奇安信

BEIJING 2022

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

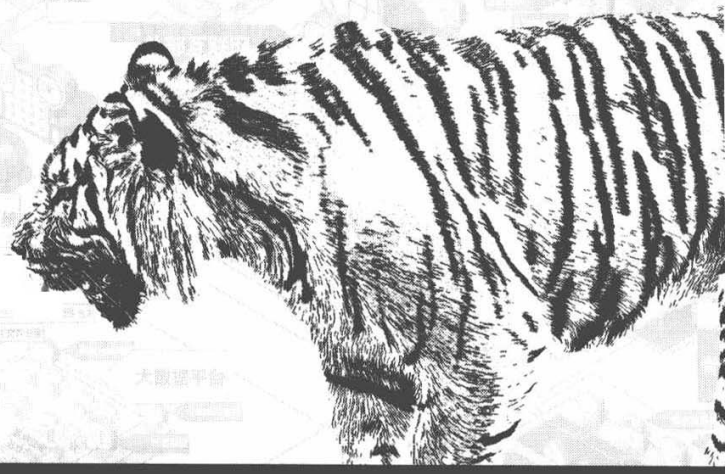
内生安全

新一代网络安全框架体系与实践

奇安信战略咨询规划部　奇安信行业安全研究中心　著

中国工信出版集团

人民邮电出版社
POSTS & TELECOM PRESS



内生安全

新一代网络安全框架体系与实践

奇安信战略咨询规划部　奇安信行业安全研究中心 著

人 民 邮 电 出 版 社
北 京

图书在版编目（CIP）数据

内生安全 ：新一代网络安全框架体系与实践 / 奇安信战略咨询规划部，奇安信行业安全研究中心著. -- 北京 ：人民邮电出版社，2021.4
ISBN 978-7-115-55848-0

Ⅰ. ①内… Ⅱ. ①奇… ②奇… Ⅲ. ①计算机网络－网络安全－研究 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2020)第268265号

内 容 提 要

本书是奇安信公司对内生安全理念以及实施策略的深度解读，详细介绍了内生安全理念的产生背景、内生安全的内涵与特性、内生安全建设的方法论基础、内生安全的关键要素等内容。本书还阐述了“新一代网络安全框架”的具体内容和建设方法，具体包括新一代身份安全、重构企业级网络纵深防御、数字化终端及接入环境安全、面向云的数据中心安全防护、面向大数据应用的数据安全防护、面向实战化的全局态势感知体系、面向资产/漏洞/配置/补丁的系统安全、工业生产网安全防护、内部威胁防护体系、密码专项十大工程，以及实战化安全运行能力建设、安全人员能力支撑、应用安全能力支撑、物联网安全能力支撑、业务安全能力支撑五大任务。

本书可以为政企“十四五”网络安全的规划、设计提供思路与建议。新一代网络安全框架从甲方视角、信息化视角、网络安全顶层视角呈现出政企网络安全体系全景，通过以能力为导向的网络安全体系设计方法，规划出面向“十四五”期间的建设实施项目库（重点工程与任务），并设计出将网络安全与信息化相融合的目标技术体系和目标运行体系，可供政企参考借鉴。

◆ 著　　奇安信战略咨询规划部
　　奇安信行业安全研究中心
　　责任编辑　傅道坤
　　责任印制　王　郁　彭志环

◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路 11 号
　　邮编　100164　　电子邮件　315@ptpress.com.cn
　　网址　https://www.ptpress.com.cn
　　大厂回族自治县聚鑫印刷有限责任公司印刷

◆ 开本：720×960　1/16
　　印张：17.25
　　字数：326 千字　　2021 年 4 月第 1 版
　　印数：1 – 6 800 册　　2021 年 4 月河北第 1 次印刷

定价：89.00 元

读者服务热线：(010)81055410　印装质量热线：(010)81055316
反盗版热线：(010)81055315
广告经营许可证：京东市监广登字 20170147 号

编委会

作者简介

奇安信战略咨询规划部：负责奇安信战略咨询规划业务，针对“十四五”规划、新基建与数字化转型，以系统工程方法，结合政企大型机构的业务战略与信息化战略，为政企机构梳理网络安全战略目标；并以“内生安全框架”体系规划设计方法与工具，从“技术、管理、运行”的多个视角，为政企机构进行它们所需的网络安全能力体系的梳理，从“顶层规划、体系设计、实现设计”不同层面，帮助政企机构进行规划设计、可研报告、概要设计、路线图等设计工作；以“三同步”原则，推进网络安全和信息化的“全面覆盖、深度融合”，帮助政企构建动态综合的网络安全防御体系及实战化运行体系，为政企数字化业务发展保驾护航。

