「国内におけるソーシャル・エンジニアリングの実態調査」

調査報告書

2000 年1 月31 日

情報処理振興事業協会

目次

【1】　ソーシャルエンジニアリングの定義

1　一般用語としての意味から

ソーシャルエンジニアリング(Social Engineering)とは、従来は日本語では「社会工学」として訳されており、主に学問の一つとして理解されてきた。辞書による用語の定義は以下の通りである。

(1)「社会工学」

人間の社会的行動を科学的に研究して、社会生活上の実際問題を解決しようとする学問。たとえば、作業グループのリーダーや組み合わせを変えて、精算の能率を高めたりする研究など。

(新明解国語辞典: 三省堂)

(2)社会工学とは？

「東京工大百年史」の「社会工学科」の章から抜粋すれば、社会工学科の目的には、「社会生活の開発計画に活用しうる人材の養成を目的とし、専攻分野の学問的基礎を確立するばかりではなく、今日わが国が直面する都市開発、公害対策、地域格差是正などの緊急課題に解決にも、関係する諸学科と協力して貢献しようとするものである。」と うたわれている。

また、社会工学という言葉についても、ハーバート・クローリー(Herbert Croly)は、すでに 1925 年に次のように述べている。" Better future would drive from the beneficient activities of expert social engineers who would bring to the service of social ideas all the technical resources which research could discover and ingenuity could devise." (「よりよき未来は、彼らの研究が発見し、彼らの英知が開発しえたあらゆる技術的資源を、社会思想実現のためにささげようとする、熟達した社会工学者たちの有為な活動によって開けるであろう。」)

(http://www.soc.titech.ac.jp/titsoc/whatissoc.html：東京工業大学工学部社会工学科、ホームページより)

また、特にいわゆるハッカーまたはクラッカーの不正アクセスの手段としてのソーシャルエンジニアリングの定義には、以下のような見解がある。

(3)社会的手口

「social engineering」という言葉をご存知だろうか。そのまま訳すと「社会工学」。なにやら学問の 1 分野のようだ。実際に工学の中の 1 分野として social engineering というものがあるが，インターネットで social engineering というと別の

意味になる。クラッキングの 1 つの手口を指す。うまい日本語訳はないが，あるメディアでは「社会的手口」としていた。

social engineering は，簡単に言うと，自分の身分を偽って，パスワードなどのクラッキングに必要な情報を関係者から直接聞き出してしまおうというものだ。いわば「からめ手」から攻めるもの。いくら頑強なセキュリティ・システムを構築していてもこれにはかなわない。

（http://nit.nikkeibp.co.jp/column/19980811/index.shtml：日経インターネットテクノロジー、インターネットコラム）

（4）“Social Engineering”

Social engineering n. Term used among crackers and samurai for cracking techniques that rely on weaknesses in wetware rather than software; the aim is to trick people into revealing passwords or other information that compromises a target system's security. Classic scams include phoning up a mark who has the required information and posing as a field service tech or a fellow employee with an urgent access problem. See also the tiger team story in the patch entry.

（http://members.tripod.com/~bernz/socenfaq.txt）

なお、上記資料を独自に翻訳したものが存在するので、これを参考までに取り上げる。

Social Engineering（社会工学）：n. クラッカー達や、ソフトウェアよりもウェットウェア（人の心理・脳）の弱点を突くクラッキング技術を持った人の間で用いられる用語で、その目的は人をだましてパスワードや目的のシステムのセキュリティーを危うくするような情報を引き出させること。ほしい情報を持った人に電話をかけ、緊急の用件を持った技術者や同僚のふりをして騙す古典的詐欺。

（http://www.members.tripod.com/~ayanamiz/shakai.html）

本来の「ソーシャルエンジニアリング」がもつ言葉の意味としては、上記（1）にて説明されている様な意味であると考える。

しかしながら、従来は「ソーシャルエンジニアリング」という用語は、「社会工学」として日本語に翻訳され、都市開発等に役立てる為の学問の名称としてのみに理解されてきたと考えられる。したがって、「社会工学」という日本語訳も、恐らく Social = 社会、Engineering = 工学、と言った具合で直訳され、この結果、いわゆる学問としての「ソーシャルエンジニアリング」の日本語訳としては違和感が感じられな

られなかった為に、このような形で定着しているものと考えられる。

犯罪的行為、あるいは犯罪性は無いが当事者の意志に反する様な行為の手口としての「ソーシャルエンジニアリング」自体は、人類の歴史の中でずっと行われてきたであろうと推測するが、最近は特に、不正アクセスの手口として「ソーシャルエンジニアリング」が注目された事により、一般的に利用されるもう一つの「ソーシャルエンジニアリング」が出てきた。

このときここで言う「ソーシャルエンジニアリング」は、従来一般的であった学問としての社会工学とは違って、本来の「ソーシャルエンジニアリング」の意味するところによるものであるから、「社会工学」という日本語訳は、馴染まないと考える。しかしながら、これにかわる良い日本語訳は無く、結局そのまま「ソーシャルエンジニアリング」と表記されているのが実態である。

したがって本レポートでは、Social Engineering の日本語訳として、「ソーシャルエンジニアリング」と表する事とする。

【２】　　ソーシャル・エンジニアリングの目的

１　本調査報告における定義から適宜変更して

「ソーシャルエンジニアリング」の定義については、基本的には、先述の１の (1) で述べられているような意味で捉えるが、レポートの焦点を絞り込む為に、以下のポイントについても、条件として定義する。

(1)その行為が、不正アクセスを目的とするものであること

犯罪的行為、あるいは犯罪性は無いが当事者の意志に反する様な行為の手口として利用されてきているが、このレポートにおいては、コンピュータの不正アクセスを目的とした行為に限定する。以下にその例を挙げる。

① 営業を目的として、巧みに特定個人の氏名、電話番号、住所等を聞き出す。

手口はソーシャルエンジニアリングではあるが、不正アクセスを目的としていないため、本レポートでは対象外とする。

② コンピュータに侵入するために、巧みにパスワードを聞き出す。

不正アクセスを目的としているため、本レポートの対象とする。

(2)人間の行為、行動における弱点、盲点を狙う行為であること

ソフトウェアのバグなどによるセキュリティーホールを突いたり、パスワード解析を行ったりするなどの、機械的、技術的問題に依存するケースや、強行突破のような手段については、本レポートでは対象外とし、あくまでも人間の行為、行動における弱点、盲点を狙った行為に限定する。以下にその例を挙げる。

