金融分野におけるサイバーセキュリティに関するガイドラインの解説

昨今のサイバー攻撃の増加などにより、サイバーセキュリティリスクへの対応の重要度は日増しに高まってきている。サイバーセキュリティ対策は経営層やリスク管理部門だけの課題ではなく、営業店職員までを含めて全社的に実行していくことが肝要である。本稿では、サイバー攻撃の現状と傾向、具体的な対策、そして従業員一人ひとりが日常業務で意識すべきポイントについて詳述する。

株式会社クニエ　福澤　尚人

1 サイバー攻撃の現状と傾向

(1) ランサムウェア攻撃、フィッシング攻撃の増加が懸念

金融庁では毎年「金融機関のシステム障害に関する分析レポート」（以下、システム障害分析レポート）を作成し、その原因分析や事例を共有している。加えて、近年のサイバー攻撃の被害状況等を踏まえて、その対策の重要性からサイバーセキュリティに特化した新たなガイドラインを作成している。

金融庁のシステム障害分析レポートによれば、サイバー攻撃の手法は高度化・巧妙化している。特に、金融機関を狙った攻撃は、その手口が年々複雑化し、被害の規模も拡大している。営業店職員にも関係するところでは、ランサムウェア攻撃やフィッシング攻撃が挙げられる。これらの攻撃による被害は、大規模な顧客情報の漏洩や業務の停止を引き起こす重大なリスクとなっている。

①ランサムウェアは3年で約4・5倍に

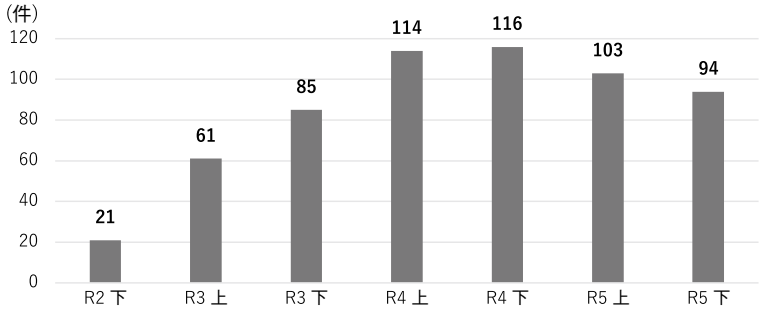
ランサムウェア攻撃は、悪意のあるソフトウェアがシステム内に侵入し、データを暗号化することから始まる。データが暗号化された状態では業務を継続することができず、業務復旧のためにはデータの復号化が必要であり、この対応に身代金を要求する。近年では新しいランサムウェア型の攻撃であるノーウェアランサム攻撃も発生している。

この攻撃では、データの暗号化を行うのではなく、顧客情報等のデータを窃取し、データを公開してほしくなければ対価を払うことを要求する。また、このような攻撃は、全方位にばら撒く一般的なスパムメールとは異なり、ターゲットの組織に関する詳細な情報を収集し、それに基づいてカスタマイズされたメールを

送信することで成功率を高めているケースもある。

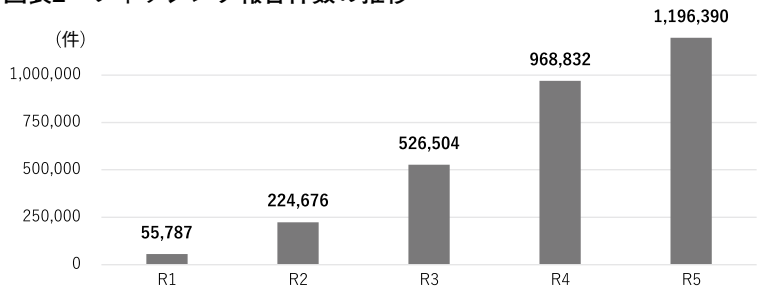
警察庁の「令和５年におけるサイバー空間をめぐる脅威の情勢等について（２０２４年３月14日公表）」によると、ランサムウェア攻撃による被害報告件数は、２０２０年下期では21件であったが、２０２３年下期には94件と約４・５倍に増加している（図表１参照）。この増加傾向にあるランサムウェア攻撃による被害の復旧に要した時間は１週間以上が52％であり、業務に甚大な影響を与える攻撃だと言える。

