编者按：本期专栏共发表了《电子商务身份认证标准化技术研究》《浅谈电子商务网络信息安全技术的优化》《浅谈电子签名技术的优势和隐患》和《电子商务标准化与信息安全的相互影响》4篇文章，介绍了基于零知识证明理论的身份认证技术、我国计算机网络技术体系在面临安全威胁时所采取的应对策略、电子签名技术所带来的优势与隐患以及电子商务标准化与网络信息安全的相关性，其中对网络信息安全技术未来的优化方向的分析极大地促进了我国互联网经济的发展，类似的像电子签名技术的普及、电子商务身份认证技术多元化的发展，都为提高工作效率、降低成本起到了推动作用，使得电子商务与信息安全联系日渐密切，互相协同，为数字商业提供了安全高效的环境。

电子商务标准化与信息安全的相互影响

高 亮

（中国标准化研究院）

摘　要：近年来，随着通信技术、网络技术的迅速发展促使电子商务技术应运而生。电子商务标准化与信息安全密不可分，相互影响，为数字商业的稳健发展提供了坚实基础。电子商务标准化包括技术互操作性、安全性、隐私保护、法规合规和支付可靠性等多个方面，旨在确保在线交易的合法性和顺畅性。信息安全是电子商务标准的核心组成部分，通过标准如：SSL/TLS、GDPR和PCI DSS，保护了数据的隐私，防止了数据泄露和黑客攻击。此外，支付标准如：ISO 20022和EMV确保了支付系统的互操作性和交易的安全性。两者相互协同，为数字商业提供了安全、可信和高效的环境，推动了电子商务的不断发展。这种相互影响有助于保护消费者和企业的权益，同时促进了信息安全和标准制定的不断演进以适应新兴威胁和技术趋势。本文通过对电子商务现状、电子商务标准化、安全需求分析，探讨了电子商务标准化与信息安全的相互影响。

关键词：电子商务，标准化，信息安全

DOI编码：10.3969/j.issn.1674–5698.2024.07.008

The Interaction between E-commerce Standardization and Information Security

GAO Liang

（China National Institute of Standardization）

Abstract: IIn recent years, with the rapid development of communication and network technologies, e-commerce technology has emerged. The standardization of e-commerce and information security are inseparable and can influence each other, providing a solid foundation for the stable development of digital commerce. E-commerce standardization

基金项目：本文是国家市场监管总局科研条件专项资金项目“面向多边贸易合作的技贸措施研究能力建设”（一期）（项目编号：[2060503]150019000000210006）研究成果。

作者简介：高亮，工程师，硕士研究生，研究方向为数据与知识工程相关技术标准化。

includes multiple aspects such as technical interoperability, security, privacy protection, regulatory compliance, and payment reliability, aiming to ensure the legality and smoothness of online transactions. Information security is a core component of e-commerce standards, which protects data privacy and prevents data leakage and hacker attacks through standards such as SSL/TLS, GDPR, and PCI DSS. In addition, payment standards such as ISO 20022 and EMV ensure the interoperability of payment systems and transaction security. The synergy between the two provides a secure, trustworthy, and efficient environment for digital commerce, driving the continuous development of e-commerce. This mutual influence helps to protect the rights and interests of consumers and businesses, while promoting the continuous evolution of information security and standards development to adapt to emerging threats and technological trends. This paper explores the mutual influence between e-commerce standardization and information security by analyzing the current situation of e-commerce, standardization of electronic internet access, and security needs.

Keywords: e-commerce, standardization, information safety

0 引言

当前，电子商务领域所面临的信息安全现状令人不容乐观。我国的信息安全研究已经历了不同阶段，包括通信保密和计算机数据保护等阶段，而如今已进入了网络信息安全研究的阶段[1]。随着互联网的普及，网络信息安全愈发凸显其重要性。然而，国内许多电子商务企业对于网络信息安全的意识并不十分强烈。很多企业更倾向于关注经济效益、交易便利性和高效速度，而将安全性、保密性以及抗攻击性等问题相对次要化。所以应加强支付信息的加密技术，建立安全的身份认证和授权机制，以及强化网络防护能力。标准化安全技术体系的建立，有助于确保各个企业在电子商务中采取一致的安全标准，共同维护整个电子商务生态的安全稳定。

