国家电子政务外网标准

GW0204—2014

国家电子政务外网安全管理系统
技术要求与接口规范

Technical Requirements and Interface Specification for Security Operation

Center of National E-Government Network

2014－11－13 发布　　2015－1－1 实施

国家电子政务外网管理中心

目　　次

前　言

为进一步规范国家电子政务外网设计部署安全管理系统的技术要求，满足各级政务外网建设安全监测技术平台的实际需求，结合政务外网建设实践及安全管理系统部署经验，编制本标准。

本标准由国家电子政务外网管理中心提出并归口。

本标准起草单位：国家电子政务外网管理中心、北京启明星辰信息安全技术有限公司、网神信息技术（北京）股份有限公司、东软集团股份有限公司、北京天融信科技股份有限公司、深圳华为技术有限公司、湖南蚁坊软件有限公司。

本标准主要起草人：吕品、马英、罗海宁、周民、邵国安、刘震、张锐卿、丁凌风、范永、苑向兵、李经通、孙燕辉、徐浩、陈亮、范仲辉、倪德东、郑玮、吴昊。

引　言

为指导中央、省（自治区、直辖市）、地（市）、县各级政务外网安全管理系统的方案设计、产品选型和系统级联，特编写本标准。本标准对政务外网安全管理系统的技术架构、功能、性能、部署方式、自身安全性、接口规范提出具体要求。

国家电子政务外网安全管理系统技术要求与接口规范

1 范围

本标准用于规范各级政务外网安全管理系统的功能、性能、安全性、部署方式、接口等技术要求，可作为指导各级政务外网设计、选型和建设安全管理系统的技术依据。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注明日期的引用文件，其随后所有的修改（不包括勘误的内容）或修订版均不适用于本标准。凡是不注明日期的引用文件，其最新版本适用于本标准。

GB/T 5271.8 信息技术词汇第 8 部分：安全

GB/T 22239 信息安全技术 信息系统安全等级保护基本要求

GB/T 20984 信息安全技术 信息安全风险评估规范

GB/Z 20985 信息技术 安全技术 信息安全事件管理指南

GB/T 18030 信息技术 中文编码字符集

GB/T 28458 信息安全技术 安全漏洞表示与描述规范

GB/T 2260 中华人民共和国行政区划代码

3 术语和定义

3.1

安全管理系统 Security Operation Center，SOC

采用多种技术手段，收集和整合各类网络设备、安全设备、操作系统等安全事件，并运用关联分析技术、智能推理技术和风险管理技术，实现对安全事件信息的深度分析和识别，能快速做出报警响应，实现对安全事件进行统一监控分析和预警处理。

3.2

网络管理系统 Network Management System，NMS

提供拓扑管理、设备配置、故障告警、性能监测和报表管理功能，实现对网络运行的集中统一管理。

3.3

脆弱性 Vulnerability

信息技术、信息产品、信息系统在需求、设计、实现、配置、运行等过程中，有意或无意产生的缺陷，这些缺陷以不同形式存在于信息系统的各个层次和环节之中，一旦被恶意主体所利用，就会对信息系统的安全造成损害，从而影响构建于信息系统之上正常服务的运行，危害信息系统及信息的安全。脆弱性又称为安全漏洞。

3.4

安全威胁 Security Threat

某个人、物、事件或概念对某一资源的保密性、完整性、可用性、真实性或可控性所造成的危害。

3.5

信息安全事态 Information Security Event

系统、服务或网络的一种可识别的状态的发生，它可能是对信息安全策略的违反或防护措施的失效，或是和安全关联的一个先前未知的状态。

3.6

信息安全事件 Information Security Incident

采集的单个或一系列的安全事态，包括各类日志、操作和其他系统或设备报送的报警信息。

3.7

告警 Alarm

针对收集到的各种安全事件进行综合关联分析后形成的报警事件。

3.8

Syslog 协议

TCP/IP 网络中用于传输系统日志的标准，设备和系统在记录和转发日志时应遵循该标准。

3.9

Web Service

基于网络的、分布式的模块化组件，它执行特定的任务，遵守具体的技术规范，其它应用通过使用相应的规范，可以与它进行互操作。

3.10

BUGTRAQ

一个公告计算机安全问题的列表，包括安全漏洞相关公告和利用这些漏洞的方法，以及如何修复它们。

4 缩略语

SOA 面向服务的体系结构 （Service-Oriented Architecture）
JDBC Java数据库连接 （Java Data Base Connectivity）
ODBC 开放数据库互连 （Open Database Connectivity）
FTP 文件传输协议 （File Transfer Protocol）
CVE 公共漏洞和暴露 （Common Vulnerabilities & Exposures）
WSDL 网络服务描述语言 （Web Service Description Language）

5 建设原则与目标

5.1 建设原则

安全管理系统按照以下原则进行建设：

a) 按照政务外网安全监测体系的统一规划，中央、省、地市政务外网应分别建成安全管理系统，并形成中央、省、地市三级系统级联；县级政务外网可根据自身情况建设安全管理系统，并与上级系统级联；
b) 各级安全管理系统应部署于本级政务外网的公用网络区，互联网区与专用网络区的安全相关信息可通过带外管理网、采集代理方式发送到安全管理系统；
c) 对于已建成和在建的安全管理系统，分步实施与中央级节点知识库共享、接口改造、系统级联等，并纳入到政务外网安全监测体系中。

5.2 建设目标

安全管理系统建设应实现如下目标：

a) 可快速集成不同厂商的各类IT资产，实现各类设备日志信息的实时采集与统一监测，并具备较强的扩展能力；
b) 提供针对安全日志的海量信息数据存储与检索能力，实现各类原始日志与各类分析数据的安全存储与快速检索；
c) 具备关联分析、风险评估、趋势分析等综合分析能力，能从被攻击的角度关联资产的脆弱性和重要程度，从攻击的角度关联不同安全设备采集到的安全事件，形成动态的安全风险评估及事件管理能力；
d) 提供全面完整、可定制的集中监测与展示工作界面与报表，可按照用户要求，提供多种形式的直观事件展现方式，针对不同的角色可灵活定制数据展现视图；
e) 为各类安全管理人员提供日常监测、事件告警与预警、应急处理与响应的工作平台；
f) 提供决策辅助与态势分析功能，实现对安全态势的掌控；通过对各类安全数据的加工、存储、深层分析为安全决策提供依据；
g) 支持多级系统的级联管理和分级部署；
h) 具备应对业务流程的变更和新业务流程扩展的能力；
i) 实现外部系统接口标准化。

