平時からインシデント時の初動対応やシステム復旧の机上訓練を

最近のサイバー攻撃の動向を踏まえて対応すべき五つの観点

金融庁総合政策局リスク分析総括課サイバーセキュリティ対策企画調整室
課長補佐　鈴木　隆太郎

金融庁では 2016 年度から、金融機関等のインシデント（事故）対応能力の向上を図ることを目的とした「金融業界横断的なサイバーセキュリティ演習（Delta Wall）」を開催している。通算6回目となる 21 年 10 月には、過去最多となる 150 社の金融機関等が参加した。本稿では、最近のサイバー攻撃の動向を踏まえ、演習シナリオを策定する際に重視している点や、インシデントの発生を想定して金融機関等が考慮すべき点について述べたい。

「複合的な」攻撃に対処できているか

近年のサイバー攻撃の特徴としては、利用者を欺く手口の巧妙化や、さまざまな手法を組み合わせた攻撃の複雑化などが挙げられる。また、サイバー攻撃が大規模な組織により行われ、その被害や社会的影響は拡大の一途をたどっている。最近のサイバー攻撃の手法に着目すると、例えば図表のような事例が有名である。

〔図表〕　最近のサイバー攻撃手法の事例

企業の内部ネットワークに侵入し、システムをランサムウエアに感染させて機密情報を含むデータを窃取するとともに、データを暗号化した上、暗号化したデータの復号と引き換えに金銭を要求する。金銭を支払わなければデータは復元できないと脅迫し、支払いがない場合にはデータを暴露すると脅す、いわゆる「二重の脅迫」を行う事例（注1）
ＩＴベンダーによるソフトウエアアップデートの仕組みを攻撃し、アップデートモジュールにバックドアを仕込むことで、企業の内部ネットワークに侵入した事例（いわゆるサプライチェーン攻撃、注2）
ランサムウエアとサプライチェーン攻撃を組み合わせ、多数の企業に身代金を要求するような事例（注3）

（注）1．「サイバーセキュリティ戦略」（21年９月28日閣議決定）９ページ。
2．「サイバーセキュリティ政策会議」報告書「実空間とサイバー空間とが融合したデジタル社会の安全・安心の確保」（21年12月17日）13ページに、米国の大手ＩＴインフラ管理ソフトウエア会社がサイバー攻撃を受け、米国の多数の政府機関を始めとする世界中の組織に影響が生じた事例が紹介されている。
3．米国のソフトウエア会社のリモート監視・管理サービスの脆弱性を利用したサプライチェーンランサムウエア攻撃について、ＣＩＳＡおよびＦＢＩが共同でガイダンスを公表している。
（出所）　筆者作成

国民生活および社会経済活動の基盤の一端を担い、顧客資産を扱う金融機関においては、巧妙化・複雑化したサイバー攻撃に対する堅牢な防御能力を備えておくことに加えて、サイバー攻撃事案が発生した際の高度なインシデント対応能力が求められる。このインシデント対応能力には、インシデントの原因調査と迅速な対処、攻撃者の狙いの分析と攻撃活動の阻止、システムの迅速な復旧などの技術的な対応が含まれる。さらに、代替手段による暫定的な業務継続、適切な顧客対応、効果的な対外公表などの経営的・組織的な対応能力も求められる。

こうした近年の状況に鑑み、当演習では不正アクセスやランサムウエア攻撃、DDoS攻撃[1]といった単一の攻撃に対する画一的な対応にとどまらず、複合的なサイバー攻撃事案に対して被害を最小化し、システムを早期に復旧させ、業務を継続できるかを確認している。そのため各業態の業務やシステムの特性も考慮しながら、業態ごとに演習シナリオを工夫して策定している。

また、単に特定の対応の結果を確認するだけにとどまらず、「事前に規程類が整備されていたか」「関係部門と意見調整ができたか」「経営層に的確に報告し、対応について承認が得られたか」などの観点をシナリオに織り込み、対応の過程を確認するための工夫も加えている。

