

计算机安全性标准： 安全性评价和安全性评估

Oracle 白皮书
2001 年7月



This product is rated B1 by NSA in accordance with the Trusted Computer System Evaluation Criteria when installed as prescribed.



This product is rated C2 by NSA in accordance with the Trusted Computer System Evaluation Criteria when installed as prescribed.

此页特设为空白页。

计算机安全性标准和安全性评价

引言

Internet的出现正在改变全世界的商业运作方式。在这个Internet时代，对信息技术（IT）日益依赖的直接影响是对产品和系统实施全面完善的安全机制已成为必要。基本的安全问题，如身份验证、加密、数据保护、用户权限、审计和网络安全等，在目前这样一个动态的计算环境中仍然是重中之重，而在IT安全诈骗中的创新也同样重要。

采购者需要购买能满足其商业需求的产品和系统，供应商需要设计和开发安全产品和系统，同时要紧记IT环境和威胁的迅速变化特性。

- 然而购买者如何从有意识的安全角度来购买产品呢？
- 根据产品安全机制的强度来测量产品的标准或尺度是什么呢？
- 供应商对其产品强大的安全性的声明的证据是什么且在何处可见得呢？

安全性评价和安全性评估在建立产品的安全可信度中扮演着关键的角色。安全性评价提供了一种可验证产品或系统的正式尺度，已被独立的权威的且公认的机构发展并承认为国际通用的安全性标准。安全性评估是一个不太正规的安全性评价活动，但同样重要，

因为它提供了一种供应商独立评估其产品的安全可信度的机制，虽然不是根据正式的评价尺度或标准。

安全性评价为信息技术（IT）产品的安全性提供了保证。

安全性评价

由独立机构进行的安全性评价为商业、政府和军事机构在信息技术（IT）产品和系统的安全性方面提供了保证。由于Internet和电子商务的不断发展，对IT日益依赖的直接影响是利用独立的安全性评价为IT产品和系统中的安全机制强度提供一个精确的评估已成为必须。基于这种评价和标准建立起一种可被IT采购者和供应商接受的信任度。此外，安全性评价标准和等级可用于精确地描述IT的安全性需求。

Oracle公司，作为安全数据库技术方面的领先供应商，它的Oracle7、Trusted Oracle7和Oracle8数据库服务器产品已经根据美国、欧洲、国际和俄罗斯评价标准成功地完成了几个独立的正式安全性评价。Oracle目前正在为其Oracle8和Oracle8i数据库服务器产品进行安全性评价。

Oracle已经在签约和支持安全性评价方面进行了实际性投资，来确保Oracle数据库服务器产品的用户能够获得他们在产品安全性设计、实施和功能性等方面所要求的信任度。另外，系统集成商会更好地将现有的这些商业产品合并入要求这种信任度的集成的安全系统中。

IT安全性评价有两个重要的组件：进行评价的标准，控制如何和由谁来正式进行此评价的方案或方法。

安全性评价标准

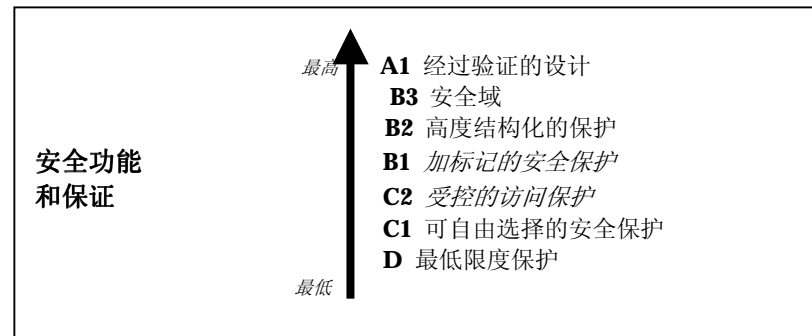
安全性评价需要客观的、定义完备的评价标准和方法。这类标准和方法有几种国际认可的版本，下面部分按其产生时间升序排列（即从最老的标准到最近的标准）描述了这些标准。

US TCSEC

US Trusted Computer System Evaluation Criteria TCSEC 或 Orange Book（橙皮书）用于对操作系统的安全性评价。

最初发表于1983年，US *Trusted Computer System Evaluation Criteria*（TCSEC，美国可信任的计算机系统评价标准，也被称为**橙皮书**）被用于操作系统的安全性评价。1991年4月，美国国家计算机安全中心(US National Computer Security Center, NCSC)出版了 *Trusted Database Interpretation (TDI)*，对数据库管理系统和其它分类产品的评价标准提出了一种解释。

