工业互联网产业联盟
Alliance of Industrial Internet

工 业 互 联 网 产 业 联 盟 标 准

AII/004-2018

工业互联网平台 安全防护要求

Security Protection Requirements for Industrial Internet Platform

工业互联网产业联盟

（2018 年 2 月 2 日发布）

目　录

前　　言

本标准是工业互联网安全系列标准之一。

—工业互联网　　安全总体要求

—工业互联网　　安全接入要求

—工业互联网平台　安全防护要求

—工业互联网　　安全能力成熟度评估规范

—工业互联网　　数据安全保护要求

随着技术的发展，还将制定后续的相关标准。

标准牵头单位：中国信息通信研究院

标准起草单位和主要起草人：

中国信息通信研究院：李艺、田慧蓉、罗成

华为技术有限公司：王雨晨、耿涛

北京奇虎科技有限公司：陶耀东、郭颖

中国移动通信集团有限公司：张峰

中兴通讯股份有限公司：黄树强

中国电子信息产业集团有限公司第六研究所：卢凯

航天云网科技发展有限责任公司：于文涛、邹萍、姜海森、梁栋

富士康科技集团：陈金星

用友网络科技股份有限公司：杨宝刚

三一集团：彭卓、张声勇

北京和利时智能技术有限公司：龚涛

中国科学院沈阳自动化研究所：李栋

海尔集团：陈云峰、张海港

工业互联网平台安全防护要求

1 范围

本标准针对工业互联网平台对于安全防护方面的需求，规定了工业互联网平台安全防护的总体要求，主要包括边缘层安全、平台IaaS层安全、平台PaaS层安全、平台SaaS层安全等。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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。

AII/002-2017	工业互联网平台 可信服务评估评测要求
工业互联网产业联盟报告	工业互联网平台白皮书（2017）
YD/T 2439-2012	移动互联网恶意程序描述格式

3 缩略语

下列缩略语适用于本文件。

IaaS	基础设施即服务	Infrastructure as a Service
PaaS	平台即服务	Platform as a Service
SaaS	软件即服务	Software as a Service
APP	应用程序	Application

4 术语和定义

下列术语和定义适用于本文件。

4.1

工业互联网平台　Industrial Internet Platform

工业互联网平台是面向制造业数字化、网络化、智能化需求，构建基于海量数据采集、汇聚、分析的服务体系，支撑制造资源泛在连接、弹性供给、高效配置的工业云平台。

5　工业互联网平台架构简介

根据《工业互联网平台白皮书（2017）》中的定义，工业互联网平台是面向制造业数字化、网络化、智能化需求，构建基于海量数据采集、汇聚、分析的服务体系，支撑制造资源泛在连接、弹性供给、高效配置的工业云平台，包括边缘、平台（工业PaaS）、应用三大核心层级。可以认为，工业互联网平台是工业云平台的延伸发展，其本质是在传统云平台的基础上叠加物联网、大数据、人工智能等新兴技术，构建更精准、实时、高效的数据采集体系，建设包括存储、集成、访问、分析、管理功能的使能平台，实现工业技术、经验、知识模型化、软件化、复用化，以工业应用程序的形式为制造企业各类创新应用，最终形成资源富集、多方参与、合作共赢、协同演进的制造业生态。

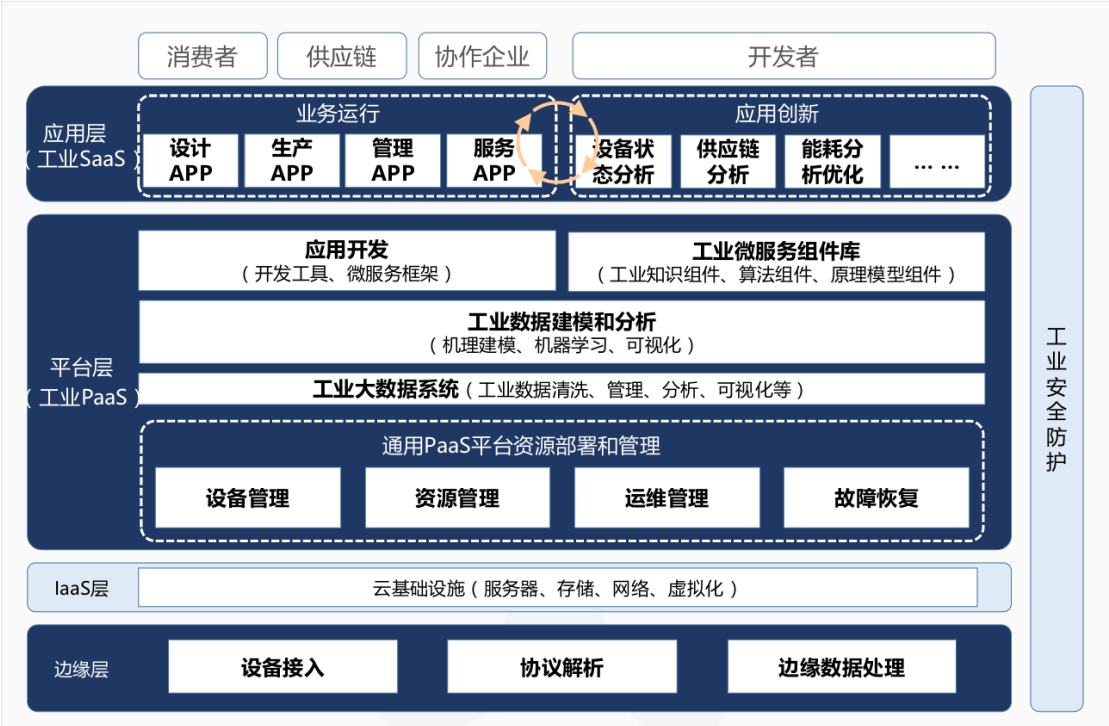

图1　工业互联网平台功能架构图

第一层是边缘，通过大范围、深层次的数据采集，以及异构数据的协议转换与边缘处理，构建工业互联网平台的数据基础。一是通过各类通信手段接入不同设备、系统和产品，采集海量数据；二是依托协议转换技术实现多源异构数据的归一化和边缘集成；三是利用边缘计算设备实现底层数据的汇聚处理，并实现数据向云端平台的集成。

