Vol.2015-MBL-74 No.41
Vol.2015-UBI-45 No.41
2015/3/3

今来たさん：SNSを利用した大学研究室向けスマートロックシステム

大野 敬子[1,a)]　椎尾 一郎[1,b)]

概要：
本研究では，電子錠と SNS を利用したスマートロックシステム “今来たさん” を提案する．今来たさんは，大学研究室での使用を想定した入室管理システムである．現在，著者の所属する研究室で 2 年半以上稼働している．本システムでは，電子錠を用い，解錠のための認証方法に暗証番号を採用した．一般に，運用の容易な認証方法ではセキュリティが弱く，運用の煩雑な認証方法ではセキュリティが強いというように認証方法とセキュリティの間にはトレードオフの関係があるといえる．そこで，暗証番号のように容易な認証方法であっても十分なセキュリティを確保することを目指し，SNS の 1 つである Twitter を利用して，ユーザ全員で研究室のドアを見張る効果が得られるような実装を行った．具体的には，ドアの解錠が行われた際に解錠を行ったユーザの Twitter アカウントをツイートする，深夜に研究室のドアが開いているとツイートする等である．これにより，ユーザが家にいながら研究室の不審な様子に気づけるようにした．この監視効果については，実験を行い，ある程度の効果があることがわかった．また，ユーザの印象評価も行い，本システムが大学研究室の入室管理システムとして受け入れられていることがわかった．本論文では，今来たさんを提案し，実装，運用結果，評価，今後の課題について述べる．

Imakita-san: smart lock system using SNS for a university laboratory

Oono Keiko[1,a)]　Siio Itiro[1,b)]

Abstract:
We propose the smart lock system named “Imakita-san” that utilizes electric lock and SNS. Imakita-san is an entry management system for a university laboratory. We have run it in our laboratory over 2 and a half years. This system uses electronic lock and a user can unlock the door by typing personal identification number (PIN). Generally speaking, ease of use authentication methods have low security and complex methods have high security. As stated above, there is a trade-off between ease-of-use and security. Then, aiming to get enough security in spite of authentication having easy operation like PIN, we implement a system using Twitter (one of SNS) to get effect virtually watching a door of a laboratory by the SNS community members. Specifically, the system tweets the Twitter account of a user who owns the PIN when the door is unlocked. The system also tweets warning if the door is kept open in midnight. This enables users to perceive suspicious of a laboratory in their home. We tested this function and found that it has a certain level of effect. In addition to this, we took some questionnaire to users and found that the system has been acceptable as an entry management system for a university laboratory.

1. はじめに

現在，コンピュータを利用した入室管理システムが広く普及している．しかしながら，それらを大学研究室で運用したいと考えた時に，認証方法が煩わしい，セキュリティが弱い，運用コストが高いなどの問題がある．そこで，本論文では，そのような問題を解決することを目指した大学研究室向け入室管理システム “今来たさん” を提案する．

一般に，IC カードを用いた認証や生体認証など運用が煩

[1] お茶の水女子大学
Ochanomizu University
[a)] kktn@is.ocha.ac.jp
[b)] siio@is.ocha.ac.jp

雑な認証方法はセキュリティが強く，暗証番号による認証など運用の容易な認証方法では，セキュリティが弱い．このように，運用の容易さとセキュリティ強度の間には，トレードオフの関係があると言える．そこで，本システムでは，認証方法として暗証番号という運用の容易な認証方法を用いながら，容易な認証により欠けてしまったセキュリティを補うために，SNS の 1 つである Twitter[*1]を利用する．SNS を利用することにより，ユーザ全員で SNS を通してドアを監視することを可能にすると考えた．以降の節で，実装，運用結果，評価，今後の課題について述べる．

2. 今来たさん

今来たさんは，大学研究室での利用を想定した入室管理システムである．本システムでは，研究室ドアに電気錠を設置し，ドア付近に設置したテンキーボードからの暗証番号入力により電気錠の解錠を行う．認証方法として数桁程度の簡単な暗証番号を用いているが，入力の際に番号を背後から盗み見られる可能性もあり，セキュリティが不十分である．そこで，十分なセキュリティを確保するために Twitter による見守りを併用する．具体的には，誰が解錠を行ったのか，ドアの開閉状態等をシステムが Twitter へ投稿する．そのツイート[*2]をユーザが見ることによって，監視効果が生まれることを期待した．また，大学研究室での利用を想定しているため，ユーザ登録や暗証番号変更などに必要な手間を簡素化し，運用コストの低いシステムを目指した．本システムの設置場所である大学研究室入り口の外観を図 1 に示す．

