情報処理学会論文誌　Vol. 51　No. 9　1692–1701 (Sep. 2010)

IDベース暗号の信頼構築フレームワーク

金岡　晃[†1]　島岡政基[†2]　岡本栄司[†1]

ID ベース暗号は近年の研究成果により実用化に向けた段階にきているが，まだ多くの課題をかかえている．その中の 1 つに信頼の確立がある．ID ベース暗号の Private 鍵を生成する鍵生成局（Key Generation Center）が複数存在する環境において，利用者が鍵生成局をいかに信頼するかという問題は，これまでの研究では解決されていなかった．本論文では，ID ベース暗号の信頼構築のためのフレームワークとして，信頼のモデルと，信頼実現のためのポリシと業務実施規程を提案した．提案するフレームワークの実現により，ID ベース暗号における信頼構造を確立することが可能となった．

Trust Framework for Identity-based Cryptography

Akira Kanaoka,[†1] Masaki Shimaoka[†2]
and Eiji Okamoto[†1]

Identity-based cryptography is approaching practical use by recent results of research. However, there are still many problems for practical use. One of the biggest problems is establishing trust. In the case of multiple Key Generation Centers, the problem how users trust Key Generation Centers, has not been resolved. In this paper, we propose trust framework for identity-based cryptography, including trust model, issuing/generating policy and practical statements. Proposed framework can establish trust in identity-based cryptography.

†1 筑波大学
University of Tsukuba
†2 セコム株式会社
SECOM CO., LTD.

1. はじめに

公開鍵暗号は，現在では公開鍵基盤（Public Key Infrastructure，以後 PKI）などの応用もあり基礎研究や応用研究の段階を過ぎ，実用化され社会基盤として定着しつつある．実用化された公開鍵暗号には RSA 暗号や楕円曲線暗号があるが，それらのいずれも公開鍵のデータとして任意のデータを設定することはできない．1984 年に Shamir が提案した ID ベース暗号は，これまでの公開鍵暗号と異なり，任意のデータを公開鍵として設定可能な暗号方式であった[1)]．任意データを公開鍵として設定可能なため，識別情報である ID 情報（Identifier）そのものを公開鍵として暗号化や署名が可能になることから名付けられたものである．

ID ベース暗号は長らく現実的な実現方式が提案されてこなかったが，2000 年になり，Sakai らにより双線形写像を用いた方式が提案されると[2)]，Boneh らによる方式も同様に双曲線写像を用いて提案されるなど[3),4)]，現実的な実現方式が複数提案され，近年ではそれらの手法の標準化が進むなど[5)]，ID ベース暗号は実用化に向けた段階にあるといえる．

しかし，ID ベース暗号の実用化にはまだ課題が多く残る．その 1 つは，ID 情報から Private 鍵を生成する鍵生成局（Key Generation Center，以下 KGC）の信頼の確立である．ID ベース暗号による暗号化は，相手の ID 情報と相手の Private 鍵を生成した KGC の公開パラメータを使った演算で実現される．そこには，「相手の Private 鍵を生成した KGC が，暗号化を行う利用者にとっていかに信頼できるか」といった信頼の確立が必要とされる．信頼の確立は，信頼される側が提供した情報により，信頼する側が信頼に値するかを判断することで行われる．そして，信頼を判断するための情報種類や情報提供の形を決めたフレームワークが提供されることで利害関係者間の信頼確立が促進される．しかし既存の ID ベース暗号のプロトコルや，その応用手法ではその信頼の確立を実現できていない．

本論文では，ID ベース暗号に必要とされる信頼を確立するための信頼構築フレームワークを提案する．

ID ベース暗号の利用において，複数の KGC の存在の考慮は運用面と暗号プロトコル面の双方で必要となる．さらに用途別 KGC のような複数 KGC がある環境であっても，ID 情報が共通の発行組織から発行されているケースや，複数の ID 発行組織から 1 つの KGC が鍵発行を請け負うケースの考慮も必要となる．それゆえ従来は同一機関で扱われていた「ID 情報の発行」と「Private 鍵の生成」を機能分割することが望ましい．そこで，それぞれ独立した機関としてあらたに ID Issuer と KGC を提案し，ID Issuer と KGC が複数存

在するユースケースを分類する．提案するフレームワークは，信頼モデルと，ポリシと業務実施規程により構成される．信頼モデルでは既存の PC 環境などに容易に実現可能なトラストリストモデルや，外部の信頼構造を用いたリポジトリモデル，また Private 鍵生成を ID 連携における 1 つのサービス形態として考慮した ID 連携技術の応用モデルの 3 つを提案する．ポリシと業務実施規程では，ID Issuer と KGC のそれぞれにポリシと業務実施規程を設ける．

本論文で提案する信頼構築フレームワークを利用することで ID ベース暗号の実用化の課題を解決することが可能である．

本論文の構成は以下のとおりである．2 章で関連研究について解説を行う．3 章では複数 KGC の必要性について述べ KGC 機能の分割を提案する．これにより信頼構造に必要な事項を明確にする．信頼構築フレームワークは 4 章で提案する．最後に 5 章でまとめる．

2. 関 連 研 究

2.1 ID ベース暗号

ID ベース暗号は 1984 年に Shamir によってそのコンセプトが提案された[1]．しかし現実的な実現方法は提案されておらず，長くコンセプトのみとなっていたが，2000 年になり Sakai らにより双線形写像 Pairing を用いた方式[2] が提案され，また Boneh らによる方式[3),4)] が提案されるなど近年研究が活発になっている．

ID ベース暗号は既存の公開鍵暗号と異なり，Identity の識別情報（Identifier，以後 ID 情報）を公開鍵情報として用いることができるため，公開鍵（証明書）の管理が簡単になる利点があるといわれている．一方でその利点は，ID ベース暗号が証明書の不要な方式であり PKI の代替技術あるいは後継技術としてしばしば誤解される．

