国 际 电 信 联 盟

ITU-T X.1500

(04/2011)

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

网络安全信息交换 – 网络安全概述

网络安全信息交换概述

ITU-T X.1500建议书

ITU 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	
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。

ITU-T X.1500建议书

网络安全信息交换概述

摘要

ITU-T X.1500建议书阐述了交换网络安全信息的技术。这些技术可随意或酌情单独使用或综合使用，以通过协调、综合、全面及时和有保障的信息交换增强网络安全。表示没有义务交换信息，这并非意味着信息交换和捕获或最终对经处理的信息的使用必不可少。网络安全信息交换（CYBEX）是提供ICT使用中的信任和安全因素之一。

沿革

版本	建议书	批准日期	研究组
1.0	ITU-T X.1500	2011-04-20	17

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

引言

本建议书旨在实现可调整性、可扩展性和非强制性，以便使多种技术（一些技术不断演进并处于不同完成阶段）用于不同情形，从而增强电信/ICT基础设施、设备和服务的网络安全信息交换。随着技术的进步，本建议书将定期修改，相关技术将作为ITU-T X.1500系列建议书出版。

我们希望本建议书所包含的技术能使包括计算机事件应急小组（CIRT）电信ICT机构在内部和相互之间：

a) 拥有促成真正加强全球电信/ICT设施和服务的保密性、完整性和可用性的决策和行动信息；

b) 拥有促进形成安全合作流程和控制的信息，提高各机构之间信息交换的保证水平；

c) 促成以统一的方式全面管理和交换网络安全信息；

d) 提高安全意识并加强合作以减少网络威胁、攻击和恶意软件。

上述技术包括：

- 用于交换的结构性网络安全信息；
- 确定并发现网络安全信息和实体；
- 在交换实体之间建立信任和政策协议；
- 要求网络安全信息并做出回应；
- 确保网络安全信息交换的完整性；

这些技术分为以下各集群：

- 缺陷、漏洞和状态；
- 事件、事故和试探；
- 信息交换政策；
- 标识、发现和查询；
- 身份保证；
- 交换协议。

ITU-T X.1500建议书

网络安全信息交换技术概述

1 范围

本建议书介绍了网络安全信息交换（CYBEX）模型并探讨了可用来促进网络安全信息交换的技术。这些技术可随意或酌情单独使用或综合使用，以通过统一、综合、全面、及时和有保障的信息交换增强网络安全。这并非意味着信息交换和捕获的方法或最终对所处理信息的使用必不可少。上述技术包括对网络安全信息的全面结构性发现和互操作性，在不断演进中考虑到多个网络安全论坛开展的重要活动和规范进展。CYBEX提供ICT使用的信任和安全的因素之一。

本建议书包括以下可以单独或酌情综合使用的功能：

- 用于交换的结构性网络安全信息；
- 确定并发现网络安全信息和实体；
- 在交换实体之间建立信任和政策协议；
- 要求网络安全信息并做出回应；
- 确保网络安全信息交换的完整性。

根据已达成一致的政策和适用法律和规定，获取信息的手段以及对信息的使用不在本建议书范围之内。一些具体的国内和区域性规定和立法可能要求实施保护个人可识别信息的机制。本建议书对所含技术及相关网络安全信息的交换没有强制性。

2 参考文献

无。

3 定义

3.1 他处定义的术语

本建议书使用了下列他处定义的术语。

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：可用性、完整性（其中可能包括真实性和不可否认性）。

注 – 一些国家的具体规定和法律可能要求落实保护个人可识别信息的机制。

3.1.2 **安全事故** [ITU-T E.409]：任何可以威胁到某些安全方面的不良事件。

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 **保证**：对流程和成果实现规定特性或目标的信任水平。

3.2.2 **交换协议**：有关两个或多个实体之间进行信息交换的一套技术规则和格式。

3.2.3 **信息交换政策**：有关网络安全信息使用和共享的条款和条件。

3.2.4 **系统状态**：系统或实体的当前状态，包括其配置、内存使用情况或其他与网络安全相关的数据信息。

3.2.5 **漏洞** (与 [b-ITU-T X.800]一致)：可能被利用来破坏系统或它包含的信息的任何缺陷。

3.2.6 **缺陷**：缺点或缺陷，本身不被认为是一个漏洞，可以在某些时候成为一个漏洞，或可能有助于引进其他漏洞。

4 缩写词和首字母缩略语

本建议书使用以下缩写词和首字母缩略语：

ARF 评估结果格式或资产报告格式（根据上下文）

BEEP 块可扩展交换协议

CA 认证机构

CAPEC 通用攻击模式列表和分类

CCE 通用配置列表

CEE 通用事件表达格式

CEEE 通用事件表达格式交换

CIRT 计算机事件响应小组

CPE 通用平台列表

CVE 通用漏洞和披露

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

CYIQL 网络安全信息查询语言

DDoS 分布式拒绝服务

EVC 扩展认证证书

EVCERT 扩展认证证书

HTTP 超文本传输协议

IC 集成电路

ICT 信息通信技术

IDS 入侵检测系统

IODEF 事故对象描述交换格式

IPS 入侵预防系统

IT 信息技术

MAEC 恶意软件属性列表和特性

OID 对象标识符

OS 操作系统

OVAL 开放漏洞和评估语言

RID 实时网络间防护

SCAP 安全内容自动化协议

SOAP 简单对象接入协议

TLP 交通灯协议

TLS 传输层安全

TNC 可信网络连接

TPM 可信平台模块

XCCDF 可扩展配置清单描述格式

5 惯例

当本建议书在一般意义上的使用术语“标准”时，应解释为包括：标准、规范和建议书。

6 基本概念 – 网络安全信息交换（CYBEX）技术

该网络安全信息交换（CYBEX）技术建议书旨在实现一个简单而有限的目标 – 描述了网络安全实体可交换有保障的网络安全信息的技术，使用的方法提供适当水平的保证。这些实体通常包括机构、个人、设备或处理或寻求网络安全信息的流程。通常，这些实体为CIRT和设备、软件或网络系统的运营商或厂商。

网络安全信息交换有益于加强网络安全和基础设施保护，有助于CIRT完成各项主要功能。

网络安全信息的交换可根据事先达成一致的政策，在公众域范围内，在遵循需要知晓原则的高度分割的可信社区内进行。有关威胁、漏洞、事故、风险和缓解及相关救治的知识是各实体之间交换的典型网络安全信息类别。本建议书所含相关技术旨在促进这种信息交换并由此加强网络安全。

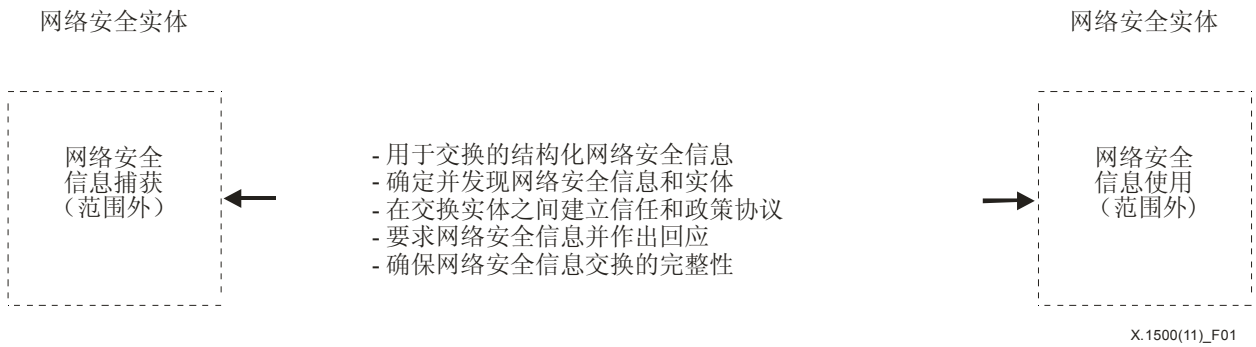


图1 – CYBEX模式

图1 所示本建议书使用的一般性网络安全信息交换模式包括可单独使用或酌情联合使用并按需求扩展的基本功能，从而促进有保障的网络安全信息交换。这些功能包括：

- 用于交换的结构化网络安全信息；
- 确定并发现网络安全信息和实体；
- 在交换实体之间建立信任和信息交换政策协议；
- 要求网络安全信息并做出回应；
- 确保网络安全信息交换的完整性；

