

(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2012-114528

(P2012-114528A)

(43) 公開日 平成24年6月14日(2012.6.14)

(51) Int.Cl.		F I				テーマコード (参考)
H O 4 L	9/08	(2006.01)	H O 4 L	9/00	6 O 1 B	5 J 1 0 4
H O 4 L	9/14	(2006.01)	H O 4 L	9/00	6 4 1	

審査請求 未請求 請求項の数 10 O L (全 37 頁)

(21) 出願番号	特願2010-259685 (P2010-259685)	(71) 出願人	000004237
(22) 出願日	平成22年11月22日 (2010.11.22)		日本電気株式会社
			東京都港区芝五丁目7番1号
		(74) 代理人	100109313
			弁理士 机 昌彦
		(74) 代理人	100124154
			弁理士 下坂 直樹
		(72) 発明者	野村 崇志
			東京都港区芝五丁目7番1号
			日本電気株式会社内
		Fターム(参考)	5J104 AA16 AA36 EA04 EA15 EA16
			NA02 NA37

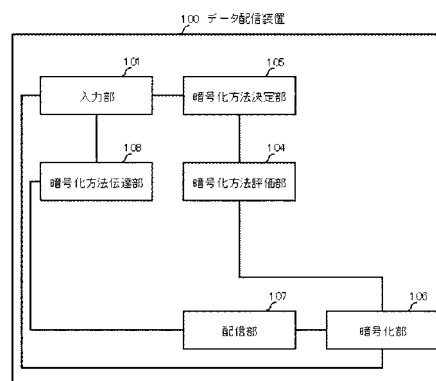
(54) 【発明の名称】 データ配信装置、データ配信方法およびデータ配信プログラム

(57) 【要約】

【課題】 データ配信装置は、暗号化データ生成時の負荷を軽減しつつ暗号化されるデータの有効期限までの秘匿性を維持しつつ有効期限後の有効利用性を保証する。

【解決手段】 データ配信装置は、データの有効期限までに解読されない暗号強度を持つ暗号化方法のうち、リソース消費量評価値に基づいてリソース量に対応する暗号化方法を特定し、特定した暗号化方法によってそのデータを暗号化し、暗号化したデータを配信する際に、その有効期限を経過している、および、宛先で示される配信先にデータが配信される、の二つの条件の少なくともいずれかが満たされる場合に、暗号化方法を識別できる暗号化方法識別子をデータの配信先に送信する。

【選択図】 図1



【特許請求の範囲】

【請求項 1】

データを識別できるデータ識別子と当該データの配信先を示す宛先とを受け取る入力部と、

前記データに対応する当該データの有効期限までに解読されない暗号強度を持つ暗号化方法を識別できる暗号化方法識別子と当該暗号化方法の暗号化処理に必要なリソース量とを特定する暗号化方法決定部と、

前記暗号化方法決定部が特定したリソース量に基づいて、それぞれのリソース量に対応する暗号化方法識別子で識別される暗号化方法が用いられる優先度を示すリソース消費量評価値を算出し、算出される当該リソース消費量評価値に基づいてリソース量に対応する暗号化方法識別子を特定する暗号化方法評価部と、

前記データ識別子で識別されるデータを、前記暗号化方法評価部が特定した暗号化方法識別子で識別される暗号化方法によって暗号化する暗号化部と、

前記暗号化部が暗号化した前記データを配信する配信部と、

前記配信部が前記データを配信する際に、前記有効期限を経過している、および、前記宛先で示される配信先に当該データが配信される、の二つの条件の少なくともいずれかが満たされる場合に、前記暗号化方法識別子を当該データの配信先に送信する暗号化方法伝達部と、

を備えるデータ配信装置。

【請求項 2】

請求項 1 に記載のデータ配信装置であって、

当該データ配信装置が備えるリソースの負荷情報を取得する負荷情報取得部と、

リソースの負荷情報の条件を示す適用条件とリソース量に基づいてリソース消費量評価値の算出方法を示すリソース消費量評価値算出方法とを対応付けて記憶するリソース消費量評価値算出方法記憶部と、を備え

前記暗号化方法評価部は、前記装置負荷情報取得部から前記リソースの負荷情報を受け取り、当該リソースの負荷情報と合致する適用条件に対応付けられているリソース消費量評価値算出方法を前記リソース消費量評価値算出方法記憶部から読み出し、

前記暗号化方法評価部は、読み出したリソース消費量評価値算出方法に基づいて、各暗号化方法のリソース消費量評価値を算出する、データ配信装置。

【請求項 3】

請求項 1 または 2 に記載のデータ配信装置であって、

データを解析して当該データの有効期限を算出するための関数である有効期限算出関数と、その関数が適用される条件を示すルール適用条件とを含む有効期限算出ルールを記憶する有効期限算出ルール記憶部と、

データを受け取ると、当該データと合致するルール適用条件を含む有効期限算出ルールを前記有効期限算出ルール記憶部から読み出し、読み出した有効期限算出ルールに含まれる有効期限算出関数と当該データとに基づいて当該データの有効期限を算出する有効期限算出部と、を備え

前記入力部は、受け取ったデータ識別子で識別されるデータを受け取ると、当該データを前記有効期限算出部に渡し、

前記暗号化方法決定部は、前記有効期限算出部が算出した有効期限までに解読されない暗号強度を持つ暗号化方法を識別できる暗号化方法識別子と当該暗号化方法の暗号処理に必要なリソース量とを特定する、データ配信装置。

【請求項 4】

請求項 3 に記載のデータ配信装置であって、

データに含まれる所定の内容を示す情報である抽出情報を当該データから抽出し、抽出した抽出情報を記憶するデータ抽出部を備え、

前記有効期限算出部は、受け取ったデータに含まれる抽出情報と共通する情報を示す抽出情報を前記データ抽出部から読み出し、読み出した抽出情報の個数に基づいて有効期限

10

20

30

40

50

を算出する、データ配信装置。

【請求項 5】

請求項 3 または 4 に記載のデータ配信装置であって、

前記ルール適用条件は、データが含む所定の要素の有無、その要素が有する属性の有無、要素の値、および要素が有する属性の値の少なくとも一つの情報の条件であり、

前記有効期限算出関数は、データが含む所定の要素の有無、その要素が有する属性の有無、要素の値、および要素が有する属性の値の少なくとも一つの情報に基づいた演算を規定する関数である、データ配信装置。

【請求項 6】

請求項 4 に記載のデータ配信装置であって、

前記抽出情報は、ある個人に関連する情報を示す情報であり、

前記有効期限算出部は、受け取ったデータに含まれる抽出情報と共通する個人に関連する情報を示す抽出情報を前記データ抽出部から読み出し、読み出した抽出情報の個数が所定の閾値以上である場合に、前記受け取ったデータの有効期限を長くする、データ配信装置。

【請求項 7】

請求項 1 ないし 6 のいずれか 1 項に記載のデータ配信装置であって、

前記リソース消費量評価値は、値が大きい場合に前記優先度が高いことを示し、

前記暗号化方法評価部は前記暗号化方法決定部が複数の暗号化方法識別子を特定した際に、当該複数の暗号化方法識別子の中から、リソース消費量評価値が最大であるリソース量に対応する暗号化方法識別子を特定する、データ配信装置。

【請求項 8】

請求項 1 ないし 7 のいずれか 1 項に記載のデータ配信装置であって、

暗号化方法識別子を受け取ると、当該暗号化方法識別子で識別される暗号化方法に基づいて、当該暗号化方法により暗号化されたデータに対する暗号解読法を適用した場合の強度指標を求め、当該強度指標に基づき前記暗号化されたデータの解読に要する時間を推定し、推定された時間に基づいて暗号強度を算出し、当該暗号化方法識別子で識別される暗号化方法を用いて所定のデータに対して暗号化処理を行い、その際に消費されるリソースの量に基づいて、リソース量を算出する暗号強度算出部を備え、

前記暗号化方法決定部は、前記暗号強度算出部が算出した暗号強度とリソース量と、算出の際に用いられた暗号化方法の暗号化方法識別子とを対応付けて記憶し、前記入力部が受け取るデータ識別子で識別されるデータの有効期限までに解読されない暗号強度を持つ暗号化方法を識別できる暗号化方法識別子と当該暗号化方法の暗号処理に必要なリソース量とを、前記記憶した暗号強度と当該有効期限とを比較することで特定する、データ配信装置。

【請求項 9】

データを識別できるデータ識別子と当該データの配信先を示す宛先とを受け取り、

前記データに対応する当該データの有効期限までに解読されない暗号強度を持つ暗号化方法を識別できる暗号化方法識別子と当該暗号化方法の暗号化処理に必要なリソース量とを特定し、

前記特定したリソース量に基づいて、それぞれのリソース量に対応する暗号化方法識別子で識別される暗号化方法が用いられる優先度を示すリソース消費量評価値を算出し、算出される当該リソース消費量評価値に基づいてリソース量に対応する暗号化方法識別子を特定し、

前記データ識別子で識別されるデータを、前記特定した暗号化方法識別子で識別される暗号化方法によって暗号化し、

前記暗号化した前記データを配信し、

前記データを配信する際に、前記有効期限を経過している、および、前記宛先で示される配信先に当該データが配信される、の二つの条件の少なくともいずれかが満たされる場合に、前記暗号化方法識別子を当該データの配信先に送信する、データ配信方法。

【請求項 10】

コンピュータに、
データを識別できるデータ識別子と当該データの配信先を示す宛先とを受け取る処理と、

前記データに対応する当該データの有効期限までに解読されない暗号強度を持つ暗号化方法を識別できる暗号化方法識別子と当該暗号化方法の暗号化処理に必要なリソース量とを特定する処理と、

前記特定したリソース量に基づいて、それぞれのリソース量に対応する暗号化方法識別子で識別される暗号化方法が用いられる優先度を示すリソース消費量評価値を算出し、算出される当該リソース消費量評価値に基づいてリソース量に対応する暗号化方法識別子を

10

特定する処理と、
前記データ識別子で識別されるデータを、前記特定した暗号化方法識別子で識別される暗号化方法によって暗号化する処理と、

前記暗号化した前記データを配信する処理と、

前記データを配信する際に、前記有効期限を経過している、および、前記宛先で示される配信先に当該データが配信される、の二つの条件の少なくともいずれかが満たされる場合に、前記暗号化方法識別子を当該データの配信先に送信する処理と、を実行させるためのデータ配信プログラム。

【発明の詳細な説明】

【技術分野】

20

【0001】

本発明は、複数の暗号化方法の中からいずれかを用いてデータを暗号化し、配信する技術に関する。

【背景技術】

【0002】

第三者から情報を秘匿したデータ配信を行うための手段として、データを暗号化して配信する方式が一般に用いられている。

【0003】

特に、暗号強度が異なる複数の暗号化方法（暗号化アルゴリズムならびに鍵長などのパラメータ）の中から、データの機密度などに応じて用いる暗号化方法を選択し、これを用いてデータを暗号化し配信する方式が提案されている。

30

【0004】

例えば、特許文献 1 は、以下の技術を開示している。すなわちこの技術は、ある期限（寿命）を迎えた時点で消滅するエージェント型プログラム（エージェント）を生成し送信する装置が、生成したエージェントの寿命までに解読されることがない適切な強度の暗号化方法を選択する。そしてこの装置は、選択した暗号化方法を用いてエージェントが持つ機密情報を暗号化する。これにより特許文献 1 に開示された技術は、暗号化処理に要するリソースを最小限に抑える。

【0005】

また、特許文献 2 は、以下の技術を開示している。特許文献 2 に記載されている技術は、機密情報を含む電子コンテンツを暗号化して管理するための暗号化コンテンツ管理に関する技術である。特許文献 2 に記載の技術は、機密度に応じて予め決められた保護強度で暗号化されている電子コンテンツに対して、ユーザ入力あるいは時間経過などにより機密度に変更があった場合に、機密度の変化量に応じて適切な保護強度を保つ。

40

【0006】

また、特許文献 3 は、以下の技術を開示している。すなわちこの技術は、機密ファイルの保護期間に基づいて、暗号化される機密ファイルの保護強度を決定する。

【0007】

また、暗号化処理を行う装置の負荷に応じて暗号化処理に用いる暗号アルゴリズムを選択する技術が知られている。例えば、特許文献 4 は、以下の技術を開示している。すなわ

50

ちこの技術は、通信装置が、C P U (Central Processing Unit) の使用率に応じて暗号処理に用いる暗号アルゴリズムを選択する。

【0008】

また、データの内容に応じてそのデータの有効期限を特定する技術が知られている。特許文献5は、以下の技術を開示している。すなわちこの技術は、ドキュメントに対して意味クラス解析技術などを用いてそのドキュメントの何らかの期限を示す期限情報および期限メタデータを抽出する。

【先行技術文献】

【特許文献】

【0009】

10

【特許文献1】特開2003-345664号公報

【特許文献2】特開2009-027642号公報

【特許文献3】特開2006-332435号公報

【特許文献4】特開2004-254286号公報

【特許文献5】特開2008-187708号公報

【非特許文献】

【0010】

【非特許文献1】反町、松井、「RC5の強度評価に関する一考察(その2)」、電子情報通信学会技術研究報告、ISEC、情報セキュリティ 96(237), 第87頁-第98頁, 1996年。

【発明の概要】

20

【発明が解決しようとする課題】

【0011】

しかし、特許文献1に記載された技術は、データを暗号化する際に暗号化データに基づいてエージェントを作成している。よって特許文献1に記載された技術は、暗号化データ生成時に、暗号化処理とエージェント作成処理とを必要とするので大きな負荷がかかる。また特許文献1に記載された技術は、データの有効期限後、エージェントにより削除される。よって特許文献1に記載された技術は、データの有効期限後の利用を考慮しておらず、暗号化データの有効期限後の有効利用性を保証することができない。

【0012】

特許文献2乃至5に記載された各技術は、データの有効期限後にそのデータを利用することについて考慮していないので、暗号化データの有効期限後の有効利用性を保証することができない。

30

【0013】

よって、各関連文献に記載された技術は、暗号化データ生成時の負荷を軽減しかつ暗号化されるデータの有効期限までの秘匿性を維持しつつ有効期限後の有効利用性を保証することができない。

【0014】

本発明の目的の一例は、暗号化データ生成時の負荷を軽減しかつ暗号化されるデータの有効期限までの秘匿性を維持しつつ有効期限後の有効利用性を保証することができるデータ暗号化装置、データ暗号化方法、およびデータ暗号化プログラムを提供することである。

