する場合、情報保持デバイス20の正当性の検証に成功したと判断して復号部115を動作させる。また、RESとf(RND)が一致しない場合は、情報保持デバイス20の正当性の検証に失敗したと判断して復号部115を動作させない。
【００４７】
復号部115は、認証部202から受信した暗号化鍵情報E_{Ks}(Ki)を復号し、画像データの暗号化に用いる鍵情報Kiを得る。復号に利用する鍵は、システム鍵保持部116が保持するシステム鍵Ksである。また、暗号アルゴリズムは、認証部202の暗号化部212が利用する暗号アルゴリズムに対応し、AESなどの様々な共通鍵暗号方式が利用可能である。さらに、鍵情報にチェックサムやハッシュ値などの完全性を検証するための情報が付加されている場合は完全性を検証することもできる。
【００４８】
鍵情報一時保持部114は、復号部115によって得られた鍵情報Kiを一時的に保持する。システム鍵保持部116は、画像入力装置10と情報保持デバイス20の間で共有するシステム鍵Ksを保持する。勿論、システム鍵Ksの保持は機密性と完全性が要求される。また、システム鍵Ksは、暗号化部212や復号部115の暗号アルゴリズムに依存する形式の鍵情報である。例えば、暗号アルゴリズムとしてAESを利用した場合は128ビット長などの鍵情報になる。
【００４９】
認証部202の演算部211は、I/F 201を介して認証部105からチャレンジデータCHAを受信する。そして、レスポンスデータRES(=f(CHA))を生成し、I/F 201を介して認証部105へ送信する。なお、レスポンスデータを生成する関数f()は、演算部112が検証データの生成に使用する関数f()と同一である。
【００５０】
鍵情報保持部213は、画像データの暗号化に用いる鍵情報Kiを保持する。勿論、鍵情報Kiの保持は機密性と完全性が要求される。また、チェックサムやハッシュ値を鍵情報に含めることによって、鍵情報の完全性を検証することが可能になる。
【００５１】
暗号化部212は、鍵情報保持部213が保持する鍵情報Kiを暗号化する。暗号化に利用する鍵は、システム鍵保持部214が保持するシステム鍵Ksである。また、暗号アルゴリズムは、認証部105の復号部115が利用する暗号アルゴリズムに対応する。
【００５２】
システム鍵保持部214は、システム鍵保持部116と同様に、画像入力装置10と情報保持デバイス20の間で共有するシステム鍵Ksを保持する。なお、システム鍵保持部214が暗号化鍵情報E_{Ks}(Ki)を保持するように構成すれば、暗号化部212を省略することが可能である。
【００５３】
［機器間認証］
図3は認証部105と212が実行する機器間認証処理の一例を示すフローチャートである。
【００５４】
まず、認証部105において、乱数生成部111は、チャレンジデータCHAとして乱数RNDを生

成し、演算部112および認証部202へ送信する(S11)。演算部112は、受信した乱数RNDから検証データf(RND)を生成する(S12)。

【００５５】

一方、認証部202において、演算部211は、認証部105から受信したチャレンジデータCHAからレスポンスデータRESを生成する(S21)。また、暗号化部212は、システム鍵保持部214が保持するシステム鍵Ksを鍵として、鍵情報保持部213が保持する鍵情報Kiを暗号化して、暗号化鍵情報E_{Ks}(Ki)を生成する(S22)。そして、認証部202は、ステップS21で生成したレスポンスデータRESと、ステップS22で生成した暗号化鍵情報E_{Ks}(Ki)を認証部105へ送信する(S23)。

【００５６】

認証部105がレスポンスデータRESと暗号化鍵情報E_{Ks}(Ki)を受信すると(S13)、比較部113は、ステップS12で生成した検証データf(RND)と、受信したレスポンスデータRESを比較する(S14)。それらが一致しない場合は処理を終了する。

【００５７】

検証データf(RND)とレスポンスデータRESが一致した場合(S15)、つまり検証に成功すると、復号部115は、システム鍵保持部116が保持するシステム鍵Ksを鍵として、受信した暗号化鍵情報E_{Ks}(Ki)を復号する(S15)。そして、鍵情報一時保持部114は、復号によって得られた鍵情報Kiを一時的に保持する(S16)。

