

# 网站防篡改整体解决方案

速龙网站智能自动防护系统

版本 v1.0

北京速龙软件科技有限公司编制

---

# 目 录

<b>第一章 项目分析 .....</b>	<b>1</b>
一、 背景分析 .....	1
二、 需求分析 .....	2
<b>解决方案 .....</b>	<b>3</b>
三、 总体目标 .....	3
四、 项目原则 .....	3
五、 平台简介 .....	3
六、 系统功能 .....	4
七、 系统特点 .....	5
八、 商务报价 .....	6
<b>第二章 项目实施 .....</b>	<b>6</b>
一、 运行环境 .....	6
1、 软件环境 .....	6
2、 硬件环境 .....	6
二、 USB KEY .....	7
三、 系统安装 .....	7
1、 部署说明 .....	7
2、 备份服务器的安装 .....	8
3、 服务器的安装 .....	8
四、 针对 XX 市 XX 局具体安装实现 .....	8
1、 网站备份 .....	8
2、 创建虚拟网站 .....	8
3、 确认网络环境 .....	8
4、 开始安装 .....	9
5、 系统升级 .....	9
6、 设置管理员 .....	9
7、 防护系统设置 .....	9
8、 安装完成 .....	9
<b>第三章 售后服务 .....</b>	<b>9</b>
一、 服务方式和内容 .....	9
二、 培训计划 .....	11
1、 培训方式 .....	12
2、 时间安排 .....	12



# 第一章 项目分析

## 一、背景分析

伴随着互联网的迅速发展，黑客行为、病毒、木马等危害网络安全的行为也越来越多，据近两年统计资料，安全事件中超过 50% 是非法篡改、删除、窃取主机内文件、数据、资料的行为。

目前，利用网上随处可见的攻击软件，攻击者不需要对网络协议的深厚理解基础，即可完成诸如更换 web 网站主页，到取管理员密码，破坏整个网站数据等等攻击。而这些攻击过程中产生的网络层数据，和正常数据没有什么区别。

通过统计国外一个黑客站点每天公布出来的黑客链接，平均每天 10 多个中国政府网站被攻破。很多用户认为，在网络中不断部署防火墙，入侵检测系统(IDS)，入侵防御系统(IPS)等设备，可以提高网络的安全性。但是为何基于应用的攻击事件仍然不断发生？其根本的原因在于传统的网络安全设备对于应用层的攻击防范，作用十分有限。目前的大多防火墙都是工作在网络层，通过对网络层的数据过滤(基于 TCP/IP 报文头部的 ACL)实现访问控制的功能；通过状态防火墙保证内部网络不会被外部网络非法接入。所有的处理都是在网络层，而应用层攻击的特征在网络层次上是无法检测出来的。IDS, IPS 通过使用深包检测的技术检查网络数据中的应用层流量，和攻击特征库进行匹配，从而识别出以知的网络攻击，达到对应用层攻击的防护。但是对于未知攻击，和将来才会出现的攻击，以及通过灵活编码和报文分割来实现的应用层攻击，IDS 和 IPS 同样不能有效的防护。

### ➤ 注入攻击：

对于和后台数据库产生交互的网页，如果没有对用户输入数据的合法性进行全面的判断，就会使应用程序存在安全隐患。用户可以在可以提交正常数据的 URL 或者表单输入框中提交一段精心构造的数据库查询代码，使后台应用执行攻击着的 SQL 代码，攻击者根据程序返回的结果，获得某些他想得知的敏感数据，如管理员密码，保密商业资料等。

### ➤ 跨站脚本攻击：

由于网页可以包含由服务器生成的、并且由客户机浏览器解释的文本和 HTML 标记。如果不可信的内容被引入到动态页面中，则无论是网站还是客户机都没有足够的信息识别这种情况并采取保护措施。攻击者如果知道某一网站上的应用程序接收跨站点脚本的提交，他就可以在网上传提交可以完成攻击的脚本，如 JavaScript、VBScript、ActiveX、HTML 或 Flash 等内容，普通用户一旦点击了网页上这些攻击者提交的脚本，那么就会在用户客户机上执行，完成从截获帐户、更改用户设置、窃取和篡改 cookie 到虚假广告在内的种种攻击行为。

