情報セキュリティ心理学研究会
《 2017 年度 月例会概要 》

１． 共有アカウントは内部不正を誘発するか？

日　時： 2017 年 04 月 21 日

報告者： 新原 功一

内　容： 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言われている．しかし共有アカウント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に匿名 ID と個別 ID をランダムに払出し，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する．本研究は実験結果を報告し，共有アカウントと内部不正の関係を明らかにする

２． InfoSec World 2017 報告

日　時： 2017 年 05 月 26 日

報告者： 内田　勝也

内　容： ４月初旬に開催された InfoSec World 2017（米国 フロリダ，オーランド） へ参加しましたので，その報告です。

ソーシャルエンジニアリング等のエンド･ユーザを対象とした心理的な攻撃に対する教育・訓練等が米国でも重要な課題になっています。

また，本研究会でのマネジメント系のセキュリティ心理学ではなく，国内でも 行動科学的な考察をマルウェア対策に考えることが盛んになってきましたが，このような流れも盛んになってきました。

毎年参加している InfoSec World の一端をセキュリティ心理学的な部分からの考察です。

３． Human Error Once More ～ セキュリティ心理学 ～

日　時： 2017 年 06 月 23 日

報告者： 内田　勝也

内　容： 国内外のセキュリティ調査をみても，ヒューマンエラー（人的エラー）は，常に上位をしめている。 更に，サーバーへの攻撃や最近の標的型攻撃では，設定ミス，パッチ未適用，ソーシャルエンジニアリング等による攻撃が多発しています。

しかし，ヒューマンエラーやソーシャルエンジニアリング対策を考える組織は少ないように感じますが，それは，エラーを起こした人 ひとりの問題だと考えているのではないだろうか？

「緊張感を持っていない」とか「操作をきちんと覚えないからだ」とかエラーが発生すると，多くの叱正やコメントがでてくるが，根本原因を考えてみる必要はないのだろうか？

ヒューマンエラーを単純問題と考えている限り，ヒューマンエラーはなくならないのではないだろうか？ ヒューマンエラーをもう一度考えてみたい

４． セキュリティ心理学研修事例の紹介 ～ ストーカー殺人事件 誘導質問術対応 ～

日　時： 2017 年 08 月 02 日

報告者： 内田　勝也

内　容： 2012 年 11 月に発生したストーカー殺人事件で，加害男性は被害女性の結婚後の名字や転居先市名を脅迫罪執行時に警察の逮捕状読み上げで知ったが，詳細な住所を知ることはできなかった．　しかし，加害男性は詳細な住所調査を依頼し，調査会社の経営者は被害女性の住所を聞き出すため，被害女性の夫を装い，当該自治体に電話し，対応職員から正確な住所を聞き出した．

個人情報漏えいから殺人事件に発展した事例は，コンピュータ犯罪史上初めてと思われる．

電話照会で大量の個人情報漏えいに至ることはなく，大きな事件・事故に繋がらなかった．

自治体職員は電話照会で個人情報を教えた記憶がないと述べており，真相は不明だが，この経営者が大量の個人情報を保持し，自治体へ頻繁に電話をかけていたことを考えると高度な誘導質問術を駆使した可能性は高い．

今回は，ソーシャルエンジニアの主要手法である誘導質問術等の観点から情報漏えいやその対応策としての教育・訓練を考える

５． セキュリティ文化とレジリエンスの考察

日　時： 2017 年 10 月 06 日

報告者： 内田　勝也

内　容： 2002 年に，OECD（経済協力開発機構）は，理事会の勧告として情報システム及びネットワークのセキュリティのためのガイドライン

～ セキュリティ文化の普及に向けて ～

を公表した。

セキュリティ文化の普及を掲げているが，

１．個人的な対応でセキュリティを確保するのではなく，「セキュリティ文化」を確立することは，組織としてセキュリティ対応を行うことの重要性の認識があった。

２．1991 年に IAEA(国際原子力機関）が，1986 年のチェルノブイリ原発事故に関連し，「Safety Culture：安全文化」を発表した。

OECD は，情報セキュリティを個人に問題として考えるのではなく，組織の問題として捉えることの重要性を，2002 年のガイドラインの述べたのはないかと考えている。

