ISO Research Grant 2024

ISO研究助成金2024

The impact of ISO/IEC 27001 certification on digital trade

ISO/IEC 27001認証がデジタル貿易に与える影響

英和対訳

一般財団法人 日本規格協会

iso.org

Foreword

This report has been developed through collaboration between the International Organization for Standardization (ISO) and China Jiliang University. It is the result of the ISO Research Grant 2024, and focuses on exploring the relationship between information security certification and digital trade. The research team from China Jiliang University consisted of three Master's degree students in the School of Economics and Management, Yujia Wu, Junjie Liu and Yuxin Niu.

The research team would like to express their gratitude to Professors Suli Zheng, Xiaoran Chang and Mingshun Song from China Jiliang University. Their guidance was invaluable throughout the process, and their knowledge and experience provided essential support for the successful completion of this research.

The team would also like to thank Sophie Boinnard and Valeriia Grekova, project manager and project support officer respectively, in the Strategy and Portfolio Management Unit of the ISO Central Secretariat. Their guidance and assistance were key to ensuring the quality and relevance of this research, and their expertise contributed to the depth and accuracy of the report's findings.

The team is also indebted to the various institutions and enterprises who agreed to participate in the study surveys. Their cooperation and sharing of practical information enriched the report's data sources, grounding the data in real-world scenarios.

This research aims to shed light on the impact of ISO/IEC 27001 certification on digital trade, providing valuable insights for policymakers, industry practitioners and researchers in related fields. The team hopes that this report will contribute to the further understanding and development of information security and digital trade.

まえがき

本報告書は，国際標準化機構（ISO）と中国計量大学の共同研究によって作成されました。ISO研究助成金2024の成果であり，情報セキュリティ認証とデジタル貿易の関係性を探ることを目的としています。中国計量大学の研究チームは，経済管理学院の修士課程学生3名（呉玉佳（Yujia Wu,），劉俊傑（Junjie Liu），牛玉新（Yuxin Niu））で構成されています。

研究チームは，中国計量大学の鄭蘇立（Suli Zheng）教授，張暁然（Xiaoran Chang）教授，宋明順（Mingshun Song）教授に深く感謝の意を表します。教授陣のご指導は研究過程全体を通して非常に貴重であり，その知識と経験は本研究の成功に不可欠な支えとなりました。

本研究チームは，ISO中央事務局戦略・ポートフォリオ管理ユニットのプロジェクトマネジャーであるSophie Boinnard氏とプロジェクトサポート担当官であるValeriia Grekova氏に感謝の意を表します。お二人のご指導とご支援は，本研究の質と妥当性を確保する上で不可欠であり，お二人の専門知識は報告書の調査結果の深みと正確性を高める上で貢献しました。

また，調査にご協力いただいた様々な機関や企業にも深く感謝いたします。皆様のご協力と実践的な情報のご提供により，報告書のデータソースが充実し，データが現実世界のシナリオに基づいたものとなりました。

本研究は，ISO/IEC 27001認証がデジタル貿易に与える影響を明らかにし，政策立案者，業界関係者，関連分野の研究者にとって貴重な知見を提供することを目的としています。本報告書が，情報セキュリティとデジタル貿易の理解と発展に貢献することを願っています。

Contents

目次

Executive summary

The rapid expansion of digital trade has become a powerful engine for the global economy. However, significant security challenges accompany this growth, including increased risks of data breaches, cyber threats, and obstacles related to data security and privacy protection, which can hinder the smooth flow of international commerce. A powerful Information Security Management System (ISMS) manages information security, network security and privacy risks, while leveraging interconnectivity.

ISO/IEC 27001:2022, *Information security, cybersecurity and privacy protection – Information security management systems – Requirements*,[1] is the world's best-known ISMS standard (Podrecca, et al., 2023). It provides companies of any size and from all sectors with guidance for establishing, implementing, maintaining and continually improving an ISMS.[2] Achieving ISO/IEC 27001 certification demonstrates to clients and stakeholders that an organization or enterprise has put in place a system to manage risks related to the security of data owned or handled by the company, and that this system, when implemented according to this standard, serves as a tool for risk management, cyber-resilience and operational excellence.[3] Today, ISO/IEC 27001 is the fourth-most widespread ISO standard worldwide (Podrecca, et al., 2022) recording almost 82 566 certifications in 2023, representing 18% year-on-year growth (ISO, 2023).

Little is known about the digital trade implications of ISO/IEC 27001, despite its growing popularity (Culot et al., 2021). To provide a deeper understanding of the digital trade implications of ISO/IEC 27001, this report focuses on the following research questions:

1. Does ISO/IEC 27001 promote digital trade?
2. What are the differences in its impact throughout countries and regions?
3. What is the impact mechanism of ISO/IEC 27001 on digital trade?

To systematically address these questions, this report undertakes three complementary

sub-studies, at an international, national and enterprise level. At the international level, this report conducts descriptive analysis and regression analysis of national panel data, to examine the impact of ISO/IEC 27001 on digital trade and further identify the differences in the effects among different types of countries. At the national level, it conducts descriptive analysis and regression analysis of provincial panel data in China to explore the effects of ISO/IEC 27001 on digital trade and further identify the differences in the effects of ISO/IEC 27001 among different provinces and regions. At the enterprise level, it focuses on two Chinese enterprises and analyses the impact mechanism of ISO/IEC 27001 on their digital trade using case studies.

The main research findings are summarized as follows:

ISO/IEC 27001 certification promotes digital trade. At the international level, ISO/IEC 27001 certification serves as a significant catalyst for a nation's digital trade development. Empirical findings indicate that its positive impact is particularly pronounced in augmenting the total volume of digital trade. Consequently, governments worldwide are encouraged to strategically promote the widespread adoption and deep integration of this certification framework. By implementing systematic policy guidance – such as aligning national regulations with international standards and incentivizing corporate certification – governments can maximize the potential of ISO/IEC 27001 to foster a secure and trustworthy digital trade environment. This, in turn, positions countries to secure broader trade advantages within the increasingly competitive global digital economy.

1 https://www.iso.org/standard/27001.
2 https://www.iso.org/standard/27001.
3 https://www.iso.org/standard/27001.

エグゼクティブサマリー

デジタル貿易の急速な拡大は，世界経済の強力な原動力となっています。しかしながら，この成長に伴い，データ漏洩，サイバー脅威，データセキュリティおよびプライバシー保護に関する障害など，重大なセキュリティ上の課題が生じており，国際商取引の円滑な流れを阻害する可能性があります。強力な情報セキュリティマネジメントシステム（ISMS）は，相互接続性を活用しながら，情報セキュリティ，ネットワークセキュリティ，プライバシーのリスクを管理します。

ISO/IEC 27001:2022 *情報セキュリティ，サイバーセキュリティ及びプライバシー保護－情報セキュリティマネジメントシステム－要求事項*[1] は，世界で最も広く知られているISMS規格です（Podrecca et al., 2023）。あらゆる規模，あらゆる業種の企業に対し，ISMSの確立，導入，維持，継続的改善に関するガイダンスを提供します。[2] ISO/IEC 27001認証を取得することで，組織や企業が，自社が所有または取り扱うデータのセキュリティに関連するリスクを管理するためのシステムを導入していること，そしてこの規格に従って導入されたシステムが，リスク管理，サイバーレジリエンス，および業務効率化のためのツールとして機能することを，顧客や利害関係者に示すことができます。[3] 現在，ISO/IEC 27001は世界で4番目に広く普及しているISO規格であり（Podrecca et al., 2022），2023年には約82,566件の認証が取得され，前年比18%の成長を記録しました（ISO, 2023）。

ISO/IEC 27001は普及が進んでいるにもかかわらず，デジタル貿易への影響についてはほとんど知られていません（Culot et al., 2021）。ISO/IEC 27001のデジタル貿易への影響をより深く理解するために，本報告書では以下の研究課題に焦点を当てます。

1. ISO/IEC 27001はデジタル貿易を促進するのか？
2. 国や地域によってその影響にどのような違いがあるのか？
3. ISO/IEC 27001がデジタル貿易に与える影響メカニズムは何か？

これらの疑問に体系的に取り組むため，本報告書は国際レベル，国家レベル，企業レベルの3つの補完的な副次的調査を実施しました。国際レベルでは，各国のパネルデータを用いた記述分析と回帰分析を行い，ISO/IEC 27001がデジタル貿易に与える影響を検証するとともに，国ごとの影響の違いを明らかにしました。国家レベルでは，中国の省レベルのパネルデータを用いた記述分析と回帰分析を行い，ISO/IEC 27001がデジタル貿易に与える影響を探るとともに，省や地域ごとの影響の違いを明らかにしました。企業レベルでは，中国の2つの企業に焦点を当て，ケーススタディを用いてISO/IEC 27001がデジタル貿易に与える影響メカニズムを分析しました。

主な研究結果は以下のとおりです。

ISO/IEC 27001認証はデジタル貿易を促進します。
国際レベルでは，ISO/IEC 27001認証は各国のデジタル貿易発展における重要な触媒として機能します。実証研究によると，ISO/IEC 27001認証はデジタル貿易の総量増加に特に顕著な効果を発揮することが示されています。そのため，世界各国の政府は，この認証フレームワークの普及と深い統合を戦略的に推進することが推奨されます。各国政府は，国内規制を国際規格に整合させ，企業認証取得を奨励するなど，体系的な政策指針を実施することで，ISO/IEC 27001が持つ可能性を最大限に引き出し，安全で信頼性の高いデジタル貿易環境を構築することができます。これにより，各国は競争が激化するグローバルデジタル経済において，より幅広い貿易上の優位性を確保することが可能になります。

1 https://www.iso.org/standard/27001.
2 https://www.iso.org/standard/27001.
3 https://www.iso.org/standard/27001.

The impact of ISO/IEC 27001 certification varies throughout different countries. Empirical findings reveal a particularly strong positive correlation in developing countries, where certification significantly expands the total volume of digital trade and substantially boosts export sales. In contrast, the marginal benefit of certification for developed economies, which often possess more mature regulatory frameworks and higher baseline levels of digital trust, is less pronounced. A notable amplification effect is observed within the context of regional trade agreements. Specifically, for countries that are not members of agreements like the Regional Comprehensive Economic Partnership (RCEP), obtaining ISO/IEC 27001 certification serves as a powerful tool to enhance their digital trade engagement, potentially by signalling compliance with internationally recognized security standards and bridging regulatory differences.

ISO/IEC 27001 certification has promoted the development of digital trade in China. At the national level, ISO/IEC 27001 certification demonstrates a statistically significant positive effect on the development of digital trade throughout Chinese provinces. Notably, its influence is more pronounced in advancing industrial digitalization – the integration of digital technologies into traditional industries –compared to enhancing the digital industrialization sector (i.e. the production of digital goods and services). This suggests that the certification's primary value lies in strengthening the digital resilience of existing economic structures rather than solely fostering purely digital sectors. Consequently, provincial policymakers and market participants in China are advised to prioritize investments in information security governance and R&D, leveraging ISO/IEC 27001 as a strategic tool to enhance trustworthiness and operational reliability in digital transactions.

The impact of ISO/IEC 27001 certification varies depending on regional conditions. The impact of ISO/IEC 27001 certification on digital trade exhibits significant regional heterogeneity, correlated with disparities in economic development and geographic location. Economically developed provinces – particularly those along the eastern coast – experience a stronger trade-promoting effect from certification, whereas less developed regions show more modest gains. Geographically, there is a significant promotional effect of ISO/IEC 27001 on digital trade in the eastern and western regions of China, yet little effect in the central area of the country. This imbalance underscores the need for regionally tailored policies, such as targeted guidance for certification in central provinces and coordinated efforts to bridge digital divides through infrastructure modernization.

ISO/IEC 27001 certification promotes digital trade by providing market access and conveying trust. ISO/IEC 27001 certification functions as a critical "passport" for enterprises seeking to compete in regulated or high-stakes markets, including government, finance and telecommunications sectors. In these domains, certification is often a mandatory qualification or a heavily weighted scoring criterion in bidding processes and digital trade. For instance, DPtech and H3C Technologies Co., Ltd. (H3C) leveraged certification to enter domestic and overseas markets with stringent data protection requirements, where it directly influenced project acquisition. By demonstrating adherence to internationally recognized security standards, certification not only enhances trust among clients and partners, but also translates into tangible business growth because it aligns with contractual and regulatory demands.

ISO/IEC 27001認証の効果は，国によって異なります。実証研究によると，特に発展途上国では認証取得がデジタル貿易の総量を大幅に拡大し，輸出額を著しく増加させるという強い正の相関関係が見られます。一方，より成熟した規制枠組みと高いデジタル信頼度を既に有する先進国では，認証取得による効果はそれほど顕著ではありません。地域貿易協定の枠組みにおいては，顕著な増幅効果が観察されます。特に，地域包括的経済連携（RCEP）などの協定に加盟していない国々にとって，ISO/IEC 27001認証の取得は，国際的に認められたセキュリティ規格への準拠を示すことで，デジタル貿易への関与を強化し，規制上の違いを解消する強力な手段となります。

ISO/IEC 27001認証は，中国におけるデジタル貿易の発展を促進してきました。国家レベルでは，ISO/IEC 27001認証は，中国全土のデジタル貿易の発展に統計的に有意なプラスの効果をもたらしています。特に，デジタル産業化（デジタル製品・サービスの生産）の強化よりも，産業のデジタル化（デジタル技術を伝統産業に統合すること）の推進において，その影響はより顕著です。これは，ISO/IEC 27001認証の主な価値は，純粋なデジタルセクターの育成だけではなく，既存の経済構造のデジタルレジリエンスを強化することにあることを示唆しています。したがって，中国の地方政策立案者および市場参加者は，情報セキュリティガバナンスと研究開発への投資を優先し，ISO/IEC 27001をデジタル取引における信頼性と運用信頼性を高めるための戦略的ツールとして活用することが推奨されます。

ISO/IEC 27001認証の影響は，地域状況によって異なります。デジタル貿易に対するISO/IEC 27001認証の影響は，経済発展と地理的位置の格差と相関する，顕著な地域差を示しています。経済的に発展した省，特に東海岸沿いの省では，認証による貿易促進効果がより強く現れる一方，発展途上地域ではその効果は限定的です。地理的に見ると，中国の東部および西部地域ではISO/IEC 27001がデジタル貿易に大きな促進効果をもたらしていますが，中央部地域ではその効果は限定的です。この不均衡は，中央部の省における認証に関する的を絞ったガイダンスや，インフラの近代化を通じたデジタルデバイド解消に向けた協調的な取り組みなど，地域に合わせた政策の必要性を浮き彫りにしています。

ISO/IEC 27001認証は，市場アクセスを提供し，信頼性を高めることで，デジタル貿易を促進します。ISO/IEC 27001認証は，政府，金融，通信などの規制市場や競争の激しい市場での競争を目指す企業にとって，重要な「パスポート」としての役割を果たします。これらの分野では，認証は入札プロセスやデジタル貿易において，必須要件または重要な評価基準となることが少なくありません。例えば，DPtechとH3C Technologies Co., Ltd.（H3C）は，認証を活用することで，厳格なデータ保護要件を持つ国内外市場への参入を果たし，プロジェクト獲得に直接的な影響を与えました。国際的に認められたセキュリティ規格への準拠を示すことで，認証は顧客やパートナー間の信頼を高めるだけでなく，契約上および規制上の要件を満たすため，具体的な事業成長にもつながります。

ISO/IEC 27001 promotes digital trade by reducing risks, improving the efficiency and effectiveness of ISMS, maintaining continuous optimization and enhancing competitive advantage. The implementation of ISO/IEC 27001 drives a structural shift in organizational governance, moving from reactive incident response to a systematic risk-based approach. By establishing a formalized ISMS, both DPtech and H3C clarified departmental roles, streamlined workflows, and optimized the alignment of security controls with operational efficiency. Notably, H3C exemplified maturity in security practices by exceeding baseline certification requirements, using the framework as a validation tool rather than a mere compliance checkpoint. This proactive stance reduces the likelihood of security incidents and strengthens operational resilience, aligning with the standard's emphasis on continuous improvement. This has laid a solid foundation for the development of digital trade.

Table 1: Research summary

Levels of analysis	Methodology	Findings
International level	• Descriptive analysis • Regression analysis	• Countries possessing more ISO/IEC 27001 certifications typically exhibit higher digital trade volumes. • ISO/IEC 27001 exerts a significant promotional effect on the digital trade. • The promoting impact of ISO/IEC 27001 on digital trade exhibits distinct heterogeneous characteristics between developed and developing countries, as well as between RCEP members and non-RCEP members.
National level (China)	• Descriptive analysis • Regression analysis • Machine learning	• ISO/IEC 27001 exerts a significant promotional effect on digital trade in China. • The promoting effect exhibits heterogeneous characteristics between provinces with high and provinces with low economic development, and among eastern, central and western China.
Enterprise level	• Case study	• From an external perspective, the impact mechanisms of ISO/IEC 27001 and its certification are market access and trust in quality. • From an internal perspective, the impact mechanisms of ISO/IEC 27001 on digital trade include: reducing risk, improving the efficiency and effectiveness of the ISMS, enhancing competitive advantage and maintaining continuous optimization.

ISO/IEC 27001は，リスクの低減，ISMSの効率性と有効性の向上，継続的な最適化の維持，そして競争優位性の強化を通じて，デジタル貿易を促進します。

ISO/IEC 27001の導入は，組織ガバナンスの構造的な変革を促し，事後対応型のインシデント対応から，体系的なリスクベースのアプローチへと移行させました。DPtechとH3Cは，正式なISMSを構築することで，各部門の役割を明確化し，ワークフローを効率化し，セキュリティ管理と業務効率の整合性を最適化しました。特にH3Cは，セキュリティフレームワークを単なるコンプライアンスチェックポイントとしてではなく，検証ツールとして活用することで，基本認証要件を上回るセキュリティ対策の成熟度を示しました。このような積極的な姿勢は，セキュリティインシデントの発生確率を低減し，業務の回復力を強化し，継続的改善を重視する規格の理念に合致しています。これにより，デジタル貿易の発展に向けた強固な基盤を築きました。

表 1: 調査概要

分析レベル	方法論	調査結果
国際レベル	• 記述分析 • 回帰分析	• ISO/IEC 27001認証を多く取得している国は，一般的にデジタル貿易量が多い傾向にある。 • ISO/IEC 27001はデジタル貿易に大きな促進効果をもたらしている。 • ISO/IEC 27001のデジタル貿易への促進効果は，先進国と発展途上国，RCEP加盟国と非加盟国の間で明確な異質性を示している。
国家レベル（中国）	• 記述分析 • 回帰分析 • 機械学習	• ISO/IEC 27001は中国のデジタル貿易に大きな促進効果をもたらしている。 • その促進効果は，経済発展の度合いが高い省と低い省，そして中国東部，中部，西部の間で異質性を示している。
企業レベル	• ケーススタディ	• 外部視点では，ISO/IEC 27001とその認証がデジタル貿易に及ぼす影響メカニズムは，市場アクセスと品質への信頼である。 • 内部視点では，ISO/IEC 27001がデジタル貿易に及ぼす影響メカニズムは，リスクの低減，ISMSの効率性と有効性の向上，競争優位性の強化，継続的な最適化の維持である。

1. Research overview

Research background

According to United Nations Conference on Trade and Development (UNCTAD), digital trade refers to cross-border digital delivery service trade. According to the UNCTADstat Data Centre, in 2024, the total import and export volume of digital delivery service trade reached USD 9.06 trillion, reflecting a year-on-year growth rate of 13.8%.[4] This sustained expansion underscores the critical role of digital trade in the global economy. However, its reliance on digital infrastructure exposes it to significant risks, including cyber-attacks, data breaches and service disruptions, which can compromise data integrity and hinder cross-border transactions. Fragmented regulatory environments and varying national cybersecurity exacerbate these challenges, often creating technical barriers to trade. Enterprises need to maintain interconnectivity while ensuring the timeliness and accuracy of information, as well as the smoothness and confidentiality of communication. A powerful ISMS leverages interconnectivity while also managing information security, network security and privacy risks.

ISO/IEC 27001 is the world's best-known ISMS standard (Podrecca, et al., 2023). It defines requirements an ISMS must meet. It also promotes a holistic approach towards information security, including vetting people, policies and technology for information security. An ISMS implemented according to ISO/IEC 27001 is a tool for risk management, cyber-resilience and operational excellence.[5]

ISO/IEC 27001 certification is the written assurance (a certificate) provided by an independent body, which demonstrates an entity's commitment to information security, cybersecurity and privacy protection through audits conducted in accordance with ISO/IEC 27001. Achieving ISO/IEC 27001 certification demonstrates to clients and stakeholders that an organization or business has put in place a system to manage risks related to the security of data owned or handled by the company, and that this system adheres to the best practices and principles enshrined in this International Standard.[6] Today, ISO/IEC 27001 is the fourth-most widespread ISO standard worldwide (Podrecca, et al., 2022) with almost 82 566 certifications in 2023, marking an 18% year-on-year growth rate (ISO, 2024).

Little is known about the digital trade implications of ISO/IEC 27001, despite its growing popularity (Culot et al., 2021). To provide a deeper understanding of the digital trade implications of ISO/IEC 27001, this report focuses on the following research questions:

1. Does ISO/IEC 27001 promote digital trade?
2. What are the differences in its impact in different countries and regions?
3. What is the impact mechanism of ISO/IEC 27001 on digital trade?

By answering these questions, this research aims to provide theoretical insights and decision-making references for policymakers, enterprises and standard setting organizations, as well as promote ISO/IEC 27001 as a catalyst for information security and sustainable growth of digital trade.

To quantify the effects of ISO/IEC 27001, this research measures ISO/IEC 27001 using the number of ISO/IEC 27001 certifications.

4 The data is sourced from https://unctadstat.unctad.org/datacentre/dataviewer/US.DigitallyDeliverableServices.
5 https://www.iso.org/standard/27001
6 https://www.iso.org/standard/27001

1. 研究概要

研究の背景

国連貿易開発会議（UNCTAD）によると，デジタル貿易とは国境を越えたデジタル配信サービス貿易を指します。UNCTADstatデータセンターによると，2024年のデジタル配信サービス貿易の輸出入総額は9兆600億米ドルに達し，前年比13.8%の成長率を示しました。[4] この持続的な拡大は，世界経済におけるデジタル貿易の重要な役割を浮き彫りにしています。しかし，デジタルインフラへの依存度が高いため，サイバー攻撃，データ漏洩，サービス停止といった重大なリスクにさらされており，データの完全性が損なわれ，国境を越えた取引が阻害される可能性があります。規制環境の分断と各国のサイバーセキュリティのばらつきは，これらの課題を悪化させ，しばしば貿易における技術的な障壁を生み出します。企業は，情報の適時性と正確性，そして円滑かつ機密性の高いコミュニケーションを確保しながら，相互接続性を維持する必要があります。強力なISMSは，相互接続性を活用しつつ，情報セキュリティ，ネットワークセキュリティ，プライバシーリスクを管理します。

ISO/IEC 27001は，世界で最も広く知られているISMS規格です（Podreccaet al., 2023）。この規格は，ISMSが満たすべき要件を定義しています。また，情報セキュリティに対する包括的なアプローチを推進しており，情報セキュリティに関する人材，ポリシー，テクノロジーの検証を含みます。ISO/IEC 27001に準拠して実装されたISMSは，リスク管理，サイバーレジリエンス，そして卓越した運用[5] を実現するためのツールとなります。

ISO/IEC 27001認証は，独立機関が発行する書面による保証（証明書）であり，ISO/IEC 27001に準拠した監査を通じて，組織の情報セキュリティ，サイバーセキュリティ，プライバシー保護への取り組みを証明するものです。ISO/IEC 27001認証を取得することで，顧客や利害関係者に対し，組織や企業が，自社が所有または取り扱うデータのセキュリティに関連するリスクを管理するためのシステムを構築しており，そのシステムがこの国際規格[6]に定められたベストプラクティスと原則に準拠していることを示すことができます。現在，ISO/IEC 27001は世界で4番目に広く普及しているISO規格であり（Podreccaet al., 2022），2023年には約82,566件の認証が取得され，前年比18%の成長率を記録しています（ISO，2024）。

ISO/IEC 27001は普及が進んでいるにもかかわらず，デジタル貿易への影響についてはほとんど知られていません（Culot et al., 2021）。ISO/IEC 27001のデジタル貿易への影響をより深く理解するために，本報告書では以下の研究課題に焦点を当てます。

1. ISO/IEC 27001はデジタル貿易を促進するのか？
2. 国や地域によってその影響に違いはあるのか？
3. ISO/IEC 27001はデジタル貿易にどのような影響を与えるのか？

これらの問いに答えることで，本研究は政策立案者，企業，標準化団体に対し，理論的な洞察と意思決定のための参考情報を提供するとともに，情報セキュリティとデジタル貿易の持続的な成長を促進する触媒としてISO/IEC 27001を推進することを目指します。

ISO/IEC 27001の効果を定量化するために，本研究ではISO/IEC 27001認証取得件数を用いてISO/IEC 27001の効果を測定します。

4 データ入手先: https://unctadstat.unctad.org/datacentre/dataviewer/US.DigitallyDeliverableServices.
5 https://www.iso.org/standard/27001
6 https://www.iso.org/standard/27001

Research significance

Theoretical significance

Deepen the research on the outcomes of ISO/IEC 27001

Existing research about ISO/IEC 27001 focuses on four main areas: motivations, implementation process, outcomes and its diffusion (Culot et al., 2021; Podrecca et al., 2023). In terms of outcomes, ISO/IEC 27001 can reduce information security (IS) risk levels (Al-Karaki et al., 2022), enhance business continuity (Rezaei et al., 2014), and serve as a "market entry ticket" for exporting firms (Dionysiou, 2011). Additionally, Podrecca et al. (2022) found that ISO/IEC 27001 certification is associated with improvements in profitability, labour productivity and sales performance. However, few scholars have examined the impact of ISO/IEC 27001 on digital trade.

This research adopts a composite methodology that combines quantitative research at the international and national levels, and qualitative analysis at the enterprise level, aiming to explore the implications of ISO/IEC 27001 for digital trade. The combination of quantitative and qualitative research provides methodological support for a comprehensive and in-depth exploration of the effects and impact mechanisms of ISO/IEC 27001 on digital trade. By doing so, the research deepens the understanding of ISO/IEC 27001's outcomes and extends its analytical scope to the digital trade context.

Expand the research on digital trade determinants

Existing studies on digital trade have extensively analysed external environmental determinants, such as the geographic location (Blum & Goldfarb, 2006), the quantity and quality of telecommunication (Abeliansky & Hilbert, 2017), internet infrastructure and institutional distance (Milner, 2006). They typically overlook the inherent risks of digital technology and digitization, namely data security breaches, privacy vulnerabilities and systemic cyber threats. Different from traditional trade, digital trade emphasizes the digitalization of trade methods and objects. Therefore, there will be a high risk of digital information leakage in digital trade. This report focuses on the risk to digital trade, and specifically investigates the impact of ISO/IEC 27001 in mitigating these risks and facilitating trade flows. In this way, the research expands the analytical dimension and enriches the understanding of digital trade determinants.

Practical significance

Beyond addressing limitations in current research, this report helps clarify the impact of ISO/IEC 27001 on digital trade. At the practical level, it provides a series of actionable directions for the three core stakeholders: international standards organizations, national governments and enterprises.

For international standards organizations, this report provides strategic support for optimizing the promotion of ISO/IEC 27001. The findings show that ISO/IEC 27001 can boost digital trade performance throughout multiple levels. However, adoption rates and resulting impacts vary considerably among countries and regions. To strengthen the standard's contribution, efforts should focus on two priorities:

1. For countries with low ISO/IEC 27001 adoption, intensify promotion to raise awareness and uptake.
2. For developed economies and RCEP member states, further reinforce ISO/IEC 27001 as a driver of digital trade growth by leveraging its proven benefits.

