计算机科学 2002Vol.29№.9

信息安全评价准则研究综述与探讨*)

Research and Development of the Information Technology Security Evaluation Criteria

梁洪亮　孙玉芳

(中国科学院软件研究所　北京 100080)

Abstract　Information technology security evaluation criteria are the navigation mark for information security technology and the activator for the market of secure information products or systems. The origin and development history of information technology security evaluation criteria are surveyed, the achievement and flaws of these criteria are analyzed, and several important problems related to security criteria are discussed. Lessons gotten from the development and further directions are proposed.

Keywords　Information security, Security evaluation, Evaluation criteria

1. 简介

现实生活离不开安全,信息系统也一样,信息安全可以说是信息系统的一种属性。从70年代开始,对信息安全系统和安全产品的研制日益得到了政府和市场的重视。但是,对于某个厂商所提供的一个安全系统或产品,人们根据什么来相信它是安全的?显然,大多数用户不是安全专家,因此,他们无法验证厂商的测试是否彻底和准确,无法检查厂商提供的正确性证据有效与否,无法决定安全商品是否正确实现了某种安全政策。因此就产生了对独立第三方的评价的迫切需要:独立的安全专家可以审查一个产品或系统的需求、设计、实现和可信度证明,从而向用户提供购买使用的可信依据。图1描述了世界各国评价准则的开发历史。

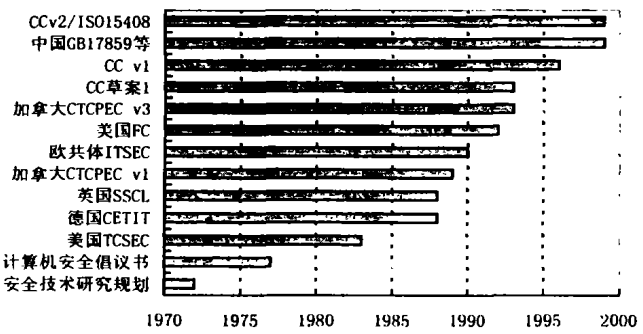

图1　安全评价准则开发历史

从图1可以看出,许多国家在制定评价准则上都作出了努力,历史上也出现了较多的评价准则。后面几部分我们将会详细考察这些标准的制定情况。另外可以看出,中国的标准开发工作是比较落后的。本文的目的在于,通过对世界上信息技术安全评价准则的研发历史进行考察,从中发现哪些问题是可以避免的,哪些长处应该是后继的标准开发者所吸取的,并探讨信息系统安全评价技术可能的发展方向。

2. 研发历史

早期的安全评价准则的研发工作主要是源于军事需要,并且主要考虑机密性。1972年,美国的Anderson所写的安全技术研究计划[1],第一次提出了进行独立的系统评价的概念。1977年,MITRE公司的David Bell和Leonard La Padula发表了著名的BLP模型[2]。可以说,他们的开创性的工作几乎构成了所有安全评价的基础,在BLP模型中定义的安全标记和支配关系至今仍在使用。

2.1　美国的TCSEC

在70年代末期,美国国防部就意识到了建立安全评价方案的必要性,并于1983年公布了可信计算机系统评价准则(TCSEC),亦即众所周知的桔皮书[3]。它分为四区七级,评价级别依次递增。D,C1,C2,B1,B2,B3和A1级分别表示最小保护、自主保护、受控保护;标记化保护、结构化保护、安全域保护及验证设计保护。图2表示了针对每个级别的安全需求。

其中,属于安全政策方面的要求有:DAC-自主访问控制,OR-客体重用,L-标记,LI-标记完整性,ELI-标记信息导出,LHO-可读标记输出,MAC-保密性访问控制,SSL-主体敏感标记和DL-设备标记。属于可追踪性方面的要求有:IA-身份表示和鉴别,A-审计和TP-可信通路。属于保证方面的要求有:SA-系统体系结构,SI-系统完整性,T-安全测试,DSV-设计规范和验证,CCA-隐蔽信道分析,TFM-可信工具管理,CM-配置管理,TR-可信恢复和TD-可信分布。属于文档方面的要求有:UG-安全特性用户指南,TFG-可信工具使用指南,TD-测试文档和DD-设计文档。

