情報基礎実習 第 8 回

2017 年 6 月 8 日（木）、6 月 9 日（金）
担当教員：逸村裕、小泉公乃
TA：木曜　中田周育　小林俊貴　末岡真里奈
金曜　久保田正啓　伊川真以　小室祐樹

1. 本日の主な作業

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。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、Web が我々に多くの恩恵をもたらす一方、その技術を悪用してこれまでには考えられなかったような犯罪を行う者も現れてきている。また、その特性を理解しないまま Web を利用することにより、思いもよらぬトラブルに巻き込まれる者も数多く存在している。

今回は、数ある Web サービスの中でもソーシャル・ネットワーキング・サービス（SNS, Social Networking Services）の代表例とされる Twitter と Facebook 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。

- セキュリティと利便性
- ソーシャル・ネットワーキング・サービス（SNS）
- 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その実施コスト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。

機密性と可用性について、傘の盗難防止策を例にセキュリティを考える。ここでは 1. 何も対策をしない、2. ユニークな傘を使う、3. 常に持ち歩く、4. 中にゴミを入れる、5. 生体認証機能をつけるという 5 つの対策を考える。各対策について、本来の所有者のみが使うことができるか（機密性）、本来の所有者が自由に使うことができるか（可用性）、盗難のリスク、その対策を実施する際に必要となる費用や物理的スペース（実施コスト）の 4 点を **表 1** にまとめた。ここで、盗難リスクには取り違えの可能性も考慮されていることに注意せよ。

表を一望すればわかるように、全ての項目が良い対策は存在しない。つまり、何らかを犠牲にする必要がある。何も対策を行わない場合、当然盗難リスクは高まる。ただし、対策を取らない分、他の手法に比べコストは最も低い。また、ビニール傘のようなありふれた傘ではなくユニークな傘を使えば、取り違えで持ち去られる可能性は低くなる。しかし、最初か

ら盗難を目的としている人に対して効果は期待できない。一方、傘を常に持ち歩くようにすれば、建物入り口の傘立てに傘を置くことに比べ盗難リスクは非常に低くなる。一方、嵩張ることや、置き忘れという別のリスクが伴う。

表 1. 傘の盗難対策と盗難リスク・実施コストの関係

盗難対策	機密性	可用性	盗難リスク	実施コスト
1. 何もしない	低い	高い	高い	低い
2. ユニークな傘を使う	低い	高い	やや高い	低い
3. 常に持ち歩く	高い	高い	低い	高い
4. 中にゴミを入れる	低い	低い	低い	低い
5. 生体認証機能をつける	高い	高い	低い	高い

少し変わった対策として、傘の中にゴミを入れておくということが考えられる。使うために掃除をしなければいけないような場合、やはり盗難される可能性はかなり低くなるだろう。しかし、この場合は所有者本人も気軽に使用できなくなるため、本末転倒と言える。最後にゲームに出てくるような、柄の部分に指紋認証などの機能を搭載することで登録者以外には使えないようにした傘について考えたい。この対策は機密性、可用性、盗難リスク共に低くなるが、その開発・購入コストは他の対策に比べ群を抜いて高くなることが予想される。なお、いずれの盗難リスクも雨天時における代用としての盗難について考察したものであり、所有者のファン/ストーカーが持ち去るという可能性はたとえ生体認証を付けたとしても残る。

傘の究極の盗難対策とは、傘を使わないことである。

まとめると、**セキュリティ性を向上させることと、そのコストを低く抑えることを両立させることは傘の例に限らず、一般に困難である**。また、**どのような対策を取ったとしても未知の不具合などにより、そのセキュリティが破られる可能性は必ず存在する**。従って、**セキュリティとコストのバランスを考え、最適な手法を採りながらも、破られた場合の善後策まで考えておくことが重要である**。

以降、身近なサービスの 1 つと考えられる、SNS におけるセキュリティについて考えていく。なお、コンピュータウィルスの対策のような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]等が広く扱っているため、それらを通読することが望ましい。

3. ブログとソーシャル・ネットワーキング・サービス

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タグ付け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、Livedoor Blog やアメーバブログ、Tumblr などがある。また、Twitter は投稿内容が短くなるような制約を課されたマイクロブログと捉えることもできる。

