情報処理学会論文誌 Vol.55 No.1 210–220 (Jan. 2014)

情報セキュリティ行動をツイートする情報共有手法の提案と受信者の情報接触行動の考察

原 賢[1,†1] 三浦 大樹[1,†2] 関 良明[2,a)] 諏訪 博彦[1]

受付日 2013年4月4日, 採録日 2013年10月9日

概要：社会の情報セキュリティレベルを高めるためには，一般ユーザが行動することが重要である．著者らは，身近な人が実際に行動しているという情報を共有できれば，自身に関連する情報セキュリティ行動に気づき，実際の行動に結びつけることができるのではないかと考えている．そこで，本稿では，身近な人の情報セキュリティ行動を情報共有する手法を提案し，そのシステムとしての実現性を確認するとともに，情報を受信した者の行動を実験により評価する．具体的には，情報セキュリティ行動を実施した際に残されるログを自動的に抽出し，Twitter ネットワークで公開する情報共有手法 Securitter を提案する．Securitter の要件と機能を検討し，アプリケーションプログラムを実装することにより Twitter との連動性を含むシステムとしての実現性を確認する．また，Twitter ネットワークを用いて，3 名の実験協力者（発信者）によるツイートを 47 名の被験者が 1 週間フォローする環境を構築して，被験者実験を実施する．その結果，30 名が情報セキュリティ行動を行うための情報を参照し，5 名が実際に情報セキュリティ行動を実施した．さらに，質問紙調査と構造化インタビューにより Securitter によるツイートを受信することの有効性，受容性を確認した．

キーワード：情報共有，情報セキュリティ行動，情報接触行動，Twitter ネットワーク

Proposal and Consideration of the Securitter which Tweets Behavior of Information Security

Satoshi Hara[1,†1] Hiroki Miura[1,†2] Yoshiaki Seki[2,a)] Hirohiko Suwa[1]

Received: April 4, 2013, Accepted: October 9, 2013

Abstract: In order to increase the security level of the information society, it is important that the end-user to act. We think that if the users can share the information that familiar person did the action, they will be aware of the security information and actually act related to their own behavior. In this paper, we propose a Securitter which is an information sharing method using Twitter network. Securitter automatically extracts the logs that are left when the users have conducted information security behavior. We consider the requirements and the functions of the Securitter and implement the application program in order to validate the feasibility of the system including the linkage with Twitter. In addition, we build a network environment using Twitter, and conduct an experiment that 47 users follow the tweets by 3 co-workers for a week. As a result, 30 users read the information to make the action, and 5 users actually did the information security action. Furthermore, we confirmed the effectiveness and acceptability of receiving tweets from the Securitter by structured interviews and questionnaires.

Keywords: information sharing, information security behavior, information contact behavior, Twitter network

[1] 電気通信大学大学院情報システム学研究科
Graduate School of Information Systems, University of Electro-Communications, Chofu, Tokyo 182–8585, Japan
[2] 日本電信電話株式会社，NTT セキュアプラットフォーム研究所
NTT Secure Platform Laboratories, NTT Corporation, Musashino, Tokyo 180–8585, Japan
[†1] 現在，NTT コムウェア株式会社
Presently with NTT COMWARE Corporation
[†2] 現在，日本電信電話株式会社，NTT ソフトウェアイノベーションセンタ
Presently with NTT Software Innovation Center, NTT Corporation
[a)] seki.yoshiaki@lab.ntt.co.jp

1. はじめに

社会活動に直結したネットワークサービスの著しい普及にともない，一般ユーザにおいても看過できない脅威が身近に迫っており，自身に関連するセキュリティ脅威を十分に認識し，対策を講じることが重要といわれている [1]．一方，情報セキュリティ上の危険な行為について，「セキュリティパッチを適用しないで使い続けること」を問題であると認識している利用者が 8 割いるが，「セキュリティパッチの更新」を実施している者は約 6 割にとどまり，問題と認識していても対策に反映されていないことが報告されている [2]．本稿では，このような対策を一般ユーザが講じることを情報セキュリティ行動と呼び，「セキュリティソフトの導入」や「セキュリティパッチの更新」，「信頼できる場所からアプリをインストールする」などの行動を指すものとする．

著者らは，身近な人が実際に情報セキュリティ行動を実施しているという事実を知れば，自身に関連する情報セキュリティ行動に気づき，実際の行動に結びつけることができるのではないかと考えている．そこで，情報セキュリティ行動を実施した際に残されるログを自動的に抽出し，ソーシャルネットワークである Twitter ネットワークに公開する情報共有手法 Securitter を提案する．Securitter の要件と機能を検討し，アプリケーションプログラムを実装することにより，Twitter との連動性を含むシステムとしての実現性を確認する．また，Securitter が一般ユーザの情報セキュリティ行動を喚起できることを確認するため，受信者を被験者とした被験者実験を行い，ツイートを受信することの有効性と受容性を評価する．以下，2 章で，情報セキュリティ行動に関するユーザの特性や，Twitter を介した情報共有に関する関連研究について述べ，3 章で，Securitter のコンセプトとシステム概要を提案する．4 章では，Securitter の発信者が円滑に情報を発信するためのアプリケーション実装を論じる．5 章では，情報セキュリティ行動に関するツイートを受信する被験者実験とその結果を述べ，6 章で，被験者に対する質問紙調査と構造化インタビューの結果からツイートを受信することの有効性と受容性を考察する．

2. 関連研究

情報セキュリティ行動を喚起する情報共有システムの発想を具体化するために，情報セキュリティに対するユーザの特性に関する研究，ユーザ同士のコミュニケーションに用いられるソーシャルメディアの特性に関する研究を以下にあげる．

2.1 ユーザ特性に関する研究

情報セキュリティに対するユーザの特性に関する研究として，ユーザが情報セキュリティ行動を行う要因を模索する研究が行われている [3], [4], [5]．

島らは，ユーザが情報セキュリティ対策を実施しないことについて，防護動機理論を用いたアプローチで調査，分析を行っている [3]．防護動機理論とは，人の対処行動は直面する問題に脅威を感じ，その問題から自分を守ろうとする動機から発生すると仮定したものである．対処行動は，利用者個人の脅威低減で完結する行動と，多数の利用者による集合的な行動に分類され，特に後者を集合的防護動機理論と呼んでいる．この集合的防護動機理論によって，「自分にはこの行動を実行する責任がある」という責任認知，「この行動は多くの人が実行しているのだろうか」という実行者割合認知，「自分がこの行動をすることを周囲の人たちは期待しているだろう」という規範認知といった集団内を意識した認知要素を示している．

菅野らは，情報セキュリティ対策を進める動機となる要因や，対策の実施を阻害する要因を求め，情報セキュリティ対策におけるモチベーション因子を求めている [4]．モチベーション因子は，一般ユーザの行動の動機となる要因と行動を阻害する要因からなり，動機要因に組織内の要求，阻害要因にユーザの技術，理解，手間が考えられるとしている．

