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

▌要　約▐

1. 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、証券市場の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。
2. 管理弁法制定の背景には、中国でサイバー関連事案（インシデント）発生への対応強化がある。全国人民代表大会は 2016 年以降、「サイバーセキュリティ法」、「データセキュリティ法」及び「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。今般の管理弁法は、上位法であるデータ三法が求める内容を証券業に適用することが目的となっている。
3. 上位法の要求を具体化するため、管理弁法では、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、④重要情報インフラ施設（CII）の安全確保、の 4 つの分野に対し、規定を設けている。また、当局による管理監督の強化措置として、証監会が主導する集中的データバックアップ制度の構築や、IT サービス提供者に対する管理監督の強化が盛り込まれている。
4. アジア証券業金融市場協会（ASIFMA）は、2022 年 4 月の管理弁法のパブリックコメント募集時に証監会に提出したフィードバック意見にて、当局へのデータ提供や当局が主導する上記施策に対し、企業の自主性を十分に発揮・尊重した上での対応が望ましいと提案し、その一部は正式版に取り入れられたように見受けられる。今後、中国の証券業界におけるサイバーセキュリティ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るのか、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。

野村資本市場研究所　関連論文等

・江夏あかね・門倉朋美「米国証券市場におけるサイバーセキュリティリスク対処に向けた SEC 規則案の公表」『野村サステナビリティクォータリー』2023 年春号。
・板津直孝「米国の外国企業説明責任法と中国におけるデータ統制－求められる国際的に自由なデータ流通の確保－」『野村資本市場クォータリー』2022 年冬号。
・宋良也「モバイルアプリを使った株式取引の普及と中国証券業界の変化」『野村資本市場クォータリー』2019 年春号。

Ⅰ はじめに

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）[1]を公布し、同年 5 月 1 日に施行した[2]。管理弁法は、中国の証券業[3]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であり、証券業分野でのサイバーセキュリティ対策を包括的に明記したものとして、市場関係者から注目されている。

本稿では、管理弁法制定の経緯を概観した上で、管理弁法の論点を整理する。そして、海外の関係機関によるパブリックコメントへのフィードバックを取り上げ、証券会社の経営に与え得る影響等について考察する。その上で、中国の証券業界におけるサイバーセキュリティで今後想定されるシナリオを展望する。

Ⅱ 管理弁法制定の経緯

本章では、管理弁法制定の経緯として、（1）管理弁法の上位法に位置付けられる「データ三法」の制定経緯、（2）制定後に発生したサイバーインシデント（サイバー攻撃等によって発生するシステム障害等）の状況、を概観する。

１．「データ三法」の公布・施行

中国では、2000 年代に入った頃から、産業界がサイバーセキュリティの面から様々なリスクに直面していた。例えば、①ハッカー等がシステムに不法侵入し、顧客情報・取引情報等を含む個人情報を盗み出すケース、②企業が顧客の承諾無しに個人情報を収集したり、必要以上に顧客情報を収集したりするケース、③ネットワークや情報管理が不十分で、外部者が個人情報等に容易にアクセスし、漏洩してしまうケース、などが散見された。公安部（日本の警察庁に相当）が 2017 年 3 月 10 日の記者会見で発表したところによれば、2016 年に中国本土において検挙された各種のプライバシー侵害案件が 1,886 件、犯罪容疑者の確保は 4,261 名に上った。また、ハッカーによるサイバー攻撃等の犯罪案件は 828 件、犯罪容疑者の確保は 1,747 名に上るとされた[4]。こうした様々なサイバーセキュリティ関連のリスクに対して、2016 年までは中国全土で包括的に適用・施行される法令レベルの

1 弁法とは、行政上の規則やルールを意味する。また、「ネットワーク及び情報セキュリティ」とは、管理弁法の中国語名称を直訳したもので、証券業におけるサイバーセキュリティを指すものである。
2 中国証券監督管理委員会「【第 218 号令】《证券期货业网络和信息安全管理办法》」2023 年 2 月 27 日。
3 同管理弁法で言及した先物とは、商品先物及び金融先物の両方が含まれる。本稿では、証券業のみを対象とするため、以降は、法律名を除き「証券・先物業」を一律「証券業」と略称する。
4 「公安部部署整治黒客攻撃破壊和網絡侵犯公民個人情報犯罪行動」公安部ウェブサイト、2017 年 3 月 13 日。

ルールが存在していなかった。そのため、法令以下の規則・指針レベル[5]で、ネットワークの安全確保、データ管理の強化、個人情報の保護に対応していたが、行政としては法執行の根拠が足りない等の点で限界があった。

