

サイバーセキュリティ教育・訓練の提言

内田勝也^{†1}

概要： インターネットやコンピュータシステムの普及に伴い、サイバーセキュリティの確保が重要になって来たが、それに伴い、誰が、何を、誰に、どのような方法で教えるかを考える必要がある。

従来は、利用者が限定的であったが、現在は、組織内で働く多くの人が、サーバ内の情報を活用し、パソコンやタブレット、スマートフォンを利用してネットワークに接続する事が普通になり、セキュリティの確保は、直接的に関係しているセキュリティ技術者等の教育・訓練だけでは対応できなくなってきた。

ここでは、サイバーセキュリティ教育・訓練全体を俯瞰したセキュリティ教育・訓練の考察を行った。

キーワード： サイバーセキュリティ、教育、訓練、

Proposal for Cyber security education and training

Katuya UCHIDA^{†1}

Keywords: Cyber Security, Education, Training, Security Psychology, Geopolitics

1. はじめに

1.1 環境の変化

(1) インフラから利用者攻撃へ

① 20 年程前の指摘だが、米国大統領重要インフラ保護委員会の副委員長 Howard Schmidt は、2002 年 7 月 Government Technology の質問『攻撃の防御に必要な技術は？』に対し『技術的な問題でない。2001 年の米国防総省の調査では、97, 8%は設定ミスかパッチの未対応』だと回答している^[1]。

② 最近では、利用者を狙った攻撃の増加がある。図 1 は 2019 年セキュリティ脅威^[2]で、2018 年 1 月～9 月に利用者を攻撃対象とした「フィッシングサイト攻撃」は 2 億 1 千万件余りで、脆弱性攻撃は 26 万件余りで、800 倍程度の差がある。

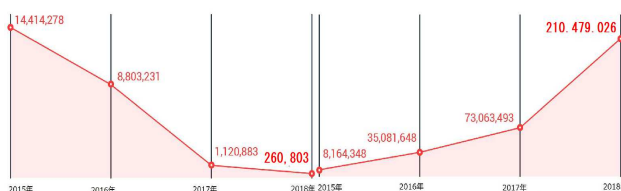


図1 エクスプロイトキット利用 フィッシングサイトの攻撃
トレンドマイクロ 2019 年セキュリティ脅威予測を基に作成

(2) ネットからサプライチェーン攻撃へ

① ネットワーク上のサーバやパソコンのソフトウェアに脆弱性があれば、インターネットを利用して感染を広げるマルウェアで有名なものは、1988 年 11 月に起こった「インターネットワーク」や 2001 年の CodeRed 等がある^[3]。

② 2017 年に世界中に大きな被害をもたらした

た「WannaCry」で、国内大手メーカー等に大きな被害をもたらした^[4]。

WannaCry は、ランサムウェアとワーム機能を持ち、感染したパソコンやサーバ内のファイルを暗号化し、身代金要求（ランサムウェア機能）だけでなく、パッチ未適用のパソコン／サーバにネットワーク経由で、感染・暗号化を繰り返し、感染を広げた。

持ち株会社やサプライチェーンを構築した企業は、関連企業とのインターネットやイントラネット接続で、WannaCry 等のワーム機能を持った有害プログラムが、今後も大きな被害をもたらす可能性がある。

1.2 変化への対応

(1) 従来の教育・訓練対象

1.1 で述べたように、2000 年代の初頭までは、サーバ等への対応が中心だったが、最近では、限られた人達を対象にしたサイバーセキュリティ対策では被害を拡大することになる。

2002 年 6 月に考察した『情報セキュリティ教育試案』では、技術者・管理者を対象にしたが、それぞれが現在の状況を十分に考慮したものではなかった^[6]。例えば、

技術者： 企業・組織内で情報セキュリティに関し、技術的な面での対応を行う。情報セキュリティを専門とする企業・組織では、情報セキュリティの技術面でのコンサルティングを行う能力を持った者も想定している。更に、単独で業務を遂行するだけでなく、少数の技術者を統率し、一緒に問題解決等に当たる能力を有する者もこの範疇と考える。

