情報基礎実習 第 9 回

2014 年 6 月 19 日（木）、6 月 20 日（金）
担当教員：逸村裕、高久雅生
TF：池田光雪

今日まで、人間は様々な技術を発明しその生活を豊かなものとしてきた。特に 1990 年代に Web が実用化されてからは様々なサービスが次々と生まれ、私達の生活を驚くほど大きく変容させた。しかし、様々な技術がもたらしたものは良いことばかりではない。今回は Facebook や mixi などの SNS と、Twitter を初めとしたマイクロブログに焦点を当てセキュリティとプライバシーに関する諸問題を扱う。

1. 今回のキーワード

- セキュリティと利便性
- SNS とマイクロブログ
- プライバシー
- ソーシャルエンジニアリング

2. 情報セキュリティと利便性

情報セキュリティ（以下、セキュリティ）とは、情報に対し許可されたもののみがアクセスできる権限を持つこと（機密性）、処理方法が正確で完全であり、改竄され得ないこと（完全性）、権限を持つ者が必要な時に自由にアクセスできること（可用性）を全て維持することを指す。セキュリティを向上させるには様々な手法があるが、一般にセキュリティと利便性は二律背反の関係にあり、バランスを取ることが非常に大切である。

ここでは、自転車の盗難防止を例にセキュリティについて考える。**表 1** に示したように盗難対策にはいくつかの手法が考えられるが、盗難リスクを最小限に抑えつつ、かつ利便性を最大限に高める手法は存在しない。

表 1. 自転車の盗難対策とリスク・利便性の関係

盗難対策	盗難リスク	利便性
1. 施錠しない	高い ↓	高い ↑
2. ワイヤー錠をつける		
3. 複数の鍵をつける		
4. 自転車を利用しない	低い	低い

施錠しない場合、鍵を忘れて立ち往生するといった煩わしさからは解放される。しかし、盗難される危険性は飛躍的に高まる。ワイヤー錠をつければそのまま乗っていかれるという心配は若干軽減される。だが、ワイヤーカッターであれば一瞬で破壊が可能であり、あ

くまでも気休めにしかならない。複数の鍵をつければ破壊までの時間はかかるが、盗難される可能性が無くなることはない。また、ワイヤーカッターでは破壊が困難な鍵を使ったとしても、それらの鍵は総じて重く、普段持ち歩くには邪魔となる。なおどのような鍵をつけたとしても、建造物などと固定[1]しない場合、車を使って鍵がついたまま本体を持ち去られるという可能性もある。さらに言うならば、鍵を破壊しないと本体の持ち去りが困難なように施錠したとしても、サドルなどのパーツを盗まれることはありうる。

究極の盗難対策とは、自転車に乗らないことである。しかし、筑波大学において何らかの交通手段を持たないことは非常に不便である。仮に徒歩以外の交通手段を持たないとすれば、こと春日地区と中地区や南地区を何度も往復しなければならない 1 年次の履修計画に大きな影響を与えると考えられる。

この自転車の盗難対策の例から分かることは、セキュリティ全般に応用することが可能である。すなわち、完璧なセキュリティは存在せず、状況に応じてどのような対策を取るべきかは変わりうる。

コンピュータウィルスの対策のような、コンピューター一般についてのセキュリティについては「『情報システムを安心・安全に利用するために』の詳細な説明」[1]等でも広く扱っているため、今回は SNS やマイクロブログにおけるセキュリティについて考えていく。

3. SNS とマイクロブログ

ブログ（Blog）とは Web 上で公開する日記の一形態であり、Web ページの一種である。Web 上で Log を取るということから Weblog という用語が考案されたが、Blog はこの略語である。一般にブログではコメント機能や引用機能などが充実しており、単なる日記のみならずニュースの紹介やエッセイなども盛んに投稿されている。日本では 2002 年頃から急速に普及し、今日に至るまで盛んに活用されている。ブログ機能を提供している有名なサービスとしては、アメーバブログや livedoor Blog、Tumblr などがある。

SNS（Social Networking Service）とは、その名の通り社会的なネットワークを Web 上で構築するサービスのことである。SNS はブログ機能に加えプロフィール機能やメッセージの送受信機能がつき、より個人とその結びつきにサービスの重点が置かれている。mixi や Facebook が有名なサービスである。

