推薦論文

P2P データ共有における暗号化データのアクセス制御

渡邊裕治† 沼尾雅之†

P2P 技術に基づくデータ共有では，従来型の静的に構成されたネットワークにおけるデータ共有と異なり，Peer のネットワークからの離脱や再参加が頻繁に行われる．一方で，データ共有システムとして一貫したセキュリティとサービスを提供するために，非接続状態にある Peer の復号鍵を必要とする場面が頻繁に起こりうる．そのため，復号鍵を行使する権限を一時的に，かつ時限的に他の Peer に委譲できれば，Peer が非接続状態となる際でも他の Peer が復号処理を継続可能にできるので，きわめて柔軟なセキュリティサービスの構築が可能となる．本論文では，「変換サーバ」と呼ぶ中立な第三者機関を利用することで，暗号文の受信者が，特定の期間，復号処理の代行を代行者に対して依頼できる枠組みを実現する．提案手法は次の特徴を持つ．(1) 閾値復号の技術を応用することで，受信者の秘密鍵の運用を変換サーバと代行者の間で分散することにより，代行者が変換サーバのチェックを通過した場合にのみ，暗号文の復号処理が行えるようにする．また，復号処理を通じて，変換サーバ・代行者のいずれも受信者の秘密鍵を知ることはできないため，複数の暗号文の復号を鍵の再配布なしに実行可能である．(2) 一方向性ハッシュ関数を利用し，復号処理に権限委譲期間のチェック機能を含めることにより，代行者は変換サーバが行う復号時間のチェックを通過しない限り復号ができず，また，権限委譲期間を偽って変換サーバに報告しても復号を継続することができない．(3) 変換サーバの公開鍵を利用することで，受信者が単独で委任鍵を生成し代行者に与えるだけで復号権限の委譲を完了することを可能にする．これにより実現される復号権限の委譲は，P2P の環境だけでなく，インターネット上の一般の端末に対しても広く利用することが可能である．

Access Control for Encrypted Data in P2P Data Sharing

Yuji Watanabe† and Masayuki Numao†

A cryptographic approach that enables a peer to transfer the right to access the encrypted data provided predetermined conditions are satisfied is presented in this paper. Our approach involves a third trusted service, called “delegation check servers” to check single or multiple conditions according to the regulations. A peer (delegator) delegates the right to decrypt the ciphertext to other peers (proxies) under certain conditions. The proxy can decrypt the ciphertext only after it passes the verification check of the delegation check server.

1. はじめに

1.1 背景

インターネット上で複数の端末がデータを安全に共有することは，ネットワークの障害に対する耐性を向上したり，多様なアクセスを可能にしたりするために必須の技術となっている．とりわけ，P2P 技術を用いたデータ共有システム（**図 1**）において，Peer のデータを権限のある Peer にだけ開示するとともに，権限のない Peer がアクセスできないようにするために暗号化技術が用いられる．暗号化により，データに対するアクセスを Peer の保持する復号鍵によりコントロールすることが可能となるが，これは同時に，Peer が非接続状態にある場合にそのデータを利用できないことを意味する．Peer がモバイル端末などから構成される場合には，Peer の接続解除・再接続が頻繁に起こりうると想定され，システム全体の可用性を下げかねない．たとえば，複数の Peer による連続処理が必要な処理を考えると，非接続状態になっている Peer の代行処理を別の信頼できる Peer に委譲することが望ましい．すなわち，Peer が非接続状態になっている間だけ，他の接続していて信頼できる Peer に復号権限

† 日本アイ・ビー・エム東京基礎研究所
Tokyo Research Laboratory, IBM Japan

本論文の内容は 2002 年 10 月の第 10 回マルチメディア通信と分散処理ワークショップにて報告され，DPS 研究会主査 により情報処理学会論文誌への掲載が推薦された論文である．

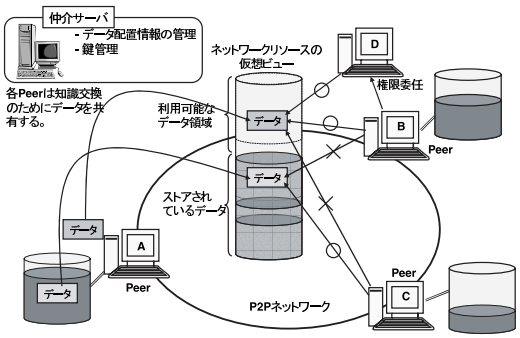

図 1 P2P データ共有
Fig. 1 P2P data sharing.