管理者： 企業・組織内や外部にいる技術者等で構成される問題解決のプロジェクトチー

^{†1} 情報セキュリティ大学院大学
Institute of Information Security

ム等を統率し、必要に応じトップ経営層に状況の報告を直接行う者を想定している。情報セキュリティについての幅広い知識はもちろんのこと、企業・組織に関連する幅広い知識・洞察力をもっており、企業・組織で CISO (Chief Information Security Officer) と考える。

とし、図 2 に示す教育概要を提案した。

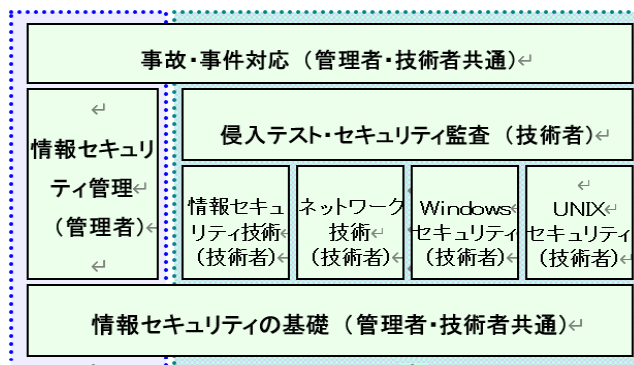


図2 管理者・技術者への情報セキュリティ教育概観図

この考えをもとに、文部科学省科学技術振興調整費 新興分野人材養成（基盤的ソフトウェア）で、『情報セキュリティ・情報保証人材育成拠点』に採択され、2003 年 8 月～2008 年 3 月の 5 年間で、中央大学研究開発機構にて実施した^[6]。

時間の経過やネットワークやコンピュータ環境の進展もあり、5 年間同一の内容ではなかったが、基本的な考えは、技術者及びそれに関連する管理者が中心で、経営層を含めた利用者等は考慮しなかった。

2. 組織、利用者への展開

2.1 OECD セキュリティガイドライン

経済協力開発機構（OECD）は、情報システムやネットワーク利用、情報技術の環境の劇的変化を見据え、1992 年のガイドラインを見直し、2002 年 8 月「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」が公表された^{[7][8]}。

ただ、OECD が「セキュリティ文化：Culture of Security」を掲げた理由が理解できなかったが、2010 年頃、国際原子力機関(IAEA: International Atomic Energy Agency) が 1991 年報告書「Safety Culture」^[9]を作成し、1986 年の旧ソ連 チェルノブイリ原子力発電所事故の根本原因は、人的・組織的要因で、安全文化の欠如が事故原因とした。OECD は「Safety Culture」を「Culture of Security」としたと推測した。

2.2 サイバーセキュリティハイジーン

サイバーセキュリティ・ハイジーン（サイバー

セキュリティ予防策）は、組織が直面している最も一般的で広範なサイバーセキュリティのリスク管理の一連の活動で、以下を実施する^[10]。

- 1 組織の主要なサービスやサポート資産を特定し、優先順位を決める
- 2 組織の主要なサービスや製品のリスクを特定し、優先順位を付け、対応する
- 3 インシデント対応計画を策定する
- 4 サイバーセキュリティ教育と啓発活動の実施
- 5 ネットワークのセキュリティ監視を策定
- 6 最小特権に基づくアクセス制御を行い、ユーザーアクセスアカウントを保持する
- 7 テクノロジーの変更管理を行い、標準化された安全な構成を使用する
- 8 データの保護および復旧管理の実施
- 9 マルウェアの感染の防止および監視
- 10 サプライヤーおよび外部に依存するサイバーリスクの管理
- 11 サイバーの脅威と脆弱性監視及び修復の実行

