M_023

マルチドメイン環境におけるプライバシー保護を考慮したID生成管理手法の実装と評価

An Implementation and Evaluation of an ID Management Scheme with Privacy Protection on Multi Domain Environment

渡辺　龍† 窪田　歩† 田中　俊昭†
Ryu Watanabe Ayumu Kubota Toshiaki Tanaka

1. はじめに

ユーザが安心して、安全にインターネット上のサービスを利用するための技術として、信頼のおける第三者を利用した認証基盤による接続仲介の技術が挙げられる。マイクロソフト社の提供する、.NETpassport サービスや、Liberty Alliance Project の提案する ID フェデレーションなどが本技術にあたる。このような、認証基盤を用いた接続仲介にあたっては、サービス側がユーザを認識するための符号（ID）を適切に取り扱わなければ、ID に基づいて利用者の行動が紐付けされるリンカビリティや、ユーザの行動を追跡するトレーサビリティといった、プライバシー上の懸念が発生しかねない。このために、著者らはこれまでに、利用者が安心してサービス利用が可能な環境構築のために、大規模なネットワークに適用可能な利用者のプライバシーの保護を考慮した ID 管理方式について検討・提案をおこなってきた[1][2][3]。このような認証基盤は、非常に規模の大きなもの、例えば、大規模プロバイダによる運用・運営されるようなケースを想定している。また、利用形態としては、認証基盤を跨いだサービス利用等も想定できる。本稿では、こうした利用形態についての検討と検討に基づいて構築した実験システムの実装と評価について述べる。

2．ID 生成管理手法

2.1 ID に関するのセキュリティ要件

認証基盤による認証代行・接続仲介を実施するにあたり、サービス提供者がユーザ識別のために利用する ID にまつわるプライバシー上の要件を次のように整理した。

1. 実際にサービスを利用する際の ID は、認証基盤がユーザ認証を経て生成し、ユーザ自身の身元はサービスに対して秘匿する。
2. 異なるサービスに対しては、同一のユーザに対しても、異なる ID を利用する。
3. あるユーザが、同じサービスを利用する場合も、接続ごとに異なる ID を利用する。
4. 認証基盤は、利用者と ID との対応関係を把握しており、必要に応じて ID の利用者を特定できる。

要件の 3 については、利用者のポリシーに依存することとなる。常に ID を利用することにより、サービスを提供する側は、ID を通じてその利用者行動履歴を取得することが可能となる。これにより、例えば、リコメンドサービスのような機能を提供することが可能となり、サービスの利便性が向上できる。このため、毎回異なる ID を利用して追跡できなくし安全性を求めるか、付加的な機能による利便性を求めるかはユーザとサービス提供者の判断によるところである。

† （株）KDDI 研究所　KDDI R&D Laboratories, Inc.

2.2 サービス対応 ID

前述した要件を満たす ID の生成・管理にあたり、認証基盤がユーザとサービスに対して個別に生成し提供する ID であることから、著者らは「サービス対応 ID」と定義した。このサービス対応 ID は認証基盤へのログイン ID と暗号化の技法を用いて生成する方式を採用した。

$$\text{サービス対応 ID} = E_{Ks}(\text{ログイン ID} \,\|\, S_{info})$$

E_{Ks}:鍵 Ks による暗号化、||: ビットの結合を示す

ログイン ID に結合させる S_{info} を毎回異なる値にすることで毎回異なる ID（匿名 ID と呼ぶ）が生成でき、毎回同じ値にしたならば、常に固定的な ID（仮名 ID と呼ぶ）が生成できることとなる。どちらの ID を生成するかは、ユーザとサービスのポリシーに依存し、ID 生成にあたって、双方のポリシーを付け合せるポリシー判定を実施する。また、このように ID を生成管理すると、利用者と ID の紐付けは、ID 自身に埋め込まれているために、認証基盤は ID 自体を管理する必要はなく、暗号化のための鍵だけを適切に保持し、ID を復号することで対応関係を把握することができる。接続ごとに異なる ID を生成し利用するような場合、大量の ID が生成されることとなるが、鍵だけを保持すればよい本方式が適しているといえる。こ