40

【課題を解決するための手段】

【0015】

本発明の一形態における第一のデータ配信装置は、データを識別できるデータ識別子と当該データの配信先を示す宛先とを受け取る入力部と、前記データに対応する当該データの有効期限までに解読されない暗号強度を持つ暗号化方法を識別できる暗号化方法識別子と当該暗号化方法の暗号化処理に必要なリソース量とを特定する暗号化方法決定部と、前記暗号化方法決定部が特定したリソース量に基づいて、それぞれのリソース量に対応する暗号化方法識別子で識別される暗号化方法が用いられる優先度を示すリソース消費量評価値を算出し、算出される当該リソース消費量評価値に基づいてリソース量に対応する暗号

50

化方法識別子を特定する暗号化方法評価部と、前記データ識別子で識別されるデータを、前記暗号化方法評価部が特定した暗号化方法識別子で識別される暗号化方法によって暗号化する暗号化部と、前記暗号化部が暗号化した前記データを配信する配信部と、前記配信部が前記データを配信する際に、前記有効期限を経過している、および、前記宛先で示される配信先に当該データが配信される、の二つの条件の少なくともいずれかが満たされる場合に、前記暗号化方法識別子を当該データの配信先に送信する暗号化方法伝達部と、を備える。

【0016】

本発明の一形態における第一のデータ配信方法は、データを識別できるデータ識別子と当該データの配信先を示す宛先とを受け取り、前記データに対応する当該データの有効期限までに解読されない暗号強度を持つ暗号化方法を識別できる暗号化方法識別子と当該暗号化方法の暗号化処理に必要なリソース量とを特定し、前記特定したリソース量に基づいて、それぞれのリソース量に対応する暗号化方法識別子で識別される暗号化方法が用いられる優先度を示すリソース消費量評価値を算出し、算出される当該リソース消費量評価値に基づいてリソース量に対応する暗号化方法識別子を特定し、前記データ識別子で識別されるデータを、前記特定した暗号化方法識別子で識別される暗号化方法によって暗号化し、前記暗号化した前記データを配信し、前記データを配信する際に、前記有効期限を経過している、および、前記宛先で示される配信先に当該データが配信される、の二つの条件の少なくともいずれかが満たされる場合に、前記暗号化方法識別子を当該データの配信先に送信する。

【0017】

本発明の一形態における第一のデータ配信プログラムは、コンピュータに、データを識別できるデータ識別子と当該データの配信先を示す宛先とを受け取る処理と、前記データに対応する当該データの有効期限までに解読されない暗号強度を持つ暗号化方法を識別できる暗号化方法識別子と当該暗号化方法の暗号化処理に必要なリソース量とを特定する処理と、前記特定したリソース量に基づいて、それぞれのリソース量に対応する暗号化方法識別子で識別される暗号化方法が用いられる優先度を示すリソース消費量評価値を算出し、算出される当該リソース消費量評価値に基づいてリソース量に対応する暗号化方法識別子を特定する処理と、前記データ識別子で識別されるデータを、前記特定した暗号化方法識別子で識別される暗号化方法によって暗号化する処理と、前記暗号化した前記データを配信する処理と、前記データを配信する際に、前記有効期限を経過している、および、前記宛先で示される配信先に当該データが配信される、の二つの条件の少なくともいずれかが満たされる場合に、前記暗号化方法識別子を当該データの配信先に送信する処理と、を実行させる。

【発明の効果】

【0018】

本発明の効果の一例は、暗号化データ生成時の負荷を軽減できかつ暗号化されるデータの有効期限までの秘匿性を維持しつつ有効期限後の有効利用性を保証できることである。

【図面の簡単な説明】

【0019】

【図1】図1は、本発明の第一の実施の形態におけるデータ配信装置の構成例を示すブロック図である。

【図2】図2は、暗号化方法記憶部が記憶する暗号化方法特徴情報の一例を示す図である。

【図3】図3は、本発明の第一の実施の形態における入力部の構成の一例を示すブロック図である。

【図4】図4は、本発明の第一の実施の形態におけるデータ配信装置の動作の概要を示すフローチャートである。

【図5】図5は、暗号化方法決定部が暗号化方法を決定する過程の具体例を示すフローチャートである。

10

20

30

40

50

【図 6】図 6 は、本発明の第一の実施の形態の第一の変形例におけるデータ配信装置の構成の一例を示すブロック図である。

【図 7】図 7 は、本発明の第一の実施の形態の第二の変形例におけるデータ配信装置の構成の一例を示すブロック図である。

【図 8】図 8 は、本発明の第一の実施の形態の第三の変形例におけるデータ配信装置の構成の一例を示すブロック図である。

【図 9】図 9 は、本発明の第二の実施の形態におけるデータ配信装置の構成例を示すブロック図である。

【図 10】図 10 は、リソース消費量評価値算出方法記憶部が記憶するリソース消費量評価値算出方法の一例を示す図である。

【図 11】図 11 は、暗号化方法記憶部が記憶する暗号化方法特徴情報の一例を示す図である。

【図 12】図 12 は、暗号化方法評価部が適切なリソース消費量評価値算出方法を特定する過程、および、特定されたリソース消費量評価値算出方法に基づいて暗号化方法評価部が暗号化方法を決定する過程の具体例を示すフローチャートである。

【図 13】図 13 は、本発明の第三の実施の形態におけるデータ配信装置 300 の構成例を示すブロック図である。

【図 14】図 14 は、本発明の第三の実施の形態における入力部の構成の一例を示すブロック図である。

【図 15】図 15 は、有効期限算出ルール記憶部が記憶する有効期限算出ルールの一例を示す図である。

【図 16】図 16 は、有効期限算出ルール記憶部が記憶する有効期限算出ルールの具体例を示す図である。

【図 17】図 17 は、入力部が受け取る平文データの具体例を示す図である。

【図 18】図 18 は、有効期限算出部がデータの有効期限を算出する手順の具体例を示すフローチャートである。

【図 19】図 19 は、本発明の第三の実施の形態の第一の変形例におけるデータ配信装置の構成例を示すブロック図である。

【発明を実施するための形態】

【0020】

以下、本発明を実施するための形態について図面を参照して詳細に説明する。なお、各図面および明細書記載の各実施の形態において、同様の機能を備える構成要素には同様の符号が与えられている。

【0021】

〔第一の実施の形態〕

図 1 は、本発明の第一の実施の形態におけるデータ配信装置 100 の構成例を示すブロック図である。

【0022】

図 1 を参照すると、データ配信装置 100 は、入力部 101 と、暗号化方法評価部 104 と、暗号化方法決定部 105 と、暗号化部 106 と、暗号データ配信部 107 と、暗号化方法伝達部 108 と、を備える。

【0023】

第一の実施の形態におけるデータ配信装置 100 は、データ識別子と宛先とを受け取ると、そのデータ識別子で識別されるデータに対応する有効期限までには解読されない暗号強度を持つ暗号化方法を特定する。そしてデータ配信装置 100 は、特定した暗号化方法のうち、各暗号化方法の暗号処理において必要となるリソース量に基づいて算出されるリソース消費量評価値を算出する。データ配信装置 100 は、リソース消費量評価値に基づいて暗号化方法を特定し、その暗号化方法によって前述のデータ識別子で識別されるデータを暗号化する。データ配信装置 100 は、暗号化したデータを配信する。この際にデータ配信装置 100 は、以下の二条件のうちの少なくとも一方を満たす場合に、前述のデー

10

20

30

40

50

タの暗号化に適用された暗号化方法を識別できる暗号化方法識別子を前述の宛先を示す配信先へ送信する。第一の条件は、有効期限を経過していることである。第二の条件は、前述の宛先が示す配信先に前述の暗号化したデータを配信することである。

【0024】

この構成により第一の実施の形態におけるデータ配信装置100は、データを暗号化する際、そのデータの有効期限には解読されない暗号強度を持つ暗号化方法のうち例えばリソース消費量が最も小さい暗号化方法によってデータを暗号化できる。

【0025】

またデータ配信装置100は、暗号化されたデータの有効期限が経過していない場合には、そのデータの正当な宛先に対してそのデータに適用された暗号化方法を識別できる暗号化方法識別子を送信する。一方、データ配信装置100は、暗号化されたデータの有効期限が経過している場合には、すべての配信先に対して前述の暗号化方法識別子を送信する。よってデータ配信装置100が配信するデータは、次の特徴を持つ。有効期限以前において、正当な配信先である宛先の装置がそのデータを復号でき、有効期限経過後において、すべての装置がそのデータを復号できる。したがってデータ配信装置100は、データの有効期限までの秘匿性を維持しつつ有効期限後のデータの有効利用性を保証できる。

【0026】

以下、データ配信装置100が備える各構成要素について説明がなされる。

【0027】

===入力部101===

入力部101は、データを識別できるデータ識別子とそのデータの配信先を示す宛先とを入力として受け取る。

【0028】

データ識別子で識別できるデータは、データ配信装置100が配信を行う平文データである。このデータは、そのデータの有効期限までの間、第三者から秘匿した状態で配信される。データ配信装置100は、このデータを入力として受け取ってもよいし、あらかじめこのデータを記憶しておいてもよい。本明細書では、入力部101がデータを入力として受け取る。

【0029】

なお、本明細書では入力部101は、データ識別子を受け取るが、入力部101はデータを入力として受け取り、受け取ったデータに基づいてそのデータを識別できるデータ識別子を生成してもよい。そして、入力部101は、生成したデータ識別子を、入力として受け取るデータ識別子の代わりとしてもよい。

【0030】

===暗号化方法決定部105===

暗号化方法決定部105は、入力部101が受け取るデータ識別子で識別されるデータに対応する有効期限までに解読されない暗号強度を持つ暗号化方法を識別できる暗号化方法識別子とその暗号化方法の暗号処理に必要なリソース量とを特定する。

【0031】

有効期限とは、対応するデータが秘匿される必要のなくなる日時を表す。

【0032】

暗号化方法決定部105は、入力部101が受け取るデータ識別子で識別されるデータごとに、対応する有効期限を特定してもよい。または、暗号化方法決定部105は、複数個のデータ識別子について、一つの有効期限を特定してもよい。または、入力部101が、データ識別子の一つ一つについてそれぞれそのデータの有効期限を受け取ってもよいし、複数個のデータ識別子について一つの有効期限を受け取ってもよい。この場合、暗号化方法決定部105は、入力部101が受け取るデータの有効期限に基づいて各データの有効期限を特定する。または、データ配信装置100が備える他のユニットが、各データに含まれる情報に基づいてそのデータの有効期限を算出してもよい。この場合、暗号化方法決定部105は、算出されたデータの有効期限に基づいて各データの有効期限を特定する

10

20

30

40

50

。

【0033】

暗号化方法とは、暗号アルゴリズムの種類、鍵長などの暗号アルゴリズムのパラメータ、暗号アルゴリズムを実行するハードウェアの情報などの少なくともいずれか、またはこれらの組み合わせである。また暗号化方法は、後述の暗号化部106による暗号化処理の手順を指定する情報である。

【0034】

暗号強度とは、第三者が暗号データを解読する、すなわち暗号鍵を用いずに暗号データを復号する、ために必要な期間を示す時間情報である。また、処理時間は、データ配信装置100がデータをその暗号化方法を用いて暗号化するのに要する時間情報である。前述のリソース量とは、例えば処理時間を示す情報であってもよい。これは一例であって、リソース量は、処理時間を示す情報に限られない。例えばデータ配信装置100は、CPUおよびメモリを含み、図1に示される各部は、プログラム制御に基づく処理に対応する機能に相当するものとする。この場合、リソース量とは、CPU使用量、メモリ使用量、などを含んでもよい。

【0035】

暗号化方法識別子は、データ配信装置100がデータを暗号化する暗号化方法を識別できる識別子である。

【0036】

暗号化方法決定部105は、暗号化方法を識別できる暗号化方法識別子と、その暗号化方法の暗号化処理に必要なリソース量とを含む暗号化方法特徴情報をあらかじめ記憶してもよい。または、暗号化方法決定部105は、図示しない暗号化方法記憶部から、暗号化方法を識別できる暗号化方法識別子と、その暗号化方法の暗号化処理に必要なリソース量とを含む暗号化方法特徴情報を読み出してもよい。

【0037】

図2は、この暗号化方法記憶部が記憶する暗号化方法特徴情報の一例を示す図である。図2に示されるように、暗号化方法記憶部は、各暗号化方法識別子T101とそれぞれに対応する暗号強度T102とそれぞれの暗号化に要するリソース量として処理時間T103とを対応付けて記憶する。

【0038】

データ配信装置100は、例えば、データに何の暗号化処理も行わずそのまま処理することを一つの暗号化方法として扱ってもよい。この場合、暗号化方法の暗号強度およびリソース量（処理時間）は、ともに0となる。

【0039】

暗号化方法記憶部が記憶する各暗号化方法特徴情報は、あらかじめ入力され記憶されてもよい。または各暗号化方法特徴情報は、データ配信装置100のユーザに入力される情報であってもよい。

【0040】

暗号化方法決定部105は、入力部101が受け取った有効期限と、暗号化方法決定部105または暗号化方法記憶部が記憶している暗号化方法特徴情報に含まれる暗号強度とを比較する。そして暗号化方法決定部105は、暗号強度が現時刻から有効期限までの期間より長い暗号化方法を特定する。有効期限が T_a 、現時刻が T_0 、暗号強度が T_e であると仮定する。このとき暗号化方法決定部105は、 $T_a - T_0 < T_e$ を満たす暗号化方法を特定する。

【0041】

暗号化方法決定部105は、特定した暗号化方法に対応する暗号化方法特徴情報を後述の暗号化方法評価部104に渡す。

【0042】

===暗号化方法評価部104===

暗号化方法評価部104は、暗号化方法決定部105から暗号化方法特徴情報を受け取

10

20

30

40

50

る。そして暗号化方法評価部 104 は、暗号化方法特徴情報に含まれるリソース量に基づいて、リソース消費量評価値を算出する。

【0043】

リソース消費量評価値は、各暗号化方法が選択される優先度を示す情報である。またこのリソース消費量評価値は、単に暗号化方法特徴情報に含まれる 1 つのリソースのリソース量の値であってもよいし、複数のリソースのリソース量の値をパラメータに取る関数に基づいて求められる値であってもよい。第一の実施の形態では暗号化方法特徴情報のうち、暗号化処理に要する処理時間の大きさの逆数が、リソース消費量評価値であると仮定する。

