4E-06

パスワード漏洩とリスト攻撃のリスクを払拭するパスワード認証代行システム

阿形 省吾，張 一凡，尾形 徹，徳永 大典
西日本電信電話株式会社
(s.agata, tyou.iifan, t.ogata, d.tokunaga)@rdc.west.ntt.co.jp

1. 概要

パスワードの使い回しなど，ユーザの不適切なパスワード運用により Web サービス利用の安全性が低下している．対策として Web サービス毎に異なるパスワードを利用できるパスワード認証代行システムが有効である．しかし，既存技術ではユーザが指定したパスワードをそのまま利用するため，不適切な運用を完全に解消することはできないなど各種課題があった．本施策では，認証代行サービスの要件・課題とその対策について検討を行った．

2. 背景

インターネット上に存在する多くの Web サービスでは ID とパスワードを用いたユーザ認証を行っている．利便性のため，複数の Web サービス間で同じパスワードを使いまわし，長期的に更新しないなど，不適切なパスワード運用を行っているユーザが多い．結果，ある Web サービスでパスワードが漏洩した場合，そのパスワードを用いて別の Web サービスに不正ログインされるパスワードリスト攻撃[1]に代表されるパスワード運用の脆弱性が問題となっている．

パスワード運用の安全性を向上するため，Web サービス毎に異なるパスワードを利用し，定期更新を行う必要があるが，管理が煩雑でありユーザの利便性が低下する．利便性を損なわずに Web サービスを利用する手段としてパスワード入力を代行する既存のパスワード認証代行技術が利用できる．

パスワード認証代行技術を用いてユーザのパスワード運用の利便性と安全性の双方を確保するために，幾つか達成すべき要件があると考える．まず，パスワードの使い回し防止，定期更新を提供するため，システムでパスワードの自動更新機能を提供する必要がある．また，パスワードを管理する本システムの安全性確保が必要となる．

An authentication proxy system to prevent dictionary attacks
Shogo Agata, Iifan Tyou, Toru Ogata, Daisuke Tokunaga
NIPPON TELEGRAPH AND TELEPHONE WEST CORPORATION

本施策では，パスワードの自動更新機能を含む安全なパスワード認証代行サービスを提案する．インターネットを利用する大規模ユーザへのサービス提供を考え，安全性と利便性を柔軟に調整できるサービス方式の検討を行う．

3. 検討方針

サービスの実現に向け，既存技術であるパスワード認証代行を利用し，不足する技術や改善点を整理する．

類似する既存技術としては認証要求をサーバ集約する構成(クラウド型)[2][3]と端末分散する構成(端末型)[4]が提案されている．

本施策ではシステム管理やユーザ環境更新への適用，開発コストにメリットのあるクラウド型を対象サービスの検討を行う．検討にあたり，既存技術では提供できない機能を 4 章で整理する．

4. 課題

クラウド型でのパスワード認証代行システムの全体構成図の例を図 1 に示す．背景で定義したパスワード更新機能は既存では実装されておらず，新たに効果的な実装方法を検討(**課題 1**)する必要がある．また，大規模のユーザ(例：100 万ユーザ)にサービスを提供するための性能確保方式についても検討(**課題 2**)が必要となる．

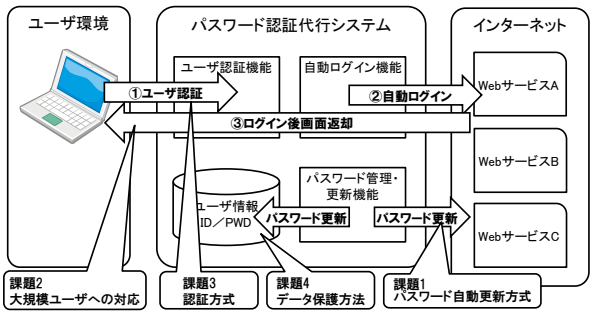

図 1　パスワード認証代行システム全体像

また，サービスの安全性を確保するために，パスワード認証代行システムをブラックボックスとしてみた時に，ユーザからのアクセス，内部の処理，Web サービスへの通信において安全性を保証する仕組みが必要となる．ユーザからのア