第二层是平台，基于通用PaaS叠加大数据处理、工业数据分析、工业微服务等创新功能，构建可扩展的开放式云操作系统。一是提供工业数据管理能力，将数据科学与工业机理结合，帮助制造企业构建工业数据分析能力，实现数据价值挖掘；二是把技术、知识、经验等资源固化为可移植、可复用的工业微服务组件库，供开发者调用；三是构建应用开发环境，借助微服务组件和工业应用开发工具，帮助用户快速构建定制化的工业应用程序。

第三层是应用，形成满足不同行业、不同场景的工业SaaS和工业应用程序，形成工业互联网平台的最终价值。一是提供了设计、生产、管理、服务等一系列创新性业务应用。二是构建了良好的工业应用程序创新环境，使开发者基于平台数据及微服务功能实现应用创新。

除此之外，工业互联网平台还包括IaaS基础设施，以及涵盖整个工业系统的安全管理体系，这些构成了工业互联网平台的基础支撑和重要保障。

泛在连接、云化服务、知识积累、应用创新是辨识工业互联网平台的四大特征。一是泛在连接，具备对设备、软件、人员等各类生产要素数据的全面采集能力。二是云化服务，实现基于云计算架构的海量数据存储、管理和计算。三是知识积累，能够提供基于工业知识机理的数据分析能力，并实现知识的固化、积累和复用。四是应用创新，能够调用平台功能及资源，提供开放的工业应用程序开发环境，实现工业应用程序创新应用。

6 工业互联网平台安全防护需求

数据接入安全：防止数据泄漏、被侦听或篡改，保障数据在源头和传输过程中安全。

平台安全：确保工业互联网平台的代码安全、应用安全、数据安全、网站安全。

访问安全：通过建立统一的访问机制，限制用户的访问权限和所能使用的计算资源和网络资源实现对工业互联网平台重要资源的访问控制和管理，防止非法访问。

7 工业互联网平台安全防护总体要求

7.1 工业互联网平台安全防护总体原则

本标准规定的工业互联网平台安全防护要求按照平台的功能和安全要求的强度，分为基本级要求和增强级要求。

基本级要求是工业互联网平台在提供服务时应具备必要的安全控制措施，保护工业互联网平台能够抵御或应对常见的攻击、威胁。

增强级要求是对基本要求的补充和强化，是工业互联网平台保障服务安全时提供的更高级别的安全控制措施。

工业互联网平台用户根据自身业务需求及存储的信息敏感程度选择相应安全防护水平的工业互联网平台提供者，或者自行搭建符合安全要求的工业互联网平台。

7.2 工业互联网平台安全防护范围

本标准的安全防护范围主要针对工业互联网平台提出安全防护要求。其防护范围包括构成工业互联网平台的各类物理或虚拟基础设施资源、数据分析服务、开发套件、工业应用等，对接入工业互联网平台的工业现场设备的安全防护要求见相应的安全防护标准，本标准不作要求。

7.3 工业互联网平台安全防护内容

工业互联网平台安全防护内容及要求可划分边缘层、平台 IaaS 层、平台 PaaS 层及平台 SaaS 层四个层面。

- 边缘层

包括为实现工业互联网场景中各类现场设备接入所提供的接口、协议解析能力及边缘计算能力等。

- 平台 IaaS 层

包括支撑工业互联网平台运行的各类物理及虚拟资源，如服务器、存储、网

络、虚拟化等。

- 平台 PaaS 层

包括数据分析服务、平台微服务组件、平台应用开发环境等。

- 平台 SaaS 层

包括面向各类工业应用场景的业务应用及其配套应用程序等。

8 基本级安全防护要求

8.1 边缘层安全防护要求

8.1.1 网络架构

应设置单独的接入安全区域，并分配已规划的地址空间。

8.1.2 边界防护

a) 工厂内部网络与工厂外部网络的边界应该具有隔离措施；
b) 能够对非授权设备的接入行为进行告警。

8.1.3 访问控制

a) 接入网络边界网关只开放接入服务相关的端口；
b) 边界安全网关通过 ACL 检测机制对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据进出。

8.1.4 入侵防范

a) 能够检测接入设备发起的 DDoS 等网络攻击行为；
b) 当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应能够告警。

8.1.5 安全审计

a) 应对接入用户的重要安全事件和重要行为进行审计；
b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；
d) 审计日志应符合相关法律法规要求。

8.2 平台 IaaS 层安全防护要求

8.2.1 服务器安全防护要求

8.2.1.1 身份鉴别认证

身份鉴别认证应符合以下要求：

a) 应对登录服务器的用户进行身份标识和鉴别。

b) 服务器管理用户身份标识应具有不易被冒用的特点，口令应有复杂度要求并定期更换。

c) 应启用登录失败处理功能，可采取结束会话、限制非法登陆次数和自动退出等措施。

d) 应采用安全方式防止用户鉴别认证信息泄露而造成身份冒用。

8.2.1.2 访问控制

访问控制应符合以下要求：

a) 应采用技术措施对允许访问服务器的终端地址范围进行限制。

b) 应关闭服务器不使用的端口，防止非法访问。

c) 应根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限。

8.2.1.3 安全审计

安全审计应符合以下要求：

a) 审计范围应覆盖到服务器上的每个用户。

b) 审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等重要的安全相关事件。

c) 审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等。

d) 保护审计记录，有效期内避免受到非授权的访问、篡改、覆盖或删除等。

e) 应支持按用户需求提供与其相关的审计信息及审计分析报告。

8.2.1.4 资源控制

资源控制应符合以下要求：

a) 应根据安全策略，设置登录终端的会话数量。

b) 应根据安全策略设置登录终端的操作超时锁定。

8.2.1.5 恶意代码防范

恶意代码防范应符合以下要求：应安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库。

8.2.1.6 入侵防范

入侵防范应符合以下要求：

a) 所使用的操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，保持系统补丁及时得到更新。

b) 应能够检测到对重要服务器进行入侵的行为，能够记录入侵的源 IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警。