諏訪らは，ユーザが情報セキュリティ行動を行わない要因を明らかにし，一般ユーザのセキュリティ行動を促進する方法を策定するために，情報セキュリティ行動モデルを構築している [5]（**図 1**）．情報セキュリティ行動モデルは，一般ユーザが情報セキュリティ行動に至るまでのモデルを構築し，「行動」に影響を及ぼす要因として「知識」と「態度」を規定したうえで，その要因と行動の関連性を明らかにしている．図 1 において，知識の各要因から態度・行動の各要因へ，および態度の各要因から行動の各要因へパスを引き，その影響の強さを係数として付記している．ここで「知識」はセキュリティ知識とセキュリティスキル，「態度」はコスト感，貢献感，外部要請，関心，無効感の 5 つの要因（**表 1**）に分別し，「行動」は，意識的セキュリティ

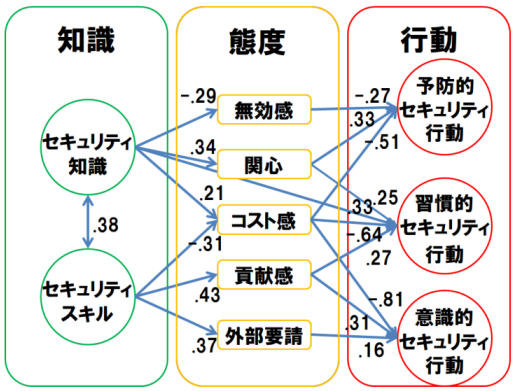

図 1 情報セキュリティ行動モデル（文献 [5] より作成）
Fig. 1 The model of information security behavior.

表 1 情報セキュリティ行動モデルの態度項目
Table 1 The attitudes in the model of information security behavior.

態度項目	例
コスト感	・情報セキュリティ行動は金銭的に負担がかかる. ・情報セキュリティ行動は手間がかかる.
貢献感	・私が情報セキュリティ行動をすると, 被害の規模を小さくする. ・被害に合う確率を下げる効果がある.
外部要請	・他者(学校や職場)から情報セキュリティ行動を求められている. ・情報セキュリティについて詳しい友人がいる.
関心	・情報セキュリティは高めるべきである. ・社会にとって情報セキュリティは重要な問題である.
無効感	・私はセキュリティ被害にあっても, 大した問題ではない. ・ウィルス感染やフィッシング詐欺は私には関係がない.

行動，習慣的セキュリティ行動，予防的セキュリティ行動の 3 つに分別している．

これらの研究より，自分の周りの他者がセキュリティ行動を実施しているという情報を共有することは，受信者の情報セキュリティ行動を促すのではないかと考える．

2.2 ソーシャルメディアの特性に関する研究

青柳らは，ゆるいコミュニケーションによって環境配慮行動の継続促進手法を提案している [6]．ゆるいコミュニケーションとは，通山らによると「明示的な意見の交換を前提にせず，特定の誰かに対するメッセージであることを意識させずに，相手の気配や存在を『感じさせる』もの」としている [7]．Twitter は明示的な意見の交換を前提としないため，心理的な抵抗感が小さいという特徴が指摘されており [7]，ゆるいコミュニケーションを実現するソーシャルメディアと考えられる．

Twitter，Facebook，mixi など普及の著しい国内のソーシャルメディアの利用実態調査における投稿理由の比較 [8] では，「自分の考えや感じたことを発信したいため」と回答した割合は，Twitter が 51.2%，Facebook が 32.0%，mixi が 45.7%であった．「発信する情報を通じて，他人の役に立ちたいため」と回答した割合も Twitter が最も高かったと報告されている．Twitter によるコミュニケーションは，付随する社会的なストレスが小さく，人々の間で好んで行われているとされ [9]，継続性が高いと考えられる．そのため情報セキュリティ行動を実施しているという情報を共有するツールとして適していると考える．

3. Securitter の提案

2 章にあげた関連研究を参考として，情報セキュリティ行動を喚起する手法を提案する．

3.1 提案コンセプト

提案コンセプトのポイントは以下の 4 点である．

1. 身近な人が情報セキュリティ行動を実施したという情報を共有する．
2. 共有する情報には，情報セキュリティ行動を促す情報が含まれている．
3. 発信者の発信コスト（手間や抵抗感）が低い．
4. 受信者の受信コスト（手間や抵抗感）が低い．

2.1 節で示したとおり，情報セキュリティ行動を促す要因として，集合的防護動機理論の集団内を意識した認知要素 [3] や組織内の要求 [4]，情報セキュリティモデルの外部要請 [5] など，自分が所属している集団内の他者の存在が指摘されている．また，情報セキュリティ行動モデルによれば，「コスト感」「無効感」を低減させること，「貢献感」，「関心」，「外部要請」「知識」を向上させることによって，情報セキュリティ行動が向上すると指摘されている．

このことから，身近な人（発信者）が実際に情報セキュリティ行動を実施しているという情報を共有した受信者は，自身に関連する情報セキュリティ行動に気づき，受信者も情報セキュリティ行動を実施すると考える．その際，情報セキュリティ行動モデルの要因に該当する情報をメッセージとして付与することは，受信者の情報セキュリティ行動をより促すと考える．

2.2 節に示した関連研究より，発信者が実施した情報セキュリティ行動を共有するための手段としては，投稿動機が高い Twitter が適当であると考える．Twitter は，フォロー関係を用いて他者とのゆるいコミュニケーションを形成できる．ゆるいコミュニケーションは，発信者および受信者の心理的な抵抗感やストレスが小さいとされており，一般的な話題になりにくいであろう情報セキュリティ行動を共有する手段として適していると考える．また，Twitter は，そのアカウントと端末が 1 対 1 に対応しないため，情報セキュリティ行動を実施したことを公開しても，端末に対して直接的な攻撃を受けにくく，プライバシーや新たなセキュリティリスクへ配慮できていると考える．

以上をふまえて，情報セキュリティ行動を実施したことをソーシャルネットワークである Twitter で共有する手法 Securitter を提案する．

3.2 システム概要

本稿で提案する Securitter の概念図を**図 2** に示す．ユーザは Twitter の利用者であることを前提とし，発信者と受信者に分けられ，図 2 中の黄線のように，受信者は任意の発信者のツイートをフォローしている．ただし，発信者は受信者ともなりうる．Securitter の利用ユーザである発信者は，自身の情報セキュリティ行動に関する情報を Twitter に投稿する．一方，受信者は Twitter を通じて自身とつながりのあるユーザの情報セキュリティ行動の実施に関するツイートを閲覧する．Securitter を用いることで，発信者は，半自動的にツイートすることができる．また，受信者は，新たな設定なしに身近な人の情報セキュリティ行動を知ることができる．

