9.2.4.6.3 测评单元(L4-CES2-16)

该测评单元包括以下要求：

a) 测评指标：云服务商的云存储服务应保证云服务客户数据存在若干个可用的副本，各副本之间的内容应保持一致。

b) 测评对象：云管理平台、云存储系统或相关组件。

c) 测评实施包括以下内容：

1) 应核查云服务客户数据副本存储方式，核查是否存在若干个可用的副本；

2) 应核查各副本内容是否保持一致。

d) 单元判定：如果 1)和 2)均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

9.2.4.6.4 测评单元(L4-CES2-17)

该测评单元包括以下要求：

a) 测评指标：应为云服务客户将业务系统及数据迁移到其他云计算平台和本地系统提供技术手段，并协助完成迁移过程。

b) 测评对象：相关技术措施和手段。

c) 测评实施包括以下内容：

1) 应核查是否有相关技术手段保证云服务客户能够将业务系统及数据迁移到其他云计算平台和本地系统；

2) 应核查云服务商是否提供措施、手段或人员协助云服务客户完成迁移过程。

d) 单元判定：如果 1)和 2)均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

9.2.4.7 剩余信息保护

9.2.4.7.1 测评单元(L4-CES2-18)

该测评单元包括以下要求：

a) 测评指标：应保证虚拟机所使用的内存和存储空间回收时得到完全清除。

b) 测评对象：云计算平台。

c) 测评实施包括以下内容：

1) 应核查虚拟机的内存和存储空间回收时，是否得到完全清除；

2) 应核查在迁移或删除虚拟机后，数据以及备份数据(如镜像文件、快照文件等)是否已清理。

d) 单元判定：如果 1)和 2)均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

9.2.4.7.2 测评单元(L4-CES2-19)

该测评单元包括以下要求：

a) 测评指标：云服务客户删除业务应用数据时，云计算平台应将云存储中所有副本删除。

b) 测评对象：云存储和云计算平台。

c) 测评实施：应核查当云服务客户删除业务应用数据时，云存储中所有副本是否被删除。

d) 单元判定：如果以上测评实施内容为肯定，则符合本单元测评指标要求，否则不符合本单元测

评指标要求。

9.2.5 安全管理中心

9.2.5.1 集中管控

9.2.5.1.1 测评单元(L4-SMC2-01)

该测评单元包括以下要求：

a) 测评指标：应对物理资源和虚拟资源按照策略做统一管理调度与分配。

b) 测评对象：资源调度平台、云管理平台或相关组件。

c) 测评实施包括以下内容：

1) 应核查是否有资源调度平台等提供资源统一管理调度与分配策略；

2) 应核查是否能够按照上述策略对物理资源和虚拟资源做统一管理调度与分配。

d) 单元判定：如果 1)和 2)均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

9.2.5.1.2 测评单元(L4-SMC2-02)

该测评单元包括以下要求：

a) 测评指标：应保证云计算平台管理流量与云服务客户业务流量分离。

b) 测评对象：网络架构和云管理平台。

c) 测评实施包括以下内容：

1) 应核查网络架构和配置策略能否采用带外管理或策略配置等方式实现管理流量和业务流量分离；

2) 应测试验证云计算平台管理流量与业务流量是否分离。

d) 单元判定：如果 1)和 2)均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

9.2.5.1.3 测评单元(L4-SMC2-03)

该测评单元包括以下要求：

a) 测评指标：应根据云服务商和云服务客户的职责划分，收集各自控制部分的审计数据并实现各自的集中审计。

b) 测评对象：云管理平台、综合审计系统或相关组件。

c) 测评实施包括以下内容：

1) 应核查是否根据云服务商和云服务客户的职责划分，实现各自控制部分审计数据的收集；

2) 应核查云服务商和云服务客户是否能够实现各自的集中审计。

d) 单元判定：如果 1)和 2)均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

9.2.5.1.4 测评单元(L4-SMC2-04)

该测评单元包括以下要求：

a) 测评指标：应根据云服务商和云服务客户的职责划分，实现各自控制部分，包括虚拟化网络、虚拟机、虚拟化安全设备等的运行状况的集中监测。

b) 测评对象：云管理平台或相关组件。

c) 测评实施：应核查是否根据云服务商和云服务客户的职责划分，实现各自控制部分，包括虚拟

化网络、虚拟机、虚拟化安全设备等的运行状况的集中监测。

d) 单元判定：如果以上测评实施内容为肯定，则符合本单元测评指标要求，否则不符合本单元测评指标要求。

9.2.6 安全建设管理

9.2.6.1 云服务商选择

9.2.6.1.1 测评单元(L4-CMS2-01)