本建议书第7节描述了完成上述功能的技术。

网络安全信息交换可以双向进行。这种双向性可以就认证的信息提出要求并做出回应，从而促进各方所需要的保证水平的实现或提供交付证书。

根据已达成一致的政策和现行法律和规定、获取信息的手段以及使用的信息不在本建议书范围之内。举例而言，一些专用网络安全信息交换实施手段，如对攻击源的追溯可能需要具体的应用机制，以便为获得所需要的信息提出一系列反向请求并做出回应。然而，其他实施，如通过使用安全自动化能力衡量和管理网络安全在本建议书的范围之内。这类和他类使用案例可通过本建议书所含的技术得到加强。本建议书对所含技术及相关网络安全信息的交换不具强制性，其他技术亦可酌情使用。

7 结构性网络安全信息交换技术

为保证任何两个实体之间的网络安全信息交换，必须以双方实体明白的一致方式组织和描述信息。CYBEX的目标是使包含“通用列表”（为同一数据类型按顺序列举的规范信息）的网络安全信息的交换更加容易。通用列表使分布式数据库和其他能力结合起来，方便进行与网络安全相关的比较。

为实现交换目的，网络安全信息包括结构化信息或知识：

- 与网络安全，尤其是漏洞的设备、软件或基于网络的系统 “状态”；

- 有关的事故或事件的取证；
- 从经历的事件中获得的试探和明显特征；
- 所涉及的网络安全实体；
- 网络安全信息交换，包括模块、架构、条款及条件和分配的编号；
- 所有网络安全信息的身份和保证属性；
- 实施要求、指导原则和做法。

为总体地描述网络安全信息交换所需要的特性，结构性信息能力按照不同的网络安全信息交换集群分为六个技术“集群”，分别为：

- 缺陷、漏洞和状态；
- 事件、事故和试探；
- 信息交换政策；
- 标识、发现和查询；
- 身份保证；
- 交换协议。

这些分集群属于广义分类，各集群中的能力可能根据使用情况在一个或多个其他集群中使用。

上述所列各集群的详情见以下子节。对各集群的描述概括了其在CYBEX中的作用并列出了实现的技术。所确定的技术不具有强制性，相反，它们仅被认为是与相关各集群目标相符的技术。处理方式的选择主要与“所有者”用户社区的专业化水平和通过植入所获得的各种收益相关。

本建议书的CYBEX技术确定了实现和促进上述及其他情形的一系列补充技术。

本节其余部分和相关的附录I阐述了各集群的情况，包括CYBEX内各集群的总体作用并列举了实现各集群的技术。这些参考资料为非规范性文件，详情见参考资料。

各集群技术的实施者和使用者须遵守所有现行国家和区域性法律、规定和政策。

7.1 缺陷、漏洞和状态 – 集群交换

与缺陷、漏洞和状态交换集群相关的能力支持缺陷和漏洞信息的交换和评估系统和应用的状态。

表I.2列举了代表可以支持交换缺陷、漏洞和状态信息类型的能力。

7.2 事件、事故和试探 – 交换集群

与事件、事故和试探交换集群有关的能力支持对已发现的事件、事故或试探结果的信息交换。

表I.2列举了在计算机事件应急小组（CIRT）和其他各方之间的结构化方式中，代表可以便于交换已发现的事件、事故或试探信息类型的能力。创建应对攻击的手段并减少缺陷和漏洞。

7.3 信息交换政策 – 交换集群

与信息政策交换集群相关的能力支持实体之间就共享信息条件和条款的网络安全信息进行的共享和使用。这种理解可与共享的具体信息挂钩，或与其所属的更宽类别信息挂钩或与相关实体关联。在必要的情况下，最好能够将这些政策通报相关实体。该通知可采取多种形式并与相关信息同时传送或通过查询响应机制单独提供。

表I.3列举了代表可便于网络安全实体之间交换政策信息类型的能力表。请注意，信息政策交换的协议和要求在信息安全交换论坛中层出不穷，因此应谨慎行事确保适当实施。

7.4 标识、发现和查询集群

与识别、发现和查询集群相关的能力支持识别、发现和查询过程。

网络安全社区在网络安全标识符及其创建、管理、发现、认证和使用上具有共同的利益，其中一些包括：

- 增强网络安全信息的价值，实现事件相关信息和分析在长时间内的广泛交换。
- 加强网络安全信息交换，实现为认证而获取的标识符信息和相关政策。
- 加强网络安全信息交换的灵活性，使新的和获得的与消息相关的额外信息得以实现，如信息状态。

不同网络安全机构可能希望为捕获和交换数据状态、漏洞、事故取证和事故试探信息实施通用的网络安全协议。由于该信息来源不同，实施者应统一确认网络安全机构、信任和信息交换政策的方法以及交换和发布的信息本身。可能有必要建立网络安全信息交换使用的全球统一标识符，这意味着它具有以下特点：

- 简单、方便使用、灵活、可扩展、可延长并可部署；
- 不同标识符方案的分布式管理；
- 标识符注册机构的长期可靠性、用来发现与任何给定标识符相关的信息的高性能工具的可用性

表I.4列举了代表可便于发现网络安全机构并发现和查询网络安全信息过程的各种类型的能力表。

7.5 身份保证集群

与身份保证集群相关的能力支持身份保证。

在CYBEX内，结构信息的实际交换可采取多种方式 – 通过网络或物理传输。这种交换的一个关键因素就是信任 – 对各方身份的信任以及所传输的信息的信任。

表I.5列举了代表可支持身份保证的各种类型的能力。

7.6 交换协议集群

交换协议集群内的能力包括可用于不同的网络安全信息交换上下文中的交换协议。信息的安全的交换需要组合下面列出的协议。实时网络间防范（RID）提供消息沟通框架，以交流事件的资料和信息相关的政策。任何封装IODEF（以及IODEF的扩展）事件文件的RID的消息的传输协议，包括列出的BEEP、SOAP和HTTPS传输选项，或未来开发的协议。RID包括安全性和保密性考虑以便从传输中将消息传送分离出来。

表I.6列举了代表可作为信息交换的交换协议的类型的能力。

附录I

网络安全信息交换技术

（本附录不是建议书的组成部分）

表 I.1 – 缺陷、漏洞和状态交换集群中的技术

技术	描述	参考文献
通用漏洞和披露（CVE）	通用漏洞和披露是确定和交换信息安全漏洞和披露的方法，旨在为众所周知的问题提供通用标识符。CVE的目的是使跨不同漏洞能力（工具、数据库和服务）的数据分享更加容易。CVE旨在允许漏洞数据库和其他资源相结合，方便各种安全手段和服务的比较。据此，CVE不包含诸如风险、影响、补救信息或详细的技术信息等资料。CVE仅包含具有状态指示、简单描述和与相关漏洞报告和建议的引证的标准标识号码。CVE的目的是使所有众所周知的漏洞和披露得到理解。虽然CVE包含成熟信息，其重点在于确定由安全工具发现的漏洞和披露并确定任何已知的新的问题，然后，解决任何需要认证的原有安全问题	[b- ITU-T X.1520]
通用漏洞评分系统（CVSS）	通用漏洞评分系统流程为通报ICT漏洞的特点和影响提供了一个开放式框架。CVSS包含三个集群：基础、临时和环境。各集群生成一个从0至10的数字分数和一个矢量，即反映用来推导评分价值的压缩文本表示法。基础组代表漏洞的内在质量。临时组反映随时变化的漏洞的特性。环境组代表与用户环境挂钩的漏洞特点。CVSS使ICT管理人员、漏洞公报提供者、安全厂商、应用厂商和研究人员通过使用ICT漏洞通用评分语言获得所有好处。	[b- ITU-T X.1521]