図表１　企業・団体等におけるランサムウェア被害の報告件数の推移



出典：警察庁　令和５年におけるサイバー空間をめぐる脅威の情勢等について（2024年3月14日）

図表2　フィッシング報告件数の推移



出典：警察庁　令和５年におけるサイバー空間をめぐる脅威の情勢等について（2024年3月14日）

②フィッシング攻撃は３年で約６倍に

フィッシング攻撃は、信頼できる組織を装った電子メールで偽のウェブサイトに誘導し、個人情報や認証情報を盗む手口である。この手法は、銀行やクレジットカード会社などの名前を騙ってメールを送信し、受信者に偽のウェブサイトにアクセスさせて情報を入力させるというものである。フィッシング攻撃は、特に電子メールを通じて行われることが多く、その報告件数は２０２０年では約22万件であったが、２０２３年には約１１９万件と６倍近くに増加している（図表２参照）。

近年の被害事例として、２０２３年７月国内の港の統一ターミナルシステムがランサムウェア攻撃を受け、約２日半の業務停止に陥った事件が挙げられる。攻撃者はシステムの脆弱性を突いて侵入し、データを暗号化することで業務を停止させた。

また、２０２４年１月には国内医療製品メーカーがフィッシング攻撃を受け、２億円相当の被害が発生している。この攻撃では、攻撃者が取引先を騙ったメールで支払先の変更を依頼し、攻撃者の銀行口座に支払いをさせた。

⑵　３メガでも脆弱性を突いた攻撃が

ランサムウェア攻撃は金融業界でも発生しており、様々な金融機関から帳票作成や発送業務を委託されている企業で個人情報の漏洩が発生している。また、その他脆弱性を突いた攻撃も三菱ＵＦＪ銀行やみずほ銀行といった３メガでも発生している。このような事例は、サイバー攻撃の深刻な影響を示しており、事前

の対策がいかに重要かを物語っている（図表3参照）。

サイバー攻撃の手法は日々進化し続けているが、システム的な技術進化だけでなく人の心理的な隙を突くような技術であるソーシャルエンジニアリングなどにも注意が必要だ。

また、近年増加している標準型攻撃は、企業や組織だけでなく、従業員個人を綿密に調査し、対象に有効的な手法で攻撃を行う。そのため、組織としての対策だけでなく従業員個人が、対岸の火事の意識ではなく、1分後には自分も被害者になるかもしれないという当事者意識を持つことが重要となる。

一人ひとりがサイバーセキュリティ対策を意識し、実施していくことが自分だけでなく、組織や顧客を守ることに繋がっていく。

図表3　金融機関におけるサイバー攻撃被害事例

発生年月	被害企業	概要
2016年	新生銀行グループ会社	従業員のパソコンがマルウェア感染し、38件の債務者情報等が漏洩
2019年	みずほ銀行	J-Coin Payの加盟店管理に関わるテスト用システムに不正アクセスがあり、1万件以上の法人代表者や窓口担当者の個人情報が漏洩
2019年	三菱UFJ銀行	ローカルキャッシュマネジメントサービスに不正アクセスが発生し、13社の口座情報と振込先等取引先明細、およびそこに含まれる取引先名・従業員名等の第三者情報1305件が漏洩
2020年	ゆうちょ銀行	認証の脆弱性を突き、被害者の銀行口座と攻撃者の決済サービスを紐づけたうえで不正送金される被害が210件発生
2024年	金融機関の業務委託先	様々な金融機関から帳票作成や発送業務を委託されている企業がランサムウェア攻撃の被害で個人情報が漏洩

出所：各金融機関のウェブサイトよりクニエ作成

2 金融庁サイバーセキュリティガイドラインの要点

前章で記述した通り、サイバー攻撃は増加しており、その対策の重要性は日に日に増している。このような時勢の中で、2024年6月28日に金融庁は新たに「金融分野におけるサイバーセキュリティに関するガイドライン」（案）（以下、ガイドライン）を公表した。従来は、金融庁の監督指針および事務ガイドラインの一部としてサイバーセキュリティに関する言及がなされていたが、新たにガイドラインが作成されたことは、金融庁が金融機関等のサイバーセキュリティ対策の重要性を深刻に捉えていることを示している。

