ICS 35.110
CCS L 78

团　体　标　准

T/WAPIA 054—2025

高质量安全无线局域网 总体要求

Secure wireless local area network with high quality—General requirements

2025-12-30 发布　　2025-12-30 实施

中关村无线网络安全产业联盟　发 布

版权声明

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。

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。

本文件由中关村无线网络安全产业联盟与工业和信息化部宽带无线IP标准工作组联合提出。

本文件由中关村无线网络安全产业联盟无线网络安全标准化工作委员会归口。

本文件起草单位：中关村无线网络安全产业联盟、无线网络安全技术国家工程研究中心、西安西电捷通无线网络通信股份有限公司、北京数字认证股份有限公司、国家无线电监测中心检测中心、广州莲雾科技有限公司、北京华信傲天网络技术有限公司、国网山东省电力公司、西安芯语慧联信息科技有限公司、新华三技术有限公司、南方电网数字电网科技（广东）有限公司、海南电网有限责任公司、深圳市国电科技通信有限公司、深圳鼎信通达股份有限公司、工业和信息化部宽带无线IP标准工作组。

本文件主要起草人：黄振海、杜志强、张国强、侯鹏亮、尹玉昂、吴泽雄、简练、张璐璐、苑超、张强、郑骊、童伟刚、李培、李楠、潘琪、王立华、刘剑昕、刘婷、于双双、周园、牛彬、段铭哲、张变玲、颜湘、李仲斌、韩曦、周华旭、李博、王学良、顾善中、付美明。

高质量安全无线局域网 总体要求

1 范围

本文件确立了高质量安全无线局域网的总体架构，规定了识别认定、网络建设、监测预警、检测评估、主动防御和应急处置等要求。

本文件适用于无线局域网产品、网络和服务。

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。

GB 15629.11（所有部分） 信息技术 系统间远程通信和信息交换 局域网和城域网 特定要求 第11部分：无线局域网媒体访问控制和物理层规范

GB/T 20984 信息安全技术 信息安全风险评估方法

GB/T 32420—2015 无线局域网测试规范

T/WAPIA 007.1 无线局域网产品工程化实现指南 第1部分：WAPI与IEEE 802.11n

T/WAPIA 007.8 无线局域网产品工程化实现指南 第8部分：WAPI与IEEE 802.11ac

T/WAPIA 007.9 无线局域网产品工程化实现指南 第9部分 ：WAPI与IEEE 802.11ad

T/WAPIA 007.10 无线局域网产品工程化实现指南 第10部分：WAPI与IEEE 802.11ax

T/WAPIA 007.11 无线局域网产品工程化实现指南 第11部分：WAPI与IEEE 802.11be

T/WAPIA 010.2 信息技术 系统间远程通信和信息交换 局域网和城域网 特定要求 第11部分：无线局域网媒体访问控制和物理层规范 第2号修改单：无线局域网证书鉴别漫游规范

T/WAPIA 010.3 信息技术 系统间远程通信和信息交换 局域网和城域网 特定要求 第11部分：无线局域网媒体访问控制和物理层规范 第3号修改单：管理帧保护技术规范

T/WAPIA 013.2 信息安全技术 数字证书管理 第2部分：证书存储和使用

T/WAPIA 013.3 信息安全技术 数字证书管理 第3部分：证书颁发

T/WAPIA 013.4 信息安全技术 数字证书管理 第4部分：证书撤销

T/WAPIA 013.5 信息安全技术 数字证书管理 第5部分：证书格式

T/WAPIA 036.1 WAPI应用接口规范 第1部分：移动终端

T/WAPIA 037.2 无线局域网测试 第2部分：设备测试规范

T/WAPIA 038 信息安全技术 终端实体证书管理

T/WAPIA 046 无线局域网安全技术规范

T/WAPIA 047.1 无线局域网系统规范 第1部分：工程设计

T/WAPIA 047.2 无线局域网系统规范 第2部分：工程施工

T/WAPIA 047.3 无线局域网系统规范 第3部分：验收测试方法

T/WAPIA 048 信息系统无线局域网密码应用基本要求

T/WAPIA 049 传感器类设备专用WLAN通信模块技术规范

T/WAPIA 050 工业串口类设备专用WLAN通信模块技术规范

T/WAPIA 052.2 无线局域网设备技术规范 第2部分：终端

T/WAPIA 052.3 无线局域网设备技术规范 第3部分：接入点和接入控制器

T/WAPIA 052.4 无线局域网设备技术规范 第4部分：鉴别服务器

T/WAPIA 052.5 无线局域网设备技术规范 第5部分：证书签发服务器

3 术语和定义

下列术语和定义适用于本文件。

3.1

安全 security

对某一系统，具有获得保密性、完整性、可用性、可核查性、真实性以及可靠性的性质。

[来源：GB/T 25069—2022，3.1]

