

NIST特别出版物1500-4r2

NIST大数据互操作框架： 第4卷：安全和隐私

内部资料
翻译：高卓

第3版

NIST大数据公共工作组
定义和分类小组

本出版物可从以下网址免费获得：
<https://doi.org/10.6028/NIST.SP.1500-4r2>

2019年10月



美国商务部

部长：Wilbur L. Ross, Jr.

国家标准和技术研究所

商务部副部长兼所长：Walter Copan

北京江南天安科技有限公司

目录

执行摘要

1. 介绍

- 1.1 背景
- 1.2 安全和隐私小组的工作范围和目标
- 1.3 报告的生成
- 1.4 报告的篇章结构

2. 大数据的安全和隐私

- 2.1 大数据的安全和隐私有什么不同
- 2.2 概述
- 2.3 安全和隐私对大数据特征的影响
 - 2.3.1 数据量
 - 2.3.2 速度
 - 2.3.3 多样性
 - 2.3.4 准确性
 - 2.3.5 可变性
- 2.4 新兴技术对大数据安全和隐私的影响
 - 2.4.1 云计算
 - 2.4.2 大数据安全和隐私保障级
 - 2.4.3 物联网和信息物理系统
 - 2.4.4 移动设备与大数据
 - 2.4.5 人与机构的融合
 - 2.4.6 系统通信器
 - 2.4.7 符合道德规范的设计
 - 2.4.7.1 自洁式系统
 - 2.4.7.2 毒性数据模型
 - 2.4.7.3 大数据安全的保障理念
 - 2.4.7.4 大数据的信任和结盟
 - 2.4.7.5 弱联盟场景下的编配
 - 2.4.7.6 征得同意和敲碎玻璃场景
 - 2.4.8 大数据的透明度

3. 安全和隐私用例举例

- 3.1 零售/营销
 - 3.1.1 消费者数字媒体的使用情况
 - 3.1.2 Nielsen Homescan: 阿波罗计划
 - 3.1.3 Web 流量分析
- 3.2 医疗卫生
 - 3.2.1 医疗信息交换系统
 - 3.2.2 基因隐私
 - 3.2.3 制药公司药物临床试验数据共享
- 3.3 网络安全

- 3.3.1 网络保护
 - 3.4 政府
 - 3.4.1 无人机传感器数据
 - 3.4.2 教育：通用核心学生成绩报告
 - 3.5 行业：航空
 - 3.5.1 传感器数据的存储和分析
 - 3.6 运输
 - 3.6.1 货运
 - 3.7 其他安全和隐私用例
 - 3.7.1 SEC 整合审计跟踪
 - 3.7.2 物联网设备管理
 - 3.7.3 全国性教育数据门户
- 4. 安全和隐私主题分类**
 - 4.1 安全和隐私主题的概念分类法
 - 4.1.1 数据的保密性
 - 4.1.2 起源
 - 4.1.3 系统健康状况
 - 4.1.4 公共政策、社会和跨机构主题
 - 4.2 安全和隐私主题的操作分类
 - 4.2.1 设备和应用注册
 - 4.2.2 身份和访问管理
 - 4.2.3 数据治理
 - 4.2.3.1 合规、治理和管理即代码
 - 4.2.4 基础设施管理
 - 4.2.5 风险和追责
 - 4.3 与安全和隐私主题相关的角色
 - 4.3.1 基础设施管理
 - 4.3.2 治理、风险管理和合规
 - 4.3.3 信息工作者
 - 4.4 角色与安全和隐私概念分类法的关系
 - 4.4.1 数据保密性
 - 4.4.2 起源
 - 4.4.3 系统健康状况管理
 - 4.4.4 公共政策、社会和跨机构主题
 - 4.5 其他分类主题
 - 4.5.1 供应、计量和计费
 - 4.5.2 数据联合
 - 4.5.3 ACM 分类法
 - 4.6 安全本体对于大数据的重要性
- 5. 大数据参考架构及安全和隐私基底**
 - 5.1 大数据安全操作分类与 NBDRA 的关系
 - 5.2 NBDRA 的安全和隐私基底
 - 5.3 安全和隐私基底原则

- 5.4 安全和隐私分析方法
- 5.5 用于数据转换的密码技术
 - 5.5.1 分类
 - 5.5.2 同态加密
 - 5.5.3 函数加密
 - 5.5.4 基于访问控制策略的加密
 - 5.5.5 安全多方计算
 - 5.5.6 区块链
 - 5.5.7 安全计算的硬件支持
 - 5.5.8 密码密钥轮换
 - 5.5.9 针对密码系统的联邦标准 FIPS 140-2
- 5.6 风险管理
 - 5.6.1 视个人可识别信息为高毒性物品
 - 5.6.2 撤销同意场景
 - 5.6.3 透明门户场景
 - 5.6.4 大数据取证和操作性事后评估
- 5.7 大数据安全建模和模拟 (MODSIM)
- 5.8 安全和隐私管理的各个阶段
- 6. 域特有的安全考虑**
- 7. 审计和配置管理**
 - 7.1 数据包层面的可追溯/可再现
 - 7.2 审计
 - 7.3 监控
- 8. 标准、最佳实践规范和差距**
 - 8.1 NIST 的网络安全框架
 - 8.2 大数据的配置管理
 - 8.2.1 DevSecOps 应运而生
 - 8.2.2 依赖关系模型
 - 8.3 大数据的 SDLC 标准和指南
 - 8.3.1 DevOps 中的大数据安全
 - 8.3.1.1 应用的生命周期管理
 - 8.3.1.2 应用发布管理中的安全和隐私事件
 - 8.3.1.3 编配
 - 8.3.1.4 API 先行
 - 8.3.2 模型驱动的开发
 - 8.3.3 大数据镜头下的其他标准
 - 8.3.3.1 ISO 21827:2008 和 SSE-CMM
 - 8.3.3.2 ISO 27018: 公共云中作为个人可识别信息处理器的个人可识别信息保护规则
 - 8.3.4 大数据的测试工程
 - 8.3.5 API 先行和微服务
 - 8.3.6 大数据的应用安全
 - 8.3.6.1 RBAC、ABAC 和工作流

- 8.3.6.2 “最少泄露”大数据实践
 - 8.3.6.3 日志
 - 8.3.6.4 通过设计实现的道德规范和隐私
 - 8.4 大数据治理
 - 8.5 新兴技术
 - 8.5.1 大数据的网络安全
 - 8.5.2 涉及大数据安全和隐私的机器学习、人工智能和分析
- 附录 A NIST 大数据安全和隐私保障级**
- 附录 B 与安全和隐私基底相关的现行标准**
- 附录 C 云生态系统的内部安全考虑**
- 附录 D 大数据行动者和角色——为适应大数据场景而改写**
- 附录 E 用例与 NBDRA 的映射对应**
 - E.1 零售/营销
 - E.1.1 消费者数字媒体的使用情况
 - E.1.2 Nielsen Homescan: 阿波罗计划
 - E.1.3 Web 流量分析
 - E.2 医疗卫生
 - E.2.1 医疗信息交换系统
 - E.2.2 制药公司临床试验数据共享
 - E.3 网络安全
 - E.3.1 网络保护
 - E.4 政府
 - E.4.1 无人机传感器数据
 - E.4.2 教育: 通用核心学生成绩报告
 - E.5 运输
 - E.5.1 货运
- 附录 F 第 2 版的变更和新增主题 (略)**
- 附录 G 缩略语**
- 附录 H 参考文献**