奇安信行业安全研究中心（以下简称中心）：奇安信集团旗下专注于行业网络安全研究的机构，为政府、公安、军队、保密、交通、金融、医疗卫生、教育、能源等行业客户及监管机构提供专业安全分析与研究服务。

中心以奇安信集团的安全大数据、全球威胁情报大数据为基础，结合前沿网络安全技术、国内外政策法规，以及两千余起应急响应事件的处置经验，全面展开行业级、领域级、国家级网络安全研究。

中心自 2016 年成立以来，已累计发布各类专业研究报告 100 余篇，共计 300 余万字，在勒索病毒、信息泄露、网站安全、APT（高级持续性威胁）、应急响应、人才培养等多个领域的研究成果受到海内外网络安全从业者的高度关注。

同时，中心还联合各个专业团队，主编出版了多本网络安全图书专著，包括《走近安全：网络世界的攻与防》《透视 APT：赛博空间的高级威胁》《应急响应》《网络安全应急响应技术实战指南》《工业互联网安全：百问百答》等，为网络安全知识的深度传播做出了重要贡献。

章节贡献人

第 1 章	信息化的发展与安全的挑战	许传朝、裴智勇
第 2 章	内生安全的内涵与特性	李建平、裴智勇
第 3 章	内生安全建设的方法论基础	韩永刚、王轴可
第 4 章	新一代网络安全框架	杨　波、刘　洋
第 5 章	新一代身份安全	张泽洲、金　一
第 6 章	重构企业级网络纵深防御	陆明烈
第 7 章	数字化终端及接入环境安全	张晓兵、林晓明
第 8 章	面向云的数据中心安全防护	刘　浩、周　灿、林玉波
第 9 章	面向大数据应用的数据安全防护	刘川意、段少明、潘鹤中、向夏雨、李新鹏
第 10 章	面向实战化的全局态势感知体系	黄　海、马江波、尹智清
第 11 章	面向资产/漏洞/配置/补丁的系统安全	赵梦虎、伍星亮、佟　彤、邬　怡
第 12 章	工业生产网安全防护	宋　强
第 13 章	内部威胁防护体系	丁大鹏
第 14 章	密码专项	乔思远、金　一
第 15 章	实战化安全运行能力建设	潘　山、尹智清
第 16 章	安全人员能力支撑	杨东晓、冯　涛、柯善学
第 17 章	应用安全能力支撑	李　钠
第 18 章	物联网安全能力支撑	刘宇馨
第 19 章	业务安全能力支撑	卢维清

序

随着数字经济时代的到来，政府和企业开始全面实施网络化、数字化，业务和数据的安全性也因此成为重中之重。尤其是伴随着 5G、数据中心、工业互联网等新型基础设施建设的推进，数字经济加速向纵深发展，传统基础设施亟需转型升级，这进而形成了融合基础设施，加速了物理与虚拟边界的消融，带来了全新的安全挑战。

内生安全重塑网络安全体系

在新的网络安全形势下，政企机构的网络安全投入不断增加，但与此同时，网络攻击、数据泄露事件依然层出不穷。网络安全行业陷入投入不断增加、安全形势却日益严峻的尴尬局面。安全威胁之所以“防不住”，主要原因是传统的产品堆叠的网络安全体系已经不能有效应对当前的网络安全挑战。在传统的互联网时代，网络安全企业和个人习惯采取“事后补救”的措施来应对网络威胁，也就是等出了事后再采取安全措施。这种方式往往是“头痛医头、脚痛医脚”，是局部的、针对单点的，而不是彻底的和全面的。这种“局部整改”为主的安全建设模式，导致网络安全体系化缺失、碎片化严重、协同能力差，使得网络安全防御能力与数字化业务的保障要求严重不匹配。

为了满足数字化建设的安全防护需求，政企机构必须抛弃这种“事后补救”的安全建设思路，将防护关口前移，防患于未然，通过内生安全系统的工程建设，构建全面的“事前防控”网络安全防护体系，用“实战化、体系化、常态化”的要求，实现动态防御、主动防御、纵深防御、精准防护、整体防控、联防联控。

“内生安全”通过系统聚合、数据聚合和人的聚合，内置于信息化环境中并不断自我生长出安全能力。内生安全有“一个中心，五个滤网”，从网络、数据、应用、行为、身份这 5 个层面来有效实现对网络安全体系的管理，从而构建无处不在、处处结合、实战化运行的安全能力体系。

