上海船研所涉密信息系统
应急计划与响应策略

舰船自动化分所

二０一五年八月

目 录

第一章 概述

1.1 编制目标

本预案的编制目的是提高上海船研所涉密信息系统（以下简称“涉密信息系统”）突发网络与信息安全及保密事件的能力。本预案通过预防措施和恢复控制相结合的方式，使得涉密信息系统发生的意外事件及造成的影响减少至最小，防止失泄密事件发生，以保障涉密信息系统的保密性、完整性及可用性。

1.2 适用范围

本文适用于上海船研所涉密信息系统安全、保密事件的应急处置工作。

1.3 事件分类

根据上海船研所涉密信息系统信息安全、保密事件的发生原因、性质和机理，网络与信息安全、保密事件主要分为以下几类:

1、系统失泄密事件应急计划

2、系统运行安全类应急计划

（1）系统故障类应急计划

a）基础设施故障

b）网络设备故障

c）安全产品故障

d）终端故障

（2）安全事件应急计划

a）网络入侵

b）病毒爆发

3、灾难类事件应急计划

1.4 应急响应体系设计

体系设计的首要任务是保护国家秘密的安全，防止失泄密事件发生，随后是保障信息的完整性与可用性。应急响应体系的基本流程如下：

1、泄密事件处理方式

当泄密事件发生时：

（1）应及时以口头或书面方式向所保密委员会如实报告。

（2）采取适当的措施（如断开网络，改变或终止用户权限等）切断泄密源头，控制泄密范围；

（3）确定泄密事件发生的原因，并及时对系统隐患进行修补；

（4）对系统的泄密隐患或风险进行重新评估，确认安全后，系统进行重新运行；

（5）对事件类型，发生原因，影响范围，补救措施和最终结果等进行详细记录。

2、运行安全事件处理方式

（1）针对可能发生的安全事件（如，病毒破坏，拒绝服务攻击等）以及所造成的对系统的损坏（如数据篡改，系统瘫痪等），制定并采取相应的应急响应和补救措施；

（2）对事件类型，发生原因，影响范围，补救措施，最终结果等进行详细记录。

3、体系设计的过程

（1）IT 应急措施的设计

对上海船研所涉密信息系统关键应用的应急保护，首先通过 IT 内部的应急措施加以实现。这些 IT 措施主要是数据备份、设备备份以及系统和网络的应急调用，断开网络，改变或终止用户权限等。

（2）非 IT 应急措施的设计

非 IT 应急措施是指在涉密信息系统应用过程中,为保证其保密性或可用性而采用的非 IT 技术手段。如切换到手工的方式进行业务的操作，或通过介质传输的方式进行半自动业务操作等。

（3）相关部门的协调

应急响应涉及组织各个部门和各个方面，需要各部门的配合和支持。

（4）应急资源的保证

应当将应急活动程序化，并通过程序化确定执行应急计划所需的组织资源，包括人员、设备、资金和其他物资，尤其是人员的保证和其他资源的统一指挥调度等。

（5）应急计划的启动条件

应当严格规定应急措施的实施和应急资源调用的程序、决策者和责任人。同时，启动应急计划的决策信息必须来自组织规范的报告制度，并有记录及可追溯。

（6）应急计划的演练

应急计划正式批准之前都必须进行演练。应急计划演练是组织应急计划完善的重要工作，包括应急计划演练的计划安排、演练过程和效果的详细记录，演练活动的评估报告和应急计划改进建议等。

第二章 应急响应组织

2.1 组织机构

为涉密信息系统的应急保障工作的执行，分所专门成立了安全保密应急响应小组。安全保密应急响应小组成员名单如下：

	职务	姓名
组长	分所所长	曹建明
组员	研究开发部主任	张欢仁
组员	综合计划部主任	黄国强
组员	综合计划部技术总监	毛奇林
组员	系统工程部副主任	张兴龙
组员	安全保密管理员	柴婉儿
组员	系统管理员	张晓慧
组员	安全审计员	耿琪

2.2 工作职责

安全保密应急响应小组负责对涉密信息系统突发失泄密事件与运行安全事件的紧急响应和恢复，在事件发生时，按照报告制度向有关领导汇报的同时，采取一切必要手段处理安全事故，并与上级部门和有关安全专业机构合作，在合适的情况下进行事故的分析和证据保护。工作职责包括：

（1）负责组织应急计划的编制和发布实施。

（2）负责对涉密系统突发安全保密事故的紧急响应和恢复。在事件发生时，按照报告制度向相关主管领导汇报的同时，采取一切必要手段处理安全事故，并与上级部门和有关安全专业机构合作，在合适的情况下进行事故的分析和证据保护。

