ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 25069—2022
代替 GB/T 25069—2010

信息安全技术　术语

Information security techniques—Terminology

2022-03-09 发布　　2022-10-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件代替GB/T 25069—2010《信息安全技术　术语》，与GB/T 25069—2010相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 在“术语和定义”中，引入了新的条目，更新了部分条目，删除了不常用条目，取消了原有分类（见第3章）；

b) 增加了“术语分类”，分为“密码机制类”“鉴别授权类”“计算安全类”“通信安全类”“应用安全类”“数据安全类”“安全服务类”“安全测评类”“安全管理类”九大类（见第4章）。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国信息安全标准化技术委员会（SAC/TC 260）提出并归口。

本文件起草单位：中电长城网际系统应用有限公司、中国电子技术标准化研究院、中国科学院软件研究所、四川大学、亚信科技（成都）有限公司、国家保密科技测评中心、微软（中国）有限公司、中电数据服务有限公司、华为技术有限公司、北京天融信网络安全技术有限公司、中国网络安全审查技术与认证中心、国家信息中心、蚂蚁科技集团股份有限公司、西安西电捷通无线网络通信股份有限公司、公安部第三研究所、上海三零卫士信息安全有限公司、中国软件评测中心、陕西省网络与信息安全测评中心、国家计算机网络应急技术处理协调中心、中国信息安全测评中心、清华大学、山东大学、国家密码管理局商用密码检测中心、北京信安世纪科技股份有限公司、北京小雷科技有限公司、成都卫士通信息产业股份有限公司、北京数字认证股份有限公司、飞天诚信科技股份有限公司、北京百度网讯科技有限公司、北京奇虎科技有限公司、西安丁度网络科技有限公司、北京赛西科技发展有限责任公司、北京泽创天成科技发展有限公司。

本文件主要起草人：闵京华、王惠莅、王姣、刘贤刚、上官晓丽、张立武、黄路曦、黄诚、庞勇、杨碧瑶、刘冬梅、周亚超、樊洞阳、葛小宇、庞婷、安高峰、程瑜琦、尤其、崔玉华、程浩、王昕、杜志强、陈长松、干露、郭永振、李怡、舒敏、石竑松、贾珂婷、孔凡玉、吕春梅、汪宗斌、柳增寿、张立廷、夏鲁宁、朱鹏飞、王海棠、吴月升、张屹、刘蓓、方勇、马卓元、赵德坤、黄寅。

本文件及其所代替文件的历次版本发布情况为：

——2010年首次发布为GB/T 25069—2010；

——本次为第一次修订。

引　言

信息安全技术术语是在信息安全领域进行技术交流的基础语言。统一规范术语和定义，有助于准确理解和表达技术内容，方便技术交流和研究。为此，本文件依据信息安全技术领域中已发布的国家标准和国际标准中的术语和定义，对基本或通用的信息安全技术术语和定义进行了规范。

本文件的术语和定义来源主要是全国信息安全标准化技术委员会(SAC/TC 260)归口管理并正式发布的国家标准和ISO/IEC JTC 1/SC 27负责制定并正式发布的国际标准。

信息安全技术　术语

1　范围

本文件界定了信息安全技术领域中基本或通用概念的术语和定义，并对其进行了分类。

本文件适用于对信息安全技术概念的理解、其他信息安全技术标准的制定以及信息安全技术的国内外交流。

2　规范性引用文件

本文件没有规范性引用文件。

3　术语和定义

3.1

安全　security

对某一系统，据以获得保密性、完整性、可用性、可核查性、真实性以及可靠性的性质。

[来源：ISO/IEC TR 15443-1：2012，3.21]

3.2

安全参数　security parameters

确定某一机制的安全强度的各个变量。

[来源：ISO/IEC 18370-2：2016，3.8]

3.3

安全策略　security policy

用于治理某一组织及其系统内管理、保护并分发影响安全及有关元素的资产（包括敏感信息）的一组规则、指导和实践。

3.4

安全大纲　security programming

〈工业控制〉在工业控制系统的安全建设中，为满足组织安全的需求和目标所采选的一系列安全控制举措。

[来源：GB/T 32919—2016，3.6，有修改]

3.5

安全多租户　secure multi-tenancy

采用安全控制措施来显式防范数据受损并对这些控制措施提供验证以便恰当治理的多租户类型。

注 1：当个人租户的风险状况不超过处于专用的单租户环境情形时，则是安全多租户。

注 2：在非常安全的环境中，甚至租户身份也是保密的。

[来源：ISO/IEC 27040：2015，3.39]

3.6

安全分级　security classification

根据业务信息和系统服务的重要性和受损后的影响，确定实施某种保护的等级。

3.7

安全服务　security service

根据安全策略，为用户提供某种安全功能及相关保障。

3.8

安全功能　security function

为实现安全要素的要求，并正确实施相应安全策略所提供的功能。

[来源：GB/T 20271—2006，3.1.6，有修改]

3.9

安全功能策略　security function policy；SFP

描述由评价对象安全功能（TSF）所实施的特定安全行为的规则集，可表达为安全功能要求（SFR）的集合。

[来源：GB/T 18336.1—2015，3.1.59，有修改：分别添加缩略语“TSF”“SFR”的中文全称“评价对象安全功能”“安全功能要求”等]

3.10

安全管理平台　security management platform

对信息系统的安全策略以及执行该策略的安全计算环境、安全区域边界和安全通信网络等方面的安全机制实施统一管理的系统。

[来源：GB/T 34990—2017，3.1，有修改：“平台”改为“系统”]

3.11

安全机制　security mechanism

实现安全功能，提供安全服务的基本方法。

3.12

安全集成电路　security integrated circuit

含有密码算法、安全功能，能实现密钥管理机制的集成电路。

[来源：GM/Z 4001—2013，2.3，有修改：“安全芯片　security chip”改为“安全集成电路　security integrated circuit”，“可实现”改为“能实现”]

3.13

安全计算环境　secure computing environment

在信息系统中，对信息进行存储、处理及实施安全策略的所有相关软硬件资源。

注：安全计算环境按照保护能力划分为一级～五级。

[来源：GB/T 34990—2017，3.9，有修改]

3.14

安全架构　security architecture

一种由多个相互协作的安全模块构成的体系结构。

[来源：GB/T 32927—2016，3.1.2，有修改]

3.15

安全控制　security controls

为保护某一系统及其信息的保密性、完整性和可用性以及可核查性、真实性、抗抵赖性、专有性和可靠性等，而对信息系统所选择并实施的管理、操作和技术等方面的控制（即防护或对抗）。

3.16

安全控制基线　security control baseline

安全控制选择过程的起始点和选择基点。

注：安全控制基线是为帮助组织选择满足安全需求的、最具成本效益的适当安全控制集而制定的最低安全基准线。

[来源:GB/T 36323—2018,3.5,有修改]

3.17

安全目标　security target;ST

对特定的已认定评价对象(TOE)的安全需求所做的依赖于实现的陈述。

[来源:GB/T 18366.1—2015,3.1.63,有修改:添加缩略语“TOE”的中文全称“评价对象”等]

3.18

安全目的　security objective

就对抗已认定的威胁和/或满足给定的组织安全策略和/或假设的意图所做的陈述。

[来源:GB/T 18336.1—2015,3.1.60,有修改]

3.19

安全评估　security assessment

按安全标准及相应方法,验证某一安全可交付件与适用标准的符合程度及其安全确保程度的过程。

注:安全评估通常是产品评价过程的最后阶段。

3.20

安全强度　security strength

与破译某一密码算法或系统所需工作量关联的数。

[来源:ISO/IEC 27040:2015,3.40]

3.21

安全区域边界　secure area boundary

对信息系统的安全计算环境边界,以及安全计算环境与安全通信网络之间实现连通并实施安全策略的相关部件。

注:安全区域边界按照保护能力划分为一级～五级。

[来源:GB/T 34990—2017,3.10,有修改]

3.22

安全权标　security token

一种与安全有关的数据集合,受到完整性和数据源鉴别的保护,以防其来源于非安全机构。

[来源:GB/T 17903.1—2008,3.5.3]

3.23

安全确保　security assurance

对声称业已或即将达到满足各项安全目的经论证的置信度的基础。

[来源:ISO/IEC TR 15443-1:2012,3.23]

3.24

安全审计　security audit

对信息系统记录与活动的独立评审和考察,以测试系统控制的充分程度,确保对于既定安全策略和运行规程的符合性,发现安全违规,并在控制、安全策略和过程三方面提出改进建议。

[来源:GB/T 5271.8—2001,08.01.05,有修改:“数据处理系统”改为“信息系统”,“审查和检查”改为“评审和考察”,“检测”改为“发现”等]

3.25

安全实现标准　security implementation standard

规定授权的安全实现方式的文档。

[来源:GB/T 29246—2017,2.81,有修改]

3.26

安全事态数据　security event data

与系统、服务或网络三方面安全状态有关的数据。

示例：在入侵检测系统中由传感器收集和管理的信息。

3.27

安全属性　security attribute

关于主体、用户(包括外部信息技术产品)、客体、信息、会话和/或资源，用于界定安全功能要求(SFR)，且其值用于实施 SFR 的性质。

[来源：GB/T 18336.1—2015，3.1.58，有修改："IT"改为"信息技术"，添加缩略语"SFR"的中文全称"安全功能要求"等]

3.28

安全套接层　secure sockets layer；SSL

一种处于网络层与应用层之间，为客户端和服务器的鉴别及保密性和完整性提供服务的协议。

3.29

安全通信网络　secure communication network

在信息系统安全计算环境之间传输信息并实施安全策略的各种设施。

注：安全通信网络按照保护能力划分一级～五级。

[来源：GB/T 34990—2017，3.11，有修改]

3.30

安全网关　security gateway

在网络或各子网之间，或在不同安全域内的软件应用之间，一种旨在按照给定的安全策略来保护网络的连接点。

[来源：GB/T 25068.1—2020，3.36]

3.31

安全问题　security problem

对界定评价对象(TOE)拟处置安全的性质和范围所做的正式陈述。

注：该陈述由下列 3 项的某种组合构成：

——有待 TOE 及其运行环境对抗的威胁；

——由 TOE 及其运行环境实施的组织安全策略(OSP)；

——确认 TOE 运行环境的假设。

[来源：GB/T 18336.1—2015，3.1.61，有修改：添加缩略语"TOE"的中文全称"评价对象"等]

3.32

安全信道　secure channel

为所交换消息提供保密性及真实性的通信信道。

[来源：ISO/IEC 24745：2011，2.30]

3.33

安全信息对象　security information object

安全信息对象类的实例。

[来源：ISO/IEC 15816：2002，3.9]

3.34

安全信息对象类　security information object class

一种针对安全使用已经做了剪裁的信息对象类。

[来源：ISO/IEC 15816：2002，3.10]

3.35

安全许可　security clearance

授予某一个体访问某一特定安全级别或低于该级别的数据或信息的许可。

[来源:GB/T 5271.8—2001,08.01.19,有修改]

3.36

安全域　security domain

遵从共同安全策略的资产和资源的集合。

[来源:GB/T 25068.1—2020,3.35]

3.37

安全主机　security host

可由内部网和外部网访问,通常构成网络接入主节点,并予以充分保护的计算机。

3.38

八位(位)组　octet

八位字节　8-bit byte

一种由八个二进制位组成的字节。

[来源:GB/T 5271.1—2000,01.02.10,有修改:"位"改为"二进制位"]

3.39

八位(位)组串　octet string

八位字节串　8-bit byte string

由八位(位)组所组成的序列。

注:适当时,只需将各八位(位)组中的位全部拼接在一起,就能将八位(位)组串解释为位串。

3.40

保护轮廓　protection profile;PP

对某一评价对象(TOE)类型的安全需求所做的独立于实现的陈述。

[来源:GB/T 18336.1—2015,3.1.51,有修改:添加缩略语"TOE"的中文全称"评价对象"等]

3.41

保密性　confidentiality

信息对未授权的个人、实体或过程不可用或不泄露的性质。

[来源:GB/T 29246—2017,2.12,有修改:"特征"改为"性质"]

3.42

保全　preservation

维护并保护潜在数字证据的完整性和/或原始状态的过程。

[来源:ISO/IEC 27037:2012,3.15]

3.43

暴露　exposure

特定的攻击利用数据处理系统特定的脆弱性的可能性。

[来源:GB/T 5271.8—2001,08.05.13,有修改:删除注]

3.44

备份文件　backup files

一种用于日后数据恢复所制备的文件。

示例:在备用场所保留的文件副本。

[来源:GB/T 5271.8—2001,08.07.05,有修改]

3.45

比较计分　comparison score

从比较得来的数值(或数值集合)。

[来源:ISO/IEC 24761:2009,3.20]

3.46

比较判定　comparison decision

基于比较计分、判定策略(包括阈值)以及可能有的其他输入,来确定识别生物特征测定样本和生物特征测定基准是否具有同一生物特征测定源的过程。

注 1:匹配是一种肯定性比较判定。

注 2:非匹配是一种否定性比较判定。

注 3:有时会给出"未确定"的判定。

[来源:ISO/IEC 19792:2009,4.3.10,有修改:删除原注 1]

3.47

标识　identification

赋予某一实体唯性标识符的过程。

[来源:GB/T 33745—2017,2.4.1]

3.48

标识符　identifier

在数据组织中,一种用于标识某一数据元素或为其命名,并可能指明其某些性质的一个或多个字符。

[来源:GB/T 33745—2017,2.4.2]

3.49

标识数据　identification data

分配给某一实体,用于对其标识的数据元素序列(包括实体的可区分性标识符)。

注:标识数据能追加数据元素,诸如,签名过程标识符、签名密钥标识符、签名密钥有效期、对密钥用法的限制、关联的安全策略参数、密钥序号或域参数等。

[来源:ISO/IEC 29150:2011,3.20]

3.50

病毒　virus

一种程序,即通过修改其他程序,使其他程序包含一个自身可能已发生变化的原程序副本,从而完成传播自身程序,当调用受传染的程序,该程序即被执行。

注:病毒经常造成某种损失或困扰,并可能被某一事件(诸如出现的某一预定日期)触发。

[来源:GB/T 5271.8—2001,08.05.47,有修改:"可以"改为"可能"]

3.51

补充校验字符　supplementary check character

不属于受保护的字符集的校验字符。

[来源:GB/T 17710—2008,2.3]

3.52

补救　remediation

为移除或减缓脆弱性而对产品或服务进行的修订。

注：补救通常采取二进制文件替换、配置更改或源代码补丁和重新编译的形式。用于“补救”的不同术语包括补丁、修复、更新、热修复和升级。缓解措施又称“解决办法”或“对策”。

[来源：ISO/IEC 29147：2018，3.7]

3.53

不符合　nonconformity

对要求的不满足。

[来源：GB/T 29246—2017，2.53]

3.54

不可恢复部分　non-recoverable part

消息中随签名一起存储或传送的部分；当对消息进行全部恢复时，此部分为空。

[来源：ISO/IEC 9796-2：2010，3.11]

3.55

不可逆加密　irreversible encryption；irreversible encipherment

单向加密　one-way encryption

一种只产生密文，而不能将密文再生为原始数据的加密方式。

注：不可逆加密用于鉴别。例如，口令可能被不可逆地加密并存储产生的密文。对以后出示的口令同样进行不可逆的加密，然后比较两串密文。当两者相同时，后出示的口令是正确的。

[来源：GB/T 5271.8—2001，08.03.03，有修改]

3.56

残余脆弱性　residual vulnerability

在评价对象（TOE）运行环境中，不能被利用，但能被攻击潜力大于预期的攻击者用于违反安全功能要求（SFR）的弱点。

[来源：GB/T 18336.1—2015，3.5.6，有修改：分别添加缩略语“TOE”“SFR”的中文全称“评价对象”“安全功能要求”等]

3.57

残余风险　residual risk

风险处置后余下的风险。

注 1：残余风险可能包含未识别的风险。

注 2：残余风险又可称“保留风险”。

[来源：GB/T 29246—2017，2.64，有修改：“可以”改为“可”等]

3.58

测度　measure

作为测量结果赋值的变量。

[来源：GB/T 29246—2017，2.47，有修改：删除注]

3.59

测量　measurement

确定一个值的过程。

[来源：GB/T 29246—2017，2.48，有修改：删除注]

3.60

测量单位　unit of measurement

按惯例被定义和被采纳的特定量，用于其他同类量与其比较，以表示它们相对于这个量的大小。

[来源：GB/T 29246—2017，2.86]

3.61

测量方法　measurement method

用于按规定的尺度量化属性的，一般描述的操作规程。

注：测量方法的类型取决于属性量化操作的性质。可区分为以下两种类型：

——主观的：涉及人为判断的量化；

——客观的：基于数字规则的量化。

[来源：GB/T 29246—2017，2.50，有修改："通用逻辑操作序列"改为"一般描述的操作规程"]

3.62

测量函数　measurement function

组合两个或两个以上基本测度的算法。

[来源：GB/T 29246—2017，2.49，有修改：删除"或计算"]

3.63

测量结果　measurement results

对信息需要的一个或多个指标及其相关解释。

[来源：GB/T 29246—2017，2.51]

3.64

测量形式　form of measurement

确定测量值的一组运算，或是一种测量方法、计算函数或分析模型。

3.65

测试　testing

使评估对象按预定方法/工具产生特定行为，以获取证据来证明其安全确保措施是否有效的过程。

[来源：GB/T 30273—2013，3.12，有修改]

3.66

策略〈访问控制〉　policy〈access control〉

实施访问控制决策所遵循的一组规则、一种规则组合算法标识和(可选的)一组义务。

[来源：GB/T 30281—2013，3.11，有修改：增加语境标识〈访问控制〉等]

3.67

策略〈组织管理〉　policy〈organization management〉

由其最高管理层正式表达的组织的意图和方向。

[来源：GB/T 29246—2017，2.60，有修改：增加语境标识〈组织管理〉等]

3.68

策略映射　policy mapping

当某个域中某一证书认证机构(CA)认证另一域中一个 CA 时，前一域中 CA 将后一域中特定证书策略进行转换，使之等价(但不必完全相同)于前一域中特定证书策略的运算。

3.69

插空攻击　interleaving attack

利用从一个或多个正在或此前进行的鉴别交换过程中导出的信息进行的冒充攻击手段。

[来源：GB/T 15843.1—2017，3.15，有修改]

3.70

差分功耗分析　differential power analysis

为获取密码操作有关的信息而对密码模块的功耗变化进行的分析。

[来源：GB/T 37092—2018，3.8，有修改]

3.71

差分密码分析　differential cryptanalysis

为获得可能性最大的密钥，通过分析特定明文差分对相应密文差分的影响的采用选择明文攻击分析特定明文差分对相应密文差分的影响。

[来源：GM/Z 4001—2013，2.4，有修改]

3.72

差分增量备份　differential incremental backup

备份自上次完全备份或增量备份后更改过的数据对象。

注：使用差分增量备份恢复数据时，需要最新的完全备份和自最新完全备份后的所有差分增量备份。

[来源：GB/T 29765—2013，3.14]

3.73

拆分知识　split knowledge

将密码密钥拆分成多个密钥组件的如下过程：各单个组件并不共享原始密钥的知识，而能由分开的实体随后将其输入密码模块或从密码模块输出，经组合来重新创建原始密码密钥。

注：能请求组件的全部或其某一子集来完成此种组合。

[来源：ISO/IEC 19790：2015，3.120]

3.74

产品　product

从某一过程得到的结果。

[来源：ISO/IEC 27034-1：2011，3.19]

3.75

持续改进　continual improvement

为提高性能而反复进行的活动。

[来源：GB/T 29246—2017，2.15，有修改]

3.76

持有者　holder

由源授权机构直接授权或由其他属性授权机构间接授权的实体。

[来源：GB/T 16264.8—2005，3.3.31，有修改]

3.77

尺度　scale

连续的或离散的值的有序集合，或者对应属性的类集合。

注：尺度的类型取决于尺度上值之间关系的性质。通常定义如下4种尺度类型：

——名义的：测量值是类别化的；

——顺序的：测量值是序列化的；

——间距的：测量值对应于属性的等同量是等距离的；

——比率的：测量值对应于属性的等同量是等距离的，其中零值对应于属性的空。

这些只是尺度类型的示例。

[来源：GB/T 29246—2017，2.80]

3.78

重放攻击　replay attack

攻击者通过记录通信会话，以便日后某个时刻重放整个或部分会话的主动攻击方式。

3.79

抽象语法记法1　abstract syntax notation one；ASN.1

一种用来组织复杂数据的抽象符号体系。

3.80

初始化向量　initialization vector

初始化值　initialization value

在密码变换中，为增加安全性或使密码设备同步而引入的用于数据变换的起始数据。

[来源：GM/Z 4001—2013，2.7]

3.81

传感器　sensor

依照一定的规则，对物理世界中的客观现象、物理属性进行监测，并将监测结果转化为可以进一步处理的信号的设备。

注 1：信号可以为电子的、化学的或者其他形式的传感器响应。

注 2：信号可以表示为 1 维、2 维、3 维或更高维度的数据。

[来源：GB/T 30269.2—2013，2.1.2]

3.82

传输层安全协议　transport layer security protocol；TLSP

一种作为安全套接层协议后继的正式互联网协议。

3.83

传输层密码协议　transport layer cryptographic protocol；TLCP

一种应用于传输层，用于构建客户端和服务端之间安全通道的安全协议。

3.84

传输抗抵赖　non-repudiation of transport

旨在为消息原发者提供证据，证明某一交付机构已将消息交付给预期接收者的行为。

[来源：GB/T 17903.1—2008，3.9.20，有修改："服务"改为"行为"]

3.85

传输抗抵赖权标　non-repudiation of transport token

允许原发者或交付机构能为某一消息建立传输抗抵赖的数据项。

[来源：GB/T 17903.1—2008，3.9.28，有修改]

3.86

传输延迟　transmission delay

数据从一方传送到另一方所需的时间。

[来源：GB/T 28457—2012，3.13，有修改]

3.87

创建抗抵赖　non-repudiation of creation

旨在防止某一实体不实地否认其已创建消息内容（即对消息的内容负责）的服务。

[来源：GB/T 17903.1—2008，3.9.13，有修改]

3.88

篡改检测　tamper detection

由密码模块自动确定已经做出破坏本模块安全性的尝试的动作。

[来源：ISO/IEC 19790：2015，3.125]

3.89

篡改响应　tamper response

篡改检测已经发生时，由密码模块采取的自动动作。

[来源：ISO/IEC 19790：2015，3.127]

3.90

篡改证据　tamper evidence

试图破坏密码模块安全性的可见迹象。

[来源:ISO/IEC 19790:2015,3.126]

3.91

脆弱性　vulnerability

可能被一个或多个威胁利用的资产或控制的弱点。

[来源:GB/T 29246—2017,2.89]

3.92

存储　storage

数据在存储器中的保存。

[来源:GB/T 5271.12—2000,12.02.04]

3.93

存储库　repository

存储证书和证书撤销列表等信息,并提供相应信息检索服务的数据库。

注:通常情况下,所检索的信息无需验证。

3.94

存储媒体　storage media

承载电子数据的物理实体,包括但不限于计算机硬盘、磁带、软盘、光盘、各种形式的存储卡等。

[来源:GB/T 31500—2015,3.2,有修改:术语中文名称“存储介质”改为“存储媒体”,“各类载体或设备”改为“物理实体”]

3.95

存储区域网络　storage area network;SAN

在服务器和存储设备之间以及存储设备之间,以数据传输为主要目的的网络。

注:SAN 由提供物理连接的通信基础设施以及将连接、存储设备和计算机系统组织起来的管理层组成,以便数据传输安全可靠。

[来源:ISO/IEC 27040:2015,3.44,有修改:添加“存储区域网络”的缩略语“SAN”]

3.96

搭进　piggyback entry

凭借授权用户的合法连接而对数据处理系统进行未经授权的访问。

[来源:GB/T 5271.8—2001,08.05.30,有修改]

3.97

大数据　big data

具有体量巨大、来源多样、生成极快、且多变等特征并且难以用传统数据体系结构有效处理的包含大量数据集的数据。

注:国际上,大数据的 4 个特征普遍不加修饰地直接用 volume、variety、velocity 和 variability 予以表述,并分别赋予了它们在大数据语境下的定义。

a) 体量(volume):构成大数据的数据集的规模。

b) 多样性(variety):数据可能来自多个数据仓库、数据领域或多种数据类型。

c) 速度(velocity):单位时间的数据流量。

d) 多变性(variability):大数据其他特征,即体量、数据和多样性等特征都处于多变状态。

[来源:GB/T 35295—2017,2.1.1]

3.98

大数据参考架构　big data reference architecture

一种用作工具以便于对大数据内在的要求、设计结构和运行进行开放性探讨的高层概念模型。

[来源:GB/T 35295—2017,2.1.3,有修改:“参考体系结构”改为“参考架构”]

3.99

大数据服务　big data service

基于大数据参考架构提供的数据服务。

[来源:GB/T 35295—2017,2.1.15,有修改:“参考体系结构”改为“参考架构”]

3.100

大数据服务提供者　big data service provider

通过大数据平台和应用,提供大数据服务的机构。

[来源:GB/T 35274—2017,3.7]

3.101

大数据平台　big data platform

采用分布式存储和计算技术,提供大数据的访问和处理,支持大数据应用安全高效运行的软硬件集合,包括监视大数据的存储、输入/输出、操作控制等大数据服务软硬件基础设施。

[来源:GB/T 35274—2017,3.6]

3.102

大数据使用者　big data user

使用大数据平台或应用的末端用户、其他信息技术系统或智能感知设备。

[来源:GB/T 35274—2017,3.8,有修改:“big data consumer”改为“big data user”]

3.103

大数据系统　big data system

实现大数据参考架构的全部或部分功能的系统。

[来源:GB/T 35295—2017,2.1.14,有修改:“参考体系结构”改为“参考架构”]

3.104

大数据应用　big data application

执行数据生存周期相关的数据采集、数据传输、数据存储、数据处理(如计算、分析、可视化等)、数据交换、数据销毁等数据活动,运行在大数据平台,并提供大数据服务的应用系统。

[来源:GB/T 35274—2017,3.5,有修改:“生命周期”改为“生存周期”]

3.105

带外　out-of-band

在事先建立的通信方法或信道之外发生的通信或传输。

[来源:ISO/IEC 27040:2015,3.31]

3.106

担保　warranty

当可交付件的操作(部署、执行或交付)不满足其安全策略时,一种对其纠正或减轻影响的安全服务。

3.107

单边鉴别　unilateral authentication

两个实体之间仅一方向另一方而不反向提供身份保证的实体鉴别。

[来源:GB/T 15843.1—2017,3.39,有修改:“单向鉴别”改为“单边鉴别”等]

3.108

单边匿名鉴别　unilateral anonymous authentication

两个实体之间仅一方向另一方而不反向提供身份保证的匿名鉴别。

[来源:GB/T 34953.1—2017,2.20,有修改:“单向匿名鉴别”改为“单边匿名鉴别”等]

3.109

单边匿名互鉴别　unilateral-anonymous mutual authentication

在两个实体之间,一方对另一方进行匿名实体鉴别,同时另一方对前者进行实体鉴别的过程。

[来源:GB/T 34953.1—2017,2.21,有修改:“单向匿名双向鉴别”改为“单边匿名互鉴别”]

3.110

单点登录　single sign on;SSO

用户一次性进行身份鉴别之后就能够访问多个授权应用的登录机制。

[来源:GM/Z 4001—2013,2.9]

3.111

单点故障　single point of failure

系统中的某一元件或组件、系统中的某一通路或者某一系统本身的故障,该故障导致整个系统或一系列系统都将无法执行其基本功能。

注:单点故障通常被认为是与关键元件相关的设计缺陷。

[来源:ISO/IEC 27040:2015,3.42]

3.112

单向函数　one-way function

具有如下性质的函数:易于计算出给定输入的输出,但找到映射到给定输出的输入在计算上不可行。

[来源:ISO/IEC 11770-3:2015,3.30]

3.113

导出测度　derived measure

定义为两个或两个以上基本测度值的函数的测度。

[来源:GB/T 29246—2017,2.22]

3.114

登记　enrolment

使某一实体在某一特定域中为人所知的过程。

注:登记过程通常包括收集和确认身份信息以识别某一实体并收集身份注册所需的身份信息;然后是身份注册本身。

[来源:ISO/IEC 24760-1:2019,3.4.3]

3.115

抵赖　repudiation

当事实体之一对已经参与全部或部分行动的否认。

[来源:ISO/IEC 29115:2013,3.23]

3.116

第三方　third party

就所涉及的问题而言,公认与相关各方均独立的个人或团体。

3.117

第三方评估　third party assessment

由信息系统所有者委托商业评估机构或其他评估机构，依据国家有关法规与标准，对信息系统安全管理进行的评估活动。

[来源：GB/T 28453—2012，3.4]

3.118

电码本工作模式　electronic codebook operation mode；ECB

在分组密码算法中，直接将明文分组作为算法的输入，对应的输出作为密文分组的工作模式。

[来源：GM/Z 4001—2013，2.10，有修改]

3.119

电子签名　electronic signature

数据电文中以电子形式所含、所附用于识别签名人身份并表明签名人认可其中内容的数据。

[来源：GB/T 35288—2017，3.2]

3.120

电子签章　electronic seal signature

使用电子印章签署电子文件的过程。

[来源：GM/Z 4001—2013，2.11，有修改："digitally seal"改为"electronic seal signature"]

3.121

电子印章　electronic seal

一种经制作者签名，包括持有者信息和图形化内容，可用于签署电子文件的数据。

[来源：GM/Z 4001—2013，2.12，有修改："digital stamp"改为"electronic seal"等]

3.122

电子印章系统　electronic seal system

由电子印章管理系统和电子签章软件两部分组成的系统。

注 1：电子印章管理系统具有印章管理员管理、电子印章制作与管理、电子印章验证服务以及安全审计等功能。

注 2：电子签章软件是一种利用电子印章对各类电子文档进行签署的软件。

[来源：GM/T 0031—2014，3.4，有修改]

