

(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2004-112461

(P2004-112461A)

(43) 公開日 平成16年4月8日(2004.4.8)

(51) Int. Cl. ⁷	F I	テーマコード (参考)
H04L 9/14	H04L 9/00 641	5B085
G06F 15/00	G06F 15/00 330E	5J104
H04L 9/08	H04L 9/00 601E	
H04L 9/32	H04L 9/00 675A	

審査請求 未請求 請求項の数 14 O L (全 29 頁)

(21) 出願番号	特願2002-273444 (P2002-273444)	(71) 出願人	000002185 ソニー株式会社 東京都品川区北品川6丁目7番35号
(22) 出願日	平成14年9月19日 (2002.9.19)	(74) 代理人	100094053 弁理士 佐藤 隆久
		(72) 発明者	大森 和雄 東京都品川区北品川6丁目7番35号 ソニー株式会社内
		(72) 発明者	本城 哲 東京都品川区北品川6丁目7番35号 ソニー株式会社内
		(72) 発明者	末吉 正弘 東京都品川区北品川6丁目7番35号 ソニー株式会社内

最終頁に続く

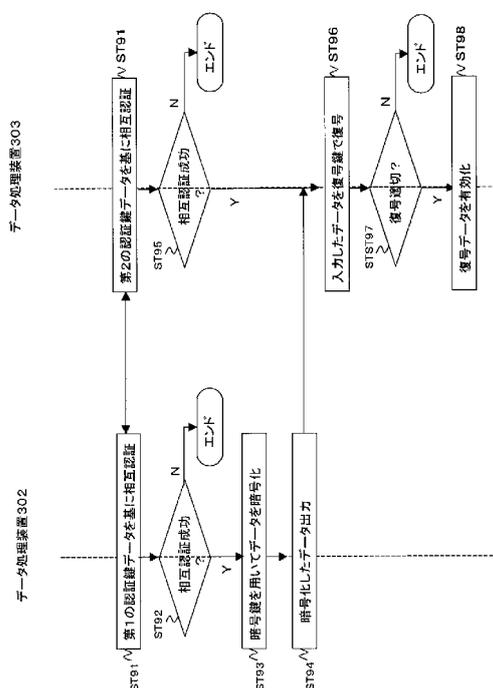
(54) 【発明の名称】 データ処理方法、そのプログラムおよびその装置

(57) 【要約】

【課題】 認証の鍵データが不正に第三者によって取得された場合でも、認証に続いて伝送された暗号化データがその第三者によって解読されないようにすることを可能にするデータ処理方法を提供する。

【解決手段】 データ処理装置302と303との間で第1および第2の認証鍵データを用いて相互認証を行う(ST91)。当該相互認証が成功すると、データ処理装置302が所定のデータを暗号鍵データを用いて暗号化してデータ処理装置303に出力する(ST93, ST94)。データ処理装置303は、復号鍵データを用いて上記暗号化データを復号し(ST96)、それが適切か否かを判断して有効化する(ST97, ST98)。

【選択図】 図4



【特許請求の範囲】

【請求項 1】

第 1 のデータ処理装置が第 1 の認証鍵データおよび暗号鍵データを保持し、第 2 のデータ処理装置が前記第 1 の認証鍵データに対応した第 2 の認証鍵データと前記暗号鍵データに対応した復号鍵データとを保持する場合に、前記第 1 のデータ処理装置と前記第 2 のデータ処理装置とが行うデータ処理方法であって、

前記第 1 のデータ処理装置が前記第 1 の認証鍵データを用い、前記第 2 のデータ処理装置が前記第 2 の認証鍵データを用いて、前記第 1 のデータ処理装置と前記第 2 のデータ処理装置との間で認証を行う第 1 の工程と、

前記第 2 のデータ処理装置が、前記第 1 の工程の前記認証により前記第 1 のデータ処理装置の正当性を認めた場合に、前記第 1 のデータ処理装置が前記暗号鍵データを用いて暗号化を行って前記第 2 のデータ処理装置に提供した暗号化データを、前記復号鍵データを用いて復号する第 2 の工程と、

前記第 2 のデータ処理装置が、前記第 2 の工程の前記復号によって得た復号データが適切に復号されたものであると判断した場合に、前記復号データを有効なものとして用いる第 3 の工程と

を有するデータ処理方法。

10

【請求項 2】

前記第 1 の工程において、前記第 1 のデータ処理装置および前記第 2 のデータ処理装置が、第 1 の暗号化アルゴリズム並びに前記第 1 の暗号化アルゴリズムに対応した第 1 の復号アルゴリズムを基に、所定のデータの暗号化および復号を行って前記認証を行い、

20

前記第 2 の工程において、前記第 2 のデータ処理装置が、第 2 の暗号化アルゴリズムを基に暗号化された前記暗号化データを、前記第 2 の暗号化アルゴリズムに対応した第 2 の復号アルゴリズムを基に前記復号する

請求項 1 に記載のデータ処理方法。

【請求項 3】

前記第 2 の工程において、前記第 2 のデータ処理装置が、前記第 1 の工程の前記認証により、前記第 1 の認証鍵データと前記第 2 の認証鍵データとが同じであると判断した場合に、前記第 1 のデータ処理装置の正当性を認める

請求項 1 に記載のデータ処理方法。

30

【請求項 4】

前記第 1 の認証鍵データが所定の鍵データを用いて所定の生成方法で生成されている場合に、

前記第 1 の工程は、

前記第 1 のデータ処理装置が、前記第 1 の認証鍵データの生成に用いられた鍵データを指定する鍵指定データを前記第 2 のデータ処理装置に提供する第 4 の工程と、

前記第 2 のデータ処理装置が、前記第 4 の工程で受けた前記鍵指定データが指定する前記鍵データを用いて前記所定の生成手法で前記第 2 の認証鍵データを生成する第 5 の工程と

、前記第 1 のデータ処理装置が前記第 1 の認証鍵データを用い、前記第 2 のデータ処理装置が前記第 5 の工程で生成した前記第 2 の認証鍵データを用いて、前記認証を行う第 6 の工程と、

40

前記第 2 のデータ処理装置が、前記第 6 の工程の前記認証により、前記第 1 の認証鍵データと前記第 2 の認証鍵データとが同じであると判断すると、前記第 1 のデータ処理装置の正当性を認める第 7 の工程と

を有する請求項 1 に記載のデータ処理方法。

【請求項 5】

第 1 の認証鍵データおよび暗号鍵データを保持する第 1 のデータ処理装置と、

前記第 1 の認証鍵データに対応した第 2 の認証鍵データと前記暗号鍵データに対応した復号鍵データとを保持する第 2 のデータ処理装置と

50

を有し、

前記第1のデータ処理装置が、前記第1の認証鍵データを用い、前記第2のデータ処理装置が前記第2の認証鍵データを用いて、前記第1のデータ処理装置と前記第2のデータ処理装置との間で認証を行い、

前記第2のデータ処理装置が、前記認証により前記第1のデータ処理装置の正当性を認めた場合に、前記第1のデータ処理装置が前記暗号鍵データを用いて暗号化を行って前記第2のデータ処理装置に提供した暗号化データを、前記復号鍵データを用いて復号し、前記第2のデータ処理装置が、前記復号によって得た復号データが適切に復号されたものであると判断した場合に、前記復号データを有効なものとして用いる

データ処理システム。

10

【請求項6】

認証鍵データおよび暗号鍵データを保持するデータ処理装置が行うデータ処理方法であって、

前記認証鍵データを用いて、認証先と認証を行う第1の工程と、

前記第1の工程の前記認証の後に、前記暗号鍵データを用いて所定のデータを暗号化する第2の工程と、

前記第2の工程の前記暗号化により得られたデータを前記認証先に出力する第3の工程とを有するデータ処理方法。

【請求項7】

鍵データを保持する前記認証先の認証手段が、第1の認証鍵データを保持する前記データ処理装置から指定された前記鍵データを用いて所定の生成手法を基に第2の認証鍵データを生成し、前記第2の認証鍵データを用いて前記データ処理装置と認証を行い、当該認証により、前記第1の認証鍵データと前記第2の認証鍵データとが同じであることを確認したことを条件に、前記第3の工程で出力された前記データを有効なものとして用いる場合に、

20

前記第1の工程は、

前記所定の生成方法を基に前記第1の認証鍵データを生成したときに用いた前記鍵データを指定する鍵指定データを前記認証手段に提供する第4の工程と、

前記第1の認証鍵データを用いて、前記認証手段と前記認証を行う第5の工程とを有する請求項6に記載のデータ処理方法。

30

【請求項8】

所定のデータを暗号化して認証先に出力するデータ処理装置であって、

認証鍵データおよび暗号鍵データを記憶する記憶手段と、

前記認証鍵データを用いて、認証先と認証を行う認証手段と、

前記認証手段の前記認証の後に、前記暗号鍵データを用いて所定のデータを暗号化する暗号化手段と、

前記暗号化手段の前記暗号化により得られたデータを前記認証先に出力する出力手段とを有するデータ処理装置。

【請求項9】

認証鍵データおよび暗号鍵データを保持するデータ処理装置が実行するプログラムであって、

40

前記認証鍵データを用いて、認証先と認証を行う第1の手順と、

前記第1の手順の前記認証の後に、前記暗号鍵データを用いて所定のデータを暗号化する第2の手順と、

前記第2の手順の前記暗号化により得られたデータを前記認証先に出力する第3の手順とを有するプログラム。

【請求項10】

認証鍵データおよび復号鍵データを保持するデータ処理装置が行うデータ処理方法であって、

前記認証鍵データを用いて、被認証手段と認証を行う第1の工程と、

50

前記復号鍵データを用いて、前記被認証手段から受けたデータを復号する第2の工程と、前記第1の工程の前記認証により前記被認証手段の正当性を認めると、前記第2の工程の前記復号により得られたデータを有効なものとして用いる第3の工程とを有するデータ処理方法。

【請求項11】

所定の鍵データを保持する前記データ処理装置が、前記鍵データを用いて所定の生成手法で生成され前記鍵データを復元困難な第1の認証鍵データを保持する前記被認証手段と認証を行う場合に、

前記第1の工程は、

前記鍵データを指定する鍵指定データを前記被認証手段から受ける第4の工程と、

10

前記第4の工程で受けた前記鍵指定データが指定する前記鍵データを用いて前記所定の生成手法で第2の認証鍵データを生成する第5の工程と、

前記第5の工程で生成した前記第2の認証鍵データを用いて、前記第1の認証鍵データを前記認証に用いる前記被認証手段と前記認証を行う第6の工程と、

前記第6の工程の前記認証により、前記第1の認証用データと前記第2の認証用データとが同じであると判断した場合に、前記被認証手段の正当性を認める第7の工程と

を有する請求項10に記載のデータ処理方法。

【請求項12】

前記第3の工程において、前記鍵データに関連付けられた、前記被認証手段に許可されたデータ処理装置の機能、または前記データ処理装置が保持するデータへのアクセスを実行する

20

請求項10に記載のデータ処理方法。

【請求項13】

認証鍵データおよび復号鍵データを保持するデータ処理装置であって、

前記認証鍵データを用いて、被認証手段と認証を行う認証手段と、

前記被認証手段からデータを入力する入力手段と、

前記復号鍵データを用いて、前記入力手段を介して前記被認証手段から入力した前記データを復号する復号手段と、

前記認証手段の前記認証により前記被認証手段の正当性を認めると、前記復号手段の前記復号により得られたデータを有効なものとして用いる制御手段と

30

を有するデータ処理装置。

【請求項14】

認証鍵データおよび復号鍵データを保持するデータ処理装置が実行するプログラムであって、

前記認証鍵データを用いて、被認証手段と認証を行う第1の手順と、

前記復号鍵データを用いて、前記被認証手段から受けたデータを復号する第2の手順と、

前記第1の手順の前記認証により前記被認証手段の正当性を認めると、前記第2の手順の前記復号により得られたデータを有効なものとして用いる第3の手順と

を有するプログラム。

【発明の詳細な説明】

40

【0001】

【発明の属する技術分野】

本発明は、認証結果を基に所定の処理を行うデータ処理方法、そのプログラムおよびその装置に関する。

【0002】

【従来の技術】

第1のデータ処理装置と第2のデータ処理装置との間で相互認証を行い、お互いの正当性を認証した後に、第1のデータ処理装置から第2のデータ処理装置に暗号化したデータを出力するシステムがある。