を委譲できれば，暗号化されたデータに対するアクセシビリティが大きく広がり，秘匿性と耐性を兼ね備えたデータ共有を構築することが可能になる．

より一般的なモデルとして，公開鍵暗号を用いた通信を考える．送信者は受信者の公開鍵でメッセージを暗号化し，公開鍵に対応する秘密鍵を持つ受信者のみが暗号文を復号することができる（以後,「受信者」という語を暗号文に対応する秘密鍵（復号鍵）を保持するメンバを指して用いる）．ここで，ネットワークに非接続状態にあるなどの理由により，受信者が秘密鍵を用いた復号処理を行使できない場面を考える．複数のホストが関わる連続処理プロセスなどにおいて，特定の受信者が非接続状態にあるために処理が中断されることが望ましくない場面は数多く存在する．このような処理の中断を避けるために，受信者が，非接続状態になる前に自身が持つ復号権限を，受信者が指名した代行者に対して委譲できる手法が望まれている．特定の受信者の復号処理を必要とし，かつその受信者が非接続状態にある場合には，あらかじめ指定された代行者に対して復号処理の代行を依頼することで，連続処理の中断を避けることが可能となる．

本論文は，有効期間を含む制約条件が成立する場合に限り暗号文を復号する権限を他のホストに対して委譲する機能を，単一または複数の制約条件の成立の検証を行う変換サーバを用いて実現する手法を示す．提案手法は次のような性質を持つ．

- 閾値復号の技術を応用することで，受信者の秘密鍵の運用を変換サーバと代行者の間で分散することにより，代行者が変換サーバのチェックを通過した場合にのみ，暗号文の復号処理が行えるようにする．また，復号処理を通じて，変換サーバ・代行者のいずれも受信者の秘密鍵を知ることはできない．
- 一方向性ハッシュ関数を利用し，復号処理に制約条件のチェック機能を含めることにより，代行者は変換サーバが行う制約条件が成立するかのチェックを通過しない限り復号ができず，また，満たすべき制約条件を偽って変換サーバに報告しても復号を継続することができない．
- 変換サーバの公開鍵を利用することで，受信者が単独で委任鍵を生成し代行者に与えるだけで復号権限の委譲を完了することを可能にする．これにより，復号権限の委譲が容易に行える．

提案手法は，P2P の環境のように多くの端末が自立分散的に機能するネットワークに対してだけでなく，一般的なインターネット環境に接続された端末間でのデータ共有の際のアクセス制御など P2P 以外の環境でも広く利用できる要素技術となりうる．提案手法は，基本方式と拡張方式の 2 つからなる．基本方式は，変換サーバがプロトコルを逸脱しない限り安全である．拡張方式は，変換サーバの不正に対する耐性を持たせるために，秘密分散の技術を利用して受信者が権限委譲時に複数の変換サーバを利用するように指定できるようにする．いずれの方式を選択するかは，受信者が単独で決定することができ，変換サーバや送信者に依存しない．

1.2 従来技術

復号権限の委譲に関する「代理復号（Proxy Cryptosystem）」としては，文献 1)~3) がある．文献 1) はある受信者 A に対して送られてきた暗号文 C_A を代行者 P に対してフォワードすることを可能にする．暗号文 C_A の復号には，本来受信者の秘密鍵 sk_A が必要であるが，これを代行者の秘密鍵 sk_B で復号可能な暗号文 C_B に変換する効率的な手法を提示している．文献 2) は，受信者 A に対する任意の暗号文を代行者 P が復号可能な暗号文にする変換関数 $\pi_{A\to B}$ の構成方法を ElGamal 暗号に対して示した．文献 2) の変換関数は任意の暗号文に適用可能であるため，変換時に受信者 A の関与を必要としないことが長所である．文献 3) は，変換関数 $\pi_{A\to B}$ の運用を複数の変換サーバに分散する手法を提案した．文献 3) は，一定以上の変換サーバの不正がなければ受信者 A の秘密鍵 sk_A が明かされず，また変換関数を構成する際に代行者 P の秘密鍵を必要としないため，秘密鍵に関する文献 2) の問題点に対する一定の解決法を示している．