このような背景の下、全国人民代表大会（全人代）常務委員会が 2015 年 7 月 1 日に制定・公布した「国家安全法」（即日施行）では、国家安全の対象として、第 25 条で「ネットワーク及び情報」分野を取り上げた。同条では、第一に、「国は、ネットワーク及び情報の安全保障体系を構築し、ネットワーク及び情報の安全保護能力を向上させ、ネットワーク及び情報のイノベーション関連研究及び開発応用を強化し、ネットワーク及び情報の中核技術、基幹インフラ及び可制御性を実現する」とされた。第二に、「国は、ネットワーク管理を強化し、ネットワーク攻撃、ネットワーク侵入、ネットワーク秘密窃取、違法有害情報流布等のネットワーク違法犯罪行為を防止し、制止し、法に従い懲罰し、国のネットワーク空間における主権、安全及び発展の利益を維持保護する」とされた。

この国家安全法の制定・施行後、ネットワーク及び情報分野での立法措置の制定作業が加速度的に進められた。最初に、2016 年 11 月 7 日、全人代常務委員会は「サイバーセキュリティ法」を可決した（2017 年 6 月 1 日施行）。次に、2021 年 6 月 10 日、全人代常務委員会は、「データセキュリティ法」を可決した（同年 9 月 1 日施行）。最後に、2021 年 8 月 20 日、全人代常務委員会は「個人情報保護法」を可決した（同年 11 月 1 日施行）。

このうち、データセキュリティ法では、データの国際移転に関し、①データ輸出管理制度、②データ利用対抗措置、③国外データの報告認可制度、等の内容を含んでおり、同法の域外適用についても規定している[6]。また、このデータ三法に共通する考え方として、サイバーセキュリティと、データや個人情報の保護・管理において、中国本土と本土外の間での移転に審査制度や制限措置を設け、中国本土のサイバーセキュリティの安全を確保しようとすることが挙げられる。

特に、サイバーセキュリティ法では、「重要情報インフラ施設」（Critical Information Infrastructure、以下、CII）[7]の安全確保について強調している。サイバーセキュリティ法の公布・施行を受け、国務院（内閣）は 2021 年 7 月 30 日に「重要情報インフラ施設安全保護条例」を公布し、上位法と本条例を組み合わせて、サイバーセキュリティ法が求める要求に応えようとしている（図表 1）。

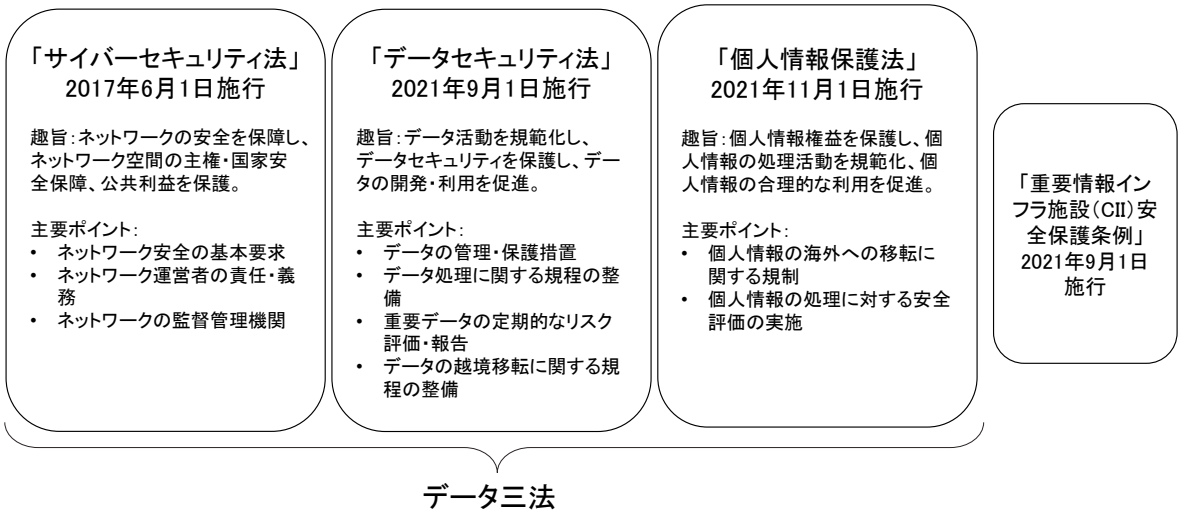
---

5 例えば、個人情報保護に関しては、2013 年に公布された「消費者権益保護法」にて「消費者の個人情報」という形で保護しようとしている。また、同年に公布された「個人情報保護指針」は、個人情報保護に関する初の国家的指針とされた。

