地震信息网自适应网络安全技术模型研究*

刘云华[1]，刘 治[1]，单新建[1]，李卫东[2]

（1. 中国地震局地质研究所，北京 100029；2. 中国地震台网中心，北京 100045）

摘要：对地震信息网存在的一些安全隐患做了初步调研，在此基础上，提出了自适应网络安全模型及法规、技术和管理三种因素相互配合的防御体系，使网络安全以合理代价控制在可以接受的范围内。

关键词：地震信息网；安全需求；自适应；管理

中图分类号：TP311.56 **文献标识码**：A **文章编号**：1000-0666(2011)01-0096-06

0 引言

随着信息化进程的深入和互联网的迅速发展，人们的工作、学习和生活方式正在发生巨大变化，效率大为提高，信息资源也得到最大程度的共享。但在网络给人们带来巨大便利的同时，紧随信息化发展而来的网络安全问题也日渐突出，如果不能很好地解决这个问题，必将阻碍信息化发展的进程，也会给我国地震事业的发展带来很大影响。

2008年汶川8.0级大地震发生时，广大民众为了得到最新的地震信息，纷纷登录地震信息网，结果造成网络过度拥挤，使得国家地震信息网和各省地震局官方网站不堪重负，可见当今信息社会网络建设的重要性和进行行业网安全风险防范及风险评估的必要性。

网络技术发展日新月异，尽管人们采取了防火墙、入侵检测系统等各种方法来加强网络安全，但还是有黑客能够通过一些系统漏洞找到新的办法绕过防御体系进行攻击。传统的防御方式是通过发放系统补丁来防止该漏洞被黑客利用，而对未知的漏洞则无应对措施，这样防御就永远落后于攻击，是一种被动式的安全措施。相比较而言，自适应网络安全模型能够根据网络动态变化情况及时做出相应的调整，进而维持网络系统相对安全稳定的状态。

鉴于自适应网络安全模型的优势，本文就地震信息网目前存在的一些安全隐患做了初步调研，在此基础上，提出针对地震信息网的自适应网络安全模型，以确保网络安全以合理代价控制在可以接受的范围内。

1 地震信息网概述

中国地震局地震信息系统的建设始于1994年，“八五”期间设立专项，在北京建立了小型的计算机网络系统，并通过我国当时的NCFC工程的科教网和INTERNET联结，成为我国最早与国际互联网接轨的行业网之一。

“九五”期间中国地震局建设了行业信息网——中国地震信息网络，中国地震信息网络通过中国电信的CHINAPAC信道将29个省级地震局计算机网络联结起来，构成了中国地震局全国地震通信网络。中国地震信息网络干线使用速率为64 Kbps的分组交换网信道（X.25）进行省地震局计算机网络之间互联，中国地震局自建Vsat卫星系统为省级节点提供了不低于9.6 Kbps的信道（阴朝民，2001）。

20世纪末，中国地震局开始组织“十五”项目的立项，全国地震信息通信系统的建设作为中国数字地震观测网络工程的6大系统之一，成为中国数字地震观测网络工程各个系统的信息基础设施。全国地震信息服务系统在“九五”全国地震信息网络建设的基础上，将中国地震信息网络扩大到

* **收稿日期**：2010-02-26.
基金项目：国家科技部地震行业专项基金（200708015，200708049）资助.

709 个节点，即 41 个省级节点，60 个大中城市节点，300 个县和 303 个地震台站节点以及 5 个大专院校、科研院所节点。全国主干信道采用8 MB的 SDH 链路，大部分省级地震计算机网络采用 SDH 链路联结到台站，为地震观测系统提供网络化平台，全面支持数字地震网络观测工程的“网络到台站，IP 到仪器”的要求（陈会忠，2007）。

2008 年该项目顺利通过验收，这一项目的建成，提升了我国地震监测能力，增强了大城市地震烈度速报能力以及强震动流动观测能力，提高了地震应急指挥的多级联动和应急信息的协同共享能力。

从覆盖范围来看，地震信息网是一个广域网，因为它覆盖了全国的 31 个省、市、自治区；如果从用途上来进行划分，应归属于专用网，因为它是地震部门为本单位的特殊工作需要而建立的网络。从这两方面来看它有着与其他部门如电力、税务、金融等专用网相似的地方，但业务性质的不同决定了它有着与这些专用网的不同之处。这些部门的专用网与互联网是物理隔离的，只是在行业网内部交换信息，而地震信息网在建设初期，考虑到业务工作展开的便利性，并没有将行业网和互联网完全隔离，大部分工作人员既处在行业网内，又挂在互联网上，这一特点使得地震信息网的安全状况比较复杂，不可避免地存在安全隐患。

