DOI: 10.19364/j.1674-9405.2019.04.003

智慧水利总体方案之网络安全

詹全忠，张　潮

（水利部信息中心，北京　100053）

摘　要：近年来，水利网络安全建设不断加强，有效保障水旱灾害防御、水资源监控等水利重要业务的安全运行，但仍存在网络安全防护水平不够高，各自为战，威胁感知能力不够，对云计算等新技术的适应手段不足等问题。结合水利行业实际，主要从纵深防御、监测预警、应急响应能力，安全管理、运营体系等建设方面提出网络安全的总体架构，为智慧水利时代建设全面、联动、主动、智能的网络安全体系指明方向，具有重要行业指导意义。

关键词：智慧水利；监测预警；网络安全；安全技术；安全管理；安全运营

中图分类号：TP393.08　　**文献标识码：**A　　**文章编号：**1674-9405(2019)04-0020-05

0　引言

近年来，水利信息化发展迅速，以水利业务网和各级数据中心为基础，水旱灾害防御、水资源监控、河湖长制管理等一大批信息系统有效部署运行，有力支撑了水利的各项业务工作。在水利信息化快速发展的同时，网络安全的重要性逐渐凸显，水利各级单位以网络安全法、安全等级保护制度为基础，以水利网络安全顶层设计为指导，初步建立了网络安全保障体系 [1]。以水利部部本级为例，在 10 多 a 前就达到等级保护三级系统的防护水平，基本建立了纵深防御体系 [2]。但从水利行业看，信息系统尤其是工控系统网络安全防护体系不健全，防护水平不高，防护措施不当，态势感知能力不够，对云计算、大数据、物联网、移动互联网等新技术的适应手段不足，容灾备份系统不完善等问题均存在不同程度的隐患 [3]。

当前水利行业正按照国家关于网络强国、数字中国、智慧社会的总体部署和“十六字”治水方针，聚焦新老水问题，贯彻“水利工程补短板、水利行业强监管”总基调，坚持问题导向，对标“安全、实用”总要求，补齐信息化短板，支撑行业强监管，加快推进智慧水利建设，不断提升水利信息化水平，为国家水治理体系和能力的现代化提供有力支撑与强力驱动 [4]。网络安全和信息化是一体之两翼、驱动之双轮，必须统一谋划、部署、推进、实施，做到协调一致、齐头并进，以安全保发展，以发展促安全。在智慧水利的发展进程中，加强网络安全的规划与建设是必要保障条件，让网络安全始终渗透在整个体系之中，建立与智慧水利发展相协调的全面、系统、主动、智能的智慧水利网络安全体系是大势所趋和必然要求。

1　网络安全总体架构

根据国家网络安全相关政策标准要求，遵循水利网络安全顶层设计和总体策略，落实网络安全法、安全等级保护和关键信息基础设施保护相关要求，以智慧水利涉及的水利基础信息网络、云计算平台/系统、大数据应用/平台/资源、物联网（IoT）、水利工程控制和业务应用系统（含移动互联技术的系统）等为保护对象，建立和完善以包含纵深防御为基础、监测预警为核心、应急响应为抓手的全要素网络安全技术体系；涵盖人员组织、制度标准、工作规程在内的全方位网络安全管理体系；贯穿安全运维和监测、响应处置、分析优化的全过程闭环安全运营体系，提升与智慧水利建设全面融合的网络安全保障能力。

