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

特許第5201716号
(P5201716)

(45)発行日　平成25年6月5日(2013.6.5)　(24)登録日　平成25年2月22日(2013.2.22)

(51)Int.Cl.		F I		
H04L 9/08	(2006.01)	H04L	9/00	601B
H04L 9/14	(2006.01)	H04L	9/00	641
G06F 21/12	(2013.01)	G06F	21/22	112C
G06F 21/64	(2013.01)	G06F	21/24	167A

請求項の数 25　(全 56 頁)

(21)出願番号　特願2007-255963(P2007-255963)
(22)出願日　平成19年9月28日(2007.9.28)
(65)公開番号　特開2009-89000(P2009-89000A)
(43)公開日　平成21年4月23日(2009.4.23)
審査請求日　平成22年6月15日(2010.6.15)

(出願人による申告)平成１５年度から平成１７年度、独立行政法人情報通信研究機構、高度通信・放送研究に関する委託事業、産業技術力強化法第１９条の適用を受ける特許出願

(73)特許権者　301063496
東芝ソリューション株式会社
東京都港区芝浦一丁目１番１号
(73)特許権者　397065136
株式会社横須賀テレコムリサーチパーク
神奈川県横須賀市光の丘３番４号
(74)代理人　100108855
弁理士　蔵田　昌俊
(74)代理人　100091351
弁理士　河野　哲
(74)代理人　100088683
弁理士　中村　誠
(74)代理人　100109830
弁理士　福原　淑弘

最終頁に続く

(54)【発明の名称】暗号モジュール配信システム、暗号管理サーバ装置、暗号処理装置、クライアント装置、暗号管理プログラム、暗号処理プログラム、およびクライアントプログラム

(57)【特許請求の範囲】
【請求項１】
互いに通信が可能な、暗号管理サーバ装置と、暗号処理装置と、クライアント装置とを部有する暗号モジュール配信システムにおいて、
前記暗号管理サーバ装置は、
暗号モジュールを格納する暗号モジュール格納部と、
前記クライアント装置を識別する端末識別情報に対応付けて、当該クライアント装置に搭載中の暗号モジュールの識別情報と、当該クライアント装置に搭載可能な暗号モジュールの識別情報とが記述された対応表を記憶する記憶手段と、
前記クライアント装置から端末情報を受信すると、当該受信した端末情報に含まれる端末識別情報に基づいて前記対応表から当該クライアント装置に搭載可能な暗号モジュールの識別情報を読み出し、当該読み出した識別情報に対応する暗号モジュールを前記暗号モジュール格納部から選定する選定手段と、
暗号処理装置と共通で利用可能な共有鍵を共有する鍵共有部と、
当該共有鍵で前記選定された暗号モジュールを暗号化する暗号モジュール暗号化部と、
当該暗号化された暗号モジュールをクライアント装置に送信するクライアント装置通信処理部と、
を有し、
前記暗号処理装置は、
暗号管理サーバ装置と共通で利用可能な共有鍵を共有する鍵共有部と、

暗号化された暗号モジュールをクライアント装置より受信し、この受信した暗号化された暗号モジュールを、前記共有鍵を用いて復号する暗号モジュール復号部と、
前記復号した暗号モジュールをクライアント装置へ送信するクライアント装置通信処理部と、を有し、
前記クライアント装置は、
自装置を識別する端末識別情報を含む端末情報を格納する端末情報格納部と、
前記端末情報格納部に格納されている端末情報を前記暗号管理サーバ装置に送信する送信手段と、
前記暗号管理サーバ装置から暗号化された暗号モジュールを受信するサーバ通信処理部と、
前記受信した暗号化された暗号モジュールを暗号処理装置に送信し、復号された暗号モジュールを前記暗号処理装置から受信する暗号処理装置通信処理部と、
前記暗号処理装置通信処理部により受信した暗号モジュールを格納する暗号モジュール格納部と、
を有することを特徴とする暗号モジュール配信システム。
【請求項２】
互いに通信が可能な、暗号管理サーバ装置と、暗号処理装置と、クライアント装置とを有する暗号モジュール配信システムにおいて、
前記暗号管理サーバ装置は、
暗号モジュールを格納する暗号モジュール格納部と、
前記クライアント装置を識別する端末識別情報に対応付けて、当該クライアント装置に搭載中の暗号モジュールの識別情報と、当該クライアント装置に搭載可能な暗号モジュールの識別情報とが記述された対応表を記憶する記憶手段と、
前記クライアント装置から端末情報を受信すると、当該受信した端末情報に含まれる端末識別情報に基づいて前記対応表から当該クライアント装置に搭載可能な暗号モジュールの識別情報を読み出し、当該読み出した識別情報に対応する暗号モジュールを前記暗号モジュール格納部から選定する選定手段と、
暗号処理装置と共通で利用可能な共有鍵を共有する鍵共有部と、
当該共有鍵で前記選定された暗号モジュールを識別する認証子を生成する認証子生成部と、
前記選定された暗号モジュールおよび認証子をクライアント装置に送信するクライアント装置通信処理部と、
を有し、
前記暗号処理装置は、
暗号管理サーバ装置と共通で利用可能な共有鍵を共有する鍵共有部と、
クライアント装置より認証子を受信し、当該受信した認証子に対して、前記鍵格納部に格納された共有鍵を用いて認証子の正当性検証を行う認証子検証部と、
前記正当性検証を行った結果をクライアント装置へ送信するクライアント装置通信処理部と、
を有し、
前記クライアント装置は、
自装置を識別する端末識別情報を含む端末情報を格納する端末情報格納部と、
前記端末情報格納部に格納されている端末情報を前記暗号管理サーバ装置に送信する送信手段と、
前記暗号管理サーバ装置より暗号モジュールおよび認証子を受信するサーバ通信処理部と、
前記サーバ通信処理部によって受信した認証子を暗号処理装置に送信し、当該認証子の正当性検証結果を受信する暗号処理装置通信処理部と、
前記暗号処理装置通信処理部により受信した認証子の正当性検証結果が正当であることを示す情報であるならば、前記受信した暗号モジュールを格納する暗号モジュール格納部

と、
を有することを特徴とする暗号モジュール配信システム。
【請求項３】
前記暗号管理サーバ装置は、
前記共有鍵で前記暗号モジュールを暗号化する暗号モジュール暗号化部を有し、
前記クライアント装置通信処理部が、前記暗号モジュール暗号化部によって暗号化された暗号モジュールをクライアント装置に送信し、
前記暗号処理装置は、
クライアント装置通信処理部が、暗号化された暗号モジュールおよび認証子をクライアント装置より受信し、前記共有鍵を用いて暗号化された暗号モジュールを復号した暗号モジュールと当該認証子の正当性検証を行った結果とをクライアント装置へ送信し、
前記クライアント装置は、
暗号処理装置通信処理部が、前記サーバ通信処理部によって受信する暗号化された暗号モジュールおよび認証子を暗号処理装置に送信し、復号された暗号モジュールおよび認証子の正当性検証結果を受信し、
前記暗号処理装置通信処理部により受信した認証子の正当性検証結果が正当であることを示す情報であるならば、復号された暗号モジュールを暗号モジュール格納部に格納する
ことを特徴とする請求項２に記載の暗号モジュール配信システム。
【請求項４】
前記暗号管理サーバ装置は、
暗号モジュールを暗号処理装置が処理可能なデータサイズに分割して分割暗号モジュールを生成する暗号モジュール分割部とを有し、
前記暗号モジュール暗号化部が、前記共有鍵で前記分割暗号モジュール毎に暗号化し、
前記クライアント装置通信処理部が、前記暗号化された分割暗号モジュール全てをクライアント装置に送信し、
前記暗号処理装置は、
クライアント装置通信処理部が、暗号化された分割暗号モジュールをクライアント装置より受信し、前記共有鍵を用いて復号した分割暗号モジュールをクライアント装置へ送信し、
前記暗号モジュール復号部が、クライアント装置より受信した暗号化された分割暗号モジュールを、前記共有鍵を用いて復号し、
前記クライアント装置は、
前記暗号処理装置通信処理部より受信した分割暗号モジュール全てを結合して暗号モジュールを復元する暗号モジュール結合部を有し、
前記サーバ通信処理部が、前記暗号管理サーバ装置より暗号化された分割暗号モジュール全てを受信し、
前記暗号処理装置通信処理部が、前記受信した暗号化された分割暗号モジュールを暗号処理装置に送信し、復号された分割暗号モジュールを受信し、
暗号モジュール結合部が、前記暗号モジュール結合部によって結合された暗号モジュールを前記暗号モジュール格納部に格納する
ことを特徴とする請求項１または請求項３のうちいずれかに記載の暗号モジュール配信システム。
【請求項５】
前記暗号管理サーバ装置は、
暗号モジュールを暗号処理装置が処理可能なデータサイズに分割して分割暗号モジュールを生成する暗号モジュール分割部とを有し、
前記認証子生成部が、共有鍵で前記分割暗号モジュール毎に認証子を生成し、
前記クライアント装置通信処理部が、前記分割暗号モジュールと前記認証子全てをクライアント装置に送信し、
前記暗号処理装置は、

クライアント装置通信処理部が、クライアント装置より分割暗号モジュールおよび認証子を受信し、前記共有鍵を用いて認証子の正当性検証を行った結果をクライアント装置へ送信し、

前記認証子検証部が、クライアント装置より受信した分割暗号モジュールおよび認証子に対して、前記共有鍵を用いて認証子の正当性検証を行い、

前記クライアント装置は、

受信した分割暗号モジュール全てを結合して暗号モジュールを復元する暗号モジュール結合部を有し、

前記サーバ通信処理部が、前記暗号管理サーバ装置より分割暗号モジュールおよび認証子全てを受信し、

前記暗号処理装置通信処理部が、前記受信した分割暗号モジュールおよび認証子を暗号処理装置に送信し、認証子の正当性検証結果を受信し、

前記暗号処理装置通信処理部により受信した認証子の検証結果が全て正当であることを示す情報であるならば、前記暗号モジュール結合部によって結合された暗号モジュールを前記暗号モジュール格納部に格納する

ことを特徴とする請求項２または請求項３のうちいずれかに記載の暗号モジュール配信システム。

【請求項６】

前記暗号化された分割暗号モジュールは、少なくとも２つ以上の異なる鍵のいずれかによってそれぞれ暗号化されていることを特徴とする請求項４に記載の暗号モジュール配信システム。

【請求項７】

前記認証子は、少なくとも２つ以上の異なる鍵のいずれかによってそれぞれ生成されていることを特徴とする請求項５に記載の暗号モジュール配信システム。

【請求項８】

暗号処理装置とクライアント装置と通信し、当該クライアント装置に暗号モジュールを配信する暗号管理サーバ装置であって、

暗号モジュールを格納する暗号モジュール格納部と、

前記クライアント装置を識別する端末識別情報に対応付けて、当該クライアント装置に搭載中の暗号モジュールの識別情報と、当該クライアント装置に搭載可能な暗号モジュールの識別情報とが記述された対応表を記憶する記憶手段と、

前記クライアント装置から端末情報を受信すると、当該受信した端末情報に含まれる端末識別情報に基づいて前記対応表から当該クライアント装置に搭載可能な暗号モジュールの識別情報を読み出し、当該読み出した識別情報に対応する暗号モジュールを前記暗号モジュール格納部から選定する選定手段と、

前記暗号処理装置と共通で利用可能な共有鍵を共有する鍵共有部と、

当該共有鍵で前記選定された暗号モジュールを暗号化する暗号モジュール暗号化部と、

当該暗号化された暗号モジュールを前記クライアント装置に送信するクライアント装置通信処理部と、

を備えることを特徴とする暗号管理サーバ装置。

【請求項９】

暗号処理装置とクライアント装置と通信し、当該クライアント装置に暗号モジュールを配信する暗号管理サーバ装置であって、

暗号モジュールを格納する暗号モジュール格納部と、

前記クライアント装置を識別する端末識別情報に対応付けて、当該クライアント装置に搭載中の暗号モジュールの識別情報と、当該クライアント装置に搭載可能な暗号モジュールの識別情報とが記述された対応表を記憶する記憶手段と、

前記クライアント装置から端末情報を受信すると、当該受信した端末情報に含まれる端末識別情報に基づいて前記対応表から当該クライアント装置に搭載可能な暗号モジュールの識別情報を読み出し、当該読み出した識別情報に対応する暗号モジュールを前記暗号モ

ジュール格納部から選定する選定手段と、
前記暗号処理装置と共通で利用可能な共有鍵を共有する鍵共有部と、
当該共有鍵で前記選定された暗号モジュールを識別する認証子を生成する認証子生成部と、
前記選定された暗号モジュールおよび前記認証子を前記クライアント装置に送信するクライアント装置通信処理部と、
を備えることを特徴とする暗号管理サーバ装置。
【請求項１０】
前記共有鍵で前記暗号モジュールを暗号化する暗号モジュール暗号化部と、をさらに有し、
前記クライアント装置通信処理部は、当該暗号化された暗号モジュールを前記クライアント装置に送信すること
をさらに特徴とする請求項９に記載の暗号管理サーバ装置。
【請求項１１】
前記暗号モジュールを暗号処理装置が処理可能なデータサイズに分割して分割暗号モジュールを生成する暗号モジュール分割部をさらに有し、
前記暗号モジュール暗号化部が、前記共有鍵で前記分割暗号モジュール毎に暗号化し、
前記クライアント装置通信処理部が、前記暗号化された分割暗号モジュール全てをクライアント装置に送信する
ことを特徴とする請求項８または請求項１０に記載の暗号管理サーバ装置。
【請求項１２】
暗号モジュールを暗号処理装置が処理可能なデータサイズに分割して分割暗号モジュールを生成する暗号モジュール分割部とを有し、
前記認証子生成部が、共有鍵で前記分割暗号モジュール毎に認証子を生成し、
前記クライアント装置通信処理部が、前記分割暗号モジュールと前記認証子全てをクライアント装置に送信する
ことを特徴とする請求項９または請求項１０に記載の暗号管理サーバ装置。
【請求項１３】
請求項８に記載の暗号管理サーバ装置と暗号処理装置と通信し、前記暗号管理サーバ装置より暗号モジュールを配信されるクライアント装置であって、
自装置を識別する端末識別情報を含む端末情報を格納する端末情報格納部と、
前記端末情報格納部に格納されている端末情報を前記暗号管理サーバ装置に送信する送信手段と、
前記暗号管理サーバ装置から暗号化された暗号モジュールを受信するサーバ通信処理部と、
前記受信した暗号化された暗号モジュールを前記暗号処理装置に送信し、復号された暗号モジュールを前記暗号処理装置から受信する暗号処理装置通信処理部と、
前記暗号処理装置通信処理部により受信した暗号モジュールを格納する暗号モジュール格納部と、
を有することを特徴とするクライアント装置。
【請求項１４】
請求項９に記載の暗号管理サーバ装置と暗号処理装置と通信し、前記暗号管理サーバ装置より暗号モジュールを配信されるクライアント装置であって、
自装置を識別する端末識別情報を含む端末情報を格納する端末情報格納部と、
前記端末情報格納部に格納されている端末情報を前記暗号管理サーバ装置に送信する送信手段と、
前記暗号管理サーバ装置より暗号モジュールおよび認証子を受信するサーバ通信処理部と、
前記サーバ通信処理部によって受信した認証子を暗号処理装置に送信し、当該認証子の正当性検証結果を受信する暗号処理装置通信処理部と、

前記暗号処理装置通信処理部により受信した認証子の正当性検証結果が正当であることを示す情報であるならば、前記受信した暗号モジュールを格納する暗号モジュール格納部と、
を有することを特徴とするクライアント装置。
【請求項１５】
前記暗号処理装置通信処理部が、前記サーバ通信処理部によって受信する暗号化された暗号モジュールおよび認証子を暗号処理装置に送信し、復号された暗号モジュールおよび認証子の正当性検証結果を受信し、
前記暗号処理装置通信処理部により受信した認証子の正当性検証結果が正当であることを示す情報であるならば、復号された暗号モジュールを暗号モジュール格納部に格納する
ことを特徴とする請求項１４に記載のクライアント装置。
【請求項１６】
前記暗号処理装置通信処理部より受信した分割暗号モジュール全てを結合して暗号モジュールを復元する暗号モジュール結合部を有し、
前記サーバ通信処理部が、前記暗号管理サーバ装置より暗号化された分割暗号モジュール全てを受信し、
前記暗号処理装置通信処理部が、前記受信した暗号化された分割暗号モジュールを暗号処理装置に送信し、復号された分割暗号モジュールを受信し、
暗号モジュール結合部が、前記暗号モジュール結合部によって結合された暗号モジュールを前記暗号モジュール格納部に格納する
ことを特徴とする請求項１３または請求項１５のうちいずれかに記載のクライアント装置。
【請求項１７】
受信した分割暗号モジュール全てを結合して暗号モジュールを復元する暗号モジュール結合部を有し、
前記サーバ通信処理部が、前記暗号管理サーバ装置より分割暗号モジュールおよび認証子全てを受信し、
前記暗号処理装置通信処理部が、前記受信した分割暗号モジュールおよび認証子を暗号処理装置に送信し、認証子の正当性検証結果を受信し、
前記暗号処理装置通信処理部により受信した認証子の検証結果が全て正当であることを示す情報であるならば、前記暗号モジュール結合部によって結合された暗号モジュールを前記暗号モジュール格納部に格納する
ことを特徴とする請求項１４または請求項１５のうちいずれかに記載のクライアント装置。
【請求項１８】
請求項８に記載の暗号管理サーバ装置とクライアント装置と通信し、前記暗号管理サーバ装置から前記クライアント装置に暗号モジュールを配信するときの暗号処理を行う暗号処理装置であって、
前記暗号管理サーバ装置と共通で利用可能な共有鍵を共有する鍵共有部と、
暗号化された暗号モジュールをクライアント装置より受信し、この受信した暗号化された暗号モジュールを、前記共有鍵を用いて復号する暗号モジュール復号部と、
前記復号した暗号モジュールをクライアント装置へ送信するクライアント装置通信処理部と、
を有することを特徴とする暗号処理装置。
【請求項１９】
請求項９に記載の暗号管理サーバ装置とクライアント装置と通信し、前記暗号管理サーバ装置から前記クライアント装置に暗号モジュールを配信するときの暗号処理を行う暗号処理装置であって、
前記暗号管理サーバ装置より暗号モジュールおよび認証子を受信するサーバ通信処理部と、

前記サーバ通信処理部によって受信した認証子を暗号処理装置に送信し、当該認証子の正当性検証結果を受信する暗号処理装置通信処理部と、
前記暗号処理装置通信処理部により受信した認証子の正当性検証結果が正当であることを示す情報であるならば、前記受信した暗号モジュールを格納する暗号モジュール格納部と、
を有することを特徴とする暗号処理装置。
【請求項２０】
前記暗号処理装置通信処理部が、前記サーバ通信処理部によって受信する暗号化された暗号モジュールおよび認証子を暗号処理装置に送信し、復号された暗号モジュールおよび認証子の正当性検証結果を受信し、
前記暗号処理装置通信処理部により受信した認証子の正当性検証結果が正当であることを示す情報であるならば、復号された暗号モジュールを暗号モジュール格納部に格納する
ことを特徴とする請求項１９に記載の暗号処理装置。
【請求項２１】
前記暗号処理装置通信処理部より受信した分割暗号モジュール全てを結合して暗号モジュールを復元する暗号モジュール結合部を有し、
前記サーバ通信処理部が、前記暗号管理サーバ装置より暗号化された分割暗号モジュール全てを受信し、
前記暗号処理装置通信処理部が、前記受信した暗号化された分割暗号モジュールを暗号処理装置に送信し、復号された分割暗号モジュールを受信し、
暗号モジュール結合部が、前記暗号モジュール結合部によって結合された暗号モジュールを前記暗号モジュール格納部に格納する
ことを特徴とする請求項１８または請求項２０のうちいずれかに記載の暗号処理装置。
【請求項２２】
受信した分割暗号モジュール全てを結合して暗号モジュールを復元する暗号モジュール結合部を有し、
前記サーバ通信処理部が、前記暗号管理サーバ装置より分割暗号モジュールおよび認証子全てを受信し、
前記暗号処理装置通信処理部が、前記受信した分割暗号モジュールおよび認証子を暗号処理装置に送信し、認証子の正当性検証結果を受信し、
前記暗号処理装置通信処理部により受信した認証子の検証結果が全て正当であることを示す情報であるならば、前記暗号モジュール結合部によって結合された暗号モジュールを前記暗号モジュール格納部に格納する
ことを特徴とする請求項１９または請求項２０のうちいずれかに記載の暗号処理装置。
【請求項２３】
暗号処理装置とクライアント装置と通信が可能なコンピュータに、
暗号モジュール格納部に暗号モジュールを格納するステップと、
記憶手段に、前記クライアント装置を識別する端末識別情報に対応付けて、当該クライアント装置に搭載中の暗号モジュールの識別情報と、当該クライアント装置に搭載可能な暗号モジュールの識別情報とが記述された対応表を記憶させるステップと、
選定手段が、前記クライアント装置から端末情報を受信すると、当該受信した端末情報に含まれる端末識別情報に基づいて前記対応表から当該クライアント装置に搭載可能な暗号モジュールの識別情報を読み出し、当該読み出した識別情報に対応する暗号モジュールを前記暗号モジュール格納部から選定するステップと、
鍵共有部に、前記暗号処理装置と共通で利用可能な共有鍵を共有するステップと、
暗号モジュール暗号化部が、当該共有鍵で前記選定された暗号モジュールを暗号化するステップと、
クライアント装置通信処理部が、当該暗号化された暗号モジュールを前記クライアント装置に送信するステップと、
を実行させるための暗号管理プログラム。

【請求項２４】
請求項８に記載の暗号管理サーバ装置と暗号処理装置と通信が可能なコンピュータからなるクライアント装置に、
端末情報格納部に、自装置を識別する端末識別情報を含む端末情報を格納するステップと、
送信手段が、前記端末情報格納部に格納されている端末情報を前記暗号管理サーバ装置に送信するステップと、
サーバ通信処理部が、前記暗号管理サーバ装置から暗号化された暗号モジュールを受信するステップと、
暗号処理装置通信処理部が、前記受信した暗号化された暗号モジュールを前記暗号処理装置に送信し、復号された暗号モジュールを前記暗号処理装置から受信するステップと、
暗号モジュール格納部が、前記暗号処理装置通信処理部により受信した暗号モジュールを格納するステップと、
を実行させるためのクライアントプログラム。
【請求項２５】
請求項８に記載の暗号管理サーバ装置とクライアント装置と通信が可能なコンピュータからなる暗号処理装置に、
鍵共有部が、前記暗号管理サーバ装置と共通で利用可能な共有鍵を共有するステップと、
暗号モジュール復号部が、暗号化された暗号モジュールをクライアント装置より受信し、この受信した暗号化された暗号モジュールを、前記共有鍵を用いて復号するステップと、
クライアント装置通信処理部が、前記復号した暗号モジュールをクライアント装置へ送信するステップと、
を実行させるための暗号処理プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、暗号管理サーバ装置と、クライアント装置と、暗号装置とを備えた暗号モジュール配信システムであって、暗号管理サーバ装置が、クライアントに暗号モジュールを配信する技術に関する。
【背景技術】
【０００２】
従来、サーバとクライアント装置から構成され、サーバとクライアント装置の間で通信を行うシステムにおいて、その通信データについて、盗聴や改ざんなどがされないように安全に送受信する方法が研究されている。また、クライアント装置で動作する暗号アルゴリズムを容易に更新・追加可能な方法が研究されている。
このような方法としては、例えば、暗号文と共に暗号文を復号するために新規暗号アルゴリズムを配信する方法（特許文献１）や、サーバとクライアント装置の間ですでに共有している暗号アルゴリズムを使って秘匿性のある情報（新規暗号アルゴリズム）を更新する方法（特許文献２）などがある。
【特許文献１】特開平１０－４１９３４号公報
【特許文献２】特開２０００－２６１４２７号公報
【発明の開示】
【発明が解決しようとする課題】
【０００３】
しかしながら、上述した特許文献１については、送られた新規暗号アルゴリズムの正当性をクライアント装置で検証することができないという問題がある。
また、上述した特許文献２については、サーバとクライアント装置の間で安全なアルゴリズムを１つ以上共有していることが予め必要であるため、そもそも、安全なアルゴリズ

ムを構築できていないシステムにおいては、秘匿性のある情報を通信することができないという問題がある。

【０００４】

本発明は、このような事情に鑑みてなされたもので、その目的は、サーバとクライアント装置から構成されるシステムにおいて、秘匿性のある情報をセキュリティを確保して通信することができる暗号モジュール配信システムを提供することにある。

