百年人寿保险股份有限公司

招
标
文
件

招标编号：AEONLIFE- IT-2015-035

项目名称：百年人寿 2015 年度 IT 设备-网络安全项目

二〇一五 年 九 月 日

投标须知前附表		
项目	内容	规定
1	项目名称	百年人寿 2015 年度 IT 设备-网络安全项目
2	招标单位	百年人寿保险股份有限公司
3	招标编号	AEONLIFE- IT-2015-035
4	投标人资格	1:投标人需提供由原厂针对招标方项目的正式授权证明（须加盖原厂相应授权印章），包含招标方名称、招标文件名称及标书编号等基本信息。
5	供货说明	中标方需根据招标方书面通知分期供货，供货期为 1 年，双方签订年度供货协议。
6	投标有效期	30 自然日（从提交投标文件的截止之日起算）
7	投标文件份数	正本壹份，副本贰份
8	投标答疑	投标人应当于投标截止日前五日将投标疑问以书面形式传递至招标人。
9	投标文件递交截止时间	地点：大连市沙河口区体坛路 22 号诺德大厦 21 楼 时间：截至 2015 年 10 月 17 日 （投标文件递交截止时间即为投标截止时间）
10	开标时间	开标时间：2015 年 10 月 18 日。 开标地点：大连市沙河口区体坛路 22 号诺德大厦 21 楼

第一部分　招标邀请

百年人寿保险股份有限公司是经中国保险监督管理委员会批准成立的全国性人寿保险公司。公司于 2009 年 6 月 3 日正式开业，总部选址大连。公司注册资本 77.9 亿元人民币，由东方资产、国电电力、融达投资、大连港集团、大商集团、时代万恒、新光集团、一方地产等 17 家股东构成。强大的股东背景、良好的法人治理结构以及优秀的管理团队为百年人寿的发展奠定了坚实基础。

本公司现拟对“**百年人寿 2015 年度 IT 设备-网络安全 项目**”进行招标，经前期综合考查评选，现诚挚地邀请贵公司参与本项目的投标。在正式投标前，请详细阅读本招标文件并确实遵守其中各项要求。