---

## 二、需求分析

各级政府机关在社会经济文化生活中不仅扮演者管理者和协调员的重要角色，而且其为企业和社会服务的职能在这场信息革命的大潮中日益明显和重要起来。各级政府部门可以充分利用网络化的信息新技术，提高各方面的办事效率，为公众提供更好的更快的服务，充分进行政策宣传教育以及促进政务公开、提高政府形象。所以政府信息化则被公认为社会信息化的基础，政府信息化的目标就是“电子政府”的实现。

通过近期与用户单位沟通联系，了解到目前用户单位网站网络现有状况，目前拥有自己的服务器，列表如下：

用户单位网站服务器情况	
服务器操作系统	Microsoft Windows Server 2003
Web 服务器类型	IIS 6.0
网络环境	TCP/IP
网站语言支持	Asp
目录结构	包含可写可执行目录

对网络安全要求上需要达到跨站脚本攻击和注入攻击等一系列攻击恶意功能的防范。

“速龙网站智能自动防护系统”由文件保护驱动、防注入攻击模块、管理员控制台、管理员远程控制台组成。主要用于阻止对 Web 主机受保护文件的非授权改动，并且能侦测与阻止注入攻击以及跨站脚本链接，该产品与防毒系统、防火墙、入侵检测系统结合在一起，共同提供完整的 Web 安全解决方案。

本软件系统本身具备一定的自我防护能力，以防止外部入侵对系统本身的攻击，并使用网上银行同等安全级别的 USB Key 进行系统本身的授权、远程管理授权，此外，管理员远程管理台使用 1024 位的 SSL 安全通信与服务器通信以进行远程管理。所有使用的 USB Key 均内含 CPU 以及独立的存储、安全模块，进行独立的运算。

互联网恰如一柄“双刃剑”，为人们工作带来便利的同时，伴随着的是日趋严重的网络入侵安全问题。作为政府公用站点，既要访问 Internet 的共享信息资源，又要把 Intranet 的一部分信息对外提供服务，资源的共享的同时也带来了安全问题；而作为政府部门内部网，事关很多政府机密、政府形象等敏感信息，网络的安全性更为重要。从某种意义上说，政府机关内部网络的信息安全也涉及到个人与集体利益、社会稳定和国家的安全等重要问题。如何保护政府内部网络的信息安全，防范来自外部网络的黑客和非法入侵者的攻击，建立起强健的网络信息安全防范系统，在某种程度上决定着政府部门信息化建设的成败。



# 解决方案

## 三、总体目标

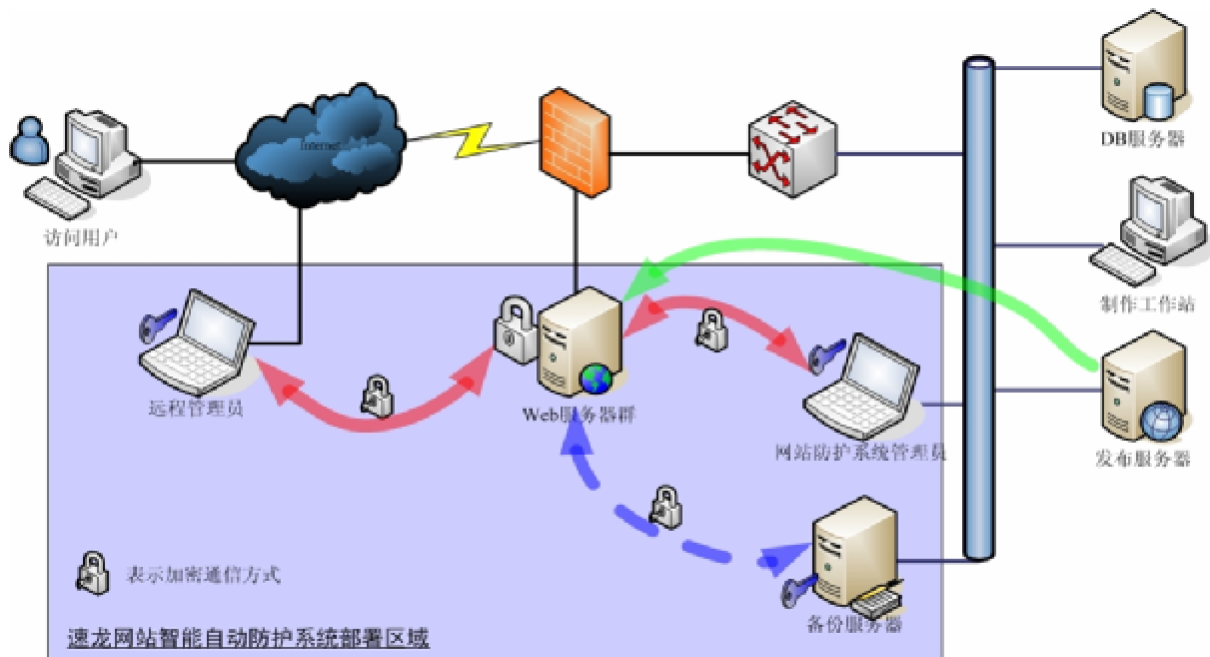
对用户单位的网站网络环境进行安全保护，通过部署速龙网站智能自动防护系统，从而达到有效阻击跨站脚本攻击和注入攻击等一系列攻击恶意功能的防范。

