プラントへのIoT 活用と安全・セキュリティ対策 セキュリティ心理学からの考察

情報セキュリティ大学院大学 内田 勝也

サイバーセキュリティ対策は技術対策と考えられるが、実際には「人間」を考えることが重要である。システム/セキュリティ機器の作成も人間であり、それらの管理や利用するのも人間である。このような状況を考えれば、人間の問題として、セキュリティ対策を考えることが大切になる。このような観点から、人間の脆弱性を踏まえて考えたのが、セキュリティ心理学である。今後、ますます発展するIoTのセキュリティでも重要な要素になると考える。

KEYWORDS: *Security Psychology, Security Management, Information Assets, Omission, Crew Resource Management*

I. はじめに

1. 「情報＝風」論

「誰か風をみたことがあるでしょうか？」から始まる「風」という童謡をご存じの方も多いが、この童謡は、英国のクリスティナ・ジョージナ・ロゼッティの詩に、大正10年、西条八十が訳詞し、草川信が作曲をした。この詩では、風は感じるが見えないと詠っている。

では、情報やデータを見たことがあるだろうか？

「紙に印刷されている」とか、「コンピュータの画面に表示されている」との回答があるが、紙という媒体に印刷されている、あるいは、コンピュータのディスプレイに表示されているのであって、媒体があって始めて情報やデータであると考えられ、情報やデータそのものとは考え難い。

我々が回答しているものは、情報そのものでなく、情報が保存されている(と思われる)物理的なものを示している。

風と同じように、「見えないもの」は保護・保全できない。そのため、それが保存されている物理的に見える印刷物やコンピュータ等を保護・保全することになる。

「情報」の場合では、①関連する人間、②テクノロジー、

③電源や通信、空調と部屋・建物などと、④それらにある情報そのものを保護・保全する。情報を含め、関連するものを「情報資産」と定義している。

もちろん、電源や通信等は部屋・建物から更に外部に広がっており、更に広範囲で考える必要があるとの指摘もあるが、通常、その部分は、第三者の管理部分で、①から④の棄損や窃盗等から保護・保全することを、「情報セキュリティ」とか「サイバーセキュリティ」の分野と考える。

なお、第三者の管理部分は、何らかの事故などにより、供給されない状況に対して、「事業継続計画(BCP)」で、その対応を考えるが、第三者の管理部分の改良・改善には通常係わらない。

2. IoT とは？

「IoT」は、英語ではInternet of Thingsで、「モノのインターネット」と訳されるが、日本語は単数と複数の区

【人、情報、テクノロジー、設備】。ひとつ欠けてもセキュリティを確保できない可能性がある

図1 情報資産の概念図

Applications of IoT to plants and issues of safety and security on the applications(3) ; Review from security psychology : Katsuya Uchida.

(2018年2月23日 受理)

■前回タイトル
セキュリティ・安全技術

別が曖昧で、実際は、「色々なモノのインターネット」との考えである。もちろん、単にインターネットに繋がっているだけでなく、繋がっているモノ同士の情報交換・情報共有があって始めて有効になる。

色々なモノの多くがインターネットと繋がれば、既存のソフトウェアの利用が増え、そのソフトウェアの脆弱性が見つかれば、そこを攻撃される可能性も増える。標準ソフトウェアでは脆弱性の数は少なくなるが、脆弱性が放置される可能性があり、攻撃される可能性は高い。

II. セキュリティにおける騙しの考察

1. 誰が騙すのか？

従来、「騙し」では、ギリシャ神話にある「トロイ戦争」のように、何らかの道具を利用するが、基本は人間が人間を騙すと考えてきた。

コンピュータ時代、特に、IoT や AI 技術 (Artificial Intelligence: 人工知能) の高度化を考えると、人間が人間を騙すだけでなく、①人間が機械を騙す、②機械が人間を騙すことも考える必要がある。