（3）负责应急计划的培训、演练和维护工作。

第三章 应急响应流程

体系设计的首要任务是保护国家秘密的安全，防止失泄密事件发生，随后是保障信息的完整性与可用性。

3.1 事件分析

信息系统失泄密与运行安全事件发生后，首先是对事件进行判断，分析系统问题，继而选择相应的应急方案。

3.2 预防控制措施

3.2.1 技术措施

基础设施

- UPS；
- 电力冗余
- 空调维修
- 物业维修
- 通讯中断抢修
- 供应商服务

网络

- 设备备件
- 配置备份与恢复
- 临时连接措施
- 线路维修
- 供应商服务
- 平台切换

主机

- 设备备件

- 供应商服务

应用系统

- 系统备份与恢复
- 改变权限
- 中断系统

数据

- 数据备份
- 数据恢复

3.2.2 非技术措施

- 信息通告
- 警戒
- 介质保护
- 业务切换到手工或半自动状态
- 调查取证、法律诉讼

3.3 通知和启动

一旦确认系统遭到破坏、紧急状况发生或即将发生，通知是最初采取的应急活动，包括通知相应人员、评估系统损失和执行相应应急计划。在启动阶段完成后，应急响应人员将执行应急措施，消除事件影响，恢复系统。

3.4 恢复措施

3.4.1 技术措施

基础设施

- 电力切换
- 基础设施修复

网络

- 备件更换
- 配置恢复
- 线路修复
- 平台切换

主机

- 操作系统恢复

应用系统

- 系统恢复

数据

- 数据恢复

3.4.2 非技术措施

- 信息通告
- 解除警戒
- 业务切换数据处理与切换

第四章 测试、培训和演练

4.1 测试

对于应急响应预案涉及的各类保障措施应进行测试，确保预案的完好有效。主要测试的内容如下：

- 响应流程是否有效
- 应急措施是否有效
- 恢复流程是否有效
- 应急计划是否与测试情况一致

预案的审核通过形式化审查与实际操作模拟两种方式进行。形式化审查主要是对计划中的内容以问答的形式进行逻辑上的验证，实际模拟则是在可控的状态下模拟各类事件的发生，并进行实际的演习。

4.2 培训与演练

对于应急响应的内容以及涉及到的人员需要进行相关的培训与演练，培训包括以下两个方面：

- 关于应急响应预案的培训
- 关于人员相关技能的培训
- 通过演练进行协作培训

第五章 应急计划的维护

应急计划应根据系统变更进行定期的复审与更新。一般要求，当应急计划中涉及的任何部分发生重大变化，应急计划需要进行相应的复审，应急计划全面复审至少每年进行一次。应急计划复审的基础内容如下：

- 安全需求
- 响应程序
- 硬件、软件和其他设备（类型、规格和数量）
- 主要设备供应商和联络方式（备品备件）
- 应急响应小组成员名单和联络方式
- 重要记录（电子、纸质）

第六章 信息系统泄密事件应急计划

泄露国家秘密事件是指使国家秘密被不应知悉者知悉，或者超出限定的知悉范围，而不能证明未被知悉者知悉的事件(以下简称“泄密事件”)。

6.1 报告程序

发生泄密事件后，部门应当及时向分所安全保密管理员报告，安全保密管理员负责向安全保密应急响应负责人报告。

报告内容为：被泄露秘密事项的内容、密级、数量及其载体形式；泄密事件的发现过程；泄密事件发生的时间、地点及经过；泄密事件造成或可能造成的危害；泄密责任人的基本情况；已进行的查找工作情况；拟采取的补救措施。

