网络安全相关的测评认证探讨

第三届中国网络安全大会（NSC2015）

倪光南　　2015年7月1日

一、加强并完善等级保护工作

- 我国推行计算机系统等级保护制度对保障网络安全、信息安全有重大作用。早在1994年国务院就颁布《中华人民共和国计算机信息系统安全保护条例》，规定计算机信息系统实行安全等级保护。2003年，中央办公厅、国务院办公厅颁发《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27号）明确指出“实行信息安全等级保护”。此后又出台了一系列文件，使这一工作全面展开，至此，等保工作已进入了规模化推进阶段。
- 实行信息安全等级保护是客观需求，也符合信息安全发展规律。当前，我们应加强并完善等级保护工作，为增强网络安全、信息安全作出更大贡献。

优先采购获得高级别认证的产品

- 等保要求对信息安全分等级、按标准进行建设、管理和监督。因此，在信息化建设中，从方案设计、采购选型开始，就应在等保制度指导下进行。
- 与等保制度相关，应当要求重要信息系统建设优先采购通过高级别的分级测评认证的安全产品，例如在招标中可对获得高级别认证的产品加分。这在国际上已有先例：美国从2002年7月起，它的政府和军队采购已经规定必须优先选用通过CC认证的产品。
- 今后可以对信息安全产品包括信息关键核心技术和设备（如CPU、OS等等）逐步实行强制认证（例如可将分级测评认证纳入3C认证），同时要求政府和重要信息系统建设优先采购通过3C认证的产品。这种做法既有利于增强网络安全，又符合市场经济自由竞争原则，可以公开、公平、公正地推行。

分级测评认证应适应新一代信息技术

- 国际上信息安全分级测评认证标准的发展情况：最早在1985年，美国颁布了TCSEC，后来演进到“国际通用准则（CC）”，到1999年成为国际标准（ISO/IEC 15408），我国于2001年等同采用这一标准成为GB/T 18336。
- 我国把信息安全产品的测评认证分为7个级，并分别对应CC评估标准的7个级别（EAL1—EAL7）。取决于实际产品，可能达到的最高级别有所不同，例如IC卡、SIM卡等最高可达到EAL5，服务器操作系统最高可达到EAL4等等。
- 目前，信息产品的分级测评认证标准应予以发展，以适应新一代信息技术要求。例如过去并没有移动操作系统这一类产品，所以最近推出的航天元心的移动操作系统通过研制单位和测评认证机构的共同努力，基本上通过了EAL4测评认证，并在此基础上有关单位正在制定相应的标准，今后这可望作为重要部门采购移动终端的一个必要条件，国产桌面操作系统也准备仿照这一先例。

等级保护标准有待于发展完善

- 目前等级保护的有关国家标准有30余个，但针对具体技术产品的分级测评标准不多，内容也不够充实，今后需增加针对新的产品和服务的标准，并增补其中的内容，以切合实际需求。
- 例如，这些标准中涉及的具体产品仅有路由器、虹膜识别系统、服务器、操作系统、数据库管理系统、入侵检测系统、网络脆弱性扫描产品、、网络和终端离部件、防火墙和应用软件等等。显然，这些种类还远远不够，有的类别还需细分。例如操作系统可细分为服务器、桌面、移动、嵌入式操作系统等等；作为生物特征识别系统，现仅针对虹膜识别系统，还应扩展到指纹、掌纹、声纹、人脸等等的识别系统；应用软件作为一类范围太大，应细分为许多子类。
- 此外，对于信息领域新业态，如云计算、大数据、移动互联、物联网、智慧城市等等，还缺乏相应的标准。

二、自主可控的评估标准

- 为使信息化建设能满足“自主可控安全可信”的要求，需建立一些新的规章制度，例如最近网信办主持制订的网络安全审查制度。类似地，建议出台自主可控的评估标准，其理由如下：
  - 自主可控是达到安全可信的必要条件但非充分条件。产品和服务等自主可控，基本上可保证不存在恶意后门并能不断地对其进行改进或修补漏洞。反之，如果产品和服务等不能自主可控，就意味着受制于人，其后果是：一般存在恶意后门，难以不断地对其改进或修补漏洞，信息安全难以治理。
  - 自主可控是产品和服务的客观属性，基本上独立于使用场景和生命周期，是可以根据各种数据资料一次性地加以评估的。相比之下，产品和服务是否安全可信与使用场景和生命周期都有关系，难以进行一次性的评估。
  - 如同性能、经济等等指标那样，自主可控可以成为重大项目立项或对产品服务进行选型采购的一项指标，为此需要制定相应的评估标准。

