

国 际 电 信 联 盟

ITU-T

国际电信联盟
电信标准化部门

X.1570

(09/2011)

X系列：数据网、开放系统通信和安全性
网络安全信息交换 – 标识和发现

网络安全信息交换中的发现机制

ITU-T X.1570 建议书

ITU-T

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	
网络安全概述	X.1500–X.1519
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。

网络安全信息交换中的发现机制

摘要

ITU-T X.1570建议书提供了网络信息发现框架和将它付诸实施的机制。发现可被视为网络安全信息周期中的一个阶段，紧邻信息的发布和获取这些信息发现中完整和必要的阶段。因此这一框架涉及公布网络安全信息、获取候选列表并取得必要信息的方法。只要发现机制符合框架要求，它可与任意机制一起实施，而这些机制当中包括也在本建议书中得到阐述的基于目标标识符（OID）和基于资源描述框架（RDF）的发现程序。

沿革

版本	建议书	批准日期	研究组
1.0	ITU-T X.1570	2011-09-02	17

关键词

网络安全信息、源头发现、信息发现。

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/>。

© 国际电联 2012

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
1 范围	1
2 参考文献	1
3 定义	1
3.1 其他地方规定的术语	1
3.2 本建议书中规定的术语	1
4 缩写词和首字母缩略语	2
5 惯例	2
6 网络安全信息来源确定和定位框架	3
7 被发现网络安全信息的种类和详细程度	3
8 网络安全信息标识符	4
9 发现机制种类	5
9.1 网络安全信息交换中基于OID的发现机制	5
9.2 网络安全信息交换中基于RDF的发现机制	6
10 目前可用的获得已发现信息的方法	7
附录I – 网络安全操作信息实例模型	8
I.1 网络安全操作域	8
I.2 职能	8
I.3 网络安全信息	9
附录II – 描述数据库和知识库的规程	12
附录III – 基于RDF发现的实施示例	13
III.1 基于RDF发现的实施示例	13
III.2 网络安全信息等级分层	13
参考资料	15

引言

目前人们比以往任何时候都更加注重网络安全信息交换。称作Cybex的一种网络安全信息交换国际标准特别引起了人们的极大关注。Cybex发现 – 提供找出网络安全信息来源的机制 – 是Cybex众多不同技术规范之一，本文件旨在解释该规范的框架及其技术。

网络安全信息交换中的发现机制

1 范围

本建议书提供了网络信息发现框架和将它付诸实施的机制。发现可被视为网络安全信息周期中的一个阶段，紧邻信息的发布和获取这些信息发现中完整和必要的阶段。因此这一框架涉及公布网络安全信息、获取候选列表并取得必要信息的方法。只要发现机制符合框架要求，它可与任意机制一起实施，而这些机制当中包括也在本建议书中得到阐述的基于目标标识符（OID）和基于资源描述框架（RDF）的发现程序。

2 参考文献

下列ITU-T建议书和其他参考文献的条款，在本建议书中的引用而构成本建议书的条款。在出版时，所指出的版本是有效的。所有的建议书和其它参考文献均会得到修订，本建议书的使用者应查证是否有可能使用下列建议书或其它参考文献的最新版本。当前有效的ITU-T建议书清单定期出版。本建议书引用的文件自成一体时不具备建议书的地位。

[ITU-T X.660] ITU-T X.660建议书 | ISO/IEC 9834-1, 信息技术 – 对象标识符注册主管机构的运营程序：国际对象标识符树的总体程序和顶级弧（2011年）

[W3C RDF] W3C Recommendation (2004), *Resource Description Framework (RDF): Concepts and Abstract Syntax*.
<<http://www.w3.org/TR/rdf-concepts/>>

3 定义

3.1 其他地方规定的术语

本建议书使用了下列其他地方规定的术语。

3.1.1 对象标识符[ITU-T X.660]：从国际对象标识符树的根至节点的一个正整数值的有序列表，未明确标识该节点。

3.1.2 实例模型 [b-Gruber]：是概念化的明确规范。

3.2 本建议书中规定的术语

本建议书规定下列术语：

3.2.1 网络安全 [b-ITU-T X.1500]：涉及以下方面的结构性信息或知识：

1. 与网络安全相关的设备、软件或网络系统的“状态”，特别是漏洞；
2. 有关事故或事件的取证；
3. 从以往事件获取的试探和签名；

4. 在网络框架范围内实施网络安全信息交换能力的有关各方；
5. 网络安全信息交换规范，其中包括模块、方案、政策以及指定编号；
6. 所有上述的身份和信任属性；
7. 实施要求、导则和做法。

注 – 该定义基于[b-ITU-T X.1500]中对于网络安全信息给出的描述。

3.2.2 交换（网络安全信息） [b-ITU-T X.1500]：两个或两个以上网络安全实体之间网络安全信息的传送，该传送可为单向、双向或多向传送，即多个至多个实体的传送。

