网络设备安全基线配置核查分析系统设计与实现

Design and Implementation of Security Baseline Configuration Verification Analysis System of Network Device

马　铮[1]，朱常波[1,2]（1. 中国联通网络技术研究院，北京 100048；2. 中国联通智能城市研究院，北京 100048）
Ma Zheng[1]，Zhu Changbo[1,2]（1. China Unicom Network Technology Research Institute，Beijing 100048，China；2. China Unicom Smart City Research Institute，Beijing 100048，China）

摘　要：
随着网络规模扩展和业务深度融合，设备安全参数和策略的配置进一步复杂，容易出现错配漏配，降低了网络可靠性和稳定性，因此，亟需加强网元安全基线配置核查能力。介绍了网络设备安全基线的定义、管控对象，分析了网络设备安全基线配置核查分析系统的功能需求，设计了系统总体架构，探讨了主要功能模块的具体实现方案。

关键词：
安全基线；配置核查；自动检测工具
doi：10.12045/j.issn.1007-3043.2019.04.002
中图分类号：TN915.08
文献标识码：A
文章编号：1007-3043（2019）04-0006-06

Abstract：
With the expansion of network scale and the deep integration of services，the configuration of equipment security parameters and strategies become more and more complex，error configurations occur frequently，which would reduce the reliability and stability of the network. So it is necessary to strengthen the verification capability of network equipment security configuration. It introduces the definition and scope of network equipment security baseline configuration，analyzes the functional requirements of the security configuration verification，designs the system architecture，and discusses the implementation of main function modules.

Keywords：
Security baseline configuration；Configuration verification；Automatic detection tool

引用格式：马铮，朱常波. 网络设备安全基线配置核查分析系统设计与实现[J]. 邮电设计技术，2019(4)：6-11.

1 概述

随着我国互联网业务模式进一步丰富，设备数量急剧增加，网络规模成倍扩展，导致网元设备参数和策略配置更加复杂，容易出现误配置或策略漏洞，造成设备带病入网和运营，增大了非法入侵、信息泄露的安全威胁，提高了后续运维的安全防护成本，降低了网络可靠性，除了影响人们的日常生活之外，还可能带来严重的经济损失，因此需要进一步提升配置合规性管理水平，但是由于设备类型版本多样，参数和策略配置项众多，传统人工手动核查的方式耗时耗力、客观性差，亟需一种平台化、自动化的解决方案，推动安全配置基线核查工作的常态化和标准化。

2 安全基线定义

网络设备安全基线是指对一个通信网元的最小安全保证，即网元需要满足现网运维和业务运维安全需求的最基本的、最重要的软硬件版本、参数设置，从而在不大规模增加网络复杂性和维护投资的前提下，使通信网络中所有系统、设备能够得到统一的、最低要求的安全保障，减少一些初级的、可预知的安全隐患，便于维护与管理，提高全网安全防护水平。

收稿日期：2019-02-13

配置基线要求涵盖范围包括通信网络中的所有网络设备、主机设备、安全设备以及运行在这些设备中的操作系统、应用程序、数据库、中间件等软硬件实体。

3 系统功能需求分析

该系统作为一款辅助运维工具，一方面要能够实现采集、核查和图表生成等操作的自动化、可视化，提高安全运维效率；另一方面则要能够具备一定的分析评估能力，为安全管理提供辅助决策。因此，本系统主要功能设计如下。

3.1 数据采集功能

支持本地和远程方式的配置参数提取功能，通过事先预置的口令和访问模式连接核查目标，通过自动化脚本收集相关设备安全配置信息，并确保系统能够在具有各种安全防护措施的实际场景下收集到完整的配置数据。在级联模式下，系统还支持向上级平台提交所采集的数据和分析的结果。