復号権限を恒久的に委譲するのであれば，明らかに受信者の持つ秘密鍵の情報を代行者に与えるか，あるいは前述の手法を応用することで対応できる．だが，

一般的な権限委譲は恒久的な権限の譲渡ではなく，その権限の行使できる条件を限定した形で行われる．たとえば，ある開始時刻から復号権限を有効にし，ある終了時刻に復号権限を無効化したいという場面は頻繁に起こりうるであろう．

時限的な復号権限の委譲を実現するために必要となる要件の 1 つとして，特定の時刻まで暗号文が復号できず，その時刻以降に復号を可能にすることがある．この問題を暗号学的に取り扱う「時間鍵暗号」の研究としては，文献 4)〜6) などがある．時間鍵暗号とは，送信者がメッセージを暗号化する際に，ある時刻以前に暗号文が復号できないように送信する暗号化および復号の手法である．文献 4) では，解の導出に一定の時間がかかるような問題に復号処理を帰着させ，提示する問題の難しさをコントロールすることで，復号可能になる時間を設定する暗号化を示している．ここでは時間の指定として，相対的な復号時間の指定のみが可能である．絶対時間の指定が可能な手法として，文献 5) では，時間に対応する公開鍵を用意することで，復号時刻を指定できる手法を示している．また，文献 6) は絶対時間を指定できる時間鍵暗号を，時刻サーバとの通信を必要とするかわりに，時間パラメータに比例しない処理量で実現する手法を示している．

本論文で考えたい時限的な権限委譲は，暗号文の受信者が復号の代行者に権限を委任する期間を制限するモデルである．復号鍵を無効化することは，復号が代行者単独で可能である限り，原理的に不可能である．したがって提案手法は，「変換サーバ」と呼ぶ権限チェックを行う第三者を置いている．そのうえで重要なことは，(1) 暗号文の送信者が権限委譲に関するいっさいを関知する必要がないこと，(2) 指定期間のみ復号権限を行使することを可能にする枠組みを提供すること，である．

2. 準　　備

2.1 定　　義

問題を定義するために参加者として次の 4 者を定義する．

- 送信者（S）：メッセージの送信者．受信者の公開鍵でメッセージを暗号化して送信する．
- 受信者（R）：暗号化されたメッセージの受信者．公開鍵 e_R に対応する秘密鍵 d_R を持つ．
- 代行者（P）：受信者 R に対する暗号文を代行して復号するメンバ．
- 変換サーバ（T）：復号時に代行者 P が，受信者 R に指定された制約条件を満足するかを検証するサーバ．公開鍵 e_T に対応する秘密鍵 d_T を持つ．

提案手法は，次の 2 つのプロトコルを構成要素とする．

- $\Psi(d_R, \phi)$：受信者 R の秘密鍵 d_R，および（有効期限などの）制約条件 ϕ を入力として委任鍵 σ を出力する委任鍵生成アルゴリズム．
- $\Gamma(\sigma, \phi, c)$：代行者 P と変換サーバ T の間のプロトコルで，制約条件 ϕ が成立する場合に限り，P は T から暗号文 c に対応する平文 m を得る．

ここで，制約条件 ϕ は有効期間を含む一般的なポリシー記述であり，変換サーバ T が検証可能な条件であるとする．たとえば，ϕ を「時刻 t_1 から時刻 t_2 までの期間，代行者 P に対して」とした場合，T は「時刻 t_1 と t_2 の間であること」かつ「検証の要求者が P であること」を判定する．

2.2 モ デ ル

提案手法では，「制約条件付きの復号権限の委任」として次のモデルを考える．

(1) 送信者 S は，メッセージ m を受信者 R の公開鍵 e_R を用いて暗号化し，得られた暗号文 c を R に送信する．

(2) R は，制約条件 ϕ が成立することを条件として，e_R を用いて暗号化された暗号文の復号権限を代行者 P に委譲する．そのために，R の秘密鍵 d_R から委任鍵 $\sigma = \Psi(d_R, \phi)$ を生成し，(σ, ϕ) を P に秘密に送信する．