从图2可以看出,评价级别实际上可以分为四类:D没有任何需求,C1/C2/B1与大多数商业操作系统的安全特性相同,B2需要对所采用的安全模型提供安全证明以及对可信计算基提供描述规范,B3/A1需要更加精确的证据描述和可信计算基的形式化设计。其中,B1和B2以及B2和B3之间的需求差距最为严格。操作系统开发人员通过对现有的操作系统进行安全化增强,可以使之达到C1或C2或B1级别。但是要达到B2级必须在操作系统的设计阶段就要增加安全性考虑。更进一步,要达到B3或A1级别,在系统设计之初,应先构造安全模型,并对之进行形式化证明。

*)本项研究受到国家863高科技项目(No.863-306-ZD12-14-2)、国家自然科学基金项目(No.60073022)、中科院知识创新工程项目(No.KGCX1-09)和北京市重点技术创新项目的支持。梁洪亮　博士生,主要研究方向为信息安全与系统软件。孙玉芳　研究员,博士生导师,主要研究方向为系统软件和中文信息处理。

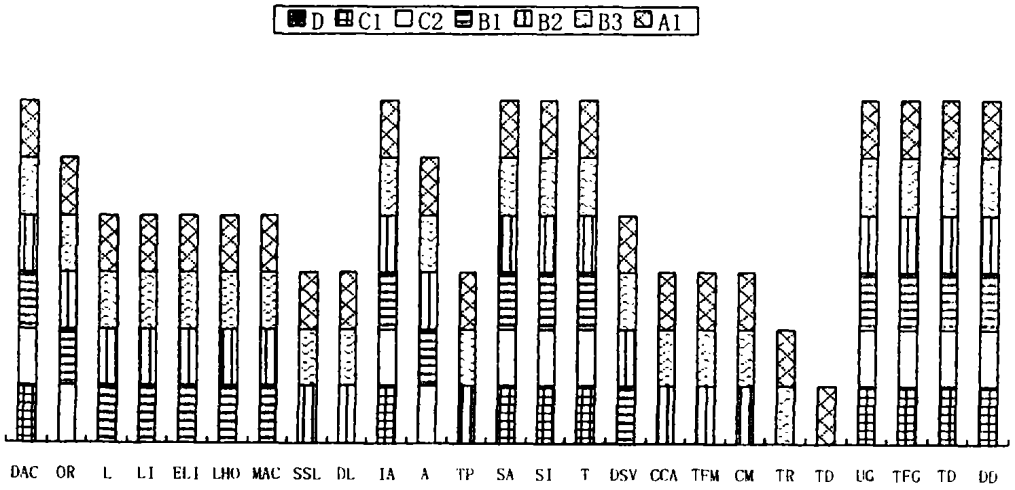

图 2 TCSEC 功能需求和评价级别的映射图

TCSEC 在当时无疑是对满足国防需求的主机(操作系统)系统的很好的评价标准,而且后面又补充发布了对网络和数据库的解释。但是它的缺点在于强迫商业领域的所有产品和系统都要遵从它的规定。它忽略了一个根本事实:政府和商业界本身具有不同的安全政策。另外一个错误是把功能特性同可信度捆绑在一起。也就是说,一个产品或系统要想达到某个可信评价级别,不管它的实际安全目的或安全需求如何,都必须遵从准则规定的那些功能特性。实际上功能特性越多,出现问题的可能就越大,并非越可信。第三,它对于隐蔽信道和审计追踪的要求太高,即使目前在技术上都是难以完全做到的。最后,它只注重了信息的保密性,而忽略了信息的完整性保护。

2.2 德国的 CETIT

英国、德国几乎同时独立地开始了评价准则的制定工作,并且在 1989 年都公布了他们的第一个标准草案。德国信息安全局(GISA)于 1988 年发布了它的第一个评价准则 CETIT(安全界称之为绿皮书)[4],其中提出了八个基本安全功能:标识和鉴别、权力的管理(任命和撤销)、权限的验证、审计、客体重用、错误恢复、持续服务和数据通信安全。这些安全功能当时被认为可以实现大多数的安全政策。其中前五个同 TCSEC 非常接近,但是后三个指明了全新的领域:数据完整性;数据源鉴别;不可否认性。为了方便用户选择安全功能集合,CETIT 定义了 10 个功能类(F1-F10)。前五个类类似于 TCSEC 的 C1 到 B3 级,类 6 针对数据库需求,类 7 针对可用性需求,类 8 针对信息完整性需求,类 9 针对加密产品,类 10 针对网络需求。在此基础上,GISA 制定了八个表示保障能力的品质级别(Q0-Q7),大体与 TCSEC 的七个可信级别相当。这些功能类和品质级别的组合能够产生 80 种不同的评价结果,但是 CETIT 并未声明所有组合都一定是有效的。表 1 列出了 CETIT 和 TCSEC 之间的对应评价关系。

