情報処理学会論文誌 Vol.56 No.12 2219–2229 (Dec. 2015)

誘導質問術からみた個人情報漏えいの考察

内田 勝也[1,a)]

受付日 2015年3月9日, 採録日 2015年9月2日

概要：2012 年 11 月に発生したストーカー殺人事件では，加害男性は被害女性の結婚後の名字や転居先市名を脅迫罪執行時に警察の逮捕状読み上げで知ったが，詳細な住所を知ることはできなかった．しかし，加害男性は詳細な住所調査を依頼し，それを受けた調査会社の経営者は被害女性の住所を聞き出すため，被害女性の夫を装い，当該自治体に電話をかけ，対応職員から正確な住所を聞き出した．この経営者は 2014 年 1 月に，逮捕された．たった 1 件の自治体からの個人情報漏えいが，殺人事件に至った．個人情報漏えいから殺人事件に発展した事例は，コンピュータ犯罪史上初めてではないかと思われる．自治体への電話照会で大量の個人情報が漏れることは少なく，大きな事件・事故につながることはなかった．自治体職員は個人情報を電話照会で教えた記憶がないと述べており，真相は不明だが，この経営者が大量の個人情報を保持し，自治体へ頻繁に電話をかけていたことを考えると高度な誘導質問術を駆使した可能性は高い．本稿では，ソーシャルエンジニアの主要手法である誘導質問術等の観点から情報漏えいやその対応策としての教育・訓練について考察した．

キーワード：誘導質問術，ソーシャルエンジニアリング，ヒューマンエラー，標的型電話攻撃，情報セキュリティ心理学

Research of Personal Information Leakage from the Point of Elicitation Techniques

Katsuya Uchida[1,a)]

Received: March 9, 2015, Accepted: September 2, 2015

Abstract: In November 2012, the stalker murder occurred in a local city of Japan. Because the victim married, and changed her address, the perpetrators man was not able to know the detailed address. The perpetrator man asked to get her detailed address to the executive of research firm. The executive was pretending to be victim's husband and made a phone call to the local government and got her exact address. The executive was arrested in January 2014. Only one personal information leakage from a local government led to the murder. Personal information leakage was developed into a murder case, probably, this is the first computer crime in its history. Staff of the local government have stated that there is no memory that he taught personal information over the telephone inquiry, the truth is unknown. Staff of local government said that there is no memory to divulging information. Because the executive has retained a large amount of personal information and has made the frequent telephone calls, he has likely made full use of the advanced elicitation. The executive has retained a large amount of personal information, so probably, he has used elicitation techniques. This paper introduces elicitation and examines an education and training for the countermeasure of elicitation.

Keywords: elicitation techniques, social engineering, human error, targeted telephone attack, information security psychology

1. はじめに

従来の大量個人情報漏えいでは，漏えい情報を利用した業者の「しつこい勧誘」電話が深夜にあり，それも 1 日に 10 回，20 回と頻繁にかかってくる，あるいは，勤務先ま

[1] 情報セキュリティ大学院大学
Institute of Information Security, Yokohama, Kanagawa 221–0835, Japan
[a)] uchidak@gol.com

でかかってくるといったことで，心的外傷後ストレス障害[*1]と思われる症状が一部の被害者に発生するといった精神的苦痛までであった [1].

しかしながら，今回の事件では，自治体から漏洩した1件の個人情報がストーカー殺人にまで発展した.

今回の事件は，大きく2つの段階に分けて考える必要がある．1つは，自治体からの個人情報漏えい，もう1つは，ストーカー殺人である.

個人情報漏えいは，従来の大量の個人情報漏えいが，主にコンピュータネットワークシステムの技術的な脆弱性や内部の特権を利用して，情報盗取が行われたが，今回は従来の大量情報漏えいとは根本的に異なる．外部から当該自治体に電話がかかり，たった1人の個人情報を盗取している．電話による個人情報の盗取は，心理学や行動科学等の知見を悪用したものと考えられ，情報セキュリティ分野でいわれる「ソーシャルエンジニアリング」による個人情報の盗取と思われる．実際には，ソーシャルエンジニアリングの中の「誘導質問術[*2]」が使われたと考えている.

本稿では，事件の概要，「誘導質問術」の考察，今回の事件を基に自治体職員向け誘導質問術への対応教育・訓練を実施し，その内容および教育・訓練結果の考察を行った.

なお，事件関係者へのインタビュー等ができなかったため，当該自治体のリリースやマスコミ報道を基に考察した．このため，真実とは異なる部分があることは否定できない.

2. 事件の概要等

今回の事件に関連した主な内容は以下のとおりである.

(1) 当該自治体の納税課には，当時，課長を含む正規職員6名と定年退職後の再任用職員2名，非常勤職員1名で，非常勤職員を除く8名はシステムを閲覧できるパソコンとID，パスワードが与えられていた.

(2) 利用された端末は，ログイン記録から，午前8時8分から午後5時13分まで，昼休みも含め，ログイン状態になっていた.

(3) 被害女性は元交際相手の男性からのストーカー被害を逃れるため，市役所に，第三者による被害女性の住民基本台帳の閲覧や住民票の交付制限等の申し出である，「住基支援申出」を行っていた.

(4) 職員が職場内のパソコン端末で，制限がかかった個人情報にアクセスすると，画面上に赤文字で「住基支援申出」と表示され，ドメスティックバイオレンス（DV）被害者や家族が閲覧制限を申請すれば認められる仕組みがあった.

(5) 被害者の住所情報収集依頼は，加害男性が依頼した探偵事務所から，さらに，調査会社の経営者に依頼された．この経営者は被害女性の夫になりすまし，市役所に電話をかけ「家内の税金の支払いの請求が来ているが，住所が間違っていないか」等と質問し，応対した市職員から被害者の正確な住所を得た.

(6) 経営者は，2011年4月から2013年7月までに複数の探偵業者から約8千万円の振込があり，パソコンに，個人や企業情報が，約120万件保存されており，個人情報収集を従前からかなり行っていたと判断される.

(7) 本事件前に，電話問合せは各自治体による判断であったが，事件後，総務省から「技術的助言」が発せられた[*3].

3. 誘導質問術

当該自治体からの個人情報盗取方法については明らかになっていないが，情報盗取を行った犯人が大量の情報を保持し，他の自治体等での同様の事例から判断する限り，誘導質問術が利用されたと考えられる.