公開鍵証明書は，公開鍵データと発行対象の Identity の結びつきを保証している．一方で，ID ベース暗号の Private 鍵は発行対象の ID 情報から生成され ID 情報が公開鍵になることから，鍵発行の段階で鍵データと Identity の結びつきが保証されていると考えることができ，公開鍵と発行対象の Identity を保証する必要はない．このために公開鍵証明書が不要という論調が形成されてきたと考えられる．しかし公開鍵証明書を基にする PKI は，単に公開鍵データと Identity を結びつけるものだけではなく，信頼の伝搬に必要な情報や制約などを証明書に記述し，信頼の基盤として使われることを想定したフレームワークであり ID ベース暗号はその基盤自体を不要にすることを意味するものではない．

ID ベース暗号では，Identity を持つ利用者（End Entity，以下 EE）に対して Private 鍵を生成する主体を KGC（Key Generation Center）と呼ぶが，複数の KGC が存在する環境（**図 1**）において，他方の KGC より Private 鍵生成を受けている利用者に対して ID ベース暗号による暗号文を届けるには，他方の KGC が公開しているパラメータを信頼できる方法で取得する必要がある．つまり，暗号文作成者と他方の KGC 間の信頼関係が必要とされる．

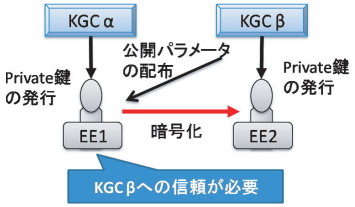

図 1　複数 KGC 環境での信頼構造の必要性
Fig. 1　Requirement for trust architecture in multiple KGC environment.

こうした複数 KGC 間の信頼関係においては，単に KGC 間の信頼関係としてとらえるのではなく，具体的なステークホルダ間である EE と KGC 間の信頼関係に着目して整理する必要がある[9]．

複数 KGC 間で ID ベース暗号を実現するには 2 つのアプローチが考えられる．1 つは信頼構造を組み込んだ新たな ID ベース暗号方式を確立するアプローチと，もう 1 つは既存の ID ベース暗号方式を適用できるような，信頼関係を持たない EE に対してパラメータを安全に配布するプロトコルなど，信頼構造のフレームワークを提案し実現するアプローチである．

前者のアプローチとしては Chen らが ID ベース暗号上での複数の信頼できる機関（TA: Trust Authority）がある場合の信頼構築方法として，従来 PKI の応用として階層構造を持つ TA 群を考慮し，上位 TA が下位 TA に対して鍵生成を行うモデルを提案している[10]．また後者のアプローチとしては Smetters らにより，電子メールと IPsec に限定したモデルとして，DNSSEC を利用し DNS のレコードに署名済みの KGC パラメータを加えることで KGC パラメータの受け渡しを実現する方法が提案されている[11]．DNSSEC は，DNS のドメイン登録情報に電子署名を付与することでその登録情報の正当性と改ざんされていないことを保証する方式である．電子署名は公開鍵暗号を利用して行われるが，PKI を用いたものではなく，署名に利用した DNS サーバの鍵は上位の DNS サーバにより保証される．つまり，信頼の基点は DNS のトップレベルドメインにおかれることとなる．

また Price らは既存の PKI ドメインと ID ベース暗号のドメイン（KGC が鍵生成を行う範囲）が相互にサービス利用をする場合のユースケースを検討し，ユースケースごとにその対応を提案した[12]．そこでは，PKI における証明書ポリシ（Certificate Policy，CP）文書や認証業務実施規程（Certification Practice Statement，CPS）と同様のものを KGC が持つことの必要性が触れられている．しかし，具体的な規程の内容については検討されていない．

2.2　ID 連携技術

近年，Web 上でさまざまなサービスが普及拡大しているが，管理コストや法の規制，あるいはセキュリティ上の問題など，サービスで利用される ID 情報を管理することの重要性が高まっている．その中で，ID 情報を各利用組織で連携させることにより管理を実現する ID 連携技術が存在する．OASIS（Organization for the Advancement of Structured Information Standards）で策定された SAML（Security Assertion Markup Language）は，ID 情報を各 Web サイトで連携させることによりシングルサインオンを実現可能にする ID 連携の代表的な技術仕様である[13]．SAML はセキュリティアサーションの表現形式とその交換のプロトコルを定めており，代表的な実装の 1 つとして，Internet2 による Shibboleth がある[14]．

また Liberty Alliance が策定する ID-WSF（Identity Web Services Framework）は，Web サービス上で ID 連携を実現するフレームワークであり，ID-WSF 2.0 では SAML 2.0 に対応している[15]．

SAML と ID-WSF に共通する関係者として，ID 情報を提供する IdP（Identity Provider），サービスを提供する SP（Service Provider），そして利用者の 3 者が存在する．

IdP より ID 情報を発行され利用者は，IdP により認証された情報を SP に提示することで，SP のサービスを受けることが可能である．他 SP のサービスを受けるときも同様であり，利用者は 1 度 IdP にログインを行うと複数 SP からサービス享受可能になる（**図 2**）．

SAML では，複数の IdP が存在する場合，サービス要求を行っている利用者がどの IdP から ID 情報発行を受けているかを発見する IdP Discovery という仕組みがある．ID-WSF でも類似の Discovery Service があるが，IdP の発見だけではなく，必要な属性情報の所在を提供できる．

ID 連携では IdP が必ずしも同じ水準で ID 情報を発行するわけではないことを前提としている．このため，ID 情報発行の水準を SP が把握するための仕組みとして保証レベルという考え方がある．Liberty Alliance が策定した Identity Assurance Framework（IAF）には 4 段階のレベルが規程されている[18]．

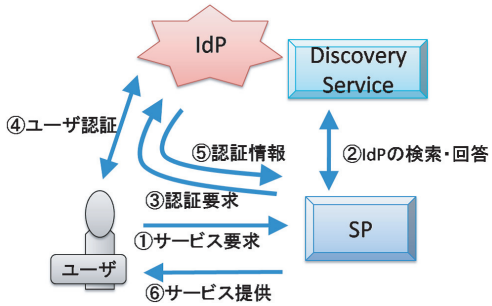

図 2　ID 連携におけるサービス享受
Fig. 2　Services on identity federation.

