国　际　电　信　联　盟

ITU-T X.1209

(12/2010)

国际电信联盟
电信标准化部门

X系列：数据网、开放系统通信和安全性

网络空间安全 – 计算机网络安全

网络安全信息共享与交换功能及其相关情境

ITU-T X.1209建议书

国际电信联盟

ITU-T X 系列建议书

数据网、开放系统通信和安全性

公用数据网	X.1–X.199
开放系统互连	X.200–X.299
网间互通	X.300–X.399
报文处理系统	X.400–X.499
号码簿	X.500–X.599
OSI组网和系统概貌	X.600–X.699
OSI管理	X.700–X.799
安全	X.800–X.849
OSI应用	X.850–X.899
开放分布式处理	X.900–X.999
信息和网络安全	
一般安全问题	X.1000–X.1029
网络安全	X.1030–X.1049
安全管理	X.1050–X.1069
生物测定安全	X.1080–X.1099
安全应用和服务	
组播安全	X.1100–X.1109
家庭网络安全	X.1110–X.1119
移动安全	X.1120–X.1139
网页安全	X.1140–X.1149
安全协议	X.1150–X.1159
对等网络安全	X.1160–X.1169
网络身份安全	X.1170–X.1179
IPTV安全	X.1180–X.1199
网络空间安全	
计算网络安全	**X.1200–X.1229**
反垃圾信息	X.1230–X.1249
身份管理	X.1250–X.1279
安全应用和服务	
应急通信	X.1300–X.1309
泛在传感器网络安全	X.1310–X.1339
网络安全信息交换	
脆弱性/状态信息交换	X.1520–X.1539
事件/事故/探索法信息交换	X.1540–X.1549
政策的交换	X.1550–X.1559
探索法和信息请求	X.1560–X.1569
标识和发现	X.1570–X.1579
确保交换	X.1580–X.1589

欲了解更详细信息，请查阅 ITU-T建议书目录。

ITU-T X.1209建议书

网络安全信息共享与
交换功能及其相关情境

摘要

ITU-T X.1209建议书介绍了网络安全信息共享和交换高级方案和配套功能，提供了支持网络安全信息共享和交换应用程序间的互操作性所需的功能。

文中描述的功能可用于支持以往独立运行的实体参加各种协调行动的情境/情况，例如防止或制止被纳入监管范围的行为或协调分析和界定工作。

上述功能的目标是通过支持互信各方的信息互操作性共享和交换，推进更为有效和有力的安全工作，共同监测、维护和全面管理系统和网络的安全。

沿革

版本	建议书	批准日期	研究组
1.0	ITU-T X.1209	2010-12-17	17

关键词

网络安全信息、信息交换、信息共享。

前言

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

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

WTSA第1号决议规定了批准建议书须遵循的程序。

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

注

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

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其它一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

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

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

目录

页码

ITU-T X.1209建议书

网络安全信息共享与
交换功能及其相关情境

1 范围

本建议书提供了支持网络安全信息共享和交换应用程序间的互操作性所需的功能。因此，第7条包含用于描述为第8条提及的功能确定场景的高级使用功能情境。为进一步说明这一功能的目的，第9条介绍了哪些功能可能在哪些情况下更具必要性。

本建议书针对的读者是受权从事安全工作的人员。

2 参考文献

无。

3 定义

3.1 其它资料定义的术语

本建议书采用了下列其它资料定义的术语：

3.1.1 网络安全[b-ITU-T X.1205]：网络安全涉及用以保护网络环境和机构及用户资产的各种工具、政策、安全理念、安全保障、指导原则、风险管理方式、行动、培训、最佳做法、保证和技术。机构和用户的资产包括相互连接的计算装置、人员、基础设施、应用、服务、电信系统以及在网络环境中全部传送和/或存储的信息。网络安全工作旨在确保防范网络环境中的各种安全风险，实现并维护机构和用户资产的安全特性。网络安全的总体目标包括下列各个方面：

- 可用性
- 完整性，其中可能包括真实性和不可否认性
- 保密性。

3.2 本建议书定义的术语

本建议书定义了下列术语：

3.2.1 网络安全信息：结构化的信息或知识可能包括但不限于设备、软件或网络系统的“状态”；相关事故或事件的取证；部署网络安全信息交换功能的各方；交换模块、架构和分配号码等网络安全信息的规范；用于上述多项内容及实施要求、指导原则和做法的身份和信任属性。

