ICS 35.020
L 09

DB11

北 京 市 地 方 标 准

DB 11/T 1599—2018

政务部门信息安全应急预案编制指南

Preparation guidelines for government departments' information security emergency plans

2018－12－17 发布　　2019－04－01 实施

北京市市场监督管理局　发布

目　　次

前　言

本标准按照GB/T 1.1—2009 给出的规则起草。

本标准由北京市经济和信息化局提出并归口。

本标准由北京市经济和信息化局组织实施。

本规范起草单位：北京市政务信息安全应急处置中心、中国科学院信息工程研究所、北京邮电大学。

本规范主要起草人：王宗君、刘鹏、刘国伟、郭子亮、康振、魏彬、刘宝旭、王枞、刘建毅、刘涛、郭立生、杨泽明、荣晓燕、肖静、王汉臣。

政务部门信息安全应急预案编制指南

1 范围

本标准规定了政务部门信息安全应急预案的预案体系、编制流程、总体预案、专项预案和现场处置方案的基本内容。

本标准适用于政务部门信息安全应急预案的编制与修订工作，其他社会组织和单位信息安全应急预案的编制可参照本标准执行。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 20984 信息安全技术 信息安全风险评估规范

GB/T 20985.1—2017 信息技术 安全技术 信息安全事件管理 第1部分：事件管理原理

GB/Z 20986—2007 信息安全技术 信息安全事件分类分级指南

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 22240 信息安全技术 信息系统安全等级保护 定级指南

GB/T 24363—2009 信息安全技术 信息安全应急响应计划规范

GB/T 25069—2010 信息安全技术 术语

GB/T 31509 信息安全技术 信息安全风险评估实施指南

GB/T 32926 信息安全技术 政府部门信息技术服务外包信息安全管理规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

信息系统 information system

由计算机及其相关的和配套的设备、设施（含网络）构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。

[GB/Z 20986—2007,定义2.2]

3.2

信息安全事件 information security incident

由于自然或者人为以及软硬件本身缺陷或故障的原因，对信息系统造成危害，或对社会造成负面影响的事件。

[GB/Z 20986—2007,定义2.2]

3.3

应急预案 emergency plan

一种关于备份、应急响应和灾后恢复的计划。
[GB/T 25069—2010,定义2.2.3.4]

3.4

关键信息基础设施 critical information infrastructure

关系国家安全、国计民生，一旦数据泄露、遭到破坏或者丧失功能可能严重危害国家安全、公共利益的信息设施。

注：《中华人民共和国网络安全法》规定：国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护办法由国务院制定，包括但不限于提供公共通信、广播电视传输等服务的基础信息网络，能源、金融、交通、教育、科研、水利、工业制造、医疗卫生、社会保障、公用事业等领域和国家机关的重要信息系统，重要互联网应用系统。

4 应急预案体系

4.1 应急预案体系架构

政务部门信息安全应急预案体系由部门信息安全总体应急预案、部门信息安全专项应急预案和现场处置方案构成，如图1所示。

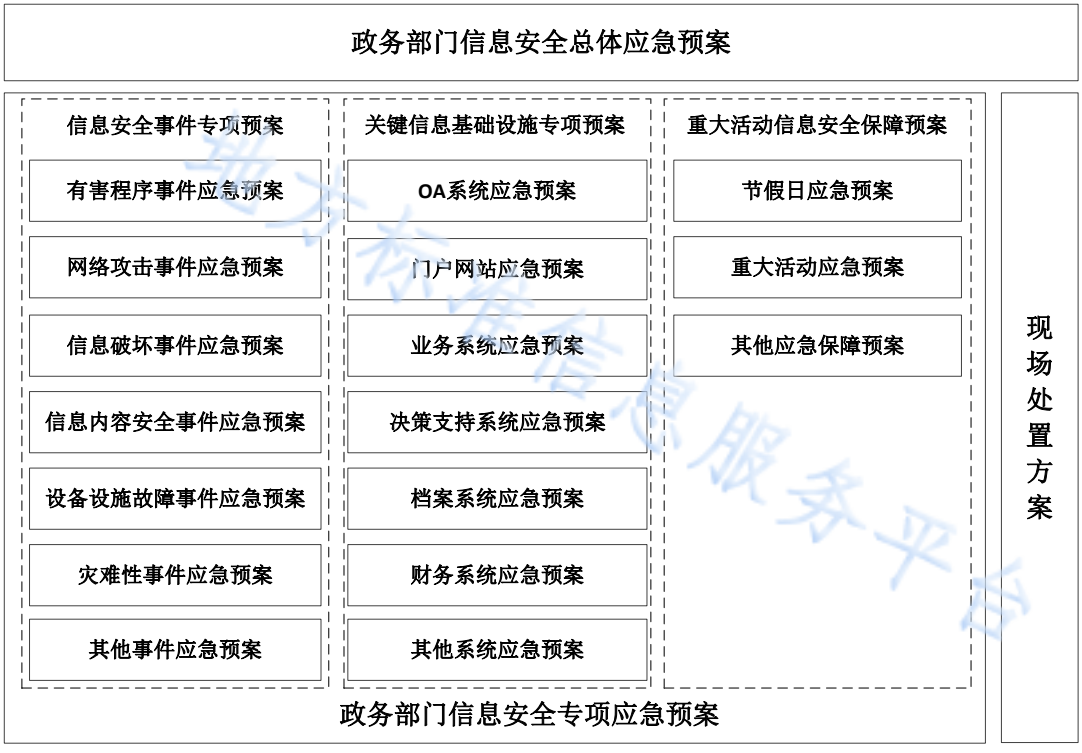


图1 政务部门信息安全应急预案体系

4.2 政务部门信息安全总体应急预案

4.2.1 政务部门信息安全总体应急预案是根据上级应急预案要求，针对信息安全事件综合性的应急响应程序和要求。是政务部门信息安全应急预案体系的总纲，是管辖范围内所有专项预案、现场处置方案的总体指导性文件。

4.2.2 政务部门信息安全总体应急预案应明确各政务部门信息安全应急工作的基本要求。

4.3 政务部门信息安全专项应急预案

4.3.1 政务部门信息安全专项应急预案是对某种类型或某几种类型的信息安全事件、对关键信息基础设施而预先制定的应急响应预案，分为信息安全事件专项预案、关键信息基础设施专项预案和重大活动信息安全保障预案三类。

4.3.2 政务部门信息安全专项应急预案是总体预案的细化，应对应急人员、应急流程、保障措施提出具体要求，对技术要求进行专项设计。

4.4 现场处置方案

现场处置方案是在总体预案和专项预案的指导下，针对政务部门网络与信息系统制定的适合现场应急处置的技术性方案，是专项应急预案的细化，具体指导现场工作人员对各个信息系统或信息安全事件应急响应的工作。

5 应急预案编制流程

5.1 基本流程

应急预案编制的基本流程为启动应急预案编制、应急体系调查、风险评估、业务影响分析、应急资源和能力评估、应急预案编制、应急预案评审及修订、应急预案发布及备案、应急预案管理与维护，应急预案编制流程如图2所示。