8.2.2 存储安全防护要求

8.2.2.1 数据产生

数据产生应符合以下要求：

a) 应具有数据敏感度的界定标准。

b) 数据产生时，应根据数据的敏感度进行分类。

8.2.2.2 数据传输

数据传输应符合以下要求：

a) 应采用技术措施保证鉴别信息（指用于鉴定用户身份是否合法的信息，如用户登录各种业务系统的账号和密码、服务密码等）传输的保密性。

b) 应支持用户实现对关键业务数据和管理数据传输的保密性。

c) 应能够检测到数据在传输过程中完整性受到破坏。

8.2.2.3 数据存储

数据存储应符合以下要求：

a) 应采用加密技术或其他保护措施实现鉴别信息的存储保密性。

b) 应支持用户实现对关键业务数据和管理数据的存储保密性。

c) 应支持用户对密码算法、强度和方式等参数的可选配置。

d) 应提供有效的磁盘保护方法或数据碎片化存储等措施，保证及时磁盘被

窃取，非法用户也无法从磁盘中获取有效的用户数据。

e) 应能够检测到数据在存储过程中完整性受到破坏。

8.2.2.4 数据使用

数据使用应符合以下要求：

应对数据的使用进行授权和验证。

8.2.2.5 数据迁移

数据迁移应符合以下要求：

a) 应进行数据迁移前的网络安全能力评估，保证数据迁移的安全实施。

b) 应保证数据在不同虚拟机之间迁移不影响业务应用的连续性。

c) 数据迁移中应做好数据备份以及恢复相关工作。

8.2.2.6 数据销毁

数据销毁应符合以下要求：

a) 应能够提供手段协助清除因数据在不同存储设备间迁移、业务终止、自然灾害、合同终止等遗留的数据，对日志的留存期限应符合国家有关规定。

b) 应提供手段清除数据的所有副本。

8.2.2.7 备份和恢复

备份和恢复应符合以下要求：

应提供数据本地备份与恢复功能，全量数据备份至少每周一次，增量备份至少每天一次，或提供多副本备份机制。

8.2.3 网络安全防护要求

8.2.3.1 网络区域划分隔离

网络区域划分隔离应符合以下要求：应根据平台服务的类型、功能及租户的不同划分不同的子网、网段或安全组，并在各子网、网段或安全组之间采取必要的技术手段进行隔离。

8.2.3.2 访问控制

访问控制应符合以下要求：

a) 应在（子）网络或网段边界部署访问控制设备并启用访问控制功能，或通过安全组设置访问控制策略。

b) 应能根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，控制力度到主机级。

8.2.3.3 安全审计

安全审计符合以下要求：

a) 应对网络系统中的网络设备运行状况、网络流量、管理员和运维人员行为等进行日志记录。

b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。

c) 应保证所有网络设备的系统时间自动保持一致。

d) 应对审计记录进行保护，有效期内避免受到非授权的访问、篡改、覆盖或删除等。

e) 应按用户需求提供与其相关的审计信息及审计分析报告。

8.2.3.4 恶意代码防范

恶意代码防范应符合以下要求：

应对恶意代码进行检测和清除。

8.2.3.5 网络设备防护

网络设备防护应符合以下要求：

a) 应对登录网络设备的用户进行身份鉴别。

b) 应对网络设备的管理员登录地址进行限制。

c) 网络设备用户的标识应唯一。

d) 身份鉴别信息应具有不易被冒用的特点，口令应有复杂度要求并定期更换。

8.2.3.6 网络安全监测要求

网络安全监测应符合以下要求：

a) 应对网络系统中的网络设备运行状况、网络流量、管理员和运维人员行为等进行监测，识别和记录异常状态。

b) 应根据用户需求支持对持续大流量攻击进行识别、报警和阻断的能力。

c) 应监视是否对平台服务存在以下攻击行为：端口扫描、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等。

d) 当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警。

8.2.4 虚拟化安全防护要求

8.2.4.1 虚拟机安全

虚拟机安全应符合以下要求：

a) 应支持虚拟机之间、虚拟机与宿主机之间的隔离。

b) 应支持虚拟机部署防病毒软件。

c) 应具有对虚拟机恶意攻击等行为的识别并处置的能力。

d) 应支持对虚拟机脆弱性进行检测的能力。

8.2.4.2 虚拟网络安全

虚拟机网络安全应符合以下要求：

a) 应部署一定的访问控制安全策略，以实现虚拟机之间、虚拟机与虚拟机管理平台之间、虚拟机与外部网络之间的安全访问控制。

b) 应支持采用 VLAN 或者分布式虚拟交换机等技术，以实现网络的安全隔离。

c) 应支持不同租户之间的网络隔离。

8.2.4.3 虚拟化平台安全

虚拟化平台安全应符合以下要求：

a) 应保证每个虚拟机能获得相对独立的物理资源，并能屏蔽虚拟资源故障，确保某个虚拟机崩溃后不影响虚拟机监控器及其他虚拟机。

b) 应保证不同虚拟机之间的虚拟 CPU 指令隔离。

c) 应保证不同虚拟机之间的内存隔离，内存被释放或再分配给其他虚拟机前得到完全释放。

d) 应保证虚拟机只能访问分配给该虚拟机的存储空间（包括内存空间和磁盘空间）。

e) 应对虚拟机的运行状态、资源占用等信息进行监控。

f) 应支持发现虚拟化平台漏洞的能力，支持漏洞修复。

8.3 平台 PaaS 层安全防护要求

8.3.1 数据分析服务安全防护要求

8.3.1.1 数据挖掘

a) 针对不同接入方式的数据挖掘用户，应采用不同的认证方式。需要检查使用数据的合法性和有效性。

b) 挖掘算法在使用前，必须申报算法使用的数据范围、挖掘周期、挖掘目的、以及挖掘结果的应用范围等内容。算法提供者必须对算法的安全性和可靠性提供必要的验证与测试方案。

