网络安全域在大型石油企业中的应用

■ 张蓓 冯梅

(中国石油勘探开发研究院 北京 100083)

摘 要：本文首先介绍了网络安全域技术和常见的安全域划分方式，分析了中国石油网络安全现状以及应用网络安全域技术的必要性，最后基于具体规划设计方案，对中国石油的网络安全域划分模型和实施要点进行了详细阐述。

关键词：网络安全域 等级保护 中国石油网络

中图分类号：TP309

1. 引言

随着社会信息化建设的逐步深入，各行各业对于信息系统的依赖程度逐渐增加。尤其像中国石油天然气集团公司（以下简称“中国石油”）这样的国有特大型企业，其规划建设的信息系统几乎涵盖了勘探生产、办公管理等所有的业务板块，承载着大量的能源数据和商业经济信息。因此，信息系统的安全直接关系到企业的生存与发展，甚至可能影响国计民生，企业必须尽力提高自身的安全保障能力，确保这些系统的安全。

纵观当前中国石油所处的应用服务环境，不难看出网络已经成为信息系统必要的承载设施，是信息传播和共享的基础平台。建设安全可靠的承载网络是保证信息系统安全可靠运行、尽可能发挥作用的基础。然而开放、互联的网络环境虽然为企业带来了丰富的资源，同时也带来了潜在的风险，使得企业面临木马、病毒、入侵等更多的威胁，信息安全问题日益凸显。因此，如何科学、全面、有效地进行网络安全防护就成为企业当前亟待解决的问题。本文将重点介绍网络安全域技术，并结合具体的规划设计方案，分析该技术在中国石油网络安全建设过程中发挥的作用。

2. 网络安全域技术

2.1 技术概述

网络安全域是指同一系统内根据信息的性质、使用主体、安全目标等元素的不同而划分的不同逻辑子网或网络。每一个逻辑区域有相同的安全保护需求，具有相同的安全访问控制和边界控制策略，区域间具有相互信任关系，相同的网络安全域共享一样的安全策略[1]。

网络安全域技术基于国际上先进的“同构性简化”的理念，将一个复杂的大型网络的安全问题转化为若干个较小区域内更为单纯的安全保护问题。通过安全域的划分，可以明确网络边界，形成清晰、简洁、稳定的组网架构；明确各区域的防护重点，实现网络之间和各系统之间的有效隔离和访问控制，从而达到化繁为简、尽在掌控的目的。

2.2 常见的划分方式

目前国内外比较常用的安全域划分方式有3种，分别是按照业务系统划分、按照防护等级划分和按照系统行为划分[2]。

2.2.1 按照业务系统划分

按照业务系统划分是指将每个业务系统划分一个独立的安全域，单独进行防护，例如按照OA系统、ERP系统、加油站系统等分类划分，

如图 1 所示。

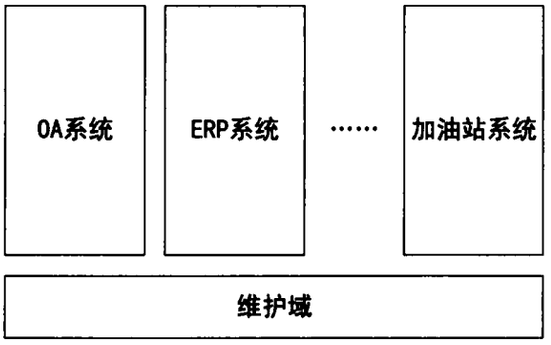

图 1 按照业务系统划分安全域

这种划分方式具有自然形成、划分简单的优点，对信息系统结构的改变最小。但是由于相同安全等级的信息系统需要采用同样的防护手段，这就产生了防护复杂、重复投资等不足。

2.2.2 按照防护等级划分

按照防护等级划分是指依据网络中信息资产的价值划分出不同的防护等级，相同等级构成相同的网络安全域。现有的信息系统将按照信息资产价值进行分级，同级别的信息系统将被划分在同一个域内，采用同样的防护手段，如图 2 所示。

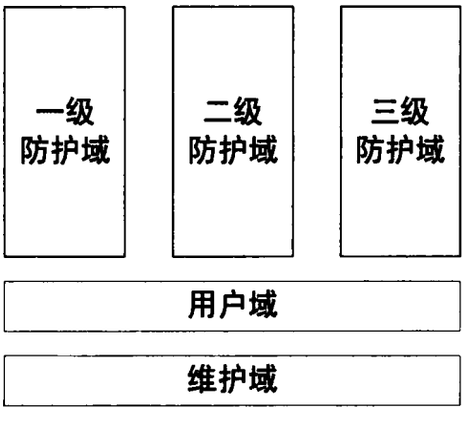

图 2 按照防护等级划分安全域

这种划分方式具有防护简单，保护投资等优点。但是由于按防护等级形成的网络区域与按业务系统形成的网络区域有较大的差别，对已有系统重新调整、整合的难度会很大，可能会对系统的正常运营和性能产生一定的影响。

