情報セキュリティ心理学研究会

《 2020 年度 月例会概要 》

１．RSA Conference 2020 参加して

日　時　2020 年 5 月 29 日

報告者　内田 勝也

概　要　1991 年 「Cryptography, Standards & Public Policy」として、主に暗号関係者の国際会議として始まった。RSA は 公開鍵暗号の１つで、３名の暗号研究者（R： Rivest、 S：Shamir、A：Adleman）の頭文字から名付けられました。

当初は、暗号関連のセッションが中心で、「RSA Data Conference」であったが、その後、「RSA Conference」になりました。2010 年頃から、暗号関係以外のセッションも行われるようになりました。

更に、海外でも会議が行われ、現在は、USA, United Kingdom, Asia & Japan, United Arab Emirates で開催されています。

人間を対象とするセッションも毎年増えていましたが、今年のメインテーマは、『Human Element』になりました。 そこで、今年度初回のセキュリティ心理学研究会の報告は、米国 サンフランシスコで開催された RSA Conference 2020 の参加報告としました

２．メンタルヘルスを考える

日　時　2020 年 6 月 26 日

報告者　内田 勝也

概　要　RSA Conference 2020 の報告でもメンタルヘルスのセッションがあったことを紹介しましたが、RSA Conference の前週に開催された『The Human Hacking Conference』 でも、メンタルヘルスのセッションがありました。 心理学の一分野として、メンタルヘルスがありますので、セキュリティ心理学でも取り上げて良い話題ではないかと思っています。

勿論、個人的にメンタルヘルスに関し、深い知識を持っている訳ではありませんので、紹介レベル（入門以下？）になります。

３．ヒューマンエラーを考える

日　時　2020 年 07 月 31 日

報告者　内田 勝也

概　要　２年程前にも、ヒューマンエラーの報告をしました。 同じような内容になる可能性もありますが、今回『テレコンファレンス』での報告です。 なお、前回の概要は以下の通りです。

安全工学やヒューマンエラーでは、「第三者の悪意」を考えなかったが、サイバーセキュリティでは、第三者（外部・内部）による悪意への対応がその中心にある。

サイバーセキュリティ攻撃は、高度な技術を持った攻撃者が華麗な技術を

使うと考えがちだが、現実世界の「空き巣被害」と同じだと考えています。 即ち、無施錠とガラス破りが ８０％ 程度あり、「不作為」が犯罪の原因です。これは、やるべきことを行わなかった（不作為）ため、そこ（脆弱性）を定めた攻撃が、インシデントの原因だと考えることができる。

本報告では、ヒューマンエラーを単なる行為者の行い（不作為や作為）として捉えるだけでなく、それらの行為により、セキュリティ・インシデントが発生する可能性があり、その対応を含めて考えてみたい。

４．インテリジェンスを考える

日　時　2020 年 08 月 28 日

報告者　内田 勝也

概　要　インテリジェンスとは、情報（即ち、観察、報告、噂、画像等、あらゆる種類の資料で、未だ評価・加工されていないもの）を収集、加工、統合・分析・評価・解釈した成果物である

情報は、人、物、場所等、多くの所にあり、人間による収集、技術による収集があるが、公開情報の収集、非公開情報の収集等、収集対象の状況も考える必要がある。　更に、情報自体が『意図的に公開』されている、『無意識に情報を公開』したなど、色々な状況がある

孫子の『敵を知り、己を知る』ことの重要性を考えてみたい

５．セキュリティ心理学 ～ セキュリティと Human Element ～

日　時　2020 年 09 月 25 日

報告者　内田 勝也

概　要　人間は最大の脆弱性ではなく、最初の攻撃対象であり、また、多くの攻撃の対象に人間がなっていることが原因と考えています。 心理的な攻撃でも、多くの状況が考えられます。

今回は、【だまし】と【物理的セキュリティ】 の報告です。

だまし は、人が人をだますだけでなく、多くのケースがサイバーセキュリティではあります。

物理的セキュリティは、建物への侵入や物理的な事故もあります。

【敵を知り、己を知れば・・・】

６．セキュリティ心理学　～セキュリティ心理学における教育・訓練環境を考える～

日　時　2020 年 10 月 30 日

報告者　内田 勝也

概　要　個人的には『教育・訓練 ＝　グライダー』と考えている。　グライダーは始め誰かに牽引して貰う必要があるが、一定レベルに到達すれば自力で空を滑空できる。　教育・訓練も同じと考えている

自分の講座の説明は非常にやさしいが、終了後、記憶に残らないと言った教員もいたが、逆に 高名な研究者であったが、講座は何を言っているかさえ分からない講義もあった

今回は、情報セキュリティ／サイバーセキュリティ分野の教育・訓練を行う環境を考えてみた。 教育・訓練が臥薪嘗胆であって欲しくない。 そのため、教科書・参考書やインストラクター、教え方、機材、教育・訓練環境等を考える必要があり、教育・訓練方法、環境、資料等の工夫も必要であろう