【0044】

暗号化方法評価部 104 は、算出したリソース消費量評価値に基づいてリソース量に対応する暗号化方法識別子を特定する。例えば、高いリソース消費量評価値は、優先度が高いことを示す場合に、暗号化方法評価部 104 は、リソース消費量評価値が最高であるリソース量に対応する暗号化方法識別子を特定してもよい。あるいは、低いリソース消費量評価値は、優先度が高いことを示す場合に、暗号化方法評価部 104 は、リソース消費量評価値が最低であるリソース量に対応する暗号化方法識別子を特定してもよい。

【0045】

暗号化方法評価部 104 が特定した暗号化方法識別子は、後述の暗号化部 106 によって用いられる。

【0046】

暗号化方法評価部 104 は、特定した暗号化方法識別子を、入力部 101 が受け取るデータ識別子とそのデータの有効期限とそのデータの宛先と対応付けて図示しない暗号データ情報記憶部に記憶してもよい。

【0047】

=== 暗号化部 106 ===

暗号化部 106 は、入力部 101 が受け取るデータ識別子で識別されるデータを、暗号化方法評価部 104 が特定した暗号化方法識別子で識別される暗号化方法によって暗号化する。

【0048】

=== 配信部 107 ===

配信部 107 は、暗号化部 106 が暗号化したデータである暗号化データを配信する。

【0049】

=== 暗号化方法伝達部 108 ===

暗号化方法伝達部 108 は、配信部 107 が暗号化データを配信する際に、次の二つの条件の少なくともいずれかが満たされるか否かを判定する。そして暗号化方法伝達部 108 は、前述の二つの条件の少なくともいずれかが満たされると判定した場合に、前述の暗号化データの配信先に、暗号化データに適用された暗号化方法の暗号化方法識別子を送信する。

【0050】

前述の二つの条件の第一の条件は、入力部 101 が受け取った、その暗号化データの元となるデータの有効期限がすでに経過していることである。前述の二つの条件の第二の条件は、その暗号化データが、入力部 101 が受け取ったその暗号化データの元となるデータの宛先で示される配信先に、配信部 107 によって配信されることである。

【0051】

暗号化方法伝達部 108 は、配信部 107 が暗号化データを配信する際に、その暗号化データの元となるデータのデータ識別子に対応付けられている有効期限と暗号化方法識別子と宛先とを前述の暗号データ情報記憶部から読み出してもよい。そして暗号化方法伝達部 108 は、読み出した有効期限および宛先に基づいて前述の二条件が成立するか否かを判定し、その読み出した暗号化方法識別子を暗号化データの配信先に送信してもよい。

【0052】

10

20

30

40

50

暗号化方法伝達部 108 が暗号化方法識別子を配信する方法は、特に限定されない。例えば、特許文献 1 に記載されているように、暗号化方法伝達部 108 が暗号化方法識別子の配信先の公開鍵を取得し、この公開鍵を用いて暗号化データを生成する際に用いられた暗号化方法の暗号化方法識別子や暗号鍵を暗号化してもよい。そして暗号化方法伝達部 108 は暗号化したデータを配信してもよい。また例えば、暗号化方法伝達部 108 は、暗号化方法識別子を暗号化データに付加してもよい。この場合、配信部 107 は、暗号化方法識別子が付加された暗号化データを配信する。

【0053】

第一の実施の形態において、入力部 101 は、データ入力部 1011 と、有効期限入力部 1012 と、宛先入力部 1013 とを備えてもよい。データ入力部 1011 は、データ識別子を受け取る。有効期限入力部 1012 は、データ入力部 1011 が受け取るデータの有効期限を受け取る。宛先入力部 1013 は、データ入力部 1011 が受け取るデータの配信先を示す宛先を受け取る。図 3 は、入力部 101 の構成の一例を示すブロック図である。

【0054】

データ入力部 1011 は、第三者から秘匿するデータである平文データを入力として受け取ってもよい。この場合、データ入力部 1011 は、平文データとともにそのデータを識別できるデータ識別子を受け取ってもよい。あるいは、データ入力部 1011 は、受け取った平文データに基づいてその平文データを識別できるデータ識別子を生成してもよい。そして、データ入力部 1011 が生成したデータ識別子は、入力部 101 が受け取るユーザ識別子とみなされてもよい。

【0055】

なお、第一の実施の形態におけるデータ配信装置 100 の各構成要素の物理的な構成に関しては、特に限定されない。データ配信装置 100 の各構成要素の典型的な構成の例として、全ての構成要素が単一のコンピュータ上にあってもよい。または各構成要素が別個のコンピュータ上にあり、各構成要素間はネットワークで接続されてもよい。

【0056】

図 4 は、本発明の第一の実施の形態におけるデータ配信装置 100 の動作の概要を示すフローチャートである。

【0057】

入力部 101 は、データ識別子とそのデータの有効期限とそのデータの配信先を示す宛先とを受け取る（ステップ S101）。入力部 101 は、データ識別子に対応するデータを受け取ってもよい。

【0058】

暗号化方法決定部 105 は、入力部 101 から有効期限を受け取る。そして暗号化方法決定部 105 は、受け取った有効期限までに解読されない暗号強度を持つ暗号化方法を識別できる暗号化方法識別子とその暗号化方法の暗号処理に必要なリソース量とを特定する（ステップ S102）。

【0059】

例えば、暗号化方法決定部 105 は、図示しない暗号化方法記憶部に記憶されている各暗号化方法のうち暗号強度が現時刻から有効期限までの期間より長いものを示すもの、すなわち、 $T_a - T_0 < T_e$ を満たす暗号化方法を特定してもよい。なお有効期限が T_a 、現時刻が T_0 、暗号強度が T_e である。そして暗号化方法決定部 105 は、特定した暗号化方法を示す暗号化方法識別子とリソース量とを含む暗号化方法特徴情報を暗号化方法記憶部から読み出してもよい。

【0060】

暗号化方法決定部 105 は、受け取った有効期限までに解読されない暗号強度を持つ暗号化方法を識別できる暗号化方法識別子とその暗号化方法の暗号処理に必要なリソース量とがあるか否か判定する（ステップ S103）。前述の条件を満たす暗号化方法がない場合（ステップ S103 の “No”）、データ配信装置 100 は、以下の処理を実行する。

すなわちデータ配信装置100は、データの暗号化および暗号化されたデータの配信を取りやめ、有効期限までの秘匿性を保証できる暗号化方法がないことを示す情報を出力する（ステップS104）。例えばこの情報は、このデータ配信装置100のユーザに対するエラーメッセージであってもよい。

【0061】

前述の条件を満たす暗号化方法がある場合（ステップS103の“Y e s”）、暗号化方法決定部105は、前述の条件を満たす暗号化方法が複数あるか否か判定する（ステップS105）。前述の条件を満たす暗号化方法が複数ある場合（ステップS105の“Y e s”）、暗号化方法決定部105は、その複数の暗号化方法の暗号化方法識別子を含む暗号化方法特徴情報を暗号化方法評価部104に渡す。暗号化方法評価部104は、受け取った暗号化方法特徴情報に含まれるリソース量に基づいて、リソース消費量評価値を算出する（ステップS106）。そして暗号化方法評価部104は、算出されるリソース消費量評価値に基づいてリソース量に対応する暗号化方法識別子を特定する（ステップS107）。 10

【0062】

一方、前述の条件を満たす暗号化方法が複数ないと判定した場合（ステップS105の“N o”）、データ配信装置100は、暗号化方法決定部105が特定した暗号化方法識別子を、暗号化方法評価部104が特定した暗号化方法識別子であるとみなす。そしてデータ配信装置100の処理はステップS108へ進む。

【0063】

なお、ステップS103における処理とステップS105における処理とは順序が入れ替わってもよいし、並列に行われてもよい。 20

【0064】

暗号化部106は、入力部101が受け取ったデータ識別子で識別されるデータを、ステップS107の処理において暗号化方法評価部104が特定した暗号化方法識別子で識別される暗号化方法によって暗号化する（ステップS108）。または、暗号化部106は、入力部101が受け取ったデータを、ステップS107の処理において暗号化方法評価部104が特定した暗号化方法識別子で識別される暗号化方法によって暗号化してもよい。配信部107は、暗号化部106が暗号化した暗号化データを配信する（ステップS109）。 30

【0065】

暗号化方法伝達部108は、配信部107が暗号化データを配信する際に、次の二つの条件の少なくともいずれかが満たされるか否か判定する（ステップS110）。第一の条件は、その暗号化データのもとになるデータの有効期限をすでに経過していることである。この有効期限は、入力部101が受け取る情報である。第二の条件は、前述の暗号化データが、その暗号化データのもとになるデータの宛先で示される配信先に配信されることである。この宛先は、入力部101が受け取る情報である。

【0066】

暗号化方法伝達部108は、前述の二条件の少なくともいずれかが満たされる場合（ステップS110の“Y e s”）、以下の処理を実行する。すなわち暗号化方法伝達部108は、前述の暗号化データの配信先に、ステップS107の処理において暗号化方法評価部104が特定した暗号化方法識別子を送信する（ステップS111）。一方、前述の二条件のいずれもが満たされない場合（ステップS110の“N o”）、データ配信装置100の処理は終了する。 40

【0067】

図5は、暗号化方法決定部105および暗号化方法評価部104が暗号化方法を決定する過程の具体例を示すフローチャートである。入力部101に有効期限として「10/06/18 17:14:59」が入力される（ステップS151）。このとき、暗号化方法決定部105は、まず現在時刻から有効期限までの時間を算出する（ステップS152）。例えば現在時刻が「10/06/18 11:45:00」とすると、有効期限まで 50

の時間は「05:29:59」となる。次に、暗号化方法決定部105は、図示しない暗号化方法記憶部から、暗号強度が有効期限までの時間以上を示す暗号化方法を特定する（ステップS153）。図2に示される暗号化方法特徴情報の例の場合、「アルゴリズムA」（T111）、「アルゴリズムB、128bit」（T112）、「アルゴリズムB、256bit」（T113）の3つが十分な暗号強度を持つものとして特定される。次に、暗号化方法決定部105は、特定された暗号化方法が複数であるか否か判定する（ステップS154）。特定された暗号化方法が2つ以上なので（ステップS154の“Y e s”）、暗号化方法評価部104は、特定された暗号化方法のリソース消費量評価値を求める（ステップS155）。本例の場合、「アルゴリズムA」のリソース消費量評価値は1、「アルゴリズムB、128bit」のリソース消費量評価値は1/3、「アルゴリズムB、256bit」のリソース消費量評価値は1/15である。結果、暗号化方法評価部104は、より高いリソース消費量評価値を示す「アルゴリズムA」を暗号化方法として特定する（ステップS156）。

10

【0068】

なお、ステップS154の処理において、特定された暗号化方法が複数でないと判定された場合（ステップS154の“N o”）、暗号化方法決定部105および暗号化方法評価部104の処理は終了する。

【0069】

第一の実施の形態におけるデータ配信装置100は、データ識別子と有効期限と宛先とを受け取ると、その有効期限までには解読されない暗号強度を持つ暗号化方法を特定する。そしてデータ配信装置100は、特定した暗号化方法のうち、各暗号化方法の暗号処理において必要となるリソース量に基づいて算出されるリソース消費量評価値を算出する。データ配信装置100は、リソース消費量評価値に基づいて暗号化方法を特定し、その暗号化方法によって前述のデータ識別子で識別されるデータを暗号化する。データ配信装置100は、暗号化したデータを配信する。この際にデータ配信装置100は、以下の二条件のうちの少なくとも一方を満たす場合に、前述のデータの暗号化に適用された暗号化方法を識別できる暗号化方法識別子を前述の宛先を示す配信先へ送信する。第一の条件は、有効期限を経過していることである。第二の条件は、前述の宛先が示す配信先に前述の暗号化したデータを配信することである。

20

【0070】

この構成により第一の実施の形態におけるデータ配信装置100は、データを暗号化する際、有効期限には解読されない暗号強度を持つ暗号化方法のうち、例えばリソース消費量が最も小さい暗号化方法によってデータを暗号化できる。

30

【0071】

またデータ配信装置100は、暗号化されたデータの有効期限が経過していない場合には、そのデータの正当な宛先に対してそのデータに適用された暗号化方法を識別できる暗号化方法識別子を送信する。一方、データ配信装置100は、暗号化されたデータの有効期限が経過している場合には、すべての配信先に対して前述の暗号化方法識別子を送信する。よってデータ配信装置100が配信するデータは、次の特徴を持つ。有効期限以前において、正当な配信先である宛先の装置がそのデータを復号でき、有効期限経過後において、すべての装置がそのデータを復号できる。したがってデータ配信装置100は、データの有効期限までの秘匿性を維持しつつ有効期限後のデータの有効利用性を保証できる。

40

【0072】

〔第一の実施の形態の第一の変形例〕

第一の実施の形態において、データ配信装置100は、前述の暗号化方法記憶部を暗号化方法記憶部103として備えてもよい。図6は、第一の実施の形態の第一の変形例におけるデータ配信装置100の構成の一例を示すブロック図である。

【0073】

〔第一の実施の形態の第二の変形例〕

第一の実施の形態または第一の実施の形態の第一の変形例において、データ配信装置1

50

00は、前述の暗号データ情報記憶部を暗号データ情報記憶部110として備えてもよい。図7は、第一の実施の形態の第二の変形例におけるデータ配信装置100の構成の一例を示すブロック図である。

【0074】

[第一の実施の形態の第三の変形例]

第一の実施の形態において、データ配信装置100は、暗号強度算出部109を備えてもよい。図8は、第一の実施の形態の第三の変形例におけるデータ配信装置100の構成の一例を示すブロック図である。

【0075】

===暗号強度算出部109===

暗号強度算出部109は、図示しない他の機能手段からある暗号化方法を示す暗号化方法識別子を受け取る。そして暗号強度算出部109は、受け取った暗号化方法識別子で識別できる暗号化方法に基づいて暗号強度を算出する。例えば暗号強度算出部109は、差分解読法や線形解読法などの暗号解読法に対する強度指標を求め、それらの値に基づき解読に要する時間を見積もってもよい。例えば暗号強度算出部109は、非特許文献1に記載されている方法を用いてもよい。強度指標とは、例えば差分解読法に対しては、「最大差分特性確率」、「差分特性確率」または「平均差分確率」のことであり、線形解読法に対しては、「最大線形特性確率」、「線形特性確率」または「平均線形確率」のことである。

【0076】

また暗号強度算出部109は、受け取った暗号化方法識別子に基づいて対応する暗号化方法の暗号化処理に必要となるリソース量を算出する。例えば暗号強度算出部109は、あらかじめ用意されている平文データに対して、その暗号化方法を用いて暗号化処理を行い、その際の各リソースの消費量をリソース量として算出してもよい。

