国 际 电 信 联 盟

ITU-T X.1605

国际电信联盟
电信标准化部门

(03/2020)

X系列：数据网、开放系统通信和安全性

云计算安全 – 云计算安全设计

云计算中公共基础设施即服务（IaaS）的安全要求

ITU-T X.1605建议书

国际电信联盟

ITU-T X系列建议书

数据网、开放系统通信和安全性

公用数据网	X.1–X.199
开放系统互连	X.200–X.299
网间互通	X.300–X.399
报文处理系统	X.400–X.499
号码簿	X.500–X.599
OSI组网和系统概貌	X.600–X.699
OSI管理	X.700–X.799
安全	X.800–X.849
OSI应用	X.850–X.899
开放分布式处理	X.900–X.999
信息和网络安全	
一般安全问题	X.1000–X.1029
网络安全	X.1030–X.1049
安全管理	X.1050–X.1069
生物测定	X.1080–X.1099
安全应用和服务(1)	
组播安全	X.1100–X.1109
家庭网络安全	X.1110–X.1119
移动安全	X.1120–X.1139
网页安全	X.1140–X.1149
安全协议(1)	X.1150–X.1159
对等网络安全	X.1160–X.1169
网络身份安全	X.1170–X.1179
PITV安全	X.1180–X.1199
网络空间安全	
计算网络安全	X.1200–X.1229
反垃圾信息	X.1230–X.1249
身份管理	X.1250–X.1279
安全应用和服务(2)	
应急通信	X.1300–X.1309
泛在传感器网络安全	X.1310–X.1319
智能电网安全	X.1330–X.1339
验证邮件	X.1340–X.1349
物联网（IoT）安全	X.1360–X.1369
智能交通系统（ITS）安全	X.1370–X.1389
分布式账簿技术安全	X.1400–X.1429
安全协议(2)	X.1450–X.1459
网络安全信息交换	
网络安全综述	X.1500–X.1519
脆弱性/状态信息交换	X.1520–X.1539
事件/事故/探索法信息交换	X.1540–X.1549
政策的交换	X.1550–X.1559
探索法和信息要求	X.1560–X.1569
标示和发现	X.1570–X.1579
确保交换	X.1580–X.1589
云计算安全	
云计算安全综述	X.1600–X.1601
云计算安全设计	**X.1602–X.1639**
云计算安全最佳实践和指导原则	X.1640–X.1659
云计算安全实现	X.1660–X.1679
其他云计算安全	X.1680–X.1699
量子通信	X.1700–X.1729

欲了解更详细信息，请查阅ITU-T建议书目录。

ITU-T X.1605建议书

云计算中公共基础设施即服务（IaaS）的安全要求

摘要

基础设施即服务（IaaS）平台和虚拟化服务，面临着与传统信息技术基础设施和应用程序不同、甚至可能更多的挑战和威胁。共享计算、存储和网络服务的IaaS平台需要应对IaaS环境中的威胁的保护。ITU-T X.1605建议书旨在记录公共IaaS的安全要求，以帮助IaaS提供商在整个规划、建设和运营阶段提高IaaS平台的安全性。

历史沿革

版本	建议书	批准日期	研究组	唯一标识（ID）*
1.0	ITU-T X.1605	2020-03-26	17	11.1002/1000/14094

关键字

云计算、IaaS、安全要求、虚拟资源

* 为获取本建议书，请在网页浏览器内键入URLhttp://handle.itu.int/，然后输入唯一ID。例如，http://handle.itu.int/11.1002/1000/11830-en。

前言

国际电信联盟（ITU）是从事电信和信息通信技术（ICT）领域工作的联合国专门机构。国际电信联盟电信标准化部门（ITU-T）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第1号决议规定了批准建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简要而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“须”或“必须”等其它一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其它机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联尚未收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此特大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：http://www.itu.int/ITU-T/ipr/。