７．セキュリティ心理学から地政学を考える

日　時　2019 年 11 月 27 日

報告者　内田 勝也

概　要　「地政学」は、地理・歴史と政治に関する学問と言われるが、個人的には、もう少し広く考えている。

即ち、地理・歴史と政治だけでなく、宗教も大きな影響を及ぼしている。 また、2001 年 9 月 11 日の『アメリカ同時多発テロ事件』以降、「テロ」と「戦争」を区別が難しくなっている。

更に、ネットワークの進展は、企業・組織だけでなく、電子政府の構築が多くの国々で行われており、サイバー攻撃は企業・組織だけでなく、電子政府への攻撃も行われている。

従来、戦争は、必ず『宣戦布告』で戦争が始まると言われてきたが、サイバー攻撃は、宣戦布告なしに攻撃されるため、サイバーセキュリティでは、その対応が必要になる。

８．ロシアの軍事ドクトリンとサイバー活動に対する米国報告についての一考察

日　時　2020 年 12 月 18 日

報告者　瀧野 修

概　要　サイバー活動と地政学的要素について米国において分析されたレポートを元に、サイバー活動と社会事情、表面化した OSINT 情報の関係性について考察を行う

９．テレワークの歴史的背景と課題

日　時　2021 年 1 月 29 日

報告者　五郎丸　秀樹

概　要　COVID-19 パンデミックによりテレワークは世界的に普及し、今後ニューノーマルの中で定着していくことが予想される。30 年以上前からからテレワークは推進されてきたが、これまで普及が進まず定着するまでには至らなかった。

感染症（2003 年の SARS）への対応により中国の DX が進んだ事例や、IBM や Yahoo がテレワーク推進から廃止へと切り替えた事例などテレワークの歴史

的背景を述べ、様々な観点（技術、コスト、セキュリｗティ、心理、健康、発想など）から、これまでのテレワークの問題や課題について述べていく。

10. セキュリティ月間　ワークショップ　(WebEX によるオンラインワークショップ)

日　時　2021 年 03 月 12 日

報告者 及び 報告テーマ

内田 勝也

セキュリティ心理学から地政学を考える

地政学への関心が高まり、サイバーセキュリティ分野でも、『脅威インテリジェンス』や『セキュリティ地政学』と言う言葉が聞かれる。しかしながら、地政学的リスクをサイバーセキュリティやセキュリティ心理学等の分野で考えると、多くの碩学の理論も大切だが、ネットワーク時代では、『インテリジェンス』（情報収集、分析、報告）の重要性を感じる。　当然ながら、インテリジェンスでの多くの情報は公開情報であり、広義のソーシャルエンジニアリングの活躍舞台でもあると考えている。

インテリジェンス：情報収集で、『予兆』を見いだす事ができれば、サイバーセキュリティでも同じ対応、即ち、孫子の言う『敵を知り、己を知れば百戦危うからず』であり、『戦わずして人の兵を屈するは、善の善なる者なり』を実践することになる。　ここでは、いくつかのセキュリティ事案を考察し、サイバーセキュリティ心理学から地政学を概観する。

高橋 優

心理学はセキュリティの「銀の弾丸」となるか

心理学という言葉には，非常に多様なアプローチやゴールが内包されている．

心理学の研究領域と「心理学」という言葉に一般の人が抱くイメージとを比較しつつ，各領域が情報セキュリティにおける諸事象の理解と対策にどのような形で貢献しうるか概観する．　その上で，パスワード管理行動を例として取り上げる．エンドユーザが利用サイトへの攻撃の脅威をどのように捉えており，それがパスワード管理行動とどのように関連しているかを検証した上で，望ましい管理行動の形成に心理学がどう貢献しうるか検討する．

五郎丸 秀樹

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

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．

上田 卓司

ナッジと行動選択・意思決定の心理学的源流について

行動経済学の隆盛とともに Nudge (Thaler & Sustein, 2009) を活用する試みがセキュリティ場面においても増えている．Nudge がどの程度セキュリティ

確保あるいは向セキュリティ行動に貢献しうるのか．本発表では Nudge の要素あるいは Nudge に連なるような心理学的概念の研究史を辿りつつ「銀の弾丸」足り得ない Nudge が，どのように有効な方策として機能できるかを検討する．

福田 健

問題解決における「失敗原因の特定」と「成功への行動修正」との不思議な関係

人は、プログラミングや機器操作や食品調理などの問題解決行動において、想定・希望していた結果が得られない場合（失敗時）に、失敗の原因を推定して次の行動を修正することがある。また、そうした失敗に対して、次の行動によって予定・希望した結果が得られるようにするために、外部から助言や行動制約を加えることがある。ただし、こうして失敗に対する原因を特定したり、成功に向けて行動を修正するためには、課題の構造に応じてその戦略を変える・合わせる必要がある。

今回の講義では、上の過程で問題とされる「失敗原因の特定」と「成功への行動修正」とが、必ずしも相補的で対称性をもったものとは限らないという事実を解説する。次に、心理・行動実験の結果として、人が課題の構造に応じて「失敗原因の特定」と「成功への行動修正」を適切に選択していることを示す。さらに、そうした選択が時間圧や先行知識や情報制限などにどのように影響されるかについて検討・議論する。