收稿日期：2019-07-01

作者简介：詹全忠（1974-），男，湖北大冶人，教授级高工，研究方向：网络安全。E-mail: zqz@mwr.gov.cn

智慧水利网络安全体系涵盖安全技术、管理、运营三大部分，其中安全技术部分又包含纵深防御、监测预警、应急响应 3 个层面的建设内容，总体架构如图 1 所示。

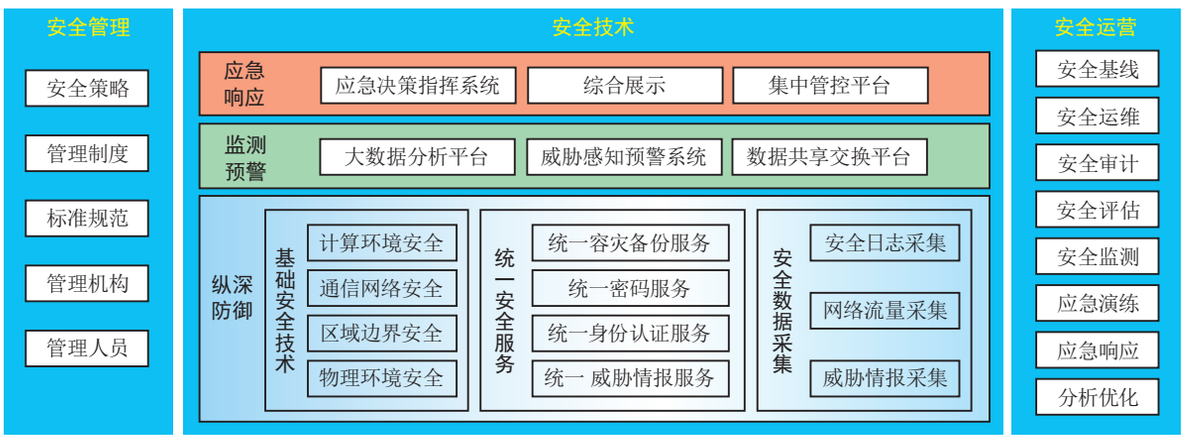

图 1　智慧水利网络安全体系总体框架图

1）安全管理。网络安全管理体系以合规合法、责任到人为中心，主要涵盖：网络安全策略、管理制度、标准规范体系、管理机构和人员，以及系统安全建设、运维管理等多方面，为智慧水利网络安全建设提供强有力的支撑。

2）安全技术。a. 纵深防御。网络安全纵深防御能力包括基础安全技术、统一安全服务、安全数据采集 3 个方面。基础安全技术构成网络安全等级保护安全合规运营的技术基础，也形成体系化的纵深防御安全能力基础。统一安全服务旨在构建智慧水利体系运行所需的统一安全服务基础设施，保证体系覆盖范围内获得一致性可持续的安全能力组件，也实现体系安全保障资源的集约化和各层级单位整合共享 [5]。安全数据采集主要用于采集外部网络安全情报和网络内与网络安全相关的各类数据信息。

b. 监测预警。网络安全监测预警能力以大数据分析平台为基础，充分利用分布式处理、深度学习、异构计算等大数据处理挖掘技术，建设威胁感知预警系统，对网内安全状态进行实时感知，并在行业内进行相关的数据共享。

c. 应急响应。网络安全应急响应能力指基于威胁情报态势感知的不同层级信息进行应急响应。智慧水利的安全能力进一步从监测响应式主动防御升级演进到威胁情报预警指挥智能处置能力，包括应急决策指挥、综合展示和集中管控平台等维度的内容。

3）安全运营。网络安全运营体系包括：安全基线制定、日常安全运维，系统运行中安全评估、安全监测、渗透测试、漏洞修复、运维审计，日常应急演练，安全事件发生后的响应处置与分析优化策略调整等完善的以数据为核心的闭环网络安全运营全流程。从而有效地对安全威胁事件进行综合研判和及时处置，并不断闭环对运营体系进行优化，充分发挥人在网络安全中的主体地位。

2　网络安全技术体系

网络安全技术体系旨在通过纵深防御建立合规网络防护基础，在此基础上通过监测预警提升网络安全风险威胁的迅速发现能力，最终通过应急响应实现网络安全事件的控制处置。

2.1　纵深防御能力

2.1.1　基础安全技术

基础安全技术主要是依据国家法律法规和网络安全等级保护相关标准，结合水利行业实际，充分考虑数据中心、移动互联网、园区网、网络边界、工控网及物联网等各类防护对象，围绕安全物理环境、通信网络、区域边界、计算环境等内容，满足网络安全等级保护安全合规要求，增强基础安全防护能力。

2.1.2　统一安全服务

统一安全服务主要包括以下内容：

1）统一身份认证服务。省级以上水利部门、大型及重要中型水利工程单位建立以密码和生物识别技术为基础的统一身份认证平台，为本单位及下级单位提供移动端与桌面端身份认证服务，实现统一的用户管理、身份认证、单点登录。

2）统一密码服务。省级以上水利部门、大型及重要中型水利工程单位建立符合国家密码管理部门要求的统一密码服务，为重要数据、指令的传输和存储提供密码服务。

3）统一威胁情报服务。省级以上水利部门、大型及重要中型水利工程单位建立安全情报中心，完善各级单位之间的情报交换机制，为安全威胁分析预警提供情报服务。

4）统一容灾备份服务。水利部建设同城灾备中心，实现关键业务的双活；建设异地灾备中心，实现重要数据的数据、关键业务的应用级等备份。流域管理机构共享水利部灾备中心，实现关键业务的数据级或应用级备份。省级水利部门充分依托地方政务云，实现同城和（或）异地容灾备份。

