中国质量检验协会文件

中检办发〔2025〕164号

中国质量检验协会关于《网络安全　主动隐形防御体系　第1部分：总体架构》团体标准征求意见的通知

各有关单位和相关专家：

中国质量检验协会(以下简称本协会)批准立项的《网络安全 主动隐形防御体系　第1部分：总体架构》团体标准经过有关专家和参编单位讨论和修改，据此形成上述团体标准征求意见稿。

按照《中国质量检验协会团体标准管理办法》的相关规定和要求，本协会现对上述团体标准公开征求意见，请各有关单位和相关专家对上述团体标准制定的修改意见和建议于2026年1月10日前反馈至本协会；如逾期未作反馈，则视为无意见和建议。

谨此感谢有关专家和参编单位与社会各界对本协会团体标准制修订工作的大力支持！

本团体标准编制工作组　联系人：于洪

手机：13319861505

邮箱：techsup@macsec.cn

中国质量检验协会碳中和绿色发展专业委员会 联系人：蔺枫

电话：010-59196500　　手机：13601123186

邮箱：zwh@chinatt315.org.cn

附件：1.《网络安全　主动隐形防御体系　第1部分：总体架构》（征求意见稿）

2.团体标准制定征求意见表

中国质量检验协会

2025年12月10日

附件 1

ICS
CCS

CAQI

团　　体　　标　　准

T/CAQI **—2025

网络安全　主动隐形防御体系
第 1 部分：总体架构

Network security　Active stealth defense system　Part 1: General architectures

（征求意见稿）

2025－XX－XX 发布　　2025－XX－XX 实施

中国质量检验协会　　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。

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。

本文件由北京北斗弘鹏科技有限公司、北京航空航天大学提出。

本文件由中国质量检验协会归口。

本文件起草单位：北京北斗弘鹏科技有限公司、北京航空航天大学、北京黑合科技有限公司、北京弘鹏智能安全科技有限公司、安徽北斗弘鹏安全科技有限公司、上海北斗弘鹏科技有限公司、江苏北斗弘鹏科技有限公司、天津北斗弘鹏科技有限公司、四川北斗弘鹏科技有限公司、北京冠群金辰软件有限公司、北京电设亚联科技有限公司、西南财经大学天府学院、绵阳科技城数字经济产业创新研究院有限公司、绵阳科技城科技服务有限责任公司、四川新投智城科技有限公司、天津滨海通用航空产业发展公司、天津滨海新区智明科技发展有限公司、四川跑哥智造科技有限公司。

本文件主要起草人：于洪、李兆森、任娜娜、刘东、王子玮、杨立生、刘聪、马旭腾、杨东华、冯军、吕茂强、于红琴、刘振华、陆宝华、文瀚唯、梅飞、付彦海、袁勋、徐鸿雁、杨永斌、杨林、欧仁良、刘勇、肖新江、刘杨、曾钟浩。

网络安全　主动隐形防御体系　第1部分：总体架构

1　范围

本文件规定了数字化网络空间建立中主动隐形防御技术体系的总体架构。

本文件适用于网络未知威胁防御、数字化智能制造安全、工业控制运行状态安全、数据传输安全、隐蔽信息交换的应用防护领域。

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/T 22239-2019 信息安全技术　网络安全等级保护基本要求

GB/T 25069-2022 信息安全技术　术语

GB/T 39204-2022 信息安全技术 关键信息基础设施安全保护要求

GM/T 0028-2024　密码模块安全技术要求

3　术语和定义

GB/T 25069-2022、GB/T 39024-2022界定的以及下列术语和定义适用于本文件。

3.1

被动防御 passive defens PD

以“防御响应”为核心的安全防护策略，其核心特征是不主动干预攻击行为的发起过程，仅在攻击发生或检测到威胁后，采取阻断、隔离、告警等措施来降低损害。

3.2

主动防御 active defense AD

对网络攻击事先达成有效防御，使攻击方对目标系统的认证优势和掌握的可利用资源在时间和空间上无法持续有效，最终使探测信息难以积累、攻击模式难以复制、攻击效果难以重现和攻击手段难以继承的目的。

