中科院高能所计算中心

网络事故应急处理预案

中国科学院高能物理研究所计算中心网络组

二〇一〇年九月

文档信息

文档名称	管理建议文档	**管理编号**	IHEPCC-NWG-Admin-001
起草人	齐法制	**起草日期**	2008 年 12 月 25 日
参与人员		**修改日期**	2010 年 9 月 1 日
审核人员		**审核日期**	2010 年 9 月 2 日
复审人		**复审日期**	
文档摘要	本管理文档只涉及计算中心的日常管理		

版本变更记录				
版本号	**日 期**	**说明**	**修改人**	**备注**
1.0	2009/12/25			
版本号	**日 期**	**说明**	**修改人**	**备注**
1.1	2009/02./16		齐法制	
1.2	2010/09/02		齐法制	

目　录

1 综述

为了规范中国科学院高能物理研究所应急响应工作内容和工作流程，提高自身的应急响应能力，完善应急响应机制，确保信息系统的安全、稳定运行和业务的连续性，特制定本文档。

该文档应根据环境的发展而相应更新。

2 日常安全管理

2.1 人员职责分配

安全管理机构建设是整个管理过程的第一步。因此我们必须依照“谁主管、谁负责，谁运营、谁负责”的以及统一领导和分级管理的原则，信息安全管理需要设立专门的管理机构，明确主管领导，落实各项工作负责人，各尽其职。

2.1.1 技术负责人

高能所计算中心安全技术负责人的主要职责如下：

1) 制定、执行并维护有效的信息安全方针、程序和指导原则

2) 协助进行风险评估、执行化解风险的行动计划

3) 评估安全供货商和产品

4) 负责实施安全控制措施

5) 协助调查信息安全入侵事件

6) 进行必要的其他活动，确保安全的信息处理环境

2.1.2 系统与应用运维负责人

系统与应用运维负责人分为 Linux 系统与系统运维负责人和 Windows 系统与应用运维负责人，系统运维负责人的主要职责如下：

1) 系统设备物理安全

2) 系统与应用程序的安装、调试与日常维护

3) 系统与应用程序的资源和权限的正确划分和分配

4) 实时监控各系统与应用程序的运行状况

5) 按照规范对系统和应用程序备份

6) 定期检查系统与各应用程序日志

7) 参与应急响应

2.1.3 网络设备运维负责人

网络设备运维负责人的主要职责如下：

1) 负责网络设备物理安全

2) 网络设备的调试、配置与日常维护

3) 对网络中所有网络设备进行实时监控

4) 新添加设备的选型

5) 按照规范对网络设备的配置进行备份

6) 定期检查网络设备的日志

7) 参与应急响应

2.1.4 数据库运维负责人

数据库运维负责人的主要职责如下：

1) 负责各数据库的调试、配置和日常运行

2) 实时监控数据库的运行状况

3) 制定数据库备份的规范和流程

4) 按照制定的规范和流程定期备份数据库

5) 数据库资源和权限的正确划分和分配

6) 定期检查数据库日志

7) 参与应急响应

2.1.5 病毒与攻击防范负责人

部病毒与攻击防范负责人的主要职责如下：

1) 病毒与攻击防范体系的设计和实施

2) 定期对整个网络杀毒、对防病毒服务器进行升级

3) 防火墙策略的设计和配置及更改记录

4) 按照规范对防火墙和 IDS 等安全设备的配置备份

5) 定期检查各安全设备（产品）的日志

6) 参与应急响应

2.2 系统管理

2.2.1 系统资产登记

系统运维负责人（Linux 系统和 Windows 系统）必须对自己所管理的系统进行详细的登记，对各系统的运行状况了如指掌。下表为登记表参考格式。

《主机设备登记表》

基本信息	设备名称：	品牌型号：
	设备提供商及联系方式：	购买日期/服务期限：
	物理位置：	主要用途：
	登记时间：	登记人员：
硬件信息	CPU：	
	内存：	

	网卡：
	硬盘：
	硬件更换历史记录：
系统信息	主机名称：
	IP 地址：
	主要功能：
	操作系统：口 Linux 口 FreeBSD 口 Solaris 口 HP-UX 口 Windows 口 AIX 口 OpenBSD 口其它系统
	系统版本：
	内核：
	当前补丁级别与分析：
	当前端口及主要应用：
	安全服务情况（风险评估与加固情况）
应用信息	
密码控制范围	
运维人员	
责任人	
备注	

2.2.2 操作系统管理

2.2.2.1 操作记录

系统运维负责人所做的最多的工作就是日常的操作管理，在日常的操作管理中主要有以下几种操作类型：添加/删除程序、应用程序问题处理、文件的拷贝和删除、调整安全策略、修改用户名和密码、进程/日志查询、系统服务的关闭/重启、系统重启或关机等。