サイバーセキュリティ・ハイジーンも、サイバーセキュリティは実践的課題を含めての対応が、サイバーセキュリティ予防策と考えている。

3. 教育・訓練方法の考察

サイバーセキュリティ環境の変化があれば、教育・訓練については、従来方法だけでなく、新しいことを考える必要がある。

また、「教育」は、「教える」だけでなく、【育てる】ことも考える必要がある。特に、利用者への教育・訓練ではそれを非常に感じており、そのための工夫が必要になる。

3.1 教育・訓練方法

教育・訓練では、誰(Who)が、誰(Whom)に、何(What)を、どこ(Where)で、どの様(How)に、何故(Why)、何時(When)の 6W1H を考える必要がある。

(1) 誰(Who)が、誰(Whom)に

(A) 教育・訓練者について

「誰が(Who)」教育・訓練を行うかは、誰を対象にするかに依存する。ネットワークや AI 等の進展により、人間が教育・訓練を行わない可能性もあるが、「誰が(Who)」が曖昧になっている。

従来、教育・訓練者は、①社内の者、②社内と社外で適宜分担する、③社外に依頼する等がある。

「社外」の教育・訓練者では、外部研修への参加の場合と教育・訓練者を招いて、社内

で研修を行う場合がある。社内での研修の場合、教育・訓練者や教育・訓練内容が適切かを考える必要がある。

更に、単なる審判・判定者で、ルールの説明と勝敗の判断を行い、対象者は単独／グループで教育・訓練を行う、あるいはゲーミフィケーションでは参加者はネット利用で与えられた課題を回答していく。

(B)教育・訓練の対象者【誰に(Whom)】

(a)対象者の区分：教育・訓練対象者は業務により、分ける必要がある。

- ①技術者
- ②セキュリティ管理者
- ③CISO 等
- ④利用者

を考える。

「①技術者」に求められるのは、「I 型」タイプでなく、最低でも「T 型」タイプが求められ、「II 型」タイプ以上の技術・経験が求められる。

「②セキュリティ管理者」は、役割としては最も広範囲な業務を担う。CISO の補佐、組織内あるいは、サプライチェーンを考慮したセキュリティ体制の構築、維持、更に、インシデント時に委託先との折衝、利用者の教育・訓練計画や教育・訓練の実施、セキュリティポリシーの見直し等が求められる。一人が全てを担う必要はなく、外部委託もあるが、組織全体のセキュリティ対応を担う広範な知識・経験が求められる。

「③CISO 等」は、セキュリティ部門全体の推進を行う役割があり、システム部門の一部でなく、リスク部門の一部と位置づけと想定している。大規模なインシデントや組織でのサイバーセキュリティ政策、戦略を考える立場と考える。

「④利用者」の想定は、パソコン等の情報機器利用の全員でなく、部門に数名を想定している。これは、最近のサイバー攻撃は、利用者対象とした標的型攻撃が多く、サイバーセキュリティの基礎的な知識を持った要員（セキュリティリーダー）がそばにいる事で、管理職や経営者が気軽に確認できるとの指摘もある。また、「三人寄れば言うがまま」と言うように、組織内でのサイバーセキュリティ推進がスムーズに行えると考えている^[11]。

(b)教育・訓練効果の測定：社内での教育・訓練でも教育・訓練の効果測定すべきである。教育・訓練評価に関しては、カークパトリックとジャック・フィリップスが受

講者に受講後アンケートを実施し、理解度・満足度について 5 段階評価の提案を行っている（図 3）。サイバーセキュリティでの教育・訓練では、最低でも「行動変容」が感じられるレベル 3 程度が求め求められる^[12]。

