第 3 章　安全功能组件和安全保障组件

由第 2 章可知，CC 提供了一套描述 IT 产品安全评估的标准化技术术语及预定义的安全功能组件和安全保障组件列表，可用于规范性地描述 IT 产品的安全要求及安全方案，并规范 TOE 安全评估过程和方法，指导 IT 产品供应商的安全功能设计、开发、测试和产业化推广等。

为理解 IT 产品客户需求（即 PP）和 IT 产品供应商解决方案（ST）的编制方法，便于按 CEM 对 IT 产品实施评估活动，有必要掌握 CC 中安全功能组件和安全保障组件结构，理解 CEM 中基于 CC 的 IT 产品安全评估模型及安全保障组件的评估活动内容。

本章将围绕 GB/T 18336—2015 第 2 部分和第 3 部分文档，对 CC 安全功能组件和安全保障组件进行解读，具体内容包括以下两个部分。

（1）GB/T 18336.2—2015（简称 CC 第 2 部分）：解释安全功能要求范型、安全功能组件层次关系、11 种安全功能类相关的族及其组件列表。

（2）GB/T 18336.3—2015（简称 CC 第 3 部分）：解释安全保障概念、保障组件层次关系、PP、ST 和 TOE 安全保障族及其组件列表，包括预定义的安全保障包（EAL）。

3.1　安全功能组件

CC 第 2 部分给出了描述 IT 产品安全功能要求（SFR）的一个标准化安全功能组件目录。这个标准化安全功能组件列表用于以下用途。

（1）在 PP/ST 中描述 TOE 预期的安全行为。

（2）满足 PP/ST 中所列 TOE 的安全目的。

（3）规范用户通过 TOE 直接交付或促使 TOE 响应用户请求的可测试安全功能。

（4）应对在 TOE 预期运行环境中的各种威胁。

（5）覆盖在 PP/ST 中所有指定的组织安全策略。

3.1.1　功能组件结构

CC 第 2 部分的安全功能组件可用于规范 TOE 的安全功能要求（SFR）。这些 SFR 可定义多个安全功能策略（SFP），以表达 TOE 必须执行的安全规则。每个这样的 SFP 必须通过定义主体、客体、资源或信息，及其适用的操作，来明确说明该安全功能策略的控制范围。IT 产品的所有 SFP 均由 TOE 安全功能（TSF）实现，即 TSF 机制执行 SFR 中定义的规则并提供必要的 TSF 自身安全保护能力。

CC 将 IT 产品的安全功能组织为一个分层功能结构（如图 3.1 所示）。

（1）类：由族组成。

（2）族：由组件组成。

（3）组件：由元素组成。

(4) 元素：一个不可分割的基本功能要求。

GB/T 18336—2015 第 2 部分共列出了 11 个类、65 个族和 136 个安全功能组件。类、族、组件和元素间的层次关系如图 3.1 所示。组件由元素组成，构成了不能再分的最小安全要求集合，它是 PP、ST、TOE 或包安全功能要求选择的最小单位。在 CC 中，以“类_族.组件号”的方式标识组件，例如组件“FDP_DAU.1 基本数据鉴别”，其中 FDP 指“用户数据保护”功能类，DAU 指“数据鉴别”族。

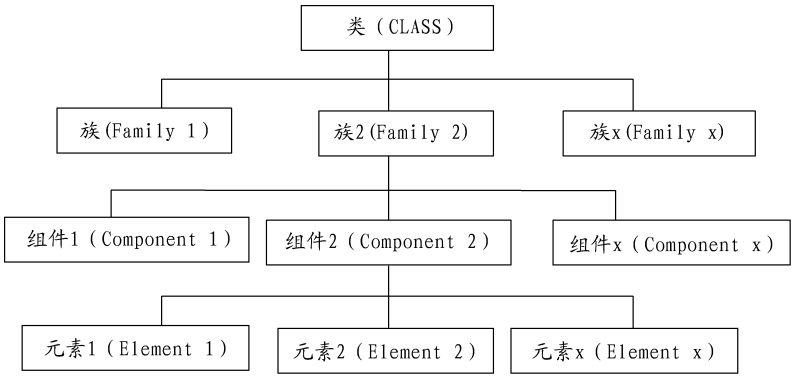

图 3.1　安全功能类、族、组件和元素的层次关系

CC 中的安全功能类是用来描述一组共享共同关注点的安全要求集合。换句话说，类中所有族成员及其安全功能组件关注共同的安全目的。CC 中的功能类安全目的是可知的，并且有一个结构化表格来描述组成类的族成员。表 3.1 列出了 CC 中 11 个安全功能类及其安全目的，其中前 7 个安全功能类与 IT 产品用户紧密相关，而后 4 个安全功能类是为确保 IT 产品自身安全的安全功能模块设置的。因此后 4 个安全功能类用于对 TOE 安全功能(TSF)模块自身安全性进行保证。CC 给每个功能类都赋予一个长名和一个以 F 开头的 3 个字母的助记符短名标识。

表 3.1　安全功能类

短　名	长　名	安 全 目 的
FAU	安全审计	监控、获取、记录、存储、分析和报告与安全事件有关的信息
FCO	通信	确认信息传送的原发者身份和接收者身份，并确保原发者不能否认发送过信息，接收者也不能否认收到过信息
FCS	密码支持	管理和控制密钥及密钥在运算过程中的使用安全
FDP	用户数据保护	保护在输入、输出和存储过程中的 TOE 内部的用户数据，以及与用户数据直接相关的安全属性数据
FIA	标识和鉴别	确保授权用户的无歧义标识以及安全属性与用户/主体的正确绑定
FMT	安全管理	管理安全属性、数据和安全功能，并定义安全角色及其相互作用，如权限分离原则
FPR	隐私	提供用户信息不被其他用户发现或滥用的保护
FPT	TSF 保护	维护 TSF 管理功能及其数据的完整性
FRU	资源利用	通过容错和服务优先等机制确保所需资源的可用性
FTA	TOE 访问	控制建立用户会话
FTP	可信路径/信道	提供用户和 TSF 之间，以及 TSF 和其他可信 IT 产品之间的可信通信路径

图 3.2 展示了 CC 安全功能类的结构，每个类包括类名、类介绍和一个或多个族成员。

注意，11 个安全功能类彼此之间是并列关系，类之间不存在层次关系。因此，在 CC 第 2 部分定义的功能类是按照类的助记符短名字母进行排序的。

从图 3.2 安全功能类结构示意图可看出，类的成员是功能族。族是用来陈述一组共享安全目的但是安全关注点或安全精确度不一样的安全功能组件。在 CC 第 2 部分中，每个功能族都在类名下面被分配了一个方便记忆的 3 个字母的助记符，它和类助记符共同构成一个功能族短名。CC 的安全功能族结构提供了标识和划分功能族所必需的分类和描述信息。每个功能族有一个唯一的名称，其标识信息由 7 个字符组成：前三个字符与类名助记符相同，后面跟一个下画线和 3 个字符组成的族名助记符。例如“FDP_DAU 数据鉴别”，其中 FDP 指“用户数据保护”类，DAU 指“数据鉴别”族。图 3.3 以框图形式展示了 CC 的功能族结构，其中族行为描述了功能族的安全目的，是对该族所有安全功能组件要求的概括描述。

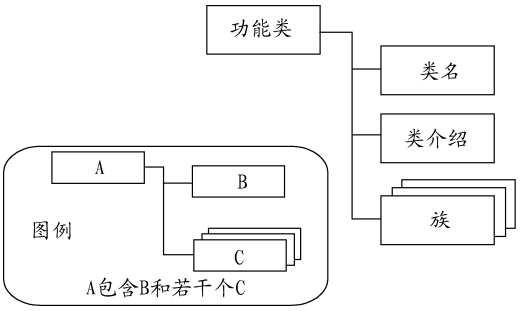

图 3.2 安全功能类结构示意

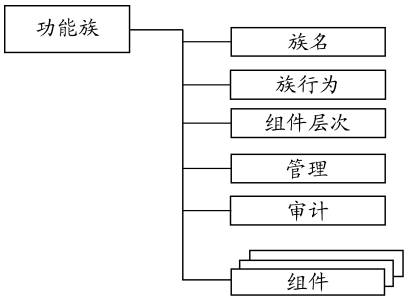

图 3.3 安全功能族结构示意

图 3.3 族结构中的“族行为”部分描述可用的组件以及使用这些组件的基本原理（及组件满足的安全目的）。如果一个族成员（组件）存在层次关系或顺序，换句话说如果一个组件相对另一个组件提供更多的安全功能或安全保障能力，那么“组件层次”部分描述这些组件之间的层次关系，即一个组件相对另一个组件来说包含了更高级别的安全功能。有关操作安全管理活动和会被审计的安全事件建议在“管理”部分描述。如果 PP/ST 中包含来自 FAU 类“安全审计”中的要求，功能族中的“审计”部分包含了可供 PP/ST 作者选择的有关该安全功能组件的可审计事件。

图 3.3 的“组件”是一组安全要求的特殊集合，它由一系列元素构建而成。组件中的元素是一个不可分割的安全要求，它可通过第 6 章介绍的 CEM 中某个安全评估工作单元来验证。

每个组件都有一个有意义的长名，用以识别和描述该组件安全要求。CC 第 2 部分给每个安全功能组件分配了一个包含了类助记符、族助记符和一个唯一的数字组成的短名。组件短名的标记结构如图 3.4 所示，每个组件可由一个或多个元素组成，每个功能元素名都有一个唯一的简化形式。图 3.4 以 FDP_IFF.4.2 组件元素为例列出了 CC 中的安全功能类、族、组件和元素的符号记法，各项意义为：F——功能要求；DP——“用户数据保护”类；_IFF——“信息流控制功能”族；.4——第 4 个组件；名为“部分消除非法信息流”；.2——该组件的第 2 个元素。如果一个组件有不止一个元素，那么在 PP/ST 编制中它们全部都要被使用，否则就必须为该 PP/ST 定义一个满足特定要求的扩展组件。

图 3.5 展示了 CC 第 2 部分的安全功能组件的结构。“组件标识”部分提供识别、分类、注册和交叉引用组件所必需的描述性信息。“依赖关系”列表提供了一个对其他功能和保障组件依赖关系的完整列表。所依赖的组件又可能依赖其他组件。组件依赖关系中提供的组件列表是直接的依赖关系，这只是为该功能要求能正确实现其功能提供参考。间接依赖关系，也就是由所依赖组件产生的依赖关系。功能组件依赖关系可参见 CC 第 2 部分的附录。注意有些组件可能列出“无依赖关系”。“功能元素”是该组件的一个安全功能要求，是一个再进一步划分将不会产生有意义评估结果的组件元素。因此组件元素是 CC 中标识和认可的最小安全功能要求，当构建包、PP/ST、TOE 安全要求时，CC 不允许 TOE 消费者和开发者从一个组件中只选择一个或几个组件元素，必须将组件的所有元素包含在 PP、ST、TOE 或包中。

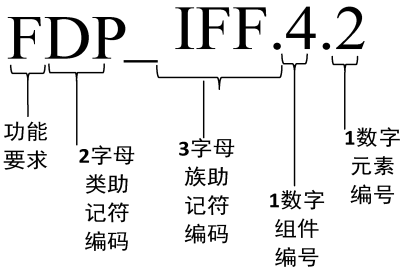

图 3.4　功能类、族、组件和元素的标准符号记法

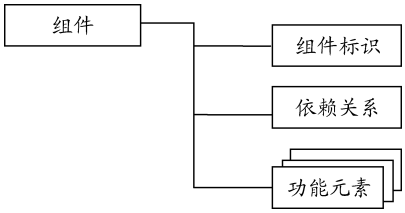

图 3.5　安全功能组件结构

用户可用 CC 第 2 部分的 11 个功能类描述 IT 产品常见的安全功能要求。当 PP/ST 编制人员选择安全功能组件去构建 TOE 的安全要求时，首先需确定合适的功能类。表 3.2～表 3.12 按照功能类列出了 CC 第 2 部分定义的 11 种安全功能类相关的族及其组件列表。

