iSiD

KnowBe4
Human error. Conquered.

セキュリティ「文化」を考える

2020

著者

アルテア・セキュリティ・コンサルティング
代表

二木真明

思考停止にならないセキュリティを目指して

本ホワイトペーパーは、セキュリティ有識者である著者が客観的な視点で記載したドキュメントです

OptimizingYourSecurity

内容

初版　2020年6月1日

はじめに

生活やビジネスの大部分を ICT に依存している「サイバー」時代、コンピュータやネットワークの能力は劇的な向上を続けています。新たな技術が次々と登場し、「人工知能」とも呼ばれる深層学習の応用により、従来、人が担ってきた領域までも、機械化、自動化が進みつつあります。しかし、それらが人の手による産物であり、人による社会やビジネス、生活を補助するための道具として作り出されたものである限り、依然として人は、それらの使い手であり続けます。様々な考え方を持つ人がいるように、これらの道具の使われ方も様々です。機能や能力が向上すればするほど、誤った目的や悪意を持った使い方がもたらす結果は深刻なものとなります。つまり、サイバー技術が進化すればするほど、人はより慎重に、高い倫理観を持って、これらを使わねばならないのです。

近年頻発している「サイバー攻撃」や「サイバー犯罪」は、悪意を持った使われ方の典型的なものでしょう。一方、これらの被害を受ける側にも「油断」があります。少し慎重に対処していれば、避けられた被害も少なくありません。技術的な対策も可能ですが、そればかりを強化すれば使い手の自由度を低下させ、生産性や創造性を損なう危険があります。ICT の使い手には、その自由度に応じて、こうした脅威の存在やその目的、手段を意識して、つけいる隙を与えないことが求められますが、これは一般に簡単ではありません。

本書では、企業・組織の ICT 利用における「人」に着目して、こうしたリスクを下げる方法を考えます。

1. すべてがICTに依存する現代

想像してみてください。世の中にコンピュータやネットワークがなかったら、家庭での生活や職場での仕事はどのようになるでしょう。パソコンやネットワーク、様々なサーバが使えなかったら、デスクワークはすべて紙と鉛筆と消しゴムの世界に戻ってしまいます。生産現場ではロボットや自動化された加工装置などの一切が使えず、昔ながらの手作業に戻ります。家庭においても、いわゆる「デジタル家電」はすべて使えなくなり、昔ながらのアナログな世界に戻ります。今から50年ほど前の世界を想像すればいいでしょう。この時代を知っている人たちは、それでも生活や仕事に問題はなかったと思うかも知れません。しかし、今、その時代に戻ったとしたら、はたしてどうなるでしょう。社会が動いているスピードは当時とは比較になりませんし、そこには高度な情報流通が欠かせません。現在の経済規模を維持するだけの生産性を得るためには、様々な自動化手段や通信手段は不可欠になっています。そう言う意味で、我々は既にICTにその命運を委ねていると言っても過言ではないのです。

東日本大震災の前、企業のIT部門でBCP（事業継続計画）策定に携わった経験がありますが、災害などでICTが使えない前提でのビジネスは成り立たないということを痛感させられました。災害に対処してビジネスを維持するには、ICTの復旧が不可欠であり、いかにそれらを迅速に復旧するかが、企業IT部門におけるBCPの第一目標なのです。大震災では、電源や通信手段が大きな被害を受け、被災地のビジネスは長期間停止を余儀なくされました。全国規模の大企業はともかく、地場の中小企業にとっては致命的な事態です。