上报时间要求：应当在 8 小时内上报。

分所所安全保密应急响应小组按照国家保密局的有关规定,向上级机关和上海市国家保密局报告，执行一事一报制度。

6.2 响应程序

部门向安全保密管理员报告后，应当及时采取补救措施，积极配合安全保密应急响应小组组织力量进行追查，努力挽回或减少泄密造成的损失。处置方式如下：

(1) 采取适当的措施（如断开网络，改变或终止用户权限等）切断泄密源头，控制泄密范围；

(2) 确定泄密事件发生的原因，并及时对系统隐患进行修补；

6.3 恢复程序

1、对系统的泄密隐患或风险进行重新评估，确认安全后，系统进行重新运行；

2、对事件类型，发生原因，影响范围，补救措施和最终结果等进行详细记

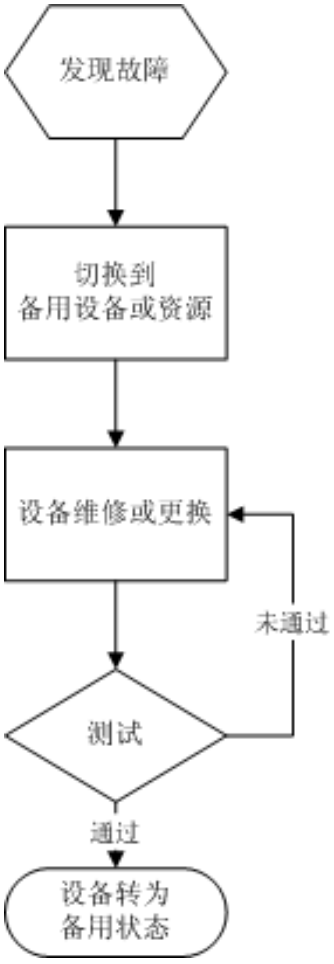
录。

3、泄密事件查清后，安全保密应急响应小组根据查证情况，按照《保密工作奖惩制度》有关规定,对泄密事件的有关责任人员做出处理决定；

4、每一泄密事件的查处工作的终结期限为 3 个月。安全保密应急响应小组负责将泄密事件的发生、发现过程，泄密事件已经或可能造成的危害，造成泄密事件的主要原因，采取的补救措施和对事件有关责任人员的查证处理情况，书面报告上级机关和上海市国家保密局。

第七章 系统运行安全事件应急计划

7.1 基础设施故障应急计划



基础设施故障应急计划流程图

1、基础设施故障包括 UPS、电力、通讯、消防设备、监控设备等出现故障，影响系统的正常使用；

2、安全保密应急响应小组在发现故障或接到故障报告后，启动基础设施故障应急计划；

3、安全保密应急响应小组应迅速判断发生故障的设备或线路，判断故障设施对系统运行的影响程度，有备用设备或线路的应迅速切换到备用设施；

4、对发生故障的设备或线路，联系有关部门进行处理，如：电力、后勤，供应商等；如需进入机房进行维护，由保密负责人向支持人员口头进行保密教育，

并由安全保密管理员负责全程监控，对进入人员进行登记；

5、故障修复或设备更换后，应对修复或更换的设备进行功能和性能测试，测试通过后将故障设备或线路转为备用状态。

7.2 网络故障应急计划

7.2.1 预案申明

网络部分是上海船研所涉密信息系统的承载主体，网络系统的故障将直接导致全部或部分业务的中断。本预案的目的是尽量保持业务连续，减小由于网络重大故障发生给业务带来的影响。

7.2.2 启动条件

1、根据上海船研所涉密信息系统的网络结构，网络部分的故障分为以下两个等级：

（1）交换机故障

H3C S5100 是上海船研所涉密信息系统的核心设备，H3C S3100 是桌面交换机，当 H3C S5100 交换机发生故障时，将会导致涉密信息系统所有用户无法进行网络相关应用操作，当 H3C S3100 交换机发生故障时，该交换机接入的部分用户无法进行网络相关应用操作。

（2）单点设备故障

当各涉密信息系统接入点发生故障时，将导致该接入点客户端无法进行网络相关应用操作。

2、本预案所指的故障指设备本身由于环境、机械方面造成的在现场无法修复的故障。或者在正常工作时间维修恢复时间预计将超过 2 小时的故障。

3、当发生网络中断，造成大部分或个别用户受到影响，经应急响应小组组员确认为上述两类故障中的一种，书面上报应急响应小组组长，由组长决定启动应急计划。

7.2.3 总体流程

7.2.3.1 响应流程

1、出现故障，首先通知系统管理员。

2、当出现骨干网络问题，系统管理员对故障进行处理与初步判断，当怀疑为网络设备故障时，立即通知安全保密应急响应小组组员，并填写相关记录。

3、安全保密应急响应小组组员应首先到现场进行进一步的分析处理工作，当确认故障满足应急启动条件，应立即通知安全保密应急响应小组组长，并填写应急计划启动申请。

4、如需进入机房进行维护，由安全保密管理员向支持人员口头进行保密教育，并负责全程监控，对进入人员进行登记；送修时应对数据介质（flash 卡等）进行妥善保护，防止数据泄露。

