［第 18 回情報システム学会シンポジウム］

ノンテクニカルセキュリティ～非技術でのセキュリティ対応～

情報セキュリティ大学院大学　名誉教授

内田　勝也 先生

この記事は，第 18 回情報システム学会シンポジウム（2025 年 5 月 24 日）にける浦昭二受賞記念講演の口述内容をまとめたものです.

はじめに

内田でございます. よろしくお願いします. あまり見慣れないタイトルだと思いますが，実は 40 年ぐらい前から，日本の中に人間を考えているセキュリティがないということを非常に疑問に感じておりました．それをいろいろ考えていたところ，2000 年ぐらいにアメリカで開催された民間主催のセキュリティ会議で，カーネギー・メロン大学のソフトウェア・エンジニアリング・インスティテュートのグループの発表があり，3 人のグループで一人は心理学者でした．この様な組み合わせは，国内では余り聞くことがありませんでした．昨日，今日の話と同じような話があり，日本では，何か言葉が出てくると，みんなそれに対して賛同し，反対の考え方をなかなか受け入れない風潮があります. それなら，1 人ぐらい別の考えをしてもいいのではないかというのがそもそもの始まりです.

ただ，旧科技庁からのセキュリティ人材育成の取り組みに 2001 年に 2 校が選抜されたことから，2 年後に，当時所属していた，中央大学研究開発機構で，応募することになり，その提案書の作成を任されました．1 ヶ月程で書いて提出しましたが，日本にないものを書けば通る可能性があると考え，海外での調査結果など踏まえて提出しました．勿論，主査の先生の努力もありましたが，2003 年にセキュリティ人材育成として，年間 1 億円，5 年間のプロジェクトを取得[1]しました．2 年前の 2 校を含め，4 校の中で，10 月からスタートできたのは中央大学だけでした．それ程，きちんと準備してきました.

更に，主査：辻井重男先生から，2003 年 4 月頃に，「来年 4 月から横浜に大学院大学を開設するが，参加するか？」と聞かれました．この手の誘いを断る理由もありませんでしたが，結構大変な作業になりました.

ただ，基本的な考えは，このプロジェクトを横浜に開設する大学院に流用することをしました.

今日は年齢が高い方の参加が多いので，ご存じと思いますが，NHK 夜 9 時のニュースキャスターをされていた宮崎緑さんは，辻井先生の教え子で，時々，中大にお見えになることがありました．3 人で 2005 年か，もう少し後かもしれませんが，議論をしている中で，辻井先生自身は，セキュリティとは総合科学[2]という論文を書いており，セキュリティを総合科学というのは非常に気に入りました.

そこで，心理学をセキュリティの一つに入れてもいいのではないかと考え，『セキュリティ心理学』として始めました. 私は今から 15 年ぐらい前にセキュリティ大学院大学を定年退職して，今，名誉教授というタイトルをもらっていますが，あまり貢献をしていないの

で，「無職です」と言っております．

ただ，セキュリティ心理学を確立したいと考え，一人勝手に動いていました．

2022 年 7 月に『セキュリティ心理学入門[3]』という書籍を上梓しました．今年の頭にセキュリティ大学院大学が 20 周年を迎えたときに，15 年前に「セキュリティ心理学は確立できない」と言った先生が，「自分が間違っていた」とおっしゃいました．こんなうれしいことはないですよね．15 年たって間違っていたというのは，それぐらい先見性がなかっただけではないかと言えますが，このような話もありました．

今日は，全部はとても話ができないのですが，セキュリティ心理学についてお話しいたします．

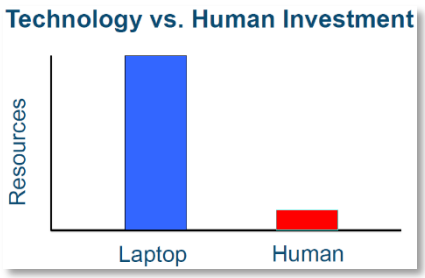
1　文部科学省科学技術振興調整費　新興分野人材養成（基盤的ソフトウェア）
2　情報セキュリティ総合科学と現代人の教養
3　内田勝也, セキュリティ心理学入門, 学術研究出版, 2022.07.10，ISBN978-4-91073351-7