3.2 数据分析功能

自动化核查系统在采集到相关配置数据后，可以在本地进行分析也可以将配置参数上报上级分析平台，由上级分析平台进行分析，相关分析功能如下。

a）能够依据用户指定相关合规指标，判断目标主机上的检查项目达标与否，并对不达标项进行告警显示。

b）支持对各种安全规范要求中的所有检查项目进行等级区分，能够进行权重调整，能够依照百分制对目标主机的达标情况打分，每个检查参数的分值可以预先设置。

c）能够进行历史数据查询、任务合并、汇总查看、对比分析、趋势分析等，能够进行多个检查任务或多个IP风险对比。

d）内置专家知识库，具备辅助分析的功能，能够对网络安全合规性进行评估，给出完善建议。

3.3 任务管理功能

安全配置基线核查系统能够对核查任务进行配置管理，支持任务命名与分组设置；支持任务定时、周期设置；支持核查模板的定制修改和导入导出；支持对核查参数的权重赋值；支持访问口令和访问模式的设置；支持核查扫描时间和周期的设置；支持核查结果上报方式设置等。

3.4 图表输出功能

为了配合操作人员进行辅助决策，要求系统具备图表定制和输出功能。

a）支持核查结果图表显示条目的自定义，除了包括核查结果软硬件版本信息、配置信息、漏洞信息等基本检查项，还要能够增加地理位置、机房信息、设备用途等标示信息。

b）支持核查图表导出，支持HTML、Excel、PDF、Word等主流格式，内容应包含整体概述、各设备的检查列表等信息。

c）支持图表远程上报。

3.5 系统管理功能

该系统应能够提供用户、角色和组织机构管理权限划分功能；实现对系统配置检查功能日志的记录与查询；提供分布式组件管理，实现对分布式离线采集器和单机代理的管理；提供对系统数据的维护配置管理，支持系统自动、手动更新。

4 系统架构设计

根据功能和工作模式需求，本系统按照软件分层及模块化的思想进行设计，不同功能模块可以灵活地以服务的形式部署在不同主机上，便于合理分配资源和性能调优。

系统架构可分为表示层、业务逻辑层、数据访问层和底层数据库，具体设计如图1所示。

a）表示层：主要表现为UI界面的形式，负责系统的可视化呈现以及处理用户与系统之间的交互，负责将用户输入的指令和数据交付给业务逻辑层进行逻辑处理，包括任务配置界面、任务报告界面、高级数据分析界面、用户角色管理界面和日志记录管理界面。

b）业务逻辑层：接收表示层提交的用户操作，调用不同的逻辑处理模块。在处理过程中，根据业务需求向数据访问层请求访问相应数据。业务逻辑层是整个系统的核心部分，负责数据信息处理及核查任务执行等关键职能。它主要包括以下几个子部分：

（a）配置核查引擎。对用户提交的核查任务进行分析、分解，获取核查任务的相关信息，包括核查设备以及所采用的模板等，之后交付协议连接引擎进行远程连接协商。

（b）协议连接引擎。每台被核查设备都事先规定了各自的远程连接方式。协议连接引擎支持多种远程连接协议，可根据设备要求选择不同的连接模块，与目标设备协商建立远程连接，其中包括参数协商以

