国 际 电 信 联 盟

ITU-T X.1752

(01/2022)

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

数据安全 – 大数据安全

大数据基础设施和平台的安全导则

ITU-T X.1752 建议书

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
消息处理系统	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（1）	X.1140 – X.1149
应用安全（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
IPTV安全	X.1180 – X.1199
网络空间安全	
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.1350 – X.1369
智能交通系统（ITS）安全	X.1370 – X.1399
分布式账簿技术（DLT）安全	X.1400 – X.1429
应用安全 (2)	X.1450 – X.1459
网页安全（2）	X.1470 – X.1489
网络安全信息交换	
网络安全概述	X.1500 – X.1519
漏洞/状态信息交换	X.1520 – X.1539
事件/事故/启发式信息交换	X.1540 – X.1549
政策的交换	X.1550 – X.1559
启发式和信息请求	X.1560 – X.1569
标识和发现	X.1570 – X.1579
确保交换	X.1580 – X.1589
网络防御	X.1590 – X.1599
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指导原则	X.1640 – X.1659
云计算安全实施方案	X.1660 – X.1679
其他云计算安全	X.1680 – X.1699
量子通信	
术语	X.1700 – X.1701
量子随机数发生器	X.1702 – X.1709
QKDN安全框架	X.1710 – X.1711
QKDN安全设计	X.1712 – X.1719
QKDN安全技术	X.1720 – X.1729
数据安全	
大数据安全	**X.1750 – X.1759**
数据保护	X.1770 – X.1789
IMT-2020安全	X.1800 – X.1819

ITU-T X.1752 建议书

大数据基础设施和平台的安全导则

概要

ITU-T X.1752建议书分析了大数据基础设施和平台的安全威胁和挑战，并规定了一个参考框架，以针对大数据基础设施和平台的威胁制定安全导则。

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.1752	2022-01-07	17	11.1002/1000/14806

关键词

大数据，基础设施，平台，安全导则。

* 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、信息和通信技术（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，因此大力提倡他们通过ITU-T网址查询适当的ITU-T数据库：http://www.itu.int/ITU-T/ipr/。

目录

ITU-T X.1752 建议书

大数据基础设施和平台的安全导则

1 范围

本建议书描述了相关论坛现有标准化工作的大数据基础设施和平台。本建议书制定了威胁评估方法，指定了保护大数据基础架构和大数据平台的安全导则。本建议书还提供了威胁和安全导则之间的对应关系。

2 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.1279] ITU-T X.1279 (2020)建议书，使用具有反欺骗检测机制的远程生物特征识别的增强认证框架

[ITU-T X.1601] ITU-T X.1601 (2015) 建议书，云计算安全框架

[ITU-T X.1603] ITU-T X.1603 (2018) 建议书，云计算监测业务的数据安全性要求

[ITU-T X.1605] ITU-T X.1605 (2020) 建议书，云计算中公共基础设施即服务（IaaS）的安全要求

[ITU-T Y.3600] ITU-T Y.3600 (2015) 建议书，数据 – 基于云计算的要求及能力

[ITU-T Y.3605] ITU-T Y.3605 (2020) 建议书，大数据 – 参考架构

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

3.1.2 审计（audit）[b-ITU-T X.800]：对系统记录和活动所做的一种独立审核和检查，以便测试系统控制的恰当性，确保符合既定策略和操作程序的要求，检测违反安全行为，并就控制、策略和程序提出修改建议。

3.1.3 认证（authentication）[b-ISO/IEC 18014-2]：为实体身份提供的保证。

3.1.4 大数据分析（big data analysis）[b- ITU-T Y.2244]：为了获得有意义的结果，如趋势或偏好，对海量数据进行的审查。

3.1.5 数据脱敏（data desensitization）[b-ITU-T X.1217]：隐藏敏感数据的过程。

3.1.6 数据完整性（data integrity）[b-ITU-T X.800]：数据未被以未授权方式修改或破坏的特性。

3.1.7 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。

3.1.8 负载平衡（load balancing）[b-ITU-T Y.2052]：一种可以分离和平衡流量负载以有效利用网络资源（例如链路带宽）的方案。

3.1.9 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。

3.1.10 入侵防御系统（intrusion prevention system）[b-ITU-T X.1361]：专门设计用于提供主动响应能力的入侵检测系统的变体。