表 1　語句の定義

語　句	定　義
ログイン ID	認証基盤がユーザ識別するための ID
サービス対応 ID	ログイン ID から生成されるサービス利用のための ID
仮名 ID	サービス提供者に対してユーザとのリンクを絶つ固定のサービス対応 ID
匿名 ID	サービス提供者に対してユーザとのリンクを絶つとともに、接続ごとに動的に変化するが、正当な利用者であることは保証するサービス対応 ID
ID 生成	要求を受けて、サービス対応 ID を生成すること
ID 逆引き	サービス対応 ID からログイン ID などを導出し、ユーザを特定すること
サービス対応 ID 生成ポリシー	仮名 ID と匿名 ID のどちらの ID を利用したいかというユーザあるいはサービスの意向を示すポリシー
ポリシー判定	サービス対応 ID の生成時に、ユーザ及びサービスのサービス対応 ID 生成ポリシーを付け合せてどちらの ID を生成し利用するかを決定すること

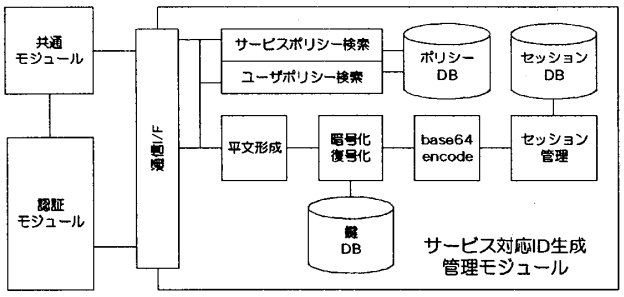

図1　認証基盤の内部構成

こで、サービス対応 ID に関する用語のまとめを表 1 に記す。

2.3　認証基盤の連携

認証基盤の連携によるサービス利用とは、あるドメインに属するユーザが別の基盤に属するサービスを利用することと定義する。また、このような形態をマルチドメインでのサービス利用と呼ぶこととする（同一ドメインの場合はシングルドメインと呼ぶ。）。この場合、二つの認証基盤が連携して ID を生成することとなり、どちらの基盤で ID を生成して管理するかについては、次のように考える。サービス対応 ID を生成するにあたっては、ポリシー判定を実施して、仮名 ID あるいは、匿名 ID のどちらかを決定した上で、ユーザのログイン ID を暗号化してサービス対応 ID を生成することとなる。ユーザが属する基盤で実施する場合には、ポリシー判定のための情報である、サービス側のサービス対応 ID 生成ポリシーをサービス側の認証基盤から取得する。一方で、サービス側の基盤で実施する場合には、ユーザのログイン ID 自体をサービス側の基盤へ渡す必要がある。このため、ユーザのログイン ID とサービス対応 ID との対応関係を双方の基盤が把握することとなり、漏洩時の危険性が増大してしまう。これに対して、サービス側のサービス対応 ID 生成ポリシーは、元来公開されているものであることから、本情報を基盤間で収受することは、セキュリティ上の懸念は発生しない。このため、基盤間を跨いだサービス利用にあたっては、ユーザの属する側の基盤にて生成する。

3. 評価システムの実装

3.1　システム構成

評価のためのシステムは、2 つの基盤を模擬するシステムから構成され、また、これら基盤に対して ID 生成や ID 逆引きの要求を発生する評価用のツールを作成した。基盤を模擬するシステム内は、ID の生成管理を行なうサービス対応 ID 生成管理モジュール、認証など、ID 生成管理以外の機能を模擬する認証モジュール、双方のモジュールの共通部分である共通モジュールから構成される（図 1）。サービス対応 ID 生成管理モジュールには、ポリシーなどの各種 DB、平文生成、暗号化のブロック等を実装した。また、認証モジュールと ID 生成管理モジュール間の

