

国 际 电 信 联 盟

ITU-T

国际电信联盟
电信标准化部门

X.1207

(04/2008)

X系列：数据网、开放系统通信和安全性
电信安全

**电信业务提供商应对间谍软件及
潜在有害软件风险的指导原则**

ITU-T X.1207建议书



国际电信联盟

ITU-T X系列建议书
数据网、开放系统通信和安全性

公众数据网	
业务和设施	X.1-X.19
接口	X.20-X.49
传输、信令和交换	X.50-X.89
网络概貌	X.90-X.149
维护	X.150-X.179
管理安排	X.180-X.199
开放系统互连	
模型和记法	X.200-X.209
服务限定	X.210-X.219
连接式协议规范	X.220-X.229
无连接式协议规范	X.230-X.239
PICS书写形式	X.240-X.259
协议标识	X.260-X.269
安全协议	X.270-X.279
层管理对象	X.280-X.289
一致性测试	X.290-X.299
网间互通	
概述	X.300-X.349
卫星数据传输系统	X.350-X.369
以IP为基础的网络	X.370-X.379
报文处理系统	X.400-X.499
号码簿	X.500-X.599
OSI 组网和系统概貌	
组网	X.600-X.629
效率	X.630-X.639
业务质量	X.640-X.649
命名、寻址和登记	X.650-X.679
抽象句法记法1(ASN.1)	X.680-X.699
OSI 管理	
系统管理协议子集和结构	X.700-X.709
管理通信服务和协议	X.710-X.719
管理信息的结构	X.720-X.729
管理功能	X.730-X.799
安全	X.800-X.849
OSI 应用	
托付、并发和恢复	X.850-X.859
事务处理	X.860-X.879
远程操作	X.880-X.889
ASN.1的一般应用	X.890-X.899
开放分布式处理	X.900-X.999
电信安全	X.1000-

欲了解更详细信息，请查阅 ITU-T 建议书目录。

电信业务提供商应对间谍软件及潜在有害 软件风险的指导原则

摘要

ITU-T X.1207建议书阐述了电信业务提供商（TSP）应对间谍软件及潜在有害软件风险的指导原则，同时旨在推广围绕明确通知、TSP万维网主机托管业务的用户认可与控制原则的最佳做法。本建议书制定并推广包括反间谍软件、防病毒、个人防火墙以及客户端系统安全更新软件在内的、有关个人计算机安全的最佳做法。

来源

ITU-T第17研究组（2005-2008）按照世界电信标准化全会（WTSA）第1号决议规定的程序，于2008年4月18日批准了ITU-T X.1207建议书。

关键词

欺骗性软件、互联网安全性、潜在的有害软件、间谍软件。

前言

国际电信联盟（ITU）是从事电信领域工作的联合国专门机构。ITU-T（国际电信联盟电信标准化部门）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定 ITU-T 各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA 第 1 号决议规定了批准ITU-T建议书须遵循的程序。

属 ITU-T 研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其他一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其他机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联尚未收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此特大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：<http://www.itu.int/ITU-T/ipr/>。

© 国际电联 2008

版权所有。未经国际电联事先书面许可，不得以任何手段复制本出版物的任何部分。

目录

页码

1	范围	1
2	参考文献	1
3	定义	1
4	缩写词和首字母缩略语	1
5	排印惯例	2
6	概述	2
7	目标	3
8	欺骗性软件和间谍软件	3
9	欺骗性软件和间谍软件为何是严重的问题	3
10	建议	4
11	电信业务提供商（TSP）指南	4
11.1	企业中的信息安全风险管理	4
11.2	网络托管业务的安全和保障要求	6
11.3	最终用户的安全和保障指南	7
附录 I – 补充资源		9
I.1	网上安全和反间谍软件方面的参考信息	9
I.2	事件上报联络人清单范例	10
参考资料		11

电信业务提供商应对间谍软件及潜在有害软件风险的指导原则

1 范围

本建议书是ITU-T为改善网络安全状况制定的一系列指导原则的组成部分，涵盖了电信业务提供商（TSP）和最终用户基本安全保障最佳做法要求，重点涉及间谍软件和其它潜在有害软件（可能是恶意和/或欺骗性软件）方面的问题。本建议书所述电信业务提供商（TSP）系指提供互联网相关业务的TSP，特别是为商业组织提供网络托管服务和为最终用户提供互联网接入的TSP。