做这些操作时应将其过程详细记录，当系统出现问题时，我们能够检查《日常操作记录表》以判断操作人员进行操作是否正确，并采取对应的措施及时恢复。

《系统日常操作记录表》

基本信息	设备名称：	设备 IP:
	系统信息：	应用信息：
操作步骤		
回退步骤		
操作时间		
操作人员		
审批人		
备注		

2.2.2.2 定期检查

判断一个系统运行是否正常，仅从“是否正常连接/访问”等表面层次来衡量是不够的，系统管理需定期检查系统内部各个部分的运行情况，以保证系统很够长期、稳定的运行。下面列出了需要检查的各项：

1) 系统账户和密码：系统运维负责人应定期检查系统中帐户和密码是否正确，是否存在不明账户（检查周期为一星期）。
2) 服务与端口：系统运维负责人应定期检查系统中各进程、服务及端口是否正常，系统中有无异常进程和端口。
3) 安全设置：系统运维负责人应定期检查系统中的帐户与密码策略、审核策略、用户权限指派策略、安全选项等是否正确，有无被非法更改。
4) 特殊文件夹：系统运维负责人应定期检查系统中各重要文件夹，查看各重要文件是否存在，有无异常文件和程序。
5) 磁盘容量：系统运维负责人应定期检查系统磁盘容量，以确保有足够的磁盘空间来运行系统和应用程序。
6) 安全补丁和更新：系统运维负责人应关注系统安全补丁和更新，及时了解和获取相关安全补丁、重要更新，经过测试后给系统安装。

7) 查看系统日志：系统运维负责人应定期检查系统中的系统日志、安全日志、应用程序日志，以检查过去一段时间内系统的运行情况。其中需要重点审核以下特权操作：

（1）充当操作系统的一部分，如试图将某账户加入到管理员组等

（2）更改系统时间

（3）从远程强制关闭系统

（4）加载和卸载设备驱动程序

（5）管理审计和安全日志

（6）关闭系统

（7）取得文件或其他对象的所有权

2.2.2.3 密码管理

1) 密码切忌存在未加保护或其它人容易进入的介质(计算机系统、纸质和其它贮存介质)；
   a) 不能贮存在可读形式的批文件、自动登入脚本、软件宏(Macro)、终端功能键、无访问控制权的计算机中或其它可以容许未授权人员可发现或使用的位置 。
   b) 不能记下并留在未授权人可能会发现的地方。
   c) 不能在相关的访问设备附近写下。
2) 个人密码应当保密，工作组密码只能由组内成员使用；
3) 密码应保证一定的长度且应定期更换，口令设置的原则如下：
   a) 不容易被猜出。禁止使用字典中的单词和用户帐号可推导出的普通特征数字 (如「123456」)，不要包含姓氏的汉语拼音。
   b) 在建立或选择密码时不要选择一些比较容易识别的名字代号，或生日代号，应该选择含有至少 8 个字符，同时包含多种类型的字母和非字母字符，比如：
      - 大写字母(A,B,C,..Z)
      - 小写字母(a,b,c..z)
      - 数字(0,1,2,…9)
      - 标点符号(@,#,!,$,%,& …)
   c) 授权访问的各个系统应采用不同的密码。
   d) 针对一些特殊的系统，每 30 天强制性更改一次
   e) 如果怀疑密码已泄露或知道已泄露给了非授权方时要立即更改。

f) 任何两个账号的密码不能相同或相近。

4) 密码不要留在自动登录过程中。

2.2.3 系统和应用程序备份

系统运维负责人应根据系统和应用程序的具体环境制定备份策略和备份流程，系统运维负责人须定期对系统和应用程序的重要数据进行备份，备份时要严格按照制定的规范和流程进行。

在备份过程中出现任何问题都要及时处理。

2.3 应用管理

2.3.1 应用程序重要信息登记

系统与应用管理员应详细记录所维护的应用程序的重要信息，这些信息能够给应用程序的日常维护工作带来较大便利。

《应用程序信息记录表》参考格式

基本信息	应用程序名称：	版本号：
	提供商及联系方式：	购买日期/服务期限：
	宿主操作系统：	IP 地址：
	主要用途：	安装时间：
	安装人员	目前运维人：
部署方式		
正常运行状态（如开启的服务、端口等）		
联动的其他应用程序		
运行所需的帐户属性		
密码控制范围		