① ソフトウェアのバグを突いて内部に侵入

ソフトウェアの技術的問題に依存するため、本レポートの対象外とする。

② ブルートフォースアタックによるパスワード取得

考えられるパスワードを総当たりして、一致する物を探すという仕組みであり、しかも実際にはプログラムによる自動処理にて行われるため、本レポートの対象外とする。

③ パスワード解析

パスワード解析自体は、一般的にはプログラムにて自動処理される為、ソーシャルエンジニアリングとは言い難い。しかしながらパスワードの解析をより効果的に行うための情報収集にソーシャルエンジニアリングを行う事は多い。したがって、本レポートでは、目的達成までの一連の行為について、その中の個別の手口について、それぞれがソーシャルエンジニアリングであるかどうかを判断する。

例えば、システム管理者のパスワードを取得するために、名前や生年月日など、システム管理者に関する様々な情報を、巧みに聞き出す行為はソーシャルエンジニアリングではあるが、その情報を元に、パスワード解析を行う事自体はソーシャルエンジニアリングとは見なさないこととする。また、事前の情報収集は全く行わずに、日本人に良くある名前や、一般的に使われている用語などを辞書化して、パスワードを解析する手口については、パスワードを容易に推測可能な値にする人間が必ず居るであろうと言うことが狙い目となっていることから、ソーシャルエンジニアリングに非常に近い。しかしながらこの問題は、技術的に解決可能であることや、行為自体がプログラムの実行だけで済む事から、本レポートでは対象としないこととする。

【３】　攻撃手法の分類

ソーシャルエンジニアリングの手口は、非常に多岐にわたっており、しかもそれらが様々な形で組み合わされて使われているのが実態である。しかも、それらが実に巧く、臨機応変に適用されることによって、その精度が高められている。ここでは、今までに確認されているソーシャルエンジニアリングの様々な手口を、大まかに分類し、それぞれの分類毎に、個別のテクニックを説明していくことで、整理していく。

１　トラッシング(Trashing, Dumpster Diving)

ゴミとして廃棄された物の中から、目的の情報を取得する方法の事を指す。特に日本では、ゴミ廃棄が無償で行われてきたことから（東京都は平成８年１２月１日より、事業系ごみを有料化した。）、ゴミ廃棄に対するコスト意識が非常に低く、機密情報を含むかも知れないであろうゴミの処理に配慮する事を怠ってきたこともあり、非常に危険な状態にある。また、コスト削減やリサイクル活動を積極的に行うために、片面しか利用していない印刷用紙等を再利用してしまい、そこから情報が漏れるということもあるため、これもまた非常に危険である。トラッシングの主な具体的な例は以下の通りである。

(1)深夜にターゲットの企業のゴミ収集所に行く。

(2)清掃員になりすまして（あるいは本当に清掃員になるか、または本当の清掃員を共犯にする事も考えられる。）内部でゴミをあさる。

(3)少々大がかりではあるが、回収業者になりすまして（あるいは本当に回収業者になるか、または本当の回収業者を共犯にする事も考えられる。）ゴミを持ち帰る。

少し変わったところでは、以下のような手口もある。

(4)いわゆる裏紙をメモ代わりに利用している店舗や窓口に出向き、何らかの口実をつけて、メモをもらう。(場合によっては、自由に使えるようになっている所もあるらしい。)

(5)飲食店等のレジカウンターで、お客様の名刺を集めている所に出向き、こっそりと名刺を取り出すか、あるいはのぞき見る。

(6)オフィスで、使用済みのフロッピーディスクを回収して、再利用をしているところから、未フォーマットのディスクを取り出す。

(7)オフィスから排出される、産業廃棄物としてのコンピュータ内のハードディスクを回収し、データを読む。

以下に、参考文献(ホームページ)における表記場所を示す。

トラッシング例① (63 ページ、12 行目より)

トラッシング例② (97 ページ、24 行目より)

トラッシング例③ (106 ページ、12 行目より)

2 構内侵入

これは、実際に建物内に侵入する行為を指す。その手段としては以下のようなものが挙げられる。

(1)偽装または拾得した ID カードでガードマンのチェックをパスする。

(2)カードリーダー等の機械的なチェックの場合は、同伴人の振りをして、他人についていく。

(3)清掃員等になりすます。あるいは本当に清掃員等になるか、または、清掃員等を共犯にする。

(4)何かの用事で訪問したついでに行う。

内部に侵入したら、その後はトラッシング、のぞき見などを行ったり、あるいは、内部のコンピュータ端末から内部ネットワークに直接侵入し、目的を達成したり、外部から侵入するための入り口を用意したりすることが出来る。また、トラッシングやのぞき見を組み合わせることも当然行われる。

以下に、参考文献(ホームページ)における表記場所を示す。

構内侵入例① (92 ページ、2 行目より)

構内侵入例②　(92 ページ、28 行目より)

構内侵入例③　(105 ページ、12 行目より)

構内侵入例④　(105 ページ、23 行目より)

3　のぞき見

本来、重要な情報が簡単にのぞき見されるような所に露出しているはずは無いのであるが、実際には様々な情報が飛び交っているものである。

(1)ディスプレイ等に張り付けた付箋紙に記入してあるパスワードを見る

(2)パスワードをキーボードに入力している場面を見る

(3)パスワードを口頭で教えているのを耳にする(場合によっては、自ら質問する)

(4)不在時に手帳等をのぞき見る

これらの手口を更に確実なものにするためのテクニックとして、ビデオカメラを持ってあらゆるシーンを撮影し、後にゆっくりとこれらの情報の確認をすると言うのがある。

以下に、参考文献(ホームページ)における表記場所を示す。

のぞき見例①　(92 ページ、16 行目より)

のぞき見例②　(105 ページ、12 行目より)

のぞき見例③　(97 ページ、19 行目より)

4　なりすまし

他人になりすまして、情報を引きだしたり、変更させたりする手口である。なりすましには、以下のようなものが挙げられる。

(1)システム管理者になりすまして、ユーザをだます

この場合、ユーザからすると、システム管理者はユーザのパスワードを管理している立場にあり、なおかつシステムのエキスパートであるという信頼感から、あまり疑うことをしないようである。これと同様の構図が、インターネットサービスプロバイダのユーザサポートとユーザの関係にある。

以下に、参考文献(ホームページ)における表記場所を示す。

管理者へのなりすまし例①　(40 ページ、11 行目より)

管理者へのなりすまし例②　(40 ページ、21 行目より)

