国 际 电 信 联 盟

ITU-T X.1604

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

云计算中网络即服务（NaaS）的安全要求

ITU-T X.1604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.1604建议书

云计算中网络即服务（NaaS）的安全要求

摘要

ITU-T X.1604建议书分析了云计算中网络即服务（NaaS）面临的安全威胁和挑战，并根据相应的云能力类型，从NaaS应用、NaaS平台和NaaS连接等方面对NaaS的安全要求进行了详细说明。

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.1604	2020-03-26	17	11.1002/1000/14093

关键字

云、网络即服务、安全要求。

* 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/。

© 国际电联 2020

版权所有。未经国际电联事先书面许可，不得以任何手段复制本出版物的任何部分。

目录

ITU-T X.1604建议书

云计算中网络即服务（NaaS）的安全要求

1 范围

本建议书分析了云计算中网络即服务（NaaS）面临的安全威胁和挑战，并根据相应的云能力类型，从NaaS应用、NaaS平台和NaaS连接等方面对NaaS的安全要求进行了详细说明。

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它参考文献构成本建议书的条款。所注明版本在出版时有效。所有建议书及其它参考文献均可能进行修订；因此鼓励建议书的使用方了解使用最新版本的下列建议书和其它参考文献的可能性。ITU-T建议书的现行有效版本清单定期出版。本建议书在引用某一独立文件时，并未给予该文件建议书的地位。

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

[ITU-T Y.3500] ITU-T X.3500建议书（2014年），*信息技术 – 云计算 – 概述和词汇*

[ITU-T Y.3512] ITU-T X.3512建议书（2014年），*云计算 – 网络即服务的功能要求*

3 定义

3.1 其他地方定义的术语

本建议书使用其他地方定义的下列术语：

3.1.1 访问控制（access control）[b-ITU-T X.800]：防止未经授权使用资源，包括防止以未经授权的方式使用资源。

3.1.2 认证（authentication）[b-ISO/IEC 18014-2]：以实体身份提供保证。

3.1.3 授权（authorization）[b-ITU-T X.1251]：授权服务旨在做出有关用户访问权限的决定，并根据用户的特权执行授权决定。授权是一项可选服务；仅在需要根据用户权限控制对资源的访问时才提供此功能。

3.1.4 保密性（confidentiality）[b-ITU-T X.800]：不向未经授权的个人、实体或过程提供或披露信息的属性。

3.1.5 数据完整性（data integrity）[b-ITU-T X.800]：数据未以未经授权的方式更改或销毁的属性。

3.1.6 防火墙（firewall）[b-ISO/IEC 27033-1]：放置在由专用设备或若干组件和技术组合而成的网络环境之间的一种安全屏障，从一个网络环境到另一个网络环境的所有通信都通过该屏障，反之亦然，只有本地安全策略定义的授权通信才允许通过。

3.1.7 侵入检测系统（intrusion detection system）[b-ISO/IEC 27039]：用于确定侵入事件已经尝试、正在发生或已经发生的信息系统。

3.1.8 密钥（key）[b-ITU-T X.800]：控制加密与解密操作的符号序列。

3.1.9 密钥管理（key management）[b-ITU-T X.800]：根据安全策略生成、存储、分发、删除、存档和应用密钥。

3.1.10 公钥证书（public-key certificate）（PKC）[b-ITU-T X.509]：实体的公钥以及一些其他信息，不能通过带有证书颁发机构（CA）的私钥的数字签名来伪造它。

3.1.11 威胁（threat）[b-ISO/IEC 27000]：可能对系统或组织造成损害的意外事故的潜在原因。

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略词和首字母缩略语：

BoD 按需带宽

CSC 云服务客户

CSP 云服务提供商

DDoS 分布式拒绝服务

DoS 拒绝服务

NaaS 网络即服务

SNMP 简单网络管理协议

vCDN 虚拟内容交付网络

vEPC 虚拟演进分组核心

vFW 虚拟防火墙

VPN 虚拟专用网

5 惯例

在本建议书中：

关键词**“须”（is required to**）指必须严格遵守的要求，如果宣称符合本文件，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。

关键字**“被禁止”（is prohibited from**）表示必须严格遵循的要求，并且如果要宣称符合本建议书，则不允许有任何偏差。

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。

6 概述

根据[ITU-T Y.3500]，云服务类别是提出一组通用数量的一组云服务。网络即服务（NaaS）是云服务类别之一，其提供给云服务客户（CSC）的功能是传输连接和任何相关的网络功能。

