气象业务信息化发展下的网络安全治理初探

周琰 蒋敏慧 曹磊 马强

随着信息化进程的不断发展，网络安全问题愈加突出。气象业务信息系统作为国家级的关键信息基础设施，在网络安全方面也面临着日益严峻的挑战。

1 现状与挑战

1.1 气象业务信息系统建设及安全现状

2016年随着全国综合气象信息共享平台（CIMISS系统）实现全国业务化，国家级业务单位内部数据资源与业务应用系统集约整合等工作的有序展开，为气象云建设夯实了基础。按照《气象信息化行动方案》部署，2017年将全面开展气象云建设，提升气象业务和政务信息化水平，气象业务、服务、科研和管理等信息化将迈上新台阶，实现“智慧气象”。此外，在初步建立的气象信息化标准框架下，已完成信息化基础设施资源池建设指南和公共云应用设计；完成气象信息化工程项目建议书，组织工程技术预研和试点建设；数值预报云初步建成，可实现数值预报产品全国范围内云上服务；众创平台试验启动，开展MICAPS和数值模式开源及众智开发；初步完成气象政务管理系统总体设计，业务管理信息系统初见成效。随着气象云和气象大数据建设的不断推进，气象部门已经进入了云和大数据时代。

为落实国家网络安全战略，保障气象业务空地一体的网络业务传输格局，主要完成了如下三方面的安全建设。一是建立了相对完善的边界安全防护体系和内部安全审计管理平台。在全国气象宽带网、互联网、外联网（国际通信、同城部委、电子政务）等主要的通信网络接入边界都部署了边界逻辑隔离设备和安全防护设施。在重要业务系统边缘和办公系统入出口都部署了入侵防御、安全审计和主机防护系统。初步构建了传统安全的纵深防御体系，实现了对气象业务系统的安全防护。二是基本完成了气象信息系统的等级保护合规建设。全国气象通信系统、全国气象资料检索服务系统、高性能计算系统、气象官方网站、突发预警平台等气象核心应用系统都完成了等级保护要求的备案、整改和测评工作。三是初步建立安全事件预警通报机制。根据公安部、国家互联网应急中心（CNCERT）和安全厂商等多种渠道发布的系统漏洞和安全威胁，再辅之以专业的攻击溯源安全设备的检测预警能力，能够及时通报相关漏洞和网络攻击事件。综上所述，在网络安全方面已经具备了应对常见网络攻击和预警处置的安全防御能力，并取得了一定的防护效果。

1.2 气象业务信息系统安全面临的挑战

虽然气象信息系统安全建设已经取得了一定的成绩，但是随着气象云和气象大数据建设的不断推进,网络攻击技术不断持续高速发展，气象业务信息系统安全仍然面临严峻的挑战。

1）攻击技术发展带来的挑战

攻击技术主要沿着两个方向不断发展，一个是攻击的隐蔽性，另一个是攻击速度。在隐蔽性方面，通过应用零日漏洞和高级逃逸技术，不断穿透现有的防御体系。在攻击速度方面，利用各大社区和社交平台共享漏洞信息和利用代码，在很短时间内发动攻击，形成以快打慢的攻击局面。

在前期进行的气象网络全面检测中，曾先后发现多个业务服务器被植入木马，并以该服务器为跳板对内网多台服务实施网络攻击，给业务系统的正常运行带来极大的安全风险，经过及时处理未造成影响。

2）新技术不断应用带来的挑战

随着业务的发展，特别是气象云和气象大数据建设的不断推进，新技术在气象业务信息系统中的应用越来越广泛。气象云基于虚拟化技术构建，从攻击者的角度，就在网络、主机、应用的基础上，又增加了虚拟化平台这个新的攻击平面，带来了虚拟机、hypervisor、快照、镜像等多个攻击点。气象大数据作为未来业务的核心支撑，其特点在于对数据一方面提出了共享的需求，另一方面又非常敏感，一旦被非法破坏将会造成严重的后果。云计算和大数据等新技术正处于高速发展中，对这些新技术的安全保护研究还处于一个相对滞后的状态。这就导致采用新技术的业务系统的安全风险比较高，易于被攻击者利用。

3）国家新法规要求带来的挑战

随着网络安全上升为国家战略，国家近期发布的多个法律法规文件都对网络安全提出了要求，如《中华人民共和国保守国家秘密法实施条例》《中华人民共和国反间谍法》《国家信息化发展战略纲要》《国家网络空间安全战略》《中华人民共和国网络安全法》等。在这些法规标准文件中，《中华人民共和国网络安全法》是专门用于规定网络安全工作的国家法律，也是气象行业信息安全建设必须遵循的工作规范。此外，信息安全等级保护相关标准规范修订版（以下简称等级保护2.0）也已经在全国信息安全标准化技术委员会网站上公开征求意见，这也标志着等级保护2.0的正式颁布实施已经提上日程。

