安全加社区

公益翻译项目

2016

CAESARS 框架扩展：企业持续监控技术参考模型

二次修订版

美国国家标准与技术研究院

2012 年 1 月

文档信息			
原文名称	CAESARS Framework Extension An Enterprise Continuous Monitoring Technical Reference Model (Second Draft)		
原文作者	Petter Mell, David WWaltermiire, Larryy Feldmman, Harold Booth, Alfred Ouyang, Zach Ragland, and Timothy McBride	**原文发布日期**	2012 年 1 月
作者简介			
原文发布单位	National Institute of Standards and Technology		
原文出处	https://scap.nist.gov/events/2011/itsac/presentations/day2/Mell%20-%20Continuous%20Monitoring%20Technical%20Reference%20Model%20Overview.pdf		
译者	小蜜蜂公益翻译组	**校对者**	小蜜蜂公益翻译组

免责声明

- 本文原文来自于互联网的公共方式，由“安全加”社区出于学习交流的目的进行翻译，而无任何商业利益的考虑和利用，“安全加”社区已经尽可能地对作者和来源进行了通告，但不保证能够穷尽，如您主张相关权利，请及时与“安全加”社区联系。

- “安全加”社区不对翻译版本的准确性、可靠性作任何保证，也不为由翻译不准确所导致的直接或间接损失承担责任。在使用翻译版本中所包含的技术信息时，用户同意“安全加”社区对可能出现的翻译不完整、或不准确导致的全部或部分损失不承担任何责任。用户亦保证不用做商业用途，也不以任何方式修改本译文，基于上述问题产生侵权行为的，法律责任由用户自负。

小蜜蜂公益翻译组

计算机系统技术报告

国家标准与技术研究院的信息技术实验室旨在通过对国家的测量和标准相关的基础架构提供技术领导来促进国家经济和公共福利。ITL 设计测试和测试方法，并提供参考数据、概念验证（POC）和技术分析来推动信息技术的发展和应用。ITL 的职责包括制定技术、物理、行政及管理方面的标准和指南，实现经济高效的安全并保护联邦计算机系统中非机密的敏感信息。该报告介绍了 ITL 在计算机安全方面的研究、指导和外展活动以及与业界、政府和各学术机构之间的协作活动。

NIST 7756 号跨部门报告，35 页（2012 年 1 月）

本文中可能提到的商业实体、设备或资料，仅为准确描述程序或概念之目的，并非暗示 NIST 推荐或者认可，也并不意味着这些实体、资料或设备是实现目的的最佳选择。

致谢

我们在此对原创研究团队协助国土安全部的联邦网络安全部门在持续监控架构方面所做的开创性工作表示感谢。本文基于 CAESARS 框架[1]，包含持续资产评估、态势感知和风险评分三个方面。该框架是在 MITRE 组织的大力支持下构建的。

此外，我们也非常感谢以下各位加入持续监控研究团队、贡献有见地的想法、并对本文进行审核：国家安全局的斯蒂芬·约克、彼得·塞尔和大卫·明奇；博思艾伦咨询公司的亚当·哈尔伯迪亚、亚当·休曼纳斯基、乔·黛伯拉和阿密特·曼南；MITRE 组织的马克·克劳特。

最后，我们要感谢美国首席信息官委员会下属的信息安全和身份管理委员会的持续安全监控团队在我们编写本文时发挥的领导作用和给予的指导。此外，我们要特别感谢以下前任或现任联合主席[2]： 美国陆军的迈克尔·琼斯上校、国务院的约翰·史特奥福特、国防部长办公室的凯文·杜兰特以及国土安全部的蒂摩尼·迈克布莱德（也参与了本文的编写）。

本文是以下组织通力合作的成果：

NIST（彼得·梅尔、大卫·沃特米尔和哈罗德·布斯）

国土安全部（蒂摩尼·迈克布莱德）

博思艾伦咨询公司（赖瑞·费德曼和扎克·拉格兰德）

MITRE（阿尔弗雷德·欧阳）。

摘要

本文及其支撑性文档介绍了实现企业持续监控的技术参考模型。该模型扩展了国土安全部联邦网络安全部门提供的基于 CAESARS 架构的框架， 具体指提供附加功能、对每个子系统进行详细定义，并且进一步利用了安全自动化标准。此外，该模型使得大型多层架构的实现成为可能，并专注于层级间必要的沟通。本文旨在提供一种参考模型，便于实现企业持续监控。通过该参考模型，组织可将各安全工具收集的数据进行汇总、分析和评分，支持用户查询，并提供整体态势感知能力。该参考模型意在使组织利用现有的安全工具实现其上述功能，而无需投入大量资源进行复杂的定制工具集成。

读者对象

本文面向计划实施企业持续监控或研发产品以实现这一能力的用户以及即将支持这一能力的用户。该模型广泛用于各种网络，包括各行业、文职政府、州政府和部落的网络以及军用网络。本文的目标读者包括首席信息安全官、首席技术官、安全工具厂商、安全工具测试实验室、安全项目经理、企业架构师以及安全方面的采购人员。

本文不要求用户了解国土安全部 CAESARS 架构[3]。但是，如果用户具备该架构的基本知识，则能够深入理解 CAESARS 框架及其扩展功能。

---

[1] http://www.dhs.gov/xlibrary/assets/fns-caesars.pdf.

[2] 美国管理和预算办公室网站上列出了联合主席：
https://max.omb .gov/community/display/Egov/Continuous+Monitoring+Working+Group+Members

[3] http://www.dhs.gov/xlibrary/assets/fns-caesars.pdf

目录

1. 导言和概述 5
1.1 导言 5
1.2 文件概述 6
2. 持续安全监控的定义与范围 7
2.1 定义 7
2.2 CM 应用范围与外部系统接口 8
3. 持续监控的企业架构视图 9
4. 基础工作 11
4.1 CAESARS 参考架构概述 11
4.1.1 传感器子系统 12
4.1.2 数据库子系统 12
4.1.3 分析/风险评分子系统 12
4.1.4 呈现/上报子系统 12
4.2 CAESARS 参考架构的局限性 12
4.2.1 缺乏接口规范 12
4.2.2 依赖企业服务总线 12
4.2.3 通信净负荷规范不完善 12
4.2.4 缺乏描述子系统功能的规范 12
4.2.5 不支持多个 CM 实例 13
4.2.6 缺乏多子系统实例能力 13
4.2.7 CM 数据库与安全基线内容集成 13
4.2.8 对所需的资产存货缺乏详细描述 13
4.2.9 风险管理要求 13
5. CAESARS 框架扩展 14
5.1 CAESARS 架构变动 14
5.2 子系统概述 14
5.2.1 展示/报告子系统 15
5.2.2 任务管理器子系统 16
5.2.3 采集子系统 17
5.2.4 数据汇总子系统 18
5.2.5 分析/评分子系统 19
5.2.6 内容子系统 20
5.3 多级能力 21
6. 支撑文档架构 23
7. 结论 24
附录 A：缩略语 25

1. 导言和概述

1.1 导言

美国管理和预算办公室于 2010 年 4 月签署了一份备忘录，要求国务院、司法部和财政部配合国土安全部对其持续监控（CM）[4]的最佳实践进行评估，并将评估结果发布给政府各部门。评估完成后，国土安全部发布了持续性资产评估、态势感知和风险评分（CAESARS）参考架构报告，版本为 1.8[5]。该报告提供了一个基于安全自动化标准的参考架构，为组织部署企业 CM 实现提供指导。

2010 年 10 月，联邦首席信息官委员会下属的信息安全和身份管理委员会的 CM 小组委员会意识到需创建有关 CAESARS 架构扩展的技术项目，让 CAESARS 架构更好地服务大型组织（如整个美国政府）。为满足这个需要，国家安全局[6]下属的信息保护署的研究团队、国土安全部的联邦网络安全部门的 CAESARS 团队以及 NIST 的信息技术实验室展开了相关合作。该文件就是此次合作的成果之一。

合作过程中，国家安全局的加入确保了该架构适用于那些有意集成目前的国防部计划（如计算机网络防御方案）的美国军用和国家安全系统。国土安全部的工作确保了该架构适用于其 CyberScope 程序[7]且该程序与 CAESARS 版本兼容。NIST 的贡献主要是两个模型：一个适用于行业和政府的模型设计，另一个很好地集成现有的及新型的安全自动化标准。

本文介绍了本次合作的成果—CAESARS 框架扩展。也就是说，基于当前 CAESARS 架构进行扩展，让其更广泛地应用于整个美国政府，包括国防部、情报机构以及民事机构。此外，扩展 CAESARS 架构也是为了让其服务于行业、州政府和部落的网络，通过采用灵活的模型满足各类用户及场景的需要。为实现这一扩展，一方面我们改进了 CAESARS 框架，使其支持需多层 CM 框架的大型实现。另一方面，我们还做了很多工作实现额外的功能，细化了子系统规范，并深挖安全自动化标准（如通信净负荷和应用接口方面）。

CAESARS 框架扩展的最终目标是利用技术参考模型实现企业持续监控。通过该模型，组织可将各安全工具收集的数据进行汇总、分析和评分，支持用户查询，并提供整体态势感知能力。该扩展的重点在于支持网络运营，并在实际安全监控和提升过程中顺带生成合规报表。在扩展设计中，我们力求使组织利用现有的安全工具实现这一目标，减少定制工具集成方面的投入。

