3ZA-5

クラウドサービスの利用者の特定ができるIDベース暗号方式

疇地　悠[†]　　毛利　公美[†]　白石　善明[‡]　土井　洋[††]

岐阜大学[†]　　名古屋工業大学[‡]　情報セキュリティ大学院大学[††]

1.　はじめに

場所や端末を問わずにサービスを利用できるなどの利点から，クラウドコンピューティングの利用が企業でも広まっている．一方では，社外へ情報を出すことの不安から利用をためらう企業もある．その不安の一因は，サービス提供者を本当に信頼できるか判断できないことである．また，サービス提供者が自身の運用の品質を対外的に示すことは顧客の獲得につながるという考え方もある．そこで，安心・安全にクラウドを利用するために中立な第三者機関による監査を行うことが考えられる[1]．利用者にとっての不安である，ファイルを社外に出すことに関しては，利用者および提供者以外の監査人により運用の信頼性を保証されていれば，保証のない提供者よりも利用時の不安が緩和されると考えられる．また，責任の所在を明らかにする際にも，当事者同士だけでは意見がまとまらない場合に，第三者が提出された証拠を基にして，客観的立場から判断することで決着がつく．しかしながら，クラウドサービスでは一般的に暗号通信でアクセスするため，あるサービスに対する利用者が誰であるか，第三者により特定することは困難である．

クラウド利用に対する不安を増やさないために，監査であっても，できるだけ部外者に情報を知られないことが望ましい．そこで，クラウドサービス提供者のサービスの運用および利用者の利用の実績を第三者に示すことを目的にするならば，普段は監査人が平文を知ることなく監査ができ，問題発生時には平文とあわせることで通信内容を確認できる暗号方式が必要となる．

本稿では，サービス利用および運用時の通信内容の秘匿できること（要件 1）と，普段は監査人によってサービスの利用および運用の実績を第三者に示すことができ（要件 2），さらに，問題発生時には通信された内容も確認できる（要件 3）クラウドサービスの利用者の特定ができる ID ベース暗号方式を提案する．

2.　要件を満たすための機能

課題を解決するための，1 章で上げた要件 1～3 を満たすのに必要な機能を以下に示す．

【要件 1】サービス利用および運用時の通信の秘匿できること

①　第三者に対する通信内容の秘匿

【要件 2】普段は監査人によってサービスの利用および運用の実績を第三者に示すことができること

②　指定された監査人に対する通信内容の秘匿

③　指定された監査人によるサービス利用者の認証

④　サービス提供者による定期監査用署名の検証・改ざんの防止

⑤　サービス利用者に対する利用の非否認性

【要件 3】問題発生時には通信された内容も確認できること

⑥　秘匿された通信内容の特定の状況における通信内容の開示

なお④は提供者による署名の偽造と，提供者が検証を行い都合の良いログを選び定期監査人に渡すことを防ぐため必要となる．

3.　提案方式

提案方式は要件 1～3 を解決するため，2 章に示した機能①～⑥を満たすような，ID-based one-pass AKE と ID-SDVS を組み合わせた，クラウドサービスの利用者の特定ができる ID ベース暗号方式である．

ID-based Encryption for Cloud Service User Identification
†Haruka AZECHI and Masami MOHRI・Gifu University
‡Yoshiaki SHIRAISHI・Nagoya Institute of Technology
††Hiroshi DOI・Institute of Information Security

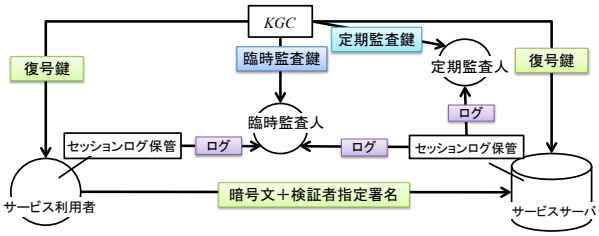

図 1　提案方式のモデル

3.1.　提案方式のモデル

提案方式のモデルを図 1 に示し，各主体の能力を以下に示す．

[サービス利用者]
信頼できる組織によって固有の ID が登録・発行されており，サービス利用のログを保存している．サービスを利用する主体であり，秘密情報を漏洩しない．

[サービス提供者]
信頼できる組織によって固有の ID が登録・発行されており，サービス提供のログを安全に保存する．サービスを提供するエンティティであり，秘密情報を漏洩しない．

[KGC]
暗号化と署名に必要な情報を公開しており，サービス利用者，提供者および定期監査人の ID 情報に対する秘密鍵・定期監査鍵の発行と，臨時監査人から渡された情報に対する臨時監査鍵を発行する主体である．プロトコルを遵守し，秘密情報の漏洩などいかなる不正も行わない TTP である．

[定期監査人]
信頼できる組織によって固有のIDが登録・発行されており，KGC から発行される自身のIDに対する定期監査鍵を用いて，サービス提供者から受け取ったログによって利用および運用の実績の監査を行う．