须注意的操作事项	
备注	

2.3.2 操作记录

系统运维负责人在工作中会对主要应用程序进行较多的配置和改变，为了让应用程序运行的更稳定及应用程序出问题后及时处理，需要详细记录对各应用程序进行的操作。

《应用程序操作记录表》

基本信息	IP:
	应用程序信息：
操作步骤	
回退步骤	
操作时间	
操作人员	
审批人	
备注	

2.3.3 日常故障错误处理记录

由于应用程序的设计缺陷或应用环境的复杂，导致应用程序在日常操作过程会出现各种现象和问题，在处理后应及时和详细地将现象和处理过程加以记录。

《操作系统日常故障错误处理记录表》参考格式

错误/故障发生时间		错误/故障结束时间	
应用程序			

名称/版本	
宿主 OS/IP	
现象描述	
处理过程（详细）	
备注	

2.3.4 可用性监控

系统运维负责人应实时监控各应用程序的运行状况，保证应用程序能实时提供服务。

2.3.5 访问权限审核

系统运维负责人应定期对应用程序所处理的资源进行访问权限的审核，为了系统和应用程序的安全，对各资源的访问应保证最小权限原则。

2.3.6 安全补丁和更新

系统运维负责人应关注各应用程序的安全补丁、重要更新、更新等，及时了解和获取相关信息和补丁，经过测试后给应用程序安装。

2.3.7 日志审计

系统运维负责人应定期审计应用程序的安全日志，检查是否有非法的连接和访问，并及时汇报和处理。

2.4 网络设备管理

2.4.1 网络设备资产登记

网络设备运维负责人必须对自己所管理的网络设备进行详细的登记，对各网络设备的运行状况了如指掌。下表为登记表参考格式。

《xxxx 网络设备登记表》

基本信息	设备名称：	产品型号：
	设备提供商/ 联系方式：	购买日期/ 服务期限：
	设备 IP:	物理位置：
IOS		
策略配置		
密码控制范围		
运维人员		
备注		

2.4.2 网络设备管理

2.4.2.1 实时监控

网络设备运维负责人应实时监控各网络设备，对出现问题的设备要及时处理。

《网络设备故障处理记录》

网络设备型号	IP 地址	事件原因	处理过程	备注

2.4.2.2 操作记录

为了保证网络设备的稳定运行和进行问题排查，对网络设备进行的操作都要详细记录。

《网络设备操作记录表》

基本信息	设备型号：
	IP 地址:
操作步骤	
回退步骤	

操作时间	
操作人员	
审批人	
备注	

2.4.2.3 定期审核策略

网络设备运维负责人应定期审核各项策略，保证各策略无重复、范围恰当，并且没有无关的策略。

2.4.2.4 安全补丁和更新

网络设备 IOS 及相关软件会出现安全漏洞，同时各厂商也会及时发布安全补丁及更新。网络设备运维负责人应关注网络设备相关信息，及时为各网络设备打上最新的补丁及更新。

2.4.2.5 定期审核日志

为了保证整个网络的安全，网络设备运维负责人应定期审核各网络设备的日志，检查是否有攻击行为，并根据日志及时报告和处理。

2.4.2.6 定期更改密码

网络设备的管理和控制是否有效和恰当直接影响到整个网络的连通性，因此各网络设备的密码（特别是 en 的密码）要定期更改。密码设置的原则同 Windows/Unix 操作系统密码设置一样，如下：

1) 不少于 8 个字符；
2) 不包含字典里的单词、不包括姓氏的汉语拼音；
3) 同时包含多种类型的字符，比如

（1）大写字母(A,B,C,..Z)

（2）小写字母(a,b,c..z)

（3）数字(0,1,2,…9)

（4）标点符号(@,#,!,$,%,& …)

