情報処理学会論文誌 Vol.60 No.9 1489–1499 (Sep. 2019)

代理人制度に向けたプロキシ再暗号化方式の要件定義とその方法

坂崎 尚生[1,a)]

受付日 2018年7月26日, 採録日 2019年6月11日

概要：近年，自治体等では様々な手続が電子化され，行政サービスの向上と行政運営の効率化が図られている．それらの手続は，本人が行うのが一般的であるが，民法では，代理人による代理行為も認めている．そこで，本論文では，代理人による安全な公共手続システムの実現に向け，安全な代理閲覧を可能とするプロキシ再暗号化方式に着目し，そのプロキシ再暗号化方式の適用方法について，日本の法制度と照らし合わせて検討を行う．そして，プロキシ再暗号化方式を公共機関等への手続システムに導入するための要件を定義する．さらに，その定義した要件をすべて満たすプロキシ再暗号化方式を提案する．

キーワード：再暗号化方式，法定代理人，任意代理人，電子政府推奨暗号（CRYPTREC）

Requirements and Methods of Re-encryption for Application Procedure from Agent

Hisao Sakazaki[1,a)]

Received: July 26, 2018, Accepted: June 11, 2019

Abstract: In the Civil Code, the use of the agent performing the legal actions in place of a user is admitted. So, it is necessary to construct electronic application systems that allow submission by agents. In those systems, even if an announcement which addressed to the mandator is encrypted, the specified agent must be able to read the encrypted announcement. As a general solution, there are proxy re-encryption methods. The proxy re-encryption method allows transforming a ciphertext computed with the encrypt-key of the mandator into a ciphertext which the agent can decrypt. Our aim is to develop the proxy re-encryption method that conforms to the legal system. In this paper, we define requirements of proxy re-encryption method derived from the Civil Code, and we propose a proxy re-encryption method that satisfies the requirements.

Keywords: re-encryption, legal representative, agent, e-government recommended cipher

1. はじめに

近年，自治体等では様々な手続が電子化され，行政サービスの向上と行政運営の効率化が図られている．自治体等では，公民館の施設予約のような簡易的な手続から，税務申告手続，介護保険手続，障害者支援手続のような機微情報を扱う手続まで，様々な手続が行われている．特に後者のように機微情報を電子的に扱う場合，手続内容によってはデータを暗号化し，プライバシ保護を図るケースが考えうる．

さて，電子化にかかわらず民法および関連法では，本人に代わって代理人にも，これらの手続を行うことを認めている．それゆえ，たとえデータが本人宛に暗号化された状態でも，必要に応じて代理人がそのデータを “代理閲覧” をし，本人に代わって代理人が “代理申請” できる仕組みが必要である．

取り分け “代理閲覧” の仕組みに注目すると，本人宛の暗号化データを第三者が復号できる仕組みとして，プロキシ再暗号化方式 [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11], [12]

[1] 株式会社日立製作所研究開発グループ，システムイノベーションセンタ
Hitachi, Ltd., Research & Development Group, Center for Technology Innovation-Systems Engineering, Yokohama, Kanagawa 244–0817, Japan
[a)] hisao.sakazaki.qc@hitachi.com

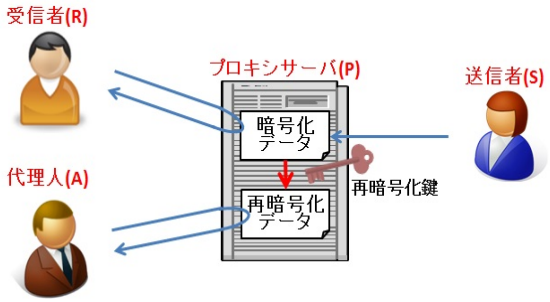

図 1 プロキシ再暗号化の仕組み
Fig. 1 Mechanism of Proxy Re-encryption.

が提案されており，プロキシ再暗号化方式はセキュアな代理人制度に対応した手続システムへの適用が期待できる[*1]．もちろん，ほかにも代理閲覧を可能とする方式は存在する．最も簡単な方式は，本人が自分宛の暗号化データをいったん復号し，それを本人が代理人宛に暗号化しなおして，代理人に転送するという方式である．しかし，この方式の場合，代理人を必要とする本人が最も重要な役割を担うことになる．そのほかの方式として，手続先機関にあらかじめ本人用と代理人用の暗号化鍵を登録し，手続先機関が本人宛だけでなく代理人宛にもそれぞれの暗号化データを送信するという方式もある．しかし，この方式において代理人を解雇するとき，本人は手続先機関ごとにその旨を伝える必要があり，複数の機関に代理人登録していると，その作業が煩雑になる．

本論文では，代理閲覧を実現する一方式として，プロキシ再暗号化方式について検討を行う．プロキシ再暗号化方式は，郵便局の私書箱のような仕組みであり，郵便局の役割を果たすプロキシサーバが，送信者，受信者，代理人との仲介を行う．具体的には，送信者がプロキシサーバに受信者宛の暗号化データを送り，プロキシサーバが受信者のメールボックスにそのデータを入れる．また，代理人が設定されている場合，プロキシサーバが受信者宛の暗号化データを復号することなく，あらかじめ登録されてある再暗号化鍵を用いて代理人宛の暗号化データに変換（再暗号化）し，代理人のメールボックスにそのデータを入れる（**図 1**）．プロキシ再暗号化方式は，プロキシサーバが再暗号化処理を行い，また，再暗号化鍵をプロキシサーバのみに登録するだけで実現できる仕組みであり，先にあげた課題を解決することができる．

しかし，単純に既存のプロキシ再暗号化方式 [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11], [12] を公共機関の手続システムに導入するわけにはいかない．なぜなら公共機関への手続は，様々な法制度に基づいて運用されるため，システム化の際には，関連する法制度と照らし合わせて設計しなければならないからである．

公共手続システムに限らずシステムを構成する場合，そこには，ルールが必要である．法制度は，社会ルールを表現したものであり，ICT 技術により新しい社会システムを構築する場合には，その構築するシステムが，どのような法制度に対応しているかを把握し，矛盾のないシステムになるように設計することが重要である．

本論文は上記状況に鑑み，プロキシ再暗号化方式を公共機関等への手続システムに導入するための要件を，日本の法制度と照らし合わせて定義する．さらにその定義した要件をすべて満たすプロキシ再暗号化方式を提案する．

なお，このようなプロキシサーバを用いた再暗号化処理方式は，たとえば，政府（内閣府）が運営するマイナポータルでの代理人による代理閲覧等への適用・拡張が想定できる．その際，プロキシサーバ側では，新たに再暗号化鍵の管理等の負荷が課せられることになるため，プロキシ再暗号化方式の適用に向けては，その費用対効果についても検討する必要がある．しかし，本論文では，費用対効果についての議論は，対象外とする．

本論文の構成は次のとおりである．2 章では本論文の背景となる公共機関への手続と代理人との関係について説明する．3 章では法制度を基にプロキシ再暗号化方式に求められる要件を定義する．4 章では上記要件を基にプロキシ再暗号化方式に必要な性質を整理する．5 章では定義した要件をすべて満たすプロキシ再暗号化方式を提案し，6 章で本論文をまとめる．