管理者へのなりすまし例③　(43 ページ、12 行目より)
管理者へのなりすまし例④　(48 ページ、13 行目より)
管理者へのなりすまし例⑤　(105 ページ、28 行目より)

(2)ユーザになりすましてシステム管理者をだます

(1) と逆の構図であるが、システム管理者は、セキュリティーに対する意識も比較的高く、だますのは決して容易ではない。したがって、様々な工夫が必要となってくる。以下にその例を挙げる

① 初心者ユーザになりすます

エキスパートである管理者からすると、初心者ユーザを指導する事ほどやっかいな仕事は無い。これを逆手に取って、初心者ユーザになりすまして、「ログインがうまくいかない」などと言い、管理者を面倒くさがらせて、手っ取り早くパスワードを言わせて早く終わらせようと思わせるのが、こつである。

以下に、参考文献 (ホームページ) における表記場所を示す。

初心者へのなりすまし例①　(10 ページ、30 行目より)
初心者へのなりすまし例②　(66 ページ、4 行目より)
初心者へのなりすまし例③　(88 ページ、35 行目より)

② 他部署の上司になりすます

他部署と言えども、十分より職位が上であれば、逆らいづらいものである。この心理を利用し、他部署の上司になりすまして、「ログインがうまくいかない」などと、わざと威圧的に怒鳴りつける。そうすると、よほど真面目なシステム管理者でなければ、そのような状況でもルールを守ってパスワードを口頭では教えないなどとはいえないであろう。

以下に、参考文献 (ホームページ) における表記場所を示す。

VIP へのなりすまし例　(69 ページ、4 行目より)

③ 女性社員になりすます

一般的に、男性よりも女性の方が疑われづらいだけでなく、管理者が男性である場合には、男性からの依頼よりも、一層親切な対応をしてくれる可能性が高い。これを利用して、女性社員になりますと言う手口がある。しかしながら、このとき、いくら電話とはいえ、誰でも女性の声を出せる物ではないので、ボイスチェンジャーのような物を使うか、あるいはメールやチャットのような物でコンタクトをとるなどのテクニックを加えなければならないだろう。

以下に、参考文献 (ホームページ) における表記場所を示す。

女性社員へのなりすまし例　(93 ページ、4 行目より)

(3)外部の第３者になりすます

外部の人間には、誰でもそう簡単には機密情報を漏らす等と言うことは、常識的にはそう簡単には無いだろうと考える。しかしながら、パスワードを直接聞き出すまでには至らなくとも、名前等を聞き出す様な事は容易に可能であり、そのような情報を元に、不正アクセスを実現すると言うことは十分あり得る事である。以下にその例を挙げる。

① 公共サービスの人間になりすます

外部の第３者の中でも、公共サービスの人間と言われれば、比較的信用し易い物である。その信頼度を逆手にとれば、言葉巧みに情報を引き出すことが出来る。

② 取引先、見込み客等になりすます

今現在取引のある企業から問い合わせがあれば、相手の機嫌を損ねてはいけないと思うあまりに、聞かれるがままに、つい重要な情報も漏らしてしまうとは、決して珍しくないようだ。また、将来の顧客になるかも知れないと思えば、出来るだけ聞かれたことに答えてあげることにより、先につなげようと思う物である。これを利用して、管理者の名前を聞き出したりすることが出来る。

以下に、参考文献（ホームページ）における表記場所を示す。

取引先へのなりすまし例　（52 ページ、24 行目より）

③ 実在する顧客になりすます

この場合は、特に苦情を申し立てると言うことが非常に有効である。特に消費者向けの製品を製造、販売している企業にとって、すべての顧客を把握しているということは極めて難しく、したがって、顧客であることを認証する術は基本的には無いのが実態である。

また、これを更に発展させた形として、苦情の常連となり、コミュニケーションを続ける事で、相手と親しくなり、それによって、相手から情報を引き出すというテクニックもある。

④ 英語で電話する

日本人は、外国人に対しては親切であると言うことと、アジア諸国に対しては無意識に優越感を持っているが、欧米人に対しては無意識に負い目を感じがちであるという事を利用したテクニックである。

方法は簡単で、企業に英語で電話をかけて、役職者や管理者等の名前と電話番号などを聞き出すだけである。不思議なことに、日本語で同じ事を行うと、「失礼ですが、どのようなご用件ですか？」と言えることが、英語ではそうしない事が多々あるようだ。

これらのテクニックは、「誰になりすますか」と言う点に重点が置かれているが、誰を

狙うかということについてのテクニックもある。以下にその例を挙げる。

(4)昼休みに、システム管理者の部下を狙う

システム管理者自身は比較的手強い相手であることは言うまでもない。しかしながら、その部下などで、普段は補助的な仕事をしているような担当者であれば話はずいぶん違ってくる。というのも、そういう人間であれば、間違ってよけいなことを行ったり、してはいけない事を間違ってしてしまったりする可能性は極めて高い。しかも、場合によっては、普段任されていない仕事が出来るとばかりに喜んで協力してくれるかも知れない。

(5)わざと別の部署に問い合わせる

代表電話や、本人が所属する部署に電話をして、その人の事について訪ねると、本人に電話を転送しようとするのは当然である。しかしながら、隣の部署などに電話した場合などはどうだろうか。本人に転送しようとするのは実は比較的親切な方であり、多くのケースはその電話に責任を負うことを面倒くさがったり、電話番号が違っていると言うことを認識させるため、場合によっては物理的に転送が出来ないなどの理由により、転送せずに、その電話を切ってしまおうと思うようである。この心理を利用し、わざと他部署へ電話して、ターゲットの人間に関する情報を引き出してしまう事が可能となる。

また、特に日本では、各自の責任範囲が曖昧な場合が多いため、それは自分の責任範囲ではないといって、その場での対応を断るという事をしない場合が多い為、成功の確率は高くなってくる。

また、なりすましの手段についても、幾つかの方法がある。

(6)電話によるなりすまし

相手の顔が見えず、声だけになるため、なりすましやすいことから、上述の殆どは、電話によってなりすましが行われる。

(7)手紙によるなりすまし

電話同様に相手の顔が見えない為、犯行が発覚するリスクは低いが、臨機応援な対応が出来ない為、成功確立も多少下がる。

以下に、参考文献（ホームページ）における表記場所を示す。

手紙によるなりすまし例①　(90 ページ、4 行目より)

手紙によるなりすまし例②　(93 ページ、35 行目より)