4) 任何两个账号的密码不能相同或相近。

2.4.3 配置文件备份

网络设备运维负责人应定期对各网络设备的配置文件进行备份，当网络设备发生故障时可以及时恢复到正确的配置，将对网络的影响时间缩短至最少。

在数据库备份过程中出现任何问题都要及时上报和处理。

2.5 数据库管理

2.5.1 数据库使用情况登记

数据库运维负责人必须对自己所管理的数据库系统进行详细的登记，包括数据库类型、版本、运行平台及所在系统 IP 地址、补丁状况等。下表为登记表参考格式。

《数据库系统登记表》

基本信息	数据库类型：	版本号：
	运行平台：	系统所在 IP:：
补丁状况		
运行 Instance		
主要结合的应用程序		
运维人员		
备注		

2.5.2 数据库管理

2.5.2.1 可用性监控

数据库运维负责人应对所管理的数据库进行实时监控，保证其能够实时提供服务。

2.5.2.2 操作记录

对数据库进行的管理性操作，如添加/删除用户、创建数据库、备份、关闭和启动数据库服务等，这些操作须进行详细的记录，在数据库发生故障时能够及时发现和处理问题。

《数据库日常操作记录表》

基本信息	数据库类型：	版本号：
	运行平台：	系统所在 IP:：
操作步骤		
回退步骤		
操作时间		
操作人员		
审批人		

2.5.2.3 日常检查

1) 账户和密码：数据库运维负责人应定期检查数据库中的帐户和密码，查看是否有非法的帐户及弱密码。
2) 安全补丁和更新：数据库运维负责人应关注各数据库系统的安全补丁和更新，以保证各数据库运行在最安全和稳定的状态。
3) 磁盘空间：数据库运维负责人应定期检查系统的磁盘空间已保证有足够的空间来满足数据库在较长时间的运行。
4) 日志：数据库运维负责人应定期检查数据库日志，以及时发现异常或非法的连接和访问。

2.5.3 备份

备份对于数据库及其相关的应用程序来说异常重要，因此数据库运维负责人必须根据每个数据库的运行环境制定相应的备份策略和详细的备份流程。

数据库运维负责人根据制定的备份策略和流程定期为数据库进行备份，并要保证备份文

件的可用性。在数据库备份过程中出现任何问题都要及时上报和处理。

2.6 病毒与攻击防范管理

2.6.1 安全设备（产品）资产登记

病毒与攻击防范负责人必须对自己所管理的安全设备进行详细的登记，登记的信息包括安全设备的类型、产品型号、厂商、IP 地址、当前策略配置等。

《安全设备登记表》

基本信息	设备类型：	产品型号：
	设备提供商/ 联系方式：	购买日期/ 服务期限：
	设备 IP:	物理位置：
策略配置		
密码控制范围		
运维人员		
备注		

2.6.2 防病毒管理

2.6.2.1 病毒服务器升级

过时的病毒扫描程序比没有病毒扫描程序好不了多少，因此病毒与攻击防范负责人必须及时升级病毒服务器，为网络提供最新的病毒定义文件。另外，需要对病毒服务器的升级过程进行记录。

《病毒服务器升级记录》

升级日期	升级前状态		升级后状态		升级过程中出现的问题说明
	引擎版本	病毒库版本	引擎版本	病毒库版本	

2.6.2.2 杀毒

病毒会给网络和系统造成巨大影响或损失，病毒与攻击防范负责人必须定期（在病毒爆发时期例外）给各防病毒客户端杀毒。另外，需要将杀毒过程记录以供以后分析和查询。

《杀毒情况报告》

杀毒开始时间	杀毒结束时间	检测出的病毒说明				备注
		病毒名称	病毒类型	病毒危害	所在 IP	

2.6.3 防攻击管理

2.6.3.1 防火墙

1) 策略更改记录

防火墙策略配置的正确与否直接影响到内网的安全，因此病毒与攻击防范负责人必须对防火墙策略进行仔细审核，不用对外开放的服务一定不要开放。另外一些由于调试原因需要暂时对外开放的端口，在调试结束后应立即将其策略删除。

病毒与攻击防范负责人在日常工作中队防火墙策略进行的修改应详细记录，以确保出现问题能够较快找到问题的根源。

《防火墙策略修改记录》

修改日期	修改类型	具体修改内容	修改后测试结果	备注

2) 策略备份

对防火墙策略进行备份是为了在防火墙出现故障时能够准确、快速地恢复到正确的配置。当策略较多时，对策略备份更有必要。

病毒与攻击防范负责人应在每次修改策略并正确运行后对防火墙策略进行备份。

3) 日志

从外网发起的攻击上一般都会在防火墙留下痕迹，定期检查防火墙日志能够发现一些攻击的迹象。病毒与攻击防范负责人应定期（发生攻击事件后例外）查看防火墙日志，及早发现和阻止各类攻击。

3 应急响应制度

技术部对所有安全事故，在发现时要确保管理措施适当、一致，步骤包括评估、上报、跟踪、调查原因、做出详细记录、补救、预防、员工培训和需要的纪律处罚。

3.1 成立应急小组

组织体系是信息安全应急响应体系的核心内容，是开展信息安全应急响应工作的主体。

应急响应小组负责发生信息安全事件的应急响应工作，其成员应包含技术主管、工程师等。应急响应小组是事先就建立好的组织，应当明确指定各成员的职责。当发生安全事件时，应急小组要及时、负责地处理安全事故。