该测评单元包括以下要求：

a) 测评指标：应选择安全合规的云服务商，其所提供的云计算平台应为其所承载的业务应用系统提供相应等级的安全保护能力。

b) 测评对象：系统建设负责人和服务合同。

c) 测评实施包括以下内容：

1) 应访谈系统建设负责人是否根据业务系统的安全保护等级选择具有相应等级安全保护能力的云计算平台及云服务商；

2) 应核查云服务商提供的相关服务合同是否明确其云计算平台具有与所承载的业务应用系统具有相应或高于的安全保护能力。

d) 单元判定：如果 1)和 2)均为肯定，则符合本单元测评指标要求，否则不符合或部分符合本单元测评指标要求。

9.2.6.1.2 测评单元(L4-CMS2-02)

该测评单元包括以下要求：

a) 测评指标：应在服务水平协议中规定云服务的各项服务内容和具体技术指标。

b) 测评对象：服务水平协议或服务合同。

c) 测评实施：应核查服务水平协议或服务合同是否规定了云服务的各项服务内容和具体指标等。

d) 单元判定：如果以上测评实施内容为肯定，则符合本单元测评指标要求，否则不符合本单元测评指标要求。

9.2.6.1.3 测评单元(L4-CMS2-03)

该测评单元包括以下要求：

a) 测评指标：应在服务水平协议中规定云服务商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等。

b) 测评对象：服务水平协议或服务合同。

c) 测评实施：应核查服务水平协议或服务合同中是否规范了安全服务商和云服务供应商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等。

d) 单元判定：如果以上测评实施内容为肯定，则符合本单元测评指标要求，否则不符合本单元测评指标要求。

9.2.6.1.4 测评单元(L4-CMS2-04)

该测评单元包括以下要求：

a) 测评指标：应在服务水平协议中规定服务合约到期时，完整提供云服务客户数据，并承诺相关

数据在云计算平台上清除。

b) 测评对象:服务水平协议或服务合同。

c) 测评实施:应核查服务水平协议或服务合同是否明确服务合约到期时,云服务商完整提供云服务客户数据,并承诺相关数据在云计算平台上清除。

d) 单元判定:如果以上测评实施内容为肯定,则符合本单元测评指标要求,否则不符合本单元测评指标要求。

9.2.6.1.5 测评单元(L4-CMS2-05)

该测评单元包括以下要求:

a) 测评指标:应与选定的云服务商签署保密协议,要求其不得泄露云服务客户数据。

b) 测评对象:保密协议或服务合同。

c) 测评实施:应核查保密协议或服务合同是否包含对云服务商不得泄露云服务客户数据的规定。

d) 单元判定:如果以上测评实施内容为肯定,则符合本单元测评指标要求,否则不符合本单元测评指标要求。

9.2.6.2 供应链管理

9.2.6.2.1 测评单元(L4-CMS2-07)

该测评单元包括以下要求:

a) 测评指标:应确保供应商的选择符合国家有关规定。

b) 测评对象:记录表单类文档。

c) 测评实施:应核查云服务商的选择是否符合国家的有关规定。

d) 单元判定:如果以上测评实施内容为肯定,则符合本单元测评指标要求,否则不符合本单元测评指标要求。

9.2.6.2.2 测评单元(L4-CMS2-08)

该测评单元包括以下要求:

a) 测评指标:应将供应链安全事件信息或威胁信息及时传达到云服务客户。

b) 测评对象:供应链安全事件报告或威胁报告。

c) 测评实施:应核查供应链安全事件报告或威胁报告是否及时传达到云服务客户,报告是否明确相关事件信息或威胁信息。

d) 单元判定:如果以上测评实施内容为肯定,则符合本单元测评指标要求,否则不符合本单元测评指标要求。

9.2.6.2.3 测评单元(L4-CMS2-09)

