ICS 35.100.01
CCS 6450

T/CAICI

中 国 通 信 企 业 协 会 团 体 标 准

T/CAICI XXXX—XXXX

网络安全中台体系架构

Network security mid-platform architecture

（征求意见稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中国通信企业协会　　发 布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由中国通信企业协会团体标准管理委员会提出并归口。

本文件主要起草单位：河北电信设计咨询有限公司

本文件主要起草人：杨欣宇、张丁丁、韩娜

本文件为首次发布。

引　言

本文件的制定，适用于网络运营者网络安全体系的规划建设，用于提升网络安全威胁发现、监测预警、应急指挥、攻击溯源等能力，支撑网络安全运营工作，提升网络安全服务水平。

本文件的编制以贯彻国家基本建设方针政策和技术经济政策为主，密切结合通信发展的实际，重在提升资源效益合理性。

本文件的发布机构提请注意，声明符合本文件时，可能涉及到相关的专利的使用。

本文件的发布机构对于该专利的真实性、有效性和范围无任何立场。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

网络安全中台体系架构

1 范围

本文件规定了网络运营者网络安全中台的体系架构，涉及网络安全中台的体系架构设计要求、体系架构设计框架、体系架构安全能力要求等方面。

本文件适用于指导网络运营者网络安全领域的规划建设工作。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

《中华人民共和国网络安全法》

《中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要》

《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》

3 术语和定义

下列术语和定义适用于本文件。

3.1

网络安全

指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

3.2

网络运营者

指网络的所有者、管理者和网络服务提供者。

4 网络安全中台体系架构

本文件对网络安全中台应该具备的架构要求、架构框架、安全能力要求进行了说明。架构框架包括数据采集层、数据处理层、安全能力层、能力编排层和能力应用层。安全能力要求主要包括网络安全能力和信息安全能力两大类，具体包括数据采集能力、数据处理能力、数据存储能力、数据分析能力、数据溯源能力、集约管控能力、集约调度能力、威胁发现能力、监测预警能力、攻击溯源能力、数据管控能力、安全编排能力、安全封装能力、安全调用能力、可视化统一展现能力、安全产品服务提供能力等。

4.1 体系架构设计要求

4.1.1 整体系统架构要求

1） 应具备安全性。
2） 应具备灵活性。
3） 应具备开放性。
4） 应具备扩展性。
5） 应具备高可用性。
6） 应具备标准接口能力。
7） 应加强云化部署程度。
8） 应加强自动化部署能力。
9） 应加强安全服务组件化能力。
10）应加强安全组件解耦合程度。
11）应加强安全组件智能协同联动能力。

4.1.2 能力提供形态要求

1）应支持多形态安全能力提供形式。
2）应加强软件定义安全能力。
3）应加强安全与服务结合能力。

4.1.3 总体功能要求

1）应具备集约管控能力。
2）应具备集约调度能力。
3）应具备集约编排能力。
4）应具备个性化需求的安全提供能力。
5）应具备面向新场景新业务的安全提供能力。
6）应具备安全开放能力。
7）应具备安全复用能力。

4.2 体系架构设计框架

网络安全中台体系架构设计框架主要包括数据采集层、数据处理层、安全能力层、能力编排层和能力应用层。

网络安全中台应集分析、研判、预警、响应、评估功能为一体，可整合已有的网络信息安全系统和设备，汇聚分析共享各系统安全数据，提升网络安全威胁发现、监测预警、应急指挥、攻击溯源等能力，支持能力调用、能力封装、能力调度，实现安全工作可视化统一门户展现。

