证券期货行业如何履行网络安全合规义务
——《证券期货业网络安全管理办法(征求意见稿)》简评

作者：杨迅 | 夏雨薇

自 2017 年《网络安全法》生效以来，网络安全一直是各行各业合规的重点之一。尤其是，包括证券基金期货在内的金融服务业，由于其在国民经济中的重要地位以及投资者个人信息的高度敏感性，网络安全和信息保护的合规一直是被关注的问题。近期，证监会颁布的《证券期货业网络安全管理办法(征求意见稿)》(“**《网安管理办法征求意见稿》**”)首次试图系统性地归纳和细化了《网络安全法》《个人信息保护法》《关键信息基础设施安全保护条例》在证券期货行业的适用。本文在简要介绍《网安管理办法征求意见稿》的基础上，就其对证券期货行业的影响作出简要评述。

1. 《网安管理办法征求意见稿》的颁布

2022 年 4 月 29 日，证监会起草并公布了《网安管理办法征求意见稿》。此次《网安管理办法征求意见稿》的起草主要反映近年来网络安全领域法律的更迭发展，尤其是落实《数据安全法》《个人信息保护法》等上位法在证券期货行业的适用。此外，证监会对核心机构、经营机构以及信息技术服务机构管理不断深化，在信息技术方面的监管也不断深化。

《网安管理办法征求意见稿》生效后将取代 2012 年《证券期货业信息安全保障管理办法》(以下简称“**《安全保障办法》**”)。较之后者，《网安管理办法征求意见稿》的重点主要体现在以下若干方面：(1)细化适用主体与监管要求；(2)对证券期货业从业机构的网络安全内部管理制度、技术措施、应急处置措施提供更高要求；(3)深化关键信息基础设施网络安全保护要求；(4)落实证券期货业有关机构的数据保护义务；(5)加强证监会对证券期货业有关机构的监管，确定多项证券期货业相关机构的备查、主动报告义务与报告对象。

如您需要了解我们的出版物，
请联系：

Publication@llinkslaw.com

2. 《网安管理办法征求意见稿》的适用范围

(一) 适用主体

《网安管理办法征求意见稿》第 2 条规定了《网安管理办法征求意见稿》的适用主体，包括:

- "**核心机构**": 指证券期货交易场所、证券登记结算机构、期货保证金安全存管监控机构等承担证券期货市场公共职能、承担证券期货业信息基础设施运营的机构及其下属机构;
- "**经营机构**": 证券公司、期货公司和基金管理公司等证券期货经营机构;
- "**信息技术服务机构**": 为证券期货业务活动提供重要信息系统的开发、测试、集成、测评、运维及日常安全管理等产品或者服务的机构。

可见，《网安管理办法征求意见稿》在《安全保障办法》的基础上扩大了适用的范围，尤其是将非证监会直接监管的"信息技术服务机构"纳入监管范围，即，除核心机构、经营机构在境内建设、运营、维护和使用网络及信息系统外，信息技术服务机构为证券期货业务提供活动产品或者服务将皆受《网安管理办法征求意见稿》的管辖。

(二) 参照适用

同时，《网安管理办法征求意见稿》第 65 条列明了可根据信息系统网络安全管理的特点所参照适用《网安管理办法征求意见稿》的企业，包括:

- 境内开展证券公司客户交易结算资金第三方存管业务、期货保证金存管业务的商业银行;
- 证券投资咨询机构;
- 基金托管机构和从事基金销售支付、份额登记、估值、评价等基金服务业务的机构;
- 借助信息系统从事证券期货业务活动的经营机构子公司;
- 借助自身运维管理的信息系统从事证券投资活动且存续产品涉及投资者人数合计一千人以上的私募证券投资基金管理人;
- 区域性股权市场运营机构。

(三) 监督检查

《网安管理办法征求意见稿》综合了《安全保障办法》与 2019 年出台的《证券基金经营机构信息技术管理办法》对证监会职权的规定，指出证监会以及其派出机构有权委托专业机构进行技术测试、技术风险评估，以监督、检查核心机构、经营机构和信息技术服务机构，以上机构有义务配合提供证券期货业网络安全管理相关信息和数据。