目录

ITU-T X.1605建议书

云计算中公共基础设施即服务（IaaS）的安全要求

1 范围

本建议分析了IaaS环境中基础设施即服务（IaaS）提供商面临的安全挑战，并规定了云计算中公共IaaS的安全要求。本建议适用于公共IaaS提供商。

这是对IaaS实施时安全要求的高级描述。详细的实施导则不属于本建议书的范围。

2 参考文献

下列ITU-T建议书及含有本建议书引用条款的其他参考文献构成本建议书的条款。所注明版本在出版时有效。所有建议书及其他参考文献均可能进行修订，因此，鼓励建议书的使用方考虑是否有可能使用下列最新版本的建议书和其他参考文献。定期公布ITUT-T建议书的现行有效版本清单。

本建议书引用的文件自成一体时不具备建议书的地位。

[ITU-T X.1642] ITU-T X.1642建议书（2016年），云计算的操作安全导则

[ITU-T Y.3502] ITU-T Y.3502建议书（2014年），| ISO/IEC 17789:2014，信息技术 – 云计算 – 参考架构

[ITU-T Y.3513] ITU-T Y.3513建议书（2014年），云计算 – 基础设施即服务的功能要求

[ISO/IEC 27002] ISO/IEC 27002:2013, *Information technology – Security techniques – Code of practice for information security controls*

[ISO/IEC 27031] ISO/IEC 27031:2011, *Information technology –Security techniques– Guidelines for information and communication technology readiness for business continuity*

3 定义

3.1 他处定义的术语

本建议书使用了以下他处定义的术语：

3.1.1 云计算（cloud computing）[b-ITU-TY.3500]：有助于网络以按需自助方式调配和管理获取一系列可伸缩和富有弹性的、可共享的物理或虚拟资源的范式。

3.1.2 云服务（cloud service）[b-ITU-TY.3500]：使用定义的接口调用通过云计算提供的一项或多项功能。

3.1.3 云服务客户（cloud service customer）（CSC）[b-ITU-T Y.3500]：使用云服务的具有业务关系的参与方。

3.1.4 云服务伙伴（cloud service partner）[b-ITU-T Y.3500]：全力以赴支持或辅助云服务提供商或云服务客户或两者的参与方。

3.1.5 云服务提供商（cloud service provider）（CSP）[b-ITU-T Y.3500]：提供云服务的参与方。

3.1.6 基础设施即服务（infrastructure as a service）（IaaS）[b-ITU-T Y.3500]：一种云服务类别，向云服务客户提供的云能力类型是一种基础设施能力类型。

3.1.7 安全挑战（security challenge）[b-ITU-T X.1601]：源自自然或云服务操作环境的安全“困难”（包括“间接”威胁），而非直接安全威胁。

3.1.8 漏洞（vulnerability）[b-NIST-SP-800-30]：可由威胁来源加以利用的信息系统、系统安全程序、内部控制或实施中存在的弱点。

3.2 本建议书定义的术语

无。

4 缩写词和首字母缩略语

本建议书使用以下缩写词和首字母缩略语：

ACL 访问控制列表

API 应用程序接口

BIA 业务影响分析

CPU 中央处理单元

CSC 云服务客户

CSP 云服务提供商

DDoS 分布式拒绝服务

DRO 灾难恢复对象

DSP 数字服务提供商

IAM 身份和接入管理

IaaS 基础设施即服务

ICT 信息通信技术

IdM 身份管理

I/O 输入/输出

NIC 网络接口卡

OS 操作系统

OTT 过顶服务

PaaS 平台即服务

RPO 恢复点目标

RTO 恢复时间目标

SaaS 软件即服务

SLA 服务水平协议

SQL 结构化查询语言

VDC 虚拟数据中心

VLAN 虚拟局域网

VM 虚拟机

VXLAN 虚拟可扩展局域网

XSS 跨站脚本

5 惯例

关键词“须”（is required to）指必须严格遵守的要求，如果宣称符合本建议书，就不得违反。

关键词“建议”（is recommended）表示是一项建议的并非需绝对遵守的要求，因此宣称符合本文件时不一定按照该要求行事。

关键用语“可选”（can optionally）表示该允许条件属可选项，不带任何建议意味。并非要求供应商的实施方案必须为网络运营商或服务提供商留有该项可以使能的选项或功能，而是指供应商可作为选项提供该功能，并仍宣称符合本规范。

