

备案号: CNCA/CTS 0050-2007

信息安全产品认证技术规范

ISCCC TS001-2007

信息技术 信息安全 网站恢复产品认证技术规范

Technical specifications for website recovery products certification

2008-03-05 发布

2008-03-05 实施

中国信息安全认证中心 发布

目 次

前 言.....	1
1 范围.....	2
2 规范性引用文件.....	2
3 术语和定义.....	2
4 系统功能要求.....	3
4.1 运行平台.....	3
4.2 检测时间间隔管理.....	4
4.3 监控目录/文件管理.....	4
4.4 界面.....	4
4.5 增量备份.....	4
5 性能评价.....	4
5.1 监控响应时间.....	4
5.2 篡改恢复时间.....	4
5.3 稳定性.....	4
5.4 资源占用.....	4
5.5 网络影响.....	4
6 安全要求.....	4
6.1 静态网页文件自动恢复功能.....	4
6.2 动态脚本文件自动恢复功能.....	5
6.3 网页目录自动恢复功能.....	5
6.4 报警功能.....	5
6.5 审计日志功能.....	6
6.6 抵御已知攻击.....	6
6.7 管理功能.....	6
6.8 备份文件的安全存储及安全传输.....	7
6.9 自身审计数据生成.....	7
7 保证要求.....	7
7.1 交付与运行保证.....	7
7.2 指导性文档.....	7
7.3 测试保证.....	8
7.4 脆弱性分析保证.....	9
7.5 生命周期支持.....	9
8 网站恢复产品安全技术要求的等级划分.....	9
附录 A.....	12
参考文献.....	14

前 言

本技术规范是网站恢复产品认证技术规范。

本技术规范参考了网站恢复产品相关技术规范制定。

本技术规范由中国信息安全认证中心（ISCCC）提出并归口。

本技术规范起草单位：中国信息安全认证中心。

网站恢复产品认证技术规范

1 范围

本技术规范规定了网站恢复产品技术要求。

本技术规范适用于第三方测评机构对网站恢复产品的检测。网站恢复产品的设计和实现也可参照使用。

2 规范性引用文件

下列文件中的条款通过本技术规范的引用而成为本技术规范的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本技术规范，然而，鼓励根据本技术规范达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本技术规范。