3.1.2　安全审计功能组件

CC 第 2 部分讨论的第一个安全功能类是安全审计(FAU)。该类由定义如何选择审计事件、产生审计数据、查阅和分析审计数据、对安全事件自动响应以及存储和保护审计数据等方面要求的功能族组成(如表 3.2 所示)。FAU 族和组件的多样化为 TSF 描述提供了全方位的安全审计要求，提供了识别、记录、存储和分析那些与 TOE 安全行为有关事件的信息。另外，FAU 族和组件也给出可用来对抗针对安全审计功能攻击的一些方式——权限误用以及绕过审计功能来阻止审计事件的获取等安全要求。

表 3.2　FAU 功能类：安全审计

族 标 识	族 名 称	功 能 描 述	包 含 组 件	组 件 名 称
FAU_ARP	安全审计自动响应	定义在检测到潜在安全侵害事件时所作出的动作	FAU_ARP.1	安全告警
FAU_GEN	安全审计数据产生	定义需要记录的安全相关事件	FAU_GEN.1	审计数据产生
			FAU_GEN.2	用户身份关联
FAU_SAA	安全审计分析	定义安全事件的自动化分析要求	FAU_SAA.1	潜在侵害分析
			FAU_SAA.2	基于轮廓的异常检测
			FAU_SAA.3	简单攻击探测
			FAU_SAA.4	复杂攻击探测

续表

族 标 识	族 名 称	功 能 描 述	包 含 组 件	组 件 名 称
FAU_SAR	安全审计查阅	定义审计工具的相关要求	FAU_SAR.1	审计查阅
			FAU_SAR.2	限制审计查阅
			FAU_SAR.3	可选审计查阅
FAU_SEL	安全审计事件选择	定义在 TOE 运行期间从所有审计事件集合中选取被审计事件的要求	FAU_SEL.1	选择性审计
FAU_STG	安全审计事件存储	定义一些 TSF 能够创建并维护一个安全审计迹的要求	FAU_STG.1	受保护的审计迹存储
			FAU_STG.2	审计数据可用性保证
			FAU_STG.3	审计数据可能丢失时的行为
			FAU_STG.4	防止审计数据丢失

3.1.3 通信功能组件

CC 第 2 部分讨论的第二个安全功能类是通信(FCO)。如类名所示的那样，FCO 安全功能从属于信息传输，特别关注如何确认在数据交换中参与方的身份、确认信息传输的原发者身份(原发证明)和信息传输的接收者身份(接收证明)。通信类有两个族用来确保原发者不能否认发送过信息，接收者也不能否认收到过信息。FCO 安全功能类提供了两个族，原发抗抵赖(FCO_NRO)和接收抗抵赖(FCO_NRR)，相关组件如表 3.3 所示，FCO 族尤其关注这些安全功能凭据的生成。

表 3.3 FCO 功能类：通信

族 标 识	族 名 称	功 能 描 述	包 含 组 件	组 件 名 称
FCO_NRO	原发抗抵赖	信息的发送者提供请求信息原发证据	FCO_NRO.1	选择性原发证明
			FCO_NRO.2	强制性原发证明
FCO_NRR	接收抗抵赖	信息的接收者提供请求信息接收证据	FCO_NRR.1	选择性接收证明
			FCO_NRR.2	强制性接收证明

3.1.4 密码支持功能组件

密码支持(FCS)类是 CC 第 2 部分第三个被讨论的安全功能类。该类应用于 IT 产品的密码模块(硬件、软件和固件)的数据加密。如 2.1 节所说，CC 并不声明哪些加密算法或密钥长度是可被接受的。取而代之的是，FCS 类关注 TOE 的数据加解密操作和密钥管理——换句话说就是 TOE 加密功能的安全使用技术要求。每当需要使用生成或验证数字签名、加密或解密数据等安全功能时，就需要调用 FCS 组件和元素。同样地，FCS 组件和元素也被调用来指定 TOE 整个生命周期内的密钥管理活动，如密钥生成、分发、存取、销毁和运算(如表 3.4 所示)。

表 3.4　FCS 功能类：密码支持

族 标 识	族 名 称	功 能 描 述	包 含 组 件	组 件 名 称
FCS_CKM	密钥管理	指定整个生命周期内的密钥管理活动	FCS_CKM.1	密钥生成
			FCS_CKM.2	密钥分发
			FCS_CKM.3	密钥存取
			FCS_CKM.4	密钥销毁
FCS_COP	密码运算	按照特定的算法和规定长度的密钥来进行运算	FCS_COP.1	密码运算

3.1.5　用户数据保护功能组件

用户数据保护(FDP)定义了 TOE 保护用户数据的各种安全要求。这些要求通过 4 组功能族(如表 3.5 所示)来描述在输入、输出和存储过程中的 TOE 内部用户数据保护,以及与用户数据保护直接相关的安全属性。

表 3.5　FDP 功能类：用户数据保护

族 标 识	族 名 称	功 能 描 述	包 含 组 件	组 件 名 称
FDP_ACC	访问控制策略	定义访问控制策略及每一策略的控制范围	FDP_ACC.1	子集访问控制
			FDP_ACC.2	完全访问控制
FDP_ACF	访问控制功能	描述在 FDP_ACC“访问控制策略”中所命名的访问控制实现	FDP_ACF.1	基于安全属性的访问控制
FDP_DAU	数据鉴别	提供保证特定数据有效性信息	FDP_DAU.1	基本数据鉴别
			FDP_DAU.2	带担保者身份的数据鉴别
FDP_ETC	从 TOE 输出	定义从 TOE 输出用户数据或与所输出用户数据与安全属性之间的安全限制	FDP_ETC.1	不带安全属性的用户数据输出
			FDP_ETC.2	带有安全属性的用户数据输出
FDP_IFC	信息流控制策略	定义信息流控制策略及每一策略的控制范围	FDP_IFC.1	子集信息流控制
			FDP_IFC.2	完全信息流控制
FDP_IFF	信息流控制功能	描述实现已信息流控制 SFP 的特定功能的一些规则	FDP_IFF.1	简单安全属性
			FDP_IFF.2	分级安全属性
			FDP_IFF.3	受限的非法信息流
			FDP_IFF.4	部分消除非法信息流
			FDP_IFF.5	无非法信息流
			FDP_IFF.6	非法信息流监视
FDP_ITC	从 TOE 之外输入	定义从 TOE 输入用户数据或与所输入用户数据与安全属性之间的安全限制	FDP_ITC.1	不带安全属性的用户数据输入
			FDP_ITC.2	带安全属性的用户数据输入
FDP_ITT	TOE 内部传输	定义用户数据通过内部信道在 TOE 各部分之间传输时的用户数据保护要求	FDP_ITT.1	基本内部传输保护
			FDP_ITT.2	按属性分隔传输
			FDP_ITT.3	完整性监视
			FDP_ITT.4	基于属性的完整性监视

续表

族 标 识	族 名 称	功 能 描 述	包 含 组 件	组 件 名 称
FDP_RIP	残余信息保护	确保当资源从一个客体释放并重新分配给另一个客体时，其中的任何数据都不可用	FDP_RIP.1	子集残余信息保护
			FDP_RIP.2	完全残余信息保护
FDP_ROL	回退	撤销最后一次或一系列操作，并返回到一个先前已知的状态	FDP_ROL.1	基本回退
			FDP_ROL.2	高级回退
FDP_SDI	存储数据的完整性	对存储在由 TSF 控制的载体内的用户数据进行保护	FDP_SDI.1	存储数据的完整性监视
			FDP_SDI.2	存储数据完整性监视和行动
FDP_UCT	TSF 间用户数据保密性传输保护	确保用户数据通过外部信道在 TOE 和其他可信 IT 产品间传输时用户数据保密性	FDP_UCT.1	基本的数据交换保密性
FDP_UIT	TSF 间用户数据完整性传输保护	用户数据在 TOE 和其他可信 IT 产品间传输时提供完整性保护	FDP_UIT.1	数据交换的完整性
			FDP_UIT.2	原发端数据交换恢复
			FDP_UIT.3	接收端数据交换恢复

本类中的 4 组功能族如下。

(1) 用户数据安全保护策略，包括访问控制策略(FDP_ACC)和信息流控制策略(FDP_IFC)功能组件，以允许 PP/ST 作者命名用户数据保护安全功能策略，并定义该安全策略的控制范围，这对于说明安全目的是必要的。

(2) 在不同类型的在线事务中保护用户数据完整性和一致性的安全功能，包括访问控制功能(FDP_ACF)、信息流控制功能(FDP_IFF)、TOE 内部传送(FDP_ITT)、残余信息保护(FDP_RIP)、回退(FDP_ROL)和存储数据的完整性(FDP_SDI)等用户数据保护形式功能组件。

(3) 在脱机事务中的用户数据保护功能，如离线导入(FDP_ITC)、导出(FDP_ETC)、数据鉴别(FDP_DAU)等数据转储安全功能。

(4) 负责处理 TSF 与其他可信 IT 产品间的通信中的用户数据完整性和一致性的安全功能，如 TSF 间用户数据保密性传送保护(FDP_UCT)和 TSF 间用户数据完整性传送保护(FDP_UIT)。

3.1.6 用户标识与鉴别功能组件

CC 第 2 部分讨论的第五个安全功能类是用户标识与鉴别(FIA)。正如名称预期，该安全功能类定义了执行和管理用户身份鉴别和认证功能的要求。授权用户的明确标识以及安全属性与用户和主体的正确绑定是实施预定安全策略的关键。本类中的安全功能族负责确认和验证使用 TOE 的用户身份、确认他们与 TOE 交互的权限、以及每个授权用户安全属

性的正确绑定。CC 中的其他安全功能类(如 FDP“用户数据保护”、FAU“安全审计”) 要求的有效性都是建立在对用户身份的正确标识和鉴别基础上的(如表 3.6 所示)。用户标识与鉴别确保潜在用户的正确身份都是确定的,无论是认证的或非认证的。用户认证确保用户的声明身份都是被验证的。相对于 TOE,每个认证用户的访问控制能力及其授予的权限都应该是确定的。另外,用户认证都应该遵循一定的安全策略,例如在认证失败达到指定次数后 TOE 要采取的行为也应是定义的。

表 3.6　FIA 功能类：标识和鉴别

族　标　识	族　名　称	功 能 描 述	包 含 组 件	组 件 名 称
FIA_AFL	鉴别失败	定义不成功的鉴别尝试次数和鉴别尝试失败时 TSF 应采取的动作	FIA_AFL.1	鉴别失败处理
FIA_ATD	用户属性定义	定义用户相关的安全属性	FIA_ATD.1	用户属性定义
FIA_SOS	秘密的规范	定义生成和提供秘密应满足规定的质量度量及度量机制	FIA_SOS.1	秘密的验证
			FIA_SOS.2	TSF 生成秘密
FIA_UAU	用户鉴别	定义 TSF 所支持的用户鉴别机制的类型	FIA_UAU.1	鉴别的时机
			FIA_UAU.2	任何动作前的用户鉴别
			FIA_UAU.3	不可伪造的鉴别
			FIA_UAU.4	一次性鉴别机制
			FIA_UAU.5	多重鉴别机制
			FIA_UAU.6	重鉴别
			FIA_UAU.7	受保护的鉴别反馈
FIA_UID	用户标识	定义用户标识其身份的条件	FIA_UID.1	标识的时机
			FIA_UID.2	任何动作前的用户标识
FIA_USB	用户-主体绑定	定义建立和维护用户安全属性与代表该用户主体间关联关系的要求	FIA_USB.1	用户-主体绑定

3.1.7　安全管理功能组件

安全管理(FMT)类指定了管理 TOE 安全功能和它们的属性和数据的要求,包括建立、撤销和终结安全属性的条件(如表 3.7 所示)。FMT 要求 TOE 安全功能被调用以及被谁调用等管理规则应是确定的。安全管理人员职责分离和责任,以及安全管理人员与其他操作人员的职责和责任分享规则等也应是建立的。安全管理类主要有以下几个目的。

