国 际 电 信 联 盟

ITU-T X.1603

(03/2018)

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 – 云计算安全设计

云计算监测业务的数据安全性要求

ITU-T X.1603 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

欲了解更详细信息，请查阅ITU-T建议书目录。

ITU-T X.1603 建议书

云计算监测业务的数据安全性要求

概要

ITU-T X.1603建议书分析了云计算监测业务的数据安全性要求，包括监测数据范围要求、监测数据生命周期、监测数据采集的安全性要求和监测数据存储的安全性要求。监测数据范围要求包括云服务提供商（CSP）应提供的、用于保持云安全性的必要的监测范围，以及云服务提供商的最大监测范围。监测数据生命周期包括数据产生、数据存储、数据使用、数据迁移、数据呈现、数据摧毁和数据备份。监测数据采集决定着监测业务采集技术的安全性要求。监测数据存储决定着在存储监测数据方面对云服务提供商提出的安全性要求。

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.1603	2018-03-29	17	11.1002/1000/13406

关键词

云、数据安全性、监测。

* 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

ITU-T X.1603 建议书

云计算监测业务的数据安全性要求

1 范围

本建议书阐述了云计算监测业务的数据安全性要求。建议书分析了与云计算环境下监测业务相关的数据安全性威胁和挑战，描述了监测业务的数据安全性要求，其中包括数据的范围、数据的生命周期、数据的获取和数据的存储。本建议书可供为云服务客户（CSC）提供监测服务的云服务提供商（CSP）使用。

2 参考资料

无。

3 术语和定义

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（authentication）[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 能力（capability）[b-ISO/IEC 19440]：有能力从事特定活动的品质。

3.1.3 云计算（cloud computing）[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。

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。

3.1.4 云服务（cloud service）[b-ITU-T Y.3500]：通过使用定义的接口启动的云计算（见第3.1.3条）实现的一种或多种功能。

3.1.5 云服务客户（cloud service customer）[b-ITU-T Y.3500]：为使用云服务（见第3.1.4条）而具有业务关系的一方（见第3.1.15条）。

注 – 业务关系不必隐含财务协议。

3.1.6 云服务合作伙伴（cloud service partner）[b-ITU-T Y.3500]：支持或辅助云服务提供商（见第3.1.7条）或云服务客户（见第3.1.5条）活动或双方活动的一方（见第3.1.15条）。

3.1.7 云服务提供商（cloud service provider）[b-ITU-T Y.3500]：提供云服务（见第3.1.4条）的一方（见第3.1.15条）。

3.1.8 云服务用户（cloud service user）[b-ITU-T Y.3500]：与使用云服务（见第3.1.4条）的云服务客户（见第3.1.5条）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 作为服务的通信（Communications as a Service (CaaS)）[b-ITU-T Y.3500]：云服务的类别，其中为云服务客户（见第3.1.5条）提供的能力是实时通信和协作。

注 – CaaS既可提供平台能力类型，也可提供应用能力类型。

3.1.10 社区云（community cloud）[b-ITU-T Y.3500]：云服务（见第3.1.4条）专门支持并由一系列特定云服务客户（见第3.1.5条）共享的云部署模式，资源至少由上述客户中的一人控制。

3.1.11 管理程序（hypervisor）[b-NIST-SP-800-125]：管理主机客户操作系统（guest OS）并控制客户操作系统与物理硬件之间指令流动的虚拟化部分。

3.1.12 作为服务的基础设施（Infrastructure as a Service）[b-ITU-T Y.3500]：云服务的类别，其中向云服务客户（见第3.1.5条）提供的云能力类型是一种基础设施能力类型。

注 – 云服务客户（见第3.1.5条）不管理也不控制下层物理和虚拟资源，但控制操作系统、存储和使用物理及虚拟资源得到部署的应用。云服务客户（见第3.1.5条）也可拥有控制特定网络成份（如主机防火墙）的有限能力。

3.1.13 多租户（multi-tenancy）[b-ITU-T Y.3500]：物理和虚拟资源的分配方法能够使多租户（见第3.1.24条）及其计算和数据相互隔离并无法实现互访。

3.1.14 作为服务的网络（Network as a Service）[b-ITU-T Y.3500]：一种类别云服务，其中向云服务客户（见第3.1.5条）提供的能力为传送连接和相关网络能力。

注 – NaaS可提供三种云能力类型中的任何一种。

3.1.15 相关方（party）[b- ISO/IEC 27729]：自然人或组织。

3.1.16 个人可识别信息（personally identifiable information）[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。