マイクロブログとは投稿内容が短くなるような制約が課されたブログのことである。この制約により、一般的なブログに対しコミュニケーションが活発になりやすいという特長がある。Twitter が有名である。

これらの 3 つのサービス形態には明確な定義や境は存在せず、複数の要素を併せ持つサービスも多く存在する。また、これら全てを包括する用語としてソーシャルメディアがある。ソーシャルメディアは「Web 上に人格を形成する」特長を持つメディアであり、上記のブログや SNS、マイクロブログに加え掲示板や Wiki も含む。

各々のメディアの特性を考えると、とりわけ SNS やマイクロブログでは現実から遊離した人格ではなく、むしろ密接に結びついた人格を形成しやすいと言える。以降では、これ

---

[1] 俗に地球ロックと呼ばれる。自転車の施錠にあたってはやり方を覚えることをお勧めする

らのサービスに関する諸問題について扱う。

4. SNS・マイクロブログにおけるプライバシー

ソーシャルメディアは、従来の紙媒体の日記や生身でのコミュニケーションと比較すれば、Web の特性を全て併せ持っていると言える。この特性とは、「基本的に時間と場所に制約を受けない」「高速に拡散される」「原則としてオープンである」「一度拡散した情報を消しきることはほぼ不可能である」等である。ソーシャルメディアの利用にあたっては、これらの特性を強く意識する必要がある。

特に Twitter や Facebook といったサービスは拡散性が非常に強く、プライバシーの確保やデマといった諸問題がより浮き彫りとなった。サービス登場以前では決して表面化しなかったはずの陰口や告白が SNS やマイクロブログを介することにより衆目に晒され、問題となるケースが近年爆発的に増加している。典型的な例として、未成年による飲酒とその告白が挙げられる。ソーシャルメディアの利用にあたって、Web 上でのあらゆる発言は完全に秘匿されたものでは決して無く、広く公開されているものということを常に意識し、現実の本人との同定を回避することは難しいことを把握する必要がある。以降、4 章では SNS やマイクロブログでの個人同定に話を絞りその諸問題について考える。

4.1 不用意な公開

SNS やマイクロブログにおいては、一般に本人が投稿を行うため、その投稿内容には本人の趣味や趣向が反映されやすく、さらには本人しか知り得ないはずの情報であることがある。したがって、その投稿内容から投稿者を推定することが可能である。また、SNS やマイクロブログで公開した情報は半永久的に Web 上に残るため、推定に必要な情報は利用時間に比例して増えていく。加えて、多くの SNS やマイクロブログでは検索機能が充実しているため、第三者が情報を収集することは容易である。

また、多くの SNS では「友達の友達まで公開」とするような投稿が可能だが、「友達の友達」は一般に非常に広い範囲である。投稿範囲を制限しているつもりでも、実際にはほとんど制限されていない場合があることに留意すべきである。また、SNS などのサービスは「6 人の知り合いを介せば世界中の誰とでも知り合いになれる」という六次の隔たり仮説を下地にしている。実際に、2011 年に Facebook が行った調査によれば、Facebook 上の任意の 2 ユーザは平均 4.74 人の友達を介することで繋がるという結果が得られている[2]。

【課題 1】

友達として 100 ユーザを登録している人（a とする）が「友達の友達まで公開」という設定で SNS に投稿をした場合、その投稿は拡散などをせずとも**最大**何人の a 以外のユーザが閲覧可能かを計算し、計算過程とともに回答を記せ。ただし、a の友達（集合 B を作るとする）はそれぞれ a 以外に 120 人ずつ友達を持つとし、おのおのの 120 人のうち 60 人は常に B に属するユーザのうちただ 1 人と友達であり，残りの 60 人は常に B に属する複数のユーザと友達であるものとする。

