ICS 35.040
L 80

中华人民共和国国家标准

GB/T 18336.1—2008/ISO/IEC 15408-1:2005
代替 GB/T 18336.1—2001

信息技术　安全技术
信息技术安全性评估准则
第1部分:简介和一般模型

Information technology—Security techniques—
Evaluation criteria for IT security—
Part 1: Introduction and general model

(ISO/IEC 15408-1:2005,IDT)

2008-06-26 发布　　2008-11-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

GB/T 18336.1—2008/ISO/IEC 15408-1:2005

中华人民共和国
国家标准
信息技术　安全技术
信息技术安全性评估准则
第1部分:简介和一般模型
GB/T 18336.1—2008/ISO/IEC 15408-1:2005
*
中国标准出版社出版发行
北京复兴门外三里河北街16号
邮政编码:100045
网址 www.spc.net.cn
电话:68523946　68517548
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230　1/16　印张 2.5　字数 67 千字
2008年10月第一版　2008年10月第一次印刷
*
书号:155066·1-33838　定价 28.00 元

GB/T 18336.1-2008

参 考 文 献

[1] Bell D E,LaPadula L J. Secure Computer Systems: Unified Exposition and MULTICS Interpretation. Revision 1. US Air Force ESD-TR-75-306, MITRE Corporation MTR-2997, Bedford MA, March 1976.

[2] Biba K J. Integrity Considerations for Secure Computer Systems. ESD-TR-372, ESD/AFSC, Hanscom AFB, Bedford MA., April 1977.

[3] Canadian Trusted Computer Product Evaluation Criteria. Version 3.0. Canadian System Security Centre, Communications Security Establishment, Government of Canada, January 1993.

[4] Federal Criteria for Information Technology Security. Draft Version 1.0, (Volumes I and II). Jointly published by the National Institute of Standards and Technology and the National Security Agency, US Government, January 1993.

[5] Goguen J A Meseguer J. Security Policies and Security Models. 1982 Symposium on Security and Privacy, pp. 11-20, IEEE, April 1982.

[6] Goguen J A Meseguer J. Unwinding and Inference Control. 1984 Symposium on Security and Privacy, pp. 75-85, IEEE, May 1984.

[7] Information Technology Security Evaluation Criteria. Version 1.2. Office for Official Publications of the European Communities, June 1991.

[8] ISO/IEC 7498-2:1989 Information processing systems - Open Systems Interconnection - Basic Reference Model, Part 2: Security Architecture.

[9] ISO/IEC 15292:2001 Information technology - Security techniques - Protection Profile registration procedures.

[10] Trusted Computer Systems Evaluation Criteria. US DoD 5200.28-STD, December 1985.

目 次

d) 如果 ST 声明遵从 PP 的要求，但需要增添更多的目的和要求来扩展 PP，那么 ST 应定义这些增添的内容，尽管 PP 的引用可能已经充分定义了 PP 的目的和要求。在某些情况下，增添是非常重要的，此时最好在 ST 中重述 PP 的内容，以便描述得更清楚。

e) ST 声明部分遵从 PP 的情形是 GB/T 18336 评估不允许的。

在选择重述还是引用 PP 的目的和要求方面，GB/T 18336 不是说明性的。基本要求是 ST 的内容是完备的、清楚的和无歧义的，这样 ST 的评估才是可能的，ST 才是 TOE 评估的可接受的基础，对任何所声明的 PP 可追溯才是清楚的。

如果作出任何 PP 一致性声明，那么对于每一个 PP 声明，其陈述应包括以下内容：

a) **PP 引用**陈述应指出声称与其一致的那个 PP，加上与此相关的任何需要补充的内容。一个有效的声明意味着 TOE 满足该 PP 的所有要求。

b) **PP 裁剪**陈述应指出那些满足许可的 PP 操作或对 PP 要求进一步限制的 IT 安全要求陈述。

c) **PP 增加**陈述应指出那些额外增添了 PP 目的和要求的 TOE 目的和要求陈述。

B.2.9 应用注释

ST 的这个可选部分可包括额外的认为与 ST 相关的或有助于理解 ST 的信息。注意，如果 ST 声明遵从一个 PP 的要求，那么将在一个潜在的 PP 应用注释条款中所包含的某些信息纳入 ST 的另一个条款中是适当的。如，关于 TOE 构建方面的信息可在“TOE 概述”或“ST 基本原理”中提出，比在单独的“应用注释”条款中提出更适合。为了轻松通过 TOE 评估，假定在本附录描述的一个 ST 陈述结构不是标准化的，一个包含评估相关材料的应用注释宜作为 ST 条款的一部分，以便于为评估提供证据。

B.2.10 基本原理

ST 的这部分内容给出了用于 ST 评估的证据。这些证据将支持：ST 是一个完整的、紧密结合的要求集合，遵从该 ST 的 TOE 将在安全环境内提供一组有效的 IT 安全对策，并且 TOE 概要规范已经说明这些要求。基本原理也将证明任何 PP 一致性声明都是合理的。基本原理应包括以下几点：

a) **安全目的基本原理**应证明所提出的安全目的可追溯到在 TOE 安全环境里所识别的所有方面，并且正好覆盖所有的这些方面。

b) **安全要求基本原理**应证明该组（TOE 及其环境）安全要求正好满足安全目的且可追溯到安全目的。应证明以下几点：

1) 关于 TOE 及其 IT 安全环境的单个功能和保证要求组件的组合满足所提出的安全目的。

2) 该组安全要求一起构成了一个互相支持且内在一致的整体。

3) 安全要求的选择是合理的。所有下列情况都应当专门论证：

——选择没有包含在 GB/T 18336.2 或 GB/T 18336.3 中的要求；

——选择的保证要求没有包含一个 EAL；

——不满足依赖关系。

4) 为 ST 选择的功能强度级别和任何明确的功能强度声明与符合 TOE 安全目的是一致的。

c) **TOE 概述规范基本原理**应说明 TOE 安全功能和保证尺度都正好满足 TOE 安全要求。应对下列情况进行证实：

1) 所指定 TOE 的 IT 安全功能组合在一起正好满足 TOE 安全功能要求；

2) 所作的 TOE 功能强度声明是有效的，或者关于这种声明是不必要的断语是有效的；

3) 关于所提出的保证措施与保证要求相一致的声明是合理的。

基本原理陈述的详细程度应与安全功能定义的详细程度相匹配。

d) **PP 声明基本原理**的陈述应解释 ST 安全目的和要求与所有声明一致的 PP 之间的任何区别。如果没有 PP 一致性声明或者 ST 安全目的和要求与任何声明的 PP 的这些内容是等同的，这部分内容可以省略。

该潜在的长篇材料，不一定对所有 ST 用户都是适当的或有用的，因此可以单独分发。