IST

彭澎 周湛 等编著

信息安全团队构建与管理

国家信息化安全教育认证(ISEC)系列教材

机械工业出版社
CHINA MACHINE PRESS

国家信息化安全教育认证(ISEC)系列教材

信息安全团队构建与管理

彭　澎　周　湛　等编著

机械工业出版社

本书全面系统地介绍了计算机信息安全团队构建与管理方面的知识。全书共分为8章，对安全响应、物理安全、通信安全、辐射安全、计算机安全、网络安全、信息安全、安全响应策略、安全响应方法论等知识作了介绍和说明。本书还详细介绍了如何构建信息安全团队，信息安全团队的工作内容、工作流程和工作方法，如何对信息安全团队进行管理，及当发生网络攻击时，应采取什么样的方法来应对相应的攻击等内容。

这是一本有关信息安全团队构建与管理的方针性、指导性指南，适合需要了解信息安全管理基础知识和信息安全中高层管理者阅读，并可以作为信息安全管理的学习教材。

图书在版编目(CIP)数据

信息安全团队构建与管理/彭澎、周湛等编著.—北京：机械工业出版社，2004.4
(国家信息化安全教育认证(ISEC)系列教材)
ISBN 7-111-14170-9

Ⅰ.信… Ⅱ.彭… Ⅲ.信息系统—安全管理—资格考核—教材
Ⅳ.TP309

中国版本图书馆CIP数据核字(2004)第019295号

机械工业出版社(北京市百万庄大街22号 邮政编码100037)
责任编辑：蔡 岩
责任印制：李 妍

北京蓝海印刷有限公司印刷·新华书店北京发行所发行

2004年4月第1版·第1次印刷
787mm×1092mm 1/16·10.5印张·257千字
0001—5000册
定价：19.00元

出版说明

随着信息化在我国的不断深入和发展，信息技术和网络给社会的经济、科教、文化和管理等各个方面注入了新的活力。人们在感受它所带来的新体验、享受它为我们带来高效率的同时，也面临着日益突出的信息安全问题。党和国家领导人多次强调，必须充分认识到做好信息安全保障工作的重要性，大力搞好技术开发和人才培养。

对信息安全专业人才的需求是多层次的。从信息安全基础理论研究到新技术的开发利用，再到各级网络信息系统信息安全保障体系的建设、运行，需要根据不同要求有针对性的进行人才培养。

国家信息化安全教育认证(ISEC)项目是由信息产业部信息化推进司推出的信息安全领域的国家级认证体系。该项目由中国电子商务协会监督，由 ISEC 国家信息化安全教育认证管理中心统一管理与实施。ISEC 国家信息化安全教育认证管理中心以行业为基础、以技术为核心制定了一套面向应用的教育方案。根据工作性质的不同，教育对象被划分为规划决策层、管理运营层和操作层三个层次。认证体系的设计，课程内容及相应的教学考试大纲的编写和指定是针对三个层次人员对信息安全知识和技能的不同需求和理解程度的不同而制定的。确保不同层次，不同需求的各类人员从各自的角度充分掌握和理解信息安全的知识和技能。

本系列教材是在国家信息化安全教育认证(ISEC)专家组的指导下，由国家信息化安全教育认证(ISEC)教材编委会组织编写的。始终以 ISEC 国家信息化安全教育认证管理中心制订的各级考试大纲为依据，坚持面向行业用户的需求和侧重技术应用两个基本原则，全面地介绍了信息安全各种主流技术和管理规范，以帮助读者深入了解信息安全本质，并熟练掌握相应的技能，从而建立完备的信息安全观念。本系列教材包括：《网络安全基础》、《防火墙原理与技术》、《入侵检测技术》、《VPN 技术》、《PKI 技术》、《数据备份与灾难恢复》、《网络隔离与网闸》、《信息安全法规与标准》、《信息安全策略与机制》、《信息安全团队构建与管理》，共计 10 本。

在写作过程中，北京正阳天马信息技术有限公司为本系列教材的编写提供了很多宝贵的建议和支持。

前　言

随着计算机技术和网络技术迅速的发展，计算机网络的应用正在不断地改变人们的生活方式。由于网络中的计算机系统和系统内存储的信息每天都在受到不安全事件的侵害，信息安全问题已越来越多地引起人们的重视。

