国 际 电 信 联 盟

ITU-T X.1641

（09/2016）

国际电信联盟
电信标准化部门

X系列：数据网、开放系统通信和安全性

云计算安全 – 云计算安全最佳做法和导则

云服务客户数据安全导则

ITU-T X.1641 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
生物测定安全	X.1080–X.1099
安全应用和服务	
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	X.1150–X.1159
对等网络安全	X.1160–X.1169
网络身份安全	X.1170–X.1179
IPTV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	
应急通信	X.1300–X.1309
泛在传感器网络安全	X.1310–X.1339
PKI相关建议书	X.1340–X.1349
网络安全信息交换	
网络安全概述	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
探索法和信息请求	X.1560–X.1569
标识和发现	X.1570–X.1579
确保交换	X.1580–X.1589
云计算安全	
云计算安全概述	X.1600–X.1601
云计算安全设计	X.1602–X.1639
云计算安全最佳做法和导则	**X.1640–X.1659**
云计算安全的落实工作	X.1660–X.1679
其他云计算安全问题	X.1680–X.1699

欲了解更详细信息，请查阅ITU-T建议书目录。

ITU-T X.1641 建议书

云服务客户数据安全导则

摘要

ITU-T X.1641建议书为云计算中的云服务客户（CSC）数据提供了通用的安全导则。本建议书分析了CSC数据安全性的生命周期，并就数据生命周期的各阶段提出了安全要求。此外，ITU-T X.1641建议书就最佳安全做法应提倡在何时使用各种控制提供了指导原则。

历史沿革

版本	建议书	批准日期	研究组	唯一识别码*
1.0	ITU-T X.1641	2016-09-07	17	11.1002/1000/12853

关键词

云服务客户数据、数据安全性控制，数据安全性生命周期。

* 欲查阅建议书，请在您的网络浏览器地址域键入URL http://handle.itu.int/，随后输入建议书的唯一识别码，例如， http://handle.itu.int/11.1002/1000/11830-en。

前言

国际电信联盟（ITU）是从事电信领域工作的联合国专门机构。ITU-T（国际电信联盟电信标准化部门）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

本建议书为简明扼要起见而使用的“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。“应该”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

页码

1 范围 1

2 参考文件 1

3 定义 1

3.1 他处定义的术语 1

3.2 本建议书定义的术语 2

4 缩写词和首字母缩略语 3

5 排印惯例 3

6 概述 3

6.1 此建议书内数据的规范 3

6.2 云服务客户的数据安全性威胁 3

6.3 数据安全性的现有要求 4

6.4 数据安全的生命周期 5

7 与数据安全相关的安全控制导则 5

7.1 创建阶段的安全控制 5

7.2 传输阶段的安全控制 5

7.3 存储阶段的安全控制 5

7.4 使用阶段的安全控制 6

7.5 迁移阶段的安全控制 6

7.6 破坏阶段的安全控制 6

7.7 备份与恢复阶段的安全控制 7

附录一 安全控制使用导则 8

参考资料 9

ITU-T X.1641 建议书

云服务客户数据安全导则

1 范围

本建议书为云计算中的云服务客户（CSC）数据安全性提供了指导原则，其所涉案例中的云服务提供商 (CSP)均负责确保数据处理具备适当的安全性。但这并非一成不变，因为有些云服务的数据安全性就由云服务客户自己负责。在其它情况下，可能会采用职责共担的方式。

例如，在某些情况下CSP可能负责限制数据的接入，而CSC仍负责决定哪些云服务用户(CSU)有权接入，以及CSU用于处理数据的所有脚本和应用的行为。

本建议书确定了可在完整数据生命周期不同阶段使用的云服务客户数据安全控制功能。这些安全控制功能可随着安全级的变化而不同。因此，本建议书就最佳安全做法应提倡在何时使用各种控制提供了指导原则。

2 参考文件

参考文献下列ITU-T建议书和其他参考文献的条款，通过在本建议书中的引用而构成本建议书的条款。在出版时，所指出的版本是有效的。所有的建议书和其他参考文献都面临修订，使用本建议书的各方应探讨使用下列建议书和其他参考文献最新版本的可能性。当前有效的ITU-T建议书清单定期出版。