《网安管理办法征求意见稿》明确和扩大其使用范围: 表明证监会对网络安全的监管不再仅仅是属人的监管，而是对证券期货行业网络安全和信息保护的全方位监管，哪怕信息技术服务机构并非证监会下的被监管主体。这也就意味着，在信息服务外包安排中，证券期货经营机构可能有必要以合同手段要求信息技术服务机构满足证监会对网络安全的监管要求。

3. 内部网络安全治理架构和管理制度

《网安管理办法征求意见稿》就网络安全管理的问题，对证券期货经营企业和信息服务企业提出了治理架构和管理制度方面的要求。

■ 管理体系

《网安管理办法征求意见稿》要求核心机构、经营机构建立的管理体系囊括以下两个方面: (1)网络安全与数据安全管理制度体系，和 (2)信息技术服务机构准入管理机制。

针对内部网络安全管理体系，《网安管理办法征求意见稿》重申了《网络安全法》《数据安全法》等法律对网络运营者、数据处理者的相关要求，包括明确网络安全与数据安全的内部管理、决策、执行、监督、问责机制，依法明确网络安全负责人(包括第一责任人和直接责任人)，配置管理机构、专职技术人员和合理架构的信息系统与基础措施，指定网络安全工作机构，建设数据分类分级管理制度，建立数据权限管理策略，构建数据质量评估框架，每年进行至少一次网络安全教育活动等。核心机构和经营机构处理重要数据、核心数据的，还应当依法明确数据安全负责人，数据安全管理机构或者部门[1]。

以上要求也是对核心机构、经营机构的双重制度建设要求，网络安全管理工作主要保护公司的信息系统安全平稳运行，数据治理管理工作旨在保证机构处理数据的安全性，有效避免不当处理数据(特别是重要数据、核心数据)对国家安全、公共权益、组织和个人权益可能造成的损害。虽两者所保护的法益不尽相同，但对证券期货业机构而言，保障网络安全是数据治理的前提与必要手段。核心机构、经营机构可根据机构内部的治理结构，有机结合并统筹网络安全管理工作和数据治理工作。

针对信息技术服务机构准入管理机制，《安全保障办法》要求核心机构和经营机构建立供应商管理制度，2021 年修订的《证券基金经营机构信息技术管理办法》要求证券基金经营机构在借助信息技术手段前开展内部审查，并与信息技术服务机构就质量考核标准、持续监控机制等内容进行明确约定与持续监督。而《网安管理办法征求意见稿》第 20 条在此基础上，进一步要求，核心机构、经营机构应当将对采购信息技术产品、服务的准入标准、风险管理措施、持续评估机制等机制落实到机构的内部管理机制层面[2]。

[1] 《网安管理办法征求意见稿》第 9、10、11、12、13 条，第 23、24、48 条

[2] 《网安管理办法征求意见稿》第 20 条 信息技术服务机构应当依法向中国证监会备案，并按照有关业务规则为证券期货业务活动提供信息技术产品或者服务。核心机构和经营机构应当建立健全内部管理机制，完善信息技术产品和服务准入标准，审慎采购并持续评估相关产品和服务的质量，加强保密管理，及时改进风险管理措施，健全应急处置机制，保障本机构网络安全和相关业务的安全平稳运行。

可见，对于证券基金经营机构而言，网络安全合规首要的就是建立内部网络安全和数据保护治理架构，而信息技术服务提供商的审核和准入也是治理结构中的重要一环。

■ **技术安全措施**

《网安管理办法征求意见稿》落实、参考了《网络安全法》《数据安全法》《证券投资基金法》《网络数据安全管理条例(征求意见稿)》以及金融行业标准对相关适应主体的技术安全措施要求，包括如下:

- **业务日志、网络日志留存要求**: 留存业务日志保存不得少于二十年，系统日志保存期限不得少于六个月(第 17 条)。
- **备份与有效性验证**: 建立同城和异地数据备份，至少每天备份数据一次，每季度至少对数据备份进行一次有效性验证，建立故障备份设施和灾难备份设施等(第 18 条)。
- **等级保护**: 核心机构、经营机构的处理重要数据的信息系统原则上应当满足三级以上网络安全等级保护要求(第 24 条)。
- **其他技术手段**: 采取网络隔离、用户认证、访问控制、数据加密、病毒防范、非法入侵检测和网络安全态势感知等技术手段(第 25 条)。
- **日常监测**: 建立网络安全风险监测预警机制，加强日常监测，定期开展漏洞扫描、安全评估等工作(第 30 条)。