1.招标编号：AEONLIFE- IT-2015-035

2.招标内容： IT 设备-网络安全

3.投标截止日期： 2015 年 10 月 17 日，招标人拒收本截止日期后送达的投标文件。

4.投标地点： 辽宁省大连市沙河口区体坛路 22 号诺德大厦 21 楼

5.标书接收人： 李超

联系电话： 0411-39828218

传真电话： 0411-39828777

电子邮件： lichao003@aeonlife.com.cn

yuguangchen@aeonlife.com.cn

6.联系方法：有关此次招标邀请之事宜，可以书面或传真或电子邮件形式与百年人寿沟通。

单位名称：百年人寿保险股份有限公司

地址：辽宁省大连市沙河口区体坛路 22 号诺德大厦 21 楼

邮编：116033

7.投标有效期： 30 日，从提交投标文件的截止之日起算。

第二部分 投标人须知

A.说明

一、适用范围

本招标文件仅适用于“**百年人寿 2015 年度 IT 设备-网络安全项目**”。

“**百年人寿 2015 年度 IT 设备-网络安全 项目**”各阶段活动内容、操作要求等方面的要求详见招标书之第三部分。

二、定义

1.“招标人”系指百年人寿保险股份有限公司。

2.“投标人”系指投标人响应招标、参加投标竞争的法人或者其他组织。

B.招标文件说明

三、本招标文件的构成

招标文件由下述部分组成：

1. 招标邀请
2. 投标人须知
3. 项目需求
4. 投标文件格式
5. 书面澄清或者修改的招标文件内容

四、招标文件的澄清与修改

招标人对已发出的招标文件进行必要的澄清或者修改的，应当在招标文件要求提交投标文件截止时间至少 5 日前，以书面形式通知所有招标文件收受人。

该澄清或者修改的内容为招标文件的组成部分。

五、投标保证金

招标人在招标文件中要求投标人提交投标保证金的，投标保证金不得超过招标项目估算价的 2%。投标保证金有效期应当与投标有效期一致。

投标截止后投标人撤销投标文件的，招标人可以不退还投标保证金。

招标人最迟应当在书面合同签订后 5 日内向中标人和未中标的投标人退还投标保证金及银行同期存款利息。

六、对招标文件的疑问

对招标文件有异议的，应当在投标截止时间 5 日前提出。招标人应当自收到异议之日起 2 日内作出答复；作出答复前，应当暂停招标投标活动。

C.投标文件的编写

七、投标文件要求

投标人应仔细阅读招标文件的所有内容，按招标文件的要求提供投标文件，并保证所提供全部资料的真实、有效、关联。

如果投标人根据招标文件载明的项目实际情况，拟在中标后将中标项目的部分非主体、非关键性工作进行分包的，应当在投标文件中载明。

八、投标语言

投标文件及投标人和招标人就投标交换的文件和来往信件，应以中文书写。

九、投标文件的组成

投标文件应包括下列部分：

1.投标书

2.投标价格表

3.投标人需提供由原厂针对招标方项目的正式授权证明（须加盖原厂相应授权印章），包含招标方名称、招标文件名称及标书编号等基本信息。

4.企业基本情况材料及资格证明文件复印件（需加盖公章），包括：

－公司营业执照复印件 1 份；

－公司税务登记证复印件 1 份；

－公司组织机构代码证复印件 1 份；

－公司近两年内成功运作的相关案例；

－…….

－其它可以证明投标人有能力履行招标文件中合同条款和执行要求规定的相关文件。

投标人应将投标文件装订成册。

十、投标文件格式

投标人应按招标文件中提供的投标文件格式填写投标书、投标价格表、投标人基本情况材料及资格证明文件，并提供产品详细方案及招标文件要求的所有内容。

十一、投标报价

1.报价方式

(1)投标者应明确说明各执行阶段每个项目的总体价格，以及价格明细。报价需由经正式授权的代表签署，并加盖投标人公司公章。

(2)投标者应按照招标人最后确定的需求报价。

2.填写时应注意下列要求：

一旦投标人中标，投标人不得以任何借口向招标人提出增加任何费用的要求。

十二、投标人基本信息

1.简述公司的基本情况、发展历史、股东情况，最近两个年度的成功案例，员工及分公司数量。

2.明确叙述公司拟参与本项目负责人与主要技术人员的简历、业绩、拟用于完成招标项目的设备及时间投入。

3.若公司将与合作伙伴一起参与本项目竞标，简述公司合作伙伴的基本情况以及将参与本项目的人员的简历和时间投入。

4.本项目联系人：

－公司名称：

－联系人姓名及职位：

－电话号码：

－传真号码：

－电子邮件地址：

十三、投标文件的签署及规定

1.投标人应准备一份正本和二份副本，在每一份投标文件上要明确注明“正本”或“副本”字样，一旦正本和副本有差异，以正本为准。同时提供全套投标文件的电子文档与正本共同封装（介质应为U盘）。

2.投标文件正本和副本须打印并由经正式授权的投标人代表签字，并加盖投标人公司公章。

D.投标文件的递交

十四、投标文件的密封和标记

1.投标人应将投标人文件正本和副本分别用信封密封，并在封签处加盖投标人公章(或合同专用章)。

2.投标文件信袋封条上应写明：

(1)招标人名称、招标文件所指明的投标送达地址；

(2)招标项目名称；

(3)标书编号；

(4)投标人名称和地址；

(5)注明"开标时才能启封"，"正本"，"副本"。

3.如投标文件由专人送交，投标人应将投标文件进行密封和明确标记后，按投标邀请注明的地址送至招标人。招标人拒收投标截止时间后送达的投标文

件。

E.开标和评标

十五、开标

1.开标于提交投标文件截止时间的同一时间在百年人寿保险股份有限公司职场公开进行。

2.开标时，在评标小组人员全部到齐后工作人员查验投标文件密封情况，确认无误后当众拆封，宣读投标人名称、投标价格和投标文件的其他主要内容，一式三份的招标文件必须在招标现场同时开标。开标过程应当记录，并存档备查。

