ID 連携技術を応用した複数ドメイン間の ID ベース暗号利用について

金岡 晃 † 島岡 政基 ‡ 岡本 栄司 †

† 筑波大学大学院 システム情報工学研究科
305-8573 茨城県つくば市天王台１－１－１

kanaoka@cs.tsukuba.ac.jp, okamoto@risk.tsukuba.ac.jp

‡ セコム株式会社
181-8528 東京都三鷹市下連雀 8-10-16 セコム SC センター

m-shimaoka@secom.co.jp

あらまし 複数ドメインにまたがって ID ベース暗号を利用するには、KGC（Key Generation Centor）のパラメータを安全にユーザへと配布する必要がある。本研究では、複数ドメイン間での利用で必要となるパラメータ交換のユースケースを検討し、ID 連携技術を利用した信頼のある KGC パラメータ交換の実現方法を提案する。

Multi-domain Identity-based Cryptography using Identity Federation Framework

Akira Kanaoka† Masaki Shimaoka* Eiji Okamoto‡

†University of Tsukuba
1-1-1 Tennodai, Tsukuba, Ibaraki 305-8573, Japan

kanaoka@cs.tsukuba.ac.jp, okamoto@risk.tsukuba.ac.jp

‡SECOM Co., Ltd.
SECOM SC Center, 8-10-16, Shimorenjaku, Mitaka, Tokyo 181-8528, Japan

m-shimaoka@secom.co.jp

Abstract When we want to use Identity-based Cryptography between several domains, parameters of Key Generation Center (KGC) should be trustworthily distributed. In this paper, at first we study usecases of parameter distribution in Identity-based Cryptography, and propose a trustworthy parameter distribution method by Identity Federation technique.

1 はじめに

ID ベース暗号は 2000 年に実現されてより広く研究が行われており、現在では IEEE や IETF などの標準化団体での標準化や、国内でも CRYPTREC で調査報告がなされるなど普及に向けた動きが進んでいる。

ID ベース暗号の普及に向けた課題の中には、複数のドメイン間で ID ベース暗号サービスを利用する方法論の構築も含まれる。ID ベース暗号では、ID を持つユーザが鍵生成センター（KGC:Key Generation Center）より Private 鍵の発行を受ける。同一の KGC（同一ドメイン）より Private 鍵発行を受けた 2 者間では ID ベース暗号サービスを利用することは容易だが、複数の KGC が存在する環境（複数ドメイン環境）では異なる。それぞれ別の KGC より Private 鍵

発行を受けた 2 者が ID ベース暗号サービスを利用することは、ID ベース暗号の手法そのものでは考慮されていない。

他の KGC 下で Private 鍵発行を受けている利用者に対し、ID ベース暗号による暗号化や署名を行うには、他の 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。そこで本稿では、ID ベース暗号を複数ドメイン間で利用するために、ID 連携技術を応用した手法を提案する。提案手法では、ID 連携の仕様である Liberty ID-WSF（Identity Web Service Framework）を利用することで安全に複数の KGC 情報の共有と配布を行うことを可能にする。

本稿の構成は以下の通りである。まず第 2 章で関連研究を紹介し、第 3 章では本提案で応用をする ID 連携技術の解説をする。第 4 章で手法を提案し、第 5 章でまとめる。

2　関連研究

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 年になり境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 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言われている。一方でその利点は誤解を生んでおり、ID ベース暗号が証明書が不要な方式であり PKI の代替技術あるいは後継技術として誤解されることも多い。

公開鍵証明書は公開鍵データと発行対象の Identity との結びつきを保証するため、「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が、公開鍵証明書を基にする PKI が提供するものは単に公開鍵データと Identity 情報を結びつけるものだけではなく、信頼構造の提供など、より大きなプラットフォームを提供する基盤であり、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 を持つユーザに対して Private 鍵を発行する主体を 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 鍵発行を受けているユーザに対して 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。こうした複数ドメイン間の信頼関係においては、単にドメイン間の信頼関係として捉えるではなく、具体的なステークホルダー間の信頼関係に着目して整理する必要がある [5]。