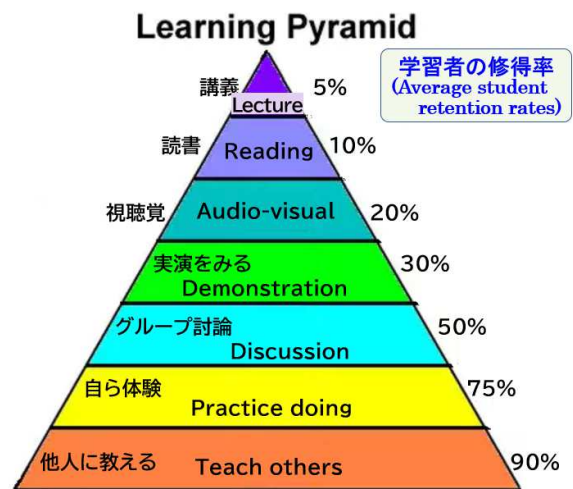
レベル	説明
1. 研修満足度	受講直後のアンケート調査等による受講者の研修に対する満足度の評価 ある基準と比較して望ましい研修が行われたかを評価 アンケート調査だけでは？
2. 学習到達度	筆記試験やレポート等による受講者の学習到達度の評価 研修受講の結果、受講者という個人に与えた効果（学習到達）を測定
3. 行動変容度	受講者自身へのインタビューや他者評価による行動変容の評価 研修受講の結果、受講者という個人に与えた効果（行動変容）を測定
4. 成果達成度	研修受講による受講者や職場の業績向上度合いの評価 受講者個人の行動がもたらした組織への影響 せめてこの程度は・・・
5. 投資収益率	効果測定は、効果を収益に換算し、収益を教育研修への投資額との比較ではじめて有意義になる 収益貢献度（レベル 5A）= その成果を収益金額に換算 顧客満足度（レベル 5B）= 顧客の満足に与えた成果を見たもの 5段階目はジャック・フィリップス (Jack J. Phillips) の提案

図3 カークパトリック／フィリップスの研修評価・効果測定

(2) どの様に(How)

(A)ラーニングピラミッド

効率的、効果的な教育・訓練が大切だが、どのような教育・訓練を受けるか、逆に、どのような方法で学ぶかについて National Training Laboratory（全米訓練所）が「Learning Pyramid」の考えを示している。教育・訓練の手段／方法で学習習得率が異なる^[13]。



Source: National Training Laboratories, Bethel, Maine

図4 教育・訓練方法による習得率

図4の「学習者の取得率」の根拠が不明で、数値（パーセンテージ）の計算方法も明らかになっていないが、教育・訓練方法を考える上では有効だと考えている。

(B)複合的方法の教育・訓練

Learning Pyramid では、個々の学習者習得率が適切であるかについては、疑問があるが、教育・訓練を行う場合、それぞれの方法を適切に使う。3時間程度のセミナーであったが、「視聴覚」資料の利用や「日常の体験」をもとにした記憶の曖昧さ等による質問、クイズ等を行い、一方的な講義でなく、複数の方法を取り入れた教育・訓練を行うことで、一定

の効果を得ることができた^[14]。

セキュリティにおけるチーム・組織力育成教育・訓練

- 遠子ストーリー殺人事件を対象に2時間程度の教育を自治体職員を対象に実施
- 「Team STEPPS」を基に、セキュリティの課題とチーム／組織力の確立を目指したカリキュラムを作成
- ストーリー殺人事件や自治体に限らず、セキュリティ全般への利用を想定
- 教育・訓練内容：今回の事件の特徴や「セキュリティポリシー」の課題等を簡単に説明し、「駐禁マーク」や「錯視」等のヒューマンエラー対策は、個人を対象とするだけでなく、グループ、組織対策の重要性を「選択的注意」等の考えかたをビデオ利用も含め行った
- アンケート結果 (37名、住民対応:26名,70%) は、以下に...

研修満足度		研修を他に勧めたいか	
大変役立った:	57% (21名)	ぜひ勧めたい:	19% (7名)
まあまあだった:	43% (16名)	勧めたい:	43% (16名)
あまり／全く役立たなかった:	0%	どちらかと云えば勧めたい:	19% (7名)
		どちらとも言えない:	8% (3名)
		どちらかと言えば勧めたくない:	3% (1名)
		勧めたくない:	3% (1名)
		未記入:	5% (2名)

研修内容の理解度	0	1	2	3	4	5	6	7	8	9	10
研修内容の理解度	0人	0	0	0	0	4	2	6	12	8	5
研修内容の業務活用度	0人	0	0	0	0	5	3	6	11	6	6
研修内容と受講動機的一致	0人	0	0	1	0	6	3	7	9	6	5