## 四、项目原则

- ◆ **安全性** 主要提供安全保障，防护严密，防止注入防护及报警服务；
- ◆ **易用性** 在部署方面要求简单易用，方便实用，并且系统资源占用要低；
- ◆ **实用性** 为客户提供灵活的用户管理，完备的日志分析功能；
- ◆ **先进性** 要求能够做到网银级别的安全防护级别；

## 五、平台简介

整个系统由服务器保护系统、备份服务器系统、管理员远程控制台组成。以下是网站智能自动防护系统部署示意图：



速龙网站智能自动防护系统部署示意图



## 六、系统功能

- **文件保护策略** 由管理员设置需要保护的文件目录，设置了保护以后的文件目录中的文件、子目录只能由授权程序【也是由管理员通过管理平台控制台设置】改动，除此以外的进程都无法对受保护的文件目录下的内容进行修改，即便黑客攻破了防火墙、获取了操作系统的管理员帐号密码，仍然无法对受保护的文件目录下的文件内容进行改动，因为管理员控制台使用单独的 USB Key，使用独立于操作系统身份认证的单独身份认证系统进行管理员控制台的授权，因此即便系统的其他安全防护措施遭到攻破，“速龙网站智能自动防护系统”依然能有效地作为最后一道保护屏障。
- **注入防护** 针对 Web 主机的注入防护是最常见的攻击手段，黑客使用注入攻击，主要是 SQL 注入攻击对存在注入安全漏洞的网站主机发起攻击，并在找到注入漏洞以后采取进一步的手段以获得系统的管理员帐号或者修改数据库系统中数据，以便进行进一步的入侵，目前该漏洞已经引起了网站管理员或者网站程序员的重视，在 Linux 系统下也有防范注入方面的模块；但是在 Windows 平台下，普遍采取的还是关键词过滤等方法，而关键词过滤的问题一是对于系统效率有影响，另外在过滤的关键词方面可谓是防不胜防，而且有些注入攻击是采取单纯的关键词过滤无法防范的。在“速龙网站智能自动防护系统”中，采用了词法分析、表达式分析、计算、关键词过滤等手段，对于客户端提交的 HTTP 数据，进行有效的分析与计算，寻找其中可能存在的注入攻击企图，并按照系统设置的策略予以处理，所能处理的包括 SQL 注入、Blind SQL 注入、XSS 攻击、文件注入攻击、Command 注入、Coldfusion 注入、SSI 注入、PHP 注入等等。
- **报警服务** 一旦检测到文件保护、注入等攻击行为，即可按照管理员设置的报警周期、报警方式进行报警，目前支持的报警方式包括邮件报警与短信报警。
- **日志审计** 针对文件防护、注入攻击、远程管理、报警信息等方面提供详细的可审计日志，管理员可能对日志进行排序、分类、输出等操作。
- **远程管理** 管理员可以在服务器上颁发远程管理授权 USB Key，该 USB Key 由管理员在服务器上采集特定信息，并结合以管理员所输入的信息，生成一个特定的安全证书，该证书内含一个 1024 位的通信密钥，可以使用该 USB Key 与服务器进行 SSL 通信，在远程对服务器进行集中式的设置和管理。



