税务电子数据安全保护平台
技术白皮书

深圳市联软科技有限公司

2015 年 5 月

版权声明

支持信息

感谢您选择并关注联软科技数据防泄露产品!

公司地址： 深圳市南山区高新区中区高新中一道9号软件大厦10层1001-1003室

服务热线：**400-6288-116** 邮编：518000

如果您希望得到更多的关于联软科技的产品信息、技术支持以及产品的报价等信息，请您查阅我公司网站：**http://www.leagsoft.com**。

目录

全文介绍

随着税收信息化建设的全面和深入开展，税务信息系统积累并存储了大量的敏感信息数据，在税收管理和服务中发挥着重要作用，但税收数据安全风险也日益突出，加强数据安全管理成为当务之急。税收数据安全管理是针对税收数据在收集、处理、存储、检索、传输、交换、显示和应用等过程中的安全管理，重点是防范数据窃取、篡改和抵赖。

本技术白皮书通过全面分析终端业务数据在使用时各类泄露途径和传统数据防泄露技术的缺陷，探索出一套领先的、自主可控的终端数据防泄露解决方案，并已经过国地税系统实践的检验，安全可靠，切实可行。

第1章 概述

1、国家高度重视以敏感数据保护为核心的数据安全问题

当前，税务系统在网络与信息安全领域面临比以往更为严峻复杂的安全局面。国家税务总局和省级局应用集中的征管数据处理模式，内外网应用、外包租赁方式和政府行政审批中心集中服务等不同应用服务场景，导致高度集中的税收数据、纳税人商业秘密和个人隐私数据，面临的安全威胁也更加复杂严峻。全国人大常委会关于《加强网络信息安全保护的决定》的发布，更加明确了税务系统信息数据安全保护的责任义务。为此，国家税务总局先后下发了《税务工作秘密管理暂行规定》、《税务电子数据安全保护总体技术框架》、《税务系统业务数据处理管理方法》、《应用系统信息安全审核规范》和《税务系统信息安全等级保护基本要求》等一系列软件和数据安全规范制度，同步强化安全检查评估和应急演练，数据安全防护和管理体系初步形成。但应用终端数据安全管理，因受技术手段少、安全规范制度难以细化、人多难管和面临的应用及安全威胁场景复杂等因素制约，导致数据易泄露、事件难取证和安全责任难追究等。

2、传统的技术方案重在用户文档保护，对敏感业务数据保护不足

当前市场上传统的终端数据安全管理仅关注自身文档的安全，忽略了终端使用者访问业务系统而产生驻留终端的业务数据安全管控。此类数据正是终端使用者内外部业务工作流转的主要业务数据来源，其使用灵活、扩散渠道多，安全保护和监控难度巨大。联软科技通过理论应用研究和开发实践相结合的方式从税收征管系统应用最主要的使用对象（业务人员和最难管控的使用位置）即终端角度出发，首次将税收征管业务应用与最新的终端数据安全技术相融合，在不改变原有征管系统的前提下，开发出税收终端数据防泄露系统，实现了终端业务应用“合规进入，安全存储，加密传输，授权使用，审核输出，销毁彻底，流程记录，可视分析，安全管控”的数据安全管理目标，确保了涉税和内部管理敏感数据在业务终端上的使用安全。

第2章 数据防泄露技术介绍

目前主流的四类终端数据防泄露技术包括数据通道封堵技术、文档加解密技术、文档权限管理技术、数据泄露防护技术。

数据通道封堵技术是早期的技术，比较成熟，目前依然被大量使用，但其缺陷也非常明显，如用户安装一个双系统就完全失效了，类似于见招拆招的防护模式，不能解决根本问题。这类技术常见于主机安全审计类产品上。

文档加解密技术是当今国内比较流行的技术，比较成熟，大量应用于制造业，政府类机构使用者很少，但其缺陷也非常明显，如加解密客户端软件与操作系统的兼容性。这类技术常见于透明加解密类产品上。

文档权限管理技术是国外软件巨头所开发的技术，国内应用案例较少，发达国家也仅推行了10 年以上，效果不尽如人意，其最大的问题就是不能防范内部人员的主动式泄露数据，这与目前主要的数据泄露源头是内部的业务终端使用者相违背。这类技术常见于微软等公司的DRM产品上。

数据泄露防护技术是国外著名安全软件公司所开发的技术，国内应用案例较少，尤其是政府类机构鲜有应用，其最大的问题就是对中文内容识别的兼容性，以及2000 年起中国有关部门规定，为了保护国家利益和经济安全，禁止中国公司购买包含外国设计的加密软件产品，国内任何组织和个人都不得出售外国商业性加密产品。这类技术常见于美国赛门铁克和迈克菲的DLP产品上。