[臨時監査人]
問題発生時にサービス提供者／要求者からログを受け取り，KGC に問題のログに対応した臨時監査鍵を要求する．入手した臨時監査鍵で暗号文を復号することで通信内容の監査を行う主体であり，プロトコルを遵守し，秘密情報の漏洩などいかなる不正も行わない TTP である．

3.2.　準備

3.2.1.　ペアリング

G_1, G_2を位数qの群とし，任意の$P \in G_1$，$a, b \in Z_q$とした際に，写像$e: G_1 \times G_1 \rightarrow G_2$が以下の性質を満たすものである．

1. 双線形性：$e(aP, bP) = e(P, P)^{ab}$
2. 非縮退性：$e(P, P) \neq 1$
3. 計算可能性：$e(P, P)$を効率的に計算可能

3.2.2. BDH 仮定

P を G_1 の任意の生成元，$a, b, c \in Z_q^*$ のとき，$e(A, B)^{abc}$ を $< P, aP, bP, cP >$を用いて計算することが困難であるという仮定である．

3.2.3.　利用する技術

提案方式は，Goranntlaらの ID-based one-pass AKE[2]と，Leeらの ID-SDVS[3]を用いる．

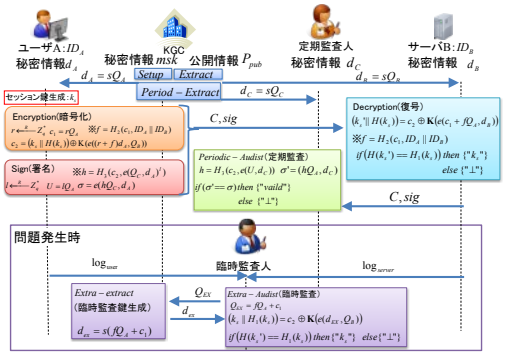

図 2 提案方式の流れ

【ID-based one-pass AKE】

ID-based one-pass AKE とは，IDベースかつ一回の通信で，送信元の認証が証明書不要で可能な，鍵確立方式である．Goranntlaらの方式では，eCK モデルをIDベースに対応するように拡張を行ったモデルにおいて，BDH 仮定に基づいてKnown Key Security, Sender forward secrecy, unknown key share, sender key compromise − impersonation, key controlが満たされることが証明されている．

【ID-SDVS】

ID-SDVS とは，ID ベースでの検証者指定署名のことである．Leeらの方式では，BDH 仮定に基づいて，Correctness, Unforgeability, Non − transferability, Strongness, Source hidingが満たされていることが証明されている．

3.3. アルゴリズム

3.1 節で示したモデルに適応する提案方式を以下に示し，提案方式の流れを図 2 に示す．提案方式は，セットアップアルゴリズムSetup，鍵生成アルゴリズムExtract，暗号化アルゴリズムEncryption，検証者指定署名を行うアルゴリズムSign，復号アルゴリズムDecryption，定期監査鍵の鍵生成アルゴリズムPeriod − Extract，定期監査アルゴリズムPeriod − Audit，臨時監査鍵の鍵生成アルゴリズムExtra − Extract，臨時監査アルゴリズムExtra − Extractの 9 つのアルゴリズムからなる．

Setup：

(1)セキュリティパラメータ1^kを入力とし，素数q，素数位数qの体Z_q^*，素数位数qの 2 つの群G_1, G_2，双線形写像$e: G_1 \times G_1 \to G_2$，ランダムな生成元$P \in G_1$を選ぶ．(2) 乱数$s \in Z_q^*$を選んで，$P_{pub} = sP$ を計算する．(3) 平文空間$\mathcal{M}_{pk} := \{0,1\}^k$，ハッシュ関数$\mathcal{H}: \{0,1\}^* \mapsto G_1, H_1: \{0,1\}^k \mapsto \{0,1\}^j, H_2: G_2 \mapsto \{0,1\}^{k+j}, H_3: G_2 \mapsto Z_q^*$，$\varkappa: G_2 \mapsto \{0,1\}^{k+j}$として，

$(params, msk) = (\langle G_1, G_2, \mathcal{M}_{pk}, \mathcal{H}, H_1, H_2, H_3, q, n, P, P_{pub}, e\rangle, s)$

を出力する．

Extract：

$(params, msk)$および$ID \in \{0,1\}^*$を入力として，(1)$Q_A = \mathcal{H}(ID_A) \in G_1$を計算し，(2)$d_A = sQ_A$を出力する．

Encryption：

セッション鍵k_sと$ID \in \{0,1\}^*$を入力として，(1)送信先と自分のIDから$Q_A = \mathcal{H}(ID_A)$, $Q_B = \mathcal{H}(ID_B)(\in G_1)$を計算し，(2)ランダムに$r \in Z_q^*$を選び，(3)$c_1 = rQ_A, f = H_2(c_1, ID_A||ID_B), c_2 = (ks||H_1(ks)) \oplus \varkappa(e((r+f)d_A, Q_B))$を計算し，$C = (c_1, c_2)$を出力する．