在本建议书及其附件中，有时会出现“须”（shall）、“不得”（shall not）、“应”（should）、“可”（may）等词语。在这些情况下，这些词语应分别理解为“须”“禁止”“建议”和“可选”。这些短语或关键字出现在附录或明确标记为资料性的材料中时，应解释为没有规范性意图。

6 概述

基础设施即服务（IaaS）是云服务的一个类别，其提供给云服务客户（CSC）的云功能类型是基础设施功能类型[b-ITU-T Y.3500]。IaaS允许CSC使用云基础设施资源（计算、存储或网络），这些资源可以通过付出最少的管理工作快速配置和发布。公共IaaS服务使CSC能够快速而容易地启动业务，而不需要建立新的信息通信技术（ICT）基础设施，而CSC可以利用这些资源灵活、弹性地按需开发、托管和运行服务和应用程序。

根据[ITU-T Y.3502]中定义的与ISO/IEC一起开发的分层框架和[ITU-T Y.3513]中定义的IaaS高级概念，IaaS安全要求的高级概念如图6-1所示。

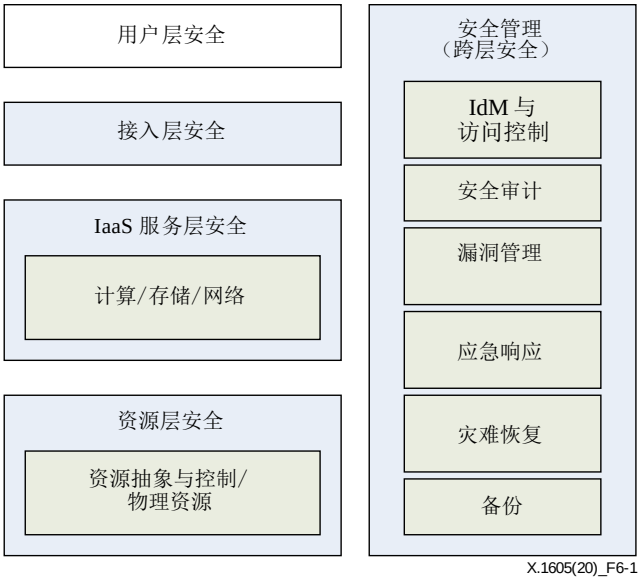

图6-1 IaaS安全要求的高级概念

用户层是CSC与云服务提供商（CSP）交互的用户界面。用户层的功能组件包括用户功能、业务功能和管理员功能，它们与CSP提供的云服务交互，执行CSC相关的管理活动，监控云服务。根据CSP和CSC之间的职责，CSC应该负责用户层的安全机制，因为他们通常使用自己的工具或系统来接入IaaS服务。否则，用户层的工具或系统由CSP提供，CSP应提供满足行业安全最佳实践的工具或系统。用户层的安全要求超出了建议的范围。

接入层为手动和自动接入服务层中可用的功能提供了一个通用界面。接入层的功能组件包括访问控制和连接管理。接入层负责在一个或多个接入机制（如web和应用程序接口（API））上显示IaaS服务功能。第8条定义了接入层的安全要求。

服务层包含CSP提供的IaaS服务的实现。它包含并控制实现IaaS服务的软件组件，并安排通过接入层向CSC提供服务。第9条定义了服务层的安全要求。

资源层组件包括资源抽象与控制，以及[ITU-T Y.3502]中定义的物理资源。虚拟化的资源是通过软件抽象来生成和控制的。第10条定义了资源层的安全要求。

安全管理提供基本的跨层安全管理功能，这些功能在用户层、接入层、服务层和资源层中实现。第11条定义了身份管理和访问控制、安全审计、漏洞管理、应急响应、灾难恢复和备份的安全管理要求。

7 IaaS环境的安全挑战

由于IaaS的巨大优势，IaaS已经成为CSP最重要的服务之一，特别是对传统电信运营商、过顶服务（OTT）和数字服务提供商（DSP）而言，并得到了迅速的发展。随着IaaS的快速发展，安全问题仍然是不容忽视的重大问题。与传统的信息技术基础设施和应用相比，IaaS平台和服务面临着更多的挑战和威胁，特别是由于虚拟化技术的广泛实施、多租户共享资源等原因。