【課題を解決するための手段】

【０００５】

上記課題を解決するために、本発明は、互いに通信が可能な、暗号管理サーバ装置（例えば、本実施形態における暗号管理サーバ装置１０１）と、暗号処理装置（例えば、本実施形態における暗号ハードウェア１０３）と、クライアント装置（例えば、本実施形態におけるクライアント装置１０２）とを有する暗号モジュール配信システムにおいて、暗号管理サーバ装置は、暗号モジュールを格納する暗号モジュール格納部（例えば、本実施形態における暗号モジュールＤＢ２０６）と、暗号処理装置と共通で利用可能な共有鍵を共有する鍵共有部（例えば、本実施形態における鍵共有部２０５）と、共有鍵で暗号モジュールを暗号化する暗号モジュール暗号化部（例えば、本実施形態における暗号モジュール暗号化部２０７）と、暗号化された暗号モジュールをクライアント装置に送信するクライアント装置通信処理部（例えば、本実施形態における通信機能２０２）と、を有し、暗号処理装置は、暗号管理サーバと共通で利用可能な共有を共有する鍵共有部（例えば、本実施形態における鍵共有部４０４）と、　暗号化された暗号モジュールをクライアント装置より受信し、この受信した暗号化された暗号モジュールを、前記共有鍵を用いて復号する暗号モジュール復号部（例えば、本実施形態における暗号モジュール復号部４０５）と、前記復号した暗号モジュールをクライアント装置へ送信するクライアント装置通信処理部と（例えば、本実施形態における通信機能４０２）と、クライアント装置より受信した暗号化された暗号モジュールを、鍵格納部に格納された鍵を用いて復号する暗号モジュール復号部と、を有し、クライアント装置は、暗号管理サーバから暗号化された暗号モジュールを受信するサーバ通信処理部（例えば、本実施形態における通信機能３０２）と、受信した暗号化された暗号モジュールを暗号処理装置に送信し、復号された暗号モジュールを暗号処理装置から受信する暗号処理装置通信処理部（例えば、本実施形態における暗号ハードウェア管理制御部３０５）と、暗号処理装置通信処理部により受信した暗号モジュールを格納する暗号モジュール格納部（例えば、本実施形態における暗号モジュールＤＢ３０３）と、を有することを特徴とする暗号モジュール配信システムである。

【０００６】

本発明は、互いに通信が可能な、暗号管理サーバ装置（例えば、本実施形態における暗号管理サーバ装置６０１）と、暗号処理装置（例えば、本実施形態における暗号ハードウェア７０１）と、クライアント装置とを有する暗号モジュール配信システムにおいて、暗号管理サーバ装置は、暗号モジュールを格納する暗号モジュール格納部と、暗号処理装置と共通で利用可能な共有鍵を共有する鍵共有部と、共有鍵で暗号モジュールを識別する認証子を生成する認証子生成部（例えば、本実施形態におけるＭＡＣ生成部６０７）と、暗号モジュールおよび認証子（例えば、本実施形態におけるＭＡＣ）をクライアント装置に送信するクライアント装置通信処理部と、を有し、暗号処理装置は、暗号管理サーバと共通で利用可能な共有鍵を共有する鍵共有部と、クライアント装置より認証子を受信し、当該受信した認証子に対して、前記鍵格納部に格納された共有鍵を用いて認証子の正当性検証を行う認証子検証部（例えば、本実施形態におけるＭＡＣ検証部７０５）と、　前記正当性検証を行った結果をクライアント装置へ送信するクライアント装置通信処理部と、を有し、クライアント装置は、暗号管理サーバより暗号モジュールおよび認証子を受信するサーバ通信処理部と、サーバ通信処理部によって受信した認証子を暗号処理装置に送信し、認証子の正当性検証結果を受信する暗号処理装置通信処理部と、暗号処理装置通信処理部により受信した認証子の正当性検証結果が正当であることを示す情報であるならば、前記受信した暗号モジュールを格納する暗号モジュール格納部と、を有することを特徴とす

る暗号モジュール配信システムである。

【０００７】

本発明は、上述に記載の暗号モジュール配信システムであって、暗号管理サーバ装置は、共有鍵で暗号モジュールを暗号化する暗号モジュール暗号化部を有し、クライアント装置通信処理部が、暗号モジュール暗号化部によって暗号化された暗号モジュールおよび認証子生成部によって生成された認証子をクライアント装置に送信し、暗号処理装置は、クライアント装置通信処理部が、暗号化された暗号モジュールおよび認証子をクライアント装置より受信し、共有鍵を用いて暗号化された暗号モジュールを復号した暗号モジュールと認証子の正当性検証を行った結果とをクライアント装置へ送信し、クライアント装置は、暗号処理装置通信処理部が、サーバ通信処理部によって受信する暗号化された暗号モジュールおよび認証子を暗号処理装置に送信し、復号された暗号モジュールおよび認証子の正当性検証結果を受信し、暗号処理装置通信処理部により受信した認証子の正当性検証結果が正当であることを示す情報であるならば、復号された暗号モジュールを暗号モジュール格納部に格納することを特徴とする暗号モジュール配信システムである。

【０００８】

本発明は、上述に記載の暗号モジュール配信システムであって、暗号管理サーバ装置は、暗号モジュールを暗号処理装置が処理可能なデータサイズに分割して分割暗号モジュールを生成する暗号モジュール分割部（例えば、本実施形態における暗号モジュール分割部１２０７）とを有し、暗号モジュール暗号化部が、共有鍵で分割暗号モジュール毎に暗号化し、クライアント装置通信処理部が、暗号化された分割暗号モジュール全てをクライアント装置に送信し、暗号処理装置は、クライアント装置通信処理部が、暗号化された分割暗号モジュールをクライアント装置より受信し、共有鍵を用いて復号した分割暗号モジュールをクライアント装置へ送信し、暗号モジュール復号部が、クライアント装置より受信した暗号化された分割暗号モジュールを、共有鍵を用いて復号し、クライアント装置は、暗号処理装置通信処理部より受信した分割暗号モジュール全てを結合して暗号モジュールを復元する暗号モジュール結合部（例えば、本実施形態における暗号モジュール結合部１３０７）を有し、サーバ通信処理部が、暗号管理サーバより暗号化された分割暗号モジュール全てを受信し、暗号処理装置通信処理部が、受信した暗号化された分割暗号モジュールを暗号処理装置に送信し、復号された分割暗号モジュールを受信し、暗号モジュール結合部が、暗号モジュール結合部によって結合された暗号モジュールを暗号モジュール格納部に格納することを特徴とする暗号モジュール配信システムである。

【０００９】

本発明は、上述に記載の暗号モジュール配信システムであって、暗号管理サーバ装置は、暗号モジュールを暗号処理装置が処理可能なデータサイズに分割して分割暗号モジュールを生成する暗号モジュール分割部とを有し、記認証子生成部が、共有鍵で分割暗号モジュール毎に認証子を生成し、クライアント装置通信処理部が、分割暗号モジュールと認証子全てをクライアント装置に送信し、暗号処理装置は、クライアント装置通信処理部が、クライアント装置より分割暗号モジュールおよび認証子を受信し、共有鍵を用いて認証子の正当性検証を行った結果をクライアント装置へ送信し、認証子検証部が、クライアント装置より受信した分割暗号モジュールおよび認証子に対して、共有鍵を用いて認証子の正当性検証を行い、クライアント装置は、受信した分割暗号モジュール全てを結合して暗号モジュールを復元する暗号モジュール結合部を有し、記サーバ通信処理部が、暗号管理サーバより分割暗号モジュールおよび認証子全てを受信し、暗号処理装置通信処理部が、受信した分割暗号モジュールおよび認証子を暗号処理装置に送信し、認証子の正当性検証結果を受信し、暗号処理装置通信処理部により受信した認証子の検証結果が全て正当であることを示す情報であるならば、暗号モジュール結合部によって結合された暗号モジュールを暗号モジュール格納部に格納することを特徴とする暗号モジュール配信システムである。

【００１０】

本発明は、上述に記載の暗号モジュール配信システムであって、暗号化された分割暗号

モジュールは、少なくとも２つ以上の異なる鍵のいずれかによってそれぞれ暗号化されていることを特徴とする暗号モジュール配信システムである。

【００１１】

本発明は、上述に記載の暗号モジュール配信システムであって、認証子は、少なくとも２つ以上の異なる鍵のいずれかによってそれぞれ生成されていることを特徴とする暗号モジュール配信システムである。

【００１２】

本発明は、暗号処理装置とクライアント装置と通信し、当該クライアント装置に暗号モジュールを配信する暗号管理サーバ装置であって、暗号モジュールを格納する暗号モジュール格納部と、暗号処理装置と共通で利用可能な共有鍵を共有する鍵共有部と、当該共有鍵で暗号モジュールを暗号化する暗号モジュール暗号化部と、当該暗号化された暗号モジュールをクライアント装置に送信するクライアント装置通信処理部と、を備えることを特徴とする暗号管理サーバ装置である。

【００１３】

本発明は、暗号処理装置とクライアント装置と通信し、当該クライアント装置に暗号モジュールを配信する暗号管理サーバ装置であって、暗号モジュールを格納する暗号モジュール格納部と、暗号処理装置と共通で利用可能な共有鍵を共有する鍵共有部と、当該共有鍵で暗号モジュールを識別する認証子を生成する認証子生成部と、暗号モジュールおよび認証子をクライアント装置に送信するクライアント装置通信処理部と、を備えることを特徴とする暗号管理サーバ装置である。

【００１４】

本発明は、共有鍵で暗号モジュールを暗号化する暗号モジュール暗号化部と、をさらに有し、クライアント装置通信処理部は、当該暗号化された暗号モジュールをクライアント装置に送信することをさらに特徴とする暗号管理サーバ装置である。

【００１５】

本発明は、暗号モジュールを暗号処理装置が処理可能なデータサイズに分割して分割暗号モジュールを生成する暗号モジュール分割部をさらに有し、暗号モジュール暗号化部が、共有鍵で分割暗号モジュール毎に暗号化し、クライアント装置通信処理部が、暗号化された分割暗号モジュール全てをクライアント装置に送信することを特徴とする暗号管理サーバ装置である。

【００１６】

本発明は、暗号モジュールを暗号処理装置が処理可能なデータサイズに分割して分割暗号モジュールを生成する暗号モジュール分割部とを有し、認証子生成部が、共有鍵で分割暗号モジュール毎に認証子を生成し、クライアント装置通信処理部が、分割暗号モジュールと認証子全てをクライアント装置に送信することを特徴とする暗号管理サーバ装置である。

【００１７】

本発明は、暗号管理サーバ装置と暗号処理装置と通信し、暗号管理サーバ装置より暗号モジュールを配信されるクライアント装置であって、暗号管理サーバから暗号化された暗号モジュールを受信するサーバ通信処理部と、受信した暗号化された暗号モジュールを暗号処理装置に送信し、復号された暗号モジュールを暗号処理装置から受信する暗号処理装置通信処理部と、暗号処理装置通信処理部により受信した暗号モジュールを格納する暗号モジュール格納部と、を有することを特徴とするクライアント装置である。

【００１８】

本発明は、暗号管理サーバ装置と暗号処理装置と通信し、暗号管理サーバ装置より暗号モジュールを配信されるクライアント装置であって、暗号管理サーバより暗号モジュールおよび認証子を受信するサーバ通信処理部と、サーバ通信処理部によって受信した認証子を暗号処理装置に送信し、当該認証子の正当性検証結果を受信する暗号処理装置通信処理部と、暗号処理装置通信処理部により受信した認証子の正当性検証結果が正当であることを示す情報であるならば、受信した暗号モジュールを格納する暗号モジュール格納部と、

を有することを特徴とするクライアント装置である。

【００１９】

本発明は、暗号処理装置通信処理部が、サーバ通信処理部によって受信する暗号化された暗号モジュールおよび認証子を暗号処理装置に送信し、復号された暗号モジュールおよび認証子の正当性検証結果を受信し、暗号処理装置通信処理部により受信した認証子の正当性検証結果が正当であることを示す情報であるならば、復号された暗号モジュールを暗号モジュール格納部に格納することを特徴とするクライアント装置である。

【００２０】

本発明は、暗号処理装置通信処理部より受信した分割暗号モジュール全てを結合して暗号モジュールを復元する暗号モジュール結合部を有し、サーバ通信処理部が、暗号管理サーバより暗号化された分割暗号モジュール全てを受信し、暗号処理装置通信処理部が、受信した暗号化された分割暗号モジュールを暗号処理装置に送信し、復号された分割暗号モジュールを受信し、暗号モジュール結合部が、暗号モジュール結合部によって結合された暗号モジュールを暗号モジュール格納部に格納することを特徴とするクライアント装置である。

【００２１】

本発明は、受信した分割暗号モジュール全てを結合して暗号モジュールを復元する暗号モジュール結合部を有し、サーバ通信処理部が、暗号管理サーバより分割暗号モジュールおよび認証子全てを受信し、暗号処理装置通信処理部が、受信した分割暗号モジュールおよび認証子を暗号処理装置に送信し、認証子の正当性検証結果を受信し、暗号処理装置通信処理部により受信した認証子の検証結果が全て正当であることを示す情報であるならば、暗号モジュール結合部によって結合された暗号モジュールを暗号モジュール格納部に格納することを特徴とするクライアント装置である。

【００２２】

本発明は、暗号管理サーバ装置とクライアント装置と通信し、暗号管理サーバからクライアント装置に暗号モジュールを配信するときの暗号処理を行う暗号処理装置であって、暗号管理サーバと共通で利用可能な共有鍵を共有する鍵共有部と、暗号化された暗号モジュールをクライアント装置より受信し、この受信した暗号化された暗号モジュールを、共有鍵を用いて復号する暗号モジュール復号部と、復号した暗号モジュールをクライアント装置へ送信するクライアント装置通信処理部と、を有することを特徴とする暗号処理装置である。

【００２３】

本発明は、暗号管理サーバ装置とクライアント装置と通信し、暗号管理サーバからクライアント装置に暗号モジュールを配信するときの暗号処理を行う暗号処理装置であって、暗号管理サーバより暗号モジュールおよび認証子を受信するサーバ通信処理部と、サーバ通信処理部によって受信した認証子を暗号処理装置に送信し、当該認証子の正当性検証結果を受信する暗号処理装置通信処理部と、暗号処理装置通信処理部により受信した認証子の正当性検証結果が正当であることを示す情報であるならば、受信した暗号モジュールを格納する暗号モジュール格納部と、を有することを特徴とする暗号処理装置である。

【００２４】

本発明は、暗号処理装置通信処理部が、サーバ通信処理部によって受信する暗号化された暗号モジュールおよび認証子を暗号処理装置に送信し、復号された暗号モジュールおよび認証子の正当性検証結果を受信し、暗号処理装置通信処理部により受信した認証子の正当性検証結果が正当であることを示す情報であるならば、復号された暗号モジュールを暗号モジュール格納部に格納することを特徴とする暗号処理装置である。

【００２５】

本発明は、暗号処理装置通信処理部より受信した分割暗号モジュール全てを結合して暗号モジュールを復元する暗号モジュール結合部を有し、サーバ通信処理部が、暗号管理サーバより暗号化された分割暗号モジュール全てを受信し、暗号処理装置通信処理部が、受信した暗号化された分割暗号モジュールを暗号処理装置に送信し、復号された分割暗号モ

ジュールを受信し、暗号モジュール結合部が、暗号モジュール結合部によって結合された暗号モジュールを暗号モジュール格納部に格納することを特徴とする暗号処理装置である。

【００２６】

本発明は、受信した分割暗号モジュール全てを結合して暗号モジュールを復元する暗号モジュール結合部を有し、サーバ通信処理部が、暗号管理サーバより分割暗号モジュールおよび認証子全てを受信し、暗号処理装置通信処理部が、受信した分割暗号モジュールおよび認証子を暗号処理装置に送信し、認証子の正当性検証結果を受信し、暗号処理装置通信処理部により受信した認証子の検証結果が全て正当であることを示す情報であるならば、暗号モジュール結合部によって結合された暗号モジュールを暗号モジュール格納部に格納することを特徴とする暗号処理装置である。

【００２７】

本発明は、暗号処理装置とクライアント装置と通信が可能なコンピュータに、暗号モジュール格納部に暗号モジュールを格納するステップと、鍵共有部に、暗号処理装置と共通で利用可能な共有鍵を共有するステップと、暗号モジュール暗号化部が、当該共有鍵で暗号モジュールを暗号化するステップと、クライアント装置通信処理部が、当該暗号化された暗号モジュールをクライアント装置に送信するステップと、を実行させるための暗号管理プログラムである。

【００２８】

本発明は、暗号管理サーバ装置と暗号処理装置と通信が可能なコンピュータに、サーバ通信処理部が、暗号管理サーバから暗号化された暗号モジュールを受信するステップと、暗号処理装置通信処理部が、受信した暗号化された暗号モジュールを暗号処理装置に送信し、復号された暗号モジュールを暗号処理装置から受信するステップと、暗号モジュール格納部が、暗号処理装置通信処理部により受信した暗号モジュールを格納するステップと、を実行させるためのクライアントプログラムである。

【００２９】

本発明は、暗号管理サーバ装置とクライアント装置と通信が可能なコンピュータに、鍵共有部が、暗号管理サーバと共通で利用可能な共有鍵を共有するステップと、暗号モジュール復号部が、暗号化された暗号モジュールをクライアント装置より受信し、この受信した暗号化された暗号モジュールを、共有鍵を用いて復号するステップと、クライアント装置通信処理部が、復号した暗号モジュールをクライアント装置へ送信するステップと、を実行させるための暗号処理プログラムである。

【発明の効果】

【００３０】

以上説明したように、本発明によれば、クライアント装置側で暗号アルゴリズム(プログラム)をまったく保持していない場合であっても、暗号処理を行う暗号処理装置を補助的に使ってクライアント装置に暗号アルゴリズムを送信することで、クライアント装置で新規暗号アルゴリズムを利用可能な状態にすることができる。

【発明を実施するための最良の形態】

【００３１】

以下、本発明の一実施形態による暗号モジュール配信システムについて図面を参照して説明する。

まず、本システムの概要について説明する。本システムにおいては、サーバとクライアント装置とが接続され、サーバとクライアント装置間において暗号モジュールを用いて暗号化された情報を送受信することが可能なシステムである。ここで、暗号モジュールを定期的に切り替えることも可能である。このような、暗号モジュールを切り替え可能な暗号システムとしては、暗号の手法ごとに暗号方式に依存しないインターフェースを規定し、各暗号ベンダが実装可能なフレームワークがいくつか存在する。例えば、Ｍｉｃｒｏｓｏｆｔ（登録商標）のＣｒｙｐｔＡＰＩやＳｕｎ（登録商標）のＪＣＡ（Java（登録商標） Cryptographic Architecture)／ＪＣＥ（Java（登録商標） Cryptographic Extensions

）やＯｐｅｎ　Ｇｒｏｕｐ（登録商標）のＣＤＳＡ（Common Data Security Architecture）などがある。

【００３２】

これらのフレームワークでは、暗号化／復号、署名生成／検証、認証子生成／検証などの暗号の手法ごとに暗号モジュールにアクセスするインターフェースを規定し、インターフェースに従って、例えば、ＤＥＳ（Data Encryption Standard）、ＡＥＳ（Advanced Encryption Standard）などの暗号方式を実装することが可能になっている。そして、暗号やセキュリティの専門家がシステム構築時に、これらの実装された暗号の中から適切な暗号方式をあらかじめ選択し、いずれの暗号方式を利用するかを示す暗号方式パラメータをフレームワークに入力して、暗号方式を切り替えることが可能である。

【００３３】

このようなフレームワークを利用する場合、アプリケーションシステムの運用上のセキュリティポリシが変更された場合、従来であれば暗号やセキュリティの専門家が、再度システムに適した暗号方式を選定する必要があり、暗号やセキュリティの専門家の人材リソースの問題やコストの問題に直面する。また、既存の暗号方式の不備が発見されたり、新しい暗号が発表されたりした際に、運用中のシステムに対して、暗号方式の変更をスムーズに適用するのが難しい。さらには、セキュリティを実施する環境に応じて、必要なセキュリティ強度や処理速度などが違う場合に、最適なセキュリティを実現することも、従来システムでは難しい問題である。

本システムにおいては、暗号方式の切り替えが可能な暗号システムでは、この問題についても解決することが可能である。

【００３４】

＜第１の実施形態＞

図１は、本発明の第１の実施形態による暗号モジュール配信システムの構成を示す概略ブロック図である。

本暗号システムは、暗号モジュール３０８と暗号評価記述ファイル３０９とを含む暗号パッケージ３０７を送信する暗号管理サーバ装置３５０と、受信した暗号パッケージ３０７を用いて暗号処理を行う暗号クライアント装置１５０とから構成される。暗号評価記述ファイル３０９に記述される暗号の評価とは、対応する暗号モジュール３０８の暗号方式の信頼度や強度等が数値化された情報であり、例えば、実装している暗号方式の安全性や暗号の処理速度、暗号に利用可能な鍵長などである。

【００３５】

暗号管理サーバ装置３５０は、暗号モジュール３０８を蓄積した暗号モジュールＤＢ３５３と、暗号評価記述ファイル３０９を蓄積した暗号評価ＤＢ３５４と、暗号モジュールＤＢ３５３と暗号評価ＤＢ３５４との管理を行う暗号管理部３５１と、暗号モジュールＤＢ３５３と暗号評価ＤＢ３５４とに新規の情報を登録する暗号登録部３５５と、暗号クライアント装置１５０の要求に応じて最適な暗号パッケージ３０７を暗号モジュールＤＢ３５３と暗号評価ＤＢ３５４とから読み出して送信する暗号配信部３５２とを備える。

【００３６】

暗号クライアント装置１５０は、暗号制御マネージャ部１５２を介して暗号実装部１５３が提供する暗号機能を呼び出して利用するアプリケーションやミドルウェアである上位システム部１５１と、暗号管理サーバ装置３５０から送信された暗号パッケージ３０７の受信や暗号実装部１５３から提供される暗号機能の切り替えを行う暗号制御マネージャ部１５２と、主要な暗号方式による暗号処理をハードウェアとして実現した耐タンパーな暗号ハードウェア部４５０と、暗号方式を実装した暗号モジュール３０８が実行可能・利用可能な状態にされて暗号機能を提供する暗号実装部１５３とから構成される。暗号管理サーバ装置３５０は、暗号クライアント装置１５０からの要求に基づき、暗号の初期登録・配信・更新の３つの手順を行うことで、適切な暗号パッケージ３０７を暗号クライアント装置１５０に送信する。

【００３７】

ここで、暗号の初期登録とは、暗号クライアント装置１５０が暗号モジュール３０８を有せず、暗号実装部１５３が存在しない場合に、暗号クライアント装置１５０の暗号ハードウェア部４５０を利用して、利用上必要不可欠な暗号モジュール３０８を暗号管理サーバ装置３５０から暗号実装部１５３に安全に送信することである。

暗号の配信とは、暗号管理サーバ装置３５０が、暗号クライアント装置１５０から受信した暗号要求に応じて、適切な暗号モジュール３０８または暗号パッケージ３０７を選定して暗号クライアント装置１５０に送信することである。暗号要求は暗号に関する条件情報を含み、条件情報は、暗号化や署名生成などの暗号方式の分類（暗号のカテゴリ）、暗号モジュール３０８を作成したメーカ、暗号モジュール３０８が動作するハードウェアの情報、および、暗号の評価情報などがある。暗号の評価情報は、本実施形態例のように、暗号評価記述ファイル３０９として、暗号モジュール３０８とは独立したファイルとして扱われることとしても良い。

【００３８】

暗号の更新とは、新規の暗号モジュール３０８を登録したり、危殆化した暗号方式を利用した該当する暗号モジュール３０８を削除したり、暗号モジュール３０８のバグを発見し既存の暗号モジュール３０８とその暗号モジュール３０８が実行されている暗号実装部１５３を更新したり、計算機の処理速度の高速化等に伴って暗号の評価を変更したりした際に、暗号管理サーバ装置３５０上の暗号モジュールＤＢ３５３や暗号評価ＤＢ３５４に」記憶された情報を更新し、この更新した暗号パッケージ３０７の情報を、暗号クライアント装置１５０に対して定期的に送信したり、暗号クライアント装置１５０からの要求に基づいて送信したりして、暗号管理サーバ装置３５０が新しい暗号モジュール３０８を送信することや既存の暗号実装部が使えなくなったことを通知することである。

【００３９】

図２は、暗号クライアント装置１５０の詳細な構成図である。暗号制御マネージャ部１５２は、暗号処理情報ＤＢ１５７を持つ暗号処理制御部１５６と、暗号モジュールＤＢ１６４と、暗号評価ＤＢ１６３と、暗号モジュール選定ポリシ１５８とハードウェアプロファイル１６０とを持つ暗号モジュール選定部１５９と、鍵情報ＤＢ１６５と、その鍵情報ＤＢ１６５へのアクセス制御ポリシが記述されたアクセス制御ポリシ１６１を持つ鍵情報管理部１６２と、暗号制御マネージャポリシ１６７を持つ暗号管理部１６６と、暗号ハードウェア部４５０と通信を行う暗号ハードウェア管理制御部１７０と、外部との通信を行う通信機能１５５と、通信機能１５５と連携するアルゴリズムネゴシエーション部１６８と、通信機能１５５と連携するセキュア通信管理部１６９とから構成される。

【００４０】

暗号処理制御部１５６は、上位システム部１５１からの暗号処理呼び出しに基づき、鍵生成処理、鍵登録処理、暗号処理を行う。

鍵生成処理の場合、暗号処理制御部１５６は、上位システム部１５１から指定された暗号方式、鍵長、暗号方式パラメータを暗号処理情報ＤＢ１５７に登録した際の暗号処理の識別子により、指定された暗号方式に対する暗号モジュール３０８を暗号モジュール選定部１５９により選定する。