2. 公共機関への手続と代理人との関係

民法では，法定・任意代理人が本人に代わって各手続を行うことを認めている．なお，法定代理人とは，民法の規定によって定められた代理人のことで，親権者，未成年後見人，成年後見人等がこれにあたり，法定代理人以外の代理人を一般的に任意代理人と呼ぶ．

自治体等では，図書館・公民館の施設予約等の簡易的な手続から，税務申告手続，介護保険手続，障害者支援，乳幼児等予防接種手続等の機微な情報を扱う手続まで，様々な手続が行われている．これらの行政サービスのうち，特に機微な情報を扱う手続において，実際に法定・任意代理人がどのように関わっているかを 4 つ例にあげて説明する．

■ 税務申告手続

国税・地方税に関する申告・申請・届出等に関する手続．任意代理人として，税理士（税理士法第 52 条），弁護士（税理士法第 51 条），行政書士（税理士法第 51 条の 2）が本人に代わり税務代理行為を行うことができる．なお，税理士または税理士法人でない者は，税理士法に別段の定めがある場合を除き，税理士業務を行ってはならない．

■ 介護保険手続

加齢にともなって生ずる心身の変化に起因する疾病等に

[*1] 代理申請の仕組みに関しては，代理人が手続先機関宛にデータを暗号化して申請すればよく，代理閲覧のときのような課題は生じない．それゆえ，本論文では主に，代理閲覧の仕組みについて論じる．

より要介護状態となり，入浴，排泄，食事等の介護，機能訓練ならびに看護および療養上の管理，その他の医療を要する者等に対し，その有する能力に応じ自立した日常生活を営むことができるように必要な保健医療サービスおよび福祉サービスを受けるための手続．

ここでこれらの手続を行う利用者本人とは，第一号被保険者および第二号被保険者のことである．しかし，介護保険手続の場合，利用者本人が手続を行うのが困難なケースもある．そこで介護サービスを受けるための要支援認定に関しては，介護保険法第 46 条第 1 項に規定する指定居宅介護支援事業者，地域密着型介護老人福祉施設もしくは介護保険施設であって厚生労働省令で定めるものまたは第 115 条の 46 第 1 項に規定する地域包括支援センターに，当該申請に関する手続を代わって行わせることができる（介護保険法 27 条，32 条）．

■ 障害者支援手続

障害者手帳申請・交付等の手続．障害者本人が申請．ただし，本人が 15 歳未満時は，親権を行う者および後見人が申請を行う（身体障害者福祉法第 15 条）．また，児童福祉法第 27 条第 1 項第 3 号または第 27 条の 2 の規定により里親に委託され，または児童福祉施設に入所した児童については，当該里親または児童福祉施設の長も申請を行うことができる．

■ 乳幼児等予防接種手続

伝染のおそれがある疾病の発生およびまん延を予防することを目的とし，乳幼児等に対し予防接種をするための手続．接種者が 16 歳未満の者または成年被後見人であるときは，代理人として予防接種法第 2 条 4 により親権を行う者または後見人が，予防接種を受けさせるための必要な措置を講ずるように努めなければならない（予防接種法第 7 条の 2 の 2）．

上記の例のように，税理士等の士業資格のある任意代理人や介護保険施設や児童福祉施設の長のような任意代理人，親権者や後見人といった法定代理人からの手続が法律によって認められている．

本論文では，上記のように法律で定められた代理人による公共機関への手続を主に扱う．また，本論文で扱う代理人とは，受任者が特定された代理人を指し，会社等での役職に応じた権限付与（ロールベース制御）とは異なるものとする．ロールベース制御は，個人に直接権限を与えるのではなく，役職・役割を通して権限を与える仕組みである．このような社内に閉じた業務ルールにまで民法が定める代理人の定義をあてはめる必要はないと考える[*2]．

[*2] なお，社外との取引業務等，社内に閉じない業務においては，民法が定める代理人の定義に従うのが望ましい．

3. プロキシ再暗号化方式に求められる要件定義

システムの脅威として，一般的にデータの盗聴や改竄，秘密鍵の漏洩等があげられるが，本論文では前提として，既存方式 [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11], [12] の適用では，それらの対策が施されているとし，ここでは，日本の法制度から導かれる要件に特化して定義を行う．

3.1 暗号方式に関する法制度

暗号方式の公共システムへの導入に関する制度として，総務省，経済産業省，情報処理推進機構，情報通信研究機構で運営している CRYPTREC（Cryptography Research and Evaluation Committees）[13] の取組みがある．CRYPTREC とは，客観的な評価により安全性および実装性に優れると判断された暗号技術をリスト化する暗号技術評価プロジェクトである．

CRYPTREC では 2003 年 2 月 20 日に電子政府における調達のための推奨すべき暗号のリスト（電子政府推奨暗号リスト）を公表し[*3]，同年 2 月 28 日には，行政情報システム関係課長連絡会議において，各府省が情報システムの構築にあたり暗号を利用する場合には，可能な限り同プロジェクトでリスト化された電子政府推奨暗号リストに掲載された暗号の利用を推進する旨の「各府省の情報システム調達における暗号の利用方針」が了承されている．

したがって，プロキシ再暗号化方式を適用する場合，同リストに準拠した暗号技術を採用することが望ましい．

3.2 代理人制度に関する法制度

わが国の代理人制度に関しては，主に民法で規定されている[*4]．代理人には法定代理人と任意代理人とがあり，法定代理人とは民法の規定によって定められた代理人のことで，親権者（民法第 818 条），未成年後見人（民法第 838 条），成年後見人（民法第 843 条）等がこれに該当する[*5]．また，任意代理人とは法定代理人以外の代理人のことであり，主に「本人代理権の授与を行う委任契約を結んだ代理人」を意味する．

なお，民法では代理人制度に関する記述は散在しているが，主に第一編第五章第三節「代理」（第 99 条～第 118 条）および第三編第二章第十節「委任」（第 643 条～第 656 条）に記載されており，このうち，代理権の発生から消滅までの要件に関する事項を抜き出すと，「代理権の発生」「代理

[*3] 最新の CRYPTREC の暗号リストは，文献 [13] で確認できる．

[*4] 民法のほか，税理士法，介護保険法，身体障碍者福祉法等の各種関連法では，税務申告手続，介護保険手続，障害者支援手続等を行える代理人を具体的に規定されている（2 章参照）．

[*5] そのほか，保佐人（民法第 876 条），補助人（民法第 876 条），不在者の財産管理人（民法第 25 条），相続財産管理人（民法第 918 条），指定遺言執行者（民法第 1006 条），遺言執行者（民法第 1010 条）が法定代理人に該当する．

権の方向」「代理権の範囲」「代理権の再委譲（復代理）」「代理権の消滅」に関する内容が記載されている．

3.2.1 代理権の発生

法定代理の場合，その代理権の発生原因（要件）は法律で定められているため，本人の意思とは関係なく代理権が発生する．

一方，任意代理人の場合，民法第 643 条（委任契約）によると「委任は，当事者の一方が法律行為をすることを相手方に委託し，相手方がこれを承諾することによって，その効力を生ずる」と記されている[*6]．

単に情報の閲覧だけであれば，必ずしも民法第 643 条による代理人を選任する必要はないが，手続代行のために代理人を選任して情報を代理閲覧をさせるケースにおいては，本人と代理人との間で代理権の授受に関する合意が必要である．したがって，プロキシ再暗号化方式により任意代理人に代理権を与える際には，本人と代理人との間で代理権の授受に関する合意を担保できる仕組みが必要である．なお，法定代理人の場合，本人の意思とは関係なく代理権が発生するため，この限りではない．