2.1 システム構成

本システムを実現するために，図 3 のような実装をした．Raspberry Pi[*3]をシステムのメインに用いている（図 2）．電気錠には，美和ロック株式会社[*4]の AUTA を用いた．

図 1 今来たさんの設置場所の外観

*1 https://twitter.com/
*2 Twitter に投稿された記事
*3 http://www.raspberrypi.org/
*4 http://www.miwa-lock.co.jp/

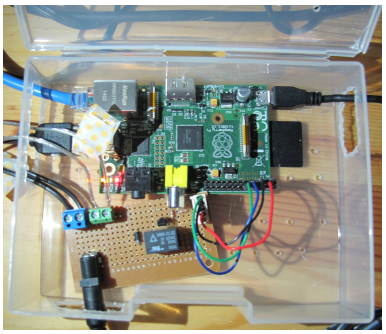

図 2 システム内の Raspberry Pi の様子

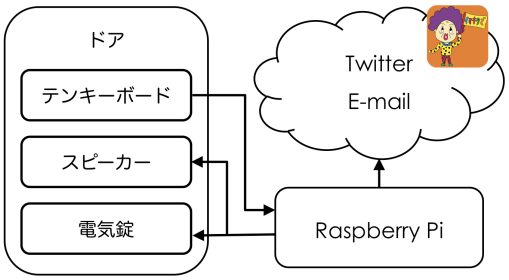

図 3 システム構成

ユーザがテンキーボードで暗証番号を入力すると，Raspberry Pi が暗証番号を受け取る．Raspberry Pi では，暗証番号が正しいかどうか確認し，その結果をスピーカーを通して音声でフィードバックする．暗証番号が正しい場合，電気錠を解錠し，スピーカーから解錠したことを伝える音声を流す．同時に，誰が解錠したのかツイートする．暗証番号を間違えた場合，スピーカーから解錠に失敗したことを伝える音声を流す．連続して 10 回暗証番号を間違えた場合，スピーカーから連続で 10 回間違えたことを伝える音声を流し，200 秒間システムをロックする．同時に，警告用のツイートと研究室のメーリングリスト等へのメールの送信を行う．なお施錠は，ドアを閉めると自動的に行われる．

暗証番号は，Raspberry Pi 上に置いたデータベースに記録されている．データベースには，暗証番号の他に，ユーザの Twitter アカウント，ユーザが研究室で使用する端末の MAC アドレス等を記録している．

3. 入室管理システムにおける課題と解決策

本節では，大学研究室で入室管理システムを運営するにあたって課題となる点とその解決策について述べる．

3.1 認証方法

現在，多くの入室管理システムでは，認証に IC カードが用いられている．企業では，IC カードを名札代わりに携帯することが義務付けられている場合が多く，IC カードを用いた認証が受け入れられやすい．著者らの大学でも IC

カードの学生証を使用しているが，これを名札として常時携帯する規則や習慣は無い．そこで，一時的な退室の度にICカードを携帯することをユーザに強いることに対して同意が得られないと考えた．最近では，スマートフォンを利用して解錠を行うスマートロックの開発も盛んである [1]．これに対しても，一時的な退出のたびにスマートフォンの携帯を義務付けることは，ICカードの場合と同様に煩わしく感じられると考えた．指紋や静脈などの生体認証を利用すれば，カードや機器を携帯しなくても認証が可能ではあるものの，ユーザの生体情報を取得して登録管理する手間が必要である．本システムでも，指紋認証デバイスを過去に利用したことがあったが，毎年入れ替わりのあるユーザに対する登録と管理の手間が面倒で利用を中止した経緯がある．

一方，利用者ごとに設定した暗証番号による認証は，何かを携帯する必要がなく解錠にかかる手間も少ないことから，大学研究室で用いる入室管理システムの認証方法として適している．そこで，本システムでは，暗証番号による認証を採用した．現在の実装では，ユーザが任意に選んだ7桁以上の番号をユーザごとの暗証番号として使用している．桁数を大きくしてセキュリティを確保すると同時に，電話番号や生年月日と同程度の桁数にすることで覚えやすい暗証番号となると考えた．