【0077】

そして暗号強度算出部109は、算出した暗号強度とリソースの量と受け取った暗号化方法識別子とを暗号化方法決定部105に渡す。暗号化方法決定部105は、暗号強度算出部109から受け取る暗号強度とリソース量と暗号化方法識別子とを対応付けて記憶してもよい。そして暗号化方法決定部105は、入力部101が受け取る有効期限までに解読されない暗号強度を持つ暗号化方法を識別できる暗号化方法識別子を、暗号強度算出部109から受け取る暗号化方法識別子から特定してもよい。

【0078】

暗号強度算出部109は、算出した暗号強度と特定したリソース量とを、受け取った暗号化方法識別子と対応付けて暗号化方法特徴情報として図示しない暗号化方法記憶部に記憶してもよい。

【0079】

第一の実施の形態の第三の変形例におけるデータ配信装置100は、使用可能な暗号化方法をユーザが任意に追加することが可能となる。

【0080】

[第二の実施の形態]

図9は、本発明の第二の実施の形態におけるデータ配信装置200の構成の一例を示すブロック図である。

【0081】

図9を参照すると、データ配信装置200は、入力部101と、暗号化方法記憶部203と、暗号化方法評価部204と、暗号化方法決定部205と、暗号化部106と、暗号配信部107と、暗号化方法伝達部108と、暗号データ情報記憶部210と、負荷情報取得部211と、リソース消費量評価値算出方法記憶部212と、を備える。図9に示されるように、データ配信装置200は、第一の実施の形態におけるデータ配信装置100に、暗号化方法記憶部203と、暗号データ情報記憶部210と、負荷情報取得部211と、リソース消費量評価値算出方法記憶部212とを備える装置である。

【0082】

第一の実施の形態におけるデータ配信装置100は、有効期限までには解読されない暗号強度を持つ暗号化方法の中から、リソース消費量評価値が最大のリソース量に対応付けられる暗号化方法を用いてデータの暗号化を行っていた。しかし例えばCPU使用率に余力がある場合には、よりメモリ消費量が小さい暗号化方法を用いることでメモリ使用量も抑制したい、といった場合も考えられる。すなわちリソースの使用状況によって使用する暗号化方法に対するリソース消費量の評価基準が変化する場合も考えられる。そこで第二の実施の形態では、暗号化部106が暗号化処理に用いるリソースの負荷を、負荷情報取得部211が監視する。この監視の結果に応じて暗号化方法評価部204が、リソース消費量評価値の算出方法を動的に選択する。これによりデータ配信装置200は、リソースの使用状況に応じてより適切な暗号化方法の選択を行うことができる。また、例えばデータ配信装置200の物理構成がネットワークで接続された複数のコンピュータである場合に、負荷情報取得部211は、ネットワークを介して各コンピュータの負荷情報を収集してもよい。

10

【0083】

以下では、第二の実施の形態において第一の実施の形態とは異なる構成について詳しく説明する。

【0084】

=== 負荷情報取得部211 ===

負荷情報取得部211は、暗号化部106が暗号化処理を行うために用いるリソースの負荷情報をその暗号化部106を備えるデータ配信装置200から取得する。リソースの負荷情報は、例えば、CPUや暗号化処理専用のチップの使用率、メモリ使用量、データ配信装置200の消費電力や残電力などであってもよい。または、リソースの負荷情報は、通信量、暗号化処理専用のチップの使用量であってもよい。または、リソースの負荷情報は、暗号化部106で暗号化されるデータの処理待ち行列長、配信部107で配信される暗号化データの配信待ち行列長であってもよい。

20

【0085】

以下の説明では、リソースの負荷情報は、CPU使用率である。前述のリソースの負荷情報は例示であり、リソースの負荷情報は、前述の情報に限られない。

【0086】

負荷情報取得部211は、取得したリソースの負荷情報を後述の暗号化方法評価部204に渡す。

30

【0087】

=== リソース消費量評価値算出方法記憶部212 ===

リソース消費量評価値算出方法記憶部212は、1つ以上のリソース消費量評価値算出方法と、各リソース消費量評価値算出方法が用いられる条件である適用条件とを対応付けて記憶する。

【0088】

図10は、リソース消費量評価値算出方法記憶部212が記憶するリソース消費量評価値算出方法の一例を示す図である。図10に示されるように、本実施形態におけるリソース消費量評価値算出方法記憶部212は、リソース消費量評価値算出方法(T302)と各算出方法の適用条件(T301)との組を記憶している。適用条件とは、暗号化部106が暗号化処理を行うために用いるリソースの条件を示す情報である。例えば図10に示されるように、適用条件とは、CPU使用率が所定の値未満である、または所定の値の範囲内である、またはCPU使用率が前述の条件を満たさない場合、という条件をそれぞれ示す情報であってもよい。

40

【0089】

=== 暗号化方法記憶部203 ===

暗号化方法記憶部203は、図11に示されるように、各暗号化方法の暗号化方法特徴情報として、暗号化処理に要するリソースの使用量を含む情報を記憶する。例えば図11

50

に示されるように暗号化方法記憶部 203 は、各暗号化方法の暗号化方法特徴情報に含まれるリソースの使用量として、メモリ使用量(T204)を記憶する。リソースの使用量は、CPU使用率、ハードディスクドライブ(Hard Disk Drive: HDD)使用率あるいはメモリ使用量などが挙げられるが、これらに限られない。

【0090】

===暗号データ情報記憶部 210===

暗号データ情報記憶部 210 は、データ識別子とデータの有効期限とデータの宛先と暗号化方法識別子とを対応付けて記憶する。暗号データ情報記憶部 210 が記憶するデータ識別子は、入力部 201 が受け取るデータ識別子である。暗号データ情報記憶部 210 が記憶するデータの有効期限は、その有効期限に対応付けられるデータ識別子で識別されるデータの有効期限である。暗号データ情報記憶部 210 が記憶するデータの宛先は、その宛先に対応付けられるデータ識別子で識別されるデータの宛先である。暗号データ情報記憶部 210 が記憶する暗号化方法識別子は、その暗号化方法識別子に対応付けられる有効期限に基づいて特定された各リソース量のうち、算出されたリソース消費量評価値に基づいてリソース量に対応する暗号化方法識別子である。暗号化方法決定部 205 は前述の有効期限に基づいてリソース量を特定する。暗号化方法決定部 205 が特定したリソース量ごとに、暗号化方法評価部 204 はリソース消費量評価値を算出する。

【0091】

===暗号化方法評価部 204===

暗号化方法評価部 204 は、負荷情報取得部 211 からリソースの負荷情報を受け取る。そして暗号化方法評価部 204 は、受け取ったリソースの負荷情報に基づいて、リソース消費量評価値算出方法記憶部 212 が記憶するリソース消費量評価値算出方法の適用条件を満たすか否かそれぞれ判定する。そして暗号化方法評価部 204 は、適用条件が受け取ったリソースの負荷情報と合致するリソース消費量評価値算出方法を選択する。

【0092】

そして暗号化方法評価部 204 は、選択したリソース消費量評価値算出方法に基づいて、各暗号化方法のリソース消費量評価値を算出する。具体的には暗号化方法評価部 204 は、暗号化方法決定部 205 から暗号化方法特徴情報を受け取る。そして暗号化方法評価部 204 は、暗号化方法特徴情報に含まれるリソース量に基づいて、各暗号化方法のリソース消費量評価値を算出する。

【0093】

暗号化方法評価部 204 は、算出したリソース消費量評価値に基づいてリソース量に対応する暗号化方法識別子を、入力部 101 が受け取るデータ識別子とそのデータの有効期限とそのデータの宛先と対応付けて暗号データ情報記憶部 210 に記憶する。

【0094】

図 12 は、暗号化方法評価部 204 が適切なリソース消費量評価値算出方法を選択する過程、および、選択されたリソース消費量評価値算出方法に基づいて暗号化方法評価部 204 が暗号化方法を特定する過程の具体例を示すフローチャートである。

【0095】

暗号化方法評価部 204 は、負荷情報取得部 211 からリソースの負荷情報である CPU 使用率として、例えば 50% という値を取得する(ステップ S251)。暗号化方法評価部 204 は、図 10 に示されるリソース消費量評価値算出方法記憶部 212 が記憶しているリソース消費量評価値算出方法の適用条件のうち、受け取ったリソースの負荷情報(CPU 使用率)が満たす適用条件を特定する(ステップ S252)。

【0096】

その結果、受け取った CPU 使用率は、「30% < [CPU 使用率] < 70%」の適用条件(T321)に合致する。よって、暗号化方法評価部 204 は、合致した適用条件に対応する「100 / [メモリ使用量] + 1 / [計算コスト]」というリソース消費量評価値算出方法(T322)を選択する(ステップ S253)。

【0097】

このとき暗号化方法決定部 205 は、選択されたリソース消費量評価値算出方法を用いて、十分な暗号強度を持つ各暗号化方法のリソース消費量評価値を算出する（ステップ S254）。例えば、図 11 に示される暗号化方法のうち、「アルゴリズム A」（T211）、「アルゴリズム B、128 bit」（T212）、「アルゴリズム B、256 bit」（T213）が十分な暗号強度であった場合を仮定する。

【0098】

この場合、暗号化方法評価部 204 は、選択された前述のリソース消費量評価値算出方法を用いて 3 つの暗号化方式のリソース消費量評価値を算出する。その結果、「アルゴリズム A」のリソース消費量評価値は 2、「アルゴリズム B、128 bit」のリソース消費量評価値は 5.83、「アルゴリズム B、256 bit」のリソース消費量評価値は 2.07 となる。よって暗号化方法評価部 204 は、「アルゴリズム B、128 bit」を

10

【0099】

以上のように、第二の実施の形態によれば、データ配信装置 200 は、暗号化処理に用いるリソースの使用状況に応じて、暗号化方法を選択する際に考慮するリソースの種類やその評価方法を変更する。したがって第二の実施の形態におけるデータ配信装置 200 は、より柔軟で効率的なリソース消費量の抑制を行うことができる。

【0100】

例えば、第二の実施の形態におけるデータ配信装置 200 は、暗号化処理の際にボトルネックとなるリソースに応じて、暗号化に用いる暗号化方法を特定する。具体的にはデータ配信装置 200 は、ボトルネックとなるリソースの消費量が小さい暗号化方法を暗号化に用いる暗号化方法と特定する。よって、データ配信装置 200 は、暗号化部 106 を備えるデータ配信装置 200 が備えるリソースを最大限活用できる。

20

【0101】

〔第二の実施の形態の第一の変形例〕

第二の実施の形態において、負荷情報取得部 211 は、暗号化部 106 が暗号化処理を行うために用いるリソースの負荷情報以外の他の情報を取得してもよい。そして、リソース消費量評価値算出方法記憶部 212 が記憶する適用条件は、リソースの条件を示す情報以外の情報を含んでもよい。また、暗号化方法評価部 204 は、受け取ったリソースの負荷情報と前述の他の情報とに基づいて、リソース消費量評価値算出方法記憶部 212 が記憶するリソース消費量評価値算出方法の適用条件を満たすか否かそれぞれ判定する。そして暗号化方法評価部 204 は、適用条件が、受け取ったリソースの負荷情報と前述の他の情報とで特定される所定の条件と合致するリソース消費量評価値算出方法を選択してもよい。

30

【0102】

負荷情報取得部 211 は、前述の他の情報として、データ配信装置 200 が使用するネットワークの遅延を示す情報、データロス率を示す情報または、パケットロス率を示す情報を受け取ってもよい。または負荷情報取得部 211 は、暗号化部 106 を備えるデータ配信装置 200 が暗号化処理専用のチップを備えているか否かを示す情報、暗号化処理を行う前後のデータ長の変化率を示す情報、通信量を受け取ってもよい。

40

【0103】

リソース消費量評価値算出方法記憶部 212 は、1 つ以上のリソース消費量評価値算出方法と、各リソース消費量評価値算出方法が用いられる条件である適用条件とを対応付けて記憶する。

【0104】

第二の実施の形態の第一の変形例におけるデータ配信装置 200 は、データ配信装置 200 自身以外のリソースまたはネットワークの状況に応じて、暗号化に用いる暗号化方法を特定する。よって、データ配信装置 200 は、データ配信装置 200 自身を含むシステム全体のリソースを最大限活用できる。

【0105】

50

〔第三の実施の形態〕

図 1 3 は、本発明の第三の実施の形態におけるデータ配信装置 3 0 0 の構成例を示すブロック図である。図 1 3 に示されるように、第三の実施の形態におけるデータ配信装置 3 0 0 は、第一の実施の形態におけるデータ配信装置 1 0 0 に、有効期限算出部 3 0 2 と、有効期限ルール記憶部 3 1 4 とをさらに備える点が異なる。

【0 1 0 6】

第一の実施の形態におけるデータ配信装置 1 0 0 および第二の実施の形態におけるデータ配信装置 2 0 0 は、データの有効期限を入力として受け取る場合がある。しかし、データの有効期限が、そのデータをデータ配信装置に配信した装置が取得できない情報に基づいて決められる場合がある。あるいは、データをデータ配信装置に配信した装置が低コストまたは低機能のセンサであるなどの理由により、その装置がデータの有効期限をデータ配信装置に入力する能力を持たない場合がある。なお、第一の実施の形態におけるデータ配信装置 1 0 0 および第二の実施の形態におけるデータ配信装置 2 0 0 は、総称してデータ配信装置と表される。これらの場合、データ配信装置は、データをデータ配信装置に配信した装置からその装置の有効期限を受け取ることが困難である。

【0 1 0 7】

そこで、第三の実施の形態では、入力部 3 0 1 が有効期限算出ルールを入力として受け取り、有効期限算出ルール記憶部 3 1 4 がその有効期限算出ルールを記憶する。有効期限算出部 3 0 2 は、有効期限算出ルール記憶部 3 1 4 に記憶されている有効期限算出ルールに基づきデータを解析することによって、そのデータの有効期限を算出する。暗号化方法決定部 3 0 5 は、有効期限算出部 3 0 2 が算出した有効期限までに解読されない暗号強度に対応付けられている暗号化方法識別子とその暗号化方法識別子に対応付けられているリソース量とを図示しない暗号化方法記憶部から読み出す。これにより、第三の実施の形態におけるデータ配信装置 3 0 0 は、データを配信してきた装置がそのデータの有効期限をデータ配信装置 3 0 0 に入力することができない場合でも、適切なデータの有効期限を算出できる。よって第三の実施の形態におけるデータ配信装置 3 0 0 は、算出したデータの有効期限に応じて適切な暗号化方法を選択することができる。

