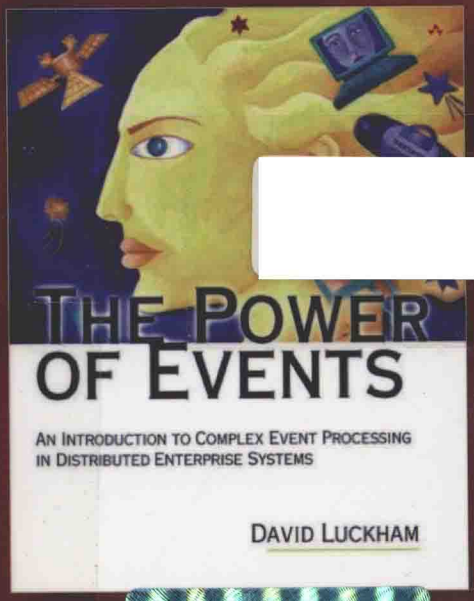
服 | 务 | 计 | 算 | 技 | 术 | 丛 | 书

PEARSON

复杂事件处理导论

〔美〕 David Luckham 著

虎嵩林 刘万涛 译



The Power of Events
An Introduction to Complex Event
Processing in Distributed Enterprise Systems

科学出版社

服务计算技术丛书

复杂事件处理导论

The Power of Events

An Introduction to Complex Event Processing in Distributed Enterprise Systems

〔美〕 David Luckham 著

虎嵩林 刘万涛 译

科学出版社

北京

图字：01-2012-5089 号

内 容 简 介

本书是国际上第一本关于复杂事件处理（CEP）的书籍，由斯坦福大学教授 Luckham 撰写。Luckham 在书中首次完整提出了 CEP 的概念，并从需求、关键技术、架构设计等不同视角对 CEP 进行了全面而系统的阐述。全书分为两大部分。第一部分的前半部细致讨论信息系统的现状，并引出对 CEP 技术的具体需求；后半部则概述 CEP 的基本概念，给出简单的应用案例。第二部分从实现的角度出发，探讨构建 CEP 系统所需的关键技术，包括事件模式的匹配、事件模式语言、事件处理网络等，并辅以生动的案例加以解释和说明。书中最后对 CEP 系统的功能模块划分、架构设计等实现技术进行论述。

该书既有关于 CEP 基本概念及其应用的详细介绍，又有针对 CEP 系统实现技术的具体探讨，还有生动易懂的案例分析，是一本广泛适宜于企业管理者和 IT 系统研究者、开发者与运维者的技术书籍。

图书在版编目（CIP）数据

复杂事件处理导论/（美）勒克姆（Luckham, D.）著；虎嵩林，刘万涛译.
—北京：科学出版社，2015.10
（服务计算技术丛书）
书名原文：The Power of Events: An Introduction to Complex Event Processing in Distributed Enterprise Systems

ISBN 978-7-03-045725-7

Ⅰ. ①复… Ⅱ. ①勒… ②虎… ③刘… Ⅲ. ①互联网络-网络服务器-研究 Ⅳ. ①TP368.5

中国版本图书馆 CIP 数据核字（2015）第 224130 号

责任编辑：余 丁 闫 悦 / 责任校对：桂伟利
责任印制：张 倩 / 封面设计：迷底书装

科学出版社 出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

文林印务有限公司 印刷
科学出版社发行 各地新华书店经销
*
2015 年 10 月第 一 版 开本：720×1 000 1/16
2015 年 10 月第一次印刷 印张：19 1/4
字数：368 000

定价：98.00 元
（如有印装质量问题，我社负责调换）

前　言

复杂事件处理(complex event processing,CEP)是帮助我们理解和控制被事件驱动的信息系统的一组技术和工具。今天,任意一种信息系统,从互联网到手机,都在被事件所驱动。那么什么是复杂事件呢?它就是一类特别的事件,仅当很多其他类型的事件发生后才会产生。

