ICS 35.040
L 80

中华人民共和国国家标准

GB/T 25069—2010

信息安全技术　术语

Information security technology—Glossary

2010-09-02 发布　　2011-02-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准的主要起草单位:中国电子技术标准化研究所、解放军信息安全测评认证中心、公安部三所、中国信息安全产品测评中心、国家保密技术研究所、中科院软件所、北京知识安全工程中心。

本标准的主要起草人:王延鸣、罗锋盈、胡啸、上官晓丽、陈星、许玉娜、任卫红、刘海龙、吉增瑞、龚奇敏。

引　言

制定信息安全技术术语标准的目的是为了方便信息安全技术的国内外交流。它给出了与信息安全领域相关的概念的术语及其定义，并明确了各术语词条之间的关系。

本标准的分类原则是根据国外信息安全术语相关的分类方法，结合国内的实践经验，和国家标准现状，按三部分来组织编制最基本的信息安全术语：

1) 信息安全一般概念术语；

2) 信息安全技术术语，包括实体类、攻击与保护类、鉴别与密码类、备份与恢复类；

3) 信息安全管理术语，包括管理活动和支持管理活动的技术，主要涉及安全管理、安全测评和风险管理等基本概念及相关的管理技术。

信息安全技术　术语

1　范围

本标准界定了与信息安全技术领域相关的概念的术语和定义，并明确了这些条目之间的关系。

本标准适用于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　术语和定义

2.1　一般概念

2.1.1

保密性　confidentiality

使信息不泄露给未授权的个人、实体、进程，或不被其利用的特性。

2.1.2

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。

2.1.3

抽象语法记法 1　Abstract Syntax Notation one

一种用来组织复杂数据的抽象符号体系。

2.1.4

对抗[措施]　countermeasure

为减小脆弱性而采用的行动、装置、过程、技术或其他措施。

2.1.5

封闭安全环境　closed-security environment

一种环境，其中通过授权、安全许可、配置控制等形式，进行数据和资源的保护，免受偶然的或恶性操作。

2.1.6

攻击者　attacker

故意利用技术上或非技术上的安全弱点，以窃取或泄露信息系统或网络的资源，或危及信息系统或网络资源可用性的任何人。

2.1.7

规程　procedure

对执行一个给定任务所采取动作历程的书面描述。

2.1.8

骇客　cracker/cracking

试图攻破他人信息系统安全并获得对其访问权的人。

2.1.9

黑客　hackers

泛指对网络或联网系统进行未授权访问，但无意窃取或造成损坏的人。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。

2.1.10

计算机安全 computer security

采取适当措施保护数据和资源，使计算机系统免受偶然或恶意的修改、损害、访问、泄露等操作的危害。

2.1.11

计算机犯罪 computer crime

通过直接介入，借助计算机系统或网络而构成的犯罪。

2.1.12

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。

2.1.13

计算机信息系统 computer information system

由计算机及其相关的和配套的设备、设施（含网络）构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。

2.1.14

计算机诈骗 computer fraud

通过直接介入，借助计算机系统或网络而进行的诈骗。

2.1.15

角色 role

在过程或组织的语境中所执行的功能。

2.1.16

开放的安全环境 open-security environment

一种环境，通过普通的操作过程即可获得对数据及资源的保护，使之免受偶然的或恶性的动作。

2.1.17

抗抵赖 non-repudiation

证明某一动作或事件已经发生的能力，以使事后不能否认这一动作或事件。

2.1.18

可核查性 accountability

确保可将一个实体的行动唯一地追踪到此实体的特性。

2.1.19

可靠性 reliability

预期行为和结果保持一致的特性。

2.1.20

可用性 availability

已授权实体一旦需要就可访问和使用的数据和资源的特性。

2.1.21

对象 object

系统中可供访问的实体。例如：数据、资源、进程等。

2.1.22

滥发 spamming

以极多的数据使资源（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使资源淹没的行为，例如：发送垃圾邮件。

2.1.23

漏报 false negative

攻击发生时检测系统没有报警的情况。

2.1.24

敏感性 sensitivity

信息拥有者分配给信息的一种重要程度的度量，以标出该信息的保护需求。

2.1.25

欺骗 spoofing

假冒成合法资源或用户的行为。

2.1.26

蠕虫 *worm*

一种独立程序，它可通过信息系统或计算机网络进行自身传播，从而造成恶意占用可用资源等损害。

2.1.27

入侵 intrusion

对某一网络或联网系统的未经授权的访问，即对某一信息系统的有意无意的未经授权的访问(包括针对信息的恶意活动)。

2.1.28

入侵者 intruder

针对主机、站点、网络等，正在或已经进行入侵或攻击的人。

2.1.29

入侵者/破解者 cracker

未受邀却试图攻破他人的系统安全并获得对其访问权的个人。

2.1.30

熵 entropy

对一个封闭系统的无序性、随机性或变异性等状态的度量。X 的熵是对通过观测 X 获得信息的一个数学度量。

2.1.31

熵源 entropy source

产生输出的部件、设备或事件。当该输出以某种方法捕获和处理时，产生包含熵的比特串。

2.1.32

事态 event

某些特定数据、情形或活动的发生。

2.1.33

授权 authorization

赋予某一主体可实施某些动作的权力的过程。

2.1.34

数据保护 data protection

采取管理或技术措施，防范未经授权访问数据。

2.1.35

数据损坏 data corruption

偶然或故意破坏数据的完整性。

2.1.36

数据完整性 data integrity

数据没有遭受以未授权方式所作的更改或破坏的特性。

2.1.37

特洛伊木马 trojan horse

一种表面无害的程序，它包含恶性逻辑程序，可导致未授权地收集、伪造或破坏数据。

2.1.38

通信安全 communication security

保护网络中所传输信息的完整性、保密性、可用性等。

2.1.39

统一资源标识符 uniform resource identifier

URI

包含名字或地址的短数据串，指向 web 上的某个对象。

2.1.40

统一资源定位符 uniform resource locator

包含地址的短数据串，指向 web 上的某个对象。URL 是 URI 的子集。

2.1.41

外联网 extranet

运行于公共基础设施上的专网。

2.1.42

完整性 integrity

保卫资产准确性和完整的特性。

2.1.43

微码 microcode

相应于可执行程序指令的处理器指令(例如汇编码)。

2.1.44

违规 breach

使信息系统安全的某一部分被避开或失去作用的行为，可能产生对信息系统的侵入。

2.1.45

误报 false positive

没有攻击时检测系统有报警的情况。

2.1.46

系统 system

具有确定目的的、分立的、可识别的物理实体，由集成的、交互的部件构成，其中每一个部件不能单独达到所要求的整体目的。

注 1：在实践中，一个系统经常用与使用有关的名词来定义，如产品系统、飞机系统等。换言之，系统这个词常常可用与系统内容相关的同义词来代替，如产品、飞机等。

注 2：一个系统在它的生存周期中为了满足其需求，往往需要其他系统。例如，一个运行系统需要一个为其概念化、开发、生产、操作、支撑或处置的系统。

2.1.47

安全服务 security service

根据安全策略，为用户提供的某种安全功能及相关的保障。

2.1.48

系统生存周期 system life cycle

系统从概念到废弃随时间演变的整个过程。

2.1.49

系统完整性 system integrity

系统能够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授权操纵的特性。

2.1.50

泄露 disclosure

违反信息安全策略，使数据被未经授权的实体使用。

2.1.51

信任 trust

两个元素之间的一种关系：元素 x 信任元素 y，当且仅当 x 确信 y 相对于一组活动，元素 y 将以良好定义的方式实施，且不违反安全策略。

2.1.52

信息安全 information security

保护、维持信息的保密性、完整性和可用性，也可包括真实性、可核查性、抗抵赖性、可靠性等性质。

2.1.53

信息安全事件 information security incident

由单个或一系列意外或有害的信息安全事态所组成的，极有可能危害业务运行和威胁信息安全。

2.1.54

信息安全事态 information security event

被识别的一种系统、服务或网络状态的发生，表明一次可能的信息安全策略违规或某些防护措施失效，或者一种可能与安全相关但以前不为人知的一种情况。

2.1.55

信息处理设施 information processing facilities

信息处理系统、服务或基础设施，或其物理放置场所。

2.1.56

信息通信技术安全 ICT security

与定义、实现和维护信息通信技术的保密性、完整性、可用性、抗抵赖，可核查性、真实性和可靠性等有关的所有方面。

2.1.57

信息系统安全 IT security

与定义、获得和维护保密性、完整性、可用性、可核查性、真实性和可靠性有关的各个方面。

2.1.58

信心 confidence

相信可交付件将以所期望的或所声称的方式(即正确地、可信赖地、实施安全策略、可靠地、高效地)执/运行。

2.1.59

行政管理的安全 administrative security

用于信息安全的行政管理措施。

2.1.60

形式化(的) formal

在完备数学概念基础上，采用具有确定语义并有严格语法的语言表达的。

2.1.61

序号 sequence number

一种时变参数，其值取自于指定的序列并在确定时间内不重复。

2.1.62

一致性 consistency

在某一系统或构件中，各文档或各部分之间统一的、标准化的和无矛盾的程度。

2.1.63

隐私 privacy

个人所具有的控制或影响与之相关信息的权限，涉及由谁收集和存储、由谁披露。

2.1.64

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。

2.1.65

用户数据 user data

由用户产生或为用户产生的数据，这些数据不影响 TSF 的运行。

2.1.66

域 field

数学中“域”的概念，即一个元素集合，在该集合上定义的二元运算加法和乘法，以及可用的域公理。

2.1.67

有效性 effectiveness

对某一系统或产品，在建议的或实际的操作使用条件下，表示其提供安全程度的性质。

2.1.68

有限状态模型 finite state model

一种由如下几部分组成的顺序状态机数学模型：一个有限的输入事件集，一个有限的输出事件集，一个有限的状态集，一个将状态和输入映射到输出的函数，一个将状态和输入映射到状态的函数（状态转移函数）和一项规定初始状态的规格说明。

2.1.69

真实性 authenticity

确保主体或资源的身份正是所声称的特性。真实性适用于用户、进程、系统和信息之类的实体。

2.1.70

正确性 correctness

在安全策略实现中，针对所指定的安全要求，某一产品或系统展现出其正确地实现了这些要求。

2.2 技术类

2.2.1 攻击与保护

2.2.1.1

安全范畴 security category

有关敏感信息访问范围的一种分组，以此分组加之分等级的安全级别能更精细地控制对数据的访问。

2.2.1.2

安全分级 security classification

根据业务信息和系统服务的重要性和受损影响，确定实施某种程度的保护，并对该保护程度给以命名。依据访问数据或信息需求，而确定的特定保护程度，同时赋予相应的保护等级。例：“绝密”、“机密”、“秘密”。

