3D-03

情報セキュリティにおける騙しの考察*

内田　勝也†

所　属†　情報セキュリティ大学院大学

1 はじめに

人を騙すことは，社会心理学の世界では古くから研究が行われてきた［1］が，主に人間に対する騙しを想定している． 医療分野では「偽薬（プラシーボ）」と言われるものがあり，薬としての効果のないものを与えることにより，患者への負担を減らす，あるいは，本物の薬の治療効果を検証するためのものがある．

最近のサイバー攻撃では，ますます人間の心理的な弱さを対象にした攻撃，ソーシャルエンジニアリング攻撃が増えてきた．

例えば，2015 年に発覚したセキュリティ事件に，「標的型攻撃」とカナダの不倫サイト「アシュレイ・マディソン」事件がある． 両者とも大量の情報漏えい（前者は，年金情報 約 125 万件，後者は，利用者情報 約3,200万件）が発生している．

国内での標的型攻撃は，既に 2000 年代後半に被害報告があり，教育・訓練も実施されている[2]．後者は，多くの女性ユーザが，人間ではなく「音声ボット」であったと言われている．

最近の IoT（Internet of Things：モノのインターネット）では，全てのモノがネットワークに接続されるといわれているが，「**モノ**」には『**者（People）**』と『**物（Machine）**』が含まれると考えると，これら，者や物，更に者と物の組みあわせが攻撃側にも被害側にもなり，騙し，騙される可能性がある．

2 攻撃側と情報資産／被害側について

情報は，単独で存在することは不可能であり，コンピュータ内やストレージ内，回線内等に存在し，情報を操作する人間やアプライアンス（コンピュータのハードウェアやソフトウェア），施設（空調，電源，建物など）の４分野を「情報資産」と呼び．心理学や犯罪学，行動科学等に依拠した攻撃（騙し）を考え，以下の攻撃側及び被害側を定義する．

(1) **人（People）**： 人が中心になって行う騙し，あるいは，騙されることであるが，対面では人だけの場合があるが、特別な内蔵プログラムなどを持たない機器（電話，FAX，郵便等）などが利用される場合も人と考える．

(2) **物（Machine）**： 高度なプログラムなどを持つ機器が中心であるが，プログラムが勝手に実装されることはないため，実装等は，人間が介在することを想定している．また，実装されたプログラム自身が学習機能を持っている場合も想定する．

(3) **人・物（People & Machine）**： 上記①及び②の両方の機能を持つものを想定し，それらが協力，連携して騙す，あるいは，騙されることを考える．

攻撃側及び被害側がそれぞれ３分野あるため，９つのケースを考えることができる．

3 攻撃／被害分類

攻撃側から被害側をみて，以下の９分類を行う．

- 攻撃側： 人（People）
  - ① 被害側： 人（People）
  - ② 被害側： 人・物（People & Machine）
  - ③ 被害側： 物（Machine）
- 攻撃側： 人・物（People & Machine）
  - ④ 被害側： 人（People）
  - ⑤ 被害側： 人・物（People & Machine）
  - ⑥ 被害側： 物（Machine）
- 攻撃側： 物（Machine）
  - ⑦ 被害側： 人（People）
  - ⑧ 被害側： 人・物（People & Machine）
  - ⑨ 被害側： 物（Machine）

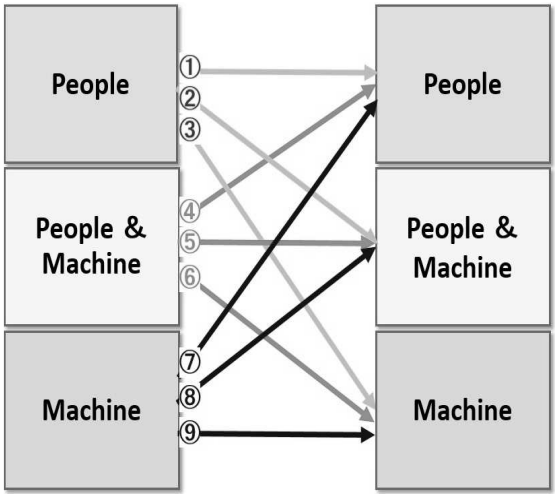

図１ 攻撃・被害図

項目毎の事例を考察する．

① 攻撃側： 人　被害側： 人

「**ソーシャルエンジニアリング**」： 最も頻繁に利用されるものでは，電話を利用して情報収集を行う．某自治体で発生したストーカー殺人事件では，電話で「被害者の夫」になりすまし，誘導質問術（Elicitation Techniques）を使って，被害者の個人情報を聞きだし，その情報収集を依頼したストーカーが被害者を殺害した［3］．

② 攻撃側： 人　被害側： 人・物

「**ショルダーハッキング**」： 被害者の利用している機器から情報を盗取するもので，被害者から直接情報を得るのではなく，「人＋物」を対象にした攻撃と考えている．

---

* Research of the Art of Deception in the Information Security

† Katsuya Uchida, Institute of Information Security

③ **攻撃側： 人　被害側： 物**

「**生体偽造**」： グミで人工指を作成（偽造）し，生体認証装置を騙すことが可能なことを実験で示した［4］.