ここで，Securitter によって共有されるツイートは，情

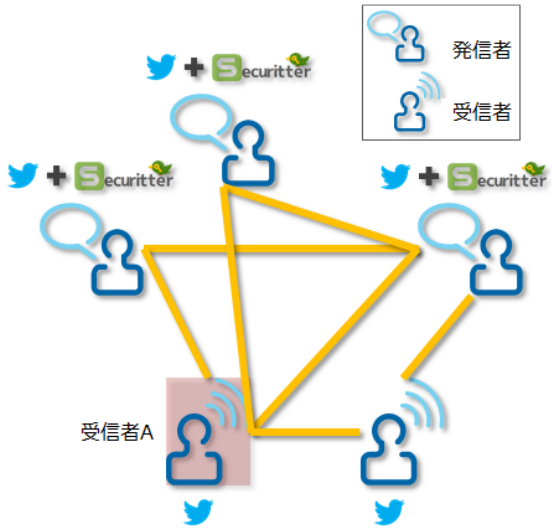

図 2 Securitter の概念図
Fig. 2 Conceptual diagram of Securitter.

報セキュリティ行動を行ったという事実に，情報セキュリティ行動モデルの「コスト感」,「貢献感」,「関心」,「知識」の 4 項目に関する情報を加えたものとする．

4. Securitter の実装

本章では，Securitter が満たすべきシステム要件と，それを実現するための機能について述べる．また，発信者の情報発信を補助するためのアプリケーションとして Securitter クライアントの実装について詳細に述べ，ユーザインタフェースを説明する．

4.1 設計方針と機能設計

情報セキュリティ行動モデルでは，情報セキュリティ行動を行わない理由として，「コスト感」が最も大きな割合を占めている [5]．情報セキュリティ行動を実施したうえで，さらにその行動に関する情報を発信することは，Securitter の発信者にとって大きなコストとなる．そのため，Securitter を実現するにあたり，発信者の手間をできるだけ削減する必要があると考える．

本システムでは，2 つの自動化によって，発信者の手間を削減することを目指している．1 つ目は，アプリケーションを端末上に常駐させ，一般ユーザの情報セキュリティ行動の実施を自動検知する機能である．2 つ目は，検知した情報から，システム上で共有されるメッセージを自動生成する機能である．この 2 つの自動化を実現するアプリケーションとして Securitter クライアントを実装することにより，発信者は自身の情報セキュリティ行動に関する情報発信を，特に意識せずに，行動から発信まで円滑に実行できると考える．

これら 2 つの自動化を考慮したうえで，本システムが満たすべき要件を**表 2** に整理する．R1〜R6 は Securitter クライアントを導入する発信者，R7，8 は受信者に関する要件である．また，**表 3** は，表 2 の要件を実現するための機能を示している．

表 2 要件一覧
Table 2 List of requirements.

要件	内容
R1	情報セキュリティ行動の情報を取得できる
R2	情報セキュリティ行動ログを生成できる
R3	メッセージを自動で生成できる
R4	メッセージを手動で編集できる
R5	メッセージを発信できる
R6	OAuth によって Twitter と API 認可ができる
R7	自身と繋がりのあるユーザを識別できる
R8	繋がりのあるユーザが発信したメッセージを表示できる

表 3 機能一覧
Table 3 Feature list.

要件	機能	内容
R1	F1	情報セキュリティ行動の情報を監視する機能
	F2	情報セキュリティ行動の情報の変化を検知する機能
R2	F3	情報セキュリティ行動ログを生成する機能
R3	F4	情報セキュリティ行動モデルに基づいたメッセージを生成する機能
R4	F5	メッセージを編集するウインドウを生成する機能
	F6	メッセージを編集する機能
R5	F7	メッセージの発信をユーザに確認する機能
	F8	メッセージを発信する機能
R6	F9	Twitter との OAuth による認可を行うウインドウを生成する機能
	F10	OAuth による認可に必要な URL を発行する機能
	F11	OAuth による認可に必要な PIN コードを発行する機能
	F12	PIN コードを入力し OAuth による認可を行う機能
R7	F13	ユーザ間の繋がりを保持する機能
	F14	発信されたメッセージを受信者によって振り分ける機能
R8	F15	繋がりのあるユーザが発信したメッセージを受信する機能
	F16	繋がりのあるユーザが発信したメッセージを閲覧する機能

要件 R1 は，発信者の情報セキュリティ行動を取得するもので，その行動を監視する機能（F1）とその変化を検知する機能（F2）が必要である．

要件 R2 は，情報セキュリティ行動の情報から情報セキュリティ行動ログを生成するものである．情報セキュリティ行動ログを生成する機能（F3）によって，発信者の情報セキュリティ行動をシステム内で扱いやすいデータ形式に変換する．

要件 R3 は，Securitter で発信するメッセージを自動で生成するものである．情報セキュリティ行動モデルに基づいたメッセージを生成する機能（F4）によって，情報セキュリティ行動ログからメッセージを生成する．

要件 R4 は，メッセージを編集するものである．自動で生成されたメッセージはそのまま発信されるだけではな

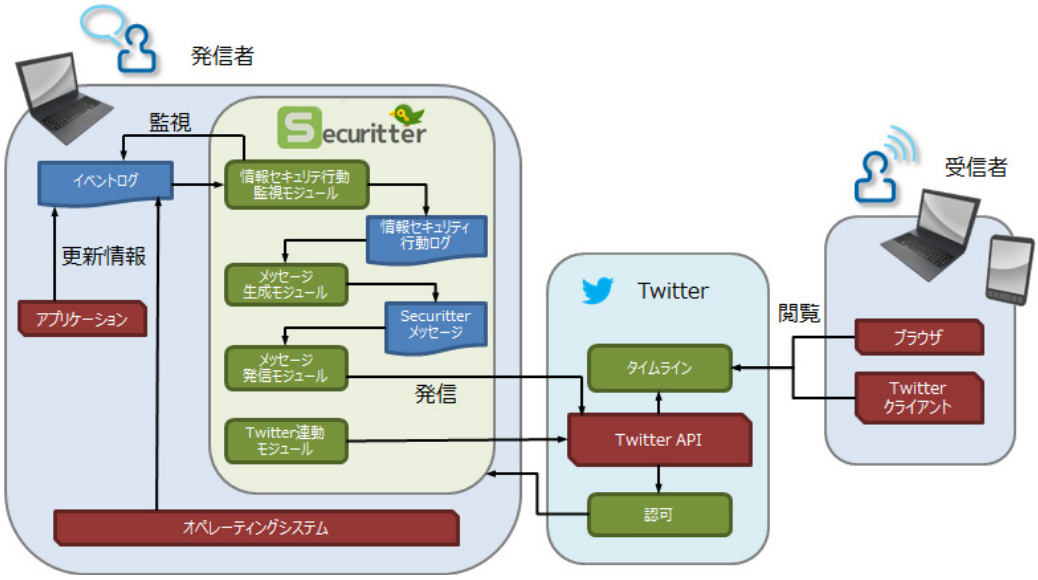

図 3 モジュール構成図
Fig. 3 Module configuration diagram.