本文介绍了框架扩展的概要设计。当然，除了此概要设计，实现这一扩展还需子系统规范、接口描述和通讯协议作为支撑。同时，安全工具厂商及其客户的参与也是非常必要的，他们可提供输入并协助制定和落实更加详尽的规范。

安全工具厂商的参与非常重要。这是因为扩展实现过程中，可能会对这些厂商的安全传感器和控制器进行适度调整，使其支持框架采用的技术模型及安全自动化标准。所幸，这些产品在符合 NIST 安全内容自动化协议（SCAP）认证计划[8]过程中已经完成了某些调整。另外，该扩展还要求新增数据汇总与分析功能以及事件管理产品。而很多现有产品目前已能够提供某些新功能，我们仅需要对这些产品进行适度调整，使其支持技术模型。

若框架扩展使用得当，组织可集中利用各类安全产品建立一个分级的数据汇总模型，为安全行业以及一般信息技术管理领域的大量用户提供 CM 服务。其中的挑战是要坚持最小功能原则，让安全工具厂商能够高效参与，并确保不同厂商的产品之间实现互通。要解决这一难题，政府与行业之间需经常进行讨论、合作和开展研发活动。

[4]请不要将本文中的 CM 与 NIST 800 系列的其他文件中的 CM（配置管理）相混淆。

[5]国土安全部的持续资产评估、态势感知和风险评分参考架构报告，版本为 1.8，第 4 页（http://www.dhs.gov/xlibrary/assets/fns-caesars.pdf）

[6]http://www.dhs.gov/xlibrary/assets/fns-caesars.pdf

[7]http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda 2010/m10-15.pdf

[8]NIST 的 SCAP 认证计划：http://scap.nist.gov/validation/index.html

1.2 文件概述

本文将在第 2 章介绍 CM 的定义。从 CM 定义中可提取一些基本技术特点，为 CM 的企业架构视图提供支持。第 3 章展示了 CM 的企业架构示例视图。该视图列出了原有的 CAESARS 架构实现的目标，有助于我们了解 CAESARS 架构的功能和限制。第 4 章介绍 CAESARS 架构的功能和限制。第 5 章概述 CAESARS 架构基于其原有功能进行的扩展。这一扩展解决了原有架构的局限性。第 7 章介绍了本文所涉及的支撑性技术文档。第 7 章为总结。

附录 A 列举了本文出现的缩略语。

2. 持续安全监控的定义与范围

本章介绍了 CM 的几种定义以及从中提炼的 CM 实现的基本技术特点。并且，本章还介绍了 CM 所涉及的范围，帮助用户了解技术模型的功能以及目前的 IT 运营所需要的服务。

2.1 定义

CM 的广义含义如下：

> *持续监控指进行持续性观察，一旦发现异常，立即发出警报。持续监控能力指持续监控系统的运行状态，分析监控数据，得出当前状态与期望状态之间的偏差，提供态势感知有关的决策支持。*

该定义适用于网络安全和一般 IT 领域（如网络管理）。本文关注的是网络安全领域，但架构本身也适用于一般 IT 领域。鉴于提供有效的 CM 解决方案需投入很多资金和精力，因此应在尽可能多的领域应用这些方案。在本文中，我们竭力使这些解决方案适用于网络安全和 IT 管理领域。

在网络安全领域，我们对安全风险管理场景中的 CM 进行了重新定义。以下是 NIST 特别刊物 800-137 中的定义：

信息安全持续监控：对组织的信息安全、漏洞和威胁进行持续监控，为其风险管理决策提供支持。

注意：这里的“持续”指定期评估和分析组织的安全风险和管控措施，且该频率足以为组织的基于风险的安全决策提供支持，并可提供充分的信息保护。

鉴于本文旨在设计技术参考架构，按照实现过程，对其详尽描述如下：

持续性安全监控是网络安全领域的一种风险管理方案，展示了组织的整体安全状况、洞察资产的安全风险，利用自动提供的数据，监控安全措施的有效性，并基于优先顺序进行修复。

从以上定义，我们可整理出 CM 的以下基本特点：

- 展示组织的整体安全状况
- 评估安全状况
- 对比当前安全状态和期望的结果，找出差距
- 洞察资产的安全风险
- 利用自动提供的数据
- 监控安全措施的持续有效性
- 基于优先顺序进行修复
- 提示用户哪些修复可自动完成，哪些需手动操作。

以上特点为第三章的 CM 的企业架构图提供了支持。

2.2 CM 应用范围与外部系统接口

本文展示了 CM 的企业架构，旨在明确该 CM 方案在企业的应用范围。因此，我们在技术参考模型中也界定了 CM 的技术实现提供的功能（如事件分析）和可接入的外部系统。在实现 CM 过程中，需连接多个外部系统，例如，若确定当前有哪些资产，CM 实现须接入资产管理系统。

图 1 表明，至少以下 11 种外部系统和技术可与 CM 能力[9]进行对接：

1. 漏洞管理
2. 补丁管理
3. 事件管理
4. 意外事件管理
5. 恶意软件检测
6. 资产管理
7. 配置管理
8. 网络管理
9. 证书管理
10. 信息管理
11. 软件保障

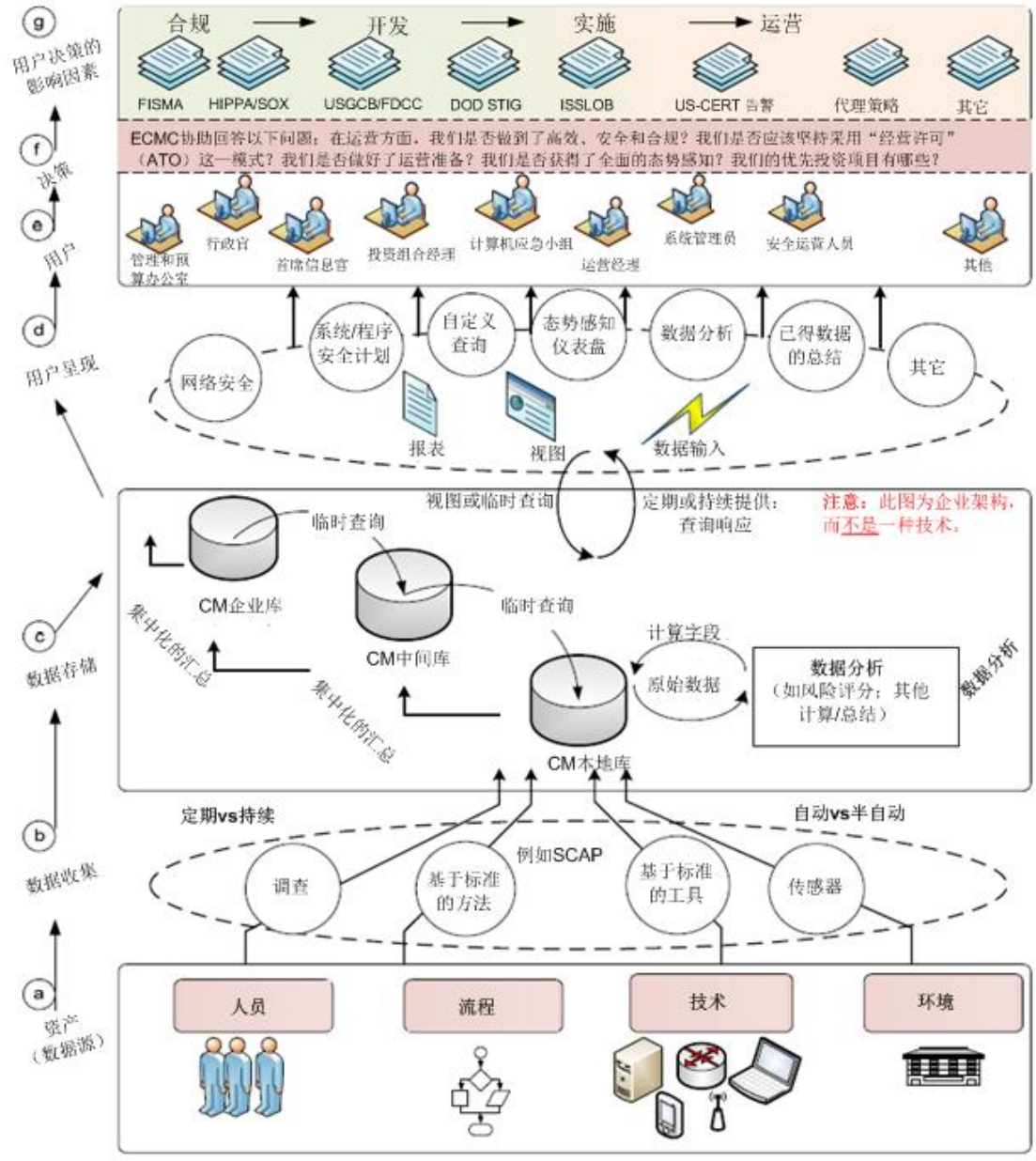
图 1 CM 数据域

- 即使支持以上数据域的工具并非是提供 CM 能力的核心部件，但若与 CM 方案进行交互仍需进行调整。为此，我们技术模型集成这些工具，并标明其为外部实体。这样，我们就可以描述与所需接口相关的需求。