GB/T18336.1 信息技术 安全技术 信息技术安全性评估准则 第1部分：简介和一般模型。

GB/T18336.2 信息技术 安全技术 信息技术安全性评估准则 第2部分：安全功能要求。

GB/T18336.3 信息技术 安全技术 信息技术安全性评估准则 第3部分：安全保证要求。

3 术语和定义

GB/T 5271.8—2001和GB/T 18336确立的术语和定义适用于本技术规范。

下列术语和定义适用于本技术规范。

3.1

网站恢复 website recovery

网站恢复是指对受保护的静态网页文件、动态脚本文件及目录的未授权更改及时地进行自动恢复的过程。

3.2

网站恢复产品 website recovery product

网站恢复产品是用以实现网站恢复的软件或软硬件组合。

3.3

网站数据 website data

与网站对外发布的网页内容相关的数据。

3.4

授权管理员 authorized administrator

可管理网站恢复产品的授权用户。

3.5

网站备份数据 backup for website data

得到授权管理员认可的网站数据副本。

3.6

本地服务器 local server

网站系统所在的服务器。

3.7

远程服务器 remote server

与本地服务器通过网络相连接的非本地服务器。

3.8

静态网页 static web page

保存在本地服务器上，但不会在本地服务器上运行，其内容不会因访问条件的不同而发生变化的一个或一组文件。

3.9

动态网页 dynamic web page

保存并运行于本地服务器上，其内容在本地服务器上动态生成，能根据访问条件的不同而发生变化的一个或一组文件。

3.10

动态脚本文件 dynamic script file

保存并运行于本地服务器上，用以支持生成动态网页内容的文件。其内容一般是一组脚本语言代码。

4 系统功能要求

4.1 运行平台

4.1.1 操作系统

网站恢复产品的所有功能能够在指定操作系统平台上正常运行。例如，支持Windows、Linux等。

4.1.2 Web 服务器

网站恢复产品的所有功能能够配合指定的Web服务器正常运行。例如，支持IIS、J2EE (Weblogic/Websphere) 等。

4.1.3 网页发布系统

安装网站恢复产品后，应当不影响网站原有的网页发布系统。

4.1.4 检测优先级

若网站恢复产品使用定时检测方式 (A.2.1.1) 进行监测，应当允许用户对待检测对象设置不同的优先级。

4.2 检测时间间隔管理

若网站恢复产品使用定时检测方式（A.2.1.1）进行监测，应当允许用户对检测时间间隔进行配置。

4.3 监控目录/文件管理

用户可增加或撤消被监控的目录/文件。

4.4 界面

网站恢复产品应为用户提供友好的操作界面。

4.5 增量备份

当网站数据授权更新后，仅对上次备份以来数据对象的变化进行备份，以形成新的网站备份数据。

5 性能评价

5.1 监控响应时间

监控响应时间是指发现网站数据被未授权更改到对其进行报警所需的时间。

该指标由监控策略、比较方式、被保护对象的属性等因素决定，时间越短，保护效率越高。

5.2 篡改恢复时间

篡改恢复时间是指发现网站数据被未授权更改到对其进行自动恢复所需的时间。

该指标由网站备份数据存放位置、传输带宽、被保护对象属性等因素决定，时间越短，保护效率越高。

5.3 稳定性

安装网站恢复产品后，网站恢复产品以及相应的网站系统均能稳定运行。稳定性可用平均无故障率等指标进行评价。

5.4 资源占用

安装网站恢复产品后，对网站系统所在的服务器资源（如CPU、内存空间和存储空间），不应长时间固定或无限制占用，不应影响网站系统授权的用户登录和资源访问。资源占用可用CPU占用率、内存占有率、存储空间占有率等指标进行评价。

5.5 网络影响

若网站恢复产品采用远程监控方式（A.2.1），不对原网络正常通讯产生长时间固定影响。网络影响可用带宽占用率等指标进行评价。

6 安全要求

6.1 静态网页文件自动恢复功能

网站恢复产品能对受保护静态网页文件的未授权更改进行识别,并能用备份文件进行自动恢复。即:

- a) 静态网页文件未授权增加的恢复;
- b) 静态网页文件未授权删除的恢复;
- c) 静态网页文件未授权修改(包括文件属性修改、重命名、移动等)的恢复。

6.2 动态脚本文件自动恢复功能

网站恢复产品能对受保护动态脚本文件的未授权更改进行识别,并能用备份文件进行自动恢复。即:

- a) 动态脚本文件未授权增加的恢复;
- b) 动态脚本文件未授权删除的恢复;
- c) 动态脚本文件未授权修改(包括文件属性修改、重命名、移动等)的恢复。

6.3 网页目录自动恢复功能

网站恢复产品能识别对受保护网页目录的未授权破坏进行识别,并能用备份目录进行自动恢复。即:

- a) 网页目录未授权增加的恢复;
- b) 网页目录未授权删除的恢复;
- c) 网页目录未授权修改(包括目录属性修改、重命名、移动等)的恢复。

6.4 报警功能

6.4.1 应对以下事件实时报警

- a) 对受保护网页文件的未授权增、删、改的报警;
- b) 对受保护网页目录及属性的未授权增、删、改的报警;
- c) 对监控保护进程异常关闭的报警。

6.4.2 报警信息的数据格式

报警信息数据项的内部数据结构定义可参考如下:

序号	名称	类型	长度
1	事件发生日期	字符	8
2	事件发生时间	字符	6
3	事件类型	字符	30
4	备注	字符	100

注:若事件为6.4.1 a)、b),则应在“备注”项中指出受破坏文件或目录的位置。

6.4.3 报警方式

应提供适当的报警方式。（例如：（1）E_mail报警；（2）以声音或屏幕提示等形式向指定计算机发送警告信息。）

6.5 审计日志功能

6.5.1 可审计事件

- a) 对受保护网页文件进行增、删、改和恢复的日志；
- b) 对受保护网页目录进行增、删、改和恢复的日志；
- c) 监控保护服务的开启和关闭的日志。

6.5.2 审计信息的数据格式

审计信息数据项的内部数据结构定义可参考如下：

序号	名称	类型	长度
1	事件发生日期	字符	8
2	事件发生时间	字符	6
3	事件类型	字符	30
4	备注	字符	100

注：若事件为6.4.1 a)、b)，则应在“备注”项中指出受破坏文件或目录的位置。

6.5.3 审计跟踪管理

授权管理员应能创建、存档、删除和清空审计记录。

6.5.4 可理解的格式

该类产品应使存储于永久性审计记录中的所有审计数据为人所理解，并可按条件或条件组合查询。

6.6 抵御已知攻击

应能抵御已知手段攻击，例如，木马、病毒。

6.7 管理功能

6.7.1 授权管理员身份鉴别

网站恢复产品应保证只有授权管理员能使用产品的管理功能。对授权管理员应进行身份鉴别。

6.7.2 授权管理员权限

网站恢复产品应保证授权管理员有下列权限：

- a) 授权管理员属性修改（更改口令等）；
- b) 启动、关闭监控保护服务；

- c) 增加或撤消对所有受保护目录的监控；
- d) 授权管理员对网页内容进行授权更新。

6.7.3 管理信息传输安全

若提供远程管理功能，应能对远程管理信息（例如，登录信息和会话）进行保密传输。

6.8 备份文件的安全存储及安全传输

- a) 仅授权管理员可指定备份端，用户可备份指定文件及目录到备份端；
- b) 备份端应对登录用户进行身份鉴别，实现备份文件在备份端的安全存储；
- c) 用备份文件对受保护网页文件的未授权更改进行恢复时，应保证备份文件的安全传输；
- d) 应提供网页内容授权更新后的及时备份。

6.9 自身审计数据生成

产品应对与自身安全相关的以下事件生成审计记录：

- a) 对产品进行操作的尝试，如关闭审计功能或子系统；
- b) 授权管理员的登录和退出；
- c) 对安全策略进行更改的操作；
- d) 读取、修改、破坏审计跟踪数据的尝试；
- e) 因鉴别尝试不成功的次数超出了设定的限值，导致的会话连接终止；
- f) 对管理角色进行增加，删除和属性修改的操作；
- g) 对其他安全功能配置参数的修改（设置和更新），无论成功与否。

7 保证要求

7.1 交付与运行保证

- a) 开发者应使用一定的交付程序交付网站恢复产品，并将交付过程文档化。
- b) 交付文档应描述在给用户方交付网站恢复产品的各版本时，为维护安全所必需的所有程序。
- c) 开发者应提供文档说明网站恢复产品的安装、生成、启动和日志生成的过程。

7.2 指导性文档

7.2.1 管理员指南

- a) 开发商应提供针对产品管理员的管理员指南。
- b) 管理员指南应描述管理员可使用的管理功能和接口。
- c) 管理员指南应描述怎样以安全的方式管理产品。

- d) 对于在安全处理环境中必须进行控制的功能和特权，管理员指南应提出相应的警告。
- e) 管理员指南应描述所有对与网站恢复产品的安全操作有关的用户行为的假设。
- f) 管理员指南应包含安全功能如何相互作用的指导。
- g) 每一种与管理功能有关的安全相关事件，包括对安全功能所控制的实体的安全特性进行的改变。
- h) 所有与系统管理员有关的IT环境的安全要求。
- i) 管理员指南应与为评价而提供的其他所有文件保持一致。

7.2.2 用户指南

- a) 开发商应提供用户指南。
- b) 用户指南应描述非管理员用户可用的功能和接口。
- c) 用户指南应包含使用产品提供的的安全功能和指导。
- d) 用户指南应描述用户可获取但应受安全处理环境控制的所有功能和权限。
- e) 用户指南应清晰地阐述产品安全运行中用户所必须负的职责，包含产品在安全使用环境中对用户行为的假设。
- f) 用户指南应描述与用户有关的IT环境的所有安全要求。
- g) 用户指南应与为评价而提供的其他所有文件保持一致。