【００５８】

なお、鍵情報保持部213が暗号化鍵情報E_{Ks}(Ki)を保持する場合、ステップS22を省略することができる。

【００５９】

［画像入力］

次に、画像入力装置10が画像を入力する際の暗号化を説明する。図4は入力画像の暗号化処理の一例を示すフローチャートである。

【００６０】

制御演算部108は、画像入力装置10のユーザが操作部104に配置されたシャッタボタンを押す（または、PCを介してリモートでシャッタを操作していもよい）と、撮影素子101などを制御し、画像処理を実行して画像データを生成する(S31)。なお、画像データはRAM 109に格納される。

【００６１】

次に、認証部105は、上述した機器間認証に関わる処理を開始し(S32)、認証部202から暗号化鍵情報E_{Ks}(Ki)などを受信する(S33)。そして、情報保持デバイス20の認証に成功すると(S34)、暗号化鍵情報E_{Ks}(Ki)を復号して鍵情報kiを取得する(S35)。

【００６２】

次に、暗号処理部107は、認証部105が保持する鍵情報kiを使用して、RAM 109に格納された画像データを暗号化する(S36)。なお、機器間認証に失敗し、認証部105が鍵情報を保持しない場合、暗号処理部107は、暗号化処理を行わない。また、暗号化画像データはRAM 109に格納される。

【００６３】

制御演算部108は、RAM 109に格納された暗号化画像データを、I/F 106を介して、情報保存デバイス204に出力する(S37)。情報保存デバイス20の制御部204は、画像入力装置10から暗号化画像データを受信すると当該データを記録部203に格納する。なお、認証部105が鍵情報を保持しない場合など暗号処理部107が暗号化処理に失敗した場合、制御演算部108は、暗号化していない画像データを出力する場合と、画像データを出力しない場合の二通りが考えられる。どちらを採用するかは、画像入力装置10の制御方針またはセキュリティ方針に依存する。

【００６４】

図4に示す処理は、シャッタボタンの操作（画像入力指示）ごとに機器間認証を実施する。しかし、先述したように、鍵情報の保持期間は、情報保持デバイス20を画像入力装置

10に接続（または装着）している間など様々に設定可能である。例えば、認証部105は、情報保持デバイス20が画像入力装置10に接続されると、機器間認証を実行して鍵情報を保持する。そして、情報保持デバイス20と画像入力装置10の接続（または装着）が解除されまで鍵情報を保持し続ける場合が考えられる。予め鍵情報を保持した認証部105は、画像入力指示ごとに機器間認証は行うことはない。また、接続、装着のほかにも、情報保持デバイス20を画像入力装置10に装着し状態で、画像入力装置10の電源を投入する場合が考えられる。同様に、接続（または装着）の解除のほかにも、画像入力装置10の電源断が考えられる。

【００６５】

また、上記では、暗号化画像データを情報保持デバイス20の記録部203に格納する例を説明した。しかし、暗号化画像データと鍵情報Kiをセットで保存する必要はない。従って、暗号化画像データの出力先として、情報保持デバイス20のほかに様々なメモリカードを利用することができる。ただし、暗号化画像データの利用には、鍵情報Kiを保持する情報保持デバイス20が必須である。

【００６６】

また、上記では、撮像素子101によって撮影した画像データの暗号化を説明した。しかし、本発明は、撮像素子101によって撮影された画像データに限らず、他の機器からデータファイルとして入力される画像データなどにも適用可能である。また、本発明の機器間認証および鍵の取得方法は、暗号化に限らず、復号、MAC生成などにも適用可能である。

【００６７】

このように、本実施例は、機器間認証後の処理が情報保持デバイス20から画像入力装置10への鍵情報の送信であることに着目する。そして、画像入力装置10から情報保持デバイス20の認証にチャレンジ/レスポンス認証方式を、逆方向の認証にメッセージ認証方式を用いて、相互認証と鍵情報の転送を同時に実現する。なお、メッセージ認証方式は、共有するシステム鍵Ksで鍵情報を暗号化して送信する方式である。

