ICT 产品信息安全北美市场准入体系研究

研究报告

项目组

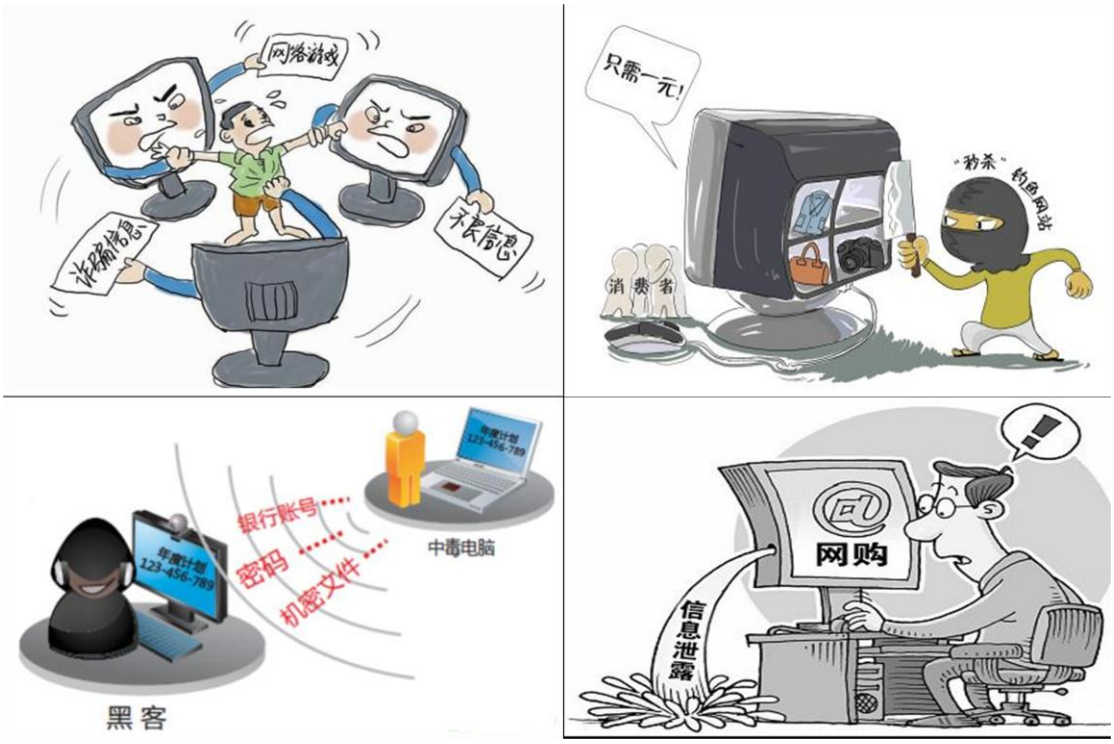
二零一八年十二月

目录

1 ICT 行业信息安全现状及发展趋势

1.1 概述

第四次工业革命的浪潮席卷全球，基于智能化的网络更多的深入到国家、经济、生产、生活的各个方面，推动全球迈入数字化时代。数字化如同一把双刃剑，一方面极大推进了人类社会的发展，另一方面也打开了新型网络威胁的潘多拉魔盒。据工信部发布的消息：2018 年第二季度，我国共监测网络安全威胁约 1841 万个，包含依然在不断蔓延的“挖矿”病毒、时发的“黑客攻击”、最新发现“熔断”与“幽灵”漏洞、大规模的“数据泄露”等，企业面临的网络安全形势日益严峻。



图片摘自网络

研究分析显示，近年来信息安全事件的数量和规模均有逐步升级的趋势，已经波及到全球个人、企业的数据安全，甚至对国家安全造成了严重威胁（见第二

小节 ICT 行业信息安全现状及发展趋势之“信息安全形势日益严峻”)。

针对日益严峻的信息安全形势，美国采取了一系列行动。例如，2018 年初，美国打倒了被大众广为熟知的大规模网络犯罪组织——infraud 组织，据称，该组织贩运了大量被偷盗的金融数据（包括多达四百万张银行卡）、身份信息和价值超过 5.3 亿美元的违禁品等，已经对社会造成了 22 亿美元的损失。目前执法部门已经逮捕了 13 名成员，并对涉案人员提起了诉讼。

执法部门对网络犯罪行为的法律制裁表明美国对信息安全的重视程度越来越高，这也意味着美国对相关产品信息安全的监管要求可能会越来越高。例如，2018 年 1 月，美国联邦贸易委员会(FTC)与香港智能玩具制造商伟易达(VTech Electronics)就网络攻击事件达成协议，伟易达因未能做好数据保护工作，导致数百万用户数据泄露而被处以 65 万美元罚款。

面对日趋严格的信息安全管理要求，如果我国企业在认知不足的情况下开展对外经济活动，将可能造成庞大的损失。例如，2018 年 1 月，由于涉及到包括军方人员在内的美国公民的信息安全，蚂蚁金服收购速汇金的计划遭到美国监管部门的反对；2 月，美国以“信息安全”为由，禁止华为通讯设备进入国内市场，这对于华为走向世界将是一个沉重的打击。

本项目从法律法规、标准、符合性评价等方面着手，对北美信息安全市场准入体系展开系统研究，将有效帮助我市企业了解相关的合规要求，减少不必要的经济损失，提高其市场竞争力。

1.2 ICT 行业信息安全现状及发展趋势

1.2.1 国内 ICT 行业快速发展

数字经济的核心之一是 ICT 行业，从较早的 ICT 制造业，到如今火热的云计算、大数据、VR、物联网及人工智能等，ICT 技术与业务发展日新月异。在

ICT 企业中，以华为、中兴、联想等为代表的 ICT 设备制造企业，占据了世界的领先位置，据统计，2017 年华为、中兴通讯的工业产值均超过千亿元；中国的 3 大运营商中国移动、中国电信、中国联通都是世界 500 强；BAT（百度、阿里、腾讯）等互联网企业的营业规模也不逊于谷歌、亚马逊、Facebook 等美国企业，截至 2017 年 9 月底，90 家上市互联网公司的市值总额达到了 8.34 万亿元，年内累计上涨了 57.6%。

如图为全球智能手机 TOP5 企业市场份额，从图中可以看到，中国品牌华为、OPPO、小米名列前茅。

	2014	2015	2016		2017前三季度	
三星	24.4%	22.7%	三星	21.2%	三星	22.8%
苹果	14.8%	16.2%	苹果	14.6%	苹果	13.1%
华为	5.7%	7.4%	华为	9.5%	华为	10.5%
联想	4.6%	5.2%	OPPO	6.8%	OPPO	7.9%
小米	4.4%	4.9%	vivo	5.3%	小米	6.2%

图 1 全球智能手机 TOP5 企业市场份额

（来源：IDC 发布及中国信息通信研究院）

下图为近几年我国 ICT 行业产值，由图可知，2017 年我国 ICT 总产值突破了 20 万亿，同比增长 14.5%，增速较 GDP 增速快得多。

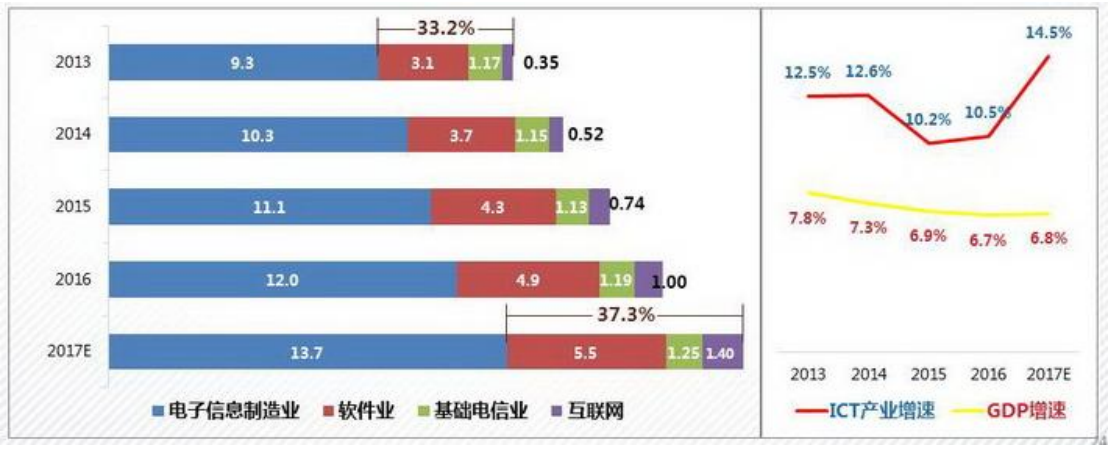


图 2 我国 ICT 行业产值

（来源：IDC 发布及中国信息通信研究院）

1.2.2 信息安全形势日益严峻

ICT 技术飞速发展的同时，也给企业与民众的信息安全带来了极大的威胁。

2018 年第 48 届世界经济论坛中发布的《2018 年全球风险报告》显示，网络安全威胁已经成为了仅次于极端气候和自然灾害的全球第三大威胁，成为 Top10 威胁场景中由人为因素造成的最高威胁，这也是网络攻击首次被列入该组织风险报告前五。

图 3 十大可能性风险威胁因素

日前，迈克菲与美国国际战略研究中心(CSIS)合作撰写的报告表明，2017 年全球网络犯罪成本估计为 6000 亿美元，相当于全球 GDP 的 0.8%，比 2014 年同比增长 20%。其中，北美地区网络犯罪成本高居榜首。

Region (World Bank)	Region GDP (USD, trillions)	Cybercrime Cost(USD, billions)	Cybercrime Loss(% GDP)
North America	20.2	140 to 175	0.69 to 0.87%
Europe and Central Asia	20.3	160 to 180	0.79 to 0.89%
East Asia & the Pacific	22.5	120 to 200	0.53 to 0.89%
South Asia	2.9	7 to 15	0.24 to 0.52%
Latin America and the Caribbean	5.3	15 to 30	0.28 to 0.57%
Sub-Saharan Africa	1.5	1 to 3	0.07 to 0.20%
MENA	3.1	2 to 5	0.06 to 0.16%
World	**$75.8**	**$445 to $608**	**0.59 to 0.80%**

图 4 2017 年网络犯罪区域分布

以美国为例，网络犯罪是其犯罪活动增长最快的类型，每年受害人数都在不断增加。据 FreeBuf 平台预测，2018 年网络犯罪带来的经济损失仅加州就将超过 3 亿美元，投诉事件将达 5.6 万起。

风险等级	城市	预计损失总额
#1	加利福尼亚州	$329,062,355
#2	纽约州	$139,450,948
#3	佛罗里达州	$111,756,654
#4	德克萨斯州	$96,024,002
#5	弗吉尼亚州	$64,313,078

图 5 FreeBuf 平台预测的 2018 年美国各州网络犯罪带来的经济损失

另外，据国家信息中心信息与网络安全部与瑞星联合发布的《中国网络安全报告》统计，全球范围内，2017 年瑞星截获恶意网址(URL)总量为 8011 万个，其中美国总量为 2684 万个，位列全球第一，中国 1350 万个位居其次，韩国 507 万个位列第三。

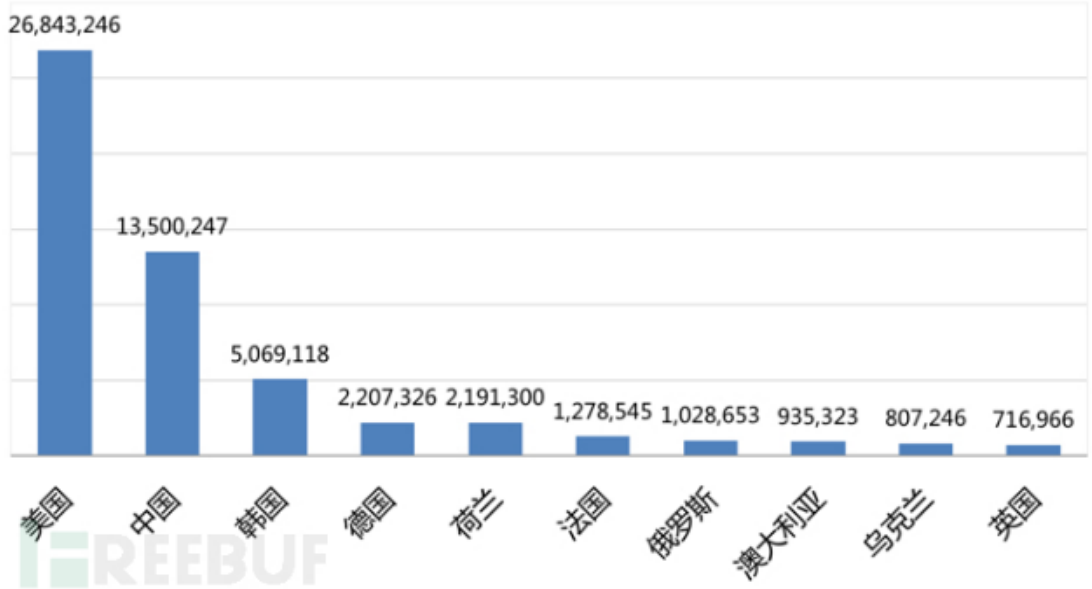


图 6 2017 年全球恶意 URL 地域分布 Top10

在信息泄露方面，据数字安全提供商 Gemalto 保守统计，仅 2017 年上半年，全球公开的网络安全入侵事件达 918 起，影响到 19 亿个数据记录，几乎每天都

有超过 1000 万数据记录被泄漏或者曝光，这些记录涉及医疗、个人信用卡、财务或者个人信息相关数据。在数量上，相比去年，受影响的数据记录增长了 164%。

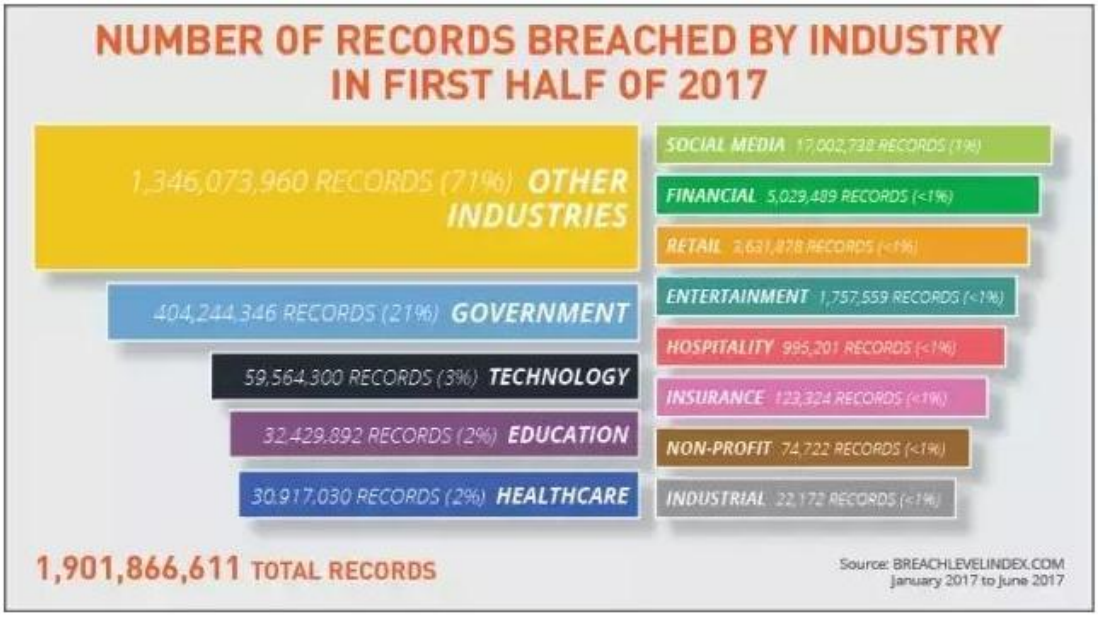


图 7 2017 年上半年网络安全入侵事件统计

总的来说，近年来全球的信息安全风险日趋增大[1]。

1.2.3 标准化建设亟需完善

中国政府历来高度重视信息安全。2014 年，习近平总书记主持召开中央网络安全和信息化领导小组第一次会议时就指出“网络安全和信息化是一体之两翼、驱动之双轮”，“没有网络安全就没有国家安全，没有信息化就没有现代化”。

2017 年 6 月 1 日，《中华人民共和国网络安全法》正式实施，该法于 2016 年颁布，是我国第一部网络安全的专门性及综合性立法，提出了应对网络安全挑战这一全球性问题的中国方案。

根据《网络安全法》第二十三条之规定，国家要建立完善网络关键设备和网络安全专用产品检测认证制度。认证离不开标准，虽然目前我国在信息安全标准

[1]附件 1 为 2017 年全球信息安全大事记

化工作上已经取得了一些成果，比如信息安全等级保护系列标准为各企业的信息系统安全等级保护状况的认可及评定提供了依据，但仍需加大投入力度，尽快建立覆盖全面的信息安全标准体系，更好地服务于信息安全产业的发展，提升我国信息产品的安全技术水平和市场竞争力。

对北美信息安全市场准入体系展开研究，可以引导国内相关标准和认证制度与国际标准进行接轨和转化，对我国进一步加强信息安全管理具有很好的借鉴意义。

1.2.4 企业亟需加强合规经营

ICT 企业作为深圳的支柱性产业，对于深圳的发展是至关重要的，但是目前 ICT 企业面临的出口风险亟需重视。有报告显示，2017 年，深圳出口产品共遭境外退运 1363 批，货值 9424 万美元，遭境外通报 54 例，退运、通报产品主要为信息设备、电子元器件设备和音视频设备，退运、通报批次居前三位的国家或地区为中国香港、美国、欧盟。可以看出，遭到退运、通报的产品主要集中在 ICT 行业，而且美国地区形势严峻。

另一方面，国外技术性贸易措施频频冲击 ICT 产业，据调查，2017 年深圳出口遭受国外技术性贸易影响集中体现在信息通讯、电子电器等支柱产业，技术性贸易措施已经成为中国出口企业面临的继汇率之后的第二大障碍。而深圳作为全国高新技术产业集聚地和出口大市，企业受到国外技术性贸易措施影响尤其值得重视。

例如，欧盟 2017 年 6 月强制实施的无线电设备指令(RED)加强了 CE 标志的市场监督，大大增加了我国通信产品的出口难度，导致我市某龙头通讯企业为应对该问题累计投入资金高达 4000 余万元。鉴于此，北美信息安全相关的市场准入要求未来也可能强制执行或相关部门可能会加大监管力度，如果企业没有充分

了解市场相关法规和规范，很可能会造成严重的后果。

2016 年 3 月，因涉嫌违反美国出口管制法律，不符合相应的法规要求，中国电信设备制造商中兴通讯，包括中兴和三家子公司在内的四家公司被美国商务部列上出口黑名单。如果没有许可，美国供应商不得与这份名单上的实体进行合作。被美国列入“实体清单”的最大风险在于，由于重要元器件自美国进口，美国供应商被美国政府禁止供货后，中兴将面临严重的元器件短缺。最终通过协商，中兴支付史上最高罚单 8.9 亿美元，美国商务部将其移出黑名单。这是典型的由于对相关法规及准入性要求缺乏了解而造成巨大经济损失的案例。

随着经济全球化的发展，中兴、华为等 ICT 企业大量出口产品到北美市场，以支付宝为代表的互联网企业也陆续进军北美市场，而这些企业的产品正是信息安全涉及的重要领域，因此，他们急需有关部门对相关的市场准入要求进行权威、系统的跟踪、研究及解读，并提出有效的应对方案，以帮助他们实现合规经营，规避风险，赢得市场先机。

2 ICT 产品信息安全北美市场准入体系

北美地区包括美国、加拿大和墨西哥等国家，本报告主要研究经济和信息技术比较发达的美国和加拿大。加拿大在产品信息安全立法和标准方面，基本与美国一致，虽然流程上略有差异，但是，其技术标准几乎是完全参照美国而来，对于我国的 ICT 企业来说，要满足加拿大的要求，研究美国的法规和标准是首要工作。

美国政府从上世纪 90 年代开始即从国家层面对信息安全进行了设计和实践，形成了包括国家战略、法制体系、管理体制等多个方面的信息安全政策措施体系，并且根据形势发展不断完善扩充。在市场准入方面，目前已经形成了包括法律法规、标准要求、符合性评价及认证标志等在内的较为完善的框架体系。

2.1 法律法规

美国是网络安全领域立法起步最早、数量最多、覆盖最全面的国家。为加强信息网络基础设施保护和打击网络犯罪，美国从 20 世纪 70 年代就开始陆续制定了多部法律。尤其是“911”事件发生之后，美国对信息安全保障的重视进入到一个新的阶段，迅速制定了一系列网络信息安全相关的规章政策。这些相关法规涉及网络基础设施保护、网络泄密与数据保密、打击网络恐怖主义、网络色情等犯罪活动治理、惩治网络信息滥用与欺诈、网络知识产权保护等方面，时至今日美国已经形成了比较完善的信息安全保障体系。

2.1.1 美国保护联邦信息安全的立法情况

美国对计算机网络高度依赖，从联邦政府到州政府，再到公民个人的大量信息，几乎全部存储在计算机系统中。由于联邦信息安全事关国家安全及政治稳定，一旦遭到破坏，后果不堪设想，因此美国极为重视对联邦信息和信息系统的保护。

目前，美国有关联邦信息安全的立法主要有：

1966 年，美国制定《信息自由法》，并且分别于 1974 年、1986 年和 1996 年进行了修订，主要内容涉及对政府信息的获取、公开方式、可分割性，以及相关的诉讼事宜等。

1977 年，美国联邦政府出台了《联邦计算机系统保护法案》，首次将计算机系统纳入法律的保护范围。

1987 年，美国政府颁布《计算机安全法》，通过法律的形式授权国家标准与技术局有权为美国联邦政府计算机系统制定网络信息安全的政策和标准。该法之后被作为美国各州制定地方法规的依据，是美国关于网络信息安全的根本大法，真正打开了网络信息安全法制建设的大门。

1996 年发布的《克林格-科恩法》，又名《信息技术管理改革法》，要求美国

政府部门长官负责制定本部门的信息安全政策和程序，并在各政府部门设立“首席信息官”。

2000 年发布的《政府信息安全改革法》，规定联邦政府部门在保护信息安全方面的责任，此法明确了商务部、国防部、司法部、总务管理局、人事管理局等部门维护信息安全的具体职责，建立了联邦政府部门信息安全监督机制。

2002 年发布的《联邦信息安全管理法》，后纳入《电子政府法》，为联邦信息系统创建了一个安全框架，进一步明确并加强国家标准与技术研究院在制订网络安全标准方面的职责，建立了联邦计算机事故反应中心。

2017 年 8 月，美参议员提出新法案《物联网网络安全改进法案》，要求联邦政府的设备供应商遵循行业范围内的安全实践，以确保美国政府“以身作则”，防止因物联网领域缺乏重大创新使联邦系统遭遇进一步入侵。

2.1.2 美国打击网络犯罪的立法情况

美国的网络犯罪立法最初是从州开始的，1978 年，佛罗里达州率先制定了计算机犯罪法，截至目前，除佛蒙特州外，其他所有的州都制定了专门的计算机犯罪法。

1984 年的《伪造连接装置及计算机欺诈与滥用法》，是美国通过的第一部关于计算机安全与犯罪的法案，规定了禁止对联邦计算机系统、银行系统、各州及对外贸易的各种攻击。

1986 年，美国政府制定了《计算机欺诈与滥用法》，扩展了 1984 年《伪造连接装置及计算机欺诈与滥用法》的范围，并对 1986 年《电子通讯隐私法》进行了补充。该法案针对入侵网络信息系统的行为，确定了两类犯罪行为，即：未经授权的带有盗窃、欺诈意图对“与联邦政府有关的计算机”进行访问以及“故意破坏”政府机构、金融机构、医疗机构及其相关的网络信息系统。在 1994 年

的修正案中，对传播病毒和其他有害代码行为也作了规定。

《计算机欺诈与滥用法》颁布以后，网络技术的发展导致计算机犯罪出现新的形式，尤其是业内人士的犯罪行为增加，但该法并没有对内部人员犯罪做出规定，加上近些年计算机犯罪的产业化趋势，使得计算机犯罪立法更为紧迫。

2.1.3 美国保护个人隐私的立法情况

随着电子商务的迅速发展，收集和分析个人信息的软件行业纷纷建立，给用户的个人隐私安全带来了极大的隐患。基于此，各国纷纷从法律层面加强对个人隐私的保护。美国有关隐私保护的立法落后于欧盟，尤其是 2001 年《爱国者法》的出台，扩大了警察机关的权限，为政府更多的涉入公民私生活创造了条件，违反了确保公民私生活隐秘的宪法原则，引起很大的争议，美国应该考虑制定适应当今时代的新的隐私保护法律。

目前，美国有关信息安全的隐私保护立法主要有：

1974 年的《隐私权法》，规定联邦机构限制个人可识别信息的披露，要求机构提供访问个人信息记录的权利。

1986 年通过的《电子通信隐私法》主要禁止未经授权的电子窃听，规定政府访问电子通信记录、拦截通信信号的范围和标准。

1997 年，美国制定了《公共网络安全法》，重在调整应用于商务、通信、教育和公共服务等领域的公共网络的信息安全。该法结合宪法、民商法、行政法的有关规定，规定法律规定的网络主体在网络社会享有的隐私权、知识产权及网络主体自身的合法权利，同时规定了网络侵权的惩罚标准。同年还颁布了《联邦互联网隐私保护暂行条例》，该法保护政府持有的与公民个人的教育、经济、医疗和就业历史有关的网上信息（包含名字、身份证号码、性别、家庭住址、通讯方式等），政府不能非法使用或泄露公民因公登记在网络中的信息。

1998 年，美国通过了《儿童网上隐私保护法》，该法规定了网站经营者必须披露其隐私保护政策，声明寻求儿童监护人同意的时间及方式，以及违反儿童隐私保护应承担的责任。该法适用于美国管辖之下的自然人或单位对 13 岁以下儿童在线个人信息的收集。

2001 年的《医治保险携带和责任法》(HIPAA)修正案，目标之一就是保护病人的电子健康记录，并提出保护的具体标准。该法详细规定了行政保障措施、物理保障措施、技术保障措施及安全责任的分配问题，对于违反安全标准的实体，规定了最高可达 25 万美元罚款和最长 10 年监禁的严厉惩罚措施。

2.1.4 美国保护关键基础设施的立法情况

关键基础设施关系到一国的经济发展与社会稳定，美国特别重视对关键基础设施的保护。20 世纪 90 年代中期，鉴于日益增长的国际恐怖主义威胁，美国从国土安全的角度对关键基础设施进行了重新定义。2001 年的《爱国者法》对其做出了详细的概念解释。2003 年布什总统发布第 7 号国土安全总统令《关键基础设施标识、优先级和保护》，对美国关键基础设施和重要资源进行优先级排序和保护。2006 年国土安全部(DHS)发布《国家基础设施保护计划》为今后的关键基础设施保护提供总体框架。相关法律主要涉及以下几部：

1996 年发布的《国家信息基础设施保护法》，规定未经授权进入受保护的计算机系统并通过各种形式进行恶意破坏行为，利用电子手段对他人和机构进行敲诈行为，或是试图这样做的行为都要受到刑事指控。

2002 年发布的《国土安全法》，明确了 DHS 的职责和组织体系、信息分析和基础设施保护、CIO 管理职责，以及加强在国土安全保护方面的合作等。

2010 年发布的《国土安全网络和物理基础设施保护法》，涵盖了部门责任义务的遵守、个人隐私保护和数据泄露应对、网络安全教育和技术研发、重要电力

基础设施保护和漏洞分析、国际合作、打击网络犯罪以及采购与供应链安全等内容。

此外，美国 111 届国会上提出《国家网络基础设施保护法案 2010》，规定在国防部(DOD)建立国家网络中心，设立主管职位直接向总统报告安全事件，建立国家网络安全项目预算全国性的网络防御应急基金，建立政府与私营部门之间协作的网络防御联盟，分享彼此的网络安全威胁信息，并互相提供技术支援。

2.1.5 小结

总结美国相继出台的信息安全立法，可以看出美国完善信息安全的法律经历了一个从“预防为主”到“先发制人”，以控制“硬件设备”到控制“网络信息内容”的演化过程。

首先，美国信息安全立法涉及范围广泛，有打击网络犯罪方面的，加强信息网络基础设施保护方面的，规范信息收集、利用、发布方面的，还有隐私权保护等方面的。

其次，注重多部门协作，为了落实信息安全政策及法律，美国将政策执行、监督、管理等权利分配给多个部门，包括 DHS、OMB、国防部、审计署、商务部、司法部等，并且根据现实需要不断增设新机构。同时建立威胁信息共享及应急支持机制，并且设立专门机构协调各方携手保护信息安全。

此外，美国还注重标准的制定，在多部法律中提到制定相应标准保护信息安全，例如规定 CIO 委员会与 NIST 协作制定安全标准，NIST 制定高性能计算的安全与隐私标准等。

