XBRL网络财务报告安全问题浅探

夏云飞

（重庆工商大学会计学院 重庆 400067）

【摘要】本文从技术特点、运作原理、安全需求等方面分析了XBRL与EDI的相似之处，指出了EDI安全策略在XBRL实施中的借鉴意义，并重点推介了互联网协议、加密技术、数字签名、VPN等网络安全技术。

【关键词】XBRL EDI 加密技术 VPN 数字签名

一、XBRL的定义

XBRL是可扩展商业报告语言的简称，这是一种新的财务和商业信息报告标准。XBRL实质上是一种数据描述语言，通过它可以使各种商业信息在不同软件、平台、技术（包括Internet）间实现数据的可靠提取和顺畅交换，并且依据底层的元数据的重新组合能够使财务报表适应变化的会计制度和报表格式要求，给财务报表数据的存储、传递、再利用提供有效的工具。

按照XBRL国际组织的定义，XBRL是商业和财务数据电子化交流的一种语言，是用来改革全世界商业报告的语言，它有助于商业信息的编制、分析和交流，为提供和使用财务数据的所有人提供低成本、高效率的服务以及可靠而准确的商业信息。布赖恩·伯杰伦对XBRL的定义如下：XBRL是一个关于对财务和商业报告数据进行及时、准确、高效和经济的存储、处理和重制以及交流的开放式的不局限于特定操作平台的国际标准。上海证券交易所给出的定义为：XBRL是XML于财务报告信息交换的一种应用，是目前应用于非结构化信息处理尤其是财务信息处理的最新标准和技术。XBRL在证券行业的应用，能够实现证券业内、业间的上市公司信息共享和互操作，进一步推动我国上市公司信息披露和证券信息服务业的规范、有序发展，实现上市公司信息网上披露。

1. 第一行至第四行的内容（包括数值）直接输入，假设员工为企业服务年限为1～36年，A5:A40的单元格输入1～36。权益归属比例根据上面的定义，在C5:C40单元格输入0～100%。

2. 企业年金测算模型建立如下：第一、二、三行事先录入相关的内容，员工为企业服务年限为1～36年，企业缴费归属个人比例的值根据企业人力资源管理规划进行确定。根据上面增长年金理论推导出的公式，可确定企业年金测算模型各单元格的公式：

B5==(($B$3/($C$3-$D$3))×((1+$C$3)^A5-(1+$D$3)^A5)+FV($C$3,A5,,-$E$3,0))×(1-$G$3)

D5=B5×C5

E5=B5−D5

F5=B5×$F$3

G5=D5+F5

只要在单元格中输入以上公式，分别选中该单元格进行公式引用，即可完成企业年金基金综合测算模型的编制。

三、企业年金基金综合测算模型的使用方法及注意事项

该模型的使用较为简单明了，只要根据企业实施年金计划的具体情况调整B3、C3、D3、E3、F3、G3单元格的参数，即可对测算模型进行数据重算。信息使用者可根据表格中的数据自行插入相关的图表，使该数据模型更为直观。从表中的数据可知，若企业实施企业年金制度，某一男员工从23岁在企业持续工作，到其退休时（60岁），其年金基金账户的数额将达到981 511.97元。企业年金制度为员工提供了较为丰厚的退休金待遇，表明企业有较好的员工薪酬福利，这无异于是企业人力资源管理战略中吸引人才的“金名片”。再结合权益归属比例、员工年金数额、员工离职损失三项参数，企业年金留住人才的“金手铐”作用一目了然。因篇幅所限，此处不再赘述。使用该数据模型进行企业年金基金测算的数据仅做参考，并不作为评判员工个人年金基金账户余额的依据。

【注】本文为云南省教育厅科学研究基金项目“云南省民营煤炭企业年金制度激励效应研究”（项目编号：09C0241）阶段性成果。

主要参考文献

1. 斯蒂芬·A.罗斯著，吴世龙译，公司理财，北京：机械工业出版社，2005

2. 杨长汉，中国企业年金投资运营研究，北京：经济管理出版社，2010

3. 殷俊，中国企业年金计划设计与制度创新研究，北京：人民出版社，2008

4. 中国养老金网编，中国企业年金规范与发展，北京：中华工商联合出版社，2007

5. 闫建华等，Excel高效办公——数据处理与分析，北京：人民邮电出版社，2006

二、XBRL 的实施与安全需求

世界上许多国家和地区,如英国、美国、加拿大、澳大利亚等都积极投入 XBRL 项目的研发应用。XBRL 引发了会计信息化领域新一轮的研究热潮,在我国的理论界和实务领域都得到了迅速的发展。在《上市公司信息披露电子化规范》框架下,上海证券交易所将 XBRL 应用于 2003 年年报摘要及 2004 年第一季度报告、中报摘要、年报摘要和年报全文摘要披露。深圳证券交易所于 2005 年 1 月正式推出改版后的基于 XBRL 的"上市公司定期报告制作系统"。2005 年 4 月上海证券交易所正式成为 XBRL 国际组织的会员;10 月 20 日,中国定期报告部分 XBRL 标准获得 XBRL 国际组织批准,成为我国上市公司年报的正式标准。

