证券期货业网络安全事件报告与调查处理办法（征求意见稿）

第一章　总　则

第一条　为了规范证券期货业网络安全事件的报告和调查处理，减少网络安全事件的发生，根据《证券法》、《证券投资基金法》、《证券公司监督管理条例》、《期货交易管理条例》、《证券期货业信息安全保障管理办法》、《证券基金经营机构信息技术管理办法》等法律、行政法规和规章，制定本办法。

第二条　证券期货业网络安全事件是指由于人为原因、软硬件缺陷或故障、自然灾害等，对证券期货业网络和信息系统或者数据造成影响，发生网络和信息系统服务能力异常或者数据损毁、泄露，对国家金融安全、社会秩序、投资者合法权益造成损害的事件。

第三条　证券期货业网络安全保障责任主体发生网络安全事件后，应当按本办法规定进行报告和调查处理。

前款所称责任主体，包括承担证券期货市场公共职能的机构、承担证券期货行业信息技术公共基础设施运营的机构等证券期货市场核心机构及其承担上述公共职能的下属机构（以下简称核心机构），证券公司、期货公司、基金管理公司及其提供证券期货相关服务的下属机构、证券期货服务

机构等证券期货经营机构（以下简称经营机构）。

第四条　核心机构、经营机构发生网络安全事件后，应当及时、准确、完整报告，不得迟报、漏报、谎报或者瞒报。

第五条　网络安全事件调查处理应当坚持实事求是、尊重科学、客观公正、及时稳妥的原则。

第二章　事件分类分级

第六条　根据网络和信息系统发生网络安全事件后，直接对国家金融安全、社会秩序、投资者合法权益造成的损害程度，网络和信息系统由高到低分为五类系统、四类系统、三类系统、二类系统和一类系统。各类系统的分类原则及典型信息系统见《信息系统分类表》和《典型系统》（附件1）。

未列在《典型系统》中的网络和信息系统，如发生网络安全事件，在应急处置和调查处理时，应依据《信息系统分类表》进行分类。

第七条　核心机构和经营机构结算系统等中后台业务系统发生网络安全事件后，按照受其影响的前台业务系统的类别和受影响程度，或按照其导致的投资者数据和结算金额差错、直接资金损失等，进行网络安全事件的分类分级。

第八条　根据服务能力异常程度，信息系统服务能力异常分为严重异常、中度异常、轻度异常。具体如下:

（一）严重异常，是指信息系统发生故障，服务能力异常80%以上的情形;

（二）中度异常，是指信息系统发生故障，服务能力异常 30%以上且未构成严重异常的情形;

（三）轻度异常：是指信息系统发生故障，服务能力异常但未构成严重异常、中度异常的情形。

不同业务类型信息系统服务能力异常的计算方法见《服务能力异常计算方法》(附件 2)。

第九条　综合考虑信息系统分类、服务能力异常、事件持续时间、数据损毁、结算金额差错数额、直接资金损失以及对国家金融安全、社会秩序、投资者合法权益造成损害的程度，网络安全事件分为特别重大事件、重大事件、较大事件、一般事件。

同时符合两类或两类以上分级情形的，应当以孰高原则分级。

第十条　特别重大事件是指对国家金融安全、社会秩序、投资者合法权益造成特别严重损害的网络安全事件。符合下列情形之一的为特别重大事件:

（一）五类系统服务能力严重异常且故障持续时间 30 分钟以上的;

（二）四类系统服务能力严重异常且故障持续时间 2 小时以上的;

（三）100 万人以上的投资者数据发生损毁、泄露或篡改的;

（四）结算金额差错100亿元以上或者给投资者造成直接资金损失10亿元以上的;

（五）其他对国家金融安全、社会秩序、投资者合法权益造成特别严重损害的事件。

第十一条　重大事件是指对国家金融安全、社会秩序、投资者合法权益造成严重损害的网络安全事件。符合下列情形之一，且未达到特别重大事件的为重大事件:

（一）五类信息系统服务能力严重异常且故障持续时间15分钟以上，或服务能力中度异常且故障持续时间30分钟以上的;

（二）四类系统服务能力严重异常且故障持续时间30分钟以上，或者服务能力中度异常且故障持续时间2小时以上的;

（三）三类系统服务能力严重异常且故障持续时间2小时以上的;