3.2.3 发现：发现目标的行为或程序，即，首次了解目标

3.2.4 检索器：是检索网络安全信息的实体。

4 缩写词和首字母缩略语

本建议书使用下列缩写词和首字母缩略语：

CCE	通用配置列表
CERT	计算机应急响应小组
CIRT	计算机事件响应团队
CPE	通用平台列表
CVE	通用漏洞和暴露
CVSS	通用漏洞评分系统
CWE	通用缺陷列表
CWSS	通用缺陷评分系统
CYBEX	网络安全信息交换
HTTP	超级文本传送协议
IODEF	事件对象描述交换格式
MAEC	恶意软件属性列表和特性
OID	对象标识符
OVAL	开放漏洞和评估语言
RDF	资源描述框架
SCAP	安全内容自动协议
SNMP	简单网络管理协议
XCCDF	可扩展配置对照清单描述格式

5 惯例

无。

6 网络安全信息来源确定和定位框架

不同网络安全组织目前正在实施通用网络安全协议，以便捕获和交换操作应用中的网络状态、漏洞、事故取证和事故试探信息。由于该信息源于多种不同渠道，因此实施方应统一它们之间确定网络安全组织、信任和信息交换政策以及被交换或分布的信息本身的方法。为解决这一问题，本节介绍网络安全信息来源确定和定位框架 – 网络安全信息发现框架。

三个实体参与找出网络安全信息：检索方、信息源和目录。检索方通过发送请求检索信息，信息源提供所要求的信息，目录对信息源信息的元数据予以登记并协助检索方找出正确的信息源。

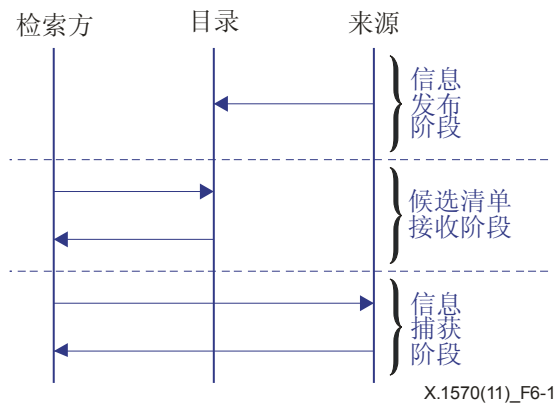
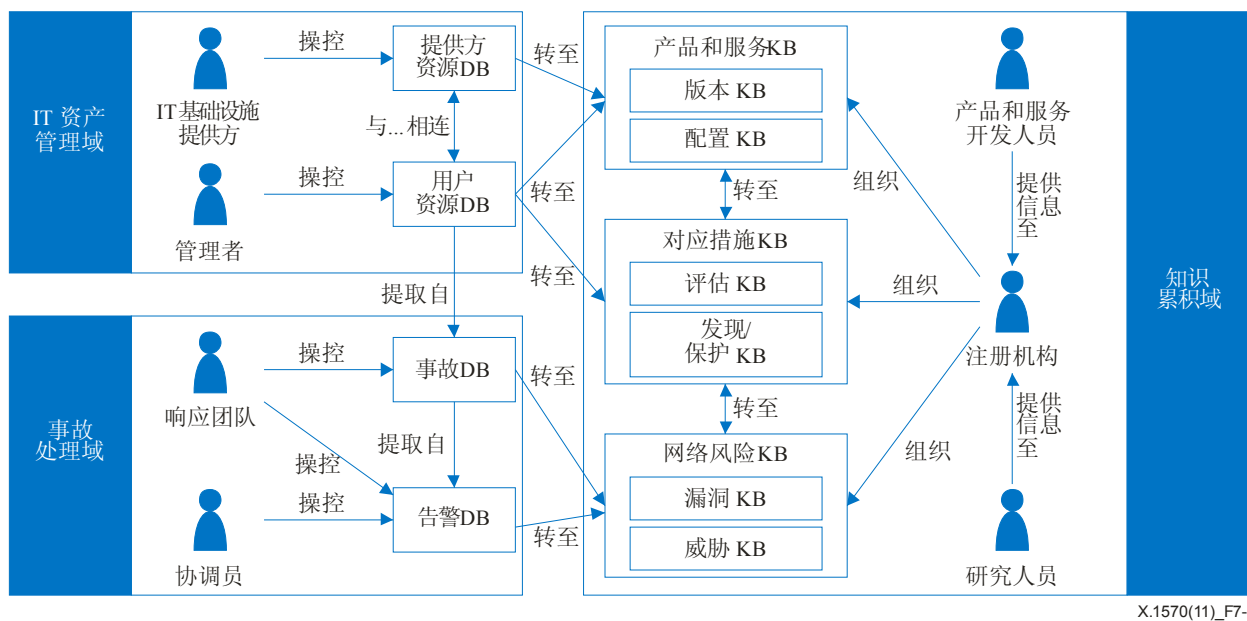


图 6-1 – 发现的三个阶段

发现程序是三个实体之间的通信程序，如图6-1所示。该程序共包括三个阶段 – 信息发布、候选清单接收和信息捕获。信息来源在信息发布阶段与目录进行注册，从而将其信息公布至网络界。检索方在候选清单接收阶段向注册机构进行查询，以接收候选信息来源清单，并从该清单中选出似乎最适合信息来源选择阶段的信息源。