3.1.17 作为服务的平台（Platform as a Service）[b-ITU-T Y.3500]：一种类别云服务，其中向服务客户（见第3.1.5条）提供的能力类型是平台能力类型。

3.1.18 私有云（private cloud）[b-IUT-T Y.3500]：云服务（见第3.1.4条）专门由一个单一云服务客户（见第3.1.5条）享用的云部署模式，资源由云服务客户（见第3.1.5条）控制。

3.1.19 公共云（public cloud）[b-IUT-T Y.3500]：云服务（见第3.1.4条）可潜在地向任何云服务客户（见第3.1.5条）提供的云部署模式，资源由云服务提供商（见第3.1.7条）控制。

3.1.20 安全域（security domain）[b-ITU-T X.810]：指一套元素、安全政策、安全管理机构和一组与安全相关的活动，其中有关元素须符合相关活动的安全政策，而安全政策则受到有关安全域中安全管理机构的管理。

3.1.21 安全事件（security incident）[b-ITU-T E.409]：安全事件系指使安全的某个方面受到威胁的有害事件。

3.1.22 服务水平协议（service level agreement）[b-ISO/IEC 20000-1]：服务提供商与客户之间书面记录的、明确服务和服务目标的协议。

注1 – 也可在服务提供商与供应商、内部集团或作为供应商行事的客户之间签订服务水平协议。

注2 – 可将服务水平协议纳入合同或另一种文件记录协议之中。

3.1.23 作为服务的软件（Software as a Service）[b-IUT-T Y.3500]：一种类别云服务，其中向云服务客户（见第3.1.5条）提供的云能力类型为应用能力类型。

3.1.24 租户（tenant）[b-IUT-T Y.3500]：共享一套物理和虚拟资源接入的一组云服务用户（见第3.1.8条）。

3.1.25 威胁（threat）[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。

3.1.26 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

本建议书定义了下列术语：

3.2.1 监测数据（monitoring data）：监测数据是云监测服务的输出内容，可帮助云服务提供商（CSP）和云服务客户（CSC）管理云平台和云资源。

3.2.2 监测服务（monitor service）[b-ITU-T Y.3502]：监测服务活动监测云服务客户与云服务提供商间服务水平协议（SLA）中定义的服务水平的质量。

3.2.3 必要的监测数据（necessary monitoring data）：必要的监测数据用于维持服务水平协议（SLA）。必要的监测数据有助于云服务提供商（CSP）保持云计算平台的安全和稳定。必要的监测数据可包括，但不限于，管理系统的监测数据、物理资源监测数据、网络监测数据等。必要的监测数据主要供CSP使用，但亦可与云服务客户（CSC）共享。

3.2.4 可选监测数据（optional monitoring data）：可选监测数据是应云服务客户（CSC）的要求提供，用于提供云监测服务。可选监测数据可包括，但不限于，虚拟机器监测数据、数据存储服务监测数据、CSC有关监测数据的应用等。

3.2.5 虚拟机器（virtual machine(VM)）[b-NIST-SP-800-145]：对真实机器的高效、隔离和逻辑复制。

4 缩写词和首字母缩略语

本建议书使用了下列缩写词和首字母缩略语：

API 应用程序界面

BCP 业务连续性计划

CaaS 作为服务的通信

CPU 中央处理单元

CSC 云服务客户

CSN 云服务伙伴

CSP 云服务提供商

CSU 云服务用户

DDOS 分布式拒绝服务

DNS 域名系统

DOS 拒绝服务

IaaS 作为服务的基础设施

IAM 身份和接入管理

ICT 信息通信技术

IP IP互联网协议

IT 信息技术

NaaS 作为服务的网络

OS 操作系统

PaaS 作为服务的平台

PII 个人可识别信息

PKI 公共密钥基础设施

SaaS 作为服务的软件

SIM 用户身份模块

SLA 服务水平协议

VM 虚拟机器

5 惯例

本建议书中：

关键词**“要求”**表示必须得到严格遵守的要求，且如果声称遵守本建议书，则不得与该要求有任何偏差。

关键词**“建议”**表示是一项建议的并非需绝对遵守的要求，因此声称遵守本文件时不一定按照该要求行事。

关键词**“禁止”**表示必须得到严格遵守的要求，且如果声称遵守本建议书，则不得与之有任何偏差。

关键词**“作为选择可以”**表示允许的一项可选择的要求，不含有任何被建议的意思。该术语并非意味着厂商在实施中一定提供这一可选功能，网络运营商/服务提供商可作为选择提供这一功能。也就是说，厂商可以作为选择提供这一功能，同时仍然声称遵守本建议书提出的规范。