4 缩写词和首字母缩略语

本建议书定义了下列缩写词和首字母缩略语：

DDoS 分布式拒绝服务

FTP 文件传输协议

HTTP 超文本传输协议

HTTPS 安全超文本传输协议（HTTP over SSL）

IPS 入侵防御系统

5 常用语

无。

6 引言

利用病毒和蠕虫进行的网络攻击，采用各种技术通过网络加快其繁殖速度，其形式也愈发具有攻击性。已开发完成的反病毒、间谍软件检测、防火墙、虚拟专用网、入侵检测和防护等多种安全解决方案，旨在采取有效对策，以快速反应系统抵御这类颇具威胁性的攻击造成的安全事故。

安全管理人员针对漏洞、病毒、蠕虫和僵尸网络最常采用的防御手段，主要是举办吸引众多安全专家参与的各种论坛。通常在几天到一周的时间内使漏洞得到填补，薄弱环节得以修复，工作也恢复正常。

遗憾的是，被漏洞、蠕虫和僵尸网络利用的弱点会在整个网络迅速蔓延。几秒钟内，整个网络就会受到重大影响。

机构可以迅速实现内部的网络安全信息交换。但是，目前采用的方法并未对机构间广泛的信息交流给予充分支持。缺少有效的沟通方式，可能会使每个机构变成一个安全的孤岛。

因此，有必要在电信运营商、电信服务提供商和安全运行中心等众多机构之间共享网络安全信息。为了实现这一信息交流，必须要有：

- 供参与者更迅速地交流信息的可靠和安全的方法
- 确保隐私得到保护的方式。

本建议书为参与者安全、可信和可靠地交换网络安全信息提供了经过深思熟虑的设想和支撑功能。

7 功能情境

为从正确看待第8条列出的功能从而理解本建议书的内容，现分五个部分介绍高级使用情况，以便对以下五个逻辑功能组做出说明。

7.1 总体情境

这一总体情境适用于所有的后续情境。

情境：信息交流合作伙伴共享有助于发现和防范与其网络遭受敌对攻击的安全事件和事故相关的信息。

这种情境的一个要点是，双方可能收集到同类数据，但其来源和/或格式不同和/或数据类型相似，但内容略有差异。

7.2 运行政策

这个情境描述了一种不同信息交流合作伙伴在接触共享信息的不同内容时受到不同局限的情况。

情境：信息交流合作伙伴签有共享安全事件和事故相关信息的业务协议。

这种情境的一个要点是，可能需要根据按事先存在的互信关系授予的访问权，对每个信息交流伙伴的信息访问加以限制。另一个重要方面是，收到的信息获得的信任可能与现存的信任关系相关。

7.3 区域政策

此情境描述了多种信息交流合作伙伴的情况，其中不同的合作伙伴都对同类共享信息的不同内容有着不同的法律和/或监管限制。与前一种情境类似，这种情境着重提出了一种可能性：即一个人可获准共享实际上可能不准他接触或查看的信息。

这与前一种情境的差异在于对信息交换施加限制的来源不同。前一种情境的限制源自每个信息交流合作伙伴做出的运行决策，而本情境中的限制则源于外部施加的区域管辖权等运行决策。

情境：在不同区域经营的双方可以按照各自地区域对他们的不同要求交换信息。

这种情境的一个要点是，除面对遵循不同运行政策的各方外，还可能面临与信息交换所在区域相关的政策。

7.4 交换格式

情境：一个信息交流合作伙伴向另一合作伙伴提供的包括相关端口或端口范围的信息，涉及产生麻烦的业务量行为模式。这一共享的信息被用来确定具体的攻击实例。

这种情境的一个要点是，交换信息的内容必须易于得到所有信息交流合作伙伴的理解和赞同。

7.5 隐私保护

本条款包含的情境重点介绍了不同的隐私相关问题，企业或个人的“隐私”均包括在内。此外，这些情境还突显了确保信息交换自身保密功能的必要性。

- 情境：一安全运营中心收集的信息涉及针对其管理的某一网络、系统或更广义的受管理资产的恶意攻击，然后将此信息提供给网络服务提供商，以确定特定恶意攻击的来源。

  这种情境的一个要点是，网络服务提供商有能力亲自识别可疑的攻击来源，但不需要向安全运营中心透露这一信息。

- 情境：由一个信息交流合作伙伴收集的信息可能包含一套完整的信息交流要素，合作伙伴可能希望将要素透露给其机构或运行工作内部的交流伙伴，但不想透露给其运行工作之外的人员。