一方、ソーシャル・ネットワーキング・サービス（Social Networking Service，SNS）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

はブログの諸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加わり、個人間の結びつきにより重点が置かれている。Twitter や Facebook、Google+、mixi 等がよく知られている。

これらのサービス形態には明確な定義や境は存在しない。複数の要素を併せ持つサービスも多く存在する。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」という特長を持つメディアを指し、上記のブログや SNS 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、SNS 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。

4. SNS におけるプライバシー

SNS 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。SNS の利用にあたってはこれらの特性を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高く、プライバシーの確保やデマの発生といった諸問題が顕在化している。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 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。例として、未成年による飲酒とその告白が挙げられる。SNS の利用に際し、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、SNS 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 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情報が投稿されうる。従って、その投稿内容から投稿者を推定することは比較的容易である。

また、SNS 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 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難しいことではない。

また、殆どの SNS では「友達の友達まで公開」とするような投稿設定が可能だが、「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。

ここで、知り合いを平均何人介せば SNS を利用している別の誰かと繋がることができるかを考えたい。これに対する一つの仮説として、「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が存在する。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]。すなわち、SNS 上であれば理論上誰とでも容易に繋がることが可能である。

【出席課題1】

詳細は授業中に指示する。Lab2017.docx に回答を記載・印刷し、1 限終了時までに提出せよ。

4.2 関連付けによる特定

ユーザ本人は自身が何者であるかを公開していなかったとしても、その断片的な投稿や、「友達」の情報からその人が何者であるか推測可能なことがある。例えば、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・図書館学類生であることが推測可能だと言える。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、より詳細な推定をすることも可能である[1]。

また、SNS では現実での繋がりを Web 上でも再構成することが多い。例えば Twitter ではフォロー・フォロワー関係やその順番を追うだけでもかなりの属性が付与可能である。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

多くの SNS では投稿を閲覧可能なユーザを制限することが可能であり、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、その機密性が完全に保障されているとは言えない。つまり、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る。例えば、過去に「『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 等の Web 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、サービスを利用する以上サービス提供者には多くのデータが渡っており、捜査機関や法的機関の要請、さらには利用規約により第三者に情報が提供されることがある。例えば、2013 年 6 月に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]。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 が流行っているが、規約の一部が問題となっている[7] 。

Web サービスを利用する以上、ユーザは何らかの見返りをサービス提供者に供していることを意識しつつ、実は不利益を被っていないかを確認するためにもサービス利用開始前に

---

[1] 「klis17」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。

利用規約はよく読むべきである。

【応用課題１】　提出については当日述べる

サービスを提供するにはコストがかかる。しかし、ソーシャルメディア（Twitter、LINE、Wikipedia など）は殆どが無料で利用可能である。そこで、基本的には使用料金が掛からないソーシャルメディアを複数取り上げ、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ことを調査、考察せよ。

4.5 炎上

SNS が開かれたものということを理解しないまま、犯罪行為等を公表した者に批難が殺到することを俗に炎上(flaming)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ことにより炎上する事例は非常に多い。例えば、東工大におけるカンニング発覚[8]などが有名である。

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。

本授業においても数年前、レポートの設問の一部を Yahoo!知恵袋に投稿し、当時の Teaching Fellow（TF）が回答したことが多くのメディアなどで取り上げられ話題となった。TF がそもそもその質問を発見できたことは、TF と相互フォロー関係にあったあるユーザが投稿を発見し、Twitter に投稿したことが大きく寄与している。

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、多くの関係者にも大きな迷惑がかかる。

5. 人間が持つ隙を突く攻撃

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、どんなに強固な暗号を使ったとしても、それを扱う者が人間である以上、かならずセキュリティの穴は存在する。極端な話、いくら通信上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。技術的な攻撃（クラッキング）と組み合わせることで、絶大な威力を持つ。

5.1 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。

【応用課題 2】

次に示す問題に対し、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、本学の全学計算機システムではログインしたまま放置されることを防ぐため、パソコンのロックはできない設定となっている。

