創英の「セキュリティ」への向き合い方

AI活用のセキュリティと、サイバー攻撃からの組織防衛

共同代表（最高経営責任者）・弁理士　柳 康樹

時代の移り変わりとともに、私たちを取り巻くビジネス環境も日々変化しております。特に、生成AIの普及や、それに伴うサイバー攻撃の高度化は、企業の知財活動においても無視できない課題となってまいりました。

私たち創英は、創業以来、お客様の大切な発明や創作をお預かりし、その権利化を支援してまいりました。しかし、デジタル技術が社会基盤となった現代において、事務所の役割は「権利化」だけにとどまりません。お客様からお預かりした情報の「機密性」を、確実な管理体制で守り抜くこと。これは、現代の事務所に求められる最も基本的、かつ重要な役割だと考えております。

そこで今回は、昨今多くのお客様からご関心をいただいている「情報セキュリティ」の観点から、創英が現在取り組んでいる二つのテーマについて、方針と具体的な施策をご紹介します。一つは「創英におけるAI活用のセキュリティ環境」、もう一つは「サイバー攻撃に対する実戦的安全性強化」です。

1 創英におけるAI活用のセキュリティ環境

(1)AIツールのセキュリティの構造

生成AIの技術は、知財実務の効率や品質を向上させる可能性を秘めています。しかし、その活用にあたっては、「入力した情報がAIの学習に使われ、意図せず流出してしまうのではないか」という懸念が払拭されなければなりません。

創英では、こうしたリスクを根本から排除するため、創英の管理下にある「閉域網」の中で動作するAIツールのみを所員が使用できる環境を構築いたしました。創英におけるAI活用の安全性確保のためのシステム構造について説明します。

①プロンプト・回答データの厳重な内部管理

お客様からお預かりした資料などと同様、私たちがAIに入力する「指示（プロンプト）」や、AIが生成した「回答内容」についても、すべて創英のセキュアなサーバー内で厳重に保管・管理しております。

②通信の完全暗号化

AIを利用する際、創英サーバーとAI処理を行う外部クラウドとの間の通信はすべて暗号化されております。

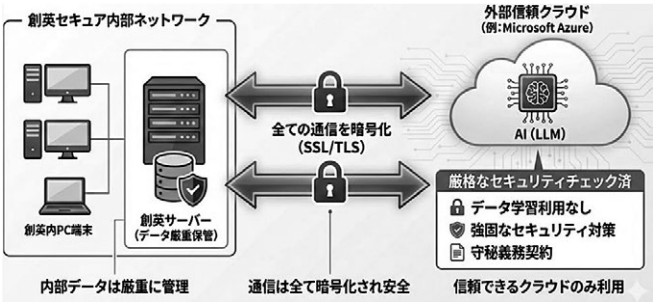
③AIによる学習利用の完全防止

AI処理を行う外部クラウドとして、創英では、Microsoft

Azureなどの信頼できる企業向けクラウド環境のみを利用しています。

これらの企業向けクラウド環境では、一般公開されている無料のAIサービスとは異なり、「入力した情報をAIの学習には一切使わない」ことが契約上保証されています。

つまり、あるお客様に関する情報がAIに記憶されてしまい、将来的に他のお客様の案件に対する回答に混入してしまう、といったことはございませんので、どうぞご安心ください。



〈図表1〉AIツールの安全性確保について

なお、上記①～③の構造自体は必ずしも創英独自の特別なものではございません。もし、貴社でMicrosoft Teamsなどのクラウドサービスをご利用であれば、基本的な構造は共通していると言えます。これらのサービスも、セキュアなクラウド環境下でAI支援機能を提供しており、安全性の考え方は同じです。

創英の所員は、独自に開発したアプリケーションを通じてのみ、この安全なAI機能にアクセス可能です。ある所員の業務で使用したデータが、別の所員の業務に混入する「情報のコンタミネーション」も発生しないよう、システム設計を行っております。

(2)一般公開AIツールの利用禁止

上述のようなAIツールを準備すれば十分でしょうか？いえ、AIツールの準備だけでは十分でなく、所内の「運用ルール」も重要であると考えております。

現在、Webブラウザで手軽に利用できる便利な無料のAIサービスが数多く存在します。これらについて、「公開情報であれば入力しても良いのではないか」「個人情報を伏せれば使えるのではないか」という声も聞かれます。

しかし、創英では、これら一般公開されているAIサービスへの情報入力を、情報の機密性にかかわらず「全面的に禁止」しております。

なぜなら、「情報は伏せたから大丈夫」「これは秘密情報ではないから大丈夫」という判断を個々の所員に委ねること自体が、セキュリティ上のリスクになり得ると考えているからです。