図2では、「人間 (People)」と「機械 (Machines)」, 「人間と機械の統合化 (People & Machines)」での騙し・騙されを考えた。

ここで、

- ①人間：人間が対面で行う場合や単純な機器 (電話、FAX、郵便等) を利用して行う騙し (騙される側も同じ、以下同様)
- ②機械：内蔵プログラム (Programmable/Programmed) を持つ機械/機器が行う騙しで、最近では単純なプログラムだけでなく、AI 技術を利用したものが増えている。
- ③人間・機械：上記①、②の両方の機能を持って騙すもの

図2 攻撃者 vs 被害者

2. 騙し・騙され事例

図2の1~9までの中で、特徴的なものを説明する。

- ・「1. 人間⇒人間」(標的型電話攻撃)で、2012年に首都圏近郊自治体で発生した「ストーカー殺人事件」では、ストーカーは被害者の詳細な住所の取得を依頼し、依頼された経営者は、ソーシャルエンジニアリングの1つである「誘導質問術」を利用し、自治体職員から個人情報情報を盗取したと考えられる¹⁾。
- ・「6. 人間・機械⇒人間・機械」(標的型メール攻撃)で、メールに興味のある内容やタイトルをつけ、添付ファイルをクリックさせるものがある。

例えば、2016年6月に発生した旅行会社のグループ会社で発生した標的型メール攻撃は、送付元 (From) のメールアドレス表示は正しかったが、送付元には当該アドレスは存在せず、また、添付ファイルの内容が旅行会社に関する情報でなかった。このため、返信をしたが、「当該メールアドレスが存在しなかったため、発信メールが届かない (Delivery has failed to these recipients or groups:)」とのメッセージが返送された。標的型メール攻撃の教育・訓練を毎月実施されていたが、クリック後の対応教育・訓練が考慮されておらず、未達メール対応が放置され、情報漏えいを許した^{2,3)}。

公開された情報からの判断だが、訓練は実施されていたが、「クリック率を下げる」ことが中心だと思われる。攻撃メールを誤ってクリックした後の対応が十分でなく、「未達メール」等の対応訓練は行われていなかった。攻撃は年々進歩しており、新たな攻撃手法が採用されているため、従来の攻撃だけでなく、「想定外」への対応を考慮した教育・訓練が必要だと思われる。

情報漏えいは未達メール受信後、4日程度後から始まっており、未達メール受信時に対応ができていれば、情報漏えいを防ぐことができた。

- ・「7. 機械⇒人間」(人間になりすます)カナダの出会い系サイト「Ashley Madison (アシュレイ・マディソン)」事件では、男性利用者とチャットをしていた女性は生身の女性でなく、音声ボット (AI) が女性になりすまし、男性利用者を騙していた⁴⁾。
- ・「9. 機械⇒機械」(プログラムの脆弱性攻撃) インターネットでのTCP接続は、クライアントとサーバ間で、「Three-way handshake」(①SYN, ②SYN ACK, ③ACK)ⁱを実施した後に通信が始まるが、クライアントが③ACKパケットを送らないと、Three-way handshakeが完成せず、サーバは最後の「③ACK」パケットを待ち続ける。大量の「①SYN」パケットを送

ⁱ SYN: 同期 (synchronize の略) ACK: 肯定 (acknowledge の略)

付すれば、サーバは大量の「③ ACK」を待つことになり、サーバの処理能力が大幅にダウンする

Ⅲ. セキュリティマネジメント、セキュリティ心理学からの対応

1. 歴史に学ぶ

従来、人間の心理的な弱さを攻撃する「ソーシャルエンジニアリング」では、人間が人間を騙すと思われているが、現在は、「Ⅱ. 2 事例」からも分かるように、人間だけではなくなっている。

ドイツの「鉄血宰相」と言われた、オットー・フォン・ビスマルクの言葉の通り、「賢者は歴史から学ぶ(a wise man learns from history)」は、セキュリティの世界でも同じである。