XBRL 的优点是显而易见的,它在不改变现有会计准则的条件下,财务报告的编报标准趋向统一,格式更加灵活,跨平台一致性显著增强。然而,在 XBRL 的实施过程中,也面临很多问题,网络安全是其中之一。由于互联网的开放性,任何终端用户都可进入和访问网络中的资源,这也使得 XBRL 实施过程中的信息安全问题日益突出。

信息安全有四个主要的指标:①保密。这是指保证信息不会被未授权的人发现、知道。②完整。保证数据的完整,凡是未授权的人都不能对其进行改变或者破坏。③有效。保证不会过度地拒绝合法使用者访问文件、计算机等资源。④授权使用。保证只有被授权的人在被授权范围内使用资源,而未被授权的人或以未授权的方式都不能使用资源。

三、EDI 与 XBRL 的相似性

EDI(Electronic Data Interchange)译为电子数据交换,也称电子数据贸易或无纸贸易。EDI 将贸易、生产、运输、保险、金融和海关等行业的商务文件,按国际统一的语法规则进行处理,使其符合国际标准格式,并通过通信网络来进行数据交换,是一种用计算机进行商务处理的新业务。国际标准化组织(ISO)将 EDI 描述为:将商业或行政事务按照一个公认的标准,形成结构化的事务处理或信息数据格式,是一种从计算机到计算机的数据传输方法。

将 EDI 与 XBRL 运行原理进行对比分析,我们可以看到二者具有极大的相似性。

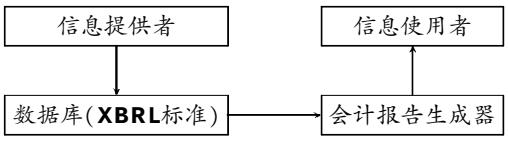

图 1 基于XBRL的会计报告披露的基本原理

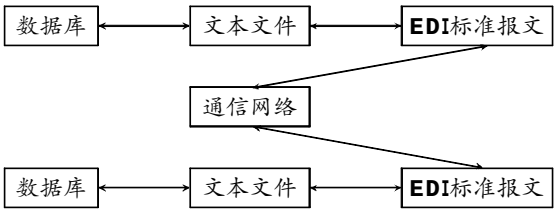

图 2 EDI运作基本原理

1. XBRL 和 EDI 实施的最终结果都是标准化的数据。XBRL 实现了财务信息特别是网络财务报表的标准化,使得不同软件、平台、技术间的交流得以实现。而 EDI 则是将商务文件转化为标准格式即 EDI 标准报文,实现了商务信息的标准化传输。

2. XBRL 和 EDI 在发展中都形成了相应的国际标准,XBRL 的技术标准为国际会计准则基金会的 XBRL 标准,EDI 采用的技术标准为 EDIFACT。

3. 两种标准化文件都可以在开放性的互联网上进行传输,提高了信息的可获取性并最终降低了信息获取成本。基于互联网的信息传输具有低成本、高效率的特征,也增强了信息的可获取性,使其更具实用价值。

4. XBRL 和 EDI 在实施中都面临互联网所带来的挑战,即信息资源更容易被黑客窃取或者被病毒破坏,如何保证信息的真实性、完整性、有效性,成为二者实施中的共同问题。

EDI 的发展已经比较成熟,由发展初期的 VAN EDI 到现在的互联网 EDI,在其转变过程中也经历了许多互联网信息安全问题的挑战,最终逐渐发展成熟并得到广泛的应用。从这一角度,部分 EDI 安全策略对基于 XBRL 会计报告的实施极具参考意义。

四、网络安全措施

网络技术可以使得会计信息的使用与传输范围大大扩展,实现了实时办公、远程操作和无纸化办公,大大提高了会计系统的操作效率,节约了企业成本,增强了企业竞争力。但是网络是一把双刃剑,在一个缺乏安个保障的网络上运行会计信息系统,将容易出现信息被非法访问、篡改或攻击的现象,可能会导致企业机密泄露、数据丢失或破坏,从而蒙受经济损失,所以,会计信息系统的网络信息数据安全是其正确、可靠运行的重要保障。常见的网络安全策略包括加密技术、数字签名、VPN、互联网协议等。

1. 因特网传输协议选择。因特网为信息传输提供了众多的方式,这些方式配上相应的安全措施可用于传输各种信息,甚至一些关键数据。因特网 EDI 的实现基于应用层,EDI 报文通常包含非文本信息,所以可采用 IETF(因特网工程任务组)制定的一系列 Internet/MIME(多用途 Internet 邮件扩展)协议。在 MIME V1.0 版本中,定义了七种报文类型,同时对每一"报文类型"又定义了"子类型",并规定在头域中采用"类型/子类型"格式予以表示。"类型"用来说明报文体的一般类型,"子类型"则说明这种类型的报文采用的具体格式。接收方在接收到采用"类型/子类型"说明的报文时,应调用相应的解释程序对报文体进行处理。