For national governments, this report provides evidence-based decision-making references to enhance the competitiveness of their digital industries. The findings reveal that ISO/IEC 27001 certification significantly boosts digital trade performance at the national, provincial and enterprise levels. Accordingly, governments should acknowledge the strategic importance of ISO/IEC 27001 for the development of digital trade in a country or region. ISO/IEC 27001 certification ought to be treated as a targeted policy instrument and explicitly integrated into

研究の意義

理論的意義

ISO/IEC 27001の成果に関する研究の深化

ISO/IEC 27001に関する既存の研究は，動機，導入プロセス，成果，普及という4つの主要分野に焦点を当てています（Culot et al., 2021; Podrecca et al., 2023）。成果という点では，ISO/IEC 27001は情報セキュリティ（IS）リスクレベルを低減し（Al-Karaki et al., 2022），事業継続性を強化し（Rezaei et al., 2014），輸出企業にとって「市場参入の切符」となる（Dionysiou, 2011）ことが示されています。さらに，Podrecca et al.（2022）は，ISO/IEC 27001認証が収益性，労働生産性，売上高の向上と関連していることを明らかにしました。しかし，ISO/IEC 27001がデジタル貿易に与える影響を検証した研究はほとんどありません。

本研究は，国際レベルおよび国家レベルでの定量的調査と企業レベルでの定性的分析を組み合わせた複合的な手法を採用し，ISO/IEC 27001がデジタル貿易に及ぼす影響を探究することを目的としています。定量的調査と定性的調査を組み合わせることで，ISO/IEC 27001がデジタル貿易に及ぼす影響とそのメカニズムを包括的かつ詳細に探究するための方法論的基盤が提供されます。これにより，本研究はISO/IEC 27001の成果に対する理解を深め，分析範囲をデジタル貿易のコンテキストにまで拡大します。

デジタル貿易の決定要因に関する研究の拡大

デジタル貿易に関する既存の研究では，地理的位置（Blum & Goldfarb, 2006），通信の量と質（Abeliansky & Hilbert, 2017），インターネットインフラ，制度的距離（Milner, 2006）といった外部環境要因が幅広く分析されてきました。一般的に，デジタル技術とデジタル化に伴う固有のリスク，すなわちデータセキュリティ侵害，プライバシー脆弱性，そしてシステム的なサイバー脅威は見過ごされがちです。従来の貿易とは異なり，デジタル貿易は貿易方法と貿易対象物のデジタル化を重視します。そのため，デジタル貿易においてはデジタル情報漏洩のリスクが高くなります。本報告書では，デジタル貿易におけるリスクに焦点を当て，特にISO/IEC 27001がこれらのリスクを軽減し，貿易の流れを促進する上でどのような影響を与えるかを検証します。このようにして，本研究は分析の次元を拡大し，デジタル貿易の決定要因に関する理解を深めます。

実務上の意義

本報告書は，既存の研究における限界を克服するだけでなく，ISO/IEC 27001がデジタル貿易に与える影響を明確にするのに役立ちます。実務レベルでは，国際規格団体，各国政府，企業という3つの主要なステークホルダーに対し，具体的な行動指針を提供します。

国際規格団体にとって，本報告書はISO/IEC 27001の普及促進を最適化するための戦略的支援を提供するものです。調査結果によると，ISO/IEC 27001は複数のレベルでデジタル貿易のパフォーマンスを向上させることができます。しかし，導入率とそれに伴う影響は国や地域によって大きく異なります。規格の貢献を強化するためには，以下の2つの優先事項に注力する必要があります。

1. ISO/IEC 27001の導入率が低い国では，認知度と導入率を高めるための普及促進を強化する。
2. 先進国およびRCEP加盟国は，ISO/IEC 27001の実証済みのメリットを活用することで，デジタル貿易成長の推進力としてISO/IEC 27001をさらに強化する。

各国政府には，本報告書はデジタル産業の競争力強化のためのエビデンスに基づいた意思決定の参考資料を提供します。調査結果は，ISO/IEC 27001認証が国，地方，企業レベルでデジタル貿易のパフォーマンスを大幅に向上させることを示しています。したがって，政府は，国または地域におけるデジタル貿易の発展にとってISO/IEC 27001が戦略的に重要であることを認識すべきです。ISO/IEC 27001認証は，的を絞った政策手段として扱われ，デジタル貿易協定，公共調

digital trade agreements, public procurement criteria and enterprise incentive schemes. Such inclusion can serve as a practical lever to enhance the global competitiveness of national and regional digital sectors.

For enterprise managers, this report highlights the strategic value of ISO/IEC 27001. The decision to pursue ISO/IEC 27001 certification should go beyond merely responding to market demand; it should aim to capture the tangible benefits the standard offers, such as enhanced credibility, reduced risks of fraud, information loss, and data breaches, and access to new business opportunities with security conscious customers and partners. Managers should regard ISO/IEC 27001 and its certification as a strategic asset that facilitates entry into global markets and strengthens long term competitiveness.

Research design[7]

To systematically address the above questions, this research conducts three sub-studies, the first one at the international level, the second one at the national level, and the third one at the enterprise level.

The impact of ISO/IEC 27001 certification on digital trade: The international level

At the international level, the report conducts descriptive analysis and regression analysis on national panel data, to examine the impact of ISO/IEC 27001 on the digital trade of a country, including total trade volume, trade export volume and trade import volume. Furthermore, regression methods are also used to identify the differences in the effects of ISO/IEC 27001 on different types of countries, such as developed and developing countries, RCEP members and non-RCEP members.

The impact of ISO/IEC 27001 certification on digital trade in China: The national level

At the national level, the report focuses on China, a major digital trading country with the highest number of ISO/IEC 27001 certifications (ISO Survey 2024[8]). It conducts descriptive analysis and regression analysis on provincial panel data in China to explore the effects of ISO/IEC 27001 on the digital trade of a province, including the level of digital trade development, and two primary indicators – digital ordering trade driven by industrial digitization, and digital products, services and technology trade. The former focuses on the digital ordering trade resulting from use of digital technology to upgrade production, circulation and transactions in traditional manufacturing, agriculture and service industries. The latter focuses on cross-border transactions of digital technology, products and services. Furthermore, this report identifies the differences in the effects of ISO/IEC 27001 between high and low economic development regions, and between China's eastern, central and western regions.

The impact of ISO/IEC 27001 certification on digital trade in China: The enterprise level

The report focuses on DPtech and H3C, and analyses the impact mechanism of ISO/IEC 27001 on their digital trade through case studies. This section first explores the core drivers motivating enterprises to pursue certification, clarifying the endogenous forces behind undertaking ISO/IEC 27001 certification. Building on this foundation, it maps the certification implementation process and evaluates its effectiveness, providing evidence-based corporate-level insights for peer enterprises.

7 The detailed methodology is available upon request. Please contact research@iso.org for more information.
8 ISO - The ISO Survey

達基準，企業奨励制度に明確に組み込まれるべきです。このような組み込みは，国および地域のデジタルセクターの国際競争力を強化するための実践的な手段となり得ます。

本報告書は，企業経営者にISO/IEC 27001の戦略的価値を強調しています。ISO/IEC 27001認証の取得は，単に市場の需要に応えるだけでなく，より深い理解に基づいて行われるべきです。この規格がもたらす具体的なメリット，例えば信頼性の向上，不正行為，情報漏洩，データ侵害のリスク低減，セキュリティ意識の高い顧客やパートナーとの新たなビジネス機会の獲得などを目指すべきです。経営者は，ISO/IEC 27001とその認証を，グローバル市場への参入を促進し，長期的な競争力を強化する戦略的資産として捉えるべきです。

研究のデザイン[7]

上記の疑問に体系的に取り組むため，本研究では3つのサブスタディを実施します。1つ目は国際レベル，2つ目は国家レベル，3つ目は企業レベルです。

ISO/IEC 27001認証がデジタル貿易に与える影響：国際レベル

国際レベルでは，各国のパネルデータを用いて記述分析と回帰分析を行い，ISO/IEC 27001が各国のデジタル貿易（総貿易量，輸出量，輸入量を含む）に与える影響を検証します。さらに，回帰分析手法を用いて，先進国と発展途上国，RCEP加盟国と非加盟国など，国の種類によってISO/IEC 27001の効果に違いがあるかどうかを特定しています。

ISO/IEC 27001認証が中国のデジタル貿易に与える影響：国家レベル

国家レベルでは，本報告書は，ISO/IEC 27001認証取得件数が最も多い主要なデジタル貿易国である中国（ISO調査2024[8]）に焦点を当てています。中国の省レベルのパネルデータを用いて記述分析と回帰分析を行い，ISO/IEC 27001が各省のデジタル貿易に与える影響，具体的にはデジタル貿易の発展レベル，そして産業のデジタル化によって促進されるデジタル発注貿易とデジタル製品・サービス・技術貿易という2つの主要指標について分析しています。前者は，伝統的な製造業，農業，サービス業における生産，流通，取引の高度化にデジタル技術を活用することで生じるデジタル注文取引に焦点を当てています。後者は，デジタル技術，製品，サービスの越境取引に焦点を当てています。さらに，本報告書では，ISO/IEC 27001の影響が，経済発展の高低地域間，および中国の東部，中部，西部地域間でどのように異なるかを明らかにしています。

中国におけるISO/IEC 27001認証がデジタル貿易に与える影響：企業レベル

本報告書は，DPtechとH3Cに焦点を当て，ケーススタディを通して，ISO/IEC 27001が両社のデジタル貿易に与える影響メカニズムを分析しています。まず，企業が認証取得を目指す動機となる主要な要因を探り，ISO/IEC 27001認証取得の背景にある内生的要因を明らかにします。この基礎に基づき，認証取得プロセスをマッピングし，その有効性を評価することで，同業他社にとってエビデンスに基づいた企業レベルの知見を提供します。

7 詳細な方法論はご要望に応じて提供いたします。詳細については，research@iso.orgまでお問い合わせください。

8 ISO - ISO調査

2. The impact of ISO/IEC 27001 certification on digital trade: International level

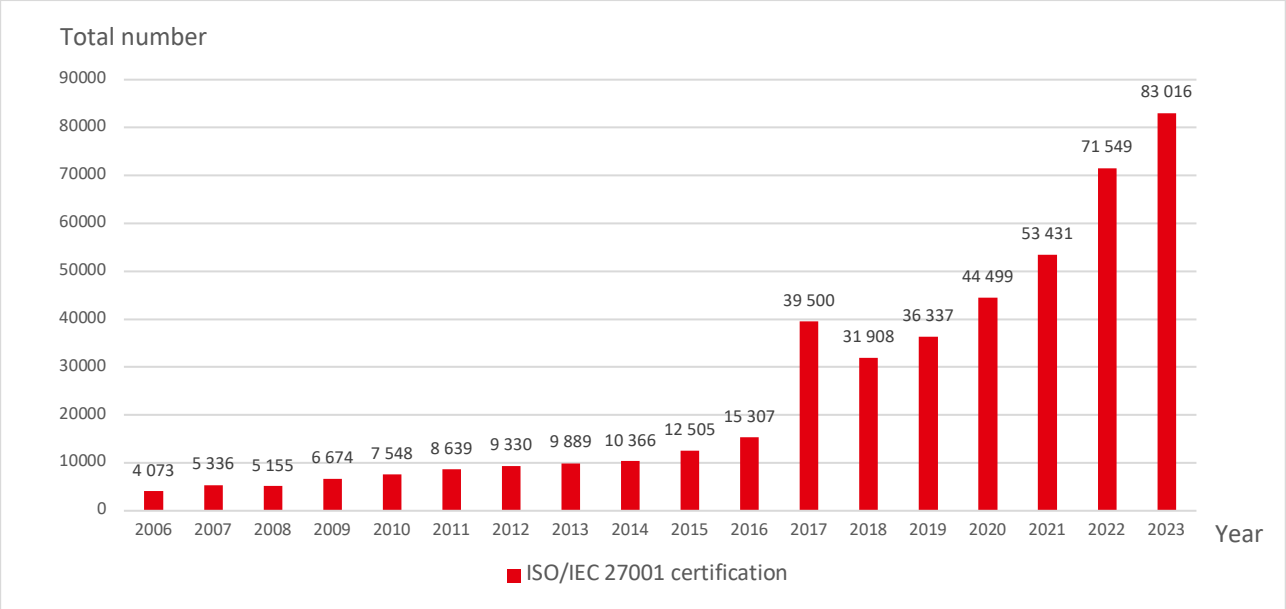
The global landscape of ISO/IEC 27001 certification

Global distribution

The ISO Survey counted the number of ISO/IEC 27001 certification certificates in 165 countries from 2006 to 2023. The total number of ISO/IEC 27001 certification certificates in 165 countries over the years is shown in Figure 1.

The first year of ISO/IEC 27001 certification was 2006, with a total of 4 073 valid certifications worldwide. By 2023, this figure had surged to 83 016 valid certifications globally. In less than two decades, the scale of valid ISO/IEC 27001 certifications has expanded more than 20-fold. This underscores the rising importance of information security within the global context of deepening digital economic development, highlighting the growing value and significance of the ISO/IEC 27001 standard, which has gained widespread recognition in global markets.

Figure 1: Total number of valid ISO/IEC 27001 certifications throughout the world



Source: ISO Survey(2006-2023): The number of ISO/IEC 27001 certifications in China in 2023 is from the National Certification and Accreditation Information Public Service Platform. After cross-checking the total number of certifications in China in the ISO Survey, due to the significant difference in data for 2023, the number of ISO/IEC 27001 certifications in China in 2023, as calculated by the State Administration for Market Regulation, was chosen as a replacement.

2. ISO/IEC 27001認証がデジタル貿易に与える影響：国際レベル

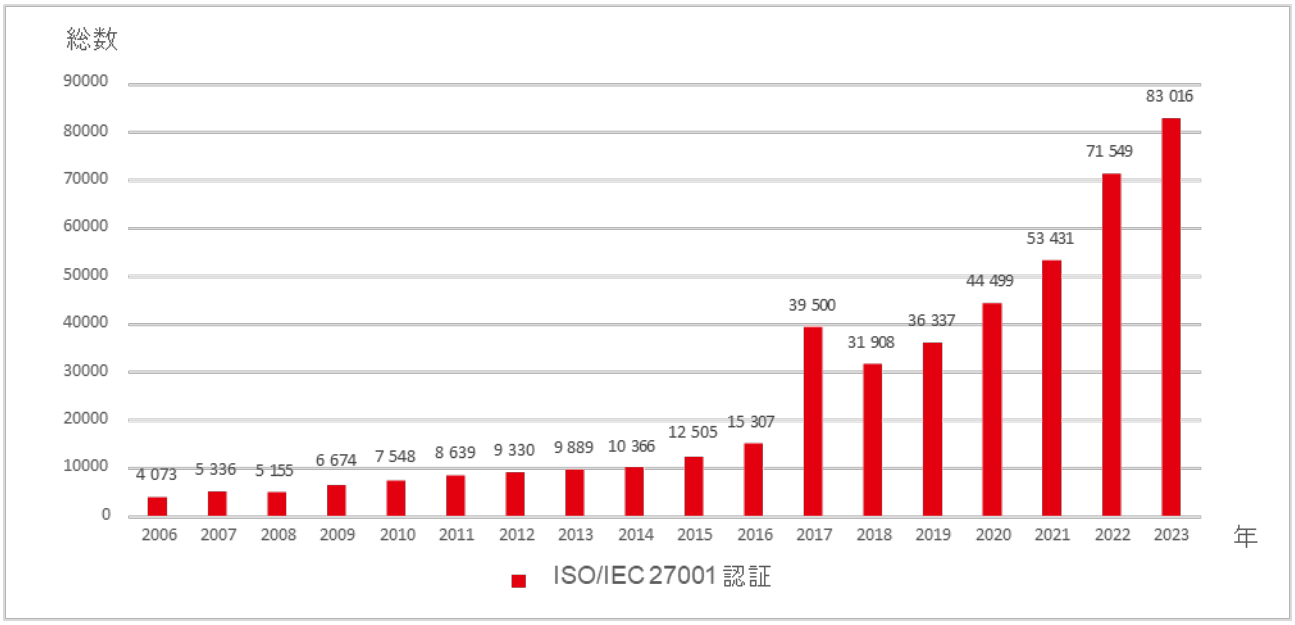
ISO/IEC 27001認証のグローバルな状況

グローバル分布

ISO調査では，2006年から2023年までの165か国におけるISO/IEC 27001認証取得件数を集計しました。165か国におけるISO/IEC 27001認証取得件数の推移は図1に示されています。

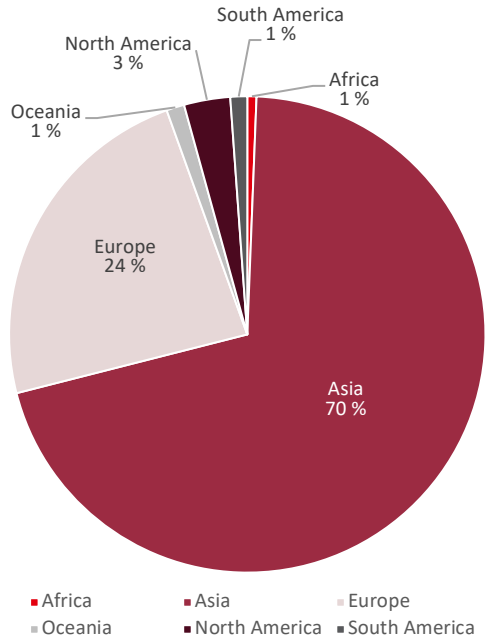
ISO/IEC 27001認証制度が始まったのは2006年で，世界全体で有効な認証件数は4,073件でした。2023年には，この数字は世界全体で83,016件にまで急増しました。わずか20年足らずで，有効なISO/IEC 27001認証の規模は20倍以上に拡大したことになります。これは，デジタル経済の発展が深化するグローバルな状況において情報セキュリティの重要性が高まっていることを示しており，世界市場で広く認知されているISO/IEC 27001規格の価値と重要性が増していることを示しています。

図 1: 世界における有効なISO/IEC 27001認証の総数



出典：ISO調査（2006～2023年）：2023年の中国におけるISO/IEC 27001認証数は，国家認証認可情報公開サービスプラットフォームのデータに基づいています。ISO調査における中国の総認証数と照合した結果，2023年のデータに大きな差異が見られたため，国家市場監督管理総局が算出した2023年の中国におけるISO/IEC 27001認証数を代替データとして使用しました。

Figure 2: Global distribution of ISO/IEC 27001 certification



Source: ISO Survey 2023

Figure 2 highlights the global distribution of ISO/IEC 27001 certifications in 2023, according to the latest findings from the ISO Survey. Distribution is uneven. Asia holds the largest share, accounting for 70% of the world's total valid ISO/IEC 27001 certifications in 2023. This substantial proportion is primarily driven by digitally active economies such as China, India and Japan, where demand for an ISMS is significant. Europe follows with approximately 24%, reflecting the stable trajectory of its mature markets. Together, these two continents (Asia and Europe) account for 94.7% of all valid certifications globally. North America, however, contributes only 3.2%, a figure disproportionate to its economic scale. The combined certifications from Africa, Oceania and South America account for less than 3% of the global total, indicating that the demand for international information security certification among enterprises and organizations in these regions remain in its nascent stages.

Changes in the number of valid ISO/IEC 27001 certifications

Table 2 presents the top ten countries in terms of ISO/IEC 27001 certification numbers from 2019 to 2023. Analysis of the ranking changes reveals that, overall, the list of countries entering the top ten has remained relatively stable.

China leads with exponential growth

China maintains a dominant position, with certifications increasing nearly fivefold over five years, from 8 356 in 2019 to 39 835 in 2023. This surge reflects China's intensified focus on cybersecurity regulations, including the Data Security Law (2021) and Personal Information Protection Law (2021), which mandate robust information security practices for businesses.

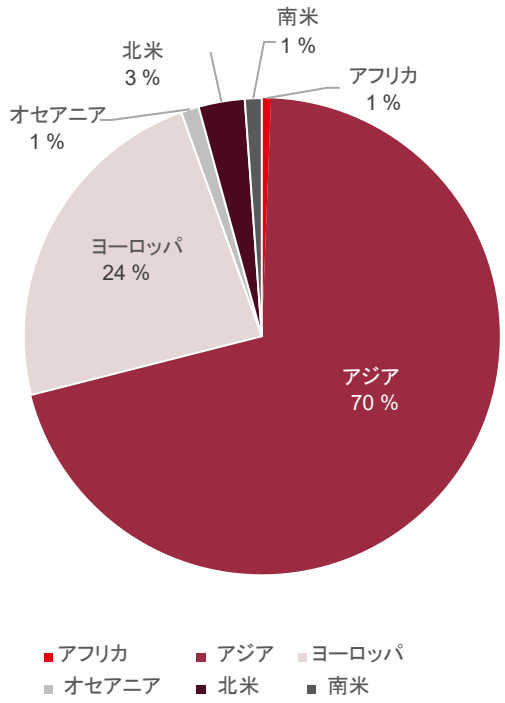
Japan and India show sustained adoption

Japan remains a consistent second, with certifications growing steadily from 5 245 (2019) to 5 599 (2023). India exhibits notable growth, rising from 2 309 (2019) to 3 877 (2023), driven by government initiatives like India's National Cybersecurity Strategy and increasing demand for compliance in IT and outsourcing sectors.

European countries dominate the top tier

Germany, the Netherlands, Spain and the UK consistently rank among the top 10, underscoring Europe's stringent General Data Protection Regulation (GDPR)-driven approach to data protection. The UK, in particular, saw a sharp rise post-Brexit, with certifications jumping from 2 818 (2019) to 6 084 (2021) before stabilizing at 3 630 (2023).

図 2: 世界のISO/IEC 27001認証分布



出典：ISO調査2023

図2は，ISO調査の最新結果に基づき，2023年におけるISO/IEC 27001認証の世界分布を示しています。分布は地域によって大きく異なります。アジアが最大のシェアを占め，2023年の世界の有効なISO/IEC 27001認証総数の70%を占めています。この大きな割合は，主に中国，インド，日本といったデジタル化が進んだ経済圏によって牽引されており，これらの地域ではISMS（情報セキュリティマネジメントシステム）への需要が非常に高いことが要因となっています。ヨーロッパは約24%でそれに続き，成熟市場の安定した成長を反映しています。アジアとヨーロッパの2大陸を合わせると，世界の有効な認証総数の94.7%を占めています。しかし，北米の貢献度はわずか3.2%に過ぎず，その経済規模に見合わない数字となっています。アフリカ，オセアニア，南米の認証取得件数を合わせても世界全体の3%未満であり，これらの地域における企業や組織の間での国際情報セキュリティ認証の需要は依然として初期段階にあることを示しています。

有効なISO/IEC 27001認証件数の推移

表2は，2019年から2023年までのISO/IEC 27001認証取得件数上位10カ国を示しています。ランキングの変動を分析すると，上位10カ国にランクインする国は全体的に比較的安定していることがわかります。

中国が驚異的な成長でリード

中国は圧倒的な地位を維持しており，認証件数は2019年の8,356件から2023年には39,835件へと，過去5年間で約5倍に増加しました。この急増は，データセキュリティ法（2021年）や個人情報保護法（2021年）など，企業に強固な情報セキュリティ対策を義務付ける法律を含む，中国政府のサイバーセキュリティ規制強化を反映しています。

日本とインドは着実な導入

日本は引き続き2位を維持し，認証件数は2019年の5,245件から2023年には5,599件へと着実に増加しています。インドも顕著な成長を見せており，2019年の2,309件から2023年には3,877件へと増加しています。これは，インド政府の国家サイバーセキュリティ戦略などの取り組みや，ITおよびアウトソーシング分野におけるコンプライアンスへの需要の高まりが要因となっています。

欧州諸国が上位を席巻

ドイツ，オランダ，スペイン，英国は常にトップ10にランクインしており，欧州における厳格な一般データ保護規則（GDPR）に基づくデータ保護への取り組みを裏付けています。特に英国では，ブレグジット（EU離脱）後に認証件数が急増し，2019年の2,818件から2021年には6,084件に増加した後，2023年には3,630件で安定しました。

The data illustrates a clear trend: ISO/IEC 27001 certification is expanding globally, driven by regulatory pressures, digital transformation and the need for secure cross-border trade. The rising adoption of ISO/IEC 27001 in diverse economies signals growing recognition of information security as a trade enabler. Countries with higher certification rates – such as China, European countries and Japan – are better positioned to mitigate cyber risks, comply with international regulations, and enhance trust in digital transactions.

Table 2: Top 10 countries for ISO/IEC 27001 certification, 2019-2023

	2019		2020		2021		2022		2023	
	Country	Certif-icates	Country	Certif-icates	Country	Certif-icates	Country	Certif-icates	Country	Certif-icates
1	China	8356	China	12403	China	18446	China	26301	China	39835
2	Japan	5245	Japan	5645	Japan	6587	Japan	6987	Japan	5599
3	UK	2818	UK	3327	India	2775	UK	6084	India	3877
4	India	2309	India	2226	Italy	1924	India	2969	UK	3630
5	Italy	1365	Italy	1827	US	1742	Italy	2424	Italy	3176
6	Germany	1175	Nether-lands	1326	Germany	1673	US	1980	US	1898
7	Nether-lands	938	Germany	1281	Nether-lands	1508	Nether-lands	1741	Israel	1712
8	Spain	938	US	1058	Taiwan, Province of China	1129	Germany	1582	Spain	1582
9	US	757	Spain	997	Israel	1056	Spain	1561	Germany	1563
10	Turkey	729	Taiwan, Province of China	895	Romania	951	Israel	1467	Romania	1510

*UK: United Kingdom of Great Britain and Northern Ireland
Source: ISO Survey 2023; The number of ISO/IEC 27001 certifications in China for 2023 is sourced from the National Certification and Accreditation Information Public Service Platform (China). After cross-checking the total number of certifications in China in the ISO Survey, due to the significant difference in data for 2023, the number of ISO/IEC 27001 certifications in China in 2023 (as calculated by the State Administration for Market Regulation) was chosen as a replacement.

Overview of world's digital trade

Global distribution

The total import and export volume of global digital trade has grown from USD 3.41 trillion in 2010 to USD 9.06 trillion in 2024 as shown in Figure 3, demonstrating a steady expansion. Growth has accelerated in recent years, surpassing the USD 9 trillion mark in 2024, reflecting digital trade's increasing penetration in the global economy. Although a minor downturn was registered in 2015, this did not alter its positive long-term trajectory, as evidenced by the rapid reversal to form in 2016. Looking ahead, the continuous advancement of information technologies, such as big data and artificial intelligence (AI), will continue to empower global digital trade, sustaining its robust growth momentum.

このデータは明確な傾向を示しています。ISO/IEC 27001認証は，規制圧力，デジタルトランスフォーメーション，そして安全な国境を越えた貿易の必要性によって，世界的に拡大しています。多様な経済圏におけるISO/IEC 27001の採用拡大は，情報セキュリティが貿易を促進する要素として認識されつつあることを示しています。中国，欧州諸国，日本など，認証率の高い国々は，サイバーリスクの軽減，国際規制の遵守，そしてデジタル取引における信頼性の向上において，より有利な立場にあります。

表 2: ISO/IEC 27001認証取得国トップ10（2019年～2023年）

	2019		2020		2021		2022		2023	
	国名	認証件数	国名	認証件数	国名	認証件数	国名	認証件数	国名	認証件数
1	中国	8356	中国	12403	中国	18446	中国	26301	中国	39835
2	日本	5245	日本	5645	日本	6587	日本	6987	日本	5599
3	英国	2818	英国	3327	インド	2775	英国	6084	インド	3877
4	インド	2309	インド	2226	イタリア	1924	インド	2969	英国	3630
5	イタリア	1365	イタリア	1827	米国	1742	イタリア	2424	イタリア	3176
6	ドイツ	1175	オランダ	1326	ドイツ	1673	米国	1980	米国	1898
7	オランダ	938	ドイツ	1281	オランダ	1508	オランダ	1741	イスラエル	1712
8	スペイン	938	米国	1058	台湾	1129	ドイツ	1582	スペイン	1582
9	米国	757	スペイン	997	イスラエル	1056	スペイン	1561	ドイツ	1563
10	トルコ	729	台湾	895	ルーマニア	951	イスラエル	1467	ルーマニア	1510

*英国：グレートブリテン及び北アイルランド連合王国

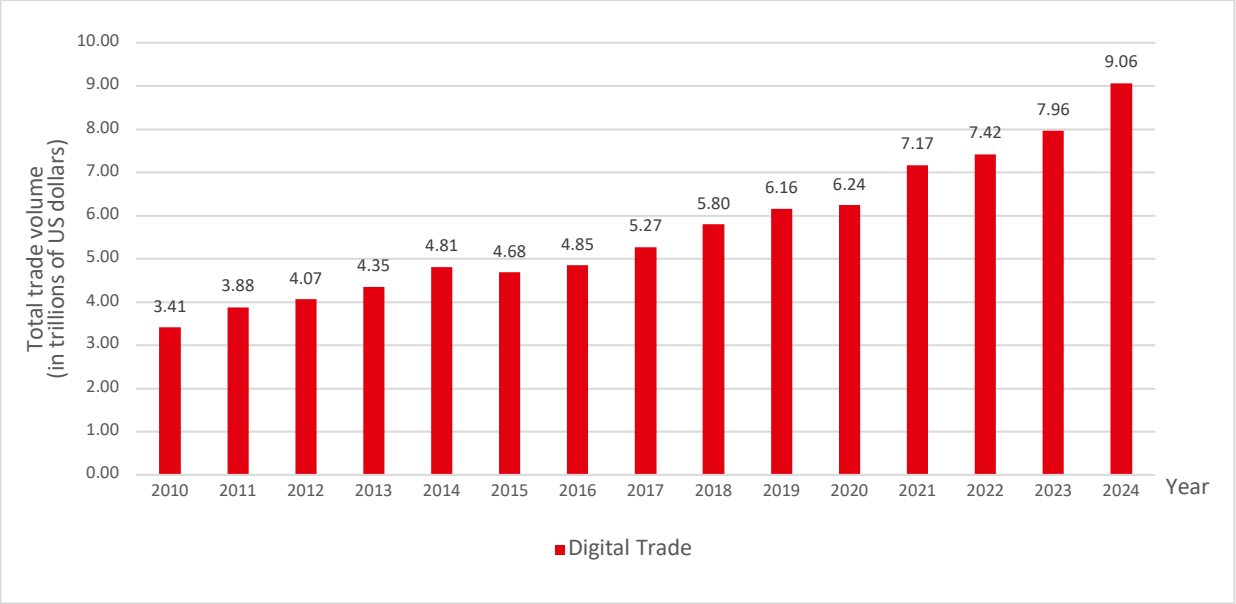
出典：ISO調査2023；2023年の中国におけるISO/IEC 27001認証件数は，国家認証認可情報公開サービスプラットフォーム（中国）のデータに基づいています。ISO調査における中国全体の認証件数と照合した結果，2023年のデータに大きな差異が見られたため，国家市場監督管理総局が算出した2023年の中国におけるISO/IEC 27001認証件数を代替値として採用しました。

世界のデジタル貿易の概要

世界分布

図3に示すように，世界のデジタル貿易の輸出入総額は，2010年の3兆4,100億米ドルから2024年には9兆600億米ドルへと着実に拡大しています。近年は成長が加速し，2024年には9兆米ドルを突破しました。これは，デジタル貿易が,世界経済に浸透しつつあることを示しています。2015年には若干の落ち込みが見られたものの，2016年の急速な回復が示すように，長期的な成長軌道は揺るぎませんでした。今後，ビッグデータや人工知能（AI）といった情報技術の継続的な進歩は，世界のデジタル貿易をさらに活性化させ，力強い成長の勢いを維持していくでしょう。

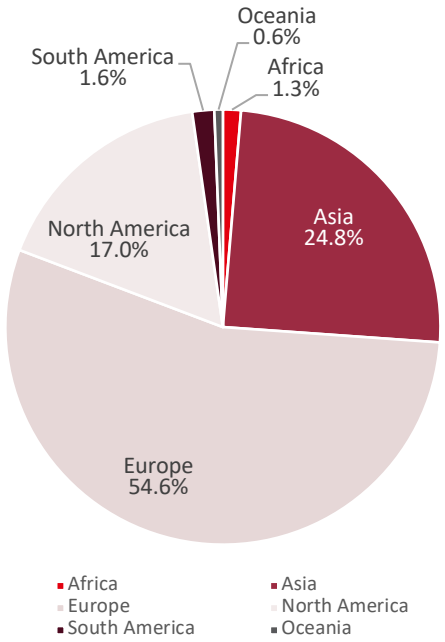
Figure 3: Changes in total digital trade volume



Source: UNCTADstat

Figure 4 illustrates the distribution of global digital trade volume throughout continents in 2024, revealing a pattern of high concentration and significant imbalance.