信息安全研究是一个很广泛的课题。它涉及到计算机、网络、信息技术，信息安全基础建设、安全策略制定、信息安全防护、信息安全法律、计算机犯罪等不同的领域，总之，为了预防信息安全事件的发生，对信息安全事件的响应，需要建立更广泛的信息安全队伍来完成这项复杂、艰巨的工作。

《信息安全团队构建与管理》这本书全面地介绍了如何组建信息安全团队，构建团队的方式和方法，并且如何对信息安全团队进行管理。全书共分 8 章。

第 1 章介绍了建立应急响应体系应注意的问题，应急响应体系中各部门的责任分工，以及与信息安全相关的知识。对安全响应方法论、安全响应过程的工作流程、构建安全响应系统的意义、架构、分类，影响构建信息安全响应系统的因素作了全面的介绍。

第 2 章介绍了如何组建信息安全团队，它的工作目标、任务、作用、架构等内容，以及信息安全团队的决策层、管理层和执行层 3 个部门是如何组建、实施的。

第 3 章介绍了信息安全团队决策部门的构建与管理方法，介绍了不同类型的信息安全团队决策者应具备的条件，在工作中应如何处理发生的问题，以及决策者的工作能力将对信息安全团队产生什么样的影响。还全面介绍了信息安全团队决策系统的系统结构、工作流程、工作指标，以及不同的组织结构之间的区别和对工作的影响。

第 4 章详细介绍了信息安全团队管理部门的人力资源，以及响应工具包的配置与管理。

第 5 章介绍了信息安全团队技术部门的构建与管理，包括技术部门人力资源的配置问题，以及技术部门机构的设置与管理。最后还介绍了在事件响应前应做哪些技术准备工作。

第 6 章主要针对商业型、政府型和内部型信息安全团队内部关系的管理与处理进行了详细的介绍，特别对政府型和内部型信息安全团队上、下级之间的关系，及相关部门之间及人员之间的关系作了全面的介绍。

第 7 章介绍了信息安全团队与外部进行沟通有哪些手段和方法，在对外响应时的响应方式，如何对客户的资产进行风险评估、风险分析，以及风险级别的定义方法。

第 8 章是全书的最后一章，它是对全书内容的一个总结。对信息安全团队构建工作流程，影响构建信息安全团队的因素，团队的资金来源、组织结构、人力资源管理、资产管理、团队档案、事件响应流程、事件响应项目检查、团队日常工作检查、安全培训等内容进行了较为全面性的综述。

由于信息安全团队的建设与管理是一项长期、艰巨、复杂的工作，而在实际工作中所遇到的问题也是多种多样的，所以应根据实际情况合理地处理所发生的问题和事件。

本书适用于信息安全管理人员和工作人员的学习和参考书，通过本书的学习，可以全面地

掌握如何构建一支信息安全团队，及如何对其进行管理的方法。

本书主要由彭澎、周湛编写，参与本书编写的还有张红、周知平、王敏英、于红。在编写过程中还得到了首都经济贸易大学盛定宇教授的指导和帮助。由于作者水平有限，书中难免出现错误，希望广大读者提出宝贵意见。

编　者

目　录

第1章　应急响应体系

本章导读：

本章介绍了建立应急响应体系应注意的问题，应急响应体系的建立需要制度化和规范化，根据各部门的职责，确定明确的责任分工，应从多方位、基础上建立相应的措施。对与信息安全相关的信息安全定义，物理安全，通信安全，辐射安全，计算机安全，网络安全，信息安全，安全响应策略进行了简单的说明。

本章还介绍了在制订安全策略时应注意的事项，发生安全事件，当采用访问攻击、修改攻击、拒绝服务攻击、否认攻击4种攻击方法时，应采取保密性服务、完整性服务、可用性服务、责任性服务的方法来应对相应的攻击方法。

通过对安全响应方法论准备、检测、抑制、根除、恢复、跟踪6个阶段任务的学习，可了解安全响应过程的工作流程，构建安全响应系统的意义，安全响应系统的架构及分类，影响构建安全响应系统的因素。