く，メッセージの編集ウインドウを表示させ（F5），メッセージを編集する機能（F6）によって，発信者がメッセージを編集できるようにする．

要件 R5 は，メッセージを発信するものである．実際にメッセージを発信する前に，発信者に確認し（F7）メッセージの発信を行う（F8）．

要件 R6 は，Twitter との連動を可能にするものである．ユーザの許可したアクセス権限をアプリケーションに付与するためのプロトコルである OAuth による認可を実行するウインドウを生成し（F9），OAuth による認可を完了する（F10–12）．

要件 R7 は，受信者とつながりのある発信者に関するものである．発信者と受信者との関係を保持し（F13），そのつながりに従って発信されたメッセージを分類する（F14）．

要件 R8 は，受信者とつながりのあるユーザの情報の取得に関するものである．メッセージの受信（F15）と閲覧（F16）機能によって実現する．

以上の要件を満たし，それを実現する機能を有するシステムを実装する．要件 R1–6 は発信者の端末に導入された Securitter クライアント，要件 R7，8 は Twitter のシステムを利用する．機能 F13 は Twitter のフォロー/フォロワーのネットワーク，機能 F14–16 はタイムライン機能によって実現できる．

4.2 Securitter クライアントのモジュール構成

Securitter クライアントの実装にあたり，表 2 の要件を情報セキュリティ行動監視モジュール，メッセージ生成モジュール，メッセージ発信モジュール，Twitter 連動モジュールの 4 つのモジュールに集約する．

モジュール間の動作を**図 3** を用いて説明する．クライアントが実行されると，端末に常駐し，監視対象とする 1 つ以上のアプリケーションのイベントログを監視する．ユーザが情報セキュリティ行動を行うと，その行動を情報セキュリティ行動監視モジュールがキャッチする．受信した情報セキュリティ行動を基に，情報セキュリティ行動の対象やその内容，行動を行った日付や時間などを整理した情報セキュリティ行動ログを生成する．次に，情報セキュリティ行動ログはメッセージ生成モジュールに送られ，情報セキュリティ行動モデルに基づいた情報を付加し，Securitter メッセージを生成する．生成された Securitter メッセージは，メッセージ発信モジュールによって Twitter へ送信され，タイムラインに表示される．

以下，各モジュールの詳細を説明する．

(1) 情報セキュリティ行動監視モジュール：

発信者の情報セキュリティ行動を自動で検知するための実現方法としては，オペレーティングシステムのサービスやバックグラウンドプロセスなどを監視する方法から，アプリケーションレベルの更新情報のファイルなどを監視する方法まで，幅広い実装が考えられる．たとえば PC 上のユーザの行動情報を取得する方法としては，Windows のバックグラウンドプロセスである System Service の監視を行う方法 [10] や，ソフトウェアのイベントログを監視する方法 [11]，USB メモリ内に監視アプリケーションを仕込み，APIHook を用いて日時や移動ファイル名のログを取得する方法 [12] などが提案されている．

バックグラウンドプロセスを監視する方法は，幅広い行動情報に対応可能であるが，解析部に工夫が必要となる．一方，アプリケーションレベルの更新情報のファイルなどを監視する方法は，実装が容易であるがアプリケーションごとの対応が必要となる．そこで，Securitter では，PC の

(a) 起動画面　(b)認証画面　(c)ツイート画面

図 4　Securitter クライアント画面
Fig. 4　Securitter client screens.

イベントログを監視し，内容を分析してその情報をシステムの内部で扱うデータ形式であるセキュリティ行動ログに変換することとする．セキュリティ行動ログは，When, What，How の情報を “201302071010, Oracle Java, 更新” のような形式で記録している．

(2) メッセージ生成モジュール：

Securitter で共有されるメッセージを自動生成するためのモジュールであり，情報セキュリティ行動ログに，情報セキュリティ行動モデルの「コスト感」,「貢献感」,「関心」,「知識」に対応する文章をランダムに付与し，Securitter メッセージを自動生成する．

メッセージ生成モジュールには，共有するメッセージを自動生成する機能と発信者が編集する機能がある．自動生成機能は，前例のセキュリティ行動ログから，“Oracle Java の脆弱性に対処しました” という文章を生成し，たとえば “面倒な手続きはいっさいありませんでした” という「コスト感」を低減させる文言を付与する．このような文言は，「コスト感」,「貢献感」,「関心」ごとにあらかじめ 1 つ以上登録しておく．メッセージを自動生成する場合，発信者の手間を省くことができるが，発信者が行動ごとに同じようなメッセージを発信することや，異なる発信者においても同じメッセージになってしまう．そのため，発信者が特別に呼びかけているように見えず，受信者の行動を促す効果が低いと考えられる．この点を考慮して，「コスト感」,「貢献感」,「関心」,「知識」に対応する文章をランダムに付与することとしている．一方で，メッセージを発信者が手動で入力する場合，発信者の手間がかかってしまうが，行動を促す効果は高いと考えられる．

また，発信者にとって，自身の情報セキュリティ行動がつねに強制的にツイートされることは，プライバシーやセキュリティの観点から抵抗感があると考える．そこで，本稿の実装では，自動生成されたメッセージを編集可能なテキストエリアに表示させ，発信者が加筆修正できる自由度を残している．これにより，発信者の手間と抵抗感を低減させ，より効果的なツイートの生成を可能としている．

(3) メッセージ発信モジュール：

このモジュールは，Securitter メッセージを Twitter に投稿する．投稿の際には，自動生成されたメッセージの確認・編集ウインドウを表示することで，発信者の判断で投稿と編集を行うことが可能である．

(4) Twitter 連動モジュール：

このモジュールは，Securitter メッセージの発信を円滑に行うために，Securitter を Twitter に連動させる認可に OAuth を用いる．OAuth はユーザの許可したアクセス権限をアプリケーションに付与するためのプロトコルである．発信者は，Securitter クライアントに対して「Twitter に投稿する」権限のみ委譲する．OAuth の仕様上，Securitter クライアントが発信者のパスワードなどを要求したり，保持したりすることはなく，発信者のセキュリティやプライバシーに配慮できると考える．

