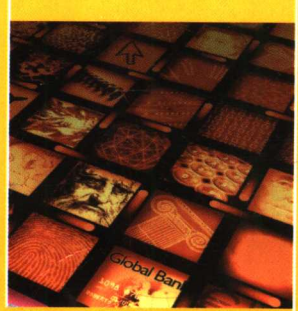
Broadview®
www.broadview.com.cn

网络安全应急实践指南



国家计算机网络应急技术处理协调中心（CNCERT/CC）
全国网络与信息技术培训项目管理中心（NTC-MC）
编著

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

网络安全应急实践指南

国家计算机网络应急技术处理协调中心（CNCERT/CC）
全国网络与信息技术培训项目管理中心（NTC-MC）
编著

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

内 容 简 介

本书由国家计算机网络应急技术处理协调中心（简称国家互联网应急中心，CNCERT/CC）总结多年的工作经历和实践经验而写就。内容包括有关网络安全应急的基础知识、应急组织的职能作用与日常运作、各类典型网络安全事件的处置办法、应急组织之间的协调合作与交流平台，以及网络安全文化的培育等内容。

本书属于实践指南或工作指导类的题材，结合并依据一定的理论基础，注重操作层面实践经验的总结和具体工作的介绍与指导，可作为相关从业人员的工具指导书，具有良好的实用价值。本书适合各类应急组织、从事网络安全工作的系统和部门、从事网络安全工作的管理人员和技术人员阅读。

图书在版编目（CIP）数据

网络安全应急实践指南 / 国家计算机网络应急技术处理协调中心（CNCERT/CC），全国网络与信息技术培训项目管理中心（NTC-MC）编著. —北京：电子工业出版社，2008.4
ISBN 978-7-121-06194-3

Ⅰ. 网… Ⅱ. ①国… ②全… Ⅲ. 计算机网络－安全技术－指南 Ⅳ. TP393.08-62

中国版本图书馆 CIP 数据核字（2008）第 033001 号

责任编辑：葛　娜
印　　刷：北京智力达印刷有限公司
装　　订：北京中新伟业印刷有限公司
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：787×980　1/16　印张：16.25　字数：218 千字
印　　次：2008 年 4 月第 1 次印刷
印　　数：4000 册　定价：45.00 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。
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。
服务热线：（010）88258888。

《网络安全应急实践指南》
编辑委员会名单

前　言

2001 年 8 月 8 日，我们这个组织也就是 CNCERT/CC（国家计算机网络应急技术处理协调中心，简称国家互联网应急中心，National Computer Network Emergency Response Technical Team/Coordination Center of China）成立了。成立之初，国内对于这样一个名称表现得相当陌生，但在国际上，CNCERT/CC 的成立却是令人注目的。这源于我们组织英文名称中的一个缩写词——CERT（计算机应急响应组织），对于世界各个国家和地区的 CERT 组织来说，CNCERT/CC 的成立无疑是一个好消息，不仅说明在中国又多了一个 CERT 组织[1]，而且说明 CNCERT/CC 是一个能够代表国家参与国际 CERT 事务的国家级机构，填补了世界在该区域的一个空白。

如果说，六年前的我们更多的是在学习、借鉴、探索和实践，今天的我们则已经具备了一套较为成熟的运行框架、机制和流程，并以此为基础卓有成效地发挥着应有的作用。我们的定位决定了我们的业务具有一定的广泛性和综合性，或多或少地涉及到各种类型的 CERT 组织的业务，尽管如此，我们还是明确了我们的工作重点，即以“全网[2]”安全为首要着眼点，在支撑信息产业部做好全网安全运行监测的同时，为国家关键基础设施及重要信息系统部门提供技术支持。正是这个原因，我们在本书中介绍的多为大规模或高危害性网络安全事件的处理办法和应对措施，希望能对尽可能广泛的互联网用户群体具有一定的借鉴意义。

根据我们的经验，做好网络安全工作不进行定岗定员是无法确保实效的，而应急响应工作更是如此，这也是世界上形形色色国家的、政府的、商业的、企业的、教育的、科研的 CERT 组织存在的理由。不管是否有明确的 CERT 职能部门，也不