(3) ϕ が成立する場合，P は ϕ，σ および c を入力として，T とプロトコル Γ を実行することにより，メッセージ m を復号する．

本論文は，上記モデルに基づき，次にあげる要件を満たす委任鍵生成 Ψ および代理復号 Γ の構成法を示す．

- Γ において，ϕ が不成立なら，P は m を得ることはできない．
- Γ は P と T の間の 1 ラウンドの通信により実現される．
- S の操作に変更を加えない．
- Ψ は，R が単独で実行でき，T や P と通信を必要としない．
- T は S，R，P に依存する情報を保持する必要がない．
- Γ において，T は d_R に関する情報を得ることができない．
- P は，σ および Γ の実行により d_R に関する情報を得ることができない．

2.3 パラメータ

以降，次のパラメータを用いる．G_q を大きな素数 q を位数とし，その上での離散対数問題を解くことが計算量的に困難な群とする．簡潔のため，そのような群として，p，q を $q|p-1$ を満たす大きな素数とし，g は有限体 Z_p 上の位数 q の元としたときに，g を生成元として構成される群をとる．以降，特に記述のない場合冪演算はすべて mod p 上，また指数に関する演算はすべて mod q 上で行われるものとする．$H(\cdot)$ を整数空間から Z_q 上への理想的な暗号学的な一方向性関数とする．E はメッセージ空間 $\mathcal{M}$ から暗号文空間 $\mathcal{C}$ への公開鍵暗号である．ここで，E は選択的暗号文攻撃に対して強秘匿な公開鍵暗号[7),8)]とする．表記 $E(e,m)$ は公開鍵 e を用いたメッセージ m の暗号化を示し，対応する復号として，復号鍵 d を用いた暗号文 c の復号を $D(d,c)$ と記す．

E とは独立に，メッセージの暗号化関数として，ElGamal 暗号[9)]を想定する．秘密鍵を $x(\in Z_q)$，公開鍵を $y=g^x$ とすると，ElGamal 暗号は次のとおりである．メッセージ $m \in Z_p^*$ に対する暗号文 (c_1,c_2) は，ランダムに選択した $r \in Z_q$ および公開鍵 y を用いて，$c_1=g^r$，$c_2=my^r$ として計算される．復号は，秘密鍵 x を用いて，$c_2/{c_1}^x=m$ により計算される．

3. プロトコル

制約条件付きの復号権限の委譲を実現する手法として，本論文では，基本方式およびその拡張方式の 2 方式を示す．2 つの違いは変換サーバ T に対する信頼の仮定の強さである．いずれの方式も，次のような状況を想定する．送信者 S が受信者 R に向けてメッセージ $m \in Z_p^*$ を ElGamal 暗号化して送信する☆．S は，乱数 $r \in Z_q$ および R の公開鍵 $e_R=g^{d_R}$ を用いて，$c_1=g^r$，$c_2=m(e_R)^r$ を計算する．暗号文 (c_1,c_2) は S から R または代行者 P に対して送信される．R は，復号権限を代行者 P に対して委譲し，制約条件 ϕ が成立する場合に限って，P に復号処理の代行を依頼するものとする．

3.1 基本方式

変換サーバ T が完全に信頼できると仮定する基本方式を示す．ここで「T を信頼する」とは，T が知りえた情報を他者に漏らしたり，他者と結託して不正を行ったりするなど，定められた手順を逸脱した行為を行わないことを意味する．

(1) 委任鍵生成アルゴリズム Ψ

Ψ は，秘密鍵 $d_R(\in Z_q)$ を持つ受信者 R が，制約条件 ϕ の下で，代行者 P に対して復号権限を委譲するための委任鍵 σ を生成するアルゴリズムである．最初に，R は，乱数 $v \in M$ を選択し，委任鍵 $\sigma=(u_T,u_P)$ を次式より計算する．

$$u_T = E(e_T, v)$$
$$u_P = d_R - H(\phi, v) \pmod q$$

(2) 代理復号 Γ

Γ は受信者 R により委任された代行者 P と変換サーバ T の間での 2 者間プロトコルである．委任鍵 $\sigma=(u_T,u_P)$ を持つ P は，Γ を実行することにより，制約条件 ϕ が成立する場合に限り，R に対する暗号文 (c_1,c_2) を復号することができる．ここで，T と P の間の通信は SSL などにより実現される安全な通信路を用いて行われるものとする．