我国地震信息网是大规模的、综合性的、高性能的大型网络系统（中国地震局监测预报司，2003）。从体系架构上分为骨干网和区域网，即在全国范围内包括 1 个国家中心，41 个区域中心以及京区直属单位，在区域中心下设市县节点及台站节点。整套系统在建设规模、系统功能、各项技术指标方面均到达了国内同行业的先进水平。行业网实现了地震系统行业内部各区域中心节点、直属单位与国家中心节点的高速互联互通，为系统内各业务应用提供基础网络平台。

（1）全国骨干网

地震局行业系统全国骨干网，涉及国家中心和41 个单位区域中心，信道数量 163 条，包括：1 条互联网出口、1 条内部光缆、8 条京区直属单位的 100 MB 专线、153 条区域中心、省直属单位的长途专线。网络拓扑结构见图 1。

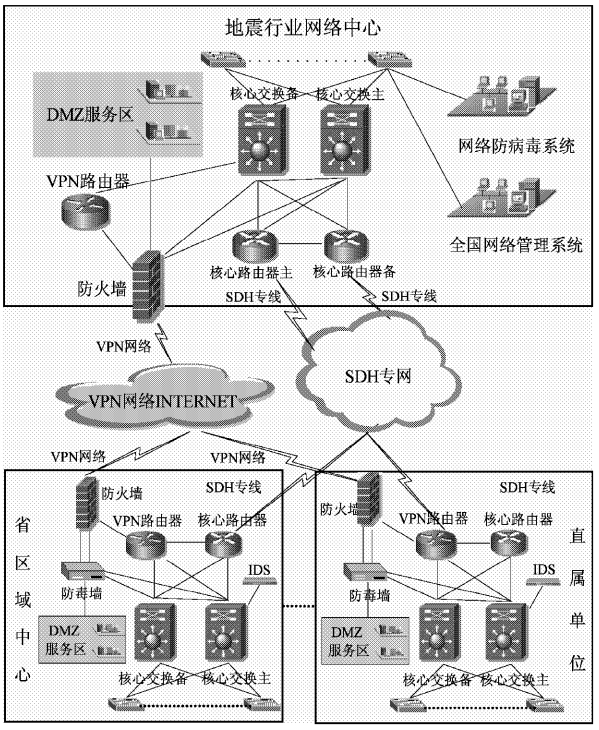

图 1　地震信息网络拓扑示意图

Fig. 1　Topological diagram of earthquake-information network

（2）区域中心网络

区域地震信息服务节点包括 31 个区域防震减灾中心地震信息服务部和 10 个直属单位地震信息节点，分别建在各省、自治区、直辖市地震局和中国地震局有关直属单位。区域地震信息服务节点担负省级地震局和直属研究单位的地震通信系统枢纽和地震数据信息共享服务的职责和任务。

通信需求是网络结构设计的主要依据，网络结构设计是系统集成工作的主要内容。中国地震台网中心等单位根据前兆、测震、应急、活断层等子项的业务需求，结合区域的具体情况，进行了以信息服务系统为基础平台的网络结构设计，对各个子项的通讯需求进行了资源整合和网络优化。典型区域中心网络整体网络结构设计为三层，设计如下：

①一级节点为核心层，即区域中心；

②二级节点为汇聚层，主要由城市、县、台站节点组成，除承担本节点的信息服务任务外，还承担三级节点的汇聚任务；

③三级节点为接入层，主要是无人值守台站，包括测震台站和前兆台站。

2 地震信息网承载业务及安全需求分析

中国地震信息网络信道作为数据传输平台，汇集了 152 个国家级数字地震台、2 个台阵、31 个区域数字地震台网、流动地震台网、火山监测台网、国家强震动台网、其他企事业单位自建地震台网的数据，汇集了全国 300 个地震前兆台站的数据，汇集了全国 31 个省级中心、60 个大中城市和 300 个县级地方地震机构节点和 300 个地震台站节点的地震监测预报、震害防御和应急响应等方面的信息和数据，以及全球主要地震数据中心的地震活动数据和信息。这些数据包括测震台网的连续波形数据和前兆台网的电磁、形变、重力、地下流体、GPS 观测数据及元数据等。

