特集

組織を揺るがすサイバー攻撃への備え

①「情報セキュリティ10大脅威2026」から読む　サイバー攻撃の最新動向

生成ＡＩの進展などにより脅威は日々変化し、金融機関には経営層から現場まで一体となった備えが求められている。本稿では、「情報セキュリティ10大脅威２０２６」を踏まえ、押さえておきたい基本的な対策の方向性を解説する。

株式会社エス・ピー・ネットワーク
総合研究部　上席研究員
宮本　知久

クレーム・不当要求対応の支援業務、個人情報管理、危機管理体制強化コンサルティング等を経て、現在は、情報漏えいやシステム障害等の企業不祥事の対策本部のコンサルティングや実務支援、従業員研修などを担当。市町村等自治体のコンプライアンス、公務員倫理、リスクマネジメント等の職員研修講師実績多数。

サイバーセキュリティは、今、金融機関の頭を悩ませている分野の1つではないでしょうか。攻撃者たちによる攻撃手口の開発スピードの速さ、どの種類の対策をどの程度の深さで行うかの決定、そして実行と定着の難しさ、ディープフェイク等の新たな脅威、生成ＡＩの登場――。明らかにこれらについての相談は多くなっています。

本稿では、独立行政法人情報処理推進機構（ＩＰＡ）の「情報セキュリティ10大脅威２０２６」を参考に、基本的な対策の方向を紹介します。

1　サイバー攻撃による経営リスク

金融機関に対するサイバー攻撃による経営リスク発生のメカニズムを整理すると、**図表1**のようになります。左側に記した事象が右側の影響・損失につながることから、サイバー攻撃によるリスクを回避、低減させるための方向は、いかに左側に近い事象や影響で食い止められるかが重要といえます。

サイバー攻撃に耐えられる態勢、もしくはサイバー攻撃を受けたとしてもシステム面での発生事象で、かつ軽微な影響で食い止められる態勢を構築することが、向かうべき1つのゴールです。

このうえで、サイバー攻撃のリスク管理の検討にあたり、攻撃の舞台となるサイバー空間の変化について、金融庁が提唱する次の点を考慮して検討する必要があります。

【サイバー空間の変化】

・国家の関与が疑われる組織化・洗練化されたサイバー攻撃や、国際的なハッカー集団等によるランサムウェア攻撃の多発
・デジタライゼーションの進展による金融サービスの担い手の多様化と、キャッシュレス決済などの連携サービスの進展
・クラウドサービスをはじめ

特集　組織を揺るがすサイバー攻撃への備え

②金融業務におけるサイバーセキュリティ関連法令とガイドライン

いま、サイバーリスクは、金融機関の事業継続を左右する経営課題となっている。本稿では、金融業務に携わるうえで押さえておきたい関連法令・ガイドラインの全体像と、実務上重要なサードパーティリスク管理のポイントを解説する。

八雲法律事務所
弁護士　山岡　裕明

カリフォルニア大学バークレー校客員研究員、内閣サイバーセキュリティセンター（NISC）タスクフォース構成員（19-20年、21-22年、25-26年）、「サイバー安全保障分野での対応能力の向上に向けた有識者会議」（24年）。

弁護士　髙間　裕貴

検事（東京・福岡・長崎・さいたま・新潟各地方検察庁（15-24年）、法務省刑事局（18-20年、24年））を経て、2024年現職。税務大学校非常勤講師（商法演習）（25年）。情報処理安全確保支援士。

Ⅰ　はじめに

深刻なサイバー攻撃が後を絶たず、JA系統組織でも被害が複数確認されています。例えば、東北地方のJAが2022年に、同じく東北地方のJAの子会社が2026年に、それぞれランサムウェア攻撃（後述）を受けています。

サイバーリスクが事業継続に関わる程に深刻化していることから、政府の有識者会議においても「サイバーリスクは大きく変容している。ゲームチェンジが起きており、これまでの情報窃取型だけではなく、システムを停止させるタイプの攻撃が増えてきている。重要インフラ事業者を含め民間事業者にとって、サイバーリスクは事業継続を損なうリスクになりつつある。このリスクの深刻度は自然災害と同程度ともいえる」と指摘されています（注1）。

また、2025年に、JA全国団体の委託先がランサムウェア攻撃を受け、個人情報漏えいに至った事例からも明らかなとおり、自社だけではなく委託先を含むサードパーティ経由でのサイバーリスクもあります（**図表1**）。