2.2.3 按照系统行为划分

按照系统行为划分是指按照信息系统的不同行为和需求来划分相应的网络安全域，并根据信息系统的等级和特点选择相应的防护手段。例如，美国国家安全局（NSA）制订的信息保障技术框架（Information Assurance Technical Framework，IATF）就建议按照系统行为划分安全域，划分方式如图 3 所示。

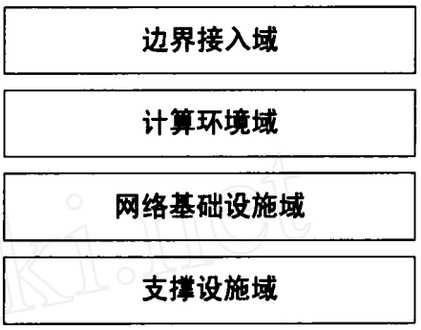

图 3 按照系统行为划分安全域

这种划分方式充分考虑了用户使用信息系统的行为和现状，同时考虑了信息系统的防护等级和防护类型，能够对常见的威胁进行更细致的防护，实施成本相对较低，对业务可用性的影响较小。但是该划分方式需要详细分析用户使用信息系统的行为、特点和面临的威胁，因此工作量较大。

3. 中国石油网络安全现状

3.1 安全威胁分析

作为中国最大的原油、天然气生产、供应商和最大的炼油化工产品生产、供应商，中国石油拥有包括生产网络、办公管理网络、矿区服务网络、海外网络等在内的多个子网。经过多年的信息化建设，已经逐步形成了应用多元、辐射全国的网络体系，同时庞大、复杂的企业网络也对网络安全建设提出了挑战。目前，中国石油在网络安全方面主要面临以下威胁：

◆ 网络的物理边界日趋模糊

随着互联网技术的发展，中国石油网络中的信息系统越来越多地与互联网发生信息交互，网络内部的子网和子网之间也存在着单向或双向的信息交互。此外由于电子商务等应用的需要，商务伙伴可以在一定权限下进入到彼此的网络内部。这些因素使得网络边界更多的是一个逻辑边

界，内外网以及子网之间的物理边界日趋模糊。

◆ Internet 出口数量大、难于管理

中国石油的网络中存在大量的 Internet 出口，同时用户数量十分庞大、用户行为不规范，这使得网络的可控性差、防护难度大。

◆ 入侵防御和审计手段不够完善

目前中国石油的网络在入侵检测和安全审计方面还存在诸多不够完善的地方，如安全策略的一致性检查不彻底，缺乏统一的规范，网络检测监控体系关联性和智能分析能力不足等等。

3.2 法律法规要求

许多国家和地区都针对信息系统的安全制定了相应的法律法规，企业在进行信息系统建设和网络规划时，必须遵守这些政策法规，满足相关的信息安全规范。2003 年，中央办公厅、国务院办公厅转发的《国家信息化领导小组关于加强信息安全保障工作的意见》(27 号文) [3] 中，已经明确指出各类信息系统必须分等级实行安全保护。2007 年，国家部委、行业组织先后下发了一系列关于信息系统等级保护方面的政策和规范，明确要求企业加强信息安全保障工作，建立完善的信息安全保障体系，并提出了对关键信息系统实施信息安全等级保护的合规性要求。中国石油作为国有特大型企业，其信息资产的安全关系着国计民生，而网络是信息系统的重要组成部分，网络安全建设必须满足等级保护相关政策和规范的要求，确保信息系统的安全、稳定运行。

4. 网络安全域在中国石油的应用方案

当前的网络安全威胁和法律法规的要求已经成为中国石油对于网络安全体系进行研究的重要驱动因素，企业专门设立课题，研究建设网络安全架构的方法和技术。由于中国石油的网络庞大而复杂，针对每一项信息资产单独进行防护是不可行的，而对整个网络设置相同的安全等级，难免会造成防护缺乏层次和重点。因此，网络安全域的“同构性简化”思路就显得非常满足中国石油网络安全防护的需求，本章将具体介绍在中国石油应用网络安全域技术的规划设计方案。

4.1 安全域划分模型

复杂而庞大的中国石油网络在网络的不同层次和不同区域，关注的角度不同。设计安全域划分方案时，既要考虑网络的管理属性和业务属性，同时要考虑安全域的实施问题，不能影响现有业务的正常运行，此外还要兼顾实施的成本。在这样的情况下，任何单一的安全域划分方式都存在不足，独立应用哪种方式都不能实现网络安全域的合理划分。因此需要 3 种方式综合应用，互相取长补短，根据网络承载的业务和企业的管理需求，有针对性地选择合理的安全域划分方式。