如[ITU-T Y.3512]所定义，NaaS服务可以提供以下三种云能力中的任何一种：NaaS应用服务、NaaS平台服务和NaaS连接服务。

- **NaaS应用服务**提供CSC云网络应用，如虚拟路由器、虚拟内容交付网络（vCDN）、虚拟演进分组核心（vEPC）和虚拟防火墙（vFW）。
- **NaaS平台服务**提供了CSC网络平台，该平台为网络功能提供了可编程的环境。
- **NaaS连接服务**提供CSC配置，并使用网络连接资源，如灵活可扩展的虚拟专用网（VPN）、按需带宽（BoD）等。

NaaS的高层概念如图1所示：

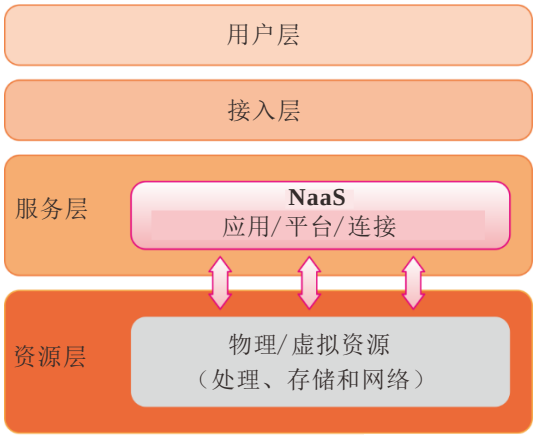

图1 – NaaS的高层概念

通过使用这三种网络服务，NaaS可以提供云计算中的网络功能，包括：通过网络功能协调计算和存储虚拟化，异构网络技术的统一控制以及按需重新配置。

另一方面，NaaS还面临一些安全挑战：

- **NaaS应用面临的安全威胁和挑战：**NaaS应用服务通过CSP向CSC提供虚拟网络应用，如虚拟防火墙（vFW）、虚拟路由器、虚拟交付网络（vCDN）等。NaaS应用服务面临应用安全漏洞方面的安全挑战，网络虚拟化、物理网络设备共享使用等安全风险。
- **NaaS平台面临的安全威胁和挑战：**NaaS平台服务是指CSP为CSC提供软件环境和管理、部署和运行网络应用的平台。NaaS平台面临的安全挑战包括但不限于对网络平台的DoS攻击、操作系统的安全漏洞、访问控制中断等。
- **NaaS连接面临的安全威胁和挑战：**NaaS连接服务是通过CSP向CSC提供网络连接，如虚拟专用网（VPN）、按需带宽（BoD）等。连接服务的安全问题不仅会给NaaS服务带来风险，还会给其他云资源和CSC的数据带来风险。NaaS连接服务面临的安全挑战包括但不限于窃听、中间人攻击等。

本建议书分析了云计算中NaaS的安全要求，包括NaaS应用、NaaS平台和NaaS连接。

7 云计算中网络即服务面临的安全威胁和挑战

[ITU-T X.1601]第7条和第8条分别记录了云计算中CSC和CSP的安全威胁和挑战。与[ITU-T X.1601]中定义的NaaS相比，云计算中的NaaS也面临类似的安全威胁和挑战，如下所示：

a) 系统漏洞；

b) 数据丢失和泄漏；

c) 业务接入不安全；

d) 未经授权的管理接入；

e) 内部威胁；

f) 失去信任；

g) 治理失灵；

h) 失去保密性；

i) 服务不可用；以及

j) 共享环境。

对于每种云功能，云计算中的NaaS都面临着特殊的安全威胁和挑战。

7.1 NaaS应用面临的安全威胁和挑战

a) 网络和系统漏洞：攻击者可能会利用NaaS应用的潜在安全漏洞。NaaS应用虚拟化的技术缺陷可能会导致一些安全风险；此外，不成熟的运维技术可能导致风险更加严重。

