专栏：信息安全

国内外行业标杆企业在网络与信息安全领域的实践分析

奚晓音，袁晓云
（中国电信股份有限公司研究院，上海 200122）

摘　要：为了更好地推进中国电信网络与信息安全治理体系建设，优化网络与信息安全产品服务体系，促进网络与信息安全核心能力的培育与发展，特选取国内外行业标杆企业开展实践案例分析，从运营商及互联网企业两大类企业出发，深入总结标杆企业在网络与信息安全领域的先进经验，并结合当前网络与信息安全领域的发展现状及未来发展趋势，进一步提出了针对性的发展建议及举措，对中国电信网络与信息安全治理体系的完善、治理能力的提升以及相关业务、产品、服务的开展提供了有益的帮助。

关键词：行业标杆；网络与信息安全；实践分析
中图分类号：TN915
文献标识码：A
doi: 10.11959/j.issn.1000−0801.2020295

Practice analysis of domestic and foreign industry benchmarking enterprises in the field of network and information security

XI Xiaoyin, YUAN Xiaoyun
Research Institute of China Telecom Co., Ltd., Shanghai 200122, China

Abstract: In order to better promote the construction of China Telecom's network and information security governance system, optimize the network and information security product service system, and promote the cultivation and development of network and information security core competence, domestic and foreign industry benchmark enterprises were selected to carry out practical case analysis. The advanced successful experience of benchmarking enterprises in the field of network and information security were summarized, and the current development status and future development trend in the field of network and information security were further combined, and targeted development suggestions and measures were put forward to improve the governance system of China's telecommunications network and information security, improve the governance ability, as well as related business, and the development of products and services provides useful help.

Key words: industry benchmark, network and information security, practice analysis

收稿日期：2020−09−10；修回日期：2020−10−10

1　引言

自 2016 年《网络安全法》颁布以来，我国先后颁布了多项与网络安全相关的政策及法律法规，并进一步将网络空间安全上升为国家战略，明确“没有网络安全就没有国家安全”。在此大背景下，我国安全产业也迎来产业发展风口期。据网络空间安全协会统计数据[1]，2019 年我国网络安全行业总收入为 668.3 亿元，同比增长 21.1%，按年复合增长率 20%计算，预测 2025 年，安全行业总收入将达近 2 000 亿元的规模，如图 1 所示。

作为具备红色基因的大型央企，中国电信充分认识“没有网络安全就没有国家安全”，主动担当综合智能信息服务运营商在网络安全方面的主体责任，全面扎实推进网络强国建设。为更好地推动中国电信自身网络安全服务能力的建设以及产品/服务体系的构建，需要充分汲取国内外行业标杆企业的发展经验，从中找到适配中国电信企业特点的发展方向与发展道路。因此，从电信运营商和互联网厂商两个维度，分别选取具有代表性的行业标杆企业，对这些企业在网络与信息安全领域的实践案例进行分析，总结得到发展的经验和方向，为后续国内运营商网络与信息安全业务的发展提供有价值的输入。

2　电信运营商标杆案例

在电信运营商标杆案例的选择上，既要重点考虑到对标运营商安全业务能力，也要兼顾对标企业的综合实力，即既要具备一定的安全业务能力，又要具备与中国电信相匹配的综合实力。在综合考虑之后，确定选取安全创新能力及营收规模两个维度作为对标运营商的选择标准。其中，安全创新能力以 Cybersecurity Ventures 发布的“2018 年网络安全创新 500 强排名”为基准，营收规模则以 2018 年财富 500 强（电信行业）中的排名为参考依据，最终选定了 AT&T Cybersecurity（网络安全创新排名第 42 位，AT&T 集团营收排名第 20 位）与 NTT Security（网络安全创新排名第 75 位，NTT 集团营收排名第 55 位）作为标杆案例研究的对象。

2.1　AT&T Cybersecurity

AT&T Cybersecurity 已构建了较为完备的网络安全治理体系，在其集团内部设立了 AT&T 安全办公室，全面负责网络安全防护工作及业务运营管理工作。办公室设置有首席安全官（CSO）、安全咨询委员会（SAC）、全球技术运营中心（GTOC）及安全研究中心等机构，共有约 600 名员工。办公室的主要职责是保护 AT&T 全球网络安全，提供从政策/策略管理到安全的解决方案；