Figure 4: Global distribution of digital trade



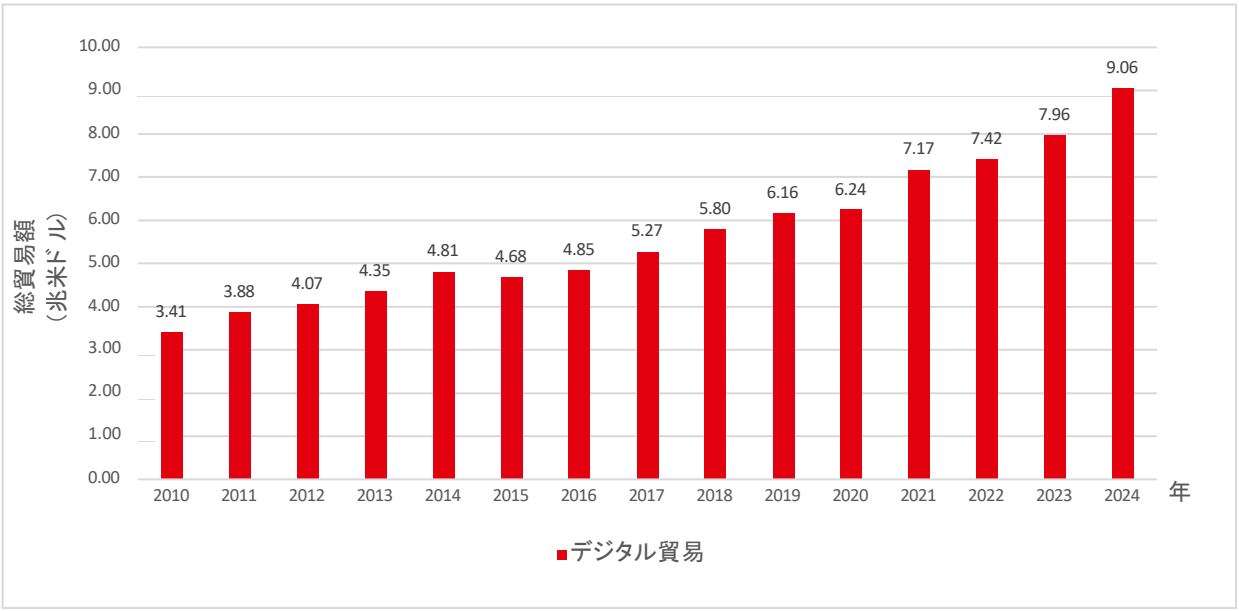
Source: UNCTADstat

The current landscape of global digital trade exhibits the following characteristics:

Dominated by the dual powerhouses of Europe and Asia

Europe accounted for 54.6% of global digital trade in 2024, exceeding one-half of the world's digital trade output. This achievement stems primarily from its robust digital infrastructure and integrated market. Asia, as the world's manufacturing hub and most populous continent, leveraged its vast domestic market to propel digital trade growth, accounting for 24.8% of the total– approximately one-quarter of the global figure. Together, these two continents accounted for 79.4% of global digital trade, signifying that nearly eight out of ten digital trade transactions occur within them. As such, they represent the core drivers and consumer markets of the global digital economy.

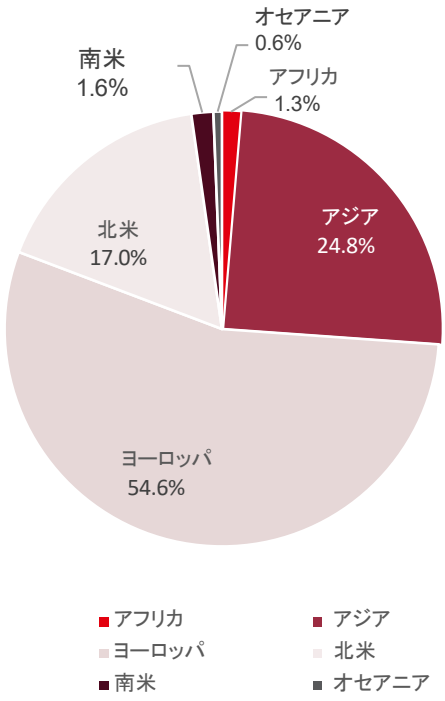
図 3: デジタル貿易総額の推移



出典：UNCTADstat

図4は，2024年における世界のデジタル貿易総額の地域別分布を示しており，高い集中度と著しい不均衡が明らかになっています。

図 4: 世界のデジタル貿易分布



出典：UNCTADstat

世界のデジタル貿易の現状は，以下の特徴を示しています。

ヨーロッパとアジアの二大勢力が支配的

2024年，ヨーロッパは世界のデジタル貿易の54.6%を占め，世界のデジタル貿易生産高の半分以上を占めました。この成果は主に，ヨーロッパの強固なデジタルインフラと統合された市場によるものです。世界の製造拠点であり，最も人口の多い大陸であるアジアは，広大な国内市場を活用してデジタル貿易の成長を牽引し，全体の24.8%を占め，世界の約4分の1を占めています。これら2つの大陸は，世界のデジタル貿易の79.4%を占めており，デジタル貿易取引の約8割がこれらの地域で行われていることを示しています。つまり，両地域は世界のデジタル経済の中核的な推進力と消費市場を担っていると言えます。

North America maintains a steady third place

North America maintains a steady third place with a share of approximately 17.0%. Although it lags significantly behind the top two regions, it continues to play a crucial role. For instance, the United States, as the birthplace of numerous global technology giants, stands as the world's largest exporter of digital intellectual property, such as cloud computing and semiconductor chips. Possessing formidable digital technologies and significant influence, it underpins its position within global digital trade.

South America, Oceania and Africa have considerable room for growth

Africa, Oceania, South America collectively account for a relatively small share of global digital trade, standing at just 3.5%. This indicates that these regions are relatively weak in the digital trade sphere and possess considerable room for improvement. Shortcomings in digital infrastructure, cross-border payments and cross-border logistics constrain room for improvement.

Changes in digital trade volume rankings

Table 3: Top 10 countries by digital trade volume*, 2020-2024

Economy	2020		2021		2022		2023		2024	
	Volume	Rank	Volume	Rank	Volume	Rank	Volume	Rank	Volume	Rank
US	871 778	1	986 740	1	1 060 477	1	1 090 186	1	1 228 311	1
Ireland	607 941	2	629 696	2	642 022	2	701 891	2	854 767	2
UK	482 031	3	571 215	3	561 223	3	667 402	3	730 488	3
Germany	396 189	4	472 444	4	464 707	4	521 319	4	562 764	4
Netherlands	304 245	5	337 961	6(↓1)	355 676	6	407 581	5(↑1)	405 049	7(↓2)
China	286 301	6	351 057	5(↑1)	364 165	5	387 583	7(↓2)	385 487	9(↓2)
France	262 743	7	300 258	8(↓1)	306 766	9(↓1)	357 799	8(↑1)	395 915	8
Singapore	254 479	8	303 074	7(↑1)	330 041	8(↓1)	349 429	9(↓1)	410 600	6(↑3)
Japan	253 697	9	269 496	10(↓1)	258 370	10	271 049	10	289 137	10
India	231 146	10	273 988	9(↑1)	340 740	7(↑2)	387 685	6(↑1)	420 046	5(↑1)

*USD at current prices in millions Source: UNCTADstat

北米は安定した第3位を維持

北米は，約17.0%のシェアで安定した第3位を維持しています。上位2地域には大きく差をつけられていますが，依然として重要な役割を果たしています。例えば，数々のグローバルテクノロジー企業の発祥地である米国は，クラウドコンピューティングや半導体チップなどのデジタル知的財産の世界最大の輸出国です。強力なデジタル技術と大きな影響力を持つ米国は，世界のデジタル貿易における地位を確固たるものにしています。

南米，オセアニア，アフリカには大きな成長の余地

アフリカ，オセアニア，南米は，世界のデジタル貿易に占める割合がわずか3.5%と比較的小さいです。これは，これらの地域がデジタル貿易の分野で比較的弱く，大きな成長の余地があることを示しています。デジタルインフラ，国境を越えた決済，国境を越えた物流における課題が，改善の余地を制限しています。

デジタル貿易量ランキングの変動

図 3: デジタル貿易量上位10カ国*（2020年～2024年）

経済圏	2020		2021		2022		2023		2024	
	貿易量	順位	貿易量	順位	貿易量	順位	貿易量	順位	貿易量	順位
米国	871 778	1	986 740	1	1 060 477	1	1 090 186	1	1 228 311	1
アイルランド	607 941	2	629 696	2	642 022	2	701 891	2	854 767	2
英国	482 031	3	571 215	3	561 223	3	667 402	3	730 488	3
ドイツ	396 189	4	472 444	4	464 707	4	521 319	4	562 764	4
オランダ	304 245	5	337 961	6(↓1)	355 676	6	407 581	5(↑1)	405 049	7(↓2)
中国	286 301	6	351 057	5(↑1)	364 165	5	387 583	7(↓2)	385 487	9(↓2)
フランス	262 743	7	300 258	8(↓1)	306 766	9(↓1)	357 799	8(↑1)	395 915	8
シンガポール	254 479	8	303 074	7(↑1)	330 041	8(↓1)	349 429	9(↓1)	410 600	6(↑3)
日本	253 697	9	269 496	10(↓1)	258 370	10	271 049	10	289 137	10
インド	231 146	10	273 988	9(↑1)	340 740	7(↑2)	387 685	6(↑1)	420 046	5(↑1)

*米ドル（時価，百万ドル）出典：UNCTADstat

Table 3 presents the specific volumes and ranking shifts of the top ten countries in global digital trade from 2020 to 2024. These figures enable further analysis of the development trajectory of global digital trade. It is evident that global digital trade exhibits a distinctly stratified pattern: the first tier comprising the top four countries maintains a stable lead, while intense competition prevails among the subsequent mid-tier countries.

First-tier countries: Germany, Ireland, the UK and the US

The US has maintained its position as the world's largest digital trade economy, with its total value growing from USD 8.71 trillion in 2019 to USD 12.28 trillion in 2024 – an increase of approximately USD 3.5 trillion over five years. Its scale is nearly one-and-a-half times that of second-placed Ireland and more than 40 times that of tenth-ranked Japan. Ireland, the UK and Germany have ranked second to fourth globally for three consecutive years, reflecting the solid foundations and sustained competitiveness of Europe's traditional economic powerhouses in the digital trade sphere. Ireland's volume grew steadily from USD 6.07 trillion in 2020 to USD 8.54 trillion in 2023, maintaining positive sustained growth despite its substantial trade volume, demonstrating its formidable competitive edge and robust digital infrastructure. The UK initially exhibited steady growth, experiencing a slight dip in 2022 before rebounding strongly in 2023 and reaching USD 7.3 trillion in 2024. Germany similarly experienced a slight dip in 2022 following gradual growth from 3.96 trillion US dollars in 2020, but resumed expansion in 2023 to reach 5.21 trillion US dollars, continuing its ascent to 5.62 trillion US dollars in 2024.

It is evident that significant disparities exist among the four countries in the first tier. All possess substantial scale and stable rankings, but the US maintains a sizeable lead in digital trade volume over subsequent countries, consistently securing the top position. Ireland follows closely behind with sustained growth.

In contrast, Germany and the UK experienced relative declines, though their subsequent recovery demonstrates remarkable resilience and recovery capacity within their digital economies. It is also noteworthy that Germany, ranked fourth, forms a watershed between the two tiers of the digital economy. The gap between its digital trade volume and that of the fifth-ranked country exceeds one trillion dollars, making it extremely difficult for latecomers to break into the top four in the short term.

Second-tier countries: China, France, India, Japan, the Netherlands and Singapore

The most notable shift was China's progression from sixth place in 2020 to fifth, followed by a decline to seventh in 2023 and ultimately ninth in 2024. Meanwhile, India and Singapore ascended to fifth and sixth positions respectively, reshaping the hierarchy of the digital trade sphere. France and the Netherlands exhibited a fluctuating yet persistent pursuit. Japan, starting at ninth place, subsequently ranked tenth for four consecutive years, with the gap to the leading positions steadily widening. The divergent performances within the second tier also reflect differing developmental models and stages in each nation's digital trade. For instance, India and Singapore are currently in an advantage-driven growth phase, leveraging their unique strengths. China's decline does not necessarily signify an absolute reduction in capability, but rather reflects its ongoing transformation.

In summary, whether through the sustained leadership of top-tier countries or the dynamic competition among mid-tier countries, both have collectively propelled the continuous expansion and development of digital trade worldwide.

表3は，2020年から2024年までの世界のデジタル貿易上位10カ国の具体的な貿易量と順位変動を示している。これらの数値は，世界のデジタル貿易の発展軌跡をさらに分析する上で役立ちます。世界のデジタル貿易が明確な階層構造を示していることが明らかです。上位4カ国からなる第一層は安定したリードを維持している一方，それに続く中位層では激しい競争が繰り広げられています。

第一層の国:ドイツ，アイルランド，英国，米国

米国は世界最大のデジタル貿易経済としての地位を維持しており，その総額は2019年の8兆7100億米ドルから2024年には12兆2800億米ドルに増加し，5年間で約3兆5000億米ドル増加しました。その規模は，2位のアイルランドの約1.5倍，10位の日本の40倍以上です。アイルランド，英国，ドイツは3年連続で世界第2位から第4位にランクインしており，欧州の伝統的な経済大国がデジタル貿易分野で強固な基盤と持続的な競争力を持っていることを示しています。アイルランドの貿易量は2020年の6兆700億米ドルから2023年には8兆5400億米ドルに着実に増加し，貿易量が多いにもかかわらず持続的なプラス成長を維持しており，その強力な競争優位性と頑健なデジタルインフラを示しています。英国は当初，着実な成長を遂げ，2022年に若干の落ち込みを見せた後，2023年には力強く回復し，2024年には7兆3,000億米ドルに達しました。ドイツも同様に，2020年の3兆9,600億米ドルから緩やかな成長を続けた後，2022年に若干の落ち込みを経験しましたが，2023年には再び拡大し，5兆2,100億米ドルに達し，2024年には5兆6,200億米ドルへと上昇を続けました。

上位4カ国間には，大きな格差が存在することは明らかです。いずれの国も相当な規模と安定した順位を維持していますが，米国はデジタル貿易量において他国を大きく引き離し，常にトップの座を確保しています。アイルランドは持続的な成長を遂げ，米国に僅差で続いています。

一方，ドイツと英国は相対的に落ち込みを経験しましたが，その後の回復は，両国のデジタル経済における驚くべきレジリエンスと回復能力を示しています。また，4位にランクインしたドイツは，デジタル経済の2つの階層を分ける分水嶺となっていることも注目に値します。デジタル貿易額において，中国と5位の国との差は1兆ドルを超えており，後発国が短期間でトップ4入りするのは極めて困難です。

第二層の国:中国，フランス，インド，日本，オランダ，シンガポール

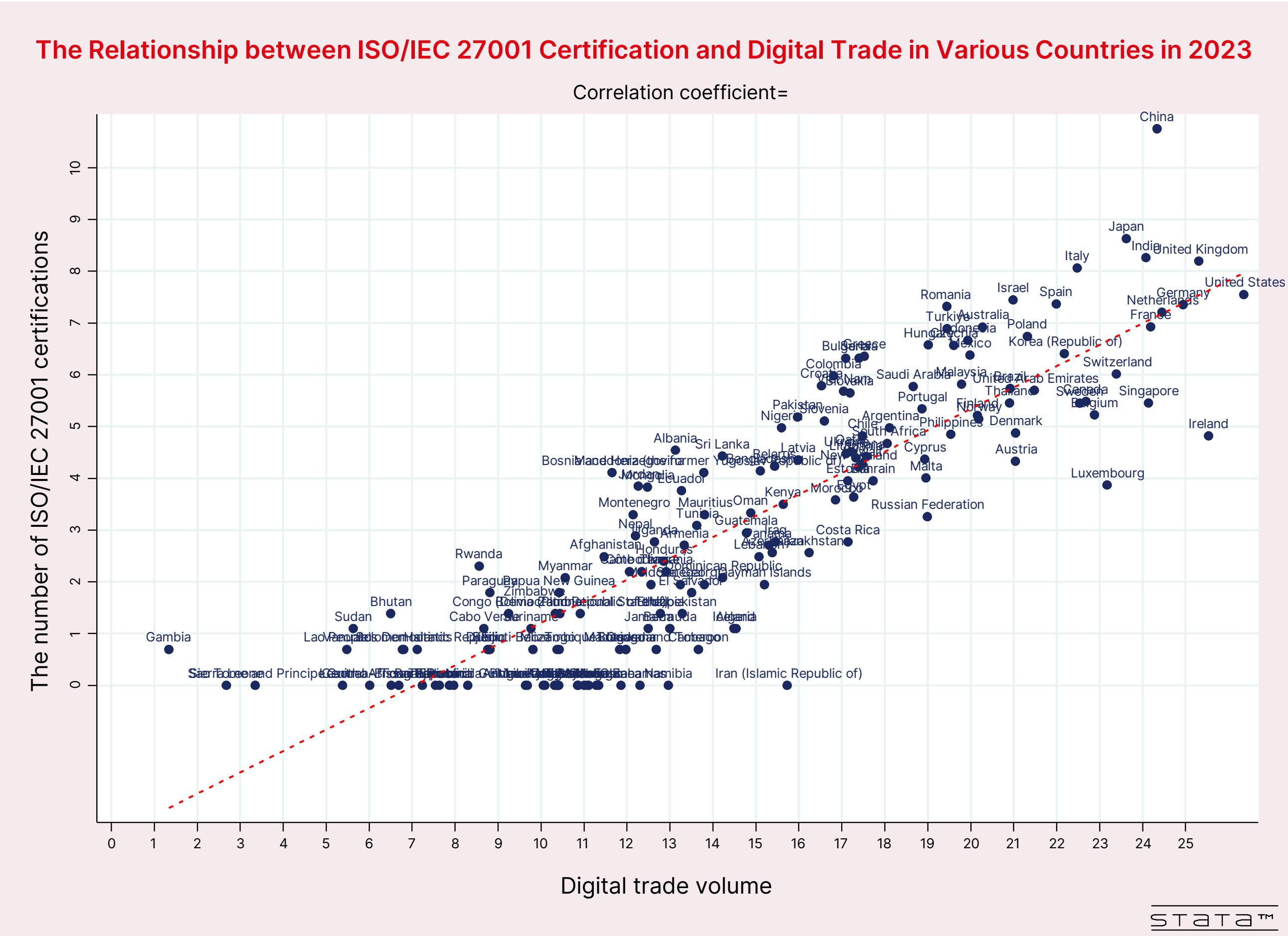
最も注目すべき変化は，中国が2020年の6位から5位に上昇したものの，2023年には7位，そして2024年には9位へと順位を落としたことです。一方，インドとシンガポールはそれぞれ5位と6位に浮上し，デジタル貿易分野の勢力図を大きく塗り替えました。フランスとオランダは，変動はあるものの着実に順位を上げ続けています。日本は9位からスタートし，その後4年連続で10位にとどまり，上位国との差は着実に拡大しています。第二層における各国のパフォーマンスのばらつきは，それぞれのデジタル貿易における発展モデルと段階の違いを反映しています。例えば，インドとシンガポールは現在，それぞれの強みを活かした優位性主導型の成長段階にあります。中国の衰退は必ずしも能力の絶対的な低下を意味するものではなく，むしろ進行中の変革を反映しています。

要約すると，上位国の持続的なリーダーシップ，あるいは中位国間のダイナミックな競争のいずれにおいても，両者が相まって世界的なデジタル貿易の継続的な拡大と発展を推進してきています。

General relationship between ISO/IEC 27001 certification and digital trade

Countries possessing more ISO/IEC 27001 certifications typically exhibit higher digital trade volumes. Figure 5 shows the general relationship between ISO/IEC 27001 certification and digital trade, with the horizontal axis representing the volume of digital trade, and the vertical axis representing the number of ISO/IEC 27001 certifications. It is observable that most countries' data points cluster closely to a trend line sloping upwards to the right. This indicates a positive correlation between the number of ISO/IEC 27001 certifications and a nation's total digital trade volume.

Figure 5: Global distribution of ISO/IEC 27001 certification and digital trade

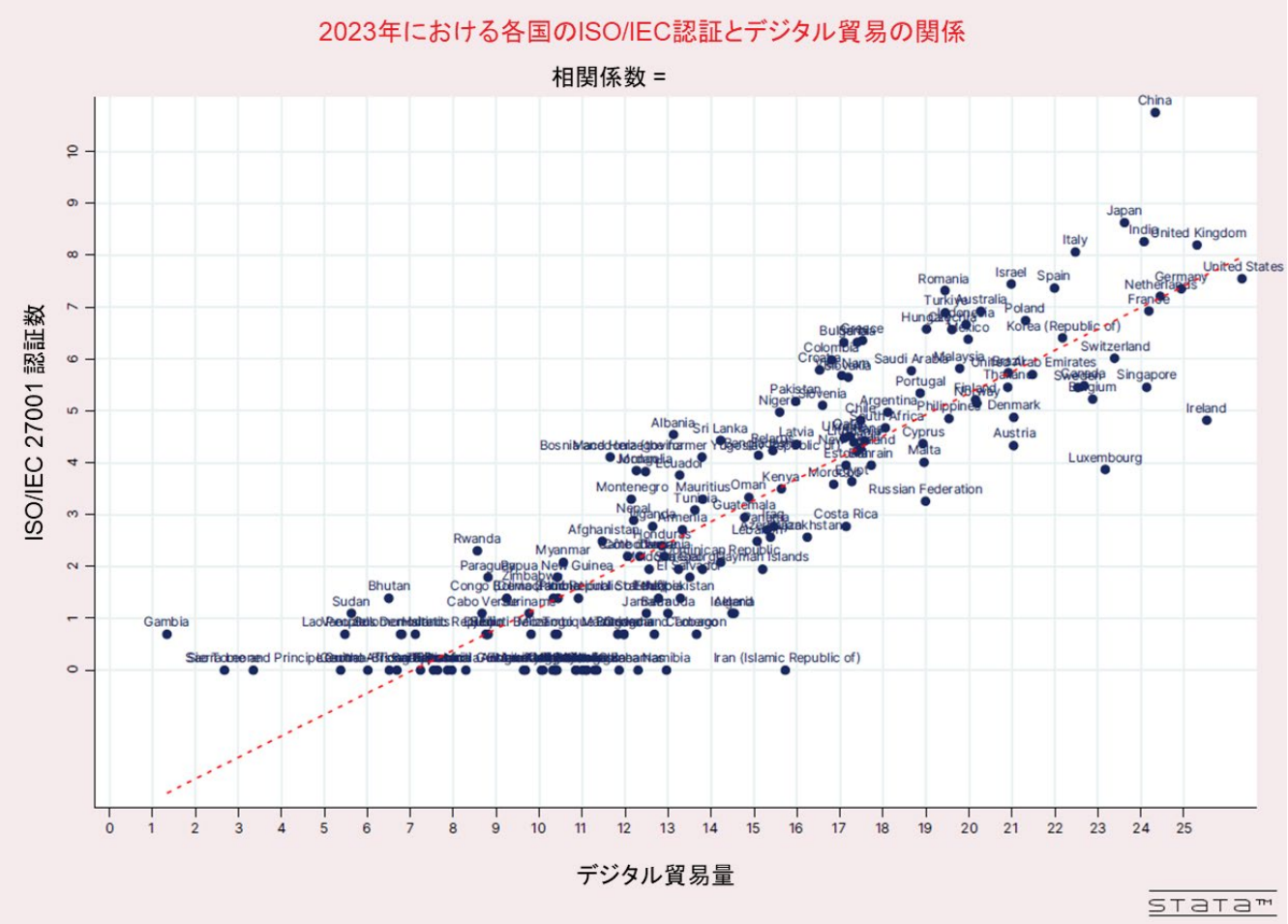


Source: Digital trade data comes from UNCTADstat. The number of ISO/IEC 27001 certifications comes from ISO Survey and National Certification and Accreditation Information Public Service Platform (China). The data has been logarithmically processed.

ISO/IEC 27001認証とデジタル貿易の一般的な関係

ISO/IEC 27001認証を多く取得している国は，一般的にデジタル貿易量が多い傾向にあります。図5は，ISO/IEC 27001認証とデジタル貿易の一般的な関係を示していて，横軸はデジタル貿易量，縦軸はISO/IEC 27001認証数を表しています。ほとんどの国のデータポイントが右肩上がりのトレンドラインに密集していることが観察できます。これは，ISO/IEC 27001認証数と国の総デジタル貿易量との間に正の相関関係があることを示しています。

図 5: ISO/IEC 27001認証とデジタル貿易の世界分布



出典：デジタル貿易データはUNCTADstatより、ISO/IEC 27001認証件数はISO調査および国家認証・認可情報公開サービスプラットフォーム（中国）より入手。データは対数変換済。

High-performing countries

Countries such as China, Japan, the UK and the US are positioned prominently in the upper-right quadrant of the graph. These countries have large digital trade volumes and a high number of ISO/IEC 27001 certifications. For example, the US has a well-developed digital economy with an array of e-commerce, software and digital service exports. In the past five years, it has not only maintained its position as the world's largest digital trading economy, but also achieved a total digital trade volume of USD 12.28 trillion (2024), maintaining an unbeatable leading advantage over other countries. At the same time, it is far ahead in terms of digital software, not only owning several best-selling applications, but also social and algorithm platforms, such as Google, mastering massive user data and global attention resources. Similarly, the China Digital Trade Development Report 2024 shows that from 2019 to 2023, China's imports and exports of digitally deliverable services achieved a surplus for five consecutive years.[9]

ISO/IEC 27001 certifications are crucial for building trust in digital trade. With the booming development of digital industries such as e-commerce and financial technology, the advantages of ISO/IEC 27001 certification have become increasingly evident. The high number of ISO/IEC 27001 certifications is often the result of a combination of national policy guidance, industry regulatory requirements and market driven factors. China has also shown a high level of participation in ISO/IEC 27001 certification, reaching 39 835 certificates by 2023. The United States also accounts for a significant proportion of the total scale of ISO/IEC 27001 certification worldwide, reaching 1 563 by 2023, ranking among the top in the world.

Middle-ranking countries

Countries like France, Germany, Italy and South Korea are located in the middle region of the graph. They have a moderate level of digital trade volume and a corresponding number of ISO/IEC 27001 certifications. These countries typically have well-established manufacturing and service sectors, which are increasingly integrating digital technologies. Their digital trade activities may focus on specific high-value-added products or services, such as automotive software, luxury goods e-commerce or advanced manufacturing solutions. The number of certifications indicates their recognition of the importance of information security in maintaining competitiveness in the digital trade market.

Low-performing countries

In the lower-left quadrant are countries with relatively small digital trade volumes and few ISO/IEC 27001 certifications. These countries may face multiple challenges. Some may have underdeveloped digital infrastructure, limiting their ability to participate in global digital trade. Additionally, a lack of awareness or resources for implementing an ISMS could contribute to the low number of certifications. For example, some least-developed countries may prioritize basic economic development needs over digital transformation and information security, resulting in their position in this quadrant.