## 七、系统特点

- **服务器系统负载低** 所采用的文件保护模块以及注入防护模块，均尽可能在算法上进行优化，使系统负载的增加降到最低，根据实际测试，对于日 Pageviews 为 10 万次左右的网站服务器，系统负载增加不到 5%。
- **防护严密** 系统提供的文件保护功能，即便服务器被黑客或者非授权人员操控，依然无法对受保护的文件夹下的内容进行修改，如果通过远程访问的方式，则困难更大；另外，系统所提供的注入攻击防护模块，也采用了高效的语法分析、表达式分析与计算模块，能非常有效的防止注入攻击。
- **安全性高** 采用网上银行级别的 USB Key 进行系统自身的授权与防护，系统本身只能通过管理员控制台进行改动，管理员的帐号密码采用独立于操作系统的帐号密码进行管理，并以非可逆方式存储在 USB Key 内，如果该 USB Key 不插在服务器上，则无法进行管理员控制台的设置；当该 USB Key 插在服务器上时，管理员仍然需要输入帐号密码才能登录控制台程序，该帐号密码以不可见形式存储在 USB Key 中，并对所输入的帐号密码进行运算并在 USB Key 内部进行校验，方可启动管理员控制台。远程管理所用的 USB Key 由管理员在服务器上颁发，并采用根据服务器相关的信息生成的 1024 位的 SSL 证书，该证书存储在服务器的 USB Key 与远程管理 Key 中，只能在匹配的情况下才能建立其通信连接，并且该 1024 位的 SSL 证书被用于加密所有通信过程中的数据。
- **便捷的远程管理** 系统提供管理员远程控制台，通过该控制台程序，管理员可以在远程对服务器进行设置与管理，由于采用了基于 1024 位密钥的 SSL 通信，远程管理可以安全的进行而无需担心中途被截获或篡改。
- **日志完整** 系统记录了完整的日志，通过对这些日志，管理员可以进行有针对性的管理，并可在适当的时候作为司法证据。



## 八、商务报价

(单位：人民币万元)

产品方案	规格型号	报价	厂家	数量	购买说明
A	网站智能自动防护系统	¥59,800 (元/套)	速龙	1套	满足 1 台 Web 服务器+1 台备份服务器+1 台同步发布服务器。每新增一台 Web 服务器，就需要单独购买 1 个服务器防护模块 [以及 1 个注入防护模块*]。备份服务器模块、管理员远程控制台模块、网站用户远程控制台模块可应用与多台 Web 服务器，不再需要单独购买。
B	新增 Web 服务器防护模块	¥25,800 (元/台)	速龙	1套	因方案 A 产品只能对 1 台 Web 服务器进行防护，如果使用了多台 Web 服务器，则需要为其他的 Web 服务器单独购买本模块。

## 第二章 项目实施

### 一、运行环境

#### 1、软件环境

服务器端包括：文件保护模块、注册表保护模块、注入防护模块、管理员控制台，这些模块运行于 Web 服务器上，支持的操作系统包括 Microsoft Windows 2000Server 系列、2003 Server，此外还支持 Windows XP 系统。

远程管理员控制台模块运行于安装了 Microsoft Windows 操作系统的 PC。

需要 TCP/IP 网络环境。

#### 2、硬件环境

服务器端由于系统负载低，对于硬件环境没有特殊要求，最低要求如下：

**CPU: PII 400 及以上**

**内存: 256M 及以上**



**硬盘空间：10M**

远程管理员控制台模块要求的硬件环境：

**CPU： PII 400 及以上**

**内存： 128M 及以上**

**硬盘空间：10M**

## 二、USB Key

本软件附带四个 USB Key：

一个是备份服务器的 USBKey，第一次使用时将要求输入管理员帐号密码，该 USBKey 是用来启动备份服务器控制台程序的，只有在启动备份服务器控制台时才需要。

一个是控制台管理员的 USBKey，第一次使用时将要求输入管理员帐号密码，并且以后在这台服务器上只能使用这个 Key。

一个 USB Key 是一个空白的 Key，用来作为 web 同步发布服务器 USBKey，该 Key 需要管理员通过“系统设置”->“远程管理设置”->“发行一个新 Key”->“发行一个同步发布 Key”进行发行，发行以后的 USB Key 才能用来登陆同步发布服务器。

另外一个 USB Key 是一个空白的 Key，用来作为管理员远程控制台的 Key，该 Key 需要管理员通过“系统设置”->“远程管理设置”->“发行一个新 Key”进行发行，发行以后的 USB Key 才能用来远程登录管理该服务器。如果需要发行多个远程管理 Key，请向软件供应商联系购买。关于如何发行一个远程管理 USB Key，请参阅《第三章 服务器控制台操作》中“远程管理设置”一节。