(1) 管理 TSF 数据。

(2) 管理安全属性。

(3) 管理 TSF 功能。

(4) 定义安全角色。

表 3.7 FMT 功能类：安全管理

族 标 识	族 名 称	功 能 描 述	包 含 组 件	组 件 名 称
FMT_MOF	TSF 中功能的管理	允许授权用户控制对 TSF 中功能的管理	FMT_MOF	安全功能行为的管理
FMT_MSA	安全属性的管理	允许授权用户控制安全属性的管理	FMT_MSA.1	安全属性的管理
			FMT_MSA.2	安全的安全属性
			FMT_MSA.3	静态属性初始化
			FMT_MSA.4	安全属性值的继承
FMT_MTD	TSF 数据管理	允许授权用户（角色）控制 TSF 数据的管理	FMT_MTD.1	TSF 数据的管理
			FMT_MTD.2	TSF 数据限值的管理
			FMT_MTD.3	安全的 TSF 数据
FMT_REV	撤销	撤销 TOE 内各种实体安全属性	FMT_REV.1	撤销
FMT_SAE	安全属性到期	对安全属性的有效性实施时间限制	FMT_SAE.1	时限授权
FMT_SMF	管理功能规范	定义 TSF 提供安全的管理功能	FMT_SMF.1	管理功能规范
FMT_SMR	安全管理角色	控制用户不同角色的分配	FMT_SMR.1	安全角色
			FMT_SMR.2	安全角色限制
			FMT_SMR.3	承担角色

3.1.8 隐私功能组件

隐私要求在 CC 第 2 部分的 FPR 类中指定。这些要求的目的是保护用户身份等个人信息不被泄露、误用或与 TOE 资源的使用相关联。如表 3.8 所示，隐私要求类由匿名、假名、不可关联性和不可观察性 4 个族组成。

表 3.8 FPR 功能类：隐私

族 标 识	族 名 称	功 能 描 述	包 含 组 件	组 件 名 称
FPR_ANO	匿名	确保用户在其使用资源或服务时，不暴露身份	FPR_ANO.1	匿名
			FPR_ANO.2	无索求信息的匿名
FPR_PSE	假名	确保用户在不暴露其真实身份的情况下使用资源或服务，但仍能对该次使用负责	FPR_PSE.1	假名
			FPR_PSE.2	可逆假名
			FPR_PSE.3	别名假名
FPR_UNL	不可关联性	一个用户可以多次使用资源和服务，但任何人都不能将这些使用联系在一起	FPR_UNL.1	不可关联性
FPR_UNO	不可观察性	用户在使用资源和服务时，其他人，特别是第三方不能观察到该资源和服务正在被使用	FPR_UNO.1	不可观察性
			FPR_UNO.2	影响不可观察性的信息的分配
			FPR_UNO.3	无索求信息的不可观察性
			FPR_UNO.4	授权用户可观察性

3.1.9　TSF 保护功能组件

TSF 保护(FPT)类包含了保护 TOE 安全功能(TSF)和 TOE 安全功能数据(安全元数据)的要求。TOE 依靠的底层硬件和操作系统等 IT 运行环境必须如预期一样执行,以确保 TOE 安全功能的正确运行。因此,FPT 类中定义了验证 TSF 正确运行的安全要求,例如自检测、重放检测、响应 TOE 物理攻击等。如表 3.9 所示,FPT 定义了 TOE 安全功能输出数据的一致性、完整性和有效性的要求,同样也定义了内部数据传输或复制数据的一致性、完整性和有效性要求。TOE 安全功能的可信启动与恢复条件在该类中声明。检测和重播消息、生成可信时间戳、同步重要安全功能时间的机制等也在该类中指定。其他族确保 TOE 安全策略的要求总是被调用并强制执行。

表 3.9　FPT 功能类：TSF 保护

族 标 识	族 名 称	功 能 描 述	包 含 组 件	组 件 名 称
FPT_FLS	失效保护	确保当确定的失效出现时,TOE 总是保持一种安全状态	FPT_FLS.1	失效即保持安全状态
FPT_ITA	输出 TSF 数据的可用性	确保向另一个可信 IT 产品提供的 TSF 数据是可用的	FPT_ITA.1	TSF 间可用性不超过既定可用性度量
FPT_ITC	输出 TSF 数据的保密性	确保在 TSF 与另一个可信 IT 产品间传输时,TSF 数据不被泄露	FPT_ITC.1	传输过程中 TSF 间的保密性
FPT_ITI	输出 TSF 数据的完整性	确保在 TSF 与另一个可信 IT 产品之间传输时,TSF 数据不会被未授权修改	FPT_ITI.1	TSF 间篡改的检测
			FPT_ITI.2	TSF 间篡改的检测与纠正
FPT_ITT	TOE 内 TSF 数据的传输	确保在 TOE 的不同部件间传输的 TSF 数据是安全和完整的	FPT_ITT.1	内部 TSF 数据传输的基本保护
			FPT_ITT.2	TSF 数据传输的分离
			FPT_ITT.3	TSF 数据完整性监视
FPT_PHP	TSF 物理保护	限制对 TSF 进行未授权的物理访问,以及阻止和抵抗对 TSF 进行未授权的物理修改或替换	FPT_PHP.1	物理攻击的被动检测
			FPT_PHP.2	物理攻击报告
			FPT_PHP.3	物理攻击抵抗
FPT_RCV	可信恢复	确保 TSF 能确定 TOE 是在没有削弱保护能力的情况下启动的,并在运行中断后能在不削弱保护能力的情况下恢复	FPT_RCV.1	手工恢复
			FPT_RCV.2	自动恢复
			FPT_RCV.3	无过度损失的自动恢复
			FPT_RCV.4	功能恢复
FPT_RPL	重放检测	要求 TSF 应能够检测出既定实体的重放	FPT_RPL.1	重放检测
FPT_SSP	状态同步协议	规定了关于 TSF 某些关键安全功能如何使用该可信协议的要求	FPT_SSP.1	简单可信回执
			FPT_SSP.2	相互可信回执
FPT_STM	时间戳	要求 TSF 为 TSF 功能提供可靠的时间戳	FPT_STM.1	可靠的时间戳

续表

族 标 识	族 名 称	功 能 描 述	包 含 组 件	组 件 名 称
FPT_TDC	TSF 间 TSF 数据的一致性	要求 TSF 提供确保 TSF 间属性的一致性	FPT_TDC.1	TSF 间基本的 TSF 数据一致性
FPT_TEE	外部实体测试	规定了由 TSF 测试外部实体的要求	FPT_TEE.1	外部实体测试
FPT_TRC	TOE 内 TSF 数据复制的一致性	要求 TSF 确保 TSF 数据在多处复制时的一致性	FPT_TRC.1	内部 TSF 的一致性
FPT_TST	TSF 自检	提供检测 TSF 是否正确运转的能力	FPT_TST.1	TSF 检测

3.1.10 资源利用功能组件

资源利用(FRU)类中的资源使用要求保证了 TOE 资源的有效性。本类提供 3 个族以支持所需资源的可用性，诸如处理能力或存储容量(如表 3.10 所示)。容错要求确保声明的 TOE 功能能够继续正确执行，即使是在经历了指定的失败状况下。FRU 允许 TOE 安全功能被分配到与其他低优先级功能相关的资源使用优先级。另外，FRU 要求允许资源在已知用户和主体间被分配，从而防止资源垄断和拒绝服务攻击。

表 3.10 FRU 功能类：资源利用

族 标 识	族 名 称	功 能 描 述	包 含 组 件	组 件 名 称
FRU_FLT	容错	确保即便发生了失效，TOE 也将维持正常运转	FRU_FLT.1	降级容错
			FRU_FLT.2	受限容错
FRU_PRS	服务优先级	确保 TSF 控制下高优先级活动均能完成，而不受低优先级活动造成的不当干扰或延迟影响	FRU_PRS.1	有限服务优先级
			FRU_PRS.2	全部服务优先级
FRU_RSA	资源分配	提供配额机制的要求，确保用户和主体不因未授权地独占资源而出现拒绝服务	FRU_RSA.1	最高配额
			FRU_RSA.2	最低和最高配额

3.1.11 TOE 访问功能组件

评估 TOE 访问控制功能的要求包含在 FTA 类中。该类定义了建立一个用户会话的 6 种类型的控制安全要求(如表 3.11 所示)。

(1) 在一个给定会话中限制用户访问的安全属性范围。

(2) 限制单独一个用户通过多个终端访问 TOE 的多个并行会话。

(3) 锁定和解锁用户会话以响应指定控制规则或参数值要求。

(4) 显示 TOE 资源使用的查询。

(5) 显示一个用户的 TOE 访问历史，包含成功的和不成功的尝试。

(6) 拒绝会话建立。

表 3.11　FTA 功能类：TOE 访问

族 标 识	族 名 称	功 能 描 述	包 含 组 件	组 件 名 称
FTA_LSA	可选属性范围限定	提供关于 TOE 在建立会话时限制会话安全属性范围定义能力	FTA_LSA.1	可选属性范围限定
FTA_MCS	多重并发会话限定	限制属于同一个用户的并发会话数	FTA_MCS.1	多重并发会话的基本限定
			FTA_MCS.2	基于属性的单用户多重并发会话限定
FTA_SSL	会话锁定和终止	提供 TSF 原发和用户原发的交互式会话的锁定、解锁和终止能力	FTA_SSL.1	TSF 原发会话锁定
			FTA_SSL.2	用户原发会话锁定
			FTA_SSL.3	TSF 原发会话终止
			FTA_SSL.4	用户原发会话终止
FTA_TAB	TOE 访问旗标	定义向用户显示有关适当使用 TOE 的一个可配置劝告性警示信息要求	FTA_TAB.1	默认的 TOE 访问旗标
FTA_TAH	TOE 访问历史	提供了 TOE 显示与先前尝试建立一个会话相关的信息的要求	FTA_TAH.1	TOE 访问历史
FTA_TSE	TOE 会话建立	提供了拒绝用户基于属性对 TOE 进行访问的要求	FTA_TSE.1	TOE 会话建立

3.1.12　可信路径/信道功能组件

可信路径/信道(FTP)类定义了可信路径和可信信道的要求。若要建立和维护一个 TOE 安全功能和其他可信 IT 产品之间的安全通信信道，就需要使用可信信道要求。在某个应用中，用户或 TOE 安全功能数据可能需要被交换以执行重要安全功能，这就需要在它们之间建立一个可信信道。相反地，若需建立和维护用户与 TOE 安全功能之间的安全通信，就需要用到可信路径要求。对于可信信道和可信路径，通信双方都在该类中被指定，数据将被保护以防止在传输中被未鉴别的非法用户进行有意或无意的修改与泄露。通信可在可信信道或可信路径的任一端被初始化。表 3.12 给出了 FTP 类族及其安全组件列表。

表 3.12　FTP 功能类：可信路径/信道

族 标 识	族 名 称	功 能 描 述	包 含 组 件	组 件 名 称
FTP_ITC	TSF 间可信信道	在 TSF 和其他可信 IT 产品之间提供一个可信信道	FTP_ITC.1	TSF 间可信信道
FTP_TRP	可信路径	在 TSF 和用户之间提供一条可信路径	FTP_TRP.1	可信路径

3.2 安全保障组件

由第 2 章的讨论可知，CC 评估模型包括两个基本原则：一是要求 PP/ST 中 TOE 安全威胁和组织安全策略应描述清楚，并且基于 CC 所提出的安全功能要求和安全保障要求（安全控制措施）来论证足以达到所期望的安全目的；二是通过使用 CEM 对 IT 产品进行安全评估（主动调查）来提供安全保障，以增强用户信任被评估过的 IT 产品是满足他们的安全需求的。

TOE 安全保障一般通过采用软件工程、开发环境控制、交付运行控制、各种安全测试等安全保障措施使得 TOE 消费者、开发者和评估者对 TOE 的安全功能正确有效地实施产生信心。CC 第 3 部分对这些安全控制措施相关的保障要求进行了规范化定义，给出了定义 IT 产品标准化安全保障要求的组件目录。

