奇安信 网络安全科普丛书

INCIDENT RESPONSE

Cyber Security

奇安信安服团队
/著/

应急响应

网络安全的预防、发现、处置和恢复

读网络安全科普书 看网络安全新鲜事

洞悉无处不在的威胁 掌握保护自己的武器
让网络更安全 让世界更美好

中国工信出版集团
電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

网络安全科普丛书

INCIDENT RESPONSE

Cyber Security

奇安信安服团队

/著/

应急响应

网络安全的预防、发现、处置和恢复

電子工業出版社
Publishing House of Electronics Industry
北京 · BEIJING

内 容 简 介

本书的内容将前沿的网络安全应急响应理论与一线实战经验相结合，从科普角度介绍网络安全应急响应基础知识。本书共 5 部分(17 章)，内容包括：网络安全应急响应概述、网络安全应急响应实践、网络安全应急响应技术与平台、网络安全应急响应人才培养、网络安全应急响应典型案例。本书旨在为全国网信干部提供理论指南、实践指导和趋势指引，也可以作为从事网络安全应急响应研究、实践和管理的专业人士的培训教材。

图书在版编目（CIP）数据

应急响应：网络安全的预防、发现、处置和恢复 / 奇安信安服团队著. —北京：电子工业出版社，2019.8
ISBN 978-7-121-36985-8

I. ①应… II. ①奇… III. ①计算机网络－网络安全－技术培训－教材 IV. ①TP393.08

中国版本图书馆 CIP 数据核字（2019）第 131885 号

责任编辑：戴晨辰
印　　刷：涿州市京南印刷厂
装　　订：涿州市京南印刷厂
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　　邮编：100036
开　　本：787×1092　1/16　印张：16.25　　字数：318.5 千字
版　　次：2019 年 8 月第 1 版
印　　次：2019 年 8 月第 1 次印刷
定　　价：65.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888，88258888。
质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。
本书咨询联系方式：dcc@phei.com.cn。

前言

Preface

当前，网络空间安全形势日益严峻，我国的政府机构、大中型企业的门户网站和重要核心业务系统常成为攻击者的主要攻击目标。为妥善处置和应对政府机构、大中型企业关键信息基础设施可能发生的突发事件，确保关键信息基础设施的安全、稳定、持续运行，防止给相关部门造成重大影响和经济损失，需进一步加强网络安全与信息化应急保障能力。网络安全应急响应服务是安全防护的最后一道防线，巩固应急防线对安全能力建设至关重要。

考虑到现今市场上网络安全应急响应相关图书极其缺乏，结合奇安信集团安服团队拥有的为全国各地 600 余家政府机构、大中型企业提供网络安全应急响应服务的经验，以及拥有的安全理念和新技术，我们决定编写本书，将工作中的经验、理念、实践技术分享给广大需要的读者。

本书旨在为网信工作的领导干部提供理论指南、实践指导和趋势指引，也可以作为从事网络安全应急响应研究、实践和管理等各类专业人士的培训教材。

本书通俗易懂，书中对所有的网络安全应急响应相关知识的介绍不涉及复杂的技术细节，重点介绍基本原理、解决思路和典型案例。作为一本科普图书，读者不需要具备通信、计算机或网络安全方面的专业知识，即可顺畅阅读本书的大部分内容。

本书内容共 5 部分。

第 1 部分为网络安全应急响应概述，主要介绍网络安全应急响应基本概念、

当前面临的形势与挑战、未来的发展趋势，国内外网络安全应急响应相关法律法规和指导机构，网络安全应急响应的标准与模型等。主要目的是让读者了解网络安全应急响应的概念及其重要意义，并从宏观层面掌握一些方法论，形成思维体系。

第 2 部分为网络安全应急响应实践，主要介绍如何建立网络安全应急响应体系、前期的攻防实战演习、发生安全事件后的具体处理方法与事后总结，以及重要活动网络安全应急保障等，以便帮助读者在具体的工作中解决一些实际问题。

第 3 部分为网络安全应急响应技术与平台，主要介绍网络安全应急响应中的关键技术、常用的平台工具，以及漏洞响应平台的基础支持等，以便为读者提供更多的知识储备。

第 4 部分为网络安全应急响应人才培养。保护网络空间安全，高水平的专业网络安全人才是核心要素。未来网络空间中的对抗，其实质是网络安全人才质量、数量，以及对人才合理调配、运用的综合比拼。因此，本部分主要介绍当前比较流行的网络安全人才培训模式，以及网络安全应急响应相关的知识体系和资质认证。本部分内容可为相关单位网络安全人才培养提供参考。

