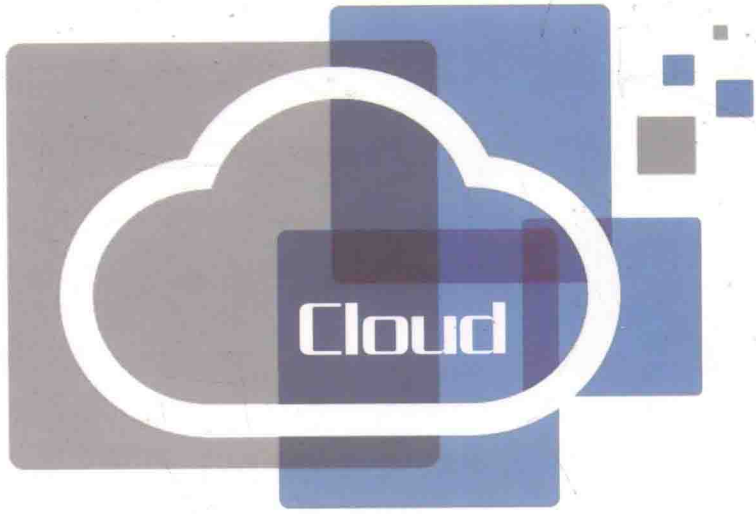
Federal Cloud Computing

——The Definitive Guide for Cloud Service Providers



美国联邦云计算

——云服务提供商权威指南

[美]Matthew Metheny 著　刘东红　何重德　李 瑛　等译

于 全　审校

国防工业出版社

National Defense Industry Press

美国联邦云计算

——云服务提供商权威指南

Federal Cloud Computing

——The Definitive Guide for Cloud Service Providers

[美]Matthew Metheny 著

刘东红 何重德 李 瑛 郭长国
邹 恒 刘俊平 孙学涛 赵 静 译
于 全 审校

国防工业出版社

·北京·

著作权合同登记　图字:军-2014-168号

图书在版编目(CIP)数据

美国联邦云计算:云服务提供商权威指南/(美)马修·梅思尼(Matthew Metheny)著;刘东红等译. —北京:国防工业出版社,2017.3

书名原文:Federal Cloud Computing—The Definitive Guide for Cloud Service Providers

ISBN 978-7-118-11114-9

Ⅰ. ①美… Ⅱ. ①马… ②刘… Ⅲ. ①云计算-研究-美国

Ⅳ. ①TP393.027

中国版本图书馆 CIP 数据核字(2017)第032539号

美国联邦云计算——云服务提供商权威指南

Federal Cloud Computing——The Definitive Guide for Cloud Service Providers

Translation from the English language edition:

Federal Cloud Computing——The Definitive Guide for Cloud Service Providers By Matthew Metheny

copyright © 2013 by Elsevier, Inc.

Syngress is an imprint of Elsevier

225 Wyman Street, Waltham, MA 02451, USA

All rights reserved.

本书简体中文版由 Elsevier, Inc. 授权国防工业出版社独家出版发行。

版权所有,侵权必究。

※

國防工業出版社出版发行

(北京市海淀区紫竹院南路23号　邮政编码100048)

北京嘉恒彩色印刷有限责任公司

新华书店经售

*

开本 710×1000　1/16　**印张** 20　**字数** 375千字

2017年3月第1版第1次印刷　**印数** 1—2000册　**定价** 99.00元

(本书如有印装错误,我社负责调换)

国防书店:(010)88540777　　发行邮购:(010)88540776

发行传真:(010)88540755　　发行业务:(010)88540717

谨以此书献给我出色的妻子。她的支持给了我撰写这本书的动力，这是无法用简单的言语表达的。感谢她持续的耐心、鼓励以及这段时间以来的无私奉献。感谢她即使在阅读和编辑不感兴趣的一些主题时，依然付出的灵感和难以置信的热情。

写给我亲爱的、深爱的妻子埃琳(Erin)

谢谢你不知疲倦地站在我的身边，支持我前进的每一个步伐。在人的生命中，很多时候的任务看起来很难，你的鼓励和祝福使我获得了巨大的力量。

在遇到挑战的时候你时常会出现。非常荣幸能和你一起分享成功的喜悦。

带着无限的爱写给我的妻子

纪念罗恩·克诺德(Ron Knode)

