ICS 35.240
A 90

GA

中华人民共和国公共安全行业标准

GA/T 699—2007

信息安全技术　计算机网络入侵报警通讯交换技术要求

Information security technology—Communication exchange criterion for alert of computer network intrusion

2007-05-14 发布　　2007-07-01 实施

中华人民共和国公安部　　发布

目　　次

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、上海金诺网络安全技术发展股份有限公司、北京中科网威信息技术有限公司、北京启明星辰信息技术有限公司、北京榕基网安科技有限公司。

本标准主要起草人：沈亮、顾健、丁鼎、肖江、徐秋芬、朱代祥。

信息安全技术　计算机网络入侵报警通讯交换技术要求

1　范围

本标准规定了报警处置系统中网络型入侵检测系统的相关接口元素定义、保存格式、命名规范和报警流程。

本标准适用于报警处置系统的开发和建设，相关开发商或集成商可参照本标准执行。

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部分。

GB/T 2260　中华人民共和国行政区划代码

GB 2312—1980　信息交换用汉字编码字符集　基本集

GB 18030—2000　信息技术　信息交换用汉字编码字符集　基本集的扩充

GA/Z 02—2005　公安业务基础数据元素代码集

GA/T 700—2007　信息安全技术　计算机网络入侵分级要求

3　术语和定义

3.1

网络型入侵检测系统　network intrusion detection system

通过监视网络中的数据包，发现是否有恶意用户或误用用户尝试非正常进入系统的产品套件。网络型入侵检测系统可以运行在目标机上监视自己的通迅，也可以在独立的机器上以混杂模式监测所有的网络通讯。本标准覆盖网络型入侵检测系统（英文简写为 NIDS），不涉及主机基入侵检测系统（英文简写为 HIDS）。

3.2

报警处置系统　alarm manager system

对来自各类业务系统的报警进行统一处置的平台，其中包含对前端入侵检测设备的数据传输接口。本标准涉及的是报警处置系统的前端信息接收部分。

3.3

上报数据　upload data

网络型入侵检测系统向报警处置系统远程接口上报的信息。上报数据应符合本标准中对数据格式的要求。

4　运行环境

4.1　系统结构

系统结构由网络型入侵检测系统、报警处置系统的远程接口组成。网络型入侵检测系统实现对网络行为的识别和处理、规则匹配和报警等功能；报警处置系统定义接收上报数据的远程接口，实现了信息收集和汇总。结构如图 1 所示。