这四类技术的实现原理和优缺点对比（见表2-1）。

表 2-1 终端数据防泄露技术对比表

实现方式	数据通道封堵技术	文档加解密技术	文档权限管理技术	数据泄露防护技术
实现原理	通过客户端程序实现对各类数据外发或传输方式的封堵。例如，网络共享、邮件、即时聊天、移动存储、蓝牙、光驱刻录、随身WIFI、3G网卡等。	通过客户端程序实现对指定格式的文档自动加密和解密。	通过客户端程序实现对办公文档的使用授权包括读、复制、打印、存储、传送、编辑等。授权可附加约束条件，如权限作用时间、持续时间等。	通过客户端程序对数据的内容按关键字进行深度内容分析，按照统一安全策略，识别、监控和保护静态存储的数据、使用中或传输中的数据。
管控效果	不好，存在明显漏洞	较好。	不好，只能做访问控制，对访问后的泄密行为管控无能为力。	一般，只能阻止部分数据，数据输出后难以控制和追踪。
环境要求	较低，如果有新的外设需要封堵，就需要随时调整策略或升级系统，例如随身WIFI设备。	最高，对终端的磁盘分区格式、操作系统版本、防病毒软件都有严格要求。	低，如果有新格式的文档需要保护，需要单独进行二次开发。	高，对客户端资源开销较大。
运维成本	低，无需专人维护。	最高，需要专人维护。	较高，需要专人维护。	高，需要专家级人员维护。
优点	技术成熟、选择面广、易实施。	对文档可实现较严格管控。	实现起来较简单。	部署简单，可大面积使用。
缺点	防护效果差、漏洞多；容易导致终端用户抵触；降低工作效率。	无法对非文档类数据进行保护；文档加密后，带来导致数据恢复、检索、无法解密等方面的新问题；稳定性差，不适合大范围使用。	对有权限的人员主动泄露数据的行为，缺少管控；新增一类甚至一个版本的文档格式，就需要进行二次开发，成本高昂；需要改变用户使用习惯；权限管理复杂。	不符合中国国情；中文深度识别准确率不高、兼容性不好；运维复杂；投资大。

从表 2-1 分析得出，当前市场中主流的四类终端数据防泄露技术，没有一类技术是可以完全适合国内税务数据防泄露的需求。基于税务机关需要的是防止业务系统产生的敏感数据、终端存储的敏感数据以及流转、外发给其他单位敏感数据的需求，联软科技基于第四种数据泄露防护技术的理念，研发出了一套适合国内税务机关需求的数据安全保护平台。采用沙箱技术对存储、使用、传输中的数据进行监控和保护。通过对数据的分级、分类，精准定位敏感数据的使用边界，在使用边界赋予是否可复制、打印、截屏、外发等多种控制手段来实现数据的防泄露。

对于业务系统产生的敏感数据，通过加强对访问控制、实现业务系统敏感数据落地加密并赋予使用权限达到有效的防泄露，大大减少管理成本；

对于终端存储、流转、外发的敏感数据，通过对网络、存储介质、外设、打印和硬盘等各方面所存的风险点，辅以控制、加密和审计的手段，实现严密的数据防泄露。

第3章 数据的分级分类

显然，如果对税务机关内各种各样的海量数据全部进行同样级别的保护，等于没有任何保护。因此数据防泄露的一个基本点就是确定信息机密性的级别和类别。对于可以完全对外公开级别和非关键业务类型的数据，不需要任何的信息防泄露防护措施；对于关系到税务机关声誉的重要业务数据，应当严格控制其存储位置、使用方式和传输方式。

如何对信息进行分级、分类呢？最根本思想的是依据信息的内容来判断其机密性级别和类别。信息的管理者（如管理人员）可以根据个人或者税务机关相关规范来理解目前机关内所有信息的机密级别和类别。

3.1 数据的分级

数据的分级指根据数据某些特定指标值来进行级别的划分，如根据数据本身的敏感度、价值、泄露后造成的损失度等指标来定义级别。

如国家税务总局则根据数据受到破坏后对国计民生造成的危害性来划分数据的级别。主要分为三个级别，具体如下：

1. 数据被破坏或泄露后，对社会秩序和公共利益造成严重损害，或者对国家安全造成损害的，属于税务第三级数据。税务机关就需要对该级别的数据进行重点保护。
2. 数据被破坏或泄露后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全，属于税务第二级数据。税务机关也需要对该级别的数据进行重点保护。
3. 数据被破坏或泄露后，会对公民、税务机关和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益，属于税务第一级数据。税务机关应该对该级别的数据进行一般性保护。

从国家税务总局对税务数据的分级来看，分级的标准在于数据泄露所带来的风险，不同级别的税务机关对数据的级别定义不同，联软科技研发的 UniBDP 平

台支持数据分级标准和级别的自定义，可满足实际应用和发展情况。

3.2 数据的分类

数据的分类指按数据的种类、等级或性质等信息来分别归类，即按某种标准给数据贴标签，再根据标签来区分归类。如人按性别分为男、女两类。

国家税务总局则根据税收数据的业务敏感程度来对税务数据进行分类，主要分为三类，具体如下：

1. 核心数据，主要包括集中存储和处理的税收业务数据集。
2. 敏感数据，主要包括国家法律法规中明确规定要求保护的税务工作秘密数据，如纳税人个人隐私、纳税人商业秘密、第三方涉税敏感信息、税收统计分析数据和口令、密钥鉴别信息等。
3. 受控数据，主要包括属于税务工作秘密但在国家法律法规中尚未明确保护的税务相关数据，如人事、财务、纪检监察、信访举报、内部审计督察等信息，以及不宜公开的纪要、讲话、批示、报告、方案、视频、文档等信息，涉及全网、重要信息系统的关键技术资料（实施方案、配置参数、程序代码、全网拓扑图、核心网络 IP 地址规划、系统和设备运行日志和审计信息）等。