3.2 安全事故等级

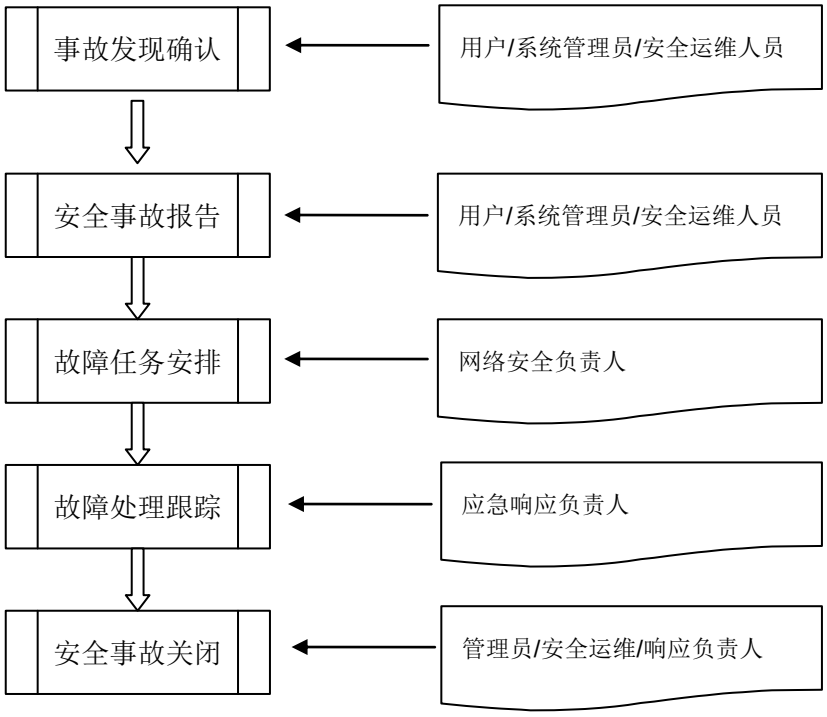
安全事故对技术部的影响按严重程度可以分类如下：

I级	*严重*	严重级别的事故的情形如下： a) 事件导致网络系统瘫痪 b) 事件对技术部信息资产的损失或损害会严重影响国家形象 要求立即采取措施解决这类安全事故。

II级	***较严重***	较严重事故的情形如下： a) 事件导致网络受影响且中断 b) 行为或事件会造成重大影响 c) 行为或事件导致或可能造成技术部的信息或系统的不可用。 d) 直接违背技术部的安全策略或方针的行为。 必须在指定的截止期限前解决该类安全事故。 处理这类事故必须指定截止期限，**截止期限不得超过 T+5 日历日(T=安全事故的报告日期)。** 如果该类安全事故未能在指定的截止日期前或经调查后发现该安全事故的威胁更严重时，该类事故的严重程度需要升级为 1 级并报告给技术部负责人。
3级	***轻微(包括安全漏洞)***	轻微级别的事故情形如下： a) 发现安全漏洞，可能需要对技术部的信息资产发出安全警报。 b) 所发生行为或事件可能会导致信息或系统的完整性受损 c) 所发生行为或事件可能会导致信息或系统的可用性受损 d) 某一行为可能会违反技术部的安全方针和程序。 处理这类事故必须指定截止期限，**截止期限不得超过 T+10 日历日(T=安全事故的报告日期)。** 如果该类安全事故未能在指定的截止日期前或经调查后发现该安全事故的威胁更严重时，该类事故的严重程度需要升级为 2 级并报告给技术部负责人。