总体而言，美国当前有关信息安全立法的发展趋势是要扩大政府部门在网络监管中的权限，并明确其职责任务，以满足应对与日俱增的信息安全风险与挑战

的需求[2]。

2.2 标准

美国的信息技术标准主要由美国国家标准化协会(ANSI)、美国国家技术标准局(NIST)制定。此外，电子工业协会(EIA)和通信工业协会(TIA)也制定了部分信息技术标准。这些标准分为：美国国家标准、美国联邦信息处理标准(FIPS)、DoD 信息安全指令和标准(DoDDI)和 IEEE 标准。

美国国家标准

ANSI 中的 NCITS 技术委员会（即 X3）负责信息技术标准，它同时也是 ISO/IEC 第一联合技术委员会(JTC1)的秘书处。NCITS 下设的分技术委员会 T4 负责 IT 安全技术，对应 JTC1 的 SC27。ANSI 中的 ASC X9 和 X12 负责金融安全，ASC X9 制定金融业务标准，ASC X12 制定商业交易标准。

美国联邦信息处理标准(FIPS)

FIPS 在 NIST 广泛搜集政府和私人部门的意见的基础上完成，在正式发布之前，FIPS 分送给每个政府机构，经再次征求意见后，NIST 把 FIPS 标准连同 NIST 的建议一同呈送给美国商务部，由部长决定同意或反对该标准。目前，已经有一系列的 FIPS 标准，而数据加密标准 DES 是 FIPS 安全标准中一个最著名的例子。

DoD 信息安全指令和标准(DoDDI)

DoD 一直非常重视信息安全，并发布了一系列有关信息安全和自动信息系统安全的指令、指示和标准。其中，DoD 5200.28-STD《可信计算机系统评价标准》受到了广泛关注。

IEEE 标准

[2] 2018 年美国的信息安全法制建设力度颇大，推出了多个相关法案或法规，具体可参考附件 2（2018 年美国信息安全最新法规动态）

IEEE 在信息安全标准方面的主要贡献是提出了 LAN/WAN 安全标准 SILS 和公钥密码标准 P1363。

下面主要介绍几个典型的信息安全相关标准。

2.2.1 TCSEC 标准

美国可信计算机系统评价标准(Trusted Computer System Evaluation Criteria，简称 **TCSEC 标准**)是计算机系统安全评估的第一个正式标准，即桔皮书，具有划时代的意义。该准则于 1970 年由美国国防科学委员会提出，并于 1985 年 12 月由美国国防部公布。TCSEC 最初只是军用标准，后来延至民用领域，主要针对保密性而言。

TCSEC 使用了可信计算基础(Trusted Computing Base, TCB)的概念，这是一种实现安全策略的机制，包括硬件、固件和软件，它们根据安全策略处理主体对客体的访问，具有抗篡改的性质和易于分析和测试的结构。

TCSEC 论述的重点是通用的操作系统，为了使其评判方法适用于网络，NCSC 于 1987 年出版了一系列有关可信计算机数据库、可信计算机网络等的指南（俗称彩虹系列）。TCSEC 的主要缺点在于：

- 主要关注保密性，不关注可用性和完整性；
- 强调的是控制用户，没有关注程序上的、物理上的和人员的安全措施；
- 并没有关注网络（后续出版的书籍弥补了这一不足）。

在 TCSEC 中，定义了系统安全的 4 个方面：安全策略、可追溯性、安全保障和文档，美国国防部按信息的等级和应用采用的响应措施，将计算机安全从高到低分为：A、B、C、D 四类七个级别，共 27 条评估准则。其中 D 为无保护级，C 为自主保护级，B 为强制保护级，A 为验证保护级。

D 类安全等级（最低保护）

D 类安全等级只包括 D1 一个级别，其安全等级最低。D1 系统只为文件和用户提供安全保护，未加任何实际的安全措施，不要求进行用户登陆和密码保护，整个系统是不可信的，硬件和软件都容易被侵袭。最普通的形式是本地操作系统，或者是一个完全没有保护的网络。

C 类安全等级（被动的自主访问策略）

该类安全等级能够提供审计的保护，并为用户的行动和责任提供审计能力。C 类安全等级可划分为 C1（自主安全保护级）和 C2（受控访问控制保护级）两类。C1 系统的 TCB 通过将用户和数据分开来达到安全的目的。在 C1 系统中，所有的用户以同样的灵敏度来处理数据，即用户认为 C1 系统中的所有文档都具有相同的机密性。C2 系统比 C1 系统加强了可调的审慎控制，引入受控访问环境（用户权限级别），在连接到网络上时，C2 系统的用户分别对各自的行为负责，C2 系统通过登录过程、安全时间和资源隔离来增强这种控制。C2 系统具有 C1 系统中所有的安全性特征。

B 类安全等级（被动的强制访问策略）

B 类安全等级可分为 B1（标记安全保护级）、B2（结构化保护级）和 B3（安全域级）三类。B 类系统具有强制性保护功能，意味着如果用户没有与安全等级相连，系统就不会让用户存取对象。B1 系统满足下列要求：

- 系统对网络控制下的每个对象都进行灵敏度标记；
- 系统使用灵敏度标记作为所有强制访问控制的基础；
- 系统在把导入的、非标记的对象放入系统前标记它们；
- 灵敏度标记必须准确地表示其所联系的对象的安全级别；
- 当系统管理员创建系统或者增加新的通信通道或 I/O 设备时，管理员必须指定每个通信通道和 I/O 设备是单级还是多级，并且管理员只能手工改变指定；

- 单级设备并不保持传输信息的灵敏度级别；
- 所有直接面向用户位置的输出（无论是虚拟的还是物理的）都必须产生标记来指示关于输出对象的灵敏度；
- 系统必须使用用户的口令或证明来决定用户的安全访问级别；
- 系统必须通过审计来记录未授权访问的企图。

B2 系统必须满足 B1 系统的所有要求。另外，B2 系统的管理员必须使用一个明确的、文档化的安全策略模式作为系统的 TCB 体制。B2 系统必须满足下列要求：

- 系统必须立即通知系统中的每一个用户所有与之相关的网络连接的改变；
- 只有用户能够在可信任通信路径中进行初始化通信；
- 可信运算基础体制能够支持独立的操作者和管理员。

B3 系统必须符合 B2 系统的所有安全需求，具有很强的监视委托管理访问能力和抗干扰能力。系统必须设有安全管理员，同时应满足以下要求：

- 除了控制对个别对象的访问外，必须产生一个可读的安全列表；
- 每个被命名的对象提供对该对象没有访问权的用户列表说明；
- 在进行任何操作前，要求用户进行身份验证；
- 验证每个用户，同时还会发送一个取消访问的审计跟踪消息；
- 设计者必须正确区分可信任的通信路径和其他路径；
- 可信任的通信基础体制为每一个被命名的对象建立安全审计跟踪；
- 可信任的运算基础体制支持独立的安全管理。

A 类安全等级（形式化证明的安全）

A 系统的安全级别最高，目前 A 类安全等级只包含 A1（验证设计级）一个安全类别。A1 类与 B3 类相似，对系统的结构和策略不作特别要求，其显著特

征是，系统的设计者必须按照一个正式的设计规范来分析系统。对系统分析后，设计者必须运用核对技术来确保系统符合设计规范。A1 系统必须满足下列要求：

- 系统管理员必须从开发者那里接收到一个安全策略的正式模型；
- 所有的安装操作都必须由系统管理员进行；
- 系统管理员进行的每一步安装操作都必须有正式文档。

在 TCSEC 的评价准则中，从 B 级开始就要求具有强制访问控制和形式化模型技术的应用（Bell&LaPadula 保密模型）。

我国于 1999 年将 TCSEC 转化为 GB/T17859《计算机信息系统安全防护等级划分准则》，两者基本等同。不同的是 GB/T17859 舍弃了 D 和 A1 级，将计算机信息系统安全性从低到高划分为 5 个等级。

2.2.2 CC 标准

1993 年，在美国的 TCSEC、欧洲的 ITSEC、加拿大的 CTCPEC、美国的 FC 等信息安全准则的基础上，由 6 个国家 7 方（美国国家安全局和国家技术标准研究所、加、英、法、德、荷）共同提出了“信息技术安全评价通用准则(The Common Criteria for Information Technology security Evaluation，简称 **CC 标准**)，它综合了已有的信息安全的准则和标准，形成了一个更全面的框架。CC 标准是一个国际框架，用来评估信息系统、信息产品的安全性，很多国家根据它来实施信息技术产品的安全性评估与认证。

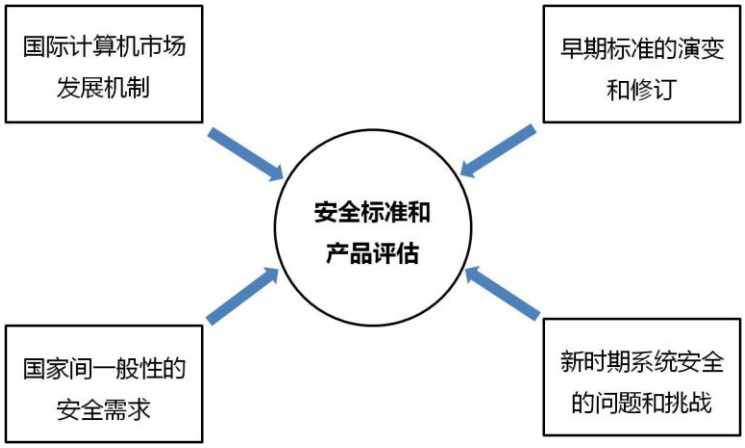


图 8 CC 的驱动因素

CC 标准的具体内容和要求将在第 3 章进行介绍。

2.2.3 FIPS 标准

美国联邦信息处理标准(Federal Information Processing Standards, 简称 **FIPS 标准**) 是标准技术与标准国家协会(National Institute of Standards and Technology, NIST)为联邦计算机系统制定的标准和指南，是一套描述文件处理、加密算法和其他信息技术标准（在非军用政府机构和与这些机构合作的政府承包商和供应商中应用的标准）的标准，其中 140 标准是用来验证信息加密的，与信息安全最为相关。

FIPS 标准的具体内容和要求将在第 4 章进行介绍。

2.2.4 UL CAP 标准

2016 年，美国政府推出“网络安全国家行动计划”(Cybersecurity National Action Plan, 简称 CNAP)，旨在进一步整合原有政策措施，并提出新的针对性措施，来应对网络安全新形势。随后，美国政府特别委托 UL(Underwriter Laboratories Inc.)协同制定了一系列网络安全标准，即 UL 网络安全保障计划(Cybersecurity Assurance Program, 简称 **UL CAP**)系列标准，旨在为联网产品和系统的安全性测试与评估提供技术准则，对相关产品的入市起到规范作用。

UL CAP 系列标准的具体内容和要求将在第 5 章进行介绍。

3 北美 CC 认证体系

3.1 概述

CC 标准的概述见 2.2 章节。在整个安全性评估准则的发展历程中，还有两个非常重要的里程碑式的标准：TCSEC 和 ITSEC 标准。其中 TCSEC 标准已经在第二章中介绍过。

3.1.1 ITSEC 标准

ITSEC 是 Information Technology Security Evaluation Criteria 的简写，即欧洲的安全评价标准，是 1991 年英国、法国、德国和荷兰联合制定的 IT 安全评估准则，比桔皮书更宽松，目的是适应各种产品、应用和环境的需要，较 TCSEC 在功能的灵活性和有关的评估技术方面均有很大的进步。

ITSEC 首次提出了信息安全的保密性、完整性和可用性(CIA)的概念，将安全性要求分为“功能”和“保证”两个部分：功能，指为满足安全需求而采取的一系列技术安全措施，如 AC、审计、鉴别等；保证，指确保功能正确实现及有效性的安全措施。ITSEC 还提出了一个基本观点，即分别衡量安全功能和安全保证。安全功能从 F1 ~ F10 共分 10 级，其中 1 ~ 5 级对应于 TCSEC 的 D 到 A 级，F6 至 F10 级分别对应数据和程序的完整性、系统的可用性、数据通信的完整性、数据通信的保密性以及机密性和完整性的网络安全。安全保证从 E0 ~ E6 共分为 7 级。

与 TCSEC 不同，ITSEC 并不把保密措施直接与计算机功能相联系，而是只叙述技术安全的要求，把保密作为安全增强功能。另外，TCSEC 把保密作为安全的重点，而 ITSEC 则把完整性、可用性与保密性作为同等重要的因素。

3.1.2 CC 标准的发展历程

TCSEC 和 ITSEC 在 CC 的发展历程中起着至关重要的作用，另外，加拿大的 CTCPEC、美国的 FC 也是 CC 形成的基础，如图所示。

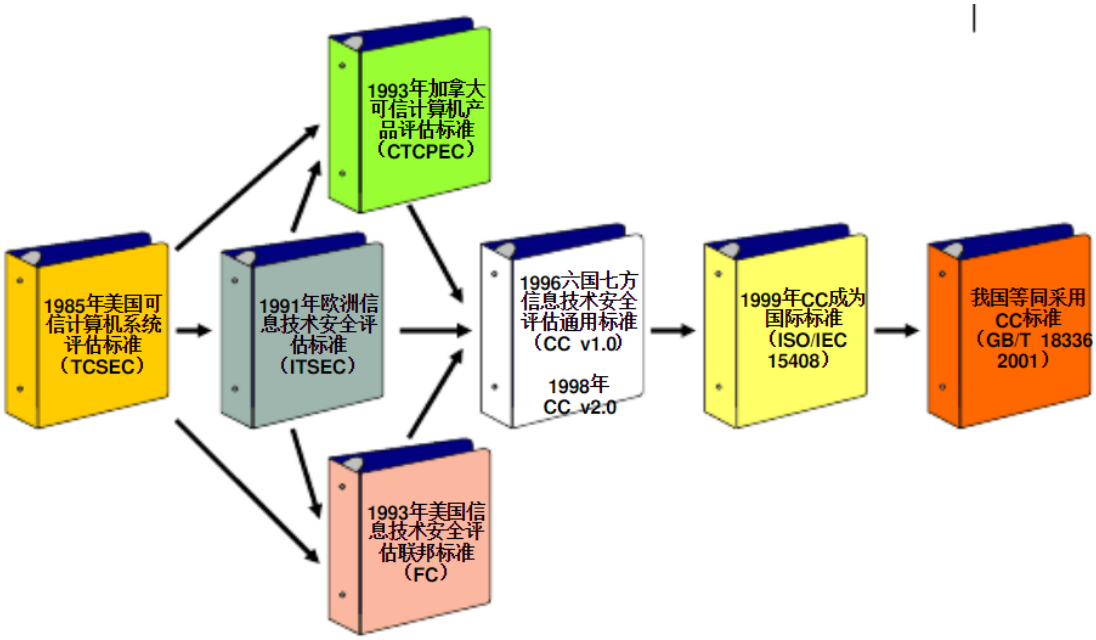


图 9 CC 标准的发展历程

国际 CC 标准由专门的 CC 开发组(CCDB)负责开发和维护，1998 年，标准开发组的参与国联合其他国家共同签署了 CC 互认协定(CCRA)，其中协定很重要的部分是明确了该体系下认证产品可以得到广泛的认可，即一个 IT 产品在英国通过 CC 评估以后，在美国就不需要再进行评估了，反之亦然。该协定组织明确规定了 CC 和 CC 评估方法论(CEM：Common Evaluation Methodology)作为互认协定所使用的标准基础。

在 CCRA 体系中，成员国家的相关政府职能机构负责签署互认协定并最终成为成员国家，同时其认证机构需要在 CCRA 监管之下开展工作。目前 CCRA

共有 28 个成员国，其中发证国（即当地有 CC 测试能力的实验室的国家）有 17 个，受证国有 11 个，如图。

图 10 CCRA 成员国（发证国 17 个）

图 11 CCRA 成员国（受证国 11 个）

1999 年，CC2.0 版成为国际标准 ISO/IEC 15408，CEM 成为 ISO/IEC 18045。我国于 2001 年等同采用为 GB/T 18336，但目前还未加入互认协议。

目前 CC 标准已经发展到第三版本，最新版本为 CC v3.1，并于 2006 年年底正式被国际体系所采用。2008 年所发布的中国国家标准 GB/T 18336 等同采用 CC 2.3 版本（即 ISO/IEC 15408: 2005），目前国际 CC 产业已经停止了 CC 2.3 版本的使用，完全采用最新版本的 3.1 版本。

表 1 CC 组织简介

CCRA	标准开发组的参与国联合了其他国家共同签署了 CC 互认协定(CCRA)。在 CCRA 体系中，成员国家的相关政府职能机构负责签署互认协定并最终成为成员国家，同时其认证机构需要在 CCRA 监管之下开展工作。
CCDB	国际 CC 标准由专门的共同准则开发组(CCDB)负责开发和维护
CCMC	理事会

CC 标准的意义在于：

- 通过评估有助于增强用户对于 IT 产品的安全信心；
- 促进 IT 产品和系统的安全性；
- 消除重复的评估。

CC 标准的局限性在于：

- CC 标准采用半形式化语言，比较难以理解；
- CC 不包括那些与 IT 安全措施没有直接关联的、属于行政性管理安全措施的评估准则，即该标准并不关注组织、人员、环境、设备、网络等方面的具体的安全措施；
- CC 重点关注人为的威胁，对于其他威胁源并没有考虑；
- CC 并没有针对 IT 安全性的物理方面的评估（如电磁干扰）；
- CC 并不涉及评估方法学；
- CC 不包括密码算法固有质量的评估。

3.1.3 CC 标准的适用范围

CC 定义了评估信息技术产品和系统安全性所需的基础准则，是度量信息技术安全性的基准。它针对在安全评估过程中信息技术产品和系统的安全功能及相应的保证措施提出一组通用要求，使各种相对独立的安全评估结果具有可比性，有助于信息技术产品和系统的开发者或用户确定产品或系统对其应用而言是否

足够安全，以及在使用中存在的安全风险是否可以容忍。CC 主要保护的是信息的 CIA 三大特性，其次也考虑了可控性、可追溯性等，适用于对信息技术产品或系统的安全性进行评估，不论其实现方式是硬件、固件还是软件，同时还可用于指导产品或系统开发。

3.1.4 CC 标准的目标读者

CC 的主要目标读者是用户、开发者和评估者。

表 2 CC 标准的主要目标读者

用户	**帮助用户定义安全需求** ● 可以用 CC 的结构和语言来定义安全需求；可用评估结果决定一个已评估的产品或系统是否满足他们的安全需求；可用评估结果比较不同的产品或系统；可为系统的使用、运行提供支持。 ● 为用户提供一个独立于实现的框架(PP)，供用户提出对被评估产品或系统的特殊的安全要求。
开发者	**帮助开发者描述产品的安全能力** ● 为开发者在确定其产品或系统所要满足的安全需求方面提供支持； ● 为开发者准备和协助对其产品或系统的评估提供支持； ● 通过评估证实产品或系统的安全功能，保证满足特定的安全需求； ● 标准中提出的安全功能可被开发者在其产品或系统中实现，促进其技术进步； ● 标准中的保证要求可帮助开发者规范其研发、生产和集成等过程，提高生产管理能力。
评估者	**帮助评估者度量产品的置信程度** ● 遵照标准，依据通用评估方法(CEM)对产品或系统的安全性进行评估，以判断产品或系统在安全性方面与标准要求的一致性，实现正确性和有效性，使评估结果具有可重复性和客观性。

3.2 CC 标准中的关键概念

3.2.1 CC 标准中的关键概念

CC 标准中的关键概念主要有以下几个。

(1) 评估对象(Target of Evaluation, TOE)

- 用于安全评估的信息技术产品、系统或子系统（如防火墙、计算机网络、密码模块等），包括相关的管理员指南、用户指南、设计方案等文档。

(2) 保护轮廓(Protection Profile, PP)

PP 是指满足特定用户需求，与一类 TOE 实现无关的一组安全要求。其含义可以理解为：

- 为既定的一类产品或系统提出安全功能和保证要求的完备集合，表达了一类产品或系统的用户需求；
- PP 与某个具体的 TOE 无关，它定义的是用户对这类 TOE 的安全需求；
- 主要内容：需保护的对象、确定安全环境、TOE 的安全目的、IT 安全要求、基本原理；
- 在标准体系中 PP 相当于产品标准（同 TCSEC 级别类似），也有助于过程规范性标准的开发；
- 国内外已对应用级防火墙，包括过滤防火墙、智能卡、IDS、PKI 等开发了相应的 PP。

表 3 PP 的内容结构

1.保护轮廓引言 1.1 PP 标识 1.2 PP 概述	 标识 PP 叙述性概括 PP
2.TOE 描述	TOE 的背景信息
3.安全环境 3.1 假设 3.2 威胁 3.3 组织性安全策略	指明安全问题（要保护的资产、已知的攻击方式、TOE 必须使用的组织性安全策略）
4.安全目的 4.1 TOE 安全目的 4.2 环境安全目的	对安全问题的相应反应（包括非技术性措施）
5.IT 安全需求 5.1 TOE 安全功能需求 5.2 TOE 安全保证需求 5.3 IT 环境安全需求	 CC 第二部分的功能组件 CC 第三部分的保证组件 IT 环境中软件、硬件、固件要求
6.基本原理 6.1 安全目的基本原理 6.2 安全要求基本原理	目的和要求可以解决已指出的安全问题
7.应用注解	附加信息

图 12 某移动设备 PP 的目录

(3) 安全目标(Security Target, ST)

ST 是指作为指定的 TOE 评估基础的一组安全要求和规范。其含义包括：

- ST 针对具体 TOE 而言，它包括该 TOE 的安全要求和用于满足安全要求的特定安全功能和保证措施；
- ST 包括的技术要求和保证措施可以直接引用该 TOE 所属产品或系统类的 PP；

- ST 是开发者、评估者、用户在 TOE 安全性和评估范围之间达成一致的基础；
- ST 相当于产品和系统的实现方案，与 ITSEC 的“安全目标”类似，例如 ST for Oracle v7。

表 4 ST 的内容结构

1.安全目标引言 1.1 ST 标识 1.2 ST 概述 1.3 CC 一致性声明	 标识 ST 和 TOE（包括版本号） 叙述性总结 ST
2.TOE 描述	TOE 的背景信息（评估环境）
3.安全环境 3.1 假设 3.2 威胁 3.3 组织性安全策略	 指明安全问题（要保护的资产、已知的攻击、TOE 必须使用的组织性安全策略、假定的安全问题）
4.安全目的 4.1 TOE 安全目的 4.2 环境安全目的	 对安全问题的相应反应（包括非技术性措施）
5.IT 安全需求 5.1 TOE 安全功能需求 5.2 TOE 安全保证需求 5.3 IT 环境安全需求	 CC 第二部分的功能组件 CC 第三部分的保证组件 IT 环境中软件、硬件、固件要求
6.TOE 概要规范 6.1 TOE 安全功能 6.2 保证措施	 IT 安全功能满足哪一个特定的安全功能需求 IT 保证措施满足哪一个特定的安全保证需求
7.保护轮廓声明 7.1 PP 参照 7.2 PP 裁减 7.3 PP 附加项	 解释、证明和其他支持材料，以证实一致性声明

图 13 某手机产品 ST 的目录

(4) TOE 安全策略(TOE Security Policy, TSP)

控制 TOE 中资产如何管理、保护和分发的规则。

(5) TOE 安全功能(TOE Security Functions, TSF)

必须依赖于 TSP 正确执行的 TOE 的所有部件。

(6) 组件(Component)

组件描述了一组特定的安全要求，是可供 PP、ST 或包选取的最小的安全要求集合。在 CC 中，以“类_子类.组件号”的方式来标识组件。

(7) 包(Package)

- 组件依据某个特定关系的组合，就构成了包；
- 构建包的目的是定义那些公认有用的、对满足某个特定安全目的有效的安全要求；
- 包可以用来构造更大的包、PP 和 ST，并且可以重复使用；
- CC 中有功能包和保证包两种形式。

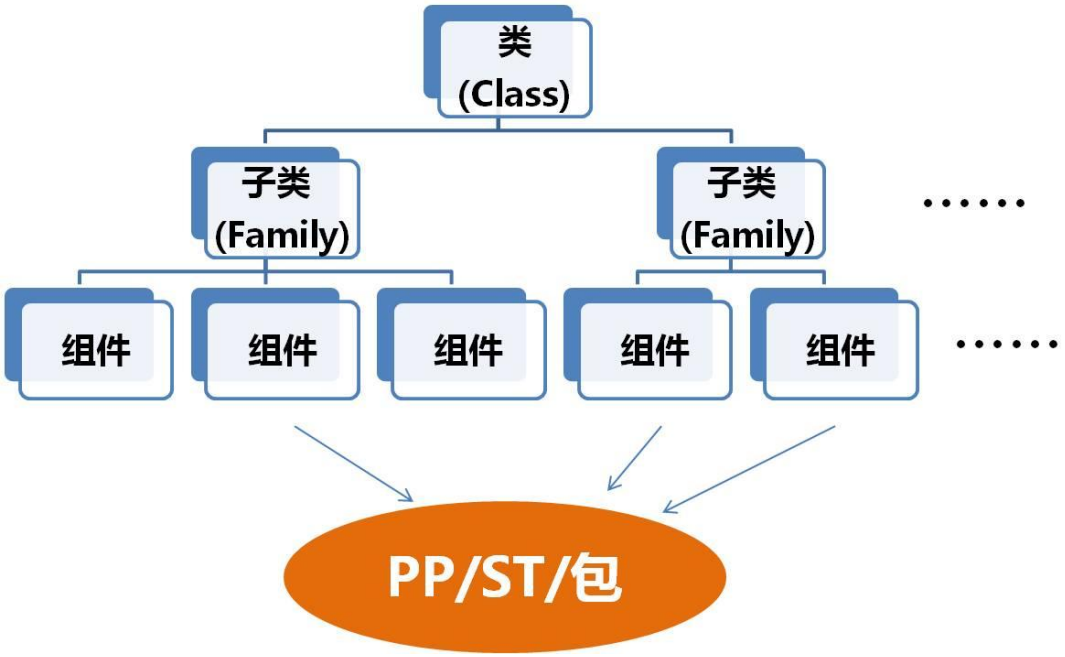


图 14 一些概念之间的关系(1)

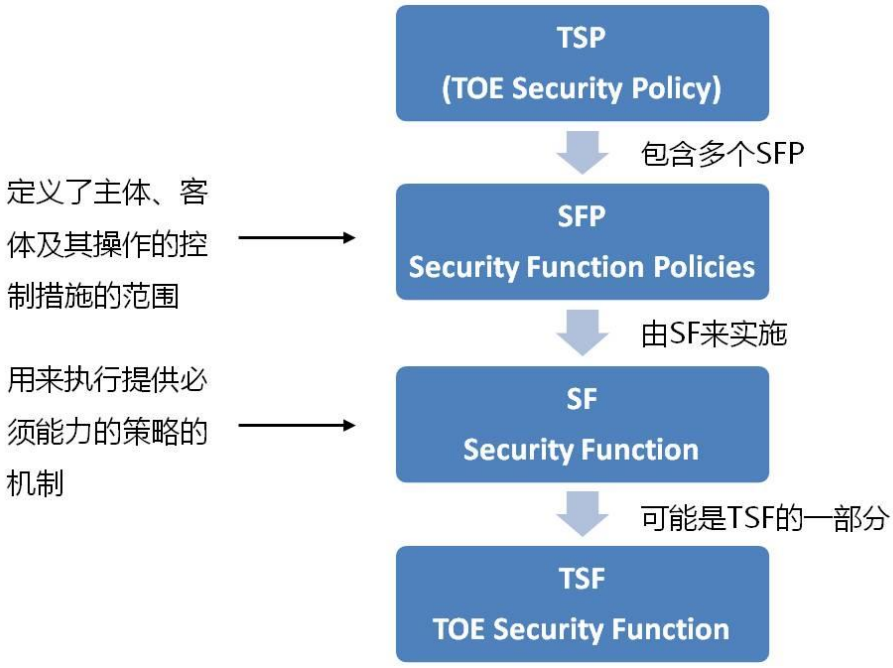


图 15 一些概念之间的关系(2)

3.2.2 TOE、PP、ST 三者的关系

TOE、PP、ST 三者之间的关系如下图所示，PP 相当于行业的一个规范或标准，它是对标整个行业的，表达“要求产品做成什么样子”。ST 是针对具体厂商而言的，表达“产品想做成什么样子”，相当于产品的安全功能说明书。TOE 即产品本身。

