情報基礎実習 第９回 セキュリティとプライバシー

2013 年 6 月 20 日，6 月 21 日
担当教員：逸村裕
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く、今までに無かった種類の問題も多く出現した。今回は特に 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。

今回の内容

- 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

今回の出席課題

詳細は演習開始時に指示する。Lab2013-1.docx に回答を記載・印刷して演習時間中に提出せよ。課題名は「第 9 回課題」とする。

なお、p.4 の**課題 2** にも関連しているため、先にそちらに取り組むこと。

今回のレポート課題

テキスト中の課題 1～5 の回答を Lab2013-1.docx に記せ。

- 締切　：木曜日組：6 月 26 日（水）15:00；金曜日組：6 月 27 日（木）15:00 厳守
- 提出先：春日エリア 2 階学務前レポートボックス
- 課題名：木曜日組：情報基礎実習 0626；金曜日組：情報基礎実習 0627
- 備考　：A4 片面印刷、いつもの通り

1. 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、原則として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。

例として自転車の盗難防止に関する 3 つの手法について考える。

1. 施錠しない
2. ワイヤーの鍵をつける
3. 自動車用のタイヤロックをつける

1 のように施錠をしなければ鍵を持ち歩くことも、暗証番号を覚える必要もない。しかし、盗難の危険性は飛躍的に増す。2 であれば 1 に比べそのまま乗って行かれる心配は無くなるが、ワイヤーカッター1 つで簡単に破壊が可能である。3 であれば鍵そのものを破壊される心配はほぼ無くなるが、サドルを盗まれる可能性等は残る。また、タイヤロックは持ち歩くには非常に重い。

これらの手法のうちどれを採用するかについては、どのような場所で自転車に乗るかも考える必要がある。たとえば、繁華街のように多くの人が居る環境では施錠に気を使う必要がある。しかし、盗もうとする人が居ないような山奥では施錠の必要性そのものが無いと言える。

また、「許可した人以外には絶対に解除することのできない施錠」があった場合を想定したい。仮にそのような施錠があったとしても、100%の安全が保証されるというわけでは決してない。たとえば施錠を忘れるということもあるだろうし、自分の意志で人に貸したが返ってこなかった、ということも考えられる。

この自転車の盗難防止の例から分かることは、セキュリティ全般に適用することも可能である。すなわち、完璧なセキュリティは存在せず、状況に応じてセキュリティのレベルは変わるべきということである。

ウィルスなど、コンピューター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。

2. SNS とマイクロブログ

ブログ（Blog）とは Web 上で個人が公開する日記であり、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、現在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を課されたブログのことである。その制約により、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には掲示板や Wiki も含まれる。ソーシャルメディアは「Web 上に人格を形成する」という特長を持つ。特に 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、これらのサービスに関する諸問題について扱う。

3. 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。従来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。典型的な例としては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、3.1.から 3.5.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ていきたい。

3.1. 不用意な公開

個人を特定する情報については、何よりもまず本人が投稿をすることが挙げられる。前述のように SNS やマイクロブログで公開した情報は半永久的に Web 上に残るということを意識した上で発言することが肝要である。また、多くの SNS では「友達の友達まで公開」とした投稿が可能だが、「友達の友達」は一般には非常に広い範囲である。また、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 3 者が情報を収集することは非常に容易である。

課題 1

友達として 100 ユーザを登録している人が「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何人のユーザが閲覧可能かを計算せよ。ただし、友達はそれぞれ 120 人ずつ友達を持つとし、おのおのの 120 人のうち 60 人は他の

ユーザと重複しているものとする。

課題 2

出席課題に取り組む前の所感と、実際に取り組んでみた結果の手ごたえなどをそれぞれ詳しく記せ。

3.2. 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た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（「klis13」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[2]ということが分かっている。

3.3. 設定の不備、バグ

SNS では見せる相手を制限することが可能であり、Twitter でも「非公開ユーザー」として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いない。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」[3]、「twitter の非公開リストが公開されるバグ」[4]などが存在した。

3.4. 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、その機能で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[5]。

さらに、最近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[6]。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。

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、3.1.から 3.4.のような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。このことを炎上と呼ぶ。特に学生においては、飲酒やカンニング行為を投稿した結果炎上する事例は数え切れないほど存在する。たとえば、東工大におけるカンニング発覚[7]などが有名な例である。

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[8]。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。極端な話では、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[9]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呟いたとされている。

課題 3

実習室で Word を使ってレポートを書いている途中、パソコンのロックを掛けず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、剽窃とされてしまった。どうすべきだったかの対策を考えよ。

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。心理的な隙とは権威（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）などである。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[10]（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』[11]が詳しい。

課題 4

lumely@gmail.com からあなたのメールアドレス（s13xxxxx@u.tsukuba.ac.jp）宛てに次の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。

> このメールは情報基礎実習履修生全員に BCC で送っています。
>
> 情報基礎実習 TF の池田光雪です。
>
> 情報基礎実習第 9 回中でも説明しましたが、セキュリティに対する意識と現状の設定を調査します。件名を「学籍番号_氏名」とした上で、全学計算機システムのパスワードを逸村先生（hits@yahoo.co.jp）と私（lumely@gmail.com）を To に入れお送り下さい。このメールへの返信をもって第 9 回を出席とします。なお、パスワードの堅牢さ・脆弱さは一切評価しません。
>
> ---
> 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

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 2 億 1000 万円をだまし取った事件[12]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。

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、「JK 実習」「RanRan」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。Twitter ではアカウントの投稿を許可したユーザ以外には見せない「非公開アカウント」に設定することも可能であるが、なりすましによりフォローを誘い巧みに許可を得ることも考えられる。

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[13]。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. 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 100 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[14]。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 Tweet をしたところ、拡散によって日本の消防関係者まで届き、母を含む 400 名以上の救助に繋がった[15]。

課題 5

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 1,000 字以上で論ぜよ。

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] 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.

[3] 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).

[4] 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).

[5] “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).

[6] 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).

[7] 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).

[8] 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.

[9] 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).

[10] 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).

[11] 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.

[12] “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 2013-06-19).

[13] 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).

[14] 110kA/いとか. “lib-officail-jp”. Twitter. https://twitter.com/lib110ka/lib-officail-jp, (参照 2013-06-19).

[15] 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).