6 中国国外の組織及び個人がデータ活動を展開して中国の国家安全、公共利益又は公民組織及び合法的権益を損なった場合、データセキュリティ法に基づき責任を追及する。

7 重要情報インフラ施設とは、「公共通信と情報サービス、エネルギー、交通、水利、金融、公共サービス、デジタル行政、国防科学技術工業等の重要な業界・分野の重要なネットワーク施設や情報システム」を指す。これらのインフラで、いったん破壊・機能喪失・データ漏洩が発生すると、国家安全、国家計画や民生、公共利益に重大な危害をもたらすこととなる（国務院「重要情報インフラ施設安全保護条例」を参照）。

図表 1　上位法としての「データ三法」と「CII 安全保護条例」



（出所）国務院・証監会ウェブサイトより野村資本市場研究所作成

２．「データ三法」施行後も頻発するサイバーインシデント

「データ三法」が制定・公布された後、証券業以外の各業界では、同法に基づいて対応を進めているものの、引き続き個人情報の漏洩につながるサイバーインシデントが頻発する傾向がみられている（図表 2）。

その一方、証券業を含む金融業界において、サイバーインシデントがどれぐらい、どのような頻度で、どういった内容で発生しているのかについて、当局や金融機関から公式に発表されているわけでない。これは、証券会社及びその情報技術サービス提供機関は、当局の許可なしにサイバーインシデントを開示してはいけないと規定されているためである[8]。ただし、海外メディアが報じた事例として、中国工商銀行（ICBC）の米国支店がランサムウェア（身代金要求型ウイルス）の攻撃を受け、情報システムが機能不全となり、米国債取引における決済ができなくなった件は記憶に新しい[9]。中国国内の事例としては、深圳証監局[10]が 2022 年 10 月、管轄下の証券会社（社名は未公開）の事務作業の自動化システム（Office Automation〔OA〕システム）が外部からのインジェクション攻撃を受けたと発表した事例がある[11]。

なお、証監会や証券取引所等が、サイバーインシデントを除く証券会社のシステム障害の事例を公表し、該当証券会社に対し処罰をすることがある（図表 3）。システム障害は、

8　証監会「証券基金経営機構信息技術管理弁法」（2018 年 12 月 19 日公布、2019 年 6 月 1 日施行）、「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」（2023 年 2 月 27 日公布、2023 年 5 月 1 日施行）を参照。

9　「中国大手銀がサイバー被害　米国債取引に影響、金利上昇」『日本経済新聞』2023 年 11 月 10 日、「中国工商銀にサイバー攻撃、米国債に影響」『ブルームバーグ』2023 年 11 月 10 日。

10　証監局は、証監会傘下の地方出先機関を指す。

11　「インジェクション攻撃」とは、コンピュータプログラムが無効なデータを処理した場合に出現するバグを、攻撃者が悪用して、不正な命令を実行する攻撃手法を指す（深圳証監局「証券期貨機構監管通訊（2022 第 5 期）」を参照）。

図表 2　中国におけるサイバーインシデントの事例（2022 年のケース）

年月	被害者	事件内容の概要
2022年2月	求人プラットフォーム	某テック会社はクローラープログラムを使用し、求人プラットフォームより2.1億人分超の個人情報を違法に収集。
2022年7月	上海市国家警察データベース	「ChinaDan」と名乗るハッカーは、上海国家警察のデータベースから取得した10億人の氏名、住所、出生地、身分証明書番号、携帯電話番号などの個人情報をハッカーフォーラム「Breach Forums」で売却すると投稿（2022年7月5日付日本経済新聞にも掲載）。
2022年8月	上海市ビッグデータセンター（上海随申コード）	上海市ビッグデータセンターが研究開発したコロナ対策のための個人コードである「上海随申コード」のデータベースがハッキングされ、4,850万人分の氏名、携帯電話番号、UUID（Universally Unique Identifier）等のユーザーデータが流出。ダークウェブフォーラム上で4,000米ドル（約 2.7万人民元）でオークションにかけられた（2022年8月13日付読売新聞にも掲載）。
2022年9月	40行を超える国内金融機関	中国国内のハッカーがトロイの木馬を使用して、2,000台以上のコンピューターを不正に制御し、40行を超える国内金融機関のイントラネット取引データベースに侵入。取引指示書と複数のインサイダー情報を不正に入手し、関連株取引を実行。被害金額は183万元。
2022年9月	西北工業大学	中国コンピュータウイルス緊急対応センターと「360株式会社」は、西北工業大学の海外でのサイバー攻撃に関する調査レポートを公表。調査報告によると、米国国家安全保障局（NSA）は西北工業大学を攻撃し、同大学の主要なネットワーク機器構成、ネットワーク管理データ、運用および保守データ、その他のコア技術データの窃取に成功。
2022年12月	上海蔚来汽車（NIO）	ハッカーによる公式アプリへのハッキングで、2021年8月以前の一部の顧客情報、取引情報、ローン情報などの重要な個人情報が漏洩されたとみられる。
2023年9月	上海市政府	上海市政府に情報システムサービスを提供する技術会社は、一部市民の個人情報（1.5万項目）の保存にプライベートクラウドを使用したことで、ハッカーに同情報をハッキングされた。