【0 1 0 8】

以下では、第三の実施の形態において第一の実施の形態とは異なる構成について詳しく説明する。

【0 1 0 9】

=== 入力部 3 0 1 ===

入力部 3 0 1 は、入力部 1 0 1 が備える機能に加え、有効期限算出ルールを入力として受け取る。有効期限算出ルールの詳細な説明は、後述される。

【0 1 1 0】

入力部 3 0 1 は、受け取った有効期限算出ルールを後述の有効期限算出ルール記憶部 3 1 4 に記憶する。

【0 1 1 1】

入力部 3 0 1 は、有効期限算出ルールを入力として受け取る有効期限算出ルール入力部 3 0 1 4 を備えてもよい。図 1 4 は、入力部 3 0 1 の構成の一例を示すブロック図である。図 1 4 を参照すると、入力部 3 0 1 は、図 3 に示される入力部 1 0 1 の構成に加え、有効期限算出ルール入力部 3 0 1 4 をさらに含む。

【0 1 1 2】

=== 有効期限算出ルール記憶部 3 1 4 ===

有効期限算出ルール記憶部 3 1 4 は、入力部 3 0 1 から受け取った有効期限算出ルールを記憶する。図 1 5 は、有効期限算出ルール記憶部 3 1 4 が記憶する有効期限算出ルールの一例を示す図である。図 1 5 に示されるように、有効期限算出ルールは、ルールが適用されるための条件を示すルール適用条件 (T 4 0 1) と、そのルール適用条件に合致したデータを解析して有効期限を算出するための関数である有効期限算出関数 (T 4 0 2) とを含む。ルール適用条件 (T 4 0 1) は、「いずれのルール適用条件を満たさない場合」

を一つのルール適用条件（T 4 4 0）として含む。そして「いずれのルール適用条件を満たさない場合」に適用される有効期限算出関数（T 4 4 2）は、任意の平文データを解析することで有効期限を算出できる関数である。

【0 1 1 3】

=== 有効期限算出部 3 0 2 ===

有効期限算出部 3 0 2 は、有効期限算出ルール記憶部 3 1 4 に記憶されている有効期限算出ルールに基づいてデータを解析し、そのデータの有効期限を算出する。入力部 3 0 1 が、有効期限算出部 3 0 2 が解析するデータを受け取ってもよい。またはデータ配信装置が、有効期限算出部 3 0 2 が解析するデータを記憶してもよい。

【0 1 1 4】

有効期限算出部 3 0 2 がデータの有効期限を算出する手順の具体的な一例が以下に示される。例えば有効期限算出ルール記憶部 3 1 4 は、図 1 6 のような有効期限算出ルールを記憶している。そして、入力部 3 0 1 は、図 1 7 に示される平文データを受け取った場合を仮定する。

【0 1 1 5】

このとき、有効期限算出部 3 0 2 は、有効期限算出ルール記憶部 3 1 4 が記憶している各有効期限算出ルールについて、前述の平文データがルール適用条件に合致するか否か判定する。

【0 1 1 6】

この場合、入力部 3 0 1 に入力された平文データは、図 1 6 に示される ‘Event.type= “人” ’、‘Event.type= “人” && Event.位置’、‘default’ の各ルール適用条件に合致する。よって有効期限算出部 3 0 2 は、それぞれのルール適用条件に対応する有効期限算出関数に基づいて平文データの有効期限を算出する。

【0 1 1 7】

結果、それぞれ "2010.07.30 09:20:00", "2010.08.01 09:17:15", "2010.07.25 09:20:03"（＝現在時刻）というデータの有効期限の候補が算出される。有効期限算出部 3 0 2 は、算出結果のうち最も後の時刻である "2010.08.01 09:17:15" をこの平文データの有効期限と算出する。

【0 1 1 8】

なお、上述の例では、図 1 7 に示されるように平文データが x m l（Extensible Markup Language）で記述されている。そして、x m l 形式のデータから、所定の要素の有無、その要素が有する属性の有無、要素の値、および要素が有する属性の値の少なくとも一つの情報の条件がルール適用条件である。また、x m l 形式のデータから所定の要素の有無、その要素が有する属性の有無、要素の値、および要素が有する属性の値の少なくとも一つの情報に基づいた演算を規定する関数が有効期限算出関数である。そして x m l 形式のデータから所定の要素の有無、その要素が有する属性の有無、要素の値、および要素が有する属性の値の少なくとも一つの情報と、ルール適用条件と、有効期限演算関数とに基づいて、条件判定や有効期限の算出が行われる。これらはあくまで一例であり、例えば有効期限算出部 3 0 2 は、自然言語で記述された平文データに対して、意味解析などを用いて平文データに含まれる情報を抽出し、抽出した情報に基づいて、ルール適用条件の判定や、有効期限の算出を行ってもよい。

【0 1 1 9】

さらに、平文データのフォーマットを示すデータの種類の種類がルール適用条件に含まれてもよい。例えば、平文データが x m l で記述されているものか、自然言語で記述されているものかを示す情報がルール適用条件に含まれてもよい。

【0 1 2 0】

また、各フォーマットの平文データに含まれる情報を解析する手順を示す情報は、ルール適用条件および有効期限算出関数に含まれてもよい。または、データ配信装置 3 0 0 は、それぞれのフォーマットで記述された平文データに対して、その平文データに含まれる情報を抽出するための手段を備えてもよい。

10

20

30

40

50

【0121】

図18は、有効期限算出部302がデータの有効期限を算出する手順の具体例を示すフローチャートである。

【0122】

有効期限算出部302は、入力部301が受け取る平文データを取得する（ステップS301）。次に、有効期限算出部302は、有効期限算出ルール記憶部314に記憶されている有効期限算出ルールのうち、ルール適用条件が平文データと合致するか否かを判定していない有効期限算出ルールがあるか否かを判定する（ステップS302）。

【0123】

ルール適用条件が平文データと合致するか否かを判定していない有効期限算出ルールがある場合（ステップS302の“Y e s”）、有効期限算出部302は、その有効期限算出ルールのいずれか一つを特定する（ステップS303）。有効期限算出部302は、平文データがステップS303にて特定した有効期限算出ルールのルール適用条件に合致するか否かを判定する（ステップS304）。平文データがルール適用条件に合致する場合（ステップS304の“Y e s”）、有効期限算出部302は、以下の処理を実行する。すなわち有効期限算出部302は、その有効期限算出ルールの有効期限算出関数に基づいて平文データを解析し、その有効期限算出ルールに基づいてその平文データの有効期限を算出する（ステップS305）。有効期限算出部302は、変数Tと、ステップS305にて算出した有効期限のうち遅い時刻を示す値を新たな変数Tの値と算出する（ステップS306）。そして有効期限算出部302の処理は、ステップS302へ戻る。一方、ステップS304の処理において、平文データがルール適用条件に合致しない場合（ステップS304の“N o”）、有効期限算出部302の処理は、ステップS302へ戻る。

【0124】

ステップS302の処理において、ルール適用条件が平文データと合致するか否かを判定していない有効期限算出ルールがない場合（ステップS302の“N o”）、有効期限算出部302は、以下の処理を実行する。すなわち有効期限算出部302は、ルール適用条件が合致する有効期限算出ルールがなかったか否かを判定する（ステップS307）。

【0125】

ルール適用条件が合致する有効期限算出ルールがなかった場合（ステップS307の“Y e s”）、有効期限算出部302は、以下の処理を実行する。すなわち有効期限算出部302は、有効期限算出ルール記憶部314に記憶されている、「いずれのルール適用条件を満たさない場合」に適用される有効期限算出関数に基づいて平文データを解析し、そのデータの有効期限を算出する（ステップS308）。そして有効期限算出部302は、算出した有効期限を変数Tの新たな値と算出する。一方、ルール適用条件が合致する有効期限算出ルールがあった場合（ステップS307の“N o”）、有効期限算出部302の処理は、ステップS309へ進む。

【0126】

有効期限算出部302は、上記手順によって算出された有効期限、すなわち変数Tの値を、平文データに対する有効期限として暗号化方法決定部305に渡す（ステップS309）。

【0127】

第三の実施の形態における暗号化方法決定部305は、有効期限算出部302が算出した有効期限をその平文データの有効期限として用いることによって、暗号化方法を選択する。

【0128】

第三の実施の形態におけるデータ配信装置300は、データを配信してきた装置がそのデータの有効期限をデータ配信装置300に入力することができない場合でも、適切なデータの有効期限を算出できる。よって第三の実施の形態におけるデータ配信装置300は、算出したデータの有効期限に応じて適切な暗号化方法を選択することができる。

【0129】

また第三の実施の形態におけるデータ配信装置 300 は、データを配信してきた装置がそのデータの有効期限を設定する必要がない。よって、データ配信装置 300 は、データを配信してきた装置が有効期限を設定するという手間を省くことができる。あるいは、データ配信装置 300 は、データを配信してきた装置が有効期限の設定を間違えるといった可能性を軽減できる。

【0130】

〔第三の実施の形態の第一の変形例〕

第三の実施の形態において、データ配信装置 300 は、入力部 301 が受け取るデータから、将来入力される平文データの有効期限の算出に用いられる可能性がある情報を抽出し記憶するデータ抽出部 315 を備えてもよい。図 19 は、第三の実施の形態の第一の変形例におけるデータ配信装置 300 の構成例を示すブロック図である。

10

【0131】

=== データ抽出部 315 ===

データ抽出部 315 は、入力部 301 が受け取るデータから、将来入力部 301 が受け取る平文データの有効期限の算出に用いられる可能性がある情報を抽出情報として抽出し記憶する。

【0132】

抽出情報とは、過去に入力部 301 が受け取ったデータのうち、ある項目における共通の情報であってもよい。特に抽出情報は、過去に入力部 301 が受け取ったデータのうち、ある個人に関連する情報を特定できる情報であってもよい。すなわち抽出情報は、特定の複数の抽出情報が組み合わせられることによって、ある所定の個人情報に推測されてしまう、何らかの情報であってもよい。

20

【0133】

例えば抽出情報とは、以下の情報を含む。過去に入力部 301 が受け取ったデータがある人物の位置情報を含む場合、抽出情報とは、所定の時間内に入力部 301 が受け取ったデータのうち所定の人物の位置情報であってもよい。所定の人物の位置情報を含むデータを所定の頻度以上入力部 301 が受け取ると、第三者がそれらのデータを組み合わせることによって、前述の所定の人物の行動を推定できてしまう。これに対処するため、データ配信装置 300 は、抽出情報が示す所定の人物の位置情報の個数が所定の閾値以上である場合に、対応するデータが第三者からより長期間秘匿されるように、適切な有効期限を設定する。例えば、データ配信装置 300 は、抽出情報が示す所定の人物の位置情報の個数が所定の閾値以上である場合に、対応するデータの有効期限を延長するように設定してもよい。

30

【0134】

データ抽出部 315 は抽出情報を有効期限算出部 302 に渡す。

【0135】

=== 有効期限算出部 302 ===

有効期限算出部 302 は、入力部 301 に入力されるデータと、過去に入力部 301 に入力されたデータからデータ抽出部 315 が抽出した抽出情報とに基づいて、そのデータの有効期限を算出する。

40

【0136】

例えば抽出情報が、所定の時間内に入力部 301 が受け取ったデータのうち所定の人物の位置情報を含んでいた場合、有効期限算出部 302 は以下の方法によってデータの有効期限を算出してもよい。有効期限算出部 302 は、入力部 301 に入力されるデータに基づいてそのデータの有効期限を算出する。この算出の具体的な方法は、第三の実施の形態における有効期限算出部 302 が行う算出方法と同様であってもよい。また、有効期限算出部 302 は、入力部 301 から受け取ったデータに含まれる抽出情報と共通する情報を示す抽出情報をデータ抽出部 315 から読み出す。そして有効期限算出部 302 は、算出した有効期限に読み出した抽出情報の個数を係数として掛け合わせることで新たな有効期限を算出してもよい。

50

【0137】

第三の実施の形態の第一の変形例におけるデータ配信装置300は、共通する情報を示す特定の抽出情報の個数が所定の閾値以上である場合に、対応するデータが第三者からより長期間にわたって秘匿されるように適切な有効期限を設定できる。

【0138】

以上、各実施の形態および実施例を参照して本発明を説明したが、本発明は上記実施の形態および実施例に限定されるものではない。本発明の構成や詳細には、本発明のScope内で当業者が理解しえる様々な変更をすることができる。

【0139】

また、本発明の各実施の形態または実施例における各構成要素は、その機能をハードウェア的に実現することはもちろん、コンピュータとプログラムとで実現することができる。プログラムは、磁気ディスクや半導体メモリなどのコンピュータ可読記録媒体に記録されて提供され、コンピュータの立ち上げ時などにコンピュータに読み取られる。この読み取られたプログラムは、そのコンピュータの動作を制御することにより、そのコンピュータを前述した各実施の形態または実施例における構成要素として機能させる。

【0140】

以下、本発明の関連技術について説明する。近年、人や物の現在の状況情報をセンサなどで観測または収集し、それらの情報を活用するコンテキストウェアサービスが現れはじめている。このようなサービスに用いられる状況情報の多くは、プライバシー情報を含むなどの理由により、不特定の第三者からは秘匿される必要がある。しかし、例えば今現在の自分の位置を不特定の第三者に知られたくないが、昨日行った場所を任意の人に公開し、新たな出会いやコミュニケーションのきっかけとしたいという場合もある。つまり、最新の状況情報を伝えるデータは、第三者から秘匿される必要がある一方で、観測から時間が経過したデータは、不特定の第三者に公開されてもよい、というケースも存在する。

【0141】

そのような、第三者から秘匿されたい期間が限られているようなデータを暗号化する場合、使用される暗号化方法は、そのデータの有効期限までには解読されない暗号強度さえ持っていれば十分である。更にいえば、それ以上の暗号強度を持った暗号化方法が用いられた場合、暗号化処理に必要な以上のリソースが消費されてしまい、他の処理が妨げられてしまう恐れがある。