3.1.11 多因素认证（multi-factor authentication）[b-ITU-T X.1158]：通过至少两个独立认证因素进行的认证。

3.1.12 冗余（redundancy）[b-ITU-T E.800]：在某一项内，存在一种以上执行所需功能的手段。

3.1.13 稳健性（Robustness）[b-ITU-T J.1014]：一个特定的ECI安全函数的执行的属性，表示破解执行的安全函数的防护措施所需要的努力和/或者代价。

3.1.14 安全配置参数（security configuration parameter）[b-ITU-T X.1046]：描述安全功能特征的一组参数，如最大带宽、最大连接数等 这些参数由安全功能、受保护对象和安全功能的安全操作提供支持。

3.1.15 单点登录（single sign-on）[b-ITU-T Y.2201]：用户使用认证声明，而从一个网络运营商/服务提供商向另一个运营商/服务提供商切换，以接入服务或者在到访网络漫游的能力。

3.1.16 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。

3.1.17 验证（validation）[b-ITU-T Z.450]：检查规范以确保其语法和语义正确并表示预期行为的过程。

3.1.18 漏洞（vulnerability）[b-ITU-T X.1524]：所有可被用来破坏系统或系统所存信息的软件弱点。

3.1.19 白名单（whitelist）[b-ITU-T X.1245]：通信服务中有关人员或来源的一个身份清单 该清单中的人员或来源是已知的、可信的或得到明确许可的。

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 大数据基础设施（big data infrastructure）：由大数据生态系统中的基本物理设备和网络环境组成的系统，为数据收集、数据处理、数据管理等提供大数据服务。

3.2.2 大数据平台（Big data platform）：大数据生态系统中执行数据分析、数据可视化和其他功能的一个系统或一组分布式系统。

4 缩写词和首字母缩略语

本建议书使用下列缩写词和首字母缩略语：

API 应用程序接口
BDAP 大数据应用提供商
BDIP 大数据基础设施提供商
DOS 拒绝服务
DDOS 分布式拒绝服务
IAM 身份和接入管理
IDS 入侵检测系统
IP 互联网协议
IPS 入侵预防系统
SSO 单点登录
VM 虚拟机

5 惯例

在本建议书中：

关键词“建议”（is recommended）指的是一项建议性的、并非绝对需遵守的要求。

6 大数据基础设施和平台面临的安全威胁和挑战

如图6-1所示（改变自[ITU-T Y.3600]的图7-1），按照[ITU-T Y.3600]的定义，大数据平台由大数据应用提供商（BDAP）提供，用于执行数据分析，实施数据可视化等功能。大数据基础设施由大数据基础设施提供商（BDIP）提供，可执行数据收集、数据处理、数据管理等大数据服务。

