方电网
POWER GRID

司科技创新系列丛书◆

信息安全设备全生命周期管理研究与实践

贵州电网有限责任公司　组编

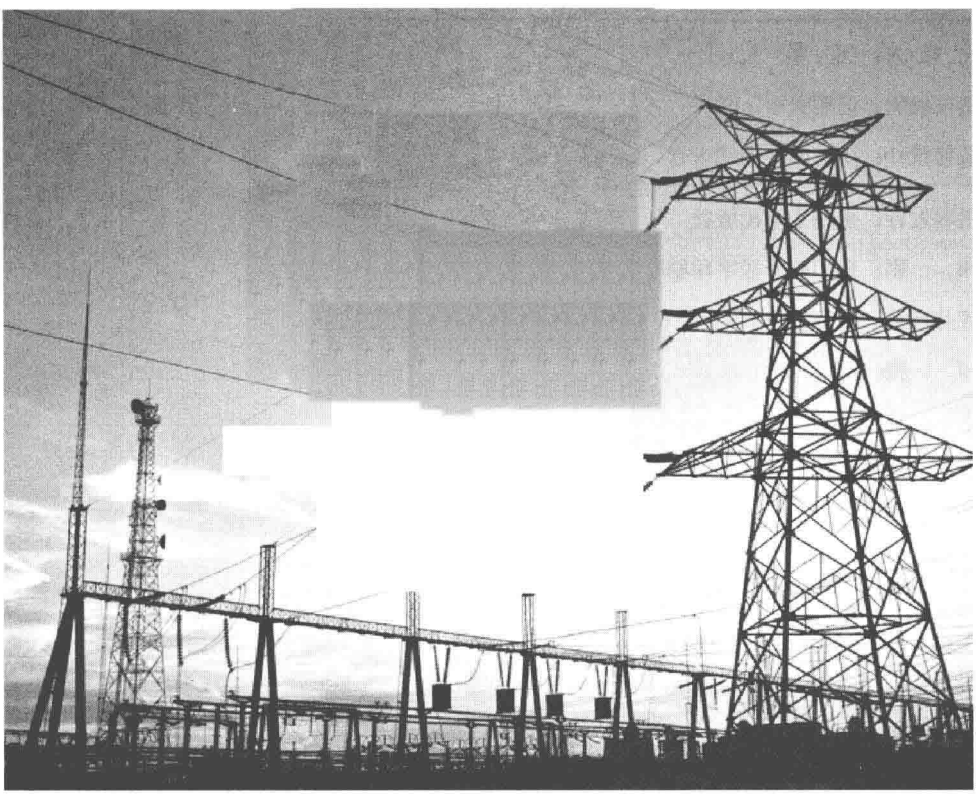
贵州大学出版社
Guizhou University Press

南方电网
ERN POWER GRID

◆贵州电网有限责任公司科技创新系列丛书◆

信息安全设备全生命周期管理研究与实践

贵州电网有限责任公司　组编



贵州大学出版社
Guizhou University Press

图书在版编目（CIP）数据

信息安全设备全生命周期管理研究与实践 / 贵州电网有限责任公司组编. —贵阳：贵州大学出版社，2017.9
（贵州电网有限责任公司科技创新系列丛书）

ISBN 978-7-5691-0020-4

Ⅰ. ①信… Ⅱ. ①贵… Ⅲ. ①信息安全—安全设备—研究 Ⅳ. ①TP309

中国版本图书馆 CIP 数据核字(2017)第 169974 号

信息安全设备全生命周期管理研究与实践

作　　者：贵州电网有限责任公司

出 版 人：闵　军

责任编辑：但明天

装帧设计：陈　艺　但明天

出版发行：贵州大学出版社

印　　刷：贵阳精彩数字印刷有限公司

成品尺寸：170 毫米×240 毫米

印　　张：31

字　　数：559 千字

版　　次：2017 年 9 月　第 1 版

印　　次：2017 年 9 月　第 1 次印刷

书　　号：ISBN 978-7-5691-0020-4

定　　价：122.00 元

编　委　会

主　编

杨　凛

副主编

张凌云　　李　巍

参　编

张　涛　　李俊杰　　廖　谦　　袁晓婷

李　卫

前言

网络安全随着信息技术的发展经历了三个阶段：一是防火墙、病毒与入侵检测系统部署的初级阶段；二是划分网络安全逻辑域，大量运用边界防护、脆弱性扫描和用户接入控制技术进行监控、审计、认证的安全建设阶段；三是把各个分离的网络部分进行统一管理、统一运营的安全体系统一管理阶段。