このようなシステムでは、上記相互認証と上記データの暗号化とで同じ鍵データを用いて

50

いる。

【0003】

【発明が解決しようとする課題】

しかしながら、上述した従来システムのよう、上記相互認証と上記データの暗号化とで同じ鍵データを用いると、相互認証の鍵データが第三者によって不正に取得された場合に、伝送される暗号化データも当該鍵データを用いて不正に解読されてしまうという問題がある。

【0004】

本発明はかかる事情に鑑みてなされたものであり、その目的は、認証の鍵データが不正に第三者によって取得された場合でも、認証に続いて提供された暗号化データがその第三者によって解読されないようにすることを可能にするデータ処理方法、そのプログラムおよびその装置を提供することを目的とする。

10

【0005】

【課題を解決するための手段】

上述した目的を達成するために、第1の発明のデータ処理方法は、第1のデータ処理装置が第1の認証鍵データおよび暗号鍵データを保持し、第2のデータ処理装置が前記第1の認証鍵データに対応した第2の認証鍵データと前記暗号鍵データに対応した復号鍵データとを保持する場合に、前記第1のデータ処理装置と前記第2のデータ処理装置とが行うデータ処理方法であって、前記第1のデータ処理装置が前記第1の認証鍵データを用い、前記第2のデータ処理装置が前記第2の認証鍵データを用いて、前記第1のデータ処理装置と前記第2のデータ処理装置との間で認証を行う第1の工程と、前記第2のデータ処理装置が、前記第1の工程の前記認証により前記第1のデータ処理装置の正当性を認めた場合に、前記第1のデータ処理装置が前記暗号鍵データを用いて暗号化を行って前記第2のデータ処理装置に提供した暗号化データを、前記復号鍵データを用いて復号する第2の工程と、前記第2のデータ処理装置が、前記第2の工程の前記復号によって得た復号データが適切に復号されたものであると判断した場合に、前記復号データを有効なものとして用いる第3の工程とを有する。

20

【0006】

第1の発明のデータ処理方法の作用は以下のようなになる。

第1の工程において、第1のデータ処理装置が第1の認証鍵データを用い、第2のデータ処理装置が第2の認証鍵データを用いて、前記第1のデータ処理装置と前記第2のデータ処理装置との間で認証を行う。

30

そして、第2の工程において、前記第2のデータ処理装置が、前記第1の工程の前記認証により前記第1のデータ処理装置の正当性を認めた場合に、前記第1のデータ処理装置が前記暗号鍵データを用いて暗号化を行って前記第2のデータ処理装置に提供した暗号化データを、前記復号鍵データを用いて復号する。

そして、第3の工程において、前記第2のデータ処理装置が、前記第2の工程の前記復号によって得た復号データが適切に復号されたものであると判断した場合に、前記復号データを有効なものとして用いる。

【0007】

第1の発明のデータ処理方法は、好ましくは、前記第1の工程において、前記第1のデータ処理装置および前記第2のデータ処理装置が、第1の暗号化アルゴリズム並びに前記第1の暗号化アルゴリズムに対応した第1の復号アルゴリズムを基に、所定のデータの暗号化および復号を行って前記認証を行い、前記第2の工程において、前記第2のデータ処理装置が、第2の暗号化アルゴリズムを基に暗号化された前記暗号化データを、前記第2の暗号化アルゴリズムに対応した第2の復号アルゴリズムを基に前記復号する。

40

【0008】

また、第1の発明のデータ処理方法は、好ましくは、前記第1の認証鍵データが所定の鍵データを用いて所定の生成方法で生成されている場合に、前記第1の工程は、前記第1のデータ処理装置が、前記第1の認証鍵データの生成に用いられた鍵データを指定する鍵指

50

定データを前記第2のデータ処理装置に提供する第4の工程と、前記第2のデータ処理装置が、前記第4の工程で受けた前記鍵指定データが指定する前記鍵データを用いて前記所定の生成手法で前記第2の認証鍵データを生成する第5の工程と、前記第1のデータ処理装置が前記第1の認証鍵データを用い、前記第2のデータ処理装置が前記第5の工程で生成した前記第2の認証鍵データを用いて、前記認証を行う第6の工程と、前記第2のデータ処理装置が、前記第6の工程の前記認証により、前記第1の認証鍵データと前記第2の認証鍵データとが同じであると判断すると、前記第1のデータ処理装置の正当性を認める第7の工程とを有する。

【0009】

第2の発明のデータ処理システムは、第1の認証鍵データおよび暗号鍵データを保持する第1のデータ処理装置と、前記第1の認証鍵データに対応した第2の認証鍵データと前記暗号鍵データに対応した復号鍵データとを保持する第2のデータ処理装置とを有し、前記第1のデータ処理装置が、前記第1の認証鍵データを用い、前記第2のデータ処理装置が前記第2の認証鍵データを用いて、前記第1のデータ処理装置と前記第2のデータ処理装置との間で認証を行い、前記第2のデータ処理装置が、前記認証により前記第1のデータ処理装置の正当性を認めた場合に、前記第1のデータ処理装置が前記暗号鍵データを用いて暗号化を行って前記第2のデータ処理装置に提供した暗号化データを、前記復号鍵データを用いて復号し、前記第2のデータ処理装置が、前記復号によって得た復号データが適切に復号されたものであると判断した場合に、前記復号データを有効なものとして用いる。

10

20

【0010】

第2の発明のデータ処理システムの作用は以下ようになる。

第1のデータ処理装置が、第1の認証鍵データを用い、第2のデータ処理装置が前記第2の認証鍵データを用いて、第1のデータ処理装置と前記第2のデータ処理装置との間で認証を行う。

そして、前記第2のデータ処理装置が、前記認証により前記第1のデータ処理装置の正当性を認めた場合に、前記第1のデータ処理装置が前記暗号鍵データを用いて暗号化を行って前記第2のデータ処理装置に提供した暗号化データを、前記復号鍵データを用いて復号する。

そして、前記第2のデータ処理装置が、前記復号によって得た復号データが適切に復号されたものであると判断した場合に、前記復号データを有効なものとして用いる。

30

【0011】

第3の発明のデータ処理方法は、認証鍵データおよび暗号鍵データを保持するデータ処理装置が行うデータ処理方法であって、前記認証鍵データを用いて、認証先と認証を行う第1の工程と、前記第1の工程の前記認証の後に、前記暗号鍵データを用いて所定のデータを暗号化する第2の工程と、前記第2の工程の前記暗号化により得られたデータを前記認証先に出力する第3の工程とを有する。

【0012】

第4の発明のデータ処理装置は、所定のデータを暗号化して認証先に出力するデータ処理装置であって、認証鍵データおよび暗号鍵データを記憶する記憶手段と、前記認証鍵データを用いて、認証先と認証を行う認証手段と、前記認証手段の前記認証の後に、前記暗号鍵データを用いて所定のデータを暗号化する暗号化手段と、前記暗号化手段の前記暗号化により得られたデータを前記認証先に出力する出力手段とを有する。

40

【0013】

第5の発明のプログラムは、認証鍵データおよび暗号鍵データを保持するデータ処理装置が実行するプログラムであって、前記認証鍵データを用いて、認証先と認証を行う第1の手順と、前記第1の手順の前記認証の後に、前記暗号鍵データを用いて所定のデータを暗号化する第2の手順と、前記第2の手順の前記暗号化により得られたデータを前記認証先に出力する第3の手順とを有する。

【0014】

50

第6の発明のデータ処理方法は、認証鍵データおよび復号鍵データを保持するデータ処理装置が行うデータ処理方法であって、前記認証鍵データを用いて、被認証手段と認証を行う第1の工程と、前記復号鍵データを用いて、前記被認証手段から受けたデータを復号する第2の工程と、前記第1の工程の前記認証により前記被認証手段の正当性を認めると、前記第2の工程の前記復号により得られたデータを有効なものとして用いる第3の工程とを有する。

【0015】

第7の発明のデータ処理装置は、認証鍵データおよび復号鍵データを保持するデータ処理装置であって、前記認証鍵データを用いて、被認証手段と認証を行う認証手段と、前記被認証手段からデータを入力する入力手段と、前記復号鍵データを用いて、前記入力手段を介して前記被認証手段から入力した前記データを復号する復号手段と、前記認証手段の前記認証により前記被認証手段の正当性を認めると、前記復号手段の前記復号により得られたデータを有効なものとして用いる制御手段とを有する。

10

【0016】

第8の発明のプログラムは、認証鍵データおよび復号鍵データを保持するデータ処理装置が実行するプログラムであって、前記認証鍵データを用いて、被認証手段と認証を行う第1の手順と、前記復号鍵データを用いて、前記被認証手段から受けたデータを復号する第2の手順と、前記第1の手順の前記認証により前記被認証手段の正当性を認めると、前記第2の手順の前記復号により得られたデータを有効なものとして用いる第3の手順とを有する。

20

【0017】

【発明の実施の形態】

以下、本発明の実施の形態を添付図面を参照して説明する。

第1実施形態

図1は、本実施形態に係わるデータ処理システムの構成図である。

図1に示すように、データ処理システム301は、例えば、データ処理装置302および303を有する。

ここで、データ処理装置302が、第1および第2の発明の第1のデータ処理装置、並びに第4の発明のデータ処理装置に対応している。

また、データ処理装置303が、第1および第2の発明の第2のデータ処理装置、並びに第7の発明のデータ処理装置に対応している。

30

【0018】

図2は、データ処理装置302の構成図である。

図2に示すように、データ処理装置302は、例えば、メモリ310、認証部311、暗号化部312、インタフェース313およびCPU314を有し、これらがバス309を介して接続されている。

ここで、メモリ310が第4の発明の記憶手段に対応し、認証部311が第4の発明の認証手段に対応し、暗号化部312が第4の発明の暗号化手段に対応し、インタフェース313が第4の発明の出力手段に対応している。

【0019】

メモリ310は、第1の認証鍵データ321、暗号鍵データ322およびプログラム323を記憶している。

40

ここで、第1の認証鍵データ321が本発明の第1の認証鍵データに対応し、暗号鍵データ322が本発明の暗号化データに対応し、プログラム323が第5の発明のプログラムに対応している。

認証部311は、第1の認証鍵データ321を用いて、データ処理装置303と相互認証を行う。

暗号化部312は、暗号鍵データ322を用いて、所定のデータを暗号化する。

インタフェース313は、上記暗号化したデータをデータ処理装置303に出力する。

CPU314は、プログラム323を実行して、後述するように、データ処理装置302

50

の各構成要素を統括的にして処理を行う。

【0020】

図3は、データ処理装置303の構成図である。

図3に示すように、データ処理装置303は、例えば、メモリ330、認証部331、復号部332、インタフェース333およびCPU334を有し、これらがバス339を介して接続されている。

ここで、メモリ330が第7の発明の記憶手段に対応し、認証部331が第7の発明の認証手段に対応し、暗号化部332が第7の発明の復号手段に対応し、インタフェース333が第7の発明の入力手段に対応している。

【0021】

メモリ330は、第2の認証鍵データ341、復号鍵データ342およびプログラム343を記憶している。

ここで、第2の認証鍵データ341が本発明の第2の認証鍵データに対応し、復号鍵データ342が本発明の復号データに対応し、プログラム343が第7の発明のプログラムに対応している。

