2024.3.1

中国风险消息<2024 No.4>

中国“信息安全等级保护”制度介绍及敝公司经验分享

【要点】
- ◆ 介绍“信息安全等级保护”的基本概念、发展历程、实施流程、安全要求和相关处罚案例。
- ◆ 结合实施等级保护的各个步骤，介绍敝公司的实际经验。
- ◆ 根据敝公司的实施案例，从实际操作的角度出发，说明实施过程中的重点。

1. “信息安全等级保护”制度的概况

(1)基本概念

信息安全等级保护制度（以下简称“等级保护”），是指对国家保密信息及公民、法人和其他组织的专有信息以及公开信息和存储、传输、处理这些信息的信息系统分等级实行安全保护，对信息系统中使用的信息安全产品按等级实行管理，对信息系统中发生的信息安全事件分等级响应、处置。

(2)发展历程

根据重要政策颁布的时间节点，列出大致的发展经历，如表 1 所示。从 2016 年网络安全法颁布后，政府部门对于等级保护的检查监督力度大大增加，而且处罚时也有法可依。

表 1 重要政策的颁布（等级保护）

1994 年 第一次提出等级保护	《中华人民共和国计算机信息系统安全保护条例》中，第一次提出了“计算机信息系统实行安全等级保护”概念。
1999 年 发布等级保护标准	《计算机信息系统安全保护等级划分准则 GB 17859-1999》，制定了等级划分原则和标准，并规定了安全保护的技术措施和管理措施。
2007 年 等级保护管理办法发布	《信息安全等级保护管理办法》中，规定了等级保护实施的具体方案和管理机构，明确了政府和企业的责任及义务。
2016 年 等级保护成为法律	制定了《网络安全法》，通过法律的形式，加强对信息基础设施的保护，确保网络空间安全和信息安全。
2019 年 等级保护 2.0 标准发布	扩大对象范围，将云计算、物联网等列入标准，统一“基本要求、设计要求和测评要求”分类框架。

(3)定级要素

等级保护对象的级别由两个定级要素决定：①受侵害的客体对象 ②对客体的侵害程度。具体内容请参考表 2。

表 2 定级要素

侵害程度 / 受侵害的客体对象	一般损害	严重损害	特别严重损害
公民/法人/其他组织的合法权益	一级	二级	二级
社会秩序/公共利益	二级	三级	四级
国家安全	三级	四级	五级

出处：GB/T 22240-2020 信息安全技术 网络安全等级保护定级指南

对于侵害程度的等级，标准中并没有给出具体的数字要求，企业难以准确判断自身的等级。在实际定级时，可以参考表 3 的案例。除了金融和基础设施行业之外，一般企业在定级时，二级和三级最为常见。

表 3 等级保护的判断标准

等级	保护程度	测评次数	案例
一级	自主保护级	不需外部测评	小型私营、个体企业、中小学，乡镇所属信息系统、县级单位中一般的信息系统。
二级	指导保护级	建议 2 年 1 次	于县级其他单位中的重要信息系统;地市级以上国家机关、企事业单位内部一般的信息系统（公开网站）
三级	监督保护级	每年至少 1 次	地市级以上国家机关、企业、医院、大学内部重要的信息系统、有大量（10 万以上）会员信息的平台等。
四级	强制保护级	半年 1 次	电力、电信、广电、铁路、民航、银行、税务等重要系统
五级	专控保护级	依据需求自查	军工、重要科研领域等极其重要的信息系统

出处：GB 17859-1999 计算机信息系统 安全保护等级划分准则

(4)实施流程

根据实施主体和对象，GB 标准中将等级保护的实施流程分为 5 个步骤，具体请参考表 4。

表 4 等级保护的实施流程

步骤	名称	内容
1	定级	自主确定信息系统的安全保护等级，并请专家、主管部门评审。
2	备案	二级（含）以上信息系统到公安机关备案，公安机关对备案材料和定级准确性进行审核，审核合格后颁发备案证明。
3	建设	根据安全保护等级，按照国家标准开展安全建设整改，建设安全设施、落实安全技术措施、建立和落实安全管理制度。
4	测评	选择符合国家要求的测评机构开展等级测评，分成初测和复测，共 2 次。
5	检查	公安机关对二级信息系统进行指导，对三、四级信息系统定期开展监督、检查。