近年来，贵州电网有限责任公司大力开展企业管理信息系统及综合数据网的建设，建成了覆盖所有地、县、所的市场营销、安全生产、财务、人资、协同办公、项目计划等企业级管理信息系统，投运了涵盖所有 500kV、220kV、1100kV、35kV 变电站及供电所的综合数据网平台。随着信息技术的大量应用，信息安全显得尤为重要，地区性的综合安全运维中心（Security Operate Center, SOC）建设也就成为必然。

本次建设的信息安全设备全生命周期管理系统虽然和 SOC 有一定的关联，但更加注重从电力企业信息安全管理需求出发，从信息安全设备部署阶段、设备测试阶段及运行阶段的策略制定、统一监控、统一管理等，关注安全设备是否满足电力企业安全基线和等保要求，主动跟踪和记录所有规则和对象的变化，并对所有信息安全设备进行变更追踪和分析，实现实时报警，同时针对其日志的分析与审计，进一步实现信息安全设备策略的优化调整。

信息安全设备全生命周期管理——安全设备全生命周期，即以“规划设计阶段、部署阶段、测试阶段、运行阶段、废弃阶段”为横轴，以“流程管理、资产管理、策略管理、变更管理、风险管理、健康管理”六个维度为纵轴来研究，有效地将时间周期与管理目标紧密地结合起来，形成安全设备全

生命周期管理评价标准，以此作为安全设备全生命周期管理中心的内涵。该管理中心对信息安全设备进行不同时段、不同纬度、不同重点的管理，有效地防范和控制信息安全风险，增强信息安全体系的检测能力、保护能力。同时，通过安全设备全生命周期管理系统，以清晰可视化的方式展现出所有信息安全设备的自身健康状态、合规性状态、生命周期阶段变更状态、安全策略变更状态、初步的安全策略合规性状态等，一旦出现异常主动告警，有效提高安全预警能力以及应急处置能力。

另外，安全设备全生命周期管理系统在对安全设备进行实时监测诊断的系统框架基础之上，通过建立相应的技术规范，有效地整合设备配置管理信息和资源，形成状态监测、分析诊断、维护维修、信息反馈，持续提高监测性能的良性循环，充分保障信息网络和设备安全。

为了将科技项目的研究成果予以推广应用，更好地使用这些新技术、新设备，贵州电网有限责任公司组织相关人员进行科技成果系列专著的编写，详细介绍了这些新技术的原理、使用方法、注意事项等内容，有助于一线人员更好地了解、应用这些新技术、新设备、新系统，更加有助于信息专业的发展。

本书由杨凛主编，张凌云、李巍副主编，张涛、李俊杰、廖谦、袁晓婷、李卫等参加了编写。本书依据近年来贵州电网有限责任公司与相关企业合作研究的科技项目成果编写而成，可供广大同行人员学习和参考，亦可作为信息安全相关工作人员的参考书和培训资料。

限于作者知识水平，书中难免有疏漏和不妥之处，敬请读者批评、指正。

编　者

目 录

第1章

信息安全设备概况

1.1 信息安全设备管理发展历程和趋势

网络安全随着网络建设技术的发展经历了三个阶段：一是防火墙、防病毒与 IDS（Intrusion Detection Systems, 入侵检测系统）部署的初级阶段。二是随着网络规模的扩大，各种业务从相互独立到共同运营，网络管理中出现了安全域的概念，利用隔离技术把网络分为逻辑的安全区域，并且大量使用区域边界防护、脆弱性扫描与用户接入控制技术，此时的安全技术分为防护、监控、审计、认证、扫描等多种体系，纷繁复杂，称为安全建设阶段。三是随着业务的增多，网络的安全管理成为网络建设的新重点，把各个分离的安全体系统一管理、统一运营，我们称为安全管理阶段，最典型的就是综合性安全运营中心（Security Operation Center, SOC）的建设。

目前国内外研究得比较多的是 SOC 的建设，SOC 建设最初是为了解决安全设备的管理与海量安全事件的集中分析的平台，后来由于安全涉及的方面

较多，SOC 逐渐演化成以风险评估为基础的 TSOC、有策略管理的 NSOC、有审计为主的 ASOC 等。

本次建设的安全设备全生命周期管理虽然和 SOC 有一定的关联，但更加注重的是从我局信息安全管理的需求出发，关注安全设备从设备部署阶段、设备测试阶段及运行阶段的策略制定、统一监控、统一管理等，关注自动监控安全设备的策略是否满足南网的安全基线要求及等保要求，主动跟踪和记录所有规则和对象的变化，对所有安全设备进行变更追踪和分析，实现实时报警，同时通过对安全设备的日志进行分析和审计，进一步优化调整安全策略，保障网络安全。