クセスでは認証などの安全性確保が必要になるが，認証の複雑さは利便性を低下させるため，安全性と利便性の両立方法について検討する(**課題 3**)必要がある．内部の処理ではパスワードの保管方法等について精査し，ユーザが信頼できる保管モデルを定義する(**課題 4**)ことが求められる．Web サービスへの通信については通信暗号化やサーバ認証により対策ができると考えられ，課題は無いと整理した．

5. 課題に対する考察

4 章で整理した各課題について，その問題点と検討の観点を以下のように整理した．

課題 1：パスワード自動更新方法

Web サービスのパスワード変更方法として電話やメールによる依頼やコマンドラインベースの処理もあるが，http フォームに必要事項を入力する方法が最も一般的である．そこでパスワード自動更新の実現のため，パスワード変更用 URL へのアクセスや http フォームへの必要事項の入力を自動化するツールを評価した作成・評価した．その結果，更新ツールによるユーザ一人あたりのパスワード更新の所要時間は 23 秒となった．そのため 100 万人規模のユーザに対してパスワード更新ツールを適用する場合には，複数のユーザを並列処理する必要となる．また今後必要に応じて http フォーム以外のパスワード変更方式の検討が必要となる．

課題 2：大規模ユーザへの対応

全ての通信がサーバを経由するため，サーバの性能がネックとなる．100 万人規模のユーザにサービスを提供するため，必要となる性能見積もった結果，処理が必要なリクエスト数は 10 万規模，TCP セッション数は 100 万規模となった．そのためサービス提供に向け，性能の観点から構築にはスケールアウトできるシステム構成を検討する必要がある．しかし，スケールアウトだけでは大規模なマシン構成を用いる必要があるので，効率化のため，認証を伴わない通信のフィルタリングなどサーバ負荷を軽減する方式もスケールアウト構成と並行して検討する必要がある．

課題 3：安全性と利便性を柔軟に調整できる認証方式

認証代行システムへのログインはパスワードを利用した認証が多く，先述のパスワードリスト攻撃の対象となる．パスワード認証と比較し安全性が高い認証方式として，複数の認証方式を組み合わせて認証する多要素認証が挙げられる．しかしサービス側で認証要素を一方的に設定した場合，ユーザの利便性は低下するため，ユーザが求めるセキュリティレベルに応じて自身が認証要素を選択できることが望ましい．複数の認証要素を提供し選択をユーザに委ねる構成は提供できるが，SIM と MAC 番号の組み合わせによる認証が端末紛失時に対策とならないなど，認証要素の組み合わせの安全性評価・ガイドライン化が必要となる．

課題 4：データの保護方式

サーバにパスワードを保管するシステムでは，運用者の悪用や漏洩のリスクを払拭し，ユーザに安心を提供する必要がある．

ユーザが委託するパスワードを保護するため，暗号化する手法がある．システム側が管理する鍵により暗号化する場合，システムでの鍵の漏洩や管理者の悪用のリスクがある．ユーザ側が管理する鍵によって暗号化する場合，ユーザでの鍵管理手間や鍵紛失のリスク，パスワードリスト攻撃リスクがある．

上記に示すように，暗号化を用いたデータ保護方式には鍵の管理リスクが存在する．これらの課題に対して秘密分散技術をパスワード管理に適用する方式[5]を提案する．

6. まとめ

Web サービスユーザのパスワード利用のリスクを払拭するため，パスワード自動変更・更新機能を持つパスワード認証代行システムを提案し，実現に向けた課題に対して検討を行った．これにより，従来方式に対して着手すべき観点を明らかにした．今後システム構築や性能評価を実施することで，継続して検討していきたい．

参考文献

[1] 独立行政法人情報推進機構セキュリティセンター, “2014 年版情報セキュリティ 10 大脅威” https://www.ipa.go.jp/security/vuln/10threats2014.html

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

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

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

[5] 張 一凡, “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” IPSJ 第 77 回全国大会