

2015 年度月例会の概要

情報セキュリティ心理学研究
代表： 内田 勝也

2015 年度

1. 日 時 2015 年 04 月 17 日

テーマ 情報セキュリティからみたストーカー殺人事件
～ ソーシャルエンジニアリング的分析 ～

発表者 内田 勝也 (情報セ大学院大学 名誉教授)

概要 自治体を持つ住民の基本 4 情報の「氏名」、「住所」、「性別」、「生年月日」の一部の漏えいは、多くの自治体にとって、必ずしも、深刻な問題ではなかった。しかしながら、今回発生したストーカー殺人事件では、被害者の夫になりすました 調査会社の経営者の電話での依頼を自治体職員が回答したため、被害者の住所がストーカーに渡り、殺人事件に発展した。個人情報の一部が漏れ、それが殺人に発展した事例は世界的にも稀有な事例と思われ、この事件を 心理学的な分野から考えてみたい。

2. 日 時 2015 年 05 月 22 日

テーマ ヒューマンエラーの考察
～ 個人特質から組織エラーへの考察 ～

発表者 内田 勝也 (情報セ大学院大学 名誉教授)

概要 情報セキュリティ分野でも、ヒューマンエラーへの対応は重要なものの 1 つだが、
ヒューマンエラー = 個人資質
と考える傾向が日本では強い感じを受ける。
緊張感がないからエラーをすると叱責を受けたこともある。
しかし、なぜ、緊張感が保てないのか？ なぜ、過ちを犯すのかといった原因を追究していくと、単に個人の問題よりも、その組織の問題の方が大きいことがわかっている。
個人がエラーを起こさない仕組みを考えることが、組織にとって重要になってきている。
今回は、単なる「ヒューマンエラー」を考察するだけでなく、組織としてヒューマンエラーをなくす仕組みを考えることの重要性を事例から考察する

3. 日 時 2015 年 07 月 03 日

テーマ ヒューマンエラーの考察 (その 2)

発表者 内田 勝也 (情報セ大学院大学 名誉教授)

概要 情報セキュリティ分野でも、ヒューマンエラーへの対応は重要なものの 1 つだが、
ヒューマンエラー = 個人資質によるエラー
と考える傾向が日本では強い感じを受けます。
ミスをしたのは、「君に緊張感がないからだ！」なんて言われたりします。 非常勤だったりすると、来月から来なくていいよなんて言われることもあります。

4. 日 時 2015 年 08 月 21 日

テーマ ソーシャルエンジニアリング欺術 (その 1)
～ Elicitation/Open & Closed Question ～

発表者 内田 勝也 (情報セ大学院大学 名誉教授)

概要 情報セキュリティ心理学を考える上でも、ソーシャルエンジニアが使う欺術を考えることも大切で、必要な情報を引き出す手法に、Elicitation (誘導質問術) があり、そのきっかけを作る Open & Closed Question がある。
ソーシャルエンジニアの使う欺術について考えてみた。

5. 日 時 2015 年 09 月 18 日

テーマ 標的型攻撃に対するセキュリティ心理学/マネジメントからの考察

発表者 内田 勝也 (情報セ大学院大学 名誉教授)

2015 年度月例会の概要

情報セキュリティ心理学研究

代表： 内田 勝也

概要 年金機構では、標的型攻撃により、大量の情報漏えいが発生した。 標的型メール攻撃は、特定の企業や個人が興味を持つテーマやメッセージを持つ電子メールを送り、受信者が添付ファイルやメッセージ内のリンクをクリックしたため、不正なプログラムが実行される。

これらの攻撃は、受信者の心理をついたソーシャルエンジニアリング攻撃の一種である。 この様な攻撃に対し、技術だけでなく、人的な対応（セキュリティ心理やセキュリティマネジメントの知見を利用した対応）も含め、包括的なセキュリティ対策を考える必要がある。 実際、技術的セキュリティ対策でも、人的セキュリティ対策でも、100%完璧な対策がないとすれば、「多重防御」を考えることが大切になる。

今回は、この様な観点から、セキュリティ心理学、セキュリティマネジメントを考察します。

6. 日時 2015年10月16日

テーマ セキュリティ教育はセキュリティ対策行動を促進しない

発表者 坂本 倫子（法政大学 人文科学研究科 心理学専攻 修士）

概要 セキュリティ教育によりセキュリティ対策行動は強化され、その結果として、インターネットトラブルは防げているのかについては疑問の余地が残る。セキュリティ対策行動を強化し、インターネットトラブルを減らすための有用なセキュリティ教育に関する示唆を得るため、本研究ではセキュリティ教育の実情把握と、セキュリティ教育はセキュリティ対策行動を促進するのかという検討を行った

7. 日時 2015年11月13日

テーマ セキュリティ教育・研修評価を考える

発表者 内田 勝也（情報セ大学院大学 名誉教授）

概要 標的型攻撃を始め、技術的なセキュリティ対策だけでは対応できなくなっており、セキュリティ教育・訓練の重要性が高まってきたが、海外では、セキュリティ教育・訓練に関し、その方法に疑問を指摘する実務家もでてきた。

一方、国内では、セキュリティ対策については、技術対策中心であり、教育・訓練について必ずしも十分でないように感じる。 その理由に、教育・訓練を行っても効果を感じられないと言った声もある。 参加者全員に対し、教育・研修が効果的に対応できる訳ではないが、技術的セキュリティ対策も 100%完全なものはない。

セキュリティ教育・訓練の効果をどの様に考えるかの考察を行い

8. 日時 2015年12月18日

テーマ 情報セキュリティ教育・訓練（その3）対象者を考慮した質問術の考察

発表者 内田 勝也（情報セ大学院大学 名誉教授）

概要 外部監査等では、「最新の OS を使っていますか？」と言ったクローズドな質問をする監査人がいる。 この様な質問には、「はい」と回答が返ってくることがある。 報告者を含め、一部の人は、XP（古い Windows の OS）を使っている、「はい」と言う。 監査人に指摘されたら、「XP が最新の OS だと思っていたから」と回答する。 この様な課題は、このほかにも多くの分野で見られます。 実例を紹介しながら、考察をします。

9. 日時 2016年01月22日

テーマ 再「情報セキュリティを測定しよう！」

発表者 中島 浩光（マインド・トゥー・アクション）

概要 2007年11月に「情報セキュリティを測定しよう！」のテーマで、某セキュリティ団体で報告したものを、現在に再度見直しをした。 情報セキュリティ測定には、PDCAのC段階が必要になるが、なかなか光が当たらないこの部分を考察する

2015 年度月例会の概要

情報セキュリティ心理学研究

代表： 内田 勝也

10. 日 時 2016 年 02 月 26 日

テーマ 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

発表者 五郎丸 秀樹（日本電信電話株式会社）

概要 標的型メール攻撃や内部者の情報漏えいが話題となっており、これら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（以下、HF）の分析評価手法の適用が考えられる。

HF 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、選択する必要があるが、分析評価手法は 50 以上あり、業界別に個別発展しており、網羅的、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 HF 分析評価手法を分類したが、要因分析は対策分析に比べ多くの手法があり、情報セキュリティに適用するため、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。

11. 日 時 2016 年 03 月 18 日

テーマ RSA Conference 2016 参加報告

発表者 内田 勝也（情報セキュリティ大学院大学 名誉教授）

概要 世界最大のセキュリティ国際会議でも、「Human Elements」のセッション等で人間に関係する問題の報告が行われており、それらを中心に参加報告を行った。

(以上)