

中国証券業における サイバーセキュリティの強化に向けた動き

関根 栄一・宋 良也

中国証券業における初のサイバーセキュリティ関連規則

中国証券監督管理委員会（証監会）は2023年2月27日に、「証券・先物業のネットワーク及び情報セキュリティ管理弁法」（以下、管理弁法）を公布し、同年5月1日に施行した。管理弁法は、中国の証券業における初めてのサイバーセキュリティに関するルールとして、証券市場に関わる公共インフラの運営機関と証券業者の義務等を定めている。

管理弁法制定の背景には、中国でサイバーセキュリティ関連事案（インシデント）発生への対応強化がある。中国当局は2016年以降、①ネットワークの安全保障を目的とした「サイバーセキュリティ法」、②データセキュリティを保護する上でのデータの越境移転・利活用を促進するための「データセキュリティ法」及び③個人プライバシーの保護を目的とした「個人情報保護法」という、いわゆる「データ三法」を順次公布・施行し、中国全体のサイバーセキュリティの基礎となる法体系を整備した。

証監会は管理弁法の制定に際し、「サイバーセキュリティを巡る情勢が厳しく複雑化している中、上位法であるデータ三法の要求を証券業に適用・具現化すべく、同管理弁法を制定した」という立法趣旨を述べている。また、証券取引所や証券登記決済機関における重要なネットワーク施設や情報システムを含む「重要情報インフラ施設（Critical Information Infrastructure、以下、CII）」の安全確保に関しても、証券業において重視する姿勢を示している。

管理弁法の適用対象と4つの重点分野

上記管理弁法の適用対象は、まず、前述の立法趣旨を踏まえて、資本市場の公共機能を担うCIIを運営するコア機関（証券取引所等）や、証券会社、公募基金管理会社（投信会社）

といった経営機関、証券業務に必要なCIIの開発、テスト、評価、運営・日常管理を担当するITサービス提供者等としている。

次に、上記管理弁法は、①ネットワーク及び情報の安全な運用、②投資家の個人情報保護、③ネットワーク及び情報の安全面での応急措置、④CIIの安全確保、という4つの重点分野に関する施策を設けている。そのうち、①のネットワーク及び情報の安全な運用においては、前述のコア機関・経営機関に対し、その重要性（社会・国家へ及ぼす影響の広さ並びに深刻度合い）をレベル分けし、異なる水準で管理を行うとしている。その上で、これらの機関が運営するCII等に対し、ストレステストを恒常的に行うメカニズムの構築が求められたことが特徴となっている。

また、④のCIIの安全確保では、コア機関に年1回のネットワークと情報安全検査及びリスク評価の実施を義務付け、その内容にはCIIの運行状況、直面する主な脅威、リスク管理の状況、応急措置の状況などを含めている。

業界を横断した集中的バックアップデータセンターの設立

上記の他に、管理弁法において特に注目されている措置として、「証券業界全体をカバーする集中的バックアップデータセンターの設置」が挙げられる。従来、証券会社をはじめとする経営機関は、データのバックアップを自社で行うのが一般的であった。一方、証監会としては、各社が保有するデータを各自にて個別バックアップをした上で、証監会が集中管理するバックアップセンターを設置して管理した方が、地震等の「重大な災害」への対応力を高めることが可能と判断している。そのため、管理弁法では証券取引所等のCIIの運営者に対し、上記の集中的バックアップデータセンターにて重要なデータをバックアップするよう奨励するとし、コア機関・経営機関は自社の必要に



応じて同センターを利用することが可能としている。

海外からの評価と今後の注目点

前述のように、証監会は証券業におけるサイバーセキュリティの管理監督に対し、サイバーインシデントの発生防止に重点を置くと同時に、中核となるネットワークシステムの持続的な運営・利用を重視する方針である。業界を横断した集中的バックアップデータセンターの設立も同方針の下で制定されていると考えられる。

一方で、海外の関連機関は異なる観点から、これらの施策に対して異論を表明しているものもある。例えば、アジア証券業金融市場協会(ASIFMA)は、管理弁法のパブリックコメント募集時に、①当局へのセンシティブなデータの共有はハッカーに狙われやすい、②ペネトレーション(侵入)テストには破壊性が

あり、企業運営に重大なリスクをもたらす可能性がある、③集中的バックアップデータセンターの設立はサイバー攻撃の標的となり、中国及びグローバル金融業に大きなシステムリスクをもたらす恐れがある、などのフィードバック意見を証監会に提出している。総じて、ASIFMAは、管理監督当局が主導するサイバーセキュリティ向けの施策よりも企業の自主性を十分に發揮するような対応が望ましい、という当局の考え方とは違うスタンスを探っている。こうした意見の一部を受け入れたためとも思われるが、証監会は、管理弁法の正式版においてペネトレーションテストの実施に関する項目を削除している。

今後、中国の証券業界におけるサイバーセキュリティでの法整備に関する取り組みがどのように現場レベルにまで反映されていくのか、管理弁法の適用対象機関のサイバーレジリエンス向上にどの程度寄与するのかが、注目される。