TCSEC和TDI主要列举了满足美国政府安全需求的安全性评价标准，它关注某保护机密信息的需求。这一标准对政府和那些拥有不保密、但却敏感的数据的商业机构而言是有益的。



美国橙皮书等级

产品根据TCSEC和TDI从预定义等级D（最低限度保护）向上直到A1（最高层次保护）来进行评价。这些等级代表固定的功能（产品的安全机制）。

C2 – 受控的访问保护

C2级产品提供细致的可自由选择的访问控制(DAC)。

C2级产品提供细致的可自由选择的访问控制(DAC)，并可通过识别过程、审核安全性相关事件和资源隔离使用户单独为他们的行为负责。

可自由选择的访问控制限制了对基于主体（如用户）识别的对象（如文件和表）的访问。利用“需要知道（need-to-know）”的策略，对象所有者或安全管理员可以定义哪些用户或用户群能够访问指定的对象。

为了达到C2等级，除通过有关产品测试、产品文档及其开发的调查外，产品必须满足这些功能性要求。

B1 – 加标记的安全保护

B1级产品提供了C2级产品的所有功能，还实现了强制性访问控制(MAC)。

B1级产品必须包含C2级产品要求的所有特性，并且还必须能够执行基于标记的强制性访问控制(MAC)。MAC对基于数据阅读权限（分类）和用户请求的正式授权（许可）的数据访问进行限定。如果用户没有数据分类等级的许可，访问将被否决，而不考虑任何试图批准用户访问的自由选择访问规则。因此，产品必须自动强制执行基于阅读权限标记的访问规则，并把这些标记和在其域中的每个用户和对象联系起来。在数据库服务器中这就意味着诸如表、单行和每个用户的数据库会话这样的对象被标记。由于用户和数据可以以不同的标记或等级同时出现在一个共享系统中，因此这类产品安全性也被称为“多级安全（MLS）”。

Information Technology Security Evaluation Criteria (ITSEC) 是欧洲权威的安全性评价标准。

为了达到B1级，除通过有关产品测试、产品文档及其开发的更加严格的调查外，产品必须满足这些功能性要求。例如，产品的安全性策略必须经过正式或非正式的模拟。

欧洲ITSEC

*Information Technology Security Evaluation Criteria (信息技术安全性评价标准, ITSEC)*是欧洲四国：法国、德国、荷兰和英国的安全性评价标准协调统一的结果。ITSEC取代了这几个国家自己的国家标准，事实上成为了欧洲标准。自1991年7月起，ITSEC已经在欧洲评价和认证计划中使用。

与TCSEC和TDI相反，为更明确的地表述军事和商业需要，ITSEC发表了对机密性、完整性和可获得性的扩充观点。ITSEC将机密性定义为对信息的未经授权获取的预防；将完整性定义为对信息的未经授权修改的预防；将可获得性定义为对资源的未经授权扣留的预防。在ITSEC的开发期间，Oracle参加了所有的评审会议，并对所有关于草案注解的恳请做出了积极响应，帮助确定用ITSEC对分层的应用软件（如数据库管理系统服务器）进行评价的必要条件。

功能性

Security Target（安全性目标）——ITSEC评价的指导技术文档，通过参考ITSEC预定义的功能类或通过指定单个功能需要，或同时通过这两项，来定义产品或系统的安全性功能。

ITSEC的附件A包含几个预定义功能类的例子，包括映射到US TCSEC类中的类，如F-C2和F-B1，分别等同于C2和B1。对于一些关系数据库服务器一般用途的方面，如数据完整性和可获得性，没有

预定义的功能类。

保证

ITSEC将“保证”定义为产品或系统如何依据其所声明的安全机制无误地完成一个任务的一个重要量度。保证通过实施的正确性及产品或系统的安全性功能和机制的有效性来测量。

ITSEC定义了从E0到E6的七个评价等级，代表产品或系统正确性的可信任程度。等级E1表示一个基本点，在此以下的等级不具有信任度，而等级E6代表最高级别的信任度，要求非常严格、正式的开发、验证和经销方法，远远超过了商业上可利用的产品或系统的范围。