4.3　ユーザインタフェース

Securitter クライアントの画面を図 4 に示す．

(a) は起動画面であり，アプリケーションを起動するとこのウインドウが表示される．(1) のテキストフィールドには認可状態が表示される．連動が完了している場合は，認可されたユーザ名が表示される．(4) の Start ボタンを押すと，監視が開始される．Securitter クライアントが情報セキュリティ行動を検知すると，メッセージが自動生成され，(c) ツイート画面に切り替わる．(9) のテキストエリアには自動生成された Securitter メッセージが表示される．発信者はこのウインドウでメッセージの編集を行うことができる．(10) の Tweet ボタンを押すと，このとき (9) に表示されているメッセージがそのまま Twitter に投稿される．もし，投稿したくない場合は (11) の Cancel ボタンを押すことで，投稿を中止することができる．投稿が完了すると，(a) の起動画面に戻り，引き続き監視が続けられる．

Twitter との連動が完了していない場合（たとえば初回起動時）には (3) の Login ボタンを押すと (b) 認証画面に切り替わる．(5) のテキストフィールドに，認可に必要な PIN

コードを発行するための URL が表示される．その URL をブラウザなどで開き，PIN コードを取得する．(6) の GO ボタンを押すことでそのページにジャンプできる．取得した PIN コードを (7) のテキストフィールドに入力し，(8) の OK ボタンを押すと連動が完了し，(a) 起動画面に戻る．

5. 被験者実験

3 章で提案した，身近な人が情報セキュリティ行動を実施した情報を共有する Securitter において，ツイートを受信することの効果を確認するために，Securitter による情報共有環境を疑似的に構築し，被験者実験を行っている．本章では，受信者を被験者として実施した Securitter の模擬運用と，その後に実施した質問紙調査と構造化インタビューの結果について述べる．

5.1 実験概要

実験は 2012 年 12 月 7 日にガイダンスを実施し，その直後から 1 週間の模擬運用を行い，終了直後の 12 月 14 日に質問紙調査を行っている．さらに，その後，構造化インタビューを 12 月 21 日から 28 日にかけて個別に実施している．また，12 月 28 日に被験者全員に実験全容を説明している．

模擬運用前のガイダンスでは，セキュリティの実験であることは明かさずに，1 週間の Twitter 利用の調査であることだけを説明し，ふだんどおりに Twitter を利用するように指示している．模擬運用後の質問紙調査では，Securitter の効果を有効性と受容性の観点から量的に確認している．また，構造化インタビューでは，より詳細に Securitter の特性を理解するために質的に確認している．最後の全容説明では，実験協力者（発信者）がツイートしていた文章が，ツイート予約サービス（後述）を利用した疑似的なものであったことを，倫理的観点 [13] から説明している．

5.2 模擬運用

模擬運用として，現実と Twitter 上の両方でつながりを持つ工学系大学に在籍する IT 系のサークル部員 47 名を被験者として，Securitter によるツイートを 1 週間受信してもらっている．具体的には，47 名の受信者に対して，全員がフォローしているサークルのリーダ的存在である 3 名の実験協力者（発信者）のアカウントを介し，疑似的な Securitter を用いて，実験協力者（発信者）1 名あたり 1 日 7 件のツイートを提示している（**図 5**）．ここで，Securitter を介したツイートを計画的に管理するために，ツイートの時間と内容（一例は図 4 (c) (9) 参照）はツイート予約サービスを利用して，コントロールしている．なお，ツイート予約サービスとは，発信者によってあらかじめ設定された時刻に，あらかじめ投稿されたツイートを発信者本人のアカウントで発信できるサービスである．

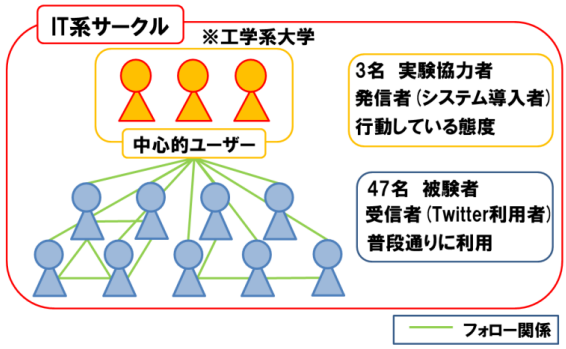

図 5 実験対象者の関係図
Fig. 5 Relationship diagram of an experimental.

ツイートによって喚起する情報セキュリティ行動は，IPA の緊急対策情報 [14] で呼びかけられているソフトウェアの脆弱性に対処するために更新するもの 5 種類（Windows Media Player，Microsoft Office，Oracle Java，Internet Explorer，Flash Player）を用意する．これらは情報セキュリティ行動モデルにおいて，習慣的行動に分類される．さらに，意識的セキュリティ行動に分類されるデータのバックアップ，USB メモリの暗号化を加え，合計 7 通りの行動を対象としている．ツイートの文章はこの 7 通りの情報セキュリティ行動に対し，「コスト感」，「貢献感」，「関心」にそれぞれ対応するメッセージ 3 種，9 種を掛けあわせた 63 通りを用意している．さらに，7 通りの情報セキュリティ行動に対応する「知識」を提供するために，IPA の記事を参照 URL として付与している．なお，ツイートの文章は，あらかじめ用意したものであり，被験者自身がツイートの文章を見る前に情報セキュリティ行動を実施している場合もあるが，その行動は被験者実験においては除外している．

被験者（受信者）は，ふだんどおりに Twitter を利用することとし，特別な制限はかけていない．

5.3 質問紙調査

模擬運用である 1 週間のツイート期間終了直後に 47 名の被験者に対して，質問紙調査を実施している．

Securitter のツイートを受信することの有効性を明らかにするために，被験者の行動を「Securitter のツイートを見る」，「ツイートの参照 URL をクリックする」，「URL 先の記事を詳細に読む」，「記事に書かれている情報セキュリティ行動を行う」という 4 段階の指標を用いて評価している．集計結果を**図 6** に示す．ここでは，模擬運用期間中に Securitter がツイートした 7 つの対象のうち，どれか 1 つでも 1 回以上該当した場合を行動としてカウントしている．

その結果，約 8 割の被験者が関連ツイートを見ており，6 割以上の被験者が URL をクリックしていることが確認できる．また，約 3 割の被験者が URL から情報を収集し，約 1 割の被験者が実際に行動していることが確認できる．

Securitter のツイートを受信することの受容性を明らか

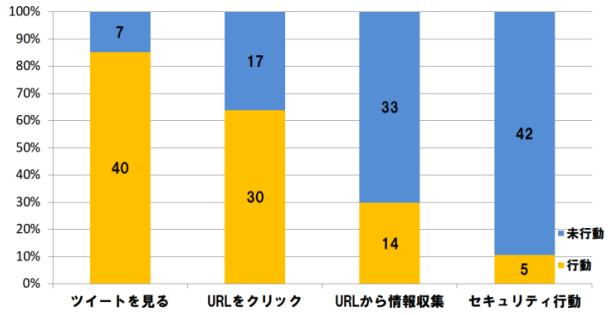

図 6 被験者の行動（有効回答数 47 名）
Fig. 6 Behavior of the subjects (Valid response 47).