しかしながら，暗証番号による認証は，ICカードによる認証や生体認証に比べ，類推が可能であり，入力の際に番号を盗み見られる可能性があることから，不正な解錠に対して脆弱である．そこで，次節で述べるような脆弱性を補う手法を併用した．

3.2 セキュリティ

入室管理システムにおいて，セキュリティを高く保つことは重要である．ICカードによる認証や生体認証は，運用が煩雑であるが，セキュリティが強いと言える．一方で，暗証番号などの運用が容易な認証方法は，セキュリティが弱い．このように，認証方法とセキュリティの強度にはトレードオフの関係があると言える．

そこで本研究では，暗証番号などの認証や運用が容易な認証方法のセキュリティ強化を図るために，SNSの利用を提案する．古い牧歌的な社会では，不審者や不審な行動が地域住民の監視にさらされることで，住居に施錠しなくても安全な生活を実現できた．SNSを活用すれば，SNS上で繋がった人々の協力により，同様のセキュリティ強化効果が得られると考えられる．

本システムでは，SNSの1つであるTwitterを利用する．ユーザが普段から使用しているTwitterをセキュリティ強化に用いることで，本システムのために新しい習慣を身につけることを必要とせず，受け入れやすいと考えた．本システムでは，ドアが解錠されたことを，その部屋を利用する人々に向けてツイートする．このように，グループメンバーが普段から使用しているSNSサービスを利用してドアの状況を伝えることで，メンバーがドアを仮想的に監視しているような効果が生まれると考える．なお，本システムがツイートするTwitterアカウントは非公開に設定し，登録ユーザのみが見られるようにした．このような手法は，実世界のドアのみならず，共有サーバへのアクセスのような，サイバー空間にある共有資源のセキュリティ確保にも有効だと考えている．

図 4 webからTwitterを見た時の通知の様子．自分が参照されたツイートが1件あることを通知している．

ドアが解錠された時，図5のようなツイートが行われる．本システムでは，各ユーザに対して固有の暗証番号を用意しているため，誰の暗証番号で解錠されたのか識別できる．そこで，解錠される度に解錠したユーザのTwitterアカウントを含めたツイートを行う．Twitterでは，“@”の後に任意のユーザのTwitterアカウントを書くと，書かれたユーザがそのツイートに気づきやすくなるように，書かれたユーザに対して通知される（図4）．以下，このようなツイートを“ユーザを参照したツイート”と呼ぶ．本システムでもその機能を利用することで，不審な解錠に気づきやすくなるようにした．例えば，自分は自宅にいるにも関わらず，自分のTwitterアカウントが含まれているツイートが行われたら，それは不正な解錠だと気づくことができる．解錠された時のツイートでは，日時を文頭に記載している．これは，Twitterの決まりとして，同じ内容のツイートを連続して投稿できないことと，文頭が@となるツイートは一部のユーザのタイムライン[*5]にしか表示されないことがあり，これらを回避するためである．2回連続で同一ユーザが解錠を行う可能性は十分にありえるが，同じ内容のツイートを連続して投稿できないため，日時のない『@kktn1109が来たで〜』というようなツイートにしてしまうと，2回目の解錠に関しては，ツイートに失敗し，監視することができないのである．また，今来たさんの通常のツイートは，今来たさんをフォロー[*6]している全ユーザのタイムラインに表示されるが，ツイートの文頭に@を書いてしまうと，今来たさんと@の後に続くアカウントを持つユーザの双方をフォローしているユーザのタイムラインにしか表示されなくなるのである．このことから監視効果が弱くなることが懸念される．そこで，以上の2点の問題

[*5] ホーム画面にあるツイートのログ．ユーザ自身のツイートとユーザが“フォロー”を行ったユーザのツイートが表示される．
[*6] フォローを行うと，タイムラインにそのユーザのツイートが表示されるようになる．公開アカウントの場合，自由にフォローできるが，非公開アカウントの場合，フォローリクエストを送り，アカウント所有者に承認される必要がある．