セキュリティ・レジリエンス（復元力）は，事件・事故からの復旧を考えた対応の重要性をセキュリティにも求めており，この考えは，CMMi(Capability Maturity Model Integration，能力成熟度モデル統合)が，『システム開発を行う組織がプロセス改善を行うためのガイドライン』をカーネギーメロン大学 SEI（Software Engineering Institute）が発表したが，これらの考えも，「組織として根本的な原因を探り，問題を未然に防ぎ，それらの施策の効果を定量的に評価し，継続的な改善を実現するものだと言われています。

６． 不作為によるヒューマンエラーを考える

日　時： 2017 年 10 月 27 日

報告者： 内田　勝也

内　容： 国内では，ヒューマンエラーを【個人によるインシデント】と捉えがちですが，本来は 【組織エラー】と考える必要があります。

情報セキュリティでは，内外の人間による【故意】から情報を守ることも，重要な事柄になっています。

現在の情報セキュリティ・インシデントの多くは【設定ミスやパッチ未適用】や【利用者への標的型攻撃】だと考えています。

このことは，

１．設定ミスやパッチ未適用 の多くは 防御側（組織や個人）の不作為（何もしなかった）によるものと考えることができます。　また，

２．利用者への標的型攻撃では，利用者への組織的な教育・訓練の未熟さによると考えると，【組織エラー／組織事故】と考えらます。

このための対応として，

① 技術

② 処理手順

③ 人間（心理的脆弱性）

の三側面から考える必要がありますが，人間の部分，即ち，【不作為によるヒューマンエラー】を考えてみたいと思っています

７． SANS 433： Securing The Human 参加報告

日　時： 2017 年 11 月 24 日

報告者： 内田　勝也

内　容： 海外のセキュリティ分野は，利用者への教育・訓練に関して，複数の企業がサービスを提供していますが，９月末にシカゴで開催された，SANS 433「Securing The Human」は，人的セキュリティを推進する人達を対象とした２日間のワークショップに参加しました。

このコースでは，利用者教育・訓練カリキュラムの作成，維持，評価をどの様に行うかについてのコースでした。　カリキュラムでは，組織における「セキュリティ文化の醸成」を最終目標としており，そのために必要な内容を各段階（５段階）で目標を構築することをめざしています。

当然ですが，利用者教育・訓練でも，インシデント発生毎に場当たり的な教育・訓練や通達発信を行うことが有効ではないことは明らかです。

今回は，このコースの概要の報告です。

８． 情報、情報システム、安全工学 そして、ソーシャルエンジニアリング ～ セキュリティ心理学を考える ～

日　時： 2018 年 01 月 19 日

報告者： 内田　勝也

内　容： 今回は、いくつかのテーマについて何を考えてきたかの報告

- 情報： 情報とは？　情報資産とは？
- 情報セキュリティ：　情報セキュリティ？　サイバーセキュリティ？
- ヒューマンエラー：　人のエラー？　組織事故？　責任は？
- セキュリティ心理学：　情報セキュリティ心理学？　セキュリティ心理学？
- セキュリティ文化：　セキュリティ文化とは？
- セキュリティ心理学：　情報セキュリティ心理学？　セキュリティ心理学？

９． 拡大研究会： ワークショップ

日　時： 2018 年 03 月 02 日

報告者(1)： 新原 功一

テーマ： 内部不正による情報漏えいを誘発する要因に関する研究

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。

報告者(2)： 西本 実苗

テーマ： 総務省「通信利用動向調査」にみる震災とソーシャルメディア利用

内　容： 2011 年の東日本大震災を機に、災害時のソーシャルメディア利用に注目が集まった。本稿では総務省「通信利用動向調査」の統計表データを分析することにより、ソーシャルメディア利用における震災の影響および災害とデジタル・ディバイドもしくは“ソーシャル”・ディバイドについて探索的に検討する。

報告者(3)：　内田 勝也

テーマ： セキュリティ心理学について

内　容： 国内でもサイバーセキュリティの傾向は、サーバーへの攻撃から、利用者への攻撃が増えてきた。　少数のサーバーへの攻撃と多数の利用者への攻撃を比べれば、当然であろう。　ソーシャルエンジニアリング欺術が益々高度化してきた。　それへの対応を考える必要があるが、20002 年に OECD のセキュリティガイドラインでは「セキュリティ文化の確立」を表明したが、残念ながら、国内ではあまり省みられなかった。しかし、現在のサイバーセキュリティを考えると、心理学や行動科学、犯罪学等を考え、理論と実践を踏まえた「セキュリティ心理学」が重要であろう。