ソーシャルメディアにおける安全な情報共有に対しての研究

1130387 前橋賢希　【 清水研究室 】

1　はじめに

近年では, ユーザ同士が情報を交換する事によってサービスが成り立つ, ソーシャルメディアというサービスが多く普及している. その中でも現在発展しているものが SNS である.

SNS のユーザ数は急速に増加している [1]. そして, SNS は知人, 家族といったクローズド空間から, 誰もがアクセスできる, オープン空間へと変化している. これに伴い, SNS ではセキュリティやプライバシーに関わる問題が表面化している. 誰もが気軽に情報を掲載する事ができるが故に, 個人情報の漏洩が懸念されるようになった. [2]

本研究では, ユーザの個人情報を抽出する実験データにおいて, ユーザが掲載している投稿情報から, 本名や家族構成, アドレス等多くの個人情報が手と取得できるという実証がされているため, 「プライバシーに関わる情報集積問題」に関して研究を行う. またこの問題に関連してサービス内だけでなく現実社会にも影響を及ぼす問題も多く起きている [3].

本研究では, サーバ間認証を用いて情報共有するユーザを特定する事で, オープン空間である SNS をクローズド空間にする. さらに投稿情報を暗号化することで, 第 3 者への情報漏洩を防ぐ事が目的である.

2　研究内容

本研究では, サーバ間認証にて情報共有するユーザを特定し, 投稿情報の暗号化により, 第 3 者からの情報漏洩を防ぎ, 特定のユーザのみに閲覧を可能にする.

2.1　提案方式

本研究では, SNS においての情報漏洩を解決するために, 情報交換を行うユーザが適当なユーザである事をサーバ間認証を用いる. サーバ間認証には SAS と呼ばれるワンタイムパスワード認証方式を用いる. ワンタイムパスワード認証方式は, 認証を行う毎にパスワードを変更するため, 第 3 者からの盗聴やなりすましに対して強い特徴がある [4]. 認証後は, 投稿情報を暗号化し, ユーザが許可していないユーザまたは管理者から投稿情報が読み取られる事がないようにする.
提案方式の手順を図 1 に示し, 手順を説明する.

1. 情報発信するユーザ A が SAS サーバと認証
2. 認証した場合, SAS サーバは鍵を生成
3. 生成した鍵を認証情報を元に暗号化し, A に返す
4. A は認証情報を用いて複合し, 鍵を取得

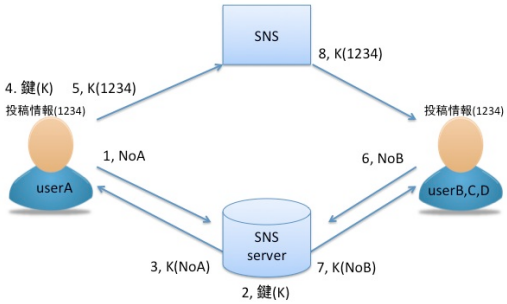

図 1　提案手法手順

5. 鍵を使って, 投稿情報を暗号化し, 投稿
6. 情報受信するユーザ B,C,D は SAS サーバと認証
7. 認証した場合, サーバは鍵を暗号化し, ユーザ B,C,D に返す
8. ユーザ B,C,D は鍵を復号し, 情報を閲覧

2.2　実験方法

提案方式の手順を実際に行い, サーバ間認証ができ, 投稿情報の暗号化が可能であること, 特定のユーザが投稿情報を閲覧可能であることを確認する.

2.3　評価

提案手法を実装した結果, サーバ間認証を行うことができ, 投稿情報を暗号化することができた. また, 投稿情報を特定のユーザから閲覧することができた.

3　おわりに

本研究で, SNS における安全な情報共有を提案する事ができた. 今後は SNS とは別のソーシャルメディアへの適用や, 情報を閲覧するまでにかかる手順を簡略化する事で, 実用性を向上させる必要がある.

参考文献

[1] 平成 23 年版情報通信白書　ソーシャルメディアの可能性と課題〞, 総務省

[2] SNS の安全な歩き方 セキュリティとプライバシーの課題と対策 JNSA SNS セキュリティWG 報告書

[3] 北野光一, 寺口敏生, 田中成典, 大谷和史, 小泉陽子,SNS の個人情報の保護に関する研究

[4] 大垣文誉, 小西竜也, 辻貴介, 清水明宏,”SAS を用いた Web 通信方式,”電子情報通信学会技術研究報告