从国家税务总局对税务数据的分类来看，分类的标准在于数据的敏感性，那么，税务机关在实际的应用和发展情况中可能会有进一步的细化，联软科技研发的 UniBDP 平台支持分类标准和类别的自定义，可满足实际应用和发展情况。

3.3 实现原理

采用敏感信息检索技术，按关键字、正则表达式、数据标识符等多个复合条件的组合自动扫描存储在内网终端上的税收数据，根据多个条件的判断，最终判定数据的级别和类别。

数据的分级分类主要通过配置模板、实时检测、自动归类三个步骤来实现。

第一步，配置模板。税务机关根据《税务工作秘密管理暂行规定》（国税发[2012]102号）和《税务电子数据安全保护总体技术框架》（国税发[2014]129号）要求，再分析不同级别、不同类别税收数据的特征，最终确定税收数据分级、分

类的标准，采用正则表达式技术，在防泄露平台确定并配置税收数据分级、分类的特征模板。

- 如定义文件内容中包含“税务管理码 、征收计划、征收金额、税种、征税比率等”信息，那么就定义该文件的级别为第三级数据、类别为核心数据；
- 如定义文件内容中包含“税务管理码 、纳税人识号、注册地址、联系电话、国籍、税务管理机关、纳税人名称（英文）等”信息，那么就定义该文件的级别为第二级数据，类别为敏感数据；
- 如定义文件内容包含“讲话、批示、报告、实施方案、拓扑图、日志等”信息，那么就定义该文件的级别为第一级数据，类别为受控数据。

税收数据分级、分类关键字模板配置，除了基于文件内容之外，还可以基于文件类型、文件大小、文件创建时间、关键字存在文件中位置不同（正文、标题、页眉、页脚）等条件进行模板配置。

第二步，实时检测。配置好关键字模板后，防泄露平台根据指定的管理要求，对终端计算机上的数据进行定时检测。不但可以实时检测终端计算机上的数据，还可以检测包括所有外接USB移动存储设备内的数据、刻入光盘的数据、打印数据、通过网络邮件或通过即时消息发送的数据等。

第三步，自动归类。根据防泄露后台制定的“税收数据分级、分类关键字模板”清单，进行自动比对，如果该数据中包含清单中指定的关键字，则按照预先设定好的级别和类别给数据贴上标签，最后再对属于同一标签的数据进行归类，从而达到数据分级、分类的目的。可实现对Office、PDF、文本等类型文件的自动、智能识别和区分，也可以针对指定数据类型。

通过以上三个步骤实现税收数据的分级分类，整个过程，无需税务工作人员人工干预，相对税务工作人员来讲，是一个透明与自动的过程，实时高效。

所有的“安全”都是相对的，都是有边界的。对税务机关内所有的数据进行同样级别的安全保护，显然会牺牲系统运行效率、牺牲用户的方便性。所以，对税务机关的数据进行分级、分类就是确定数据防泄露的边界。针对不同级别、不同类别的数据进行不同的安全管控手段，采取“抓大放小”的建设原则，解决高级别、重要类型敏感数据的泄露，从而实现层次化数据防泄露架构的建设。

第4章 平台简介

税务电子数据安全保护平台（UniBDP：Unique Business Data Protection）通过对敏感税务电子数据的监控和保护，保证了敏感数据不被非法的存储、使用和传输，从而实现税务电子数据防泄露的目标；主要防范税务电子数据被非法复制、打印、截屏、外传等多种泄露手段。并提供基于时间、身份、非法行为、终端位置等详尽记录的系统。突破业务类型、数据库类型和文件类型的限制，在泄露防护、追踪定位以及安全取证等方面更精确、高效。

4.1 平台架构

如下图 4-1 所示，UniBDP 平台按照“疏导型”思路设计，采用终端守护和应用访问控制相结合的工作模式，从业务系统最主要的使用对象（业务人员、运维人员、开发人员），即终端角度出发，构建一套管控信息系统合规使用和业务数据不被非法存储、使用和传输的安全环境，实现“合规进入、安全存储、加密传输、授权使用、审核输出、销毁彻底、流程记录、可视分析、安全管控”的数据安全管理目标，确保重要业务系统和敏感数据在业务终端上的使用安全。同时具备“免改造、易实施、易使用、见效快”的技术优势。