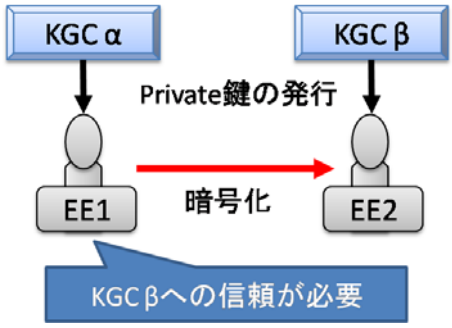

図 1: 複数 KGC 環境での信頼構造の必要性

1 つの KGC により提供されるサービス範囲を「ドメイン」とすると、複数ドメイン間で 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 に対して鍵発行を行うモデルを提案している [7]。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 [8]。

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 [9]。そこでは、PKIにおける証明書ポリシ（CP:Certificate Policy）文書や認証局運用規程（CPS：Certification Practice Statement）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。

3 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Identity情報を管理することの重要性が高まっている。その中で、Identity情報を各ドメイン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。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、代表的な実装としてはInternet2によるShibbolethがある。

またLiberty AllianceがSAMLを策定するID-WSF (Identity Web Services Framework)は、Webサービス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。

SAMLとID-WSFでは、プレーヤがIdentity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。

利用者はIdPよりID情報が発行されており、IdPにより認証された情報をSPに提示することにより、SPのサービスを受けることが可能である。他の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のSPからサービス享受を可能になる (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。

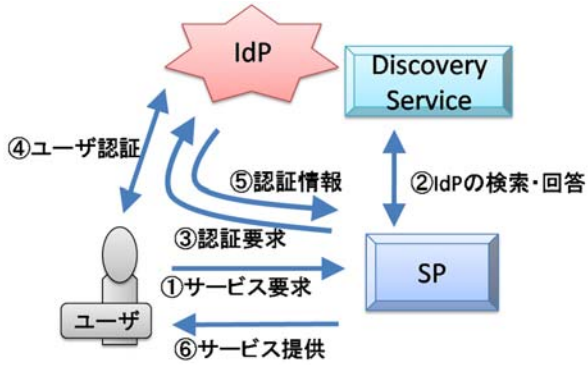

図 2: ID連携におけるサービス享受

4 複数ドメイン間でのIDベース暗号利用

4.1 ユースケースの分類

これまでのIDベース暗号では、ID情報を持つ利用者（EE:End Entity）と、利用者にPrivate鍵発行を行うKGCの2種類のプレーヤで議論されていた。しかし実際の運用を考慮すると、KGCがPrivate鍵を発行する際には、EEが持つID情報が真にそのIdentityに対し発行され、管理されているかの保証（認証）が必要である。

そこで本稿ではEEとKGCに加えてID情報の発行と管理を行う主体（ID Issuer）をプレーヤに含めて議論を行う。また本稿ではこれまでに「ドメイン」という用語を「KGCにより提供されるサービス範囲」としていたが、これ以降は「ID Issuerにより提供されるサービス範囲」を「ドメイン」と呼ぶこととする。

ID IssuerはEEに対しIdentityの確認と、ID情報の発行を行う機関であり、PKIで言う登録機関（RA：Registration Authority）に相当する。KGCはIDベース暗号のPrivate鍵をEE

に発行する機関である。そして EE は ID Issuer より発行された ID 情報と KGC より発行された Private 鍵により ID ベース暗号による暗号化や電子署名を行う（図 3）。

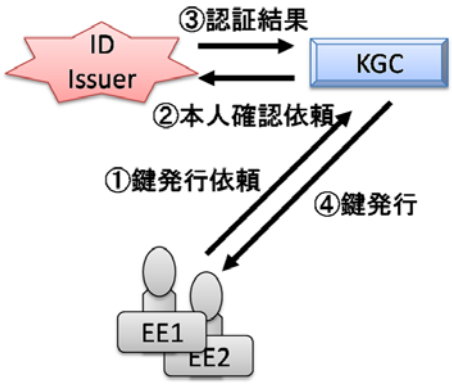

図 3: ID Issuer を含めた ID ベース暗号のプレーヤ

ID ベース暗号サービスを利用する 2 人の EE が、同一の ID Issuer と KGC より ID と Private 鍵を発行されているケースでは問題なく暗号化・電子署名のサービスを利用できる。一方、ID Issuer が複数あるケースや、KGC が複数あるケースでは問題が発生する。