3.3 安全事故处理流程

发生意外事件后，任何员工只要怀疑该事件对安全构成潜在的威胁，都要按照下述程序报告安全事故：



安全事故处理流程

3.3.1 安全事故发现与确认

a) 管理员/安全运维人员须密切关注网络中各系统的运行状态。

b) 当发生突发安全事件或异常状况时，管理员/安全运维人员应能迅速发现。

c) 管理员/安全运维人员应根据现场情况分析事故的原因和类型，并初步评估事件性质、危害程度和影响范围。

3.3.2 安全事故报告（直接报告或越级报告）

a) 管理员/安全运维人员必须通知安全负责人。

b) 安全负责人评估事件的性质。

c) 安全负责人作初步判定并做决定。

d) 安全负责人记录安全事故，包括具体的时间和报告人。

e) 如果安全负责人认为在指定截止期限之前或在可预见的限定时间内无法解决，可升级安全事故的安全等级。

f) I 级(严重)和 II 级(较严重)安全事故须立即报告给部门负责人和中心主任，确定进一步措施并联系应急响应人员。

g) 对于 I 级(严重)安全事故，管理员/安全运维人员须立即通告给应急人员。

3.3.3 安全事故任务安排

a) 应急响应负责人需协调并推动有关的支持组提出解决方案并记录解决方案。

b) 需要时技术工程师要恢复事故影响的服务或系统。

c) 未经安全负责人或其授权代表的预先同意，任何人不得调查安全事故或测试安全漏洞。

3.3.4 安全事故处理和跟踪

a) 安全事故应急响应负责人负责调查安全事故、找出根本原因并保证事故得到处理。

b) 安全事故应急响应负责人应评估安全事故是否需要修改或变动应用并及时通报技术负责人，以便其与有关应用方协调。

c) 安全事故应急响应应跟踪安全事故处理的进展情况。

d) 安全事故应急响应应在增加的控制措施成功实施后在问题和变更管理工具中关闭该安全事故。

e) 安全负责人必须在安全事故管理过程的各阶段了解到安全事故的所有信息，包括状态及逐步实施的步骤。

3.3.5 安全事故关闭

在完成下列步骤后，该安全事故可视为已解决。

a) 已找出安全事故的根本原因。

b) 导致安全事故的所有的安全弱点和漏洞都要受到控制以减少风险和接触的机会。

c) 出现问题的安全控制措施已经得到改善。

d) 改进或加强既定安全控制措施的计划。

e) 需要时决定对人员的一切必要纪律措施。

f) 应急响应负责人及时向技术负责人提交了《安全事故处理记录表》。

《事故处理记录表》参考格式

现象描述：		
系统信息（尽量详细）：		
应用信息：		
事故持续时间：		
解决方案：		
参与人员：		
注意事项：		
记录人：	审核人：	技术负责人：
备注		

另外，如果有新的解决方式，安全事故响应方必须保证将解决方式和步骤形成文档并递交给事故方技术负责人。

3.4 事后分析

事后分析能够及时吸取经验教训，避免相同或类似安全事件的再次发生。事后分析工作的意义不仅体现在本次信息安全事件的处理上，更重要的是有助于确定安全问题的深层次原因，总结处理紧急安全问题的经验和教训，评估和修正现有安全机制的不足，为后续可能发生的信息安全事件的响应过程提供参考。

事后分析工作的目标是回顾并整理发生信息安全事件的各种相关信息，尽可能将所有情

况记录到文档中，研究事件发生的全过程，分析导致事件发生的根本原因，评估系统遭受的损失，并根据分析和评估结果对现有的工作方案作出调整。对累次事件或同期多个事件的事后联合分析也更有意义。

针对信息安全事件的事后分析工作包括损失评估、审计分析以及对应急预案的评估修正。

a) 损失评估

评估信息安全事件对受保护信息系统在各方面所造成的损失。由于受保护系统本身的特性和安全需求有所不同，例如功能定位、服务需求、网络状况、系统状况、人员状况等，损失评估必须综合考虑信息安全事件造成的直接和间接的影响，需考虑的因素包括：

- 受损设备和设施：包括受到信息安全事件破坏或影响的服务器、客户机、输入输出设备、网络设备、通信线路、办公设备、安全设施、建筑物以及所有其它相关的设备设施。
- 受损数据：包括受保护系统中由于信息安全事件而遭到窃取、篡改或删除的数据，例如人事档案、公文、政务材料、安全日志等。
- 受损服务：由于受到信息安全事件的影响，无法向正常用户或公众提供相应的服务，例如 Web 服务器由于遭受拒绝服务攻击，无法为公众提供信息。
- 人力耗费：发生信息安全事件后，应急响应体系为了完成事件分析、事件处理、灾难恢复等工作所耗费的人力资源。
- 公众形象：由于信息安全事件的发生而影响到的公众形象，由此导致的无形资产损失。
- 重建资源：发生信息安全事件后，为了完成系统的重建恢复工作所耗费的各种资源，包括硬件、软件、人员、经费、通讯、能源、运输等。

b) 审计分析

对发生的信息安全事件进行审计分析，确定受保护信息系统中被安全事件所利用的漏洞，查明事件发生的原因，并提出相应的整改措施，综合利用技术、人员、管理等各方面的手段，避免相同或类似信息安全事件的再次发生。该项工作内容包括以下三个方面：

- 漏洞定位：安全威胁对系统造成影响的根本原因是受保护系统本身存在可被攻击的脆弱性（漏洞），例如软硬件漏洞、人员失误、管理制度缺陷等。为了从已经发生的信息安全事件中及时吸取经验教训，避免同类安全事件的再次发生，必须确定导致本次安全事件发生的漏洞，才能有针对性地确定整改措施，弥补系统漏洞。

- 查明原因：信息安全工作要坚持责任到人的原则，信息安全规划的首要工作是确定信息系统中的安全角色和对应的职责。在发生信息安全事件后，应根据事先确定的角色和职责，结合审计分析的结果，确定对安全事件的发生负有相关责任的人员，便于对信息安全事件的调查处理。
- 确定整改措施：根据上述漏洞定位和责任定位的分析结果，确定用于弥补系统漏洞的整改措施，例如更换存在缺陷的硬件设备、软件系统升级、安装系统补丁、修改系统配置、购置安全和监控设备、加强人员安全培训、制定并实施更为严格的安全管理制度等。

c) 应急预案的评估修正

对事先制定的信息安全事件应急预案进行评估，包括预案与实际事件的吻合性，预案的合理性、实用性、可操作性，分析预案在制定和实施过程中存在的问题和缺陷，在此基础上提出相应的整改方案建议，经批准后供应急预案修正使用。