【００４１】

暗号処理制御部１５６が、選定された暗号モジュール３０８をメモリ上にロードし暗号実装部１５３として実行状態にさせる。暗号処理制御部１５６が、指定された暗号処理の識別子に対応する鍵生成のための暗号方式パラメータを鍵情報管理部１６２経由で鍵情報ＤＢ１６５から引き出す。暗号処理制御部１５６が、指定された鍵長と引き出した暗号方式パラメータで暗号実装部１５３を呼び出すと、暗号実装部１５３は鍵情報を生成する。暗号処理制御部１５６は、生成された鍵情報を受け取る。暗号処理制御部１５６は、暗号実装部１５３が生成した鍵情報を鍵情報管理部１６２経由で鍵情報ＤＢ１６５に登録してその鍵情報に対応する鍵識別子を受け取り、処理結果として新しく発行した暗号処理の識別子と鍵識別子の関連付けを暗号処理情報ＤＢ１５７に保存し、暗号処理の識別子を上位システム部１５１に返す。

【００４２】
鍵登録の場合、暗号処理制御部１５６は、上位システム部１５１から指定された鍵情報を、鍵情報管理部１６２を経由して鍵情報ＤＢ１６５に登録して鍵識別子を受け取り、処理結果として新しく発行した暗号処理の識別子と鍵識別子の関連付けを暗号処理情報ＤＢ１５７に保存し、暗号処理の識別子を上位システム部１５１に返す。
【００４３】
暗号処理の場合、上位システム部１５１から指定された暗号に関する条件情報と暗号処理対象データ（平文）と鍵生成または鍵登録を行った際に受け取った暗号処理の識別子とを受け取り、暗号に関する条件情報を参照して適切な暗号モジュール３０８を暗号モジュール選定部１５９により選定し、選定された暗号モジュール３０８をメモリ上にロードして暗号実装部１５３として実行させ、指定された暗号処理の識別子に対応する鍵情報を鍵情報管理部１６２経由で鍵情報ＤＢ１６５から引き出し、指定された暗号処理対象データと引き出した鍵情報とを、呼び出した暗号実装部１５３に入力し、対応して処理された暗号データを受け取り、処理結果として新しく発行した暗号処理の識別子と鍵識別子の関連付けを暗号処理情報ＤＢ１５７に保存し、暗号処理の識別子を返す。暗号処理の際に利用した鍵情報などを暗号処理の識別子に結びつけることにより、暗号処理の再実行や復号を簡単に実施することができるようにする。
【００４４】
暗号モジュールＤＢ１６４は、暗号管理サーバ装置３５０から受信した暗号モジュール３０８を格納する記憶部である。
暗号評価ＤＢ３５４は、暗号管理サーバ装置３５０から受信した暗号評価記述ファイル３０９を格納する記憶部である。
暗号モジュール選定部１５９は、暗号化や署名生成などの暗号のカテゴリ、暗号モジュール３０８を作成したメーカ、暗号モジュール３０８が動作するハードウェアの情報、および、暗号の評価情報などの暗号に関する条件情報を、上位システム部１５１からの入力を元に、暗号モジュールＤＢ１６４が記憶している暗号モジュール３０８の中から一番適切な暗号モジュール３０８を選定する。暗号モジュール３０８の選定にあたっては、暗号クライアント装置１５０のハードウェア情報を記述したハードウェアプロファイル１６０に適合するものの中から選び、かつ、暗号クライアント装置１５０を利用する利用者のポリシを記述した暗号モジュール選定ポリシ１５８にも従うようにする。
【００４５】
ハードウェアプロファイル１６０とは、例えば、暗号クライアント装置１５０のＣＰＵアーキテクチャ、ＣＰＵクロック、搭載メモリ量などの情報を含む情報である。暗号モジュール選定ポリシ１５８とは、例えば、入力条件により選定された暗号が複数ある場合に利用者が優先したい条件、利用者が優先的に利用したい暗号のメーカ、利用者が利用禁止にしたい暗号方式などを含む情報である。
【００４６】
このように、暗号モジュール選定部１５９は、上位システム部１５１からの入力情報と、ハードウェアプロファイル１６０と、暗号モジュール選定ポリシ１５８とを参照して、入力情報に一致する暗号モジュール３０８を選定する。暗号モジュール選定部１５９が暗号モジュール３０８を一意に選定した場合には、選定した暗号モジュール３０８を暗号モジュールＤＢ１６４から取り出す。暗号モジュール選定部１５９は、暗号モジュール３０８が一意に選定できなかった場合は、エラーを出力する。
【００４７】
鍵情報管理部１６２は、暗号実装部１５３を呼び出す際に指定される鍵情報や暗号方式パラメータなどの情報を鍵情報ＤＢ１６５へデータを記憶させ、または読み出す。鍵情報管理部１６２は、指定される鍵情報や暗号方式パラメータの情報がひとつではない場合、複数の情報をひとつにまとめて引き出せるように関連付けを行って、鍵情報ＤＢ１６５に登録する。また、鍵情報管理部１６２は、鍵情報ＤＢ１６５から鍵情報や暗号方式パラメータを引き出す際には、暗号モジュール選定ポリシ１５８に従い、複数ある上位システム

部１５１からの鍵情報へのアクセス制御を行う。

【００４８】

鍵情報管理部１６２は、上位システム部１５１から指定されたクレデンシャル（アクセスのための鍵やパスワードなど）とアクセスしたい鍵識別子と鍵識別子に関連付けられた暗号処理の識別子とにより、そのクレデンシャルの正当性を検証する。鍵情報管理部１６２は、クレデンシャルの持ち主に対してアクセス可能な鍵情報ＤＢ１６５の鍵情報の規定を記述したアクセス制御ポリシ１６１に基づき、アクセス可否を判定し、アクセス可ならば、暗号処理の識別子に対応する鍵識別子を鍵情報ＤＢ１６５から引き出し、鍵識別子に対応する鍵情報や暗号方式パラメータを引き出し、上位システム部１５１にこれを返す。一方、アクセス不可ならば、上位システム部１５１にエラーを返す。

【００４９】

暗号管理部１６６では、通信機能１５５を介して暗号管理サーバ装置３５０と通信を行い、暗号の初期登録・配信・更新の手順に従って、暗号パッケージ３０７等の受信を行う。暗号管理部１６６が暗号管理サーバ装置３５０から暗号パッケージ３０７等を受信する際には、暗号制御マネージャポリシ１６７の内容に従って処理する。暗号制御マネージャポリシ１６７の内容は、例えば、以下の５つである。１つめは、暗号管理サーバ装置３５０との通信におけるサーバ認証の実施可否である。２つめは、暗号管理サーバ装置３５０からの暗号パッケージ３０７等の受信時の暗号化可否である。３つめは、暗号管理サーバ装置３５０からの暗号パッケージ３０７等の受信時の改ざん検出子（ＭＡＣ（Message Authentication Code））付加可否である。４つめは、受信した暗号パッケージ３０７等の認証子の検証実施可否である。５つめは、暗号評価ＤＢ１６３と暗号モジュールＤＢ１６４とに記憶された暗号パッケージ３０７を定期的に更新可否や更新頻度などを示す定期更新に関する設定情報、などとする。

【００５０】

暗号ハードウェア管理制御部１７０は、暗号ハードウェア部４５０と通信を行い、暗号管理サーバ装置３５０から、暗号の初期登録の手順に従って暗号パッケージ３０７の受信を行う。暗号パッケージ３０７の受信の際には、暗号パッケージ３０７自身が暗号化されている場合、暗号ハードウェア部４５０にて暗号パッケージ３０７を復号する。また、暗号モジュール３０８に改ざん検出子が付加されていることを検出すると、暗号ハードウェア部４５０が暗号モジュール３０８の改ざん検出を行う。

【００５１】

アルゴリズムネゴシエーション部１６８は、通信機能１５５と連携し、２つの暗号クライアント装置間で安全な通信セッションを構築する事前に、通信セッションの構築で利用する暗号方式、通信セッションで利用する暗号方式の調停を行う。暗号方式の調停を行う際には、以下の４つの調停方法のいずれかで調停を行えるようにする。

【００５２】

第１の調停方法は、自身の暗号モジュールＤＢ１６４に記憶された暗号モジュール３０８が提供する暗号方式群のみからアルゴリズムネゴシエーション部１６８が一方的に暗号方式を決定する。自身のアルゴリズムネゴシエーション部１６８は、上位システム部１５１から指定された１つ以上の暗号方式の分類（暗号のカテゴリ）、暗号制御マネージャポリシ、ハードウェアプロファイル、暗号に関する条件情報から、暗号評価ＤＢ１６３と暗号モジュールＤＢ１６４とを参照して適切な暗号モジュール３０８を選定し、暗号方式を決定する。暗号方式の分類が複数指定された場合は、個々の暗号方式の分類ごとに選定を行い、暗号方式を決定する。

【００５３】

このとき、アルゴリズムネゴシエーション部１６８は、上位システム部１５１から暗号方式が未決定である暗号方式の分類が指定された場合は、指定された暗号に関する条件情報を参照して暗号の配信の手順を行い暗号管理サーバ装置３５０から暗号モジュール３０８を受信し、その暗号モジュール３０８の暗号方式を結果とする。それでも未決定の場合は、アルゴリズムネゴシエーション部１６８は、上位システム部１５１にエラーを返す。

【００５４】
アルゴリズムネゴシエーション部１６８が暗号方式を決定すると、上位システム部１５１から指定された相手方の暗号制御マネージャ部１５２の宛先に対して、暗号方式調停方法番号と、結果として出力された暗号方式の分類と暗号方式の対応群と、暗号モジュール３０８が足りない場合の暗号管理サーバ装置３５０からの受信可否に関する情報を送信する。受信した相手方の暗号制御マネージャ部１５２は、指定された暗号方式の暗号モジュール３０８を所持しているかを暗号評価ＤＢ１６３および暗号モジュールＤＢ１６４から検索し、すべての暗号方式に対して適切な暗号モジュール３０８が存在する場合には通信可能である返信を行う。
【００５５】
相手方の暗号制御マネージャ部１５２は、存在しない暗号モジュール３０８があった場合、暗号管理サーバ装置３５０からの受信可否に関する情報に従って処理する。すなわち、受信可の場合は、暗号の配信の手順に従って、暗号方式に対する暗号モジュール３０８を受信し、受信完了後、通信可能である返信を行う。受信不可の場合や、受信可の場合でも適切な暗号モジュール３０８が受信できなかった場合、通信不可能である返信を行う。自身の暗号制御マネージャ部１５２は、相手方の暗号制御マネージャ部１５２からの返信を上位システム部１５１に転送する。
【００５６】
第２の調停方法は、相手方の暗号制御マネージャ部１５２が保持する暗号方式群のみから相手の暗号制御マネージャ部１５２が一方的に暗号方式を決定する。これは上記第１の調停方法と対称の処理となり同様の手順である。
【００５７】
第３の調停方法は、双方の暗号制御マネージャ部１５２が保持する暗号方式群から自身の暗号制御マネージャ部１５２が共通の暗号方式を決定する。
自身の暗号制御マネージャ部１５２のアルゴリズムネゴシエーション部１６８は、上位システム部１５１から指定された１つ以上の暗号方式の分類（暗号のカテゴリ）、相手方の暗号制御マネージャ部１５２の宛先から、相手方の暗号制御マネージャ部１５２に対して暗号方式調停方法番号、暗号方式の分類を送信する。相手方の暗号制御マネージャ部１５２は、受信した暗号方式の分類、ハードウェアプロファイルから、暗号評価ＤＢ１６３および暗号モジュールＤＢ１６４を参照して該当するすべての暗号モジュール３０８を選び、選んだすべての暗号モジュール３０８が対応する暗号方式一覧を作成する。
【００５８】
この際、相手方の暗号制御マネージャ部１５２は、暗号方式の分類が複数指定された場合は、個々の暗号方式の分類ごとに暗号モジュール３０８を選び、暗号方式一覧を作成する。相手方の暗号制御マネージャ部１５２は、暗号方式の分類ごとの暗号方式一覧を自身の暗号制御マネージャ部１５２に送信する。暗号方式の分類ごとの暗号方式一覧を受信した自身の暗号制御マネージャ部１５２は、上位システム部１５１から指定された１つ以上の暗号方式の分類（暗号のカテゴリ）、暗号制御マネージャポリシ、ハードウェアプロファイル、暗号に関する条件情報から、暗号評価ＤＢ１６３および暗号モジュールＤＢ１６４を参照して適切な暗号モジュール３０８を選定し、選定した暗号モジュール３０８から暗号方式を決定する。
【００５９】
この際、暗号制御マネージャ部１５２は、暗号方式の分類が複数指定された場合は、個々の暗号方式の分類ごとに選定を行い、暗号方式を決定する。例えば、次の場合、暗号方式の分類に対する暗号方式は決定されたとする。まず、自身の暗号制御マネージャ部１５２で選定した暗号方式が暗号方式一覧に存在する場合。次に、自身の暗号制御マネージャ部１５２が受信した暗号方式一覧のいずれかの暗号方式に対応する暗号モジュール３０８を所持している場合。それ以外の場合、暗号方式の分類に対する暗号方式は未決定とする。
【００６０】

暗号制御マネージャ部１５２は、未決定の暗号方式の分類がある場合、受信した暗号方式一覧のいずれかを指定して、暗号の配信の手順に従い、暗号管理サーバ装置３５０から暗号モジュール３０８を受信する。暗号制御マネージャ部１５２は、対応する暗号モジュール３０８を受信できるまで暗号方式一覧のすべての暗号方式について同様の処理を繰り返す。それでも未決定の場合、該当の暗号方式の分類に関する暗号方式は未決定とする。すべての暗号方式の分類に対して、上記の処理が完了したら、相手方の暗号制御マネージャ部１５２に対して、すべての暗号方式の分類に対する暗号方式の決定／未決定を送信する。

【００６１】

第４の調停方法は、双方の暗号制御マネージャ部の保持する暗号方式群から相手方の暗号制御マネージャ部１５２に共通の暗号方式を決定する。これは第３の調停方法の場合と対称の処理となり同様の手順である。

アルゴリズムネゴシエーション部１６８は、以上の４つの調停方法のいずれかで調停を行う。

【００６２】

セキュア通信管理部１６９は、通信機能１５５と連携し、他の暗号クライアント装置１５０との間で安全な通信セッションを構築する。セキュア通信管理部１６９は、安全なセッションを構築する際には、アルゴリズムネゴシエーション部１６８により、通信セッション構築で利用するための暗号方式と通信セッションで利用するための暗号方式を決定した後に、セッション鍵共有を行う。安全な通信セッションの構築後は、決定した暗号方式に従い、セッション鍵を利用して、通信データの暗号化や通信データの改ざん防止のための認証子の付加を行うことができるようにする。また、セキュア通信管理部１６９は、一度、構築した通信セッションは、一定時間内は再利用できるように、通信セッションの保持を行うことができるようにする。

【００６３】

セキュア通信管理部１６９は、上位システム部１５１から指定された通信相手の宛先にセキュア接続要求を送信し、セキュア接続の開始を通知する。次に、セキュア通信管理部１６９は、事前にアルゴリズムネゴシエーション部１６８が決定した暗号方式の分類に従ってセキュア接続を確立する。暗号方式の分類には、例えば、認証、鍵共有、共通鍵情報暗号化（ストリーム暗号あるいはブロック暗号）、公開鍵暗号、データ認証（ＭＡＣ認証または署名認証）、擬似乱数生成（ストリーム暗号および公開鍵暗号の場合のみ）、セッション鍵導出、ＭＡＣ鍵導出（ＭＡＣ認証の場合のみ）、などの分類がある。セキュア通信管理部１６９は、セキュア接続に認証が必要な場合、認証処理を行う。

【００６４】

次に、セキュア通信管理部１６９は、鍵共有処理により鍵の共有を行い、セキュアセッションを確立する。ただし、公開鍵暗号の暗号方式が調停されている場合、鍵共有処理は行わない。公開鍵暗号なしで暗号化通信を行う場合には、共有した鍵からセッション鍵導出方式により、セッション鍵を作成し、共通鍵情報暗号化方式に従って送信したいデータを暗号化し、暗号化データを相手に送信する。通信相手は、同様の方法でセッション鍵を作成し、共通鍵情報暗号化方式に従って受信したデータを復号する。

【００６５】

セキュア通信管理部１６９は、公開鍵暗号ありで暗号化通信を行う場合には、擬似乱数生成方式に従ってランダムなセッション鍵を作成し、共通鍵情報暗号化方式に従ってセッション鍵で送信したいデータを暗号化し、信頼機関から通信相手の公開鍵を受信し、公開鍵暗号方式に従って通信相手の公開鍵でセッション鍵自体を暗号化し、暗号化データと暗号化セッション鍵を相手に送信する。通信相手は、自分の秘密鍵で暗号化セッション鍵を復号し、共通鍵情報暗号化方式に従ってセッション鍵で受信したデータを復号する。

【００６６】

セキュア通信管理部１６９は、データ認証子付き通信を行う場合であってＭＡＣ認証の場合、共有した鍵からＭＡＣ鍵導出方式により、ＭＡＣ鍵を作成し、ＭＡＣ認証方式に従

って送信したいデータにＭＡＣデータを付加し、ＭＡＣ付きデータを相手に送信する。通信相手は、同様の方法でＭＡＣ鍵を作成し、ＭＡＣ認証方式に従って受信したデータのＭＡＣを検証する。

【００６７】

セキュア通信管理部１６９は、データ認証子付き通信を行う場合で署名認証の場合、自分の秘密鍵で署名を付加し、署名付きデータを相手に送信する。通信相手は、相手の公開鍵が登録されている信頼機関から通信相手の公開鍵を受信し、相手の公開鍵の正当性を検証し、検証が正しく終了した場合、署名認証方式に従って相手の公開鍵で受信した署名付きデータを検証する。

【００６８】

図３は、暗号管理サーバ装置３５０の詳細な構成図である。暗号管理サーバ装置３５０は、暗号モジュールＤＢ３５３と、暗号評価ＤＢ３５４と、暗号モジュールＤＢ３５３と暗号評価ＤＢ３５４とに記憶された情報の読み出しや更新等の処理を行う暗号管理部３５１と、暗号モジュールＤＢ３５３と暗号評価ＤＢ３５４とに情報の登録を行う暗号登録部３５５と、暗号クライアント装置１５０へ暗号の送信を行う暗号配信部３５２とから構成される。

【００６９】

暗号モジュールＤＢ３５３は、予め記憶するかユーザによって入力される暗号モジュール３０８を記憶するデータベースである。

暗号評価ＤＢ３５４は、予め記憶するかユーザに入力される暗号評価記述ファイル３０９を記憶するデータベースである。

【００７０】

暗号管理部３５１は、暗号管理サーバ装置３５０のユーザに対して、暗号モジュールＤＢ３５３と暗号評価ＤＢ３５４に格納された暗号モジュール３０８や暗号パッケージ３０７の検索、暗号評価部の内容表示、管理している暗号のリスト表示、既存の暗号の更新、既存の暗号の削除、新規の暗号の登録、暗号配信部の起動／終了を行うインターフェースを備える。暗号管理部３５１は、新規の暗号を登録する場合は、暗号登録部３５５へ登録依頼を行う。

【００７１】

暗号登録部３５５は、暗号パッケージ登録部３５７と複合型記述生成部３５８とを備えている。

暗号配信部３５２は、暗号パッケージ配信制御部３５９と、配布ポリシ３７１を持つ暗号パッケージ配布構成部３７０と、配布ポリシ３７１を持つ配布暗号モジュール選定部３６０とを備える。暗号配信部３５２は、暗号クライアント装置１５０からの要求を解釈し、暗号の初期登録・配信・更新の３つの手順を実施する待ち受けサービスを実行する。また、この待ち受けサービスは、処理内容のログを記録する。

【００７２】

配布暗号モジュール選定部３６０では、暗号の初期登録・配信・更新の３つの手順と暗号クライアント装置１５０からの要求に基づき、配信に適切な暗号モジュール３０８を選定する。暗号の初期登録の場合、配信する暗号モジュール３０８は、利用上必要不可欠であると規定し、配布ポリシ３７１に記述された暗号方式である。

暗号パッケージ配布構成部３７０では、配布暗号モジュール選定部３６０で選定された暗号モジュール３０８を元に、配布ポリシ３７１に従って、暗号モジュール３０８と、暗号モジュール３０８に対応する暗号評価記述ファイル３０９とを暗号パッケージ３０７として配布可能な形にするための構成処理を行う。配布ポリシ３７１は、例えば、以下の４つの項目が記述されている。

【００７３】

第１の項目は、暗号パッケージ３０７の配布の際の暗号化の可否である。第２の項目は、暗号パッケージ３０７の暗号化の暗号方式である。第３の項目は、暗号パッケージ３０７の配布の際の改ざん検出子の付加の可否である。第４の項目は、暗号パッケージ３０７

の改ざん検出子の暗号方式である。
暗号パッケージ配布構成部３７０が行う構成処理では、暗号評価ＤＢ３５４に格納された内容を暗号評価記述ファイル３０９として特定の形式で生成し、暗号パッケージ３０７に対して暗号管理サーバ装置３５０が配布認定する目的で認証子を付加し、暗号モジュール３０８と暗号評価記述ファイル３０９とをペアにして、暗号パッケージ３０７としてまとめる。
【００７４】
また、暗号パッケージ配布構成部３７０は、複数の暗号モジュール３０８を組み合わせた暗号モジュール３０８を、複数の暗号モジュール３０８とそれぞれに対応する暗号評価記述ファイル３０９とをまとめて１つの暗号パッケージとしても良い。また、暗号パッケージ配布構成部３７０が行う構成処理では、暗号クライアント装置１５０の暗号制御マネージャポリシや暗号管理サーバ装置３５０の配布ポリシ３７１に従って、暗号パッケージ３０７の暗号化および改ざん検出子の付加、そのための鍵生成と鍵管理を行う。
【００７５】
＜第２の実施形態＞
第１の実施形態では、最適な暗号方式の選定を、暗号クライアント装置が処理する場合について説明したが、第２の実施の形態は、暗号管理サーバ装置が最適な暗号方式の選定を主導で行う。すなわち、図４に示す暗号モジュール配信システムでは、暗号管理サーバ装置１３５０が選定した暗号方式の結果情報をモジュール選定ポリシ記憶部１１０が管理および利活用するサーバ強連携機構である。特に、モジュール選定ポリシ記憶部１１０の計算能力が乏しい場合、暗号管理サーバ装置１３５０が演算支援することで、暗号クライアント装置１１００内の応答パフォーマンスを向上させることができる。
【００７６】
具体的には、上位システム部１１５１からの要求に最適な暗号モジュール３０８の選定を暗号管理サーバ装置１３５０が実施し、暗号クライアント装置１１００の暗号制御マネージャ部１１５２はその結果を受け取り、その要求条件と最適な暗号モジュール３０８との関係を当該装置内の暗号情報記憶部１６００で管理する。暗号制御マネージャ部１１５２は、上位システム部１５１からの要求とこの要求に最適な暗号モジュール３０８との関係に基づき、上位システム部１５１からの暗号処理制御要求に応じた処理を行う。よって、第１の実施形態と異なり、暗号クライアント装置１１００は、暗号モジュール３０８の全選定機能や暗号モジュール３０８の選定に必要となる暗号パッケージ３０７の管理および暗号管理サーバ装置１３５０らの受信を必ずしも必要としない。
【００７７】
図４は、本発明の第２の実施形態による暗号モジュール配信システムの概略構成を示すブロック図である。本システムは、１個以上の暗号クライアント装置１１００、１個以上の暗号ハードウェア１４５０及び暗号管理サーバ装置１３５０を備えている。暗号ハードウェア１４５０は、第１の実施形態と同様である。ここで、暗号ハードウェア１４５０は、１個の暗号クライアント装置１１００につき、複数接続する形態でもよい。また暗号ハードウェア１４５０を暗号クライアント装置１１００内部に実装する形態でもよい。
【００７８】
図５は、暗号クライアント装置１１００の構成を示すブロック図である。暗号クライアント装置１１００は、上位システム部１１５１と、暗号制御マネージャ部１１５２と、暗号実装部１１５３と、通信機能１１５５とを備えている。また選定ポリシ１１５８は、安全性、処理速度、リソースに関する優先情報を設定したファイルである。上位システム部１１５１および暗号実装部１１５３は、第１の実施形態と同様の構成・機能である。
【００７９】
暗号制御マネージャ部１１５２は、暗号処理制御部１１５６と、鍵管理部１１６２と、暗号情報記憶部１６００と、暗号パッケージ管理部１１６６と、暗号ハードウェア管理制御部１１７０とを備えている。
暗号処理制御部１１５６は、上位システム部１１５１から暗号処理条件を含む暗号処理

制御要求を受け付ける機能と、暗号情報記憶部１６００を参照して暗号処理条件に紐づいた暗号モジュール１１５３を特定する機能と、暗号処理実行タイミングに従って暗号実装部１１５３へ暗号処理を要求する機能と、当該暗号処理に対する暗号処理ＩＤを発行して当該暗号処理に関する情報と関連付けて暗号情報記憶部１６００に記憶させる機能と、暗号実装部１１５３からの暗号処理結果および当該暗号処理に関する暗号処理ＩＤとを上位システム部１１５１へ出力する機能とをもっている。