3.2

等级测评 testing and evaluation for classified cybersecurity protection

测评机构依据国家网络安全等级保护制度规定，按照有关管理规范和技术标准，对非涉及国家秘密的网络安全等级保护状况进行检测评估的活动。

[来源：GB/T 28448—2019，3.6]

3.3

第三方 third party

就所涉及的问题而言，公认与相关各方均独立的个人或团体。

[来源：GB/T 25069—2022，3.116]

3.4

风险 risk

对目标的不确定性影响。

注 1：影响是指与期望的偏离（正向的或反向的）。

注 2：不确定性是对事态及其结果或可能性的相关信息、理解或知识缺乏的状态（即使是部分的）。

注 3：风险常被表征为潜在的事态和后果，或者它们的组合。

注 4：风险常被表示为事态的后果（包括情形的改变）和其发生可能性的组合。

注 5：在信息安全管理体系的语境下，信息安全风险可被表示为对信息安全目标的不确定性影响。

注 6：信息安全风险与威胁利用信息资产或信息资产组的脆弱性对组织造成危害的潜力相关。

[来源：GB/T 29246—2017，2.68]

3.5

高质量安全无线局域网 secure wireless local area network with high quality

符合了本文件对产品、网络和服务的质量评价要求的无线局域网。

注：高质量包括网络服务的高质量、网络运行的高质量、网络建设过程的高质量、产品的高质量、产品模块的高质量、基础技术和工程技术的高质量。

3.6

关键信息基础设施（关基） critical information infrastructure

公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等。

[来源：GB/T 39204—2022，3.1]

3.7

供应链 supply chain

将多个资源和过程联系在一起，并根据服务协议或其他采购协议建立连续供应关系的组织系列。

注：其中每一组织充当需方、供方或双重角色。

[来源：GB/T 39204—2022，3.2]

3.8

核查 examine

测评人员通过对测评对象（如制度文档、各类设备及相关安全配置等）进行观察、查验和分析，以帮助测评人员理解、澄清或取得证据的过程。

[来源：GB/T 28448—2019，3.2]

3.9

极限情况 extreme conditions

遭遇到大规模、有组织、持续的网络攻击或严重自然灾害等，对网络运行环境、网络运行秩序产生巨大、破坏性影响，包括但不限于通信设施、电力、机房等环境因素遭到破坏对网络设施、信息系统造成影响。

3.10

接入点 access point

任何一个具备无线局域网站点功能，通过无线媒体为关联的站点提供访问分布式服务的能力的实体。

[来源：GB 15629.11—2003，3.2]

3.11

接入点控制器 AP controller

提供对AP的集中控制管理、包括版本下发、配置下发、射频管理和用户流量管理等。

[来源：GB/T 32420—2015，3.1]

3.12

评估 assessment

对于某一产品、系统或服务，对照某一标准，采用相应的方法，以建立合规性并确定其所做是否得到确保的验证。

[来源：GB/T 25069—2022，3.446，有修改]

3.13

评价 evaluation

实体满足其规定准则程度的系统性判定。

[来源：GB/T 25069—2022，3.447]

3.14

商用密码应用安全性评估（密评） commercial cryptographic application security assessment

在采用商用密码技术、产品和服务集成建设的网络和信息系统中，对其密码应用的合规性、正确性和有效性进行评估。

注：《中华人民共和国密码法》提出，密码是保障网络与信息安全的核心技术和基础支撑，并明确要求关键信息基础设施使用密码保护，并要求开展密码应用安全性评估(简称“密评”)。

3.15

设备 device

具有特定用途的机械、电气或电子装置。

[来源：GB/T 25069—2022，3.507]

3.16

实体 entity

存在或者可能存在的任何具体或抽象的事物，包括这些事物间的关系。

示例：人、对象、事件、理念、过程。

注：实体的存在和与之有关的数据是否可用无关。

[来源：GB/T 25069—2022，3.550]

3.17

网络安全 network security

对网络环境下存储、传输和处理的信息的保密性、完整性和可用性的保持。

[来源：GB/T 25069—2022，3.616]

3.18

网络安全等级保护（等保） classified protection of cybersecurity

对网络（含信息系统、数据）实施分等级保护、分等级监管、对网络中使用的网络安全产品实行按等级管理，对网络中发生的安全事件分等级响应、处置。其中“网络”是指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统，包括网络设施、信息系统、数据资源等。

注：术语及翻译来源于GB/T 22239—2019标准名称。《中华人民共和国网络安全法》明确了国家实行网络安全等级保护制度。

3.19

网络空间安全 cybersecurity

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。

[来源：GB/T 22239—2019，3.1]

3.20

无线局域网 wireless local area network

用于局部区域范围内固定式、便携式与移动式站点使用射频信号连通、交换数据的网络，涉及的网络实体包括站点（STA）、接入点（AP）、接入点控制器（AC）、鉴别服务器（AS）、证书签发服务器（CIS）等。在中国符合GB 15629.11系列国家及相关行业和团体标准。