(a) P は u_T，ϕ および c_1 を T へ送信する（u_P は送信しない）．

(b) T は ϕ を評価する．ϕ が成立する場合には，T は $c_T={c_1}^{H(\phi,D(d_T,u_T))}$ を計算し，P へ送る（ここで，離散対数問題の困難性から P は c_T から $H(\phi,D(d_T,u_T))$ を計算できない）．不成立の場合には，エラーメッセージを送る．

(c) P は c_1，c_2，c_T を用いて，
$$m = c_2{c_1}^{-u_P}{c_T}^{-1}$$
を計算することによりメッセージを復号する．

基本方式の安全性を考える．まず，代理復号 Γ において代行者 P は変換サーバ T から送信される c_T の情報なしにメッセージを復号できないこと，(2b) の段階で変換サーバにより制約条件 ϕ の正当性をチェックされていること，(2a) の段階で送られる ϕ を偽った場合，(2b) において復号を可能にする c_T を得ることができないこと，により，P が復号を実行できるのは，ϕ が満たされる場合に限定される．次に，代理復号 Γ の実行中に変換サーバが d_R に関して知るのはたかだか d_R-u_P のみである．u_P は変換サーバ T に明かされないため，変換サーバ T が d_R に関する情報を得ることはできない．一方，P が得ることのできるすべての情報は ϕ，c_1，c_2，c_T，u_P，e_R，e_T である．秘密鍵 d_R に関して $d_R=u_P+H(\phi,D(d_T,u_T))$ が成立すること，および d_T を用いた復号 $D(d_T,u_T)$

☆ より一般的には，メッセージ M を鍵 K を用いて対称鍵暗号で暗号化し，その鍵 K を ElGamal 暗号化して送信する場面があるが，この場合鍵 K を送信対象メッセージ m と見なすことで同一視することが可能である．

は T のみが知りうることから，d_R を得ることはできない．

3.2 拡張方式

基本方式は T が完全に信頼できると仮定する．T が不正に $w = D(d_T, u_T)$ を代行者 P へ知らせた場合，代行者 P は $d_R = u_P + H(\phi, w)$ により d_R を計算できるため，安全性は T の信頼性に大きく依存する．そこで，複数の変換サーバ $T_1, \ldots, T_n$ を利用することで，単一の変換サーバによる不正を防止する拡張方式を示す．拡張方式は代理復号 Γ の完了するために，n 個のサーバのうち $t(> n/2)$ 個の変換サーバの検証を通過することを必要とする．一方，t 個の変換サーバが正確に動作する限り不正な変換サーバおよび代行者はメッセージを不正に復号したり，d_R を知ったりすることはできない．以下，T_i の公開鍵を e_i，復号鍵を d_i，ID を i とする．

(1) 委任鍵生成アルゴリズム Ψ

Ψ は秘密鍵 $d_R(\in Z_q)$ を持つ受信者 R が，制約条件 ϕ の下で代行者 P に対して復号権限を委譲するための委任鍵 σ を生成するアルゴリズムである．R は代理復号 Γ に必要な変換サーバ集合 $T_1, \ldots, T_n$ を選択する．選択されたサーバの ID 集合を $\Lambda = \{1, \ldots, n\}$ とする．各サーバ T_i $(i \in \Lambda)$ に対し，R は $v_i \in Z_q$ をランダムに選び，$u_{T_i} = E(e_i, v_i)$ を計算する．次に，$f(0) = d_R$ および $f(i) = H(\phi, v_i)$ $(i \in \Lambda)$ を満たす n 次の多項式を

$$f(x) = \lambda_0(x) \times d_R + \sum_{i \in \Lambda} \lambda_i(x) \times H(\phi, v_i) \bmod q$$