私たちは、所内のPCからこれら外部のAIサービスサイトへのアクセス自体を技術的に制限しています。技術的に「利用できない」状態を作り出すことで、人為的な判断ミスによる情報漏洩を未然に防ぐ体制を整えました。AI活用については「やってはいけないこと」の線引きを明確にし、システム的に管理することが事務所としての責任であると考えています。

2 サイバー攻撃に対する「実戦的」安全性強化

昨今、日本企業を取り巻くサイバーセキュリティの脅威は、かつてないほど深刻さを増しています。特に、近年急増しているのが、ランサムウェア（身代金要求型ウイルス）や、AIを悪用した巧妙なフィッシング詐欺メールによる被害です。

国内でもランサムウェアの攻撃件数は大幅に増加しており、製造業や小売業の大手企業がシステム停止に追い込まれたり、数百万件規模の個人情報が流出したりする事例が後を絶ちません。

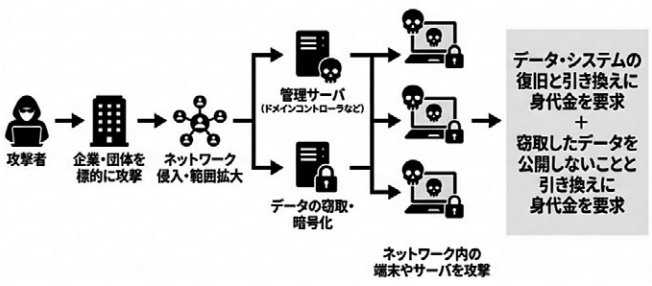
(1)AIが悪用される時代の「人間」の脆弱性

恐ろしいことに、私たちが業務効率化のために活用しようとしているAI技術は、攻撃者にとっても強力な武器となっています。

かつての詐欺メールは、不自然な日本語や怪しいレイアウトですぐに見抜くことができました。しかし、生成AIの発達により、攻撃者は流暢かつ自然な日本語で、日本企業の商習慣に完全に即した「本物そっくり」のメールを、24時間体制で大量生成できるようになりました。

こうした攻撃は、ファイアウォールなどのシステム的な防御壁を正面から突破するのではなく、メールを受信する「人」の心理的な隙を突き、内部から鍵を開けさせる手口です。どれほど高価なセキュリティソフトを導入しても、所員がワンクリックしてしまえば、そこが侵入経路となります。

つまり、現代のセキュリティ対策においては、システム強化と並行して、所員一人ひとりの「防衛力」を高めることが不可欠となります。



〈図表2〉ランサムウェア攻撃について

(2)外部委託ではなく「内製化」された訓練

そこで創英では、全所員を対象とした「標的型攻撃メール訓練」を実施しています。これは、詐欺メールを模したテストメールを所員に送信し、擬似的に攻撃を体験させる訓練です。

多くの企業様でも同様の訓練が行われているかと思いますが、創英の訓練には決定的な違いがあります。それは、訓練の企画・設計・実行を外部業者に丸投げせず、創英のサイバーセキュリティ対策チーム(以下、「対策チーム」)が完全に内製で行っているという点です。

創英も以前は、外部業者の訓練サービスを利用しておりましたが、どうしても定型的な文面のメールが定期的に送られてくるだけになりがちでした。これでは回を追うごとに所員が「また訓練か」と慣れてしまい、形式的な消化試合になってしまいます。攻撃者は日々進化しているのに、守る側の訓練がマンネリ化していては意味がありません。

私たちは、この課題を克服するため、あえて「内製」にこだわりました。創英の対策チームは、最新のサイバー攻撃の手口を常に分析し、外部業者よりもはるかに難易度の高い、巧妙な訓練メールを作成しています。

その「巧妙さ」の最たるものが、「タイミング」です。

実際のサイバー攻撃者は、私たちのスケジュールを知っているわけではありません。しかし、脅威となるのは、無差別な攻撃が、たまたま私たちの「繁忙期」や「心理的な隙」と重なってしまった瞬間、すなわち「不幸な偶然」です。いつもなら無視できるメールでも、忙殺されている最中に届くと、十分な確認をせず「業務連絡か」と誤認してしまう。これこそが事故の最大の原因です。

私たちの対策チームは、あえて所員にとっての隙になりやすいタイミングを狙い、システム部門からの緊急連絡を装った訓練メールを送信することもあります。もちろん、訓練メールには注意して読めば偽物であることが判別できるヒントを散りばめています。

