金融行业需要关注《网络安全法》的6个要点

金融技术部 俞琛

关键词：网络安全法 金融机构 互联网金融

摘要：《网络安全法》正式出台，对于加强互联网和网络安全方面的法律约束具有重要意义，对金融机构提出新的网络安全工作思路和要求，起到推进作用。

本文梳理的关注点分布在工作依据、工作原则、网络运行、个人信息、监测与预警、内部审计 6 个方面，期许通过完善和加强这些方面的管理机制和技术防护措施，从而整体提升金融行业网络安全防护水平。

《中华人民共和国网络安全法》（以下简称《网安法》）规定了网络安全等级保护、关键信息基础设施安全保护、网络安全监测预警和信息通报、用户信息保护、网络信息安全投诉举报等制度，以及网络安全事件应急预案 / 处置、漏洞等网络安全信息发布、网络安全人员背景审查和从业禁止、网络安全教育和培训、数据留存和协助执法等制度。本文根据《网安法》的要求，对金融机构在网络安全方面需要关注的内容进行梳理。

【关注点一】金融机构需根据网络安全等级保护制度的要求履行安全保护义务

【法律要求】原文第二十一条提到“国家实行网络安全等级保护制度。”原文第三十四条提到“关键信息基础设施的运营者安全保护义务……”。第三十八条提到“关键信息基础设施的运营者应当自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行一次检测评估……”。

【专家解读】《网安法》新提出“网络安全等级保护制度”和“关键信息基础设施的运营者”、“网络运营者”这些概念。《网安法》未对“网络安全等级保护制度”做进一步规定，既未解释该制度的内涵、也没有说明该制度将如何实施，以及“网络安全等级”具体如何划分和确定。建议银行业金融机构进一步关注未来中央网信办和银监会具体如何划分和确定网络安全等级保护制度的文件和通知要求。

根据银监办发 [2016]107 号《中国银监会办公厅关于开展银行业网络安全风险专项评估治理及配合做好关键信息基础设施网络安全检查工作的通知》（以下简称“107 号通知”）通知指出，银行业网络和重要信息系统是国家关键信息基础设施。因此，明确银行业金融机构是关键信息基础设施的运营者，证券、基金、保险行业，以及互联网金融行业暂未明确是否属于国家关键信息基础设施，需按照网络运营者要求执行。

《网安法》对关键信息基础设施的运营者要求一系列安全保护义务，如监测记录网络运行状态并留存相关的网络日志不少于六个月，又如对其网络的安全性和可能存在的风险每年至少进行一次检测评估，相较于人民银行发布《金融行业信息系统信息安全等级保护实施指引》【JR/T 0071—2012】要求，延长了日志保存时限，提高了风险评估频率。对于银行业金融机构，该法要求应设置专门安全管理机构和安全管理负责人并进行安全背景审查等，明确受到治安管理处罚或刑事处罚的人员信息安全关键岗位的从业禁止，要求所有金融机构必须加强对人员背景的调查，建议编写明确的岗位说明书，尤其是信息安全岗位的人员，人员招募时采取人力背景调查问卷、第三方机构背调等方式进行安全背景调查。

【关注点二】银行业网络和重要信息系统建设需遵循“三同步原则”

【法律要求】第三十三条提到“建设关键信息基础设施应当确保其具有支持业务稳定、持续运行的性能，并保证安全技术措施同步规划、同步建设、同步使用。”

【专家解读】《网安法》明确建设关键信息基础设施必须同时开展信息安全保障工作。这个要求符合目前信息安全实践趋势，如重要信息系统在立项之前，从概念阶段伊始信息安全工作就已经介入，在项目立项、安全需求、安全设计、安全开发、安全测试，直至系统上线验收全生命周期的保障。

对于安全技术措施遵循“三同步原则”的好处是立项目标与安全需求定义相匹配，系统功能实现和系统安全流程设计相匹配，如某信息系统立项定位是重要信息系统，关注系统交易过程数据安全，安全需求定义认为登录密码与交易（支付）密码的保护等级不同，功能实现中设定登录密码重置可通过验证手机短消息方式，但交易（支付）密码重置必须到现场柜台，从而避免因功能实现变更引起的返工和开发延期，降低安全风险，提高效率，减少系统开发成本。

【关注点三】金融机构需制定网络安全事件应急预案，并定期组织演练

【法律要求】第二十五条提到“网络运营者应当制定网络安全事件应急预案”。第五十三条提到“制定网络安全事件应急预案，并定期组织演练工作分工和工作要求”。

【专家解读】《网安法》新提出网络安全事件应急预案及演练的相关要求，金融机构制定应急预案应覆盖所有网络安全场景，包括网络扫描攻击、拒绝服务攻击等，系统方面有恶意代码、后门程序等；另外，根据应急预案涉及的各方面内容，建议由负责应急预案工作的部门组织预案中各角色相关人员开展应急预案培训。