（四）10万人以上的投资者数据发生损毁、泄露、篡改的;

（五）结算金额差错10亿元以上或者给投资者造成直接资金损失1亿元以上的;

（六）其他对国家金融安全、社会秩序、投资者合法权益造成严重损害的事件。

第十二条　较大事件是指对国家金融安全、社会秩序、

投资者合法权益造成较大损害的网络安全事件。符合下列情形之一，且未达到重大事件的为较大事件:

（一）五类系统服务能力严重异常且故障持续时间 5 分钟以上，或者服务能力中度异常且故障持续时间 15 分钟以上，或者服务能力轻度异常且故障持续时间 30 分钟以上的;

（二）四类系统服务能力严重异常且故障持续时间 10 分钟以上，或者服务能力中度异常且故障持续时间 30 分钟以上,或者服务能力轻度异常且故障持续时间 2 小时以上的;

（三）三类系统服务能力严重异常且故障持续时间 30 分钟以上，或者服务能力中度异常且故障持续时间 2 小时以上的;

（四）二类系统服务能力严重异常且故障持续时间 2 小时以上的;

（五）1 万人以上的投资者数据发生损毁、泄露、篡改的;

（六）因审核不严或信息系统被非法入侵，相关信息平台直接向 10 万人以上发送不良信息，造成恶劣的社会影响;

（七）结算金额差错达到 1 亿元以上或者给投资者造成直接资金损失达到 1000 万元以上的;

（八）其他对国家金融安全、社会秩序、投资者合法权益造成较大损害的事件。

第十三条　一般事件是指对国家金融安全、社会秩序、

投资者合法权益造成损害的网络安全事件。符合下列情形之一，且未达到较大事件的为一般事件:

（一）一类、二类、三类、四类、五类系统出现服务能力严重异常、中度异常、轻度异常等情形的;

（二）1 万人以下的投资者数据发生损毁、泄露、篡改的;

（三）因审核不严或信息系统被非法入侵，相关信息平台直接向 10 万人以下发送不良信息，造成恶劣的社会影响;

（四）结算金额差错 1 亿元以下或者给投资者造成直接资金损失 1000 万元以下;

（五）其他对国家金融安全、社会秩序、投资者合法权益造成损害的事件。

第十四条　存在明显过错、疏忽且社会影响较大的网络安全事件，可酌情提高事件定级。

第十五条　符合以下情形之一的，未发现明显过错、疏忽且不良影响较小的，可酌情从轻分级，或不认定为网络安全事件:

（一）自主研发的信息系统上线一年内发生网络安全事件的;

（二）基金销售、会计核算、注册登记系统发生网络安全事件后及时修复，未对行业及投资者权益造成影响的;

（三）具有冗余架构的信息系统或基础设施，在合理的

切换时间内不影响系统提供正常服务的;

（四）经营机构面向50名以下投资者提供服务或者网络安全事件发生前一个月日均成交笔数不足50笔的信息系统、分支机构信息系统发生故障，处置得当，受影响客户得到妥善安抚的;

（五）其他未发现明显过错、疏忽且不良影响较小的网络安全事件。

第十六条　本办法所指故障持续时间是指证券期货信息系统生产时段发生故障的持续时间，按照以下方式计算:

（一）网络安全事件发生在连续竞价交易时段时，故障持续时间为实际影响时间计算;

（二）网络安全事件发生在集合竞价、大宗交易等交易时段时，故障持续时间为实际影响时间减半计算。

第十七条　本章所称的“以上”包括本数，所称的“以下”“不足”不包括本数。

第三章　事件报告

第十八条　核心机构和经营机构应当建立网络安全风险监测预警体系，发现风险隐患应当尽快加以核实，采取必要的防范措施，如有重大情况应当及时进行预警报告。

预警报告应当包括：事件基本情况（包括预警发生的时间、地点、经过等），可能造成的影响范围和后果，已采取的防范措施及相关建议、需要有关部门和单位协调处置的有

关事宜。

第十九条　核心机构和经营机构应当建立网络安全应急处置机制，及时处置网络安全事件，尽快恢复信息系统的正常运行，保护事件现场和相关证据，并按照下列要求进行应急报告:

（一）信息系统发生故障，可能构成网络安全事件的，应当立即报告。可能构成特别重大、重大网络安全事件的，应当每隔 30 分钟至少上报一次事件处置情况，直至信息系统恢复正常运行；对较大和一般网络安全事件，第一次上报后，无须持续上报事件处置情况；如有重要情况应当立即报告;

（二）发生涉及犯罪的网络安全事件，应当立即报告。在事件解决前，如有重要情况应当立即报告。

第二十条　核心机构和经营机构进行应急报告时应当先通过电话或事件报送平台进行报告，随后书面报送《网络安全事件情况报告书》（见附件 3），内容包括：事件初步定级、事件发生时间、地点、简要经过、影响范围初步评估、影响程度初步评估、影响人数初步评估、经济损失初步评估、后果初步判断、原因初步判断、事件性质初步判断、已采取的措施及效果、需要有关部门和单位协助处置的有关事宜、报告单位、签发人和报告时间、联系人与联系方式、与本事件有关的其他内容。

第二十一条　核心机构和经营机构应当在网络安全事件应急处置结束、系统恢复正常运行后 5 个工作日内，组织内部调查，准确查清事件经过、原因和损失，查明事件性质，认定并追究事件责任，提出整改措施，并进行事件总结报告。事件总结报告内容应当包括:

（一）事件基本情况，包括事件发生时间、地点、经过、影响范围、影响程度、损失情况等;

（二）应急处置情况，包括事件报告的情况、采取的措施及效果;

（三）事件调查情况，包括事件原因、事件级别、责任认定和结论;

（四）事件处理情况，包括事件暴露出的问题及采取的整改措施，责任追究情况。

暂时无法确定事件原因、责任和结论的，应当提交事件的初步分析报告，同时尽快查找原因，认定并追究事件责任，采取整改措施，并在事件应急处置结束、系统恢复正常运行后 30 个工作日内提交事件补充报告。

第二十二条　核心机构和经营机构接到中国证监会及其派出机构关于系统漏洞、安全隐患、产品缺陷的网络安全通报书后，应当立即核实情况，采取必要的处置措施，并根据要求进行事件总结报告。

事件总结报告内容应当包括：事件基本情况，可能或者

已经造成的影响范围和后果，已采取的防范措施及相关建议。

第二十三条　核心机构或者经营机构应当按照下列规定向有关机构进行报告:

（一）核心机构应当向中国证监会进行预警报告、应急报告和事件总结报告;

（二）核心机构发生网络安全事件影响到其它机构的，应当及时向有关机构进行应急通报;

（三）经营机构应当向住所地中国证监会派出机构进行预警报告、应急报告和事件总结报告，经营机构分支机构应当向所在地中国证监会派出机构进行预警报告、应急报告和事件总结报告。事件总结报告同时抄送中国证券业、期货业或者证券投资基金业协会;

（四）经营机构发生网络安全事件影响到证券期货交易业务时，应当同时向相关证券期货交易场所进行应急报告和事件总结报告；影响到证券登记结算业务时，应当同时向中国证券登记结算公司进行应急报告和事件总结报告；影响到转融通业务时，应当同时向中国证券金融公司进行应急报告和事件总结报告；影响到其他机构的，应当及时向有关机构进行应急通报;

（五）核心机构或者经营机构发生涉及犯罪的网络安全事件，核心机构和经营机构应当向公安机关进行应急报告。

第四章　调查处理

第二十四条　中国证监会及其派出机构依据本办法规定对核心机构、经营机构的网络安全事件进行调查处理。

网络安全事件相关的核心机构、经营机构应当配合中国证监会及其派出机构对事件进行调查和处理。

第二十五条　调查人员有权向网络安全事件相关的核心机构、经营机构和个人了解事件有关的情况，可采取听取报告、询问当事人、调阅文件资料、调阅系统日志、实地核查等工作方式。

在事件调查期间，发生网络安全事件的机构相关人员应当能够接受询问，如实介绍情况，提供证据和所需的文件、资料，并签名确认。

第二十六条　调查人员应当诚信公正，认真履职，遵守工作纪律，做好笔录，严格保守事件调查的秘密，以及在调查过程中了解到的商业秘密、技术秘密。未经允许，不得泄露或者擅自发布事件调查中知悉的有关信息。

