

1. 情報セキュリティを支える心理学の基礎知見

(1) 意思決定に関わる研究プログラムから

日 時： 2013 年 4 月 22 日

発表者： 福田 健

内 容： 情報セキュリティ心理学を考える上で、心理学の知見からみた考え方の報告です。

2. InfoSec World 2013 参加報告

日 時： 2013 年 5 月 29 日

発表者： 内田 勝也

内 容： InfoSec World は、2001 年から始まっているが、それ以前は異なる名前で開催していた。ただ、3 月末から 4 月上旬に開催されてきたことと CSI(Computer Security Institute <http://www.gocsi.com/>)に参加することしか考えなかったため、気づかなかつた (CSI の Conference & Expo は 2011 年以降中止になった)。

InfoSec World の基本的コンセプトは、CSI と同様、技術だけでなく、マネジメント、リスク、コンプライアンス等の分野もカバーしている。

今回は、1 日の Pre-Conference と 2.5 日の Main Conference (2 日間の Expo) に参加した。米国での情報セキュリティの潮流が大きく変化してきているのを感じた。その特徴を一言で言えば、情報セキュリティ分野が、技術だけでなく、「人間、文化創造」にも注視してきているのを感じた。情報セキュリティの新たな潮流について報告した。

3. 銀行における安全文化の醸成についての考察

日 時： 2013 年 6 月 28 日

発表者： 持田 恭子

内 容： 想定外／想定内の状況に対しても必要な動作を維持することができる能力をレジリエンスと呼んでいる。

最近のサイバーセキュリティ分野では、技術だけでは限界があり、組織文化を変える (構築する) ことが大切であるとの考えが海外を中心にでてきている。4 月の本研究会で報告した「InfoSec World 2013」では、文化の重要性を 2 人の基調講演者が述べており、6 月 5 日～6 日に開催された「RSA Asia 2013」でも、技術だけの対応でなく、組織文化の必要性を述べていた基調講演者もあり、セキュリティ文化／サイバー文化の醸成が重要になってきている。

今回は、銀行における安全文化を考慮した修士論文を執筆している社会人学生に、修論の研究の報告を行った。IAEA (国際原子力機関) の「Safety Culture」の考え方や「レジリエンス」の考えを、セキュリティ分野に取り入れたもの。

なお、今回は、(一般社団法人) [経営情報学会「官の情報システム」研究部会](#)¹と共同主催の研究会です。

4. レジリエンスエンジニアリングについて

日 時： 2013 年 8 月 5 日

発表者： 北村 正晴 (東北大学名誉教授)

内 容： 大規模システムでのレジリエンス/レジリエンスエンジニアリングについて研究を行っている事柄についての報告。

5. 日本心理学会 第 77 回大会 参加報告

日 時： 2013 年 9 月 26 日

発表者： 内田 勝也/福田 健

内 容： 9 月中旬 (19~21 日) に開催される日本心理学会 第 77 回大会の参加報告。公募シンポジウムとして、「情報セキュリティ心理学研究 2013」の内容報告及び、ポスター展示等、大会の様子の報告。

6. ソーシャルエンジニアリング

日 時： 2013 年 10 月 31 日

発表者： 木村 英樹

内 容： 今年 5 月に開催された Chris Hadnagy (クリス・ハドナジー「ソーシャルエンジニアリング」 日経 B P 社 の著者) のセミナーを中心に、ソーシャルエンジニアリングについての話題提供です。

7. 電子投票における情報セキュリティ対応

日 時： 2013 年 11 月 27 日

発表者： 宮川 龍一郎

共 催： 経営情報学会特設研究部会 「官の情報システム」

内 容： 国内では政治にコンピュータを利用する機会が非常に少ないですが、今年 (2013 年) 4 月、岡山県新見市で電子投票が行われた。

電子投票は、第 1 世代 (投票所投票：スタンドアローン型)、第 2 世代 (投票所投票型、オンライン集計型)、第 3 世代 (インターネット投票方式) がありますが、新見市は、第 1 世代の電子投票方式を採用したが、投票での都市伝説 (ウソ、誤解等々、心理学的な面も含め) について、現実の投票で判明したこと等の報告がされた。