2.2.1.3

安全功能 security function

在系统中实施安全策略的部分。

2.2.1.4

安全功能策略 security function policy

SFP

描述了特定安全行为的一组规则，由系统安全功能执行并可表达为对系统的一组安全功能需求。

2.2.1.5

安全机制 security mechanism

实现安全功能，提供安全服务的一组有机组合的基本方法。

2.2.1.6

安全级别 security level

有关敏感信息访问的级别划分，以此级别加之安全范畴能更精细地控制对数据的访问。

2.2.1.7

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、私有性和可靠性等，而对信息系统所选择并施加的管理、操作和技术等方面的控制(即防御或对抗)。

2.2.1.8

安全审计 security audit

对信息系统的各种事件及行为实行监测、信息采集、分析，并针对特定事件及行为采取相应的动作。

2.2.1.9

安全事态数据 security event data

反映与系统、服务或网络安全状态有关的数据。例如：在入侵检测系统中由传感器收集和管理的信息。

2.2.1.10

安全套接层 secure sockets layer

SSL

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

2.2.1.11

安全外壳 secure shell

一种利用不安全的网络提供安全的远程登录的协议。

2.2.1.12

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系统之间，一种旨在按照给定的安全策略来保护网络的连接点。安全网关不仅仅包括防火墙，还包括提供访问控制和加密功能的路由器和交换机等。

2.2.1.13

安全相关要求 security-related requirements

直接影响系统安全的操作要求，或遵从某一安全策略的要求。

2.2.1.14

安全信息对象 security information object

SIO

安全信息对象类的一个实例。

2.2.1.15

安全信息对象类 security information object class

一种已经针对安全使用作了剪裁的信息对象类。

2.2.1.16

安全许可 security clearance

允许个体访问某一特定安全级别或低于该级别的数据或信息。

2.2.1.17

安全域 security domain

在信息系统中，单一安全策略下运行的实体的汇集。例如，由单个或一组认证机构采用同一安全策略创建的各公钥证书的汇集。

2.2.1.18

安全属性 security attribute

主体、用户(包括外部的IT产品)、客体、信息、会话和/或资源的某些特性，这些特性用于定义安全功能需求，并且其值用于实施安全功能需求。

2.2.1.19

被动模式 passive mode

文件传送协议的连接建立模式。

2.2.1.20

本体 principal

其身份能被鉴别的实体。

2.2.1.21

参照确认机制 reference validation mechanism

参照监视器概念的一种实现，具有以下特性：防篡改的、总是被调用的，而且相当简单的，能彻底地对其进行分析和测试。

2.2.1.22

操作者 operator

得到授权担任一个或多个角色的个人或代表个人运行的进程(主体)。

2.2.1.23

测量 measurement

针对实体的某一属性，采用一种测量单位，获得测量值的动作或一系列动作。

2.2.1.24

测量方法 measurement method

描述有关测量的操作逻辑序列。测量方法的类型取决于用于量化特征的操作类型。

主要有两种类型：

主观型——根据人判断予以量化；

客观型——根据数值规则予以量化。

2.2.1.25

测量形式 form of measurement

一组运算，或是一种测量方法、计算函数，或是分析模型，目的是确定测量值。

2.2.1.26

插空攻击 interleaving attack

一种冒充，使用了从一个或多个正在进行的或以前鉴别交换中所导出的信息。

2.2.1.27

传感器 sensor

监视器 monitor

探针 probe

从被观察的信息系统中，通过感知、监测等收集事态数据的一种部件或代理。

2.2.1.28

传输层安全协议 transport layer security protocol

一种作为安全套接层协议的后继的正式互联网协议。

2.2.1.29

传输抗抵赖 non-repudiation of transport

NRT

为消息原发者提供证据的服务，证明交付机构已经将消息发送给了指定的接收者。

2.2.1.30

传输抗抵赖权标 NRT token

允许原发方或交付机构为某一消息建立传送抗抵赖的数据项。

2.2.1.31

串行线互联网协议 serial line internet protocol

一种采用电话线(串行线)传送数据的包成帧协议。

2.2.1.32

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(无需验证)的数据库。

2.2.1.33

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。

2.2.1.34

带外 out of band

通过通常的物理方式进行一些信息处理事务。

2.2.1.35

抵赖 repudiation

在通信系统所涉及的若干实体中，一个实体否认参与全部或部分通信过程。

注：在技术与机制的描述中，术语“抗抵赖”经常用来表示在通信系统中所涉及的若干实体，没有一个实体能否认它参与了通信。

2.2.1.36

点对点协议 Point-to-Point Protocol

PPP

在点对点链路上，封装网络层协议信息的一种标准方法。

2.2.1.37

端口 port

某一个连接的端点。对于物理连接，端口就是物理接口；对于逻辑连接，端口则是传输控制协议或用户数据报协议的逻辑信道端点，例如80端口是默认的超文本传送协议(http)信道的端点。

2.2.1.38

多级设备 multilevel device

一种功能单元，它能同时处理两个或多个安全级别的数据而不会危及计算机。

2.2.1.39

发送抗抵赖 non-repudiation of sending

防止发送者否认已发送了消息的服务。

2.2.1.40

反射攻击 reflection attack

将以前接收的消息发回给其原发者的一种冒充攻击手段。

2.2.1.41

访问级别 access level

主体对受保护的客体进行访问所要求的权限级别。

2.2.1.42

访问控制 access control

一种保证数据处理系统的资源只能由被授权主体按授权方式进行访问的手段。

2.2.1.43

访问控制[列]表 access control list

由主体以及主体对客体的访问权限所组成的列表。

2.2.1.44

访问类型(用于计算机安全) access type(in computer security)

由访问权所规定的操作类型。例如:读、写、执行、添加、修改、删除与创建。

2.2.1.45

访问期 access period

访问权的有效期限。

2.2.1.46

访问权 access right

允许主体以某一类型的操作访问某一客体。

2.2.1.47

访问受控系统 controlled access system

使物理访问控制达到自动化的手段。例如:使用磁卡、智能卡、生物测定(生物特征)阅读器等进行自动化物理访问控制的系统。

2.2.1.48

访问许可 access permission

主体针对某一客体所拥有的访问权。

2.2.1.49

非军事区 demilitarised zone

介于网络之间作为“中立区”的安全主机或小型网络(又称“掩蔽子网”),形成的一个安全缓冲区。

2.2.1.50

分析攻击 analytical attack

运用分析方法试图解开代码或找到密钥的行动。

2.2.1.51

封装安全净载 encapsulating security payload

一种基于IP、对数据提供保密性服务的协议。具体地讲,该协议提供加密安全服务,以保护IP包的数据内容。

2.2.1.52

高级功能强度 SOF-high

安全功能强度级别中较高的，其功能足以使评价对象对抗高潜力攻击者有计划、有组织的攻击。

2.2.1.53

跟入 to tailgate

未经授权尾随授权人通过控制机制获得物理/逻辑访问。

2.2.1.54

公证 notarization

公证方就某一活动或事件中涉及的各实体、所存储或通信的数据的性质而出具证据的过程。

2.2.1.55

公证方 notary

公证机构 notary authority

一种可以提供证据的可信第三方，可以为涉及某动作或事件的实体和存储或通信的数据提供证据，或者将现有权标的生命期延长到期满和被撤销以后。

2.2.1.56

公证权标 notarization token

由公证人生成的抗抵赖权标。

2.2.1.57

功能强度 strength of function

SOF

信息系统/产品的安全功能的一种指标：表示通过直接攻击其基础安全机制，攻破所设计的安全功能所需要的最小代价。

2.2.1.58

攻击 attack

在信息系统中，对系统或信息进行破坏、泄露、更改或使其丧失功能的尝试(包括窃取数据)。

2.2.1.59

攻击潜力 attack potential

成功实施一次攻击或将要发起一次攻击的潜在能力，用攻击者的专业水平、资源和动机来表示。

2.2.1.60

攻击特征 attack signature

执行某种攻击的计算机活动序列或其变体，通常通过检查网络流量或主机日志加以确定，入侵检测系统也依其来发现已经发生的攻击。

2.2.1.61

过滤 filtering

根据规定的准则，接收或拒收网络数据流的过程。

2.2.1.62

互联网安全多用途邮件扩展 multipurpose internet mail extensions

MIME

一种用于提供安全的多用途邮件交换的协议。

2.2.1.63

环境变量 environmental variables

授权决策所需要的与策略有关信息，它们不包括在静态结构中，但特定权限的验证者可通过本地手

段来获得(例如,当天时间或当前的账目结余)。

2.2.1.64

回调 call-back

在发生错误或故障时,为确保数据的完整性,将处理返回到预先确定位置的过程。

2.2.1.65

基本级功能强度 SOF-basic

安全功能强度级别中较低的,其功能足以使评价对象对抗低潜力攻击者的偶发攻击。

2.2.1.66

基准监视器 reference monitor

执行 TOE 访问控制策略的抽象机概念。

2.2.1.67

计算机系统审计 computer-system audit

检查计算机系统所用的规程,评估它们的有效性和准确性,并提出改进建议。

2.2.1.68

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

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

2.2.1.69

技术控制 technical controls

信息系统通过该系统内包含在硬件、软件或固件等部件中的机制来实现和执行的安全控制措施(防御措施和对抗措施)。

2.2.1.70

简单功率分析 simple power analysis

对指令执行的模式(或各单个指令的执行)所作的一种直接分析:监视某一加密模块用电功耗的变化,以便揭示加密算法的特征和实现,得到密钥的值。

2.2.1.71

简单邮件传送协议 simple mail transfer protocol

一种用于向邮件服务器发送邮件的互联网协议。

2.2.1.72

交付抗抵赖 non-repudiation of delivery

NRD

防止接收方否认已接收过消息并认可消息内容的服务。

2.2.1.73

交付抗抵赖权标 NRD token

允许原发方为某一消息建立交付抗抵赖的数据项。

2.2.1.74

接收抗抵赖 non-repudiation of receipt

防止接收者否认已接收了消息的服务。

2.2.1.75

拒绝服务 denial of service

一种使系统失去可用性的攻击。

2.2.1.76

抗抵赖策略 non-repudiation policy

一组提供抗抵赖服务的准则。具体而言，可以用于生成和验证证据及裁决的一组规则。

2.2.1.77

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

要求为某特定事件或动作生成抗抵赖证据的实体。

2.2.1.78

抗抵赖交换 non-repudiation exchange

以抗抵赖为目的，一次或多次传送抗抵赖信息所组成序列。

2.2.1.79

抗抵赖权标 non-repudiation token

一种特殊类型的安全权标，包括证据及可选的附加数据。

2.2.1.80

抗抵赖信息 non-repudiation information

NRI

由以下三部分组成的一个信息集合：

1) 关于为其生成证据并加以验证的某一事件或动作的信息；

2) 证据本身；

3) 实行中的抗抵赖策略。

2.2.1.81

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 PPP 的多个、任选的鉴别机制(包括纯明文口令、询问-响应和任意的问答)的框架。