3.21

无线局域网保密基础结构 WLAN privacy infrastructure

用于无线局域网中数据传输保护的安全方案，包括数据加密、数据鉴别和重放保护等功能。

[来源：T/WAPIA 046—2021，3.27]

3.22

无线局域网鉴别基础结构 WLAN authentication infrastructure

用于无线局域网接入控制的身份鉴别和密钥管理安全方案。

[来源：T/WAPIA 046—2021，3.21]

3.23

无线局域网鉴别与保密基础结构 wireless local area network authentication and privacy infrastructure

由无线局域网鉴别基础结构（WAI）和无线局域网保密基础结构（WPI）组成，为无线局域网接入点、终端提供对等身份鉴别和数据机密性服务。

[来源：T/WAPIA 046—2021，3.22]

注：WAPI技术规范见GB 15629.11（所有部分）和T/WAPIA 046。

3.24

无线局域网设备 WLAN equipment

包含符合GB 15629.11（所有部分）媒体访问控制和物理层规范的无线局域网装置。

3.25

无线局域网终端 WLAN terminal

包含符合GB 15629.11（所有部分）媒体访问控制和物理层规范的无线局域网STA功能模块的设备。

3.26

信息技术安全性评估通用准则 common criteria for information technology security evaluation

评估信息技术产品和系统安全性所需的基础准则，是度量信息技术安全性的基准。

3.27

信息系统 information system

应用、服务、信息技术资产或其他信息处理组件的组合。

[来源：GB/T 25069—2022，3.696]

3.28

站点 station

包含WLAN无线媒体的MAC和PHY接口的任何设备。

[来源：GB 15629.11—2003，3.42，有修改]

3.29

证书签发服务器 certificate issue server

对无线局域网终端、无线接入点和鉴别服务器提供证书签发管理服务的设备。

注：该管理服务包括证书签发、证书吊销列表签发、证书吊销、证书查询和证书更新等。

[来源：T/WAPIA 040.1—2021，3.3，有修改]

3.30

证书认证机构 certificate authority

对数字证书进行全生存周期管理的实体。

[来源：GB/T 25069—2022，3.785]

3.31

终端实体证书管理 certificate management for end entity

对终端实体证书进行管理涉及的安全操作。

示例：涉及的安全操作包括证书的申请、更新、恢复、撤销、查询和获取等。

注：终端实体证书管理技术规范见T/WAPIA 038。

3.32

组件 component

根据结构或功能划分的系统组成部分，仍然能实现独立的子功能。

4 缩略语

下列缩略语适用于本文件。

AC 接入点控制器（AP Controller）
AP 接入点（Access Point）
AS 鉴别服务器（Authentication Server）
CIS 证书签发服务器（Certificate Issue Server）
CMEE 终端实体证书管理（Certificate Management for End Entity）
FTP 文件传输协议（File Transfer Protocol）
HTTP 超文本传输协议（HyperText Transfer Protocol）
MAC 媒体访问控制（Medium Access Control）
SMTP 简单邮件传输协议（Simple Mail Transfer Protocol）
SNMP 简单网络管理协议（Simple Network Management Protocol）
STA 站点（STAtion）
Telnet 远程登录网络（Teletype network）
TFTP 简单文件传输协议（Trivial File Transfer Protocol）
WAI 无线局域网鉴别基础结构（WLAN Authentication Infrastructure）
WAPI 无线局域网鉴别与保密基础结构（WLAN Authentication and Privacy Infrastructure）
WLAN 无线局域网（Wireless Local Area Network）
WPI 无线局域网保密基础结构（WLAN Privacy Infrastructure）