  这种情境的一个要点是，参与信息交流的各方可能选择共享的所有信息或仅共享其中的一部分，也可能在某种程度上混淆其共享的部分或所有信息之间的界限。

- 情境：双方经“公共”网络交流敏感信息。

  这种情境的一个重要方面是，无论使用哪种通信方式，都必须能够保证交换信息的私密性。

7.6 访问粒度

这种情境重点说明了可在不同条件下和根据不同条件共享不同类型或成份的安全信息的情况。

情境：服务以免费及订购方式发布公告和警示，根据订购业务对服务的定义提供不同等级的信息。

等级差异的例子说明，在某一等级只提供原始数据时，另一等级则同时提供原始和经分析的数据。

这种情境的一个要点是，尽管提供的所有信息都可能属一特定类型，但对于不同的另一方可能提供不同“等级”的信息。

7.7 来源验证

这种情境突出了认证信息交流合作伙伴的必要性。

情境：一个信息交流合作伙伴收到另一合作伙伴发来的信息，并验证该信息确实来自另一合作伙伴。

这种情境的一个要点是，互换信息的双方需要验证信息确实来自预计的发送方，而不是来自企图冒名顶替预计发送方的第三方。

7.8 多渠道分发

这种情境虽然类似“访问粒度”，但重点说明的是利用不同方法提供不同等级信息的情况。

情境：一个信息交流合作伙伴通过不同的手段，在不同条件下发出安全通报和提示。其数据既可以免费自可搜索目录下载，也可以在一个服务等级上有选择地通过电子邮件传递，或在另一个服务等级上以机器可读和可访问的形式提供。

这种情境的一个要点是，相同或不同类型的信息可经由不同的途径和在不同条件下提供。

7.9 后向兼容性

情境：两个信息交流合作伙伴已经在利用特定格式和协议交换具体信息。现提供的一项支持现行交换方式的新标准，可以提供新的附加功能。

这种情境的一个要点是，应对现有应用提供最大限度的支持，同时提供一个在新标准发布后升级的途径。

8 功能

以下各款列出了支持以上第7条所列各类情境的不同功能。

8.1 格式/编码功能

- 双方必须知道和了解安全信息的格式和结构。
  - 交换的安全信息具有异质性，如防火墙或其它网络安全设备的信息和特征，以及不同类型的应用专有信息，如事件和事故报告、分析和响应、取证数据交换等。
  - 交换信息的格式代表着异构系统环境产生并适用于这种环境的各类安全信息。
- 必须能够共享多种类型的安全相关信息。这方面的例子包括但不限于业务流量行为特征、系统访问特征、源IP地址、源和/或目标端口范围等
- 各方必须能够包容各种层次的信息，从单一的分组内容到全网络范围的 DDoS攻击涉及的所有分组。
- 安全信息的内容需要双方的了解和理解。
- 信息的主题、可用性和适用性必须具有可识别性。

8.2 传送/交换功能

- 各方必须能够通过分布广泛的分配和传输媒介，发送和接收安全信息。
- 应用程序可能需要支持各方在安全信息的共享和交换期间的同步和异步交流。
- 应用程序可能需要支持推式、拉式和基于订阅的信息传递。
- 应用程序需要在交换和处理大量安全信息期间支持稳定的运行。
- 采用的交换协议需要使用和/或基于广泛使用的现有协议。

8.3 安全功能

- 安全信息共享和交流涉及的网络安全信息必须能够得到验证与核实。
- 应用程序必须支持信息和服务的可靠性、保密性，完整性和可用性。
- 有关各方的身份必须是可核查和可验证的。
- 应用程序必须防范通过伪造和/或假造所含信息或所含信息来源/目的地的方式，对网络安全信息共享和交换发起的攻击。
- 源各方必须确保只允许受权方访问敏感信息。这一做法是为了通信的保密性，并适用于个人身份信息或私企信息所需的保密性，也适用于必须保密和仅供受权者使用的所有信息。
- 源各方必须能够在颗粒级控制访问，仅限受权的各方访问一特定安全信息具体内容，但无法接触他们未受权访问的部分。
- 各方必须能够保证安全相关信息的安全，即便在一个开放的环境中，在所有人，包括未经授权的各方都可获得安全相关信息的情况下，防止未经授权方获取信息。