我们生活在一个开放的世界中，世界上每天都充满着不安全的因素。地区性战争、争端，恐怖主义事件，地震、洪水、飓风、森林火灾等自然灾害，疫病的流行，飞机、火车、轮船失事，大规模的停电事故，计算机病毒在互联网上的传播造成人们无法正常使用计算机、无法正常地进行通信，各种各样的意外突发事件经常发生在每个人的身边，给人们的工作和生活造成影响，有时对一个国家的国民经济乃至世界经济都会带来严重的负面影响，引发经济危机，使世界的局势变得动荡不安。

2002年11月16日在我国广东佛山发现第一起传染性非典型肺炎（以下简称非典型肺炎，SARS）的病例，在极短的时间内，该疾病在我国的北京、香港、台湾、河北省、内蒙古自治区、山西省和天津等地区迅速蔓延，同时也在世界更大的范围内传播。据世界卫生组织发表的报告，截止到2003年8月7日，全球累计非典型肺炎病例共8422例，涉及32个国家和地区。中国内地累计病例5327人，死亡349人；中国香港：1755例，死亡300人；中国台湾：665例，死亡180人；加拿大：251例，死亡41人；新加坡：238例，死亡33人；越南：63例，死亡5人。非典型肺炎的传播给全球的经济带来了巨大的负面影响，人们的工作、生活和学习等方面都受到了不同程度的影响。

为防治非典型肺炎疫情，我国各级财政部门安排逾百亿元专项基金、经费。到2003年6月18日，中央财政非典防治基金支出近13亿元人民币，地方各级财政也安排了100多亿元人民币用于非典型肺炎防治工作。

与此同时，在世界卫生组织的指导下，世界其他国家或地区也投入大量资金和人力用于非典型肺炎的研究与防治工作。欧委会决定至少投资900万欧元用于攻克非典型性肺炎的新研究，并鼓励中国等亚洲国家的科研机构积极参与。

2003年8月14日美国东北部和中西部地区发生该国历史上最大规模的断电，5000多万人的工作和生活被打乱，但事故没有引发连锁性灾难。这主要是美国经过多年努力建立了一

套成熟、严密的应急响应体系，特别是在2001年“9.11”恐怖袭击事件后大力强化应急响应能力的建设，否则，此次停电造成的破坏恐怕比现在要大得多。

以上两个例子都属于突发事件。突发事件是指正常运行的程序突然中断，陷入一种危机，这种危机达到了一定程度后影响了社会秩序正常运行的事件。为了应对突发事件，每个国家、部门、组织都设有或应当设立相应的应急响应体系。

1. 应急响应体系的建立需要制度化和规范化

国家需要通过立法来界定政府机构在紧急情况下的职责和权限，理顺各方之间的关系。美国为了应对紧急事件的发生，先后制订了上百部针对自然灾害和其他意外突发事件的法律法规，并且经常根据实际情况的变化不断地对其进行修改完善，为应急响应体系的制度化和规范化奠定了基础。在我国，经过此次成功地防治和控制非典型肺炎的流行后，政府及卫生部门出台了相应的预防控制非典型肺炎流行的措施，如北京市人民政府于2003年9月12日出台了《非典应急预案》，将防治非典型肺炎工作制度化、规范化，形成一套完整的防控体系和救治措施。当2004年在广东再次出现非典型肺炎病例时，政府卫生部门对非典疑似病人采取了有效的防范、控制、治疗措施，并在全国范围内启动了相应级别的应急方案，虽然非典疑似病例最后被确诊为非典型肺炎，但并没有造成大面积疫病的传染和流行。

2. 根据各部门的职责，确定明确的责任分工

以美国“联邦应急方案”为代表的应急体系主要强调对紧急事件既要做出一体化、统一快速的反应，同时还要通过独特的应急功能模块的划分，使应急响应体系在组织结构上具有较大的灵活性。美国“联邦应急方案”将应急响应工作细分为交通、通信、消防、大规模救护、有害物质处理等12个职能，每个职能由特定的机构指挥领导，并指定若干辅助机构协助工作。这样的组织结构方式使执行各职能的领导机构的专长得以发挥，在遇到不同灾难及紧急事件时，可视情况启动全部或部分职能系统。各政府机构既遵循国家应急体系的指导原则与其他机构协调，同时又具有一定的主动权。