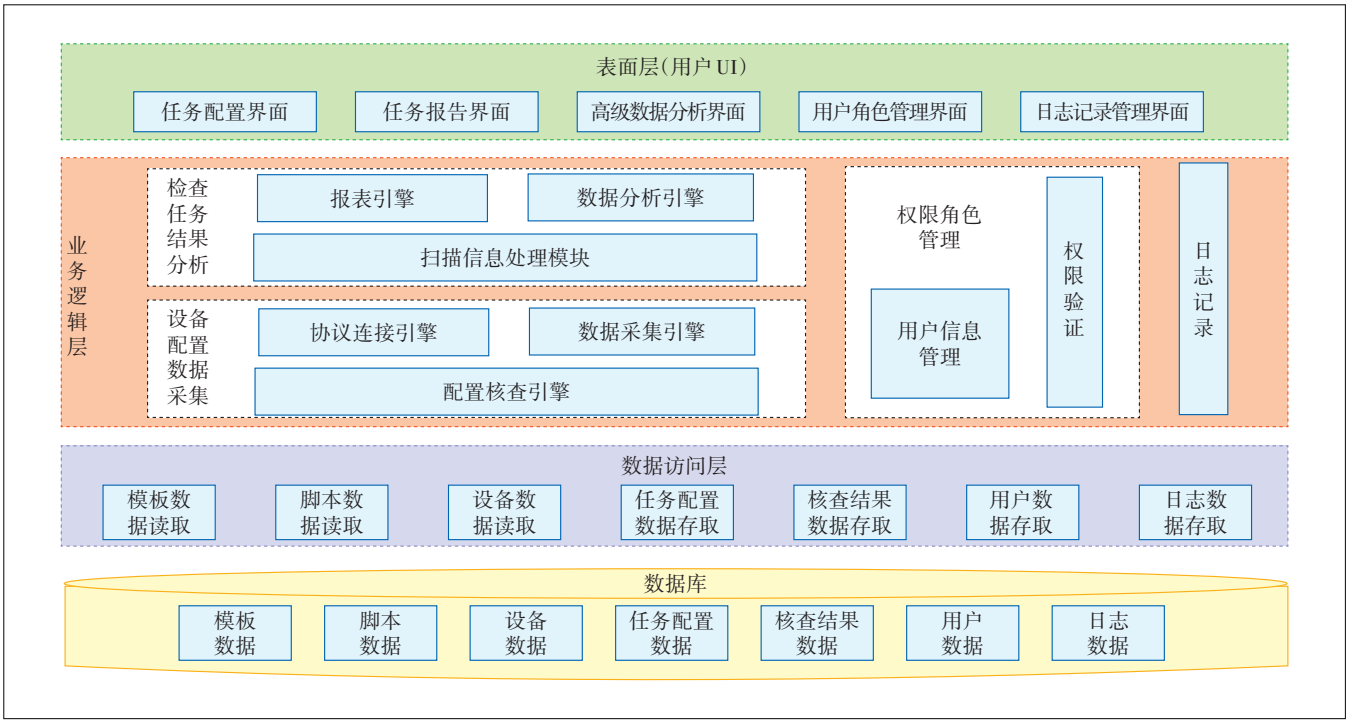

图1　系统架构

及身份认证等。

（c）数据采集引擎。远程连接上目标设备后，通过连接执行模板中各个检查项对应的脚本，将采集到的设备配置保存到结果文件中。

（d）扫描信息处理模块。对数据采集引擎返回的结果文件进行处理和判断，交付到报表引擎等模块进行数据分析。

（e）报表引擎。报表展示的核心处理模块，借助表格、图像等UI控件将核查结果以可视化的形式展现给用户。

（f）数据分析引擎。根据用户的需求，对特定核查任务数据进行高级数据分析，支持的分析方法有对比分析、趋势分析等。

（g）用户信息管理。负责处理用户个人信息的修改以及管理员增加或删除用户等操作。

（h）权限验证。提供系统授权使用的信息，包含登录用户权限、授权使用模块、授权存取信息等。

（i）日志记录。提供系统日志，实时记录用户的敏感操作，并支持管理员用户维护日志。

c）数据访问层：该层封装了存取数据的接口，根据业务逻辑层的需要提供相应的数据服务。在本系统中，对于模板、脚本和设备数据，数据访问层只需提供数据读取接口，至于任务配置、核查结果、用户和日志等数据，则要求数据访问层支持读取和写入。

d）数据库：存储设备安全基线配置核查分析系统所需的各种数据，至少应该包括以下7个方面：模板数据、脚本数据、设备数据、任务配置数据、核查结果数据、用户数据和日志数据。

5 主要功能模块实现

5.1 设备配置数据采集功能

设备配置数据采集模块支持用户通过在线的方式采集子网内目标设备的配置数据。用户可以根据自身的需求，选用不同的采集模板收集多项设备配置数据。当确定模板之后，用户还需要指定目标设备，启动采集任务。