5 通则

5.1 高质量安全 WLAN 基础架构

高质量安全WLAN，应从高质量产品模块、高质量产品、高质量网络建设、高质量网络运行和高质量网络服务五方面进行评价，高质量安全WLAN基础架构见图1。

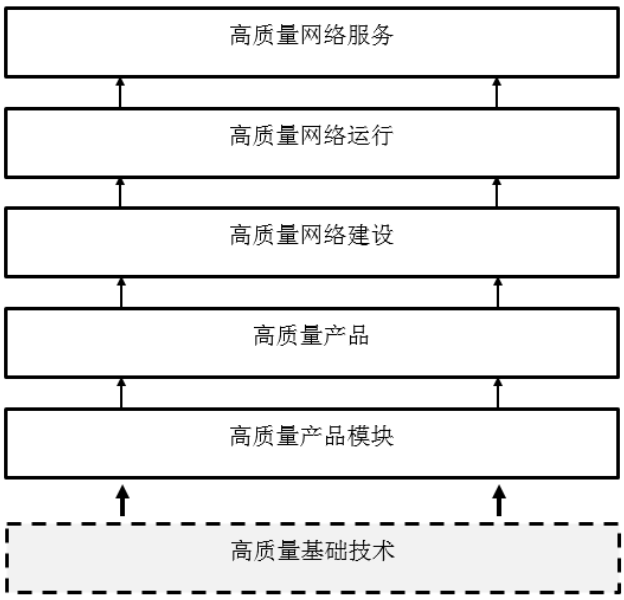

图 1 高质量安全 WLAN 基础架构

5.2 高质量安全 WLAN 技术标准体系

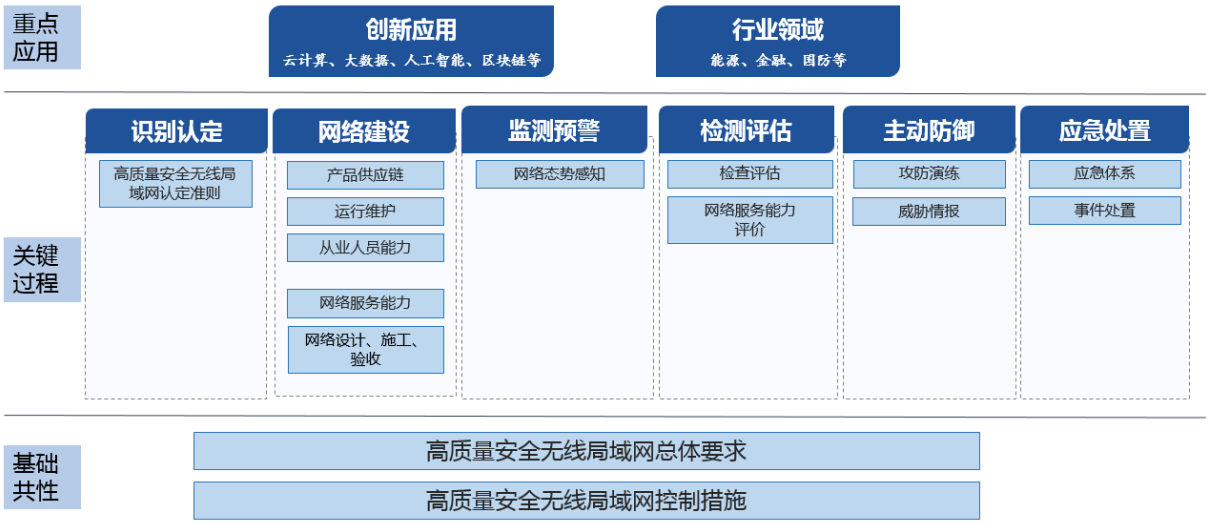

图 2 高质量安全 WLAN 技术标准体系

高质量安全WLAN技术标准体系见图2，包含基础共性、关键过程和重点应用三个层次的标准。其中，关键过程包括识别认定、网络建设、监测预警、检测评估、主动防御和应急处置六个方面：

a） 识别认定：围绕高质量安全 WLAN 服务、运行、建设和产品，开展依赖性识别、关键资产识别和风险识别等活动，包括演进中的技术风险和管理风险，如量子计算产生的潜在威胁。本过程是网络建设、监测预警、检测评估、主动防御和应急处置等过程的基础；

b） 网络建设：在高质量安全 WLAN 的建设和运维管理等方面实施安全管理和技术保护措施，包括网络高质量扩容，提升 WLAN 建设质量；

c） 监测预警：建立并实施网络监测预警和信息通报制度，针对发生的网络安全事件或发现的网络安全威胁，提前或及时发出安全警示。建立针对 WLAN 的漏洞库等威胁情报和信息共享机制，落实相关措施，提高对网络攻击的主动发现能力；

d） 检测评估：为检验保障网络服务、运行、建设和产品高质量措施的有效性，发现网络安全风险隐患，应建立相应的检测评估制度，确定检测评估的流程及内容等，开展安全检测与风险隐患评估，分析潜在安全风险可能引发的安全事件；

e） 主动防御：以应对网络攻击行为的监测发现为基础，主动采取收敛暴露面、捕获、溯源、干扰和阻断等措施，开展攻防演习和威胁情报工作，提升对网络威胁与攻击行为的识别、分析和主动防御能力；

f） 应急处置：网络运营者对网络安全事件进行报告和处置，并采取适当的措施，恢复由于网络安全事件而受损的功能或服务。

6 识别认定

6.1 概述

围绕高质量安全WLAN服务、运行、建设和产品，开展依赖性识别、关键资产识别和风险识别等活动，包括演进中的技术风险和管理风险，如量子计算产生的潜在威胁。制定适宜的检测评估方法，对WLAN服务、运行、建设、产品和模块进行质量分析，确定符合需求的程度，进行认定。

识别认定过程是网络建设、监测预警、检测评估、主动防御和应急处置等过程的基础。

6.2 关键活动

风险识别：应按GB/T 20984的要求，对WLAN关键业务链开展安全风险和质量依赖性分析，识别关键业务链各环节的威胁、脆弱性，分析主要安全风险点，确定风险处置的优先级，制定新的或者确认已有控制措施。