図 5 解錠された時に行われるツイートの一例

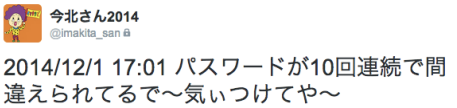

図 6 暗証番号が 10 回間違えられた時に行われるツイート

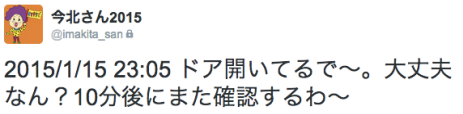

図 7 22 時 00 分から 6 時 59 分の間にドアが開いていると行われるツイート

を解決するために解錠された時のツイートは，文頭に日時を入れるようにした．次節で紹介する登録／削除を行った際のツイートでもこの工夫を用いた．

10 回暗証番号を間違えた時，200 秒間システムをロックする．そして，危険を知らせるため，図 6 のようなツイートが行われる．同時に大学研究室のメーリングリストや本システム管理者へメールが送られる．

22 時 00 分から 6 時 59 分の間にドアが開いていると，図 7 のようなツイートが行われる．ドアの状態は 10 分に 1 回確認し，ドアが開いているとその度にツイートを行う．著者の所属する研究室では，ドアを閉め忘れて帰ることが数回あったため，閉め忘れを防ぐためにこの機能を用意した．

3.3 運用にかかるコスト

大学研究室では，入室管理システムを運用するために多額のコストを払えない．そのため，運用にかかるコストをできるだけ抑えたシステムを利用するべきである．入室管理システムの運用にかかるコストとして，ユーザの登録／削除，鍵をなくした場合の対応，一時ユーザへの対応があげられる．

本システムでは，登録／削除に web ページを利用する．用意した web ページは，研究室のローカルネットワークからのみアクセスできるようにし，ユーザ自身が登録／削除を行えるようにする．認証方法として，IC カードや生体情報を採用した場合，登録の際に，専用の読み取り機器とこれを使用した作業が必要となるが，暗証番号を採用したことで，web ページから簡単に登録を行うことができる．登録に必要な情報は，Twitter のアカウント名とドアを開ける時に使用する暗証番号のみである．ユーザ登録が行われた時には，図 8 のようなツイートが行われる．前小節で述べたように，@を文頭に置いたツイートでは，今来たさんと@の後に続くアカウントを持つユーザの双方をフォローしているユーザーのタイムラインにしか表示されない．これでは，監視効果が弱いため，文頭に “.” を置くことで，今来たさんをフォローする全ユーザのタイムラインに表示されるようにした．

図 8 ユーザ登録が行われた時に行われるツイートの一例

図 9 ユーザが削除された時に行われるツイートの一例

研究室のローカルネットワークへのアクセス権限を持つ人が，解錠の権限を必ずしも持っているとは限らない．例えば，外部からの来客が研究室のローカルネットワークを使用することがあるが，その客に解錠の権限を与えるべきではない．しかし，ローカルネットワークにアクセスできるため，web ページからユーザ登録を行えてしまう．そこで，ユーザ登録に使用できる Twitter アカウントは，本システムの Twitter アカウントをフォローしている Twitter アカウントのみとした．本システムの Twitter アカウントは，非公開アカウントであるため，フォローをするためにはフォロー申請を送り，本システムの Twitter アカウントからその申請を許可する必要がある．そこで，解錠の権限を与えて良いユーザかどうかを人間によって判断できる．これは，管理者の手間となってしまうが，全てを自動化することは難しいと考えたため，この手法を採用した．

削除は，web ページから，全てのユーザが全てのユーザに対して行える．削除した時には，図 9 のようなツイートが行われる．ここでも，前述したように，今来たさんをフォローする全ユーザのタイムラインに表示されるように，文頭に “.” を置いた．

物理的なカードや鍵を使用した一般的な入室システムでは，鍵をなくした時の対応が面倒である．本システムでは，Twitter のダイレクトメッセージ機能[*7]を利用して，簡単に暗証番号を変更できる機能を搭載した．ユーザは，暗証番号を変更したい時に，本システムの Twitter アカウントに新しい暗証番号をダイレクトメッセージで伝える．本システムの Twitter アカウントは，メッセージを受信すると，メッセージを送信した Twitter アカウントと，送られてきた暗証番号を確認し，メッセージを送信した Twitter アカウントを持つユーザーの暗証番号を変更する．図 10 にその様子を示す．変更後，ユーザにパスワードを変更したことを伝えるメッセージを送信する．暗証番号変更の際に古いパスワードを必要としないため，暗証番号を忘れても問題無い．一時ユーザへの対応にもこの機能を利用できる．