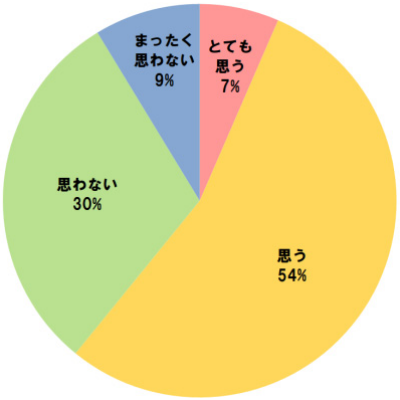

図 7 受信希望回答（有効回答数 46 名）
Fig. 7 Intention of receiving (Valid response 46).

にするために，「Securitter を使って情報を受信したいと思うか」という質問を設けている．それに対する回答結果を**図 7** に示す．被験者に「とても思う」，「思う」，「思わない」，「まったく思わない」の 4 件法で回答してもらった結果，有効回答数 46 名のうち「とても思う」，「思う」が 28 名，「思わない」，「まったく思わない」が 18 名であった．

また，被験者の特性を確認するため，対象とした 7 通りの情報セキュリティ行動に対するふだんの実施状況と，今回参照している IPA からの情報取得の習慣について，「よく行う」，「比較的行う」，「あまり行わない」，「まったく行わない」の 4 件法で回答してもらった（**図 8**）．

その結果，Flash Player の更新以外の行動は 4 割以下の実施率であり，意識的セキュリティ行動に分類される USB メモリの暗号化にいたっては，1 名のみの実施であることが確認されている．また，IPA から情報を取得している被験者も 1 名のみであることが確認されている．なお，「データのバックアップ」と「USB の暗号化」は，1 名未回答で有効回答数 46 名であった．

5.4 構造化インタビュー調査

ツイートがどのように行動に結びついたのか，また行動した人と行動しなかった人にどのような違いがあったのかを明らかにするために，構造化インタビュー調査を行っている．質問紙調査の集計結果をもとに，情報セキュリティ

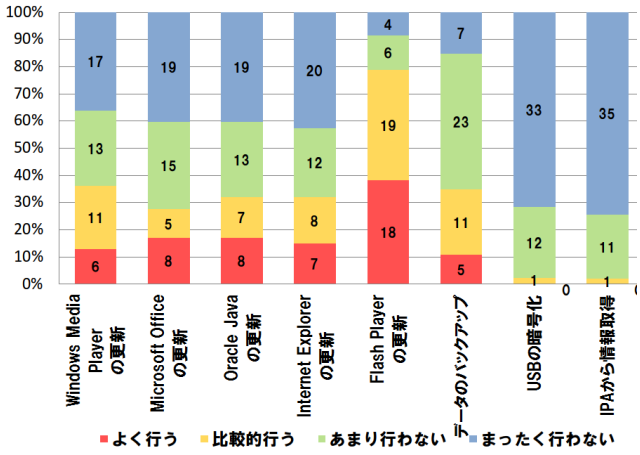

図 8 被験者のセキュリティに対するふだんの態度（有効回答数 47 名，一部 46 名）
Fig. 8 Usual attitude to the security of the subject (Valid response 47, partly 46).

行動を実施した行動者 5 名（A1～A5 とする）に行動した理由を，情報セキュリティ行動を実施しなかった 42 名からランダムに選定した未行動者 5 名（N1～N5 とする）に行動しなかった理由をインタビューしている．

行動者（A1～A5）に対する質問

1. 行動したときの状況と行動した理由を教えてください．
2. やらなかった対象との差はありますか．
3. 実験を通じて感想，気づいたことはありますか．

未行動者（N1～N5）に対する質問

1. 行動しなかった理由について教えてください．
2. 何を工夫すると行動しそうだと思いますか．
3. 実験を通じて感想，気づいたことはありますか．

インタビュー結果の中から主な回答内容を回答番号とともに以下にまとめる．

行動者の回答

- 大体のセキュリティはすべて自動化するように設定済みである．ただ，バックアップのつぶやきを見た際に，バックアップに関しては自分でやらなければいけないものなので実行した．バックアップのやり方については自分で確立したやり方があるため，URL を特別見るようなことは行わなかった（A3-1）．
- 何気なく Twitter を見ていたときに，目についたのでなんとなく URL をクリックしようと思った．その URL の内容を見て，セキュリティについて，ふだんは特に気にしていないので，そのツイートを見たことをきっかけにやろうと思った（A4-1）．
- 知り合いもやっているのであれば，「仮に被害に合っても自分だけでない」，「何か問題があった場合もすぐに修正がくるだろう」という思いがあった（A1-3, A4-3）．
- 知り合いが珍しい話題であるセキュリティについてツ

イートしていると特別に呼びかけているような意図を感じた（A2-3）．
- 「簡単です」や「手軽です」といった文章で，かつ短い期間に多く存在すると，感染してスパムを拡散してしまっているように見えて，かえって怪しかった（A3-3）．
- 知り合いだからふだんのコミュニケーションに混じって，情報が得られてよかった．ただ，情報の出どころがとても気になる．URL 内容の専門性の高さがとても良いと思ったので，URL 先が専門的な機関だということが URL の段階から分かると良いと思った（A5-3）．

未行動者の回答
- Twitter で流れてきても特に感動がない話題で，Windows Update すればいいだけの話なので，とりわけ新しい情報がない（N1-1）．
- やらなかった一番大きい理由はとにかく面倒くさいと感じたから．次いで必要ないと思ったから（N2-1）．
- 面倒くさいことがやらなかった最も大きな理由．よく読むと面倒くさくないことが分かるが，そのよく読むこと自体が面倒くさく，なかなかその一歩が踏み出せない（N3-1）．
- ネタや面白い内容でないと読もうと思わない（N4-1）．
- 対象のツイートは十分に見たが，行動が面倒くさいと感じたため行わなかった（N5-1）．
- もっと大量のユーザが行動していたら，自分もやらないといけないと感じたと思う（N2-2）．
- 簡単であること，よくまとまっていることが分かる形で URL へと誘導されるとその最初の一歩が進み，一気に行動の改善にまでつながるかもしれない（N3-2）．
- Twitter で互いに興味を持ち合っている者同士のつながりを利用するのであれば，もっと踏み込んだコミュニケーションがあれば良い（N4-2）．
- 「その行動がとても求められているから頑張って送信しました！」っていう姿勢が見えると良い（N5-2）．
- 情報の信頼度より，情報の面白さのほうが Twitter では拡散力があるから，リツイート件数が多いと，信頼性が高いのか面白いネタなのか，その判断ができない（N1-3）．