---

① CNCERT/CC 成立之前，国内已有教育网的 CCERT。

② 中国大陆境内的互联网。

管是否有明确的专业 CERT 人员，我们相信在全国的各行各业和各级部门都一定有类似的部门或人员在从事着网络安全应急响应的工作。我们的书正是写给他们看的，我们尽力总结我们在这六年的实践当中所积累的经验，挖掘我们对于网络安全应急响应工作不断深化的理解，梳理我们经过无数次考察、学习、交流和培训而获得的知识，最后以十几名经验丰富的老同事的集体智慧和劳动编纂出本书。我们相信，本书的出版对于从事网络安全应急响应工作的人员具有普遍的指导意义，特别是对那些尚未建立 CERT 小组的部门来说，本书更能够指导他们如何有效地组建和运作一个 CERT 组织并开展工作。同时，我们还就网络上最典型和最具危害性的几类安全事件给出了比较具体的处理措施和建议，以帮助他们根据自身的情况有针对性地采取行动。我们也没有忘记就这些安全事件给终端用户提出安全建议，目的是希望非专业人员和普通读者也能够从本书中获益。

我们发现，自 2005 年开始，利用系统漏洞进行传播的蠕虫已经不再是安全事件中的独家主角，而以僵尸网络、间谍软件、身份窃取为代表的各类恶意代码逐渐成为最大威胁，同时，拒绝服务攻击、网络仿冒、垃圾邮件等安全事件仍然猖獗；此外，与政治纪念日和时政相关的网络攻击活动也时有发生，网络安全事件在保持整体数量显著上升的同时，也呈现出技术复杂化、动机趋利化、政治化的特点。根据中国互联网信息中心 2007 年 7 月公布的《中国互联网络发展状况统计报告》显示，截至 2007 年 6 月，我国上网用户总数为 1.62 亿人，上网计算机达到 6710 万台，网络用户和网络主机的数量仍然在持续增长，与此同时，电子政务、电子商务、网络游戏、网络博客等互联网业务正在快速扩展，新的操作系统、新应用软件不断投入使用，这些都导致大量人为主观疏忽和网络系统客观漏洞的存在。而黑客攻击动机已经从单纯地追求“荣耀感”向获取多方面实际利益和表达政治情绪的方向转移，黑客技术的发展也将重点放在网上木马、间谍程序、恶意网站、网络仿冒、僵尸网络等方面，因此，网络安全问题变得更加错综复杂，涉及范围将不断扩大。我们估计，由于黑客发动攻击的目的的转变，今后发生大规模的网络安全事件的可能性比较小，而以僵尸网络、间谍软件、身份窃取为代表的恶意代码，以及网络仿冒、网址嫁接/劫持类安全事件将会继续增加，因此，我们将继续对此类安全事件保持密切关注，对此类事件的处理力度也会不断加强。由于此类事件通常不会是单点孤立地

发生，受到一次事件影响的往往涉及多个部门和个人，或者说，遭受一次事件威胁或危害的很可能是多个部门和个人，因此，我们非常希望所有牵涉事件中的相关部门和个人能够通力合作，尽可能迅速有效地处理事件，将事件可能会对各个部门和个人造成的不良影响降低到最小程度。这也是为什么我们在书中所描述的那些事件的处理过程会涉及那么多的部门或个人。无疑，了解了这些事件的处理过程将会有助于读者很快找到正确的办法、途径和部门来解决问题。

本书将与《网络与信息安全》（清华大学出版社）教材共同列入信息产业部网络与信息安全技术培训认证项目（NTC-NISE）的教学体系中，作为信息产业部 IT 职业技术培训指定教材与广大读者见面。信息产业部网络与信息安全技术培训认证项目（NTC-NISE）是信息产业部全国网络与信息技术培训项目（NTC）的组成部分，是根据国家职业技术标准要求及国家对专业技术人员加强培训且须持证上岗等文件精神所推出的面向各行政、企事业单位及行业系统的专业技术人员、管理人员进行资格认证的培训项目，由国信高科技术培训中心（信息产业部批准设立的信息化培训认证机构）负责具体的运营工作。

实际上，本书的写就与我们的成长相关，而我们的成长得益于四年前国家公共互联网安全事件应急处理体系的确立。依赖于这个体系，我们得以在与各个合作单位和部门的互动中发展壮大并日趋成熟，我们这些年来所取得的工作成绩离不开体系中各个合作单位和部门的大力协助与支持，在此，我们要对所有的合作单位和部门表示衷心的感谢。很遗憾，限于篇幅原因，我们无法细数和列出所有的合作单位和部门，那会是一份相当长的名单。