3. 应急响应体系应从多方位、基础上建立相应的措施

应急响应体系不仅仅是对某一事件的应急处理，更应注重经济应急、信息应急和心理应急。当天灾人祸到来时，其破坏性是多方面的，不仅能动摇国家安全，导致社会不安定因素增加，给国家的经济造成巨大的损失，同时也使公众产生心理恐惧。应对紧急事件必须从多方位入手，有健全的配套措施。

应急响应体系的参考模型如图1-1所示。

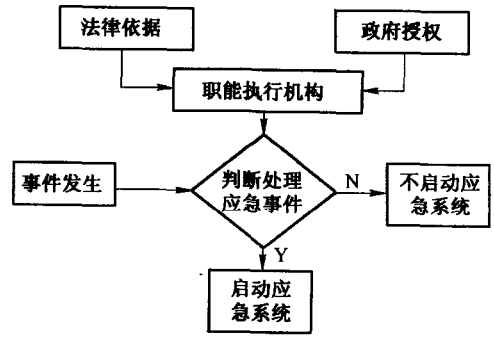

图1-1 应急响应体系模型

应急响应体系的复杂性和多样性。由于突发事件发生的原因复杂多变，其处理方法具有多样性，相应的应急响应体系也各不相同。

应急响应体系的共同性。无论应对什么样的突发事件，什么样的应急响应体系，都需要对事件的信息进行处理。如何保障信息在处理过程中的安全将是任何一个应急响应体系需要解决的最基本问题。

在介绍信息安全应急响应体系之前，先介绍与信息安全有关的一些概念。

1.1　信息安全

计算机与互联网正在不断地改变着犯罪和计算机安全的形式和方法。计算机犯罪行为或计算机安全事件已越来越多地引起人们的重视，如窃取信息、未经授权的非法访问、网络色情，都已经触犯了法律。如何防止信息被窃取，保护公司与顾客的信息和隐私，对每个公司来说变得尤为重要，为实现信息安全，应建立一种信息安全应急响应机制，通过该机制，迅速地通过调查、使用等多种技术手段，采取法律或行政手段来保护自身的财产安全，免受攻击者的攻击，使损失降低到最小程度。

1.1.1　信息安全定义

在不同的国家、不同的行业对信息及信息安全的定义各不相同。

信息：在《现代汉语词典》中的定义：信息即消息。在信息论中信息是指用符号传送的报道。报道中的内容，对接收符号者来说，预先是不知道的。

安全：没有危险，平安的；不受威胁；不出事故。

信息安全：为了防止未经授权就对知识、事实、数据或能力进行使用、滥用、修改或拒绝使用而采取的措施。

ISO 17799 中对信息及信息安全做了如下定义：信息是一种资产，同其他重要的商业资产一样，它对一个组织而言具有一定价值，因而需要适当的保护。信息安全是要在很大的范围内保护信息免受各种威胁，从而确保业务的连续性、减少业务损失并且使投资和商务机会获得最大的回报。

信息可以以多种形式存在。它能被打印或者写在纸上；能够电子化存储；也可以由邮局或者以电子方式发送；还可以在电影中展示或者在交谈中提到。无论以任何形式存在，或者以何种方式共享或存储，信息都应当得到恰当的保护。

在本书中信息安全特指信息保护。概括地讲，信息的安全主要有 3 个方面：

1）信息的保密性：确保信息只能够由得到授权的人访问。

2）信息的完整性：保护信息的正确性和完整性以及信息的处理方法。

3）信息的有效性：保证经授权的用户可以访问到信息。如果需要的话，还能够访问相关资讯。

信息安全通过实施一整套的控制措施达到保护信息安全的目的。控制措施可能是策略、做法、程序、组织结构或者软件功能。需要通过建立这些控制措施以确保实现能够达到特殊的安全目标。