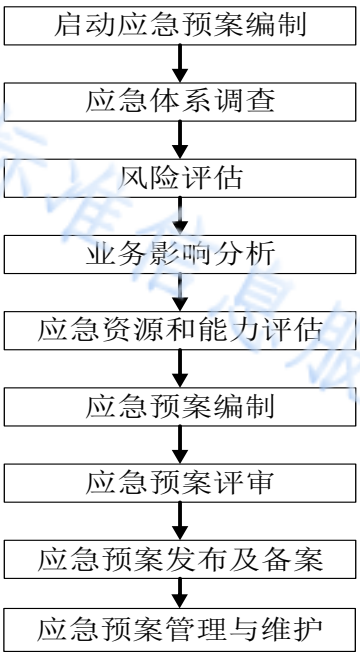


图2 应急预案编制流程

5.2 启动应急预案编制

5.2.1 根据应急处置目标政务部门应成立由应急工作负责人员、相关专业的外部专家、专业技术队伍、相关系统使用人员组成的应急预案编制工作组，应急预案编制工作组的组成，包括但不限于，各业务部门、各信息部门、各保障小组、各专家组。

5.2.2 制定应急预案编制计划，明确各小组的职责及接口人，外聘专家名单；预案编制计划时间表及各阶段的具体目标；预案编制工作开展的方式及方法。

5.2.3 提供开展应急预案编制工作所需的各项资源。

5.3 应急体系调查

5.3.1 收集了解政务部门的基本情况、组织环境、现有的应急体系等信息；收集已有的应急预案、已发生应急事件及处置手段和方法及其他应急相关资料；评估现有应急体系的完备性。

5.3.2 应急体系调查应包括但不限于以下内容：

——已有的应急预案，包括正在使用及废弃的预案；
——应急处置事件总结，包括原因、过程、处置手段及方法；
——现有的应急体系情况，包括但不限于人力、物质、技术、制度；
——现有应急体系分析、评价。

5.4 风险评估

5.4.1 风险评估是编制应急预案关键过程，风险评估的结果是确定重点考虑的应急对象，划分应急响应优先级的依据，政务部门应结合已有的安全措施和结合风险评估的结果确定应急响应工作的重点。

5.4.2 风险评估工作应按照 GB/T 20984 和 GB/T 31509 的要求，完成以下工作：

——对关键信息基础设施列表；
——确定风险评估的目标；
——制定风险评估的工作计划，确定工作方式方法；
——对资产、威胁和脆弱性进行识别；
——甄别现有安全措施；
——对残余风险及其可能导致的后果进行评估。

5.5 业务影响分析

业务影响分析应分析信息安全事件发生时所产生的损失和恢复所需信息系统资源，并符合GB/T 22239 和 GB/T 22240 中所规定的要求，包括但不限于以下内容：

——业务现状分析，明确业务流程、功能、渠道和连续性；
——信息系统现状分析，明确功能、拓扑、关联关系、中断影响；
——分析信息安全事件影响分析；
——分析信息系统应急处置优先级及恢复目标的确定。

5.6 应急资源和能力评估

应急资源和能力评估至少应包括物质资源、人力资源、技术资源、流程资源、外包服务商评估，具体评估包括但不限于以下内容：

——物质资源评估：应评估可用于信息安全应急响应工作的各项工具、设备和设施资源，确定在应急响应工作中可投入使用的物质资源，包括资源的类型、功能、作用和投入时间等；

——人力资源评估：应评估在信息安全应急响应工作中可以投入的人力资源、组织架构、技术支撑等，重点评估各应急岗位投入人员的数量、人员的技术能力和相关经验；

——技术资源评估：应评估在信息安全应急响应工作中的技术资源，包括采用的安全技术和安全产品，以及安全产品之间的互补性及可能存在的缺陷等；

——流程资源评估：应评估信息安全应急响应工作中现有的流程资源，包括明确资产和安全风险、应急响应工作的职责分配、现有的应急预案和灾难恢复计划、应急社会网络和其他应急机构的应急支援流程、应急资源的统一调配流程、以往信息安全事件及处理经验等；

——外包服务商评估：评估外包服务商在实际操作中的能力和应急响应程度，包括但不限于服务商资质、应急响应能力、应急响应物资等，并按照 GB/T 32926 对外包服务商进行安全评估。

5.7 应急预案编制

应急预案编制应符合信息安全相关法律法规、标准和其他应急预案编制的相关要求，政务部门应结合实际工作，完成应急预案的编制。应急预案应符合以下要求：

——应符合信息安全相关法律法规，国家应合规国家、行业和地方标准的相关要求；

——应合规、准确、完整；

——应方便查阅；

——在紧急情况启用时应便于实施。

5.8 应急预案评审

5.8.1 应急预案编制完成后，政务部门应对应急预案的适用性、科学性、合理性、针对性及规范性进行审核。应急预案的审核分为内部审核和专家评审，审核后应及时根据评审意见对应急预案进行修订。

5.8.2 政务部门内与信息安全应急管理相关的人员对应急预案应进行内部审查，审查应包括但不限于以下内容：

——应急组织体系；

——应急需求；

——预案可操作性；

——信息一致性；

——有效性；

——可控性；

——文字内容可读性。

5.8.3 应组织政务部门外信息安全、应急保障、应急管理等领域的专业人员成立的预案评审组对应急预案进行专家审查，评审组专家应不少于 5 人，审查应包括但不限于以下内容：

——应急预案规范性；

——应急预案体系的合理性；

——应急处置过程风险可控性；

——应急处置流程的科学性。

5.9 应急预案发布及备案

评审通过后的应急预案应按规定审批并正式发布。应急预案发布后，政务部门应组织相关人员进行应急预案培训和演练，明确职责、分工、安全事件处置方法和流程等，并根据相关要求将应急预案报有关部门备案。

5.10 应急预案管理和维护

5.10.1 正式发布的应急预案文档的管理，应符合以下要求：

——专人负责保存与发放应急预案；
——应急预案修订后应统一更新；
——最新版本的应急预案应及时发放给参与应急响应工作的相关人员；
——应急预案废止版本应按有关规定处理。

5.10.2 为确保应急预案的有效性，应急预案的维护应包括但不限于以下情况：

——业务流程的变化、信息系统的变更、组织机构调整、人员的变更及时在应急预案文档中反映；
——应急预案在测试、演练和实际执行均有详细的记录，对测试、演练和执行的效果进行评估，根据评估对应急预案文档进行相应的修订；
——每年组织一次评审或修订。

6 总体应急预案基本内容

6.1 基本内容及编制要求

6.1.1 政务部门信息安全总体应急预案包括总则、事件分类分级、组织机构及职责、预警及信息报告、应急响应、后期处置、保障措施及监督管理等内容，对应急处置的基本原则、应急组织结构、组织职责、应急响应的总体思路及应急救援活动的组织协调等提出具体要求。

6.1.2 总体应急预案应根据有关应急预案体系的要求，全面考虑，科学划分事件等级，覆盖应急工作全过程。政务部门信息安全总体应急预案可参见附录A。

6.2 总则

总则包括至少应急预案的编制目的、编制依据、工作原则、适用范围、应急预案体系及其他等内容，具体要求如下：

——编制目的：介绍制定信息安全应急预案的原因和制定应急预案的目标；
——编制依据：应急预案编制依据的法律、法规、规章、标准和规范性文件以及相关应急预案等；
——工作原则：应急工作的原则应简明扼要，明确具体；
——适用范围：应急预案的作用范围，解决哪些问题，不解决哪些问题；
——应急预案体系：可用框图形式表述应急预案体系的构成情况；
——其他：其他需要说明事项。