【出席確認課題】

詳細は演習開始時に指示する。Lab2014-9.docx に回答を記載・印刷し、2 限開始時までに提出せよ。

【課題 2】

出席確認課題に取り組む前に考えたこと（課題の困難性や意気込みなど）と、実際に取り組んでみた手ごたえなどをそれぞれ詳しく記せ。

4.2 関連付けによる特定

本人は情報そのものを公開していなかったとしても、本人の断片的な投稿や、「友達」の情報から推測可能な場合が多々ある。たとえば Twitter においては任意の名前をつけてユーザをまとめる「リスト」という機能がある。まとめられた本人は一切個人が推測可能な情報を投稿していないとしても、知識情報・図書館学類生であることを公言している別のユーザが作成した「klis」というリストに入っていれば知識情報・図書館学類生だということが推測可能である。さらに、klis リストに入っているユーザの投稿時間や内容を見ることにより、さらに詳しい特定が可能である（「klis14」リストに入っているユーザを 1・2 クラスと 3・4 クラスに細分するなど）。また、SNS やマイクロブログにおいては現実での繋がりを Web 上でも再構成することが多いため、たとえば Twitter におけるフォロー・フォロワー関係を追うだけでもかなりの属性の絞り込みが可能である。これは論文においても示されており、ロサンゼルスとニューヨークの住民を対象とした実験では、フォロー、フォロワー関係のみから本人の位置を 8 割は特定可能[3]という結果が得られている。

4.3 設定の不備、バグ

SNS では投稿を閲覧可能なユーザを制限することが可能だが、Twitter でも「非公開ユーザ」になることで閲覧を許可したもののみに発言を見せることが可能である。しかし、これらのサービスはあくまでも人間が作成したものであり、その機密性は完全には保証されておらず、設定ミスやプログラムのバグで公に公開されてしまうことがあり得る。

過去の例では「『誰かの Facebook 非公開写真』を簡単に見れるバグ」[4]、「twitter の非公開リストが公開されるバグ」[5]などが存在した。

4.4 知らずのうちに公開

特に Facebook が有名だが、SNS やマイクロブログなどのサービスは様々な機能を試験的に取り入れ、ユーザの反応を見て機能の続投・廃止を決定することを盛んに行っている。この機能追加はプライバシーに関する事項についても例外ではなく、いつの間にか新しい機能が増え、その機能により情報が公開されているということも多々ある。

また、2013 年 6 月にはアメリカの国家安全保障局がテロ対策の一環として大手通信会社や IT 企業から通信記録を大量に収集していることが発覚したが、Facebook は NSA から半年間で約 1 万件の情報提供要請を受けたと明らかにしている[6]。

さらに、近年ではスマートフォン向けのインターネット電話、チャットアプリとして

LINE やカカオトーク、comm が流行している。しかし、comm は 2012 年時点では「当社は、すべての comm 会員記述情報を無償で複製その他あらゆる方法により利用し、また、第三者に利用させることができるものとします。」という規約を設けており、大きな問題となった[7]。これらのことから、サービス利用の際はまず利用規約を確認することが非常に大切であると言える。

【課題 3】

高速かつ安定的にサービスを提供するにはかなりの運営費が必要だが、ソーシャルメディア（Twitter、LINE、Wikipedia など）はほとんどが無料で利用できる。

基本的に使用料金がかからないソーシャルメディアを複数とりあげ、それらはなぜ利用者から直接料金を取らず運営できているかという観点から調査、考察せよ。

3.5 炎上

SNS やマイクロブログが開かれたものということを理解しないまま、これまでに述べた理由で犯罪行為や規約違反を公にして注目を集め批難が殺到、通報などが行われ、人生に多大な影響を及ぼすということがある。このことを俗に炎上と呼ぶ。特に学生においては未成年の飲酒や、カンニング行為を投稿した結果炎上する事例は非常に多い。たとえば、東工大におけるカンニング発覚[8]などが有名である。これは本学においても例外ではなく、2014 年 5 月にある学生が Twitter に「明日授業中人を殺すことを考えている」などと不用意な複数の投稿を行ったところ、その投稿を見た別の学生が警察に通報し、結果逮捕されたという事例があった[9]。この件は公開アカウントで投稿したということが問題というわけではなく、たとえ LINE のような非公開なサービスにおいてもその投稿内容を警察に通報され、逮捕に繋がった例は数多く存在する。

犯罪行為、及びそれの自慢をすることは論外だが、犯罪行為をしていると受け止められかねない投稿をすることは絶対に慎むこと。一度炎上してしまうとその流れを止めることは非常に困難であり、関係者にも大きな迷惑がかかる。