2 参考文献

无。

3 定义

间谍软件这一术语的使用很宽泛，目的是将众多用户不请自来的、具有某些侵犯隐私性质行为的软件纳入其定义之内。因此，为确保术语的一致性和理解的统一，本建议书提供了间谍软件和相关欺骗性软件的工作定义。

3.1 欺骗性软件：在用户计算机上进行操作，但却未 1) 事先通知用户该软件将在用户的计算机上进行哪些操作；或 2) 请示用户是否同意其进行这些操作。欺骗性软件的示例包括，强行控制用户配置程序，或产生无休止弹出式广告、而用户却不易将其关闭的各类程序。

3.2 潜在的有害软件：潜在的有害软件是指各类欺骗性软件，包括病毒、蠕虫、特洛伊木马等恶意软件和具有欺骗性软件和间谍软件特征的非恶意软件。

3.3 间谍软件：本建议书中定义的间谍软件系指专门收集用户计算机中个人信息的特定类型欺骗性软件。个人信息可能包括最常访问的网站或密码等更为敏感的信息。

4 缩写词和首字母缩略语

本建议书使用如下缩写词和首字母缩略语：

CERT	计算机应急响应组
CIRT	计算机事件响应组
ICT	信息通信技术
ISMS	信息安全管理体系
ISMS-T	信息安全管理体系 – 电信要求
ISV	独立软件供应商

SQL	结构化查询语言
TSP	电信业务提供商
URI	统一资源标识符

5 排印惯例

无。

6 概述

互联网的普及催生出各类新型业务并为家庭用户和办公用户带来了诸多益处。互联网与生俱来的开放性和互连性及其提供的接入速度，使其成为企业和消费者进行通信的有效平台，并可用于大规模的商业性营销活动。近年来，网络罪犯和一些诈骗公司越来越多地利用互联网的开放性及其在通信与连接方面的便利性，通过使用各类恶意软件获取经济上的好处或用于其它犯罪目的。

目前，安全保障方面越来越严峻的挑战来自间谍软件和欺骗性软件，这些软件会危及个人信息的安全，造成生产力大幅下降并会打击最终用户对网上合法企业的信心和信任。

各相关方，特别是监管机构和企业用户通常依赖电信业务提供商（TSP），为最终用户（包括普通消费者和企业用户）提供安全而有保障的互联网服务。如果在TSP网络托管的网站中发现存在恶意内容，包括间谍软件或欺骗性软件，且这些内容影响到最终用户计算机系统的安全，人们会期望TSP协助处理这些问题，而这些事件久拖不决或频繁出现都会影响人们对该TSP在提供安全且有保障的服务方面的信任和信心，令客户不满并转而使用其它TSP的服务。

从监管的角度来看，许多国家的监管机构要求TSP在安全与保障措施方面提供更多的承诺，并要求TSP在为消费者和最终用户安全使用互联网提供帮助方面做出更多努力。

为应对互联网安全保障方面发生的变化，对TSP而言，至关重要的是采取一套业界公认的最佳做法标准，对最低基本要求¹做出规定，确保通过TSP托管的互联网服务的安全性，并在使用该网络的最终用户中推广相关做法。基本标准的实施还将使TSP有机会向监管机构和最终用户展示其遵守业界最佳做法的行为，维护或增强监管机构和最终用户对该TSP网络及其服务安全性的信心与信任。

¹ 目前还不存在此类基本要求，因此本导则建议书便是向提供此类最低限度基本要求迈出的第一步。

7 目标

本建议书的目标是：

- 1) 推广围绕明确通知、托管业务用户认可和用户控制原则的最佳做法；
- 2) 向家庭用户宣传使用个人计算机和互联网方面的最佳安全做法（通过电信业务提供商），其内容包括防病毒软件、反间谍软件、个人防火墙的使用以及自动安全更新。

8 欺骗性软件和间谍软件

各类欺骗性软件程序（包括间谍软件）有别于合法应用的共同特点是，用户并未发出通知亦并未做出选择。重要的一点是，人们均注意到，通过适当的披露、用户授权和控制，欺骗性软件/间谍软件完成的任务可为用户带来多种益处。例如，这些程序能够促进个性化设置，经用户批准后改变配置并播放经用户许可的广告，从而为电子邮件等高成本服务提供补贴。简而言之，欺骗性软件主要不是技术性问题，而是因欺骗或欺诈行为产生的问题。