なお，誘導質問術について，米国・連邦捜査局（FBI）の資料 [2] 等に基づいて，概要を説明する.

3.1 誘導質問術とは？

誘導質問術とは，当該対象者から直接，その内容を聞くことなく，情報収集する方法で，FBIでは以下のように述べている.

誘導質問術は，慎重に情報収集するために利用される技術で，特定の目的，すなわち，容易に入手できない情報を対象者（被害者）に疑いをいだかせずに収集することである．会話は，対面でも，電話でも，書面でも行われる.

高度な誘導質問術利用者にかかると，通常の会話の中でも，専門的な会話の中でも使われ，対象者は，誘導質問術の対象になっているとか，重要な情報を提供していることさえも気づかないことがある.

『人々が尋問されているように感じることなく，情報を収集する高度な会話術で，路上や電話，会議，インターネットでも行われる可能性がある』

とある.

3.2 誘導質問術の例

実際に誘導質問術と思われる話術が行われた場面にいた（聞いた）ことがある.

① 1994年11月に開催されたCSI Annual Conference[*4]において，夜間に開催された特別セッション

[*1] PTSD: Posttraumatic stress disorder.
[*2] 誘導質問術：Elicitation または，Elicitation techniques.
[*3] 総務省からの直接通知が存在するが，入手困難なため，兵庫県が県内市町村に通知したものが公開されている．http://www.hygshinko.or.jp/gyozai/pdf/05_kankeishiryo/pdf/02-38.pdf
[*4] CSI: Computer Security Institute．1974年からAnnual Conferenceを毎年秋に開催していた民間のセキュリティ団体であったが，2010年（第37回）を最後にAnnual Conferenceを含め，その活動を休止した.

の1つ「Meet the Enemy（ハッカーと語ろう）」[*5]での出来事である．このセッションは，ハッカーとConference参加者であるセキュリティ関係者との電話会議で，その最中に突然割り込んできた電話会社のオペレータがハッカーと会話をする中で，ごく自然に，オペレータは自分のユーザIDとパスワードをハッカーに明かしてしまった．オペレータは自分のユーザIDとパスワードを話したことさえも自覚がない様子で，それらを明かした後に，ハッカーの言葉に従い，オペレータは電話会議から抜けていった．

② ハッカーとオペレータの会話では，ハッカーは非常にリラックスして会話をしており，オペレータもごく自然に会話をしていた．ハッカーの話術の凄さと考えているが，この話術の背景に，質問方法，すなわち，初対面（電話では声だけであるが）から始まり，必要な情報を収集するまでの会話のプロセスが大きく影響していたと考えている．

③ 一般的に，質問方法には，「オープンな質問」と「クローズドな質問」方法がある．クローズドな質問では，質問への回答は「はい（Yes）」または，「いいえ（No）」で回答ができる．一方，オープンな質問では，「はい」や「いいえ」では，回答できない．ハッカーは，この質問形式を巧みに使い，最初はクローズドな質問方法を使って簡単な回答を引き出し，次第に相手が会話に慣れてくると，オープンな質問方法を使って，電話オペレータが自由に話せる雰囲気を作っていったように感じた．

④ この2人の会話内容を会場にいた約80名のセキュリティ関係者が聞いており，ハッカーが巧みな会話（誘導質問術）を使い，ユーザIDとパスワードを聞き出した技術，聞き出した後に，オペレータを電話会議から退出させた話術の巧みさに，参加者全員が感激し，拍手喝采した．

⑤ 誘導質問術もいろいろあり，簡単な方法では，攻撃対象組織の社員になりすまし，「パスワードを忘れてしまった．来週締切りの報告書作成にコンピュータを使えないので，新しいパスワードを発行してほしい」とパスワード管理部門に電話をし，条件付きで発行を認めてもらうという訓練[3]等が知られている．

3.3 誘導質問術はなぜ機能するのか？

心理学や行動科学等を利用した誘導質問術のようなものがなぜ有効に機能するのだろうか？

社会心理学者のロバート・チャルディーニは，人間には，以下のような6つの脆弱性があり，この脆弱性を利用すれば，相手から承諾や情報等を簡単に得ることができると述べている[4]．

① 返報性：親切や贈り物，招待等を受けると，それを与えてくれた人にお返しをせずにいられない気持ちになる特性．

② コミットメントと一貫性：自分の意志でとった行動がその後の行動にある拘束をもたらすもので，以下の3つの手法がある．

[②-1] ローボールテクニック：最初にある決定をさせるが，決定した事柄が実現不可能であることを示し，最初の決定より高度な要求を認めさせる．

[②-2] ドア・イン・ザ・フェイス テクニック：最初に実現不可能な要求を行い，対応できない状況で，それに比べ負担の軽い要求をしてそれを実現させる．

[②-3] フット・イン・ザ・ドア テクニック：最初に誰もが断らないようなごく軽い要求を依頼し，行ってもらい，次のより重い要求の承諾を得る．たとえば，最初に簡単な署名を依頼し，その後時間がかかる調査に協力してもらう．

③ 社会的証明：他人の考えにより，自分が正しいかどうかを判断する特性．

④ 好意：好意を持っている人から頼まれると，承諾してしまう特性．

⑤ 権威：企業・組織の上司等権威を持つ者の命令に従ってしまう特性．

⑥ 希少性：入手し難い物であるほど，貴重なものに思え，手に入れたくなってしまう特性．

前述のFBI資料では，

– 目的とする情報を収集するには，攻撃対象となる人間や文化的特性を十分理解したうえで，訓練された誘導質問術者は情報収集を行う．
– 誘導質問術者は，対象者が持ついくつかの特性を理解し，それを利用する．

具体的には，攻撃対象者が持つ以下のような特性を利用すると考えられている．

(1) 知らない人や初めて知った人に対してさえも，礼儀正しく，また，有用でありたいと願っている．
(2) 重要な問題に対して，自分は評価されており，貢献していると思っている．
(3) 褒められると，さらに多くの事柄を話したいと思っている．
(4) 特に，その情報について詳しくない場合には，その情報の価値を過小評価する傾向がある．
(5) 他人が胡散臭いと考えるより，他人は正直だと思う．
(6) 率直な質問をされると，事実を正直に回答する傾向がある．

