ICS 35.240
A 90

GA

中华人民共和国公共安全行业标准

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

Information security technology—Subsistence function requirements for security audit data of network communications

2007-05-14 发布　　2007-07-01 实施

中华人民共和国公安部　　发布

中华人民共和国公共安全
行业标准
信息安全技术　网络通讯安全审计
数据留存功能要求
GA/T 695—2007
*
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 0.5　字数 9 千字
2007年8月第一版　2007年8月第一次印刷
*
书号:155066·2-18032

前　言

本标准由公安部公共信息网络安全监察局提出。

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。

本标准主要起草人：沈亮、张奕、陆臻、顾玮、赵婷、张岚、顾健。

信息安全技术　网络通讯安全审计
数据留存功能要求

1　范围

本标准规定了网络通讯安全审计数据留存相关产品的自身安全功能要求、安全功能要求和保证要求。

本标准适用于网络通讯安全审计数据留存相关产品的生产及检测。

2　规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GB/T 18336.3—2001　信息技术　安全技术　信息技术安全性评估准则　第3部分：安全保证要求(idt ISO/IEC 15408-3：1999)

3　术语和定义

下列术语和定义适用于本标准。

3.1

网络通讯安全审计数据留存相关产品　security audit data subsistence correlation products of network communications

网络通讯安全审计数据留存相关产品(以下简称安全审计产品)是对网络或指定系统的使用状态进行跟踪并记录的产品。

3.2

审计日志　audit log

安全审计产品自身审计产生的信息。

3.3

审计记录　audit recordation

跟踪网络或指定系统的使用状态产生的信息。

3.4

审计信息　audit information

所有的审计日志和审计记录的总称。

4　网络通讯安全审计数据留存相关产品的安全功能要求

4.1　信息采集

4.1.1　审计记录

记录网络中数据包的相关信息，记录内容至少应包括：记录时间、源IP地址、源MAC地址、源端口、目标IP地址、源MAC地址、目的端口、协议类型、数据包长度。

4.1.2　审计日志

记录安全审计产品自身的审计，记录内容至少应包括：