7 被发现网络安全信息的种类和详细程度

发现机制能够发现网络安全信息。该机制旨在发现下列七种信息：用户资源数据库、提供商资源数据库、事件数据库、告警数据库、产品和服务知识库、网络风险知识库和对策知识库。图7-1所示的实例模型对上述各类信息进行了确定。



DB: 数据库 KB: 知识库

图7-1 – 网络安全信息实例模型

该实例模型描述网络安全信息知识的捕获、积累和使用，这种知识由一系列不同类型、特性和关系构成。图中的实线表示信息类型之间的关系，箭头表示从一个实体输入到知识库/数据库中的信息。右侧所示功能为一般性功能和实体，如CIRT（可能包含图中一个或多个功能）。该模型用于确定网络安全运营域，之后用于确定为支持每个域的运营而需要的网络安全实体。实例模型的细节见附录I的描述。

表II.1示出了符合该实例模型中描述的七类信息的安全规范。因此，被发现网络安全信息的详细程度符合规范的详细程度。由于引入和采用多种可根据具体目标制定的规范，因此这一详细程度十分灵活。

8 网络安全信息标识符

需要独一无二的标识符来确定网络安全信息。任何用于全球网络安全信息交换的全球独一无二的标识符都必须具有下列特性：

- 简单、易用、灵活、具有时空扩展性和可部署性
- 多种标识符方案的分布管理
- 长期可靠的标识符注册管理机构和随时可用的高性能工具，以发现与任何给定标识符相关的信息。

目前存在满足上述要求的两个候选独特标识符：对象标识符（OID）框架和资源描述框架（RDF）。如下列第9节所述，上述两个标识框架是通用服务和信息发现的首要手段。

9 发现机制种类

只要发现机制符合框架，即可利用任意机制对其加以实施。发现机制分为两类 – 集中和非集中机制（从其注册和管理安全信息的注册机构角度划分）。

在集中发现机制中，目录管理一个或多个“中央”注册机构，从而方便人们轻而易举地对目标信息进行定位和快速发现（在该情况下可略去候选清单接收阶段），但搜索方在使用注册机构时需首先知道存在这一机构。维护集中式存储库所涉及到的各种资源和费用也可能使资源有限的人们对其望而却步。此方面具有代表性的机制是基于OID的发现机制。

在非集中式机制中，目录管理多个“分布式”注册机构。该机制的优势是最大限度地降低了提供信息所需的资源和费用，同时信息提供方和搜索方均无需事先相互了解各自的存在。然而，为了在毫不知情的情况下找到信息，搜索方几乎需要查遍整个互联网。此种情形的代表机制是以RDF为基础的发现机制。

9.1 网络安全信息交换中基于OID的发现机制

基于OID的发现机制提供使用OID来确定和定位网络安全信息来源的方法和机制。该机制的基本理念和每阶段程序解释如下。OID有助于确定相关资源，按照OID树可找到任何已登记的网络安全信息。网络安全信息按照网络安全信息交换对象标识符弧 {joint-iso-itu-t(2) cybersecurity(48)} [b-ITU-T X.1500.1]进行登记。

第6节介绍的各项发现阶段在下述第9.1.1至9.1.3节中予以详细说明。

9.1.1 信息公布阶段

在登记信息时，信息源提供多种类型的元数据信息，其中主要信息种类包括国家/区域、组织身份（ID）、信息种类和信息描述格式。国际/区域信息明确规定组织的国家，或组织所在的区域（如来源为跨国组织（如国际电信联盟））。组织ID明确规定组织并使用股票代码或独特企业名称对其描述。信息种类规定信息类别。信息类别规定的信息种类在第7节中得到阐述。信息描述格式规定相关格式，如与CVE兼容的格式[b-ITU-T X.1520]或与ARF兼容的格式[b-ARF]。

目录一经收到信息来源提出的登记请求，即根据元数据登记和存储信息，并建立OID树。虽然本建议书并未规定该树的规范性结构，但附录I和附录II说明一些候选结构。

9.1.2 候选清单接收阶段

检索方不一定需要向拥有一个统一一致OID树的注册机构的目录进行查询，它可以事先知道该树的结构，并遵循该树在无需发出查询的情况下确定所需信息。由于树结构ID有利于提供多种多样的子树，因此检索方可非常有效地缩小候选清单范围。

目录可接受任意查询（包括文本搜索查询）并利用候选清单做出答复。

9.1.3 信息捕获阶段

根据候选清单或遵循直到树叶的树，检索方选定一个信息来源，然后向信息来源发送请求，后者即提供网络安全信息。

对于基于OID的发现，候选清单接收和信息捕获阶段可谓无法分离，因为通过遵循树而缩小候选范围可使人们最终选定一个单一的信息来源。

9.2 网络安全信息交换中基于RDF的发现机制

基于RDF的发现机制提供确定和定位以RDF为基础的网络安全信息源的方法和机制，其理念和能力描述如下。图9-1所示为该机制理念。信息来源可与一个或多个目录（包含注册机构）进行登记，以方便检索方检索信息。在发现过程中，有关网络安全实体身份和能力的信息在实体之间进行交换。网络安全实体向目录发送发现请求（其中每一个实体均有不同信息来源），并由此成为搜索引擎的广泛搜索。