7.3 测试保证

7.3.1 功能测试

- a) 开发商应测试产品的功能，并记录结果。
- b) 开发商在提供产品时应同时提供该产品的测试文档。
- c) 测试文档应由测试计划、测试过程描述、预期的测试结果和实际测试结果组成。
- d) 测试文档应标识将要测试的产品功能，并描述将要达到的测试目标。
- e) 测试过程应标识要执行的测试，并描述每个安全功能的测试概况，这些概况包括对其它测试结果的顺序依赖性。
- f) 开发商的期望测试结果应表明测试成功后的预期输出。实际测试结果应表明每个被测试的安全功能能按照规定进行运作。

7.3.2 测试覆盖面分析报告

- a) 开发商应提供对产品测试覆盖范围的分析报告。
- b) 测试覆盖面分析报告应证明测试文件中确定的测试项目可覆盖产品的所有安全功

能。

7.3.3 测试深度分析报告

- a) 开发商应提供对产品的测试深度的分析报告。
- b) 测试深度分析报告应证明测试文件中确定的测试能充分表明产品的运行符合安全功能规范。

7.3.4 独立性测试

开发商应提供用于适合测试的部件，且提供的测试集合应与其自测产品功能时使用的测试集合相一致。

7.4 脆弱性分析保证

7.4.1 指南检查

- a) 开发者应提供指南性文档。
- b) 在指南性文档中，应确定对产品的所有可能的操作方式（包含失败和操作失误后的操作）、它们的后果以及对于保持安全操作的意义。指南性文档中还应列出所有目标环境的假设以及所有外部安全措施（包含外部程序的、物理的或人员的控制）的要求。指南性文档应是完整的、清晰的、一致的、合理的。

7.4.2 脆弱性分析

- a) 开发者应从用户可能破坏安全策略的明显途径出发，对产品的各种功能进行分析并提供文档。对被确定的脆弱性，开发者应明确记录采取的措施。
- b) 对每一条脆弱性，应有证据显示在使用产品的环境中该脆弱性不能被利用。在文档中，还需证明经过标识脆弱性的产品可以抵御明显的渗透性攻击。
- c) 脆弱性分析文档应明确指出产品已知的安全隐患、能够侵犯产品的已知方法以及如何避免这些隐患被利用。

7.5 生命周期支持

- a) 开发者应提供开发安全文件。
- b) 开发安全文件应描述在产品的开发环境中，为保护产品设计和实现的保密性和完整性，而在物理上、程序上、人员上以及其他方面所采取的必要的安全措施。开发安全文件还应提供在产品的开发和维护过程中执行安全措施的证据。

8 网站恢复产品安全技术要求的等级划分

网站恢复产品分为两个等级：基本级和增强级，如表9.1所示。

表9.1网站恢复产品等级划分表

		基本级	增强级	
4 功能要求	4.1 运行平台	4.1	4.1	
	4.2 网页发布系统	4.2	4.2	
	4.3 检测优先级		4.3	
	4.4 配置检测时间间隔	4.4	4.4	
	4.5 监控目录/文件管理	4.5	4.5	
	4.6 界面	4.6	4.6	
	4.7 增量备份		4.7	
5 性能评价	5.1 监控响应时间	5.1	5.1	
	5.2 篡改恢复时间	5.2	5.2	
	5.3 稳定性	5.3	5.3	
	5.4 资源占用		5.4	
	5.5 网络影响		5.5	
6 安全功能要求	6.1 静态网页文件自动恢复功能	6.1	6.1	
	6.2 动态脚本文件自动恢复功能		6.2	
	6.3 网页目录自动恢复功能	6.3	6.3	
	6.4 报警功能	6.4.1 实时报警	6.4.1	6.4.1
		6.4.2 报警信息的数据格式		6.4.2
		6.4.3 报警方式	6.4.3	6.4.3
	6.5 审计日志 功能	6.5.1 可审计事件	6.5.1	6.5.1
		6.5.2 审计信息的数据格式		6.5.2
		6.5.3 审计跟踪管理	6.5.3	6.5.3
		6.5.4 可理解的格式	6.5.4	6.5.4
	6.6 抵御已知攻击			6.6
	6.7 管理功能	6.7.1 授权管理员身份鉴别	6.7.1	6.7.1
		6.7.2 授权管理员权限	6.7.2	6.7.2
		6.7.3 管理信息传输安全		6.7.3
6.8 备份文件的安全存储及安全传输		6.8	6.8	
6.9 自身审计数据生成			6.9	
7 保证要求	7.1 交付与运行保证	7.1	7.1	
	7.2 指导性文档	7.2	7.2	
	7.3测试保证		7.3	
	7.4 脆弱性分析保证		7.4	