ここで問題が発生するケースを分類したものを表 1 に示す。

表 1: ユースケースの分類

分類	ID Issuer/KGC	ドメイン構成
A	単一 ID Issuer/複数 KGC	単一ドメイン
B	複数 ID Issuer/複数 KGC	複数ドメイン
C	複数 ID Issuer/単一 KGC	複数ドメイン

複数の KGC があるケース A,B では、他方の KGC より Private 鍵発行を受けた EE に対して安全にパラメータを配布する必要がある。一方、複数の ID Issuer があるケースではその ID 情報がどの ID Issuer から発行されたのかを KGC が知る必要がある。

本稿では EE と KGC 間の情報配布に焦点を置くこととし、ケース A （図 4），B（図 5）での利用法を検討する。

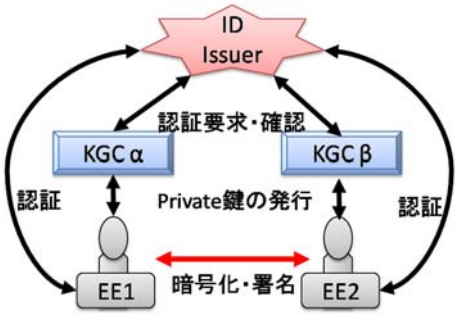

図 4: ケース A

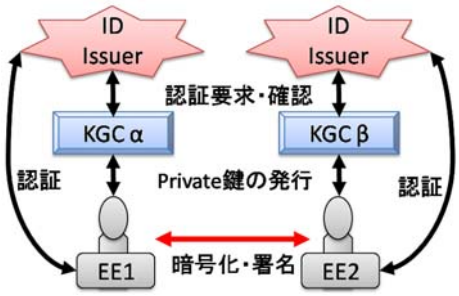

図 5: ケース B

4.2 KGC パラメータの取得方法

ケース A、B は「別の KGC から鍵発行を受けているユーザへの暗号化・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 の情報を安全に受け取ることが必要となる。

本稿ではその解決法を 2 つ提案する。

4.2.1 トラストリストの利用

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。

4.2.2 ID 連携技術の利用

ID 連携のプレーヤを、本稿で検討している ID ベース暗号のプレーヤと比較した時、その構成はほぼ同様のものになっていることがわかる（図 6）。

そこで、ID Issuer を IdP、KGC を SP と考えることとする。特に KGC は「EE に対して Private 鍵を発行するサービス」を提供する SP と考える。

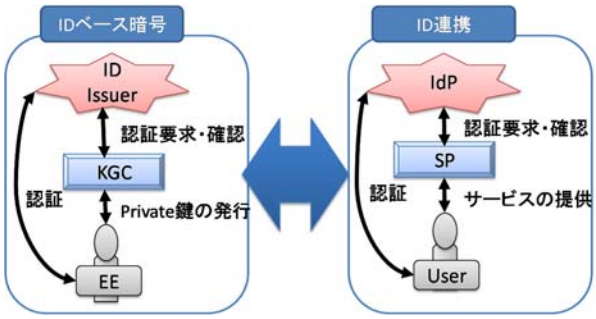

図 6: ID ベース暗号と ID 連携のプレーヤ

提案方式では IdP としての ID Issuer、SP としての KGC、そして EE の 3 者の他に、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 鍵発行を受けているかを発見・回答する Discovery Service である。ある ID がどの KGC から Private 鍵発行を受けたかの情報は、ID 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 の技術や仕様で実現が可能である。

もう 1 つは、要求された ID 情報の Private 鍵発行を行っている 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 6 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。