2.1 前兆、测震业务实时数据传输接收

信息网络中智能化数据管理系统对汇集到国家台网中心的地震观测数据和前兆观测数据进行常规的数据处理；统一管理集中与分布结合的存储资源，按照各类数据不同的特点和格式进行存储；产生地震目录、地震观测报告和地震事件波形数据的地震台网常规数据产品以及综合前兆观测报告（王建国等，2009）。系统能方便地通过网络自动进行检索和提取，进行综合数据服务。

2.2 电视会议、VOIP 等业务

中国地震台网中心、各一、二类区域及直属单位都布设了 VOIP 系统。在地震应急工作中，当外界通讯受到限制时，该系统就可发挥作用，也可以召开电视会议，提高工作效率（李俊，秦嘉政，2009）。

2.3 政务办公业务

由 1 个国家中心、41 个区域中心组成的功能完备的政务系统、带宽为 2 MB。地震政务系统涉及到两个网络平台（涉密网、行业网）的多套软件，如涉密公文传输系统、涉密 OA 系统、行业网办公应用系统、门户网站、地震政务数据、地震政务标准规范等。涉密网部署包括涉密公文传输系统、涉密 OA 系统和地震政务数据。公文传输系统发的文件同时可以保存到 OA 系统，再由 OA 系统保存到涉密网档案库中，供用户查询使用；行业网部署包括办公应用系统、门户网站以及政务数据。办公系统和门户网站之间有数据交换，门户网站通过办公系统由领导行使行政审批动作。

2.4 对外公共服务业务

地震信息网络是全国地震科技文献服务的信息化平台，它构建了种类齐全、结构合理的地震科技文献资源保障体系和网络服务体系，为地震监测预报、地震灾害预防、地震紧急救助和地震科研服务。

地震信息网络也是中国地震数据共享平台，它分级分类地向各种目标用户，如政府、科研机构、社会公众以及本单位内部工作人员等，提供地震科学数据共享服务，并与国际数据中心进行地震数据交换。地震部门通过地震信息网络发布权威的震情信息和地震灾情信息、地震监测预报、震害防御、应急响应三大体系的工作信息等。地震部门的门户网站是公众了解地震灾情、学习地震知识、接受服务的窗口。

从以上业务描述可以看出，地震信息网作为地震监测数据传输处理平台、电子政务服务平台、地震数据共享平台和地震社会服务平台，承担着行业计算机信息网络的核心管理任务，保证其安全的重要性可见一斑。其承载的数据极其重要，其发布的地震信息具有敏感性，涉及社会稳定和谐。因此，地震信息网络系统一方面要考虑内部网络的安全，另一方面要考虑面向公众服务的网络安全，具有很高的网络信息安全需求，在信息保密、权限控制、信息存储、信息传输、系统安全等方面均须高度重视。

（1）信息传输的机密性、完整性

重力、GPS 等数据涉及国家地理信息秘密，具有保密要求，因此要求在业务处理中必须使用涉密政务网来传递这部分信息，以保证其安全。

（2）权限控制

电子政务需要划分成若干个安全域。不同的安全域中，对安全的要求、级别是不一样的，因此需要把使用不同级别政务信息资源的用户划分成不同类型，实现不同类型人员对不同级别信息访问的控制策略。

（3）信息存储

地震科研工作需要长期观测资料的积累，因

此对各个台站采集、传输过来的专业数据应保证其长期存储的安全性。

（4）信息传输的可用性

观测资料要具有连续性，因此要求数据传输过程不能中断，保证传输信道安全、畅通。

（5）系统安全

对于资料的处理分析需要系统的支持，因此需要保证各专业系统的安全。

网络是变化的、风险是动态的，鉴于目前网络技术更新快的特点，传统的静态防护技术受到了严峻的挑战，笔者将动态网络防御这一概念引入到地震信息网，探索适用于本行业专用网的安全模式。