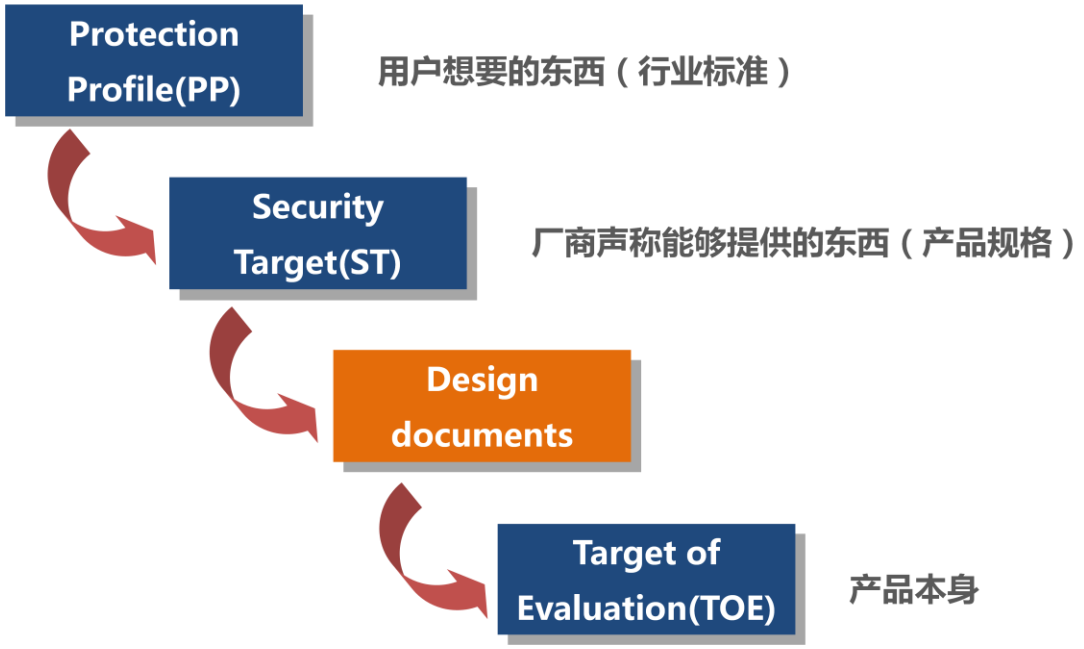


图 16 PP、ST 和 TOE 之间的关系

图 17、图 18 进一步解释了三者的关系。CC 相当于一个标准化的安全需求目录，它并非针对具体的产品，具有较大的灵活性。PP 是指在特定的领域里，用户驱动的安全需求，它是针对具体某一类产品而言的，例如手机要做成什么样子、APP 要做成什么样子，均是用 PP 来规范。有了 PP，用户便可以借助 PP 来定义需求。ST 则是厂商对用户需求作出的响应，它是针对具体某一个产品而言的，例如某品牌手机要做成什么样子，厂商通用 ST 向用户陈述对自身 IT 产品的安全承诺。

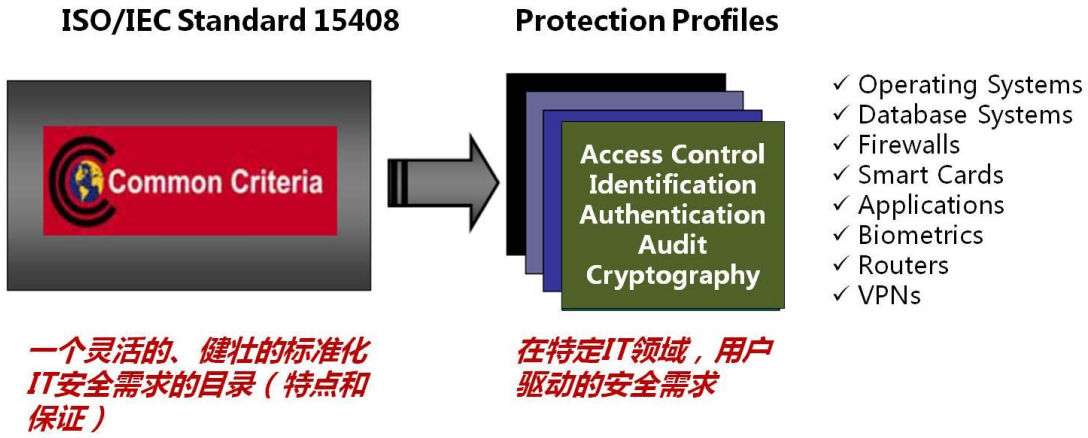


图 17 用户借助 PP 来定义需求

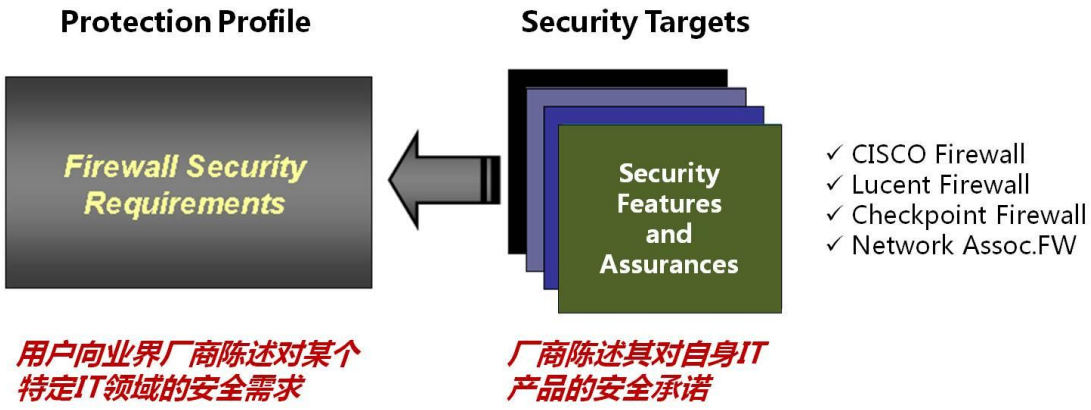


图 18 厂商对用户需求作出响应

3.3 技术要求及标准解读

CC 在标准结构和撰写形式上一共包含三个部分：

第一部分：介绍了 CC 的基本思路和一般模型，定义了评估目标（Target of Evaluation，简称 TOE）、安全目标（Security Target，简称 ST）和保护轮廓（Protection Profile，简称 PP）等重要的基本概念，并且规定了撰写 ST 和 PP 这类文档的格式及要点。

第二部分：详细描述了可供 ST 或 PP 选用的安全功能组件，共分十一个大类，包括安全审计、通信、密码支持、用户数据保护、标识和鉴别、安全管理、隐秘、TSF 保护、资源利用、TOE 访问和可信路径/信道。

第三部分：详细描述了可供 ST 或 PP 选用的安全保证要求。安全保证要求覆盖到对 ST 的评估准则、TOE 的开发、生命周期支持、指导性文档、测试、脆弱性评定在内的六个方面，根据在每个方面安全保障要求的数量多少和松紧程度，该部分中又定义了七个评估保障级（Evaluation Assurance Level，简称 EAL）。

图 19 CC 的内容组织

这三个部分在内容上可以说是唇齿相依、融会贯通、缺一不可的，如果其中任何一个部分被孤立起来，则不能独立地构成一个有任何应用价值的标准，孤立的部分也无法确保产品的安全性能有效地被评估出来。

CC 中最核心的内容是定义了两类安全需求：功能需求和保证需求，分别在 CC 第二部分和第三部分中详细描述。满足 CC 标准要求的产品须同时满足功能需求和保证需求。

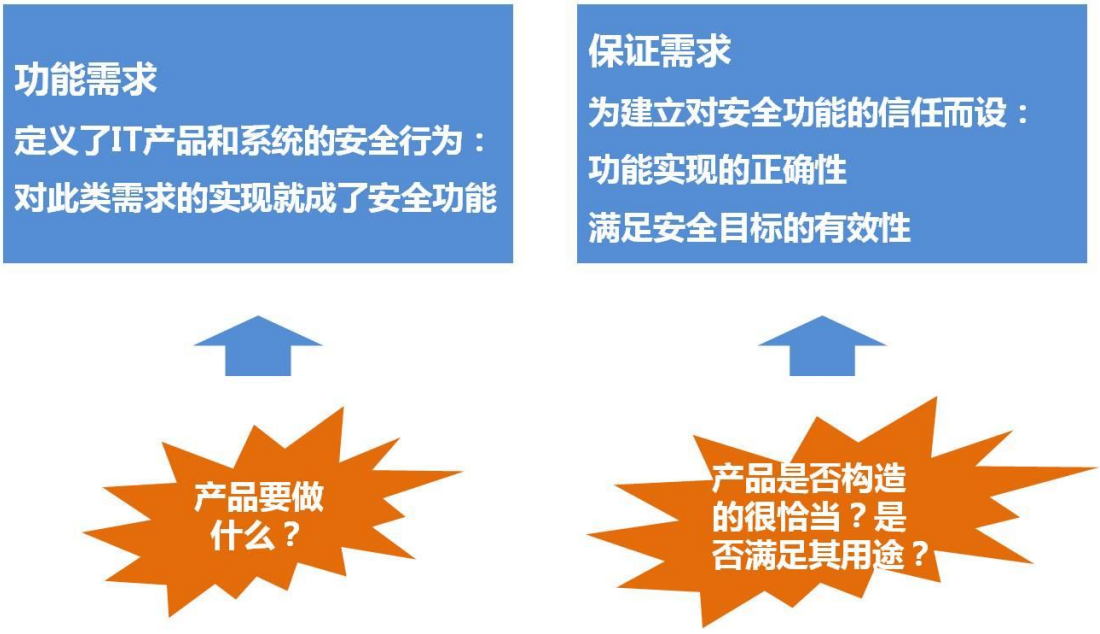


图 20 CC 定义的功能需求和保证需求

在开展 CC 认证时，评估者的主要职责即是评估产品是否满足了对应的功能

要求和保证要求。

3.3.1 CC 标准的第一部分

CC 标准第一部分的内容如下：

1 范围

2 定义

- 常用的缩略语、基本术语

3 概述

- CC 的目标受众
- 评估上下文（评估体制框架）
- CC 的内容组织

4 一般模型

- 一般性的安全上下文关系模型（如图 21），IT 安全上下文
- CC 的途径，安全概念，CC 的描述性材料，评估的类型（评估 PP、ST、TOE）

5 CC 需求和评估结果

- PP 和 ST 的需求，TOE 的需求，关于评估结果

附录 A CC 项目介绍

- CC 的项目背景，CC 的开发，资助 CC 项目的组织

附录 B PP 规范

- 概述
- PP 的内容包括：PP 介绍，TOE 描述，TOE 安全环境，安全目标，IT 安全需求，应用要点

附录 C ST 规范

- 概述
- ST 的内容包括：ST 介绍，TOE 描述，TOE 安全环境，安全目标，IT 安全需求，TOE 概要规范，PP 声明

附录 D 参考书目

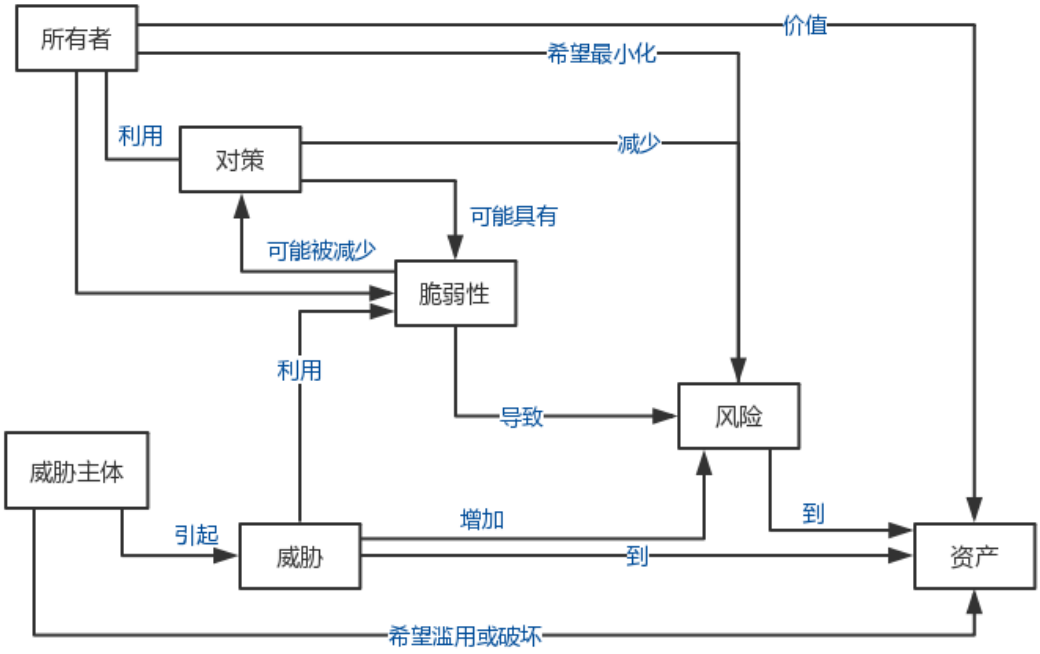


图 21 一般性安全关系模型

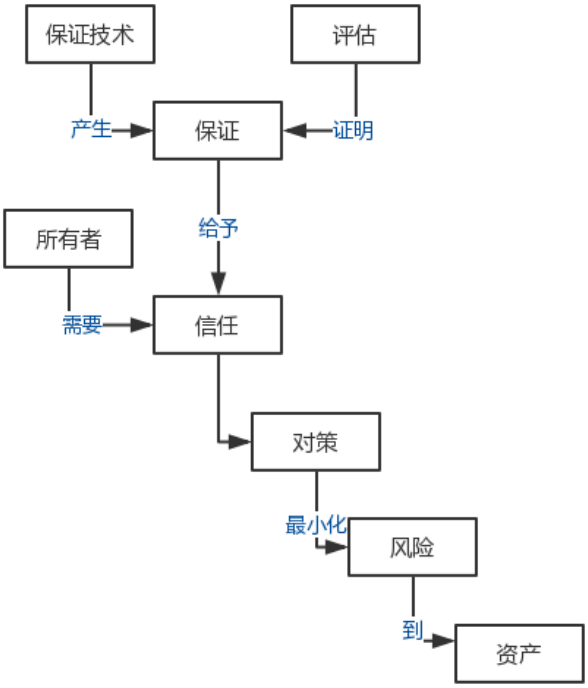


图 22 评估概念及关系

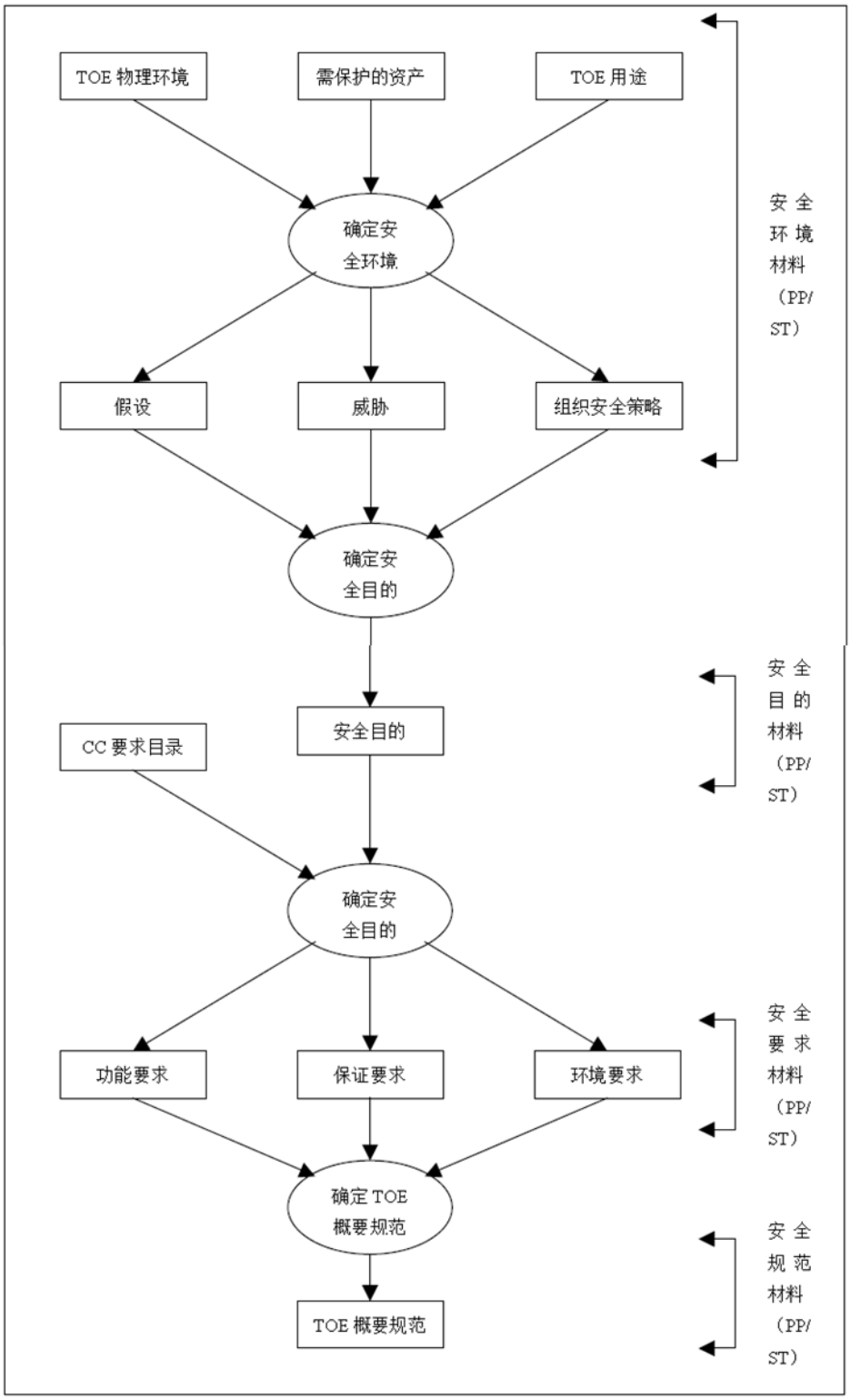

TOE 物理环境
需保护的资产
TOE 用途
确定安全环境
假设
威胁
组织安全策略
确定安全目的
安全目的
CC 要求目录
确定安全目的
功能要求
保证要求
环境要求
确定 TOE 概要规范
TOE 概要规范
安全环境材料（PP/ST）
安全目的材料（PP/ST）
安全要求材料（PP/ST）
安全规范材料（PP/ST）

图 23 要求和规范导出

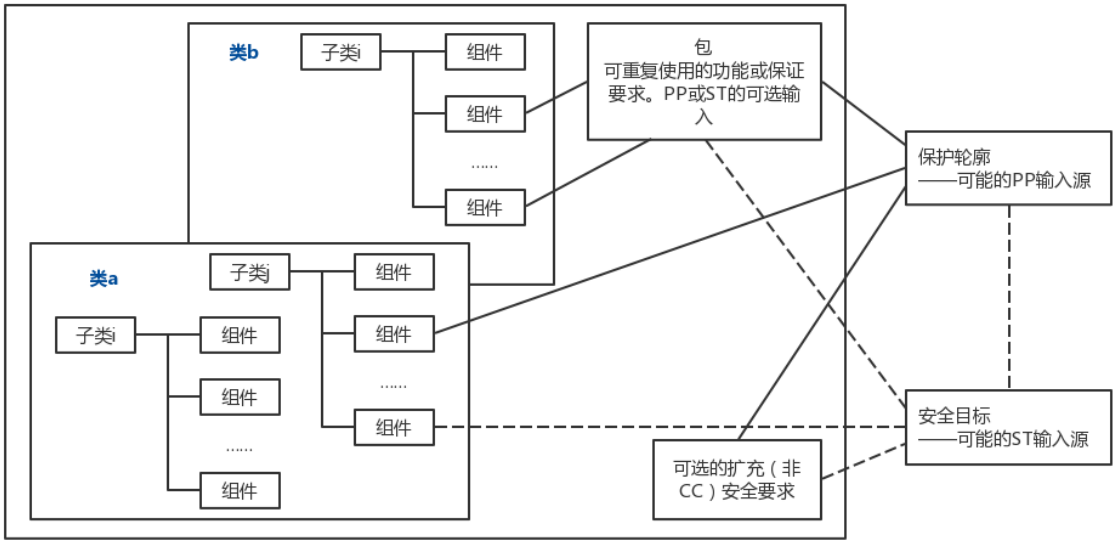


图 24 表达安全需求的各种构造形式

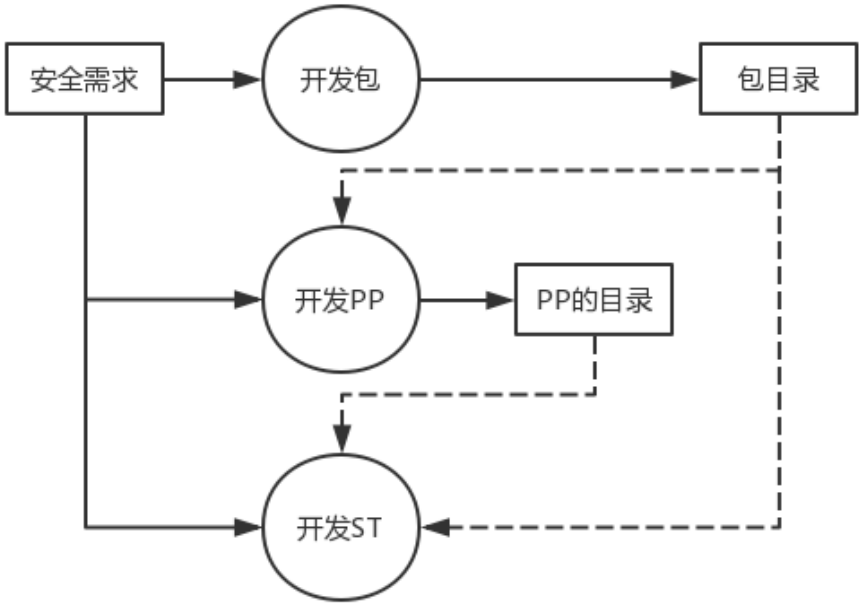


图 25 对安全需求的应用

3.3.2 CC 标准的第二部分

CC 标准第二部分定义了 CC 的安全功能要求。安全功能要求分为 11 类，包括：审计(FAU)、通信(FCO)、密码支持(FCS)、用户数据保护(FDP)、识别和鉴权(FIA)、安全管理(FMT)、隐私(FPR)、TSF 保护(FPT)、资源利用(FRU)、TOE

访问(FTA)和可信路径/通道(FTP)。

CC 标准第二部分的内容如下：

1 范围

2 安全功能组件（Class、Family、Component 的结构，Component catalogue）

3 Class FAU: Security Audit

- 安全审计包括识别、记录、存储和分析那些与安全行为有关的信息。审计记录的检查结果用来判断发生了哪些安全行为，以及哪个用户要对这些行为负责。
- 6 个子类：安全审计自动应答(FAU_ARP)，安全审计数据产生(FAU_GEN)，安全审计分析(FAU_SAA)，安全审计查阅(FAU_SAR)，安全审计事件选择(FAU_SEL)，安全审计事件存储(FAU_STG)

4 Class FCO: Communication

- 用于确保在数据交换中参与方的身份。既确保发送者不能否认，又确保接收者不能否认收到。
- 2 个子类：原发抗抵赖(FCO_NRO)，接收抗抵赖(FCO_NRR)

5 Class FCS: Cryptographic support

- 产品或系统含有密码功能时，将使用密码支持类。
- 2 个子类：密钥管理(FCS_CKM)，密码运算(FCS_COP)

6 Class FDP: User data protection

- 规定了与保护用户数据相关的所有安全功能要求和策略。涉及用户数据输入、输出和存储。
- 13 个子类：访问控制策略(FDP_ACC)，访问控制功能(FDP_ACF)，数据鉴别(FDP_DAU)，输出到 TSF 控制之外(FDP_ETC)，信息流控制策略(FDP_IFC)，信息流控制功能(FDP_IFF)，从 TSF 控制之外输入(FDP_ITC)，TOE 内部传送(FDP_ITT)，残余信息保护(FDP_RIP)，反转(FDP_ROL)，存储数据的完整性(FDP_SDI)，TSF 间用户数据传送的保密性保护(FDP_UCT)，TSF 间用户数据传送的完整性保护(FDP_UIT)

7 Class FIA: Identification and authentication

- 提出了用户身份确定和验证、与 TOE 交互的授权，以及每个授权用户安全属性的正确关联等三方面的安全要求。
- 6 个子类：TSF 功能管理(FMT_MOF)，安全属性管理(FMT_MSA)，TSF 数据管理(FMT_MTD)，撤销(FMT_REV)，安全属性到期(FMT_SAE)，安全管理角色(FMT_SMR)

8 Class FMT: Security Management

- 规定了安全属性、数据和功能三方面的管理，也定义不同管理角色及其相互作用。
- 6 个子类：安全审计自动应答(FAU_ARP)，安全审计数据产生(FAU_GEN)，安全审计分析(FAU_SAA)，安全审计查阅(FAU_SAR)，安全审计事件选择(FAU_SEL)，安全审计事件存储(FAU_STG)

9 Class FPR: Privacy

- 要求为用户提供其身份不被其他用户发现或滥用的保护。
- 4 个子类：匿名(FPR_ANO)，假名(FPR_PSE)，不可关联性(FPR_UNL)，不可观察性(FPR_UNO)

10 Class FPT: Protection of the TSF

- TSF 指的是 TOE 安全功能，TSF 类侧重于保护 TSF 数据，而不是用户数据。
- 16 个子类：根本抽象机测试(FPT_AMT)，失败保护(FPT_FLS)，输出 TSF 数据的可用性(FPT_ITA)，输出 TSF 数据的保密性(FPT_ITC)，输出 TSF 数据的完整性(FPT_ITI)，TOE 内 TSF 数据的传送(FPT_ITT)，TSF 物理保护(FPT_PHP)，可信恢复(FPT_RCV)，重放检测(FPT_RPL)，参照仲裁(FPT_RVM)，域分离(FPT_SEP)，状态同步协议(FPT_SSP)，时间戳(FPT_STM)，TSF 间 TSF 数据的一致性(FPT_TDC)，TOE 内 TSF 数据复制的一致性(FPT_TRC)，TSF 自检(FPT_TST)

11 Class FRU: Resource utilization

- 支持所需资源的可用性。
- 3 个子类：容错(FRU_FLT)，服务优先级(FRU_PRS)，资源分配(FRU_RSA)

12 Class FTA: TOE access

- 规定了用以控制建立用户会话的一些功能要求，是对标识和鉴别类安全要求的进一步补充。
- 6 个子类：可选属性范围限定(FTA_LSA)，多重并发会话限定(FTA_MCS)，会话锁定(FTA_SSL)，TOE 访问旗标(FTA_TAB)，TOE 访问历史(FTA_TAH)，TOE 会话建立(FTA_TSE)

13 Class FTP: Trusted path/channels

- 规定了关于用户和 TSF 之间可信通信路径，以及 TSF 和其他可信 IT 产品间可信通信信道的要求。
- 2 个子类：TSF 间可信信道(FTP_ITC)，可信路径(FTP_TRP)

附录 A 安全功能需求应用要点

附录 B

……

……　对 11 个功能类及其子类、具体需求点的详细解释

……

附录 M

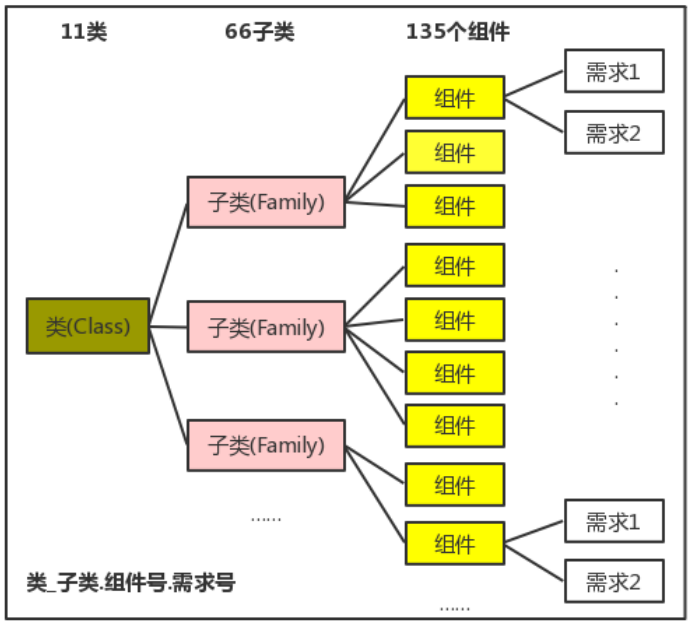


图 26 安全功能需求层次关系

序号	安全功能	解析举例
1	安全审计类	操作记录下的行为日志等，不可擦除
2	通信类	主要是身份的真实性和抗抵赖性，如设备之间的通信是如何保证安全的（仅针对被测设备自己开发的通信链路之间）
3	密码支持类	如何实现加密的，加密机制是否可信赖，如FIPS
4	用户数据保护类	如何实现用户数据的保护，如通话时长、计费结果
5	标识和鉴别类	给管理员等用户身份提供识别标志
6	安全管理类（与TSF有关的管理）	安全功能本身的管理方式，如权限设置
7	隐私类（保护用户隐私）	个人信息的保护机制，如GDPR要求的隐私数据保护
8	TSF保护类（TOE自身的安全保护）	设备自检自校等
9	资源利用类	资源管理角度如何确保系统安全，如内存泄漏
10	TOE访问类	为确保安全，对TOE的访问控制机制
11	可信路径\信道类	可信通道