④ **攻撃側： 人・物　被害側： 人**

「**ビッシング（Vishing）**」： 電話を利用したフィッシングで，自動音声ガイダンスを利用し，ガイダンスに従い，被害者が電話のダイヤル”９”を押すと，電話に攻撃者が現れ，被害者の個人情報等を求める攻撃［5］.

「**発信者番号偽装(Caller ID Spoofing)**」： 攻撃側の電話番号や音声を偽装するツールにより，発信者の性別，発信者番号等を偽装した攻撃.

⑤ **攻撃側： 人・物　被害側： 人・物**

「**水飲み場型攻撃(Watering hole attack)**」： 標的型攻撃の一種で，標的とする組織がよく利用するウェブを改ざんし，マルウェア等を実装し，そのウェブを閲覧した利用者（被害者）のコンピュータをマルウェアに感染させる．標的以外の組織の利用者が閲覧しても，感染しない仕組みを採用されていることもある.

⑥ **攻撃側： 人・物　被害側： 物**

「**標的型メール攻撃**」： メールに興味ある内容やタイトルをつけ，メール本文内の URL をクリックすると，ドライブバイダウンロードでマルウェアがダウンロードされ，感染する.

⑦ **攻撃側： 物　被害側： 人**

「**『音声ボット』によるなりすまし**」： カナダの「アシュレイ・マディソン」事件では，男性利用者とチャットをしていた多くの女性は，生身の女性ではなく，音声ボットが女性になりすましていた.

⑧ **攻撃側： 物　被害側： 人・物**

「**ファイル添付マルウェア**」： 件名や本文に興味のある内容が書かれたメールが送られ，添付ファイルをクリックするとマルウェアに感染する.

⑨ **攻撃側： 物　被害側： 物**

「**SYN Flood attack**」： インターネットでの TCP 接続は，クライアントとサーバ間で，３ウェイハンドシェイク（①SYN，②SYN ACK，③ACK）によって，通信が始まるが，クライアントが③ACK パケットを送らないと，３ウェイハンドシェイクが完成しないため，サーバは最後の「③ACK」パケットを待ち続ける． 大量の「①SYN」パケットを送付すれば，サーバは大量の「③ACK」を待つことになり，サーバの処理能力が大幅にダウンする.

４ まとめと今後の課題

心理学では，「騙し(Deception)」は，原則として人間が人間を騙すことを想定し，騙す態度（Cues to Deception）を 150 以上の分類を行っている［6］.

しかしながら，セキュリティ分野は，人間が人間を騙す，ソーシャルエンジニアリングが課題の１つになっているが，人間が機器を，機器が人間や機器を騙す例が古くから報告されており[7]，それを使った攻撃も発生しており，今後も益々「騙し」を利用した攻撃が行われると考えている.

セキュリティ分野の騙しは，ソーシャルエンジニアリングやセキュリティ心理学として考えてきたが，今後，AI 技術の進展や IoT の発展は，人間の心理的な弱さへの攻撃だけを考えるだけでなく，従来からある機器の脆弱性への攻撃や人間と機器を統合した形での脆弱性を狙ったものも考える必要がある.

更に，システム構築後にセキュリティを考えるのでなく，製品（ハードウェア，ソフトウェア等）設計やシステム構築の段階から，セキュリティを考えることが大切になる.

勿論，心理学や行動科学，犯罪学等の他分野の知見をセキュリティ分野の騙しやその対応に利用するために，更なる調査・研究が必要だと考えている.

発生した多くの事例の情報収集を行い，整理・分類を行う必要がある.

５ 謝辞

本研究は，公益社団法人 日本心理学会「助成研究集会『情報セキュリティ心理学研究会』」［8］での成果の一部で，参加された方々の協力を得ました.

参考資料

[1] Ekman.P & Friesen..W.V, Nonverval Leakage and Clues to Deception

[2] 山口健太郎他，ユーザへの予防接種というアプローチによる標的型攻撃対策，2009 年 3 月，情報処理学会第 71 回全国大会

[3] 内田勝也，誘導質問術からみた個人情報漏えいの考察，情報処理学会研究報告，Vol. 56 No. 12，pp. 2219-2229(Dec. 2015)

[4] 山田浩二他，ISEC2000-45 指紋照合装置は人工指を受け入れるか，2000 年 7 月，電子情報通信学会技術研究報告

[5] NTT 東日本，お客様の被害防止に向け、報道機関の皆様を通じた注意喚起にご協力をいただきますようよろしくお願いします，2008 年 7 月（http://www.ntt-east.co.jp/release/0807/080717a.html）

[6] DePaulo etal, Cues to deception, Psychological Bulletin, Vol 129(1), Jan 2003, 74-118

[7] Robert T. Morris, A Weakness in the 4.2BSD Unix† TCP/IP Software, 1985 年 2 月，https://pdos.csail.mit.edu/~rtm/papers/117.ps

[8] 公益社団法人日本心理学会，2014 年度助成研究集会，http://www.psych.or.jp/study/list.html