【0142】

特許文献1は、エージェントの寿命までには解読されない暗号強度の暗号化方法を選択する技術を提示する。しかし特許文献1は、情報の秘匿性が持続する期間である有効期限への言及はない。つまり特許文献1に記載された技術は、暗号化方法を選択する際に機密情報の有効期限を考慮して処理を行う機能は備えていない。そのため、特許文献1に記載の技術は、例えばデータの有効期限がエージェントの寿命より短くてよい場合にも、エージェントの寿命相当の暗号強度をもつ暗号化方法を用いる必要があり、必要以上のリソースを消費してしまう。加えて、特許文献1に記載の技術は、エージェントの寿命までには解読されない暗号強度の暗号化方法が複数ある場合には、暗号化処理に要する時間計算量がより小さい暗号化方法を採用するのみである。つまり特許文献1に記載の技術は、その他のリソース消費の大小を考慮することはできない。

【0143】

さらに、特許文献1に記載された技術は、データを暗号化する際に暗号化データに基づいてエージェントを作成している。よって特許文献1に記載された技術は、暗号化データ生成時に、暗号化処理とエージェント作成処理とを必要とするので大きな負荷がかかる。また特許文献1に記載された技術は、データの有効期限後、エージェントにより削除される。よって特許文献1に記載された技術は、データの有効期限後の利用を考慮しておらず、暗号化データの有効期限後の有効利用性を保証することができない。

【0144】

また、特許文献2は、機密度の変化に応じた保護強度の修正方法を示している。しかし

特許文献 2 は、はじめに平文コンテンツを暗号化する際に、「予め決められた機密度に応じた保護強度」による、と示唆するのみで、はじめに用いられる保護強度が機密度に対して適切なものであるかを判断する技術を示していない。そのため、これらの技術のみでは、適切な暗号化方式を選択することにより、情報の有効期限までの間、第三者から情報を秘匿できることを保証することはできない。

【0145】

また、特許文献 2 乃至 5 に記載された各技術は、データの有効期限後にそのデータを利用することについて考慮していないので、暗号化データの有効期限後の有効利用性を保証することができない。

【0146】

よって、各関連文献に記載された技術は、暗号化データ生成時の負荷を軽減しかつ暗号化されるデータの有効期限までの秘匿性を維持しつつ有効期限後の有効利用性を保証することができない。

【0147】

一方、本発明は、効果の一例として、暗号化データ生成時の負荷を軽減できかつ暗号化されるデータの有効期限までの秘匿性を維持しつつ有効期限後の有効利用性を保証できる。

【0148】

上記の実施の形態または実施例の一部又は全部は、以下の付記のようにも記載されうるが、以下には限られない。

【0149】

(付記 1)

データを識別できるデータ識別子と当該データの配信先を示す宛先とを受け取る入力部と、

前記データに対応する当該データの有効期限までに解読されない暗号強度を持つ暗号化方法を識別できる暗号化方法識別子と当該暗号化方法の暗号化処理に必要なリソース量とを特定する暗号化方法決定部と、

前記暗号化方法決定部が特定したリソース量に基づいて、それぞれのリソース量に対応する暗号化方法識別子で識別される暗号化方法が用いられる優先度を示すリソース消費量評価値を算出し、算出される当該リソース消費量評価値に基づいてリソース量に対応する暗号化方法識別子を特定する暗号化方法評価部と、

前記データ識別子で識別されるデータを、前記暗号化方法評価部が特定した暗号化方法識別子で識別される暗号化方法によって暗号化する暗号化部と、

前記暗号化部が暗号化した前記データを配信する配信部と、

前記配信部が前記データを配信する際に、前記有効期限を経過している、および、前記宛先で示される配信先に当該データが配信される、の二つの条件の少なくともいずれかが満たされる場合に、前記暗号化方法識別子を当該データの配信先に送信する暗号化方法伝達部と、

を備えるデータ配信装置。

【0150】

(付記 2)

付記 1 に記載のデータ配信装置であって、

当該データ配信装置が備えるリソースの負荷情報を取得する負荷情報取得部と、

リソースの負荷情報の条件を示す適用条件とリソース量に基づいてリソース消費量評価値の算出方法を示すリソース消費量評価値算出方法とを対応付けて記憶するリソース消費量評価値算出方法記憶部と、を備え、

前記暗号化方法評価部は、前記装置負荷情報取得部から前記リソースの負荷情報を受け取り、当該リソースの負荷情報と合致する適用条件に対応付けられているリソース消費量評価値算出方法を前記リソース消費量評価値算出方法記憶部から読み出し、

前記暗号化方法評価部は、読み出したリソース消費量評価値算出方法に基づいて、各暗

10

20

30

40

50

号化方法のリソース消費量評価値を算出する、データ配信装置。

【0151】

(付記3)

付記1または2に記載のデータ配信装置であって、

データを解析して当該データの有効期限を算出するための関数である有効期限算出関数と、その関数が適用される条件を示すルール適用条件とを含む有効期限算出ルールを記憶する有効期限算出ルール記憶部と、

データを受け取ると、当該データと合致するルール適用条件を含む有効期限算出ルールを前記有効期限算出ルール記憶部から読み出し、読み出した有効期限算出ルールに含まれる有効期限算出関数と当該データとに基づいて当該データの有効期限を算出する有効期限算出部と、を備え

10

前記入力部は、受け取ったデータ識別子で識別されるデータを受け取ると、当該データを前記有効期限算出部に渡し、

前記暗号化方法決定部は、前記有効期限算出部が算出した有効期限までに解読されない暗号強度を持つ暗号化方法を識別できる暗号化方法識別子と当該暗号化方法の暗号処理に必要なリソース量とを特定する、データ配信装置。

【0152】

(付記4)

付記3に記載のデータ配信装置であって、

データに含まれる所定の内容を示す情報である抽出情報を当該データから抽出し、抽出した抽出情報を記憶するデータ抽出部を備え、

20

前記有効期限算出部は、受け取ったデータに含まれる抽出情報と共通する情報を示す抽出情報を前記データ抽出部から読み出し、読み出した抽出情報の個数に基づいて有効期限を算出する、データ配信装置。

【0153】

(付記5)

付記3または4に記載のデータ配信装置であって、

前記ルール適用条件は、データが含む所定の要素の有無、その要素が有する属性の有無、要素の値、および要素が有する属性の値の少なくとも一つの情報の条件であり、

前記有効期限算出関数は、データが含む所定の要素の有無、その要素が有する属性の有無、要素の値、および要素が有する属性の値の少なくとも一つの情報に基づいた演算を規定する関数である、データ配信装置。

30

【0154】

(付記6)

付記4に記載のデータ配信装置であって、

前記抽出情報は、ある個人に関連する情報を示す情報であり、

前記有効期限算出部は、受け取ったデータに含まれる抽出情報と共通する個人に関連する情報を示す抽出情報を前記データ抽出部から読み出し、読み出した抽出情報の個数が所定の閾値以上である場合に、前記受け取ったデータの有効期限を長くする、データ配信装置。

40

【0155】

(付記7)

付記1ないし6のいずれか1項に記載のデータ配信装置であって、

前記リソース消費量評価値は、値が大きい場合に前記優先度が高いことを示し、

前記暗号化方法評価部は前記暗号化方法決定部が複数の暗号化方法識別子を特定した際に、当該複数の暗号化方法識別子の中から、リソース消費量評価値が最大であるリソース量に対応する暗号化方法識別子を特定する、データ配信装置。

【0156】

(付記8)

付記1ないし7のいずれか1項に記載のデータ配信装置であって、

50

暗号化方法識別子を受け取ると、当該暗号化方法識別子で識別される暗号化方法に基づいて、当該暗号化方法により暗号化されたデータに対する暗号解読法を適用した場合の強度指標を求め、当該強度指標に基づき前記暗号化されたデータの解読に要する時間を推定し、推定された時間に基づいて暗号強度を算出し、当該暗号化方法識別子で識別される暗号化方法を用いて所定のデータに対して暗号化処理を行い、その際に消費されるリソースの量に基づいて、リソース量を算出する暗号強度算出部を備え、

前記暗号化方法決定部は、前記暗号強度算出部が算出した暗号強度とリソース量と、算出の際に用いられた暗号化方法の暗号化方法識別子とを対応付けて記憶し、前記入力部が受け取るデータ識別子で識別されるデータの有効期限までに解読されない暗号強度を持つ暗号化方法を識別できる暗号化方法識別子と当該暗号化方法の暗号処理に必要なリソース量とを、前記記憶した暗号強度と当該有効期限とを比較することで特定する、データ配信装置。

10

【0157】

(付記9)

付記1ないし8のいずれか1項に記載のデータ配信装置であって、

前記暗号化方法伝達部は、暗号化方法識別子の配信先の公開鍵を取得し、当該公開鍵を用いて当該暗号化方法識別子を暗号化し、暗号化した当該暗号化方法識別子を前記配信部が配信するデータに付加する、データ配信装置。

【0158】

(付記10)

付記1ないし9のいずれか1項に記載のデータ配信装置であって、

データを暗号化する暗号化方法を識別できる暗号化方法識別子と、当該暗号化方法の暗号処理に必要なリソース量と、当該暗号化方法の暗号強度と、を対応付けて記憶する暗号化方法記憶部を備え、

20

前記暗号化方法決定部は、前記入力部が受け取るデータ識別子で識別されるデータに対応する有効期限までに解読されない暗号強度に対応付けられている暗号化方法識別子とリソース量とを読み出す、データ配信装置。

【0159】

(付記11)

付記1ないし10のいずれか1項に記載のデータ配信装置であって、

前記暗号化方法は、暗号処理のアルゴリズムの種類を示す情報、当該アルゴリズムのパラメータを示す情報、および、当該アルゴリズムを実行するハードウェアを示す情報、の少なくとも一つを含む、データ配信装置。

30

【0160】

(付記12)

付記1ないし11のいずれか1項に記載のデータ配信装置であって、

データの有効期限は、当該データを秘匿する必要がなくなる日時を示す、データ配信装置。

【0161】

(付記13)

付記1ないし12のいずれか1項に記載のデータ配信装置であって、

前記入力部は、データと当該データのデータ識別子と当該データの有効期限とを受け取る、データ配信装置。

40

【0162】

(付記14)

付記1ないし13のいずれか1項に記載のデータ配信装置であって、

データの有効期限は、複数のデータの有効期限を示す、データ配信装置。

【0163】

(付記15)

付記3ないし6のいずれか1項に記載のデータ配信装置であって、

50

前記ルール適用条件は、前記有効期限算出ルール記憶部が記憶しているいずれのルール適用条件を満たさないデータに適用される条件を含む、データ配信装置。

【0164】

(付記16)

付記1ないし15のいずれか1項に記載のデータ配信装置であって、

前記暗号強度は、当該暗号強度に対応する暗号化方法を用いて暗号化されたデータが解読されるために必要な時間を示す情報である、データ配信装置。

【0165】

(付記17)

付記2に記載のデータ配信装置であって、

前記リソース量は、複数のハードウェアがそれぞれ暗号処理の際に消費するリソースの量を示す情報であり、

前記リソース消費量評価値算出方法は、リソース量が示す所定のハードウェアが当該暗号処理の際に消費するリソースの量に基づいて算出する関数を示す、データ配信装置。

【0166】

(付記18)

付記17に記載のデータ配信装置であって、

前記リソース消費量評価値算出方法は、リソース量が示す単一の種類のハードウェアが当該暗号処理の際に消費するリソースの量に基づいて算出する関数を示す、データ配信装置。

【0167】

(付記19)

付記2に記載のデータ配信装置であって、

前記リソースの負荷情報は、CPUの使用率、暗号化チップの使用率、メモリ使用量、データが前記暗号化部において処理待ちとなっている待ち行列の長さ、暗号化されたデータが前記配信部において処理待ちとなっている待ち行列の長さ、前記データ配信装置の消費電力、および前記データ配信装置の残電力の少なくとも一つを含む、データ配信装置。

【0168】

(付記20)

データを識別できるデータ識別子と当該データの配信先を示す宛先とを受け取り、

前記データに対応する当該データの有効期限までに解読されない暗号強度を持つ暗号化方法を識別できる暗号化方法識別子と当該暗号化方法の暗号化処理に必要なリソース量とを特定し、

前記特定したリソース量に基づいて、それぞれのリソース量に対応する暗号化方法識別子で識別される暗号化方法が用いられる優先度を示すリソース消費量評価値を算出し、算出される当該リソース消費量評価値に基づいてリソース量に対応する暗号化方法識別子を特定し、

前記データ識別子で識別されるデータを、前記特定した暗号化方法識別子で識別される暗号化方法によって暗号化し、

前記暗号化した前記データを配信し、

前記データを配信する際に、前記有効期限を経過している、および、前記宛先で示される配信先に当該データが配信される、の二つの条件の少なくともいずれかが満たされる場合に、前記暗号化方法識別子を当該データの配信先に送信する、データ配信方法。

【0169】

(付記21)

付記20に記載のデータ配信方法であって、

リソースの負荷情報の条件を示す適用条件とリソース量に基づいてリソース消費量評価値の算出方法を示すリソース消費量評価値算出方法とを対応付けて記憶部に記憶し、

当該データ配信装置が備えるリソースの負荷情報を受け取り、当該リソースの負荷情報と合致する適用条件に対応付けられているリソース消費量評価値算出方法を前記記憶部か

10

20

30

40

50

ら読み出し、

前記読み出したリソース消費量評価値算出方法に基づいて、各暗号化方法のリソース消費量評価値を算出する、データ配信方法。

【0170】

(付記22)

付記20または21に記載のデータ配信方法であって、

データを解析して当該データの有効期限を算出するための関数である有効期限算出関数と、その関数が適用される条件を示すルール適用条件とを含む有効期限算出ルールを記憶部に記憶し、

データを受け取ると、当該データと合致するルール適用条件を含む有効期限算出ルールを前記記憶部から読み出し、読み出した有効期限算出ルールに含まれる有効期限算出関数と当該データとに基づいて当該データの有効期限を算出し、

前記算出した有効期限までに解読されない暗号強度を持つ暗号化方法を識別できる暗号化方法識別子と当該暗号化方法の暗号処理に必要なリソース量とを特定する、データ配信方法。

【0171】

(付記23)

付記22に記載のデータ配信方法であって、

データに含まれる所定の内容を示す情報である抽出情報を当該データから抽出し、抽出した抽出情報を記憶部に記憶し、

受け取ったデータに含まれる抽出情報と共通する情報を示す抽出情報を前記記憶部から読み出し、読み出した抽出情報の個数に基づいて有効期限を算出する、データ配信方法。

【0172】

(付記24)

付記22または23に記載のデータ配信方法であって、

前記ルール適用条件は、データが含む所定の要素の有無、その要素が有する属性の有無、要素の値、および要素が有する属性の値の少なくとも一つの情報の条件であり、

前記有効期限算出関数は、データが含む所定の要素の有無、その要素が有する属性の有無、要素の値、および要素が有する属性の値の少なくとも一つの情報に基づいた演算を規定する関数である、データ配信方法。