保証レベルを ID 連携のフレームワーク全体として明確に定義しておくことで，IdP と SP が別々の運用主体でも安心して連携できる仕組みを実現したのが ID 連携の特徴でもある．

2.3　PKI における CP/CPS の事例分析

PKI では，認証局（Certification Authority，以下 CA）を運用するにあたり，証明書ポリシ（Certificate Policy，以下 CP）と認証業務実施規程（Certification Practice Statement，以下 CPS）が策定されている．CP は「証明書発行にあたって関係者が何をしなければならないか」という方針を規定し，CPS は「CP への適合をどのように実現しているか」という具体的な実施内容を規定するものである．

CP/CPS は実際には単一の文書で規定されることが多いが，CP と CPS を独立した文書として規定したり，たとえば非自然人である Web サーバを対象としたサーバ証明書と自然人を対象としたクライアント証明書では CP を使い分けたいなどの理由で，1 つの CA が複数の異なる CP を規定するケースも存在する．こうした場合 CPS は，CP によらない CA に一意な業務実施内容を規定するものとして位置づけられることになる．また CP/CPS は，組織間での信頼確立や，利用者が CA を信頼する場合に参照される重要な情報の 1 つであり，それぞれの CA が独自に CP と CPS を策定していたのでは混乱を生じるため，CP/CPS の文書構造が RFC 3647 として標準化されている[16]．

ID ベース暗号における複数の II と KGC の混在環境でも，II や KGC の信頼性を評価するうえで網羅性が確保されたポリシや業務実施規程の文書構造が整備されるべきである．本論文ではポリシと業務実施規程を独立した形で文書構造を規定するため，同様に CP と CPS を独立した文書として規定している PKI サービスの事例を調査した．調査の結果を

表 1　CP/CPS の文書構造と事例分析
Table 1　Case study for CP/CPS document structure.

	CP 1 19),20)	CP 2 21)	CP 3 22)	CPS 4 23)	CPS 5 24)
1. はじめに	○	○	○	○	○
2. 公開とリポジトリの責任		○	○	○	○
3. 識別と認証	○	○	○		
4. 証明書のライフサイクル運用要件	○	○	○		
5. 設備，運営および運用統制		△	△	○	○
6. 技術面のセキュリティ統制		△	△	○	△
7. 証明書などのプロファイル	○	○	○		
8. 準拠性監査		○	○	○	○
9. 他の案件と法的事項	○	○	○	○	△

表 1 に示す．○は RFC 3647 における当該章の全項目を規定していることを，△は同じく一部の項目のみを規定していることを表す．

RFC 3647 が規定する内容と表 1 の結果をふまえて，まずポリシと業務実施規程に独立させる場合の文書構造について考察する．CP/CPS 2 章は，認証局が公開する証明書失効リストなどの情報と，それらの情報を公開するリポジトリの責任について記述するものであることから，ポリシによらない内容として業務実施規程には不可欠である．CP/CPS 3 章は，証明書発行における本人確認の方法などについて記述するものであることから，ポリシごとに異なる可能性がある．CP/CPS 4 章は，証明書の発行・更新・失効などに関する申請手続きや受領手続きについて記述するものであることから，やはりポリシごとに異なる可能性がある．CP/CPS 5 章は，認証局の設備などに関する物理的な運用・管理や要員配備について記述するものであることから，業務実施規程に不可欠である一方で，要員配備など場合によっては一部ポリシに関連する内容も含まれる．CP/CPS 6 章は，鍵ペアや認証局システムの技術的な管理について記述するものであることから，業務実施規程に不可欠である一方，EE の鍵ペアに言及する場合はポリシにも関連する可能性がある．CP/CPS 7 章は，証明書などのデータフォーマットについて記述するものであることから，ポリシごとに異なる可能性がある一方，CA 証明書などポリシによらない内容は業務実施規程に記述される場合もある．CP/CPS 8 章は，準拠すべき基準や，その基準に対する評価方針について記述するものであることから，業務実施規程に不可欠であり，また必要に応じてポリシにおいても規定される場合がある．CP/CPS 9 章はその他の条項として必要に応じてポリシおよび業務実施規程で規定される．

3. KGC 機能の分割

本章では，まず 3.1 節において現実的な利用を考慮したときの複数 KGC の必要性について述べる．さらに複数の KGC がある環境においては，ID 情報が共通の発行組織から発行されているケースや，複数の ID 発行組織から鍵発行を請け負う共通 KGC が存在するケースが考えられる．そこで，3.2 節では従来は同一機関で扱われていた「ID 情報の発行」と「Private 鍵の生成」を機能分割することを提案し，そのユースケースの分類を行う．それにより信頼構築に必要な事項を明確にする．

3.1　複数 KGC の必要性

ID ベース暗号を利用することを考えたときに，Private 鍵を生成する組織である KGC は，利用者あるいはサービスに求められるレベルに応じて，適切な強度を持つ Private 鍵を生成すべきである．これは鍵強度として必要かつ十分な鍵サイズの Private 鍵を生成することが，暗号化・復号化時の計算量や Private 鍵や暗号文・署名文などを保管するデータサイズが必要以上に増えることをおさえることが可能だからである．

また，実際の KGC 運用を考えた場合，暗号文を交換する可能性があるすべての利用者を網羅する KGC というのは，現実的ではないということが，先達である PKI の展開状況からも学ぶことができる．つまり実用化を視野に入れた場合には，複数の KGC が存在することを前提とする必要がある．

複数 KGC の前提は運用面で自明だが，ID ベース暗号の方式によっては一部の運用要件を満たすうえで，複数 KGC を用意する必要が生じる場合がありうる．

ここでは代表的な ID ベース暗号方式として境らによる方式（以後，境–笠原方式），Boneh, Franklin による方式（以後，BF 方式），Boneh，Boyen による方式（BB1 方式）に着目して議論を進める．また，それぞれの暗号プロトコルについては，現在 ID ベース暗号の標準化を進めている IEEE P1363[5] に提出されている各方式の仕様[6)–8)] を参照とする．