2.1.3 安全数据采集

安全数据采集主要用于采集外部网络安全情报，以及网络内安全设备、主机、应用的日志及重要边界网络流量等与网络安全相关的各类数据信息，形成威胁预警体系中进一步分析的数据基础。通过流量探针、日志服务器、API 接口等灵活适应化的数据接口部署，实现对网内安全设备、主机、应用的日志，以及重要边界网络流量、内外部威胁情报等安全相关数据采集的初步处理；通过数据清洗、范式化、归一化等数据治理技术对数据进行整理，形成有意义、可分类的安全数据。安全数据采集能力建设架构如图 2 所示。

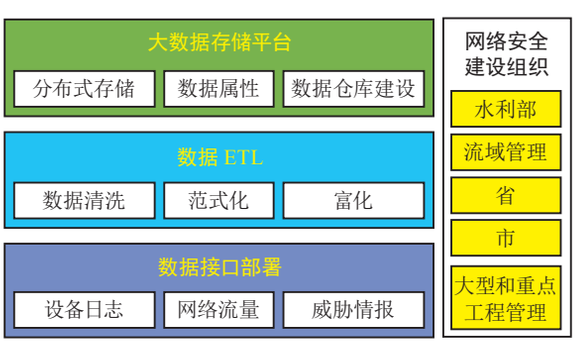

图 2 智慧水利安全数据采集能力建设架构图

2.2 监测预警能力

网络安全监测预警能力是水利网络安全由被动防御向主动控制转变的关键，架构图如图 3 所示。

2.2.1 大数据分析平台

大数据分析平台对网络安全相关各类数据进行分析计算，通过分布式存储、实时总线、模型算法基础计算框架等，为威胁感知预警等安全业务系统

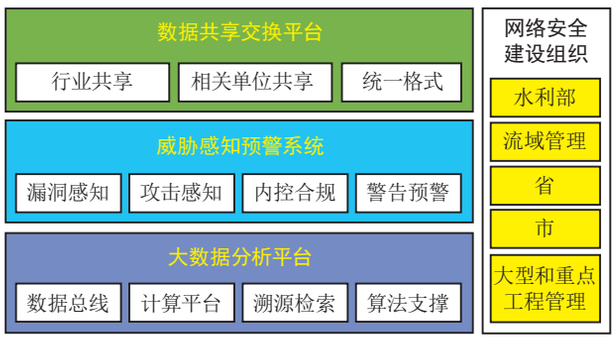

图 3 智慧水利安全监测预警能力建设架构图

提供数据、存储和计算等资源。为全面的漏洞、规则、统计、资产、知识库等的关联分析奠定基础，为各类网络安全分析模型算法提供计算引擎和数据治理能力。

2.2.2 威胁感知预警系统

省级以上水利部门、关键信息基础设施运营单位建立威胁感知预警系统，基于安全数据采集系统采集的数据，在大数据分析平台的基础上，实现海量数据快速分析、安全日志集中关联分析、异常行为分析检测、用户行为画像、攻击溯源分析等能力，实现对本级及下级单位的网络安全漏洞感知、攻击感知、内控合规和威胁告警。

在传统态势感知的算法和模型基础上，通过机器、强化学习等人工智能相关技术进一步构建各类安全威胁的数据流或模型，加强态势感知系统发现威胁的速度和准确度，提升应对未知威胁的自适应能力。

2.2.3 数据共享交换平台

数据共享交换平台实现威胁情报、安全事件、安全相关通知通告等安全信息的共享交换。省级以上水利部门、关键信息基础设施运营单位建立安全数据共享交换平台，实现相互之间及与公安、网信部门的数据共享交换；省级以下单位建立数据共享交换节点，与上级单位进行安全数据交换共享。

2.3 应急响应能力

网络安全应急响应能力是时刻维护水利网络安全，及时处置网络安全事件，控制减少网络安全威胁的重要抓手，架构图如图 4 所示。

2.3.1 集中管控平台

各级单位建设集中管控平台，实现对本单位网络安全设备设施的统一管理与控制，实现统一的网络安全设备管理安全策略编制、服务管理等，自动控制安全设备设施动作。集中管控平台是连接应急