c) 在数据挖掘过程中，应对挖掘算法使用的数据范围、数据状态、数据格式、数据内容等进行监控。

d) 禁止挖掘算法对数据存储区域内的原始数据进行增加、修改、删除等操作，以保证原始数据的可用性和完整性。

e) 禁止将挖掘算法产生的中间过程数据与原始数据存储于同一空间，以防数据使用的混乱、加大数据存储的管理难度。同时，应周期性的检查用户操作数据的情况，统一管理数据使用权限。

f) 不同应用之间应进行数据关联性隔离，防止不同应用之间的 ECA 分析，产生数据泄露。

g) 应对挖掘内容、过程、结果、用户进行安全审计。主要包括挖掘内容的合理性、挖掘过程的合规性、挖掘结果的可用性，以及挖掘用户的安全性。

h) 应对源数据和挖掘结果进行签识，防止数据被恶意删除、随意篡改、无约束的滥用。

i) 如需将收集到的信息共享给第三方应用，应对信息进行脱敏处理，严格保护用户隐私不被泄露。

8.3.1.2 数据输出

a) 应对应用数据的各种操作行为、操作结果予以完整记录，确保操作行为的可追溯。

b) 应对所有输出的数据内容都进行合规性审计，审计范围包括数据的真实性、一致性、完整性、归属权、使用范围等。

c) 应对数据输出的接口进行规范管理，管理内容包括数据输出接口类型、加密方式、传输周期、使用用途、认证方式等。

d) 如需将数据输出到平台以外的实体时，在输出前应对数据进行脱敏操作，确保输出的数据满足约定的要求且不泄露敏感信息。

e) 应对所有审计行为留有记录并独立存储，严禁在任何情况下开放对审计结果的修改与删除权限。

8.3.2 微服务组件安全防护要求

8.3.2.1 身份鉴别

身份鉴别认证应符合以下要求：

a) 应对管理微服务组件的用户进行身份标识和鉴别。

b) 管理微服务组件的用户身份标识应具有不易被冒用的特点，口令应有复杂度要求并定期更换。

c) 应启用登录失败处理功能，可采取结束会话、限制非法登陆次数和自动退出等措施。

d) 应采用安全方式防止用户鉴别认证信息泄露而造成身份冒用。

8.3.2.2 访问控制

在微服务组件权限配置能力内，根据用户的业务需要，配置其所需的最小权限。

8.3.2.3 安全审计

安全审计应符合以下要求：

a) 审计范围应覆盖到使用微服务组件的每个用户。

b) 审计内容应包括重要用户行为、微服务组件资源的异常使用和重要操作命令的使用等重要的安全相关事件。

c) 审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等。

d) 保护审计记录，有效期内避免受到非授权的访问、篡改、覆盖或删除等。

e) 应支持按用户需求提供与其相关的审计信息及审计分析报告。

8.3.2.4 开放接口

a) 微服务组件应有与外部组件或应用之间开放接口的安全管控措施，接口协议操作应通过接口代码审计、黑、白名单等控制措施确保交互符合接口规范。

b) 应对开放接口调用有认证措施。

c) 应对关键接口的调用情况进行技术监控，如调用频率、调用来源等。

d) 应用开放接口生成的业务应用或应用程序在供用户下载之前应通过安全检测。

e) 应制定开放接口管理机制和网络安全应急管理制度。

8.3.3 平台应用开发环境安全防护要求

8.3.3.1 身份鉴别

a) 对保留用户个人信息或用户服务信息的业务，应对登录用户进行身份标识和鉴别。

b) 对要求提供登录功能的开发环境，应提供并启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施。

c) 对要求提供登录功能的开发环境，应提供并启用用户身份标识唯一检查功能，保证开发环境中不存在重复用户身份标识。应提供并启用用户鉴别信息复杂度检查功能，保证身份鉴别信息不易被冒用。

d) 应采用加密方式存储用户的账号和口令信息。

8.3.3.2 访问控制

a) 应由授权主体配置访问控制策略，并严格限制默认用户的访问权限。

b) 应严格限制各用户的访问权限，按安全策略要求控制用户对业务、数据、网络资源等的访问。

8.3.3.3 安全审计

a) 审计范围应覆盖到每个用户的关键操作。

b) 审计内容应包括对用户的重要行为、资源使用情况等重要事件。

c) 应保护审计记录，保证无法删除、修改或覆盖等。

d) 相关审计记录应包括事件日期、时间、发起者信息、类型、描述和结果等，并且保留一定期限（具体期限应符合相关法律法规要求）。

8.3.3.4 资源控制

当用户和开发环境的通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话。

8.3.3.5 信息保护

a) 开发环境中各功能的提供、控制与管理过程应保护用户隐私，未经用户同意，不能擅自收集、修改、泄漏用户相关敏感信息。
b) 应保护相关信息的安全，避免相关数据和页面被篡改和破坏。
c) 应禁止不必要的内嵌网络服务，应禁止在用户端自动安装恶意软件和插件。
d) 应对通信过程中的敏感信息字段进行加密。
e) 应对敏感信息(如用户信息、订单信息、应用软件下载路径等)进行加密存储。
f) 应对开发环境相关功能的关键数据（如业务数据、系统配置数据、管理员操作维护记录、用户信息、业务应用与应用程序购买、下载信息等）应有必要的容灾各份。
g) 应能对诈骗、虚假广告等信息建立处理机制，防止类似信息的扩散。