图 27 CC 安全功能解析

3.3.3 CC 标准的第三部分

CC 标准第三部分定义了 CC 的安全保证要求。安全保证要求分为 10 类，即保护轮廓评估(APE)、安全目标评估(ASE)、配置管理(ACM)、交付和运行(ADO)、开发(ADV)、指导性文档(AGD)、生命周期支持(ALC)、测试(ATE)、脆弱性评估(AVA)和保障维护(AMA)。

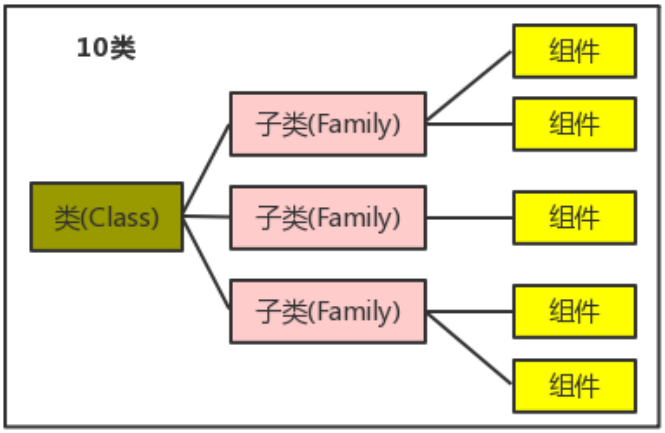


图 28 安全功能需求层次关系

CC 标准第三部分的内容如下：

1 范围

2 安全保证需求

- Class、Family、Component、EAL 的结构
- 组件分类，PP 和 ST 评估标准类结构，保证分类，维护分类

3 PP 和 ST 评估标准

- PP 和 ST 是评估 TOE 及其功能和保证需求的基础，在评估 TOE 之前需要证明 PP 和 ST 对 TOE 评估来说是否适用，即确定 PP 和 ST 是否完整、一致、技术上可靠，以至于适合用作一个或多个待评估 TOE 的需求声明。
- 用以下两个类来规范对 PP 和 ST 的评估。

4 Class APE: Protection Profile evaluation

- 该类相当于规范了对产品或系统标准的评审，评估过的 PP 可进一步到权威机构注册并发布。
- 该类提出了 TOE 描述、安全环境、安全目的和安全需求等方面的评估要求。

5 Class ASE: Security Target evaluation

- 提出了 TOE 描述、安全环境、安全目的、PP 声明、安全需求和 TOE 概要规范等方面的评估要求。

6 评估保证等级

- 一个保证等级(EAL)是评估保证要求的一个基线集合——保证包。每一评估保证级定义一套一致的保证要求，合起来构成一个预定义 CC 保证级尺度。CC 定义了 7 个递增的评估保证等级。

7 保证类、子类和组件

- 保证系指对功能产生信心的方法。保证要求包含开发者行为、产生的证据以及评估者行为。
- 以下 7 个保证类，确保安全功能在 TOE 的整个生命周期中正确有效地实施，这些保证类是定义评估保证等级的基础，是具体 TOE 评估的依据和准则。

8 Class ACM: Configuration Management

- 通过跟踪 TOE 的任何变化，确保所有修改都已授权，以保证 TOE 的完整性。特别是，通过配置管理确保用于评估的 TOE 和相关文档正是预先所准备的那份。
- 3 个子类：配置管理自动化(ACM_AUT)，配置管理能力(ACM_CAP)，配置管理范围(ACM_SCP)

9 Class ADO: Delivery and Operation

- 该类规定了 TOE 交付、安装、生成和启动方面的措施、程序和标准，以确保 TOE 所提供的安全保护在这些关键过程中不被泄漏。
- 2 个子类：交付(ADO_DEL)，安装、生成和启动(ADO_IGS)

10 Class ADV: Development

- 该类涉及将 ST 中定义的 TOE 概要规范细化为具体的 TOE 安全功能(TSF)实现，以及安全要求到最低级别表示之间的映射两个方面。
- 7 个子类：功能规范(ADV_FSP)，高层设计(ADV_HLD)，实现表示(ADV_IMP)，TSF 内部(ADV_INT)，低层设计 (ADV_LLD)，表示对应性(ADV_RCR)，安全策略模型(ADV_SPM)

11 Class AGD: Guidance documents

- 规定用户指南和管理员指南编写方面的要求。
- 2 个子类：管理员指南(AGD_ADM)，用户指南(AGD_USR)

12 Class ALC: Life cycle support

- 在 TOE 开发和维护阶段，对相关过程进一步细化并且建立相应的控制规则，

以确保 TOE 与其安全要求之间的符合性。

- 4 个子类：开发安全(ALC_DVS)，缺陷纠正(ALC_FLR)，生命周期定义(ALC_LCD)，工具和技术(ALC_TAT)

13 Class ATE: Tests

- 测试关心的是 TOE 是否满足其安全功能要求。
- 4 个子类：覆盖范围(ATE_COV)，深度(ATE_DPT)，功能测试(ATE_FUN)，独立性测试(ATE_IND)

14 Class AVA: Vulnerability assessment

- 该类定义了与识别可利用的脆弱性相关的安全要求，这些脆弱性可能在开发、集成、运行、使用和配置时进入 TOE。
- 3 个子类：隐蔽信道分析(AVA_CCA)，误用(AVA_MSU)，TOE 安全功能强度(AVA_SOF)

15 保证维护范例

- 保证维护的目的是确保 TOE 或其环境发生变化时，还能继续满足安全目标。
- 对保证进行维护的一种方法是再次评估 TOE，但势必增加开销。
- CC 通过 AMA 类定义一套要求，确保有关保证都得到维护，而不需要全面再评估。

16 Class AMA: Maintenance of assurance

- 该类提出的要求必须在 TOE 通过 CC 认证之后才适用，这些要求旨在确保 TOE 或其环境变更后，继续满足安全目标。
- 4 个子类：保证维护计划(AMA_AMP)，TOE 组件分类报告(AMA_CAT)，保证维护证据(AMA_EVD)，安全影响分析(AMA_SIA)

附录 A 保证组件依从性交叉引用

附录 B EALs 及保证组件交叉引用

评估保证级(EAL)

(1) EAL1：功能测试

- 基础级别的安全保障；
- 适用于对正确运行需要一定信任的场合，对该场合的安全威胁应视为并

不严重；

- 依据一个规范的独立性测试和对所提供指导性文档的检查来为用户评估 TOE。没有开发者帮助也能评估，通过评估，可以确信 TOE 的功能与其文档在形式上是一致的，且对已标识的威胁提供了有效的保护。

(2) EAL2：结构测试

- 增加开发者测试及脆弱性分析和基于 TOE 规范的独立性测试来实现 EAL1 更高级别的安全保障；
- 功能和接口的规范、指导性文档和 TOE 的高层设计的评估分析；
- 要求开发者递交设计信息和测试结果，但不需要开发者增加过多费用或时间投入；
- 评估证据包括安全功能的独立性测试、开发者自测结果的确认、功能强度分析、脆弱性报告、TOE 的配置表和安全交付程序；
- 适用于：在缺乏现成可用的完整的开发记录时，开发者或用户需要一种低等到中等级别的独立保证的安全性。

(3) EAL3：系统地测试和检查

- 增加更完备的安全功能测试及提供开发过程中不会被篡改的可行性机制或程序来实现 EAL2 更高级别的安全保障；
- EAL3 级需要在 EAL2 的基础上增加开发环境现场核查，核查配置管理、开发过程管理、交付过程管理等；
- 适用于：开发者或用户需要一个中等级别的独立保证的安全性，且在不带大量重建费用的情况下，对 TOE 及其开发过程进行彻底审查。

(4) EAL4：系统地设计、测试和复查

- 增加更多的设计描述、实现的子集，以及提供开发或交付过程中不会被篡改的可信性改进机制或程序来实现 EAL3 更高级别的安全保障；

- 在 EAL3 的基础上增加对抵御攻击的能力的独立脆弱性分析、开发环境控制措施如自动化的额外的配置管理和安全交付程序、源码审查；
- 需要分析 TOE 模块的低层设计和实现的子集；
- 适用于：开发者或用户对传统的商品化的 TOE 需要一个中等到高等级别的独立保证的安全性，并且准备负担额外的安全专用工程费用。

(5) EAL5：半形式化设计和测试

- 需要分析所有的实现，还需要额外分析功能规范和高层设计的形式化模型和半形式化表示和论证；
- 适用于：开发者和使用者在有计划的开发中，采用严格的开发手段，以获得一个高级别的独立保证的安全性，不会因采取专业性安全工程技术而增加一些不合理的开销。

(6) EAL6：半形式化验证的设计和测试

- 适用于在高风险环境下的特定安全产品或系统的开发，且要保护的资源值得花费一些额外的人力、物力和财力。

(7) EAL7：形式化验证的设计和测试

- 适用于一些安全性要求很高的 TOE 开发，这些 TOE 将应用在风险非常高的地方，或者所保护资产的价值很高的地方；
- 目前，该级别的 TOE 比较少，一方面是对安全功能全面的形式化分析难以实现，另一方面在实际应用中也很少有这类需求。

序号	认证级别定义	基本解析
EAL 1	•功能测试	•验证相关安全功能
EAL 2	•结构测试	•即白盒测试，从程序的控制结构导出测试用例
EAL 3	•系统地测试和检查	•系统性地测试和代码审查
EAL 4	•系统地设计、测试和复查	•系统性地设计、测试和代码审查
EAL 5	•半形式化设计和测试	•用确定语义和严格语法的语言逻辑来进行程序设计，确保安全并进行完整的安全测试。
EAL 6	•半形式化验证的设计和测试	•用确定语义和严格语法的语言逻辑来验证程序设计的安全性，证明它能得到预期的结果，并测试。
EAL 7	•形式化验证的设计和测试	•用具有确定语义的语言逻辑（建立在公认的数学概念上）来验证程序设计的安全性，证明它能得到预期的结果，并测试。

图 29 CC 评估保证等级基本解析

注：

- 形式化规范就是用一套基于明确定义的数学概念的符号来书写，并且通常伴随着支持性的解释（非形式化）语句。这些数学概念被用来定义符号的句法和语义，以及支持逻辑推理的证明规则。支持形式化符号的句法和语义规则应该定义如何明确地识别其结构和确定其含义，并且必须有证据表明矛盾不可能产生，支持符号的所有规则都有定义或者引用。
- 半形式化规范就是用一种受限制的句法语言来书写，并且通常伴随着支持性的解释（非形式化）语句。这里的受限制句法语言可以是一种带有受限制句子结构和具有特殊意义的关键字的自然语言，也可以是图表式的（如：数据流图、状态转换图、实体关系图、数据结构图、流程或程序结构图）。不论基于图表还是自然语言必须用一套规范来定义句法限制。
- 非形式化规范就是像散文一样用自然语言来书写。在这里使用自然语言作为任何普通口头语言（如：荷兰语、英语、法语、德语）中意思的沟通。非形式化规范不像常规语言的传统用法（如：文法和句法）一样受一些符号或特殊的限制。虽然没有符号限制，非形式化规范也要求为上下文中的术语定义其意思，除非作为常规用法已认可。

信息安全产品分级评估是指依据 CC 标准，综合考虑产品的预期应用环境，通过对信息安全产品的整个生命周期，包括技术，开发、管理、交付等部分进行全面的安全性评估和测试，验证产品的保密性、完整性和可用性程度，确定产品对其预期应用而言是否足够安全，以及在使用中隐含的安全风险是否可以容忍，产品是否满足相应评估保证级的要求。等级越高，表示通过认证需要满足的安全保证要求越多，系统的安全特性越可靠。需要注意的是，EAL 不衡量系统本身的安全性，只表示测试的严格程度[3]。

各评估保证等级所含组件	保证类	保证子类	EAL保证组件						
			EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
	配置管理	ACM_AUT				1	1	2	2
		ACM_CAP	1	2	3	4	4	5	5
		ACM_SCP			1	2	3	3	3
	交付和运行	ADO_DEL		1	1	2	2	2	3
		ADO_IGS	1	1	1	1	1	1	1
	开发	ADV_FSP	1	1	1	2	3	3	4
		ADV_HLD		1	2	2	3	4	5
		ADV_IMP				1	2	3	3
		ADV_INT					1	2	3
		ADV_LLD				1	1	2	2
		ADV_RCR	1	1	1	1	2	2	3
		ADV_SPM				1	3	3	3
	指导性文档	AGD_ADM	1	1	1	1	1	1	1
		AGD_USR	1	1	1	1	1	1	1
	生命周期支持	ALC_DVS			1	1	1	2	2
		ALC_FLR							
		ALC_LCD				1	2	2	3
		ALC_TAT				1	2	3	3
	测试	ATE_COV		1	2	2	2	3	3
		ATE_DPT			1	1	2	2	3
		ATE_FUN		1	1	1	1	2	2
		ATE_IND	1	2	2	2	2	2	3
	脆弱性评估	AVA_CCA					1	2	2
		AVA_MSU			1	2	2	3	3
		AVA_SOF		1	1	1	1	1	1
		AVA_VLA		1	1	2	3	4	4

7个EAL等级是递增的关系，这一种递增靠替换成同一保证子类中的一个更高级别的保证组件（即增加严格性、范围和深度）和添加另外一个保证子类的保证组件（如添加新的要求）来实现

图 30 各评估保证等级所含组件

[3] 附件 5 为 ELA3 的基本要求实例

表 5 CC 的 EAL 与其他标准等级的比较

CC	中国 GB17859	美国 TCSEC	美国 FC	加拿大 CTCPEC	欧洲 ITSEC
EAL1		D	-	-	-
EAL2	第一级：用户自主保护级	C1	-	-	E1
EAL3	第二级：系统审计保护级	C2	T-1	T-1	E2
EAL4	第三级：安全标记保护级	B1	T-2	T-2	E3
-		-	T-3	T-3	-
-		-	T-4	-	-
EAL5	第四级：结构化保护级	B2	T-5	T-4	E4
EAL6	第五级：访问验证保护级	B3	T-6	T-5	E5
EAL7		A1	T-7	T-6	E6
-		-	-	T-7	-

表 6 安全保证需求总结

1 个 PP 和 ST 评估类	用来证明 PP 和 ST 对 TOE 评估是否适用，是评估 TOE 的前提和基础。
7 个评估保证类	安全保证需求的主体，是定义评估保证等级的基础，是具体 TOE 评估的依据和准则。
1 个保证维护类	适用于 TOE 通过 CC 认证之后，确保 TOE 或环境变化时，还能继续满足安全目标。

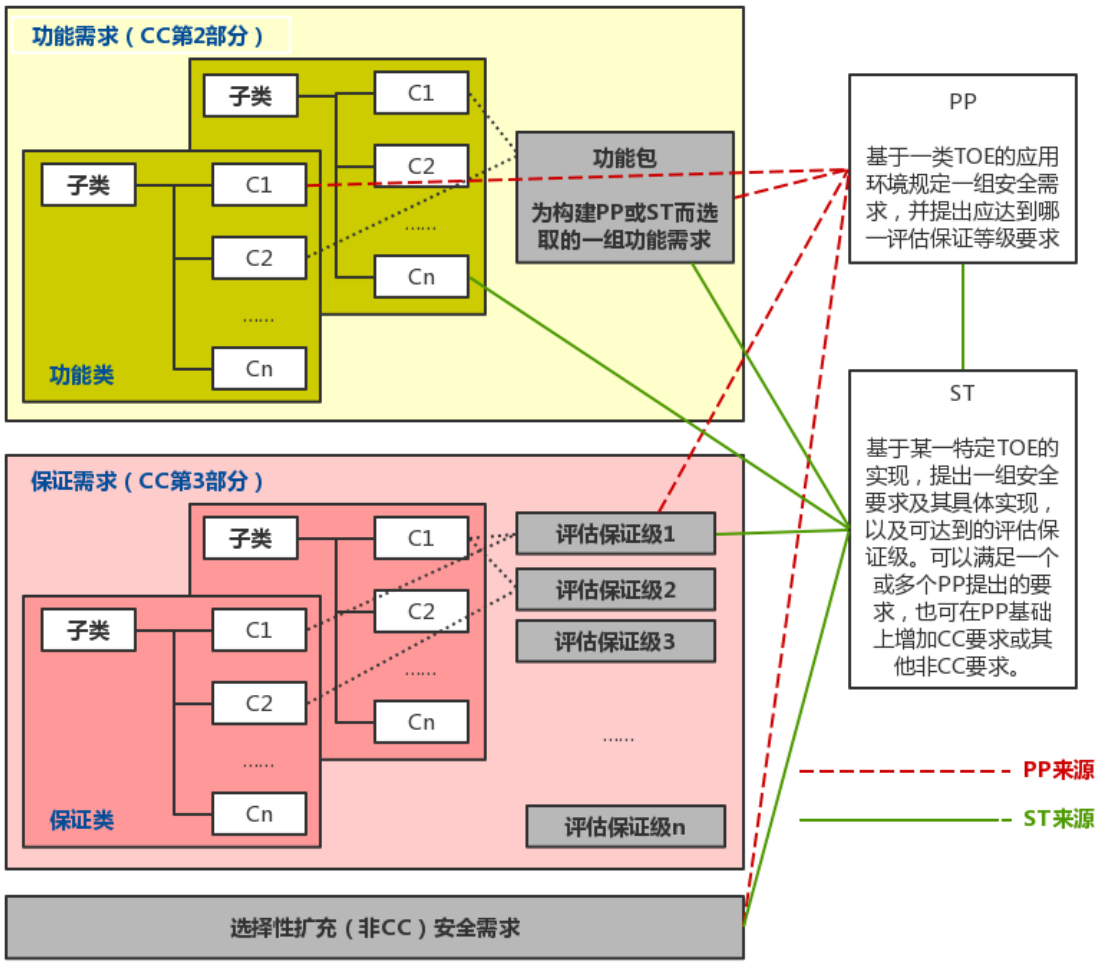


图 31 CC 总体结构

3.4 安全评估

3.4.1 安全评估框架

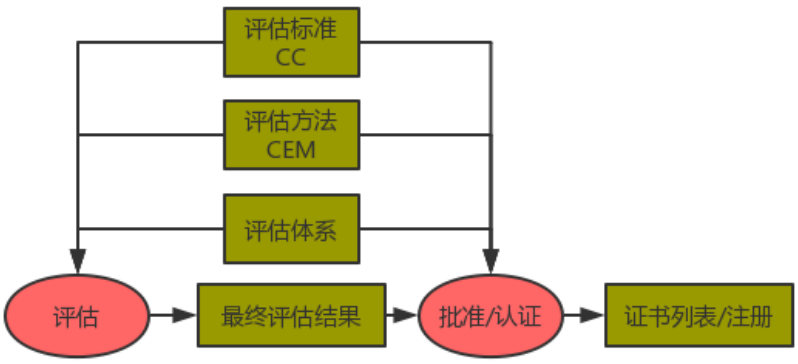


图 32 安全评估框架模型

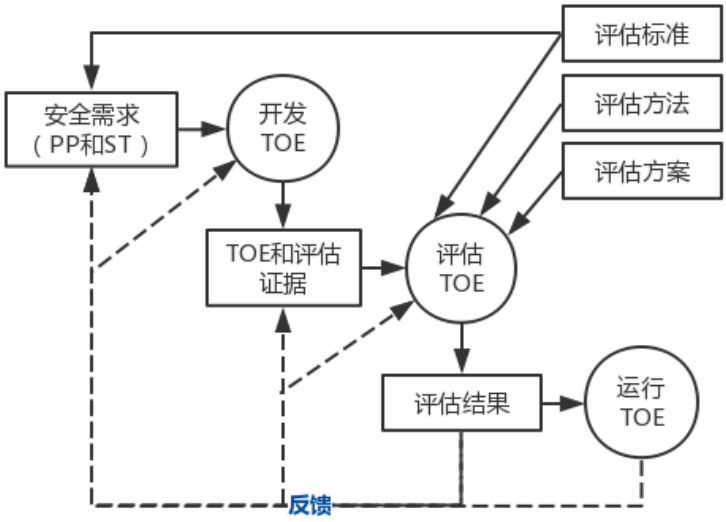


图 33 TOE 评估过程

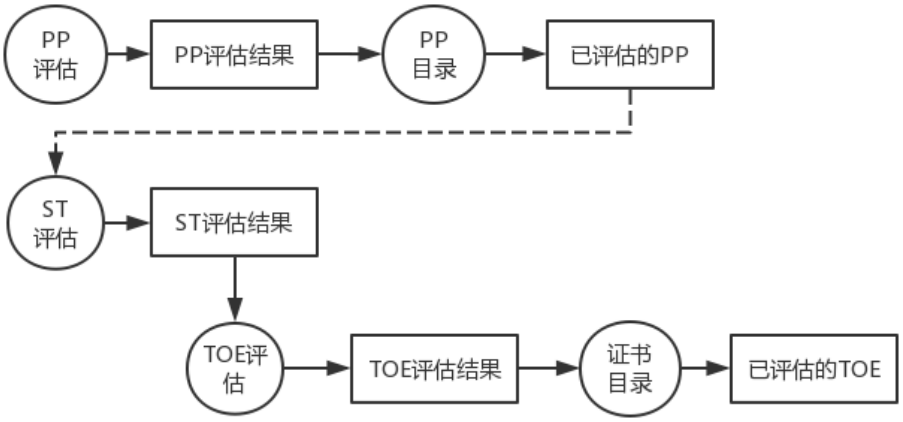


图 34 PP、ST 和 TOE 评估的关系

3.4.2 安全评估方法

通用评估方法(Common Evaluation Methodology, CEM)是为 CC 评估而开发的一种国际公认方法，支撑着信息安全评估的国际互认。它主要是针对评估者而开发的，其他团队（开发者、监督者等）也可从 CEM 中得到一些有用的信息。

PP 开发者（一组用户代表或 IT 产品的一个制造商）使用 CEM，有利于在执行 PP 评估的一致性和独立性方面证实 PP 方面的应用。

TOE 开发者（产品制造商、系统集成商或其他解决方案提供者）使用 CEM，

有利于：

- 在 PP 和 ST 中，文档化提出的安全特性可被独立地证实和验证；
- 开发者的顾客将更容易确信 TOE 提供了所声称的安全特性；
- 评估后的产品在所组成的安全系统中可以更有效地使用。

评估发起者（启动一个评估的组织实体，可以是开发者或顾客）把 CEM 用于以文档形式提出 TOE 的安全特性，并要求评估者独立地证实和验证。评估者使用 CC 时要与 CEM 一致。

监督者是确保所进行的评估过程与 CC、CEM 一致性的实体。

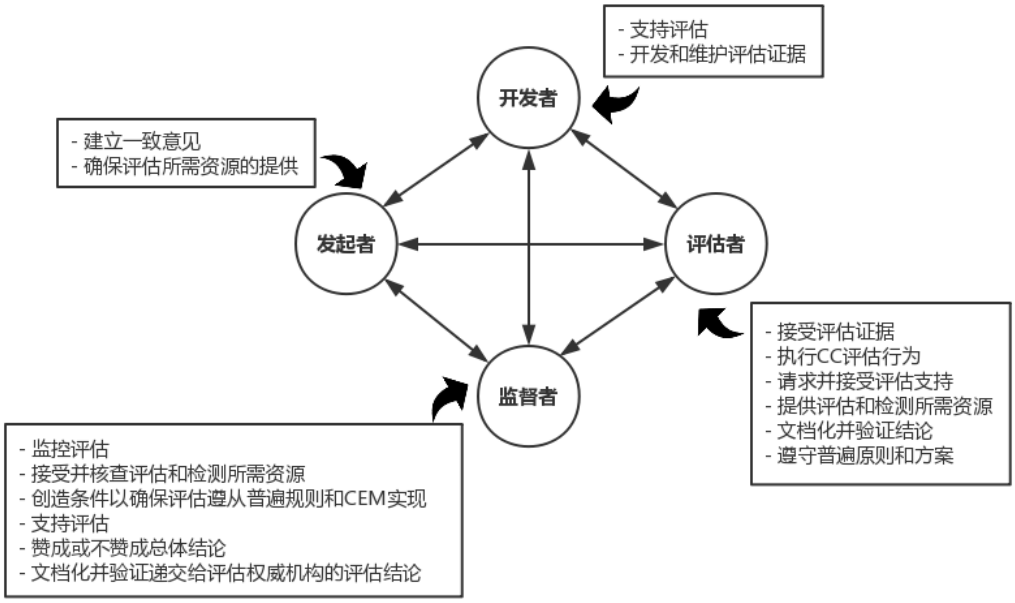


图 35 评估的角度和职责的关系

评估的普遍原则包括：

(1) 适当性原则：为达到一个预定的保证级所采取的评估活动应该是适当的。

(2) 公正性原则：所有的评估应当没有偏见。

(3) 客观性原则：应当在最小主观判断或主张的情形下，得到评估结果。

(4) 可重复性和可再现性原则：依照同样的要求，使用同样的评估证据，对同一 TOE 或 PP 的重复评估应该导出同样的结果。

(5) 结果完善性原则：评估结果应当是完备的并且采取的技术恰当。

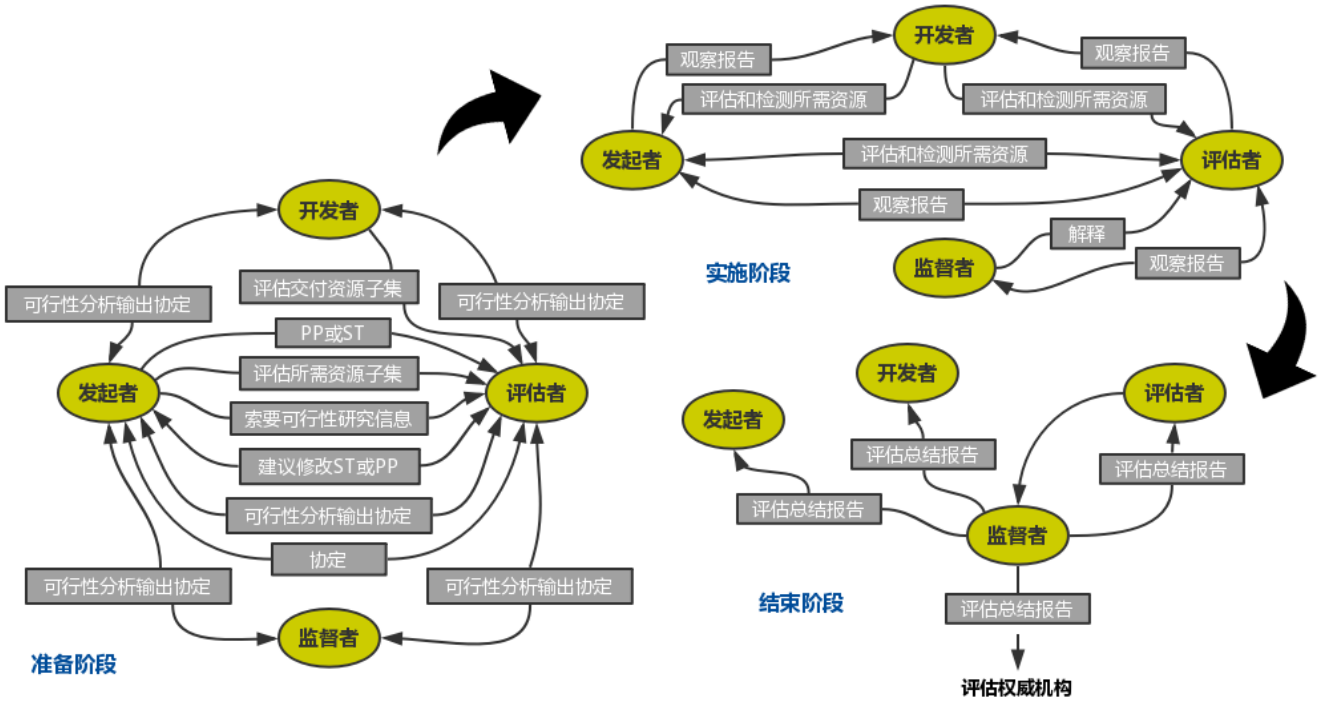


图 36 评估过程概述

3.5 认证流程

3.5.1 CC 认证基本流程

如图 37 为美国 CC 认证的基本流程（实际上不同国家的流程会有所差异），首先是厂商向 CCEVS 提出申请，此处 CCEVS（通用准则评估与认证制度）是对美国信息技术安全性评估与认证的一项基本制度，这项制度由美国国家信息安全保障合作组织(NIAP)负责运行与管理。