举例来说,假设你在自己喜欢的汽车销售商店看到了一辆钟爱的轿车。那辆车之所以能够停放在展厅里,就是因为已经发生过了一系列其他的事件,包括销售商的库存控制系统中的事件、生产事件、运输事件、海关的入关事件等。当然,当你在展厅中看到自己想要的汽车时,并不会追问这是为什么或者是如何做到的。但如果你没有看到理想的车型、结构或者颜色,并向店员询问起原因的时候,你将会得到细致的解答,涉及一连串如销售商得到的分配配额、工厂里的货物积压或者其他一些因素。实际上,正是这些因素影响着因果历史链条中的那些事件,并最终把你所中意的轿车带到了你的面前。

这个例子说明了 CEP 背后的一个基本思想。事件之间存在着因果、时序以及构成关系等各种形式的联系。当 CEP 技术被应用到电子信息系统中时,它就可以利用事件之间的关联问答一些问题,例如,“我们的系统是否在为用户提供正确的服务”,“我们的船是否会按时到达”,以及“是否有人正在试图盗窃我们的信息”。在现有的事件驱动的信息系统上,CEP 为事件的处理提供了一个新的维度。

为何会存在对 CEP 的需求?让我们来简要地审视一下当前的现状。

当今的信息社会构建在信息收集和共享的基础上。所有的机构——商业的、政府的还有军事组织——都依赖于电子信息的处理。他们所需要的基础骨干(foundational backbone) 就是这样一个被称为一个组织结构的“信息技术层”(或 IT 层)的基于计算机网络的分布式计算系统。过去十年中,为了应对日益增长的自动化、电子商务以及互联网爆炸的需求,这些系统的应用范围迅速扩张。我们付出了巨大的技术投入,以使这些 IT 系统更加高效,使之有能力处理规模越来越大的信息,并同其他的系统协同工作。今天我们生活在一个开放企业(open enterprise)的时代,商务活动和信息的流动跨越了组织和国家的边界,社会也开始越来越依赖 IT 系统。

相比之下,对于理解 IT 系统发生了什么这一日益突出的问题方面的研发投入却又明显不足。当发生了一个危机时——一个拒绝服务攻击或者一个系统的错

误——我们开始根本不知道发生了什么或者应该如何去应对，因此在善后处理中，需要争分夺秒地忙碌数个星期去寻找其根源。毫无疑问，我们需要更好地理解并且控制自己的核心信息基础设施。

IT 系统中的许多信息从来就没有被充分认识。消息或者说事件就像毫无关联的通信片段，在我们的信息系统中无声无息地来回往复地传输。它们其实蕴含着巨大威力。当这些事件被聚集到一起并关联（correlated）起来，且它们之间的关系被充分理解时，将会产生丰富的信息。我们需要一种新的技术以利用全球信息系统中的事件威力，而这正是本书的关注点。

关于 CEP，我们需要讨论几点——它是什么，以及用在哪里。

CEP 由一些非常简单的技术构成，融合了许多新旧技术。它们中有些已经在其他的计算机应用领域中享有盛名，如智能程序中基于规则的系统；有些则是新兴的技术，如在大规模分布式计算机系统中跟踪事件的因果历史，或者利用事件的模式以及事件之间的关系来识别出那些由成百上千个 IT 系统中的简单事件所引发的复杂事件。在 CEP 中，这些新技术将会和那些为大众所熟识的技术一起，被整合到一个统一的框架中。

金融交易就是这种电子复杂事件的一个例子，它可能涉及全球交易网络上的一组金融合约，由多个商业银行和券商参与到交易行为当中。一个交易完成的事件本身可能就是其他众多简单事件的结果：在两三天时间内数百条电子消息以及实体被存储到位于世界各地的若干个不同的数据库中。这些简单事件并不需要按照一个优美的线性顺序一个接一个地发生。有些事件可能彼此独立地同步发生，却与来自其他交易事务的事件混合在一起。我们在交易网络中应用 CEP 技术，不仅可以识别何时发生了复杂的事件，更重要的是，可以预测它是否要发生，或者它是否正在偏离预期的发展轨道而不可能发生，还可以追本溯源，探知其背后的原因。