【００８０】

鍵管理部１１６２は、上位システム部１１５１からの要求に従い、暗号情報記憶部１６００の鍵情報ＤＢ１１６５への鍵情報の登録、削除、取得、検索、更新処理を行う機能と、暗号鍵の登録が正常に実施された場合に鍵ＩＤを発行して当該登録処理に関する情報と関連づけて暗号情報記憶部１６００に記憶させる機能と、各処理結果を場合により暗号処理ＩＤや鍵ＩＤを含めて上位システム部１１５１へ出力する機能をもっている。

【００８１】

暗号情報記憶部１６００は、選定ＤＢ１６０１と、暗号モジュールリンクＤＢ１６０２と、暗号モジュールＤＢ１６０３と、鍵情報ＤＢ１１６５と、暗号処理ＤＢ１６０４とを記憶する機能を備えている。また、暗号情報記憶部１６００は、鍵管理部１１６２や暗号処理制御部１１５６および暗号パッケージ管理部１１６６からの要求に従い、暗号情報記憶部１６００が備える各ＤＢを制御管理する機能をもっていることとしても良い。

【００８２】

選定ＤＢ１６０１のデータ構造は、図６に示す通りである。暗号モジュールリンクＤＢ１６０２のデータ構造は、図７に示す通りである。暗号モジュールＤＢ１６０３のデータ構造は、図８に示す通りである。鍵情報ＤＢ１１６５のデータ構造は、図９に示す通りである。暗号処理ＤＢ１６０４のデータ構造は、図１０に示す通りである。図１１に、暗号情報記憶部１６００が備える各データベースの論理関係を示す。

【００８３】

暗号パッケージ管理部１１６６は、以下に説明する機能を有している。

まず、暗号パッケージ管理部１１６６は、上位システム部１１５１から入力された選定条件、選定ポリシ及びハードウェアプロファイルを含む情報を通信機能１１５５経由で暗号管理サーバ装置１３５０へ送信して得られる、選定された暗号パッケージ３０７のアルゴリズムＩＤ、 暗号評価記述ＩＤ、 暗号モジュールＩＤ及び推奨される鍵長情報を暗号情報記憶部１６００に登録する機能を持っている。

【００８４】

また、暗号パッケージ管理部１１６６は、上位システム部１１５１から入力された選定条件を基に選定ＤＢを特定して暗号化アルゴリズムから対応される鍵生成エンジンのアルゴリズムＩＤを特定する機能を持っている。

また、暗号パッケージ管理部１１６６は、暗号管理サーバ装置１３５０にて選定された鍵生成エンジンのアルゴリズムＩＤ、暗号評価記述ＩＤ及び暗号モジュールＩＤを暗号情報記憶部１６００に登録する機能を持っている。

【００８５】

また、暗号パッケージ管理部１１６６は、上位システム部１１５１から入力された要求に基づき通信機能１１５５経由で暗号管理サーバ装置１３５０に対して最終初期登録日時および最終初期登録ドメインを入力として暗号パッケージ初期登録プロトコルを実行し、必要最低限の暗号パッケージ３０７を暗号管理サーバ装置１３５０からダウンロードして暗号情報記憶部１６００に登録する機能を持っている。

【００８６】

また、暗号パッケージ管理部１１６６は、上位システム部１１５１から入力された選定条件、選定ポリシ、ハードウェアプロファイル及び端末内に保持する暗号パッケージ３０７のリストを含む情報を通信機能１１５５経由で暗号管理サーバ装置１３５０へ送信し、当該暗号管理サーバ装置１３５０にて選定された暗号パッケージ３０７の実体及びその付帯情報（アルゴリズムＩＤ、暗号評価記述ＩＤ、暗号モジュールＩＤ）を入手して暗号情

報記憶部１６００に登録する機能を持っている。
【００８７】
また、暗号パッケージ管理部１１６６は、暗号管理サーバ装置１３５０からの更新通知の通知先登録及び更新事象発生時に暗号制御マネージャ部１１５２が行うアクションのポリシ設定を行える機能を持っている。
また、暗号パッケージ管理部１１６６は、上位システム部１１５１から要求された内容と暗号制御マネージャ部１１５２に保持した最後の更新通知識別子に基づき通信機能１１５５経由で暗号管理サーバ装置１３５０と連携して暗号制御マネージャ部１１５２に保持している暗号パッケージ３０７の実体と暗号パッケージ３０７の選定ポリシと暗号パッケージ３０７の紐付けについて更新処理を実行する機能を持っている。
【００８８】
また、暗号パッケージ管理部１１６６は、上位システム部１１５１から要求された暗号パッケージ３０７の実体を暗号情報記憶部１６００から削除して当該暗号パッケージ３０７に紐付けられた暗号情報記憶部１６００が備える各データベースの関連付けを解除する機能を持っている。
また、暗号パッケージ管理部１１６６は、上位システム部１１５１から入力された移行先ドメイン情報、ハードウェアプロファイル及び当該装置内に保持する暗号パッケージ３０７のリストを含む情報を通信機能１１５５経由で暗号管理サーバ装置１３５０へ送信し、暗号管理サーバ装置１３５０にて選定された持ち出し規制の対象となる暗号パッケージ情報を取得して暗号クライアント装置１１００内に保持する対象の暗号パッケージ３０７を削除する機能とをもっている。
【００８９】
暗号ハードウェア管理制御部１１７０は、暗号制御マネージャ部１１５２の各部からの要求に応じて通信機能１１５５経由で暗号ハードウェアへの通信制御を行う機能をもっている。
通信機能１１５５は、暗号パッケージ管理部１１６６や暗号ハードウェア管理制御部１１７０と相手通信装置または暗号ハードウェアとが相互に通信するための機能をもっている。
【００９０】
図１２は、暗号管理サーバ装置１３５０の構成を示す機能ブロック図である。暗号管理サーバ装置１３５０は、サーバ上位システム部１３８０と、通信機能１３５６と、暗号管理サーバ制御部１３５２と、暗号パッケージ記憶部１３５５と、サーバ暗号制御マネージャ部１３９０とを備えている。
【００９１】
サーバ上位システム部１３８０は、暗号クライアント装置１１００のサーバ上位システム部１３８０と同様の機能に加え、暗号管理に関するシステム管理者からの制御要求を暗号管理サーバ制御部１３５２に送信する機能とをもっている。
通信機能１３５６は、暗号管理サーバ制御部１３５２やサーバ暗号制御マネージャ部１３９０と相手通信装置、暗号ハードウェアまたは暗号ハードウェアの動作を模擬したシミュレータとが相互に通信するための機能をもっている。
【００９２】
暗号管理サーバ制御部１３５２は、暗号パッケージ管制部１３５９と、暗号パッケージ管理部１３５１と、暗号パッケージ配布構成部１３７０と、配布暗号パッケージ選定部１３７３とを備えている。
暗号パッケージ管制部１３５９は、サーバ上位システム部１３８０からの要求により暗号パッケージ３０７を登録する機能と、サーバ上位システム部１３８０からの要求により既に登録済みの暗号パッケージを更新する機能と、ベンダからの暗号パッケージ提供時に該当する暗号パッケージの出所の確認を行うためのベンダ認定認証子を検証する機能と、複数の単体型暗号評価記述部または複数の複合型暗号評価記述部を組み合わせて複合型暗号評価記述部を生成する機能と、暗号モジュールＤＢ１３５５に登録されている暗号パッ

ケージ３０７を検索および一覧を取得する機能と、サーバ上位システム部１３８０からの要求により暗号モジュール３０８及び関連する暗号パッケージ３０７を暗号モジュールＤＢ１３５５から削除する機能と、暗号パッケージ記憶部１３５５に対して行った登録・更新・削除処理に対するログを出力する機能とをもっている。

【００９３】

暗号パッケージ管理部１３５１は、複数の暗号クライアント装置１１００からの管制要求を同時に並行して処理する機能と、暗号パッケージ３０７の初期登録処理、配信処理、更新処理、選定処理、更新通知処理および暗号管理ドメイン移行処理を行う機能と、暗号クライアント装置１１００と暗号管理サーバ装置１３５０との間でセキュリティ保護された通信路を確立するための機能と、当該暗号管理サーバ装置１３５０が管理するドメイン内に存在する暗号クライアント管理装置の状況を管理する機能と、暗号パッケージ３０７の初期登録処理、配信処理、更新処理、選定処理、更新通知処理および暗号管理ドメイン移行処理に対するログを生成する機能とをもっている。

【００９４】

暗号パッケージ配布構成部１３７０は、配布暗号パッケージ選定部１３７３で選ばれた暗号パッケージ３０７を暗号モジュールＤＢ１３５５から取得する機能と、暗号モジュールＤＢ１３５５に格納された各記述項目のデータをＸＭＬといった暗号評価記述形式で構成して出力する機能と、暗号パッケージ官制部１３５９のセキュリティ通信で使用する鍵に関して指定のセキュリティ方式に応じてサーバ暗号制御マネージャ部１３９０に処理を依頼して鍵生成を行う機能と、暗号クライアント装置１１００のＩＤや鍵のセキュリティ方式を含む情報を元に鍵に関する情報の管理を行う機能と、暗号管理サーバ装置１３５０の配布ポリシで定義されたセキュリティレベル及びセキュリティ方式に応じて暗号管理サーバ装置１３５０から暗号クライアント装置１１００に対して送信する情報に対するデータ秘匿やデータ認証のセキュリティ処理を行う機能とをもっている。

【００９５】

配布暗号パッケージ選定部１３７３は、暗号パッケージ初期登録処理における初期登録判定、暗号方式の選択及び暗号パッケージ選択を行う機能と、暗号パッケージ配信処理における配信判定及び暗号パッケージの選択を行う機能と、暗号パッケージ更新処理における配信判定を行う機能と、暗号パッケージ更新処理における更新暗号リスト取得及び暗号パッケージの選択を行う機能と、暗号パッケージ選定処理における選択判定及び暗号パッケージ選択を行う機能と、暗号管理ドメイン移行処理のおける移動判定およびドメイン移動処理情報の生成を行う機能と、選定条件、選定ポリシ及びハードウェアポリシを満たす暗号パッケージを暗号パッケージ記憶部から検索する機能とをもっている。

【００９６】

暗号モジュールＤＢ１３５５は、登録されている暗号モジュール３０８を記録管理する暗号モジュールＤＢ１３５３と暗号評価記述ファイル３０９を記録管理する暗号評価ＤＢ１３５４とを備えている。

サーバ暗号制御マネージャ部１３９０は、暗号クライアント装置１１００の暗号制御マネージャ部１１５２と同様の機能に加え、暗号管理サーバ制御部１３５２と連携して暗号管理サーバ装置１３５０内の暗号資産管理制御や他通信装置との暗号認証通信を行う機能をもっている。

【００９７】

＜第３の実施形態＞

次に、上述した暗号モジュール配信システムにおける暗号の初期登録処理にて、暗号管理サーバが、暗号処理ハードウェアを用いてクライアント装置に暗号モジュールを配信する動作例について、詳細に説明する。

また、本実施形態例では、暗号処理装置として暗号処理ハードウェアを用いることとするが、暗号処理装置は、ハードウェアに限るものではなく、ソフトウェアで実装することとしても良い。

【００９８】

図１３は、本発明による第３の実施形態の暗号モジュール配信システムの構成を示す図である。

本実施形態による暗号モジュール配信システムは、暗号管理サーバ装置１０１と、クライアント装置１０２と、クライアント装置１０２に接続された暗号ハードウェア１０３とを備えている。暗号管理サーバ装置１０１は、暗号モジュールを記憶し、暗号処理をハードウェアとして実現した耐タンパーな暗号ハードウェア１０３との間で、セキュアセッションを確立して、クライアント装置１０２に暗号モジュールを安全に配信する。

第３の実施形態では、初期暗号モジュールを共通鍵暗号方式にて暗号化し、暗号管理サーバ装置１０１から暗号ハードウェア１０３に配信する。この際、暗号管理サーバ装置１０１と暗号ハードウェア１０３とが、共通鍵を用いて通信を行う。

【００９９】

以下、本発明による第３の実施形態の構成について説明する。

図１４は、本発明による第３の実施形態の暗号管理サーバ装置の構成を示すブロック図である。暗号管理サーバ装置２０１は、通信機能２０２と、配布暗号モジュール選定部２０３と、鍵生成部２０４と、鍵共有部２０５と、暗号モジュールＤＢ２０６と、暗号モジュール暗号化部２０７とを備えている。暗号管理サーバ装置２０１は、図１３における暗号管理サーバ装置１０１に対応する。

【０１００】

通信機能２０２は、クライアント装置３０１と通信し、各種情報の送受信を行う。配布暗号モジュール選定部２０３は、例えば、クライアント装置３０１の端末識別情報に基づいて、暗号モジュールＤＢ２０６から暗号モジュールを読み出す。鍵生成部２０４は、暗号ハードウェア４０１へ暗号モジュールを送信するための共通鍵を生成する。鍵共有部２０５は、暗号ハードウェア４０１の鍵共有部４０４と連携して鍵共有を行い、生成したセッション鍵を用いて鍵生成部２０４に生成された共通鍵を暗号ハードウェア４０１に送信する。暗号モジュールＤＢ２０６には、予め複数の暗号モジュールが記憶されている。暗号モジュール暗号化部２０７は、暗号ハードウェア４０１へ送信する暗号モジュールを鍵生成部２０４によって生成される鍵を用いて暗号化する。

【０１０１】

図１５は、本発明による第３の実施形態のクライアント装置の構成を示すブロック図である。クライアント装置３０１は、通信機能３０２と、暗号モジュールＤＢ３０３と、端末情報格納部３０４と、暗号ハードウェア管理制御部３０５と、暗号実装部３０６とを備えている。クライアント装置３０１は、図１３におけるクライアント装置１０２に対応する。

通信機能３０２は、暗号管理サーバ装置２０１と通信し、各種情報の送受信を行う。暗号モジュールＤＢ３０３は、暗号管理サーバ装置２０１から送信される暗号モジュールを記憶する。端末情報格納部３０４は、クライアント装置３０１の個体の情報である端末情報を記憶し、クライアント装置３０１の識別情報である端末識別情報に対応付けて、例えば、ＣＰＵやメモリ容量などを数値化した情報である性能情報や、インストール済みのアプリケーションの情報などが記憶される。暗号ハードウェア管理制御部３０５は、暗号ハードウェア４０１と通信を行い、暗号管理サーバ装置２０１から送信される暗号モジュールを取得する。暗号実装部３０６には、受信する暗号モジュールが利用可能な状態に実装されており、暗号処理を行う。

【０１０２】

図１６は、本発明による第３の実施形態の暗号ハードウェアの構成を示すブロック図である。暗号ハードウェア４０１は、通信機能４０２と、鍵格納部４０３と、鍵共有部４０４と、暗号モジュール復号部４０５とを備えている。暗号ハードウェア４０１は、図１３における暗号ハードウェア１０３に対応する。

通信機能４０２は、クライアント装置３０１と、またはクライアント装置３０１の暗号ハードウェア管理制御部３０５を介して暗号管理サーバ装置２０１と通信を行う。鍵格納部４０３は、暗号管理サーバ装置２０１から送信される共通鍵を記憶する。鍵共有部４０

４は、暗号管理サーバ装置２０１の鍵共有部２０５と連携して鍵共有を行い、生成したセッション鍵を用いて鍵生成部２０４に生成された共通鍵を暗号ハードウェア４０１に送信する。暗号モジュール復号部４０５は、鍵格納部４０３に記憶された共通鍵を用いて、受信するデータ（暗号モジュール）を復号する。

【０１０３】

次に、図１７を参照して、第３の実施形態の動作例を説明する。

図１７は、本発明による第３の実施形態による暗号モジュール配信システムの動作例を示すシーケンス図である。

まず、クライアント装置３０１の通信機能３０２が、暗号管理サーバ装置２０１に、初期暗号モジュール登録要求を送信する（ステップＳ１）。暗号管理サーバ装置２０１の通信機能２０２が、初期暗号モジュール登録要求を受信すると、クライアント装置３０１に対し、端末情報要求を送信する（ステップＳ２）。

【０１０４】

クライアント装置３０１の通信機能３０２が、送信された端末情報要求を受信すると、通信機能３０２が、端末情報格納部３０４に格納されているクライアント装置３０１の端末情報を暗号管理サーバ装置２０１へ送信する（ステップＳ３）。暗号管理サーバ装置２０１の通信機能２０２が、端末情報を受信すると、配布暗号モジュール選定部２０３が、例えば、端末の識別情報ごとに暗号モジュールの識別情報との対応表を予め記憶しておくこととして、受信した端末情報に含まれる端末識別情報に基づいてこの対応表を参照して、要求を送ってきたクライアント装置３０１の端末識別情報に対応する暗号モジュールを、クライアント装置３０１で利用可能な暗号モジュールとして暗号モジュールＤＢ２０６から選定し、読み出す（ステップＳ４）。ここで、端末の識別情報と暗号モジュールの識別情報との対応表のデータ例を図３４に示す。図３４に示されるように、対応表には、例えば、端末の識別情報である端末ＩＤに対応付けて、搭載中の暗号モジュールの識別情報と、搭載可能暗号モジュールの識別情報とが記憶される。

【０１０５】

配布暗号モジュール選定部２０３が、暗号モジュールＤＢ２０６から暗号モジュールを選定した場合は、暗号管理サーバ装置２０１の通信機能２０２が、クライアント装置３０１に処理の続行を示す情報を送信する。一方、配布暗号モジュール選定部２０３が、クライアント装置３０１にて利用可能な暗号モジュールを選定できなかった場合は、通信機能２０２からクライアント装置３０１に処理の終了を示す情報を送信する（ステップＳ５）。

【０１０６】

クライアント装置３０１の通信機能３０２が、暗号管理サーバ装置２０１から処理の続行を示す情報を受信すると、初期登録情報の要求を暗号管理サーバ装置２０１へ送信する（ステップＳ６）。一方、クライアント装置３０１の通信機能３０２が、暗号管理サーバ装置２０１の通信機能２０２から処理の終了を示す情報を受信した場合、クライアント装置３０１と暗号管理サーバ装置２０１との間の通信を終了する。

【０１０７】

暗号管理サーバ装置２０１の通信機能２０２が、初期登録情報の要求を受信すると、鍵生成部２０４が、クライアント装置３０１に送信する暗号モジュールを暗号化するための共通鍵を生成する（ステップＳ７）。そして、暗号管理サーバ装置２０１の鍵共有部２０５が、暗号ハードウェア４０１の鍵共有部４０４と鍵共有方式による鍵共有を行う。鍵共有方式は、例えば、Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ鍵共有などでも良い。

【０１０８】

上記Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ鍵共有とは、共通鍵暗号方式における鍵の受け渡しを安全に行うために提案された方式である。すなわち、暗号管理サーバ装置２０１の鍵生成部２０４と、暗号ハードウェア４０１の鍵共有部４０４が、それぞれ公開鍵と秘密鍵を用意し、公開鍵を公開する。そして、それぞれが自身の秘密鍵に基づいて生成するデータを相手に送信し、それぞれが自身の秘密鍵と受信したデータとに基づいて共有鍵（以下、

セッション鍵）を生成する方法である。このように鍵共有を行うことで、送受信されるデータが第三者に盗聴されても、第三者は秘密鍵を持たないためにセッション鍵を生成することができない。

【０１０９】

暗号管理サーバ装置２０１の鍵共有部２０５が、このような鍵共有方式によりセッション鍵の生成に成功すると、クライアント装置３０１の暗号ハードウェア管理制御部３０５を介して、暗号ハードウェア４０１に、セキュアセッションの確立を通知する。同様に、暗号ハードウェア４０１の鍵共有部４０４は、セッション鍵の生成に成功すると、暗号管理サーバ装置２０１に、セキュアセッションの確立を通知する（ステップＳ８、ステップＳ９）。ここで、暗号管理サーバ装置２０１の鍵共有部２０５と暗号ハードウェア４０１の鍵共有部４０４とが、生成したセッション鍵を用いて、送信側が情報を暗号化し、受信側が情報を復号化して通信を行うことを、セキュアセッションにより通信するという。

【０１１０】

暗号管理サーバ装置２０１と暗号ハードウェア４０１との間にセキュアセッションが確立すると、暗号管理サーバ装置２０１の鍵共有部２０５が、セッション鍵で共通鍵を暗号化して、セキュアセッションにより、クライアント装置３０１の通信機能３０２を介して暗号ハードウェア４０１に送信する（ステップＳ１０）。暗号ハードウェア４０１は、受信した共通鍵を、鍵共有部によってセッション鍵を用いて復号して、鍵格納部４０３に格納する（ステップＳ１１）。

【０１１１】

暗号ハードウェア４０１は、共通鍵を取得すると、通信機能４０２を介して、クライアント装置３０１にセキュアセッション切断通知を送信する（ステップＳ１２）。暗号管理サーバ装置２０１は、セキュアセッション切断通知を受信すると、暗号モジュール暗号化部２０７が、ステップＳ４で選定した暗号モジュールを、ステップＳ７で生成した共通鍵に基づいて暗号化する（ステップＳ１３）。暗号管理サーバ装置２０１の通信機能２０２は、暗号化された暗号モジュールを、クライアント装置３０１に送信する（ステップＳ１４）。

【０１１２】

クライアント装置３０１の通信機能３０２が、暗号化された暗号モジュールを受信すると、暗号管理サーバ装置２０１に、暗号モジュールを正常に受信できたことを示す暗号モジュール受信結果通知を送信する（ステップＳ１５）。そして、暗号管理サーバ装置２０１の通信機能２０２が暗号モジュール受信結果通知を受信すると、暗号管理サーバ装置２０１の通信機能２０２が、クライアント装置３０１に、初期暗号エンジン登録処理の終了を示す情報を送信する（ステップＳ１６）。

【０１１３】

また、クライアント装置３０１の通信機能３０２が、暗号化された暗号モジュールを受信できなければ、クライアント装置３０１の通信機能３０２が、暗号管理サーバ装置２０１に、暗号モジュールを正常に受信できなかったことを示す暗号モジュール受信結果通知を送信する。そして、暗号管理サーバ装置２０１の通信機能２０２が暗号モジュール受信結果通知を受信すると、暗号管理サーバ装置２０１の通信機能２０２は、暗号モジュールを再送信する。通信機能２０２は、予め設定された回数を超えて暗号モジュールの再送信処理を行い、暗号モジュールを正常に受信できなかった場合には、エラーとして処理を終了する。

【０１１４】

クライアント装置３０１の通信機能３０２が、初期暗号エンジン登録処理の終了を示す情報を受信した場合、暗号ハードウェア管理制御部３０５が、暗号ハードウェア４０１に、暗号管理サーバ装置２０１から受信した暗号モジュールを送信する（ステップＳ１７）。

そして、暗号ハードウェア４０１の通信機能４０２が、暗号化された暗号モジュールを受信すると、暗号エンジン復号部４０５が、鍵格納部４０３に記憶された共通鍵を読み出

して、この共通鍵を用いて暗号モジュールを復号し（ステップＳ１８）、復号された暗号モジュールを通信機能４０２により暗号管理サーバ装置２０１に送信する（ステップＳ１９）。クライアント装置３０１の暗号ハードウェア管理制御部３０５が暗号モジュールを受信すると、暗号モジュールを暗号実装部３０６に実装して、利用可能状態にさせる。さらに、暗号モジュールＤＢ３０３に、暗号実装部３０６に格納した暗号モジュールを格納する（ステップＳ２０）。

【０１１５】

＜第４の実施形態＞

次に、上述した暗号モジュール配信システムの鍵の配送について、他の実施形態について説明する。第３の実施形態では、暗号モジュールは暗号化された状態で送信されたが、第４の実施形態では、暗号モジュールは暗号化されず、完全性を検証可能なＭＡＣを付加する。ＭＡＣは、メッセージ認証子であり、例えば、秘密鍵であるＭＡＣ鍵とハッシュ関数とを組み合わせて算出するＭＡＣ値である。メッセージとＭＡＣを取得した受信者は、メッセージからＭＡＣ値を算出することで、送信者が秘密鍵の所有者であることの確認や、メッセージ送信中に改ざんなどの不正行為が行われていないかを検証することができる。

【０１１６】

第４の実施形態による暗号モジュール配信システムは第３の実施形態と同様の構成をしており、同様の構成・処理については説明を省略する。以下、第４の実施形態に特有の構成・処理についてのみ説明する。

図１８は、本発明による第４の実施形態の暗号管理サーバ装置の構成を示すブロック図である。暗号管理サーバ装置６０１は、通信機能６０２と、配布暗号モジュール選定部６０３と、鍵生成部６０４と、鍵共有部６０５と、暗号モジュールＤＢ６０６と、ＭＡＣ生成部６０７とを備えている。暗号管理サーバ装置６０１は、図１３における暗号管理サーバ装置１０１に対応する。ＭＡＣ生成部６０７は、暗号ハードウェア７０１へ送信する暗号モジュールに、鍵生成部６０４に生成される鍵を用いて生成するＭＡＣを付加する。

【０１１７】

クライアント装置３０１は、第３の実施形態と同様の構成である。

図１９は、本発明による第４の実施形態の暗号ハードウェアの構成を示すブロック図である。暗号ハードウェア７０１は、通信機能７０２と、鍵格納部７０３と、鍵共有部７０４と、ＭＡＣ検証部７０５とを備えている。暗号ハードウェア７０１は、図１３における暗号ハードウェア１０３に対応する。