【００６８】

さらに、本実施例は、チャレンジ/レスポンス認証方式のメッセージ交換にメッセージ認証方式のメッセージを含めることで再送攻撃を防ぎ、2パスのメッセージ交換で相互認証を実現する。

【００６９】

つまり、本実施例の機器間認証は、まず、画像入力装置10がチャレンジ/レスポンス方式によって、処理前に、情報保持デバイス20を認証（片側認証）する。次に、情報保持デバイス20がメッセージ認証方式によって暗号化に使用する鍵Kiを画像入力装置10に供給する。言い替えれば、この時点で鍵の共有が実現する。従って、処理後のデータ（暗号化画像データ）は、正しい情報保持デバイス20だけが利用可能（復号可能）なデータになる、という形態で画像入力装置10の認証（相互認証）が実現する。

【００７０】

また、一般に効率的な相互認証方式は、同一の脅威に対抗する必要があるため、同じ認証方式を双方から実行する必要がある。異なる認証方式を単純に組み合わせた相互認証方式の場合、各認証方式の特徴の差が脆弱性となる可能性がある。しかし、本実施例は、認証後の処理に特化することにより、異なる認証方式を組み合わせることが可能になる。さらに、本実施例は、異なる認証方式で送信されるメッセージを結合することで、メッセージ認証方式の欠点である再送攻撃を防ぎ、チャレンジ/レスポンス認証方式の欠点であるメッセージ交換回数を削減することができる。

【実施例２】

【００７１】

以下、本発明にかかる実施例2の情報処理を説明する。なお、実施例2において、実施例1と略同様の構成については、同一符号を付して、その詳細説明を省略する。

【００７２】

実施例1の認証の手順において、認証部202から認証部105に送信されるデータはレスポ

ンスデータRESと暗号化鍵情報E_{Ks}(Ki)である。当該データは全体としては認証ごとに異なる。しかし、レスポンスデータRESは乱数であるチャレンジデータCHAに応じて認証ごとに異なるが、固定値の鍵情報Kiとシステム鍵情報Ksから生成される暗号化鍵情報は固定値である。実施例2では、この点に着目し、暗号化鍵情報を固定値としない方法を説明する。

【００７３】

［機器間認証用の構成］

図5は実施例2における認証部105と202の構成例を示すブロック図である。

【００７４】

認証部202の暗号化部212は、システム鍵保持部214が保持するシステム鍵Ksとチャレンジデータ CHAを排他的論理和したデータを鍵として暗号化情報E_{Ks}(Ki)を暗号化する。また、認証部105の復号部115は、システム鍵保持部116が保持するシステム鍵Ksとチャレンジデータ CHAを排他的論理和したデータを鍵として暗号化情報E_{Ks}(Ki)を復号する。

【００７５】

なお、復号部115と暗号化部212が使用する鍵を生成する方法は、一対の方法であって、双方で同じ鍵が得られなければならない。勿論、同じ鍵が得られれば、他の方法を利用することが可能である。上記では、システム鍵Ksとチャレンジデータ CHAを排他的論理和して鍵を生成する方法を示すが、各データを排他的論理積する方法、データを結合してハッシュ値を得る方法など様々な二入力の関数を利用することができる。

【００７６】

また、鍵の生成方法は、システム鍵Ksとチャレンジデータ CHAの利用に限らず、システム鍵Ksとレスポンスデータ RESの利用、システム鍵Ks、チャレンジデータ CHAおよびレスポンスデータ RESの三つのデータの利用でもよい。とくに、レスポンスデータ RESを利用する場合、レスポンスデータ RESが認証部105の乱数生成部111と認証部202の演算部211の出力の影響を受けるため、一方の機器を改竄する鍵の固定化を防ぐことができる。

【００７７】

このように、実施例2によれば、実施例1と同様の効果を得られるほか、認証部202から認証部105へ送信される暗号化鍵情報も認証ごとに異なるデータになるため、実施例1よりも強固な再送攻撃防止を実現することができる。