- 预案效果：应急预案是在信息安全事件发生时，用于指示应急操作的指导文件。为了使应急预案能够最大程度地满足应急响应的实际需求，保证应急响应工作的准确性和高效性，每次启动应急预案并完成事件处理后必须对预案的实际效果进行评估，例如评估其是否符合本单位的应急响应需求、预案的实际操作效率、对于解决信息安全事件的实际效果等。
- 预案缺陷：受到各方面因素的约束，安全预案不可避免地存在一些设计和实施缺陷，本阶段工作的目的是确定预案制定和执行过程中的问题和不足，为预案的整改和修正提供基础。
- 预案更新：根据上述预案效果和预案缺陷分析的结果，提出针对信息安全事件应急预案的更新方案，经批准后在规定时间内完成预案的更新和审查工作，并予以发布实施。

4 应急预案

纵观网络安全发展的过程，应急体系是大家对网络安全的认识的第三个阶段（第一阶段为安全产品；第二阶段为安全产品+管理）。在许多人的潜意识中，网络安全应急指的是当发生安全事件时，去处理和补救的一种过程，称之为应急。这是一个错误的认识，是对应急

体系中一个过程的片面理解。我们之所以对网络加强安全，最重要的是保障网络业务的连续性。网络安全防护体系是从常规方面保障网络的安全，应急体系是基于网络防护体系上的一个扩充，最显著的是增加了对网络发生异常情况时，如何进行应急处理，即通常提及的应急预案。

网络是一个虚拟的社会，在现实社会中发生的各种现象，同样在网络中也发生。通过对SARS 事件的总结，我们国家建立了 SARS 应急预案；通过对密云观灯事件的总结，北京市已经逐步完善重大突发事件的应急预案。在网络中，通过对各种安全事件的总结，有必要建立网络安全应急预案，进而形成应急体系。依据国内外的相关标准和要求，我们对应急过程做如下分析：

PDCERF(Preparation、Detection、Containment、Eradication、Recovery、Follow-up)是对安全事件应急的通用过程。

1、 准备（Preparation）

通过对本单位网络的分析，采取必要的措施加强网络安全。应该包含安全支撑平台、日常安全管理和应急预案。安全支撑平台至少应该含有边界控制设备（如防火墙）和预警设备（如入侵检测设备——IDS）。日常安全管理应该能够保障安全支撑平台的正常运转，并不断根据需要调整安全策略。应急预案是对安全事件的应急处理流程，当发生异常情况，影响网络安全时，如何进行应对和处理，必要时获取外部资源的协助。对于重大安全事件的分析和处理，需要专业的安全人员来处理，大部分单位缺少这样的人才，因此，在建立安全预案时，如何获取外部资源，比如专业的安全服务厂商，就显得尤为重要。

2、 检测（Detection）

如何发现发生安全事件？有主动发现和被动发现两种途径。我们可以从网络使用者报告的异常情况中，确定发生了安全事件，这属于被动发现。

确定发生了安全事件时，我们首先想到，这是发生在一台主机上，还是发生在多台主机上，整个网络哪些主机已经发生，还有哪些主机处在危险之中。

如果在网络中部署了入侵检测设备，建立了全局预警系统，则可以主动发现网络安全事件。主动发现的好处是显而易见的，它具有及时性和全局性两个优点，而这恰恰是应急所必需的。同时也为后续的应急处理争取了宝贵的黄金时间。

3、 抑制（Containment）

对于已经发生安全事件的主机，采取可行的措施，避免影响其它的主机，必要时加以隔离。通过边界控制设备，防止网络的各个区域之间相互影响。对于处在危险之中的主机，也

应采取及时的补救措施。

4、 根除（Eradication）

通过对安全事件的分析，确定对主机的危害程度，分析发生安全事件的原因，找到防范措施，调整整个安全支撑平台的安全策略。

5、 恢复（Recovery）

包含对主机的恢复和对网络控制的恢复。对主机的漏洞及时修补，如果数据遭到破坏，从备份中加以恢复。在抑制阶段，为了避免事态的扩大，而采取的紧急措施中，可能存在影响部分业务正常运转的控制策略，这时候也应该恢复原来的状态。