由于公共IaaS可能有来自许多不同组织的共存CSC，所以当CSC评估公共IaaS服务的选择时，安全和隐私保护是最重要的因素。

总之，公共IaaS面临的安全挑战可能来自以下几个方面：

1) 虚拟化：虚拟化技术是云计算的一个重要技术特性，它可以使不同的虚拟机（VM）在同一个虚拟机监控程序上运行，同时也使虚拟机所含文件容易受到非法修改。此外，一旦虚拟机监控程序的漏洞被利用，在其上运行的所有虚拟机都将面临相同的安全风险，造成这些风险的原因如下：
   - 物理主机配置和网络隔离不当。攻击者可以直接利用虚拟机监控程序的漏洞。
   - 虚拟机和虚拟机监控程序之间接口的漏洞。攻击者可利用这些漏洞控制虚拟机监控程序（称为VM escape）。
2) 开放API：作为自动管理虚拟机的前提，开放API可以通过滥用或利用缺乏认证、授权或完整性检查等漏洞来扩大攻击面，从而破坏许多应用。
3) 网络和互联网连接：分布式拒绝服务（DDoS）攻击、中间人攻击、IP欺骗攻击等网络威胁不仅可以从传统网络发起，也可能从同一主机上的虚拟机中产生，在虚拟化网络的模糊边界环境中，防御难度更大。
4) 高度的资源共享：该技术特性可能提供一个更具体的目标，如果物理主机或物理网络被破坏，其所有虚拟机都会受到影响。失效存储设备或替换存储设备的处理涉及所有CSC数据的保密性。这也会给不同CSC之间的隔离带来更大的困难。如果不同虚拟机之间的隔离配置不正确，则不同虚拟机之间发生数据泄漏甚至网络攻击的可能性可能会显著增加。任何发生的事故都会造成重大的安全风险和后果。
5) 虚拟资源的可扩展性：虚拟资源的弹性扩展和虚拟网络安全边界的动态调整，带来了东西网流量的快速增长和新的复杂安全需求。它要求安全设施具有灵活性，能够协同工作，但大多数安全设备和系统都是独立运行的，缺乏有效的协同机制。
6) 配置管理：云计算环境包含多种类型、海量资产、不同服务类型，对配置提出了很高的要求，包括访问控制、隔离、数据备份等，配置不当可能会暴露新的攻击面，甚至直接泄露敏感信息。
7) 日志问题：操作系统、应用和安全设备的各种日志数据可以帮助操作人员提前避免灾难，甚至发现安全事件的根本原因。在云计算环境下，日志的获取、保护和时间同步变得更加复杂。例如，忽略日志保护会带来篡改的风险，而缺乏时间同步则会使异构日志难以关联。

8 IaaS接入层的安全要求

IaaS的接入层负责为CSC提供IaaS服务能力，以便通过一个或多个接入机制进行接入和管理。接入机制包括但不限于：

– 网络接入。

– API接入。

接入层的另一个职责是实现适当的连接管理机制，以提供关于来自和/或到用户层功能组件的流量和连接的QoS策略、负载平衡和安全传输的实施。

8.1 web接入的安全要求

1) IaaS CSP须对CSC应用身份验证和授权措施，以便通过web接入来接入IaaS服务，例如通过CSC的认证信息验证请求并验证CSC的授权。

2) IaaS CSP须对CSC应用访问控制机制，以使用相关的服务能力。

3) 建议IaaS CSP通过web接入为CSC提供一个安全的通信信道。

4) 建议IaaS CSP为CSC提供web接入保护，如输入和输出的有效性检查、请求完整性检查、针对web入侵行为的防御能力，如结构化查询语言（SQL）注入、跨站脚本（XSS）、远程命令执行等。