CCEVS 受理申请后下发至授权实验室，由实验室负责实际测评工作，整个测评过程由实验室完成，过程中 CCEVS 负责监督工作。美国 CC 认证流程与国内 CCC 认证类似，不同的是 CC 认证需要定期召开过程会议，周期为一至两个月一次，会议上将由实验室讲述评估进程，比如测评过程进行到了哪一个步骤，发现了哪些不符合项等，对于不符合项，厂商需要进行补充，如针对不符合项做

了哪些处理，如何去改进，直到 CCEVS 确认通过，才能进行下一步流程。

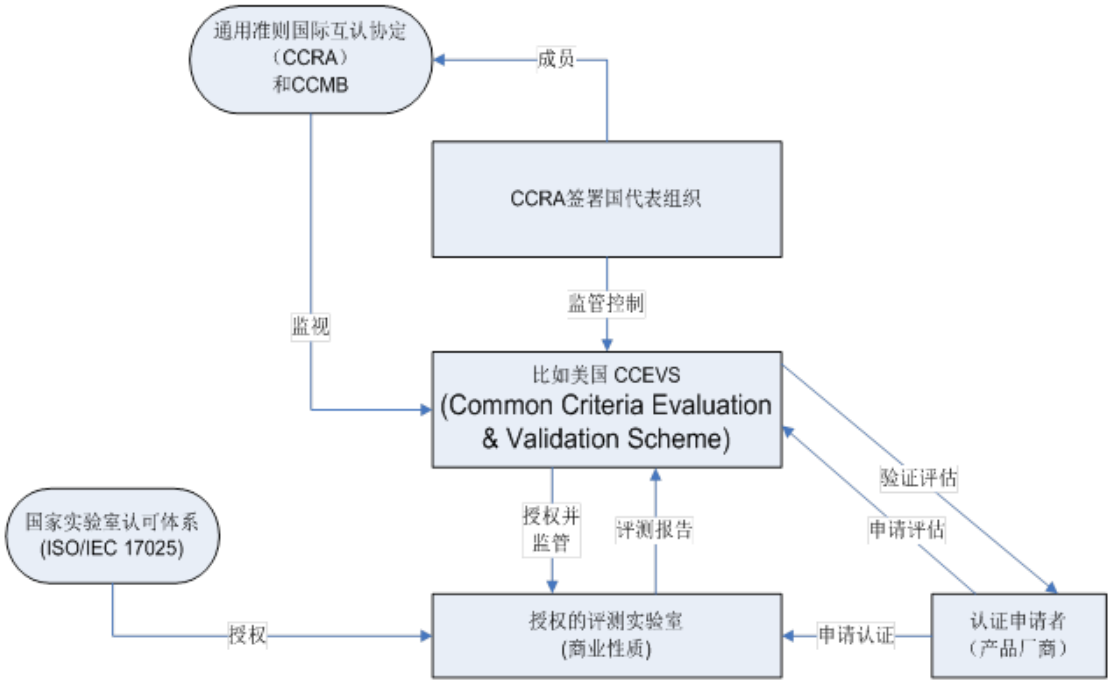


图 37 美国 CC 认证流程

更详细的 CCEVS 认证可参考附件 4——美国 CCEVS 认证要点解读。

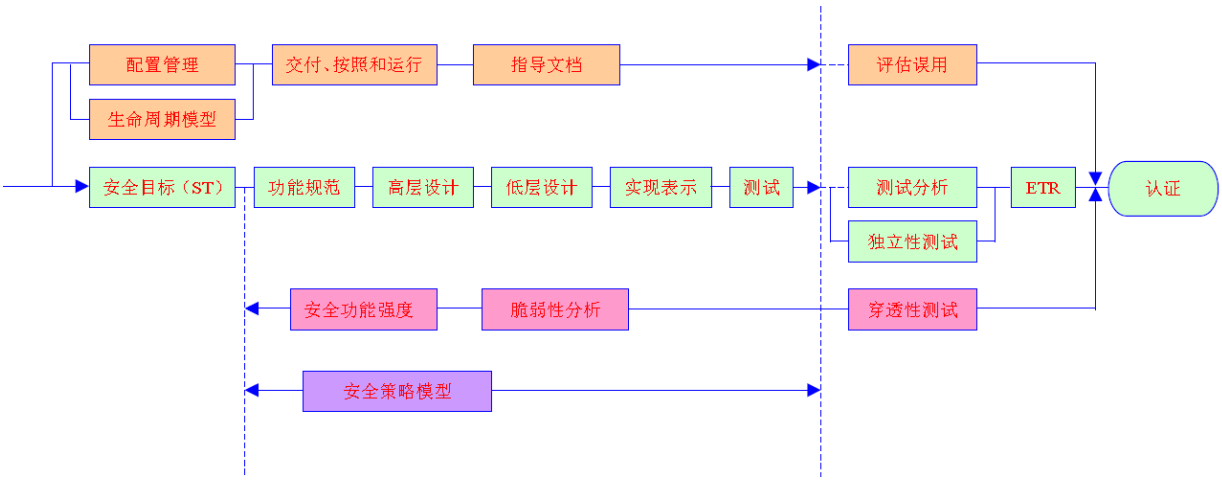


图 38 认证的主要过程

3.5.2 CC 认证要点

CC 评估的两个关键步骤：

第一步：评估 ST

- ST 可以遵从于某个保护轮廓 PP，也可以没有遵从的保护轮廓而是针对某个特定产品撰写；
- ST 的制定应符合 CC 标准的第一部分一般威胁模型的方法；
- 如果 ST 实现了所要求的安全功能组件，并且这些功能的设计和实现是达到了所要求的安全保障级别，那么从理论（即 CC 的理想）上讲此产品有能力抵御来自所处环境的威胁，因而能够有效保护所拥有的信息资产。

第二步：评估 TOE

- 这一步的评估要点在于通过对产品的设计文档、代码实现、生产流程、使用安装、功能测试、脆弱性分析等等多个角度和方面来衡量判定此产品是否真正地实现了在其 ST 中所宣称的安全功能，是否真正地达到了所宣称的安全保障级；
- ST 中指定的安全保障级中包含的安全保障要求，将贯彻覆盖到所选用的全部的安全功能组件。

图 39-图 42 为 CC 常见保障级别的评审要求，企业可根据此来了解 CC 评估的基本内容。从图中可以看出，每一级的评审要求均是从 CC 的六大保障类别，即开发类、指导性文档类、生命周期支持类、安全目标类、测试类、脆弱性分析类这六大维度出发，来描述不同级别的组件要求，级别越高，要求越多且越详细。

Assurance Class	Assurance components
ADV: Development	ADV_FSP.1 Basic functional specification
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.1 Labelling of the TOE
	ALC_CMS.1 TOE CM coverage
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.1 Security objectives for the operational environment
	ASE_REQ.1 Stated security requirements
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_IND.1 Independent testing - conformance
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey

图 39 EAL1 保障级别评审要求

Assurance Class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.2 Use of a CM system
	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_DEL.1 Delivery procedures
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

图 40 EAL2 保障级别评审要求

Assurance Class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.3 Functional specification with complete summary
	ADV_TDS.2 Architectural design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.3 Authorisation controls
	ALC_CMS.3 Implementation representation CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

图 41 EAL3 保障级别评审要求

Assurance Class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Basic modular design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.3 Focused vulnerability analysis

图 42 EAL4 保障级别评审要求

CC 认证的关键活动：

1. Pre-Assessment

首先是预评估，这不属于正式评估的一部分，涉及到第三方认证机构的介入，由他们来评估公司的产品是否符合认证的条件、还有哪些差距等。

- 了解产品及公司现状；
- 评估 CC 的适用性及差距。

2. Document Preparation

接下来即是大量的文档准备工作，如 ST 和各大保障类别的文档准备，该步骤实际上是准备证据的过程，即提供大量的文档以证明公司在安全保障方面满足了产品安全的相关要求。

认证活动中最主要的一项工作就是提交并修订各类认证文档。认证所需的文档会根据所申请的 EAL 级别的不同而略有不同，但是一些常见的文档，如功能规范、高层设计、低层设计等文档都是需要的。

3. Kick-off meeting

在启动会中，认证机构、实验室、开发者三方需签订保密协议，然后进行项目开题，需要厂商对产品展开陈述，如介绍其安全架构、安全功能等。

- NDA；
- 承诺书；
- 项目开题-产品陈述。

4.测试评估

- TOE 样品测试

TOE 的样品测试需要较长的时间，测试的依据就是提交的各类文档。

- 现场审查

通过查阅文件和记录、现场观察和询问等方式进行现场审核。

- Progress Meeting

-测评过程中需要定期召开过程会议，对测评过程进行报告；

-认证官监督的评审。

5. Close Meeting

- 结案评审
- 报告结果

6. Certificate Release

- 签发证书
- 上传官网

CC 认证最终交付的成果包括：测试报告和证书，如图所示。

图 43 CC 认证测试报告示例

National Information Assurance Partnership

Common Criteria Certificate

is awarded to

Samsung Electronics Co., Ltd.

for

Samsung Galaxy Devices on Android 8

The IT product identified in this certificate has been evaluated at an accredited testing laboratory using the Common Methodology for IT Security Evaluation (Version 3.1) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1). This certificate applies only to the specific version and release of the product in its evaluated configuration. The product's functional and assurance security specifications are contained in its security target. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

Date Issued: 2018-05-29

Validation Report Number: CCEVS-VR-VID10898-2018

CCTL: Gossamer Security Solutions

Assurance Level: PP Compliant

Protection Profile Identifier:
PP-Module for VPN Client Version 2.1
Protection Profile for Mobile Device Fundamentals Version 3.1
Extended Package for Wireless LAN Client Version 1.0

Original Signed By
Director, Common Criteria Evaluation and Validation Scheme
National Information Assurance Partnership

Original Signed By
Deputy National Manager National Security Systems
National Security Agency

图 44 CC 认证证书示例

3.5.3 CC 认证机构和实验室

	认证机构	测评实验室举例
澳大利亚	AISEP Aca.certifications@defence.gov.au	CSC, BAE
加拿大	CSE: ccs-sccc@cse-cst.gc.ca	EWA, LightShip, CGI IT
法国	ANSSI: certification@ssi.gouv.fr	AMOSSYS, OPPIDA
德国	BSI: zerti@bsi.bund.de	Atsec, TUV Info.
印度	IC3S:aloke@stqc.gov.in	Common Criteria Test Lab
意大利	OCSI: ocsi@mise.gov.it	Atsec, CCLab, LVS
日本	JISEC: jisec@ipa.go.jp	Brightsight,ECSEC,TUV Info.
马来西亚	CyberSecurity: mycc@cybersecurity.my	BAE,Cyver Security
荷兰	NSCIB(by TUV Rheinland): info@nl.tuv.com	Brightsight,
挪威	SERTIT: post@sertit.no	Brightsight,Advanced Data Security
韩国	ITSCC: itscc@nsr.re.kr	KTC,TTA
西班牙	CCN.CNI: organismo.certificacion@cni.es	Applus,Epoche, Epoche and Espri
瑞典	CB for IT Security: csec@fmv.se	Atsec,Combitech
土耳其	TSE: ccraturkey@tse.org.tr	Brightsight,BEAM,Epoche and Espri
英国	UKITSECS: cc@ncsc.gov.uk	GI,UL
美国	NIAP: niap@niap-ccevs.org	Atsec,Gossamer,UL

图 45 CC 认证机构和实验室

目前 CC 认证做得较多的企业有三星、LG、苹果等，国内企业相对较少。

4 北美 FIPS 认证体系

4.1 概述

FIPS 标准的概述见 2.2 章节。FIPS 由 NIST 制定并发布，NIST 成立于 1901 年，负责制定针对联邦计算机系统的标准和指南，包括 3 种形式：联邦信息处理标准(FIPS)、特别出版物(SP)和机构间报告(IR)。

- FIPS 主要用于发布密码基础原理相关的标准，如分组密码、数字签名算法、杂凑函数等；
- SP 800 系列主要关注计算机安全领域的一些热点研究，介绍信息技术实验室在计算机安全方面的指导方针、研究成果以及与工业界、政府、科研机构的协作情况等；

- IR 主要用于发布会议报告、密码面临的新挑战讨论等。

NIST 还担任美国密码算法的征集活动的责任单位。早在 1973 年，在总结了美国政府的计算机安全需求之后，NIST 发起了 DES 算法征集评估活动，形成了在世界上应用最为广泛的 DES 算法标准 FIPS-46；1997 年 NIST 发起了 AES 算法征集计划，形成了高级数据加密标准 FIPS-197；2007 年 NIST 发起了杂凑函数 SHA-3 的征集活动，并于 2014 年公布了关于 SHA-3 的 FIPS 202 草案。

FIPS 的密码标准如下表所示。

表 7 FIPS 密码标准

标准号	标准名称
FIPS 140-2	密码模块安全要求
FIPS 140-3(Draft)	密码模块安全要求（草案）
FIPS 180-4	安全杂凑标准
FIPS 181	自动口令生成器
FIPS 185	密钥托管加密标准
FIPS 186-4	数字签名标准
FIPS 190	高级鉴别技术使用指南
FIPS 196	使用公钥密码技术的实体鉴别
FIPS 197	高级数据加密标准(AES)
FIPS 198-1	带密钥杂凑函数的消息鉴别(HMAC)
FIPS 202(Draft)	SHA-3 标准：基于置换的杂凑和可扩展输出函数

本章主要介绍 FIPS 中与信息安全最为相关的 140 标准。

FIPS 140 是 NIST 所发布的针对密码模块的安全要求(Security requirements for cryptographic modules)，其提供了密码模块评测、验证和最终认证的基础。目前该标准一共有 3 个版本，其中最初版本 FIPS 140-1 于 1994 年 1 月公布，它

将加密模块的安全等级分成四级，同时 NIST 宣布 FIPS 140-1 的加密模块产品验证(Cryptographic Module Validation, CMV)计划，并在 1994 年 6 月 30 日正式生效。1997 年 1 月，美国政府下令相关产品需要通过此项标准的认证，随后又对该标准进行了改进。FIPS 140-2 的最新版本发表于 2002 年 12 月 3 日，随后在 2007 年 7 月 13 日，NIST 又公布了 FIPS 140 的最新版本 FIPS 140-3（草案），FIPS 140-3 最终将取代 FIPS 140-2，但其进程缓慢，直到现在也没有正式发布。本章主要讨论影响最为广泛的 FIPS 140-2 标准。

2006 年 ISO/IEC 颁布了 19790 标准，几乎全部涵盖了 FIPS 140-2 的需求。2012 年，ISO/IEC 19790 发布了 2012 版本，包含了 FIPS 140-3 所要求的全部特性。

4.2 技术要求及标准解读

FIPS140-2 标准指定了密码模块需要被满足的安全需求，该模块被应用在安全系统之中保护敏感数据，而不是未经分类的信息。

4.2.1 FIPS140-2 的 4 个安全级别

为了适应广泛的密码模块应用和环境，FIPS140-2 定义了四个逐次增加、定性的安全级别：Level 1、Level 2、Level 3、Level 4。

Level 1：最低的级别

安全级别 1 提供最低级别的安全，是为一个加密模块所规定的基本安全要求(如至少采用一个经批准算法或经批准安全功能)。在安全级别 1 的加密模块中，没有专门对物理提出超过产品级元器件基本要求之外的安全构造要求，该级别加密模块的一个例子是个人计算机(PC)的加密板。

安全级别 1 允许一个加密模块的软件和固件成分，在带有未经验证操作系统的一般用途计算系统上运行。这种运行适合于一些低安全级别的应用，此时，一

些其他的控制手段如物理安全性、网络安全、管理上的程序受到限制或根本不存在。用加密软件来实现安全保证，可能比相应的以硬件结构为主的加密手段更为经济合理，是供一些有低安全级别要求的机构选择的加密解决方案。

Level 2：增加明显的防窜挠外壳、封条或防撬锁等要求来改进密码模块的物理安全

安全级别 2 加强了安全级别 1 加密模块的物理安全性结构，以防止明显的破坏，这是通过增加识别入侵证据的要求来实现的。这些可识别的入侵证据包括：可识别入侵证据涂复或密封、或在可移动的盖子与加密模块的门上装防撬的锁，可识别入侵证据涂复或密封应当置于加密模块上，并且只有破坏了涂复或密封，才能从物理上进入获取组件内部的明文密钥与关键安全参数(CSP)。可识别入侵证据密封或防撬的锁，应当置于所保护防止从物理非法进入的盖子与门上。

安全级别 2 至少要求一个基于角色的验证机制，通过此验证，加密模块可以验证一个操作员承担某个特定角色与执行相应服务的授权。

安全级别 2 允许加密模块的软件和固件成分，在以友善目的的计算机系统上，使用一个操作系统，该操作系统须：符合在附件 B 中列出的通用规则(CC)保护概要(PPs)中规定的功能要求，以及可用 CC 评估保证级别 EAL2(或更高的级别)来评估。

可以用于一个经过同等评估的可靠的操作系统，一个可靠的操作系统可提供一个可靠的安全级别，以便使加密模块在一般用途的计算平台上执行的安全级别，可以与专门利用硬件系统来执行的加密模块相当。

Level 3：除了明显的防窜挠要求外，如果覆盖物被除掉或门被打开，任何未保护的关键安全参数(CSP)都被清零

安全级别 3 要求基于身份的认证。密码模块认证操作员的身份和检查被认证的操作员是否是授权的假定的特定角色，并执行对应的服务集合。

安全级别 3 要求输入和输出 CSPs 的数据端口与其他的数据端口在物理上分开。

安全级别 3 允许在多用户分时系统中使用软件密码，但所使用的操作系统需满足要求：满足 CAPP 中描述的功能要求和可信通路(FTP_TRP.1)功能要求；满足 CC 中的评估保证级别 EAL3 和具有非形式化的 TOE 的安全政策模型(ADV_SPM.1)的保证要求。

Level 4：最高级别的安全性

物理安全在密码模块周围提供可以检测察觉从任何方向试图渗透的保护封套（检测到破坏后所有的关键安全参数被清零）。

安全级别 4 也保护密码模块对抗由于环境的条件或波动外部电压和温度带来的影响。

安全级别 4 允许在多用户分时系统中使用软件密码，但所使用的操作系统需满足要求：满足级别 3 的功能要求；满足 EAL4 和形式化的 TOE 安全策略模型(ADV_SPM.3)，隐通道分析(AVA_CCA.1)和模块化(ADV_INT.1)保证要求。

4.2.2 FIPS140-2 的 11 类安全要求

安全要求涵盖了密码模块安全设计和实现的相关领域，每个领域在特定的安全级别上开展评估。

这些领域包括：

- 密码模块的规格
- 密码模块端口和接口
- 角色、服务和认证
- 有限状态模型
- 物理安全

- 操作环境
- 密钥管理
- 电磁干扰/电磁兼容性(EMI/EMC)
- 自我测试
- 设计保障
- 其它攻击减缓

表 10 为这 11 类安全要求的摘要，详细要求可直接参考标准原文。

表 8 FIPS 标准安全要求摘要

序号	安全要求	Level 1	Level 2	Level 3	Level 4
1	**加密模块的规格**	加密模块的规格、加密范围边界、认可的加密算法、认可的运行模式、加密模块的说明，包括所有硬件、软件与固件，组件安全策略的描述。			
2	**加密模块的端口和接口**	要求与供选的接口，所有接口的规格与所有输入、输出数据的路径。		对用于未保护的关键安全参数的数据连接端口，应当在逻辑上与其它数据连接端口分开。	
3	**角色、服务和认证**	要求逻辑上分开的供选角色与服务	基于角色与基于身份识别的操作员验证	基于身份识别的操作员验证	
4	**有限状态模式**	有限状态模式的规格，要求的规定与供选的规定，规定的转换图与规定转换的规格			
5	**物理安全性**	生产合格设备	锁或入侵证据	对盖与门的入侵检测与反应	入侵检测与反应的封装、EFP 或 EFT
6	**操作环境**	单独操作员，可执行的密码与认可的集成技术	在 EAL2 中已引用的外壳防护评价，按规定自由选择登录控制机制与监测	在 EAL3 中已引用的外壳防护与可信路径评价，加上安全策略的模式	在 EAL4 中已引用的外壳防护与可信路径评价
7	**密钥管理**	密钥管理构造：随机数与密钥的产生，密钥的建立、分配，密钥的输入与输出，密钥的存储与密钥的清除。			
8	**EMI/EMC**	47 CFR FCC 15B 分册，A 类（商用）适用的 FCC 要求（收音机用）		47 CFR FCC 15B 分册，B 类（家用）	
9	**自检**	通电测试，加密算法测试，软件/固件集成测试，关键功能测试，状态测试			
10	**设计保证**	设置管理(CM)，保密安装与设置，设计与策略的一致性，指导文件	CM 系统，加密的配置，功能规格	高级语言的实现	正式的型号，详细的说明书（非正式封装的），预处理与后处理
11	**其它攻击减缓**	验证其他攻击减缓的任何措施，可能包括简单功耗分析(SPA)，差分功耗分析(DPA)、时序攻击和差分错误分析攻击			

4.2.3 FIPS 140-2 认证需提供的文档说明

密码模块的规格

密码模块硬件、软件和固件组件的规格说明，这些组件环境的密码边界详细说明，以及模块的物理配置描述；

密码模块中任何与标准中安全需求相排斥的硬件、软件或者固件组件的详细说明，并针对此排斥点做出原理解释；

密码模块中物理端口(port)逻辑接口(interface)的规格说明；

密码模块中人工方式或者逻辑控制的详细说明，物理或逻辑状态指示器，以及有效的物理、逻辑和电子方面的属性；

包括经过认可的和非认可的所有安全功能的列表，这些功能由经过认可或者非认可的密码模块所使用，并针对所有操作模式进行详细说明；

所有密码模块主要硬件组件和组件交互结构图(block diagram)描述，包括任何微处理器、缓冲区输入/输出、明文/密文缓冲区、控制缓冲区、关键存储、工作存储器、以及程序存储器；

密码模块中硬件、软件和固件组件的设计说明；

所有安全相关的信息说明，包括密钥和私钥（明文和经过加密的），认证数据（比如密码、PIN）、重要安全参数(CSP)、以及其他受保护的数据（比如审计事件、审计数据），这些信息的泄露或修改可能会影响密码模块的安全性；

密码模块安全策略的说明，包括源自于标准的规则和来源于开发者定义的其他需求说明。

密码模块端口和接口

针对密码模块及其物理端口和逻辑端口的详细说明，以及定义的输入输出数据路径进行审核，使其与标准的源自测试需求(DTR)相一致或提供可接受的解释说明。

角色、服务和认证

所有密码模块所支持的经授权的角色详细说明；

密码模块所提供的经认可的和未获得认可的服务、操作和功能详细说明。对于服务，说明文档应包括服务输入、相应输出和在该服务中可被执行的授权角色；

针对第二级和第二级以上的安全级别，应说明密码模块支持的认证机制，实现此认证机制的认证数据类型，首次初始化认证机制时用于模块访问控制的授权方法，以及模块支持机制的相应强度。

有限状态模型

应验证有限状态模型（或同类）的表述，该验证工作通过使用状态跳转图和/或状态跳转表来指定所有的操作和错误状态、状态间的跳转以及状态跳转结果的输出事件（包括内部模块条件、数据输出和状态输出），验证其与密码模块的实现相一致。

物理安全

针对密码模块及其产品资料进行审核，验证其 DTR 的一致性和可接受的解释说明；

应验证物理形态的规格说明，实现密码模块的物理安全机制的安全级别，以及模块所使用的物理安全机制的详细说明；

如果密码模块中存在维护角色需要物理层面访问模块的内容，或者设计的模块允许物理访问，需要提供维护访问接口的详细说明，并提供一旦维护访问接口被访问，明文形式的密钥、私钥和 CSP 是如何清零的；

在第四安全级别，需要验证密码模块的一般操作范围，密码模块所使用的环境保护失败的特性说明，或环境保护失败所执行的测试说明需要进行验证。

操作环境

针对密码模块的操作环境规格说明进行审核。在第二安全级别或以上，应包括密码模块所使用的操作系统正确性鉴别，验证所采用的保护轮廓(PP)和通用准则(CC)保障级别。

密钥管理

所有密码模块所使用的密钥、密钥组件、以及重要安全参数(CSP)的规格说明；

密码模块所使用的每个任意数生成器 RNG（经认可和未经认可）的规格说明；

密码模块所使用的每个密钥生成方法（经认可和未经认可）的规格说明；

密码模块使用的密钥确立方法规格说明；

密码模块所使用的密钥进入和输出方法详细说明；

在第三安全级别或以上，如果使用单独的知识流程，需要验证如果重建最初的密钥需要 n 个密钥组件知识，那么任何 n-1 个密钥组件不能提供最初密钥的关于强度以外的任何信息，需要提供密钥模块所使用的独立知识流程的详细说明；

密码模块所使用的密钥存储方法说明；

密码模块所使用的密钥清零方法说明。

电磁干扰/电磁兼容性

针对所要求的 EMI/EMC 规定，进行一致性验证；

应由经授权的专业 EMI/EMC 评测实验室开展验证工作。

自我测试

密码模块执行的自我测试说明，包括上电自我测试和条件测试；

密码模块自我测试失败进入的错误状态说明，以及退出错误状态并恢复一般操作模式的必要的条件和行为的说明；

所有与密码模块安全操作密切相关的安全功能说明，以及密码模块所执行的适用的上电测试和条件测试的相关鉴定功能；

如果密码模块实现旁路的能力，提供机制说明或转换流程的逻辑控制说明。

设计保障

密码模块关于安全安装、生成和启动的流程说明；

密码模块的硬件、软件和固件组件，与密码模块安全策略之间的对应性说明（比如操作规则）；

如果密码模块包括软件和固件组件，提供软件和固件组件的源代码，并配有清晰注释描述该组件与模块设计的对应性；

第二安全级别或以上，应明确分发或交付密码模块版本供授权的操作员进行安全维护的流程。

其它攻击减缓

验证其他攻击减缓(mitigation of other attacks)的任何措施；

其他攻击减缓针对的攻击可能包括简单功耗分析(SPA)，差分功耗分析(DPA)、时序攻击(Time attack)和差分错误分析攻击(Differential Fault analysis)。

安全策略

参见 FIPS 140-2 附录 C。

4.3 认证模式及认证流程

4.3.1 CAVP 和 CMVP

FIPS140-2 认证包括 CAVP（Cryptographic Algorithm Validation Program，即加密算法验证程序）和 CMVP（Cryptographic Module Validation Program，即加密模块验证程序）两部分。CAVP 和 CMVP 认证证书是密码产品走向国际市场的通行证，对有志于开拓国际市场的信息安全产品提供商，FIPS140-2 认证是必须迈过的一道门槛。

加密算法验证程序(CAVP)由 NIST 于 1995 年 7 月建立，旨在根据 FIPS/NIST/CSE 推荐的加密算法及算法组件展开验证测评，验证测试包括分组密码、分组密码模式、数字签名、密钥管理、信息验证、随机数列生成、安全散列

等。加密算法验证是加密模块验证程序(CMVP)下的FIPS140-2验证的先决条件。

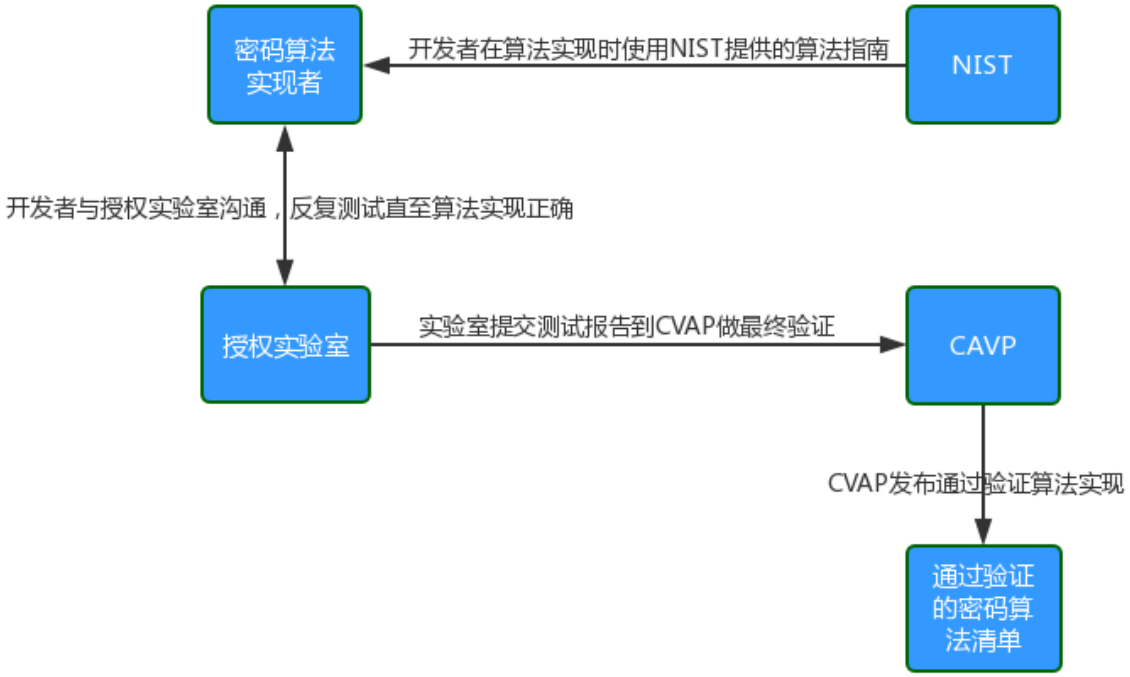


图 46 FIPS 140-2 加密算法验证流程图

CMVP 由美国 NIST 和加拿大政府的通讯安全组织(Communications security establishment, CSE)于 1995 年共同建立，其目标是提供一份可供采购使用的 IT 安全产品列表，列表上的产品已成功通过 FIPS 140-2 标准验证。所有基于 CMVP 的评测由第三方的授权实验室展开，这些实验室被美国国家实验室自愿认可体系(National Voluntary Laboratory Accreditation Program, NVLAP)授权为密码和安全测评(Cryptographic and Security Testing, CST)实验室。