TOE 安全保障要求划分是以保障类为依据的，每个保障类又细分为多个保障族，每个保障族都有相关的安全目的。保障族又由一个或多个保障组件组成。每个保障组件也有为完成保障族中安全目的而分隔出来的子安全目的，通过保障组件安全目的实现而支持此保障族所有的安全目的。保障组件是由一组保障元素组成，每个保障元素分别从 TOE 开发者、评估者和评估内容与证据的角度对保障组件所包含的内容和评估依据进行阐述。

CC 第 3 部分包括以下几部分。

（1）评估保障级（EAL）——为度量 TOE 的安全保障能力定义的一种尺度。

（2）组合保障包（CAP）——为度量组合 TOE 的安全保障能力提供的一种尺度。

（3）评估保障级和组合保障包的保障组件集合——为不同评估保障级和组合保障包尺度预定义的一组安全保障组件集合。

（4）PP/ST/TOE/ACO 评估方法——评估 PP、ST、TOE 和组合保障包（ACO）以及 TOE 开发者和评估者活动及其工作单元。

通过第三方机构对 TOE 进行测试和评估是一种经典的提供 IT 产品安全保障的有效手段，并且也是 CC 提出前各个国家、区域等 IT 产品安全评估准则文档的基础。为了与这些业界公认的 IT 产品安全保障方法保持一致，CC 采用了相同的理念，建议由专业的评估机构以递增 TOE 评估范围、评估深度和评估过程的严格程度这种方式来度量 PP、ST、组合保障包（ACO）和对应 IT 产品安全功能实现（TOE）的有效性和可信度。CC 测试实验室采用的 TOE 安全评估技术包括但不限于以下这些。

（1）分析并检查 TOE 开发者定义的开发过程和程序。

（2）检查 TOE 开发过程和程序是否正在被使用。

（3）分析 TOE 各设计表示之间的一致性。

（4）对照 TOE 安全架构，分析 TOE 的设计表示。

（5）验证 TOE 开发者提供的各种评估证据。

（6）分析 TOE 的各种指导性文档。

（7）分析 TOE 开发者的功能测试和所提供的测试数据。

（8）评估者独立地对 TOE 功能进行测试和分析。

（9）评估者对 TOE 进行脆弱性分析。

（10）评估者对 TOE 进行穿透性测试等。

CC 不排斥也不评论其他获得 TOE 安全保障方法的相关优点。安全保障可从诸如未经证实的声明、评估者先前相关经验或者特定经验等相关文档中导出。然而，CEM 建议通过主动调查来提供安全保障。主动调查就是以确定 TOE 安全功能（即 ST）为目的，对 IT 产品按照通用评估准则的方法进行安全评估。

CC 基本原则确信，更高的安全保障级别源于 TOE 开发者和评估者更多的开发和评估努力，其目的是运用最小的花销来获得必要的安全保障级。努力程度的增长基于以下几点。

（1）评估范围——努力越多表明该 IT 产品被纳入了评估范围的部分越多。

（2）评估深度——努力越多表明对该 IT 产品的设计和实现细节评估得越细。

（3）严格程度——努力越多表明对该 IT 产品的评估采用了越具结构性和形式化的方法。

3.2.1　保障组件结构

与 CC 第 2 部分结构一样，CC 第 3 部分将安全保障要求中最抽象的集合称作类。每一类包含多个保障族，每一族又包含多个保障组件，每一组件同样又包含多个保障元素。CC 第 3 部分按照安全保障类、族、组件和元素的层次结构来组织安全保障组件（如图 3.6 所示）。

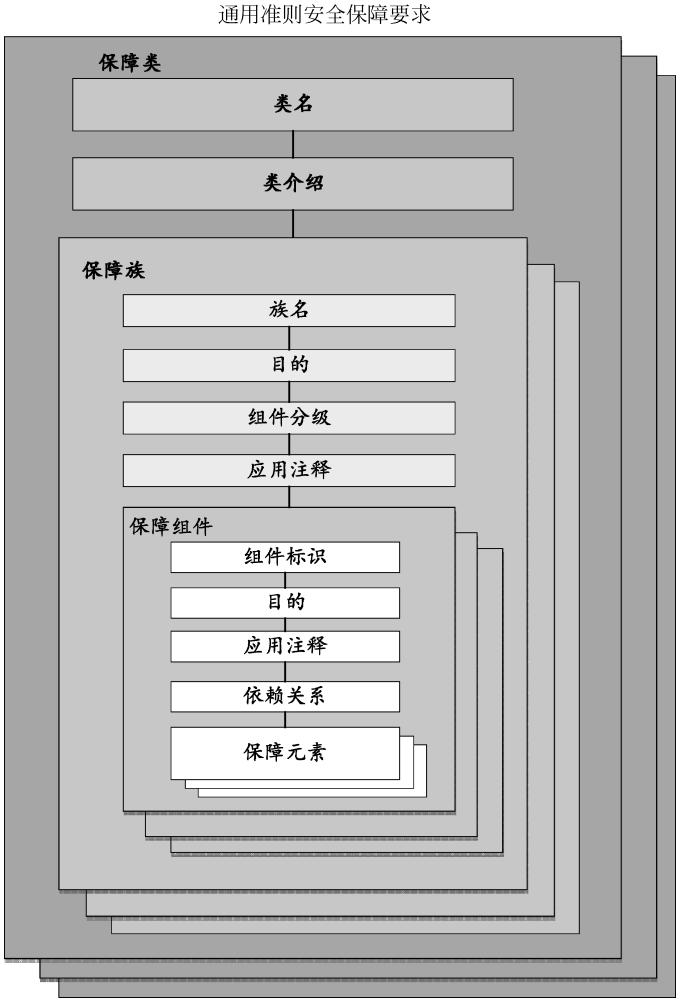

图 3.6　保障类、族、组件、元素的层次结构

安全保障类和族用于对保障要求进行分类，而组件用来详细定义 PP/ST 中的安全保障要求，例如对 TOE 开发过程的严格程度约束以及要求查找并分析潜在安全脆弱性的影响。每个保障要求组件包含开发者行为、产生的证据以及评估者行为 3 方面的元素。

每个保障类都被指定了一个长名和一个以“A”开头的助记的 3 个字母的短名。每个保障类有一段介绍，描述保障类的组成，并且包含涉及该类意图的支持性文字。CC 第 3 部分定义了 3 个类型的安全保障类：用于 PP/ST 验证的；用于 TOE 安全评估的和用于组合 TOE 安全评估的。

CC 第 3 部分共列出了 PP/ST 评估这 2 个保障类和 TOE 以及组合 TOE 的 6 个评估保障类、38 个族和 89 个安全保障组件。PP 评估(APE)和 ST 评估(ASE)这两个类是分别来评估 PP 和 ST 的，其他 6 个评估保障类是验证一个 TOE 或组合 TOE 是否符合其 PP/ST。表 3.13 按照字母序列出了 CC 第 3 部分所有 8 个安全保障类并给出了它们的安全目的。

表 3.13 安全保障类

短 名	长 名	应用类型	安全目的
ACO	组合	TOE	提供确信一个组合 TOE 依靠过去评估过的软件、固件或硬件等组成部分所提供的安全功能是能够安全运行的信心
APE	PP 评估	PP/ST	证实 PP 是完整的、内部一致的和技术合理的
ASE	ST 评估	PP/ST	证实 ST 是完整的、内部一致的和技术合理的，且适合作为 TOE 评估的基础
ADV	开发	TOE	提供 TOE 在不同级别和不同抽象形式上组织和表示 TOE 安全功能的相关信息。从这些信息中所获得的知识可作为执行 TOE 脆弱性分析和测试的基础
AGD	指导性文档	TOE	确保 TOE 使用和所有安全操作都在用户和管理指南指导性文档中描述
ALC	生命周期支持	TOE	确保 TOE 在开发和维护期间，建立规则和对 TOE 的细化过程进行控制，以确保 TOE 的完整性
ATE	测试	TOE	确保有足够的测试覆盖率、测试深度，以及独立的功能测试
AVA	脆弱性评定	TOE	处理在 TOE 开发或者运行过程中引入可被利用脆弱性的可能性

CC 第 3 部分保障类之间是并列关系，它们之间没有层次关系。和功能类一样，保障类也是 CC 用户开始依照 TOE 安全目的选择安全保障要求的最高层次实体，类下面是保障族。保障族表示方法与前面介绍的安全功能族一样，短名是所在保障类名的缩写后紧跟着一个下画线，然后再加上与保障族名有关的 3 个字母，长名提供了与保障族所涵盖主题相关的描述性信息。每个保障族归属于一个保障类，这个保障类包括具有相同意图的多个保障族。每个保障族被分配了一个唯一的族名，这是引用该保障族的主要方式。

保障族的安全目的内容描述了该保障族在 TOE 中能满足的安全目的。保障族的这部分安全目的描述是通用性概述，TOE 安全目的的细节都包含在特定的保障组件安全目的描述中。

保障组件是由若干元素组成的特殊安全要求集合。图 3.7 展示了保障组件的结构。组件标识提供了识别、分类、注册和引用某一组件所必要的描述信息。每个保障组件被分配了一个唯一的组件名。该组件名提供关于该保障组件所涵盖主题的描述性信息。每个保障组

件均被放置在与其具有相同安全目的的保障族之内。CC 也提供了保障组件名字的一个唯一缩写形式，这是引用保障组件的主要手段，其形式是保障族名缩写，后面加一个点，然后是一个数字。这个数字是根据保障组件在族内的顺序从 1 开始编号的。组件之间的层次关系通过这些序号被指定。此外，应用注释可能包含表达保障组件附加的背景信息和详情。

元素是保障组件中一个独立的安全要求，它是可被评估的最底层安全要求。如果再进一步细分的话，将不会产生有意义的评估结果。每个组件被逐个地声明了一个或多个元素。如果一个组件具有多个元素，那么每个组件的所有这些元素都必须在 PP/ST 中被全部使用。保障组件中保障元素分为以下 3 组。

(1) **开发者行为元素**：由 TOE 开发者实施的行为。这组行为靠随后的一组元素中所引用的证据材料来进一步限制。开发者行为要求用元素号后附加一个字母 D 来标识。

(2) **证据的内容和形式元素**：安全评估所需证据，包括应证实的内容和证据应表达哪些信息。证据的内容和形式要求用元素号后附加字母 C 来标识。

(3) **评估者行为元素**：由评估者实施的行为。这组行为明确包含确认在“证据的内容和形式”元素中规定的要求是否都已满足，也包含 TOE 开发者除已完成的动作之外还需实施的行为和分析要求。隐藏的 TOE 评估者行为作为 IT 产品开发者行为元素的结果，虽然没有被“证据的内容和形式”元素覆盖，也应当在 TOE 评估中被执行。评估者行为要求用元素号后附加字母 E 来标识。

“开发者行为”和“证据的内容和形式”元素定义的一组保障要求是用来表示 TOE 开发者的职责，以便于论证 TOE 满足 PP/ST 中安全功能要求的保障级别。

“评估者行为”从评估的两个方面定义评估者的职责。一方面是依据 APE 类和 ASE 类对 PP/ST 进行验证；另一方面是验证 TOE 样品与其 ST 中描述的功能要求和保障要求的符合性。通过证实 PP/ST 文档是有效的，并且 TOE 样品满足 ST 中的这些要求，TOE 用户可以确信 TOE 在未来运行环境中能够解决 PP/ST 已定义的安全问题。

开发者行为元素、证据的内容和形式元素以及显式的评估者行为元素，确定了在验证 TOE 的 ST 所作安全声明时 TOE 评估者在 IT 产品评估工作中应花费的精力。