6 系统总体架构

6.1 总体功能架构

安全管理系统监测全网重要 IT 资源的运行状态，对安全事件、脆弱性、配置、可用性与安全相关的数据进行统一采集、集中分析，并进行宏观可视化展现，发现事件或安全风险时可实时触发告警。安全管理系统提供标准外部通信与数据接口，与上下级平台和第三方系统实现连接。安全管理系统的整体功能框架如图 1 所示：

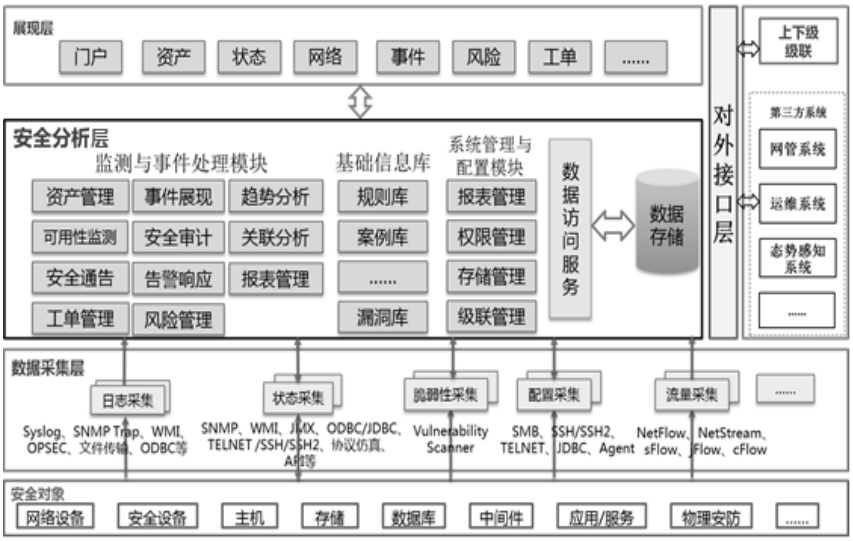

图 1 安全管理系统整体功能框架图

6.1.1 数据采集层

数据采集层采集安全管理系统所关注监测对象的运行状态信息、安全事件信息、脆弱性信息、安全配置信息和流量信息，并将所采集的安全事件信息转化为安全管理系统内部统一的数据格式。

6.1.2 安全分析层

通过综合分析方法对采集数据进行关联分析以识别判断安全事件或事态，由监测与事件处理模块、系统管理与配置模块、基础信息库等组成。监测与事件处理模块主要包括资产管理、可用性监测、关联分析、事件展现、趋势分析、告警响应、风险管理、安全审计、安全通告、工单管理；系统管理与配置模块主要包括报表管理、权限管理、存储管理、级联管理；基础信息库主要包括规则库、案例库、漏洞库。

6.1.3 展现层

通过可视化的方式将监测对象的运行状态、安全事件、安全风险展现给用户。

6.1.4 对外接口层

在安全管理系统中应构建标准化接口服务层，实现与上下级安全监测系统、外部系统接口连接。安全管理系统对外接口应具有良好的兼容性，可以方便地与第三方系统进行连接，支持 Syslog 事件转发、SNMP Trap 事件转发、Web Service 接口调用等常用标准接口。在展现层上，安全管理系统应与第三方 B/S 架构的系统实现 Portal 统一展现。

6.2 总体技术要求

6.2.1 系统技术架构

系统技术架构应采用面向服务的体系架构（SOA），具备跨平台、可伸缩和高可靠的特性。系统采用 B/S 访问方式。

6.2.2 系统运行环境

支持主流操作系统部署，支持主流网络浏览器。

6.2.3 部署方式

支持灵活的部署方式，既支持集中式部署，也可进行分布式部署；既支持单级部署，也支持多级级联式部署。

6.2.4 数据库

支持主流数据库或国产数据库。

6.2.5 综合展现

支持图形化的展现方式，采用仪表板、统计图展现数据统计分析的结果，使用趋势分析图展现指定时间段内监测数据的变化趋势；支持动态事件分析，能够实时展现当前的事件变化；支持使用数据钻取方式进行事件追溯。

7 系统功能要求

7.1 资产管理

实现对网络中 IT 资产的管理，按照安全域的方式管理资源，提供便捷的资产添加、修改、删除、查询与统计功能，便于安全管理和系统管理人员查找所需设备资产的信息。资产记录中应包括资产名称、IP 地址、类型、责任人、业务价值，以及其机密性、完整性、可用性等资产属性，可根据需要添加资产属性。

支持将自动发现到的资产自动添加到资产库中，并可对这些资产记录信息进行补充修改。

支持手工录入资产记录，也可以基于系统提供的资产模板（XLS、CSV、XML 格式）进行资产批量导入。

7.2 可用性监测

可用性监测主要通过监测各类安全设备，实时了解设备的可用性状态，出现异常时可根据预先设定的阈值产生告警。除安全设备以外的其他设备或系统的可用性监测可作为安全管理系统中的可选模块，各建设单位可以根据本单位的实际情况自主选择。

7.2.1 安全设备监测

安全管理系统能够对网络中的安全设备进行可用性监测，应对设备的通断及时告警。同时安全管理系统还应具备安全设备的健康度监测。通过对关键运行指标，包括 CPU、内存、磁盘的运行状态数据进行阈值管控，实时产生相关报警，执行预定义的响应动作。

7.2.2 系统运行环境监测

安全管理系统应能对网络中的服务器、数据库、中间件、存储、通用服务、网络设备等对象的可用性进行监测，同时安全管理系统还应具备上述对象的健康度监测，可对关键指标设置阈值，触发阈值时可产生告警，执行预定义的响应动作。

7.2.3 业务系统监测

安全管理系统除能按设备和系统类型对业务系统相关对象的可用性进行监测外，还应提供以业务系统为监测对象的监测功能，可以集中监测业务系统的 URL 响应时间等关键可用性指标，分析当前业务系统的可用性，当业务系统异常时，通过业务监测视图可以迅速定位故障原因。