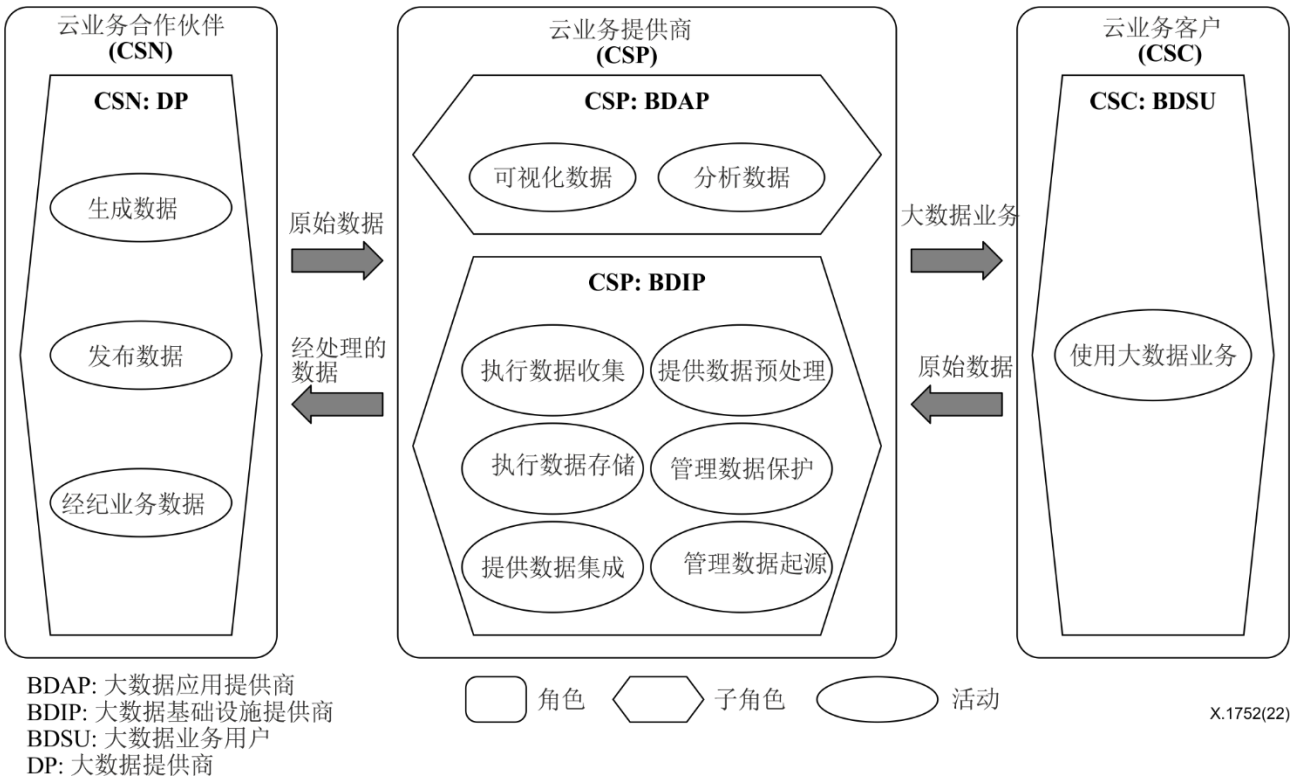

图 6-1 – 基于云计算的大数据系统

6.1 大数据基础设施面临的安全威胁和挑战

大数据基础设施面临的安全威胁和挑战涉及数据收集、数据存储、数据集成、数据预处理和数据管理。

6.1.1 数据收集面临的安全威胁和挑战

数据收集安全方面的威胁和挑战包括：

a) 未授权的数据收集：攻击方或可在未经用户许可或授权的情况下收集数据。

b) 数据收集接口漏洞：攻击者可能利用数据收集接口漏洞访问采集过程，造成数据丢失。

c) 未经授权的管理接入：未经授权的管理接入可能会导致数据丢失。例如，攻击者可能利用系统漏洞来获得对数据收集系统未经授权的管理接入，并将数据收集目标的互联网协议（IP）地址修改为攻击者的IP地址。

6.1.2 数据存储面临的安全威胁和挑战

数据存储安全方面的威胁和挑战包括：

a) 数据丢失和泄漏：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极大损害。此外，多源数据的大规模融合增加了数据存储访问控制的难度。大数据存储和流动的复杂场景使得数据加密难以实施。

b) 服务不可用：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，数据存储硬件可能会出现故障且造成数据损失或破坏。

c) 数据存储物理设施面临的安全威胁和挑战：物理设施安全面临着类似于[ITU-T X.1601]第9.3节和[ITU-T X.1605]第7节所述的安全威胁和挑战。

d) 数据存储终端面临的服务威胁和挑战：对于数据存储终端，安全威胁和挑战集中于终端软硬件的安全配置参数，其中包括操作系统、办公软件、浏览器、邮件系统等的安全配置参数。这方面的主要的安全威胁和挑战包括安全配置参数设置错误、安全配置参数更新不及时、安全配置参数存在漏洞等。