表 I.1 – 缺陷、漏洞和状态交换集群中的技术

技术	描述	参考文献
常见缺陷列表（CWE）	常见缺陷列表是为确定和交换统一可衡量软件缺陷集的流程。CWE有助于更有效地讨论、描述、选择和使用可以在源代码和操作系统中寻找到这些缺陷的软件安全工具和服务。它还有助于更好地理解和管理与架构和设计相关的缺陷。CWE的实施和更新是通过来自业界、学术界和政府机构的国际专家组进行的，确保其内容的深度和广度。CWE提供标准化技术，使服务提供商将具体潜在的缺陷通知用户并提出解决方案，使软件购买者对不同厂商提供的相似产品予以比较。	[b-CWE]
常见缺陷评分系统（CWSS）	常见缺陷评分系统为通报软件缺陷的特点和影响提供了一个开放式框架。	[b-CWSS]
开放漏洞和评估语言（OVAL）	开放漏洞和评估语言是一项国际规范，旨在促进开放并向公众提供安全内容并使信息在通过各种安全手段和服务的传输标准化。OVAL包括用来对系统详情进行编码的语言和整个社区内接不同内容分类的数据库。语言对评估流程的三个主要部分进行标准化：为测试显示系统配置信息；为显示具体机器状态分析系统（漏洞、配置、补丁状态等）并报告该评估的结果。数据库是对使用该语言的公众可获取的开放内容的收集。 用XML编写的OVAL方案的开发用作OVAL语言的框架和词汇表。这些方案对应于评估流程的三个步骤：用于表示系统信息的OVAL系统特性方案，表示具体机器状态的OVAL定义方案以及用于报告评估结果的OVAL结果方案。	[b-OVAL]
扩展配置清单描述格式（XCCDF）	扩展配置清单描述格式是编写安全检查列表、基准和相关文件类型的规范语言。XCCDF文件代表一些目标系统集安全配置规则的结构性收集。该规范旨在支持信息交换、文件生成、组织和状态适应、自动合规测试和合规评分。该规范还确定了存储基准合规测试结果的数据模式和格式。XCCDF的目的是为表述安全检查列表、基准和其他配置指南提供统一的基础并由此促进更广泛的应用良好的安全做法。XCCDF文件用XML表述。	[b-XCCDF]

表 I.1 – 缺陷、漏洞和状态交换集群中的技术

技术	描述	参考文献
通用平台列表（CPE）	通用平台列表（CPE）是确定和描述企业计算机资产库存中软件系统和硬件设备的标准化方法。CPE提供了：命名规范，包括结构完好的CPE名称逻辑结构以及用于将这些名称与机器可读编码捆绑和解绑的程序、匹配规范（定义了比较CPE名称以确定是否针对一些或全部相同产品或平台的程序）、字典规范（定义了标识符字典概念并为字典管理者规定了高层规则）。	[b-CPE]
通用配置列表（CCE）	通用配置列表提供了有关系统配置问题的独一无二的标识符，以便促进快速和准确地将多个信息源和工具的配置数据相关起来。举例而言，CCE标识符可用来将配置评估工具中的相关核对项目与配置最佳做法文件中的声明关联起来。	[b-CCE]
评估结果格式（ARF）	评估结果格式（ARF）是一个开放性规范，为在评估工具、资产数据库和其他管理资产信息的产品之间交换各设备评估结果提供了结构化语言。该格式旨在用于收集详细的IT资产配置数据的工具。ARF还包括综合报告规范，以报告多资产的信息，它还包含任务和查询语言以查询评估结果。安全自动化规范描述了向数据存储提供评估内容的端对端流程，要求按照内容进行评估，报告评估结果并汇总企业评估结果	[b-ARF]

表I.2 – 有关事件、事故和试探交换集群的技术

技术	描述	参考文献
通用事件表达格式（CEE）	通用事件表达格式是描述、登录和交换计算机事件的标准化方法。通过使用CEE通用语言和语句、企业登录管理、相关、综合、审计和事故处理可得到更加有效地执行并获得更好的结果。这项工作的主要目的是对电子系统的日志显示和交换进行标准化。CEE将日志记录和交换分为四（4）个组成部分：事件分类、日志语句、日志传输和登录建议。	[b-CEE]

表I.2 – 有关事件、事故和试探交换集群的技术

技术	描述	参考文献
事故对象描述交换格式（IODEF）	事故对象描述交换格式定义了一种数据表示方法，为CIRT通常交换的有关计算机安全事故的信息提供了框架。IODEF描述了一个信息模型，提供了使用XML方案确定的相关数据模型。	[b-IETF RFC 5070]
钓鱼、欺诈和滥用格式	钓鱼、欺诈和滥用交换格式扩展了事件对象描述交换格式（IODEF），以便对钓鱼、欺诈和其他类型的滥用报告提供支持。这些延伸还支持交换有关普遍的垃圾信息事故情况。这些扩展使用灵活，得以支持在整个电子欺诈或垃圾信息周期活动中出现的信息。由于可以综合多重事故，它可以进行简单的报告和完整的取证报告。 注 — 本建议书仅描述了通常理解的技术，确保网络安全实体交换网络安全信息的手段，不包含对该信息的使用。	[b-IETF RFC 5901]
常见攻击模式列表和分类（CAPEC）	CAPEC是标识、描述攻击模式并予以编号的规范方法。攻击模式是捕获和通报攻击者情况的有利机制。这些描述是使用软件的常见方法。描述源于破坏性，而不是建设性环境中采用的设计模式概念并来自于对具体现实世界使用事例的深层分析。CAPEC的目标是提供一个公众可获取的攻击模式目录以及全面的XML方案和分类法。	[b-CAPEC]
恶意软件属性列表及特性格式	恶意软件属性列表和特性格式（MAEC）是一种规范语言，包含为通用列表属性和行为词汇提供语句并为有关这些数据元素的结构信息提供互换格式的方案。列表的抽象水平不同：低层行动、中层行为和高层机制。在最低一层，MAEC描述了与基本功能相关的属性和恶意软件的低层运行。在中层，MAEC语言为确定中层行为将上述低层行动组织成各组。在更高的概念层，MAEC词汇可以建设根据更高级分类的成就而提取中层恶意软件行为集群的机制。	[b-MAEC]

表I.3 – 有关政策交换集群的技术

技术	描述	参考文献
交通灯协议（TLP）	交通灯协议（TLP）的创建用来鼓励对敏感信息的更广泛共享。发起方说明其希望信息传送的范围。TLP提供一种实现上述目标的简单方法。该协议旨在改进个人、组织或社区之间以受控和可信的方式流动信息的方法。TLP基于发起方使用四种颜色之一为信息加注标签的理念以说明接收方可进行的进一步信息传播。接收方在需要进一步传播的情况下必须与发起方磋商。TLP被30多个国家接受为安全社区可信信息交换模式。四种用来处理敏感信息的“信息共享级别为： 红色 – 个人信息。该信息仅用于命名接收方。例如，在会议中，红色信息仅限于与会者。在多种情况下，口头或亲身传送红色信息。 琥珀色 – 有限发布。接收方可在其机构内与其他人共享琥珀色信息，但只能在“需知晓”的基础上进行。 绿色 – 社区范围内。该类别的信息可在某一社区广泛传送。然而，该信息不得在互联网上发表或公布或在社区以外公布。 白色 – 无限制。根据标准版权规则，白色信息可自由传播，没有限制。	[b-TLP]

表I.4 – 有关标识、发现和查询集群的技术

技术	描述	参考文献
网络安全信息交换中的发现机制	这些技术包括可用来发现并定位网络安全信息来源、网络安全信息类别、具体的网络安全信息状况的方法和机制、获取网络安全信息的方法以及可用来接入网络安全信息的政策。	
用于网络安全信息交换的OID弧的管理指南	该指南描述了通用网络安全标识符命名空间以及管理要求，作为OID弧的一部分并包括以下标识符： • 网络安全信息 • 网络安全机构 • 网络安全政策	
网络安全信息查询语言	网络安全信息查询语言定义了灵活的数据表示方式，为查询计算机事件响应小组（CIRT）通常交换的有关计算机安全事故的信息提供了框架。该规范描述了有关CYIQL的信息模型，使用XML方案提供了相关数据模型。	