罗恩是一个天才,微笑的表情,和蔼的语言,令人鼓舞的精神状态,以及独特的方式引发人们从不同的视角来思考和观察。有机会认识并得到罗恩的指导我感到非常荣幸。

罗恩,你在许多方面给我留下的印象我将永远不会忘记。

此为试读,需要完整PDF请访问: www.ertongbook.com

作者简介

马修·梅思尼(Matthew Metheny)是一企业咨询集团公司(1ECG)的创始人,该公司是民营咨询公司,提供云战略和体系结构、云安全评估、云迁移和云计算培训等专业服务。梅思尼先生是云安全联盟(CSA)主任委员会的成员、云信任协议(CTP)工作组副组长、CSA 认证的云安全知识认证(CCSK)讲师。在创办 1ECG 公司之前,梅思尼先生在支持联邦政府和私营部门的多个咨询公司担任高级计划管理和经理级的职位,这些公司重点关注行政管理、风险管理、新兴技术和安全规范。此外,他是 FedRAMP. net 的创始人,该网站主要支持云服务提供商和联邦机构解决联邦风险和授权管理计划(FedRAMP)的需求。梅思尼先生拥有马里兰大学信息保证专业的硕士学位和多个国际公认的资格认证。

技术编辑简介

贾妮斯·奥西诺(Janis Orsino)是一个信息技术(IT)安全顾问,有20多年为美国联邦政府提供技术和业务咨询服务的经验,涉及民政部门和国防部门。她目前是一个高级管理顾问,负责IBM全球商业服务、美国联邦网络空间安全和隐私咨询案例。

2009年至2011年,在通过合同委派参与国防领域信息保证计划时,贾妮斯帮助制定联邦风险和授权管理计划(FedRAMP),从起初的重要顾问到国防部联合授权委员会。她还参与了联邦首席信息官理事会,信息安全和身份管理委员会网络和基础设施安全委员会的云计算安全指南的制定工作。

贾妮斯拥有帕克大学社会心理学学士学位、乔治华盛顿大学法律学研究生学历,以及一系列的认证,包括认证的信息系统安全专家(CISSP)、认证的信息系统安全经理(CISM)、风险和信息系统控制领域的认证(CRISC)、GIAC安全领导能力认证(GSLC)和云安全知识认证(CCSK)。

威廉·科林顿(William Corrington)撰写的前言

近年来,“云计算”已作为一种提供 IT 基础设施、资源和服务的模式出现,通过提高 IT 效率、灵活性和创新理念,给各个组织机构带来巨大价值潜力。然而,美国联邦机构作为云计算的较早采用者,已经发现要达成这些效果,还面临着许多挑战和风险。

早期采用者已经发现,使用云服务提供商(CSP)的服务,IT 系统日常配置和交付方式将发生根本性变化。成功采用云计算,还需要改变在安全、隐私、终端用户支持、运行、采办和合同管理方面的方法。云服务提供商也同样面临着挑战,这个新兴市场的许多参与者都是第一次与联邦政府合作。因此,他们不仅需要了解联邦采办流程的细节,而且需要解决各种联邦用户特有的安全、隐私和认证需求。

为了面对这些挑战,并且在联邦政府内促进云计算的采用,《美国联邦云计算战略》于 2011 年 8 月颁布。美国国家标准与技术研究院(NIST)和总务管理局(GSA)在实施这个“云优先”战略的过程中扮演关键角色。NIST 编写了许多专业出版物,提供云计算的定义、体系结构标准和路线图。GSA 制定了联邦风险与授权管理计划(FedRAMP),为美国联邦机构使用云计算定义安全、审计、持续监控和其他运行需求。美国联邦机构和进入联邦市场的云服务提供商都必须遵循这些要求。

我赞赏 NIST 和 GSA 带头发起的开创性倡议。迄今,这些努力已经开创出了独有的新局面,它们必须由希望服务于联邦市场的联邦机构和云服务提供商来指引。目前缺少权威的参考指南,使每个人有一套联邦 IT 标准,用于快速了解联邦云计算战略的目的、目标、实施和运行情况。梅思尼先生的著作填补了这一空白,本书在关于云计算如何以及在何处适合联邦政府,云优先战略的关键组成部分将如何以补充的方式共同发挥作用方面作了全面介绍。

我相信本书对需要成功进入联邦云计算这个五彩缤纷新世界的任何人而言都是宝贵的资源。云服务提供商通过这本书,将对安全和运行需求有更加全面的了解,给联邦机构提供基于云的服务,这些需求是必须满足的。希望提供服务给联邦机构或云服务提供商的云审计员,将从本书中了解到成为第三方评估机