[9]NIST 特别刊物 800-137，《联邦信息系统和组织的信息安全持续监控》中的附录 D.1：http://csrc.nist.gov/publications

3. 持续监控的企业架构视图

本章提供了 CM 的企业架构视图[10]，用于说明 CAESARS 架构扩展的技术参考模型的主要目标及相关实现。图 2 为实现持续性企业监控能力（ECMC）的企业架构视图。



上图并非一个技术架构，而是意在明确 CAESARS 框架扩展的技术模型所要实现的主要目标。下文将介绍企业架构视图的每个层级，并对所需的技术模型进行总体评价。首先介绍数据源如何为数据收集活动提供数据，然后描述如何收集和分析数据并呈现给用户，供其综合各种影响因素做出决策。

[10]企业架构视图由国家安全局下属的信息保护署创建。为了介绍临时查询和数据变动汇总，本文的作者对 EA 视图进行了微调。

a. 数据源

CM 的数据源包括以下类别：人员、流程、技术和环境。尽管很多 CM 实现最初可能只关注技术，但仍需一个非常全面的 CM 技术架构来包含其它类别的数据源。人员、流程和环境方面的数据类型并未完全实现自动数据采集，大多数情况下仍需手动操作。

b. 数据采集

可通过自动和手动方式采集数据。需注意的是，应通过工具内基于标准的方法收集数据，以降低集成成本、实现子系统的即插即用功能，使 CM 实现集成各类安全实现。然而，并非所有的数据源目前均已进行了标准化，因此该技术模型仍需要接受与处理一些专有的数据净荷。针对手工产生的数据数据（如，源自用户调查或安全合规文档的数据），应通过采用了自动化和标准化方法的机制来收集。此外，数据收集周期应视具体的数据源而定。某些数据源将一直收集数据，而有些则在特定时间段内定期收集。在某些情况下，数据源在事件发生时收集数据更为合适。

c. 数据存储和分析

收集的数据最初存储在采集点附近的本地库中，随后将在组织内的更高层级进行汇总。每一层级均有 CM 数据，因此各层级的用户可通过一个合理抽象化的视图，了解组织安全状况。一般，每个层级的用户只需了解下层 CM 数据的抽象化视图，因此没有必要复制整个层级的全部数据。此外，在组织内多个层级中复制所有的下层安全数据将会导致更大的安全风险并带来认证和扩展性方面的挑战。

鉴于此，CM 的企业架构视图显示，当将 CM 数据从下层库传输至上层库时，将进行“集中化的汇总”。在此过程中，只传输和复制上层所需的数据。对于任意 CM 实现来说，确定这些必要的预定义视图是非常重要的一步。理论上，绝大部分 CM 数据，尤其是多数敏感数据只存储于本地库中。因此，本地库中的数据最接近权威数据源（如数据采集器）并支持细粒度的访问控制。而且，这些数据是最新收集的，其汇总风险最小。

一般来说，CM 实现通过使用预定义视图的模型汇总数据。有时，上级用户可能需查询可用的预定义视图之外的数据。这种情况下，组织可能有意汇总各层级中更多的数据。极端的情况下，组织可能会汇总并复制所有层级的全部数据。这将导致额外的安全风险，并带来网络带宽和数据存储方面的挑战。为缓解这一需求，CM 的企业架构视图可使某一层级的用户向下层下发操作查询或临时查询进行数据检索。如果在本地库中未检索到所需数据，上级将下发操作查询，由下级收集数据。CM 的技术架构在集成必要的任务管理系统时需支持操作查询，以便审批这些查询，保证此等查询不会导致本地网络或系统的性能下降。

关于数据存储，最后要考虑的一点是，不管哪个层级在进行通信，均需使用同一技术模型（如接口、协议和净荷）汇总数据。这样就无需为每个层级提供不同的 CM 汇总方案。

d. 用户呈现

数据存储层中的每个层级均为用户提供一份数据视图。鉴于 CM 实现将支持各种类型的用户，呈现层需非常灵活，能够满足各种数据显示需求。CM 实现的首要目标是支持操作任务，以协助保障组织的安全（可能使用态势感知仪表盘）。此外，这些实现仍需支持合规报表、管理层报表以及非安全用例的报表功能。

e. f 和 g：用户、决策和用户决策影响因素

很多用户，包括系统管理员、组织的首席信息官以及可能的外部合规或审计实体，都需要 CM 数据。这些用户将基于一系列因素做出决策。CM 架构须为这些用户提供决策所需的必要信息。

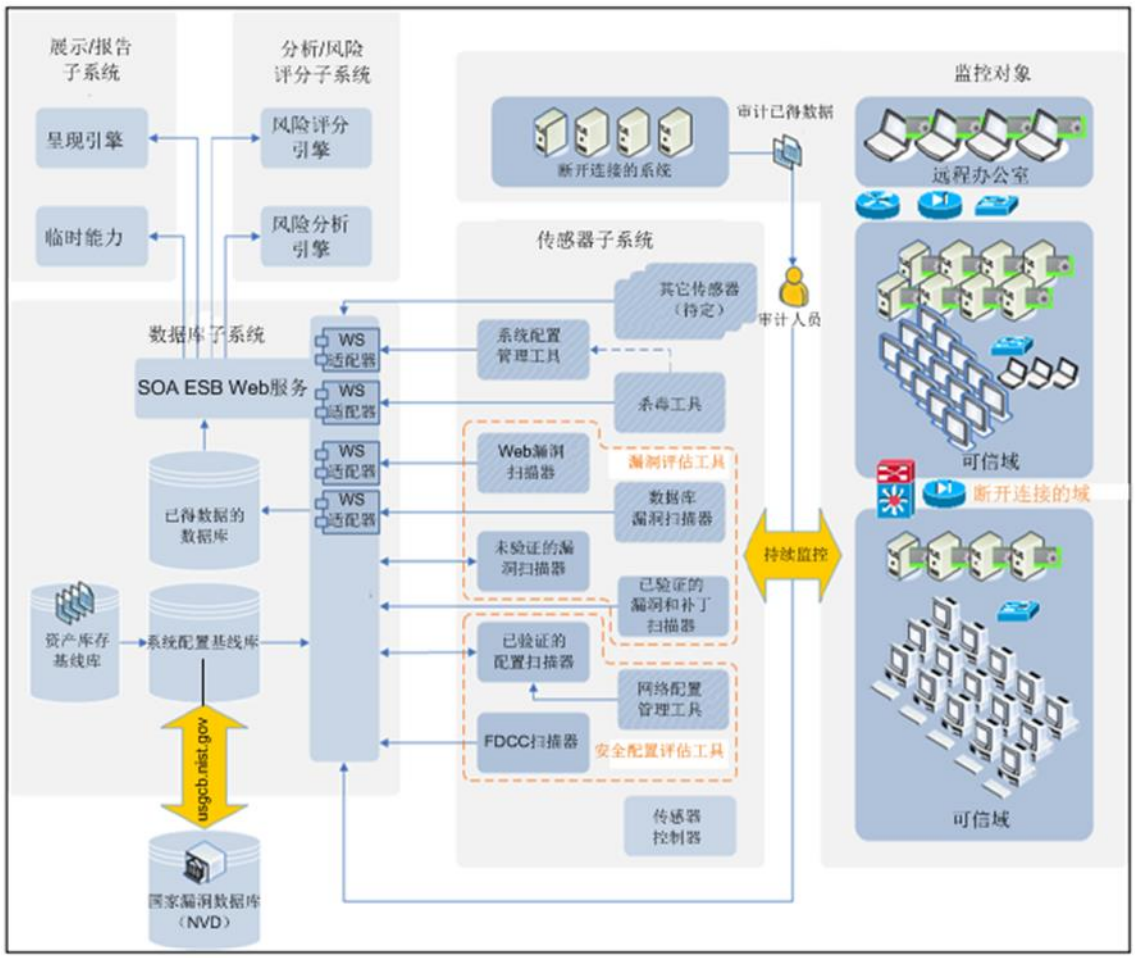
4. 基础工作

国土安全部对美国美国国务院、司法部和财政部的 CM 成功实现进行了评估，并基于评估结果构建了 CAESARS，发表了持续性资产评估、态势感知和风险评分（CAESARS）参考架构报告[11]。这种工作对于 CM 来说是史无前例的。DHS 总结了这些文职机构的定制化方案所采用的方法的共性和优势，并在此基础上构建了 CAESARS 参考架构。CAESARS 架构实现了 CM 的企业架构视图的很多（并非全部的）目标。

4.1 CAESARS 参考架构概述

利用 CAESARS，组织可构建一个包含四个子系统的 CM 实例： 传感器、数据库、展现/报告以及分析/风险评分。除了数据库子系统，其他三个子系统都集成了多种工具，提供独立观察或分析。单个数据库可监控来自传感器子系统、各种传感器产品及其组织范围内的实例化过程的数据。中央数据库也用作展现/报告子系统和分析/风险子系统的监控数据来源。所有子系统通过企业服务总线进行内部通信。

