互联网网络安全信息通报实施办法

索引号：ZJJX-05-01-201212-00003
发布机关：工信部
文号：工信部保[2009]156 号
发布日期：2009-05-05

各省、自治区、直辖市通信管理局、国家计算机网络应急技术处理协调中心、中国互联网络信息中心、政府和公益机构域名注册管理中心、部电信研究院、中国互联网协会、中国电信集团公司、中国移动通信集团公司、中国联合网络通信集团有限公司、其他相关单位：

为规范通信行业互联网网络安全信息通报工作，制定《互联网网络安全信息通报实施办法》，现印发给你们，请遵照执行。

联系人：付景广 010－66022774

二〇〇九年四月十三日

互联网网络安全信息通报实施办法

第一条 为规范通信行业互联网网络安全信息通报工作，促进网络安全信息共享，提高网络安全预警、防范和应急水平，依据《互联网网络安全应急预案》制定本办法。

第二条 本办法适用于通信行业互联网等 IP 网络和系统的网络安全信息通报（以下简称信息通报）工作。

第三条 工业和信息化部指导、监督、检查全国信息通报工作，工业和信息化部通信保障局（以下简称通信保障局）负责信息通报具体工作。省、自治区、直辖市通信管理局（以下简称通信管理局）指导、监督、检查本行政区域内信息通报工作。

第四条 通信管理局、基础电信业务经营者、跨省经营的增值电信业务经营者、国家计算机网络应急技术处理协调中心（以下简称 CNCERT）、互联网域名注册管理机构、互联网域名注册服务机构、中国互联网协会为信息报送单位。

第五条 通信保障局委托 CNCERT 收集、汇总、分析、发布互联网网络安全信息（以下简称信息）。

第六条 信息报送应遵循及时、客观、真实、准确、完整的原则，不得迟报、谎报、瞒报、漏报。

第七条 基础电信业务经营者、跨省经营的增值电信业务经营者、CNCERT、互联网域名注册管理机构、互联网域名注册服务机构应建立并完善本单位信息监测机制，提高监测能力，自主监测涉及

本单位管理范围内的信息。

第八条 信息报送单位应制定并完善本单位信息通报机制，明确负责信息通报工作的主管领导和承担信息通报工作的责任部门、负责人和联络人，及时汇总本单位内部不同部门、不同渠道掌握的网络安全信息。信息报送单位应将本单位信息通报机制报通信保障局备案。

第九条 各单位需要报送的信息项目见附件一，通信保障局负责对项目内容进行调整。

第十条 报送的信息分为事件信息和预警信息。

事件信息是指已经发生的网络安全事件信息。

预警信息是指存在潜在安全威胁或隐患但尚未造成实际危害和影响的信息，或者对事件信息分析后得出的预防性信息。

第十一条 事件信息分为特别重大、重大、较大、一般共四级。预警信息分为一级、二级、三级、四级，分别用红色、橙色、黄色、蓝色标识，一级为最高级。具体分级规范见附件二，通信保障局负责对分级规范进行修订。

第十二条 信息报送单位应按照本办法第十条、第十一条规定对信息进行分类、分级，并根据本办法的相应规定报送信息。

基础电信业务经营者集团公司负责汇总、核实、报送省级分公司/子公司的信息。省级分公司/子公司将信息同时抄送当地通信管理局。

第十三条 对于特别重大、重大事件信息以及一级、二级预警信

息，信息报送单位应于2小时内向通信保障局及相关通信管理局报告，抄送CNCERT。

对于较大事件信息以及三级预警信息，信息报送单位应当于4小时内向相关通信管理局报告，抄送CNCERT；对于跨省（自治区、直辖市）的较大事件信息，应同时向通信保障局报告。

对于一般事件信息，信息报送单位应按月及时汇总，于次月5个工作日内报送 CNCERT，抄送相关通信管理局；对于四级预警信息，信息报送单位应当于发现或得知预警信息后5个工作日内报送CNCERT，抄送相关通信管理局。

第十四条 事件信息报送的内容应包括：

（一）事件发生单位概况；

（二）事件发生时间；

（三）事件简要经过；

（四）初步估计的危害和影响；

（五）已采取的措施；

（六）其他应当报告的情况。

第十五条 预警信息报送的内容应包括：

（一）信息基本情况描述；

（二）可能产生的危害及程度；

（三）可能影响的用户及范围；

（四）截至信息报送时，已知晓该信息的单位/人员范围；

（五）建议应采取的应对措施及建议。

第十六条 事件发生后出现新情况的，信息报送单位应当及时补报。

CNCERT 在接到预警信息后，应立即组织对预警信息进行跟踪、分析，有重要情况应及时向通信保障局报告。

第十七条 通信保障局根据信息性质、内容、紧急程度等，必要时组织相关单位、专家对信息进行研判。

第十八条 各单位应以书面形式报送信息，并加盖单位公章。紧急情况可以先电话联系，后补书面报告。

第十九条 对于特别重大、重大、较大事件信息以及一级、二级、三级预警信息，由通信保障局审核后，根据有关规定直接或委托 CNCERT 及时通告相关单位、人员或互联网用户，并抄送各通信管理局。