認証部331は、第2の認証鍵データ341を用いて、データ処理装置302と相互認証を行う。

復号部332は、復号鍵データ342を用いて、インタフェース333を介してデータ処理装置302から入力したデータを復号する。

インタフェース333は、データ処理装置302から上記暗号化されたデータを入力する。

CPU334は、プログラム343を実行して、後述するように、データ処理装置303の各構成要素を統括的に制御して処理を行う。

【0022】

以下、図1に示すデータ処理システム301の動作例を説明する。

以下に示す処理は、CPU314によるプログラム323の実行、並びにCPU334によるプログラム343の実行に応じて行われる。

図4は、当該動作例を説明するためのフローチャートである。

ステップST91:

データ処理装置302の認証部311が第1の認証鍵データ321を用い、データ処理装置303の認証部331が第2の認証鍵データ341を用いて、相互認証を行う。

このとき、認証部311および331は、それぞれ第1の認証鍵データ321および341を用いて、第1の暗号アルゴリズム並びに当該第1の暗号化アルゴリズムに対応する第2の復号アルゴリズムを基に所定のデータの暗号化および復号を行って上記認証を行う。

当該相互認証には、第2実施形態で後述する相互認証の方法が用いられる。

【0023】

ステップST92:

データ処理装置302のCPU314が、ステップST91の相互認証によりデータ処理装置303との間でお互いの正当性が認められたと判断した場合にステップST93の処理に進む、そうでない場合には処理を終了する。

【0024】

ステップST93:

データ処理装置302の暗号化部312が、暗号鍵データ322を用いて、第2の暗号アルゴリズムで所定のデータを暗号化する。

【0025】

ステップST94:

データ処理装置302のインタフェース313が、ステップST93で暗号化したデータをデータ処理装置303に出力する。

【0026】

10

20

30

40

50

ステップ S T 9 5 :

データ処理装置 3 0 3 の C P U 3 3 4 が、ステップ S T 9 1 の相互認証によりデータ処理装置 3 0 2 との間でお互いの正当性が認められたと判断した場合にステップ S T 9 6 の処理に進む、そうでない場合には処理を終了する。

【 0 0 2 7 】

ステップ S T 9 6 :

データ処理装置 3 0 3 の復号部 3 3 2 が、復号鍵データ 3 4 2 を用いて、ステップ S T 9 4 でインタフェース 3 3 3 を介してデータ処理装置 3 0 2 から入力した暗号化されたデータを、上記第 2 の暗号アルゴリズムに対応した第 2 の復号アルゴリズムで復号する。

【 0 0 2 8 】

ステップ S T 9 7 :

データ処理装置 3 0 3 の C P U 3 3 4 が、ステップ S T 9 6 の復号によって得られた復号データが、適切に復号されたものであるか否かを判断し、適切に復号されたものであると判断した場合にはステップ S T 9 8 の処理に進み、そうでない場合には当該復号データを破棄（無効化）する。

【 0 0 2 9 】

ステップ S T 9 8 :

データ処理装置 3 0 3 の C P U 3 3 4 が、ステップ S T 9 7 で得られた復号データを有効なものとして用いて処理を行う。

【 0 0 3 0 】

以上説明したように、データ処理システム 3 0 1 によれば、相互認証と暗号化データの生成とを異なる鍵データを用いて行うため、相互認証により用いた第 1 および第 2 の認証鍵データが第三者によって不正に取得された場合でも、暗号化データは暗号鍵データを用いて暗号化されているため、当該第三者は当該暗号化データを解読できない。そのため、データ処理システム 3 0 1 によれば、暗号化データを適切に保護できる。

また、データ処理システム 3 0 1 によれば、相互認証と暗号化データの生成とで異なる暗号・復号アルゴリズムを用いているため、相互認証で用いた第 1 の暗号・復号アルゴリズムが第三者に漏れた場合でも、暗号化データは第 2 の暗号アルゴリズムで暗号化されているため、当該第三者は解読できない。

【 0 0 3 1 】

第 2 実施形態

図 5 は、本実施形態の通信システム 1 の全体構成図である。

図 5 に示すように、通信システム 1 は、店舗などに設置されたサーバ装置 2、IC カード 3、カードリーダー・ライター 4、パーソナルコンピュータ 5、ASP (Application Service Provider) サーバ装置 19、SAM (Secure Application Module) ユニット 9 a, 9 b, . . .、管理装置 20、IC モジュール 4 2 が内蔵された携帯通信装置 4 1 を用いて、インターネット 10 を介して通信を行って IC カード 3 あるいは携帯通信装置 4 1 を用いた決済処理などの手続き処理を行う。

【 0 0 3 2 】

通信システム 1 では、管理装置 20 および SAM ユニット 9 a, 9 b が本発明に対応した実施の形態に係わる処理を行う。

すなわち、管理装置 20 は、管理者等によって許可された所定の処理を SAM ユニット 9 a, 9 b に行わせるために用いる IC を内蔵したカード（例えば、後述するオナカードおよびユーザカード）を発行する処理を行う。これにより、相互認証に用いられる認証鍵データが被認証手段に対して提供される。

また、管理装置 20 は、上記発行されたカードを管理者やユーザが用いて、SAM ユニット 9 a, 9 b との間で上記認証鍵データを基に相互認証を行う。

そして、当該相互認証によって互いの正当性が認められると、暗号化鍵データを用いて暗号化された所定の暗号化データが管理装置 20 から SAM ユニット 9 a, 9 b に出力され

10

20

30

40

50

、SAMユニット9a, 9bが復号鍵データを用いて、当該暗号化データを復号する。
この場合に、管理装置20が本発明の第1のデータ処理装置および被認証手段となり、SAMユニット9a, 9bが本発明の第2のデータ処理装置、認証先および認証手段となる。

【0033】

図6は、管理装置20の機能ブロック図である。

図6に示すように、管理装置20は、例えば、AP編集ツール51、管理ツール52、カードリーダー・ライター53、ディスプレイ54、I/F55および操作部56を有する。

【0034】

AP編集ツール51および管理ツール52は、データ処理装置でプログラム(第5の発明のプログラム)を実行して実現してもよいし、電子回路(ハードウェア)によって実現してもよい。

管理ツール52は、例えば、SAM管理機能部57およびカード管理機能部58を有する。

カードリーダー・ライター53は、以下に示す種々のカードのICとの間で、非接触式あるいは接触式でデータの授受を行う。

ディスプレイ54は、カード発行画面やAP管理画面を表示するために用いられる。

I/F55は、SAMユニット9a, 9bとの間で、非接触式あるいは接触式でデータの授受を行う。

操作部56は、AP編集ツール51および管理ツール52に対して、指示やデータを入力するために用いられる。

【0035】

図7は、管理装置20が行う処理手順の概要を説明するためのフローチャートである。

図7において、ステップST2~ステップST4が、図4のステップST91に対応し、ステップST5~ST7が図4のステップST93~ST98に対応している。

この場合に、管理装置20がデータ処理装置302に対応し、SAMユニット9a, 9bがデータ処理装置303に対応する。

【0036】

ステップST1:

管理装置20は、管理者の操作に応じて、カード管理機能部58により、カードリーダー・ライター53にセットされたデフォルトカード71を用いて、所定のデータが格納されたオナーカード72を作成する。また、オナーカード72を用いてユーザカード73を作成する。

すなわち、管理装置20は、SAMユニット9a, 9b(本発明の認証手段)に係わる処理のうち、オナーカード72およびユーザカード73を用いた被認証手段に許可する処理に関連付けられた相互認証鍵データを用いて、後述するデバイス鍵データを所定の暗号化方法で暗号化して、上記相互認証鍵データを復元困難な縮退鍵データ(本発明の第1の認証鍵データ)を生成する。

そして、管理装置20は、上記生成した縮退鍵データと、当該縮退鍵データの生成に用いた上記相互認証鍵データを指定する鍵指定データとを、オナーカード72およびユーザカード73のICに書き込む。

また、同様に、管理装置20は、トランスポートカード74およびAP暗号化カード75を作成する。

【0037】

ステップST2:

オナーカード72またはユーザカード73の使用者が、これらのカードを用いて、管理装置20を介して、当該使用者に権限が与えられた処理をSAMユニット9a, 9bに行わせる場合に、上記使用者が管理装置20のカードリーダー・ライター53に、オナーカード72またはユーザカード73のICに記憶された上記鍵指定データを読み込ませる。

管理装置20のSAM管理機能部57は、当該読み込んだ鍵指定データをSAMユニット

9 a , 9 b に出力する。

【 0 0 3 8 】

ステップ S T 3 :

S A M ユニット 9 a , 9 b が、上記鍵指定データが指定する相互認証鍵データを用いて、上記デバイス鍵データを上記所定の暗号化方法で暗号化して縮退鍵データ（本発明の第 2 の認証鍵データ）を生成する。

【 0 0 3 9 】

ステップ S T 4 :

S A M 管理機能部 5 7 がカード 7 2 または 7 3 から読み出した縮退鍵データを用い、S A M ユニット 9 a , 9 b が上記生成した縮退鍵データを用いて、第 1 の暗号化アルゴリズムおよび第 1 の復号アルゴリズムを基に相互認証を行う。

【 0 0 4 0 】

ステップ S T 5 :

ステップ S T 4 の相互認証により互いの正当性が認められると、管理装置 2 0 が、暗号鍵データを用いて、第 2 の暗号化アルゴリズムで所定のデータを暗号化して S A M ユニット 9 a , 9 b に出力する。

【 0 0 4 1 】

ステップ S T 6 :

S A M ユニット 9 a , 9 b が、復号鍵データを用いて、ステップ S T 5 で入力した暗号化されたデータを、上記第 2 の暗号アルゴリズムに対応した第 2 の復号アルゴリズムで復号する。

【 0 0 4 2 】

ステップ S T 7 :

S A M ユニット 9 a , 9 b が、ステップ S T 6 の復号データが、適切に復号されたものであるか否かを判断し、適切に復号されたものであると判断した場合には、ステップ S T 6 で得られた復号データを有効なものとして用いて、オーナカード 7 2 等に許可した上記鍵データに関連付けられた処理を実行する。

一方、S A M ユニット 9 a , 9 b が、上記復号データが適切に復号されたものではないと判断した場合には、当該復号データを破棄（無効化）する。

【 0 0 4 3 】

図 8 は、図 6 に示す A P 編集ツール 5 1 および管理ツール 5 2 に係わる処理において用いられるカードを説明するための図である。

図 8 に示すように、管理装置 2 0 の管理ツール 5 2 を用いて、S A M ユニット 9 a , 9 b にアクセスする場合に、オーナカード 7 2 およびユーザカード 7 3 が用いられる。

また、A P 編集ツール 5 1 で生成した A P パッケージファイルを管理ツール 5 2 に提供する場合に、A P 暗号化カード 7 5 の I C に記憶された暗号化鍵データを用いて、当該 A P パッケージファイルが暗号化される。

すなわち、図 8 に示すように、ユーザが、A P 編集ツール 5 1 を用いて、S A M モジュール 8 内のアプリケーションプログラム A P を構成するアプリケーションエレメントデータ A P E を作成する。

そして、A P 編集ツール 5 1 が、単数または複数のアプリケーションエレメントデータ A P E を含む A P パッケージファイルを作成し、これを A P 暗号化カード 7 5 に格納された暗号鍵データを用いて暗号化して管理ツール 5 2 に提供する。

管理ツール 5 2 は、上述したように、S A M ユニット 9 a , 9 b と相互認証を行い、当該相互認証に用いた相互認証鍵データに関連付けて許可された S A M ユニット 9 a , 9 b 内の A P 記憶領域に対して、A P 編集ツール 5 1 から受けた A P パッケージファイルを書き込む。

また、トランスポートカード 7 4 は、S A M ユニット 9 a , 9 b が保持する鍵データなどのセキュリティに係わるデータを取り出して他の機器に転送したり、保存等するために用いられる。

10

20

30

40

50

【 0 0 4 4 】

〔 I C カード 3 および 携帯通信装置 4 1 〕

図 9 は、 I C カード 3 の機能ブロック図である。

図 9 に示すように、 I C カード 3 は、メモリ 5 0 および C P U 5 1 を備えた I C (I n t e g r a t e d C i r c u i t) モジュール 3 a を有する。