五つの観点でインシデント対応を

次に、金融機関等が演習に取り組む上で、インシデント対応の主要な要素である五つの観点から考慮すべき点について述べる。なお、本項で記載されていない事項についても、金融情報システムセンター「金融機関等におけるコンティンジェンシープラン策定のための手引書（第3版、第3版追補、第3版追補2、第3版追補3）」等を参考に、自社のシステムや業務に合わせた検討を行うことが望ましい。

①情報共有・情報連携

標的型攻撃メールの受信時などインシデントの初期段階において、必要な報告がCSIRT（セキュリティー事故の対応チーム）およびCISO（最高情報セキュリティー責任者）等のセキュリティー責任者に対して行われるように、平時から不審メール受信時の報告手順等を整備し、社内に周知しておく必要がある。また、受信した標的型攻撃メールの特徴を周知・共有することで全社員の注意喚起を図り、被害を最小限にとどめることが求められる。

経営層への報告が、インシデントの初期段階から遅行してシステム障害や情報漏洩の発生後となる場合には、全社的な対応が手遅れになる恐れがある。社内端末のマルウエア感染や、外部との不正な通信が検知されるなど、サイバー攻撃が疑われる状況が発生した時点で、遅滞なくCISO等のセキュリティー責任者に報告すること

[1] サイバー攻撃手法の一つ。攻撃対象となるウェブサーバーなどに対し、複数のコンピューターから大量のパケットを送信することで、正常なサービス提供を妨害する。

が求められる。インシデントの初期段階で躊躇せず責任者に報告するように、報告基準を明確化し、マニュアル化しておくことが望ましい。

金融庁や財務局等の関係省庁、CEPTOAR[2]等の関係機関への報告については、インシデントの初期段階で第一報を上げることが適切であるが、その後の進展や状況変化に応じて、新たに判明した事実や被害状況、業務への影響、顧客対応の状況などを適時に報告することが求められる。

②初動対応・業務継続

ネットワークへの不正侵入やシステムのマルウエア感染を検知した際に、被害の拡大防止に向けたネットワークの遮断やシステムの切り離しを迅速に行うことが求められる。対応方法を誤ると被害拡大を阻止できず、誤った遮断・停止対応が無用の業務停滞をもたらす懸念もある。自社のシステムが攻撃を受けた際に備えて、対応フローを整備しておくことが有効である。

社内の重要なシステムがサイバー攻撃の被害を受けた際には、複数の部門や業務が影響を受ける場合がある。一時的な業務継続のためのリソースが限られる場合において、優先すべき業務および業務継続の手段について、具体的に整理しておくことが望ましい。

事後対応のためのマニュアルを準備

③インシデント調査

実際にインシデントが発生した際には、その原因や侵入方法、被害状況について、外部委託先とも相談しつつ、最終的には自社で調査方針を決定する必要がある。サーバーやネットワーク機器のログの種類や取得期間、分析方法について、外部委託先任せにせず、自社で把握しておくことが求められる。

マルウエア感染や不正侵入によりシステムが攻撃を受けた際には、他のシステムに被害が及んでいないか、機密情報が窃取されていないかを含め、被害範囲を特定することが求められる。攻撃者の侵入方法や侵入経路に関する仮説を設定し、ログに基づいて検証することが有効である。

④顧客対応や対外公表

顧客アカウントへの不正アクセスや、口座からの不正送金が疑われる際には、迅速な利用停止措置や、送金先金融機関に対する出金停止依頼等が求められる。事前にこれらの措置の判断基準を文書化しておくことが求められる。

インシデントの発生時には、顧客を適切に誘導し、社会的な信用の低下を最小限に防ぐために、効果的な対外公表を行うことが求められる。その一方で、公表に便乗

---

[2] 重要インフラ事業者等の情報共有・分析機能および当該機能を担う組織（Capability for Engineering of Protection, Technical Operation, Analysis and Response）。22 年2月現在、各重要インフラ分野の業界団体等が事務局となり、全 13 分野で計 18 のCEPTOARが活動している。

した二次被害の発生や、公表を契機とした信用の失墜、不安の拡大も想定される。平時からインシデントの内容に応じた公表要否の判断基準や公表内容について、文書化しておくことが望ましい。

対外公表後には顧客からの問い合わせが殺到することも想定される。専用の問い合わせ窓口を設置することやコンタクトセンターの増員、対応マニュアルの周知・徹底を図ることが望ましい。