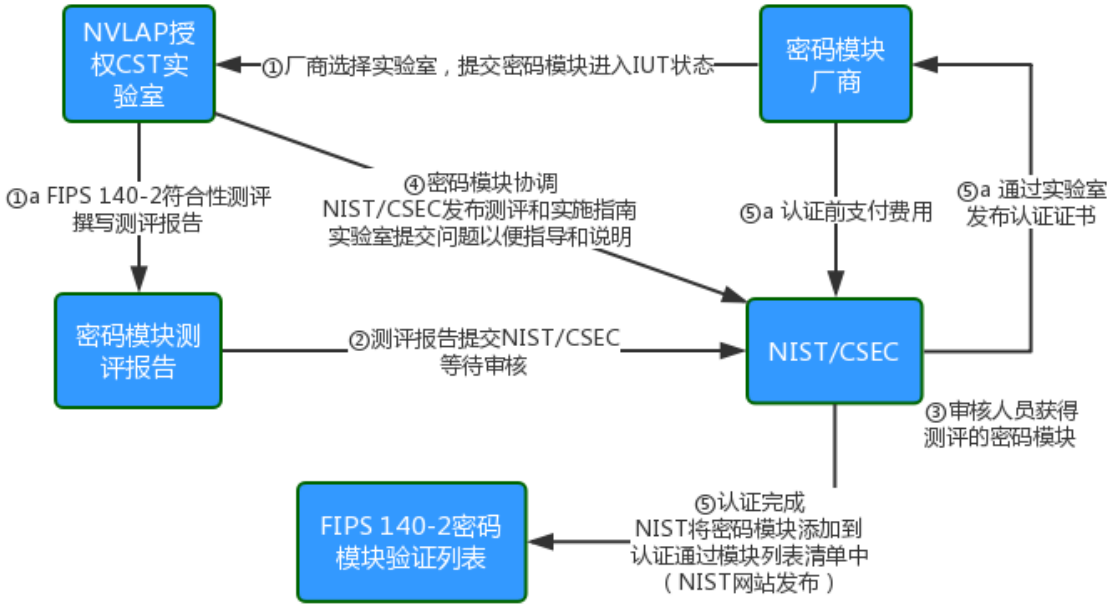


图 47 FIPS 140-2 密码模块验证流程图

4.3.2 哪些机构可从事 FIPS140-2 测评

CMVP 接受美国国家实验室自愿认可体系(NVLAP)授权的密码模块测试实验室的评测结果和验证。该授权过程经过对实验室 QMS 进行完整细致的审核，并通过技术熟练度测试。NIST 公布的 NVLAP 授权实验室有：

- ADVANCED DATA SECURITY (USA - CA)
- ÆGISOLVE, INC. (USA - CA)
- Atsec Information Security Corporation (USA - TX)
- Booz Allen Hamilton (BAH) Commercial Solutions Testing Laboratory (CSTL) (USA - MD)
- CEAL: a CygnaCom Solutions Laboratory (USA - A)V
- CGI IT Security Evaluation & Test Facility (Canada)
- COACT Inc. CAFÉ Laboratory (USA - MD)
- Computer Sciences Corporation (USA - MD)
- Detica Lab (Australia)

- ECSEC Laboratory Inc. (Japan)
- Epoche&Espri (Spain)
- EWA – Canada IT Security Evaluation & Test Facility (Canada)
- ICSA Labs, An Independent Division of Verizon Business (USA - PA)
- InfoGard Laboratories, Inc. (USA - CA)
- Information Technology Security Center (Japan)
- Penumbra Security (USA - CA)
- SAIC Accredited Testing & Evaluation (AT&E) Labs (USA - MD)
- TTC IT Security Evaluation Laboratory (Taiwan, R.O.C)
- TUV Informationstechnik GmbH (Germany)
- UL Transaction Security (Australia)
- Underwriters Laboratories, Inc. (USA - IL)

目前国内通过 FIPS 140-2 认证的中兴通讯、握奇数据等选择的授权实验室是 Atsec 公司，Atsec 是一家全球化的信息安全咨询与评估公司，于 2000 年在德国慕尼黑成立，并且通过美国、德国、瑞典和中国的办公室开展了广泛的国际业务。Atsec 提供的服务包括正式的实验室测评和评估、独立的测试和评估以及信息安全咨询。

4.4 小结

4.4.1 FIPS 认证的必要性

美国政府已授权并且加拿大政府建议，对所有敏感但非密级的数据使用 FIPS140-2 验证加密模块，也就是说，任何想要向美国联邦政府出售的此类数据加密产品，都必须经过 FIPS140-2 加密模块测试的验证。

FIPS 140-2 是密码模块安全需求最为重要的标准之一，也是业界衡量密码实

现的准则。经过 FIPS 标准符合性认证的产品模块将使其满足联邦政府以及相关机构的关于密码系统的技术要求。作为接受度最为广泛的密码模块安全评估体系，目前世界上很多国家机构的采购和招标要求中也明确地提出具有密码模块的产品 FIPS140 的合规要求。

如果机构的信息或者数据需要通过密码的方式进行保护，那么 FIPS 140-2 则被适用。FIPS 140-2 禁止在联邦系统中使用敏感或者重要数据的密码保护未经验证的密码系统。

4.4.2 FIPS 140-2 与 CC 的关系

CC 是业界安全功能和安全保障评估的通用准则，并实现了国际互认。而在美国 NIAP 体系下的 CC 产品评估，如果产品包括密码模块或者密码算法，该产品的 CC 认证证书上将标明该产品是否通过 FIPS 140 认证。事实上，CC 和 FIPS 140 标准相辅相成，存在强烈的相关性，但关注点各有侧重。

在 FIPS 140 验证中，如果操作环境是可以更改的，那么 CC 的操作系统需求适用于安全级别 2 或者更高。

CC 和 FIPS 140-2 标准分别关注产品测评的不同层面。FIPS 140-2 测评针对定义的密码模块，并提供 4 个级别的一系列符合性测评包。FIPS 140-2 描述了密码模块的需求，包括物理安全、密钥管理、自评测、角色和服务等。该标准最初开发于 1994 年，早于 CC 标准。而 CC 是针对于具体的保护轮廓(PP)或安全目标(ST)的评估，典型的模式是某个 PP 可能涉及广泛的产品范围。

总之，CC 评估不能替代 FIPS 140 的密码验证，FIPS 140-2 中定义的 4 个安全级别也不能够直接与 CC 预定义的任何 EAL 级别或者 CC 功能需求相对应。

5 北美 UL CAP 认证体系

5.1 概述

5.1.1 UL CAP

UL CAP 的概述见 2.2 章节。

UL CAP 是全球首个、也是目前唯一一个基于标准（即 UL 2900 系列标准）对联网设备和系统进行安全评估的计划，主要关注软件漏洞、软件缺陷以及安全策略的充分实施。

UL CAP 可为各个产业的企业客户找出产品与系统中的安全风险，并提供降低风险的建议，包括工控系统、医疗设备、汽车、暖通空调制冷设备(HVAC)、照明产品、智能家庭、家电、警报系统、火警系统、建筑自动化、智能电表、网络设备与消费电子产品等。

更具体来说，UL CAP 提供可靠的第三方测试与认证服务，评估联网产品与系统的安全性，以及供货商的运作流程，使其能以安全为核心，开发并维护产品与系统。这项计划可让供货商运用新兴的技术与能力，专注于开发市场时所需的产品创新。针对供货商日益要求的灵活性，UL CAP 服务最能满足厂商的各种要求。

5.1.2 UL 2900 系列标准

UL 2900 网络安全系列标准为联网产品与系统提供了网络安全的测试准则，其能评估软件漏洞与弱点、降低被入侵的风险、处置已知的恶意软件、检查保全

控件，并提升安全意识。

目前 UL 2900 已经获得了美国国家标准协会 (ANSI)、美国食品和药品管理局 (FDA) 和其他监管机构的认可。

UL 2900 系列标准能针对以下的要求，提供相关的测试与评估服务：

- **产品模糊测试(Fuzz Testing)**可识别所有接口上“零时差漏洞(Zero Day Vunlnerabilities)”的攻击风险；
- 采用一般性安全弱点（可被攻击的程序漏洞）编号(Common Vulnerability Enumerations，CVE)评估产品中尚未修复的**已知漏洞(Known Vulnerabilities)**；
- 识别产品中的**已知恶意软件(Known Malware)**；
- 通过一般性安全弱点 (Common Vulnerability Enumerations，CVE)所识别的软件弱点进行**静态源代码分析(Static Source Code Analysis)**；
- 通过 CWE、开放源代码软件与第三方程式库所识别的软件弱点进行**静态二进制分析(Static binary analysis)**；
- 辨识用在产品的**特定安全控制(Specific Security Controls)**，以降低安全风险，包括：
  - 产品的访问控制与授权码；
  - 产品中的密码保护机制；
  - 与产品的远程通信；
  - 产品的软件更新；
  - 产品的停用；
- 根据其他测试发现的缺陷进行**结构化渗透测试(Structured Penetration Testing)**；
- 针对产品中的威胁防御机制进行**风险评测(Risk Assessment)**。

UL 2900 标准所提及的组织评测(Organizational Assessment)能协助评估供货商、系统整合商、资产所有人无疑虑地进行安全产品与系统的设计、开发及维护等流程。UL 2900 也能视各市场形成的安全需求成熟度，适时建立与整合其他技术准则。

5.2 技术要求及标准解读

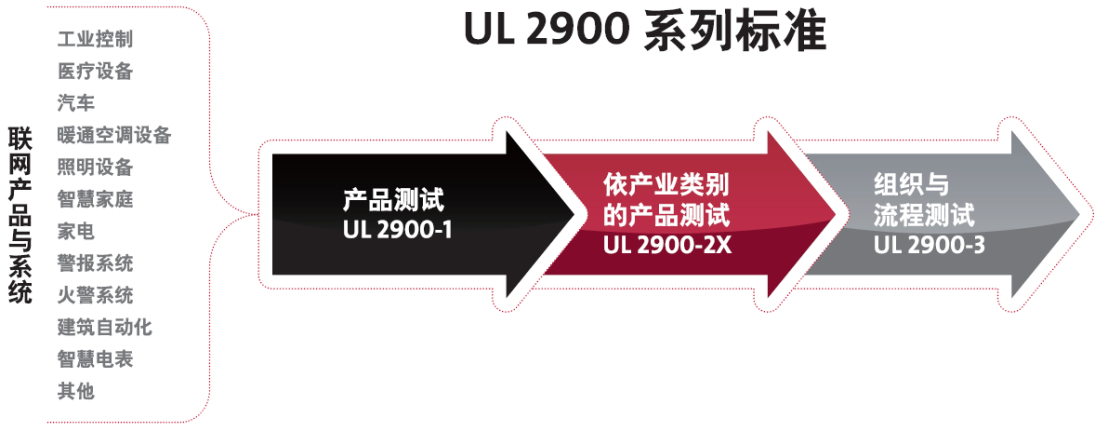
5.2.1 概述

目前 UL 2900 系列共有 4 个标准，UL 2900-1 是针对常规联网产品软件网络安全的通用要求，该标准于 2017 年 7 月 5 日被指定为美国国家标准(ANSI/UL 2900-1)，随后被加拿大标委会采纳为加拿大国家标准(SCC)。

UL 2900-2 是基于不同行业的特性和用户的实际安全需要发布的加强版本，涉及到的行业分别有联网医疗设备和系统、工业控制系统以及安防及生命安全产品。制造商可基于它产品的类别和实际应用场合确认对应的网络安全标准和安全等级。

标准	范围	对应行业
UL 2900-1	常规可联网设备及产品的软件网络安全：通用要求	联网IT和消费类等产品
UL 2900-2-1	卫生保健系统网络可连接部件的特定要求	联网医疗设备及系统
UL 2900-2-2	工业控制系统的特定要求	联网工业控制类产品
UL 2900-2-3	安防及生命安全等网络设备的网络安全特定要求（适用于制造商，业主，集成商）	安防及生命安全产品

图 48 **UL 2900 网络安全系列标准简介**



UL 2900 系列标准适用于需要评估和测试漏洞、软件缺陷和恶意软件的联网产品，并描述：

- 对其产品的软件开发人员(供应商或其他供应链成员)风险管理流程的要求；
- 评估和测试产品是否存在漏洞、软件缺陷和恶意软件的方法；和
- 关于在产品的体系结构和设计中存在安全风险控制的需求。

5.2.2 UL 2900-1 标准解读

UL 2900-1 标准一共有六大章节以及三个附录，其中第一章节主要介绍标准适用的范围、参考文献以及术语的定义，第二至第六章节则详细描述了对联网产品/系统在各关键环节的要求，其中关键环节包括：产品文档、风险控制、风险管理、漏洞和缺陷、软件弱点分析。

(1) 产品文档

产品供应商应提供以下说明文件，以便于进行安全风险评估：

1) 产品使用说明、所有的功能描述，包括管理功能和安全功能；

2) 产品预期配置中的所有外部接口、物理输入或输出端口的列表，包括：远程接口、本地接口、无线接口以及这些接口上支持的通信协议、文件输入等；

3) 所有可执行文件和库的列表，包括第三方开源软件；

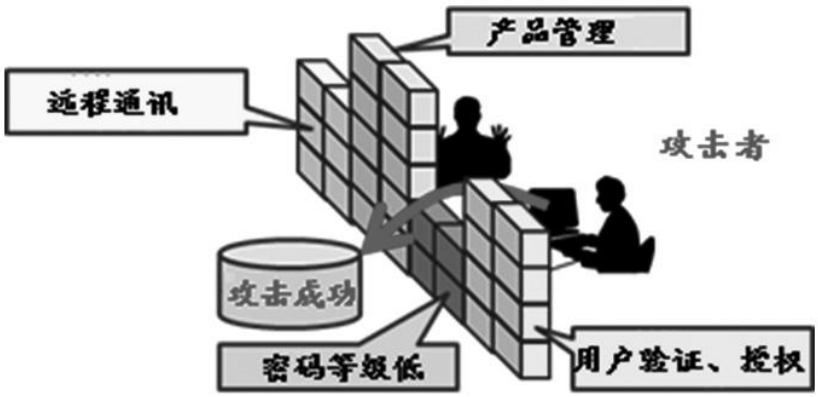
4) 产品中所有软件的源代码，包括所有脚本，库，环境变量，构建配置参数等；

5) 产品软件构建和集成过程的信息，所有软件的二进制代码和/或字节码，除非供应商没有访问这些二进制、字节码的权限；

6) 安装产品所需的环境以及软件安全使用的有效期（告知消费者及时更新）。

(2) 风险控制

风险控制可理解为：产品在开发设计过程中，针对网络安全风险，应遵守并运用的防御保护措施。它包括访问控制（用户验证和/或用户授权）、远程通讯、密码、产品管理四个部分，这四部分相互关联，缺一不可，如图所示。若产品供应商一定要选择不遵守一个或多个这些风险控制，供应商应在风险分析（见 3 风险管理）中提供记录和证明，并确保其无法对产品进行攻击。



- **访问控制**

访问控制，也可称为用户验证和/或用户授权。具体要求如下：

1) 可能影响或者改变产品安全的管理服务，在访问之前需要进行用户验证；

2) 产品的用户验证服务，应实施超时或其它适当的防止永久授权的机制；

3) 可通过远程或无线接口访问的服务,在访问之前需要进行用户验证；

4) 如果产品使用用户名和密码机制来认证用户：

①产品应使用符合 ISO/IEC 11889 要求的安全机制来存储密码；

②产品提供的验证错误信息不允许枚举有效用户名；

③产品应支持对密码长度、更新频率、复杂性设定要求的可能性；

④产品应防止字典攻击和暴力攻击（目的是防止登录尝试）；

⑤产品不得有无法删除或更改的硬编码密码。

5) 对于使用根据角色访问机制的产品，供应商应清楚记录所有现有的角色及其相关权限，同时应有一个“管理员”或“系统”角色，具有与之相关的特权来管理产品，且这种特权不得授予其他角色；

6) 产品应支持通过添加、删除来管理有效用户帐户列表和/或暂停用户帐户的可能性；

7) 对可认证的每个帐户执行最低权限的原则；

8) 如果通过远程接口的通信会话丢失或终止，则产品需要在允许通过远程接口访问之前重新认证，存储的从前数据会话不得用于启动新会话；

9) 不提供命令、控制功能或不传输敏感数据、个人身份数据，并且只输出状态或历史交易数据等服务，可以提供未经身份验证的访问。

- **远程通讯**

具有远程通讯功能（如带有无线和/或远程接口）的产品，要求如下：

1) 产品应确保通过任何无线和/或远程接口传送的所有数据的完整性和真实性。为此，产品使用的安全功能应符合相关标准要求，具体见下表。

表 1　相关规范性标准

标准序列	标准名称
ISO/IEC 9796	让信息复原的数字签名方案
ISO/IEC 9797	信息认证码（MACs）
ISO/IEC 9798	实体身份验证
ISO/IEC 10118	散列函数
ISO/IEC 11770	密钥管理
ISO/IEC 15946	基于椭圆曲线的加密
ISO/IEC 18033	加密算法
ISO/IEC 19772	身份验证加密
详情参见 UL 2900-1:2016 APPENDIX C[1]	

2) 如仅是报告产品状态的无线和/或远程接口，且不提供命令和控制功能、不传输敏感数据等，可不必保证其数据的完整性和真实性。

- **密码**

产品应确保所有由产品生成、存储、使用或传输的敏感数据和个人身份数据的机密性，产品采用的安全机制应符合 ISO/IEC 11889 要求。具体要求如下：

1) 供应商应识别并记录哪些被认定为是敏感的数据，至少包括所有个人身份信息和任何被披露就可能危及产品的安全属性的数据，如加密密钥和密码；

2) 产品应仅使用上表中列出的密码算法作为安全保护协议；

3) 产品应为每个服务、操作或功能使用单独的加密密钥加密，例如：传输层加密、运营商角色认证、远程软件升级映像完整性确认等，供应商还应清楚记录产品使用的每个密钥的预期用途。

- **产品管理**

产品管理是确保产品在发布或出厂后，运行相当一段时间（例如：家电产品的生命周期 5 ~10 年），也能应对网络中的各种风险，具体要求如下：

1) 产品设计和运行的软件版本应能够进行更新，并在更新过程中如果出现失败，能完整地返回到当前版本；

2) 在安装更新之前，产品应运用密码验证任何软件更新的真实性和完整性。

若可以在离线环境中进行产品软件版本更新，也应该支持真实性和完整性的验证；

3) 产品应能够维护并保持所有安全相关事件的一个或多个日志，例如：成功和不成功的登录尝试、更改用户身份验证凭据、更改有效的用户帐户列表、成功和不成功的软件更新等；

4) 除非将其传输到外部数据存储，否则产品应把安全相关的日志全部存放在非易失性存储器中，且不允许非特权用户删除或更改它们；

5) 在初始运行之前，产品需要更改任何在产品安全方面发挥作用的系统默认值，如密码和密钥，产品应有文件建议更改系统默认值；

6) 退出使用产品时，应能完全清除配置数据、敏感数据和个人身份数据。这些数据的归零是可以接受的，并且可以作为操作或过程程序来执行；

7) 核准软件更新的完整性可使用以下机制（所使用的机制应符合表 1 要求）：

①在软件和固件组件上生成消息认证码；

②在软件和固件组件上生成数字签名；

③在软件和固件组件上生成散列函数值。

(3) 风险管理

在设计产品时，供应商应建立并记录安全风险分析文档，文档包括：

1) 记录产品所有的功能，存储、处理或使用的数据；

2) 所有可能威胁产品功能和数据的列表（案例可参见 common attack pattern enumeration and classification(CAPEC)）；

3) 评估每个确定的威胁的影响，例如：出现敏感的信息被暴露的情况；

4) 评估每个确定的威胁的可能性；

5) 根据其影响，确定每个威胁造成的风险等级；

6) 风险接受的标准（即确定某一风险水平是否明确为可接受的或不可接受的）；

7) 确定适当的风险控制措施（参见“3 风险控制”），以减轻不可接受的风险的威胁水平；

8) 在对这些风险采取控制措施后，对每个威胁的剩余风险水平进行评估。

另外，如果供应商允许任何已知的漏洞存在产品中，供应商对产品的安全风险分析应包含每个接受的已知的安全漏洞的说明。同样，如果供应商了解并接受任何软件缺陷存在在产品上，供应商对产品的安全风险分析应包含每个接受的缺陷的说明。是否可以接受，可分别通过“4 漏洞和缺陷”进行验证评价。

(4) 漏洞和缺陷

- **软件漏洞及测试方法**

被测试产品的二进制代码和字节码（包括由第三方提供的）不能含有已知的漏洞或无漏洞可被利用（案例可参见 Common vulnerabilities and exposures(CVE)）、不能包含恶意软件（案例可参见 CWE/SANS Top 25 Most Dangerous Software Errors）。发现漏洞的方法可选用：畸形输入测试、结构化渗透测试。

- **软件缺陷及分析方法**

被测试产品的任何源代码或其衍生代码应不存在软件缺陷，可按照相关平台或机构最新发布的所有软件缺陷进行评估(案例可参见 Commonweakness enumeration(CWE)和 Common Weakness Risk Analysis Framework (CWRAF))。

查找软件缺陷的方法可选用：静态源代码分析法、静态二进制和字节码分析法。

新版 UL 2900-1 调查大纲适用于对可联网产品软件中可能存在的漏洞和缺陷，进行评估和测试，该大纲主要描述了供应商对其产品的风险管理流程的要求、产品架构和设计中存在安全风险控制的要求、对产品的漏洞和缺陷进行测试和分析的方法。但不包含对产品功能测试的要求（参见 IEC 61508 系列标准）、不包

含产品中硬件的要求（参见产品的相关安全标准）。[4]

5.3 认证模式

UL 针对联网产品与系统所提供的信息安全服务包括：

- 以 UL 2900 网络安全标准或特定要求为基础的安全性测试准则；
- 根据 UL 2900 网络安全标准的测试与认证；
- 提供供货商流程的评估与风险评测，以协助安全产品与系统的开发与维护；
- 针对产品设计与向第三方采购组件等方面提供安全准备教育。

只要符合 UL 2900 系列标准所定义的条件，该产品或系统就能获 UL 认定为“符合 UL 2900”而取得证书与详细测试报告。除此之外，根据 UL 2900-1 部分要求或客户指定要求所执行的测试，也能取得测试报告。

5.4 认证流程

如图为 UL CAP 认证的基本流程。认证项目发起后，厂商向 UL 提交相关资料，资料审核通过后开始进行测试，得到测试报告，接下来会进行报告评估，并对其做出相关决策，如果不符合要求，厂商需要整改，并提供修改的相关资料，

[4]注：本部分内容来自期刊论文：廖亮,冯坚,林永明.解读新版 UL 2900-1 可联网产品软件的网络安全调查大纲[J].日用电器,2017,(第 10 期).

直到评估机构认为合格为止，最终交付的成果为测试报告和认证证书。

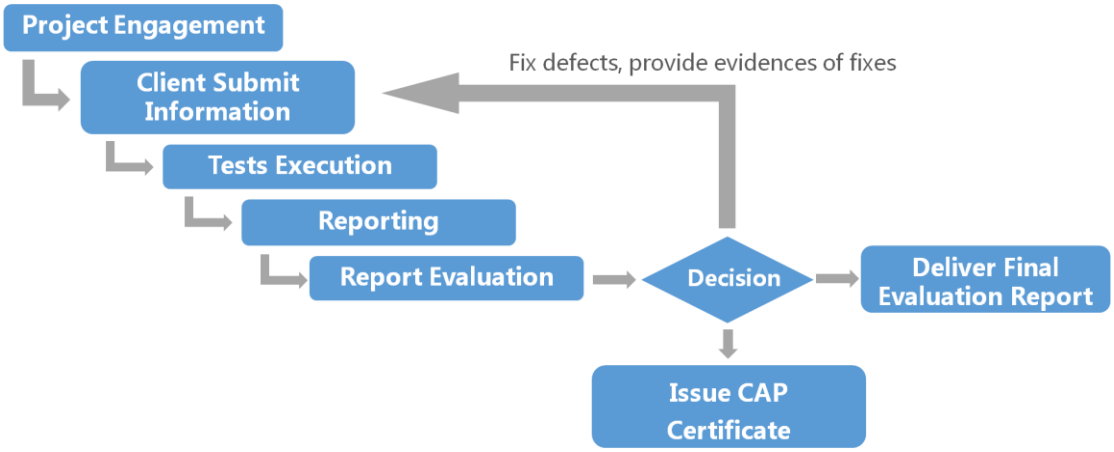
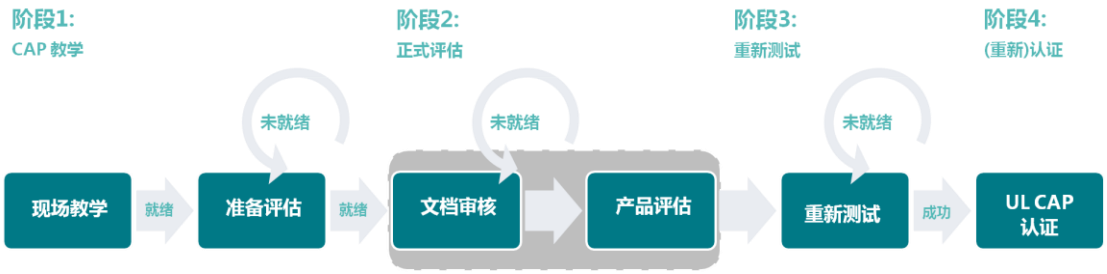


图 49 UL CAP 认证的基本流程

更具体来说，UL CAP 认证包括 4 个阶段。



阶段 1：现场教学

目标：介绍 UL CAP，产品学习，评估文档初审

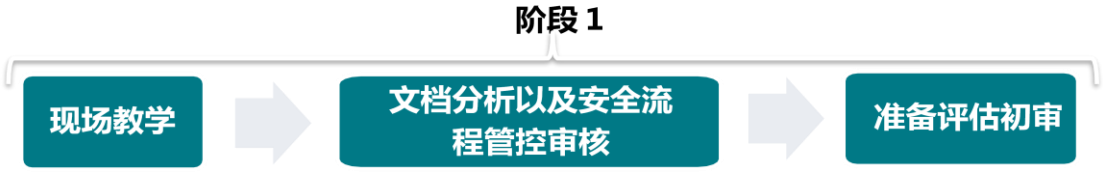
内容：

- 介绍 CAP
- 产品学习
- 文档要求
- 安全要求讨论
- 差异分析
- 文档模板
- 制定评估范围/价格
- 准备清单

首先会进行一场两到三天的现场教学，客户需要准备产品文档（UL 可以在教学前提供一份文档要求的概述）以供进行评估初审。教学内容如下：

第 1 天	第 2 天	第 2/3 天
◆ 介绍 UL CAP ◆ 产品学习 ◆ 审核客户文档，包含风险分析/评估流程等 ◆ 解读 CAP 安全要求细则(第 1 部分)	◆ 解读 CAP 安全要求细则(第 2 部分) ◆ 异常处理 ◆ 差异分析	准备评估初审 ◆ 可行/不可行 决策
备注： ◆ 单独报价和提案； ◆ 可就已完成的文档和已实施的安全控制机制进行初步审核和讨论； ◆ 所有的文档都必须用英文编写； ◆ 阶段 1 的费用需在正式评估之前支付。		