2.2.1.82

可信路径 trusted path

用户与 TSF 间的一种通信手段，通过该手段它们能以必要的可信度进行通信。

2.2.1.83

可信通道 trusted channel

TSF 和远程可信 IT 产品间的一种通信手段，通过该手段它们能以必要的可信度(信心)进行通信。

2.2.1.84

TSF 控制外传送[数据] transfers outside TSF control

向不在 TSF 控制下的实体传输数据。

2.2.1.85

流量分析 traffic analysis

通过观察通信流量而推断所关注的信息，例如通信流量的存在、不存在、数量、方向和频次等。

2.2.1.86

路由器 router

用来建立和控制两个不同网络间数据流的网络设备，它是通过基于路由协议机制和算法来选择路线或路由来实现建立和控制的，它们自身可以基于不同的网络协议。路由信息被存储在路由表内。

2.2.1.87

逻辑炸弹 logic bomb

一种恶性逻辑程序，当被某个特定的系统条件触发时，造成对数据处理系统的损害。

2.2.1.88

冒充 masquerade

一个实体伪装成另一个实体。

2.2.1.89

迷惑 to spoof

为欺骗用户、观察者(如监听者)或骗取资源而采取的行动。

2.2.1.90

蜜罐 honeypot

一种用来欺骗、扰乱和引开攻击者的诱饵系统,促使攻击者把时间花在虚假信息上。

2.2.1.91

免前缀表示 prefix free representation

数据元素的一种表示,若将该表示与任何其他数据拼接时都不产生一种有效表示。

2.2.1.92

敏感标记 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标记作为强制访问控制决策的依据。

2.2.1.93

目录服务 directory service

一种从明确定义的对象的分类目录中搜索和检索信息的服务,可包括证书、电话号码、访问条件、地址等信息。

2.2.1.94

能力[列]表 capability list

标识主体对所有客体访问类型的列表。

2.2.1.95

凭证 credentials

为确定实体所声称的身份而提供的数据。

2.2.1.96

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。

2.2.1.97

区分性标识符 distinguishing identifier

无歧义地区分出某一实体的信息。

2.2.1.98

认可多重性参数 accreditation multiplicity parameter

一个正整数,它等于由认可机构为一个实体所提供的秘密认可信息项的数目。

2.2.1.99

冗余标识 redundant identity

从一个实体的标识数据通过增加冗余而得到的数据项序列。

2.2.1.100

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，以及何时发生及如何发生。

2.2.1.101

入侵检测系统　intrusion detection system

IDS

在信息系统和网络中，一种用于辨识某些已经尝试、正在发生或已经发生的入侵行为，并可对其做出响应的技术系统。

2.2.1.102

设置陷阱　entrapment

通过在信息系统中故意设置若干纰漏，以检测到蓄意的侵入，或使入侵者弄不清要利用哪一个纰漏。

2.2.1.103

审计踪迹(用于计算机安全)　audit trail(in computer security)

收集的数据，以备在安全审计时使用。

2.2.1.104

渗透　penetration

绕过系统安全机制的、未经授权的动作。

2.2.1.105

隧道　tunnel

在联网的设备之间，一种隐藏在其他可见性更高的协议内部的数据路径。

2.2.1.106

提交抗抵赖　non-repudiation of submission

NRS

一种提供证据的服务，证明交付机构已接受到需传送的消息。

2.2.1.107

提交抗抵赖权标　NRS token

允许原发方(发送方)或交付机构为已经提交供传送的消息建立提交抗抵赖的数据项。

2.2.1.108

网络访问服务器　network access server

为远程客户端提供对某一基础设施访问的系统(通常是一台计算机)。

2.2.1.109

网络扫描　network scanning

对网络上的在用主机进行鉴识的过程，是进行网络安全评估或实施网络攻击的前提。

2.2.1.110

文件保护　file protection

为了防止对文件未经授权地访问、修改或删除，而采取的管理、技术或物理手段。

2.2.1.111

文件传输协议　file transfer protocol

数据文件从一个计算机运动到另一个计算机，以 TCP 为基础、应用层的互联网标准协议。

2.2.1.112

无线保真　Wireless Fidelity

WiFi

由无线保真联盟推动使用无线局域网设备的标志。

2.2.1.113

无线保真保护接入 WiFi protected access

一种为无线通信提供保密性和完整性的安全增强规范。该规范包括临时密钥实现协议。无线保真保护的接入是有线等效隐私的后继。

2.2.1.114

物理保护 physical protection

使用物理手段保护密码模块、关键安全参数和公开安全参数等。

2.2.1.115

物理访问控制 physical access control

使用物理机制实施访问控制。例如将计算机放在上锁的房间内。

2.2.1.116

响应 response

由声称方产生的规程参数，并由验证方处理，以校验声称方身份。

2.2.1.117

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。

注：在虚拟私有网(VPN)技术中这种方法可用于建立隧道。

2.2.1.118

信息安全指示器 information security indicator

应用于一个或多个度量单位的分析模型而产生的结果，其中度量单位与决策准则或信息要求是有关的。

2.2.1.119

虚拟专用网 virtual private network

一种采用隧道技术连接的虚拟网络，即受限使用的逻辑计算机网络，该网络基于物理网络系统资源所构建，穿越实际网络建立连接。

2.2.1.120

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：黑客可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以合法地利用嗅探器来排查网络中的问题。

2.2.1.121

隐蔽通道 covert channel

允许进程以违背系统安全策略的方式传输信息的通信信道。

2.2.1.122

隐私保护 privacy protection

为保护隐私而采取的措施。例如：对个人数据的收集、处理和使用加以限制。

2.2.1.123

用户数据报协议 user datagram protocol

一种用于无连接通信的互联网联网协议。

2.2.1.124

有线等效保密 wired equivalent privacy

一种在IEEE82.2.1.11(无线局域网规范)中定义，采用128比特密钥提供流密码加密的密码协议。

2.2.1.125

原发方 originator

一种实体，将消息发送给接收方，或提供可用的抗抵赖服务消息。

2.2.1.126

源抗抵赖 non-repudiation of origin

NRO

防止消息原发者否认已创建消息内容并且已发送了消息的服务。

2.2.1.127

源抗抵赖权标 NRO token

允许接收方为某一消息建立原发抗抵赖的数据项。

2.2.1.128

远程访问 remote access

从另一网络或者从一个并不永久连接到所访问网络的终端设备上访问网络资源的过程。

2.2.1.129

远程访问拨入用户服务 remote access dial-in user service

一种用于鉴别远程用户的互联网安全协议。

2.2.1.130

远程访问服务 remote access service

提供远程访问的硬件和软件。

2.2.1.131

远程用户 remote user

物理地点不在其正使用的网络资源所处位置的用户。

2.2.1.132

运行控制 operational controls

主要由人(而不是系统)对信息系统配备并执行的安全控制(例如，安全防护和对策)。

2.2.1.133

证据 witness

一个为验证方提供证明的数据项。

2.2.1.134

证明 proof

用于证实某一事物的真实性和存在性的一种证据。例如：在抗抵赖中，按照有效抗抵赖策略验证证据是合法的。

2.2.1.135

知晓抗抵赖 non-repudiation of knowledge

防止接收方否认已关注接收消息内容的服务。

2.2.1.136

质询 challenge

由验证者随机选择并发送给声称者的数据项，声称者使用此数据项连同其拥有的秘密信息产生一个发给验证者的应答。

2.2.1.137

中级功能强度 SOF-medium

评价对象的安全功能强度级别中居中的，其功能足以使评价对象对抗中等潜力攻击者直接或故意的攻击。

2.2.1.138

重放攻击 replay attack

一种主动攻击方法，攻击者通过记录通信会话，并在以后某个时刻重放整个会话或者会话的一部分。

2.2.1.139

注册 registration

项进行赋值的过程。

2.2.1.140

注册簿 register

包含项标号及其关联的定义和有关信息的一组文件(电子版或电子版与纸版的结合)。

2.2.1.141

追踪 tracing

在两个实体集合之间的一种简单有向关系，即可从第一个集合中的一些实体追溯到第二个集合中一些实体。

2.2.1.142

最小特定权限 minimum privilege

主体的访问权限的最低限度，即仅执行授权活动所必需的那些权利。

2.2.2 **鉴别和密码类**

2.2.2.1

安全信封 secure envelope

一个由某一实体构造的数据项集合，其构造方式为：持有秘密密钥的实体能验证其完整性和原发方。

2.2.2.2

八位位组串 octet string

由八位位组所组成的序列。

注：适当时，只需将各八位位组分量全部拼接在一起，就可以将八位位组串解释为比特串。

2.2.2.3

比特串 bit string

具有 0 或 1 值的二进制数序列。

2.2.2.4

***n* 比特分组密码 *n*-bit block cipher**

一种其明文和密文分组的长度均为 n 比特的分组密码。

2.2.2.5

标记 label

一种八位组串，以非易变方式绑定到密文的公开信息。它既可作为非对称密码中加解密算法的输入，也可作为数据封装机制的输入。

2.2.2.6

标识数据 identification data

一种分配给某一实体，用于对其进行标识的数据项序列，该序列包括实体的可区分标识符。

注：标识数据可包含附加的数据项，例如签名过程标识符、签名密钥校对符、签名密钥有效期、对密钥用法的限制、关联的安全策略参数、密钥系列号或域参数等。

2.2.2.7

补充的校验字符 supplementary check character

不属于受保护的字符集的校验字符。

2.2.2.8

不可恢复部分　non-recoverable part

消息中的一部分，与签名一起存储或发送；当对消息进行全部恢复时，此部分为空。

2.2.2.9

不可逆加密　irreversible encryption/irreversible encipherment

单向加密　one-way encryption

一种加密，它只产生密文，而不能将密文再生为原始数据。

注：不可逆加密用于鉴别。例如，口令可被不可逆地加密，产生的密文被存储。以后出示的口令将同样被不可逆的加密，然后将两串密文进行比较。如果它们是相同的，则后来出示的口令是正确的。

2.2.2.10

操纵检测码　manipulation detection code

MDC

一种位串，它是附属于数据的一种函数，以允许操纵检测。

注1：可以加密结果消息(数据加 MDC)，以便获得保密性或数据鉴别。

注2：用于生成 MDC 的函数必须是公开的。

2.2.2.11

差分能量分析　differential power analysis

为提取与加密操作相关的信息，对密码模块的用电功耗的变化所作的分析。

2.2.2.12

拆分知识　split knowledge

将某一密钥拆分成多个部分的过程，使各个部分没有原密钥的共享知识，可由不同实体作为密码模块的输入或输出，并予组合来重新生成原来的密钥。

2.2.2.13

策略映射　policy mapping

当某个域中的一个 CA 认证另一个域中的一个 CA 时，第一个域中的证书认证机构将第二个域中的特定证书策略进行转换，使之等价(但不必完全相同)于第一个域中的特定证书策略。