表I.5 – 有关身份保证集群的技术

技术	描述	参考文献
可信平台	具有嵌入式可信平台模块（TPM）的计算和通信产品提高了企业、机构、政府部门和消费者进行可信信息交换的能力，因此，TPM与多数CYBEX实施相关。TPM是内置于多种平台的专用集成电路（IC），以便更有利地实现用户认证和机器确认 – 是防止不适当获取保密和敏感信息并保护网络免受损坏必不可少的方式。 可信平台模块技术基于开放式标准，确保混合厂商环境中不同产品的互操作性。广泛使用的TPM标准包含一套可信计算组（TCG）开发和维护规范以及有关按照通用标准评估安全的保护概要文件。 设计原则给出了TPM的基本概念和有关TPM功能的一般性信息。TPM设计人员必须审议并实施TPM主要规范（1-3部分）中的信息并为指定平台审议与平台相关的文件。与平台相关的文件包含规范性说明，影响到TPM的设计和实施。TPM设计人员必须审议并实施要求，其中包括TCG合规性工作组确定的测试和评估要求。TPM必须符合要求并通过合规性工作组的评估。TPM可经过更多的严格测试和评估。	[b-TPM]
可信网络连接	ICT安全运作通常希望发现操作系统（OS）的状态 – 支持网络所使用的应用软件。举例而言，当系统缺少OS安全补丁或防病毒签名时，可靠的通知对于应对网络攻击造成的破坏至关重要。做出评定需要可靠的信息，即连接系统处于特别状态之中。 为防止系统（如被黑客系统）误导信息，成功地评估需要硬件基础，可信平台内置于硬件之中以记录一些有关启动程序的事实并以数字签名的方式加以传送。此外，主要芯片厂商目前正在使用“延迟发射”能力补充可信平台，允许在启动序列中延迟执行可信代码。这样可使事件在硬件启动程序后可靠地得到记录。 网络配置管理是对系统认证部署的有效实施：企业设备上的软件代理定期向中央数据库发送配置报告，评估非合规系统并贴注标签。这些软件代理提供的数据尽管宝贵，但很容易被攻击者修改。使用广泛部署的可信平台，可实现更令人信任的系统状态评估，从而大大加强企业对其配置管理数据的信心。 可信网络连接（TNC）是有关网络接入控制的开放架构，其目的是使网络运营商在每个网络连接点提供终点集成，从而在多厂商网络终点实现互操作性。	[b-TNC]

表I.5 – 有关身份保证集群的技术

技术	描述	参考文献
实体认证保证	该标准为管理实体身份保证提供了认证生命周期框架及其相关身份信息。具体而言，它提供了以下方法1) 量化衡量并分配实体身份及其相关身份信息的保证水平；2) 通报相关认证保证级别	[b-NIST EAA]
扩展认证证书框架	扩展认证证书框架包括对技术、协议、身份证明、生命周期管理和审计做法（描述发布和获取扩展认证证书（“EV证书”）的最低要求）的综合技术。该框架包含广泛的安全、本地化和通知要求。	[b-EVCERT]
发布公共密钥证书的认证机构的政策要求	所规定的文件确定了与发布公共密钥证书（包括扩展认证证书（EVC）的认证机构（CA））的政策要求。它定义了有关发布和管理证书的认证机构的运行和管理要求，使用户、CA认证的对象和依赖方在支持加密机制中对证书的使用充满信心。	[b-ETSI TS 102 042]

表I.6 – 有关交换协议集群的技术

技术	描述	参考文献
实时网络间防范 (RID)	实时网络间防范 (RID) 为事件信息的交换提供了一个框架。RID标准提供了一套在实体之间安全交流IODEF文件所必须的事件协调消息。RID为 IODEF 文件，包括扩展的IODEF包装。标准的消息和交换格式包括全球性事件协调计划中必须的安全、隐私和政策选择/考虑。RID是IODEF和文件传输协议之间的安全层。由交流事件信息的实体决定所选择的传输。传输可以是指定的RID传输(HTTP/TLS)、BEEP、SOAPAK或在未来指定的协议。	[b-IETF RFC 6045]
实时网络间防范（RID）消息的传输	该机制规定了实时网络间防范（RID）消息在通过TLS传送的HTTP请求和响应消息中的传输。	[b-IETF RFC 6046]
用于CYBEX的块可扩展交换协议（BEEP）概要文件	CYBEX信息交换技术BEEP概要文件规定了在CYBEX内使用的BEEP概要文件。BEEP是RFC3080所描述的面向连接的异步互动通用应用协议核。在BEEP核中有一个成帧机制，可以在同类之间进行同步和独立信息交换。所有交换发生在一个信道中 – 与定义完好的应用方面相结合，诸如传输安全、用户认证或数据交换。各信道具有相关的“概要文件”，确定所交换信息的语句和语义。	[b-IETF RFC 3080]
CYBEX简单对象接入协议（SOAP）	SOAP是非集中、分布式环境中信息交换的轻量协议。它是基于XML的协议，包含三个部分：确定阐述消息内容和如何处理的框架包封，一套表述应用确定的数据类型的编码规则和代表远程程序呼叫和响应的惯例。SOAP可与多种其他协议综合使用，但是，只有本文件规定的结合点阐述了如何将SOAP与HTTP和HTTP扩展框架联合使用。	[b-W3C SOAP]

附录II

网络安全信息交换实例

（本附录不是本建议书的组成部分）

附录II提供了一个网络安全信息交换实例。它显示了CYBEX的运行环境以及有效的网络安全生态系统的产生。从报告、测试和经验中获取的知识用来产生并发展缺陷和漏洞信息，结合系统状态信息衡量并增强安全。

该附录包含CYBEX实例，定义了以下术语：

1) **网络安全运作**：用来监测和管理符合以下运行限制的方法和流程：
   - 可能影响安全的信息收集和分析。
   - 对安全造成不良影响或由此确定可能会对未来造成不良影响的行为或事件的发现。
   - 因所发生的不良行为或事件采取的行动，以便限制、缓解并/或防止未来事故的发生。
   - 有关系统状态和条件的安全通信。
2) **网络安全实体**：作为网络安全信息交换组成部分的实体，包括信息对象本身。
3) **网络安全运行信息**：网络安全实体运行网络安全所需要的任何信息。

CYBEX中描述的网络安全技术在CYBEX实例中得到进一步有益的阐述。这是一个阐述网络安全运行抽象世界的模型。该实体包括类型集、属性和关系。见图II.1。实线表示信息类型之间的关系，箭头则表示从功能实体向知识库/数据库的信息输入。右边的功能实体为一般性实体，CIRT等实体可完成一个或多个上述功能。