遠子ストーリー殺人事件
加害男性が被害女性の住所を取得し殺人に及んだ。女性の住所は調査会社の経営者が被害女性の夫になりすまし電話をした。経営者は「誘導質問法(Elicitation Techniques)」に長けており、職員は無意識に回答した可能性が高い

図5 複合的教育・訓練例

また、講義内で、3, 4名のグループにより、課題の検討を行い、それを発表することも、一定の効果を得ている。

4. サイバーセキュリティ教育・訓練案

個々の教育・訓練を述べる前に、全体像を図6に示す^[15]。

前述したが、対象者を①技術者、②セキュリティ管理者、③CISO等、④利用者の4分類しているが、教育・訓練では共通項目を設け、基礎的(essential)な教育・訓練を考える。



図6 教育・訓練概要

(1) 基礎的教育・訓練：共通講座

共通講座の目的の1つに、異なる目的を持った人達が共通の講座に集まることにある。これは、他の対象者の考え方を知ることでもでき、また、緊急時に始めて会うより、情報交換がスムーズにいくと考えている。

勿論、各対象者が学ぶ課題は、同じであるが、修得内容の「修得の深さ」は同じではない。実際、技術者であれば、基礎的なセキュリティツール等の利用を駆使できるレベルが必要であるが、他の対象者はツールの機能を理解できれば十分であろう。

(2) 技術者向け教育・訓練

(A) 技術者教育・訓練の考え方

セキュリティ技術は多くの変化・進展があり、常に適切な指導者がいるとは限らない。このこともあり、

「教育・訓練 = グライダー論」

と考えている。即ち、グライダーは、地上から舞い上がるには、牽引され、所定の高度まで上昇した後、牽引綱を切り離し、滑空する。

教育・訓練でも全て講師から学ぶのではなく、一定レベル以上であれば、必要な環境を与えることで個人やグループで学ぶ。実演を見る、グループ討論を行う、更に、自ら考えることができる知識・経験を習得する。グループでは他人に教える機会もあり、個人またはグループで問題解決を行うことにより、「想定外」をなくす訓練を行うことにより、実際のインシデント時に遭遇した「想定外」への対応を可能にし、問題解決をはかれる知見・経験を修得する。

(B) 技術者の考え方

セキュリティ技術者には、大きく2つに分けられると考えている。

① ハードウェアやソフトウェアのサービス提供を行う企業や大規模なインターネットを利用した商取引を行う企業での技術者で、基本ソフト等の開発やインシデントの解析等を行う。

② 政府・自治体や一般的な企業の技術者は次項で述べるセキュリティ管理者に近く、ハードウェアやソフトウェア製品を熟知しているが、それらの開発や保守をやることはしない。①の技術者等と一緒に問題解決に当たる。

(3) セキュリティ管理者・リーダー教育・訓練

(A) セキュリティ管理者・リーダーとは

セキュリティ部門全体をカバーする役割であり、サイバーセキュリティの企画、推進、維持などを行う部門の主要メンバーである。

サイバーセキュリティとか、情報セキュリティと呼ばれる分野については、情報システム部門の一部でなく、企業や組織のリスク部門の1つと考えるべきであろう。

組織におけるリスクを図7に示す^[16]が、図の右側の五分野や戦略リスクの多くの部分はサイバーセキュリティも関係する。

(B) 管理者／リーダーへの教育・訓練

最も広範囲の業務業務等を必要とするが、組織の状況を理解していることが大切で、リスクマネジメントやプロジェクトマネジメントの基礎知識を必要とする。



図7 コーポレートリスクの例

(4) 経営者／CISO の教育・訓練

(A) CISO とは

Chief Information Security Officer の略で、CISO と表す。図7からも明らかなように、組織のリスク戦略の一部分を担い、その範囲も広く、深くなってきた。そのため、情報システムの下位部門とか、その一部と考えることは、適切でない。CIO（情報システム統括）に関して、ビジネスリーダーにその役割を担うべきとの指摘^[17]もあるが、CISO も同じと考えている。