3.3

主动隐形防御技术 active stealth defense technology ASDT

利用加密、隐写和隐蔽信道传输等技术，实现对网络、数据、信道等隐形，从而起到安全防御的作用。

3.4

主动隐形防御 active stealth defense ASD

通过主动隐形、主动变换、主动控制、主动加密的一系列主动执行策略，面对网络中的未知威胁和已知威胁采取主动隐形和主动加密控制等机制，利用主动防御技术在有限时间和空间内主动提升网络安全生存空间，主动隐形防御区别被动防御是对抗未知威胁的安全保护能力。

3.5

主动隐形防御战略 active stealth defense strategy ASDS

通过自主领先的非对称主动隐形技术在数字网络空间中获得先发制人的优势，利用主动隐形技术手段来对抗未知威胁、隐形攻击和各类网络渗透攻击的机制手段，从而达到抵近拒止战略或反介入战略优势，在拥有网络空间主权的前提下和平利用数字化网络空间资源，具有主动干预、主动响应执行的全新安全防御思路而建立的隐形安全防御战略。

3.6

主动隐形防御理论 active stealth defense theory ASD theory

采用非传统被动识别检测机制，创新通过主动隐形机制来对抗网络入侵攻击的一种创新技术实现理论。

注：在数字化网络空间中主动隐形防护理论是利用自身隐藏、网络中链接拓扑结构隐藏、各设备间通讯隐藏、设备间传输数据隐藏、路由交换层逻辑控制隐藏及存储内容隐藏的一种主动防护技术的实现机制或方法而形成的安全防护理论。

3.7

主动隐形防御架构 active stealth defense architecture ASDA

在因特网上全方位、立体化、全域安全管控的多层次、多维度安全防御的架构设计，由：设计原则、分类实现、安全域划分三个方面构成，通过：主动隐形防御软件系统、主动隐形防御执行硬件、主动隐形防御管理进行展现，利用隐形计算、隐形通讯、隐形网络、隐形存储手段来实现。

3.8

主动隐形防御体系 active stealth defense multi-system ASDM

以主动隐藏攻击面、阻断攻击链为核心目标的立体化防御系统，由：防探测隐形、自身信道隐形、数据交互隐形、防攻击隐形四个方面组成，融合在物理层、数据链路层、网络层、传输层、会话层、表示层、应用层中，采用“资产隐形、数据加密隐形、信道传输隐形”全域安全防护实现网络安全的整体防护。

3.9

主动隐形防御系统 active stealth defense system ASDS

支撑主动隐形防御产品运行，支撑硬件和嵌入式软件一体化的操作系统。在无MAC地址、无网络IP地址、无接口路由信息的状态下，主动隐形防御系统接入网络中将自身设备隐藏同时使被保护网络隐形，从而不被恶意攻击者探测发现、不被渗透攻击。

3.10

主动隐形设备 active stealth equipment ASE

部署于网络环境中，具备通讯数据处理、数据转发、安全接入、安全防护或网络管控能力的硬件装置和系统。本设备是构建网络拓扑、实现数据传输与业务支撑的核心物理载体。

3.11

主动隐形资产特征 active stealth assets characteristics AASC

主动隐形资产包括逻辑网络架构、数字资产、设备性能、运行控制行为及安全属性的核心指标与固有属性集合，贯穿网络设计、数字化部署、数据运维及数字安全防护全生命周期。

3.12

主动隐形资产系统 active stealth asset system ASAS

构成主动隐形系统网络的所有可识别、可管控且具有实际价值的要素集合，涵盖硬件设备、软件系统、数据资源、网络链路及相关管理权限，能作为网络运行、业务支撑与安全防护的核心对象。

4 缩略语

下列缩略语适用于本文件。

APT：高级可持续威胁（Advanced Persistent Threat）

OSI：开放式系统互联参考模型 （Open System Interconnection）

CPU：中央处理器 （Central Processing Unit）

ASIC：专用集成电路 （Application-Specific Integrated Circuit）

FPGA：现场可编程门阵列 （Field-Programmable Gate Array）

AI：人工智能（Artificial Intelligence）

MAC：媒体访问控制 （Media Access Control）

APP：应用程序 （Application）

WIFI：无线网络 （Wireless Fidelity）

DNS：域名系统（domain name system）

IP：互联网协议地址（Internet Protocol Address）

5 设计原则

主动隐形防御战略设计需围绕“主动性、隐藏性、动态性、抗攻击性、兼容性”五大基本原则。

5.1 主动性

区别于传统被动防御，主动隐形防御理论强调以主动干预、主动塑造攻防态势的方式，实现对网络攻击的前置化、精准化防御。

5.2 隐藏性

通过主动隐形防御理论收敛暴露面，主动隐藏受保护的主动隐形资产特征、网络特征指纹、通信数据、逻辑拓扑连接关系、传输控制指令等，从而全面保护主动隐形资产系统免遭入侵攻击。