4） 网络架构演进带来的挑战

SDN（软件定义网络）是公认的网络架构的演进方向。在SDN架构下，网络的控制层和数据层解耦合，流量调度也更加灵活。因此，必须采取全新的安全机制与之相匹配。安全界提出了SDS软件定义安全的全新安全模式，通过安全控制器与网络控制器联动的设计，实现网络和安全在软件定义模式下的统一。但如何将SDS从理论研究应用到生产实际，依然有许多具体工作需要进一步落实。

2 气象信息网络安全治理需求分析

2.1 业务系统运行保障需求

保障气象业务信息系统的安全运行，是气象信息网络安全治理的根本目的。经过多年的安全建设，气象信息网络安全治理工作已经形成了应对常见网络攻击的能力。因此，当前需要重点考虑的是业务系统运行过程中面临的新问题和新风险。主要包括检测和防御新型攻击、控制采用新技术业务系统的安全风险、快速处置网络安全事件等三方面的需求。

1）检测和防御新型攻击的需求

以高级持续性威胁（APT）为代表的新型攻击，利用零日漏洞和多阶段攻击技术绕过现有的以特征库匹配为主的检测体系，达到了较高的攻击成功率，对气象业务信息系统的安全运行形成了较大的威胁。

2）控制采用新技术业务系统的安全风险的需求

云计算、大数据等新技术能够提高信息资产的使用效率，提高气象数据分析的广度和深度，是增强气象业务信息系统运行能力的基础技术，已经在现有系统中开始应用。然而，从安全的角度，新技术的应用也带来了新的风险，如基于虚拟化的云计算平台也给攻击者增加了新的攻击平面，一旦hypervisor层被黑客利用，运行于其上的VM都可能被完全控制。如果气象大数据在共享过程中被非法篡改，就可能导致基于此产生的天气预报、气候预测和领导决策出现偏差，导致不可估量的后果，造成严重的社会影响。

3）快速处置网络安全事件的需求

随着新技术的应用和攻防技术的发展，气象业务信息系统面临的安全风险不断加大，出现安全事件的概率不断增高。因此，必须建立一套较为完善的网络安全事件处置机制，在安全事件发生之初就加以控制，将危害控制在最小的范围内。

2.2 合规性需求

在合规性需求中，主要考虑网络安全法和等级保护2.0两方面的合规需求。

1）网络安全法

网络安全法于2016年11月7日发布，2017年6月1日起正式实施。它是我国第一部专用于网络安全方向的国家法律，在气象信息网络安全治理方面具备非常重要的指导意义。网络安全法的第三章专门对网络运行安全提出了具体规定。其中对关键信息基础设施的安全运营专门列出了一节的内容，规定了关键信息基础设施运营者应当履行的安全保护义务以及国家对关键信息基础设施安全保护采取的措施等相关内容。气象业务信息系统总体上属于国家关键信息基础设施的范畴，必须依法进行安全保护。这也就要求气象信息网络安全治理必须满足网络安全法的相关要求。

2）等级保护2.0

信息安全等级保护的主要工作自2007年开展以来，已历经了十年且一直在持续推进。从在国家安全标准委员会网站上公开征求意见的等级保护2.0标准规范分析，等级保护从1.0升级到2.0，整体架构和要求内容上都发生了较大的变化。在架构方面，从单一的基本要求，转变为1+N的模式，即一个安全通用要求加不同应用方向的安全扩展要求的模式。在要求内容方面，也对新型攻击的检测和防范提出了具体要求。气象业务信息系统的安全保护一直以等级保护为基本依据，今后也需要继续依托新修订后的2.0标准加强建设，形成气象业务信息的基线安全能力。

3 当前网络安全体系发展情况

1）威胁情报

威胁情报就是收集、评估和应用关于安全威胁、攻击利用、恶意软件、漏洞和漏洞指标的数据集合。从安全体系看，威胁情报弥补了当前静态安全防护体系中被动反应、延后反应的不足，形成了在安全事件发生前就可进行预判的能力。

2）安全大数据分析

基于大数据对安全事件进行分析，是安全界公认的发展方向。大数据能够通过对海量历史数据进行安全分析建模，分析其中可能存在的多阶段攻击、未知攻击，加强对有组织攻击的检测和防御能力。