系统响应用户发出的启动命令，开始通过远程连接协议尝试连接目标设备。成功连接之后，系统向目标设备发送采集脚本命令。目标设备执行完脚本命令后，将执行结果（即相应的配置数据）返回给系统，交由系统保存。根据目标设备的类型需要采用不同的远程连接协议。系统支持实现3种远程连接协议：Telnet、SSH和WinRM。图2为设备配置数据采集模块的结构示意图。

设备配置数据采集模块的输入有2项，分别是采集模板的ID和目标设备的IP，输出则是以XML文件

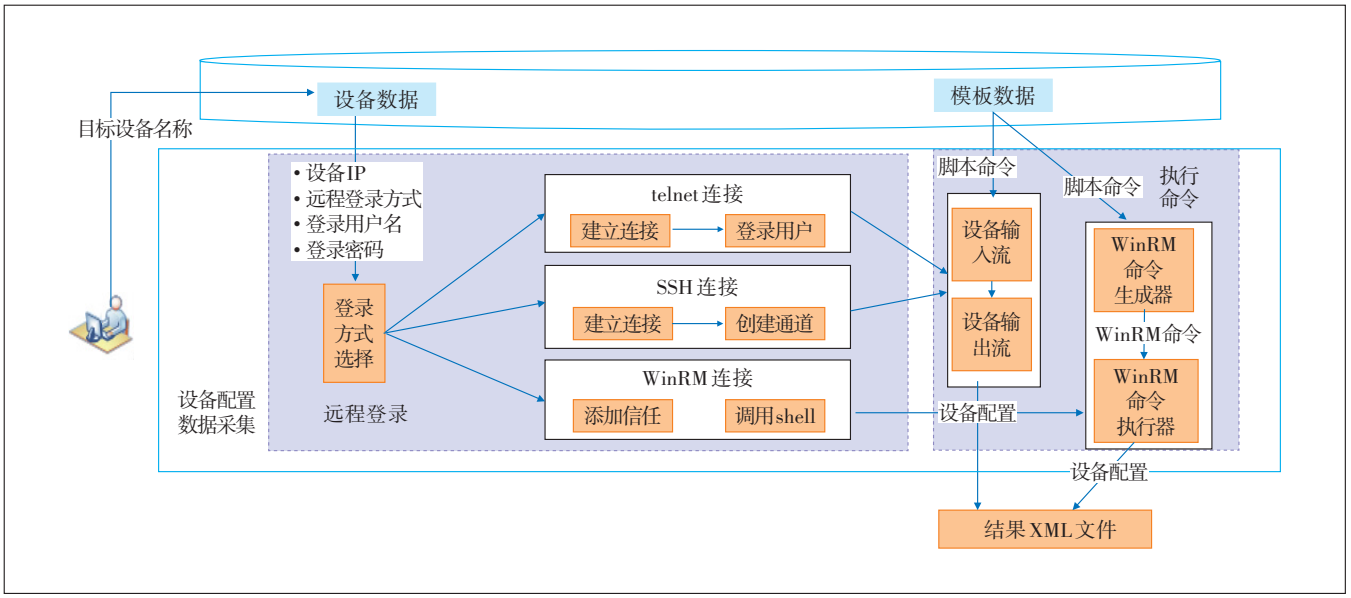

图2　设备配置数据采集模块的结构示意图

形式保存的设备配置数据。当操作人员输入功能命令（即启动任务）后，界面UI将操作人员输入的采集模板ID与目标设备IP传入设备配置数据采集模块，模块开始进行配置数据的采集工作。模块首先根据目标设备的IP从数据库的设备数据中读取目标设备的其他信息，其中包括目标设备的远程登录方式、登录用户名及密码等。之后根据预设的远程登录方式选择调用不同的远程连接子模块，如Telnet、SSH和WinRM。在成功连接上目标设备之后，再根据模板ID从数据库的模板数据中读取相应的脚本命令，根据远程连接协议采用不同的方式将脚本命令交由目标设备执行，并实时地将收集到的设备配置（即脚本命令的执行结果）保存至一个XML文件。等到所有设备都扫描完毕时，设备配置数据采集模块的工作结束。