因此，在ITSEC的管理下，给产品或系统一个评价或保证等级（如，E3），就代表用户能拥有产品或系统在其安全目标中所声明的功能性提供的信任等级。

迈向更加统一的北美标准，其中一些要素已经被并入新近开发、并得到国际标准化组织(ISO)批准的*通用标准 (Common Criteria)*。

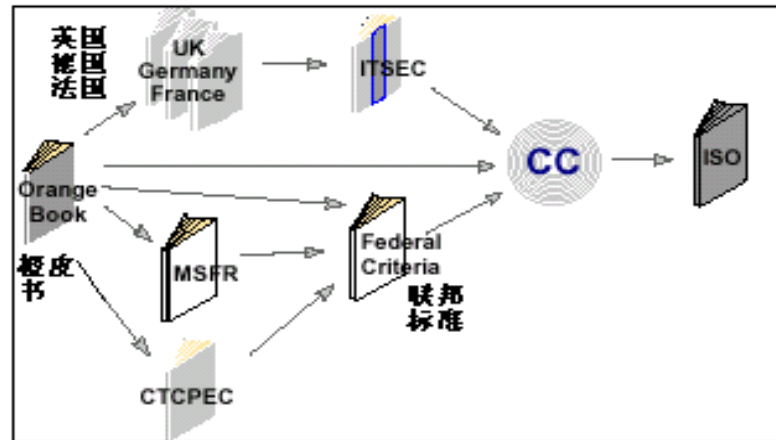
International Common Criteria（国际通用标准）

通用标准是北美与几个欧洲国家为开发一套国际承认的安全性评价标准共同努力的结果。

International Common Criteria for Information Technology Security Evaluation（*信息技术安全性评价国际通用标准*，也称*通用标准*，CC）是北美与欧洲联盟为开发一套的国际承认的安全性标准共同努力的结果。最近被规定作为一种ISO标准(编号：15408)，CC取代了美国的TCSEC、欧洲的ITSEC和加拿大的CTCPEC。事实上它已成为国际上通用的安全性评价标准。

与国际标准接轨

在过去十年中，安全性评价标准在评价目标规范、与政府和商业的相关性方面朝着更加灵活的方向发展，并将关注点集中到集成了大量不同产品的系统的评价问题上来。这种有益的趋势可协助确保实用性产品和确实独立的产品为最广大的用户所获得。



安全性标准的评价

准备按不同的标准和不同的评价方案对统一产品进行评价。CC减少了这种繁烦的要求，因此以被参与国互相认可为主要目标的，CC成为全世界的标准。

CC 是安全性评价的全球性标准。

为此，一份关于IT安全领域通用标准认证的相互认可协议于1998年10月正式签署。此协议的目的是使签署国接受相互间的CC认证，而不需在每个国家对产品进行再评价，从而防止了评价过程的

重复。协议通过声明与该协议签署国相关联的认证（或确认）主体满足安全性评价高度一致的标准，陈述了每个国家初次认证所基于的判断的可靠性上的可信度基础。它详细说明了每个参与者接受安全性评价结果和由其他参与者所指导的相关认证所要求的条件，并为其他相关合作活动做准备。

与ITSEC相同，为更明确地满足军事和商业需求，CC发表了对机密性、完整性和可获得性的扩充观点。曾经主要为政府和军事部门所关注的信息安全，随着Internet的出现，也逐渐成为计划进行电子商务的各类商业机构的关注焦点。商业企业也能够从政府对商用软件产品和系统的正规评价需求的同类保证中获益。

与 ITSEC 相同，CC 将功能性与保证独立分开。

与ITSEC相同，CC将功能性与保证相分离。根据指定的安全目标（Security Target, ST）、指定安全功能性CC主要技术指导文档或保护文档（Protection Profile, PP，一种以所要求的保证等级为目标的高级文档），对产品或系统进行评价。

功能性

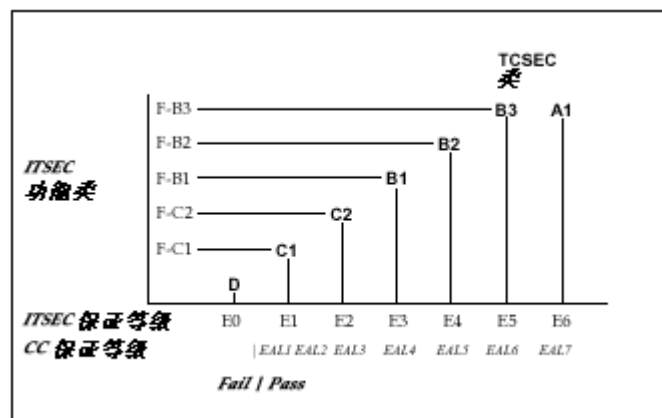
主办者（或供应商）在从所要求的保证等级中分离出的安全目标或保护文档中首先定义产品的安全功能性。从EAL1到EAL7的评价等级代表产品或系统在正确性方面的可信任程度。