6 概述

本建议书分析了云计算监测服务的数据安全性要求，其中包括监测数据的范围、监测数据的生命周期、安全威胁与挑战和对云计算的数据安全性要求进行监测。

监测数据的范围阐述了两类云监测数据；必要数据和可选数据，并对其使用方式做出解释。

监测数据生命周期以及安全威胁与挑战，阐述了云监测数据的收集、存储、使用、迁移、分析、呈现、销毁和备份的内容和其面临的安全威胁与挑战。

监测数据安全性的要求阐述了云监测数据各生命周期阶段的详细要求。

7 云计算监测数据的范围

有云计算环境内，存在两类监测数据：必要的监测数据和可选监测数据。

必要的监测数据是用于维持服务水平协议（SLA）的数据。必要的监测数据可帮助CSP安全稳健地运行云计算平台。必要的监测数据可能包括，但不限于，管理系统监测数据、物理资源监测数据和网络监测数据。必要的监测数据主要供CSP使用，但亦可与云服务客户（CSC）共享。

可选监测数据是应云服务客户（CSC）的要求提供，用于提供云监测服务。可选监测数据可包括，但不限于，虚拟机器监测数据、数据存储服务监测数据、CSC有关监测自身数据的应用等。

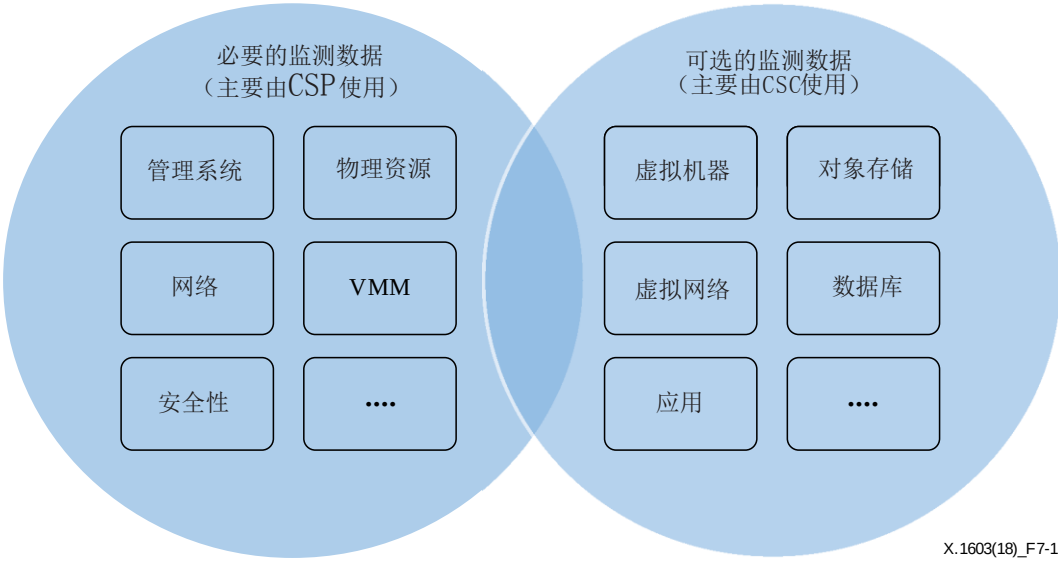

图7-1 – 两类监测数据的使用案例

必要的监测数据主要供CSP使用，但亦可供CSC使用。例如，云物理资源的监测数据主要由CSP用来维持云平台的稳定性，但亦可在将与云相关的资源作为服务提供给客户的情况下，供CSC使用。

可选监测数据是应CSC的请求提供，且主要供CSC使用。CSP可使用可选监测数据维持SLA。例如，CSC可要求CSC数据与监测云内自有的应用建立关联。此数据由CSP提供，用于改善云内相关应用的管理。例如，CSP使用服务即数据库（DBaaS）的监测数据来维持云内数据库资源和服务的安全与稳定。