5.2 核查任务结果分析功能

核查任务结果分析模块主要完成以下3个方面的功能。

5.2.1 结果判定

分析设备配置数据采集模块生成的结果XML文件，根据通信网络安全基线规范，判断核查设备的检查项目是否达标，并对不达标的项目进行高亮显示。每个检查项目的判定结果包含6个状态：符合、不符合、待确认、不适用、采集失败、未执行。

a）符合：表示设备配置符合配置规范的要求。

b）不符合：表示设备配置不符合配置规范的要求。

c）待确认：表示设备配置的最终结果需要评估人根据现场情况确认。

d）不适用：表示设备配置没有正常获取，例如访问权限不足、相关配置文件不存在、设备版本不匹配等情况。

e）采集失败：表示设备配置访问未能成功，例如连接失败、账号口令不正确等。

f）未执行：表示设备配置评估没有执行。

5.2.2 评分和生成报告

在对目标设备的各个检查项的达标情况进行判定之后，依照百分制为目标主机打分，其中各个检查项的权重在模块设置中指定。在评分之后，进行其他数据的统计，最后生成一份评估报告来展示本次任务的核查结果。

5.2.3 高级数据分析

a）历史数据查询：查询历史任务信息以及它们的评测结果。

b）任务汇总：汇总多个任务的评测结果。

c）对比分析：对比同一设备在不同任务的核查情况。

d）趋势分析：观察设备安全状态的时间趋势。

图3为核查任务结果分析模块的整体结构。模块总共完成3个方面的功能：结果分析、评分和生成报告以及高级数据分析。因此，也相应地将整个模块划分为3个子模块分别实现。其中结果分析子模块用于分析设备配置数据采集模块的输出结果XML文件，它主