実際に、独立行政法人情報処理推進機構（IPA）が毎年公表している情報セキュリティ10大脅威「組織」編において、「ランサム攻撃による被害」が2026年の1位（11年連続11回目のランクイン）、「サプライチェーンや委託先を狙った攻撃」が2026年の2位（8年連続8回目のランクイン）となっています。

本稿では、まず金融機関に関係するサイバーセキュリティ関連法令・ガイドラインの全体像を整理し、そのうえで、金融機関からご相談を特に多く受けるテーマであるサードパーティリスク管理を紹介します。

特集 組織を揺るがすサイバー攻撃への備え

③組織における危機管理と経営層の意思決定

サイバー攻撃への備えは、システム部門だけの課題ではなく、経営層と現場が一体となった危機管理が不可欠。本稿では、その本質を整理するとともに、JAに求められる平時からの備えや、有事に組織を止めないための実践的な対応を解説する。

合同会社セルフディフェンスパートナーズ
代表社員　西田 千尋

防衛大学校（女子第3期生）卒業後、航空自衛隊入隊。22年にわたり総務・人事業務を中心に従事。2等空佐で退官後、縄文アソシエイツ株式会社でコンサルタントを務めるかたわら、2024年合同会社セルフディフェンスパートナーズを設立。自衛隊で培った危機管理・マネジメント経験を活かし、リーダーシップや組織づくりに関する講演・研修を多数行っている。

サイバー攻撃は「システム部門の問題」である――。そう認識しているJA系統組織は少なくないのではないでしょうか。しかし、その認識こそが有事に組織をもろくする最大の要因です。攻撃を受けた瞬間から、組織は「全員参加の有事対応」に入らざるを得ません。誰が顧客への説明窓口になるのか、いつ経営層に報告を上げるのか、業務継続をどこまで続けるのか。これらはITの問題ではなく、経営と現場の意思決定の問題です。

本稿では、危機管理の本質を整理したうえで、有事に組織が止まらないために平時から何を準備すべきか、自衛隊での経験と企業支援の実績を基にお伝えします。

1 危機管理とは何か（リスク管理との違い）

まず概念の整理から始めましょう。「リスク管理」と「危機管理」は混同されがちですが、目的は根本的に異なります。

●リスク管理（Risk Management）

予測可能なリスクに、事前の予防・低減・移転・保有で備え、「起きないようにする」活動。セキュリティ強化やバックアップ整備が典型例。

●危機管理（Crisis Management）

重大な事態が発生・切迫した際に、被害を最小化し組織機能を維持したまま「どう切り抜けるか」を経営として判断する活動。

重要なのは、「リスク管理を徹底しても危機は起きる」という事実です。どれだけセキュリティを強化してもサイバー攻撃がゼロになることはなく、だからこそ「起きた後にどう動くか」を平時から設計しておくことが不可欠です。

サイバー攻撃への対応を「システム部門任せ」にできない理由もここにあります。

特別企画

JAグループにおける相続相談態勢の強化について

JAバンクでは、「JAバンク中期戦略（2025～2027年度）」において、「相続相談態勢の強化」を重点施策の1つに位置づけています。本稿では、その背景や足元の課題、今後の対応方針等について整理します。

農林中央金庫　JAバンクリテール実践部　LPS企画グループ

1 なぜ今、「相続相談態勢の強化」なのか

JAバンクの総合的戦略となる「JAバンク中期戦略（2025～2027年度）」のうち、「くらし」の領域においては、ライフプランサポートにおけるつながり強化に向けた3本柱の1つとして「相続相談態勢の強化」を掲げています。

これまでの同戦略においては、この「相続相談」に関する取組みについて、あまり強く表に出てくることはありませんでしたが、国内の人口動態やJAバンク利用者の世代構成等を踏まえ、組合員・利用者の皆様のニーズに応えるべく、改めての注力・強化を図ることとなった経緯があります。

(1) 相続相談を巡る環境変化

これまでのJAグループにおける「相続相談」の取組みについては、土地持ち資産家の組合員の方々の資産管理の重要性が高いことなどから、一部の都市型JAを中心に、この分野を発展させてきました。また、JAグループ全体においても、10年以上前から、「相続相談」およびその先の次世代層との接点構築の重要性は言及されていました。

他方、JAグループ全体としてこの分野の重要性は認識しつつも、具体的な施策の展開にまでは至らず、運動論に始終してきた背景もあります。また、前述のとおり、これまでのJAバンクにおいては、この「相続相談」の分野について今ほど重要な位置づけにはありませんでした。その理由は様々ですが、「次世代の方々もJAで取引をいただく」という観点以上に、「事業量の伸長」「新規基盤の獲得」といった、直接的かつ