CETIT 的目标是可以评价系统,也可以评价产品;既可以是军事应用,也可以是商业应用。并且把可信度同功能特性分隔开来。另一个贡献是允许使用商业评价方案来支持评价。缺点是没有描述如何构造功能类,也没有说明如何使新增加的功能类被接受为官方认可的。

2.3 英国的 SSCL

英国工商部和国防部合作开发,并在 1989 年公布了第一个英国标准 SSCL[5]。它的基础是一种称作断言语言的元语言。安全产品或系统制造商可以用它宣布一个产品或系统的安全功能。这种语言由许多带参数的行为短语和目标短语组成。通过替换参数和组合短语,可以声明一个安全产品或系统的安全功能。它实际上提供了一个开放的需求描述结构,开发商和评价方可以分别用它进行功能声明和验证。除了断言语言外,定义了六个可信评价级别(Q1-Q6),大致与 TCSEC 的 C1 到 A1 或德国绿皮书的 Q1 到 Q6 相当。

表 1 CETIT 和 TCSEC 的关系

	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7
F1		=C1						>A1
F2			=C2					>A1
F3				=B1				>A1
F4					=B2			>A1
F5						=B3	=A1	>A1
F6	新的功能类							
F7	新的功能类							
F8	新的功能类							
F9	新的功能类							
F10	新的功能类							

值得一提的是,断言语言有意设计为开放的结构,因为他们认为事先决定生产商在产品中选择那些功能是不可能的和不现实的。与此相反,德国和美国应该指导生产商具体选择哪些功能。其缺点是可能会出现这种情况:某个厂商的一个产品经过了一个或几个很弱断言的评价,却声称它是已经过评价的产品。很明显,这样会误导用户。

2.4 欧共体的 ITSEC

除英德以外,加拿大、澳大利亚和法国也在制订评价标准。并且他们的工作具有很多共同之处,这主要因为他们都得益于先前制定的标准。尽管各个国家都作出了自己的工作,仍然有三个问题明显定地暴露出来:各个国家的标准的兼容性,已评价产品的可转移性和产品的可销售性。实际上这是一个问题的三个方面。鉴于此,英德法荷四个国家在欧共体的支持和赞助下,合作开发了一个共同标准,供欧共体的所有成员国使用,此即 1991 年共同公布的信息技术安全评价准则(ITSEC)[6]。它保留了德国绿皮书中的十个功能类,又采纳了英国 SSCL 中的断言语言,还有与 TCSEC(D-A1)和德国绿皮书(E0-E7)类似的有效性组件。它指出评价对象(TOE)可以是产品,也可以是系统。生产商应该指明:系统安全政策、安全

功能规范、实施机制的定义和强度声明以及目标评价级别。评价机构应对如下几个方面作出评价：功能的适用性、功能的协调融合、脆弱性分析、易用性和机制强度。表 2 列出了 ITSEC 与 TCSEC 的不同之处及利弊分析[7]。

表 2　ITSEC 和 TCSEC 的比较

ITSEC 特性	优　点	缺　点
新的功能需求类	克服了传统的 TCSEC 的机密性要求；指明了需要安全产品的其他领域	需要用户作出较多选择
功能特性和可信度的分离	允许低可信级或高可信级的产品	需要用户决定何时使用高可信级别的产品；一些功能特性可能本身要求较高的可信级别，但不能保证得到
允许新的功能定义；可以独立于具体的安全政策	可对任何安全产品进行评价；厂商可以决定市场需要何种产品	难以对描述不同但功能类似的产品进行比较；厂商要尽量描述清楚产品的特性；预定义的特性集合可能不是有层次的
商业评价方案	由市场决定时间、价格和方案	政府对评价没有直接控制；厂商支付评价费用