(B) CISO への教育・訓練

①サイバー攻撃シミュレーション：国内では、大規模災害やパンデミック（大規模感染症）に関し、BCP（事業継続計画）として、サイバーセキュリティ対応の一課題と考える必要がある。また、大規模なサイバー攻撃への対応も CISO や CIO、経営者の専管事項と考えられ、大規模なサイバー攻撃のシミュレーションの実施も必要である。米国では既に大規模なサイバー攻撃のシミュレーションのための教育・訓練が行われている^[18]。

②地政学（Geopolitics）：国内では、地政学の知見を持っている人も少なく、知見がある人も戦争のための学問と考えていることが多い。

戦争は「宣戦布告」からと考えられていたが、テロを近代戦争の1つと考えており、宣戦布告はない。ただ、現時点で大規模サイバー攻撃も「サイバーテロ」と定義されていないが、今後もない保証はない。地政学は、

「地政学」＝「歴史」＋「地理学」

との考えであり、北東アジアに位置し、海外からの重要な原材料等を輸入に頼る日本の現状は、グローバルに広がったサプライチェーンを考える必要があり、サイバーセキュリティ

分野も地政学を考える時代が目の前にある。

(4) 利用者の教育・訓練

(A) 利用者とは

利用者は組織内で情報機器を使う全ての職員でなく、セキュリティリーダーとか、セキュリティアンバサダーと呼ばれる人達で、各部門に数名を想定している。

米国の教育・訓練^[19]では、組織文化の変革には、3～10年必要と指摘がある。数名の国内の実務家等への簡単なヒアリングでも、利用者を遍く教育・訓練するより、数名の選抜された者の育成が有効との回答も得ている。

(B) 教育・訓練方法の検討

対象者の連携も大切であることを考えると、集合教育・訓練が望ましいが、対象者の場所を考えれば、当初の数回は集合教育・訓練が必要だが、リモート会議や非公開の SNS 等の利用で、情報共有、意見交換等を行う教育・訓練が考えられる。

(C) 利用者の教育・訓練

①セキュリティ情報提供：昨今のサイバー攻撃は、利用者（End Point）への攻撃、標的型攻撃が多いが、それらの多くは海外で発生し、その後、国内で行われることが多い。このため、セキュリティベンダー等が持つ情報を提供するなど注意喚起をはかる。

例えば、米国連邦捜査局（FBI）は2015年8月「ビジネスメール詐欺（BEC）」に関し、2013年10月～2015年8月被害状況を報告^[20]しており、国内のセキュリティベンダーでも2016年6月にブログ^[21]を書いて注意喚起している。しかしながら、国内でのBEC詐欺は、2017年9月に多額の被害（3億6千万円）を受けた。

②標的型メール訓練：単に「クリック率」を下げるだけの訓練では、図8に示すようにクリック率を数%まで下げることが限度で、ゼロにはならない^[22]。

標的型添付メール訓練

(1) 国内での訓練結果		クリック割合
1. 事前の情報提供せず訓練を実施・・・	約40%	%
2. 事前に情報提供を行って訓練を実施・・・	約10%	%
3. 訓練実施2年後、事前の情報提供をせず実施・・・	約12.5%	%
4. 訓練実施2年後、事前に情報提供し実施・・・	約6.3%	%
1. 3自治体（横浜、豊島区、藤沢）の結果		
2. 中央官庁（NSC）		
3. 1自治体での結果（豊島区）		
4. 1自治体での結果（豊島区）		
(2) 米国：Lance Spitzner（SANS.org RSA Conf. 2014）		
◆ 訓練間隔を短くすればするほど、効果はある・・・		
> 四半期	19%	
> 2ヶ月毎	12%	
> 毎月	4%	
◆ 毎回、内容を難しくして行く必要がある		