メモリ 5 0 は、図 1 0 に示すように、クレジットカード会社などのサービス事業者 1 5 __ 1 が使用する記憶領域 5 5 __ 1、サービス事業者 1 5 __ 2 が使用する記憶領域 5 5 __ 2、並びにサービス事業者 1 5 __ 3 が使用する記憶領域 5 5 __ 3 を有する。

また、メモリ 5 0 は、記憶領域 5 5 __ 1 へのアクセス権限を判断するために用いられる鍵データ、記憶領域 5 5 __ 2 へのアクセス権限を判断するために用いられる鍵データ、並びに記憶領域 5 5 __ 3 へのアクセス権限を判断するために用いられる鍵データを記憶している。当該鍵データは、相互認証や、データの暗号化および復号などに用いられる。

また、メモリ 5 0 は、 I C カード 3 あるいは I C カード 3 のユーザの識別データを記憶している。

10

【 0 0 4 5 】

携帯通信装置 4 1 は、携帯電話網およびインターネット 1 0 を介して A S P サーバ装置 1 9 a , 1 9 b と通信を行う通信処理部 4 3 と、通信処理部 4 3 との間でデータ授受可能な I C モジュール 4 2 とを有し、アンテナからインターネット 1 0 を介して S A M ユニット 9 a と通信を行う。

I C モジュール 4 2 は、携帯通信装置 4 1 の通信処理部 4 3 とデータ授受を行う点を除いて、前述した I C カード 3 の I C モジュール 3 a と同じ機能を有している。

20

なお、携帯通信装置 4 1 を用いた処理は、 I C カード 3 を用いた処理と同様に行われ、 I C モジュール 4 2 を用いた処理は I C モジュール 3 a を用いた処理と同様に行われるため、以下の説明では、 I C カード 3 および I C モジュール 3 a を用いた処理について例示する。

【 0 0 4 6 】

以下、 S A M ユニット 9 a , 9 b について説明する。

図 5 に示すように、 S A M ユニット 9 a , 9 b は、外部メモリ 7 と S A M モジュール 8 とを有する。

ここで、 S A M モジュール 8 は、半導体回路として実現してもよいし、筐体内に複数の回路を収容した装置として実現してもよい。

30

【 0 0 4 7 】

〔 S A M モジュール 8 のソフトウェア構成 〕

S A M モジュール 8 は、図 1 1 に示すようなソフトウェア構成を有している。図 1 1 に示すように、 S A M モジュール 8 は、下層から上層に向けて、ハードウェア H W 層、周辺 H W に対応した R T O S カーネルなどを含めたドライバ層 (O S 層)、論理的にまとまった単位の処理を行う下位ハンドラ層、アプリケーション固有のライブラリなどをまとめた上位ハンドラ層および A P 層を順に有している。

ここで、 A P 層では、図 5 に示すクレジットカード会社などのサービス事業者 1 5 __ 1 , 1 5 __ 2 , 1 5 __ 3 による I C カード 3 を用いた手続きを規定したアプリケーションプログラム A P __ 1 , A P __ 2 , A P __ 3 が、外部メモリ 7 から読み出されて動作している。 A P 層では、アプリケーションプログラム A P __ 1 , A P __ 2 , A P __ 3 相互間、並びに上位ハンドラ層との間にファイアウォール F W が設けられている。

40

【 0 0 4 8 】

〔 S A M モジュール 8 のハードウェア構成 〕

図 1 2 は、 S A M モジュール 8 のハードウェア構成、並びに外部メモリ 7 の記憶領域を説明するための図である。

図 1 2 に示すように、 S A M モジュール 8 は、例えば、メモリ I / F 6 1、外部 I / F 6 2、メモリ 6 3、認証部 6 4 および C P U 6 5 を有し、これらがバス 6 0 を介して接続されている。

50

また、SAMモジュール8が、第7の発明のデータ処理装置に対応し、以下に示す各手順を含むプログラムを実行して、その機能を実現してもよい。

【0049】

メモリI/F61は、外部メモリ7との間でデータ授受を行う。

外部I/F62は、図5に示すASPサーバ装置19a, 19bおよび管理装置20との間で、データおよびコマンドの授受を行う。

メモリ63は、後述するSAMユニット9a, 9bの相互認証などに用いられる種々の鍵データなどを記憶する。当該鍵データは、外部メモリ7のAP管理用記憶領域221に記憶されていてもよい。

認証部64は、後述する相互認証に係わる処理を行う。認証部64は、例えば、所定の鍵データをを用いた暗号化および復号などを処理を行う。

CPU65は、SAMモジュール8の処理を統括して制御する。

CPU65は、後述するように、相互認証で正当な相手であることを確認すると、被認証手段に対して、後述する相互認証鍵データに関連付けられた処理を許可し、これを実行する。

SAMモジュール8による相互認証処理については、後に詳細に説明する。

【0050】

〔外部メモリ7〕

図12に示すように、外部メモリ7の記憶領域には、サービス事業者15__1のアプリケーションプログラムAP__1が記憶されるAP記憶領域220__1(サービスAPリソース領域)、サービス事業者15__2のアプリケーションプログラムAP__2が記憶されるAP記憶領域220__2、サービス事業者15__3のアプリケーションプログラムAP__3が記憶されるAP記憶領域220__3、並びにSAMモジュール208の管理者が使用するAP管理用記憶領域221(システムAPリソース領域および製造者APリソース領域)がある。

【0051】

AP記憶領域220__1に記憶されているアプリケーションプログラムAP__1は、図13に示すように、後述する複数のアプリケーションエレメントデータAPEによって構成されている。AP記憶領域220__1へのアクセスは、ファイアウォールFW__1によって制限されている。

AP記憶領域220__2に記憶されているアプリケーションプログラムAP__2は、図13に示すように、複数のアプリケーションエレメントデータAPEによって構成されている。AP記憶領域220__2へのアクセスは、ファイアウォールFW__2によって制限されている。

AP記憶領域220__3に記憶されているアプリケーションプログラムAP__3は、図13に示すように、複数のアプリケーションエレメントデータAPEによって構成されている。AP記憶領域220__3へのアクセスは、ファイアウォールFW__3によって制限されている。

本実施形態では、上記アプリケーションエレメントデータAPEは、例えば、SAMユニット9aの外部から外部メモリ7にダウンロードされる最小単位である。各アプリケーションプログラムを構成するアプリケーションエレメントデータAPEの数は、対応するサービス事業者が任意に決定できる。

【0052】

また、アプリケーションプログラムAP__1, AP__2, AP__3は、例えば、それぞれ図5に示すパーソナルコンピュータ16__1, 16__2, 16__3を用いて、サービス事業者15__1, 15__2, 15__3によって作成され、SAMモジュール8を介して外部メモリ7にダウンロードされる。

【0053】

なお、AP管理用記憶領域221に記憶されたプログラム、並びにデータも、上述したアプリケーションエレメントデータAPEを用いて構成されている。

10

20

30

40

50

【0054】

図14は、上述したアプリケーションエレメントデータAPEを説明するための図である。

アプリケーションエレメントデータAPEは、図14に示すように、APEの属性(種別)を基に規定された分類を示すAPEタイプによって規定されたインスタンスを用いて構成される。

各インスタンスは、エレメントIDと、エレメントプロパティと、エレメントバージョンとによって規定されている。

APEタイプを基に、当該アプリケーションエレメントデータAPEが、サービスAP記憶領域220__1, 220__2, 220__3およびAP管理用記憶領域221の何れに格納されるかが規定される。

サービスAP記憶領域220__1は、各サービス事業者がアクセス可能なデータを記憶する。

なお、AP管理用記憶領域221は、システムの管理者がアクセス可能なデータを記憶するシステムAP記憶領域と、システムの製造者がアクセス可能なデータを記憶する製造者AP記憶領域とを有する。

また、サービスAP記憶領域220__1, 220__2, 220__3およびAP管理用記憶領域221によって、AP記憶領域が構成される。

本実施形態では、上述したサービスAP記憶領域220__1, 220__2, 220__3およびAP管理用記憶領域221の各々にはID(AP記憶領域ID)が割り当てられており、APEタイプ、インスタンス、並びにエレメントバージョンの各々には識別用の番号(APEタイプ番号、インスタンス番号、並びにエレメントバージョン番号)が割り当てられている。

【0055】

図15は、APEタイプの一例を説明するための図である。

図15に示すように、APEタイプには、ICシステム鍵データ、ICエリア鍵データ、ICサービス鍵データ、IC縮退鍵データ、IC鍵変更パッケージ、IC発行鍵パッケージ、IC拡張発行鍵パッケージ、ICエリア登録鍵パッケージ、ICエリア削除鍵パッケージ、ICサービス登録鍵パッケージ、ICサービス削除鍵パッケージ、ICメモリ分割鍵パッケージ、ICメモリ分割素鍵パッケージ、障害記録ファイル、相互認証用鍵、パッケージ鍵、ネガリストおよびサービスデータテンポラリファイルがある。

各APEタイプには、APEタイプ番号が割り当てられている。

【0056】

以下、図15に示すAPEタイプのうち一部を説明する。

ICシステム鍵データ、ICエリア鍵データ、ICサービス鍵データおよびIC縮退鍵データは、ICカード3およびICモジュール42のメモリ50に対してのデータの読み書き操作に用いられるカードアクセス鍵データである。

相互認証用鍵データ同一SAM内にあるAP間相互認証にも使用される。SAM相互認証用鍵データとは、対応するアプリケーションエレメントデータAPEを同一SAM内の他のAPまたは他のSAMからアクセスする際に用いられる鍵データである。

【0057】

ICメモリ分割用鍵パッケージは、サービス事業者がICカード3を用いたサービスの運用開始前に、外部メモリ7やICカード3のメモリの記憶領域を分割するために使用するデータである。

ICエリア登録鍵パッケージは、サービス事業者がICカード3を用いたサービスの運用開始前に、ICカード3のメモリの記憶領域にエリア登録を行う場合に使用するデータである。

ICエリア削除用鍵パッケージは、カードアクセス鍵データからSAM内部で自動生成が可能なパッケージである。

ICサービス登録用鍵パッケージは、サービス事業者がICカード3を用いたサービスの

10

20

30

40

50

運用開始前に、外部メモリ7のアプリケーションエレメントデータAPEを登録するために用いられる。

ICサービス削除用鍵パッケージは、外部メモリ7に登録されているアプリケーションエレメントデータAPEを削除するために用いられる。

【0058】

〔オナカード72およびユーザカード73の作成〕

図16は、オナカード72およびユーザカード73の作成手順を説明するためのフローチャートである。

図16は、図7に示すステップST1を詳細に示すものである。

ステップST11：

例えば、管理者が、オナカード72を作成する場合には、オナカード72の使用者に許可するSAMユニット9a, 9bに係わる処理を選択する。

また、管理者等が、ユーザカード73を作成する場合に、ユーザカード73の使用者に許可するSAMユニット9a, 9bに係わる処理を選択する。

SAMユニット9a, 9bに係わる処理には、例えば、SAMユニット9a, 9bが提供する機能を実行する処理、またはSAMユニット9a, 9bが保持するデータ(例えば、アプリケーションエレメントデータAPE)へのアクセスなどがある。

【0059】

ステップST12：

管理者等が、ステップST11で選択した処理に関連付けられた相互認証鍵データを選択して、管理装置20のカード管理機能部58に入力あるいは指定する。

当該相互認証鍵データについては後に詳細に説明する。

【0060】

ステップST13：

管理装置20のカード管理機能部58が、ステップST12で選択された単数または複数の相互認証鍵データを用いて後述する縮退処理方法を基に縮退鍵データを生成する。

当該縮退処理については後に詳細に説明する。

【0061】

ステップST14：

管理装置20のカード管理機能部58が、ステップST13で縮退鍵データの生成に用いた、相互認証鍵データを識別する相互認証コードを示す鍵指定データを生成する。

当該鍵指定データは、オナカード72またはユーザカード73の使用者が取得した、SAMユニット9a, 9bに係わる処理の実行権限を示すデータとなる。

【0062】

ステップST15：

管理装置20のカード管理機能部58が、ステップST13で生成した縮退鍵データと、ステップST14で生成した鍵指定データとを、オナカード72またはユーザカード73のICに書き込む。