CAESARS 系统的使用环境如图 3[12]所示。本节对该图中的每个子系统进行了介绍， 其中，所有的引用均出自 2010 年 9 月出版的 CAESARS 刊物，版本为 1.8[13]。



[11] http://www.dhs.gov/xlibrary/assets/fns-caesars.pdf

[12] 图 3 出自 CAESARS 版本 1.8，第 11 页。

[13] http://www.dhs.gov/xlibrary/assets/fns-caesars.pdf

4.1.1 传感器子系统

“传感器子系统包含了所有的 IT 资产，即 CAESARS 的监控活动的对象， 包括 CAESARS 的所有预期上报平台，如最终用户的设备、数据库服务器、网络服务器和安全设备。” 图 3 展示了 9 种传感器。需注意的是，针对企业内的信息系统安全业务线[14]所涉及的产品类型，国土安全部将持续进行政府采购。

4.1.2 数据库子系统

“CAESARS 数据库主要作为中央存储库使用，存储所有 CAESARS 数据，包括传感器子系统的各平台的传感器上报的原始数据以及在清洗、预处理、分析和评分过程中 CAESARS 分析/风险评分子系统中生成的数据。【CAESARS 数据库】还包含 CAESARS 数据库/存储库从传感器子系统平台提取数据时所使用的工具。”需注意的是，数据库子系统包含“配置基线库”，因此该子系统中也存储组织内各系统所需的基线安全状况（机器可读的）、已知漏洞及其风险等级（如 NVD 中数据）。此外，该子系统还包含了资产存货基线库，但本文未对其进行详细介绍。

4.1.3 分析/风险评分子系统

“CAESARS 分析/风险评分子系统由各种分析工具构成，这些工具可能会从本地（针对某一地区或网站）或企业的角度查询数据库子系统的相同或不同部分，并确保各种类型的分析互不影响。” 这是因为 CAESARS 架构是基于独立的即插即用的组件构建的，可使各种风险评分方案和工具同时部署，且互不干扰。

4.1.4 呈现/上报子系统

“CAESARS 呈现和上报子系统可从本地或企业的角度集成多个呈现工具，并确保不同类型的呈现互不影响。”该子系统实现了各种显示方案，可满足不同类型的用户的需求。并且，这些工具可同时部署，且互不干扰。

4.2 CAESARS 参考架构的局限性

CAESARS 参考架构为构建 CM 技术架构以实现 CM 的企业架构目标奠定了坚实的基础。然而，该参考架构在某些方面存在局限性，阻碍 CAESARS 提供更强大的能力。

4.2.1 缺乏接口规范

CAESARS 并未指定设备层面的接口用于子系统之间的通信。这就限制了 CAESARS 的即插即用功能，使得 CAESARS 的每个实现均需自定义集成。

4.2.2 依赖企业服务总线

CAESARS 规定使用企业服务总线实现子系统之间的通信。对于某些类型的通信，企业服务总线可能并非理想的通信机制，并且可能也不适用于某些厂商的产品。

4.2.3 通信净负荷规范不完善

CAESARS 探究了传感器子系统与数据库子系统通信的净负荷规范，但并没有提供完整规范全面覆盖各种传感器类型。而实际操作中，厂商需使用各种传感器搭建与 CAESARS 兼容的安全工具。 另外，CAESARS 也并未规定其它子系统之间的通信净负荷。

4.2.4 缺乏描述子系统功能的规范

CAESARS 仅概述了每个子系统，并未提供详细规范。而子系统规范可为采购活动提供支持，使各厂商调整其工具支持子系统的功能，并制定产品测试方法为产品验证计划（如 SCAP 验证[15]）提供支持。

[14] http://www.us-cert.gov/GFIRST/presentations/Information Systems Security Line of Business ISSLOB Overview.pdf

[15] http://scap.nist.gov/validation/index.html

4.2.5 不支持多个 CM 实例

CAESARS 的设计能力很单一，也就是说，每个组织只能利用该能力创建一个 CM 实例。CAESARS 还要求每类子系统只能有一个实例，因此组织的所有安全数据均需在同一 CM 中央数据库内进行复制。这与很多倾向于采用分散式 IT 管理方法的组织（尤其是联邦政府的组织）的结构不符。并且，这也与企业架构的 CM 目标相左。企业架构的 CM 目标是进行集中化的汇总，并将最新的 CM 数据留在分级结构的叶子节点上。因此，多数大型组织需多个 CM 实例。

4.2.6 缺乏多子系统实例能力

CAESARS 规定，针对每类子系统，每个 CM 实例仅能有一个。而 CAESARS 支持并鼓励每个子系统集成各类独立的安全工具。例如，展现/报告子系统可集成多种呈现工具。这就增加了复杂性，因为 CAESARS 没有明确规定子系统中的这些工具在子系统内部如何通信以及他们如何与技术模型的其他部分独立通信。为避免复杂性，需针对每类子系统，创建多个实例，并保证每个相关的安全工具（如呈现系统）均有各自的实例。尽管 CAESARS 用户可通过在每个子系统中只使用某一厂商的工具来避免此问题，但这一方法可能会限制 CAESARS 对平台和安全特性的全面覆盖的能力。使用多种工具（尤其是多个安全传感器）可在收集过程中增进可信度，并扩大收集范围，实现更深入的数据分析。

4.2.7 CM 数据库与安全基线内容集成

CAESARS 在数据库子系统中集成了系统配置基线库和存储已得数据的数据库。很多厂商的工具仅能实现其中的一种能力。为了便于 CAESARS 集成多个厂商的工具，可考虑将配置基线和数据库已得数据划分为多个子系统。

此外，组织的不同部门可能会需要根据其安全状况定制不同的策略以适合其环境和各种不同的任务。这些定制的策略将与那些从上层下发并在下层修改的策略进行垂直管理。而在单个数据库子系统中使用单一基线库，也就更加难以根据预期的安全状况定制策略。

4.2.8 对所需的资产存货缺乏详细描述

CAESARS 并未详细说明如何维护资产存货以及资产存货如何与配置基线库进行关联。

4.2.9 风险管理要求

CAESARS 要求分析/风险评分子系统评估安全风险。根据 NIST 的风险管理刊物 SP 800-37（修订版 1[16]），风险的定义如下：

“衡量潜在情形或事件，且通常为实体本身的某一功能，为实体带来的威胁的程度：（i）若情形或事件发生，所带来的负面影响。（ii）发生的可能性。”

风险评估需计算事件发生的概率以及产生的负面影响对组织的危害有多大。因此，进行风险评估非常困难，并且 CM 方案通常缺乏必要的输入。鉴于此，CM 架构应考虑采用一种更为简单且适应性更强的方案对安全状况或安全措施[17]的有效性进行评估，同时我们并不排除构建一种能够计算风险的 CM 系统（如果能够提供必要的输入）。

[16] http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf

[17] 低层的安全有效性评估结果可作为风险管理能力的输入(这很必要但仍不足)。

5. CAESARS 框架扩展

CAESARS 框架扩展基于国土安全部的 CAESARS 参考架构，为企业持续监控（CM）提供技术参考模型。CAESARS 框架扩展保留了大多数的 CAESARS 子系统，只是上级架构中做了少许改动，以增强功能，实施多级持续监控。

本节概括介绍了 CAESARS 框架扩展模型、子系统以及多级能力。与 CAESARS 一样，CAESARS 框架扩展可用于支持运营安全以及合规性评估与报告。与 CAESARS 不同的是，它的设计用途为数据域无关模型（data domain agnositic model），允许针对各种 IT 领域（包括安全与一般 IT 管理）进行采集、汇总、分析、展示与报告，模型还可实例化为针对具体数据域的各种架构。

CM 工作流、子系统规范与接口规范，本节不作具体描述，相关信息详见 NIST 7799 号跨部门报告（Interagency Report）。本节也不会将模型与具体的数据域（如资产、漏洞和配置管理）对应或捆绑，相关信息详见 7800 号 NIST 跨部门报告。相关文件信息，参见第 6 节。

5.1 CAESARS 架构变动

CAESARS 框架扩展旨在克服前文所述 CAESARS 架构的局限性。为此，它提供如下能力：

- 可定义各种子系统接口（移除了 CAESARS 数据库子系统内的必选件企业服务总线）（见 4.2.1 与 4.2.2 节）；
- 提供了具体的子系统通信净负荷规范（见 4.2.3 节）；
- 为各子系统提供具体规范，以支持工具开发与产品验证计划或代理采购（如国土安全部信息系统安全业务线）（见 4.2.4 节）；
- 允许创建多个 CM 实例（见 4.2.5 节）；
- 允许建立多级分层 CM 架构（见 4.2.5 节）；
- 允许单个子系统拥有多个实例（见 4.2.6）；
- 创建了单独的任务管理器子系统（从 CAESARS 传感器子系统中抽取“传感器控制器”，使各传感器成为自己的采集子系统）（见 4.2.6 节）；
- 抽取 CAESARS 的数据库子系统中的“配置基线库”，为安全内容服务器创建单独的子系统（见 4.2.7 节）；
- 进一步定义了资产存货数据库规范（见 4.2.8 节）；
- 提供了灵活的企业总体衡量方法，而非实际风险的衡量（见 4.2.9 节）。

