情報セキュリティ心理学研究会

《 2017 年度 月例会概要 》

１．InfoSec 2018 参加報告

日　時　2018 年４月 13 日

報告者　内田　勝也

概　要　2018 年 3 月 19 日から 21 日に開催された「InfoSec World 2018」の参加報告です。

サイバーセキュリティ推進者（Security Ambassadors）; 国内では「セキュリティ・リーダー」と言ってきたが、利用者部門のサイバーセキュリティ対応を考える必要があると指摘している。

2014 年に米国 国防総省のウェブの脆弱性を探すことが行われたが、約 140 件の脆弱性が発見されたが、発見内容により、報償金（100～15,000 ドル）を支払ったようであるが、企業・組織のネットワークの問題は、技術の問題より、「不作為」に起因する課題が多い。

また、最近のセキュリティ事件（情報漏えい等）では、利用者への心理的な弱さを攻撃しており、技術だけでは解決しない点も指摘されている。

２．セキュリティ警告は利用者エラーを防いでいるか？　～ マイクロソフトとアップルの相違から考える ～

日　時　2018 年５月 18 日

報告者　野々下 幸治

概　要　ＯＳのセキュリティ警告やセキュリティの考え方は、マイクロソフトとアップルでは必ずしも同じではない。

しかしながら、最近はＭＳ社の考えが次第にアップル社の考えに近くなってきた。

ユーザがいかに間違いを犯さないようにするのかについての努力をしてきているように思える。　セキュリティ技術と心理学とを繋ぐ考えである「Foolproof（ユーザが誤った操作をしても危険な状況を招かない考え方)」から考えてみた。

３．IoT と CPS 時代の新たなリスク管理手法の調査

日　時　2 018 年 5 月 18 日

報告者　五郎丸 秀樹

概　要　自動車や工場などに存在する制御系システムは，近年 IoT や CPS(Cyber Physical System)の技術の発展によりセンサや通信機能を有するようになった．その結果，自動車の自動運転や工場の遠隔監視などの新しいサービスが実施できるようになってきた．しかし制御系システムや IoT 機器に感染する Stuxnet，Mirai や Brickerbot を代表とする新たなマルウェアによってセキュリティも開発時に考慮する必要が出てきた．本稿では，まず自然災害からセキュリティ上の脅威までの従来のリスクとリスク管理手法について整理し，

現在の開発の現場から見えてくるリスク管理の問題点や課題を示す．そしてこれらの問題点や課題を解決するためにリスクの発見から対応策の策定までの思考プロセスについて吟味し，IoT と CPS 時代の新たなリスク管理手法に必要な条件について調査した 。

４．とある市区町村の情報セキュリティのはなし

日　時　2018 年 7 月 20 日

報告者　遠藤 芳行

概　要　最近のサイバーセキュリティインシデントでは、「<B>標的型メール攻撃が大きな課題になっていますが、重要な個人情報を保持している自治他や公共サービス等では、電話による標的型攻撃があります。

国内で最も有名なのは「逗子市のストーカー殺人事件」です。この事件では、ソーシャルエンジニアリング攻撃による「世界初の殺人事件」ではないかと思っています。　今回は、自治体での経験、実践のお話の予定です。

５．SNS における「フェイク」とセキュリティに関する一考察

日　時　2018 年 9 月 07 日

報告者　瀧野 修

概　要　今や、多くのフェイクニュース等が、SNS に満ちあふれています。

企業組織において、フェイクニュースは、セキュリティリスクと考える必要もあります。

今回は、フェイクとセキュリティに関しての考察です。

６．「風を見たかい？　～Have you ever seen the wind～」

日　時　2018 年 10 月 19 日

報告者　日野 麻美

概　要　個人情報の可視化への取り組み　～ ある自治体での管理・運用の実態 ～

- 戸籍と年金事務をやって気づいたこと： どうして知っているの？
- 社会保険庁崩壊に繋がった「年金記録盗み見事件」
- 個人情報ビジネスの闇 「プライム事件」
- ソーシャルエンジニアリングの出現「逗子ストーカー殺人事件」
- マイナンバー制度。　特定個人情報の適正な取扱い
- アクセスログで風をみたい