本建议书中引用某个独立文件，并非确定该文件具备建议书的地位。

[ITU-T X.1601] Recommendation ITU-T X.1601 (2015)， *Security framework for cloud computing.*

[ITU-T X.1631] Recommendation ITU-T X.1631 (2015) | ISO/IEC 27017： 2015，*Information technology - Security techniques - Code of practice for* information *security controls based on ISO/IEC 27002 for cloud service.*

3 定义

3.1 他处定义的术语

本建议书使用了下列他处定义的术语：

3.1.1 认证[b-NIST-SP-800-53]：核实用户、程序或装置的身份，这常常是允许获取信息系统资源的前提条件。

3.1.2 云计算[b-ITU-T Y.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，可提供自我配置和按需管理。

注 – 资源的例子包括服务器、操作系统、网络、软件、应用和存储设备。

3.1.3 云服务[b-ITU-T Y.3500]：实现的一种或多种能力，通过使用声明接口（declared interface）启动。

3.1.4 云服务客户[b-ITU-T Y.3500]：使用**云服务**的具有业务关系的一方。

注 – 业务关系不必隐含财务协议。

3.1.5 云服务客户数据 [b-ITU-T Y.3500]**：**云服务客户因法律或其它原因对其实施控制并将其输入云服务的数据对象类别，此类数据亦可能是因云服务客户本身或其代理通过云服务的公布界面提供云服务而产生的。

注1 – 版权的法律控制便是一例。

注2 – 云服务包含或操作使用的数据可能并非云服务客户数据；这些数据可能由云服务提供商提供，或取自其它来源，抑或是公开提供的数据。但根据版权的一般原则，云服务客户对此数据应用云服务功能所产生的输出数据有可能是云服务客户数据，除非云服务协议中的特别条款做出了相反的规定。

3.1.6 云服务衍生数据[b-ITU-T Y.3500]：云服务提供商控制下的数据对象种类，是云服务客户同云服务互动的结果。

3.1.7 云服务提供商[b-ITU-T Y.3500]：提供云服务的一方。

3.1.8 云服务用户[b-ITU-T Y.3500]：与使用云服务的云服务客户相关联的自然人或其代表实体。

注 – 这类实体的例子包括设备和应用。

3.1.9 基础设施即服务（IaaS） [b-ITU-T Y.3500]：一种类别云服务，其中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。

3.1.10 多租户[b-ITU-T Y.3500]：物理或虚拟资源的分配方法能够使多租户及其计算和数据相互隔离并无法实现互访。

3.1.11 平台即服务（PaaS）[b-ITU-T Y.3500]：一种类别云服务，其中向服务客户提供的能力类型是平台能力类型。

3.1.12 一方[b-ISO/IEC27729]：自然人或法人，不论是否成立公司，或上述两类之一的群体。

3.1.13 个人可识别信息[b-ISO/IEC 29100]：(a) 可被用于识别相关信息与之关联的PII（个人可识别信息）主体，或(b) 能被或可能被直接或间接与PII主体联系起来的任何信息。