3　基于自适应网络安全模型的安全体系

现代安全观强调安全的整体性，安全被看成一个与环境相互作用的动态循环过程，在此思想指导下，笔者提出如图 2 所示的动态防御模式。

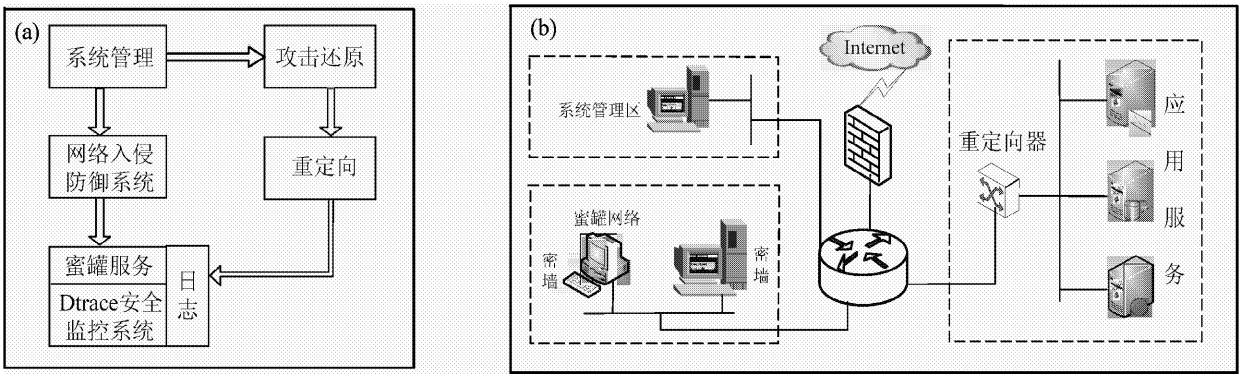

图 2　自适应网络安全模型

（a）流程图；（b）拓扑图

Fig. 2　Topological diagram of self-adaptable network security model

（a）Flow chart；（b）Topography

图 2 为基于动态跟踪的主动防御系统的总体架构，该主动防御系统部署在内部网中。下面对每部分作简单说明。

（1）蜜罐网络。蜜罐网络的工作原理就是采用蜜罐技术，用特有的特征吸引攻击者，“诱敌深入”，对攻击者的各种攻击行为进行分析处理，找到有效的应对方法。通过部署这样的网络，对黑客攻击进行追踪和分析，能够捕获黑客的击键记录，了解黑客所使用的攻击方法等（赵晓飞，2008），为防御入侵提供实时、动态的策略。在蜜罐网络中，使用蜜墙作为蜜网与外界的交互。

（2）网络入侵防御系统。网络入侵防御系统部署在蜜墙上，是蜜网与外界交互的通道。该系统对外能识别已知攻击，对内则对黑客从蜜网发出的攻击进行过滤和修改，使之无法威胁其他网络设备。可使用 Linux 下的 netfilter/iptables 和 snort－inline 联动的方式进行设计（The honeynet project，2004）。

（3）安全监控系统。安全监控系统是负责主机安全和攻击检测的关键模块，部署在蜜罐上，用于监控黑客行为，检测未知攻击。可利用 Linux 下的开源工具 DTrace 实现（Mallela，2006），它是一个强大的动态跟踪框架，用户通过它能够对正在运行的系统跟踪来查看问题。

（4）系统日志。系统日志分为 2 类，分别是本地日志和系统日志数据库。本地日志部署在蜜罐上，用于保存 DTrace 对蜜罐主机的监控记录（Nakhimovsky，Herrington，2006）；系统日志数据库部署在蜜墙上。

（5）攻击还原。攻击还原部署在系统管理主机上，对网络攻击行为进行还原。可根据系统日志数据库中的记录，利用 Linux 下的开源工具重建攻击数据包，然后对相应的蜜罐进行攻击试验以确定该攻击行为。

（6）重定向器。重定向器部署在真正的应用服务网络上。该模块的主要功能是将异常通信转移至提前设计和部署好的蜜网诱骗模块中进行监测，并保证正常访问和工作的网络连通。可以通过智能路由器重定向交换机或者重定向防火墙来具体实现。

以上思路只考虑了技术方面的因素，而忽略了法规和管理因素。尽管技术措施是实施网络安全防护的基础，但仅依靠技术来实现网络安全是不可能的，完善的网络安全体系需要合理地协调法规、技术和管理三者之间的关系。因为网络安全本身就是一个集技术、管理和法规综合作用为一体的系统工程，只有三者相互配合才能增强网络系统抵御风险的能力。

因此我们应该建立以法规为依据，以安全管理为核心，以技术为手段的网络安全体系（图 3），由图 3 可见，该体系的核心是安全管理，可将人工智能领域中的 Agent 技术融入到安全管理体系中。Agent 表示具有一定智能，在不确定的环境中根据自身能力、状态、资源、相关知识以及所处外部环境信息，通过规划、推理和决策实现问题求解，并进行相应的活动，自主地完成特定任务送达某一目标的实体（段鹏等，2003）。单个 Agent 的智能是有限的，通过适当的结构可以把 Agent 组织起来形成包含多 Agent 的系统，从而弥补单个 Agent 的不足，使得整个系统的能力超过单个的 Agent（齐跃斗，2006）。该框架通过各 Agent 之间自独立，自治地、主动地、实时地，通过通讯的方式进行协作，检测异常行为，从而构建一个基于安全管理的动态自适应网络安全模型。