内生安全落地的关键是框架

内生安全的实施是一套复杂的系统工程，需要一个新形态的能力体系做支撑，需要用工程化、体系化的方式实施，而实施的关键就是安全框架。

在信息化系统功能越来越多、规模越来越大、与用户的交互越来越深时，单一的、堆叠的安全产品和服务（哪怕是最新最先进的）都无法保证不被黑客攻破。但是，内生安全系统能够让安全产品和服务相互联系、相互作用，在整体上具备单个产品和服务所没有的功能，从而保障复杂系统的安全。

过去 20 年，在信息化建设方面，国内外采用的是系统工程思想，通过行之有效的 EA（Enterprise Architecture，企业架构）方法论与框架，引导与推动了大规模、体系化、高效整合的信息化建设，很好地支撑了各行业的业务运营。针对网络安全，有些西方国家采用体系化思想，设计出了适应它们的发展阶段的 NIST（美国国家标准与技术研究院）等框架。但由于我国的网络安全基础比较薄弱，无法套用西方现成的框架进行安全体系建设，因此采用了“局部整改”为主的安全建设模式。

针对我国的国情，我们提出了“内生安全——新一代网络安全框架”，从工程实现的角度，将安全需求分步实施，逐步建成面向未来的安全体系。这套框架从顶层视角出发，以系统工程的方法论结合内生安全的理念，支撑各行业的建设模式从“局部整改外挂式”走向“深度融合体系化”，在数字化环境内部建立无处不在的网络安全“免疫力”，真正实现内生安全。

框架实施的关键是组件

内生安全要想成功落地，最理想的情况是建设一个完整的框架。但现实情况是，大多数政府和企业的信息化系统都是新老结合，往往需要花费若干年的时间，才能完成对老系统的替换。这是一个“立新破旧”的过程。从安全系统与信息化系统聚合的实施角度来看，如果对老系统用老办法，对新系统用新办法，则未来老系统被替代时，老的安全系统也不得不替换掉，这种割裂的处理方式将造成巨大的浪费。这就要求我们对安全体系进行统一设计，并分步实施。在安全体系的基础上，把安全框架组件化，让这些组件既是新体系的一部分，又能部署到老系统中，从而适应信息化系统这种渐进式的、立新破旧的过程，以避免不断地把安全系统推倒重来，并确保现在安全上的投资是面向未来的。

我们用工程化的思想，把安全体系中的安全能力，映射成为可执行、可建设的网络安全能力组件，由此构成了内生安全框架。这些组件与信息化系统进行体

系化的聚合，是安全框架落地的关键。

在“内生安全——新一代网络安全框架”中，我们设计解构出了“十大工程、五大任务”，这是该框架的具体落地指导，涵盖了当前所有的主流场景以及与技术相关的信息化系统所需要的安全能力。这个体系中包含了130多个信息化组件、79类网络安全组件，覆盖了29个安全域场景。这相当于打造了一个信息化巨系统内生安全框架的建设样板，每一个工程和任务都可以理解成样板房里的不同“房间”。政企机构可以结合自身信息化的特点，选取不同的“房间”进行组合，定义自己的关键工程和任务。

“内生安全——新一代网络安全框架”的意义

“内生安全——新一代网络安全框架”是从信息化的角度规划安全建设，立足解决未来10～20年的网络安全问题。这一框架可以指导政企机构进行体系化的网络安全规划建设，从过去“局部整改为主的外挂式”建设模式走向“深度融合的体系化”建设模式，使之能够输出体系化、全局化、实战化的网络安全能力，构建出动态综合的网络安全防御体系。

“内生安全——新一代网络安全框架”催生了新的安全需求，为网络安全生态发展创造了更大的空间。要满足新的网络安全需求，必须借助生态整合的力量，协同网络安全厂商、基础设施厂商、应用开发厂商，以及教育、科研机构、主管部门和用户，共同打造“产、学、研、用、管”一体化的网络安全产业生态。

——齐向东，奇安信集团董事长

前 言

经历了过去二十多年的发展，网络安全已经落后于以体系化发展的信息化，与信息化发展不匹配，不仅仅是安全能力达不到要求，还存在规模落差、成熟度落差和覆盖面落差。这不但无法支撑数字化、智能化时代的信息化保障，同时也带来了网络安全产业发展自身的诸多问题，比如小规模、零散化、同质化。要解决网络安全发展问题，不能依靠单个产品创新，也不是等待政策的来临，更不能要求客户无限制地增加预算。