认定：应制定适宜的检测评估方法，对WLAN服务、运行、建设、产品、模块和技术进行质量分析，确定满足需求的程度。

变更：在WLAN服务、运行、建设、产品、模块和技术发生较大变化时，应重新开展识别和认定工作。

6.3 识别的关键要素

高质量安全WLAN，应符合现行有效的国家标准、行业标准、团体标准及对应的企业标准。

高质量安全WLAN，应具备数据链路层安全能力，包括身份鉴别与保密通信安全能力。

高质量安全WLAN，应以数字证书身份为基础进行身份鉴别，且数字证书所对应的私钥应被保护，私钥全生存周期均应在独立的硬件媒体中，私钥不能离开硬件安全媒体。

高质量安全WLAN，应维持其数据链路层安全能力不降级，产品所采用的WLAN芯片本身应具备片内安全能力，即保密通信阶段的数据加解密应在射频芯片中完成。

6.4 高质量安全 WLAN 能力指标体系

6.4.1 能力指标结构描述

高质量安全WLAN能力指标采用“类-族-组件”层次化的结构来表达，其层次关系见图3。

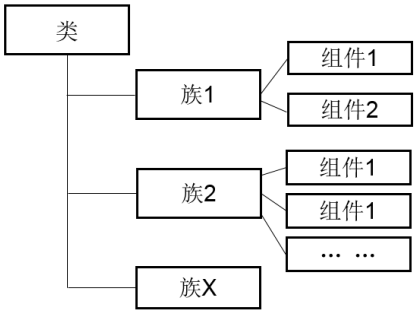

图 3 类-族-组件层次关系

一个能力类包括若干个能力族，每个能力族包括若干个能力组件，每个能力组件包括一个或多个指标项。能力类是最通用的一组能力指标的组合，能力类的编号为类别名称英文首字母缩写。

每个能力类包括若干个具有相同意图的能力族，即能力族是在能力类别框架下进一步的分类，每个能力族被分配了一个唯一的族名，能力族的表示方式是所在类名的缩写、“_”和与族名有关的若干个字母按先后顺序的组合。

每个能力族包括若干个能力组件。组件的表达方式是在族名的缩写后加一个点，然后根据组件在族内的顺序从 1 开始编号。组件的定义是围绕能力族的安全目的进行分类描述，这是能力分级的基础。

如各能力指标项的表述不足以表达高质量安全WLAN的完整要求，实施者可在类和族的框架下扩展相应的组件，扩展组件的表述应在需要扩展的族下面在族名缩写的后面补充“.EXT”后再对扩展组件排序，如：在针对高质量模块类的合规能力族下扩展组件，组件的名称可命名为“HM_CC _EXT.1”。实施者也可采取不扩展组件的方式，仅针对既有能力组件存在不适用的情况进行标注说明等方式。

6.4.2 能力指标体系构成

高质量安全WLAN能力指标体系包括5个类、12个族，见表1。基于高质量安全WLAN的质量评价要求，本文件定义了5个类，分别为高质量模块（HM）类、高质量产品（HP）类、高质量建设（HC）类、高质量运行（HO）类和高质量服务（HS）类。

表1 指标体系构成

能力类	能力族	能力组件	说明	是否区分不同能力等级
HM：高质量模块类	HM_CC：合规能力	HM_CC.1 符合 T/WAPIA 049（适用于传感器类设备专用 WLAN 通信模块）		否
		HM_CC.2 符合 T/WAPIA 050（适用于工业串口类设备专用 WLAN 通信模块）		否
		HM_CC.3 具有符合国家密码主管部门批准的 WLAN 专用商密算法能力（国家密码管理局第 7 号公告）		否
		HM_CC.4 具有符合国家密码主管部门批准的通用商密算法能力（SM2/3/4）		否
	HM_KSC：密码安全能力	HM_KSC.1 私钥应产生和存在于硬件安全媒体中	低功耗 WAPI 模组，采用的硬件安全媒体应具备符合国家密码主管部门批准的 WLAN 算法运算能力	否
		HM_KSC.2 密码运算中私钥不泄露	低功耗 WAPI 模组，采用的硬件安全媒体应具备符合国家密码主管部门批准的 WLAN 算法运算能力	否
HP：高质量产品类	HP_CC：合规能力	HP_CC.1 符合 GB 15629.11（所有部分）《信息技术　系统间远程通信和信息交换　局域网和城域网　特定要求　第 11 部分：无线局域网媒体访问控制和物理层规范》		否
		HP_CC.2 符合 T/WAPIA 046《无线局域网安全技术规范》		否
		HP_CC.3 符合 T/WAPIA 037.2《无线局域网测试 第 2 部分：设备测试规范》的要求。 注：T/WAPIA 037.2 引用了 GB/T 32420—2015	WLAN 设备测试的基本框架和方法，为测试设备提供依据	否
		HP_CC.4 符合 T/WAPIA 052.2《无线局域网设备技术规范　第 2 部分：终端》（适用于终端产品）	WLAN 设备的功能、性能，物理层技术要求和测试方法	否
		HP_CC.5 符合 T/WAPIA 052.3《无线局域网设备技术规范　第 3 部分：接入点和接入控制器》（适用于接入点和接入控制器产品）		否