3.123

顶级域　top level domain

域名系统名字空间中根节点下最顶层的域。

[来源：GB/T 33562—2017，3.5，有修改：删除顶级域分类和举例]

3.124

订户　subscriber

从电子认证服务机构接收证书的实体。

[来源：GB/T 35288—2017，3.7]

3.125

订户协议　subscriber agreement

电子认证服务机构与订户共同签署，规定了双方在证书使用和管理过程中各自承担的责任和义务的文件。

[来源：GB/T 31508—2015，3.15，有修改："协议"改为"文件"等]

3.126

定时炸弹　time bomb

在预定时间被激活的逻辑炸弹。

[来源:GB/T 5271.8—2001,08.05.52]

3.127

动态口令 dynamic password

基于时间、事件等方式随机生成的一次性口令。

[来源:GM/Z 4001—2013,2.15,有修改:删除“one-time-password (OTP)”,“动态”改为“随机”]

3.128

动态口令令牌 dynamic password token

生成并显示动态口令的媒体。

[来源:GM/Z 4001—2013,2.16,有修改:“one-time-password token”改为“dynamic password token”]

3.129

度量 metric

为完成对一个或多个属性的测量而界定的测量形式(测量方法、计算函数或分析模型)和尺度。

3.130

端口 port

连接的端点。

注:在互联网协议的语境下,端口是传输控制协议(TCP)连接或用户数据报协议(UDP)消息的逻辑信道端点。基于 TCP 或 UDP 的应用协议,通常已分配默认端口号,如为超文本传输协议(HTTP)的端口号是 80。

[来源:GB/T 25068.1—2020,3.31,有修改:调换缩略语和其中文全称的位置]

3.131

断言 assertion

验证方所作出的不包含有效证据的声明。

[来源:GB/T 36633—2018,3.8]

3.132

对称加密系统 symmetric encryption system

基于对称密码技术,加密和解密采用同一秘密密钥的系统。

[来源:GB/T 36624—2018,3.9,有修改]

3.133

对称密码技术 symmetric cryptographic technique

加密和解密变换采用同一密钥的密码技术。

3.134

对称密码算法 symmetric cryptographic algorithm

加密和解密采用同一密钥的密码算法。

[来源:GB/T 37033.1—2018,3.2,有修改]

3.135

对称密钥 symmetric key

对称密码算法的密钥。

[来源:GM/Z 4001—2013,2.20,有修改]

3.136

对象〈计算机安全〉 object〈computer security〉

客体〈计算机安全〉

一种实体,对该实体的访问是受控。

示例:文件、程序、主存区域;收集和维护的有关个人的数据。

[来源:GB/T 5271.8—2001,08.01.31,有修改:添加同义术语中文“对象〈计算机安全〉”等]

3.137

对象〈人工智能〉 object〈in artificial intelligence〉

客体〈人工智能〉

具有一种或多种属性的物理或概念实体。

注:对象一般借助符号推理或关系与其他存储对象相关联。

[来源:GB/T 5271.28—2001,28.02.06,有修改:添加同义术语中文“对象〈用于人工智能〉”等]

3.138

对象标识符 object identifier;OID

客体标识符

用于无歧义地标识对象的全局唯一值。

[来源:GB/T 37695—2019,3.1,有修改:添加“对象标识符”的缩略语“OID”,删除注]

3.139

多因素鉴别 multi-factor authentication

采用以下两个或多个因素的鉴别:

——知晓因素,“个人知道的”;

——拥有因素,“个人持有的”;

——生物因素,“个人是什么或能够做什么的”。

[来源:ISO/IEC 27040:2015,3.27]

3.140

多用途互联网邮件扩展 multipurpose internet mail extensions;MIME

一种利用电子邮件提供安全传送文件手段的适用性协议。

3.141

恶意软件 malware

被专门设计用于损坏或中断系统、破坏保密性、完整性和/或可用性的软件。

注:病毒和特洛伊木马都是恶意软件。

[来源:GB/T 25068.1—2020,3.22]

3.142

二元序列 binary sequence

由“0”和“1”组成的位串。

[来源:GB/T 32915—2016,2.1,有修改:“比特”改为“位”]

3.143

发起方 initiator

按某一协议运行时发送首轮交换信息的用户。

[来源:GB/T 32918.3—2016,3.3,有修改]

3.144

发送抗抵赖 non-repudiation of sending

旨在防范发送者不实否认其已经发送某一消息的服务。

[来源:GB/T 17903.1—2008,3.9.18,有修改]

3.145

反射攻击 reflection attack

将以前传输的消息发回给其原发者的一种冒充攻击手段。

[来源:GB/T 15843.1—2017,3.30]

3.146

防火墙　firewall

设置在网络环境之间的一种安全屏障,它由一台专用设备或若干组件和技术的组合组成,网络环境之间两个方向的所有通信流均通过此屏障,并且只有按照本地安全策略定义的、已授权的通信流才允许通过。

[来源:GB/T 25068.1—2020,3.12]

3.147

访问控制　access control

一种确保数据处理系统的资源只能由经授权实体以授权方式进行访问的手段。

[来源:GB/T 5271.8—2001,08.04.01,有修改]

3.148

访问控制(列)表　access control list;ACL

由实体以及实体对资源的访问权限所组成的列表。

[来源:GB/T 5271.8—2001,08.04.02,有修改:添加“访问控制(列)表”的缩略语“ACL”,删除“访问(列)表　access list”等]

3.149

非对称加密系统　asymmetric encryption system

基于非对称密码技术的系统,其公开变换用于加密,而私有变换用于解密。

[来源:GB/T 15843.1—2017,3.2]

3.150

非对称密码算法　asymmetric cryptographic algorithm

公钥密码算法　public key cryptographic algorithm

加密和解密使用不同密钥的密码算法。其中一个密钥(公钥)可公开,另一个密钥(私钥)必须保密,且由公钥求解私钥是计算不可行的。

[来源:GB/T 37033.1—2018,3.3,有修改:“可以”改为“可”]

3.151

非对称密钥对　asymmetric key pair

非对称密码算法中相关联的公钥和私钥。

[来源:GM/Z 4001—2013,2.24]

3.152

非对称签名系统　asymmetric signature system

在基于非对称密码技术中,私有变换用于签名,公开变换用于验证的系统。

[来源:GB/T 15843.1—2017,3.4,有修改]

3.153

非法控制　illegal control

使系统或网络按非法控制者的意愿运行的行为。

[来源:GB/T 31495.2—2015,3.13,有修改:删除“违反规范”,“行动”改为“行为”]

3.154

非军事区　demilitarized zone;DMZ

屏蔽子网

介于网络之间作为“中立区”的边界网络。

[来源:GB/T 25068.1—2020,3.8,有修改]

3.155

非入侵式攻击　non-invasive attack

一种针对密码模块,对其边界内的组件不直接物理接触,也不更改其状态的攻击。

[来源:GM/T 0028—2014,3.55,有修改]

3.156

非易失性存储　non-volatile storage

断开电源后仍保有其内容的存储。

[来源:ISO/IEC 27040:2015,3.30]

3.157

分布式拒绝服务攻击　distributed denial-of-service attack;DDoS

通过洪水攻击带宽或目标系统的资源,破坏多个系统的方式来未授权访问系统资源或者延迟系统操作和功能,导致经授权用户失去可用性。

[来源:GB/T 28454—2020,3.7,有修改:“授权用户”改为“经授权用户”等]

3.158

分布式控制系统　distributed control system;DCS

以计算机为基础,在系统/单位内部对生产过程进行分布控制、集中管理的系统。

注:DCS 系统一般包括现场控制和控制管理两级,前者主要是对单个子过程进行控制,后者主要是对多个分散的子过程进行数据采集、集中显示、统一调度和管理。

[来源:GB/T 36323—2018,3.2,有修改]

3.159

分析攻击　analytical attack

密码分析攻击　crytanalytical attack

运用分析方法解开代码或找到密钥的企图。

[来源:GB/T 5271.8—2001,08.05.20,有修改:删除例和注]

3.160

分析模型　analytical model

将一个或多个基本测度和/或导出测度关联到决策准则的算法或计算。

[来源:GB/T 29246—2017,2.2,有修改]

3.161

分组密码　block cipher

加密算法在明文分组(即界定了长度的位串)上运算,以此产生密文分组的对称加密系统。

[来源:ISO/IEC 10116:2017,3.1]

3.162

分组密码算法　block cipher algorithm

将输入数据划分成固定长度的分组来加解密的对称密码算法。

[来源:GM/Z 4001—2013,2.25,有修改]

3.163

分组密码算法工作模式　block cipher algorithm operation mode

采用分组密码算法的如下主要工作模式:电码本(ECB)、密文分组链接(CBC)、密文反馈(CFB)、输出反馈(OFB)、计数器(CTR)等。

[来源：GM/Z 4001—2013，2.26，有修改："block cipher operation mode"改为"block cipher algorithm operation mode"]

3.164

风险　risk

对目标的不确定性影响。

注 1：影响是指与期望的偏离(正向的或反向的)。

注 2：不确定性是对事态及其结果或可能性的相关信息、理解或知识缺乏的状态(即使是部分的)。

注 3：风险常被表征为潜在的事态和后果，或者它们的组合。

注 4：风险常被表示为事态的后果(包括情形的改变)和其发生可能性的组合。

注 5：在信息安全管理体系的语境下，信息安全风险可被表示为对信息安全目标的不确定性影响。

注 6：信息安全风险与威胁利用信息资产或信息资产组的脆弱性对组织造成危害的潜力相关。

[来源：GB/T 29246—2017，2.68]

3.165

风险处置　risk treatment

改变风险的过程。

注 1：风险处置可能涉及如下方面：

——通过决定不启动或不继续进行引发风险的活动来规避风险；

——承担或增加风险以追求机会；

——消除风险源；

——改变可能性；

——改变后果；

——与另一方或多方共担风险(包括合同和风险融资)；

——有根据地选择保留风险。

注 2：处理负面后果的风险处置有时称为"风险缓解""风险消除""风险防范""风险降低"。

注 3：风险处置可能产生新的风险或改变现有风险。

[来源：GB/T 29246—2017，2.79，有修改："产生风险"改为"引发风险"]

3.166

风险分析　risk analysis

理解风险本质和确定风险级别的过程。

注 1：风险分析提供风险评价和风险处置决策的基础。

注 2：风险分析包括风险估算。

[来源：GB/T 29246—2017，2.70，有修改："风险等级"改为"风险级别"]

3.167

风险沟通与咨询　risk communication and consultation

组织就风险管理所进行的，提供、共享或获取信息以及与利益相关方对话的持续和迭代过程。

注 1：这些信息可能涉及风险的存在、性质、形式、可能性、重要性、评价、可接受性和处理。

注 2：咨询是对问题进行决策或确定方向之前，在组织和其利益相关方之间进行知情沟通的双向过程。

咨询是：

——通过影响力而不是权力来影响决策的过程；

——决策的输入，而非联合决策。

[来源：GB/T 29246—2017，2.72]

3.168

风险管理　risk management

指导和控制组织相关风险的协调活动。

[来源：GB/T 29246—2017，2.76]

3.169

风险管理过程　risk management process

管理策略、规程和实践在沟通、咨询、语境建立以及识别、分析、评价、处理、监视和评审风险活动上的系统性应用。

注：GB/T 31722 使用术语“过程”来描述全面风险管理。风险管理过程中的要素称为“活动”。

[来源：GB/T 29246—2017，2.77，有修改：“ISO/IEC 27005”改为“GB/T 31722”等]

3.170

风险规避　risk avoidance

不卷入风险处境的决定或撤离风险处境的行动。

[来源：GB/T 33132—2016，3.2]

3.171

风险级别　level of risk

以后果和其可能性的组合来表示的风险大小。

[来源：GB/T 29246—2017，2.44，有修改：“风险程度”改为“风险级别”]

3.172

风险降低　risk reduction

为降低风险的可能性和/或负面结果所采取的行动。

[来源：GB/T 33132—2016，3.4，有修改]

3.173

风险接受　risk acceptance

承担特定风险的知情决定。

注 1：可不经风险处置或在风险处置过程中做出风险接受。

注 2：接受的风险要受到监视和评审。

[来源：GB/T 29246—2017，2.69]

3.174

风险评估　risk assessment

风险识别、风险分析和风险评价的整个过程。

[来源：GB/T 29246—2017，2.71]

3.175

风险评价　risk evaluation

将风险分析的结果与风险准则比较，以确定风险和/或其大小是否可接受或可容忍的过程。

注：风险评价辅助风险处置的决策。

[来源：GB/T 29246—2017，2.74，有修改]

3.176

风险识别　risk identification

发现、识别和描述风险的过程。

注 1：风险识别涉及风险源、事态及其原因和潜在后果的识别。

注 2：风险识别可能涉及历史数据、理论分析、知情者和专家的意见以及利益相关方的需要。

[来源：GB/T 29246—2017，2.75]

3.177

风险责任者　risk owner

具有责任和权威来管理风险的个人或实体。

[来源：GB/T 29246—2017，2.78，有修改]

3.178

风险转移　risk transfer

与另一方对风险带来的损失或收益的共享。

注：在信息安全风险的语境下，对于风险转移仅考虑负面结果(损失)。

[来源：GB/T 31722—2015，3.9]

3.179

风险准则　risk criteria

评价风险重要性的基准。

注 1：风险准则是基于组织的目标以及外部语境和内部语境。

注 2：风险准则可源自标准、法律、策略和其他要求。

[来源：GB/T 29246—2017，2.73，有修改："参照条款"改为"基准"等]

3.180

封闭安全环境　closed-security environment

以授权、安全许可、配置控制等形式，特别关注于保护数据和资源，使其免受偶然或恶性操作的环境。

[来源：GB/T 5271.8—2001，08.01.21，有修改]

3.181

服务　service

给定层及其以下各层为其高一层的实体提供的能力。

注：对给定层的服务，在该层与其高一层之间的边界处提供。

[来源：GB/T 5271.18—2008，18.01.11，有修改：删除注 2]

3.182

服务变更　service change

任何可能对服务产生影响的新增、修改或解除的活动。

注：服务变更可能涉及服务的范围、人员、内容、形式、价格、时间、方案、流程、工具、服务级别等。

[来源：GB/T 32914—2016，3.13]

3.183

服务方案　service plan

基于服务目标，对服务各阶段中所需执行的过程、任务、活动以及相关服务要素、服务级别进行详细描述的文档。

[来源：GB/T 32914—2016，3.11，有修改："service plans"改为"service plan"]

3.184

服务工具　service tool

为达成服务目标或提高服务质量和效率所需要的设备、软件、模板、知识库等。

[来源：GB/T 32914—2016，3.12，有修改："service tools"改为"service tool"]

3.185

服务级别　service level

在服务协议中对服务交付成果明确约定，可测量和文档化的一系列服务差异化指标。

[来源：GB/T 32914—2016，3.5，有修改："服务指标"改为"服务差异化指标"]

3.186

服务级别协议　service level agreement；SLA

规定技术支持或业务性能目标的文件，包括服务提供方能为其客户提供保证性能和承担失败后果的措施。

[来源:GB/T 28454—2020,3.27,有修改:“合同”改为“文件”,“测量”改为“措施”等]

3.187

服务目录 service catalogue

在服务协议中明确展示服务内容、服务形式、服务价格、服务交付成果和服务级别等的列表。

[来源:GB/T 32914—2016,3.6,有修改:删除“一份”]

3.188

服务器 server

在计算机网络中的,一种为工作站、微型计算机或为其他功能单元提供服务的功能单元。

示例:文件服务器,打印服务器,邮件服务器。

注:服务可为专用的或共享的。

[来源:GB/T 5271.18—2008,18.02.15,有修改:“个人计算机”改为“微型计算机”、删除注 2 等]

3.189

服务协议 service agreement

服务需求方和服务提供方在服务开始前共同签署,在服务过程中共同遵守的约定。

注:通常包含服务原则、服务形式、服务级别、服务价格、服务安全要求等,在形式上可为服务合同及其附属的工作说明书。

[来源:GB/T 32914—2016,3.4,有修改]

3.190

服务要素 service element

设计和实施服务的关键要素,包括服务人员、服务流程、服务工具、规章,以及其他服务所需的资源。

[来源:GB/T 32914—2016,3.10,有修改:“service factors”改为“service element”]

3.191

服务组合 service portfolio

多个服务类别或服务项目以及其他工作的集合。

[来源:GB/T 32914—2016,3.7]

3.192

符合性 conformity

对要求的满足。

[来源:GB/T 29246—2017,2.13,有修改:删除注]

3.193

复制保护 copy protection

使用特殊技术检测或防止未授权复制数据、软件或固件的安全措施。

[来源:GB/T 5271.8—2001,08.08.01,有修改:删除术语中文“拷贝保护”,“拷贝”改为“复制”等]

3.194

个人标识码 personal identification number;PIN

用于鉴别某一身份的数字代码。

[来源:ISO/IEC 19790:2015,3.89]

3.195

个人敏感信息 personal sensitive information

一旦泄露、非法提供或滥用就有可能危害人身和财产安全,极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。

注 1:个人敏感信息包括公民身份号码、个人生物特征信息、银行账号、通信记录和内容、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息、14 岁以下(含)儿童的个人信息等。

注 2：个人信息控制者通过个人信息或其他信息加工处理后形成的信息，如一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的，也属于个人敏感信息。

[来源：GB/T 35273—2020，3.2，有修改："身份证件号码"改为"公民身份号码"，"个人生物识别信息"改为"个人生物特征信息"，删除原注 2 等]

3.196

个人信息　personal information

以电子或者其他方式记录的能够单独或者与其他信息结合来识别特定自然人身份或者反映其活动情况的各种信息。

注 1：个人信息包括姓名、出生日期、公民身份号码、个人生物特征信息、住址、联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息等。

注 2：个人信息控制者通过个人信息或其他加工处理后形成的信息，例如，用户画像特征标签，能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的，也属于个人信息。

[来源：GB/T 35273—2020，3.1，有修改："身份证件号码"改为"公民身份号码"，"个人生物识别信息"改为"个人生物特征信息"，删除原注 2 等]

3.197

个人信息安全影响评估　personal information security impact assessment

针对个人信息处理活动，检验其合法合规程度，判断其对个人信息主体合法权益有可能造成损害的各种风险，以及评估保护个人信息主体各项措施有效性的过程。

[来源：GB/T 35273—2020，3.9，有修改]

3.198

个人信息处理　personal information processing

对个人信息执行的操作或一组操作。

注：个人信息处理操作包括但不限于收集、存储、变更、检索、咨询、披露、匿名化、假名化、传播或以其他方式提供、删除或销毁。

3.199

个人信息处理者　personal information processor

代表并按照个人信息控制者的指示处理个人信息的利益相关方。

3.200

个人信息控制者　personal information controller

有能力决定个人信息处理目的、方式等的组织或个人。

[来源：GB/T 35273—2020，3.4]

3.201

个人信息主体　personal information subject

个人信息所标识或关联的自然人。

[来源：GB/T 35273—2020，3.3，有修改]

3.202

个性化展示　personalized display

基于特定个人信息主体的网络浏览史、兴趣爱好、消费记录和习惯等信息，向该主体展示信息内容、提供商品或服务的搜索结果等活动。

[来源：GB/T 35273—2020，3.16，有修改]

3.203

根对象标识符　root OID

构成对象标识符集合中的第 1 个、第 2 个和后续公共弧的特定对象标识符（因此是公共根）。

注：根对象标识符加上相对对象标识符等于完整的对象标识符。

[来源:GB/T 29261.3—2012,05.01.18]

3.204

根密钥 root key

用来生成派生密钥的密钥。

[来源:GM/T 0035.1—2014,3.7,有修改:“derivation key”改为“root key”]

3.205

工业控制系统 industrial control system;ICS

在工业部门和关键基础设施中应用于各种工业生产的控制系统。

注:工业控制系统包括监控和数据采集系统(SCADA)、分布式控制系统(DCS)和其他较小的控制系统,例如可编程逻辑控制器(PLC)。

[来源:GB/T 32919—2016,3.1,有修改]

3.206

工作产品 work products

在执行任何过程中产出的所有文档、报告、文件、数据等。

[来源:GB/T 30271—2013,3.1.13,有修改:删除注 1]

3.207

工作指导 work instruction

对如何执行并记录某一过程的详细描述。

[来源:ISO/IEC 27041:2015,3.23]

3.208

公开安全参数 public security parameter;PSP

与安全有关,对其修改能损害密码模块安全的公开信息。

示例:公开密码密钥、公钥证书、自签证书、信任锚、与某一计数器及内部保有的日期和时间关联的一次性口令。

注:当某一 PSP 不能被修改,或对其修改能由此模块确定时,即认为是受保护的。

[来源:ISO/IEC 19790:2015,3.99]

3.209

公开披露 public disclosure

向社会或非特定人群发布信息的行为。

[来源:GB/T 35273—2020,3.11,有修改:“不特定人群”改为“非特定人群”]

3.210

公开验证密钥 public verification key

实现公开验证变换过程的公开密钥。

[来源:GB/T 15843.1—2017,3.28]

3.211

公钥 public key

非对称密码算法中可公开的密钥。

[来源:GB/T 25056—2018,3.11,有修改:“可以公开”改为“可公开”]

3.212

公钥基础设施 public key infrastructure;PKI

基于公钥密码技术,具有普适性,可用于提供机密性、完整性、真实性及抗抵赖性等安全服务的基础设施。

[来源:GM/Z 4001—2013,2.29,有修改]

3.213

公钥信息 public key information

至少包含实体区分性标识符和公钥,此外也能包含关于认证管理机构、实体、密钥使用限制、有效期以及相关算法等其他静态数据的信息。

[来源:GB/T 34953.2—2018,3.12,有修改]

3.214

公钥证书 public key certificate

由证书认证机构对一个实体签发并不可伪造的、有关其公钥信息的数据结构。

[来源:GB/T 17901.1—2020,3.15]

3.215

公证 notarization

将数据在可信的第三方注册,以便能在以后确保数据特性(诸如内容、原发、时间与交付)的准确性的过程。

[来源:GB/T 5271.8—2001,08.06.29,有修改]

3.216

公证权标 notarization token

由公证人生成的抗抵赖权标。

[来源:GB/T 17903.1—2008,3.9.24]

3.217

公证人 notary

公证机构 notary authority

就所涉及的实体以及所存储或通信的数据的性质提供证据,或者将现有权标的生存期延长到期满或作废以后的可信的第三方。

[来源:GB/T 17903.1—2008,3.9.23,有修改]

3.218

攻击 attack

企图破坏、泄露、篡改、损伤、窃取、未授权访问或未授权使用资产的行为。

[来源:GB/T 29246—2017,2.3]

3.219

攻击潜力 attack potential

当攻击发起时感知到的,以攻击者的专业水平、资源和动机来体现成功攻击的潜力。

[来源:ISO/IEC 27032:2012,4.9]

3.220

攻击特征 attack signature

预先界定的据以能发现一次攻击事件正在发生的特定信息。

[来源:GB/T 31499—2015,3.10,有修改]

3.221

攻击者 attacker

故意利用技术和非技术安全控制的脆弱性,以窃取或损害信息系统和网络,或者损害合法用户对信息系统和网络资源可用性为目的的任何人。

[来源:GB/T 25068.1—2020,3.3]

3.222

共享 sharing

信息控制者向其他控制者提供信息,且双方分别对信息拥有独立控制权的行为。

[来源:GB/T 35273—2020,3.13,有修改:“个人信息”改为“信息”,“过程”改为“行为”]

3.223

供应链 supply chain

将多个资源和过程联系在一起,并根据服务协议或其他采购协议建立起连续供应关系的组织系列。其中每一组织充当需方、供方或双重角色。

[来源:GB/T 32914—2016,3.8,有修改]

3.224

供应商 vendor

开发产品/服务或负责维护产品/服务的个人或者组织。

[来源:ISO/IEC 30111:2013,3.7]

3.225

固件 firmware

功能上独立于主存储器,通常存储在只读存储器(ROM)中的指令和相关数据的有序集。

[来源:GB/T 5271.1—2000,01.01.09]

3.226

关键安全参数 critical security parameter;CSP

与安全有关,其泄露或修改会危及密码模块安全的信息。

示例:秘密和私有密码密钥、口令之类的鉴别数据、个人标识码(PIN)、证书或其他信任锚。

注:关键安全参数(CSP)可为明文的或加密的。

[来源:ISO/IEC 17825:2016,3.3,有修改:分别添加缩略语“PIN”“CSP”的中文全称“个人标识码”“关键安全参数”]

3.227

观察报告 observation report

由评价者编写的请求澄清或标识评价过程中存在问题的报告。

[来源:GB/T 30270—2013,3.10,有修改]

3.228

管理体系 management system

组织中相互关联或相互作用,用来建立策略和目标以及达标过程的元素集合。

注 1:管理体系可能专注于单一学科或多个学科。

注 2:体系元素包括组织的结构、角色和责任、规划以及运行。

注 3:管理体系范围可包括组织的整体、组织的具体且确定的功能和部门,或者跨组织群的一项或多项功能。

[来源:GB/T 29246—2017,2.46,有修改]

3.229

光纤信道协议 fibre channel protocol

用于光纤信道互连的串行小型计算机系统接口(SCSI)传输协议。

[来源:ISO/IEC 27040:2015,3.18]

3.230

规程 procedure

活动过程的文档化描述。

3.231

过程　process

一组相互关联或相互作用的活动，使用输入来交付预期的结果。

[来源：ISO/IEC 9000：2015，3.4.1，有修改：删除注]

3.232

过程保障　process assurance

通过对过程活动的评估而获得的保障。

注：过程是指将输入转换为输出的一组有组织的活动；为达到预期目标，某一过程所具有的能力称为“过程能力”。

3.233

过程管理　process management

用于预见、评价和控制过程执行的活动系列和体系结构。

[来源：GB/T 20282—2006，3.11，有修改]

3.234

过程能力　process capability

某一过程达到所要求目标的能力。

[来源：GB/Z 29830.3—2013，2.13，有修改]

3.235

过滤　filtering

依照所规定的准则，接受或拒绝数据流通过某一网络的过程。

[来源：GB/T 25068.1—2020，3.11，有修改]

3.236

骇客　cracker

试图攻破他人信息系统安全并获得对其访问权的个人。

3.237

核查　check

评估者采用简单比较形成裁决。

注：使用此动词的语句描述了需要核查的内容。

[来源：GB/T 30273—2013，3.1，有修改]

3.238

核心配置　core configuration

对关键的配置项进行参数设置的过程。

注：通过核心配置限制或禁止存在安全隐患或漏洞的功能，启用或加强安全保护功能，来增强计算机抵抗安全风险的能力。

[来源：GB/T 35283—2017，3.2，有修改]

3.239

核心配置基线　core configuration baseline

能满足计算机安全基本要求的一组或多组核心配置项基值所构成的集合。

[来源：GB/T 35283—2017，3.3，有修改]

3.240

核心配置基线包　core configuration baseline package

为实现核心配置基线自动化部署而制定的一种具有特定语法格式的核心配置数据文件。

[来源：GB/T 35283—2017，3.4]

3.241

核心配置项(配置项) core configuration item

计算机操作系统、办公软件、浏览器、基本输入输出系统(BIOS)和防恶意代码软件等基础软件中影响计算机安全的关键参数选项。

注:核心配置项类型包括开关项、枚举项、区间项和复合项,可根据安全要求对其进行赋值。

[来源:GB/T 35283—2017,3.1,有修改:“BIOS 系统”改为“基本输入输出系统(BIOS)”,“关键参数可选项”改为“关键参数选项”,“可以根据”改为“可根据”]

3.242

核准机构 approval authority

受委托对某项功能进行审批和/或评价的组织。

3.243

黑客 hacker

对网络或联网系统进行未授权访问,但无意窃取信息或造成损坏的个人。

注:黑客的动因被认为是想了解系统如何工作,或是想证明或反驳现有安全措施的有效性。

3.244

后果 consequence

事态影响目标的结果。

注 1:一个事态可能导致一系列后果。

注 2:一个后果可能是确定的或不确定的,在信息安全的语境下通常是负面的。

注 3:后果可能被定性或定量地表示。

注 4:初始后果可能因连锁效应升级。

[来源:GB/T 29246—2017,2.14,有修改:“可以”改为“可能”]

3.245

后向安全性 backward secrecy

保证经过当前或者此前数据的泄露不能破坏后续数据安全的属性。

[来源:GM/Z 4001—2013,2.30,有修改:“保密性”改为“安全性”]

3.246

后向恢复 backward recovery

通过使用后期版本和记录在日志中的数据,对早期版本数据进行的数据重组。

[来源:GB/T 5271.8—2001,08.07.06]

3.247

互联网 the Internet

在公共领域中由相互连接的网络组成的全球系统。

[来源:GB/T 25068.1—2020,3.14]

3.248

互联网安全协议 IP security;IPSec

用于保护互联网协议(IP)通信的一套安全协议。

注:属于互联网协议第 4 版(IPv4)的一个可选协议系列,也是互联网协议第 6 版(IPv6)的组成部分。

[来源:GB/T 32922—2016,3.2,有修改:术语中文名称“IP 安全协议”改为“互联网安全协议”,分别添加缩略语“IP”“IPv4”“IPv6”中文名称“互联网协议”“互联网协议第 4 版”“互联网协议第 6 版”等]

3.249

环境　environment

〈授权〉与授权决策有关，独立于特定的主体、资源或者动作的属性集合。

[来源：GB/T 30280—2013，3.16，有修改：增加语境标识〈授权〉等]

3.250

环境变量　environmental variables

〈授权〉与授权决策所需策略有关，不包括在静态结构中，但特定权限的验证者可通过本地途径来获得的信息（例如，当天或当前的账目结余）。

[来源：GB/T 16264.8—2005，3.3.28，有修改：增加语境标识〈授权〉等]

3.251

环境失效防护　environmental failure protection；EFP

为防止由于密码模块正常运行范围外的环境条件危及模块安全而采用的各种功能。

[来源：ISO/IEC 19790：2015，3.39]