2. 数字加密。数字加密技术可以防止公用或私有化信息在网络上被拦截或窃取。上市公司可以根据需要对全部资料进行加密,在考虑成本效益的情况下也可以对部分重要资料进行加密。加密方式主要有两种,即对称加密与非对称加密(又称公钥加密),二者构成了整个信息安全体系的基础。对称加密方式的算法主要有 DES、3DES、RC2、IDEA 等,其中 IDEA 算法在形式上与 DES 类似,但使用 128 位的密钥,强度

高于 DES。加密和解密密钥都可从同一个主密钥派生出来。IDEA 的设计倾向于软件实现,到目前为止,从公开发表的文献看,对 IDEA 尚未找到破译方法。对称加密方式加密解密速度快,适用于大量文件的加密,但其密钥管理难度较大。公开密钥加密算法主要为 RSA 算法。该算法已经成为事实上的公开密钥密码算法标准,得到了广泛使用。由于使用者只需一把公开密钥,密钥保管难度较小,但公开密钥加密算法加密解密速度相对较慢。

基于这两种加密方法的特点,实务中二者经常被结合使用,通过公开密钥加密技术来简化对称密钥的管理,同时也可解决纯对称密钥模式中存在的可靠性和鉴别问题,贸易方可以为每次交换的信息(如每次的 EDI 交换)生成一次性的会话密钥。

3. 数字签名。数字签名是密码学理论中的一个重要分支,它的提出是为了对电子文档进行签名,以替代传统纸质文档上的手写签名,可以验证消息源的可靠性,还可以保证消息发送者不能否认发出的消息,因此它必须具备五个性质:①签名是可信的;②签名是不可伪造的;③签名是不可重用的;④签名的文件是不可改变的;⑤签名是不可抵赖的。数字签名的实现,一般是由信息的发送者通过一个单向函数对要传送的消息进行处理产生其他人无法伪造的一段数字串,用以认证消息的来源并检测消息是否被修改。消息接收者用发送者的公钥对所收到的用发送者私钥加密的消息进行解密后,就可以确定消息的来源以及完整性,并且发送者不能对签名进行抵赖。

4. 虚拟专用网(VPN)。VPN 技术是实现安全传输的重要手段之一,VPN 充分利用隧道、认证、加密等技术手段,使用户可以利用现有的 Internet 等公共网络,安全地远程访问内部网络资源的网络系统。它通过在公共网络建立临时、安全和稳定的隧道来扩展企业内部网络,在远程用户、公司分支机构、商业合作伙伴与公司的内部网之间建立可信的安全链接,实现对重要信息的安全传输和保护。

VPN技术结构如图 3 所示。

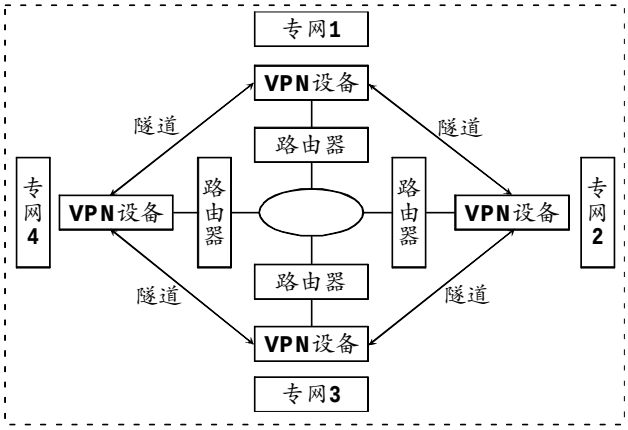

图 3 VPN技术结构

五、总结

信息安全问题是网络应用系统最大的问题之一,尤其是对于存储了许多机密数据和商业数据的网络会计信息系统而言。针对信息安全技术的原则与策略,结合网络会计信息系统的特点,可以构建一个信息策略的基本框架,结合密码管理、权限设定、防火墙设置等方式,将网络会计信息系统的安全风险降到最低。

XBRL 在包括我国在内的全球范围内得到了迅速的发展,网络信息安全成为其发展过程中不得不关注的问题。通过上文的分析我们可以看到 EDI 与 XBRL 的相似之处,EDI 安全策略中的加密技术、数字签名、VPN、互联网协议等网络安全技术在 XBRL 的实施过程中有很强的现实意义。目前理论界和实务界多关注于 XBRL 信息在财务信息交换中的应用,然而安全问题是 XBRL 财务报告在互联网上传输必须面对的问题,只有在 XBRL 理论体系的构建中充分考虑相关安全技术的应用,从根本上解决基于 XBRL 会计报告的安全问题,才能使基于 XBRL 的网络财务报告获得更快的发展。

主要参考文献

1. 布赖恩·伯杰伦著,廉小红等译.XBRL 语言精要——21 世纪的财务报告.北京:中国人民大学出版社,2004

2. George H. Bodner, William S. Hopwood 著. 卢俊译.会计信息系统.北京:清华大学出版社,2003

3. 张天西.网络财务报告:XBRL 标准的理论基础研究.会计研究,2006;9

4. 许勇,吴国新,顾冠群.因特网 EDI 的安全研究及实现.东南大学学报(自然科学版),2002;32