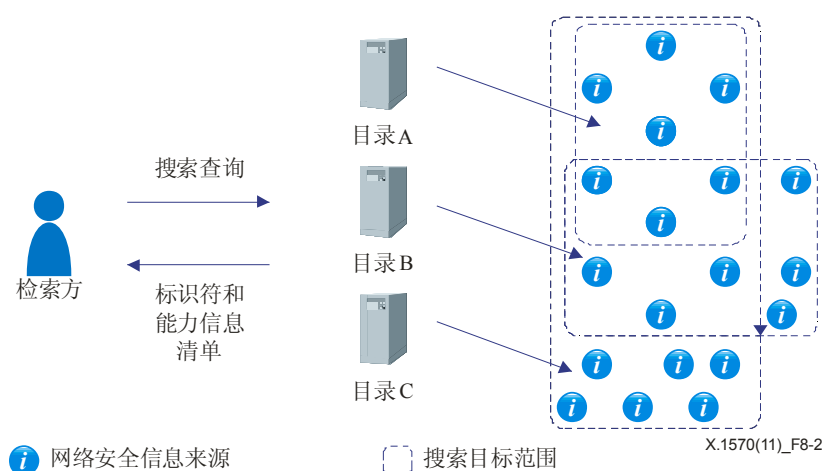


图 9-1 – 基于RDF的发现理念

与基于OID的发现不同，基于RDF的发现拥有包含多个实体的目录，见图8-3。从功能角度而言，目录包含一个发现代理和一个注册机构代理。发现代理与检索方（接收机界面）进行通信，注册机构代理与信息来源进行通信（信息源界面）。某些情况下，发现代理和注册机构代理可置于同一计算机内。四个实体之间交换能力和标识符信息。

第6节介绍的发现阶段的具体描述见第9.2.1至9.2.3节。

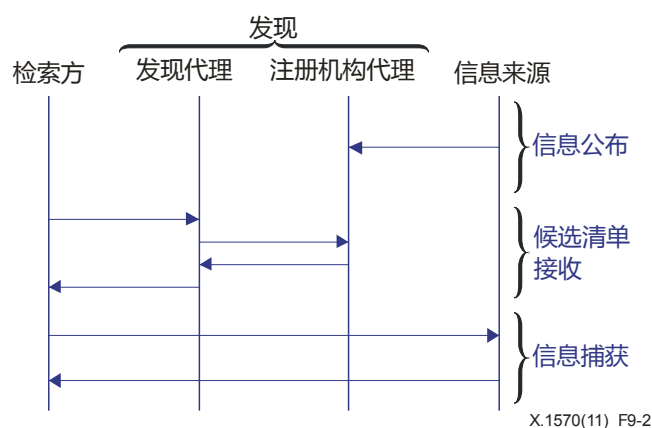


图 9-2 – 基于RDF的发现序列图

9.2.1 信息公布阶段

信息来源向注册机构代理登记其信息，后者在信息公布阶段生成和安排数据的适当元数据。与基于OID的发现相同，信息源在登记网络安全信息时提供多种类型元数据信息，其中主要类别包括国家/区域、组织身份（ID）、信息类型和信息描述格式。国家/区域明确规定组织所属的国家或组织所属的区域（如来源为像国际电联这样的跨国组织）。组织身份明确规定组织并可通过使用股票代码或独特企业名称对其进行描述。信息种类规定第7节所述的信息类别。信息描述格式规定相关格式，如与CVE兼容或ARF兼容的格式。

目录在从信息来源处收到登记请求后，即根据元数据对信息进行登记和存储，并更新RDF数据库。由于注册机构代理常常使用分层式注册机构，因此注册机构代理需要确定应在哪个注册机构中存储数据。

虽然本建议书并未规定RDF元数据格式的规范性结构，但附录I和附录II给出了一些候选结构。

9.2.2 候选清单接收阶段

检索方向发现代理发送查询，后者将其前转至一个或多个适当的注册机构代理，注册机构代理在其元数据数据库中进行检索，并在候选清单接收阶段以候选信息来源清单做出回复。发现代理将收自多个注册机构代理的信息进行汇总并将其发至检索方。

9.2.3 信息捕获阶段

检索方在信息捕获阶段从清单中选出最适合的信息来源。

10 目前可用的获得已发现信息的方法

可采用各种通信协议交换网络安全信息，包括HTTP（使用RDF）和SNMP（使用OID）。

有些人可能希望通过制定访问控制政策限制访问已发现信息的相关方面。这些政策的主要标准包括IP地址：域名、通信协议、身份和密码以及识别证书。

任何搜索网络安全信息的方面都需交换多种信息，包括请求信息。X.1500系列建议书对这些方法做出了规定。

附录I

网络安全操作信息实例模型

(本附录不构成本建议书的组成部分)

本建议书第7节采用了图7-1描述的网络安全操作信息实例模型。本附录将详细介绍该实例模型。

该模型包括网络安全域、在这些域内执行操作所需的职能以及与这些职能有关的网络安全信息。下面对此详细介绍。

I.1 网络安全操作域

“网络安全操作”一词涵盖网络安全社会的一系列网络安全操作，但该实例模型集中在保护网络社会信息安全的网络安全操作。信息安全是保护信息的保密、完整和可用，有时也包括信息的安全、真实和可靠性。