[*7] Twitter 内で使えるメールのようなもの．ツイートと違い，他の人から内容を見られることがない．

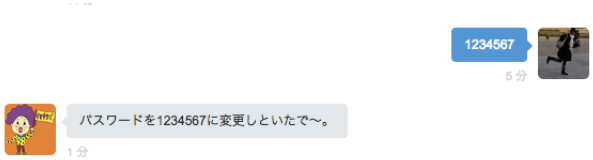

図 10 暗証番号を変更する様子

ツイートを行った日時	リプライ（返信）が来た日時	参照されたユーザ	最初に気づいたユーザ
2014/12/23 23:25	2014/12/23 23:43	実験者	J
2014/12/24 03:43	×	A	×
2014/12/24 06:14	×	B	×
2014/12/25 02:21	2014/12/25 12:23	C	C
2014/12/25 04:53	2014/12/25 08:06	D	J
2014/12/25 08:51	2014/12/25 10:28	E	F
2014/12/26 00:17	2014/12/26 00:18	×	N
2014/12/26 05:37	2014/12/26 13:38	F	F
2014/12/27 01:45	2014/12/27 01:52	G	G
2014/12/27 02:53	×	H	×
2014/12/27 08:12	2014/12/27 08:18	×	P
2014/12/27 23:46	2014/12/28 01:30	I	K
2014/12/28 00:57	2014/12/28 00:59	J	J
2014/12/28 07:11	2014/12/28 12:27	K	K
2014/12/29 01:18	2014/12/29 01:26	L	K
2014/12/29 04:23	2014/12/29 17:02	M	M
2014/12/29 06:43	×	N	×
2014/12/30 03:02	2014/12/30 05:57	O	O
2014/12/30 05:09	×	P	×
2014/12/30 07:46	×	×	×

図 11 ツイートが行われてからツイートに気づくまでの時間

一時的に，暗証番号を適当な数字に変更し，権限を付与したい者にその番号を伝え，権限をなくしたい時に元の暗証番号に戻すことで，一時ユーザに対応できる．

4. 運用実績と評価

著者の所属する研究室にて本システムを運用した結果と，SNS を利用したセキュリティ強化についての評価，印象評価の結果を述べる．

4.1 運用実績

本システムは，2012 年 6 月に運用を開始し，以後，2 年半以上稼働している．当初は，MacOSX の入った小型コンピュータを用いており，システムが停止することもあったが，現在は，Raspberry Pi に移行し，改良したことで，安定して動作している．

暗証番号による認証は様々な場面で使われていることもあり，新入生や留学生などの新しいユーザも戸惑うことなく解錠を行った．また，今までに使用を中止しているユーザがいないことを考えると，本システムは，大学研究室という環境に適した解錠方法であったことが伺える．

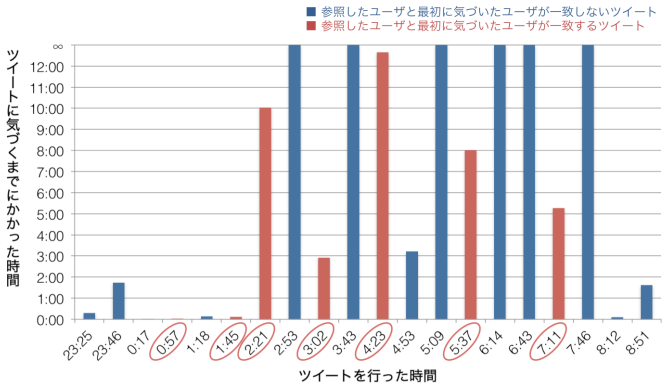

図 12 ツイートが行われてからツイートに気づくまでの時間．ツイート内で参照したユーザと最初に気づいたユーザが一致するツイートの横軸の値（ツイートを行った時間）を楕円で囲った．