该测评单元包括以下要求:

a) 测评指标:应将供应商的重要变更及时传达到云服务客户,并评估变更带来的安全风险,采取措施对风险进行控制。

b) 测评对象:供应商重要变更记录、安全风险评估报告和风险预案。

c) 测评实施:应核查供应商的重要变更是否及时传达到云服务客户,是否对每次供应商的重要变更都进行风险评估并采取控制措施。

d) 单元判定：如果以上测评实施内容为肯定，则符合本单元测评指标要求，否则不符合本单元测评指标要求。

9.2.7 安全运维管理

9.2.7.1 云计算环境管理

9.2.7.1.1 测评单元(L4-MMS2-01)

该测评单元包括以下要求：

a) 测评指标：云计算平台的运维地点应位于中国境内，境外对境内云计算平台实施运维操作应遵循国家相关规定。

b) 测评对象：运维设备、运维地点、运维记录和相关管理文档。

c) 测评实施：应核查运维地点是否位于中国境内，从境外对境内云计算平台实施远程运维操作的行为是否遵循国家相关规定。

d) 单元判定：如果以上测评实施内容为肯定，则符合本单元测评指标要求，否则不符合本单元测评指标要求。

9.3 移动互联安全测评扩展要求

9.3.1 安全物理环境

9.3.1.1 无线接入点的物理位置

9.3.1.1.1 测评单元(L4-PES3-01)

该测评单元包括以下要求：

a) 测评指标：应为无线接入设备的安装选择合理位置，避免过度覆盖和电磁干扰。

b) 测评对象：无线接入设备。

c) 测评实施包括以下内容：

1) 应核查物理位置与无线信号的覆盖范围是否合理；

2) 应测试验证无线信号是否可以避免电磁干扰。

d) 单元判定：如果 1)和 2)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.3.2 安全区域边界

9.3.2.1 边界防护

9.3.2.1.1 测评单元(L4-ABS3-01)

该测评单元包括以下要求：

a) 测评指标：应保证有线网络与无线网络边界之间的访问和数据流通过无线接入网关设备。

b) 测评对象：无线接入网关设备。

c) 测评实施：应核查有线网络与无线网络边界之间是否部署无线接入网关设备。

d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.3.2.2 访问控制

9.3.2.2.1 测评单元(L4-ABS3-02)

该测评单元包括以下要求：

a) 测评指标：无线接入设备应开启接入认证功能，并支持采用认证服务器认证或国家密码管理机构批准的密码模块进行认证。

b) 测评对象：无线接入设备。

c) 测评实施：应核查是否开启接入认证功能，是否采用认证服务器或国家密码管理机构批准的密码模块进行认证。

d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.3.2.3 入侵防范

9.3.2.3.1 测评单元(L4-ABS3-03)

该测评单元包括以下要求：

a) 测评指标：应能够检测到非授权无线接入设备和非授权移动终端的接入行为。

b) 测评对象：终端准入控制系统、移动终端管理系统或相关组件。

c) 测评实施包括以下内容：

1) 应核查是否能够检测非授权无线接入设备和移动终端的接入行为；

2) 应测试验证是否能够检测非授权无线接入设备和移动终端的接入行为。

d) 单元判定：如果 1)和 2)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.3.2.3.2 测评单元(L4-ABS3-04)

该测评单元包括以下要求：

a) 测评指标：应能够检测到针对无线接入设备的网络扫描、DDoS 攻击、密钥破解、中间人攻击和欺骗攻击等行为。

b) 测评对象：抗 APT 攻击系统、网络回溯系统、威胁情报检测系统、抗 DDoS 攻击系统和入侵保护系统或相关组件。

c) 测评实施包括以下内容：

1) 应核查是否能够对网络扫描、DDoS 攻击、密钥破解、中间人攻击和欺骗攻击等行为进行检测；

2) 应核查规则库版本是否及时更新。

d) 单元判定：如果 1)和 2)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.3.2.3.3 测评单元(L4-ABS3-05)