(8)変装によるなすまし

例えば清掃員になりすますなどがあるが、この場合は構内侵入を伴う場合が多い。

(9)メールによるなりすまし

メールの差出人を偽る方法である。場合によっては、メールヘッダー情報などを偽造し、返送などについても盗聴を行うことによって、完全に他の誰かになりかわる方法もある。

以下に、参考文献（ホームページ）における表記場所を示す。

メールによるなりすまし例① （94 ページ、20 行目より）

メールによるなりすまし例② （102 ページ、2 行目より）

（10） Web によるなりすまし

この手口は、Web spoofing と呼ばれている。これについては、後に解説する。

以下に、その他の参考文献（ホームページ）における表記場所を示す。

チャットによるなりすまし例 （91 ページ、23 行目より）

他段階なりすまし例① （43 ページ、21 行目より）

他段階なりすまし例② （45 ページ、26 行目より）

他段階なりすまし例③ （98 ページ、18 行目より）

なりすましテクニック （47 ページ、6 行目より）

他。

5 チャット、BBS

チャット自体は、公開された場で行われているものの、実際に参加している人数が限られているため、当事者達は、自分達だけの閉じた空間で会話しているように錯覚し易い。したがって、そこは油断が生じやすい空間であると言える。BBS に関しても、公開された場であるにも関わらず、特定の人物とのメッセージのやり取りがおこなわれる事が多いため、油断が生じやすい。

例えばこのような例がある。

チャットや BBS に「パスワードの付け方には気をつけなくてはならない」などという話題を持ちかけ、誰かが、「ではどうすれば良いのか？」と質問してきたら、すかさず「名前と誕生日をつなげて複雑にする。」とアドバイスする。あとは、その人のパスワードを、アドバイスしたパターンで解析すれば良い。

以下に、参考文献（ホームページ）における表記場所を示す。

チャットによる誘導例① （57 ページ、26 行目より）

チャットによる誘導例② （59 ページ、5 行目より）

6 リバース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の手口は、基本的にはソーシャルエンジニアリングを行う側が、何らかの形でターゲットに近づき、目的を達成する。これに対して、リバースソーシャルエンジニアリングとは、必用に応じてあらかじめ何らかの仕掛けをしておき、あとはターゲット側が自らの意志で、行動を起こすことによって目的が達成される種類の手口を指す。以下にその例を挙げる。

(1)偽の緊急連絡先

ハードウェアやソフトウェアなどの保守業者の緊急連絡先が変わったという偽のメールを、システム管理者宛に出し、トラブルがあったときにその連絡を受ける。保守業者であると思いこみ、しかもトラブルの最中であると言うことから、相手は何でもしゃべってくれるに違いないであろう。この場合、トラブルを待つだけでなく、外部から使用不能攻撃などを加える事もある。

また、同様の手口としては、連絡先を携帯電話・ＰＨＳ等にした、偽造名刺を渡す手口もある。

(2)偽のホームページ

本物と思わせた偽のホームページにアクセスさせ、パスワード等を入力させる。詳細は Web Spoofing の項にて説明する。

(3)トロイの木馬

何らかの形であるユーザのコンピュータ内にプログラムを仕掛け、そのプログラムの誘導によって、ユーザが認証情報などを入力する事により、その情報を獲得する仕組み。

以下に、参考文献（ホームページ）における表記場所を示す。

トロイの木馬によるリバースエンジニアリング例 （106 ページ、1 行目より）

7 Web Spoofing

これは要するに何らかの形で本物と思わせた偽の Web サイトにアクセスさせ、そこで入力した情報を取得してしまう方法である。偽のサイトと言うことから、なりすましでもあると同時に、自らが起こす行動によって実現することから、リバースエンジニアリングの一種でもある。

偽のサイトにアクセスさせる方法には以下の例が挙げられる

(1)偽りの DNS 情報を流す

(2)まぎらわしい URL やドメイン名にして、偽りの URL にリンクされたものを押させる。

(3)E-mail 内の偽りの URL を押させる。

(4)有名なサーチエンジンにこれら偽りの情報を登録したりする。

(5)偽りのリンク集を作り、 偽りの URL でユーザを騙す。

また、別に本物が存在する様な偽物になりすまさなくとも、 Web を通じて情報を入力させる手段がある。以下にその例を挙げる。

(6)JAVA スクリプトで、そのページを開いたときに、あたかもプロバイダーがそれを行っているがごとく、ID とパスワードの入力を促すダイアログボックスを表示させて、情報を得る。

(7)懸賞を行うサイトを立ち上げ、応募させて、情報を得る。

(8)フリーメールサービスのサイトを立ち上げる。ある程度の個人情報が得られるだけでなく、フリーメール用のパスワードは、その人が他でも同じパスワードを利用している可能性が高いため、パスワードの推測も容易となる。

以下に、参考文献 (ホームページ) における表記場所を示す。

Web Spoofing 例① (54 ページ、28 行目より)
Web Spoofing 例② (71 ページ、3 行目より)
Web Spoofing 例③ (111 ページ、17 行目より)

【４】　　事例（参考文献、ホームページから抜粋して）

１　書籍

(1)ＦＢＩが恐れた伝説のハッカー　上
ジョナサン・リットマン／著　東江一紀／訳
出版社 草思社
発行年月 1996 年 10 月
ISBN 4-7942-0726-3

(2)ＦＢＩが恐れた伝説のハッカー　下
ジョナサン・リットマン／著　東江一紀／訳
出版社 草思社
発行年月 1996 年 10 月
ISBN 4-7942-0727-1

(3)サイバースペースの決闘
ジョシュア・クウィットナー／著　ミシェール・スラターラ／著　鶴岡雄二／訳
出版社 角川書店
発行年月 1995 年 12 月
ISBN 4-04-791237-9

(4)シークレット・オブ・スーパーハッカー　あなたのコンピュータも狙われている
ナイトメア／〔著〕　松藤留美子／訳　オフィス宮崎／訳
出版社 日本能率協会マネジメントセンター
発行年月 1995 年 11 月
ISBN 4-8207-1133-4

(5)セキュリティ入門ｆor Linux
高橋克己／著　トップマネジメントサービス／著
出版社 ローカス
発行年月 1999 年 11 月
ISBN 4-89814-034-3

(6)ネット・ビジネス最前線　アメリカ情報産業に学ぶインターネットの未来
前川徹／著
発行年月 1998 年 5 月
ISBN 4-89621-207-X

2　ホームページ

（以下本文は省略）

(1)IPA セキュリティーセンター - RFC - RFC2504 ユーザーズ セキュリティ ハンドブック
(http://www.ipa.go.jp/SECURITY/index-j.html)