[*5] Ray Kaplanが主催した電話会議（Tele-conference）で，会場に集まったセキュリティ関係者と複数名のハッカーが電話を通して，会議を行ったもので，ハッカーのセキュリティに関する考えや会場に集まったセキュリティ関係者の質問等にハッカーが回答する方法で開催されていた．

3.4 自治体等の窓口の特性

FBIの誘導質問術の考え方だけでなく，さらに，自治体等の窓口サービスや電話対応では，以下のようなことがいわれている[*6]が，最初の3項目は，FBIの誘導質問術とほぼ同じものだと考えられる．

(1) 親切に対応することが良いことだと考える．
(2) 困っている場合には，助けてあげたいという気持ちがある．
(3) うまくいってほしいという気持ちがある．
(4) トラブルに巻き込まれたくない気持ちもある．
(5) 組織の内部用語（ジャーゴン）を使われるとその組織の職員だと思ってしまう．
(6) 誰でも知っている組織や親族を名乗られると，警戒が緩くなる可能性がある．
(7) 時間が迫っていると言われると，回答をしてしまいがちである．
(8) 月末や週の繁忙時に，通常の手段以外の手順を言われると対応を誤ることがある．
(9) 外部からの電話で，ケータイやスマートフォンを利用していると言われると，電話のかけ直しの意味がなくなると考えてしまう．
(10) 強圧的な態度で攻められることに弱い．

3.5 誘導質問術は特別なものではない

誘導質問術や自治体等の窓口等の特性を知っているだけで，ただちに成果をあげられるわけではないのは，初対面の人と会って，すぐに打ち解けた会話が成立するわけではないことと同じである．

攻撃対象組織の体制や業務で使われる言葉，業務処理の常識等を知っていれば，誘導質問術の効果を高めることができる．

以下は，銀行のオンラインシステムが一般的に使われるようになり，預金の預け払いを当該銀行の支店であればどこでも可能になった時代に国内で発生した事件である．

当該銀行で使われている特別な言葉を犯人の1人が使ったため，電話を受けた支店の預金係主任は自行内の職員であると信じ，言われた指示を実行した [5]．

1981年10月に，H相互銀行[*7]で発生したオンラインを悪用した事件で，2人組の犯人の1人が田無支店に「コムセンの者だが，新宿支店と田無支店を結ぶ回線の調子がおかしい．テストをするから指示する口座に3,500万円を振り込んでくれ．機械が正常なら，30分後に入金を訂正する」と電話で指示があった．このため，預金係主任は女子行員に端末機から新宿支店の指定された口座に振り込むように指示した．

新宿支店の当該口座は数日前に，もう1人の犯人が，新宿支店に来店して口座を開設し，数日後に3,500万円が振り込まれるので，現金で，3,000万円を引き出したいと申し出ていた．

テスト送金指示の電話の直後に，再度，口座開設をした犯人が新宿支店に通帳を持って来店し，3,500万円が振り込まれているので，3,000万円を引き出したいと言って，支店で事前に準備していた現金，3,000万円を受け取った．

「コムセン」は，この相互銀行のコンピュータセンターの略称で，コンピュータセンターは，当時子会社が運用していたが，従来どおり，コムセンと呼んでいた．

この銀行でも，オンラインテストは全店いっせいで，営業時間外に限られ，前日までに支店長代理以上に文書で通達をだすと，同相互銀行の取締役の1人は述べているが，窓口の行員に徹底されていなかったと思われる．

もちろん，銀行の支店間で，平日の日中にテストをすること等，冷静に考えればありえないことであるが，通常業務とまったく異なる対応を指示され，さらに，銀行内の特別の言葉が使われたため，コンピュータセンターにいる行員からの電話だと預金係主任は判断したものと思われる．

2人組の犯人は，銀行で使われる言葉や多額の現金を引き出すには事前に告知しない限り，新宿支店のような大きな支店でも受け取れないことを知っており，犯人は退職者の可能性も指摘されているが，元行員でなくても，攻撃先である相互銀行に関連する情報を事前に調査・収集し，また，多額の現金で受け取るには事前に依頼しなければ無理であることも知って，犯行に及んでいる．

さらに，厳密には，誘導質問術ではないが，「コムセン」というこの相互銀行内での言葉（「ジャーゴン[*8]」）を使うことで，暗に行員からの電話だと判断させ，誘導質問術をより効果的にしている．

また，情報セキュリティ関連の事件ではないが，大きな社会問題になっている「振り込め詐欺」でも，被害者をだますため，なりすましを含め，いくつかの欺術を学んでおり，実際に対象者に電話をしながら，誘導質問術の実践を行い，その方法を修得している．振り込め詐欺では，詳細なシナリオがあり，それを単に覚えるのでなく，なりすました人物になりきって電話をし，また，被害者の名前や関係等について事前に詳しく知ることで，誘導質問術をより効果があるようにし，詐欺を成就させている [6]．

相互銀行事件や振り込め詐欺のような犯罪だけで誘導質問術が使われるわけではない．あるTV番組で，キャスタのお笑い芸人が，ゲストの女優から情報を聞きだした．

年齢の異なる2人のゲスト女優の主演番組で，年上の女

*6 後述する自治体職員への研修資料作成時等に，自治体の窓口の経験がある職員等に作成した項目について，その適否を確認し，作成したもの．正式なアンケート調査ではない．

*7 相互銀行は，1968年に成立した「金融機関の合併および転換に関する法律」に基づき，普通銀行（第二地方銀行）に転換した．

*8 （英語：jargon）その組織でしか通用しない専門用語であり，「隠語」とか「符丁」といわれることもある．

優は年齢をあかさなかったが，若い女優は自己紹介で自分の年齢を述べた．キャスタは 2 人の関係を尋ねると，若い女優が「姉と同級生」と述べたため，すかさず，「姉さんといくつ違うの？」と聞き，若い女優が姉との年齢差を言ったため，年上の女優の年齢が分かってしまった．隠しておきたかった年上の女優の年齢は若い女優の回答で分かってしまった．

3.1 節で述べた FBI の資料にあるように，犯罪的な利用だけでなく我々の日常の会話等でもしばしば利用されている．しかし，いろいろな事柄を「誘導質問術」と考えなかったため，今回のストーカー事件でも，自治体や対応職員の問題と判断された可能性がある．