9 https://12335.mofcom.gov.cn/article/zymysyq/202507/1942494_1.html

高パフォーマンス国

中国，日本，英国，米国などの国々は，グラフの右上象限に目立って位置しています。これらの国々は，デジタル貿易量が大きく，ISO/IEC 27001認証の取得数も多いです。例えば，米国は，電子商取引，ソフトウェア，デジタルサービスの輸出が盛んな，高度に発達したデジタル経済を有しています。過去5年間，米国は世界最大のデジタル貿易経済としての地位を維持しただけでなく，デジタル貿易総額は12兆2800億米ドル（2024年）に達し，他国に対して圧倒的な優位性を維持しています。同時に，デジタルソフトウェアの分野でも大きくリードしており，ベストセラーアプリを多数保有しているだけでなく，Googleなどのソーシャルプラットフォームやアルゴリズムプラットフォームを擁し，膨大なユーザーデータとグローバルな注目度というリソースを掌握しています。同様に，中国デジタル貿易発展報告書2024によると，2019年から2023年にかけて，中国のデジタルサービス輸出入は5年連続で黒字を達成しました。[9]

ISO/IEC 27001認証は，デジタル貿易における信頼構築に不可欠です。電子商取引やフィンテック（ファイナンス・テクノロジー）といったデジタル産業の急速な発展に伴い，ISO/IEC 27001認証のメリットはますます明らかになっています。ISO/IEC 27001認証の取得件数の多さは，多くの場合，国家政策の指針，業界規制要件，そして市場主導の要因が複合的に作用した結果です。中国もISO/IEC 27001認証に積極的に参加しており，2023年までに39,835件の認証を取得しています。米国も世界のISO/IEC 27001認証取得件数において大きな割合を占めており，2023年までに1,563件に達し，世界トップクラスとなっています。

中位ランク国

フランス，ドイツ，イタリア，韓国などの国々は，グラフの中央部に位置しています。これらの国々は，デジタル貿易量が中程度であり，ISO/IEC 27001認証の取得数もそれに応じています。これらの国々は，一般的に確立された製造業とサービス業を有しており，デジタル技術の統合が進んでいます。デジタル貿易活動は，自動車ソフトウェア，高級品電子商取引，高度な製造ソリューションなど，特定の高付加価値製品やサービスに焦点を当てている可能性があります。認証の取得数は，デジタル貿易市場における競争力維持のために情報セキュリティの重要性を認識していることを示しています。

低パフォーマンス国

左下象限には，デジタル貿易量が比較的少なく，ISO/IEC 27001認証の取得数も少ない国々が位置しています。これらの国々は，複数の課題に直面している可能性があります。デジタルインフラが未発達な国もあり，グローバルなデジタル貿易への参加能力が制限されている可能性があります。さらに，ISMS（情報セキュリティマネジメントシステム）の導入に関する認識不足やリソース不足も，認証取得件数の少なさにつながっていると考えられます。例えば，一部の後発開発途上国は，デジタル変革や情報セキュリティよりも基本的な経済発展を優先しているため，この象限に位置している可能性があります。

9 https://12335.mofcom.gov.cn/article/zymysyq/202507/1942494_1.html

Outliers

There are also some outliers in the graph. For instance, some countries may have a relatively high number of certifications but a smaller digital trade scale. This could be due to various reasons, such as a focus on domestic information-intensive industries that require high-level information security compliance but have limited international digital trade exposure. On the other hand, countries with a large digital trade scale but relatively few certifications may be operating in a more laissez-faire information security environment. They may also have alternative information security management approaches not reflected in the ISO/IEC 27001 certification system.

In conclusion, the relationship between ISO/IEC 27001 certification and digital trade scale varies significantly among different countries, influenced by factors such as digital infrastructure, economic development level and information security policies. Further exploration of these patterns can help international organizations and national governments formulate targeted policies to promote the healthy development of digital trade while ensuring information security.

The impact of ISO/IEC 27001 certification on digital trade: a regression analysis

This section conducts regression analysis of national panel data to examine the impact of ISO/IEC 27001 on the digital trade of a country, including total trade volume, trade export volume and trade import volume. Regression methods are also used to identify the differences in the effects of ISO/IEC 27001 among different types of countries, such as developed and developing countries, RCEP[10] members and non-RCEP members.

Regression analysis model and variables

Regression analysis model

To empirically test the impact of ISO/IEC 27001 certification on digital trade, this report constructed a fixed effects panel model. The specific form is as follows:

$$Digital\ trade_{it} = \beta_0 + \beta_1 ISO/IEC27001_{it} + \beta_2 X_{it} + \mu \quad (1)$$

$Digital\ trade_{it}$ represents the digital trade level of country i in year t. In empirical analysis, it measures the logarithmic values of digital trade totals, digital exports and digital imports to explore the impact of $ISO/IEC27001_{it}$ on digital trade from three aspects. $ISO/IEC27001_{it}$ is the core explanatory variable, representing the number of ISO/IEC 27001 certifications of country i in year t, measured as the logarithm of the number of ISO/IEC 27001 certifications in each country over the years. X_{it} represents a series of control variables that may affect digital trade, such as level of economic development, political relations, international direct investment and digital infrastructure.

Variables

Table 4 summarizes the dependent, independent and control variables used for this study, including their relevant data sources and use.

10 RCEP is the world's largest free trade agreement, and it not only covers traditional goods trade, but also incorporates digital trade rules. RCEP has a profound impact on member countries' digital trade. Therefore, it is meaningful to explore the difference in effects of ISO/IEC 27001 on digital trade between RCEP members and non-RCEP members. RCEP comprises 15 member states: the eleven ASEAN countries (Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, the Philippines, Singapore, Thailand, Vietnam, and Timor-Leste), alongside

外れ値

グラフには外れ値もいくつか見られます。例えば，認証取得件数は比較的多いものの，デジタル貿易規模が小さい国があります。これは，高度な情報セキュリティコンプライアンスを必要とする国内の情報集約型産業に重点を置いている一方で，国際的なデジタル貿易への露出が限られているなど，様々な理由が考えられます。一方，デジタル貿易規模は大きいものの，認証取得件数が比較的少ない国は，より自由放任主義的な情報セキュリティ環境で運営されている可能性があります。また，ISO/IEC 27001認証システムに反映されていない，独自の情報セキュリティ管理手法を採用している可能性もあります。

結論として，ISO/IEC 27001認証とデジタル貿易規模の関係は，デジタルインフラ，経済発展レベル，情報セキュリティ政策などの要因によって国ごとに大きく異なります。これらのパターンをさらに詳しく分析することで，国際機関や各国政府は，情報セキュリティを確保しつつデジタル貿易の健全な発展を促進するための的を絞った政策を策定するのに役立ちます。

ISO/IEC 27001認証がデジタル貿易に与える影響：回帰分析

本節では，各国のパネルデータを用いた回帰分析を行い，ISO/IEC 27001が総貿易量，輸出入量を含む各国のデジタル貿易に与える影響を検証します。また，回帰分析を用いて，先進国と発展途上国，RCEP[10]加盟国と非加盟国など，異なるタイプの国におけるISO/IEC 27001の影響の違いを明らかにします。

回帰分析モデルと変数

回帰分析モデル

ISO/IEC 27001認証がデジタル貿易に与える影響を実証的に検証するため，本報告書では固定効果パネルモデルを構築しました。具体的な形式は以下のとおりです。

$$Digital\ trade_{it} = \beta_0 + \beta_1 ISO/IEC27001_{it} + \beta_2 X_{it} + \mu \quad (1)$$

$Digital\ trade_{it}$ は，t 年における国 i のデジタル貿易水準を表します。実証分析では，デジタル貿易総額，デジタル輸出，デジタル輸入の対数値を測定し，$ISO/IEC27001_{it}$ がデジタル貿易に与える影響を3つの側面から分析します。$ISO/IEC27001_{it}$ は主要な説明変数であり，国 i における t 年のISO/IEC 27001認証取得件数を表します。これは，各国のISO/IEC 27001認証取得件数の対数として算出されます。X_{it} は，経済発展レベル，政治関係，国際直接投資，デジタルインフラなど，デジタル貿易に影響を与える可能性のある一連の制御変数を表します。

変数

表4は，本研究で使用した従属変数，独立変数，制御変数を，関連するデータソースと使用方法とともにまとめたものです。

10 RCEPは世界最大の自由貿易協定であり，従来の物品貿易だけでなく，デジタル貿易に関するルールも包含しています。RCEPは加盟国のデジタル貿易に大きな影響を与えています。したがって，RCEP加盟国と非加盟国におけるISO/IEC 27001がデジタル貿易に与える影響の違いを探ることは有意義です。RCEPは15の加盟国から構成されています。11のASEAN諸国（ブルネイ，カンボジア，インドネシア，ラオス，マレーシア，ミャンマー，フィリピン，シンガポール，タイ，ベトナム，東ティモール）と並んで。

Table 4: Variable definitions and data sources

Variable name		Measurement method	Source of data	Purpose
Dependent variable	Digital trade	Perform logarithmic processing on the data on the digital delivery services trade for each country in each year.	UNCTADstat	Estimate the overall scale and import/ export scale of digital delivery services trade.
Independent variable	ISO/IEC 27001 certification	The number of ISO/IEC 27001 certifications for each country in each year.	ISO survey/ State Administration for Market Regulation[11]	Core independent variable.
Control variable[12]	Political relations	The political stability and non-violence level in the World Governance Index for each country.	World Bank	Political risks may have a negative impact on digital trade.
	International direct investment	The ratio of net inflow of international direct investment to GDP in each country.	International Monetary Fund (IMF) database/ World Bank	The higher the level of international direct investment, the greater the supportive effect on digital trade.
	Digital infrastructure	The proportion of residents within the coverage area of broadband signals in each country.	ITU	Higher levels of digitization contribute to increased digital trade flows.
Conditional variable	Developed countries	The 0-1 variable is assigned a value of 1 for developed countries and 0 for developing countries.	IMF	Compare the differences in the effect of ISO/IEC 27001 between developed countries and developing countries.
	RCEP members	The 0-1 variable is assigned a value of 1 to RCEP members, and 0 to non-RCEP members.	RCEP	Compare the differences in the effect of ISO/IEC 27001 between RCEP members and non-RCEP members.

11 Based on previous work by Boubakri et al. (2019), Guo et al. (2024) – see reference list.
12 After cross-checking the total number of China in the ISO Survey, due to the significant difference in data for 2023, the number of ISO/IEC 27001 certifications in China in 2023, as calculated by the State Administration for Market Regulation, was chosen as a replacement.

表 4: 変数定義とデータソース

変数名		測定方法	データソース	目的
従属変数	デジタル貿易	各国のデジタル配信サービス貿易に関するデータを対数変換する。	UNCTADstat	デジタル配信サービス貿易の全体規模および輸出入規模を推定する。
独立変数	ISO/IEC 27001認証	各国のISO/IEC 27001認証取得件数（各年）	ISO調査／国家市場監督管理総局[11]	主要独立変数
制御変数[12]	政治関係	各国の世界ガバナンス指数における政治的安定性および非暴力レベル	世界銀行	政治リスクはデジタル貿易に負の影響を与える可能性がある。
	国際直接投資	各国のGDPに対する国際直接投資の純流入額の比率	国際通貨基金（IMF）データベース／世界銀行	国際直接投資の水準が高いほど，デジタル貿易への支援効果は大きくなる。
	デジタルインフラ	各国におけるブロードバンド信号のカバーエリア内の居住者の割合	ITU	デジタル化の水準が高いほど，デジタル貿易フローの増加に貢献する。
条件変数	先進国	0-1変数は，先進国には1，発展途上国には0の値が割り当てられる。	IMF	先進国と発展途上国におけるISO/IEC 27001の効果の違いを比較する。
	RCEP加盟国	0-1変数は，RCEP加盟国には1，非RCEP加盟国には0の値が割り当てられる。	RCEP	RCEP加盟国と非RCEP加盟国におけるISO/IEC 27001の効果の違いを比較する。

11 Boubakri et al. (2019) , Guo et al. (2024)による先行研究に基づきます。– 参考文献リストを参照

12 ISO調査における中国の総数を相互参照した結果，2023年のデータに大きな差異が見られたため，国家市場監督管理総局が算出した2023年の中国におけるISO/IEC 27001認証取得件数を代替値として採用しました。

Descriptive statistics

Following data acquisition, manual processing was undertaken to exclude cases lacking complete data for one or more variables between 2016 and 2023, or where data was unavailable for more than 50% of years. For variables where non-response did not exceed 10%, missing values were processed via the imputation method using the statistical software, Stata. The final dataset comprises panel data for 165 countries or regions spanning 2016-2023, yielding 1 320 observations.

Descriptive statistics for each variable are presented in Table 5. The mean and standard deviation of the total digital trade volume are 14.1 and 5.148, respectively, indicating that there are significant differences between countries. The maximum value of ISO/IEC 27001 certification reaches 10.593, while the minimum value is 0, reflecting that the current global ISO/IEC 27001 certification is not evenly distributed, but concentrated in a few technologically advanced countries, such as China, Germany, Japan and the US.

Table 5: Descriptive statistics

Variable name	Sample size	Mean	Standard deviation	Minimum values	Median	Maximum values
Digital trade	1 320	14.137	5.148	1.099	13.600	26.354
Digital trade export	1 320	6.763	2.888	-1.609	6.659	13.431
Digital trade import	1 320	7.374	2.369	1.099	7.121	12.923
ISO/IEC 27001 certification	1 320	2.748	2.446	0.000	2.303	10.593
International direct investment	1 320	6.127	4.458	-12.792	7.033	13.038
Digital infrastructure	1 320	87.325	19.831	5.200	97.000	100.000
Political relations	1 320	-0.089	0.901	-2.795	-0.054	1.661

記述統計

データ収集後，2016年から2023年の間に1つ以上の変数でデータが不完全なケース，または50%以上の年でデータが入手できないケースを除外するために，手作業による処理を行いまった。無回答率が10%を超えない変数については，統計ソフトウェアStataを用いて欠損値を補完しました。最終的なデータセットは，2016年から2023年までの165の国または地域に関するパネルデータで構成され，1,320件の観測値が含まれます。

各変数の記述統計は表5に示されています。デジタル貿易総額の平均値と標準偏差はそれぞれ14.1と5.148であり，国によって有意な差があることがわかります。ISO/IEC 27001認証の最大値は10.593，最小値は0であり，現在のグローバルなISO/IEC 27001認証は均等には分布しておらず，中国，ドイツ，日本，米国などの少数の技術的に先進的な国に集中していることを示しています。

表 5: 記述統計

変数名	サンプルサイズ	平均値	標準偏差	最小値	中央値	最大値
デジタル貿易	1 320	14.137	5.148	1.099	13.600	26.354
デジタル貿易輸出	1 320	6.763	2.888	-1.609	6.659	13.431
デジタル貿易輸入	1 320	7.374	2.369	1.099	7.121	12.923
ISO/IEC 27001認証	1 320	2.748	2.446	0.000	2.303	10.593
国際直接投資	1 320	6.127	4.458	-12.792	7.033	13.038
デジタルインフラ	1 320	87.325	19.831	5.200	97.000	100.000
政治関係	1 320	-0.089	0.901	-2.795	-0.054	1.661

Overall analysis of the impact of ISO/IEC 27001 certification on digital trade

Table 6 presents the benchmark regression results, with models 1, 2 and 3 representing the benchmark regressions for total digital trade, digital trade exports and digital trade imports respectively. This reveals that ISO/IEC 27001 standard certification exerts a significant positive influence on digital trade, digital trade exports and digital trade imports alike, reflecting the role of standard certification in reducing transaction costs, though the degree of impact varies.

Empirical regression results indicate that ISO/IEC 27001 certification exerts a significant positive effect on the total volume of digital trade, as well as on both exports and imports. Examining the robustness of these effects reveals that the certification's influence on total digital trade volume is the most stable, with a regression coefficient of 0.220. This signifies that a 1% increase in the number of ISO/IEC 27001 certifications correlates with a 0.22 percentage point rise in total digital trade volume. This indicates that ISO/IEC 27001, as the most influential and credible international information security standard certification, effectively reduces information asymmetry and compliance costs, thereby providing crucial institutional safeguards for global digital trade.

The promoting effect on digital trade exports is secondary, with a regression coefficient of 0.123. This indicates that a 1% increase in certification volume corresponds to a 0.123 percentage point rise in digital trade export value. Although this figure is lower than its impact on total trade volume, it still demonstrates the certification's significant value in international markets. It assists digital service providers in overcoming trade barriers, enhancing overseas buyers' trust and acceptance, thereby functioning as an international "passport". In contrast, its impact on imports is comparatively limited, with a regression coefficient of 0.097 significantly lower than that for total trade and exports. This indicates that a 1% increase in ISO/IEC 27001 certifications yields only a 0.097 percentage point rise in digital trade imports. This disparity likely stems from import decisions being more heavily influenced by domestic market demand, technological capabilities and other intrinsic factors, where the certification's influence is relatively weaker.

Table 6: Baseline regression results

Variables	(1)		(2)		(3)	
	Digital trade		Digital trade export		Digital trade import	
ISO/IEC 27001 certification	0.239*** (5.87)	0.220*** (5.28)	0.131*** (5.05)	0.123*** (4.74)	0.108*** (4.83)	0.097*** (4.24)
International direct investment		0.007 (1.23)		0.003 (0.87)		0.003 (1.49)
Digital infrastructure		0.006*** (2.70)		0.002* (1.69)		0.003*** (2.66)
Political relations		0.322** (2.00)		0.207 (1.65)		0.115* (1.76)
Constant	13.479*** (120.34)	13.006*** (65.60)	6.403*** (89.72)	6.215*** (44.95)	7.076*** (114.99)	6.791*** (58.45)
Observations	1,320	1,320	1,320	1,320	1,320	1,320
Number of countries	165	165	165	165	165	165
R-squared	0.059	0.080	0.038	0.050	0.051	0.076

Robust *t*-statistics in parentheses *** p<0.01, ** p<0.05, * p<0.1

ISO/IEC 27001認証がデジタル貿易に与える影響の総合分析

表6はベンチマーク回帰分析の結果を示しており，モデル1，2，3はそれぞれデジタル貿易総額，デジタル貿易輸出，デジタル貿易輸入に関するベンチマーク回帰分析を表しています。この分析結果から，ISO/IEC 27001規格認証はデジタル貿易，デジタル貿易輸出，デジタル貿易輸入のいずれにも有意な正の影響を与えていることが明らかになりました。これは，規格認証が取引コストの削減に貢献していることを反映していますが，その影響の度合いはそれぞれ異なります。

実証的な回帰分析の結果，ISO/IEC 27001認証はデジタル貿易総額，輸出入のいずれにも有意な正の影響を与えていることが示されました。これらの影響の頑健性を検証すると，デジタル貿易総額に対する認証の影響が最も安定しており，回帰係数は0.220となっています。これは，ISO/IEC 27001認証件数が1%増加すると，デジタル貿易総額が0.22パーセントポイント上昇することを示しています。つまり，最も影響力があり信頼性の高い国際情報セキュリティ規格認証であるISO/IEC 27001は，情報非対称性とコンプライアンスコストを効果的に削減し，グローバルなデジタル貿易にとって重要な制度的保護を提供していると言えます。

デジタル貿易輸出への促進効果は二次的で，回帰係数は0.123です。これは，認証件数が1%増加すると，デジタル貿易輸出額が0.123パーセントポイント上昇することを示しています。この数値は貿易総額への影響よりも小さいものの，国際市場における認証の重要な価値を依然として示しています。認証は，デジタルサービスプロバイダーが貿易障壁を克服し，海外バイヤーの信頼と受容を高めるのに役立ち，国際的な「パスポート」としての役割を果たします。一方，輸入への影響は比較的限定的で，回帰係数は0.097と，総貿易額や輸出額の回帰係数よりも大幅に低い値となっています。これは，ISO/IEC 27001認証取得率が1%上昇しても，デジタル貿易輸入額の増加はわずか0.097パーセントポイントに過ぎないことを示しています。この差は，輸入決定が国内市場の需要，技術力，その他の内在的要因に大きく左右され，認証の影響力が相対的に弱いことに起因していると考えられます。

表 6: ベースライン回帰分析結果

変数	(1)		(2)		(3)	
	デジタル貿易		デジタル貿易輸出		デジタル貿易輸入	
ISO/IEC 27001認証	0.239*** (5.87)	0.220*** (5.28)	0.131*** (5.05)	0.123*** (4.74)	0.108*** (4.83)	0.097*** (4.24)
国際直接投資		0.007 (1.23)		0.003 (0.87)		0.003 (1.49)
デジタルインフラ		0.006*** (2.70)		0.002* (1.69)		0.003*** (2.66)
政治関係		0.322** (2.00)		0.207 (1.65)		0.115 * (1.76)
定数	13.479*** (120.34)	13.006*** (65.60)	6.403*** (89.72)	6.215*** (44.95)	7.076*** (114.99)	6.791*** (58.45)
観測数	1,320	1,320	1,320	1,320	1,320	1,320
対象国数	165	165	165	165	165	165
決定係数（R二乗）	0.059	0.080	0.038	0.050	0.051	0.076

括弧内はロバストt 統計量 *** p<0.01, ** p<0.05, * p<0.1

Comparative analysis of the impact of ISO/IEC 27001 certification among countries

Developed and developing countries

The IMF has divided 165 sample countries into developing and developed countries based on criteria including productivity, industrial structure, economic operating mechanisms, technological modernization and capital internationalization. The IMF's report conducted regression analysis of these two sets of samples separately to compare the impact of ISO/IEC 27001 between developing and developed countries. Its results are shown in Table 7.

Table 7: Sub-group analysis results by economic level

Variables	Developed			Developing		
	Digital trade	Digital export	Digital import	Digital trade	Digital export	Digital import
ISO/IEC 27001 certification	0.027 (0.56)	0.007 (0.26)	0.021 (0.83)	0.088* (1.77)	0.037 (1.12)	0.051* (1.73)
International direct investment	0.004 (1.30)	0.001 (0.45)	0.003* (1.84)	0.015 (1.40)	0.009 (1.05)	0.006 (1.43)
Digital infrastructure	-0.005 (-0.49)	-0.005 (-0.94)	-0.000 (-0.03)	-0.003 (-1.32)	-0.004** (-2.18)	0.00 (0.33)
Political relations	-0.038 (-0.17)	-0.017 (-0.16)	-0.021 (-0.17)	0.373** (2.23)	0.220 (1.58)	0.153** (2.41)
Constant	19.855*** (16.41)	10.264*** (17.05)	9.591*** (15.26)	12.208*** (59.79)	5.838*** (39.95)	6.371*** (54.76)
Observations	288	288	288	1,032	1,032	1,032
Number of countries	36	36	36	129	129	129
R-squared	0.737	0.711	0.714	0.179	0.144	0.124

Robust t-statistics in parentheses *** p<0.01, ** p<0.05, * p<0.1

各国におけるISO/IEC 27001認証の影響に関する比較分析

先進国と発展途上国

IMFは，生産性，産業構造，経済運営メカニズム，技術近代化，資本の国際化などの基準に基づき，165のサンプル国を発展途上国と先進国に分類しました。IMFの報告書は，これら2つのサンプルセットをそれぞれ回帰分析し，発展途上国と先進国におけるISO/IEC 27001の影響を比較しました。その結果は表7に示されています。

表 7: 経済レベル別サブグループ分析結果

変数	先進国			発展途上国		
	デジタル貿易	デジタル輸出	デジタル輸入	デジタル貿易	デジタル輸出	デジタル輸入
ISO/IEC 27001認証	0.027 (0.56)	0.007 (0.26)	0.021 (0.83)	0.088* (1.77)	0.037 (1.12)	0.051* (1.73)
国際直接投資	0.004 (1.30)	0.001 (0.45)	0.003* (1.84)	0.015 (1.40)	0.009 (1.05)	0.006 (1.43)
デジタルインフラ	-0.005 (-0.49)	-0.005 (-0.94)	-0.000 (-0.03)	-0.003 (-1.32)	-0.004** (-2.18)	0.00 (0.33)
政治関係	-0.038 (-0.17)	-0.017 (-0.16)	-0.021 (-0.17)	0.373** (2.23)	0.220 (1.58)	0.153** (2.41)
定数	19.855*** (16.41)	10.264*** (17.05)	9.591*** (15.26)	12.208*** (59.79)	5.838*** (39.95)	6.371*** (54.76)
観測数	288	288	288	1,032	1,032	1,032
対象国数	36	36	36	129	129	129
決定係数（R二乗）	0.737	0.711	0.714	0.179	0.144	0.124

括弧内はロバストt 統計量 *** p<0.01, ** p<0.05, * p<0.1

In developing countries, ISO/IEC 27001 certification continues to exert a significant positive influence on total digital trade and imports, with its impact on total digital trade being more pronounced than on imports. This finding further validates the catalytic role of ISO/IEC 27001 certification in digital trade. By obtaining certification, enterprises in developing countries also enhance their attractiveness for introducing internationally advanced digital services and technologies, thereby significantly boosting imports. Regarding digital trade exports in developing countries, the coefficient remains positive but has become non-significant. This does not imply the disappearance of ISO/IEC 27001 certification's promoting effect, but rather reflects that the drivers of digital trade in developing countries involve the combined influence of multiple dimensions. On the one hand, ISO/IEC 27001 may not directly impact the export process. On the other hand, relatively weak digital infrastructure and other factors may still constrain developing countries, meaning the certification's enabling effect has not been efficiently converted and manifested in digital trade exports.

The impact of ISO/IEC 27001 certification on developed countries' digital trade levels, whether in terms of total volume or imports and exports, is not significant in any dimension. Having commenced their digital development earlier, most enterprises and key sectors in developed countries typically focus on competing within the higher-value segments of global digital value chains. Consequently, ISO/IEC 27001 certification, as one such threshold requirement, is already widely met, rendering its additional promoting effect on digital trade limited.

RCEP members and non-RCEP members

According to the RCEP, the 165 sample countries in this report are divided into two groups, namely RCEP members (15 countries) with the rest being non-RCEP members. This report conducted regression analysis on these two sets of samples separately to compare the impact of ISO/IEC 27001 on RCEP members and non-RCEP members. Results are shown in Table 8.

Table 8: Sub-group analysis results by RCEP membership status

Variables	Developed			Developing		
	Digital trade	Digital export	Digital import	Digital trade	Digital export	Digital import
ISO/IEC 27001 certification	-0.012 (-0.06)	-0.006 (-0.04)	-0.006 (-0.07)	0.090** (2.33)	0.041* (1.75)	0.049** (2.01)
International direct investment	-0.017 (-0.62)	-0.027 (-0.94)	0.010** (2.27)	0.008** (2.19)	0.005* (1.90)	0.003* (1.75)
Digital infrastructure	-0.001 (-0.23)	-0.001 (-0.17)	-0.001 (-0.34)	-0.005** (-2.13)	-0.004** (-2.59)	-0.001 (-0.59)
Political relations	1.091* (1.79)	0.986* (1.86)	0.105 (0.97)	0.200 (1.51)	0.095 (1.09)	0.104 (1.54)
Constant	16.959*** (20.63)	8.323*** (14.81)	8.636*** (25.80)	13.556*** (67.74)	6.583*** (46.28)	6.973*** (58.91)
Observations	120	120	120	1,200	1,200	1,200
Number of countries	15	15	15	150	150	150
R-squared	0.455	0.345	0.597	0.232	0.187	0.158

Robust t-statistics in parentheses *** p<0.01, ** p<0.05, * p<0.1

発展途上国では，ISO/IEC 27001認証はデジタル貿易総額と輸入総額に引き続き有意な正の影響を与えており，デジタル貿易総額への影響は輸入への影響よりも顕著です。この調査結果は，デジタル貿易におけるISO/IEC 27001認証の触媒的役割をさらに裏付けるものです。認証を取得することで，発展途上国の企業は国際的に先進的なデジタルサービスや技術を導入する際の魅力を高め，輸入を大幅に増加させることができます。発展途上国のデジタル貿易輸出に関しては，係数は依然として正の値を示していますが，統計的に有意ではなくなりました。これはISO/IEC 27001認証の促進効果が消滅したことを意味するのではなく，発展途上国におけるデジタル貿易の推進要因が複数の要素の複合的な影響によるものであることを反映しています。一方では，ISO/IEC 27001は輸出プロセスに直接的な影響を与えない可能性があります。他方では，比較的脆弱なデジタルインフラなどの要因が依然として発展途上国を制約している可能性があり，認証の促進効果がデジタル貿易輸出に効率的に結びついていないことを意味します。

ISO/IEC 27001認証が先進国のデジタル貿易レベルに与える影響は，総量，輸出入額のいずれの面においても，有意なものではありません。先進国ではデジタル開発を早期に開始しているため，多くの企業や主要産業は，グローバルなデジタルバリューチェーンにおける高付加価値セグメントでの競争に注力しています。したがって，ISO/IEC 27001認証は，こうした要件の一つとして既に広く満たされており，デジタル貿易への追加的な促進効果は限定的です。

RCEP加盟国と非加盟国

RCEPの規定に基づき，本報告書のサンプル国165カ国は，RCEP加盟国（15カ国）と非加盟国の2つのグループに分けられます。本報告書では，これら2つのサンプルグループに対してそれぞれ回帰分析を行い，ISO/IEC 27001がRCEP加盟国と非加盟国に与える影響を比較しました。結果は表8に示されています。

表 8: RCEP加盟状況別サブグループ分析結果

変数	先進国			発展途上国		
	デジタル貿易	デジタル輸出	デジタル輸入	デジタル貿易	デジタル輸出	デジタル輸入
ISO/IEC 27001認証	-0.012 (-0.06)	-0.006 (-0.04)	-0.006 (-0.07)	0.090** (2.33)	0.041* (1.75)	0.049** (2.01)
国際直接投資	-0.017 (-0.62)	-0.027 (-0.94)	0.010** (2.27)	0.008** (2.19)	0.005* (1.90)	0.003* (1.75)
デジタルインフラ	-0.001 (-0.23)	-0.001 (-0.17)	-0.001 (-0.34)	-0.005** (-2.13)	-0.004** (-2.59)	-0.001 (-0.59)
政治関係	1.091* (1.79)	0.986* (1.86)	0.105 (0.97)	0.200 (1.51)	0.095 (1.09)	0.104 (1.54)
定数	16.959*** (20.63)	8.323*** (14.81)	8.636*** (25.80)	13.556*** (67.74)	6.583*** (46.28)	6.973*** (58.91)
観測数	120	120	120	1,200	1,200	1,200
対象国数	15	15	15	150	150	150
決定係数（R二乗）	0.455	0.345	0.597	0.232	0.187	0.158

括弧内はロバストt 統計量 *** p<0.01, ** p<0.05, * p<0.1

For non-member countries, a 1% increase in ISO/IEC 27001 certification yields a 0.090% rise in total digital trade volume. The boost to imports (0.049%) slightly exceeds that for exports (0.041%), underscoring how ISO/IEC 27001 certification functions as a "passport" for accessing multinational markets within digital trade. Without the institutional conveniences afforded by the RCEP, obtaining international certification provides non-member states with a compliant and reliable form of proof. This enhances their ease of access, serving as a steppingstone for entering RCEP markets.