(2)日経インターネットテクノロジー　インターネット・コラム（０８月１１日）
(http://nit.nikkeibp.co.jp/column/19980811/index.shtml)

(3)日本テレビ　特命リサーチ 200X ！　「彼らはどうやって情報を盗み出したのか?」1999 年 6 月 6 日放送
(http://www.ntv.co.jp/FERC/research/19990606/f1231.html)

(4)YAMAGATA Hiroo: The Official Page
(http://mars.post1.com/home/hiyori13/asahi/beyondhope.html)
(山形浩生氏主催のホームページに掲載される、同氏の寄稿記事)
Hackers in New York―― Beyond HOPE 参加記 (朝日パソコン 1997 年、ただし掲載は一部削除) 山形浩生

(5)CNET Japan TECH News

(http://japan.cnet.com/News/1998/Item/980710-8.html)

十代のハッカーがフォックス TV 系サイトを襲撃

By Jim Hu/日本語版 赤木順彦

Wed 8 July 1998 13:45 PT

(6)PC WEEK ONLINE JAPAN

(http://www.zdnet.co.jp/pcweek/archives/981221/981221p3501.html)

セキュリティ対策はどこから手をつけるべきか

自社にとって重要な知的財産とは。これらがどんな危険にさらされているかをまず考える

PC WEEK 日本版：98.12.21 号--

(7)プレジデント社　編集室より～Editor's Letter　1999 年 6 月 7 日
(http://www.president.co.jp/pre/editor/990607.html)
あなたの会社の情報は守られていますか？

(8)東京大学　東京大学生産技術研究所　第 3 部 藤田研究室　学生　三田 信氏

① (http://www.iis.u-tokyo.ac.jp/~makoto/security/)

② (http://www.iis.u-tokyo.ac.jp/~makoto/security/imp.html)

③ (http://www.ecei.tohoku.ac.jp/~mita/imp2.html)

(9)Wired NEWS　日本語版

(http://www.hotwired.co.jp/news/news/technology/story/775.html)

(原文: http://www.wired.com/news/news/technology/story/t12758.html)

「破滅」という名のインスタント・メッセージ

James Glave

（10） UG Akademeia

（管理者等は不明。タイトルより、いわゆるアンダーグラウンド情報と理解する。）

① （http://www.net-web.ne.jp/ipusiron/kiso_sosyaru.htm）

② 標準ソーシャルエンジニアリング講座

（http://www.net-web.ne.jp/ipusiron/hyoujyunn_so-syaru.htm）

標準ソーシャルエンジニアリング講座

③ ソーシャル・エンジニアリングの状況サンプル集 1

（ http://www.net-web.ne.jp/ipusiron/source/ug_text_so-syaru_sample1.htm）

ソーシャル・エンジニアリングの状況サンプル集 1

written by ipusiron(2000,2,18)

④ ソーシャル・エンジニアリングの状況サンプル集 2

（ http://www.net-web.ne.jp/ipusiron/source/ug_text_so-syaru_sample2.htm）

ソーシャル・エンジニアリングの状況サンプル集 2

written by ipusiron(2000,2,20)

⑤ 基礎 web spoofing 講座

（http://www.net-web.co.jp/ipusiron/kiso_web_spoofing.htm）

基礎 web spoofing 講座

written by ipusiron(1999,11,2)

（11） Bernz's Homepage - Social Engineering Homepage
(http://members.tripod.com/~bernz/socenfaq.txt)

THE COMPLETE SOCIAL ENGINERING FAQ!

"There's a sucker born every minute." PT Barnum

"Don't touch me, sucka." Mr. T

（12） Weird NEWS 記事

(http://www.wired.com/news/news/technology/story/15673.html)

AOL: 'You've Got Weak Security!'

by Michael Stutz

3:50 p.m. 16.Oct.98.PDT

（13） About.com 記事

（http://netsecurity.miningco.com/compute/netsecurity/library/weekly/aa101998.htm）

Loose Lips Sink Networks

Dateline: 10/19/98

（14） System Security

(http://www.artsci.net/~johnm/docs/security/se.html)

（1個人が開設するホームページであろうと思われる。トップページ不在の為、詳細は不明。）

（15） The University of Memphis - Department of Mathematical Sciences – Paul Ryburn, Instructor – Computer Literacy – Computers in Society
(http://www.msci.memphis.edu/~ryburnp/cl/cis/crime.html)

（16） Cafe au Lait Java FAQs, News, and Resources - Java Lecture Notes - Introduction to Java Programming: Week 5（ノースカロライナ大学をはじめ、複数の企業が出資する団体で、様々な資料や最新情報が掲載されている。）

① User Security Issues and Social Engineering
（http://metalab.unc.edu/javafaq/course/week5/15.html）

② Preventing Applet Based Social Engineering Attacks
（http://metalab.unc.edu/javafaq/course/week5/15.5.html）

【５】　　認識度調査報告

１　定性調査

一般的にはフォーカスグループインタビューというような、調査対象者をグルーピングして、１名のモデレーター（進行役）が、全員に質問をしながら、個々から回答を引き出し、場合によっては臨機応変に、理由等を深く聞き出す等の事をしながら、目的の情報を引き出す事を行う。

今回の定性調査に関しては、その内容が、各企業のセキュリティーに関する事であり、第3者には聞かれたくない内容であるということから、フォーカスグループインタビューの形式が、調査対象から受け容れられ難いという判断から、調査員が個別訪問を行う形で行った。なお、調査員と調査対象とは、機密保持契約が締結されており、調査結果については、その調査対象が特定できない範囲内での調査結果の公表までが許されている。

また、本来であれば、調査対象の企業に関して、業種等は分散出来たが、調査対象者については、セキュリティーに関わる情報システム担当者に限定される結果となった。

(1)基礎データ

① 調査対象の抽出方法

弊社タイガーチームサービスの顧客数百社から、業種毎に１社を無作為に抽出し、個別に依頼した。

② 調査対象のプロファイル

商社、製造、金融、情報技術関連、公共の各業種から１社。

いずれも従業員数は２００名以上の１部上場企業。

③ 調査方法

予約された日時に、調査対象企業に調査員２名が訪問し、各項目毎にヒアリングを行った。ヒアリングは、各企業のセキュリティーに関わる情報システム担当者（システム管理者）１名に対して行った。調査項目の大半は、選択形式ではあるが、質問毎にその回答の理由などを聞いた。