ITSEC 很好地结合了 SSCL 和 CETIT 的工作，使评价准则的制定工作前进了一大步。但是它的缺点是把易用性作为一个主要评价目标。一个原因是，要求一个复杂的安全系统使用方便不太可能；另外，易用性本身是个主观的度量，例如有人喜欢用基于图形界面的浏览器，而有人喜欢基于文本的。

2.5　美国联邦准则

可能是作为对欧洲国家工作的回应，美国于 1992 年开始对 TCSEC 进行修改。并于当年由国家标准和技术局和国家安全局联合公布了美国联邦准则草案 FC[8]。它显然是受到了之前加拿大刚刚公布的标准草案和 ITSEC 的影响，把安全特性和保证要求进行区分。另外还考虑了向后兼容性的问题（因为有的产品已经或正在接受评价）。该草案始终未能作为正式标准出现，因为在接受了一轮反馈意见后，美国宣布同加拿大和欧共体一起制定通用准则（CC）。

该草案的主要贡献是提出了保护轮廓书（PP）和安全对象书（ST）的概念。PP 指明一种专门环境和一类通用环境下的功能和保证两个方面的保护要求。ST 是评价的基础，详述针对哪些威胁、满足哪些功能需求、采用了哪些机制以及可以达到什么保证级别，并给出令人信服的理论依据。另外它为一些特定应用（如网络通信交换和主机操作系统等）开发了专门的保护需求包。缺点是因为要保持同 TCSEC 的兼容性，使得它的通用性较差。

2.6　国际 CC 标准

从 1990 年起，国际标准组织（ISO）开始制定一个通用的国际安全评价准则，并且由联合技术委员会的第 27 分会的第三工作组具体负责。另一方面，各国都存在寻求共同认可的安全评价标准的意愿（事实上，加拿大的 CTCPEC V3 和美国的 FC 即是在这方面所作实验的成果）。为了融合各国所开展的安全评价工作，1993 年 6 月，CTCPEC、FC、TCSEC 和 ITSEC 的开发组织联合起来，组成了通用准则编辑部（CCEB），决定共同开展一项称为通用准则（CC）的项目。CCEB 于 1996 年 1 月完成了 CC v1，并用它做了大量的实验性评价，在对反馈意见进行广泛调研的基础上，于 1998 年完成了 CC v2，并最终被 ISO 接受为国际标准 ISO/IEC 15408[9]。基于历史原因及保持连续性起见，第三工作组同意 CC 术语可以继续使用。目前英、法、美、德等 14 个国家签署了 CC（ISO/IEC 15408）相互认可协议，即是说 CC 将会得到这些国家的广泛使用。

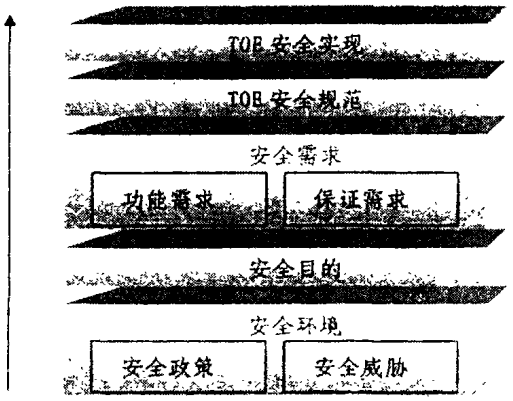

图 3　安全层次框架

CC 认为信息技术安全可以通过在开发、评价和使用中所采用的措施来达到。它清楚地提出了对信息技术安全产品或系统的功能需求和保证需求。功能需求定义了必需的安全行为；保证需求是得到用户信任的基础，以保证所宣称的安全措施是有效的并得到了正确的实现。如图 3 所示，CC 认为安全的实现应构建在如下的层次框架之上。