出处：GB/T 25058-2019 信息安全技术 网络安全等级保护实施指南

(5)安全要求

等级保护的安全要求分为技术和管理 2 个部分，随着等级上升，每一级的项目内容更多，各种要求更加严格。表 5 中列举了一级~三级的要求。

表 5 安全要求（技术方面、管理方面）

大分类	中分类	小分类
技术要求	安全管理中心	系统管理、审计管理、安全管理、集中管控
	安全计算环境	身份鉴别、访问控制、安全审计、恶意代码防范、可信验证、数据完整性、入侵防范、数据备份恢复、剩余信息保护、个人信息保护、数据保密性
	安全区域边界	边界防护、访问控制、入侵防范、可信验证、恶意代码和垃圾邮件防范、安全审计
	安全通信网络	网络架构、通信传输、可信验证
	安全物理环境	物理位置选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防火防潮、防静电、温湿度控制、电力供应、电磁防护
管理要求	安全管理制度	安全策略、管理制度、制定和发布、评审和修订
	安全管理机构	岗位设置、人员配备、授权和审批、沟通和合作、审查和检查
	安全管理人员	人员录用、人员离岗、安全意识教育和培训、外部人员访问管理
	安全建设管理	定级和备案、安全方案设计、产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统交付、等级测评、服务供应商选择
	安全运维管理	环境管理、资产管理、介质管理、设备维护管理、漏洞和风险管理、网络和系统安全管理、恶意代码防范管理、配置管理、密码管理、备份和恢复管理、变更管理、安全事件处置、应急预案管理、外包运维管理

出处：GB/T 28448-2019 信息安全技术 网络安全等级保护测评要求

(6)处罚案例

从《网络安全法》实施开始，各地公安机关定期检查各企业的信息系统，并实施警告、罚款等措施，如表 6 所示。

表 6 基于网络安全法的处罚案例

案例 1	2022 年 7 月，广州警方发现，广州某教育科技有限公司使用的“某在线 1 对 1 系统”确定为第二级信息系统，且在 2021 年 7 月到公安机关进行了等级保护备案。但该系统上线运行前后，该公司一直未按规定对系统的安全等级状况开展等级保护测评，未充分落实等级保护制度。根据《广东省计算机信息系统安全保护条例》第四十条第一款第（二）项之规定，广州警方对该公司作出行政处罚，并责令其限期改正。
案例 2	2023 年 3 月，北京市公安局发现，北京市某企业管理集团有限公司使用的 OA 系统被攻击入侵。经查，该公司未履行网络安全保护义务，未采取防范网络攻击、网络入侵等危害网络安全行为的技术措施，未留存网络日志，导致公司 OA 系统被黑客入侵并篡改。根据《中华人民共和国网络安全法》第二十一条第二项、第三项、第五十九条第一款之规定，北京警方给予该企业警告并处罚款五万元，网络安全主管人员罚款五千元，责令限期改正。

2.敝公司获得证书的经验报告（等级保护 2 级）

下面是敝公司从认识到实施等级保护的必要性，到取得等级保护 2 级证书为止的经验报告。按照时间节点，划分成 4 个阶段，说明每个阶段需要实施的措施、是否需要外部公司的协助以及产生的大致费用等内容。