8.4 政策功能

- 各方要能够独立定义和发布适用于提供和/或访问现有网络安全信息的地方和/或区域政策。就此的一个可能的例子是，不透露可能作为“政策”问题披露的路由信息。
- 各方要能够以符合各自适用于安全信息提供和/或访问政策的方式，提供和访问安全信息。
- 各方要能够宣布特定的政策声明适用于哪个管辖范围。
- 各方要能够独立确定和公布有关在各自司法管辖范围内提供和/或访问安全信息的可行的司法管辖要求和限制。
- 各方要能够以符合各自司法管辖要求的方式，提供和访问安全信息。

8.5 厂商中立功能

为了支持尽可能广泛的网络安全信息的共享和交换，应用程序在服务提供过程中应尽可能少地依赖具体厂商的系统或厂商专有数据，最好也不排斥任何一家厂商的系统或数据。

9 功能的适用性

本建议书描述的情境和功能提供了一套离散“工具”，人们可以有选择地混合匹配其应用来创建自己的应用。某些例如数据整合和/或信息搜索等复杂度较低的应用程序，可能只需上述功能当中的少数几项，而其它功能丰富并提供更广泛服务的应用，则可能需要综合上述功能并增加其部署。

以下探讨的是何时更需要特定类型的功能，以及它们何时能够更具可选性。

9.1 格式/编码功能

为给所有网络安全信息的共享和交换创造条件，信息的发送者和接收者必须能够准确了解他们交换的内容。因此，格式和编码功能应适用于任何和所有网络安全信息共享和/或交换的情境。

9.2 传送/交换功能

与格式和编码功能同样重要的是，两个或更多的信息交流合作伙伴需要一种将信息由发送方传送至接收方的方法。

9.3 安全功能

如没有至少某种程度的交换合作伙伴身份识别作为保障，并且不能保证他们之间通信信道的安全，交换安全相关的信息就没有什么意义。

但是，不同的情况和应用有着不同的安全要求，因此采用者和执行者必须充分考虑其具体的应用需要。

例如，两个交流合作伙伴在一个应用程序中有一条采用自己的安全措施的专用通信线路，他们在交流环境已经提供的条件之外，几乎或根本无须专门考虑安全问题。

另一方面，如果信息是通过可公开访问的通信渠道提供的，就可能需要广泛的安全措施。

9.4 政策功能

并非所有支持网络安全信息共享和交换功能的应用都需要利用这一功能公布限制、限度和/或授权。然而，公布这类政策相关信息的功能，在许多商业和个人情境当中发挥着重要作用。