安全环境　使用评价对象（TOE）时须遵照的法律和组织安全政策以及存在的威胁。

安全目的　对防范威胁、满足所需的组织安全政策和假设的声明。

TOE 安全需求　对安全目的的细化，主要是一组对安全功能和保证的技术需求。

TOE 安全规范　对 TOE 实际实现或计划的实现的定义。

TOE 实现　与规范一致的 TOE 实际实现。

CC 对安全需求按照相关性进行分类，每一类子集称为一个组件。满足共同安全目的的一组组件构成一个族，具有相同意向的一组族构成一个类，对多个组件的直接组合构成一个包。对组件可以原样直接使用，也可以进行裁剪以满足具体的安全政策。每个组件表示和定义了允许的操作、应用的环境和结果。允许的操作包括迭代、复制、选择和求精。一个组件不能自足时就会产生与其他组件的依赖关系。每个组件应该指出它应当满足的依赖关系。

CC 中包含的安全功能类和安全保证类如表 3 所示。

表 3　CC 中的类

安全功能类	审计类，加密类，通讯类，用户数据保护类，表示和鉴别类，安全管理类，隐私权类，安全功能保护类，资源利用类，评价对象访问类，可信路径/通道类
安全保证类	PP 评价类，ST 评价类，配置管理类，交付和使用类，开发类，指南文档类，生命周期支持类，测试类，弱点评估类，可信度维护类

EAL1-功能测试级别
EAL2-结构化测试级别
EAL3-系统化测试和检查级别
EAL4-系统化设计、测试和审查级别
EAL5-半形式化设计和测试级别
EAL6-经过半形式化验证的设计和测试级别
EAL7-经过形式化验证的设计和测试级别

图 4 CC 的保证级别

CC 使用保证组件预定义了一组保证级别(见图 4)。一是为了向后兼容先前各种准则,也是为了保持通用保证包的内部一致性。较高的级别相对较低级别而言,要么使用同族中高可信度的组件替换低可信度的组件,要么是增加其它族中的保证组件。CC 允许对组件进行其他分组。为了满足具体的安全目的,可以通过增加一个或多个附加组件扩展某个保证级别。

可以认为,国际 CC 标准是目前最为完善的一个标准,它继承了先前各国标准的优势,并解决了以前标准中存在的概念和技术上的差别。它在具备向后兼容性的同时又具有开放性,可以适应未来技术的发展。但是,因为是一个新的标准,它的有效性还有待在实践中检验。

2.7 中国国家标准

中国于 1999 年公布并于 2001 年开始实施"计算机信息系统安全保护等级划分准则 GB17859"以及 GB/T 17900 网络代理服务器的安全技术要求、GB/T 18018 路由器安全技术要求等国家标准[10]。GB17859 规定了计算机系统安全保护能力的五个等级,分别接近于 TCSEC 的 C1-A1 级。它对 TCSEC 的扩展是,在每个等级里增加了对数据完整性的保护要求。客观地说,由于中国对安全评价的研究起步较晚,尽管没有太多的创新,但是这个标准的制定标志着中国对安全评价的重视。2001 年又公布了"信息技术-安全技术-信息技术安全性评估准则"系列标准 18336.1-.3(即国际 CC 标准的等同标准)。

3. 讨论

在考察了几个主要的评价准则以后,我们认为有三个问题值得探讨。

1)这些评价标准之间有没有相互的对应关系?如果有,是什么?

2)怎样来衡量一个评价准则本身的成功与否?

3)中国在信息安全评价领域可以吸取的经验和教训是什么?

第一,分析和对比几个主要准则的内容,我们发现在使用它们进行评价时,评价结果之间大体有着相互的对应关系,如表 4 所示。

表 4 TCSEC、ITSEC、CC 和中国 GB17859 的评价级别对应关系

TCSEC	ITSEC	CC	GB17859
D	E0	—	—
—	—	EAL1	—
C1	E1	EAL2	L1
C2	E2	EAL3	L2
B1	E3	EAL4	L3
B2	E4	EAL5	L4
B3	E5	EAL6	L5
A1	E6	EAL7	—

我们认为,这种对应关系的存在,一方面是因为在准则开发中考虑了兼容性的原因,另一方面是因为信息安全技术发展的共性和各国在安全评价领域有着大致相同的认识。

第二,衡量一个评价准则,我们认为可以考虑以下几个因素。

1)准则的可操作性;

2)准则的可扩展性(或开放性);

3)评价结果的连贯性;

4)准则的向后兼容性;

5)经过评价的产品的种类和数目以及这些产品的市场接受度。

其中,1)保证了准则可以得到具体实施;2)提供了适应未来信息安全技术发展的途径;3)和 4)保证了在不同的评价机构或不同时期,对用户的产品或系统应用同一准则得到的评价结果是一致的;5)是从最终用户的角度进行判断。