b) 物理网络设备的共享使用：由于物理网络设备是共享的，一台共享设备上的数据可能会丢失，泄漏或滥用。

c) 不安全的接入：NaaS应用的不安全接入可能会导致应用数据丢失，泄漏或滥用。

d) 未经授权的管理接入：NaaS应用的未经授权的管理接入可能会导致数据丢失。

e) 应用不可用：NaaS应用可能受到拒绝服务（DoS）或分布式拒绝服务（DDoS）攻击的攻击；此外，该攻击还可能导致硬件设备损坏并导致数据丢失或破坏。

7.2 NaaS平台面临的安全威胁和挑战

a) 网络平台上的DoS攻击：当一个或多个平台受到拒绝服务（DoS）攻击时，该平台和其他虚拟化平台由于CPU和内存转换消耗而无法响应。

b) 操作系统的安全漏洞：NaaS平台上的数据可能会丢失；此外，操作系统的安全漏洞可能会导致病毒传播和其他严重的安全风险。

c) 访问控制中断：访问控制中断可能会导致数据丢失、泄漏或滥用。

d) 网络平台不可用：NaaS平台不可用可能导致NaaS服务不可用，因此，相关的NaaS应用和NaaS连接可能无法正常工作。

e) 未经授权的管理接入：对NaaS平台的未经授权的管理接入可能会导致数据丢失、泄漏或滥用。例如，攻击者可能利用系统漏洞来获得对NaaS平台的未经授权的管理接入，并将数据收集目标IP地址修改为攻击者的IP地址。

f) 内部人员威胁：如果NaaS服务的客户是公司或组织，而不是个人，该组织员工将共享“管理者”密码，NaaS服务提供商也是如此。粗心或培训不足的用户（或消费者环境中的家庭成员），或心怀不满的员工的恶意行为始终会构成严重威胁。

7.3 NaaS连接面临的安全威胁和挑战

a) 窃听：攻击者可能会对连接数据和传输数据进行窃听。

b) 网络连接攻击：网络连接过程中可能会发生网络攻击，例如中间人攻击、DoS攻击等。

c) 数据丢失和泄漏：使用NaaS服务时，NaaS客户通常使用NaaS提供商提供的网络来传输数据。这些数据可能涉及个人隐私、商业秘密和政治问题。因此，数据泄漏是对NaaS用户的严重威胁。

d) 欺骗：攻击者可能伪装成云计算NaaS的管理系统或数据存储服务器，这可能会导致连接或传输数据丢失。

e) 篡改和拦截：网络设备损坏、黑客入侵和NaaS服务提供商的破产很可能导致无法恢复丢失的数据。此外，如果黑客成功进入网络，也可以篡改数据。

f) 不安全的网络接入：不安全的网络接入可能导致连接或传输数据丢失、泄漏或滥用。

g) 不安全的身份认证：不安全的身份认证可能导致连接或传输数据丢失、泄漏或滥用。

h) 网络不可用：NaaS连接网络可能受到DoS或DDoS攻击的攻击；此外，DoS或DDoS攻击可能导致云计算中的NaaS服务器崩溃。

i) 获取接口漏洞：攻击者可能使用监测数据获取来利用接口漏洞。

j) 未经授权的管理接入：对NaaS连接系统的未经授权的管理接入可能会导致传输数据丢失。

8 NaaS应用的安全要求

本条确定了云计算NaaS的安全要求。.

8.1 NaaS应用的安全要求

NaaS应用的安全要求包括：

a) 须保持NaaS应用数据的完整性和准确性。

b) 建议提供对NaaS应用数据（如白名单、黑名单等）的访问控制方法。

c) 建议CSP向CSC提供适当的访问控制方法，如白/黑名单、账户和密码等，以防止未经授权的用户访问未经授权的系统或数据。[ITU-T X.1601]提供了云计算常用的访问控制解决方案。

d) CSP须支持NaaS应用使用情况的日志记录和审计。

e) CSP须支持对NaaS应用系统漏洞的防御；例如，CSP可以使用渗透测试方法来防止NaaS应用系统的漏洞。

f) CSP须提供防止NaaS应用数据丢失的备份方法，如使用物理磁盘备份、分布式数据存储方法等，常用备份方法在[ITU-T X.1601]。

表8-1提供了NaaS应用安全威胁到安全要求的摘要映射。

表8-1 – NaaS应用：安全威胁映射到安全要求

安全威胁	安全要求
应用安全漏洞	b), d), e), f)
网络虚拟化的安全风险	a), b), c), d), f)
物理网络设备的共享使用	a), b), c), d), f)
不安全接入	b), c), d), e), f)
未经授权的管理接入	b), c), d), f)
应用不可用	d), e), f)