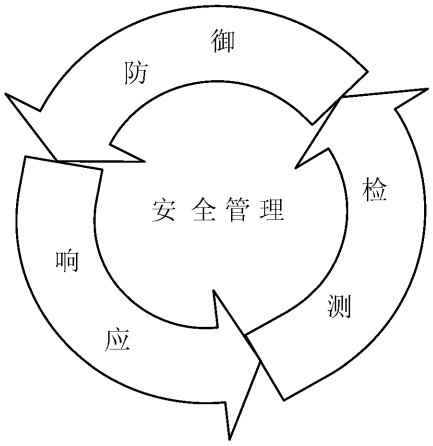

图 3 基于管理的网络安全体系

Fig. 3 Network security system based on management

4 结论与讨论

在对地震信息网存在的安全隐患做了初步调研后，笔者针对地震信息网的行业安全需求，提出了基于安全管理的动态自适应网络安全模型。该模型系统不但能够对已知攻击进行防御，而且能够对未知攻击进行检测。这样，就能够对传统的被动防御式网络安全技术（如防火墙等）提供改进措施，不断完善它们的入侵特征库以及时应对新的入侵行为，弥补其在安全防范领域的不足。这种主动防御的安全模式是信息时代发展的需要，是未来网络安全发展的趋势。

需要注意的是，信息网络安全管理与技术，对信息网络的安全具有同等重要的作用，因此，管理与技术协调发展才能有效保障地震信息网络的安全。

地震信息网这样一个庞大的网络系统，运行着许多关键业务，其安全管理任务是相当重要且艰巨的，并且由于网络安全问题的特殊性，网络安全是永恒的话题。网络安全问题可以在一定程度上解决但是不可能彻底解决。随着技术的进步以及管理手段的进一步跟进，网络安全完全可以以合理代价控制在可接受的范围内。

参考文献：

陈会忠 . 2007. 地震信息系统发展综述[J]. 地球物理学进展,22(4):1142 – 1146.

段鹏,谷雨,范菁,等 . 2003. 人工智能 Agent 技术与 Internet 信息服务的研究[J]. 云南民族学院学报(自然科学版),12(2):117 – 119.

李俊,秦嘉政 . 2009. 地震应急中的应用层多播技术网络视频会议系统[J]. 地震研究,32(3):316 – 321.

齐跃斗 . 2006. 基于 Agent 技术的 Web – Based Training 应用研究[J]. 微计算机信息,22(14):295 – 297.

王建国,栗连弟,崔晓峰,等 . 2009. 数字化地震前兆台网日常工作管理软件[J]. 地震研究,32(1):79 – 83.

阴朝民 . 2001. 防震减灾技术系统的建设与发展[J]. 地震地磁观测与研究,22(6):1 – 12.

赵晓飞 . 2008. 基于软硬件结合的动态网络安全体系[J]. 安阳师范学院学报,(5):54 – 56.

中国地震局监测预报司 . 2003. 地震信息网络[M]. 北京：地震出版社 .

The honeynet project. 2004. Know your enemy: Learning about security threats[M]. Boston: Addison Wesley Professionnl.

Mallela V. 2006. Sun Solaris10 系统 DTrace 的使用方法[J]. 程序员，(3):122 - 124.

Nakhimovsky G, Herrington M. 2006. Dtrace：应用程序崩溃时数据收集利器[J]. 程序员，(5):125 - 127.

Self-adaptable Network Security Model and Its Application to Earthquake-information Network

LIU Yun-hua[1], LIU Zhi[1], SHAN Xin-jian[1], LI Wei-dong[2]

(1. *Institute of Geology*, *CEA*, *Beijing* 100029, *China*)

(2. *China Earthquake Networks Center*, *Beijing* 100045, *China*)

Abstract

Based on a preliminary investigation into the potential hazard that the earthquake-information network may experience, we propose an adaptive network security model, along with a defense system containing three factors, namely regulations, technology and management, so that the network security can be under control at a reasonable cost.

Key words: earthquake-information network; security requirement; adaptation; management