6.3 信息安全事件分类分级

6.3.1 按照GB/Z 20986—2007第4章信息安全事件分类要求，政务部门应根据信息安全事件的起因、表现和结果等实际情况，对应急预案中的信息安全事件分类进行适当删减和细化。

6.3.2 按照GB/Z 20986—2007第5章信息安全事件分级要求，政务部门应根据信息系统的重要程度、系统损失程度和社会影响程度等实际情况，对应急预案中的信息安全事件分级进行适当调整和细化。

6.4 角色及职责

角色及职责应符合GB/T 24363—2009中6.3条的要求。

6.5 预警及信息报送

6.5.1 政务部门应加强信息安全监测、预防和预警工作，信息安全事件的监测方式方法，预防和预警工作应符合 GB/T 24363—2009 中 6.4 条的要求。

6.5.2 政务部门应建立信息安全事件报告和通报制度，规定发生信息安全事件后，应立即向应急响应日常运行小组报告，应急响应日常运行小组对信息安全事件进行评估，明确事件的类别与级别，跟进事件级别，上报应急响应领导小组、相关主管或监管单位的要求。

6.6 应急响应

应急响应包括基本响应、分级响应、响应程序、处置措施、应急结束要求、应急总结等内容，对发生信息安全事件后所要采取的紧急措施，事件级别确定后的上报流程和分级响应，根据应急事件的变化对响应级别的调整等都应具体要求，基本要求如下：

——基本响应：应规定当发生信息安全事件后需首先开展的工作，包括紧急措施、事件识别、信息上报和情况通报等；

——分级响应：应规定根据信息安全事件危害程度、影响范围和对控制事态的能力，按照信息安全事件的分级启动应急响应；

——响应程序：应规定根据信息安全事件级别和发展态势，启动应急指挥机构、调配应急资源、应急救援及扩大应急等响应程序；

——处置措施：应规定根据信息安全事件风险、信息安全事件危害程度和影响范围制定的应急处置措施原则和具体要求；

——应急结束：应规定现场应急响应结束的基本条件和要求；

——应急总结：应规定收集、整理和记录信息安全事件过程的各种相关信息，对应上报的事件应规定准备的相关材料和上报的部门。

6.7 后期处置

6.7.1 应急响应工作结束后，应对信息安全事件造成的损失和影响以及恢复重建能力进行分析评估，根据评估结果制定相应的系统加固方案，通过版本升级、漏洞修复、修改安全配置和增加安全机制等方法，对系统的安全性进行加强或对系统进行重建。

6.7.2 应急响应总结宜按照 GB/T 20985.1—2007 中 5.6 条的要求，总结应急响应工作，具体要求包括但不限于以下内容：

——分析和总结事件发生的原因；

——分析和总结事件的现象；

——评估系统的损坏程度；

——评估事件导致的损失；

——分析和总结应急处置记录；

——评审应急响应计划的效果和效率，提出改进建议；

——评审应急响应措施的效果和效率，提出改进建议；

——对相关单位和人员的表彰和惩罚。

6.8 保障措施

保障措施包括应急队伍的保障、应急通信保障、专业应急设备保障及重要数据备份保障等内容，保障措施基本内容如下：

——应急队伍保障：应急响应的人力资源，包括应急咨询专家、专业应急队伍、兼职应急队伍和外部合作队伍等；

——应急装备保障：信息网络硬件、软件的清单和管理责任人及其联系方式等内容，罗列应急通信保障措施和重要数据备份机制等；

——其他保障：根据应急工作需求确定其他相关保障措施，包括但不限于经费保障、交通运输保障、治安保障、技术保障及后勤保障。

6.9 监督管理

监督管理部分基本内容如下：

——应急预案培训：政务部门对人员开展应急预案培训的计划、方式和要求，培训应达到有关人员了解应急预案内容，熟悉应急职责、应急程序和处置方案；

——应急预案演练：不同类型应急预案演练的形式、范围、频次、内容、演练评估和总结等要求；

——应急预案修订：应急预案修订的基本要求和修订周期，并应规定应急预案评审周期；

——应急预案备案：应急预案的报备部门及备案要求；

——应急预案实施：应急预案发布与实施的具体时间以及负责制定与解释的部门。

6.10 附件

政务部门信息安全总体应急预案的附件应包括但不限于以下内容：

——应急处置流程图：根据信息安全事件级别与类型，使用图表形式展现各处置阶段的参与部门与处置权限，包括完整的应急响应过程中的各个环节；

——有关应急部门、机构或人员的联系方式：编制至少包括小组名称、姓名、职位、工作电话、家庭电话、手机及电子邮箱等内容的联系人表，列出应急工作中需要联系的部门、机构或人员的多种联系方式，当发生变化时应及时进行更新，信息系统较多政务部门可利用制定呼叫树的方法来规避人员无法联系；

——应急信息接报、处理、上报等规范化格式文本：信息安全事件报告文本内容应包括单位名称、报告人、联系电话、通讯地址、电子邮件、事件报告时间、信息系统名称、主要用途及信息安全事件的简要描述等信息；

——有关协议或备忘录：应包括与相关应急救援部门签订的应急救援协议或备忘录。

7 专项应急预案基本内容

7.1 基本内容及编制要求

政务部门在制定信息安全专项预案时，应针对政务部门的关键信息基础设施、信息安全事件的特点，进行应急组织、流程和技术保障措施的设计。政务部门信息安全专项应急预案可参见附录B。

7.2 总则

总则部分基本内容如下：

——编制目的：制定专项应急预案的原因和制定预案的目标；

——工作原则：专项应急工作的原则应简明扼要，明确具体；

——适用范围：专项预案的作用范围，解决哪些问题，适用于哪些系统；

——其他：根据需求的其他应说明事项。

7.3 组织机构及职责

应急机构涉及到相关的单位和人员应包括：系统责任单位、系统业务人员、基础运维人员、安全运维人员、系统建设单位及系统使用各类设备设施的生产商或代理商等。根据政务部门的关键信息基础设施、信息安全事件或者重大活动保障中的安全风险，明确应急组织形式、构成单位或人员；明确各机构的工作任务及主要负责人的职责。

7.4 风险分析与预案启动

应对关键信息基础设施或重大活动保障发生某种具体或特定类型信息安全事件的可能性进行分析，预判信息安全事件发生的风险、严重程度、影响范围等，结合信息系统的重要程度或重大活动保障级别，启动相应等级的应急预案。包括但不限于以下内容：

——可能发生的信息安全事件类型；

——信息安全事件可能发生的时间；

——信息安全事件发生前可能出现的征兆；

——信息安全事件可能引发的次生、衍生信息安全事件；

——信息安全事件对关键信息基础设施业务运行产生的危害程度及影响范围。

7.5 应急响应流程

应针对关键信息基础设施，根据信息安全事件响应的级别，明确应急响应的报告程序和内容、报告方式和责任人等内容，对信息安全事件接报和记录、应急指挥机构启动、资源调配、应急处置、扩大应急等响应程序提出具体要求。