3.2.2 代理権の方向

本人（被代理人）と代理人との関係を整理する．法定代理人とは，未成年者や成年被後見人等の制限行為能力者である本人（被代理人）を保護するために法律によって定められている代理人である．それゆえ，本人（被代理人）と代理人とが入れ替わることはない．

任意代理人の場合においても，民法第 643 条（委任契約）の解釈では「委任契約は原則として片務契約である」とされいる．したがって，委任契約の片務性を考慮するとプロキシ再暗号化方式により任意代理人に代理権を与える場合，どちらからどちらへ代理権が与えられたのか代理権の方向を明示でき，1 つの委任契約において逆方向への再暗号化は行えない仕組みにする必要がある．

3.2.3 代理権の範囲

民法第 99 条第 1 項（代理行為の要件及び効果）では「代理人がその権限内において本人のためにすることを示してした意思表示は，本人に対して直接にその効力を生ずる」と記されている．つまり，代理人にはその権限の範囲内で行為を行わなければならない[*7]．

したがって，プロキシ再暗号化方式により代理人に代理権を与える際，代理閲覧させる範囲を明示でき，その範囲外では再暗号化をできなくする仕組みが必要である．

3.2.4 代理権の再委譲（復代理）

民法第 106 条では「法定代理人は，自己の責任で復代理人を選任することができる」と記されている．また，民法第 104 条では「委任による代理人は，本人の許諾を得たとき，またはやむを得ない事由があるときでなければ，復代理人を選任することができない」と記されている．つまり民法では，法定代理人は自己責任において復代理を認めており，任意代理人に対しては，本人の許諾を得たときまたはやむをえない理由があるときに復代理を認めている．

それゆえ，プロキシ再暗号化方式では，必要に応じて代理人宛に再暗号化したデータを，さらに復代理人宛にも再暗号化できるようにし，民法で認めている復代理制度を可能とする仕組みにする必要がある．

3.2.5 代理権の消滅

民法第 111 条（代理権の消滅事由）では「代理権は，次に掲げる事由によって消滅する．(1) 本人の死亡 (2) 代理人の死亡又は代理人が破産手続開始決定若しくは後見開始の審判を受けたこと．委任による代理権は，前項各号に掲げる事由のほか，委任の終了によって消滅する」と記されている．また民法第 651 条第 1 項（委任の解除）では「委任は，各当事者がいつでもその解除をすることができる」と記されている．

したがって，プロキシ再暗号化方式により法定・任意代理人に代理権を与える場合，その代理権を消滅させる仕組みも当然必要となってくる．

以上より，代理人制度のシステム化に向けたプロキシ再暗号化方式の要件を以下にまとめる．なお，括弧内は各要件を導き出した根拠法制度を示す．

【要件 1】適用するプロキシ再暗号化方式は，CRYPTREC の暗号リストに準拠すること（CRYPTREC）．

【要件 2】本人と代理人との間で代理権の授受に関する合意を担保できること（民法第 643 条）．

【要件 3】代理権授受の方向に従い，再暗号化処理は一方向であること（民法第 643 条）．

【要件 4】代理閲覧させる範囲を明示でき，範囲外の再暗号化はできない仕組みにすること（民法第 99 条）．

【要件 5】再暗号化したデータをさらに再暗号化できるようにし，復代理を可能にすること（民法第 104，106 条）．

【要件 6】代理権を消滅できる仕組みを備えること（民法第 111，651 条）．

4. プロキシ再暗号化方式に必要な性質

プロキシ再暗号化の研究は従来より行われており，公開鍵暗号を基にした方式 [1], [2], [3], [4]，共通鍵暗号を基にした方式 [5], [6], [7]，ID ベース暗号を基にした方式 [8], [9], [10]，属性ベース暗号を基にした方式 [11]，関数型暗号を基にした方式 [12] 等がある．

*6 代理の依頼と引受を意味する「委任契約」と，代理権を授けるという「授権行為」とは，別個の存在であるという考えもある．それらが別個の存在であると考えたとき，学説では，授権行為は「代理人の承諾を不要とする “本人の単独行為”」とする説と「本人と代理人の合意に基づいてされる “無名契約”」とする説とに解釈が分かれている．

*7 なお，法定代理人と任意代理人により代理権の範囲が異なる．法定代理人の場合，代理権の範囲は法律によって定められている．任意代理人の場合，代理権の範囲は委任契約の内容によって決まる．いずれもその権限の範囲内で行為を行わなけければならない．

表 1 プロキシ再暗号化方式の種類
Table 1 Type of Re-encryption Scheme.

性質と種類		該当方式
再暗号化処理の方向性	Unidirectional	[10], etc.
	Bidirectional	[2][3], etc.
再暗号化処理の可能回数	Single-Hop	[10], etc.
	Multi-Hop	[2], etc.
再暗号化鍵生成方法	Non-interactive	[4], etc.
	Interactive	[9], etc.

各方式は，「再暗号化処理の方向性が一方向の Unidirectional（A ⇒ B のみ）か，双方向の Bidirectional（A ⇔ B）か」，「再暗号化処理の可能回数が 1 回のみ許されている Single-Hop か，複数回許されている Multi-Hop か」「再暗号化鍵生成が本人単独で生成できる Non-interactive か，再暗号化鍵生成のたびに本人と代理人とで通信が必要となる Interactive か」という性質に分類することができる（**表 1**）．

このようにプロキシ再暗号化方式は多種多様な方式が提案されているが，代理人制度のシステム化において，どのような性質を持つプロキシ再暗号化方式を適用するべきかの検討はされていない．そこで，前章で導いた要件との比較を行い，代理人制度のシステム化に向けたプロキシ再暗号化方式に必要な性質を整理する．

4.1 再暗号化処理の方向性

再暗号化処理の方向性は，代理権の方向性と関連する．

つまり要件 3「代理権授受の方向に従い，再暗号化処理は一方向であること（民法第 643 条）」より，Unidirectional の性質を持つプロキシ再暗号化方式の方が代理人制度のシステム化に適していることが分かる．

4.2 再暗号化処理の可能回数

再暗号化処理が可能な回数は，復代理制度と関連する．

つまり要件 5「再暗号化したデータを更に再暗号化できるようにし，復代理を可能にすること（民法第 104，106 条）」より，複数回再暗号化処理が可能な Multi-Hop の性質を持つプロキシ再暗号化方式の方が適していることが分かる．

4.3 再暗号化鍵生成方法

最後に再暗号化鍵生成方法に関してである．再暗号化鍵を生成し登録するという行為は，代理人に代理権を与える行為であり，民法での代理権の発生要件である双方合意と関連してくる．

つまり，要件 2「本人と代理人との間で代理権の授受に関する合意を担保できること（民法第 643 条）」より，再暗号化鍵の登録に本人と代理人の双方で処理する必要がある Interactive 型の再暗号化鍵生成機能を持つプロキシ再暗号化方式の方が代理人制度のシステム化に適している．

もちろん，「再暗号化鍵の登録」と「代理権の双方合意」を切り離して考え，本人単独で再暗号化鍵を登録し，別途，双方合意の念書を交わすといった運用による対策を組み込むことで Non-Interactive 型のプロキシ再暗号方式でも要件 2 を満たすこともできるが，Interactive 型を採用することによりシステム的に要件 2 を満たすことができる．

以上より，代理人制度のシステム化に向けたプロキシ再暗号化方式に必要な性質を**表 2** にまとめる．

表 2 代理人制度に向けたプロキシ再暗号化方式に必要な性質
Table 2 Required Property of Re-encryption for Application Procedure from Agent.