5.2 子系统概述

CAESARS 框架扩展包括 6 个独立的子系统，这些子系统协同工作，构成 CM 模型。下文将对这些子系统详细论述：

- 展示/报告子系统（Presentation/Reporting）：该子系统接受用户输入，创建明确的数据查询请求，并输出可用结果。
- 内容子系统（Content）：该子系统储存数字政策及辅助数据（如系统状态检查数据）。
- 采集子系统（Collection）：该子系统根据组织政策检测系统状态信息。
- 数据汇总子系统（Data Aggregation）：该子系统储存系统状态信息、相关计算结果及关联元数据。
- 分析/评分子系统（Analysis/Scoring）：该子系统分析数据，对系统状态信息进行评分。

- 任务管理器子系统（Task Manager）：该子系统调控其他子系统活动，并与其他 CM 实例通信，以支持用户数据的查询。

图 4 为一个具体的 CM 实例，内含子系统及其关联组件。

大型组织可能会有多个通信实例，像美国政府这样的特大组织则会需要大型的协作性 CM 实例体系，为各种本地化运营、上级决策及整个政府部门内部的安全运营（如国土安全部的 CyberScope 程序）提供支持。

需注意的是，采集子系统在模型中被标为外部系统，这是因为此类系统很可能独立于 CM 实现，但是在模型中又需要它们来采集 CM 数据。内容子系统是模型的核心部件，也可以独立存在，但同时又集成在系统内以提供数据策略管理服务。其他四个子系统形成紧密核心，是任何 CM 架构必不可少的组件。

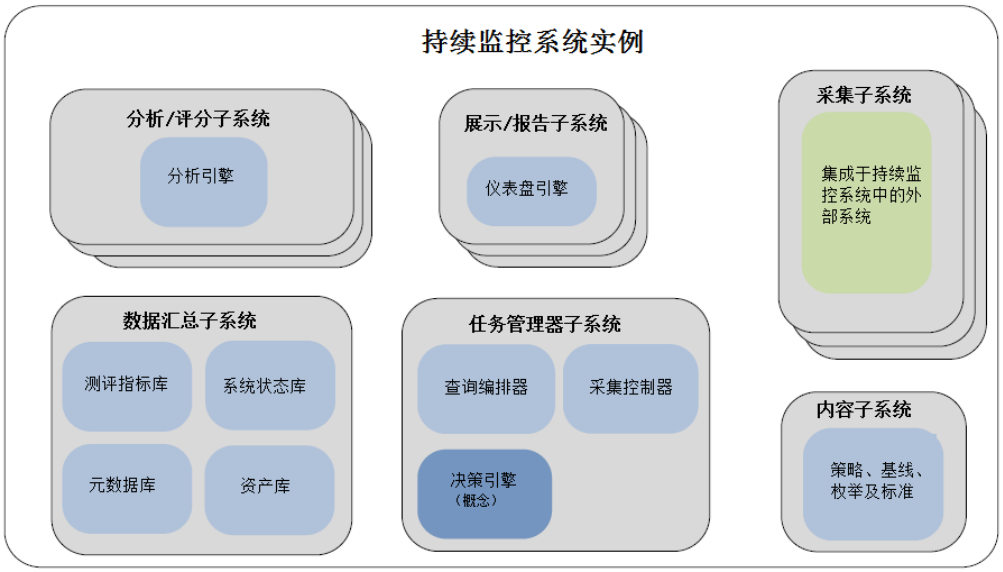


图 4 CAESARS 框架扩展子系统及部件

该模型的一个主要目标是帮助组织利用从各一流厂商采购的工具来实施 CM 方案，不同的工具用于实现不同的子系统需求，并可结合起来，共同实施 CM 解决方案。通过采用通用接口及数据标准化能力，工具集成会非常划算，因其最大程度地减少了定制集成，只有涉及必要的私有数据输入时才需要定制集成。即使是这种情况，通过提供"包装"私有数据的标准接口，也会降低集成成本。

5.2.1 展示/报告子系统

展示/报告子系统与 CAESARS 同名子系统功能类似，但与 CAESARS 不同的是，一个 CM 实例会有多个这样的子系统。这样，通过定制接口，满足了不同 CM 用户的实际需要。

该子系统仅有一个部件：仪表盘引擎。如图 5 所示，展示/报告子系统与任务管理器的查询编排器通信。

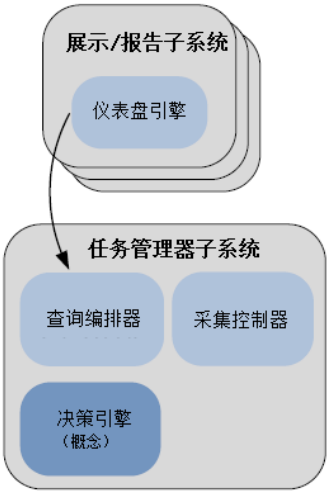


图 5 展示/报告子系统通信

该子系统的仪表盘引擎是 CM 方案的主要用户界面，用户可以在界面描述需要的数据，子系统用统一格式将这些请求包装成目的明确的查询，然后将查询发送给任务管理器来实现。收到回复后，子系统将数据展示在界面上或按用户要求提供报表。

5.2.2 任务管理器子系统

任务管理器子系统通过协调其他 CM 子系统的活动来完成 CM 查询，包括控制所采集的数据、激活评分程序、提供查询内容。该子系统在 CM 各层级的通信中相当于各 CM 实例的中央控制器，解析针对多个 CM 实例的数据的查询。

其他子系统多衍生自 CAESARS 的子系统，但任务管理器却不是。在 CAESARS 中，数据采集管理由传感器控制器承担。此外，CAESARS 中，展示/报告子系统与分析/风险评分子系统独立运行，无需任务管理器的协调。

CAESARS 框架扩展中增加了任务管理器，CM 方案可以自我修正，以最恰当地回应用户查询。这意味着来自展示/报告子系统的查询应动态触发要求的数据采集；数据采集的完成应触发数据冲突解决（data deconfliction）（参见 5.2.5 节）、分析与评分；评分的完成应触发对相关查询的响应。除此之外，还应与多个 CM 实例通信，回应其查询。接下来，任务管理器启动具有不同功能的各种安全工具，这些工具协调一致，共同运行，让企业及时了解安全态势。

图 6 为任务管理器的 CM 实例内部通信过程：任务管理器收到展示/报告子系统的查询，将其转发给采集子系统以采集需要的数据；它与下层 CM 实例通信，接收其数据并储存到数据汇总子系统；然后，将查询请求发送给分析/评分子系统以获取相关结果；任务管理器最后会将结果反馈给请求方（通常是展示/报告子系统，但也有可能是上级 CM 实例）。任务管理器可分别同上级和下级 CM 实例通信，这在下图并未体现。

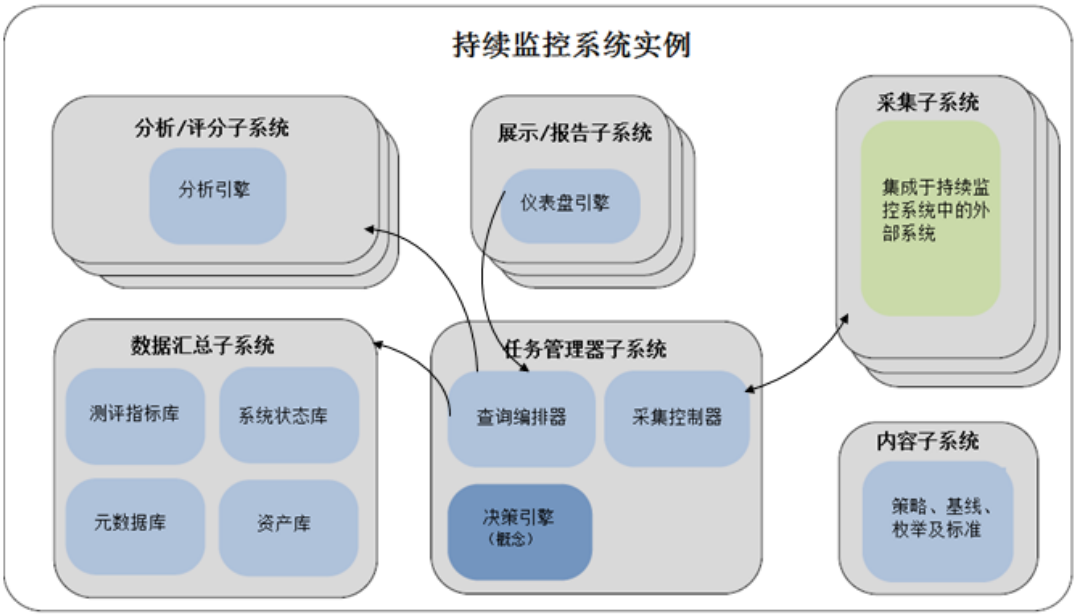


图6 任务管理器子系统通信

每个 CM 实例有一个任务管理器子系统，内含三个部件：查询编排器、采集控制器、决策引擎（目前还只是概念）。

查询编排器（Query Orchestrator）

查询编排器部件接收展示/报告子系统或上级 CM 实例的查询请求，然后应用策略，决定是否允许查询，还可能会触发人工审批流程。它与分析/评分子系统协作，无需采集数据便可查找结果。若未查找到结果，则协调相关方进行数据采集。若数据须从下级 CM 实例采集，查询编排器则会将该查询请求广播给所有的下级实例，查询到的结果会被储存在数据汇总子系统；若数据须从当前 CM 实例中收集，查询编排器会将查询请求发送至采集控制器。在采集完所有数据后，再将查询请求发送到分析/评分子系统，并接收后者回复的查询响应，最后，将响应转发给请求方。