3.252

环境失效测试　environmental failure testing；EFT

为合理确保密码模块安全不受模块正常运行范围外的环境条件危及而采用的特定方法。

[来源：ISO/IEC 19790：2015，3.40]

3.253

恢复点目标　recovery point objective

为使活动能够恢复操作而需将其所用信息恢复到的时间点。

[来源：GB/T 30146—2013，3.44，有修改]

3.254

恢复时间目标　recovery time objective

从事件发生到完成恢复产品或服务、活动或者资源之间的时间段。

注：对于产品、服务和活动，恢复时间目标需小于组织无法接受的导致产品/服务停止供应或活动无法执行等负面影响所需的时间。

[来源：GB/T 30146—2013，3.45，有修改]

3.255

会话密钥　session key

在一次会话中使用的数据加密密钥。

[来源：GB/T 37033.1—2018，3.4]

3.256

活动　activity

某一过程的内聚性任务的集合。

[来源：ISO/IEC 27043：2015，3.2]

3.257

获取　acquisition

〈调查取证〉在界定的集合之内创建数据副本的过程。

注：获取的产品是一种潜在数字证据副本。

[来源：ISO/IEC 27037：2012，3.1，有修改：增加语境标识“〈调查取证〉”]

3.258

机构证书　authority certificate

签发给机构(例如,证书认证机构或者属性授权机构)的证书。

[来源:GB/T 16264.8—2005,3.3.7,有修改:“发布”改为“签发”]

3.259

机密性　confidentiality

采用密码技术保证信息不泄露的性质。

3.260

基本测度　base measure

用某一属性及其量化方法界定的测度。

注:基本测度在功能上独立于其他测度。

[来源:GB/T 29246—2017,2.10,有修改]

3.261

基础信息网络　fundamental information networks

承担国家公共通信、广播电视传输的电信网、互联网、广播电视网等信息网络。

[来源:GB/T 31495.2—2015,3.1]

3.262

基线控制　baseline controls

为某一系统或组织建立的最低防护措施的集合。

3.263

基于角色的访问控制　role-based access control

一种对某一角色授权,许可其访问相应对象的访问控制方法。

[来源:GM/T 0028—2014,3.76,有修改]

3.264

基于三元对等架构的访问控制　TePA-based access control

通信双方依据基于三元对等架构(TePA)的实体鉴别结果进行端口控制的访问控制方法。

[来源:GB/T 29828—2013,3.14,有修改:添加“三元对等架构”的缩略语“TePA”等]

3.265

基于身份的密码标识　identity-based cryptographic identity

表示某一实体身份或属性的字符串。

[来源:GM/T 0024—2014,3.3,有修改:术语中文名称“IBC 标识”改为“基于身份的密码标识”等]

3.266

基于身份的密码算法　identity-based cryptographic algorithm

一种能以注册身份派生公钥的非对称密码算法。

[来源:GM/T 0024—2014,3.2,有修改:术语中文“IBC 算法”改为“基于身份的密码算法”等]

3.267

激活数据　activation data

用于使密码模块进入可操作状态的数据。可为口令、生物特征等。

[来源:GB/T 31508—2015,3.13,有修改:“可以是”改为“可为”等]

3.268

集线器　hub

一种工作在开放系统互联(OSI)参考模型第 1 层的网络设备。

注:网络集线器不是智能设备,它只为联网系统或设备提供物理连接点。

[来源:GB/T 25068.1—2020,3.13]

3.269

计数器工作模式　counter operation mode;CTR

一种用分组密码算法构造序列密码的模式,将计数器的值作为算法的输入序列进行分组运算,再将运算输出的若干位与明文逐位做异或得到密文,然后对计数器作增量或减量运算并作为算法下一时刻的输入序列。

[来源:GM/Z 4001—2013,2.37,有修改:“比特”改为“位”等]

3.270

计算机安全　computer security

为保护计算机系统的数据和资源,免受偶然或恶意的修改、损害、访问、泄露等操作所采取的适当措施。

[来源:GB/T 5271.8—2001,08.01.01,有修改]

3.271

计算机犯罪　computer crime

借助或直接介入数据处理系统或计算机网络而构成的犯罪。

[来源:GB/T 5271.8—2001,08.05.02,有修改:删除注]

3.272

计算机滥用　computer abuse

影响或涉及数据处理系统的安全,蓄意的或无意的未经授权操作计算机的活动。

[来源:GB/T 5271.8—2001,08.05.01,有修改]

3.273

计算机系统审计　computer-system audit

检查计算机系统所用的规程,评估其有效性和准确性,并提出改进建议的过程。

[来源:GB/T 5271.8—2001,08.06.19,有修改;“处理系统”改为“计算机系统”等]

3.274

计算机信息系统　computer information system

由计算机及其关联和配套的设备、设施(含网络)构成的,按既定应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的系统。

[来源:GB 17859—1999,3.1,有修改:将“人机系统”改为“系统”等]

3.275

计算机信息系统可信计算基　trusted computing base of computer information system

计算机信息系统内的保护装置,包括硬件、固件、软件等并负责执行安全策略的组合体。

注:计算机信息系统可信计算基建立了一个基本的保护环境并提供一个可信计算系统所要求的附加用户服务。

[来源:GB 17859—1999,3.2,有修改]

3.276

计算机诈骗　computer fraud

借助或直接介入数据处理系统或计算机网络而构成的诈骗。

[来源:GB/T 5271.8—2001,08.05.03]

3.277

记录　record

〈评估〉为使得评估过程中所做的工作能在日后重建,而对程序、事件、观察结果、所了解事项和结果等所做的详细书面记载。

[来源:GB/T 30273—2013,3.9,有修改:增加语境标识“〈评估〉”,“详细书面描述和记载”改为“详

细书面记载”等]

3.278

加密　encipherment encryption

对数据进行密码变换以产生密文的过程。

[来源:GB/T 36322—2018,3.5]

3.279

加密密钥对　encryption key-pair

非对称算法中用于加解密的一对密钥。

3.280

加密算法　encryption algorithm

将明文转换为密文的算法。

[来源:ISO/IEC 18033-2:2006,3.17,有修改:“过程”改为“算法”]

3.281

加密系统　encryption system

由加密算法、解密算法和密钥生成这三种处理过程组成的系统。

[来源:GB/T 36624—2018,3.5,有修改:删除“用于保护数据的保密性”]

3.282

加密证书　encipherment certificate

用于密钥协商或保护数据加密密钥的数字证书。

[来源:GM/Z 4001—2013,2.43,有修改]

3.283

假冒攻击　masquerade attack

攻击者假冒用户,欺骗验证者的攻击方法。

[来源:GM/Z 4001—2013,2.38]

3.284

假冒验证者攻击　verifier impersonation attack

攻击者假冒验证者,欺骗被验证者的攻击方法。

[来源:GM/Z 4001—2013,2.39]

3.285

架构　architecture

构成系统的各组成部分及其相互关系,以及该系统与环境的关系,还包括指导其设计和演进的基本原则。

[来源:GB/T 25068.1—2020,3.2]

3.286

间谍软件　spyware

从计算机用户处收集私人或保密信息的欺骗性软件。

注:信息可能包括最频繁访问的网站或口令之类更敏感的信息。

[来源:ISO/IEC 27032:2012,4.43]

3.287

监控和数据采集系统　supervisory control and data acquisition system

工业生产控制过程中,对资产和设备在网环境下进行集中式数据采集与监控管理的控制系统。

注:监控和数据采集系统以计算机为基础,对远程分布运行设备进行监控调度,其主要功能包括数据采集、参数测量和调节、信号报警等。监控和数据采集(SCADA)系统一般由设在控制中心的主终端控制单元(MTU)、通信

线路和设备、远程终端单位(RTU)等组成。

[来源:GB/T 36323—2018,3.3,有修改:添加缩略语“SCADA”的中文全称“监控和数据采集”等]

3.288

监视　monitoring

确定系统、过程或活动状态的行为。

注:为确定状态可能需要检查、监督或严密观察。

[来源:GB/T 29246—2017,2.52]

3.289

检查　examination

测评人员通过对测评对象(文档、设备、安全配置等)进行观察、查验、分析和取得证据的过程。

[来源:GB/T 28448—2019,3.2,有修改:“如制度文档、各类设备、安全配置等”改为“文档、设备、安全配置等”,“以帮助测评人员理解、澄清或取得证据”改为“和取得证据”]

3.290

检查评估　inspection assessment

由所评估信息系统所有者的上级主管部门、业务主管部门或国家相关监管部门发起,依据国家有关法规与标准,对信息系统安全管理进行的评估活动。

[来源:GB/T 28453—2012,3.3,有修改]

3.291

检错码　error-detection code

为了检测(但不能校正)数据是否改变,而将从该数据某一特定函数计算出的值作为检测值附在该数据上的冗余位。

3.292

简单功耗分析　simple power analysis

对指令执行(或单个指令的执行)模式的直接(主要是可视化的)分析,它与密码模块的功耗有关,并用以获取密码操作相关的信息。

[来源:GB/T 37092—2018,3.18]

3.293

简单邮件传送协议　simple mail transfer protocol;SMTP

一种用于向邮件服务器发送邮件的互联网协议。

3.294

健壮性　robustness

对某一系统或组件在无效数据输入或者在高强度输入等环境下,描述其各项功能均能保持正确运行的性质。

[来源:GB/T 28457—2012,3.8,有修改:“可保持”改为“能保持”等]

3.295

健壮性测试　robustness testing

应对系统错误(包括无效、高强度或非期望的输入或者恶意攻击)的有效处理能力进行的测试。

[来源:GB/T 28456—2012,3.23,有修改:“对 IPsec 协议应用应对措施”改为“应对系统错误”等]

3.296

鉴别　authentication

验证某一实体所声称身份的过程。

[来源:GB/T 5271.8—2001,08.01.11,有修改]

3.297

鉴别权标　authentication token

一种在强鉴别交换期间传送，可用于鉴别其发送者的权标。

[来源：GB/T 16264.8—2005，3.3.5，有修改]

3.298

鉴别式加密　authenticated encryption

一种可逆的数据转换，这种数据转换利用加密算法产生数据的对应密文，未经授权实体无法在不被发现的情况下对其修改，即提供了数据保密性、数据完整性与数据源鉴别。

[来源：GB/T 36624—2018，3.1，有修改："可鉴别的加密"改为"鉴别式加密"]

3.299

鉴别数据　authentication data

用于验证用户所声称身份的信息。

[来源：GB/T 18336.1—2015，3.1.7]

3.300

交付抗抵赖　non-repudiation of delivery

旨在防止接收者不实否认已经收到消息并认可其内容的服务。

[来源：GB/T 17903.1—2008，3.9.14，有修改]

3.301

交付抗抵赖权标　non-repudiation of delivery token

允许原发者为消息建立交付抗抵赖的权标。

[来源：GB/T 17903.1—2008，3.9.25，有修改：术语中英文"NRD 权标　NRD token"改为"交付抗抵赖权标　non-repudiation of delivery token"，"发送者"改为"原发者"，"数据项"改为"权标"等]

3.302

交换机　switch

利用内部交换机制来提供联网设备之间连通性的设备，其中的交换技术通常在开放系统互连(OSI)参考模型的第 2 层或第 3 层实现。

[来源：GB/T 25068.1—2020，3.39，有修改：添加缩略语"OSI"的中文全称"开放系统互连"]

3.303

接口　interface

界面

在两个功能单元之间，由这两个功能单元的功能特性、物理互连特性、信号交换特性及其他适当特性界定的共享边界。

[来源：GB/T 5271.9—2001，09.01.06，有修改]

3.304

接收抗抵赖　non-repudiation of receipt

旨在防止接收者不实否认其已经收到消息的服务。

[来源：GB/T 17903.1—2008，3.9.17，有修改]

3.305

解密　decipherment；decryption

与加密过程对应的逆过程。

[来源：GB/T 36322—2018，3.3，有修改]

3.306

解密算法　decryption algorithm

将密文转换为明文的算法。

3.307

解释　interpretation

〈证据〉关于构成调查的一系列检查和分析所得出证据的事实信息，在约定限度内对其所做的综合阐释。

[来源：ISO/IEC 27042：2015，3.9，有修改：增加语境标识“〈证据〉”]

3.308

解析器　resolver

向域名服务器发出域名解析请求，并且从所返回的响应消息中提取所需信息的程序。解析器通常集成到操作系统内核或者应用软件中。

[来源：GB/T 33562—2017，3.19，有修改]

3.309

经授权用户　authorized user

依据安全策略可执行某项操作的用户。

[来源：GB/T 30284—2020，3.1.4，有修改：术语中文名称“授权用户”改为“经授权用户”]

3.310

警报　alert

信息系统和网络可能受到攻击或者因意外事件、故障或人为错误而处于危险之中的“即时”指示。

[来源：GB/T 25068.1—2020，3.1]

3.311

纠正　correction

消除已查明的不符合的措施。

[来源：GB/T 29246—2017，2.18]

3.312

拒绝服务　denial of service；DoS

阻止对系统资源的经授权访问或延迟系统的运行和功能，并导致经授权用户可用性受损。

[来源：GB/T 25068.1—2020，3.9，有修改：“授权”改为“经授权”]

3.313

决策　decision

规则、策略或策略集的评估结果。

[来源：GB/T 30280—2013，3.12]

3.314

决策准则　decision criteria

用于确定行动或进一步调查的需要或者描述给定结果置信度的阈值、目标或模式。

[来源：GB/T 29246—2017，2.21，有修改]

3.315

角色　role

组织语境中赋予用户具有相应权力和责任的一种职能。

[来源：GB/T 25062—2010，3.5，有修改]

3.316

抗抵赖策略　non-repudiation policy

一组提供抗抵赖服务的准则。

注：具体而言，用于生成和验证证据以及裁决的一组规则。

[来源：GB/T 17903.1—2008，3.9.10，有修改]

3.317

抗抵赖服务请求者　non-repudiation service requester

请求为某特定事件或动作生成抗抵赖证据的实体。

[来源：GB/T 17903.1—2008，3.6.4，有修改]

3.318

抗抵赖交换　non-repudiation exchange

以抗抵赖为目的，抗抵赖信息(NRI)的一次或多次传送所组成的序列。

[来源：GB/T 17903.1—2008，3.9.12，有修改]

3.319

抗抵赖权标　non-repudiation token

GB/T 18794.1 中定义，由证据和可选的附加数据组成的一种特殊类型的安全权标。

[来源：GB/T 17903.1—2008，3.9.21，有修改]

3.320

抗抵赖信息　non-repudiation information；NRI

包括证据的生成和验证所涉及的事件或动作的信息、证据本身以及有效的抗抵赖策略的一组信息。

[来源：GB/T 17903.1—2008，3.9.11，有修改：添加“抗抵赖信息”的缩略语“NRI”等]

3.321

抗抵赖性　non-repudiation

不可否认性

证明一个已经发生的操作行为无法否认的性质。

[来源：GM/Z 4001—2013，2.46，有修改]

3.322

抗碰撞散列函数　collision-resistant hash-function

满足如下性质的散列函数：找出映射到同一输出的任何两个不同输入在计算上是不可行的。

注：计算可行性依赖于特定安全要求和环境。

[来源：GB/T 18238.1—2000，2.1，有修改：术语中文“无碰撞散列函数”改为“抗碰撞散列函数”等]

3.323

可编程逻辑控制器　programmable logic controller；PLC

采用可编程存储器，通过数字运算操作对装备进行控制的电子设备。

注：PLC 主要执行各类运算、顺序控制、定时等指令，用于控制装备的动作，是控制系统的基础单元。

[来源：GB/T 36323—2018，3.4，有修改：“工业生产装备”改为“装备”，“工业控制系统”改为“控制系统”]

3.324

可辨别编码规则　distinguished encoding rules；DER

适用于抽象语法记法 1(ASN.1)符号体系所界定的类型值的编码规则。

注：应用这些编码规则会为这些值生成一个传输语法。隐含的是，同样的规则也用于解码。如果编码值小到足以

装入可用内存并需要快速跳过某些嵌套值时，DER 更适合。

[来源：ISO/IEC 18014-2：2009，3.9，有修改：添加缩略语“ASN.1”的中文全称“抽象语法记法 1”，删除原注 1]

3.325

可重复性　repeatability

在同一测试环境（同一计算机、硬盘驱动器、操作模式等）中实施而得到相同测试结果的过程的性质。

[来源：ISO/IEC 27037：2012，3.17]

3.326

可核查性　accountability

确保从一个实体的行为能唯一地追溯到该实体的性质。

[来源：GB/T 5271.8—2001，08.01.10，有修改]

3.327

可靠性　reliability

与预期行为和结果一致的性质。

[来源：GB/T 29246—2017，2.62，有修改]

3.328

可扩展鉴别协议　extensible authentication protocol

一种由远程鉴别拨入用户服务所支持的，并支持用于点对点协议（PPP）的多个任选的鉴别机制（包括纯明文口令、询问-响应和任意问答）的一组规则。

3.329

可能性　likelihood

某事发生的机会。

[来源：GB/T 29246—2017，2.45，有修改]

3.330

可视性　visibility

某一系统或过程使各系统元素和过程能被记录并对监控和检查可用的性质。

[来源：ISO/IEC 27036-1：2014，3.15]

3.331

可卸封盖　removable cover

允许有意设计的非破坏性访问密码模块物理内容的物理手段。

[来源：ISO/IEC 19790：2015，3.101]

3.332

可信报告根　root of trust for reporting

能可靠报告可信存储根所保存信息的计算引擎。

[来源：GB/T 29827—2013，3.4，有修改]

3.333

可信存储根　root of trust for storage

能可靠进行安全存储的计算引擎。

[来源：GB/T 29827—2013，3.3，有修改]

3.334

可信第三方　trusted third party；TTP

在安全相关活动方面，被其他实体信任的安全机构或其代理。

[来源:ISO/IEC 18014-1:2008,3.20]

3.335

可信度量根　root of trust for measurement

用作信任传递链的起始点,能可靠进行完整性度量的计算引擎。

[来源:GB/T 29827—2013,3.2,有修改]

3.336

可信计算密码支撑平台　cryptographic support platform for trusted computing

为可信计算平台自身的完整性、身份可信性和数据安全性提供密码支持的,由密码算法、密钥管理、证书管理、密码协议和密码服务等组成的系统。

注:可信计算密码支撑平台的产品形态主要表现为可信密码模块和可信密码服务模块。

[来源:GB/T 29829—2013,3.1.2,有修改]

3.337

可信计算平台　trusted computing platform

构建在计算系统中,用于实现可信计算功能的支撑系统。

[来源:GB/T 29829—2013,3.1.1]

3.338

可信连接架构　trusted connect architecture;TCA

一种基于三元对等架构,实现双向用户身份鉴别和平台鉴别的可信网络连接架构。

[来源:GB/T 29828—2013,3.17,有修改:"三元对等鉴别"改为"三元对等架构"等]

3.339

可信路径　trusted path

用户和评价对象安全功能(TSF)能以必要的信任度进行通信的手段。

[来源:GB/T 18336.1—2015,3.1.80,有修改:添加缩略语"TSF"的中文全称"评价对象安全功能"等]

3.340

可信密码模块　trusted cryptography module;TCM

可信计算平台中,提供密码运算功能,具有受保护存储空间的物理装置。

[来源:GB/T 29829—2013,3.1.7,有修改:添加"可信密码模块"的缩略语"TCM","硬件模块"改为"物理装置"]

3.341

可信平台控制模块　trusted platform control module

一种集成在可信计算平台中,用于建立和确保信任源,为可信计算提供完整性度量、安全存储、可信报告以及密码服务等功能的硬件核心模块。

[来源:GB/T 29827—2013,3.20,有修改]

3.342

可信信道　trusted channel

评价对象安全功能(TSF)和另一可信信息技术(IT)产品能以必要的信任度进行通信的手段。

[来源:GB/T 21050—2019,3.1.2,有修改:分别添加缩略语"TSF""IT"的中文全称"评价对象安全功能""信息技术"等]

3.343

可信信息通信实体　trusted information communication entity

支持在信息共享社区内进行信息交换的自主组织。

[来源:GB/T 29246—2017,2.85]

3.344

可信应用　trusted application

支持网站可信标识验证及展示的应用，包括浏览器、搜索引擎、即时通信软件等。

[来源：GB/T 35287—2017，3.3]

3.345

可用性　availability

可由经授权实体按需访问和使用的性质。

[来源：GB/T 29246—2017，2.9，有修改："特性"改为"性质"等]

3.346

可再现性　reproducibility

在不同测试环境中，为获得相同测试结果的过程所具有的性质。

注：不同测试环境指不同的计算机、硬盘驱动器、操作员等。

[来源：ISO/IEC 27042：2015，3.18]

3.347

可追踪性　traceability

在整个供应链上，允许对身份、过程或元素的活动进行跟踪的性质。

[来源：ISO/IEC 27036-3：2013，3.4]

3.348

控制〈名词〉　control

改变风险的措施。

注 1：控制包括任何改变风险的过程、策略、设备、实践或其他措施。

注 2：控制未必总能达到预期或假定的风险改变效果。

[来源：GB/T 29246—2017，2.16，有修改：增加词性标识"〈名词〉"等]

3.349

控制目标　control objective

描述控制的实施结果所要达到目标的声明。

[来源：GB/T 29246—2017，2.17]

3.350

口令　password

作为一种需熟记的弱秘密，用于实体鉴别的秘密的字、短语、数字或字符序列。

[来源：ISO/IEC 11770-4：2017，3.27]

3.351

口令鉴别式密钥检索　password-authenticated key retrieval

一种密钥检索过程，在这种密钥检索过程中，实体 A 具有从某一口令导出的弱秘密，而另一实体 B 具有与 A 的弱秘密关联的强秘密；这两个实体利用各自的秘密，协商一个可由 A 检索但不(必)可由 B 导出的秘密密钥。

[来源：ISO/IEC 11770-4：2017，3.29]

3.352

口令鉴别式密钥协商　password-authenticated key agreement

使用先前共享的基于口令的信息(即两个实体或者都具有同一共享口令，或者一个具有口令而另一个具有口令验证数据)，在两个实体之间建立一个或多个共享秘密密钥，而两个实体都不能预先确定共享秘密密钥的值的过程。

[来源：ISO/IEC 11770-4：2017，3.28]

3.353

口令验证数据　password verification data

用于验证某一实体具备特定口令相关知识的数据。

[来源:ISO/IEC 11770-4:2017,3.31]

3.354

块　block

分组

作为一个单位记录或传输的元素序列。

注:这里的元素可为字符、字或记录。

[来源:GB/T 5271.4—2000,4.07.07,有修改:增加同义名称“分组”,“可以是”改为“可为”]

3.355

垃圾邮件　spam

电子邮件使用者事先未提出请求或同意接收的电子邮件。

注:垃圾邮件一般具有如下特征:

——未经电子邮件使用者请求而发送;

——同时发送给大量用户;

——伪造的发件人信息。

[来源:GB/T 30282—2013,3.1,有修改]

3.356

滥发　spamming

以大量的数据使资源(网络、服务等)不堪重负的行为;或者,以各种不相干或不适当的消息将资源淹没的行为。

示例:发送大量垃圾邮件。

3.357

累积增量备份　cumulative incremental backup

备份自上次完全备份后更改过的所有数据对象。

注:使用累积增量备份恢复数据时,只需要上次完全备份和自上次完全备份后的累积增量备份。

[来源:GB/T 29765—2013,3.13,有修改]

3.358

利益相关方　interested party (preferred term);stakeholder (admitted term)

对于一项决策或活动,可能对其产生影响,或被其影响,或认为自己受到其影响的个人或组织。

[来源:ISO/IEC 27000:2018,3.37]

3.359

连带口令密钥权标　password-entangled key token

从一个弱秘密和一个密钥权标因子两者一起导出的密钥权标。

[来源:ISO/IEC 11770-4:2017,3.30]

3.360

连接拆除时延　connection-released delay

将连接拆除所需的时间,这种拆除包括客户端完成服务后请求将连接拆除和服务器主动将连接拆除。

[来源:GB/T 28456—2012,3.29,有修改]

3.361

连接建立时延　connection-established delay

从连接建立请求开始,到连接建立完成所经过的时间。

[来源:GB/T 28456—2012,3.27]

3.362

联系点　point of contact;PoC

作为事件管理活动相关信息的协调者或聚集点的组织功能或角色。

[来源:GB/T 20985.1—2017,3.8,有修改]

3.363

令牌　token

权标

由与特定通信相关的数据字段构成的一种权限符号,包含使用密码技术变换后信息的消息。

[来源:GB/T 15843.1—2017,3.37,有修改:增加同义术语中文“权标”]

3.364

流量分析　traffic analysis

通过观察通信流量来推断所关注信息的过程。

示例:对通信流量的存在与否、数量、方向和频次的分析。

[来源:GB/T 5271.8—2001,08.05.41,有修改]

3.365

漏报　false negative

安全事态或事件发生时检测系统没有报警的情况。

3.366

路由器　router

一种用于建立通过一个或不止一个计算机网络的路径的功能单元。

注:在符合 OSI 模型的计算机网络中,路由器在网络层运行。

[来源:GB/T 5271.18—2008,18.02.11]

3.367

轮密钥　round key

根据输入密钥用密钥编排算法推导得出,用于控制迭代分组密码每一轮转换的密钥。

[来源:GB/T 32907—2016,2.5,有修改]

3.368

逻辑炸弹　logic bomb

当由某一特定系统条件触发时,对数据处理系统造成损害的恶性逻辑程序。

[来源:GB/T 5271.8—2001,08.05.51,有修改]

3.369

冒充　masquerade

为获得未经授权的访问权,一个实体伪装成另一个不同实体的行为。

[来源:GB/T 5271.8—2001,08.05.29,有修改]

3.370

迷惑〈动词〉　to spoof

欺骗用户、观察者(如监听者)或资源。

[来源:GB/T 5271.8—2001,08.05.33,有修改]

3.371

秘密　secret

只有经授权实体才知晓的值。

[来源:ISO/IEC 11770-4:2017,3.34]

3.372

秘密参数　secret parameter

不在公开域中出现，仅供某一声称方使用的数字或位串。

注：例如，私钥。

[来源：ISO/IEC 9798-5：2009，2.26]

3.373

秘密共享　secret sharing

将秘密分解成多个子秘密，使用超过阈值数目的子秘密才能恢复该秘密的机制。

[来源：GM/Z 4001—2013，2.59，有修改]

3.374

秘密密钥　secret key

采用对称密码技术，只能由一组指定实体使用的密钥。

[来源：GB/T 36624—2018，3.8，有修改]

3.375

密码边界　cryptographic boundary

为密码模块的所有组件（即硬件、软件或固件的集合）明确界定并建立的物理和/或逻辑边界。

[来源：GB/T 37092—2018，3.4，有修改]

3.376

密码分析　cryptanalysis

为获取安全参数或明文等，解析或破译密码系统的过程。

3.377

密码机　cryptographic machine

能独立运行，实现密码运算、密钥管理等功能，并提供密码服务的设备。

[来源：GM/Z 4001—2013，2.51，有修改]

3.378

密码理论　cryptographic theory

研究密码的编制、破译、管理和应用的理论。

[来源：GM/Z 4001—2013，2.52，有修改]

3.379

密码模块　cryptographic module

实现密码运算功能，相对独立的软件、硬件、固件或这三者组合。

[来源：GB/T 37033.1—2018，3.6，有修改：“其组合”改为“这三者组合”]

3.380

密码算法　cryptographic algorithm

描述密码处理过程的算法。

[来源：GM/Z 4001—2013，2.54，有修改：“运算规则”改为“算法”]

3.381

密码算法标识符　cryptographic algorithm identifier

用于对密码算法进行唯一标识的一组字符。

[来源：GM/Z 4001—2013，2.124，有修改：术语中文“算法标识”改为“密码算法标识符”，“符号”改为“一组字符”]

3.382

密码算法集成电路　cryptographic algorithm integrated circuit

实现密码运算功能的集成电路。

[来源:GM/Z 4001—2013,2.55,有修改:术语中英文“密码算法芯片　cryptographic algorithm chip”改为“密码算法集成电路　cryptographic algorithm integrated circuit”,“集成电路芯片”改为“集成电路”]

3.383

密码同步　cryptographic synchronization

加密和解密过程的协调。

[来源:ISO/IEC 10116:2017,3.4]

3.384

密码系统　cryptographic system

由密码算法、密码协议、密码设备及相关技术构成,以实现某种密码功能(加密传输、加密存储、鉴别认证、密钥管理等)的系统。

[来源:GM/Z 4001—2013,2.56,有修改]

3.385

密码校验函数　cryptographic check function

以秘密密钥和任意字符串为输入,以密码校验值为输出的函数。

注:缺少秘密密钥就不能获取正确的校验值。

[来源:GB/T 15843.1—2017,3.8,有修改:“密码变换过程”改为“函数”]

3.386

密码协议　cryptographic protocol

两个或两个以上参与者使用密码算法,为达到某种特定目的而约定的规则。

[来源:GM/Z 4001—2013,2.57,有修改]

3.387

密码学　cryptology

研究密码与密码活动本质和规律,指导密码实践的学科。

注:主要探索密码的编制、破译以及管理的一般规律。

[来源:GM/Z 4001—2013,2.50,有修改]

3.388

密文　ciphertext

采用密码算法,经过变换将其信息内容隐藏起来的数据。

[来源:GB/T 15843.1—2017,3.7,有修改]

3.389

密钥　key

控制密码变换操作的符号序列。

注:例如,加密、解密、密码校验函数计算、签名生成或签名验证。

[来源:GB/T 15843.1—2017,3.16]

3.390

密钥备份　key backup

从密码设备中将密钥安全复制到存储媒体的过程。

注:密钥备份用于密钥恢复。

[来源:GM/Z 4001—2013,2.64,有修改:“载体”改为“媒体”等]

3.391

密钥编排　key schedule

分组密码算法中由工作密钥扩展生成轮密钥的方法。

[来源:GM/Z 4001—2013,2.65,有修改:“实现方法”改为“方法”]

3.392

密钥生成　key generation

按特定规则产生密钥的过程。

[来源:GM/Z 4001—2013,2.66,有修改:“密钥产生”改为“密钥生成”]