上記 3 つの ID ベース暗号方式は，*Setup*，*Key Extract*，*Encrypt*，*Decrypt* の 4 つアルゴリズムに分けられる．ここでは ID 情報から Private 鍵を算出するそれぞれの *Key Extract* を以下に示す．なお，式中の ID は利用者の ID 情報を示し，利用者 ID の Private 鍵は D_{ID} で表すこととする．まず境–笠原方式は以下の式で Private 鍵が算出される．

$$D_{\mathrm{ID}} = g_2^{1/(s+H_1(\mathrm{ID}))} \tag{1}$$

ここで g_2 は素数 p のオーダを持つ乗法巡回群 G_2 の生成元であり，$s \in Z_p$ は KGC のマス

タシークレット，H_1 は任意のビット列入力からを Z_p 上の元に出力するハッシュ関数である．次に BF 方式は以下の式で Private 鍵が算出される．

$$D_{\mathrm{ID}} = H(\mathrm{ID})^s \tag{2}$$

ここで $s \in Z_p$ は KGC のマスタシークレット，H は任意のビット列入力から素数 p のオーダを持つ乗法巡回群 G 上の元に出力するハッシュ関数である．

最後に BB1 方式の Private 鍵算出を示す．

$$D_{\mathrm{ID}} = \left(\hat{g}^{\alpha\beta+(\alpha H(\mathrm{ID})+\gamma)}, \hat{g}^r\right) \tag{3}$$

ここで $\hat{g}$ は素数 p のオーダを持つ乗法巡回群 $\hat{G}$ の生成元であり，α，β，$\gamma \in Z_p$ とともに KGC のマスタシークレット，H は任意のビット列入力から素数 p のオーダを持つ乗法巡回群 G 上の元に出力するハッシュ関数である．また $r \in Z_p$ は利用者ごとの生成される乱数である．なお，$\hat{g}$ はマスタシークレットに分類されているが必ずしも秘匿しなければならないものではない．しかし，公開を必須とするものでもないためマスタシークレットに分類されている[8]．

式 (1)，(2)，(3) より，いずれの Private 鍵も利用者の ID 情報とマスタシークレットをもとに，乗法巡回群上のべき乗剰余計算により求められることが分かる．そのため，乗法巡回群や曲線，素数 p を変えずに異なる Private 鍵のサイズを実現するには，べき乗剰余計算の結果の値を任意に変更可能でなければならない．しかし，計算は容易ではないことに加え，マスタシークレットの変更や利用者の ID 情報に制限を加える必要性が高いことを考慮すると，同一の曲線や乗法巡回群，マスタシークレットを用いた KGC が，異なるサイズの Private 鍵を生成することは現実的ではなく，複数の KGC を用意して対応することとなる．

このように運用的にも数学的にも，ID ベース暗号のアーキテクチャは複数 KGC を前提として設計されることが望ましい．

3.2　KGC 機能の分割とユースケースの分類

複数の KGC を考慮する場合，Private 鍵生成のポリシは異なるが，ID 情報自体の発行に関しては同一のポリシを用いる場合が考えられる．たとえば，企業内利用としてセキュリティ強度の異なる 2 つの KGC が Private 鍵発行を行っているが，ID 情報は社員 ID として共通の発行がされているケースがそれにあたる．一方で，Private 鍵生成のポリシは同一だが，ID 情報の発行は異なるポリシを用いる場合も考えられる．たとえば，ID 発行はそれぞれの企業で発行しているが，複数企業の Private 鍵発行を共通 KGC が行うケースがそれにあたる．

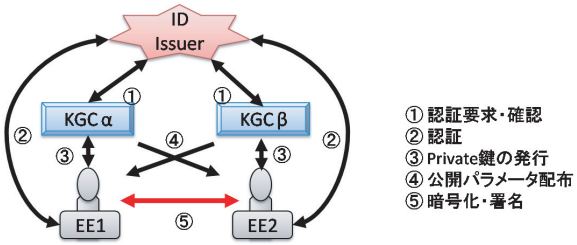

図 3　ケース A：単一 II，複数 KGC
Fig. 3　Case A: single II, multiple KGCs.

これまでの ID ベース暗号では KGC の機能は ID 情報の発行管理業務と Private 鍵生成管理業務を兼ねていたが，KGC の複数利用が現実的になる場合，この 2 つの業務は明確に分けられるほうが信頼を確立するうえで望ましい．

そこで，本論文では，上記 2 つの業務をそれぞれ 2 つの機関に分けて考えることとする．

- Identifier Issuer（II）：ID 情報の発行管理を行う機関
- Key Generation Center（KGC）：Private 鍵の生成管理を行う機関

一番単純な構造では，1 つの II と KGC という構成であるが，II が複数，あるいは KGC が複数，という構造も考えられる．そこで，それらをユースケースとして分類する．またそれらの具体例を示す．

3.2.1　ケース A：単一 II，複数 KGC

ケース A は単一の II のもと，複数の KGC が存在するものである（**図 3**）．

単一組織での ID ベース暗号利用だが，利用用途に応じて Private 鍵のサイズを変えるために KGC を複数運用する場合がケース A にあたる．

3.2.2　ケース B：複数 II，単一 KGC

ケース B は，複数の II があるが，KGC は単一であるケースである（**図 4**）．

ID 情報の発行はそれぞれの機関で行うが，Private 鍵生成による ID ベース暗号利用は 1 つの KGC が請け負うもので，すでに ID 情報を発行してサービスをしているさまざまな事業者に対して新たなサービスとして ID ベース暗号の鍵生成サービスを KGC が実施する形態はケース B にあたる．

3.2.3　ケース C：複数 II，複数 KGC

ケース C は，複数の II と複数の KGC が存在するケースであり，複数の II から ID 発行を受けた EE が，それぞれ対応する KGC から鍵生成をしてもらうものである（**図 5**）．

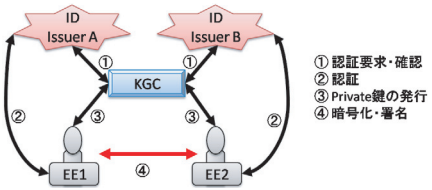

図 4　ケース B：複数 II，単一 KGC
Fig. 4　Case B: multiple IIs, single KGC.

