国际 CC 认证体系和 CCRA 简介

刘岩，atsec 中国，2015 年 4 月

关键词：产品安全评估、通用评估准则、Common Criteria

标准历史和发展

通用评估准则（Common Criteria，以下简称 CC）标准源于世界多个国家的信息安全的准则规范，包括欧洲 ITSEC、美国 TCSEC（桔皮书）、加拿大 CTCPEC 以及美国的联邦准则（Federal Criteria）等。这些准则规范在 CC 发展历程上均得到了各国大力支持，因为早在 CC 制定之初便达成了共识：采用一套公共的准则规范为 IT 保障类产品的广泛用户群体提供最大的便利。CC 标准很有意义的贡献之一便是将安全功能需求（Security functional requirements）和安全保障需求（Security assurance requirements）通过标准独立的两个部分分开（Part2 和 Part3）。评估将在特定的安全功能要求上选择适合产品自身条件和产品用户要求的安全保障需求，或者选择预定义的安全保障级别（EAL）。

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了其他国家共同签署了 CC 互认协定（CCRA）[1]，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，目前互认的安全保障级别（EAL）最高为 4 级。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。

除此之外，许多尚未加入到互认协定的国家和机构，也将 CC 作为关键的标准进行使用，并对 CC 的发展起到了重要的作用。经过国际范围的不断审核，国际标准组织（ISO）正式采纳 CC 标准为 ISO/IEC 15408（Parts 1-3），CEM 为 ISO/IEC 18045。CC 标准不仅仅用于 CCRA 成员国家 [1]，还广泛应用于其它国家和地区，例如欧盟范围所采用的另一个认可体系 SOGIS。中国引入了 ISO/IEC 15408 标准作为 GB/T 18336 国家标准，但中国目前并没有加入到 CCRA。

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（也即 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。。

标准概述

CC 是专注于信息安全领域且具有奠基意义的一部标准。在标准所定义的同一个框架内，使用的是同一种专业语言，使得计算机信息产品的使用者能够用严格规范的方式来明确提出产品的安全功能的要求。同时，产品的研发商能进而实现这些所要求的安全功能或是声明他们的产品具有怎样的安全特性，实验室的测试评估人员也能评测产品是否真正地达到了研发商所宣称的安全功能。由此可以看出，CC 是为计算机信息产品的安全功能说明、实现以及评估提供安全保证的一部通用标准。

CC 在标准结构和撰写形式上一共包含三个部分，就像是一本书的三个大章。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。为了更清晰地说明三部分间的关系，每一部分说明如下：

CC 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）这些重要的基本概念，并且规定了撰写 ST 和 PP 这类文档的格式及要点。评估目标简单说来就是要对此进行评估的对象产品。安全目标是对某个特定的评估目标提出的要其满足的安全功能要求（Security Functional Requirements，简称 SFR）和安全保障要求（Security Assurance Requirements，简称 SAR）。保护轮廓是对某一类产品提出的安全功能和安全保障要求。

CC 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，其中有安全审计、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。每一大类内，又逐步细分到不同的族、组件及组成要素。CC 第二部分提供的安全功能组件集合了当前信息安全产业界最普遍使用的技术方法，是非常有价值的可供参考的安全功能描述。然而，CC 第二部分既不强迫任何产品必须选用一些特定的安全功能组件，也不能保证所有信息安全产品所需的安全功能都已存在相应描述。CC 是有弹性可扩展的框架性体系，它允许 ST 或 PP 的作者按照 CC 第二部分提供的对已定义的安全功能组件的格式来定义描述新的安全功能组件。

CC 第三部分详细描述了可供 ST 或 PP 选用的安全保障要求。安全保障要求覆盖到对 ST 的评估准则、TOE 的开发、生命周期支持、指导性文件、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，CC 第三部分中又定义了七个评估保障级（Evaluation Assurance Level，简称 EAL），每个评估保障级都是将六个方面的安全保障要求的细节按一定方式搭配并固定下来。从 EAL1 到 EAL7，在六个方面的安全保障要求由少到多、由松到紧逐渐递增。

CC 评估具有两个重要环节。第一步是对确定的安全目标的评估。安全目标可以遵从于某个保护轮廓（Protection Profile，简称 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的。提出安全目标和保护轮廓的基本准则是根据某个或某类产品需要保护的信息资源的价值，以及此（类）产品使用环境受到敌意攻击的威胁程度，来选取合适的安全功能组件和安全保障级别。如果此（类）产品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的，那么从理论（即 CC 的理想）上讲此（类）产品有能力抵御来自所处的使用环境的威胁，因而能够有效保护所拥有的信息资产。安全目标的制定应符合 CC 标准的第一部分一般威胁模型的方法。