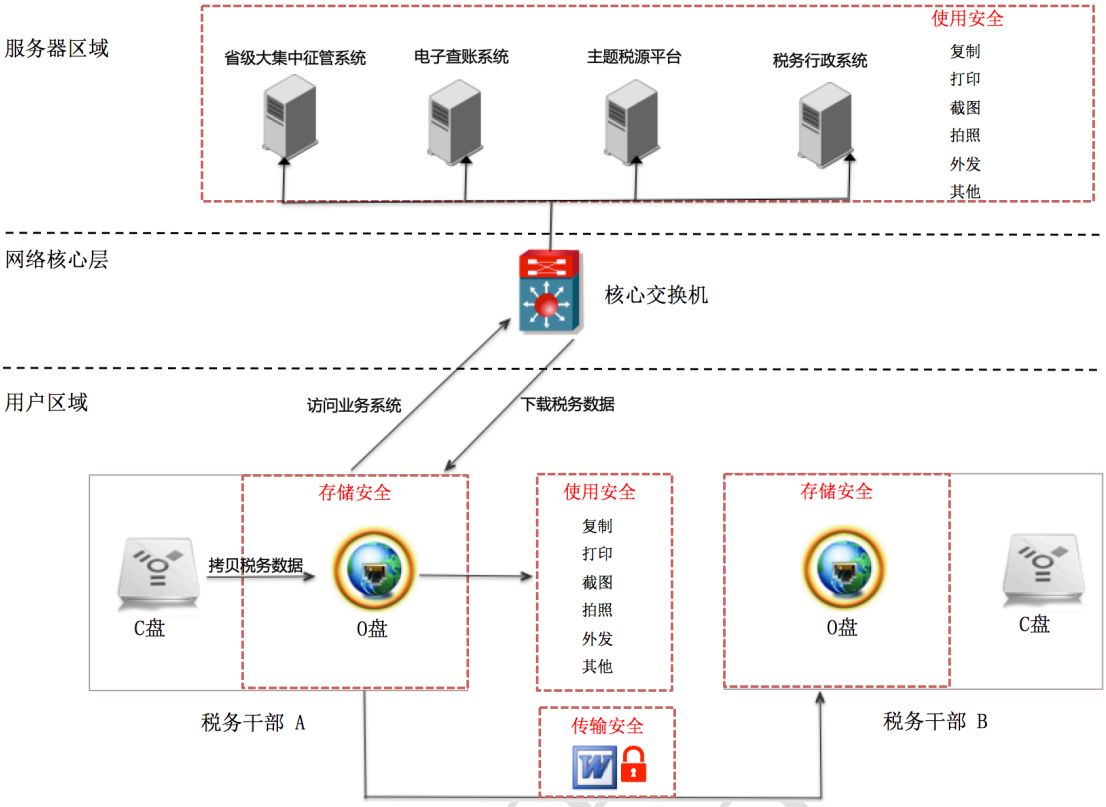

图 4-1 税务电子数据安全保护平台架构图

UniBDP 平台主要由三个部分组成：

1. 电子数据的存储安全

指的是电子数据存储的磁盘区域是安全可控的，该安全存储区域我们称之为 O 盘，所有和业务相关的敏感税务电子数据都要求存入到 O 盘，对 O 盘内数据的访问只能是授予了访问权限的用户。

2. 电子数据的使用安全

指的是税务电子数据在使用过程中的安全防护。包含对税收业务系统敏感数据的操作保护和落地到 O 盘内敏感税收数据的保护。主要是保护敏感数据不被被非法复制、打印、截屏、外传等。

3. 电子数据的传输安全

指的是税务电子数据在内部网络传输过程中都是采用加密方式进行传输，在保证数据的完整性、保密性时，还能够对数据的发送者进行身份验证。防止非法人员截取带来的安全隐患。

4.2 电子数据的存储安全

保证电子数据的存储是安全可控，保证税务电子数据的完整性、可用性和保密性。电子数据存储的磁盘区域就是 UniBDP 平台的 O 盘，O 盘，就是一个虚拟的磁盘区域，其读写操作的权限都是受后台配置的策略控制，主要用于终端电脑上业务数据的集中管理。其主要的数据来源为终端电脑其他磁盘区域和业务系统。

终端电脑其他磁盘区域，就是防泄露客户端根据规则自动区分和鉴别终端上其他磁盘区域的税收数据，并将其强制存入 O 盘，整个过程无需人工干预。

业务系统，就是当业务人员下载业务系统的敏感数据时，只能下载存储在 O 盘中，不能下载到其他的非 O 盘区域，从而保证业务系统落地数据的存储安全。

4.3 电子数据的使用安全

电子数据的使用安全主要分为在线电子数据（业务系统）的使用安全和离线电子数据（O 盘）的使用安全以及数据在流转过程中的使用安全三个部分。

在线电子数据使用安全，指的是税务干部登录业务系统，查询出敏感数据后，对敏感数据进行复制、下载、截图、拍照、打印等多种数据使用方式时的安全保护。在线对敏感数据的所有泄露操作都会受到平台策略的审核和控制。

离线电子数据使用安全，指的是税收敏感数据落地到 O 盘的数据，税务干部对 O 盘内敏感数据进行复制、截图、拍照、打印、外发等多种数据使用方式时的安全保护

数据流转使用安全，根据用户的职能或者税收数据的用途赋予其对应的操作数据权限。例如个人所得税岗位的人员之间可以传输和处理其职能范围内的与个人所得税相关的数据，不能接受其他部门发送的如与企业所得税相关的数据。保证数据不被非授权人员查看。在向第三方单位提供税收数据时，必须控制数据的打印和使用次数等相关权限，以保证数据的安全。

4.4 电子数据的传输安全

电子数据的传输安全，指的是税收数据在内部不同 O 盘之间的流转采用加密方式进行传输。当税收数据脱离 O 盘时，防泄露客户端就会对数据进行自动加密。当接收方将接收到的税务数据拷贝到自己的 O 盘时，系统就会自动的进行解密。保证数据在整个传输的过程中都是出于加密的状态。

第5章 平台主要功能

UniBDP 平台围绕电子数据生命周期开展，在创建、使用、传输、存储、销毁等各个环节，通过安全控制措施实现数据的保密性、完整性、可用性、可控性和不可否认性的安全目标，做到对外部攻击、信息泄露、篡改、越权和抵赖等威胁的防范。