网络安全产业要改变零散发展的模式，重要的是从信息化的角度，采用面向规划的新一代网络安全框架，构建内生安全能力，同时布局产业增长。

根据中国信息通信研究院2019年的数据，我国网络安全产业规模为608亿元，在整个数字经济产业中占比只有1.7%；而IDC（国际数据公司）的数据显示，网络安全投入在IT整体预算中的占比仅为1.84%，不仅远低于美国的4.78%，甚至低于全球平均的 3.74%。网络安全产业规模与市场预期不平衡，与数字化转型和数字经济发展所需要的信息化保障能力不匹配，网络安全产业亟待破解规模小的困局。

奇安信自2014年成立以来，一直在开展技术创新，提出了包括数据驱动安全等创新理念。但在逐渐壮大规模的过程中，奇安信也碰到了业界很多网安企业都面临的问题——如何破解产业规模小的困局。

回顾网络安全产业的发展历程，过去主要受事件和合规驱动，并没有相应的方法论，网络安全建设非常零散，而且多是应激式的局部建设。网络安全建设长期存在缺规划、缺预算、缺人手、缺运营的情况，这导致其难以支撑数字化、智能化时代的信息化保障。

近年来，实战演练正在成为监督、检查和检验网络安全工作和能力水平的常

态化手段。事实证明，实战演练对于网络安全的推动效果十分明显，如何常态化对抗威胁是亟待解决的难题。

如何解决这一难题，扩大网络安全产业规模，这一直困扰着网络安全行业的每个人。

在信息化的重构和新建过程中，在云网改造、大数据系统建设，以及业务、数据和应用发生变化时，通过系统融合、数据融合、人员融合，实现网络安全能力与信息化环境的融合内生，在这个过程中可以有效地把安全方法论与 IT（信息技术）对标，解决网络安全落后于信息化发展的主要问题。

信息化使用 EA（企业架构）方法论，将信息化从零散的建设发展到系统化的服务，使信息化有更好的发展和未来。对网络安全来说，在规划建设信息化系统时就嵌入安全机制和措施；同时，在规划时确立安全运行的机制；这种机制可以有效破解产业规模小、发展散乱的困境。

要改变过去网络安全零散发展的模式，以甲方视角，从信息化角度，用面向规划的内生安全框架来布局产业增长。所谓内生安全框架，是指奇安信基于长期政企网络安全防护实践形成的安全框架。该框架的核心是指导政企机构体系化的网络安全规划建设，从过去局部整改为主的外挂式建设模式走向深度融合的体系化建设模式，使之能够输出体系化、全局化、实战化的网络安全能力，以内生安全理念建立数字化环境内部无处不在的“免疫力”，构建出动态综合的网络安全防御体系。而在这个过程中，通过规划、建设、服务等扩大网络安全预算，进而提升网络安全产值。内生安全框架具有集约化和工程化的特点，更符合我国政企机构通过开展“五年规划”来集中力量办大事、解决大问题的成功做法。

内生安全框架的落地实践可以总结为：一套方法论、四个放大器、两个全景模型、贯穿项目全生命周期和两个确保。其中，一套方法论是指从信息化角度，用系统工程思想与 EA 方法进行网络安全规划设计，以能力为导向，以架构为驱动。基于这套方法论形成了安全产业的四个放大器：一是基于 SANS（美国系统网络安全协会）的滑动窗口模型识别出客户所需的所有安全能力；二是安全能力与信息化深度融合；三是安全能力全面覆盖信息化环境；四是形成可闭环运行体系。通过采用工程化思想，规划建设内生安全框架，最终会生成两个全景模型——通过规划形成政企机构防御技术全景模型和政企机构防御运行全景模型，以此指导政企机构的网络安全防御体系的建设和运行。与此同时，网络安全

服务过程将贯穿项目全生命周期——从规划、可研、立项、招投标、集成交付到可运行，确保客户安全项目可建设、能运行。

由此，可以形成一个巨大的网络安全服务化的市场。以内生网络安全框架体系的两个全景模型为基础可以生成网络安全建设视图和网络安全产业机遇地图，可用于指导网络安全产业的创新和发展。

内生安全框架对于政企机构来说，可以帮助规划设计和落地，同时推动政企机构需求侧的不断打开，由此拓宽供给侧的市场。这对于网络安全行业而言，可实现标准化、体系化、集约化生产，加快形成布局合理、分工有序、相互衔接的规模效应，从而告别此前的“小零同”（小规模、零散化、同质竞争）状况，在更宽的赛道上发展。

