L-011

ヒューマンファクターズの対策方法と情報セキュリティへの適用の考察

Study on Applying Human Factors Measures to Information Security

五郎丸 秀樹†
Hideki Goromaru

1. はじめに

近年、多くの産業分野での安全性が脅かされている。例えば、実在する会社・組織・関係者を騙り不信感を持たせない巧妙な手口で、メール受信者を攻撃者の思い通りの行動へと誘導する標的型攻撃 [1]がある。また最近では原子力発電所の一部の機能を乗っ取る事件[2]など各種産業の制御系システムへの脅威も増えてきている。

ISMS[3]や CC 認証[4]などの対策を行っているにも関わらず未だ被害が発生し続けている背景として、技術的な対策だけでは防ぎきれない人的な要因が残っている可能性がある。その対策としては、訓練や学習が有効だといわれている[5]。例えば専門家を雇い、攻撃者と同じ攻撃を模倣する訓練を実施し、攻撃の手口を学習することで、やがて騙されにくくなり、攻撃者の攻撃がわかるようになっていく。

しかし、人は周りの環境によって状態が変化し認知や行動が変わってくる。その変化に気づかず放置すると資産を適切に管理できず情報漏えいの危険性が高まるなど、不適切な管理稼働が発生するため、価値と防御のバランスのとれた適切な管理が必要になる。

本研究では、人的な要因による事故を防ぐために既に産業界で用いられているヒューマンファクターズ[6]の対策を紹介し、情報セキュリティへ適用していくことを検討する。２章ではヒューマンファクターズと産業安全について説明し、３章では新たな産業災害の問題、４章ではヒューマンファクターズで用いられる人的な要因への対策を提案する。

2. ヒューマンファクターズと産業安全について

ヒューマンファクターズの定義は様々存在するが[7][8]、ここでの定義は「人々の能力や限界に適合するように機器、作業、そして作業環境を設計・改善するための学問分野」[6]とする。産業革命が始まってから、産業における安全について様々な検討が行われてきた。Andrew Hale & Jan Hovden [9]によると、産業の安全を考える場合、技術の時代、ヒューマンファクターズの時代、安全マネジメントの時代の 3 つの時代に大きく分けられる。ここでは E. Hollnagel[10][11]の産業安全に対する考え方を参考にして、ヒューマンファクターズの歴史的な位置づけを示すと共に、産業安全に対する考え方を紹介する。

2.1.1 技術の時代

1769 年のジェームズ・ワットの低圧蒸気機関の特許取得の年が産業革命の始まりといわれ、同時に技術の時代の始まりでもある。産業革命以降、事故は「技術（機械）の問題」という捉え方が出てきた。

2.1.2 ヒューマンファクターズの時代

技術が発達し技術的要因による事故が減っていくと、産業災害の要因としてヒューマンエラーが徐々に目立ち始めてきた。特に 1979 年に米国のスリーマイル島での原子力発電所の事故をきっかけに、技術よりもヒューマンエラーに注目が集まった。その後、人のエラーの要因には人だけではなく人以外（組織、装置、設備、手順、作業環境等）の要因の影響が大きいことがわかり始め、「ヒューマンエラー」では表現不可となり、人もシステムの一部とみなす「ヒューマンファクターズ」の考え方が出てきた。2010 年における産業災害の要因の７割以上がヒューマンファクター（人的要因）である[11]。

2.1.3 安全マネジメント（組織）の時代

1979 年のスリーマイル島の原発事故がきっかけに、Charles Perrow [12]は、スリーマイル島の原発事故をもたらした組織的要因の解明に着手し、1984 年に Normal Accident Theory（以下 NAT）を唱えた。これは、システムの複雑さ(Complex)と事故の拡大し易さ(Tight)がアクシデントを引き起こし、システムにとってアクシデントは避けられないシステムの固有の特性という理論である。

1980 年代後半、NAT に対抗する理論として、バークレー・グループと Weick & Sutcliffe の研究が現れた[13]。事故の危険性が高い状況下にあっても高い信頼性を保っている組織（HROs)の分析が試みられ、事故を防ぐ要因としての組織特性を考察したものである。

さらに 2004 年には、レジリエンス工学という学問分野を Hollnagel[14]が唱えた。レジリエンスとは、予期できなかった条件下でも、求められるオペレーションを継続可能にする本質的能力であり、レジリエンス工学では、うまくいかない事象を減らす事よりも、うまくいく事象の数を増加させることを目的としている。