对于一般事件信息，由 CNCERT 负责汇总、分析全部信息，于次月 10 个工作日内将当月信息向通信保障局报送，向相关单位、人员通告，并抄送各通信管理局；对于四级预警信息，由 CNCERT 根据实际情况及时向相关单位、人员通告，并抄送各通信管理局。

第二十条 事件信息通告内容主要包括：事件统计情况、造成的危害、影响程度、态势分析、典型案例。

预警信息通告内容主要包括：受影响的系统、可能产生的危害和危害程度、可能影响的用户及范围、建议应采取的应对措施及建议。

第二十一条 信息报送单位应将本单位信息通报工作主管领导，

责任部门负责人、联系人、联系方式报送通信保障局，抄送CNCERT。以上信息发生变更，应在3个工作日内报送变更情况。

第二十二条 通信保障局建立会商制度，通报当前网络安全情况，与相关单位和专家研讨网络安全形势、网络安全问题及其应对策略等。

第二十三条 CNCERT应与网络安全研究机构、网络安全技术支撑单位、非经营性互联单位、网络安全企业、国际网络安全组织等广泛合作，积极拓展网络安全信息获取渠道。

第二十四条 国家网络安全保障专项工作对信息通报工作另有规定的，从其规定。

第二十五条 通信管理局应参照本办法制定本行政区域信息通报管理办法。

第二十六条 本办法自2009年6月1日起实施。

附件一：

信息报送项目

（一）基础电信业务经营者

1、本单位提供互联网接入服务的普通电信用户、专线用户、重要信息系统用户业务发生阻断、拥塞等异常情况。

2、本单位 IP 基础网络设施，包括互联网国际设施、国内互联网设备和链路、IDC 等发生瘫痪、阻断等异常情况。

3、本单位域名解析服务系统发生瘫痪、解析异常、域名劫持等异常情况。

4、本单位网上营业厅、门户网站、移动 WAP 类业务，或与互联网相连的网络和系统发生系统瘫痪、阻断、用户数据丢失等异常情况。

5、影响互联网业务正常运营、影响用户正常访问互联网、造成重大社会影响和经济损失等异常情况。

6、本单位网内漏洞等网络安全隐患及处置情况。

7、本单位网内发生拒绝服务攻击或其他流量异常事件情况。

8、本单位网内木马和僵尸网络、病毒等恶意代码传播情况。

9、本单位网内路由系统出现的路由劫持情况（路由劫持指若同一 IP 地址前缀有多个自治系统为宣告者，且自治系统之间无隶属关系或未得到该 IP 地址前缀的授权，则判定为域间路由劫持）。