4. 自治体での事件・事故対応

4.1 従前の自治体の状況

自治体での個人情報研修は，事件・事故発生後に行うことが多い．住民の個人情報漏えいは，民間企業と異なり，大量の個人情報漏えいの発生は，パソコンや USB メモリの紛失で，他人情報の誤配布では，数件以下が多い．

さらに，今回の事件以前には，自治体からの情報漏えいで，あまり大きな問題になることはなかった[*9]．

このため，今回の事件を起こした自治体の担当部門も，職員が出勤すると自分のパソコンを起動し，パソコンは一日中ログイン状態で，誰でもそのパソコンを利用できた．大きな事件・事故がないことや問合せ時にログイン/ログオフが面倒で，時間もかかるため，セキュリティポリシを順守していない．さらに，セキュリティ監査等も適切に行われていなかったと思われ，セキュリティポリシどおりの運用ができていなかった．

また，他の自治体でも，今回の事件以降，電話照会等について，従前の方法に大きな問題があるとの危機感を持つ職員は多くいるが，どのような教育・訓練を行う必要があるかは模索状態のところが多い．

このため，自分の自治体で発生した事件・事故でないと，自治体内のウェブや冊子の内容を更新し，それをもとに会議や朝礼等で，注意喚起する程度であった[*10]．

冊子やウェブでは，情報提供が主体で，「やってはいけないこと」，「やらなければならないこと」が主体になり，今回のような事件の本質を突いた教育・訓練は少ない．

ある自治体の冊子は，以下の記述だけだった．

① 即答しない ～連絡先を確認し，一度電話を切る．
② 組織で対応 ～応答の可否を上司と相談．
③ 疑わしきは回答しない ～連絡先と登録情報が異なっていたら答えない．

しかし，この程度の情報提供では，誘導質問術のような攻撃には，個人情報漏えいを防げないであろう．

最近，自治体の多くは，非常勤職員や再任用職員等の非正規職員を採用しており，これらの職員も正規職員と同等に窓口や電話対応を行うが，特に非正規職員の情報共有や教育・訓練が不十分で，正規職員を含め，以下のような課題がある．

① ウェブ情報（通達等）の場合，職員が見に行く必要があり，すべてを見ることが困難な場合が多い．
② ウェブ情報の場合，非正規職員は，パソコンを利用できず，情報はもっぱら，正規職員から得ることが多く，必ずしも危機感が伝わってこない．
③ 電子メール（メーリングリスト）は，非正規職員には，パソコンが与えられていても，メールが送られてこないこともある．
④ さらに，集合教育に非正規職員が参加することは希で，当該自治体には，再雇用者 2 名，非正規職員 1 名がおり，9 名のうち，3 名が集合教育等には参加していない可能性もある．
集合教育が知らない情報を参加者に提供する場合には，参加者が不参加者にその知識を後日説明すればよい．しかし，参加者間の討議やビデオ視聴，体験型教育・訓練では，不参加者に，教育・訓練内容を伝えることができても，教育効果は限定されてしまう．
⑤ 今回の事件で自治体からの情報漏えいを発生させたと思われる「誘導質問術」のようなソーシャルエンジニアリング攻撃の教育・訓練は，まったく経験がないと思われる．また，通達や冊子の配布等で，誘導質問術にも，対応できると考える職員もいるが，一種の「正常化バイアス[*11]」ではないかと考えられる．

なお，今回の事件報道を見る限り，自治体の当該課内の正規および非正規職員に対する，自治体による事情聴取では，全員が「記憶にない」等と回答している [7]．

自治体職員が気付かずに情報を教えたため，情報漏えいが起こったとの報道は，マスコミ 1 社だけが報道 [8] しており，他のマスコミ報道では，見いだせなかった．

誘導質問術等のソーシャルエンジニアリングを利用した犯罪は，振り込め詐欺があるが，ソーシャルエンジニアリング等の研究が少ないため，今回の事件でも個人情報の盗取は自治体の職員個人の問題との考えが主流を占めているように思われる．

5. 新しい教育・訓練の構築

5.1 新しい教育・訓練実施の前提

ソーシャルエンジニアリング等，人間の弱さを利用した攻撃に対して，どのような教育・訓練を行うか検討した．

[*9] 参考文献 [1] に示した事件では，被害を受けた顧客が PTSD 的な症状を示しているが，自治体ではこのような事例は見当たらない．
[*10] 複数の基礎自治体の友人，知人へのヒアリング等による．
[*11] 社会心理学等で使われる言葉で，自分の都合の良い方に解釈すること．

① 情報セキュリティ分野の基本の 1 つに，孫子の「敵を知り，己を知る」があるが，特に「己を知る」は，各個人を考えるだけでなく，組織の問題を含めて考えた．

② 今回の事件では明らかになっていないが，電話照会の回答をし，情報漏えいを許した職員とパソコンをログイン状態にしていた職員は異なる可能性もあり，セキュリティポリシや総務省通達を順守するとの意識が低いように思われる．

今回の事件はヒューマンエラーと考えられ，ヒューマンエラーは組織の問題ととらえる必要がある．しかし，多くの組織では刑事責任を回避するために，事件・事故は個人の問題に起因する [9] と考えがちである．組織事故としてとらえることが事件・事故の根本的な防止に役立つ．

③ 今回の事件・事故を想定した教育・訓練を自治体の職員を対象にした場合，窓口対応職員が中心となるため，2 時間から，半日程度が限界になる．1 日程度が望ましいが，2 回に分けて実施することも考えられる．

④ 数時間での教育・訓練を効果的に行うためには，単なる講義形式でなく，考えるヒントを与える工夫を考える必要がある．

⑤ 海外のソーシャルエンジニアリング教育も参考になるが，多くは，4，5 日で効果的な教育・訓練を行っているが，「敵を知る」に重点がおかれており，また，国内との社会的な環境の違いもあり，その内容をそのまま導入できない項目もある．

参考：海外のソーシャルエンジニアリング教育・訓練例

基本的には，ソーシャルエンジニアとしての知識・経験を深めることに重点が置かれ，ソーシャルエンジニアとして，被害者の弱点，脆弱性を知る教育・訓練を行っている．

(a) Advanced Practical Social Engineering [10] は，5 日間の教育・訓練で，講義が中心だが，数年前に英国で開催されたコースでは「Social Engineering For Penetration Testers」のタイトルで，前半は講義終了後にパブで顧客情報を収集する課題が課された．パブにいる他の顧客の仕事内容/学生には専攻等を聞き，さらに，個人特性（名前，年齢等）等を聞き出し，翌朝に発表する課題があった．