构(3PAO)的详细需求。联邦机构首席信息官(CIO)、首席技术官(CTO)、首席信息安全官(CISO)将更加清晰地了解迁移到云计算将对他们现有的 IT 战略和运行的影响。

云优先战略是正在开展的更大范围的工作,是 21 世纪改革联邦 IT 工作的关键组成部分。本书将给每个希望踏上这段旅程的人提供非常好的指南。

威廉·科林顿

Stony Point Enterprises 公司创始人和首席云战略家

(美国内政部前首席技术官)

吉姆·雷维斯(Jim Reavis)撰写的前言

云计算是人类技术使用的一个划时代的变化。广泛地考虑,它代表着技术转变的方向,即把计算机作为一个整体来使用,具有深刻的意义。正如当初各国的电气化发展、新工业的出现、社会的重新组织以及其他未预料到的结果一样,已经确定无疑地来到了我们的身边。超级计算能力的使用,以前仅限于那些拥有数百万资产的小群体,目前所有的人都可以使用。

个人、小企业主和大型企业对虚拟的无限供应的计算力和存储的按需访问能力,给我们的创新能力带来挑战。从发现新的药物到解开宇宙的奥妙,寻求新的更好的方法改善人类生存条件的方法,我们只怕想不到,不怕做不到。

在偏好受到云计算影响并充分利用云计算方面,政府部门和其他组织机构并没有什么不同。政府部门面临的最大问题很大一部分都可以通过云计算来解决。云计算将迫使政府机构在信息方面更加透明并加强协作。同时,仓促采用云计算而没有合理地考虑其潜力和风险可能会遭遇挫折。《美国联邦云计算——云服务提供商权威指南》一书让我们及时了解什么是云计算,其内在的风险,法规要求,以及相关标准和最佳的案例。

云安全联盟是一个非营利的组织,是在云计算内构建信任方面引领全球的力量。我们热烈祝贺作者,同时也是云安全联盟成员的马修·梅思尼在美国联邦政府云计算这一主题上的杰出贡献。我们认为本书对于关注我们政府 IT 的每个人而言都是必读的。政府用户和提供商都必须了解法规要求、使云计算可用的流程以及最佳案例,以降低风险并安全运行云系统。

云计算不仅存在于未来,而且存在于现在。无论你在这个主题上扮演什么角色,你都需要寻求策略以灵活的方式可靠地采用云计算。《美国联邦云计算——云服务提供商权威指南》帮助读者制定策略提供有益的辅导。

吉姆·雷维斯

云安全联盟执行主任

目　录

第 1 章　联邦云计算战略简介 …… 1
1.1　引言 …… 1
1.2　联邦 IT 的历史回顾 …… 3
1.3　云计算:联邦 IT 转型的推动器 …… 12
1.4　云迁移的决策框架 …… 17
1.5　小结 …… 19
参考文献 …… 20
第 2 章　云计算标准 …… 22
2.1　引言 …… 22
2.2　标准制定入门 …… 24
2.3　云计算标准化的推动器 …… 25
2.4　明确联邦云计算标准 …… 28
2.5　小结 …… 37
参考文献 …… 37
第 3 章　开放源码案例 …… 39
3.1　引言 …… 39
3.2　开源和联邦政府 …… 41
3.3　采用开源软件面临的挑战:采办与安全 …… 45
3.4　开源软件与联邦云计算 …… 48
3.5　小结 …… 51
参考文献 …… 51
第 4 章　公共云计算的安全与隐私 …… 54
4.1　引言 …… 54
4.2　公共云环境中的安全与隐私 …… 56
4.3　联邦隐私法与政策 …… 57
4.4　保护隐私信息 …… 63
4.5　安全和隐私问题 …… 74
4.6　小结 …… 75
参考文献 …… 75