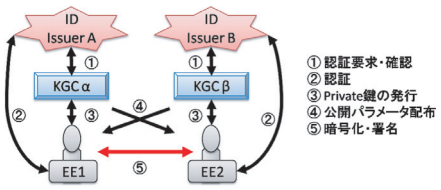

図 5　ケース C：複数 II，複数 KGC
Fig. 5　Case C: multiple IIs, multiple KGCs.

各組織がそれぞれ独自に ID 情報と Private 鍵を生成し，相互に利用するという形態がケース C にあたる．

4. 信頼構築フレームワーク

各ユースケースで，それぞれの EE が ID 情報発行と Private 鍵生成を受け，ID ベース暗号を利用するには，EE は II や KGC を信頼し，信頼した KGC から公開のパラメータを安全に受け取らなければならない．

本章ではそういった信頼を構築するためのフレームワークとして，4.1 節では EE が KGC から公開パラメータを安全に受け取るための信頼モデルを提案し，4.2 節では KGC や II を信頼するためのポリシと業務実施規定を提案する．

4.1 信頼モデル

ケース A（図 3），C（図 5）は「別の KGC から鍵生成を受けている利用者への暗号化・署名」を行うものであり，EE1 が EE2 に対して暗号化を行う場合には，EE1 が KGCβ の持つ公開パラメータ（乗法巡回群の情報や，乗法巡回群の生成元など）を安全に受け取ることが必要となる．

本論文ではその解決法を 3 つ提案する．

4.1.1 トラストリスト

1 つは各 EE が信頼済みの KGC 情報をリスト化して保持するトラストリストの利用である．それぞれの EE は，信頼できる KGC のパラメータのリストを持っており，相手の KGC を知り，その KGC パラメータを用いることで暗号化や署名を行うものである．これは PKI 環境において，複数の信頼済み CA のリストを保持しておく方式と同様のものであり，現在のブラウザや Windows OS などの PKI 環境で広く使われている方式であることから，既存環境との親和性の高さがある，と考えられる．

4.1.2 外部信頼構造を利用したリポジトリ

各 EE が信頼する KCG パラメータのリストを持つのではなく，各 EE が参照可能なリポジトリに，信頼可能な KGC パラメータのリストを置き，利用者に配布することも可能である．

その際，EE がリポジトリを信頼することが必要となるが，外部の信頼構造を利用することも可能である．たとえば 2.1 節で述べた Smetters らの方式は，DNSSEC という外部の信頼構造を利用したリポジトリとなっている．

現実的な ID ベース暗号の利用を考えた場合，すでに広く普及している PKI の信頼構造を EE が利用可能である環境も十分考えられる．そこで本項では，外部信頼構造を利用したリポジトリの実現方法として SSL/TLS を用いる手法を示す．

リポジトリの実現方法としては要件が単純であることからさまざまな方法が考えうるが，既存の技術との親和性や普及コストの観点を考慮すると Smetters らの手法や，以下の手法を利用すること合理的であると考える．

4.1.2.1 SSL/TLS を用いた Web の利用

SSL（Secure Socket Layer）や TLS（Transport Layer Security）と HTTP を利用した Web アクセスは，現在ではほとんどすべての端末で利用可能であり，SSL/TLS に利用される証明書を発行する CA はブラウザや Windows OS にあらかじめ格納されており利用は容易である．

リポジトリの提供者が，信頼できる KGC の名称とパラメータなどのリストを Web サーバ上に公開することで，利用者は安全に情報を得ることができる．これは SSL/TLS を用いることによって，信頼の基点を既存の PKI においた安全な配布を実現するものである．

ただし，この方法だけでは配布経路上の安全性確保にとどまっており，公開されている情報の信頼性については，4.2.4 項で示すように別の方法で確保する必要がある．

4.1.3 ID 連携技術の応用

ID 連携の関係者を，本論文で検討している ID ベース暗号の関係者と比較したとき，その構成はほぼ同様のものになっていることが分かる（**図 6**）．

そこで，II を IdP（Identity Provider），KGC を「EE に対して Private 鍵を生成する SP（Service Provider）」と考えることとする．

提案方式では IdP としての II，SP としての KGC，そして EE の 3 者のほかに，2 つの新たなサービスを用意する．まず 1 つは要求された ID 情報がどの KGC より Private 鍵生成を受けているかを発見・回答する Discovery Service である．ある ID 情報がどの KGC か

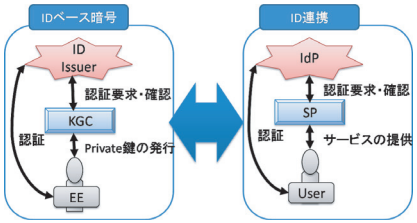

図 6　ID ベース暗号と ID 連携の関係者
Fig. 6　Identity-based encryption players and identity federation players.

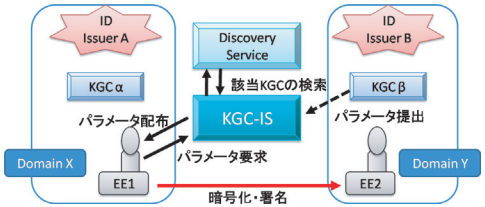

図 7　ID 連携技術の応用による提案モデル
Fig. 7　Proposed model using identity federation technique.

