AIが開けたサイバーセキュリティーパンドラの箱

金融機関、企業はいかに対策すべきか

グローバルリサーチ研究所代表
青木　武

あおき・たけし　慶大卒。99年米ニューヨーク大学経営学修士（MBA）取得。信金中金総合研究所ニューヨーク駐在主任研究員等を経て、09年7月米国内にグローバルリサーチ研究所（IGR）を設立。http://www.igrlc.com/

人工知能（AI）の分野では、ここ数カ月、アンソロピック社の「ミュトス」が話題となっている。もともとはソフトウエアの脆弱性を見つけることができるAIツールであるが、悪用されれば金融機関や企業のソフトウエアの脆弱性をスピーディーに発見することができるため、大いなる脅威であると考えられた。一方、これは上場を目指すアンソロピック社の上手なマーケティング、という見解もある。「真実は中庸にある」とも考えられるが、ミュトスがAIによるサイバー攻撃に対する可能性、というパンドラの箱を開けた今となっては、金融機関や企業はその対策も必要となっている。

(1)はじめに

ミュトスとは、アンソロピック社が開発したAIツールであり、ソフトウエアの小さな脆弱性を見つけて、それをチェーンのようにつないで企業等のシステムに侵入することを可能にするソフトウエアである。つまり、同じサイバーセキュリティーへの脅威でも量子コンピューターのように、暗号を無力化してすべてを破壊してしまう、というよりは、相手の防衛網を巧妙にかいくぐって侵入する仕組みである。いわば、量子コンピューターがソ連の核弾頭ミサイルだとすれば、ミュトスはイランのドローンのような脅威である。ただし、現実の戦争の主役はドローンであり、甘く見るわけにはいかない。ミュトス自体の能力については、さまざまな評価があると思われる。しかしながら、ミュトスが明らかにしたのは、「攻撃型サイバーAIを作ればもうかる」ということである。よって、アンソロピック以外のAI業者もこぞってミュトス的なAIを開発し、競争が激化し、同時にその性能も飛躍的に向上するだろう。中には、ブラックマーケットに流れ、攻撃側に悪用されることも時間の問題かもしれない。そうした意味で、ミュトスは攻撃型サイバーAIのパンドラの箱を開けてしまったと言える。米国の金融テクノロジーのイベントであるマネー20/20、フィノベート、フィンテックミートアップなどでも、AIとサイバーセキュリティーの話題はこれまでもあったが、今後はさらに重視されるテーマになっていくものと思われる。

今、金融機関等のサイバーセキュリティーの現場で実際に何が起きているか、というと、膨大なパッチワークである。ベライゾン社の今年のデータ侵害調査レポートによると、攻撃手口としては、脆弱性攻撃が31%とこれまでトップだったクルデンシャル盗用（なりすまし、13%）やフィッシング（16%）を上回った。ただし、ここでいう脆弱性攻撃は、

ミュトスのような攻撃型サイバーＡＩによる未知の脆弱性発見・攻撃という現在恐れられているパターンではなく、主に企業が既知の脆弱性を適切にパッチしていなかったことによるものとなっている。米国では、既知のソフトウエア脆弱性は連邦政府のCISA KEVというデータベースに掲載・公開されるが、当該データベースに掲載されているのに、企業等がパッチ対応していないため攻撃されている、というのが実情である。つまり、過去1～2年に発見された既知脆弱性が現実には攻撃の中心であり、攻撃型サイバーＡＩが引き起こすような未知の脆弱性ではない。このように、既知の脆弱性への対応でもアップアップなのに、さらに攻撃型サイバーＡＩが脆弱性を大量に見つけてくることになる。これに現場が現実的に対応できるのか？が課題である。ソフトウエアの脆弱性が発見され、重要なものであればパッチを当てる必要があるが、実際には安全な環境でテストして、大丈夫だ、となってから本番環境に適用する。つまり時間がかかる。いまですら、そのボトルネックに膨大な数のパッチが順番待ちしているところに、さらに攻撃型サイバーＡＩが脆弱性を見つけてくるので、その順番待ちの列がさらに長くなる。つまり攻撃型サイバーＡＩの課題は新しい課題、というよりは、すでにある課題をより深刻にする、という影響をサイバーセキュリティーの現場には与えている。また、攻撃型サイバーＡＩを使えば使うほど企業・金融機関にとってはトークンコストがかかることになる。つまり、どこまでサイバーセキュリティーにカネを使うべきか、という古くて新しい疑問も湧き上がる。