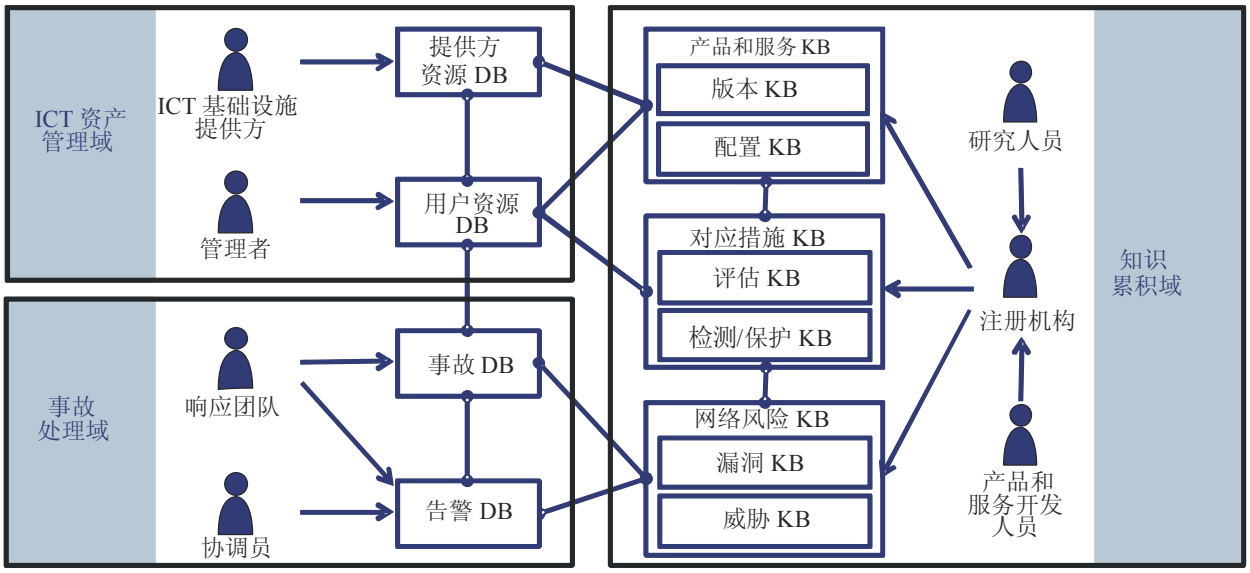


图 II.1 – CYBEX实例模型

在此实例中，模型用来定义网络安全运作域，然后用来确定所需要的支持各域运作的网络安全实体。以下子节将推导出详细的实例。这些实例显示出CYBEX技术是如何用来支持该实例的。

II.1 运作域

网络安全运作主要包含三个域：事故处理、ICT资产管理和知识累积。

事故处理域包括通过监测事故、构成事故的计算机事件和在事故中发现的攻击行为对事故的检测和响应。举例而言，该域通过检测器告警检测到异常行为，之后，通过收集各种日志获得详情。有时，该域提供告警和建议，如针对用户机构可能受到的威胁发出早期预警。

ICT资产管理域包括各用户组织内的网络安全运作，包括机构中ICT资产的安装、配置和管理。它包括事故防范域以及各组织的损坏控制运作。

知识累积域包括与网络安全相关的信息，生成并累积可重新用于其他组织的知识。

II.2 网络安全实体

基于上述运作域，可在各域中确认运行网络安全必不可少的网络安全功能实体。

在事故处理域中，共有两个运作实体：响应团队和协调员。响应团队是监测和分析各类事故（如非授权接入、DDoS攻击和钓鱼）并对此予以分析的实体，同时收集事故信息。根据该信息，响应团队可实施应对措施，如将钓鱼网址注册在黑名单中。协调员是与其他实体协调的实体，根据已知事故信息应对可能的威胁。

在ICT资产管理域中，有两个运行实体：管理者和ICT基础设施提供方。管理者管理其组织系统并掌握有关自身ICT资产的信息。各组织内的ICT管理者就是典型的例子。ICT基础设施提供方为各组织提供ICT基础设施，包括网络连接、云计算服务（如作为服务的软件（SaaS）、作为服务的平台（PaaS）和作为服务的基础设施（IaaS））以及身份服务。互联网服务提供商（ISP）和应用服务提供商（ASP）就是典型的例子。

在知识累计域中，共有三个运作实体：研究人员、产品和服务开发人员和注册机构。研究人员研究网络安全信息，提取并累计知识。产品和服务开发人员拥有有关产品和服务的信息，如名称、版本、漏洞、补丁和配置信息。软件厂商、ASP和各软件程序员就是典型的例子。注册机构是一个将研究人员、开发人员和厂商提供的网络安全知识进行分类和组织的实体，使其他组织得以使用上述知识。

II.3 网络安全运作信息

该子节以运作域和实体为基础介绍了各运作域中功能实体提供的网络安全运作信息。

II.3.1 事故处理域

在事故处理域中，有事故数据库和报警数据库。事故数据库包含有关应急团队提供的事故信息，它包括三种记录：事件、事故和攻击。事件记录包括登入系统的优先用户计算机事件，它还包括与事故相关的数据包、文档和交易信息。通常，多数记录是由计算机自动提供的。事故记录包括可能造成事故的事件。该记录通常从若干事件记录及其相关内容中推导得出，这些内容自动并/或手动生成。攻击记录基于对事故的分析并包括攻击的具体日期和时间及其发生序列。

告警数据库包括有关应急团队和协调员提供的网络安全告警信息。这些告警基于事故数据库以及网络风险知识库。

II.3.2 ICT资产管理域

在ICT资产管理域中有两个数据库：用户资源数据库和提供方资源数据库。

用户资源数据库累积各组织内资产信息并包含诸如软件、硬件及其配置清单、资源使用状况、包括接入控制政策在内的安全政策、安全水平评估结果和内联网拓扑等信息。这些信息是由网管提供的。

提供方资源数据库累积有关各组织以外的资产信息。它主要包括外部资源信息和外部网络信息。外部资源信息包括有关各组织在其组织外正在使用的资源信息，如外部云服务（如数据中心和SaaS）的清单和状况。外部网络信息包括有关将各组织连接到其它组织的网络信息，如拓扑、路由信息、接入控制政策、流量状况和安全水平。这些信息是由ICT基础设施提供方提供的。

II.3.3 知识累积域

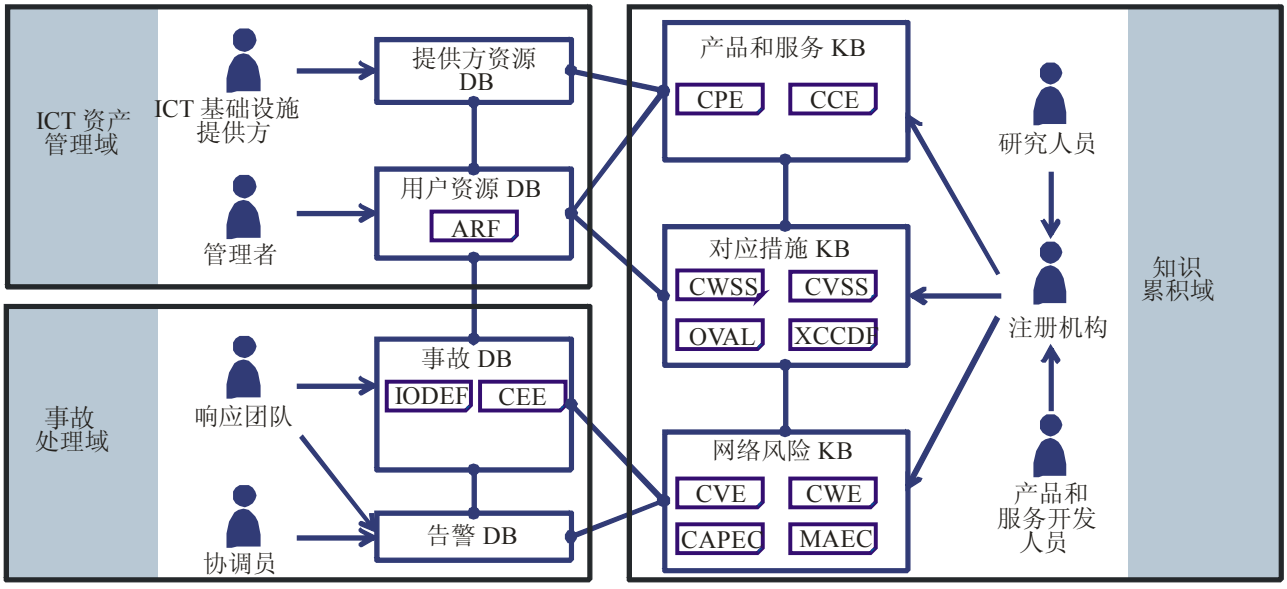
知识累积域中存在着三个知识库：网络风险、对应措施和产品及服务。这些数据库收集由研究人员和产品和服务开发人员提供的并在之后由注册机组织并分类的有关网络安全的知识。