7.6 应急处置措施

信息安全事件应急处置措施主要分为：应急准备、分析确认、抑制根除、恢复运行。应针对关键信息基础设施可能发生的信息安全事件的风险、信息安全事件危害程度和影响范围，制定相应的应急处置措施，明确处置原则和具体要求。

7.7 保障措施

应明确专项预案各类应急响应的人力资源、技术资源及后勤保障资源等，包括专项应急队伍、专项应急设备保障、应急保障经费等。

7.8 宣传、培训和演练

对专项预案的宣传教育和信息安全相关知识培训等工作提出要求，包括对信息化工作人员定期培训，使其熟悉信息安全相关知识，掌握故障排除步骤及实操技能；定期开展信息安全应急演练以检验信息化工作人员的业务技能。

7.9 附件

附件应包括但不限于以下内容：

——应急物资装备的名录或清单：包括应急预案涉及的主要物资和装备名称、型号、性能、数量、存放地点、运输和使用条件、管理责任人和联系电话等；

——关键的路线标识、应急工具清单和图纸：包括详细的网络拓扑图，应急专用工具清单、位置及保管人，应急专用工具操作指导书，机房相关平面布置图纸等。

8 现场处置方案基本内容

8.1.1 现场处置方案应组织各类信息安全的专业组织和技术专家、部门运维技术人员共同参与制定，对应急处置中的各个方面提出的具体细致的要求，确保其针对性和指导性。现场处置方案可参见附录 C。

8.1.2 应针对发生的信息安全事件，从技术操作的角度加以规范，明确处置原则和具体处置步骤，细化各类作业指导书、操作手册及故障排除方案。现场处置方案要包括但不限于：

——恶意进程检查作业指导书；
——病毒木马检查作业指导书；
——数据恢复作业指导书；
——系统迁移作业指导书；
——拒绝服务攻击事件作业指导书；
——网络及安全设备配置变更操作手册；
——硬件故障应急处置手册；
——网络故障应急处置手册。

附 录 A
（资料性附录）
北京市某局信息安全事件总体应急预案示例

A.1 总则

A.1.1 编制目的

为完善北京市某局应急预案体系，健全网络与信息安全应急工作机制，提高应对信息安全突发事件的能力，预防信息安全事件的发生，降低造成的损失和危害，特编制此预案。

A.1.2 编制依据

《中华人民共和国网络安全法》《中华人民共和国突发事件应对法》、《北京市实施<中华人民共和国突发事件应对法>办法》、《北京市信息化促进条例》等法律法规，《国家突发公共事件总体应急预案》、《国家网络安全事件应急预案》、《北京市突发事件总体应急预案》、《北京市网络与信息安全事件应急预案》等相关规定。

A.1.3 工作原则

坚持统一指挥、密切协同、快速反应、科学处置；坚持以预防为主，预防与应急相结合；坚持谁主管谁负责、谁运营谁负责等原则。充分发挥各方面技术力量，共同做好某局信息安全事件的预防与应对工作。

A.1.4 事件分类分级

A.1.4.1 事件分类

信息安全事件分为有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障事件、灾害性事件、其他信息安全事件，每个基本分类可以分别包括若干个子类。

（1）有害程序事件分为计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合程序攻击事件、网页内嵌恶意代码事件和其他有害程序事件。

（2）网络攻击事件分为拒绝服务攻击事件、后门攻击事件、漏洞攻击事件、网络扫描窃听事件、网络钓鱼事件、干扰事件和其他网络攻击事件。

（3）信息破坏事件分为信息篡改事件、信息假冒事件、信息泄露事件、信息窃取事件、信息丢失事件和其他信息破坏事件。

（4）信息内容安全事件是指通过网络传播法律法规禁止信息，组织非法串联、煽动集会游行或炒作敏感问题并危害国家安全、社会稳定和公众利益的事件。

（5）设备设施故障分为软硬件自身故障、外围保障设施故障、人为破坏事故和其他设备设施故障。

（6）灾害性事件是指由自然灾害等其他突发事件导致的网络与信息安全事件。

（7）其他事件类别是指不能归为以上6个基本分类的信息安全事件。

A.1.4.2 事件分级

按照GB/Z 20986—2007《信息安全技术 信息安全事件分类分级指南》第5章信息安全事件分级及电子政务实际建设需要，并结合北京市某局信息安全事件影响程度和响应级别，将信息安全事件分为特别

重大（Ⅰ级）、重大(Ⅱ级)、较大(Ⅲ级)、一般（Ⅳ级）、较小（自管级）事件。涉及特别重大（Ⅰ级）、重大(Ⅱ级)、较大(Ⅲ级)的按照《北京市网络与信息安全事件应急预案》要求执行，由上级信息化主管部门负责事件的应急处置工作，局信息化相关部门配合完成信息安全事件的现场应急处置工作；某局本级信息化部门负责一般（Ⅳ级）、较小（自管级）信息安全事件的处置工作。

特别重大（Ⅰ级）、重大(Ⅱ级)、较大(Ⅲ级)信息安全事件的分级标准参照《北京市网络与信息安全事件应急预案》执行。

一般（Ⅳ级）信息安全事件：

①网站或信息系统在非敏感时期发生的网页篡改事件，被篡改内容涉及反动标语或不当言论；

②网站或信息系统被恶意入侵，被攻击者植入木马、暗链、后门等，存在严重的安全隐患；

③等保二级信息系统中断2小时以内，业务受到影响；等保三级信息系统中断30分钟以内，业务受到影响；

④对国家安全、社会秩序、经济建设和公众利益构成威胁、造成一定影响的事件。

较小（自管级）信息安全事件：

①敏感信息泄露，重要备份数据丢失等安全事件；

②由于各种原因导致的各类系统中断、服务中断、设备故障等安全事件；

③未达到一般信息安全事件（Ⅳ级）条件的事件为自管级事件。

A.1.5 适用范围

本预案适用于北京市某局信息安全事件的总体预防和处置工作。

A.2 组织机构与职责

北京市某局信息安全事件应急组织机构，由信息安全领导小组、信息安全工作组和信息安全实施组组成，负责信息安全事件的预防和应对工作。信息安全组织机构涉及的相关角色分配如下：

A.2.1 信息安全领导小组

组　长：局长

副组长：信息技术处处长

信息中心主任

组　员：XXX

负责北京市某局电子政务领域信息安全管理协调工作；协调电子政务信息安全和信息安全保障体系建设；指导监督各部门的重要信息系统与重要信息基础设施的安全保障工作；协调处理电子政务领域的重大信息安全事件。

A.2.2 信息安全工作保障组

组　长：信息技术处处长

副组长：信息中心主任

组　员：XXX

负责北京市某局信息安全技术方面的应急处置工作；负责信息安全的监测预警工作；负责开展信息安全应急预案制定和应急演练的技术保障工作；负责信息安全基础设施的规划和管理工作；负责对信息系统进行安全性评估及测试；负责安全管理人员的培训；提供安全管理和安全技术方案的咨询服务。

