证券期货业网络安全事件
报告与调查处理办法

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，包括证券期货交易场所、证券登记结算机构等承担证券期货市场公共职能、承担证券期货业信息技术公共基础设施运营的证券期货市场核心机构及其承担上述相关职能的下属机构（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 系统分类与事件分级

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系统见《网络和信息系统分类表》和《典型系统》（见附件 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《网络和信息系统分类表》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，网络和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，是指网络和信息系统发生故障，服务能力异常 80%以上的情形;

（二）中度异常，是指网络和信息系统发生故障，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，是指网络和信息系统发生故障，服务能力异常但未构成严重异常、中度异常的情形。

不同业务类型网络和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》（见附件 2）。

第九条 综合考虑网络和信息系统类别、服务能力异常程度、事件持续时间、数据损毁程度、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100亿元人民币以上，或者给投资者造成直接资金损失10亿元人民币以上的；

（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）五类系统服务能力严重异常且故障持续时间15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10亿元人民币以上，或者给投资

者造成直接资金损失1亿元人民币以上的;

（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）因审核不严或系统被非法入侵，相关信息平台发送违法和不良信息造成恶劣的社会影响或者直接向10万人以上发送相关信息的;

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

（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）因审核不严或网络和信息系统被非法入侵，相关信息平台发送违法和不良信息造成社会影响的;

（四）结算金额差错 1 亿元人民币以下且未能及时完成差错处理，或者给投资者造成直接资金损失 1000 万元人民币以下;

（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，中国证监会及其派出机构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）具有冗余架构的系统或基础设施，在合理的切换时间内完成切换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20个交易日日均成交笔数不足50笔的系统、分支机构系统发生故障，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

第十七条 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。

第十八条 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）网络和信息系统发生故障，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。

第十九条 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 7 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。

第二十一条 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。

第二十二条 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；事件总结报告应当抄送中国证券业协会、中国期货业协会或者中国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，应当向中国证券登记结算有限责任公司进行应急报告和事件总结报告；影响到转融通业务时，应当向中国证券金融股份有限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

第二十三条　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和发生事件的机构对事件进行调查和处理。

第二十四条　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积极配合接受询问，如实介绍情况，提供证据和所需的文件、资料，并签名确认。

第二十五条　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。

第二十六条　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。

第二十七条 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。

第二十八条 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，对事件相关机构及其负责人员采取监督管理措施或者实施行政处罚。事件相关机构应当对相关责任人员进行内部责任追究。

第二十九条 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，对相关机构和负责人员采取监督管理措施或者实施行政处罚。

第五章 附 则

第三十条 本办法自公布之日起施行。《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。