【0063】

ステップST16：

管理装置20のカード管理機能部58が、ステップST13の縮退鍵データの生成に用いた、相互認証鍵データをSAMユニット9a, 9bに登録する。

【0064】

以下、上述した図16に示すステップST12で選択する対象となる相互認証鍵データについて説明する。

図17は、図16に示すステップST12で選択する対象となる相互認証鍵データを説明するための図である。

図17に示すように、当該相互認証鍵データには、例えば、デバイス鍵データ、ターミネーション鍵データ、製造設定サービス相互認証鍵データ、機器管理サービス相互認証鍵データ、通信管理サービス相互認証鍵データ、相互認証サービス相互認証鍵データ、AP記

10

20

30

40

50

憶領域管理サービス相互認証鍵データ、サービスAP記憶領域相互認証鍵データ、システムAP記憶領域相互認証鍵データ、並びに製造者AP記憶領域相互認証鍵データがある。

【0065】

また、図17および図18に示すように、相互認証鍵データの相互認証コードが、図14を用いて説明したAP記憶領域ID、エレメントタイプ番号、エレメントインスタンス番号およびエレメントバージョン番号から構成される。

【0066】

以下、上述した図16に示すステップST14で生成する鍵指定データについて説明する。

当該鍵指定データは、上述した複数の相互認証鍵データの相互認証コードを用いて構成される、相互認証コードリストである。 10

図19は、鍵指定データの一例を説明するための図である。

図16のステップST12で、例えば、図17に示すデバイス鍵データ、機器管理サービス相互認証鍵データ、通信管理サービス相互認証鍵データ、AP記憶領域管理サービス相互認証鍵データ、サービスAP記憶領域相互認証鍵データ、並びにターミネーション鍵データが選択された場合には、図19(A)に示すように、当該選択された全ての相互認証鍵データの相互認証コードを示す鍵指定データが生成される。

図16に示すステップST13において、図19(A)に示す相互認証コードの相互認証鍵データを用いて縮退鍵データが生成された場合には、当該縮退鍵データを用いたSAMユニット9a, 9bとの相互認証により、管理装置20に対して、図19(B)に示すように、機器管理サービス、通信管理サービス、ICサービス(ICカード3およびICモジュール421に関するサービス)、相互認証サービスおよびAP記憶領域管理サービスが許可される。 20

【0067】

このように、本実施形態では、SAMユニット9a, 9bの機能と、SAMユニット9a, 9bが保持するデータ(例えば、アプリケーションエレメントデータAPE)へのアクセスを含む複数の処理にそれぞれ関連付けられた相互認証鍵データを用いて縮退鍵データを生成できる。

これにより、単数の縮退鍵データを用いた相互認証により、SAMユニット9a, 9bが、SAMユニット9a, 9bの機能と、SAMユニット9a, 9bが保持するデータへのアクセスとの双方について、それらを被認証手段に対して許可するか否かを一括して判断できる。 30

そして、SAMユニット9a, 9bは、被認証手段が正当であると認証した場合に、当該被認証手段の指示に応じて、上記相互認証鍵データに関連付けられた所定の機能に係わる処理を実行すると共に、SAMユニット9a, 9bが保持するデータへの上記被認証手段からのアクセスを許可する。

【0068】

以下、図16に示すステップST13の縮退処理方法について説明する。

図20は、当該縮退処理方法を説明するためのフローチャートである。

ステップST21:

管理装置20のカード管理機能部58が、デバイス鍵データをメッセージとし、図16に示すステップST12で選択されたデバイス鍵データおよびターミネーション鍵データ以外の相互認証鍵データのうち最初の一つを暗号鍵として用いて、デバイス鍵データを暗号化し、中間鍵データを生成する。 40

ここで、ステップST12で選択されたデバイス鍵データおよびターミネーション鍵データ以外の相互認証鍵データが一つの場合には、カード管理機能部58は、上記中間鍵データを用いて次のステップST22の処理を行う。

一方、ステップST12で選択されたデバイス鍵データおよびターミネーション鍵データ以外の相互認証鍵データが2以上の場合には、カード管理機能部58は、上記中間鍵データをメッセージとして、次の相互認証鍵データを暗号鍵として用いて暗号化を行う。 50

カード管理機能部 5 8 は、ステップ S T 1 2 で選択されたデバイス鍵データおよびターミネーション鍵データ以外の全ての相互認証鍵データを暗号鍵として用いて上記暗号化を行うまで上記処理を繰り返し、終了したらステップ S T 2 2 の処理に進む。

ステップ S T 2 2 :

カード管理機能部 5 8 が、ステップ S T 2 1 で得られた中間鍵データをメッセージとして、ターミネーション鍵データを暗号鍵として用いて暗号化を行って縮退鍵データを生成する。

当該ターミネーション鍵データは、改竄防止鍵データであり、管理者のみが保持している。これにより、管理者以外の者が、不正に縮退鍵データを改竄することを防止できる。

【 0 0 6 9 】

以下、上述したターミネーション鍵データとして、管理者（オナ）のみが所有するオナターミネーション鍵データと、上記管理者から権限を与えられたユーザが所有するユーザターミネーション鍵データとを用いて、所定の縮退処理方法で、縮退鍵データを生成する場合を説明する。

図 2 1 は、当該縮退処理方法を説明するためのフローチャートである。

図 2 1 において、ステップ S T 3 1 , S 3 2 の処理は、ターミネーション鍵データとして、上記オナターミネーション鍵データを用いる点を除いて、図 2 0 を用いて説明したステップ S T 2 1 , 2 2 の処理と同じである。

ステップ S T 3 2 で生成された縮退鍵データは、ユーザターミネーション鍵データを与えられたユーザが、拡張できるという意味で拡張可能な縮退鍵データである。

ステップ S T 3 3 :

管理装置 2 0 のカード管理機能部 5 8 が、オナが生成した拡張可能縮退鍵データをメッセージとし、ユーザが選択したユーザターミネーション鍵データ以外の相互認証鍵データのうち最初の一つを暗号鍵として用いて、デバイス鍵データを暗号化し、中間鍵データを生成する。

ここで、上記選択されたユーザターミネーション鍵データ以外の相互認証鍵データが一つの場合には、カード管理機能部 5 8 は、上記中間鍵データを用いて次のステップ S T 2 2 の処理を行う。

一方、上記選択されたユーザターミネーション鍵データ以外の相互認証鍵データが 2 以上の場合には、カード管理機能部 5 8 は、上記中間鍵データをメッセージとして、次の相互認証鍵データを暗号鍵として用いて暗号化を行う。

カード管理機能部 5 8 は、上記選択されたユーザターミネーション鍵データ以外の全ての相互認証鍵データを暗号鍵として用いて上記暗号化を行うまで上記処理を繰り返し、終了したらステップ S T 3 4 の処理に進む。

ステップ S T 3 4 :

カード管理機能部 5 8 が、ステップ S T 3 3 で得られた中間鍵データをメッセージとして、ユーザターミネーション鍵データを暗号鍵として用いて暗号化を行って縮退鍵データを生成する。

当該ユーザターミネーション鍵データは、改竄防止鍵データであり、上記オナおよび上記ユーザのみが保持している。

これにより、上記オナおよび上記ユーザ以外の者が、不正に縮退鍵データを改竄することを防止できる。

【 0 0 7 0 】

図 2 1 に示す処理によって生成された縮退鍵データは、図 2 2 に示すような階層で相互認証鍵が暗号化されたものになる。

【 0 0 7 1 】

また、本実施形態では、単数の相互認証鍵データ（例えば、図 1 7 に示すサービス、システム、製造者 A P 記憶領域相互認証鍵データ）に、複数のアプリケーションエレメントデータ A P E を関連付けてもよい。

これにより、縮退鍵データを用いた認証により、S A M ユニット 9 a , 9 b が、単数の相

10

20

30

40

50

互認証鍵データに関連付けられたアプリケーションエレメントデータ A P E へのアクセスを許可するか否かを一括して判断できる。

例えば、図 2 3 では、相互認証鍵データ 5 0 0 に、アプリケーションエレメントデータ A P E のインスタンス a のパーミッション C と、インスタンス b のパーミッション B とが関連付けられている。そのため、相互認証鍵データ 5 0 0 を縮退した縮退鍵データを用いた認証が成功すれば、S A M ユニット 9 a , 9 b がインスタンス a , b の双方へのアクセスを許可する。

【 0 0 7 2 】

本実施形態では、図 1 7 を用いて説明した相互認証鍵データの全てである一部について、図 2 4 に示すように、オンライン相互認証鍵データ M K 1 とオフライン相互認証鍵データ M K 2 とをペアで用いる。 10

この場合には、相互認証を行う場合にはオンライン鍵データ M K 1 を用い、相互認証を行った相手とはデータ授受を行う場合には、それに対応するオフライン鍵データ M K 2 を用いて授受するデータを暗号化する。

これにより、仮にオンライン鍵データ M K 1 が不正に他人に取得された場合でも、被認証手段と認証手段とで授受するデータはオフライン鍵データ M K 2 で暗号化されているため、その情報が不正に漏れることを防止できる。

すなわち、第 1 実施形態における第 1 の認証鍵データ 3 2 1 がオンライン鍵データ M K 1 に対応し、第 1 実施形態における暗号鍵データ 3 2 2 がオフライン鍵データ M K 2 に対応している。また、第 1 実施形態における第 2 の認証鍵データ 3 4 1 がオンライン鍵データ M K 1 に対応し、第 1 実施形態における復号鍵データ 3 4 2 がオフライン鍵データ M K 2 に対応している。 20

【 0 0 7 3 】

以下、例えば、図 7 に示すステップ S T 3 などで行われる管理装置 2 0 の S A M 管理機能部 5 7 と S A M ユニット 9 a , 9 b との間の相互認証について説明する。

この場合に、管理装置 2 0 が被認証手段となり、S A M ユニット 9 a , 9 b が認証手段となる。

図 2 5 および図 2 6 は、管理装置 2 0 の S A M 管理機能部 5 7 と S A M ユニット 9 a との間の相互認証について説明するためのフローチャートである。

S A M ユニット 9 b についても、以下に示す S A M ユニット 9 a の場合と同じである。 30

【 0 0 7 4 】

ステップ S T 5 1 :

先ず、管理者またはユーザが、オナカード 7 2 またはユーザカード 7 3 を、カードリーダー・ライター 5 3 にセットする。

そして、オナカード 7 2 およびユーザカード 7 3 に記憶された縮退鍵データ K a (本発明の第 1 の認証鍵データ) および鍵指定データが、管理装置 2 0 の S A M 管理機能部 5 7 に読み込まれる。

S A M 管理機能部 5 7 が、乱数 R a を発生する。

【 0 0 7 5 】

ステップ S T 5 2 :

S A M 管理機能部 5 7 が、ステップ S T 5 1 で読み込んだ縮退鍵データ K a を用いて、ステップ S T 5 1 で生成した乱数 R a を、暗号化アルゴリズム 1 で暗号化してデータ R a ' を生成する。 40

ステップ S T 5 3 :

S A M 管理機能部 5 7 が、ステップ S T 5 1 で読み込んだ鍵指定データと、ステップ S T 5 2 で生成したデータ R a ' とを S A M ユニット 9 a に出力する。

S A M ユニット 9 a は、図 1 2 に示す外部 I / F 6 2 を介して、当該鍵指定データおよびデータ R a ' を入力して、これをメモリ 6 3 に格納する。

【 0 0 7 6 】

ステップ S T 5 4 :