1. セキュリティは技術だけで対応できるのか？

民間企業が主催する海外のセキュリティカンファレンスに，1993 年から毎年参加してきましたが，そこで感じるのは，なぜ色々な分野の専門家が，セキュリティ関連の話題を提供できるのかでした．日本ではセキュリティ技術以外の話をできる人が非常に少なくて，1 カ月ぐらい前に，セキュリティ心理学の専門家は何人いるのかと ChatGPT に聞いたら，4 人しかいないということでした．それは誰かというと，セキュリティ大学院大学にいる女性 1 人と，私と，私の知らない同じ大学の方 2 名でした．たかだかそんなレベルでしかやれないようなことを本当にやるのかと言われますが，1 人位いても良いと考えています．

実際に色々な話題が海外から入ってきました．2002 年 7 月 1 日に Web：Government Technology で，「Security First[4]」のタイトルで，Howard Schmidt： オバマ政権時のサイバーセキュリティコーディネーターが，「攻撃を回避する必要な技術は，強力なウイルス対策ソフトが必要ですか」との質問に対し，「セキュリティを技術的な問題と誤解されている．**国防総省（DoD）の 2001 年の調査では，97～98%はパッチ未適用か設定ミスが原因**」と述べている．これは明らかに人間の問題ですと 2002 年 7 月に述べており，この話題を 2002 年 12 月頃に話をしましたが，セキュリティ技術だと言われると全員がそれしか見えなくなるのが，日本の特徴で，心理学では，『**非注意性盲目**[5]』と言われます．セキュリティ関係はいかに底が浅いかということがよく分かります．

また，セキュリティ分野では，人間は『ウィーケストリンク（最弱部分）』だといわれますが，最近は，ウィーケストリンクでなく，最初に攻撃されるのが人間であるため，被害を受けるのが最初だとの話があります．



右図は，米国 Lance Spitzner[6] が示した図ですが，人間への教育・訓練が非常に少なければ，ウィーケストリンクであっても仕方ないと言っていました．

もし人間がそれなりの形で教育訓練を受けていて，なおかつ 1 番目ではなくて 3 番目，5 番目辺りで攻撃を受ければ，ウィーケストリンクが人間だなんて言う人はいなくなります．

もっと過激な言葉を言っている人もいます.

技術でセキュリティ問題を解決できると思うのは，問題も技術も理解していない

と Bruce Schneier[7] は言っています.

4 Security First, https://www.govtech.com/security/security-first.html: 現在このウェブでは，July 27, 2010, Jim McKay と署名がありますが，この日付，署名は誤りで，Question 6 番目に内容がありますが，2010 年のコンピュータウイルス対応ではないことがわかります.

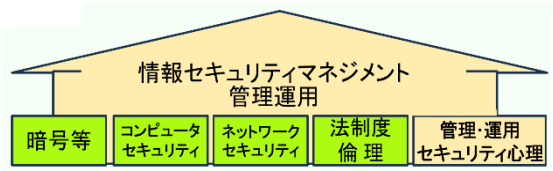
5 非注意性盲目： ひとつの物事に集中すると，他の物が見えなくなること

6 Lance Spitzner: Director, SANS Institute, RSA Conference 2014 で発表した内容

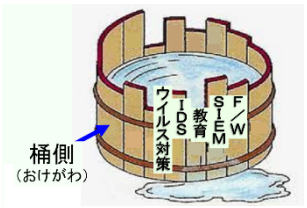
7 Bruce Schneier：アメリカの暗号，情報セキュリティの研究者，Harvard Kennedy School の講師