7.3 事件管理

对所有 IT 资源产生的安全事件信息进行统一的实时监控和关联分析，对来自外部的入侵和内部的违规和误操作行为进行监控、审计分析、调查取证，并出具报告，实现 IT 资源的合规性管理。信息安全事件管理包括事件的采集、标准化、集中存储、实时展现、关联分析和应急响应。

7.3.1 事件采集

安全管理系统可对信息系统中的网络设备、安全设备、主机系统、应用系统及其他系统进行日志采集。

为避免采集日志过程中对业务系统造成影响，需制定合理的日志采集及传输策略。

为保证系统可靠工作，系统应可以监控各采集点的日志传输状态，当有采集点无法正常发送日志信息时，系统可以自动进行告警，通知管理员进行处理。

7.3.2 事件标准化

安全管理系统对系统采集的日志信息进行事件标准化处理，将异构的日志变成系统可识别的统一的日志，屏蔽了不同厂商以及不同类型的产品之间的日志差异。

7.3.3 事件展现

安全管理系统应提供多种形式的事件展现方式，包括列表、图表等方式。

安全管理系统应提供多种条件的过滤查询，实现不同场景的事件查看。提供当前事件和历史事件的查询功能，提供事件导出功能。

7.3.4 事件集中存储

安全管理系统应具备海量的数据存储能力，应有合理的数据存储管理及备份恢复策略，可支持磁盘阵列柜、存储区域网络（Storage Area Network， SAN）和网络储存设备（Network Attached Storage，NAS）等存储方式。

7.4 关联分析

安全管理系统应提供关联分析功能，将来自不同事件源的事件进行分析，能从海量事件中过滤出有逻辑关系的事件序列，并根据告警策略、资产的业务价值和资产的脆弱性，形成相应的告警事件。

安全管理系统应提供关联分析规则，针对主机扫描、端口扫描、DDOS 攻击、蠕虫、口令猜测、跳板攻击等攻击行为提供相应的关联分析规则。安全管理系统应内置关联分析规则库，提供界面友好完备的规则编辑器，使事件分析人员可方便地编写关联分析规则。

安全管理系统可依据最佳实践原则自动判断所收集的各类事件的重要性，并形成相应的告警。针对关联分析产生的安全事件可追溯其关联事件。

7.5 统计分析

指针对一段时间内的历史信息进行统计和呈现。可从不同维度对历史信息进行统计，包括信息发生数量、信息排行、疑似攻击和违规事件、不同状态的统计分布；分析人员也可自定义策略进行统计分析。

7.6 趋势分析

对指定时间段内满足指定条件的事件数量进行趋势分析，生成趋势分析统计图，分析人员可以从宏观上掌握指定时间范围内某类事件的趋势。

7.7 告警响应

当安全管理系统监测到可用性异常或安全事件时，可以触发预先设定的告警阈值或触发事件分析规则，执行预定义的告警响应动作。告警响应动作应涵盖常见的响应方式，包括电子邮件告警、手机短信告警、创建工单、通过 Syslog 或 SNMP Trap 向第三方系统转发告警事件。

安全管理系统应提供告警过滤功能，在指定时间范围内，同一事件只进行一次告警；或在工单处理期间同一事件只进行一次告警，直到工单处理完毕，重新打开告警。

7.8 风险管理

安全管理系统需实现被保护资产的风险计算功能，展现当前被保护资产的风险值和风险等级，并进一步计算安全域的风险。对于单个资产的风险计算，需要依据资产价值、资产当前的脆弱性及资产面临的安全威胁，资产的风险计算结果应比较准确地体现上述三方面的要素对资产安全风险的影响。在计算得到安全域中资产的安全风险后，可据此计算安全域的风险。

安全管理系统应能以图形化的方式展现当前资产和安全域的风险级别、当前风险的排名统计。

风险管理依据资产管理（需评估资产价值）、资产的脆弱性及资产面临的威胁（针对资产的安全事件）进行安全风险计算。

7.8.1 资产价值评估

资产价值评价的依据主要是资产对业务系统的重要性，需要在创建资产记录时由管理员根据其在业

务系统中的实际作用来进行评估，并量化为 1 至 5 的不同等级，5 为最高，1 为最低。

7.8.2 脆弱性管理

创建资产记录并评估其价值后，需要创建并维护资产的脆弱性列表。资产的脆弱性可由安全服务人员评估后手工创建，也可根据漏洞扫描系统的扫描结果导入生成。脆弱性赋值由脆弱性的严重程度确定。

安全管理系统应支持国内主流的漏洞扫描系统的扫描结果导入。支持多次导入漏洞扫描系统的扫描结果，支持漏洞列表的合并及更新。

7.8.3 威胁管理

资产面临的威胁可根据针对该资产的安全事件来生成，通过相应的安全分析规则，将满足设定条件的事件视为对目标资产的安全威胁，创建相应的威胁记录，威胁的赋值由威胁发生的频率来确定。

7.8.4 安全风险计算

在获得上述三个相关要素的值后，安全管理系统可以计算目标资产的安全风险，进而可计算所在安全域或所属业务信息系统的安全风险。安全风险的计算周期可通过配置进行设定。计算方法建议符合国家标准《信息安全技术信息安全风险评估规范》（GB/T 20984-2007）要求，可采用矩阵法或相乘法，在使用时应予以说明。

7.9 安全审计

安全管理系统可以根据合规的要求，采集所需的数据，根据预置的或定制的策略及规则模版，生成相应的审计结果数据，对危害信息系统运行及不合规的行为进行报告。分析人员可自行设定查询条件进行人工审计，获得所需的审计查询结果，并可将结果以文件形式导出。

7.10 安全通告

安全管理系统提供安全通告功能，可以创建或导入安全风险通告，通告中一般包括通告内容、描述信息、CVE、BUGTRAQ 编号、影响的操作系统及其他信息。安全管理系统可以根据通告提示受安全风险影响的操作系统，提供受影响的被保护资产列表。安全管理人员可以据此采取相应的保护措施。

7.11 工单管理

安全管理系统提供工单管理的功能，支持创建工单的流转流程。支持手工创建工单，也可在告警响应动作中创建工单，将工单指派给指定的处理人。

7.12 报表管理

安全管理系统应内置常用统计报表的报表模版，并提供界面友好的报表编辑器以使用户可以自定义报表。生成的报表可以多种格式导出，包括 PDF、HTML、CSV、XLS。应支持报表调度任务，可以在指定时间内一次或周期性执行报表任务。还应支持报表投递功能，可以将生成的报表以电子邮件方式直接发送给指定接收人。