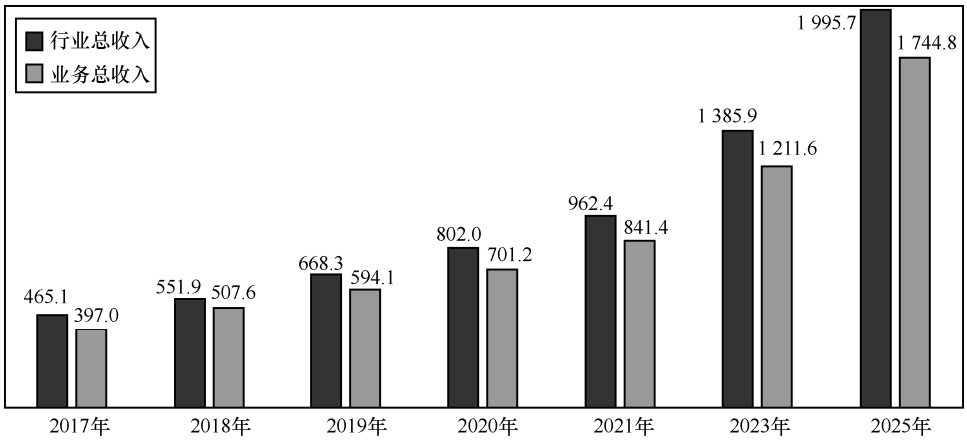

图 1　2020—2025 年中国安全行业规模预测

评审安全措施是否满足行业发展、合规要求及业务需求等。

AT&T Cyberseurity 作为 AT&T Business 的重要组成部分，经过多年的发展与对外并购，已逐渐成长为网络安全业务领域的一个重要力量。截至 2017 年年底，AT&T Cybersecurity 共拥有两千余名员工，在 AT&T 集团所有员工中占比 0.79%。AT&T Cybersecurity 已初步构建了包括资产发现能力、入侵检测能力、安全自动化能力、通信网络安全能力、终端检测与响应能力、威胁检测能力、威胁情报能力及漏洞评估能力在内的八大类核心能力体系。基于核心能力体系，AT&T Cybersecurity 建设了评估与计划、保护与预防、检测与响应三大类产品服务。其中，评估与计划类产品服务主要提供咨询和规划服务，解决客户在安全领域的基本问题，如战略和路线图规划、合规咨询、漏洞扫描和网络安全评估等需求；保护与预防类产品服务包含了入侵检测与预防、DDoS 防护、AT&T 应用层安全等 14 项安全产品服务，通过充分利用专家资源来增强客户在安全事件管理上的能力，有效帮助客户减少因安全事件而引起的损失；检测与响应类产品服务借助 AT&T 威胁管理、AT&T 通用安全管理平台等产品服务，为客户提供网络流量过滤、自动告警、阻止和分析流量等服务，帮助客户有效应对各类网络安全威胁。

AT&T Cybersecurity 依托全球技术运营中心（GTOC），负责对网络安全威胁进行监控、调查、响应、处置等，实行 7×24 h 不间断运营。同时，运营中心也是安全管理办公室的重要组成部分和业务运营的重要保障机构。

2.2 NTT Security

NTT Security 是 NTT 集团的专业安全公司和卓越安全中心，专注于管理安全服务和咨询，并为客户提供集成安全解决方案。NTT Security 在全球范围内共部署了 10 个 SOC，雇佣超过 1 500 名员工，安全从业人员约占 NTT 集团员工总数的 0.53%。

NTT Security 已初步完成了网络安全能力体系的构建，具备威胁情报能力、威胁检测能力、入侵检测能力、企业安全监控能力、漏洞评估能力和安全事件管理系统化能力六大核心能力。并依托网络安全能力体系构建了以威胁信息平台和托管安全服务平台为核心的安全平台体系。其中，全球威胁信息（GTIP）平台用于收集和存储大量威胁信息，用于对威胁信息的管理、分析及自动关联处理。全球托管安全服务（GMSSP）平台为用户提供安全管理平台和安全托管服务，平台具备高级分析能力，能有效检测复杂和新出现的安全威胁，降低用户的安全风险。NTT Security 还充分利用企业内部的安全专家能力和研究开发能力，将这些能力作为 NTT Security 安全能力体系及平台体系的基础保障和发展动力来源。

NTT Security 共部署了 3 个全球威胁情报中心，分别位于日本、美国和欧洲。这些全球威胁情报中心的职能包括威胁研究、脆弱性研究、探测技术开发、威胁情报管理以及为客户提供全天候风险和威胁的检测、防护等服务。

