未来につなげる心のセキュリティ

ドコモ・システムズ株式会社
山畳　秀人

はじめに

2014年7月に大手通信教育会社にて、2000万件を超える、大量の顧客情報流出事件が発生しました。なぜそのような事件が起きてしまったのでしょうか。

顧客データベースのシステム操作権限を持つ業務委託先社員は、私生活の中で金銭面に苦しんでいました。扱っている顧客情報を不正に持ち出し、名簿業者に販売することを画策しているとは、周囲の人は誰も気が付くことができませんでした。顧客情報の不正持出防止のために導入していたセキュリティシステムは、最新のスマートフォン対策を行っていなかったため、スマートフォンを通して、1年間も不正持出を許すこととなってしまったのです。

たとえ、高度なセキュリティシステムを構築しても、コンピュータデバイスの進化スピードに合わせられなければ、権限者のモラルに依存するしかありません。セキュリティルールを理解させるだけでなく、不正を引き起こす人間心理を理解し、心のセキュリティ強化に向けた対策が、より重要な時代になってきたと言えます。

本稿は、私見ではありますが、心のセキュリティのあり方に関して、議論していくきっかけになれば幸いです。

不正行為を早期発見するために

不正行為に至る可能性のある社員、不正行為を働いている社員を早期発見するためには、どのような対策が必要なのでしょうか。セキュリティ研修で理解度テストを行っても、１００点満点を取れば、問題なしとなります。セキュリティルールを理解しているので、ヒューマンエラーも少なく、要注意人物とはならないかもしれません。ずる賢ければ、形式的になっているルールの穴をかいくぐる方法に気づき、その方法を秘匿し、チャンスをうかがっているかもしれません。悪意に気づかれないよう、まじめな言動を心掛け、油断させてくるかもしれません。

そのような、要注意人物の存在に気づく方法はないのでしょうか。要注意人物を改心させ、心のセキュリティを育成する方法はないのでしょうか。

人のなにげない表情、言動から、隠された心情を読み解くことができれば、不正に至る前に対処ができるかもしれません。私生活での苦境を早期に気づいてあげることができれば、周囲のフォローにより、不正行為に至らずにすむのかもしれません。

不正防止に向けたポイント
① なにげない表情、言動の変化に注意する
② 隠された心情を読み解く
③ 私生活の苦境に早期に気づく
④ 周囲のフォローで不正行為を予防する

心理プロファイリング手法の活用

隠された心情に気づき、見えない私生活での問題を見抜く、「プロファイリング」という専門能力を持った人たちがいます。警察等の犯罪捜査で活躍されている方が多いかと思われますが、一般的な研修講師においても、心理面のプロファイリング能力を用いながら活躍されている方もいます。この心理プロファイリング手法を用いて、不正行為に至る可能性のある社員を、早期発見、対処する手順を考察してみました。

最初に、自意識のコントロール状況を確認します。仕事中の意識と私生活の意識にアンバランスがある場合、そのギャップから生じるストレス発散をどのように行っているかで、心理面のリスクが見えてきます。ギャップがなければ大丈夫というわけではなく、本人に自覚がない場合もあり、自己観察できていない場合は要注意です。

次に、心の弱みに対する自覚状況を確認していきます。心理誘導に弱い部分を自覚できていない場合は、無意識に不正に加担してしまう場合があります。強い思い込みや特定の感情に固執しやすいことを自覚できていない場合は、突発的に不正行為に至りやすいので要注意です。

最後に、組織と個人の価値観の違いから生じる心理矛盾がないか確認していきます。組織の命令は守るべきとわかっていても、私生活の苦境脱出を優先させたいという心理矛盾に至っている場合は要注意です。愚痴を何も言わず、心理矛盾をひとりでかかえこんでいる場合も注意する必要があります。

これら、心理プロファイリングによるチェック内容を参考に、周囲の社員、委託先社員へ気配りをしていただくことで、不正防止につながるものと思われます。

心理プロファイリング・チェックポイント
① 仕事意識と私生活意識にギャップがないか
② ギャップのストレス解消方法に問題はないか
③ 心の弱みを自覚できているか
④ 心理矛盾をかかえこんでいないか