该测评单元包括以下要求：

a) 测评指标：应能够检测到无线接入设备的 SSID 广播、WPS 等高风险功能的开启状态。

b) 测评对象：无线接入设备或相关组件。

c) 测评实施：应核查是否能够检测无线接入设备的 SSID 广播、WPS 等高风险功能的开启状态。

d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.3.2.3.4 测评单元（L4-ABS3-06）

该测评单元包括以下要求：

a) 测评指标：应禁用无线接入设备和无线接入网关存在风险的功能，如：SSID 广播、WEP 认证等。

b) 测评对象：无线接入设备和无线接入网关设备。

c) 测评实施：应核查是否关闭了 SSID 广播、WEP 认证等存在风险的功能。

d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.3.2.3.5 测评单元（L4-ABS3-07）

该测评单元包括以下要求：

a) 测评指标：应禁止多个 AP 使用同一个鉴别密钥。

b) 测评对象：无线接入设备。

c) 测评实施：应核查是否分别使用了不同的鉴别密钥。

d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.3.2.3.6 测评单元（L4-ABS3-08）

该测评单元包括以下要求：

a) 测评指标：应能够定位和阻断非授权无线接入设备或非授权移动终端。

b) 测评对象：终端准入控制系统、移动终端管理系统或相关组件。

c) 测评实施包括以下内容：

1) 应核查是否能够定位和阻断非授权无线接入设备或非授权移动终端接入；

2) 应测试验证是否能够定位和阻断非授权无线接入设备或非授权移动终端接入。

d) 单元判定：如果 1)和 2)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.3.3 安全计算环境

9.3.3.1 移动终端管控

9.3.3.1.1 测评单元（L4-CES3-01）

该测评单元包括以下要求：

a) 测评指标：应保证移动终端安装、注册并运行终端管理客户端软件。

b) 测评对象：移动终端和移动终端管理系统。

c) 测评实施：应核查移动终端是否安装、注册并运行移动终端客户端软件。

d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.3.3.1.2 测评单元(L4-CES3-02)

该测评单元包括以下要求:

a) 测评指标:移动终端应接受移动终端管理服务端的设备生命周期管理、设备远程控制,如:远程锁定、远程擦除等。

b) 测评对象:移动终端和移动终端管理系统。

c) 测评实施包括以下内容:

1) 应核查移动终端管理系统是否设置了对移动终端进行设备远程控制及设备生命周期管理等安全策略;

2) 应测试验证是否能够对移动终端进行远程锁定和远程擦除等。

d) 单元判定:如果 1)和 2)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

9.3.3.1.3 测评单元(L4-CES3-03)

该测评单元包括以下要求:

a) 测评指标:应保证移动终端只用于处理指定业务。

b) 测评对象:移动终端和移动终端管理系统。

c) 测评实施:应核查移动终端是否只用于处理指定业务。

d) 单元判定:如果以上测评实施内容为肯定,则符合本测评单元指标要求,否则不符合本测评单元指标要求。

9.3.3.2 移动应用管控

9.3.3.2.1 测评单元(L4-CES3-04)

该测评单元包括以下要求:

a) 测评指标:应具有选择应用软件安装、运行的功能。

b) 测评对象:移动终端管理客户端。

c) 测评实施:应核查是否具有选择应用软件安装、运行的功能。

d) 单元判定:如果以上测评实施内容为肯定,则符合本测评单元指标要求,否则不符合本测评单元指标要求。

9.3.3.2.2 测评单元(L4-CES3-05)

该测评单元包括以下要求:

a) 测评指标:应只允许系统管理者指定证书签名的应用软件安装和运行。

b) 测评对象:移动终端管理客户端。

c) 测评实施:应核查全部移动应用的签名证书是否由系统管理者指定。

d) 单元判定:如果以上测评实施内容为肯定,则符合本测评单元指标要求,否则不符合本测评单元指标要求。

9.3.3.2.3 测评单元(L4-CES3-06)

该测评单元包括以下要求:

a) 测评指标:应具有软件白名单功能,应能根据白名单控制应用软件安装、运行。

b) 测评对象:移动终端管理客户端。

c) 测评实施包括以下内容：

1) 应核查是否具有软件白名单功能；

2) 应测试验证白名单功能是否能够控制应用软件安装、运行。

d) 单元判定：如果 1)和 2)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.3.3.2.4 测评单元(L4-CES3-07)

该测评单元包括以下要求：

a) 测评指标：应具有接受移动终端管理服务端推送的移动应用软件管理策略，并根据该策略对软件实施管控的能力。

b) 测评对象：移动终端。

c) 测评实施：应核查是否具有接受移动终端管理服务端远程管控的能力。

d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.3.4 安全建设管理

9.3.4.1 移动应用软件采购

9.3.4.1.1 测评单元(L4-CMS3-01)

该测评单元包括以下要求：

a) 测评指标：应保证移动终端安装、运行的应用软件来自可靠分发渠道或使用可靠证书签名。

b) 测评对象：移动终端。

c) 测评实施：应核查移动应用软件是否来自可靠分发渠道或使用可靠证书签名。

d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.3.4.1.2 测评单元(L4-CMS3-02)