6. 考察

情報セキュリティ行動を実施したという身近な人からのツイートを受信することの有効性と受容性を質問紙調査と構造化インタビューの結果から考察する．また，未行動者に対するインタビューから得られた改善に関する知見を中心にまとめる．さらに，長期的な運用によって解決すべき課題を述べる．

6.1 ツイートを受信することの有効性

被験者がとった行動の集計結果（図 6）より，Securitter のツイートを見た被験者 40 名中 30 名が参照 URL を確認し，14 名が詳細に参照 URL 先の IPA による記事を読み，さらに 5 名の被験者が実際に情報セキュリティ行動を実施したことが分かる．この 5 名の行動者は，ふだんの態度（図 8）として，当該の情報セキュリティ行動を「よく行う」および「比較的行う」ユーザであるが，行動者へのインタビュー（A4-1）により，ツイートを受信することが実際の情報セキュリティ行動に結びついた事例が確認できた．一方，1 週間の模擬運用期間において，Securitter のツイート受信を契機とした情報セキュリティ行動を 42 名が起こさなかった．被験者の情報セキュリティに対するふだんの態度（図 8）として，「セキュリティパッチの更新」をまったく行わない者が約 4 割存在し，今回の被験者集団が 1 章で紹介した IPA の調査結果 [2] と合致する一般的な集団であることを示している．未行動者が行動を起こさない理由などについては，6.3 節で議論する．

また，IPA から情報を取得する習慣がよくあると回答した被験者は 47 名中 1 名（図 8）のみであったが，1 週間で 14 名の被験者をセキュリティ知識へアクセスさせる効果を確認できた．

さらに，行動者へのインタビュー（A1-3，A4-3，A2-3，A5-3）により，知人が呼びかけていることが効果的であることが確認できている．行動者の中には，Securitter のツイート自体は見ているが，参照 URL は見なかった者もいた．その行動者は，インタビュー（A3-1）によりふだんからセキュリティ意識が高く，参照 URL からセキュリティの知識を得る必要がないことが分かるが，ツイートを見たことがきっかけとなり行動したと回答している．以上より，情報セキュリティに対する意識が高いユーザに対しても効果がある可能性が示された．

6.2 ツイートを受信することの受容性

Securitter の受信希望回答（図 7）より，47 名の被験者中 28 名が Securitter を使って情報を受信したいと回答しており，過半数に受け入れてもらえる結果となった．インタビュー（A4-1，A5-3）より，Twitter によるコミュニケーションが手軽であると考えた被験者がおり，この手軽さが受容性を高めたと考えられる．

一方，インタビュー（N4-1）から読み取れるように，ソーシャルネットワークとしての Twitter ネットワークが，情報セキュリティ行動を公表する場として，ふさわしい場であるかという議論も必要と考えられる．本稿では，身近な人が情報セキュリティ行動を実施しているという情報を共有できれば，自身に関連する情報セキュリティ行動に気づき，実際の行動に結びつけることができるのではないかという発想を具体化する場として，ゆるいコミュニケーショ

ンを実現するソーシャルメディアという観点から，Twitterを選択した．今後，社会活動に協調したネットワークサービスの進展にともない，さらなる議論が必要と考える．

6.3 情報セキュリティ行動を喚起するための知見

未行動者のインタビュー（N2-1，N3-1，N5-1）より，行動しなかった理由として最も大きかったものが，面倒くさいと思ったことだと分かる．既存のタイムライン上に情報が載ってくるSecuritterは受信者に新たなコストを要求しないため，他の情報提供手段より優位であると考えられるが，情報セキュリティ行動モデルでも明らかであるように，コスト感の影響が顕著であった．同様に，インタビュー（N1-1，N1-3，N4-1）より，被験者の関心や信頼を高めることができなかったことも示されている．Twitter自身が手軽な情報発信メディアであり，それを読むことに面白さのみを求めるユーザに対しては，他のメディアなどを活用した動機づけも必要と考えられる．

また，行動者のインタビュー（A3-3）からも，コスト感を低減させる目的で作成した文章が怪しく感じたという指摘もある．模擬運用で用いた文章は情報セキュリティ行動モデルを参考として作成したが，文章については今後さらに検討が必要であり，インタビューから得られた以下の意見が参考となる．

- 簡潔にURLへ誘導できること（N3-2）
- 行動者（発信者）の意図が感じられること（N5-2）
- 共感や関心を持てるコミュニケーションがとれること（N4-2）

ユーザ同士がコミュニケーションをとることで，ツイート文の怪しさの低減や，分かりやすい情報源への誘導，手段の直接教授などが考えられ，コミュニケーション促進機能の追加など長期的な運用時の工夫が示唆されている．

さらに，インタビュー（N2-2）より，Securitter提案時に検討した「実行者割合認知」が作用しており，発信者数を増加させることを示唆している．これについてはSecuritterを普及させることによって解決できる．普及に際しては，発信者の立場での検討も必要である．

6.4 長期的運用によって解決すべき課題

Securitterは，ソーシャルネットワークにおける集合的防護動機理論に着目し，集団内での相互監視や相互認知といった社会心理的側面に働きかけるものである．ここで，集団内である身近な人からのツイートと集団外であるIPAなどの公的な組織からのツイート[15], [16], [17]とでは，情報セキュリティ行動に対する態度変容に差が生じることが考えられる．質的な評価にとどまるが，前述の行動者へのインタビュー（A1-3，A4-3，A2-3，A5-3）では，集団内である知人が呼びかけている効果が確認できている．しかし，14名の被験者をセキュリティ知識へアクセスさせた要因や5名の被験者を情報セキュリティ行動に導いた要因が，Securitterの効果によるものなのか，単にセキュリティ情報に触れる機会が増した効果によるものなのかを区別するための量的な評価は十分ではない．

これについて，ゲティノンとロバートソンによるマーケティング論的普及モデルでは，社会システム内の人びとが同類的であるほど普及の速度は速くなり，最大浸透水準も高くなるという命題を示しており[18]，集団内の身近なツイートがより効果が高いという仮説が考えられる．また，集合的防護動機理論より，集団内外にかかわらず同じ情報でもより多くの人から受信することで行動が促されるという仮説も考えられる．これらの仮説の検証には，長期的にシステムを運用してユーザのフォロー数やフォロー相手との関係，ツイートの閲覧回数なども含めて分析する必要があると考えている．

発信者と受信者の信頼関係は，現実のつながりと，Securitterを含むTwitterにおけるつながりを観察する必要がある．被験者実験の模擬運用では，サークルのリーダ的存在である3名が発信者であるが，Twitterネットワークはこのような単純な形態だけとは限らないので，長期的なシステム運用を行い，発信者と受信者の関係も含めて評価していくべきである．