1.2 信息安全设备全生命周期管理的由来

电力企业信息安全的重点在于设备安全管理。

1.2.1 设备通用型管理方式及其弊端

以往，安全设备往往仅注重于单点防护，而且需要配置专人管理。各个安全设备的部署往往不集中，导致需要投入极大的人力物力进行维护，而且由于无法综合各类信息进行汇总分析，无法起到整体层面的安全态势的获知和监控。而通过使用该系统，我局只需投入少量的人力物力即可综合管理所有的安全设备，并且能够从整体层面来获知信息安全态势。

1.2.2　信息安全设备全生命周期管理简介

信息安全设备全生命周期管理以安全设备全生命周期即“规划设计阶段、部署阶段、测试阶段、运行阶段、废弃阶段”为横轴线，以“流程管理、资产管理、策略管理、变更管理、风险管理、健康管理”六个纬度为纵轴线来研究，简称“五横、六纵”的管理模式进行研究，有效地将时间周期与管理目标紧密的结合起来，形成安全设备全生命周期管理评价标准，以此作为安全设备全生命周期管理中心的内涵。该管理中心对安全设备进行不同时间阶段、不同纬度、不同重点的管理，有效地防范和控制信息安全风险，增强信息安全体系的检测能力、保护能力。

对安全设备全生命周期的管理采集器性能进行图表展示、故障分级报警、策略配置统一分发等功能，尤其是对网络中数量较多、分布地域较广，品牌庞杂的网络环境进行统一管理，为用户开展信息安全建设提供专家级管理平台；用户仅需通过同一个界面即可对所有品牌产品进行配置和信息管理。同时，相比于传统的安全管理平台（SOC）产品，安全设备全生命周期管理中心不仅对全生命周期各个维度进行了有效的监管，而且还可实现关键信息记录和回溯，方便后续的记录回溯分析等业务。

1.3　信息安全设备全生命周期管理的适用范围

安全设备全生命周期管理中心主要负责安全设备全生命周期中各个流程的规范和记录，同时对该系统中相关的数据信息进行展示，接收安全设备全

生命周期信息采集器上报来的数据，经分析整理后对有必要的漏洞风险进行告警。

安全设备全生命周期管理中心采用 B/S 架构，对安全设备的整个生命周期的相关信息进行集中管理和展示，同时在该系统中规范化各个阶段的流程，并对流程的每一步都进行记录。

安全设备全生命周期管理中心集中管理和展示的主要内容包括：

- 安全设备资产信息管理。
- 安全设备健康管理。
- 系统流程管理。
- 安全设备风险信息管理。
- 安全设备策略信息管理。
- 系统内知识库信息管理。
- 系统用户管理。

第2章

设备全生命周期管理理论及意义

2.1 信息安全设备的构成

安全设备全生命周期管理中心全面集成了日志采集器、数据库、日志分析、审计、报表等功能部件，支持对合作厂商的防火墙、IPS、UAG、漏洞扫描、网站防护等各类产品的统一安全管理，全面的网络流量分析和上网行为管理功能，用于帮助管理员了解全网安全状况，该功能提供了第三方接口以供接入管理中心的安全厂商的设备使用。