Sign：

暗号文$\mathbf{c_2}$と自身のID_A，秘密鍵d_A，指定された検証者のIDであるID_Cを入力として，(1) $Q_C = \mathcal{H}(ID_C) \in G_1$を計算し，(2)ランダムに$l \in Z_q^*$を選んで，(3) $U = lQ_A, h = H_3(c_2, e(Q_C, d_A)^l)$，$\sigma = e(hQ_C, d_A)$を計算し，$sig = (\sigma, U)$を出力する．

Decryption：

暗号文C, ID_A, ID_B，秘密鍵d_Bを入力とし，(1) $(ks'||H_1(ks)') = c_2 \oplus \varkappa(e(c_1 + fQ_A, d_B))$を計算して，(2) $H_1(ks)' = H_1(ks')$が成り立つか確認し，成り立たない場合は⊥を，成り立つ場合はks'を出力する．

Periodic − Extract：

$(params, msk)$，定期監査人のID $\in \{0,1\}^*$を入力として(1) $Q_C = \mathcal{H}(ID_C) \in G_1$を計算し，(2)$d_C = sQ_C$を出力する．

Periodic − Audit：

署名sig,暗号文C,指定検証者の秘密鍵d_Cと，ID_A, ID_Cを入力とし，(1)$h' = H_3(c_2, e(U, d_C))$を計算し，(2)$\sigma' = e(h'Q_A, d_C)$を計算して，$\sigma' = \sigma$となるか確認する．成り立たない場合はrejectを出力し，成り立つ場合はValidを出力する．

Extra − Extract：

$(params, msk)$，臨時監査人から渡された入力Q_{EX}に対して(1)$d_{EX} = sQ_{EX} = s(fQ_A + c_1)$を計算して，出力する．

Extra − Audit

C, ID_A, ID_B，を入力とし，(1)**Extra − Extract**に$Q_{EX} = fQ_A + c_1$を送信し，d_{EX}を得る．(2) $(ks||H_1(ks)) = c_2 \oplus \varkappa(e(d_{EX}, Q_B))$を計算し，(3) $H_1(ks)' = H_1(ks')$が成り立つか確認し，成り立たない場合は⊥を，成り立つ場合はks'を出力する．

4. 安全性評価

提案方式の暗号化部分，検証者指定署名部分に対してそれぞれ攻撃を行うことを考える．

【暗号化部分】

暗号化部分の識別不可能性を破るアルゴリズムが存在すると，それを用いて[2]の方式を破るアルゴリズムを構成できるため，提案方式は[2]の安全性に基づき安全である．

【検証者指定署名部分】

検証者指定署名部分に対して，Unforgeabilityを破るアルゴリズムが存在すると，そのアルゴリズムを用いて[3]のUnforgeabilityを破るアルゴリズムが構成可能となるため，提案方式は[3]に基づきUnforgeabilityを満たす．また，提案方式のCorrectness, Non − transferability, Strongness, Source hidingについても同様に[3]の方式に基づき満たす．

5. まとめ

本稿では，クラウドサービス利用への不安を軽減し，安心・安全にクラウドを利用するために必要な，第三者がサービスの品質や安全性をチェックし保証する仕組みとして，クラウドサービスの利用者／提供者以外の第三者（監査人／臨時監査人）による，クラウドサービスの利用／運用の監査を可能にするための，クラウドサービスの利用者が特定できる ID ベース暗号方式を提案した．

提案方式では，2 章で示した要件を満たすために必要な機能のうち，①と②を ID-based one-pass AKE を用いた暗号化により実現している．実際，通信内容の秘匿は，提案方式の暗号化の安全性に基づき満たされている．また，③，④，⑤については，暗号文に対する ID-SDVS によって実現している．このとき，指定された監査人による署名者の認証と，指定された監査人以外による署名の検証・改ざんの防止，署名者の非否認性は，提案方式の署名部分に基づき満たされている．また，⑥については ID ベース暗号全体の性質である，KGC によるキーエスクロー（鍵供託）の機能により実現している．

以上より提案方式は，利用している鍵確立／署名の安全性に基づいて安全であり，要件 1〜3 を満たしていることを確認した．

参考文献

[1] 経済産業省：クラウドサービス利用のための情報セキュリティマネジメントガイドラインについて，クラウドサービス利用のための情報セキュリティマネジメントガイドラインの公表〜クラウドサービスの安全・安心な利用に向けて〜，入手先〈http://www.meti.go.jp/press/2011/04/20110401001/20110401001-2.pdf〉，（参照 2012-01-13）

[2] Gorantla, M.C., Boyd, C., and Nieto, J.M.G.: ID-based One-pass Authenticated Key Establishment, *AISC'08*, Vol. 81, pp.39-46, (2008)

[3] Lee, J., Chang, J.H., and Lee, D.H.： Forgery attacks on Kang et al.'s identity-based strong designated verifier signature scheme and its improvement with security proof, Computers and Electrical Engineering, vol.36, no.5, pp.948-954, DOI:10.1016/j.compeleceng.2010.02.001, (2010)