

关于建立信息系统安全性评估准则的几点考虑

中国信息安全产品测评认证中心

张利 江常青 王贵骊

“十五”期间，我国将大力推进信息化建设，江总书记指出要用信息化带动工业化的发展。电子政务、电子商务以及国家关键基础设施信息化建设的步伐非常快。但是，信息化建设需要以信息安全为前提。因此，在信息化建设中如何构造健全的信息安全保障体系显得尤为重要。在构造信息安全保障体系时，对信息安全问题需要做到心中有数；并且我们整个信息安全产业界需要统一思想，对信息安全问题有着大致相同的认识。这样，建立信息系统安全性通用评估准则这样的国家标准就显得非常重要，对构造我国的信息安全保障体系具有非常重要的战略地位。

1 国外研究进展

ISO 15408（俗称 CC）自从 1999 年 5 月公布以来，得到了广大国家的认可，被广泛用于 IT 安全性评估。目前世界上有 15 国参与 CC 互认，日本、韩国和俄罗斯三国也表达了加入的意愿。因此，采用 CC 进行 IT 安全性评估是大势所趋。我国在 2001 年将 CC 等同采用为国家标准 GB/T 18336，在短短的两年时间内，中国信息安全产品测评认证中心采用该标准对 158 个产品进行了认证。同时，为了推广 CC，不断地充实并修正 CC，迄今为止共召开了三届信息安全测评认证标准与互认国际会议（简称 CC 大会）。

尽管 CC 在很多国家得到了广泛的应用，但是，人们发现 CC 能有效的应用于信息安全产品的评估认证，在信息系统的安全性评估方面具有局限性。然而，随着全球信息技术的发展，人们越来越发现信息系统的安全性认证非常重要，无论从国家安全的角度，还是市场需求的角度，非常有必要建立一个适用于信息系统安全性评估认证的通用准则。

国际社会对于建立信息系统安全性评估通用准则非常重视，很多国家的专门部门和机构均致力于这方面的研究。1995 年英国标准局 BSI 发布了用于信息系统评估的国家标准 **BS7799**，该标准共两个部分，第一部分于 2000 年 12 月被国际标准化组织采纳为国际标准 ISO17799。由于 BS7799 对于信息系统的安全性评

估主要集中在安全管理方面，对于技术层面则涉及过少，存在一定的局限性，因此，该标准遭到了美国、加拿大等国家的抵制。

美国技术标准局 NIST 长期研究信息系统安全性认证的标准流程研究，并计划于 2002 年 10 月底公布 NIST SP800-37“IT 系统安全性认证与认可联邦政府指南”，将对信息系统安全性认证的流程和方法作出明确的规定。美国国防部早在 1997 年 10 月就公布了国防部 IT 安全认证与认可过程，于 2000 年 7 月发布了该过程的应用手册。2002 年初，美国国防部公布了信息系统安全性评估的指令 8500，该指令将对信息系统的安全性评估分为了 16 个方面。

在今年 5 月加拿大举行的第三届 CC 大会上，如何在 CC 的基础上进行信息系统的安全性评估成为一个讨论的热点。美国、法国、日本和俄罗斯等国的代表均介绍了进行信息系统安全性评估方面的一些经验。分析了信息安全产品的测评与信息系统的测评之间的不同，普遍认为，CC 的思想同样可以应用于信息系统的评估，但是需要将 CC 的内容进行扩充，以使之适用于信息系统的安全性评估。从这些国家的学者在会上交流的内容，这些国家对于信息系统安全性评估通用准则的研究已经进行，而且通过实践积累了一定的经验。可以说，在不久的将来，世界认可的用于信息系统安全性评估的通用准则肯定会出现。