3. 新たな産業災害の問題

2010 年の Stuxnet[2]や 2011 年の東日本大震災は、事前の予想は難しく、予想ができたとしても確率は非常に小さいため殆ど対処されなかったと思われる。人間の行動や認知では錯誤や限界がある。状態の変化に気づかないことや、気づいたとしても対処が面倒であったり誤った対処を行ったりなど適切な対処が行われない可能性があり、新たに人を支援する仕組みが必要となる。

4. ヒューマンファクターズでの対策の提案

ヒューマンファクターズでの対策手法として、河野[6]の対策立案の発想手順の簡易版４ＳＴＥＰ／Ｍというものがある。これは人的要因への対策を考えるためのヒントとなる手法であり、①やめる、②できないようにする、③判り易くする、④やりやすくする、⑤知覚能力を持たせる、⑥予測させる、⑦安全を優先させる、⑧できる能力を持たせる、⑨自分で気づかせる、⑩検出する、⑪備える、という手順があり、①は機会最小、②～⑧は最小確率、⑨⑩は多重検出、⑪被害局限、という括りに分けられる。状況の変化を検知する対策は、「⑨自分で気づかせる、⑩検出する」の多重検知であり、今回はこの多重検知について検討した。

† 日本電信電話株式会社

4.1 ウェアラブルデバイスを用いた検知と対策

現在 IoT を使ったウェアラブルデバイスが普及し、脳波や心拍や皮膚抵抗、人の位置、体温などを取得するデバイスを身につけることが可能になり、人の状態を調べることができるようになった[15]。そこで、これらの技術を用いて、自動的に人や資産の変化を検知し、その変化に合わせて人や資産のセキュリティ管理の変更を自動的に実施したり、実施できない場合は支援を要請したりする仕組みを提供することを可能にするシステムについて検討し、下記のように３つのモジュールで構成するシステムを考えた（図 1）。

（１）検知部:人や資産の状態が変化したことを検知し、検知結果から検知情報を作成する。

（２）判断部:検知情報を受取り、検知情報を基に対処を判断し、セキュリティ管理の変更が必要と判断した場合に判断結果に応じてセキュリティ管理の変更を実行するための情報を含む判断情報を作成する。

（３）実行部:判断情報を受取り判断情報から実行情報を抽出し実行情報の内容を実行する。

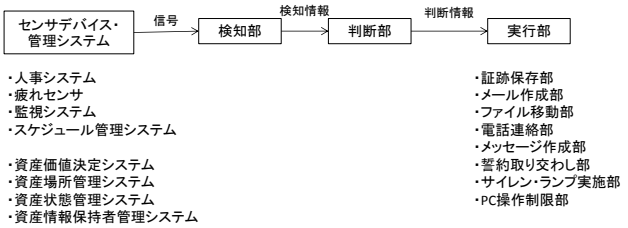

図 1　セキュリティ管理支援システムの例

図 1 の「センサデバイス・管理システム」は様々な市販のセンサや既存のシステムである。

4.2 適用分野について

ここでは実施例（標的型攻撃の対策への対処）として、人の疲れを検知し、疲れた人への攻撃を防ぐための仕組みを示す。

(1)社員の A 氏は、PC を使用して仕事をしている。市販の疲れセンサの信号を検知部は検知する。検知情報の変更識別子の例を表 1 に示す。検知した信号から A 氏の疲れが、表 1 の識別番号 2−2 の重い疲れ(値:4)へ変更したときに発生する信号であることが判明し、変更時刻と、操作者（A）と、疲れのレベル（４）、を取得し検知情報電文を作成し送信する。

(2)判断部は、検知情報電文を受信し、電文のデータに変更識別子があれば、電文から検知情報を取り出し、変更識別子の値に対応した処理を判断し、疲れのレベルに対応した判断情報を作成する。疲れのレベル（４：重い疲れ）の場合は、メッセージ作成部［メッセージ（A さん、働きすぎです。今すぐに作業をやめて帰宅してください。これからメールの機能が一部使用できなくなります）］、メール作成部［To:情報管理者 C さん、Subject:A さんの代替要求、内容：A さんが働きすぎのため、すぐに代替者を用意してください。］、PC 操作制御部［対象 PC: A 氏の PC、制限事項：１.メールに書かれている URL から直接 Web を起動させる動作を禁止、２.メールの添付ファイルの起動を禁止］へ送信される３つの判断情報を作成し送信する。