1.1.2　物理安全

在远古时代，所有财产都是物理的。重要的信息也是物理的，因为那时的信息都刻写在贝壳或石头上，在我国四大发明之一，即纸张发明之后，信息就被记载到了纸上。

1. 信息是一种财产，同样也需要保护

古时，人们为了保护自己的财产，修筑了墙——伟大的长城，并派士兵站岗放哨，保护国土与财产不被外族人掠夺。信息作为一种不被外人知晓的内容，也是一种财产，在保存、传递过程中需要加以保护，不被外人所得。

2. 财产（钱或书面信息）容易失窃

财产一旦失窃，最初的财产所有者将丧失对它的控制权。古时信息作为一种物理存在的财产，只能从物理上拿到它，没有任何别的办法可以获取。因此，信息也要像保护自己的财产一样加以保护，避免信息的丢失。

1.1.3 通信安全

消息在传递过程中存在着危险，如果信息被截获，信息内容就会被截获者知晓，因此，要保证信息在传递过程中的安全就需要对传递的信息采取相应的保密措施。

1. 加密

早在凯撒大帝时代就使用了由尤里乌斯·凯撒（Julius Cassar）发明的凯撒密码来解决通信中的安全问题。经过密码加密的信息，在传递过程中即使被截获，截获者也无法正确地读出加密的信息。在通信中，最常用的安全保密方法就是使用密码对信息进行加密，其加密与解密的过程如图 1-2 所示。

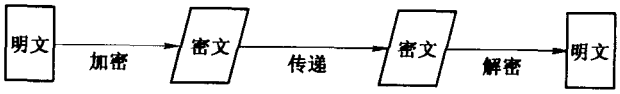

图 1-2 加密与解密

2. 密钥

密钥是在明文转换为密文或将密文转换为明文的算法中输入的数据。加密类型可以分为：私钥加密和公钥加密两种。私钥加密要求授权读信息的所有各方都使用同样的密钥，它是使用广泛的加密类型，将保护信息的整个问题简化为对密钥的保护。私钥加密过程如图 1-3 所示。

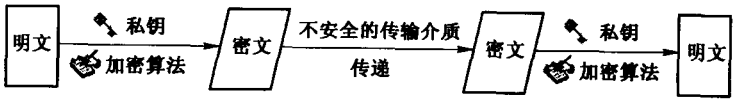

图 1-3 私钥加密

公钥加密比私钥加密出现的时间要晚一些，公钥加密与私钥加密的区别是在使用过程中使用的密钥数量不同。私钥加密在使用过程中使用一个相同的密钥来加密和解密信息，而公钥加密在使用过程中使用两个密钥，其中一个密钥用于加密信息，另一个密钥用于解密信息。在用公钥加密时，两个密钥之间的关系是：由密钥 Key1 加密的信息只能由密钥对中的另一个密钥 Key2 来解密。如果由密钥 Key2 加密信息，则只能由密钥 Key1 来解密。在公钥加密的过程中，其中一个密钥称为私钥，由密钥对的拥有者安全妥善地保管，而公钥则可以随其拥有

者使用的信息对外公布。公钥加密的特点是如果不知道密钥对中的一个密钥，则通过计算来找出另一个密钥的可能性很小。公钥的使用方法有两种：第一种是对机密信息进行加密时，信息加密过程要使用公钥加密，对信息解密的过程只有使用密钥对中的私钥才能进行。第二种是对信息认证，密钥对的拥有者利用私钥对信息进行加密，拥有正确公钥的使用者在收到加密信息后，对信息进行解密，检查信息是否完整。通过以上两种加、解密方法都可以保证传输过程中信息的完整。公钥加密的过程如图 1-4 所示。