6.1.3 数据集成面临的安全威胁和挑战

数据集成安全方面的威胁和挑战包括：

a) 数据滥用：数据集成过程中数据可在不同物理位置间迁移。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) 欺骗：正如[ITU-T X.1279]中定义的那样，通过展示一幅记录的图像或其他生物特征识别数据样本或者人工衍生的生物特征识别特性，欺骗通过将一个实体伪装为另一不同的实体，以实现冒充。攻击方可伪装成管理系统或数据存储服务器，从而在数据集成过程中造成数据的损失或滥用。

c) 数据集成期间的网络安全威胁：面临类似于[ITU-T X.1601]第9.5节所述的安全威胁和挑战。此外，大数据基础设施中的特殊安全挑战集中于跨实体网络、虚拟网络和云环境的集成安全管理。

6.1.4 数据预处理面临的安全威胁和挑战

数据预处理安全方面的威胁和挑战包括：

a) 内部威胁：BDAP的员工可能会在未经用户许可的情况下，在数据预处理过程中将用户的数据用于非预期目的。

b) 系统漏洞：由于系统的漏洞，在数据预处理过程中数据可能会丢失。

6.1.5 数据管理面临的安全威胁和挑战

数据管理安全方面的威胁和挑战包括：

a) 软件漏洞：攻击者可能会利用大数据管理所用软件的潜在安全漏洞。系统虚拟化的技术缺陷可能会导致若干安全风险；此外，不成熟的运维技术可能导致风险更加严重。此外，大数据基础设施和平台的大规模分布式存储和计算模型给大数据管理使用的软件带来了更高的安全配置参数风险。

b) 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。

c) 未经授权的管理接入：对大数据管理系统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大数据系统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。