UniBDP 平台中为保证电子数据安全操作使用，主要从以下几个方面进行全面的管控：合规进入、安全存储、加密传输、授权使用、审核输出、记录流程和可视呈现，构建一套综合性的防护平台。如图 5-1 所示：

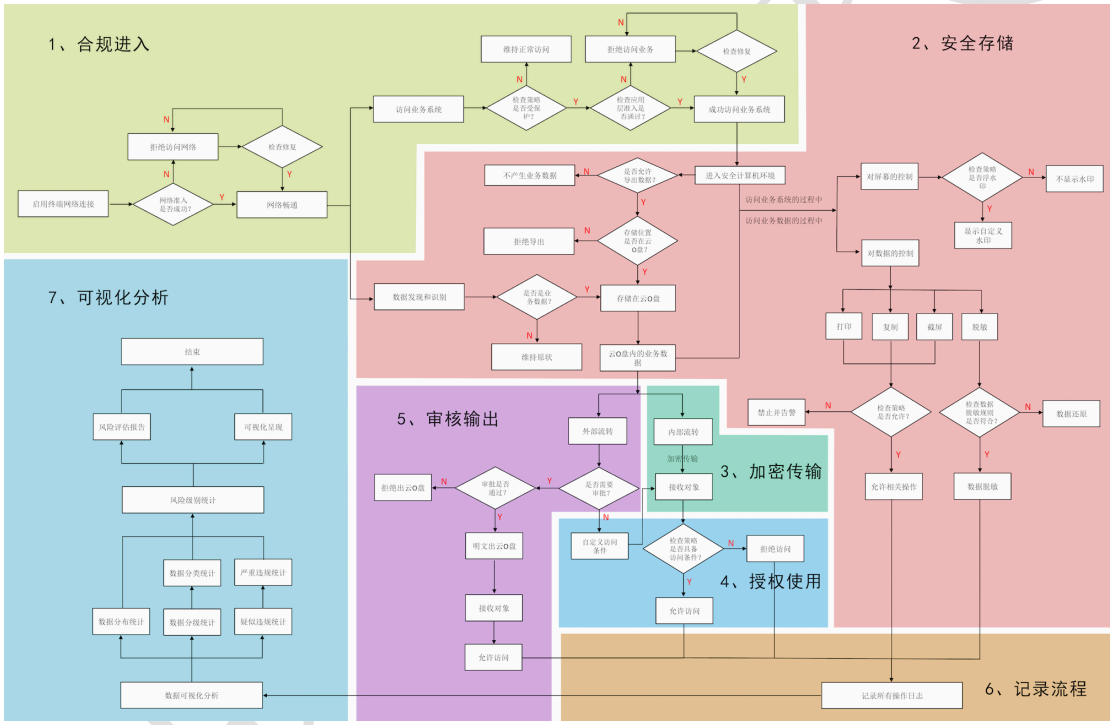

图 5-1 税务电子数据安全保护平台功能流程图

5.1 合规进入

应用层的合规进入的关键点为访问业务系统的业务账号、访问时间和访问业务系统的应用程序三种条件的判断。

对于业务账号， UniBDP 采用自主开发的工具，自动抓取通过特定进程登录特定地址时的 post 包，获取其登录的用户名，用于比对。亦可将业务管理帐号与终端的 ip 地址和 mac 地址进行绑定，当不符合绑定关系时，自动告警。