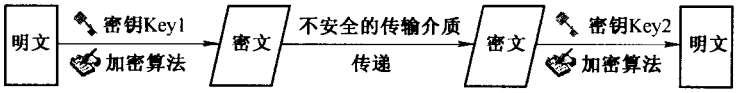

图 1-4　公钥加密

3. 密钥保护

无论是公钥加密还是私钥加密，使用密钥加密的信息都需要用密钥来解密，密钥需要妥善保管。对密钥的保护与管理应注意以下几个方面的内容：

1）公钥对中的公钥不需要机密性保护，但公钥对中的私钥必须妥善地保管，因为得到公钥对中的私钥就可以破解出发送给密钥对拥有者的所有加密信息。

2）私钥的保护包括它的所有副本，以及带有私钥的文件及文件的备份介质。

3）利用密码对私钥进行保护，以防读取存储私钥的介质。

4）精心地选择、设计保护密钥所使用的密码，防止攻击者使用强力猜测方法破解密码。

5）密钥的使用是有时间限制的，公钥对的有效期限一般为 1～2 年，因此公钥在发布时要给出有效期限。

6）当密钥丢失或被破解时，应及时通知用户密钥不再有效，及时更换密钥。

破译密码——即找到密钥，找到密钥的方法多种多样，其中通过对未加密信息与加密信息进行比较，可以很容易地找出加密机制。

4. 加密系统都可以被攻破

加密是一个很重要的安全工具，加密机制有助于保护信息的机密性和完整性，有助于识别信息的来源，它只是安全程序的一部分。加密本身只能起到延迟破译者破译密文的时间，所有加密系统都可以被破译，只不过破译加密方法保护的信息所花费的时间和资源多少而已。表 1-1列出了破解不同位数的密钥所用的时间。

表 1-1　不同长度位密钥破解时间

私钥位数及加密算法	破解所需的时间	使用的计算机数量
56 位　DES 密钥	4.5 天	一台 EFF 计算机
40 位　RC5 密钥	3.5 小时	250 台计算机
48 位　RC5 密钥	315 小时	3500 台计算机

1.1.4　辐射安全

所有电子系统都会产生电子辐射，造成信息泄漏。在日常的工作和生活中，都需要大量使

用电子设备，这些电子设备都会或多或少地产生电子辐射，通过对电子辐射的接收，很容易得到电子系统在工作时使用的信息，如图 1-5 所示。

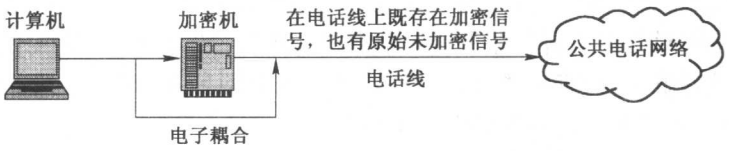

图 1-5 未加密电子信号绕过加密机

针对电子辐射这个问题，世界各国都制定了相应的防止电子辐射泄露的规范。美国制定了 TEMPEST 规范，规定了在敏感环境中使用计算机的电子辐射标准。我国也制定了相应的规范，如国标 GB12190《高性能屏蔽室屏蔽效能的测量方法》、军标 GJB2《军用电磁屏蔽室通用技术要求和检验方法》、国家保密标准 BMB3《处理涉密信息的电磁屏蔽室技术要求和测试方法》，其目的都是为了减少可以被用于收集信息的辐射。

1.1.5 计算机安全

现在很多组织的信息以电子形式移植到计算机当中，随着计算机技术和网络技术的发展及计算机的普及应用，人们可以方便地访问这些信息。

20 世纪 70 年代初期，专家提出保护计算机模型。模型是基于不同级别的分类信息和不同级别的许可的管理概念，即某个人（或主体）的许可级别高于文件（对象）的分类级别时，这个人即可访问该文件；而低于文件的分类级别的人，将无权访问该文件。

1983 年美国国防部制定了可信计算机系统评估标准（Trusted Computing System Evaluation Criteria TCSEC，也称为橙皮书）。该标准按照下列级别定义了计算机系统，计算机系统安全级别说明如表 1-2 所示。

表 1-2 计算机系统安全级别

级 别	说 明
D	最低保护或未经分类
C1	自主安全保护
C2	受控的访问保护
B1	标识的安全保护
B2	结构化保护
B3	安全域
A1	经验证的设计

对于每一种划分，该标准对功能要求和保证要求都作了定义。为了使系统能够达到某一级别的认证要求，均必须满足功能要求和保证要求。

用于较高安全级别认证的保证要求需要花费很长的时间和经费，在那时只有很少的系统被认证为 C2 以上的级别。由于计算机系统技术发展速度很快，当老的系统还没有得到认证时，新的操作系统和硬件设备已经被开发出来并生产上市，两者之间产生了巨大的矛盾，使认