＜STEP1＞ 准备阶段

实施事项	根据自己公司系统的特征，自主定级，向公安局备案。
实施主体	仅需要自己公司处理
外包成本	0
所需时间	1 个月
具体措施	说明
①根据公司信息系统的特征，自主评定等级（1 级）	敝公司内部使用的系统主要有财务系统、文件服务器、OA 系统、邮件系统和公司网站。除了公司网站之外，都属于内部系统。公司网站虽然对外公开，但没有互动功能（论坛及网络交易功能等），没有用户数据。因此当时认为是“1 级”，不需要有资质的测评公司进行强制测评（后面得知是判断错误）。
②受到公安局的检查修改了定级（1 级⇒2 级）	不久之后，敝公司收到了公安局的通知，要求参加网络安全学习会。公安局指出，公司网站可能被黑客篡改，万一登载违反国家法律或政策的内容，将会损害公众及国家利益，因此不管网站内容是什么，都应该列入二级范围内，需要进行定级备案，实施等级保护测评。会议结束后，公安局网络安全部门（以下简称“网安”）向参加学习会的各家公司开具了网络安全监督检查通知书和限期整改通知书。
③决定尽量独立实施等级保护	向外部咨询公司询问后，得知以下信息。 ・必须聘请有资质的测评公司才能进行等级保护测评。 ・测评费用按照级别和系统复杂程度来区分，一般二级是 RMB 4~8 万元。 ・在后续整改时，还需要另行购买网络防火墙等安全产品，整体费用可能超过 RMB 20 万元。 ・向测评公司电话咨询，对方建议由于测评中专业内容很多，最好再委托一家专业的软件服务商来协助实施。敝公司出于增加网络安全经验和成本考虑，决定自行实施。（最后判断难以独立完成）
④填写资料，向公安局申请备案	敝公司根据网安的要求，填写了二级所需的《信息系统安全等级保护备案表》和《信息系统安全等级保护定级报告》。由于没有掌握资料填写的详细要求，敝公司反复多次修改资料的用词和文件格式，且网安的审核人员较少，提交时间仅有上午和下午各 2 个小时，因此花费了较多的时间。在提交备案资料的 2 周后，敝公司收到了备案号码，可以正式与测评公司签订合同了。

＜STEP2＞ 测评阶段

实施事项	测评公司实施测评。
实施主体	・敝公司 ・有资质的测评公司（←必须委托） ※建议委托软件服务商会更加顺利。（敝公司当时独立实施）
外包成本	约 RMB 2 万元（←测评公司的必要测评费用）
所需时间	测评后约 2 周，得到测评报告 ※测评 1 天可以完成

具体措施	说明
测评标准	由于敝公司的网站内容简单，没有论坛及网络交易等互动内容，因此测评公司 1 天完成了整体的测评（2 名测评师，各自测评技术和管理方面）。测评属于扣分制，二级合格分是满分 100 分中的 70 分。如果分数不足 70 分，需要整改后再进行复测。而且不符合项根据优先权重，设定为高中低 3 级，高风险属于“一票否决”，即只要有 1 个高风险的不符合项，即使分数是 70 分以上，也无法通过。
测评要求 （技术方面）	技术要求按照 GB 国家标准实施，项目达到 130 个左右。每一项都需要展示具体的证明，例如网站服务器的远程登陆密码需要达到强密码要求，即 8 位以上，包含大写字母、小写字母、数字和符号等，最长有效期是 90 天。如果网站中使用到数据库，还需要确认专门的项目。例如数据库的日志备份和审计、数据库的备份和恢复、数据库的密码设定等。 敝公司的网站是存放在外部专业公司的云服务器上，因此在检测机房硬件项目中，还需要提供对方的等级保护证书。 除此之外，公司内部登陆远程服务器的办公 PC 也需要采取相应的安全措施，例如密码设定、权限分离、日志记录、防病毒等。最后，还需要对网站进行漏洞扫描。
测评要求 （管理方面）	管理要求按照国家标准实施，每一项还需要有相应的记录文档来证明。例如设置安全管理部门的职能、岗位设置、文件审批和发布管理，信息系统的安全设计要求、软件开发管理、系统交付验收等相关的资料等。没有相应的经验的话，普通公司难以制定符合要求的全面管理制度。敝公司在管理方面的不符合项达到了 60 项左右。
测评结果	测评结束后 1 周左右，敝公司收到了结果报告，技术和管理 2 方面一共有 80 个左右的不符合项。但在报告中，仅列出问题内容，并没有详细的整改措施。因此敝公司难以判断整改所需的人力和资金成本，感觉到还是需要软件服务商的协助。