For RCEP member states, the impact of ISO/IEC 27001 certification has become insignificant, with a negative coefficient. This may stem from two factors: on the one hand, as member states are predominantly major trading countries, or countries with high trade dependency, large enterprises may have already obtained ISO/IEC 27001 certification. On the other hand, the RCEP agreement incorporates several official measures to safeguard data security, reducing member states' reliance on third-party certification in digital trade. For instance, Chapter XII outlines provisions for e-commerce, establishing relevant measures and policies for cross-border information transmission. Consequently, the level of certification among member states does not affect their access to trade facilitation measures, diminishing the marginal utility of certification. This demonstrates diminishing marginal returns for acquiring additional certifications.

Conclusions and recommendations

Conclusions

The analysis of ISO/IEC 27001 certification at the national level, conducted on data ranging from 2016 to 2023, offers multiple insights into the influence of the standard on digital trade. Notably, the findings indicate:

Firstly, ISO/IEC 27001 exerts a significant promoting effect on digital trade. Specifically, ISO/IEC 27001 certification exerts the greatest promoting effect on a country's total digital trade volume, followed by exports, with the least pronounced effect observed on imports. This indicates that ISO/IEC 27001 certification, as the most influential and credible international information security standard certification, can establish a trust foundation in cross-border digital trade, reduce information asymmetry and compliance costs, and significantly increase total trade flows. Moreover, exporters transmit efficient quality signals of their security governance capabilities to the international market through certification, helping them stand out in fierce international competition. Although certification can also enhance the confidence of domestic buyers, domestic market demand, cost-effectiveness, and product characteristics typically drive import decisions, rather than depending on whether foreign suppliers hold a specific management certification. Therefore, the impact of ISO/IEC 27001 certification on digital trade imports is relatively small.

Secondly, the promoting impact of ISO/IEC 27001 certification on digital trade exhibits distinct heterogeneous characteristics. Firstly, there are significant differences in the promoting effect of ISO/IEC 27001 certification between developed and developing countries. Although it has had a strong positive impact on the total trade volume and exports of developing countries, its influence on imports remains insignificant due to the complexity of digital trade drivers

非加盟国では，ISO/IEC 27001認証が1%増加すると，デジタル貿易総額が0.090%増加します。輸入の増加率（0.049%）は輸出の増加率（0.041%）をわずかに上回っており，ISO/IEC 27001認証がデジタル貿易における多国籍市場へのアクセスを可能にする「パスポート」として機能していることを裏付けています。RCEPが提供する制度的な便宜がない非加盟国にとって，国際認証の取得は，法令遵守と信頼性を証明する有効な手段となります。これが足がかりとなり，RCEP市場への参入が容易になります。

一方，RCEP加盟国にとって，ISO/IEC 27001認証の影響はマイナス係数となり，ほとんど意味をなさなくなっています。これは，2つの要因が考えられます。一つは，加盟国は主に主要貿易国，あるいは貿易依存度の高い国であるため，大企業は既にISO/IEC 27001認証を取得している可能性があることです。もう一つは，RCEP協定にはデータセキュリティを保護するための公式措置が複数盛り込まれており，加盟国がデジタル貿易において第三者認証に依存する度合いが低下していることです。例えば，第XII章では電子商取引に関する規定が示され，国境を越えた情報伝達に関する関連措置と政策が定められています。その結果，加盟国間の認証レベルは貿易円滑化措置へのアクセスに影響を与えず，認証取得の限界効用は低下します。これは，追加認証取得による限界収益逓減を示しています。

結論と提言

結論

2016年から2023年までのデータに基づき，各国レベルでISO/IEC 27001認証に関する分析を行った結果，この規格がデジタル貿易に与える影響について，複数の知見が得られました。特に，以下の点が明らかになりました。

第一に，ISO/IEC 27001はデジタル貿易に対して顕著な促進効果を発揮します。具体的には，ISO/IEC 27001認証は，国のデジタル貿易総量に対して最も大きな促進効果を発揮し，次いで輸出，輸入に対しては最も効果が小さいことが分かりました。これは，最も影響力があり信頼性の高い国際情報セキュリティ規格認証であるISO/IEC 27001認証が，国境を越えたデジタル貿易における信頼基盤を構築し，情報非対称性とコンプライアンスコストを削減し，貿易総額を大幅に増加させることを示しています。さらに，輸出業者は認証を通じて，セキュリティガバナンス能力に関する効率的な品質シグナルを国際市場に発信し，激しい国際競争において優位性を確立することができます。認証は国内バイヤーの信頼を高める効果もありますが，輸入決定は外国サプライヤーが特定の管理認証を保有しているかどうかではなく，国内市場の需要，費用対効果，製品特性によって左右されるのが一般的です。したがって，ISO/IEC 27001認証がデジタル貿易輸入に与える影響は比較的小さいと言えます。

第二に，ISO/IEC 27001認証がデジタル貿易に及ぼす促進効果は，明確な異質性を示しています。まず，先進国と発展途上国では，ISO/IEC 27001認証の促進効果に大きな違いが見られます。発展途上国では，総貿易量と輸出に強いプラスの影響を与えているものの，デジタル貿易の推進要因の複雑さや，脆弱なデジタル基盤による制約のため，輸入への影響は限

and constraints imposed by weak digital foundations. For developed countries, no significant effects are observed in either total digital trade volume or import/export figures. The reason may be that developed countries got into the sector earlier and gradually became more competitive with the high-end links in the global digital value chain. For developed countries, their information security management technology and measures are relatively mature. Although ISO/IEC 27001 certification is required in the international market, its additional benefits on digital trade imports are relatively small.

Secondly, there are significant differences in the promoting effect of ISO/IEC 27001 between RCEP member countries and non-RCEP member countries. ISO/IEC 27001 certification has a significant promoting effect on non-member countries' digital trade, whereas it exerts no significant effect on member countries. The reason may be that the e-commerce chapter of RCEP establishes common rules for data security and network security, digital trade facilitation, etc., which establishes a certain level of institutional trust, and may partially replace the need for enterprises to rely solely on ISO/IEC 27001 certification to establish trust.

Recommendations

Firstly, governments should widely promote ISO/IEC 27001 to accelerate the development of digital trade. As global digital trade undergoes profound evolution, information security risks are becoming increasingly prominent. The protective role of ISO/IEC 27001 in digital trade is growing ever more critical. Consequently, governments at all levels should persistently enhance the prevalence and application depth of ISO/IEC 27001 within their jurisdictions to leverage the convenience brought by ISO/IEC 27001 for digital trade. This not only requires the government to implement incentive policies to effectively reduce certification costs, but also requires a systematic layout from the top-level design to promote certification in coordination with the construction of domestic digital infrastructure, the cultivation of digital talents and the formulation of cross-border data flow rules. This will guide more enterprises to obtain ISO/IEC 27001 certification, thereby overcoming market access barriers and improving data reliability and compliance in trade.

Secondly, countries should pay attention to the coordinated development of driving forces from multiple dimensions. With countries increasingly prioritizing digital trade advancement, the global competitive landscape has become complex. ISO/IEC 27001 certification serves as a significant driver for digital trade advancement, though it is not the sole impetus. Consequently, countries should establish a multi-dimensional, synergistic framework of drivers. While promoting the use of ISO/IEC 27001, they must also prioritize technological innovation, economic development, international cooperation, and other facets to avoid dependency or diminishing marginal returns from ISO/IEC 27001.

定的です。先進国では，総デジタル貿易量，輸出入ともに，有意な効果は認められません。その理由としては，先進国はデジタル分野への参入が早く，グローバルなデジタルバリューチェーンのハイエンド段階において，徐々に競争力を高めてきたことが考えられます。先進国では，情報セキュリティ管理技術と対策が比較的成熟しています。ISO/IEC 27001認証は国際市場で必須となっていますが，デジタル貿易輸入に対する追加的なメリットは比較的小さいと言えます。

第二に，ISO/IEC 27001の普及促進効果には，RCEP加盟国と非加盟国との間で大きな違いが見られます。ISO/IEC 27001認証は非加盟国のデジタル貿易に対して顕著な促進効果を発揮する一方，加盟国に対しては顕著な効果は示していません。その理由としては，RCEPの電子商取引章において，データセキュリティ，ネットワークセキュリティ，デジタル貿易の円滑化などに関する共通ルールが定められており，一定レベルの制度的信頼が確立されているため，企業が信頼構築のためにISO/IEC 27001認証のみに頼る必要性が部分的に軽減されていることが考えられます。

提言

まず，各国政府はデジタル貿易の発展を加速させるため，ISO/IEC 27001を広く普及させるべきです。グローバルなデジタル貿易が大きく進化するにつれ，情報セキュリティリスクはますます顕著になっています。デジタル貿易におけるISO/IEC 27001の保護的役割は，ますます重要性を増しています。したがって，あらゆるレベルの政府は，ISO/IEC 27001がデジタル貿易にもたらす利便性を最大限に活用するため，管轄区域内におけるISO/IEC 27001の普及と適用範囲の拡大を継続的に推進していくべきです。そのためには，政府が認証コストを効果的に削減するためのインセンティブ政策を実施するだけでなく，国内デジタルインフラの構築，デジタル人材の育成，国境を越えたデータフロー規則の策定と連携し，認証を促進するための体系的な計画をトップレベルから策定する必要があります。これにより，より多くの企業がISO/IEC 27001認証を取得し，市場参入障壁を克服し，貿易におけるデータの信頼性とコンプライアンスを向上させることができます。

第二に，各国は多方面からの推進力の協調的な発展に注力すべきです。各国がデジタル貿易の推進をますます重視するようになるにつれ，グローバルな競争環境は複雑化しています。ISO/IEC 27001認証はデジタル貿易推進の重要な推進力となりますが，唯一の原動力ではありません。したがって，各国は多角的かつ相乗効果のある推進力の枠組みを構築する必要があります。ISO/IEC 27001の利用促進と並行して，技術革新，経済発展，国際協力などの側面にも優先順位を付け，ISO/IEC 27001への依存や限界収益逓減を回避する必要があります。

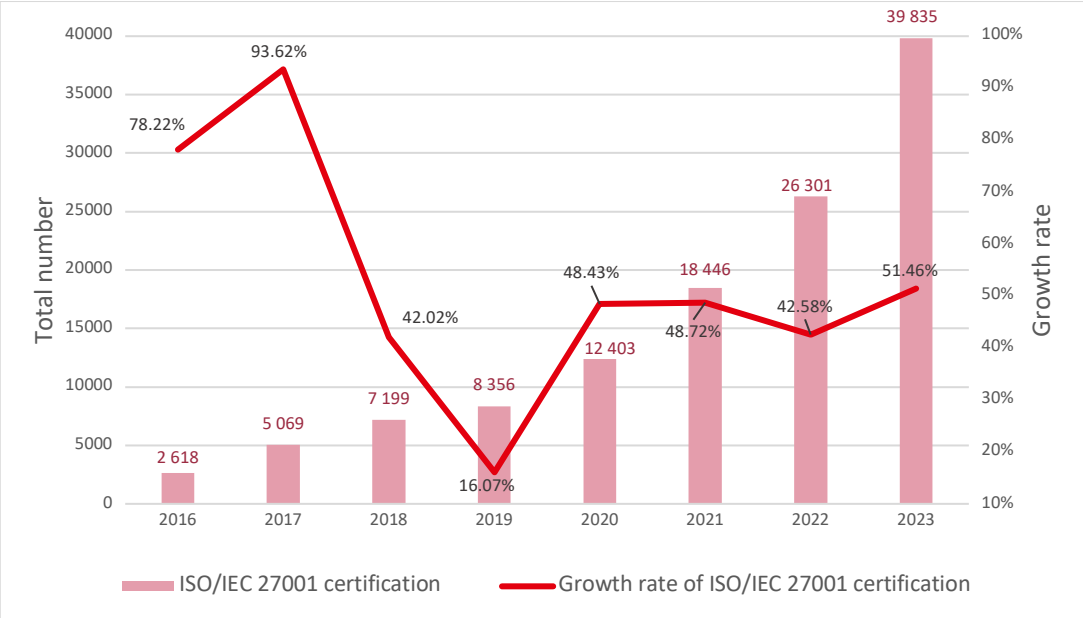
3. The impact of ISO/IEC 27001 certification on digital trade in China: National level

Basic overview of ISO/IEC 27001 certification in China

Overall distribution in China

ISO/IEC 27001 has provided crucial support for enhancing information security management. China has closely followed international ISMS standardization trends while addressing domestic needs, actively advancing the development of its ISMS standards (China Standardization Newsletter 2023). This includes accelerating the national adoption of relevant international standards, such as issuing GB/T 22080:2025, *Cybersecurity Technology – Information Security Management Systems – Requirements*, through the equivalent adoption of ISO/IEC 27001:2022. The timely adoption of Chinese national standards has reduced compliance risks for enterprises within provincial jurisdictions in implementing information security management. This enables businesses to align with international best practices at a lower comprehension cost, directly stimulating rapid growth in certification demand, as illustrated in Figure 6.

Figure 6: Changes in the total number of valid ISO/IEC 27001 certificates in China



Source: ISO Survey 2023. China's 2023 ISO/IEC 27001 certification figures sourced from the National Certification and Accreditation Information Public Service Platform (China).

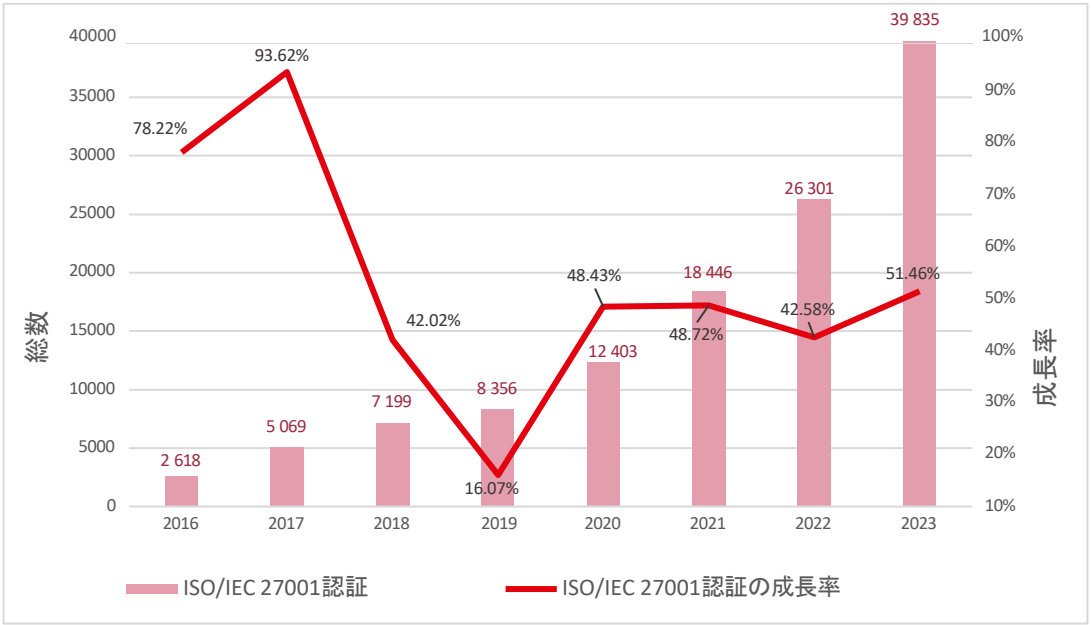
3. ISO/IEC 27001認証が中国のデジタル貿易に与える影響：国家レベル

中国におけるISO/IEC 27001認証の概要

中国におけるISO/IEC 27001の普及状況

ISO/IEC 27001は情報セキュリティマネジメントの強化に不可欠な支援を提供してきた。中国は国際的なISMS標準化の動向を注視しつつ，国内ニーズにも対応し，ISMS規格の開発を積極的に推進している（中国標準化ニュースレター2023）。これには，GB/T 22080:2025 *サイバーセキュリティ技術－情報セキュリティマネジメントシステム－要求事項* の発行など，関連する国際規格の国内導入を加速させる取り組みも含まれており，これはISO/IEC 27001:2022の同等性を採用することによって実現されている。中国国家規格の迅速な導入により，省管轄区域内の企業は情報セキュリティ管理の実施におけるコンプライアンスリスクが軽減されました。これにより，企業はより低い理解コストで国際的なベストプラクティスに準拠できるようになり，図6に示すように，認証需要の急速な増加を直接的に促進しています。

図 6: 中国における有効なISO/IEC 27001認証総数の変化



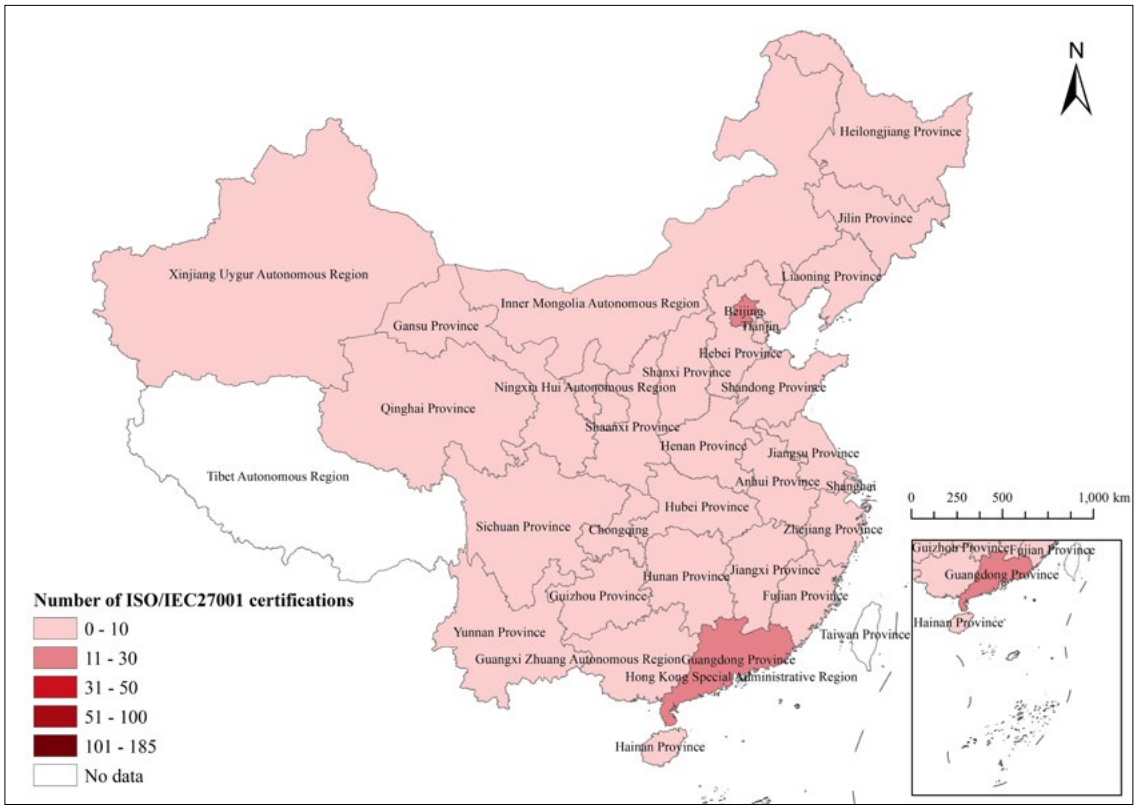
出典：ISO調査2023。中国の2023年ISO/IEC 27001認証データは，国家認証認可情報公開サービスプラットフォーム（中国）より引用。

In terms of volume, China had 2 618 valid certifications in 2016,[13] which surged to 39 835 by 2023.[14] Over this eight-year period, the scale of ISO/IEC 27001 valid certifications expanded more than 15-fold, reflecting Chinese enterprises' growing recognition of the importance of ISO/IEC 27001 certification and the gradual advancement of information security management towards large-scale, standardized implementation. In terms of growth rate, prior to the pandemic, the annual average growth rate of certifications exceeded 70%. Subsequently, the growth rate gradually stabilized, maintaining an annual increase of approximately 50%. This indicates that China's digital economy is shifting from pursuing greater scale to building a high-quality development stage centred on security and trust.

Distribution of listed companies throughout Chinese provinces

Based on data from the China National Certification and Accreditation Information Public Service Platform, this report selected three representative years spanning a significant time period: 2016, 2020 and 2023. ArcGIS software was employed to map the number of ISO/IEC 27001 certifications in Chinese provinces, as shown in Figure 7.

Figure 7: Number of ISO/IEC 27001 certifications for listed companies in each province in 2016, 2020 and 2023



(a) 2016

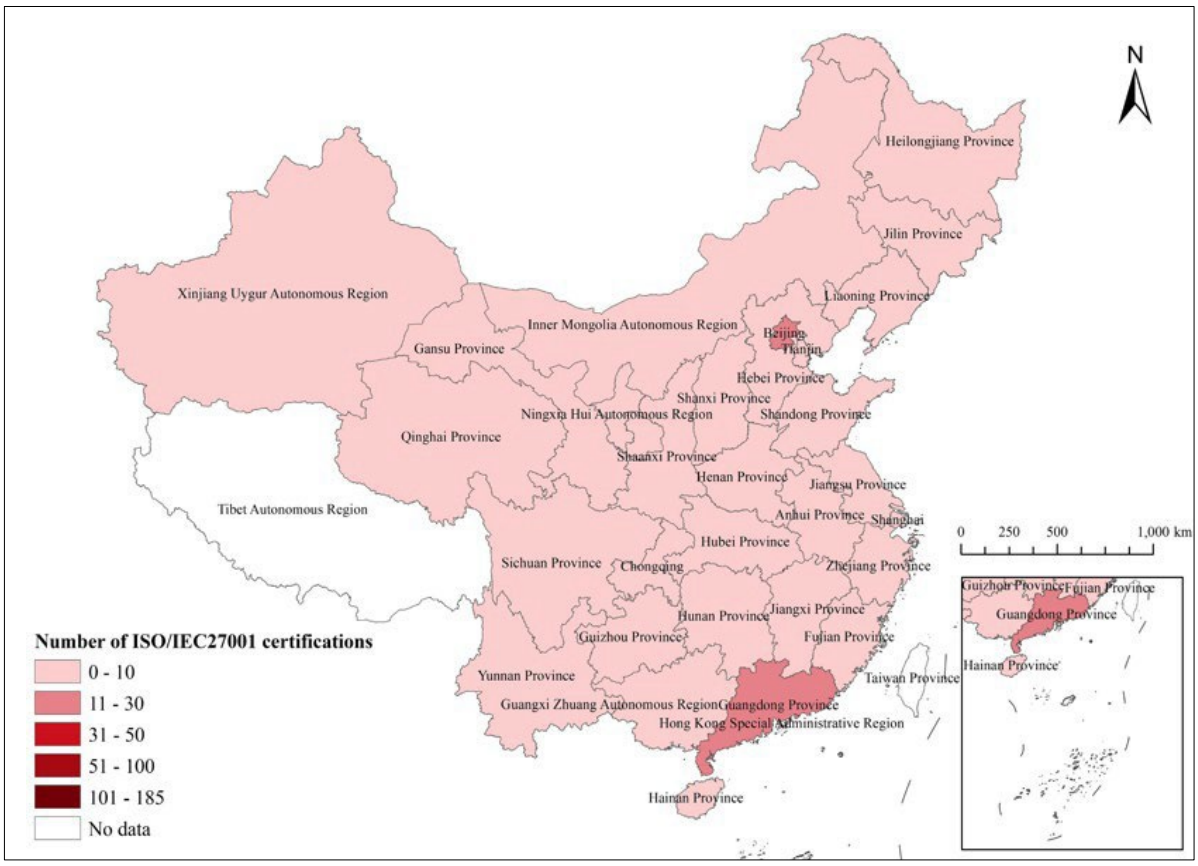
13 ISO - The ISO Survey
14 National Certification and Accreditation Information Public Service Platform: http://cx.cnca.cn/CertECloud/

件数で見ると，中国では2016年に有効な認証件数が2,618件[13]でしたが，2023年には39,835件[14]に急増しました。この8年間で，ISO/IEC 27001の有効な認証件数は15倍以上に拡大し，中国企業におけるISO/IEC 27001認証の重要性に対する認識の高まりと，情報セキュリティ管理の大規模かつ標準化された導入への段階的な進展を反映しています。成長率で見ると，パンデミック以前は認証件数の年間平均成長率は70%を超えていました。その後，成長率は徐々に安定し，年間約50%の増加率を維持しています。これは，中国のデジタル経済が規模の拡大追求から，セキュリティと信頼を中心とした質の高い発展段階の構築へと移行していることを示しています。

中国各省における上場企業の分布

本報告書は，中国国家認証・認可情報公開サービスプラットフォームのデータに基づき，重要な期間を網羅する代表的な3年間（2016年，2020年，2023年）を選定しました。図7に示すように，ArcGISソフトウェアを用いて，中国各省におけるISO/IEC 27001認証取得件数を地図上に示しました。

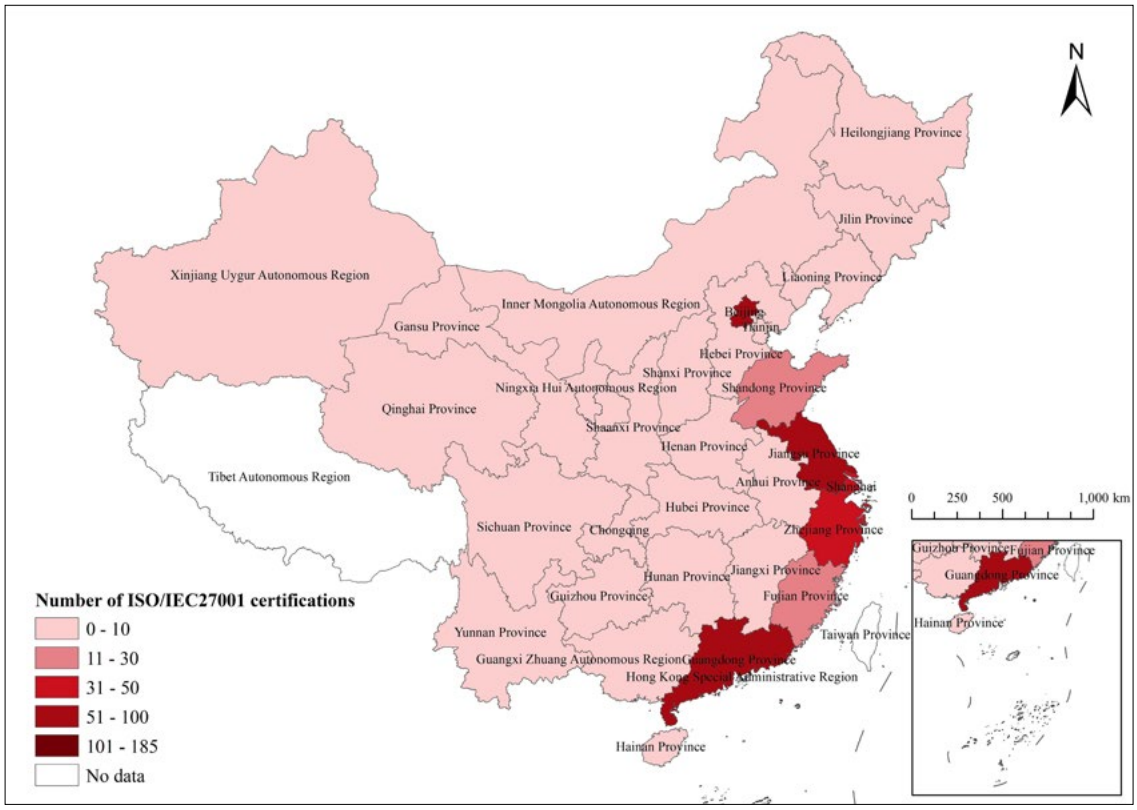
図 7: 2016年，2020年，2023年における各省の上場企業のISO/IEC 27001認証取得件数