以降では、当ガイドラインの重要なポイントおよびそれが企業やITセキュリティ担当部署ではなく個人単位での対策にどのように繋がっていくのかを説明する。

(1) サイバーセキュリティ管理態勢の構築

ガイドラインには、経営陣が主体となって全社的にサイバーセキュリティ管理態勢を構築する必要があるといった記載がある。この管理態勢の構築には、基本方針の策定、規程類の策定、経営資源の確保、人材の育成、リスク管理部門による牽制、内部監査が挙げられる。

これらの対策は経営レベルの目線ではあるものの、従業員一人ひとりの目線で考えることも重要である。従業員一人ひとりが策定された基本方針を理解し、遵守することが求められる。また、サイバーセキュリティ対策に限らず、情報管理規程などの様々な管理規程を遵守することも必要

である。

(2) 情報資産管理

管理態勢の構築という全体の話だけではなく、個人にも関わりがあるデータの領域についてもサイバー攻撃への対策が必要である。

データには取得・使用・保管・廃棄といったライフサイクルが存在し、その全体を通じて管理する必要がある。また、データは機密性・完全性・可用性の観点で重要度を分類し、その重要度に応じて適切な保護対策を講じることが求められる。

機密性とは、許可された人だけがアクセス可能であることを確保することである。完全性とは、データへの書き込みや消去等の操作が制限され、データが正確で改ざんされていないことを確保することである。

可用性とは、必要な時にデータにアクセスできる状態を確保することである。適切なタイミングで最適な管理を行うことでサイバー攻撃による被害を極小化や局所化することに効果的である。

顧客情報を例にとると、上場企業の公開されているデータは機密性が低いが、非上場企業である取引先から提出された決算書等の非公開データは機密性が高いため、厳格な取り扱いが求められる。

また、M&Aの情報は機密性が極めて高く、一層厳格な取り扱いが必要である。このように営業店の一担当者が取り扱う情報でも機密性は様々である。

機密性が極めて高い情報を個人のパソコンのローカルフォルダに保存するなど、規程類に定められた適切な管理を実施していない場合、規程上起きるはずのない被害がサイバー攻撃によって発生してしまうことになる。

そのため、従業員一人ひとりがルールを遵守することが必要である。これにより、自身がサイバー攻撃にあった場合でも被害を最小限に食い止めることが可能となる。

(3) ハードウェア・ソフトウェア等の脆弱性管理

次に、ITセキュリティ担当部署が社内外で収集したハードウェアおよびソフトウェアに関する脆弱性情報に基づき、パッチ適用等の適切な対応を実施することが求められる。○月△日の深夜に「セキュリティパッチの更新があるため××してください」といった社内連絡を受けたことがあるかもしれないが、これも脆弱性管理対応の一環である。

企業で使用するパソコンには様々なソフトウェアがインストールされているが、それらを提供している各社は、世界のどこかでサイバー攻撃を受けたことで脆弱性に気付き、同様の被害が別の企業で発生しないよう全世界の顧客に脆弱性対応情報(修正パッチ等)を日々配布している。

社内連絡に従って適切な対応を行わないことは、世界のどこかでサイバー攻撃にあった被害者と同じ状態を維持することになる。そのため、ITセキュリティ担当部署の指示のもと、パソコンやスマートフォン等のツールは最新のセキュリティ状態を保つことが必要である。

(4) 継続的な改善活動

日々進化しているサイバー攻撃に対策するためには、社内外での最新の脅威情報等を収集し、その発生可能性や影響を評価し、対応を適宜適切なものに変化させる改善活動を継続的に実施することが必要である。情報収集や改善活動自体は社内のITセキュリティ担当部署が担当することが多いが、その改善活動を踏