SAMユニット9aの認証部64が、メモリ63あるいは外部メモリ7に記憶された相互認証鍵データのなかから、ステップST53で入力した鍵指定データが示す相互認証鍵データを特定する。

ステップST55：

SAMユニット9aの認証部64が、ステップST54で特定した相互認証鍵データを用いて、図20あるいは図21を用いて前述した縮退処理を行って縮退鍵データKbを生成する。

ステップST56：

SAMユニット9aの認証部64が、ステップST55で生成した縮退鍵データKbを用いて、上記暗号化アルゴリズム1に対応した復号アルゴリズム1で、ステップST53で入力したデータRa'を復号して乱数Raを生成する。

【0077】

ステップST57：

SAMユニット9aの認証部64が、上記縮退鍵データKbを用いて、暗号化アルゴリズム2で、ステップST56で生成した乱数Raを暗号化して、データRa''を生成する。

ステップST58：

SAMユニット9aの認証部64が、乱数Rbを生成する。

【0078】

ステップST59：

SAMユニット9aの認証部64が、上記縮退鍵データKbを用いて、ステップST58で生成した乱数Rbを、暗号化アルゴリズム2で暗号化してデータRb'を生成する。

ステップST60：

SAMユニット9aの認証部64が、ステップST57で生成したデータRa''と、ステップST59で生成したデータRb'とを管理装置20に出力する。

【0079】

ステップST61：

管理装置20のSAM管理機能部57が、縮退鍵データKaを用いて、上記暗号化アルゴリズム2に対応した復号アルゴリズム2で、ステップST60で入力したデータRa''およびRb'を復号してデータRa, Rbを生成する。

ステップST62：

管理装置20のSAM管理機能部57が、ステップST51で生成した乱数Raと、ステップST61で生成したデータRaとを比較する。

そして、SAM管理機能部57が、上記比較と結果が同じであることを示す場合に、SAMユニット9aが保持する上記縮退鍵データKbが、SAM管理機能部57が保持する上記縮退鍵データKaと同じであり、SAMユニット9aが正当な認証手段であると認証する。

【0080】

ステップST63：

管理装置20のSAM管理機能部57が、縮退鍵データKaを用いて、暗号化アルゴリズム1で、ステップST61で生成したデータRbを暗号化して、データRb''を生成する。

ステップST64：

管理装置20のSAM管理機能部57が、ステップST63で生成したデータRb''をSAMユニット9aに出力する。

【0081】

ステップST65：

SAMユニット9aの認証部64が、縮退鍵データKbを用いて、ステップST64で入力したデータRb''を、復号アルゴリズム1で復号してデータRbを生成する。

ステップST66：

10

20

30

40

50

S A Mユニット 9 a の認証部 6 4 が、ステップ S T 5 8 で生成した乱数 R b と、ステップ S T 6 5 で生成したデータ R b とを比較する。

そして、認証部 6 4 が、上記比較と結果が同じであることを示す場合に、S A Mユニット 9 a が保持する上記縮退鍵データ K b が、S A M管理機能部 5 7 が保持する上記縮退鍵データ K a と同じであり、S A M管理機能部 5 7 が正当な被認証手段であると認証する。

【 0 0 8 2 】

上述した図 2 5 および図 2 5 を用いて説明した相互認証方法は、例えば、図 4 に示すステップ S T 9 1 の相互認証で用いてもよい。

この場合には、データ処理装置 3 0 2 が上述した管理装置 2 0 に対応した処理を行い、データ処理装置 3 0 3 が上述した S A Mユニット 9 a , 9 b に対応した処理を行う。

10

【 0 0 8 3 】

以下、図 2 5 および図 2 6 を用いて説明した相互認証の結果を基に、S A Mユニット 9 a , 9 b が行う処理を説明する。

図 2 7 は、S A Mユニット 9 a , 9 b の処理を説明するための図である。

ステップ S T 7 1 :

図 1 2 に示す S A Mユニット 9 a , 9 b の C P U 6 5 が、図 2 6 に示すステップ S T 6 6 において、認証部 6 4 が認証手段が正当であると認証したか否かを判断し、正当であると認証したと判断した場合にはステップ S T 7 2 の処理に進み、そうでない場合には処理を終了する(すなわち、処理に係わる権限を有しないと判断し、処理を実行しない)。

【 0 0 8 4 】

20

ステップ S T 7 2 :

S A Mユニット 9 a , 9 b の C P U 6 5 が、復号鍵データを用いて、管理装置 2 0 から入力した暗号化されたデータ(暗号化データ)を、上記第 2 の暗号アルゴリズムに対応した第 2 の復号アルゴリズムで復号する。

そして、S A Mユニット 9 a , 9 b が、上記復号データが、適切に復号されたものであるか否かを判断し、適切に復号されたものであると判断した場合には、当該復号データを有効なものとして用いて、オナカード 7 2 等に許可した上記相互認証鍵データに関連付けられた処理を実行する。

一方、S A Mユニット 9 a , 9 b が、上記復号データが適切に復号されたものではないと判断した場合には、当該復号データを破棄(無効化)する。

30

【 0 0 8 5 】

以上説明したように、通信システム 1 によれば、管理装置 2 0 と S A Mユニット 9 a , 9 b との間の相互認証と、管理装置 2 0 から S A Mユニット 9 a に出力する暗号化データの生成とを異なる鍵データを用いて行うため、相互認証により用いた縮退鍵データが第三者によって不正に取得された場合でも、暗号化データは暗号鍵データを用いて暗号化されているため、当該第三者は当該暗号化データを解読できない。そのため、暗号化データを適切に保護できる。

また、通信システム 1 によれば、相互認証と暗号化データの生成とで異なる暗号・復号アルゴリズムを用いることで、相互認証で用いた暗号・復号アルゴリズムが第三者に漏れた場合でも、暗号化データは他の暗号アルゴリズムで暗号化されているため、当該第三者は解読できない。

40

【 0 0 8 6 】

また、管理装置 2 0 によれば、図 1 6 および図 2 0 等を用いて説明したように、S A Mユニット 9 a , 9 b に係わる処理に関連付けられた複数の相互認証鍵データを用いて縮退処理を行い、縮退鍵データを生成する。

そして、オナカード 7 2 やユーザカード 7 3 に、当該縮退鍵データ、並びにその生成に用いた相互認証鍵データを特定するための鍵指定データを書き込む。

また、オナカード 7 2 等を用いた管理装置 2 0 と S A Mユニット 9 a , 9 b との間で、図 2 5 ~ 図 2 7 を用いた相互認証を行うことで、S A Mユニット 9 a が管理装置 2 0 から受けた鍵指定データを基に縮退鍵データを生成し、当該縮退鍵データが管理装置 2 0 が保

50

持するものと一致した場合に、被認証手段である管理装置 20 の正当性を確認できる。
また、その確認と共に、鍵指定データによって指定された相互認証鍵データに関連付けられた処理を、管理装置 20 に許可された処理であると判断できる。

そのため、認証手段である SAM ユニット 9 a , 9 b は、従来のように全ての被認証手段（例えば、オーナーカード 7 2 およびユーザカード 7 3 を用いた管理装置 20 等）に対応した相互認証鍵データを保持する必要がなく、しかも、被認証手段に許可した処理を管理テーブルで管理する必要もなく、処理負担が軽減される。

【0087】

本発明は上述した実施形態には限定されない。

本発明は、例えば、オーナーカード 7 2、ユーザカード 7 3、トランスポートカード 7 4 および AP 暗号化カード 7 5 の何れかのカードの IC に、そのカードの使用者の生体情報を記憶させ、SAM ユニット 9 a , 9 b が、上述した相互認証と共に、当該カードに記憶された生体情報をさらに用いて、その使用者の正当性を認証してもよい。

【0088】

例えば、上述した実施形態では、SAM ユニット 9 a , 9 b が管理装置 20 と相互認証を行う場合を例示したが、SAM ユニット 9 a , 9 b が ASP サーバ装置 19 a , 19 b や他の SAM ユニットなどの被認証手段と認証を行ってもよい。この場合には、当該被認証手段が、上述した縮退鍵データおよび鍵指定データを保持する。

また、上述した実施形態では、オーナーカード 7 2 およびユーザカード 7 3 が、上述した縮退鍵データおよび鍵指定データを保持する場合を例示したが、その他の携帯装置などに、これらのデータを保持させてもよい。

【0089】

【発明の効果】

以上説明したように、本発明によれば、認証の鍵データが不正に第三者によって取得された場合でも、認証に続いて提供された暗号化データがその第三者によって解読されないようにすることを可能にするデータ処理方法、そのプログラムおよびその装置を提供することができる。

【図面の簡単な説明】

【図 1】図 1 は、本発明の第 1 実施形態に係わるデータ処理システムの構成図である。

【図 2】図 2 は、図 1 に示す出力側のデータ処理装置の構成図である。

【図 3】図 3 は、図 1 に示す入力側のデータ処理装置の構成図である。

【図 4】図 4 は、図 1 に示すデータ処理システムの動作例を説明するためのフローチャートである。

【図 5】図 5 は、本発明の第 2 実施形態の通信システムの全体構成図である。

【図 6】図 6 は、図 5 に示す管理装置の機能ブロック図である。

【図 7】図 7 は、図 6 に示す管理装置が行う処理手順の概要を説明するためのフローチャートである。

【図 8】図 8 は、図 6 に示す AP 編集ツールおよび管理ツールに係わる処理において用いられるカードを説明するための図である。

【図 9】図 9 は、図 5 に示す IC カードの機能ブロック図である。

【図 10】図 10 は、図 9 に示すメモリに記憶されたデータを説明するための図である。

【図 11】図 11 は、図 5 に示す SAM モジュールのソフトウェア構成を説明するための図である。

【図 12】図 12 は、図 5 に示す SAM モジュールのハードウェア構成、並びに外部メモリ 7 の記憶領域を説明するための図である。

【図 13】図 13 は、図 12 に示す AP 記憶領域を説明するための図である。

【図 14】図 14 は、アプリケーションエレメントデータを説明するための図である。

【図 15】図 15 は、アプリケーションエレメントデータ APE のタイプを説明するための図である。

【図 16】図 16 は、オーナーカードおよびユーザカードの作成手順を説明するためのフロ

ーチャートである。

【図17】図17は、相互認証鍵データを説明するための図である。

【図18】図18は、相互認証コードを説明するための図である。

【図19】図19は、相互認証鍵データとサービスとの関係を説明するための図である。

【図20】図20は、縮退鍵データの生成方法を説明するための図である。

【図21】図21は、縮退鍵データのその他の生成方法を説明するための図である。

【図22】図22は、縮退鍵データの暗号化の階層を説明するための図である。

【図23】図23は、縮退鍵データの特性の一例を説明するための図である。

【図24】図24は、相互認証鍵データの使用形態の一例を説明するための図である。

【図25】図25は、図5に示す管理装置のSAM管理機能部とSAMユニットとの間の相互認証について説明するためのフローチャートである。 10

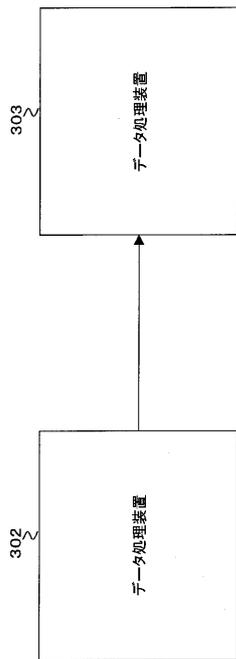
【図26】図26は、図5に示す管理装置のSAM管理機能部とSAMユニットとの間の相互認証について説明するための図25の続きのフローチャートである。