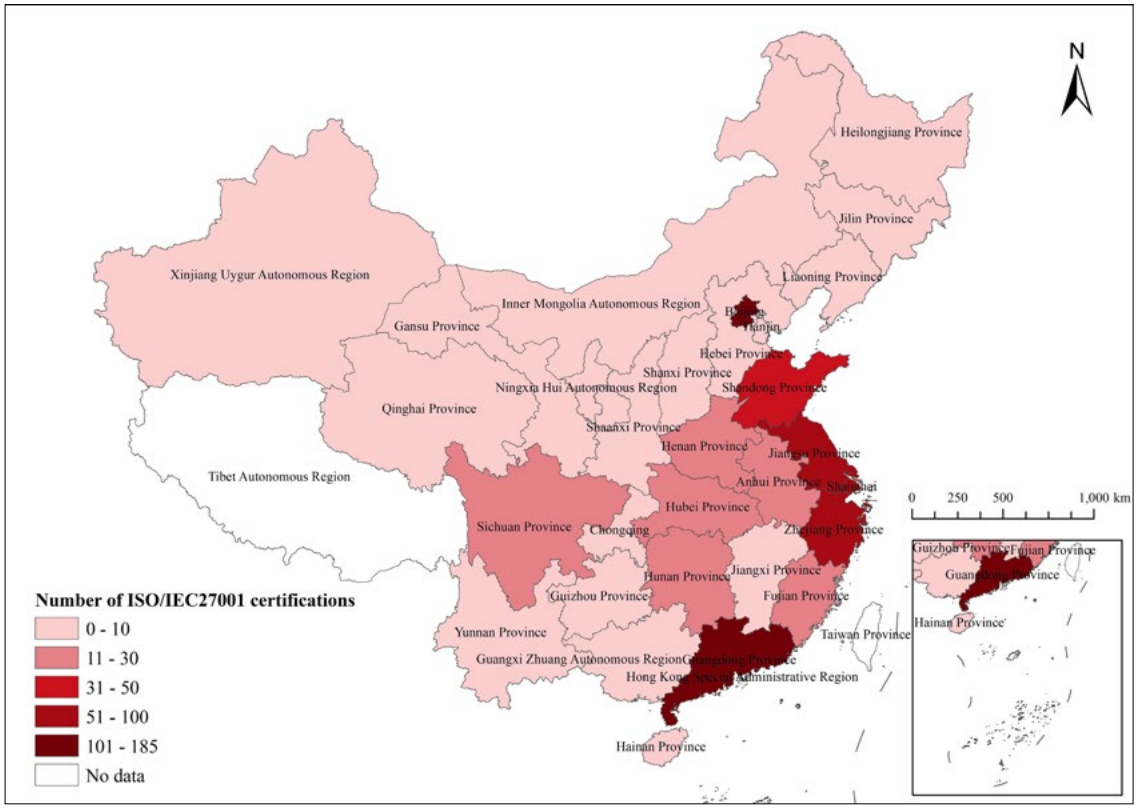
(a) 2016年

13 ISO - ISO調査

14 国家認証・認可情報公開サービスプラットフォーム：http://cx.cnca.cn/CertECloud/

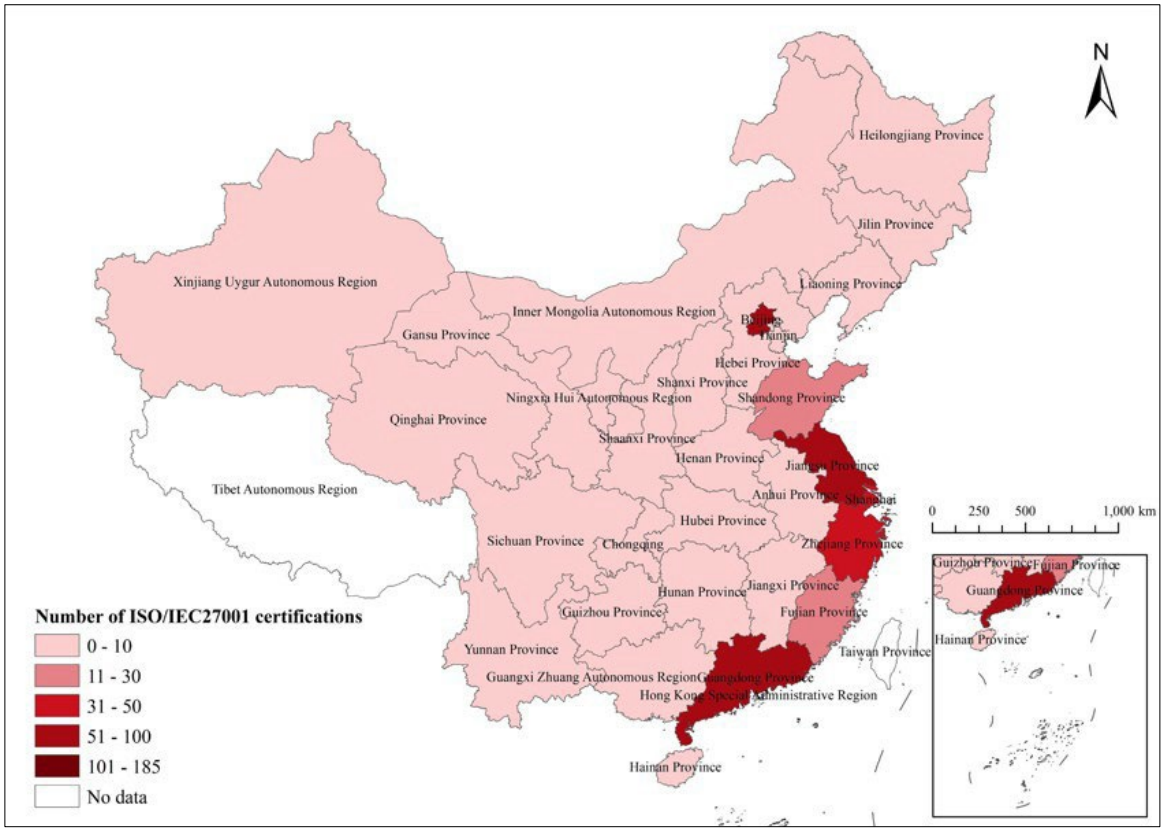


(b) 2020

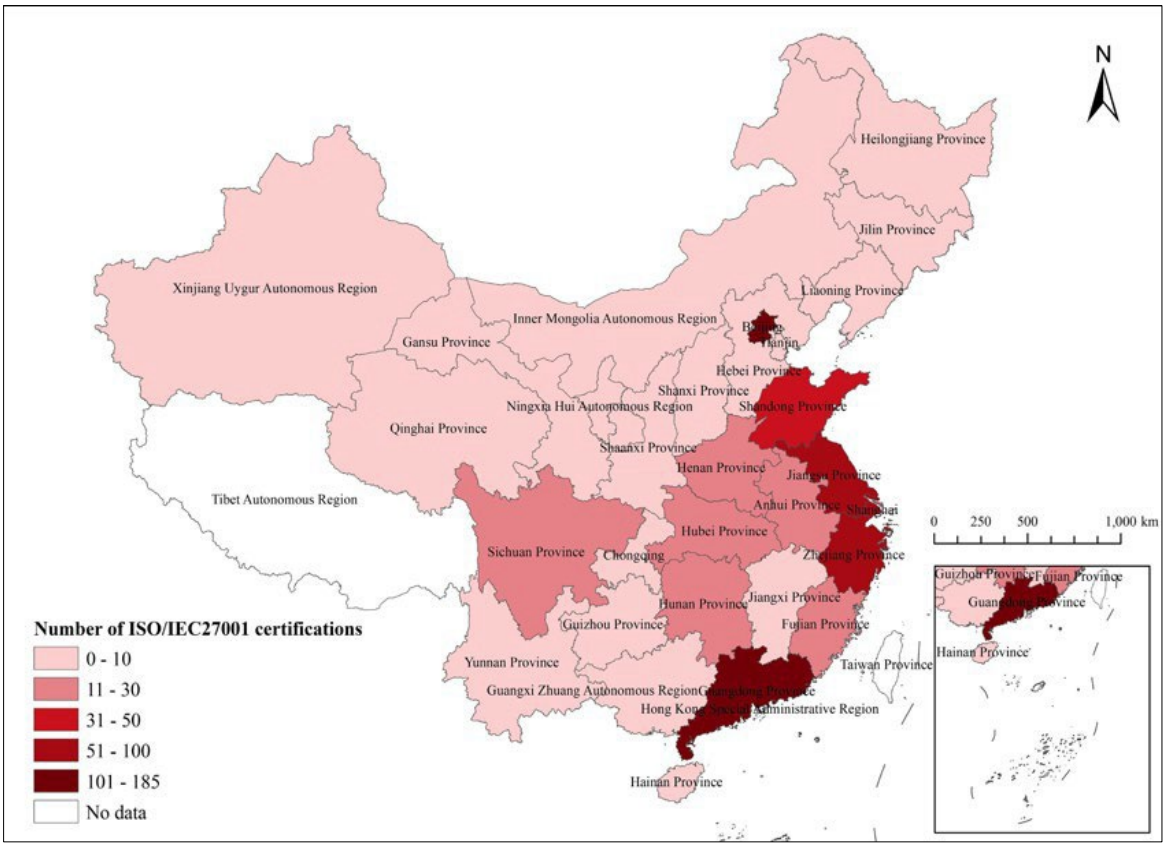


(c) 2023

Source: National Certification and Accreditation Information Public Service Platform (China).
Note: Produced based on the standard map with review number GS(2024)0650 downloaded from the Standard Map Service Website of the Ministry of Natural Resources of China. No modifications were made to the base map boundaries.



(b) 2020年



(c) 2023年

出典：国家認証・認可情報公開サービスプラットフォーム（中国）
注記：中国自然資源部標準地図サービスウェブサイトからダウンロードした，審査番号GS(2024)0650の標準地図に基づいて作成。ベースマップの境界線に変更は加えていません。

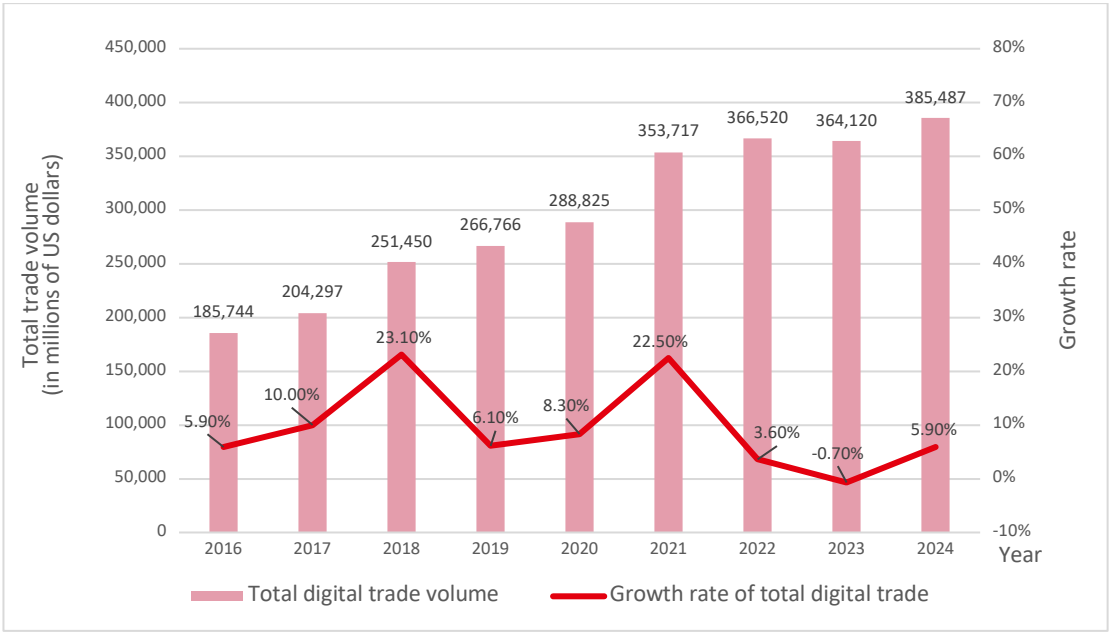
As shown in Figure 7, the number of ISO/IEC 27001 certifications among listed companies varies significantly throughout provinces. In 2016, ISO/IEC 27001 certification first gained traction in Guangdong Province and Beijing Municipality, and gradually spread to other eastern provinces such as Jiangsu, Shandong and Zhejiang. By 2023, listed companies in the eastern provinces continued to deepen their ISO/IEC 27001 certification efforts, and the certification trend expanded into central and western regions, including Anhui, Hebei and Henan.

Overview of digital trade in China

Distribution in China

In response to the accelerating structural transformation of the global digital economy, China continues to strengthen the overarching design and policy guidance for digital trade. It seizes opportunities presented by the digital economy, is deepening reform and opening its market to digital trade and enhancing international cooperation in digital transactions. This approach has sustained the robust momentum of digital trade development, achieving steady growth in scale, as illustrated in Figure 8.

Figure 8: Volume and growth rate of digital trade in China



*USD at current prices in millions
Source: UNCTADstat

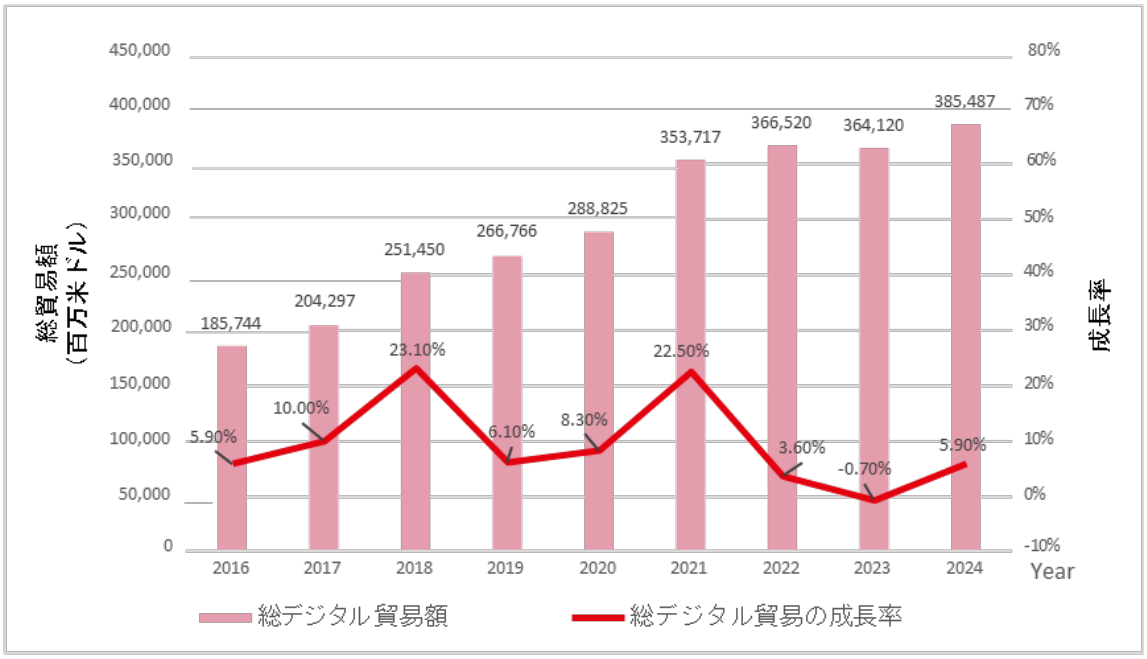
図7に示すように，上場企業におけるISO/IEC 27001認証の取得数は，省によって大きく異なっている。2016年，ISO/IEC 27001認証は広東省と北京市で最初に普及し始め，その後，江蘇省，山東省，浙江省などの東部諸省へと徐々に拡大しました。2023年までに，東部諸省の上場企業はISO/IEC 27001認証取得への取り組みをさらに強化し，認証取得の傾向は安徽省，河北省，河南省などの中部・西部地域にも広がりました。

中国におけるデジタル貿易の概要

中国における流通状況

グローバルなデジタル経済の構造転換の加速に対応し，中国はデジタル貿易に関する包括的な設計と政策指導を継続的に強化しています。デジタル経済がもたらす機会を捉え，改革を深化させ，デジタル貿易への市場開放を進めるとともに，デジタル取引における国際協力を強化しています。このアプローチは，図8に示すように，デジタル貿易発展の力強い勢いを維持し，規模の着実な拡大を実現してきました。

図 8: 中国のデジタル貿易量と成長率



*米ドル（時価，百万米ドル）
出典：UNCTADstat

Figure 9 illustrates the evolution of China's total digital trade volume from 2016 to 2024. In aggregate terms, China's digital trade surged from USD 0.186 trillion in 2016 to USD 0.385 trillion in 2024, reflecting a steady expansion that underscores the growing dynamism of China's digital trade sector. In terms of growth rate, China's digital trade volume exhibits a wave-like pattern with three-year cycles, particularly pronounced between 2016 and 2021, before levelling off. This pattern may stem from China's 2016 implementation of new cross-border e-commerce retail import policies. The positive list plus customs declaration model impacted cross-border digital ordering trade. Meanwhile, 2019 witnessed escalating global trade protection measures that undermined the free, open and mutually beneficial multilateral trading system, hindering China's digital trade development.

Ranking changes in digital trade development volume throughout Chinese provinces

Table 9 presents the digital trade development levels and ranking variations throughout 30 provinces in China for 2016, 2020 and 2023. The top six provinces, including Beijing, Guangdong and Jiangsu are located in eastern China. These regions exhibit relatively advanced levels of digital trade development and maintain relatively stable rankings, with no significant fluctuations in their positions. By contrast, the rankings of the remaining provinces exhibit considerable volatility, predominantly concentrated in central and western China. This indicates that digital trade development in most Chinese provinces remains in an early competitive phase, with no province having achieved a pronounced, decisive lead.

Table 9: Digital trade development levels by province in 2016, 2020 and 2023

	2019		2020		2021	
Province	Digital trade development level	Rank	Digital trade development level	Rank	Digital trade development level	Rank
Guangdong	0.355	1	0.628	1	0.733	1
Jiangsu	0.337	2	0.406	3(↓1)	0.476	3
Beijing	0.211	3	0.407	2(↑1)	0.555	2
Shandong	0.203	4	0.263	6(↓2)	0.402	5(↑1)
Shanghai	0.193	5	0.268	5	0.431	4(↑1)
Zhejiang	0.180	6	0.306	4(↑2)	0.359	6(↓2)
Liaoning	0.126	7	0.105	15(↓8)	0.100	12(↑3)
Fujian	0.118	8	0.145	8	0.146	8
Hubei	0.114	9	0.126	10(↓1)	0.128	10
Sichuan	0.099	10	0.183	7(↑3)	0.169	7
Shaanxi	0.095	11	0.104	16(↓5)	0.071	17(↓1)
Chongqing	0.071	12	0.115	12	0.142	9(↑3)
Anhui	0.057	13	0.112	13	0.110	11(↑2)
Hainan	0.057	14	0.047	26(↓12)	0.047	21(↑5)
Hunan	0.051	15	0.137	11(↑4)	0.093	14(↓3)

図9は，2016年から2024年までの中国の総デジタル貿易額の推移を示しています。総計で見ると，中国のデジタル貿易は2016年の0.186兆米ドルから2024年には0.385兆米ドルへと急増しており，中国のデジタル貿易セクターのダイナミズムの高まりを裏付ける着実な拡大を示しています。成長率に関して言えば，中国のデジタル貿易量は3年周期の波状パターンを示しており，特に2016年から2021年にかけて顕著な伸びを見せた後，横ばい状態となっています。このパターンは，中国が2016年に新たな越境電子商取引小売輸入政策を導入したことに起因する可能性があります。ポジティブリストプラス税関申告モデルは，越境デジタル注文貿易に影響を与えました。一方，2019年には世界的な貿易保護措置が強化され，自由で開かれた互恵的な多国間貿易体制が損なわれ，中国のデジタル貿易の発展が阻害されました。

中国各省におけるデジタル貿易発展量のランキング変動

表9は，2016年，2020年，2023年の中国30省におけるデジタル貿易発展レベルとランキングの変動を示しています。北京，広東，江蘇省を含む上位6省は中国東部に位置しています。これらの地域はデジタル貿易発展レベルが比較的高く，順位も比較的安定しており，大きな変動は見られません。対照的に，残りの省のランキングは大きな変動を示しており，その変動は主に中国の中部および西部に集中しています。これは，中国のほとんどの省におけるデジタル貿易の発展が依然として競争の初期段階にあり，どの省も明確な優位性を確立していないことを示しています。

表 9: 2016年，2020年，2023年における省別デジタル貿易発展レベル

	2019		2020		2021	
省	デジタル貿易発展レベル	順位	デジタル貿易発展レベル	順位	デジタル貿易発展レベル	順位
広東省	0.355	1	0.628	1	0.733	1
江蘇省	0.337	2	0.406	3(↓1)	0.476	3
北京市	0.211	3	0.407	2(↑1)	0.555	2
山東省	0.203	4	0.263	6(↓2)	0.402	5(↑1)
上海市	0.193	5	0.268	5	0.431	4(↑1)
浙江省	0.180	6	0.306	4(↑2)	0.359	6(↓2)
遼寧省	0.126	7	0.105	15(↓8)	0.100	12(↑3)
福建省	0.118	8	0.145	8	0.146	8
湖北省	0.114	9	0.126	10(↓1)	0.128	10
四川省	0.099	10	0.183	7(↑3)	0.169	7
陝西省	0.095	11	0.104	16(↓5)	0.071	17(↓1)
重慶市	0.071	12	0.115	12	0.142	9(↑3)
安徽省	0.057	13	0.112	13	0.110	11(↑2)
海南省	0.057	14	0.047	26(↓12)	0.047	21(↑5)
湖南省	0.051	15	0.137	11(↑4)	0.093	14(↓3)

Province	2019		2020		2021	
	Digital trade development level	Rank	Digital trade development level	Rank	Digital trade development level	Rank
Tianjin	0.048	16	0.075	21(↓5)	0.096	13(↑8)
Jilin	0.044	17	0.040	27(↓10)	0.024	29(↓2)
Henan	0.042	18	0.137	9(↑9)	0.089	16(↓7)
Yunnan	0.042	19	0.096	17(↑2)	0.044	22(↓5)
Guizhou	0.037	20	0.087	18(↑2)	0.051	19(↓1)
Hebei	0.037	21	0.106	14(↑7)	0.066	18(↓4)
Qinghai	0.034	22	0.029	29(↓7)	0.036	25(↑4)
Jiangxi	0.034	23	0.080	20(↑3)	0.089	15(↑5)
Ningxia	0.033	24	0.027	30(↓6)	0.032	27(↑3)
Gansu	0.030	25	0.047	25	0.028	28(↓3)
Guangxi	0.030	26	0.084	19(↑7)	0.048	20(↓1)
Heilongjiang	0.027	27	0.037	28(↓1)	0.023	30(↓2)
Inner Mongolia	0.024	28	0.049	24(↑4)	0.042	24
Shanxi	0.022	29	0.054	22(↑7)	0.043	23(↓1)
Xinjiang	0.013	30	0.051	23(↑7)	0.034	26(↓3)

Eastern region Central region Western region

Note: The digital trade development level is measured and evaluated using the entropy method described in the next section.

	2019		2020		2021	
省	デジタル貿易発展レベル	順位	デジタル貿易発展レベル	順位	デジタル貿易発展レベル	順位
天津市	0.048	16	0.075	21(↓5)	0.096	13(↑8)
吉林省	0.044	17	0.040	27(↓10)	0.024	29(↓2)
河南省	0.042	18	0.137	9(↑9)	0.089	16(↓7)
雲南省	0.042	19	0.096	17(↑2)	0.044	22(↓5)
貴州省	0.037	20	0.087	18(↑2)	0.051	19(↓1)
河北省	0.037	21	0.106	14(↑7)	0.066	18(↓4)
青海省	0.034	22	0.029	29(↓7)	0.036	25(↑4)
江西省	0.034	23	0.080	20(↑3)	0.089	15(↑5)
寧夏回族自治区	0.033	24	0.027	30(↓6)	0.032	27(↑3)
甘粛省	0.030	25	0.047	25	0.028	28(↓3)
広西チワン族自治区	0.030	26	0.084	19(↑7)	0.048	20(↓1)
黒竜江省	0.027	27	0.037	28(↓1)	0.023	30(↓2)
内モンゴル自治区	0.024	28	0.049	24(↑4)	0.042	24
山西省	0.022	29	0.054	22(↑7)	0.043	23(↓1)
新疆ウイグル自治区	0.013	30	0.051	23(↑7)	0.034	26(↓3)

● 東部地域 ● 中部地域 ● 西部地域

注記：デジタル貿易発展レベルは，次節で説明するエントロピー法を用いて測定・評価されています。

Comparative analysis of the annual average development level of digital trade throughout Chinese provinces

To provide an intuitive comparison of the overall development levels of digital trade throughout China's provinces, Figure 8(A) reports the annual average values of each province's digital trade development level. From this perspective, the national average for 2016-2023 stands at 0.123. Among these, eight provinces and regions exceed China's nationwide average, accounting for approximately 26.67%. Conversely, 22 provinces and regions fall below China's nationwide average, representing about 73.33%.

This indicates that the digital trade development level in the majority of China's provinces currently remains below its nationwide average, primarily in the central and western regions. This is because central and western provinces not only have relatively less access to capital and human resources, but also lag eastern regions in digital capital investment and digital infrastructure, significantly constraining the advancement of digital trade in these areas. By contrast, the average level of digital trade development in the eastern provinces has reached 0.232, almost twice China's nationwide average. This reflects their abundant digital capital and a more favorable digital environment, including more advanced digital infrastructure, which effectively promotes the development of digital trade. Consequently, digital trade development remains uneven in eastern, central and western regions, indicating that bridging the digital divide between these areas remains a significant challenge.

Comparative analysis of the average annual growth rates in digital trade development throughout Chinese provinces

To analyse whether the growth of digital trade development levels in Chinese provinces faces bottlenecks, Figure 8(B) displays the growth rates of digital trade development levels in each province from 2016 to 2023. China's nationwide average annual growth rate for digital trade development stands at 9.6%. Among the three major regions, the central and western ones recorded an average annual growth rate of 10.1% for digital trade development, exceeding the national average. Meanwhile, the average annual growth rates for digital trade development in provinces within the eastern and central regions were slightly below the nationwide average.

Looking at the annual average growth rates of digital trade development in provincial regions, 18 provinces recorded growth rates exceeding China's nationwide average, accounting for 60% of the total. The top five provinces by growth rate were Xinjiang, Henan, Guangxi, Jiangxi and Shanxi. Notably, Shaanxi, Hainan and Jilin recorded negative average annual growth rates in digital trade development, indicating bottlenecks in advancing digital trade in these provinces. This may stem from accelerated outflows of high-end talent and capital, posing challenges to digital trade development in these areas.