第 5 部分为网络安全应急响应典型案例。本部分内容结合奇安信集团为上百家政企机构提供安全服务和应急响应的工作经验，总结不同行业的典型案例与解决方案，可让读者更加生动地了解实际工作中可能遇到的安全事件和处理方法。

此外，在附录部分还提供了勒索病毒和恶意挖矿的网络安全应急响应自救手册，能够帮助读者在遇到相关问题时快速解决问题，恢复生产经营与工作活动。

本书的出版要感谢奇安信集团各业务线同事的支持，包括但不局限于：张翀斌、张龙、汪列军、丁丽萍、张永印、马红丽、刘洋、裴智勇、刘川琦、鲍旭华、郑新华、李忠宇、苏和、刘雪花、黄蒙、李闯、张鑫、熊瑛、罗博文、杨毅、赵佳伟、白雪、崔凯、贾斌、顾鑫、李志全、翟少君、李明、许旺、胡怀亮、吕欣研、孙红娜、高继明、胡晓。还要感谢电子工业出版社戴晨辰编辑的大力支持，以及其他工作人员的辛勤付出。

由于作者水平所限，不妥之处在所难免，恳请广大网络安全专家、读者朋友批评指正。

作　者

奇安信安服团队简介

奇安信安服团队是奇安信集团旗下为用户提供全周期安全保障服务的团队。奇安信安服团队以网络攻防技术为核心，聚焦威胁检测和响应，在云端安全大数据的支撑下，为用户提供咨询规划、威胁检测、攻防演习、应急响应、预警通告、安全运营等一系列实战化的服务。

奇安信安服团队在数据分析、攻击溯源、应急响应、重保演习等方面有丰富的实战经验，曾多次参与国内外知名 APT 事件的分析溯源工作，曾参与 APEC 会议、G20 峰会、两会、纪念抗战胜利 70 周年阅兵、上合组织峰会等国家重大活动的网络安全保障工作，获得国家相关部门和广大政企单位的高度认可。

自 2016 年以来，奇安信安服团队平均每年参与处置各类网络安全应急响应事件近千起，救援部门的服务对象涵盖各个行业，处置事件包括服务器病毒告警、PC 病毒告警、WebShell 告警、木马告警、数据泄露等多种类型，为用户挽回经济损失数千万元。

目录

Contents

第 1 部分　网络安全应急响应概述

第 2 部分　网络安全应急响应实践

第1部分 Part 1 网络安全应急响应概述

第 1 章

网络安全应急响应综述

1.1 什么是应急响应

应急响应，其英文是 Incident Response 或 Emergency Response，通常是指一个组织为了应对各种意外事件的发生所做的准备，以及在事件发生后所采取的措施。其目的是减少突发事件造成的损失，包括人民群众的生命、财产损失，国家和企业的经济损失，以及相应的社会不良影响等。

应急响应所处理的问题，通常为突发公共事件或突发的重大安全事件。通过由政府或组织推出的针对各种突发公共事件而设立的各种应急方案，使损失降到最低。应急响应方案是一项复杂而体系化的突发事件应急方案，包括：预案管理、应急行动方案、组织管理、信息管理等环节。其相关执行主体包括：应急响应相关责任单位、应急响应指挥人员、应急响应工作实施组织、事件发生当事人。

为防范化解重特大安全风险，健全公共安全体系，整合优化应急响应力量和资源，推动形成统一指挥、专常兼备、反应灵敏、上下联动、平战结合的中国特色应急响应管理体制，提高防灾、减灾、救灾能力，确保人民群众生命财产安全和社会稳定，2018 年 3 月，中华人民共和国应急管理部正式设立，其主要职责包括：组织编制国家应急总体预案和规划，指导各地区各部门应对突发事件工作，推动应急预案体系建设和预案演练；建立灾情报告系统并统一发布灾情，统筹应急力量建设和物资储备，并在救灾时统一调度，组织灾害救助体系建设，指导安全生产类、自然灾害类应急救援，承担国家应对特别重大灾害的指挥工作，负责安全生产综合监督管理和工矿商贸行业安全生产监督管理等。

1.2 什么是网络安全应急响应

网络安全和信息化是我国经济社会健康、稳定发展驱动之双轮、一体之两翼。

网络安全已上升为国家战略，并且成为网络强国建设的核心。习近平总书记在2014年曾指出：“没有网络安全就没有国家安全，没有信息化就没有现代化。”在2018年全国网络安全和信息化工作会议上，再次强调：“没有网络安全就没有国家安全，就没有经济社会稳定运行，广大人民群众利益也难以得到保障。”网络安全问题不再是简单的互联网技术领域的安全问题，而是与经济安全、社会安全息息相关，甚至是军事、外交等关系国计民生的国家层面的战略问题。