3 互联网公司标杆案例

在互联网公司标杆案例的选择上，从重点安全业务领域出发，聚焦数据安全和内容安全两大重点领域，有针对性地选取阿里云和网易作为主要对标对象。

3.1 数据安全代表：阿里云

阿里云作为中国最大的云服务商，承载着中国 40%的网站，建立世界级防御能力应对云上新型攻击。IDC 发布的《中国云服务提供商，2017 厂商安全评估》，从安全能力、安全策略、安全投入 3 个维度出发，考核 20 余项云安全的相关指标，覆盖云基础设施安全、威胁情报能力、技术先进性、交付与服务能力、合规、生

态等，对中国地区的 11 家最具代表性的云服务提供商进行评估。阿里云成为国内安全等级最高的云服务商之一。

阿里云将安全作为核心竞争力之一纳入战略整体考虑，在组织、制度、机制队伍等方面不断创新。2009 年阿里云成立，设立了安全部。2018 年，阿里云事业群升级为阿里云智能事业群。事业群下设智能安全事业部，主要包含云安全相关的信息安全团队、满足合规性要求的安全审计团队和保护数据中心物理安全及云计算基础设施安全的物理安全团队。同年 8 月，成立数据安全研究院，阿里云数据保护大事记见表 1。

表 1　阿里云数据保护大事记

时间	阿里云数据保护大事记
2012年	阿里云成为BSI在国内审核通过ISO27001的第一家云计算安全服务提供商
2014年	阿里云发布了V1.2版《安全白皮书》，公开透明地公布阿里云的安全体系、数据安全机制
2015年	阿里云第一个发起《数据保护倡议》，将不碰客户数据写入正式文本；同年，通过“全球最严”的数据安全审计，共有内部核心控制点217项通过审计
2016年	阿里云电子政务云平台首批通过中央网络安全和信息化委员会办公室云安全审查（增强级）
2017年	阿里云与国家密码管理局联合为“云上贵州”提供国家级加密保护，是国内首个国家级的加密保护
2018年	成立数据安全研究院

在技术引领方面，阿里云已实现全局威胁感知、全链路数据加密确保用户数据安全。在合规方面，阿里云是全球首家通过 CSA、ISO 22301、德国 C5 附加条款合规审计的云服务商，也是国家首批通过中共中央网络安全和信息化委员会办公室云安全审查（增强级）和云等级保护的四级测评的云服务商。

对内，阿里云制订了《阿里巴巴集团数据安全规范（总纲）》，围绕数据的生成、使用、存储、传输、销毁各阶段，落实数据安全的组织、人员、环境、使用、合作方面的 5 项策略，对数据的全生命周期进行管理。

对外，阿里云积极探索以数据为中心的安全出路，构建以数据为中心的动态、连续的数据安全防护体系。体系包括发挥数据流动价值过程中防止危害到社会、企业及个人利益；通过打通产学研三方联动机制，探索数据安全保护的新方法；加强政策研究和标准输出。在平台安全性方面，通过安全融入设计、自动化监控与响应以及红蓝对抗与持续改进来强化安全运营管控理念，提升大数据平台数据产品的安全性。在确保用户数据安全方面，阿里云建立了面对客户层的客户数据安全方案和保护体系。为确保云平台基础设施安全，设置了云平台自身数据安全认证体系和第三方审计机构审计的 3 套体系。

经过多年努力，阿里云的数据安全能力不断输出，在 2018（第三届）数据安全与隐私保护大会上，阿里巴巴数据安全研究院联合多家单位发布业内首份《数据安全能力建设实施指南 V1.0》征求意见稿，从组织建设、制度流程、技术工具和人员能力 4 个方面入手，为各行业进行数据能力建设提供帮助。同时阿里云还参与了 ITU-T、ISO、CCSA 等国内外组织的标准研究。

3.2　内容安全代表：网易

内容安全日渐成为互联网企业 Top 风控项。国外，Facebook CEO 曾表示，除了在技术上大力投入外，从事内容审核工作的人数也已增加到 3 万多人，每年在安全方面投入高达数十亿美元。YouTube 除了在人力和技术方面投入之外，还成立了“紧急事件负责人”一起协调合作。国内，网易由于其业务（邮箱、博客等）天然的内容安全需求，较早成立了反垃圾（现在称为内容安全）团队，是国内最早以技术驱动的内容安全团队，隶属于网易安全部。经历 20 多年的发展，网易内容安全形成对内、对外两只团队，对内是网易安全部，承担集团服务的基础技术研究工作；对外为易盾团队，是一只商业化安全产品团队，是盈利中心。