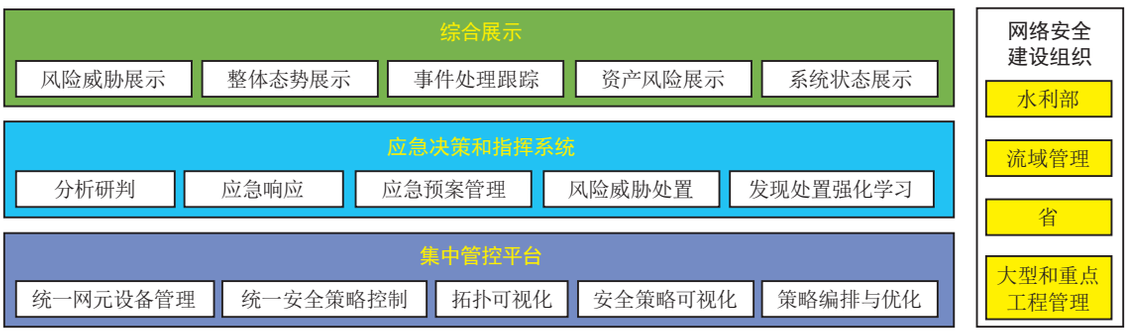

图 4　应急响应能力建设架构图

响应措施与设备系统动作的桥梁，是网络安全运维人员提升运维效率的重要基础，更是实现网络安全防御向智能化发展的中枢神经。

2.3.2　应急决策和指挥系统

省级以上水利部门、关键信息基础设施运营单位建设应急决策和指挥系统，其他单位建立基层指挥联动平台，实现与上级应急决策和指挥系统的对接，形成覆盖各级水利部门的网络安全应急响应和指挥调度体系，对安全威胁事件应急响应准备、检测、控制、恢复等进行全过程管理。在与集中管控平台实现联动的基础上，探索开展利用人工智能、强化学习等技术加强网络安全应急决策系统的自主判断和决策处置能力，逐渐由人工处理向自主处理转变。

2.3.3　综合展示

综合展示是利用可视化呈现技术，对网络安全状况、事件处置过程等进行可视化展现，主要包括以下 3 种展示：1）整体风险展示。从宏观层面展示整体安全风险状态，直观展示网络、漏洞、威胁、安全事件等安全态势，为指挥决策提供技术支撑。2）重要信息系统安全展示。以信息系统资产为核心，展示信息系统可能面临的安全风险或遭受的攻击事件，为安全运维人员进行安全监测提供技术支撑。3）事件处置过程展示。在安全应急响应过程中，针对安全事件处置流程及状态的跟踪情况，协助相关安全人员随时掌握安全事件的遏制情况。

3　网络安全管理体系

网络安全管理能力建设主要包括组织机构、人才队伍、制度规范体系等方面的建设。通过网络安全管理制度体系建设，形成高效的网络安全建设管理、运行维护、应急响应和监督检查等机制，利用统一的安全组织体系，遵照统一的安全制度体系开展工作，使各单位的网络安全管理具有统一水平，避免局部的管理漏洞 [2]。

1）组织机构建设。各单位建立健全水利网络安全工作组织机构，建设包括安全管理、运行、监督 3 个维度的安全组织体系，明确信息化和业务 2 个部门全员参与的网络安全管理机制，落实各层次角色职责，构建完善的网络安全组织机构。

2）人才队伍建设。人才队伍建设主要包括网络安全管理、运维人员等网络安全工作主要参与者的能力建设。应着力培养诸如规划设计型、规范编制型、统筹管理型的人才，以及技术专家、安全数据分析师、设备系统运行维护专家等方面的水利网络安全人才。逐渐培养打造懂业务、系统、安全的水利网络安全和信息化支撑人才队伍，为智慧水利建设提供智力支撑。

3）制度规范体系建设。以合规合法、责任到人为中心，建立由办法、制度、规范、流程和规程构成的网络安全管理制度标准体系，覆盖网络安全组织、人员、建设、运维的管理，以及应急响应和监督检查等各项工作。制度规范体系是水利网络安全管理体系的重要组成部分，为网络安全管理提供依据和行为准则。制度规范体系建设主要包括识别现有的法律法规、标准规范，在工作中落地实施，及完善安全标准体系等 2 个层面的工作。

4　网络安全运营体系

网络安全运营是网络安全各类技术支撑落地，切实防范处理安全预警威胁，充分发挥人在体系中主观能动性的核心，是网络安全能力提升的直接表现。各单位开展网络安全运营机制建设，依托网络安全技术体系，依据网络安全管理体系，开展日常