性質	結果	根拠法
再暗号化処理の方向性	Unidirectional	民法第 643 条
再暗号化処理の可能回数	Multi-Hop	民法第 104，106 条
再暗号化鍵生成方法	Interactive	民法第 643 条

5. 要件を満たすプロキシ再暗号化方式の提案

プロキシ再暗号化方式では，本人宛の暗号化鍵で暗号化したデータを復号することなく，別の鍵で暗号化されたデータに書き換える機能が必要である．それには暗号化関数として，“準同型の性質” または “可換性の性質” が必要であり，先行研究の多くは，“準同型の性質” を利用した公開鍵暗号を基に設計されている．

しかし，CRYPTREC 暗号リスト [13] には，守秘用途で用いられる公開鍵暗号は RSA-OPEP のみであり，準同型または可換性の性質を持つ公開鍵暗号は登録されていない．また，ID ベース暗号，属性ベース暗号，関数型暗号も登録されてない．

ゆえに本研究では，先の 6 つの要件を満たす方式の一例として，坂崎らの方式 [6], [7] をベースに実現した．坂崎らの方式 [6], [7] は，共通鍵暗号を基にした方式であり，CRYPTREC 準拠の暗号関数の組合せで実現できる．

5.1 関連研究

ここでは，坂崎らの方式 [6], [7] の概要を説明する．坂崎らの方式 [6], [7] では，k_x をユーザ X の秘密鍵（鍵長 $= l$）とし，あらかじめユーザ X とユーザ Y との再暗号化鍵 $rk_{xy} = k_x \oplus k_y$ が Protocol 1 でプロキシ—サーバ P に登録され，Hardware Security Module（HSM）等で安全に管理されている．

Protocol 1: Re-encryption Key Registration

Entities: User X, User Y, Proxy Server P,

(1) X makes a re-encryption key registration request to P.
(2) P generates a random number r and sends r to X.
(3) X sends the ciphertext $e_1 = r \oplus k_x$ to Y.
(5) Y sends the ciphertext $e_2 = e_1 \oplus k_y$ to P.
(6) P calculates $rk_{xy} = r \oplus e_2 = k_x \oplus k_y$ and registers it as a re-encryption key.

また，坂崎らの方式 [6], [7] では，認証付き暗号関数 ENC を用いる．この認証付き暗号関数 ENC は，データの秘匿性，完全性および認証性を同時に提供する暗号利用モードであり，AES 暗号等の共通鍵暗号方式を用いて，メッセージを暗号化してから暗号文にメッセージ認証コード（MAC）を付加することで容易に実現できる．そして，以下の暗号化関数 MOTE（Masked One-Time Encryption）を定義する．なお，“ || ” はデータの結合を意味する．また，r_m はメッセージ m ごとに生成されるワンタイム暗号化鍵（長さ l の乱数）である．

$$\mathtt{MOTE}(m, k_x) = (k_x \oplus r_m) \,||\, \mathtt{ENC}(m, r_m)$$

ユーザ X が暗号化データ $c_x = \mathtt{MOTE}(m, k_x)$ をプロキシサーバ P に送った際，プロキシサーバ P では Algorithm 1 を用いてユーザ Y 宛の再暗号化データ $c_y = \mathtt{MOTE}(m, k_y)$ に変換する．再暗号化データ $c_y = \mathtt{MOTE}(m, k_y) = (k_y \oplus r_m) \,||\, \mathtt{ENC}(m, r_m)$ を受信したユーザ Y は，c_y の左側の $(k_y \oplus r_m)$ と自身の秘密鍵 k_y との排他的論理和をとることでワンタイム暗号化鍵 r_m を取り出し，そのワンタイム暗号化鍵 r_m で c_y の右側の $\mathtt{ENC}(m, r_m)$ を復号することでメッセージ m を取得する．

Algorithm 1: re-encryption

INPUT: $c_x = \mathtt{MOTE}(m, k_x) = (k_x \oplus r_m) \,||\, \mathtt{ENC}(m, r_m)$, $rk_{xy} = k_x \oplus k_y$

OUTPUT: $c_y = \mathtt{MOTE}(m, k_y) = (k_y \oplus r_m) \,||\, \mathtt{ENC}(m, r_m)$,

(1) $(k_x \oplus r_m),\ \mathtt{ENC}(m, r_m) \leftarrow c_x$
(2) $(k_y \oplus r_m) \leftarrow (k_x \oplus k_y) \oplus (k_x \oplus r_m)$
(3) $c_y \leftarrow (k_y \oplus r_m) \,||\, \mathtt{ENC}(m, r_m)$
(4) **return** $c_y = \mathtt{MOTE}(m, k_y)$

坂崎らの方式 [6], [7] は，CRYPTREC 暗号リスト準拠の暗号関数の組合せのみで構成された Bidirectional，Multi-Hop，Interactive 型のプロキシ—再暗号化方式である．したがって，CRYPTREC 暗号リスト準拠より要件 1 を，Multi-Hop の性質より要件 5 を，Interactive の性質より要件 2 を満たしている．また，プロキシサーバに登録してある再暗号化鍵を削除することにより，以後，代理閲覧権限を無効化することができる．つまり要件 6 も満たすことができる．

しかし，坂崎らの方式 [6], [7] は，ユーザ X 宛の暗号化データをユーザ Y 宛に変換する再暗号化鍵 $rk_{xy} = k_x \oplus k_y$ と，ユーザ Y 宛の暗号化データをユーザ X 宛に変換する再暗号化鍵 $rk_{yx} = k_y \oplus k_x$ は，同じ値であるため，双方向に再暗号化が可能である．つまり Bidirectional であるため，要件 3 を満たしていない．また，坂崎らの方式 [6], [7] は，代理閲覧範囲を明示する機能を具備しておらず，それゆえ，このままでは要件 4 も満たしていない．

したがって，本提案では，CRYPTREC 暗号リスト準拠の暗号関数のみを用いて，坂崎らの方式 [6], [7] を Unidirectional（要件 3）にし，かつ，代理閲覧範囲を明示（要件 4）できるようにする．

5.2 前提条件

まず，提案方式の前提について説明する．提案方式のエンティティは，送信者 S，受信者 R，代理人 A，復代理人 A'，プロキシサーバ P である．一般的にインターネット上の脅威として，メッセージの盗聴・改竄，なりすまし等があげられるが，ここでは，本提案のシステムに対し，以下の状況を前提とする．

【前提条件】

(1) 各エンティティ間の通信路は，IPsec や TLS 等によって盗聴から守られている．
(2) メッセージ m には，送信者の電子署名等が施されており，改竄対策もされている．
(3) 各エンティティ間は相互に認証されていて，なりすましによる脅威からも守られている．
(4) 送信者 S，受信者 R，代理人 A，復代理人 A' は，提案方式のプロトコルに正しく従い，不正は働かない．なお，ここでの不正とは，故意によるメッセージの盗聴，秘密鍵の漏洩，エンティティ間の結託とする．
(5) プロキシサーバ P は，基本的に不正を行わないが，ある時点でマルウェア等により危殆化する可能性がある．