2.2.2.14

初始变换　initial transformation

算法起始时所应用的函数。

2.2.2.15

初始化值　initializing value

一个函数(例如：消息鉴别码函数)起始时所赋予的值。

2.2.2.16

纯非确定性随机比特生成器　pure non-deterministic random bit generator

一种其所有熵源都属于非确定性的(物理的或非物理的)非确定性随机比特生成器。

2.2.2.17

纯确定性随机比特生成器　pure deterministic random bit generator

一种其所有熵源都是种子的确定性随机比特生成器。

2.2.2.18

从 A 到 B 的密钥证实　key confirmation from A to B

向实体 B 保障，实体 A 拥有所指正确密钥。

2.2.2.19

从 A 到 B 的隐式密钥鉴别　implicit key authentication from A to B

向实体 B 保障，实体 A 可能是拥有正确密钥的唯一实体。

2.2.2.20

从A到B的显式密钥鉴别 explicit key authentication from A to B

对实体B保障，A是除B之外拥有正确密钥的唯一实体。

注：从A到B的隐式密钥鉴别和从A到B的密钥证实，隐含着从A到B的显式密钥鉴别。

2.2.2.21

篡改响应 tamper response

当检测到发生篡改时，密码模块自动采取的行动。

2.2.2.22

单向函数 one-way function

具有如下特性的函数，对给定输入，易于计算其输出，但对于给定输出，找到映射为该输出的输入在计算上是不可行的。

2.2.2.23

点对点密钥建立 Point-to-Point key establishment

在两个实体之间，不涉及第三方直接建立密钥。

2.2.2.24

电子密钥传输 electronic key transport

采用计算机网络等电子手段，通常以加密形式传送密钥的操作。

2.2.2.25

电子密钥注入 electronic key entry

采用智能卡或密钥装入器等电子方法把密钥注入到密码模块的操作。

注：该密钥的操作员可能不知道正注入的密钥的值。

2.2.2.26

对称密码 symmetric cipher

一种在加密和解密算法中都使用相同的秘密密钥的密码技术。

2.2.2.27

对称密码技术 symmetric cryptographic technique

原发方的变换和接收方的变换均采用同一秘密密钥的密码技术。

2.2.2.28

多重对参数 pair multiplicity parameter

在鉴别机制的某一实例中，所涉及的非对称数对的个数。

2.2.2.29

反馈缓冲区 feedback buffer

为加密过程存储输入数据的变量。反馈缓冲区初始化的值为初始变量的值。

2.2.2.30

非对称加密体制 asymmetric encipherment system

非对称密码 asymmetric cipher

基于非对称密码技术的体制，公开变换用于加密，私有变换用于解密。反之，亦然。

2.2.2.31

非对称密码技术 asymmetric cryptographic technique

一种采用了两种相关的变换，由公钥定义的公开变换和由私钥定义的私有变换的密码技术。这两个变换具有如下特性，即对给定的公钥导出私钥在计算上是不可行的。

2.2.2.32

非对称密码体制 asymmetric cryptosystem

加密和解密使用相关但不相同的密钥，则这个密码体制被称为非对称的。

2.2.2.33

非对称密钥对　asymmetric key pair

一对相关的密钥，其中私有密钥规定私有变换，公开密钥规定公开变换。

2.2.2.34

非对称签名体制　asymmetric signature system

基于非对称密码技术的体制，私有变换用于签名、公开变换用于验证。

2.2.2.35

CRL 分布点　CRL distribution point

一个 CRL 目录项或其他 CRL 分发机构，由其分发的 CRL 可以包括仅对某 CA 所发证书全集的某个子集的撤销条目，或者可以包括有多个 CA 的撤销条目。

2.2.2.36

分组长度　block length

一个信息分组的比特位数。

2.2.2.37

附录　appendix

由签名和一个任选文本字段构成的比特串。

2.2.2.38

赋值　assignment

是一个数据项，它是消息的证据函数或可能是部分消息的证据函数，赋值形成签名函数的部分输入。

2.2.2.39

个人安全环境　personal security environment

为保存实体的私钥、直接可信的认证机构密钥及(可能的)其他数据而使用的本地安全存储。根据该实体或系统要求的安全策略，这种环境可以是(例如)经加密保护的文件，也可以是防篡改的硬件令牌。

2.2.2.40

公开安全参数　public security parameter

与安全有关的公开信息，对其修改可损害密码模块的安全。例如公钥、公钥证书、自签证书、可信锚、与计数器关联的一次性口令等。

2.2.2.41

公开加密变换　public encipherment transformation

由非对称加密系统和非对称密钥对的公开密钥确定的加密变换。

2.2.2.42

公开加密密钥　public encipherment key

用于定义公开加密变换的公开密钥。

2.2.2.43

公开密钥/公钥　public key

在某一实体的非对称密钥对中，能够公开的密钥。

2.2.2.44

公开验证密钥　public verification key

一种数据项，在数学上与私有签名密钥相对应，可为所有实体所知，并由验证方在签名验证过程中使用。

2.2.2.45

公钥导出函数 public key derivation function

一个域参数，它的功能是将比特串映射成正整数。

注1：这个函数用于将实体标识数据转换成实体验证密钥，并符合下列两个性质：

要找出任何一对映射成同一输出的两个不同的输入数据，在计算上是不可行的。

随机选取数值Y，Y在函数值域范围内的概率小到可以忽略；或者对给定的输出数据，找出可映射成该输出的输入，在计算上是不可行的。

注2：可忽略性与计算上的不可行性依赖于具体的安全要求和环境。

2.2.2.46

公钥体系（用于数字签名） public key system (for digital signature)

由以下三种功能组成的密码体制：

密钥产生，即一种用于生成密钥对（由一个私有签名密钥和一个公开验证密钥构成）的方法。

签名产生，即一种用于从消息代表F和私有签名密钥生成签名Σ的方法。

签名打开，即一种用于从签名Σ和公开验证密钥来恢复消息代表F^*的方法。这一功能的输出还包含关于签名打开规程成败的指示。

2.2.2.47

公钥信息 public key information

至少包含实体可区分标识符和公钥的信息。该信息被限制为关于一个实体的数据和该实体的公钥。该信息还可包括认证机构、实体、公钥、密钥应用限定、有效期或相关算法等相关内容。

2.2.2.48

公钥证书 public key certificate

由证书权威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。

2.2.2.49

固件 firmware

存储在密码边界内的硬件（如ROM，PROM或者FLASH）中的密码模块程序和数据，在执行时不能被动态地写或修改。

2.2.2.50

关键安全参数 critical security parameter

CEP

与安全有关的信息（例如：秘密的和私有密码密钥，口令之类的鉴别数据，个人身份号、证书或其他可信锚），其泄露或修改会危及密码模块的安全。

注：关键安全参数可能是明文的或加密的。

2.2.2.51

归纳函数 reduction-function

一种应用于长度为L_Φ的块H_q，生成长度为L_p的散列/杂凑码H的函数。

2.2.2.52

S盒 S-box

用于实现密码变换的非线性代替表。

2.2.2.53

后向保密 backward secrecy

不能从当前值或后续的各值确定先前各种值的保障。

2.2.2.54

环境失效保护 environmental failure protection

使用一些特定功能来保护由于环境条件或环境波动超出模块正常操作范围所造成的密码模块泄密。

2.2.2.55

环境失效测试 environmental failure testing

使用特定方法提供合理保障：当环境条件或环境波动超出某一密码模块的正常运行范围时该模块不会泄密。

2.2.2.56

混合密码 hybrid cipher

将非对称密码技术和对称密码技术结合起来的非对称密码机制。

2.2.2.57

混合型非确定性的随机比特生成器 hybrid non-deterministic random bit generator

Hybrid NRBG

采用种子值作为附加熵源的(物理的或非物理的)非确定性随机比特生成器。

2.2.2.58

混合型确定性的随机比特生成器 hybrid deterministic random bit generator

Hybrid DRBG

采用非确定性熵源作为附加熵源的确定性随机比特生成器。

2.2.2.59

获准的操作模式 approved mode of operation

仅使用已获批准的安全功能的密码模块的一种模式。

2.2.2.60

加密 encipherment/encryption

对数据进行密码变换以产生密文的过程。一般包含一个变换集合，该变换使用一套算法和一套输入参量。输入参量通常被称为密钥。

2.2.2.61

加密鉴别机制 authenticated encryption mechanism

一种用于保护数据的保密性并保证数据的原发地和数据完整性的密码学技术，由加密算法、解密算法和生成密钥方法三个分过程组成。

2.2.2.62

加密选项 encryption option

一种可传递给非对称密码的或密钥封装机制的加密算法的选项，以控制输出密文的格式。

2.2.2.63

检错码 error-detection code

一种依据数据计算出的值，由为了检测(但不能校正)该数据无意改变而设计的冗余比特组成。

2.2.2.64

鉴别加密 authenticated encryption

对某一数据串的加密，旨在保护数据保密性、数据完整性以及数据原发鉴别。

2.2.2.65

鉴别码 authentication code

由消息鉴别码算法输出的比特串。

注：MAC有时称为密码校验值。

2.2.2.66

鉴别数据 authentication data

用来验证用户所声称身份的信息。

2.2.2.67

鉴别权标 authentication token

在强鉴别的交换过程中传送的一种信息，可用于鉴别其发送者。

2.2.2.68

交换多重性参数 exchange multiplicity parameter

一个正整数，用以表达在一个鉴别机制中信息交换次数。

2.2.2.69

解密 decipherment/decryption

将密文转换为明文的处理，即加密对应的逆过程。

2.2.2.70

抗抵赖 non-repudiation

也称不可否认，证明一个操作或事件已经发生且无法否认的机制。

2.2.2.71

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

满足如下性质的散列函数：找到两个不同的输入能映射到同一个输出，在计算上是不可行的。

注：计算上的可行性依赖于特定的安全要求和环境。

2.2.2.72

可辨别编码规则 distinguished encoding rules

DER

一类编码规则，可应用于 ASN.1 符号体系所定义的类型的值。应用这些编码规则产生了这些值转换句法，这意味着可用同样的规则进行解码。

注：DER 更适用于要求编码值足够小，且能够快速跳过某些嵌套值的情形。

2.2.2.73

可卸封盖 removable cover

允许触及密码模块物理内容的一种物理手段。

2.2.2.74

客户 client

在公钥密码体制中，使用 PKI 来获得证书并且去验证证书和签名的功能的人或终端实体。

2.2.2.75

控制信息 control information

注入到密码模块中，用于引导该模块运行的信息。

2.2.2.76

口令 password

用于身份鉴别的秘密的字、短语、数或字符序列，通常是被默记的弱秘密。

2.2.2.77

口令鉴别密钥检索 password-authenticated key retrieval

一种密钥检索过程。其中，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 检索到，但不能由 B 导出的秘密密钥。

2.2.2.78

口令鉴别密钥协商 password-authenticated key agreement

使用预共享的基于口令的信息，在两个实体之间建立一个或多个共享秘密密钥的过程。其中，共享的基于口令的信息是指这两个实体具有相同的共享口令，或一个具有口令而另一个具有口令验证数据；共享秘密密钥的值对两个实体而言都不能预先确定。