4. ソーシャルエンジニアリング

古来より、より強固で安全な暗号の考案とその解読は堂々巡りを続けて来た[10]。しかし近年では理想状態では理論上完全な安全性を誇る量子暗号が登場し、この問題に終止符が打たれたかのようにも思える。しかし、暗号を扱う者が人間である以上、かならずセキュリティの穴というものは存在する。極端な話、いくら通信ではその秘匿性が担保されていたとしても、本人が ID とパスワードを漏らしてしまうのであれば意味が無い。

ソーシャルエンジニアリングとは技術的な隙ではなく、人間が持つ隙につけ込んでセキュリティを破る手法全般を指す用語である。技術的なハッキング（クラッキング）と組み合わせることで、絶大な威力を持つ。

4.1 ソーシャルハッキング

ソーシャルハッキングとは、ソーシャルエンジニアリングのうちコンピュータに被害を

加えず ID とパスワードを入手してシステムに不正に侵入する手法を指す。

実害が及ばなかったが有名な例としては、日本の政治家である橋下徹が 2013 年 6 月 1 日に「スマイルプリキュア」と Twitter 上で発言したこと[11]が挙げられる。橋下によれば Twitter に認証済みの iPhone を放置していたところ、小学 1 年生の娘が勝手に操作して投稿したとされている。

【課題 4】

実習室で Word を使ってレポートを書いている途中トイレに行ったところ、他の受講生にレポートをコピーして先に提出され、剽窃の疑いを掛けられてしまった。この問題に対し、どうすべきだったかの対策を考え、答えよ。**ただし、自身が今後行うことがないような理想を書くのではなく、これから実践する、あるいは既にしている対策を書け**。なお、全学計算機システムではパソコンのロックはできない設定となっている。

4.2 ソーシャルエンジニアリング

ソーシャルエンジニアリングとは、人間の心理的な隙などを利用して、セキュリティを破る手法全般を指す。心理的な隙には権威（担当教員や学類長を名乗る）、好き嫌い（自分の好みのタイプや性格の人からの頼み）、お礼（あえて貸しを作り頼みを断りにくくする）、希少性（今限定や先着何名）などが挙げられる。狭義には、本人しか知らないはずの情報を断片的に集め、それらを駆使することであらゆる情報を引き出すという手法を指す。たとえば、Twitter のアカウントを乗っ取るために使われた手段が公開されている[12]（現時点では各サービスのセキュリティが強化されこの手段は使えない）。

電話を使ったソーシャルエンジニアリングについては、この技術に関してアメリカで最も有名だったケビン・ミトニックが著した『欺術』[13]が詳しい。

【課題 5】

あなたのメールアドレス（s14xxxxx@u.tsukuba.ac.jp）宛てに、差出人が lumely@slis.tsukuba.ac.jp である図 1 に示すようなメールが送られてきた。あなたであればどのように対処するか、およびその理由を詳しく述べよ。

4.3 フィッシング

フィッシングとは、Web サイトやメールを使った詐欺の一種である。たとえば、2011 年には AKB48 の前田敦子を装い 2,100 名を騙し、計 2 億 1000 万円をだまし取った事件[14]があった。SNS やマイクロブログで事細かな情報得ることが簡単になった今日、なりすましを行うことはかなり容易となっている。

セキュリティを考える上で、メールはしばしばハガキに例えられる。すなわち、ハガキの差出人は書こうと思えばいくらでも嘘を書けるように、メールも差出人情報をやろうと思えばいくらでも変えることができる。フィッシング詐欺の対策としては、メールの送信者表記や本文中のリンクは信用しないことが第一に挙げられる。

#このメールは情報基礎実習の受講生に BCC で一斉送信しています.
情報基礎実習受講生各位

情報基礎実習 TF の池田光雪です.

情報基礎実習第 9 回の追加課題として, セキュリティに対する意識と現状の設定を調査します。次の Web サイトのフォームから統一認証のパスワードを入力し、各質問に回答してください.
http://example.com/jk14/examine.htm

なお, パスワードの堅牢さ・脆弱さは成績には一切影響しません.