图 3.8 描述了保障类、族、组件和元素的标准记法。

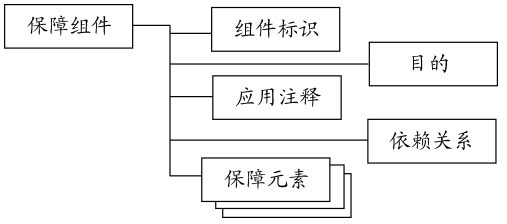

图 3.7　保障组件结构

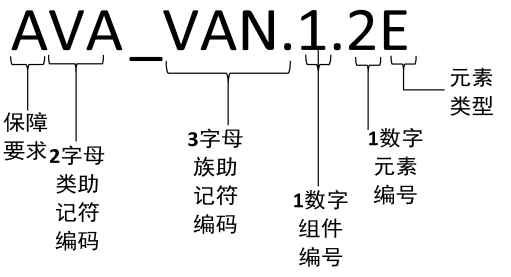

图 3.8　保障类、族、组件和元素的标准记法

3.2.2　PP 评估保障组件

PP 评估(APE)要求证实 PP 是技术合理和内部一致的，并且，如果 PP 是基于一个或多

个 PP 或者包，那么 PP 必须是这些 PP 或包的一个正确的实例化。PP 适于作为编写 ST 或其他 PP 的基础，上述这些评估要求是必需的。如果评估成功，PP 是被认证的并且会注册到国际评估机构管理的 PP 注册列表中。CC 第 3 部分给出的 PP 评估保障组件是为 PP 文档的相关章节内容评估而建立的（如表 3.14 所示）。

表 3.14 APE 保障类：PP 评估

族 标 识	族 名 称	功 能 描 述	包 含 组 件	组 件 名 称
APE_INT	PP 引言	证实 PP 已被正确标识，并且 PP 参考和 TOE 概述是相互一致的	APE_INT.1	PP 引言
APE_CCL	符合性声明	证实声明 ST 和其他 PP 是与本 PP 符合的	APE_CCL.1	符合性声明
APE_SPD	安全问题定义	证实 TOE 及其运行环境所负责处理的安全问题已明确定义	APE_SPD.1	安全问题定义
APE_OBJ	安全目的	证实安全目的充分而且完备地处理了安全问题，并证实 TOE 及其运行环境的安全问题已准确地区分和定义	APE_OBJ.1	运行环境安全目的
			APE_OBJ.2	安全目的
APE_ECD	扩展组件定义	确定 TOE 的扩展组件定义是准确的、没有歧义的并且是必要的	APE_ECD.1	扩展组件定义
APE_REQ	安全要求	确保对 TOE 获得保障而采取的预期活动进行了清晰、无歧义且规范的描述	APE_REQ.1	陈述的安全要求
			APE_REQ.2	推导出的安全要求

（1）APE_INT：PP 标识信息是否是对 PP 的准确反映？TOE 描述是否是连贯的、内部一致的以及与 PP 提示是否一致？

（2）APE_CCL：是否指出本 PP 对应的 CC 版本？是否给出了 ST 和其他 PP 与本 PP 符合的声明？

（3）APE_SPD：TOE 安全问题定义在被操作的安全环境下是否被合理理解？

（4）APE_OBJ：TOE 的安全目的和运行环境安全目的是否能充分对抗已识别威胁、覆盖组织安全策略和安全假设？

（5）APE_ECD：为 PP 描述的 TOE 特定安全要求定义的扩展组件是否准确、没有歧义并且是必要的？

（6）APE_REQ：TOE 安全要求是否内部一致？它们是否会导致 TOE 开发符合声明的安全目的？安全要求是否是显式声明的、清楚的和无歧义的？

3.2.3 ST 评估保障组件

ST 评估（ASE）要求证实 ST 是合理和内在一致的，如果 ST 是基于一个或多个 PP 或者包，那么 ST 必须是 PP 或包的一个正确的实例化。ST 作为 TOE 评估的基础，上述这些属性是必需的。一个 ST 可在 TOE 实现之前或与 TOE 开发并行地被交付评估。但是，如果 ST 的正式评估先于 TOE 开发，这将在成本和进度角度更有意义；例如，错误和 ST 的理解误区会先于 TOE 开发而被纠正。CC 第 3 部分给出的 ST 评估保障组件是为 ST 文档的相关章节内容建立的（如表 3.15 所示）。

表 3.15　ASE 保障类：ST 评估

族　标　识	族　名　称	功 能 描 述	包 含 组 件	组 件 名 称
ASE_INT	ST 引言	证实 ST 和 TOE 被正确标识，TOE 的三层抽象方式描述正确，并且这三方面的描述相互一致	ASE_INT.1	ST 引言
ASE_CCL	符合性声明	证实声明 ST 和 PP 是符合的	ASE_CCL.1	符合性声明
ASE_SPD	安全问题定义	证实 TOE 及其运行环境所负责处理的安全问题已准确地定义	ASE_SPD.1	安全问题定义
ASE_OBJ	安全目的	证实安全目的充分而且完备地处理了定义的安全问题，并证实 TOE 及其运行环境的安全问题已准确地区分和定义	ASE_OBJ.1	运行环境安全目的
			ASE_OBJ.2	安全目的
ASE_ECD	扩展组件定义	证实 TOE 扩展组件定义是准确的、没有歧义的并且是必要的	ASE_ECD.1	扩展组件定义
ASE_REQ	安全要求	证实 TOE 安全要求是清晰的、无歧义的并且是准确定义的	ASE_REQ.1	陈述的安全要求
			ASE_REQ.2	推导出的安全要求
ASE_TSS	TOE 概要规范	证实 TOE 概要规范和 ST 中 TOE 的其他叙述性描述是一致的	ASE_TSS.1	TOE 概要规范
			ASE_TSS.2	具有结构设计概述的 TOE 概要规范

(1) ASE_INT：标识信息是否是 ST 的精确反映？TOE 描述是否是连贯的、内部一致的以及与 ST 提示一致？

(2) ASE_CCL：是否指出本 ST 对应的 CC 版本？ST 是否是指定 PP 的一个正确实例化？是否给出了 TOE 是与本 ST 符合的声明？

(3) ASE_SPD：TOE 安全问题定义在被操作在的安全环境下是否被理解？

(4) ASE_OBJ：TOE 及运行环境的安全目的是否充分对抗已识别威胁、覆盖组织安全策略和安全假设？

(5) ASE_ECD：为 ST 描述的 TOE 特定安全要求定义的扩展组件是否准确、没有歧义并且是必要的？

(6) ASE_REQ：安全要求是否内部一致？它们会导致 TOE 开发满足已声明的安全目的吗？这些安全要求是否是显式声明的、清晰的和无歧义的？

(7) ASE_TSS：是否所有的 SFR 都被 TOE 安全功能满足？是否所有的 SAR 都被 TOE 安全保障措施满足？

3.2.4　TOE 评估保障组件

CC 第 3 部分将 TOE 评估保障组件分为 5 类，分别是开发类(ADV)、指导性文档类(AGD)、生命周期支持类(ALC)、测试类(ATE)和脆弱性评定类(AVA)。

1. 开发类保障组件

开发类保障组件提供了 TOE 开发过程安全保障相关的要求信息。正如后面的 TOE 脆弱性评定(AVA)和 TOE 测试(ATE)类所描述的那样，从开发类中所获得的 TOE 开发

知识可作为执行 TOE 脆弱性评定和 TOE 测试的基础。CC 为开发类定义了 6 个保障族，这些族在不同安全保障级别和不同抽象层次上组织和表示 TOE 安全功能保障要求。这 6 个开发族分为以下 4 类安全要求。

(1) 安全功能要求设计和实现在不同抽象层次下的描述要求(ADV_FSP、ADV_TDS、ADV_IMP)。

(2) 域分离、TSF 自保护和安全功能的不可旁路性等面向安全架构特征的描述要求(ADV_ARC)。

(3) 安全策略模型以及安全策略模型和 TOE 功能规范之间的对应性映射要求(ADV_SPM)。

(4) TSF 内部结构的要求，包括诸如模块化、层次化以及复杂度最小化等要求方面(ADV_INT)。

表 3.16 列出了 ADV 类涉及的保障族及其保障组件。CC 第 3 部分规定 TOE 开发者可用 3 种类型方式来描述他们的 TOE 开发文档：非形式化、半形式化和形式化。TOE 功能规范和 TOE 设计文档一般以非形式化或者半形式化方式进行描述。半形式化方式描述的文档与非形式化文档相比能降低文档的歧义性。除半形式化的描述之外，高保障级别的 TOE 开发类文档一般需要使用形式化方式对其进行描述。当然 TOE 开发者也可综合使用上述 3 种方式对 TOE 安全功能进行描述，以完全准确地描述 TSF 开发的安全保障要求。

表 3.16 ADV 保障类：开发

族 标 识	族 名 称	功 能 描 述	包 含 组 件	组 件 名 称
ADV_ARC	安全架构	提供对 TSF 安全架构的描述，并且提供这些描述 TSF 特性的证据	ADV_ARC.1	安全架构描述
ADV_FSP	功能规范	功能规范是用户可见接口和 TSF 行为的一个高层描述。它描述 TSF，并且一定是 TOE 安全功能要求的一个完备和正确的实例化。功能规范也详细描述 TOE 的外部接口(TSFI)。TSFI 包括所有的通过外部实体(或者位于 TSF 之外 TOE 内部的主体)向 TSF 提供数据、接收来自 TSF 的数据并且调用 TSF 的服务的方法	ADV_FSP.1	基本功能规范
			ADV_FSP.2	安全执行功能规范
			ADV_FSP.3	带完整摘要的功能规范
			ADV_FSP.4	完备的功能规范
			ADV_FSP.5	附加错误信息的完备的半形式化功能规范
			ADV_FSP.6	附加形式化描述的完备的半形式化功能规范
ADV_IMP	实现表示	TSF 的最低抽象表示，它根据可用的源代码、硬件图纸等，论述 TSF 详细的内部工作方式	ADV_IMP.1	TSF 实现表示
			ADV_IMP.2	TSF 实现表示完全映射
ADV_INT	TSF 内部	负责处理 TSF 的内部结构，提出了有关模块化、层次化(抽象性分层和最少循环依赖)、策略实施机制的复杂性最小化、TSF 中非 TSP-实施功能性的数目最小化等方面的要求	ADV_INT.1	结构合理的 TSF 内部子集
			ADV_INT.2	内部结构合理
			ADV_INT.3	内部复杂度最小化

续表

族　标　识	族　名　称	功 能 描 述	包 含 组 件	组 件 名 称
ADV_SPM	安全策略模型	建立一个形式化的 TSF 安全策略模型，以及功能规范与安全策略模型之间的对应关系来提供额外的保障	ADV_SPM.1	形式化 TOE 安全策略模型
ADV_TDS	TOE 设计	提供与 TSF 描述的上下文，以及对 TSF 的详尽描述，以便确定是否实现了安全功能要求。设计文档的目的是为确定 TSF 边界以及描述 TSF 如何实现安全功能要求提供充足的信息	ADV_TDS.1	基础设计
			ADV_TDS.2	结构化设计
			ADV_TDS.3	基础模块设计
			ADV_TDS.4	半形式化模块设计
			ADV_TDS.5	完全半形式化模块设计
			ADV_TDS.6	带形式化高层设计表示的完全半形式化模块设计

2. 指导性文档类

指导性文档(AGD)类为 TOE 所有用户角色规范的指南文档要求(见表 3.17)。为了安全地准备(安装配置)和操作(运营管控)被评估的 IT 产品，TOE 开发者有必要描述 TOE 操作安全相关的所有操作指南内容。这个类同时也描述了 TOE 用户无意错误配置和错误操作 TOE 等安全问题的解决方案等内容。指导性文档类细分为两个族，分别是关于准备程序用户指南(使交付的 TOE 达到与 ST 中描述的一致的运行环境评估配置状态)和操作用户指南(在 TOE 处于评估配置状态下的操作)。