> **あなたは大学の計算機室で Word を使ってレポートを書いている途中、10 分程トイレに行った。すると、その間に他の受講生にあなたのレポートをコピーされてしまい、同一レポートとして担当教員に剽窃の疑いを掛けられてしまった。他の利用者は居なかったため、あなたが被害者であることを証言できる人は居なかった。**
>
> **一般に、剽窃は試験におけるカンニングと同等のものとして扱われるが、見せた方にも責任があるとして両者共に処分の対象となることはかなり一般的である。あなたは担当教員に対し自らが被害者であることを必至に説明したが、証拠がないとして当該授業の単位取り消し処分となってしまった。**

5.2 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異性からの頼み）、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」といったフレーズ）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。例えば、過去に 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]。

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。

【応用課題 3】

第 8 回授業修了後、あなたの全学計算機のメールアドレス（s17xxxxx@s.tsukuba.ac.jp）宛てに差出人が hits@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とする。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。

なお、メール中に示された Web ページは実在しないが、次のような仮定を行い課題に取り組むこと。

- 実際にアクセスしたところ、統一認証システムの Web ページ（https://idp.account.tsukuba.ac.jp/idp/Authn/UserPassword）と全く同じ見た目の Web ページが表示され、ユーザ ID とパスワード入力を求められた
- この追加課題に対し、授業中に説明は無かった
- メールは 2016 年 6 月 10 日（金）22:00 に受信した
- 他の受講生全員にも全く同じメールが届いているのは確かである

5.3 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 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、メールにおいても差出人情報は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、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などが第一に挙げられる。

5.4 SNS 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基本的にある特定の 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、「エアつくば勢」と呼ばれるアカウントが多く存在する。また、「JKJ」「フレセミ」「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、さらには同学年の誰かと錯覚する確率は非常に高い。

From: Hiroshi Itsumura <hits@slis.tsukuba.ac.jp>
To: jk16staff_alt <jk16staff_alt@googlegroups.com>

※このメールは情報基礎実習受講生の皆様に BCC でお送りしています.
情報基礎実習受講生各位

情報基礎実習担当の逸村裕です.
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.
【第 10 回授業開始までに】次の Web サイトのフォームから各質問に回答してください.
http://klis.tsukuba-ac.jp/jk16/examine.htm

入力頂いた内容は成績には一切影響しませんが，本課題に取り組まなかった場合は何らかの措置を行います.
なお、不調によりメーリングリストを変更しました．本件に対する問合せは jk16staff_alt@googlegroups.com に行ってください.

逸村裕(Itsumura Hiroshi)　筑波大学 図書館情報メディア系　教授

図 1. 情報基礎実習受講生全員に届いたメール

5.5 SNS と生産性

SNS は心地よさを感じさせ、誰かに認められたいという人間の根源的な欲求を満たして

くれる。しかし、ある研究によれば、学生の本分である勉学に悪影響を及ぼす恐れがある。アメリカの女子学生 483 名（平均年齢 18.1 歳）を対象とした研究では、Facebook や Twitter といったメディアが成績に悪影響を及ぼしたと結論づけている[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。

6. 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、これ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、何気ない発言が本来の意図とは違った解釈を受け、結果として炎上することがある。特に、Twitter においては 1 つ 1 つの発言は高々140 文字に過ぎず、一切の誤解を生まないような発言のみを行うことは困難であり、また SNS の本質とそぐわない。例えば、「筑波大学の 1 年生」と名乗り、それが嘘ではなかったとしてもそれは学部 1 年生とは限らない。修士 1 年生、さらには博士 1 年生という可能性は残されている。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。

7. SNS・マイクロブログの活用

これまでではSNS の負の側面のみ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。例えば、従来のラジオやテレビ、新聞といったメディアを利用できない団体等において、最初に取り上げた SNS の拡散性は非常に強力な武器となる。図書館においても SNS 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 300 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、サービスを使いこなせているかの判断基準として、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に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]。

【応用課題 4】

これまでの授業内容を踏まえ、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 1,200 字以上で論じよ。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せよ。

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簡単にカウントすることができる。

【出席課題 2】

詳細は授業中に指示する。Lab2017.docx に回答を記載・印刷し，午前 11 時までに提出せよ。

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 2016-06-06).

[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).