（注）　2022 年 2 月の事例の「クローラープログラム」とは、ウェブ上の情報を自動的に収集してデータベースを構築するプログラムを指す。

（出所）中国ビジネス COMPASS やその他報道より野村資本市場研究所作成

図表 3　証券会社のシステム障害（サイバーインシデントを除く）事例

年月	事業者	システム障害（サイバーインシデントを除く）の内容
2006年1月	中信証券	北京市の支店のオークション取引システムに故障が発生。約1時間の間、投資家は発注ができなかった。
2014年2月	中信証券	オークション取引のシステムサーバーに問題が発生し、約30分間、投資家は発注ができなかった。
2023年3月	東方財富証券	午前・午後にわたって、投資家はアプリにログインできない、保有残高に異常表示、取引が不可等の問題があった。
2023年5月	華宝証券	約2時間の間、投資家はアプリにログインできない、取引が出来なかった。
2023年6月	中信証券	UPS電源の故障により、オークション取引のシステムサーバーがシャットダウンされ、一部の顧客がアプリへのログインやオンライン取引が19分間実行不可能となった。

（出所）証監会（深圳証監局）、上海・深圳証券取引所ウェブサイトより野村資本市場研究所作成

①証券会社の株式取引システムサーバーが、通常の運用や補修等の過程において、投資家が取引の発注をできないケース、②オンラインやモバイルアプリにアクセスができないケース、が多いようである。

証監会は、2018 年 12 月に公布した「証券基金経営機構信息技術管理弁法」において、システム障害が発生し、投資家の注文に応じられない場合等についての社内の業務分担や、顧客向け開示の手順を定めている。これは、証監会が、管理弁法の制定以前から、①どのようにシステム障害への証券会社の意識・対応を高めていくのか、②どのように取引インフラを整備してシステム障害を未然に防止するのか、③既に発生したシステム障害の影響をどのように取り除き、早期復旧を実現するのか、といった問題意識を有してきたことを示唆していると言える。

Ⅲ 証券業のネットワーク及び情報セキュリティ管理弁法の概要

本章では、今般の管理弁法の立法趣旨や適用対象となる機関を明示した上で、管理弁法が上位法であるデータ三法をどのように具体化しているかを紹介する。また、証監会の管理下におけるバックアップデータセンターの設立や IT サービス提供者の証監会への届出制度についても触れる。

１．管理弁法の全体像

１）管理弁法の立法趣旨と適用対象機関

今般の管理弁法の公布時に、証監会は立法趣旨について、「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、データ三法上の要求を証券業においても適用し実施していくことが必要」との認識を示している。また、前述の「重要情報インフラ施設安全保護条例」の要求を証券業でも適用されるための内容が管理弁法に盛り込まれでいる。

以上の立法趣旨等を踏まえて、今般の管理弁法の適用対象は、前述の通り、①主に証券取引所や証券登記決済機構といった市場の公共機能を担いかつ CII の運営をするコア機関と、②証券会社、先物会社、公募基金管理会社等の経営機関、③証券業務上必要とする 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[12]、の 3 種類に分けられる。管理弁法は、各適用対象機関がそれぞれ果たすべきサイバーセキュリティ面での役割や責任を明記している。また、原則として、各機関の役割・責任は、サイバーセキュリティ関連の商品・サービスを提供している他の関連業者に転嫁したり、軽減したりすることはない。