该系统的总体组网拓扑示意图如图 2-1 所示。

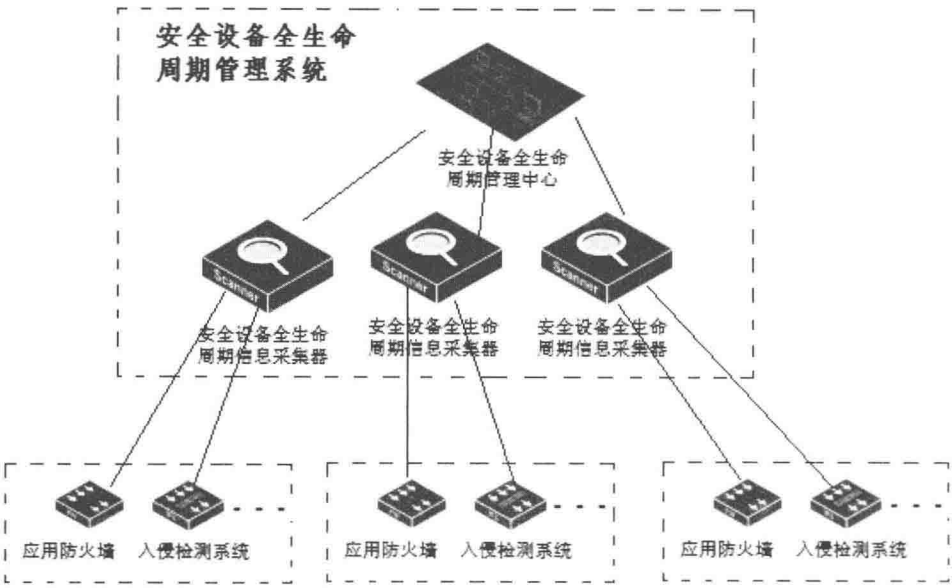


图 1-1　组网拓扑示意图

2.2　设备全生命周期管理的概念及必要性

2.2.1　信息安全设备全生命周期管理的概念

安全设备全生命周期管理主要负责安全设备全生命周期中各个流程的规范和记录，规范化安全设备的流程操作；接收处理安全设备全生命周期信息采集器上报来的数据（包括健康信息、策略配置信息等）后，通过良好的方式展示出来，并根据配置的告警设置进行必要的告警操作；通过关联安全设备全生命周期信息采集器进行漏洞、基线检查，检查结果经分析整理后，可以导出形式多样、内容丰富的检查报告，进而对有必要的漏洞风险进行告警

操作。

2.2.2　信息安全设备全生命周期管理的必要性

近些年，类似 APT（高级持续性威胁攻击）的新型网络攻击正呈爆炸式的发展。高级持续性威胁即 APT（Adavanced Persistent Threat），是指针对明确目标的持续、复杂的网络攻击。这个概念最早是在 2006 年左右由美国波音公司（United States Air Force）提出的，在 2010 年 Google 公司承认遭受严重黑客攻击后，APT 攻击已经成为信息安全行业热议的话题之一。

2013 年 4 月，Verizon 发布的《2013 年数据破坏调查报告》分析了全球 47000 多起数据破坏安全事故，621 宗确认的数据泄漏案例，以及至少 4400 万份失窃的记录。《报告》指出有高达 92%的数据破坏行为来自外部，有 19%的数据破坏行为来自国家级别的行为，利用脆弱或者窃取到的用户身份访问凭据进行入侵的行为占到了 76%，而各种黑客行为和恶意代码依然是主要的信息破坏手段。《报告》将包括 APT 攻击在内的信息破坏的敌对方分为有组织犯罪集团、国家或国家资助的组织、黑客活跃分子三类。FireEye 发布的《2012 年下半年高级威胁分析报告》详细分析了 APT 攻击的发展态势。《报告》指出，平均一个组织和单位每三分钟就会遭受一次恶意代码攻击，尤指是带有恶意附件、恶意 Web 链接或者 C&C 通信的邮件。在所有遭受攻击的企业和组织中，拥有核心关键技术的技术类企业占比最高。在定向钓鱼邮件（spear phishingemail）中经常使用通用的商业术语，具有很大的欺骗性。92%的攻击邮件都使用 ZIP 格式的附件。

此外，国际上尤其是美国着重炒作来自中国的 APT 攻击。最典型的是 Mandiant 公司发布的《对 APT1 组织的攻击行动的情报分析报告》，将 APT1 攻击行动的发起者直接定位到中国军方。在美国旧金山举办的 RSA 2013 大会上，直接以中国 APT 攻击为主题的报告就有 6 个之多。以防范 APT 攻击为契机，各国纷纷加强国家级的网络空间安全研究、相关政策制定与发布。美国、加拿大、日本、欧盟各国、北约等国家和组织纷纷强化其网络空间安全的国家战略，其中包括应对 APT 在内的国家级的敌对方的攻击。ENISA（欧洲网络与信息安全局）、北约 CCDCOE（协作网络空间防御卓越中心）、兰德公司、欧洲智库 SDA 公司都对世界主要国家的网络空间安全战略思想、安全威胁特征、安全防御水平等进行了较为深入的对比分析与研究。

各国对新型威胁的重视，也带动了整个网络空间安全市场的崛起。2012 年 6 月，MarketandMarket 公司发布了一份市场分析报告，称到 2017 年，全球的网络空间安全市场将达到 1200 亿美元的规模，而在 2011 年市场价值已经有 637 亿美元。该报告明确指出，网络空间安全未来将首要应对的问题就是 APT，此外还包括僵尸网络、传统蠕虫和病毒等。

2013 年 6 月，前美国中情局（CIA）职员爱德华·斯诺登将两份绝密资料交给英国《卫报》和美国《华盛顿邮报》，并告之媒体何时发表。按照设定的计划，2013 年 6 月 5 日，英国《卫报》先扔出第一颗舆论炸弹。美国国家安全局有一项代号为“棱镜”的秘密项目，要求电信巨头威瑞森够公司必须每天上交数百万用户的通话记录。6 月 6 日，美国《华盛顿邮报》披露，过去 6 年间，美国国家安全局和联邦调查局通过进入 Microsoft、Google、Apple、Yahoo