【0173】

(付記25)

付記23に記載のデータ配信方法であって、

前記抽出情報は、ある個人に関連する情報を示す情報であり、

受け取ったデータに含まれる抽出情報と共通する個人に関連する情報を示す抽出情報を前記記憶部から読み出し、読み出した抽出情報の個数が所定の閾値以上である場合に、前記受け取ったデータの有効期限を長くする、データ配信方法。

【0174】

(付記26)

付記20ないし25のいずれか1項に記載のデータ配信方法であって、

前記リソース消費量評価値は、値が大きい場合に前記優先度が高いことを示し、

複数の暗号化方法識別子を特定した際に、当該複数の暗号化方法識別子の中から、リソース消費量評価値が最大であるリソース量に対応する暗号化方法識別子を特定する、データ配信方法。

【0175】

(付記27)

付記20ないし26のいずれか1項に記載のデータ配信方法であって、

暗号化方法識別子を受け取ると、当該暗号化方法識別子で識別される暗号化方法に基づいて、当該暗号化方法により暗号化されたデータに対する暗号解読法を適用した場合の強度指標を求め、当該強度指標に基づき前記暗号化されたデータの解読に要する時間を推定

10

20

30

40

50

し、推定された時間に基づいて暗号強度を算出し、当該暗号化方法識別子で識別される暗号化方法を用いて所定のデータに対して暗号化処理を行い、その際に消費されるリソースの量に基づいて、リソース量を算出し、

前記算出した暗号強度とリソース量と、算出の際に用いられた暗号化方法の暗号化方法識別子とを対応付けて記憶部に記憶し、前記受け取るデータ識別子で識別されるデータの有効期限までに解読されない暗号強度を持つ暗号化方法を識別できる暗号化方法識別子と当該暗号化方法の暗号処理に必要なリソース量とを、前記記憶部に記憶した暗号強度と当該有効期限とを比較することで特定する、データ配信方法。

【0176】

(付記28)

付記20ないし27のいずれか1項に記載のデータ配信方法であって、

暗号化方法識別子の配信先の公開鍵を取得し、当該公開鍵を用いて当該暗号化方法識別子を暗号化し、暗号化した当該暗号化方法識別子を前記配信するデータに付加する、データ配信方法。

【0177】

(付記29)

付記20ないし28のいずれか1項に記載のデータ配信方法であって、

データを暗号化する暗号化方法を識別できる暗号化方法識別子と、当該暗号化方法の暗号処理に必要なリソース量と、当該暗号化方法の暗号強度と、を対応付けて記憶部に記憶し、

前記受け取るデータ識別子で識別されるデータに対応する有効期限までに解読されない暗号強度に対応付けられている暗号化方法識別子とリソース量とを前記記憶部から読み出す、データ配信方法。

【0178】

(付記30)

付記20ないし29のいずれか1項に記載のデータ配信方法であって、

前記暗号化方法は、暗号処理のアルゴリズムの種類を示す情報、当該アルゴリズムのパラメータを示す情報、および、当該アルゴリズムを実行するハードウェアを示す情報、の少なくとも一つを含む、データ配信方法。

【0179】

(付記31)

付記20ないし30のいずれか1項に記載のデータ配信方法であって、

データの有効期限は、当該データを秘匿する必要がなくなる日時を示す、データ配信方法。

【0180】

(付記32)

付記20ないし31のいずれか1項に記載のデータ配信方法であって、

データと当該データのデータ識別子と当該データの有効期限とを受け取る、データ配信方法。

【0181】

(付記33)

付記20ないし32のいずれか1項に記載のデータ配信方法であって、

データの有効期限は、複数のデータの有効期限を示す、データ配信方法。

【0182】

(付記34)

付記22ないし25のいずれか1項に記載のデータ配信方法であって、

前記ルール適用条件は、前記有効期限算出ルール記憶部が記憶しているいずれのルール適用条件を満たさないデータに適用される条件を含む、データ配信方法。

【0183】

(付記35)

10

20

30

40

50

付記 20 ないし 34 のいずれか 1 項に記載のデータ配信方法であって、
前記暗号強度は、当該暗号強度に対応する暗号化方法を用いて暗号化されたデータが解読されるために必要な時間を示す情報である、データ配信方法。

【0184】

(付記 36)

付記 21 に記載のデータ配信方法であって、
前記リソース量は、複数のハードウェアがそれぞれ暗号処理の際に消費するリソースの量を示す情報であり、
前記リソース消費量評価値算出方法は、リソース量が示す所定のハードウェアが当該暗号処理の際に消費するリソースの量に基づいて算出する関数を示す、データ配信方法。

10

【0185】

(付記 37)

付記 36 に記載のデータ配信方法であって、
前記リソース消費量評価値算出方法は、リソース量が示す単一の種類のハードウェアが当該暗号処理の際に消費するリソースの量に基づいて算出する関数を示す、データ配信方法。

【0186】

(付記 38)

付記 21 に記載のデータ配信方法であって、
前記リソースの負荷情報は、CPU の使用率、暗号化チップの使用率、メモリ使用量、データが前記暗号化部において処理待ちとなっている待ち行列の長さ、暗号化されたデータが前記配信部において処理待ちとなっている待ち行列の長さ、前記データ配信装置の消費電力、および前記データ配信装置の残電力の少なくとも一つを含む、データ配信方法。

20

【0187】

(付記 39)

コンピュータに、
データを識別できるデータ識別子と当該データの配信先を示す宛先とを受け取る処理と、
前記データに対応する当該データの有効期限までに解読されない暗号強度を持つ暗号化方法を識別できる暗号化方法識別子と当該暗号化方法の暗号化処理に必要なリソース量とを特定する処理と、

30

前記特定したリソース量に基づいて、それぞれのリソース量に対応する暗号化方法識別子で識別される暗号化方法が用いられる優先度を示すリソース消費量評価値を算出し、算出される当該リソース消費量評価値に基づいてリソース量に対応する暗号化方法識別子を特定する処理と、

前記データ識別子で識別されるデータを、前記特定した暗号化方法識別子で識別される暗号化方法によって暗号化する処理と、

前記暗号化した前記データを配信する処理と、

前記データを配信する際に、前記有効期限を経過している、および、前記宛先で示される配信先に当該データが配信される、の二つの条件の少なくともいずれかが満たされる場合に、前記暗号化方法識別子を当該データの配信先に送信する処理と、を実行させるためのデータ配信プログラム。

40

【0188】

(付記 40)

付記 39 に記載のデータ配信プログラムであって、
リソースの負荷情報の条件を示す適用条件とリソース量に基づいてリソース消費量評価値の算出方法を示すリソース消費量評価値算出方法とを対応付けて記憶部に記憶する処理と、

当該データ配信装置が備えるリソースの負荷情報を受け取り、当該リソースの負荷情報と合致する適用条件に対応付けられているリソース消費量評価値算出方法を前記記憶部か

50

ら読み出す処理と、

前記読み出したリソース消費量評価値算出方法に基づいて、各暗号化方法のリソース消費量評価値を算出する処理とを前記コンピュータに実行させるためのデータ配信プログラム。

【0189】

(付記41)

付記39または40に記載のデータ配信プログラムであって、

データを解析して当該データの有効期限を算出するための関数である有効期限算出関数と、その関数が適用される条件を示すルール適用条件とを含む有効期限算出ルールを記憶部に記憶する処理と、

10

データを受け取ると、当該データと合致するルール適用条件を含む有効期限算出ルールを前記記憶部から読み出し、読み出した有効期限算出ルールに含まれる有効期限算出関数と当該データとに基づいて当該データの有効期限を算出する処理と、

前記算出した有効期限までに解読されない暗号強度を持つ暗号化方法を識別できる暗号化方法識別子と当該暗号化方法の暗号処理に必要なリソース量とを特定する処理とを前記コンピュータに実行させるためのデータ配信プログラム。

【0190】

(付記42)

付記41に記載のデータ配信プログラムであって、

データに含まれる所定の内容を示す情報である抽出情報を当該データから抽出し、抽出した抽出情報を記憶部に記憶する処理と、

20

受け取ったデータに含まれる抽出情報と共通する情報を示す抽出情報を前記記憶部から読み出し、読み出した抽出情報の個数に基づいて有効期限を算出する処理とを前記コンピュータに実行させるためのデータ配信プログラム。

【0191】

(付記43)

付記41または42に記載のデータ配信プログラムであって、

前記ルール適用条件は、データが含む所定の要素の有無、その要素が有する属性の有無、要素の値、および要素が有する属性の値の少なくとも一つの情報の条件であり、

前記有効期限算出関数は、データが含む所定の要素の有無、その要素が有する属性の有無、要素の値、および要素が有する属性の値の少なくとも一つの情報に基づいた演算を規定する関数である、データ配信プログラム。

30

【0192】

(付記44)

付記42に記載のデータ配信プログラムであって、

前記抽出情報は、ある個人に関連する情報を示す情報であり、

受け取ったデータに含まれる抽出情報と共通する個人に関連する情報を示す抽出情報を前記記憶部から読み出し、読み出した抽出情報の個数が所定の閾値以上である場合に、前記受け取ったデータの有効期限を長くする処理を前記コンピュータに実行させるためのデータ配信プログラム。

40

【0193】

(付記45)

付記39ないし44のいずれか1項に記載のデータ配信プログラムであって、

前記リソース消費量評価値は、値が大きい場合に前記優先度が高いことを示し、

複数の暗号化方法識別子を特定した際に、当該複数の暗号化方法識別子の中から、リソース消費量評価値が最大であるリソース量に対応する暗号化方法識別子を特定する処理を前記コンピュータに実行させるためのデータ配信プログラム。

【0194】

(付記46)

付記39ないし45のいずれか1項に記載のデータ配信プログラムであって、

50

暗号化方法識別子を受け取ると、当該暗号化方法識別子で識別される暗号化方法に基づいて、当該暗号化方法により暗号化されたデータに対する暗号解読法を適用した場合の強度指標を求め、当該強度指標に基づき前記暗号化されたデータの解読に要する時間を推定し、推定された時間に基づいて暗号強度を算出し、当該暗号化方法識別子で識別される暗号化方法を用いて所定のデータに対して暗号化処理を行い、その際に消費されるリソースの量に基づいて、リソース量を算出する処理と、

前記算出した暗号強度とリソース量と、算出の際に用いられた暗号化方法の暗号化方法識別子とを対応付けて記憶部に記憶し、前記受け取るデータ識別子で識別されるデータの有効期限までに解読されない暗号強度を持つ暗号化方法を識別できる暗号化方法識別子と当該暗号化方法の暗号処理に必要なリソース量とを、前記記憶部に記憶した暗号強度と当該有効期限とを比較することで特定する処理とを前記コンピュータに実行させるためのデータ配信プログラム。

10

【0195】

(付記47)

付記39ないし46のいずれか1項に記載のデータ配信プログラムであって、

暗号化方法識別子の配信先の公開鍵を取得し、当該公開鍵を用いて当該暗号化方法識別子を暗号化し、暗号化した当該暗号化方法識別子を前記配信するデータに付加する処理を前記コンピュータに実行させるためのデータ配信プログラム。

【0196】

(付記48)

付記39ないし47のいずれか1項に記載のデータ配信プログラムであって、

データを暗号化する暗号化方法を識別できる暗号化方法識別子と、当該暗号化方法の暗号処理に必要なリソース量と、当該暗号化方法の暗号強度と、を対応付けて記憶部に記憶する処理と、

20

前記受け取るデータ識別子で識別されるデータに対応する有効期限までに解読されない暗号強度に対応付けられている暗号化方法識別子とリソース量とを前記記憶部から読み出す処理とを前記コンピュータに実行させるためのデータ配信プログラム。

【0197】

(付記49)

付記39ないし48のいずれか1項に記載のデータ配信プログラムであって、

前記暗号化方法は、暗号処理のアルゴリズムの種類を示す情報、当該アルゴリズムのパラメータを示す情報、および、当該アルゴリズムを実行するハードウェアを示す情報、の少なくとも一つを含む、データ配信プログラム。

30

【0198】

(付記50)

付記39ないし49のいずれか1項に記載のデータ配信プログラムであって、

データの有効期限は、当該データを秘匿する必要がなくなる日時を示す、データ配信プログラム。

【0199】

(付記51)

付記39ないし50のいずれか1項に記載のデータ配信プログラムであって、

データと当該データのデータ識別子と当該データの有効期限とを受け取る処理を前記コンピュータに実行させるためのデータ配信プログラム。

40

【0200】

(付記52)

付記39ないし51のいずれか1項に記載のデータ配信プログラムであって、

データの有効期限は、複数のデータの有効期限を示す、データ配信プログラム。

【0201】

(付記53)

付記41ないし44のいずれか1項に記載のデータ配信プログラムであって、

50

前記ルール適用条件は、前記有効期限算出ルール記憶部が記憶しているいずれのルール適用条件を満たさないデータに適用される条件を含む、データ配信プログラム。

【0202】

(付記54)

付記39ないし53のいずれか1項に記載のデータ配信プログラムであって、
前記暗号強度は、当該暗号強度に対応する暗号化方法を用いて暗号化されたデータが解読されるために必要な時間を示す情報である、データ配信プログラム。

【0203】

(付記55)

付記40に記載のデータ配信プログラムであって、
前記リソース量は、複数のハードウェアがそれぞれ暗号処理の際に消費するリソースの量を示す情報であり、
前記リソース消費量評価値算出方法は、リソース量が示す所定のハードウェアが当該暗号処理の際に消費するリソースの量に基づいて算出する関数を示す、データ配信プログラム。

10

【0204】

(付記56)

付記55に記載のデータ配信プログラムであって、
前記リソース消費量評価値算出方法は、リソース量が示す単一の種類のハードウェアが当該暗号処理の際に消費するリソースの量に基づいて算出する関数を示す、データ配信プログラム。

20

【0205】

(付記57)

付記40に記載のデータ配信プログラムであって、
前記リソースの負荷情報は、CPUの使用率、暗号化チップの使用率、メモリ使用量、データが前記暗号化部において処理待ちとなっている待ち行列の長さ、暗号化されたデータが前記配信部において処理待ちとなっている待ち行列の長さ、前記データ配信装置の消費電力、および前記データ配信装置の残電力の少なくとも一つを含む、データ配信プログラム。

【0206】

(付記58)