(b) Social Engineering Capture the Flag [11] は，チームで競技を行い，訓練を行う．参加者は，与えられた組織の事前調査をウェブ等で行い，競技時は，電話や電子メールを利用して，必要な情報を与えられた企業等から収集し，その収集内容ごとに得点を得ることで，他の参加者と得点を競う．

⑥ 情報セキュリティの教育・訓練では，他分野，特に医療事故防止を想定した教育・訓練 [12] や考え方 [13] 等で有用なものを活用する．医療事故は，患者の命にも影響を及ぼす点で，情報セキュリティよりはるかに危機感がある．また，多くは医者，看護師等が関係しており，ヒューマンエラーやチーム内の情報共有の有用性等を追求した教育・訓練が多く，今回の事件でも，参考になる点が多いと考え，取り入れることにした．

5.2 教育・訓練カリキュラムの作成

以上のような前提を考慮し，カリキュラムを作成した．

① 教育・訓練時間は 2 時間とした

対象自治体の教育・訓練担当との打合せを行い，自治体職員 30〜40 名程度を対象にし，自治体の状況を考え，2 時間で計画した．このため，5，6 名程度のグループ討議・発表は難しいと考え，誘導質問術や関連するソーシャルエンジニアリングについては，講師側，参加者側とも質問形式等を多用することにした．また，今回の事件では，想定以上のことが発生した可能性や今後，さらに攻撃が高度化する可能性のあることの説明も行う．

② ビデオ視聴により，チームワークの重要性の理解

心理学の知見で有名なビデオの視聴により，講義以上のものを与えることにした．

③ 教育・訓練の考え方

教育・訓練の進め方でも，工夫が必要であり，**図 1** に示す左右のマークを見て，正しい駐車禁止マークが左右どちらかを回答させるが，多くの参加者は解答できない．1 つのマークを示し，「駐車禁止マークはこれだ」としか教えない方法は，図 1 のように示すと，参加者の記憶には，正しい駐車禁止マークは残らないことが知られている．このため，特に，短い時間での教育・訓練の場合，教育・訓練内容が長く参加者の記憶に残る工夫も必要で，重要な事柄でも繰り返し教えられないという前提で考えた．

④ 今回の事件の概要

当該自治体からの情報漏えいの詳細はほとんど公開されていないため，「2. 事件の概要等」以上の情報があまりないが，自治体職員が知っている内容と判断し，簡単な説明にした．

⑤ 当該自治体におけるセキュリティ上の課題の解説

情報セキュリティに関する技術的な問題より，はるか

図 1 正しい駐車禁止マークは？
Fig. 1 “No parking sign”. Left or right?

にセキュリティマネジメントの問題が大きい．
- セキュリティポリシが順守されていない．
- 守られないことが恒常化しており，それが当然だと思っている．
- 首長等は，ICT や情報セキュリティに関心がなかったと思われる．

といった問題点の説明を行う．

特に，3 項目目は，首長等が ICT や情報セキュリティの知識を持つことは難しいが，関心を持つことが，結果的にセキュリティ意識を高める可能性があると判断し，以下の例を示すことにした．

注）ICT や情報セキュリティの知識より，経営者が関心を持つことの重要性の実例．

某大企業の社長は，SQL Slammer ワームで，韓国のインターネットが大混乱に陥っている TV 報道を見て，自社ネットワークの状況について，担当役員に電話で確認した．担当役員は担当課長に電話をし，確認を求めた．担当課長は「昨年夏にワーム対応を行っており，被害を受けることはない」と回答した．回答は担当役員から社長に伝えられた．社長が ICT やワームを十分理解しているとは思えないが，自社ネットワークにも影響があるのではないかという関心はあった．担当課長以下は社長が ICT に関心を持っていることに意を強くしたと聞いた．

⑥ 住基支援申出の課題：今回は，電話照会に回答しているが，総務省はストーカー等の被害者が「住基支援申出」をした場合，住基台帳の閲覧や，住民票の写しの交付等に制限を設ける通知 [14] をしている．しかし，強制力がなく自治体の裁量に任されており，当該自治体も「電話で個人情報を伝えないのが原則だが，氏名，生年月日，住所，納税通知書番号等，本人確認ができれば，状況に応じ対応する」[15] としていた．電話で情報取得できることを知っていた犯人に狙われた可能性も高い．

なお，DV とストーカーでは，加害者が異なることがある．ストーカーは，元夫・元妻・元恋人が加害者になるが，DV では異なる．今回，誘導質問術を利用した調査会社の経営者は，「被害女性の夫」になりすまし，自治体職員に対し，誘導質問術を使って，情報盗取をした可能性がある．

⑦ 誘導質問術の特徴や事例を示すとともに，相互銀行の 3,000 万円詐取と同じような例 [16]（税務署員になりすまし，電話照会で情報を詐取された）が自治体でも発生しており，他人事ではない．ただ，基本に忠実に行うことで，個人情報漏えいを阻止した例 [17] も説明する．

窓口や電話照会等の対応は，従来，親切さ等が大切との認識であったが，誘導質問術を利用し，住民情報の盗取への対応も必要であることも説明する．

さらに，電話照会では，回答時間の制約や携帯・スマホへの回答依頼等，従来なかった方法で要求に対応できるのか？　また，今後も新しい方法を使った要求も出てくる可能性についても説明する．

⑧ ICT を利用した防御も重要な要素であり，「住基支援申出」の場合の対応，職員の認証は，ログインより，ログオフの重要性を理解させる．生体認証の限界，電話照会に対する録音の検討，電話照会を中止することの検討，窓口対応のマニュアル/チェックリストの作成等について説明を行う．

⑨ 組織的な課題の説明：今後，誘導質問術を含めたソーシャルエンジニアリングへの対応は個々人の対応だけでなく，組織対応が重要であり，組織の重要性はヒューマンエラーの調査研究の知見やビデオ利用で参加者に実感させる．