つまり，本前提のセキュリティモデルでは，攻撃者とは，プロキシサーバ P に感染したマルウェア等であり，そのマルウェア等が，プロキシサーバ P 上にある情報を用いて，受信者 R 宛の暗号化データを解読することと，受信者 R 宛の暗号化データを閲覧権限のない代理人 $\tilde{A}$ 宛に不正に再暗号化をすることを脅威とする．

この前提モデルの妥当性（特に前提条件 (4)，(5) の妥当性）は，政府（内閣府）が運営するマイナポータル等での適用を例にすると，理解を助けるかもしれない．

この場合，送信者 S は，マイナポータルと接続されている官庁（税務申告手続等）や自治体（介護保険手続等）の行政機関であり，行政機関の職員は，内部統制等の制度・規制・罰則により，不正を働かないとする．内部不正が問題視されるケースもあると思えるが，ここでは，内部統制等の制度・規制・罰則により，運用的な不正対策が施されていることを前提としている．

受信者 R は，行政機関からお知らせを受け取る本人であり，あえて不正をする意味がない．

代理人 A および復代理人 A' は，本人との信頼関係/契約で結ばれており，不正を行わないという前提を置いている．もちろん，現実の世界でも代理人等による不正は考えられるが，代理人等の不正行為は，忠実義務違反等の措置（運用的対策）で扱うとする．

プロキシサーバ P は，ここでは，政府が運営するポータ

ルサーバである．同サーバを運営・保守をしている職員も内部統制等の制度・規制・罰則により，不正対策済という前提を置いている．しかしながら，プロキシサーバ P は，常時インターネットに接続されているため，マルウェア等の脅威につねに晒されており，マルウェア対策を施しているとしてもマルウェア等に感染する可能性は否めない．それゆえ，ある時点でプロキシサーバ P は，マルウェアに感染し，感染後は，マルウェアによって不正を働く可能性があるとする．これは，参考文献 [16] で起きた情報漏洩事故のように，実際に起こりうるシナリオと考える．なお，ある時点とは，本論文では Protocol 1 の再暗号化鍵登録後とする．もちろん，マルウェア感染後に再暗号化鍵が追加登録されることも考えられるが，ここでは，そのリスクに対して別途対策を施すとし，検討の対象から外す．この前提は，参考文献 [7] と同じである．

それゆえ，本論文では，上記状況に鑑み，攻撃者をプロキシサーバ P に感染したマルウェア等とし，そのマルウェア等が，プロキシサーバ P 上にある情報を用いて，受信者 R 宛ての暗号化データを解読することと，受信者 R 宛ての暗号化データを閲覧権限のない代理人 $\tilde{A}$ 宛に不正に再暗号化をすることを脅威とする．

5.3 提案手法

5.3.1 委任状生成

本提案手法では，まず，ユーザ X からユーザ Y に与えた代理権の内容を委任状データ PA_{xy} として用意する．委任状データ PA_{xy} は，「本人情報（From）」と「代理人情報（To）」，「権限範囲情報」および「1 つ前の委任状データのハッシュ値」からなり，上記 4 つの情報を順序を保ちながら連結したデータとする．たとえば，送信者 S から受信者 R へ税分野の情報を送り，受信者 R が代理人 A にその税分野に関する代理権を与え，さらに代理人 A が復代理人 A' にその代理権を与える場合，委任状データはそれぞれ以下になる．

$$
\begin{aligned}
PA_{sr} &= \{\ ID_s,\ ID_r,\ \text{“}tax\text{”},\ Null\ \} \\
PA_{ra} &= \{\ ID_r,\ ID_a,\ \text{“}tax\text{”},\ h(PA_{sr})\ \} \\
PA_{aa'} &= \{\ ID_a,\ ID_{a'},\ \text{“}tax\text{”},\ h(PA_{ra})\ \}
\end{aligned}
$$

なお，本手法では，送信者 S から受信者 R へデータを送る場合でも委任状データを用いる．

5.3.2 鍵生成

本手法ではユーザ X ごとにマスタ秘密鍵 K_x を準備する．そして送信者 S から受信者 R 宛の委任状に基づく暗号化鍵 $k_s^{PA_{sr}}$ は，委任状データ PA_{sr} と送信者 S のマスタ秘密鍵 K_s を入力とした鍵付きハッシュ関数の出力値を，暗号化鍵としてそのつど動的に生成し，利用後には消去する．

$$
\begin{aligned}
k_s^{PA_{sr}} &= H(PA_{sr},\ K_s) \\
&= h((K_s \oplus opad)||h((K_s \oplus ipad)||PA_{sr}))
\end{aligned}
$$

なお，ここでのハッシュ関数 $h()$ は，原像計算困難性，第二原像計算困難性，衝突困難性を有する CRYPTREC 準拠の暗号学的ハッシュ関数であり，$H()$ は，$h()$ を繰り返し用いた HMAC [*8] に代表される鍵付ハッシュ関数とする．

また，受信者 R の復号鍵 $k_r^{PA_{sr}}$ も委任状データ PA_{sr} と受信者 R のマスタ秘密鍵 K_r を入力とした鍵付ハッシュ値としてそのつど動的に生成し，利用後に消去する．

$$
\begin{aligned}
k_r^{PA_{sr}} &= H(PA_{sr},\ K_r) \\
&= h((K_r \oplus opad)||h((K_r \oplus ipad)||PA_{sr}))
\end{aligned}
$$

5.3.3 再暗号化鍵登録

本手法では再暗号化鍵は委任状データごとに生成され，このとき，委任状データ PA_{sr} に依存した再暗号化鍵 $rk^{PA_{sr}}$ は，暗号化鍵 $k_s^{PA_{sr}}$ と復号鍵 $k_r^{PA_{sr}}$ より Protocol 1 を用いてプロキシサーバ P に委任状データ PA_{sr} と紐付けて登録される．

$$
rk^{PA_{sr}} = k_s^{PA_{sr}} \oplus k_r^{PA_{sr}} \quad \text{with} \quad PA_{sr}
$$

また，受信者 R-代理人 A 間の再暗号化鍵 $rk^{PA_{ra}}$ および代理人 A-復代理人 A' 間の再暗号化鍵 $rk^{PA_{aa'}}$ も，各々の鍵より Protocol 1 を用いて各委任状データとともに登録される．

$$
\begin{aligned}
rk^{PA_{ra}} &= k_r^{PA_{sr}} \oplus k_a^{PA_{ra}} \quad \text{with} \quad PA_{ra} \\
rk^{PA_{aa'}} &= k_a^{PA_{ra}} \oplus k_{a'}^{PA_{aa'}} \quad \text{with} \quad PA_{aa'}
\end{aligned}
$$