d) 内部威胁：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可能会造成数据丢失。

6.2 大数据平台面临的安全威胁和挑战

大数据平台面临的安全威胁和挑战涉及数据可视化和数据分析等。

6.2.1 数据分析面临的安全威胁和挑战

数据分析安全方面的威胁和挑战包括：

a) 系统漏洞：由于数据分析系统的漏洞，可能造成数据丢失。

b) DoS/DDoS攻击：数据分析服务器可能遭受DoS或DDoS攻击。

c) 数据分析应用程序的共享使用：数据分析应用程序通常由不同的用户使用，这可能导致虚拟机（VM）逃逸、数据泄漏等。

d) 不安全的接入：不安全接入可能会导致应用数据丢失，泄漏或滥用。

e) 未经授权的管理接入：未经授权的管理接入可能会导致数据丢失。

6.2.2 数据可视化面临的安全威胁和挑战

数据可视化安全方面的威胁和挑战包括：

a) 数据滥用：在数据可视化过程中，测数据可能遭BDAP滥用（或不经用户许可便呈现）

b) 系统漏洞：由于数据呈现系统的漏洞，报告和分析数据可能会丢失。

c) 错误的呈现：由于访问控制策略的失败，在未经用户许可的数据可视化过程中，数据可能会出现呈现错误。

7 大数据基础设施和平台的安全导则

根据[ITU-T Y.3605]的定义，大数据参考架构使用的分层框架有四层，外加一组跨层的功能。这四层为：

- 接入层；
- 应用层；
- 处理层；和
- 数据源层。

跨越各层的功能称为多层功能。

分层框架如图7-1所示（改编自[ITU-T Y.3605]的图8-2）。

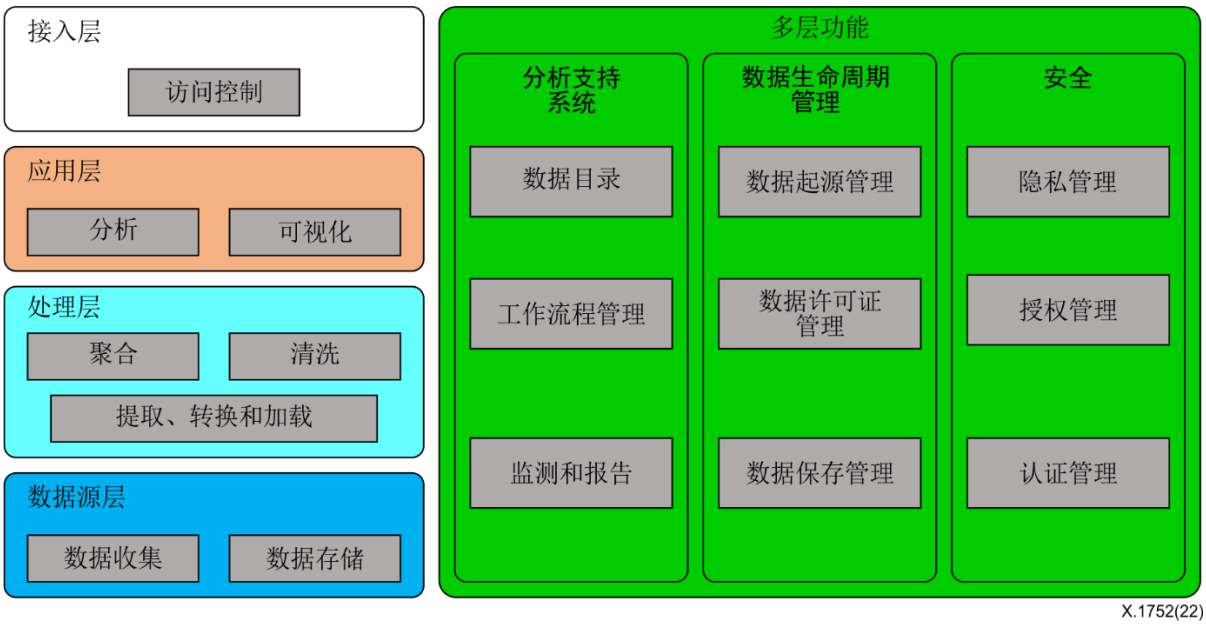

图7-1 – 大数据分层框架

基于图7-1显示的分层框架，本建议书使用了如图7-2所示的大数据基础设施和平台安全架构。

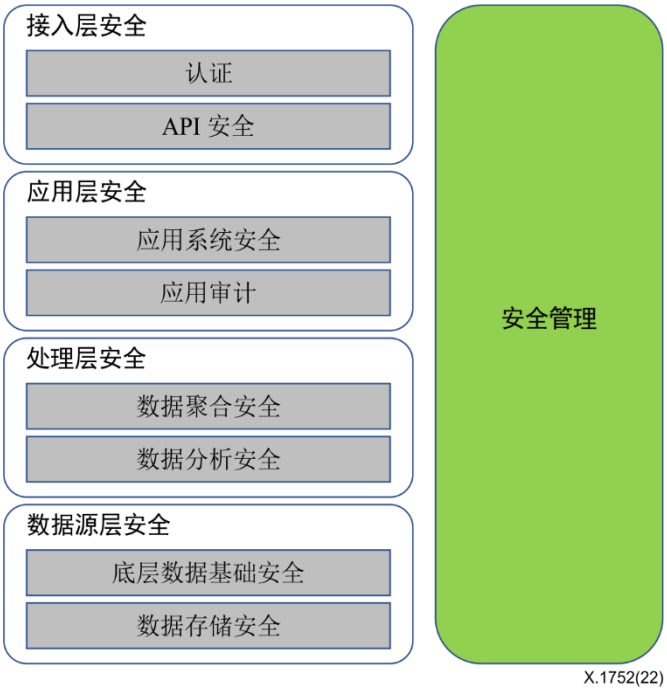

图7-2 – 大数据基础设施和平台安全性的体系结构

本建议书规定了大数据基础设施和平台的安全导则，包括：

a) 数据源层的安全导则
b) 处理层的安全导则
c) 应用层安全导则
d) 接入层的安全导则
e) 安全管理导则

7.1 数据源层的安全导则

数据源层的安全导则侧重于底层基础设施安全和数据存储安全。

7.1.1 底层基础设施的安全导则

底层基础设施的安全导则包括以下内容：

a) 建议将虚拟基础设施划分为内部和外部安全域，按需实施不同的安全策略。建议在内部和外部安全域之间提供有效隔离机制。

b) 建议在虚拟基础设施的安全域之间实施严格的访问控制策略。建议使用最小特权原则，从而根据角色职责分配进行用户身份认证和授权，以允许对虚拟基础设施实施访问控制。