【実施例３】

【００７８】

以下、本発明にかかる実施例3の情報処理を説明する。なお、実施例3において、実施例1、2と略同様の構成については、同一符号を付して、その詳細説明を省略する。

【００７９】

実施例1、2においては、画像入力装置10と情報保持デバイス20の間で機器間認証を行うシステムを説明した。しかし、このようなシステムは、画像データを生成する画像入力装置だけに適用可能なシステムではない。そこで、実施例3では、画像データを利用する画像閲覧装置に上記システムを適用する例を説明する。

【００８０】

［認証システムの構成］

図6は機器間認証機能を有する画像処理装置の構成例を示すブロック図である。

【００８１】

画像処理装置は、PCなどの画像閲覧装置30および情報保持デバイス20から構成される。なお、画像処理装置の実現に当り、図6に示す全構成要素の使用は必須ではない。また、画像閲覧装置30で閲覧（再生）可能な画像は静止画像に限らず、動画像も含む。

【００８２】

●画像閲覧装置

画像閲覧装置30において、制御演算部306は、RAM 307をワークメモリとして、ROM 308に格納されたプログラムを実行して、画像閲覧装置30の各部を制御する。

【００８３】

暗号処理部305は、認証部303が保持する鍵情報を復号鍵として暗号化画像データを復号

する。なお、暗号化アルゴリズムは、AESなど様々な共通鍵暗号方式を利用することができる。

【００８４】

認証部303は、情報保持デバイス20の正当性を認証する。そして、実施例1と同様に、情報保持デバイス20を認証した場合、情報保持デバイス20から受信した暗号化鍵情報を復号して、復号した鍵情報を一時的に保持する。

【００８５】

このような構成により、暗号処理部305は、情報保持デバイス20の記録部203から読み込んだ暗号化画像データを復号し、RAM 307に格納する。制御演算部306は、RAM 307に格納された画像データに必要な画像処理（伸長処理やビデオ信号処理など）を施し、再生した画像を表示部301により表示する。画像閲覧装置30の利用者は、操作部302を操作して、表示する画像や表示方法などをの各種指示を入力する。

【００８６】

実施例1、2は、処理対象のデータが撮像素子101などから入力した画像データ、暗号処理部107の動作が暗号化である。これに対して、実施例3は、処理対象のデータが情報保持デバイス20から入力した暗号化画像データ、暗号処理部305の動作が復号になる。しかし、機器間認証、暗号化または復号用の鍵の取得方法などは変わらない。

【００８７】

従って、実施例3によれば、画像閲覧装置において、実施例1、2と同様に、機器間認証と鍵転送を同時に実現することができる。また、再送攻撃を防ぎ、メッセージ交換を2パスで実現することができる。

【００８８】

［他の実施例］

なお、本発明は、複数の機器（例えばホストコンピュータ、インタフェイス機器、リーダ、プリンタなど）から構成されるシステムに適用しても、一つの機器からなる装置（例えば、複写機、ファクシミリ装置など）に適用してもよい。

【００８９】

また、本発明の目的は、上記実施例の機能を実現するソフトウェアを記録した記憶媒体（記録媒体）をシステムまたは装置に供給し、そのシステムまたは装置のコンピュータ（CPUやMPU）が前記ソフトウェアを実行することでも達成される。この場合、記憶媒体から読み出されたソフトウェア自体が上記実施例の機能を実現することになり、そのソフトウェアを記憶した記憶媒体は本発明を構成する。

【００９０】

また、前記ソフトウェアの実行により上記機能が実現されるだけでなく、そのソフトウェアの指示により、コンピュータ上で稼働するオペレーティングシステム(OS)などが実際の処理の一部または全部を行い、それによって上記機能が実現される場合も含む。

【００９１】

また、前記ソフトウェアがコンピュータに接続された機能拡張カードやユニットのメモリに書き込まれ、そのソフトウェアの指示により、前記カードやユニットのCPUなどが実際の処理の一部または全部を行い、それによって上記機能が実現される場合も含む。