3.1.14 PII主体 [b-ISO/IEC 29100]：与个人可识别信息（PII）相关的自然人。

注 – 根据管辖权和专项数据保护和隐私立法的不同，可使用“数据主体”这一同义词替代“PII主体”。

3.1.15 软件即服务（SaaS）[b-ITU-T Y.3500]：一种云服务类别，其中向云服务客户提供的云功能类型应用功能类型。

3.1.16 租户[b-ITU-T Y.3500]：共享一套物理和虚拟资源接入的一组云服务用户。

3.1.17 威胁[b-ISO/IEC 27000]：可能对系统或机构造成伤害的有害事件的潜在起因。

3.2 本建议书定义的术语

无。

4 缩写词和首字母缩略语

本建议书使用了下述缩写词和首字母缩略语：

CSC 云服务客户

CSP 云服务提供商

CSU 云服务用户

IaaS 基础设施即服务

PaaS 平台即服务

PII 个人可识别信息

SaaS 软件即服务

5 排印惯例

无。

6 概述

6.1 此建议书内数据的规范

CSC数据包含存储在云平台的客户专用数据和通过云服务为CSC提供的相关数据，例如账户信息、登录记录和操作日志。

CSC（见第3.1.4节）与CSU（见第3.1.8节）术语间的差别，在下文做出了进一步澄清。

CSC是与CSP形成法律关系的个人或组织。所以CSC可以是一家企业、附属公司、政府部门或独立的消费者。

CSU是使用签约云服务的个人、设备或应用。CSU可以是政府雇员、智能手机上运行的应用程序或儿童等家庭成员。CSC通常会指定一些CSU作为管理员，管理CSC和CSP之间的关系。CSU总是代表CSC操作。大多受雇的CSU基本不需要或完全不需要了解CSP运行哪些内容或如何运行，也不需了解CSC签约的服务，除非CSC决定其有必要知晓（例如，管理员和内部审计员）。

一个CSC可包括多个云租户。一个租户可包括多个CSU。

6.2 云服务客户的数据安全性威胁

由于云服务环境通常为多租户环境，因此，数据丢失或泄漏对CSC是一项严重威胁。不能恰如其分地管理加密信息（如加密密钥）、认证代码和接入特权，可能会带来诸如数据丢失和向外界意外透露数据等重大损害。例如，造成这一威胁的主要原因可能是认证、授权和审计控制不足、加密或认证密钥的使用不统一、操作失败、处理不当、管辖权和政治问题、数据中心的可靠性以及数据恢复情况。

对存储数据的安全性而言，鉴于所有CSC数据实际都存储在CSP设备内，且存储资源由不同CSC共享，因此其可能面临多重风险，这其中包括：

1) 拥有高优先级接入权利的CSP内部人员能够引发未经授权的访问，造成CSC数据泄漏；

2) 意用户或黑客亦能引发未经授权的访问并造成CSC数据泄漏；

3) 跨境数据流动能导致数据泄漏，特别是敏感数据；

4) 软硬件故障，停电和自然灾害亦能造成数据损失。

数据安全问题亦存在于传输过程之中。传输过程中数据可能失窃或被篡改，因此在数据加密不当的情况下可能导致机密泄露。如果CSC尚未采用足够的加密，CSP应验证数据的完整性并采取相应加密措施。

另一威胁是剩余数据的泄漏。当CSC取消订购的服务后，其数据将被消除且存储空间将被释放并重新分配给其它CSC。CSP应负责确保某CSC或租户的剩余数据不被另一用户恢复。

6.3 数据安全性的现有要求

“[ITU-T X.1601]中规定的云计算的安全框架”对数据安全性提出了要求，其中包括数据隔离、保护、和隐私保护。

1) 数据隔离

在云计算环境中，租户不能接入属于另一租户的数据，即便数据得到加密也是如此，但明确得到授权的情况除外。根据所要求的隔离梯度和云计算软件及硬件的具体部署情况，可以逻辑或物理方式实现数据隔离。

注 – 在云计算中，隔离出现在租户层面。例如，在云中，一个特定CSC可能拥有多个租户，目的是为了将不同下属机构、处室或业务单位相互分开。

2) 数据保护

数据保护确保云计算环境中保存的CSC数据和衍生数据得到适当保护，使其只能按照CSC的授权（或按照适用法律）得到访问或修改。这种保护可包括合并采用访问控制清单、完整性核实、误码纠正/数据恢复、加密和其它适当机制。当CSP为CSC提供存储加密时，该加密可以是客户机一侧加密（如，在CSP应用内）或服务器一侧加密。

3) 隐私保护

私密信息可包括PII和公司保密数据，对私密信息的收集、使用、传送、处理、存储和销毁须遵守有关隐私的规则和法律，这一限制既适用于CSP，也适用于CSC。如，CSC必须有能力永久删除包含私密信息的数据表，即便CSP并不知晓该表的内容。CSP可能还需要以经过改造或加密的形式支持信息的处理，如搜索CSC数据。

隐私保护还包括觉察到的或由CSC活动衍生的私密信息，如业务趋势、与其它各方的关系或通信、活动程度和规律。

隐私保护亦负责确保所有隐私信息（包括观测或推导出的数据）仅用于CSC与CSP间商定的目的。

隐私信息的风险评估(称为“隐私风险评估”)可帮助CSP确定可预测操作涉及的特定隐私侵犯风险。CSP应确定并采用相应功能，处理风险评估和隐私信息处理确定的隐私风险。