7.13 权限管理

安全管理系统在权限管理上应做到系统管理员、安全管理员和安全审计员三权分立。权限的分配采取基于角色的访问控制机制，根据需要创建角色和用户，为角色赋予权限，为用户赋予所需的角色。

7.14 存储管理

安全管理系统应能够存储海量数据，提供自动的数据备份归档功能，可以根据预设的策略定时自动归档数据。对于已归档的数据，可以根据需要重新导入系统以进行查询和统计分析。

7.15 级联管理

安全管理系统提供松耦合的级联功能，实现跨省事件协同处理。上级系统可以监测下级系统的运行状态；下级系统的安全风险、安全告警和安全统计报表可根据需要定期上报给上级系统；下级系统可按要求将满足条件的事件转发给上级系统；中央级节点建立知识库，下级节点可以访问并可上传案例。

7.16 知识库管理

安全管理系统提供知识库管理功能，知识库类别包括但不限于规则库、案例库、预案库、策略库、漏洞库。用户可以根据需要扩展知识库的类别，知识库的内容可以导入、导出，支持对知识库的全文检索和按关键字检索。

中央级节点应创建共享知识库，各下级节点通过安全管理系统可访问中央级节点的知识库，并可上传案例。

7.17 综合展现

安全管理系统提供多种可视化的数据展现方式，包括事件列表、事件统计图、趋势分析图、事件GIS 图、可用性统计图、业务系统健康统计图、资产及业务系统风险统计图。

针对不同的角色，可根据其工作职责和关注重点，提供不同的数据展现视图，视图的内容可灵活定制。

支持以方便灵活的方式与其它 B/S 架构系统的页面整合。

7.18 时间同步

安全管理系统支持时间同步功能，要求被采集对象使用相同的 NTP 时间源。

7.19 数据采集与预处理

安全管理系统支持主动和被动两种形式的数据采集方式，支持常见的标准协议，包括 Syslog、SNMP、SNMP Trap、Log File、Opsec、ODBC/JDBC 等协议。

支持对采集的数据进行过滤、归并、将数据转换为内部统一格式。

原始数据应单独保存在一个独立的数据库或便于检索的文件中，其保存期应满足合规要求。如果原始数据不能独立存储，而是与转换为内部统一格式后的数据一起保存在系统的数据库中，应满足其内容及格式均未被修改，其保存期限应满足合规要求。

系统能够对历史数据进行追溯。数据的存储需要有序、归类并适当建立索引，在查询时能够及时响应。

7.20 系统互联

安全管理系统在管理方式上应能够依据管理制度的需求实现分级管理，并可根据级联管理的需求提供上下级级联的指令和数据的传输。同时，安全管理系统应有良好的接口架构设计，对外实现对其他安全子系统的接入以及与第三方管理系统的互联和互操作，并提供二次开发接口，可通过接口开发扩展系统功能。

7.21 扩展性

安全管理系统应使用模块化设计，可根据需要进行功能扩展。

支持包括 Syslog、SNMP Trap、Web Service 等多种主流接口标准，可方便地实现对各类设备的采集以及与第三方系统的互联。

对新设备、新系统的支持应通过编写、加载配置文件的方式实现，而不需要对系统的代码进行修改。

7.22 访问控制

安全管理系统支持系统管理员、安全管理员和安全审计员三类角色，在权限上做到三权分立。系统中不设置超级管理员角色。

7.23 系统升级

系统软件版本升级时，应实现平滑升级，升级不应对原系统中已有数据造成影响。对于规则库、案例库及其他知识库内容，可通过提供离线升级包的方式实现增量式升级。

8 系统性能要求

8.1 稳定性

稳定性指标要求：

a) 支持系统主要组件7*24小时运行；
b) 系统年正常运行时间不低于99.9%；
c) 对被采集对象的内存资源占用率不超过5%，对网络带宽占用率不超过10%。

8.2 数据处理性能

8.2.1 中央/省级安全管理系统性能要求

a) 原始数据并发采集能力不低于6000条/s；
b) 事件分析处理能力不低于5000条/s；
c) 事件告警延迟不超过5min；
d) 查询1000万条数据时间小于10s；
e) 查询1亿条数据时间小于30s。

8.2.2 地市/县级安全管理系统性能要求

a) 原始数据并发采集能力不低于4000条/s；
b) 事件分析处理能力不低于2000条/s；
c) 事件告警延迟不超过5min；
d) 查询1000万条数据时间小于20s；
e) 查询1亿条数据时间小于60s。

8.3 数据存储要求

安全管理系统在数据存储方面应满足以下要求：

a) 数据的保存期限不少于 6 个月；
b) 系统数据可保存在安全管理系统所在服务器的硬盘中，也可以保存在专用的存储设备中。

9 自身安全性

9.1 等级保护合规性要求

依据信息安全等级保护的相关制度和标准要求，确定安全管理系统的安全保护等级；原则上地市级以上系统安全保护等级不低于第三级，县级系统安全保护等级不低于第二级。

9.2 系统安全要求

在遵循等级保护合规性要求的基础上，安全管理系统应重点满足以下安全要求：

a) 网络通信应采用加密协议；
b) 重要数据应加密存储；
c) 系统应提供对其自身运行状态的监测，并可产生告警；
d) 对系统的操作应记录日志，日志不可删除，系统自身的操作日志查看权限仅授予审计员；
e) 提供系统配置信息和数据的备份功能，系统崩溃时可通过已备份的配置信息和数据快速恢复系统。