8.3.3.6 上线前检测

a) 开发环境应在业务应用与工业应用程序上线前对其进行安全审核，以确保其不包含恶意代码、恶意行为等，经过安全审核后才能进行上线处理、正式发布。
b) 开发环境可提供用户数据同步功能，但开发环境同步的用户数据不应保存在位于境外的服务器上。
c) 开发环境应支持对工业应用程序的移动代码签名机制，对应用程序检测审核后，对其进行数字签名。移动终端在下载安装工业应用程序之前，对经过签名的应用程序进行签名验证，只有通过签名验证的应用程序才能被认为是可信的，继而被安装到终端上。

d) 开发环境应对已经上线的业务应用与工业应用程序进行拨测抽查，并记录拨测过程及结果，针对违规行为、可疑行为等进行相应的处理。业务应用与工业应用程序拨测应采用自动拨测与人工拨测相结合的方式进行。

e) 开发环境应要求开发者在提交业务应用与工业应用程序时声明其调用的API，并对业务应用与工业应用程序调用终端 API 的行为进行检测。业务应用与工业应用程序不应调用与其业务功能无关的API以及在其声明范围之外的 API。

8.4 平台 SaaS 层安全防护要求

8.4.1 业务应用安全防护要求

8.4.1.1 身份鉴别

身份鉴别应符合以下要求：应采用一种或一种以上组合的鉴别技术来进行身份鉴别。

8.4.1.2 访问控制

访问控制应符合以下要求：

a) 应严格限制用户的访问权限，按安全策略要求控制用户对业务应用的访问。

b) 应严格限制应用与应用之间相互调用的权限，按照安全策略要求控制应用对其他应用里用户数据或特权指令等资源的调用。

8.4.1.3 安全审计

安全审计应符合以下要求：

a) 审计范围应覆盖到用户在业务应用中的关键操作、重要行为、业务资源使用情况等重要事件。

b) 应对审计记录进行保护，有效期内避免受到非授权的访问、篡改、覆盖或删除等。

c) 应定期针对审计日志进行人工审计。

d) 应支持按用户需求提供与其相关的审计信息及审计分析报告。

8.4.1.4 资源控制

资源控制应符合以下要求：

a) 应限制对应用访问的最大并发会话连接数等资源配额。

b) 应提供资源控制不当的报警及响应。

c) 应在会话处于非活跃一定时间或会话结束后终止会话连接。

8.4.2 工业应用程序安全防护要求

8.4.2.1 逻辑安全

逻辑安全应符合以下要求：

8.4.2.1.1 身份鉴别

a) 应提供专门的登录控制模块对登录用户进行身份标识和鉴别，并保证用户身份标识的唯一性。

b) 应提供并启用用户登录口令复杂度检查功能，保证身份信息不易被冒用。

c) 应提供并启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施。

d) 应采用加密方式存储用户的登录口令信息。

8.4.2.1.2 访问控制

a) 应由经过授权的主体配置访问控制策略，严格限制各用户的访问权限，按安全策略要求控制用户对业务、数据、网络资源等的访问。

b) 应严格设置登录策略，按安全策略要求具备防范账户暴力破解攻击措施的能力（如限定用户连续错误输入密码次数，超过设定阈值，对用户进行锁定，并设定锁定时间，在锁定时间内被锁定的用户需通过注册时的标志信息进行密码重新设定或者凭有效证件进行设定）。

c) 当进行业务权限更改时（如密码重置、密码找回等），应设置相关策略，防止暴力破解攻击。

d) 业务订购、变更、退订流程应根据实际业务需求，应采用“认证码”或“二次短信认证”等方式加强安全性，应限定同一用户每日业务订购次数。

8.4.2.1.3 安全审计

a) 审计范围应覆盖到每个用户的关键操作、重要行为、业务资源使用情况

等重要事件（如普通用户异常登录、发布恶意代码、异常修改账号信息等行为，以及管理员在业务功能及账号控制方面的关键操作）。

b) 应保护审计记录，保证无法删除、修改或覆盖等。

c) 业务相关审计记录应包括事件日期、时间、发起者信息、类型、描述和结果等。

d) 应具备对审计记录数据进行统计、查询、分析及生成审计报表的功能。

8.4.2.1.4 其他

a) 当工业应用程序和平台服务的通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话。

b) 应能对含有恶意代码链接的信息建立发现和处理机制，防止类似信息的扩散。

c) 工业应用程序运行时，未经用户同意，不得擅自为用户自动开启其他服务功能（如定位等）。

8.4.2.2 原生应用及后台系统安全

原生应用及后台系统安全应符合以下要求：

8.4.2.2.1 输入验证

应对输入数据做严格验证，默认所有输入都可能包含恶意信息。

8.4.2.2.2 身份认证

a) 应确保身份认证模块不能被非法绕过。

b) 软件的用户身份鉴别模块应对用户身份鉴别信息进行保护，防止泄露。

8.4.2.2.3 会话管理

应采取会话保护措施保障工业应用程序与平台服务之间的会话不可被窃听、篡改、伪造、重放等。

8.4.2.2.4 数据存储

应确保工业应用程序配置信息、用户认证信息等敏感数据采用加密方式存储。

8.4.2.2.5 日志记录

a) 后台日志记录范围应覆盖到每个用户的关键操作、重要行为、业务资源使用情况等重要事件（如普通用户异常登录、发布恶意代码、异常修改账号信息等行为，以及管理员在业务功能及账号控制方面的关键操作）。