对于非工作时间段访问业务系统，UniBDP 自动记录其登录信息，用于事后分析。

对应用程序名称、进程名称、应用程序 crc 值等多个特征属性识别判断，判定用户采用符合规定的应用程序访问业务系统。

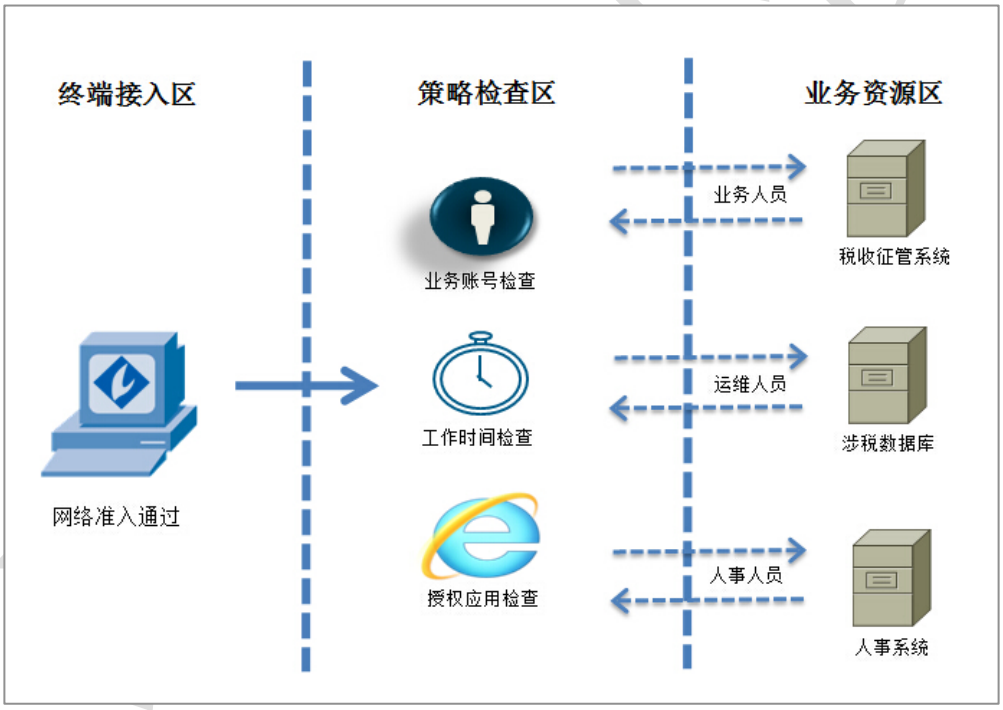

图 5-2 业务系统合规进入访问示意图

如上图5-2所示，在终端接入区，内网终端是通过网络层进行身份验证和网络层接入的安全检查，确定正常接入税务内网的的终端是合规终端；在策略检查区，主要是通过检查登录税务征管系统的登录账户、登录时间、登录软件进程等来判断访问者本次登录是否合规，三者缺一不可，否则就视为异常登录。在业务资源区，则是在通过网络层接入成功和防泄露策略检查以后，确定不同岗位业务

人员可以正常访问各自授权的业务系统，如人事部门相关人员登录人事管理系统。而在非授权的情况下，登录该账户未被授权的其他业务系统将会禁止登录。

5.2 安全存储

在 UniBDP 中，所有敏感数据都存放在 O 盘，O 盘拥有其独有的安全性、稳定性和先进性。

1. 安全性：O 盘对应的实体文件是加密的。当应用程序读写 O 盘的文件时，O 盘的内核驱动会在 O 盘的文件和实体文件之间自动加解密。因此，即使丢失物理硬盘也不会导致 O 盘的数据泄露。只有指定的合法进程才能访问 O 盘，而这些进程一旦打开了 O 盘里面的文件，就会立即进入受控状态，一切可能导致数据泄露的行为都会根据策略做不同程度的控制。策略配置的行为主要有：允许、审计、禁止、审批。
2. 稳定性：O 盘的工作原理是：在本地物理磁盘上创建一个文件（下面称为实体文件），其大小即为 O 盘的容量，然后把该文件映射成一个盘符，对该盘符的操作和正常盘符没有区别，只是读写 O 盘的据会被重定向成读写上述实体文件，由此可看出，O 盘的可靠性和操作系统的文件系统是一致的。
3. 先进性：云端服务器的硬盘或硬盘阵列中的容量，按照一一对应关系，为每个用户单独分配一块自由空间。同时，云端服务器也会自动的将该自由空间，以网络映射的方式映射为一个本地 O 盘到用户的终端计算机，并最终以云 O 盘盘符名称的方式展现出来。

5.3 加密传输

数据流转过程中的加密传输：税收数据在不同O盘之间的流转是以加密方式进行，保证了税收数据在不同O盘之间流转的保密性。此时源点是O盘，终点是另一个O盘。税收数据内部流转加密传输方式采用了端对端加密传输，可以采用DES、AES、RC 等对称算法，也可以采用RSA、DSA、ECC 等非对称算法，同时也可以采用国家商用密码管理办公室指定的SM4分组密码算法。

5.4 授权使用

UniBDP 可以对多种类型的使用操作进行授权管控，具体包括：

1. 安装、卸载软件：对安装了不应该安装的软件（如：游戏），或者卸载了不应该卸载的软件（如：防病毒软件）；
2. 外联授权：支持对 USB 硬盘、Modem 拨号、无线通讯、红外、蓝牙、同时使用内外网卡等硬件设备的授权使用；
3. 网络访问控制授权：访问的网站、使用外部邮件服务器、从本机网络 COPY 机密文件的授权；
4. 网络资源的授权：对网上聊天、BT 下载的授权；
5. 文件操作行为授权：对本机硬盘、注册或未注册 U 盘软盘、网络共享目录的文件读写操作的授权。
6. 对上述软硬件和行为的授权，一方面可以防止内部保密文件的外泄，同时也是对网络安全的保护。 UniBDP 支持离线管理，可以支持电脑在离开网络之后（如：离开单位），各种管理策略（如：禁止使用 USB 存储）仍然有效。

5.5 审核输出

当税务工作人员需要外发税收敏感数据到第三方单位时，UniBDP支持根据税务机关定义的审核标准对数据进行审核审批。

1. 自动审批：指定用户外发策略为自动审批，用户外发时需要提出外发申请，系统自动审批通过，文件自动从出盘待审批文件夹移动到出盘审批通过文件夹。系统备份外发文档并在日志中记录外发操作。
2. 人工审批：指定用户外发策略为人工审批。用户提出外发申请，外发申请的文档上传给到服务器，由审批管理员审核文件是否能外发；审批通过后，文件自动从出盘待审批文件夹移动到出盘审批通过文件夹。
3. N小时无人审批，系统会自动切换为自动审批。用户提出外发申请，外发申请的文档上传给到服务器，如果定义的时间段内没有审判员审批，系统则会自动切换到自动审批状态，审批通过后，文件则会自动从出盘待审批文件夹