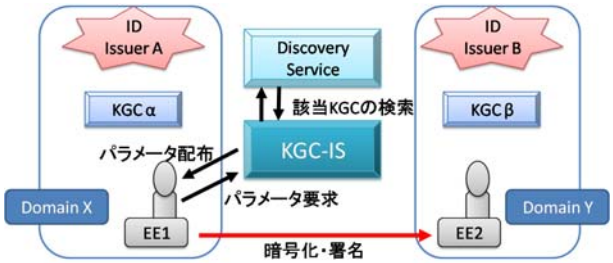

図 7: ID 連携技術の応用による提案モデル

4.3 パラメータ配布プロトコル

実際に ID 連携技術を応用した提案方式でパラメータ配布を行う場合には、その配布時の通信プロトコルも信頼のあるものでなければならない。

提案方式は ID-WSF を応用することで実現可能な方式であるが、ID-WSF では通信は SOAP を利用する。さらに SOAP は SSL/TLS と HTTP の上で動くことが考えられているため、SSL/TLS により信頼のある通信が行われる。

SSL/TLS は従来 PKI を利用する方式であり、Smetters らの方式 [8] と同様に、外部信頼構造の利用によるパラメータ配布の 1 手法と考えることができるが、一方で、小澤らにより提案されている SSL/TLS への ID ベース暗号拡張方式 [10] を利用することで、外部信頼構造を用いることなく信頼のある通信を実現することも可能である。

5 まとめ

ID ベース暗号は普及に向けたフェーズにあるが、まだ多くの課題を残している。その 1 つに、複数ドメイン間での暗号サービス利用がある。その解決手法として本稿では「トラストリスト方式」と「ID 連携技術応用方式」の 2 手法を提案した。特に ID 連携技術を応用した方式では、既存の ID 連携技術である ID-WSF（Identity Web Service Framework）を応用することで実現可能なモデルであり、既に存在する実装を用いることで容易に環境構築が行えることが予想される。

今後は、提案手法を実装する試作システムを開発し実証実験を行う予定である。

参考文献

[1] A. Shamir: Identity-based cryptosystems and signature schemes, *Proceedings of CRYPTO 84 on Advances in cryptology* , pp.47-53, 1984

[2] R. Sakai, K. Ohgishi, M. Kasahara: Cryptosystems Based on Pairing, 2000 年暗号と情報セキュリティシンポジウム（SCIS2000）, 2000

[3] D. Boneh, M. Franklin: Identity-Based Encryption from the Weil Pairing, *SIAM J. of Computing*, Vol.32, No.3, pp. 586-615, 2003

[4] D. Boneh, X. Boyen: Efficient Selective-ID Secure Identity Based Encryption Without Random Oracles: *In proceedings of Eurocrypt 2004*, pp. 223-238, 2004

[5] M. Shimaoka, N. Hastings, R. Nielsen: Memorandum for Multi-Domain Public Key Infrastructure Interoperability, *RFC 5217*, http://www.ietf.org/rfc/rfc5217.txt, 2008

[6] D. Boneh, X. Ding, G. Tsudik: Identity-Based Mediated RSA *In proceedings of 3rd International Workshop on Information and Security Applications, WISA '02*, 2002.

[7] L. Chen, K. Harrison, A. Moss, D. Soldera, N. Smart: Certification of Public Keys within an Identity Based System, *In proceedings of the 5th International Conference on Informatino Security*, pp. 322-333, 2002

[8] D.K. Smetters, G. Durfee: Domain-Based Administration of Identity-Based Cryptosystems for Secure Email and IPSEC, *In proceedings of the 12th conference on USENIX Security Symposium*, pp. 215-229, 2003

[9] G. Price, C. J. Mitchell: Interoperation between a conventional PKI and an ID-based infrastructure, *In proceedings of the Second European PKI Workshop*, pp. 73-85, 2005

[10] 小澤 洋、金岡 晃、岡本 栄司: ID ベース暗号の SSL/TLS 適用と OpenSSL 実装, 2009 年暗号と情報セキュリティシンポジウム（SCIS2009）, 2009