ISS-P-130

複数の IdP を用いたシングルサインオンの提案と実装

伊藤　友浩†　　岡部　寿男††
† 京都大学大学院情報学研究科　　†† 京都大学学術情報メディアセンター

1. はじめに

シングルサインオンによって複数のサービスを単一の認証で利用できるようになり，ユーザーの負担を軽減することに成功した．一方で，認証部分で障害が起きた場合や攻撃を受けた場合においては，全てのサービスが影響を受けてしまう恐れがあった．そこで本研究では，複数の認証サーバー(IdP)を用いたシングルサインオンについて提案と実装を行う．

2. 関連技術

2.1 シングルサインオン

シングルサインオンとは，複数のサービスを一度の認証で利用出来るようにすることである．これによって，ユーザーは 1 つのパスワードのみを記憶するだけで良くなり，負担を軽減することができる．シングルサインオンを達成するためには，SAML(Security Assertion Markup Language)[1]や OpenID[2]が用いられる．

2.2 SAML

SAML とは，OASIS(Organization for the Advancement of Structured Information Standards)で策定された認証情報を交換するための XML の仕様である．SAML にはユーザーの属性情報を記述することができ，認証だけでなくアクセス制御などの認可を実現することも可能である．SAML を用いたシングルサインオンではサービスを提供する SP(Service Provider)の他に，認証を行う IdP(Identity Provider)を用いる．ユーザーは IdP で認証を行い，SP は IdP で行われた認証結果を信頼し，ユーザーにサービスを提供する．

2.3 秘密分散

秘密分散とは，秘密にしたい情報を複数の情報に分割することで暗号化を行い，分割した情報を集めることで元の情報を復元することができる暗号のことである．集めた分散情報の数が一定数に満たない場合は，元の情報を復元することができない．分割の仕方については様々な方法があるが，本稿では Shamir の(k,n)閾値秘密分散共有法について紹介する[3]．

Shamir の手法では元々の情報を n 個に分割し，k 個以上の分割した情報の断片が集まった時，元の情報を復元することができる．具体的には，まず初めに，ユーザーは分散したい情報を切片とした k-1 次の方程式を x-y 直交座標系でランダムに決定する．次に，この方程式の構成点の座標を重複しないように n 個とり，(x, y)座標を分割した情報とする．k-1 次の方程式では，k 個の構成点がわかれば，方程式を一意に定めることができるので，秘密の情報である切片がわかり，閾値型の秘密分散が達成できる．また，k-1 個以下の座標情報を集めたとしても，残りの点がわからない限り方程式が定まらず，切片に関する情報が何も得られないことから，閾値以下の情報を集めたとしても，元の情報の部分的な情報さえも手に入れることができない性質を有している．

3. 提案手法

提案手法を図 1 に示す．本研究では複数の IdP を利用し，一定の数の IdP で認証結果が得られた場合のみ，SP でサービスを提供することにより，攻撃や障害への耐性を高める．また，IdP に登録されているユーザーの属性情報を秘密分散することにより，1 つの IdP を乗っ取っただけではユーザーの属性情報について何も情報が得られない環境を目指す．

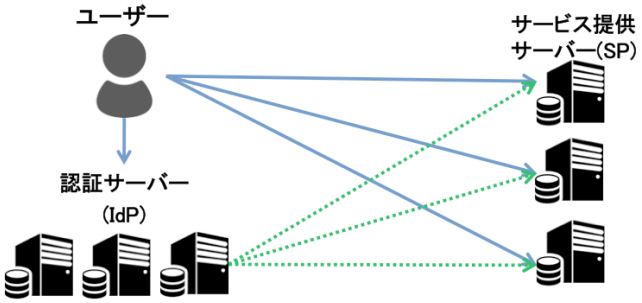

図1. 複数の IdP を用いたシングルサインオン

4. 今後の方針

複数の IdP を用いたシングルサインオンの実現に向けて，今後は実装モデルの検討を行う．最終的には，実装と評価を行う予定である．

参考文献

[1] S. Cantor, *et al.*, “Assertions and protocols for the oasis security assertion markup language.” OASIS Standard (March 2005), 2005.

[2] D. Recordon, *et al.*, “OpenID 2.0: a platform for user-centric identity management.” Proceedings of the second ACM workshop on Digital identity management, pp. 11–16, 2006.

[3] A. Shamir, “How to share a secret.” Communications of the ACM, vol. 22, no. 11, pp. 612–613, 1979.