此为试读,需要完整PDF请访问: www.ertongbook.com

第 5 章　应用 NIST 风险管理框架 …… 77
5.1　联邦信息安全管理法案介绍 …… 77
5.2　风险管理框架概述 …… 82
5.3　NIST RMF 流程 …… 86
5.4　小结 …… 125
参考文献 …… 125
第 6 章　风险管理 …… 128
6.1　风险管理引言 …… 128
6.2　联邦信息安全风险管理实践 …… 130
6.3　全企业风险管理概述 …… 132
6.4　NIST 风险管理流程 …… 138
6.5　NIST 与 ISO/IEC 风险管理流程的比较 …… 143
6.6　小结 …… 146
参考文献 …… 147
第 7 章　联邦和国际安全认证标准的对比 …… 148
7.1　引言 …… 148
7.2　认证与认可概述 …… 149
7.3　NIST 和 ISO/IEC 信息安全标准 …… 156
7.4　小结 …… 163
参考文献 …… 164
第 8 章　FedRAMP 入门 …… 166
8.1　FEDRAMP 简介 …… 166
8.2　FEDRAMP 政策备忘录 …… 167
8.3　FEDRAMP 运行概念 …… 173
8.4　第三方评估机构程序 …… 182
8.5　小结 …… 183
参考文献 …… 184
第 9 章　FedRAMP 云计算安全要求 …… 185
9.1　安全控制选择流程 …… 185
9.2　FEDRAMP 云计算安全要求 …… 187
9.3　小结 …… 232
参考文献 …… 232
第 10 章　安全评估与授权:管控、准备与执行 …… 234
10.1　安全评估流程简介 …… 234
10.2　安全评估管控 …… 236
10.3　安全评估准备 …… 238

10.4 执行安全评估计划 …… 247
10.5 小结 …… 248
参考文献 …… 248
第 11 章 持续监控策略 …… 249
11.1 持续监控简介 …… 249
11.2 持续监控流程 …… 255
11.3 FedRAMP 内部持续监控 …… 261
11.4 小结 …… 267
参考文献 …… 267
第 12 章 利用安全自动化,实现高效费比的合规性 …… 269
12.1 引言 …… 269
12.2 CM 参考体系结构 …… 271
12.3 安全自动化标准和规范 …… 279
12.4 运行可视性和连续监控 …… 281
12.5 小结 …… 283
参考文献 …… 284
第 13 章 云服务提供商案例研究 …… 285
13.1 案例研究:“保健交流” …… 285
13.2 应用 FEDRAMP 中的风险管理框架 …… 286
13.3 小结 …… 304
参考文献 …… 304

第1章　联邦云计算战略简介

本章内容

- 引言
- 联邦 IT 的历史回顾
- 云计算:联邦 IT 转型的推动器
- 云迁移的决策框架

1.1　引言

2011 年 2 月,前任美国首席信息官(CIO) Vivek Kundra,发布了“联邦云计算战略”,其中提到了“云战略”①。“云战略”如图 1.1 所示,是美国首席信息官在《联邦信息技术管理改革的 25 项重要实施计划》中提出的云发展路线图六项主要组成部分中的一项。

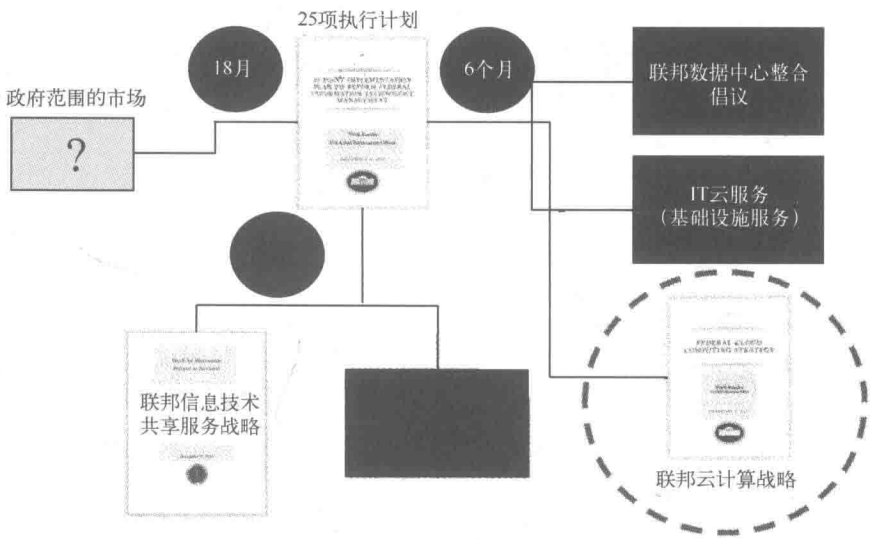


图 1.1　关键执行 IT 改革规划——“云路线图”

① 联邦云计算战略。参见 http://www.cio.gov/documents/Federal-Cloud-Computing-Strategy.pdf。

“云战略”是用于描述美国联邦政府使用云计算技术的战略方法，包括云计算的潜在利益、转型代价以及两者之间的权衡[1]。云战略为联邦政府提供使用云计算的决策框架，联邦机构可参照框架制定各自的云计算使用计划，提升信息技术的投资价值，控制共享设施与投资资金的规模。该框架致力于指导政府将云计算集成到已有的信息技术产品中，推动信息技术管理的变革。

