金融業界におけるサイバーセキュリティ トレンドレポート **2025**

Librus株式会社
コンサルティングサービス事業部

エグゼクティブサマリー

2024年度は、金融業界におけるサイバーセキュリティの脅威が質的・量的に大幅に高度化した転換点となった。国家系攻撃グループによる標的型攻撃、サプライチェーン経由の大規模インシデント、DDoS攻撃の多発により、金融機関は従来の境界型防御を超えた包括的な対策が求められている。本レポートでは、2024年度の主要インシデント分析から2025年の展望まで、金融業界のサイバーセキュリティ動向を網羅的に解説する。

1. 2024年度の主要インシデント分析

1.1 標的型ソーシャルエンジニアリング攻撃

2024年度最も深刻な事案として、北朝鮮を背景とするサイバー攻撃グループ「TraderTraitor」による標的型ソーシャルエンジニアリング攻撃が挙げられる。同攻撃では、従業員へのなりすましによる内部承認プロセスの突破、正規取引のリクエスト改ざんにより、約482億円相当の暗号資産（ビットコイン）が不正に流出した。

攻撃の特徴

- 高度な人的心理操作による内部システム侵入
- 正規業務プロセスの悪用によるセキュリティ回避
- 多要素認証の設定不備を狙った標的型攻撃
- WindowsSandBoxの悪用による証跡隠滅

1.2 ランサムウェア攻撃とサプライチェーン被害

2024年5月、金融機関や地方公共団体等の委託を受けた情報処理・印刷・発送業者への大規模ランサムウェア攻撃が発生。暗号化に加えて窃取された個人情報がダークウェブ上に公開され、複数の金融機関の顧客情報が流出する事態となった。

また、海外支店のプライベートクラウド環境での不正アクセスから国内外拠点への水平展開が試みられる事案も確認され、グローバルな金融機関における統一的なセキュリティ管理の重要性が浮き彫りになった。

1.3 DDoS攻撃の多発と高度化

2024年12月から2025年1月の年末年始にかけて、金融機関を標的とした大規模DDoS攻撃が相次いで発生。IoTボットネットを利用したUDPフラッド攻撃、HTTPフラッド攻撃など複数の攻撃手法が併用され、インターネットバンキングへのログイン障害や決済サービスの利用困難な状況が発生した。

2024年度サイバーインシデント発生件数：約**1,800**件（金融機関全体）

うちサイバー攻撃由来：**50.3%**（前年度比増加）

2. 新たな脅威とトレンド

2.1 攻撃手法の進化

Living Off The Land戦術

システム内寄生戦術として、侵入後にシステム内の正規管理ツールや機能を悪用して認証情報窃取やシステム情報収集を行う手法が確認された。この戦術により、従来の境界型防御やマルウェア検知が困難となっている。

中国系攻撃グループ「**MirrorFace**」

2019年12月から継続的に行われている中国の関与が疑われる攻撃キャンペーンでは、主に安全保障や先端技術に係る情報窃取を目的とした高度な攻撃が確認された。WindowsSandBoxの悪用により証跡や調査を困難にする新たな手口が公開されている。

2.2 クラウドとサードパーティリスク

デジタル変革の進展に伴い、クラウドサービスの利用拡大と外部委託の増加により、サードパーティ経由の攻撃が顕著に増加。設定ミスや委託先のセキュリティ管理不備を悪用した攻撃が多発している。

3. 対策技術の最新動向

3.1 多要素認証の強化

フィッシング耐性を向上させるため、生体認証やパスキーなどの次世代認証技術の導入が推奨されている。特に、従来のSMS認証やワンタイムパスワードでは対応困難な高度な攻撃に対する有効性が確認されている。

3.2 ゼロトラスト・アーキテクチャ

「内部は安全、外部は危険」という従来の境界型セキュリティモデルから、すべてのアクセスを信頼せず常に監視・検証するゼロトラスト・アーキテクチャへの移行が進んでいる。サプライチェーン全体における認証と資産管理の統合が重要な要素となっている。

3.3 脅威ベースのペネトレーションテスト（**TLPT**）

金融機関のサイバーセキュリティ対策の実効性を検証するため、現実の攻撃手法を再現したTLPTの導入が拡大している。特に大手金融機関、金融市場インフラ事業者において、本番環境での実戦的な検証が行われている。

TLPTの主要な検証項目

- 攻撃の検知・対応能力
- インシデント対応体制の実効性
- 重要業務継続能力
- 経営陣への報告・意思決定プロセス

4. 規制動向とガイドライン

4.1 金融庁ガイドラインの策定

2024年10月、金融庁は「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」を策定し、金融機関に対する包括的なサイバーセキュリティ管理態勢の構築を要請した。本ガイドラインは、経営陣の主体的関与、基本的対策の徹底、侵入を前提とした対応の強化、サードパーティリスク管理を4つの柱としている。

4.2 FISC安全対策基準の改訂

2025年3月、金融情報システムセンター（FISC）は「金融機関等コンピュータシステムの安全対策基準・解説書（第13版）」を公表し、金融庁ガイドラインとの整合性を図った技術的・運用的対策の詳細を提供した。

4.3 暗号資産関連規制の強化

2024年10月の監督指針改正により、暗号資産交換業者も金融庁ガイドラインの適用対象となり、従来の金融機関と同等のサイバーセキュリティ対策が求められることとなった。