【図27】図27は、SAMユニットの処理を説明するためのフローチャートである。

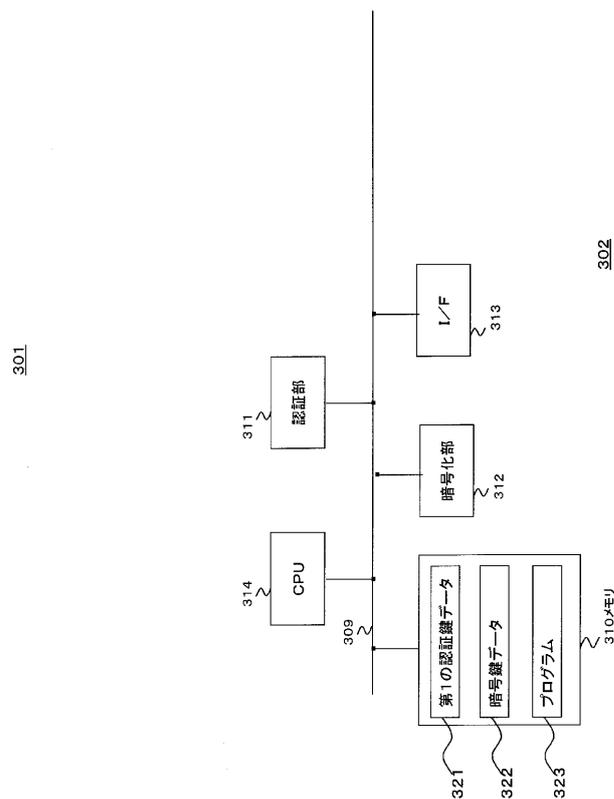
【符号の説明】

- 1 ... 通信システム、2 ... サーバ装置、3 ... ICカード、4 ... カードRW、6 ... PC、7 ... 外部メモリ、8 ... SAMモジュール、9 a , 9 b ... SAMユニット、19 a , 19 b ... ASPサーバ装置、20 ... 管理装置、51 ... AP編集ツール、52 ... 管理ツール、53 ... カードリーダー・ライター、54 ... ディスプレイ、55 ... I/F、56 ... 操作部、57 ... SAM管理機能部、58 ... カード管理機能部、61 ... メモリI/F、62 ... 外部I/F、63 ... 20
- メモリ、64 ... 認証部、65 ... CPU、71 ... デフォルトカード、72 ... オーナカード、73 ... ユーザカード、74 ... トランスポートカード、75 ... AP暗号化カード、301 ... データ処理システム、302 , 303 ... データ処理装置302、310 ... メモリ、311 ... 認証部、312 ... 暗号化部、313 ... インタフェース、314 ... CPU、330 ... メモリ、331 ... 認証部、332 ... 復号部、333 ... I/F