セキュリティインシデント(事件・事故)の簡単な情報収集(データベース化)を行っているが、以下は、IoT 関連のインシデントと考えられる。

- ・1994 年 01 月 書籍「Secrets of a Super Hacker」の「Appendix B: Common Defaults」に UNIX で利用される既知のユーザ ID、パスワード(以下、ID/PW と記す)は 50 余りの単語が利用されていると記述している⁵⁾。
- ・2004 年 10 月 インターネット接続の DVD ビデオレコーダーの LINUX オペレーティングシステムが既知の ID/PW になっていたため、「踏み台」にされた⁶⁾。
- ・2010 年 11 月 国内の官公庁、企業、大学等に導入されている「ネットワーク接続の複合機」に保存されているイメージファイル(コピーや FAX、印刷に利用したファイル)が、複合機の ID/PW が既知になっており、外部からのアクセスでイメージファイルが盗取され、一部が公開された。
- ・2013 年 11 月 監視カメラの多くがインターネットに接続されるようになり、既知の ID/PW を利用しているケースでは、監視カメラの映像が丸見えになっていた⁷⁾。
- ・2015 年 01 月 WiFi ルータの初期 ID/PW がメーカー/機種毎に一律で、ただ乗りや乗っ取りが発生した。
- ・次に来るのは？(自社製品/自社利用製品【IoT 製品】の可能性は？)

- ①脆弱性の指摘：書籍「Secret of a Super Hacker」
- ②踏み台：インターネット接続ビデオレコーダー
- ③情報漏えい：ネットワーク接続複合機
- ④無権限アクセス：WiFi ルータ
- ⑤ライブ映像のぞき見：ネットワーク接続監視カメラ

図3 同種インシデントの時系列分析

同種のインシデントを時系列的にみると、全てインターネット接続の課題で、「Internet of Things」でのインシデントとも考えられる。次は、IoT 機器の可能性も高く、自社開発/利用の IoT 機器を導入した場合、リスクを考えた対応が大切になる。

図3「同種インシデントの時系列分析」は、これらをまとめたものだが、「モグラ叩き」的セキュリティ対応では見えなかったものも時系列(歴史)的分析で、明確になることも多い。

2. 他分野の知見から学ぶ

ビスマルクの考えからは、従来の情報セキュリティや IoT 等のセキュリティ分野における過去の知見からだけでなく、他分野での知見も参考にできる。

(1) CRM (Crew Resource Management)

1976 年、NASA(米国航空宇宙局)は技術や経験豊富なクルー 20 組を集め、シミュレータを使った実験を行い、問題点を明確にした。即ち、問題の多くは技術や技量の問題でなく、人間の問題(リソースマネジメント)であることが判明した。チーム・組織でのインシデント対応訓練が事故の未然防止や事故拡大を防止する。このことは、IoT セキュリティでも有用と考えられる。

当初、CRM は、Cockpit Resource Management と言われていたが、キャビンアテンダントや整備士等、関係者を含め、Crew Resource Management と呼ぶようになった。

また、かつて CRM では悪天候時に、格納庫(Hangar)に関係者が集まり、過去のインシデントや回避方法等の情報交換を行い、「安全文化」の構築・共有を行った。これを「Hangar Flight」と呼んでいる。

(2) Team STEPPS (Team Strategies and Tools to Enhance Performance and Patient Safety)

CRM の考えを医療分野に取り入れたもので、パイロットを頂点とした権威勾配が航空業界にあるように、病院でも、医者を頂点とした権威勾配があり、それらを越え、チームとして役割を果たすことが重要であることを学ばせる。

(3) 利用者側での対応

CRM や Team STEPPS は、利用者側からのセキュリティ対応と考えることができる。

高度で緻密な設計が行われ、それが実装され、セキュリティの技術ツールが導入されても、100% 完全には防ぐ事ができない。これは、実装までの段階でも、運用段階でも脆弱性が発生する可能性があるためである。2002 年 7 月に、米ホワイトハウスのサイバーセキュリティコーディネータ、ハワード・シュミット(Howard Schmidt)は、2001 年米国防総省の調査では、97%~98% は、「パッチⁱⁱを適用していなかったか、設定ミス」だと述べている。