此外，《网安管理办法征求意见稿》同样对核心机构、经营机构提出了新的技术措施与要求:

- **重要系统变更的风险评估与报告**: 核心机构和经营机构新建上线、运行变更、下线移除重要信息系统的，应当进行风险评估，可能对市场运行产生较大影响时应当提前报告中国证监会及其派出机构(第 15 条)。
- **压力测试**: 核心机构与经营机构每半年至少开展一次重要信息系统压力测试，制定压力测试方案，测试完成后形成压力测试报告存档备查(第 19 条)。

尤其值得注意的是，当核心机构、经营机构的信息系统完成安全等级认定时，应当参照《网络安全等级保护基本要求》《网络安全等级保护安全设计技术要求》等国家标准，满足相应的技术要求和管理要求。

■ **安全事件应对与应急处置措施**

《网安管理办法征求意见稿》第 30 条至第 35 条主要明确了核心机构、经营机构、信息技术服务机构应当如何进行风险监测预警，漏洞扫描和网络安全应急演练，以及网络安全事件发生后的应急处理机制与调查义务。

- 核心机构、经营机构和信息技术服务机构应当对发现的网络安全产品、服务的风险隐患进行及时核实与整改，可能产生较大影响的应当上报中国证监会及其派出机构。(第 30 条)
- 根据业务影响分析建立健全网络安全应急预案。(第 31 条)

- 及时处置网络安全事件，恢复正常运行后，组织内部调查与责任认定，向中国证监会及其派出机构及时报告安全事件以及调查结果(第 33、34 条)，本条的执行可以参考证监会 2021 年 6 月颁布的《证券期货业网络安全事件报告与调查处理办法》。
- 在发生网络安全事件后提示风险，公示应急措施与替代方案，中国证监会及其派出机构有权要求其向投资者履行相应的告知义务(第 35 条)。

值得注意的是，《网安管理办法征求意见稿》第 32 条特别规定，要求核心机构与经营机构开展网络安全应急演练。其中，核心机构与本机构信息系统和网络通信设施相关联主体，**每年最少开展一次网络安全应急演练**，并在完成后的 15 个工作日内报告相关情况至中国证监会。而核心机构与经营机构的应急演练报告均应**存档备查**。

4. 数据的保护

证券期货经营者往往掌握着大量的投资者个人信息，也有可能涉及到大量与金融市场安全有关的重要数据。因此，个人信息和其他数据的安全保护成为《网安管理办法征求意见稿》的重要主题之一。

■ 个人信息保护

《网安管理办法征求意见稿》第 26 条[3]根据《个人信息保护法》对个人信息处理的相关规定重申了核心机构和经营机构对投资者个人信息的保护义务。以上机构处理投资者个人信息的，应当展示个人信息处理规则，获得个人同意，采取有效技术措施以保证个人信息的安全，防止滥用个人信息，在对外提供、公开个人信息、处理敏感个人信息时取得投资者的“单独同意”。

《网安管理办法征求意见稿》也在本条第 2 款列明了处理个人信息获得“个人同意”的法定例外，即为了**法定职责、法定义务或者监管要求所必需时，处理个人信息则不需要获得个人同意。**

核心机构和经营机构在处理投资者的个人信息时，一般可以通过要求投资者签署个人信息处理规则同意书、勾选隐私政策等方式，以获取投资者的知情同意。但在处理敏感个人信息的场景下，以上阅读个人信息处理规则、隐私政策并同意的行为，难以满足“单独同意”的要求，更有可能被认为未能使得投资者清晰了解处理敏感个人信息对个人的权益影响与潜在风险。

[3] 《网安管理办法征求意见稿》第 26 条 核心机构和经营机构应当遵循合法、正当、必要和诚信原则处理投资者个人信息，依法履行投资者个人信息保护义务，包括但不限于下列要求: (一)收集个人信息，应当告知投资者个人信息处理的目的、方式和范围，并取得个人同意; (二)采取必要的安全技术措施存储、传输个人信息，防止个人信息泄露、篡改、丢失; (三)合理确定个人信息使用策略和操作权限，不得滥用个人信息; (四)处理证券期货账户等敏感个人信息、向他人提供或者公开个人信息的，应当取得个人的单独同意。