在描述此类操作域时，实例模型提供三种网络安全操作域：IT资产管理，事故处理以及知识积累。

IT资产管理：该域负责在诸如对IT资产的安装、配置和管理等用户组织内执行网络安全操作，既包括事故预防，也包括损失控制操作。IT资产不仅包括用户的自身IT资产，也包括网络连接，云服务，以及由外部实体为用户提供的身份识别服务。

事故处理：该域负责对网络设和发生的事故通过检测计算机事件方式进行侦测和回应，事故包括多个计算机事件以及导致事故发生的攻击行为。更具体的，它监测计算机事件，当侦测到异常事件时，它给出一个事故报告。基于该报告，它对事故进行详细调查，以便其能够解释攻击的模式及其反制措施。基于事故分析，它可以向用户组织提供警报和提示，比如潜在威胁预警。

知识积累：该域负责收集和产生网络安全信息，并为其他组织提取可用知识。为便于重复使用，它提供通用命名和分类，并籍此组织和积累知识。该域充当组织边界之外的全局合作基础。

I.2 职能

基于以上定义的网络安全操作域，本节给出每个域内开展网络安全操作的必要职能。IT资产管理域包括一个管理者和一个IT基础设施提供者，事故处理域包括一个应急小组和一个协调员，知识积累域包括一个研究者、一个产品和服务开发者以及一个操作记录者。这里要注意的是，这些职能是从功能角度定义的；因此，一个实体可能根据情况承担若干职能。

管理者：该职能负责管理组织系统并维持其功能。该职责负责监控系统的使用，通过运行完整性测试、扫描漏洞环节以及执行渗透测试等对系统进行诊断，并据此对系统的安全等级进行评估。每个组织内部的系统管理者是一个典型事件。如果一个组织将上述一些操作外包给一个被管理的安全业务提供者（MSSP），则后者也充当一个管理者。

IT基础设施提供者：该职能负责为一个组织提供IT基础设施。基础设施包括网络连接和云服务，如软件即服务（SaaS），平台即服务（PaaS），以及基础设施即服务（IaaS）。IT基础设施提供者占有组织间网络信息；如网络拓扑信息和云服务规范。一个互联网业务提供商（ISP），应用服务提供商（ASP）以及云服务提供商（CSP）是典型实例。

应急小组：该职能负责监控和分析网络社会的各种事故，如非授权接入，分布拒绝服务（DDoS）攻击和钓鱼，并积累事故信息。基于这些信息，它可以实施反制措施，如封锁流量和在黑名单中记录钓鱼网站网址。MSSP内部的事故响应小组是一个典型实例。

协调者：该职能负责协调其他职责并根据已知的事故相关信息处理潜在的威胁。它与其他组织提供警报，并在一些情况下牵头开展合作补偿措施，处理毁灭性及大规模攻击，如DDoS攻击。CERT协调中心（CERT/CC），不论其是商业性的或非商业性的，都是一个典型实例。

研究者：该职能负责研究网络安全问题，包括漏洞环节和攻击，从研究中提取知识并积累。它通过记录者公开很多可重用信息，从而使个体组织可实施必需的反制措施。国际商用计算机公司（IBM）内部的X-force，小地球公司（Little eArth Corporation Co., Ltd.，LAC）网络空间风险研究所（RRICS），以及麦咖啡公司（McAfee Inc.）的麦咖啡实验室等都是典型的实例。

产品和业务开发者：该职能负责开发产品和业务，并积累相关信息，如版本，配置，漏洞及补丁。它负责通过记录者公布可重用信息，从而使单个组织可以与研究者一道实施必要的反制措施。软件销售和单个私人软件程序员是典型实例。

记录者：该职能负责分类，组织并积累研究者和产品及业务开发者提供的网络安全知识，从而使得知识能够被其他组织所重复利用。NIST和日本信息技术促进局是典型实例。在某些情况下，一个作为研究者或产品及业务开发者的实体也可能充当记录者并公布信息。

1.3 网络安全信息

基于操作域和职能，本节介绍操作必需的网络安全信息。考虑到每个所涉职责的信息，本实例模型定义四个数据库；用户资源，提供者资源，事故，和警告，以及三个知识库：产品和业务，反制措施，以及网络威胁。

1.3.1 用户资源数据库

用户资源数据库负责累积个体组织内部资产的信息，所含信息包括软件/硬件信息及其配置，资源利用状况，安全政策，包括接入控制政策，安全登记评估结果，以及内联网拓扑。它还包括个体用户组织使用的外部资源信息，如云业务订购列表（如数据中心和SaaS）及其使用记录。管理者控制此类信息。ARF和CRF可用于描述IT资产评估结果，而CVSS和CWSS得分可用于对IT资产安全登记进行打分。得分有助于管理者评估IT资产安全操作的紧急优先级。