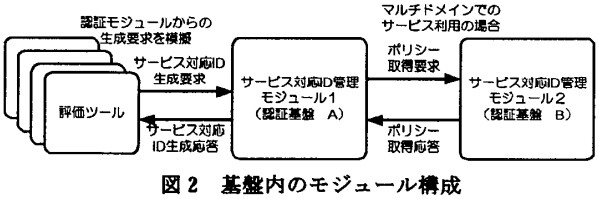

図2　基盤内のモジュール構成

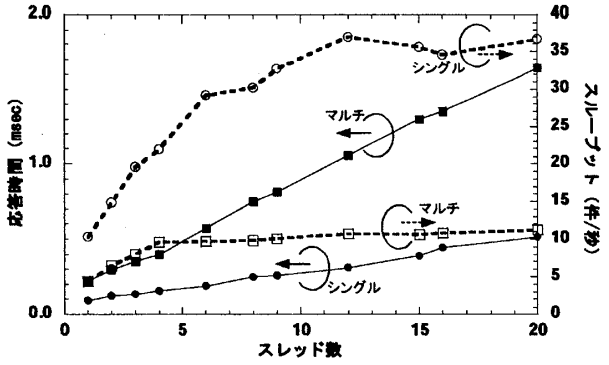

図3　性能評価結果（サービス対応 ID の生成）

通信は基盤の内部は多種のモジュールの疎結合で構成されるとの前提を置き、XML/SOAP により実装した。また、基盤間の通信には SSL を用いて暗号化通信路を生成し利用している。各モジュールの実行サイズ(ステップ数)は、ID 生成部分が、2,624 (1970)、認証モジュールが、2,668 (4,274)、共通モジュールが 49 (1,057)KB であった。ID 生成管理モジュールの評価にあたっては、認証モジュールからの ID 生成要求等を模擬する評価ツールを作成し、評価実験を行なった（図 2）。システムの実装には、CPU: Pentiumu4 (3.4 GHz)の PC を、評価ツールについては、CPU: Pentium4 (3.2 GHz)の PC を利用した（メモリは共に 1 GByte）。

3.2　性能評価試験

評価ツールより ID 生成等の要求をモジュールに対して発生させ、応答時間とスループットを評価した。図 3 は、その際の応答時間とスループットである。図中のスレッド数とは、ID 生成管理モジュールにかかる同時接続数を示している。スレッド数を増加させると共に、スループットは増加し、シングルドメインの場合で、35 件/秒、マルチドメインの場合で、10 件/秒程度であることが確認された。また、ID 生成に要する時間は、シングルドメインの場合で、90 ミリ秒、マルチドメインの場合で、220 ミリ秒程度であった。サーバのログによりマルチドメインの応答時間のうち約 110 ミリ秒程度が、基盤間の通信のための時間であることが確認された。現状、基盤間の通信を行なうにあたっては、通信ごとに SSL の通信路を構築する実装となっている。例えば、連携にあたり通信路を構築したままにし、その後の通信で利用等により更なる高速化が実現できると考えられる。

4. おわりに

本稿では、認証基盤におけるプライバシー保護を考慮した ID 生成管理手法の実装とその評価について説明した。評価の結果マルチドメインの場合でも 220 ミリ秒程度で ID を生成する 可能であり、大規模ネットワークにおいても十分対応可能な手法であることが確認された。

謝辞

本研究は、総務省からの委託研究の成果である。この場を借りて関係各位に深謝する。

参考文献

[1]　渡辺他, 2005 年電子情報通信学会総合大会, B-7-20, 2005.
[2]　渡辺他, 2005 年 5 月 NS 研究会, NS2005-28, 2005.
[3]　渡辺他, 2006 年電子情報通信学会総合大会, B-7-121, 2006.