阶段 1 的后期会进行评估文档初审，并做出决策，若可行，进入下一阶段，否则需要重新完善文档资料，直到认为能够进行下一阶段。



阶段 2：正式评估

在这个阶段中，UL 会报告给客户在风险分析中应注意和修复的问题，并基于阶段 2.2 所发现的并且客户在风险分析中已确认的问题进行结构化渗透测试。

阶段 2.1：文档审核

目标：验证文档是否齐全，审核产品安全要求文档并制定测试计划

内容：

- 验证文档完整度
- 审核产品安全要求

- 制定测试计划

阶段 2.2：产品评估

目标：验证产品是否符合 UL 2900 标准要求

内容：

- 执行测试计划
- 编写报告
- 差异分析
- 通过/通过
- 含一次重测机会
- 签发 UL 证书（如果通过）

若产品在第 2 阶段通过评估了，UL 直接签发证书，否则需要进行重测，即进入第 3 阶段。

注意：阶段 2.1 文档审核完成后支付文档审核费用，阶段 2.2 产品评估完成后支付产品评估费用。

阶段 3：重新测试

目标：基于阶段 2.2 的结果进行重测

内容：

- 重新测试
- 通过/未通过
- 签发 UL 证书（如果通过）

该阶段主要是针对 2.2 阶段发现的问题，提供一次重测机会，其中第 1 次是免费的，但重测所花费的时间是有一定限制的，额外的重测费用需要依据重测的

工作量/时长来进行估算。

阶段 4：重新认证

目标：每年重新认证

内容：

- 执行测试计划
- 编写报告
- 签发 UL 证书（如果通过）

目前 UL CAP 的证书有效期是一年（无 UL 标志/无 UL 监管，证书的维护依赖于制造商合作），所以需要每年进行重新认证。

可以看出，在整个 UL CAP 认证流程中，关键环节主要有 3 个：现场教学、文件审核以及产品评估与认证。需要注意的是，对于一个 UL CAP 评估，UL 要求在产品的最新软件版本（即将生产的版本）上进行评估。

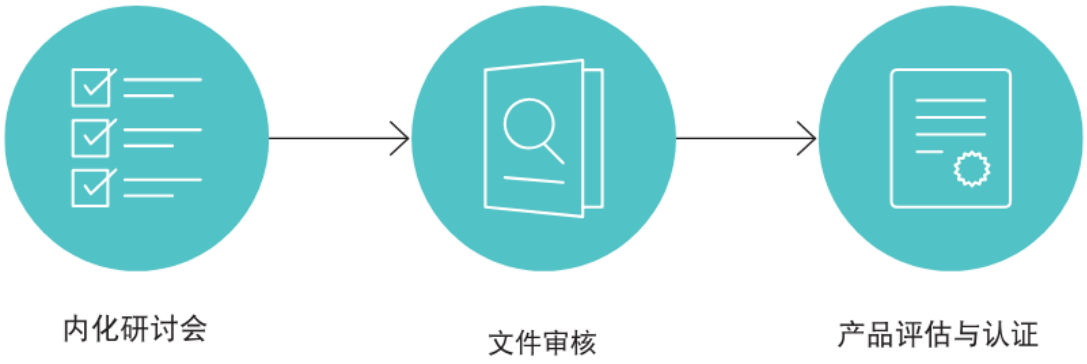
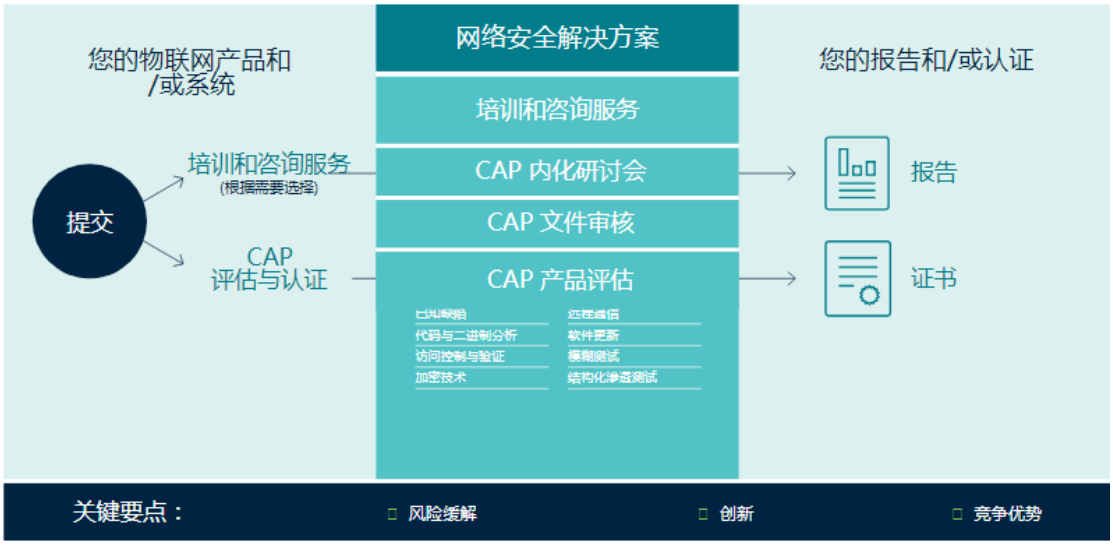


图 50 UL CAP 认证的关键环节



5.5 小结

UL CAP 是依据美国联邦政府、学术界与产业界等重要利益相关者建议所制定的计划，目的是将安全评测导入重要基础设施的供应链中。事实上，UL CAP 服务与对软件安全的投入不仅受到美国白宫“网络安全国家行动计划”的认可，甚至被视为 loT 供应链提供联网装置重要的测试与认证方法。

及早采用 UL CAP，不仅可利用市场细分早日取得竞争优势，并可降低因网络攻击所产生的信息安全风险：

- 非预期的停机与生产损失；
- 昂贵的资产损失；
- 信誉毁损。

6 CC、FIPS、UL CAP 对比

在内容上，CC 是业界的一个通用准则，包括了安全功能和安全保证的要求，其涵盖的范围较广，很多现有信息安全规范的定义都来自 CC。而 FIPS 主要是针对加密这一领域，是 CC 的支撑，或者说是 CC 的一个分支，进行 CC 认证的时候一定会进行与加密相关的内容，但不一定要包含 FIPS 认证。例如，某企业的

产品进行 CC 认证，若其产品包含密码模块或者密码算法，该产品的 CC 认证证书上将标明该产品是否通过 FIPS 140 认证。若产品之前已经进行过 FIPS 认证，那么进行 CC 认证的时候加密这一模块就不用重复进行认证了，实验室会直接承认。总的来说，CC 和 FIPS 是相辅相成的[5]。

UL CAP 主要针对物联网，其在技术上跟 CC 有所相关，但是对文档的要求较少，侧重漏洞评估、缺陷查找和安全控制策略。

[5] 参考第 4 章第 4.4 节

表 9 CC、FIPS、UL CAP 对比

安全认证	FIPS	Common Criteria(CC)	UL 2900
类别	加解密模块	信息技术安全	网络安全保障计划
目标	软件模块或设备	软件模或设备或芯片	设备
范围	软件 硬件 网络设备 储存设备	软件 硬件 网络设备 储存设备	物联网设备
验证地点	授权实验室	授权实验室	UL 实验室
标准制定单位	美国政府	CC 受发证国家	UL
关注重点	加解密程序严谨性	物理和逻辑安全保护，系统维护，流程规范，数据生命周期，危机处理等	设备系统 性和信息安全保护
认证效益	取得美国政府部门招标案资格	取得不同国家政府的要求	展现物联网产品安全
相关联单位	加解密程序开发部门	开发部门	物联网设备开发部门
特性	测试时需有加解密运算的程序 代码	测试时需要有产品程序代码及安全设计文件，流程文件等	测试时需有产品程序代码及安全设计文件
周期及费用	分 CAVP 和 CMVP 两种情况 CAVP：周期一般为两个月，费用约 20-30 万，不同的实验室差异很大； CMVP：以二级为例，周期一般为半年，费用约 50-100 万，级别越高，费用越高，周期越长。	周期和费用取决于产品的复杂程度和认证的级别，以一般的网络管理系统的三级认证为例，认证费用为 100 万左右，周期为 12 个月左右。	可参考 UL 官方报价

7 应对策略及建议

当前，信息安全形势日益严峻，信息安全保障要求日趋严格，然而，诸多企业还不知道或者完全在观望，很多企业基本不知道该做什么、怎么做，更缺乏对北美信息安全标准政策的动态跟踪。因此，基于我国、我市 ICT 行业的实际情况，结合现有的技术准入条件和市场监管模式，深入研究北美信息安全市场准入体系后，项目组提出以下建议。

7.1 政府层面

1. 政府支持下，组建 ICT 行业安全联盟或行业协会，为企业构建可依赖的信息交流和共享平台，通过该平台实现信息共享、资源互补，支持企业快速有效地获得准确的行业资讯，从而使其能够快速、可持续地应对行业变化，同时该平台也能为政府拟定产业政策提供专业知识支撑。

2. 考虑到深圳 ICT 行业缺乏独立的、专业的、能力完善的网络与信息安全测评机构，建议深圳市政府在产业政策方面给予引导和支持，在深圳本地培育和发展几家有能力、有竞争力的信息安全测评、咨询和培训机构，完善深圳 ICT 行业的布局，让更多 ICT 企业在实现安全合规时有公共平台可以依赖，减少企业们的重复投入，也减少企业的负担。

3. 考虑到强化数据和网络安全管理是国际社会的大势所趋，而深圳恰好有着敢为天下先的社会环境和优良传统，建议深圳率先建立具有先进性的信息安全地方标准，并在深圳的企事业单位优先推行，从自身的标准做起，引导企业养成良好的信息安全意识和习惯，减少企业走出国门后的安全合规风险和隐患。

7.2 检测认证行业层面

在政府支持下，国内实验室能够建立起信息安全相关的资质、测试能力及合

作渠道，以便为企业提供信息安全准入方面最有效率和最经济的整体解决方案，包括检测、认证和咨询服务等，减少企业出口成本。

7.3 企业层面

1. 主动学习，积极参与国际/国外行业活动，如参加相关标准组织的活动，及时获取标准制定修订动态，甚至是直接参与标准制定修订工作，掌握话语权；或参加国内外行业组织活动，与业界先进企业共同评估法规标准制修订的影响，积极表达企业自身的诉求。

2. 利用技术驱动，建立先进测试能力，以最严格的标准和质量控制保障产品符合相关法规或标准的要求。

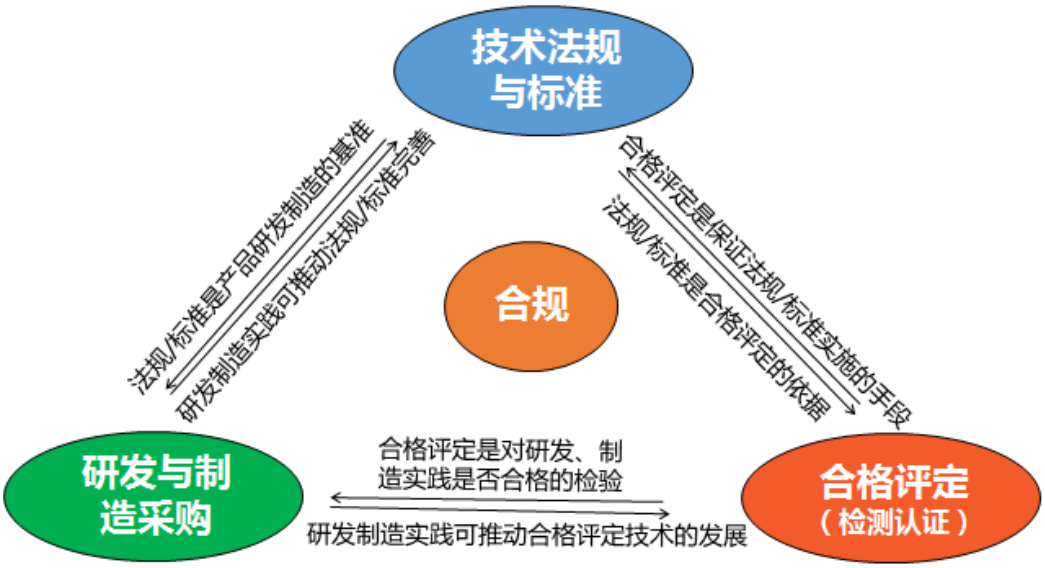
3. 与专业行业组织、检测认证机构、外部研究机构合作，实现共赢，保障产品无准入合规风险，如主动参与有影响力的专业行业组织，积极获取法规标准最新动态及表达企业自身的意见；与检测认证机构共享信息，共同探讨测试法规标准要求，合作完成认证交付；与外部力量合作，完成产品在目标国的准入需求及合规风险调研。

4. 利用规则解决相关市场准入问题：除了主动跟踪相关法规标准信息外，可积极寻求与国家商务部、市场监管总局、标准院、海关等政府机构合作，利用 WTO 规则解决技术性贸易壁垒问题。

7.4 小结

总的来说，企业掌握着信息、技术与研发，政府掌握着规则，检测机构恰好可以提供相应的平台，若政府、企业与检测认证机构可以相互合作，充分发挥三方的作用，实现信息共享、应对联动，将企业转化为国家力量，如图所示，若能够在政府支持下建立三位一体应对机制，那对于有效应对技术性贸易措施将是非

常大的优势。



企业紧密跟踪相关法规或标准的发布，积极与行业协会、标准组织开展合作，适时引导法规或标准的建立，同时将技术法规或标准遵从融入产品研发、制造、采购的整个流程中，提高产品的市场竞争力；检测机构完善检测认证能力，建立专业检测实验室，与权威认证机构广泛开展合作，以给企业提供切实有效的解决方案；而政府可给企业与检测认证机构提供政策上的支持与引导。

8 结语

北美拥有全球最大的消费市场，许多企业都希望在其中抢得一席之地，因此，面对其严酷的信息安全新规，企业需要积极准备合规工作。然而在国内，很多企业对相关规定认识不足，导致真正面临时无所适从；部分企业只围绕各自的业务领域展开研究，研究缺乏通用性，对整个行业欠缺指导性。因此，研究 ICT 产品信息安全北美市场准入体系，系统解读相关法规和标准，全面梳理其在相关领域带来的重大影响，既为企业提供参考，也为我国政府考虑大数据背景下的信息安全管理制度引入先进理念，同时还对我国的技术性贸易措施工作起到一定的指导作用。

附件 1——2017 年全球信息安全大事记

1 月，美国政府承包商泄露了美国特种作战司令部(SOCOM) 11G 员工数据，均为明文，且可公开访问，其中包含至少 2 名特种部队专家的姓名和地址，以及心理学家和其它 SOCOM 医疗工作人员的工资标准、住处和住宅。

2 月，纽约斯图尔特国际机场被曝将 750 GB 备份数据暴露在互联网上，没有密码保护且无须任何身份验证。泄漏的数据包括 107 GB 邮件通信内容、员工社会保障号(SSN)、机场系统的密码列表、内部机密文件等。

3 月底，58 同城被曝对求职者简历毫无防护，平台存在多个漏洞，黑客通过采集工具就能轻易获取后台数据。甚至有商家在网上出售 700 元一套的爬虫软件，可采集全国 430 多个城市，以及 464 个职业的简历数据。

4 月，12306 官方网站再现安全漏洞，有媒体记者在订票时发现，当退出个人账号后，网站页面竟自动转登他人账号，且与账号相关联的身份证号码、联系方式等个人信息均可见。

5 月，新型“蠕虫”式勒索病毒 WannaCry 爆发，席卷全球。这场全球最大的网络攻击已经造成至少 150 个国家和 20 万台机器受到感染，受害者包括中国、英国、俄罗斯、德国和西班牙等国的医院、大学、制造商和政府机构。

6 月，全球因 Hadoop 服务器配置不当导致海量数据被暴露，涉及使用 Hadoop 分布式文件系统的近 4500 台服务器，数据量高达 5120TB，中国和美国受影响最深。

7 月，美国征信企业 Equifax 对外宣布，因公司网站遭到黑客攻击，1.43 亿美国公民的信息数据或已被泄露。

9 月，巴黎安全研究人员发现身份不明的黑客攻击了荷兰一台开放访问的服务器，该服务器的 7.11 亿个电子邮件账户数据被泄，其中包含来自全球各地的

电子邮件账号、邮箱地址、密码组合（有些是明文形式）以及 SMTP 凭证和配置文件。

10 月，有外媒曝出了南非史上规模最大的数据泄露事件——共有 3160 万份南非公民的身份号码、个人收入、年龄，甚至就业历史、公司董事身份、种族群体、婚姻状况、职业、雇主和家庭地址等敏感信息都被长时间在网络上完全公开，甚至连总统祖马和多位部长都未能幸免。

11 月底，亚马逊公共储存 AWS 服务器泄露了美国陆军情报与安全司令部(INSCOM)至少 100 GB 的“军事机密”文件，其中包含美国当局在全球社交媒体平台中收集到的 18 亿用户的个人信息。

此外，美国选民数据被泄露、黑客团队公开美国国家安全局(NSA)黑客武器库等类似大大小小的信息安全事故不计其数，对国家和民众的利益造成了严重的威胁。

附件 2——2018 年美国信息安全最新法规动态

1. 美国海关和边境保护局发布《电子设备边境搜查指令》

1 月 5 日，美国海关和边境保护局(CBP)发布新修订的《电子设备边境搜查指令》(Border Search of Electronic Device Directive)，以作为边境官员的执法依据。

新规将取代 2009 年发布的指导原则，理清边境执法人员在搜查电子设备时的权责。依照新规，在所有进出美国的边界，执法人员均可以对出入境的旅客，广泛地搜查电子设备，要求旅客提供密码，必要时，可以扣留设备及其内的相关信息。边境官员在搜查所有进出境旅客的电子设备时，应遵循下列原则：可通过电子设备的软件，搜索储存在其内的信息，但不能从该电子设备中，取得储存在设备以外的信息；可要求旅客将其电子设备置于离线模式或禁止网络连接，并且确保他们没有改变设备中的内容。

美国海关和边境保护局(U.S. Customs and Border Protection，CBP)副执行助理主任在一份声明中表示，“CBP 致力于维护公民权利和公民自由，将持续谨慎且负责任地在边界行使搜索电子设备的权力，以获得公众的信赖。”

发表于 2018 年 1 月 8 日，链接：

http://www.sohu.com/a/215334567_99932916

指令原文链接：

https://www.cbp.gov/sites/default/files/assets/documents/2018-Jan/CBP-Directive-3340-049A-Border-Search-of-Electronic-Media-Compliant.pdf

2. 美众议院通过《网络漏洞披露报告法案》

1 月 9 日，美国众议院通过《网络漏洞披露报告法案》（Cyber Vulnerability

Disclosure Reporting Act）。

该法案要求在该法案生效之日起 240 天内，国土安全部部长应向众议院国土安全委员会和参议院国土安全和政府事务委员会提交一份报告，内容包括描述为协调网络漏洞披露而制定的政策和程序。在可能的范围内，报告还应包括附件，以说明在提交报告前一年之前使用这些政策和程序披露网络漏洞的情况，并提供这种情况下由行业和其他利益相关者采取行动的信息。报告还可能包含有关国土安全部长如何与其他联邦实体以及关键基础设施所有者和运营商合作以防止、检测和减轻网络安全漏洞的描述内容。此外，该法案还明确报告应以非保密形式提交，但应包含一份保密分类的附件。接下来，该法案将提交美国参议院进行审议。（公安部第三研究所网络安全法律研究中心编译）

法案原文链接：

https://www.congress.gov/bill/115th-congress/house-bill/3202?r=57

3. 美国提出新法案，禁止政府机构等使用中国通讯产品

1 月 9 日，美国提出《保护美国政府通信法案》（Defending U.S. Government Communications Act），禁止政府机构及其相关单位使用中国公司的通讯产品。法案指出国家对中国经济的影响难以量化，华为已经与中国政府共享了其所涉及到的丰富的涉外电信系统情报等内容。法案规定禁止使用的电信服务或设备包括：

1）华为技术有限公司或中兴公司（或其附属公司）生产的电信设备。

2）由上述实体或使用其电信设备所提供的电信服务。

3）当相关机构负责人有理由相信某实体由外国政府（法案明确所指的外国政府为中华人民共和国）拥有、控制或其他联系时，禁止使用该实体生产或提供

的电信设备及服务。

对此，商务部新闻发言人表示，这在某种程度上对市场发出了一个错误信号，不利于中美信息通讯产业的合作，动摇了中国企业对美国营商环境、投资环境的信心。希望美方一些人能够真正从消费者的角度出发，客观、公正的对待中国企业和中国产品，努力营造更加开放、公正、透明、便利的市场环境，从而让美国广大消费者真正从中受益。（公安部第三研究所网络安全法律研究中心编译）

法案原文链接：

https://www.congress.gov/bill/115th-congress/house-bill/4747/text?q=%7B%22search%22%3A%5B%22H.R.4747%22%5D%7D&r=1

发表于 2018 年 1 月 18 日，链接：

http://www.chinanews.com/cj/2018/01-18/8427235.shtml

4. 美国参议院提出《数据泄露预防和赔偿法案 2018》

1 月 10 日，美国参议院提出《数据泄露预防和赔偿法案 2018》（Data Breach Prevention and Compensation Act of 2018）。该法案旨在在联邦贸易委员会设立一个网络安全办公室，负责对消费者报告机构的数据安全进行监督，以及要求颁布条例针对消费者报告机构建立有效的网络安全标准，对信用报告机构将消费者敏感数据置于危险之中的网络安全违规行为进行处罚。该法案的主要内容包括：

1）个人识别信息（personally identifying information）的界定。该法明确个人识别信息是指：社会安全号码，驾照号码，护照号码，外国人登记号码以及其他政府颁发的唯一识别号，唯一的生物特征数据如脸纹、指纹、声纹、虹膜图像或其他唯一的物理表征，自然人的姓和名，或与其他信息结合可以与该自然人的

过去、现在或将来的身体或心理健康状况相关联的姓名的首字母或姓氏，金融账号、借记卡号码、消费者信用卡号码及密码，以及网络安全办公室主任确定的其他信息。

2）网络安全标准及 FTC 的权力。该法案明确 FTC 将成立一个网络安全办公室。该办公室的职责主要在于：监督消费者报告机构的数据安全，颁布有效的数据安全规则，对消费者报告机构的网络安全措施进行年度检查等。

3）通知与执行。该法案规定消费者报告机构应当在发生数据泄露事件之后的 10 天内向 FTC 报告。FTC 应当在接到通知后的 30 天内向地区法院针对发生数据泄露事件的消费者报告机构提起民事诉讼。

4）赔偿。根据法案的规定，法院有权要求泄露数据的消费者报告机构进行民事赔偿。赔偿的标准为：涉及泄露个人信息的最低赔偿 100 美元，每多泄露一项个人信息，则增加赔偿 50 美元，最高赔偿额不超过该机构上一年度总收入的 50%。但消费者报告机构未在规定的事件向 FTC 报告或者违反 FTC 颁布的数据安全规则的，法院可要求该机构进行双倍赔偿，赔偿数据以该机构上一年度总收入的 75%为限。

5）民事赔偿费用的用途。该法案明确赔偿费用的 50％将用于网络安全办公室从事网络安全研究和检查。另外的 50％由 FTC 分配给受影响的消费者。（公安部第三研究所网络安全法律研究中心编译）

法案原文链接：

https://www.congress.gov/bill/115th-congress/senate-bill/2289/text

5. 美国参议员提出法案，惩治通过网络干预选举的行为

1 月 16 日，美国参议员马克·卢比奥和克里斯·范·霍伦提出《2018 年通过设立红线保护选举法》（Defending Elections from Threats by Establishing Redlines Act of 2018），阻止外国对美国选举或出于其它目的的干涉，向企图干涉美国选举的外国势力发出强硬信号：攻击美国大选候选人、竞选活动或投票基础设施将面临严重的后果。

根据法案要求，美国国家情报总监（DNI）必须在每次联邦选举之后的一个月内，向美国国会报告是否有外国政府干涉此次选举活动。美国必定进行报复的选举干涉行动包括：

1）外国政府或其代理人不得购买广告（包括在线广告）影响美国选举。

2）外国政府或其代理人不得使用社交及传统媒体向美国公民传播大量虚假信息。

3）外国政府或其代理人不得入侵、公开或篡改美国选举及竞选基础设施，包括选民登记数据库和竞选电子邮件。

4）外国政府或其代理人不得阻止或妨碍选举基础设施的访问权，例如提供投票位置信息的网站。

对于制裁方式，该法案提出，如果美国国家情报总监（DNI）认定克林姆宫再次干涉美国联邦选举，俄罗斯将面临一系列严厉的制裁，且在 DNI 认定后 10 天内执行，对俄罗斯经济主要行业实施制裁，包括金融、能源、国防、金属及采矿业。根据美国 2017“通过制裁打击美国对手”法案确定的俄罗斯高层政治人物或寡头政治者将被列入黑名单，禁止其入境美国，并冻结资产。

法案还要求美国政府与欧盟合作共同阻止俄罗斯干涉选举的网络攻击活动，协调制定类似与此法案的立法，扩大影响力。

除俄罗斯之外，美国国家情报总监（DNI）已经将中国、伊朗和朝鲜列为主要的网络威胁国，认为这些国家也可能会在美国下一个选举周期利用其薄弱环节发起攻击。根据法案要求，美国政府应向美国国会提交计划，详述如何防止这些国家以及其它国家干涉美国选举。

法案原文链接：

https://www.congress.gov/bill/115th-congress/senate-bill/2313/text?r=16

6. 美国众议院通过《2017 年网络外交法案》

1 月 17 日，美国国会众议院通过《2017 年网络外交法案》（Cyber Diplomacy Act of 2017）（以下简称该法案）。该法案最初由众议院外交事务委员会主席罗伊斯（Ed Royce）于 2017 年 9 月 14 日提出，2018 年 1 月 17 日在众议院进行投票通过，接下来该法案将提交至参议院审议。

在该法案中，美国国会详细阐述了颁布法案的理由和目的。美国国会认为，在 2011 年 5 月 16 日发布的网络空间国际战略中，美国的国家目标在于“通过国际合作提升支撑美国国际商贸活动的信息和通信基础设施的开放性、交互性、安全性和可靠性，强化国际安全，促进言论自由和创新。”

该法案确定了美国网络空间的一般性国际政策，要求美国与盟国和其他合作伙伴进行国际合作，采取“多利益攸关方”的模式开展互联网治理，促进网络空间的开放性、交互性、可靠性和安全性，保障人权和民主，包括促进言论自由、创新和经济繁荣，同时尊重隐私，防范欺骗、欺诈和盗窃。

该法案要求设立网络事务办公室，其负责人与外交大使具有相同的职权，由总统任命，主要负责开展网络空间外交工作；在全球促进信息和通信技术基础设

施的开放性、交互性、可靠性和安全性；代表国务卿参与机构间发展和推进美国国际网络空间政策的工作等工作。

该法案要求发布针对人权实践的年度国家报告，主要针对外国涉及电子信息言论自由的评估，包括评估信息管控的程度；评估与自由表达相关的处罚程度；评估政府对个人信息不当利用的程度；评估网络监控的程度。（公安部第三研究所网络安全法律研究中心编译）

法案原文链接：

https://www.congress.gov/bill/115th-congress/house-bill/3776/actions?q=%7B%22search%22%3A%5B%22Cyber+Diplomacy+Act%22%5D%7D&r=1

7. 特朗普签署《FISA 修正案再授权法 2017》

1 月 19 日，美国总统特朗普签署《外国情报监控法修正案再授权法 2017》（FISA Amendments Reauthorization Act of 2017）。该法旨在对 1978 年通过的《外国情报监控法》进行修订，以改进外国情报的收集、安全保障、问责和监督等制度，同时延长该法第 702 条的有效期。该法案的主要内容包括：

1）明确情报信息的查询程序。根据该法的规定，总检察长应与国家情报局局长协商决定，采用符合美国宪法第四修正案要求的查询程序，并对于涉及美国公民的情报查询加以记录。联邦调查局(FBI)不得基于与国家安全无关的刑事调查获取美国公民的通信信息，除非获得法庭授权或有合理理由确信该内容可帮助减轻或消除生命威胁或严重的人身伤害。

2）明确情报信息的使用和披露限制。该法明确根据 702 条获取的情报信息原则上不能作为指控美国公民刑事犯罪的证据使用。除非 FBI 获得了情报监控法

庭的授权或者总检察长认为该信息与国家安全有关等。

3）要求总检察长对电子监控情况进行报告。该法规定，每年四月总检察长应向美国法院行政办公室、国会情报委员会，以及众议院和参议院司法委员会提交关于上一年度实施电子监控的情况报告。

4）规定国家安全局和联邦调查局应当任命隐私和公民自由保护官员。

5）将第 702 条的有效期延长至 2023 年 12 月 31 日。美国国会曾在 2008 年通过了《外国情报监控法》第 702 条，授权美国国家安全局在无需获得法院授权的情况下就可以监控境外的外籍人士，该条本于 2018 年 1 月 19 日到期。此次修订案对其有效期加以延长意味着美国情报机构将能继续在没有授权的情况下，监控美国境外目标的电邮和短信等通信。