十六、评标小组

招标人将针对此次招标工作成立评标小组，评标小组成员的名单在中标结果确定前应当保密。

评标小组对投标文件进行审查、质疑、评估和比较，采用综合打分法（本项目的报价将作为最主要评估因素）进行评标。

十七、投标文件的澄清

投标文件中有含义不明确的内容、明显文字或者计算错误，评标小组认为需要投标人作出必要澄清、说明的，应当书面通知该投标人。投标人的澄清、说明应当采用书面形式,并不得超出投标文件的范围或者改变投标文件的实质性内容。

十八、对投标文件的评估和比较

1.招标人及其组织的评标小组将对实质性响应的投标文件进行评估和比较。

2.评标时除考虑投标价格外，还将考虑以下因素：

(1) 投标方所报的实施方案

(2) 所投产品的售后服务体系、技术人员实施能力。

十九、保密

1.有关投标文件的审查、澄清、评估和比较以及有关授予合同的意向的一切情况都不得透露给任何投标人或与上述评标工作无关的人员。

2.本项目招标书属于招标人所有。未经招标人的书面许可，不得将本项目招标书的任何内容以任何形式泄露给任何其它第三方，否则，投标人应承担给招标人造成的所有损失。

F.中标和合同

二十、定标准则

中标人的投标应当符合下列条件之一：

1.能够最大限度地满足招标文件中规定的各项综合评价标准；

2.能够满足招标文件的实质性要求，并且经评审的投标价格最低；但是投

标价格低于成本的除外。

二十一、中标结果的通知

招标人负责向中标人发出《中标通知书》，并同时将中标结果通知所有未中标的供应人。投标人如对评标过程有异议或对评标结果不服可向招标人合规经营部投诉。

二十二、合同的签订和履约保证金

招标人和中标人应当自《中标通知书》发出之日起三十日内，按照招标文件和中标人的投标文件订立书面合同。

招标文件要求中标人提交履约保证金的，中标人应当提交。

二十三、否决投标

有下列情形之一的，评标小组否决其投标：

1.投标文件未经投标单位盖章和单位负责人签字；

2.投标联合体没有提交共同投标协议；

3.投标人不符合国家或者招标文件规定的资格条件；

4.同一投标人提交两个以上不同的投标文件或者投标报价，但招标文件要求提交备选投标的除外；

5.投标报价低于成本或者高于招标文件设定的最高投标限价；

6.投标文件没有对招标文件的实质性要求和条件作出响应；

7.投标人有串通投标、弄虚作假、行贿等违法行为。

第三部分　项目需求

一、服务商简介

二、百年人寿 2015 年度 IT 设备-网络安全 项目要求

1、设备需求，详见《**附件 2：网络安全项目技术参数**》

2、招标方采购设备的型号和数量，投标方参考本招标文件的《**附件 3：投标价格表**》填写。

3、制定详细的百年人寿网络协议分析系统租赁项目现场实施方案和现场技术支持流程，必须保证现场实施。

4、设备送货，安装、调试服务的费用由投标方承担。

5、租赁期间设备免维保费用，同时厂商提供最新型号的设备支持和系统及时更新，招标方不额外支付硬件故障和维保费用。

6、投标方在设备保修期内为招标方免费提供维保服务，具体要求如下：

（1）服务范围：维保服务覆盖《**附件 3：投标价格表**》清单中的设备和自带软件。

（2）服务工程师：技术维保工程师应具备上述维保对象的硬件系统、软件系统、管理/操作系统等方面的知识，具备相应的技术资格认证，并有 3 年以上从业经验；

（3）服务级别：7×24 技术服务支持，2 小时到达现场；

（4）故障响应及处理：

- 对系统性能严重损坏，接到支持需求必须立即做出回应；
- 对系统运行正常，仅受到有限的影响或未受到严重影响，接到支持需求必须在 30 分钟内做出回应；

（5）备品备件：按照原厂商承诺提供服务。

（6）现场巡检：每年进行一次设备现场巡检。

（7）产品升级：提供产品升级评估和现场升级服务，包括网络设备 OS 系统版本升级、升级方案提供与升级后验收。