网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭到破坏、更改、泄露，保证系统连续、可靠、正常运行，网络服务不中断。面对各种新奇怪异的病毒和不计其数的安全漏洞，建立有效的网络安全应急体系并使之不断完善，已成为信息化社会发展的必然需要。

网络安全应急响应(以下简称“应急响应”，本书后续章节提到的“应急响应”均指“网络安全应急响应”)是指针对已经发生或可能发生的安全事件进行监控、分析、协调、处理、保护资产安全的活动。主要是为了对网络安全有所认识、有所准备，以便在遇到突发网络安全事件时做到有序应对、妥善处理。

另外，在发生确切的网络安全事件时，应急响应实施人员应及时采取行动，限制事件扩散和影响的范围，限制潜在的损失与破坏，实施人员协助用户检查所有受影响的系统，在准确判断安全事件原因的基础上，提出基于安全事件的整体解决方案，排除系统安全风险，并协助追查事件来源，提出解决方案，协助后续处置。

国家对网络安全高度重视，且机构和企业面临越来越多、越来越复杂的网络安全问题，使得应急响应工作举足轻重。应急响应活动主要包括以下两方面。

第一，未雨绸缪，即在事件发生前先做好准备。例如，开展风险评估，制订安全计划，进行安全意识的培训，以发布安全通告的方式进行预警，以及各种其他防范措施。

第二，亡羊补牢，即在事件发生后采取的响应措施，其目的在于把事件造成的损失降到最小。这些行动措施可能来自人，也可能来自系统，例如，在发现事件后，采取紧急措施，进行系统备份、病毒检测、后门检测、清除病毒或后门、隔离、系统恢复、调查与追踪、入侵取证等一系列操作。

以上两方面的工作是相互补充的。首先，事前的计划和准备可为事件发生后的响应动作提供指导框架，否则，响应动作将陷入混乱，毫无章法的响应动作有可能引起比事件本身更大的损失；其次，事后的响应可能会发现事前计划的

不足，从而吸取教训，进一步完善安全计划。因此，这两方面应该形成一种正反馈的机制，逐步强化组织的安全防范体系。

网络安全的应急响应需要机构、企业在实践中从技术、管理、法律等各角度综合应用，保证突发网络安全事件应急处理有序、有效、有力，确保涉事机构、企业损失降到最低，同时威慑肇事者。网络安全应急响应就是要对网络安全有清晰认识，有所预估和准备，从而在发生突发网络安全事件时，有序应对、妥善处理。

1.3 网络安全应急响应的形势与挑战

在数字化转型的时代背景下，以云计算、大数据、物联网和人工智能为代表的新一代信息革命带来了新一轮的信息化建设浪潮，以大数据驱动的“智能”推动着经济社会和基础设施转型升级的同时，也改变了机构和企业的信息化与业务环境，带来了新的安全威胁和安全需求。数据开放带来的数据安全威胁，云计算带来的业务集中后的业务安全风险，物联网带来的更广泛攻击面，都将对机构和企业的正常运行，甚至社会稳定、国家安全带来更加直接的影响和威胁。机构和企业数字化转型中对安全的“内生”需求将迫使其加强安全建设，构建应急响应体系。

另外，攻击者的国家化、组织化、集团化的倾向越来越明显，攻击手法的多样化、体系化，使得安全防御的难度越来越高，这种攻防双方在资源、能力和投入上的明显不对称性，也不断驱动着机构和企业加强安全建设，构建应急响应体系。

无论是内生安全需求还是攻防对抗的不对称，都需要机构和企业通过自我变革来满足新时代的安全需求。构建网络安全应急管理体系，对日益增多的网络安全事件具有重要意义。

1. 国际网络空间竞争日益激烈

2013 年 6 月，英国《卫报》和美国《华盛顿邮报》报道，美国国家安全局和联邦调查局于 2007 年启动了一个代号为“棱镜”的秘密监控项目，通过进入微软、谷歌、苹果、脸书、雅虎等九大网络公司的服务器，跟踪用户的上网信息，以此全面监督用户的行动。

2018 年 5 月 17 日，美国国防部网络司令部宣布，其下的 133 支网络任务部队(CMF，包括陆军 41 支，海军 40 支，空军 39 支，海军陆战队 13 支)已全部

实现全面作战能力。国家网络部队经过充分的训练和武装后或具备保卫国家网络空间安全的能力。

还有一些国际组织会专门针对中国政府部门发起 APT(Advanced Persistent Threat，高级持续性威胁)攻击。APT 攻击与普通网络攻击的本质区别在于其特有的针对性，主要目的是情报的刺探、收集和监控，在某些情况下也会有牟利意图和破坏意图。截至 2019 年 3 月，国内安全企业已累计监测到针对中国境内目标发动攻击的境内外 APT 组织 39 个。这些 APT 组织发动的攻击行动，至少影响了中国境内超过万台的计算机，攻击范围遍布国内 31 个省级行政区。