等级EAL1只要求最低程度的功能测试，等级EAL4要求具有安全目标的详细说明、详细设计的非正式描述、功能测试、源代码分析、安全机制的测试、配置控制系统和经核准的产品经销过程。等级EAL7代表可信任程序的最高等级，要求非常严格的正式开发、验证和经销方法，远远超过了用于商业的产品或系统的范围。

在方法上类似于ITSEC，通过各种分析来评估产品或系统的功

效，如调查产品或系统中的机制与其安全目标是否匹配。在所有关键的安全强制机制的强度分析基础上，产品或系统也被指定了最小的机制等级强度。

因此，在CC评价中，产品或系统的评价或保证等级(如，EAL4)就代表了用户对产品或系统在其安全目标或保护文档中声明所提供的功能性所具有的信任程度。



TCSEC、ITSEC和CC的保证等级的对比

评价方案

不同的认证主体通过评价标准执行IT安全性评价的过程有所不同。这些处理过程的不同影响着评价者、主办者和开发者的职责，评价的成本和持续时间，以及要求用来进行和支持评价的资源。

美国的TCSEC评价方案

在美国由国家计算机安全中心(NCSC)进行安全性评价。

在美国由美国国家计算机安全中心(NCSC)进行安全性评价，NCSC是国家安全局(National Security Agency, NSA)的组成部分。评价在“可信的产品评价程序(Trusted Product Evaluation Program, TPEP)”的支持下完成，成功地完成此程序的产品被指定一个TCSEC等级，并列在美国经过评价的产品列表(Evaluated Products List, EPL)中。

现在NSA已经正式取消了TPEP，产品不必再进行任何TCSEC评价。

欧洲的ITSEC评价方案

在政府机构监督下，商业评价机构(Commercial Evaluation Facilities, CLEFs)根据ITSEC进行评价。

在英国，Commercial Evaluation Facilities(CLEFs)执行英国IT安全性评价和认证方案范围内评价。作为认证方(Certification Body, CB)的政府机构对方案进行监督，此认证方由Communications-Electronics Security Group(电子通信安全小组, CESG)操作。

ITSEC方案也清楚地定义了评价产品的过程，并发表在IT Security Evaluation Methodology(ITSEM, IT安全性评价方法论)上。

在评价成功完成时，认证方发布一份认证报告和证书。

在ITSEC评价成功完成时，CB发布一份认证报告和一份基于CLEF的决定及其分析的证书。然后产品或系统会收到一个评价和保证等级，并列入UKSP06中，UKSP06是一个类似于美国EPL的列表。

ITSEC努力做到协调统一，这对供应商和购买者都非常重要，其最终目标是实现这些认证的国际共识。例如，确保在德国成功完成的评价在英国也将得到承认。1996年4月，美国国家标准与技术学会

(US National Institute of Standards and Technology, NIST)发表了一份公告，允许美国采购机构在无法获得所需的以美国EPL评价的产品时，可以购买美国的被评价系统中ITSEC F-C2/E2 (或更好)或CTCPEC C2/T1等级的系统。

另外，1997年11月，Information Security Certification Body (信息安全认证机构)的高级官员最初来自法国的SCSSI、德国的BSI和英国的CESG。

国际CC评价方案

CC 评价方案的目标是实现认证在全世界的相互认可。

CC的方案类似于欧洲的ITSEC，它由英国的CESG、美国的NSA和加入CC的各国自己的控制方进行监督。

经过成功的CC评价的产品被指定一个评价保证等级，并列入Certified Products List (认证产品列表)。

发展CC的最初原则之一就是实现认证在全世界的互相认可。为此，国际标准组织(ISO)采纳了CC的2.1版本作为一个ISO标准，其编号为15408。

其它的评价和认证方案

Oracle 也参与了其它的验证和评价方案。

除了前面部分提到的评价方案外，Oracle还参与了其他评价标准的制定及其各自的方案。

US Federal Information Processing Standard (美国联邦信息处理标准)

Federal Information Processing Standard (*FIPS*) *PUB 140-1*,

Security Requirements for Cryptographic Modules（加密模块的安全要求），是由美国国家标准与技术学会(NIST)和加拿大政府通讯安全机构(Canadian Government's Communication Security Establishment, CSE)建立的。FIPS 140-1标准由这两个机构联合支持维护。