移动到出盘审批通过文件夹。

审批可支持多个审批服务器、多个审批管理员，可由熟悉业务的部门管理人员查看、审批文件。

5.6 销毁彻底

在 UniBDP 的防泄露客户端中，集成有专业级的文件销毁工具，用户可以选择性的对高敏感的税务数据进行销毁，销毁方法就是将该文件所在簇上的数据用垃圾数据全部替换掉，这样就算能够找到这些簇，得到的也是一些无用的数据，不能恢复原来的文件。同时将该文件的名字、创建时间、大小等信息全部清零。数据粉碎后，关于该文件的一切信息（文件目录项、FAT 表中登记的项、文件所占用的簇等）都会被清零，都不能被恢复。

5.7 流程记录

UniBDP 系统能全方位地记录税收数据使用过程中所发生的所有可记录的事项。如网络层准入的流程记录、应用层准入的流程记录、征管系统登录记录、文件打印的记录、数据在线导出的记录、数据的内部流转过程记录、外部流转过程记录、终端上文件操作过程的记录。

对税收数据的在线和离线使用流程记录，可采用精准监督、合理控制、即时预警、完整报告四个环节来实现。

1. 精准监督

审计的结果要准确到人、设备、位置、时间和动作等。从审计准确精度入手，做到五审， 即“审用户、审角色、审权限、审设备、审行为”。

a) 审用户主要针对访问网络中各项业务的用户。对于需要访问业务资源的用户，采取了身份认证系统， 当认证用户得到确认后， 方可进行业务的操作。

b) 审角色是根据业务用户在业务流程中所扮演的角色进行分类（主要是基于岗位进行分类），从而有效地定义可读性更强的审计规则与策略。由于审计记录不仅包括源 IP、目的 IP 等原始信息， 还包含用户的角色或者身份信息，

根据审计记录中的用户角色，可以得到更有意义的审计结果。相关的用户角色或者身份信息还可用于辅助界定事件责任。

c) 审权限主要包括用户权限和操作权限， 当每一个用户被赋予角色后， 角色就有执行操作的可能， 在执行操作的过程中，就需要有权限设立， 从而达到规范角色行为的目的。

d) 审设备能够明确区分内部设备与外部设备、合规设备与不合规设备，对于不合规设备的接入进行实时告警。

e) 审行为能够对税务系统与税收数据操作的行为进行有效地记录，方便形成完整的流程记录。

审用户、审角色、审权限、审设备、审行为五者有机结合， 从而达到审计信息系统精确定位到人和设备的目的。

2. 合理控制

记录过程不要影响到正常的业务开展，只对必要的操作进行审计。例如，只对 O 盘内税收数据的操作进行审计和控制，对 O 盘外的税收数据的操作不进行审计和控制。

3. 即时预警

对于严重的事件要能够通过多种方式进行实时通知和预警，尤其是一些对数据的高风险操作。

4. 完整报告

能够对税收数据的使用全过程，进行记录并输出详细的报告内容。从用户的易用性角度， 做到三给， 即“给证据、给分析、给报告”。

（1）给证据是对不合规定的行为（如不合规的网络接入，不合规的数据导出操作，不合规的后台数据库直接访问，使用未经许可的软件对重要税收系统的访问，不按规定使用他人账号登录税收系统的行为等）作出详实的审计记录， 为下一步采取措施提供依据。

（2）给分析是在一定的时间周期内，系统可以对各类行为的审计结果进行自动分析和判断，从而判断是否发生了针对业务的安全事件。同时， 系统也可以分析审计记录中各类人员的企图， 一步步的追查出违规者。

（3）给报告可以根据税务机关重点关心的问题与范围， 设定审计输出报告，使用户能迅速的得到自己最关心的信息， 让审计报告更容易理解。

5.8 可视呈现

UniBDP系统中建立了数据防泄露的可视化治理模型，并构建其系统架构，最终采用数据可视化技术，将数据终端防泄露的管理提升到更高的层次。

数据可视化技术的主要特点：

1. 交互性，使用者可以方便的以交互方式管理和使用数据。
2. 多维性，使用者可以看到表示对象或事件数据的多个属性或变量，而数据可以按其每一维的值，将其分类、排序、组合和展示。
3. 可视性，数据可以用图像、曲线、二维图形、三维体和动画等，来显示并可以对其模式和相互关系进行可视化分析。

UniBDP从业务系统使用入手，按照从简单到复杂、从单一到整体、从底层到高层的思路，将数据管理人员关心的终端业务数据防泄露问题，及其可视化治理方法转换成五个环节，如图5-3所示：