这样，查询编排器就在多个子系统（有时会涉及多个 CM 层级）间对查询进行了编排，也就是说，它协同构成 CM 实例的多个安全工具共同完成任务。

采集控制器（Collection Controller）

采集控制器收到查询编排器的查询请求后，在当前 CM 实例内安排必要的数据采集。具体来说，它将查询分解为一组数据采集任务，发送给相关的采集子系统，然后追踪任务完成情况，在所有的数据收集完毕后通知查询编排器。这样，就完成了对某一特定查询的支持。

决策引擎（Decision Engine）

决策引擎是一个概念部件，对数字政策的实施提供支持和帮助。根据目前想法，决策引擎接收数字政策，根据该政策监控合规性。具体来说，决策引擎确保采集子系统采集的是正确的数据，并使用分析/评分子系统定期分析采集到的数据。简单地将机器生成的查询下发给查询编排器，就可以实现这些目标。

决策引擎的实现使得 CM 方案并不仅仅是响应人工查询请求，更是基于数字政策指令的全自动安全保障。

5.2.3 采集子系统

采集子系统与 CAESARS 的传感器子系统类似，区别在于，前者的每个实例须包含且只能包含一个厂商的解决方案。因此，会有一个管理控制台提供各种工具，与 CAESARS 的传感器类型一一对应。还有一个不同，CAESARS 的传感器控制器被转移到了 CAESARS 框架扩展的任务管理器子系统中，并被改名为采集控制器（详见“任务控制器”部分）。

图 7 为采集子系统的通信过程：该子系统接受任务管理器的任务，按照后者指示，采集用户请求的数据；采集子系统还会从内容子系统查找内容，确保其采集到的数据符合组织政策；最后，子系统将采集到的数据传送给数据汇总子系统储存。该模型还提供一个选择，采集到的数据在被储存之前可被传回任务管理器处理。

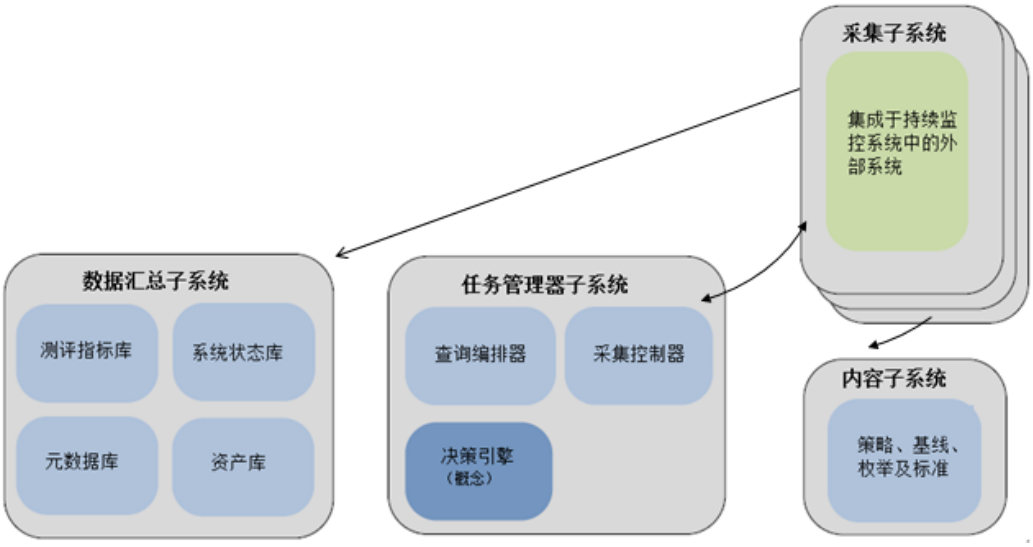


图 7 采集子系统通信

CM 实例并不一定会有采集子系统，比如，在多级分层 CM 实例中，上级 CM 实例无需监控任何资产。这种情况下，CM 实例仅依赖从下级 CM 实例获取的数据。话虽如此，多数 CM 实例不仅有、而且有多个采集子系统，以方便使用多种传感器工具。

5.2.4 数据汇总子系统

数据汇总子系统与 CAESARS 的数据库子系统有相似之处，但有明显差异。与 CAESARS 一样，数据汇总子系统提供库来储存与检索数据。但是，它没有企业服务总线，也不是将其他子系统连接在一起的中央集线器，更不包含配置基线信息，这些信息存在于内容子系统中。两者功能有重叠，它们都储存数据与系统状态信息（在 CAESARS 被称为“已得数据（findings）”）.不过，数据汇总子系统还储存其他数据，包括原始数据、分析后数据（CAESARS 框架扩展已得数据）、计算得分及元数据，这是 CAESARS 中所没有的。

图 8 为数据汇总子系统的通信过程：该子系统从采集子系统接收原始数据（亦或已得数据）；对于分层 CM 架构，也有可能从任务管理器接收下级 CM 实例的查询结果；最后，它向分析/评分子系统提供数据检索与存储服务，以便后者进行数据分析和评分。

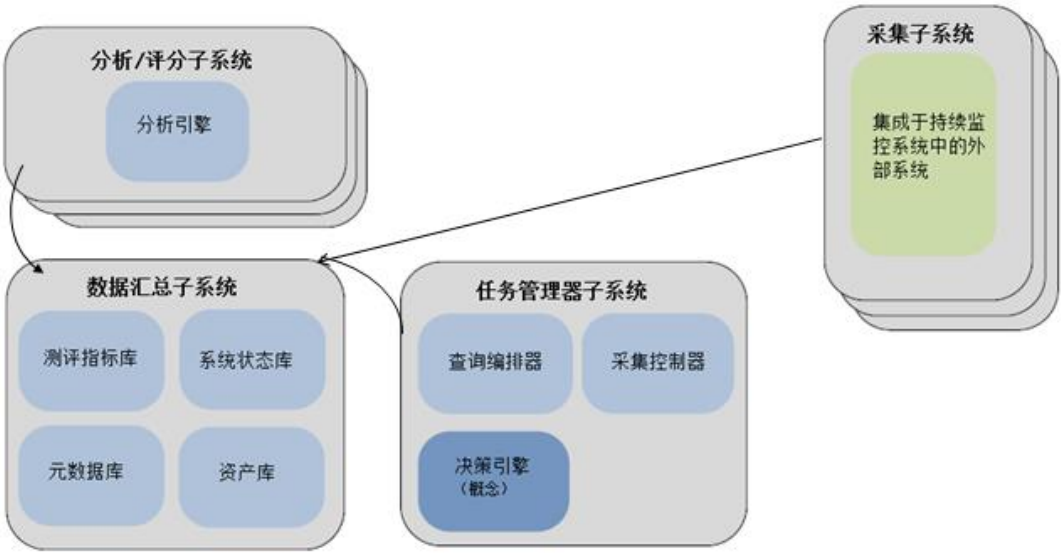


图8 数据汇总子系统通信

每个 CM 实例须有且仅有一个数据汇总系统，保证每个 CM 实例有一个统一的权威 CM 数据来源。每个实例包含以下四个部件：

- 系统状态库（System State Repository）

系统状态库包含原始数据与采集子系统提供的已得数据。这里可能会进行数据预处理以提高数据质量，但并不强制要求。数据预处理会影响评分流程的分析，因此，分析/评分子系统内部会进行数据冲突解决，以便使用自己的技术。

- 资产库（Asset Repository）

资产库储存从采集子系统获取的标准格式资产数据，它本身并非资产存货系统，仅仅是个汇总数据库。进行资产管理与评估的采集子系统会为资产库提供信息，此外，某些工具在主要功能（如配置扫描）之外会提供资产识别之类的辅助功能，这些工具也会为资产库提供信息。

- 测评指标库（Metrics Repository）

测评指标库储存的是分析/评分子系统生成的评分结果。部件生成数据后，数据以相关部件命名，这样，分析/评分子系统就能缓存不同的测评指标而不会破坏其他子系统的数据，也易于追踪。

- 元数据库（Metadata Repository）

元数据库储存元数据，用于原始数据冲突解决与评分。冲突解决规则本质上为过滤规则，针对的是如何处理表述不同但所指明显重复的数据元素。这些规则的内容中可包含不同采集子系统的相对准确性。

5.2.5 分析/评分子系统

分析/评分子系统与 CAESARS 同名子系统功能类似，区别在于，它提供总体的分析及评分服务，而非“风险”衡量。当然，可以使用这个子系统进行风险衡量，因为此种衡量为总体评分概念的子集，并且在实施安全型 CM 时，应把风险评分作为一个目标[18]。另一个区别是分析与评分（以及数据冲突解决）仅由分析引擎处理。