ら Private 鍵生成を受けたかの情報は，ID 情報に付随する属性情報と考えることが可能であることから，属性情報の Discovery Service を提供する ID-WSF（Identity Web Service Framework）の技術や仕様で実現が可能である．

もう 1 つの新たなサービスは，要求された ID 情報の Private 鍵生成を行っている KGC パラメータの情報を回答する KGC Information Service（KGC-IS）である．

KGC-IS は要求された ID 情報をもとに，Discovery Service より KGC 情報を得て，その KGC 情報に基づいて EE にパラメータを返す（**図 7**）．パラメータは KGC-IS が保持することも可能であり，要求ごとに KGC より提供を受けてもよい．

図 7 では各サービスや SP は分かれて表現されているが，Discovery Service と KGC-IS の双方のサービスを 1 台のサーバで実現することも可能であり，さらには KGC と合わせた 3 つを 1 台のサーバで実現することも可能である．

4.2　ポリシと業務実施規程

ID ベース暗号が，複数の II や複数の KGC が存在する環境で利用されるためには，II と KGC はお互いの組織や EE から信頼をされないとならない．本節では，KGC が II をいかに信頼するか，EE が KGC や II をいかに信頼するかという信頼の構築に焦点を当てる．

そこで本論文では，II と KGC のそれぞれのポリシと業務実施規程の構成内容を提案する．なお，CA が CA 鍵という秘密情報の運用管理基準として CPS を策定しているのに対して，II の場合には運用管理の対象となるべき秘密情報が必ずしも存在しないため，CPS に相当する業務実施規程については本論文では議論しない．

4.2.1　ID ベース暗号への CP/CPS の適用

2.3 節の考察に基づき，また ID ベース暗号固有の事情に配慮しながら，II と KGC のポリシと業務実施規程の文書構造について検討を行った結果を**表 2** に示す．●は RFC 3647 における当該章の全項目について必須で，▲は同じく一部の項目に関して必須で，△は同じく一部の項目に関して任意で，それぞれ規定するものとする．具体的な検討結果について，次項以降で述べていく．

表 2　II および KGC におけるポリシと業務実施規定の文書構造
Table 2　Contents of policy and practical statement for II and KGC.

	IP	KGP	KGPS
1. はじめに	●	●	●
2. 公開とリポジトリの責任		△	●
3. 識別と認証	●	●	
4. 証明書のライフサイクル運用要件	●	●	
5. 設備，運営および運用統制	▲	△	●
6. 技術面のセキュリティ統制		▲	▲
7. 証明書などのプロファイル	●	●	
8. 準拠性監査	△	△	△
9. 他の案件と法的事項	△	△	△

なお 8 章の「準拠性監査」と 9 章の「他の案件と法的事項」については，現時点では ID ベース暗号に関連する準拠すべき基準や法適用件が存在していないため，策定については任意での規定とした．

4.2.2　ID 情報ポリシ

ID 情報ポリシ（Identifier Policy，以下 IP）は，II が発行する ID 情報についての運用管理のルールを定めたものである．PKI において，EE が CP の内容を理解・評価することによって CA や RA に対する信頼を構築するように，ID ベース暗号においても，KGC や EE が ID 情報ポリシの内容を理解・評価することによって，II に対する信頼を構築できると考えられる．

表 2 に示す IP の文書構造のうち，必須（●および▲）とする章節について特に留意すべき点を考察した．

まず IP 2 章は，II が特に公開すべき情報を持つわけではなく，また ID に関連した公開リポジトリを運用する必要はないと考えられることから，記述は不要とした．

IP 3 章では，本題である申請者の本人確認に加えて，どのような ID 情報が割り当てられるのかといった ID 情報の命名ルールが明確に指定されることが重要である．これはたとえば，II から一方的に割り当てられるのか，あるいは重複しない範囲で希望する文字列が利用できるのか，といった内容が示されるべきである．また，ID 情報は同一 Identity に対して 1 度だけ発行される場合もあれば，更新や失効などを考慮し複数の ID 情報が提供され

る場合もあることから，IP 4 章ではこうした ID 情報の一意性についても明示されるべきである．IP 5 章は，主に業務実施規程で記述される内容であるが，II に関しては業務実施規程を規定しないことから，IP の中で要員統制や運用手続きについて規定しておくべきである．ただし，II の場合は CA と異なり運用管理の対象となる秘密情報が存在しないため，必ずしもすべての項目について規定する必要はないと考えられる．IP 7 章で示されるべき ID 情報の表現方法やデータフォーマットは，本論文の対象外とするが，IP を策定する場合にはたとえば使用可能な文字集合などが明確に規定されるべきである．

なお，ID 情報の発行や管理については，PKI を一部包含する形で，より広い電子認証の分野ですでに扱われており，米国の標準技術局（NIST）が策定した電子認証ガイドライン SP 800-63[17] や，Liberty Alliance が策定した Identity Assurance Framework（IAF）[18] といった関連仕様も存在するため，こうした仕様の適用も視野に入れて検討するべきと考えられる．

4.2.3　鍵生成ポリシ

鍵生成ポリシ（Key Generation Policy，以下 KGP）は，KGC が生成する Private 鍵について運用管理のルールを定めたものである．4.2.2 項と同様に，EE が鍵生成ポリシの内容を理解・評価することによって，また次項で述べる鍵生成業務実施規程の内容も合わせて理解・評価することによって，KGC に対する信頼を構築できると考えられる．

表 2 に示す KGP の文書構造のうち，必須（●および▲）とする章節について特に留意すべき点を考察した．

KGP 2 章は，次項で述べるとおり KGC は II と違って KGC パラメータなど公開すべき情報を持っており，これをリポジトリで公開する必要があるが，少なくとも KGPS で規定すべき内容であるため，KGP での記述は任意とする．ただし記述する場合には，その内容は KGPS のそれと整合していなければならない．

KGP 3 章では，KGC が発行する Private 鍵にひもづく ID 情報の信頼性をどのように担保するのかを明確にするために，KGC が Private 鍵を生成するにあたって認証を要求する II と，その II に対する要求方法などが具体的に規定されるべきである．KGP 4 章では，ID ベース暗号の技術的制約という観点から，特に Private 鍵の更新可否や，失効した場合の Private 鍵の取扱いなどについて規定すべきである．ID ベース暗号の手法によっては同一の ID 情報から Private 鍵が一意に決まるものもあり，運用の手法によっては Private 鍵の更新が不可能なものもあるが，たとえば ID 情報のプロファイルにおいて，ID 情報以外に識別子を加えることで Private 鍵の識別子を排除し，鍵更新に対応することが可能な場合もある．