により計算する．ここで，$\lambda_i(x)$ は Lagrange の係数を計算する関数で，

$$\lambda_i(x) = \prod_{i \in \Lambda, j \neq i} (x - j)/(i - j) \bmod q$$

である．R は，P が Γ 実行時に検証を通過する必要のあるサーバの数 t を決定し，$Z_q \backslash (\Lambda \cup \{0\})$ から $n - t + 1$ 個の要素の集合 Ω を選ぶ．そして，$\tau_j = f(j)$ により，$u_P = \{(j, \tau_j) | j \in \Omega\}$ を計算する．委任鍵 σ は u_P および $u_{T_1}, \ldots, u_{T_n}$ により構成される．

(2) 代理復号 Γ

Γ は代行者 P と t $(\leq n)$ 個の変換サーバの間でのプロトコルである．P は，委任鍵 σ および制約条件 ϕ を用いて，t 個の変換サーバの検証を通過した後，受信者 R に対する暗号文 (c_1, c_2) を復号できる．P が選択した t 個のサーバの ID 集合を $\mathcal{T} = \{1, \ldots, t\}$ とする．このとき，P は以下のプロセスをすべての $i \in \mathcal{T}$ に対して繰り返す．

(a) P は ϕ, u_{T_i}, c_1 を T_i に対して送信する．

(b) T_i は ϕ を検証し，不成立の場合はエラーを返す．成立する場合は，$c_{T_i} = {c_1}^{H(\phi, D(d_i, u_{T_i}))}$ を計算し，P へ送信する．

P は $c_{T_1}, \ldots, c_{T_t}$ を受信した後，P はメッセージ m を

$$m = c_2 {c_1}^{-(\Sigma_{i \in \Omega} \theta_i \tau_i)} \left(\prod_{i \in \mathcal{T}} {c_{T_i}}^{\theta_i}\right)^{-1}$$

ここで θ_i は，

$$\theta_i = \prod_{j \in \Omega \cup \mathcal{T}, j \neq i} j \times (j - i)^{-1} \bmod q$$

とする．

$t - 1$ 個のサーバ $T_1, \ldots, T_{t-1}$ と P が結託した場合を考える．すなわち，P が $d_1, \ldots, d_{t-1}$ を持っているものとする．この場合，メッセージ m を復号することと，ϕ が成立しない限り，P は m を計算することができない．その場合，T_t からの応答 c_{T_t} を計算することは等価である．だが，$c_{T_t} = {c_1}^{H(\phi, D(d_t, u_{T_t}))}$ であるから，H および D の性質から，T_t の秘密鍵 d_t なしに，c_{T_t} を計算することはできない．したがって，$t - 1$ 個のサーバと結託してもメッセージを不正に復号することはできない．

一方，$d_R = \theta_t \times H(\phi, D(d_t, u_{T_t})) + \sum_{i \in \mathcal{T} \backslash \{t\}} \theta_i \times H(\phi, D(d_i, u_{T_i})) + \sum_{i \in \Omega} \theta_i \tau_i$ であるため，d_t を用いて $H(\phi, D(d_t, u_{T_t}))$ を計算しなければ d_R を導出することはできない．

すべての変換サーバが結託しても d_R を求めることはできない．$u_{T_1}, \ldots, u_{T_n}$ はランダムに生成されるため，d_R に関する情報を含まない．これは，トラブル時に問題の原因を特定する際に役立つ（d_R が漏洩した場合，P は自身の不正を否認できない）．

拡張方式は，Γ を成功するために，R が指定した変換サーバの中の $t(> n/2)$ 個のサーバによるチェックを通過することが必要になるので，t 個のサーバが正確に動作すれば安全性が保証される．したがって単一のサーバに対する信頼に依存しない点で基本方式より優れる．一方，σ のメッセージ長，および Γ に必要となる通信量は t に比例してしまう．だが，t は受信者自身が復号権限のチェックにどの程度の安全性を求めるかによって自由に選択することができるパラメータであり，高度な安全性を求める場合にはより多くのコストを必要とする点で実世界のモデルと適合してい

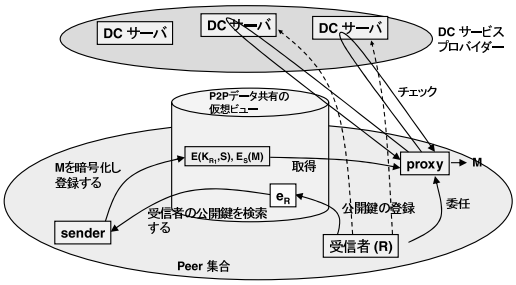

図 2 代理復号サービスプロバイダ
Fig. 2 Delegation check service provider.

