月例会の内容について

情報セキュリティ心理学研究

２０１６年度

１．情報セキュリティへのヒューマンファクターズ分析評価手法の適用　（その 2）

日　時：　2016 年 04 月 22 日

報告者：　五郎丸 秀樹

内　容：　標的型攻撃メールや内部関係者による情報漏えいが話題となっている．これらの人間の行為によって発生する情報漏えいの分析に，ヒューマンエラーの防止を含む学問分野であるヒューマンファクターズの分析評価手法を適用することが考えられる．

ヒューマンファクターズの分析評価手法を情報セキュリティに適用するには分析評価手法の特徴を理解した上で選別する必要があるが、分析評価手法は 50 以上存在し，業界ごとに個別の発展を遂げているが，網羅的にかつプロセスごとに分析評価手法を分類したものはなかった．

そこで各分析評価手法のプロセスのうち“要因と対策”および“対策前と対策後”に着目し，各業界で使われているヒューマンファクターズの分析評価手法を分類したところ，要因分析は対策分析に比べ多くの手法があることが判った．また情報セキュリティに適用するために，分析評価手法の問題点と課題を取り上げ，今後の進め方について検討する．

２．ｅラーニングをモデルとした 内部犯行の予測因子の識別

日　時：　2016 年 05 月 13 日

報告者：　新原 功一（明治大学大学院　博士課程）

内　容：　昨今、組織に深刻な影響を与える内部不正への対策は非常に大きな課題である．内部不正は様々な要因によって引き起こされるが、職場環境において適切なマネジメントが行われていないと、内部不正を招くことがある。

また、最近の研究によると、システムへのログイン ID を共有すると不正者の特定ができないため、内部不正が発生しやすくなるといわれている.しかし、これらの要因が内部不正を誘発する影響の度合いについては明らかではなかった。

そこで、クラウドソーシングで集めた被験者ごとに異なる内部不正誘発要因を発生させ、筆者らが構築した疑似環境にて被験者が行った各作業にて発生する不正事象の数を観測した。測定結果を統計解析の手法を用いて分析し、誘発要因と不正事象の相関関係を明らかにした。

３．ソーシャルエンジニアリングトレーニング参加報告

日　時：　2016 年 06 月 24 日

報告者：　内田 勝也

内　容：　米国 SANS（国内は NRT セキュアテクノロジー）の教育・訓練の１つに、「SEC567 ソーシャルエンジニアリング」（2 日間）が、新たに開催されますので、

参加しましたので、その参加報告です。

2012 年 11 月に、Chris Hadnagy の「Social Engineering Penetration Tester」（５日間）に参加し、その報告を 2013 年 01 月の研究会で報告をしました。 Chris は、今でも英国での教育・訓練と BlachHat（Las Vegas)で、５日間の教育・訓練を行っています。

今回の SANS の教育・訓練は、２日間の教育・訓練ですが、国内の SANS 教育・訓練でも、今後、開催される可能性がありそうですが・・・

SANSFIRE 2016 （SEC567）

https://www.sans.org/event/sansfire-2016/course/social-engineering-for-penetration-testers

４． 事故とヒューマン・組織のモデル

日　時： 2016 年 07 月 29 日

報告者： 氏田　博士（環境安全学研究所）

内　容： ① 事故とエラーのモデルと人間特性、 ② レジリエントシステム、 ③ レジリエンス分析グリッドと良好事例

2016 年 6 月に「銀行における安全文化の醸成についての考察」と題した修士論文の研究発表がありましたが、当時は、一部の学者から、セキュリティ分野にレジリエンスは関係ないとの指摘があったと聞いています（本研究会内ではありません)。

今回は、長年、原子力関係の安全の研究からの報告

５． 起こり得る危ういことを正しく想定できるか

日　時： 2016 年 08 月 18 日

報告者： 福田　健（清泉女子大学）

内　容： セキュリティの問題は、単一の問題空間を、自己（防御側）と他エージェント（攻撃側）とが共有しながらも、自己と他エージェントが別々の目標状態を目指して、それぞれが可能な操作（行動）を選択していく問題解決活動として抽象化できる。

こうした複数エージェント間で問題構造共有・目標非共有という特性をもった問題解決においては、自己の目標状態に即した状態評価と他エージェントの目標状態に即した状態評価の両方を同時並置しながら、状態探索・操作選択を進める必要がある。

要するに、自己（防御側）にとっての「次の最善手」は、他エージェント（攻撃側）にとっての「その次の最善手」を想定した上でこそ判断できる、という再帰性をもった読み込みが求められる。