A.2.3 信息安全实施组

组　长：信息技术处处长

副组长：信息中心主任

组　员：XXX

负责信息安全事件的技术响应，调查事件原因，分析事件影响范围，制定具体处置方案，实施具体的应急处置工作。

A.2.4　信息安全日常运行组

组　长：信息中心主任

组　员：XXX

负责北京市某局信息系统的日常运维，负责备份中心的日常管理、应急监控系统的运作和维护、参与和协助应急响应计划的测试、培训和演练。

A.2.5　信息安全专家组

负责提供紧急情况下的应急技术方案和应急技术支援体系，对重大信息安全事件进行评估，提出启动应急响应的建议，分析信息安全事件的原因及造成的危害，为应急响应提供技术支持。

A.3　监测预警

A.3.1　监测

北京市某局在落实国家信息安全等级保护工作制度基础上，重点做好信息安全事件的风险评估和预警监测工作。

A.3.1.1　风险评估

北京市某局信息安全工作组负责本局政务信息系统的风险评估与控制的监督、检查、指导工作，指导关键信息基础设施运营使用管理单位开展风险评估工作，定期开展局内信息安全技术检查与自查，了解掌握分管领域内关键信息基础设施的风险状况，根据需要建立风险源管理系统，加强风险管理，提高关键信息基础设施安全防护水平。

A.3.1.2　安全监控

北京市某局信息安全监测系统建设、运营和管理工作由信息安全实施组负责，根据需要对局内信息系统、网站域名、流量数据进行持续性安全监测，定期进行日志分析、设备告警分析，及时发现网站及信息系统的安全隐患，修复安全漏洞，抑制信息安全事件的发生。

A.3.2　预警响应

如收到市级信息安全主管单位发布的信息安全预警信息，或针对某项重大活动本单位进行信息安全保障，信息安全工作组应依据发布的预警级别、保障级别，启动相应的应急预案，组织部署所属技术力量、应急救援队伍进行响应，进入应急状态。

A.4　应急响应

A.4.1　事件发现和汇报

根据各自职责分工，及时收集、分析、汇总网络与信息系统安全运行情况信息，一旦发生安全事件及时上报局信息安全实施组。

对于暂时无法判明等级的信息安全事件，立即将事件简要情况及联系人通过电话、邮件、传真等途径上报局信息安全领导小组，事件详细情况应在4小时内上报。

A.4.2 先期处置

信息安全事件发生后

（1）控制事态发展，防控蔓延。责任单位根据需要及时采取断网（拔网线）等技术措施及时控制事态发展，最大限度地降低事件危害。

（2）及时报告信息。在先期处置的同时要按照预案要求，及时向上级主管部门汇报。

（3）尽快分析事件发生原因，根据信息系统运行和承载业务情况，初步判断事件的影响、危害和可能波及的范围，提出应对措施建议。

（4）做好事件发生、发展、处置的记录和证据留存。在先期处置过程中应尽量保留安全日志信息、设备告警信息、路由配置信息、数据包信息等相关证据，采取手工记录、截屏、文件备份和影像设备记录等各种手段，对事件发生、发展、处置的过程、步骤、结果进行详细记录，尽可能保存原始证据，为事件处置、调查、处理提供客观证据。

（5）信息安全工作组在接报事件信息后及时掌握事件的发展情况，评估事件的影响和可能波及的范围，研判事件的发展态势。根据需要提供相应的技术支持。

A.4.3 基本响应

信息安全事件发生后，在先期处置基础上，由信息安全领导小组启动信息安全事件应急预案，及时掌握事件的发展情况，协调成员单位负责同志、部署应急力量，必要时配合市信息化主管单位组建现场指挥部应对信息安全突发事件的应急处置工作。

A.4.4 分级响应

对于特别重大（Ⅰ级）、重大(Ⅱ级)、较大(Ⅲ级)信息安全事件的应急响应按照《北京市网络与信息安全事件应急预案》要求执行，某局信息安全工作组配合市级信息化主管部门完成信息安全突发事件的现场应急处置工作。

A.4.4.1 IV级响应

信息安全领导小组启动IV级响应，统一指挥、协调、组织应急处置工作，局内各成员单位做好事件处置过程中的配合和协助工作，上级预案有特殊规定的，按照上级预案规定执行。

（1）启动指挥体系

信息安全组织机构进入应急状态，各成员保持24小时联络畅通，信息安全领导小组统筹协调事件应急处置工作。

（2）掌握事件动态

①跟踪事态发展。信息安全实施组及时将事态发展变化情况和处置进展情况报信息安全领导组。

②检查影响范围。信息安全工作小组及时了解主管范围内的其他信息系统是否受到事件的波及或影响，组织相关人员对事态进行研究，并根据需要组织对受到影响的系统进行核查。

③及时通报情况。信息安全工作小组负责汇总上述有关情况报信息安全领导小组及市级信息化部门。

（3）处置实施

①控制事态防止蔓延。信息安全实施组在信息安全领导小组的指挥下及时采取技术措施阻止事件蔓延，督促、指导相关运行单位有针对性地加强防范。

②消除安全隐患。信息安全实施组尽快分析事件发生原因，并根据原因有针对性地采取恢复措施，消除安全隐患，恢复受破坏网站正常运行。必要时请求市级信息安全技术支撑机构派遣应急队伍支援处置。

③时开展调查取证。信息安全工作组组织开展事件调查和责任评估工作，并将调查评估结果报信息安全领导小组。

④信息发布。信息安全领导小组根据事件应急的实际情况，形成各阶段工作简报，根据需要报告上级主管部门。

A.4.4.2 自管级响应

信息安全实施组启动自管级响应，按照相关预案进行应急处置，指挥协调所属技术力量进行事件处置工作；信息安全实施组负责将事件信息、处置进展情况及时向局信息安全工作小组报告。

A.4.4.3 响应升级

根据事态发展，当事件影响没有得到有效抑制，或人力物力资源不能够满足应急处置的需要、超出本单位的应急处置能力时，应及时提升响应等级，报上级业务主管部门，请求市级技术力量的协助。

A.4.5 应急结束

根据应急处置进展情况，信息安全工作小组会同专家组进行综合评估，在确认信息安全突发事件得到抑制、信息系统业务恢复正常，其衍生危害已经根除，安全隐患已在可控范围内的前提下，提出应急结束建议，并报相关部门批准。

Ⅳ级响应结束由信息安全工作组报信息安全领导小组审核后，由信息安全领导小组决定。

自管级响应结束由信息安全工作小组自行决定。

A.5 后期处置

A.5.1 系统重建

恢复重建工作按照“谁主管谁负责，谁运行谁负责”的原则，如有需要由信息安全工作小组负责组织制定恢复、整改或重建方案，报信息安全领导小组批准后，报行业主管及信息化主管部门审核实施。

自管级事件的恢复重建由局信息安全领导小组审核批准。

A.5.2 事件总结

信息安全事件应急处置工作结束后，信息安全工作组适时组织相关部门针对信息安全事件进行原因分析和责任调查，对突发事件的应急处置过程的处置效率和应急响应流程进行全面评估，并在20天内将评估报告报送信息安全领导小组。