CC 评估的第二步是对安全目标中所定义的 TOE 的评估。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。这里要强调指出的是，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。

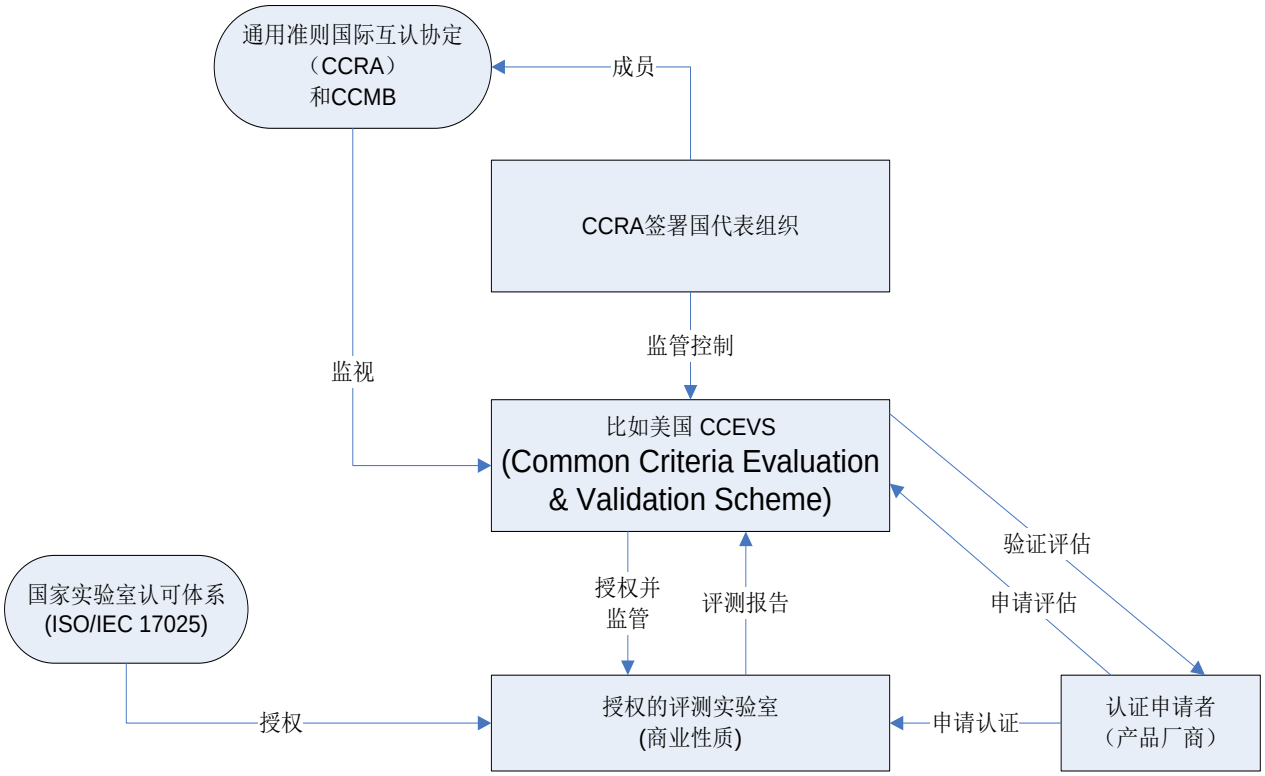
对于 EAL1 到 EAL4 的 CC 评估，CCRA 还发布了通用标准评估方法论（Common Criteria Evaluation Methodology，简称 CEM），并被接纳为国际标准 ISO/IEC 18405。据作者所知，中国信息安全领域的专家们对 CEM 已作了中文翻译，目前尚未看到该部分发布为一个国家标准。

概括来讲，CC 评估是基于 CC 第一部分提出安全威胁模型，该模型根据产品面临的安全问题（假定、威胁和组织安全策略），确定安全目标，并根据 CC 第二部分的安全功能要求选择产品的安全功能，基于 CC 第三部分的安全保障要求开展 CC 评估。