さらに、管理弁法では、前述の適用対象 3 機関以外の商業銀行や公募基金販売会社、私募基金管理会社など、一部の関連機関に対し、「本管理弁法を参照した上で適用す

[12] 金証股份、恒生電子が代表的な会社である。

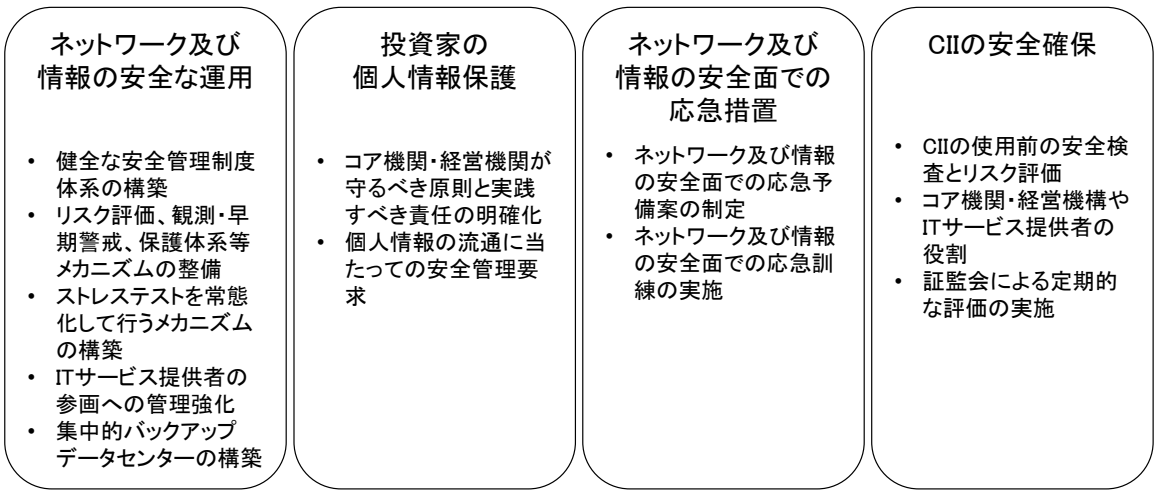
る」と規定している。これらの機関は管理弁法の直接の適用対象とはならないが、証券業でのサイバーセキュリティの関連事案が発生した場合、管理弁法は一定の参考基準として適用されることで、包括的かつ柔軟に証監会が対応する余地を残していく狙いがあるものと考えられる。なお、証監会では、「科技監督司」が証券・先物・ファンド業界のサイバーセキュリティ、データセキュリティ等への管理監督を担当している。

2）証券業における「データ三法」上の要求を具体化

前述のように、管理弁法は上位法である「データ三法」が求める内容を証券業で適用をすることを目的としており、その要求内容の具体化を図っている。管理弁法上では、主に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、の 4 つの分野に分けている（図表 4）。

これらの 4 つの分野の中で、特に注目すべき点として、①のネットワーク及び情報の安全な運用が挙げられる。本分野では、コア機関・経営機関に対し、上位法のサイバーセキュリティ法で定めているサイバーセキュリティのレベルに応じた保護制度[13]を適用するとともに、ストレステストを常態化して行うメカニズムを構築すること等を求めている。また、後述の通り、コア機関・経営機関の IT サービス提供者に対する管理監督を強化することや、証監会主導による集中的データバックアップ制度を構築することも規定されている。

図表 4　証券業のネットワーク及び情報セキュリティ管理弁法の概要



（出所）「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」より野村資本市場研究所作成

[13] 「サイバーセキュリティ等級保護制度」と呼ばれ、情報システムで障害もしくは情報漏洩が発生した際に、システムを保有する主体を含め、社会・国家へ及ぼす影響の広さ並びに深刻度合いによって、システムごとの重要性（等級）を定め、その重要性に応じて、しかるべきセキュリティ対策内容を定義し、管理する制度を指す。

加えて、④の CII の安全確保では、CII の使用前における安全検査とリスク評価について、管理弁法では、コア機関に対し、年 1 回のネットワークと情報安全検査と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が含まれる。また、コア機関は、CII の運用状況に対する継続的な監視が必要とされる。特に CII のシステムの性能については、その容量が常に過去のピーク時の 3 倍以上、取引時間内におけるネット容量は 1 年以内の使用ピーク時の 2 倍以上という数値基準が設けられている。

２．当局による管理監督強化措置の内容

１）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構築

今般の管理弁法で特に注目されている管理監督上の措置として、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、証券会社などの経営機関では、自社の管理下でデータのバックアップをするのが一般的な措置として行われてきた[14]。一方、証監会としては、各社が保有するデータを各自に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、「重大な災難への対応力」[15]を高めることが可能と判断している。