10、本单位垃圾邮件监测、预警和处置情况。

11、获知的由本单位提供服务的重要信息系统用户内部发生的网

络安全异常情况。

12、通过各种渠道获得的其它信息。

（二）互联网域名注册管理、服务机构

1、本单位域名系统解析服务异常等情况，包括系统稳定性、解析成功率、响应时间、解析数据和数据库等方面出现的异常情况。

2、网页挂马、网络仿冒、域名劫持等网络安全事件。

3、域名系统相关的系统漏洞等网络安全风险信息及处置情况。

4、可疑域名或域名注册行为等情况。

5、通过各种渠道获得的其它信息。

（三）增值电信业务经营者（IDC、门户网站、搜索引擎服务提供商等）

1、IDC：

（1）IDC 网络出口链路中断或拥塞。

（2）由 IDC 提供服务的网站或托管主机感染病毒、木马和僵尸恶意代码，或被利用实施网络攻击、网络仿冒等网络安全事件的情况。

（3）通过各种渠道获得的其它信息。

2、门户网站、搜索引擎服务提供商等：

（1）网络接入链路中断或拥塞。

（2）系统瘫痪、遭到入侵或控制、应用服务中断等。

（3）用户数据被篡改、丢失等。

（4）垃圾邮件发现和处置情况。

（5）系统感染恶意代码情况。

（6）网页篡改、网络仿冒等情况。

（7）通过各种渠道获得的其它信息。

（四）中国互联网协会

1、垃圾邮件相关情况。

2、互联网用户反映的影响互联网业务的重要网络安全情况。

3、通过各种渠道获得的其它信息。

（五）CNCERT

1、本单位自主监测到的信息。

2、各信息报送单位报送的信息。

3、通过国际、国内合作单位等渠道获得的信息。

4、通过各种渠道获得的其他信息。

（六）通信管理局

1、重点报送本行政区域内或与本行政区域相关的重要网络安全信息。

2、通过各种渠道获得的其他信息。

附件二：

信息分级规范

一、预警信息分级

1、一级（红色）预警信息：可能导致发生特别重大网络安全事件的信息为一级预警信息。

2、二级（橙色）预警信息：可能导致发生重大网络安全事件的信息为二级预警信息。

3、三级（黄色）预警信息：可能导致发生较大网络安全事件的信息为三级预警信息。

4、四级（蓝色）预警信息：可能导致发生一般网络安全事件的信息为四级预警信息。

二、事件信息分级

分类	对象	特别重大事件	重大事件	较大事件	一般事件
IP 业务	互联网接入（含宽带、窄带接入，固定、移动或无线接入）	基础电信业务经营者本单位全国网内 100 万以上互联网接入用户无法正常访问互联网 1 小时以上。	基础电信业务经营者本单位全国网内 10 万以上互联网接入用户无法正常访问互联网 1 小时以上。	基础电信业务经营者本单位某省、直辖市、自治区网内 5 万以上互联网接入用户无法正常访问互联网 1 小时以上。	基础电信业务经营者本单位某省、直辖市、自治区网内 1～5 万互联网接入用户无法正常访问互联网 1 小时以上。
	专线接入	N/A	基础电信业务经营者本单位专线接入业务 500 端口以上阻断 1 小时以上。	基础电信业务经营者本单位专线接入业务 100 端口以上阻断 1 小时以上。	基础电信业务经营者本单位专线接入业务 20 端口以上阻断 1 小时以上。

	重要信息系统数据通信	N/A	造成某个全国级重要信息系统用户数据通信中断 1 小时以上。	造成某个省级重要信息系统用户数据通信中断 1 小时以上。	造成某个地市级重要信息系统用户数据通信中断 1 小时以上。
基础 IP 网络	国际互联	50％以上国际互联带宽电路阻断 1 小时以上。	30％以上国际互联带宽电路阻断 1 小时以上。	10％以上国际互联带宽电路阻断 1 小时以上。	国际互联设备、电路阻断，但未造成上述严重后果。
	国内骨干网互联	某个全网直连点 1 个以上互联单位方向全阻 1 小时以上。	某全网直连点 1 个互联单位方向网间直连（或某个交换中心）全阻 1 小时以上。	交换中心 1 个互联单位方向全阻 1 小时以上。	直连设备、电路阻断，但未造成上述严重后果。
	运营单位 IP 网	2 个以上省网（或 2 个以上 3.2 级以上城域网）脱网或严重拥塞 1 小时以上。	1 个省网（或 1 个以上 3.1 级以上城域网）脱网或严重拥塞 1 小时以上。	1 个以上城域网（3.1 级以下）脱网或严重拥塞 1 小时以上。	IP 骨干网重要节点或链路阻断，但未造成上述严重后果。
	IDC	N/A	3.1 级以上 IDC 全阻或严重拥塞 1 小时以上。	2 级 IDC 全阻或严重拥塞 1 小时以上。	其它 IDC 全阻或严重拥塞 1 小时以上。
域名系统	国际根镜像和 gTLD 镜像服务器	N/A	N/A	国际根和通用顶级域名镜像服务器解析服务瘫痪。	N/A
	国家顶级域名 (.CN)	国家域名解析系统瘫痪，对全国互联网用户的域名解析服务失效。	国家域名解析系统半数及以上顶级节点解析成功率低于 50％或解析响应时间高于 5 秒；国家域名顶级节点解析数据缺失或出错超过 0.1%；国家域名解析	国家域名解析系统半数以下顶级节点解析成功率低于 50%或解析响应时间高于 5 秒；国家域名顶级节点解析数据缺失或出错超	国家域名系统注册服务性能下降或查询服务不可用。