1 电子商务标准化

电子商务标准化的实施通常由国际标准化组织[2]（ISO）、国际电信联盟[3]（ITU）等国际性组织以及各国的标准制定机构负责。这些组织协同制定标准，确保它们能够在全球范围内得到广泛应用。

1.1 技术标准

技术标准是电子商务中最重要的一部分。这些标准涵盖了数据交换、编码、通信协议等方面。例如：XML（可扩展标记语言）是一种常用的数据交换标准，它允许不同系统之间共享和理解数据。此外，HTTP（超文本传输协议）和HTTPS（HTTP安全）是用于互联网通信的标准协议，确保了网站和客户端之间的安全数据传输。

1.2 安全标准[4]

电子商务安全标准旨在保护交易和数据的机密性和完整性。SSL/TLS是用于安全数据传输的协议，它确保了在互联网上的信息传输是加密的，从而防止了数据被窃取或篡改。此外，PCI DSS是为了保护支付卡数据而制定的标准，它规定了商家和支付处理者必须采取的安全措施。

1.3 隐私标准[5]

隐私标准是为了保护个人信息隐私，确保其合法和安全处理而制定的一系列规范和指导原则。这些标准旨在确保组织和企业在收集、存储、处理和分享个人信息时遵守适用的法律法规，并采取适当的措施来保护这些信息免受不当访问、泄露或滥用。

1.4 支付标准

支付标准是用于确保支付交易的安全、有效和互操作性的一组规范和指南。这些标准覆盖了各种支付方法，包括信用卡支付、电子转账、数字货币和移动支付等。以下是一些与支付标准相关的主要标准和协议。

（1）ISO 20022：ISO 20022是国际金融通信标准，旨在规范金融机构之间的交流和数据交换，包括支付交易。它提供了一种统一的方式来描述和交换各种金融消息，包括付款指令、交易确认和支付通知。ISO 20022已经在全球范围内广泛应用，促

进了国际支付的互操作性和效率。

（2）PCI DSS：PCI DSS（支付卡行业数据安全标准）是为了保护支付卡数据而制定的一组标准。它规定了商家和支付处理者必须采取的安全措施，以防止支付卡数据泄露和滥用。PCI DSS的合规性是必要的，以便企业能够处理信用卡支付。

（3）SEPA：SEPA（单一欧元支付区域）是欧洲的支付标准，旨在统一欧元区内的支付交易。SEPA标准化了欧元区内的直接借记和信用转账，使国际和国内支付更加便捷和一致。

（4）支付应用协议：不同的支付应用通常使用特定的协议和标准来实现交易。例如：支付宝和微信支付在中国采用了自己的支付应用协议，以支持移动支付。

2 信息存储安全所面临的严重威胁

信息存储安全隐患是指在数据存储、处理和传输过程中存在的潜在威胁和漏洞，可能导致数据泄露、丢失、破坏或未经授权的访问。信息存储安全面临严重威胁源于多种原因，包括不断增长的网络攻击；员工，合作伙伴或供应商的不慎行为或恶意行为；自然灾害和硬件故障可能导致存储设备的物理损坏以及云安全漏洞等。数据泄露、黑客攻击、勒索软件以及内部威胁都可能导致敏感信息的丢失或被盗取。物理损坏、无意间泄露以及云安全风险也加剧了存储安全问题。信息存储安全面临的威胁主要包括两个方面，（1）信息存储安全隐患，（2）信息传输安全隐患。

2.1 信息存储安全隐患[6]

信息存储安全是指电子商务中信息在静态存储过程中的安全保障措施。然而，这一领域存在着多种潜在的信息安全隐患，其中包括非授权调用信息和篡改信息内容等问题。随着企业的联网发展，电子商务的信息存储安全不仅仅涉及内部管理，还需应对外部威胁。

为了应对这些隐患，企业需要采取一系列有效的安全措施。在内部方面，建立严格的访问控制机制，确保只有授权人员能够访问和修改存储的信息。此外，加强员工安全培训，提高他们对信息存储安全的重视程度，减少不慎操作带来的风险。在外部方面，应使用强大的防火墙和入侵检测系统，以阻止恶意入侵者进入系统。加密存储数据可以有效保护数据的机密性，而定期的数据备份和恢复计划可以在系统遭受攻击时快速恢复业务运营。