CEP 在信息系统的挑战中具有非常广泛的应用空间，其中包含：

（1）互联网以及电子交易市场上的业务流程自动化；

（2）从生产线到空中交通领域的自动调度和控制计算机系统；

（3）网络监控以及性能预测；

（4）计算机系统的入侵或者攻击意图检测。

CEP 的广泛应用有一个根本性的原因，那就是所有的信息系统都是事件驱动的。确切地说，一个系统或者系统上运行的一个应用，都依赖于不同类型的事件。网络事件与数据库事件不同，而数据库事件也有别于金融交易事件。但是，CEP 的核心主题就是：这些不同的事件都相互关联。CEP 提供了定义和分析利用事件间关系的技术。CEP 可以应用到计算机应用、网络，或者一个信息系统中的任意类型的事件上。事实上，其中的一个技术就是让你将自己的事件定义成为计算机

系统中的事件模式。当事件发生时,CEP 会让你看到它。这是理解系统中正在发生什么的一个行之有效的方法。

这将我们带到一个新的要点上——柔性。CEP 允许用户在任何时间定义他们所感兴趣的事件。根据用户个体的角色和视角的不同,事件的兴趣可以是低层次的网络监控预警或者是高层次的企业管理智能信息。不同类型的事件可以同时被定义并被监控。另外,事件兴趣的定义,包括事件的视图以及事件的行为,都可以在系统运行中实时在线地更改。

CEP 的用户可以是人,也可以是自治的进程。由于管理企业的流程变得更加复杂,在商业交易中,支持公文流转的线性工作流技术已经无力管理开放的电子企业。未来,为了得到企业所操作的特定类型的事件,企业管理流程将与复杂事件集成在一起。

下面简单介绍本书的结构以及读者可以期待的内容。首先,本书包括两个部分。

第一部分服务于对信息社会的不同侧面感兴趣的一个庞大的读者群,涉及电子商务、互联网、B2B 协同,或者是普遍意义上的电子信息处理等。此部分回答关于 CEP 的两个问题:它为何而生——也就是说,CEP 可以被用来解决信息社会的哪些类型的问题;它是什么——提供一个关于 CEP 基本概念和易懂的应用范例的简单介绍。

第一部分包括 1 ~7 章。前面 4 章描述能够应用 CEP 的 IT 系统中的一些问题。后面 3 章介绍 CEP 的基本概念,例如,"事件"是什么,事件之间的因果和时序关系,事件的模式,事件的层次化结构,以及如何应用它们来解决前 4 章提到的问题。

第二部分包括从第 8 章开始的所有后续章节,服务于具有软件领域知识背景的信息系统专家。该部分给出开发 CEP 系统的技术细节以及 CEP 应用的案例分析。此部分的目的是描述实现 CEP 应用并解决现实世界真实问题所需的内容。它首先包括一个复杂事件处理语言、反应式(reactive)事件模式规则以及事件模式约束的详尽描述。其次,它展示如何利用事件模式规则和约束来设计事件处理代理(event processing agent,EPA)以及通信代理的体系结构,并进而构造完整的解决方案。此部分还包括案例分析,在一个章节的限制范围内尽可能全面、详尽地加以论述。

本书的第 15 章解决如何构造 CEP 基础设施。我们可以在这一章中纵览当今商务世界中已有的基于分布式计算、互联网以及私有网络的事件驱动的应用。可以预期,考虑到中间件、Java 社区、. Net 社区以及安全社区等的发展趋势,CEP 必将发展成为一个具有竞争优势的技术。本章关注如何利用这些研发进展来构造一个 CEP 的基础设施。

关于参考文献我们需要强调一下,互联网技术无时不在迅猛变化,任何人尝试

给出的完整参考文献都会在六个月内变得过时。不仅如此，任何不尽完整的参考文献对一些人都是不公平的。假设所有的读者都可以访问互联网并能够搜索当前的参考文献，例如，“中间件”或者“应用服务器”，因此，我倾向于仅仅包括一小部分参考文献，包含网站的通用的参考地址或者是一些不易获取的研究文章的引用。

当今社会，任何试图查看并控制 IT 系统的技术都会被一些人认为是与安全或者隐私相冲突的。实际上，CEP 可以提供一个基础以调解一些可能的冲突，然而，我在这里不能也不会去讨论这个话题。