心のセキュリティ研修の進め方

心のセキュリティを向上させるためには、各個人が努力するだけでは不十分で、社員や委託先との間で、心のセキュリティのあり方をディスカッションし、不正心理に至らないよう相互フォローしていくことが重要となります。

心理プロファイリング手順を参考に、研修形式で展開していく方法について考察してみました。

最初に、意識の裏表に関するテーマに取り組みます。仕事意識と私生活意識のギャップとストレス発散方法を共有していくことで、不正に至る動機につなげないための工夫を生み出していきます。

次に、心の弱みと心理矛盾に関するテーマに取り組みます。不正への心理誘導パターンを共有し、強い思い込みや特定の感情から生じる心理矛盾が、どのようなリスクを生み出すのか想像しながら、想定外の事態に備えられるようにしていきます。

最後に、組織と個人で取り組む、心のセキュリティのあり方についてディスカッションしていくことで、各自の心の弱さを補完しあえる組織風土作りにつなげていきます。

心のセキュリティ研修ステップ	
1	意識の裏表を持つ動機を探る
2	不正行為に至る心理矛盾を分析する
3	心のセキュリティのあり方を考える

心のC－I－A

心のセキュリティを向上させていくための具体的な指針は、心理学方面では整備されていないため、情報セキュリティの指針である、C－I－Aに準拠し、情報資産を心に置き換えて定義してみます。

C（機密性）は、情報資産を守るためのアクセスコントロール、暗号化等を行う指針で、心理面でも同様に、秘密を守る心がけを持ち、信頼できる相手を選び、相手に応じた心の開示方法を考えるようにしていきます。

I（完全性）は、情報資産の改ざんを防ぐためのチェック、不正操作監視等を行う指針で、心理面でも同様に、不正を起こさない心がけを持ち、不正な心理誘導や思考操作で心理矛盾を持っていないか、自分自身の心情を確認するようにしていきます。

A（可用性）は、システムの不具合に備え、いつでも情報資産にアクセスできるための二重化、バックアップ対策等を行う指針で、心理面でも同様に、柔軟に対応する心がけを持ち、ひとつの考え方にこだわらず、感情に固執せず、反省しながら間違いを正していく意志を持ち続けるようにしていきます。

情報セキュリティを意識する際に、自身の心とも向き合うことが、心のC－I－Aの基本動作となり、各自の心模様に合った対策を考えていただければと思います。

心のC－I－A		
C	機密性	秘密を守る心がけ
I	完全性	不正を起こさない心がけ
A	可用性	柔軟に対応する心がけ

脳とコンピュータがつながる未来

この先、コンピュータを扱う人の心は、どのように進化していくことができるのでしょうか。コンピュータ技術の進化に、追随していけるのでしょうか。少し先の未来のことについて考察してみたいと思います。

2045年頃には「シンギュラリティ」と呼ばれる技術的特異点を迎え、コンピュータが人間の脳をシミュレーションできるようになり、人工知能に依存する時代になると予測されています。脳神経科学も進化し続けており、脳神経ネットワークを通して記憶をコンピュータにアップロードしたり、ダウンロードしたりできるようになり、100年後あたりでは、人の心と心をつなぐ、心のインターネット時代が実現できるのではないかと予測されています。

セキュリティ技術者であれば、そのような時代に何が問題となるか、容易に想像できると思います。コンピュータインシデントと同様に、心へのサイバーアタック、不正アクセス、ウイルス感染、記憶改ざん等のセキュリティ脅威が発生し、人の心にもコンピュータセキュリティと同様のセキュリティ機能の構築が必要になるのではないでしょうか。

心のインターネットから流入してくる感覚、感情、思考をフィルタリングする、心のファイアウォール機能。正常なコミュニケーションに見せかけた不正な心理操作から心を守る、心の不正検知機能。心を崩壊させる感情や思考の埋め込みを排除するための、心のアンチウイルス機能。これら心のセキュリティ機能を、心のインターネット時代が始まる前までに、人の心に実装していくことはできるのでしょうか。