1.3.2 提供者资源数据库

提供者资源数据库负责累积个体组织之外资产的信息。为开展有效高效的网络安全操作，数据库需要与用户资源数据库连接，这是因为内部和外部IT资产的边界变得越来越不清楚，特别是在云计算中。IT基础设施提供者控制此类信息。数据库主要包括提供者网络和云业务信息。提供者网络信息是指有关各个组织与其他组织之间相连接的网路的信息，如拓扑结构，路由信息，接入控制政策，流量状态，以及安全登记。云业务信息包括业务规程，工作负荷信息，以及各个云业务的安全政策信息。这里要注意的是针对用户组织的信息，如每个云业务的本地配置信息是储存在用户资源数据库中的。

1.3.3 事故数据库

事故数据库包含事故信息，其中此类信息的生成基于对用户资源数据库信息的分析。应急小组控制这些新消息。该数据库包括三类记录：事件记录，事故记录，以及攻击记录。

事件记录包含计算机事件信息，这包括分组、文件以及交易的信息。通常，计算机自动提供大部分记录，如计算机登录，比如当根用户登入一个系统时的登入时间和日期以及终端时间。这些登录数据是此类记录的实例。CEE可用于描述这些记录。

事故记录包含安全事故信息，并提供诸如用户系统当前状态和进一步威胁的信息。该记录来自对若干事件记录及其推测的分析，这些分析是自动或手动方式产生的。比如，当监测到一台计算机的接入过多时，计算机状态（过多接入一台计算机）及预期结果（业务拒绝）应在事故记录上记载。事故的危害性以及反制措施的必要性可通过该记录做出判断。这里要注意的是事故记录可能记载虚假事故；也即事故的初期调查认定为不是事故。事故目标描述交换格式（IODEF）可用于描述该记录。

攻击记录包含事故记录分析获得的攻击信息。它描述攻击的顺序；比如攻击是如何发起的，IT资产的哪个部分作为目标，以及攻击的损失是如何传播出去的。这里要注意的是该记录需要与事故记录相连接。

1.3.4 警告数据库

警告数据库包含网络安全警告信息。该信息设计用以提供给公众或特定组织使用。供公众使用的通常包含统计信息和提醒，而供特定组织使用的则包含为该组织量身定做的安全建议。信息的生成是基于事故数据库和网络威胁知识库的信息。协调者和应急小组控制此类信息。基于这些警告，用户组织可以采取对被警告网络安全风险的反制措施。

1.3.5 网络风险知识库

网络风险知识库负责累积网络安全风险信息。这些信息由研究者和产品及业务开发者提供，然后由记录者进行组织和分类。知识数据库包括漏洞和威胁知识库。

漏洞知识库：该知识库负责累积已知的漏洞信息，包括命名、分类和对已知软件和系统漏洞信息的列举。它也包括人类漏洞信息，这指的是人类IT用户可能出现的漏洞。国家漏洞数据库（NVD）和开放源漏洞数据库（OSVDB）是该数据库的现实例证，且CVE和CWE可用于描述知识库内容。

威胁知识库：该知识库负责累积已知网络安全威胁信息。它包括对知识库的攻击和误用。攻击知识库累积攻击信息，诸如攻击模式、攻击工具（如恶意软件）及其趋势。举例来说，趋势信息包括过往攻击在地理和攻击目标方面的趋势以及过往攻击的统计分析信息。CAPEC和MAEC可用于描述知识库的内容。

误用知识库负责累积误用信息，包括用户不正确使用（不论是善意还是恶意的）导致的误用信息。善意使用包括由于非故意视盲、误解造成的打印和识字错误，并被钓鱼陷阱抓住。恶意使用包括不遵守规定，如非授权业务使用和接入不该接入的资料。这里要注意的是，为简单起见，图7-1中忽略了攻击和误用知识库。

1.3.6 反制措施知识库

反制措施知识库负责累积网络安全风险的反制措施信息。该信息由研究者和产品及业务开发者提供，并随后由记录者进行组织和分类。知识库包括对知识库的评估和检测/保护。

评估知识库：该知识库负责累积已知的用于对IT资产安全等级进行评估的规则和标准、配置一览表，以及包括最佳实践在内的探索性步骤。CVSS/CWSS公式是评估安全登记最佳实践的两个最佳案例，并在该数据库中累积。除此外，XCCDF和OVAL可用于描述清单的规则，并可提供清单。

数据库的监测/保护：该知识负责累积已知的有关监测/保护安全威胁的规则和规定。除此之外，它也累积有关最佳实践等探索性尝试。

1.3.7 产品和业务知识库

产品和业务知识库负责累积产品和业务方面的信息。这些信息由研究者和产品提供，然后由记录者进行组织和分类。知识库包括版本和配置知识库。

版本知识库：该知识库负责累积产品和业务的版本信息，其中包括命名以及版本列举。在产品方面也包括安全补丁。CPE可用于列举通用平台。

配置知识库：该知识库负责累积产品和服务方面的配置信息。它包括命名，分类和对现有产品和业务配置的列举。在业务配置方面也包括业务使用指南。CCE也可用于列举产品的通用配置。

有关本实例模型的一些补充信息，可参照[b-Ontology]以及[b-ITU-T X.1500]的附录II。

附录II

描述数据库和知识库的规程

(本附录不构成本建议书的组成部分)