图 9 为分析/评分子系统通信过程：子系统可接受任务管理器的查询并进行分析与评分，并可从数据汇总子系统检索并在其中储存数据，此外，还可以更新自己的评分算法、评分参数以及从内容子系统获取的关联评分数据。

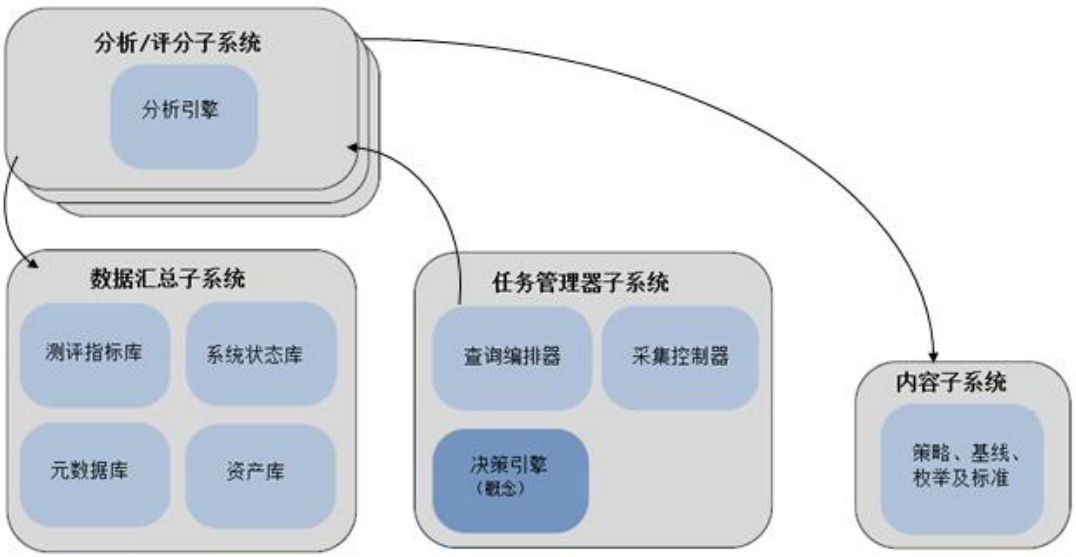


图9 分析/评分子系统通信

CM 实例必须有至少一个分析/评分子系统，这样，组织便可以利用多个分析引擎支持不同的评分算法。该子系统的分析基于这样一个原则：原始数据在数据汇总子系统的系统状态库中收集。分析引擎根据数据汇总子系统的元数据库（若有）提供的规则解决数据冲突，在相同数据被屡次上报（结果可能不同）时，须确定权威来源以解决数据冲突。原始数据冲突解决后，子系统使用评分算法及从内容子系统获取的策略产生已得数据，这些数据多为布尔值（“真”、“假”值），代表的是原始数据与描述原始数据期望值的策略之间的比较结果。已得数据储存在数据汇总子系统的测评指标库中供缓存与复用。接下来，子系统须将已得数据转化为

[18]真正的风险评分使用 NIST SP 800-37 第 1 次修订版本中的定义很难实现，并且许多的风险评分方法并没有展示同真正的风险衡量的相关性，相反，它们通常衡量的是一整套安全能力与控制措施的状态。

分值，这意味着取一个或多个已得数据，运用算法，生成一个数值解。完成一个查询请求可能需要在产生已得数据后进行评分。这种对原始数据、已得数据及评分过程的描述构成了 CAESARS 框架扩展模型的一个重要部分，有了这个部分，中间计算的复用才成为可能。此外，它还提供了一个架构，我们可以围绕这个架构设计规范，描述各种分析及评分方法。

5.2.6 内容子系统

内容子系统与 CAESARS 数据库子系统中的系统配置基线库类似，不过，它的范围更广，包括组织的总体数字政策及辅助数据（如数据标准化所需的枚举与标准），还包括非安全性政策及相关数据。因此，内容子系统与 CAESARS 中最初的预想不同，更像是一个数字政策管理库。因为这种变化，内容子系统提供的数据可支持系统状态信息与组织政策和数据标准化的对比。

内容子系统只有一个部件，这个部件同采集子系统和分析/评分子系统通信，也会同内容提供程序和内容开发工具通信，如图 10 所示。内容子系统还会同组织的 CM 方案所涉及的其他内容子系统通信，这个功能并未在下图体现。

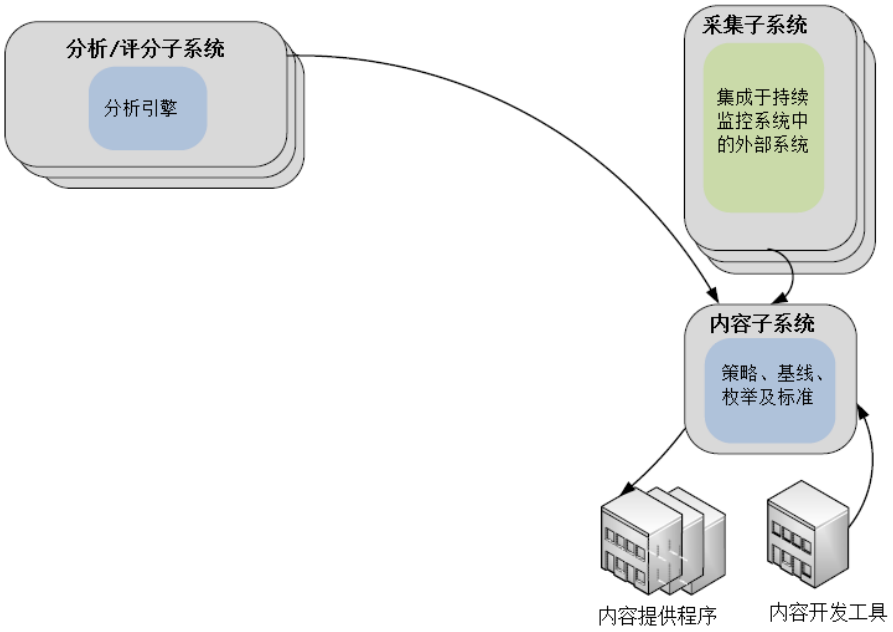


图10 内容子系统通信

子系统与内容提供程序及其他的内容子系统通信以获取内容，同内容开发工具通信则提供了内容裁剪与写作功能。在获取内容后，子系统将其储存、打上时间戳、标记来源以及内容来源于内部还是外部。子系统可获取两种类型的数据：组织政策与辅助数据。组织政策数据包括基准要求（如组织层面的安全配置策略）及基线（如为个别系统定制的安全配置策略）。辅助数据元素包括各种数据类型及关联评分（如产品名、漏洞名和漏洞影响评分）以及系统状态检测方法。CM 架构中提供此类数据的目的是为了按要求状态对系统进行评估，此外，这种标准化数据的使用使得多个 CM 实例可利用相似语言上报系统状态。

下面列举了内容子系统中包含的典型（非强制）组织政策类型：

- 软件资产基线（允许的软件及要求的版本）
- 安全配置基准要求（如联邦桌面核心配置（FDCC））
- 强制补丁列表
- 授权软件列表
- 网络端口要求配置

下面列举了内容子系统中包含的典型（非强制）辅助数据元素类型：

- 已知漏洞列表及影响力评分
- 已知配置问题列表及影响力评分
- 可应用的资产名称列表（非系统中的实际资产）

应尽可能使用常用规范表示这些数据，使其更利于复用、修改与标准化。下面列举了一些可使用的典型（非强制）规范：

- 可扩展配置清单描述格式（XCCDF）
- 开放式漏洞和评估语言（OVAL）
- 开放检查表交互式语言（OCIL）
- 通用漏洞披露（CVE）
- 通用配置枚举（CCE）
- 通用平台枚举（CPE）
- 通用漏洞评分系统（CVSS）
- 通用配置评分系统（CCSS）

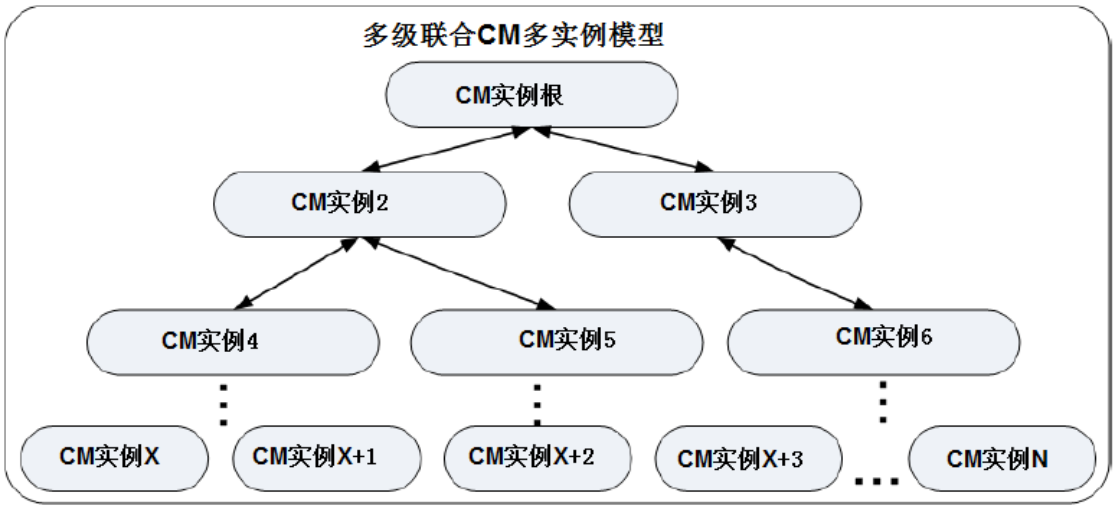
使用规范便于将各种要求输入到厂商工具中。更重要的是，采用规范后可自动化汇总与对比工具输出的内容；否则，很难或根本无法从一大堆工具中汇总及对比系统状态数据。在安全领域里，安全内容自动化协议（SCAP[19]）与国家漏洞数据库（NVD[20]）可提供多种规范，为策略措辞及系统状态数据标准化提供了坚实的基础。关注安全的 CM 实现可能会用到 SCAP，但不限于此类规范。还有许多其他规范在制订过程中，可以支持 SCAP 覆盖范围之外的 CM 领域。