无论在世界还是本地层面，欺骗性软件和间谍软件都已成为政府、行业和消费者最为关注的问题，因其范围已超越了“ICT政策”的范畴。尽管欺骗性软件利用互联网和计算机作为媒介，但其本质还是一种源于欺诈行为的消费者保护问题。

9 欺骗性软件和间谍软件为何是严重的问题

在消费者这一层面，此类软件会影响用户对计算机和/或上网的感受（有时甚至认为计算机无法使用）并使用户有一种挫败感和丧失“控制”的感觉。可以毫不夸张地说，特别是在消费者层面，对大部分用户而言欺骗性软件造成的威胁可能会彻底抹煞互联网和计算机本身带来的巨大益处。

欺骗性软件不仅会对消费者产生显而易见的巨大影响，同时亦是众多ICT公司面临的一个主要问题。在某种程度上，许多客户误将其计算机操作问题归咎于软件制造商和开发商，在对这些厂家的声誉造成损害的同时使客户对这些产品产生了不良印象。显而易见的是，因欺骗性软件而引发的问题，使人们在针对软硬件的求助电话方面浪费了数以百万计美元的资金。

如上文第6段所述，TSP无法逃避间谍软件和欺骗性软件提出的挑战，因为诈骗公司和网络罪犯可能直接在其托管的网站使用此类软件，并且其用户会直接感受到这些负面影响，从而要求TSP为其提供帮助和支持。除此以外，各监管机构和最终用户都认为应由TSP为解决此类问题提供充分的安全保障措施。如果TSP拒绝履行应对此类挑战的职责，则其声誉以及最终用户对其的信心与信任必将遭受打击。

10 建议

遏制间谍软件最有效的方式可能是综合使用一系列调动各利益攸关方的战略：

- 业界的最佳做法，即与所有重要相关方合作，确定间谍软件和其它有害软件并对其进行打击；
- 普及用户教育，为用户了解如何才能删除并避开间谍软件和其它有害软件提供一种可靠的资源；
- 创新的技术解决方案，保护用户免受间谍软件和其它潜在有害软件的危害，并为防止成为此类软件的受害者不断进行更新；
- 政府的立法与执法，即在业界的帮助下遏制欺骗性软件和间谍软件的滋生。

本导则侧重于在为业界提供最佳做法的同时加强对消费者的教育，以协助TSP在应对欺骗性软件和间谍软件所带来的挑战方面，发挥积极的作用。

11 电信业务提供商（TSP）指南

为处理欺骗性软件和间谍软件问题，本导则将重点集中在三个主要领域，即TSP机构自身的内部安全管理；TSP应要求其网络托管客户实施的安全要求；使用互联网接入业务的最终用户（或签约用户）安全指南。这些建议由三个相关分节构成，其内容如下：

- a) 企业中的信息安全风险管理
- b) 网络托管业务的安全和保障要求
- c) 最终用户的安全和保障指南

11.1 企业中的信息安全风险管理

11.1.1 信息安全管理系统

在企业这一层面应采用正式的信息安全管理系统，以确定并管理与TSP业务相关的信息安全风险。[b-ITU-T X.1051建议书]提供了实施此类系统所需的指南和最佳做法。

TSP实施ISMS-T的一项重要考虑是，确保TSP作为企业组织能够拥有一个系统，该系统能够不断确定、评估、处理和管理与其直接向最终用户/签约用户、通过网络托管业务间接向客户提供网上业务相关的信息安全风险。

TSP将能够通过ISMS-T连续的风险管理流程，了解其风险特征并可向监管机构及其它相关方展示其网络和服务的安全性。

TSP亦可考虑根据ISO/IEC 27001认证机制，对其是否符合ISMS-T建议书进行正式认证。

作为实施ISMS-T或相关信息安全管理系统的一部分，TSP还应具备事件监测与响应的能力，并与该国的外部计算机事件响应组（CIRT）或计算机应急响应组（CERT）就事件响应活动开展协调。事件和应急响应机制应包括对TSP网络中最终用户和托管网站安全状况的监测与评估，并帮助受影响的各方有效响应安全事件。

11.1.2 提供安全保障产品

有些TSP可能会制定²或发布其自有的网络浏览器工具条，拨号盘或某种代码，用于为最终用户提供增值服务或为其使用互联网服务提供便利。在这种情况下，应当提供一种适当的最终用户协议，其中包括TSP编码政策、隐私政策的适用语言和表述，并为用户将来改变接受条件或提出政策和做法方面的问题提供手段。使用此类协议时，TSP应确保最终用户签署此类协议且其版本前后一致。