(2)調査項目とその目的

定性調査における、基本的な調査項目については、以下の仮説を前提として作成した。

「殆どの企業は、技術的な防御は施していたとしても、ソーシャルエンジニアリングに対しては、全くの無防備である。」

Q1、ソーシャルエンジニアリングという言葉をご存じでしたか？

ソーシャルエンジニアリングの基本的な認知度を確認します。ただし、調査依頼をする上で、やむを得ず「ソーシャルエンジニアリング」という言葉が使われている場合もありますので、質問の趣旨は、調査依頼以前に知っていたかということを求めます。

Q2、ソーシャルエンジニアリングという言葉の意味はご存じですか？

ソーシャルエンジニアリングについての理解度を確認します。その回答を確認する意味で、知っている場合には、その意味を答えて頂きます。

Q3、ソーシャルエンジニアリングに関する公式な社内活動はありますか？

企業全体で、ソーシャルエンジニアリングについて意識を持っているかどうかを確認する手段として、ソーシャルエンジニアリングという言葉が使われた公式な社内活動の有無について聞きます。例えば、情報システムにおけるユーザーマニュアル等への記載、公式な掲示板への掲載、全社員向けのメールによる周知徹底等の有無を確認します。

Q4、ソーシャルエンジニアリングを意識した上でのセキュリティー保持の為の公式な社内ルールは何かありますか？

意識を持っているだけでなく、具体的な対策を施しているかどうかを確認します。

Q5、Q4で「ある」と答えた方について、そのルールが守られているかどうかを確認し、それを守らせるようにする手段はありますか？

さらなる意識を高さを確認するために、ルールを徹底する手段があるかどうかを確認します。

これ以降は、周知のソーシャルエンジニアリングの手口について、どのように対応

するかを確認する事により、ソーシャルエンジニアリングへの対応について、改めて確認します。

Ｑ６、パスワードを忘れた場合の対処方法はどうなっていますか？

管理者からネットワークパスワードを聞き出したり、推測可能なパスワードに変更させたりする手法についての対策を確認します。

Ｑ７、対策がある場合、その対策内容に不安はありませんか？

Ｑ８、社内から発生した文書、帳票等の処分方法はどうなっていますか？

Trashing といわる、ゴミの中から、不正侵入に有用な情報を獲得する手法についての対策を確認します。

Ｑ９、対策がある場合、その対策内容に不安はありませんか？

Ｑ１０、貴社建物またはフロアへの部外者の侵入についてのチェックはされていますか？

人間が直接侵入する事によって、直接目的を達成したり、ネットワークを介した不正侵入に有用な情報を得たりする手法についての対策を確認します。

Ｑ１１、対策がある場合、その対策内容に不安はありませんか？

以下の質問は、その企業における過去の不正侵入に関する実績を確認します。

Ｑ１２、貴社は、過去に何らかの不正侵入が行われた事がありますか？（認識していますか？）

Q13、Q12で「ある」と答えた場合、それは犯人が特定出来ましたか？

Q14、Q12で「ある」と答えた場合、不正侵入の方法は特定出来ましたか？

Q15、Q14で「できた」と答えた場合、それはソーシャルエンジニアリングによるも

のでしたか？

最後に、このような質問をしてみました。

Ｑ１６、これまでと同様の質問を含んだアンケート依頼が、郵送にて届いた場合に、どのような対応をとられますか？

Ｑ１７、このインタビュー自体がソーシャルエンジニアリングだとは思いませんでしたか？

(3)調査結果

Q1、ソーシャルエンジニアリングという言葉をご存じでしたか？

回答内容	人数
知っている	5名
知らない	0名

この結果については、そもそも調査対象者が、既に技術的な対策を施している企業のセキュリティー担当者であるため、全員がこの言葉を認識していた。

Q2、ソーシャルエンジニアリングという言葉の意味はご存じですか？

回答内容	人数
知っている	5名
知らない	0名

この結果についても、Q1と同様である。ただし、理解の内容については、電話でパスワードを聞き出すといった、特定のケースの事にたとえて理解しているケースが5名中3名おり、様々なケースが考えられるということについての理解は決して十分ではないという事が伺える。

Q3、ソーシャルエンジニアリングに関する公式な社内活動はありますか？

回答内容	人数
ある	0名
ない	5名

これは、ソーシャルエンジニアリングについて、セキュリティー担当部門内では取り扱ってはいるものの、全社的にこの言葉が使われた実績は未だに無いということのようである。また、ユーザーマニュアル等で、パスワードの管理について十分注意するような記述はあるものの、それがソーシャルエンジニアリングによる危険についてまでの具体的な記述は無い様である。

Q4、ソーシャルエンジニアリングを意識した上でのセキュリティー保持の為の公式な社内ルールは何かありますか？

回答内容	人数
全てに意識している	0名
一部に意識したものがある	4名
意識したものは無い	1名

この回答の実態は、パスワードを忘れたときの運用方法について、従来から書面による依頼によってのみ受け付けるというルールが存在していたということをもって、一部意識したものがあるという回答となった。したがって、実質的にはソーシャルエンジニアリングを意識したルール作りというのは殆ど行われていないというのが実態であると考えられる。

Q5、Q4で「ある」と答えた方について、そのルールが守られているかどうかを確認し、それを守らせるようにする手段はありますか？

回答内容	人数
ある	4名
ない	1名

これは、管理者の作業履歴がログファイルとして残り、これを保存しているということであり、実際にその内容をチェックしているかどうかは、全くの別問題の様である。

Q6、パスワードを忘れた場合の対処方法はどうなっていますか？

回答内容	人数
申請書にて、直属上司の承認を得て、管理者に依頼する。変更後のパスワードは、最初の最初の1回限り有効のものが管理者から口頭にて伝えられる。	4名
電話にて、管理者に直接依頼する。変更後のパスワードは、最初の1回限り有効のものが管理者から口頭にて伝えられる。	1名

Q7、Q6の対処方法に不安はありませんか？

回答内容	人数
ある	5名
ない	0名

基本的には、全員が不安を感じてはいるが、現実的には、コンピュータの利用に関してそれ程長けていない人の数がまだまだ多く、これ以上厳しい運用は、ユーザーの混乱と管理者の工数負担の増大を招くために、踏み切れないでいるというのが実態であるようだ。

Q8、社内から発生した文書、帳票等の処分方法はどうなっていますか？

回答内容	人数
コンピュータ出力帳票は、専門業者に委託。それ以外は各自の責任にて処分	1名
裏紙として社内利用している	1名
資源ゴミとして回収している	2名
社内で裁断している	1名