为履行法定职责、法定义务或者监管要求所必需，核心机构和经营机构可以在未取得个人同意的情况下，处理个人信息。

然而，证券期货业基于监管要求(例如法律规定的客户账户身份识别义务，反洗钱、反恐怖融资，反欺诈，交易留痕等监管要求)，不可避免将处理大量的敏感个人信息(例如生物识别、特定身份、金融账户信息)[4]，且处理敏感个人信息的场景遍及了核心机构与经营机构向投资者提供证券期货服务的全生命周期，实践中如何就所有种类的敏感个人信息、所有处理敏感个人信息的场景均获取“单独同意”的，《网安管理办法征求意见稿》并未给出更具体的指引。

此外，第 26 条第 2 款之“个人同意”的例外，是否可以作为第 26 条第 1 款第(4)项处理敏感个人信息“单独同意”之例外，也亟待实务中的探索与澄清。现阶段而言，除遵守上述法律要求外，证券期货业相关机构处理敏感个人信息的，应当根据《个人信息保护法》的要求明确各处理场景，清晰告知投资者其对个人权益存在的影响与潜在风险，以确保投资者的知情权。

- **重要数据、核心数据治理**

除个人信息保护义务外，核心机构和经营机构如处理重要数据和核心数据的，应当明确数据安全负责人、制定安全管理机构或者部门，对处理重要数据的信息系统原则上应满足三级以上的网络安全等级保护要求，从严保护处理核心数据的信息系统。

虽《数据安全法》要求各部门应当按照数据分类分级保护制度，确定相关行业领域的重要数据具体目录，但目前证监会尚未明确证券期货业的数据分级分类标准。目前，核心机构和经营机构应首先参考概括性定义，根据 2021 年 12 月通过的《网络安全标准实践指南—网络数据分类分级指引》，重要数据为 “一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能危害国家安全、公共利益的数据”，核心数据即“关系国家安全、国民经济命脉、重要民生、重大公共利益等的数据。”

5. 关键信息基础设施网络安全保护要求

目前，如何认定“关键信息基础设施”，仍需依据《关键信息基础设施安全保护条例》内的相关释义，并且取决于相关保护工作部门的认定。本次《网安管理办法征求意见稿》没有在“关键信息基础设施”的释义与认定规则上进一步细化，在《关键信息基础设施安全保护条例》的基础上为运营关键信息基础设施的核心机构和经营机构(以下简称“**关基单位**”)提出了更高的网络安全保护要求，增加新的义务。

	新增义务
关键信息基础设施，是指公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等。	

[4] 敏感个人信息，是一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。

1. 第 37 条	- 将关键信息基础设施安全保护情况纳入网络安全第一责任人、直接责任人和相关人员的责任考核机制。 - 配备至少五名网络安全专职人员，为每个关键信息基础设施指定一名网络安全管理责任人，并明确岗位职责和分工。
2. 第 38 条	- 关基单位对关键信息基础设施实施运行变更或者下线移除，可能产生较大影响的，应当组织多机构专家开展专项评审； - 证券期货业关键信息基础设施停止运营或者发生较大变化，可能影响认定结果的，相关机构应当及时将相关情况报告中国证监会及其派出机构。
3. 第 39 条	关基单位每年网络安全检测和风险评估的内容包括但不限于：关键信息基础设施的运行情况、面临的主要威胁、风险管理情况、应急处置情况等。
4. 第 41 条	对关键信息基础设施的安全运行进行持续监测，定期开展压力测试，确保系统性能容量不低于历史峰值的三倍，网络带宽不得低于历史峰值的两倍。
5. 第 42 条	建设同城和异地灾难备份中心，实现数据同步保存。

6. 证券期货业相关机构的备查和报告义务

《网安管理办法征求意见稿》多处规定了核心机构、经营机构和信息技术服务机构对内部信息系统、网络安全的审查、风险评估义务。除此之外，上述机构同时需将相关事项上报至中国证监会及其派出机构，或存档备查。

进一步地，根据《网安管理办法征求意见稿》第 63 条的规定，在报告相关事项时,核心机构应当向中国证监会报告。经营机构和信息技术服务机构原则上应当向属地中国证监会派出机构报告，中国证监会另有要求的除外。