3.393

密钥撤销　key revocation

确保密钥安全失效的服务。

[来源:ISO/IEC 11770-1:2010,2.30]

3.394

密钥传送　key transportation

实体间传送受保护密钥的过程。

[来源:GM/Z 4001—2013,2.68]

3.395

密钥存储　key storage

将密钥保存在指定受控空间的过程。

[来源:GM/Z 4001—2013,2.69]

3.396

密钥对　key pair

非对称密码系统中由一个公钥和一个私钥组成的对。

[来源:ISO/IEC 29150:2011,3.22,有修改]

3.397

密钥分发　key distribution

按照安全协议将密钥分配给对应实体的过程。

[来源:GM/Z 4001—2013,2.70]

3.398

密钥分发中心　key distribution centre;KDC

生成或获得密钥,并分发到其他实体的可信实体。

[来源:ISO/IEC 11770-5:2011,3.15,有修改]

3.399

密钥分量　key division

利用秘密共享技术将密钥分割成的多个部分之一。

[来源:GM/Z 4001—2013,2.71,有修改]

3.400

密钥更新　key update

用新密钥替换旧密钥的过程。

[来源:GM/Z 4001—2013,2.72,有修改:“来代替”改为“替换”等]

3.401

密钥管理　key management

在密钥全生存周期，根据安全策略，对密钥的产成、分发、存储、使用、更新、归档、撤销、备份、恢复和销毁等进行的管理。

[来源：GM/Z 4001—2013，2.73，有修改："生命周期"改为"生存周期"，并增加"使用"环节等]

3.402

密钥管理中心　key management center；KMC

负责密钥管理的组织。

[来源：GM/Z 4001—2013，2.75，有修改："机构"改为"组织"]

3.403

密钥归档　key archive

将已分发且不再使用的密钥分类记录并安全保存的管理过程。

[来源：GM/Z 4001—2013，2.76]

3.404

密钥互鉴别　mutual key authentication

能保证两个实体之间只有对方才拥有正确密钥的鉴别方式。

[来源：ISO/IEC 11770-4：2017，3.25]

3.405

密钥恢复　key recovery

将归档或备份的密钥恢复到可用状态的过程。

[来源：GM/Z 4001—2013，2.77]

3.406

密钥加密密钥　key encryption key

对密钥进行加密保护的密钥。

[来源：GB/T 36322—2018，3.6]

3.407

密钥建立　key establishment

使某一共享的秘密密钥对一个或多个实体可用的过程。

注：密钥建立包括密钥协商、密钥传送和密钥检索。

[来源：ISO/IEC 11770-4：2017，3.17]

3.408

密钥空间　key space

所有可能的密钥形成的集合。

[来源：GM/Z 4001—2013，2.79，有修改："组成"改为"形成"]

3.409

密钥流　keystream

由序列密码算法产生的密钥序列。

3.410

密钥流函数　keystream function

一种以密钥流生成器的当前状态和(可选地)先前生成的部分密文作为输入，而以该密钥流接下去

的部分作为输出的函数。

[来源:ISO/IEC 18033-4:2011,3.9]

3.411

密钥流生成器 keystream generator

一种进行如下处理的基于状态的过程(即一种有限状态机):以一个密钥、一个初始化向量以及于必要时的密文作为输入,而以一个任意长度的密钥流(即位序列或位块)作为输出。

[来源:ISO/IEC 18033-4:2011,3.10]

3.412

密钥派生函数 key derivation function

通过作用于共享秘密和双方都知晓的其他参数,产生一个或多个共享秘密密钥的函数。

[来源:GB/T 32918.3—2016,3.2,有修改:“知道”改为“知晓”]

3.413

密钥权标 key token

在执行密钥建立机制期间,从一个实体向另一实体发送的密钥建立消息。

[来源:ISO/IEC 11770-4:2017,3.20]

3.414

密钥确认 key confirmation

某一实体确信已识别的另一实体拥有正确密钥的过程。

[来源:GM/Z 4001—2013,2.80,有修改]

3.415

密钥生存期 key lifetime

密钥从产生开始到销毁的整个过程。

[来源:GM/Z 4001—2013,2.81,有修改:删除“最终”,“生命周期”改为“过程”等]

3.416

密钥销毁 key destruction

通过物理或逻辑手段使密钥无法恢复的过程。

[来源:GM/Z 4001—2013,2.82,有修改]

3.417

密钥协商 key agreement

密钥交换 key exchange

在至少两个实体之间,通过相互传送消息来共同建立共享秘密密钥,且各方均无法预先确定该秘密密钥值的过程。

[来源:GM/Z 4001—2013,2.83,有修改:“协议”改为“过程”等]

3.418

密钥长度 key length

密钥的位数。

[来源:GB/T 32907—2016,2.2,有修改:“比特位数”改为“位数”]

3.419

密钥转换中心 key translation centre

将一方生成并加密的密钥解密后再为另一方重新加密的可信实体。

[来源:ISO/IEC 11770-1:2010,2.32]

3.420

蜜罐 honeypot

一种如下诱饵系统的通称,用于欺骗、分散、转移和鼓励攻击者,使其把时间花在看似很有价值但实际上是伪造的、合法用户不会感兴趣的信息上。

[来源:ISO/IEC 27039:2016,2.13]

3.421

敏感安全参数 sensitive security parameters;SSP

关键安全参数(CSP)和公共安全参数(PSP)。

[来源:ISO/IEC 19790:2015,3.110]

3.422

敏感性 sensitivity

信息拥有者赋予信息,以标明其保护需求重要程度的一种度量。

[来源:GB/T 5271.8—2001,08.01.26,有修改]

3.423

敏感性标记 sensitivity label

表示主体/客体安全级别和安全范畴的一组信息。

注:在可信计算基中把敏感性标记用作强制访问控制决策的依据。

3.424

明示同意 explicit consent

信息主体通过书面、口头等方式主动作出纸质或电子形式的声明,或者自主作出肯定性动作,对其信息进行特定处理作出明确授权的行为。

注:肯定性动作包括信息主体主动勾选、主动点击“同意”“注册”“发送”“拨打”、主动填写或提供等。

[来源:GB/T 35273—2020,3.6,有修改:“个人信息”改为“信息”]

3.425

明文 plaintext

未加密的信息。

[来源:GB/T 15843.1—2017,3.19]

3.426

命名属性 named attribute

属性的特定实例,具体值取决于属性名、类型、持有者和属性颁发者。

[来源:GB/T 30281—2013,3.9]

3.427

模数 modulus

一个整数,用作整除计算的除数以得到一个整数余数。

[来源:GB/T 17710—2008,2.4,有修改:删除“它”]

3.428

默许同意 tacit consent

在信息主体无明确反对的情况下,默认其已同意。

[来源:GB/Z 28828—2012,3.10,有修改,“个人信息”改为“信息”,“认为个人信息主体同意”改为“默认其已同意”]

3.429

目标　objective

要实现的结果。

注 1：目标可能是战略性的、战术性的或操作性的。

注 2：目标可能涉及不同学科(诸如金融、健康与安全以及环境目标)，可能适用于不同层次(诸如战略、组织、项目、产品和过程)。

注 3：目标可能以其他方式表示，例如，作为预期结果、意图、操作准则，作为信息安全目标，或者使用具有类似含义的其他词(例如，目的或标靶)。

注 4：在信息安全管理体系的语境下，组织制定与信息安全策略一致的信息安全目标以实现特定结果。

[来源：GB/T 29246—2017，2.56，有修改："可以"改为"可能"]

3.430

目标　target

通过主体、资源和动作进行限定的决策请求的集合，是规则、策略和策略集评价的对象。

[来源：GB/T 30280—2013，3.31，有修改：删除定义中的英文]

3.431

目录服务　directory service

一种从明确界定的对象分类目录中搜索和检索信息的服务。

注：目录中可包括对象的证书、电话号码、访问条件、地址等信息。

[来源：ISO/IEC 15945：2002，3.6，有修改：删除示例]

3.432

内部通信信道　internal communication channel

评价对象(TOE)各分离部分间的通信信道。

[来源：GB/T 18336.1—2015，3.1.40，有修改：添加缩略语"TOE"的中文全称"评价对象"]

3.433

内部网络　internal network

在组织范围内部，与外部网络隔离的受保护的网络。

[来源：GB/T 31499—2015，3.3，有修改："受保护的可信网络区域"改为"受保护的网络"等]

3.434

内部语境　internal context

组织寻求实现其目标的内部环境。

注：内部语境可能包括如下方面：

——治理、组织结构、角色和职责；

——策略、目标及其实现战略；

——在资源和知识方面的能力(例如，资本、时间、人员、过程、系统和技术)；

——信息系统、信息流和决策过程(正式的和非正式的)；

——与内部利益相关方的关系及其认知和价值观；

——组织的文化；

——组织采用的标准、指南和模型；

——合同关系的形式和范围。

[来源：GB/T 29246—2017，2.42，有修改："可以"改为"可能"等]

3.435

能力　competence

应用知识和技能实现预期结果的才能。

[来源：GB/T 29246—2017，2.11]

3.436

能力成熟度模型　capability maturity model

一种模型，该模型包含遵从一个或多个行为准则的有效过程的基本要素，并描述从临时的、不成熟的过程到有序的、成熟的、质量和有效性得到改进的过程的进化改进路径。

[来源：ISO/IEC/IEEE 24765：2017，3.472]

3.437

匿名　anonymity

对于信息，不能直接或间接识别出其主体的特性。

[来源：ISO/IEC 29100：2011，2.1，有修改]

3.438

匿名化　anonymization

通过对信息的技术处理，使信息主体无法被识别或关联，且经处理的信息不能复原的过程。

[来源：GB/T 35273—2020，3.14，有修改："个人信息"改为"信息"，删除注等]

3.439

匿名强度　anonymity strength

未经授权的实体可能从给定特征来确定真实签名者的概率值。

注：匿名强度为 n 意味着未经授权的实体可能从一个特征正确猜测到真实签名者的概率为 $1/n$。

[来源：GB/T 34953.1—2017，2.1，有修改："可以"改为"可能"、"给定签名"改为"给定特征"，"概率"改为"概率值"等]

3.440

匿名实体鉴别　anonymous entity authentication

对某一实体拥有某些特定属性的证实，但不能以此将该实体从与该实体具有相同属性的其他实体中识别出来。

[来源：GB/T 34953.1—2017，2.2，有修改]

3.441

匿名数字签名　anonymous digital signature

可利用一个组公钥或多个公钥进行验证，但不能被未经授权的实体（包括签名验证者）追踪到签名者的可区分标识符的签名。

[来源：GB/T 34953.1—2017，2.3，有修改："可以使用"改为"能利用"等]

3.442

派生密钥　derived key

由根密钥和非保密可变数据一起生成的对称密钥。

3.443

配置管理　configuration management；CM

应用技术和行政指导及监督的如下行为准则：识别和记录配置项的功能和物理特性，控制对这些特性的变更，记录和报告变更处理和实施状态，并验证是否符合规定的要求。

[来源：GB/T 18336.1—2015，3.4.3，有修改：删除注等]

3.444

配置管理系统　configuration management system

开发者在产品生存周期内开发和维护产品配置所使用的一套规程和工具（包括其文档）。

[来源：GB/T 18336.1—2015，3.4.10，有修改：删除注等]

3.445

平台配置寄存器　platform configuration register;PCR

可信计算平台中用于存储完整性度量值的存储单元。

[来源:GB/T 29828—2013,3.7,有修改:“可信平台控制模块内部”改为“可信计算平台中”]

3.446

评估　assessment

对于某一产品、系统或服务,对照某一标准,采用相应的评估方法,以建立合规性并确定其所做是否得到确保的验证。

[来源:GB/Z 29830.1—2013,2.3,有修改]

3.447

评价　evaluation

实体满足其规定准则程度的系统性判定。

[来源:GB/T 25000.2—2018,4.1]

3.448

评价对象　target of evaluation;TOE

软件、固件和/或硬件的集合,包括相关说明文档。

[来源:GB/T 18336.1—2015,3.1.70,有修改:“评估对象”改为“评价对象”,“可能附带指南”改为“包括相关说明文档”]

3.449

评价对象安全功能　TOE security functionality;TSF

正确执行安全功能要求(SFR)所依赖的评价对象(TOE)的所有硬件、软件和固件的组合功能。

[来源:GB/T 18336.1—2015,3.1.74,有修改:添加该术语的缩略语“TSF”,分别添加缩略语“TOE”“SFR”的中文全称“评价对象”“安全功能要求”]

3.450

评价对象内部传送　internal TOE transfer

在评价对象(TOE)各分离部分之间的数据通信。

[来源:GB/T 18336.1—2015,3.1.41,有修改:添加缩略语“TOE”的中文全称“评价对象”]

3.451

评价对象评价　TOE evaluation

对照所规定的准则,对评价对象(TOE)进行的评估。

[来源:GB/T 18336.1—2015,3.1.72,有修改:添加缩略语“TOE”的中文全称“评价对象”等]

3.452

评价机构　evaluation authority

开展评价活动的第三方机构。

3.453

评价技术报告　evaluation technical report

由评价者提交给评价机构的以文档形式给出总体结论及其理由的报告。

[来源:GB/T 30270—2013,3.6,有修改:“评估”改为“评价”等]

3.454

评价确保级　evaluation assurance level;EAL

由确保组件构成,代表通用准则预先界定的确保尺度上某一点的一组确保要求。

3.455

评审　review

针对实现所设立目标的主题，为确定其适宜性、充分性和有效性而采取的活动。

[来源：GB/T 29246—2017，2.65]

3.456

评审对象　review object

被评审的特定事项。

[来源：GB/T 29246—2017，2.66]

3.457

评审目标　review objective

描述评审结果所要达到的陈述。

[来源：GB/T 29246—2017，2.67]

3.458

凭证　credential

用于鉴别的身份代表。

注 1：凭证通常是为了方便与它所代表的身份相关信息的数据鉴别。数据鉴别通常用于授权。

注 2：例如，凭证表示的身份信息能打印在人类可读的媒体上，或者存储在物理令牌中。通常，这种信息能以一种旨在增强其感知有效的方式呈现。

注 3：凭证可能是用户名、带口令的用户名、个人标识码(PIN)、智能卡、令牌、指纹、护照等。

[来源：ISO/IEC 24760-1：2019，3.3.5，有修改：删除原注 1]

3.459

欺骗　spoofing

假冒成合法资源或用户的行为。

[来源：GB/T 25068.1—2020，3.38]

3.460

签名策略　signature policy

生成并验证电子签名的规则集，界定了电子签名生成和验证过程中的技术和过程要求，以满足特定的商业需求，并说明在何种情况下能确定电子签名有效。

[来源：GB/T 25065—2010，3.19，有修改："可确定"改为"能确定"]

3.461

签名过程　signature process

以消息、签名密钥和域参数作为输入，给出签名作为输出的过程。

[来源：GB/T 17902.1—1999，4.19，有修改]

3.462

签名密钥　signature key

签名过程中特定于某一实体并只能由该实体使用的私有密钥。

[来源：GB/T 17902.1—1999，4.18，有修改："秘密数据项"改为"私有密钥"]

3.463

签名密钥对　signature key-pair

由签名密钥和验证密钥组成的密钥对，其中：

——签名密钥应保持部分或完全保密，仅供签名人使用；

——验证密钥可以公开，供任何验证者使用。

[来源：ISO/IEC 20008-1：2013，2.51]

3.464

签名验证　signature verification

验证者使用签名者的公钥对数字签名进行验证的过程。

[来源：GM/T 0027—2014，3.14]

3.465

签名者　signer

生成数字签名的实体。

[来源：GB/T 17903.1—2008，3.9.34]

3.466

签名证书　signature certificate

用于证明签名公钥的数字文件。

[来源：GM/Z 4001—2013，2.90，有修改："数字证书"改为"数字文件"]

3.467

前向安全性　forward secrecy

保证通过当前或者后续数据的泄露不能破坏以前数据安全的属性。

[来源：GM/Z 4001—2013，2.91，有修改]

3.468

前向恢复　forward recovery

通过使用早期版本和记录在日志中的数据，对后期版本数据进行的数据重组。

[来源：GB/T 5271.8—2001，08.07.07]

3.469

潜在脆弱性　potential vulnerability

可疑但未经确认的弱点。

注：怀疑是借助某一假设的攻击路径去违反安全功能要求(SFR)来进行的。

[来源：GB/T 18336.1—2015，3.5.5，有修改：添加缩略语"SFR"的中文全称"安全功能要求"等]

3.470

潜在数字证据　potential digital evidence

以二进制形式存储或传输，尚未通过检查分析过程以确定与所做调查是否相关的信息或数据。

[来源：ISO/IEC 27043：2015，3.12]

3.471

强鉴别　strong authentication

借助以密码方式派生的凭证进行的鉴别。

[来源：ISO/IEC 27040：2015，3.51]

3.472

清零　zeroisation

零化

销毁存储的数据和无保护的敏感安全参数(SSP)，以防止检索和重用的方法。

[来源：ISO/IEC 19790：2015，3.134，有修改：添加缩略语"SSP"的中文全称"敏感安全参数"]

3.473

穷举攻击　exhaustive attack

通过尝试口令或密钥所有的可能值以获得真实口令或密钥的攻击方法。

[来源:GM/Z 4001—2013,2.92]

3.474

区分性标识符 distinguishing identifier

无歧义地区分出某一实体的一组字符。

[来源:ISO/IEC 11770-1:2010,2.9,有修改:“information”改译为“一组字符”]

3.475

去标识化 de-identification

通过对信息的技术处理,使其在不借助额外信息的情况下,无法识别或者关联信息主体的过程。

[来源:GB/T 35273—2020,3.15,有修改:“个人信息”改为“信息”删除注]

3.476

确保 assurance

对某一交付件满足其各项安全目的的置信度的基础工作。

注:这一定义在安全业界已得到普遍认可;而在 ISO 范围内,更普遍采用的定义是:导致在陈述中给出某一产品、过程或服务所满足要求的置信度的活动。

[来源:ISO/IEC 21827:2008,3.5,有修改:删除原注 1]

3.477

确保方法 assurance method

为获得可重复确保结果而经认可,描述如何进行确保的文件。

3.478

确保分类 assurance typing

对各种确保方法,为指明其某些确定方面的相似性而进行的分组。

3.479

确保机构 assurance authority

为使用可交付件建立信心,并有权对有关可交付件的确保做出决定(即选择、规范、接受、实施)的个人或组织。

注:在特定的模式或组织中,所用术语可能与“确保机构”有所不同,例如,有时称作“评价机构”。

3.480

确保级 assurance level

按照确保方法采用的特定尺度所达到的确保程度。

[来源:ISO/IEC 19792:2009,4.1.1,有修改:删除注]

3.481

确保阶段 assurance stage

在可交付件的生存周期中,特别关注给定的某一确保方法的阶段。

注:对可交付件的确保应考虑贯穿其生存周期的所有确保方法所产生的结果。

3.482

确保结果 assurance result

对可交付件给出的定量或定性保证的文档化陈述。

3.483

确保论据 assurance argument

清楚地表明确保需求如何得到了满足,并由证据和推理支持的结构化确保声称的集合。

[来源:ISO/IEC 21827:2008,3.6]

3.484

确保目标　assurance goal

正式和非正式的评估活动所要达到的整体安全期望。

[来源:GB/Z 29830.3—2013,2.6,有修改]

3.485

确保声称　assurance claim

某一系统满足所陈述安全需要的断言或支持性断言。

注:各声称既针对直接威胁(例如,保护系统数据不受外界攻击),也针对间接威胁(例如,使系统代码缺陷最少)。

[来源:ISO/IEC TR 15443-1:2012,3.10,有修改:删除注 2]

3.486

确保用例　assurance case

对一项或多项声称及其支持论据的表述。

注:确保用例是一种合理的、可审核的制品,用于支持声称得到满足。它包含下列各项及其关系:

——关于各性质的一项或多项声称;

——逻辑上将证据和对声称的全部假设衔接起来的论据;

——对各项声称,支持这些论据的证据和可能有的假设的主体。

[来源:ISO/IEC TR 15443-1:2012,3.9]

3.487

确保证据　assurance evidence

关于某一确保声称的判断或结论可能依据的数据。

注:证据可能由观察、测试结果、分析结果以及鉴定组成。

[来源:ISO/IEC 21827:2008,3.8]

3.488

确认　validation

通过提供客观证据,证实满足特定预期使用或应用要求的行为。

[来源:GB/T 29246—2017,2.87]

3.489

认可　accreditation

对认证机构、检查机构、实验室以及从事评审、审核等活动的人员,由认可机构对其能力和执业资格进行的合格评定活动。

3.490

认可机构　accreditation authority

完成认可并颁发认可证书的机构。

3.491

认证　certification

由认证机构证明产品、服务、管理体系符合相关技术规范或标准的合格评定活动。

3.492

认证路径　certification path

目录信息树中对象的证书序列。通过处理该序列及其起始对象的公钥,能获得末端对象的公钥。

3.493

冗余标识　redundant identity

让一个实体的标识数据增加冗余所得到的数据项序列。

3.494

蠕虫　worm

一种通过数据处理系统或计算机网络传播自身的独立程序。

注：蠕虫经常被设计用来占满可用资源，如存储空间或处理时间。

[来源：GB/T 5271.8—2001，08.05.48，有修改]

3.495

入侵　intrusion

对网络或联网系统的未授权访问，即对信息系统进行有意或无意的未授权访问，包括针对信息系统的恶意活动或对信息系统内资源的未授权使用。

[来源：GB/T 25068.1—2020，3.17]

3.496

入侵防御　intrusion prevention

积极应对以防止入侵的正规过程。

[来源：GB/T 25068.1—2020，3.20]

3.497

入侵防御系统　intrusion prevention system；IPS

特别设计用来提供主动响应能力的入侵检测系统的变体。

[来源：GB/T 28454—2020，3.19]

3.498

入侵检测　intrusion detection

检测入侵的正式过程，该过程一般特征为采集如下知识：反常的使用模式、被利用的脆弱性及其类型、利用的方式，以及何时发生和如何发生。

[来源：GB/T 28454—2020，3.17]

3.499

入侵检测和防御系统　intrusion detection and prevention system；IDPS

为了防范恶意活动而监视系统的入侵检测系统（IDS）和入侵防御系统（IPS）的软件应用或设备，IDS仅能对发现的这些活动予以报警，而IPS则有能力阻止某些检测到的入侵。

注：如果需要防范攻击，IPS将主动部署在网络中。如果部署在被动模式下，它将不能提供上述功能，其有效功能仅能像常规IDS那样提供报警。

[来源：GB/T 28454—2020，3.20，有修改]

3.500

入侵检测系统　intrusion detection system；IDS

用于识别已尝试、正在发生或已经发生的入侵的信息系统。

[来源：GB/T 28454—2020，3.18，有修改]

3.501

入侵者　intruder

针对目标主机、站点、网络或组织，正在或已经进行入侵或攻击的个人或组织。

[来源：GB/T 28454—2020，3.15，有修改："个体"改为"个人或组织"]

3.502

弱秘密　weak secret

一种能让人容易记住的秘密。

注：通常这意味着这种秘密的熵是有限的，因此，要是知道对该秘密能区分猜测对与猜测错，穷举搜索到该秘密（或字典攻击）也许是可行的。

[来源：ISO/IEC 11770-4：2017，3.38]

3.503

三元对等架构　tri-element peer architecture；TePA

引入在线第三方，实现两个实体对等鉴别的架构。

[来源：GB/T 29828—2013，3.13，有修改]

3.504

三元可扩展鉴别协议　tri-element authentication extensible protocol；TAEP

满足基于三元对等架构的访问控制技术的如下可扩展鉴别协议：采用复用模型，即鉴别协议的传输需经两次封装过程。

[来源：GB/T 29828—2013，3.15，有修改："三元对等鉴别"改为"三元对等架构"等]

3.505

散列函数　hash-function

杂凑函数

将任意长位串映射为定长位串的函数，并满足下列性质的函数：

——给定一个输出位串，寻找一个输入位串来产生该输出位串，在计算上不可行；

——给定一个输入位串，寻找另一不同的输入位串来产生相同的输出位串，在计算上不可行。

[来源：GB/T 15843.6—2018，3.6，有修改：增加同义术语中文"散列函数"，"比特"改为"位"等]

3.506

散列函数标识符　hash-function identifier

标识特定散列函数的字节。

[来源：GB/T 18238.3—2002，3.2]

3.507

设备　device

具有特定用途的机械的、电气的或电子的装置。

[来源：ISO/IEC 27040：2015，3.14]

3.508

设陷　entrapment

在数据处理系统中，通过故意设置若干明显的瑕疵，以便检测到蓄意的渗透或使入侵者弄不清该利用哪一瑕疵的防入侵措施。

[来源：GB/T 5271.8—2001，08.06.17，有修改]

3.509

射频标签　radio frequency tag

标签　tag

应答器　transponder

电子标签　electronic label

代码牌照　code plate

用于物体或物品标识，具有信息存储功能，能接收读写器的电磁场调制信号，并返回响应信号的数据载体。

[来源：GB/T 29261.3—2012，05.04.01，有修改：术语英文"RF tag"改为"radio frequency tag"]

3.510

射频模块　radio frequency module

读写器产生和接受射频信号的部分。

[来源:GB/T 29261.3—2012,05.04.10,术语英文“RF module”改为“radio frequency]

3.511

射频识别　radio frequency identification;RFID

在频谱的射频部分,利用电磁耦合或感应耦合,通过各种调制和编码方案,与射频标签交互通信唯一读取射频标签身份的技术。

[来源:GB/T 29261.3—2012,05.01.01,有修改:添加“射频识别”的缩略语“RFID”]

3.512

身份　identity

部分身份　partial identity

与某一实体相关的一组属性。

注 1:一个实体能有多个身份。

注 2:几个实体能有同一的身份。

[来源:ISO/IEC 24760-1:2019,3.1.2,有修改:删除注 3]

3.513

身份管理系统　identity management system

由策略、规程、技术和其他资源组成,用于维护身份信息(包括相关的元数据)的系统。

注:身份管理系统通常用于实体的标识或鉴别。能予以部署来支持基于身份管理系统的域中所识别的某一实体的身份信息的其他自动化决策。

[来源:ISO/IEC 24760-1:2019,3.4.8]

3.514

身份核验　identity proofing

初始实体鉴别　initial entity authentication

基于身份证据,旨在达到具体确保级的验证。

注 1:身份核验通常作为登记的组成部分来进行。在维护已登记的身份信息(例如,用户账户恢复)期间,也可能需要身份证据。

注 2:身份核验通常涉及所提供的身份信息的验证,并可能包括有可能基于生物特征识别技术的唯一性检查。

注 3:对身份核验的验证通常基于登记策略,其中包括对实体所提供的身份证据的验证准则的规范。

注 4:在进行身份核验时获得的经验证的身份信息,能包括在注册中,并能有助于日后对此实体的识别。

[来源:ISO/IEC 24760-1:2019,3.4.2]

3.515

审核　audit

审计

获取审核证据并对其进行客观评价以确定满足审核准则程度的,系统的、独立的和文档化的过程。

注 1:审核可以是内部审核(第一方)或外部审核(第二方或第三方),也可以是结合审核(结合两个或更多学科)。

注 2:“审核证据”“审核准则”在 GB/T 19011 中定义。

[来源:GB/T 29246—2017,2.5,有修改:增加同义术语中文“审计”等]

3.516

审核范围　audit scope

审核的程度和边界。

[来源:GB/T 29246—2017,2.6]

3.517

审计工具 audit tools

一种辅助分析审计日志内容的自动化工具。

[来源:GB/T 25068.1—2020,3.5]

3.518

审计日志 audit logging

以评审、分析和持续监视为目的的相关信息安全事态的数据记录。

[来源:GB/T 25068.1—2020,3.4]

3.519

渗透 penetration

绕过系统安全机制、未经授权的行为。

[来源:GB/T 28454—2020,3.21]

3.520

渗透测试 penetration testing

以未经授权的动作绕过某一系统的安全机制来检查信息系统的安全功能,以发现信息系统安全问题的手段。

3.521

生产档 production-grade

已测试完毕满足运行规范的产品、组件或软件。

[来源:ISO/IEC 19790:2015,3.95]

3.522

生产系统 production system

正常情况下支持机构日常运作的信息系统。

[来源:GB/T 30285—2013,3.1]

3.523

生存周期 life cycle

系统、产品、服务、项目或其他人造实体从概念一直到退役的演变过程。

[来源:ISO/IEC 27036-1:2014,3.4]

3.524

生日攻击 birthday attack

一种采用生日悖论的密码分析方法。

注:所谓"生日悖论"是指,随机地选择23人或23人以上时,至少两人的生日相同的概率大于50%。这与一般直觉抵触,在这种意义上称得上是个悖论,但却是个数学事实。

[来源:GM/Z 4001—2013,2.99,有修改:增加注等]

3.525

生物特征参考 biometric reference

属于生物特征数据主体并作为生物特征比对对象的一个或多个已存储的生物特征样本、生物特征模板或生物特征模型。

示例:护照上的人脸图像、身份证上的指纹细节特征点模板和数据库中的用于说话人识别的高斯混合模型。

注1:生物特征参考的产生可能或隐或显都要借助于使用辅助数据,例如,通用背景模型。

注 2：在比对中标记的主体/对象可能是任意的。在一些比对中，生物特征参考可能被用作与其他生物特征参考或输入样本进行比对的主体，并输入到生物特征比对算法中。例如，在重复注册检查中，生物特征参考被用作与数据库中的所有其他生物特征参考进行比对的主体。

[来源：GB/T 5271.37—2021，3.3.16]

3.526

生物特征模板　biometric template

参考生物特征项集合　reference biometric feature set

可直接与检测的生物特征项进行比对的已存储的生物特征项的集合。

示例：包含指纹细节点集合的记录是生物特征模板。

注 1：由原始、增强或压缩形式的图像或其他生物特征采集样本组织的生物特征参考不是生物特征模板。

注 2：生物特征项不被视为生物特征模板，除非它们被存储为参考。

[来源：GB/T 5271.37—2021，3.3.22]