2.2.2.79

口令验证数据 password verification data

用于验证某一实体是否知晓特定口令的数据。

2.2.2.80

块/分组 block

在本术语中，块是指一种定义了长度的比特串。

注：在本标准中，“块”限定为八比特组串(通常被解释为比特串)。

2.2.2.81

块/分组链接 block chaining

对信息加密时，每一密文块在加密时都依赖于前一密文块的方式。

2.2.2.82

块/分组密码 block cipher

所用密码算法对明文块(即定义了长度的比特串)进行运算，以产生的密文块的对称密码。

注：在本标准中，明文块与密文块均限制为八比特比特组串(通常被解释为比特串)。

2.2.2.83

块/分组密码密钥 block cipher key

控制块密码运算的密钥。

2.2.2.84

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这两者所导出的密钥权标。

2.2.2.85

流/序列密码 stream cipher

具有如下性质的对称密码体制：其加密算法利用某一可逆函数将明文符号序列与密钥流符号序列一次一个符号地组合起来进行变换。它可分为两种类型：同步流/序列密码和自同步流/序列密码。

2.2.2.86

轮函数 round function

迭代分组密码算法中重复使用的一种函数，通过数次迭代调用该函数，最后完成加解密运算。

注：轮函数作为散列/杂凑函数的组成部分迭代使用，将长度为 L_1 的数据串与以前输出的长度为 L_2 的数据串合一。

2.2.2.87

轮密钥 round keys

经密钥扩展函数运算产生的，在每次轮函数迭代运算中使用的密钥。

2.2.2.88

秘密 secret

为了执行特定安全功能策略，只能由授权用户或被评对象安全功能知晓的信息。

2.2.2.89

秘密参数 secret parameter

不在公开域中出现，仅供声称方使用的比特串或整数，例如一个私有整数。

2.2.2.90

秘密密钥 secret key

用于对称密码技术中的一种密钥，并仅由一组规定实体所使用。

2.2.2.91

秘密值导出函数 secret value derivation function

利用一个密钥权标因子、一个密钥权标和其他参数作为输入，输出一个秘值的函数，该函数用来计

算一个或多个秘密密钥。

2.2.2.92

密码 cipher

一种用于保护数据保密性的密码学技术，由加密算法、解密算法和密钥生成方法及相应运行过程组成。

2.2.2.93

密码边界 cryptographic boundary

一个明确定义的连续周界，该周界确定了密码模块的物理界限，并包含密码模块的所有硬件、软件和/或固件成分。

2.2.2.94

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。

2.2.2.95

密码分析攻击 cryptanalytical attack

运用密码分析方法，解开代码或找到密钥的企图或行为。

例：统计分析密码模式；搜索加密算法中的纰漏。

2.2.2.96

密码管理员 crypto office

由个体或过程（如“主体”）所担当的角色，代表个体行使密码模块初始化或密码模块管理功能。

2.2.2.97

密码破译 code breaking

在未知预先约定的情况下，采取适当的方法和技术，由密文获得明文的过程。

2.2.2.98

密码体制 cryptographic system

从明文到密文和从密文到明文的变换规则的集合，其中通常用一种数学算法来定义这些变换。

2.2.2.99

密码同步 cryptographic synchronization

一种相互协调的加密和解密过程。

2.2.2.100

密码系统 cryptosystem

具有信息加密和解密功能的系统，由算法、协议、部件和设备等构成。

2.2.2.101

密码校验函数 cryptographic check function

以秘密密钥和任意字符串作为输入，并以密码校验值作为输出的密码变换。不知道秘密密钥就不可能正确计算校验值。

2.2.2.102

密码校验和 cryptographic checksum

一种赋予文件的数值，用于后期对该文件进行“测试”，以便验证其中包含的数据是否遭到恶意更改。

2.2.2.103

密码校验值 cryptographic check value

通过在数据单元上执行密码变换而得到的信息。

2.2.2.104

密码学 cryptology

研究编制、分析和破译密码的学科，包括密码算法、密码协议和密码系统等的设计与分析的原理、方法和工具。

2.2.2.105

密文 ciphertext

利用加密技术，经变换，信息内容被隐藏起来的数据。

2.2.2.106

密钥 key

一种用于控制密码变换操作(例如加密、解密、密码校验函数计算、签名生成或签名验证)的符号序列。

2.2.2.107

密钥部件 (cryptographic)key component

在安全功能中，执行密码功能所用的参数。

2.2.2.108

密钥材料 keying material

确立和维持密码密钥关系所必需的数据(如密钥，初始化值)。

2.2.2.109

密钥长度 key length

密钥的比特位数。

2.2.2.110

密钥传送 key transport

在适当保护下，从一个实体到另一个实体传送密钥的过程。

2.2.2.111

密钥分发服务 key distribution service

由密钥分发中心提供的，将密钥安全地分发到予以授权实体的服务。

2.2.2.112

密钥分发中心 key distribution centre

KDC

一个实体，受信产生或获得密钥，并将其分发给每个与 KDC 具有共享密钥的实体。

2.2.2.113

密钥封装机制 key encapsulation mechanism

与非对称密码类似，但其加密算法采用一个公钥作为输入，生成一个秘密密钥并对该秘密密钥进行加密。

2.2.2.114

密钥管理 key management

根据安全策略，实施并运用对密钥材料进行产生、登记、认证、注销、分发、安装、存储、归档、撤销、衍生、销毁和恢复的服务。

2.2.2.115

密钥互鉴别 mutual key authentication

向两个实体保证，只有对方才有可能拥有正确密钥。

2.2.2.116

密钥加密密钥 key encryption key

用于对其他密钥进行加密或解密的密钥。

2.2.2.117

密钥检索 key retrieval

一种如下口令检索过程：其中实体 A 具有从某一口令导出的弱秘值，而另一实体 B 具有与 A 的弱秘值关联的强秘值；这两个实体利用各自的秘值，协商一个可由 A 重新找回（但未必可由 B 导出）的秘密密钥。

2.2.2.118

密钥建立 key establishment

为一个或多个实体产生一个可用的、共享的秘密密钥的过程。密钥建立包括密钥协商、密钥传送等。

2.2.2.119

密钥交换 key exchange

在通信实体之间安全地建立一个共享密钥的协商过程。

2.2.2.120

密钥控制 key control

选择密钥或选择密钥计算中所用参数的能力。

2.2.2.121

密钥流 keystream

有意保密的、由流密码的加密解密算法所使用的符号伪随机序列。即使攻击者知道部分密钥流，推导出该密钥流其余部分的任何信息，在计算是不可行的。

2.2.2.122

密钥流函数 keystream function

一种函数，其输入是密钥流生成器的当前状态和先前输出的部分密文（可选地），其输出为该密钥流的下一部分。

2.2.2.123

密钥流生成器 keystream generator

一种基于状态的过程（即一种有限状态机），以一个密钥、一个初始化向量以及密文（必要时）作为输入，输出是一个密钥流（即任意长度的比特序列或比特块）。

2.2.2.124

密钥派生函数 key derivation function

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

2.2.2.125

密钥权标 key token

在密钥建立机制执行期间，一个实体向另一个实体发送密钥建立的消息。

2.2.2.126

密钥权标生成函数 key token generation function

在密钥建立机制执行期间，利用某一密钥权标因子与其他参数作为输入，输出一个密钥权标的函数。

2.2.2.127

密钥权标校验函数 key token check function

在密钥建立机制执行期间，利用一个密钥权标与某些公开的其他已知参数作为输入，并输出一个布

尔值的函数。

2.2.2.128

密钥权标因子 key token factor

一种保密的整数，可与某一弱密值连接，生成一个密钥权标。

2.2.2.129

密钥生成算法 key generation algorithm

主要指生成非对称密钥对的方法。

2.2.2.130

密钥生成指数 key generation exponent

一个只有可信第三方才知道的，用于生成密钥的正整数。

2.2.2.131

密钥协商 key agreement

在实体之间建立一个共享的秘密密钥的过程，其中任何实体都不能预先确定该密钥的值。

2.2.2.132

密钥证实 key confirmation

使某一实体确信，另一已标识实体拥有正确的密钥。

2.2.2.133

密钥转换中心 key translation centre

KTC

为实体间提供密钥转换的受信实体，每个实体与 KTC 共享一个密钥。

2.2.2.134

密钥装载器 key loader

一种自包含装置，能够至少存储一个加密或未加密的密钥，或者密钥部件，根据请求可将其传送给某一密码模块。

2.2.2.135

明文 plaintext/cleartext

未加密的信息。

2.2.2.136

明文密钥 plaintext key

未加密的密钥。

2.2.2.137

模数 modulus

一个非负整数，其因子是保持秘密的，求解其因子在计算上是不可行的。模数可用做签名者参数或域参数。

2.2.2.138

平衡型口令鉴别密钥协商 balanced password-authenticated key agreement

一种基于口令鉴别的密钥协商，其中实体 A 与 B 都采用一个共享的基于口令的公共弱秘数值，对一个或多个共享的秘密密钥进行鉴别和协商。

2.2.2.139

起始变量 starting variable

一种可能从某一初始化值导出，并用于定义操作模式起始点的变量。

2.2.2.140

签名 signature

签名生成过程产生的一个或多个数据元素。用实体的私钥对相关数据进行密钥变换。

2.2.2.141

签名方 signer

生成某一数字签名的实体。

2.2.2.142

签名方参数 signer parameter

在一个特定域内，针对给定的签名方所提供的公开数据项、数或比特串。

2.2.2.143

签名方程 signature equation

一种用于定义签名函数的方程。

2.2.2.144

签名过程 signature process

输入消息、签名密钥和域参数，输出签名的过程。

2.2.2.145

签名函数 signature function

在签名过程中，一种由所用签名密钥和各个域参数定义的函数。

2.2.2.146

签名验证过程 signature verification process

其输入为已签署的消息、验证密钥和域参数，其输出为恢复后的消息(如果有效)的过程。

2.2.2.147

签名检验密钥 signature check key

与实体的签名密钥具有数学相关性并在检验过程中由验证者使用的数据项，即签名者的公钥。

2.2.2.148

签名密钥 signature key

在签名过程中，实体所特有的并只能由这个实体所使用的秘密数据项。

2.2.2.149

签名系统 signature system

一种基于非对称密码技术，其私有密钥用于签署变换，其公开密钥用于验证变换的系统。

2.2.2.150

签名检验过程 signature check process

输入签名消息、检验密钥和系统参数，确定输出数字签名是否有效的过程。

2.2.2.151

签名指数 signature exponent

一种与验证指数有关，用于产生各种签名的秘密数。

2.2.2.152

前向保密 forward secrecy

保障不能根据当前的值或以前的值来确定以后的值的一种途径。

2.2.2.153

前向互保密 mutual forward secrecy

在某一密钥协商运行后，对手利用实体 A 和 B 两者的长期私钥的知识，不可能重新计算出先前导出的密钥的特性。

2.2.2.154

强鉴别 strong authentication

通过密码技术产生凭证的方法进行的鉴别。

2.2.2.155

强秘密 strong secret

具有足够熵的秘值，即使给了能从猜想中区分出正确猜想的知识，对其进行穷尽搜索是不可行的。

2.2.2.156

增强型口令鉴别的密钥协商 augmented password-authenticated key agreement

一种口令鉴别的密钥协商，其中实体 A 采用一个基于口令的弱秘数值，实体 B 采用由 A 的弱秘数值的单向函数派生的验证数据来对一个或更多个共享秘密密钥进行鉴别和协商。