＜STEP3＞ 整改阶段

实施事项	整改测评中的不符合项。
实施主体	・敝公司 ・软件服务商（←敝公司感到难以独立完成，需要外部协助）
外包成本	・约 RMB 7 万元（购买安全产品） ・约 RMB 5 万元（委托软件服务商的费用，包含 STEP4 的复测）
所需时间	约 2 个月
具体措施	说明
委托软件服务商	此时，敝公司选择了一家咨询公司来提供协助。通过咨询公司，我们得以明确哪些项目（不符合项）可以整改，以及需要采取何种程度的措施。而且敝公司还发现，在硬件和软件整改时，使用咨询公司的服务器和安全产品也很方便。
整改	通过与软件服务商的多次协商后，根据结果报告的不符合项，共同确定了需要整改的技术和管理项目。根据二级要求，需要整改所有的高风险项以及总分数在 70 分以上，并不是所有的整改项都需要改正。因此，敝公司选择了所有的高风险项和部分中风险项，而低风险项中选择容易整改且扣分较高的项目。

	实施技术方面的整改项目，例如 HTTPS 的强制跳转、备份网站数据和日志、配置不同权限的账户实施权限分离、强密码的设定、云防火墙、web 应用防火墙、安全审计、安全监控等。 由于需要购买安全产品，支付了约 RMB 7 万元的成本。管理方面的整改项目参考软件服务商提供的制度模板修改制定了自己的软件制度。
预约复测	为了避免复测时出现新的不符合项，建议预约与初期测评时相同的测评师。由于评测公司的日程非常紧张，因此敝公司在计算整改时间后，提前 1 个月预约了复测的时间。

＜STEP4＞ 复测阶段

实施事项	通过测评公司复测，获得证书。
实施主体	・敝公司 ・有资质的测评公司（←必须委托） ・软件服务商（从 STEP3 开始，继续协助）
外包成本	约 RMB 2 万元（←测评公司的必要测评费用）
所需时间	约 2 个月 ※复测花费 1 天
具体措施	说明
复测要求	从复测要求上来看，与初期测评的要求完全一样。测评师会以不符合项为中心开始确认（当情况变化较大时，例如迁移网站等，也会将所有项目重新测评一遍）。复测不合格时，可以在复测后再整改不符合项，以达到及格分数以上。由于最终测评报告提交给网安后，对方也会根据最新要求进行微调，因此需要比合格分数提高几分才能保证通过。
复测项目	复测中，测评师会提出各种问题，敝公司回答时以自己人员为主，也请同时出席的软件服务商进行协助回答。软件服务商通常与评测师比较熟悉，沟通方面会更加顺畅。 在技术方面，测评师会针对整改项目，逐一确认系统设置，需要频繁登陆网站服务器、防火墙平台等系统。为了不影响日常办公和加快检查，敝公司选择了 1 台笔记本 PC 作为专用终端，提前进行相关的安全设置，仅保存等级保护相关的文件。 在管理方面，仅有软件制度还不行，还必须提供记录、表格等细节资料作为实施的证据。敝公司已经提前将各种记录、检查表等资料打印并填写，同时这些资料的时间都要求至少在 1 年内，否则仍然会被认为是不符合项。 测评结束后，测评师会总结不符合项，这时可以向其询问大致的分数，判断是否需要继续整改。
复测结果	在复测结束后 1 周，敝公司收到了结果报告，分数为 81 分。这时，可以对报告提出修正，但合格分以上的分数高低不会影响获得等级保护的证书。 网安收到测评公司的最终测评报告后，再经过约 1 个月，就可以领取等级保护的证书了。

3.从操作者角度提出实施等级保护的重点

在本章中，敝公司通过获得等级保护 2 级证书的经验，整理企业在推进等级保护中需要注意的重点。

(1)确定首要目标

实施等级保护的过程中，不少企业认为可以“提升网络安全水平”“整合现有系统”。由于实施等级保护时，如果要求同时满足多个目的，可能会导致要解决的问题复杂化，并可能增加获得证书的难度。因此，建议专注于“通过等级保护测评”工作。