5、安全保密应急响应小组组长批准应急预案启动申请，并组织安全保密应急响应小组成员以及供应商启动应急计划。

7.2.3.2 恢复流程

1、安全保密应急响应小组根据故障的类型，调换发生故障的设备，采取相应应急措施（应急措施 1、2，见下节）。

2、对发生故障的设备进行故障分析，进行调试与检修直至设备恢复正常状态；

3、在下班或休息时间，安全保密应急响应小组对已修复或更换的设备进行性能和功能测试，测试通过后恢复系统。

7.2.4 应急措施 1－交换机失效

对于核心交换机失效的风险，如果是硬件故障，将立即通知设备厂商，由设备厂商 4 小时内提供备用交换机，导入原有核心交换机相关配置备份文件。备份机应可以完成与核心交换机相同的路由转发和访问控制等功能。

操作步骤：

（1） 将备用交换机上架，加电

（2） 跳线按原位置接入

（3） 调试

（4） 运行

7.2.5 应急措施 2－单点网络故障

对于接入点故障，采用布设应急线路的措施。

（1） 测量线路长度

（2） 制作符合安全保密要求的线路

（3） 测试

（4） 运行

7.3 主机故障应急计划

7.3.1 预案申明

本预案的目的是尽量保持上海船研所涉密信息系统应用服务器的连续可用性，减小由于主机故障发生给网络应用带来的影响。

7.3.2 启动条件

本预案所指的故障指设备本身由于环境、机械方面造成的在现场无法修复而使应用中断的故障。或者在工作时维修恢复时间预计将超过 4 小时的故障。

当发生业务中断或效率严重降低，造成应用受到影响，经安全保密应急响应小组组员确认为上述故障中的一种，书面上报安全保密应急响应小组组长，由组

长决定启动应急计划。

7.3.3 总体流程

7.3.3.1 响应流程

1、出现故障，发现问题，首先通知系统管理员。

2、系统管理员对故障进行处理与初步判断，当怀疑为主机设备故障时，立即通知安全保密应急响应小组组员，并填写相关记录。

3、安全保密应急响应小组组员应首先到现场进行进一步的分析处理工作，当确认故障满足应急启动条件，应立即通知安全保密应急响应小组组长，并填写应急计划启动申请。

4、如需进入机房进行维护，由安全保密管理向支持人员口头进行保密教育，并负责全程监控，对进入人员进行登记；维护时应对数据介质进行妥善保护，防止数据泄露。

5、安全保密应急响应小组组长批准应急预案启动申请，并组织安全保密应急响应小组成员以及供应商启动应急计划。

7.3.3.2 恢复流程

1、安全保密应急响应小组根据故障的类型，调换发生故障的设备，采取应急措施。

2、对发生故障的设备进行故障分析，进行调试与检修直至设备恢复正常状态；

3、安全保密应急响应小组对已修复或更换的设备进行性能和功能测试，重新安装各类软硬件并对服务器进行安全配置，测试通过后恢复系统。

7.4 安全产品问题应急计划

7.4.1 预案申明

本预案的目的是减小由于安全产品故障对业务造成的影响。

7.4.2 启动条件

根据上海船研所涉密信息系统的现状，安全产品事件有以下情况：

（1）安全审计故障

安全审计用于对重要的服务器区进行协议分析监控，安全审计的故障将会影响到业务的安全运行。当出现安全审计故障时，应暂停网络服务，服务人员按照预定的步骤定位故障问题，并进行问题的恢复。

7.4.3 总体流程

7.4.3.1 响应流程

1、首先通知系统管理员。

2、系统管理员对故障进行处理与初步判断，当怀疑为安全产品故障且无法进行排除时，立即通知厂商技术负责人，并填写相关记录。

3、供应商应按照服务承诺的要求立即赶赴现场，如经确定是硬件损坏必须4小时内携带全新设备到现场，同安全保密应急响应小组组员在现场确认问题，选择应急措施，并通知安全保密应急响应小组组长，同时填写应急计划启动申请。