5. 国際連携の強化

5.1 G7サイバーセキュリティ作業部会

2024年6月、イタリア議長国の下でG7サイバーセキュリティ作業部会が設立され、日本も積極的に参画している。2025年5月にはカナダでプリンシパル級会合が開催され、「IoT　Security」に関する文書が発表された。

5.2 脅威情報の共有と共同対応

北朝鮮系攻撃グループ「TraderTraitor」に関する米国との共同パブリックアトリビューション、中国系攻撃グループ「APT40」に関する豪州主導の国際アドバイザリーへの参加など、脅威情報の共有と共同対応が活発化している。

5.3 業界横断的な情報共有

金融ISAC（Information Sharing and Analysis Center）を中心とした業界横断的な情報共有体制が強化され、DeltaWall演習には2024年で170社の金融機関が参加（前年比5社増）している。

6. 新技術への対応

6.1 耐量子計算機暗号（**PQC**）

量子コンピュータの発達に伴う暗号化技術の脆弱性に対応するため、金融庁は2024年11月に耐量子計算機暗号への移行を検討する検討会の報告書を公表した。2025年内を目途に移行の方向性を検討することとしている。

6.2 AI利活用のリスク管理

生成AIの業務利用拡大に伴い、2025年2月に政府機関等における生成AIを含む約款型サービスの業務利用に関する注意喚起が行われた。金融機関においても、AI利活用に伴うセキュリティリスクの管理が重要課題となっている。

6.3 IoTセキュリティ

IoT製品に対するセキュリティ要件適合評価及びラベリング制度（JC-STAR）の政府機関等における選定基準への反映が2025年度内に予定されており、金融機関のIoT機器調達においても同基準の適用が見込まれる。

7. 2025年の展望と課題

7.1 能動的サイバー防御の導入

2025年5月に成立したサイバー対処能力強化法により、金融機関等の基幹インフラ事業者は政府への報告義務が強化される。これにより、平時からのインシデント管理態勢の構築と、攻撃の予兆把握・報告体制の整備が必要となる。

7.2 サイバーセキュリティ人材の育成

2025年度内に官民共通の「人材フレームワーク」が策定される予定であり、金融機関においても体系的な人材育成計画の策定が求められる。特に、経営層のサイバーセキュリティリテラシー向上が重要な課題となっている。

7.3 中小企業のサイバーセキュリティ対策

サプライチェーン全体のセキュリティ強化のため、中小企業におけるサイバーセキュリティ対策実施のための環境整備が進められており、2026年度内にサプライチェーン強化に向けたセキュリティ対策評価制度の導入が予定されている。

8. 推奨される対策

8.1 経営層の主体的関与

サイバーセキュリティをトップリスクとして認識し、経営層による定期的な評価・方針決定・モニタリング（EDM）の実施が不可欠である。十分な専門知識の習得と、適切な予算配分・リソース確保が求められる。

8.2 多層的なセキュリティ対策

- 境界防御に加えた多層的な防御体制の構築
- 多要素認証の必須化（特にフィッシング耐性技術の導入）
- EDR（Endpoint Detection and Response）の導入
- DMARC・BIMIによるメールなりすまし対策

8.3 サードパーティリスク管理

- 委託先のセキュリティ基準の契約明示
- 定期的な実地調査・第三者評価の実施
- インシデント発生時の対応体制構築
- 重要度に応じた管理・モニタリング強化

8.4 インシデント対応体制

- インシデント発生を前提とした対応計画策定
- SOC・CSIRTの機能強化
- 定期的な机上演習・実地訓練の実施
- 関係当局・外部専門機関との連携体制構築

9. 結論

2024年度は金融業界のサイバーセキュリティにとって重要な転換点となった。国家系攻撃グループによる高度な攻撃、サプライチェーン経由の大規模インシデント、DDoS攻撃の多発により、従来の境界型防御の限界が明確になった。

金融機関は、経営層の主体的関与の下、多層的なセキュリティ対策、サードパーティリスク管理、インシデント対応体制の強化を通じて、包括的なサイバーセキュリティ管理態勢を構築する必要がある。また、業界横断的な情報共有と国際連携を通じて、変化する脅威に対応する集合的な防御力の向上が求められる。

2025年は、能動的サイバー防御の導入、耐量子計算機暗号への移行準備、AI利活用のリスク管理など、新たな技術動向への対応が本格化する年となる。金融機関には、これらの課題に対する戦略的な取り組みと継続的な投資が求められる。

重要な行動指針

- サイバーセキュリティを経営の最優先課題として位置づける
- 侵入を前提とした多層的な防御体制を構築する
- サプライチェーン全体のリスク管理を強化する
- 業界横断的な情報共有と国際連携に積極的に参加する
- 新技術導入に伴うリスクを適切に評価・管理する

本レポートは2025年6月時点の公開情報に基づいて作成されております。
最新の動向については、各企業・機関の公式発表をご確認ください。

監修者:
鎌田光一郎:青山学院大学法学部卒業。SMBC日興証券株式会社にて証券営業、経営管理業務に従事したのちPwCコンサルティンク゛合同会社に転籍。金融機関に対するコンサルティンク゛業務に従事。その後、Librus株式会社を設立、代表取締役に就任。

お問い合わせ先
Librus株式会社(代表取締役 鎌田光一郎)
105-0004東京都港区新橋6丁目13-12 VORT新橋Ⅱ 4F
03-6772-8015
お問い合わせフォーム
https://librus.co.jp/contact