在安全功能当中，可能由于业务或合同协议的原因，政策相关的功能是在特定应用之外提供的，因此可能无需应用内部的政策公布和执行功能。

9.5 厂商中立功能

厂商中立性具有很强的情境依赖性。如果一个人利用一特定厂商的交换格式和/或交换协议分享或交换这一厂商的产品产生的分享或交换数据，厂商中立性就不能付诸实施。

另一方面，如果特定应用程序的目标是最广泛的应用和提供信息交换支持，那么，对于厂商专用方法和/或信息保持中立立场就会被视为具有重要意义。

附录 I
关于网络安全信息共享和交换的介绍

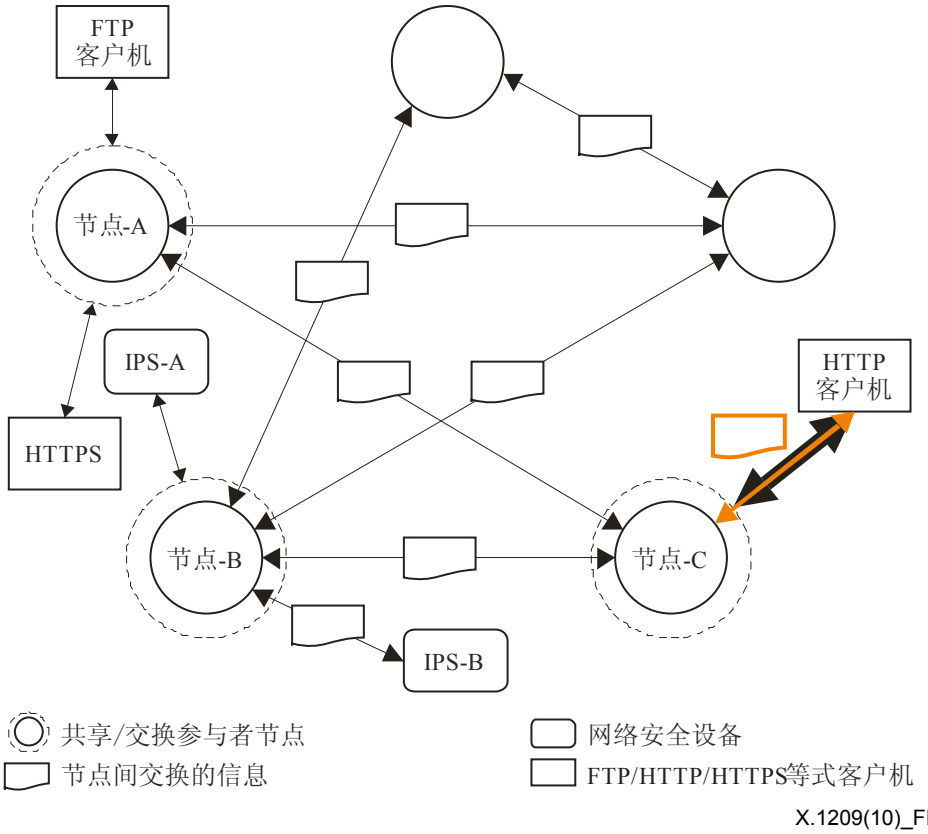
（本附录不构成本建议书的组成部分）

本附录介绍了图I.1和I.2所示的信息网络安全应用实例的概念结构。两幅图表显示了由第7条所列功能实现的应用拓扑的两个不同视图。虽然还可能有其它拓扑结构，这里显示的拓扑包括了所有功能的使用，而其它可能的拓扑结构和应用程序则可能只需要一个上述功能的子集。

第一个图表描述了许多信息共享合作伙伴的情境，而每个情境共享的功能、应用和信息都不相同。它显示了利用该信息的应用以不同方式访问一特定节点的信息的情况。

应当指出，虽然本附录并未确切指定该信息的使用方式和目的，只提到可以通过多种方式对它进行访问。另外，第一个图表还显示，所有节点间的交换都是通过采用标准化的消息格式加以支持的。

第二个图表是第一个图表的三维透视图，展示了两个信息交流合作伙伴的实例，并介绍了每个伙伴为参与交流过程而可能需要配属的功能。与第一个图表相同的是，实际的事实或应用可能并不需要上述能力支持的所有功能，因此可以自由选择将哪些功能真正纳入特定的实施/应用。



图I.1　网络安全信息共享和交换部署实例

- 所有参与者节点都通过标准化的信息进行交流。

  以下能力对于支持这项功能非常重要：

  – 格式/编码功能（第8.1条）

  – 传送/交换功能（第8.2条）

- 要求一个节点提供的信息，实际上可能由另一节点提供。

  以下能力对于支持这项功能非常重要：

  – 安全功能（第8.3条）

  – 政策功能（第8.4条）

- 一特定节点可能实施框架协议，或通过其它协议/服务提供框架数据，例如FTP 或HTTP被用于从A节点访问框架数据。

  以下能力对于支持这项功能非常重要：

  – 格式/编码功能（第8.1条）

  – 传送/交换功能（第8.2条）

  – 厂商中立功能（第8.5条）

- 连接B节点的入侵防御系统（IPS-A）和另一入侵防御系统（IPS-B）等安全设备，可通过IPS-B等直接访问或经IPS-A等包装服务访问网络安全信息，要么以网络安全和信息共享和交换的标准方式或利用设备依赖/专有的方法，使设备能够使用共享和交换功能。