2.2.2.157

清零/零化 zeroisation

将已存储的数据和关键安全参数加以销毁的一种方法，以防止检索和重用。

2.2.2.158

穷举攻击/蛮力攻击 exhaustive attack/brute-force attack

通过尝试口令或密钥所有可能的值，以获取实际口令或密钥，并实施违反信息安全策略的行为。

2.2.2.159

(算法的)确定性 determinacy

给出相同输入，总能产生相同输出的算法的特征。

2.2.2.160

确定性随机比特生成器 deterministic random bit generator

DRBG

一种随机比特生成器，通过将确定性算法应用于适当的随机初始值(称为“种子”)产生随机样式的比特序列，其安全性可能不依赖于该随机比特生成器的某些二次输入。特别地，非确定性源还可能形成这些二次输入的组成部分。

2.2.2.161

人工密钥传送 manual key transport

带外(网络外)传送密钥的手段。

2.2.2.162

人工密钥注入 manual key entry

利用键盘之类的设备，将密钥录入到密码模块。

2.2.2.163

认证机构撤销列表 certification authority revocation list

一种撤销列表，它包含一系列颁发给证书认证机构的公钥证书，证书颁发者认为这些证书不再有效。

2.2.2.164

认证路径 certification path

目录信息树中对象的证书有序序列，通过处理该有序序列及其起始对象的公钥可以获得该路径的末端对象的公钥。

2.2.2.165

弱秘密 weak secret

一种能够方便地让人记住的秘密值，这意味着该秘密值的熵是局限的，有可能通过给定的正确猜想和不正确猜想的知识，猜到此秘密值。

2.2.2.166

散列/杂凑函数 hash function

将比特串映射为固定长度的比特串的函数，该函数满足下列两特性：

——对于给定输出，找出映射为该输出的输入，在计算上是不可行的；

——对于给定输入，找出映射为同一输出的第二个输入，在计算上是不可行的。

注：计算上的可行性取决于特定安全要求和环境。

2.2.2.167

散列/杂凑函数标识符 hash-function identifier

用于标识特定散列/杂凑函数的字节。

2.2.2.168

散列/杂凑化口令 hashed password

把一个散列/杂凑函数应用于一个口令所得的结果。

2.2.2.169

散列/杂凑码 hash-code

散列/杂凑函数的输出的比特串。

注：在相关文献中包含的各种术语，与“散列/杂凑代码”具有相同或类似的含义。例如“修改检测码(modification detection code)”、“摘要(digest)”、“散列/杂凑结果(hash-result)”、“散列/杂凑值(hash-value)”和“印迹(imprint)”。

2.2.2.170

散列/杂凑权标 hash-token

一个散列/杂凑码与一个可选的控制字段拼接而成的消息，该控制字段可用于标识所指散列/杂凑函数和填充方法。

注：除非散列/杂凑函数是由签名机制或由域参数唯一确定的，否则必须给出带有散列/杂凑函数标识符的控制字段。

2.2.2.171

声称方 claimant

为了鉴别的目的，本身是本体或代表本体的实体。声称方具备代表本体进行鉴别交换所必需的各种功能。

2.2.2.172

声称方参数 claimant parameter

在给定的声称方所在域内，其持有的公开数据项、数或比特串。

2.2.2.173

输出变换 output transformation

应用在算法中，对迭代操作的输出所进行的变换。

2.2.2.174

数-串转换 converting a number to a string

在缩约函数的运算期间，整数需要被转换为长度为 L 的比特串。其中要求这个比特串应该等同于该整数的二进制表示，该串的最左比特对应于二进制表示的最高有效位。如果比特串长度小于 L，则应在该串左侧以适当个数的 0 填充，使之长度为 L。

2.2.2.175

数据鉴别 data authentication

验证数据真实性的过程。例如：验证所收到的数据与所发送的数据是否相同。

2.2.2.176

数字签名 digital signature

附加在数据单元上的数据，或是对数据单元所作的密码变换，这种数据或变换允许数据单元的接收者用以确认数据单元的来源和完整性，并保护数据防止被人（例如接收者）伪造或抵赖。

2.2.2.177

私有解密变换 private decipherment transformation

由非对称加密系统和非对称密钥对的私有密钥确定的解密变换。

2.2.2.178

私有解密密钥 private decipherment key

用于定义私有解密变换的私有密钥。

2.2.2.179

私有密钥/私钥 private key

在某一实体的非对称密钥对中，只应由该实体使用的密钥。

注1：正常情况下，私钥不应泄露。

注2：在非对称签名体制的情况下，私钥定义签名变换。而在非对称加密体制的情况下，私钥定义解密变换。

2.2.2.180

私有签名密钥 private signature key

一种特定于某一实体的秘密数据项，在签名生成过程中只能由该实体使用。

2.2.2.181

随机比特生成器 random bit generator

一种设备和算法，其输出是一个比特序列，该比特序列表现为统计独立的和无偏的。

2.2.2.182

随机数 random number

其值不可预测的时变参数。

2.2.2.183

随机数发生器 randomizer

生成具有随机特性数值的机制。

2.2.2.184

随机数序列 random number sequence

数列中的每一项在已知其他项的情况下都无法被推断的一种数列。

2.2.2.185

随机元素导出函数 random element derivation function

一种利用某一口令和其他多个参数作为输入，其输出为随机元素的函数。

2.2.2.186

添加变量 salt

作为单向函数或加密函数的二次输入而加入的随机变量，可用于导出口令验证数据。

2.2.2.187

填充 padding

对数据串附加额外比特。

2.2.2.188

唯密文攻击 ciphertext-only attack

密码分析者只占有密文的一种分析攻击。

2.2.2.189

伪随机 pseudorandom

数或比特的一个序列，看似随机选出的，其实是通过确定性算法生成的。

2.2.2.190

伪随机比特生成器 pseudo-random bit generator

一种确定性算法，当给定某种形式、长度为 k 的比特序列时，该算法输出一个长度为 $l>k$ 的比特序列，将输出与真随机比特进行区分在计算上是不可行的。

2.2.2.191

伪随机数序列 pseudo-random number sequence

满足一定统计特性，并在具体情况下可用作随机数序列的数列。

2.2.2.192

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。可确认权限声称者特定权限的真实性。

2.2.2.193

无前缀集 prefix free set

由比特串或八位位组串组成的集合 S，其中不存在 x，$y \in S$，使 x 是 y 的前缀。

2.2.2.194

相互鉴别 mutual authentication

两个实体彼此提供身份保障的实体鉴别。

2.2.2.195

消息 message

有特定语义的、任意有限长度的比特串。

2.2.2.196

消息代表 message representative

采用散列/杂凑函数，依据一种格式机制，由消息导出的比特串。

2.2.2.197

消息分组 message block

杂凑算法中消息运算的块。消息分组的长度可为 128、256、512 等比特。

2.2.2.198

消息摘要 message digest

散列/杂凑算法的最终输出值。

2.2.2.199

消息鉴别 message authentication

验证消息是由声明的始发者发给预期的接收者，并且该消息在转移中未被更改。

2.2.2.200

消息鉴别码 message authentication code

MAC

消息鉴别码算法的输出的比特串。

2.2.2.201

消息鉴别码算法 MAC algorithm

一种带密钥的密码算法，用于计算将比特串和秘密密钥映射为定长比特串的函数，并满足以下两种性质：

——对任意密钥和任意输入串，该函数都能有效进行计算；

——对任一固定的密钥，该密钥在未知情况下，即便已知输入串集合中的第 i 个输入串和对应的函数值，且串集合中的第 i 个输入串值在观测前面的第 $i-1$ 个函数值之后可能已经选定，要算出该函数对任意新输入串的值在计算上是不可行的。

2.2.2.202

消息鉴别码算法密钥　MAC algorithm key

一种用于控制消息鉴别码算法运算的密钥。

2.2.2.203

校验　check

通过简单比对作出裁决，不需要评估专门知识。

2.2.2.204

校验值　check-value

由校验值函数计算并输出的比特串，由数据原发方发送给数据接收方，以使接收方能以此检查该数据的正确性。

2.2.2.205

校验值函数　check-value function

将各比特串和一个短秘密密钥(即从某一用户设备录入或从中读出的密钥)映射到定长比特串的函数 f，该函数满足以下性质：

——对任一密钥 k 和输入串 d，能高效算出函数 $f(d, k)$；

——在计算上不可能找到一对数据串(d, d')，使满足 $f(d, k)=f(d', k)$的密钥数多于可能的密钥集合的一小部分。

注 1：在实践中，短密钥一般包含 4～6 个数比特或字母数字字符。

注 2：在实践中，当校验值函数的可能的输出集合与可能的密钥集合的元素数相等时，安全达到最大化。

2.2.2.206

校验字符　check character

可通过该串的数学关系来验证串的正确性所使用的附加字符。

2.2.2.207

校验字符体系　check character system

产生校验字符的和校验包含校验字符的串的一组规则。

2.2.2.208

(安全参数)泄密　compromise

对关键安全参数的未授权的泄露、修改、替代或使用，或对公共安全参数的未经授权修改或替代。

2.2.2.209

选择明文攻击　chosen-plaintext attack

已知明文攻击　known-plaintext attack

密码分析者能选取有限的明文消息和相对应的密文的一种分析攻击。

2.2.2.210

压缩函数　compression function

基于布尔函数、置换函数和多次迭代变换而构成的一种函数。

2.2.2.211

掩码生成函数　mask generation function

一种将各种比特串映射为任意指定长度比特串的函数，并满足如下特性：根据给出输出(而不是输入)的一部分预测该输出的另一部分，在计算上是不可行的。

2.2.2.212

验证过程 verification process

输入经签署的消息、验证密钥和域参数，输出签名验证结果(即有效或无效)的过程。

2.2.2.213

验证密钥 verification key

与实体的签名密钥有关，在验证过程中由验证方使用的一个数据项。

2.2.2.214

已签消息 signed message

一组由签名中不能恢复的消息部分、签名以及可选的文本字段等数据项组成的集合。

2.2.2.215

印迹 imprint

一种比特串，或是一个数据串的散列/杂凑码，或是该数据串本身。

2.2.2.216

预签名 pre-signature

由签名过程计算出来的值，该值是一个随机生成器的函数但与消息无关。

2.2.2.217

域模数 domain modulus

又称域参数，它是一个只有可信第三方才知道的、由两个不同的素数相乘产生的正整数。

2.2.2.218

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。

2.2.2.219

CA 证书 CA-certificate

由一个 CA 颁发给另一个 CA 的证书。

2.2.2.220

证书策略 certificate policy

命名的一组规则，指出证书对具有共同安全要求的特定团体和/或应用的适用性。

2.2.2.221

证书撤销列表 certificate revocation list

CRL

由证书认证机构签署的一个失效证书列表，它给出了一套证书发布者认为无效的证书。

2.2.2.222

证书确认 certificate validation

确认证书在给定时间内有效的过程，包含一个证书路径的构造和处理，确保所有证书在给定时间内在路径上的有效性(也就是说没有废除或者期满)。

2.2.2.223

证书认证机构 certificate authority

CA

负责产生、签发和管理证书的、受用户信任的权威机构。用户可以选择该机构为其创建特定密钥。

2.2.2.224

证书认证机构撤销列表 certificate authority revocation list

是一种撤销列表，由上级 CA 颁发给下级 CA 失效的公钥证书的列表。

2.2.2.225

证书使用系统 certificate using system

由证书用户所使用的、实现应用策略所定义的功能系统。

2.2.2.226

证书序列号 certificate serial number

为每个证书分配的唯一整数值，在 CA 颁发的证书范围内，该值与 CA 所颁发的证书一一对应。

2.2.2.227

证书用户 certificate user

具有并使用数字证书的实体。

2.2.2.228

直接可信认证机构密钥 directly trusted CA key

用于验证证书的直接可信认证机构的公钥，该公钥在被获取后以一种安全的、可信的形式存储在某一端实体中，并且无需借助其他认证机构创建的证书来验证其自身。

例如：如果几个组织的认证机构相互交叉认证，那么实体的直接可信认证机构可能就是实体组织的认证机构。每个实体的各直接可信认证机构及其密钥可以不尽相同。一个实体可以将几个认证机构视为直接可信认证机构。