従来は連続帳票を使用した集中印刷処理が一般的であったため、廃棄も非常にやりやすかったのだが、最近は、各ユーザーが自由に単票用紙に印刷する方法が一般的になっているため、基本的には各自の責任に依存せざるを得ないようになってきている。

また、裏紙として利用することによる経費削減や、資源ゴミとして回収することにより、安価にリサイクルを実践する等の行為は、その行為の正当性に、セキュリティーの意識が完全に埋没してしまっている形となっている。

Q9、その処分方法に不安はありませんか？

回答内容	人数
ある	5名
ない	0名

やはり、各ユーザーがセキュリティーの意識を高く持って、各自のゴミを処分しているかどうかについては、常に不安があるようである。

また、安全な処分方法を実現するためには、それなりのコストも発生することから、踏み切れていない企業が多い様だ。

Q10、貴社建物またはフロアへの部外者の侵入についてのチェックはされていますか？

回答内容	人数
ある	3名
ない	2名

あると答えた3名の企業は、いずれも社員証または入館（室）許可書のチェックが行われている。

Q11、チェックがある場合、その内容に不安はありませんか？

回答内容	人数
ある	3名
ない	0名

入館（室）許可のある者についていくことによって、チェックを受けずに済ます事が出来るようである。

また、清掃員や工事関係者等に扮装してしまうと、わからなくなる様である。

Q12、貴社は、過去に何らかの不正侵入が行われた事がありますか？（認識していますか？）

回答内容	人数
ある	4名
ない	1名

Q13、Q12で「ある」と答えた場合、それは犯人が特定出来ましたか？

回答内容	人数
特定出来た	0名

特定できない	4名

Q14、Q12で「ある」と答えた場合、不正侵入の方法は特定出来ましたか？

回答内容	人数
特定できた	2名
特定出来ない	2名

Q15、Q14で「できた」と答えた場合、それはソーシャルエンジニアリングによるものでしたか？

回答内容	人数
はい	0名
いいえ	1名
わからない	1名

これまでと同様の質問を含んだアンケート依頼が、郵送にて届いた場合に、どのような対応をとられますか？

回答内容	人数
答える	0名
答えない	4名
発信者に確認する	1名

これについては、基本的には、担当者自身はソーシャルエンジニアリングに対して、十分留意しようとい意志の現れであると考える。

このインタビュー自体がソーシャルエンジニアリングだとは思いませんでしたか？

回答内容	人数
思う	2名
思わない	3名

「思う」と答えた2名は、一般論として、個々で得た情報を利用するかどうかに関わらず、このインタビュー自体は、一種のソーシャルエンジニアリングの手法になりうるという意味で答えられました。また、「思いません」と答えられた方々は、契約に基づいた信頼関係によって、個々で得た情報を利用して不正侵入を行うということは無いという意味で答えられました。

(4)総括

この結果から判断すると、殆どの企業はソーシャルエンジニアリングに対しては無防備であるという仮説が成り立つと考える。また、セキュリティーに関わる情報システ

ム担当者に対して行った結果がこのレベルであることから察するに、一般社員の意識のレベルは相当低い物であることは容易に想像できる。

2　定量調査

一般的には、定量調査は、調査対象セグメントの全体に対して、一斉に調査用紙を郵送等で発送し、回答を返送していただき、その結果を集計して、判断するという手続きをとる。

今回の調査においては調査対象セグメント全体の企業数が２００社と、定量調査としては数が制限されており、基本的に回収出来る数も限られてくることは否めない。

そのうえ、定性調査の結果からもわかるように、定量調査自体が逆にソーシャルエンジニアリングとして疑われる可能性もあり、更に回収数は少なくなる物と予想される。

しかしながら、今回アンケート票を発送した調査対象セグメント200社の中から２０社より回答を得る事ができた。

以下にその集計結果を記載する。

基礎データ

① 調査データ収集方法

弊社タイガーチームサービスを実施した顧客２００社に対しアンケート票を送付した。

② 調査データ収集できた企業プロファイル

業種毎の内訳は以下のとおり

商社	3社
製造	5社
金融	3社
情報技術関連	3社
公共	2社
流通	1社
サービス、その他	3社

いずれも従業員数は２００名以上の１部上場企業あるいは同等規模の企業。

(2)調査項目とその目的

定性調査の結果から導き出された仮説は、

「殆どの企業およびその従業員は、ソーシャルエンジニアリングによる不正アクセスに無防備である。」

と考えた。

したがって、その仮説を検証するための調査項目としては、極めて基本的、初歩的な質問に成らざるを得ず、結局、定性調査と同様の項目を、定量調査でも使用する事となった。ただし、一部に修正を加えたので、それを以下に示す。

Q4、ソーシャルエンジニアリングを意識した上でのセキュリティー保持の為の公式な社内ルールは何かありますか？

意識したものがある

意識したものはない

また、Q6、Q8については、定性調査ではフリーアンサーであったが、今回は項目を分割して、選択形式とした。

Q6、パスワードの運用について

Q6-1､パスワードを忘れた場合の復旧依頼はどのように行いますか？

文書（ワークフローシステムを含む）で依頼

電子メールで依頼

口頭で依頼可能

直接管理部門に出向かなければならない

Q6-2､その場合に与えられるパスワードはどのような形ですか

現在のパスワード

管理者が新パスワードを決定（または自動的に）

規定の初期値に戻す

Q6-3､その直後のパスワードの設定はどうなっていますか

必ず再変更しなければならないような仕組みになっている

各自に任されている

勝手に変更は出来ない

Q８、ゴミの処分について

Q8-1､帳票類、書類の処理方法は何ですか

主に可燃ゴミとして廃棄

裁断して可燃ゴミとして廃棄

主に資源ゴミとして廃棄

専門業者に委託して廃棄

Q8-2､いわゆる「裏紙」を活用していますか

はい

いいえ

(3)調査結果

Q1、ソーシャルエンジニアリングという言葉をご存じでしたか？

回答内容	人数
知っている	１８名
知らない	２名

定性調査と同様に、技術的なセキュリティー対策を施している企業の担当者を対象にしている為、セキュリティーに関する用語の一つとして認知されているようである。

Q2、ソーシャルエンジニアリングという言葉の意味はご存じですか？

回答内容	人数
知っている	１６名
知らない	４名

言葉は知っているが、その意味がよくわからないという方も居られるが、大半は言葉の意味も理解しているようである。ただしその理解が正しいか、あるいは十分であるかということについては不明である。