  以下能力对于支持这项功能非常重要：

  – 格式/编码功能（第8.1条）

  – 传送/交换功能（第8.2条）

  – 厂商中立功能（第8.5条）

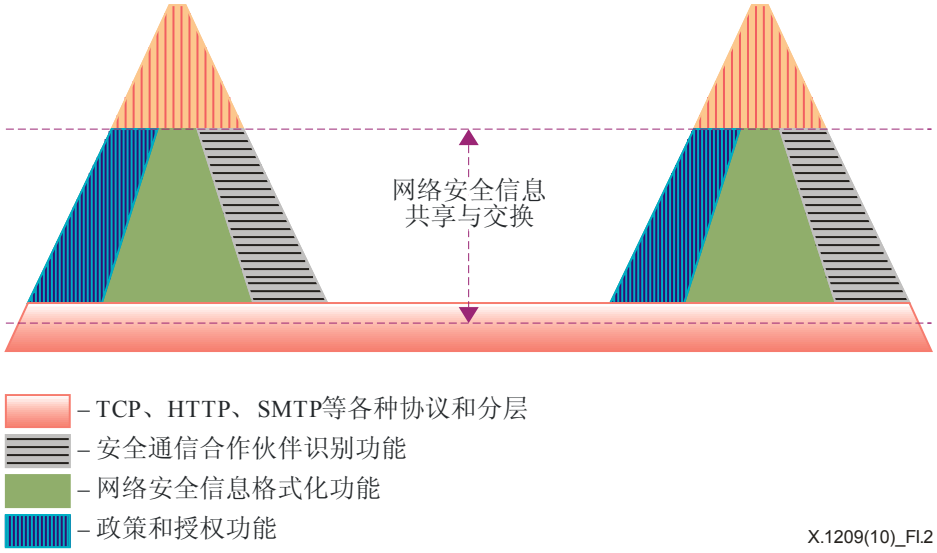
- 安全设备可利用所有支持承载信息的协议或协议层，例如客户端用于向C节点申请服务的TCP/IP、HTTP、HTTPS和SSL。

  以下能力对于支持这项功能非常重要：

  – 格式/编码功能（第8.1条）

  – 传送/交换功能（第8.2条）

  – 厂商中立功能（第8.5条）



图I.2 双节点透视图

- 参与节点通过各种协议和分层协议交换申请和响应。

  以下能力对于支持这项功能非常重要：

  – 格式/编码功能（第8.1条）

  – 传送/交换功能（第8.2条）
- 许多应用程序需要可信的通信伙伴识别方式。

  以下能力对于支持这项功能非常重要：

  – 安全功能（第8.3条）

  – 政策功能（第8.4条）
- 节点获得并利用其它节点提供的数据。

  以下能力对于支持这项功能非常重要：

  – 格式/编码功能（第8.1条）

  – 安全功能（第8.3条）

  – 政策功能（第8.4条）

  – 厂商中立功能（第8.5条）
- 应用程序利用各种授权验证功能，根据应用的需要满足各种安全相关要求。

  以下能力对于支持这项功能非常重要：

  – 政策功能（第8.4条）
- 应用程序可能出于各种原因，如A节点的客户端要求访问B节点提供的网络安全信息，需要利用来自其它节点的身份信息。

  以下能力对于支持这项功能非常重要：

  – 政策功能（第8.4条）

- 一特定节点的核心功能包括：
  - 接收网络安全信息。
  - 存储/存档网络安全信息。
  - 处理网络安全信息申请。

  以下能力对于支持上述功能非常重要：
  - 格式/编码功能（第8.1条）
  - 传送/交换功能（第8.2条）
  - 政策功能（第8.4条）
- 应用程序利用相关的授权和授权验证工具处理与访问相关的问题。

  以下能力对于支持这项功能非常重要：
  - 安全功能（第8.3条）
  - 政策功能（第8.4条）
- 应用程序利用通用的数据模型处理节点间的访问相关问题。

  以下能力对于支持上述功能非常重要：
  - 格式/编码功能（第8.1条）
  - 传送/交换功能（第8.2条）
  - 厂商中立功能（第8.5条）
- 应用程序将可靠的识别符用于节点间以及节点与客户端之间的通信。

  以下能力对于支持这项功能非常重要：
  - 安全功能（第8.3条）
  - 政策功能（第8.4条）
- 节点间的请求与响应被视为“规范”，而应用程序可能在节点对客户端的请求与响应之间，向未实施标准化方式的客户端和/或用于节点间的协议提供应用层接口。