8.2 NaaS平台的安全要求

NaaS平台的安全要求包括以下内容：

a) 须保持NaaS平台数据的完整性和准确性。

b) 建议提供对NaaS平台数据（例如白名单、黑名单等）的访问控制方法。

c) 建议CSP向CSC提供适当的访问控制方法，如白/黑名单、账户和密码等，以防止未经授权的用户访问未经授权的系统或数据。[ITU-T X.1601]提供了云计算常用的访问控制解决方案。

d) CSP须支持NaaS平台使用情况的日志记录和审计。

e) CSP须对NaaS平台系统的漏洞进行防御；例如，CSP应防止NaaS平台上的数据丢失和泄漏。

f) CSP须提供防止NaaS平台数据丢失的备份方法，如使用物理磁盘备份、分布式数据存储方法等，常用备份方法在[ITU-T X.1601]中。

表8-2提供了NaaS平台安全威胁到安全要求的摘要映射。

表8-2 – NaaS平台：安全威胁映射到安全要求

安全威胁	安全要求
网络平台上的DoS攻击	a), b), c), d), e), f)
操作系统安全漏洞	a), b), d), e), f)
访问控制中断	a), b), c), d), e), f)
网络平台不可用	a), d), e), f)
未经授权的管理接入	b), c), d), f)
内部员工威胁	b), d), f)

8.3 NaaS连接的安全要求

NaaS连接的安全要求包括以下内容：

a) 须保持NaaS连接数据的完整性和准确性。

b) 建议对NaaS连接的接口提供访问控制方法，如白名单、黑名单等。

c) 建议提供加密方法，以确保连接和传输数据的安全。

d) 建议在云资源和NaaS连接服务器之间使用标准网络协议，如简单网络协议（SNMP）或其他标准网络协议。

e) 建议CSP向CSC提供适当的访问控制方法，如白/黑名单、账户和密码等，以防止未经授权的用户访问未经授权的系统或数据。[ITU-T X.1601]提供了云计算常用的访问控制解决方案。

f) CSP须支持NaaS连接使用情况的日志记录和审计。

g) CSP须实施身份认证方法以保护对NaaS连接数据的接入，例如双重认证或其他方法。[ITU-T X.1601]中提供了用于云计算的常用身份认证方法。

h) CSP须支持对NaaS连接系统漏洞的防御；例如，CSP可以使用渗透测试方法来防止NaaS连接系统的漏洞。

表8-3提供了NaaS平台安全威胁到安全要求的摘要映射。

表8-3 – NaaS连接：安全威胁映射到安全要求

安全威胁	安全要求
窃听	b), c), d), e), f), g) h)
网络连接攻击	d), f), h)
数据丢失和泄漏	a), b), c), d), e), f), g) h)
欺骗	a), b), d), e), f), g) h)
篡改和拦截	a), b), c), d), e), f), g) h)
不安全的网络接入	b), c), d), e), f), g) h)
不安全的身份认证	b), c) , e), f), g) h)
网络不可用	d), f), h)
获取接口漏洞	a), b), c), d), f), h)
未经授权的管理接入	c), f), g)

参考资料

[b-ITU-T E.409] ITU-T E.409建议书（2004年），事件组织和安全事件处理：电信组织指南。

[b-ITU-T X.509] ITU-T X.509建议书（2019年）|ISO / IEC 9594-8：2020，信息技术 – 开放系统互联 – 目录：公钥和属性证书框架。

[b-ITU-T X.800] ITU-T X.800建议书（1991年）| ISO/IEC 7498-2:1989，CCITT应用的开放系统互联的安全架构。

[b-ITU-T X.810] ITU-T X.810建议书 | ISO / ISO/IEC 10181-1 :1995，信息技术 – 开放系统互联 – 开放系统的安全框架：概述。

[b-ITU-T X.1251] ITU-T X.1251建议书 (2019)，结构化威胁信息表达式的用例

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

[b-ISO/IEC 18014-2] ISO/IEC 18014-2:2009, *Information technology – Security techniques – Time-stamping services – Part 2: Mechanisms producing independent tokens*.

[b-ISO/IEC 19440] ISO/IEC 19440: 2007, *Enterprise integration – Constructs for enterprise modelling*.

[b-ISO/IEC 19944] ISO/IEC 19944:2017, *Information technology – Cloud services and devices: data flow, data categories and data use*.

[b-ISO/IEC 20000-1] ISO/IEC 20000-1:2011, *Information technology –Service management – Part1: Service management system requirements.*

[b-ISO/IEC 27000] ISO/IEC 27000:2018, *Information technology –Security techniques – Information security management systems – Overview and vocabulary*.

[b-ISO/IEC 27033-1] ISO/IEC 27033-1:2015, *Information technology – Security techniques – Network security – Part 1: Overview and concepts*.

[b-ISO/IEC 27039] ISO/IEC 27039:2015, *Information technology – Security techniques – Selection, deployment and operations of intrusion detection and prevention systems (IDPS)*.

[b-ISO/IEC 27729] ISO/IEC 27729：2012, *Information and documentation – International standard name identifier (ISNI).*

[b-ISO/IEC 29100] ISO/IEC 29100：2011, *Information technology –Security techniques – Privacy framework.*

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