（2）対策

筆者が欧米の主要金融機関のサイバーセキュリティー担当者に伺ったところ、現実的に金融機関等ができる対策は以下の通りである。

①情報の分類を厳密にする

通常、金融機関はトップシークレット、極秘、社内限り、公開などといくつかの段階に情報を分類している。まずは、何が何でも守らなければならない情報資産を定義する必要がある。金融機関では、もっとも重要な資産を「クラウン・ジュエル（王冠の宝石）」と表現することがあるが、その金融機関や企業にとって、王冠の宝石は何か、を明確にする必要がある。そして、脆弱性にさらされているのが王冠の宝石なのであれば、ボトルネックの行列に一番先に割り込ませて、早急にパッチ処理をする必要がある。

ただし、言うはやすし、行うは難しである。情報を分類するといっても、金融機関等の多くの情報はＰＤＦのような非構造化データである。その中から、ＡＩ等を使って重要な情報を探し出すことになるが、そのＡＩをどのように学習させるのか、本当に正確なのか、漏れはないのか、といった課題は常に発生する。

また、王冠の宝石が多過ぎれば、それを守る手間やコストも膨大となる。そのため、ミニマリゼーション、つまりできるだけ重要な情報を持たないことが必要となる。持っていない情報は流出しないのである。データの時代に、情報を持たないことは反対のことをしているようにも感じてしまうが、現実的にその情報を持つことが本当に必要なのか、考える必要がある。例えば、顧客に生年月日を何気なく聞いている場合、それが本当に必要なのかどうかを再考する必要がある。もし、顧客が18歳以上であることを確認できればよいだけであれば、確認した段階で生年月日の情報を破棄してもいいかもしれない。つまり、アウトかセーフかだけを記録すれば済むはずである。どうしても生データを保有する必要があれば、その保有年限を厳密に管理する。さらに、用途によっては、生年月日ではなく「30代半ば」といった情報に置き換える。

②バイキンは入ってくることを前提にする

サイバーセキュリティー上、米国には2種類の銀行があるといわれる。すでに攻撃者に侵入されている銀行と、すでに攻撃者に侵入されているが、それに気付いていない銀行である。つまり、いずれにしても攻撃者はすでに銀行に侵入していることを前提に対策を考える必要がある。筆者は２０２２年4月に米国から日本に出張したが、成田空港で唾液を採られる検査があり、2時間も待たされた。つまり、当時の日本は水際対策として「バイキン（コロナ）は入ってくるな」というスタンスであった。しかしながら、そのわずか4カ月後には、日本は世界で一番コロナ

感染者が多い国になっていた。つまり、いくら水際対策をしてもバイキンは入ってくるのである。よって、現実的には、バイキンが入ってきても大丈夫なようにワクチンを接種するとか、健康になる、といった本質的な対策が必要になる。サイバーセキュリティーでも同様に、攻撃型サイバーＡＩ後の世界では侵入を１００％阻止することはできない。よって、入っていた侵入者を、こちらもＡＩなどを利用して迅速に発見する必要がある。そして、もし侵入者がサーバーＡに侵入したのであれば、そこからサーバーＢとかＣに移動できないように、サーバーＡを隔離する必要がある。一方、サーバーＡを隔離したからといって、業務をストップさせるわけにはいかない。このため、企業・金融機関のシステム全体の依存関係などをリアルタイムに把握し、侵入されたサーバーを隔離しても事業が継続できるように準備しておく必要がある。フィノベートやフィンテックミートアップなど最近のフィンテック企業のイベントでは、金融機関のシステム全体をスキャンして状態を把握するような仕組みが人気があるが、その背景にはこうしたこともあるかもしれない。ただし、机上の空論で隔離したとしても、実際にサーバーＡを隔離できなければ意味がない。このため、実際の訓練が必要である。例えば、レッドチーム（金融機関等に雇われたハッカー）を利用して攻撃させ、侵入されたらその部分を早急に発見して隔離する、といったリアリスティックな訓練が必要となる。