5) IaaS CSP须支持web接入行为的无限制日志记录、分析和安全审计功能。

8.2 API接入的安全要求

1) 在调用服务API时，IaaS CSP须支持CSC的身份验证和用户认证信息的验证，例如登录到API以确保仅使用合法的调用方。

2) IaaS CSP须在调用服务API时为CSC提供访问控制机制。

3) 建议IaaS CSP通过API接入为CSC提供一个安全的通信信道。

4) 建议IaaS CSP为CSC提供API接口保护，如请求完整性检查、攻击行为（如重放攻击、代码注入等）防御能力。

5) IaaS CSP须支持API调用行为的日志记录、分析和安全审计功能。

9 IaaS服务层的安全要求

IaaS的服务层包含CSP提供的服务的实现。服务层包含并控制实现IaaS服务（如计算服务、网络服务、存储服务等）的软件组件，并安排通过接入层向CSC提供这些IaaS服务。

9.1 计算服务的安全要求

1) IaaS CSP须为虚拟资源提供隔离机制，包括中央处理单元（CPU）、内部网络、内存和存储等的隔离，只允许在虚拟机等不同虚拟资源单元之间满足安全策略的通信。

2) IaaS CSP须支持物理主机中单个虚拟资源单元的资源上限设置，避免特定虚拟资源单元的过度占用导致性能下降。

3) 建议IaaS CSP支持在托管服务器出现故障时自动迁移虚拟资源单元的服务，这样可以防止虚拟资源中运行的服务中断。

4) IaaS CSP须支持对虚拟资源单元镜像的完整性检查，防止恶意篡改，并保证一个逻辑卷只能由一个虚拟资源单元同时挂载。

5) IaaS CSP须支持安全策略的迁移，这将使它们与虚拟资源单元同时得到同步。

6) IaaS CSP须向CSC管理员提供定制虚拟资源单元间安全策略的能力。

7) IaaS CSP须向CSC提供完全删除其自身数据的能力。一旦CSC删除了一个虚拟资源单元，图像文件、快照和备份也应该同时删除。

9.2 存储服务的安全要求

1) 建议IaaS CSP支持数据冗余机制。CSC的数据应该保证在不同的物理位置至少有两个备份，并且该机制应该对CSC透明。

2) 建议IaaS CSP支持使用同一存储系统的多个虚拟机的并发输入/输出（I/O）控制和安全并行接入。

3) IaaS CSP须保证对存储数据的访问控制，这些数据可以在逻辑和物理存储实体上执行，不应由存储的物理位置的任何更改所忽视。

4) IaaS CSP须保证CSC的数据可以被完全删除，包括：

- 在将存储资源重新分配给新的CSC之前，应执行完整的数据擦除。
- 一旦CSC的文件/对象被删除，物理卷中相应的存储区域应正确覆盖或标记为只写，避免未经授权的恢复。
- 一旦CSC的数据被迁移，CSC的元数据须立即被完全删除。

9.3 网络服务的安全要求

1) 建议IaaS CSP向CSC提供监控其自身虚拟资源的南北、东西网络流量的能力。
2) 建议IaaS CSP为CSC提供实现虚拟资源网络接口带宽控制的能力。
3) IaaS CSP须提供CSC虚拟化网络与IaaS平台和管理网络之间的隔离措施，如禁止CSC接入主机或管理节点。
4) IaaS CSP须实现网络访问控制列表（ACL）机制，实现虚拟化网络内的安全隔离和访问控制。
5) 建议IaaS CSP支持防御网络攻击，如虚拟局域网（VLAN）或虚拟可扩展局域网（VXLAN）跳跃。

10 IaaS资源层的安全要求

根据IaaS资源层的功能组件，IaaS资源层的安全要求包括：

– 资源抽象与控制的安全要求；以及
– 物理资源的安全要求。

10.1 资源抽象与控制的安全要求

资源抽象与控制功能组件使CSP能够提供快速弹性、资源池和按需自助服务等特性。它包括虚拟资源池（如虚拟计算资源、虚拟网络资源等）和虚拟资源管理平台。从虚拟资源提供和管理的角度阐述了资源抽象与控制的安全要求。