由美国和加拿大政府机构购买的加密产品要求经过FIPS 140-1确认。因而，这些产品需要根据FIPS 140-1的从等级1（最低）到等级4（最高）的安全等级范围来得到确认。等级2要求正式文档和严格的测试，是软件供应商安全等级的最高级别目标。等级4通常只有硬件供应商能实现，例如需要经过等级4所要求的更加严格的文档、检验和测试的硬件加密设备。

根据FIPS 140-1标准对产品进行测试和确认是由经NIST和CSE核准和认可的认证实验室进行的。

俄罗斯联盟认证标准和方案

俄罗斯联盟认证标准和方案由五个包含认证规则、等级和标准的指导文档集组成。

Oracle安全性评价状态

在美国和欧洲，Oracle在开放系统平台上已经完成了Oracle、Trusted Oracle和Oracle Advanced Security的多种安全性评价。Oracle选择开放系统平台是因为在政府、国防和工业部门中对开放安全系统的需求越来越多。

由于CC作为一个ISO标准得到国际认可和接受，Oracle不再寻求其他TCSEC或ITSEC评价。因此，Oracle已经完全将CC做为它的实际评价标准，并决定只根据此标准对其未来的所有数据库服务器产

Oracle 已经完全将 CC 做为它的实际评价标准，因此不会再参与 TCSEC 或 ITSEC。

品进行评价。

Oracle是第一家根据CC标准成功地生产和评价了保护文档（Protection Profile, PP）的数据库供应商。而且，Oracle还是正式实现了对其Oracle7数据库服务器的CC EAL4评价的第一家供应商。从那时起，Oracle 就根据CC的EAL4标准对其Oracle8和Oracle8i数据库服务器产品进行了正式评价，并在高保证级别上开发和评价了多个业界认可的PP。

Oracle也是第一家并且是唯一一家成功地完成了俄罗斯联盟安全性评价标准认证的数据库供应商。然而，Oracle将不再采用俄罗斯标准对其数据库服务器产品进行评价。

此外，Oracle的加密产品——Oracle Advanced Security，在首次评价中成功通过了FIPS 140-1的第2等级验证。Oracle Advanced Security的FIPS 140-1测试及其验证是由InfoGard Laboratories公司进行的，InfoGard Laboratories是一个经NIST和CSE授权和认可的美国认证实验室。

附录A中提供的表总结了Oracle已完成的和正在议事日程上的安全性评价。

系统评价和鉴定合格发布

Oracle的服务器产品（Oracle7、Oracle8和Oracle8i、MLS服务器产品、Trusted Oracle7和其加密产品——Oracle Advanced Security）的评价为程序认证和鉴定（美国）或为作为重要的强制安全组件并入Oracle数据库服务器中的系统的评价和认证（欧洲）提供了重要的依据。例如，在欧洲评价案例中，Oracle和其服务器组件依赖于满足系统安全策略的要求。在决定是否需要进行再评价和需要多少次再评价、再测试或其它评价工作来满足系统安全要求，或自不执行额

外评价工作的风险是否能被满意地控制等方面都需考虑这些因素。

例如，因为所有的安全性评价标准均检验了Oracle的IT环境和设计、开发、测试其产品的过程，其可信任度均合理地来自于这些评价的结果，这足以证明：1)Oracle数据库服务器的相同版本在运行着相同操作系统的不同硬件配置上能安全地运行，2)Oracle数据库服务器的不同维护版本能在相同或相似的操作系统上安全地运行；3)Oracle服务器的不同维护版本能在类似Unix的操作系统上安全地运行。

相关性能

Oracle已经在美国和英国评价了Oracle7和Trusted Oracle7的标准商业版本，这确保了商业非定制(Commercial off-the-shelf, COTS)软件能满足严格的安全要求。另外，也满足许多其它标准和功能性指标。例如，Oracle7和Trusted Oracle7已经过美国国家标准与技术学会(NIST)的认证，100%地符合ANSI SQL 1989 (ISO 9075:1989)标准，包括完整性加强特性。

Oracle 经评价的数据库服务器是符合 Year2000 标准的。

Oracle8、Oracle7和Trusted Oracle7数据库服务器的评价版本是符合Year 2000标准的。除最近记录于ITSEC认证报告中的Year 2000安全检查之外，Oracle自己也验证了这些版本为符合Year 2000(或Y2K)要求的产品。