4、如需进入机房进行维护，由安全保密管理员向支持人员口头进行保密教育，并负责全程监控，对进入人员进行登记；维护时应对数据介质进行妥善保护，防止数据泄露。

5、安全保密应急响应小组组长批准急预案启动申请，组织安全保密应急响应小组组员、供应商启动应急计划。

7.4.3.2 恢复流程

1、安全保密应急响应小组根据故障的类型，调换发生故障的设备，采取应急措施；

2、对发生故障的设备进行故障分析，进行调试与检修直至设备恢复正常状态；

3、安全保密应急响应小组对已修复或更换的设备进行性能和功能测试，并进行安全策略配置，测试通过后恢复系统。

7.4.4 应急措施 1－安全审计

7.4.4.1 事件定位

对故障进行分析，分析为安全审计产品故障并且无法在 4 小时内排除应立即进行维修。

7.4.4.2 备机替换

备机由厂商提供，应将系统配置导入备用机，将备用机联入网络。

7.4.4.3 系统恢复

当原有设备维修好，将配置文件导入到维修好的设备中，在非工作时间测试通过后，替换备用机恢复系统，替换的备机存储介质必须经过安全处理后才能用做他途。

7.5 终端故障应急计划

7.5.1 预案申明

本预案的目的是尽量保持上海船研所涉密信息系统接入终端的可用性，减小由于终端故障发生后可能出现的失泄密问题。

7.5.2 启动条件

本预案所指的故障指设备本身由于环境、机械方面造成的在现场无法修复而使应用中断的故障。或者在工作时维修恢复时间预计将超过 4 小时的故障。经安全保密应急响应小组组员确认为上述故障中的一种，书面上报安全保密应急响应小组组长，由组长决定启动应急计划。

7.5.3 总体流程

7.5.3.1 响应流程

1、当终端出现故障时，应首先切断电源，通知安全保密员。

2、安全保密管理员赶赴现场，隔离设备，设法保护数据。

3、分析设备出现的问题，则按照要求拆除存储介质，并送指定地点（PC 厂商）进行维修。如发生攻击事件，则按照入侵事件应急计划进行处置。（7.6.4）

4、记录问题的现象、时间、故障原因、处理方式等。

7.5.3.2 恢复流程

1、设备厂商对发生故障的设备进行故障分析，进行调试与检修直至设备恢复正常状态；

2、安全保密应急响应小组对已修复或更换的设备进行性能和功能测试，对终端进行安全配置，重新安装各类软硬件测试通过后恢复系统。

7.6 安全事件应急计划

7.6.1 预案申明

本预案的目的是减小由于人员或者恶意代码的原因对业务造成的影响，以及尽可能挽回事件造成的损失。

7.6.2 启动条件

根据上海船研所涉密信息系统的现状，信息安全事件分为以下几种情况：

（1）入侵

入侵事件将对主机或应用系统产生重大的影响，事件主要包括拒绝服务攻击、未经授权使用、植入木马、数据破坏等，入侵事件将造成系统的可用性下降甚至业务中断。当发现系统出现性能效率急剧下降，或入侵检测出现异常报警，以及防火墙或系统日志异常时，启动本预案。

（2）病毒或恶意代码

病毒或恶意代码将对主机系统的可用性造成影响，目前新型的病毒或恶意代码利用操作系统本身存在的漏洞进行攻击，一旦在网络内部传播，会大量占用系统和网络资源，严重影响业务的开展。当防病毒控制台出现异常病毒警报，或IDS 发现可疑流量，客户端报告异常现象时，启动本预案。

当发生系统效率严重降低、甚至应用中断，造成大部分或局部用户受到影响，经安全保密应急响应小组组员初步分析认定为信息系统安全事件，书面上报安全保密应急响应小组组长，由组长决定启动应急计划。