(2)综合考虑所有信息系统

企业需要按照国家标准，针对信息系统的等级，进行单独测评。可以说，作为实施等级保护的第一步，有必要对企业使用的所有信息系统进行筛选，实施自主定级。万一遗漏了需要测评的信息系统，尽管采取了等级保护措施，但无法获得该系统的等级保护证书，因此必须慎重考虑。

(3)使用软件服务商

敝公司最初实施等级保护中，面临着“不知道如何改进不符合项（应采取何种程度的措施才能通过测评）”的问题。如果盲目地采取整改措施，可能花费更多的时间和成本，消耗的资源也会超过所需要的。因此，在初次实施等级保护时，希望尽早使用经验丰富的软件服务商。当然，不同的软件服务商需要不同的委托费用（也会包含整改所需的安全产品购买费用），有必须要提前确认多家公司的提案内容。

(4)扩大可以自主实施的范围

等级保护测评首次通过并不代表合规方面一劳永逸。二级系统要求每 2 年测评 1 次（测评要求与首次相同）。因此企业如果将所有的工作都交予软件服务商的话，外包成本就会成为长期的固定费用。为了回避这种情况，让自身员工一同参与，通过积累实施等级保护测评的知识，在第二次及之后的实施中，可以扩大自主实施的范围，这一点非常重要，可以最大限度地降低与外包相关的成本。

执笔：瑛得管理咨询（上海）有限公司 高级经理 张若亭

参考资料:

- 《信息安全等级保护管理办法》 https://www.gov.cn/gzdt/2007-07/24/content_694380.htm
- 标准清单:

GB/T 22240-2020	信息安全技术　网络安全等级保护定级指南
GB/T 25058-2019	信息安全技术　网络安全等级保护实施指南
GB/T 25070-2019	信息安全技术　网络安全等级保护安全设计技术要求
GB/T 22239-2019	信息安全技术　网络安全等级保护基本要求
GB/T 28448-2019	信息安全技术　网络安全等级保护测评要求
GB/T 28449-2018	信息安全技术　网络安全等级保护测评过程指南
GB/T 36958-2018	信息安全技术　网络安全等级保护安全管理中心技术要求
GB/T 36959-2018	信息安全技术　网络安全等级保护测评机构能力要求和评估规范
GB/T 36627-2018	信息安全技术　网络安全等级保护测试评估技术指南
GB　17859-1999	计算机信息系统　安全保护等级划分准则

- 测评公司目录：网络安全等级保护网 https://www.djbh.net/agency?q=agencyIn&tab=2
- 处罚案例：广州市人民政府公共服务、腾讯网北京市昌平区委宣传部官方账号

  https://www.gz.gov.cn/zwfw/zxfw/ggfw/content/post_9129540.html

  https://new.qq.com/rain/a/20230913A05GBX00

MS&AD InterRisk综研隶属于MS&AD保险集团控股株式会社，是一家专门从事风险管理有关的调查研究以及咨询相关的专业公司。
面向有意向中国进军的企业有关咨询・研讨会方面的洽谈可以联系我公司下述联络方式或是联系三井住友海上、爱和谊日生同和各营业担当。

联系方式　MS&AD InterRisk综研　风险咨询本部 国际业务组
TEL.03-5296-8920　　http://www.irric.co.jp/

瑛得管理咨询（上海）有限公司是在中国上海设立的隶属于ＭＳ＆ＡＤ保险集团的风险管理公司，主要提供诸如工厂/仓库的风险查勘、BCP 计划的制定等各种风险相关的咨询服务。如欲联系或申请等请联系下述地址。
联系方式　瑛得管理咨询（上海）有限公司　（日语：インターリスク上海）
上海市浦东新区世纪大道 100 号　环球金融中心 34 层 T10 室-2
TEL:+86-(0)21-6841-0611（代表）