(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 105956460 A
(43)申请公布日 2016.09.21

(21)申请号 201610313523.0

(22)申请日 2016.05.12

(71)申请人 浪潮电子信息产业股份有限公司
地址 250101 山东省济南市高新区浪潮路1036号

(72)发明人 张彬

(74)专利代理机构 济南信达专利事务所有限公司 37100
代理人 姜明

(51)Int.Cl.
G06F 21/45(2013.01)

权利要求书1页 说明书3页 附图1页

(54)发明名称

一种信息安全管理的权限系统

(57)摘要

本发明提供一种信息安全管理的权限系统，属于信息技术领域，本发明包括：(1)终端、(2)管理系统、(3)模块、(4)业务、(5)数据、(6)业务权限、(7)数据权限。将权限细分为业务权限与数据权限。通过将三权分立的思想深化用运到管理系统的权限设计上，将权限系统中各个角色的权限范围更加细化，并且使得各个角色间相互制约的关系。

			系统管理员	安全管理员	审计管理员
安全中心	首页		√	√	√
资产管理	客户端管理	客户端检索、客户端配置等	√		
		客户端备注、描述	√		
		客户端查询	√		
	属性管理	属性添加、删除、修改	√		
		属性查询	√		
	分组管理	分组添加、删除、修改	√		
		分组查询	√		
平台配置	用户管理	用户信息设置	√		
		身份验证设置	√		
		客户端权限分配	√		
	授权管理	License 查询、导入、删除	√		
	其他配置	日志存储配置（大小、天数限制）	√		
	升级	管理端升级补丁	√		
策略管理	策略管理	策略查询		√	
		策略添加		√	
		策略删除		√	
		策略修改		√	
	策略配置	策略配置下发		√	
日志报表	操作日志	查看（浏览/查询）		√	
	报表管理	生成自动报表		√	
		手动生成报表		√	
		查看报表		√	
		报表配置		√	
	审计管理员操作日志	查看（浏览/查询）	√		
	其他管理员操作日志	查看（浏览/查询）			√

CN 105956460 A

1.一种信息安全管理的权限系统，其特征在于包括：

(1)终端、(2)管理系统、(3)模块、(4)业务、(5)数据、(6)业务权限、(7)数据权限；

其中

(1)、终端：信息管理系统所要管理的最小单位；

(2)、管理系统：为了完成一个信息安全管理目标建立的管理系统，管理的手段是通过对信息的管理完成；系统通过对管理的信息进行分类分为了相应的模块，每一个模块都对应着一类信息；

(3)、模块：管理系统的模块是相似相近的功能组成的功能集合；

对一个信息安全管理系统而言，模块基本可以分为以下几块：(3.1)、平台配置：配置管理系统的基本信息；(3.2)、资产管理：管理系统涵盖的资产：个人终端、服务器等；(3.3)、安全中心：是对当前安全情况的时时展现；(3.4)、日志报表：是对整个系统的日志和报表的管理；

(4)、业务：管理系统为了完成一个目标需要组织数个模块所涵盖的信息内容进行加工、处理；这一过程成为一个业务；

(5)、数据：系统管理的信息涵盖系统本身的信息和所管理的终端的信息；

(6)、业务权限：某一业务需要管理系统中一个或数个模块的管理权限；细分信息系统的模块，分析业务需求后可以针对一个业务组成一个权限的需求，最终形成了一组针对管理系统模块的权限划分，这一权限划分称为业务权限；

(7)数据权限：管理系统所管理的最小单位的信息以及信息系统本身的配置信息等都是系统的资源也是系统中的数据；这些数据根据使用的目的不同，可以划分为不同的组，这些分组对应着一个管理权限范围；这一管理权限范围成为数据权限；

管理系统通过对模块管理权限的划分形成了业务权限，通过对业务权限进行组织与划分形成了业务权限；针对系统本身的数据以及所管理终端的数据进行划分形成了数据权限；最终通过对业务权限和数据权限进行分析建立了角色，每个角色有相应的业务权限和数据权限以完成其职能的基本要求。