質問＼評価	5	4	3	2	1
Q1	2人	6人	1人	4人	3人
Q2	0人	2人	1人	1人	12人
Q3	11人	6人	0人	0人	0人
Q4	2人	2人	0人	8人	4人
Q5	0人	11人	0人	4人	1人
Q6	4人	3人	7人	1人	1人

	回答人数	最頻値
Q1	16人	4
Q2	16人	1
Q3	17人	5
Q4	16人	2
Q5	16人	4
Q6	16人	3

図 13 本システムについてアンケートを行った結果

4.2 セキュリティ強化についての評価

本システムに，どれくらいの監視効果があるか調べるために実験を行った．2014 年 12 月 23 日から 2014 年 12 月 31 日にかけて，どれくらい本システムのツイートに気づくことができるのか調べた．被験者は，本システムの Twitter アカウントをフォローしている全員から著者の内の 1 人である実験者を抜いた 16 人である．大学にいる人が少ないと思われる 23 時 00 分から 8 時 59 分に，気づいたら応答するよう依頼するツイートを行った．ツイートは，任意の被験者 1 名もしくは実験者を参照したツイートを 17 回，ユーザを参照しないツイートを 3 回行った．ユーザを参照したツイートでは，全被験者と実験者を各 1 回ずつ参照した．結果は図 11，図 12 のようになる．23 時〜2 時は，起きている人が多いため，比較的早く気づかれることが多かったが，寝ている人の多い深夜は，ユーザを参照したツイートにも関わらず気づかれないことや気づくのに時間がかかることが多かった．この実験結果より，セキュリティとして足りない部分はあるものの，夜であってもある程度の監視効果があることが伺える．

4.3 印象評価

本システムのユーザ全員から著者の内の 1 人である実験者 1 名を除いた 17 名に対し，印象評価を行った．ユーザは，著者の所属する研究室の学生，学部教育研究協力員，教授である．ある程度の匿名性を保ちたいと考え，名前の

記入は求めず，学年のみ記入してもらった．質問は，7つ用意し，回答によって6つ又は7つ回答するようになっている．ただし，1名 Twitter を利用していないユーザがいるため，そのユーザは，Q3 のみ回答した．また，最後に，自由記述欄を設けた．結果を，図 13 に示す．以下に，質問内容と回答の詳細を示す．

Q1:“今来たさんのツイートを見て「◯◯が来たみたいだから研究室へ行こう」と思ったことがありますか？”
『よくある』,『時々ある』,『どちらとも言えない』,『あまりない』,『1 度もない』という五段階の回答を用意した．図 13 では，『よくある』を 5,『1 度もない』を 1 とした．この質問では，『よくある』または『時々ある』と答えたユーザが全体の半分となった．これにより，研究室に誰がいるのか，もしくは．誰かがいることを知ることが登校意欲の向上に繋がることが伺える．次節で，この結果を利用し，登校意欲の向上を目指した応用について述べる．

Q2:“今来たさんのツイートを見て「◯◯が来たみたいだから研究室へ行くのをやめよう」と思ったことがありますか？”
『よくある』,『時々ある』,『どちらとも言えない』,『あまりない』,『1 度もない』という五段階の回答を用意した．図 13 では，『よくある』を 5,『1 度もない』を 1 とした．この質問では，2 名のユーザが『時々ある』と答えており，少なからず，誰かがいることで登校意欲が減退するユーザがいることがわかる．後述のように，この 2 名は自分が研究室に来たことを他のメンバーに知らせたくないと考える傾向があり，人が居ない静かな環境で気兼ねなく過ごすことを望んでいると考えられる．

Q3:“解錠の際に暗証番号を入力することを煩わしく感じますか？”
『全く感じない』,『あまり感じない』,『どちらとも言えない』,『少し感じる』,『とても感じる』という五段階の回答を用意した．図 13 では，『全く感じない』を 5,『とても感じる』を 1 とした．この質問では，全員が『全く感じない』または『あまり感じない』という高評価をした．これは，本システムがユーザに負担をかけないシステムを目指していたことに対し，良い評価が得られたと言える．