ＭＡＣ検証部７０５は、鍵格納部７０３に記憶されたＭＡＣ鍵を用いて、受信するデータ（暗号モジュール）のＭＡＣを検証する。

【０１１８】

次に、図２０を参照して、第４の実施形態の動作例を説明する。

図２０は、本発明による第４の実施形態による暗号モジュール配信システムの動作例を示すシーケンス図である。

まず、クライアント装置３０１の通信機能３０２は、暗号管理サーバ装置６０１に、初期暗号モジュール登録要求を送信する（ステップＳ３１）。暗号管理サーバ装置６０１の通信機能６０２が、初期暗号モジュール登録要求を受信すると、クライアント装置３０１に対し、端末情報要求を送信する（ステップＳ３２）。

【０１１９】

クライアント装置３０１の通信機能３０２が、送信された端末情報要求を受信すると、通信機能３０２が、端末情報格納部３０４に格納されているクライアント装置３０１の端末情報を暗号管理サーバ装置６０１へ送信する（ステップＳ３３）。暗号管理サーバ装置６０１の通信機能６０２が、端末情報を受信すると、配布暗号モジュール選定部６０３が、例えば、端末の識別情報ごとに暗号モジュールの識別情報との対応表を予め記憶しており、受信した端末情報に含まれる端末識別情報に基づいてこの対応表を参照して、要求を送ってきたクライアント装置３０１の端末識別情報に対応する暗号モジュールを、クライ

アント装置３０１で利用可能な暗号モジュールとして暗号モジュールＤＢ６０６から選定し、読み出す（ステップＳ３４）。

【０１２０】

配布暗号モジュール選定部６０３が、暗号モジュールＤＢ６０６から暗号モジュールを選定した場合は、暗号管理サーバ装置６０１の通信機能６０２が、クライアント装置３０１に処理の続行を示す情報を送信する。一方、配布暗号モジュール選定部６０３が、クライアント装置３０１にて利用可能な暗号モジュールを選定できなかった場合は、通信機能６０２からクライアント装置３０１に処理の終了を示す情報を送信する（ステップＳ３５）。

【０１２１】

クライアント装置３０１の通信機能３０２が、暗号管理サーバ装置６０１から処理の続行を示す情報を受信すると、初期登録情報の要求を暗号管理サーバ装置６０１へ送信する（ステップＳ３６）。一方、クライアント装置３０１の通信機能３０２が、暗号管理サーバ装置６０１の通信機能６０２から処理の終了を示す情報を受信した場合、クライアント装置３０１と暗号管理サーバ装置６０１との間の通信を終了する。

【０１２２】

暗号管理サーバ装置６０１の通信機能６０２が、初期登録情報の要求を受信すると、鍵生成部６０４が、クライアント装置３０１に送信する暗号モジュールにＭＡＣを付加するためのＭＡＣ鍵を生成する（ステップＳ３７）。そして、暗号管理サーバ装置６０１の鍵共有部６０５が、暗号ハードウェア７０１の鍵共有部７０４と鍵共有方式による鍵共有を行う。鍵共有方式は、例えば、Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ鍵共有などでも良い。

【０１２３】

暗号管理サーバ装置６０１の鍵共有部６０５が、このような鍵共有方式によりセッション鍵の生成に成功すると、クライアント装置３０１の暗号ハードウェア管理制御部３０５を介して、暗号ハードウェア７０１に、セキュアセッションの確立を通知する。同様に、暗号ハードウェア７０１の鍵共有部７０４は、セッション鍵の生成に成功すると、暗号管理サーバ装置６０１に、セキュアセッションの確立を通知する（ステップＳ３８、ステップＳ３９）。ここで、暗号管理サーバ装置６０１の鍵共有部６０５と暗号ハードウェア７０１の鍵共有部７０４とが、生成したセッション鍵を用いて、送信側が情報を暗号化し、受信側が情報を復号化して通信を行うことを、セキュアセッションにより通信するという。

【０１２４】

暗号管理サーバ装置６０１と暗号ハードウェア７０１との間にセキュアセッションが確立すると、暗号管理サーバ装置６０１の鍵共有部６０５が、セッション鍵でＭＡＣ鍵を暗号化して、セキュアセッションにより、クライアント装置３０１の通信機能３０２を介して暗号ハードウェア７０１に送信する（ステップＳ４０）。暗号ハードウェア７０１は、受信したＭＡＣ鍵を、鍵共有部によってセッション鍵を用いて復号して、鍵格納部７０３に格納する（ステップＳ４１）。

【０１２５】

暗号ハードウェア７０１は、ＭＡＣ鍵を取得すると、通信機能７０２を介して、クライアント装置３０１にセキュアセッション切断通知を送信する（ステップＳ４２）。暗号管理サーバ装置６０１は、セキュアセッション切断通知を受信すると、ＭＡＣ生成部６０７が、ステップＳ３４で選定した暗号モジュールを、ステップＳ３７で生成したＭＡＣ鍵に基づいてＭＡＣ（値）を算出する（ステップＳ４３）。暗号管理サーバ装置６０１の通信機能６０２は、暗号モジュールと算出したＭＡＣとを、クライアント装置３０１に送信する（ステップＳ４４）。

【０１２６】

クライアント装置３０１の通信機能３０２が、暗号モジュールとＭＡＣとを受信すると、暗号管理サーバ装置６０１に、暗号モジュールを正常に受信できたことを示す暗号モジュール受信結果通知を送信する（ステップＳ４５）。そして、暗号管理サーバ装置６０１

の通信機能６０２が暗号モジュール受信結果通知を受信すると、暗号管理サーバ装置６０１の通信機能６０２が、クライアント装置３０１に、初期暗号エンジン登録処理の終了を示す情報を送信する（ステップＳ４６）。

【０１２７】

また、クライアント装置３０１の通信機能３０２が、暗号化された暗号モジュールとＭＡＣとを受信できなければ、クライアント装置３０１の通信機能３０２が、暗号管理サーバ装置６０１に、暗号モジュールとＭＡＣとを正常に受信できなかったことを示す暗号モジュール受信結果通知を送信する。そして、暗号管理サーバ装置６０１の通信機能６０２が暗号モジュール受信結果通知を受信すると、暗号管理サーバ装置６０１の通信機能６０２は、暗号モジュールを再送信する。通信機能６０２は、予め設定された回数を超えて暗号モジュールとＭＡＣとの再送信処理を行い、暗号モジュールとＭＡＣとを正常に受信できなかった場合には、エラーとして処理を終了する。

【０１２８】

クライアント装置３０１の通信機能３０２が、初期暗号エンジン登録処理の終了を示す情報を受信した場合、暗号ハードウェア管理制御部３０５が、暗号ハードウェア７０１に、暗号管理サーバ装置６０１から受信した暗号モジュールとＭＡＣとを送信する（ステップＳ４７）。

そして、暗号ハードウェア７０１の通信機能７０２が、暗号モジュールとＭＡＣとを受信すると、ＭＡＣ検証部７０５が、鍵格納部７０３に記憶したＭＡＣ鍵を読み出して、このＭＡＣ鍵を用いてＭＡＣを検証する（ステップＳ４８）。すなわち、ＭＡＣ検証部７０５は、ＭＡＣが暗号モジュールとＭＡＣ鍵とに基づいて算出されたものであれば、ＭＡＣが正当であることを示す検証結果を生成し、ＭＡＣが暗号モジュールとＭＡＣ鍵とに基づいて算出されたものでなければ、ＭＡＣが正当ではないことを示す検証結果を生成する。

【０１２９】

ＭＡＣ検証部７０５は、検証結果を通信機能７０２により暗号管理サーバ装置６０１に送信する（ステップＳ４９）。クライアント装置３０１の暗号ハードウェア管理制御部３０５は、検証結果を受信し、検証結果が正当であることを示す場合は、受信した暗号モジュールを暗号実装部３０６に実装して、利用可能状態にさせる。さらに、暗号モジュールＤＢ３０３に、暗号実装部３０６に格納した暗号モジュールを格納する（ステップＳ５０）。暗号ハードウェア管理制御部３０５は、受信した検証結果が、正当でないことを示す場合は、エラーとして処理を終了する。

【０１３０】

＜第５の実施形態＞

次に、上述した暗号モジュール配信システムの鍵の配送について、他の実施形態について説明する。第５の実施形態では、配信する暗号モジュールを共通鍵で暗号化した上で、ＭＡＣを付加する。

【０１３１】

第５の実施形態による暗号モジュール配信システムは第３の実施形態および第４の実施形態と同様の構成をしており、同様の構成・処理については説明を省略する。以下、第５の実施形態に特有の構成・処理についてのみ説明する。

図２１は、本発明による第５の実施形態の暗号管理サーバ装置の構成を示すブロック図である。暗号管理サーバ装置９０１は、通信機能９０２と、配布暗号モジュール選定部９０３と、鍵生成部９０４と、鍵共有部９０５と、暗号モジュールＤＢ９０６と、ＭＡＣ生成部９０７と、暗号モジュール暗号化部９０８とを備えている。暗号管理サーバ装置９０１は、図１３における暗号管理サーバ装置１０１に対応する。

【０１３２】

クライアント装置３０１は、第３の実施形態と同様の構成である。

図２２は、本発明による第５の実施形態の暗号ハードウェアの構成を示すブロック図である。暗号ハードウェア１００１は、通信機能１００２と、鍵格納部１００３と、鍵共有部１００４と、暗号モジュール復号部１００５と、ＭＡＣ検証部１００６とを備えている

。暗号ハードウェア１００１は、図１３における暗号ハードウェア１０３に対応する。
【０１３３】
次に、図２３を参照して、第５の実施形態の動作例を説明する。
図２３は、本発明による第５の実施形態による暗号モジュール配信システムの動作例を示すシーケンス図である。
まず、クライアント装置３０１の通信機能３０２は、暗号管理サーバ装置９０１に、初期暗号モジュール登録要求を送信する（ステップＳ６１）。暗号管理サーバ装置９０１は、通信機能９０２にて初期暗号モジュール登録要求を受信すると、通信機能９０２からクライアント装置３０１に対し、端末情報要求を送信する（ステップＳ６２）。
【０１３４】
クライアント装置３０１の通信機能３０２が、送信された端末情報要求を受信すると、通信機能３０２が、端末情報格納部３０４に格納されているクライアント装置３０１の端末情報を暗号管理サーバ装置９０１へ送信する（ステップＳ６３）。暗号管理サーバ装置９０１の通信機能９０２が、端末情報を受信すると、配布暗号モジュール選定部９０３が、例えば、端末の識別情報ごとに暗号モジュールの識別情報との対応表を予め記憶しておくこととして、受信した端末情報に含まれる端末識別情報に基づいてこの対応表を参照して、要求を送ってきたクライアント装置３０１の端末識別情報に対応する暗号モジュールを、クライアント装置３０１で利用可能な暗号モジュールとして暗号モジュールＤＢ９０６から選定し、読み出す（ステップＳ６４）。
【０１３５】
配布暗号モジュール選定部９０３が、暗号モジュールＤＢ９０６から暗号モジュールを選定した場合は、暗号管理サーバ装置９０１の通信機能９０２が、クライアント装置３０１に処理の続行を示す情報を送信する。一方、配布暗号モジュール選定部９０３が、クライアント装置３０１にて利用可能な暗号モジュールを選定できなかった場合は、通信機能９０２からクライアント装置３０１に処理の終了を示す情報を送信する（ステップＳ６５）。
【０１３６】
クライアント装置３０１の通信機能３０２が、暗号管理サーバ装置９０１から処理の続行を示す情報を受信すると、初期登録情報の要求を暗号管理サーバ装置９０１へ送信する（ステップＳ６６）。一方、クライアント装置３０１の通信機能３０２が、暗号管理サーバ装置９０１の通信機能９０２から処理の終了を示す情報を受信した場合、クライアント装置３０１と暗号管理サーバ装置９０１との間の通信を終了する。
【０１３７】
暗号管理サーバ装置９０１の通信機能９０２が、初期登録情報の要求を受信すると、鍵生成部９０４が、クライアント装置３０１に送信する暗号モジュールを暗号化するための共通鍵と、暗号モジュールにＭＡＣを付加するためのＭＡＣ鍵とを生成する（ステップＳ６７）。ここで、暗号モジュールを暗号化するための共通鍵とＭＡＣを生成するためのＭＡＣ鍵は同一でも良い。そして、暗号管理サーバ装置９０１の鍵共有部９０５が、暗号ハードウェア１００１の鍵共有部１００４と鍵共有方式による鍵共有を行う。鍵共有方式は、例えば、Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ鍵共有などでも良い。
【０１３８】
暗号管理サーバ装置９０１の鍵共有部９０５が、このような鍵共有方式によりセッション鍵の生成に成功すると、クライアント装置３０１の暗号ハードウェア管理制御部３０５を介して、暗号ハードウェア１００１に、セキュアセッションの確立を通知する。同様に、暗号ハードウェア１００１の鍵共有部１００４は、セッション鍵の生成に成功すると、暗号管理サーバ装置９０１に、セキュアセッションの確立を通知する（ステップＳ６８、ステップＳ６９）。ここで、暗号管理サーバ装置９０１の鍵共有部９０５と暗号ハードウェア１００１の鍵共有部１００４とが、生成したセッション鍵を用いて、送信側が情報を暗号化し、受信側が情報を復号化して通信を行うことを、セキュアセッションにより通信するという。

【０１３９】
暗号管理サーバ装置９０１と暗号ハードウェア１００１との間にセキュアセッションが確立すると、暗号管理サーバ装置９０１の鍵共有部９０５が、セッション鍵で共通鍵とＭＡＣ鍵とを暗号化して、セキュアセッションにより、クライアント装置３０１の通信機能３０２を介して暗号ハードウェア１００１に送信する（ステップＳ７０）。暗号ハードウェア１００１は、受信した共通鍵とＭＡＣ鍵とを、鍵共有部によってセッション鍵を用いて復号して、鍵格納部１００３に格納する（ステップＳ７１）。
【０１４０】
暗号ハードウェア１００１は、共通鍵とＭＡＣ鍵とを取得すると、通信機能１００２を介して、クライアント装置３０１にセキュアセッション切断通知を送信する（ステップＳ７２）。暗号管理サーバ装置９０１は、セキュアセッション切断通知を受信する。そして、暗号モジュール暗号化部９０８が、ステップＳ６７で生成した共通鍵に基づいて暗号モジュールを暗号化する（ステップＳ７３）。さらに、ＭＡＣ生成部９０７が、ステップＳ６７で生成したＭＡＣ鍵に基づいて、暗号モジュールのＭＡＣ（値）を算出する（ステップＳ７４）。ここで、暗号モジュールのＭＡＣを算出した後に、暗号モジュールとＭＡＣとを合わせてステップＳ６７で生成した共通鍵に基づいて暗号化した情報をクライアント装置３０１に送信しても良い。暗号管理サーバ装置９０１の通信機能９０２は、暗号化された暗号モジュールと算出したＭＡＣとを、クライアント装置３０１に送信する（ステップＳ７５）。
【０１４１】
クライアント装置３０１の通信機能３０２が、暗号化された暗号モジュールとＭＡＣとを受信すると、暗号管理サーバ装置９０１に、暗号化された暗号モジュールとＭＡＣとを正常に受信できたことを示す暗号モジュール受信結果通知を送信する（ステップＳ７６）。そして、暗号管理サーバ装置９０１の通信機能９０２が暗号モジュール受信結果通知を受信すると、暗号管理サーバ装置９０１の通信機能９０２が、クライアント装置３０１に、初期暗号エンジン登録処理の終了を示す情報を送信する（ステップＳ７７）。
【０１４２】
また、クライアント装置３０１の通信機能３０２が、暗号化された暗号モジュールとＭＡＣとを受信できなければ、クライアント装置３０１の通信機能３０２が、暗号管理サーバ装置９０１に、暗号モジュールとＭＡＣとを正常に受信できなかったことを示す暗号モジュール受信結果通知を送信する。そして、暗号管理サーバ装置９０１の通信機能９０２が暗号モジュール受信結果通知を受信すると、暗号管理サーバ装置９０１の通信機能９０２は、暗号化された暗号モジュールとＭＡＣとを再送信する。通信機能９０２は、予め設定された回数を超えて暗号化された暗号モジュールとＭＡＣとの再送信処理を行い、暗号化された暗号モジュールとＭＡＣとを正常に受信できなかった場合には、エラーとして処理を終了する。
【０１４３】
クライアント装置３０１の通信機能３０２が、初期暗号エンジン登録処理の終了を示す情報を受信した場合、暗号ハードウェア管理制御部３０５が、暗号ハードウェア１００１に、暗号管理サーバ装置９０１から受信した暗号化された暗号モジュールとＭＡＣとを送信する（ステップＳ７８）。
そして、暗号ハードウェア１００１の通信機能１００２が、暗号化された暗号モジュールとＭＡＣとを受信すると、暗号モジュール復号部１００５が、鍵格納部１００３に記憶された共通鍵を読み出して、この共通鍵を用いて暗号化された暗号モジュールを復号する（ステップＳ７９）。さらに、ＭＡＣ検証部１００６が、鍵格納部１００３に記憶したＭＡＣ鍵を読み出して、このＭＡＣ鍵を用いてＭＡＣが正当であるか否かを検証し（ステップＳ８０）、検証結果を生成する。
【０１４４】
通信機能１００２は、復号した暗号モジュールと検証結果とを暗号管理サーバ装置９０１に送信する（ステップＳ８１）。クライアント装置３０１の暗号ハードウェア管理制御

部３０５は、暗号モジュールと検証結果とを受信し、検証結果が正当であることを示す場合は、受信した暗号モジュールを暗号実装部３０６に実装して、利用可能状態にさせる。さらに、暗号モジュールＤＢ３０３に、暗号実装部３０６に格納した暗号モジュールを格納する（ステップＳ８２）。暗号ハードウェア管理制御部３０５は、受信した検証結果が、正当でないことを示す場合は、エラーとして処理を終了する。

【０１４５】

＜第６の実施形態＞

次に、上述した暗号モジュール配信システムの鍵の配送について、他の実施形態について説明する。

第１から第５の実施形態では、配信する暗号モジュール全体を１ファイルとして暗号化またはＭＡＣを付加して送信しているが、暗号ハードウェアの処理能力の制限等により、暗号ハードウェアが大きなデータを処理できない場合がありえる。そこで、暗号モジュールを予め決められたサイズに分割して送信する。すなわち、図２７に示すように、暗号管理サーバ装置が暗号モジュールを予め定められたサイズに分割し、鍵を用いて暗号化した上で、クライアント装置に送信する。クライアント装置は、受信したぞれぞれの分割暗号モジュールを１つずつ暗号ハードウェアに復号させ、復号された暗号モジュールを結合する。これにより、暗号ハードウェアが一度に復号するデータの容量が小さくて済む。

【０１４６】

第６の実施形態では、第１の実施形態に加えて、暗号モジュールを予め決められたサイズに分割して送信する動作例を示す。すなわち、配信する暗号モジュールを共通鍵で暗号化した上で、暗号モジュールを分割する。第６の実施形態による暗号モジュール配信システムは第３の実施形態と同様の構成をしており、同様の構成・処理については説明を省略する。以下、第６の実施形態に特有の構成・処理についてのみ説明する。

図２４は、本発明による第６の実施形態の暗号管理サーバ装置の構成を示すブロック図である。暗号管理サーバ装置１２０１は、通信機能１２０２と、配布暗号モジュール選定部１２０３と、鍵生成部１２０４と、鍵共有部１２０５と、暗号モジュールＤＢ１２０６と、暗号モジュール分割部１２０７と、暗号モジュール暗号化部１２０８とを備えている。暗号管理サーバ装置１２０１は、図１３における暗号管理サーバ装置１０１に対応する。

【０１４７】

図２５は、本発明による第６の実施形態のクライアント装置の構成を示すブロック図である。クライアント装置１３０１は、通信機能１３０２と、端末情報格納部１３０４と、暗号ハードウェア管理制御部１３０５と、暗号実装部１３０６と、暗号モジュール結合部１３０７とを備えている。クライアント装置１３０１は、図１３におけるクライアント装置１０２に対応する。

暗号ハードウェア４０１は、第３の実施形態と同様の構成である。

【０１４８】

次に、図２６を参照して、第６の実施形態の動作例を説明する。

図２６は、本発明による第６の実施形態による暗号モジュール配信システムの動作例を示すシーケンス図である。

まず、クライアント装置１３０１の通信機能１３０２は、暗号管理サーバ装置１２０１に、初期暗号モジュール登録要求を送信する（ステップＳ９１）。暗号管理サーバ装置１２０１の通信機能１２０２が、初期暗号モジュール登録要求を受信すると、クライアント装置１３０１に対し、端末情報要求を送信する（ステップＳ９２）。

【０１４９】

クライアント装置１３０１の通信機能１３０２が、送信された端末情報要求を受信すると、通信機能１３０２が、端末情報格納部１３０４に格納されているクライアント装置１３０１の端末情報を暗号管理サーバ装置１２０１へ送信する（ステップＳ９３）。暗号管理サーバ装置１２０１の通信機能１２０２が、端末情報を受信すると、配布暗号モジュール選定部１２０３が、例えば、端末の識別情報ごとに暗号モジュールの識別情報との対応

表を予め記憶しておくこととして、受信した端末情報に含まれる端末識別情報に基づいてこの対応表を参照して、要求を送ってきたクライアント装置１３０１の端末識別情報に対応する暗号モジュールを、クライアント装置１３０１で利用可能な暗号モジュールとして暗号モジュールＤＢ１２０６から選定し、読み出す（ステップＳ９４）。

【０１５０】

配布暗号モジュール選定部１２０３が、暗号モジュールＤＢ１２０６から暗号モジュールを選定した場合は、暗号管理サーバ装置１２０１の通信機能１２０２が、クライアント装置１３０１に処理の続行を示す情報を送信する。一方、配布暗号モジュール選定部１２０３が、クライアント装置１３０１にて利用可能な暗号モジュールを選定できなかった場合は、通信機能１２０２からクライアント装置１３０１に処理の終了を示す情報を送信する（ステップＳ９５）。

【０１５１】

クライアント装置１３０１の通信機能１３０２が、暗号管理サーバ装置１２０１から処理の続行を示す情報を受信すると、初期登録情報の要求を暗号管理サーバ装置１２０１へ送信する（ステップＳ９６）。一方、クライアント装置１３０１の通信機能１３０２が、暗号管理サーバ装置１２０１の通信機能１２０２から処理の終了を示す情報を受信した場合、クライアント装置１３０１と暗号管理サーバ装置１２０１との間の通信を終了する。

【０１５２】

暗号管理サーバ装置１２０１の通信機能１２０２が、初期登録情報の要求を受信すると、鍵生成部１２０４が、クライアント装置１３０１に送信する暗号モジュールを暗号化するための共通鍵を生成する（ステップＳ９７）。ここで、鍵生成部１２０４は、暗号モジュールを暗号化するための共通鍵を複数個生成しても良い。そして、暗号管理サーバ装置１２０１の鍵共有部１２０５が、暗号ハードウェア４０１の鍵共有部４０４と鍵共有方式による鍵共有を行う。鍵共有方式は、例えば、Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ鍵共有などでも良い。

【０１５３】

暗号管理サーバ装置１２０１の鍵共有部１２０５が、このような鍵共有方式によりセッション鍵の生成に成功すると、クライアント装置１３０１の暗号ハードウェア管理制御部１３０５を介して、暗号ハードウェア４０１に、セキュアセッションの確立を通知する。同様に、暗号ハードウェア４０１の鍵共有部４０４は、セッション鍵の生成に成功すると、暗号管理サーバ装置１２０１に、セキュアセッションの確立を通知する（ステップＳ９８、ステップＳ９９）。ここで、暗号管理サーバ装置１２０１の鍵共有部１２０５と暗号ハードウェア４０１の鍵共有部４０４とが、生成したセッション鍵を用いて、送信側が情報を暗号化し、受信側が情報を復号化して通信を行うことを、セキュアセッションにより通信するという。

【０１５４】

暗号管理サーバ装置１２０１と暗号ハードウェア４０１との間にセキュアセッションが確立すると、暗号管理サーバ装置１２０１の鍵共有部１２０５が、鍵生成部１２０４に生成された１または複数の共通鍵をセッション鍵で暗号化して、セキュアセッションにより、クライアント装置１３０１の通信機能１３０２を介して暗号ハードウェア４０１に送信する（ステップＳ１００）。暗号ハードウェア４０１は、受信した１または複数の共通鍵を、鍵共有部によってセッション鍵を用いて復号して、鍵格納部４０３に格納する（ステップＳ１０１）。

【０１５５】

暗号ハードウェア４０１は、１または複数の共通鍵を取得すると、通信機能４０２を介して、クライアント装置１３０１にセキュアセッション切断通知を送信する（ステップＳ１０２）。暗号管理サーバ装置１２０１は、セキュアセッション切断通知を受信すると、暗号モジュール分割部１２０７が、ステップＳ９４で選定した暗号モジュールを、予め定められたサイズ以下になるように分割し、複数（例えば、Ｎ個）の分割暗号モジュールとする（ステップＳ１０３）。暗号モジュール暗号化部１２０８が、鍵生成部１２０４に生