2.2.2.229

终端实体 end entity

不以签署证书为目的而使用其私钥的一种证书主体。

2.2.2.230

终端实体公钥证书撤销列表 end-entity public-key certificate revocation list

EPCRL

一类撤销列表，它包含一系列已向持有者(不包括 CA)发布的，但对证书发布者来说已不再有效的公钥证书。

2.2.2.231

终端实体属性证书撤销列表 end-entity attribute certificate revocation list

EACRL

一类撤销列表，它包含一系列已向持有者(不包括 AA)发布的，但对证书发布者来说已不再有效的属性证书。

2.2.2.232

种子 seed

一种用作某一确定性随机比特生成器输入的比特串。DRBG 的部分状态由种子确定。

2.2.2.233

种子密钥 seed key

用于初始化加密函数或操作的秘密值。

2.2.2.234

种子生存期 seedlife

从以某一种子初始化确定性随机比特生成器开始，到以另一种子重新完全初始化该确定性随机比特生成器之间的时间周期。

2.2.2.235

属性管理机构 attribute authority

AA

受一个或者多个实体的信托，创建并签署属性证书的实体。

注：CA 也可以是一个 AA。

2.2.2.236

属性管理机构撤销列表 attribute authority revocation list

一个撤销列表，它包含有一系列已发布给 AAs 的属性证书的索引，对于认证机构来说这些证书不再有效。

2.2.2.237

属性证书 attribute certificate

属性管理机构进行数字签名的一种数据结构，该结构将持有者的身份信息与一些属性值加以绑定。

2.2.2.238

属性证书撤销列表 attribute certificate revocation list

由发布机构发布的、不再有效的属性证书的索引表。

2.2.2.239

字典式攻击 dictionary attack

用遍历给定口令或密钥列表的方式对密码系统的攻击。如，使用存储的特定口令值或密钥值列表，或使用来自自然语言字典中的单词列表。

2.2.2.240

自同步流密码 self-synchronous stream cipher

具有如下性质的流密码：其后续生成的密钥流符号，是一个秘密密钥和先前固定数目密文比特的函数输出。

2.2.3 **备份与恢复**

2.2.3.1

备份文件 backup files

一种用于以后数据恢复的文件。

2.2.3.2

后向恢复 backward recovery

使用后期版本数据和记录在日志中的数据，通过重组恢复早期版本的数据。

2.2.3.3

拷贝保护/复制保护 copy protection

使用特殊技术检测或防止未授权地复制数据、软件或固件。

2.2.3.4

应急预案 contingency plan

一种关于备份、应急响应和灾后恢复的计划。

2.2.3.5

灾难恢复计划 disaster recovery plan

信息系统灾难恢复过程中所需要的任务、行动、数据和资源的文件，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支持的关键业务功能。

2.2.4 **实体技术**

2.2.4.1

安全主机 security host

可由内部网和外部网访问的，通常构成网络接入主节点的计算机。它在信息系统中通常应予以充分保护。

2.2.4.2

定时炸弹 time bomb

在预定时间被激活的逻辑炸弹。

2.2.4.3

基线 baseline

经过一个正式评审并通过的规约或产品，作为后续开发的基础。对其变更只有通过正式的变更控制规程方可进行。

2.2.4.4

集线器 hub

一种工作于开放系统互连参考模型中的第一层的网络设备。网络集线器中并没有真正的智能，仅为被联网系统或资源提供物理接点。

2.2.4.5

交换机 switch

在联网的设备之间，一种借助内部交换机制来提供连通性的设备。交换机不同于其他局域网互联设备(例如集线器)，原因是交换机中使用的技术是以点对点为基础建立连接。这确保了网络通信量只对有地址的网络设备可见，并使几个连接能够并存。交换技术可在开放系统互连参考模型的第二层或第三层实现。