认证体系

截至 2015 年 4 月份，CCRA 成员国总计 26 个国家，其中已有 17 个国家的相关政府机构拥有自己的评估认证体系可进行认证证书的颁发并接受互认（Certificate authorizing），它们是澳大利亚、加拿大、法国、德国、印度、意大利、日本、马来西亚、荷兰、新西兰、挪威、韩国、西班牙、瑞典、土耳其、英国和美国；而另外的 9 个国家可以接受和认可来自上述国家颁发的认证结果（Certificate consuming），它们是奥地利、捷克、丹麦、芬兰、希腊、匈牙利、以色列、巴基斯坦、新加坡。

如下图所示，CCRA 各个成员国家所采用 CC 评估和认证体系均设有认证机构和授权的评估实验室，他们与评估发起者（申请者）合作完成产品的评估和认证。



图：国际 CCRA 评估和认证体系

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。

而 CCRA 体系，管理职责一方面由 CCRA 承担，通过周期性审核评定确保各个国家测评认证体系的质量，该任务基于 CCRA 附录 D、附录 G.3、以及附录 H 的要求说明开展工作。另一方面由国家层面的管理职能机构负责，比如美国体系下，其 CC 评估与认证体系（CCEVS）是美国国家信息安全保障合作组织（NIAP）的一部分，而 NIAP 则隶属于美国国防部（DoD）下属的国家安全部（NSA）的信息保障部门。在德国，CC

评测认证体系由德国 BSI（The Bundesamt fur Sicherheit in der Informationstechnik）负责开展，总部位于波恩（Bonn）的德国 BSI 机构成立于 1991 年，该机构作为德国联邦政府的 IT 安全权威部门，协同德国内部和国际合作伙伴负责全面的信息安全工作，如密码、网络安全以及各类相关认证。

各个国家评测实验室的授权和认可工作都十分的谨慎和严格，如 CCRA 等相关文件规定，需要遵从一系列的审核以及符合性要求，例如 ISO/IEC 17025 针对测评实验室的授权要求。CCRA 体系之下，美国的 CC 评测实验室授权工作是由美国国家标准和技术学会（NIST）下属的国家实验室自愿认可组织（NVLAP）联合 NIAP 共同展开的。截至 2015 年 4 月，美国体系下授权评测实验室共计 9 家，包括 atsec information security corporation 等。德国 BSI 体系下的评测实验室共有 9 家，包括 atsec information security GmbH 等。下图展示了 CCRA 文件中提及的实验室需要符合 ISO/IEC 17025 实验室的管理和技术要求：

a) the *Evaluation Facility*

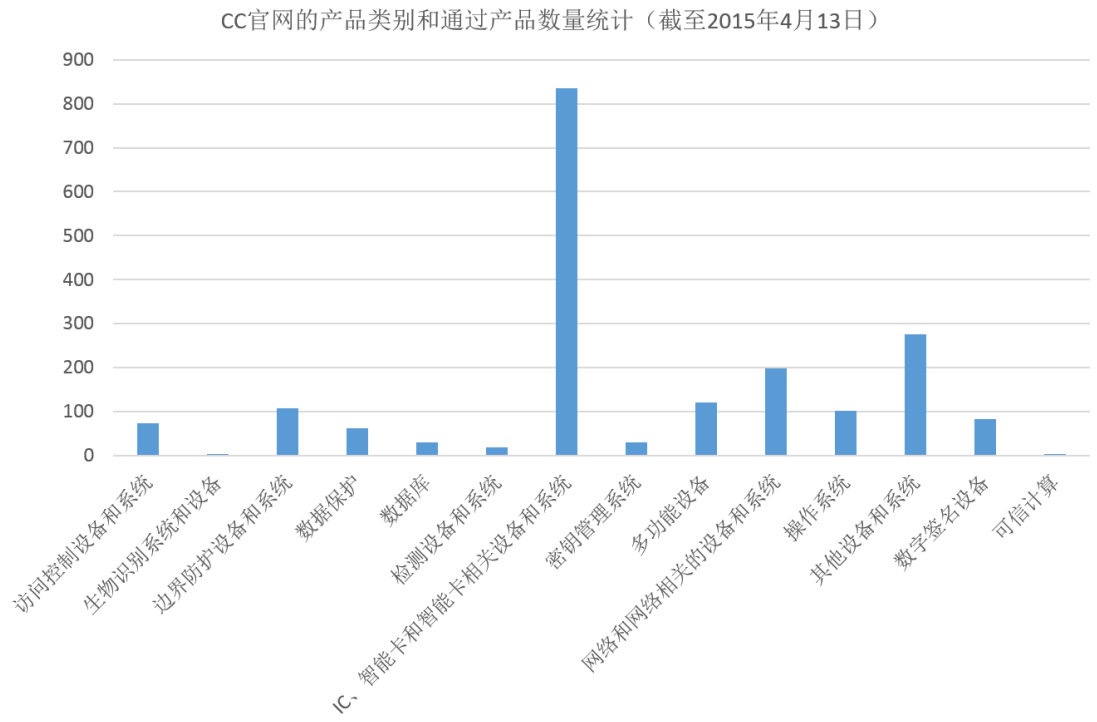
- either has been *Accredited* in its respective country by a Recognised *Accreditation Body* in accordance with ISO/IEC 17025, its successors, or in accordance with an interpretation thereof approved by all Participants, and has been *Licensed* or *Approved* in accordance with Annex B.3,