第7节用一系列网络安全规程介绍了七类信息，其中包括ITU-T X.1500兼容规程（如CVE 和 IODEF），如表1.1所示。因此，发现的网络安全信息的细节程度要遵守规程的细节程度。采用这种方法后，细节程度可以灵活，因此，可以为具体应用构建不同的规程。

表 II.1 – 支持实例模型的规程

域	KBs/DBs		规程
IT资产管理	用户资源DB		ARF, AI, CVSS/CWSS 得分
	提供者资源DB		---
事故处理	事故 DB		CEE, IODEF
	警告 DB		IODEF
知识积累	网络威胁KB	漏洞KB	CVE, CWE, CVRF
		威胁 KB	CAPEC, MAEC
	反制参数 KB	评估KB	CVSS/CWSS 公式
		检测/保护 KB	OVAL, XCCDF
	产品和业务KB	版本KB	CPE
		配置 KB	CCE
注 – DB: 数据库; KB: 知识库。			

附录III

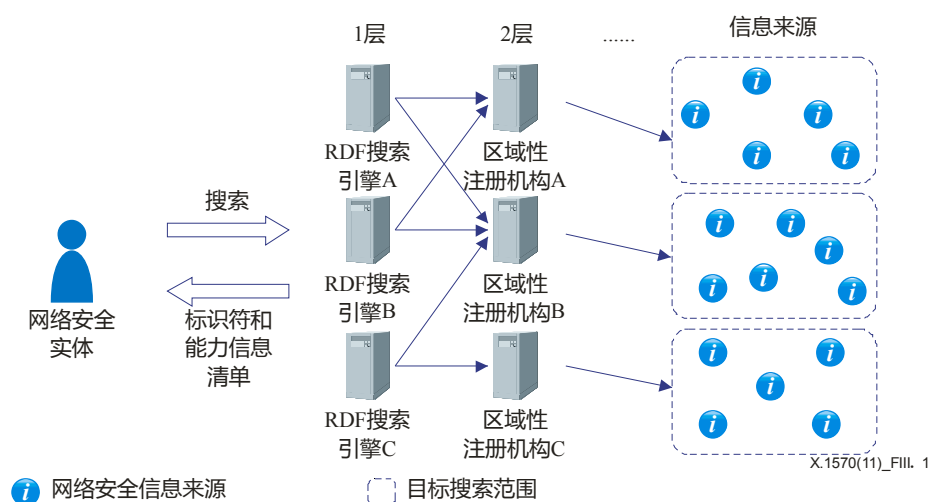
基于RDF发现的实施示例

(本附录不构成本建议书的组成部分)

III.1 基于RDF发现的实施示例

图9-1表明基于RDF发现的具体实施，发现代理和注册机构代理均置于RDF搜索引擎内。网络安全实体向RDF搜索引擎发送一个发现请求，后者返回身份及其能力清单。请注意，每一搜索引擎均具有不同的信息来源，这便是其搜索范围。

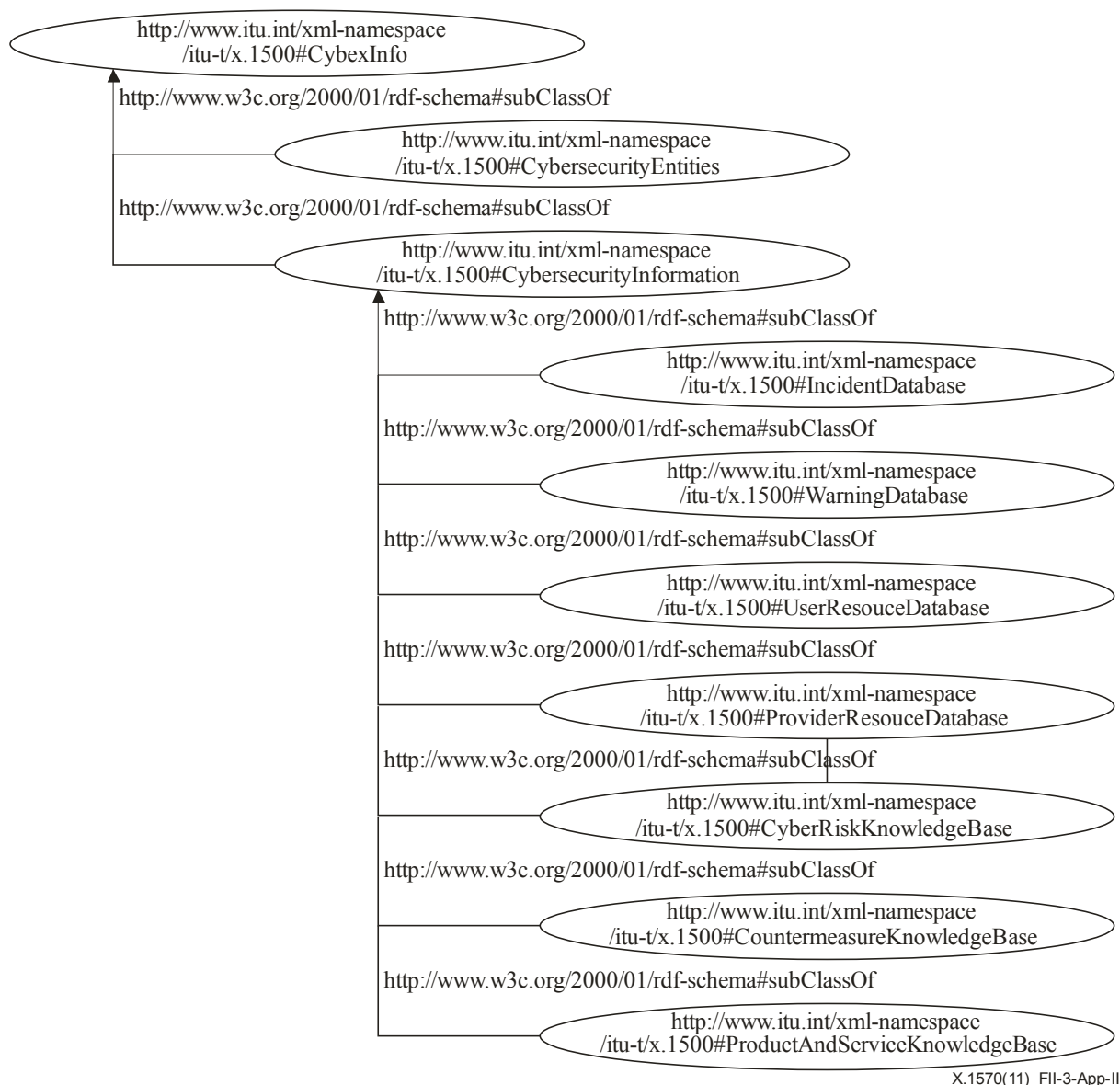
在实际应用环境中，为确保可扩展性，可按照图III.1所示对信息源进行分层登记和管理。第1层为与发现代理工作的单个RDF搜索引擎，第2层为区域性注册机构，如ARIN、RIPE或APNIC，同时可根据具体实施采用更多的分层。信息来源可以是CERT或任何其它网络安全实体。