第二十七条　中国证监会或者其派出机构督促发生网络安全事件的机构落实整改措施，并对整改措施落实情况进行监督。

发生网络安全事件的机构应当认真吸取事件教训，尽快落实整改措施，消除风险隐患。

第二十八条　中国证监会视情况将网络安全事件有关

情况向全行业通报，中国证监会派出机构视情况向本辖区证券期货经营机构通报。

第二十九条　核心机构、经营机构在研发、测试、上线及运维等系统管理过程中未能严格执行相关法律法规和行业相关技术管理规定、技术规则、技术指引和技术标准，造成网络安全事件的，中国证监会及其派出机构依照有关法律、行政法规和规章，对发生网络安全事件的机构及相关负责人员采取监督管理措施或者实施行政处罚。

第三十条　妨碍网络安全事件报告与调查处理的，中国证监会或者其派出机构依照有关法律、行政法规和规章，对相关机构和责任人员采取监督管理措施或者实施行政处罚。

第三十一条　核心机构、经营机构在研发、测试、上线及运维等系统管理过程中未能严格执行相关法律法规和行业相关技术管理规定、技术规则、技术指引和技术标准，造成网络安全事件，被中国证监会及其派出机构采取监督管理措施或者实施行政处罚的，应当对相关责任人员进行内部责任追究。

第五章　附　则

第三十二条　本办法自 2021 年 1 月 1 日起施行。《证券期货业信息安全事件报告与调查处理办法》（证监会公告〔2012〕46 号）同时废止。

附件 1:

信息系统分类表

	对相应客体的侵害程度		
信息系统发生网络安全事件时侵害的客体	一般损害	严重损害	特别严重损害
投资者合法权益	一类	二类	三类
社会秩序	二类	三类	四类
国家金融安全	三类	四类	五类

典型系统/模块

系统类别	核心机构	经营机构
五类系统	1、证券期货交易场所的集中竞价交易系统、依法应实时公布的行情系统。	无
四类系统	1、除集中竞价交易系统以外的其他实时交易系统。	1、近 20 交易日日均活跃用户数超过 100 万的实时交易系统及相关的行情系统。
三类系统	1、承载生产业务的行业基础通讯系统、大宗交易等业务系统。	1、近 20 交易日日均活跃用户数超过 10 万但不足 100 万的实时交易系统及相关的行情系统； 2、近 20 交易日日均活跃用户数超过 100 万的新股申购、基金销售等非实时交易系统，基金账户数超过 1000 万的基金注册登记结算、资金清算、会计估值核算等系统。
二类系统	1、近 20 交易日日均活跃用户数超过100万的具有账户开立、银证银期转账、信息查看功能等各类非交易业务功能的系统； 2、其他行情系统； 3、官方网站。	1、近 20 交易日日均活跃用户数超过 1000 但不足 10 万的实时交易系统及相关的行情系统； 2、近 20 交易日日均活跃用户数超过 10 万但不足 100 万的新股申购、基金销售等非实时交易系统，基金账户数超过 100 万的基金注册登记结算、资金清算、会计估值核算等系统； 3、近 20 交易日日均活跃用户数超过 100 万的具有账户开立、银证银期转账、信息查看功能等各类非交易业务办理功能的系统。
一类系统	1、近 20 交易日日均活跃用户数不足100万的具有账户开立、银证银期转账、信息查看功能等各类非交易业务功能的系统。	1、近 20 交易日日均活跃用户数不足 1000 的实时交易系统及相关的行情系统； 2、近 20 交易日日均活跃用户数不足 10 万的新股申购、基金销售等非实时交易系统，基金账户数不足 100 万的基金注册登记结算、资金结算、会计估值核算等系统； 3、近 20 交易日日均活跃用户数不足 100 万的具有账户开立、银证银期转账、信息查看功能等各类非交易业务功能的系统； 4、官方网站。

注 1：活跃客户数是指实际访问并使用相关信息系统的客户数量，计算口径以账户数、认证用户数或者 IP 地址数等指标孰高者为准。其中，交易类系统应当计算故障前 15 个交易日和故障后 5 个交易日交易时间实际访问并使用相关信息系统的客户数量，非交易业务办理和信息查看类系统应当计算故障前 15 个交易日和故障后 5 个交易日故障所处时间段实际访问并使用相关信息系统的客户数量。基金账户数计算口径以信息系统中有基金份额的投资者账户合并计算。

注 2：本附件所称的“超过”包括本数，“不足”不包括本数。

附件 2:

服务能力异常计算方法

根据信息系统承载的业务类型，服务能力异常的计算标准如下:

（一）证券期货交易类信息系统服务能力异常比例的计算公式为:（1－故障期间成交笔数×市场交易变动因素/故障前 15 个交易日和故障后 5 个交易日同时间段成交笔数的均值）×100%; 或（1－故障期间正确交易证券期货只数/故障期间应正确交易证券期货只数）×100%。

注 1: 证券或期货经营机构“市场交易变动因素”的计算公式为: 故障前 15 个交易日和故障后 5 个交易日故障同期证券或期货交易场所成交笔数均值/故障期间证券或期货交易场所成交笔数。

注 2: 部分证券或期货交易场所发生故障，发生故障的证券或期货交易场所“市场交易变动因素”的计算公式为: 故障期间其他证券或期货交易场所成交笔数的均值/故障前 15 个交易日和故障后 5 个交易日其他证券或期货交易场所故障同期成交笔数均值。

注 3: 全部证券或期货交易场所发生故障，发生故障的证券或期货交易场所“市场交易变动因素”的计算公式为: 故障期间全部证券或期货交易场所成交笔数历史峰值的均值/故障前 15 个交易日和故障后 5 个交易日全部证券或期货

交易场所故障同期成交笔数的均值。

注 4：应急处置时预估事件级别，可用“故障前 15 个交易日同时间段成交笔数的均值”替代“故障前 15 个交易日和故障后 5 个交易日同时间段成交笔数的均值”。

（二）证券交易场所交易基金销售类信息系统证券交易时段服务能力异常比例的计算公式为：（1－故障期间基金销售份额×市场交易变动因素/故障前 15 个交易日和故障后 5 个交易日同时间段基金销售份额的均值）×100%。

注 1：“市场交易变动因素”的计算公式为：故障前 15 个交易日和故障后 5 个交易日故障同期全市场基金销售份额均值/故障期间全市场基金销售份额。

注 2：应急处置时预估事件级别，可用“故障前 15 个交易日同时间段基金销售份额的均值”替代“故障前 15 个交易日和故障后 5 个交易日同时间段基金销售份额的均值”。

（三）基金销售、会计核算或者注册登记系统服务能力异常比例的计算公式为：如果影响投资者当日或者后续交易日基金正常申购赎回为 100%，否则为 0。

（四）行情计算发布类信息系统服务能力异常比例的计算公式为：（1－故障期间正确发布行情品种数量/故障期间应正确发布行情品种数量）×100%。

（五）开户类信息系统服务能力异常比例的计算公式为：（1－故障期间开户数量×市场开户变动因素/故障前 15

个交易日和故障后 5 个交易日同时间段开户数的均值）×100%。

注 1：证券期货经营机构“市场开户变动因素”的计算公式为：故障前 15 个交易日和故障后 5 个交易日故障同期证券期货交易场所开户数量均值/故障期间证券期货交易场所开户数量。

注 2：证券期货交易场所“市场开户变动因素”的计算公式为：故障前 15 个交易日和故障后 5 个交易日故障同期开户笔数均值/历史峰值开户笔数。

注 3：应急处置时预估事件级别，可用“故障前 15 个交易日同时间段开户数量的均值”替代“故障前 15 个交易日和故障后 5 个交易日同时间段开户数的均值”。

（六）网站类信息系统服务能力异常比例的计算公式为：（1－故障期间首页可访问的栏目数/首页所有的栏目数）×100%。

（七）行业基础通信系统服务能力异常比例的计算公式为：（1－故障期间仍能通信的机构数/接入机构总数）。

（八）其他信息系统服务能力异常比例的计算公式按照实际提供的服务类型比照计算。

附件 3:

网络安全事件情况报告书

报告时间:　　年　　月　　日　　时　　分　　第　　次

单位名称		报告人	
联系电话		传　真	
签发人		联系方式（含手机）	
事件初步定级	一般□　　较大□　　重大□　　特别重大□		
事件发生时间、地点			
事件简要经过			
事件影响范围、影响程度、影响人数、直接资金损失情况			
事件导致的后果、发生原因和事件性质判断			
已采取的措施及效果			
需要有关部门和单位协助处置的有关事宜			
备注			

注：单位名称处需加盖公章或者由机构信息技术负责人签字。