(a) チーム力の育成：自治体内の担当部門内の情報共有等と同時に，自治体全体として対応できる環境作りが必要と考え，以下のものを組み入れた．

- 業務処理体制の不備や業務処理が複雑になると，担当職員のエラーを誘発する．多くの組織では，ヒューマンエラーは個人の特質に起因すると考える傾向があり，ヒューマンエラーに関する基礎的な話題を提供する [18]．
  - ヒューマンエラーは，個人に起因すると考えがちであるが，実際には組織的な問題が大部分である．
  - 個人が注意力を高めても，人の注意力が継続する時間は 30 分程度 [19] との実験があり，エラーもゼロにはならない．
  - ヒューマンエラーのための教育・訓練は，「知らない」や「できない」，「やらない」等を防ぐには有効だが，今回の自治体では，セキュリティポリシで禁止されているいくつかのルール違反をしていた．このような「不安全行動」を行うことが事件・事故につながることを説明する．
  - エラーを複数人で確認・チェックすると，他人が行っているという意識が働き，検出力が下がり，1 人の場合より検出力が悪くなることもあり，「社会的手抜き」や「リンゲルマン効果」といわれ，綱引きの事例を基に，より効果的な方法を説明する．
  - これらを通し，ヒューマンエラーを個人に帰するのでなく，どこに課題があるかを明確にし，組織的な対応の大切さを理解させる．
- 多くの人は 1 つのことに集中するとほかが見え

なくなることはよく知られているが，認知心理学では，これを「非注意性盲目[*12]」と呼んでおり，この非注意性盲目を理解するうえで有効な実験用ビデオ「The Invisible Gorilla」がある [20]．

このビデオは，白と黒のシャツを着た2チームがボールをそれぞれのチーム内の選手にトスする簡単なもので，研修参加者に白シャツを着たチーム内のボールが何回パスされたかを数えさせる．ビデオの途中で「ゴリラの着ぐるみ」が現れ，画面の真ん中で胸を叩き，立ち去るが，この実験の真の目的は，白シャツチームでのパス回数を正しく数えることと，研修参加者がゴリラを見たかを確認することにある．参加者は事前にゴリラが現れることは知らせず，白いシャツを着たチーム内でのボールのパス回数を正確に数えることを求め，ビデオを見せる．

ビデオ視聴後に，参加者にパスの回数を尋ね，その後，画面で何か変わったことがなかったかを尋ねるが，多くの参加者は，ゴリラの存在に気づかない[*13][21]．

このビデオ視聴実験の目的は，人間は1つのことに集中すると，周りが見えないことがあるが，複数で対応すれば，全体が見えることを説明する．

(b) 提言・課題の報告体制の確立：一般的に，システムや端末の利用者は，多くの問題に対して寡黙になりがちで，システム等の操作時に，エラーをしてもそれを隠す，あるいは，自分の「愚かさ」や「不注意さ」を責めようとする．本来は，「悪いのはデザインであるが，皆同じようなエラーをしている」と考えない傾向がある [22]．課題等を指摘できる場や気軽に上司に報告できる場の重要性を説明する．

⑩ 他分野（医療分野）でのチーム力育成教育・訓練，および問題解決手法を紹介する [23]．

5.3 教育・訓練アンケート結果等

約2時間を使って，上記カリキュラムを実施した．3カ所で実施したが，初回ではカリキュラムの検討が不十分であったため，初回開催後，課題を修正し，以降の教育・訓練を行った．

第1回と第2回は，自治体職員を対象にして行ったが，実施対象組織等は非公開とした．

多くの自治体職員は，電話照会による個人情報漏えいに起因したストーカー殺人事件が発生したことについて，従来の教育・訓練では対応できないとの認識は高かった．

第2回の教育・訓練実施後に行ったアンケートは，受講者38名のうち，37名からアンケートを回収できた．主な内容は以下のとおり．

① 所属部門
- 窓口部門：70%（26名）
- その他：30%（11名）

② 研修満足度
- 大変役立った：57%（21名）
- まあまあ役だった：43%（16名）
- あまり/まったく役立たなかった：0%

③ 役だった理由（主なもの）
- 組織力の大切さや組織としてどう対応するか？
- 現状の情報周知方法の課題を考える機会になった．
- 業務分析の大切さを再認識した．
- ストーカー事件を再認識する良い機会になった．
- ヒューマンエラーを多方面から考える良い機会になった．
- 個人情報を守るうえでの心構えが身についた．
- 考え方，チェック方法等が参考になった．
- 作業者に沿った仕組みづくりを考えるという視点が参考になった．

④ この研修を他の人に勧めたいと思うか
- ぜひ勧めたい/勧めたい/どちらかといえば勧めたい：19%（7名）/43%（16名）/19%（7名）
  合計 81%（40名）
- どちらともいえない/未記入：8%（3名）/5%（2名）
- どちらかといえば勧めたくない/勧めたくない：3%（1名）/3%（1名）

⑤ 研修内容の理解/業務活用等（評価：0低～10高）
- 研修内容を理解できたか？

0～4	5	6	7	8	9	10
0名	4名	2名	6名	12名	8名	5名

- 研修内容は業務に活用できそうか？

0～4	5	6	7	8	9	10
0名	5名	3名	6名	11名	6名	6名

- 研修内容は受講動機等と一致していたか？

0～2	3	4	5	6	7	8	9	10
0名	1名	0名	6名	3名	7名	9名	6名	5名

- 講師の説明やテキスト，進め方は？

0～4	5	6	7	8	9	10
0名	4名	4名	5名	11名	5名	8名

[*12] 非注意性盲目：(Inattentional Blindness)「非注意による盲目状態」ということもある．

[*13] 約半数の参加者がゴリラに気づかなかったと記しているが，本研修で，ビデオを見た各回参加者，それぞれ約40人は事前にこの実験を知っている参加者を除くと，1人か2人しか気づかなかった．また，ゴリラを見たと回答した参加者は，正確にパス回数を数えられないとの指摘もあるが，ゴリラを見た参加者数が少ないため，その結論を得られなかった．

⑥ 研修全体に対する意見・感想等

- 次年度も同趣旨の研修をぜひ実施し，今回同様他部の職員も受講させてほしい．
- 全職員を対象として実施したほうが良い．
- 危機管理についてはどんなに重複しても，繰り返し毎年実施してほしい．
- とても参考になった．職員からの質問も含め良かった．
- 悪いことを考える人や組織は増え，手口も巧妙化しており，毅然と対処するために活かしていきたい．
- 危機管理やリスクについて，正答はないが，講義の中で様々なヒントを得られた．
- ビデオの着ぐるみにまったく気がつかなかった．ミスをしないようにするには，組織として対応が大事だと感じた．
- いつもの見方でいると他の大きなことに気がつかないことを検証するビデオは大変興味深かった．
- ビデオは目から鱗で，全体を俯瞰する人がいることの重要性を感じた．