図8 標的型メール訓練例

そのため、標的型訓練では、
(a) 行動心理学等の知見による訓練^[23]
(b) クリック後の対応
などを考えた訓練を想定している。

ナッジ実験(机上訓練)振り返り	
今回の机上訓練について	
1. 机上訓練でも、一定の効果はある。	22名
2. あまり効果を感じない。	1名
② 本来、訓練メールやメッセージはツールを使って、効果を測定するものですが、	
1. 従来の訓練(10%程度クリック)より遙かに効果。(数%程度)があると思われる	10名
2. 従来の訓練程度だと考える	10名
3. あまり効果がないと思われる	2名
- 机上訓練でも一定の効果はある - シミュレーションゲームとしても考えられる - 企業や自治体だけでなく、中等高等学校での利用もできる - フィッシング画面も工夫は必要 - コンピュータを使って画面の送付やログ解析等も必要	
謝辞	
(公社)日本心理学会情報セキュリティ心理学研究会 月例会の参加者	

図9 標的型メール訓練例

実際、(a)は簡単な机上訓練を行い、図9に示す一定の知見を得ることができた。

なお、(b)は机上訓練では実施不可能であったため、そのための工夫が必要であった。標的型訓練では、図8で明らかだが数%~10%程度の人が、標的型メールをクリックする。

しかし、情報漏えいでは、クリック後、情報漏えいが始まるまでに時間差がある(注)。

(注) 2015年5月に発覚した日本年金機構の情報漏えいでは、標的型メール攻撃から情報漏えいが発生するまでに、15日程度時間があつた。また、大手旅行会社の事例では、5日程度時間があつた。

逆に考えると、クリック前やクリック時点で当事者が何らかの行動ができるかの検討・議論をしてみる必要がある。

例えば、年金機構では、公開メールは「外部調達用メールアドレス」であつた。外部調達用メールアドレスを公開する必要があつたのか、外部調達以外のメールが送付されても、削除すべきであつた等の方法が考えられる。

また、大手旅行会社では「自社へのメール内容ではない」と送付元に返信したが、当該メールアドレスがないため「未達メール」即ち、当該メールアドレスがないと回答があつたと思われる。送付先のメールアドレスがなければ、未達メールが戻ってくる事を知っていれば防げた可能性がある。

5. まとめと今後の課題

- 2002年に、それまでの調査・研究を基にして「技術者・管理者向け情報セキュリティ教育試案^[5]」を発表したが、2019年7月には「サイバーセキュリティにおけるナショナルセキュリティの検討分科会 最終報告書^[15]」を

作成した。日本心理学会 情報セキュリティ心理学研究会での議論を通して、検討してきた教育・訓練について考察を行った。

サイバーセキュリティ分野の教育・訓練に終わりはなく、また、サイバーセキュリティは人間が担っており、心理学、行動経済学、社会学、犯罪学、ヒューマンエラー等の分野での知見を含めて考えが必要である。

- 利用者教育・訓練で述べた「標的型訓練」も利用者への標的型教育・訓練ツールを利用することができれば、より効果的な教育・訓練が可能になる。

予算的な制約のため、机上教育・訓練を行ったが、予算獲得ができれば、更に効果的な教育・訓練ができると考えている。

- 利用者の教育・訓練では、利用者の判断が重要だが、判断をしないできる方法の検討を考えている。

また、ナッジの利用では空港の小便器にハエの絵で清掃費を80%削減した^[22]が、サイバーセキュリティでは、100%を目指す必要がある。

- サイバーセキュリティでは、事前、事中、事後の3つの観点から考える必要があるが、技術者では「Bug Bounty (報償金制度)」^[22]、一種のペネトレーションテストだが、「ゼロデイの脆弱性」や「コバートチャネル」等の発見も事前対応(Proactive)が求められ、利用者教育・訓練も、標的型攻撃の対処も同じで、益々、事前対応を考えた教育・訓練の必要性が求められている。

6. 謝辞

日本心理学会情報セキュリティ心理学研究会[4]の月例会の参加者から多大な協力を頂きました。

特に、「サイバーセキュリティにおけるナショナルセキュリティの検討分科会 最終報告書」では、立入健太郎氏(GRC-Lab 代表)、野々下幸治氏(トレンドマイクロ(株))との協力により作成しました。