3）云地结合防护

安全即服务（SECaaS）是利用云端的安全服务能力解决基于设备进行防护存在的不足。威胁情报即可看成一种云服务，此外常见的云服务还包括：DDoS云清洗、云扫描服务、网站云监控服务等，这些云安全服务和本地安全防护体系相结合，可以极大增强安全防御效果，提升安全防护水平。

4 气象信息网络安全治理架构设计

气象信息网络安全治理的基本思路是在已有安全防护体系的基础上，以网络安全法和信息安全等级保护2.0为指导，以保障气象业务信息系统的安全运行为目标，综合内外部安全资源，打造预警、防护、检测、响应闭环的气象信息网络安全治理体系。总体架构如图1所示。

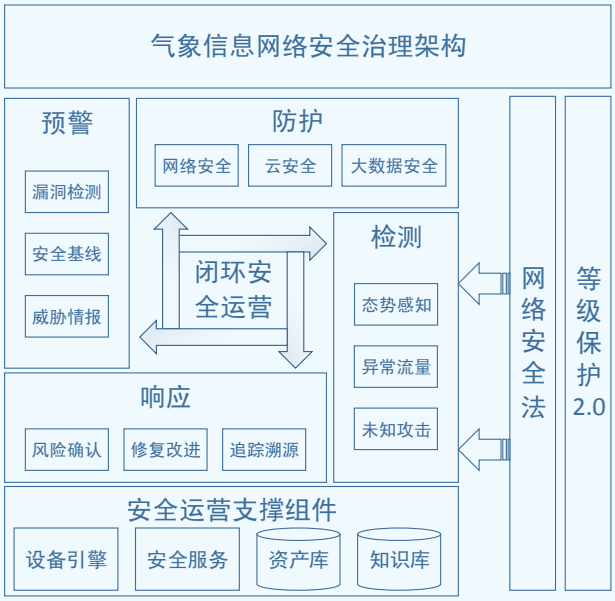

图1 气象信息网络安全治理架构

4.1 安全预警能力

安全预警能力主要针对气象业务信息系统自身脆弱性的监测和防护，主要考虑全面性和时效性两个方面。全面性方面，既要考虑气象业务信息系统组件自身固有的脆弱性，如操作系统、数据库、中间件的漏洞等；也要考虑自研系统由于设计不当导致的特有缺陷，如流程设计导致的数据泄露等；还要考虑系统组件自身安全功能配置不当导致的人为问题，如弱口令、策略配置不当等。针对全面性方面的安全预警能力，主要体现在长期监控内网资产存在的安全漏洞，并根据安全行业的最佳实践不断调整气象业务信息系统的安全基线，同时引入外部安全专家对系统开发过程中产生的安全问题进行检测、发现和评估，对于重大漏洞及时修复。在时效性方面主要针对当前网络攻击速度不断加快的现实状况，结合威胁情报对发现的安全漏洞进行评估，对于在黑客社区活跃度高、出现漏洞利用代码或出现相关安全事件的漏洞，要提升其优先级并快速修补。

4.2 安全防护能力

安全防护能力主要在已有等级保护1.0纵深防护体系的基础上，参照网络安全法和等级保护2.0的相关要求进行建设，重点做好云计算和大数据等新技术方面的安全防护。一是按照相关合规要求，建设和提升无线安全防护、垃圾邮件防护、个人信息防护、边界信息内容过滤等方面的防护能力，二是建设气象云安全防护资源池，形成泛在接入、弹性可伸缩、安全配置的安全防护能力，三是建设气象大数据防护机制，形成覆盖数据采集、传输、存储、使用和开放等大数据全生命周期的防护能力。

4.3 安全检测能力

安全检测能力主要以现有重要资产监控体系和网络入侵检测能力为基础，重点做好两个方面的能力提升。一是进一步丰富网络攻击检测方法，增加基于流量模型的深度流检测技术和基于行为模型的未知攻击检测技术，形成多维度的检测方法体系；二是增强对检测结果的分析，实现深度流检测和深度包检测结合分析，已知攻击和未知攻击结合分析，大数据安全分析和安全可视化相结合的多种复合分析和展示能力。

4.4 安全响应能力

安全响应能力主要以现有的应急预案体系和应急响应机制为基础，进一步增加基于互联网外部的安全专家团队的协同响应模式，实现安全事件和安全风险的快速识别和确认，安全应急措施的快速拟制和应用，安全修复结果的快速确认和验证，以及网络攻击事件过程的全面取证和溯源，总体上达到小时级的安全响应能力。

深入阅读

吴世忠, 李斌, 张晓菲, 等, 2014. 信息安全技术. 北京: 机械工业出版社.
张格苗. 全国气象信息化工作稳步推进 78个业务应用系统对接CIMISS. 中国气象报, 2016年8月12日.

（作者单位：国家气象信息中心）