  以下能力对于支持上述功能非常重要：
  - 格式/编码功能（第8.1条）
  - 传送/交换功能（第8.2条）
  - 厂商中立功能（第8.5条）
- 这一框架同时支持推式和拉式运作模式以及有状态和无状态运作模式。

  以下能力对于支持上述功能非常重要：
  - 传送/交换功能（第8.2条）
- 应用程序的结构可以提供进入应用程序所需的可靠认证和识别模型的“钩子”。

  以下能力对于支持这项功能非常重要：
  - 安全功能（第8.3条）
  - 政策功能（第8.4条）

附录 II
相关活动

（本附录不构成本建议书的组成部分）

II.1 通用安全信息

通用安全信息是美国计算机应急响应协调中心（CERT/CC）、 MITRE等非营利机构或开放项目公开提供的安全信息，其中涉及常见漏洞和披露（CVE）、常见缺陷列表（CWE）、共同恶意软件列表（CME）、常见共同攻击样式列举与分类（CAPEC）、开放源代码弱点数据库（OSVDB）、[b-Snort]或[b-Bro]提供的特征等。

在MITRE看来，CVE是一众所周知的信息安全漏洞和披露目录，被用作美国国家标准与技术研究院开发国家漏洞数据库（NVD）的依据。常见缺陷列表（CWE）提供了一个统一可测的软件漏洞集，从而提高了讨论、描述、选择和使用可在源代码和操作系统中发现这些弱点的软件安全工具和服务的效率。共同恶意软件列表（CME）提供了统一的新病毒威胁和最流行新生病毒威胁的标识符，以减少恶意软件事件在公众中引起的混乱。其目的并不在于取代厂商对病毒和其它类形恶意软件所用的名称，而是方便采用共享的恶意软件中立索引功能。常见共同攻击样式列举与分类（CAPEC）提供了一个有关攻击模式的公开目录，并附有全面架构和分类。

开放源代码弱点数据库（OSVDB）是安全业界开发并为该业界服务的独立开放源代码数据库，旨在提供有关安全漏洞的准确、详细、及时和公正的技术信息，同时促进公司和个人之间更广泛和开放的合作，消除重复工作，并减少内部开发与维护漏洞数据库的固有开支。

Snort是一个开源网络入侵防范和侦测系统，采用规则驱动语言并综合了基于特征、协议和异常的检测方法。Snort的规则通过了比照漏洞研究小组（VRT）用于客户的相同标准进行的严格测试。

最后，Bro是一个以被动监控网络流量并侦测可疑活动的网络入侵检测为基础的开放源代码项目。Bro的规则可以进行活动描述，说明哪些活动应该得到提示，或提供描述已知攻击的特征或对已知漏洞的访问。

II.2 新型安全信息

新型安全信息是自动生成的有关新的威胁或攻击、异常流量、未知蠕虫等攻击的特征。攻击特征的生成是近来的热门研究课题，而且“Early bird”和“测谎”（Polygraph）等一些试验性解决方案已经推出。这些解决方案的主要作用是检测网络攻击和捕捉字节序列，即攻击身份的代表。FirstLight特征服务或Endeavor Security 公司的主动恶意软件防范和韩国电子通信研究院（ETRI）的零日攻击特征管理基础设施（ZASMIN）提供了不断更新、修订和扩展的新特征。这些研发中的先进图形生成技术使我们能够根据攻击流量自动生成特征。虽然在提高特征质量方面取得了进展，但特征共享还处于初级阶段。

II.3 与安全信息共享相关的活动

II.3.1 计算机事件响应小组（CIRT）

计算机事件响应小组（CIRT）研究网络安全漏洞和网络系统的长期变化，并提供有助于提高安全性的信息和培训。它们持续对重大安全事件做出响应，并对产品漏洞进行分析。随着互联网规模的迅速扩张及其在关键职能中的应用，入侵者的伎俩也在不断花样翻新，破坏的程度加大，而且并增加了发现攻击和捕捉攻击者的难度。