KGP 6 章は主に業務実施規程で記述される内容であるが，KGP では生成した EE の Private 鍵が安全に EE に配布されることを担保するために，生成された Private 鍵がどのように EE に配布され防護されるかについて，明確に規定されなければならない．KGP 7 章では，生成する Private 鍵の暗号強度について評価できるよう，使用する KGC パラメータや暗号方式などが明示されなければならない．

4.2.4　鍵生成業務実施規程

鍵生成業務実施規程（Key Generation Practice Statement，以下 KGPS）は，KGC が公開する KGC パラメータや，KGC の秘密情報に関する運用管理のルールを定めたものである．4.2.3 項と同様に，EE が KGPS の内容を KGP と合わせて理解・評価することによって，KGC に対する信頼を構築できると考えられる．

表 2 に示す KGPS の文書構造のうち，必須（●および▲）とする章節について特に留意すべき点を考察した．

KGP/KGPS は原則として EE に公開されるべき情報であり，KGPS 2 章ではその公開手法とリポジトリの場所，アクセス方法などを規定する必要がある．また，KGC パラメータの公開にあたって，4.1 節で提案したリポジトリを利用する場合は，同様にその手法とリポジトリの場所，アクセス方法などについてもあらかじめ KGPS に規定しておくことによって，信頼性を確保することが可能となる．

KGC は，マスタシークレットなど Private 鍵生成に必要ないくつかの秘密情報を保持している必要があるため，KGPS 5 章および 6 章ではこうした秘密情報を安全に保持するうえで必要となる運用統制や技術的なセキュリティ統制について明示しておく必要がある．なお KGPS 6 章は一部を KGP に記載していることから▲とした．

KGPS 7 章は，4.2.3 項で述べたとおり生成される鍵のプロファイルについては KGP で規定されるべきであることと，2.3 節における PKI の事例分析においても業務実施規程では規定していないことから，KPGS においても記載しないこととした．

4.3　ポリシと業務実施規程を利用した信頼の構築

4.1 節で信頼モデルを提案し，4.2 節ではポリシと業務実施規程を提案した．これら 2 つにより，信頼の確立を行うためのフレームワークが提供され，従来では解決されなかった複数 KGC 環境での KGC への信頼確立など，利害関係者が他者との信頼を確立することを容易にする．たとえば各ユースケースでの II と KGC 間の信頼はポリシと業務実施規程による判断により確立され，EE と KGC の信頼は信頼モデルにより確立される．

本節では，信頼モデルとポリシ，業務実施規定を利用することでの EE による KGC への信頼構築の実現方法を検討する．

信頼モデルでトラストリストを利用する場合，EE 自身が他の KGC について信頼を判断しなければならない．リポジトリや ID 連携技術の応用手法を利用する場合では，EE はリポジトリや Discovery Service を信頼し，リポジトリや Discovery Service が KGC の信頼性を判断するという階層的な信頼構造となる．EE からみると，直接信頼する相手は一定数におさえられるため，信頼の制御という点ではトラストリストよりも分かりやすいものとなる．

リポジトリや Discovery Service は，その KGC の KGP/KGPS によって信頼性を判断する必要がある．また，KGC が Private 鍵を生成する際には，II から発行された EE の ID 情報が，KGP の ID 情報プロファイルと整合することを確認する必要がある．

リポジトリや ID 連携技術の応用手法を利用する場合には，EE は各 KGC を直接信頼するわけではないものの，KGC の信頼性を判断する根拠となる KGP/KGPS（場合によっては IP も含まれる）は，いずれの信頼モデルにおいても最終的な信頼者である EE に開示されているべきである．このため，KGP/KGPS や IP の配布場所（URL など）を記述可能なデータフォーマットが必要となる．

これらの信頼モデルと，ポリシと業務実施規程により，複数の II と複数の KGC が混在する環境での信頼の確立が容易になる．

本提案は，信頼モデルの中での信頼構築フレームワークを定義したものだが，ポリシ（と業務実施規程）の文書構想を定義したことによって，異なるポリシを持つ複数の信頼ドメインどうしが相互接続する場合においても，ポリシの比較評価を行ううえで有益になると考えられる．

5. ま と め

ID ベース暗号は長らく現実的な実現方式が提案されてこなかったが，2000 年以降に現実的な実現方式が複数提案され近年ではそれらの手法の標準化が進んでおり，ID ベース暗号は実用化に向けた段階にあるといえる．

しかし，ID ベース暗号の実用化にはまだ課題が多く残る．その 1 つは，ID 情報から Private 鍵を生成する鍵生成局（Key Generation Center）の信頼構造の実現である．しかし既存の ID ベース暗号のプロトコルや，その応用手法ではその信頼の確立を実現できていなかった．

そこで本論文は，ID ベース暗号に必要とされる信頼を確立するための信頼構築フレームワークを提案した．提案するフレームワークは，信頼モデルと，ポリシと業務実施規程により構成される．信頼モデルでは，既存の PC 環境などに容易に実現可能なトラストリストモデルや，外部の信頼構造を用いたリポジトリモデル，また Private 鍵生成を ID 連携における 1 つのサービス形態として考慮した ID 連携技術の応用モデルの 3 つを提案した．これらは，既存の環境や信頼構造，技術などを応用するものである．そしてポリシと業務実施規程では，実際に ID 情報を発行する Identity Issuer と鍵生成を行う Key Generation Center のそれぞれにポリシと業務実施規程を設けた．

本論文で提案した信頼構築フレームワークを利用することで ID ベース暗号の実用化の大きな課題であった信頼構造の確立を実現した．残る課題は，鍵や ID 情報のデータフォーマットの共通化や鍵の配布方式，保護方式，また鍵の再生成や危殆化にともなう Key Generation Center 自体の移行など技術面や制度面，運用面と多岐にわたるが，信頼構造のフレームワークが確立されたたことで，それぞれの面での課題に方向性を持たせることが可能となり ID ベース暗号の実用化を促進するであろう．