今後、更に 電子投票の推進を行う上での、セキュリティ上の課題や心理学的な不安、誤解などについて、今回の電子投票を推進した 宮川氏からの報告と参加者との意見交換を行った。

なお、今回は、(一般社団法人) [経営情報学会「官の情報システム」研究部会](#)と共同

¹ (一般社団法人) 経営情報学会 研究部会 http://jasmin.jp/activity/kenkyu_bukai/index.html

主催の研究会です。

8. ITAC 2013 参加報告

日 時： 2013 年 12 月 19 日

発表者： 内田 勝也

内 容： ボストンで行われた ITAC 2013 Conference (2013.11.18~21 + 22) の参加報告。

ITAC は IT Audit & Control conference の略だが、開催されてセッションの多くは、セキュリティ関連であり、Post Conference で、"Ethical Hacking" もあり、これに参加した。

国内でも、大手企業や官公庁に標的型攻撃が猛威を振るっているようだが、米国でも、同様に、現在の最大の懸案事項だとの話を何人かのプレゼンター、参加者からあった。セキュリティの最大の脆弱性である人間、特に経営者などのトップ層を狙う標的型攻撃は技術では対応できず、心理学や行動科学の知見を使った教育・訓練等の重要性が増してきている。

この面からも、本情報セキュリティ心理学研究会の意義は大きくなってきていると言える。

9. ケース方式によるソーシャルエンジニアリング／ヒューマンエラー対策（その1）

日 時： 2014 年 1 月 22 日

発表者： 内田 勝也

内 容： 国内でも人間の心理的な弱さを狙った「ソーシャルエンジニアリング」による犯罪が顕在化しており、今後、更に増えるものと思われる。

実際、自治体で発生したソーシャルエンジニアリング攻撃では、漏れた情報により、ストーカーの被害者が殺害されてしまった。

今回はこの例をケースとして、どのような課題があり、これを防ぐには何を行えば良かったかを参加者と一緒に検討した。

新しい試みを行ったが、多くの意見があり、話題性の高いケースであり、大いに議論も盛り上がった。

10. ケース方式によるソーシャルエンジニアリング／ヒューマンエラー対策（その2）

日 時： 2014 年 2 月 10 日

発表者： 内田 勝也

内 容： 前回と同様、実際の例をケースとして、どのような課題があり、それを防ぐには何を行えば良かったか等について、参加者と一緒に検討した。

今回は、個人情報を含む USB メモリーの紛失とパスワード保護されたフォルダー内のファイルをご送信したケースを取り上げた。

多くの意見高官ができ、参加者にとっても、有益な時間を過ごすことができた。

1 1. RSA Conference 参加報告

日 時： 2014 年 3 月 25 日

発表者： 内田 勝也

内 容： RSA Conference 参加報告

2 月 24 日（月）～28 日（金）に 米国サンフランシスコで情報セキュリティ最大の国際会議「RSA Conference 2014」が開催されたが、今年から、Human Element（人的セキュリティ）というセッションが新たに設けられた。

Human Element は、25 日（火）～28 日（金）までにあったが、このセッションでの 1 つに、ポスターやビデオ、ニュースレター等による「Security Awareness training（セキュリティ周知教育）」が十分機能していない、そのため、心理学、行動科学等の知見を利用した新しいセキュリティ周知教育の必要性を述べていた。

他は、最近国内でも機密情報を持ち出し、退職後にその情報と一緒に自分を他社に売込むことが発生したが、機密情報を持ち出す「内部犯行」のタスクフォースが組織化されている。

教育・訓練の有効性評価については、数値化しやすい例、例えばフィッシングメール等では簡単にできるが、それ以上になると今後の課題だと言わざるを得ない状況だとか。

(以上)