7.6.3 总体流程

7.6.3.1 响应流程

1、首先通知系统管理员。

2、系统管理员对故障进行处理与初步判断，当怀疑为安全事件时，立即通知安全保密应急响应小组组员，并填写相关记录。

3、安全保密应急响应小组组员应首先到现场进行进一步的分析处理工作，当确认安全事件满足应急启动条件，应立即通知安全保密应急响应小组组长，并填写应急计划启动申请。

4、如需进入机房进行维护，由安全保密管理员向支持人员口头进行保密教育，并负责全程监控，对进入人员进行登记；维护时应对数据介质进行妥善保护，防止数据泄露。

5、安全保密应急响应小组组长批准应急预案启动申请，并组织安全保密应急响应小组组员启动应急计划。

7.6.3.2 恢复流程

安全保密应急响应小组根据制定的响应方案采取相应应急措施。具体步骤见下节。

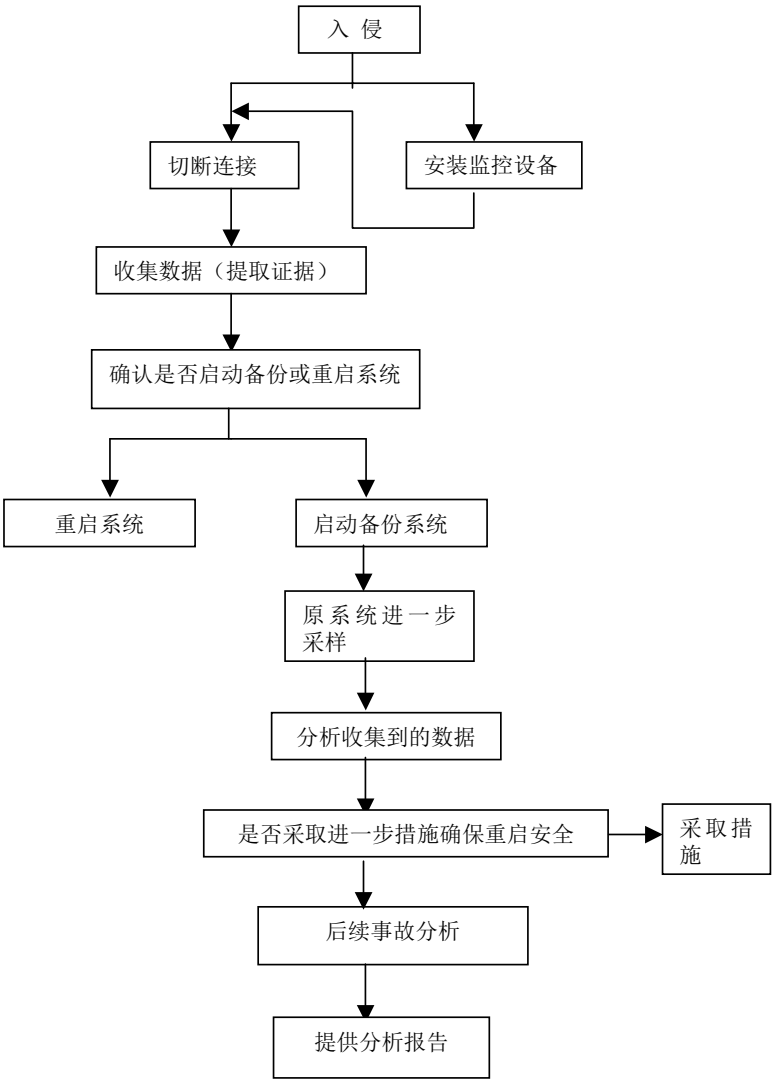
7.6.4 应急措施 1－入侵事件

7.6.4.1 事件响应

当安全保密应急响应小组接到系统管理员有关事件的汇报后，应准备工具赶赴现场，当怀疑为网络入侵时应首先中断网络服务，保存日志。

7.6.4.2 调查分析

安全保密应急响应小组到达现场对操作系统、审计、应用系统的日志进行分析，定位事件的类型，事件产生并保存相应的数据（如日志）。调查分析流程如下：



7.6.4.3 制定方案

根据调查分析的结果，评估事件影响的主机与系统。根据事件的影响选择安全措施，制定响应方案。

7.6.4.4 安全措施

1、抑制措施

对系统进行安全措施隔离，抑制进一步的破坏。涉密信息系统中可以采取的访问抑制策略如下：

a）防火墙策略：在防火墙设置策略，关闭相应的端口或阻止特定的访问。

b）核心交换机策略：在核心交换机设置策略，如禁止某些 VLAN 的通讯，或设置访问控制列表，禁止特定 VLAN 的访问等。

c）断开连接，将服务器暂时从网络中断开，待做好恢复措施后再接入。

采取破坏抑制措施时安全保密应急响应小组组员应根据措施影响范围书面上报安全保密应急响应小组组长，由组长通知受影响的部门访问限制的决定。

2、系统恢复

应首先组织对系统的重新风险评估，并执行相应的加固工作，确认满足安全运行要求时，方可执行系统恢复。如果数据已经被破坏，由安全保密应急响应小组进行系统的恢复工作，恢复措施见主机应急响应预案。