中国各省におけるデジタル貿易の年間平均発展レベルの比較分析

中国各省におけるデジタル貿易の全体的な発展レベルを直感的に比較するため，図8(A)では各省のデジタル貿易発展レベルの年間平均値を示しています。この観点から見ると，2016年から2023年までの全国平均は0.123です。これらのうち，8つの省・地域が中国全国平均を上回っており，全体の約26.67%を占めています。逆に，22の省・地域が中国全国平均を下回っており，全体の約73.33%を占めています。

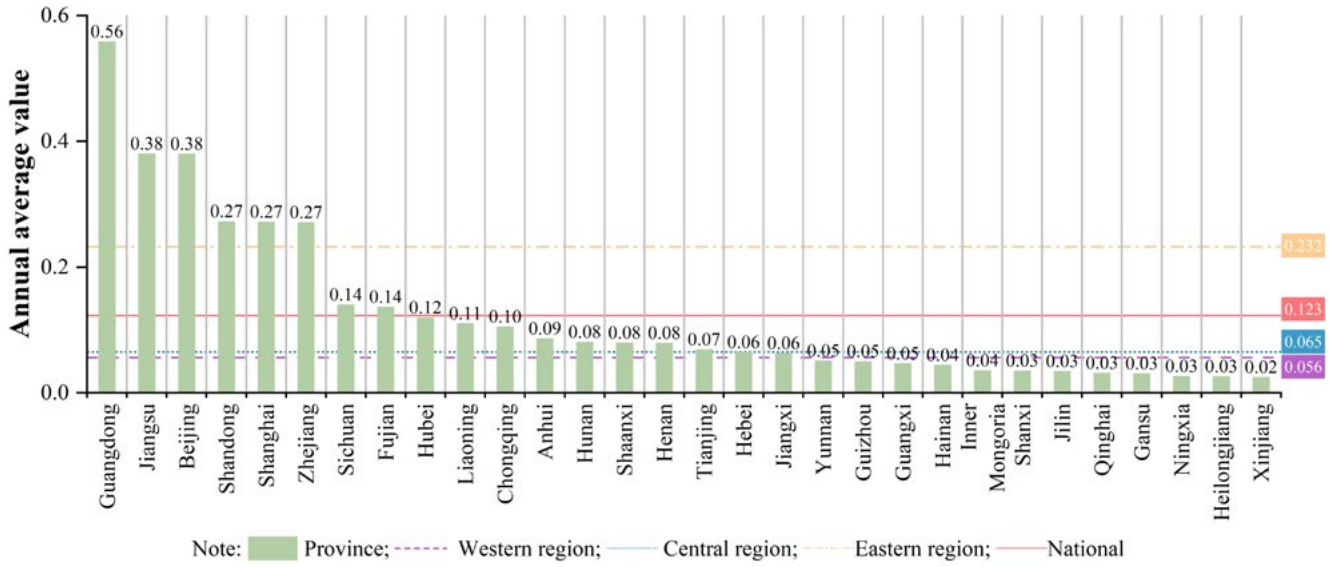
これは，中国の大多数の省・地域，特に中部・西部地域において，デジタル貿易の発展レベルが依然として全国平均を下回っていることを示しています。これは，中部・西部地域は資本と人材へのアクセスが比較的少ないだけでなく，デジタル資本投資とデジタルインフラの整備においても東部地域に遅れをとっており，これらの地域におけるデジタル貿易の発展を著しく阻害しているためです。対照的に，東部諸省のデジタル貿易発展レベルの平均は0.232に達し，中国全国平均のほぼ2倍となっています。これは，東部諸省の豊富なデジタル資本と，より高度なデジタルインフラを含む，より良好なデジタル環境を反映しており，デジタル貿易の発展を効果的に促進しています。その結果，東部，中部，西部地域におけるデジタル貿易発展は依然として不均衡であり，これらの地域間のデジタルデバイドの解消は依然として大きな課題であることを示しています。

中国各省におけるデジタル貿易発展の年間平均成長率の比較分析

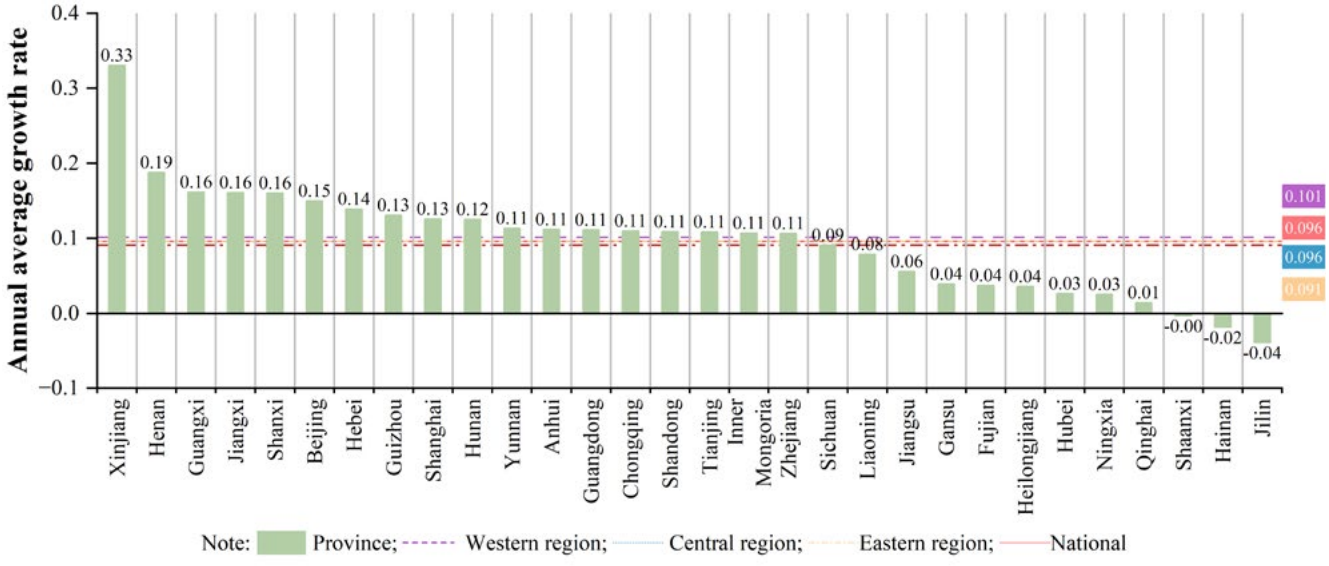
中国各省におけるデジタル貿易発展レベルの成長がボトルネックに直面しているかどうかを分析するため，図8(B)は2016年から2023年までの各省におけるデジタル貿易発展レベルの成長率を示しています。中国全国におけるデジタル貿易発展の年間平均成長率は9.6%です。3大地域のうち，中部と西部ではデジタル貿易発展の年間平均成長率が10.1%と，全国平均を上回っています。一方，東部・中部地域の各省におけるデジタル貿易発展の年間平均成長率は，全国平均をわずかに下回りました。

省レベルのデジタル貿易発展の年間平均成長率を見ると，18の省が中国全国平均を上回る成長率を記録し，全体の60%を占めました。成長率上位5省は，新疆ウイグル自治区，河南省，広西チワン族自治区，江西チワン族自治区，山西チワン族自治区でした。特筆すべきは，陝西省，海南省，吉林省ではデジタル貿易発展の年間平均成長率がマイナスを記録しており，これらの省におけるデジタル貿易の発展にボトルネックが生じていることを示しています。これは，ハイエンド人材と資本の流出加速が，これらの地域におけるデジタル貿易発展の課題となっていることが原因と考えられます。

Figure 8: 2016-2023 average annual value and average annual growth rate of digital trade development throughout Chinese provinces

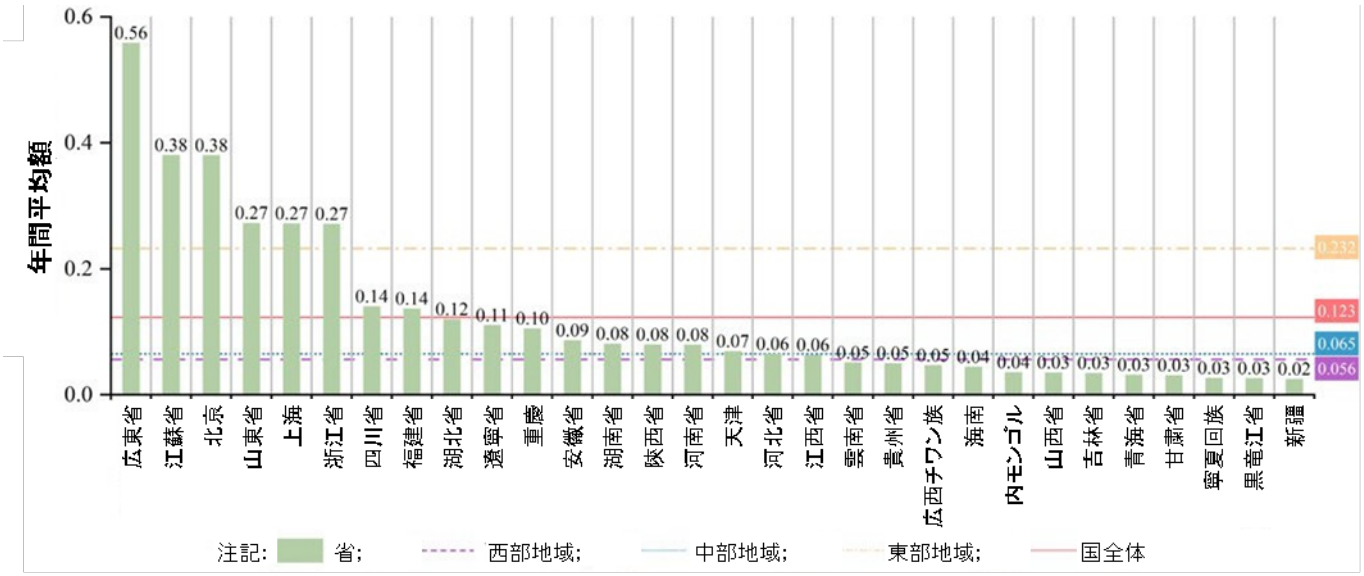


(A) Annual average value

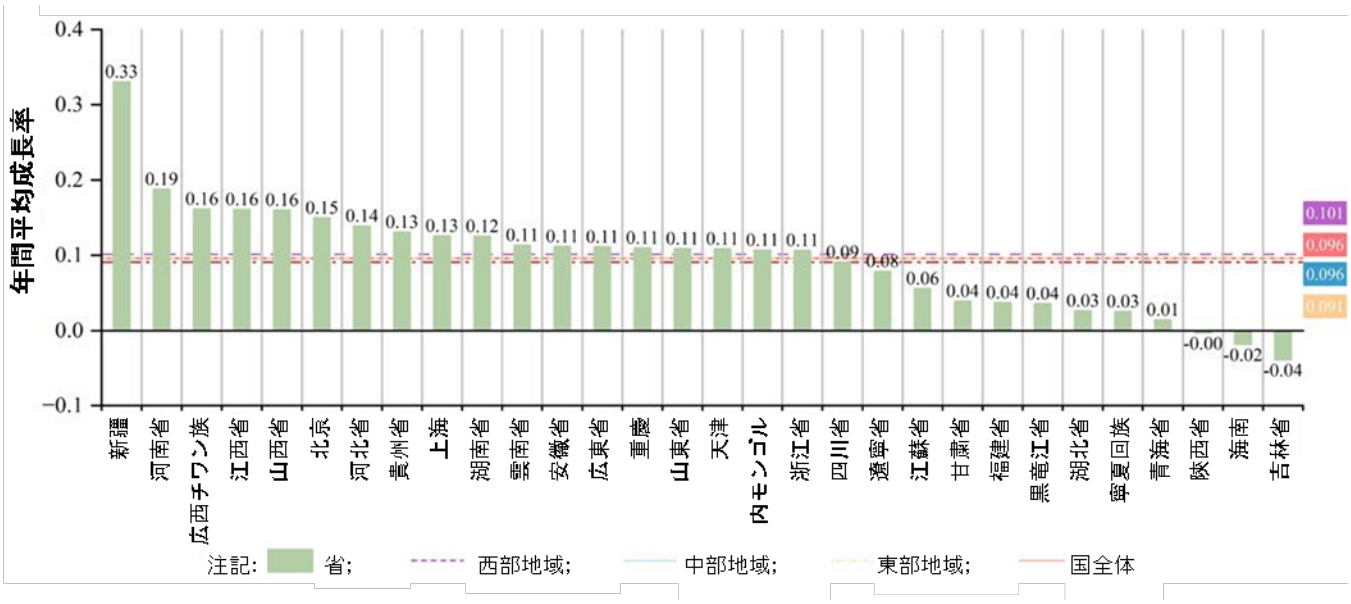


(B) Annual average growth rate

図 8: 2016年～2023年の中国各省におけるデジタル貿易発展の年間平均額と年間平均成長率



(A) 年間平均額



(B) 年間平均成長率

The impact of ISO/IEC 27001 certification on digital trade in China: A regression analysis

Digital trade, as a new form of commerce, leverages IT and internet channels to facilitate rapid transactions and delivery of goods and services through e-commerce, platform economies and other scenarios. Throughout this process, the value creation enabled by digital trade requires compliance safeguards, such as ISO/IEC 27001 certification. The ISO/IEC 27001 operates on a risk-based approach with a focus on continuous improvement, following the Plan-Do-Check-Act (PDCA) cycle. According to data released in the Global Digital Trade Development Report 2024, China has emerged as a major force in the global digital trade arena, ranking third worldwide in terms of scale, demonstrating the robust growth momentum of emerging economies.

Therefore, this section focuses on examining the impact of ISO/IEC 27001 certification on the development level of digital trade in China's provinces. Addressing this question will help enterprises within provincial regions prioritize cybersecurity and digital technology risks, accelerate the integration of ISO/IEC 27001 and other information security standards into internal management systems, and establish new information-based and digital management frameworks.

Regression analysis model and variables

Dual machine learning offers distinct advantages in variable selection and model estimation, mitigating issues inherent in ordinary multiple linear regression models such as the "curse of dimensionality", biased estimation and model specification errors (Yang et al., 2020). Based on this, this report employs the dual machine learning (DML) model proposed by Chernozhukov et al. (2017) to analyse the impact of ISO/IEC 27001 on digital trade in China. A partially linear dual machine learning model validated by peer experts is constructed as follows:

$$Digital\ trade_{it} = \theta_0 ISO/IEC27001_{it} + g(X_{it}) + U_{it}, \quad E(U_{it} | ISO/IEC27001_{it}, X_{it}) \tag{2}$$

$$ISO/IEC27001_{it} = m(X_{it}) + V_{it}, E(V_{it} | X_{it}) \tag{3}$$

In this context, the subscript i denotes the province, and t denotes the year. Equation (2) represents the base regression equation, where the dependent variable Digital $trade_{it}$ measures the level of digital trade development in Chinese province i during year t. The core explanatory variable $ISO/IEC27001_{it}$ represents the total number of *ISO/IEC 27001* certifications held by listed companies in province i during year t; θ_0 denotes the coefficient of the key variable under examination; X_{it} constitutes the set of high-dimensional control variables influencing digital trade development; U_{it} denotes the error term with conditional mean 0. Equation (3) is the auxiliary regression equation, where $m(X_{it})$ represents the regression coefficient of the explanatory variable on the high-dimensional control variables, and V_{it} similarly denotes the error term with conditional mean 0.

ISO/IEC 27001認証が中国のデジタル貿易に与える影響：回帰分析

デジタル貿易は，新たな商取引形態として，ITとインターネットチャネルを活用し，電子商取引，プラットフォーム経済，その他のシナリオを通じて，商品やサービスの迅速な取引と提供を促進します。このプロセス全体を通して，デジタル貿易によって実現される価値創造には，ISO/IEC 27001認証などのコンプライアンス対策が不可欠です。ISO/IEC 27001は，PDCA（計画・実行・評価・改善）サイクルに基づき，継続的な改善に重点を置いたリスクベースのアプローチを採用しています。2024年版グローバルデジタル貿易発展報告書によると，中国は世界のデジタル貿易分野において主要な勢力として台頭し，規模で世界第3位にランクインしており，新興経済国の力強い成長を物語っています。

したがって，本節では，ISO/IEC 27001認証が中国の各省におけるデジタル貿易の発展レベルに与える影響について考察します。この課題に取り組むことで，省域内の企業はサイバーセキュリティとデジタル技術リスクの優先順位付けを行い，ISO/IEC 27001をはじめとする情報セキュリティ規格を内部管理システムに迅速に統合し，新たな情報ベースのデジタル管理フレームワークを構築することが可能になります。

回帰分析モデルと変数

デュアル機械学習は，変数選択とモデル推定において明確な利点を持ち，「次元の呪い」，推定値の偏り，モデル仕様の誤差といった，通常の重回帰モデルに内在する問題を軽減します（Yang et al., 2020）。このことを踏まえ，本報告書では，Chernozhukov et al. (2017) が提案したデュアル機械学習（DML）モデルを用いて，ISO/IEC 27001が中国のデジタル貿易に与える影響を分析します。専門家による検証済みの部分線形デュアル機械学習モデルは，以下のように構築されます。

$$Digital\ trade_{it} = \theta_0 ISO/IEC27001_{it} + g\ (X_{it}) + U_{it},\quad E\ (U_{it} | ISO/IEC27001_{it}, X_{it}) \tag{2}$$

$$ISO/IEC27001_{it} = m\ (X_{it}) + V_{it}, E\ (V_{it} | X_{it}) \tag{3}$$

ここで，添え字 i は省を，t は年を表します。式（2）は基本回帰式を表し，従属変数 $Digital\ Trade_{it}$ は，t 年における中国の省 i のデジタル貿易発展レベルを表します。主要説明変数 $ISO/IEC27001_{it}$ は，t 年における省 i の上場企業が保有するISO/IEC 27001認証の総数を表します。θ_0 は，分析対象となる主要変数の係数です。X_{it} は，デジタル貿易発展に影響を与える高次元制御変数の集合です。U_{it} は，条件付き平均が 0 の誤差項を表します。式（3）は補助回帰式であり，$m(X_{it})$ は，高次元制御変数に対する説明変数の回帰係数を表し，V_{it} も同様に，条件付き平均が 0 の誤差項を表します。

Number of ISO/IEC 27001 certifications

Drawing on the research of Wu et al. (2021), this report measures the number of ISO/IEC 27001 certifications obtained by listed companies in Chinese provinces by aggregating data and applying natural logarithms. The indicator is constructed as follows:

1. Using Tesseract for OCR recognition on the National Certification and Accreditation Information Public Service Platform to crawl ISO/IEC 27001 certification data from listed companies.
2. Manually screening crawled content to verify whether listed companies completed annual surveillance audits and triennial recertifications on schedule.
3. Aggregating the annual certification status of listed companies by their registered location to the corresponding province.

Level of digital trade development

Drawing on the research of Zhu et al. (2024) and considering the Chinese context of digital trade development and data availability, this report constructs an index system for digital trade development level (as shown in Table 10) by selecting 10 secondary indicators from two dimensions: digital ordering trade driven by industrial digitization, and digital products, services and technology trade. The former focuses on the digital ordering trade resulting from the use of digital technology to upgrade production, circulation and transactions in traditional manufacturing, agriculture and service industries. The latter focuses on cross-border transactions of digital technology, products and services. Using panel data from 30 Chinese provinces spanning 2016-2023, the entropy weighting method and linear weighting method were employed to measure digital trade development levels in Chinese provinces.

The steps were as follows:

1. Standardize the data. The results of standardization are shown below:

$$x_{ikt}^{*} = \frac{x_{ikt} - min(x_{ikt})}{max(x_{ikt}) - min(x_{ikt})} \quad (4)$$

Here, i denotes each province, autonomous region or municipality, where i = 1, 2, ..., n; k represents each indicator measuring China's digital trade development level, where k = 1, 2, ..., m; t indicates the year, where t = 1, 2, ..., s. x^{*}_{ikt} denotes the standardized result of the k^{th} indicator for the i^{th} province in the t^{th} year.

2. Calculate the weight assigned to the k^{th} indicator for the i^{th} province in the t^{th} year:

$$p_{ikt} = \frac{x_{ikt}^{*}}{\sum_{i=1}^{n} x_{ikt}^{*}} \quad (5)$$

3. Calculate the information entropy (e_{kt}) of the k^{th} indicator in year t:

$$e_{kt} = -\frac{1}{\ln n} \sum_{i=1}^{n} p_{ikt} \ln(p_{ikt}) \quad (6)$$

4. Calculate the information entropy redundancy (g_{kt}) of the k^{th} indicator in year t:

$$g_{kt} = 1 - e_{kt} \quad (7)$$

5. Measure the k_{th} indicator (w_{kt}) in year t:

$$w_{kt} = \frac{g_{kt}}{\sum_{k=1}^{m} g_{ut}} \quad (8)$$

6. Using the linear weighted method, calculate the level of China's digital trade development for province i in year t.

$$Digtal\ trade_{it} = \sum_{k=1}^{m} w_{kt} x_{ikt}^{*} \quad (9)$$

ISO/IEC 27001認証数

Wu et al.の研究（2021年）に基づく本報告書は，中国の各省に所在する上場企業が取得したISO/IEC 27001認証の数を，データを集計し自然対数を適用することで測定しています。指標は以下のように構築されています。

1. 国家認証認可情報公開サービスプラットフォーム上でTesseractを用いてOCR認識を行い，上場企業のISO/IEC 27001認証データを収集します。
2. 収集したデータを手作業で精査し，上場企業が年次監視監査および3年ごとの再認証を予定通りに完了しているかどうかを確認します。
3. 上場企業の登録所在地別に，各省における年次認証状況を集計します。

デジタル貿易発展レベル

Zhu et al.の研究（2024年）に基づき，中国のデジタル貿易発展状況とデータ入手可能性を考慮し，本報告書では，産業デジタル化によるデジタル発注貿易とデジタル製品・サービス・技術貿易という2つの側面から10の二次指標を選択し，デジタル貿易発展レベルを示す指標システムを構築しました（表10参照）。前者は，伝統的な製造業，農業，サービス業における生産，流通，取引の高度化にデジタル技術が活用された結果として生じるデジタル注文貿易に焦点を当てています。後者は，デジタル技術，製品，サービスの越境取引に焦点を当てています。2016年から2023年までの中国30省のパネルデータを用いて，エントロピー加重法と線形加重法により，中国各省のデジタル貿易発展レベルを測定しました。

手順は以下のとおりです。

1. データの標準化。標準化の結果は以下のとおりです。

$$x^*_{ikt} = \frac{x_{ikt} - min(x_{ikt})}{max(x_{ikt}) - min(x_{ikt})} \quad (4)$$

ここで，i は各省，自治区，直轄市を表し，$i = 1, 2, ..., n$ です。k は中国のデジタル貿易発展レベルを測定する各指標を表し，$k = 1, 2, ..., m$ です。t は年を表し，$t = 1, 2, ..., s$ です。x^*_{ikt} は，t 年における i 番目の省の k 番目の指標の標準化の結果を表します。

2. t 年における i 番目の省の k 番目の指標に割り当てられる重みを計算します。

$$p_{ikt} = \frac{x^*_{ikt}}{\sum_{i=1}^{n} x^*_{ikt}} \quad (5)$$

3. t 年における k 番目の指標の情報エントロピー（e_{kt}）を計算します。

$$e_{kt} = -\frac{1}{\ln n} \sum_{i=1}^{n} p_{ikt} \ln(p_{ikt}) \quad (6)$$

4. t 年における k 番目の指標の情報エントロピー冗長性（g_{kt}）を計算します。

$$g_{kt} = 1 - e_{kt} \quad (7)$$

5. t 年における k 番目の指標（w_{kt}）を測定します。

$$w_{kt} = \frac{g_{kt}}{\sum_{k=1}^{m} g_{ut}} \quad (8)$$

6. 線形加重法を用いて，t 年における i 省の中国デジタル貿易発展レベルを計算します。

$$Digtal\ trade_{it} = \sum_{k=1}^{m} w_{kt} x^*_{ikt} \quad (9)$$

Table 10: Indicator system for digital trade development level

Overall indicator	Primary indicators	Secondary indicators
Level of digital trade development.	Digital ordering trade driven by industrial digitization.	Number of websites per hundred enterprises. Percentage of enterprises engaged in e-commerce transactions. E-commerce sales. E-commerce procurement volume. Online retail sales.
	Digital products, services and technology trade.	Total telecommunications business volume. Software business revenue. IT services revenue. Number of enterprises in the software and IT services sector. Number of manufacturing enterprises in the electronic information industry.

Control variables

1. Level of fiscal support: the ratio of local government general budget expenditures to regional GDP.
2. Economic development level: the natural logarithm of per capita regional GDP.
3. Industrial structure: the ratio of the value added by the tertiary sector to that of the secondary sector.
4. Social consumption level: the ratio of consumer goods retail sales to regional gross domestic product.
5. Conversion of scientific and technological achievements: the ratio of technology market transaction volume to regional GDP.
6. Population density: the total resident population at year-end divided by the region's area.
7. Level of foreign investment: the ratio of actual foreign direct investment to regional gross domestic product.
8. Level of informatization: the ratio of postal and telecommunications business volume to regional gross domestic product.
9. Level of financial development: the ratio of outstanding loans from financial institutions to regional gross domestic product.

表 10: デジタル貿易発展レベル指標システム

総合指標	主要指標	副次指標
デジタル貿易発展レベル	産業デジタル化によるデジタル注文貿易	企業100社当たりのウェブサイト数 電子商取引に従事する企業の割合 電子商取引売上高 電子商取引調達量 オンライン小売売上高
	デジタル製品，サービス，技術貿易	通信事業総取引量 ソフトウェア事業売上高 ITサービス売上高 ソフトウェア・ITサービス業の企業数 電子情報産業製造業の企業数

制御変数

1. 財政支援水準：地方政府一般予算支出の地域GDP比
2. 経済発展水準：一人当たり地域GDPの自然対数
3. 産業構造：第三次産業の付加価値の第二次産業の付加価値の比率
4. 社会消費水準：消費財小売売上高の地域GDP比
5. 科学技術成果の転換：技術市場取引高の地域GDP比
6. 人口密度：年末時点の総居住人口の地域面積比
7. 外国投資水準：実際の外国直接投資額の地域GDP比
8. 情報化レベル：郵便・通信事業の事業規模と地域GDPの比率
9. 金融発展レベル：金融機関からの融資残高と地域GDPの比率

Sample selection and data sources

The formal release in 2016 of China's GB/T 22080:2016, *Information Technology Security Techniques Information Security Management Systems Requirements* (the aforementioned recommended national standard adopted ISO/IEC 27001:2013 as equivalent), effectively promoted and standardized the development of an ISMS among listed companies within provincial jurisdictions. This report utilizes panel data from 30 Chinese provinces (excluding Tibet, Hong Kong, Macao, and Taiwan due to data collection constraints) spanning 2016-2023, to empirically examine the impact of ISO/IEC 27001 certification on the development levels of digital trade in Chinese provinces. The relevant indicator datasets are sourced from the China Statistical Yearbook, China Science and Technology Statistical Yearbook, China Software Industry Statistical Yearbook, and the National Certification and Accreditation Information Public Service Platform established by the State Administration for Market Regulation.

Descriptive statistics

Table 11 presents the results of descriptive statistics and correlation analysis. To verify the validity of variable selection, this report examined multicollinearity issues. The results indicate that the Variance Inflation Factor (VIF) for each variable is below 5, confirming the absence of multicollinearity among variables. The mean and standard deviation of digital trade development levels were 0.123 and 0.136, respectively. This indicates uneven development between provinces and significant variability in digital trade levels. The mean for ISO/IEC 27001 certification is 0.123, with a minimum of 0 and a maximum of 0.733. This reflects that the overall number of ISO/IEC 27001 certifications held by listed companies in provinces is still in its early stages, with considerable disparities remaining.

Table 11: Descriptive statistics and correlation analysis

Variable name	Sample size	Mean	Standard deviation	Minimum values	Maximum values	VIF
Digital trade	240	0.123	0.136	0.012	0.733	/
ISO/IEC 27001	240	1.473	1.413	0	5.226	3.47
Level of fiscal support	240	0.255	0.105	0.105	0.675	1.97
Economic development level	240	1.880	0.410	1.008	2.997	4.43
Industrial structure	240	1.527	0.797	0.755	5.690	2.46
Social consumption level	240	0.385	0.066	0.180	0.504	1.48
Conversion of scientific and technological achievements	240	0.025	0.035	0	0.195	2.76
Population density	240	0.048	0.072	0.001	0.395	2.09
Level of foreign investment	240	0.017	0.018	0	0.101	1.36
Level of informatization	240	0.070	0.062	0.015	0.290	1.17
Level of financial development	240	1.531	0.438	0.743	2.774	2.08

サンプル選択とデータソース

2016年に正式に発行された中国のGB/T 22080:2016 *情報技術 セキュリティ技術 情報セキュリティマネジメントシステム 要求事項*（前述の推奨国家規格はISO/IEC 27001:2013を同等規格として採用）は，省管轄区域内の上場企業におけるISMS（情報セキュリティマネジメントシステム）の発展を効果的に促進・標準化しました。本報告書では，2016年から2023年までの中国30省（データ収集上の制約によりチベット，香港，マカオ，台湾を除く）のパネルデータを用いて，ISO/IEC 27001認証が中国各省のデジタル貿易発展レベルに与える影響を実証的に検証します。関連する指標データセットは，中国統計年鑑，中国科学技術統計年鑑，中国ソフトウェア産業統計年鑑，および国家市場監督管理総局が設置した国家認証認可情報公共サービスプラットフォームから取得しました。

記述統計

表11は，記述統計と相関分析の結果を示しています。変数選択の妥当性を検証するため，本報告書では多重共線性の問題を検討しました。結果によると，各変数の分散膨張係数（VIF）は5未満であり，変数間の多重共線性は認められないことが確認されました。デジタル貿易発展レベルの平均値と標準偏差は，それぞれ0.123と0.136でした。これは，省間で発展にばらつきがあり，デジタル貿易レベルに大きな変動があることを示しています。ISO/IEC 27001認証の平均値は0.123で，最小値は0，最大値は0.733でした。これは，各省の上場企業におけるISO/IEC 27001認証取得件数が依然として初期段階にあり，大きな格差が存在することを示しています。

表 11: 記述統計と相関分析

変数名	サンプルサイズ	平均値	標準偏差	最小値	最大値	VIF
デジタル貿易	240	0.123	0.136	0.012	0.733	/
ISO/IEC 27001	240	1.473	1.413	0	5.226	3.47
財政支援レベル	240	0.255	0.105	0.105	0.675	1.97
経済発展レベル	240	1.880	0.410	1.008	2.997	4.43
産業構造	240	1.527	0.797	0.755	5.690	2.46
社会消費レベル	240	0.385	0.066	0.180	0.504	1.48
科学技術成果の転換	240	0.025	0.035	0	0.195	2.76
人口密度	240	0.048	0.072	0.001	0.395	2.09
外国投資レベル	240	0.017	0.018	0	0.101	1.36
情報化レベル	240	0.070	0.062	0.015	0.290	1.17
金融発展レベル	240	1.531	0.438	0.743	2.774	2.08

Overall analysis of the impact of ISO/IEC 27001 certification on digital trade in China

A dual machine learning model was employed to estimate the impact of ISO/IEC 27001 certification on the digital trade development levels in provinces. The sample was split in a 1:4 ratio, with both the main regression and auxiliary regression using random forest algorithms. Table 12 reports the estimation results.

Column (1) controls for time-fixed effects, province-fixed effects, and first-order terms of other control variables. To more comprehensively model the relationship between control variables and the dependent variable and enhance the accuracy of causal effect estimation, Column (2) further incorporates second-order terms of control variables. The regression coefficient is significantly positive at the 1% level. The results indicate that ISO/IEC 27001 certification significantly enhances the digital trade development level in provinces. Holding other conditions constant, a one-unit increase in ISO/IEC 27001 certification corresponds to a 0.031-unit increase in digital trade development. Columns (3) and (4) report the specific impacts of ISO/IEC 27001 certification on each dimension of digital trade development. Results show that ISO/IEC 27001 certification promotes digital ordering trade (0.033) and digital products, services and technology trade (0.028) in provinces, with a stronger effect on digital ordering trade.