(3)実行部では、受信した判断情報を基に各実行部が処理を実行する。

識別番号	名称	内容
1−1	資産価値（VA）	変更した資産価値の価値レベルを示す．値は-1～4．
2−1	基本防御（BHD）	変更した人の役職の防御レベルを表す．値は-1～4．
2−2	外部リスク（OHR）	変更した人の疲れのリスクレベルを示す．値は1～4．
2−3	内部リスク（IHR）	変更した人の内部犯行のリスクレベルを表す．値は0～．
3−1	基本防御（BMD）	変更した資産の保管場所の防御レベルを示す．値は-1～4．
3−2	追加防御（AMD）	変更した資産のアクセス制御や暗号化の防御レベルを示す．値は0～4．

表 1　検知情報の変更識別子の例

5. おわりに

今回情報セキュリティへヒューマンファクターズの対策手法として多重検知に着目し、IoT デバイスを活用したセキュリティ管理支援システムを考案した。今後はこのシステムを実装しその効果を検証していく予定である。

参考文献

[1] 不正アクセスによる情報流出事案に関する調査委員会、 “不正アクセスによる情報流出事案に関する調査結果報告”、 日本年金機構 (2015) 、 http://www 。 nenkin 。 go 。 jp/files/kuUK4cuR6MEN2。pdf（2015 年 10 月 13 日閲覧)。

[2] Kim Zetter: Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon、 Crown(2014)。

[3] 日本規格協会、 “情報技術―セキュリティ技術―情報セキュリティマネジメントシステム―要求事項”、 JIS Q 27001:2014 (2014)。

[4] 日本規格協会、 “情報技術―セキュリティ技術―情報セキュリティの評価基準―総則及び一般モデル”、 JIS 5070-1:2011 (2011)。

[5] Christopher Hadnagy（訳者：成田光彰）, “ソーシャル・エンジニアリング”, 日経 BP 社（2012 年）.

[6] 行待武生、 “ヒューマンエラー防止のヒューマンファクターズ”、株式会社テクノシステムズ(2004)。

[7] Meister、D、 “Human Factors: Theory and Practice (Wiley series in human factors)”、 John Wiley & Sons Inc(1971)。

[8] 佐相邦英、 “原子力教科書 ヒューマンファクター概論”、 オーム社(2009)。

[9] HALE、 A。 R。 and HOVDEN、 J。、 “Management and culture: the third age of safety。 A review of approaches to organizational aspects of safety、 health and environment”、 In Anne-Marie Feyer and Ann Williamson (Eds)、 Occupational Injury: Risk Prevention and Intervention、 Taylor & Francis (1998)。

[10] Erik Hollnagel、 “安全文化－セーフティ・マネジメントとレジリアンス・エンジニアリング”、 http://www。atec。or。jp/Forum_09_Hollnagel_J。pdf（2016 年 6 月 1 日閲覧)。

[11] Erik Hollnagel、 “On How (Not) To Learn from Accidents”、 http://www 。 uis 。 no/getfile 。 php/Konferanser/Presentasjoner/Ulykkesgransking%202010/EH_AcciLearn_short。pdf（2016 年 6 月 1 日閲覧)。

[12] Charles Perrow、 “Normal Accidents: Living With High-Risk Technologies (Princeton Paperbacks)”、 Princeton Univ Pr(1998)。

[13] 藤川なつこ、 “高危険組織の構造統制と組織化―ノーマル・アクシデント理論と高信頼性理論の統合的考察ー”、経済科学第 60 巻 3 号、 pp。51-69 (2013)。

[14] 長谷川尚子、 “不測の事態を抑止し、 対処できる組織の要件～高信頼性組織レジリエンス、 安全文化を踏まえて～”、 REAJ 誌 2014Vo。。36。No。2、 pp。113-120 (2014)。

[15] James Reason and Alan Hobbs、 “Managing Maintenance Error: A Practical Guide”、 Ashgate Publishing Limited (2003)。

[16] Erik Hollnagel（他 3 名）、北村正晴、小松明哲（監修）、 “実践レジリエンスエンジニアリング”、 日科技連(2014)。

[17] 株式会社ＮＴＴデータ, “絵で見てわかる IoT/センサの仕組みと活用”, 翔泳社（2015）.