6、 跟踪（Follow-up）

对安全事件进行总结，用于指导今后的应急；对于严重的安全事件，必要申请司法程序介入。

通过对应急过程的分析，结合网络系统中的重点防御部位和可能发生的一些突发情况，简要写出了相应的应急预案。

4.1 网络完全瘫痪

当遇到火灾、地震等意外情况导致网站完全瘫痪时，应急步骤如下：

1. 紧急领导小组开始应急工作，负责总体指挥和协调应急；
2. 应急响应人员开始进行现场清理，重建机房，整理和恢复网站设备，修复受损的设备，并在技术人员的指导下重新部署系统；
3. 设备硬件故障恢复后，如果备份磁带库可以使用，开始恢复数据；
4. 数据恢复并同步后，对系统重新进行测试；
5. 测试通过后，重新对外开放。

4.2 关键设备发生故障

当网络中的关键设备或关键应用设备发生故障时，应急步骤如下：

1. 应急响应人员通知相关领导；
2. 应急响应人员检查发生故障的设备，并尽力恢复设备，若设备损坏，紧急向厂家报修；
3. 设备维修完毕后，在技术人员的指导下重新部署系统；

4. 应急响应人员记录故障的处理过程。

4.3 黑客入侵

当发生黑客入侵事件时，应急步骤如下：

1. 应急响应人员上报领导小组，紧急求助安全专家和协助小组；
2. 检查网络和主机入侵检测设备，对黑客攻击的方式和目标进行判断和定位；
3. 如果可以，使用主机入侵检测设备的相应功能保护主机，切断黑客攻击；
4. 由安全专家小组紧急查找漏洞，并进行相应补救措施；
5. 安全专家小组查找攻击源头，并根据情况选择是否报告公安机关；
6. 安全响应人员对攻击情况进行记录。

4.4 DOS 攻击

当发生 DOS 攻击事件时，应急步骤如下：

1. 应急响应人员紧急上报领导小组，并求助安全专家和 ISP；
2. 应急响应人员在安全专家的帮助下调整相应设备功能，尽量阻断 DOS 攻击；
3. 联系 ISP，从 ISP 端对 DOS 攻击进行阻断；
4. 安全相应人员上报有关部门；
5. 对攻击事件进行记录。

4.5 病毒大规模爆发

当发生病毒大规模爆发事件时，应急步骤如下：

1. 应急相应人员联系安全专家；
2. 联合防病毒厂商，对病毒进行分类，并采取紧急手段杀毒；
3. 如果是未知病毒，由防病毒厂商采集相应特征码，并立刻进行分析，尽快研发出相应的杀毒软件并升级病毒库；
4. 记录该事件。

至于详细的安全预案，需要在对客户具体环境进一步了解的基础上制定。以下是某主机 IP 地址变动后的应急预案：

XXX 主机 IP 地址变动后需做如下应急操作命令		
操作过程	操作机器	具体执行命令
第一步： 终止 A 主机和 B 服务器上的 XXXX、XXXX 程序	A 主机	XXXXXXXXXXX
	B 服务器	XXXXXXXXXXXXXXXXX
第二步： 修改 XXX 主机和 XXXX 主机上配置文件中有关 IP 地址的部分	XXX 主机	修改主目录下 XXX 目录中的 XXXXXX 文件： ①将 XXXXXXXXX 的值改为新的 XXX； ②将 XXXXXXXXX 的值改为新的 XXX； ③将 XXXX 一段中 XXX 的值改为新的 XXX；
	XXXX 服务器	修改主目录下 XXX 目录中的 XXXXXX 文件： ①将 XXXXXXXXX 的值改为新的 XXX； ②将 XXXX 一段中 XXX 的值改为新的 XXX；
第三步： 重新运行 A 主机和 B 服务器上的 XXXX、XXXX 程序		

5 安全相关人员列表

网络安全负责人员	安德海	负责人	adh@ 电话：88236835 13910695575
	齐法制		qfz@ 电话：88236835 18910760801
	刘宝旭		liubx@ 电话：882368039
网络安全应急人员	安德海	负责人	adh@ 电话：88236835 13910695575
	杨泽明		yangzm@电话：
	刘宝旭		liubx@ 电话：882368039
	吴春珍		wucz@ 电话：882368039
	学生		
网络	安德海	负责人	adh@ 电话：88236835 13910695575

安全运维人员	马兰馨		ma@
	刘瑞荣		Liurr@
系统管理人员	吴玲	Mail/VPN	Wl@
	马兰馨	防火墙	Ma@
	刘瑞荣	防病毒	Liurr@
	石京燕	数据区服务器	shijy@
	张红梅	数据库管理员	Hmzhang@
网络管理人员	王彦明	校园网	wym@
	崔涛	数据区网络	cuit@
	李飞	在线网络	lifei@
	王春红	加速器控制网	wangch@