る．また，t の変化は，S の処理や T の記憶領域サイズに影響を及ぼさず，R と P の間にだけ影響を及ぼす点も，スケーラビリティの観点から望ましい．

4. 応　　用

4.1 代理復号サービスプロバイダ

ネットワーク上のホスト A が，トラフィックの増大や一時的な故障などにより暗号文の復号処理を行えなくなった場合には，代行者となるホスト B に復号処理を委託したい．その一方で，ホスト A の機能が復旧した後は，ホスト B から復号権限を取り戻したいというケースが考えられる．このような代理復号をサポートするために，本論文における変換サーバの役割を担うサービスプロバイダをネットワーク上で提供する（**図 2**）．このサービスプロバイダは，(1) 復号時刻のチェック，(2) 復号処理のサポート，(3) 復号回数に応じた課金，などを行う．

(1) ホスト A は代行者となるホスト B に委任鍵を渡す．
(2) ホスト A は自分へ到着した暗号文をホスト B へフォワードするように設定する．
(3) ホスト B は到着した暗号文を復号するため，サービスプロバイダへ問い合わせる．
(4) サービスプロバイダは復号時刻をチェックし，復号処理のサポートを行う．場合によっては，復号回数に応じてホスト A へ課金を行う．

課金をともなうシステムでは，権限委譲自体には課金が発生せず，復号処理に対して課金がされるため，使用回数に応じた料金を支払えばよいという長所がある．また課金をともなわなくても，サービスプロバイダとして機能させることで，ネットワーク上での安全な復号権限の時限委譲を実現するサービスを提供できる．

4.2 P2P 技術に基づく可用性・秘匿性のあるデータ共有

P2P データ共有においては，従来型の静的に構成されたネットワークにおけるデータ共有と異なり，Peer のネットワークからの離脱や（再）参加が頻繁に行われる．一方で，データ共有サービスとして一貫したセキュリティ（たとえば，暗号化されたデータに対するアクセス）を提供するために，非接続状態にある Peer の復号鍵を必要とする場面が頻繁に起こりうる．そのため，時限的制約を含めたアクセス制御ポリシーに基づいて復号鍵を行使する権限を他の Peer に委任できれば，柔軟なセキュリティサービスの構築が可能となる．

4.3 P2P マルチキャストのためのグループ鍵生成

P2P ネットワークにおいて，送信者があるグループに対してメッセージを配信する際に，一定数以上のグループメンバの承認があった場合のみメッセージを復号可能にしたいというケースがある．文献 10) はこの目的を実現する達成するグループ鍵生成法を示している．一方，Peer の中には承認する意思があるものの，非接続状態にあるために承認プロトコルに参加できず，グループ全体としてメッセージを復号できない場合がある．文献 10) では非接続な Peer が存在する場合に備え，必要となる承認の数を送信者側でコントロールする手法を示しているが，復号権限の時限的な委譲を可能にする提案手法を適用すれば，送信者側だけでなく受信者側の Peer が非接続状態になる前に自ら対策をとることが可能になる．

4.4 暗号化データのアクセス制御——暗号文の送信者と受信者が同一の場合

提案手法において，送信者と受信者は別のエンティティである必要はない．受信者 A 自身が暗号文の送信者 S となることで，受信者 A はあらかじめ自分の秘密鍵でのみ復号できる暗号文を生成しておいて，後のその暗号文の代理復号を代行者 B に依頼することを可能にできる．この場合でも，代行者 B の権限行使に一定の条件を課すことが可能となる．たとえば，パソコンから携帯電話に対してメールなどの手段を用いて委任鍵を渡しておけば，パソコンが手元にないときでも携帯電話から変換サーバへ通信を行うことで暗号文を安全に復号することができる．この場合にも，携帯電話での代理復号が可能になるための制約条件をあらかじめ記述しておくことで，携帯を紛失した場合に，他人に暗号文を復号されてしまう危険性を回避できる．