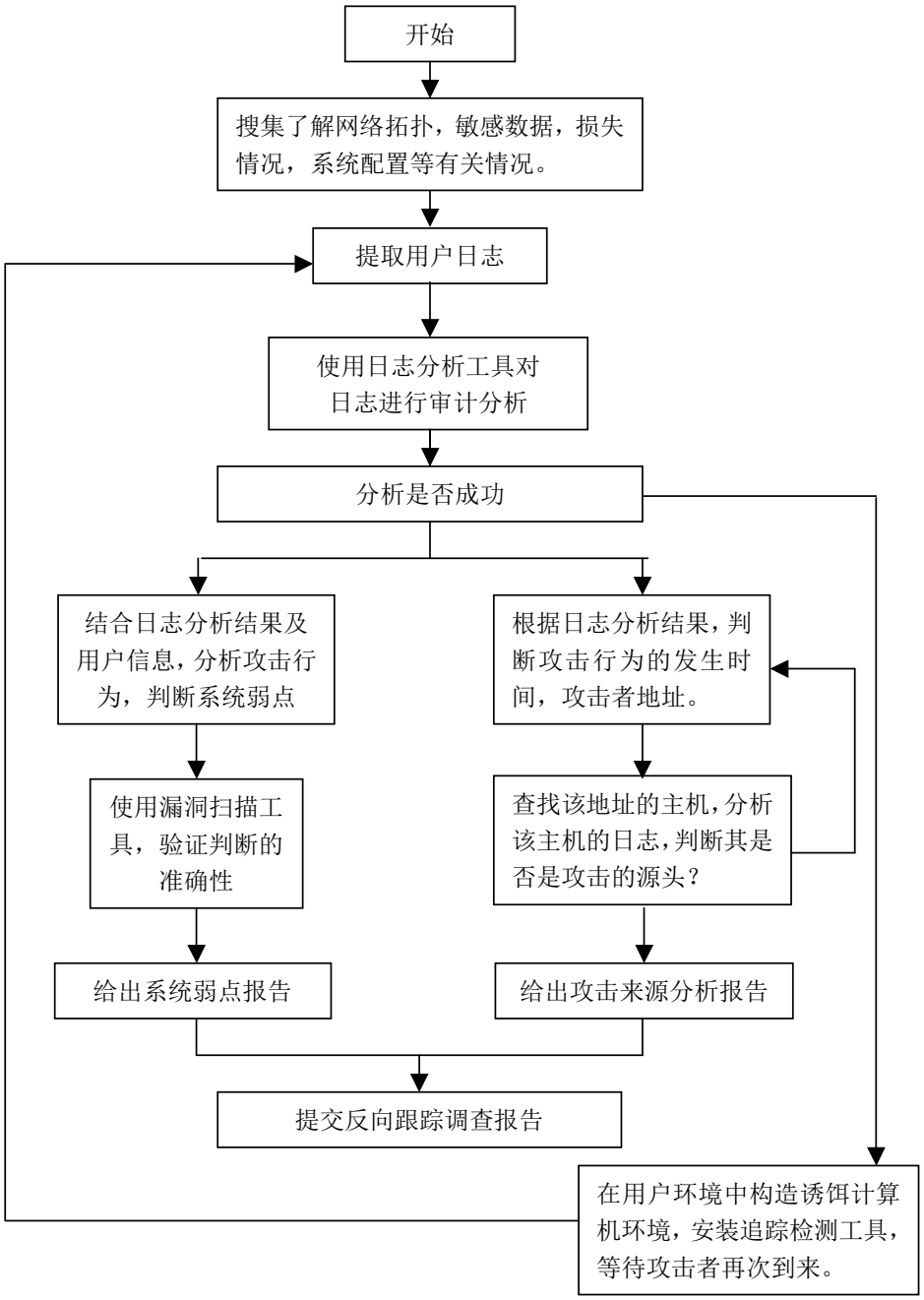
3、系统加固

系统加固是针对相应的主机操作系统进行的补丁修补或安全配置操作，防止进一步的侵袭。系统加固尽量在非工作时间进行，并且加固前应进行测试。

4、反相追踪

安全保密应急响应小组组员应根据系统分析的结果对入侵行为进行追查，寻找事件的根源。将事件追查的结果形成报告，上报安全保密应急响应小组组长。

事件追踪流程如下：


开始
搜集了解网络拓扑，敏感数据，损失情况，系统配置等有关情况。
提取用户日志
使用日志分析工具对日志进行审计分析
分析是否成功
结合日志分析结果及用户信息，分析攻击行为，判断系统弱点
根据日志分析结果，判断攻击行为的发生时间，攻击者地址。
使用漏洞扫描工具，验证判断的准确性
查找该地址的主机，分析该主机的日志，判断其是否是攻击的源头？
给出系统弱点报告
给出攻击来源分析报告
提交反向跟踪调查报告
在用户环境中构造诱饵计算机环境，安装追踪检测工具，等待攻击者再次到来。