例えば、所員にとっての繁忙時期や、メール処理が増えやすい時間帯などにあえて訓練メールを送ることもあります。あるいは、社内で「災害時の安否確認訓練」などを実施した後に、「先日の訓練結果を以下のリンクから確認してください」のような文面の訓練メールを送ることもあります。「先日訓練があったばかりだから、その連絡だろう」という思い込みと、実際の攻撃メールの着弾が不幸にも一致してしまった状況を、安全な訓練の中で体験してもらうのです。

実際、攻撃者の立場からすると、日本で大きな地震が起きたときなどは、偽の安否確認メールを送ったり、防災アプリのダウンロードと偽って不正なアプリをインストールさせようとするメールを送ったりすることは容易に想定されます。災害への備えと同様に、こうした便乗攻撃への備えも必要不可欠です。

これは一見、厳しいやり方に見えるかもしれません。しかし、実際の事故は、こうした「不運なタイミング」でこそ発生します。

「訓練で失敗することは、恥ではない。むしろ、本番で騙されないための貴重な『免疫』になる」

私たちはそう考え、失敗しても実害のない訓練の中で、あえて「ヒヤリとする経験」を積むようにしております。この高難易度の訓練を日常的に繰り返すことで、所員一人ひ

とりの中に、「怪しいメールは開かない」という基本動作だけでなく、「わずかな違和感で立ち止まる」高度なセキュリティ感覚が養われています。

(3)経営陣の参加

さらに、この訓練体制の構築には、私を含む経営陣が深く関与しています。

ただし、私が具体的なメールの文面やトリックを考案しているわけではありません。対策チームが所員に対して不必要な遠慮や躊躇なく、「本番に即した、意味のある訓練」を実行できるようにするための環境作りが私の役割です。

通常、こうした訓練をシステム部門だけに任せてしまうと、同僚である所員に対して「業務の妨げになってはいけない」「難しすぎては申し訳ない」という配慮をしてしまいがちです。その優しさが、結果として「形式的で簡単な訓練」を生み、本番での脆弱性につながってしまうことがあります。

そこで私は、経営トップとして、「この訓練は、お客様の情報を守るための重要なものである」と、システム部門だけでなく、全所員に向けて明確に宣言しています。

これにより、システム担当者は必要以上の遠慮を捨て、プロフェッショナルとして躊躇なく、実戦的な訓練を設計できるようになります。

一方、訓練を受ける所員たちも、「なぜこれほど厳しい訓練が必要なのか」という背景を理解しているため、高難易度のメールに対しても「意地悪だ」と反発するのではなく、「自分たちの守備力を高めるための重要な機会」として、前向きに受け止めることができます。

このように、攻める側(システム部門)と守る側(所員)の双方が、共通の目的意識を持つことで、初めて健全かつ高度な訓練が成立するのです。

なお、訓練の対象は一般所員だけではありません。私を含む経営陣に対しても、容赦のない攻撃訓練を行うよう指示を出しています。経営陣が持つ権限や情報の重要性を考えれば、攻撃に引っかかってしまった場合のリスクは、一般所員よりも格段に高くなります。そのため、経営陣に対しては、一般所員向けよりもさらに難易度を上げた、巧妙な攻撃メールを送るよう、対策チームに指示しています。

経営陣自らが「聖域」を作らず、最も厳しい訓練の対象となり、全所員とともにセキュリティ意識を高めていく。これは、高度な情報化社会において、お客様の情報を守ることを重要課題と位置づける、創英の経営方針の表れです。

3 結び
～信頼という名の「無形資産」を守り抜くために～

創業40周年を迎え、新体制となった創英は、「第二の創業」として組織のあり方を大きく進化させています。しかし、どれほど組織が変わろうとも、私たちが守るべきものの本質は変わりません。

それは、お客様からお預かりした知的財産であり、お客様との間に築き上げてきた「信頼」という無形資産です。

テクノロジーの活用による業務品質の向上と、セキュリティの強化。

この二つは、これからの事務所にとって車の両輪です。どちらか一方が欠けても、お客様に安心して業務をお任せいただくことはできません。

「創英に任せておけば、技術面でもセキュリティ面でも安心だ」
「さすが創英、ここまで徹底しているのか」

そう言っていただくために、私たちは、目に見えるサービスの向上だけでなく、目に見えない「安全」の基盤づくりにも、妥協なく投資してまいります。

進化する環境に対応し、お客様の知的財産を守り抜く「ベストパートナー」として。新生・創英の挑戦に、どうぞご期待ください。