5. ま と め

本論文では，「変換サーバ」と呼ぶ中立な第三者機関を利用することで，暗号文の受信者が，特定の期間，復号処理の代行を代行者に対して依頼できる枠組みを提案した．また，本手法を不安定なネットワークから構成される P2P データ共有への応用と，システムモデルを提案した．本手法を用いることで，暗号化データへのアクセス権限を安全な形で他の Peer へ委任することができる．要求される安全性に応じて任意のセキュリティパラメータを各 Peer が独自に設定できる点，および，すべての委任チェックサービスプロバイダが結託したとしても秘密鍵が漏れないことから，代行者の不正に対する否認不可性を実現している点で優れている．

一方，不安定なネットワーク上で，安定した P2P データ共有サービスを実現するためには，ロバストなデータ配置や複製制御が必須である．これらの機能と本手法を組み合わせることで，より効率的で安全な P2P データ共有サービスを構築することが今後の課題である．

参 考 文 献

1) Mambo, M. and Okamoto, E.: Proxy cryptosystems: Delegation of the power to decrypt ciphertexts, *IEICE Trans. Fund. Electronics Communications and Comp. Sci.*, E80-A/1, pp.54–63 (1997).
2) Blaze, M., Bleumer, G. and Strauss, M.: Divertible protocols and atomic proxy cryptography, *Proc. EUROCRYPT'98*, pp.127–144 (1998).
3) Jakobsson, M.: On quorum controlled asymmetric proxy re-encryption, *Proc. PKC'99*, pp.112–121 (1999).
4) Rivest, R.L., Shamir, A. and Wagner, D.A.: Time-lock puzzles and timed-release crypto, *MIT/LCS/TR-684* (1996).
5) Kudo, M.: Secure electronic sealed-bid auction protocol with public key cryptography, *IEICE Trans. Fundamentals*, E81-A, 1, pp.20–26 (1998).
6) Crescenzo, G.D., Ostrovsky, R. and Rajagopalan, S.: Conditional oblivious transfer and timed-release encryption, *Proc. EUROCRYPT'99*, pp.74–89 (1999).
7) Bellare, M. and Rogaway, P.: Optimal asymmetric encryption, *Proc. EUROCRYPT'94*, pp.92–111 (1994).
8) Cramer, R. and Shoup, V.: A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack, *Proc. CRYPTO'98*, pp.13–25 (1994).
9) El Gamal, T.: A public key cryptosystem and a signature scheme based on discrete logarithms, *Proc. CRYPTO'84*, pp.10–18 (1984).
10) 沼尾雅之，渡邊裕治：P2P マルチキャストのための動的グループ鍵生成法，SCIS2002 予稿集（7B-1）(2002).

(平成 14 年 11 月 29 日受付)
(平成 15 年 9 月 5 日採録)

推 薦 文

本論文は，P2P データ共有において復号鍵を一時的に他の Peer に委譲することで柔軟なセキュリティサービスを実現する手法を提案しているものであり，第 10 回マルチメディア通信と分散処理（DPS）ワークショップにおいて，同プログラム委員会の審査により高評価を得て Best Paper Award を受賞しており，これを推薦することとした．

（DPS 研究会主査 東野 輝夫）

渡邊 裕治

昭和 48 年生．平成 13 年東京大学大学院工学系研究科電子情報工学専攻博士課程修了．同年日本アイ・ビー・エム株式会社入社．東京基礎研究所副主任研究員．ネットワークセキュリティ，プライバシー保護方式に関する研究開発に従事．工学博士．

沼尾 雅之（正会員）

昭和 33 年生．昭和 58 年東京大学大学院工学系研究科電子情報工学専攻修士課程修了．同年日本アイ・ビー・エム株式会社入社．現在，同社東京基礎研究所にて ID&プライバシーグループ担当，専任研究員．ネットワークセキュリティ，プライバシー保護方式に関する研究開発に従事．人工知能学会理事．