Q3、ソーシャルエンジニアリングに関する公式な社内活動はありますか？

回答内容	人数
ある	１名
ない	１９名

この調査項目の意図は、全社的にソーシャルエンジニアリングの対策を施しているかどうかを把握するためのものだが、この結果からすると、やはり殆どの企業はソーシャルエンジニアリングに無防備であると言うことが考えられる。

Q4、ソーシャルエンジニアリングを意識した上でのセキュリティー保持の為の公式な社内ルールは何かありますか？

回答内容	人数
意識したものがある	１名
意識したものはない	１９名

この項目の意図は、仮に全社的な取り組みは無くとも、部門単位ででもソーシャルエンジニアリング対策を行っているかどうかを把握するための物だが、ボトムアップ型の啓蒙活動は非常に難しいらしく、そのような事が行われているケースも殆ど見受けられないようだ。なお、定性調査の結果は、調査員から例を提示した事によって得られたが、定量調査ではそのような事は全く行わなかったため、このような結果になったと考える。

Q5、Q4で「ある」と答えた方について、そのルールが守られているかどうかを確認し、それを守らせるようにする手段はありますか？

回答内容	人数
ある	１名
ない	０名

６パスワードの運用について

Q6-1､パスワードを忘れた場合の復旧依頼はどのように行いますか？

回答内容	人数
文書（ワークフローシステムを含む）で依頼	５名
電子メールで依頼	１０名
口頭で依頼可能	４名
管理部門に出向かなければならない	１名

ここでは、一例として、パスワードの不正取得がしやすいようになっているかどうかを把握するのが目的である。この結果、最も危険な口頭での依頼および次に危険な電子メールでの依頼が大半を占めている事から、やはり、大半の企業は非常に危険な状態にあると考える。ちなみに、直接出向かなければならないというのはいわゆるワンタイムパスワード装置を利用しているからのようである。

Q6-2､その場合に与えられるパスワードはどのような形ですか

回答内容	人数
現在のパスワード	０名
管理者が（または自動的に）新パスワードを決定	１３名
規定の初期値に戻す	７名

さすがに殆どのシステムでは、管理者と言えどもパスワードの表示がシャドウになっているため、現在のパスワードを教えると言うことは無いようだ。しかしながら、規定の初期値に戻すというのは、運用は楽ではあるが、そのようなルールになっていると言うのがわかってしまえば非常に危険であると言う認識は低いようである。

Q6-3､その直後のパスワードの設定はどうなっていますか

回答内容	人数
必ず再変更しなければならないような仕組みになっている	１０名
各自に任されている	８名
勝手に変更は出来ない	２名

パスワードの変更は、頻繁に行われるほど、安全度は高まる一方で、様々

なレベルのユーザを多く持つ企業にとっては、そのことによるトラブルや問い合わせ等も多くなり、負荷が増える事から、出来れば避けたいと言うのが本音であろうと思われる。勝手に変更が出来ないというのは、システムの都合上ユーザにパスワードの変更権限が無いということのようであり、業務システムの中には未だにこのようなシステムが存在するのも事実である。

Ｑ７、Ｑ６の運用に不安はありませんか？

回答内容	人数
ある	１９名
無い	２名

この結果は、本当は管理者サイドでは、より安全な運用ルールを確立したいのではあるが、実際の運用における管理業務の負荷が増えることに対する不安と葛藤しているであろうということを裏付ける結果であると考える。

Ｑ８、ゴミの処分について

Q8-1､帳票類、書類の処理方法は何ですか

回答内容	人数
主に可燃ゴミとして廃棄	０名
裁断して可燃ゴミとして廃棄	５名
主に資源ゴミとして廃棄	１０名
専門業者に委託して廃棄	５名

やはり、リサイクルを推進するあまりに、機密情報が危険にさらされているという、皮肉な結果が現れていると考える。

Q8-2､いわゆる「裏紙」を活用していますか

回答内容	人数
はい	１５名
いいえ	５名

ここでもまた、目先の経費削減に、セキュリティーが埋没している事が示されていると考える。

Ｑ９、その処分方法に不安はありませんか？

回答内容	人数
ある	１９名
ない	１名

この結果も、Ｑ７と同様に、セキュリティーの担当者としては、あるべき姿がわかっているが、ゴミの廃棄を有償にて安全に行わせるためには、それを管轄するのが、通常は総務部門などが行っているため、難しいという実態があり、そこまでに踏み

込めていないと言うことを裏付けていると考える。

Ｑ１０、貴社建物またはフロアへの部外者の侵入についてのチェックはされていますか？

回答内容	人数
ある	１８名
ない	２名

ちなみに無いと答えた２社は、貸しビルをフロアまたはスペース単位で借りている企業である。自社ビルあるいは一棟借りをしている企業は警備員によるチェックがおこなわれているようであり、フロアまたはスペース単位で借りている企業でも、カードキー等の認証による開鍵装置がつけられているようである。

Ｑ１１、チェックがある場合、その内容に不安はありませんか？

回答内容	人数
ある	１５名
ない	３名

警備員の徹底的なチェックと認証装置が組み合わされている様な所では、安心出来る場合もあるようだが、殆どがいずれか一方であり、運用上便宜を図る目的で盲点が生まれている様である。

Ｑ１２、貴社は、過去に何らかの不正侵入が行われた事がありますか？（認識していますか？）

回答内容	人数
ある	１４名
ない	６名

ここで言う不正侵入は、内部犯行も含んでいる。

Q13、Q12で「ある」と答えた場合、それは犯人が特定出来ましたか？

回答内容	人数
特定できた	１名
特定出来ない	１３名

特定出来ないという中の大半は、特定する事をしていないのが実態のようである。

Q14、Q12で「ある」と答えた場合、不正侵入の方法は特定出来ましたか？

回答内容	人数
特定できた	８名
特定出来ない	６名

内部犯行の場合、アクセスする事自体は正当な行為だと、方法はいくらでもあり、特定出来ないというのが実態のようである。

Q15、Q14で「できた」と答えた場合、それはソーシャルエンジニアリングによるものでしたか？

回答内容	人数
はい	０名
いいえ	２名
わからない	６名

ソーシャルエンジニアリングによる場合は、そのターゲットになった人物が、そのことを理解していなかったり、わかっていても自分の責任を回避するために、そのことを告白しない場合があり、基本的に発覚しづらい様である。