2.2.4.6

可信第三方 trusted third party

在同安全相关的活动方面，被其他实体信任的安全机构或其代理。

2.2.4.7

敏感信息 sensitive information

由权威机构确定的必须受保护的信息，该信息的泄露、修改、破坏或丢失会对人或事产生可预知的损害。

2.2.4.8

热噪声 thermal noise

在元器件(例如运算放大器、反向偏压二极管或电阻器)中，通常情况下不希望出现的，但却内在产生的杂散电子信号(又称“白噪声”)。

注：通常都会尽力将这一现象最小化，然而由于此现象的不可预测性，在随机比特流生成中，可将其作为一种熵源加以利用。

2.2.4.9

数据路径 data path

数据流经的物理或逻辑路径。一般情况下，一条物理数据路径可由多条逻辑数据路径所共享。

2.2.4.10

虚拟电路 virtual circuit

一种建立在网络设备之间，采用数据包交换或信元交换技术(X.25、异步传输模式、帧中继等)的数据通路。

2.2.4.11

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。

2.2.4.12

子网 subnet

在某一网络中，共享某一公共地址成分的部分。

2.3 **管理类**

2.3.1

IT 安全策略 IT security policy

在某一组织特别是其信息技术系统中，管理、保护和分发信息技术资产的各种规则、指令和惯例。

2.3.2

安全策略 security policy

用于治理组织及其系统内在安全上如何管理、保护和分发资产(包括敏感信息)的一组规则、指导和实践,特别是那些对系统安全及相关元素具有影响的资产。

2.3.3

安全服务 security service

由某一可交付件、组织或个人完成的安全过程或任务。

2.3.4

安全机构 security authority

一种负责界定或强制执行安全策略的实体。

2.3.5

安全目标 security target

ST

一组安全要求与规范,用作评价某一确定的IT产品或系统是否安全的基准。

注:对一个确定的评价对象,其安全目标是关于安全需求的、与实现有关的陈述。

2.3.6

安全目的 security objective

旨在对抗已知的威胁、满足组织安全策略和假设的陈述。

2.3.7

安全评估 security assessment

依照安全标准以及相应的方法,验证某一安全可交付件与标准的符合程度及其安全保障程度。

注:安全评估通常是产品评价过程的最后阶段。

2.3.8

(通用准则中的)包 package

为了满足一组确定的安全目的而集合在一起的、可重用的一组功能组件或保证组件,例如:EAL。

2.3.9

保护轮廓 protection profile

PP

针对一类满足特定用户需要的IT产品或系统,而给出的一组与实现无关的安全需求。

2.3.10

保障 assurance

为使他人获得可交付件满足其安全目标的信心,而履行的适当行为和过程。

2.3.11

保障方法 assurance method

为获得可重复保障结果,而被认可的、描述如何进行保障的规范。

2.3.12

保障分类 assurance typing

为指明各种保障方法在某些确定方面的相似性而对其进行的分组。

2.3.13

保障管理员 assurance administrator

选择、执行或接受可交付件的负责人。

2.3.14

保障机构 assurance authority

为使可交付件的使用建立信心、有权对相关可交付件的保障做出决定(即选择、规范、接受、执行)的

个人和组织。

注：在特定的模式或组织中，保障机构这一术语可能是不同的，例如：有时称作“评价机构”。

2.3.15

保障级 assurance level

通过所用保障方法按照特定尺度获得的不同保障。

注1：保障级别可能无法以量化指标测量。

注2：所得的保障一般与该活动所付出的努力有关。

2.3.16

保障阶段 assurance stage

可交付件的一个生存周期阶段，在该阶段中突出一个给定的保障方法。可交付件的保障应考虑贯穿于可交付件生存周期应用的所有保障方法所产生的结果。

2.3.17

保障结果 assurance result

对可交付件给出的定量或定性的文档化的保障陈述。

2.3.18

保障论据 assurance argument

一组由证据和推理支持的、有结构的保障声明，可清楚地表明是如何满足保障要求的。

2.3.19

保障评估 assurance assessment

验证和记录与可交付件（作为保障论据的一部分）相关的保障类型和数量。

2.3.20

保障声明 assurance claim

系统满足安全要求的断言或其相关表述。该声明既针对直接威胁（例如，防止系统数据遭受外部攻击）也针对间接威胁（例如，使系统代码漏洞尽可能小）。

2.3.21

保障事项 assurance concern

对用户保障指南进行分析并给出结论，通用于一组重要保障机构的保障目标的元素。

2.3.22

保障特性 assurance property

保障方法中可支持得到保障结果的特征。

2.3.23

保障途径 assurance approach

根据所检验的内容而建立的一组保障方法。

2.3.24

保障证据 assurance evidence

在对可交付件进行保障分析中所产生的、支持保障声明的工作产品。

2.3.25

被授权用户 authorized user

依据评价对象的安全策略可执行某一操作的用户。

2.3.26

残留风险 residual risk

在实现防护措施之后仍然存在的风险。

2.3.27

策略 policy

由管理层正式表述的总体意图和指向。

2.3.28

产品/系统保障途径 product/system approach to assurance

通过检查并给出结果以获得保障的一种保障方法。

2.3.29

产品评估 product assessment

应用特定的文档化评估准则，对特定软件模块、软件包或产品进行的动作，以确定其是否可以接受或发布。

2.3.30

脆弱性 vulnerability

资产中能被威胁所利用的弱点。

2.3.31

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。

2.3.32

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。

2.3.33

度量 metric

为了完成对一个或几个属性的测量，所定义的测量形式（测量方法、计算函数或分析模型）和尺度。

2.3.34

防护 safeguard

处置风险的惯例、规程或机制。

2.3.35

风险 risk

一个给定的威胁，利用一项资产或多项资产的脆弱性，对组织造成损害的潜能。可通过事件的概率及其后果进行度量。

2.3.36

风险标识 risk identification

查明、列出风险的各个因素并描述其特征的过程。

2.3.37

风险处置 risk treatment

选择和实现控制措施以缓解风险的过程。

2.3.38

风险分析 risk analysis

系统地使用信息，辨识风险源并估算风险。

2.3.39

风险管理 risk management

识别、控制、消除或最小化可能影响系统资源的不确定因素的过程。

注：典型的风险管理包括风险评估、风险应对、风险容忍及风险交流（在决策者和承担者之间交换和分享风险信息）。

2.3.40

风险规避 risk avoidance

不卷入某一风险事态的决策，或者从风险事态撤出的行动。

2.3.41

风险缓解 risk mitigation

对一个特定事件的负面后果所施加的限制。

2.3.42

风险降低 risk reduction

为减少与风险关联的事件概率和(或)负面后果而采取的行动。

2.3.43

风险接受 risk acceptance

一种管理性的决定，该决定通常根据技术或成本因素，接受某种程度的风险。

2.3.44

风险评估 risk assessment

风险标识、分析和评价的整个过程。

2.3.45

风险评价 risk evaluation

为确定风险严重性程度，将估算的风险与给定的风险判据进行比较的过程。

2.3.46

风险转移 risk transfer

对某一风险，与另一方分担风险或分享利益的做法。

注1：法律、法规的要求可以限制、禁止或强制确定风险的转移；

注2：风险转移可能产生新的风险或改变现存的风险。

2.3.47

工作产品 work product

在完成开发和供应可交付件的过程中产生的所有项，如文档、报告、文件、数据等。

2.3.48

观察报告 observation report

在评估期间，一种由评估方撰写的、要求澄清或辨识某一问题的报告。

2.3.49

管理 management

指导或控制一个组织的协调活动。

2.3.50

管理机构证书 *authority certificate*

对管理机构(例如属性管理机构)发布的证书。

2.3.51

管理控制 management controls

针对关注风险管理和信息系统安全管理的信息系统而施用的安全控制(即防护措施和对抗措施)。

2.3.52

过程保障 process assurance

通过对过程活动的评估而获得的保障。

注：过程是指将输入变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。

2.3.53

基线控制 baseline controls

为一个系统或组织建立的防护措施的最小集合。

2.3.54

TSF 间传送 inter-TSF transfer

在 TOE 与其他可信 IT 产品的安全功能之间交换数据。

2.3.55

间接度量 indirect metric

对某一属性的度量是由其他属性的一个或更多个度量导出。其中通过一个计算函数(公式或方程)来计算,并且利用了其他直接或间接度量所获得的值。

2.3.56

监督定论 oversight verdict

根据评价监督活动的结果,由监督方就确认或拒绝总体定论所发布的陈述。

2.3.57

监视方 monitor/monitoring authority

对动作和事件进行监视,并受托就已经进行的监视提供证据的可信第三方。

2.3.58

交付机构 delivery authority

被发送方信任的机构,该机构可以把数据从发送方交付给接收方,并且向发送方提供按要求提交和传输数据的证据。

2.3.59

可交付件 deliverable

信息技术(IT)安全产品、系统、服务、过程、环境因素(例如:人员素质、组织资质)或保障评价对象。

2.3.60

控制 control

管理风险的一种手段(包括策略、规程、指南、惯例或组织结构等)。这些手段可以是行政的、技术的、管理的或法律性质的。

2.3.61

TSF 控制范围 TSF scope of control

服从 TSP 规则的,可与 TOE 交互或在 TOE 中发生的交互的集合。

2.3.62

利益相关方 stakeholder

在某一工作、项目等特定活动中,可能影响他人、被他人所影响或意识到自己要被其他组织的行为所影响的任何个人、团体或组织。

2.3.63

连通性 connectivity

允许一个产品和/或系统与其之外的 IT 实体进行交互的特性,包括在任何环境和配置下通过任意距离的有线或无线方式的数据交换。

2.3.64

TOE 内部传送 internal TOE transfer

在 TOE 各分离部分之间交换数据。

2.3.65

内部通信信道 internal communication channel

评价对象中各分离部分间的通信信道。

2.3.66

评估 assessment

系统化的检验一个实体满足所规约的需求的程度。当用于可交付件时，与评价是同义的。

2.3.67

评估体制 evaluation scheme

一种行政管理和监督管理框架，在此框架下评估管理机构在特定团体中实施指定标准。

2.3.68

评价保障级 evaluation assurance level

保障组件构成的包，该包代表了通用准则预先定义的保证尺度上的某个位置。

2.3.69

评价对象 target of evaluation

TOE

被评价的信息技术产品或系统及其相关的指南文档。

2.3.70

评价对象安全策略 TOE security policy

TSP

为评价对象中有关资产的管理、保护和分配而指定的一组规则。

2.3.71

评价对象安全策略模型 TOE security policy model

评价对象执行的安全策略的结构化表示。

2.3.72

评价对象安全功能 TOE security function

TSF

正确实施安全功能需求所必须依赖的全部 TOE 硬件、软件和固件等构成的集合。

2.3.73

评价对象安全功能接口 TOE security function interface

一组人机交互或应用编程接口，通过它可访问 TSF、调配 TOE 资源，或者从 TSF 中获取信息。

2.3.74

评价对象资源 TOE resource

评价对象中可使用的或可消耗的任何事物。

2.3.75

评价方案 evaluation scheme

针对一个特定的团体，由某一评价机构根据指定标准制定的行政管理的与规章制度的框架。

2.3.76

评价机构 evaluation authority

一个实体，该实体按照一个评估体制，为一个特定团体实施评估，在评估实践中为该团体建立相应的评估标准并监控该团队所进行的评估质量。

2.3.77

评价技术报告 evaluation technical report

由评估者产生的并提交给评估机构的报告，其中以文档形式给出了整个定论及其理由。

2.3.78

评价可交付件 evaluation deliverable

为进行一项或多项评估或评估监督活动，而由评估方或监督方向评估发起方和开发方索要的任一资源。

2.3.79

评价证据 evaluation evidence

一种有形的评估可交付件。

2.3.80

确认 validation

通过检查并提供客观证据，证实明确提出的预期使用的特定需求得以满足。

2.3.81

认可 accredit

同意一个实体或个人去执行特定活动。

2.3.82

认可 accreditation

权力机构为了对以下三个方面给出正式的认同、批准并且接受它们残余风险所采取的规程：

a) 有关自动化系统的运行，其中该系统运行在特定的安全模式下，使用一套特定的防护措施；

b) 有关承担特定任务的安全机构或个人；

c) 有关针对目标环境的安全服务。

2.3.83

认可机构 accreditation authority

一种受信任的实体，该实体生成私有认可信息。

2.3.84

认证 certification

对可交付件是否符合规定需求所给出的正式保证陈述的规程。可由第三方执行认证或自行认证。

2.3.85

申请方 applicant

请求分配注册项及其标号的实体(组织、个人等)。

2.3.86

审批机构 approval authority

受委托进行安全功能审批和/或评价的国内组织或国际组织。

2.3.87

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的方式，检查数据处理系统的安全功能，以发现信息系统安全问题的手段。也称渗透性测试或逆向测试。

2.3.88

适用性声明 statement of applicability

描述适用于所指组织的信息安全管理体系和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：风险评估和风险处理过程的结果和结论、法律或规章的要求、合同义务及该组织对于信息安全的业务需求。

2.3.89

TSF 数据 TSF data

TOE 产生的或为 TOE 产生的数据，这些数据可影响 TOE 的操作。

2.3.90

外部 IT 实体　external IT entity

在评价对象之外与其交互的任何可信或不可信的 IT 产品或系统。

2.3.91

外部运行系统　external operational system

与评估所涉及的运行系统相分离，但有接口的运行系统。

2.3.92

网络安全策略　network security policy

由陈述、规则和惯例等组成的集合，说明使用其网络资源的组织途径，并指明如何保护网络基础设施和服务。

2.3.93

网络管理　network management

对网络进行规划、设计、实现、运行、监视和维护的过程。

2.3.94

威胁　threat

对资产或组织可能导致负面结果的一个事件的潜在源。

2.3.95

威胁方　threat agent

故意或意外的人为威胁的原发方和/或发起方。

2.3.96

威胁分析　threat analysis

对信息处理系统的威胁源所做的查考及其可能引起负面结果的推断。

2.3.97

维护　maintenance

交付后为了纠正缺陷、改进性能以及其他属性或适应环境变化而对系统或组件进行修改的过程。

2.3.98

响应(不测事件响应或入侵响应)　response (incident response or intrusion response)

当攻击或入侵发生时，为了保护和恢复信息系统正常运行的条件以及存储在其中的信息而采取的行动。

2.3.99

项标记　entry label

唯一地标识所注册保护轮廓或包的命名信息。

2.3.100

信息安全管理过程　information security management process

信息安全管理过程是一个系统化的过程，用于持续标识和管理危害环境的风险，其中环境危害与信息处理中的信息、过程和系统有关。

2.3.101

信息安全管理体系　information security management system

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，是一个组织整个管理体系的一部分。

注：该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。

2.3.102

信息安全事件响应组 information security incident response team

由组织中具备适当技能且可信的成员组成的一个小组，负责处理与信息安全事件相关的全部工作。有时，小组可能会有外部专家加入，例如来自一个公认的计算机事件响应组或计算机应急响应组(CERT)的专家。

2.3.103

验证 verification

将某一活动或处理过程的输出与其相对应的安全需求或规范相比较，并证实该输出满足需求或规范的过程。例如：在安全操作系统的开发中，将某一安全策略的实现与相应的规范相比较。

2.3.104

信息通信技术安全策略 ICT security policy

在某一组织及其信息通信技术系统中，关于资产(包括敏感信息)管理、保护和分配的导则、规则和惯例。

2.3.105

影响 impact

事件的后果。在信息安全中，一般指不测事件的后果。

2.3.106

(表达安全要求的)元素 element

一个不可再分的安全要求。

2.3.107

证据 evidence

用来证明一个事件或动作的信息，可单独使用或与其他信息一起使用。

2.3.108

证据主体 evidence subject

对某个行为负责或与某个事件相关的实体，该实体产生与行为或事件有关的证据。

2.3.109

职责分割 separation of duties

关于敏感信息的分权制衡，使单独行动的个人只能危及信息系统有限部分的安全。

2.3.110

指南文档 guidance documentation

对所评价对象，当用户、管理员或集成方从事交付、安装、配置、操作、管理和使用等活动时，用于指导这些活动的各种文件。对指南文档的范围和内容的要求，在保护轮廓或安全目标中规定。

2.3.111

质量评价 quality evaluation

对实体满足规定要求程度而进行的系统性检查。

2.3.112

注册簿项 register entry

在注册簿内，与特定保护轮廓或包有关的信息。

2.3.113

资产 asset

对组织具有价值的任何东西。

2.3.114

总体定论　overall verdict

由评价方就评估结果发布的通过或不通过的陈述。

2.3.115

族　family

一组具有共同安全目的，但侧重点或严格程度存在不同的组件的集合。

2.3.116

组件　component

可包含在某一保护轮廓、安全目标或包中最小可选元素的集合。

2.3.117

组织安全策略　organizational security policies

组织为保障其运行而规定的若干安全规则、规程、实践和指南。

索　引

汉语拼音索引

D

F

G

H

J

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

Q

R

S

T

U

V

W

Z