表 3.17　AGD 保障类：指导性文档

族　标　识	族　名　称	功 能 描 述	包 含 组 件	组 件 名 称
AGD_OPE	操作用户指南	描述 TSF 所提供的安全功能，提供说明和指南(包括警告)，以帮助理解 TSF 及其安全使用所必需的关键信息和动作	AGD_OPE.1	操作用户指南
AGD_PRE	准备程序	用于保证 TOE 以开发者预期的安全方式被接收和安装	AGD_PRE.1	准备程序

3. 生命周期支持类

生命周期支持类是由 TOE 开发者负责或者用户负责来区分 IT 产品生命周期阶段，而不是按照 TOE 所处的开发环境或用户环境区分的。将 TOE 移交给用户的时间点，也就是从 ALC(“生命周期支持”类)到 AGD(“指导性文档”类)的时间点。ALC 类由 7 个族组成(如表 3.18 所示)。生命周期定义(ALC_LCD)族是 TOE 生命周期的高级描述，CM 能力(ALC_CMC)族要求对 TOE 配置项的管理进行详细描述，CM 范围(ALC_CMS)族要求以定义的方式管理一个最小的配置项集合。开发安全(ALC_DVS)族与 TOE 开发者物理的、

程序的、人员的以及其他的安全控制措施有关，工具和技术（ALC_TAT）族关于 TOE 开发者使用的开发工具和实现技术与机制，缺陷纠正（ALC_FLR）族负责 TOE 安全缺陷的处理。交付（ALC_DEL）族定义将 TOE 从 TOE 开发环境移交给 TOE 消费者使用环境的过程程序。注意在 TOE 开发过程中产生的交付过程不是由 ALC_DEL 处理，应该由本类其他族中定义的模块集成和接受程序来处理。

表 3.18 ALC 保障类：生命周期支持

族标识	族名称	功能描述	包含组件	组件名称
ALC_CMC	CM 能力	要求在 TOE 和相关信息的细化和修改过程中遵守一定的规章制度和采取一定的控制措施	ALC_CMC.1	TOE 标识
			ALC_CMC.2	CM 系统的使用
			ALC_CMC.3	授权控制
			ALC_CMC.4	生产支持和接受程序及其自动化
			ALC_CMC.5	高级支持
ALC_CMS	CM 范围	标识出纳入配置管理系统的配置项，并满足 ALC_CMC“CM 能力”族提出的 CM 要求	ALC_CMS.1	TOE CM 覆盖
			ALC_CMS.2	部分 TOE CM 覆盖
			ALC_CMS.3	实现表示 CM 覆盖
			ALC_CMS.4	问题跟踪 CM 覆盖
			ALC_CMS.5	开发工具 CM 覆盖
ALC_DEL	交付	阻止和检测在 TOE 交付过程中不恰当地对 TOE 进行修改	ALC_DEL.1	交付程序
ALC_DVS	开发安全	减少开发过程中潜在的物理、程序、人员以及其他对 TOE 的安全威胁	ALC_DVS.1	安全控制措施标识
			ALC_DVS.2	充分的安全控制措施
ALC_FLR	缺陷纠正	确保开发者跟踪并纠正已发现的安全缺陷	ALC_FLR.1	基本的缺陷纠正
			ALC_FLR.2	缺陷报告程序
			ALC_FLR.3	系统的缺陷纠正
ALC_LCD	生命周期定义	评估开发使用的生命周期模型的适当性、标准化和可测性	ALC_LCD.1	开发者定义的生命周期模型
			ALC_LCD.2	可测量的生命周期模型
ALC_TAT	工具和技术	评价用于开发、分析和实现 TOE 安全功能工具和技术的适当性	ALC_TAT.1	明确定义的开发工具
			ALC_TAT.2	遵从实现标准
			ALC_TAT.3	遵从实现标准（所有部分）

生命周期支持类是评估 TOE 开发者用来预防和探测被意外的或蓄意的安全漏洞利用的 IT 产品生命周期过程的有效性。以下 4 个关键领域应被检查与检验。

（1）生命周期过程是否降低了开发环境中的物理的、过程的和人员安全威胁的风险？

（2）TOE 漏洞修复过程是否有效？

（3）生命周期模型是否是良好定义的、适当的以及可度量的？生命周期模型是否在 TOE 开发过程中确实被遵循？

（4）用于开发、分析和实现 TOE 安全功能的工具和技术是否恰当？

4. 测试类

测试类包括 4 个“测试”相关的保障族(如表 3.19 所示)：覆盖(ATE_COV)、深度(ATE_DPT)、独立测试(例如由评估者执行的功能测试)(ATE_IND)和功能测试(ATE_FUN)。对 TOE 进行各种测试能为 TSF 是否符合前面开发类所述功能规范、TOE 设计及实现描述等提供保障。评估 TOE 测试覆盖率的充分性(如测试计划、测试过程和测试分析报告记录)是为了确定 TOE 安全功能是否已经被 TOE 开发者充分测试过，这是通过检查 TOE 开发者的相关测试证据来实现的。由 TOE 开发者执行的测试深度分析用于检验开发者做的测试所能达到的详细程度，目的是降低在 TOE 开发中存在某些错误的风险。由开发者执行的功能测试范围被分析以确认其充分性。另外，评估者可能要自主执行独立的功能测试。ATE 将测试分为开发者测试和评估者测试。覆盖分析(ATE_COV)和深度测试(ATE_DPT)族涉及 TOE 开发者的所有测试数据及其相关的证据材料，前者说明功能规范已被严格测试，后者说明针对其他设计描述(安全结构、TOE 设计、实现说明)的测试是否被满足。

表 3.19　ATE 保障类：测试

族　标　识	族　名　称	功 能 描 述	包 含 组 件	组 件 名 称
ATE_COV	覆盖	通过检查开发者的对应性证据确定测试覆盖充分性	ATE_COV.1	覆盖证据
			ATE_COV.2	覆盖分析
			ATE_COV.3	严格覆盖分析
ATE_DPT	深度	通过检查开发者的对应性证据确定测试深度覆盖充分性	ATE_DPT.1	测试：基本设计
			ATE_DPT.2	测试：安全执行模块
			ATE_DPT.3	测试：模块设计
			ATE_DPT.4	测试：实现表示
ATE_FUN	功能测试	确定由开发人员实施的功能测试的充分性	ATE_FUN.1	功能测试
			ATE_FUN.2	顺序的功能测试
ATE_IND	独立测试	确定由评估人员实施的功能测试的充分性	ATE_IND.1	独立测试(符合性)
			ATE_IND.2	独立测试(抽样)
			ATE_IND.3	独立测试(完全)

注意，本类不涉及评估 TOE 安全性的穿透性测试，穿透性测试是基于对 TSF 的分析专门查找并标识 TSF 设计与实现过程中的脆弱性，在 AVA“脆弱性评定”类中将作为脆弱性评估的一个方面单独处理。

5. 脆弱性评定类

脆弱性评定类负责评估在 TOE 开发或者运行过程中引入可被利用的脆弱性的可能性(脆弱性利用)。通常，脆弱性评定活动涉及 TOE 开发和运行中的各种潜在的安全攻击。脆弱性利用的是在开发过程中引入的 TOE 的一些属性，例如通过篡改、直接攻击或绕过 TSF 等攻破 TSF 自我保护，或者通过绕过、直接攻击 TSF 等攻破 TSF 域分隔，或者通过绕过(旁路)TSF 攻破不可旁路性。通过非技术措施中的脆弱性的利用去破坏 TOE 安全功能要求，例如误用或错误配置。“误用”考察的是在 TOE 的管理员或用户被认为是安全时，TOE 是否会以一种不安全的方式被配置或使用。脆弱性评估是由表 3.20 中的脆弱性评定保障族 AVA_VAN 相关的保障组件来处理的。

表 3.20 AVA 保障类：脆弱性评定

族 标 识	族 名 称	功 能 描 述	包 含 组 件	组 件 名 称
AVA_VAN	脆弱性分析	确定在评估 TOE 开发和预期运行期间潜在的脆弱性是否已被标识	AVA_VAN.1	脆弱性调查
			AVA_VAN.2	脆弱性分析
			AVA_VAN.3	关注点脆弱性分析
			AVA_VAN.4	系统的脆弱性分析
			AVA_VAN.5	高级的系统的脆弱性分析

3.2.5 ACO 评估保障组件

组合 TOE 的一个依赖部件可用一个先前已评估或认证过的基本部件来满足环境中的 IT 产品安全要求，但这种方式不提供任何关于部件之间的交互或组合是否会引入脆弱性的保障。组合 TOE 评估保障组件（ACO）在更高的保障级别中考虑了这些交互，将部件之间的接口纳入了测试范围。同时，通过对组合 TOE 进行脆弱性分析来考虑部件组合引入脆弱性的问题。

ACO 类的“组合”为 TOE 集成者提供了一种可选的方法被用于 CC 中由两个或更多的成功评估过的 TOE 合成的组合 TOE 评估过程中获得信心，而不需要重新评估合成的 TSF。（在整个 ACO 类中用组合 TOE 集成者指代“开发者”，任何与基本或依赖部件相关的开发者都这样阐述。）

ACO“组合”类包括表 3.21 所示的 5 个族。它们是为了提供确信一个组合 TOE 依靠过去评估过的软件、固件或硬件等组成部分所提供的安全功能是能够安全运行的信心。

表 3.21 ACO 保障类：组合

族 标 识	族 名 称	功 能 描 述	包 含 组 件	组 件 名 称
ACO_COR	组合基本原理	证实基本部件能为组合产品提供有效合适的保障级	ACO_COR.1	组合基本原理
ACO_DEV	开发证据	确认提供安全功能支持依赖部件是合适的，且是相关要求所必需的（依赖信息中表示的）	ACO_DEV.1	功能描述
			ACO_DEV.2	基本的设计证据
			ACO_DEV.3	详细的设计证据
ACO_REL	依赖部件的依赖性	提供描述依赖基本部件的依赖性证据	ACO_REL.1	基本的依赖信息
			ACO_REL.2	依赖信息
ACO_CTT	组合 TOE 测试	要求执行组合 TOE 测试以及组合 TOE 中用到的基本部件测试	ACO_CTT.1	接口测试
			ACO_CTT.2	严格的接口测试
ACO_VUL	组合脆弱性分析	开发者应提供部件评估期间报告的任何残余脆弱性的详细资料	ACO_VUL.1	组合脆弱性审查
			ACO_VUL.2	组合脆弱性分析
			ACO_VUL.3	增强的基本组合脆弱性分析

3.2.6 PP 配置评估保障组件

为了适应当前日益复杂的 IT 产品设计趋势，当前版本的 CC/CEM 标准修订过程加入了对模块化（Modularization）产品安全功能描述和评估技术的支持：在 2017 年发行的 CC

v3.1 r5 版本中扩展了评估模型，提出了 PP 模块(PP Module)、基本 PP(Base PP)和 PP 配置(PP Configuration)等概念，并增加了相应的安全保障要求和评估方法，特别是增加了面向 PP 配置评估的安全保障类(ACE)，用来评估由一个或多个基本 PP 或 PP 模块组成的可配置的 PP。这种支持有利于增强 CC 评估过程中的复用程度，节省评估开销(注：读者可参见本书 4.9 节了解更多内容)。

ACE 要求证实 PP 配置是技术合理和内部一致的。这些特性是未来保证 PP 配置可用于 ST 和其他 PP 或 PP 配置的编制依据。ACE 类评估要求必须结合新版 CC 第 1 部分附录定义的 PP 配置概念及其样例使用。表 3.22 给出了 PP 配置保障族及其保障组件，这些族在不同级别和不同抽象形式上组织和表示 PP 配置评估要求(注：目前颁布的 GB/T 18336 标准由于是针对 CC v3.1 r3 进行的转标处理，其中并没有给出新版 CC 中 PP 配置相关的概念)。