b) 应禁止在后台以及客户端日志中记录用户登录口令等敏感信息，如果确实需要记录敏感信息，则应进行模糊化处理。

c) 应防止日志欺骗，如果在生成后台日志时需要引入来自非受信源的数据，则需要进行严格校验，防止日志欺骗攻击。

d) 应确保后台日志数据的安全存储并严格限制日志数据的访问权限，可对后台日志记录进行签名来实现防篡改。

8.4.2.2.6 其他

a) 工业应用程序不应含有移动互联网恶意程序。移动互联网恶意程序的判定依据见 YD/T 2439-2012 的相关要求。

b) 应确保软件内存管理不存在逻辑缺陷，如未释放资源、敏感信息驻留内存等。

c) 应确保软件不非法操作与自身功能不相关的文件（如图片、通信录、其他应用软件等）。

d) 客户端软件应进行代码变量隐藏。

8.4.2.3 Web 应用及后台系统安全

Web 应用及后台系统安全应符合以下要求：

8.4.2.3.1 输入验证

a) 应对输入数据（如文件路径、URL 地址等）做安全验证，默认所有输入都可能包含恶意信息，并尽量使用白名单验证方法。

b) 应在服务器端进行输入验证，避免客户端输入验证被绕过。

c) 关键参数应直接从服务器端提取，避免从客户端输入，防止关键参数被篡改。

8.4.2.3.2 身份认证

a) 应禁止明文传输用户密码，可采用 SSL/TLS 加密隧道确保用户密码的传输安全。

b) 应禁止在数据库或文件系统中明文存储用户密码，可采用单向散列值在数据库中存储用户密码，降低存储的用户密码被字典攻击的风险。

c) 应禁止在 COOKIE 中保存明文用户密码。

d) 应采取措施防止暴力破解、恶意注册、恶意占用资源等行为。

e) 应对关键业务操作进行二次鉴权，例如修改用户认证鉴权信息（如密码、密码取回问题及答案、绑定手机号码等），避免用户身份被冒用。

f) 应避免认证错误提示泄露信息，在认证失败时，应向用户提供通用的错误提示信息（如不应区分是账号错误还是密码错误），避免这些错误提示信息被攻击者利用。

g) 应支持密码策略设置，从业务系统层面支持强制的密码策略，包括密码长度、复杂度、更换周期等，特别是业务系统的管理员密码。

h) 应支持账号锁定功能，系统应限制连续登录失败次数，在客户端多次尝试失败后，服务器端需要对用户账号进行短时锁定，且锁定策略支持配置解锁时长。

i) 应确保用户不能访问到未授权的功能和数据，未经授权的用户试图访问受限资源时，系统应予以拒绝或提示用户进行身份鉴权。

8.4.2.3.3 会话管理

a) 应确保会话的安全创建。在用户认证成功后，应为用户创建新的会话并释放原有会话；创建的会话标识应满足随机性和长度要求，避免被攻击者猜测；会话与 IP 地址可绑定，降低会话被盗用的风险。

b) 应确保会话数据的存储安全。用户登录成功后所生成的会话数据应存储在服务器端，并确保会话数据不能被非法访问；当更新会话数据时，要对数据进行严格的输入验证，避免会话数据被非法篡改。

c) 应确保会话数据的传输安全，防止泄露会话标识。

d) 应确保会话的安全终止。当用户登录成功并成功创建会话后，应在 Web 应用系统的各个页面提供用户登出功能，登出时应及时删除服务器端的会话数据；当处于登录状态的用户直接关闭浏览器时，需要提示用户执行安全登出或者自动为用户完成登出过程，从而安全的终止本次会话。

e) 应设置合理的会话超时阈值，在合理范围内尽可能减小会话超时阈值，

可以降低会话被劫持和重复攻击的风险，超过会话超时阈值后立刻销毁会话，清除会话的信息。

f) 应限制会话并发连接数，限制同一用户的会话并发连接数，避免恶意用户创建多个并发的会话来消耗系统资源，影响业务的可用性。

g) 在涉及到关键业务操作的 Web 页面，应为当前 Web 页面生成一次性随机令牌，作为主会话标识的补充。在执行关键业务前，应确保用户提交的一次性随机令牌与服务器端保存的一次性随机令牌匹配，以避免跨站请求伪造等攻击。

8.4.2.3.4 数据存储

a) 对于不同类别的数据，比如日志记录和业务数据，应采取相应的隔离措施和安全保护措施。

b) 禁止在客户端本地存储用户敏感数据，如用户密码、身份信息等。

c) 应避免在代码中硬编码密码（即在代码中直接嵌入密码，会导致密码修改困难，甚至密码的泄露），可从配置文件载入密码。

d) 在配置文件中禁止明文存储数据库连接密码、FTP 服务密码、主机密码、外部系统接口认证密码等。

8.4.2.3.5 数据传输

应确保通信信道的安全，在客户端与 Web 服务器之间使用并正确配置 SSL/TLS，应使用 SSL3.0/TLS1.0 以上版本，对称加密密钥长度不少于 128 位，非对称加密密钥长度不少于 1024 位，单向散列值位数不小于 128 位。

8.4.2.3.6 日志记录

a) 后台日志记录范围应覆盖到每个用户的关键操作、重要行为、业务资源使用情况等重要事件。如普通用户异常登录、发布恶意代码、异常修改账号信息等行为，以及管理员在业务功能及账号控制方面的关键操作。