一方、2020年に発生した新型コロナウイルスのパンデミックでは、世界的に人の流れが止まることによる経済への影響が深刻化した一方、ICTの活用やテレワークによって業務を維持した企業も少なくありません。しかし、急激なテレワークへの移行は通信回線や関連する設備に想定外の負荷をかけ、当初、様々な問題が生じました。また、こうしたICT活用への不慣れが原因の問題も多発しています。とりわけ学校のオンライン授業や自治体業務のオンライン化などにおいては多くの課題を残しました。情報セキュリティの面でも、急激な変化はリスクをはらみます。十分なセキュリティ対策を講じる余裕もなく、不慣れな社員にテレワークをさせるという状況が生じ、そこを狙ったフィッシング詐欺やサイバー攻撃が頻発することで、被害も発生しています。しかしながら、こうした経験を経て、社会のICT依存はさらに強まっていくでしょう。

このように、社会やビジネスの基盤がICT化されていくにつれ、それらを狙った犯罪の手段もICT化されていきます。かつて、技術を誇示したい者たち（ハッカー[1]）が、これみよがしに行っていたサイバー攻撃やコンピュータウイルスの技術は、今や企業の情報や消費者の個人情報などを狙った「サイバー犯罪」の手段となりつつあります。旧来からの詐欺の一部は電子メールやフィッシングサイトを使ったものに、窃盗は、電子メールやオンラインバンキングや通販サイトへの不正アクセスを手段としたものにと、次第に変化しつつあります。社会がICT依存を強めれば強めるほど、犯罪者もまたICTを手段として使うようになっていくのです。

このような「悪意あるICT利用者」に備えるためには、新たな「常識」が必要です。現実世界では、犯罪の抑止のために、様々な「常識」が存在します。外出時の戸締まり確認や「鍵」の管理、暗い夜道の一人歩きは避けるといった基本的なものから、ひったくり防止のために、鞄は道路側の手に持たず、自転車のカゴにはネットをかけるといったものなど様々あり、多くが習慣となっています。一方で、ICT活用、すなわち「サイバー」社会での犯罪抑止の方策については、まだまだ常識と言うには、周知が不十分なものが少なくありません。技術やサービスの変化の速さも、その点ではマイナスに働きます。

1…Hacker：一般にはコンピュータシステムの侵害を企てる者の意味で使われるが、インターネットの黎明期においては、高い技術を持つ技術者への敬称として使われた経緯があり、いまだに、この言葉を悪者の意味で使うことに抵抗感を持つ人たちもいる。彼らは悪者のことを「クラッカー」と呼称する。

著者紹介

二木真明　（ふたぎ　まさあき）

アルテア・セキュリティ・コンサルティング（個人事業）　代表

1956年生まれ

17年間の制御系やUNIXシステムプログラマー、SEとしてのキャリアの中で、ファイアウォール製品を開発し、商品化したことから情報セキュリティの世界に踏み込む。その後、現在まで25年近く、情報セキュリティの様々な分野で経験を積んだ。2000年以降は、大手商社系SIerに勤務し、海外セキュリティ製品の発掘や技術評価などにたずさわる一方で、自社内の情報システム部を兼務し、様々なセキュリティ対策の導入やルール整備、社内SOCの業務等を主導した。2012年に独立して、その後は経験を活かして、主にユーザサイドの様々なセキュリティ案件の支援や社内教育サポート、セキュリティベンダーの製品開拓、立ち上げのアドバイスなどを行っている。

CISSP: (ISC)2認定情報システムセキュリティプロフェッショナル
CISA: ISACA認定情報システム監査人

その他経歴など

2014年4月～2017年3月　埼玉県警察サイバー犯罪対策技術顧問
CSAジャパン（日本クラウドセキュリティアライアンス）運営委員
同IoT ワーキンググループリーダー
JNSA（NPO 日本ネットワークセキュリティ協会）幹事
株式会社　電通国際情報サービス　金融システム事業部　セキュリティ戦略アドバイザー

主な執筆書籍：

IT管理者のための情報セキュリティガイド　インプレス Next Publishing

【共著】

IoTセキュリティ　日経BP社　　（3-3 IoTシステムのリスク評価を考える）
APT対策入門　日本セキュリティ監査協会編　インプレス Next Publishing

その他、Web等、執筆記事多数