表1 （续）

能力类	能力族	能力组件	说明	是否区分不同能力等级
HP：高质量产品类	HP_CC：合规能力	HP_CC.6 符合 T/WAPIA 052.4《无线局域网设备技术规范 第 4 部分：鉴别服务器》（适用于鉴别服务器产品）		否
		HP_CC.7 符合 T/WAPIA 052.5《无线局域网设备技术规范 第 5 部分：证书签发服务器》（适用于证书签发服务器产品）		否
		HP_CC.8 符合 T/WAPIA 007.1《无线局域网产品工程化实现指南 第 1 部分：WAPI 与 IEEE 802.11n》		否
		HP_CC.9 符合 T/WAPIA 007.8《无线局域网产品工程化实现指南 第 8 部分：WAPI 与 IEEE 802.11ac》		否
		HP_CC.10 符合 T/WAPIA 007.9《无线局域网产品工程化实现指南 第 9 部分：WAPI 与 IEEE 802.11ad》		否
		HP_CC.11 符合 T/WAPIA 007.10《无线局域网产品工程化实现指南 第 10 部分：WAPI 与 IEEE 802.11ax》		否
		HP_CC.12 符合 T/WAPIA 007.11《无线局域网产品工程化实现指南 第 11 部分：WAPI 与 IEEE 802.11be》		否
		HP_CC.13 符合 T/WAPIA 010.2《信息技术 系统间远程通信和信息交换 局域网和城域网 特定要求 第 11 部分：无线局域网媒体访问控制和物理层规范 第 2 号修改单：无线局域网证书鉴别漫游规范》		否
		HP_CC.14 符合 T/WAPIA 010.3《信息技术 系统间远程通信和信息交换 局域网和城域网 特定要求 第 11 部分：无线局域网媒体访问控制和物理层规范 第 3 号修改单：管理帧保护技术规范》		否
		HP_CC.15 符合 T/WAPIA 013.2《信息安全技术 数字证书管理 第 2 部分：证书存储和使用》		否
		HP_CC.16 符合 T/WAPIA 013.3《信息安全技术 数字证书管理 第 3 部分：证书颁发》		否

表1 （续）

能力类	能力族	能力组件	说明	是否区分不同能力等级
HP：高质量产品类	HP_CC：合规能力	HP_CC.17 符合 T/WAPIA 013.4《信息安全技术 数字证书管理 第4部分：证书撤销》		否
		HP_CC.18 符合 T/WAPIA 013.5《信息安全技术 数字证书管理 第5部分：证书格式》		否
		HP_CC.19 符合 T/WAPIA 038《信息安全技术 终端实体证书管理》		否
		HP_CC.20 符合 T/WAPIA 036.1《WAPI 应用接口规范 第1部分：移动终端》（适用于终端产品）	是针对移动终端的应用层面的高质量能力体现，提高不同产品间的互联互通能力，可扩展性和用户体验	否
	HP_LD：安全漏洞处理能力	HP_LD.1 禁用涉及的不安全协议	禁用 Telnet, FTP, SMTP, TFTP, SNMPv1, HTTP 协议	否
		HP_LD.2 禁用涉及的不安全端口号	23：Telnet 服务端口； 20 和 21：通常用于 FTP 服务； 25：SMTP 端口； 69：TFTP 端口 161/162：SNMPv1/2 80 和 8080：HTTP 端口	否
		HP_LD.3 设备应具备通过安全漏洞扫描的能力	1、利用国产或开源漏洞扫描工具对产品进行检查； 2、及时关注实时发布的最新漏洞，并评估对当前产品是否有影响	否
		HP_LD.4 设备应具备安全漏洞的识别、扫描、监测预警和应急处理能力		否
	HP_KSC：密码安全能力	HP_KSC.1 私钥应产生和存在于硬件安全媒体中	产品若集成低功耗 WAPI 模组，模组应符合高质量要求	否
		HP_KSC.2 密码运算中私钥不泄露	产品若集成低功耗 WAPI 模组，模组应符合高质量要求	否