5.3 动态性

对网络通信链路中传输的数据进行主动隐形防御技术，对数据进行加密特征的处理机制。

5.4 抗攻击性

通过主动隐形来构建多层次的防护体系，对抗未知威胁和APT时能有效保护数字资产或系统。

5.5 兼容性

兼容当前网络的二层交换接入、三层路由通信设备，通过数据化的接口与其他主流设备无缝对接。

6 总体架构

6.1 概述

主动隐形防御总架构是与传统安全防御体系互补融合，上下协同，主动隐形防御总体架构依托主动隐形防御战略和主动隐形防御体系，通过主动隐形防御理论和主动隐形防御技术形成主动隐形资产系

统，实现对网络设备和系统的安全防护。基于主动隐形防御架构的应用作用于终端设备和网络边界，涵盖的相关产业链和领域有：低空经济、军工网络、工控网络、卫星网络、计算机网络、车联网、物联网、智慧城市、航空航天、无人智能装备、应急救援、音频视频监控等。主动隐形防御总架构如图1 总体架构图。

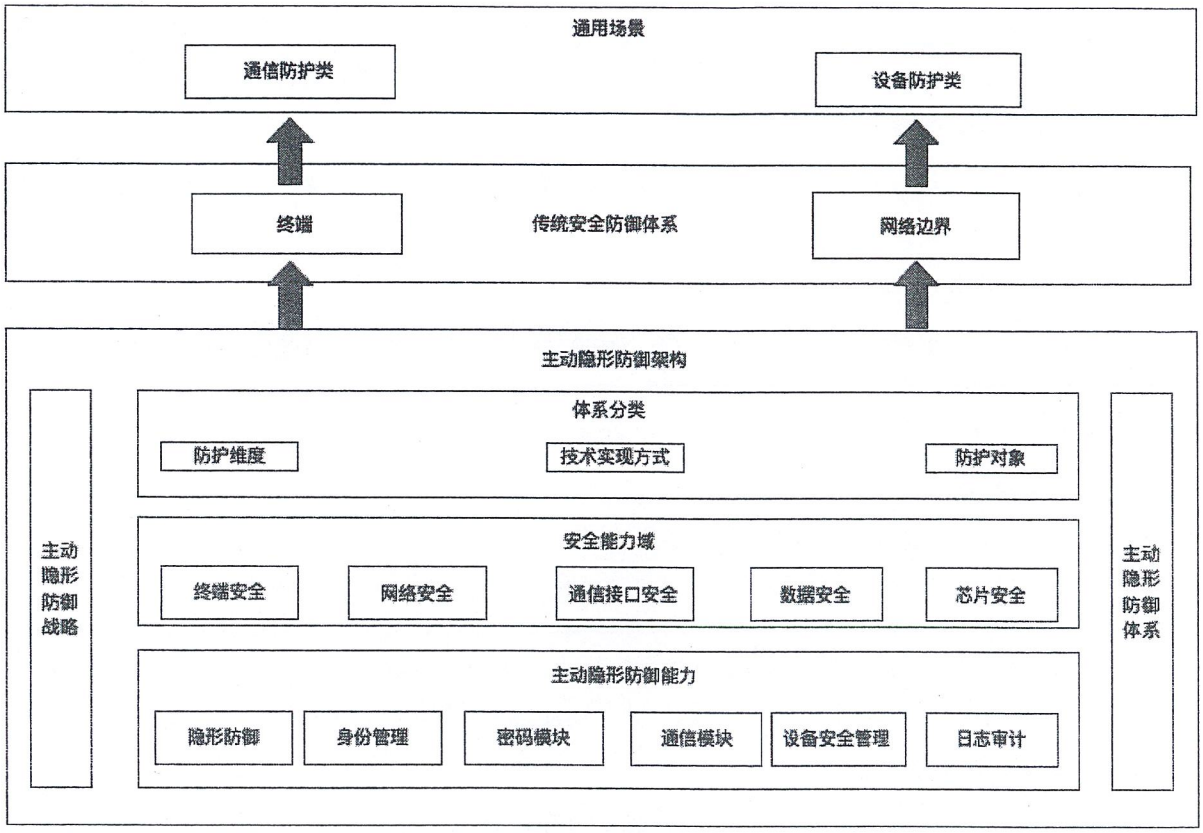

图1 总体架构图

6.2 核心目标

主动隐形防御理论为各网络安全产品提供商、网络安全建设商、网络安全产品使用者提供网络安全建设的开发依据、使用依据和应用推广的主动隐形防御架构提供支撑。

6.3 建设思路

主动隐形防御架构描述了基于主动隐形防御体系的安全防护各能力要素、安全能力域以及通用应用场景。通过在网络的关键节点部署基于主动隐形防御技术的设备，使受保护的网络在设备终端安全、网络安全、数据安全三大领域得到安全防护能力的增强。为应用提供在远程办公、安全接入、工业互联网、车联网、低空经济等场景下的网络安全防护能力和终端设备的安全防御能力。

6.4 设计原则

6.4.1 技术融合无感知

主动隐形防御系统在不改变原有算法、技术实现机制的前提下，主动隐形防御架构与新兴技术深度协同，如与云计算、AI人工智能、量子计算等技术趋势适配和融合。

6.4.2 方案设计部署无影响

主动隐形防御系统在方案设计与方案实现时，在加入主动隐形技术时不会改变原有网络架构设计，不改变原有网络接入模式、不增加网络接入地址或路由、不改变原有访问方式、不改变原有操作特点、不改变原有网络的吞吐、延时、抖动等性能特性。

6.4.3 体系化防护广泛覆盖

主动隐形防御系统产品可以部署在单点或者全链路上，通过独立硬件、模组、服务器软件、用户端软件、芯片组等多种形态，适应于构建覆盖资产、数据、业务、人员的全域安全防护体系。