所有的 Key 在第一次使用时需要输入管理员/使用者的帐号密码，该帐号密码存储在 Key 中，而且采用不可逆方式加密，即便是软件开发商也无法获取该帐号密码，因此请一定牢记该帐号密码，否则管理员 Key 只能退回我公司进行重置，远程管理 Key 只能退回管理员进行重新发行。

## 三、系统安装

### 1、部署说明

主模块安装在 Web 服务器上，提供防护功能。每台 Web 服务器需安装一次。

一个 Web 服务器群只需要安装一台备份服务器(可选，非必需)，一台远程管理计算机(可选，非必需)。Web 发布服务器既可以是与内容管理系统、发布系统在同一台物理服务器上、也可以是与内



容管理系统、发布系统分别配置在不同服务器上。可以与任意内容管理系统及发布系统配合使用。

## 2、备份服务器的安装

在备份服务器上运行“速龙网站智能自动防护系统-备份服务器.exe”安装程序，点击“下一步”按钮即可完成安装。

安装完成以后无需重启系统。

## 3、服务器的安装

在服务器上根据服务器的系统配置运行“速龙网站智能自动防护系统.exe”或者“速龙网站智能自动防护系统（64）.exe”安装程序，如果操作系统是 64 位，那么在安装前请安装光盘目录下的 dotnetfx35.exe 对系统进行补丁更新，然后运行安装程序，确定好安装目录以后，再点击“下一步”即可。

系统提供的服务器授权 USB Key 请在防护系统安装完成以后再插入到服务器的 USB 口中。

## 四、针对 xx 市 xx 局 具体安装实现

### 1、网站备份

为了保证服务器数据的安全，在系统安装前，我们将对整个需要受保护的网站系统进行数据备份，备份内容包括：网站目录、网站 web 程序、相关脚本及数据库文件等。

### 2、创建虚拟网站

为了应对系统安装有可能造成的网站无法对外提供 web 服务或者特殊的未知情况对网站的影响，我们将对网站进行完整复制并建立虚拟网站，一旦在安装过程或者安装结束后发现原网站无法提供相应 web 服务，那么我们会及时的切换到虚拟网站进行无差别的 web 服务来应对突发事件。

### 3、确认网络环境

再次确认备份信息完整和虚拟网站系统完整性，并检测确认网络环境畅通，系统稳定运行后准备“速龙网站智能自动防护系统”的安装。



## 4、开始安装

根据获悉的资料,我们将安装32位“速龙网站智能自动防护系统”安装程序,安装过程详见“2.3.3 服务器的安装”,安装完成后重新启动系统,并配置“本地连接”服务,并安装“Sulong web Inject Protector Driver”服务。

## 5、系统升级

安装完成后,查看是否有最新升级信息,并根据最新升级信息对系统进行升级。

## 6、设置管理员

完成全部安装后,插入“控制台管理员 USBKey”开始设置新用户,并由 xx市xx局 相关技术人员设定基本用户参数。

## 7、防护系统设置

根据现场网站文件目录运行情况,对相关文件目录进行保护服务设置,以及注入、报警、备份等相关设置,完成调试作业。

## 8、安装完成

到此,安装过程结束。

# 第三章 售后服务

## 一、服务方式和内容

北京速龙软件科技有限公司坚定执行“用户至上”的企业理念,为社会提供最高质量和最大可能价值的商品和服务做出了不懈努力,深受用户的喜爱。对提供给用户所有产品都有相应产品说明书、质量保证书等。高水平高素质的技术人员队伍是服务与支持的基础。

北京速龙软件科技有限公司对技术人员的要求相当地严格,为了不断提高北京速龙软件科技有限公司的技术人员的业务素质,北京速龙软件科技有限公司经常不断的派技术人员参加 CISCO、HP、



Intel、 Microsoft 等公司的技术培训，并取得了相应的授权资格认证。

## **第一条、 服务总则**

为了保护最终用户的合法权益、明确北京速龙软件科技有限公司及其代理商的售后服务责任、规范服务行为、提高服务质量，特制定本法则。北京速龙软件科技有限公司及其代理商严格执行，并接受用户及有关政府部门的监督。北京速龙软件科技有限公司直接销售的软件产品由指定代理商负责售后服务，而代理商销售的本公司软件产品也由代理商承担售后服务工作，其售后服务收费的标准是统一的。代理商可依据本法则的有关规定，制定具体的服务办法和相关服务措施。