在这个过程中，整个国家的网络空间安全亦将受益。因为通过体系化的建设，关键信息行业与机构真正拥有的网络安全能力体系，将成为国家网络空间中有效防御的一环，保障整体的国家网络安全战略落地。

在《中共中央关于制定国民经济和社会发展第十四个五年规划和二〇三五年远景目标的建议》（以下简称《建议》）中，提出了加快数字化发展，并明确要求保障国家数据安全，加强个人信息保护；《建议》提出了统筹发展和安全的新理念，网络安全作为国家安全能力体系的一部分，要全面加强网络安全保障体系和能力建设。

网络安全行业要抓住“十四五”规划机会，落实中央要求，面向国家大数据战略的信息化发展保障需要，依托内生安全框架进行网络安全顶层规划，指引网络安全建设从“零散”走向“全局”，彻底改变过去“头痛医头、脚痛医脚”的局部的、针对单点的建设模式，走向彻底、全面解决问题的体系化全局建设模式，全面加强网络安全保障体系和能力建设，为国家大数据战略保障护航。

本书组织结构

本书分为以下 3 个部分。

- 第 1 部分：为什么需要内生安全

本部分通过梳理我国信息化发展历程和网络安全发展历程，结合国家网络安全战略的新要求和数字化时代安全的新挑战，解释当前的信息化为什么需要内生安全。

- 第 2 部分：什么是内生安全

本部分详细阐述了内生安全的理念、特点、优势、价值，以及落地的三大关键因素，首次披露了内生安全的方法论基础，并且对新一代网络安全框架进行了全面解读。

- 第 3 部分：怎样建设内生安全

本部分详细介绍了落实“内生安全——新一代网络安全框架”的十大工程、五大任务的具体内容，对每一个工程或任务的产生背景、基本概念、设计思想、总体架构、关键技术、预期成效、建设要点与方法进行了说明。

致谢

在本书的内容组织过程中，以及“内生安全——新一代网络安全框架”理论的梳理、归纳和提升中，信息化和网络安全专家王轴可贡献了大量实践经验和智慧，帮助提升了本书内容的系统性、专业性、指导性和实用性，在此特别表示感谢。

——吴云坤，奇安信集团总裁

资源与支持

本书由异步社区出品，社区（https://www.epubit.com/）为您提供相关资源和后续服务。

提交勘误

作者和编辑尽最大努力来确保书中内容的准确性，但难免会存在疏漏。欢迎您将发现的问题反馈给我们，帮助我们提升图书的质量。

当您发现错误时，请登录异步社区，按书名搜索，进入本书页面，单击“提交勘误”，输入勘误信息，单击“提交”按钮即可。本书的作者和编辑会对您提交的勘误进行审核，确认并接受后，您将获赠异步社区的 100 积分。积分可用于在异步社区兑换优惠券、样书或奖品。

扫码关注本书

扫描下方二维码，您将会在异步社区微信服务号中看到本书信息及相关的服务提示。

与我们联系

我们的联系邮箱是 contact@epubit.com.cn。

如果您对本书有任何疑问或建议，请您发邮件给我们，并请在邮件标题中注明本书书名，以便我们更高效地做出反馈。

如果您有兴趣出版图书、录制教学视频，或者参与图书翻译、技术审校等工作，可以发邮件给我们；有意出版图书的作者也可以到异步社区在线投稿（直接访问 www.epubit.com/ selfpublish/submission 即可）。

如果您所在的学校、培训机构或企业，想批量购买本书或异步社区出版的其他图书，也可以发邮件给我们。

如果您在网上发现有针对异步社区出品图书的各种形式的盗版行为，包括对图书全部或部分内容的非授权传播，请您将怀疑有侵权行为的链接发邮件给我们。您的这一举动是对作者权益的保护，也是我们持续为您提供有价值的内容的动力之源。

关于异步社区和异步图书

“异步社区”是人民邮电出版社旗下 IT 专业图书社区，致力于出版精品 IT 技术图书和相关学习产品，为作译者提供优质出版服务。异步社区创办于 2015 年 8 月，提供大量精品 IT 技术图书和电子书，以及高品质技术文章和视频课程。更多详情请访问异步社区官网 https://www.epubit.com。

“异步图书”是由异步社区编辑团队策划出版的精品 IT 专业图书的品牌，依托于人民邮电出版社近 30 年的计算机图书出版积累和专业编辑团队，相关图书在封面上印有异步图书的 LOGO。异步图书的出版领域包括软件开发、大数据、AI、测试、前端、网络技术等。

异步社区

微信服务号

目 录

第1部分 为什么需要内生安全

第 2 部分　什么是内生安全