10.1.1 虚拟资源池的安全要求

10.1.1.1 虚拟计算资源的安全要求

1) 虚拟计算资源单元（如虚拟机、容器等）须在逻辑上相互隔离。
2) 虚拟计算资源单元在遇到异常事故或故障时，须不受其他单元或主机的影响。
3) 虚拟计算资源单元须不能超出其限额使用。
4) 建议在不同的虚拟计算资源单元之间或主机之间禁止“复制”“粘贴”等命令。
5) 建议IaaS CSP支持通过带内或带外模式对虚拟资源进行实时监控，一旦发现异常就报警。对于每个虚拟资源单元，监控对象应包括运行状态、资源消耗和迁移状态等。

10.1.1.2 虚拟网络资源的安全要求

1) 通过实施VLAN、VXLAN、ACL等措施，CSC的虚拟网络在逻辑上须相互隔离。
2) 须在不同的虚拟资源单元之间提供网络流量的监控能力。
3) 须在虚拟端口上提供比特率控制能力。

4) 建议可以检测和防止源自虚拟资源内部的网络攻击行为（如IP欺骗、蠕虫等）。

5) 须禁止虚拟网络接口卡（NIC）的混杂模式，防止网络流量嗅探。

10.1.1.3 虚拟存储资源的安全要

1) 虚拟存储资源池须在不同的CSC之间隔离。

2) 存储数据的安全措施须在逻辑和物理存储实体上都执行。

3) 须禁止直接接入物理存储资源。

4) 为了支持使用同一存储实体的多个虚拟资源单元，须具备并发I/O控制和安全并行接入的功能。

5) 建议虚拟存储资源支持弹性扩展，不中断正常的存储服务。

10.1.2 虚拟资源管理平台的安全要求

1) 为防止对虚拟资源管理平台的非法接入，须适当实施访问控制措施。

2) 建议只安装必要的组件和应用，关闭无关的服务端口，遵循风险最小化原则。

3) 须能及时检测和报警虚拟资源管理平台上的攻击行为，并记录日志，包括源IP地址、攻击类型、时间戳等。

4) 须提供对虚拟资源的实时监控能力，包括运行状态、资源占用、迁移等。

5) 建议禁用不必要和空闲的虚拟资源。

6) 虚拟资源管理平台上的管理命令需要在安全隧道中传输。

7) 建议在远程执行特权命令时对其进行限制。

8) 须对非法的虚拟资源单元进行适当的隔离和处理，以减小对整个虚拟资源的后续影响。

9) 须提供恶意代码的检测和处理能力。

10) 建议在虚拟资源单元同时迁移之后迁移安全策略。

11) 一旦发现虚拟资源管理组件（如虚拟机监控程序、容器引擎、管理组件等）的安全漏洞，就须及时实施安全补丁或安全增强配置，并及时更新。

12) 为了保持上层服务的连续性，须提供故障管理，即故障主机上的虚拟资源单元可以及时迁移到其他主机上。

13) 需要记录虚拟资源管理平台上的所有操作和事件，以便以后追踪和审计。

10.2 物理资源的安全要求

物理资源是指一些硬件资源，如计算机、网络设备、存储组件和其他物理计算基础设施元素等，CSP需要这些资源来运行和管理提供给CSC的IaaS服务。

10.2.1 物理环境的安全要求

IaaS物理环境的安全要求包含于**[ISO/IEC 27002]**。

10.2.1.1 物理资源的安全要求

物理资源是指一些硬件资源，如物理网络基础设施、存储设备、主机、管理终端和其他物理基础设施元素。

1) 须提供对物理资源（如网络设备、主机、存储设备等）的故障检测和定位能力，以保持底层物理基础设施的可用性和可靠性。
2) 建议及时发现和标记物理资源的变化。
3) 建议在某些物理组件出现故障时提供数据恢复功能。
4) 须提供IaaS平台的DDoS防御能力。
5) 基础设施网络须划分为不同的网络安全域，在逻辑上相互隔离。
6) 须执行网络流量监测和入侵行为的检测机制，在网络边界部署保护设备，包括身份和接入管理（IAM）、IPS、防火墙等。
7) 建议可以检测和防止从IaaS资源发起的传出网络攻击行为。
8) 须提供恶意代码的检测和处理能力，特别是对于管理终端、主机和其他应用服务器。
9) 须执行安全策略基线，只有满足安全策略的终端和服务器才能接入IaaS平台。
10) 须记录物理资源上的所有操作和事件，以便以后追踪和审计。