2.根据权利要求1所述的系统，其特征在于，终端可以是一台个人PC、一台服务器或一台虚拟主机。

3.根据权利要求1所述的系统，其特征在于，系统本身的用户信息和配置信息，所管理终端的配置信息都是数据。

一种信息安全管理的权限系统

技术领域

[0001] 本发明涉及信息技术领域，尤其涉及一种信息安全管理的权限系统。

背景技术

[0002] 随着信息技术的发展，特别是云计算、大数据等新型技术的发展，信息安全的要求越来越高，而信息安全管理系统要管理的终端在数量和种类上也越来越多。这对系统本身的安全性和管理的合理性都提出了更高的要求。必须在保证系统本身安全性的要求上，是的管理系统在使用上更加方便合理，将复杂的安全事件转化为简单的视图。

发明内容

[0003] 为了解决该问题，本发明提出了一种信息安全管理的权限系统，将权限细分为业务权限与数据权限。通过将三权分立的思想深化用运到管理系统权限系统的设计上，将权限系统中各个角色的权限范围更加细化，并且使得各个角色间相互制约的关系。此外在分权分域的思想基础上对系统的数据权限进行了划分。

[0004] 本发明的技术方案是：

一种针对信息安全管理系统的权限模块

(1)终端(2)管理系统(3)模块(4)业务(5)数据(6)业务权限(7)数据权限

(1)、终端：信息管理系统所要管理的最小单位，可以是一台个人PC、一台服务器或者一台虚拟主机等。

[0005] (2)、管理系统：为了完成某一信息安全管理目标建立的管理系统，管理的手段是通过对信息的管理完成。系统通过对管理的信息进行分类分为了相应的模块，每一个模块都对应着一类信息。

[0006] (3)、模块：管理系统的模块是某些相似相近的功能组成的功能集合。对一个信息安全管理系统而言，模块基本可以分为以下几块：(3.1)、平台配置：配置管理系统的基本信息；(3.2)、资产管理：管理系统涵盖的资产：个人终端、服务器等；(3.3)、安全中心：是对当前安全情况的时时展现；(3.4)、日志报表：是对整个系统的日志和报表的管理。

[0007] (4)、业务：管理系统为了完成某一目标需要组织几个模块所涵盖的信息内容进行加工、处理。这一过程成为一个业务。

[0008] (5)、数据：系统管理的信息涵盖系统本身的某些信息和所管理的终端的某些信息，例如系统本身的用户信息和配置信息，所管理终端的配置信息等。这些信息都是数据。

[0009] (6)、业务权限：某一业务需要管理系统中某一个或几个模块的管理权限。细分信息系统的模块，分析业务需求后可以针对某一业务组成一个权限的需求，最终形成了一组针对管理系统模块的权限划分，这一权限划分称为业务权限。

[0010] (7)数据权限：管理系统所管理的最小单位的某些信息以及信息系统本身的某些配置信息等都是系统的资源也是系统中的数据。这些数据根据使用的目的不同，可以划分为不同的组，这些分组对应着一个管理权限范围；这一管理权限范围成为数据权限；

管理系统通过对模块管理权限的划分形成了业务权限，通过对业务权限进行组织与划分形成了业务权限。针对系统本身的数据以及所管理终端的数据进行划分形成了数据权限。最终通过对业务权限和数据权限进行分析建立了角色，每个角色有相应的业务权限和数据权限以完成其职能的基本要求。

[0011] 在业务权限上，将信息安全管理系统的业务权限细分为三大类：一、系统平台配置类型；二、安全事件及相关类型；三、审计类型；通过这三类区分形成了三种角色：系统管理员、安全管理员和审计管理员。这一设计符合了三权分立思想。使得不同角色的系统使用者各司其职。借鉴了分权分域的思想，对权限进行了细分，除了上面提到的业务权限还提出了数据权限，通过数据权限的划分，更加方便的管理大量的终端。

[0012] 本发明提出的基于三权分立和分权分域思想的权限系统正是应对信息安全管理信息本身的特殊要求而成的。这一权限模块加强了管理系统本身的安全性，并且针对大量、海量终端的管理，通过数据权限的划分简化了管理的难度。