6.4.4 防护价值合理性

主动隐形防御系统是从合规性资本投入导向到风险防范损失投入转变，可实现网络安全防护投入与安全防护价值的最大化。

6.4.5 协同治理全局化

主动隐形防御系统通过全局架构的部署，满足跨组织和跨领域的安全联动，通过政府、企业、产业链协同共同构建安全主动隐形防御战略空间。

6.5 防护效果体系分类

6.5.1 安全防护

1) 在物理层和数据链路层实现主动隐形效果；
2) 在网络层和传输层实现防探测发现、防劫持、防未知威胁攻击的隐形效果；
3) 在全局网络规划设计、网络逻辑拓扑结构设计层实现防探测发现、防信息收集的主动隐形效果；
4) 在数据通讯交换传输时实现隐形加密数据防攻击的主动隐形效果；
5) 在应用层和会话层实现客户操作访问方式与终端路径隐藏的主动隐形效果。

6.5.2 技术实现方式

1) 通过硬件方式实现隐形效果，如CPU、FPGA、模组、板卡等；
2) 通过软件方式实现隐形效果：如服务、中间件、客户端程序等；
3) 通过硬件组合软件混合方式实现隐形效果，如板卡结合服务端程序。

6.5.3 资产防护对象

1) 对设备资产的隐形；
2) 对数据传输的隐形；
3) 对流量特征的隐形；
4) 对某一类业务场景的整体隐形。

6.5.4 实现效果

1) 降低资产可见性：通过“IP/MAC 隐形 + 设备指纹隐藏 + 网络逻辑拓扑隐形”，使网络资产从攻击者视角“物理存在但逻辑不可见”；
2) 阻断攻击扫描探测：通过“去流量特征化 + 创建隐蔽传输信道”，使攻击者无法通过端口扫描、协议识别、流量分析定向分析，在前期“探测 - 渗透”环节阻断攻击链；
3) 全生命周期数据安全：通过“多维叠加加密 + 密钥动态管理 + 全密态处理”，确保数据从传输到存储的“可用不可见”，即使攻击者获取数据包也无法破解。

6.6 安全域分类

6.6.1 安全域分类原则

基于主动隐形防御体系架构，可以解决目前大部分的数据通信类、网络设备类的安全防护需求。该类场景多涉及到同类型网络内部、网络之间和不同类型的网络之间的数据通信，需要对数据做加密传输，同时要对新接入的网络、设备进行身份验证，只有基于主动隐形防御技术的设备才可以入网通信。以及在网络的渗透攻击的初始扫描探测阶段，能够抵御各类探测行为，降低价值资源的暴露面。主动隐形防御体现在以下安全域，并符合GB/T 22239-2019和GB/T 39204-2022的安全要求。