“云战略”建立了一组基础原则和指导方针，通过这些原则和方针，联邦机构中的决策者们能更安全快捷地使用云服务。这个战略赋予联邦机构相应的自主决策职责，他们可自主决策如何向云计算迁移，以支持政府的云优先政策（Cloud First Policy）。云优先政策的目标是使联邦机构主动使用云计算服务，该策略要求联邦机构选择三项“云就绪”①的 IT 服务，从而逐步向安全可靠地云解决方案迁移。

在“云迁移的决策框架”一节中，介绍了一个三步骤的框架，该框架描述了一个成功迁移方案基本而必需的要素②。另外，云优先政策使联邦机构有机会验证他们的迁移方案③，并在迁移过程中分享彼此的经验和教训。该计划鼓励开发“政府就绪”的云服务，满足联邦安全和隐私需求。云优先战略也提出了建设 FedRAMP 的计划需求④⑤。

美国联邦政府从传统的基于资产模式向基于服务的模式转变，不仅是一种技术变革，更是组织内部的文化转型。基于资产的模式重点在于 IT 产品，基于服务的模式则由云计算来推动。向云服务转变还要求组织机构在管理与云服务相关的人员和程序上做出改变⑥。云计算在技术的规划、选择和集成方面的重要性日益显现。基于服务的方法要求联邦机构要学会如何管理服务，管理服务更甚于管理资产。为了有效利用云服务实现资源优化利用，联邦政府在进行战略规划时要充分考虑云计算的效益⑦。另外，联邦机构也必须建立一套新的管理流程，确保云服务能满足信息安全和隐私保护的要求。

---

① 决定哪些 IT 服务需要迁移时，云就绪是风险评估的一个方面。就绪包括以下因素：安全性，服务特征、市场特征、网络设施、应用和数据准备、政府准备以及技术的生命周期。

② 联邦云计算战略中提到的迁移方案应包括：主要里程碑、执行风险、目标资源需求以及云服务上线之后老旧服务的退役计划。

③ 联邦信息技术管理改革的 25 项重要实施计划提到“云计算技术应鼓励使用可用的商业云技术，发展政府云，鼓励地方政府制定私有云的三方面策略中得到发展”。

④ 联邦风险和授权管理计划在第 8 章和第 9 章中详细介绍。

⑤ “政府准备”云服务适用于那些能满足广泛的联邦安全和隐私的需求，包括法律义务、数据安全、隐私相关信息的保护、完整性、连接控制、监管和安全管理。

⑥ 参见 OMB A－11 公告号第七部分“固定资产的规划、预算、使用和管理”。http://www.whitehouse.gov/omb/circulars_all_current_year_all_toc。

⑦ 参见 OMB A－11 号公告第六部分“战略规划的准备和提交，年度性能计划，年度程序性能报告”。http://www.whitehouse.goc/omb/circulars_all_current_year_all_toc。

提示：

联邦 IT 战略规划中使用云计算的要点。

自从联邦机构开始使用信息技术以来，政府级别 IT 战略规划中信息和信息技术管理被作为一种体系型挑战越来越受重视。早在 1960 年①，美国总审计局（GAO）②“呼吁重视政府执行部门内的中长期规划，通过有效的规划提高自处理设备的使用效率，降低投资成本”[2]。

然而，1980 年③，联邦信息技术的管理当局已成为美国联邦政府中央机构的一部分。美国管理和预算办公室（OMB）被赋予了政府级别的责任“监督信息资源在提高政府服务性事务方面的效率以及经费的使用情况”[3]。要求联邦机构指派一个关键部门的官员（普遍认为是首席信息官）兼职监督部门级别的信息资源管理（IRM）④。随着政府级别的信息资源管理演变，机构首席信息官（Agency CIO）新增额外的职能，包括“为其他所有政府机构制定信息和信息技术管理的战略规划⑤”[4]。

IT 战略规划⑥特别期望通过云计算显著提高生产力。机构首席信息官将 IT 战略规划调整至部门级别的战略规划⑦时要更加结合实际，使开发与监管的性能参数可直接用于评估云服务的经济效益。因此，信息化局制定的 IT 战略规划要侧重标准的建立，这些标准应能提出可量化的方法来估算在云计算方面投资所获得的效益。

