附件5：

认证认可行业标准草案编制说明

（参考格式）

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **1、基本信息** | | | | | |
| 1.1 标准草案名称 | 中文 | 实时数据库系统安全评价要求 | | | |
| 英文 | Security techniques requirement for Real Time Database | | | |
| 1.2 与国际标准和国外先进标准一致性程度情况 | □等同采用  □修改采用  □非等效采用  ■未采用 | 标准编号 |  | | |
| 英文名称 |  | | |
| 中文名称 |  | | |
| 1.3 任务来源 | 批准立项的文件名称和文件号 |  | | 计划编号 | 2016RB046 |
| 1.4制（修）订 | ■制定 □修订（被修订标准名称及编号： ） | | | | |
| 1.5 起止时间 | 2016年 7 月--- 2016 年12月 | | | | |
| 1.6 标准起草单位 | 中国信息安全认证中心 | | | | |
| 1.7 起草团队 | 兰丹妮、布宁、霍珊珊、刘健、董晶晶、毕强、吴迪、刘思蓉、张怡、贾雪飞、 | | | | |
| 1.8 标准体系表内编号 | 2016RB046 | | | | |
| 1.9调整情况 | 无 | | | | |

|  |  |
| --- | --- |
| **2、背景情况** | |
| 2.1 目的、意义  （工作开展背景及要求） | **1、研究意义**  实时数据库系统是一种采集、存储和分析随时间快速变化的海量数据的软件产品，适用于处理不断更新的快速变化的数据及具有时间限制的事务处理，是数据库系统发展的一个重要分支，是现代工业系统中生产信息化的核心基础软件。  随着信息化建设的加速发展，实时数据库系统已经被广泛应用于电力、钢铁、石油、化工等工业系统中，用于采集和存储工业生产过程中产生的大量随时间变化的实时数据。实时数据库系统既为企业保留了极为重要的历史数据，也为企业提供了及时和有效的实时信息，已成为工业信息系统中数据的“生产中心”，在对历史数据和实时数据分析的基础上，可以对工业生产实时监控及管理，在整个工业信息系统建设中起着关键作用。  **2、已有工作基础**  中国信息安全认证中心于2011年8月开始对IT产品实施信息安全认证。依据GB/T 18336-2015（等同转化ISO/IEC 15408:2008，对应CC V3.1）和相关安全技术要求，对IT产品的安全性进行评价，旨在保护用户信息安全，维护用户利益。生产企业的IT产品获得信息安全认证证书，表明该产品符合相应的标准和技术要求。  由目前国内外尚无统一的实时数据库安全技术相关标准，在数据接口、数据存储和使用上有一些应用规范，在某些行业出现过实时数据库系统的测试规范，如在电力行业发布的（DRZ/T 02-2004）《火力发电厂厂级监控信息系统 实时/历史数据库系统基准测试规范》，该规范仅规定了火力发电厂厂级监控信息系统中实时/历史数据库系统的测试内容和方法。  **3、项目必要性分析**  近年来，工业系统面临的风险与日俱增，实时数据库系统的安全也备受关注。因此，开展实时数据库系统安全评价研究就显得尤为迫切，制定《实时数据库系统安全评价要求》不仅可为用户选择实时数据库系统提供合理依据，也可为实时数据库系统的研制、生产、测试、评估和认证提供指导，对于保障工业信息系统有序高效发展具有重要的意义。  另外，目前国内实时数据库系统的实现水平不一，安全性参差不齐，与国外水平也存在很大的差距，在未来的应用中必将存在很大的安全隐患。因此，必须尽快地建立一套实时数据库系统的安全技术评价标准，来规范实时数据库系统功能及安全性的实现，为实时数据库系统在未来的应用中能够提供更安全的服务奠定更坚实的基础。 |