简单介绍一点本书的历史。CEP 发源于斯坦福大学一个名为 RAPIDE 的基于事件的模拟系统的研究项目。这项研究工作开展于 1999 ~ 2000 年。从 RAPIDE 中演化出了一些早期的 CEP 应用实验，监视在商业中间件之上实现的小型通信系统，或者识别一所大型大学 IT 层中黑客热衷于制造的、正在发生的安全威胁。这些项目在 http://pavg. stanford. edu/rapide/和 http://pavg. stanford. edu/cep/两个网站中有文档说明。

致　谢

我必须感谢所有为 RAPIDE 和 CEP 的发展作出贡献的人。首先是在过去十年中参与 Stanford Program Analysis and Verification Group(PAVG)的研究工作的学生和工作人员,尤其是开发 RAPIDE 基于事件的仿真系统和早期 CEP 原型系统的人。由于篇幅限制,我无法在这里一一列出他们的名字,但读者可以在 http://pavg. stanford. edu/rapide/的 contributors 部分找到。

特别感谢下列 PAVG 的长期成员 Doug Bryan、Walt Mann、John Kenney、Louis Perrochon、Sigurd Meldal、James Vera、Wolfgang Polak、Alex Santoro、Benoit Gennart、Woo-Sang Park 和 Frank Belz (TRW)。他们不断地讨论并实现了本书中描述过的概念,并通过实验证实了这些概念的有效性。我总是回顾这段日子,他们是一群了不起的研究者,能和他们一起工作是我的荣幸。

我还要感谢国防先进研究项目局(DARPA)对 PAVG 等项目的支持。

最后,我衷心感谢本书的审稿人 Armond Inselberg、Doug Bryan、Geoff Mendal 和 Louis Perrochon,他们在很多方面给予我帮助。

斯坦福大学电子工程系名誉研究教授

David Luckham

目　录

第二部分　构建 CEP 的解决方案

第一部分

复杂事件处理简介

- 保持人类对当今电子信息系统的控制权的挑战
- CEP 的基本概念
- CEP 如何应对这些挑战

第 1 章　全球信息社会和新技术的需求

- 信息系统中的事件无所不在
- 互联网以及意大利面条式的全球通信体系的扩张
- 企业系统架构中的分层结构
- 全球电子交易——理解正在发生着什么
- 敏捷系统——未来的现实抑或仅仅是一个梦
- 一个开放的电子社会能够自我保护吗?
- 信息聚合的风暴——全球化的一致性或者全球的混乱

利用计算机系统在全球范围内进行信息处理已经成为 21 世纪人类生活不可或缺的组成部分。它负责运行政府、工业企业、运输系统、医院以及应急服务。在新的千年中,它无疑是全球经济和全球电子交易的基础。

在世界各地,信息处理系统按着“Web 速度”飞速增长,仅仅比科幻中的“Warp 速度①”稍慢一点。互联网或者说 Web 一直是人类社会发展的重要驱动力。新兴的技术被研究出来以促进信息系统的这种飞速增长。它们被用来构建这些信息系统,使系统更加快捷高效,从而能够处理和路由越来越庞大的信息。新的应用层出不穷,将我们引入深化 IT 系统应用的崭新道路之上。

但是,我们尚未研发出相应的基础技术,以帮助人类监控和管理流动在全球信息系统中的信息。事实是:如果我们不了解这些系统中正在发生着什么——我指的是以人类理解的方式“知道”——我们就无法保护这些系统,并且无法利用它们使这些系统的优势最大化。本章将描述这个基于事件的世界以及其中的一些挑战性问题。

1.1　无处不在的分布式信息系统

分布式计算和信息系统的典型例子是那些支持商业企业自动运行的系统,例如,银行和金融交易处理系统、数据仓库系统以及自动化工厂。互联网促进了分布式信息系统的发展,并使这种发展不断提速,超越了单个企业的范围,跨越了企业之间的边界。企业间的信息通信为交易伙伴关系和业务协作的自动化奠定了基础。

① 这里指的是科幻电影《星际旅行》中的装备有曲速引擎飞行器所能够达到的速度。