在美国和德国等国际 CC 评估体系下，认证机构（CB）并不直接为评估申请者进行产品评测，而评测工作由上述授权的商业评测机构来完成，例如美国 CCEVS 和德国 BSI，作为 CB 只负责产品的认证，对评估机构提供结果的审核，以及对评估机构的定期监督审计和监管。而对于评估申请者（一般是产品厂商），需要与评测实验室直接联络来完成评测认证工作。

认证活动

CC 标准的面向对象是信息技术产品的安全性。面对各个类型的产品。只要该产品具有安全功能，则可以采用这个标准致力于安全测评和评估工作。

基于 CCRA 体系由 CCRA 官方网站数据显示的产品认证情况如下图所示[2]。



图：国际 CCRA 体系产品认证分类图

下表显示了国际体系的一些认证结果数据。CCRA 的数据来源于 CC 官方网站所显示的列表，其中显示仅限截至 2015 年 4 月 13 日官方所公布的产品信息，也不包括 EAL5 或者更高级别的产品；另外有些认证申请者由于机密性考虑，要求不公开其证书和产品信息，故而此统计数据也不包括这些产品。

	评测实验室个数	完成认证产品总数
澳大利亚	2	60
加拿大	4	233
法国	5	490
德国	9	565
意大利	4	12
日本	5	169
马来西亚	2	19
荷兰	1	34
挪威	4	44
韩国	7	76
西班牙	3	61
瑞典	2	12

土耳其	3	19
英国	3	29
美国	9	113
CCRA 合计	63	1939

国际 CC 会议和 CCUF

每年度的国际 CC 会议（ICCC：International Common Criteria Conference）吸引了来自认证机构、评估实验室、厂商、最终用户、以及研究机构的诸多专家前来参加。自 2000 年第一届 CC 会议在美国召开的 15 年来，CC 会议分别在英国、加拿大、瑞典、德国、日本、西班牙、意大利、韩国、挪威、土耳其、马来西亚、法国、美国、印度，2015 年的 ICCC 将在英国举办。

此外，atsec 和产业长期以来一直在呼吁 CC 标准的发展应该吸取更多来自最终客户的声音，故而 2012 年 CC 用户论坛（CCUF：Common Criteria User Forum）正式启用，并定期召集产业展开技术研讨，旨在提供产业各方更好的交流平台。参见：http://www.ccusersforum.org/

结束语

本文简要地描述了 CC 标准的国际使用情况和现状。无论是 CC 认证机构、评估机构，还是产品开发者、产品最终用户，整个产业均理解和认可高质量的 CC 评估的真正价值和意义，他们对于标准的发展也起到了至关重要的作用，比如目前国内外很多切实从产品用户需求角度提出的经典的保护轮廓（PP）被广为采纳和使用。

来自中国的 CC 领域专家已经和国际 CC 组织开展了很多技术层面的交流，相信通过各国的共同努力，产品认证体系和测评标准会进一步的完善和提高。atsec 作为专注在信息安全领域中立的测评机构，也很高兴能够成为世界和中国信息安全产业的桥梁，为信息安全保障做出我们的贡献。

更多的相关 CC 的资源和信息，可以参见 atsec 官方网站：

http://www.atsec.cn/cn/common-criteria-laboratory.html

参考文献：

[1] Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security, July 2014

[2] CC 官方网站 http://www.commoncriteriaportal.org

[3] atsec CC 官方网站 http://www.atsec.cn/cn/common-criteria-laboratory.html