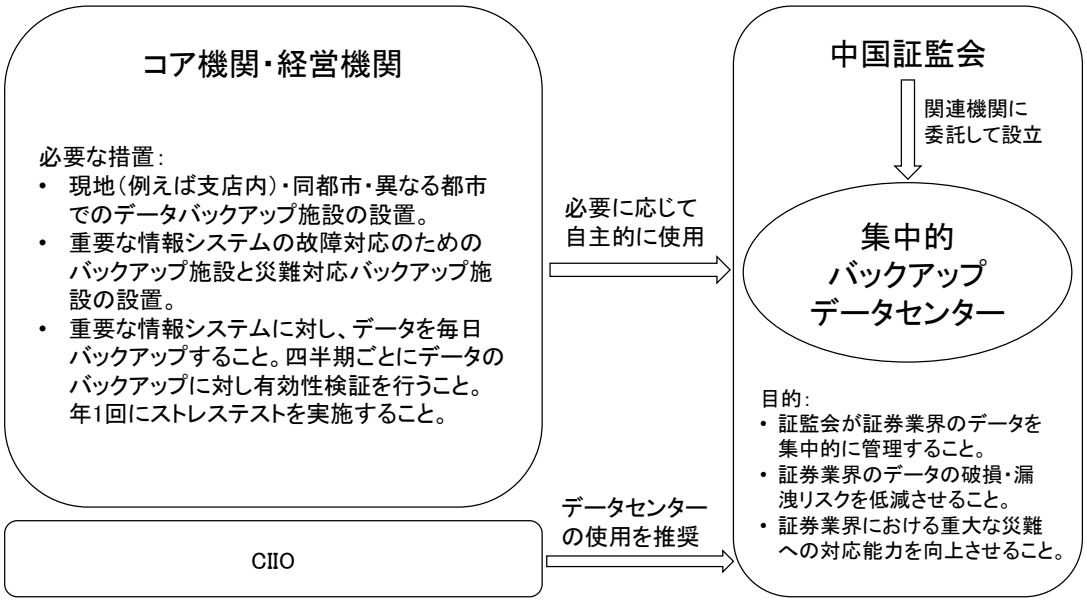
そのため、管理弁法では、証券業における重要情報インフラ施設運営者（Critical Information Infrastructure Operators、以下、CIIO）[16]に対し、上記の集中的バックアップデータセンターにおいて、必要なデータのバックアップするよう奨励すると規定している。コア機関・経営機関は、自社の必要に応じて、自主的に集中バックアップデータセンターの利用を選択することが可能である（図表 5）。コア機関・経営機関は、証監会の意向を踏まえた対応をしていくものと思われる。

[14] 例えば、深圳証券取引所は、自社のバックアップデータセンターを北京市や広東省・東莞市に設置しており、また、北京市、上海市、広東省・東莞市にて災害対応のための応急センターを設立している。

[15] 「重大な災難への対応力」とは、「地震等の災害が起こった場合、情報システムが所在都市・地域の電力、通信、交通がマヒ状態となり、人的被害もある状況で、情報システムの早期復旧・継続運用する能力を確保する能力」を指す（証監会「証券・先物経営機構情報システムバックアップ能力標準」〔2011 年 4 月 14 日公布・同日施行〕を参照）。