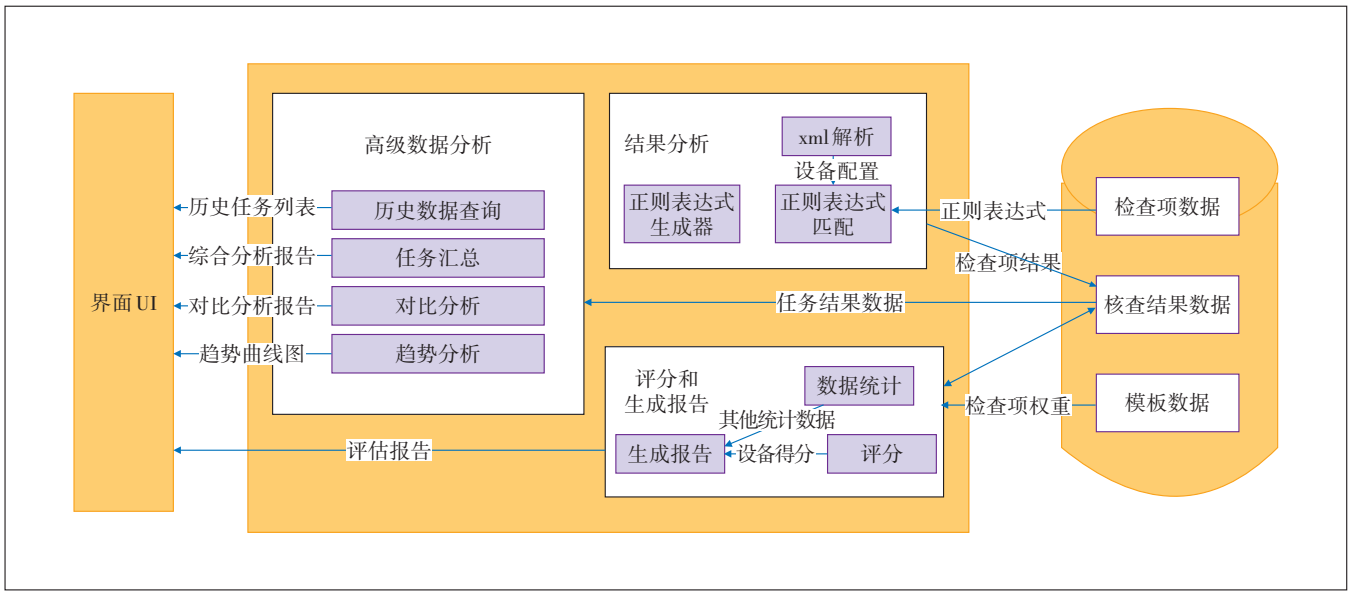

图3　核查任务结果分析模块结构

要是在后台执行,从数据库中的检查项数据获取各个检查项的安全基线指标值,与实际采集的配置进行比对、分析,然后将核查结果存入数据库。在结果分析完成之后,启动评分和生成报告子模块,根据任务中各个检查项的核查结果以及在模板中对应的权重进行评分,同时统计其他数据,最后生成一份评估报告展现给用户。而最后的高级数据分析子模块是在前两者分析的结果数据基础上进行,根据操作人员的操作指令进行相应的分析,分析完成后通过界面UI展示。

5.3 系统安全管理功能

设备安全基线配置核查分析系统通过日志记录模块和权限角色管理模块来保障系统的安全性和保密性。

5.3.1 日志记录功能

本系统要求具有维护日志记录的功能,当操作人员进行某项操作时,以数据库的形式实时将其操作记录下来,这有利于及早发现非法入侵和进行系统维护。

根据需求,日志记录记录的信息一共有六大类,分别是登录信息、任务管理信息、设备管理信息、模板管理信息、检查项管理信息和脚本管理信息。各类信息记录的具体操作如下。

a) 登录信息。登录操作记录。

b) 任务管理信息。启动在线扫描任务、导入任务配置文件、导出任务配置文件、导出离线脚本、导入离线采集结果和删除任务记录。

c) 设备管理信息。添加设备信息、修改设备信息、删除设备信息、导入设备信息和导出设备信息。

d) 模板管理信息。添加新模板、修改模板、删除模板、导入模板和导出模板。

e) 检查项管理信息。添加新检查项、修改检查项、删除检查项、导入检查项和导出检查项。

f) 脚本管理信息。添加新脚本、修改脚本、删除脚本、导入脚本和导出脚本。

5.3.2 权限角色管理功能

为了保障系统数据的安全性,系统提供相应的用户、角色管理和权限验证功能。权限包括以下2个方面:功能资源的操作权限和数据资源的存取权限。其中功能资源权限指的是配置检查工具的各个功能模块的使用权限,而数据资源权限指的是对象资源(网络设备)和基本配置检查结果信息的查看权限。

根据要求,系统的任何一个合法用户都必须从属于某个角色,并拥有角色对应的权限。在用户执行任何操作之前,都需要审核用户的权限范围。如果用户权限不足,则禁止本次操作。

图4为权限角色管理模块的结构,在操作人员登录系统之后,权限角色管理模块正式启动,首先通过与数据库中的用户数据进行交互,获取操作人员对应的角色,之后根据操作人员的角色管理权限。

权限角色管理模块可分为2个子模块,分别为权限验证子模块和用户管理子模块。其中权限验证子

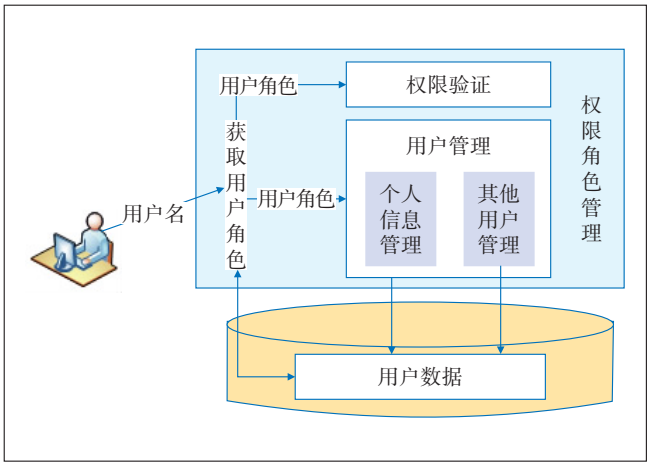

图4　权限角色管理模块的结构示意图

模块主要用来判断用户的某项操作是否在其对应角色的权限范围内，如果权限不足，则予以禁止。而用户管理子模块主要是负责用户信息的管理，供用户修改用户名、密码等个人信息。由于只有管理员用户才可以执行这项操作。因此在调用其他用户管理子模块之前，需要由权限验证子模块判断用户的角色是否为管理员用户。