这两类监测数据的关系见图7-1。

8 云计算的监测数据生命周期

本节阐述了云计算的监测数据生命周期并澄清了该生命周期与云计算内其它数据生命周期的差异。

8.1 监测数据采集

监测数据采集源自监测数据的获取和将该数据发送给存储服务器的过程。大多数监测数据的创建是通过CSC对云服务的使用。必要的监测数据亦可通过其它云服务监测活动创建。

8.2 监测数据存储

在创建了监测数据采集之后，云监测数据可存储于本地的CSC云资源或CSP的监测数据存储服务器。

8.3 监测数据的使用

监测数据可用于维持云平台和CSP提供云服务的性能与安全；它亦可用于维持CSC云资源的性能与安全。

8.4 监测数据迁移

云资源迁移后，监测数据可与云资源一同迁移。

8.5 监测数据分析

CSP和CSC可对监测数据加以分析，以了解云平台资源的状态，从而更好地管理并提高其安全性。

8.6 监测数据的呈现

建议以有意义的方式呈现监测数据，以便更好地管理SLA和云安全。鉴于云监测数据量可能很大，因此建议以可控且可理解的方式对其加以归纳。

8.7 监测数据的销毁

为持续监测数据安全性，要求CSP按CSC的要求销毁监测数据。

在创建监测数据之后合适的时间段，CSP可选择销毁监测数据。

8.8 监测数据的备份

要求创建监测数据的备份并从备份中恢复数据。

9 云计算监测数据安全威胁与挑战

[b-ITU-T X.1601]第7和第8节对云计算中有关CSC和CSP安全威胁与挑战分别加以阐述；云监测数据同样也面临着[b-ITU-T X.1601定义的类似安全威胁与挑战。云监测数据面临的部分安全威胁与挑战，包括但不限于以下内容：

a) 数据丢失和泄漏；

b) 不安全的服务获取；

c) 未经授权的管理获取；

d) 内部威胁

e) 丧失信任；

f) 丧失管理；

g) 丧失隐私；

h) 服务不可用；

i) 盗用知识产权；

j) 共享环境；

k) 管辖冲突；

l) 不良的过渡和集成；

对于监测数据生命周期各阶段，云监测数据面临着特定的安全威胁与挑战。

9.1 监测数据采集阶段的安全威胁与挑战

a) 未授权的数据采集：CSP或攻击方可在未经许可或授权的情况下采集CSC的监测数据。

b) 获取接口的脆弱性：攻击方可能会利用监测数据获取接口的脆弱性。

c) 欺诈：攻击方可伪装为云监测服务的管理系统或数据存储服务器，造成监测数据的损失。

d) 伪造和监听：攻击方可使用中间人或其它网络攻击伪造或监听监测数据。

e) 不安全的服务接入：在监测数据采集阶段，不安全接入数据采集接口可造成监测数据损失。

f) 未经授权获取管理员权限：未经管理员授权接入CSP监测数据采集系统或CSC系统，可造成监测数据损失。例如，攻击方可利用系统弱点，在不经授权的情况下获取CSC系统的管理员权限，并将监测采集的目的地IP地址改为攻击方的地址。

9.2 监测数据存储阶段的安全威胁与挑战

a) 数据损失与泄露：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和CSP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的极大损害。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、加密和/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等重大威胁。

b) 服务不可用：监测数据存储服务器可受到拒绝服务（DoS）或分布式拒绝服务(DDoS)的攻击；此外，监测数据存储硬件可能会出现故障且造成数据损失或破坏。

9.3 监测数据使用阶段的安全威胁与挑战

a) 数据滥用：CSC监测数据可能被CSP滥用。监测数据可供CSP用于维持云计算平台和资源操作的SLA；但是， CSC监测数据亦可在没有CSC许可的情况下用于其它目的。