c) 建议在虚拟基础设施上部署防病毒软件等安全软件，增强安全防护，定期更新病毒和恶意代码数据库。

d) 建议部署网络攻击检测和防护设备，如入侵防御系统（IPS）/入侵检测系统（IDS）、防火墙、DDoS防护等，并定期将攻击特征数据库更新到最新版本。

e) 建议在内部和外部网络边界实施严格的隔离和访问控制策略，以防止对底层基础设施的未授权访问。

f) 建议监控底层基础设施的网络流量并对网络流量统计、网络流量异常等关键信息进行深度检查。

g) 建议在检测到攻击时显示攻击信息，如攻击类型、源/目的IP地址、时间戳等。

h) 建议集中对各种物理和虚拟资源的运行状态等进行实时安全监控。

7.1.2 数据存储的安全导则

数据存储的安全导则包括以下内容：

a) 建议实施安全功能的数据存储组件，如安全的分布式文件系统、安全的索引存储等，以确保存储环境的安全性。

b) 建议支持多租户环境中不同用户数据的隔离策略。

c) 建议制定数据存储的安全策略和管理规定，如访问控制策略、安全数据传输策略、数据完整性策略、多副本一致性策略、个人信息和必要数据加密策略等。

d) 建议支持多种数据脱敏机制。

e) 建议支持文件系统加密，以防止数据损坏和泄露。此外，建议支持基于数据敏感级别的分类加密：不加密、部分加密、完全加密等。

f) 建议提供检测存储数据完整性损坏和损坏发生后恢复数据完整性的功能。

g) 建议支持可选的加密安全配置参数供用户选择。

h) 建议CSP应支持用户选用第三方加密机制对关键数据进行加密。

i) 建议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。

j) 建议支持对长期存储媒介备份采用适当的加密算法，例如使用长加密密钥，并规划用经改进的加密算法进行替代。

k) 建议明确定义数据共享、数据使用授权、数据删除的及时性和权限。

l) 建议授权数据使用的有效期，并通知关联的大数据提供商和用户。

m) 建议支持数据删除、备份和恢复功能。

7.2 处理层的安全导则

处理层的安全导则侧重于数据聚合安全和数据分析安全。

7.2.1 数据聚合的安全导则

数据聚合的安全导则包括以下内容：

a) 建议数据聚合组件支持认证机制，建议对数据源终端和大数据平台运营商进行认证和授权。

b) 建议在数据聚合过程中执行严格的安全规定，包括分类、传输和临时存储。

c) 建议各种数据源建立具有相应安全管理策略的数据分类策略，该分类策略应涵盖传输和临时存储的过程。对于每一类数据源，建议通过机密性、完整性和可用性定义相应的安全管理策略。