⑤システム復旧

システム復旧においては、当該システムのRTO（目標復旧時間）やRPO（目標復旧時点）を意識した具体的な復旧計画を策定する必要がある。これらは、対象業務の許容停止時間やデータのバックアップにおける取得・保管状況と整合している必要がある。有事の対応を外部委託先に一任せず、許容停止時間内の復旧が可能であるか、バックアップが適切な頻度と方法で取得・保管されているか、復旧方法が具体的に文書化されているか等について詳細に把握しておくことが求められる。

システムの再稼働に向けて、再開判断プロセスおよび再開判断基準を定義し、承認権者を明確にしておく必要がある。インシデントの原因となったマルウエアの駆除結果や脆弱性対処の確認方法に加え、システムおよびデータが正しく復旧もしくは復元されたか、システム障害が再発する懸念がないかについて、事前にテスト項目を整備しておくことが求められる。

このほか、外資系金融機関等で、CSIRT機能を海外本社が担う場合においては、日本国内で発生したインシデントへの対応が迅速に行われるかについて、本社との共同訓練を実施するなど、情報連携体制の確認をしておくことが望ましい。

テレワーク増加による復旧作業遅延を懸念

テレワークが増加したことにより、有事の際におけるシステム停止やネットワーク遮断等の初動対応、インシデントの原因の調査およびシステム復旧作業が遅延することが懸念される。初動対応やシステム復旧が所要時間内に行われるかについて、平時から机上訓練などでシミュレーションしておくことが重要である。

その一方で、テレワークの増加を契機として、社内の情報共有の仕組みが整備され、各部門のインシデント対応状況がグループウエア上に一元化されることにより、情報連携の円滑化が進むことも期待される。一般的に、平時から以下のような取り組みを行っている金融機関等については、インシデント発生時の対応能力も高く、演習結果も優れている。

・ 経営層の意識が高く、平時からサイバーセキュリティーに関する自社の対応方針や対応状況を把握している
・ 情報資産管理台帳やネットワーク構成図を適時に更新し、自社システムを正しく把握している

・ セキュリティー教育や人材育成に投資している
・ 業界内における情報共有や情報交換に努めている

不本意な演習結果に終わった金融機関等においては、本件を機に対応できなかった項目の再確認を行うとともに、自社の業務・サービスに応じたセキュリティー全体の在り方を見直し、改善に努めていただくことを期待したい。

金融機関役職員に望む三つの視点

金融機関等の役職員においては、インシデント対応能力をさらに高めるため、以下の三つの視点を持っていただくことが有効である。

一つ目は、経営者の視点である。経営層がサイバーセキュリティーを経営課題として捉えるのはもちろんのこと、IT部門においては、システム障害が事業や顧客にどのような影響をもたらすのか、営業部門においては、顧客の情報や資産がどのように保護されているのか、それぞれ俯瞰的な視点を持っていただくことが有効である。

二つ目は、攻撃者の視点だ。仮に自分が攻撃者なら、自社のシステムをどのように攻撃するか、イメージトレーニングしておくことが重要である。そのためには、最新の攻撃手法に関する情報を収集するとともに、自社のシステムをしっかりと把握しておくことが前提となる。また、攻撃事例の多様化や社内の人事異動も考慮し、定期的な演習を実施することや、各種セキュリティーの技術者認定の取得、セキュリティートレーニングの受講などで専門人材の育成に努めることも有効である。

最後に、顧客の視点である。インシデント発生時にシステムの復旧対応に追われ、顧客への対応が後手に回ってはならない。顧客の資産を預かり、円滑な金融機能を提供するサービスの担い手として、インシデントが発生したときの被害をいかに最小限に抑えるか、顧客目線で対応を進めることが重要である。

（本稿において、意見にわたる部分は筆者の個人的見解であり、所属する組織の見解を示すものではない。）

すずき りゅうたろう
94 年慶應義塾大学環境情報学部卒業後、システム開発業務やITコンサルティング業務に従事。09 年金融庁証券取引等監視委員会事務局、20 年7月から現職。CISSP、日本証券アナリスト協会認定アナリスト（CMA）。