在具体划分网络安全域时，需要采用分区的方式，有计划分步骤地实施。通过前期对国内外大型企业网络安全建设的调研，我们发现按照业务类型将网络进行隔离，已经成为一种趋势，其优点是可以有效地隔离威胁，保障企业的核心业务安全运行。例如某国家级电力公司系统安全防护模型就将网络划分为生产控制和管理信息两个大区，如图 4 所示。

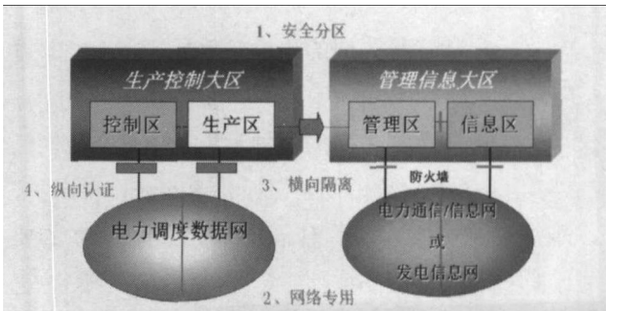

图 4 某国家级电力公司系统安全防护模型

另一方面，中国石油进行网络安全建设的根本目标是要保障业务的正常运行，因此业务类型就成为企业划分网络安全域的第一要素。具体而言，整个网络按照业务类型将划分为内网和外网两部分，内网和外网用户端之间实行隔离，这样就实现了对内、外服务的分离，规避了来自外网的威胁，大大降低了内网发生安全事件的风险。

接下来分别在内网和外网内按照业务系统方式进一步划分安全域，从而得到如图 5 所示的网络安全域初步划分模型。可以看出，安全域的划分可以清晰地标识出网络边界，明确网络防护的

对象和目标，区分安全责任和范围，从而使得大而复杂的网络的安全问题由繁化简；而且安全域的划分原则充分考虑了企业信息化建设不断发展的大背景，在未来会有更多的子网加入进来，到时只需对相应的安全子域进行调整，整个网络的组网架构将保持简洁、稳定。