5.3.4 暗号化

本手法において送信者 S が受信者 R に税分野のメッセージ m を送る場合，送信者 S は，暗号化鍵 $k_s^{PA_{sr}}$ を動的に計算し，以下の暗号化データを生成する．

$$
c_s^{PA_{sr}} = \texttt{MOTE}(m, k_s^{PA_{sr}})
$$

そして暗号化データ $c_s^{PA_{sr}}$ を委任状データ PA_{sr} とともにプロキシサーバ P へ受信者 R 宛のデータとして送る．

5.3.5 再暗号化

受信者 R 宛の暗号化データ $c_s^{PA_{sr}}$ を受信したプロキシサーバ P は，添付の委任状データ PA_{sr} から該当再暗号化鍵 $rk^{PA_{sr}} = k_s^{PA_{sr}} \oplus k_r^{PA_{sr}}$ を選択し，再暗号化鍵 $rk^{PA_{sr}}$ と暗号化データ $c_s^{PA_{sr}}$ から Algorithm 1 を用いて，受信者 R が復号可能な暗号化データ $c_r^{PA_{sr}}$ へと変換する．

$$
c_r^{PA_{sr}} = \texttt{MOTE}(m, k_r^{PA_{sr}})
$$

5.3.6 復号

受信者 R は，プロキシサーバ P から自分宛の再暗号化

[*8] HMAC：Hash-based Message Authentication Code [14]．なお，ここで用いられる $opad, ipad$ は，HMAC を計算する際に利用される 2 つの異なる固定文字列である．

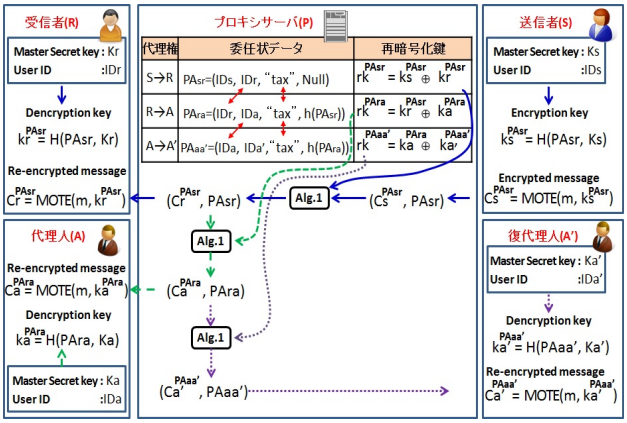

図 2 提案方式
Fig. 2 Proposed Scheme.

データ $c_r^{PA_{sr}}$ と添付の委任状データ PA_{sr} を受け取ると，自身のマスタ秘密鍵 K_r と添付の委任状データ PA_{sr} から復号鍵 $k_r^{PA_{sr}}$ を動的に計算し，再暗号化データ $c_r^{PA_{sr}}$ を復号する．

5.3.7 代理閲覧

プロキシサーバ P は，受信者 R 宛に再暗号化処理をした際，受信者 R の代理人宛にも再暗号化処理を施す．

プロキシサーバ P は，データベースに管理されている委任状データ PA_{ra} の中から，「委任状データ PA_{sr} の第 2 引数」と「委任状データ PA_{ra} の第 1 引数」が一致し，かつ「第 3 引数どうし」も一致する委任状データ PA_{ra} をすべて検索する．そして見つかった委任状データ PA_{ra} の第 4 引数が，委任状データ PA_{sr} のハッシュ値と等しいか確認する．

該当する委任状データ PA_{ra} が存在した場合，暗号化データ $c_r^{PA_{sr}}$ を閲覧する権限を有しているとして，委任状データ PA_{ra} に紐付く再暗号化鍵 $rk^{PA_{ra}}$ より再暗号化処理を施す．

また，同様にして委任状データ PA_{ra} の引数を比較し，復代理権を持つ委任状データ $PA_{aa'}$ を検索して，復代理人宛にも再暗号化処理を施す．以上の一連の流れを**図 2** に示す．

5.4 安全性

暗号方式の安全性評価に関するアプローチとして暗号理論に基づく安全性証明と形式手法に基づく自動検証がある．前者は，想定モデル内のあらゆる攻撃者に対する安全性を保証することができるが，証明が複雑になる傾向がある．一方後者は，特定の攻撃が可能かどうかのみの検査になるが，検証が比較的容易という利点がある．

坂崎らの既存方式の安全性評価 [7] は，形式手法による検証であり，具体的には，暗号化関数 MOTE および Protocol 1，Algorithm 1 は，5.2 節の前提条件の下，秘密鍵 k_x，k_y が漏洩しない限り，危殆化したプロキシサーバ P が P 上

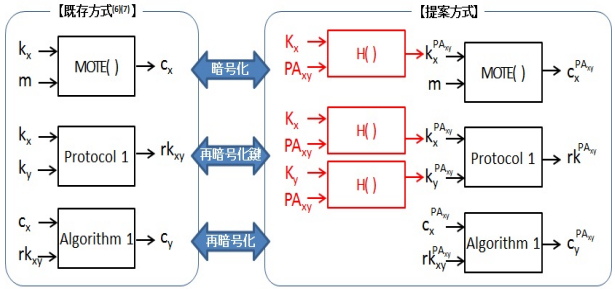

図 3 既存方式との違い
Fig. 3 Difference from the Existing Method.

にある情報を用いても，暗号化データを解読できないこと，閲覧権限のないユーザ宛に再暗号化できないこと，を形式手法を用いて検証している．なお，この形式手法による検証では，誕生日攻撃のような確率事象は考慮していない．本論文でも同様とする．詳しくは文献 [7] を参照していただきたい．

ここで，提案方式について考察する．提案方式は，既存方式において，鍵の生成方法を改良したものである．より具体的には，**図 3** に示すように提案方式では，ユーザ X の秘密鍵 k_x の代わりに，マスタ秘密鍵 K_x と委任状データ PA_{xy} を入力とする HMAC によって生成される鍵 $k_x^{PA_{xy}}$ を用いることが大きな改良点である．

ここで HMAC の安全性に関する補題 1 を紹介する．なお，補題 1 は，Bellare によって証明されている [15]．

補題 1 HMAC で使われているハッシュ関数内の圧縮関数が擬似ランダム関数であれば，HMAC も擬似ランダム関数であり，理想的なメッセージ認証コードとしての安全性を満たしている．すなわち十分大きなハッシュ長に対して秘密鍵 k が漏洩しない限り，第三者は，メッセージ M に対する正しい MAC 値 $= H(M, k)$ を生成することはできない．

実際に利用されるハッシュ関数には擬似ランダム関数とはいえない特性があるが，ここでは，HMAC で使われているハッシュ関数内の圧縮関数が擬似ランダム関数という仮定の下，提案方式（Proposed）の安全性が既存方式（Existing）と同等（Proposed ≡ Existing）であることを証明する．

命題 1 十分大きな HMAC で使われているハッシュ関数内の圧縮関数が擬似ランダム関数という仮定の下，提案方式は，マスタ秘密鍵 K_x，K_y が漏洩しない限り，危殆化したプロキシサーバ P が P 上にある情報を用いても，暗号化データを解読できない，また，閲覧権限のないユーザ宛に再暗号化できない．すなわち，同仮定の下，提案方式（Proposed）の安全性は，既存方式（Existing）と同等である．

証明 1 提案方式は，既存方式と比べて「5.3.2 鍵生成」のみに違いがあり，「5.3.3 再暗号化鍵登録」「5.3.4 暗号化」「5.3.5 再暗号化」「5.3.6 復号」は，既存方式そのものを用

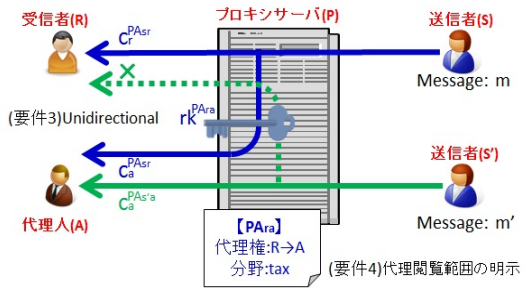

図 4 実現したいモデル
Fig. 4 Requirements Model.