（3）当局の動き

規制当局も動き出している。欧州中央銀行（ＥＣＢ）は、欧州の金融機関に対して、攻撃型サイバーＡＩの攻撃に対してどのように対応するかについての計画を10月までに提出するよう求めている。ＥＣＢは金融機関に対し、インターネットに接続されたシステムの保護を最優先し、サードパーティー製ソフトウエアやオープンソースを含む外部にさらされているＩＴ資産の保護に努めるとともに、脆弱性の修正を迅速に行い、監視体制を強化すること、老朽化した技術の近代化、サイバーセキュリティー管理の改善、および危機管理、復旧、情報共有の態勢強化を求めている。

つまり、金融機関に対し、パッチ適用を迅速化し、インターネットに面した攻撃対象領域を縮小し、サポート終了となった技術を更新し、サイバーセキュリティーに関する意思決定を取締役会レベルに引き上げるよう求めていることになる。具体的には、サードパーティー製ソフトウエアやオープンソース、クラウド環境、外部ベンダーへの接続などを含め、インターネットに接続されているすべてのシステムと外部への依存関係を洗い出し、銀行にとって不要なものを廃止または隔離することになる。各計画では、ＡＩを活用した攻撃に対抗するために銀行が講じる具体的な措置を明記し、その実施責任者を指名し、作業に必要な資金と人員を確保し、完了期限を設定しなければならない。もちろん、米銀など欧州以外の金融機関であっても、欧州でビジネスをしている場合はこの対象となる。もっとも、主要米銀はすでに量子コンピューター対応を進めているため、外部のインターネットに接続している部分を特定したり、不要な接続を廃止したりすることはすでに行動を開始しているように思われ、攻撃型サイバーＡＩ対策と量子コンピューター対応は重複も多いと思われる。また、ＥＣＢはレガシー、サポート対象外、またはサポート終了となったシステムを置き換え、老朽化したＩＴシステムをモダナイズすることも必要としている。いわゆる陳腐化管理であるが、この分野も先進的な銀行は実施しているが、そうではない銀行との差が大きい分野であるように思われる。さらに、ＥＣＢは、ＡＩを活用した脅威の問題を経営レベルの議題にアップグレードするよう求めている。攻撃型サイバーＡＩ対応の責任は金融機関の経営陣にあることが明確になり、ＩＴセキュリティー投資、人員配置、リスク許容度などの見直しが必要になるかもしれない。

これとは別に、欧州システミックリスク委員会（ＥＳＲＢ）は、大規模なサイバー混乱が金融機関への信頼を損ない、セキュリティーが脆弱と見なされる企業や国に対する取り付け騒ぎさえ引き起こす可能性があると指摘した。短期間に大量の重要な脆弱性が発見されると、金融機関は「未パッチの重大リスクを残すか」「テストを簡略化して運用障害リスクを受容するか」の二択に追い込ま