7.6.5 应急措施 2－病毒

7.6.5.1 事件响应

当安全保密应急响应小组组员接到系统管理员有关事件的汇报后，应首先初步对问题进行分析，根据问题的情况，进行现场响应工作。

7.6.5.2 现场分析

安全保密应急响应小组到达现场通过防病毒控制台与入侵检测系统共同定位病毒源。

7.6.5.3 制定方案

安全保密应急响应小组根据分析的结果，选择安全措施，制定响应方案。书面上报安全保密应急响应小组组长，由组长批准实施。

7.6.5.4 抑制措施

对系统进行安全措施隔离，抑制进一步的破坏。涉密信息系统中可以采取的访问抑制策略如下：

（1）定位病毒源，并与其他系统隔离。

（2）利用病毒专杀工具。

（3）断开连接，将服务器暂时从网络中断开，待做好恢复措施后再接入。

采取破坏抑制措施时，安全保密应急响应小组组员应根据措施影响范围书面上报安全保密应急响应小组组长，由组长通知受影响的部门访问限制的决定。

7.6.5.5 后续工作

1、系统恢复

如果数据已经被破坏，由安全保密应急响应小组进行系统的恢复工作。恢复措施见主机应急响应预案。

2、病毒库升级

病毒库升级是针对相应的防病毒系统特征库进行的升级更新，防止病毒进一步的侵袭。

7.7 灾难性事件应急计划

7.7.1 预案申明

本预案的目的是减小由于人为或自然原因所引发灾难(如火灾、水灾、爆炸、地震等)对业务造成的影响，以及尽可能挽回事件造成的损失。

7.7.2 启动条件

当发生灾害情况（火灾、水灾、地震）引起机房设备损坏、业务中断，应立即启动应急计划。

7.7.3 总体流程

7.7.3.1 响应流程

1、首先通知系统管理员。

2、系统管理员立即拨打应急电话（火警 119，急救 120）并通知安全保密应急响应小组组长，并采取紧急措施进行灭火，防水。

3、安全保密应急响应小组组长立即通知所有小组成员到场，组织救灾工作，抢救人员、物资，对损坏的数据介质由专人负责看管。

4、灾情控制后，安全保密应急响应小组对损失情况进行评估，并制定应急方案，同时填写应急计划启动申请。

5、安全保密应急响应小组组长批准急预案启动申请，并组织组员实施应急计划。

7.7.3.2 恢复流程

1、安全保密应急响应小组根据制定的方案组织协调各部门、协调供应商、

内部调集资源采取应急措施恢复业务。

2、安全保密应急响应小组协调系统承建商进行系统的采购并执行系统的恢复工作。

7.7.4 应急措施

7.7.4.1 清点评估

当灾害受到控制后，安全保密应急响应小组应对涉密信息系统损害情况进行评估，评估应根据系统的文档资料对硬件设备、介质进行清点与测试，整理出完好的设备以及介质，损坏的设备到指定的部门进行报废。

7.7.4.2 制定方案

安全保密应急响应小组根据清点分析的结果，结合备份的物资，制定系统恢复方案，明确最小恢复策略需要的缺口物资。

7.7.4.3 恢复措施

1、物资调拨

应急响应小组根据恢复方案协调物资的购置与调拨，确保恢复业务的物资。

2、基础设施恢复

见 7.1 基础设施故障应急计划，首先应恢复电力供应以及空调。

3、网络恢复

见 7.2 网络故障应急计划。

4、系统与数据恢复

恢复措施见 7.3 主机故障应急计划。

5、系统最终恢复

系统恢复工作完成后需要按照工程的标准进行重新的评估与验收，确保系统得到了恢复。

附件 1：应急计划启动申请表

编号：

系统管理员：	日期：
情况描述	
事件分析	
分析人：	
建议启动预案	
领导批示： 签名： 日期：	
处理结果	
 签名： 日期：	
领导批示： 签名： 日期：	
备注：情况描述包括审计日志异常，病毒警报，发现入侵行为等各种安全事件，描述时应写明分析的依据。	

附件 2：涉密计算机房内安全检查表

在下班或休息时间定期进行检修，设备连接、环境、状态，发现问题及时进行更换、维修，确保各类设备的完好。

涉密计算机房内安全检查表

日期：			
检查项			
设备	**检查内容**	**检查结果**	**备注**
电源	是否有异常		
交换机	是否正常工作		
服务器	是否正常工作		
介质	涉密介质是否放入保险柜中		
文件	涉密文件是否放入保险柜中		
保险柜	是否妥善关闭		
安全审计设备	是否正常工作，日志是否将满		
门	是否妥善关闭		
其他			
检查人：	离开时间：		