表 3.22　ACE 保障类：PP 配置评估

族 标 识	族 名 称	功 能 描 述	包 含 组 件	组 件 名 称
ACE_INT	PP 配置引言	证实 PP 模块(PP Module)已被正确标识，并且 PP 模块和 TOE 概述是相互一致的	ACE_INT.1	PP 配置引言
ACE_CCL	符合性声明	证实符合性声明有效性。不同于一般 PP，PP 模块不能说明符合其他 PP 或 PP 模块，也不能包括 CC 第 3 部分或保障组件包的符合性	ACE_CCL.1	符合性声明
ACE_SPD	安全问题定义	和 APE_SPD 一样，证实 TOE 及其运行环境所负责处理的安全问题被明确定义	ACE_SPD.1	安全问题定义
ACE_OBJ	安全目的	和 APE_SPD 一样，证实安全目的充分而且完备地处理了安全问题，并证实 TOE 及其运行环境的安全问题被准确地区分和定义	ACE_OBJ.1	安全目的
ACE_ECD	扩展组件定义	确定面向 PP 模块的扩展组件是准确的、没有歧义的并且是必要的	ACE_ECD.1	扩展组件定义
ACE_REQ	安全要求	确保对 TOE 获得保障而采取的预期活动进行了清晰、无歧义且规范的描述	ACE_REQ.1	安全要求

3.2.7　预定义评估保障级别

CC 第 3 部分预定义了 7 个评估保障级(EAL)。每个 EAL 相应的结构如图 3.9 所示，其中“目的”项表示的是评估保障级的安全意图，“应用注释”项包含评估保障级的使用者(如 PP/ST 作者，以该评估保障级为目标的 TOE 设计者、评估者)特别感兴趣的信息，“保障组

件”给出了该保障级别包含的保障组件信息。

PP/ST 作者可以用以下方法，得到一个比 CC 预定义 EAL 更高级别的评估保障级别。

（1）包含来自其他保障族的额外的保障组件。

（2）从相同的保障族中用更高级别的保障组件替换保障组件。

图 3.10 说明了 CC 定义的保障要求和保障级之间的关系。当保障组件进一步分解为保障元素时，保障元素不能被保障级单独引用。需要注意的是，图中的箭头表示评估保障级（EAL）与保障类中组件的引用关系。

在 CC 第 3 部分中对 TOE 的安全保障预定义了如表 3.23 所示的 7 个级别。它们按保障能力进行排序，每个评估保障级比其较低的评估保障级表达了更多的安全保障要求，即高级别的 EAL 靠替换低级别 EAL 同一保障族中的一个更高级别的保障组件（即增加严格性、范围和（或）深度）和添加另外一个保障族的保障组件（即添加新的要求）来实现。

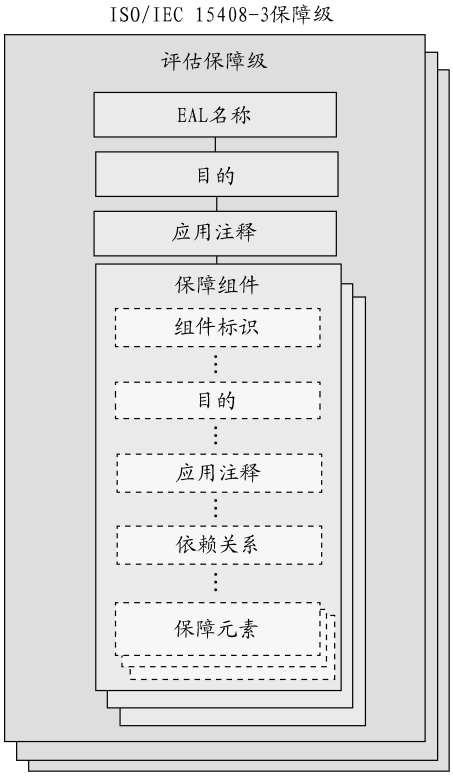

图 3.9 评估保障级结构

表 3.23 CC 预定义 EAL 保障级别描述

预定义 EAL	保障要求描述
EAL 1 功能测试	EAL 1 级依据一个规范的独立性测试和对所提供的指导性文档的检查来为用户评估 TOE。在这个级上，没有 TOE 开发者的帮助也能成功地进行评估，并且所需费用也最少。通过该级的一个评估，可以确信 TOE 的功能与其文档在形式上是一致的，并且对已标识的威胁提供了有效的保护
EAL2 结构测试	EAL 2 级要求评价时在设计信息和测试结果的提供方面得到 TOE 开发人员的配合，要求 TOE 开发者递交设计信息和测试结果。EAL 2 适用于在缺乏现成可用的完整的开发记录时，TOE 开发者或用户需要一种低到中等级别的独立安全保障的安全性
EAL 3 系统测试	EAL 3 级要求在设计阶段实施积极的安全工程思想，提供中级的独立安全保障，EAL 3 可使 TOE 开发者在设计阶段能从正确的安全工程中获得最大限度的安全保障。EAL 3 适用于 TOE 开发者或用户需要一个中等级别的独立安全保障的安全性，并在不带来大量的再构建费用的情况下，对 TOE 及其开发过程进行彻底审查。开展该级的评估，需要分析基于“灰盒子”的测试结果、TOE 开发者测试结果的选择性独立确认、TOE 开发者搜索已知脆弱性的证据等。还要求使用开发环境控制措施、TOE 的配置管理和安全交付程序
EAL 4 系统设计、测试和复查	EAL 4 级要求按照良好的商业化开发惯例实施积极的安全工程思想，提供中高级的独立安全保障。EAL 4 级的评估，需要分析 TOE 模块的安全架构、底层设计和实现的子集。在测试方面将侧重于对已知的脆弱性进行独立搜索。开发控制方面涉及生命周期模型、开发工具标识与自动化配置管理等方面

续表

预定义 EAL	保障要求描述
EAL 5 半形式化设计和测试	EAL 5 级要求按照严格的商业化开发惯例，应用专业安全工程技术实施安全工程思想，提供高等级的独立安全保障。如果某个 TOE 要想达到 EAL5 要求，TOE 开发者需要在设计和开发方面下一定工夫，应具备相关的一些专业技术。开展该级的评估，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，以及它们之间对应性的半形式化论证。对已知脆弱性的搜索方面，必须确保 TOE 可抵御中等攻击潜力的穿透性攻击者。还要求采取隐蔽信道分析和模块化的 TOE 设计
EAL 6 半形式化验证的设计和测试	EAL 6 级通过在严格的开发环境中应用安全工程技术来获取高等级的安全保障，使产品能在高度危险的环境中使用。开展该级的评估，需要分析设计的模块和层次化方法以及实现的结构化表示。在对已知脆弱性的独立搜索方面，必须确保 TOE 可抵御高等攻击潜力的穿透性攻击者。对隐蔽信道的搜索必须是系统性的，且开发环境和配置管理的控制也应进一步增强
EAL 7 形式化验证的设计和测试	EAL 7 级的目标是使产品能在极端危险的环境中使用，目前，该级别的实际应用只限于其安全功能可以进行广泛的形式化分析的安全产品。开展该级的评估，需要分析 TOE 的形式化模型，包括功能规范和高层设计的形式化表示。要求 TOE 开发者提供基于“白盒”测试的证据，在评估时必须对这些测试结果全部进行独立确认，并且设计复杂程度必须是最小的

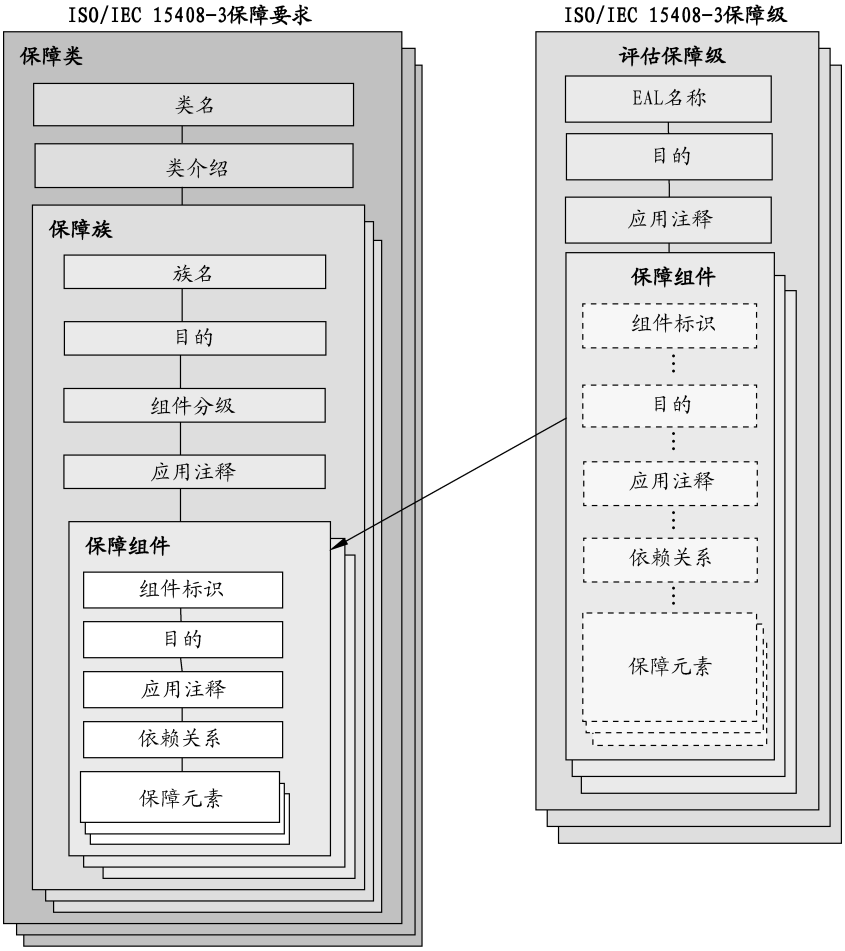

图 3.10　保障要求和保障级别之间的保障组件对应关系

虽然在 CC 中已经预定义这些评估保障级所包括的组件(表 3.24 所示)，但 PP/ST 编制者还是可以依据用其他保障组件的组合来表示某类特殊的安全保障要求。特别是“增强”这个概念允许(从没有包括在评估保障级中的保障族)向评估保障级中增加保障组件，或允许替换评估保障级中的(用同一个保障族的其他更高级别的保障组件)组件。在 CC 中定义的保障结构中，只有评估保障级可以增强。“评估保障级减去一个组成保障组件”这样的想法在 CC 应用中不被认为是一个有效的主张。要求“增强”者有义务证明对评估保障级添加保障组件的实际意义和潜在的价值。一个评估保障级也可以用扩展的保障要求来增强。

表 3.24 评估保障级组件列表

保障类	保障族		评估保障级依据的保障组件						
			EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7
开发	ADV_ARC	安全架构		1	1	1	1	1	1
	ADV_FSP	功能规范	1	2	3	4	5	5	6
	ADV_IMP	实现表示				1	1	2	2
	ADV_INT	TSF 内部					2	3	3
	ADV_SPM	安全策略模型						1	1
	ADV_TDS	TOE 设计		1	2	3	4	5	6
指南类文档	AGD_OPE	操作用户指南	1	1	1	1	1	1	1
	AGD_PRE	准备程序	1	1	1	1	1	1	1
生命周期支持	ALC_CMC	CM 能力	1	2	3	4	4	5	5
	ALC_CMS	CM 范围	1	2	3	4	5	5	5
	ALC_DEL	交付		1	1	1	1	1	1
	ALC_DVS	开发安全			1	1	1	2	2
	ALC_FLR	缺陷纠正							
	ALC_LCD	生命周期定义			1	1	1	1	2
	ALC_TAT	工具和技术				1	2	3	3
ST 评估	ASE_CCL	符合性声明	1	1	1	1	1	1	1
	ASE_ECD	扩展组件定义	1	1	1	1	1	1	1
	ASE_INT	ST 引言	1	1	1	1	1	1	1
	ASE_OBJ	安全目的	1	2	2	2	2	2	2
	ASE_REQ	安全要求	1	2	2	2	2	2	2
	ASE_SPD	安全问题定义		1	1	1	1	1	1
	ASE_TSS	TOE 概要规范	1	1	1	1	1	1	1
测试	ATE_COV	覆盖范围		1	2	2	2	3	3
	ATE_DPT	深度			1	2	3	3	4
	ATE_FUN	功能测试		1	1	1	1	2	2
	ATE_IND	独立测试	1	2	2	2	2	2	3
脆弱性评定	AVN_VAN	脆弱性分析	1	2	2	3	4	5	5