b) 内部威胁：CSP或CSC的员工可能会将CSC监测数据滥用于其它目的。

c) 系统脆弱性：由于系统的脆弱性，在数据使用过程中监测数据可能会丢失。

d) 窃听：监测数据可能受遭到攻击方窃听。

9.4 监测数据迁移阶段的安全威胁与挑战

a) 数据滥用：监测数据可在不同位置间迁移。十分重要的是不能允许监测数据在发往不同位置的过程中遭到滥用。

b) 欺诈：攻击方可伪装成管理系统或数据存储服务器，从而造成监测数据的损失或滥用。

c) 伪造和监听：攻击方可使用中间人或其它网络攻击伪造和监听拦截数据。

9.5 监测数据分析阶段的安全威胁与挑战

a) 数据滥用：CSP数据分析期间，CSC监测数据可能遭滥用。

b) 系统脆弱性：由于系统的脆弱性，数据分析可能造成监测数据丢失。

c) DoS攻击：监测数据分析服务器可能遭受DoS或DDoS攻击。

9.6 监测数据呈现阶段的安全威胁与挑战

a) 数据滥用：在数据呈现过程中，CSC 监测数据可能遭CSP滥用（或不经CSC许可便呈现）。

b) 系统脆弱性：由于数据呈现系统的脆弱性，报告和分析数据可能会丢失。

c) 错误的呈现：数据呈现过程中CSC监测数据可能会出现错误。

9.7 监测数据销毁阶段的安全威胁与挑战

a) 欺诈：攻击方可伪装成云监测服务的管理系统，从而造成其它监测数据的损失。

b) 操作系统的脆弱性：由于系统的脆弱性，数据使用过程中可能造成监测数据丢失。

9.8 监测数据备份阶段的安全威胁与挑战

a) 操作系统脆弱性：由于系统的脆弱性，数据备份期间可能造成监测数据丢失，从而导致数据无法恢复。

10 云计算监测数据的安全性要求

本节确定了云计算监测服务的数据安全性要求。

10.1 监测数据采集的安全要求

监测数据采集的数据安全性要求包括以下内容：

a) 仅可应CSC请求创建可选监测数据；

b) 建议在创建了必要的监测数据后，向CSC发出通知；

c) 建议将监测数据的范围通知CSC；

d) 须保持监测数据的完整性和精度；

e) 建议使用标准的数据获取技术；

f) 建议为监测数据获取接口提供接入控制方法，例如白名单、黑名单等；

g) 建议提供加密方法，以确保监测数据获取接口的安全；

h) 建议在云资源和监测数据存储服务器之间使用标准网络协议。

表10-1归纳了监测数据采集过程中安全威胁与对安全性要求之间的对映关系。

表10-1 – 监测数据采集：安全威胁与安全性的要求之间的对映关系

安全威胁	对安全性的要求
未经授权进行数据采集	a), b), c)
获取接口的脆弱性	d), e), f), g)
欺诈	d), e), f), g), h)
伪造和监听	h)
不安全的服务接入	b), d), e), f), g), h)
未经授权获取管理权限	d), e), f), g), h)

10.2 监测数据存储对安全性的要求

监测数据存储的数据安全性要求包括以下内容：

a) 建议CSP为监测数据存储服务器提供适当的接入控制方法；

b) 建议CSP为保留监测数据确定最长的时间段；

c) 建议CSP为监测数据提供适当的加密方法。

表10-2归纳了监测数据存储的安全威胁与安全性要求之间的对映关系。

表10-2 – 监测数据存储：安全威胁与安全性要求之间的对映关系

安全威胁	对安全性的要求
数据损失与泄露	a), b), c)
服务不可用	a), c)

10.3 使用监测数据对安全性的要求

使用监测数据对安全性的要求包括如下内容：

a) 要求CSP明确确定CSC如何使用监测数据；

b) 建议CSP向CSC提供一个正式的监测数据使用声明，如图10-1所示。

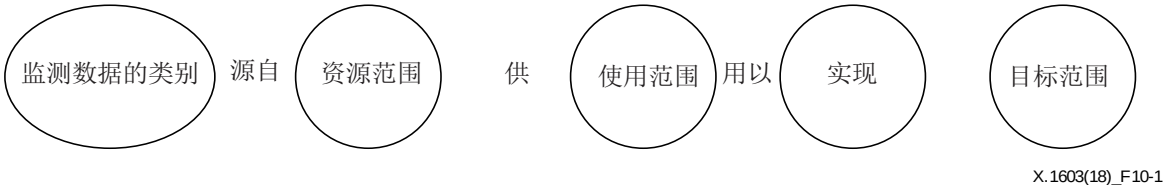

图10-1 – 推荐使用的监测数据声明

c) 要求CSP在将监测数据用于其它目的前，提供通知并获得CSC的许可；

d) 要求CSP支持监测数据使用的记录和审计。

表10-3归纳了使用监测数据的安全威胁与安全性要求之间的对映关系。

表10-3 – 使用监测数据：安全威胁与安全性要求之间的对映关系

安全威胁	对安全性的要求
数据滥用	a), b), c), d)
内部威胁	a), b), c), d)
系统的脆弱性	d)
窃听	d)