Q4:“Twitter に今来たさんのツイートが流れてくることを邪魔だと感じることはありましたか？”
『よくある』,『時々ある』,『どちらとも言えない』,『あまりない』,『1 度もない』という五段階の回答を用意した．図 13 では，『よくある』を 5,『1 度もない』を 1 とした．『よくある』と答えたユーザが 2 名,『時々ある』と答えたユーザが 2 名いた．少数ではあるが，今来たさんのツイートを煩わしく感じているユーザがいることがわかる．これらのユーザには今来たさんによるツイートが負担になっていると言える．どのようなツイートが負担になっているのか調べるために,『よくある』又は『時々ある』と答えたユーザにのみ，次の質問を行った．

Q4-2:”上の質問に対して，よくある，時々あると答えた方に質問です．それは，どんなツイートですか？”
『「◯◯が来たで〜」というツイート』,『ドアが開いていることを知らせるツイート』,『意味のないツイート（ぶっ殺す！野菜高いっす！金ない！等)』,『デバッグ中のツイート(何度も「◯◯が来たで〜」が投稿される等)』,『その他』という 5 つの回答を用意し，複数選択可能とした．結果として，Q4 で『時々ある』と回答した 2 名は，この質問に対し,『意味のないツイート（ぶっ殺す！野菜高いっす！金ない！等)』と回答した．現在，今来たさんは，ユーザを楽しませる目的で，2 時間に 1 回程度，研究室メンバーが残した名言をツイートする．この 2 名の回答では，この機能によって行われるツイートを煩わしく感じるということであった．しかしながら，この 2 名から「種類が増えれば楽しいと思う」,「違う名言であれば良いと思う」という意見も得ているため，今後はツイートの内容や頻度について再考し，改善したい．Q4 に対して『よくある』という評価をした 2 名は，1 名が『ドアが開いていることを知らせるツイート』と『意味のないツイート（ぶっ殺す！野菜高いっす！金ない！等)』と回答しており，もう 1 名は,『「◯◯が来たで〜」というツイート』と回答している．煩わしいと感じているということは監視効果が高いとも言えるが，今後こういったユーザへの配慮を考える必要がある．

Q5:“今来たさんのツイートを見て不安に思ったことがありますか？”
『よくある』,『時々ある』,『どちらとも言えない』,『あまりない』,『一度もない』という五段階の回答を用意した．図 13 では，『よくある』を 5,『1 度もない』を 1 とした．この質問では,『時々ある』という評価が一番多く，ユーザが今来たさんのツイートを気にしていることがわかり，監視効果があることが伺える．実際に，「ドアが開いているというツイートがあり，不安に思ったので，その時は，Twitter をこまめに見るようにした．その後，研究室にいることをツイートしている人がいたため安心した.」という意見も聞かれた．しかしながら，現在のシステムでは，自発的に研究室の様子を確認することや不審者への対応を行うことができない．不審に思った時には，大学の警備員に連絡するようにしているが，これは，実行する際のハードルが高いように感じる．そこで，研究室の様子を確認する術や外部から不審者への対応を行える機能を用意する必要があると考える．今来たさんにリプライ[*8]を送ることによって，ドアの開閉状態，研究室の在室状況を知ることができるような応用を考えている．在室状況を得る方法については，次節で述べる．

Q6:“自分が解錠を行ったのが研究室のメンバーに知られ

[*8] 特定の人に宛てたツイート．この場合は，今来たさんに宛てたツイート

てしまうことについてどう思いますか？”
『嬉しい』,『少し嬉しい』,『どちらとも言えない』,『少し嫌だ』,『とても嫌だ』という五段階の回答を用意した．Q6では,『嬉しい』を 5,『とても嫌だ』を 1 とした．この質問に対して,『嬉しい』,『少し嬉しい』という高評価をしているユーザが半数近くいるが,『少し嫌だ』,『とても嫌だ』という低評価をするユーザも 2 名いる．高評価をするユーザにとって，本システムを使うメリットが解錠以外に存在しており，本システムの運用を続けるにあたって良い傾向と言える．しかしながら，低評価をするユーザへの配慮も必要だろう．プライバシー面の問題からこのような回答をしていると予想するため，解錠がされたことの伝え方を考慮する必要がある．この質問に対し低評価をした 2 名は，Q2 で『時々ある』と答えた 2 名，Q4 で『よくある』と答えた 2 名と一致している．