７．サイバーセキュリティからヒューマンエラーを考える

日　時　2018 年 11 月 16

報告者　内田　勝也

概　要　安全工学やヒューマンエラーでは、「第三者の悪意」を考えてこなかった。

しかし、サイバーセキュリティでは、第三者（外部・内部）による悪意を考え

ることがその中心にあった。
サイバーセキュリティへの攻撃は、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」と同じではないかと考えている。　即ち、警視庁管内の空き巣被害では、無施錠とガラス破りが ８０％程度あり、「不作為」が犯罪の原因と考えることもできる。　即ち、やるべきことを行わなかった（不作為）ため、そこ（脆弱性）への攻撃が、インシデントの原因になった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。

（金）　18:30～20:30

８．理論と実践を考える　～ セキュリティ心理学から学んだこと ～

日　時　2018 年 12 月 21 日
報告者　内田　勝也
概　要　大昔、まだ若かりし頃、システム関連業務を行っていた時代、先輩・上司から言われ、自分で考えたことは、「理論と実践」を考えることが大切であるということでした。
ただ、ノーベル経済学賞を２度も心理学関係の人が受賞している。2002 年にダニエル・カーネマンが、2017 年には リチャード・セイラーが、「行動経済学」の功績で受賞している。
従来（今？）の経済学では、「経済人」と言われる【経済的合理性に基づいた行動をする人間】を前提に成り立っていた。
しかしながら、行動経済学では、人間の行動は少しも合理的に行動するとは限らないとの考えで活動をしてきた。
翻って、セキュリティ心理学で扱う人間も、ソーシャルエンジニアリングや誘導質問術（Elicitation Techniques）で、重要情報を公開する。また、「Hacker Technic」と（私が）呼んでいる方法により、非常に困難だと思われたことを簡単に解決する高度なハッカーの存在も確認されている。
今回は『理論』を構築し、それに基づいて『実践』を行うことが正しいことなのかを考えてみたい。

９．テーマ　教育・訓練を考える

日　時　2019 年２月１日
報告者　内田　勝也
概　要　本研究会を始め、大学・大学院や企業（勤務先、顧客）でのセミナーなど 教育・訓練を行ってきたが、2019 年１月中旬、米国 Executive course のサイバーセキュリティコース（5 日間）を受講してきました。

従来、行ってきた自分自身の教育・訓練や国内での教育・訓練で感じてきたこと、及び、今回の受講から学んだ教育・訓練について、教育・訓練の実施側及び受講側の両面から教育・訓練について考えてみたい。

10. 情報セキュリティ心理学研究会 ワークショップ ～ サイバーセキュリティ月間 行事 ～

国の「サイバーセキュリティ月間」への協力依頼があり、また、公益社団法人 日本心理学会 から後援を頂きました。

～～～ プログラム ～～～

日 時 2019 年 3 月 12 日

＊ 10:00～10:05 開会挨拶 （内田 勝也： セキュリティ心理学研究会 主査）

＊ 10:05～10:55 テーマ セキュリティ心理学を概括する

報告者 内田 勝也 （セキュリティ心理学研究所）

概 要 2000 年 1 月 NHK「世紀を越えて」の放映で机上訓練を知り，「The Day After...in Cyberspace II」(1996 年) では 【セキュリティの運用面（人，手順，規制への対応）は極めて重要】とあり，【Human Firewalls】についても述べている。 2000 年頃の米国 CSI のヒューマンファイアウォールのワークショップでも人間（Human Firewalls）の重要性を指摘していた.