表1 （续）

能力类	能力族	能力组件	说明	是否区分不同能力等级
HC：高质量建设类	HC_CC：合规能力	HC_CC.1 符合 T/WAPIA 047.1《无线局域网系统规范 第 1 部分：工程设计》		否
		HC_CC.2 符合 T/WAPIA 047.2《无线局域网系统规范 第 2 部分：工程施工》		否
		HC_CC.3 符合 T/WAPIA 047.3《无线局域网系统规范 第 3 部分：验收测试方法》	应符合功能、性能和安全等要求	否
	HC_VE：可验证能力	HC_VE.1 设备应通过第三方专业机构（如中关村无线网络安全产业联盟测试实验室）的检测后方可采购使用		否
		HC_VE.2 应制定验收方案并实施测试验收		否
	HC_NE：扩容能力	HC_NE.1 应具备高质量扩容能力，包括对网络建设所采用不同厂家设备的兼容性和互联性要求		否
HO：高质量运行类	HO_CC：合规能力	HO_CC.1 符合 T/WAPIA 047.3《无线局域网系统规范 第 3 部分：验收测试方法》	适用于判定 WLAN 运维场景下的能力和质量	否
	HO_LD：安全漏洞处理能力	HO_LD.1 网络应具备安全漏洞的识别、扫描、监测预警和应急处理能力		否
	HO_OP：运维能力	HO_OP.1 运维管控，应定期进行维护管理		否
		HO_OP.2 应对维护人员进行技能培训		否
HS：高质量服务类	HS_CC：合规能力	HS_CC.1 网络开启安全 WLAN 接入鉴别服务		否
		HS_CC.2 网络开启安全 WLAN 保密通信服务		否
		HS_CC.3 网络开启管理帧保护服务		否
		HS_CC.4 符合 T/WAPIA 048《信息系统无线局域网密码应用基本要求》	针对整体 WLAN，通过密码应用的不同安全级别来划分	是，目前共四级。

7 网络建设

应在 WLAN 建设、改造和升级等环节，采取产品测试、系统评审（可包含商用密码应用安全性评估）

和系统攻防演练等多种形式验证。必要时，可搭建关键业务的仿真验证环境，予以验证。

针对网络扩容能力，网络建设方应有明确的技术规范要求，以及产品测试和验证手段。

网络建设高质量指标体系见表 1 中能力类为“HC：高质量建设类”的内容。

8 监测预警

8.1 基本要求

应建立并实施WLAN监测预警和信息通报制度，针对发生的网络安全事件或发现的网络安全威胁，提前或及时发出安全警示。

应建立针对WLAN的漏洞库等威胁情报和信息共享机制，落实相关措施，提高对网络攻击的主动发现能力。

8.2 监测

宜在WLAN边界、网络出入口等网络关键节点部署监测设备，发现网络攻击和未知威胁。

应对WLAN系统进行监测（如：对系统运行状态、系统承载的网络流量进行监测等），对监测信息采取保护措施，防止其受到未授权的访问、修改和删除。

宜全面收集WLAN安全日志，构建违规操作模型、攻击入侵模型和异常行为模型，强化监测预警能力。

宜采用自动化机制，对WLAN系统的所有监测信息进行整合分析，以便及时关联资产、脆弱性和威胁等，分析WLAN安全态势。WLAN系统涉及跨组织、跨地域建设时，构建集中统一指挥、多点全面监测和多级联动处置的动态感知能力。

宜通过安全态势分析结果来确定安全策略和安全控制措施是否合理有效，必要时进行更新。

8.3 预警

当发现可能危害WLAN系统的迹象时，应报警（报警方式宜自动），并自动采取相应措施，降低WLAN系统被影响的可能性，如弹出对话框、发出声音或者向相关人员发出电子邮件等方式进行报警。

应对WLAN安全共享信息和报警信息等进行综合分析、研判，必要时生成内部预警信息。对于可能造成较大影响的，应按相关部门要求进行通报。内部预警信息的内容应包括：基本情况描述、可能产生的危害及程度、可能影响的用户及范围、宜采取的应对措施等。

应能持续获取预警发布机构的安全预警信息，分析、研判相关事件或威胁对自身WLAN系统安全保护对象可能造成损害的程度，必要时启动应急预案。获取的安全预警信息应按规定通报给相关人员和相关部门。

应采取相关措施对预警进行响应，当安全隐患得以控制或消除时，应执行预警解除流程。

9 检测评估

基本要求：为检验保障网络服务、运行、建设和产品高质量措施的有效性，发现网络安全风险隐患，应建立相应的检测评估制度，确定检测评估的流程及内容等，开展安全检测与风险隐患评估，分析潜在安全风险可能引发的安全事件。

应建立健全WLAN检测评估制度，包括但不限于检测评估流程、方式方法、周期、人员组织和资金保障等。

应自行或者委托网络质量检测服务机构（如中关村无线网络安全产业联盟测试实验室）对WLAN系统安全性和可能存在的风险，每年至少进行一次检测评估，并及时整改发现的问题。

在检测评估时，内容宜包括但不限于网络安全制度（国家和行业相关法律法规政策文件及网络运营者制定的制度）落实情况、技术防护情况、风险评估情况、应急演练情况和攻防演练情况等。

在WLAN系统发生改建、扩建等较大变化时，应自行或者委托网络质量检测服务机构进行检测评估，分析变更情况，评估上述变更给WLAN系统带来的风险变化情况，并依据风险变化以及发现的安全问题进行有效整改后方可上线。