11 安全管理要求

安全管理负责应用与安全相关的控制，来缓解云计算环境中的安全威胁。安全管理的功能组件包括所有须支持云服务的安全设施。

安全管理的功能组件包括：

- 身份管理和访问控制；
- 安全审计；
- 漏洞管理；
- 应急响应；
- 灾难恢复；及
- 备份。

11.1 IdM和访问控制

IaaS平台应为CSC和IaaS平台管理员提供统一的身份管理（IdM）和访问控制功能。

1) 生命周期中CSC的身份须在每个IaaS服务中是唯一的，并与安全审计相关联。CSC的身份须进行管理、维护和保护，以防止未经授权的接入、修改或删除。
2) IaaS平台须为CSC提供密码策略管理，包括但不限于：
   – 须使用复杂密码策略。
   – 须使用密码重新设置周期机制。
   – 须随机生成CSCs的初始密钥，初始密钥必须在首次登录时修改。
3) 建议IaaS平台支持对CSC身份的异常检测，并将报警通知给相关CSC。

4) IaaS平台须支持CSC的多因素认证，认证技术包括但不限于密码、数字证书、IC卡或生物验证。

5) 须根据CSC和接入资源的组定义，支持细粒度的授权策略。IaaS平台须保护CSC认证信息的保密性和完整性。

6) CSC认证、授权等与IdM相关操作的详细日志需要保存，以备日后审计。

7) 建议IaaS平台支持与CSC的IdM系统对接。

8) IaaS平台管理员的角色和相关权限须授予不同的账户。

9) IaaS平台须对管理员使用多因素身份验证。

10) IaaS平台须使用管理员权限最小化的原则。

11) 在存储和传输过程中，需要对认证数据、授权数据等敏感数据进行加密。

11.2 安全审计

1) IaaS平台须使用各种记录进行安全审计，这些记录包括但不限于：
   - CSC和IaaS平台管理员的日志、身份认证和授权信息。
   - IaaS平台管理员在IaaS基础设施上的操作和维护记录。
   - IaaS平台管理员在CSC资源上的操作日志。
   - CSC对CSC自身资源的操作日志。
   - IaaS平台运行过程中的运行和维护日志。