参 考 文 献

1) Shamir, A.: Identity-based cryptosystems and signature schemes, *Proc. CRYPTO 84 on Advances in Cryptology*, pp.47–53 (1984).
2) Sakai, R. and Kasahara, M.: ID based cryptosystems with pairing on elliptic curve, Cryptology ePrint Archive, Report 2003/054 (2003).
3) Boneh, D. and Franklin, M.: Identity-based encryption from the Weil pairing, *SIAM Journal of Computing*, Vol.32, No.3, pp.586–615 (2003).
4) Boneh, D. and Boyen, X.: Efficient selective-ID secure identity based encryption without random oracles, *Advances in Cryptology–EUROCRYPT 2004*, Vol.3027 of Lecture Notes in Computer Science, pp.223–238, Springer-Verlag (2004).
5) IEEE P1363: Standard Specifications For Public Key Cryptography. http://grouper.ieee.org/groups/1363/
6) Barbosa, M., Chen, L., Cheng, Z., Chimley, M., Dent, A., Farshim, P., Harrison, K., Malone-Lee, J., Smart, N.P. and Vercauteren, F.: SK-KEM: An Identity-Based KEM (June 2006). http://grouper.ieee.org/groups/1363/IBC/submissions/Barbosa-SK-KEM-2006-06.pdf
7) Boyen, X.: The BF Identity-based encryption system (Aug. 2006). http://grouper.ieee.org/groups/1363/IBC/submissions/Boyen-bf_ieee.pdf
8) Boyen, X.: The BB1 Identity-based cryptosystem: A standard for Encryption and

Key Encapsulation (Aug. 2006). http://grouper.ieee.org/groups/1363/IBC/submissions/Boyen-bb1_ieee.pdf
9) Shimaoka, M., Hastings, N. and Nielsen, R.: Memorandum for Multi-Domain Public Key Infrastructure Interoperability, RFC 5217 (2008). http://www.ietf.org/rfc/rfc5217.txt
10) Chen, L., Harrison, K., Moss, A., Soldera, D. and Smart, N.: Certification of Public Keys within an Identity Based System, *Proc. 5th International Conference on Informatino Security*, pp.322–333 (2002).
11) Smetters, D.K. and Durfee, G.: Domain-Based Administration of Identity-Based Cryptosystems for Secure Email and IPSEC, *Proc. 12th Conference on USENIX Security Symposium*, pp.215–229 (2003).
12) Price, G. and Mitchell, C.J.: Interoperation between a conventional PKI and an ID-based infrastructure, *Proc. 2nd European PKI Workshop*, pp.73–85 (2005).
13) OASIS Security Services (SAML) TC. http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security
14) Shibboleth. http://shibboleth.internet2.edu/
15) Liberty Alliance ID-WSF 2.0 Specifications including Errata v1.0 Updates. http://www.projectliberty.org/resource_center/specifications/liberty_alliance_id_wsf_2_0_specifications_including_errata_v1_0_updates
16) Chokhani, S., Ford, W., Sabett, R., Merrill, C. and Wu, S.: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, RFC 3647 (2008). http://www.ietf.org/rfc/rfc3647.txt
17) Burr, W.E., Dodson, D.F. and Polk, W.T.: Electronic Authentication Guideline, *NIST Special Publication 800-63*, Ver.1.0.2 (2006).
18) Cutler, R., et al.: Liberty Identity Assurance Framework 1.1. http://www.projectliberty.org/resource_center/specifications/liberty_alliance_identity_assurance_framework_iaf_1_1_specification_and_associated_read_me_first_1_0_white_paper
19) AMANO RootCA for TA/TSA TA 用証明書ポリシ，Version 1.00 (2006). https://www.e-timing.ne.jp/pdf/atb_free_ta_cp_v1p00.pdf
20) AMANO RootCA for TA/TSA TSA 用証明書ポリシ，Version 1.00 (2006). https://www.e-timing.ne.jp/pdf/atb_free_tsa_cp_v1p00.pdf
21) JASDEC 認証局証明書準則，Version 1.21 (2009). https://www.jasdec.com/download/ds/cp.pdf
22) 国立情報学研究所オープンドメイン認証局 2 証明書ポリシ，第 1.10 版 (2010). https://repo1.secomtrust.net/sppca/nii/odca2/NIIODCA2-CP-V1.pdf
23) AMANO RootCA for TA/TSA 認証局運用規程，Version 1.00 (2006). https://www.e-timing.ne.jp/pdf/atb_cps_v1p00.pdf
24) セコム電子認証基盤認証運用規程，Version 2.00 (2006). https://repo1.secomtrust.net/spcpp/SECOM-CPS.pdf

(平成 21 年 11 月 30 日受付)
(平成 22 年 6 月 3 日採録)

金岡　晃（正会員）

2004 年筑波大学大学院博士課程システム情報工学研究科修了．同年セコム株式会社入社．ネットワークセキュリティ，電子認証の研究開発に従事．2007 年より筑波大学大学院システム情報工学研究科研究員．2008 年より筑波大学大学院システム情報工学研究科助教．ネットワークシステムの安全設計方式，電子認証に関する研究に従事．博士（工学）．IEEE, ACM，電子情報通信学会各会員．

島岡　政基

1998 年慶應義塾大学大学院理工学研究科修士課程修了．同年セコム株式会社入社，2004 年より同 IS 研究所，現在に至る．2005 年より国立情報学研究所特任助教授（非常勤）を経て 2009 年まで同客員准教授．ネットワークサービス，ネットワークセキュリティ，電子認証の研究開発，また IETF にて PKI 相互運用に関する標準化に従事．

岡本　栄司（正会員）

1973 年東京工業大学工学部電子工学科卒業．1978 年同大学院博士課程修了．工学博士．同年日本電気中央研究所入社．その後，北陸先端科学技術大学院大学，東邦大学を経て 2002 年より筑波大学教授．情報セキュリティの教育・研究に従事．1990 年電子情報通信学会論文賞，1993 年本会ベストオーサ賞受賞．著書『暗号理論入門』（共立出版），『電子マネー』（岩波書店）等．