TSP应记录代码的行为并对其行为是否可被看作是间谍软件或欺骗性软件进行评估。对于后一种情况，TSP应使用适当的合格评估软件评估该代码是否符合反间谍软件厂商制定的客观标准，是否遵循最佳做法，从而TSP为最终用户提供的软件工具不被反间谍软件厂商当作间谍软件/广告软件。许多反间谍软件厂商根据其发布的标准对软件³进行评级。

TSP应对其二进制代码使用数字代码签名，这样反间谍软件厂商便能够轻松地确定某份文件的所有者，甚至在进行分析之前，便有可能将一贯遵照最佳做法编写软件的独立软件供应商（ISV）归入安全厂商范围之列。

如果TSP发现了某些有助于减少间谍软件问题的软件技术，则TSP应考虑与该供应商建立伙伴关系，并共同推广这些技术的使用。

11.1.3 网络检测和响应

TSP普遍采用网络监测的方式来确保网络业务的可靠性和质量。与此同时，可使用这一功能来查询异常的网络流量状况，检测网络中出现的恶意行为。总而言之，TSP应进行如下工作：

- 了解网络中流量的状况 – 何为正常状态，何为异常状态。
- 使用网络管理工具确定流量中的高峰、“异常”流量/端口，并确保具备能够排查原因并对其做出响应的工具。
- 在将响应机制用于实际事件之前对其进行测试。根据定期演练的结果，对响应技术、流程及工具进行调整。
- 分别了解各个组成部分 – 如果通常处于不活跃状态的用户突然占用了100%的可用带宽，则应将其隔离直至找到出现这一情况的原因。网络隔离能够阻止恶意软件（malware）的传播，尽管有些实施程序可能需要用户的认可或对服务条款进行更新。

11.1.4 支持和问题的上报

TSP通常设有支持服务，回答客户提出的问题，并提供技术帮助和支持来处理最终用户的问题。通过上报网上恶意软件，TSP将收到有关恶意软件和间谍软件产生的感染与问题方面的报告。此类信息十分重要，可供相关厂商对恶意软件的情况进行风险评估，并更新各类必要的工具，以确保能够有效地删除或隔离所有新检测到的恶意软件或间谍软件。为此，TSP应与安全软件厂商建立联系，并向这些厂商提交相关报告和恶意软件样本 – 特别是在这

² 内部制定或通过第三方提供商制定。

³ 作为业内多家厂商代表的反间谍软件联盟亦在其网站公布了一系列定义和标准。欲了解更多详细信息，请参见附录I。

些恶意软件盛行之时，供其跟进。多数厂商均建有接收此类报告/样本的电子邮件清单），以便于分析和跟进，有关具体示例见表I.1。

11.1.5 与最新发展情况保持同步

作为为管理企业信息安全风险而实施的ISMS-T的组成部分，并确保TSP能够一直采用业界的最佳做法，同时研究最新出现的漏洞和恶意使用/病毒攻击的情况，TSP应参加相关的团体或产业论坛，与伙伴提供商分享最佳做法并向他们学习。

注 – 欲了解更多信息，请参见附录I。

11.2 网络托管业务的安全和保障要求

大部分TSP提供的服务中均包括其网络和数据中心的网络托管业务。经网络托管用户再次打包后这些业务将被提供给最终用户/消费者和/或小型企业，并转售给最终用户。如果网络托管用户设置了一台不安全的服务器，或在其网站中托管恶意内容，则最终客户的安全和保障将受到不利影响。因此，TSP非常有必要为网络托管用户规定安全保障最佳做法方面的最低标准，作为协议条款的组成部分。

协议条款中应包括下述内容：

- a) 明确的通知，用于描述网站安全和隐私方面的习惯做法、数据采集方面的习惯做法以及该网站可能会在最终用户电脑桌面或网络浏览器环境中传播并执行的所有代码（例如浏览器帮助对象）的行为。
- b) 用户的认可，方便用户对通知中所述的业务条款表达同意或不同意的意愿，使用户可以作出判断，并决定是否接受业务条款。
- c) 用户控制，方便用户改变设置或在将来的某一时刻不再接受最初的协议。