10 安全管理系统接口

10.1 总体框架

安全管理系统的接口主要有三部分组成：数据采集接口、级联接口和外部接口，总体框架如图 2 所示：

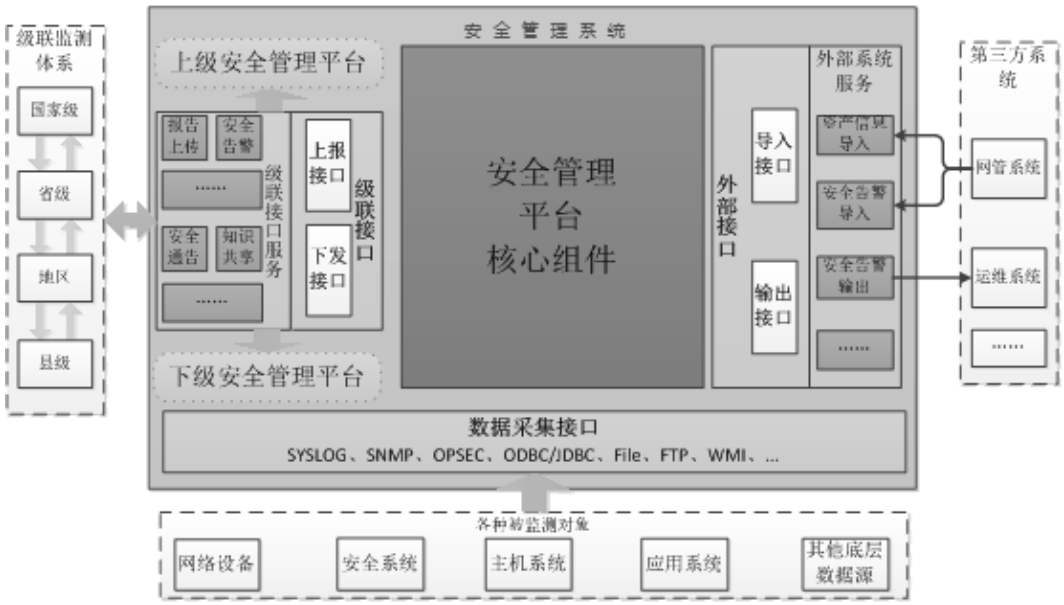

图 2 安全管理系统接口总体框架图

a) 数据采集接口：是安全管理系统从各种监测对象中采集日志数据、脆弱性数据、配置数据和状态数据的接口；

b) 级联接口：是处于不同管理层次上的上下级之间进行管理信息和安全运行数据交互的接口。建立级联关系的安全管理系统之间，应采用基于可靠的身份认证手段实现可靠的访问控制。

c) 外部接口：安全管理系统通过各种外部接口与其他应用系统（日志审计系统、数据网络管理系统、4A 系统）之间实现集成和数据交互。本标准着重说明安全管理系统与外部系统接口的工作方式，以及由安全管理系统提供接口的方式和数据规范。

10.2 数据采集接口

数据采集接口应实现安全管理系统从安全对象采集日志数据、脆弱性数据、配置数据和状态数据信息。

10.2.1 数据采集方式要求

应支持（但不限于）通过下述手段实现数据的主动或被动采集。

a) SNMP Trap

应启动 SNMP Service 服务，使用统一的团体串在默认或自定义端口上监听，以获取安全设备发来的 SNMP Trap 信息。

b) SYSLOG

应启动 SYSLOG 服务，使用默认或自定义端口监听，以获取安全设备发来的 SYSLOG 信息。

c) 文件

应具备网络文件、本地文件的定期或触发提取功能，获取其中的日志信息。

d) 数据库

应具备网络数据库、本地数据库的定期或触发提取功能，获取其中的日志信息。

e) 代理

对于特殊的、缺乏共性的信息存储方式，应支持通过编写代理程序方式获取其中的日志信息，代理程序应支持与目标数据部署在一起，也支持远程部署。

10.2.2 数据采集内容要求

a) 日志数据采集

应采集政务外网中的网络设备、安全设备、服务器设备所产生的所有日志信息。

b) 脆弱性数据采集

应采集政务外网中的网络设备、安全设备、操作系统、应用系统的脆弱性、补丁信息。安全管理系统可直接采集脆弱性数据，也可支持将其他相关设备的脆弱性数据导入到安全管理系统。

c) 配置数据采集

应采集政务外网中的网络设备、安全设备、服务器设备的账号安全策略、口令安全策略、授权安全策略和日志安全策略信息。安全管理系统可直接采集配置数据，也可支持第三方的配置数据导入。

d) 状态（性能）数据采集

应采集政务外网中的网络设备、安全设备、服务器设备的运行状态、性能相关数据。

10.3 系统级联接口

10.3.1 接口协议

系统级联接口按 Web Service 标准对外提供服务，通讯过程中请求和响应的数据采用标准 XML 格式来封装。对于开放的接口函数，厂商需发布相应的 WSDL 文档，用于描述 Web Service 的接口信息。

系统级联接口函数分为两类。一类是同步调用函数，即函数的返回值就是结果；另一类是异步调用函数，返回结果通过回调函数发送至调用方。异步类函数的返回值只表示“是/否接受命令”，调用方应提供满足标准的回调函数。

10.3.2 接口格式定义

接口格式定义包括函数名称、参数列表及返回值类型，参与交互数据的编码应符合 GB/T 18030-2005 标准。参数与返回值的具体 XML 格式由接口提供者根据具体业务的实际情况制定，应层次简单、结构清晰，接口提供者需提供相应的 WSDL 文档及接口的详细说明文档。

函数基本格式如下：

public String methodName(String xml);

说明：

a) methodName 为函数名，由接口提供者根据具体业务确定；

b) XML 为调用参数，应采用 XML 标准描述；

c) 返回结果为 XML 标准格式数据。

10.3.3 系统级联认证接口

为保证各级安全管理系统之间的通讯安全，系统之间在进行通讯前应进行有效的认证与授权。

系统级联认证接口主要包括系统级联注册接口和系统级联注销接口。系统级联注册接口完成下级系统至上级系统的注册功能，保证上下级系统之间通信的安全性。系统级联注销接口用于上下级系统之间的认证注销，当上下级系统出现变更或废止时，由上级系统进行系统间级联的注销。