| 2.2 与国内外相关标准、文献的关系 | **1、CC标准**  CC标准（Common Criteria for Information Technology Security Evaluation，）是信息技术安全性通用评估标准，用于评估信息产品的安全性。CC标准是目前在国际上得到广泛认可和应用，具有一定权威性信息技术安全基础标准。  CC标准最初由美国NSA（National Security Agency，美国国家安全局,隶属于美国国防部）、美国NIST（National Institute of Standards and Technology，美国国家标准与技术研究院,隶属于美国商务部）、英国、法国、德国、荷兰、加拿大等六国七方于1996年推出，并于1999年被ISO采纳为国际标准 ISO/IEC 15408。我国于2001年将ISO/IEC 15408等同转化为国家标准，即GB/T18336-1,2,3:2001《信息技术 安全技术 信息技术安全性评估准则》。CC目前的稳定版本发展到3.1版（2009年7月发布），而4.0版本的开发工作也已启动和讨论。我国目前的GB/T18336:2015 对应的CC版本为3.1版。且等同采用ISO/IEC 15408:2008的GB/T 18336替代2008版的征求意见稿已发布，现正在征求意见中。  CC标准作为评估信息技术产品和系统安全性的基础准则，提出了目前国际上公认的表述信息技术安全性的结构，即把安全要求分为规范产品和系统安全行为的功能要求,以及解决如何正确有效的实施这些功能的保证要求。CC的先进性体现在其结构的开放性、表达方式的通用性、结构和表达方式的内在完备性和实用性四个方面。  CC标准共分为三部分，第一部分为简介和一般模型，描述了信息安全相关的基本概念和模型，以及保护轮廓（PP-Protection Profile）和安全目标（ST-Security Target）的要求。PP是为一类产品或系统定义信息安全技术要求，包括功能要求和保证要求。ST则定义了一个既定评估对象（TOE-Target of Evaluation）的IT安全要求，并规定了该TOE应提供的安全功能和保证措施以满足所提出的安全要求。ST是开发者、评估者和用户之间对TOE安全特性和评估范围达成一致的基础。第二部分和第三部分描述了安全功能要求和安全保证要求，“功能要求”是对产品希望提供的安全功能或特征的描述，“保证要求”是功能要求能够得到满足的程度。CC根据安全保证要求预先定义了7个安全保证级（EAL1~EAL7），安全保证能力由低到高逐级增强。  PP是应用CC的核心技术依据。随着近年来PP和CCRA成员国数量的增长，CCRA需要权衡CCRA成员国政府机构、产品厂商、实验室之间更多的利益，以协调CCRA成员国研发和应用PP。为此管理委员会发布了应用CC和CCRA的远景说明 。其中，明确指出，CCRA互认级别将仅限于EAL2，而且，未来PP的研发将采取由技术委员会协作研发的形式，即研发cPP(collaborative Protection Profiles，协作保护轮廓)。这一观点一方面体现了信息技术信息安全评估认证逐渐成为国际社会焦点的发展趋势，也显示了国际方面对信息安全认证结果互认采取审慎态度的倾向。截至目前，CC标准体系下已发布面向产品的PP（类似我国的产品安全标准）263个，其中美国最多，德国次之。  总之，CC标准为信息技术产品安全性检测评价标准的研制提供通用技术依据。在我国，GB/T 18336作为广泛应用的国家基础标准，已成为各种信息技术及产品信息安全标准研制的重要基础。  **2、行业标准草案**  目前国内外尚无统一的实时数据库安全技术相关标准，在数据接口、数据存储和使用上有一些应用规范，在某些行业出现过实时数据库系统的测试规范。 |