こうした自己と相手との間での再帰性をもった選択肢の読みあいは、セキュリティ問題に限らず、戦争から、国家外交、スポーツ、ゲーム、企業経営、他者との素朴

な駆け引きまで、多くの場面で見られるものであり、人が得意とする知的振る舞いの一要素として捉えられてきた。

しかしながら、最近の心理学研究を眺めると、そうした「自分勝手にいかない未来予測」について、本質的には、人が苦手である、エラーが多い、バイアスがかかっているなどのことが読み取れる。

今回は、こうした「自分勝手にいかない未来予測」を中心に、人の未来予測の困難性の問題について整理し、それをどのような枠組みで捉えることができるかを提案し、また、補うことができるかについても考えてみたい。

６．Blackhat USA 2016 参加報告

日　時：　2016 年 09 月 16 日

報告者：　荒木　粧子（(株）ソリトンシステムズ）

内　容：　Blackhat USA 2016 では、AI、IoT に加え、Human Factor のセッションが多く見られました。心理学的なアプローチによる研究も複数発表されており、Weakest Link である「人」に、いかにパッチをあてるのか？　という議論がにぎやかになってきた感があります。

特に印象に残った以下のセッションです。　これらを中心にご報告します。

- EXPLOITING CURIOSITY AND CONTEXT: HOW TO MAKE PEOPLE CLICK ON A DANGEROUS LINK DESPITE THEIR SECURITY AWARENESS
  https://www.blackhat.com/us-16/briefings.html
- BLUNTING THE PHISHER'S SPEAR: A RISK-BASED APPROACH FOR DEFINING USER TRAINING AND AWARDING ADMINISTRATIVE PRIVILEGES
  https://www.blackhat.com/us-16/briefings.html

７．セキュリティ心理学を俯瞰する

日　時：　2016 年 10 月 14 日

報告者：　内田　勝也　（情報セ大学院大学）

内　容：　人的セキュリティを考えると、まず、ソーシャルエンジニアリングを考えがちであるが、孫子の「敵を知り、己を知る」ことが大切であるが、「己」を単に個人だけでなく、チームや組織まで敷衍することが可能です。

最近の研究会では、各論的な報告を取り上げてきましたが、今回は、セキュリティ心理学全体として、何を考える必要があるかの報告です。

８．セキュリティ文化の構築を考える

日　時：　2016 年 11 月 25 日

報告者：　内田　勝也　（情報セ大学院大学）

内　容： ネットワークを中心とした情報通信システムでは、技術的なセキュリティ対策が中心になりがちであるが、人的面の対応も大切だが、教育・訓練などの重要性の認識が低い、あるいは、どの様な教育・訓練を行うかの理解が少ないのではないかと感じます。

今回は、ソーシャルエンジニアリング的な手法により、ネットワークに侵入した（内部犯行的要素もあるが）ことと、基礎的、実践的セキュリティの知識の低さが、大きな事件を引き起こしたと考えることができます。

セキュリティ心理学の主要な部分とも言える「セキュリティ文化」を再考してみたいと考えています。

９．監査（Audit）を考える　～ ITAC 2016 参加報告と監査／Audit を考える ～

日　時： 2017 年 01 月 27 日

報告者： 内田 勝也　（情報セ大学院大学）

内　容： 2016 年 12 月上旬に開催された ITAC 2016 の参加報告を中心に報告を行います。

「IT 監査&コントロール」と聞くと，すぐに「システム監査」とのイメージがあります。国内では，1980 年代の初めにシステム監査の勉強会があり，1984 年 12 月に EDPAA（EDP Audit Association）東京支部が設立されました（1994 年に，ISACA に名称変更）。

前回（2014 年）ITAC に参加して感じたのは，従来のシステム監査的ではなく，サイバーセキュリティに対するこのトロール，サイバーセキュリティ／監査のリスク等の内容が多くなってきました。

この辺りは，今回も大きな動きはありませんでした。

１０．欺術（騙しのテクニック：数字で騙す／騙される）

日　時： 2017 年 03 月 01 日

報告者： 内田 勝也　（情報セ大学院大学）

内　容： 多くの場合，数字で示されると 正しいと考えがちですが，本当に，正しいものか考えてみる必要があります。

結果だけ見て，正しいと判断するのではなく，元のデータ自体やデータ収集方法などが正しくなければ，結果は正しくありません（Garbage in garbage out）。最近はやりの「ビッグデータ」でも，どの様にデータを集め，分析したかを考えないと，「騙される」こともありそうですが・・・