网络风险知识库累积网络安全风险信息，包含漏洞知识和风险知识。漏洞知识库累积已知的漏洞信息，包括名称、分类和包括对已知漏洞的命名、分类和列表。它还包括ICT使用者面临的人为漏洞。风险知识库累积已知的风险信息，包括攻击知识和滥用知识。攻击知识包括有关攻击模式、攻击工具（如恶意软件）及其趋势的信息，如有关以往攻击的区域性趋势信息和攻击目标。它还包括有关以往攻击的统计信息。滥用知识包括有关使用者毫无恶意地滥用ICT的知识。打字错误信息和违规情况亦包含在内。

对应措施知识库累积有关对应网络安全风险的措施信息，包括两个知识库：评估和检测/保护。评估知识库累积评估ICT资产安全水平的已知规则和标准以及配置清单。检测/保护知识库累积检测/保护安全风险的已知规则和标准，如IDS/IPS签名和相关检测/保护规则。

产品和服务知识库收集有关产品和服务的信息。它包括两个知识库：版本知识和配置知识。版本知识库收集有关产品和服务的版本信息，包括版本的名称和列表。有关产品版本，安全补丁亦包含在各知识库中。配置知识库收集有关产品和服务的配置信息。有关产品配置，它包括已知配置的名称、分类和列表。

上述各数据库和知识库可能使用不同的信息描述技术，见图II.2。



图II.2 – CYBEX使用显示技术的详细实例模型

有关CYBEX实例模型的更多信息，请查阅参考资料[b-Takahashi]。

附录III

CYBEX安全自动化方案示例

（本附录不是本建议书的组成部分）

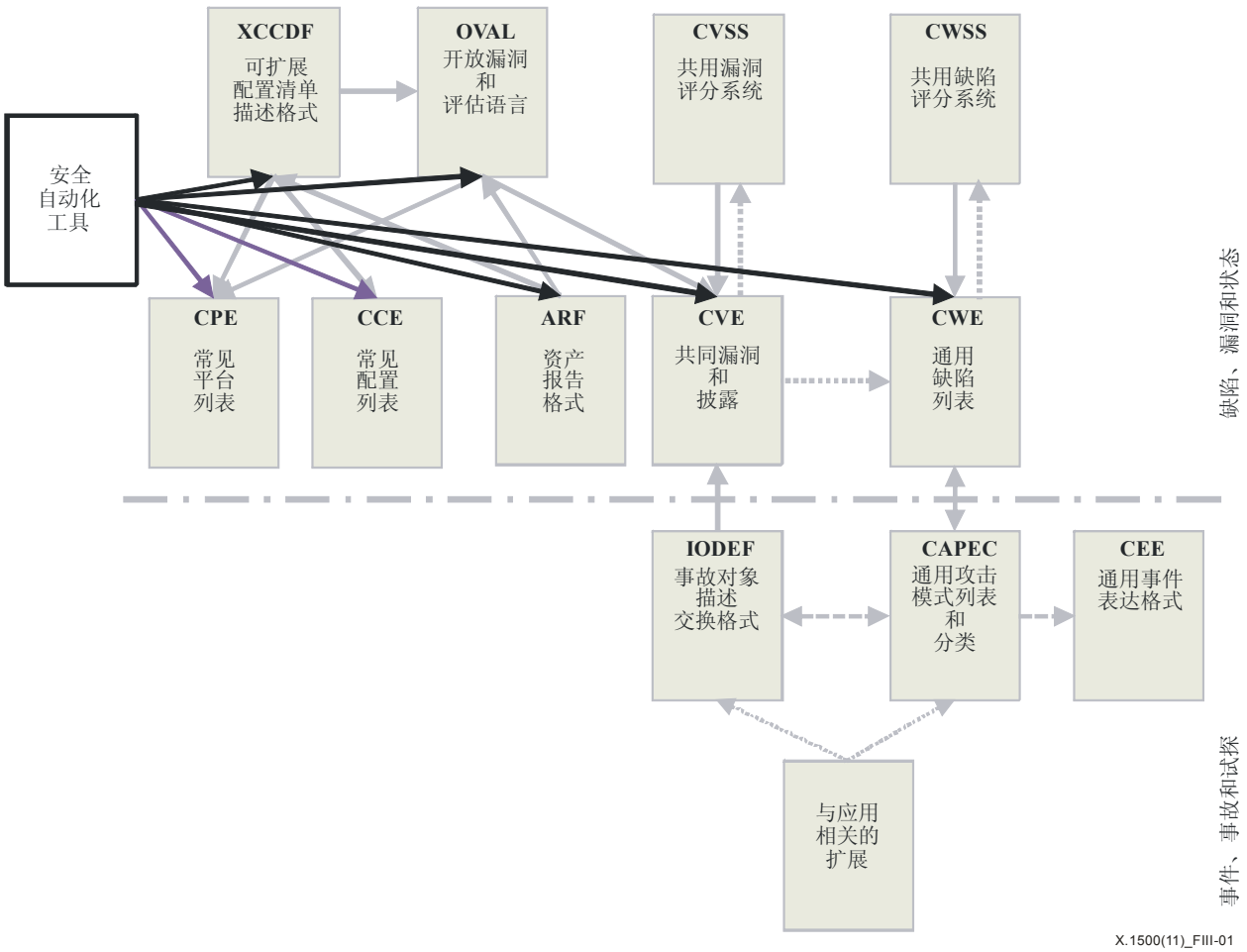
附录III提供了两个安全自动化模式的例子。这些功能可用于创建具体的CYBEX实例，包括对已知的软件、服务和系统的安全或信任“状态”自动化，检测恶意软件，捕捉事件和试探信息。

预计将有大量实施方式出现，特别是为确保ICT系统适当配置和补丁的安全自动化方案。两个突出的示例包括：

1) 美国标准和技术研究院（NIST）实现台式机核心配置（FDCC）及其更换的安全内容自动化协议（SCAP），美国政府配置基准（USGCB），

2) 日本JVN安全内容自动化框架。

本附录简要介绍以上各项内容。总而言之，这些安全自动化工具的实施采用图III.1显示的形式，包括不同的CYBEX信息交换平台，在图中用重叠指示器表示。



图III.1 – 网络安全保证和完整性自动化

III.1 举例：美国联邦台式机核配置/美国政府配置基线

联邦台式机核配置（FDCC）及其替换、美国政府配置基线（USGCB），使用NIST安全内容自动化协议（SCAP），该协议包括用标准方式组织和表达安全信息的规范以及相关参考数据，如各种漏洞的独特标识符。上述两项举措的目的是为广泛部署于各联邦机构的ICT产品建立安全配置基准。USGCB基准由联邦台式机核心配置手册演进而来。USGCB是一个联邦政府举措，为各机构就改进和保持有效配置设置提供指南，重点考虑安全问题。

USGCB技术规范描述了确保一致而准确地交换SCAP内容所使用的要求和惯例以及可靠运行SCAP认证工具的能力。最早的版本包括六种规范：XCCDF、OVAL、CPE、CCE、CVE和CVSS。这些规范分为三个类别：语言、列表和漏洞测量及评分系统。

SCAP实施1) 安全软件产品通报软件错误和安全配置信息的具体格式和名称术语，2) 具体软件错误和安全配置标准参考数据，即SCAP内容。SCAP的目标包括对系统安全管理进行标准化，促进安全产品的可互操作性并推进安全内容标准表达法的使用。由于不同系统和安全等级导致而出现多项SCAP内容，结构化标签、发现和目前方案的保证确认是必不可少的要求。USGCB基于SCAP规范创建内容和指南。