采集和分析/评分子系统从内容子系统获取内容，这样，采集子系统采集的是正确的数据，而分析/评分子系统则可根据组织政策对数据进行恰当分析与评分。

CM 实例并不一定要有内容子系统，但是在组织的 CM 实现中应有至少一个内容子系统。为组织的 CM 实现确定内容子系统的数量是也是一种组织政策。若组织各部门要求使用完全一致的安全配置，一个内容子系统可以满足需要。若有些是通用要求，有些是针对特定环境的特别要求，可构建多层内容子系统，每层满足一种需要。另外，只有当最底层有内容子系统时，可使用分散处理的方法，赋予组织内各部门最大的灵活性，定义自己的安全要求，但是这在汇总及比较 CM 结果时会很麻烦。

5.3 多级能力

大型组织一般需要多个 CM 实例，部分原因是需要避免将所有的安全数据汇总到一个库中，还有部分原因是出于组织内部结构的需要，这些部门独立管理自己的 IT，他们更希望创建联合 CM 实例。CAESARS 框架扩展支持这个需求，将 CM 实例组成树形结构，构成逻辑层级，如图 11 所示）。



[19] http://scap.nist.gov

[20] http://nvd.nist.gov.

图 11 多级联合持续安全监控实例模型

汇总数据报表及合规信息一般按图中层级向上传递，数据调用与安全配置要求则向下传递。这就限制了向上传递的数据量，保证上一层级可获取更多需要的数据。如前文所述，该模型减少了发送所有的 CM 数据至所有层级所带来的带宽、存储、安全与数据新鲜度问题。

节点之间可进行横向联系（并有下级规范支持），但这并不是 CAESARS 框架扩展模型明确要求的功能。根据组织政策，可赋予 CM 实例自主性(Autonomy)，形成更为紧密的关系，同时保持多级结构。这种情况下，CM 实例或会要求在释放数据或进行额外数据采集时从上级获得人工批准。在接收请求会消耗大量系统资源、需通过计划与调度来尽可能降低组织负荷时，可以采用这个方法。

6. 支撑文档架构

为了帮助组织实施 CAESARS 框架扩展企业架构及子系统模型，我们还单独制订了技术设计规范。这种模块化方法使我们可以根据设计变化及逐步增加的新功能定期更新规范。此外，还有两个单独的技术规范：一个关注的是数据域无关（data domain agnostice）规范，适用于所有的持续监控（CM）实例，另一个关注数据域相关（data domain specific）CM 要求（如资产管理）。这样，我们便可以更频繁地修订数据域相关要求，以适应 CAESARS 框架扩展模型中新增的数据域（如漏洞管理）。图 12 展示了支持技术 CM 实现的计划出版物模型。

数据域无关规范关注的是任何 CM 实现中都必须包括的工作流，不受数据域限制。组织可利用这些工作流采集 CM 数据并解决数据冲突、分析、评定并储存结果。这样，对于不同消费者的各种查询请求，可以提供结果检索。通过这种方式，为组织提供了态势感知能力。要启用工作流，我们须在 CM 子系统与部件之间定义必要接口，每个接口都有通信规范保证 CM 方案所涉及产品间的互通性（可使用如资产报告格式（ART）和资产识别（AI）等的 NIST 规范）。最后，我们为每个子系统与部件提供规范，描述实现工作流的必要功能。

数据域相关规范描述子系统、部件、接口所要支持的特定数据域。根据信息技术与身份管理委员会（ISLMC）的 CM 子群组要求，我们的最初关注点是为资产、配置及漏洞管理提供规范，这些规范将上级数据无关规范与针对特定数据域的下级通信规范绑定。对于我们最初关注的领域，我们会充分利用如 SCAP 之类的安全自动化标准，而上级数据域无关规范会充分但并不唯一利用 ARF 与 AI。

7. 结论

本文件为实现持续监控（CM）能力提供了一个企业架构与子系统模型，该模型以 CAESARS 为基础，增加了一些新功能，尤其适用于大型组织。

有些组织设计了自己的 CM 系统，本模型对其也适用。但是，只有将模型与 NIST IR 7799 和 NIST IR 7800 中的下级技术规范结合，并且厂商工具采用了这些规范后，模型才能发挥其最大效用。因此，我们会与厂商群体紧密合作，以协助规范的使用与审查。

我们已设计了下级规范，以加强通用功能，使厂商产品与客户获益。厂商工具在采用 CM 规范后，组织就可以使用现有安全工具构建 CM 实现。在创建此类实现时，集成成本将会因为工具采用了规定的互通标准而大幅度削减。此外，使用该模型的 CM 实现具有互通性，在多个组织间（即便如整个美国政府那么庞大的组织）实现统一报表、数据分析及关联。

附录 A：缩略语

本附件列出了文中出现的部分缩略语的定义。

AI	Asset Identification	资产识别
AO	Authorizing Official	授权主管
ARF	Asset Reporting Format	资产报告格式
ATO	Approval to Operate	批准后方可经营
CAESARS	Continuous Asset Evaluation, Situational Awareness, and Risk Scoring	持续资产评估、态势感知与风险评分
CC	Collection Controller (a Task Manager component)	采集控制器
CCE	Common Configuration Enumeration	通用配置枚举
CCSS	Common Configuration Scoring System	通用配置评分系统
CIO	Chief Information Officer	首席信息官
CM	Continuous Monitoring	持续监控
CPE	Common Platform Enumeration	通用平台枚举
CVE	Common Vulnerabilities and Exposures	通用漏洞披露
CVSS	Common Vulnerability Scoring System	通用漏洞评分系统
DE	Decision Engine (a Task Manager component)	决策引擎（任务管理器部件）
DHS	Department of Homeland Security	美国国土安全部
DOD	Department of Defense	美国国防部
DOS	Department of State	美国国务院
EA	Enterprise Architecture	企业架构
ECMC	Enterprise Continuous Monitoring Capability	企业持续监控能力
ESB	Enterprise Service Bus	企业服务总线
FDCC	Federal Desktop Core Configuration	联邦桌面核心配置
FE	Framework Extension	框架扩展
FISMA	Federal Information Security Management Act	联邦信息安全管理法案
HIPPA	Health Insurance Portability and Accountability Act	健康保险便利和责任法案
IAD	Information Assurance Directorate	NSA 信息保护署
IR	Interagency Report	跨部门报告
ISIMC	Information Security and Identity Management Committee	信息技术与身份管理委员会
ISSLOB	Information Systems Security Line of Business	信息技术安全业务线
IT	Information Technology	信息技术
ITL	Information Technology Laboratory	信息技术实验室
NIST	National Institute of Standards and Technology	国家标准与技术研究院
NIST IR	National Institute of Standards and Technology Interagency Report	国家标准与技术研究院跨部门报告
NIST SP	National Institute of Standards and Technology Special Publication	国家标准与技术研究院特别刊物
NSA	National Security Agency	国家安全局
NVD	National Vulnerability Database	国家漏洞数据库
OCIL	Open Checklist Interactive Language	开放检查表交互式语言

OMB	Office of Management and Budget	管理和预算办公室
OSD	Office of the Secretary of Defense	国防部长办公室
OVAL	Open Vulnerability and Assessment Language	开放式漏洞和评估语言
QO	Query Orchestrator (a Task Manager component)	查询编排器（任务管理器部件）
SCAP	Security Content Automation Protocol	安全内容自动化协议
SOA	Service-oriented Architecture	面向服务架构
SOX	Sarbanes Oxley	萨班斯-奥克斯利法案
SP	Special Publication	特别刊物
STIG	Security Technical Implementation Guide	安全技术执行指南
US-CERT	United States Computer Emergency Readiness Team	美国计算机应急准备小组
USGCB	United States Government Configuration Baseline	美国政府配置基线
WS	Web Service	Web 服务
XCCDF	Extensible Configuration Checklist Description Format	可扩展配置清单描述格式

CAESARS 框架扩展：
企业持续监控技术参考模型

网络安全公益译文项目旨在分享国外先进网络安全理念，将网络安全战略性文档翻译为中文，促进国内安全组织在相关方面的思考和交流。该项目由安全加社区发起，安全加社区是国内的网络安全社区，社区欢迎网络安全人士的加入，并致力于交付网络安全问题的解决能力。