b) 应禁止在后台日志中记录用户密码等敏感信息，如果确实需要记录敏感信息，则应进行模糊化处理。

c) 应防止日志欺骗，如果在生成后台日志时需要引入来自非受信源的数据，则需要进行严格校验，防止日志欺骗攻击。

d) 应禁止将后台日志保存到 Web 目录下，确保日志数据的安全存储并严格限制日志数据的访问权限，可对日志记录进行签名来实现防篡改。

8.4.2.3.7 其他

a) 应有技术手段检测和避免 Web 业务系统域名、访问链路的异常、访问延迟、解析错误等情况，并有应急处理能力。

b) 应避免存在常见的 Web 漏洞（如 SQL 注入、跨站脚本、跨站请求伪造等）。

c) 应能检测挂马、暗链等 Web 业务系统入侵事件，并有应急处理能力。

9 增强级安全防护要求

9.1 边缘层安全防护要求

9.1.1 网络架构

除满足基本级的要求之外，还应符合以下要求：

避免接入设备与重要信息系统直接互连，可通过信息交换系统或者共享系统来进行数据的交互。

9.1.2 传输保护

a) 应保证通信过程中的数据完整性。

b) 应保证通信过程中的关键信息的保密性。

9.1.3 边界防护

除满足基本级的要求之外，还应符合以下要求：

a) 能够对非授权设备的接入行为进行告警和阻断。

b) 对于有线和无线接入，确保通过受控的边界防护设备或者其上的指定端口接入网络。

9.1.4 访问控制

除满足基本级的要求之外，还应符合以下要求：

a) 对接入网络数据进行深度包检测。

b) 采用白名单控制方式，只允许合法设备接入网络。

c) 采用 IP-MAC 绑定、802.1x、证书、标识码等技术对接入的 PC 机、便携机、智能终端等设备进行注册认证。

d) 终端接入后，限制该终端的访问权限，并限制其他设备与该终端的非授权通信。

e) 在一个非活动时间周期后，可以通过自动方式或者手动方式终止用户远程连接。

9.1.5 入侵防范

除满足基本级的要求之外，还应符合以下要求：

能够对未知威胁进行分析和防范。

9.1.6 安全审计

除满足基本级的要求之外，还应符合以下要求：

审计记录产生时的时间应由系统范围内唯一确定的时钟产生，以确保审计分析的正确性。

9.2 平台 IaaS 层安全防护要求

9.2.1 服务器安全防护要求

9.2.1.1 身份鉴别认证

除满足基本级的要求之外，还应符合以下要求：

当对服务器进行远程管理时，应采取加密措施，防止鉴别信息在网络传输过程中被窃取。

9.2.1.2 访问控制

同基本级要求。

9.2.1.3 安全审计

除满足基本级的要求之外，还应符合以下要求：

a) 应能够根据记录数据进行分析，并生成审计报表。

b) 应保护审计进程，避免受到未预期的中断。

c) 应能汇聚服务范围内的审计数据，支持第三方审计。

9.2.1.4 资源控制

除满足基本级的要求之外，还应符合以下要求：

应对重要服务器进行性能监测，包括服务器的 CPU、硬盘、内存、网络等资源的使用情况，发现异常情况提供告警，并进行相应处置。

9.2.1.5 恶意代码防范

除满足基本级的要求之外，还应符合以下要求：

应支持对防恶意代码的统一管理。

9.2.1.6 入侵防范

除满足基本级的要求之外，还应符合以下要求：

应能够对重要程序的完整性进行检测，并在检测到完整性受到破坏后具有恢复的措施。

9.2.2 存储安全防护要求

9.2.2.1 数据产生

同基本级要求。

9.2.2.2 数据传输

除满足基本级的要求之外，还应符合以下要求：

应能够检测到数据在传输过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施。

9.2.2.3 数据存储

除满足基本级的要求之外，还应符合以下要求：

a) 应能够检测到数据在存储过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施。

b) 应支持用户选择第三方加密及密钥管理机制对用户关键数据进行加密。

c) 应提供有效的虚拟机镜像文件加载保护机制，保证即使虚拟机镜像被窃取，非法用户也无法直接在其计算资源上进行挂卷运行。

9.2.2.4 数据使用

除满足基本级的要求之外，还应符合以下要求：

应对敏感数据的使用进行审计，并形成审计日志。

9.2.2.5 数据迁移

除满足基本级的要求之外，还应符合以下要求：

数据迁移准备应制定迁移方案，并进行迁移方案可行性评估与风险评估，确定制定数据迁移风险控制措施。

9.2.2.6 数据销毁

除满足基本级的要求之外，还应符合以下要求：

a) 应保证用户鉴别信息所在的存储空间被释放或再分配给其他用户前得到完全清除。

b) 应确保文件、目录和数据库记录等资源所在的存储空间被释放或重新分配给其他用户前得到完全清除。

c) 应提供手段禁止被销毁数据的恢复。

9.2.2.7 备份和恢复

除满足基本级的要求之外，还应符合以下要求：

a) 应建设生产备份中心和同城灾备中心，即双活中心。双活中心应具备基本等同的业务处理能力并通过高速链路实时同步数据，日常情况下可同时分担业务及管理系统的运行，并可切换运行，灾难情况下应支持灾备应急切换，保持业务连续运行。