III.2 举例：日本漏洞信息门户网站，JVN

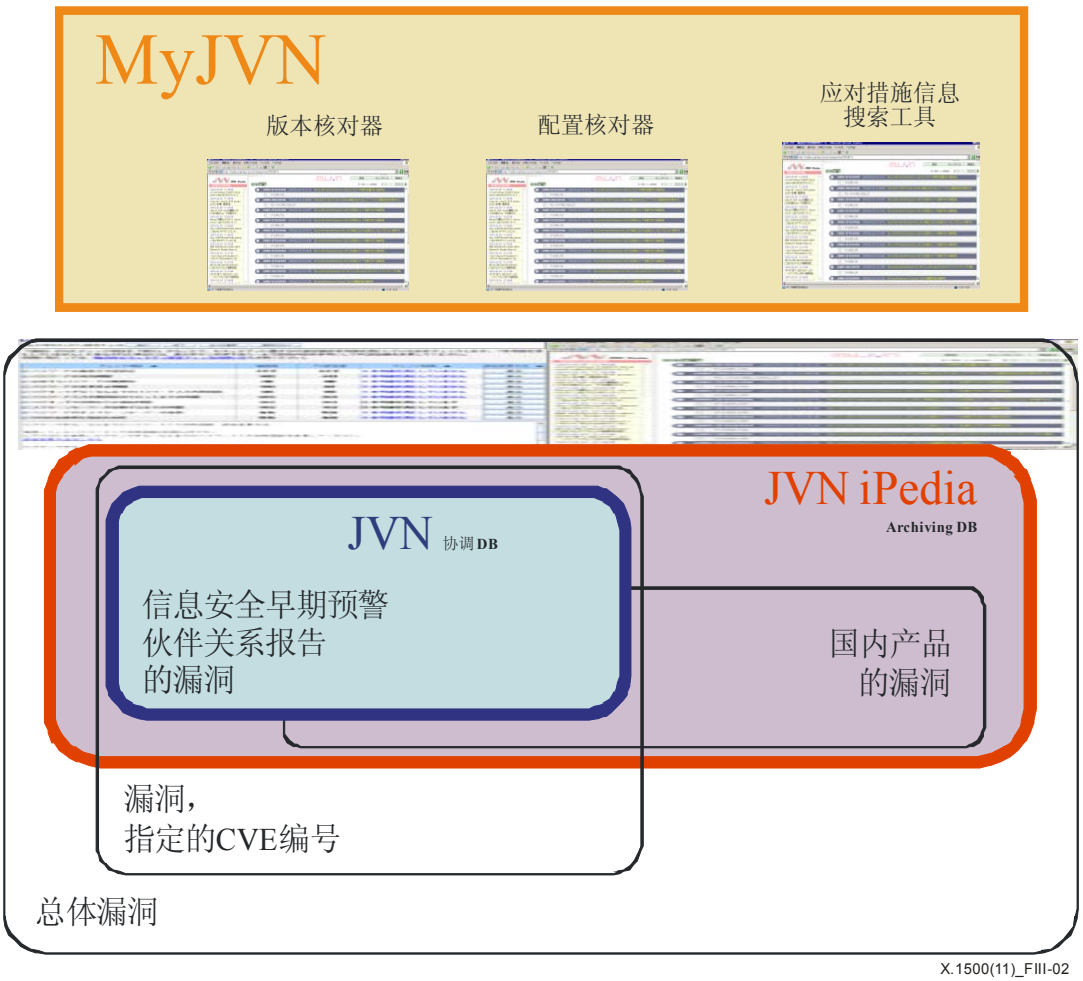
JVN代表“日本漏洞通知”，提供日本使用的软件中的漏洞和相关信息。JVN旨在帮助应对网络威胁。为促使应用开发人员在开放的界面上使用数据，JVN通过了SCAP并将本地（国内）信息和国际信息包含其中，形成JVN安全内容自动化框架。像国家漏洞数据库（NVD）一样，各项漏洞信息拥有一个CVE号码，提供CVSS评分和CWS编号。此外，受到影响的产品的CPE名称亦提供在内。

该框架包括三个组成部分：MyJVN、JVN和JVN iPedia（见图III.2），各项内容详情见下文。

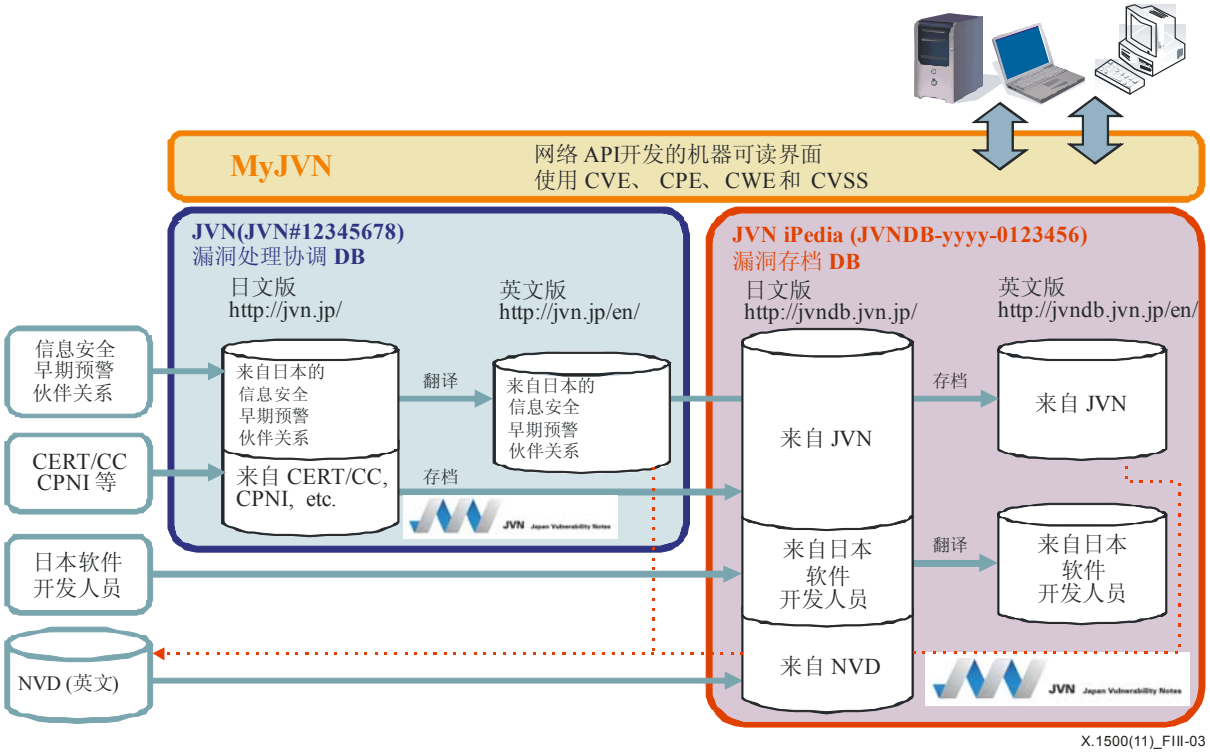
MyJVN通过MyJVN API提供了漏洞应对措施信息。这是一个包括Web APIs在内的可读界面和诸如文本核对器的MyJVN工具。它改进了对存储在JVN和JVN iPedia内的漏洞应对措施信息的使用，使用户更加轻而易举并有效地通过诸如定制过滤、自动搜索和检查列表创建收集目标信息。此外，“MyJVN版本核对器”（基于SCAP的工具）使人们得以方便地检查安装在其PC上的软件是否为最新版本。

JVN提供漏洞应对措施信息，日本厂商对“信息安全早期预警伙伴关系”报告的漏洞做出的反应。该公众私营伙伴关系框架的建立旨在促进软件产品和万围网站安全并防止因计算机病毒或非授权接入而对大量计算机造成破坏。当漏洞信息报告给IPA（信息技术促进机构日本）时，该信息传送至作为协调机构的JPCERT/CC。JPCERT/CC确定受到影响的软件产品并与开放人员协调。当确定诸如补丁或软件更新等用户解决方案时，包含漏洞详情在内的开发人员声明将公布在JVN上。

JVN iPedia提供软件产品（如日本使用的操作系统、应用、图书和内嵌系统）漏洞应对措施信息。JVN旨在尽快向公众提供漏洞和应对措施信息。协调机构与厂商就何时披露新报告的漏洞予以接洽。JVN iPedia另一方面的使命是收集非JVN公布的日本日常软件产品上出现的其他漏洞和应对措施信息。