（8）特殊要求：提供特殊时段（春节、劳动节、国庆节、年终、招标方重大应用测试、投产），以及系统变更和迁移、系统升级等的现场支持服务。

（9）建立与招标方的沟通机制，现场支持指定专人负责。

（10）在保修期内，投标方应无偿并迅速替换由于部件缺陷及制造工艺等问题而发生故障的产品。如因产品有设计、生产之缺陷而造成设备的性能和质量与合同规定不符，投标方将协调原厂商来排除缺陷，修理或替换出现故障的部件、元件和设备，所有费用由投标方承担。

7、关于人员配置。讲标人员必须是投标方配备本项目经理，否则将视为自动放弃投标；同时，投标文件中需要提供配备本项目的工程师和实施人员的类似项目经历，以及专业能力 证明。

8、投标方须具有厂商针对百年人寿项目原厂授权。

三、报价

1) 1.投标人应提供完整详尽的计划方案、详细报价（单价、数量、总价等），以及付款方式。

第四部分　投标文件格式

附件 1：项目投标书

致：百年人寿保险股份有限公司

根据贵方为**百年人寿 2015 年度 IT 设备-网络安全项目**招标邀请，签字代表_____(全名、职务)经正式授权并代表投标人_____(投标人名称、地址)全权办理对上述项目的投标、谈判、签约等具体工作，并签署全部有关的文件、协议及合同。

提交下述文件正本一份和副本一式二份。

1.投标价格表。

2.公司基本情况材料及资格证明文件复印件。

据此函，签字代表以及投标人宣布同意如下：

1.投标人将按招标文件的规定履行合同责任和义务。

2.投标人已详细审查全部招标文件，包括修改文件(如有的话)以及全部参考资料和有关附件。我们完全理解并同意放弃对这方面有不明及误解的权利。

3.投标自提交投标文件的截止之日起有效期为 30 日。

4.投标人同意提供按照贵方可能要求的与其投标有关的一切数据或资料，完全理解贵方不一定要接受最低价的投标或收到的任何投标。

5.与本投标有关的一切正式往来通讯请寄：

地址：　　邮编：

电话：　　传真：

投标人代表签字：

投标人代表职务：

投标人名称：

(公章)：

日期：　　年　　月　　日

全权代表签字：

附件 2：网络安全采购项目技术参数及其投标机构表

WAF 产品参数：

指标项	指标要求
规格	标准专用千兆硬件平台 标配 1+1 冗余电源，电源可热插拔
网口数量	标配： 4*工作口（2*GE 电口，2*GE 光口），端口可扩展
性能参数	网络吞吐量系统最高处理能力 6000Mbps 应用吞吐量不小于 6000Mbps HTTP 并发连接 30 万 HTTP 新建连接(CPS)3 万
部署方式	透明桥部署：防护口不占用 IP 地址，实现完全透明部署，无需以先终结用户的 TCP 会话后再发起新的 TCP 会话到服务器方式处理，并支持路由不对称场景
	透明代理部署：防护口不占用 IP 地址，实现应用层透明部署，支持 TCP 连接复用，并优化服务器会话处理改善服务器处理性能
	端口镜像部署：镜像服务器流量即可实现安全审计和告警
	反向代理部署：可支持代理和路由牵引两种模式，客户端源 IP 可采用透明和非透明两种转发机制，非透明可指定字段进行识别，支持多台 WAF 设备冗余和集群部署
	路由模式部署：可支持静态路由、动态路由分发，无缝路由切换
	支持链路聚合，提升网络带宽、增加容错性和链路负载均衡
	支持 VLAN 子接口，业务口可承载多个 VLAN 通道
高可用性	支持全透明集群模式、主-主模式、主备模式、硬件 BYPASS、软件 BYPASS
保护对象	支持多条链路数据的防护，防护网段数量不限
	支持以域名和 IP 多种方式进行防护
	支持 ipv4/ipv6 双协议栈
WEB 服务自发现	支持 WEB 站点服务自动侦测功能
	支持识别 VLAN 信息
防御功能	能够识别恶意请求含：跨站脚本(XSS)、注入式攻击（包括 SQL 注入、命