3.2.8 预定义组合保障包

组合 TOE 由已经通过评估(或即将通过评估)的 TOE 部件组成。单个部件将被认证为满足某个 EAL 或在 ST 中说明的其他保障包。通过从公开渠道获取部件的信息进行

EAL 1 评估，一个组合 TOE 预计可达到基本的保障级别（部件和组合 TOE 的评估都可应用 EAL 1）。通过应用高于 EAL 1 的 EAL 可以进行组合 TOE 的更高保障级的评估，而组合保障包（CAP）为此目的提供了另一种解决方法。

CAP 在权衡所获得的保障级与达到该组合 TOE 保障程度所需的代价和可行性上提供了一个递增的尺度。组合保障包是建立在先前已评估的实体（基本部件和依赖部件）之上，因此仅有少部分族和组件被包含在组合保障包中。表 3.25 概括性地描述了 CC 第 3 部分对组合 TOE 的保障等级定义了 3 个组合保障包，表格中的每个数字标识出了此处适宜的具体保障组件。每个 CAP 最多包含每个保障族中的一个组件，并满足每个组件的所有保障依赖关系。

表 3.25　组合保障级别组件列表

保　障　类	保　障　族	组合保障包依赖的保障组件		
		CAP-A	**CAP-B**	**CAP-C**
组合	ACO_COR	1	1	1
	ACO_CTT	1	2	2
	ACO_DEV	1	2	3
	ACO_REL	1	1	2
	ACO_VUL	1	2	3
指导文档	AGD_OPE	1	1	1
	AGD_PRE	1	1	1
生命周期支持	ALC_CMC	1	1	1
	ALC_CMS	2	2	2
ST 评估	ASE_CCL	1	1	1
	ASE_ECD	1	1	1
	ASE_INT	1	1	1
	ASE_OBJ	1	2	2
	ASE_REQ	1	2	2
	ASE_SPD		1	1
	ASE_TSS	1	1	1

组合保障包按级别排序，因为高级别的 CAP 比所有较低的 CAP 表达更多的保障。从 CAP-A 到 CAP-C，保障增加是通过替换成同一保障族中的一个更高级别的保障组件（即增加严格性、范围和/或深度）和添加另外几个保障族的保障组件（即添加新的要求）来实现。这些增加导致更多的综合分析来识别对单个 TOE 获得的评估结果的影响。

3 类组合保障包的目的及其保障内容分别如下。

（1）**结构组合（CAP-A）**：适于组合 TOE 是完整的，且需要对产生组合的正确安全操作具有信心的情况。该组合保障包通过分析组合 TOE 的 ST 提供保障。利用 TOE 组成部件的评估输出（如 ST、指导性文档等）和 TOE 组成部件之间的接口规范对组合 TOE 的 ST 中的安全功能要求进行分析，以理解安全行为。例如以下内容可为该分析提供支持：针对关联信息中描述的依赖部件与基本部件之间的接口进行的独立测试；开发者基于关联信息、开发信息和组合原理进行测试的证据；对开发者测试结果的选择性确认；由评估者进行的组合 TOE 的脆弱性审查等。

（2）**系统组合（CAP-B）**：可使组合 TOE 开发者在子系统层面上通过理解各组成部件之间的相互影响，获得最大程度的保障，同时还可使基本部件开发者的参与量最小。CAP-B 通过全面分析组合 TOE 的 ST 提供保障。利用 TOE 组成部件的评估输出（如 ST、指导性文档等），TOE 组成部件之间的接口规范，以及包含在组合开发过程中的 TOE 设计信息（描述 TSF 系统），对组合 TOE 的 ST 中的安全功能要求进行分析，以理解安全行为。以下内容可为该分析提供支持：对关联信息（包括 TOE 设计）中描述的依赖部件与基本部件之间的接口进行的独立测试、开发者基于关联信息、开发相关信息和组合原理而进行测试的证据，以及对开发者测试结果的选择性独立确认。对评估者为证实组合 TOE 可抵御基本攻击潜力攻击者的攻击而进行的脆弱性分析也可提供支持。

（3）**系统组合、测试和复查（CAP-C）**：可使开发者从对组合 TOE 部件之间交互的正确分析获得最大限度的保障，虽然这种实践很严格，但不需要获得所有的对基本部件的评估证据。CAP-C 通过全面分析组合 TOE 的 ST 提供保障。利用 TOE 组成部件的评估输出（如 ST、指导性文档等），TOE 组成部件之间的接口规范，以及包含在组合开发过程中的 TOE 设计信息（描述 TSF 模块）对组合 TOE 的 ST 中的安全功能要求进行分析，以理解安全行为。以下内容可为该分析提供支持：对关联信息（包括 TOE 设计）中描述的依赖部件与基本部件之间的接口进行的独立测试、开发者基于关联信息、开发相关信息和组合原理而进行测试的证据、对开发者测试结果的选择性独立确认来进行。对评估者为证实组合 TOE 可抵御基本增强理攻击潜力攻击者的攻击而进行的脆弱性分析也可提供支持。

CAP-A 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到中等级别的独立保障的安全性的情况。与 CAP-A 相比，CAP-B 通过要求更完备的安全功能测试，在保障方面提供了有意义的增强。因此 CAP-B 适用于开发者或用户需要一个中等级别的独立保障的安全性，以及在没有对组合 TOE 进行实质性改造的情况下，要求对组合 TOE 及其开发过程进行彻底的调查。

与 CAP-B 相比，CAP-C 通过要求更完备的设计描述和抵御更高的攻击潜力，在保障方面提供了有意义的增强。因此 CAP-C 适用于开发者或用户在传统的商品化 TOE 中需要一个中等到高等级别的独立保障的安全性，并准备负担额外的安全专用工程费用。

自从组合保障包 CAP 提出以来，国内外鲜见实际使用该概念的评估案例。实际上依据 CAP 的评估存在一些基本问题，这妨碍了其被实际应用，主要包括以下基本问题。

（1）CAP 要求组合部件必须都进行过 EAL 评估，这不利于一个组合产品的实际评估状况，其中所有的部件或至少部分部件是没有被评估过的。

（2）采用 CAP 方法进行评估后得到的 CAP 级别无法和 EAL 级别进行比较，因而无法论述一个 CAP 组合评估产品和一个按 EAL 进行整体评估的产品的安全保障程度。

（3）由于前两点，无法对包含 3 个及以上依赖层次的组合产品进行 CAP 评估，因为虽然可以对下两层进行 CAP 评估，但却无法将第三层的 EAL 评估结果和下两层的 CAP 评估结果进行组合评估。

为了改善这种状况，正在编修的 CC v4.0 版本提出了新的组合评估概念，并给出了某些组合模型下的评估方法。在这种评估方法中，一个基础部件需要预先进行 EAL 评估，其上层依赖部件没有经过 EAL 评估，通过在现有的评估保障类中增加特定的保障族（主要包括 ASE_COMP、ADV_COMP、ALC_COMP、ATE_COMP 和 AVA_COMP 等），可以最终

输出一个体现 EAL 级别的组合评估结果，因此这个方法将与基本的 EAL 评估方法一致，并可以支持多于三层的组合产品评估需求。

3.3 本章小结

基于 CC/CEM 的安全评估为客户提供 IT 产品安全行为和安全保障的评估证据，而不是通过安全理论模型和系统仿真方法为 IT 产品客户提供安全功能证明。为此，我们需要使用 CC 定义的安全组件来描述 IT 产品的安全要求。本章重点是介绍用于规范某个 IT 产品安全功能要求表达的 CC 安全功能组件和安全保障组件的内容及其使用方法，即 CC 第 2 部分列出的 11 个类、65 族和 136 个安全功能组件和 CC 第 3 部分列出的 PP/ST 评估这 2 个保障类和 TOE 以及组合 TOE 的 6 个评估保障类、38 个族和 89 个安全保障组件。

CC 第 2 部分定义的功能类描述了标准用户可能需要的各种潜在安全功能组件。当 PP/ST 编制者开始选择安全功能要求时，功能类是选择安全功能组件的出发点。CC 第 2 部分的安全功能类彼此之间是并列关系，并没有层次关系。在 CC 文档中的功能类定义的助记符短名是按照其字母排序的。功能族是用来陈述一组共享安全目的，但是安全关注点或安全精确度上不一样的安全要求。在确定了功能类后，可依据 PP/ST 定义的安全目的，为 TOE 选择相应的功能族。组件是一个安全要求的特殊集合，它是由各种元素构成的。CC 规定组件中的元素是一个不可分割的安全要求，它应可通过一个安全评估被验证。组件被分配了一个长名并且相关的要求在 CC 第 2 部分都被准确地描述了。一个组件和另一个组件之间的层次关系是在功能族中指定的，在此基础上，我们分别介绍了 11 个安全功能类相关的族及其组件。

CC 第 3 部分给出了描述 IT 产品安全保障要求的标准化组件。在 CC 中 TOE 的安全保障级别划分是以保障类为依据的，而保障类由多个保障族组成，每个保障族都有一个保障安全目的，保障族又由一个或多个保障组件组成，每个保障组件也有一个安全目的，表明该组件的安全意图。保障组件又由一组保障元素组成，保障元素分别从 TOE 开发者、评估者和评估证据内容和格式的角度对保障组件所包含的内容和评估依据进行阐述。为便于理解，我们按照评估项目目标对象的不同，分别介绍了保护轮廓评估组件、安全目标评估组件、评估对象保障组件和组合评估对象保障组件，并在最后介绍了 CC 预定义的评估保障级别和组合保障包含义及相应的安全保障组件。

3.4 问题讨论

1. 简述安全功能组件结构、功能类和功能族的主要目的。
2. 安全审计类安全功能组件有哪些？简述它们的用途。
3. 通信功能类安全功能组件有哪些？简述它们的用途。
4. 密码支持类安全功能组件有哪些？简述它们的用途。
5. 用户数据保护类安全功能组件有哪些？简述它们的用途。

6. 用户标识和鉴别类安全功能组件有哪些？简述它们的用途。

7. 安全管理类安全功能组件有哪些？简述它们的用途。

8. 隐私要求类安全功能组件有哪些？简述它们的用途。

9. TSF 保护类安全功能组件有哪些？简述它们的用途。

10. 资源利用类安全功能组件有哪些？简述它们的用途。

11. TOE 访问类安全功能组件有哪些？简述它们的用途。

12. 可信路径/信道类安全功能组件有哪些？简述它们的用途。

13. 以某个操作系统、数据库管理系统或应用系统的访问控制安全功能为例，选择用户数据管理类某个相应的组件，描述该 TOE 的组件元素操作。

14. 以某个操作系统、数据库管理系统或应用系统为例，定义其需要记录的安全相关事件。

15. 以某个操作系统、数据库管理系统或应用系统为例，从 CC 用户鉴别组件列表中选择合适的组件，描述该 TOE 的组件元素操作。

16. 简述 TSF 间可信信道和可信路径的区别，并通过案例说明。

17. 简述安全保障要求组件结构、功能类和功能族的主要目的。

18. 简述安全保障评估努力有哪些要素。

19. 阐述功能和保障类、族和元素的标准记法。注意相似性和不同，如果存在的话。

20. CC 给出预定义评估保障级别的目的是什么？为何要定义组合保障包？

21. 保障组件元素分 3 类，简述它们各自的通途。

22. PP 保障组件有哪些？简述它们的用途。

23. ST 保障组件有哪些？简述它们的用途。

24. 开发类保障组件有哪些？简述它们的用途。

25. 指导文档类保障组件有哪些？简述它们的用途。

26. 生命周期类保障组件有哪些？简述它们的用途。

27. 测试类保障组件有哪些？简述它们的用途。

28. 脆弱性评定类保障组件有哪些？简述它们的用途。

29. 组合 TOE 保障组件有哪些？简述它们的用途。