## **第二条、 服务签约**

凡是北京速龙软件科技有限公司的合法用户，一经购买，即可享受北京速龙软件科技有限公司及其代理商单位提供的售后服务。

## **第三条、 服务内容**

用户购买北京速龙软件科技有限公司软件产品后，北京速龙软件科技有限公司及其代理商单位可以为用户提供以下售后服务项目：

1. 热线电话支持（010-82809450/62/92）。
2. 电子邮件服务：用户可以通过 Email 方式提出问题，而技术支持人员将随时通过 Email 将问题的解决方法、升级程序及相关文档等发送到用户的邮箱里，避免由于一时疏忽造成的麻烦，服务邮箱为：support@slsoft.com.cn。
3. 远程技术服务：当用户提出技术支持要求后，由技术支持部门的技术支持工程师对客户的要求通过互联网远程技术做出技术支持。
4. 在线交流：用户可以访问本公司的网站，并在在线交流区中提出问题，我们将对用户提出的问题进行归纳，然后做出统一的回答。
4. 上门服务：对于客户使用软件中提出的产品技术问题，一般问题保证在当日内予以解决；但当问题没现成答案时，将根据情况的严重程度做出相应响应，提供现场支持服务。
5. 培训服务：提供产品售后技术实施培训。分现场培训和集中培训两种。
6. 定期回访服务：定期与您沟通，了解软件、硬件和环境的运行状况，使您的系统处于最佳运行状态。分电话回访和上门回访两种。
7. 保修与版本升级服务：针对本项目提供三年的保修期。用户可以根据自已的情况对软件进行版本升级。

## **第四条、 服务标准**



1. 一般常见问题作到当时解决；
2. 对于无法立即提供解决方法的问题，在寻找到解决方法后，将采用电话回复、传真或 Email 等方式通知用户予以解决；
3. 确实无法解决的问题，技术部会将问题备案并通知用户；
4. 如果是上门服务，支持工程师将在与用户商定的时间内到达现场。
5. 如遇无法当场解决的问题，支持工程师将与用户商定下一次服务的时间。如遇非支持范围的问题，支持工程师确认问题后将提出建议解决方法。

## 第五条、软件服务收费标准

凡北京速龙软件科技有限公司产品用户，其免费升级及维护期限为 3 年。北京速龙软件科技有限公司对用户承诺终生维护，在合同商定免费升级及维护期满后，软件维护方式及费用如下：

### 1. 软件维护（每年）

- ◇ 所有电话技术咨询及远程服务均不收费；
- ◇ 对于使用中的技术问题，用户应将情况写明并传真至北京速龙软件科技有限公司或代理商处，以得到及时准确的答复；
- ◇ 对于一般维护，1 小时内相应，8 小时内响应解决；对于复杂维护，24 小时内上门。

### 2. 软件退换与保修

- ◇ 光盘、加密盒及印刷资料在用户开封时发现损坏，给予免费更换；
- ◇ 正常使用时损坏，致使软件无法正常运行给予免费更换；
- ◇ 非正常使用造成软件损坏，免费保修；原加密设备需退回；
- ◇ 对不符合上述保修条件者，不予保修。

### 3. 上门服务

- ◇ 免费上门服务期限为项目交割后一年内，一年以后上门服务由用户按标准支付交通、食宿及适当服务费用。

## 二、培训计划

针对速龙网站智能自动防护系统的实际应用，我们将负责提供全面培训系统的培训服务，以保证软件系统的正常维护与使用。



## 1、培训方式

培训对象	培训范围	培训形式
网站中心管理 人员	<ul style="list-style-type: none"><li>◆ 网站智能自动防护系统软件安装、卸载、部署及故障排除。</li><li>◆ 网站智能自动防护系统各功能模块的授权、操作和维护等。</li></ul>	<ul style="list-style-type: none"><li>◆ 软件安装调试时由工程师现场边安装边指导，同时完成软件的安装部署工作。</li><li>◆ 安装过程中，现场答疑。</li></ul>

## 2、时间安排

根据客户情况确定。



# 安装过程审计表

安装对象	用户单位	
软件名称	速龙网站智能自动防护系统	
系统环境	Microsoft Windows Server 2003 IIS 6.0 web 服务器 Asp 网站 TCP/IP 网络环境	
安装项目	操作过程	备注
网站备份		
创建虚拟网站		
确认网络环境		
开始安装		
系统升级		
设置管理员		
防护系统设置		
安装完成		

北京速龙软件科技有限公司