由此,我们认为,TCSEC 的可操作性和可扩展性很有限,联邦标准 FC 提供了较好的兼容性,英国标准强调评价结果的连贯性。根据英美等国在网站上发布的官方资料[11~13],我们可以分析国外几个主要标准的产品评价情况,如图 5 所示。从图中可以看出,ITSEC 出现以后,就逐渐替代了 TCSEC;而 CC 的出现,又逐渐替代了 ITSEC。

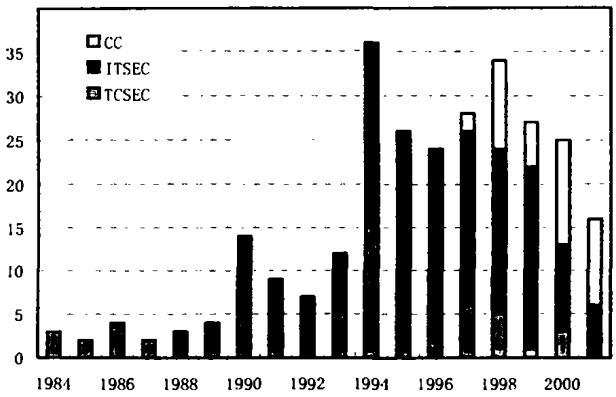

图 5 TCSEC、ITSEC、CC 产品评价比较

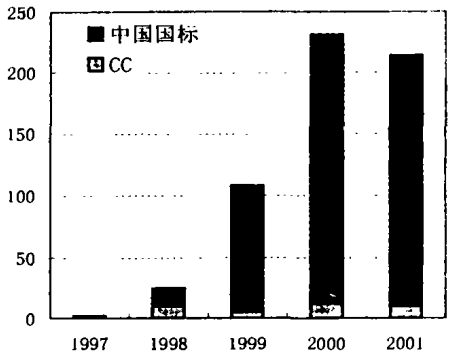

图 6 中国国标同国际 CC 产品评价比较

由文[14,15]提供的材料,我们可以得出我国 GB17859 等国标同国际 CC 标准的产品评价情况,如图 6 所示。可以看出,1999 年中国经过评价的产品数比 CC 五年间评价产品的数目还要多(实际上,根据美国、澳大利亚和英国等的官方报告,自 1984 第一个评价产品开始,目前共有 283 个产品经过了各国的评价)。一方面说明了中国信息安全市场很大和厂家的日益重视;另一方面也暴露了安全评价发展过速的问题。另外存在的一个情况是,除了公安部所属评价机构以外,中国国

家信息安全测评认证中心也称是代表国家对信息技术、信息系统、信息安全产品以及信息安全服务的安全性实施公正评价的技术职能机构，而且宣称，“中华人民共和国国家信息安全认证”是国家对信息安全技术、产品或系统安全质量的最高认可。

第三，通过分析上述安全评价准则的制定和执行情况，我们认为可以从中吸取如下的经验和教训：

1. 政府应该保证获得评价的产品可以在市场上得到使用。英国就是强制政府部门购买使用经过 ITSEC 或 CC 评价的产品。相反因为美国政府并不强制使用安全评价产品，使得最初开发的一些安全系统（如 KSOS、SCOMP、MULTICS 等）没能得到应用，最终变成了历史的见证人。产品如果在市场上都不能立足，那么就谈不上进一步的发展了。

2. 要制定或采纳统一的评价准则，并由专门的权威机构进行管理。否则会使产品开发者陷入迷茫，或者需要付出较高的代价（如需要接受多次评价认证）。

3. “他山之石，可以攻玉”，充分吸取国外或国际准则中的众多安全工作者的智慧。制定准则时应该考虑不同的安全政策、威胁和目的，区分功能需求和保证需求，尤其是要保证准则的可操作性和开放性。

4. 为了保证评价质量和方便厂商产品的评价，应建立统一的评价认证方案和多个评价实施机构。事实上，在 2000 年，世界上所有的 CC 评价认证机构总共评价了 12 个产品，而我国在同年评价的产品数为 219。