系统级联注册接口规范见附件 A.1，系统级联注销接口规范见附件 A.2。

10.3.4 系统运行状态上报接口

上级安全管理系统需要对下级系统的上报接口实施周期检测，及时发现接口异常，减少上报数据的丢失。

下级安全管理系统周期性上报自己状态的心跳消息，上级系统根据是否能周期收到下级状态的心跳消息，来判断下级系统上报是否正常。

上报接口状态分为：

1——正常：上级系统收到下级系统的上报消息后，将下级的上报接口判断为正常；

0——离线：当上级系统在一个上报周期内未收到上报信息，则判断下级系统的上报接口离线，同时产生该下级安全管理系统上报接口离线告警。

上报频率为 10 分钟一次。

系统运行状态上报接口规范见附件 A.3。

10.3.5 风险上报接口

下级安全管理系统需要向上级系统上报本级系统的安全域的风险值和风险等级。上报频率至少为10分钟一次。

风险的上报由上级安全管理系统进行请求。下级安全管理系统按照请求的内容进行风险的实时上报。

风险上报的内容包括：系统所属行政区编码，安全域名称，风险值，风险等级。

风险上报接口规范见附件A.4。

10.3.6 告警上报接口

下级安全管理系统将本系统发现的告警信息通过告警上报接口向上级安全管理系统进行上报。

告警的上报由上级安全管理系统进行订阅，订阅信息中包含是否上报、上报的时间范围和级别信息。下级安全管理系统按照请求的内容进行告警的实时上报或停止上报。

本级安全管理系统将本级发生的告警进行实时上报，传输采用面向连接的方式。相同的告警信息仅发送一次。若本级安全管理系统的告警清除，则向上级发送该告警消除的消息，上级安全管理系统进行相应的处置。

告警上报的内容应包括：告警的 ID、系统所属行政区编码、告警名称、告警内容描述、告警的级别、告警发生的时间、告警涉及的IP地址、告警清除标志和预留字段信息。

告警上报接口规范见附件A.5。

10.3.7 案例上报接口

下级安全管理系统应将本系统发生的典型案例进行上报，以便上级系统对各种典型案例进行汇总。

下级安全管理系统从本系统数据库中将本系统发生的典型案例取出，调用案例上报接口，将本系统发生的案例上报给上级系统，上级系统获取到案例后可根据知识库的类别（规则库、案例库、预案库、策略库、漏洞库）对案例进行分类汇总并存储在数据库中，以便下级系统查询并为处置类似事件提供技术支撑。

案例上报接口仅为下级系统使用，接口要求的相关字段需按照字段类型、是否必填信息传递给上级系统，接口参数为XML格式。

接口返回值为XML格式，应说明调用该接口返回成功或失败的状态，返回值为失败时应给出失败原因提示。

案例上报接口规范见附件A.6。

10.3.8 远程知识库查询接口

下级安全管理系统可查询上级系统的知识库共享内容。

下级系统调用知识库查询接口，根据传递的接口参数获取相应的知识库案例内容，如该案例存在附件，则附件文档可供下载导出。

知识库查询接口为下级系统使用，下级系统可调用本接口，以触发查询功能；根据接口的参数，获取知识库内容，本接口为触发调用。

本接口的参数可为空，如为空则表明要查询所有知识库内容，知识库标题为模糊匹配，开始时间、结束时间可按时间段查询，结束时间需大于开始时间。

远程知识库查询接口规范见附件A.7。

10.3.9 报表上报接口

下级安全管理系统应按要求向上级系统汇报本系统的月报报表汇总信息。

下级安全管理系统将本系统产生的月报定期自动上报给上级安全管理系统，报表以文件方式传送，文件类型包括DOC、DOCX、XLS、XLSX、PDF、HTML、CSV等。文件名称遵循一定格式要求，报表文件上传方式采用SFTP加密传输方式。

报表上报内容应包括系统所属行政区编码、报表名称、内容。

报表上报接口规范见附件 A.8。

10.4 外部接口

安全管理系统应建立开放式的架构，能够通过必要的定制或使用内置的接口服务实现与 IT 运维管理平台等第三方平台的信息交换和管理协同。

10.4.1 安全管理系统外部接口要求

安全管理系统的外部接口内容：

a) 安全管理系统向第三方系统提供的信息（包括但不限于）：告警信息；
b) 安全管理系统从第三方系统接收的信息（包括但不限于）：资产信息、告警信息。

安全管理系统的外部接口方式：

a) 数据文档导入/导出：提供数据的导出功能，提供格式化文档的数据导入处理；
b) 使用通用协议进行数据动态交换：通过 SYSLOG、SNMP trap 实现安全管理系统与其他平台的信息交换；
c) 提供 Socket 或 Web Service 接口实现不同系统之间的同步或异步的数据交互。

10.4.2 外部数据导入接口

导入数据包括：资产信息、告警信息。

接口方式：

a) 安全管理系统通过文件方式，获取并导入资产信息；
b) 安全管理系统通过 Syslog 或 SNMP Trap 的接口方式从第三方系统获取其告警信息；
c) 安全管理系统通过 FTP 或 HTTP 方式获取数据文件，并提供导入解析接口。

10.4.3 内部数据导出接口

安全管理系统提供安全告警信息内容的导出功能，可导出为 Excel、TXT、RTF、PDF、HTML 等标准格式。具体内容的组织和文档格式根据业务需要确定，本标准不作进一步的限定。

10.4.4 与其他系统动态数据接口

安全管理系统可根据需要与其他系统建立接口，将告警和事件信息传送给其他系统，如事件处理系统，集中告警管理系统，实现相关安全信息的动态交换。并可将工单和运维信息传送给第三方运维管理系统，通过工单流程化处理，实现告警和事件的应急响应。也可将资产信息传送给资源管理系统或网络管理系统，实现资产信息交互。

接口方式可采用 Web Service 或 Socket 协议。具体的数据格式根据业务需要确定，本标准不作进一步的限定。

附 录 A
（规范性附录）
国家电子政务外网安全管理系统接口规范

A.1 系统级联注册接口规范

功能描述：

系统级联注册时采用上级主动添加下级信息的方式注册，下级提供接口接收上级通知。

接口函数定义为：

public String platformRegister(String xml**);**

请求参数 xml 格式如下：

```
<?xml version="1.0" encoding="UTF-8"?>
<PlatformInfo>
    <Higher><!-- 上级信息节点 -->
        <PlatformCode></PlatformCode>
        <IP></IP>
        <Port></Port>
    </Higher>
    <Lower><!-- 下级信息节点 -->
        <PlatformCode></PlatformCode>
        <IP></IP>
        <Port></Port>
    </Lower>
</PlatformInfo>
```

字段说明（*表示必选）：

标签名	名称	备注	类型	必选
PlatformCode	系统所属行政区编码	遵从GB/T 2260 《中华人民共和国行政区划代码》	char(32)	*
IP	IP 地址	Web访问地址	char(128)	
Port	端口	Web访问端口	char(32)	