随着国内外大规模 APT 攻击事件的升级、WannaCry(“永恒之蓝”勒索蠕虫病毒)的席卷全球、“核武器”级工具的持续曝光，网络安全已经成为全球焦点。当今的网络安全态势早已不再局限于个人或企业，已经上升到国家与国家之间的博弈对抗。

网络安全深刻影响世界各国的经济社会发展，影响面涉及政治、社会、军事、外交等众多领域。世界主要国家都在积极加强国际网络空间政策制定能力，美国、英国、以色列等国已深刻认识到网络空间安全的重要意义，纷纷出台相关安全战略，增设相应机构，加强网络安全建设。

近几年，针对我国的网络窃密、监听等攻击事件频发，网络空间的安全攻防对抗日趋激烈。在复杂多变的网络与信息安全形势下，我们必须从保证经济发展、维护社会稳定、确保国家安全、保障公共利益等方面，充分认识网络与信息安全应急保障工作的重要性，高度重视并切实做好应急准备工作。

2. 国家对网络安全应急响应的高度重视

2017 年 6 月 1 日，《中华人民共和国网络安全法》(以下简称“《网络安全法》”)正式实施。标志着我国网络安全从此有法可依，网络空间治理、网络信息传播规范、网络犯罪惩治等将翻开崭新的一页。

《网络安全法》中对网络安全应急响应及演练工作明确指出：关键信息基础设施的运营者应制定网络安全事件应急预案，并定期进行演练；国家网信部门应当统筹协调有关部门定期组织关键信息基础设施的运营者进行网络安全应急演练，提高应对网络安全事件的水平和协同配合能力；负责关键信息基础设施安全保护工作的部门应当制定本行业、本领域的网络安全事件应急预案，并定期组织演练。

2017 年 1 月 10 日，《中央网信办关于印发〈国家网络安全事件应急预案〉

的通知》(中网办发文〔2017〕4号)的发布，为从国家层面组织应对涉及多部门、跨地区、跨行业的特别重大网络安全事件的应急处置提供了政策性、指导性和可操作性方案。

2017年，中华人民共和国工业和信息化部(以下简称“工业和信息化部”)针对通信部门、互联网企业、网络安全企业发布《工业和信息化部关于印发〈公共互联网网络安全威胁监测与处置办法〉的通知》(工信部网安〔2017〕202号)、《工业和信息化部关于印发〈公共互联网网络安全突发事件应急预案〉的通知》(工信部网安〔2017〕281号)等应急响应相关规定。

《网络安全法》及相关标准与规范的发布，使我国网络安全有法可依、有规可依，网络安全行业将由合规性驱动过渡到合规性和强制性驱动并重。

3. 业务发展越来越依靠网络化和智能化

2019年2月21日，工业和信息化部部长苗圩在北京召开的工业互联网峰会的开幕致辞中表示：工业互联网已广泛应用于石油石化、钢铁冶金、家电服装、机械、能源等行业。国内具有一定行业和区域影响力的工业互联网平台总数超过了50家，重点平台平均连接的设备数量达到了59万台。

计算机网络和系统变得越来越复杂，计算机软件(包括操作系统和应用软件)的安全缺陷往往与软件的规模和复杂性成正比。从设计、实现到维护阶段，都留下了大量的安全漏洞。应急响应将有助于降低这些漏洞一旦被攻破所带来的影响。

为了保持商业运营的竞争力，机构、企业需要依靠IT运维信息系统来管理日常业务和大量的业务数据及信息，为机构、企业的业务发展决策提供依据。信息技术平台是机构、企业商业运作强有力的信息支持系统，在一些重要业务系统中通常存储着大量的核心数据，通常，损坏或丢失都会带来利益损失。

不同行业的业务发展越来越依靠网络化和智能化，迫使相关机构、企业对网络安全及应急响应更加重视。

4. 网络威胁已经危害到了各行各业的安全

自2013年斯诺登事件以来，全球数据泄露规模连年加剧。2016年，某准大学生因诈骗电话损失学费9900元，郁结于心最终导致心脏骤停，抢救后不幸离世。2018年11月，某国际酒店集团宣布，其旗下某酒店的数据库被黑客入侵，可能有约5亿顾客的信息泄露，包括顾客的姓名、通信地址、电话号码、电子邮箱、护照号码、出生日期、性别等。