注 – 在一些管辖区内，出于隐私考虑，独立自然人（即人类用户）的处理与其雇主被分别对待。在这种情况下，除CSC或租户之外，CSU的隐私将得到适当的保护。

6.4 数据安全的生命周期

基于云服务的实际情况，云服务客户数据安全的生命周期包括：

1) 创建：似乎更应将其命名为创建/更新，因为其适用于创建或改变数据/内容的要素，而不仅是一份文件或数据库。创建旨在生成新的数据内容或改变/更新现有内容。
2) 传输：此为将数据从一处传至另一处的通信流程。
3) 存储：存储是指将数字化的数据存入某种存储库内，通常几乎与创建同时发生。
4) 使用：将数据用于查询、处理、共用或在某类活动中使用。
5) 迁移：数据迁移是指在不同存储类型、形式或计算机系统间传输数据的过程。这是所有系统实施、更新或汇总中需要考虑的关键因素。数据迁移的原因有很多，其中包括服务器或存储设备的更换或更新；网站合并；服务器维护和数据迁址。
6) 破坏：使用物理或数字手段将数据永久性地破坏（例如，密码粉碎）。
7) 备份和恢复：用户可创建数据备份并从备份中恢复数据。

7 与数据安全相关的安全控制导则

本节提供了与第6.4节所述数据安全生命周期各阶段相关的安全控制导则。

7.1 创建阶段的安全控制

创建阶段的安全控制导则内容包括以下内容：

a) CSP应定义数据敏感度的类别。用户的数据标识可用于帮助实施数据分类。
b) 数据创建后应根据敏感度实施分组。
c) CSP应考虑企业数字权机制或通过加密限止未经授权访问敏感数据。

7.2 传输阶段的安全控制

传输阶段的安全控制导则内容包括以下内容：

a) CSP应采用技术方法确保鉴权数据的安全。
b) CSP应支持关键操作数据和管理数据的安全传输。
c) 传输期间应立即检测数据操作完整性受到的破坏，并采用必要措施，在检测到差错后恢复数据的完整性。