附图说明

[0013] 图1是本发明的权限示意图。

具体实施方式

[0014] 下面对本发明的内容进行更加详细的阐述：

本发明包括：(1)终端、(2)管理系统、(3)模块、(4)业务、(5)数据、(6)业务权限、(7)数据权限；

(1)、终端：信息管理系统所要管理的最小单位；

(2)、管理系统：为了完成一个信息安全管理目标建立的管理系统，管理的手段是通过对信息的管理完成；系统通过对管理的信息进行分类分为了相应的模块，每一个模块都对应着一类信息；

(3)、模块：管理系统的模块是相似相近的功能组成的功能集合。对一个信息安全管理系统而言，模块基本可以分为以下几块：(3.1)、平台配置：配置管理系统的基本信息；(3.2)、资产管理：管理系统涵盖的资产：个人终端、服务器等；(3.3)、安全中心：是对当前安全情况的时时展现；(3.4)、日志报表：是对整个系统的日志和报表的管理；

(4)、业务：管理系统为了完成一个目标需要组织数个模块所涵盖的信息内容进行加工、处理；这一过程成为一个业务；

(5)、数据：系统管理的信息涵盖系统本身的信息和所管理的终端的信息；

(6)、业务权限：某一业务需要管理系统中一个或数个模块的管理权限；细分信息系统的模块，分析业务需求后可以针对一个业务组成一个权限的需求，最终形成了一组针对管理系统模块的权限划分，这一权限划分称为业务权限；

(7)数据权限：管理系统所管理的最小单位的信息以及信息系统本身的配置信息等都是系统的资源也是系统中的数据；这些数据根据使用的目的不同，可以划分为不同的组，这些分组对应着一个管理权限范围；这一管理权限范围成为数据权限；

管理系统通过对模块管理权限的划分形成了业务权限，通过对业务权限进行组织与划分形成了业务权限；针对系统本身的数据以及所管理终端的数据进行划分形成了数据权

限；最终通过对业务权限和数据权限进行分析建立了角色，每个角色有相应的业务权限和数据权限以完成其职能的基本要求。

[0015] 本发明对信息安全管理系统的角色进行分析，在保证系统运行状况下形成了三个角色：系统管理员、安全管理员、审计管理员；这样划分的原则是：每一个角色都有一个管理目标，系统管理员的管理目标是对管理系统进行管理；安全管理员的管理目标是对安全事件及相关进行管理；审计管理员的管理目标是审计其他角色的操作行为，这样的划分完成了三权分立。

[0016] 此外，本发明中，系统管理员可以管理用户和资产以及用户能够管理的资产范围，通过这一操作系统管理员可以制约控制安全管理员的操作。审计管理员通过审计系统管理员和安全管理员的操作日志监督了系统管理员和安全管理员的操作行为。并且，考虑到系统管理员本身的操作也需要人审计，将审计管理员的操作日志的管理权限交给系统管理员来完成。这样三种角色间互监督，保证了平台本身的安全性。

[0017] 最后，通过系统管理员为安全管理员划分数据权限（系统管理员授权的终端安全管理员才能管理），方便在终端数量巨大的时候进行管理。

			系统管理员	安全管理员	审计管理员
安全中心	首页		√	√	√
资产管理	客户端管理	客户端卸载、客户配置等	√		
		客户端备注、描述	√		
		客户端查询	√		
	属性管理	属性添加、删除、修改	√		
		属性查询	√		
	分组管理	分组添加、删除、修改	√		
		分组查询	√		
平台配置	用户管理	用户增删改查	√		
		身份鉴别设置	√		
		客户端权限分配	√		
	授权管理	License 查询、导入、删除	√		
	其他配置	日志存储配置（大小、天数、阈值）	√		
	升级	管理升级补丁	√		
策略管理	策略库管理	策略查询		√	
		策略添加		√	
		策略删除		√	
		策略修改		√	
	策略配置	策略配置下发		√	
日志报表	特性日志	查看（浏览/查询）		√	
	报表管理	生成自动报表		√	
		手动生成报表		√	
		查看报表		√	
		报表配置		√	
	审计管理员操作日志	查看（浏览/查询）	√		
	其他管理员操作日志	查看（浏览/查询）			√

图1