池田光雪(Ikeda Kosetsu)
筑波大学大学院 図書館情報メディア研究科
博士後期課程

図 1. 情報基礎実習受講生に届いたメール

4.4 SNS・マイクロブログにおけるソーシャルエンジニアリング

ソーシャルエンジニアリングでは、本人や同僚、友人などの「身内」であると装い巧みに情報を引き出す。この点ではフィッシングにおけるなりすましと似ているが、フィッシングが多くの人を一度に対象とする手法なことに対し、ソーシャルエンジニアリングは一般には特定の 1 ユーザを狙った手法であるという違いがある。

「身内」であるかの判定方法には、そのグループしか知らないはずの専門用語を知っている、ということがまず挙げられる。しかし、今日では多くの情報が Web 上では公開されているため、身内であるかのように振る舞うことは比較的容易である。たとえば、Twitter においては筑波大生でないにも関わらずあたかも筑波大生かと思うような、「エアつくば」というアカウントが多く存在する。また、「JKJ」「RanRan」「本学」などの用語を普段から呟いていればつくばの関係者だと錯覚する確率は非常に高い。

4.5 SNS・マイクロブログと生産性

SNS やマイクロブログといったサービスは Web 上で心地よさを感じさせる反面、学生の本分であるはずの勉学に悪影響を及ぼすという研究結果がある。アメリカの女子学生 483 名（平均年齢 18.1 歳）を対象とした研究によれば、Facebook や Twitter といったメディアが成績に悪影響を及ぼしたとしている[15]。大学での学びは自学自習にその本質がある。SNS やマイクロブログはその学びを助ける要因にも、時間を取り、学びを妨げる要因にもなりうる。どのような利用をするのかは各自の自由だが、サービスに流されることの無いよう節度とメリハリをもった利用をすることが望ましい。

5. マイクロブログにおける投稿

マイクロブログは気軽に利用できることが大きな利点の 1 つだが、この点は問題点にもなりうる。たとえば、投稿した内容を総合的に判断するとかなりの推測が可能になることは前述した通りだが、個々の投稿は断片的であるがゆえに投稿者の意図とは違った解釈がされる可能性がある。これにより、炎上に繋がる可能性がある。また、「筑波大学の 1 年生」と名乗り、それが事実であったとしてもそれは学部 1 年生とは限らず、修士 1 年生、さらには博士 1 年生という可能性もある。

しかし、誤解を与える恐れがないかを毎回入念に検証しているようではその意義が大幅に薄れる。マイクロブログを始めとしたソーシャルメディアの利用にあたっては、その長所と短所をよく理解した上で、節度を持った利用をすることが望ましい。

6. SNS・マイクロブログの活用

これまででは SNS・マイクロブログの負の側面を多く取り上げてきたが、当然これらには悪い面のみならず良い点もたくさんある。

たとえば図書館においても SNS やマイクロブログは広報の手段として活発に利用されている。特に Twitter では現状 200 以上の公式アカウントが存在し、様々な情報を発信している[16]。また就職活動において、とくに IT 関連であれば Facebook のアカウントを「必須」としている企業も少なくない。

2011 年の東日本大震災においては Twitter により人命が救われた例もある。ある被災者が電池切れ寸前の中、ロンドン在住の息子にメールを打ったところ、息子は Twitter に母の困窮を訴える投稿をした。その投稿内容は拡散によって日本の消防関係者が知るところとなり、母を含む 400 名以上の救助に繋がった[17]。

【課題 6】

これまでの内容を踏まえ、Twitter や Facebook といったサービスを今後どのように活用していくか、あるいはしないかを理由も含め 800 字以上で論ぜよ。また、論述の末尾に（n,nnn 文字）というように本文の文字数を記載すること。Word であれば数えたい部分をドラッグした上で、[校閲]タブ内の[文字カウント]機能を使えば文字数をカウントすることができる。