暗号化されたデータを識別できるデータ識別子と、当該データの有効期限と、当該データの配信先を示す宛先と、当該暗号化されたデータの暗号化方法を示す暗号化方法識別子とを対応付けて記憶する暗号データ情報記憶部と、
一のデータ識別子に対応付けられている有効期限と暗号化方法の暗号化方法識別子と宛先とを前記暗号データ情報記憶部から読み出し、当該有効期限を超過している、および、当該宛先が示す配信先へ送信する、の二つの条件の少なくともいずれかが満たされる場合に、当該暗号化されたデータの配信先に当該暗号化方法の暗号化方法識別子を送信する暗号化方法伝達部を備える暗号化方法伝達装置。

30

【産業上の利用可能性】

40

【0207】

本発明のデータ配信装置は、データの有効期限までの間は第三者から秘匿可能な暗号強度の暗号化方法を用いてデータを第三者から秘匿しつつ、暗号化処理に用いるリソースを必要最小限に抑えるといった用途に適用されうる。

【符号の説明】

【0208】

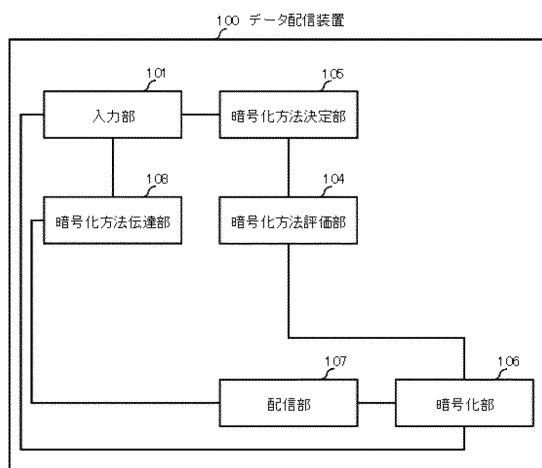
100、200、300 データ配信装置
101、301 入力部
103、203 暗号化方法記憶部
104、204 暗号化方法評価部

50

- 105、205、305 暗号化方法決定部
106 暗号化部
107 配信部
108 暗号化方法伝達部
109 暗号強度算出部
110、210 暗号データ情報記憶部
211 負荷情報取得部
212 リソース消費量評価値算出方法記憶部
302 有効期限算出部
314 有効期限算出ルール記憶部
315 データ抽出部
1011 データ入力部
1012 有効期限入力部
1013 宛先入力部
3014 有効期限算出ルール入力部

10

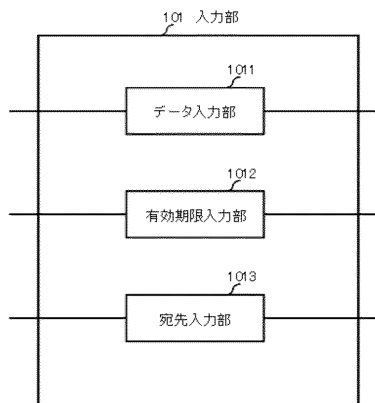
【図1】



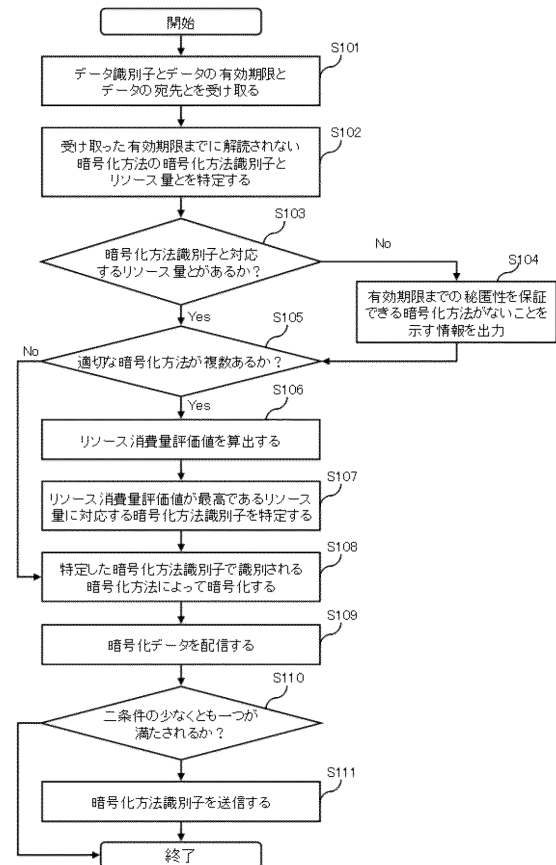
【図2】

暗号化方法		暗号強度	処理時間	
平文まま		0	0	T110
アルゴリズムA		18 hour	1 sec/MB	T111
アルゴリズムB	128bit	10 year	2 sec/MB	T112
	256bit	10 ²³ year	15 sec/MB	T113

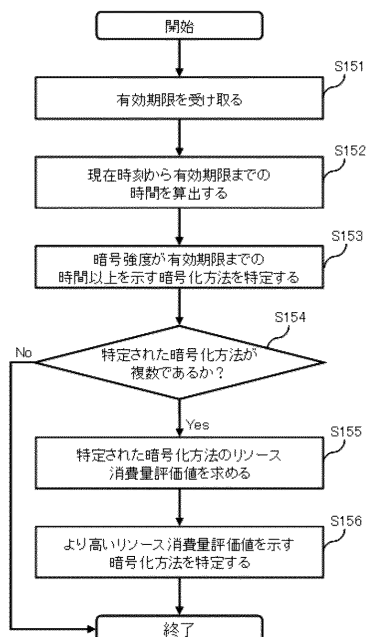
【図 3】



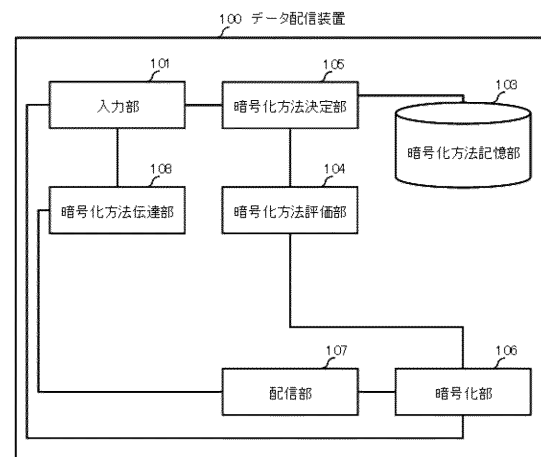
【図 4】



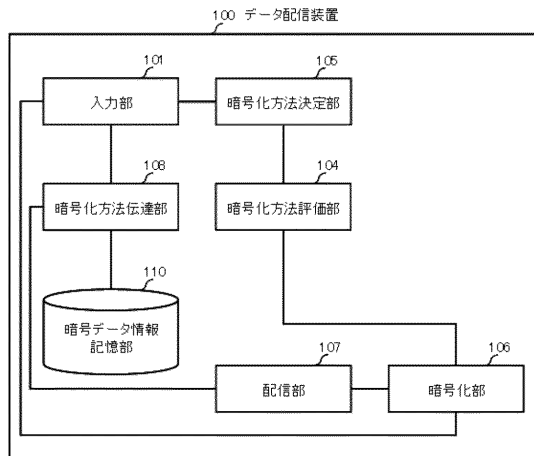
【図 5】



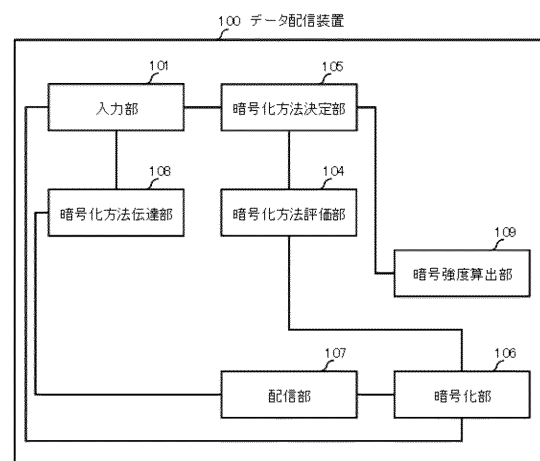
【図 6】



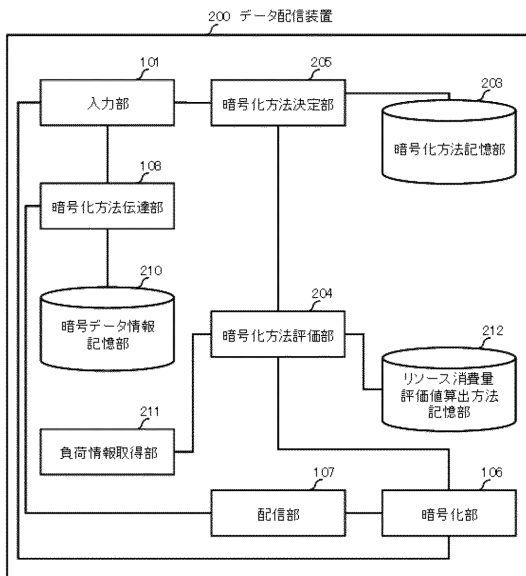
【図 7】



【図 8】



【図 9】



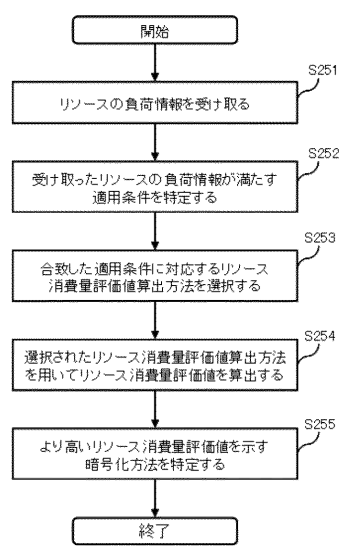
【図 10】

適用条件		算出方法
T311 T321 T331	[CPU使用率] < 30%	100 / [メモリ使用量]
	30% < [CPU使用率] < 70%	100 / [メモリ使用量] + 1 / [処理時間]
	(default)	1 / [処理時間]
		T312 T322 T332

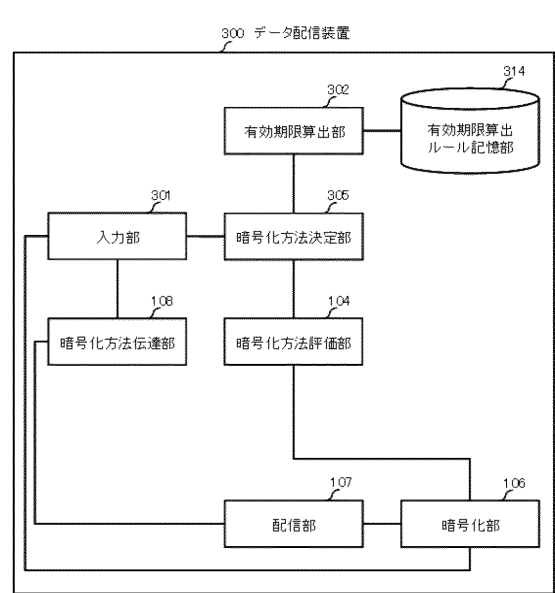
【図 11】

暗号化方法	暗号強度	処理時間	メモリ使用量
平文まま	0	0	0
アルゴリズムA	18 hour	1 sec/MB	100KB
アルゴリズムB	128bit	10 year	2 sec/MB
	256bit	10 ²³ year	15 sec/MB

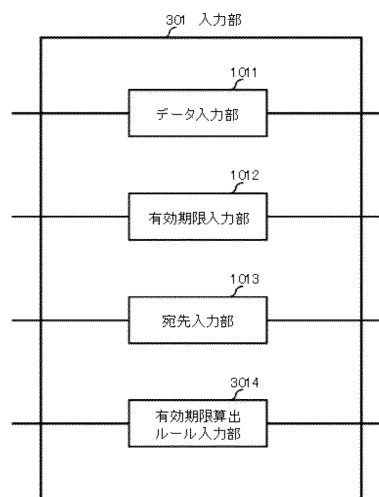
【 図 1 2 】



【 図 1 3 】



【 図 1 4 】



【 図 1 5 】

ルール適用条件	有効期限算出関数
条件 matchA()	関数 calculateA()
条件 matchB()	関数 calculateB()
⋮	⋮
(default)	関数 calculateDefault()

【図 16】

ルール適用条件	有効期限算出関数
Event.type="人"	Event.生成日時+1Day
Event.type="人" && Event.購買記録	Event.購買記録.購入日時+365Days
Event.type="人" && Event.位置	Event.位置.測定日時+3Days
Event.type="人" && Event.位置.粒度 < 10m	Event.位置.測定日時+30Days
(default)	<現在時刻>

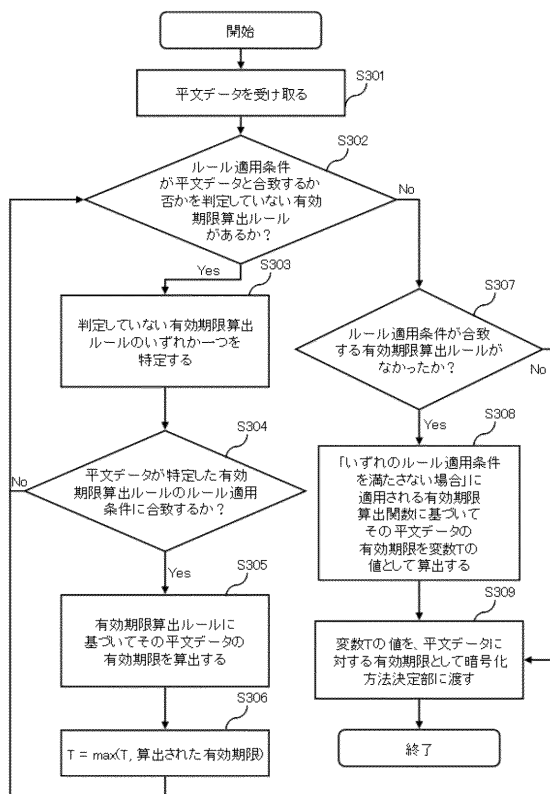
【図 17】

```

<?xml version="1.0" ?>
<Event type="人" id="A00000XX" 生成日時="2010.07.29 09:20:00">
  <位置 測定日時="2010.07.29 09:17:15" 粒度="100m" 座標系="WGS-84">
    <x>35.572272</x>
    <y>139.665509</y>
  </位置>
</Event>

```

【図 18】



【図 19】

