[倫理委員会活動報告]
開かれた技術者倫理のありかた：「セキュリティ心理学～セキュリティ最大の脆弱性を考える～」

電気学会 倫理委員会

倫理委員会では「開かれた技術者倫理のありかた」の勉強会として種々の業界の方に講演をして頂いています。本稿では，「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」などの調査研究でご活躍されている情報セキュリティ大学院大学名誉教授　内田勝也氏に，「セキュリティ心理学～セキュリティ最大の脆弱性を考える～」と題しご講演（2016/12/16）頂いた内容を紹介します。

1. 情報セキュリティへの考え方／何故，セキュリティ心理学か？ 何を目指すのか？

情報セキュリティの関心が高まっていますが，「基礎，基本」から逸脱しているケースが見られます。リスク・ファースト（Risk First）を考える必要があります。リスクの大きさは，脅威，脆弱性，資産価値の大きさを考えますが，環境変化や時間経過によってリスクは変わります。情報は機密性，完全性，可用性の３つを確保することが必要です。セキュリティでも，「Weakest Link」即ち，最も弱い所がそのシステムのセキュリティレベルです。一般に，情報資産を①人間，②情報（アナログ／デジタル），③技術（ソフト／ハード），④設備に分類します。

最近，サイバーセキュリティといった表現が使われますが，情報は単独では存在できません。決して，サイバーの世界でなく，リアルな世界なのです。また，「情報セキュリティはコンピュータやインターネット技術の問題である」と誤解をしている人が多いですが，「暗号技術」「コンピュータセキュリティ」「ネットワークセキュリティ」「管理，運用」「法制度，倫理」の５つの分野があります。国内外のインシデント調査では，その殆どが，設計ミスや管理不足に起因します。海外では既に人間やマネジメントの問題を考えない限りセキュリティは確保できないと言われており，ヒューマンエラーや Deception（欺術）が Key となっています。このように，情報セキュリティはセキュリティ技術者だけでは解決できない問題であり，「セキュリティ心理学」が求められているのです。

情報セキュリティをセキュリティ心理学の観点で概観すると，攻撃者の問題と防御をする者の問題があります。「Deception」，即ち，人間が人間を騙す，人間が機械を騙す，機械が人間を騙す，機械が機械を騙す等が考えられます。また，物理的な問題もあり，環境犯罪学や状況的犯罪防止論といった知見も必要になってきます。

2. セキュリティ心理学：攻撃手段＆手法

過去の事例から，その攻撃手段，手法には大きく４つあります。①なりすまし：標的型電話攻撃【誘導質問術の利用】，②ゴミ箱漁り（Dumpster Diving），③サイト侵入（なりすまし），④のぞき見（Shoulder Surfing），⑤その他：（親切！ 一瞬のスキ？ など）です。①は 2012 年の「逗子市ストーカ殺人事件」，②は 1979 年の「イランの米国大使館封鎖」でストレートカットのシュレッダーゴミ片を手作業で復元した事例がありました。（注）

3. セキュリティ心理学：攻撃技法

攻撃は人間の持つ６つの脆弱性をついてきます。①返報性，②コミットメント一貫性，③社会的証明，④好意，⑤権威，⑥希少性　です。特に「誘導質問術（Elicitation）」は当該の対象者から直接，その内容を聞くことなく，情報収集する方法で，効果的に使えば，人を誘導し，望みの行動を行わせる質問を考え出せます。（注）

4. セキュリティ心理学：防衛対策／まとめ

防衛対策の基本は「敵を知り己を知れば百戦危うからず」です。最近の事件の多くが，過去の事件の模倣やいくつかの欺術の組み合わせです。イランの核施設攻撃事件のように可搬媒体（USB など）による攻撃もあり，ネットワーク攻撃だけではありません。

情報セキュリティは，「性弱説」（人間は弱いもので，誘惑に負けてしまうことがあるという説）で考えるべきです。日本では「性善説」を前提として対応する企業が多いのですが，性善説でも管理をしないで良いことにはなりません。効果的対策としては，「環境犯罪学，状況的犯罪予防」からの知見の活用や個人だけでなくチームとしての教育訓練が重要だと考えています。（注）

（注）具体的な事例の詳細は省略。ご講演の詳細資料に興味のある方は電気学会倫理委員会事務局（rinri@iee.or.jp）まで連絡ください。

（まとめ：倫理委員会　幹事　石橋　邦夫(株)日立製作所）