3.527

生物特征模型　biometric model

由生物特征数据生成的已存储的函数。

示例：生物特征模型可以是隐马尔可夫模型、高斯混合模型或人工神经网络。

注 1：在大多数情况下，生物特征模型是一个依赖于生物特征数据主体的函数。

注 2：该函数可通过训练得到。

注 3：一个生物特征模型可能会涉及与生物特征项提取相似的中间处理过程。

[来源：GB/T 5271.37—2021，3.3.13]

3.528

生物特征识别　biometric recognition；biometrics

基于个体的生物学特性和行为特性对该个体的自动识别。

注 1：在生物特征识别领域“个体”的范围仅指人类。

注 2：Biometrics 的一般含义包括生物科学（包括相关医学科学）中各种类型数据的计数、测量和统计分析。

注 3：生物特征识别包括生物特征验证和生物特征辨识。

注 4：自动识别意味着基于机器的系统用于整个过程或有人类辅助的过程。

注 5：行为和生物学特性无法完全分开，这就是为什么该定义使用“和”而不是“和/或”的原因。例如，指纹图像是由手指脊纹的生物学特性和呈现手指的行为引起的。

注 6：弃用“鉴别”作为“生物特征验证”或“生物特征辨识”的同义词；优先术语是生物特征识别。

[来源：GB/T 5271.37—2021，3.1.3，有修改：删除注 1 中“（如本文件中所定义）”]

3.529

生物特征属性　biometric property

通过自动方式从生物特征样本估计或获得的生物特征数据主体的描述性属性。

示例：指纹可以依据脊谷的生物特征属性分为三类：弓型、箕型和环型。从人脸识别中估计的年龄或性别也是生物特征属性。

[来源：GB/T 5271.37—2021，3.3.15]

3.530

生物特征数据　biometric data

处于任何处理阶段的生物特征样本或生物特征样本的集合，例如，生物特征参考、生物特征探针、生物特征项或生物特征属性。

注：生物特征数据不需要归属于特定个体，例如，通用背景模型。

[来源：GB/T 5271.37—2021，3.3.6]

3.531

生物特征特性　biometric characteristic

个体的生物学特性和行为特性，可以从这些特性中提取有区别的、可重复的生物特征项用于生物特征识别。

示例：生物特征特性的例子有：指纹脊线结构、脸型、面部皮肤纹理构造、掌形、指形、虹膜结构、手部静脉血管结构、手掌脊状结构、视网膜图案和动态手写签名等。

[来源：GB/T 5271.37—2021，3.1.2]

3.532

生物特征项　biometric feature

从生物特征样本中提取的用于比对的数值或标记。

注 1：生物特征项是完整的生物特征项提取的输出。

注 2：该术语的使用与其在模式识别和数学领域的使用需相一致。

注 3：生物特征项集也能被看作一个处理过的生物特征样本。

注 4：生物特征项可从中间生物特征样本中提取。

注 5：应用于生物特征样本的过滤器本身不是生物特征项，如特征脸不是生物特征项，但是过滤应用于样本的输出可能是生物特征项。

[来源：GB/T 5271.37—2021，3.3.11]

3.533

生物特征验证　biometric verification

通过比对来确认生物特征声称所属个体身份的过程。

注：弃用术语“鉴别”来代替生物特征验证。

[来源：GB/T 5271.37—2021，3.8.3]

3.534

生物特征样本　biometric sample

在生物特征项提取之前的生物特征特性的模拟表示或数字表示。

示例：包含指纹图像的记录是生物特征样本。

[来源：GB/T 5271.37—2021，3.3.21]

3.535

声称方　claimant

被鉴别的本体本身或者是代表本体的实体。

注：声称方拥有其代表本体从事鉴别交换时所必需的功能和私有数据。

[来源：GB/T 15843.1—2017，3.6]

3.536

声称方参数　claimant parameter

特定于域内某一给定声称方的公开数据项、数或位串。

[来源：ISO/IEC 9798-5：2009，2.9]

3.537

剩余错误比率　residual error ratio

在给定的时间间隔内，传送不正确、丢失或者重复的数据量与传输正确的数据量之比。

[来源：GB/T 28456—2012，3.31]

3.538

失败概率　probability of failure

连接建立失败概率、传送失败概率以及连接拆除失败概率等的统称。

[来源:GB/T 28456—2012,3.32,有修改]

3.539

时变参数　time variant parameter

一种用于验证消息非重放的数据项。

示例:随机数、序列号、时间戳。

[来源:GB/T 15843.1—2017,3.36,有修改:删除注等]

3.540

时耗分析　timing analysis;TA

对某一安全功能操作在响应或执行时间上的变化进行的分析。

注:这种分析可能揭示对诸如密钥或个人标识码(PIN)等安全参数的知晓。

[来源:ISO/IEC 17825:2016,3.16,有修改:添加缩略语"PIN"的中文全称"个人标识码"等]

3.541

时间戳　time stamp;TS

对时间和其他待签名数据进行签名得到的,用于表明数据时间属性的数据。

[来源:GM/Z 4001—2013,2.100,有修改]

3.542

时间戳策略　time-stamping policy

指明时间戳令牌对具有共同安全要求的特定团体和/或应用类的适用性的规则集合。

[来源:ISO/IEC 18014-1:2008,3.23]

3.543

时间戳服务　time-stamping service;TSS

为某一数据项在某个时间点之前存在提供证据的服务。

[来源:ISO/IEC 18014-1:2008,3.18]

3.544

时间戳机构　time-stamp authority;TSA

用来产生和管理时间戳的可信服务机构。

[来源:GM/Z 4001—2013,2.101]

3.545

时间戳令牌　time-stamp token;TST

包含某一数据项的表示和时间值之间的可验证绑定关系的令牌。

注:时间戳令牌还能在绑定关系中包含附加数据项。

[来源:ISO/IEC 18014-1:2008,3.15,有修改:"data structure"改译为"令牌"]

3.546

时间戳请求方　time-stamp requester

处理需要时间戳的数据的实体。

注:时间戳请求方也可能是某一包含时间戳机构的可信第三方。

[来源:ISO/IEC 18014-1:2008,3.14]

3.547

时间戳协议　time-stamp protocol;TSP

描述时间戳的格式及相关消息格式的协议。

[来源:GM/Z 4001—2013,2.103]

3.548

时间戳验证方　time-stamp verifier

持有数据并要验证其绑定了有效时间戳的实体。

注:验证过程可由验证方本身或由可信第三方执行。

[来源:ISO/IEC 18014-1:2008,3.16]

3.549

识别 identification

在一个特定域中辨认出一个实体区别于其他实体的过程。

注 1:识别过程适用于对所声称的或观察到的属性进行验证。

注 2:标别通常是一个域中某一实体和各服务之间交互以及对资源访问的组成部分。实体在域中已知时,识别能发生多次。

[来源:ISO/IEC 24760-1:2011,3.2.1]

3.550

实体 entity

存在或者可能存在的任何具体或抽象的事物,包括这些事物间的关系。

示例:人、对象、事件、理念、过程。

注:实体的存在和与之有关的数据是否可用无关。

[来源:GB/T 5271.17—2010,17.02.05]

3.551

实体鉴别 entity authentication

证实某一实体就是所声称的实体的过程。

[来源:GB/T 15843.1—2017,3.14,有修改]

3.552

事件 incident

试图改变目标状态,并造成或可能造成损害行为的发生。

[来源:GB/T 20945—2013,3.1,有修改]

3.553

事件处理 incident handling

发现、报告、评估、响应和处理信息安全事件并总结经验的行为。

[来源:GB/T 20985.1—2017,3.6,有修改]

3.554

事件响应 incident response

为缓解或解决信息安全事件而采取的行动,包括为保护信息系统及其存储的信息并将其恢复至正常运行状态而采取的行动。

[来源:GB/T 20985.1—2017,3.7]

3.555

事件响应小组 incident response team;IRT

由组织中具备适当技能且可信的成员组成,负责在事件生存周期中处理事件的团队。

注:IRT 通常称为“计算机应急响应小组(CERT)”和“计算机安全事件响应小组(CSIRT)”。

[来源:GB/T 20985.1—2017,3.2,有修改]

3.556

事态 event

一组特定情形的发生或改变。

注 1:一个事态可能是一次或多次发生,并可能有多种原因。

注 2:一个事态可能由一些未发生的事情组成。

注 3:一个事态有时可能称为“事件”或“事故”。

[来源:GB/T 29246—2017,2.25,有修改]

3.557

适用性声明　statement of applicability;SoA

描述适用于所指组织的信息安全管理体系(ISMS)以及与该体系有关的控制目标和控制措施的文档。

注：控制目标和控制措施均基于：风险评估和风险处置过程的结果和结论，法律或规章的要求，合同义务以及该组织对于信息安全的业务需求。

3.558

收集　collect

获得对信息控制权的行为。

[来源：GB/T 35273—2020，3.5，有修改："个人信息"改为"信息"，删除注]

3.559

授权　authorization

根据预先认可的安全策略，赋予主体可实施相应行为权限的过程。

3.560

授权同意　consent

信息主体对其信息进行特定处理作出明确授权的行为。

注：包括通过积极的行为作出授权(即明示同意)，或者通过消极的不作为而作出授权(如信息采集区域内的信息主体在被告知信息收集行为后没有离开该区域)。

[来源：GB/T 35273—2020，3.7，有修改："个人信息"改为"信息"]

3.561

属性　attribute

被命名的实体性质。

[来源：GB/T 5271.17—2010，17.02.12，有修改]

3.562

属性列表　attribute list

由属性名称和属性值构成的数据列表。

[来源：GB/T 31501—2015，3.6]

3.563

数据安全性受损　data breach

导致受保护的数据在传输、存储或其他处理过程中发生意外或非法的损毁、丢失、改动或者未授权的披露或访问的安全性降低。

[来源：ISO/IEC 27040：2015，3.7]

3.564

数据保护　data protection

管理、技术或物理措施的实现，以防范未经授权访问数据。

[来源：GB/T 5271.8—2001，08.06.02，有修改：删除注]

3.565

数据服务　data service

提供数据的采集、传输、存储、处理(包括计算、分析、可视化等)、交换、销毁等数据生存形态演变的一种信息服务。

[来源：GB/T 35274—2017，3.3，有修改："网络信息服务"改为"信息服务"等]

3.566

数据共享　data sharing

让不同的数据用户能够访问大数据服务所整合的各种数据资源，并通过大数据服务或数据交换技

术对这些数据资源进行相关的计算、分析、可视化等处理的行为。

[来源:GB/T 35274—2017,3.12,有修改]

3.567

数据供应链 data supply chain

对大数据服务提供者提供的数据活动(包括采集、预处理、聚合、交换、访问等)进行计划、协调、操作、控制和优化所需的可用数据资源形成的链状结构。

注:数据供应链目标是将大数据服务所需的各种数据和系统资产,通过计划、协调、操作、控制、优化等数据活动,确保大数据服务提供者能在正确的时间,按照正确的数据服务协议发送给正确的大数据使用者。

[来源:GB/T 35274—2017,3.10,有修改]

3.568

数据恢复〈备份〉 data recovery〈backup〉

利用备份数据将目标数据还原为某一备份时间点的内容或状态的过程。

[来源:GB/T 29765—2013,3.3,有修改:增加语境标识"〈备份〉"]

3.569

数据恢复〈修复〉 data recovery〈repair〉

通过计算机专用软硬件技术,修复存储媒体内无法正常读取的数据的过程。

[来源:GB/T 31500—2015,3.3,有修改:增加语境标识"〈修复〉","存储介质"改为"存储媒体"等]

3.570

数据交换 data interchange

为满足不同系统间数据传送和处理需要,依据一定规则,实现不同系统间数据交互的过程。

[来源:GB/T 35274—2017,3.11,有修改:"平台或应用"改为"系统","原则"改为"规则","数据流动"改为"数据交互"等]

3.571

数据起源鉴别 data origin authentication

对于接收到的数据,确认其真实来源的过程。

[来源:GB/T 15843.6—2018,3.3,有修改]

3.572

数据生存周期 data lifecycle

数据从产生,经过采集、传输、存储、处理(包括计算、分析、可视化等)、交换,直至销毁等各种生存形态的演变过程。

[来源:GB/T 35274—2017,3.2,有修改:"生命周期"改为"生存周期"等]

3.573

数据损坏 data corruption

偶然或故意破坏数据完整性。

[来源:GB/T 5271.8—2001,08.05.42,有修改:"违反"改为"破坏"]

3.574

数据完整性 data integrity

数据所具有的特性,即无论数据形式作何变化,数据的准确性和一致性均保持不变。

[来源:GB/T 5271.8—2001,08.01.07]

3.575

数据元 data element

在某一语境下视为不可分的一种数据单位。

示例:数据元"人的年龄",其值由三个十进制数字的所有组合组成。

[来源:GB/T 5271.4—2000,04.07.01,有修改]

3.576

数字签名　digital signature

签名　signature

附加在数据单元上的一些数据,或是对数据单元做密码变换,这种附加数据或密码变换被数据单元的接收者用以确认数据单元的来源和完整性,达到保护数据,防止被人(例如接收者)伪造的目的。

[来源:GB/T 15843.1—2017,3.11]

3.577

数字信封　digital envelope

附加到消息中的数据,它允许消息的预期接收方验证该消息内容的完整性。

[来源:GB/T 5271.8—2001,08.06.10]

3.578

数字证据　digital evidence

以二进制形式存储或传输,且通过分析过程已确定与调查相关的信息或数据。

[来源:ISO/IEC 27042:2015,3.5,有修改:删除注 1 和注 2]

3.579

数字证书　digital certificate

由国家认可的,具有权威性、可信性和公正性的第三方证书认证机构(CA)进行数字签名的一个可信的数字化文件。

[来源:GB/T 20518—2018,3.7]

3.580

私钥　private key

非对称密码算法中只能由拥有者使用的不公开密钥。

[来源:GB/T 25056—2018,3.10]

3.581

算法　algorithm

为解决问题严格定义的有限的有序规则集。

[来源:GB/T 5271.1—2000,01.05.05]

3.582

RSA 算法　Rivest-Shamir-Adleman algorithm

一种基于大整数因子分解问题的公钥密码算法。

[来源:GM/Z 4001—2013,2.93]

3.583

SM2 算法　SM2 algorithm

由 GB/T 32918 定义的一种椭圆曲线公钥密码算法。

[来源:GB/T 25056—2018,3.14,有修改]

3.584

SM3 算法　SM3 algorithm

由 GB/T 32905 定义的一种密码杂凑算法。

[来源:GB/T 25056—2018,3.15,有修改:术语中英文名称“SM3 密码杂凑算法　SM3 cryptographic hash algorithm”改为“SM3 算法　SM3 algorithm”等]

3.585

SM4 算法　SM4 algorithm

由 GB/T 32907 定义的一种分组密码算法。

3.586

SM9 算法　SM9 algorithm

一种基于身份标识的椭圆曲线公钥密码算法。

[来源：GM/Z 4001—2013，2.122，有修改：术语中文名称“SM9 密码算法”改为“SM9 算法”，添加术语英文名称“SM9 algorithm”等]

3.587

随机数　random number

从已知的一组数中选出的一个数，该组数中，每个数出现的概率相同。

[来源：GB/T 5271.2—1988，02.03.07]

3.588

随机数生成器　random number generator

生成随机二元序列的器件或程序。

[来源：GB/T 32915—2016，2.2，有修改：术语中文名称“随机数发生器”改为“随机数生成器”]

3.589

随机数序列　random number sequence

每个数都不能只根据其前面的诸数而预知此数的数列。

[来源：GB/T 5271.2—1988，02.03.08，有修改]

3.590

随机性测试　randomness test

用于二元序列测试，能据以判断是否接受随机性原假设的函数或过程。

[来源：GB/T 32915—2016，2.4，有修改：“检测”改为“测试”等]

3.591

隧道　tunnel

在现有网络基础设施上建立的联网设备之间的数据路径。

注：可通过使用诸如协议封装、标签交换或虚电路等技术建立隧道。

[来源：GB/T 25068.1—2020，3.40]

3.592

特定权限策略　privilege policy

描述了特定权限验证者为具有资格的特定权限声明者提供/执行敏感服务的条件。

注：特定权限策略与服务相连的属性相关，也和与特权声明者相连的属性相关。

[来源：GB/T 16264.8—2005，3.3.41，有修改：“特权”改为“特定权限”等]

3.593

特定权限管理基础设施　privilege management infrastructure；PMI

支持授权服务的综合基础设施，与公钥基础设施有着密切的联系。

[来源：GB/T 16264.8—2005，3.3.40]

3.594

特洛伊木马　trojan horse

一种伪装成良性应用软件的恶意程序。

[来源:GB/T 28454—2020,3.32]

3.595

提交抗抵赖　non-repudiation of submission

旨在为交付机构已收下所传输消息提供证据的服务。

[来源:GB/T 17903.1—2008,3.9.19,有修改]

3.596

提交抗抵赖权标　non-repudiation of submission token

让原发者(发送者)或交付机构能为已提交供传输消息建立提交抗抵赖的权标。

[来源:GB/T 17903.1—2008,3.9.27,有修改:术语中英文名称“NRS 权标　NRS token”改为“提交抗抵赖权标　non-repudiation of submission token”,“数据项”改为“权标”]

3.597

添加变量　salt

盐值

作为辅助输入并入单向或加密函数,用于导出口令验证数据的随机变量。

[来源:ISO/IEC 11770-4:2017,3.33]

3.598

填充　padding

向某一数据串附加额外位的操作。

[来源:GB/T 18238.1—2000,2.6,有修改]

3.599

挑战　challenge

由验证方随机产生并发送给声称方的数据项,声称方将该数据项和其拥有的秘密信息共同产生一个响应发送给验证方。

[来源:GB/T 15843.1—2017,3.5]

3.600

通信安全　communication security

对通信网络中所传输信息的保密性、完整性和可用性等的保持。

3.601

统一威胁管理　unified threat management;UTM

通过统一部署的安全策略,融合多种安全功能,针对面向网络及应用系统的安全威胁进行综合防御的网关型设备或系统。

[来源:GB/T 31499—2015,3.1]

3.602

统一资源标识符　uniform resource identifier;URI

包含了名称或地址,指向 Web 上某一对象的短数据串。

[来源:GB/T 19771—2005,3.29,有修改]

3.603

统一资源定位符　uniform resource locator;URL

包含地址,指向 Web 上某一对象的短数据串。

注:URL 是统一资源标识符(URI)的子集。

[来源:GB/T 19771—2005,3.30,有修改:添加缩略语“URI”的中文全称“统一资源标识符”等]

3.604

透明性　transparency

系统或过程意味着开放性和可核查性的性质。

[来源:ISO/IEC 27036-3:2013,3.3]

3.605

吞吐量　throughput

丢包率为零的情况下,单位时间内传输有效数据的数量。

[来源:GB/T 28456—2012,3.30]

3.606

椭圆曲线密码算法　elliptic curve cryptography algorithm;ECC

基于有限域上椭圆曲线离散对数问题的非对称密码算法。

[来源:GM/Z 4001—2013,2.128]

3.607

外包服务　outsourcing service

服务提供方使用其自身资源来支持服务需求方业务功能的服务提供。

注 1:外包并不免除服务需求方满足所有顾客要求和法律法规要求的责任。

注 2:服务需求方对过程控制的类型和程度受下列因素影响:

a) 外包的过程对服务需求方提供满足要求的服务能力的潜在影响;

b) 对外包过程控制的分担程度。

[来源:GB/T 33770.1—2017,2.3]

3.608

外部网络　external network

在组织范围以外处理、传递公共资源的公开网络。

[来源:GB/T 31499—2015,3.4,有修改:“网络区域”改为“网络”]

3.609

外部信息系统　external information system

云计算平台之外的信息系统。

注:外部信息系统的所有权、控制权一般不由云服务商掌握,其安全措施的使用或有效性不由云服务商直接控制。

[来源:GB/T 31168—2014,3.9]

3.610

外部语境　external context

组织寻求实现其目标的外部环境。

注:外部语境可以包括如下方面:

——文化、社会、政治、法律、法规、金融、技术、经济、自然和竞争环境,无论是国际的、国家的、地区的或地方的;

——影响组织目标的关键驱动力和趋势;

——与外部利益相关方的关系及其认知和价值观。

[来源:GB/T 29246—2017,2.27]

3.611

完全备份　full backup

备份所有指定的数据对象,而不论这些数据自上次备份后是否更改过的过程。

注:完全备份是增量备份的基础。

[来源:GB/T 29765—2013,3.11]

3.612

完整性　integrity

准确和完备的性质。

[来源:GB/T 29246—2017,2.40,有修改:“特性”改为“性质”]

3.613

完整性度量　integrity measurement

在可信计算中,采用密码杂凑算法对被度量对象计算其杂凑值,并与基准值进行比对的过程。

3.614

完整性度量值　integrity measurement value

组件经杂凑算法计算后得到的杂凑值。

[来源:GB/T 29828—2013,3.3,有修改]

3.615

完整性基准值　predefined integrity value

组件在发布时或在可信状态下经度量得到的杂凑值,作为完整性校验的参考基准。

[来源:GB/T 29828—2013,3.5,有修改]

3.616

网络安全　network security

对网络环境下存储、传输和处理的信息的保密性、完整性和可用性的保持。

[来源:GB/T 20270—2006,3.1.1,有修改:“网络环境下”改为“对网络环境下”,“表征”改为“保持”]

3.617

网络安全策略　network security policy

组织为使用网络资源所制定的一组声明、规则和措施,以保护网络基础设施和服务。

[来源:GB/T 25068.1—2020,3.29]

3.618

网络钓鱼　phishing

在电子通信中,通过伪装成可信赖的实体来尝试获取隐私或保密信息的欺诈过程。

注:网络钓鱼可能会通过社会工程或技术欺骗来实现。

[来源:ISO/IEC 27032:2012,4.38]

3.619

网络分析器　network analyzer

用于观察和分析网络中信息流的软件或设备。

注:在进行信息流分析之前,常以特定的方式收集信息,例如,使用网络嗅探器。

[来源:GB/T 25068.1—2020,3.25,有修改:注中“宜”改为“常”]

3.620

网络管理　network management

对网络进行规划、设计、实施、运行、监视和维护的过程。

[来源:GB/T 25068.1—2020,3.27]

3.621

网络监视　network monitoring

连续观察和评审在网络活动和运行中所记录数据(包括日志审计、警报和分析)的过程。

[来源:GB/T 25068.1—2020,3.28]

3.622

网络空间　cyberspace

网络、服务、系统、人员、过程、组织以及驻留或穿越其中的互联数字环境。

[来源：ISO/IEC 27102:2019，3.6，有修改]

3.623

网络扫描　network scanning

对网络上在用主机进行鉴识的过程。

注：网络扫描是进行网络安全评估或实施网络攻击的前提。

3.624

网络瘫痪　network paralyzed

信息网络丧失通信功能的状态。

[来源：GB/T 31495.2—2015，3.12]

3.625

网络嗅探器　network sniffer

用于捕获网络中信息流的软件或设备。

[来源：GB/T 25068.1—2020，3.30]

3.626

网元　network element

与网络连接的信息系统。

[来源：GB/T 25068.1—2020，3.26]

3.627

网站可信标识　website trusted identity

具有唯一性、防伪造及可鉴别性质，用于描述网站真实信息的数据段。

[来源：GB/T 35287—2017，3.1，有修改：删除“简称可信标识”等]

3.628

威胁　threat

可能对系统或组织造成危害的不期望事件的潜在因素。

[来源：GB/T 29246—2017，2.83，有修改：“原由”改为“因素”]

3.629

威胁主体　threat agent

对资产施加不利行为的实体。

[来源：GB/T 18336.1—2015，3.1.71，有修改：删除“可以”]

3.630

微码　microcode

对应于可执行程序指令的处理器指令。

示例：汇编码。

[来源：ISO/IEC 19790:2015，3.71]

3.631

违规　breach

绕过计算机安全的某一元素或使其功能丧失的行为。无论是否有检测，它都可能造成数据处理系统遭到渗透。

[来源:GB/T 5271.8—2001,08.05.17,有修改:删除注等]

3.632

唯密文攻击 ciphertext-only attack

密码分析者只拥有密文进行的密码攻击。

[来源:GB/T 5271.8—2001,08.05.21,有修改]

3.633

维护 maintenance

旨在使功能单元保持在或恢复到能履行所要求功能的状态的一组活动。

[来源:GB/T 5271.14—2008,14.01.05,有修改:删除同义名称“维修”]

3.634

伪随机数序列 pseudo-random number sequence

由某种给定的算法过程来求得,但对于所要求的目的而言,能有效地用作一种随机数序列的数列。

[来源:GB/T 5271.2—1988,02.03.09,有修改]

3.635

委托 delegation

持有特定权限的实体将特定权限移交给另一个实体的过程。

[来源:GB/T 16264.8—2005,3.3.22,有修改]

3.636

委托路径 delegation path

一个有序的证书序列,将该序列与权限声称者标识的鉴别共同确认权限声称者特定权限的真实性。

[来源:GB/T 16264.8—2005,3.3.23]

3.637

位 bit

比特

二进制数字 binary digit

二进制记数制中使用的数字 0 或 1。

[来源:GB/T 5271.1—2000,01.02.08]

3.638

位串 bit string

比特串

0 或 1 的二进制数字序列。

3.639

n 位分组密码 n-bit block cipher

明文分组和密文分组的长度均为 n 位的分组密码。

[来源:ISO/IEC 10116:2017,3.9]

3.640

文档化信息 documented information

组织需要控制和维护的信息及其媒体。

注 1:文档化信息可采用任何格式,在任何媒体中,出自任何来源。

注 2:文档化信息可涉及:

——管理体系,包括相关过程;

——为组织运作所创建的信息(文档);

——所取得结果的证据(记录)。

[来源:GB/T 29246—2017,2.23,有修改:“载体”改为“媒体”,“可以采用”改为“可采用”,“可能涉及”改为“可涉及”等]

3.641

文件保护 file protection

为防止对文件未经授权访问、修改或删除而采取的适当的管理、技术或物理手段。

[来源:GB/T 5271.8—2001,08.01.08,有修改]

3.642

文件传输协议 file transfer protocol

适用于数据文件从某一计算机传输到另一计算机,以传输控制协议(TCP)为基础,应用层的互联网协议。

3.643

无线局域网鉴别与保密基础结构 wireless local area network authentication and privacy infrastructure;WAPI

由无线局域网鉴别基础结构(WAI)和无线局域网保密基础结构(WPI)组成,为无线局域网接入点、终端提供对等身份鉴别和数据机密性服务的基础结构。

[来源:GB 15629.11—2003,3.49,有修改]

3.644

物理保护 physical protection

〈密码〉采用物理手段保护密码模块、关键安全参数(CSP)和公开安全参数(PSP)的措施。

[来源:ISO/IEC 19790:2015,3.90,有修改:增加语境标识〈密码〉,分别添加缩略语“CSP”“PSP”的中文全称“关键安全参数”“公开安全参数”]

3.645

物理访问控制 physical access control

采用物理机制提供的访问控制。

示例:将计算机放在上锁的房间内。

[来源:GB/T 5271.8—2001,08.04.18,有修改]

3.646

物联网 internet of things;IoT

通过感知设备,按照约定协议,连接物、人、系统和信息资源,实现对物理和虚拟世界的信息处理并做出相应反应的智能服务系统。

注:物即物理实体。

[来源:GB/T 33745—2017,2.1.1,有修改]

3.647

误报 false positive

没有攻击或故障时检测系统却有报警的情况。

3.648

系统 system

为达到一个或多个既定目的而组织起来的相互作用元素的组合。

注:系统可被视为一种产品或其提供的服务。

[来源:ISO/IEC 27036-1:2014,3.12,有修改:删除注 2]

3.649

系统参数　system parameters

〈密码〉用于密码计算，具有如下性质的参数：包括从某一密码方案或函数族中，或者从某一数学空间族中，选择一个特定密码方案或函数。

[来源：ISO/IEC 18033-5：2015，3.17，有修改：增加语境标识〈密码〉]

3.650

系统生存周期　system life cycle

系统从其概念建立到终止使用所经过的一系列发展演变过程。

[来源：GB/T 5271.20—1994，20.01.05]

3.651

系统完整性　system integrity

系统能以不受损害的方式执行其预定功能，避免对系统故意的或意外的未经授权操作的性质。

3.652

系统用户　system user

在应用软件系统中，通过系统操作界面进行特定操作，实现对应用软件系统的特定功能进行控制的用户。

示例：应用软件系统的管理员、安全员和审计员。

注：系统用户具有一般用户所不具备的特殊权限，所以又称“特权用户”。

[来源：GB/T 28452—2012，3.1.15，有修改]

3.653

线性密码分析　linear cryptanalysis

一种分析明文、密文和密钥之间的若干位的线性关系来进行密码攻击的方法。

[来源：GM/Z 4001—2013，2.132，有修改：“比特”改为“位”等]

3.654

相互鉴别　mutual authentication

实体双方均向对方提供身份保证信息的鉴别机制。

[来源：GB/T 15843.1—2017，3.18，有修改]

3.655

相互匿名鉴别　mutual anonymous authentication

双方实体均向对方提供实体身份合法性保证的匿名实体鉴别。

[来源：GB/T 34953.1—2017，2.11，有修改：术语中文名称“双向匿名鉴别”改为“相互匿名鉴别”等]

3.656

响应　response

当攻击或入侵发生时，针对信息系统及所存储数据采取保护措施并恢复正常运行环境的行为。

[来源：GB/T 20275—2013，3.8，有修改]

3.657

响应者　responder

提供在线证书状态查询服务的主体。

[来源：GB/T 19713—2005，3.4]

3.658

消息　message

任意有限长度的位串。

[来源:GB/T 32918.2—2016,3.1,有修改:“比特”改为“位”]

3.659

消息代表　message representative

作为消息的函数导出,并与私密签名密钥结合而产生签名的位串。

[来源:ISO/IEC 9796-2:2010,3.9]