れ、いずれもオペレーショナル・リスクを大きく押し上げると懸念している。

ＥＳＲＢは、金融セクター全体で利用されている共通の技術プロバイダーや共有ソフトウエアを通じて、サイバー攻撃の影響が急速に拡大する恐れがあると指摘している。また、システミックに重要な決済・決済インフラなどがＡＩによる脆弱性にさらされ得ることを前提に、サイバーセキュリティーフレームワークを再点検・更新することを推奨している。そして、取締役会レベルでＡＩによるサイバーリスクへのコミットメント、ガバナンス、責任枠組みを明確化し、迅速な対応計画と投資を用意することを求めている。金融機関の対策としては、①パッチ・脆弱性対応の速度と網羅性を底上げする②ＡＩ前提のサイバー・レジリエンスを経営レベルで再設計する③共通インフラ・サードパーティー依存を見直し、セクター横断で情報共有と対応する―ことが必要となる。

つまり、欧州当局のラインに沿うなら、金融機関が実務としてやるべきことは、外部公開システム（インターネットに接続されたチャネル、アプリケーションプログラミングインターフェース〈ＡＰＩ〉、外向きポータル等）の防御を最優先し、サードパーティーソフトウエアを含む外部にさらされた技術資産を特定・保護する方針の策定が必要となる。また、特に重要な脆弱性におけるパッチ適用のスピードアップ、監視（ログ、異常検知など）の強化が必要となる。そして、老朽インフラの近代化として、旧式の基本ソフト（ＯＳ）、ミドルウエア、ネットワーク機器など、技術的負債となっている要素の刷新を計画することになる。また、サイバー管理・危機管理・復旧・情報共有の強化、つまり基本的なサイバーセキュリティー対策（パスワード管理、権限管理、バックアップ、ネットワーク分割など）の徹底、危機管理・復旧、業界・当局との情報共有メカニズムの強化が必要となる。

米国では、トランプ政権はゴールド・イーグルと称するサイバーセキュリティー情報共有制度の運用を開始したと発表した。これは6月のＡＩに関する大統領令に基づくものである。ゴールド・イーグルは、最先端のＡＩ技術を活用して連邦政府および民間部門に、優先順位付けされた実用的な脅威情報および是正措置情報を提供する仕組みである。金融機関や企業等がこのゴールド・イーグルに参加するかどうかは任意であるが、例えば銀行が自社開発したソフトウエアをゴールド・イーグルに提供し、攻撃型サイバーＡＩで脆弱性を調査してもらい、その情報は参加するほかの金融機関や企業に共有される、というイメージである。

一方、米国の監督当局は金融機関に対して一律に攻撃型サイバーＡＩ対策の要請は行っていない。もともと、米国の銀行監督方針は箸の上げ下ろしまで指図するようなマイクロマネジメントではなく、法令の範囲内で金融機関の好きなようにやらせ、不備があれば厳しく懲罰する、というスタイルであり、今回も同様のようである。ただし、実際の現場では米国の金融機関でも、担当の検査官から、攻撃型サイバーＡＩ等の対策をどのようにしているのか、質問の嵐のようである。

（4）おわりに

トランプ政権は一時アンソロピック社のミュトス5やファブル5などのＡＩを輸出禁止とした。これは「脱獄リスク」、つまりガードレールを外して悪用できる可能性が指摘されたためであり、その後同社が修正に応じたので制約は解除されたが、政府がＡＩモデルをより積極的に管理しようとし始めている動きとも言える。トランプ政権は、中国との競争もあり、ＡＩについては、できるだけ規制をせずに民間企業に自由にさせる方針であったが、ＡＩが既存ソフトウエアのセキュリティーを脅かす可能性が出てきたため、以前ほどもろ手を上げて推進、というわけにもいかなくなっている。もともと、ＡＩには映画「ターミネーター」のスカイネットのような不気味さがあったが、今回の攻撃型サイバーＡＩ騒動は、ＡＩのダークサイドについて明らかにしたという意味でも、パンドラの箱を開けてしまったような状況となっている。もちろん、これはよく分からないから不安なのであり、企業・金融機関などはまずは自社・自行のＩＴシステムがどうなっているかを理解し、それがどのように外部と接続されているか、どのベンダーに依存しているのか、などを体系的に把握することが不安解消への第一歩となる。