返回格式如下：

```
<?xml version="1.0" encoding="UTF-8"?>
<PlatformInfo>
    <Status></Status> <!--1：成功，0：失败-->
    <Desc></Desc>
</PlatformInfo>
```

字段说明（*表示必选）：

标签名	名称	备注	类型	必选
Status	状态	1-注册成功；0-注册失败	int	*
Desc	描述	返回出错信息，调试用	char(128)	

A.2 系统级联注销接口规范

功能描述：

系统级联注销时采用上级主动注销下级的方式，下级提供接口接收上级通知。

接口函数定义为：

public String platformLogout(String xml**);**

请求参数 xml 格式如下：

```
<?xml version="1.0" encoding="UTF-8"?>
<PlatformInfo>
    <PlatformCode ></PlatformCode>
</PlatformInfo>
```

字段说明（*表示必选）：

标签名	名称	备注	类型	必选
PlatformCode	上级系统所属行政区编码	遵从GB/T 2260 《中华人民共和国行政区划代码》	char(32)	*

返回格式如下：

```
<?xml version="1.0" encoding="UTF-8"?>
<PlatformInfo>
    <Status></Status> <!--1：成功，0：失败-->
    <Desc></Desc>
</PlatformInfo>
```

字段说明（*表示必选）：

标签名	名称	备注	类型	必选
Status	状态	1-注销成功；0-注销失败	int	*
Desc	描述	返回出错信息，调试用	char(128)	

A.3 系统运行状态上报接口规范

功能描述：

上级安全管理系统对下级安全管理系统的运行状态进行查询，下级安全管理系统向上级系统上报本系统的运行状态信息。

接口函数定义为：

public String systemStatusQuery();

返回格式如下：

```
<?xml version="1.0" encoding="UTF-8"?>
<SystemStatus>
    <PlatformCode></PlatformCode>
    <IP></IP>
    <Status></Status>
</SystemStatus>
```

字段说明（*表示必选）：

标签名	名称	备注	类型	必选
PlatformCode	系统所属行政区编码	遵从GB/T 2260 《中华人民共和国行政区划代码》	char(32)	*
IP	IP地址	被查询安全管理系统IP。	char(128)	*
Status	状态	1-正常，0-离线	int	*

A.4 风险上报接口规范

功能描述：

上级安全管理系统向下级安全管理系统下发风险上报请求，下级安全管理系统向上级系统上报本系统的风险信息。

接口函数定义为：

public String riskInformationQuery(String XML);

请求参数 xml 为

```
<?xml version=”1.0” encoding=”UTF-8”?>
<RiskRequest>
    <Enable></Enable>
</RiskRequest>
```

字段说明（*表示必选）：

标签名	名称	备注	类型	必选
Enable	使能发送	1-允许上报风险；0-禁止上报风险	int	*

返回格式如下：

```
<?xml version="1.0" encoding="UTF-8"?>
<RiskInformationRespone>
    <PlatformCode></PlatformCode>
    <Domain>
        <DomainName></DomainName>
        <RiskValue></RiskValue>
        <RiskLevel></RiskLevel>
    </Domain>
    ……
</RiskInformationRespone>
```

字段说明（*表示必选）：

标签名	名称	备注	类型	必选
PlatformCode	系统所属行政区编码	遵从GB/T 2260 《中华人民共和国行政区划代码》	char(32)	*
DomainName	安全域名称	名称有“互联网区”和“公用网络区”，并可根据情况增加“专用网络区”	char(64)	*
RiskValue	风险值	风险值	int	*
RiskLevel	风险等级	风险等级，分为5级(1-5)，数字越大表示风险越高	int	*

A.5 告警上报接口规范

功能描述：

告警上报接口信息。在有告警发生时，下级安全管理系统需要向上级系统进行通报。上级安全管理系统向下级系统下发“订阅”指令，指定下级系统将符合订阅要求的告警上报给上级安全管理系统。下级安全管理系统依据订阅指令开始或停止告警信息的上报。

订阅采用 Web Service 方法，接口函数定义为：

public String alarmsInformationQuery(String xml);

请求参数 xml 为

```
<?xml version=”1.0” encoding=”UTF-8”?>
<AlarmsInformationRequest>
    <Enable></Enable>
    <Starttime></Starttime>
    <Endtime></Endtime>
    <Level></Level>
</AlarmsInformationRequest>
```

字段说明（*表示必选）：

标签名	名称	备注	类型	必选
Enable	使能发送	1-允许上报告警；0-禁止上报告警	int	*
Starttime	告警发生时间	当内容为空时，默认全部未发送告警。时间格式 YYYY-MM-DD HH24:MM:SS。	date	
Endtime	告警结束时间			
Level	告警安全级别	整型，分5级(1-5)，数字越大表示级别越高。表示发送所有大于等于该级别的告警，当内容为空时，表示发送最高级告警。	int	

上报采用 Web Service 方法，接口函数为：

public String alarmsInformationReport(String xml);

参数 xml 为

```
<?xml version=”1.0” encoding=”UTF-8”?>
<AlarmsInformationReport>
    <Alarm>
        <DeviceIP></DeviceIP>
        <DeviceName></DeviceName>
        <ID></ID>
        <ClearFlag></ClearFlag>
        <PlatformCode></PlatformCode>
        <Name></Name>
        <Desc></Desc>
        <Type></Type>
        <Level></Level>
        <OccurTime></OccurTime>
        <IP></IP>
        <Reserved></Reserved>
    </Alarm>
    ……
</AlarmsInformationReport>
```

字段说明（*表示必选）：

标签名	名称	备注	类型	必选
Alarm	告警信息元素	告警信息的元素，可为多个		
DeviceIP	设备(系统)IP	发送告警的安全管理系统的IP地址，	char(128)	*

		格式支持IPv4/IPv6		
DeviceName	设备(系统)名称	发送告警的安全管理系统的名称	char(64)	
ID	告警ID	告警的ID，标识该告警的唯一标识，为长整型。	long(64)	*
ClearFlag	告警清除标志	标识当前消息是告警报文还是恢复报文，1：告警报文；0：恢复报文；	int	*
PlatformCode	系统所属行政区编码	遵从GB/T 2260《中华人民共和国行政区划代码》	char(32)	*
Name	告警名称	告警名称	char(256)	*
Desc	告警描述	告警描述的详细内容	char(256)	*
Type	告警分类	告警所属类型	char(64)	
Level	告警等级	告警严重性等级(1-5)，数字越大级别越高	int	*
OccurTime	发生时间	告警发生的时间，采用长整型	long(8)	*
IP	告警涉及的IP	告警涉及的IP	char(128)	
Reserved	保留	保留字段，供后期使用	char(256)	