Trusted Oracle7 包含所有的 Oracle 功能，外加多级安全性能。

Trusted Oracle7包含Oracle7的所有功能。这两个产品均提供了先进的数据库管理系统(DBMS)技术，能通过不同操作系统、网络服务、交易处理系统和其它数据源提供透明的数据共享。有关此主题的更多信息参见这个白皮书中题为“附加信息”的最后章节。

安全性评价的好处

安全性评价具有了大量的好处。任何供应商都可以声明他的产品具备适当的安全性。这种声明的独立验证和由经认证的国际性组织做出的批准印记也服从于独立的评价测试，这种测试对产品安全机制实施中的潜在弱点进行额外的质量保证检查。直到所有发现的安全弱点都被供应商解决其产品才会通过评价。因此，最后的结果是政府或商业所使用的是一个经过严格测试、仔细检验的安全产品。

安全性评估

CC、ITSEC和TCSEC及前面部分所描述的其他标准的缺点之一是正式评价的高额成本。另一缺点是完成一个特定评价需要很长时间。

为对产品的安全声明进行独立验证的安全性评价的一个技术补充就是*安全性评估*。安全性评估以已有的安全风险评估技术为广泛基础，提供了一种在相对短的时间推断出供应商产品明显的安全性的卓越方法。

安全性评估可由机构自己的安全产品团队或由已签订合约协议的第三方来执行。利用已建立的第三方团体的优势就是他们能够为产品或系统提供一个无偏见的、独立的评估。

最近Oracle扩大了其安全性评价组的范围，把安全性评估包括在内。Oracle正对这些产品进行内部评估，并利用合约协议下独立的第三方团体的服务进行评估。

Oracle最普通的评估类型如下所述：

产品安全性评估（**Product Security Assessment**）

产品安全性评估通常只在理论文档水平上进行评估。通常评估者要求进行产品评估的供应商提供所有可用的有关产品的体系结构、设计和说明性文档。他们对产品体系结构可能具有的安全缺陷进行分析，然后在评估结束后生成的最终报告中提出建议。

这种方法很少单独使用，它常与如下所述的更加复杂的安全性评估方法中的渗透测试与攻击结合使用。

渗透测试（Penetration Testing）

渗透测试主要针对基于网络的软件产品和系统（如，在线商店、拍卖商、B2B的电子商务等等）进行渗透测试。渗透测试也对系统级体系结构进行分析。

产品攻击（Product Attack）

产品攻击通过聚焦某一特定产品对其进行深层的补充渗透测试。这一技术假设一个攻击者、外部实体或系统内部的人员已经获取对目标硬件（和软件）的控制级访问权限。产品攻击有以下两种类型：

- *黑匣子测试*。这类攻击试图决定一个知识渊博的攻击者企图违犯产品安全可能产生的结果。只通过分析其文档和其他可从公共途径获取的信息的对遭受攻击的产品进行此评估。
- *白匣子测试*。这类攻击是对黑匣子测试的扩展，它允许评估者获取产品的内在技术诀窍，如体系结构、说明书与技术文档以及产品原代码。

进行评估

利用前面所述的三种方法进行一个全面评估的过程与安全性评价相类似，但不需要像安全性评价一样要求必须有正式的产品文档。评估与评价间的另一个不同是评估者和评价者可获取的信息量不同。安全性评价要求对产品或系统进行深度分析，因此需要所有可获得的产品和/或系统文档。安全性评估不是非常正规，因此不要求同样数量的深层文档。因为安全性评估需要的时间比安全性评价所需要的要少许多，因此甚至在安全性评估的最初阶段，评估者也倾向于使用更加实际的（实用的，与理论相对）方法。评估者通常：

- 经历一个理解产品的过程，如：
 - 产品安全特性；
 - 产品运行环境；
 - **Internet**上的资源；
 - 初期研究与分析结果；
 - 已知的故障；
 - 在类似产品和体系结构方面的经验。
- 利用所收集的信息设计测试，并在开发的可能性和由此引起的潜在故障的数量的基础上按其优先次序进行排序。
- 执行前面所述的测试，并在适当的时候展开其他测试。

发布一份最终报告，详细描述所进行的测试的性质和所获得的结果。

安全性评估的益处

尽管安全性评估是安全性评价的删减形式，但它同样具备众多

的优点。安全性评估与安全性评价一样，能帮助改进产品的安全性。在评估过程中，评估者利用不同的技术发现潜在的或现存的安全隐患。评估通常在产品的开发阶段进行，因此，供应商有机会在产品向市场发布之前修复产品安全缺陷。即使产品已经开发完成并已用于政府部门和商业，潜在或现存弱点的发现并由供应商迅速响应解决此问题同样将极大地改进供应商和产品在安全性方面的信誉。其最终结果是经过严格测试、仔细检验和得到安全性证明的产品。