信息安全实施小组据处置报告，总结经验教训，建立事件案例库，提出改进工作的要求和意见。

A.6 保障措施

A.6.1 技术支撑队伍

由信息安全工作小组选择若干经国家有关部门资质认可的，管理规范、服务能力较强的企事业单位作为信息安全的应急支援队伍，通过财政经费采购信息安全技术支持与应急服务；加强与市级信息安全保障机构的联系，确保必要时能够有效调动机关团体、企事业单位等保障力量，进行技术支援。

A.6.2 经费保障

局信息中心，将信息安全事件预防和应急工作列入年度经费预算。

A.7 宣传、培训和演练

A.7.1 宣传教育

局信息中心每年组织有关部门，通过信息安全通知公告、宣传展板制作、法律法规教育等形式开展宣传教育工作，普及局内人员的信息化知识，提升安全意识。

A.7.2 培训

局信息中心组织各有关单位，开展信息安全法规标准、风险评估、事件分析处置、容灾备份等方面的专业技术培训，使信息化工作人员熟练掌握相关技能。

A.7.3 演练

局信息中心每年不定期组织开展信息安全应急演练，模拟处置信息安全事件，提高实战能力，检验和完善预案。

A.8 预案管理

A.8.1 预案制定与解释

本预案由北京市某局信息安全实施组制定并负责解释。

A.8.2 预案审核

本预案由北京市某局信息安全领导小组组织审核。

A.8.3 预案修订

本预案原则上每年评估一次，根据实际情况适时修订。

A.8.4 预案实施

本预案自发布之日起正式实施。

A.9 附件

A.9.1 信息安全事件应急处置流程图

A.9.2 信息安全领导小组名单

A.9.3 信息安全工作组名单

A.9.4 信息安全实施组

A.9.5　信息系统及责任人列表

A.9.6　信息安全应急事件通报表

A.9.7　关键信息基础设施及IP列表

附 录 B
（资料性附录）
北京市某局网页篡改事件专项应急预案示例

B.1 总则

B.1.1 编制目的

为建立健全北京市某局信息安全应急机制，规范网页篡改事件中各单位工作责任，提高应对网页篡改事件的应急处理能力，最大程度地降低网页篡改事件造成的损害，保障某局各项业务的正常运行，特制定本预案。

B.1.2 编制依据

《北京市网络与信息安全事件应急预案》
《北京市某局信息安全事件总体应急预案》

B.1.3 适用范围

本预案针对北京市某局发生的网页篡改事件。

B.2 应急组织机构及职责

B.2.1 安全运行维护单位

在信息安全工作组指导下，负责监控内网安全事件，实施网络攻击信息系统应急处理方案，并在安全服务厂商、信息系统网络维护单位和各部门单位的协助下，实施应急处理工作，尽快恢复信息系统的正常运转。

B.2.2 第三方安全服务机构

在信息安全实施组的指导下，对网络攻击事件影响分析，给出处理解决方案，并负责网页篡改事件应急响应处理，协助安全运行维护单位解决安全维护工作。

B.2.3 信息系统网络维护单位

在信息安全工作组协调下，协助安全运行维护单位进行网页篡改事件的应急处理工作，提供必要的详细网络配置文档、服务器配置文档、业务数据配置清单。对被篡改的服务器数据进行数据备份，处置完成后对系统业务进行恢复。

B.2.4 各部门单位

各部门单位负责配合安全运行维护单位和信息系统网络维护单位进行网页篡改事件的应急处理工作，提供网络、系统配置文档和重要数据清单。

B.3 事件分类分级

B.3.1 事件分类

按照网页篡改事件的表现形式，本处置预案将网页篡改事件大致分为如下三类：

域名劫持事件：网站内容并非真正遭到篡改，而是域名指向被修改，用户访问时会发现网站内容异常。

图片/文字被篡改事件：网站页面的图片或者文字被篡改，用户通过浏览器可以看到被篡改的内容。

挂马/暗链事件：网站被篡改的内容用户通过浏览器不可见，但植入的代码会被执行。

B.3.2 事件分级

引用《北京市某局信息安全事件总体应急预案》分级标准。

B.3.3 应急启动

发生突发事件后，第一时间向信息安全工作组报告，通报相关人员，安全运行维护单位根据突发事件的分类分级标准分析事件的影响程度并预判事件级别，由信息安全工作小组初步确定事件级别，并进行先期应急处置。

如确定为Ⅳ级事件，报信息安全领导小组，并按照总体预案处置。

如为自管级事件，启用本预案响应流程。

B.4 应急响应

网页篡改是针对网站的较常见攻击方法，经现场确认网站发生网页篡改事件后，应立即通知应急响信息安全工作组，针对网页篡改事件展开应急处置工作，对于超出应急响应处理能力的工作，可以请求北京市信息安全应急队伍提供相应的技术支持。

网页篡改事件应急响应流程主要分为：事件通报、应急准备、分析确认、抑制根除、恢复运行和分析总结六个阶段。

B.4.1 事件通报

值班人员发现并确认网页篡改事件后，应立即对服务器进行物理隔离（断网），并将事件基本情况上报信息安全工作组，为减小社会影响，断网后可发布系统维护公告页面。

信息安全工作组接到报告后，立即组织开展应急响应，判断事件影响范围，并视情况通报上级主管单位和各相关处室。

B.4.2 应急准备

通知应急处置人员迅速及时赶赴现场开展事件处置，如发现不能处置此次事件，应及时请求北京市信息安全应急队伍协助进行处置。

准备事件分析所需软件和硬件，软件主要有日志分析工具，木马扫描工具，账号、进程、端口查看工具，挂马、暗链检查工具，硬件主要有应急笔记本和移动硬盘，笔记本要安装好上述软件。

B.4.3 分析确认

事发后应尽最大可能收集事件相关信息，鉴别事件性质，确定事件来源，以确定事件范围和评估事件带来的影响和损害。通过详细分析明确事件发生的原因和事件的经过，详细分析过程包括但不仅限于以下几个方面：

（1）分析网站访问日志，查找攻击者攻击的过程，包括实施的扫描、利用的漏洞及篡改的时间。

访问日志对于安全分析至关重要，因此要保护好访问日志，有条件的可以单独服务器存储，没条件要及时转储；

（2）利用专用工具扫描网站程序，查找攻击者植入的木马；

（3）利用工具查看服务器账户、进程、端口等信息，看攻击者是否留有其他后门；

（4）利用工具检查网站是否有挂马、暗链。

B.4.4 抑制根除

（1）修复相关漏洞，清除被植入木马，清除页面中的挂马、暗链；

（2）更换 WEB 服务器操作系统用户帐号密码和 WEB 服务应用程序用户帐号密码；

（3）部署防篡改软件或者防篡改设备，也可将 WAF 防护设备开启防篡改功能以达到防篡目的；

（4）妥善保存日志信息(单独服务器存储或者定期转储)，强化安全防范措施。

B.4.5 恢复运行

抑制根除完成后，恢复被篡改的网页，对网站服务器进行安全加固，并进行全面的安全检测，消除隐患后将网站重新投入使用，在上线后一定时期内严密监控信息系统，一旦发现异常及时处置。