107 号通知指出，银行业网络和重要信息系统是国家关键信息

基础设施，为进一步加强互联网安全风险应对，提升银行业整体防护能力，按照国家关键信息基础设施保护、网络安全风险专项应对工作的整体安排，决定组织开展银行业网络安全风险专项评估治理工作。建议银行业金融机构可根据中国银监会《银行业突发事件应急预案》等相关规章和标准，结合近年银行业发生的安全事件和面临的安全风险，制定符合自身组织架构的网络安全应急预案，预案中明确科技部内部及业务部门的应急响应责任，准备措施以及应对突发事件的配合机制，并组织演练。

【关注点四】金融机构需建立健全网络安全监测预警和信息通报制度

【法律要求】第二十九条提到“国家支持网络运营者之间在网络安全信息收集、分析、通报和应急处置等方面进行合作，提高网络运营者的安全保障能力。”

第五十一条提到“国家建立网络安全监测预警和信息通报制度。”第五十二条提到“负责关键信息基础设施安全保护工作的部门，应当建立健全本行业、本领域的网络安全监测预警和信息通报制度，并按照规定报送网络安全监测预警信息。”

【专家解读】《网安法》提出在网络安全信息的合作、分享，提高保障能力的思路，这与当下行业内部少部分事前心存侥幸、发生信息安全事件后企图瞒报、少报的应对思路形成鲜明对比。

绿盟科技高级副总裁叶晓虎指出“现阶段的企业在安全防护工作中已经能够切实感觉到整个生态链的影响，而单个企业的数据总是不够完整，希望能够与更多产业链伙伴进行信息通道的打通和数据的交换，以保障更快地进行安全响应。”建议采取与合作伙伴或供应商签署保密协议，保证网络日志、安全告警信息不向社会公开的前提下，可以自建或招募一些通过背景审查的安全人员形成安全团队，对同一行业、同一领域的金融机构租用一套行业公有云监测预警平台，解决缺少 7*24 小时值守人员、缺乏高效运营监管工具的问题，快速高效的提升防护水平。如采用网站安全监测和预警平台解决，可以协同运营，降低成本。

【关注点五】金融机构需采取措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失

【法律要求】第四十二条　网络运营者不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

【专家解读】《网安法》对网络运营者进行个人信息收集、存储、处理、使用和转让等各环节都作出明确规定，突出强调了信息收集者的责任。对于个人信息收集或使用环节应以明确、易懂和合理的方式如实公示其收集或使用个人信息的目的、个人信息的收集和使用范围、个人信息安全保护措施等信息，接受公共监督。《网安法》的一大亮点就是赋予个人在一定条件下要求删除和更正其个人信息的权利。目前，中央网信办正制定个人信息收集规范标准，将更好地保护

个人信息。

互联网金融行业做好自有信息系统的前台和后台数据访问控制，采取合理、有效措施，如业务流程评估、账号和权限管理、数据库审计等，降低个人信息泄露、毁损、丢失风险。建议系统设计开发阶段考虑账号权限分配和访问控制设定功能，避免因内部工作人员因职权便利，违规查询或批量下载客户个人信息和交易记录。运行阶段，制定数据使用、获取、存储规范，对内部工作人员的行为进行制度约束，开展技术渗透测试评估，避免功能实现上存在平行提权、拖库缺陷。

【关注点六】金融机构需开展内部审计，确保网案法贯彻实施

【法律要求】原文第六章法律责任相关要求

【专家解读】《网安法》在第六章“法律责任”中提高了违法行为的处罚标准，加大了处罚力度，有利于保障《网络安全法》的实施。为了避免被罚，蒙受经济损失和名誉损失，金融机构需建立内部审计机制并开展内审工作。金融机构需明确制定内部审计检查方法、标准、检查项，开展内审验证措施有效性，如定期审计信息系统使用过程中是否存在内部人员违规数据获取行为，验证控制措施效果。

【结语】

《网络安全法》正式出台，对于加强互联网和网络安全方面的法律约束具有重要意义，对金融机构提出新的网络安全工作思路和要求，起到推进作用。

本文梳理的关注点分布在工作依据、工作原则、网络运行、个人信息、监测与预警、内部审计 6 个方面，归纳如下：

- 根据网络安全等级保护制度的要求履行安全保护义务
- 网络和重要信息系统建设需遵循“三同步原则”
- 制定网络安全事件应急预案，并定期组织演练
- 建立健全网络安全监测预警和信息通报制度
- 采取措施防止信息泄露、毁损、丢失
- 开展内部审计，确保网案法贯彻实施

综上，期许通过完善和加强这些方面的管理机制和技术防护措施，从而整体提升金融行业网络安全防护水平。

参考文献：

中共中央网络安全和信息化领导小组办公室 http://www.cac.gov.cn/

西安交通大学法学院、公安部第三研究所 黄道丽 .《关键信息基础设施安全保护办法》亟待制定 . 保密科学技术 .2016（07）