いている．

すなわち提案方式は，秘密鍵 k_x の代わりに鍵 $k_x^{PA_{xy}}$ が用いられるという違いのみが生じる．したがって提案方式は，文献 [7] より，「$k_x^{PA_{xy}}$，$k_y^{PA_{xy}}$ が漏洩しない限り，危殆化したプロキシサーバ P が P 上にある情報を用いても，暗号化データを解読できない，また，閲覧権限のないユーザ宛に再暗号化できない」ということが導かれる．

また，補題 1 より，疑似ランダム関数の存在の仮定の下では，マスタ秘密鍵 K_x がない限り，その MAC 値にあたる鍵 $k_x^{PA_{xy}} = H(PA_{xy}, K_x)$ を計算することはできない．

したがって，同仮定の下，提案方式は，マスタ秘密鍵 K_x，K_y が漏洩しない限り，危殆化したプロキシサーバ P が P 上にある情報を用いても，暗号化データを解読できない．また，閲覧権限のないユーザ宛に再暗号化できない．

すなわち，HMAC で使われているハッシュ関数内の圧縮関数が擬似ランダム関数という仮定の下，以下が成り立つ．

$$\text{Proposed} \equiv \text{Existing}\ .$$

5.5 要件 3 および要件 4 を満たす追加機能について

提案方式では，鍵生成方法の改良により，「委任状単位で再暗号化を制御すること」と「委任内容を表示すること」を実現し，要件 3（Unidirectional）と要件 4（代理閲覧範囲の明示）を満たすようにしている（図 4）．

本節では，要件 3 および要件 4 の充足性について説明する．まず要件 3 についてである．

命題 2 5.2 節の前提条件および補題 1 の HMAC が疑似ランダム関数という仮定の下，代理閲覧権限の付与に関して受信者 R 宛の暗号化データ $c_r^{PA_{sr}}$ を代理人 A 宛に変換する再暗号化鍵 $rk^{PA_{ra}}$ のみが登録されている状況下において，提案方式におけるプロキシサーバ P は，逆方向の再暗号化，すなわち，送信者 S' から委任状データ $PA_{s'a}$ に基づく代理人 A 宛の暗号化データ $c_a^{PA_{s'a}}$ を再暗号化鍵 $rk^{PA_{ra}}$ を用いて受信者 R 宛に正しく変換することはできない．

証明 2 5.2 節の前提条件より，各ユーザは，プロトコルに従い，正しい再暗号化鍵を登録する．また，送信者は，正しい暗号化データを送信する．

既存方式では，受信者 R 宛を代理人 A 宛に変換する再暗号化鍵 rk_{ra} と代理人 A 宛を受信者 R 宛に変換する再暗号化鍵 rk_{ar} が同じ値になるのに対し，提案方式では，受信者 R 宛の暗号化データ $c_r^{PA_{sr}}$ を代理人 A 宛に変換する再暗号化鍵 $rk^{PA_{ra}}$ と代理人 A 宛の暗号化データ $c_a^{PA_{s'a}}$ を受信者 R 宛に変換する再暗号化鍵 $rk^{PA_{ar}}$ は，偶然の一致を除いて異なる値になる．それゆえ，この状況下では，受信者 R には，該当データの閲覧権限は与えられていない．

ゆえに，命題 1 より，プロキシサーバ P は，閲覧権限のない受信者 R 宛には，暗号化データ $c_a^{PA_{s'a}}$ を再暗号化することはできない．

次に要件 4 についてである．提案方式は，代理権の範囲を委任状データ PA_{ra} として明示できる．ここではプロキシサーバ P に登録されている委任状データの改竄に関し，以下の命題を証明する．

命題 3 ユーザ Y' にユーザ X' 宛の暗号化データ $c_{x'}^{\hat{P}A_{s'x'}}$ の閲覧権限を与える委任状データを $\hat{P}A_{x'y'}$ とする．また，ユーザ Y にユーザ X 宛の暗号化データ $c_x^{PA_{sx}}$ の閲覧権限を与える委任状データを PA_{xy} とし，PA_{xy} に基づく再暗号化鍵 $rk^{PA_{xy}}$ がプロキシサーバ P に登録されているとする．

このとき，5.2 節の前提条件および補題 1 の HMAC が疑似ランダム関数という仮定の下，ユーザ X' 宛の暗号化データ $c_{x'}^{\hat{P}A_{s'x'}}$ をユーザ Y' 宛に再暗号化する権限は何も与えられていない状況下で，プロキシサーバ P に登録されている委任状データ PA_{xy} を $\hat{P}A_{x'y'}$ に改竄しても提案方式におけるプロキシサーバ P は，ユーザ X' 宛の暗号化データ $c_{x'}^{\hat{P}A_{s'x'}}$ をユーザ Y' 宛に正しく変換することはできない．

証明 3 5.2 節の前提条件より，各ユーザは，プロトコルに従い正しい再暗号化鍵を登録する．また，送信者は，正しい暗号化データを送信する．

この状況において，プロキシサーバ P に登録されている委任状データ PA_{xy} を $\hat{P}A_{x'y'}$ に改竄しても実際に閲覧権限を与える再暗号化鍵 $rk^{PA_{xy}}$ 自身は変わらない．再暗号化鍵 $rk^{PA_{xy}}$ は，元々の委任状データ PA_{xy} に基づいて生成されているため，委任状データ PA_{xy} を $\hat{P}A_{x'y'}$ に改竄しても，ユーザ X' 宛の暗号化データ $c_{x'}^{\hat{P}A_{s'x'}}$ をユーザ Y' 宛に再暗号化する権限は与えられていない，という状況は変わらない．

ゆえに，命題 1 より，プロキシサーバ P は，閲覧権限のないユーザ Y' 宛にユーザ X' 宛の暗号化データ $c_{x'}^{\hat{P}A_{s'x'}}$ を再暗号化することはできない[*9]．

[*9] もっとも，プロキシサーバ上の委任状データを改竄することによって本来閲覧できる正当な権利者でも閲覧できなくするような攻撃は可能であり，それらの攻撃はサービス上，問題となりうるが，閲覧不可にする攻撃は，プロキシ再暗号化方式の導入にかかわらず，危殆化されたプロキシサーバ上では，各データを消去すれば起こりうる課題であり，これは危殆化したシステム全体の課題として扱うべきであろう．

表 3 既存方式との比較
Table 3 Comparison with the Existing Method.