2) IaaS平台须实现安全机制以保护各种记录不被篡改。

3) 所有网络时钟须在整个IaaS平台内保持同步，以便系统地记录接入和操作。

4) 安全审计记录应当包括安全事件的主体、对象、时间、类型和结果。

5) CSC内部审计记录必须相互隔离。

6) CSC须能够收集和查看与自身资源相关的审计记录。

7) 审计记录必须得到安全保护，如禁止未经授权接入审计记录，防止意外删除、修改、覆盖和丢失。

8) 审计记录的保存期限须满足法律合规性和CSC的具体保存要求。

9) 建议IaaS平台支持CSC使用第三方审计系统或接口来实现CSC职责范围内的审计目标。

11.3 漏洞管理

IaaS平台的漏洞可能存在于流程、管理、配置、硬件、软件等方面。

1) 须记录所有资产和IaaS平台版本的信息，并定期更新。

2) 建立漏洞评估机制，明确漏洞评估的对象、频率和评估策略。

3) 须定期对IaaS平台所有资产进行漏洞评估，生成漏洞评估报告，提出漏洞修复建议。

4) 须管理修补程序和修复过程：

- 须跟踪各个供应商发布的安全威胁和安全补丁，确定哪些补丁应该安装在IaaS平台上。
- 在安装之前须测试安全补丁，以确保补丁与现有系统和应用兼容。

- 须创建IaaS平台所有组件的补丁更新计划，按照计划进行补丁安装，并在安装过程中创建记录。

5) 须制定IaaS平台的安全配置基线，并根据该基线配置IaaS平台的组件。

6) 须定期对IaaS平台所有资产进行安全基线检查，形成基线检查报告，提出整改建议。

7) 须对IaaS平台的配置策略变更进行审计，以验证每个配置项的正确性、一致性、完整性和有效性，确保配置变更不会带来新的安全缺陷。

11.4 应急响应

IaaS的应急响应注意事项应符合[ITU-T X.1642]中的第8.9条。

11.5 灾难恢复

IaaS的灾难恢复注意事项应该符合现有的IT技术的通用规范，例如[ISO/IEC 27031]标准。然而，作为一种快速发展的技术，IaaS的灾难恢复也应该考虑：

1) 为每个CSC定义灾难恢复对象。基于IaaS平台上关键组件和主要安全风险的识别，须启动业务影响分析（BIA）来确定不同业务的灾难恢复对象。灾难恢复对象可以由优先级、RPO/RTO等定义，不同的DRO决定相应的SLA和业务架构，包括跨远程虚拟数据中心（VDC）的高可用性技术、跨区域数据备份等。

2) 系统和数据的定期备份。需要支持跨区域数据存储和容灾能力。此外，应向IaaS平台的租户提供系统级备份和数据级备份的类型以及相应的灾难恢复能力，以帮助CSP和CSC实现故障转移。对于CSC，他们甚至可以定期将数据备份到不同的CSP，以避免单个CSP长时间终止的风险。

3) 定期验证灾难恢复计划。虽然CSC的系统和数据可能保持相对稳定，但CSP启动的基础设施更新也可能带来新的安全风险。因此，应定期进行灾难恢复演练，记录关键信息，包括灾难恢复计划的可用性、完整性和有效性，以及过程中存在的问题和相应的解决方案等。

4) 定期评估风险。为支持CSC的业务连续性，CSP应评估可能影响CSC业务连续性计划的安全风险，包括IaaS服务故障、CSP与CSC之间的网络中断、云服务终止等，并将结果认真勤勉地告知CSC。此外，应提前通知应急响应、灾难恢复计划和支持CSC业务连续性的活动，甚至根据CSC的要求进行调整。

11.6 备份

IaaS的备份注意事项应符合[ITU-T X.1642]中第8.10条。

参考资料

[b-ITU-T X.1601] ITU-T X.1601建议书（2015年），云计算的安全框架

[b-ITU-TY.3500] ITU-T Y.3500建议书（2014年）| ISO/IEC 17788:2014，信息技术 – 云计算 – 概述与词汇

[b-NIST 500-291] NIST SP 500-291,2011, NIST Cloud Computing Standards Roadmap

[b-NIST-SP-800-30] NIST Special Publication 800-30, 2012, Guide for Conducting Risk Assessments

ITU-T 建议书系列

系列 A	ITU-T 工作的组织
系列 D	资费及结算原则和国际电信/ICT 的经济和政策问题
系列 E	综合网络运行、电话业务、业务运行和人为因素
系列 F	非话电信业务
系列 G	传输系统和媒介、数字系统和网络
系列 H	视听及多媒体系统
系列 I	综合业务数字网
系列 J	有线网络和电视、声音节目及其他多媒体信号的传输
系列 K	干扰的防护
系列 L	环境与 ICT、气候变化、电子废物、节能；线缆和外部设备的其他组件的建设、安装和保护
系列 M	电信管理，包括 TMN 和网络维护
系列 N	维护：国际声音节目和电视传输电路
系列 O	测量设备的技术规范
系列 P	电话传输质量、电话设施及本地线路网络
系列 Q	交换和信令，以及相关联的测量和测试
系列 R	电报传输
系列 S	电报业务终端设备
系列 T	远程信息处理业务的终端设备
系列 U	电报交换
系列 V	电话网上的数据通信
系列 X	**数据网、开放系统通信和安全性**
系列 Y	全球信息基础设施、互联网协议问题、下一代网络、物联网和智慧城市
系列 Z	用于电信系统的语言和一般软件问题

瑞士印刷
2020年，日内瓦