			系统重点域名相关解析数据出错。	过0.01%；国家域名系统注册服务不可用4小时以上。	
	域名注册服务机构管理的权威域和递归解析服务器	1家或多家重点注册服务机构域名解析服务瘫痪。	1家或多家重点注册服务机构域名解析服务性能下降，解析成功率低于50%或解析响应时间高于5秒,或解析数据缺失或出错，超过1%。注册服务机构域名系统核心数据库丢失或非正常修改，并影响到国家域名核心数据库导致产生国家顶级域名重大事件。	1家或多家注册服务机构域名解析服务性能下降，解析成功率低于80%或解析响应时间高于5秒,或解析数据缺失或出错，超过0.1%。	1家或多家注册服务机构域名注册系统服务不可用。
	基础和增值运营企业的权威域域名解析服务器	N/A	重点域名解析权威服务器瘫痪1小时以上。	N/A	N/A
	基础运营企业的递归服务器	N/A	为一个或多个省份提供服务的递归服务器瘫痪1小时以上。	N/A	N/A

基础电信运营企业网上营业厅、移动WAP业务、门户网站		系统瘫痪或故障，造成业务中断1个小时以上，或造成100万以上用户数据丢失、泄漏。	系统瘫痪或故障，造成业务中断1个小时以下，或造成10万以上用户数据丢失、泄漏。	系统瘫痪或故障，造成业务中断或造成1万以上用户数据丢失、泄漏。	系统瘫痪或故障，但未造成上述严重后果。
公共互联网环境	计算机病毒事件、蠕虫事件、木马事件、僵尸网络事件	涉及全国范围或省级行政区域的大范围病毒和蠕虫传播事件，或单个木马和僵尸网络规模达100万个以上IP，对社会造成特别重大影响。	涉及全国范围或省级行政区域的大范围病毒和蠕虫传播事件，或同一时期存在一个或多个木马和僵尸网络总规模达50万个以上IP，对社会造成重大影响。	涉及全国范围或省级行政区域的大范围病毒和蠕虫传播事件，或同一时期存在一个或多个木马和僵尸网络总规模达10万个以上IP，对社会造成较大影响。	涉及全国范围或省级行政区域的大范围病毒和蠕虫传播事件、木马和僵尸网络事件等，对社会造成一定影响，但未造成上述严重后果。
	域名劫持事件、网络仿冒事件、网页篡改事件	N/A	发生涉及重点域名、重要信息系统网站的域名劫持、仿冒、篡改事件，导致10万以上网站用户受影响，或造成重大社会影响。	发生涉及重点域名、重要信息系统网站的域名劫持、仿冒、篡改事件，导致1万以上网站用户受影响，或造成较大社会影响。	其他域名劫持、网络仿冒、网页篡改事件，造成一定社会影响，但未造成上述严重后果。

	网页挂马事件	发生涉及重要信息系统网站、重要门户网站的网页挂马事件，受影响网站用户达100万人以上，造成特别重大社会影响。	发生涉及重要信息系统网站、重要门户网站的网页挂马事件，受影响网站用户达10万人以上，造成重大社会影响。	发生涉及重要信息系统网站、重要门户网站的网页挂马事件，受影响网站用户达1万人以上，造成较大社会影响。	其他网页挂马事件，但未造成上述严重后果。
	拒绝服务攻击事件	N/A	发生涉及全国级重要信息系统的拒绝服务攻击，造成重大社会影响。	发生涉及省级重要信息系统的拒绝服务攻击，造成较大社会影响。	其他拒绝服务攻击，造成一定社会影响。
	后门漏洞事件、非授权访问事件、垃圾邮件事件及其他网络安全事件	N/A	发生涉及全国级重要信息系统的后门漏洞事件、非授权访问事件、垃圾邮件事件及其他网络安全事件，造成重大社会影响。	发生涉及省级重要信息系统的后门漏洞事件、非授权访问事件、垃圾邮件事件及其他网络安全事件，造成较大社会影响。	发生的后门漏洞事件、非授权访问事件、垃圾邮件事件及其他网络安全事件，造成一定社会影响。

〔注〕：

1、严重拥塞是指链路时延>110ms 或丢包率超过 8%。

2、本办法中重要信息系统指政府部门、军队以及银行、海关、税务、电力、铁路、证券、保险、民航等关系国计民生的重要行业使用的信息系统。

3、“信息分级规范”中所称“以上”包括本数，所称“以下”不包括本数。

附件三：

联系方式

（1）通信保障局

主管领导： 熊四皓 010-66069910

联 系 人： 闫宏强 010-66069895，13011881107

付景广 010-66022774，13701353949

（2）工业和信息化部 24 小时值班电话：010-66014249

（3）CNCERT

主管领导： 云晓春 010-82990501

联 系 人： 孙蔚敏 010-82990103 13911218086

何世平 010-82990286 13810058717

CNCERT 24 小时值班电话： 010-82990999

邮件： yteam@cert.org.cn