2. セキュリティ分野の俯瞰図

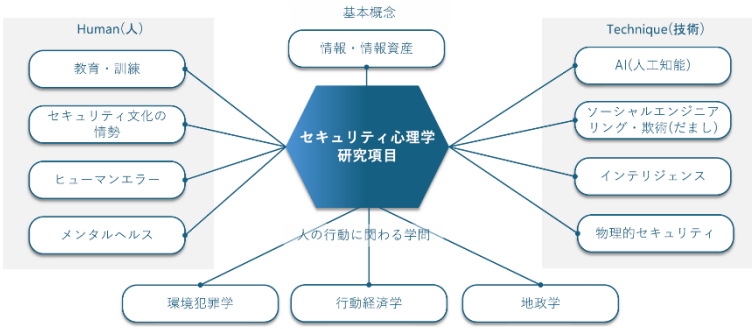
セキュリティ関係はいろいろな形で分類ができますが，五分野を考えるのが私の考えです．即ち，①暗号等，②コンピュータセキュリティ，③ネットワークセキュリティ，④法制度倫理,そして⑤管理･運用．セキュリティ心理を入れるのは少しおこがましいですが，人間の問題と考え対応する必要があります．これ全体をセキュリティマネジメントという形の管理運用ができればいいと考えました.



「御社のセキュリティレベルはどれくらいですか」と聞くと，「うちはこれぐらいのことをやっているので，ほぼ 80%」と言う人がいます．そこで，右図のような桶の絵をお見せし，「桶の中の水はどこから漏れますか」と伺います．桶側が一番低いところから漏れます．セキュリティレベルは最も低い桶側の部分だと分かります．でも，結構，セキュリティ対応の平均値がセキュリティレベルと言う方がいます．セキュリティを基礎から学んでいるのかなぁ？と思うことがあります.



セキュリティ心理学では，右図の様な項目を考えています．勿論，理論的な考察や新しい分野も出現すると考えています.



特にメンタルヘルスは，国内では余り表に出てこないですが，10 年程前に【セキュリティ心理学研究会】で，終了後に，「実はメンタルヘルスの問題を抱えています」とこっそり述べた参加者もいました．個人を特定することはありませんが，国内ではオープンにできないことが，国内でのセキュリティの問題にあります.

3. Elicitation Techniques（誘導尋問）とは？

ソーシャルエンジニアリングや Elicitation Techniques（誘導質問術）ですが，この機能を利用するのは，いわゆる，ハッカーだけではありません.『Elicitation』というパンフレットは，FBI の Web にあります．また，日本語もウェブに掲載されていますので，参考にして下さい.

誘導質問術が機能する理由ですが，後半の①～⑧では，丁寧な言葉で

きちんと話すこと，ここでは「礼儀正しく」とあり，きちんと言うことが大切です．それが逆に言うとソーシャルエンジニアリング的には問題になります．ソーシャルエンジニアリングの定義については，時間がないので割愛します．

セキュリティ以外の例を紹介します．お笑い芸人の情報収集です．ソーシャルエンジニアリングやElicitation Techniquesと言いませんでしたけれども，もう10年近く前かもしれません．たまたまテレビを見ていたら，お笑い芸人が若い女優を2人連れ，若い女優に「おまえは幾つだ」と聞きました．すると「24」と答えました．年上の女優に同じ質問をしたら，「女性に年を聞くのは失礼ですよ」と．そこで，年下の女優に対し「2人の関係は？」と聞くと，「姉の同級生です」と答えました．すると，「おまえと姉は幾つ違うんだ」と聞きました．「3歳」と回答がありました．これソーシャルエンジニアリングの最たるものです．

誘導質問術はなぜ機能するのか？

- **ＦＢＩ資料では，目的とする情報収集には，攻撃対象の人間や文化的特性を十分理解し，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以下のような特性を理解し，利用する**
  - **① 知らない人や初めて知った人にも，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，更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**
- **窓口サービスやコールセンター等での電話対応も，同様で，最初の３項目は，上記とほぼ同じ**
  - **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 うまくいって欲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，ケータイやスマホ利用だと言われると，電話のかけ直しの意味がないと考えてしまう**
  - **⑩ 強圧的な態度で攻められることに弱い**