这些条款的重要性在于能够确保最终用户清楚地了解该网站在最终用户的安全、隐私和保障方面所做的工作和采取的做法。这些条款的制定应在法律专业人士的协助下进行，以确保TSP在因该网站出现恶意内容或因政策与做法模糊不清而造成了损失或伤害的情况下，免受最终用户可能提出的法律诉讼。

除网站的数据保护、个人隐私和安全规定之外，TSP应要求其网络内托管的网站在开始工作之前，于应用层面实施一套安全措施方面的最佳做法，其中包括但不仅限于下述内容：

- a) 安全网站开发和网页编码做法指南，其内容包括：
 - i) 显示简短的隐私问题通知，用一页篇幅明晰、简要概述（表达通信）该公司在联机隐私方面的基本做法。这样，用户在提供联机信息时便可做到做出知情选择。此类简短的通知应符合所有规则要求，并提供与完整的法律声明及其它相关信息的链接，使希望了解更多详细内容的客户通过点击便可轻而易举地阅读到更完整的内容。使用单一的通知，将相同的隐私标准和期望值扩展到多个站点，可使客户对该公司的各项特性产生更为一致的感受。
 - ii) 安全处理cookies；

- iii) 为防止SQL injection等常见攻击而进行的安全输入验证和处理。由于点击率高的网站越来越多地被用来传播恶意代码，活动内容及动态内容均应实施输入和输出验证。
- iv) 为防止cross-site scripting（跨站脚本攻击）等常见攻击而编写的安全网页脚本；
- v) 代码安全性审查与测试。

作为TSP网络托管基础设施的一部分，应采取下述安全措施，保护网络服务器免受未经授权的使用或被迫托管欺骗性软件和间谍软件等恶意内容：

- b) 根据基本安全性配置指南，配置包括底层操作系统在内的网络服务器。这一工作应包括对网络服务器用户和管理员的恰当定义，对程序、系统目录和文件实施接入控制，并支持审核跟踪功能，特别是针对系统中出现的安全和其它故障事件。此外，还建议在服务器安装一个最小系统，以减少攻击向量。
- c) 采用一种系统测试和部署安全性更新，并确保网络服务器操作系统和应用在新的安全更新推出后立即得到更新；
- d) 通过定期审查审核跟踪的结果监测网络服务器的性能；
- e) 在服务器上同时运行防病毒和反间谍软件；
- f) 使用最新定义定期扫描所有托管和上载的内容。由于信息不完整的限制，可能会造成：根据当前的定义未检测出某份文件是间谍软件或恶意软件，但该文件仍有可能属于此类软件的情况；
- g) 定期对网站进行安全渗透测试，以确保其安全性得到充分保障且未被网络罪犯破坏。

为执行这些安全措施，特别是与网站安全相关的措施，TSP应考虑将这些规定纳入服务协议的条款。

11.3 最终用户的安全和保障指南

11.3.1 用户指南和教育

针对如何安全上网提供指南。TSP 既可直接制定指南，亦可请用户参见提供相关指南的网站。针对最终用户如何能为互联网的安全性做出贡献开展教育工作至关重要。各项指南工作和活动的示例包括：

- a) 定期（例如，每月）发布有关安全问题的新闻函件，就具体安全技术（例如，如何选择好的密码）提出建议；安全趋势方面的最新内容；提供可由TSP网络门户或其它安全内容提供商提供的安全网播、其它按需提供的视频、音频广播和安全信息通知；
- b) 直接播放按需提供的安全教育录像和/或网播，其内容涵盖安全议题的各个方面，目的在于改善用户在安全问题上的习惯做法并提高这方面的意识；
- c) 在TSP寄送到家庭或办公地址的纸质新闻函件中加入安全栏目，突出显示关键的安全事件或内容；并
- d) 与业内其它相关方、厂商以及各国政府合作，每年或定期举办最终用户安全问题研讨会或路演。

11.3.2 最终用户技术安全措施

作为打击欺骗性软件和间谍软件的用户安全教育与指导工作的组成部分，TSP应建议最终用户采用适当的技术安全措施，以保护其系统免受已知的恶意使用和攻击的伤害。最低保护标准应包括：