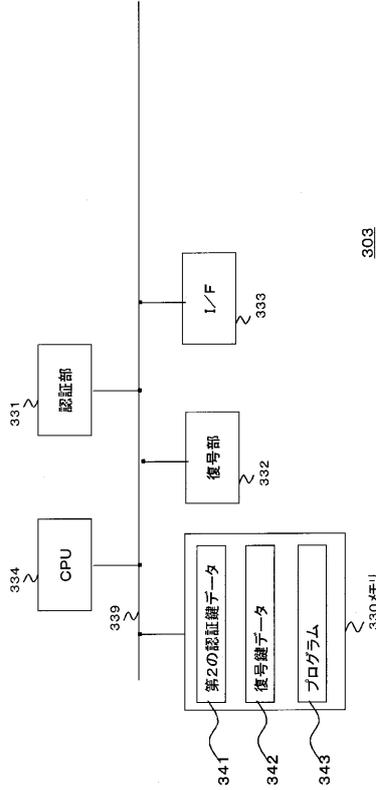
【図1】



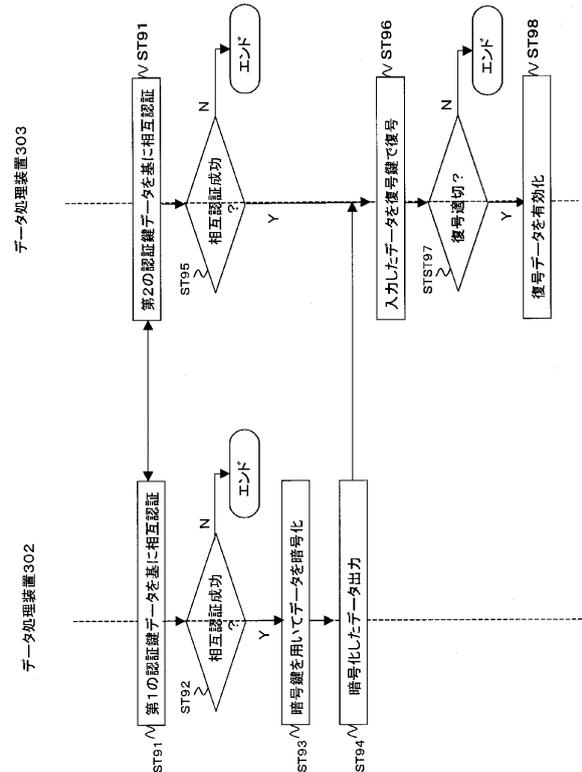
【図2】



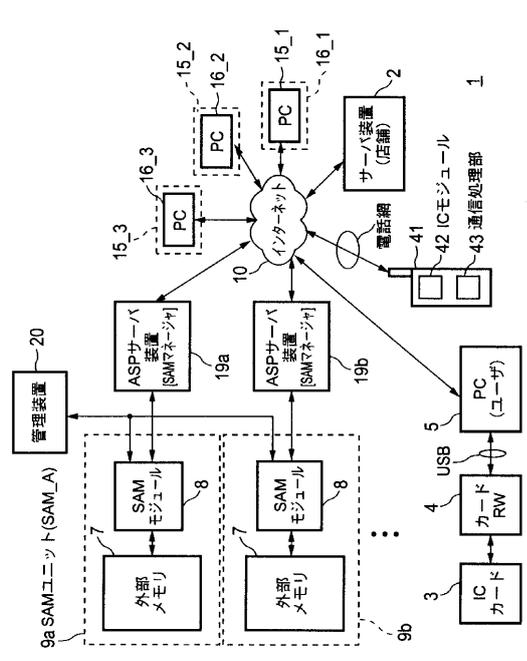
【 図 3 】



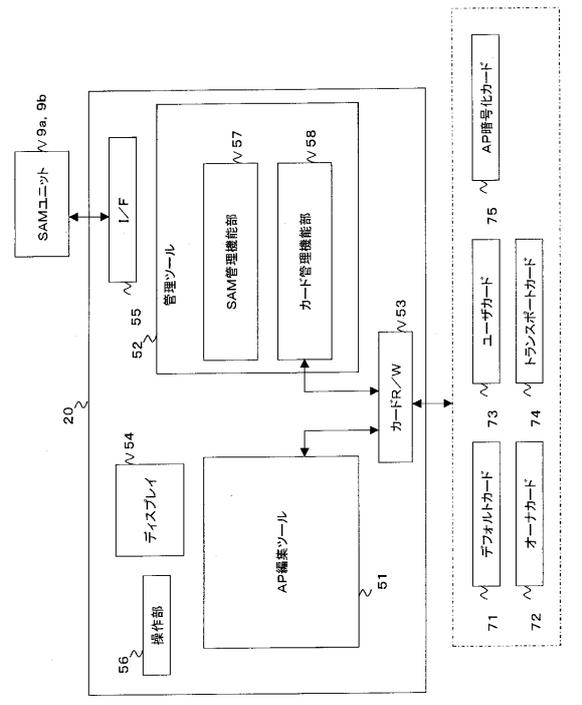
【 図 4 】



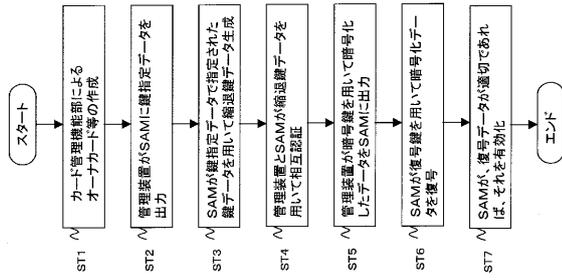
【 図 5 】



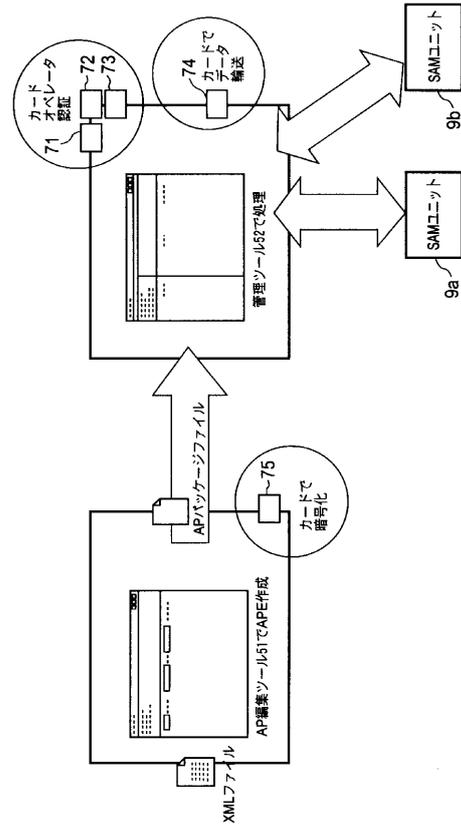
【 図 6 】



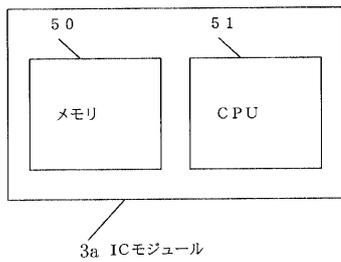
【 図 7 】



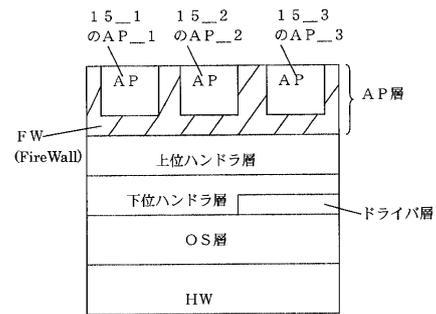
【 図 8 】



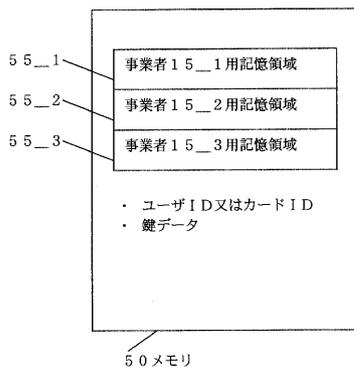
【 図 9 】



【 図 1 1 】

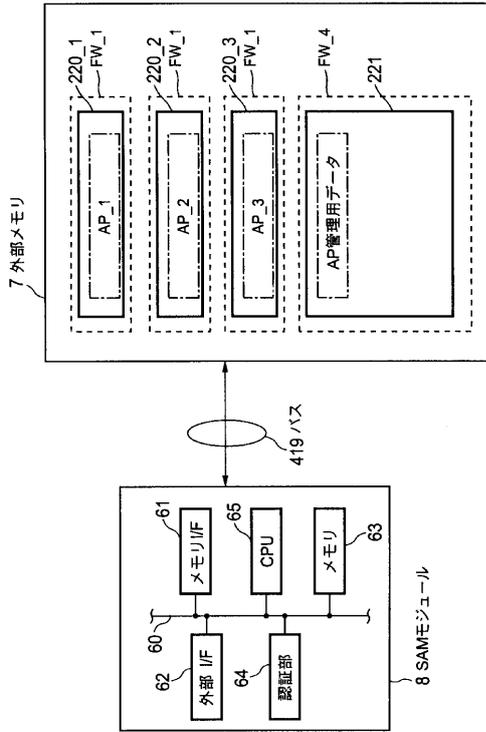


【 図 1 0 】

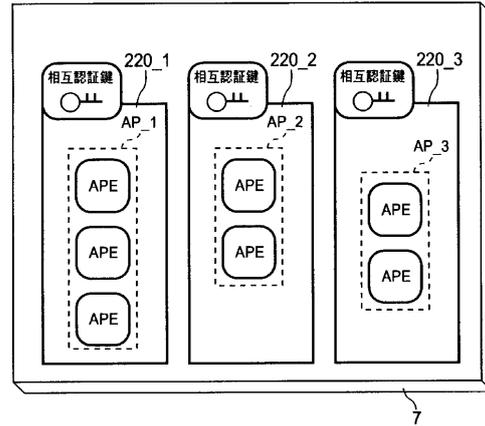


SAMモジュールのソフトウェア構成

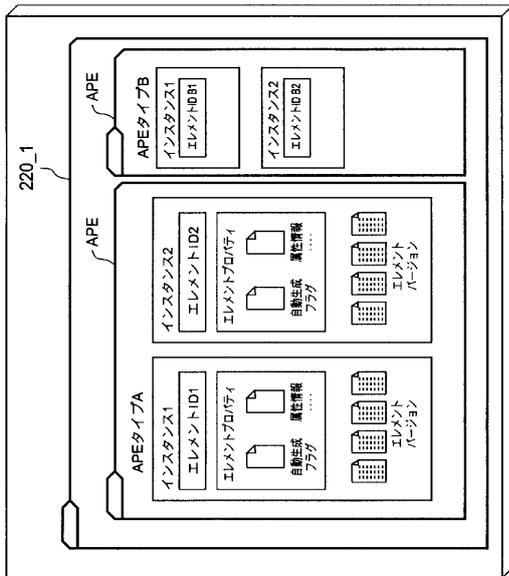
【図 1 2】



【図 1 3】



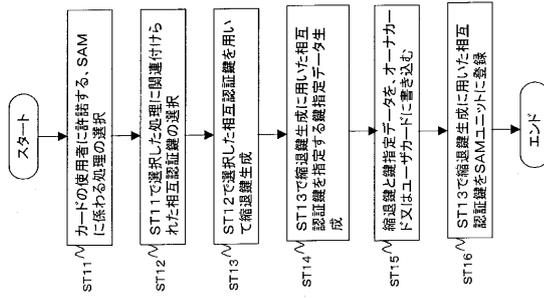
【図 1 4】



【図 1 5】

APE タイプ番号	APEタイプ
...	ICシステム鍵
...	ICエリア鍵
...	ICサービス鍵
...	IC縮退鍵
...	IC鍵変更パッケージ
...	IC発行鍵パッケージ
...	IC拡張発行鍵パッケージ
...	ICエリア登録鍵パッケージ
...	ICエリア削除鍵パッケージ
...	ICサービス登録鍵パッケージ
...	ICサービス削除鍵パッケージ
...	ICメモリ分割鍵パッケージ
...	ICメモリ分割素鍵パッケージ
...	障害記録ファイル
...	相互認証用鍵
...	パッケージ鍵
...	ネガリスト
...	サービスデータテンポラリファイル

【 図 1 6 】



【 図 1 7 】

相互認証鍵名	AP記号領域・ID	APEタイプ番号	インスタンス番号	エレメントバージョン
デバイス鍵
ターミネーション鍵
製造設定サービス相互認証鍵
機器管理サービス相互認証鍵
通信管理サービス相互認証鍵
相互認証サービス相互認証鍵
AP記号領域管理サービス相互認証鍵
サービスAP・記号領域相互認証鍵
システムAP・記号領域相互認証鍵
製造者AP記号領域相互認証鍵

【 図 1 8 】

AP記号領域ID	エレメントタイプ番号	エレメントインスタンス番号	エレメントバージョン番号
2バイト	2バイト	2バイト	2バイト
所属するAPリソース領域	相互認証鍵 (固定値)	リリース鍵リングのID	使用する鍵のバージョン番号

相互認証コード

【 図 1 9 】

相互認証鍵名	AP記号領域ID	APEタイプ番号	インスタンス番号	エレメントバージョン番号
デバイス鍵
機器管理サービス相互認証鍵
通信管理サービス相互認証鍵
AP記号領域管理サービス相互認証鍵
サービスAP記号領域AP-R相互認証鍵
ターミネーション鍵

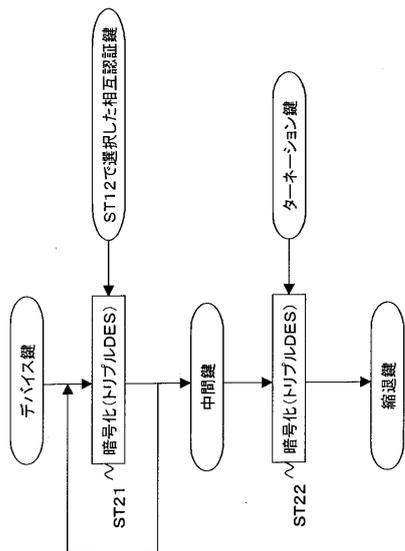
・実行可能なコマンド

サービス種別	コマンド名
機器管理サービス	...
通信管理サービス	...
ICサービス	...
相互認証サービス	...
AP記号領域管理サービス	...

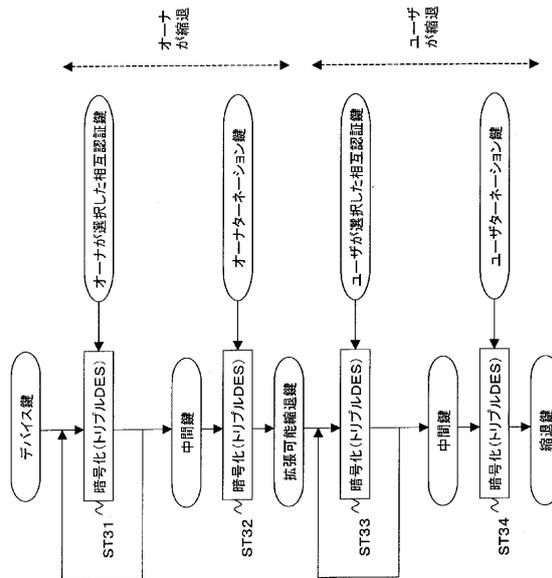
(A)

(B)

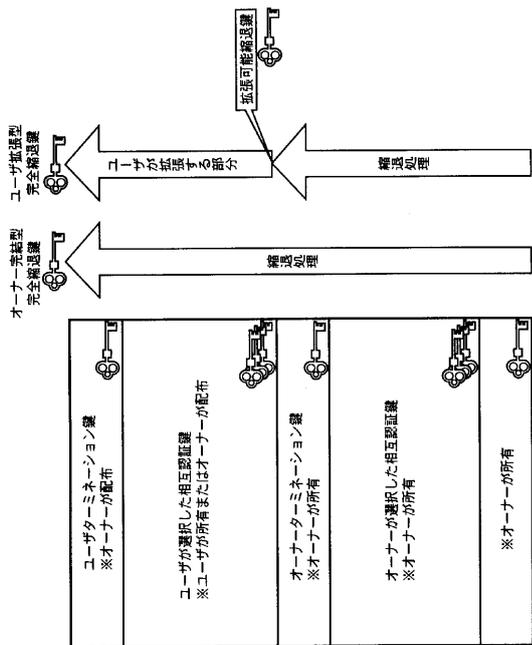
【 図 2 0 】



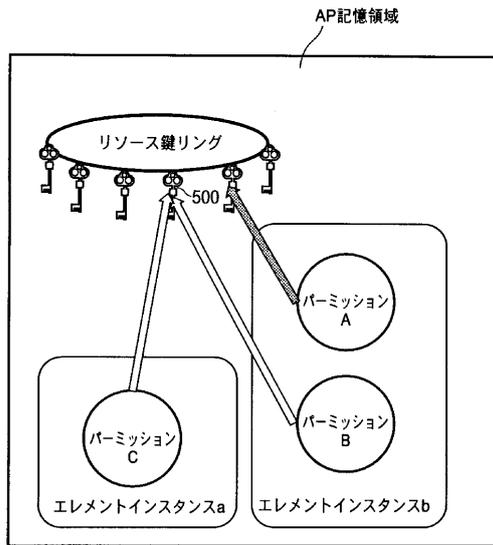
【 図 2 1 】



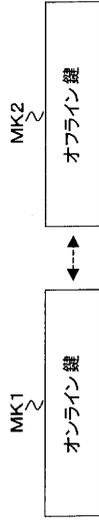
【 図 2 2 】



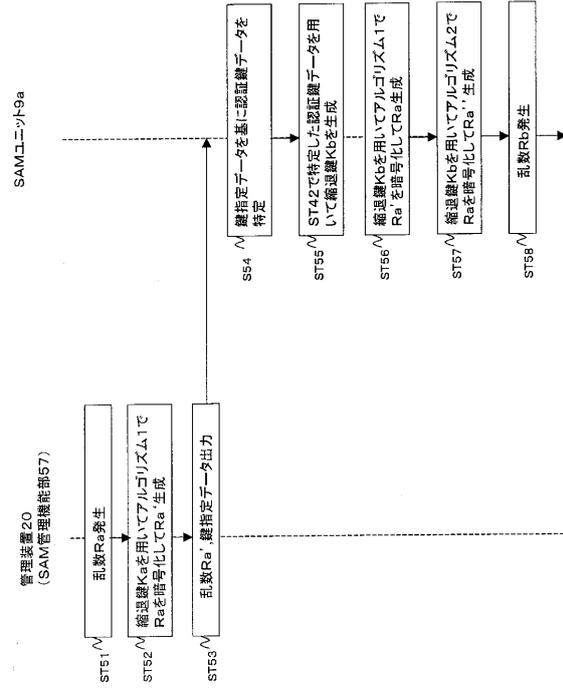
【 図 2 3 】



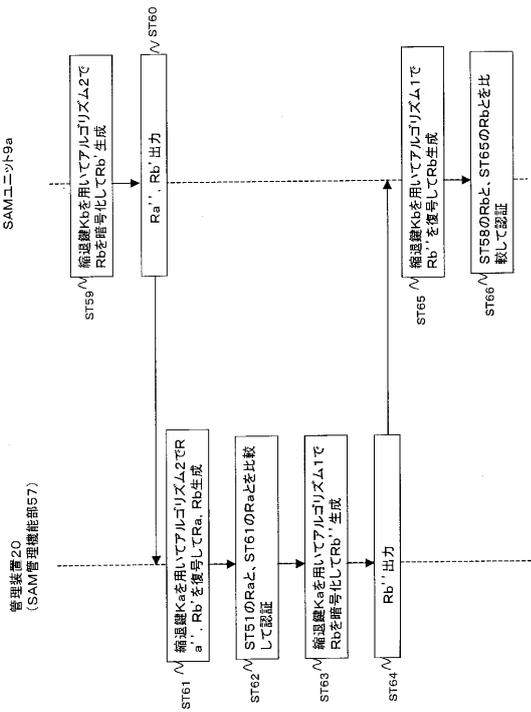
【 図 2 4 】



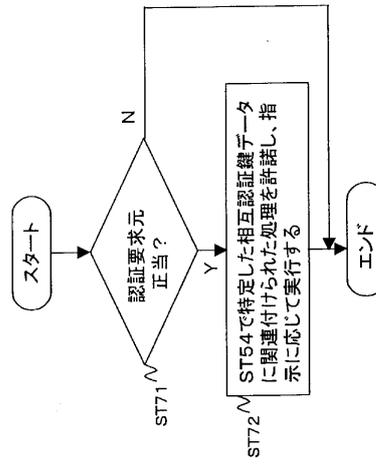
【 図 2 5 】



【 図 2 6 】



【 図 2 7 】



フロントページの続き

(72)発明者 花木 直文

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(72)発明者 館野 啓

東京都品川区北品川6丁目7番35号 ソニー株式会社内

Fターム(参考) 5B085 AE04 AE09 AE29

5J104 AA07 AA16 EA04 EA18 EA22 JA03 JA13 JA31 KA02 KA04

KA06 NA02 NA35 NA37 NA40 PA07