こういうことを平気でやるような環境があります．振込詐欺や架空請求など，色々流行っていますが，若い人も被害に遭っています．ただ，やることは同じです．

4. ヒューマンエラー

ヒューマンエラーでは，一昨年でしょうか，マイナンバーの保険証に関し，エラーが出て，それが1000件，2000件あった，あるいは100件しかなかったということで，マスコミにも大きく報道されました．一部の有識者は，そんなものは大した問題ではないとの報道がありましたが，大した問題なのです．それを理解できていないところに，問題があるのではないかと僕は思っています．

実験例が多々あります．例えば**【ビジランスの30分効果】**では，時計の針が動くのを見

て，時々，1 秒ごとではなくて 2 秒進む，3 秒進むという現象があると，それを指摘しますが，30 分以上たつと検出能力が落ちるというものです．

ヒューマンエラーに対しては非常に素晴らしい人がいて，12 個あると言っていたので，四つ加えて，16 にして『**セキュリティ心理学入門**』という本を書きました．

5. 事故から考える（その 1）

事故を考える時，事故の心理的な部分を考えると，多くは事故が起こる前に予測ができるのではないかということです．セキュリティ技術は予測はしません．こんな問題があるからといって，ただ単に機器を入れたり，ツールを入れたりしているだけですが，人間の問題は，それが起こる可能性があるということがある面で分かると思っています．【予兆】という言葉で言っても良いと考えています．

2024 年 1 月 2 日に起こった羽田の航空機事故では，海上保安庁の飛行機には 6 人搭乗していましたが，6 人全員が管制官との交信で，滑走路に行っていいと聞いたと考えています．勿論，滑走路手前で待てと聞いた人もいた可能性がありますが，機長に言えなかった，**【クルー・リソース・マネジメント（CRM）】**と言われたり，最近は，**【心理的安全性】**と言われています．

もう一つは，【非注意性盲目】と心理学では言われている事柄ですが，あくまで個人的な推測です．非注意性盲目は，『見えないゴリラ』という動画で有名になりましたので，ご存じの方もいらっしゃると思います．

事故の状況を考えてみると，海上保安庁の飛行機は，能登半島地震のため物資を運んでいましたが，遅れがあり，かなり急いでいたと思われます．滑走路の手前で待てと管制官が言ったけど，滑走路で待てと誤解したと思っています．色々なことを同時にやると，必ず一つ，二つ抜けます．聖徳太子ではないから，10 人の言うことを聞いて全て完璧にできないという話です．

もし，管制官が海上保安庁の飛行機が滑走路に出ていないかを確認できていたら，この事故は起こらなかったと思っています．もちろん，管制官にその余裕はないと言われますが，新人管制官の教育・訓練として，考えることができないかと思っています．

6. 犯罪心理学

環境犯罪学はセキュリティ心理学として考えると，非常に面白い内容があります．国内では，事故を起こすと社長が出てきて，「**当社は性善説でやっている**」と言うのです．性善説でどういう管理をしていたのですかと記者は聞くべきなのです．要するに，性善説と言われたためにそこから先の質問が出てこないというのは，記者も不勉強です．忖度しているということもあるのかも知れませんが，少なくとも学会や研究者は，性善説だと言ったら，「どういう管理方法をやっていたのですか，丸投げだったのではないですか」と質問すべきです．丸投げということをマスコミなども言う割には，記者会見になった途端に丸投げが出てきません．非常に不思議な話なのですが，こういうところをもっともっときちんとやるべきではないかと思っています．