【００９２】

本発明を前記記憶媒体に適用する場合、その記憶媒体には、先に説明したフローチャートに対応するソフトウェアが格納される。

【図面の簡単な説明】

【００９３】

【図１】機器間認証機能を有する画像処理装置の構成例を示すブロック図、

【図２】認証部2の構成例を示すブロック図、

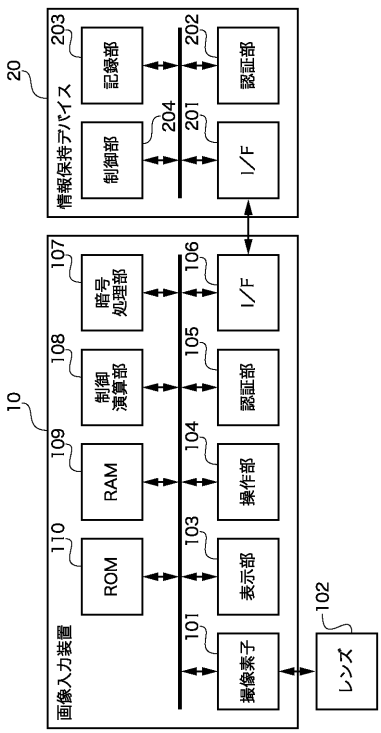
【図３】認証部が実行する機器間認証処理の一例を示すフローチャート、

【図４】入力画像の暗号化処理の一例を示すフローチャート、

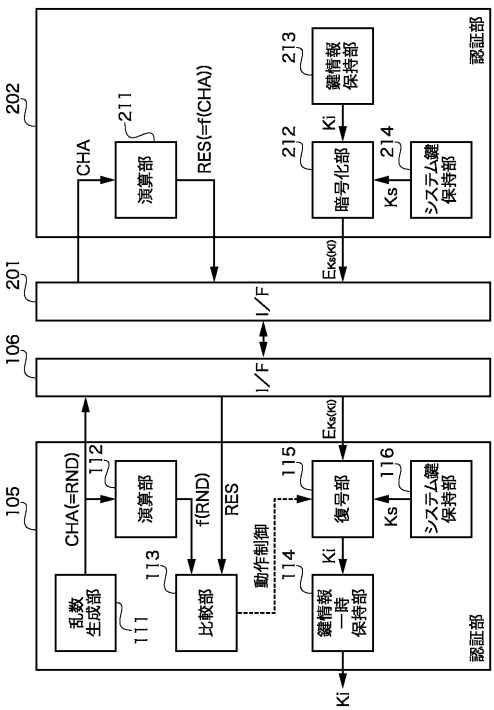
【図５】実施例2における認証部の構成例を示すブロック図、

【図６】実施例3の機器間認証機能を有する画像処理装置の構成例を示すブロック図である。

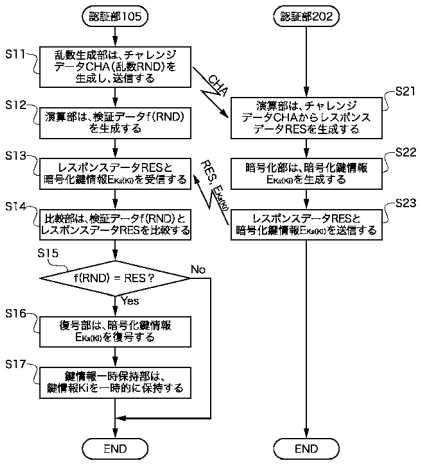
【図１】



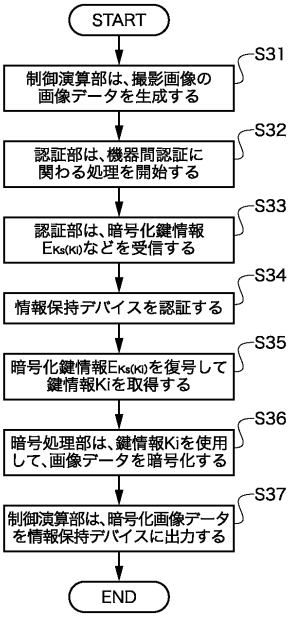
【図２】



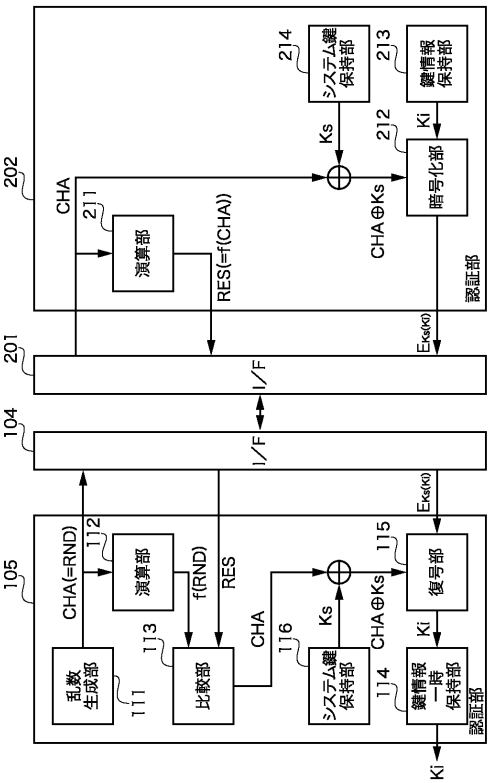
【図３】


認証部105
認証部202
S11
乱数生成部は、チャレンジデータCHA（乱数RND）を生成し、送信する
CHA
S21
演算部は、チャレンジデータCHAからレスポンスデータRESを生成する
S12
演算部は、検証データf(RND)を生成する
S13
レスポンスデータRESと暗号化鍵情報EKs(Ki)を受信する
RES、EKs(Ki)
S22
暗号化部は、暗号化鍵情報EKs(Ki)を生成する
S23
レスポンスデータRESと暗号化鍵情報EKs(Ki)を送信する
S14
比較部は、検証データf(RND)とレスポンスデータRESを比較する
S15
