4D-02

銀行経営における個人情報保護及び サイバーセキュリティ管理に関する環境

氏　名† 高正　智

所　属† 金沢学院大学大学院経営情報学研究科

1. はじめに

2019 年の世界の銀行経営におけるサイバーセキュリティ管理上の最大級の事案として、米国のキャピタルワン銀行での個人情報流出発生がある。アマゾン・ウェブ・サービス社の元社員が 106 百万人分の個人情報を詐取した事件だった。その後 2020 年８月に同行の内部統制が不十分だったという理由から米国政府通貨監督局によって 80 百万ドル（約 83 億円）の制裁金が同行に対し確定した。なお同行は 4 億ドル（約 416 億円）のサイバー保険に加入している事を開示している［1］。

これを機会に日本の銀行経営における個人情報保護及びサイバーセキュリティ管理の環境を整理する。

2. 各国における個人情報保護法対応

日本では平成１５年制定、１７年適用された個人情報保護法に基づき、すべての産業で個人情報保護が法令化された。以降平成２７年及び令和２年に改正が行われ、厳格化が進んでいる。銀行業は預金などを通じ、個人情報を大量に保有することが前提なのでその影響を強く受けている。

令和２年６月に承認された改正により初めて報告が努力義務から義務に移行するとされ、報告期限は３０日以内とすることが検討されている段階である。全面適用は 2022 年だが、罰則のみについては 2020 年 12 月から適用になっており、管理を怠った場合の法人に対する罰則は罰金を最大１億円まで引き上げるなど以前より厳しくなった。

日本には海外に進出する銀行も多く、メガバンクなどは多数の法人向け海外拠点を設け、一部にはリテール業務を展開する子会社も展開している。欧米はもちろん東南アジアに集中的に海外展開しており、その東南アジアに近年個人情報保護やサイバーセキュリティ関連の法令が施行されている。これにより、管理の強化が迫られている。

各国の法令による罰則の罰金は日本よりも高額な上限を設けている国や、情報漏洩の報告が義務化されているばかりか数日以内の時間制限を設けている国もある。情報セキュリティに関する意識は海外において高くなっている。

表１．各国の個人情報保護関連法

地域	法令	適用時期
日本	個人情報保護法	2005
	平成 27 年改正	2017
	令和 2 年改正	罰則 2020/12 全面 2022/6
EU	GDPR	2018/5
米カリフォルニア州	カリフォルニア CCPA	2020/1
シンガポール	個人情報保護法（PDPA2012）	2014/7
ベトナム	サイバーセキュリティ法	2019/1
タイ	個人情報保護法（PDPA）	2021/5

出典：法律事務所公表資料から筆者作成

3. 各国銀行監督におけるサイバーセキュリティ管理

日本の主要な銀行に対する金融庁の監督指針にみるサイバーセキュリティ管理の着眼点は以下のとおり［2］。

表２．主要な銀行等向け総合的な監督指針

Ⅲ－３－７－１－２（５）

項番	内容
1	取締役会におけるサイバーセキュリティの重要性の認識
2	サイバーセキュリティについての組織体制の整備、社内規程の策定
3	サイバー攻撃に備えた多層防御
4	サイバー攻撃の被害があった場合の拡大防止策
5	システムの脆弱性対策

6	セキュリティ水準の定期評価
7	インターネット等による非対面取引のセキュリティ向上のための対策
8	サイバー攻撃を想定した演習への参加
9	サイバーセキュリティに係る人材の育成

これとは別に金融情報システムセンター（FISC）の安全対策基準・解説書があり、網羅性を確保している。

また米国の連邦金融機関検査委員会（FFIEC）におけるサイバーセキュリティ上の文書群は次のようになっている［3］。

表３．FFIEC の WEB サイト上の主要なサイバーセキュリティ管理に関する文書

項番	内容
1	クラウドコンピューティング環境におけるセキュリティ・リスク管理
2	サイバーセキュリティに関するリソースガイド（支援団体・組織の案内）
3	サイバー保険のリスク管理プログラム上の潜在的役割
4	サイバーセキュリティ準備に関する標準的な評価基準
5	NIST サイバーセキュリティ・フレームワークなど

このほかに教育セミナーの資料などが多数提供され網羅性を確保している。

このように日米ともサイバーセキュリティ管理に関する具体的な監督指針の文書化が重層的に行われている。

4. 銀行のサイバーセキュリティ管理を取り巻く環境の変化とむすび

前節および最近の産業界全体の動きを合わせ、銀行経営におけるサイバーセキュリティ管理を取り巻く圧迫要因を以下の表と図にまとめた。

表４．銀行経営におけるサイバーセキュリティ管理への主な圧迫要因

項番	内容
1	内外の個人情報保護法の適用強化
2	銀行業務の国際展開
3	サイバー攻撃・不正の高度化
4	コロナによるテレワーク対応
5	銀行取引のキャッシュレス化
6	費用低減等を目的とした業務のクラウド化および異なるスキルへの対応
7	クレジットカード業務の拡大
8	低金利環境下の経費節減、収益模索

図１．銀行経営におけるサイバーセキュリティ管理への圧迫状況（表４の項目の相関）

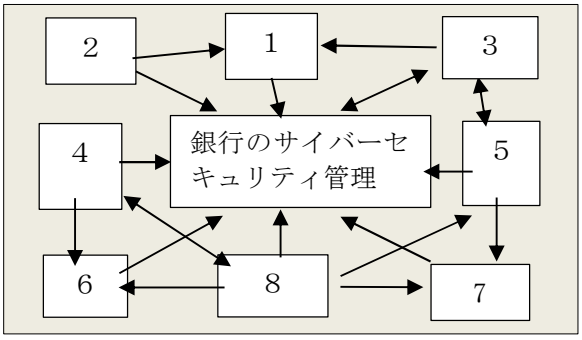

表４および図１：筆者作成

これら銀行経営におけるサイバーセキュリティ管理を取り巻く圧迫要因を「８つのフォース」と呼ぶことにしたい。今後これらの相関関係を実証する必要があるが、定性的な因果関係を図１に示す。

日本では金融庁がすべてを統括しているわけではなく、７は経済産業省が、６は総務省がそれぞれのサービスプロバイダーを統括し、３には個人情報保護委員会および警察庁が係わるなどしている。米国では FFIEC のサイバーセキュリティタスクフォースがワンストップな対応をしている模様である。

今後、日本の銀行はサイバーセキュリティ管理上のリスクの回避、低減はもちろんだが、経営レベルにおいてリスクの受容、移転を迫られる可能性がある。対策としてサイバー保険の更なる検討や資本配賦の検討が考えられる［4］。

参考文献

［1］米国 Edgar 上の Capital One に関する 10-Q 開示, 2019/10/31 および 2020/9/30
［2］ 金融庁、「主要な銀行等向け総合的な監督指針」、2020 年７月、251 頁
［3］FFIEC,”Cybersecurity Awareness”, https://www.ffiec.gov/cybersecurity.htm
［4］佐久間・猪俣、「サイバー保険の調査・分析による加入率向上への提案」、情報処理学会研究報告、2019/3/7

The environment for personal data protection and cyber-security control in banking management
Satoshi Takamasa†
Graduate school of Business administration and information science, Kanazawa Gakuin University