B.4.6 分析总结

分析总结事件全部情况，形成报告上报信息安全领导小组。若涉及应急支援的，还需上报情况到市通信保障和信息安全应急指挥部办公室。

B.5 后期处置

B.5.1 跟踪后续处理

应急响应结束后，制定相应的系统加固方案，尽快恢复系统正常工作，运维单位加强安全监测，跟踪后续处理情况。

B.5.2 情况汇报和经验总结

应急处理结束后，安全运行维护单位和系统运维单位对事件处理情况进行总结并提交书面应急处置报告及安全加固报告，达到Ⅳ级事件级别的，需向信息安全领导小组汇报，信息安全工作组相关人员总结事件经验教训，以便以后更好的完成应急响应工作。

B.6 宣传、培训和演练

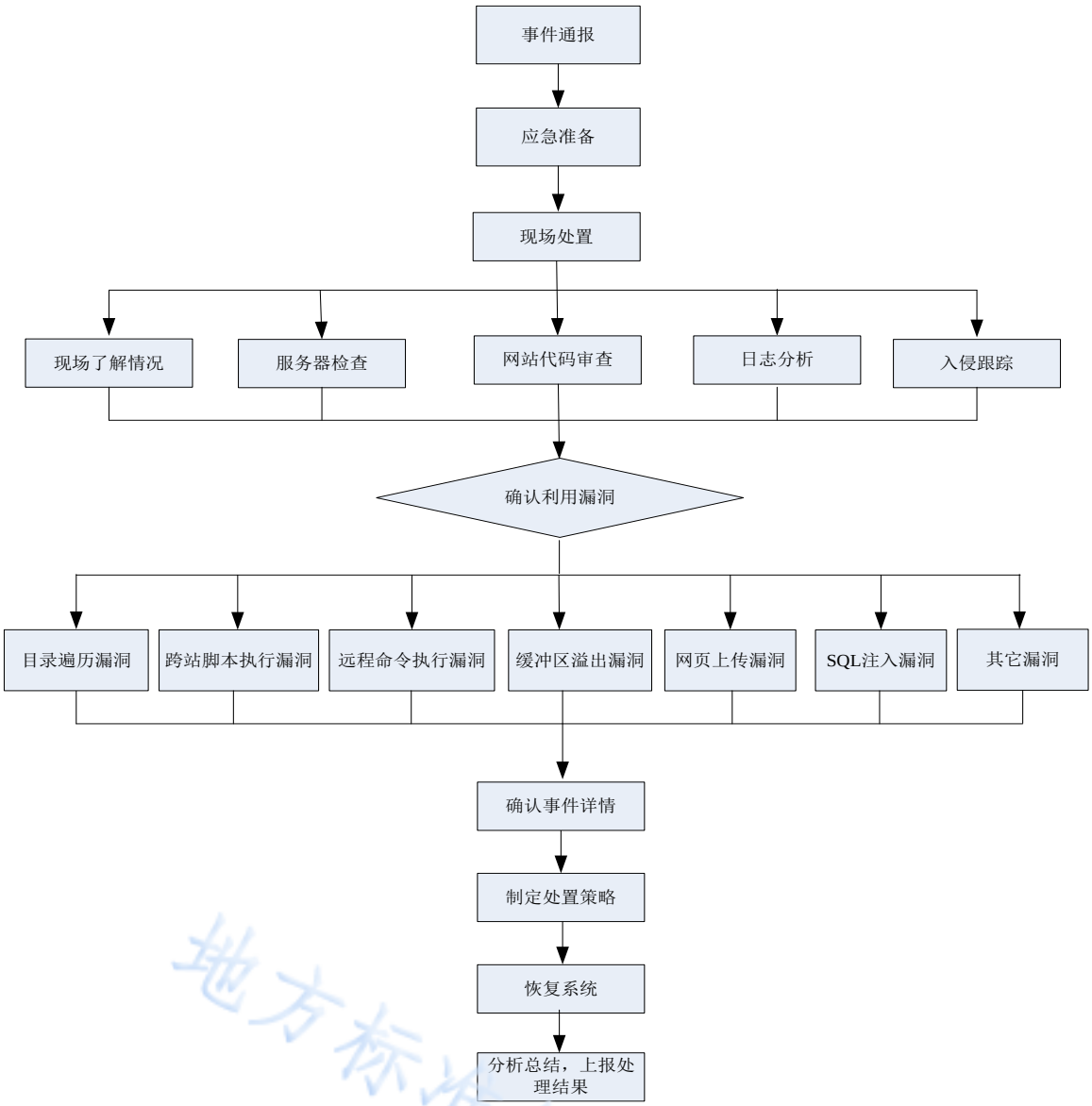
应加强对系统运维人员及其他相关人员的宣传教育工作，定期对有关人员进行技术培训，组织针对网页篡改事件的应急演练，确保专项应急预案的有效实施，不断提高应急处理的能力。

B.7 预案的管理与更新

本预案由网站信息化安全工作小组负责管理和更新，坚持周期性的评审，根据技术的发展、系统的变更、策略的更新及时对预案进行修订，修订后的预案经评审通过后发布生效。

B.8 附件

B.8.1　应急响应流程图



图B.1　应急响应流程图

B.8.2　责任单位成员名单

B.8.3　运维机构人员和联系方式

B.8.4　服务器及相关设备IP地址及物理位置

B.8.5　故障处置操作方法及流程

附 录 C
（资料性附录）
北京市某局网页篡改事件现场处置方案示例

C.1 应急准备阶段

C.1.1 保障对象识别

——网站基本情况：网站域名、IP 地址、责任单位、软件开发单位、硬件厂商、日常运维和安全运维单位等。
——网站开发运行环境：网站使用的开发平台和编程语言、网站服务器操作系统类型及版本、web 服务器软件类型及版本、后台数据库软件类型及版本、内容管理系统（CMS）相关情况等。
——网站外围支撑情况：网络安全域划分情况、防火墙访问控制策略设置、域名解析系统的部署和配置情况、安全监测和审计措施部署情况等。
——网站保障目标：若存在多个保障网站信息系统，应划分优先级，以确保重要保障网站能够优先获得足够的人力物力资源。

C.1.2 风险识别评估

根据网页篡改事件可能的路径，对安全风险进行识别与评估，了解已采取的安全措施及仍存在的安全风险。

表 C.1 安全风险识别评估表

可能攻击路径	要素	漏洞描述
网络层	域名系统	所有提供域名访问的网站
	互联网路由	所有需要经过互联网的网站
	局域网 ARP 劫持	使用 2 层交换机接入的网站
主机层	操作系统账号弱口令	所有网站
	操作系统的系统软件存在安全漏洞	所有网站
	操作系统上安装的应用软件存在安全漏洞	所有网站
应用层	应用代码安全漏洞	所有内容动态显示的网站
内容管理系统	内容管理系统账号弱口令	使用内容管理系统的网站
	内容管理系统所在主机操作系统存在安全问题	使用内容管理系统的网站
	内容管理系统的应用程序存在安全漏洞	使用内容管理系统的网站

C.1.3 应急资源准备

——网站服务器备份：对网站服务器硬件、网站源代码、数据库等进行备份。
——应急处置工作：日志分析工具、网站代码对比工具、漏洞扫描工具、恶意进程检查工具、数据包分析工具等。