成された共通鍵を使って分割暗号モジュールを暗号化する（ステップＳ１０４）。
【０１５６】
この際、ステップＳ９７で複数の共通鍵を生成し、暗号ハードウェア４０１に送信している場合は、分割暗号モジュール毎にそれぞれ異なる共通鍵を用いて暗号化するようにしても良い。また，暗号管理サーバ装置１２０１と暗号ハードウェア４０１で予め決められた関数を共有することにより、送信した１つの鍵からその関数を用いて複数の鍵を導出し、それら導出した複数の鍵の範囲で分割暗号モジュール毎に暗号化する鍵を変えても良い。
【０１５７】
暗号管理サーバ装置１２０１の通信機能１２０２が、暗号化された分割暗号モジュールを、クライアント装置１３０１に、１個ずつＮ回送信する（ステップＳ１０５、ステップＳ１０６）。
【０１５８】
クライアント装置１３０１の通信機能１３０２が、暗号化された分割暗号モジュールを受信すると、暗号管理サーバ装置１２０１に分割暗号モジュールを正常に受信できたことを示す暗号モジュール受信結果通知を送信する（ステップＳ１０７）。そして、暗号管理サーバ装置１２０１の通信機能１２０２が暗号モジュール受信結果通知を受信すると、暗号管理サーバ装置１２０１の通信機能１２０２が、クライアント装置１３０１に、初期暗号エンジン登録処理の終了を示す情報を送信する（ステップＳ１０８）。
【０１５９】
また、クライアント装置１３０１の通信機能１３０２が、暗号化された分割暗号モジュールを受信できなければ、クライアント装置１３０１の通信機能１３０２が、暗号管理サーバ装置１２０１に、暗号モジュールを正常に受信できなかったことを示す暗号モジュール受信結果通知を送信する。そして、暗号管理サーバ装置１２０１の通信機能１２０２が暗号モジュール受信結果通知を受信すると、暗号管理サーバ装置１２０１の通信機能１２０２は、暗号モジュールを再送信する。通信機能１２０２は、予め設定された回数を超えて暗号モジュールの再送信処理を行い、分割暗号モジュールを正常に受信できなかった場合には、エラーとして処理を終了する。
【０１６０】
クライアント装置１３０１の通信機能１３０２が、初期暗号エンジン登録処理の終了を示す情報を受信した場合、暗号ハードウェア管理制御部１３０５が、暗号ハードウェア４０１に、暗号管理サーバ装置１２０１から受信した暗号モジュールを送信する（ステップＳ１０９）。
そして、暗号ハードウェア４０１の通信機能４０２が、暗号化された分割暗号モジュールを受信すると、暗号エンジン復号部４０５が、鍵格納部４０３に記憶された共通鍵を読み出して、この共通鍵を用いて分割暗号モジュールを復号し（ステップＳ１１０）、復号された分割暗号モジュールを通信機能４０２によりクライアント装置１３０１に送信する（ステップＳ１１１）。
【０１６１】
分割暗号モジュールの送受信は分割数と同じ回数（Ｎ回）行う。クライアント装置１３０１の暗号ハードウェア管理制御部１３０５が、分割暗号モジュールの分割数と同じ回数だけ分割暗号モジュールを受信すると、暗号モジュール結合部１３０７が、受信した全ての分割暗号モジュールを結合する（ステップＳ１１２）。クライアント装置１３０１の暗号ハードウェア管理制御部１３０５が、結合された暗号モジュールを受信すると、暗号モジュールを暗号実装部１３０６に実装して、利用可能状態にさせる。暗号ハードウェア管理制御部１３０５は、暗号モジュールＤＢ１３０３に、暗号実装部１３０６に格納した暗号モジュールを格納する（ステップＳ１１３）。
【０１６２】
＜第７の実施形態＞
次に、上述した暗号モジュール配信システムの鍵の配送について、他の実施形態につい

て説明する。第６の実施形態では、第３の実施形態に加えて暗号モジュールを予め定められたサイズに分割して送信する動作例を示したが、第４の実施形態のような、ＭＡＣを付加した暗号モジュールを配信する場合にも、暗号モジュールを予め定められたサイズに分割して送信するようにしても良い。

【０１６３】

第７の実施形態では、配信する暗号モジュールを分割した後、それぞれの分割暗号モジュールに対してＭＡＣを付加して配信する。第７の実施形態による暗号モジュール配信システムは第４の実施形態と同様の構成をしており、同様の構成・処理については説明を省略する。以下、第７の実施形態に特有の構成・処理についてのみ説明する。

【０１６４】

図２８は、本発明による第７の実施形態の暗号管理サーバ装置の構成を示すブロック図である。暗号管理サーバ装置１４０１は、通信機能１４０２と、配布暗号モジュール選定部１４０３と、鍵生成部１４０４と、鍵共有部１４０５と、暗号モジュールＤＢ１４０６と、暗号モジュール分割部１４０７と、ＭＡＣ生成部１４０８とを備えている。暗号管理サーバ装置１４０１は、図１３における暗号管理サーバ装置１０１に対応する。

【０１６５】

図２９は、本発明による第７の実施形態のクライアント装置の構成を示すブロック図である。クライアント装置１５０１は、通信機能１５０２と、端末情報格納部１５０４と、暗号ハードウェア管理制御部１５０５と、暗号実装部１５０６と、暗号モジュール結合部１５０７とを備えている。クライアント装置１５０１は、図１３におけるクライアント装置１０２に対応する。

暗号ハードウェアは、第４の実施形態と同様の構成である暗号ハードウェア７０１とする。暗号ハードウェア７０１は、図１３における暗号ハードウェア１０３に対応する。

【０１６６】

次に、図３０を参照して、第７の実施形態の動作例を説明する。

図３０は、本発明による第７の実施形態による暗号モジュール配信システムの動作例を示すシーケンス図である。

まず、クライアント装置１５０１の通信機能１５０２は、暗号管理サーバ装置１４０１に、初期暗号モジュール登録要求を送信する（ステップＳ１２１）。暗号管理サーバ装置１４０１の通信機能１４０２が、初期暗号モジュール登録要求を受信すると、クライアント装置１５０１に対し、端末情報要求を送信する（ステップＳ１２２）。

【０１６７】

クライアント装置１５０１の通信機能１５０２が、送信された端末情報要求を受信すると、通信機能１５０２が、端末情報格納部１５０４に格納されているクライアント装置１５０１の端末情報を暗号管理サーバ装置１４０１へ送信する（ステップＳ１２３）。暗号管理サーバ装置１４０１の通信機能１４０２が、端末情報を受信すると、配布暗号モジュール選定部１４０３が、例えば、端末の識別情報ごとに暗号モジュールの識別情報との対応表を予め記憶しておくこととして、受信した端末情報に含まれる端末識別情報に基づいてこの対応表を参照して、要求を送ってきたクライアント装置１５０１の端末識別情報に対応する暗号モジュールを、クライアント装置１５０１で利用可能な暗号モジュールとして暗号モジュールＤＢ１４０６から選定し、読み出す（ステップＳ１２４）。

【０１６８】

配布暗号モジュール選定部１４０３が、暗号モジュールＤＢ１４０６から暗号モジュールを選定した場合は、暗号管理サーバ装置１４０１の通信機能１４０２が、クライアント装置１５０１に処理の続行を示す情報を送信する。一方、配布暗号モジュール選定部１４０３が、クライアント装置１５０１にて利用可能な暗号モジュールを選定できなかった場合は、通信機能１４０２からクライアント装置１５０１に処理の終了を示す情報を送信する（ステップＳ１２５）。

【０１６９】

クライアント装置１５０１の通信機能１５０２が、暗号管理サーバ装置１４０１から処

理の続行を示す情報を受信すると、初期登録情報の要求を暗号管理サーバ装置１４０１へ送信する（ステップＳ１２６）。一方、クライアント装置１５０１の通信機能１５０２が、暗号管理サーバ装置１４０１の通信機能１４０２から処理の終了を示す情報を受信した場合、クライアント装置１５０１と暗号管理サーバ装置１４０１との間の通信を終了する。

【０１７０】

暗号管理サーバ装置１４０１の通信機能１４０２が、初期登録情報の要求を受信すると、鍵生成部１４０４が、クライアント装置１５０１に送信する暗号モジュールにＭＡＣを付加するためのＭＡＣ鍵を生成する（ステップＳ１２７）。ここで、鍵生成部１４０４は、暗号モジュールを暗号化するためのＭＡＣ鍵を複数個生成しても良い。そして、暗号管理サーバ装置１４０１の鍵共有部１４０５が、暗号ハードウェア７０１の鍵共有部７０４と鍵共有方式による鍵共有を行う。鍵共有方式は、例えば、Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ鍵共有などでも良い。

【０１７１】

暗号管理サーバ装置１４０１の鍵共有部１４０５が、このような鍵共有方式によりセッション鍵の生成に成功すると、クライアント装置１５０１の暗号ハードウェア管理制御部１５０５を介して、暗号ハードウェア７０１に、セキュアセッションの確立を通知する。同様に、暗号ハードウェア７０１の鍵共有部７０４は、セッション鍵の生成に成功すると、暗号管理サーバ装置１４０１に、セキュアセッションの確立を通知する（ステップＳ１２８、ステップＳ１２９）。ここで、暗号管理サーバ装置１４０１の鍵共有部１４０５と暗号ハードウェア７０１の鍵共有部７０４とが、生成したセッション鍵を用いて、送信側が情報を暗号化し、受信側が情報を復号化して通信を行うことを、セキュアセッションにより通信するという。

【０１７２】

暗号管理サーバ装置１４０１と暗号ハードウェア７０１との間にセキュアセッションが確立すると、暗号管理サーバ装置１４０１の鍵共有部１４０５が、鍵生成部１４０４に生成された１または複数のＭＡＣ鍵をセッション鍵で暗号化して、セキュアセッションにより、クライアント装置１５０１の通信機能１５０２を介して暗号ハードウェア７０１に送信する（ステップＳ１３０）。暗号ハードウェア７０１は、受信した１または複数のＭＡＣ鍵を、鍵共有部によってセッション鍵を用いて復号して、鍵格納部７０３に格納する（ステップＳ１３１）。

【０１７３】

暗号ハードウェア７０１は、１または複数のＭＡＣ鍵を取得すると、通信機能７０２を介して、クライアント装置１５０１にセキュアセッション切断通知を送信する（ステップＳ１３２）。暗号管理サーバ装置１４０１は、セキュアセッション切断通知を受信すると、暗号モジュール分割部１４０７が、ステップＳ１２４で選定した暗号モジュールを、予め定められたサイズ以下になるように分割し、複数（例えば、Ｎ個）の分割暗号モジュールとする（ステップＳ１３３）。ＭＡＣ生成部１４０８が、鍵生成部１４０４に生成されたＭＡＣ鍵を使って分割暗号モジュールのＭＡＣを生成する（ステップＳ１３４）。

【０１７４】

この際、ステップＳ１２７で複数のＭＡＣ鍵を生成し、暗号ハードウェア７０１に送信している場合は、分割暗号モジュール毎にそれぞれ異なるＭＡＣ鍵を用いてＭＡＣ生成するようにしても良い。また，暗号管理サーバ装置１４０１と暗号ハードウェア７０１で予め決められた関数を共有することにより、送信した１つの鍵からその関数を用いて複数の鍵を導出し、それら導出した複数の鍵の範囲で分割暗号モジュール毎にＭＡＣ生成する鍵を変えても良い。

【０１７５】

暗号管理サーバ装置１４０１の通信機能１４０２が、ＭＡＣが付加された分割暗号モジュールを、クライアント装置１５０１に、１個ずつＮ回送信する（ステップＳ１３５、ステップＳ１３６）。

【０１７６】
クライアント装置１５０１の通信機能１５０２が、ＭＡＣが付加された分割暗号モジュールを受信すると、暗号管理サーバ装置１４０１に分割暗号モジュールを正常に受信できたことを示す暗号モジュール受信結果通知を送信する（ステップＳ１３７）。そして、暗号管理サーバ装置１４０１の通信機能１４０２が暗号モジュール受信結果通知を受信すると、暗号管理サーバ装置１４０１の通信機能１４０２が、クライアント装置１５０１に、初期暗号エンジン登録処理の終了を示す情報を送信する（ステップＳ１３８）。
【０１７７】
また、クライアント装置１５０１の通信機能１５０２が、ＭＡＣが付加された分割暗号モジュールを受信できなければ、クライアント装置１５０１の通信機能１５０２が、暗号管理サーバ装置１４０１に、暗号モジュールを正常に受信できなかったことを示す暗号モジュール受信結果通知を送信する。そして、暗号管理サーバ装置１４０１の通信機能１４０２が暗号モジュール受信結果通知を受信すると、暗号管理サーバ装置１４０１の通信機能１４０２は、暗号モジュールを再送信する。通信機能１４０２は、予め設定された回数を超えて暗号モジュールの再送信処理を行い、分割暗号モジュールを正常に受信できなかった場合には、エラーとして処理を終了する。
【０１７８】
クライアント装置１５０１の通信機能１５０２が、初期暗号エンジン登録処理の終了を示す情報を受信した場合、暗号ハードウェア管理制御部１５０５が、暗号ハードウェア７０１に、暗号管理サーバ装置１４０１から受信したＭＡＣが付加された分割暗号モジュールを送信する（ステップＳ１３９）。
そして、暗号ハードウェア７０１の通信機能７０２が、ＭＡＣが付加された分割暗号モジュールを受信すると、暗号エンジン復号部４０５が、鍵格納部７０３に記憶された共通鍵を読み出して、このＭＡＣ鍵を用いてＭＡＣ検証を行い、（ステップＳ１４０）、ＭＡＣが正当であるか否かを示す検証結果を通信機能７０２によりクライアント装置１５０１に送信する（ステップＳ１４１）。
【０１７９】
分割暗号モジュールの送受信（ステップＳ１３９～ステップＳ１４１の処理）は分割数と同じ回数（Ｎ回）行う。クライアント装置１５０１の暗号ハードウェア管理制御部１５０５が、分割暗号モジュールの分割数と同じ回数だけ分割暗号モジュールを受信すると、暗号モジュール結合部１５０７が、受信した全ての分割暗号モジュールを結合する（ステップＳ１４２）。クライアント装置１５０１の暗号ハードウェア管理制御部１５０５が、結合された暗号モジュールを受信すると、暗号モジュールを暗号実装部１５０６に実装して、利用可能状態にさせる。暗号ハードウェア管理制御部１５０５は、暗号モジュールＤＢ１５０３に、暗号実装部１５０６に格納した暗号モジュールを格納する（ステップＳ１４３）。
【０１８０】
＜第８の実施形態＞
次に、上述した暗号モジュール配信システムの鍵の配送について、他の実施形態について説明する。第７の実施形態では、第４の実施形態に加えて暗号モジュールを予め定められたサイズに分割して送信する動作例を示したが、第５の実施形態のような、暗号化された上にＭＡＣを付加した暗号モジュールを配信する場合にも、暗号モジュールを予め定められたサイズに分割して送信するようにしても良い。
【０１８１】
第８の実施形態では、配信する暗号モジュールを分割した後、それぞれの分割暗号モジュールを暗号化し、さらにＭＡＣを付加して配信する。第８の実施形態による暗号モジュール配信システムは第５の実施形態と同様の構成をしており、同様の構成・処理については説明を省略する。以下、第８の実施形態に特有の構成・処理についてのみ説明する。
【０１８２】
図３１は、本発明による第８の実施形態の暗号管理サーバ装置の構成を示すブロック図

である。暗号管理サーバ装置１７０１は、通信機能１７０２と、配布暗号モジュール選定部１７０３と、鍵生成部１７０４と、鍵共有部１７０５と、暗号モジュールＤＢ１７０６と、暗号モジュール分割部１７０７と、ＭＡＣ生成部１７０８と、暗号モジュール暗号化部１７０９とを備えている。暗号管理サーバ装置１７０１は、図１３における暗号管理サーバ装置１０１に対応する。

【０１８３】

図３２は、本発明による第８の実施形態のクライアント装置の構成を示すブロック図である。クライアント装置１８０１は、通信機能１８０２と、暗号モジュールＤＢ１８０３端末情報格納部１８０４と、暗号ハードウェア管理制御部１８０５と、暗号実装部１８０６と、暗号モジュール結合部１８０７とを備えている。クライアント装置１８０１は、図１３におけるクライアント装置１０２に対応する。

暗号ハードウェアは、第５の実施形態と同様の構成である暗号ハードウェア１００１とする。暗号ハードウェア１００１は、図１３における暗号ハードウェア１０３に対応する。

【０１８４】

次に、図３３を参照して、第８の実施形態の動作例を説明する。

図３３は、本発明による第８の実施形態による暗号モジュール配信システムの動作例を示すシーケンス図である。

まず、クライアント装置１８０１の通信機能１８０２は、暗号管理サーバ装置１７０１に、初期暗号モジュール登録要求を送信する（ステップＳ１５１）。暗号管理サーバ装置１７０１の通信機能１７０２が、初期暗号モジュール登録要求を受信すると、クライアント装置１８０１に対し、端末情報要求を送信する（ステップＳ１５２）。

【０１８５】

クライアント装置１８０１の通信機能１８０２が、送信された端末情報要求を受信すると、通信機能１８０２が、端末情報格納部１８０４に格納されているクライアント装置１８０１の端末情報を暗号管理サーバ装置１７０１へ送信する（ステップＳ１５３）。暗号管理サーバ装置１７０１の通信機能１７０２が、端末情報を受信すると、配布暗号モジュール選定部１７０３が、例えば、端末の識別情報ごとに暗号モジュールの識別情報との対応表を予め記憶しておくこととして、受信した端末情報に含まれる端末識別情報に基づいてこの対応表を参照して、要求を送ってきたクライアント装置１８０１の端末識別情報に対応する暗号モジュールを、クライアント装置１８０１で利用可能な暗号モジュールとして暗号モジュールＤＢ１７０６から選定し、読み出す（ステップＳ１５４）。

【０１８６】

配布暗号モジュール選定部１７０３が、暗号モジュールＤＢ１７０６から暗号モジュールを選定した場合は、暗号管理サーバ装置１７０１の通信機能１７０２が、クライアント装置１８０１に処理の続行を示す情報を送信する。一方、配布暗号モジュール選定部１７０３が、クライアント装置１８０１にて利用可能な暗号モジュールを選定できなかった場合は、通信機能１７０２からクライアント装置１８０１に処理の終了を示す情報を送信する（ステップＳ１５５）。

【０１８７】

クライアント装置１８０１の通信機能１８０２が、暗号管理サーバ装置１７０１から処理の続行を示す情報を受信すると、初期登録情報の要求を暗号管理サーバ装置１７０１へ送信する（ステップＳ１５６）。一方、クライアント装置１８０１の通信機能１８０２が、暗号管理サーバ装置１７０１の通信機能１７０２から処理の終了を示す情報を受信した場合、クライアント装置１８０１と暗号管理サーバ装置１７０１との間の通信を終了する。

【０１８８】

暗号管理サーバ装置１７０１の通信機能１７０２が、初期登録情報の要求を受信すると、鍵生成部１７０４が、クライアント装置１８０１に送信する暗号モジュールを暗号化するための共通鍵と、暗号モジュールにＭＡＣを付加するためのＭＡＣ鍵とを生成する（ス

テップＳ１５７）。ここで、鍵生成部１７０４は、共通鍵とＭＡＣ鍵とをそれぞれ複数個生成しても良い。そして、暗号管理サーバ装置１７０１の鍵共有部１７０５が、暗号ハードウェア１００１の鍵共有部１００４と鍵共有方式による鍵共有を行う。鍵共有方式は、例えば、Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ鍵共有などでも良い。

【０１８９】

暗号管理サーバ装置１７０１の鍵共有部１７０５が、このような鍵共有方式によりセッション鍵の生成に成功すると、クライアント装置１８０１の暗号ハードウェア管理制御部１８０５を介して、暗号ハードウェア１００１に、セキュアセッションの確立を通知する。同様に、暗号ハードウェア１００１の鍵共有部１００４は、セッション鍵の生成に成功すると、暗号管理サーバ装置１７０１に、セキュアセッションの確立を通知する（ステップＳ１５８、ステップＳ１５９）。ここで、暗号管理サーバ装置１７０１の鍵共有部１７０５と暗号ハードウェア１００１の鍵共有部１００４とが、生成したセッション鍵を用いて、送信側が情報を暗号化し、受信側が情報を復号化して通信を行うことを、セキュアセッションにより通信するという。

【０１９０】

暗号管理サーバ装置１７０１と暗号ハードウェア１００１との間にセキュアセッションが確立すると、暗号管理サーバ装置１７０１の鍵共有部１７０５が、鍵生成部１７０４に生成された１または複数の共通鍵およびＭＡＣ鍵をセッション鍵で暗号化して、セキュアセッションにより、クライアント装置１８０１の通信機能１８０２を介して暗号ハードウェア１００１に送信する（ステップＳ１６０）。暗号ハードウェア１００１は、受信した１または複数の共通鍵およびＭＡＣ鍵を、鍵共有部によってセッション鍵を用いて復号して、鍵格納部１００３に格納する（ステップＳ１６１）。

【０１９１】

暗号ハードウェア１００１は、１または複数の共通鍵およびＭＡＣ鍵を取得すると、通信機能１００２を介して、クライアント装置１８０１にセキュアセッション切断通知を送信する（ステップＳ１６２）。暗号管理サーバ装置１７０１は、セキュアセッション切断通知を受信すると、暗号モジュール分割部１７０７が、ステップＳ１２４で選定した暗号モジュールを、予め定められたサイズ以下になるように分割し、複数（例えば、Ｎ個）の分割暗号モジュールとする（ステップＳ１６３）。暗号モジュール暗号化部１７０９が、鍵生成部１７０４に生成された共通鍵に基づいて、分割暗号モジュールを暗号化する。さらに、ＭＡＣ生成部１７０８が、鍵生成部１７０４に生成されたＭＡＣ鍵を使って分割暗号モジュールのＭＡＣを生成する（ステップＳ１６４）。ここで、暗号モジュールのＭＡＣを生成した後に、暗号モジュールとＭＡＣとを合わせて鍵生成部１７０４に生成された共通鍵に基づいて暗号化しても良い。

【０１９２】

この際、ステップＳ１５７で複数の共通鍵を生成し、暗号ハードウェア１００１に送信している場合は、分割暗号モジュール毎にそれぞれ異なる共通鍵を用いて暗号化するようにしても良い。また，暗号管理サーバ装置１７０１と暗号ハードウェア１００１で予め決められた関数を共有することにより、送信した１つの鍵からその関数を用いて複数の鍵を導出し、それら導出した複数の鍵の範囲で分割暗号モジュール毎に暗号化する鍵を変えても良い。さらに、ステップＳ１５７で複数のＭＡＣ鍵を生成し、暗号ハードウェア１００１に送信している場合は、分割暗号モジュール毎にそれぞれ異なるＭＡＣ鍵を用いてＭＡＣ生成するようにしても良い。また，暗号管理サーバ装置１７０１と暗号ハードウェア１００１で予め決められた関数を共有することにより、送信した１つの鍵からその関数を用いて複数の鍵を導出し、それら導出した複数の鍵の範囲で分割暗号モジュール毎にＭＡＣ生成する鍵を変えても良い。

【０１９３】

暗号管理サーバ装置１７０１の通信機能１７０２が、暗号化かつＭＡＣが付加された分割暗号モジュールを、クライアント装置１８０１に、１個ずつＮ回送信する（ステップＳ１６５、ステップＳ１６６）。

【０１９４】
クライアント装置１８０１の通信機能１８０２が、暗号化かつＭＡＣが付加された分割暗号モジュールを受信すると、暗号管理サーバ装置１７０１に暗号化かつ分割暗号モジュールを正常に受信できたことを示す暗号モジュール受信結果通知を送信する（ステップＳ１６７）。そして、暗号管理サーバ装置１７０１の通信機能１７０２が暗号モジュール受信結果通知を受信すると、暗号管理サーバ装置１７０１の通信機能１７０２が、クライアント装置１８０１に、初期暗号エンジン登録処理の終了を示す情報を送信する（ステップＳ１６８）。

【０１９５】
また、クライアント装置１８０１の通信機能１８０２が、暗号化かつＭＡＣが付加された分割暗号モジュールを受信できなければ、クライアント装置１８０１の通信機能１８０２が、暗号管理サーバ装置１７０１に、暗号モジュールを正常に受信できなかったことを示す暗号モジュール受信結果通知を送信する。そして、暗号管理サーバ装置１７０１の通信機能１７０２が暗号モジュール受信結果通知を受信すると、暗号管理サーバ装置１７０１の通信機能１７０２は、暗号モジュールを再送信する。通信機能１７０２は、予め設定された回数を超えて暗号モジュールの再送信処理を行い、分割暗号モジュールを正常に受信できなかった場合には、エラーとして処理を終了する。

【０１９６】
クライアント装置１８０１の通信機能１８０２が、初期暗号エンジン登録処理の終了を示す情報を受信した場合、暗号ハードウェア管理制御部１８０５が、暗号ハードウェア１００１に、暗号管理サーバ装置１７０１から受信した暗号化かつＭＡＣが付加された分割暗号モジュールを送信する（ステップＳ１６９）。
そして、暗号ハードウェア１００１の通信機能１００２が、暗号化かつＭＡＣが付加された分割暗号モジュールを受信すると、暗号モジュール復号部１００５が、鍵格納部１００３に記憶された共通鍵を読み出して、読み出した共通鍵に基づいて分割暗号モジュールを復号する。また、ＭＡＣ検証部１００６が、鍵格納部１００３に記憶されたＭＡＣ鍵を読み出して、このＭＡＣ鍵を用いてＭＡＣ検証を行う（ステップＳ１７０）。通信機能１００２が、復号された分割暗号モジュールと、ＭＡＣが正当であるか否かを示す検証結果とをクライアント装置１８０１に送信する（ステップＳ１７１）。