4. 展望

我们认为，以后信息安全评价的研究方向可能会集中在如下几点：

1. 针对各种安全产品和系统的面向不同可信等级的保护轮廓书的制定。对于大多数安全产品开发商来说，他们或许能够编写产品的安全对象书，但是很少有能力制定该类产品或系统的保护轮廓书。因此，针对某类安全产品或系统，制定面向特定可信等级的保护轮廓书，既可以促进信息安全技术的进一步发展，又可以对信息安全市场起一定的规范作用。

2. 目前信息安全保护的主要目的是保证保密性和完整性，以后对可用性、可靠性及可生存能力的保护的评价研究将会得到重视。一方面是因为安全需求正在逐渐从军方和政府扩大到商业和生活领域，另一方面，随着信息网络的迅速发展，出现了各色各样崭新的威胁和攻击。

3. 各种辅助评测技术和评估工具的研究和开发。对于一个安全产品或系统，既要按照开发商提供的各类文档（和代码）进行审查，又要测试其是否实现了宣称的安全功能。研制各种辅助评估工具，将对提高测试的质量和加快测试的周期起到非常重要的作用。

结论 随着计算机技术的广泛应用和国际互联网络的不断发展，信息安全问题也愈趋复杂和多样。信息安全产品和系统的评价也日益得到人们的重视。为了对我国安全评价领域提供指导和参考，本文首次考察了近二十年的信息技术安全评价准则的发展历史和评价情况，并对它们的贡献和不足之处进行了详尽的分析，对几个得到广泛使用的标准进行了相关性比较。然后对安全评价相关的几个重要问题进行了探讨，并结合我国信息安全评价的情况，指出了我们可以从中吸取的经验和教训。最后给出了安全评价技术未来可能的研究方向。随着信息技术的发展和人们开发和评价经验的不断积累，我们有理由对我国未来信息安全的评价持乐观态度。

参 考 文 献

1 Anderson J P. Computer Security Technology Planning Study Volume II, ESD-TR-73-51, Vol. II, Electronic Systems Division, Air Force Systems Command, Hanscom Field, Bedford, MA 01730, Oct. 1972

2 Bell D E, LaPadula L J. Secure Computer Systems: Mathematical Foundations. : [ESD-TR-73-278]. Vol. I, AD 770 768, Electronic Systems Division, Air Force Systems Command, Hanscom AFB, Bedford, Massachusetts, Nov. 1973

3 Department of Defense. Department of Defense Trusted Computer System Evaluation Criteria. DoD 5200. 28-STD, Washington, DC, Dec. 1985

4 Federal republic of Germany. Criteria for the evaluation of trustworthiness of information technology systems, ISBN 3-88784-200-6, Jan. 1989

5 Communication-electronics security group. UK systems security confidence levels. United Kingdom, Feb. 1989

6 Office for Official Publications of the European Communities. Information Technology Security Evaluation Criteria, Version 1.2. Jun. 1991

7 Pfleeger C P. Security in Computing, Second Edition. Prentice Hall PTR, 1997

8 National security agency. Combined Federal Criteria. 1992

9 Common Criteria Project Sponsoring Organizations. Common Criteria for Information Security Evaluation, Version 2.1. ISO/IEC 15408, Aug. 1999

10 中国. 计算机信息系统安全保护等级划分准则. GB17859-1999, 1999

11 http://www.cesg.gov.uk/assurance/iacs/itsec/cpl/index.asp

12 http://niap.nist.gov/cc-scheme/ValidatedProducts.html

13 http://www.radium.ncsc.mil/tpep/epl/historical.html

14 http://www.infosec.org.cn/gonggao/

15 http://www.mctc.gov.cn/cpjs.htm

（上接第 100 页）

参 考 文 献

1 Bahreman A, Tygar J D. Certified Electronic Mail. In: Proc. of the Internet Society Symposium On Network and Distributed System Security, Internet Society, 1994. 3～19

2 Micali S. Simultaneous electronic transactions with visible trusted parties. U.S. Patent 5,629,982,13 13 May 1997

3 Asokan N, Schunter M M. Optimistic protocol for fair exchange. ACM Computer and communications security, 1997. 7

4 崔国华，等. 安全的电子保证邮件. 计算机工程

5 Bruce Schneier 著，吴世忠等译. 应用密码学. 机械工业出版社