网易以“构建‘四位一体’安全防御体系”

为安全抓手，同时将人工智能、大数据分析等新兴技术嵌入“四位”过程中，形成场景化、精细化、智能化的内容安全能力。“四位”包括：基于内容安全场景建立的内容反垃圾技术，实现广告过滤、智能鉴黄、涉政监测等；多技术联动的业务安全防御体系，联动账户安全、全链路联动识别分析，采用验证码、注册保护、登录保护等反作弊技术有效减少有害内容的产生；App 全生命周期的安全防护，包括渠道监测、移动安全加固、移动安全应用于评估等；构建抗 DoS、WAF、漏洞扫描、风险监测、入侵评估、安全培训等多层次立体防护的网络安全能力。

在反垃圾技术方面，网易已经通过了 3 代的升级：纯文本垃圾阶段，通过建立在关键词、黑白名单、过滤器和分类器上关键技术进行识别过滤；图文垃圾阶段，反垃圾技术基于内容特征识别、贝叶斯过滤、相似度匹配和规则系统；融媒体实时检测阶段，升级 AI 反垃圾，通过大数据分析（用户行为、用户分类）、人机识别、人工智能和机器学习（语义识别、图像识别），覆盖了文本、图片、语音和视频等领域。

在对外产品上，网易易盾提供文本监测、图片监测、音频监测和视频监测四大类基础服务，以及合规解决方案、人工审核、舆情管家、智能审核系统等增值服务。

4 标杆案例分析

在运营商领域，通过对 AT&T 和 NTT 两大国际标杆运营商网络安全业务的对标分析，可以发现这些标杆运营商均已在企业内部构建了较为完备的网络安全治理体系、网络安全核心技术能力及安全运营能力体系，并以此为依托对外开展网络安全业务。运营商构建的网络安全能力一般包含合规管控能力、不良信息治理能力、威胁检测能力、入侵检测能力、漏洞评估能力、安全事件系统化管理能力、威胁情报能力、安全态势感知能力等，通过构建网络安全核心能力体系来推动企业网络安全能力的不断提升。在网络安全业务的具体发展模式上，不同运营商的业务发展重心略有差异，如 NTT Security 更侧重安全咨询业务，而 AT&T Cybersecurity 更侧重传统的网络安全业务。

在互联网厂商领域，通过对国内互联网头部企业的对标发现，互联网公司更侧重基于人工智能的数据和内容安全核心能力建设，通过 AI 技术强化对数据和内容安全的保护能力，形成真正的智能防御屏障。在安全运营能力的沉淀和开放方面，互联网公司中以输入基础架构、能力和标准为主，开放平台引入安全厂商合作专业产品和解决方案。

5 未来展望

从国家战略视角看，习近平总书记曾明确提出“网络安全就是国家安全”，将网络安全上升到国家安全的高度，由此可见网络安全问题对国家、社会和企业带来的巨大影响。对企业而言，只有搭建起健全完善的网络安全体系，才能切实提高其经营管理、生产发展的整体效率，实现企业的安全性、规范性、有效性。

从社会发展视角看，随着“新基建”战略的加深布局和加快落地，未来必将带来新一轮信息化基础设施建设的高峰。在推动社会经济模式和产业模式发生根本性变革的过程中，网络安全作为“新基建”必不可少的安全保障，将会迎来新一轮的发展机遇。国家在交通、能源、制造等行业信息基础设施的建设过程中，将进一步加大网络安全的投资力度，行业整体市场有望得到快速增长。未来，随着智慧城市、数字经济的进一步发展，网络安全更趋向于综合安全能力和运维能力一体化需求，从网络、云、终端、用户和业务等全维度为经济的发展提供安全保障[2]。

从技术发展视角看，随着新技术在网络安全领域应用的广度不断加大，深度不断加深，整个网络安全产业将呈现横纵向同步扩展的模式。如 5G、AI、大数据、云计算等新兴技术将进一步推动 IT 与 CT 的融合，促进网络安全防御能力的智能化与云化，使安全成为推动新兴技术持续发展的关键要素[3]。而新技术在带来技术进步的同时，也同步催生海量的网络安全市场需求。以大数据技术为例，大数据是监测网络状态、分析网络行为和诊断网络故障的关键技术手段之一。基于大数据的网络安全态势感知则是未来网络安全技术发展的重要方向之一。通过构建基于大数据的网络安全态势感知体系，能在充分了解当前网络安全态势的基础上实现科学分析和预测，以便有效应对网络安全新威胁和新挑战[4]。