宜经有关部门批准或授权，采取模拟网络攻击方式，检测WLAN在面对实际网络攻击时的防护和响应能力。

在检测评估工作中，应配合提供网络安全管理制度、网络拓扑图、重要资产清单和网络日志等必要的资料和技术协助，针对发现的安全隐患和风险建立清单，制定整改方案，并及时整改。

10 主动防御

10.1 基本要求

以应对网络攻击行为的监测发现为基础，主动采取收敛暴露面、捕获、溯源、干扰和阻断等措施，开展攻防演习和威胁情报工作，提升对网络威胁与攻击行为的识别、分析和主动防御能力。

10.2 收敛暴露面

应识别和减少 WLAN 的网络地址、端口和应用服务等暴露面，压缩 WLAN 对互联网的出口数量。

不应在公共存储空间（如：代码托管平台、文库、网盘等）存储可能被攻击者利用的技术文档。如：WLAN 拓扑图、源代码、网络地址规划等。

10.3 攻击发现和阻断

应分析针对 WLAN 攻击的方法、手段，针对拒绝服务攻击等各类攻击，采取有针对性的防护策略和技术措施，制定总体技术应对方案。

应针对监测发现的攻击活动，分析攻击路线、攻击目标，设置多道防线，采取捕获、干扰、阻断、封控和加固等多种技术手段，切断攻击路径，快速处置网络攻击。

应及时对网络攻击活动开展溯源，对攻击者进行画像，为案件侦查、事件调查、完善防护策略和措施提供协助。

应系统全面地分析网络攻击意图、技术与过程，进行关联分析与还原，依此改进安全保护策略，并加以落实。

10.4 攻防演练

应围绕WLAN的可持续运行设定演练场景（宜包括极限情况），定期组织开展攻防演练。在不适合开展实网攻防演练场景下，宜采取沙盘推演的方式进行攻防演练。

应针对攻防演练中发现的安全问题及风险进行及时整改，消除结构性、全局性风险。

10.5 威胁情报

应建立WLAN威胁情报共享机制，组织联动上下级单位，开展威胁情报搜集、加工、共享和处置。

应建立外部协同网络威胁情报共享机制，与权威网络威胁情报机构开展协同联动，实现跨行业领域网络安全联防联控。

11 应急处置

11.1 基本要求

网络运营者对影响WLAN运行的事件进行报告和处置，并采取适当的措施，恢复由于事件而受损的功能或服务。

11.2 网络安全事件报告

当发生有可能危害WLAN运行的事件时，应及时向网络管理机构报告，并组织研判，形成事件报告。

应及时将可能危害WLAN运行的安全事件通报到可能受影响的内部部门和人员，并按规定向供应链涉及的、与事件相关的其他组织通报安全事件。

11.3 事件处理和恢复

应按事件处置流程、应急预案进行事件处理，恢复WLAN信息系统到已知的状态。

应按先应急处置、后调查评估的原则，在事件发生后尽快收集证据，按要求进行网络安全运行取证分析，并记录所有涉及的响应活动，便于日后分析。在进行取证分析时，应与业务连续性计划相协调。

在事件处理完成后，应采用手工或者自动化机制形成完整的事件处理报告。事件处理报告包括：不同部门对事件的处理记录、事件的状态和取证相关的其他必要信息、评估事件细节、趋势和处理。

在恢复WLAN信息系统后，应对信息系统和承载关键业务的恢复情况进行评估，查找事件原因，并采取措施防止遭受再次破坏、危害或故障。

在进行事件处理活动时，应协调组织内部多个部门和外部相关组织，以更好地对事件进行处理，并将事件处理活动的经验教训纳入事件响应规程、培训以及测试，并进行相应变更。

宜及时将事件及其处置情况通报到可能受影响的部门和相关人员，向供应链涉及的、与事件相关的其他组织提供安全事件信息，并按法律政策规定报告相关部门。

11.4 重新识别

应根据检测评估、攻防演练和监测预警中发现的系统隐患和发生的安全事件，以及处置结果，并结合安全威胁和风险变化情况开展评估，必要时重新开展业务、资产和风险识别工作，并更新安全策略。

参考文献

[1] GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求
[2] GB/T 25069—2022 信息安全技术 术语
[3] GB/T 28448—2019 信息安全技术 网络安全等级保护测评要求
[4] GB/T 29246—2017 信息技术 安全技术 信息安全管理体系 概述和词汇
[5] GB/T 39204—2022 信息安全技术 关键信息基础设施安全保护要求
[6] T/WAPIA 040.1—2021 关键信息基础设施无线局域网技术要求 第1部分：通用要求
[7] 关键信息基础设施安全保护条例（2021年4月27日国务院第133次常务会议通过，中华人民共和国国务院令第745号）.
[8] 中华人民共和国网络安全法[2016年11月7日第十二届全国人民代表大会常务委员会第二十四次会议通过，中华人民共和国主席令（第53号）].
[9] 中华人民共和国国家通用语言文字法[2000年10月31日第十九届全国人民代表大会常务委员会第十八次会议通过，中华人民共和国主席令（第37号）].