また，受信者の行動として，Twitterの投稿をリアルタイムに必ず見るものとは限らず，まとめて見る場合も考えられる．被験者実験の模擬運用では，同じ行動についてツイートの文章を変えて9回ツイートしている．さらに，ツイートする時間帯もランダムになるように設定している．このようにより多くのユーザが受信できるように工夫しているが，情報の受信回数や時間帯については，むしろユーザの行動に依存する部分が大きいと考えられる．長期的なシステム運用を行って，ユーザタイプ別の評価も必要であると考える．

7. おわりに

本稿では，一般ユーザへの情報セキュリティ行動を促す新手法の検討を行った．情報セキュリティ行動モデルと，集合的防護動機理論に着目し，より身近な一般ユーザ間で情報セキュリティ行動を喚起しあうこと，実行者割合認知の観点に基づき実際に情報セキュリティ行動を実施したことを共有することが有効であると考え，Twitterを用いて情報共有する手法Securitterを提案した．

Securitterの実現においては，情報発信を円滑に行うために，常駐による情報セキュリティ行動の監視と，共有するメッセージの自動生成の2つの特徴を持つアプリケーションであるSecuritterクライアントの実装を行った．

さらに，3名の実験協力者（発信者）と47名の被験者（受信者）による被験者実験を行い，質問紙調査の結果から，情報セキュリティ行動の実施に関するツイートを受信

することの有効性と受容性を確認した．また，構造化インタビューの結果より，Twitter の手軽さや，知人の呼びかけが有効であったことが示された．この結果より，本稿で提案する情報共有手法 Securitter によるツイートを受信することによって，一般ユーザの情報セキュリティ行動に結びつけることができると考えられる．

今後は，提案した手法について発信者の立場での検討や自動生成されるメッセージ内容の検討を行うことで，より効果的な情報セキュリティ行動の促進が実現できると考える．

参考文献

[1] IPA：2013 年版 10 大脅威～身近に忍び寄る脅威～，IPA（オンライン），入手先 ⟨http://http://www.ipa.go.jp/security/vuln/documents/10threats2013.pdf⟩（参照 2013-04-02）．

[2] IPA：2012 年度情報セキュリティの脅威に対する意識調査報告書，IPA（オンライン），入手先 ⟨http://www.ipa.go.jp/security/fy24/reports/ishiki/documents/2012_ishiki_report.pdf⟩（参照 2013-04-02）．

[3] 島成 佳，高木大資，吉開範章ほか：情報セキュリティ対策の推進を促す説得コミュニケーションによる態度変容の調査報告，暗号と情報セキュリティシンポジウム，SCIS2011, No.2F2-1, pp.1–8 (2011).

[4] 菅野泰子，寺田真敏，山田安秀ほか：企業の情報セキュリティ対策におけるモチベーションの構造に関する考察，情報処理学会論文誌，Vol.50, No.9, pp.2193–2206 (2009).

[5] 諏訪博彦，原 賢，関 良明：情報セキュリティ行動モデルの構築—人はなぜセキュリティ行動をしないのか，情報処理学会論文誌，Vol.53, No.9, pp.2204–2212 (2012).

[6] 青柳西蔵，岡村智明ほか：ゆるいコミュニケーションによる環境配慮行動促進手法の提案，ヒューマンインタフェースシンポジウム論文集，No.1435 (2011).

[7] 通山和裕，西尾信彦：公共空間における周囲の第三者とのコミュニケーション支援のための自己プレゼンス，情報処理学会シンポジウムシリーズ，No.1, pp.1305–1313 (2007).

[8] DAC：ソーシャルメディアのユーザー調査，DAC（オンライン），入手先 ⟨http://www.advertimes.com/20110630/article21585/⟩（参照 2013-03-08）．

[9] 村本由紀子：集合と集団状態の曖昧な境界：早朝の公園で見出される多様なアイデンティティ，社会心理学研究，Vol.12, No.2, pp.113–124 (1996).

[10] 島本大輔，大山恵弘，米澤明憲：System service 監視による windows 向け異常検知システム機構，情報処理学会論文誌，Vol.47, No.12, pp.420–429 (2006).

[11] 越智貴夫, 小島孝夫, 外川政夫, 板倉征男：ホットデジタルフォレンジックによるインシデント検知方法の提案（セッション a-10：検知），情報処理学会研究報告，Vol.2008, No.21, pp.267–272 (2008).

[12] 小崎真寛，芝口誠仁，中山佑輝，岡田謙一：USB メモリを介したファイル移動の監視とそのログ視覚化，情報処理学会研究報告，Vol.2010, No.4, pp.1–8 (2010).

[13] 日本社会心理学会：日本社会心理学会倫理綱領，日本社会心理学会（オンライン），入手先 ⟨http://www.socialpsychology.jp/kitei/kitei02.html⟩（参照 2013-03-08）．

[14] IPA：重要なセキュリティ情報一覧，IPA（オンライン），入手先 ⟨http://www.ipa.go.jp/security/announce/alert.html⟩（参照 2013-03-08）．

[15] IPA 公式アカウント「緊急対策情報」（オンライン），入手先 ⟨https://twitter.com/ICATalerts/⟩（参照 2013-07-10）．

[16] IPA 公式アカウント「脆弱性対策情報」（オンライン），入手先 ⟨https://twitter.com/JVNiPedia⟩（参照 2013-07-10）．

[17] IPA 公式アカウント「ソフトウェアバージョン更新情報」（オンライン），入手先 ⟨https://twitter.com/MyJVN⟩（参照 2013-07-10）．

[18] 宇野善康：《普及学》講義，有斐閣 (1990).

原 賢

2011 年電気通信大学電気通信学部卒業．2013 年電気通信大学大学院情報システム学研究科博士前期課程修了．同年 NTT コムウェア株式会社入社．

三浦 大樹

2011 年電気通信大学電気通信学部卒業．2013 年電気通信大学大学院情報システム学研究科博士前期課程修了．同年日本電信電話株式会社入社．現在，NTT ソフトウェアイノベーションセンタ所属．

関 良明 （正会員）

1985 年東北大学工学部通信工学科卒業．同年日本電信電話株式会社入社．以来，グループウェア，オフィスシステム，情報セキュリティの研究開発に従事．博士（情報科学，東北大学）．電気通信大学大学院情報システム学研究科客員准教授．現在，NTT セキュアプラットフォーム研究所所属．電子情報通信学会シニア会員．社会情報学会，ACM，IEEE 各会員．

諏訪 博彦 （正会員）

1998 年群馬大学社会情報学部卒業．2006 年電気通信大学大学院情報システム学研究科博士後期課程修了．博士（学術）．現在，電気通信大学大学院情報システム学研究科研究員．情報処理学会・GN 研究会運営委員，社会情報学会および経営情報学会・研究部会幹事．ソーシャルメディア，リスク対策等の研究に従事．