返回格式如下：

```
<?xml version="1.0" encoding="UTF-8"?>
<PlatformInfo>
    <Status></Status> <!--1：成功，0：失败-->
    <Desc></Desc>
</PlatformInfo>
```

字段说明（*表示必选）：

标签名	名称	备注	类型	必选
Status	上报结果状态	1-成功；0-失败	int	*
Desc	描述	返回出错信息	char(128)	

A.6 案例上报接口规范

功能描述：

下级安全管理系统通过本接口将本级系统的案例上报给上级系统。

接口函数定义为：

public String lowerDataSyn(String xml);

请求参数 xml 格式如下：

```
<?xml version="1.0" encoding="UTF-8"?>
<CaseAnalyselist>
    <PlatformCode></PlatformCode>
    <CaseAnalyse>
        <Id></Id>
        <Casetitle></Casetitle>
        <Createtime></Createtime>
        <Content></Content>
        <Keyproperty></Keyproperty>
```

```
            <Createman></Createman>
            <Attachflag></Attachflag>
            <Attachment></Attachment>
            ......
            <Attachment></Attachment>
            <Reserved></Reserved>
        </CaseAnalyse>
        ......
</CaseAnalyselist>
```

字段说明（*表示必选）：

标签名	名称	备注	类型	必选
PlatformCode	系统所属行政区编码	遵从GB/T 2260 《中华人民共和国行政区划代码》	char(32)	*
Id	案例标识	案例标识，用以区分案例及类别	int	*
Casetitle	案例标题	案例标题	char(32)	*
Createtime	创建时间	案例创建时间,格式 YYYY-MM-DD HH24:MM:SS	date	*
Content	案例内容	案例内容	char(512)	*
Keyproperty	关键字	案例关键字说明，用于关键字索引	char(32)	*
Createman	案例创建人	案例创建人姓名、单位和联系方式	char(32)	*
Attachflag	是否带附件标识	1-有附件；0-无附件	int	*
Attachment	附件URL	附件文件上传的URL，采用FTP方式，可以存在多个附件，每个附件对应一个URL。	char(256)	
Reserved	保留字段	保留字段，供系统使用	char(256)	

返回格式如下：

```
<?xml version="1.0" encoding="UTF-8"?>
<CaseAnalyseStatus>
    <PlatformCode></PlatformCode>
    <CaseAnalyse>
        <Id></Id>
        <Status></Status>
        <Desc></Desc>
    </CaseAnalyse>
    ......
</CaseAnalyseStatus>
```

字段说明（*表示必选）：

标签名	名称	备注	类型	必选

PlatformCode	系统所属行政区编码	遵从GB/T 2260 《中华人民共和国行政区划代码》	char(32)	*
Id	案例标识	案例标识	int	*
Status	案例上报状态	成功或失败，1-成功，0-失败	int	*
Desc	描述	成功失败描述，失败需写明失败理由	char(128)	

A.7 远程知识库查询接口规范

功能描述：

下级系统应能够共享上级系统的知识库内容。

接口函数定义为：

public String queryDocument(String xml);

请求参数xml格式如下：

```
<?xml version="1.0" encoding="UTF-8"?>
<Datadoc>
    <Titlekeyword></Titlekeyword>
    <Starttime></Starttime>
    <Endtime></Endtime>
</Datadoc>
```

字段说明（*表示必选）：

标签名	名称	备注	类型	必选
Titlekeyword	标题关键字	支持标题模糊查询	char(32)	*
Starttime	开始时间	时间格式 YYYY-MM-DD HH24:MM:SS	date	*
Endtime	结束时间	时间格式 YYYY-MM-DD HH24:MM:SS	date	*

返回格式如下：

```
<?xml version=”1.0” encoding=”UTF-8”?>
<Datadoclist>
    <Title></Title>
    <Cnt></Cnt>
    <Datadoc>
        <Createtime></Createtime>
        <Datasource></Datasource>
        <Content></Content>
        <Doc_url></Doc_url>
    </Datadoc>
    ……
</Datadoclist>
```

字段说明（*表示必选）：

标签名	名称	备注	类型	必选

Title	标题	查询标题关键字	char(32)	*
Cnt	文档数量统计	查询到的文档数量统计	int	*
Datadoc	返回数据	可为空（<Cnt>为0时，该元素为空）		
Createtime	创建时间	知识创建时间，格式YYYY-MM-DD HH24:MM:SS	date	*
Datasource	数据来源	标识知识来源的省及地市代码，格式为“省级代码_地市代码”	char(32)	*
Content	内容	知识详细内容	char(256)	*
Doc_url	文档URL地址	附件URL下载地址（多个文件时为目录）	char(256)	

A.8 报表上报接口规范

功能描述：

下级安全管理系统向上级系统定期发送月报文件。服务器端为每个下级安全管理系统设置目录，供下级安全管理系统上传文件。目录和文件属性设定为可读写，不可删除。

接口协议：

接口协议采用FTP或SFTP，必要时设定上传用户名和口令。

文件命名标准：

系统所属行政区编码-报表名称-类型-YYYYMMDD-N.扩展名。

类型：周报、月报。

N：表示序号。

A.9 省级单位代码表

省级代码	省份名称		省级代码	省份名称
000000	无归属地		410000	河南省
110000	北京市		420000	湖北省
120000	天津市		430000	湖南省
130000	河北省		440000	广东省
140000	山西省		450000	广西壮族自治区
150000	内蒙古自治区		460000	海南省
210000	辽宁省		510000	四川省
220000	吉林省		520000	贵州省
230000	黑龙江省		530000	云南省
310000	上海市		540000	西藏自治区
320000	江苏省		550000	重庆市
330000	浙江省		610000	陕西省
340000	安徽省		620000	甘肃省

350000	福建省		630000	青海省
360000	江西省		640000	宁夏回族自治区
370000	山东省		650000	新疆维吾尔自治区
			660000	新疆生产建设兵团