网络安全中台体系架构设计框架如下图所示：

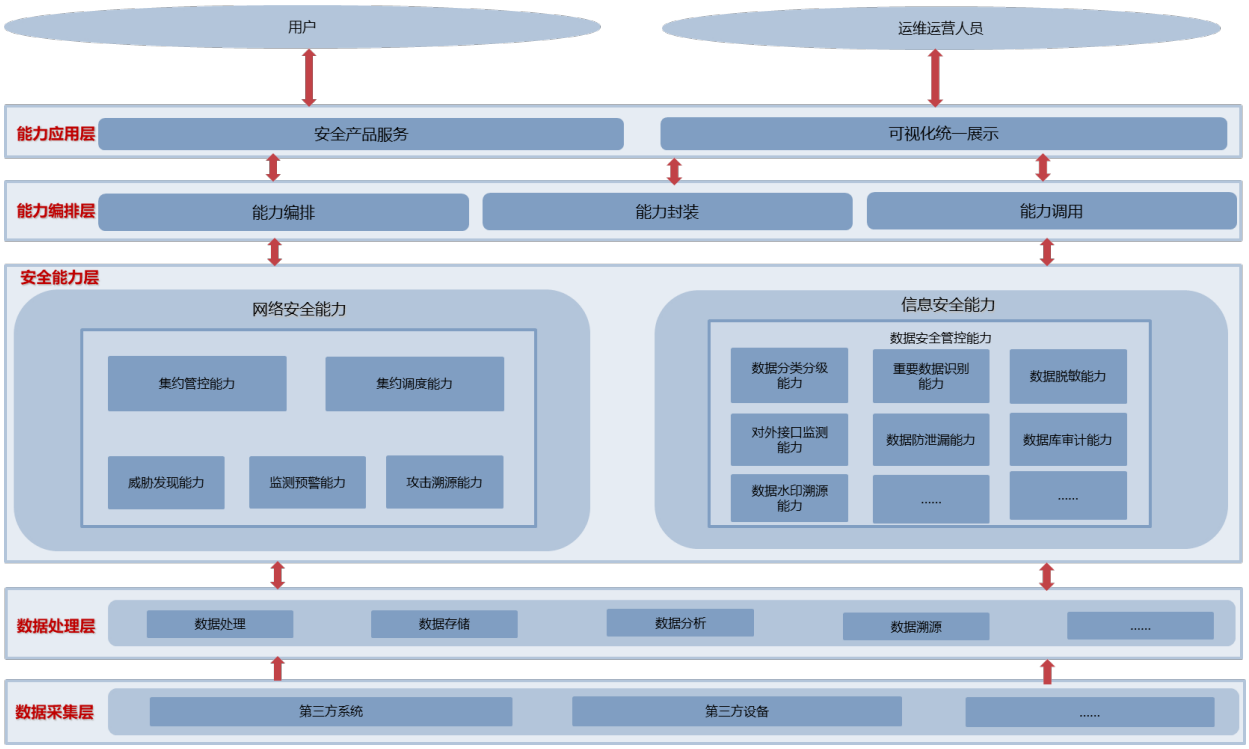

图1：网络安全中台体系架构框架

4.2.1 数据采集层

数据采集层可采集第三方系统或第三方设备的安全数据。

4.2.2 数据处理层

数据处理层包括数据处理、数据存储、数据分析、数据溯源等。

4.2.3 安全能力层

能力层包括网络安全能力和信息安全能力。

4.2.4 能力编排层

编排层包括能力编排、能力封装、能力调用等。

4.2.5 能力应用层

能力应用层包括安全产品服务提供能力和可视化统一展现能力等。

4.3 体系架构安全能力要求

4.3.1 数据采集能力

1）应支持多种采集协议，如FTP、WebService等。

2）应支持多种采集方式，如主动采集、被动采集等。
3）应支持多种数据采集，如日志数据采集、流量数据采集、网管数据采集等。
4）应支持自适应解析能力。

4.3.2 数据处理能力

1）应具备异构数据处理能力。
2）应具备数据预处理能力，包括数据清洗、数据修改、数据删除等。
3）应具备数据标准化能力，可对异构原始数据进行统一格式化处理。
4）应具备数据关联补齐能力，采集数据通过关联补齐后可形成完整数据。
5）应具备数据检索能力，可支持组合查询检索。

4.3.3 数据存储能力

1）应具备数据实时存储能力。
2）应具备数据实时检索能力。
3）应保证存储数据的可用性、完整性和保密性。

4.3.4 数据分析能力

1）可支持大数据、AI等技术进行数据分析。

4.3.5 数据溯源能力

1）可支持通过特定条件进行快速检索、在线解析。
2）可支持解析网络协议内容。

4.3.6 集约管控能力

1）应具备汇聚多源异构安全监测数据能力。
2）应具备融合多源异构安全监测数据能力。
3）应具备集约管控多源异构安全监测数据能力。
4）应具备业务生命周期管理能力。
5）应统一网络安全监测数据自身的数据安全保护标准。
6）应可作为统一数据出口，对接相关系统。
7）应可按照规定格式提交数据。

4.3.7 集约调度能力

1）应实现主动安全探测能力和被动安全探测能力的联动。
2）应实现自动化安全工作的统一管理与调度。
3）应支持闭环管理处置流程。
4）应具备实时监控能力。可对任务过程每个环节进行检查与复核。
5）应具备异构管理能力。支持对异构检测工具的集中管理。

4.3.8 威胁发现能力

1）应支持主动威胁发现和被动威胁发现。
2）应支持对异构检测工具的集中管理。
3）主动威胁发现可主动采集最新漏洞数据并进行流程化处理。
4）主动威胁发现应支持全面发现系统脆弱性问题。
5）主动威胁发现应支持从海量数据中快速定位风险。

6）主动威胁发现应支持在非虚拟化环境和虚拟化环境中部署和检测。
7）被动威胁发现可通过采集设备解码网络流量。
8）被动威胁发现可检测多种攻击行为。
9）被动威胁发现可识别网络攻击行为。
10）被动威胁发现可支持对行为信息和告警信息的快速存储和快速搜索。
11）被动威胁发现可支持根据攻击阶段进行结果过滤。
12）被动威胁发现可支持图形化威胁态势展示。

4.3.9 监测预警能力

1）应具备安全态势感知能力。
2）应具备安全资产管控能力。
3）应支持多视角多纬度的监测能力。

4.3.10 攻击溯源能力

1）应具备网络攻击行为溯源能力。
2）应具备安全数据溯源分析。

4.3.11 数据管控能力

1）应具备数据分类分级能力。可实现对数据资产的识别和分级管理。
2）应具备重要数据识别能力。依据规则将重要数据进行归类。
3）应具备数据脱敏能力。可通过脱敏规则定义相关策略。
4）应具备对外接口管控能力。保障数据的合规使用，防范敏感数据泄漏。
5）应具备数据水印溯源能力。可对文件数据进行水印标识。
6）应具备数据库审计能力。可实现对数据库异常访问的预警。
7）应具备数据防泄漏能力。可实现数据导入导出渠道的实时监控。

4.3.12 安全编排能力

1）应具备业务编排能力。
2）应具备流量编排能力。

4.3.13 安全封装能力

1）应可按需进行安全能力封装。

4.3.14 安全调用能力

1）应可按需进行安全能力调用。
2）应具备标准接口能力。

4.3.15 可视化统一展现能力

1）应支持多维度统一展现能力。
2）应具备运营和运维门户。支持用户管理、能力管理等。
3）应具备用户门户。支持用户对安全能力的浏览、选择和使用。
4）应支持权限管理。
5）可辅助各类安全事件的分析、研判及处置。

4.3.16 安全产品服务提供能力

1）应可按需提供个性化安全产品服务。
2）应加强安全产品服务间的智能协同联动能力。