まえて変わった社内のルールやツールを正しく運用することが従業員一人ひとりに求められている。

日々お客様と接していると、社内ルールの変更は読むのも煩わしいことであり、ツールの変更は慣れた手法を変える手間のかかる作業と捉えてしまいがちである。しかしながら、サイバーセキュリティ対策は一度決めたことを続ければ良いということではなく、対策も日々変化する必要がある。このことを意識し、改善活動の結果に対しても前向きに取り組む姿勢が大切である。

サイバー攻撃に前向きに取り組めていない際の一例として、社内で使用しているソフトウェアが使用しづらいため、プライベートでも利用しているソフトウェアを会社用のパソコンやスマートフォンにインストールしてしまうことが挙げられる。

企業では様々なセキュリティソフトウェアでパソコンやスマートフォンを守っているため、それらが及ばないものを勝手にインストールすることはサイバー攻撃を受けるリスクを高める行為である。

シャドーＩＴと呼ばれるこれらの行為は絶対に行わないよう自身が意識するとともに、同僚が行っている場合は即座に止めるよう声掛けする等の企業全体としてのリスク管理意識を持つことができるとなお良い。

⑸　教育・研修

データの取り扱い等、これまでに記載した内容は各社のルールやツールとして様々な形で表れているはずである。

この各社独自のルールを徹底し、ツールを正しい方法で運用するためには、教育・研修が欠かせない。多くの企業ではｅラーニング等の手法を用いて定期的な教育を実施している。

繰り返し記載するが、サイバー攻撃は日々進化しており、対策も日進月歩しているため、従業員一人ひとりが定期的にセキュリティの動向および対策に関する情報をアップデートすることが最も大切である。

ｅラーニングは受け身な手法であるため、内容を全社に浸透させるために各社様々な工夫が必要である。例えば一定時間経たないと教材を次のページに送ることができない、習熟度テストで満点回答になるまで何度もテストを受ける必要がある等の仕組みだ。

これらは受講者のリテラシーの低さから生まれた機能であるが、このような機能がなくとも、サイバーセキュリティ対策の重要性を理解し、真剣に取り組むことが必要である。

3　銀行業界を取り巻く環境とサイバーセキュリティの展望

日本全体の課題である人口減少や高齢化に加え、低金利環境の長期化等によって、銀行業界は厳しい状況にあり、業務の維持のためにはＩＴ・デジタル技術が欠かせない要素となっている。また、ＩＴ・デジタル技術の発展により暗号資産交換業者等の新たな金融プレイヤーが登場し、金融機関でも利用者ニーズの多様化に対応するため、ビジネスモデルの変革が進んでいる。

現在でもＩＴシステムが無ければ業務が停止してしまう環境であるが、今後はその傾向がより一層進むと考えられ、サイバーセキュリティ対策の重要性も一段と増していく。そのような未来が予想される中で、技術の発展はサイバーセキュリティ対策にポジティ

ブな影響を与える。例えば、AIによる膨大なデータ解析により、過去の攻撃者の挙動を学習し、将来の攻撃パターンを予測することが可能となる。

現在でもこのような機能を持ったセキュリティサービスは存在し、今後はより精度が高まっていくと考えられる。この例を見ると安心するかもしれないが、攻撃者もIT・デジタル技術の恩恵を享受するため、結局は攻撃者と対策手法のいたちごっこは続くと考えられる。

4 お客様のために一人ひとりが意識のアップデートを

これまでサイバーセキュリティの現状と傾向、金融庁の新たなサイバーセキュリティガイドラインの内容、金融業界を取り巻く環境と今後の展望について述べてきた。過去を踏まえて未来でも言えることはサイバー攻撃の手法は日々変化し、対策も変化していくということである。

セキュリティは目に見えないものであり、事後的に対策を徹底的に実施したところで一度大規模な被害に遭った際に低下したお客様の信用を回復することは容易ではない。銀行法の第一条には、「この法律は、銀行の業務の公共性にかんがみ、信用を維持し、預金者等の保護を確保するとともに金融の円滑を図るため、銀行の業務の健全かつ適切な運営を期し、もつて国民経済の健全な発展に資することを目的とする。」とある。銀行は公共的なサービスであり、信用が特に重要であることを改めて意識し、サイバーセキュリティに関する意識を一人ひとりがアップデートし続けることが必要である。