5. 登校意欲の向上を目指した応用

前節で述べたように，研究室の在室状況を知ることが登校意欲の向上に繋がる可能性がある．しかしながら現在のシステムで，研究室に在室していることを知ることができるのは，解錠を行ったユーザのみである．昼間の人が多い時間帯は，ドアストッパーでドアを解放していることも多いため，その間に入室したユーザの情報は伝達されない．加えて，退室については，管理していないため，解錠を行ったユーザが研究室にいるのどうかを知ることは出来ない．

そこで在室状況の取得機能の実装を進めている．グループメンバーの登校頻度を可視化することによって，他者との共同作業を促進する研究が行われている [6]．本システムでは，現在の在室状況を SNS を通して伝えることにより，他者との共同作業やコミュニケーションの活性化を支援したい．

現在，大多数のユーザがスマートフォンやタブレット端末を通学の際に持ち歩いている．ユーザが研究室にいる時，ユーザのスマートフォンも研究室にあり，研究室から帰るときには，スマートフォンも研究室から出る．また，スマートフォンやタブレット端末を持ち歩かないユーザであっても，研究室に来た時に研究室に置いた自分の PC を起動し，帰宅する時に PC の電源を切って帰ると考えられる．これらの機器の多くは，研究室内のローカルネットワークに接続され DHCP サーバから IP アドレスを取得する．以上の状況を利用し，在室状況を，その MAC アドレスを利用して取得する機能の実装をすすめている．ユーザが所有している機器の MAC アドレスは，登録ページで本システムへの登録を行う際に，登録に使用した端末のものを取得する．また，登録ページでは，ログインして，登録した情報の変更を行えるマイページを用意しており，この時にもログインに使用した端末の MAC アドレスを同様に取得する．これらの MAC アドレスは，複数登録可能であり，マイページから削除することもできる．これを元に，数十分おきに IP アドレスが割り振られている MAC アドレスを調べることで，どの端末が起動しているかを調べることができ，その所有者の在室状況を取得できる．

6. 関連研究

研究室の行き先をツイートし，ドアの解錠を行うシステムとして, 川上らの研究がある [2]．これは IC カードを使ったシステムであった．また，近年，August Smart Lock[1] 等のスマートフォンを利用したスマートロックシステムの開発が盛んだが，本システムでは，何も持たずに解錠できるよう認証方法として暗証番号を採用した．入室管理システムとして，Tweeting Cat Door[3] がある．これは，認証に RFID を利用し，猫がドアを通る様子を，Twitter で知らせている．一方，様々なセンサを利用した家庭向けセキュリティシステムを Zhao らが提案している [4]．これは火事のような非常事態の検知も行っている．またユーザの負担にならない新しい認証方法も数多く提案されている．たとえば EpisoPass[5] ではユーザしか知らない地味な思い出を認証に使用することで，強いセキュリティを確立しようとしている．本研究では，ドアをスムーズに解錠出来るよう単純な暗証番号による認証を用いた．

7. まとめと今後の課題

本論文では，SNS の 1 つである Twitter を利用した大学研究室向けのスマートロックシステムを提案し，実装，運用結果，評価を述べた．本システムでは，監視効果を得る目的で Twitter を利用したが，実験，アンケートによりある程度の監視効果があることを確認した．

今後の課題として，不審に思った時にユーザが実際の状況を確認する術が少ないこと，不審者への対応策があまりないことがあげられる．また，登校意欲の向上を目指し，研究室の在室状況を伝える機能を加えたいと考えている．

参考文献

[1] August Smart Lock: http://august.com/
[2] 川上 あゆみ，水上 彩，塚田 浩二，椎尾 一郎: 人々の行動を手軽に共有する生活空間エージェント，ヒューマンインタフェースシンポジウム 2009 論文集，pp.613-616
[3] Tweeting Cat Door: https://sites.google.com/site/ioanghip/
[4] Zhao Yanbo, Ye Zhaohui: A Low Cost GSM/GPRS Based Wireless Home Security System IEEE Trans. on Consum. Electron. (Volume:54, Issue:2)
[5] 増井 俊之: EpisoPass: エピソード記憶にもとづくパスワード管理，インタラクティブシステムとソフトウェアに関するワークショップ 2013，pp. 109-114
[6] Huang Elaine M., MynattElizabeth D.: Semi-public Displays for Small, Co-located Groups, Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp.49-56