b) 应建立异地灾难备份中心，提供异地实时备份功能，配备灾难恢复所需的通信线路、网络设备和数据处理设备等，利用通信网络将数据实时备份至灾难备份中心。

9.2.3 网络安全防护要求

9.2.3.1 网络区域划分隔离

同基本级要求。

9.2.3.2 访问控制

除满足基本级的要求之外，还应符合以下要求：

应实现对 HTTP、FTP、TELNET、SMTP、POP3 等协议命令级的控制。

9.2.3.3 安全审计

除满足基本级的要求之外，还应符合以下要求：

a) 应能够根据记录数据进行分析，发现异常能及时告警，并生成审计报表。

b) 应能汇聚服务范围内的审计数据，支持第三方审计。

9.2.3.4 恶意代码防范

除满足基本级的要求之外，还应符合以下要求：

应周期性地维护恶意代码库的升级和检测系统的更新。

9.2.3.5 网络设备防护

除满足基本级的要求之外，还应符合以下要求：

a) 当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃取。

b) 应对网络设备进行分权分域管理，限制默认用户或者特权用户的权限，做到最小授权。

9.2.3.6 网络安全监测要求

除满足基本级的要求之外，还应符合以下要求：

a) 应周期性地对攻击、威胁的特征库进行更新，并升级到最新版本。

b) 应支持对违法和不良信息或非法域名的检测发现并告警。

c) 应支持对攻击行为进行分析，明确攻击目标范围，并协助回溯到攻击源头。

d) 应在网络边界处部署异常流量和对未知威胁的识别、监控和防护机制，并采取技术措施对网络进行行为分析，实现对网络攻击特别是未知的新型网络攻击的检测和分析。

9.2.4 虚拟化安全防护要求

9.2.4.1 虚拟机安全

除满足基本级的要求之外，还应符合以下要求：

a) 应保证虚拟机迁移过程中数据和内存的安全可靠，保证迁入虚拟机的完整性和迁移前后安全配置环境的一致性。

b) 应确保虚拟机操作系统的完整性，确保虚拟机操作系统不被篡改，且确保虚拟机实现安全启动。

c) 应对虚拟机镜像文件进行完整性校验，确保虚拟机镜像不被篡改。

d) 应提供最新版本的虚拟机镜像和补丁版本。

e) 应支持发现虚拟机操作系统漏洞的能力，支持漏洞修复。

9.2.4.2 虚拟网络安全

除满足基本级的要求之外，还应符合以下要求：

a) 应支持对虚拟网络的逻辑隔离，在虚拟网络边界处实施访问控制策略。

b) 应对虚拟机网络出口带宽进行限制。

c) 可支持用户选择使用第三方安全产品。

9.2.4.3 虚拟化平台安全

同基本级要求。

9.3 平台 PaaS 层安全防护要求

9.3.1 数据分析服务安全防护要求

同基本级要求。

9.3.2 微服务组件安全防护要求

同基本级要求。

9.3.3 平台应用开发环境安全防护要求

9.3.3.1 身份鉴别

除满足基本级的要求之外，还应符合以下要求：

需要登录访问的开发环境，应对用户访问和操作的有关环节（如注册、登录、操作、管理、浏览等）提供有效的保护措施（如对用户注册口令进行强度检查、用户检测和账号保护、以图形验证码保护各类提交信息、对用户重要操作进行确认和验证、授权访问页面使用安全连接等）。

9.3.3.2 访问控制

同基本级要求。

9.3.3.3 安全审计

同基本级要求。

9.3.3.4 资源控制

除满足基本级的要求之外，还应符合以下要求：

a) 根据需要对用户与开发环境之间相关通信过程中的全部报文或整个会话过程提供必要的保护（如进行通信数据加密），并提供对相关访问、通信等数据的防抵赖功能。

b) 定义服务水平阈值，能够对服务水平进行监测，并具备当服务水平降低到预先规定的阈值时进行告警的功能。

9.3.3.5 信息保护

除满足基本级的要求之外，还应符合以下要求：

a) 与开发环境中的重要功能相关的数据应进行异址备份。

b) 开发环境应提供数据自动保护功能，当发生故障后应保证开发环境能够恢复到故障前的业务状态。

9.3.3.6 恶意代码防范

应提供有效的恶意代码检测和过滤技术手段，对开发环境向用户提供的各类信息（如用户发布和上传的文件、资源站点可供下载的立件、即时通信用户间传送的文件、电子邮件附件）进行必要的安全检查和过滤。

9.3.3.7 上线前检测

除满足基本级的要求之外，还应符合以下要求：

a) 业务应用与工业应用程序在上线前或升级后应进行代码审计，形成报告，并对审计出的问题进行代码升级完善。

b) 业务应用与工业应用程序应避免使用含有已公开漏洞的开源第三方应用组件及代码（漏洞库可参考 CVE、CNVD 等）。

9.4 平台 SaaS 层安全防护要求

9.4.1 业务应用安全防护要求

9.4.1.1 身份鉴别

除满足基本级的要求之外，还应符合以下要求：

a) 应采用两种或两种以上组合的鉴别技术来进行身份鉴别，并保证一种身份鉴别机制是不易伪造的。

b) 应具备防范暴力破解等攻击的能力。

9.4.1.2 访问控制

同基本级要求。

9.4.1.3 安全审计

除满足基本级的要求之外，还应符合以下要求：

a) 应具备对审计记录数据进行统计、查询、分析及生成审计报表的功能。

b) 应具备自动化审计功能，监控明显异常操作并响应。

c) 应能汇聚服务范围内的审计数据，支持第三方审计。

9.4.1.4 资源控制

同基本级要求。

9.4.2 工业应用程序安全防护要求

9.4.2.1 逻辑安全

除满足基本级的要求之外，还应符合以下要求：

9.4.2.1.1 身份鉴别

a) 登录验证模块应能防止身份鉴别暴力攻击（如登录模块应采用随机验证码进行验证，并且保证验证码不易被自动预测、识别）。

b) 加强密码复杂度要求，应不含有常用字符组合、数字组合、键盘顺序等可预测密码组合。

c) 应采用两种或两种以上组合的鉴别技术实现用户身份鉴别。

9.4.2.1.2 访问控制

工业应用程序管理后台不应暴露在公网，管理接口通信内容不应使用明文协议。

9.4.2.1.3 其他

a) 应定义服务水平阈值，能够对服务水平进行检测，并具备当服务水平降低到预先规定的阈值时进行告警的功能。

b) 应保证工业应用程序中使用的第三方软件、运维软件无已知后门、漏洞。

c) 应提供有效的病毒和攻击检测过滤技术手段，能够对用户之间传送的文件进行必要的安全检查和过滤。

9.4.2.2 原生应用及后台系统安全

同基本级要求。

9.4.2.3 Web 应用及后台系统安全

同基本级要求。

参考文献

GB/T 31167-2014	信息安全技术 云计算服务安全指南
YD/T 3157-2016	公有云服务安全防护要求
YD/T 2587-2013	移动互联网应用商店安全防护要求
YD/T 2694-2014	移动互联网联网应用安全防护要求
GB/T 25070-XXXX	信息安全技术 网络安全等级保护安全设计技术要求
YD/T XXXX-XXXX	电信运营商的大数据应用业务安全技术要求