6 安全基线合规管理优化建议

为了更好地提升安全基线合规管理能力，除了提高自动化运维水平之外，还要推动核查范围由点到面的全覆盖，建立总部平台，实现大数据集中分析平台，持续积累各种异常案例和配置知识库，并对全网安全态势进行综合评估，挖掘提取容易配错的设备类型和参数指标，在日常运维中做好预防工作。

此外，安全防护工作一定要做到技管并重，既要有自动化、智能化的运维工具，更要有制度化、体系化的管理机制，因此一方面要增强运维人员的安全合规意识，做好规范教育和技术培训，防止出现各类低级错误，另一方面则要加强合规运维的考核力度，将合规操作、漏洞封堵纳入各级单位考核范畴，定期组织自查和第三方抽检，并对整改效果进行持续跟踪和后评估，引起各个层面重视，保证考核工作的常态化。

7 结束语

综上所述，安全基线是网络和业务稳定运行的最根本基础，如果设备带病入网和运行，无论后续加载多少防护措施都成了无本之木、空中楼阁，不但会增加防护成本也会降低防护效果，整个服务运营的可靠性也就无从谈起。

因此，必须要高度重视安全基线管理体系的建设，一方面要积极进行技术创新，引入相关安全工具提高基线核查工作的自动化和智能化，降低安全运维人工成本，另一方面还要不断完善管理机制，加强职业素养培训，优化奖惩制度，充分调用相关人员积极性，全面保障网络合规稳定运行。

参考文献：

[1] CNNIC. 第34次中国互联网络发展状况统计报告[R]. 北京：中国互联网信息中心，2014.
[2] 黄成哲. 信息安全风险评估工具综述[J]. 黑龙江工程学院学报，2006(3).
[3] 周季礼. 美国打造自主可控信息安全产业链的主要举措及启示[J]. 信息安全与通信保密，2014(11).
[4] 于飞. 信息安全测评工具的发展现状和建议[J]. 信息安全与通信保密，2014(8).
[5] SYMANTEC. Products & Solutions[EB/OL]. [2019-01-22]. http://www.symantec.com.
[6] 佚名. 启明星辰推出安全配置核查管理系统[J]. 中国信息安全，2013(10).
[7] 布兰切特，萨默菲尔德. C++ GUI Qt 4 编程[M]. 闫锋欣，译. 2版. 北京：电子工业出版社，2008.
[8] 王甜. 信息系统安全等级测评配置检查工具研究与实现[J]. 计算机应用与软件，2014，31(7).
[9] POSTEL J, REYNOLDS J. Telnet Protocol Specification, RFC854 [EB/OL]. [2019-01-22]. http://www.networksorcery.com/enp/default0702.htm.
[10] YLONEN T. The Secure Shell (SSH) Authentication Protocol, RFC4252[EB/OL]. [2019-01-22]. http://tools.ietf.org/html/rfc4252. 2006-01.
[11] Windows Remote Management[EB/OL]. [2019-01-22]. https://msdn.microsoft.com/en-us/library/windows/desktop/aa384426(v=vs.85).aspx.
[12] 李晨，王伟. 安全基线控制在风险管理过程中的应用[J]. 网络安全技术与应用，2009(9)：4-7.
[13] 桂永宏. 业务系统安全基线的研究及应用[J]. 计算机安全，2011(10)：23-27.

作者简介：
马铮，高级工程师，硕士，主要研究方向为移动互联网安全优化及智能管控相关领域；朱常波，中国联通智能城市创新研究院院长，中讯邮电咨询设计院有限公司、中国联通网络技术研究院副总经理，博士，主要研究方向为网络安全、网络优化、大数据分析处理等。