ICS 35.240
A 90

GA

中华人民共和国公共安全行业标准

GA/T 695—2014
代替 GA/T 695—2007

信息安全技术
网络通信审计产品技术要求

Information security technology—
Technical requirements for audit products of network communication

2014-05-23 发布　　2014-05-23 实施

中华人民共和国公安部　　发 布

目　　次

前　言

本标准按照GB/T 1.1—2009给出的规则起草。

本标准代替GA/T 695—2007《信息安全技术　网络通讯安全审计数据留存功能要求》，与GA/T 695—2007相比主要技术变化如下：

——标准名称改为《信息安全技术　网络通信审计产品技术要求》(见封面，2007年版的封面)；

——增加了缩略语(见第4章)；

——增加了网络通信审计产品描述(见第5章)；

——增加了安全环境，包括假设、威胁和组织安全策略(见第6章)；

——增加了安全目的，包括产品安全目的和环境安全目的(见第7章)；

——增加了数据采集要求(见8.1)；

——修改了数据还原要求(见8.2，2007年版的4.2)；

——增加了统计要求(见8.3)；

——增加了分析处理要求(见8.4)；

——增加了统计报表要求(见8.5.2)；

——修改了标识与鉴别要求(见8.6，2007年版的4.3和4.4)；

——修改了数据传输安全要求(见8.7，2007年版的4.6)；

——修改了数据存储安全要求(见8.8，2007年版的4.6)；

——修改了安全保证要求(见第9章，2007年版的第5章)；

——增加了技术要求基本原理，包括安全功能要求基本原理和安全保证要求基本原理(见第10章)。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由公安部网络安全保卫局提出。

本标准由公安部信息系统安全标准化技术委员会归口。

本标准起草单位：公安部计算机信息系统安全产品质量监督检验中心、公安部第三研究所、深圳市深信服电子科技有限公司、蓝盾信息安全技术股份有限公司。

本标准主要起草人：王志佳、顾玮、李毅、顾健、沈亮、张武健、方卫东。

本标准所代替标准的历次版本发布情况为：

——GA/T 695—2007。

引　言

本标准详细描述了与网络通信审计产品安全环境相关的假设、威胁和组织安全策略，定义了网络通信审计产品及其支撑环境的安全目的，规定了网络通信审计产品的安全功能要求和安全保证要求，通过基本原理论证安全功能要求能够追溯并覆盖产品安全目的，安全目的能够追溯并覆盖安全环境相关的假设、威胁和组织安全策略。

本标准基本级参照了 GB/T 18336.3—2008 中规定的 EAL2 级安全保证要求，增强级在 EAL4 级安全保证要求的基础上，将脆弱性分析要求提升到可以抵御中等攻击潜力的攻击者发起的攻击。

本标准仅给出了网络通信审计产品应满足的安全技术要求，但对网络通信审计产品的具体技术实现方式、方法等不做要求。

信息安全技术
网络通信审计产品技术要求

1 范围

本标准规定了网络通信审计产品的安全功能要求、安全保证要求及等级划分要求。

本标准适用于网络通信审计产品的设计、开发及测试。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB 17859—1999 计算机信息系统 安全保护等级划分准则

GB/T 18336.1～18336.3—2008 信息技术 安全技术 信息技术安全性评估准则

GB/T 25069—2010 信息安全技术 术语

3 术语和定义

GB 17859—1999、GB/T 18336.1～18336.3—2008 和 GB/T 25069—2010 界定的以及下列术语和定义适用于本文件。

3.1

网络通信审计 audit of network communication

对网络通信进行记录和分析，并针对特定事件采取相应的动作。

3.2

审计记录 audit recordation

审计产品对网络通信进行记录和分析得到的信息。

3.3

日志 log

审计产品对自身事件进行记录和分析得到的信息。

3.4

审计中心 audit center

审计产品中记录、分析、处理网络通信数据的功能部件。

3.5

审计代理 audit agent

审计产品中采集网络通信数据并发送给审计中心的功能部件。

4 缩略语

下列缩略语适用于本文件。

CPU：中央处理器(Central Processing Unit)

DOS：拒绝服务(Denial of Service)