	令注入 、Cookie 注入等)、跨站请求伪造等应用攻击行为
	能够识别服务端响应内容导致的缺陷：敏感信息泄露、已有的网页后门、错误配置、目录浏览等缺陷
	能基于访问行为特征进行分析，能识别盗链、爬虫攻击的能力
	能识别网站中的网页木马程序，通过策略可防止木马网页被用户访问
	内置主流 Webshell 特征库，对上传内容进行检查，防止恶意 Weshell 上传
	支持丰富的自定义规则，可以针对多个条件组合，形成深度的 WEB 防护规则
	支持服务器隐藏 可配置删除服务器响应头信息
	支持 Cookie 安全机制，支持 Cookie 自学习 支持 Cookie Httponly 支持 Cookie 防篡改、防劫持
智能自学习功能	支持网站自学习建模功能，能通过自学习形成网站 URL 树； 通过自学习能生成安全防护策略； 通过自学习能发现参数的名称、类型、匹配频率； 可配置匹配到自学习特征后放行； 可配置匹配不到自学习特征直接阻断请求；
智能攻击者锁定	支持智能识别攻击者，对网站连接发起攻击的 IP 地址进行自动锁定禁止访问被攻击的网站 可配置攻击者识别策略和算法 可配置攻击者锁定时间 可配置将攻击者直接加入网络黑名单 可展示攻击者发生的时间和攻击者所在的地理位置
虚拟补丁自动生成	支持导入扫描器结果形成 WAF 策略 扫描器扫出的漏洞信息可直接导入 WAF，形成专用防护规则
防御动作	针对触发安全规则的行为进行阻断并发出告警页面

	告警页面支持重定向至其它 URL
	能将攻击者列入网络黑名单进行网络阻断该 IP 的访问
	对攻击报文丢弃
WEB 访问行为合规	支持对访问流程的校验 可配置页面合规页面流程 可配置页面思考时间 发现访问违反合规的直接被拦截并产生告警日志
CC 防护功能	支持多种算法检测方法：对指定 URL 访问速率、对指定 URL 访问集中度检测 支持多种条件匹配算法：可基于 URL、请求头字段、目标 IP、请求方法等多种组合条件进行检测 检测对象支持 IP 或 IP+URL 算法,IP 可支持 X_Forwarded-For 字段解析，并支持自定义检测字段功能 支持挑战模式,客户端访问时 WAF 发起 302 重定向与 js 挑战验证是真实客户还是 CC 工具发起的访问 支持学习业务流量模型，在业务流量异常时开启 CC 防护，并支持启动配置阈值 支持基于地理位置的识别，可设置不同地理区域的检测算法 支持统计访问流量信息，进行人机对抗
篡改监控	系统提供防篡改功能,能够防止被篡改内容被浏览者访问到,一旦检测到被篡改，实时发送告警信息给管理员。
安全审计	能详细记录攻击事件的 HTTP 请求头信息，含请求的 URL、UserAgent、POST 内容，cookie 等所有的请求头内容
	能详细记录服务器响应头信息，服务器响应内容
日志分析	根据产生的安全日志进行智能分析，提高人工分析效率，减小规则误判概率
报表	根据 PCI-DSS 要求，对用户的应用进行合规性评估，生成合规报表