图III.1 – 信息来源注册机构的分层

III.2 网络安全信息等级分层

图III.2所示为发现机制的等级分层。每一级均代表[b-ITU-T X.1500]附录II介绍的类别。有关每一类别的详情请参见上述建议书。请注意，本建议书使用了ITU-T确定的XML名空间[b-ITU-T X.1500]。



X.1570(11)_FIL-3-App-II

图 III.2 – 网络安全信息等级分层

注 – 图III.3中使用的.int顶级域名旨在举例，并非意在在实际工作中加以使用。

通常每一网络安全等级包括下列属性：

- entry_date: 存储数据输入/修改日期
- issuer_name: 存储发布者姓名（发布者可以是个人或公司）
- contact_email: 存储联系方的电子邮件地址
- resources: 存储标识符，如网络地址，以进一步找到资源
- Info_type: 存储信息种类，如，CVE、CWSS[b-CWSS]、CVSS[b-ITU-T X.1521]、OVAL[b-OVAL]、SCAP[b-SCAP]、XCCDF [b-XCCDF]、CPE[b-CPE]、CCE[b-CCE]和ARF。

搜索网络安全信息的任何一方都可在任何具体等级的单位中请求数据。搜索信息的标准包括等级名称、等级属性和最后修改日期及时间。

以下网站在线提供发现机制的实验性实施：<http://cybiet.sourceforge.net/>。

注 – 通过实施发现的网络安全信息的结构符合图7-1所述的实例模型。

参考资料

- [b-ITU-T X.1500] ITU-T X.1500建议书（2011年），网络信息安全交换技术。
- [b-ITU-T X.1500.1] ITU-T X.1500.1(2012)建议书，网络安全信息交换OID。
- [b-ITU-T X.1520] ITU-T X.1520建议书（2011年），常见漏洞和暴露（CVE）。
- [b-ITU-T X.1521] ITU-T X.1521 (2011)建议书，通用漏洞评分系统。
- [b-AI] NIST, *The Asset Identification*.
<<http://scap.nist.gov/specifications/ai/>>
- [b-ARF] *Assessment Results Format*
<<https://measurablesecurity.mitre.org/incubator/arf/>>
- [b-CCE] *Common Configuration Enumeration*.
<<https://cce.mitre.org/>>
- [b-CPE] *Common Platform Enumeration*.
<<https://cpe.mitre.org/>>
- [b-CWSS] *Common Weakness Scoring System*.
<<https://cwe.mitre.org/cwss/>>
- [b-Gruber] Gruber T.R. (1993), *Toward principles for the design of ontologies used for knowledge sharing*. International Journal of Human-Computer Studies, Vol. 43, Issues 4-5, November 1995, pp. 907-928.
- [b-Ontology] Takahashi T., Kadobayashi Y., Fujiwara H. (2010), *Ontological Approach toward Cybersecurity in Cloud Computing*, International Conference on Security of Information and Networks (SIN), September 2010.
- [b-OVAL] *Oval – Open Vulnerability and Assessment Language*.
<<https://oval.mitre.org/>>
- [b-SCAP] *Security Content Automation Protocol (SCAP)*.
<<http://scap.nist.gov/>>
- [b-XCCDF] *XCCDF – The Extensible Configuration Checklist Description Format*
<<http://scap.nist.gov/specifications/xccdf/>>

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