3.660

消息鉴别码　message authentication code;MAC

消息鉴别码算法输出的位串。

[来源:GB/T 15843.6—2018,3.8,有修改:“比特”改为“位”等]

3.661

消息鉴别码算法　message authentication code algorithm

输入为密钥和消息,输出为一个固定长度的位串的算法,满足下面两个性质:

——对于任何密钥和消息,消息鉴别码(MAC)算法都能够快速有效地计算;

——对于任何固定的密钥,攻击者在没有获得密钥信息的情况下,即使获得了一些(消息,MAC)对,对任何新的消息预测其 MAC 在计算上是不可行的。

注 1:MAC 算法有时被称为“密码校验函数”。

注 2:计算不可行性依赖于使用者具体的安全要求及其环境。

[来源:GB/T 15852.1—2020,3.11,有修改:“比特”改为“位”,添加缩略语“MAC”的中文全称“消息鉴别码”等]

3.662

消息鉴别码算法密钥　MAC algorithm key

用于控制消息鉴别码算法运算的密钥。

[来源:GB/T 15852.1—2020,3.12,有修改:术语中文“MAC 算法密钥”改为“消息鉴别码算法密钥”]

3.663

消息摘要　message digest

散列/杂凑算法的最终输出值。

3.664

校验值　check-value

由校验值函数计算,并由数据原发者发送给数据接收者,以使接收者能以此检查该数据的正确性的位串。

3.665

校验值函数　check-value function

函数 f,将一个位串和一个短密钥(即能容易地被输入到用户设备或从中读取的密钥)映射为一个定长位串,该函数满足以下性质:

——对于任何密钥 k 和任何位串 d,函数 $f(d,k)$ 均能被有效计算;

——寻找两个不同的位串 (d,d'),使 $f(d,k)=f(d',k)$ 在计算上不可行,尽管能满足上述等式的 k 在其取值空间中并非一小部分。

注:在实践中,典型的短密钥包含 4 个~6 个数字或字母。

[来源:GB/T 15843.6—2018,3.2,有修改:“检验函数”改为“校验值函数”,“比特串”改为“位串”,“定长为 b 位的检验值”改为“定长位串”,“属性”改为“性质”,“可容易地”改为“能容易地”,“可以被有效

计算”改为“均能被有效计算”等]

3.666

校验字符　check character

可通过某一串的数学关系来验证其正确性所使用的附加字符。

[来源:GB/T 17710—2008,2.1,有修改]

3.667

校验字符体系　check character system

产生串的校验字符且使用校验字符对该串进行校验的一组规则。

[来源:GB/T 17710—2008,2.2,有修改]

3.668

DH 协议　Diffie-Hellman protocol

一种基于离散对数问题、用于密钥协商的密码协议。

[来源:GM/Z 4001—2013,2.14,有修改:术语中文名称“Diffie-Hellman 协议”改为“DH 协议”等]

3.669

协议封装　protocol encapsulation

通过传输包裹在另一协议内的协议数据单元,将一个数据流封装在另一数据流中的过程。

注:在虚拟专用网(VPN)技术中,这种方法可用于建立隧道。

3.670

泄露　disclosure

违反信息安全策略,导致数据被未经授权的实体使用的行为。

[来源:GB/T 5271.8—2001,08.05.15,有修改]

3.671

信任　trust

在两个实体和/或元素之间,由一组活动和某一安全策略组成的如下关系:元素 x 信任元素 y,当且仅当 x 确信 y 会以一种良好界定的方式(关于各项活动)行事,不会违反给定的安全策略。

[来源:ISO/IEC 27036-1:2014,3.13]

3.672

信任链　trust chain

在计算系统启动和运行过程中,使用完整性度量方法在部件之间所建立的信任传递关系。

[来源:GB/T 29827—2013,3.19]

3.673

信息安全　information security

对信息的保密性、完整性和可用性的保持。

注:另外,也可包括诸如真实性、可核查性、抗抵赖和可靠性等其他性质。

[来源:GB/T 29246—2017,2.33,有修改:注中的“其他特性”改为“其他性质”]

3.674

信息安全保障　information security assurance

对信息和信息系统的安全属性及功能、效率进行保障的一系列适当行为或过程。

[来源:GB/T 31495.1—2015,3.1]

3.675

信息安全保障措施　measures for information security assurance

为达到信息安全目的所采用的保障手段的集合。

[来源:GB/T 31495.1—2015,3.3]

3.676

信息安全保障能力　capability of information security assurance

被保障实体安全防御、响应和恢复等特性的体现。

[来源:GB/T 31495.1—2015,3.4]

3.677

信息安全保障评价　evaluation of information security assurance

收集信息安全保障证据,并获得信息安全保障值的过程和途径。

[来源:GB/T 31495.1—2015,3.2]

3.678

信息安全保障效果　effects of information security assurance

被保障实体的信息安全保障目标和属性的实现程度。

[来源:GB/T 31495.1—2015,3.5]

3.679

信息安全产品　information security product

专门用于保障信息安全的软件、硬件或其组合。

[来源:GB/T 25066—2020,3.1]

3.680

信息安全持续性　information security continuity

保障信息安全持续运行的过程和规程。

[来源:GB/T 29246—2017,2.34,有修改:“确保”改为“保障”]

3.681

信息安全风险　information security risk

特定威胁利用单个或一组资产脆弱性的可能性以及由此可能给组织带来的损害。

注:它以事态的可能性及其后果的组合来度量。

[来源:GB/T 31722—2015,3.2]

3.682

信息安全服务　information security service

面向组织或个人的各类信息安全需求和信息安全保障需求,由服务提供方按照服务协议所执行的信息安全过程或任务。

注 1:信息安全服务通常是基于信息安全技术、产品或管理体系,通过外包的形式,由专业信息安全人员所提供的支持和帮助。

注 2:信息安全服务通常以信息安全服务提供方和信息安全服务需求方之间的服务项目方式进行。

[来源:GB/T 32914—2016,3.1,有修改]

3.683

信息安全管理体系　information security management system;ISMS

基于业务风险方法,建立、实施、运行、监视、评审、保持和改进信息安全的体系。

注 1:信息安全管理体系是一个组织整个管理体系的组成部分。

注 2:信息安全管理体系包括组织结构、方针策略、规划活动、职责、实践、规程、过程和资源。

3.684

信息安全事件　information security incident

与可能危害组织资产或损害其运行相关的、单个或多个被识别的信息安全事态。

[来源:GB/T 20985.1—2017,3.4]

3.685

信息安全事件管理　information security incident management

采用一致和有效方法处理信息安全事件的行为。

[来源:GB/T 20985.1—2017,3.5]

3.686

信息安全事态　information security event

表明可能的信息安全违规或某些控制失效的发生。

[来源:GB/T 20985.1—2017,3.3,有修改]

3.687

信息安全调查　information security investigation

为帮助理解信息安全事件而进行的检查、分析和解释。

[来源:GB/T 20985.1—2017,3.1]

3.688

信息安全意识　information security awareness

人们面对有可能对个人或组织造成损失的外在环境条件的戒备心态。

[来源:GB/T 31495.2—2015,3.9,有修改:删除“人们对信息安全现实的高级心理反应形式”,“戒备”改为“戒备心态”]

3.689

信息安全治理　governance of information security

指导和控制组织信息安全活动的体系。

[来源:GB/T 32923—2016,3.3]

3.690

信息处理设施　information processing facilities

任何信息处理系统、服务或基础设施,或者其安置的物理设施。

[来源:GB/T 29246—2017,2.32,有修改:“位置”改为“设施”]

3.691

信息共享社团　information sharing community

同意共享信息的组织群体。

注:组织可为一个人。

[来源:GB/T 29246—2017,2.38,有修改]

3.692

信息技术　information technology;IT

信息通信技术　information and communication technology;ICT

为采集、表示、处理、传输、交换、描述、管理、组织、存储、检索、输出数字信息而开发、维护和使用的技术。

3.693

信息技术产品　information technology product

具有采集、处理、传输、交换、控制、存储、检索、输出数据或信息功能的硬件、软件、系统和服务。

注:信息技术产品包括计算机及其辅助设备、通信设备、网络设备、自动控制设备、操作系统、数据库、应用软件与服务等。

[来源:GB/T 32921—2016,3.1,有修改:“采集、存储、处理、传输、控制、交换、显示”改为“采集、处理、传输、交换、控制、存储、检索、输出”]

3.694

信息技术产品安全检测机构 security testing bodies of information technology products

从事信息技术产品安全检测活动的机构。

注:信息技术产品安全检测机构可以是一个组织,或是一个组织的一部分。

[来源:GB/T 35280—2017,3.3,有修改:“第三方机构”改为“机构”,删除注 2]

3.695

信息技术产品供应方 information technology product supplier

提供信息技术产品的组织。

注:信息技术产品供应方包括生产商、销售商、代理商、集成商、服务商等。

[来源:GB/T 32921—2016,3.2]

3.696

信息系统 information system

应用、服务、信息技术资产或其他信息处理组件的组合。

[来源:GB/T 29246—2017,2.39,有修改:句尾增加“的组合”]

3.697

信息需要 information need

对目标、风险和问题进行管理所需的了解。

[来源:GB/T 29246—2017,2.31,有修改]

3.698

性能 performance

一种可测量的属性。

注 1:性能可与定量或定性的调查发现相关。

注 2:性能可与活动、过程、产品(包括服务)、系统或组织的管理相关。

[来源:GB/T 29246—2017,2.59,有修改:“可测量的结果”改为“一种可测量的属性”]

3.699

嗅探器 sniffer

一种用于捕获计算机网络中流动信息的程序或设备。

注 1:黑客能利用嗅探器来捕获信息,例如,用户身份名和密码。

注 2:网络运行维护人员可合法地利用嗅探器来排查网络中的问题。

3.700

虚拟机 virtual machine;VM

一种虚拟的数据处理系统,它看起来是在某个特定用户的独立使用下,但其功能是通过共享真实数据处理系统的各种资源得以实现的。

[来源:GB/T 5271.1—2000,01.01.50,有修改]

3.701

虚拟专用网 virtual private network;VPN

一种在公共通信基础网络上通过逻辑方式隔离出来的网络。

[来源:GB/T 32922—2016,3.3]

3.702

序号 sequence number

其值取自在一定时期内不重复出现的特定序列数的一种参数。

[来源:GB/T 15843.1—2017,3.32,有修改:删除注等]

3.703

序列密码　stream cipher algorithm

流密码算法

对明文逐位逐字符运算的一种对称密码算法。

[来源:GM/Z 4001—2013,2.136,有修改:增加同义名称“流密码算法”,“逐比特/字符”改为“逐位逐字符”等]

3.704

选择密文攻击　chosen-ciphertext attack

一种选择特定密文和对应明文进行分析的密码攻击方法。

[来源:GM/Z 4001—2013,2.138]

3.705

选择明文攻击　chosen-plaintext attack

一种选择特定明文和对应密文进行分析的密码破译攻击方法。

[来源:GM/Z 4001—2013,2.139]

3.706

延迟　latency

在实时信息通信系统中,由安全机制引入的时延。

[来源:ISO/IEC 29192-1:2012,2.5,有修改:“communication systems”改译为“信息通信系统”,“cryptographic mechanism”改为“安全机制”]

3.707

验证　verification

通过提供客观证据,证实满足规定要求的行为。

注:又可称“符合性测试”。

[来源:GB/T 29246—2017,2.88,有修改]

3.708

验证方　verifier

要求鉴别其他实体身份的实体本身或其代表。

注:验证方包含了从事鉴别交换所必需的功能。

[来源:GB/T 15843.1—2017,3.40,有修改]

3.709

验证过程　verification process

输入签名消息、验证密钥和域参数,输出签名验证结果(有效或无效)的过程。

[来源:GB/T 17902.1—1999,4.23,有修改:“验证进程”改为“验证过程”等]

3.710

验证函数　verification function

用于验证两个数据集合完全相同的函数。

注1:两个不完全相同的数据集合不会从验证函数产生完全相同的匹配值。

注2:验证函数通常利用诸如 MD5、SHA1 等散列函数来实现,但也可利用其他方法。

[来源:ISO/IEC 27037:2012,3.25]

3.711

验证密钥　verification key

在数学上与实体的签名密钥相关,并由验证方在验证过程中使用的公开数据元素集。

[来源:GB/T 17902.1—1999,4.22,有修改]

3.712

要求　requirement

明示的、通常隐含的或强制性的需要或期望。

注 1:“通常隐含的”意指所考虑的需要或期望是不言而喻的,对于组织和利益相关方是惯例或常见做法。

注 2:某一指定要求是明示的,例如在文档化信息中明示。

[来源:GB/T 29246—2017,2.63,有修改]

3.713

业务功能　business function

满足信息主体的具体使用需求的服务类型。

注:如地图导航、网络约车、即时通信、网络社区、网络支付、新闻信息、网上购物、快递配送、交通票务等。

[来源:GB/T 35273—2020,3.17,有修改:“个人信息主体”改为“信息主体”,“即时通讯”改为“即时通信”,“新闻资讯”改为“新闻信息”]

3.714

业务连续性管理　business continuity management

识别对组织的潜在威胁及其一旦发生可能对业务运行所带来影响的整套管理过程,该过程为建立具有有效响应能力的组织韧性提供框架,以保护其关键相关方利益、声誉、品牌以及价值创造活动。

[来源:GB/T 30146—2013,3.4,有修改]

3.715

业务影响分析　business impact analysis

对活动和业务中断可能带来影响的分析过程。

[来源:GB/T 30146—2013,3.8,有修改]

3.716

一致性　consistency

在某一系统或组件的各文档或各部分之间的一致性、标准化和无矛盾的程度。

[来源:ISO/IEC 21827:2008,3.14]

3.717

依赖(证书)方　relying party

依赖证书中的数据来做决定的用户或代理。

[来源:GB/T 16264.8—2005,3.3.46]

3.718

依赖方协议　relying party agreement

证书认证机构与依赖方共同签署,通常规定在验证数字签名或其他使用证书过程中有关方所拥有权利和义务的约定。

[来源:GB/T 26855—2011,3.12,有修改]

3.719

移动终端　mobile terminal

可移动的便携式计算设备。

注:移动终端包括带有无线上网功能的智能移动通信终端、平板式计算机、便携式计算机。

[来源:GB/T 35282—2017,3.1,有修改:“手机”改为“移动通信终端”,“平板”改为“平板式计算机”,“笔记本电脑”改为“便携式计算机”等]

3.720

已签消息　signed message

由签名、无法从该签名恢复的消息部分和可选文本字段组成的一组数据元素。

[来源:GB/T 17902.1—1999,4.20,有修改:“已签名消息”改为“已签消息”,删除注等]

3.721

已知明文攻击　known-plaintext attack

一种利用大量互相对应的明文和密文进行分析的密码攻击方法。

[来源:GM/Z 4001—2013,2.140]

3.722

易失性存储　volatile storage

断电后无法保有其内容的存储。

[来源:ISO/IEC 27040:2015,3.53]

3.723

易失性数据　volatile data

特别容易变化或能轻易修改的数据。

注:变化可能源自切断电源或穿过磁场。易失性数据还包括随系统状态变化而变化的数据。例如,存储在随机存取存储器(RAM)中的数据和动态的互联网协议(IP)地址。

[来源:ISO/IEC 27037:2012,3.26,有修改:分别添加缩略语“RAM”“IP”的中文全称“随机存取存储器”“互联网协议”]

3.724

隐蔽信道　covert channel

一种能用于以违背安全策略的方式传送数据的传输信道。

[来源:GB/T 5271.8—2001,08.05.45,有修改]

3.725

影响　impact

对所达到业务目标的不利改变。

注:在信息安全中,一般指不测事件的后果。

[来源:GB/T 31722—2015,3.1,有修改:添加注]

3.726

应对措施　countermeasure

为最小化脆弱性而设计的行动、装置、过程、技术或其他措施。

[来源:GB/T 5271.8—2001,08.06.03,有修改]

3.727

应急响应　emergency response

组织为应对突发/重大信息安全事件发生所做的准备,以及在事件发生后所采取的措施。

[来源:GB/T 24363—2009,3.4,有修改]

3.728

应急响应计划　emergency response plan

组织为应对突发/重大信息安全事件而编制的,对业务运行(包括信息系统运行)进行维持或恢复的策略和规程。

[来源:GB/T 24363—2009,3.5,有修改]

3.729

应急演练　emergency drill

为训练有关人员和提高应急响应能力而根据应急预案和应急响应计划所开展的活动。

[来源:GB/T 31495.2—2015,3.10,有修改]

3.730

应用软件　application software

应用程序　application program

专门解决应用问题的软件或程序。

注:应用软件不同于控制计算机本身的软件。

示例:电子表格程序。

[来源:GB/T 5271.1—2000,01.04.01,有修改:添加注]

3.731

应用软件系统　application software system

信息系统中对特定业务进行处理的软件系统。

[来源:GB/T 28452—2012,3.1.1,有修改]

3.732

硬件　hardware

信息处理系统物理组成部分的全部或部分。

示例:计算机、外围设备。

[来源:GB/T 5271.1—2000,01.01.07]

3.733

用户　user

使用产品和服务的个人、组织、设备或程序等任何实体。

[来源:GB/T 30276—2020,3.1,有修改:删除“网络”,添加“设备或程序等任何实体”]

3.734

用户标识　user ID;user identification

信息系统用于标识用户的一种字符串或模式。

[来源:GB/T 5271.8—2001,08.04.22,有修改]

3.735

用户画像　user profiling

通过收集、汇聚、分析个人信息,对某特定自然人个人特征,如职业、经济、健康、教育、个人喜好、信用、行为等方面作出分析或预测,形成其个人特征模型的过程。

注:直接使用特定自然人的个人信息,形成该自然人的特征模型,称为“直接用户画像”。使用来源于特定自然人以外的个人信息,如其所在群体的数据,形成该自然人的特征模型,称为“间接用户画像”。

[来源:GB/T 35273—2020,3.8]

3.736

用户数据　user data

由用户产生或为用户服务的数据。

[来源:GB/T 30284—2020,3.1.12]

3.737

用户相关信息　user related information

与自然人或法人有关的信息以及界定和描述这些信息的数据。

注：用户相关信息包括用户身份信息，用户生成的文档、程序、多媒体资料，用户通信的内容、地址、时间，产品的配置、运行及位置数据，系统运行过程产生的日志等。

[来源：GB/T 32921—2016，3.3，有修改]

3.738

有效性　effectiveness

实现所计划活动和达成所计划结果的程度。

[来源：GB/T 29246—2017，2.24]

3.739

预警　warning

针对即将或正在发生的网络安全事件或威胁，提前或及时发出的警示。

[来源：GB/T 32924—2016，3.5，有修改："网络安全事件"改为"信息安全事件"]

3.740

预签名　pre-signature

在签名生成过程中，由随机数发生器产生的，与消息独立的八位字节串。

[来源：GB/T 15851.3—2018，3.10，有修改]

3.741

域　domain

〈网络〉在单一安全策略下运行的一组实体。

示例：由单一机构或一组采用同一安全策略的机构创建的公钥证书。

[来源：ISO/IEC 14888-1：2008，3.4，有修改：增加语境标识"〈网络〉"]

3.742

域　field

〈数学〉一个如下元素集合：连同该集合上加法和乘法的二元运算，使得通常的域公理适用。

[来源：ISO/IEC 18033-2：2006，3.19]

3.743

域参数　domain parameter

对域中所有实体都是公共的且已知的或者可访问的数据元素。

[来源：GB/T 17902.1—1999，4.6，有修改]

3.744

域名　domain name

域名系统名字空间中，从当前节点到根节点的路径上所有节点标记以点分顺序连接的字符串。

示例：域名"www.bj.cn"。

[来源：GB/T 33562—2017，3.3，有修改]

3.745

域名系统　domain name system

一种将域名映射为某些预定义类型资源记录的分布式互联网服务系统。

注：网络中域名服务器之间通过相互协作，实现将域名最终解析到相应的资源记录。

[来源：GB/T 33562—2017，3.1，有修改：删除定义中的英文等]

3.746

元数据　metadata

关于数据或数据元素的数据（可能包括其数据描述），以及关于数据拥有权、存取路径、访问权和数

据易变性的数据。

[来源:GB/T 5271.17—2010,17.06.05]

3.747

原发抗抵赖　non-repudiation of origin

旨在防止原发者不实否认其已创建消息内容并已发送消息的服务。

[来源:GB/T 17903.1—2008,3.9.16,有修改]

3.748

原发抗抵赖权标　non-repudiation of origin token

允许接收者为某一消息建立原发抗抵赖的数据项。

[来源:GB/T 17903.1—2008,3.9.26,有修改]

3.749

原发者　originator

向接收者发送消息,或者使消息具有抗抵赖性的实体。

[来源:GB/T 17903.1—2008,3.9.29,有修改:“产生有待于对其提供抗抵赖服务的消息”改为“使消息具有抗抵赖性”]

3.750

远程访问　remote access

从另一网络或从一个终端设备访问网络资源的过程,这种访问通过物理的或逻辑的方式且不会永久连接所访问的资源。

[来源:GB/T 25068.1—2020,3.32]

3.751

远程用户拨入鉴别服务　remote authentication dial-in user service;RADIUS

一种用于鉴别远程拨号入网用户的互联网安全协议。

3.752

远程用户　remote user

通过远程访问获取网络资源的用户。

3.753

云服务　cloud service

云计算服务　cloud computing service

通过云计算已定义的接口提供的一种或多种能力。

[来源:GB/T 32400—2015,3.2.8,有修改:增加同义术语中英文“云计算服务　cloud computing service”]

3.754

云服务客户　cloud service customer

为使用云计算服务而处于一定业务关系的参与方。

注:业务关系不一定包含经济条款。

[来源:GB/T 32400—2015,3.2.11]

3.755

云服务审计者　cloud service auditor

负责审计云服务的供应与使用(包括运营、性能与安全)的独立第三方审计机构。

[来源:GB/T 35279—2017,3.5,有修改:“云审计者　cloud auditor”改为“云服务审计者　cloud

service auditor”等]

3.756

云服务提供者　cloud service provider

提供云服务的参与方。

[来源:GB/T 32400—2015,3.2.15]

3.757

云计算　cloud computing

一种通过网络将可伸缩、弹性的共享物理和虚拟资源池以按需自服务的方式供应和管理的模式。

注:资源包括服务器、操作系统、网络、软件、应用和存储设备等。

[来源:GB/T 32400—2015,3.2.5]

3.758

云计算环境　cloud computing environment

云服务商提供的云计算平台以及客户在云计算平台之上部署的软件和有关组件的集合。

[来源:GB/T 31167—2014,3.8,有修改]

3.759

云计算基础设施　cloud computing infrastructure

由硬件资源和资源抽象控制组件构成,支撑云计算的基础设施。

注:硬件资源包括所有的物理计算资源,包括服务器(中央处理器(CPU)、内存等)、存储组件(硬盘等)、网络组件(路由器、防火墙、交换机、网络链路和接口等)及其他物理计算基础元素。资源抽象控制组件对物理计算资源以软件来抽象化,云服务商通过这些组件提供和管理对物理计算资源的访问。

[来源:GB/T 31167—2014,3.6,有修改:添加缩略语“CPU”的中文全称“中央处理器”等]

3.760

云计算平台　cloud computing platform

云服务商提供的云计算基础设施及其上的服务软件的集合。

[来源:GB/T 31167—2014,3.7]

3.761

运行环境　operational environment

〈密码〉密码模块安全运行所需要的各种软件、固件和硬件的集合。其中包括操作系统和硬件平台。

注:运行环境分为可修改的、不可修改的以及受限制的。

[来源:GB/T 37092—2018,3.12,有修改:增加语境标识〈密码〉等]

3.762

运行控制　operational controls

对某一信息系统,主要通过人员(与系统相对)来实现并执行的各种安全控制(即保护措施和对策)。

[来源:ISO/IEC TR 19791:2010,3.4]

3.763

运行系统　operational system

处于特定运行环境中的信息系统(包括其非信息技术部分)。

3.764

杂凑值　hash value

密码杂凑运算的结果。

[来源:GM/Z 4001—2013,2.141]

3.765

灾难备份中心　backup center for disaster recovery

备用站点　alternate site

灾难发生后用于接替主系统进行数据处理并支持关键业务功能运作的场所。

注：灾难备份中心能提供备用的系统、基础设施、专业技术支持及运行维护管理能力，并能为此场所内或周边提供备用的生活设施。

[来源：GB/T 20988—2007，3.1，有修改]

3.766

灾难恢复　disaster recovery

为了将信息系统从灾难造成的故障或瘫痪状态恢复到可正常运行状态，并将其支持的业务功能从灾难造成的不正常状态恢复到可接受状态，而设计的活动和流程。

[来源：GB/T 20988—2007，3.9]

3.767

灾难恢复计划　disaster recovery plan

信息系统灾难恢复过程中筹划所需的任务、行动、数据和资源，用于指导相关人员在预定的灾难恢复目标内恢复信息系统所支持关键业务功能的文件。

3.768

增量备份　incremental backup

仅备份自上次备份后更改过的数据对象。

注：包括累积增量备份和差分增量备份。

[来源：GB/T 29765—2013，3.12]

3.769

真实性　authenticity

一个实体是其所声称实体的性质。

[来源：GB/T 29246—2017，2.8，有修改]

3.770

整改措施　corrective action

消除不符合根源以防再次发生的措施。

[来源：GB/T 29246—2017，2.19，有修改："成因"改为"根源"]

3.771

正确性　correctness

针对所规定的各项安全要求，某一产品或系统展现其正确实现这些要求的性质。

[来源：ISO/IEC 21827：2008，3.15]

3.772

证据　evidence

凭自身或与其他信息结合，用于就某一事件或动作确立证明的信息。

注：证据未必证明某事的真实或存在(见证明)，但能有助于这种证明的确立。

[来源：GB/T 17903.1—2008，3.9.5，有修改]

3.773

证据篡改　spoliation

对潜在的数字证据进行或允许改变以降低其证据价值的行动。

[来源:ISO/IEC 27037:2012,3.19]

3.774

证据生成者　evidence generator

产生抗抵赖证据的实体。

[来源:GB/T 17903.1—2008,3.6.1]

3.775

证据验证者　evidence verifier

验证抗抵赖证据的实体。

[来源:GB/T 17903.1—2008,3.6.3]

3.776

证据用户　evidence user

使用抗抵赖证据的实体。

[来源:GB/T 17903.1—2008,3.6.2]

3.777

证据主体　evidence subject

对某一行动负责或与某一事件关联,并对其生成证据的实体。

[来源:GB/T 17903.1—2008,3.9.7,有修改]

3.778

证明　proof

按照有效的抗抵赖策略,对证据有效性的证实。

注:证明是用于提供某事真实或存在的证据。

[来源:GB/T 17903.1—2008,3.9.30,有修改]

3.779

证书　certificate

关于实体的一种数据,该数据由认证机构的私钥或秘密密钥签发,并无法伪造。

[来源:GB/T 37092—2018,3.1]

3.780

证书策略　certificate policy

指明证书对于具有普通安全需求的特定团体和/或应用类的适用性的规则集合。

示例:特定的证书策略能指明某一类型的证书对一定价格幅度下商品交易的电子数据处理的认证适用性。

[来源:GB/T 25056—2018,3.3,有修改:“注”改为“示例”等]

3.781

证书撤销列表　certificate revocation list;CRL

由证书认证机构(CA)签发并发布的被撤销证书的列表。

[来源:GM/Z 4001—2013,2.144]

3.782

证书撤销列表分发点　CRL distribution point

一个证书撤销列表(CRL)目录项或其他 CRL 分发源。所分发的 CRL 可只含有某证书认证机构(CA)所颁发证书全集中某一子集的撤销项,也可包括有多个 CA 的撤销项。

[来源:GB/T 20518—2018,3.6,有修改:分别添加缩略语“CRL”“CA”的中文全称“证书撤销列表”

“证书认证机构”等]

3.783

证书持有者　certificate holder

与有效证书的主体相对应的实体。

[来源:GB/T 19714—2005,3.3,有修改]

3.784

证书确认　certificate validation

按照验证策略确认证书有效性和真实性的过程。

[来源:GM/Z 4001—2013,2.147,有修改:术语中文“证书验证”改为“证书确认”]

3.785

证书认证机构　certificate authority;CA

电子认证服务机构

对数字证书进行全生存周期管理的实体。

[来源:GB/T 25056—2018,3.5,有修改:添加“证书认证机构”的缩略语“CA”,“生命周期”改为“生存周期”等]

3.786

证书认证机构证书　CA certificate

由上一级 CA 颁发给下一级 CA 的证书。

示例:根 CA 颁发给运行 CA 的证书。

3.787

证书认证系统　certificate authentication system

对数字证书的签发、发布、更新、撤销等数字证书全生存周期进行管理的系统。

[来源:GM/Z 4001—2013,2.146,有修改:“生命周期”改为“生存周期”]

3.788

证书序列号　certificate serial number

在某一证书认证机构所签发的证书中用于唯一标识数字证书的一个整数。

[来源:GB/T 25056—2018,3.8,有修改]

3.789

证书依赖方　certificate relying party

依赖于证书真实性的实体。

[来源:GB/T 35289—2017,3.10]

3.790

证书用户　certificate user

具有并使用数字证书的实体。

3.791

证书注册机构　certificate registration authority;RA

受理数字证书的申请、更新、恢复和注销等业务的实体。

[来源:GM/Z 4001—2013,2.148,有修改:在“registration authority”前增加“certificate”]

3.792

知晓抗抵赖　non-repudiation of knowledge

旨在防止接收者不实否认其已关注到所收到消息内容的服务。

[来源:GB/T 17903.1—2008,3.9.15,有修改:“认知抗抵赖”改为“知晓抗抵赖”等]

3.793

执行管理层　executive management

由组织治理者委派,负有实现战略和策略以达成组织目标责任的个人或小组。

注1:执行管理层是最高管理层的组成部分。为了明晰角色,在最高管理层内区分了两个群体:治理层和执行管理层。

注2:执行管理层可能包括首席执行官/行政总裁(CEO)、政府机构领导、首席财务官/财务总监(CFO),首席运营官/运营总监(COO),首席信息官/信息总监(CIO),首席信息安全官员/信息安全总监(CISO)以及类似的角色。