针对该法的通过，1 月 19 日，白宫发表声明称：情报信息对于保障国家安全至关重要，美国面临着来自外国恐怖主义网络和其他外国分子的威胁。为尽早发现和预防攻击，美国在特定情形下应当有权力拦截外国目标的通信。第 702 条为此提供了必要的权限。此外，白宫表示，第 702 节为美国公民提供了强有力的隐私保护，第 702 节所规定的监听对象仅限于境外的外国人，而不包括美国公民以及位于美国的外国人。此外，根据第 702 节的规定进行监控时涉及到对美国公民的通信进行监听时，该法确立了一套附加程序为美国公民提供保护。（公安部第三研究所网络安全法律研究中心编译）

法案原文链接：

https://www.congress.gov/bill/115th-congress/senate-bill/139/text

白宫声明链接：

https://www.whitehouse.gov/briefings-statements/statement-president-fisa-amendments-reauthorization-act-2017/

附件 3——全球 ICT 行业信息安全相关认证

（一）法国 CSPN 认证

CSPN(Certification de Sécurité de Premier Niveau, 即一级安全认证)是 2008 年法国国家网络安全机构(ANSSI)采用的认证方案，CSPN 认证的主要目标是从以下三个方面验证特定产品是否符合相关安全要求：

1) 验证产品安全规范的符合情况；

2) 评估类似产品的原理和已知漏洞；

3) 产品安全功能绕过测试。

这种评估进行的是符合度分析（验证产品符合其安全规范，将产品作为一个整体进行相关分析）和效率分析（评定安全功能和安全机制的理论强度，并确定漏洞）。

对于评估目标（通用准则中的 TOE），CSPN 会分析其安全性，然后对 TOE 合规进行不同程度的入侵测试。需要重点强调的是，CSPN 主要对适配产品开发生命周期进行短期评估，如有强安全需求时，则要考虑协调新产品进入市场的时间。

CSPN 评估由 ANSSI 许可的测试实验室进行，以此确保竞争力和独立性。

CSPN 方法的主要步骤为：

- 准确描述安全对象评估范围（需要时，产品的部分功能可从评估项中排除），这一步由开发人员和评估者共同完成。
- ANSSI 检验安全目标。
- 开发人员将所有评估材料交给评估者。这个评估材料可不包括源代码，但至少应包括一个完整功能版本的产品，并详细描述所实施的加密协议。
- 产品评估。首先，双方会协商整体产品评估时间，在这一步中，评估者

和开发人员之间会进一步交流。开发商可能需向评估人员提供额外材料，或者回答评估人员的部分提问。该步骤结束后，评估者会提供列出所有测试评估结果的详细报告，以及所有未披露的安全问题清单。

- 验证 ANSSI 报告的结论。
- 由 ANSSI 交付 CSPN 证书。

CSPN 是 CC 的互补而不是替代，其主要在受限时间内完成对 TOE 的安全分析并发现安全漏洞。典型的 CSPN 认证需时 25 天左右，明显低于典型的 CC 认证。

（二）英国 CPA 认证

CPA(Commercial Product Assurance, 即商业产品认证)是英国政府通信总部(GCHQ)下属的电子通信安全工作组(CESG)所使用的安全认证方法，其提高了商业产品在信息安全方面的可信度。CPA 旨在确定产品符合相关安全要求，英国政府相关机构会根据已发布的CPA 安全特征对产品的软硬件进行安全测试和认证，以确保敏感数据和信息的安全性。此外，其主要目标之一是通过提供基于证书的安全产品认证，巩固以前的 CESG 计划。

CPA 对通过评估的安全产品会授予认证证书，证书意味着该产品被证明表现出良好的商业性安全实践，适合较低的威胁环境。CPA 认证有效期为两年，并允许产品在认证期限内进行必要的更新。

虽然 CPA 旨在取代其他信息安全认证方法，如通用准则 CC，但由于没有 CPA 的互认协议(MRA)，在英国测试的产品通常不会在其他市场被接受。

（三）云端安全认证之云安全联盟 CSA STAR

CSA STAR 云安全评估是基于国际权威非盈利组织云安全联盟(CloudSecurity Alliance, CSA)推出的云控制矩阵(Cloud Control Matrix，CCM)，满足云计算安全领域特定要求，针对云计算安全特性的一项国际性认证。同时它也是 ISO/IEC 27001 的增强版本，将云安全的特有问题可视化，为云服务商的安全管控能力提供了直观的评估框架。

CSA 与行业工作组共同开发出云控制矩阵 CCM，规定了云安全相关的常用控制措施，填补了相关空白。英国标准协会 BSI 与 CSA 通力合作，基于该矩阵开发出全新的安全、信任和保证注册(Security, Trust & Assurance Registry, STAR)云安全评估。该评估分为三个层级，每个层级为云服务供应商提供增量级别的信任和融合度，也为云用户提供更高安全级别的安全保障。

三个级别的认证描述分别为：

1) 第一级：自我评估。由云端服务提供商填写自我评鉴问卷，自我宣告对于 CCM 的遵循程度，并上传至 CSA 的官方网站供公众查阅。

2) 第二级：独立第三方认证。由第三方机构依据 ISO27001、CCM 及管理能力模型进行认证，确保供应商满足 CSA 的 CCM 要求。

3) 第三级：持续监控。云服务提供商公布基于 CSA 云计算信任协议的安全监控结果，对云服务相关安全要求进行持续的审计和评估。

CSA STAR 评估方案在企业采用云服务方面提供协助，拥有更高的透明度，使云服务供应商(CSP)能够增强其利益相关方的信心，使用户相信供应商已部署了必要的控制措施来确保云端数据安全。

附件 4——美国 CCEVS 认证要点解读

通用准则评估与认证制度(CCEVS)是对美国信息技术安全性的评估与认证的一项基本制度。这项制度由美国国家信息安全保障合作组织(NIAP)负责运行与管理。NIAP 由美国国家标准与技术研究院(NIST)和美国国家安全局(NSA)联合成立并进行管理。同时，NIAP 也负责通用准则测试实验室(CCTL)的管理与使用。当然这些实验室也要满足 NIST 管理的国家实验室自愿认可程序(NVLAP)的要求。

申请 CCEVS 认证有三个关键阶段。

第一阶段：初始确认监督审核(IVOR)，主要是确定安全目标(ST)，评估人员能否清晰准确定义评估对象(TOE)以及相应的安全措施和要求，还有 CCTL 对安全目标进行了正确的评估活动。IVOR 后，进行启动会议制度，通过后 CCEVS 接受此次申请，并把申请认证的产品加入网站上“在评估中”的列表里。

第二阶段：测试确认监督审核(TVOR)，主要是在完成 ST 的评估活动后，CCTL 根据申请方的技术资料和认证产品制定测试计划，准备实施测试。

第三阶段： 最终确认监督审核(FVOR)，主要是审核评估 CCTL 的测试评估结果，确认所有遗留问题都已经解决，可以获得认证证书。

本部分就 CCEVS 对于评估认证过程中关注度较高的一些要求和制度进行总结与解读。

一、实验室的选择

申请美国 CCEVS 认证，评估测试工作和与 CCEVS 认证人员的沟通交流都由 CCTL 完成。申请方确定要申请认证后，要准备评估所需的技术资料和认证产品，以及提供通过评估要求的各种证据资料和其他必要的支持。CCTL 帮助申请方准备评估资料和完成 ST 的评估活动，并向 CCEVS 提出认证申请，完成 CCEVS 要求的各种报告，最终通过认证。所以 CCTL 的选择对于是否能够获得认证证书

很重要。

申请方可从 CCEVS 网站上公布的认可的 CCTL 列表中选择，并综合考虑实验室人员的技术能力、认可的评估范围、已经完成的评估产品、费用等因素，完成评估产品并获得认证证书的经验对于通过认证会有很大帮助。目前 CCEVS 公布了 9 家认可的实验室。

某些情况下，尤其是对美国 CCEVS 了解不多时，可以考虑选择一些咨询服务帮助通过认证。咨询人员的经验和能力决定了能否帮助申请方较快通过认证，包括通用评估准则(CC)的理解、CCEVS 的了解、认证产品技术知识掌握等因素。如果选择的咨询服务不合适，可能会导致认证时间更长，甚至不能通过认证。大多数 CCTL 可以提供咨询业务，当然，也可以选择非 CCTL 的咨询人员。但是，要与 CCTL 进行沟通，因为有些 CCTL 不受理某些特定咨询人员参与的评估项目。

二、保护轮廓(PP)或认证级别的选择与确定

保护轮廓为一类产品定义了一组与实现无关的 IT 安全要求，相当于我国信息安全产品认证体制中的产品标准，例如，我国发布的 GB/T 2028l - 2006 信息安全技术防火墙技术要求和测试评价方法，实际上就是一个保护轮廓。

认证级别或者 PP 的选择将会影响评估认证需要时间的长短，甚至会影响最终能否获得认证证书。根据最新要求，CCEVS 一般不受理超过 EAL2（EAL 为评估保证级）或不符合 NIAP 认可 PP 的认证申请，而且在不断减少 EAL4 的申请。英国、加拿大、澳大利亚和新西兰认证制度与美国有类似的改革倾向。所以，申请方在启动认证项目之前，要与 CCTL 深入沟通咨询，慎重选择在认证依据的 PP 以及级别。

总结 CCEVS 以往的认证经验，认证级别不断提高、评估所需时间较长、代价过大、不适应 IT 技术的快速更新等因素，2011 年 12 月，发布白皮书《Technical

Communities: A Collaborative Approach for Protection Profile Development》，用于指导 PP 的编写与维护。在这之前，PP 的编写主要是由 NIST 或 NSA 主导，而根据白皮书的要求，不同领域的 PP 编写将由相应的技术委员会负责。技术委员会的负责人由 NIAP 指定，但是成员构成可以来自不同国家、不同组织、厂商等各个领域。

每当 NIAP 发布新 PP 时，会有 6 个月过渡期(TW – Transition Window)，同时发布 TW 的开始与结束日期。过渡期内，申请方可以根据 PP，或者根据 EAL2 的 ST（需持有政府客户的意向书(LOI)，如美国政府、北约(NATO)和通用准则互动协议(CCRA)下的外国政府）进行认证申请。如果过了过渡期，必须根据 PP 进行申请。在根据 NIAP 公布的 PP 进行评估时，必须完全符合 PP，不能采用高于或多于 PP 规定的测试要求和评估要求。如果没有公布的 PP，申请方可以与 NIAP 联系协商解决。而高于 PP 规定等级的评估，超出了 NIAP/CCEVS 的职权范围。

目前，NIAP 制定公布的 PP 非常有限，而且其他制度中还有一些规定，要求索引以前 PP 规定的级别，如基本级、中级或高级等。如联邦信息处理标准 FIPS I40-2（密码模块安全要求）安全级别 4 (Level4)要求密码模块通过 EAL4 的认证，NIAP 正在努力与其他政府机构协调，更改这些要求，包括 NIST 在其他标准中删除关于评估保证级或强壮级的索引需求，又如信息安全保证(DOD8500)关于特定强壮性的需求（基本级或中级），已在 2003 年版中不再要求。

三、安全目标的编写与准备

ST 描述了一个特定 TOE（评估对象——Target of Evaluation）的安全要求，并规定了用于满足这些安全要求应该提供的安全功能和保证措施。ST 是申请方与评估者之间对于 TOE 安全特性和评估范围达成一致的基础。实践证明，如果 ST 对产品的认证范围定义不够清晰，将严重影响评估进度，甚至会影响最终是否能够通过 CCEVS 认证。因此，CCEVS 对于提交认证申请时的 ST 的质量要求

越来越高，要求 ST 中必须清晰定义 TOE 的认证范围和安全特征。

ST 是 IVOR 重要输入资料之一，只有通过 IVOR 审核，CCEVS 才会给认证申请分配相应的审核资源和相应的项目编号，允许认证产品公布在 CCEVS 网站上“在评估中”列表中。因此，ST 必须清晰、完整、准确地描述 TOE 的物理与逻辑边界。边界描述能够为界定产品认证范围提供充分的信息，并清晰描述属于产品认证范围，但是不支持满足安全功能要求的内容。产品认证范围应该包括产品具有的市场行为的安全特征，否则在认证版本中关闭这些功能。如果 CCEVS 认为产品范围没有包含其本身应该具备的安全特征，可能会拒绝受理认证申请。在进行 IVOR 审核之前，CCTL 已经对 ST 进行了评估，并且要形成评估技术报告(ETR—Evaluation Technical Report)，与 ST 一起提交。

四、影响认证时间的因素

随着信息技术的快速发展，产品的生命周期不断缩短，对完成评估认证所需时间提出了更高的要求。所以，CCEVS 要求所有符合 NIAP 认可的 PP 的评估必须在 12 个月内完成，但对于某些要求的 EAL4 (没有 PP 或者超过 PP EAL 定义的要求)评估除外，这种情况要在 24 个月内完成。评估时间的计算从启动会议日期开始，到所有 FVOR 会议中的问题都根据 CCEVS 的要求进行了纠正或解决为止。如果不能在规定的时间期限内完成评估，将导致认证申请失败。考虑到 CCEVS 对于评估时间期限以及评估过程中的阶段点（如 TVOR 或 FVOR）严格的要求，而且通常申请数量多于可用资源，所以在评估准备阶段或者评估进程中，要密切关注 CCEVS 对于审核资源的安排计划与优先级。CCEVS 在网站上公布了一年内的审核资源和时间安排，申请方与 CCTL 根据具体情况，选择合适的时间段。一般来讲，CCEVS 按照以下优先级顺序安排审核资源。

(1) FVOR 具有第一优先级，如果资源不够，按照下面的顺序分配资源： (a)根据 NIAP 的 PP 进行认证的产品； (b)非 NIAP 认可 PP 的产品。

(2) TVOR，如果资源不够，按照(1)的顺序。

(3) IVOR，如果资源不够，按照(1)的顺序。如果资源还是不够，将顺延到下一个月。

在某些特殊情况下，根据关键客户的需求，可能存在例外情况。

五、认证结果的公示

美国 CCEVS 认证结果的公示方式大致分为两个阶段：(1)在评估过程中，将在 CCEVS 网站上“在评估中”列表中公示； (2)获得认证证书后，将在 CCEVS 网站的认证产品列表中公示，而且 CCEVS 将根据 CCRA 协议，联系协调在通用评估准则(CC)网站上公示认证产品。

在通过 IVOR 后，根据申请方的需要，认证产品可以列在 CCEVS 网站上“在评估中”的列表中。当 CCEVS 认为评估活动已经停止时，认证产品将从“在评估中”列表中移除。如果 CCTL 多次尝试联系申请方获取评估需要的证据而没有收到回应，或者评估活动的里程碑（如 TVOR 或 FVOR）不能在合理的时间内安排，CCEVS 则认为评估活动已经停止。此时，CCEVS 将与 CCTL 沟通确认评估项目的状态，并且书面通知 CCTL、申请方和认证人员将要终止此认证项目。如果 CCEVS 通知书上条款不能满足（以前的要求是收到 CCEVS 的通知后，30 天内没有响应），评估项目将被关闭，评估产品将从“在评估中”列表中移除，分配给认证项目的认证资源也将被撤销。CCEVS 将书面通知 CCTL、申请方和认证人员正式停止项目的日期。

值得注意的是，根据 CCEVS2011 年 12 月 29 日发布的公告，在 2012 年 8 月 1 日后，对于认证产品和 PP 的“在评估中”列表将不再使用。因为根据 CCEVS 的要求，现在申请认证必须选择符合 NIAP 认可发布的 PP，并在 12 个月内完成评估，因此“在评估中”列表最初的作用已经不适用。

认证产品获得认证证书后，将在 CCEVS 的网站上进行公示。为了避免具有

已知脆弱性的产品获得认证证书，CCEVS 要求在评估前或评估进行中的任何时候，发现的认证范围内的任何脆弱性，必须在颁发证书前进行纠正。CCEVS 不能接受重新定义 TOE 边界的方式处理已经发现的脆弱性。同时，CCEVS 也建议纠正产品具有的、在认证范围之外的脆弱性，但这些脆弱性是否处理不影响获得认证证书。如果在发证时，已知的脆弱性没有得到纠正，CCEVS 将在其网站上公布的获证产品列表中进行提示，并将这些脆弱性写入认证报告[6]。

[6]注：本部分内容来自期刊论文：崔占华.美国 CCEVS 认证要点解读[J]. 认证技术, 2012, (第 7 期).

EAL3 级认证申请附件的基本要求

1 安全目标

申请者提供的文档《安全目标》(《安全目标》编写方法参见《PP 和 ST 产生指南》)应包括如下内容：

1.1 引言

1.1.1 ST 和 TOE 的标识

1) 包括 ST 标识信息，如 ST 标题、版本号、出版日期和作者；
2) 包括 TOE 标识信息，如 TOE 名称、TOE 版本号；
3) 包括开发此 ST 所依据的国家标准 GB/T18336 或 PP 的标识信息：版本号，名称和出版日期。

1.1.2 ST 概述

ST 概括介绍 TOE 的主要组成、功能、应用环境。

1.1.3 一致性声明

列出 TOE 与国家标准 GB/T18336 和 PP 的符合性声明。
说明 TOE 安全功能强度等级：基本级功能强度（SOF-basic)、中级功能强度（SOF-medium)、 高级功能强度（SOF-high)。

1.2 TOE 描述

1.2.1 产品类型

介绍 TOE 所属的产品类型，如防火墙、智能卡、加密调制解调器、Web 服务器和企业内部网等。

1.2.2 TOE 结构

详细介绍 TOE 的组成,如 TOE 由几个模块或子系统组成,每个模块或子系统的组成及其功能和 TOE 各个组成部分对运行环境的要求等。

1.2.3 TOE 的范围和边界

1) 物理范围和边界，详细介绍构成 TOE 的硬件、软件和固件，并介绍 TOE 的配置；
2) 逻辑范围和边界，描述 TOE 提供的 IT 安全特征。

1.2.4 应用环境

描述 TOE 的使用环境及在其中发挥的作用。

1.3 TOE 安全环境

1.3.1 假设

1) 包括 TOE 预期使用方面的假设，如 TOE 预期应用、需要 TOE 保护的资产的潜在价值、以及使用 TOE 可能存在的限制；
2) 包括为保证 TOE 安全地行使功能，对 TOE 使用环境的物理、人员、连接性方面的假设：
   a) 物理方面，对 TOE 的物理位置或附加外围设施做的假设；
   b) 人员方面，对安全环境内的用户和 TOE 管理员，或其他人员所作的假设；
   c) 连接性方面，对 TOE 与 TOE 之外的 IT 产品或系统相连的假设。
3) 列出上述所有的假设（对假设进行标识并作出相应的解释)。

1.3.2 威胁

列出所有与 TOE 安全运行相关的威胁（对威胁进行标识并作出相应的解释)。

1.3.3 组织安全策略

主要包括 TOE 及其应用环境必须遵守的法律、法规、规定或指南。

1.4 安全目的

列出所有的安全目的：TOE 安全目的和环境安全目的，并对确定每个安全目的的理由作出详细地解释。如这个安全目的能够对抗前文中所述的哪些威胁，满足了哪些组织安全策略或假设。

1.5 IT 安全要求

如果有对应的 PP，这部分按照 PP 的相应部分来写，否则，按照下面的要求来提供 IT 安全要求。

详细描述 TOE 或其环境应满足的 IT 安全要求：TOE 安全要求和 IT 环境安全要求，最好参照国家标准 GB/T18336 第二部分或第三部分要求的表述方式。

TOE 安全要求指的是为实现 TOE 安全目的而提出要求，TOE 及其相关的支持性文档应满足的这些要求。IT 环境安全要求指的是为实现 IT 环境安全目的，必须通过其应用环境、而非 TOE 本身满足的要求。

1) TOE 安全要求包括 TOE 安全功能要求和 TOE 安全保证要求。
   a) TOE 安全功能要求主要指的是从 GB/T18336 第二部分功能要求组件中抽取的那些功能要求，还可以有非 GB/T18336 第二部分功能要求组件中的功能要求；
   b) TOE 安全保证要求主要指的是从 GB/T18336 第三部分保证要求组件中抽取的那些保证要求，还可以有非 GB/T18336 第三部分保证要求组件中的保证要求。
2) IT 环境安全要求应确定 TOE 的 IT 环境应满足的 IT 安全要求。
   IT 环境安全要求包含 IT 环境安全功能要求和 IT 环境安全保证要求。例如，TOE 为防火墙产品，它依赖底层操作系统，操作系统提供管理员的身份认证和审计数据的永久储存。因此，IT 环境安全要求应包含 FAU 类和 FIA 类（参见 GB/T18336 第二部分）的功能组件。

1.6 TOE 概要规范

TOE 概要规范指的是 TOE 安全要求的具体实现，应详细描述符合 TOE 安全要求的 TOE 安全功能和保证措施。

1) TOE 安全功能包含 IT 安全功能，并说明这些功能是如何满足 TOE 安全功能要求的。可以通过功能和要求间双向映射的方式来表达。
2) TOE 的保证措施应列出所有符合 TOE 安全要求的保证措施，并说明这些保证措施是如何满足 TOE 安全保证要求的。可以通过保证措施和要求间双向映射的方式来表达。

1.7 PP 声明

如果在 ST 引言中声称符合一个或多个 PP，本节应该介绍这些 PP，还应说明为满足 ST 要求，对 PP 进行的裁剪和附加项。

1.8 基本原理

1.8.1 安全目的基本原理

阐明安全目的能够映射到 TOE 安全环境里的所有方面：假设、威胁和组织安全策略：

1) 这些安全目的的符合了列出的所有假设和组织安全策略的要求，能够对抗列出的所有威胁；
2) 所有安全目的的都是必需的；
3) 可以通过安全目的和 TOE 安全环境（假设、威胁和组织安全策略）间双向映射的方式来表达。

1.8.2 安全要求基本原理

阐明 TOE 及其环境安全要求适于满足、并能够映射到安全目的：

1) TOE 及其安全环境的功能和保证要求组件能够满足列出的所有安全目的；

2) 所有 TOE 及其环境安全要求组件都是必需的；
3) 可以通过 TOE 及其环境安全要求和安全目的间双向映射的方式来表达。

1.8.3 TOE 概要规范基本原理

说明 TOE 安全功能和保证措施适于满足 TOE 安全要求：

1) TOE 安全功能能协同运作，满足 TOE 安全功能要求；
2) TOE 功能强度声明是有效的；
3) TOE 保证措施与保证要求相一致的声明是合理的。

1.8.4 PP 声明基本原理

解释 ST 安全目的和要求与所有声明一致的 PP 之间的区别。没有区别，则无须说明。

2 配置管理文档

应包含配置管理范围、配置清单和配置管理计划。

2.1 配置管理范围

配置管理范围应包括在 TOE 的整个生命周期中，对 TOE 的实现表示、设计文档、测试文档、用户和管理员指南、配置管理相关文档等方面进行配置管理。

2.2 配置清单

配置清单应包括达到相应保证级别的所需的全部文档，列出 TOE 各组成部分的配置项，不仅要唯一标识出每个配置项的版本信息（如版本号、制造方等），还要作出详尽的解释。

2.3 配置管理计划

配置管理计划应包括如何使用配置管理系统保持 TOE 配置项完整性的描述、配置管理系统记录及防止对配置项被未授权的修改，还应包括 TOE 整个生命周期中标识每个配置项的方法。

3 交付和运行文档

3.1 交付文档

应描述为保证 TOE 安全地提交给用户而必需的所有交付程序。
交付程序适用于整个 TOE，包括可用的软件、硬件、固件和文档；交付程序适用于从生产环境到安装环境的整个交付过程（例如打包、存储、发布）的各个阶段；

3.2 安装、生成和启动程序

应描述为达到 ST 中安全配置，TOE 所必需的所有安装、生成和启动程序。

4 功能规范

描述 TOE 安全功能及其所有外部接口；
TOE 安全功能描述应比 ST 中 TOE 概要规范的安全功能描述更详尽。

5 高层设计

高层设计应满足所有的 ST 安全功能要求。可以从 TOE 安全功能子系统的角度，对每个子系统的安全功能进行描述，并标识所有子系统接口和子系统外部可见接口。如果 TOE 安全功能的实现依赖 IT 环境的安全要求，那么还要描述在底层硬件、固件、软件中实现的保护支持机制提供的功能。

6 开发活动的对应性分析文档

应该包括以下两种对应性分析：

1. ST 中的 TOE 概要规范和功能规范之间的对应性分析；

该对应性分析应该阐明 TOE 概要规范的安全功能和功能规范中的接口描述之间的关系，能够证明两者的安全功能是相同的。

2. 功能规范和高层设计之间的对应性分析；

该对应性分析应该阐明功能规范中的每项安全功能能够映射到高层设计中的 TSF 子系统之间的关系（即针对每项安全功能而言，该分析能够说明是由哪个 TSF 子系统来实现的）；能够表明高层设计正确并完整地描述了功能规范。

7 指导性文档

7.1 用户指南

应详细说明 TOE 安全功能和接口及有关 TOE 安全使用方面的信息。

7.2 管理员指南

应就管理员如何以安全方式管理 TOE 进行详细而全面地说明。

8 测试相关文档

包括测试文档、测试范围分析和测试深度分析。

8.1 测试文档

包括测试计划、测试程序、预期测试结果和实际测试结果和测试方法、测试工具和测试步骤。必要时，应提供测试工具和手段。

8.2 测试范围分析

阐明测试文档中列出的测试与功能规范是一致的。可采用表格或矩阵的形式来描述其对应关系。

8.3 测试深度分析

阐明测试文档中列出的测试与高层设计是一致的。可采用表格或矩阵的形式来描述高层设计和测试计划与过程之间的对应关系。此外，还应说明高层设计中的所有子系统和内部接口，以及每个子系统都相应测试。

9 生命周期支持相关文档

为保护 TOE 及其相关设计信息在 TOE 开发和维护期间免受干扰或暴露，开发者应提供生命周期有关的支持活动，即应包括 TOE 开发全过程的安全措施。

9.1 开发安全文档

开发安全文档是指开发者对开发环境的安全控制。

应包括在 TOE 的开发环境中用于保护 TOE 设计和实现过程的机密性与完整性的物理、过程、人员等方面安全措施。

10 脆弱性分析

包括 TOE 安全功能强度分析和脆弱性分析。

10.1 TOE 安全功能强度分析

对在 ST 中做出安全功能强度声明的安全功能进行分析。

10.2 脆弱性分析

阐明经过在 TOE 所有有关领域（如所有提交评估的文档和 TOE 本身等）的查找，在预期使用环境中 TOE 是否存在明显可利用的脆弱性；如果有，应列出所有存在的明显脆弱性，并加以说明，如在预计的环境中是否有阻止利用明显脆弱性的措施。

11 质量保证体系文件

11.1 文件控制程序

申请方应提交组织内部的文件控制程序；

文件控制程序应对如下方面进行控制：

a） 文件发布前得到批准，以确保文件是充分与适宜的；

b） 必要时对文件进行评审与更新，并再次批准；

c） 确保文件的更改和现行修订状态得到识别；

d） 确保在使用处可获得适用文件的有关版本；

e） 确保文件保持清晰、易于识别；

f） 确保外来文件得到识别，并控制其分发；

g） 防止作废文件的非预期使用，若因任何原因而保留作废文件时，对这些文件进行适当的标识。

11.2 过程控制

申请方应明确定义产品的生命周期阶段划分，并对各个阶段的质量和安全控制措施进行描述。

11.3 质量检测报告

申请方应对产品实施检测，并如实提交其全部的自测报告。

11.4 资源管理

申请方应描述产品实现过程中所需的全部资源，如：人力、工具和技术。

11.5 记录控制

申请方应提交组织内部的记录控制程序；

列举产品实现过程中的全部记录清单，如：需求分析、设计分析等。

11.6 不合格品控制

描述产品实现过程中的不合格品控制措施。

11.7 质量手册

申请方应提供其质量手册的最新版本；

11.8 管理评审、内审

申请方应提供其最近一次管理评审和内审的记录；

11.9 采购控制

指出产品实现过程中所需的外购部件，包括外包。描述选择、评价和重新评价外购供应商能力的准则。提供近期的评价结果及评价所引起的任何必要措施的记录。

描述如何对外购部件或外包行为进行质量控制。

11.10 纠正和预防程序

提供组织的纠正程序。

纠正程序应覆盖如下内容：

a） 评审不合格（包括顾客抱怨）；

b） 确定不合格的原因；

c） 评价确保不合格不再发生的措施的需求；

d） 确定和实施所需的措施；

e） 记录所采取措施的结果

f） 评审所采取的纠正措施。

提供组织的预防程序。

预防程序应覆盖如下内容：

a） 确定潜在不合格及其原因；

b） 评价防止不合格发生的措施的需求；

c） 确定和实施所需的措施；

d） 记录所采取措施的结果；

e） 评审所采取的预防措施。

11.11 服务过程控制

提供产品售后服务内容和规定。