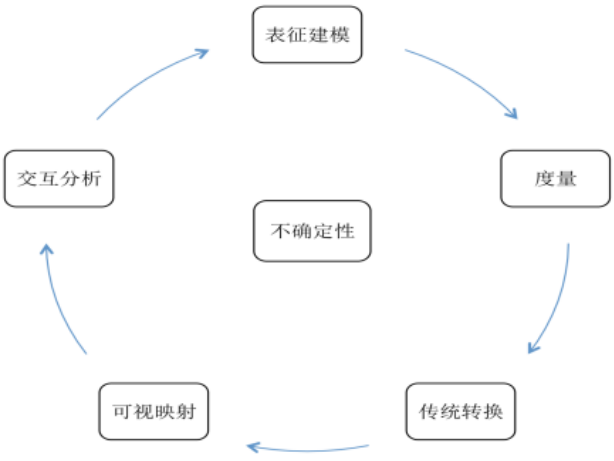

图 5-3 数据可视化治理

从这5个环节出发，结合数据可视化的一般流程和标准模型，UniBDP系统构建了一种适用于数据防泄露可视化分析的概念模型。如图5-4所示：

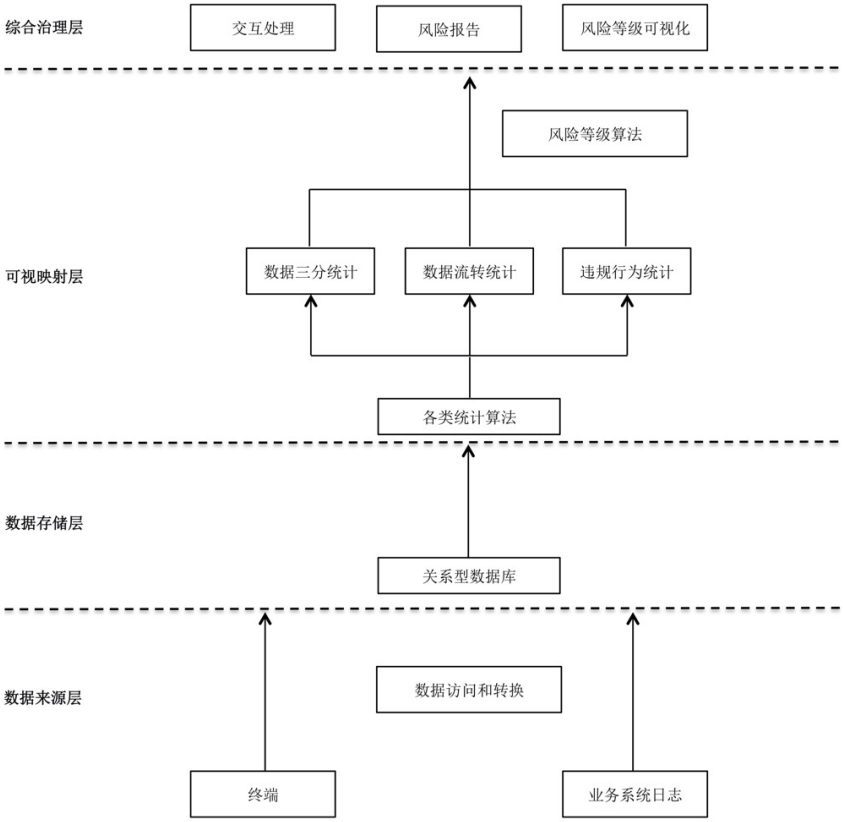

图 5-4　数据防泄露可视化分析模型

第6章 平台价值

1. 免改造

UniBDP 不需要对业务系统、网络架构、文件类型、应用程序进行改造即可达到数据防泄露的效果。

2. 提升了安全等级，降低了数据泄露风险

UniBDP 在每个阶段都提供了完善的安全控制手段，为用户提供端到端的安全交付方案。从整体上提升了税务机关的安全等级，降低了数据泄露的风险。

3. 投入低，有效增加了投资回报

UniBDP 的软件价格和实施费用相对国外厂商较低，且研发、实施力量都在国内，可随时支持用户现场；同时，相对加解密产品，UniBDP 后期的维护和服务成本较低，不需要像加解密产品一样需要经常去维护密钥和解密失败等诸多问题。

4. 风险可视、可控

UniBDP 可实现敏感数据分布、分类、分级、违规行为、风险分析的可视化管理，风险状态实时地以视图形式进行展现，让税务机关可以快速及时的了解目前存在风险的部门、人员，从而对风险做出控制。

5. 改善内部管理

UniBDP 不仅仅是一个数据安全保护项目，同时也是一个信息安全风险控制项目。通过数据防泄露的平台搭建，一是可以有效保障数据安全管理制度的落地，同时也可以对数据安全管理制度进行重新梳理，通过实际环境的运行进一步发现和改善制度中存在的各种问题。

6. 满足国家/监管部门法令法规

UniBDP 可以减少与法规遵从相关的直接成本， 使审计更容易，同时减少违规的风险。

附录一 产品参数

1. 运行环境

1) 总控中心

平台	支持的操作系统	系统需求
Windows	Windows Server 2003、2008系列	-4×CPU(四核主频)，2.0G Hz以上 -推荐 16GB 内存 -200GB 磁盘空间

2) 数据库

数据库支持 SQL Server、PostgreSQL。

3) 安全代理

平台	支持的操作系统	系统需求
Windows	Microsoft Windows 2000系列 Microsoft Windows XP系列 Microsoft Windows7系列 Microsoft Windows8系列	- Pentium 4 2.0GHz 以上 -512M内存

2. 性能指标

1) 总控中心最大可管理注册主机数量：50000 台

2) 总控中心网络带宽占用：100K/1000 客户端

3) 终端监控引擎 CPU 占用(静态模式)：＜1%

4) 终端监控引擎内存占用(静态模式)：12M

附录二 产品资质

1) 公安部颁发的《计算机信息系统安全专用产品销售许可证》

2) 中国国家信息安全测评认证中心颁发的《国家信息安全测评信息技术产品安全测评证书》

3) 中国人民解放军信息安全测评认证中心颁发的《军用信息安全产品认证证书》

构建可控的互联世界！

http://www.leagsoft.com

文档维护：刘群检

E-MAIL：support@leagsoft.com

如有版本更新，恕不另行通知，请向联软科技销售代表索取。