ICS 35.240
A 90

GA

中华人民共和国公共安全行业标准

GA/T 1143—2014

信息安全技术
数据销毁软件产品安全技术要求

Information security technology—
Security technical requirements for data destruction software products

2014-03-14 发布　　2014-03-14 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、中国科学院高能物理研究所网络安全实验室、北京金元龙脉信息科技有限公司、厦门市美亚柏科信息股份有限公司、公安部第三研究所。

本标准主要起草人：陆臻、赵婷、顾健、顾玮、邱梓华、梁薇、林帆、黄志炜、吴焕发。

引　言

本标准详细描述了与数据销毁软件产品安全环境相关的假设、威胁和组织安全策略，定义了数据销毁软件产品及其支撑环境的安全目的，论证了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。

本标准仅给出了数据销毁软件产品应满足的安全技术要求，但对数据销毁软件产品的具体技术实现方式、方法等不做要求。

信息安全技术
数据销毁软件产品安全技术要求

1 范围

本标准规定了数据销毁软件产品的安全功能要求、安全保证要求及等级划分要求。

本标准适用于计算机信息系统中使用的、针对磁性存储介质的数据销毁软件产品的设计、开发和检测。

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—2008(所有部分) 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—2008(所有部分)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

数据覆写 data overwriting

将非敏感数据写入以前存有敏感数据的存储位置，达到清除数据的目的。

3.2

3 次数据销毁方法 3 times data destruction method

对指定目标磁盘以数据覆写的方式进行擦写，磁头经过各区段覆写 3 次，第 1 次通过固定字符，第 2 次通过固定字符的补码，第 3 次通过随机字符进行覆写。

3.3

7 次数据销毁方法 7 times data destruction method

对指定目标磁盘以数据覆写的方式进行擦写，磁头经过各区段覆写 7 次，第 1 次和第 2 次通过固定字符及其补码覆写，接下来分别用单字符、随机字符，然后再分别用固定字符及其补码覆写，最后使用随机字符进行覆写。

4 数据销毁软件产品描述

数据销毁软件产品以软件的形式安装在需要销毁数据的主机上，将非敏感数据覆写入以前存有敏感数据的存储位置，达到清除数据的目的。

数据销毁软件产品保护的资产是用户不再需要但仍然敏感的信息，这些信息对用户而言虽然不再