感谢参加本书编写的其他同志：张雪浩（“前言、部分基础篇”的编写），刘洋、顾嘉（“第 8 章 网络仿冒事件的处置”的编写），宋轶南（“第 9 章 拒绝服务攻击事件的处置”的编写），吴冰、何松（“第 2 章 国家级网络安全应急响应组织”的编写）。

国家计算机网络应急技术处理协调中心

二〇〇七年八月

目　　录

应急响应　基础篇

应急响应　组织篇

应急响应　实践篇

应急响应　协作篇

应急响应　文化篇

1

应急响应

基 础 篇

在信息时代，我们每个组织、每个人、每天都在面对着形形色色的网络安全问题，安全事件不再是发生在别人身上的事情。网络空间无时无刻地在有能力发现并且利用信息技术（IT）脆弱性的恶意个体和组织的攻击之下，它们以难以承受的频率、速度和严重程度迅速膨胀。尽管我们通过诸多技术的、管理的、操作的方法来应对安全事件，但迄今为止，我们尚未找到某种技术防护措施或实施某些安全策略来对信息系统提供绝对的保护。这就是计算机应急响应组织应运而生并且得以蓬勃发展的理由。

计算机应急响应旨在减少信息安全突发事件对组织和业务的影响，它体现了一个组织驾驭事件的能力：一个组织在威胁显现之时能够迅速地对威胁做出反应，在发生计算机安全事件时拥有一个行之有效的处置手段以响应事件，就有可能有效地减少损失和降低恢复系统的代价。否则，我们将面临非常严重的问题并可能伴随着非常严重的后果。

1. 计算机安全事件

计算机安全事件是指由于自然或者人为，以及软硬件本身缺陷或故障的原因，对信息系统造成危害，或者在信息系统内发生对社会造成负面影响的事件。计算机安全事件通常由单个或一系列意外或有害的信息安全事态所组成，本指南特指那些由恶意的技术活动导致的事件，特别是那些在没有技术专家响应时会造成严重损害的事件，如由计算机病毒、蠕虫及其他恶意代码、内部或外部的系统入侵导致的事件。其可定义为：所有涉及计算机系统或计算机网络的非法、未授权或不可接受的行为。这种行为可能包括以下任一类型事件：

- 窃取商业秘密；
- 垃圾邮件或邮件骚扰；
- 对计算机系统的未授权访问或非法入侵；
- 盗用；

- 拥有或分发非法内容（如色情等）；
- 拒绝服务（DoS）攻击；
- 商业关系的侵权冲突；
- 敲诈；
- 不当使用；
- 其证据可存储在计算机介质中的任何非法行为（如欺骗、恐吓等）。

安全事件发生的方式具有多样性，根据事件的不同类型可划分如下：

- **拒绝服务攻击**：一种攻击，通过消耗 CPU、内存、带宽或磁盘空间等资源的方式来阻止和破坏已经经过授权的用户对网络、系统等的正常使用。
- **恶意代码**：指的是一种被隐蔽插入到另一个程序中的程序，能够感染主机的病毒、蠕虫、特洛伊木马或其他基于代码的恶意实体。其目的是破坏数据、执行破坏性和入侵性程序或破坏受害者数据的安全性和完整性。一般来说，恶意代码是用来在系统用户不知情的情况下实现其邪恶功能。恶意代码攻击可以分成五类：病毒、木马、蠕虫、网页代码和混合型攻击。
  - 病毒被设计成自我复制，生成自身的副本，并将副本分发到其他文件、程序或计算机中。病毒将自己嵌入在主机程序中，当被感染文件执行时（一般通过用户交互，比如打开文件、运行程序、点击邮件附件）实现传播。病毒又分为文件感染型病毒、引导区病毒、宏病毒和病毒恶作剧。
  - 特洛伊木马是根据古希腊神话中的木马来命名的，木马通常不容易被发现，因为它们看起来是在完成一项有用的功能，而实际上却是一个恶意程序执行恶意功能如收信口令、账户信息等。目前多数木马的目的是远程控制，或者作为 DDoS 攻击的代理。为了达到这个目的，木马一般都包括一个客户端和一个服务器端。还有些木马只是为了隐藏证据，比如使恶意进程不