C.2 事件确认与应急处置阶段

步骤一：判断是否由于遭受域名劫持造成的“伪”篡改。用 ping 命令实现，若 ping 命令返回的 IP 地址信息与实际不一致，则通过正确的 IP 地址访问受害网站，检查网站内容是否正常。当确定是由于域名系统遭受攻击而造成域名解析被错误定向，则应及时修改域名服务器的相关解析数据，并检查域名服务器是否遭受攻击。对于大型门户网站，应尽快协调运营商，及时将各重要公共域名解析服务器中错误的域名解析缓存记录清除，以降低事件造成的影响。

步骤二：判断是否由于遭受局域网 ARP 攻击造成网页被“伪”篡改。从两个方面进行检查，一是直接本地登录网站所在服务器，从本地访问网站，检查网页内容是否被篡改；二是使用网络协议分析工具，检查局域网是否存在异常的 ARP 数据报文。当确定局域网 ARP 攻击是造成网页篡改的原因时，应定位局域网中实施 ARP 攻击的主机。

步骤三：分析日志，确认攻击方式。通过分析 web 访问日志、网络审计日志、设备记录日志等，可以对通过 web 应用系统实施攻击进行准确判断，确定网页篡改的方式，有针对性地从管理和技术上采取措施，避免事件再次方式。

步骤四：检查漏洞。当因日志信息保存不完整或无法从日志中获知网页篡改的途径时，则只能通过检查漏洞来尝试处置。漏洞检查的范围应包括主机系统安全漏洞、网站应用代码安全漏洞、数据库软件安全漏洞等。对发现的各类安全漏洞进行必要的修补后，更换后台登陆密码后重新恢复网站系统运行并加强监测，以防止事件重复发生。

步骤五：综合分析。当未发现任何已知的安全漏洞，或在完成漏洞修补后篡改事件重复发生，则本次事件可能是利用未知的安全漏洞实施，需要进行更加全面的综合分析。

C.3 事后期处置

即使准确定位了事件发生的技术原因与实施路径，也很难完全在原有系统上根除，当攻击者实施攻击并获得了系统控制权限后，是否安装了后门程序难以准确掌握，尤其是系统级（rootkit）的后门程序更难以判断。因此还需进行一系列的事后处置工作，具体包括：

——根据入侵者可能使用的技术手段制订相应的安全加固方案，完善相关的安全机制等。

——对应用防火墙和安全防护系统作相应的配置调整使之自动检测和阻止该类攻击的再次发生(视具体情况而定)。

——对整个网站系统进行重新部署，包括重新安装操作系统、优化软件架构、重新部署应用系统等。

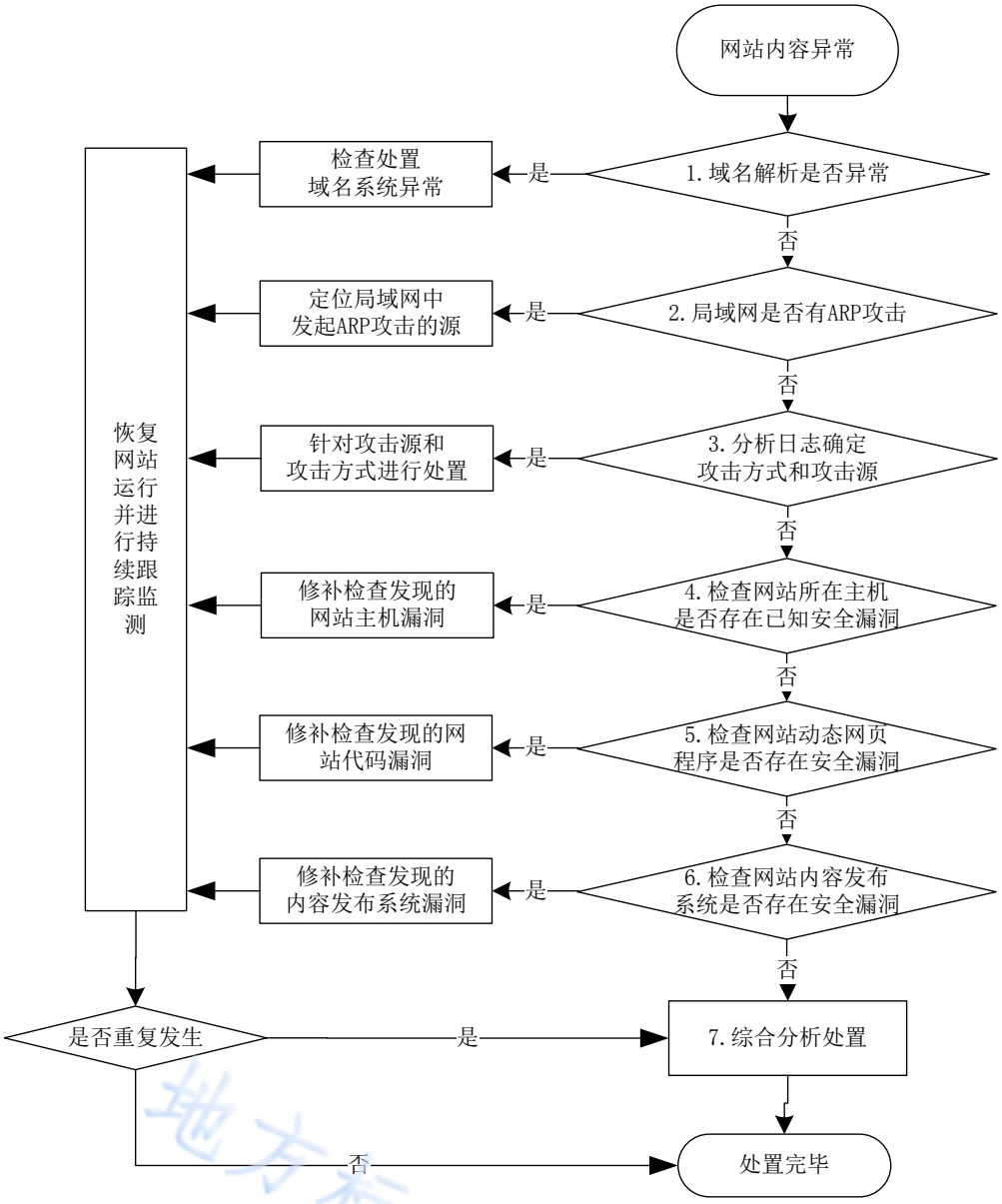
——进行全面的安全检测，包括源代码安全审查、安全漏洞的修复、禁用不必要的服务和端口等。

——更换所有相关口令，包括操作系统、数据库、中间件、应用系统(管理)等。

——恢复经过安全加固后的被入侵主机的网络连接，使系统重新上线，并进行严密监控。

C.4 附件

C.4.1 网页篡改事件分析处置流程图



图C.1　网页篡改事件分析处置流程图

C.4.2　机房平面图

C.4.3　网络拓扑结构图

C.4.4　服务器及相关设备IP地址及物理位置

C.4.5　木马后门检测方法及操作手册

C.4.6　日志分析操作手册

C.4.7　恶意进程排查操作手册