II.3.2 欧洲网络与信息安全局

欧洲网络与信息安全局（ENISA）提交了首份有关欧洲信息共享和警报系统（EISAS）的可行性研究报告，向中小型企业（SME）和欧盟公民通报威胁、漏洞和攻击信息。可行性研究报告认为，促进欧盟信息共享的最理想的方式，是在研讨过程中承担起推动方和主持人的作用，在国家信息共享和预警系统之间扮演“良好做法守护人”的角色，而不是亲自挂帅，履行运行职能。为了开展有关欧洲信息共享和警报系统（EISAS）的可行性研究，必须承担起经认证的职能。欧洲信息共享和警报系统建议的通用模型包括三个主要组成部分，而且该模型的目的在于确定欧洲信息共享和警报系统可为成员国现有的信息共享活动带来增值的领域，并填补功网络和信息安全（NIS）信息的覆盖空白。这三个组成部分是信息收集部分（IGC）、信息处理部分（IPC）和信息传播部分（IDC）。

II.3.3 事件响应与安全组织论坛

事件响应和安全组织论坛（FIRST）是首屈一指和公认的全球事件响应的佼佼者。加入该论坛可以提高响应团队对安全事件事后和事前的应对效率。这次论坛汇集了来自政府、商业和教育机构的多支电脑安全事故应急队伍，旨在促进事故预防工作，以激厉快速反应合作与协调，并促进广大成员和社会各界之间的信息共享。

II.3.4 亚太地区计算机应急响应组

亚太地区计算机应急响应组（APCERT）与计算机事件响应小组（CIRT）和计算机安全事件响应小组（CSIRT）联手确保围绕真正的信息共享、信任与合作的亚太区域互联网安全。他们既可以促进包括成员之间的安全信息、病毒和恶意代码信息的共享和技术交流，也能推进针对其成员关注议题的合作研发工作，还能够为解决关系跨区域安全信息和应急响应的法律问题提出建议。

II.3.5 日本信息共享与分析中心

互联网和其它电信网络构成了世界范围内社会经济结构的基础。确保信息安全成为社会经济生活中的紧迫问题。

日本信息共享与分析中心（Telecom-ISAC）旨在收集、分析和分享事件的信息，并及时采取措施，确保电信业务无阻和稳定的运行。此外，分析中心创建了一个由广泛的合作成员组成的论坛，以分享他们的真知灼见与经验，包括安全风险、漏洞和安全解决方案等信息。

附录 III
相关活动

（本附录不构成本建议书的组成部分）

[APCERT] 亚太地区计算机应急响应组。*http://www.apcert.org*

[CERT] 计算机事件响应小组。*http://www.cert.org*

[ENDEAVOR] Endeavor Security公司。*http://www.endeavorsecurity.com*

[FIRST] 事件响应与安全组织论坛。*http://www.first.org*

[MITRE] MITRE。*http://makingsecuritymeasurable.mitre.org/*

[Telecom-ISAC] 日本信息共享与分析中心。*https://www.telecom-isac.jp*

[WIKI] 维基百科。*http://en.wikipedia.org*

参考资料

[b-ITU-T X.1205] ITU-T X.1205建议书（2008年4月），《网络安全概览》。

[b-Bro] Bro（2004年11月）《快速入门指南》。

[b-EISAS] 欧洲信息共享和警报系统（2006/2007年），《可行性研究》。

[b-OSVDB] 开放源代码弱点数据库。《项目的宗旨与目标》。

[b-Snort] Snort（2008年5月），《Snort 用户手册2.8.2》。

[b-ZASMIN] 韩国电子通信研究院信息安全研究处，《零日攻击特征管理基础设施》。

ITU-T系列建议书

A系列	ITU-T工作的组织
D系列	一般资费原则
E系列	综合网络运行、电话业务、业务运行和人为因素
F系列	非话电信业务
G系列	传输系统和媒质、数字系统和网络
H系列	视听及多媒体系统
I系列	综合业务数字网
J系列	有线网络和电视、声音节目及其它多媒体信号的传输
K系列	干扰的防护
L系列	电缆和外部设备其它组件的结构、安装和保护
M系列	电信管理，包括TMN和网络维护
N系列	维护：国际声音节目和电视传输电路
O系列	测量设备的技术规范
P系列	电话传输质量、电话设施及本地线路网络
Q系列	交换和信令
R系列	电报传输
S系列	电报业务终端设备
T系列	远程信息处理业务的终端设备
U系列	电报交换
V系列	电话网上的数据通信
X系列	**数据网、开放系统通信和安全性**
Y系列	全球信息基础设施、互联网协议问题和下一代网络
Z系列	用于电信系统的语言和一般软件问题

瑞士印刷
2011，日内瓦