	7.5 生命周期支持		7.5
--	------------	--	-----

注：

- 1) 基本级主要对网站恢复产品最低安全级别提出要求；
- 2) 增强级在基本级基础上进一步提出提升网站恢复产品安全功能和可用性的附加要求。

|

附录 A

(资料性附录)

网站恢复过程举例

网站恢复一般是在监测到网站数据内容被未经授权更改后，及时产生报警，并进行准实时的自动恢复。网站恢复一般涉及3个环节：备份环节，监测环节和恢复环节。

A.1 备份环节

备份环节主要对网站数据进行备份，保存或更新网站备份数据。网站备份数据可以存放在本地服务器或远程服务器；

A.2 监测环节

监测环节主要检查网站数据内容是否被未经授权更改，并根据检查结果产生相应报警。

A.2.1 监测方式

监测操作可以在本地服务器或远程服务器上进行，采用定时检测方式、触发方式或其他方式。

A.2.1.1 定时检测方式

定时检测方式根据设定的时间定时读出要监控的网站数据(或其他能用以判断网站数据是否被更改的信息，例如，相应的文件属性等)，将其与网站备份数据相比较，从而判断网站数据是否被更改。

为提高检测效率，可能将网站数据分为不同等级，对不同等级的网站数据设置不同的检测时间。例如，将高等级网站数据的检测时间间隔设得较短，以获得较好的实时性；而将等级较低的网站数据检测时间间隔设得较长，以减轻系统的负担。

A.2.1.2 触发方式

触发方式通过一些特定的事件来触发检测操作，而不是定时地、主动地对网站数据进行检测。这些特定事件可能是文件被访问、创建、修改或删除等。

例如，当用户访问某个网页的时候触发对该网页进行完整性检查。或利用一些特殊技术(例如，文件过滤驱动程序)捕获网站文件被访问、创建、修改或删除等事件，从而触发检测操作。

A.2.2 比较方式

在判断文件是否被修改时，往往采用将被保护的网站数据和网站备份数据进行比较的方式进行。

A.2.2.1 全文比较

这是最常用的比较方式，它能直接、准确地判断出该文件是否被修改。然而全文比较在文件较大较多时效率十分低下。

一些保护软件采用文件的属性如文件大小、创建修改时间等进行比较。这种方法虽然简单高效，但也有严重的缺陷：恶意入侵者可以通过精心构造，把替换文件的属性设置得和原文件完全相同，从而使被恶意更改的文件无法被检测出来。

A. 2. 2. 2 函数比较

通过比较文件的Hash值（例如，MD5算法）判断文件是否被修改。这种比较方式效率高，难以伪造，能比较精确地发现文件被篡改。

A. 3 恢复环节

当监测到网站数据内容被未经授权更改后启动恢复环节，使用网站备份数据替换被未经授权更改的网站数据。

根据网站备份数据存放的位置不同，恢复操作可以分为本地或远程方式。

如果网站备份数据存放在本地服务器，则需要拥有对被保护目录或文件的写权限。如果网站备份数据存放在远程服务器，则需要通过其他方式进行，例如，文件共享或FTP的方式，相应地，需要文件共享或FTP的帐号，并且该帐号拥有对被保护目录或文件的写权限。

参考文献

- [1] MSCTC-GFJ-08 信息技术 网站恢复产品安全检验规范
- [2] 高延玲, 张玉清等. 网页保护系统综述[J]. 计算机工程, 2004 30(10): 113