f(RND) = RES ?
No
Yes
S16
復号部は、暗号化鍵情報EKs(Ki)を復号する
S17
鍵情報一時保持部は、鍵情報Kiを一時的に保持する
END
END

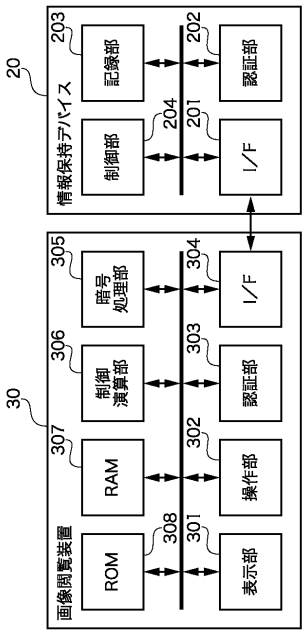
【図４】


START
S31
制御演算部は、撮影画像の画像データを生成する
S32
認証部は、機器間認証に関わる処理を開始する
S33
認証部は、暗号化鍵情報EKs(Ki)などを受信する
S34
情報保持デバイスを認証する
S35
暗号化鍵情報EKs(Ki)を復号して鍵情報Kiを取得する
S36
暗号処理部は、鍵情報Kiを使用して、画像データを暗号化する
S37
制御演算部は、暗号化画像データを情報保持デバイスに出力する
END

【図５】


214
システム鍵保持部
213
鍵情報保持部
Ks
212
Ki
暗号化部
202
CHA
211
演算部
CHA⊕Ks
RES(=f(CHA))
認証部
EKs(Ki)
201
I/F
104
I/F
EKs(Ki)
105
CHA(=RND)
112
演算部
f(RND)
RES
115
復号部
CHA⊕Ks
Ki
113
CHA
116
Ks
111
乱数生成部
比較部
システム鍵保持部
114
鍵情報一時保持部
認証部
Ki

【図６】


20
情報保持デバイス
203
記録部
202
認証部
204
201
制御部
I/F
30
画像閲覧装置
305
暗号処理部
304
I/F
306
制御演算部
303
認証部
307
RAM
302
操作部
308
301
ROM
表示部

フロントページの続き

Ｆターム(参考) 5J104 AA07 AA16 EA04 EA15 EA16 JA03 KA02 KA04 NA02 NA05
NA27 NA37 NA38