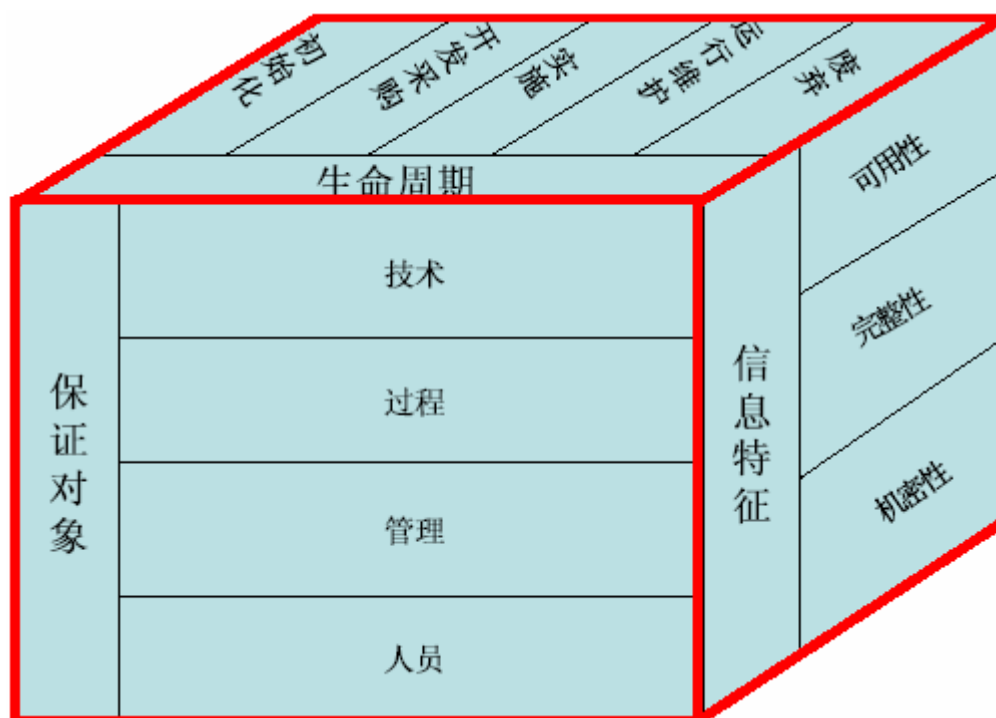
我国应当顺应国际上信息安全评估方法研究发展的潮流，及早进行信息系统安全性评估方法及准则的研究，建立既符合我国信息化发展特征，又能与当今信息安全评估方法和技术发展趋势相吻合的可操作性强的信息系统安全性通用评估准则。

2 考虑要素

本节主要说明在建立信息系统通用评估准则（SCC）时应当考虑的要素。信息系统通用评估准则（SCC）应当建立在信息技术通用评估准则（CC, ISO 15408）的基础上，这是国际上很多专家认可的一个看法。应当说，CC 对于信息技术的功能组件和保障组件概括得比较全面，在信息系统通用评估准则（SCC）中可以将这部分内容略去，这部分安全需求的满足通过在信息系统中对于安全产品的要求来达到。

但是，信息系统比单纯的信息产品要复杂得多，信息系统的构成除其固有的

IT 部分外，还包括很多的 Non-IT 部分。因为，所有信息系统存在于某种非常特定的环境中，其运行脱离不了人的因素，人与环境以及信息技术的交互使得信息系统的安全性需要考虑的要素非常多。信息系统的安全性需要考虑其全生命周期过程，是一个完善的风险管理过程。在这个风险管理过程中，涉及信息系统的技术架构、安全工程实施过程、管理体系等方面的内容；信息系统的安全目标主要是使处理的信息达到一定程度的可用性、完整性和机密性，当然现在很多学者又提出了抗抵赖性和可靠性。综合起来，我们可以给出如下的信息系统的安全保障模型。



信息系统安全保障模型

3 信息系统安全性评估准则（SCC）的内容

CC(ISO15408)的贡献不仅仅是为信息技术的安全评估提供了一个世界公认的通用的标准，同时，它为描述信息安全提供了一种通用的语言和格式。CC 中关于保护轮廓（PP）和安全目标（ST）的概念在信息系统中同样适用。而且，对于信息系统的安全建设可以起到非常重要的作用。

信息系统安全性评估准则应当在 CC 的基础上建立，它在内容上是对 CC 的

继承和扩展。应当充分考虑信息系统相对于单纯的信息技术的新特征，在内容上应当涵盖信息系统全生命周期的安全状态，对于信息技术部分的安全要求在信息系统安全性评估准则中将通过对于信息安全产品的要求来满足。但是，需要扩充信息系统技术体系架构、工程实施过程和管理等方面的要求。

中国信息安全测评认证中心在总结多年信息安全测评认证工作经验的基础上，借鉴国内外相关的研究成果，已经完成了信息系统安全性评估准则（Draft版）的开发。在经过专家评审讨论后，该评估准则在不久的将来就会与大家见面。