分析预测、威胁防护、持续监测、响应处置等网络安全运营工作，形成闭环安全运营体系，有效保障网络安全技术、管理要求落地，网络安全运营体系框架如图 5 所示。

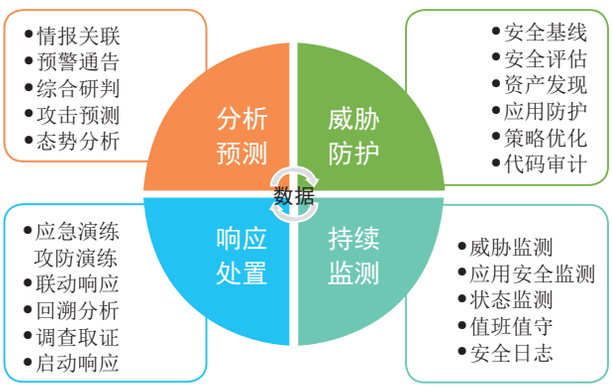

图 5 网络安全运营体系架构图

1）分析预测。从攻击预测的角度进行资产发现，梳理基础设备信息、开放端口信息、部署应用类型等，掌握信息资产运行情况；定期开展主机、网络、应用、终端的安全检查整改；与威胁情报进行关联发出预警等。

2）威胁防护。主要进行以下几方面的防护：a. 从事件预防的角度开展对主机、设备、应用的安全基线评估加固工作，发现存在的安全风险及防护的短板，通过安全加固增强内外部防护能力。b. 开展安全产品运行维护，包括产品、系统维护，安全审计日志分析及配置备份更新等内容，保障安全产品高效可靠的运行。c. 基于预测及安全基线评估，发现安全策略不足，对防护体系进行防护能力的优化提升；对访问控制进行优化增强访问控制，杜绝越权访问带来的威胁；对行为审计进行优化，实现全面审计无“死角”，达到安全策略优化效果。d. 开展系统上线及周期性安全检查，避免系统“带病”上线及运行影响全局。e. 实现安全事件可预防。

3）持续监测。从事件监测的角度持续开展应用失陷监测，发现存在的各类漏洞并进行验证，经确认后及时整改；通过对终端日志分析发现账户安全、恶意文件、邮件病毒、APT、非法外联等事件，快速验证并进行改进。多层次全面持续监测动态发现威胁快速定位。

4）响应处置。从事件控制的角度对出现的安全事件迅速开展研判分析，为安全应急响应提供决策依据，响应处置内容包括抑制、清除、恢复，并形成处置报告。定期开展安全检查，发现安全隐患，快速整改，重点时期安排技术人员安全值守，保障全程安全；必要时开展网络安全攻防演练，检验安全技术、管理、运营体系的健壮性，提高安全保障能力。

5 结语

“水利工程补短板、水利行业强监管”已成为新时期水利工作的总基调，坚持问题导向，对标“安全、实用”的水利信息化发展总要求，在智慧水利建设的设计、实施、运行等阶段，要切实提高对网络安全的认识，同步规划、推进、加强网络安全体系的建设。在网络安全威胁感知和应急响应方面更要加强行业的统筹联动，整体性提高水利行业的网络安全防护水平，更好地保障以大数据、云计算、物联网、移动互联网、人工智能等新技术为基础的智慧水利健康发展。

参考文献：

[1] 蔡阳. 贯彻《网络安全法》构建水利网络安全保障体系[J]. 水利信息化，2017 (3): 1-4.

[2] 詹全忠，陈岚. 水利部本级信息系统安全等级保护整改设计[J]. 信息网络安全，2012 (2): 84-86.

[3] 陈岚，周维续. 水利网络安全监测与预警方法[J]. 水利信息化，2017 (3): 29-32.

[4] 水利部网络安全与信息化领导小组办公室. 智慧水利总体方案[R]. 北京：水利部网络安全与信息化领导小组办公室，2019.

[5] 詹全忠. 水利网络与信息安全资源整合共享探讨[J]. 水利信息化，2014 (6): 22-26.

Cyber security in Smart Water Conservancy general scheme

ZHAN Quanzhong, ZHANG Chao

(*Water Resources Information Center*, *the Ministry of Water Resources*, *Beijing* 100053, *China*)

Abstract: In recent years, cyber security has been developed rapidly in water industry, which guaranteed the secure running of many important business systems, such as systems of prevention of flood and drought disasters, water

（下转第 29 页）