	报告条件	报告主体	报告对象	报告事项
一. 核心机构、经营机构和信息技术服务机构				
1. 第 14 条	完成网络安全等级保护定级	核心机构和经营机构	中国证监会及其派出机构	及时报告网络安全等级保护定级、变更和日常工作开展情况
2. 第 15 条	新建上线、运行变更、下线移除重要信息系统的，进行风险评估后认为可能对证券期货市场安全平稳运行产生较大影响的	核心机构和经营机构	中国证监会及其派出机构	报告可能对证券期货市场安全平稳运行产生较大影响的情况
3. 第 19 条	每半年开展重要信息系统压力测试后	核心机构和经营机构	中国证监会及其派出机构	测试完成后形成压力测试报告存

				档备查
4. 第 27 条	管理本机构和用户发布信息时，发现违反法律法规和有关监管规定的	核心机构和经营机构、为证券期货业务活动提供产品或者服务的信息技术服务机构	中国证监会及其派出机构	报告相关情况
5. 第 30 条	发现网络安全产品或者服务存在安全缺陷、系统漏洞等风险隐患的，可能对证券期货业网络安全产生较大影响的	核心机构、经营机构和信息技术服务机构	中国证监会及其派出机构	可能对证券期货业网络安全产生较大影响的网络安全产品或者服务
6. 第 32 条	网络安全应急演练后的 15 个工作日内	核心机构	中国证监会	网络安全紧急演练的相关情况
7. 第 32 条	网络安全应急演练后	核心机构和经营机构	中国证监会及其派出机构	形成应急演练报告，存档备查
8. 第 33 条	发生网络安全事件的	核心机构和经营机构	向中国证监会及其派出机构	进行应急报告，不得瞒报、谎报、迟报、漏报。
9. 第 34 条	系统恢复正常运行,完成网络安全事件的责任认定和追究后	核心机构和经营机构	中国证监会及其派出机构	相关调查内容
10. 第 51 条	每年 4 月 30 日前	核心机构和经营机构	中国证监会及其派出机构	完成上一年的网络安全工作的网络安全专项评估并编制的网络安全管理年报(网络安全治理情况、人员情况、投入情况、风险情况、处置情况和下一年度工作计划等)
二. 关基单位				
1. 第 38 条	证券期货业关基设施停止运营或者发生较大变化，可能影响认定结果的	关基单位	中国证监会及其派出机构	关基设施停止运营或者发生较大变化的相关情况

2. 第 40 条	采购网络产品和服务	关基单位	中国证监会及其派出机构	评估网络产品和服务投入使用后可能对关基设施安全保护、金融安全和国家安全带来的风险隐患的风险评估报告
3. 第 51 条	每年 4 月 30 日前	关基单位	中国证监会及其派出机构	完成上一年的网络安全工作的网络安全专项评估并编制的网络安全管理年报(网络安全治理情况、人员情况、投入情况、风险情况、处置情况和下一年度工作计划、关键信息基础设施网络安全检测和风险评估情况)

上述报告将意味着证监会及其派出机构将全面掌握证券经营机构的网络安全状况。同时，考虑到在信息技术服务外包中，信息技术服务机构掌握了部分一手的涉及网络安全和数据保护的信息，因此，满足上述报告义务的要求与条款可能也需要在相关的信息技术服务外包协议中有所体现。

如您希望就相关问题进一步交流，请联系:

杨 迅
+86 21 3135 8799
xun.yang@llinkslaw.com

如您希望就其他问题进一步交流或有其他业务咨询需求，请随时与我们联系: **master@llinkslaw.com**

上海	北京	深圳
上海市银城中路 68 号 时代金融中心 19 楼 T: +86 21 3135 8666 F: +86 21 3135 8600	北京市朝阳区光华东里 8 号 中海广场中楼 30 层 T: +86 10 5081 3888 F: +86 10 5081 3866	深圳市南山区科苑南路 2666 号 中国华润大厦 18 楼 T: +86 755 3391 7666 F: +86 755 3391 7668
香港	伦敦	
香港中环遮打道 18 号 历山大厦 32 楼 3201 室 T: +852 2592 1978 F: +852 2868 0883	1/F, 3 More London Riverside London SE1 2RE T: +44 (0)20 3283 4337 D: +44 (0)20 3283 4323	

www.llinkslaw.com

Wechat: LlinksLaw

本土化资源 国际化视野