5.4 教育・訓練効果の測定

時間的な制約があったが，アンケート結果を見る限り，参加者の理解度も高く，研修結果に対する満足度も高かった．

カーク・パトリックは，教育・訓練を 4 段階で評価している [24]．すなわち，

レベル 1．研修満足度：受講直後のアンケート調査等による受講者の研修に対する満足度評価

レベル 2．学習到達度：筆記試験やレポート等による受講者の学習到達度評価

レベル 3．行動変容度：受講者自身へのインタビューや他者評価による行動変容評価

レベル 4．成果達成度：研修受講による受講者や職場の業績向上度合い評価

としており，さらに，ジャック・フィリップスは「研修の効果測定は，その効果を収益に換算し，収益を教育訓練への投資額と比較することによってはじめて有意義になる」と考え，カーク・パトリックの 4 段階評価にさらに 2 段階追加した [24]．また，カウフマンとケーラーは，社会的影響，すなわち，顧客への影響をレベル 5 に加えると提案している．

今回の教育・訓練の効果を，電話照会に対して，適切な対応ができたかであるとすれば，レベル 3 以上が求められる [24]．

誘導質問術やなりすまし等のソーシャルエンジニアリングに対する教育・訓練は，参加者が実際にソーシャルエンジニアリング攻撃を受けたときに，その対応ができてはじめて効果ありと判断できるが，レベル 3 以上の判断は，教育・訓練後に十分な時間が必要であり，現状は研修終了後のアンケートが限度であろう．

5.5 誘導質問術への効果

誘導質問術等のソーシャルエンジニアリングに対する教育・訓練は，短時間での対応は難しい．海外でのソーシャルエンジニアリング教育は，数日から 5 日間程度であり，今回の教育・訓練は，十分な時間を使ったものとはいえないが，従来の情報セキュリティ教育・訓練とは異なる内容であり，それなりの効果はあったと思われる．

- 誘導質問術が使われていることの理解：参加者全員が，共通の言葉で対応できるようになった．
- 誘導質問術と思われる場合，組織やチームでの対応が効果的との認識を持った．
- 他組織での情報も含め，組織内での誘導質問術等の情報共有や対応策の話し合いが有効であることが理解できた．
- 誘導質問術では，人間の弱さを狙われるため，どのような弱さがあるかの理解ができた．

今回の教育・訓練では時間の関係でできなかったが，想定した誘導質問術に対し，どのような対応が可能かをチームで議論できれば，以下の課題にも対応できるようになると考えられる．

- より実践的な訓練になり，誘導質問術への対応力が増す．

5.6 教育・訓練の振り返り

今回の事件は，個人情報に対する「標的型電話攻撃」ともいえるが，従来，氏名，住所，性別，年齢の基本 4 情報の漏えいが，殺人にまで発展することはなかった．

この事件を「他山の石」とし，いくつかの要因が重なっても，情報漏えいを起こさない体制を構築する必要がある．

特に，電話照会や窓口対応では，人間（職員）が関与する部分が大きいため，技術的な対応だけでなく，複数の職員による組織的な対応も重要になる．これは，自治体だけでなく，個人情報を扱う企業等でも同じである．

今回の事件から誘導質問術やなりすまし等のソーシャルエンジニアリング欺術は，注意喚起だけでは防げない．対策の基本的な考え方は，孫子の「敵を知り，己を知れば，百戦危うからず」であり，そのための教育・訓練を計画したが，講義中心の教育・訓練だけで終わらせるのではなく，継続的な教育・訓練が必要であり，1 回の教育・訓練で，どの程度理解されたかの検討も必要になる．

今回の教育・訓練は，比較的満足度が高かったが，実際の業務での活用になると，十分な解決方法を見いだせているか疑問も残る．5.3 節 ⑥ で記述したアンケート以外を下記に示す．

- 後日，グループで共有して電話対応で皆がやりがちなことを反省して業務改善ができそうである．
- 個人情報を不正に聞き出そうとする側の技術も日々向上しており，いざというときに適切な対応を係全員が

行えるかは疑問で，対策が必要になる．
- 実際の事例での原因をしっかり分析することで，効果的な再発防止策を考えられることが分かった．
- 多面的に個人情報漏えいの可能性を考えることができた．忙しいとき，あせっているとき，上司不在時等，いろいろな状況を想定して対処する必要があると気付いた．
- 内容自体はすでに知っていることが多かったがここまで深く掘り下げて考えたことはなかった．
- 何度も研修を受けている職員だけでなく，特に嘱託，アルバイト，再任用，任期付職員等を必須にしないと，十分に個人情報の取扱いを理解しないまま窓口，電話対応してしまう危険性が高いと感じた．

6. 今後の課題

(1) 今回の研修では，時間的な制約から，4，5 名からなるチームでの議論や簡単な作業等，組織全体で誘導質問術に対応する体験等は断念した．今後，半日から 1 日程度で実施する教育・訓練内容を検討したい．特に，実際に誘導質問術等を行う仕組みを検討し，参加者に体験させることは，費用や時間的な課題はあるが，検討に値すると思われる．

(2) 医療分野における組織の安全文化を醸成するチームトレーニングに，Team STEPPS [23] 等があるが，単に理論を教えるだけでなく，参加者がチームに分かれ，課題に対する議論や簡単な作業の経験を重ねながら研修を行うものである．情報セキュリティ事件・事故やミス等で，原因を個人に帰す傾向があり，「緊張して対応していない」とか，「注意力が散漫」等といわれるが，誰もが自由に発言できる環境の構築や関連する人全員に周知することの大切さ，リーダシップ等を学ぶようになっている．ビデオ視聴やチーム作業を通して，学ぶことも必要だと思われる．

(3) 誘導質問術やなりすまし等のソーシャルエンジニアリングは，国内での振り込め詐欺や海外での置き引き等からも分かるが，各個人が経験しても対応できず，繰り返し被害にあうこともあり，技術的な対応も検討する必要がある．たとえば，パデュー大学の CERIAS 研究所では，電話によるソーシャルエンジニアリングへの対応ができないかの机上調査 [25] を行っており，また，国内では振り込め詐欺対策用電話機も発売 [26] されており，今後，これらの有効性も検討してみたい．