[16] CIIO は、前述の CII を運営する主体である。証券業においては、証券・先物取引所、証券登記決済機関等が CIIO に該当すると想定されている。

図表 5　証券業の集中的バックアップデータセンターの仕組み

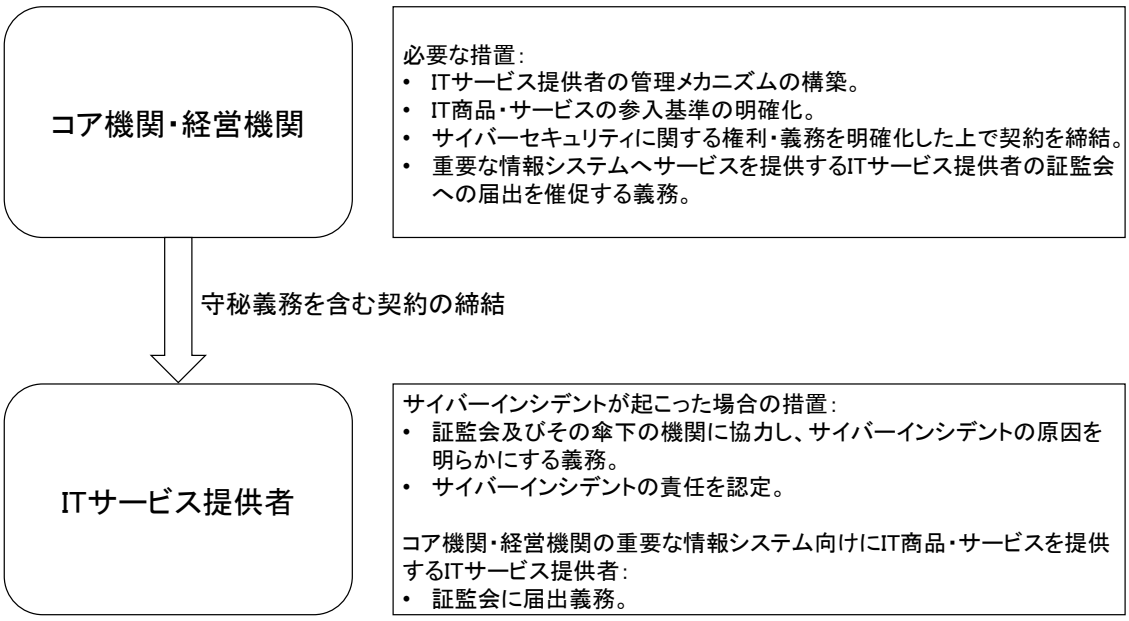


（注）　「重要な情報システム」とは、「証券業の重要な業務活動を担うシステム」を指す。同システムを使ったサービスで、異常やデータ漏洩が発生した場合、証券市場や投資家に重大な影響をもたらす事態が想定されている。
（出所）「証券・先物業のネットワーク及び情報セキュリティ管理弁法」より野村資本市場研究所作成

2）証監会への IT サービス提供者による届出制度

管理弁法では、コア機関・経営機関の IT サービス提供者に対する管理監督強化に関する内容を盛り込んでいる。第一に、IT サービス提供者は、コア機関・経営機関が証監会による IT 商品・サービスの参入基準に満たしているかどうかを確認し、各分野のサイバーセキュリティに関する権利及び義務を明らかにした上で契約を結ぶことが求められる。第二に、CII へサービスを提供する IT サービス提供者は、証監会への届出が必要とされ、当該サービス・商品が国家安全に影響を及ぼす可能性がある場合、国家インターネット弁公室へのサイバーセキュリティ審査の申告も必要とされる（図表 6）。上記の 2 点目のうち、2022 年 4 月の管理弁法のパブリックコメント募集時は、全ての IT サービス提供者が証監会への届出が必要とされたのに比べて、正式版は CII の IT サービス提供者のみを対象としている。管理監督にも強弱を付け、サービス提供機関の届出コスト等も考慮したものと思われる。

図表 6　証監会への IT サービス提供者による届出制度の仕組み



（出所）「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」より野村資本市場研究所作成

Ⅳ 海外からの評価

本稿で概観したように、証監会は、証券業におけるサイバーセキュリティでの管理監督に対し、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・利用を重視している。管理弁法における業界を横断した集中的バックアップセンターの設立といった施策も、こうした方針を基に制定されていると考えられる。

ただし、海外の関係機関からは、こうした施策に対して異論も表明されている。例えば、アジア証券業金融市場協会（Asia Securities Industry & Financial Markets Association、以下、ASIFMA）[17]は、2022 年 4 月の管理弁法のパブリックコメント募集時に、①センシティブなデータ[18]の共有、②ペネトレーション（侵入）テスト[19]、③証券業界全体に適用する集中的バックアップデータセンターの設立、④IT サービス提供者の当局への届出政策、の 4 分野に対し、フィードバック意見を証監会に提出している[20]（図表 7）。

[17] ASIFMA は、香港を拠点に、アジア・太平洋地域の金融機関（銀行、ノンバンク、アセットマネジメント会社）から構成される自主組織である。2024 年 1 月時点でのメンバー数は 161 機関で、日系では、メガバンク 3 行（MUFG、三井住友フィナンシャルグループ、みずほフィナンシャルグループ）、野村ホールディングス、野村アセットマネジメント等がメンバーとなっている。

[18] 個人のプライバシー等に関する事項等、慎重に扱われるべき情報を指す。

[19] ペネトレーションテストとは、想定されるサイバー攻撃の手法に基づき、ホワイトハッカー（本件では証監会及びその委託を受けた第三者が担当すると想定される）が実践的にシステムに「侵入」をすることで、システムのサイバー攻撃に対する耐性を図るためのテストである。

[20] ASIFMA「『証券・先物業ネットワーク安全管理弁法（パブリックコメント版）』へのフィードバック意見」2022 年 5 月 31 日。
＜https://www.asifma.org/wp-content/uploads/2022/06/asifma-response-to-csrc-consultation-on-cybersecurity-measures-final-chinese-translation-pdf-2.pdf＞