该测评单元包括以下要求：

a) 测评指标：应保证移动终端安装、运行的应用软件由指定的开发者开发。

b) 测评对象：移动终端。

c) 测评实施：应核查移动应用软件是否由指定的开发者开发。

d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.3.4.2 移动应用软件开发

9.3.4.2.1 测评单元(L4-CMS3-03)

该测评单元包括以下要求：

a) 测评指标：应对移动业务应用软件开发者进行资格审查。

b) 测评对象：系统建设负责人。

c) 测评实施：应访谈系统建设负责人，是否对开发者进行资格审查。

d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.3.4.2.2 测评单元(L4-CMS3-04)

该测评单元包括以下要求:

a) 测评指标:应保证开发移动业务应用软件的签名证书合法性。

b) 测评对象:软件的签名证书。

c) 测评实施:应核查开发移动业务应用软件的签名证书是否具有合法性。

d) 单元判定:如果以上测评实施内容为肯定,则符合本测评单元指标要求,否则不符合本测评单元指标要求。

9.3.5 安全运维管理

9.3.5.1 配置管理

9.3.5.1.1 测评单元(L4-MMS3-01)

该测评单元包括以下要求:

a) 测评指标:应建立合法无线接入设备和合法移动终端配置库,用于对非法无线接入设备和非法移动终端的识别。

b) 测评对象:记录表单类文档、移动终端管理系统或相关组件。

c) 测评实施:应核查是否建立无线接入设备和合法移动终端配置库,并通过配置库识别非法设备。

d) 单元判定:如果以上测评实施内容为肯定,则符合本测评单元指标要求,否则不符合本测评单元指标要求。

9.4 物联网安全测评扩展要求

9.4.1 安全物理环境

9.4.1.1 感知节点设备物理防护

9.4.1.1.1 测评单元(L4-PES4-01)

该测评单元包括以下要求:

a) 测评指标:感知节点设备所处的物理环境应不对感知节点设备造成物理破坏,如挤压、强振动。

b) 测评对象:感知节点设备所处物理环境和设计或验收文档。

c) 测评实施包括以下内容:

1) 应核查感知节点设备所处物理环境的设计或验收文档,是否有感知节点设备所处物理环境具有防挤压、防强振动等能力的说明,是否与实际情况一致;

2) 应核查感知节点设备所处物理环境是否采取了防挤压、防强振动等的防护措施。

d) 单元判定:如果 1)和 2)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

9.4.1.1.2 测评单元(L4-PES4-02)

该测评单元包括以下要求:

a) 测评指标:感知节点设备在工作状态所处物理环境应能正确反映环境状态(如温湿度传感器不

能安装在阳光直射区域)。

b) 测评对象:感知节点设备所处物理环境和设计或验收文档。

c) 测评实施包括以下内容:

1) 应核查感知节点设备所处物理环境的设计或验收文档,是否有感知节点设备在工作状态所处物理环境的说明,是否与实际情况一致;

2) 应核查感知节点设备在工作状态所处物理环境是否能正确反映环境状态(如温湿度传感器不能安装在阳光直射区域)。

d) 单元判定:如果 1)和 2)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

9.4.1.1.3 测评单元(L4-PES4-03)

该测评单元包括以下要求:

a) 测评指标:感知节点设备在工作状态所处物理环境应不对感知节点设备的正常工作造成影响,如强干扰、阻挡屏蔽等。

b) 测评对象:感知节点设备所处物理环境和设计或验收文档。

c) 测评实施包括以下内容:

1) 应核查感知节点设备所处物理环境的设计或验收文档,是否具有感知节点设备所处物理环境防强干扰、防阻挡屏蔽等能力的说明,是否与实际情况一致;

2) 应核查感知节点设备所处物理环境是否采取了防强干扰、防阻挡屏蔽等防护措施。

d) 单元判定:如果 1)和 2)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

9.4.1.1.4 测评单元(L4-PES4-04)

该测评单元包括以下要求:

a) 测评指标:关键感知节点设备应具有可供长时间工作的电力供应(关键网关节点设备应具有持久稳定的电力供应能力)。

b) 测评对象:关键感知节点设备的供电设备(关键网关节点设备的供电设备)和设计或验收文档。

c) 测评实施包括以下内容:

1) 应核查关键感知节点设备(关键网关节点设备)电力供应设计或验收文档是否标明电力供应要求,其中是否明确保障关键感知节点设备长时间工作的电力供应措施(关键网关节点设备持久稳定的电力供应措施);

2) 应核查是否具有相关电力供应措施的运行维护记录,是否与电力供应设计一致。

d) 单元判定:如果 1)和 2)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

9.4.2 安全区域边界

9.4.2.1 接入控制

9.4.2.1.1 测评单元(L4-ABS4-01)

该测评单元包括以下要求:

a) 测评指标:应保证只有授权的感知节点可以接入。

b) 测评对象:感知节点设备和设计文档。

c) 测评实施包括以下内容:

1) 应核查感知节点设备接入机制设计文档是否包括防止非法的感知节点设备接入网络的机

制以及身份鉴别机制的描述；

2） 应对边界和感知层网络进行渗透测试，测试是否不存在绕过白名单或相关接入控制措施以及身份鉴别机制的方法。

d） 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.4.2.2 入侵防范

9.4.2.2.1 测评单元（L4-ABS4-02）

该测评单元包括以下要求：

a） 测评指标：应能够限制与感知节点通信的目标地址，以避免对陌生地址的攻击行为。

b） 测评对象：感知节点设备和设计文档。

c） 测评实施包括以下内容：

1） 应核查感知层安全设计文档，是否有对感知节点通信目标地址的控制措施说明；

2） 应核查感知节点设备，是否配置了对感知节点通信目标地址的控制措施，相关参数配置是否符合设计要求；

3） 应对感知节点设备进行渗透测试，测试是否能够限制感知节点设备对违反访问控制策略的通信目标地址进行访问或攻击。

d） 单元判定：如果 1）～3）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.4.2.2.2 测评单元（L4-ABS4-03）

该测评单元包括以下要求：

a） 测评指标：应能够限制与网关节点通信的目标地址，以避免对陌生地址的攻击行为。

b） 测评对象：网关节点设备和设计文档。

c） 测评实施包括以下内容：

1） 应核查感知层安全设计文档，是否有对网关节点通信目标地址的控制措施说明；

2） 应核查网关节点设备，是否配置了对网关节点通信目标地址的控制措施，相关参数配置是否符合设计要求；

3） 应对感知节点设备进行渗透测试，测试是否能够限制网关节点设备对违反访问控制策略的通信目标地址进行访问或攻击。

d） 单元判定：如果 1）～3）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.4.3 安全计算环境

9.4.3.1 感知节点设备安全

9.4.3.1.1 测评单元（L4-CES4-01）

该测评单元包括以下要求：

a） 测评指标：应保证只有授权的用户可以对感知节点设备上的软件应用进行配置或变更。

b） 测评对象：感知节点设备。

c） 测评实施包括以下内容：

1） 应核查感知节点设备是否采取了一定的技术手段防止非授权用户对设备上的软件应用进

行配置或变更；

2） 应通过试图接入和控制传感网访问未授权的资源，测试验证感知节点设备的访问控制措施对非法访问和非法使用感知节点设备资源的行为控制是否有效。

d） 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.4.3.1.2 测评单元（L4-CES4-02）

该测评单元包括以下要求：

a） 测评指标：应具有对其连接的网关节点设备（包括读卡器）进行身份标识和鉴别的能力。

b） 测评对象：网关节点设备（包括读卡器）。

c） 测评实施包括以下内容：

1） 应核查是否对连接的网关节点设备（包括读卡器）进行身份标识与鉴别，是否配置了符合安全策略的参数；

2） 应测试验证是否不存在绕过身份标识与鉴别功能的方法。

d） 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.4.3.1.3 测评单元（L4-CES4-03）

该测评单元包括以下要求：

a） 测评指标：应具有对其连接的其他感知节点设备（包括路由节点）进行身份标识和鉴别的能力。

b） 测评对象：其他感知节点设备（包括路由节点）。

c） 测评实施包括以下内容：

1） 应核查是否对连接的其他感知节点设备（包括路由节点）设备进行身份标识与鉴别，是否配置了符合安全策略的参数；

2） 应测试验证是否不存在绕过身份标识与鉴别功能的方法。

d） 单元判定：如果 1）和 2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.4.3.2 网关节点设备安全

9.4.3.2.1 测评单元（L4-CES4-04）

该测评单元包括以下要求：

a） 测评指标：应设置最大并发连接数。

b） 测评对象：网关节点设备。

c） 测评实施：应核查网关节点设备是否配置了最大并发连接数参数。

d） 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.4.3.2.2 测评单元（L4-CES4-05）