	支持自定义报表、定时报表、支持各类导出格式（WORD,PDF 等）
	报表可自动发至管理员邮箱
告警方式	支持 Syslog、手机短信、邮件等多种告警方式
访问审计	具备审计网站正常访问流量的能力，提供按小时，日期、月份生成报表
	能记录、查询所有用户对网站的访问情况
	能分析出访问量最大的 URL，IP 地址
	能分析出访问流量最大的文件类型
加速功能	系统内嵌应用加速模块，通过对各类静态页面及部分脚本高速缓存，提高访问速度
	支持响应内容压缩，并支持对压缩的响应内容识别
SSL 透明代理	支持 HTTPS 服务器的防护，可支持第三方认证机构颁发的证书链，WEB 应用防火墙前端与后端均为 HTTPS 加密链路，实现 HTTPS 应用系统的防御
	部署在 SSL 网关后面，能够解析到真实的访问者 IP，并能对真实的 IP 进行防护和阻断
负载均衡	工作在代理模式时，对保护的多台负载 WEB 服务器，达到平均分发、按比例分发、热备等多种负载均衡模式。
设备管理	配置变更时不影响在线业务
	规则库支持手工、在线升级两种方式，在线升级可支持规则定时检查新版本和在线更新，确保 WAF 能够针对新型的、突发型的 Web 攻击进行防护
	支持 HTTPS 方式进行设备管理
	设备管理采用管理员与审计员分离
	操作界面支持全中文界面
	支持集中管理，对多台 WAF 进行统一管理，实现日志收集、策略分发等功能
	支持 LDAP 认证
	与风暴中心交互，对用户安全情况进行分析并提供安全预警、反馈机制

网站防篡改产品参数：

基本要求	指标
产品及公司资质	公安部检测报告以及销售许可证书，软件著作权证书。
产品形态	产品为软件。
OS 类型、版本	支持 Windows Server2000/2003/2008/XP/Unix/Linux/等。
WEB 发布类型	IIS、Apache、Weblogic、Tomcat、WebSphere 等所有主流的 Web 服务器。
管理模式	C/S 架构，可以支持多个客户端管理。
核心技术	采用基于文件过滤驱动保护技术、事件触发机制相结合方式。
功能指标	

类别	子类	指标
日志功能	系统日志功能	系统能够对用户操作、文件操作和修改、安全日志以及策略配置事件进行完整日志记录。
	日志查询	系统支持日志记录查询及导出，支持 excel 报表导出查询。
	日志统计分析	系统需提供独立的日志统计分析软件,根据操作类型,篡改文件等提供数据统计。
	网管支持	系统日志支持 SYSLOG 接口，与网管平台结合。
防篡改功能	对文件的保护能力	支持各类网页文件的保护，包括静态和动态网页以及各类文件信息。
	对文件夹保护功能	支持对指定文件夹以及子文件夹的保护，避免上传非法文件及木马等恶意文件或插入恶意代码。
	篡改恢复功能	支持篡改后的自动恢复功能，恢复不依赖访问事件，直接由篡改动作触发恢复机制进行恢复。
	第三方支持	系统能够与所有第三方发布系统无缝结合，做到全自动发布。
	支持断线检测	系统配置完成后，系统后台运行，支持断线检测。
	支持断线监控保护	系统支持在断线情况下对网页文件目录的防护功能。
	支持进程管理	系统支持黑白名单设置功能，提供进程黑白名单设置。(需提供功能截图)
	支持服务监控	系统支持对服务进行监控功能。(需提供功能截图)
同步功能 系统管理	网页文件自动同步功能	系统可以从本地或异地备份文件夹自动同步到监测目录内。
	支持手工文件同步	系统支持手工文件同步功能。(需提供功能截图)
	支持手工文件备份	系统支持手工指定文件或文件夹从监测目录到指定目录的备份
	支持增量备份	系统支持增量备份功能。
	支持管理端上传下载功能	系统支持通过管理端受限用户进行文件上传下载功能。(需提供功能截图)
	许可机制认证	系统支持添加许可路径，排除保护内容。
	支持手工文件同步	系统支持手工文件同步功能。