另外，安全性评价标准主要集中定位于操作系统、传统网络和数据库服务器，而没有关于评估基于Internet的产品和新开发范例（如网络编程）的信息。因为安全性评估不遵循严格的安全性评价风格方针，使评估者可超出传统安全性评价技术的领域，应用更新更根本的评估方法。

安全性评估的缺陷

即使安全性评估能为改进产品的总体质量起到巨大的作用，但其主要缺陷是以这种方式进行评估的产品不能有效地对照安全可信度（安全性标准）。

全球范围内的安全承诺

在Internet时代，安全性问题不仅只局限于政府部门和军事机构。随着对数据库服务器中的海量数据存储、安全可靠的网络、功能更强大的操作系统和大量更新的支持现代商业过程的基于Internet的产品和技术的日益依赖，对产品和系统的安全可信度的认证需求急剧增加。IT产品和系统的购买者不能再仅仅依赖于供应商的言辞。需要一种独立而公认的正式或非正式的标准来确保购买者正在使用的产品和系统是经过安全性证明的，安全性评价和安全性评估就是关键的两种测量标准。

Oracle向其用户承诺：提供独立的安全数据库服务器产品。为此，Oracle已与各种评价标准的主办者合作，以确保其标准适合于像数据库服务器这样的分层软件产品。为了用户和供应商双方的利益，Oracle还致力于使评价标准和方案向一致和互相认可的方向发展。Oracle安全性承诺的最好证明就是其自己出资对其产品进行广泛的安全性评价和安全性评估，并且成功地获得了比其他任何数据库供应商都多的世界安全性评价标准的高级保证认证。

通过采纳这两种技术，Oracle承诺为政府机构、军事部门和商业上的需求开发高质量、有安全意识和经过安全认证的产品。

Oracle公司对现有和正在发展的国际安全性标准的承诺使其处于开放的安全数据库技术的最前沿。

附录A


其它Oracle产品安全信息

<http://otn.oracle.com/deploy/security>
<http://www.oracle.com/ip/solve/continuity/security/>

下页提供的表格显示了已完成的和正在进行的安全性评价项目的当前状态。

关于 Oracle 安全性评价的所有问题，请直接联系 seceval_us@oracle.com

Oracle安全性评价的状态



	产品	版本	等级	标准	平台	状态
通用标准 (CC)	Oracle8	8.1.7	EAL4	ISO 15408	Solaris 2.6, NT 4.0	通过
	Oracle8	8.0.5	EAL4	ISO 15408	NT 4.0	通过
	Oracle7	7.2.2.4.13	EAL4	C.DBMS PP	NT 3.51	通过
	Oracle7	7.2.2.4.13	EAL3	C.DBMS PP	NT 3.51	通过
	Oracle7	7.3.4.0.0	E3/F-C2	E3/F-C2	NT 4.0	通过
	Oracle7	7.2.2.4.13	E3/F-C2	E3/F-C2	NT 3.51	通过
	Oracle7	7.0.13.6	E3/F-C2	E3/F-C2	Solaris 2.2	通过
	Trusted Oracle7	7.2.3.0.4	E3/F-B1	E3/F-B1	HP-UX CMW 10.16	通过
	Trusted Oracle7	7.1.5.9.3	E3/F-B1	E3/F-B1	Trusted Solaris 1.2	通过
	Trusted Oracle7	7.0.13.6	E3/F-B1	E3/F-B1	Solaris CMW 1.0	通过
	Oracle7	7.0.13.1	C2	C2	HP-UX BLS 8.0.4	通过
	Trusted Oracle7	7.0.13.1	B1	B1	HP-UX BLS 8.0.4	通过
	俄罗斯新 标准	Oracle8	8.0.3	IV	Russian Criteria	HP-UX 10.20
Oracle7		7.3.4	III	Russian Criteria	NT 4.0	通过
Oracle Advanced Security		8.1.6	2	FIPS 140-1	Solaris 2.6 SE	通过

附录B

其它安全性评价信息

US NSA 出版物

若要在美国订购NCSC文档，请用带公司抬头的信纸列出所要的文档名称和数量，发送此书面请求到下列地址：

National Computer Security Center(国家计算机安全中心)
Attention: S93
9800 Savage Road
Fort George G. Meade, MD 20755-6000
USA