- a) 使用装有最新安全补丁的最新操作系统；
- b) 使用防病毒和反间谍软件工具。如有可能，TSP应与可信赖的安全软件厂商⁴建立伙伴关系，作为TSP签约内容中的组成部分向他们提供这些工具，这样在签约之时或更新时便可提供这些安全措施；
- c) 启用弹出屏蔽程序（Pop-up Blocker）。公共网络浏览器及浏览器的工具栏现已具备这一功能，该功能将防止恶意网站显示包含间谍软件或/欺骗性软件的窗口（这些软件利用系统或浏览器的弱点或使用“社会工程攻击”诱骗用户下载并将其安装在用户的系统中）。应当对一系列建议使用的弹出屏蔽程序进行比较，并相应推动在鼓励用户使用这些工具的同时，指导用户如何启用这些工具以及如何允许在经用户许可的网站弹出窗口；
- d) 启用个人防火墙。个人防火墙是控制网络服务使用用户系统或用户系统使用网络服务的另一重要工具。一批更新的操作系统已安装了个人防火墙。尽管在默认状态下处于启用状态，但用户或其它应用可将其关闭，从而造成人们不希望出现的网络安全漏洞。TSP应鼓励使用个人防火墙功能和/或推荐使用经TSP评估后被归为可信任软件的第三方个人防火墙产品，同时教育并帮助用户在最终用户系统层面启用基本网络安全措施；
- e) 启用自动更新。尽管上述技术安全措施能够处理在相应操作层面出现的大部分恶意软件，但它们在对付恶意利用现有操作系统和应用产品中存在的漏洞方面并不十分有效。为防止此类恶意使用，应启用操作系统中可用的、以及由用户信赖的应用（例如经可信赖的第三方评估的反间谍软件和防病毒产品）提供的更新功能，以进行自动更新。这一做法将确保系统在最新的安全补丁推出之后立即得到更新，使恶意利用无机可乘。

附录I列出了可为上述建议的实施提供支持的一系列参考和在线资源。

⁴ 可信赖的安全软件厂商可能是TSP的业务伙伴和/或其产品和服务在经评估后可满足TSP安全政策与要求的厂商。

附录I

补充资源

(本附录不构成此建议书不可分割的组成部分)

I.1 网上安全和反间谍软件方面的参考信息

与互联网安全和保障相关的更多信息，可参见并利用一系列网站，其中包括：

- **反间谍软件联盟** (<http://www.antispywarecoalition.org/>) — 为在关于间谍软件和其它潜在的有害技术的争论过程中，就定义和最佳做法达成一致而专门成立的团体。反间谍软件联盟 (ASC) 由反间谍软件公司、学术机构和消费者集团组成，通过集思广益为控制间谍软件和其它潜在的有害技术指明方向。
- **保持清醒的网络意识 (Be Web Aware)** (<http://www.bewebaware.ca>) — 一项关于互联网安全的双语国家公众教育计划，旨在确保加拿大的年轻一代能够从互联网获益，在保证自身安全的同时以负责任的态度从事网上活动。
- **互联网安全使用与责任中心** (<http://csriu.org>) — 为安全、负责地使用互联网提供延伸服务的组织。
- **国际儿童网** (<http://www.childnet-int.org>) — 一个非营利性组织，该组织与世界上其它相关组织合作，力求将互联网办成儿童向往的安全乐园。
- **国际禁止拐卖儿童和强迫儿童卖淫组织 (ECPAT)** (<http://www.ecpat.net>) — 多个组织和个人合作消除商业性儿童性剥削的网络。
- **明智上网 (GetNetWise)** (<http://www.getnetwise.org>) — 由互联网行业的多家公司和公众利益组织联盟提供的公众服务，这些组织希望用户在选择自己和其家庭使用互联网的方式时，与做出知情决定所需的资源仅有“一击之遥”。
- **互联网安全性全球基础设施联盟 (GIAIS)** (<http://www.microsoft.com/security/msra/default.msp>) — 由服务提供商组成的联盟，其成立的宗旨是提高网络的安全和保障，在较大范围内统一应对各类威胁，同时确定并减少现有漏洞。
- **国际互联网热线协会 (INHOPE)** (<http://inhope.org>) — 为支持以互联网热线的方式对非法内容报告做出响应从而使互联网更为安全而成立的国际协会。
- **互联网安全小组** (www.netsafe.org.nz) — NetSafe网站是新西兰互联网安全小组 (ISG) 和Hector the Protector网上家园。
- **国际失踪与受剥削儿童援助中心** (<http://www.icmec.org>) — 通过积极活动、政策的制定和跨国协调改善儿童安全与福祉的全球性机构。
- **国际刑事警察组织** (<http://www.interpol.int>) — 国际刑警组织旨在促进警察的跨境合作，同时支持并协助以遏制或打击国际犯罪为宗旨的各类组织、当局和服务机构。
- **iSafe** (<http://www.isafe.org>) — 互联网安全教育方面的世界性领导机构；结合课堂教学和动态的社区服务，使学生、教师、家长、执法人员及相关成年人有能力将互联网变得更为安全。