|  |  |
| --- | --- |
| **3 编制过程** | |
| 3.1 分工情况 | 标准的整体工作由项目负责人布宁负责，贾雪飞负责组织实施，霍珊珊、刘健、董晶晶、毕强、吴迪、刘思蓉、张怡、兰丹妮提供技术支持。 |
| 3.2 起草阶段 | 2016年7月-2016年8月  研究国内外实时数据库产品技术和标准规范，根据标准验证应用情况，在目前的草案基础上提出《实时数据库系统安全评价要求》初稿。  2016年7月-2016年11月  对《实时数据库系统安全评价要求》初稿征求业界意见，形成征求意见稿。 |
| 3.3 征求意见阶段 | 2016年12月-2017年3月  对《实时数据库系统安全评价要求》（征求意见稿）面向社会广泛征求意见，进一步完善，形成送审稿。 |

|  |
| --- |
| **4 主要技术内容的确定** |
| 为适应实时数据库系统技术的发展，本项目旨在集成认证、检测机构和相关产业的最佳实践，通过研究实时数据库产品工作原理、功能特点分析、确定产品安全边界和应用环境，结合相关法律法规及实际应用有关要求，参考相关技术标准和规范，提出我国实时数据库产品的评价规范，完善我国实时数据库产品相关信息安全标准。  **1、研究内容**  本项目研究内容包括：  1） 通过分析国内外实时数据库产品涉及的关键技术及工作原理，确定产品安全边界并分析其“安全环境”。  2） 结合产品功能和实际需求，识别实时数据库产品应用可能存在的威胁及安全假设。  3） 基于安全环境、安全威胁和应用假设的分析结果，提炼、标识实时数据库产品应达到的技术和管理“安全目标”。  4） 根据确定的安全目标，结合现有标准和法律法规要求提出对实时数据库产品的安全评价规范。  5） 基于产品功能和安全功能评价规范，研究制定相应的检测方法，并建立相关评价准则。  6） 根据我国产业发展现状，及用户应用和国家信息安全管理需要，确定有效实现实时数据库产品安全目标导出的安全要求，产品研发生产者信息安全保障能力应达到的级别，明确相关要求及方法。  7） 综合产品功能、安全功能、安全保障能力要求，及相应测试评价方法的研究结果，形成标准草案。  8） 根据标准验证应用结果、专家评审意见等需要，修订标准草案。包括：在检测认证活动中验证应用标准，组织专家对标准草案及验证应用情况进行评审，遵循保证标准科学性、可操作性、一定前瞻性等原则，对标准进行修订。  **2、技术方案**  本项目拟采取的技术路线如下：  1） 广泛调研国内外实时数据库产品技术现状，深入分析实时数据库产品实际需求。根据需求调研和技术发展趋势要求，分析提炼实时数据库产品的过程及模型；  2） 基于分析调研结果，确定产品安全边界，并分析产品“安全环境”，识别可能存在的威胁、组织安全策略及安全用户假设；  3） 根据识别的安全环境和威胁，标识技术和管理“安全目标”；  4） 依据安全目标，从《GB/T 18336 信息技术 安全技术 信息技术安全性评估准则》第二部分中选取相应的安全功能要求，，研究制定相应的检测和评价方法，并增加标识产品的功能和性能要求，及相应测试评价方法；  5） 根据当前管理和应用需求，确定产品应达到的信息安全保障能力级别，规定相关评估方法和评价准则；  6） 制定实时数据库安全评价规范草案；  7） 在检测、认证活动中验证实时数据库系统安全评价要求草案，并根据需要进行标准修订。  8) 项目研究过程中，组织3-4次认证机构、检测机构、产业、研究机构等相关专家研讨，并根据专家意见对产品标准草案进行修订。 |

|  |  |  |  |
| --- | --- | --- | --- |
| **5 验证情况（适用于方法类标准）** | | | |
| 5.1 验证单位情况 | 验证单位 | 验证人员 | 验证时间 | |
| 信息产业信息安全测评中心 | 董晶晶 | 2016年12月30日 | |
|  |  | 年 月 日 | |
|  |  | 年 月 日 | |
|  |  | 年 月 日 | |
| 5.2 验证过程 | 信息产业信息安全测评中心对北京庚顿数据科技有限公司的实时数据库产品进行检测。 | | |
| 5.3 验证数据分析 | 产品满足规范要求的所有项目。 | | |
| 5.4 验证评价 | 规范能够对产品的主要功能进行很好的覆盖，范围和强度能较为适当。 | | |
| 5.5 其他应说明的情况 |  | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **6 附加说明（可选项）** | | | | | | |
| 6.1 宣贯标准的建议 | / | | | | | |
| 6.2 修订和废除现行有关标准的建议 | / | | | | | |
| 6.3 作为强制性标准或推荐性标准的建议 | / | | | | | |
| 6.4 其他需要说明的情况 | / | | | | | |
| 6.5 参考文献 | 《GB/T 18336信息技术 安全技术 信息技术安全评估准则》 | | | | | |
| 联系人 | | 兰丹妮 | 联系电话 | 010-65994539 | 电子邮箱 | landn@isccc.gov.cn |
| 注 1：本格式的通用部分为第1章、第2章、第4章和第6章。  注 2：3.4适用于标准草案送审稿，3.5适用于标准草案报批稿，3.6中“预期的管理目标”适用于规程类标准，3.6中“技术指标”适用于方法类标准，第5章适用于方法类标准编制说明的编写。  注 3：3.1和第6章为可选项，其余为必填项。 | | | | | | |
| 编写日期：2017年5月3日 | | | | | | |