7.3 存储阶段的安全控制

存储阶段的安全控制导则内容包括以下内容：

a) CSP应确定其与存储库中提取的数据（例如[ITU-T X.1631]中定义的数据）共用的接入控制。

b) CSP应采用加密技术或其它安保技术确保鉴权数据存储的保密性。

c) CSP应支持用户维持关键操作数据和管理数据存储的保密性。

d) CSP应提供有效的硬盘保护方法或采用碎片化的存储机制，防止未经授权的用户从丢失的硬盘中获取有效用户数据。

e) 传输期间应立即检测数据操作完整性受到的破坏，并采用必要措施，在检测到差错后恢复数据的完整性。

f) 用户的可选加密参数配置，例如算法、强度和方案，应得到支持。

g) CSP应支持用户选用第三方加密机制对关键数据进行加密。

h) CSP应支持使用安全密钥进行数据加密，并支持在本地对安全密钥进行存储与维护。

i) CSP应支持有效的虚拟机器图像文件加载保护法，限止未经授权的用户在设备失窃的情况下在硬盘上运行其自己的计算资源。

7.4 使用阶段的安全控制

使用阶段的安全控制导则内容包括以下内容：

a) CSP应授权并验证数据的使用。

b) 应对敏感数据的使用进行审计，并生成审计日志。

c) CSP应根据其在检测数据使用威胁和控制方面的权利与义务，应用恶意行动监测和执法机制。

7.5 迁移阶段的安全控制

迁移阶段的安全控制导则内容包括以下内容：

a) 应在数据迁移之前评估网络连通性，确保迁移进程的安全性。

b) CSP应确保在迁移期间数据完整性和隐私不受影响。

c) CSP应确保数据迁移不影响服务和应用的连续性。

d) 在数据迁移过程中，CSP应恰当开展与数据备份和恢复相关的工作。

e) CSP应建立迁移机制，评估其可行性与风险，然后在筹备数据迁移期间开发相关的风险控制措施。

7.6 破坏阶段的安全控制

破坏阶段的安全控制导则内容包括以下内容：

a) CSP应能够消除与加密数据相关的所有关键资料。

b) CSP应使用物理销毁，例如物理硬件退役过程中的物理媒介消磁。

c) CSP应使用数据恢复技术进行销毁过程确认。

d) CSP应能够提供方法，帮助消除因数据在不同云平台间迁移、服务和合同终止及自然灾害产生的遗留数据。

e) CSP应为删除所有数据拷贝提供方法。

f) CSP应确保用户账户和口令等用户鉴权信息的存储空间，在信息全部消除完毕之前，不会释放并重新划分给其它用户。

g) CSP应确保在相关资源全部消除完毕之前，不会把文件、目录和数据库记录等资源的存储空间释放并重新划分给其它用户。

h) CSP应提供禁止恢复被毁数据的方法。

7.7 备份与恢复阶段的安全控制

备份与恢复阶段的安全控制导则内容包括以下内容：

a) CSP应使用防止数据丢失等内容恢复机制，帮助确定并审计有待备份的数据。

b) CSP应支持对长期（存档）存储媒介备份采用适当的加密算法，例如使用长加密密钥，并用经改进的加密算法进行替代。

c) CSP应提供本地数据备份和恢复功能。完整的数据备份应至少每周一次，并至少每天进行一次增量备份。

d) 应建立远程灾害恢复中心，配备通信线路、网络设备和数据处理设备等将灾害恢复功能纳入的必备产品。

e) 可建立冗余灾害恢复中心。该中心可具备与业务操作相对应的基本能力，并通过高速链路实时同步数据。该中心可同时分享业务与管理操作，并在灾害情况下通过应急切换保护业务的连续性。

f) 对归入重要或敏感类别的数据而言，CSP应在提供远程数据备份功能的同时，应提供及时恢复数据的能力。提供此服务的方法之一是利用灾害恢复中心的网络。

附录一

安全控制使用导则

（此附录并非本建议书不可分割的组成部分）

表I.1提供了控制集合的示例，这些示例可满足在数据分类和生命周期各阶段基础上制定的示范数据方案导则的要求。

表I.1 – 控制集的示例

类型	数据生命周期						
	创建	传输	存储	使用	迁移	破坏	备份与恢复
IaaS	7.1 a), b), c)	7.2 a), b), c)	7.3 a), b), c), d), e), h), i)	7.4 a), b), c)	7.5 a), b), c), d), e)	7.6 a), b), c), d), e), f), g), h)	7.7 a), c), d), e), f)
PaaS	7.1 a), b), c)	7.2 a), b), c)	7.3 a), b), c), d), e), f), i)	7.4 a), b), c)	7.5 a), b), c), d), e)	7.6 a), b), c), d), e), f), g), h)	7.7 a), b), c), d), e), f)
SaaS	7.1 a), b), c)	7.2 a), b), c)	7.3 a), b), c), d), e),f), g), h), i)	7.4 a), b), c)	7.5 a), b), c), d), e)	7.6 a), b), c), d), e), f), g), h)	7.7 a), b), c), d), e), f)

参考资料

[b-ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014) | ISO/IEC 17788:2014, *Information technology – Cloud computing – Overview and vocabulary*.

[b-ISO/IEC 27000] ISO/IEC 27000:2014, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

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

[b-NIST-SP-800-53] NIST Special Publication 800-53 Revision 4 (2015), *Security and privacy controls for Federal information systems and organizations*, Available [viewed 2016-12-10] at: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>

ITU-T 系列建议书

A系列	ITU-T工作的组织
D系列	一般资费原则
E系列	综合网络运行、电话业务、业务运行和人为因素
F系列	非话电信业务
G系列	传输系统和媒质、数字系统和网络
H系列	视听及多媒体系统
I系列	综合业务数字网
J系列	有线网络和电视、声音节目及其它多媒体信号的传输
K系列	干扰的防护
L系列	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
M系列	电信管理，包括TMN和网络维护
N系列	维护：国际声音节目和电视传输电路
O系列	测量设备的技术规范
P系列	电话传输质量、电话设施及本地线路网络
Q系列	交换和信令
R系列	电报传输
S系列	电报业务终端设备
T系列	远程信息处理业务的终端设备
U系列	电报交换
V系列	电话网上的数据通信
X系列	**数据网、开放系统通信和安全性**
Y系列	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
Z系列	用于电信系统的语言和一般软件问题

瑞士印刷
2017年，日内瓦