最后，我们对图 5 中的每一个子域按照系统行为和防护等级相结合的方式进行安全域细分，划分出边界接入域、服务集中域和基础保障域，其中，

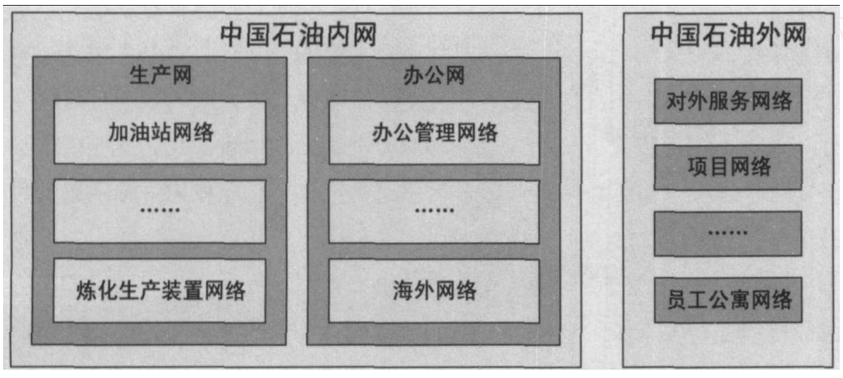

图 5 中国石油网络安全域初步划分模型

◆ 边界接入域的防护对象是信息系统的边界。

◆ 服务集中域的防护对象是信息系统，包括信息系统之间的防护以及信息系统内部防护，在服务集中域中，信息系统将按照等级保护的要求分级防护。

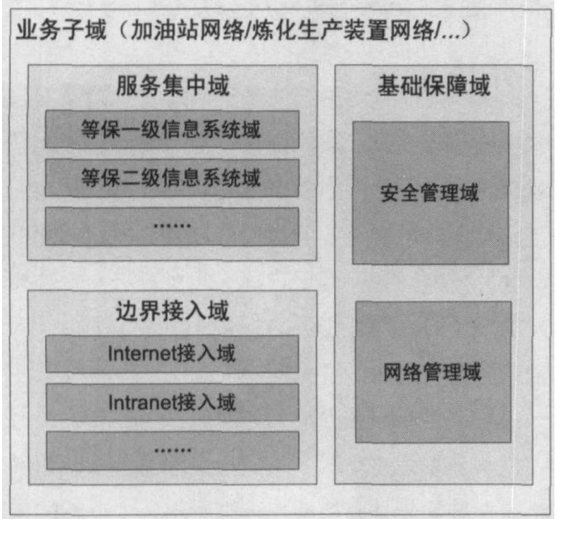

图 6 业务子域安全域划分通用模型

◆ 基础保障域是各个安全设备、软件以及系统的管理控制中心的集合。

业务子域安全域划分的通用模型如图 6 所示。

整个网络经过安全域划分形成若干个小的区域，接下来将根据各个区域的安全需求、防护重点，因地制宜地实施安全防护策略。我们将从可用性、机密性、完整性、可控性和可审查性 5 方面对安全威胁和风险进行分析，确定最佳的安全防护策略，配套实施安全审计、资源控制、检测监控、身份认证等相应的技术和产品，最终实现对中国石油网络的整体防护。

4.2 安全域实施要点

以上对安全域划分模型进行了说明，在具体实施安全域划分方案时，需要注意以下几点：

◆ 合理划分安全域，明确子域边界

目前中国石油的各个网络之间还存在着边界划分不清的问题，如办公管理网络和矿区服务网络、项目网络等子网互相融合，边界模糊。在业务域划分时必须明确各网络的分割以及网络之间的关系和防护标准，形成清晰的安全域边界。

◆ Internet 出口统一集中

来自 Internet 的安全威胁多种多样，各种攻击技术不断地出现和发展，网络安全防护技术总是处于滞后，过多的 Internet 出口不但增加了防护和维护的费用，也给来自网外的各种威胁提供了更多的通道。根据国内外大型企业的网络安全实践，集中 Internet 出口能够实现统一管理、节省网络安全防护和维护的费用。因此，安全域的划分方案应尽可能地集中 Internet 出口。

◆ 建立安全管理保障体系

网络安全是三分技术，七分管理，必须通过

一系列严格的管理制度和行为准则进行约束，由管理层自上而下的严格执行，才是解决网络安全问题的最根本方法。

5. 结论

网络安全域技术在中国石油的应用将使得企业网络满足相关法律法规对等级保护的要求，从网络层面有效杜绝来自外部的安全威胁，大大降低生产及业务重要数据的安全风险，整体提高信息系统安全性。同时，通过有效的网络安全域结构划分，以及 Internet 访问集中部署，能够有效规范、控制及管理生产及业务的网络流量，节省链路带宽，减少运维成本。当然，技术只是保障网络安全的手段，而最终确保网络安全的关键在于企业的管理，网络安全必须得到高级管理层的高度重视和密切配合，必须制定一系列的安全管理制度来保障，并将其切实地落实下去。最后，网络安全建设是一个长期的、不断完善的过程，需要随时研究、评估新的威胁带来的安全风险，并针对安全风险，将控制措施不断地整合到网络安全系统中。

参考文献：

1. 张智杰．安全域划分关键理论与应用实现[D]．昆明：昆明理工大学，2008.

2. 赵新亮．江西国税信息系统安全域划分与等级保护设计 [D]. 上海：同济大学，2006.

3. 中共中央办公厅，国务院办公厅．《国家信息化领导小组关于加强信息安全保障工作的意见》(中办发 [2003]27 号). 2003.

作者简介：

张蓓，中国石油勘探开发研究院，在职研究生，油气信息工程专业；

冯梅，中国石油勘探开发研究院计算机应用研究所，总工程师，信息工程专业。

惠普助力 AJ Lucas 集团 IT 变革，为未来发展铺平道路

本刊讯 9 月 23 日，惠普和 Astron Technology 公司宣布与 AJ Lucas 集团有限公司（ASX：AJL）签订为期 5 年，价值 600 万澳元的服务协议，以继续支持其业务增长，降低技术成本。

AJ Lucas 是一家为澳大利亚和亚太地区的企业和机构提供工程和建筑服务的供应商。惠普和惠普钻石级代理商 Astron Technology 公司与其达成合作协议，对 AJ Lucas 的数据中心、台式电脑和企业通信基础设施实施变革。随着项目前期阶段告一段落，惠普将基于一个为期 5 年的远程监控服务协议，负责管理操作环境和数据中心。

AJ Lucas 总部最近迁至澳大利亚悉尼，这为优化业务技术基础设施提供了绝佳的机会。惠普和 Astron Technology 公司负责帮助 AJ Lucas 迁移至新一代数据中心，其中包括了 32 台惠普刀片系统服务器和刀片系统服务器。

此外，惠普为 AJ Lucas 在公司范围内设计和实施了整合的统一通信解决方案。该方案以新公司总部为核心，集成了移动电话、IP 电话、台式机和笔记本电脑，并包含 300 多台惠普笔记本电脑。