自主可控的五方面评估标准

建议从以下五个方面对自主可控程度进行评估：

1. 知识产权，
2. 能力，
3. 发展，
4. 供应链，
5. “国产”资质。

1. 知识产权（包括标准）自主可控

- 在当前的国际竞争格局下，知识产权自主可控十分重要，做不到这一点就一定会受制于人。如果所有知识产权都能自己掌握，当然最好，但实际上不一定能做到，这时，如果部分知识产权能完全买断，或能买到有足够自主权的授权，也能满足自主可控。
- 然而，如果只能买到自主权不够充分的授权，例如某项授权在权利的使用期限、使用方式等方面具有明显的限制，就不能达到知识产权自主可控。
- 目前国家一些计划对所支持的项目，要求首先通过知识产权风险评估，才能给予立项，这种做法是正确的、必要的。标准的自主可控似可归入这一范畴。

2. 能力自主可控

- 能力自主可控，主要指技术能力的自主可控，这意味着要有足够规模的、能真正掌握该技术的科技队伍。
- 技术能力可以分为一般技术能力、产业化能力、构建产业链能力和构建产业生态系统能力等层次。产业化能力的自主可控要求使技术不能停留在样品或试验阶段，而应能转化为大规模的产品和服务。产业链的自主可控要求在实现产业化的基础上，围绕产品和服务，构建一个比较完整的产业链，以便不受产业链上下游的制约，具备足够的竞争力。产业生态系统的自主可控要求能营造一个支撑该产业链的生态系统。

3. 发展自主可控

- 除了知识产权和能力的自主可控，还需要有发展的自主可控，因为我们不但要着眼于现在，还要求在今后相当长的时期里，对相关技术和产业而言，都能不受制约地发展。
- 为此，根据我国具体情况，要着眼国家安全和长远发展，制订信息核心技术设备的发展战略。如果某些技术在短期内似乎能自主可控，但长期看做不到自主可控，一般说来是不可取的。只顾眼前利益，有可能会在以后造成更大的被动。

4. 供应链自主可控

- 一个产品的供应链可能很长，如果其中的一个或某些环节不能自主可控，也就不能满足自主可控要求。例如对复杂的CPU芯片来说，即使拥有知识产权，也有技术能力掌握，做到在设计方面不受制于人，但如需依赖外国才能进行生产，那么仍然达不到自主可控的要求。
- 所以，应当评估一个产品的供应链是否能完全掌控？像上述复杂的CPU芯片，如果必须依赖外国进行生产加工，就不能满足自主可控的要求。如果能够依靠本国厂商生产出来，即使性能指标略低一些，还是可以容许的。

5. “国产”资质

- 一般说来，“国产”产品和服务容易符合自主可控要求，因此实行国产替代对于达到自主可控是完全必要的。不过现在对于“国产”还没有统一的评估标准。
- 过去有人提出的某些评估标准显然是不合适的。例如：认为只要公司在中国注册、交税，就是“中国公司”，它的产品和服务就是“国产”；或认为“本国产品是指在中国关境内生产，且国内生产成本比例超过50%的最终产品”。这里，突出“生产成本”完全不适用于高技术领域。众所周知，高技术产品和服务的成本主要是开发成本、智力成本，生产成本甚至可以忽略不计，这种“生产成本”准则是帮进口高技术产品的忙，因为它们只要用中国原材料做个包装，就可以摇身一变成为“国货”了。

“国产”资质（续1）

- 美国国会在1933年通过的《购买美国产品法》，要求联邦政府采购要买本国产品，即在美国生产的、增值达到50%以上的产品，进口件组装的不算本国产品。美国采用上述“增值”准则来评估“国产”，比较合理。这方面我们理应学习发达国家行之有效的做法。
- 现在人们大多根据产品和服务提供者资本构成的“资质”进行评估，包括内资（国有、混合所有制、民营）、中外合资和外资等，还包括近来出现的“VIE”这类资质。

“国产”资质（续2）

- 考察资质是必要的，但除此以外，还应采用“增值”准则对“国产化程度”加以评估，因为如某项产品和服务在中国的增值很小，意味着它可能就是从国外进口的，达不到自主可控要求。例如进口硬件可能通过“贴牌”、“组装”变成“国产”，进口软件和服务可能通过“集成”变成“国产解决方案”的一部分。如果实行“增值”估算，这类“假国产”就难以立足了。建议有关方面尽快出台合理的“国产”评估准则。
- 综上所述，制订自主可控的评估标准是可行的，也是对保障网络安全、信息安全有实际意义的，建议有关部门予以考虑。

谢谢大家！