- **微软家庭安全计划** (<http://www.microsoft.com/protect>) –为帮助公众保护计算机、进行自我保护并保护其家人而提供的信息和资源。
- **全国儿童暨母亲咨询委员会** (<http://www.nccm.org.eg>) –埃及从权利的角度专门为支持儿童和母亲而成立的组织。
- **网络家庭新闻** (<http://netfamilynews.org>) –一项非营利性公众服务，为50多个国家的父母和教育人士提供了一个论坛并提供“儿童技术方面的新闻”。
- **NetAlert Limited** (<http://www.netalert.gov.au>) –由澳大利亚政府成立的非营利性社区组织，为管理网上内容的使用提出独立的建议并开展这方面的教育。
- **NetSmartzKids** (<http://www.netsmartzkids.org>) –NetSmartz是国际失踪与受剥削儿童援助中心（NCMEC）和美洲儿童俱乐部（BGCA）提供的一种互动性教育安全资源，主要针对5至17岁的儿童，家长、监护人、教育界人士以及根据儿童所处年龄段采用3-D的方式向儿童传授网络安全知识的执法者。
- **世界儿童安全组织** (<http://www.safekids.org>) –由多个组织构成的全球性网络，其使命是防止儿童受到意外伤害（这是14岁及以下儿童的致命杀手）。
- **SafeKids.com** (<http://www.safekids.com>) –为向众多家庭提供帮助，使互联网及相关技术有趣、安全且富有成效而提供的资源。
- **StaySafe.org** (<http://www.staysafe.org>) –旨在帮助消费者了解互联网积极的一面以及如何管理网上存在的各类安全保障问题而设立的教育网站。
- **联合国儿童基金会（UNICEF）** (<http://www.unicef.org>) –保护儿童权利的全球倡导者，致力于向发展中国家的儿童及其家长提供长期的人道主义和发展援助。
- **WebSafe Crackerz** (<http://www.websafecrackerz.com>) –互动式游戏和智力测验，旨在为少年提供帮助并为处理垃圾信息、网上钓鱼和骗局等各类上网问题提供策略。

I.2 事件上报联络人清单范例

下文中的表I.1提供了互联网安全和保障事件上报的联络人清单范例：

表I.1—安全问题上报联络方式清单范例

组织名称	联系人
思科系统公司	mailto:safetyandsecurity@cisco.com http://www.cisco.com/security
事件响应和安全小组论坛（FIRST）	http://www.first.org/about/organization/teams/
微软公司	mailto:avsubmit@submit.microsoft.com mailto:secure@microsoft.com
日本电信资讯共享与分析中心（Telecom-ISAC）	https://www.telecom-isac.jp/contact/index.html

参考资料

- [b-ITU-T X.1051] ITU-T X.1051 建议书（2004年），信息安全管理系统－电信要求（ISMS-T）。
- [b-ISO/IEC 27001] ISO/IEC 27001:2005，信息技术－安全技术－信息安全管理体系统－要求（Information Technology – Security techniques – Information Security Management Systems – Requirements.）。
- <http://www.iso.org/iso/catalogue-detail?csnumber=42103>

ITU-T 系列建议书

A系列	ITU-T工作的组织
D系列	一般资费原则
E系列	综合网络运行、电话业务、业务运行和人为因素
F系列	非话电信业务
G系列	传输系统和媒质、数字系统和网络
H系列	视听和多媒体系统
I系列	综合业务数字网
J系列	有线网和电视、声音节目及其他多媒体信号的传输
K系列	干扰的防护
L系列	线缆的构成、安装和保护及外部设备的其他组件
M系列	电信管理，包括TMN和网络维护
N系列	维护：国际声音节目和电视传输电路
O系列	测量设备技术规程
P系列	电话传输质量、电话装置、本地线路网络
Q系列	交换和信令
R系列	电报传输
S系列	电报业务终端设备
T系列	远程信息处理业务的终端设备
U系列	电报交换
V系列	电话网上的数据通信
X系列	数据网和开放系统通信及安全
Y系列	全球信息基础设施、互联网的协议问题和下一代网络
Z系列	用于电信系统的语言和一般软件问题