6.6.2 终端架构安全域

1） 浏览器安全控制类；
2） 操作系统安全控制类；
3） SDK开发插件安全控制类；
4） APP小程序插件安全控制类；
5） 存储安全软件控制类；
6） 编译器安全软件控制类；
7） 运维状态监控软件控制类。

6.6.3 网络安全架构防护域

1） 防火墙访问控制类；
2） 加密通讯网关类；
3） 入侵检测类；
4） 堡垒机网关类；
5） 边界隔离控制类；
6） 边界防绕过网关类；
7） 日志审计类；
8） 单向隔离网关类；
9） 交换、路由域控制类。

6.6.4 安全通信接口域

1） ETH以太接口类；
2） FDDI光纤接口类；
3） WIFI接口安全类；
4） 自组网接口类；
5） 雷达接口类；
6） 通讯接口类；
7） 接口安全类；
8） 3GPP接口类。

6.6.5 数据安全域

1） 数据防泄露类；
2） 数据权限控制类；
3） 数据微隔离类；
4） 数据分析挖掘类；
5） AI大模型类；

6） 大屏显示过滤控制类；
7） 精准分析类。

6.6.6 安全专用芯片域

1） FPGA芯片类；
2） ASIC芯片类；
3） CPU芯片类；
4） 其他类型芯片防护类。

6.6.7 应用场景域

1） 无人智能化装备领域；
2） 工控网络领域；
3） 计算机网络领域；
4） 通信领域；
5） 智慧城市领域；
6） 车联网领域；
7） 低空经济领域；
8） AI大模型领域。

6.7 系统能力组成

6.7.1 隐形防御模块

主动隐形防御系统本身在网络中不被网络扫描工具探测发现，可实现OSI七层模型的隐形效果。

6.7.2 身份管理模块

按照GB/T 39204-2022中的身份认证和校验机制，支持不同主动隐形防御设备间安全的同步配置参数数据和敏感数据。

6.7.3 密码模块

按照GM/T 0028-2024中对随机数、密码算法和密钥管理的相关安全要求。

6.7.4 通信模块

主动隐形防御系统在通信中隐藏通信路径、网络指纹去特征化、兼容各类通信协议，使通信内容不被截获，不能被抓包工具分析数据包内容。

6.7.5 设备安全管理

主动隐形防御体系架构在网络中能防止物理探测工具探测设备真实主动隐形设备等基本信息，无法探测出主动隐形系统硬件信息或接口信息，无法获取主动隐形系统使用的核心处理器信息，无法获取主动隐形系统的电气属性和其他属性信息。

6.7.6 日志审计

主动隐防御系统具备自身监控的基础信息等，支持对外输出标准化的监控审计日志数据或文件。

6.8 通用场景

6.8.1 通信防护类

适用 GB/T 22239-2019 和 GB/T 39204-2022 中的针对通信类的通用场景和扩展场景，并能抵御网络中对数据包的截获和破解。

6.8.2 设备防护类

适用 GB/T 22239-2019 和 GB/T 39204-2022 中的针对设备的通用场景和扩展场景，能在攻防演练中对网络、设备的各类扫描探测行为进行安全防护。

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 25070-2019：信息安全技术 网络安全等级保护设计技术要求

[3] GB/T 32907-2016：信息安全技术 SM4 分组密码算法

[4] GB/T 39786-2021：信息安全技术 信息系统密码应用基本要求

[5] GB/T 40813-2021：信息安全技术 工业控制系统安全防护技术要求和测试评价方法

[6] GB/T CAMETA 001006.1-2022：工业网关通用技术要求标准

[7] CCRC-TR-103-2020：中国网络安全审查技术与认证中心 产品认证技术规范

[8] ISO/IEC 27002：信息安全、网络安全和隐私保护-信息安全控制

附件 2

团体标准制定征求意见表

单位名称或 专家姓名			单位盖章或 专家签名	
联系人			联系方式	
标准名称		网络安全　主动隐形防御体系　第 1 部分：总体架构		
序号	章节	修改意见		具体理由
备注：修改意见和具体理由，可另附相关说明				

本团体标准编制工作组联系人：于洪，手机：13319861505，邮箱：techsup@macsec.cn。

抄送：本协会会员工作部，本协会存档（2）。

中国质量检验协会　　2025年12月10日印发