4E-07

秘密分散技術を利用したパスワード認証代行システムのデータ管理

張 一凡，阿形 省吾，尾形 徹，徳永 大典

西日本電信電話株式会社

†(tyou.iifan, s.agata, t.ogata, d.tokunaga)@rdc.west.ntt.co.jp

1. 概要

ネットワーク上のサービスにアクセスする際のパスワード入力の手間を払拭するパスワード認証代行（シングルサインオン）システムが実現されている．ユーザの利便性を向上できるが，利用に際してユーザはパスワード情報をシステムに登録する必要があり，セキュリティの不安を伴っていた．本施策では秘密分散技術を用いて，ユーザパスワードを外部システムに預けることなく，安全にパスワード認証代行システムを利用する方式について紹介する．

2. 背景

クラウドの普及に伴い，ネットワーク(Web)上のサービスに機密情報を保管するユーザが増加している．Web サービスアクセスの際の認証ではパスワードが一般的に用いられるが，パスワードリスト攻撃が問題となっている．リスクの回避には Web サービス毎に異なる ID・パスワードを利用することが望ましいが，利便性が低下するため実施しているユーザは少数に止まっている．この利便性の問題はパスワード入力を代行する（パスワード認証代行）システムを利用することで解決できると考えられる．

既存のパスワード認証代行システムはクライアント側のアプリケーションとして実装されている場合[3]（以降：**端末処理**）とクラウドサービスとして提供される場合[1][2]（以降：**クラウド処理**）がある．

端末処理ではユーザが Web サービスへアクセスする際にローカルで管理するパスワード情報を投入する．パスワードをローカルで管理するため，運用の不備以外で自身の意図と反して第三者に漏洩するリスクが低い．しかし，パスワード情報を保持していない端末では Web サービスへのログインを実施できない．また，ローカル端末の故障や紛失などによりパスワード情報を紛失した場合，利用している Web サービスへログインできなくなる可用性リスクがある．

クラウド処理ではユーザは Web サービスへアクセスする際に認証代行システムを経由し，システム内で管理されるパスワード情報を投入する．そのため，任意の端末で保管済みのパスワードを用いて Web サービスにアクセスでき，自身の運用不備によって紛失・漏洩するリスクが少ない．しかし，認証代行システム上に自身のパスワードを委託・保管する必要があり，自身が関与しないところで，システムへの攻撃や運用者の悪用などによる漏洩のリスクがあった．

本施策では認証代行システムでパスワードを保管する際にユーザがその安全性と可用性を把握できるサービス方式を検討する．

3. 課題

パスワード認証代行システムを提供するための課題を機密性と可用性の両立と整理した．

課題 1. パスワード保管の機密性保証

端末処理の場合，ユーザが自身でパスワードを保管するため，ユーザは管理するパスワードのアクセス状況の把握が用意であるが，自身の運用に起因する盗難・紛失などのリスクを払拭できない．対策例として，暗号化してパスワード情報を保管できる．しかし，運用の徹底が難しく，端末盗難やパスワード攻撃により復号されるリスクが伴う．

クラウド処理の場合，認証代行システムでパスワードを保管するため，ユーザは自身の運用リスクから開放されるが，認証代行システムでの漏洩・紛失について把握できない．対策例として，機密性保証のためにユーザの鍵を元にパスワード情報を暗号化してシステムで保管できる．しかし，鍵の扱いや外部からの攻撃，運用者の悪用に起因する情報漏洩について，ユーザはシステムを信用せざるを得ず，リスクを把握ができない．

課題 2. パスワード保管の可用性保証

端末処理では運用をユーザに委託するため，パスワード情報を管理する端末の故障や紛失に起因した可用性低下のリスクがある．対策例として，パスワード情報をユーザが指定するクラウドに保管し，可能性を向上する方法がある．

Secret sharing scheme on password management of an authentication proxy system

Iifan Tyou, Shogo Agata, Toru Ogata, Daisuke Tokunaga

NIPPON TELEGRAPH AND TELEPHONE WEST CORPORATION

しかし，この方法では冗長化数を増加させた際に情報漏洩のリスクも増加してしまう．

クラウド処理では認証代行システムでパスワード情報を管理するため，システムで適切に冗長化することにより，データ保管の可用性を確保が可能となる．しかしシステム停止に対する可用性低下のリスクがある．対策例として．ロードバランシングによって負荷を分散する方式があるが，DDoS 攻撃などによりサービスが提供できなくなると，ユーザが一切の Web サービスにログインできなくなるリスクを伴う．