d) 在数据聚合过程中，建议支持通过受限访问控制功能访问临时存储文件夹，从而禁止用户访问不需要的进程或用户数据，禁止对数据聚合组件的存储地址进行未经授权的修改。

e) 建议为数据聚合组件提供负载均衡功能，这样便可以通过多通道缓解大数据流的负载压力。

f) 建议为数据聚合组件提供检测和保护功能，如IPS/IDC，以便对过度或不必要的数据收集加以限制。

g) 建议为数据聚合组件提供故障转移和恢复机制，使传输的数据流可以切换到备用组件。

h) 建议为数据聚合提供日志记录，并对异常情况发出警报，这些异常情况包括：重复收集数据、数据流大于设定门限值、数据流被中断或超过收集的数据存储量。

7.2.2 数据分析的安全导则

数据分析的安全导则包括以下内容：

a) 建议提供认证方法，以确保只有合法用户或应用程序才能启动数据分析请求。

b) 建议根据大数据用户识别策略和用户认证策略，使用数据分析访问控制模块，实现访问控制及时性的管理和验证、访问数据合法性的验证机制等。

c) 建议支持分析分布式数据的安全审计，建议对审计信息进行保护性存储和控制。

d) 建议提供脱敏机制，维护数据分析的安全性和健壮性，并建议不影响业务连续性。此外，使用脱敏机制后，建议不对系统性能产生巨大影响。

e) 建议能够根据不同用户的需求和不同数据设置不同的脱敏机制。

f) 建议支持用户提出查询或需求后的脱敏算法配置。

g) 建议可以动态添加或删除脱敏机制，支持系统在业务不中断的情况下顺利升级。

7.3 应用层安全导则

应用层安全导则侧重于应用系统和应用审计。

7.3.1 应用系统的安全导则

应用系统的安全导则包括以下内容：

a) 建议为应用系统提供检测和保护方法，如防火墙、防病毒系统和IDS/IPS。

b) 建议要针对应用系统的漏洞实施防御。

c) 建议提供认证方法，防止未经授权访问应用系统。

d) 建议不同应用之间保持隔离，避免因不同应用发起的数据关联分析导致数据泄露。

7.3.2 应用程序审计的安全导则

应用程序审计的安全导则包括以下内容：

a) 建议审计管理员对应用程序的操作，可藉此跟踪事件并提取安全事件的证据。

b) 建议审核用户对应用程序的操作，以便能够检测、警告恶意行为的出现并对此作出快速响应。

c) 建议审核告警、恶意行为快速响应等安全配置参数的修改。

7.4 接入层的安全导则

接入层的安全导则侧重于认证机制和应用程序接口（API）。

7.4.1 认证机制的安全指南

身份认证机制的安全导则包括以下内容：

a) 建议支持增强的身份认证服务，如单点登录（SSO）身份认证、多因素身份认证等。

b) 建议实施强密码策略，如增加密码的复杂性、定期更新密码等。

c) 建议支持白名单认证机制，如IP地址白名单等。

7.4.2 API的安全导则

应用程序接口的安全导则包括以下内容：

a) 建议管理员能授权访问应用程序接口，例如能够配置用户可以访问应用程序接口的最多次数、应用程序接口可以支持的总连接数等。

b) 建议支持实时监控客户端和应用程序接口之间的网络流量特征，生成警报，并对异常网络流量做出事件响应。

c) 建议验证应用程序接口的输入，以防止各种安全攻击。

d) 建议支持通过安全通道传输重要数据，例如通过加密通道等。

e) 建议在传输数据之前，在客户端和应用程序接口之间双向执行检查和脱敏。

f) 建议支持数据完整性检查，并检测传输过程中的数据损坏或丢失。

7.5 安全管理的安全导则

安全管理的安全导则包括以下内容：

a) 建议使用身份和访问管理（IAM）和访问控制审计，内容包括操作和维护记录、数据访问日志、访问行为检查、密钥管理和数据加密。

b) 建议使用合理有效的检测和保护机制，包括基础设施的安全冗余、漏洞扫描、IPS/IDS、防火墙和虚拟化安全设备。

c) 建议使用安全强化技术，减少基础设施和平台的受攻击面。

d) 建议定期升级大数据基础设施和平台的补丁和版本。

参考书目

[b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

[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.1158] Recommendation ITU-T X.1158 (2014), *Multi-factor authentication mechanisms using a mobile device*.

[b-ITU-T X.1217] Recommendation ITU-T X.1217 (2021), *Guidelines for applying threat intelligence in telecommunication network operation*.

[b-ITU-T X.1245] Recommendation ITU-T X.1245 (2010), *Framework for countering spam in IP-based multimedia applications*.

[b-ITU-T X.1361] Recommendation ITU-T X.1361 (2018), *Security framework for the Internet of things based on the gateway model*.

[b-ITU-T X.1524] Recommendation ITU-T X.1524 (2012), *Common weakness enumeration*.

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

[b-ITU-T Y.2052] Recommendation ITU-T Y.2052 (2008), *Framework of multi-homing in IPv6-based NGN*.

[b-ITU-T Y.2201] Recommendation ITU-T Y.2201 (2009), *Requirements and capabilities for ITU-T NGN*.

[b-ITU-T Y.2244] Recommendation ITU-T Y.2244 (2019), *Service model for a cultivation plan service at the pre-production stage*.

[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 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 19944:2016, *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*.

ITU-T系列建议书

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
2022年，日内瓦