1.2 联邦 IT 的历史回顾

在“云战略”一文中，联邦 IT 环境被贴上了“资产利用低效，资源需求琐碎，系统冗余，管理困难，新能力形成周期长”[1]等标签。联邦 IT 环境的这些特征是由于 IT 资产过多又疏于管理，问题累积多年所造成的。

---

① 回顾联邦政府的自动数据处理发展。

② 美国总审计局是在 2007 年 7 月 7 日根据“Budget and Accounting Act of 1921”法案建立的，审计总局更改为政府受托责任办公室。

③ 参见“Paperwork Reduction Act of 1980”。http://www.archives.gov/federal-register/laws/paperwork-reduction。

④ 联邦首席信息官：提升信息技术管理的机遇“信息资源管理是完成部门任务并提高效率的一个有效过程”。

⑤ 参见 OMB 公告 A-130 号，http://www.whitehouse.gov/omb/fedreg_a130notice。“IRM 战略规划是部门的 IT 视角或路线图，用于联合信息资源、商业战略和投资决策。”

⑥ 参见 OMB 公告 A-130 号，http://www.whitehouse.gov/omb/fedreg_a130notice。“Clinger-Cohen 法案指导联邦机构在共同的目标下合作，使用信息技术提高生产率、效率，加强联邦程序的互操作、安全和共享政府级别的信息资源设施。”

⑦ 参见 OMB 公告 A-130 号，http://www.whitehouse.gov/omb/fedreg_a130notice。“IRM 战略规划应支撑部门战略规划，描述信息资源师如何帮助业务的，以确保 IRM 集成组织规划、预算、经费管理、采购、人力资源管理以及计划决策。”

本节着重介绍美国联邦政府历史上几个重要的时间点，在这几个关键的时间点中，美国联邦政府大规模采购 IT 产品导致联邦 IT 预算激增。图 1.2 概略展示了美国联邦政府的 IT 预算是如何随着 IT 新技术发展而逐步演变的。

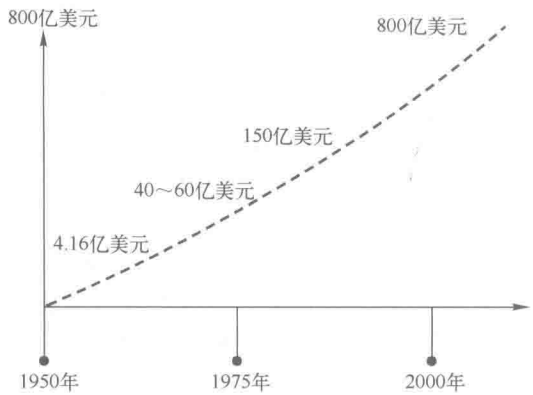


图 1.2　联邦 IT 产品的发展历史

本文的回顾始于大型机（高度集中环境）时代，结束于移动时代（高度分布式环境）。为了表达演变过程的完整性，还简要回顾了联邦 IT 法规和政策的演变，主要涉及美国联邦政府如何进行采办和治理，同时还包括对隐私和安全的管理。

1.2.1　早期的大型机时代

现代计算机的起源[①]与美国政府直接相关。作为计算机第一位重要的用户[②]，美国政府最终成为计算机技术革新与研究最主要的经济来源。早些年，计算机非常昂贵，速度慢，性能低，笨重[③]，只有美国政府和研究机构使用。尽管如此，美国政府仍然持续地支持计算机技术的发展。尽管早期计算机只应用于军事[④]，但是最初的投资最终推动了一个庞大的工业产业的发展，也形成了今天美国政府使用计算机的局面。

20 世纪 50 年代之前，美国联邦政府使用的第一台数字计算机[⑤]主要服务于

① Maunchly 与 ENIAC 计算机的发展。参见 http://www.library.upenn.edu/exhibits/rbm/mauchly/jwmintro.html。

② 参见 Whirlwind 项目报告。http://dome.mit.edu/handle/1721.3/37456。

③ 数字经济的兴起“世界上第一台可编程的计算机，电子数字电路和计算机（ENIAC），高 10 英尺，宽 150 英尺，花费百万美元，每秒只能进行 5000 次操作”。

④ 美军研究实验室（ARL）计算历史。参见 http://www.arl.army.mil/www/default.cfm?page=148。

⑤ 历史：Univac I. 人口普查的历史职员。参见 http://www.census.gov/history/www/innovations/technology/univac_html。

此为试读，需要完整PDF请访问：www.ertongbook.com