6　对中国电信的启示

中国电信作为国内三大电信运营商之一，与其他互联网公司及安全厂商相比，全网管道连接和流量汇聚是核心优势所在。同时，中国电信作为具备红色基因的大型央企，肩负着助推社会发展的社会历史责任，在国家深化落实“新基建”战略的过程中，做好国家的通信网络安全保障工作更是中国电信义不容辞的责任。对中国电信而言，为更好地应对网络安全的发展趋势，可以从以下几个方面加强建设工作。

首先，在组织和战略层面，应建立独立、垂直的安全治理架构，强化网络安全组织的能力建设，通过岗位体系架构针对性优化和完善，起到提升组织治理能力的目的。同时，全面规划中国电信安全战略及发展路径，做好网络安全架构的顶层设计，为后续的网络安全业务发展提供良好的组织保障。

其次，在技术和能力层面，接应中国电信 CTNet2025 网络演进目标，构建企业网络安全技术架构，打造自主可控的网络安全核心技术能力体系。加快网络安全能力资源的池化、云化和智能化，聚焦预测、检测、响应和防御四大类网络安全能力，形成持续自适应的主动防御体系。聚焦 5G、工业互联网、物联网等重点应用场景，推动基于应用场景的安全技术创新。加强对前瞻技术领域研发投入力度，积极开展量子安全、零信任架构等重点领域的技术前瞻研究[5]。

再次，在产品和服务层面，基于中国电信端到端云网融合安全能力，打造“一站式、一体化、一条龙”网络安全产品服务集群，为政府及企业、家庭及个人客户提供“事前预防检测、事中防护与控制、事后审计与恢复”的安全服务。进一步强化 AI 赋能，提供智能化的安全产品与服务，构建智能化的 ToG、ToB、ToC 和 ToH 产品与服务体系。

最后，在趋势和生态层面，积极参加国家网络安全产业园区建设，加强标准创新、赋能产业生态、创新协作机制，成为同业领先的网络信息安全能力聚合引擎。加大创新核心科技的研发力度，推动自主可控的平台建设。同时，继续秉承开放合作的理念，充分利用管道和资源优势，加大能力开放、整合产业资源、聚焦行业应用、联合产业上下游，协同构建网络安全新生态[6]。

参考文献：

[1] 中国网络空间安全协会. 2020年中国网络安全产业统计报告[R]. 2020.
CyberSecurity Association of China. Statistical report of China’s network security industry in 2020[R]. 2020.

[2] 孙会峰. “新基建”视野下网络安全新趋势[J]. 中国信息安全, 2020(5): 41-43.
SUN H F. New trend of CyberSecurity from the perspective of “New Infrastructure”[J]. China Information Security, 2020(5): 41-43.

[3] 陈山枝. 发展 5G 的分析与建议[J]. 电信科学, 2016, 32(7): 1-10.
CHEN S Z. Analysis and suggestion of future 5G directions[J].

Telecommunications Science, 2016, 32(7): 1-10.

[4] 王海涛, 向婷婷, 王雪梅. 网络安全态势浅析和安全技术趋势展望[J]. 数据通信, 2020(4): 35-37.
WANG H T, XIANG T T, WANG X M. Analysis of current network security situation and prospect of security technology trends[J]. Data Communications, 2020(4): 35-37.

[5] 朱光. 信息网络安全技术未来发展趋势[J]. 河南科技, 2020(1): 26-28.
ZHU G. On the future development trend of information network security technology[J]. Journal of Henan Science and Technology, 2020(1): 26-28.

[6] 朱常波. 中国联通网络安全战略的思考与实践[J]. 邮电设计技术, 2019(4): 1-5.
ZHU C B. Consideration and practice on China Unicom network security strategy[J]. Designing Techniques of Posts and Telecommunications, 2019(4):1-5.

[作者简介]

奚晓音（1981− ），男，现就职于中国电信股份有限公司研究院，主要研究方向为网络与信息安全领域的政策、法规、标准、行业趋势、安全产品及服务。

袁晓云（1983− ），女，现就职于中国电信股份有限公司研究院，主要研究方向为网络安全政策、法规、行业趋势、网络安全产品与服务。