

# 《Java编码指南》

## 图书基本信息

书名：《Java编码指南》

13位ISBN编号：9787115403716

出版时间：2015-12

作者：Fred Long,Dhruv Mohindra,Robert C. Seacord,Dean F. Sutherland,David Svoboda

页数：263

译者：刘先宁,尤青松

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：[www.tushu111.com](http://www.tushu111.com)

# 《Java编码指南》

## 内容概要

《Java编码指南 编写安全可靠程序的75条建议》是《Java安全编码标准》一书的扩展，书中把那些不必列入Java安全编码标准但是同样会导致系统不可靠或不安全的Java编码实践整理了出来，并为这些糟糕的实践提供了相应的文档和警告，以及合规解决方案。读者可以将本书作为Java安全方面的工具书，根据自己的需要，找到自己感兴趣的规则进行阅读和理解，或者在实际开发中遇到安全问题时，根据书中列出的大致分类对规则进行索引和阅读，也可以通读全书的所有规则，系统地了解Java安全规则，增强对Java安全特性、语言使用、运行环境特性的理解。

## 作者简介

Fred Long 英国Aberystwyth大学计算机科学系的高级讲师，自1992年起一直担任软件工程研究所（Software Engineering Institute）的客座科学家。

Dhruv Mohindra 印度Persistent Systems有限公司安全实践小组的技术领导，为金融、电信、健康领域的很多公司提供咨询服务。

Robert C. Seacord 出版过多本软件安全与软件工程方面的书籍，是CERT安全编码倡议小组的技术经理，另外他还在卡内基-梅隆大学教计算机科学。

Dean F. Sutherland CERT高级软件安全工程师，之前是Tartan公司技术组的高级成员，他在Tartan公司主要负责开发优化编译器。

David Svoboda CERT软件安全工程师，是多个CMU项目的主要开发者。

### 译者简介

刘先宁 ThoughtWorks高级咨询师，长期从事一线软件开发工作，对Java、面向对象、敏捷方法论都有较深理解。其译作还包括《HTML5移动Web开发实战》。

尤青松 ThoughtWorks咨询师，在敏捷软件交付团队中担任技术领导人，尤其对Java企业软件开发及其安全编程有较深理解。

## 书籍目录

### 第1章 安全

- 指南1：限制敏感数据的生命周期
- 指南2：不要在客户端存储未经加密的敏感数据
- 指南3：为敏感可变类提供不可修改的包装器
- 指南4：确保安全敏感方法被调用时参数经过验证
- 指南5：防止任意文件上传
- 指南6：正确地编码或转义输出
- 指南7：防止代码注入
- 指南8：防止XPath注入
- 指南9：防止LDAP注入
- 指南10：不要使用clone()方法来复制不可信的方法参数
- 指南11：不要使用Object.equals()来比较密钥
- 指南12：不要使用不安全的弱加密算法
- 指南13：使用散列函数存储密码
- 指南14：确保SecureRandom正确地选择随机数种子
- 指南15：不要依赖可以被不可信代码覆盖的方法
- 指南16：避免授予过多特权
- 指南17：最小化特权代码
- 指南18：不要将使用降低安全性检查的方法暴露给不可信代码
- 指南19：对细粒度的安全定义自定义安全权限
- 指南20：使用安全管理器创建一个安全的沙盒
- 指南21：不要让不可信代码误用回调方法的特权

### 第2章 防御式编程

- 指南22：最小化变量的作用域
- 指南23：最小化@SuppressWarnings注解的作用域
- 指南24：最小化类及其成员的可访问性
- 指南25：文档化代码的线程安全性
- 指南26：为方法的结果值提供反馈
- 指南27：使用多个文件属性识别文件
- 指南28：不要赋予枚举常量的序号任何特殊意义
- 指南29：注意数字提升行为
- 指南30：对可变参数的类型做编译时类型检查
- 指南31：不要把其值在以后版本里可能会发生变化的常量设置为public final
- 指南32：避免包之间的循环依赖
- 指南33：使用用户自定义的异常而非宽泛的异常类型
- 指南34：尽量从系统错误中优雅恢复
- 指南35：发布接口前请谨慎设计
- 指南36：编写对垃圾收集机制友好的代码

### 第3章 可靠性

- 指南37：不要在子作用域里遮蔽或者掩盖标识符
- 指南38：不要在一个声明里声明多个变量
- 指南39：在程序逻辑中用有意义的符号常量代表文字值
- 指南40：在常量定义中恰当地表示相互之间的关系
- 指南41：对于返回数组或者集合的方法，用返回一个空数组或者集合来替代返回一个空值
- 指南42：只在异常的情况下使用异常
- 指南43：使用try—with—resources语句安全处理可关闭的资源
- 指南44：不要使用断言来验证不存在的运行时错误

指南45：在条件表达式中，第二个和第三个操作数应使用相同类型

指南46：不要序列化直接指向系统资源的句柄

指南47：更倾向于使用迭代器而不是列举

指南48：对于短生存周期、不常用的对象不要使用直接缓冲区

指南49：从长生存周期容器对象中移除短生存周期对象

第4章 程序的可理解性

指南50：谨慎使用视觉上有误导性的标识符和文字

指南51：避免歧义重载变参方法

指南52：要避免使用带内错误指示器

指南53：不要在条件表达式中进行赋值

指南54：请使用大括号把if、for或while代码体括起来

指南55：不要直接在if、for或while条件语句后面加分号

指南56：在每一个case分支的代码块中加上break语句

指南57：避免不当的计算循环计数器

指南58：使用括号表示操作的优先级

指南59：不要对文件的创建做任何假设

指南60：做浮点运算前把整数转换为浮点数

指南61：确保对象的clone()方法中有调用super.clone()

指南62：保持注释的一致性和可读性

指南63：检测并移除冗余的代码和值

指南64：尽量保证逻辑完备

指南65：避免有歧义的重载或者误导性的重载

第5章 程序员的常见误解

指南66：不要假设使用volatile关键字声明引用可以保证引用所指对象的安全发布

指南67：不要假设sleep()、yield()或getState()方法提供了同步语义

指南68：不要假设对整数做取余运算总是返回正整数

指南69：不要弄混抽象对象的相等性和引用的相等性

指南70：理解按位运算符和逻辑运算符之间的差异

指南71：理解加载字符串时如何做特殊字符转义

指南72：不要使用重载的方法来区分运行时类型

指南73：不要弄混引用的不可变性和对象的不可变性

指南74：谨慎使用序列化方法writeUnshared()和readUnshared()

指南75：不要试图通过把本地引用变量设置为null来帮助垃圾收集器

附录 Android

术语表

参考文献

## 版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:[www.tushu111.com](http://www.tushu111.com)