来自美国国外的订单应直接通过适用于各国的美国国防部
(Department of Defense, DoD) 文档订购渠道来订购：
<http://www.radium.ncsc.mil/>

US FIPS 出版物

若要订购关于FIPS标准和验证过程的文档和出版物，请与NIST
联系：

National Institute of Standards and Technology
(国家标准和技术协会)
National Technical Information Service
(NTIS, 国家技术信息服务部)

5285 Port Royal Road
Springfield, VA 22161
USA

欧洲出版物

ITSEC

若需要 Information Technology Security Evaluation Criteria (ITSEC, 信息技术安全性评价标准) 的副本, 请向下列地址索取:

Commission of the European Communities

Directorate XIII/F
SOG-IS Secretariat, TR61 02/28
Rue de la Loi, 200
B-1049 Brussels
比利时

info@itsec.gov.uk

<http://www.itsec.gov.uk/docs/pdfs/formal/ITSEC.PDF>

英国方案

若需要UK ITSEC Scheme (英国ITSEC方案) 的副本, 请向下列地址索取:

UK ITSEC Scheme
Certification Body
PO Box 152
Cheltenham GL52 5UE
United Kingdom

电话: +44 1242 238739

传真: +44 1242 235233

info@itsec.gov.uk

<http://www.itsec.gov.uk/docs/pdfs/formal/UKSP01.PDF>

英国经过认证的产品列表

若需要经过认证的产品列表(UKSP06)的副本, 请向下列地址索取:

UK ITSEC Scheme
Certification Body
PO Box 152
Cheltenham GL52 5UE
United Kingdom

电话: +44 1242 238739

传真: +44 1242 235233

国际出版物

国际通用标准 (CC)

关于CC的信息可从下列地址获得:

Communications Security Establishment
Criteria Coordinator
R2B IT Security Standards and Initiatives
PO Box 9703, Terminal
Ottawa, Canada, K1G 3Z4

电话: +1 (613) 991-7409

criteria@cse-cst.gc.ca

<http://www.cse.dnd.ca>

Service Central de la Securite des Systemes d'Information

Bureau Normalisation, Criteres Communs
18 rue du docteur Zamenhof
92131 Issy les Molineux
France

电话: +33 (1) 41 46 37 84

ssi20@calva.net

Bundesamt für Sicherheit in der Informationstechnik

Abteilung V
Postfach 20 03 63
D-53133 Bonn
Germany

电话: +49 228 9582 300

cc@bsi.de

Netherlands National Communications Security Agency

Postbus 20061
NL 2500 EB Den Haag
Netherlands

电话: +31 70 348 5637

criteria@nlncsa.minbuza.nl

Communications-Electronics Security Group

Compusec Evaluation Methodology
P.O. Box 144
Cheltenham GL52 5UE
United Kingdom

电话: +44 1242 221 491 ext 4134

criteria@cesg.gov.uk

<http://www.cesg.gov.uk/>

National Institute of Standards and Technology

Computer Security Division
NIST North Building, Room 426
Gaithersburg, Maryland 20899
USA

电话: +1 (301) 975-2934

criteria@nist.gov

<http://www.csrc.nist.gov/cc>

National Security Agency

Attn: V2, Common Criteria Technical Advisor
Fort George G. Meade, Maryland 20755
USA

电话: +1 (410) 859-4458

common_criteria@rdium.ncsc.mil

<http://www.radium.ncsc.mil/tpep>

俄罗斯出版物

关于俄罗斯评价标准的信息可写信至下列地址获得：

State Technical Commission
Military Publishing House
03160, Moscow K-160
Small Enterprise “PRINT”
119633, Moscow, Prirechnaya St. 3
Russian Federation

2000年10月

本文件目的仅为提供信息，文中信息发生改变不另行通知。请将文中的错误之处通知Oracle公司。Oracle公司不提供任何保证，并明确表示不承担与此文件相关的任何责任。

Oracle和Software Powers the Internet为注册商标。Oracle7、Oracle8、Oracle8i、Trusted Oracle和Security Without Compromise都是Oracle公司的商标。

ORACLE

Oracle 公司
世界总部
500 Oracle Parkway
Redwood Shores, CA 94065
USA.

全球咨询方式:

电话:+1.650.506.7000

传真:+1.650.633.0489

网址: <http://www.oracle.com/>

版权©1995、1996、1997、1998、1999、2000归Oracle公司所有，未经允许，不得以任何方式和手段复制和使用。
美国印刷