2.2 信息传输安全隐患

信息传输安全隐患可能导致广泛的影响，其中最常见和最严重的后果之一是数据泄露。数据泄露可能由多种原因引发，包括黑客攻击、内部员工恶意或不慎的员工行为，以及系统漏洞。无论是在个人还是组织层面，数据泄露都可能产生以下一系列负面影响[7]。

（1）数据泄露可能导致严重的个人隐私侵犯。当包含个人身份信息、金融数据或医疗记录等敏感信息的数据被泄露时，黑客或恶意用户可能会滥用这些信息，从而对受害者的个人隐私造成侵犯。这可能包括身份盗用、欺诈活动以及个人信息的不当使用，对个人造成长期和广泛的负面影响。

（2）数据泄露可能对财务状况造成重大损害。组织可能面临多重财务压力，包括支付恶意攻击者要求的勒索软件赎金，为数据恢复而支付高昂的费用，以及应对法律诉讼所需的支出。此外，由于信息存储安全事件可能导致业务中断，因此组织还可能遭受与业务停滞有关的收入损失。

（3）法律责任也是一个重要的考虑因素。在许多国家和地区，法律要求组织采取适当的措施来保护客户和员工的敏感信息。如果组织未能履行这些法律义务，可能会面临法律诉讼和罚款。因此，信息存储安全隐患可能对组织的合规性产生严重影响，从而导致法律和财务风险。

3 电子商务交易双方的信息安全技术

3.1 电子商务对信息安全的需求

在电子商务交易中，买家和卖家都面临着潜在的信息安全隐患。对于买家而言，支付信息泄露、身份盗用、虚假商品、恶意软件攻击和公共Wi-Fi网络上的不安全交易都构成了威胁。卖家则需要应

对支付处理风险、数据泄露、虚假订单、供应链攻击以及虚假评价等问题。为了减轻这些风险，电子商务参与者需要采取安全措施，包括使用安全支付系统、提供身份验证、定期更新和维护系统、为员工提供信息安全培训，并与可信赖的供应链伙伴合作，以确保电子商务交易的安全性和可靠性

3.2 电子商务的信息安全技术

电子商务的信息安全技术是确保在线交易和用户数据安全的重要支柱[8]。这包括数据加密、身份认证、网络安全措施、漏洞管理、实时监控、恶意软件防护、员工培训以及数据备份和灾难恢复计划。这些技术[9]的综合应用有助于保护客户数据，防止支付欺诈，维护商业声誉，遵守法规，降低风险，确保业务的可持续性，并为用户提供信心，使电子商务企业能够在竞争激烈的市场中取得成功。此外，新兴技术如：区块链和智能安全分析也为电子商务提供了更高级别的安全性和可信度。

（1）网络层技术

网络层技术[10]是计算机网络的关键组成部分，它们负责管理和优化数据的传输和路由。IP协议为全球范围内的数据包提供地址，而路由协议确定最佳传输路径。子网和子网掩码允许有效地管理IP地址，而ARP解析IP地址到物理MAC地址。DHCP自动分配网络配置信息，NAT允许多个设备共享单个IP地址。IPv6解决了IPv4地址短缺问题，VPN[11]提供了安全的远程访问，IPsec确保了数据的安全传输，而IGMP管理多播通信。VLAN创建逻辑网络分区，以实现更灵活的网络管理。这些技术和协议共同构建了网络层的基础，支持着互联网、局域网和广域网等各种网络环境的可靠和安全运行。

（2）加密层技术

加密层技术[12]在计算机和通信领域中扮演着关键的角色，其主要任务是确保数据的隐私和安全性。这些技术和协议包括SSL/TLS、SSH、VPN、IPsec、PGP/GPG、HTTPS、AES、RSA、Diffie-Hellman等，它们提供了数据加密、身份验证、完整性验证和密钥交换等功能，广泛应用于互联网通信、电子商务、金融交易、远程访问以及敏感信息的存储和传输。通过采用这些加密层技术，组织和个人能够更好地保护其数据免受未经授权的访问和恶意攻击，确保通信和数据交换的安全性和可信度。