今日会場に多くの方がいるので質問です．お金が落ちているが，絶対に見つからないとします．いや，そんなことはあり得ないというのは駄目で，見つからないという条件だったら，皆さん方はどうされますか．落ちていた金額が 500 円，100 万円，3 億円だったらどうでしょうか．今日は年齢の高い人が多いので非常にうれしいのですが，「1. 警察に届ける」という方はいらっしゃいますか．多いですね．「2. 懐に入れる」，素晴らしい．いいですね．「3. 無視する」，すごいですね．この学会はお金持ちですね．

これは僕だったら，3 億円あったら，1%か 2%の確率で自分の懐に入れるかもしれません．だって 3 億円あったら，これは可処分所得で税金かかりませんので，こんないいことはないですね．年金に上乗せするとか，3 億円は非常に魅力的です毎年 1000 万円使っても 30 年です．もう，30 年は生きていませんが，去年の区民検診で「まだ 20 年大丈夫だ」と言われましたが，高々その程度です．要するに，環境が変わることによって人はやり方が変わるのではないかということで，私は性弱説と言っています．人間の心というのは弱いです．だから，環境が変われば変わってくることがあるということを考えておいていただきたいのです．

7. 事故から考える（その 2）

もう一つは，貸金庫の問題です．昨日，貸金庫の話をしたら，若い人に貸金庫がどうなっているか分からないと言われたのですが，一般的には貸金庫は，個々人に貸金庫の小さな部分を割り当てて，銀行側が持っている鍵と個人の鍵と二つがないと開けられない仕組みなっています．今回，大手銀行の貸金庫での窃盗事件のケースでは，2 種類の鍵，顧客用と銀行用の鍵がありましたが，1 人の女性が両方の鍵を保持（管理）していました．1 人の人が 2 種類の鍵を管理していたらどうなるかは，セキュリティを少し教えた中学生でも分かりますね．これは日本を代表する大手銀行の話です．

要するに，2 種類の鍵を 1 人の人が持った状況で，当初の環境，個人でも，個人を取り巻く環境が変わることがあります．

そこで，これを『**性弱説**』と言っています．性弱説を考えることが必要と考えています．今回のケースでは，その女性は FX 取引等で膨大な赤字を出し，それを補填するため顧客の資産（貸金庫の内容）で，一時的に穴埋めができないかを考えます．でも，ほとんどうまくいきません．最近オンラインカジノがはやっていますが，たくさんもうかったという人はほとんどいません．40 年ぐらい前に，パソコン関係の協会のツアーでアメリカに行ったときにラスベガスに寄った人たちが一部いました．翌日，利益がでた人は一人だけで，40 ドルでした．

今回の事件で，非常に気になったのは，頭取が記者会見で，その犯人である女性行員が悪いことをするなどという考え方がなかったとの雰囲気がありました．他の人はどう感じたか知りません．

8. 楽しいセキュリティを！

私は，セキュリティを「**楽しいセキュリティ**」であると言っています．楽しくないとい

うのは,セキュリティレベルの低い人がセキュリティをやっているからだと思っています.

最近，心理的安全性といわれる内容が話題になっていますが，日本では，なかなか難しいと思っています．なぜか．日本ではファーストネームで呼ぶということがほとんどありません. 最近,「いや, うちはさん付けにはしています」ということは結構聞いたのですが，多分，ブレーンストーミングをやるところでファーストネームで呼ぶことはほとんどないのではないかと思います.「ギャル式ブレスト」もブレーンストーミングの形式で，話題になりましたが，どんな状況なのでしょうか？　国内で心理的安全性の推進で，非常に難しいのは，ファーストネームで呼ぶという習慣がなく，社長だって役員だってみんなファーストネームで呼べということが難しいからです.

9. セキュリティ心理学会へのお誘い

現在，日本セキュリティ心理学会を作って，実行することで考えていますので，興味があれば，ぜひ．今，情報システム学会と提携しようと提言をしていますが，セキュリティ心理学を考える人たちが増える必要があると思っています．以上です．ありがとうございました.

（文責：編集委員会）