(4) 今回の教育・訓練を実施した自治体で実際に誘導質問術等のソーシャルエンジニアリングに対して効果があったかの検証を行ってみたい．

(5) 誘導質問術が実際に行われたかの判断が非常に困難で，3.2 節で述べた CSI では，ハッカーと電話オペレータの会話を聞いたが，ストーカー事件では 1 社のマスコミ報道を基に判断した．インシデントの詳細を多くの研究者・実務家が共有することができれば，今回のようなインシデントに関係する人的セキュリティ対策の高度化につなげることができる．

参考文献

[1] IT Pro：[詳報] 業績に大きな打撃，補償には適切に対応—三菱 UFJ 証券の秋草社長が会見（オンライン），入手先 ⟨http://itpro.nikkeibp.co.jp/article/NEWS/20090418/328650/⟩（参照 2015-03-01）．

[2] FBI: Elicitation Techniques, available from ⟨http://www.fbi.gov/about-us/investigate/counterintelligence/elicitation-techniques⟩ (accessed 2015-03-01).

[3] NHK：世紀を超えて：電脳社会 闇の侵入者（ハッカー），2000 年 1 月 30 日放映．

[4] ロバート・B・チャルディーニ (著)，社会行動研究会 (訳)：影響力の武器［第二版］—なぜ，人はうごかされるのか，誠信書房 (2007).

[5] 日本経済新聞：続報 オンライン犯罪，1981 年 10 月 18 日朝刊，13 版．

[6] 鈴木大介：奪取「振り込め詐欺」10 年史，pp.54–58，宝島社 (2015).

[7] 朝日新聞：逗子市の端末，共用状態　ストーカー被害者情報，閲覧者特定できず，入手先 ⟨http://digital.asahi.com/articles/TKY201311070650.html⟩（参照 2015-03-01）．

[8] 全国新聞ネット：【逗子ストーカー殺人】市職員，気付かず情報漏えいか　巧みなうそ，隙を突く，入手先 ⟨http://www.47news.jp/47topics/e/247443.php⟩（参照 2015-03-01）．

[9] シドニー・デッカー（著），芳賀　繁（監訳）：ヒューマンエラーは裁けるか　安全で公正な文化を築くには，東京大学出版会．

[10] Social Engineering, Advanced Practical Social Engineering, available from ⟨https://www.social-engineer.com/store/#!/5-9-October-2015-Advanced-Practical-Social-Engineering-Baltimore-MD/p/43984300/category=3286162⟩ (accessed 2015-03-01).

[11] Social Engineering, Social Engineering Capture the Flag, available from ⟨http://www.social-engineer.org/interesting-se-articles/social-engineering-capture-flag-roundup/⟩ (accessed 2015-03-01).

[12] 東京慈恵会医科大学附属病院：医療安全の推進に向けて，入手先 ⟨http://www.jikei.ac.jp/hospital/honin/teamstepps.html⟩（参照 2015-03-01）．

[13] 河野隆太郎：医療におけるヒューマンエラー，p.147，医学書院 (2006).

[14] 神奈川新聞社：個人情報を調査会社が聞き出した疑い　逗子ストーカー殺人で課題浮上，入手先 ⟨http://www.kanaloco.jp/article/61921⟩（参照 2015-03-01）．

[15] 神奈川新聞社：逗子ストーカー事件，市役所から住所聞き出しか/神奈川，入手先 ⟨http://www.kanaloco.jp/article/61982⟩（参照 2015-03-01）．

[16] 埼玉県吉川市：官公庁職員を名乗って市役所に電話で問い合わせ（平成 25 年 11 月 29 日発表），入手先 ⟨http://www.city.yoshikawa.saitama.jp/sp/index.cfm/26,42250,181,942,html⟩（参照 2015-03-01）．

[17] 朝日新聞：探偵，自治体に電話 2000 件　全国の個人情報標的　愛知県警調べ，入手先 ⟨http://digital.asahi.com/articles/NGY201311170030.html?_requesturl=articles/NGY201311170030.html⟩（参照 2015-03-01）．

[18] 中條武志：人間信頼性工学：エラー防止への工学的アプ

ローチ，入手先 ⟨http://www.indsys.chuo-u.ac.jp/~nakajo/open-data/Healthcare_Errorproofing2.pdf⟩（参照 2015-03-01）．
[19] 総務省消防庁：消防活動における安全管理に係わる検討会，p.5，入手先 ⟨http://www.fdma.go.jp/html/new/161129kentou.html⟩（参照 2015-03-01）．
[20] Simons and Chabris: The Invisible Gorilla, available from ⟨http://www.theinvisiblegorilla.com/videos.html⟩ (accessed 2015-03-01).
[21] クリストファー・チャブリス，ダニエル・シモンズ（著），木村博江（訳）：錯覚の科学，pp.16–20，文藝春秋 (2011).
[22] D.A. Norman（著），野島久雄（訳）：誰のためのデザイン 認知科学者のデザイン言論，新曜社 (2009).
[23] Team STEPPS Japan Alliance，チーム STEPPS，入手先 ⟨http://www.mdbj.co.jp/medsafe/index.html⟩（参照 2015-03-01）．
[24] 独立行政法人雇用・能力開発機構，職業能力開発総合大学校能力開発研究センター：公共能力開発施設の行う訓練効果測定—訓練効果測定に関する調査・研究，調査資料，No.114, pp.39–44 (2005).
[25] Hoeschele, M.D. and Rogers, M.K.: Social Engineering Defense Architecture, available from ⟨http://www.cerias.purdue.edu/news_and_events/events/symposium/2005/materials/pdfs/D04-6B4.pdf⟩ (accessed 2015-03-01).
[26] 朝日新聞：振り込め詐欺撃退 新機能ファクス電話機発売 シャープ，入手先 ⟨http://www.asahi.com/articles/ASH255K6SH25ULFA02P.html⟩（参照 2015-03-01）．

内田 勝也 （正会員）

情報セキュリティ大学院名誉教授．電気通信大学（1968 年）卒業，中央大学大学院理工学研究科（2006 年）修了．博士（工学）．情報セキュリティマネジメント，情報セキュリティ心理学等の調査研究を行っている．