[来源:GB/T 32923—2016,3.1,有修改]

3.794

职责分离　separation of duties

为使单独行动的个人只能危及信息系统有限部分的安全而对敏感信息的分权制衡。

[来源:GB/T 5271.8—2001,08.06.16,有修改:术语中文“责任分开”改为“职责分离”等]

3.795

指标　indicator

提供估算或评价的测度。

[来源:GB/T 29246—2017,2.30,有修改]

3.796

治理层　governing body

对组织的绩效和合规负有责任的个人或小组。

注:治理层是最高管理层的组成部分。为了明晰角色,在最高管理层内区分了两个群体:治理层和执行管理层。

[来源:GB/T 32923—2016,3.2,有修改]

3.797

智能卡　smart card

具有中央处理器的集成电路卡。

注:从数据传输方式上可分为接触式智能卡和非接触式智能卡。

[来源:GB/T 36950—2018,3.2]

3.798

智能移动终端　smart mobile terminal

能接入通信网,提供应用软件开发接口,并能安装和运行应用软件的移动终端。

[来源:GB/T 32927—2016,3.1.9,有修改:术语中英文“移动智能终端　mobile smart terminal”改为“智能移动终端　smart mobile terminal”,“移动通信网”改为“通信网”等]

3.799

中间人攻击　man-in-the-middle attack

一种拦截并选择性修改通信数据以冒充通信中合法实体的攻击方法。

[来源:GM/Z 4001—2013,2.151,有修改]

3.800

终端实体　end entity

不以签署证书为目的而使用其私钥的证书主体或依赖(证书)方。

[来源:GB/T 16264.8—2005,3.3.25,有修改]

3.801

终端实体证书　entity certificate

用户证书

由证书认证机构签发的个人证书、机构证书、设备证书等。

[来源：GM/T 0015—2012，3.4，有修改："数字证书认证机构"改为"证书认证机构"等]

3.802

重要信息系统　critical information systems

关系国家安全、经济命脉、社会稳定的信息系统。

[来源：GB/T 31495.2—2015，3.2]

3.803

主机　host

在基于传输控制协议/互联网协议(TCP/IP)的网络(如互联网)中，可设定地址的系统或计算机。

[来源：GB/T 28454—2020，3.14，有修改：添加缩略语"TCP/IP"的中文全称"传输控制协议/互联网协议"，"Internet"改为"互联网"等]

3.804

主体　principal

其身份能被鉴别的实体。

[来源：GB/T 15843.1—2017，3.20]

3.805

转让　transfer of control

将信息控制权由一个控制者向另一个控制者转移的过程。

[来源：GB/T 35273—2020，3.12，有修改："个人信息"改为"信息"]

3.806

资产　asset

对个人、组织或政府具有价值的任何东西。

[来源：ISO/IEC 27032:2012，4.6，有修改：删除注]

3.807

资源　resource

计算机资源　computer resource

执行所要求的操作而必需的计算机系统的任何组成部分。

示例：存储器、输入输出设备、一个或多个处理器、数据、文件和程序。

[来源：GB/T 5271.1—2000，01.01.23，有修改："数据处理系统"改为"计算机系统"等]

3.808

子网　subnet

在某一网络中，共享某一公共地址组件的网络段。

[来源：GB/T 28454—2020，3.29]

3.809

自颁发证书　self-issued certificate

证书的主体和颁发者相同的证书。

[来源：GB/T 19714—2005，3.25，有修改："CA 证书"改为"证书"]

3.810

自评估　self-assessment

由信息系统所有者自身发起，组成组织内部的评估小组，依据国家有关法规与标准，对信息系统安全管理进行的评估活动。

[来源：GB/T 28453—2012，3.2，有修改]

3.811

自同步流密码　self-synchronous stream cipher

具有如下性质的流密码：其密钥流符号，作为一个秘密密钥和一个先前密文的固定位数的函数所生成。

[来源：ISO/IEC 18033-1：2015，2.35]

3.812

字　word

为给定目的而作为一个单位的字符串或位串。

[来源：GB/T 5271.4—2000，04.06.01，有修改]

3.813

字典攻击　dictionary attack

一种由可能的密钥或口令组成字典，遍历其中的所有条目以猜测密钥或口令的攻击方法。

[来源：GM/Z 4001—2013，2.153，有修改]

3.814

总体裁定　overall verdict

评价者就评价结果宣布的通过与否的声明。

[来源：GB/T 30270—2013，3.11，有修改："评估"改为"评价"等]

3.815

组件　component

在系统中，实现其部分功能的可识别区分的部分。

[来源：ISO/IEC TR 19791：2010，3.1，有修改："operational system"改译为"系统"]

3.816

组织　organization

具有自身的职责、权威和关系以实现其目标的个人或集体。

注：组织的概念包括但不限于个体经营者、公司、法人、商行、企业、机关、合伙关系、慈善机构或院校，或者其部分或组合，无论注册成立与否、是公共的还是私营的。

[来源：GB/T 29246—2017，2.57，有修改]

3.817

组织安全策略　organizational security policies

组织为确保其运行而制定的若干安全规则、规程、实践和指南。

3.818

最高管理层　top management

在最高级别上指导和控制某一组织的个人或小组。

注 1：最高管理层具有在组织内授权和提供资源的权力。

注 2：如果管理体系的范围仅涵盖组织的一部分，则最高管理层就是指导和控制组织这一部分的个人或小组。

注 3：最高管理层有时称为“执行管理层”，可包括首席执行官、首席财务官、首席信息官和类似的角色。

[来源：GB/T 29246—2017，2.84，有修改：增加注 3 等]

3.819

最小特权　minimum privilege

对某一主体，其访问权限仅限于执行所授权任务所必需的权限。

[来源：GB/T 5271.8—2001，08.04.15，有修改]

3.820

佐证　witness

向验证方提供声称者身份证据的规程参数。

[来源：GB/T 15843.5—2005，3.30，有修改：“数据项”改为“规程参数”]

4　术语分类

4.1　密码机制类

4.2 鉴别授权类

4.3 计算安全类

4.4 通信安全类

4.5 应用安全类

4.6 数据安全类

4.7 安全服务类

4.8 安全测评类

4.9 安全管理类

4.9.1 管理通用子类

4.9.2 风险管理子类

4.9.3 事件管理子类

参 考 文 献

[1] GB/T 5271.1—2000 信息技术 词汇 第1部分:基本术语

[2] GB/T 5271.2—1988 数据处理词汇 02部分:算术和逻辑运算

[3] GB/T 5271.4—2000 信息技术 词汇 第4部分:数据的组织

[4] GB/T 5271.7—2008 信息技术 词汇 第7部分:计算机编程

[5] GB/T 5271.8—2001 信息技术 词汇 第8部分:安全

[6] GB/T 5271.9—2001 信息技术 词汇 第9部分:数据通信

[7] GB/T 5271.10—1986 数据处理词汇 10部分:操作技术和设施

[8] GB/T 5271.12—2000 信息技术 词汇 第12部分:外围设备

[9] GB/T 5271.13—2008 信息技术 词汇 第13部分:计算机图形

[10] GB/T 5271.14—2008 信息技术 词汇 第14部分:可靠性、可维护性与可用性

[11] GB/T 5271.15—2008 信息技术 词汇 第15部分:编程语言

[12] GB/T 5271.17—2010 信息技术 词汇 第17部分:数据库

[13] GB/T 5271.18—2008 信息技术 词汇 第18部分:分布式数据处理

[14] GB/T 5271.20—1994 信息技术 词汇 第20部分:系统开发

[15] GB/T 5271.23—2000 信息技术 词汇 第23部分:文本处理

[16] GB/T 5271.25—2000 信息技术 词汇 第25部分:局域网

[17] GB/T 5271.28—2001 信息技术 词汇 第28部分:人工智能 基本概念与专家系统

[18] GB/T 5271.32—2006 信息技术 词汇 第32部分:电子邮件

[19] GB/T 5271.37—2021 信息技术 词汇 第37部分:生物特征识别

[20] GB/T 9387.2—1995 信息处理系统 开放系统互连 基本参考模型 第2部分:安全体系结构

[21] GB 15629.11—2003 信息技术 系统间远程通信和信息交换 局域网和城域网 特定要求 第11部分:无线局域网媒体访问控制和物理层规范

[22] GB/T 15843.1—2017 信息技术 安全技术 实体鉴别 第1部分:总则

[23] GB/T 15843.2—2017 信息技术 安全技术 实体鉴别 第2部分:采用对称加密算法的机制

[24] GB/T 15843.3—2016 信息技术 安全技术 实体鉴别 第3部分:采用数字签名技术的机制

[25] GB/T 15843.4—2008 信息技术 安全技术 实体鉴别 第4部分:采用密码校验函数的机制

[26] GB/T 15843.5—2005 信息技术 安全技术 实体鉴别 第5部分:使用零知识技术的机制

[27] GB/T 15843.6—2018 信息技术 安全技术 实体鉴别 第6部分:采用人工数据传递的机制

[28] GB/T 15851.3—2018 信息技术 安全技术 带消息恢复的数字签名方案 第3部分:基于离散对数的机制

[29] GB/T 15852.1—2020 信息技术 安全技术 消息鉴别码 第1部分:采用分组密码的机制

[30] GB/T 15852.2—2012 信息技术 安全技术 消息鉴别码 第2部分:采用专用杂凑函数的机制

[31] GB/T 15852.3—2019 信息技术 安全技术 消息鉴别码 第3部分:采用泛杂凑函数的机制
[32] GB/T 16262.1—2006 信息技术 抽象语法记法一(ASN.1) 第1部分:基本记法规范
[33] GB/T 16264.8—2005 信息技术 开放系统互连 目录 第8部分:公钥和属性证书框架
[34] GB/T 17710—2008 信息技术 安全技术 校验字符系统
[35] GB 17859—1999 计算机信息系统 安全保护等级划分准则
[36] GB/T 17901.1—2020 信息技术 安全技术 密钥管理 第1部分:框架
[37] GB/T 17902.1—1999 信息技术 安全技术 带附录的数字签名 第1部分:概述
[38] GB/T 17902.2—2005 信息技术 安全技术 带附录的数字签名 第2部分:基于身份的机制
[39] GB/T 17902.3—2005 信息技术 安全技术 带附录的数字签名 第3部分:基于证书的机制
[40] GB/T 17903.1—2008 信息技术 安全技术 抗抵赖 第1部分:概述
[41] GB/T 17903.2—2008 信息技术 安全技术 抗抵赖 第2部分:采用对称技术的机制
[42] GB/T 17903.3—2008 信息技术 安全技术 抗抵赖 第3部分:采用非对称技术的机制
[43] GB/T 17964—2008 信息安全技术 分组密码算法的工作模式
[44] GB/T 18018—2019 信息安全技术 路由器安全技术要求
[45] GB/T 18238.1—2000 信息技术 安全技术 散列函数 第1部分:概述
[46] GB/T 18238.2—2002 信息技术 安全技术 散列函数 第2部分:采用n位块密码的散列函数
[47] GB/T 18238.3—2002 信息技术 安全技术 散列函数 第3部分:专用散列函数
[48] GB/T 18336.1—2015 信息技术 安全技术 信息技术安全评估准则 第1部分:简介和一般模型
[49] GB/T 18336.2—2015 信息技术 安全技术 信息技术安全评估准则 第2部分:安全功能组件
[50] GB/T 18336.3—2015 信息技术 安全技术 信息技术安全评估准则 第3部分:安全保障组件
[51] GB/T 19713—2005 信息技术 安全技术 公钥基础设施 在线证书状态协议
[52] GB/T 19714—2005 信息技术 安全技术 公钥基础设施 证书管理协议
[53] GB/Z 19717—2005 基于多用途互联网邮件扩展(MIME)的安全报文交换
[54] GB/T 19771—2005 信息技术 安全技术 公钥基础设施 PKI组件最小互操作规范
[55] GB/T 20008—2005 信息安全技术 操作系统安全评估准则
[56] GB/T 20009—2019 信息安全技术 数据库管理系统安全评估准则
[57] GB/T 20011—2005 信息安全技术 路由器安全评估准则
[58] GB/T 20261—2020 信息技术 系统安全工程 能力成熟度模型
[59] GB/T 20269—2006 信息安全技术 信息系统安全管理要求
[60] GB/T 20270—2006 信息安全技术 网络基础安全技术要求
[61] GB/T 20271—2006 信息安全技术 信息系统通用安全技术要求
[62] GB/T 20272—2019 信息安全技术 操作系统安全技术要求
[63] GB/T 20273—2019 信息安全技术 数据库管理系统安全技术要求
[64] GB/T 20274.1—2006 信息安全技术 信息系统安全保障评估框架 第1部分:简介和一般模型
[65] GB/T 20274.2—2008 信息安全技术 信息系统安全保障评估框架 第2部分:技术保障

[66] GB/T 20274.3—2008 信息安全技术 信息系统安全保障评估框架 第3部分:管理保障
[67] GB/T 20274.4—2008 信息安全技术 信息系统安全保障评估框架 第4部分:工程保障
[68] GB/T 20275—2013 信息安全技术 网络入侵检测系统技术要求和测试评价方法
[69] GB/T 20276—2016 信息安全技术 具有中央处理器的IC卡嵌入式软件安全技术要求
[70] GB/T 20277—2015 信息安全技术 网络和终端隔离产品测试评价方法
[71] GB/T 20278—2013 信息安全技术 网络脆弱性扫描产品安全技术要求
[72] GB/T 20279—2015 信息安全技术 网络和终端隔离产品安全技术要求
[73] GB/T 20280—2006 信息安全技术 网络脆弱性扫描产品测试评价方法
[74] GB/T 20281—2020 信息安全技术 防火墙安全技术要求和测试评价方法
[75] GB/T 20282—2006 信息安全技术 信息系统安全工程管理要求
[76] GB/T 20283—2020 信息安全技术 保护轮廓和安全目标的产生指南
[77] GB/T 20518—2018 信息安全技术 公钥基础设施 数字证书格式
[78] GB/T 20520—2006 信息安全技术 公钥基础设施 时间戳规范
[79] GB/T 20945—2013 信息安全技术 信息系统安全审计产品技术要求和测试评价方法
[80] GB/T 20979—2019 信息安全技术 虹膜识别系统技术要求
[81] GB/T 20984—2007 信息安全技术 信息安全风险评估规范
[82] GB/T 20985.1—2017 信息技术 安全技术 信息安全事件管理 第1部分:事件管理原理
[83] GB/Z 20986—2007 信息安全技术 信息安全事件分类分级指南
[84] GB/T 20988—2007 信息安全技术 信息系统灾难恢复规范
[85] GB/T 21050—2019 信息安全技术 网络交换机安全技术要求
[86] GB/T 21052—2007 信息安全技术 信息系统物理安全技术要求
[87] GB/T 21053—2007 信息安全技术 公钥基础设施 PKI系统安全等级保护技术要求
[88] GB/T 21054—2007 信息安全技术 公钥基础设施 PKI系统安全等级保护评估准则
[89] GB/T 22032—2021 系统工程 系统生存周期过程
[90] GB/T 22080—2016 信息技术 安全技术 信息安全管理体系 要求
[91] GB/T 22081—2016 信息技术 安全技术 信息安全控制实践指南
[92] GB/T 22186—2016 信息安全技术 具有中央处理器的IC卡芯片安全技术要求
[93] GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求
[94] GB/T 22240—2020 信息安全技术 网络安全等级保护定级指南
[95] GB/Z 24294.1—2018 信息安全技术 基于互联网电子政务信息安全实施指南 第1部分:总则
[96] GB/Z 24294.2—2017 信息安全技术 基于互联网电子政务信息安全实施指南 第2部分:接入控制与安全交换
[97] GB/Z 24294.3—2017 信息安全技术 基于互联网电子政务信息安全实施指南 第3部分:身份认证与授权管理
[98] GB/Z 24294.4—2017 信息安全技术 基于互联网电子政务信息安全实施指南 第4部分:终端安全防护
[99] GB/T 24363—2009 信息安全技术 信息安全应急响应计划规范
[100] GB/Z 24364—2009 信息安全技术 信息安全风险管理指南
[101] GB/T 25000.2—2018 系统与软件工程 系统与软件质量要求和评价(SQuaRE) 第2部分:计划与管理
[102] GB/T 25056—2018 信息安全技术 证书认证系统密码及其相关安全技术规范

[103] GB/T 25058—2019 信息安全技术 网络安全等级保护实施指南
[104] GB/T 25061—2020 信息安全技术 XML 数字签名语法与处理规范
[105] GB/T 25062—2010 信息安全技术 鉴别与授权 基于角色的访问控制模型与管理规范
[106] GB/T 25064—2010 信息安全技术 公钥基础设施 电子签名格式规范
[107] GB/T 25065—2010 信息安全技术 公钥基础设施 签名生成应用程序的安全要求
[108] GB/T 25066—2020 信息安全技术 信息安全产品类别与代码
[109] GB/T 25067—2020 信息技术 安全技术 信息安全管理体系审核和认证机构要求
[110] GB/T 25068.1—2020 信息技术 安全技术 网络安全 第 1 部分:综述和概念
[111] GB/T 25068.2—2020 信息技术 安全技术 网络安全 第 2 部分:网络安全设计和实现指南
[112] GB/T 25068.3—2010 信息技术 安全技术 IT 网络安全 第 3 部分:使用安全网关的网间通信安全保护
[113] GB/T 25068.4—2010 信息技术 安全技术 IT 网络安全 第 4 部分:远程接入的安全保护
[114] GB/T 25068.5—2021 信息技术 安全技术 网络安全 第 5 部分:使用虚拟专用网的跨网通信安全保护
[115] GB/T 25069—2010 信息安全技术 术语
[116] GB/T 25070—2019 信息安全技术 网络安全等级保护安全设计技术要求
[117] GB/T 26855—2011 信息安全技术 公钥基础设施 证书策略与认证业务声明框架
[118] GB/T 28447—2012 信息安全技术 电子认证服务机构运营管理规范
[119] GB/T 28448—2019 信息安全技术 网络安全等级保护测评要求
[120] GB/T 28449—2018 信息安全技术 网络安全等级保护测评过程指南
[121] GB/T 28450—2020 信息技术 安全技术 信息安全管理体系审核指南
[122] GB/T 28451—2012 信息安全技术 网络型入侵防御产品技术要求和测试评价方法
[123] GB/T 28452—2012 信息安全技术 应用软件系统通用安全技术要求
[124] GB/T 28453—2012 信息安全技术 信息系统安全管理评估要求
[125] GB/T 28454—2020 信息技术 安全技术 入侵检测系统(IDPS)的选择、部署和操作
[126] GB/T 28455—2012 信息安全技术 引入可信第三方的实体鉴别及接入架构规范
[127] GB/T 28456—2012 IPsec 协议应用测试规范
[128] GB/T 28457—2012 SSL 协议应用测试规范
[129] GB/T 28458—2020 信息安全技术 网络安全漏洞标识与描述规范
[130] GB/Z 28828—2012 信息安全技术 公共及商用服务信息系统个人信息保护指南
[131] GB/T 29240—2012 信息安全技术 终端计算机通用安全技术要求与测试评价方法
[132] GB/T 29241—2012 信息安全技术 公钥基础设施 PKI 互操作性评估准则
[133] GB/T 29242—2012 信息安全技术 鉴别与授权 安全断言置标语言
[134] GB/T 29243—2012 信息安全技术 数字证书代理认证路径构造和代理验证规范
[135] GB/T 29244—2012 信息安全技术 办公设备基本安全要求
[136] GB/T 29245—2012 信息安全技术 政府部门信息安全管理基本要求
[137] GB/T 29246—2017 信息技术 安全技术 信息安全管理体系 概述和词汇
[138] GB/T 29261.3—2012 信息技术 自动识别和数据采集技术词汇 第 3 部分:射频识别
[139] GB/T 29765—2013 信息安全技术 数据备份与恢复产品技术要求与测试评价方法
[140] GB/T 29766—2013 信息安全技术 网站数据恢复产品技术要求与测试评价方法
[141] GB/T 29767—2013 信息安全技术 公钥基础设施 桥 CA 体系证书分级规范

[142] GB/T 29827—2013 信息安全技术 可信计算规范 可信平台主板功能接口
[143] GB/T 29828—2013 信息安全技术 可信计算规范 可信连接架构
[144] GB/T 29829—2013 信息安全技术 可信计算密码支撑平台功能与接口规范
[145] GB/Z 29830.1—2013 信息技术 安全技术 信息技术安全保障框架 第1部分:综述和框架
[146] GB/Z 29830.2—2013 信息技术 安全技术 信息技术安全保障框架 第2部分:保障方法
[147] GB/Z 29830.3—2013 信息技术 安全技术 信息技术安全保障框架 第3部分:保障方法分析
[148] GB/T 30146—2013 公共安全 业务连续性管理体系 要求
[149] GB/T 30269.2—2013 信息技术 传感器网络 第2部分:术语
[150] GB/T 30270—2013 信息技术 安全技术 信息技术安全性评估方法
[151] GB/T 30271—2013 信息安全技术 信息安全服务能力评估准则
[152] GB/T 30272—2013 信息安全技术 公钥基础设施 标准一致性测试评价指南
[153] GB/T 30273—2013 信息安全技术 信息系统安全保障通用评估指南
[154] GB/T 30275—2013 信息安全技术 鉴别与授权 认证中间件框架与接口规范
[155] GB/T 30276—2020 信息安全技术 网络安全漏洞管理规范
[156] GB/T 30278—2013 信息安全技术 政务计算机终端核心配置规范
[157] GB/T 30279—2020 信息安全技术 网络安全漏洞分类分级指南
[158] GB/T 30280—2013 信息安全技术 鉴别与授权 地理空间可扩展访问控制置标语言
[159] GB/T 30281—2013 信息安全技术 鉴别与授权 可扩展访问控制标记语言
[160] GB/T 30282—2013 信息安全技术 反垃圾邮件产品技术要求和测试评价方法
[161] GB/T 30283—2013 信息安全技术 信息安全服务 分类
[162] GB/T 30284—2020 信息安全技术 移动通信智能终端操作系统安全技术要求
[163] GB/T 30285—2013 信息安全技术 灾难恢复中心建设与运维管理规范
[164] GB/Z 30286—2013 信息安全技术 信息系统保护轮廓和信息系统安全目标产生指南
[165] GB/T 31167—2014 信息安全技术 云计算服务安全指南
[166] GB/T 31168—2014 信息安全技术 云计算服务安全能力要求
[167] GB/T 31495.1—2015 信息安全技术 信息安全保障指标体系及评价方法 第1部分:概念和模型
[168] GB/T 31495.2—2015 信息安全技术 信息安全保障指标体系及评价方法 第2部分:指标体系
[169] GB/T 31495.3—2015 信息安全技术 信息安全保障指标体系及评价方法 第3部分:实施指南
[170] GB/T 31496—2015 信息技术 安全技术 信息安全管理体系实施指南
[171] GB/T 31497—2015 信息技术 安全技术 信息安全管理 测量
[172] GB/T 31499—2015 信息安全技术 统一威胁管理产品技术要求和测试评价方法
[173] GB/T 31500—2015 信息安全技术 存储介质数据恢复服务要求
[174] GB/T 31501—2015 信息安全技术 鉴别与授权 授权应用程序判定接口规范
[175] GB/T 31502—2015 信息安全技术 电子支付系统安全保护框架
[176] GB/T 31503—2015 信息安全技术 电子文档加密与签名消息语法
[177] GB/T 31504—2015 信息安全技术 鉴别与授权 数字身份信息服务框架规范
[178] GB/T 31505—2015 信息安全技术 主机型防火墙安全技术要求和测试评价方法

[179] GB/T 31506—2015 信息安全技术 政府门户网站系统安全技术指南
[180] GB/T 31507—2015 信息安全技术 智能卡通用安全检测指南
[181] GB/T 31508—2015 信息安全技术 公钥基础设施 数字证书策略分类分级规范
[182] GB/T 31509—2015 信息安全技术 信息安全风险评估实施指南
[183] GB/T 31722—2015 信息技术 安全技术 信息安全风险管理
[184] GB/T 32213—2015 信息安全技术 公钥基础设施 远程口令鉴别与密钥建立规范
[185] GB/T 32400—2015 信息技术 云计算 概览与词汇
[186] GB/T 32905—2016 信息安全技术 SM3 密码杂凑算法
[187] GB/Z 32906—2016 信息安全技术 中小电子商务企业信息安全建设指南
[188] GB/T 32907—2016 信息安全技术 SM4 分组密码算法
[189] GB/T 32914—2016 信息安全技术 信息安全服务提供方管理要求
[190] GB/T 32915—2016 信息安全技术 二元序列随机性检测方法
[191] GB/Z 32916—2016 信息技术 安全技术 信息安全控制措施审核员指南
[192] GB/T 32917—2016 信息安全技术 WEB 应用防火墙安全技术要求与测试评价方法
[193] GB/T 32918.1—2016 信息安全技术 SM2 椭圆曲线公钥密码算法 第 1 部分:总则
[194] GB/T 32918.2—2016 信息安全技术 SM2 椭圆曲线公钥密码算法 第 2 部分:数字签名算法
[195] GB/T 32918.3—2016 信息安全技术 SM2 椭圆曲线公钥密码算法 第 3 部分:密钥交换协议
[196] GB/T 32918.4—2016 信息安全技术 SM2 椭圆曲线公钥密码算法 第 4 部分:公钥加密算法
[197] GB/T 32918.5—2017 信息安全技术 SM2 椭圆曲线公钥密码算法 第 5 部分:参数定义
[198] GB/T 32919—2016 信息安全技术 工业控制系统安全控制应用指南
[199] GB/T 32920—2016 信息技术 安全技术 行业间和组织间通信的信息安全管理
[200] GB/T 32921—2016 信息安全技术 信息技术产品供应方行为安全准则
[201] GB/T 32922—2016 信息安全技术 IPSec VPN 安全接入基本要求与实施指南
[202] GB/T 32923—2016 信息技术 安全技术 信息安全治理
[203] GB/T 32924—2016 信息安全技术 网络安全预警指南
[204] GB/T 32925—2016 信息安全技术 政府联网计算机终端安全基本要求
[205] GB/T 32926—2016 信息安全技术 政府部门信息技术服务外包信息安全管理规范
[206] GB/T 32927—2016 信息安全技术 移动智能终端安全架构
[207] GB/T 33131—2016 信息安全技术 基于 IPSec 的 IP 存储网络安全技术要求
[208] GB/T 33132—2016 信息安全技术 信息安全风险处理实施指南
[209] GB/T 33133.1—2016 信息安全技术 祖冲之序列密码算法 第 1 部分:算法描述
[210] GB/T 33134—2016 信息安全技术 公共域名服务系统安全要求
[211] GB/T 33560—2017 信息安全技术 密码应用标识规范
[212] GB/T 33562—2017 信息安全技术 安全域名系统实施指南
[213] GB/T 33563—2017 信息安全技术 无线局域网客户端安全技术要求(评估保障级 2 级增强)
[214] GB/T 33565—2017 信息安全技术 无线局域网接入系统安全技术要求(评估保障级 2 级增强)
[215] GB/T 33745—2017 物联网 术语

[216] GB/T 33746.1—2017 近场通信(NFC)安全技术要求 第1部分:NFCIP-1安全服务和协议
[217] GB/T 33746.2—2017 近场通信(NFC)安全技术要求 第2部分:安全机制要求
[218] GB/T 33770.1—2017 信息技术服务 外包 第1部分:服务提供方通用要求
[219] GB/T 34095—2017 信息安全技术 用于电子支付的基于近距离无线通信的移动终端安全技术要求
[220] GB/T 34942—2017 信息安全技术 云计算服务安全能力评估方法
[221] GB/T 34953.1—2017 信息技术 安全技术 匿名实体鉴别 第1部分:总则
[222] GB/T 34953.2—2018 信息技术 安全技术 匿名实体鉴别 第2部分:基于群组公钥签名的机制
[223] GB/T 34975—2017 信息安全技术 移动智能终端应用软件安全技术要求和测试评价方法
[224] GB/T 34976—2017 信息安全技术 移动智能终端操作系统安全技术要求与测试评价方法
[225] GB/T 34977—2017 信息安全技术 移动智能终端数据存储安全技术要求与测试评价方法
[226] GB/T 34978—2017 信息安全技术 移动智能终端个人信息保护技术要求
[227] GB/T 34990—2017 信息安全技术 信息系统安全管理平台技术要求和测试评价方法
[228] GB/T 35101—2017 信息安全技术 智能卡读写机具安全技术要求(EAL4增强)
[229] GB/T 35273—2020 信息安全技术 个人信息安全规范
[230] GB/T 35274—2017 信息安全技术 大数据服务安全能力要求
[231] GB/T 35275—2017 信息安全技术 SM2密码算法加密签名消息语法规范
[232] GB/T 35276—2017 信息安全技术 SM2密码算法使用规范
[233] GB/T 35277—2017 信息安全技术 防病毒网关安全技术要求和测试评价方法
[234] GB/T 35278—2017 信息安全技术 移动终端安全保护技术要求
[235] GB/T 35279—2017 信息安全技术 云计算安全参考架构
[236] GB/T 35280—2017 信息安全技术 信息技术产品安全检测机构条件和行为准则
[237] GB/T 35281—2017 信息安全技术 移动互联网应用服务器安全技术要求
[238] GB/T 35282—2017 信息安全技术 电子政务移动办公系统安全技术规范
[239] GB/T 35283—2017 信息安全技术 计算机终端核心配置基线结构规范
[240] GB/T 35284—2017 信息安全技术 网站身份和系统安全要求与评估方法
[241] GB/T 35285—2017 信息安全技术 公钥基础设施 基于数字证书的可靠电子签名生成及验证技术要求
[242] GB/T 35286—2017 信息安全技术 低速无线个域网空口安全测试规范
[243] GB/T 35287—2017 信息安全技术 网站可信标识技术指南
[244] GB/T 35288—2017 信息安全技术 电子认证服务机构从业人员岗位技能规范
[245] GB/T 35289—2017 信息安全技术 电子认证服务机构服务质量规范
[246] GB/T 35290—2017 信息安全技术 射频识别(RFID)系统通用安全技术要求
[247] GB/T 35291—2017 信息安全技术 智能密码钥匙应用接口规范
[248] GB/T 35295—2017 信息技术 大数据 术语
[249] GB/T 36322—2018 信息安全技术 密码设备应用接口规范
[250] GB/T 36323—2018 信息安全技术 工业控制系统安全管理基本要求
[251] GB/T 36324—2018 信息安全技术 工业控制系统信息安全分级规范