该测评单元包括以下要求：

a） 测评指标：应具备对合法连接设备（包括终端节点、路由节点、数据处理中心）进行标识和鉴别的能力。

b） 测评对象：网关节点设备。

c) 测评实施包括以下内容：

1) 应核查网关节点设备是否能够对连接设备(包括终端节点、路由节点、数据处理中心)进行标识并配置了鉴别功能；

2) 应测试验证是否不存在绕过身份标识与鉴别功能的方法。

d) 单元判定：如果 1)和 2)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.4.3.2.3 测评单元(L4-CES4-06)

该测评单元包括以下要求：

a) 测评指标：应具备过滤非法节点和伪造节点所发送的数据的能力。

b) 测评对象：网关节点设备。

c) 测评实施包括以下内容：

1) 应核查是否具备过滤非法节点和伪造节点发送的数据的功能；

2) 应测试验证是否能够过滤非法节点和伪造节点发送的数据。

d) 单元判定：如果 1)和 2)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9.4.3.2.4 测评单元(L4-CES4-07)

该测评单元包括以下要求：

a) 测评指标：授权用户应能够在设备使用过程中对关键密钥进行在线更新。

b) 测评对象：感知节点设备。

c) 测评实施：应核查感知节点设备是否对其关键密钥进行在线更新。

d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.4.3.2.5 测评单元(L4-CES4-08)

该测评单元包括以下要求：

a) 测评指标：授权用户应能够在设备使用过程中对关键配置参数进行在线更新。

b) 测评对象：感知节点设备。

c) 测评实施：应核查是否支持对其关键配置参数进行在线更新及在线更新方式是否有效。

d) 单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

9.4.3.3 抗数据重放

9.4.3.3.1 测评单元(L4-CES4-09)

该测评单元包括以下要求：

a) 测评指标：应能够鉴别数据的新鲜性，避免历史数据的重放攻击。

b) 测评对象：感知节点设备。

c) 测评实施包括以下内容：

1) 应核查感知节点设备鉴别数据新鲜性的措施，是否能够避免历史数据重放；

2) 应将感知节点设备历史数据进行重放测试，验证其保护措施是否生效。

d) 单元判定：如果 1)和 2)均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评

单元指标要求。

9.4.3.3.2 测评单元(L4-CES4-10)

该测评单元包括以下要求:

a) 测评指标:应能够鉴别历史数据的非法修改,避免数据的修改重放攻击。

b) 测评对象:感知节点设备。

c) 测评实施包括以下内容:

1) 应核查感知层是否配备检测感知节点设备历史数据被非法篡改的措施,在检测到被修改时是否能采取必要的恢复措施;

2) 应测试验证是否能够避免数据的修改重放攻击。

d) 单元判定:如果 1)和 2)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

9.4.3.4 数据融合处理

9.4.3.4.1 测评单元(L4-CES4-11)

该测评单元包括以下要求:

a) 测评指标:应对来自传感网的数据进行数据融合处理,使不同种类的数据可以在同一个平台被使用。

b) 测评对象:物联网应用系统。

c) 测评实施包括以下内容:

1) 应核查是否提供对来自传感网的数据进行数据融合处理的功能;

2) 应测试验证数据融合处理功能是否能够处理不同种类的数据。

d) 单元判定:如果 1)和 2)均为肯定,则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

9.4.3.4.2 测评单元(L4-CES4-12)

该测评单元包括以下要求:

a) 测评指标:应对不同数据之间的依赖关系和制约关系等进行智能处理,如一类数据达到某个门限时可以影响对另一类数据采集终端的管理指令。

b) 测评对象:物联网应用系统。

c) 测评实施:应核查是否能够智能处理不同数据之间的依赖关系和制约关系。

d) 单元判定:如果以上测评实施内容为肯定,则符合本测评单元指标要求,否则不符合本测评单元指标要求。

9.4.4 安全运维管理

9.4.4.1 感知节点管理

9.4.4.1.1 测评单元(L4-MMS4-01)

该测评单元包括以下要求:

a) 测评指标:应指定人员定期巡视感知节点设备、网关节点设备的部署环境,对可能影响感知节点设备、网关节点设备正常工作的环境异常进行记录和维护。

b) 测评对象:维护记录。