今回のレポート課題

- **締め切り**
  - 木曜クラス：6 月 25 日（水）15:00
  - 金曜クラス：6 月 26 日（木）15:00
- **内容**

  テキスト中の課題 1〜6 の回答を記せ
- **提出先**

  春日エリア 7B 棟 2 階 学務前レポートボックス

- **書式**

  Lab2014-1docx を適宜書き換えて使用し、1 ページ/枚で A4 片面モノクロ印刷。複数枚になる場合はステイプラー（針無しは不可）で左上 1 箇所を綴じること
- **備考**
  - これまでのテキストや演習中、返却レポート内などで指示・指摘された細かいレポートの書式（ページ番号の付与や使用フォントなど）は全て遵守すること。既に周知した書式を満足していなかった場合は減点の対象となる
  - 提出後におけるいかなるレポートの差し替えも認めない
  - レポート中のあらゆる箇所において手書きは不可とする
  - 提出先を間違った場合、原則として採点の対象外とする
  - 課題名はふさわしいものを各自で考案し記述すること

参照文献

[1] 情報環境企画室. “「情報システムを安心・安全に利用するために」の補足説明”. 筑波大学情報環境機構. http://www.oii.tsukuba.ac.jp/oii-security/, (参照 2013-06-19).

[2] Lars Backstrom. “Anatomy of Facebook”. Facebook. https://www.facebook.com/notes/facebook-data-team/anatomy-of-facebook/10150388519243859, (accessed 2014-06-17).

[3] Sadilek, Adam. et al. Finding your friends and following them to where you are. Proceedings of the fifth ACM international conference on Web search and data mining. 2012, p. 723-732.

[4] Zetter, Kim. “「誰かの Facebook 非公開写真」を簡単に見れるバグ”. livedoor NEWS. http://news.livedoor.com/article/detail/6096891/, (参照 2013-06-19).

[5] picopicohummer. “twitter の非公開リストが公開されるバグが発生し阿鼻叫喚 まとめ”. NAVER まとめ. http://matome.naver.jp/odai/2136144993837348701, (参照 2013-06-19).

[6] “フェイスブック・マイクロソフト 当局からの情報提供要請数公表”. NHK NEWSWEB. http://www3.nhk.or.jp/news/html/20130615/t10015325671000.html, (参照 2013-06-19).

[7] emo.tam. “知らない人が勝手に私を一方的に・・・高木浩光先生の『comm』ファーストインプレッション”. NAVER まとめ. http://matome.naver.jp/odai/2135098484968662401, (参照 2013-06-19).

[8] 東浩紀. “Twitter / hazuma: これ、カンニングだよね。これツイートするって、きみなに考えて ...”. Twitter. https://twitter.com/hazuma/status/22816859314, (参照 2013-06-19).

[9] “ツイッター:「僕だってのこぎりで…」筑波大２年生を逮捕”. 毎日新聞. http://mainichi.jp/select/news/20140529k0000m040125000c.html, (accessed 2014-06-16).

[10] シン, サイモン. 暗号解読 : ロゼッタストーンから量子暗号まで. 新潮社, 2001, 493p.

[11] 橋下徹. “Twitter / t_ishin: スマイルプリキュア”. Twitter. https://twitter.com/t_ishin/status/340640143058825216, (参照 2013-06-19).
[12] 深津 貴之. “iCloud ハック事件の手口がガード不能すぎてヤバイ”. fladdict. http://fladdict.net/blog/2012/08/icloud-hack.html, (参照 2013-06-19).
[13] ミトニック, ケビン. サイモン, ウィリアム. 欺術. ソフトバンク パブリッシング株式会社, 2003, 539p.
[14] “サクラサイト:アイドル装い課金メール、千葉でサイト運営者逮捕　２１００人、２億円超被害”. 毎日.jp. http://mainichi.jp/select/news/20130410dde041040007000c.html, (参照 2014-06-18).
[15] SIMONE COSIMI. “試験に合格する秘訣は「オフライン」だった”. WIRED.jp. http://wired.jp/2013/04/29/how-to-pass-the-exam/, (参照 2013-06-19).
[16] 110kA/いとか. “lib-officail-jp”. Twitter. https://twitter.com/lib110ka/lib-officail-jp, (参照 2013-06-19).
[17] 猪瀬直樹. “気仙沼の奇跡の救出劇、発信元はロンドン”. 日経 BP ネット. http://www.nikkeibp.co.jp/article/column/20120319/302831/, (参照 2013-06-19).