【０１９７】
分割暗号モジュールの送受信（ステップＳ１６９～ステップＳ１７１の処理）は分割数と同じ回数（Ｎ回）行う。クライアント装置１８０１の暗号ハードウェア管理制御部１８０５が、分割暗号モジュールの分割数と同じ回数だけ分割暗号モジュールを受信すると、暗号モジュール結合部１８０７が、受信した全ての分割暗号モジュールを結合する（ステップＳ１７２）。クライアント装置１８０１の暗号ハードウェア管理制御部１８０５が、結合された暗号モジュールを受信すると、暗号モジュールを暗号実装部１８０６に実装して、利用可能状態にさせる。暗号ハードウェア管理制御部１８０５は、暗号モジュールＤＢ１８０３に、暗号実装部１８０６に格納した暗号モジュールを格納する（ステップＳ１７３）。

【０１９８】
以上説明したように、本発明によれば、サーバが端末装置に暗号アルゴリズム(プログラム)を送信する場合、端末装置は暗号処理を行うハードウェアを使って、送信されたデータ(プログラム)の正当性を検証し、正しい場合に端末装置に組み込むことで、送信されたアルゴリズム(プログラム)が正当なものであるか否かを検証する。また、一旦、サーバから暗号アルゴリズム(プログラム)が送信され、端末装置に組み込んだ場合は、暗号処理を行うハードウェアは使わずに暗号アルゴリズム(プログラム)を受信し、組み込む。この場合も送られたデータ(プログラム)の正当性を検証可能である。

【０１９９】
すなわち、クライアント装置側で暗号アルゴリズム(プログラム)を全く保持していない場合に、暗号処理を行うハードウェアを補助的に使ってサーバからクライアント装置に暗

号アルゴリズムを送信することで、クライアント装置で新規暗号アルゴリズムを利用可能な状態にすることができる。

【０２００】

なお、本発明における処理部の機能を実現するためのプログラムをコンピュータ読み取り可能な記録媒体に記録して、この記録媒体に記録されたプログラムをコンピュータシステムに読み込ませ、実行することにより暗号モジュールの配布を行ってもよい。なお、ここでいう「コンピュータシステム」とは、ＯＳや周辺機器等のハードウェアを含むものとする。また、「コンピュータシステム」は、ホームページ提供環境（あるいは表示環境）を備えたＷＷＷシステムも含むものとする。また、「コンピュータ読み取り可能な記録媒体」とは、フレキシブルディスク、光磁気ディスク、ＲＯＭ、ＣＤ－ＲＯＭ等の可搬媒体、コンピュータシステムに内蔵されるハードディスク等の記憶装置のことをいう。さらに「コンピュータ読み取り可能な記録媒体」とは、インターネット等のネットワークや電話回線等の通信回線を介してプログラムが送信された場合のサーバやクライアントとなるコンピュータシステム内部の揮発性メモリ（ＲＡＭ）のように、一定時間プログラムを保持しているものも含むものとする。

【０２０１】

また、上記プログラムは、このプログラムを記憶装置等に格納したコンピュータシステムから、伝送媒体を介して、あるいは、伝送媒体中の伝送波により他のコンピュータシステムに伝送されてもよい。ここで、プログラムを伝送する「伝送媒体」は、インターネット等のネットワーク（通信網）や電話回線等の通信回線（通信線）のように情報を伝送する機能を有する媒体のことをいう。また、上記プログラムは、前述した機能の一部を実現するためのものであっても良い。さらに、前述した機能をコンピュータシステムにすでに記録されているプログラムとの組み合わせで実現できるもの、いわゆる差分ファイル（差分プログラム）であっても良い。

【図面の簡単な説明】

【０２０２】

【図１】本発明の第１の実施形態による暗号モジュール配信システムの構成を示すブロック図である。

【図２】本発明の第１の実施形態による暗号クライアント装置の構成を示すブロック図である。

【図３】本発明の第１の実施形態による暗号管理サーバ装置の構成を示すブロック図である。

【図４】本発明の第２の実施形態による暗号モジュール配信システムの構成を示すブロック図である。

【図５】本発明の第２の実施形態による暗号クライアント装置の構成を示すブロック図である。

【図６】本発明の第２の実施形態による選定ＤＢのデータ構成例を示す図である。

【図７】本発明の第２の実施形態による暗号モジュールリンクＤＢのデータ構成例を示す図である。

【図８】本発明の第２の実施形態による暗号モジュールＤＢのデータ構成例を示す図である。

【図９】本発明の第２の実施形態による鍵情報ＤＢのデータ構成例を示す図である。

【図１０】本発明の第２の実施形態による暗号処理ＤＢのデータ構成例を示す図である。

【図１１】本発明の第２の実施形態によるデータベースの論理構成を示す図である。

【図１２】本発明の第２の実施形態による暗号管理サーバ装置の構成を示すブロック図である。

【図１３】本発明の第３の実施形態による暗号モジュール配信システムの構成を示す図である。

【図１４】本発明の第３の実施形態による暗号管理サーバ装置の構成を示すブロック図である。

【図１５】本発明の第３の実施形態によるクライアント装置の構成を示すブロック図である。
【図１６】本発明の第３の実施形態による暗号ハードウェアの構成を示すブロック図である。
【図１７】本発明の第３の実施形態による暗号モジュール配信システムの動作例を示すシーケンス図である。
【図１８】本発明の第４の実施形態による暗号管理サーバ装置の構成を示すブロック図である。
【図１９】本発明の第４の実施形態による暗号ハードウェアの構成を示すブロック図である。
【図２０】本発明の第４の実施形態による暗号モジュール配信システムの動作例を示すシーケンス図である。
【図２１】本発明の第５の実施形態による暗号管理サーバ装置の構成を示すブロック図である。
【図２２】本発明の第５の実施形態による暗号ハードウェアの構成を示すブロック図である。
【図２３】本発明の第５の実施形態による暗号モジュール配信システムの動作例を示すシーケンス図である。
【図２４】本発明の第６の実施形態による暗号管理サーバ装置の構成を示すブロック図である。
【図２５】本発明の第６の実施形態によるクライアント装置の構成を示すブロック図である。
【図２６】本発明の第６の実施形態による暗号モジュール配信システムの動作例を示すシーケンス図である。
【図２７】本発明の第６の実施形態による暗号モジュール配信システムの動作例を示す概念図である。
【図２８】本発明の第７の実施形態による暗号管理サーバ装置の構成を示すブロック図である。
【図２９】本発明の第７の実施形態によるクライアント装置の構成を示すブロック図である。
【図３０】本発明の第７の実施形態による暗号モジュール配信システムの動作例を示すシーケンス図である。
【図３１】本発明の第８の実施形態による暗号管理サーバ装置の構成を示すブロック図である。
【図３２】本発明の第８の実施形態によるクライアント装置の構成を示すブロック図である。
【図３３】本発明の第８の実施形態による暗号モジュール配信システムの動作例を示すシーケンス図である。
【図３４】本発明の実施形態による端末の識別情報と暗号モジュールの識別情報との対応表を示す図である。
【符号の説明】
【０２０３】
１０１　暗号管理サーバ装置
１０２　クライアント装置
１０３　暗号ハードウェア
１５０　暗号クライアント装置
１５１　上位システム部
１５２　暗号制御マネージャ部
１５３　暗号実装部
１５４　暗号実装Ｉ／Ｆ部

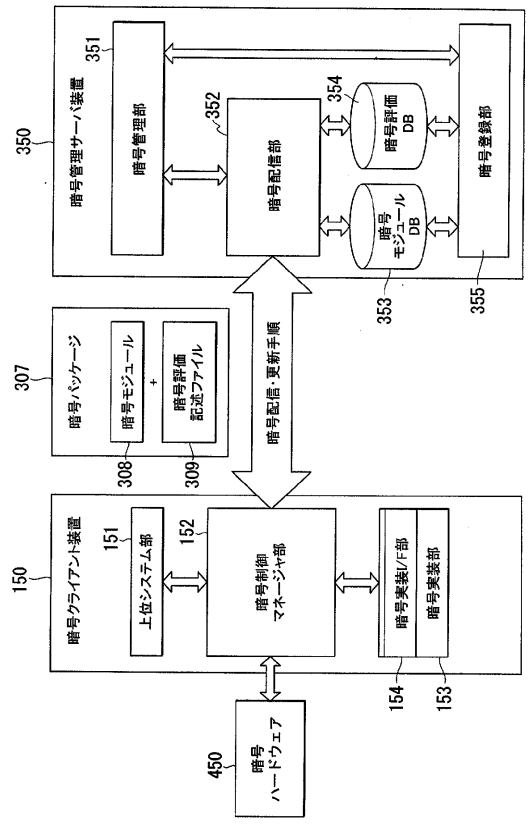
１５５　通信機能
１５６　暗号処理制御部
１５７　暗号処理情報ＤＢ
１５８　暗号モジュール選定ポリシ
１５９　暗号モジュール選定部
１６０　ハードウェアプロファイル
１６１　アクセス制御ポリシ
１６２　鍵情報管理部
１６３　暗号評価ＤＢ
１６４　暗号モジュールＤＢ
１６５　鍵情報ＤＢ
１６６　暗号管理部
１６７　暗号制御マネージャポリシ
１６８　アルゴリズムネゴシエーション部
１６９　セキュア通信管理部
１７０　暗号ハードウェア管理制御部
２０１　暗号管理サーバ装置
２０２　通信機能
２０３　配布暗号モジュール選定部
２０４　鍵生成部
２０５　鍵共有部
２０６　暗号モジュールＤＢ
２０７　暗号モジュール暗号化部
３０１　クライアント装置
３０２　通信機能
３０３　暗号モジュールＤＢ
３０４　端末情報格納部
３０５　暗号ハードウェア管理制御部
３０６　暗号実装部
３０７　暗号パッケージ
３０８　暗号モジュール
３０９　暗号評価記述ファイル
３５０　暗号管理サーバ装置
３５１　暗号管理部
３５２　暗号配信部
３５３　暗号モジュールＤＢ
３５４　暗号評価ＤＢ
３５５　暗号登録部
３５６　通信機能
３５７　暗号パッケージ登録部
３５８　複合型記述生成部
３５９　暗号パッケージ配信制御部
３６０　配布暗号モジュール選定部
３７０　暗号パッケージ配布構成部
３７１　配布ポリシ
４０１　暗号ハードウェア
４０２　通信機能
４０３　鍵格納部
４０４　鍵共有部
４０５　暗号モジュール復号部

４５０　暗号ハードウェア部
６０１　暗号管理サーバ装置
６０２　通信機能
６０３　配布暗号モジュール選定部
６０４　鍵生成部
６０５　鍵共有部
６０６　暗号モジュールＤＢ
６０７　ＭＡＣ生成部
７０１　暗号ハードウェア
７０２　通信機能
７０３　鍵格納部
７０４　鍵共有部
７０５　ＭＡＣ検証部
９０１　暗号管理サーバ装置
９０２　通信機能
９０３　配布暗号モジュール選定部
９０４　鍵生成部
９０５　鍵共有部
９０６　暗号モジュールＤＢ
９０７　ＭＡＣ生成部
９０８　暗号モジュール暗号化部
１００１　暗号ハードウェア
１００２　通信機能
１００３　鍵格納部
１００４　鍵共有部
１００５　暗号モジュール復号部
１００６　ＭＡＣ検証部
１１５１　上位システム部
１１５２　暗号制御マネージャ部
１１５３　暗号実装部
１１５５　通信機能
１１５６　暗号処理制御部
１１５８　選定ポリシ
１１６０　ハードウェアプロファイル
１１６２　鍵管理部
１１６５　鍵情報ＤＢ
１１６６　暗号パッケージ管理部
１１７０　暗号ハードウェア管理制御部
１２０１　暗号管理サーバ装置
１２０２　通信機能
１２０３　配布暗号モジュール選定部
１２０４　鍵生成部
１２０５　鍵共有部
１２０６　暗号モジュールＤＢ
１２０７　暗号モジュール分割部
１２０８　暗号モジュール暗号化部
１３０１　クライアント装置
１３０２　通信機能
１３０３　暗号モジュールＤＢ
１３０４　端末情報格納部

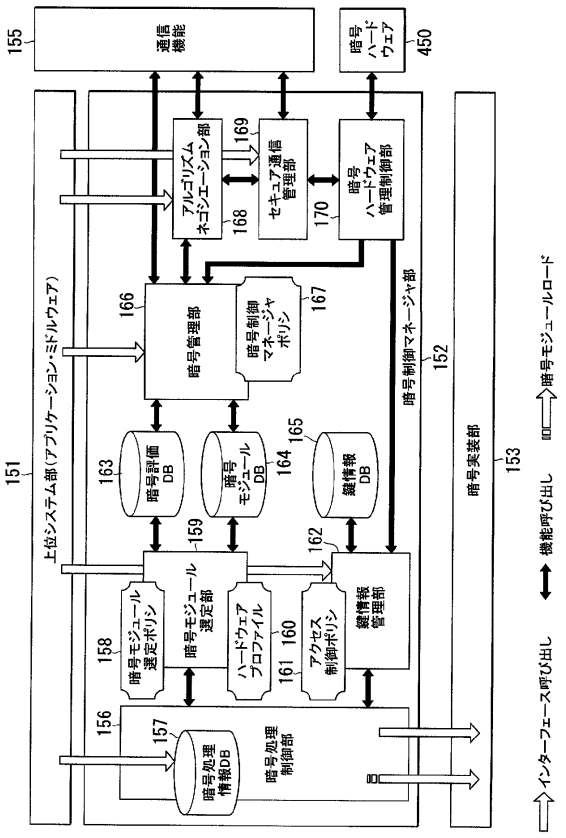
１３０５　暗号ハードウェア管理制御部
１３０６　暗号実装部
１３０７　暗号モジュール結合部
１３５０　暗号管理サーバ装置
１３５１　暗号パッケージ管理部
１３５２　暗号管理サーバ制御部
１３５３　暗号モジュールＤＢ
１３５４　暗号評価ＤＢ
１３５５　暗号パッケージ記憶部
１３５６　通信機能
１３５９　暗号パッケージ官制部
１３７０　暗号パッケージ配布構成部
１３７１　配布ポリシ
１３７２　ドメイン情報
１３７３　配布暗号パッケージ選定部
１３８０　サーバ上位システム部
１３９０　サーバ暗号制御マネージャ部
１４０１　暗号管理サーバ装置
１４０２　通信機能
１４０３　配布暗号モジュール選定部
１４０４　鍵生成部
１４０５　鍵共有部
１４０６　暗号モジュールＤＢ
１４０７　暗号モジュール分割部
１４０８　ＭＡＣ生成部
１４５０　暗号ハードウェア
１５０１　クライアント装置
１５０２　通信機能
１５０３　暗号モジュールＤＢ
１５０４　端末情報格納部
１５０５　暗号ハードウェア管理制御部
１５０６　暗号実装部
１５０７　暗号モジュール結合部
１６００　暗号情報記憶部
１６０１　選定ＤＢ
１６０２　暗号モジュールリンクＤＢ
１６０３　暗号モジュールＤＢ
１６０４　暗号処理ＤＢ
１７０１　暗号管理サーバ装置
１７０２　通信機能
１７０３　配布暗号モジュール選定部
１７０４　鍵生成部
１７０５　鍵共有部
１７０６　暗号モジュールＤＢ
１７０７　暗号モジュール分割部
１７０８　ＭＡＣ生成部
１７０９　暗号モジュール暗号化部
１８０１　クライアント装置
１８０２　通信機能
１８０３　暗号モジュールＤＢ

１８０４　端末情報格納部
１８０５　暗号ハードウェア管理制御部
１８０６　暗号実装部
１８０７　暗号モジュール結合部

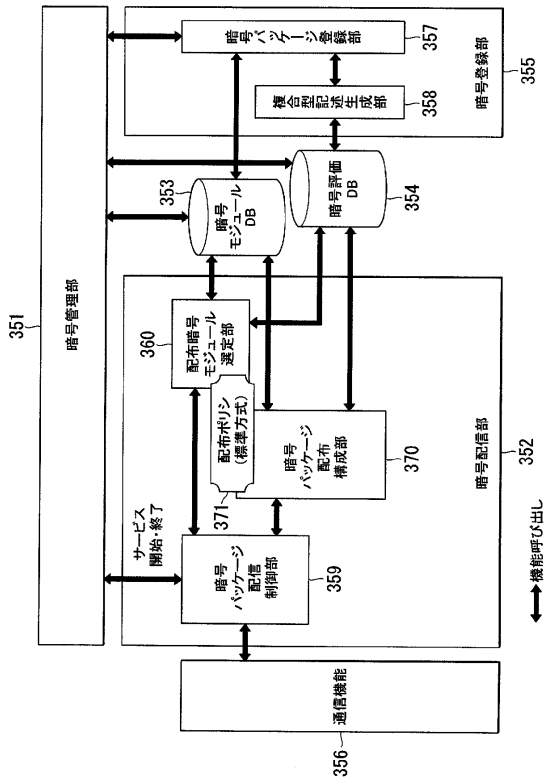
【図１】



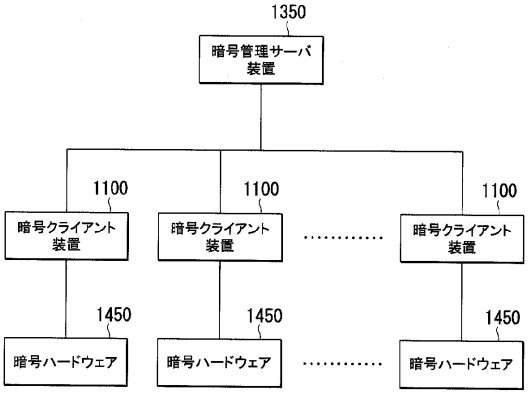
【図２】



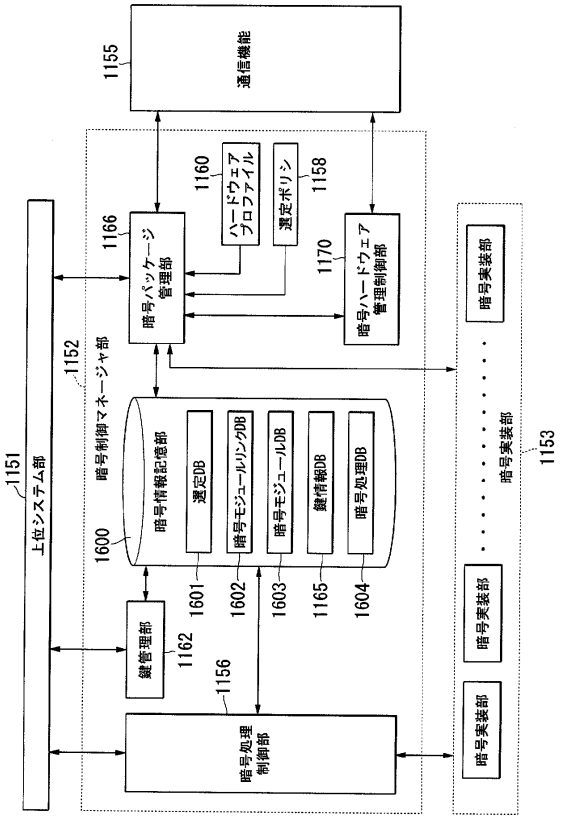
【図３】



【図４】



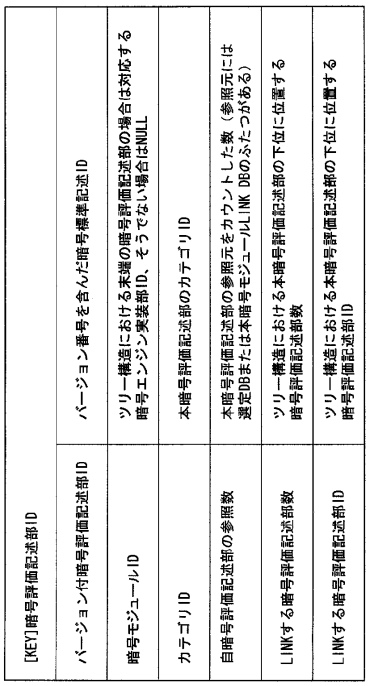
【図５】



【図６】

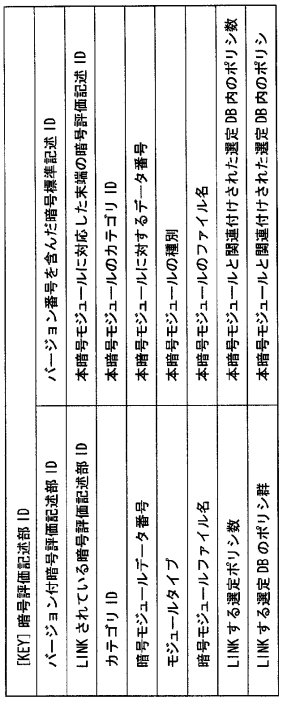
[KEY]ポリシ（カテゴリ情報を含む暗号モジュールの条件情報を文字列化したもの）	
最上位暗号評価記述部ID	当該ポリシに対応づけられる暗号モジュールの最上位の暗号評価記述部ID
アルゴリズムID	当該ポリシに対応づけられるアルゴリズムID
LINKする暗号モジュール数	当該ポリシに対応づけられる末端の暗号モジュール数
LINKする暗号モジュールID群	当該ポリシに対応づけられる末端の暗号モジュールID（複数）
鍵長	暗号処理実行時に使用する暗号鍵の長さ

【図７】



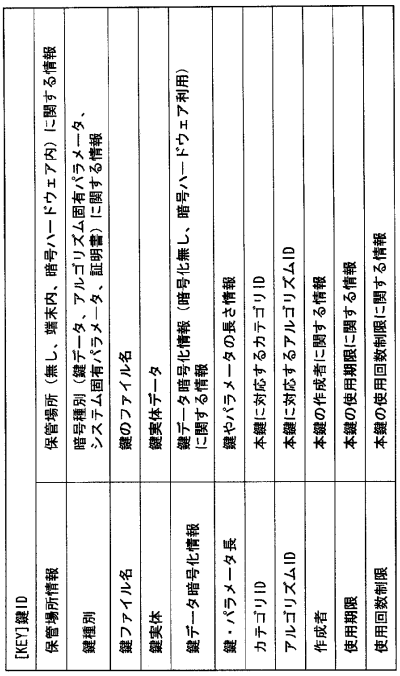
[KEY]暗号評価記述部ID	
バージョン付暗号評価記述部ID	バージョン番号を含んだ暗号標準記述ID
暗号モジュールID	ツリー構造における末端の暗号評価記述部の場合は対応する暗号エンジン実装部ID、そうでない場合はNULL
カテゴリID	本暗号評価記述部のカテゴリID
自暗号評価記述部の参照数	本暗号評価記述部の参照元をカウントした数（参照元には選定DBまたは本暗号モジュールLINK DBのふたつがある）
LINKする暗号評価記述部数	ツリー構造における本暗号評価記述部の下位に位置する暗号評価記述部数
LINKする暗号評価記述部ID	ツリー構造における本暗号評価記述部の下位に位置する暗号評価記述部ID

【図８】



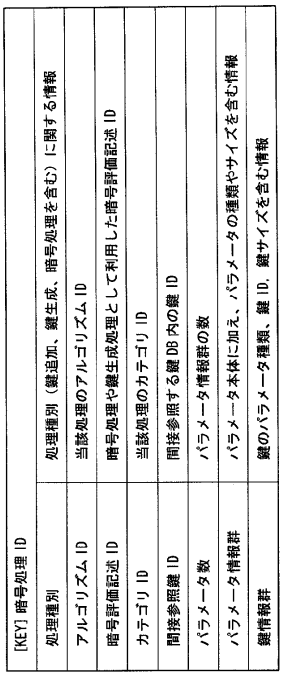
[KEY] 暗号評価記述部 ID	
バージョン付暗号評価記述部 ID	バージョン番号を含んだ暗号標準記述 ID
LINK されている暗号評価記述部 ID	本暗号モジュールに対応した末端の暗号評価記述 ID
カテゴリ ID	本暗号モジュールのカテゴリ ID
暗号モジュールデータ番号	本暗号モジュールに対するデータ番号
モジュールタイプ	本暗号モジュールの種別
暗号モジュールファイル名	本暗号モジュールのファイル名
LINK する選定ポリシ数	本暗号モジュールと関連付けされた選定 DB 内のポリシ数
LINK する選定 DB のポリシ群	本暗号モジュールと関連付けされた選定 DB 内のポリシ