[252] GB/T 36466—2018 信息安全技术 工业控制系统风险评估实施指南
[253] GB/T 36470—2018 信息安全技术 工业控制系统现场测控设备通用安全功能要求
[254] GB/T 36618—2018 信息安全技术 金融信息服务安全规范
[255] GB/T 36619—2018 信息安全技术 政务和公益机构域名命名规范
[256] GB/T 36624—2018 信息技术 安全技术 可鉴别的加密机制
[257] GB/T 36626—2018 信息安全技术 信息系统安全运维管理指南
[258] GB/T 36627—2018 信息安全技术 网络安全等级保护测试评估技术指南
[259] GB/T 36629.1—2018 信息安全技术 公民网络电子身份标识安全技术要求 第1部分:读写机具安全技术要求
[260] GB/T 36629.2—2018 信息安全技术 公民网络电子身份标识安全技术要求 第2部分:载体安全技术要求
[261] GB/T 36629.3—2018 信息安全技术 公民网络电子身份标识安全技术要求 第3部分:验证服务消息及其处理规则
[262] GB/T 36630.1—2018 信息安全技术 信息技术产品安全可控评价指标 第1部分:总则
[263] GB/T 36630.2—2018 信息安全技术 信息技术产品安全可控评价指标 第2部分:中央处理器
[264] GB/T 36630.3—2018 信息安全技术 信息技术产品安全可控评价指标 第3部分:操作系统
[265] GB/T 36630.4—2018 信息安全技术 信息技术产品安全可控评价指标 第4部分:办公套件
[266] GB/T 36630.5—2018 信息安全技术 信息技术产品安全可控评价指标 第5部分:通用计算机
[267] GB/T 36631—2018 信息安全技术 时间戳策略和时间戳业务操作规则
[268] GB/T 36632—2018 信息安全技术 公民网络电子身份标识格式规范
[269] GB/T 36633—2018 信息安全技术 网络用户身份鉴别技术指南
[270] GB/T 36635—2018 信息安全技术 网络安全监测基本要求与实施指南
[271] GB/T 36637—2018 信息安全技术 ICT供应链安全风险管理指南
[272] GB/T 36639—2018 信息安全技术 可信计算规范 服务器可信支撑平台
[273] GB/T 36643—2018 信息安全技术 网络安全威胁信息格式规范
[274] GB/T 36644—2018 信息安全技术 数字签名应用安全证明获取方法
[275] GB/T 36651—2018 信息安全技术 基于可信环境的生物特征识别身份鉴别协议框架
[276] GB/T 36950—2018 信息安全技术 智能卡安全技术要求(EAL4+)
[277] GB/T 36951—2018 信息安全技术 物联网感知终端应用安全技术要求
[278] GB/T 36957—2018 信息安全技术 灾难恢复服务要求
[279] GB/T 36958—2018 信息安全技术 网络安全等级保护安全管理中心技术要求
[280] GB/T 36959—2018 信息安全技术 网络安全等级保护测评机构能力要求和评估规范
[281] GB/T 36960—2018 信息安全技术 鉴别与授权 访问控制中间件框架与接口
[282] GB/T 36968—2018 信息安全技术 IPSec VPN技术规范
[283] GB/T 37002—2018 信息安全技术 电子邮件系统安全技术要求
[284] GB/T 37024—2018 信息安全技术 物联网感知层网关安全技术要求
[285] GB/T 37025—2018 信息安全技术 物联网数据传输安全技术要求
[286] GB/T 37027—2018 信息安全技术 网络攻击定义及描述规范

[287] GB/T 37033.1—2018 信息安全技术 射频识别系统密码应用技术要求 第1部分:密码安全保护框架及安全级别

[288] GB/T 37033.2—2018 信息安全技术 射频识别系统密码应用技术要求 第2部分:电子标签与读写器及其通信密码应用技术要求

[289] GB/T 37033.3—2018 信息安全技术 射频识别系统密码应用技术要求 第3部分:密钥管理技术要求

[290] GB/T 37044—2018 信息安全技术 物联网安全参考模型及通用要求

[291] GB/T 37046—2018 信息安全技术 灾难恢复服务能力评估准则

[292] GB/T 37076—2018 信息安全技术 指纹识别系统技术要求

[293] GB/T 37090—2018 信息安全技术 病毒防治产品安全技术要求和测试评价方法

[294] GB/T 37091—2018 信息安全技术 安全办公U盘安全技术要求

[295] GB/T 37092—2018 信息安全技术 密码模块安全要求

[296] GB/T 37093—2018 信息安全技术 物联网感知层接入通信网的安全要求

[297] GB/T 37094—2018 信息安全技术 办公信息系统安全管理要求

[298] GB/T 37095—2018 信息安全技术 办公信息系统安全基本技术要求

[299] GB/T 37096—2018 信息安全技术 办公信息系统安全测试规范

[300] GB/T 37695—2019 智能制造 对象标识要求

[301] GB/T 37931—2019 信息安全技术 Web应用安全检测系统安全技术要求和测试评价方法

[302] GB/T 37932—2019 信息安全技术 数据交易服务安全要求

[303] GB/T 37933—2019 信息安全技术 工业控制系统专用防火墙技术要求

[304] GB/T 37934—2019 信息安全技术 工业控制网络安全隔离与信息交换系统安全技术要求

[305] GB/T 37935—2019 信息安全技术 可信计算规范 可信软件基

[306] GB/T 37939—2019 信息安全技术 网络存储安全技术要求

[307] GB/T 37941—2019 信息安全技术 工业控制系统网络审计产品安全技术要求

[308] GB/T 37950—2019 信息安全技术 桌面云安全技术要求

[309] GB/T 37952—2019 信息安全技术 移动终端安全管理平台技术要求

[310] GB/T 37953—2019 信息安全技术 工业控制网络监测安全技术要求及测试评价方法

[311] GB/T 37954—2019 信息安全技术 工业控制系统漏洞检测产品技术要求及测试评价方法

[312] GB/T 37955—2019 信息安全技术 数控网络安全技术要求

[313] GB/T 37956—2019 信息安全技术 网站安全云防护平台技术要求

[314] GB/T 37962—2019 信息安全技术 工业控制系统产品信息安全通用评估准则

[315] GB/T 37964—2019 信息安全技术 个人信息去标识化指南

[316] GB/T 37971—2019 信息安全技术 智慧城市安全体系框架

[317] GB/T 37972—2019 信息安全技术 云计算服务运行监管框架

[318] GB/T 37973—2019 信息安全技术 大数据安全管理指南

[319] GB/T 37980—2019 信息安全技术 工业控制系统安全检查指南

[320] GB/T 37988—2019 信息安全技术 数据安全能力成熟度模型

[321] GB/T 38249—2019 信息安全技术 政府网站云计算服务安全指南

[322] GM/T 0015—2012 基于SM2密码算法的数字证书格式规范

[323] GM/T 0024—2014 SSL VPN技术规范

[324] GM/T 0027—2014 智能密码钥匙技术规范

[325] GM/T 0028—2014 密码模块安全要求

[326] GM/T 0031—2014 安全电子签章密码应用技术规范

[327] GM/T 0035.1—2014 射频识别系统密码应用技术要求 第1部分:密码安全保护框架及安全级别

[328] GM/T 0043—2015 数字证书互操作检测规范

[329] GM/Z 4001—2013 密码术语

[330] ISO 7498-2:1989 Information processing system—Open systems interconnection—Basic reference model—Part2: Security architecture

[331] ISO 9241-20:2008 Ergonomics of human-system interaction—Part 20: Accessibility guidelines for information/communication technology (ICT) equipment and services

[332] ISO 22301:2019 Security and resilience—Business continuity management systems—Requirements

[333] ISO 22600-3:2014 Health informatics—Privilege management and access control—Part 3: Implementations

[334] ISO 3534-2:2006 Statistics—Vocabulary and symbols—Part 2: Applied statistics

[335] ISO/IEC 7064:2003 Information technology—Security techniques—Check character systems

[336] ISO/IEC 9594-8:2017 Information technology—Open systems interconnection—The directory—Part 8: Public-key and attribute certificate frameworks

[337] ISO/IEC 9796-2:2010 Information technology—Security techniques—Digital signature schemes giving message recovery—Part 2: Integer factorization based mechanisms

[338] ISO/IEC 9796-3:2013(Corrected 2006) Information technology—Security techniques—Digital signature schemes giving message recovery—Part 3: Discrete logarithm based mechanisms

[339] ISO/IEC 9797-1:2011 Information technology—Security techniques—Message Authentication Codes (MACs)—Part 1: Mechanisms using a block cipher

[340] ISO/IEC 9797-2:2011 Information technology—Security techniques—Message Authentication Codes (MACs)—Part 2: Mechanisms using a dedicated hash-function

[341] ISO/IEC 9797-3:2011 Information technology—Security techniques—Message Authentication Codes (MACs)—Part 3: Mechanisms using a universal hash function

[342] ISO/IEC 9798-1:2010 Information technology—Security techniques—Entity authentication—Part 1: General

[343] ISO/IEC 9798-2:2008 Information technology—Security techniques—Entity authentication—Part 2: Mechanisms using symmetric encipherment algorithms

[344] ISO/IEC 9798-3:1998/AMD.1:2010 Information technology—Security techniques—Entity authentication—Part 3: Mechanisms using digital signature techniques—AMENDMENT

[345] ISO/IEC 9798-4:1999 Information technology—Security techniques—Entity authentication—Part 4: Mechanisms using a cryptographic check function

[346] ISO/IEC 9798-5:2009 Information technology—Security techniques—Entity authentication—Part 5: Mechanisms using zero-knowledge techniques

[347] ISO/IEC 9798-6:2010 Information technology—Security techniques—Entity authentication—Part 6: Mechanisms using manual data transfer

[349] ISO/IEC 10116:2017 Information technology—Security techniques—Modes of operation for

an n-bit block cipher

[349] ISO/IEC 10118-1:2016 Information technology—Security techniques—Hash-functions—Part 1: General

[350] ISO/IEC 10118-2:2010 Information technology—Security techniques—Hash-functions—Part 2: Hash-functions using an n-bit block cipher

[351] ISO/IEC 10118-3:2018 Information technology—Security techniques—Hash-functions—Part 3: Dedicated hash-functions

[352] ISO/IEC 10118-4:1998 Information technology—Security techniques—Hash-functions—Part 4: Hash-functions using modular arithmetic

[353] ISO/IEC 11770-1:2010 Information technology—Security techniques—Key management—Part 1: Framework

[354] ISO/IEC 11770-2:2018 Information technology—Security techniques—Key management—Part 2: Mechanisms using symmetric techniques

[355] ISO/IEC 11770-3:2015 Information technology—Security techniques—Key management—Part 3: Mechanisms using asymmetric techniques

[356] ISO/IEC 11770-4:2017 Information technology—Security techniques—Key management—Part 4: Mechanisms based on weak secrets

[357] ISO/IEC 11770-5:2011 Information technology—Security techniques—Key management—Part 5: Group key management

[358] ISO/IEC 11770-6:2016 Information technology—Security techniques—Key management—Part 6: Key derivation

[359] ISO/IEC 11889-1:2015 Information technology—Trusted platform module library—Part 1: Architecture

[360] ISO/IEC 11889-2:2015 Information technology—Trusted platform module library—Parts 2: Structures

[361] ISO/IEC 11889-3:2015 Information technology—Trusted platform module library—Parts 3: Commands

[362] ISO/IEC 11889-4:2015 Information technology—Trusted platform module library—Parts 4: Supporting Routines

[363] ISO/IEC 13157-1:2014 Technical specification of NFC security—Part 1: NFCIP-1 security services and protocol

[364] ISO/IEC 13157-2:2016 Technical specification of NFC security—Part 2: Security mechanism requirements

[365] ISO/IEC 13888-1:2009 Information technology—Security techniques—Non-repudiation—Part 1: General

[366] ISO/IEC 13888-2:2010 Information technology—Security techniques—Non-repudiation—Part 2: Mechanisms using symmetric techniques

[367] ISO/IEC 13888-3:2009 Information technology—Security techniques—Non-repudiation—Part 3: Mechanisms using asymmetric techniques

[368] ISO/IEC TR 14516:2002|ITU-T X.842 Information technology—Security techniques—Guidelines on the use and management of Trusted Third Party services

[369] ISO/IEC 14888-1:2008 Information technology—Security techniques—Digital signatures with appendix—Part 1: General

[370] ISO/IEC 14888-2:2008 Information technology—Security techniques—Digital signatures with appendix—Part 2: Integer factorization based mechanisms

[371] ISO/IEC 14888-3:2018 Information technology—Security techniques—Digital signatures with appendix—Part 3: Discrete logarithm based mechanisms

[372] ISO/IEC 15408-1:2014 Information technology—Security techniques—Evaluation criteria for IT security—Part 1: Introduction and general model

[373] ISO/IEC 15408-2:2011 Information technology—Security techniques—Evaluation criteria for IT security—Part 2: Security functional components

[374] ISO/IEC 15408-3:2011 Information technology—Security techniques—Evaluation criteria for IT security—Part 3: Security assurance components

[375] ISO/IEC TR 15443-1:2012 Information technology—Security techniques—Security assurance framework—Part 1: Introduction and concepts

[376] ISO/IEC TR 15443-2:2012 Information technology—Security techniques—Security assurance framework—Part 2: Analysis

[377] ISO/IEC TR 15446:2017 Information technology—Security techniques—Guide for the production of protection profiles and security targets

[378] ISO/IEC 15816:2002|ITU-T X.841 Information technology—Security techniques—Security information objects for access control

[379] ISO/IEC 15945:2002|ITU-T X.843 Information technology—Security techniques—Specification of TTP services to support the application of digital signatures

[380] ISO/IEC 15946-1:2016 Information technology—Security techniques—Cryptographic techniques based on elliptic curves—Part 1: General

[381] ISO/IEC 15946-5:2017 Information technology—Security techniques—Cryptographic techniques based on elliptic curves—Part 5: Elliptic curve generation

[382] ISO/IEC 17825:2016 Information technology—Security techniques—Testing methods for the mitigation of non-invasive attack classes against cryptographic modules

[383] ISO/IEC 17922:2017|ITU-T X.1085 Information technology—Security techniques—Telebiometric authentication framework using biometric hardware security module

[384] ISO/IEC 18014-1:2008 Information technology—Security techniques—Time-stamping services—Part 1: Framework

[385] ISO/IEC 18014-2:2009 Information technology—Security techniques—Time-stamping services—Part 2: Mechanisms producing independent tokens

[386] ISO/IEC 18014-3:2009 Information technology—Security techniques—Time-stamping services—Part 3: Mechanisms producing linked tokens

[387] ISO/IEC 18014-4:2015 Information technology—Security techniques—Time-stamping services—Part 4: Traceability of time sources

[388] ISO/IEC 18031:2011 Information technology—Security techniques—Random bit generation

[389] ISO/IEC 18032:2005 Information technology—Security techniques—Prime number generation

[390] ISO/IEC 18033-1:2015 Information technology—Security techniques—Encryption algorithms—Part 1: General

[391] ISO/IEC 18033-2:2006 Information technology—Security techniques—Encryption algo-

rithms—Part 2：Asymmetric ciphers

[392] ISO/IEC 18033-3:2010 Information technology—Security techniques—Encryption algorithms—Part 3：Block ciphers

[393] ISO/IEC 18033-4:2011 Information technology—Security techniques—Encryption algorithms—Part 4：Stream ciphers

[394] ISO/IEC 18033-5:2015 Information technology—Security techniques—Encryption algorithms—Part 5：Identity-based ciphers

[395] ISO/IEC 18033-6:2019 Information technology—Security techniques—Encryption algorithms—Part 6：Homomorphic encryption

[396] ISO/IEC 18045:2014 Information technology—Security techniques—Methodology for IT Security Evaluation

[397] ISO/IEC 18367 Information technology—Security techniques—Cryptographic algorithms and security mechanisms conformance testing

[398] ISO/IEC 18370-1:2016 Information technology—Security techniques—Blind digital signatures—Part 1：General

[399] ISO/IEC 18370-2:2016 Information technology—Security techniques—Blind digital signatures—Part 2：Discrete logarithm based mechanisms

[400] ISO/IEC 19086-4:2019 Information technology—Cloud computing - Service Level Agreement (SLA) framework—Part 4：Components of security and protection of PII

[401] ISO/IEC TS 19249:2017 Information technology—Security techniques—Catalogue of architectural and design principles for secure products，systems，and applications

[402] ISO/IEC 19592-1:2016 Information technology—Security techniques—Secret sharing—Part 1：General

[403] ISO/IEC 19592-2:2017 Information technology—Security techniques—Secret sharing—Part 2：Fundamental mechanisms

[404] ISO/IEC TS 19608:2018 Information technology—Security techniques—Guidance for developing security and privacy functional requirements based on ISO/IEC 15408

[405] ISO/IEC 19678:2015 Information technology—BIOS Protection Guidelines

[406] ISO/IEC 19770-1:2017 Information technology—IT asset management—Part 1：IT asset management systems—Requirements

[407] ISO/IEC 19772:2009 Information technology—Security techniques—Authenticated encryption

[408] ISO/IEC 19790:2015 Information technology—Security techniques—Security requirements for cryptographic modules

[409] ISO/IEC TR 19791:2010 Information technology—Security techniques—Security assessment for operational systems

[410] ISO/IEC 19792:2009 Information technology—Security techniques—Security evaluation of biometrics

[411] ISO/IEC 19896-1:2018 Information technology—Security techniques—Competence requirements for information security testers and evaluators—Part 1：Introduction，concepts and general requirements

[412] ISO/IEC 19896-2:2018 Information technology—Security techniques—Competence requirements for information security testers and evaluators—Part 2：Knowledge，skills and effective-

ness requirements for ISO/IEC 19790 testers

[413] ISO/IEC 19896-3:2018 Information technology—Security techniques—Competence requirements for information security testers and evaluators—Part 3: Knowledge, skills and effectiveness requirements for ISO/IEC 15408 evaluators

[414] ISO/IEC TR 20004:2015 Information technology—Security techniques—Refining software vulnerability analysis under ISO/IEC 15408 and ISO/IEC 18045

[415] ISO/IEC 20008-1:2013 Information technology—Security techniques—Anonymous digital signatures—Part 1: General

[416] ISO/IEC 20008-2:2013 Information technology—Security techniques—Anonymous digital signatures—Part 2: Mechanisms using a group public key

[417] ISO/IEC 20009-1:2013 Information technology—Security techniques—Anonymous entity authentication—Part 1: General

[418] ISO/IEC 20009-2:2013 Information technology—Security techniques—Anonymous entity authentication—Part 2: Mechanisms based on anonymous digital signature schemes

[419] ISO/IEC 20009-4:2017 Information technology—Security techniques—Anonymous entity authentication—Part 4: Mechanisms based on weak secrets

[420] ISO/IEC TS 20540:2018 Information technology—Security techniques—Guidelines for testing cryptographic modules in their operational environment

[421] ISO/IEC 20889:2018 Information technology—Security techniques—Privacy enhancing data de-identification terminology and classification of techniques

[422] ISO/IEC 21827:2008 Information technology—Security techniques—Systems Security Engineering—Capability Maturity Model® (SSE-CMM®)

[423] ISO/IEC 21878:2018 Information technology—Security techniques—Security guidelines for design and implementation of virtualized servers

[424] ISO/IEC 24745:2011 Information technology—Security techniques—Biometric information protection

[425] ISO/IEC 24759:2017 Information technology—Security techniques—Test requirements for cryptographic modules

[426] ISO/IEC 24760-1:2019 Information technology—Security techniques—A framework for identity management—Part 1: Terminology and concepts

[427] ISO/IEC 24760-2:2015 Information technology—Security techniques—A framework for identity management—Part 2: Reference architecture and requirements

[428] ISO/IEC 24760-3:2016 Information technology—Security techniques—A framework for identity management—Part 3: Practice

[429] ISO/IEC 24761:2009 Information technology—Security techniques—Authentication context for biometrics

[430] ISO/IEC 27000:2018 Information technology—Security techniques—Information security management systems—Overview and vocabulary

[431] ISO/IEC 27001:2013 Information technology—Security techniques—Information security management systems—Requirements

[432] ISO/IEC 27002:2013 Information technology—Security techniques—Code of practice for information security controls

[433] ISO/IEC 27003:2017 Information technology—Security techniques—Information security

management systems—Guidance

[434] ISO/IEC 27004:2016 Information technology—Security techniques—Information security management—Monitoring, measurement, analysis and evaluation

[435] ISO/IEC 27005:2018 Information technology—Security techniques—Information security risk management

[436] ISO/IEC 27006:2015 Information technology—Security techniques—Requirements for bodies providing audit and certification of information security management systems

[437] ISO/IEC 27007:2017 Information technology—Security techniques—Guidelines for information security management systems auditing

[438] ISO/IEC TR 27008:2019 Information technology—Security techniques—Guidelines for the assessment of information security controls

[439] ISO/IEC 27009:2016 Information technology—Security techniques—Sector-specific application of ISO/IEC 27001—Requirements

[440] ISO/IEC 27010:2015 Information technology—Security techniques—Information security management for inter-sector and inter-organizational communications

[441] ISO/IEC 27011:2016|ITU-T X.1051 Information technology—Security techniques—Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations

[442] ISO/IEC 27013:2015 Information technology—Security techniques—Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1

[443] ISO/IEC 27014:2013 Information technology—Security techniques—Governance of information security

[444] ISO/IEC TR 27016:2014 Information technology—Security techniques—Information security management—Organizational economics

[445] ISO/IEC 27017:2015|ITU-T X.1631 Information technology—Security techniques—Code of practice for information security controls based on ISO/IEC 27002 for cloud services

[446] ISO/IEC 27018:2019 Information technology—Security techniques—Code of practice for PII protection in public clouds acting as PII processors

[447] ISO/IEC 27019:2017 Information technology—Security techniques—Information security controls for the energy utility industry

[448] ISO/IEC 27021:2017 Information technology—Security techniques—Competence requirements for information security management systems professionals

[449] ISO/IEC TR 27023:2015 Information technology—Security techniques—Mapping the Revised Editions of ISO/IEC 27001 and ISO/IEC 27002

[450] ISO/IEC 27031:2011 Information technology—Security techniques—Guidelines for ICT readiness for business continuity

[451] ISO/IEC 27032:2012 Information technology—Security techniques—Guidelines for cybersecurity

[452] ISO/IEC 27033-1:2015 Information technology—Security techniques—Network security—Part 1: Overview and concepts

[453] ISO/IEC 27033-2:2012 Information technology—Security techniques—Network security—Part 2: Guidelines for the design and implementation of network security

[454] ISO/IEC 27033-3:2010 Information technology—Security techniques—Network securi-

ty—Part 3: Reference networking scenarios—Threats, design techniques and control issues

[455] ISO/IEC 27033-4:2014 Information technology—Security techniques—Network security—Part 4: Securing communications between networks using security gateways

[456] ISO/IEC 27033-5:2013 Information technology—Security techniques—Network security—Part 5: Securing communications across networks using Virtual Private Network (VPNs)

[457] ISO/IEC 27033-6:2016 Information technology—Security techniques—Network security—Part 6: Securing wireless IP network access

[458] ISO/IEC 27034-1:2011 Information technology—Security techniques—Application security—Part 1: Overview and concepts

[459] ISO/IEC 27034-2:2015 Information technology—Security techniques—Application security—Part 2: Organization normative framework

[460] ISO/IEC 27034-3:2018 Information technology—Security techniques—Application security—Part 3: Application security management process

[461] ISO/IEC 27034-5:2017 Information technology—Security techniques—Application security—Part 5: Protocols and application security controls data structure

[462] ISO/IEC TS 27034-5-1:2018 Information technology—Security techniques—Application security—Part 5-1: Protocols and application security control data structure—XML Schemas

[463] ISO/IEC 27034-6:2016 Information technology—Security techniques—Application security—Part 6: Case studies

[464] ISO/IEC 27034-7:2018 Information technology—Security techniques—Application security—Part 7: Application security assurance prediction model

[465] ISO/IEC 27035-1:2016 Information technology—Security techniques—Information security incident management—Part 1: Principles of incident management

[466] ISO/IEC 27035-2:2016 Information technology—Security techniques—Information security incident management—Part 2: Guidelines to plan and prepare for incident response

[467] ISO/IEC 27036-1:2014 Information technology—Security techniques—Information security for supplier relationships—Part 1: Overview and concepts

[468] ISO/IEC 27036-2:2014 Information technology—Security techniques—Information security for supplier relationships—Part 2: Requirements

[469] ISO/IEC 27036-3:2013 Information technology—Security techniques—Information security for supplier relationships—Part 3: Guidelines for ICT supply chain security

[470] ISO/IEC 27036-4:2016 Information technology—Security techniques—Information security for supplier relationships—Part 4: Guidelines for security of cloud services

[471] ISO/IEC 27037:2012 Information technology—Security techniques—Guidelines for identification, collection, acquisition and preservation of digital evidence

[472] ISO/IEC 27038:2014 Information technology—Security techniques—Specification for digital redaction

[473] ISO/IEC 27039:2016 Information technology—Security techniques—Selection, deployment and operations of intrusion detection and prevention systems (IDPS)

[474] ISO/IEC 27040:2015 Information technology—Security techniques—Storage security

[475] ISO/IEC 27041:2015 Information technology—Security techniques—Guidance on assuring suitability and adequacy of incident investigation methods

[476] ISO/IEC 27042:2015 Information technology—Security techniques—Guidelines for the

analysis and interpretation of digital evidence

[477] ISO/IEC 27043:2015 Information technology—Security techniques—Incident investigation principles and processes

[478] ISO/IEC 27050-1:2016 Information technology—Security techniques—Electronic discovery—Part 1: Overview and concepts

[479] ISO/IEC 27050-2:2018 Information technology—Security techniques—Electronic discovery—Part 2: Guidance for governance and management of electronic discovery

[480] ISO/IEC 27050-3:2017 Information technology—Security techniques—Electronic discovery—Part 3: Code of practice for electronic discovery

[481] ISO/IEC 27102:2019 Information security management—Guidelines for cyber insurance

[482] ISO/IEC TR 27103:2018 Information technology—Security techniques—Technical report on cybersecurity and ISO and IEC Standards

[483] ISO/IEC TR 27550:2019 Information technology—Security techniques—Privacy engineering for system life cycle processes

[484] ISO/IEC 27701:2019 Security techniques—Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management—Requirements and guidelines

[485] ISO/IEC 29003:2018 Information technology—Security techniques—Identity proofing

[486] ISO/IEC 29100:2011 Information technology—Security techniques—Privacy framework

[487] ISO/IEC 29101:2013 Information technology—Security techniques—Privacy architecture framework

[488] ISO/IEC 29115:2013|ITU-T X.1254 Information technology—Security techniques—Entity authentication assurance framework

[489] ISO/IEC 29128:2011 Information technology—Security techniques—Verification of cryptographic protocols

[490] ISO/IEC 29134:2017 Information technology—Security techniques—Privacy impact assessment—Methodology

[491] ISO/IEC 29146:2016 Information technology—Security techniques—A framework for access management

[492] ISO/IEC 29147:2018 Information technology—Security techniques—Vulnerability disclosure

[493] ISO/IEC TR 29149:2012 Information technology—Security techniques—Best practices for the provision and use of time-stamping services

[494] ISO/IEC 29150:2011 Information technology—Security techniques—Signcryption

[495] ISO/IEC 29151:2017|ITU-T X.1058 (03/2017) Information technology—Security techniques—Code of practice for PII protection

[496] ISO/IEC 29190:2015 Information technology—Security techniques—Privacy capability assessment model

[497] ISO/IEC 29191:2012 Information technology—Security techniques—Requirements for partially anonymous, partially unlinkable authentication

[498] ISO/IEC 29192-1:2012 Information technology—Security techniques—Lightweight cryptography—Part 1: General

[499] ISO/IEC 29192-2:2012 Information technology—Security techniques—Lightweight cryptography—Part 2: Block ciphers

[500] ISO/IEC 29192-3:2012 Information technology—Security techniques—Lightweight cryptography—Part 3: Stream ciphers

[501] ISO/IEC 29192-4:2013 Information technology—Security techniques—Lightweight cryptography—Part 4: Mechanisms using asymmetric techniques

[502] ISO/IEC 29192-5:2016 Information technology—Security techniques—Lightweight cryptography—Part 5: Hash-functions

[503] ISO/IEC 29192-6:2019 Information technology—Security techniques—Lightweight cryptography—Part 6: Message Authentication Codes

[504] ISO/IEC 29192-7:2019 Information technology—Security techniques—Lightweight cryptography—Part 7: Broadcast authentication protocols

[505] ISO/IEC TS 30104:2015 Information technology—Security techniques—Physical security attacks, mitigation techniques and security requirements

[506] ISO/IEC 30111:2013 Information technology—Security techniques—Vulnerability handling processes

[507] ISO/IEC 30145-2:2020 Information technology—Smart City ICT reference framework—Part 2: Smart city knowledge management framework

[508] ISO/IEC 38500:2015 Information technology—Governance of IT for the organization

[509] ISO/IEC/IEEE 24765:2017 Systems and software engineering—Vocabulary

[510] ISO/IEC/IEEE 8802-11:2018 Telecommunications and exchange between information technology systems—Requirements for local and metropolitan area networks—Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications

索　引

汉语拼音索引

F

G

H

J

K

L

M

N

P

Q

R

S

T

W

X

Y

Z

英文对应词索引

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W

Z