4. 提案手法

本施策では，3 章で整理した課題を解決するため，秘密分散技術を用いたパスワード管理手法を提案する．秘密分散技術[4][5]とは，1 つの情報を複数(m 個)の断片に分散し，そのうちの一定数(n 個)(m>=n)の断片を収集することで元の情報を復元できるようにする暗号技術(**図 2**)である．共通鍵を用いた暗号化ではパスワード攻撃により復元される可能性があるが，秘密分散では断片情報が不足する限り復号される可能性がない．

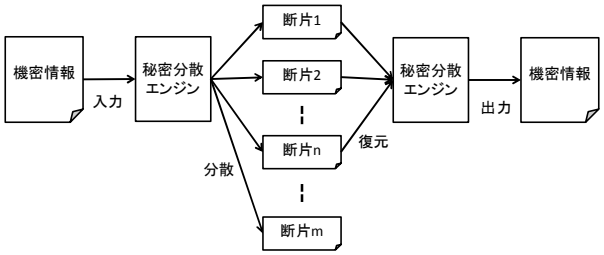

図 1 秘密分散技術

秘密分散技術を認証連携に用いたシステムでの認証フローとして，図 2 を検討した．

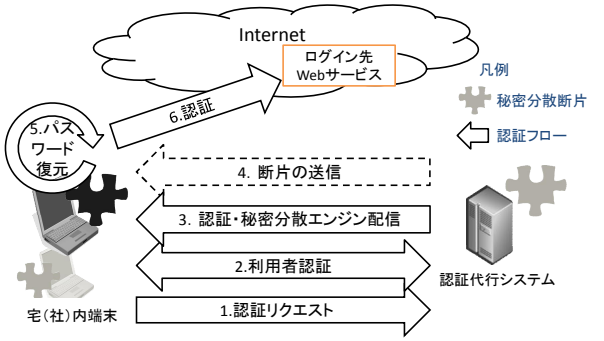

図 2 秘密分散を利用した認証代行システム

図 2 の認証代行システムでは秘密分散エンジンと必要に応じて断片情報を保管し，認証済みのユーザに提供する．パスワードの復元をクライアント端末で実施することにより，平文のパスワード情報は認証代行システムを含む第三者を経由しない．このシステムでは 3 章の課題に対して以下の様に解決できる．

課題 1. パスワード保管の機密性保証

パスワード情報の断片は認証代行システムにあるが，クライアントの断片抜きではパスワードを復号できない．認証代行システムからはユーザ端末を自由に操作できず，システム側で情報漏洩が発生しても，情報量的にパスワードを復号できないため，図 2 モデルではパスワードの機密性をユーザ操作によって担保できる．

課題 2. パスワード保管の可用性保証

ユーザは管理する断片数(m)を増加させて複数端末＋クラウドで保管することによりユーザ側の断片紛失時の機密性を確保しながら可用性を担保できる．認証代行システムに疎通できない場合もローカルの断片だけでパスワードの復号が可能であり，全体の可用性も向上できる．

5. サービス実現に向けた課題

図 2:フロー3. のエンジン配信方法としてリッチインターネットアプリケーション，ブラウザアドオン，ネイティブアプリケーションなどが考えられる．これらの実装ではそれぞれ異なる性能特性を持つと考えられるため，サービス提供に向けてはユーザの利用シーンを選定し，評価することが残課題と考えられる．

6. まとめ

パスワード認証代行サービスを利用する際に不安が残る第三者にパスワード管理委託するモデルを解消するため，秘密分散を利用したサービスモデルを提案した．これによりパスワード運用を改善でき，現在問題となっているパスワードリスト攻撃に対する対策の可能となる．システムの実装と実装方法による性能影響の評価は継続して取り組む必要があり，継続して検討していきたい．

参考文献

[1] forgerock, “OpenAM” http://forgerock.com/products/open-identity-stack/openam/

[2] forgerock, “OpenIG” http://openig.forgerock.org/

[3] LastPass, “LastPass” https://lastpass.com/

[4] Blakley, G. R, "Safeguarding cryptographic keys", National Computer Conference 48: 313–31

[5] Shamir, Adi, "How to share a secret", Communications of the ACM 22 (11): 612–613.