システム設計やシステム構築側を考えると、パッチ未適用や設定ミスのようなヒューマンエラーの除去を考える必要がある。設定ミスの多くは、単純なヒューマンエラーだと考えられ、また、パッチ未適用は、「不作為」によるヒューマンエラーと考えることもできる。これは、サイバーセキュリティでは、悪意を持った第三者が攻撃を仕掛けることもあり、何もしなかった(不作為)ことが、結果としてインシデントに繋がる可能性がある。このような不作為でのインシデントは、「窃盗」でもある。無施錠で近隣に外出したため、「空き巣」被害を受けた例を考えれば明らかであろう。

(4) 攻撃者いろいろ！

歴史から学ぶだけでなく、今後の IoT では人間が関与する割合が低下し、機器(Smart Devices)や AI 技術などの関与が高まれば、図 2 に示した「機械」部分が大きな割合を占めると考えられる。

騙しやソーシャルエンジニアリングは飛躍的に広範囲なものになり、それらの調査・分析も必要になる。攻撃相手が人間であるか、機械(AI 等)であるかの判断をすることも困難であり、ますます巧妙になると考えている。

(5) セキュアデザイン, セキュアプログラミング

従来の情報セキュリティでは、ネットワーク構築時点や構築後の管理・運用段階での安全確保が中心と考えられがちであるが、システム全体を考慮して安全を確保することが大切である。今後、ますます増大する IoT 機器では、IoT の開発・設計段階やプログラミング段階のセキュリティ対策、即ち、セキュアデザイン、セキュアプログラミングは情報セキュリティより遙かに重要になり、機器認証だけでなく、心理学や認知科学の知見を考慮した利用者目線での設計も必要だと考えている⁹⁾。

IV. まとめ

国内では、サイバーセキュリティ対策は技術的対策が中心だが、海外では、2002 年、OECD(経済協力開発機構)の「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～」の公表以降、「セキュリティ文化の確立」が重要なものであると考えられるようになってきた。

また、サイバーセキュリティ対策として、人間への対応、即ち、心理学や行動科学、犯罪学等の知見を取り入れるようになってきた¹⁰⁾。

このような傾向は、IoT 分野でも同じであると考えている。

－ 参考資料 －

- 1) 内田勝也, 誘導質問術からみた個人情報漏えいの考察, 情報処理学会誌, Vol. 56 No. 12, pp. 2219-2229 (Dec. 2015).
- 2) (株)ジェーティービー, 個人情報流出の可能性のあるお客様へのご連絡について, 2016 年 6 月.
<http://www.jtbcorp.jp/jp/160616.htm> (既に削除されている)
- 3) 日経コンピュータ, [詳報]JTB を襲った標的型攻撃, 2016.06.15, 日経 BP.
<http://itpro.nikkeibp.co.jp/atcl/column/14/346926/061500549/>
- 4) 日経テクノロジー, 男性の相手は「会話ロボット」, 不倫サイトが見せた技術力, 日経 BP.
<http://techon.nikkeibp.co.jp/atcl/column/15/425482/092500020/>
- 5) Knightmare, Secrets of a Super Hacker, Loompanics Unlimited, 1994.01.
- 6) Internet Watch, 東芝, HDD 搭載 DVD レコーダ「RD」シリーズが「踏み台」になる危険性, 2004.10.06.
<http://internet.watch.impress.co.jp/cda/news/2004/10/06/4882.html>
- 7) 読売新聞, 監視カメラ覗き見? パスワード未設定が原因か, 2016.01.22.
<http://www.yomiuri.co.jp/science/goshinjyutsu/20160122-OYT8T50085.html>
- 8) Government Technology, Security First, 2002.07.01.
<http://www.govtech.com/security/Security-First.html>
- 9) D. A. ノーマン, 野島久雄訳, 誰のためのデザイン? 増補改訂版一認知科学者のデザイン原論, 新曜社, 2015.04.
- 10) OECD, 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(仮訳), 外務省, 2002.07.25.

著者紹介

内田勝也 (うちだ・かつや)

情報セキュリティ大学院大学 名誉教授
セキュリティ心理学, セキュリティマネジメント, リスクマネジメント等, サイバーセキュリティ分野における人的対象の研究およびコンサルティング

ⁱⁱ プログラムの一部を更新し、バグ修正や機能変更を適用する処理のこと