图III.2 – JVN 安全内容自动化框架概念



图III.3 – 国内和本地信息数据库

采用RSS等标准格式的用户可能拥有包含国际和本地信息的数据库（见图III.3）。在三个组成部分之中，MyJVN作为用户界面，其使用情况得益于下一节所述工具和API。

MyJVN工具和API

MyJVN工具是基于SCAP的安全工具，改进漏洞应对措施的使用和信息交换环境。目前，我们提供的主要工具包括：

- **过滤漏洞应对措施信息工具** — 该工具改进对存储在JVN和JVN iPedia中的漏洞应对措施信息的使用，使用户更加方便而有效地通过CPE定制过滤等服务收集目标信息。
- **版本核对器** — 版本核对器是一个基于OVAL的在线扫描器，使人们得以方便地检查安装在其PC中的软件是否为最新版本。使用鼠标点击一次，人们就可以检查多种软件的版本。检查结果方便易懂：划钩表示最新的版本，划叉表示过时版本。如软件不是最新版本，用户可通过几次点击接入厂商下载网站。MyJVN版本核对器支持互联网相关的软件产品，寻求与其他厂商的合作。
- **MyJVN安全配置核对器** — 是一个基于XCCDF和OVAL的在线扫描器。该工具免费并方便获取Windows安全配置，包括账户政策，如最短密码长度、密码到期日、屏保自动开关、USB自动运行功能等。

- **MyJVN API —** 此API是一个软件界面，用来接入和使用存储在JVN和JVN iPedia当中的漏洞应对措施信息。为使应用开发者通过开放界面使用数据，JVN iPedia采用了SCAP，即用于描述漏洞应对措施信息的一套标准。通过使用MyJVN API，任何定制应用可接入JVN iPedia中的数据，各种漏洞管理服务现在均可有效地利用漏洞应对措施信息。

  MyJVN API基本功能是过滤的信息服务API和SCAP合作服务API。前一个API支持过滤漏洞应对措施信息工具所使用的“获取产品清单”、“获取漏洞概况清单”等。后一个API支持MyJVN版本核对器和MyJVN安全配置核对器使用的“获取OVAL定义清单”、“获取OVAL定义数据”等。

  有关JVN的更多信息，请参阅文章[b-Terada]。

参考资料

[b-ITU-T E.409] Recommendation ITU-T E.409 (2004), *Incident organization and security incident handling: Guidelines for telecommunication organizations*.

[b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

[b-ITU-T X.1205] Recommendation ITU-T X.1205 (2008), *Overview of cybersecurity*.

[b-ITU-T X.1520] Recommendation ITU-T X.1520 (2011), *Common vulnerabilities and exposures (CVE)*.

[b-ITU-T X.1521] Recommendation ITU-T X.1521 (2011), *Common vulnerability scoring system*.

[b-ETSI TS 102 042] ETSI TS 102 042 (2011), *Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates*.

[b-IETF RFC 3080] IETF RFC 3080 (2001), *The Blocks Extensible Exchange Protocol Core*. http://datatracker.ietf.org/doc/rfc3080/

[b-IETF RFC 5070] IETF RFC 5070 (2007), *The Incident Object Description Exchange Format*. http://datatracker.ietf.org/doc/rfc5070/

[b-IETF RFC 5901] IETF RFC 5901 (2010), *Extensions to the IODEF-Document Class for Reporting Phishing*. http://datatracker.ietf.org/doc/rfc5901/

[b-IETF RFC 6045] IETF RFC 6045 (2010), *实时网络间防范 (RID)*. http://datatracker.ietf.org/doc/rfc6045/

[b-IETF RFC 6046] IETF RFC 6046 (2010), *Transport of 实时网络间防范 (RID) Messages*. http://datatracker.ietf.org/doc/rfc6046/

[b-ARF] Assessment Results Format. https://measurablesecurity.mitre.org/incubator/arf/

[b-CAPEC] Common Attack Pattern Enumeration and Classification. https://capec.mitre.org/

[b-CCE] Common Configuration Enumeration. https://cce.mitre.org/

[b-CEE] Common Event Expression. https://cee.mitre.org/

[b-CPE] Common Platform Enumeration. https://cpe.mitre.org/

[b-CWE] Common Weakness Enumeration. https://cwe.mitre.org/

[b-CWSS] Common Weakness Scoring System. https://cwe.mitre.org/cwss/

[b-EVCERT] CA/Browser Forum, *Guidelines for the Issuance and Management of Extended Validation Certificates*, Ver. 1.3

[b-MAEC] Malware Attribute Enumeration and Characterization. https://maec.mitre.org/

[b-NIST EAA] *Electronic Authentication Guideline*, NIST Special Publication 800-63 Version 1.0.2, April 2006

[b-OVAL] Open 漏洞 and Assessment Language. https://oval.mitre.org/

[b-Takahashi] Takahashi, T., Kadobayashi, Y., and Fujiwara, H. (2010), *Ontological Approach toward Cybersecurity in Cloud Computing*, International Conference on Security of Information and Networks, September.

[b-Terada] Terada, Masato, et al. (2009), *Proposal of MyJVN (Web Service APIs) for Security Information Exchange infrastructure*, 21st Annual FIRST Conference on Computer Security Incident Handling, June. http://jvnrss.ise.chuo-u.ac.jp/jtg/doc/21thFirstConference_paper.pdf

[b-TLP] *CPNI Traffic Light Protocol* (2010), Information Sharing Levels, CPNI Information Exchange, UK, April.

[b-TNC] Trusted Computing Group, *Trusted Network Connect*.

Integrity Measurement Collectors – TCG Version (IF-IMC, Specification Ver. 1.2 Rev. 8, 5 Feb. 2007)

Integrity Measurement Verifiers – TCG Version (IF-IMV Specification Ver. 1.2 Rev. 8, 5 Feb. 2007)

Trusted Network Connect Client-Server – TCG Version (IF-TNCCS TLV Binding Specification Ver. 2.0 Rev. 16, 22 Jan. 2010)

Trusted Network Connect Client-Server Statement of Health – TCG Version (IF-TNCCS-SOH TLV Binding Specification Ver. 2.0 Rev. 10, 23 Jan. 2008)

Policy Enforcement Point – TCG Version (IF-PEP Protocol Bindings for RADIUS Specification Ver. 1.1 Rev. 0.7, 5 Feb. 2007)

Binding for SOAP – TCG Version (IF-MAP Specification Ver. 2.0 Rev. 36, 30 July 2010)

Platform Trust Services Interface – TCG Version (IF-PTS Specification Ver. 1.0 Rev. 1.0, 17 Nov. 2006)

Clientless Endpoint Support Profile – TCG Version (CESP Specification Ver. 1.0 Rev. 13, 18 May 2009)

[b-TPM] Trusted Computing Group, *Trusted Platform Modules*.

Design Principles – TCG Version (TPM Main, Part 1, Specification Ver. 1.2, Level 2 Rev. 103, 9 July 2007), ISO/IEC Version (11889-2, 2009-05-15, Information technology – TPM – Part 2)

TPM Structures – TCG Version (TPM Main, Part 2. Specification Ver. 1.2, Level 2 Rev. 103, 9 July 2007), ISO/IEC Version (11889-3, 2009-05-15, Information technology – TPM – Part 3)

Commands – TCG Version (TPM Main, Part 3, Specification Ver. 1.2, Level 2 Rev. 103, 9 July 2007), ISO/IEC Version (11889-4, 2009-05-15, Information technology – TPM – Part 4)

The TPM 1.2 specifications have also been adopted as ISO/IEC 11889. Overview – TCG Version (N/A), ISO/IEC Version (11889-1, 2009-05-15, Information technology – TPM – Part 1)

[b-W3C SOAP] W3C Recommendation Simple Object Access Protocol (SOAP), 2007.

SOAP Version 1.2 Part 1: Messaging Framework.

SOAP Version 1.2 Part 2: Adjuncts.

[b-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

瑞士印刷
2012年，日内瓦