10.4 监测数据迁移对安全性的要求

监测数据迁移对数据安全性的要求包括以下内容：

a) 建议CSP向CSC发出监测数据迁移通知；

b) 要求CSP确保监测数据迁移过程中的安全传输；

c) 要求CSP支持监测数据迁移操作的记录和审计。

表10-4归纳了监测数据迁移安全威胁与安全性要求之间的对映关系。

表10-4 – 监测数据迁移：安全威胁与安全性要求之间的对映关系

安全威胁	对安全性的要求
数据滥用	a), c)
欺诈	b), c)
伪造和监听	b), c)

10.5 监测数据分析对安全性的要求

监测数据分析的数据安全性要求包括以下内容：

a) 要求CSP就监测数据分析的目的向CSC发出通知；

b) 要求CSP实施监测数据分析系统脆弱性防护措施，例如CSP应防止监测数据分析系统的数据损失了泄漏；

表10-5归纳了监测数据分析安全威胁与安全性要求之间的对映关系。

表10-5 – 监测数据分析：安全威胁与安全性要求之间的对映关系

安全威胁	对安全性的要求
数据滥用	a)
系统脆弱性	b)

表10-5 – 监测数据分析：安全威胁与安全性要求之间的对映关系

安全威胁	对安全性的要求
DoS攻击	b)

10.6 监测数据呈现对安全性的要求

监测数据呈现对安全性的要求包括以下内容：

a) 要求CSP保持呈现监测数据的完整性与准确性；

b) 要求CSP为保护监测数据呈现的使用实施认证方法；

c) 要求CSP支持为监测数据呈现系统的脆弱性提供保护，例如CSP可使用渗透测试法为监测数据呈现系统提供脆弱性防护。

表10-6归纳了监测数据呈现的安全威胁与安全性要求之间的对映关系。

表10-6 – 监测数据的呈现：安全威胁与安全性要求之间的对映关系

安全威胁	对安全性的要求
数据滥用	a), b)
系统脆弱性	b), c)
错误的呈现	a), b), c)

10.7 监测数据的销毁对安全性的要求

监测数据的销毁对安全性的要求包括以下内容：

a) 要求CSP为监测数据提供适当的销毁方法；

b) 要求CSP防止使用规划外的监测数据销毁方法；

c) 要求CSP防止出现监测数据销毁不完整；

d) 要求CSP删除所有针对加密数据的特定CSC密钥；

e) 要求CSP销毁监测数据的拷贝；

f) 要求CSP向CSC提供监测数据销毁的通知。

表10-7归纳了监测数据销毁的安全威胁与安全性要求之间的对映关系。

表10-7 – 监测数据的销毁：安全威胁与安全性要求之间的对映关系

安全威胁	对安全性的要求
欺诈	a), b), c), d), e), f)
操作系统脆弱性	b), c), d), e), f)

10.8 监测数据备份对安全性的要求

监测数据备份对安全性的要求包括如下内容：

a) 要求CSP为防止监测数据损失提供备份方法；

b) 要求CSP保证恢复监测数据的完整性和准确性；

c) 要求CSP支持监测数据恢复的记录和审计。

表10-8归纳了监测数据备份的安全威胁与安全性要求之间的对映关系。

表10-8 – 监测数据的备份：安全威胁与安全性要求之间的对映关系

安全威胁	对安全性的要求
操作系统脆弱性	a), b), c)

参考资料

[b-ITU-T E.409] Recommendation ITU-T E.409 (2004), *Incident organization and security incident handling: Guidelines for telecommunication organizations*.

[b-ITU-T X.810] Recommendation ITU-T X.810 (1995), *Information technology – Open System Interconnection – Security frameworks for open system: Overview*.

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

[b-ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014), *Information technology – Cloud computing – Overview and vocabulary*.

[b-ITU-T Y.3502] Recommendation ITU-T Y.3502 (2014), *Information technology – Cloud computing – Reference architecture*.

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

[b-ISO/IEC 19944] ISO/IEC 19944 (2016), *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 – Part 1: Service management system requirements*.

[b-ISO/IEC 27000] ISO/IEC 27000 (2016), *Information technology –Security techniques – Information security management systems – Overview and vocabulary*.

[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*.

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

[b-NIST-SP-800-53] NIST Special Publication 800-53 Rev. 3 (2013), *Recommended Security Controls for Federal Information Systems and Organizations*.

[b-NIST-SP-800-125] NIST Special Publication 800-125 (2011), *Guide to Security for Full Virtualization Technologies*.

[b-NIST-SP-800-145] NIST Special Publication 800-145 (2011), *The NIST Definition of Cloud Computing*.

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
2019年，日内瓦