	要件 1	要件 2	要件 3	要件 4	要件 5	要件 6
既存方式 [6], [7]	○	○	×	×	○	○
提案方式	○	○	○	○	○	○

5.6 既存方式との比較

表 3 に記すように提案方式は，既存方式と比べて要件 3，要件 4 を満たす機能が追加されている．一方で既存方式は，本人–代理人間で再暗号化鍵を登録するのに対し，提案方式は，委任状ごとに再暗号化鍵を登録しなければならない．それゆえ，プロキシサーバでは，既存方式よりも多くの再暗号化鍵を管理する必要がある．

しかしながら本論文では，法律で定められた業務における手続を題材にしており，依頼する業務ごと，すなわち委任状ごとに代理人が選ばれることが多く，委任状の数と代理人の数との差はさほど生じない．稀に税理士資格を持った介護保険施設の長に税務処理と介護保険手続を依頼する場合があるかもしれない．その場合，既存方式では，2 つの手続を同一人物に依頼するのでプロキシサーバに登録する再暗号化鍵を 1 つにすることができたのに対し，提案方式では，たとえ同一人物に依頼したとしても税務処理用と介護保険手続用と 2 つの再暗号化鍵を登録しなければならなくなる．

ここで参考のため，プロキシサーバにおける再暗号化鍵管理コストを比較する．なお，ここでは，再暗号化鍵のデータ長は，ハッシュ関数の出力長の 32 byte として換算する．

行政手続等の棚卸結果 [17] によると平成 29 年度時点で 46,385 種類の手続等が存在する．仮に A さんがすべての手続に対して B さんを代理人にしたとすると，A-B 間で登録される再暗号化鍵の総データ長は，既存方式では 32 byte であるのに対し，提案方式では 32 byte × 46,385 = 約 1.5 Mbyte となる．上記は一例であるが，この差は，昨今の情報機器の容量を考慮するとそれほど大きな差ではないと考える．

むしろこの場合，46,385 個の委任状の管理の方が煩雑になる．ただし本論文で扱う業務は，法律で定められた業務であるため，暗号プロトコルによらず，委任状は法律に基づき依頼の数だけ要求される．それゆえ，既存方式を用いても何らかの委任状を別途管理する必要があり，委任状の管理コストに関して，提案方式とさほど変わりはないと考える．

6. まとめ

公共手続システムに限らずシステムを構成する場合，そこには，ルールが必要である．法制度は，社会ルールを表現したものであり，ICT 技術により新しい社会システムを構築する場合には，その構築するシステムが，どのような法制度に対応しているかを把握し，矛盾のないシステムになるように設計することが重要である．

本論文では，上記状況に鑑み，安全な代理閲覧を実現する一方式として，プロキシ再暗号化方式の適用について，日本の法制度に沿って分析を行い，プロキシ再暗号化方式に求められる 6 つの要件を定義した．

また，本論文では，代理人制度のシステム化においては，Unidirectional，Multi-Hop，Interactive の性質が備わったプロキシ再暗号化方式が適していることを導いた．

さらに，要件 1，2，5，6 を満たす既存方式 [6], [7] をベースに，要件 3，4 も満たすように鍵生成部分を改良し，上記 6 要件をすべて満たす方式を提案した．

なお，情報分野において法律と技術の両方から検討している関連研究として，情報法制研究会 [18] の研究がある．

多種多様な技術・サービスの普及やグローバル化によって情報通信を取り巻く環境は大きく変化しており，情報分野においても個人情報保護を取り巻く諸課題，パーソナルデータの利活用，諸外国の制度との整合性等，将来を見据えた法的課題の検討が必要である．

情報法制研究会 [18] では，全 8 回のシンポジウムを通じて，国内外における情報法制に関する法的課題の調査および研究を行っており，ここで議論された資料は，参考文献 [18] より入手可能である．参考にされたい．

参考文献

[1] Blaze, M., Bleumer, G. and Strauss, M.: Divertible Protocols and Atomic Proxy Cryptography, *EUROCRYPT*, Vol.1403 of LNCS, pp.127–144 (1998).
[2] Canetti, R. and Hohenberger, S.: Chosen-Ciphertext Secure Proxy Re-encryption, *Proc. 14th ACM Conference on Computer and Communications Security-ACM, CCS 2007*, pp.185–194 (2007).
[3] 草川恵太：関連鍵攻撃に対する識別不可能性と双方向代理人再暗号化，SCIS2011 2A2-5 (2011).
[4] 林良太郎，松下達之，吉田琢也，藤井吉弘，岡田光司：プロキシ再暗号化における結託攻撃に対する再暗号化鍵偽造不可能性，SCIS2012 2A1-4 (2012).
[5] Angelos, D.C., Cook, D.L. and Keromytis A.D.: Conversion and Proxy Functions for Symmetric Key Ciphers, *IEEE International Conference on Information Technology: Coding and Computing* (*ITCC*), pp.552–557 (2005).
[6] 坂崎尚生，安細康介，細矢 淳：共通鍵暗号ベースの再暗号方式の検討，SCIS2014, 2D4-1 (2014).
[7] Watanabe, D., Sakazaki, H. and Miyazaki, K.: Representative System and Security Message Transmission using Re-encryption Scheme Based on Symmetric-key Cryptography, *Journal of Information Processing*, Vol.25, pp.67–74 (Jan. 2017).
[8] Green, M. and Ateniese, G.: Identity-Based Proxy Reencryption, *Applied Cryptography and Network Security*, Vol.4521 of LNCS, pp.288–306 (2007).
[9] He, Y.-J., Chim, T.W., Hui, L.C.K. and Yiu, S.-M.: Non-Transferable Proxy Re-Encryption Scheme for

Data Dissemination Control, *Cryptology ePrint archive*, available from ⟨http://eprint.iacr.org/2010/192.pdf⟩ (accessed 2019-03).
[10] 清藤武暢，野倫太郎，四方順司：ID ベース暗号による代理人再暗号化方式の一般的構成法，SCIS2014 4E1-1 (2014).
[11] Liang, X., Cao, Z., Lin, H. and Shao, J.: Attribute based proxy re-encryption with delegating capabilities, *Proc. 4th International Symposium on Information, Computer, and Communications Security, ASIACCS'09*, pp.276–286, ACM (2009).
[12] Kawai, Y. and Takashima, K.: Fully-Anonymous Functional Proxy-Re-Encryption, Cryptology ePrint Archive (2013), available from ⟨http://eprint.iacr.org/2013/318.pdf⟩ (accessed 2019-03).
[13] Cryptrec, available from ⟨http://www.cryptrec.go.jp/index.html⟩ (accessed 2019-03).
[14] The Keyed-Hash Message Authentication Code (HMAC), FIPS PUB 198-1, available from ⟨https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.198-1.pdf⟩ (accessed 2019-03).
[15] Bellare, M.: New proofs for NMAC and HMAC: Security without collision-resistance, *Proc. Advances in Cryptology, CRYPTO'06, 26th Annual International Cryptology Conference*, Dwork, C. (Ed.), Lecture Notes in Computer Science Vol.4117, pp.602–619, Springer-Verlag (2006).
[16] Credit Card Processor Says Some Data Was Stolen, New York Times, January 20 (2009), available from ⟨http://www.nytimes.com/2009/01/21/technology/21breach.html?_r=3&ref=technology⟩ (accessed 2019-03).
[17] 行政手続等の棚卸結果等の概要，内閣官房 IT 総合戦略室 総務省（平成 30 年 3 月 30 日），入手先 ⟨https://cio.go.jp/sites/default/files/uploads/documents/tanaoroshi_gaiyou.pdf⟩（参照 2019-03）.
[18] 情報法制研究会：一般財団法人日本データ通信協会，入手先 ⟨https://www.dekyo.or.jp/kenkyukai/symposium8.html⟩（参照 2019-03）.

坂崎 尚生 （正会員）

1971 年生．1999 年北陸先端科学技術大学院大学情報科学研究科博士後期課程修了．博士（情報科学）．同年（株）日立製作所システム開発研究所入社．セキュリティに関する研究に従事．