図表 7　管理弁法のパブリックコメント募集時の ASIFMA からのフィードバック

項目	主な意見
センシティブなデータの共有	• 管理弁法（パブリックコメント版）では、各種目的により、データの共有を経営機関に要求している。 • 経営機関にとって、一部のサイバーセキュリティ関連のセンシティブなデータは、ハッカー等に狙われやすい。 • 我々は、このようなデータ収集を軽減するよう証監会に勧める。
ペネトレーション（侵入）テスト	• 管理弁法（パブリックコメント版）の第52条では、証監会及びその委託を受けた第三者は、コア機関・経営機関に対しペネトレーションテストを行うことができると規定している。 • 証監会によるペネトレーションテストには破壊性があり、企業運営に重大な影響をもたらすリスクがある • 我々は、経営機関が主導するペネトレーションテストの実施を容認し、経営機関と協力した上で、セキュリティホールを管理することを証監会に勧める。
証券業界全体に適用する集中的バックアップデータセンターの設立	• 管理弁法（パブリックコメント版）では、証券業界全体に適用する集中的バックアップデータセンターを設立し、経営機関に積極的に使用するよう求めている。 • 前述のように、経営機関が保有するデータ（特にセンシティブなデータ）は、ハッカー等不法な主体にとって極めて有用である。集中的バックアップデータセンターはハッカー等によるサイバー攻撃の目標となりやすい。 • 集中的バックアップデータセンターがサイバー攻撃の標的となり、データが破壊もしくは漏洩されたときのリスクは、クローバル金融業の相互接続性が広がっている現状の下で、コア機関・経営機関自身だけでなく、中国及びグローバル金融業に大きなシステミックリスクをもたらす恐れがある。 • 我々は、企業自身によるサイバーセキュリティの評価・管理を容認するという国際的な標準に適合した方法で、サイバーセキュリティの強化を図ることを証監会に勧める。
ITサービス提供者の当局への届出政策	• 管理弁法（パブリックコメント版）では、ITサービス提供者の活動に対し、証監会が直接的に管理監督する要求が含まれる。 • 国際的なやり方では、ITサービス提供者は金融管理監督当局による許可・監督を受けない。 • ITサービス提供者は、コア機関・経営機関と契約を結び、サービスの提供及び報告義務の履行をするのが一般的である。 • 我々は、証監会が国際的なやり方に寄り添い、直接ITサービス提供者に情報を求めないことを勧める。

（出所）ASIFMA ウェブサイトより野村資本市場研究所作成

上記フィードバック意見の共通点としては、センシティブなデータをサイバー攻撃に遭わないようにするためとは言え、当局へのデータの提供といった形でのデータの移転・バックアップについて、消極的な態度をとっている。また、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発揮した上での対応が望ましいと提案しており、当局と考え方の乖離が見られる。

なお、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。また、管理弁法における IT サービス提供者の当局への届出政策についても、前述のように、パブリックコメント募集版と比べて、大きく緩和している。証監会としても、サイバーセキュリティでの管理監督の強化を進める一方、合理的と判断すれば、ASIFMA のような海外での管理監督や事例を踏まえた意見についても取り入れる姿勢を示したとも考えられる。

V 今後の注目点

管理弁法が公布・施行されてから、当局は引き続きサイバーセキュリティ関連の法制度の整備を進めている。直近の動きとして、国家インターネット情報弁公室（CAC）[21]が2023年12月8日に「サイバーセキュリティ事件報告管理弁法」のパブリックコメントを募集したことが注目されている。同弁法は、サイバーインシデント・システム障害等を含めた「社会への影響が大きい」サイバーセキュリティ事件[22]の当局への報告体制を整備することを目的としている。サイバーセキュリティ事件の種類・レベルに応じて、該当するネット運営者は国への報告義務があるとしている。これを受け、管理弁法の内容が実際に現場で適用・運用される際には、コア機関・経営機関は同弁法の制定機関である証監会だけでなく、CAC、国家発展改革委員会傘下の国家データ管理局（2023年3月に新設）、情報産業を所管する工業・情報化部や情報犯罪を取り締まる公安部へ報告しなければならない可能性がある。また、これらの政府部門の間で、協力・連携を図るメカニズムが必要と想定される。加えて、同管理弁法の実施細則や、証券取引所・中国証券業協会等の自主規制機関による規則制定も行われていくことになるとみられる。

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。

[21] CACは、国務院の認可を得て2011年5月4日に設立された国務院傘下の機関である。CACは、工業・情報化部の情報化推進・ネット情報セキュリティの機能を担っている。また、同機関は、2014年に組織改正され、インターネットコンテンツに対する管理監督・法執行権限が加えられたほか、中国共産党中央委員会での内部機関の役割も持ち、党側では「中央インターネットセキュリティ・情報化委員会弁公室」の名称も付された。

[22] ここでのサイバーセキュリティ事件は、「人為的な原因、ソフトウェアやハードウェアの欠陥や故障、自然災害等により、ネットワーク及び情報システム又はその中のデータに危害を与え、社会に対してマイナス影響を与える事件」と定義されている（「サイバーセキュリティ事件報告管理弁法〔パブリックコメント版〕」を参照）。