	支持各种发布工具或发布方式	系统支持各种发布工具或发布方式。
	支持内容管理系统	系统支持内容管理系统。
	支持网络异常的自动恢复	系统支持网络异常的自动恢复。
	支持发布失败的自动重发	系统支持发布失败的自动重新发布。
	支持 SSL 安全协议进行通信和文件传输	系统支持 SSL 安全协议进行通信和文件传输，保证通信过程安全性。
	支持多虚拟主机 / 目录的并发同步	系统支持多虚拟主机 / 目录的并发同步功能。
	支持跨平台自动同步	系统支持跨操作系统平台的同步。
	支持一对多的自动同步方式	系统支持文件变化自动同步到多个 Web 服务器。
	网站管理	可支持对 web 服务器的远程维护管理功能，如远程接管、远程唤醒、远程关机、远程用户注销等。(需提供功能截图)
	网页分类	支持对各类网页文件分类。
	实时规则生效	策略下发后，无需重启服务器，实时生效。
	一对多管理	系统支持高效的一对多集中管理模式。
	服务器性能监控	支持对服务器性能实时监控功能，包括：内存、CPU 占用率等。(需提供功能截图)
	服务器实时信息监控	支持对服务器实时信息监控，包括：实时进程，服务信息，系统日志。(需提供功能截图)
用户管理	支持多用户分级	系统需支持用户权限分级,只有日志管理员才可查看管理员操作日志,可以设立多个基于文件目录的受控管理员。
自身安全性	通信保护	指系统各个模块之间、进程之间的通讯、交互和自身配置均采用加密传输和保护。
	卸载密码保护	卸载时需要提供管理员口令才可执行。(需提供功能截图)
	文件保护	支持对系统关键配置信息进行加密保护。
	备份目录保护	支持对备份目录文件的保护。(需提供功能截图)
	系统文件保护	支持系统安装文件保护功能。(需提供功能截图)
可扩展模块	保护动态页面模块	能够有效防止 SQL 注入攻击、跨站攻击、溢出代码攻击、对危险文件类型的访问、对危险系统路径的访问、特殊字符构成的 URL 利用、防止构造危险的 Cookie 等。
报警方式	声音报警	支持声音提示报警，对非授权用户篡改网页提供实时声音报警。
	邮件报警	支持邮件提示报警，对非授权用户篡改网页提供实时邮件报警提示。
	报警提示	系统支持报警提示框，对对非授权用户篡改网页提供实时报警框弹出提示。

性能指标	
类别	**指标**
响应时间要求	当网站文件遭到篡改恢复最短时间小于 2ms。
最多可保护对象	系统能够保护站点的最大文件和目录的数量不限。
最大保护目录深度	系统能够保护站点的最长路径不得小于 10 级。
资源占用率	系统运行过程中，被保护主机的 CPU 资源占用率和内存占用率小于 2%。

附件三：投标价格表

投标人名称：

项目名称： **百年人寿 2015 年度 IT 设备-网络安全项目**

招标编号： **AEONLIFE-IT-2015-035**

包一：

序号	产品型号	产品描述	单价 (人民币)	数量	投标总价 (人民币)
1		**WAF 产品**		2	
2		**网站防篡改产品**		2	
3					
总计					

附件 4：投标人基本情况及资格证明文件

公司基本情况

1.公司名称：_____ 电话号码：_____

2.地址：_____ 传真：_____

3.注册资金：_____ 经济性质：_____

4.营业注册执照号：_____

(随本表格附交一份最新营业执照副本的复印件并加盖公章)

5.公司简介

(自行描述)

6.其它