【図９】



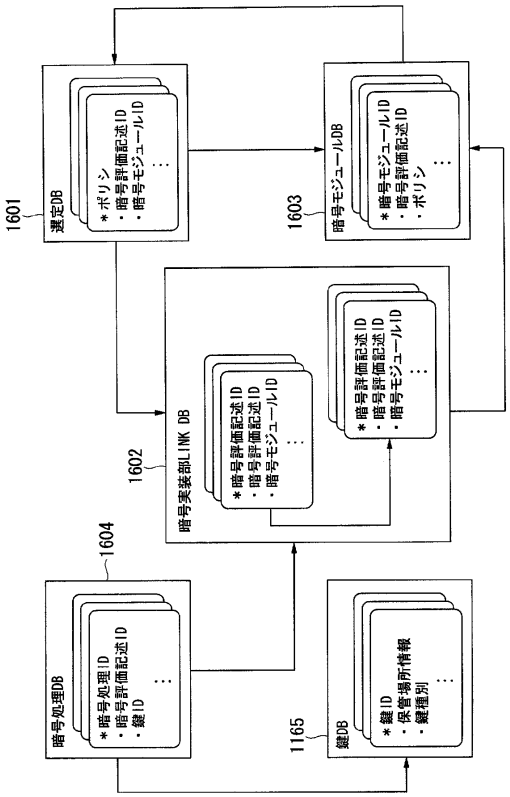
[KEY]鍵ID	
保管場所情報	保管場所（無し、端末内、暗号ハードウェア内）に関する情報
鍵種別	暗号種別（鍵データ、アルゴリズム固有パラメータ、システム固有パラメータ、証明書）に関する情報
鍵ファイル名	鍵のファイル名
鍵実体	鍵実体データ
鍵データ暗号化情報	鍵データ暗号化情報（暗号化無し、暗号ハードウェア利用）に関する情報
鍵・パラメータ長	鍵やパラメータの長さ情報
カテゴリID	本鍵に対応するカテゴリID
アルゴリズムID	本鍵に対応するアルゴリズムID
作成者	本鍵の作成者に関する情報
使用期限	本鍵の使用期限に関する情報
使用回数制限	本鍵の使用回数制限に関する情報

【図１０】

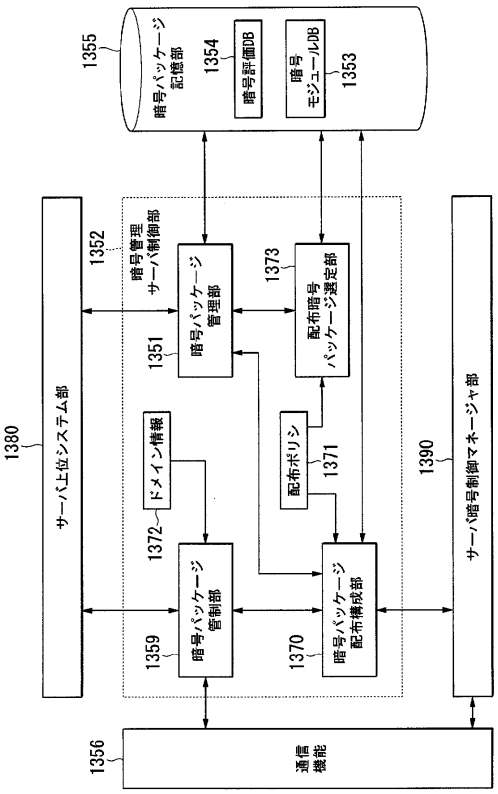


[KEY] 暗号処理 ID	
処理種別	処理種別（鍵追加、鍵生成、暗号処理を含む）に関する情報
アルゴリズム ID	当該処理のアルゴリズム ID
暗号評価記述 ID	暗号処理や鍵生成処理として利用した暗号評価記述 ID
カテゴリ ID	当該処理のカテゴリ ID
間接参照鍵 ID	間接参照する鍵 DB 内の鍵 ID
パラメータ数	パラメータ情報群の数
パラメータ情報群	パラメータ本体に加え、パラメータの種類やサイズを含む情報
鍵情報群	鍵のパラメータ種類、鍵 ID、鍵サイズを含む情報

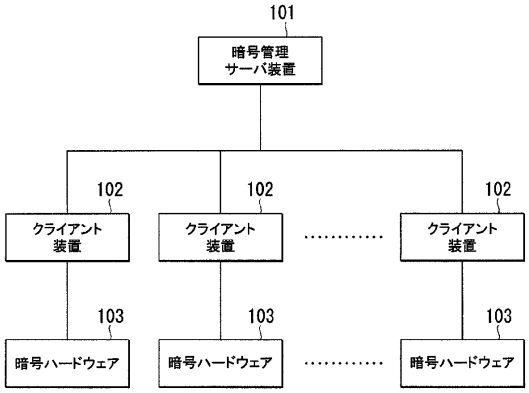
【図１１】



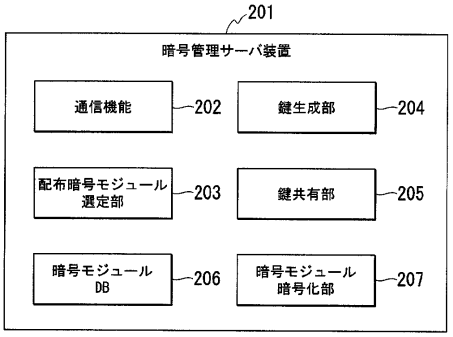
【図１２】



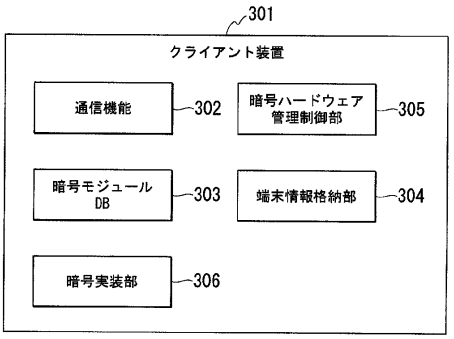
【図１３】



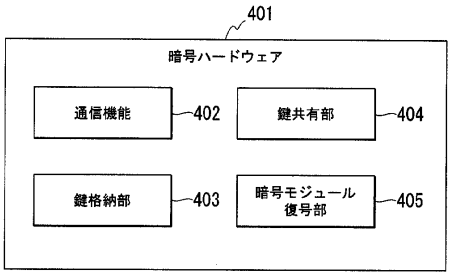
【図１４】



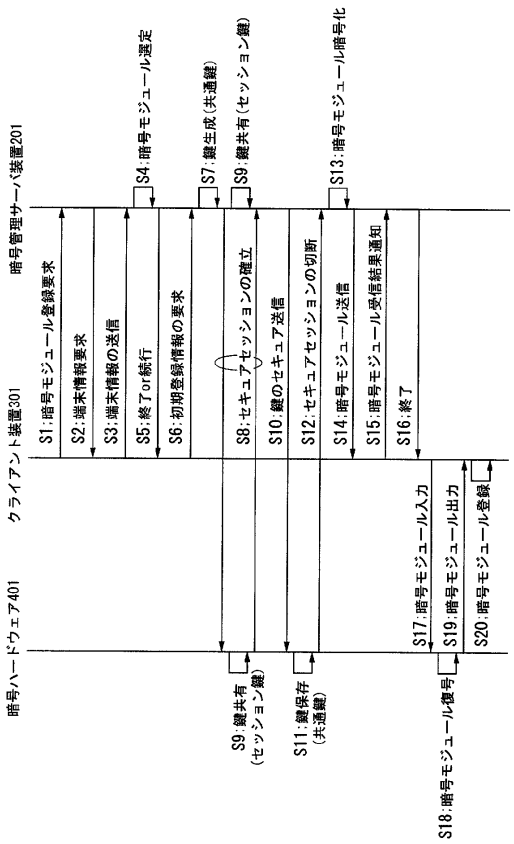
【図１５】



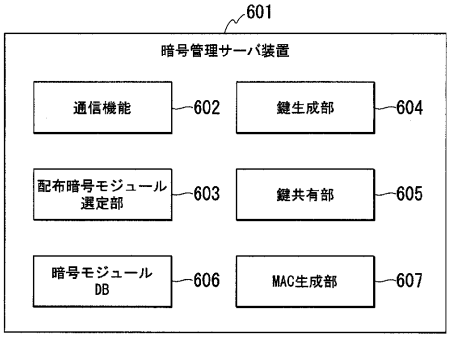
【図１６】



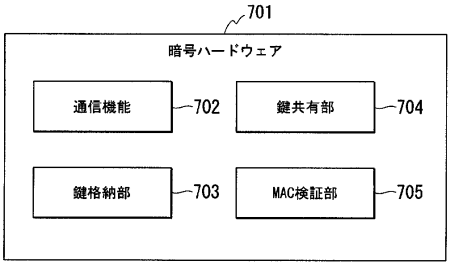
【図１７】



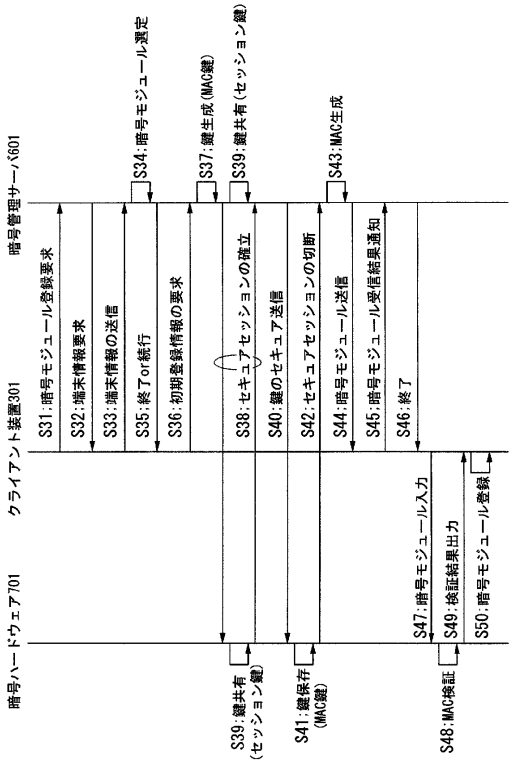
【図１８】



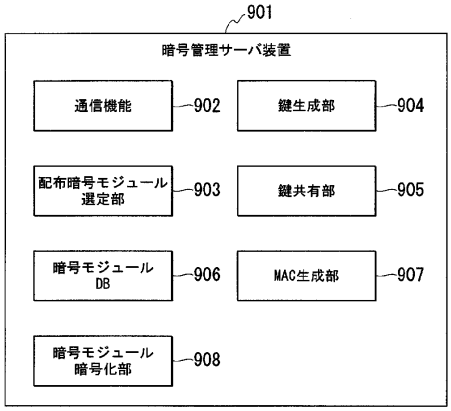
【図１９】



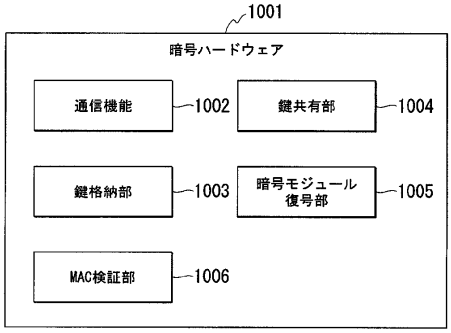
【図２０】



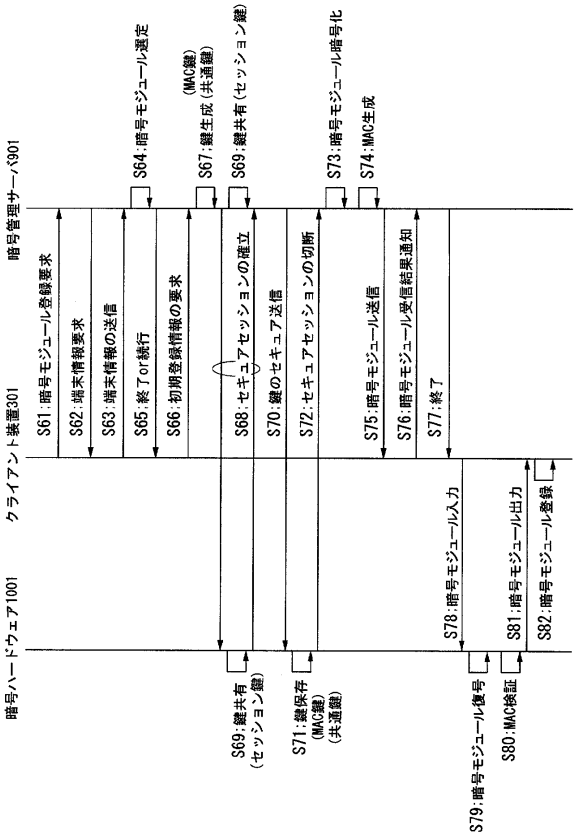
【図２１】



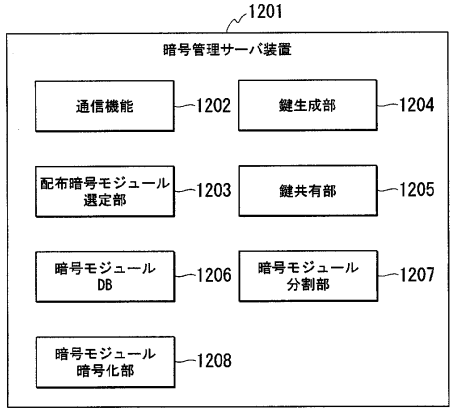
【図２２】



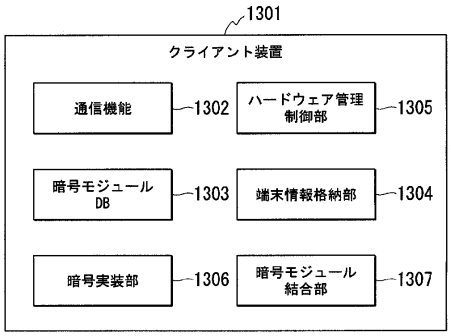
【図２３】



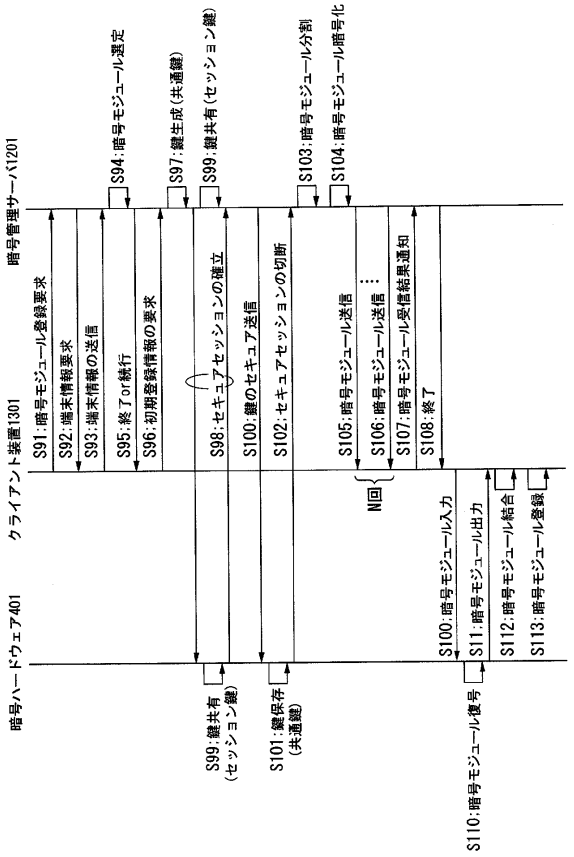
【図２４】



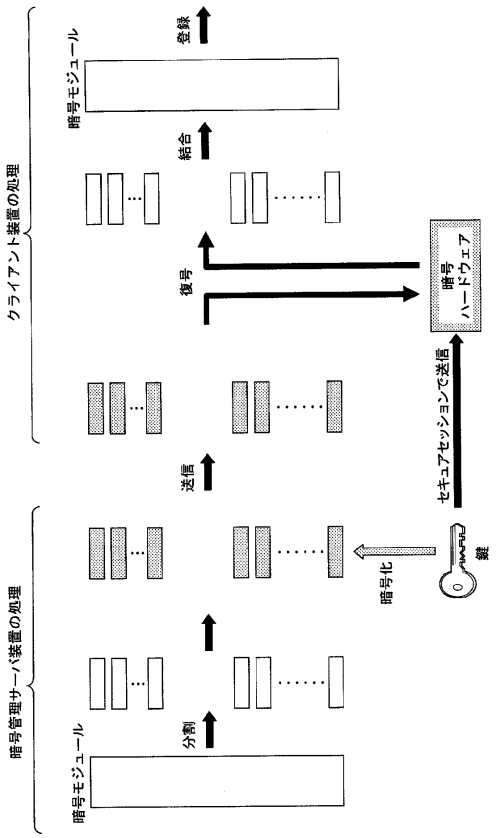
【図２５】



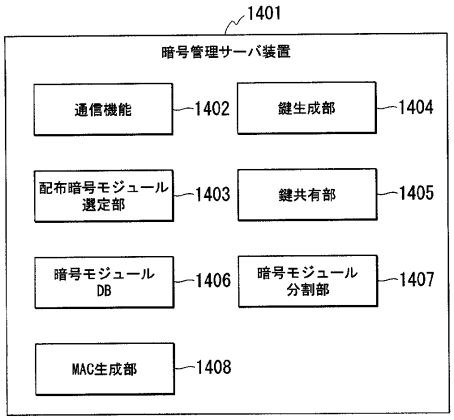
【図２６】



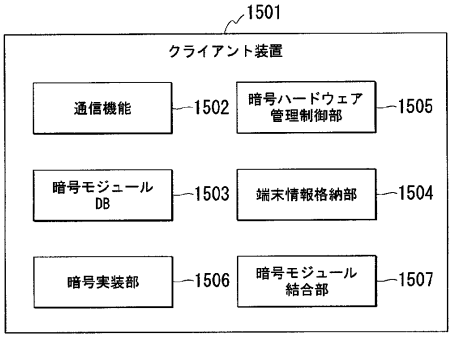
【図２７】



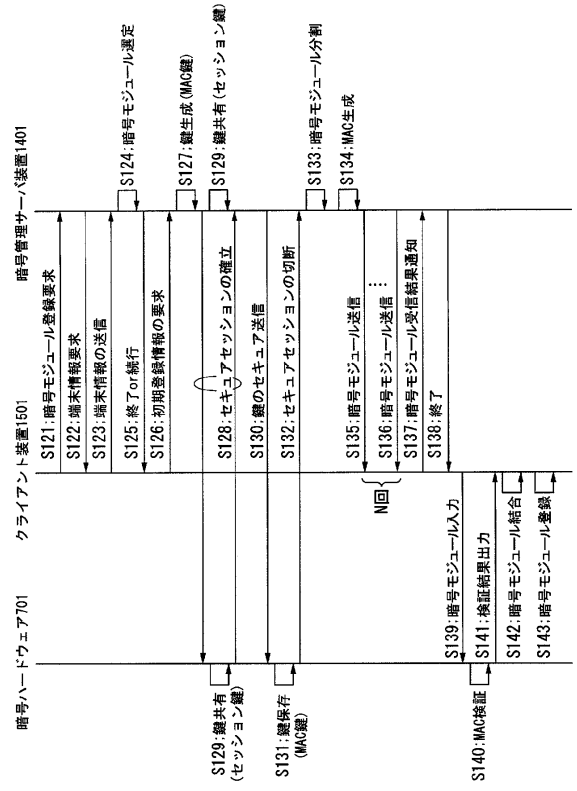
【図２８】



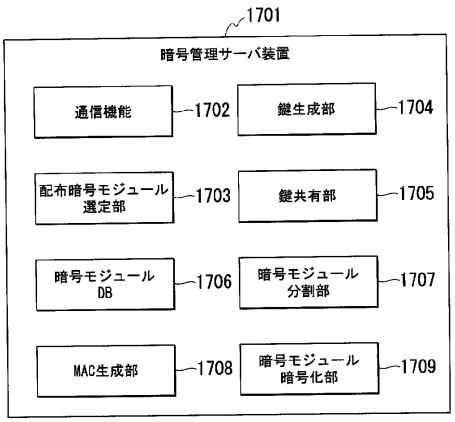
【図２９】



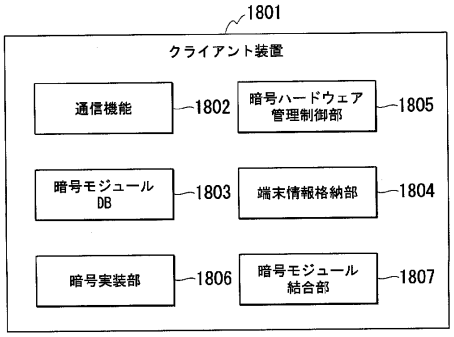
【図３０】



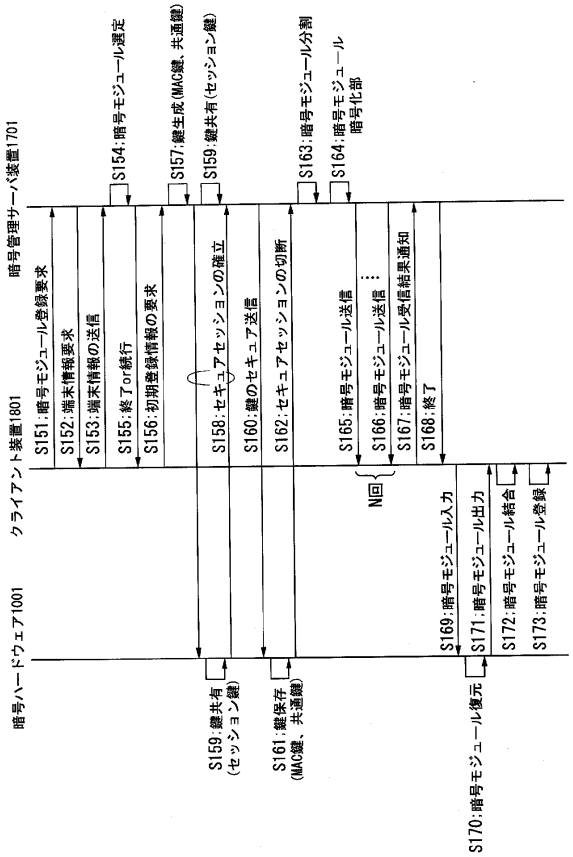
【図３１】



【図３２】



【図３３】



【図３４】

端末ＩＤ	暗号モジュールＩＤ	
	搭載中暗号モジュール	搭載可能暗号モジュール
00000001	020200021061 060200021061 0902000F0001 ……	020200021062 060200021062 060200021063 ……
00000002	050200021061 0902000F0001 ……	050200021062 050200021063 060200021063 ……

フロントページの続き

(74)代理人 100075672
弁理士 峰 隆司
(74)代理人 100095441
弁理士 白根 俊郎
(74)代理人 100084618
弁理士 村松 貞男
(74)代理人 100103034
弁理士 野河 信久
(74)代理人 100119976
弁理士 幸長 保次郎
(74)代理人 100153051
弁理士 河野 直樹
(74)代理人 100140176
弁理士 砂川 克
(74)代理人 100101812
弁理士 勝村 紘
(74)代理人 100100952
弁理士 風間 鉄也
(74)代理人 100070437
弁理士 河井 将次
(74)代理人 100124394
弁理士 佐藤 立志
(74)代理人 100112807
弁理士 岡田 貴志
(74)代理人 100111073
弁理士 堀内 美保子
(74)代理人 100134290
弁理士 竹内 将訓
(74)代理人 100127144
弁理士 市原 卓三
(74)代理人 100141933
弁理士 山下 元
(72)発明者 栃窪 孝也
東京都港区芝浦一丁目１番１号 東芝ソリューション株式会社内
(72)発明者 福島 茂之
東京都港区芝浦一丁目１番１号 東芝ソリューション株式会社内
(72)発明者 岡田 光司
東京都港区芝浦一丁目１番１号 東芝ソリューション株式会社内
(72)発明者 丹羽 朗人
東京都港区芝浦一丁目１番１号 東芝ソリューション株式会社内
(72)発明者 中溝 孝則
東京都港区芝浦一丁目１番１号 東芝ソリューション株式会社内
(72)発明者 宮崎 真悟
東京都品川区西五反田２－２０－１ 第２８興和ビル 株式会社横須賀テレコムリサーチパーク
ＹＲＰユビキタス・ネットワーキング研究所内
(72)発明者 石川 千秋
東京都品川区西五反田２－２０－１ 第２８興和ビル 株式会社横須賀テレコムリサーチパーク
ＹＲＰユビキタス・ネットワーキング研究所内

(72)発明者　越塚　登
東京都品川区西五反田２－２０－１　第２８興和ビル　株式会社横須賀テレコムリサーチパーク
ＹＲＰユビキタス・ネットワーキング研究所内
(72)発明者　坂村　健
東京都品川区西五反田２－２０－１　第２８興和ビル　株式会社横須賀テレコムリサーチパーク
ＹＲＰユビキタス・ネットワーキング研究所内

審査官　石田　信行

(56)参考文献　特開２００４－２７４４８０（ＪＰ，Ａ）
特開平０４－２６８８４４（ＪＰ，Ａ）
特開２００２－０４１４８３（ＪＰ，Ａ）
特開２００６－１５７７３５（ＪＰ，Ａ）
特開２００６－２１１７２８（ＪＰ，Ａ）
特開２００４－３４３８１２（ＪＰ，Ａ）
特開２００３－０３２２４１（ＪＰ，Ａ）
特開２００３－３１８８７４（ＪＰ，Ａ）
特開２００２－２３６６１８（ＪＰ，Ａ）
特開２００１－３３９３８４（ＪＰ，Ａ）
特開２００１－１２７７５１（ＪＰ，Ａ）
特開２０００－２３２４４２（ＪＰ，Ａ）
特開平１０－２４２９５７（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／０８
Ｈ０４Ｌ　　９／１４
Ｇ０９Ｃ　　１／００
Ｇ０６Ｆ　　９／４４５
Ｇ０６Ｆ　２１／１２
Ｇ０６Ｆ　２１／６４