（3）认证层技术

认证层技术[13]是计算机和网络安全领域的重要组成部分，其主要任务是验证用户、设备或应用程序的身份，以确保安全的访问和通信。这些技术包括用户名和密码认证、多因素身份验证、生物特征认证、公钥基础设施（PKI）、OAuth、Kerberos等，它们提供了多种方式来确认身份的有效性和授权权限。通过采用这些技术，组织和个人能够建立更可信的安全环境，有效地应对身份盗用和未经授权访问的威胁。

（4）协议层技术

协议层技术[14]在计算机和通信领域扮演着至关重要的角色，它们定义了数据通信和交流的规则和标准，确保不同设备和系统之间的有效互操作性和可靠通信。这些技术包括HTTP/HTTPS、SMTP/POP3/IMAP、TCP/IP、DNS、SNMP、FTP、SSH、VoIP、XMPP、BGP、OSPF、SIP等，它们涵盖了从Web通信、电子邮件传输、网络管理、文件传输、远程访问到实时通信等各种应用领域。协议层技术为数字通信提供了必要的基础，也为电子商务安全提供了保障。

4 结语

随着电子商务的发展，电子交易手段的多样化，信息安全问题将会变得更加重要和突出。电子商务标准化与信息安全密切相关，它们共同为确保在线交易和通信的安全性、隐私性和合法性提供了重要支持。这些标准不仅保护了企业和消费者的利益，还有助于促进电子商务的可持续增长和全球化发展。在一个充满威胁的数字化环境中，信息安全和电子商务标准化将继续发挥关键作用，以确保在线交易和业务的安全性和可信度。由于电子商务的实现是一项复杂的系统工程，其信息安全问题的解决有赖于各相关技术的发展，如：公钥基础设施（pki）技术的研究与应用；电子商务采购协议、支

付协议及物流配送协议的进一步完善等。同时，除技术问题外，电子商务的信息安全还有赖于电子商务发展所需的有关政策和相应的标准规范要求的完善。这些课题的研究不仅具有重要的理论价值和实用价值，而且对于推动电子商务的发展具有重要的现实意义。

参考文献

[1] 王丽蕊. 电子商务与信息安全技术的相互影响[J]. 商情, 2014(36):202.

[2] 沈言. 国际标准化组织[J]. 质量与市场, 2007(1): 24–25.

[3] 郑海燕. 国际电信联盟发起价值数百万美元的项目弥合全球数字鸿沟[J]. 国外社会科学, 2002(1):100–100.

[4] 钱富珍. 电子商务安全策略及其安全标准化[J]. 上海标准化, 1999, 000(006):26–30.

[5] 马敏,陈焕新. 电子商务中隐私权保护的新制度经济学分析[J]. 科技进步与对策, 2001,18(6):135–136.

[6] 许皓炫. 基于计算机信息安全存储与利用的相关对策分析[J]. 信息与电脑, 2015(12):169–170.

[7] 陈驰.计算机网络信息安全面临的问题与对策[J]. 电子技术与软件工程, 2014(18):.238–239

[8] 李艳. 电子商务信息安全策略研究[J]. 甘肃科技, 2005, 21(6):53–54.

[9] 郭大亮,范清芬. 电子商务的信息安全技术与管理研究[J]. 信息安全与通信保密, 2012(4):70–72+75.

[10] 米军,季林,金环. 在网络层实现安全传输通道技术的研究[J]. 网络安全技术与应用, 2006(8):83–84+87.

[11] 魏广科. VPN技术及其应用的研究[J]. 计算机工程与设计, 2005,26(3):714–715+724.

[12] 邓永红. 加密套接字协议层技术综述[J]. 有线电视技术, 2005,12(1):5–11.

[13] 张丹,吴晓富,颜俊,等. 物理层认证PHY–PCRAS应用于OFDM传输的性能分析[J]. 计算机技术与发展, 2016, 26(1):137–141.

[14] 孟庆华,管文,沈昌祥,等. 大规模网络协议层协同安全管理模型的研究[J]. 计算机应用, 2004,24(2):30–32.