ありがとうございました。

参考文献

(注) 以下の参考文献で URL 表記のないもの([3], [11], [14], [17], [19], [22], [23])を除き、全て2020年2月17日に確認済み。

- [1] Government Technology, Security First, <https://www.govtech.com/security/Security-First.html>
- [2] トレンドマイクロ, 2019年セキュリティ脅威予測, <https://resources.trendmicro.com/jp-docdownload-form-m099-web-2019prediction.html>
- [3] 内田勝也, 高橋正和, 有害プログラム, 2004, 共立

出版

- [4] 日立製作所, 日立評論「サイバー攻撃事案の教訓と社内堅牢化の取り組み」, 2018 Vol. 100 No.3, <http://www.hitachihoron.com/jp/archive/2010s/2018/03/05b02/index.html>
- [5] 内田勝也, 技術者・管理者向け情報セキュリティ教育試案, 日本セキュリティマネジメント学会 第 16 回全国大会, 2002.06, <http://www2.gol.com/users/uchidak/Seminar/JSSM200206.pdf>
- [6] 文部科学省, 情報セキュリティ・情報保証 人材育成拠点, https://www.mext.go.jp/component/a_menu/science/detail/_icsFiles/afieldfile/2016/10/14/1378278_068.pdf
- [7] OECD, ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, <http://www.oecd.org/dataoecd/59/2/1946962.doc>
- [8] 経済協力開発機構, 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 (外務省仮訳), https://www.mofa.go.jp/mofaj/gaiko/oecd/security_gl_a.html
- [9] IAEA, Safety series, Safety Culture, 1991, https://www-pub.iaea.org/MTCD/Publications/PDF/Pub882_web.pdf
- [10] Matthew Trevors, Cyber Hygiene: 11 Essential Practices, SEI, Carnegie Mellon University, <https://insights.sei.cmu.edu/insider-threat/2017/11/cyber-hygiene-11-essential-practices.html>
- [11] 池谷裕二, 三人寄れば言うがまま, あすへの話題. 日本経済新聞, 2007 年 11 月 28 日夕刊
- [12] (独法) 高齢・障害・求職者雇用支援機構, 公共能力開発施設の行う訓練効果測定 - 訓練効果測定に関する調査・研究 第 6 章 研修評価と効果測定の一般的な考え方と進め方, <http://www.tetras.uitec.jeed.or.jp/files/kankoubutu/a-114-07.pdf>
- [13] 名古屋商科大学, アクティブラーニング, <https://www.nucba.ac.jp/active-learning//tpl/amp.html>
- [14] 内田勝也, 誘導質問術からみた個人情報漏えいの考察, 情報処理学会論文誌, Vol.56 No.12 2219-2229
- [15] 内田勝也 他, サイバーセキュリティにおけるナショナルセキュリティの検討分科会 最終報告書, http://www.uchidak.com/seminar/CySec_FINALRep.pdf
- [16] 喜入博, 企業にとってのリスクと事業影響度分析, <https://www.itmedia.co.jp/im/articles/0611/30/newsl25.html>
- [17] R. D. Austin 他, ビジネスリーダーに IT がマネジメントできるか - ある IT リーダーの冒険, 日経 BP 社
- [18] Harvard Kennedy School, Cybersecurity: The Intersection of Policy and Technology, <https://www.hks.harvard.edu/educational-programs/executive-education/cybersecurity>
- [19] Lance Spitzner, MGT433: SANS Security Awareness
- [20] FBI, BUSINESS EMAIL COMPROMISE, 2015 年 8 月, <https://www.ic3.gov/media/2015/150827-1.aspx>
- [21] トレンドマイクロ, 財務責任者を狙う, ビジネスメール詐欺「BEC」, <https://blog.trendmicro.co.jp/archives/13500>
- [22] 内田勝也, 標的型メール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, 経営情報学会 2015

年秋期全国研究発表大会

- [23] 内田勝也, 行動科学を援用したサイバーセキュリティ対応 - セキュリティ心理学の確立を目指して -, 情報処理学会 第 82 回全国大会