心のセキュリティ機能		
C	機密性	心のファイアウォール
I	完全性	心の不正検知
A	可用性	心のアンチウイルス

心のセキュリティ発展に向けて

現代において、人の心の中にも「無意識」という心のインターネットのような世界があります。無意識に生じる様々な感覚、あふれ出る感情、とりとめのない発想を、無意識のインターネット側からの情報と仮定すれば、それらを「意識」というクライアント機能で受け取って選別し、認識していることになります。「意識」では、特定の感覚ネットワークに接続し、不要な感情パケットを制御し、必要な発想データのみをダウンロードしていきます。無意識の心のインターネット側には、意識を守るためのセキュリティ機能が存在していて、過剰な感覚、感情、妄想を発生させないよう制御しています。このように、セキリティ技術者の視点で心をリバースエンジニアリングしていくことで、コンピュータに劣らない、心の潜在能力が解明されていくのかもしれません。

心のC－I－Aを定着化させ、心のセキュリティ機能を育成し、無意識に動いている心のセキュリティ機能とも連携できるようになるためには、どのくらいの年数がかかるのでしょうか。

心のC－I－Aについては、浸透に向けて努力していくことで、企業社員を中心に、数年程度で定着化が期待できると思われます。

高度な心のセキュリティ機能を身に着けるためには、幼少の頃から本能レベルの訓練が必要になるかもしれません。そのためには、親たちの理解を得る必要があります。親たちの理解を得るためには、親自身が子供時代に学校教育の中で、心のセキュリティの必要性を学ばなければ、育成もできないと思われます。学校教育の中に組み込むためには、政府の理解も必要です。政府の理解を得るためには、根拠のある実証実験が必要となります。

心のセキュリティ展開ステップ	
1	企業に心のC－I－Aを定着化
2	政府による心のセキュリティ研究開始
3	学校教育制度への組み込み
4	親による幼少教育の定着化

現実的には、心のセキュリティ機能実装の早期展開は困難で、心のインターネット時代を迎えた時に、心のセキュリティ事件・事故が発生し、コンピュータセキュリティ時代と同様に、遅れながら対策をとっていくのかもしれません。

数世代にわたる研究課題

心のインターネット時代を100年後と仮定すれば、その間にどのような課題が発生するのでしょうか。未来のことは誰にもわかりませんが、予測して備えることも重要かと思われます。

2045年頃のシンギュラリティによる影響前後で課題は変わるものと推測され、脳神経科学の発展によって、心がインターネットに接続できるようになる前後でも、課題が異なると思われます。それら課題分類で世代を分けると4世代となります。

世代を超えて実現させていく、心のセキュリティの研究については、有志による「心のセキュリティ研究会」でとりまとめた内容を参照ください。

心のセキュリティ世代	
第一世代	シンギュラリティ前
第二世代	シンギュラリティ後
第三世代	心のインターネット前
第四世代	心のインターネット後

出典：心のセキュリティ研究会
URL：http://security.cocoroai.net/

おわりに

コンピュータ技術の進化にセキュリティ対策技術は遅れをとりながら、人のモラルに依存するスタイルは、今後も変わらないかもしれません。人の心には潜在的な脆弱性があり、教育による理性でセキュリティマインドを保っているのが現状です。セキュリティルールを理解させるだけでなく、人間心理を理解し、心の脆弱性対策を行うことが求められています。2045年頃の「シンギュラリティ」と呼ばれる技術的特異点を超えたあたりから、脳とコンピュータがつながり始め、心と心をつなぐインターネット時代が幕を開けようとしています。人の意識レベルではコントロールできない、無意識レベルでのセキュリティ対策が求められ、対策の遅れは心の崩壊につながります。人の心は簡単に進化するものでなく、数世代かけて計画的に心のセキュリティ機能を開発していく必要があると思われます。

未来の子孫のために、どのような心のセキュリティ対策を残していくことができるのでしょうか。今しかできないこと、今だからできることに、それぞれの立場、役割の中で、共に取り組んでいきましょう。