内部犯行は 2005 年頃にカーネギーメロン大学(SEI ： MIRIT) の研究を知り，代表者を招いたワークショップを開催したが，もう少し幅広い勉強会の必要性を感じ，2012 年に『セキュリティ心理学研究会』を日本心理学会の研究助成研究会として発足した．情報セキュリティも多くの人間が関係しており，『心理学』や『行動科学』等を考える必要がある.

本セッションは，人間を中心に据えた セキュリティ心理学を俯瞰する.

＊ 10:55～12:05 テーマ ネットワークサービスの重要性評価と管理行動

報告者 高橋 優 （埼玉工業大学）

概 要 ネットワークサービスを利用する上でパスワードの適切な管理は欠かせない.

しかし，実際にはユーザのさまざまな不適切行動が観察されている.

こうした不適切な行動の背景には，サービスやパスワードに関するユーザの重要性評価があると考えられる． そこで，ユーザがサービスやパスワードの重要性をどのように評価しているのか調査した． 本報告ではその結果をもとに，ユーザのセキュリティ意識および行動との関係について検討する.

＊ 13:05～14:15 テーマ 高信頼性組織の心理学

報告者 中西 晶（明治大学）

概 要 NISC「サイバーセキュリティは全員参加！」というキャッチフレーズや「みんなでしっかりサイバーセキュリティ」というテーマからも理解できるように，セキュリティを考えるには，「個人」あるいは「対人」の心理学のみ

ならず,「集団」あるいは「組織」の心理学を検討することも重要である. ここでは, 組織心理学者 K.Weick らが紹介する高信頼性組織 (HRO: High Reliability Organization (Organizing))の概念を発展させ,「組織行動」「組織マネジメント」「組織文化」の 3 層構造で議論する.

＊ 14:15～15:25　テーマ　質問紙調査から何を引き出すか：　心理尺度作成を中心とした質問項目・回答方法の工夫について

報告者　上田　卓司（早稲田大学）

概　要　ユーザや利用者あるいはセミナー等の受講者の行動・判断傾向を探る手段としてアンケート調査が多く利用されがちである. しかしアンケート調査の回答から適切な情報を引き出すためには, 多くの留意点や工夫が必要である. 本発表では, 主に心理尺度作成や社会調査場面における, 質問紙調査の構成方法や回答バイアスに関する研究を紹介しつつ, 適切かつ妥当性の高いアンケートを実施し, データを解釈する際に求められるポイントをまとめる.

＊ 15:45～16:30　テーマ　行為を支える心理過程を想定してエラーの定義と分類を再考する

報告者　福田　健（清泉女子大学）

概　要　リスクやセキュリティについて分析・対応するにあたりヒューマンエラーは避けて通れない問題である. このエラーは,「計画された内的または外的な行為」が「意図された結果」を導けなかったものとして定義されることが多い. しかし,「いまだ生じていないが将来生じる可能性があるタイプの誤った行為」を予測して防ぐためには, 行為を支える認識や思考や記憶の段階での誤りについて積極的に取り組むことが必要である. ここでは, そうした心理過程における誤りを扱うための枠組みを示す.

＊ 16:30～17:40　テーマ　AI、IoT 時代のセキュリティ心理学を考える

報告者　内田　勝也　(セキュリティ心理学研究所)

概　要　情報セキュリティは, 情報システムの一部で, その対策も少数の技術者と導入技術やツールで解決してきた。 しかし, サプレイチェーンや AI, IoT 時代になり, 個人情報の窃取・漏えいだけでなく, 知的財産等の窃取や大規模セキュリティ事故の発生は, コーポレートリスク, ナショナルセキュリティを考えなければならなくなっている.

『最大のセキュリティホールは人間』と言われるが,『技術やツールへの過信が最大のセキュリティホール』である. 技術やツールも完璧でなく,『教育・訓練』で対応能力を磨き, 予兆を探り, 事前・事後対応が大切になる.

＊ 17:40～17:45　閉会挨拶　西本　実苗　(関西学院大学)