Table 12: Baseline regression results

Variables	(1)	(2)	(3)	(4)
	Digital trade development level	Digital trade development level	Digital ordering trade	Digital products, services and technology trade
ISO/IEC 27001	0.025*** (4.77)	0.031*** (4.20)	0.033*** (5.04)	0.028*** (4.69)
Control variable single term	Yes	Yes	Yes	Yes
Control variable quadratic term	No	Yes	Yes	Yes
Provincial fixed effects	Yes	Yes	Yes	Yes
Year fixed effect	Yes	Yes	Yes	Yes
Sample size	240	240	240	240

Values in parentheses represent robust z-test values *** p<0.01, ** p<0.05, * p<0.1

中国におけるISO/IEC 27001認証がデジタル貿易に与える影響の総合分析

ISO/IEC 27001認証が各省のデジタル貿易発展水準に与える影響を推定するために，デュアル機械学習モデルが用いられました。サンプルは1:4の比率で分割され，主回帰と補助回帰の両方にランダムフォレストアルゴリズムが用いられました。表12に推定結果を示します。

I列(1)は，時間固定効果，省固定効果，およびその他の制御変数の一次項を制御しています。制御変数と従属変数の関係をより包括的にモデル化し，因果効果推定の精度を高めるため，列(2)では制御変数の二次項をさらに組み込んでいます。回帰係数は1%水準で有意に正の値を示しています。この結果は，ISO/IEC 27001認証が各省のデジタル貿易発展レベルを著しく向上させることを示しています。他の条件を一定とした場合，ISO/IEC 27001認証が1単位増加すると，デジタル貿易発展レベルは0.031単位増加します。列(3)と(4)は，ISO/IEC 27001認証がデジタル貿易発展の各側面に及ぼす具体的な影響を示しています。結果によると，ISO/IEC 27001認証は各省のデジタル注文貿易（0.033）とデジタル製品・サービス・技術貿易（0.028）を促進し，特にデジタル注文貿易への影響が強いことが示されています。

表 12: ベースライン回帰分析結果

変数	(1)	(2)	(3)	(4)
	デジタル貿易発展レベル	デジタル貿易発展レベル	デジタル注文貿易	デジタル製品，サービス，技術貿易
ISO/IEC 27001	0.025*** (4.77)	0.031*** (4.20)	0.033*** (5.04)	0.028*** (4.69)
制御変数（単項）	Yes	Yes	Yes	Yes
制御変数（二次項）	No	Yes	Yes	Yes
省固定効果	Yes	Yes	Yes	Yes
年次固定効果	Yes	Yes	Yes	Yes
サンプルサイズ	240	240	240	240

括弧内の数値はロバストz 検定値を示す *** p<0.01, ** p<0.05, * p<0.1

Comparative analysis of the impact of ISO/IEC 27001 certification among regions

Disparities in economic development levels

The level of economic development reflects a region's overall economic scale and growth rate. Differences in this broader environment may limit the effectiveness of ISO/IEC 27001 certification. To examine the impact of economic development on ISO/IEC 27001 certification, this report divides the sample into two subgroups based on the average per capita regional GDP (logarithm): provinces with high economic development and provinces with low economic development. The estimation results are shown in Column 1 and 2 of Table 13.

It is evident that ISO/IEC 27001 certification exerts a significant and positive promoting effect on the development of digital trade in both low and high economic development regions. Moreover, its promoting effect is substantially greater in provinces with high economic development than in provinces with low economic development. This demonstrates that the effectiveness of information security governance, exemplified by ISO/IEC 27001 certification, is strongly correlated with local economic development. As economic conditions improve, socioeconomic security risks become more complex, leading to increased emphasis on information security governance. Consequently, the promoting effect becomes more pronounced, boosting provincial digital trade development levels.

Geographical location differences

Geographical location-induced disparities in resource endowments are highly likely to influence the promoting effect of ISO/IEC 27001 certification on regional digital trade development levels. This report divides the sample into eastern, central and western regions based on three major economic belts, with estimation results presented in columns 3 to 5 of Table 13.

The findings indicate that ISO/IEC 27001 certification significantly enhances digital trade development in eastern and western regions, while exhibiting no significant effect on central regions. A possible explanation is that the eastern region benefits from its advantageous geographical location, abundant resources and well-developed cybersecurity infrastructure, enabling faster detection and resolution of service disruptions, ransomware attacks and information leaks, thereby significantly advancing regional digital trade development. By contrast, central and western regions grapple with inadequate digital infrastructure development, relatively lagging digital technology adoption, and weak support for development factors, particularly a severe shortage of high-end digital talent. In addition, the central region is located inland, not by the sea or along the border, and has a low degree of openness to the outside world, particularly a low level of service trade.[15] These constraints significantly diminish the promoting effect of ISO/IEC 27001 on regional digital trade development.

15 https://finance.sina.com.cn/jjxw/2025-03-14/doc-ineprcmk9753323.shtml.

地域間におけるISO/IEC 27001認証の影響に関する比較分析

経済発展レベルの格差

経済発展レベルは，地域の全体的な経済規模と成長率を反映しています。このような広範な環境の違いは，ISO/IEC 27001認証の有効性を制限する可能性があります。経済発展がISO/IEC 27001認証に与える影響を検証するため，本報告書ではサンプルを地域別一人当たりGDP（対数）の平均値に基づき，経済発展度の高い省と低い省の2つのサブグループに分けました。推定結果は表13の第1列と第2列に示されています。

ISO/IEC 27001認証は，経済発展度の低い地域と高い地域の両方において，デジタル貿易の発展に有意かつ肯定的な促進効果をもたらしていることが明らかになりました。さらに，その促進効果は経済発展度の高い省の方が低い省よりも著しく大きいことが分かりました。これは，ISO/IEC 27001認証に代表される情報セキュリティガバナンスの有効性が，地域経済の発展と強い相関関係にあることを示しています。経済状況が改善するにつれて，社会経済的な安全保障リスクはより複雑化し，情報セキュリティガバナンスへの重視度が高まります。その結果，促進効果がより顕著になり，各省のデジタル貿易発展レベルが向上します。

地理的差異

地理的な位置による資源賦存量の格差は，ISO/IEC 27001認証が地域デジタル貿易発展レベルに及ぼす促進効果に大きな影響を与える可能性が高いです。本報告書では，サンプルを3つの主要経済圏に基づき，東部，中部，西部の3地域に分け，推定結果を表13の第3～5列に示します。

調査結果によると，ISO/IEC 27001認証は東部および西部地域におけるデジタル貿易発展を著しく促進する一方，中部地域には有意な影響は与えていません。考えられる説明としては，東部地域は地理的に有利な位置，豊富な資源，高度に発達したサイバーセキュリティインフラの恩恵を受けており，サービス障害，ランサムウェア攻撃，情報漏洩の迅速な検知と解決が可能であるため，地域デジタル貿易発展が大きく促進されていることが挙げられます。対照的に，中部および西部地域は，デジタルインフラ整備の不十分さ，デジタル技術導入の遅れ，開発要因への支援の弱さ，特に高度なデジタル人材の深刻な不足といった課題を抱えています。さらに，中部地域は海沿いや国境沿いではなく内陸部に位置し，外部世界への開放度が低く，特にサービス貿易の水準が低いです。[15] これらの制約は，ISO/IEC 27001が地域デジタル貿易の発展に及ぼす促進効果を著しく低下させています。

15 https://finance.sina.com.cn/jjxw/2025-03-14/doc-ineprcmk9753323.shtml.

Table 13: Sub-group analysis results

Variables	(1)	(2)	(3)	(4)	(5)
	Provinces with high economic development	Provinces with low economic development	Eastern region	Central region	Western region
ISO/IEC 27001	0.038*** (4.56)	0.011*** (2.83)	0.066*** (6.94)	0.002 (0.61)	0.012** (2.46)
Control variable single term	Yes	Yes	Yes	Yes	Yes
Control variable quadratic term	Yes	Yes	Yes	Yes	Yes
Time-fixed effect	Yes	Yes	Yes	Yes	Yes
Provincial fixed Effects	Yes	Yes	Yes	Yes	Yes
Sample size	106	134	88	64	88

Values in parentheses represent robust z-test values *** p<0.01, ** p<0.05, * p<0.1

Conclusions and policy recommendations

Conclusions

This report employs provincial panel data from 2016 to 2023 to measure the level of digital trade development in China's 30 provinces (excluding Tibet and the Hong Kong, Macao and Taiwan regions). By constructing a dual machine learning model, it empirically examines the impact of ISO/IEC 27001 certification on digital trade development in Chinese provinces, yielding the following conclusions. Firstly, ISO/IEC 27001 certification exerts a significant promoting effect on digital trade development in Chinese provinces. Secondly, the promoting effect exhibits heterogeneous characteristics: compared to provinces with low economic development, ISO/IEC 27001 certification primarily drives the digital trade development in provinces with high economic development. ISO/IEC 27001 certification has demonstrated more pronounced effectiveness in enhancing digital trade development in eastern and western China. In central China, however, its promoting impact on digital trade development has yet to materialize, potentially owing to insufficient levels of opening-up and other related issues.

Policy recommendations

Firstly, the international standards organizations should promote widespread adoption of ISO/IEC 27001 by enterprises. China's practice has proven that ISO/IEC 27001 is conducive to promoting digital trade. International standards organizations should vigorously promote the role of ISO/IEC 27001 and its certification in promoting digital trade, such as reducing trade costs and enhancing trust. This helps to encourage enterprises to view ISO/IEC 27001 as a key factor in strengthening ISMS and enhancing digital trade.

Secondly, governments should consider ISO/IEC 27001 and its certification as a catalyst for digital trade. ISO/IEC 27001 can address the cyber-risks and digital technology risks faced by enterprises during digital trade operations. Governments, especially those at all levels in central China and lower economic development provinces, should accelerate the development of a certification system tailored to local enterprises' information management needs. This ensures enterprises in these provinces take information security management seriously, enabling them to adapt to the new development landscape driven by the digital trade wave.

表 13: サブグループ分析結果

変数	(1)	(2)	(3)	(4)	(5)
	経済発展度の高い省	経済発展度の低い省	東部地域	中部地域	西部地域
ISO/IEC 27001	0.038*** (4.56)	0.011*** (2.83)	0.066*** (6.94)	0.002 (0.61)	0.012** (2.46)
制御変数(単項)	Yes	Yes	Yes	Yes	Yes
制御変数(二次項)	Yes	Yes	Yes	Yes	Yes
年次固定効果	Yes	Yes	Yes	Yes	Yes
省固定効果	Yes	Yes	Yes	Yes	Yes
サンプルサイズ	106	134	88	64	88

括弧内の数値はロバストz 検定値を示す。*** p<0.01, ** p<0.05, * p<0.1

結論と政策提言

結論

本報告書は，2016年から2023年までの省レベルのパネルデータを用いて，中国の30省(チベット自治区，香港，マカオ，台湾を除く)におけるデジタル貿易の発展レベルを測定しています。デュアル機械学習モデルを構築することで，ISO/IEC 27001認証が中国の各省におけるデジタル貿易の発展に与える影響を実証的に分析し，以下の結論を得ました。第一に，ISO/IEC 27001認証は中国の各省におけるデジタル貿易の発展に顕著な促進効果をもたらしています。第二に，その促進効果は地域によって異なり，経済発展の低い省と比較して，経済発展の高い省では主にデジタル貿易の発展を促進しています。ISO/IEC 27001認証は，中国東部および西部においてデジタル貿易の発展を促進する上でより顕著な効果を示しています。しかしながら，中国中部では，開放レベルの不足やその他の関連問題が原因で，デジタル貿易の発展に対する促進効果はまだ顕在化していません。

政策提言

第一に，国際規格団体は，企業によるISO/IEC 27001の普及を促進すべきです。中国の事例は，ISO/IEC 27001がデジタル貿易の促進に有効であることを証明しています。国際規格団体は，貿易コストの削減や信頼性の向上など，デジタル貿易促進におけるISO/IEC 27001とその認証の役割を積極的に推進すべきです。これにより，企業はISO/IEC 27001を情報セキュリティマネジメントシステム(ISMS)の強化とデジタル貿易の促進における重要な要素として認識するようになるでしょう。

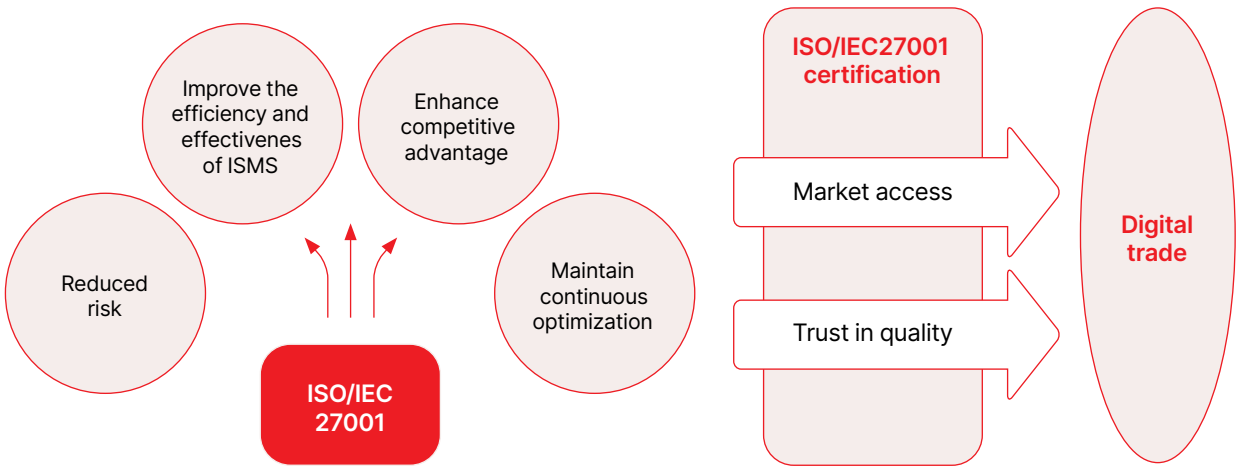
第二に，政府はISO/IEC 27001とその認証をデジタル貿易の触媒として捉えるべきです。ISO/IEC 27001は，企業がデジタル貿易業務において直面するサイバーリスクやデジタル技術リスクに対処することができます。政府，特に中国中部および経済発展の遅れた省の各級政府は，地元企業の情報管理ニーズに合わせた認証制度の開発を加速させるべきです。これにより，これらの省の企業は情報セキュリティ管理を真剣に取り組み，デジタル貿易の波によってもたらされる新たな発展環境に適応できるようになります。

4. ISO/IEC 27001 certification and digital trade: Enterprise level

Research at national and international levels has confirmed that ISO/IEC 27001 certification promotes the growth of digital trade, but the corporate-level mechanisms underpinning this relationship require further exploration.

Two Chinese enterprises were selected as case studies for this exercise, based on criteria of typicality, relevance and data availability – H3C and DPtech. The in-depth analysis included interviewing corporate executives and collecting secondary materials, such as annual reports and official website reports of the enterprise to obtain relevant information on ISO/IEC 27001 and its certification for those case companies. This section systematically sorts out the reasons, processes and effects of enterprises applying for ISO/IEC 27001 certification. Finally, the impact mechanisms of ISO/IEC 27001 and its certification on digital trade are identified, as shown in Figure 9.

Figure 9: The impact mechanisms of ISO/IEC 27001 and its certification on digital trade

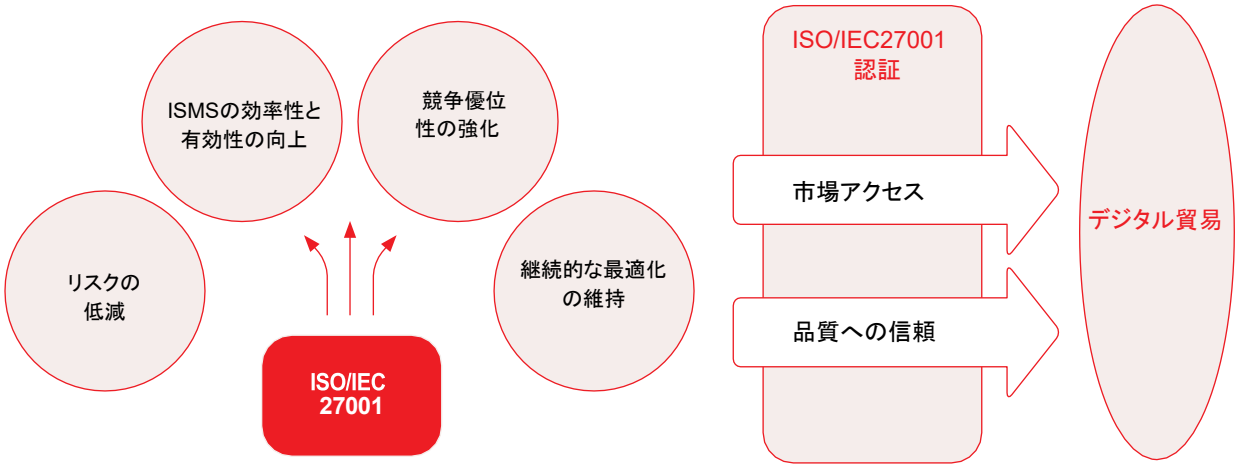


4. ISO/IEC 27001認証とデジタル貿易：企業レベル

国内外の研究により，ISO/IEC 27001認証がデジタル貿易の成長を促進することが確認されていますが，この関係を支える企業レベルのメカニズムについては，さらなる調査が必要です。

本調査では，代表性，関連性，データ入手可能性という基準に基づき，中国の2社（H3CとDPtech）をケーススタディとして選定しました。詳細な分析では，企業幹部へのインタビューに加え，年次報告書や公式ウェブサイトの報告書などの二次資料を収集し，ISO/IEC 27001とその認証に関する関連情報を収集しました。本節では，企業がISO/IEC 27001認証を申請する理由，プロセス，効果を体系的に整理します。最後に，図9に示すように，ISO/IEC 27001とその認証がデジタル貿易に及ぼす影響メカニズムを明らかにします。

図 9: ISO/IEC 27001とその認証がデジタル貿易に及ぼす影響メカニズム



The case of H3C Technologies Co., Ltd.

H3C is a core digital solutions provider under the New Tsinghua Holdings Group. Headquartered in Hangzhou, it was established in 2003. The company focuses on full-stack ICT infrastructure including cloud computing, AI and industrial internet. It offers one-stop digital technology services and maintains market leadership in areas such as intelligent connectivity and smart computing. As a core participant in digital transformation, H3C has ranked first in China's network management software market for seven consecutive years.[16] In 2024, the Ministry of Industry and Information Technology awarded it First Prize for Digital Economy Innovation Achievements for its Intelligent Computing Edition Digital Brain solution.

H3C stays at the industry forefront in product innovation. Its upgraded Lingsi Intelligent Computing Solution in 2025, featuring the high-density deployment of 64 cards per cabinet to support trillion-parameter model training, has become a benchmark for AI computing infrastructure. Strategically, H3C achieves in-depth local development and global expansion. In China, it has established nine major bases, nine industrial centres and more than 50 sales and service organizations nationwide, enabling rapid response to demand and creating quality services for customers and ecosystem partners. In overseas markets, it has set up 17 branches throughout Africa, Asia, Europe and Latin America, with products available in nearly 100 countries and services covering 176 countries, supporting the overseas digital transformation of Chinese-funded enterprises. Upholding its vision of "enabling an intelligent world where everything is connected", H3C is driving global digitalization towards greater efficiency, security and inclusiveness through continuous innovation.

Drivers behind H3C's ISO/IEC 27001 certification

Market access needs: Meeting bidding and international market requirements

Meeting the needs of domestic and international market access stands as a primary driver for H3C's certification. In the domestic market, especially in key sectors such as government, finance and telecommunications, ISO/IEC 27001 certification has become an indispensable prerequisite for participating in bidding. Without this certification, H3C would face significant obstacles in securing major projects. Many customers not only regard the certification as a mandatory qualification for equipment procurement, but also integrate it directly into their bid evaluation systems. Interviewees confirmed this. One interviewee said: "The initial certification was primarily driven by market demand. Essentially, the certification is for bidding needs, to enhance competitiveness in bidding." They elaborated: "We participate in bidding for projects involving network equipment, security devices, servers and related items. Purchasers in this field typically require fundamental credentials related to information security, along with items such as proof of sales qualification and software copyrights. ISO/IEC 27001 certification is essentially a prerequisite – a threshold requirement. Without this certification, entry into many market projects would be impossible."

In the international market, as global information security regulations become increasingly stringent, enterprises operating internationally must adhere to multi-jurisdictional mandates, including the EU GDPR and China's Cybersecurity Law. To support overseas business expansion and meet local data protection requirements, H3C must take proactive measures to leverage the certification. An interviewee stated: "We have foreign business, so we also need to comply with the EU GDPR, relevant regulations in some South-East Asian and South American countries, and conduct business

16 Based on IDC data: China Quarterly IT Services Tracker

H3C Technologies Co., Ltd. の事例

H3Cは，新清華控股集団傘下のコアデジタルソリューションプロバイダーです。杭州に本社を置き，2003年に設立されました。クラウドコンピューティング，AI，産業用インターネットを含むフルスタックICTインフラストラクチャに注力しています。ワンストップのデジタルテクノロジーサービスを提供し，インテリジェントコネクティビティやスマートコンピューティングなどの分野で市場をリードしています。デジタル変革の中核を担う企業として，H3Cは中国のネットワーク管理ソフトウェア市場で7年連続1位を獲得しています。[16] 2024年には，インテリジェントコンピューティング版デジタルブレインソリューションで，工業情報化部からデジタル経済イノベーション成果賞一等賞を受賞しました。

H3Cは製品イノベーションにおいて業界の最先端を走り続けています。2025年に発表されたアップグレード版「霊思（Lingsi）インテリジェントコンピューティングソリューション」は，1キャビネットあたり64枚のカードを高密度に搭載し，数兆パラメータのモデルトレーニングをサポートするという特長を持ち，AIコンピューティングインフラストラクチャのベンチマークとなっています。戦略的に，H3Cは地域に根ざした開発とグローバル展開を両立させています。中国国内では，9つの主要拠点，9つの産業センター，そして全国に50以上の販売・サービス拠点を設立し，顧客とエコシステムパートナーへの迅速な対応と質の高いサービス提供を実現しています。海外市場では，アフリカ，アジア，ヨーロッパ，ラテンアメリカに17の支社を設立し，約100カ国で製品を提供，176カ国でサービスを展開し，中国資本企業の海外デジタル変革を支援しています。「すべてがつながるインテリジェントな世界を実現する」というビジョンを掲げ，H3Cは継続的なイノベーションを通じて，グローバルなデジタル化をより高い効率性，安全性，そして包摂性へと推進しています。

H3CのISO/IEC 27001認証取得の動機

市場参入ニーズ：入札および国際市場要件への対応

Meeti H3Cの認証取得の主な動機は，国内外市場への参入ニーズへの対応です。国内市場，特に政府，金融，通信などの主要セクターでは，ISO/IEC 27001認証は入札参加に不可欠な前提条件となっています。この認証がなければ，H3Cは大型プロジェクトの受注において大きな障害に直面することになります。多くの顧客は，この認証を機器調達の必須条件とみなすだけでなく，入札評価システムに直接組み込んでいます。インタビュー対象者もこれを認めています。あるインタビュー対象者は，「最初の認証取得は主に市場ニーズによるものでした。本質的に，この認証は入札における競争力強化のためのものです」と述べています。彼らはさらに詳しく説明しました。「当社はネットワーク機器，セキュリティ機器，サーバー，および関連製品を含むプロジェクトの入札に参加しています。この分野の購入者は通常，情報セキュリティに関する基本的な資格に加え，販売実績やソフトウェアの著作権証明などの書類を求めます。ISO/IEC 27001認証は事実上必須条件であり，最低限の要件です。この認証がなければ，多くの市場プロジェクトへの参入は不可能でしょう。」

国際市場において，グローバルな情報セキュリティ規制がますます厳格化するにつれ，国際的に事業を展開する企業は，EU一般データ保護規則（GDPR）や中国のサイバーセキュリティ法など，複数の法域にわたる規制を遵守しなければなりません。海外事業の拡大を支援し，現地のデータ保護要件を満たすため，H3Cは認証を活用するための積極的な対策を講じる必要があります。あるインタビュー対象者は，「当社は海外事業を展開しているため，EU GDPR，東南アジアおよび南米諸国の関連規制を遵守し，法令に準拠した事業運営を行う必要があります」と述べました。これに関

16　IDCデータに基づく：中国四半期ITサービストラッカー

in compliance." Corresponding to this, they added: "We have uploaded the English version of ISO/IEC 27001 certification on the official English website of the group for overseas customers to view." This further reflects the certification's role in facilitating compliance with local market requirements.

Internal management needs: Validating existing security system effectiveness

Evaluating and improving the effectiveness of its internal ISMS is a core objective of H3C's certification. As the company expands its global operations, internal information flows have become increasingly complex, necessitating efficient and secure management mechanisms. Unlike newly established or small enterprises that rely on certification to build security systems from scratch, H3C already has a solid foundation in information security.

For H3C, the ISO/IEC 27001 certification process serves as a third-party validation of its existing security framework rather than a ground-up construction. The certification requirements help clarify departmental responsibilities, standardize information processes and promote secure information circulation. Interviewees emphasized this distinction. One said: "H3C already had a strong foundation in information security. The main purpose of implementing ISO/IEC 27001 certification for H3C is to enable third-party organizations to evaluate the effectiveness of the company's existing system. H3C does not rely on third-party assistance to establish a new security system. This differs from the situation of new or small companies." They further noted: "H3C has actually implemented many standards, not relying solely on ISO/IEC 27001 to build the system. For us, ISO/IEC 27001, like national laws and regulations, is a bottom-line requirement. If we only meet the bottom line, we cannot manage safety well. Our goals are far higher than the bottom line."

H3C's ISO/IEC 27001 certification status

H3C has obtained ISO/IEC 27001 Information Security Management System certification and holds five Level 3 Cybersecurity Protection Certification systems, undergoing annual re-evaluation as required by cybersecurity authorities. The company strictly adheres to Chinese laws and regulations while also complying with the EU GDPR and relevant laws in South-East Asia and South America for its overseas operations, ensuring globally compliant cross-border business activities. H3C's ISO/IEC 27001 certification covers all business operations and product lines, not limited to specific departments or individual services. For international adaptation, the global applicability of ISO standards enhances the certification's value. The company specifically selected a Norwegian certification body operating in China to issue the certificate, thereby strengthening its international credibility. To meet regional requirements, H3C has established an English section on its official website to display English certificates. For regions like Italy that place greater emphasis on TÜV qualifications, H3C prioritizes collaboration with joint-venture certification bodies to ensure the certificates' validity and recognition worldwide.

Additionally, H3C has established a dedicated information security department to handle daily operations and formed a cross-departmental information security task force covering all first-level departments. At the strategic level, the "President's Office Meeting" determines information security strategies, annual priorities and resource allocation, forming a top-down management model. Core protection targets primarily include technical information and operational information. Technical information encompasses core technical assets, such as code and R&D materials, while operational information covers sensitive business data, including annual financial reports, compensation information, customer data and product pricing. In terms of information security management direction, technical protection focuses on defending against various cyberattacks. With the adoption of cloud computing, Software as a Service

連して，彼らはさらに，「海外のお客様が閲覧できるよう，ISO/IEC 27001認証の英語版をグループの公式英語ウェブサイトに掲載しています」と付け加えました。これは，認証が現地市場の要件への準拠を促進する役割をさらに明確に示しています。

内部管理ニーズ：既存セキュリティシステムの有効性の検証

H3Cの認証取得における主要な目的は，社内ISMSの有効性を評価し，改善することです。グローバル事業の拡大に伴い，社内情報フローはますます複雑化し，効率的かつ安全な管理メカニズムが不可欠となっています。セキュリティシステムをゼロから構築するために認証に頼る新規設立企業や小規模企業とは異なり，H3Cは既に情報セキュリティにおいて強固な基盤を有しています。

H3Cにとって，ISO/IEC 27001認証プロセスは，セキュリティフレームワークをゼロから構築するのではなく，既存のセキュリティフレームワークを第三者機関が検証する役割を果たします。認証要件は，部門の責任を明確化し，情報プロセスを標準化し，安全な情報流通を促進するのに役立ちます。インタビュー対象者は，この点を強調しました。ある担当者は，「H3Cは既に情報セキュリティにおいて強固な基盤を築いていました。H3CがISO/IEC 27001認証を取得する主な目的は，第三者機関が当社の既存システムの有効性を評価できるようにすることです。H3Cは，新たなセキュリティシステムの構築に第三者機関の支援を必要としません。これは，新規企業や小規模企業とは異なります」と述べました。さらに，「H3Cは，システム構築においてISO/IEC 27001だけに頼るのではなく，実際には多くの規格を導入してきました。当社にとって，ISO/IEC 27001は，国内法規と同様に，最低限の要件です。最低限の要件を満たすだけでは，安全管理を適切に行うことはできません。当社の目標は，最低限の要件をはるかに超えたところにあります」と付け加えました。

H3CのISO/IEC 27001認証取得状況

H3Cは，ISO/IEC 27001情報セキュリティマネジメントシステム認証を取得しており，サイバーセキュリティ当局の要求に基づき毎年再評価を受けているレベル3サイバーセキュリティ保護認証システムを5つ保有しています。当社は中国の法令を厳格に遵守するとともに，海外事業においてはEU一般データ保護規則（GDPR）および東南アジア・南米の関連法規にも準拠し，グローバルな法令遵守に基づいた国境を越えた事業活動を実現しています。H3CのISO/IEC 27001認証は，特定の部門や個々のサービスに限定されず，すべての事業活動および製品ラインを対象としています。国際的な適応性という観点から，ISO規格のグローバルな適用性は認証の価値を高めています。当社は，認証発行機関として中国で事業を展開するノルウェーの認証機関を選定し，国際的な信頼性を強化しています。地域的な要件を満たすため，H3Cは公式ウェブサイトに英語セクションを設け，英語の認証情報を掲載しています。イタリアのようにTÜV認証を重視する地域においては，H3Cは認証機関との合弁事業による連携を優先し，認証の有効性と世界的な認知度を確保しています。

さらに，H3Cは日常業務を担う情報セキュリティ専門部署を設置し，すべての第一線部門を網羅する部門横断的な情報セキュリティタスクフォースを編成しました。戦略レベルでは，「社長会議」において情報セキュリティ戦略，年間優先事項，リソース配分を決定し，トップダウン型の経営モデルを構築しています。主要な保護対象は，主に技術情報と運用情報です。技術情報には，コードや研究開発資料などのコア技術資産が含まれ，運用情報には，年次財務報告書，報酬情報，顧客データ，製品価格などの機密性の高いビジネスデータが含まれます。情報セキュリティ管理の方向性としては，技術保護は様々なサイバー攻撃への防御に重点を置いています。クラウドコンピューティング，SaaS（Software as a Service），AI技術の導入に伴い，AIを活用した運

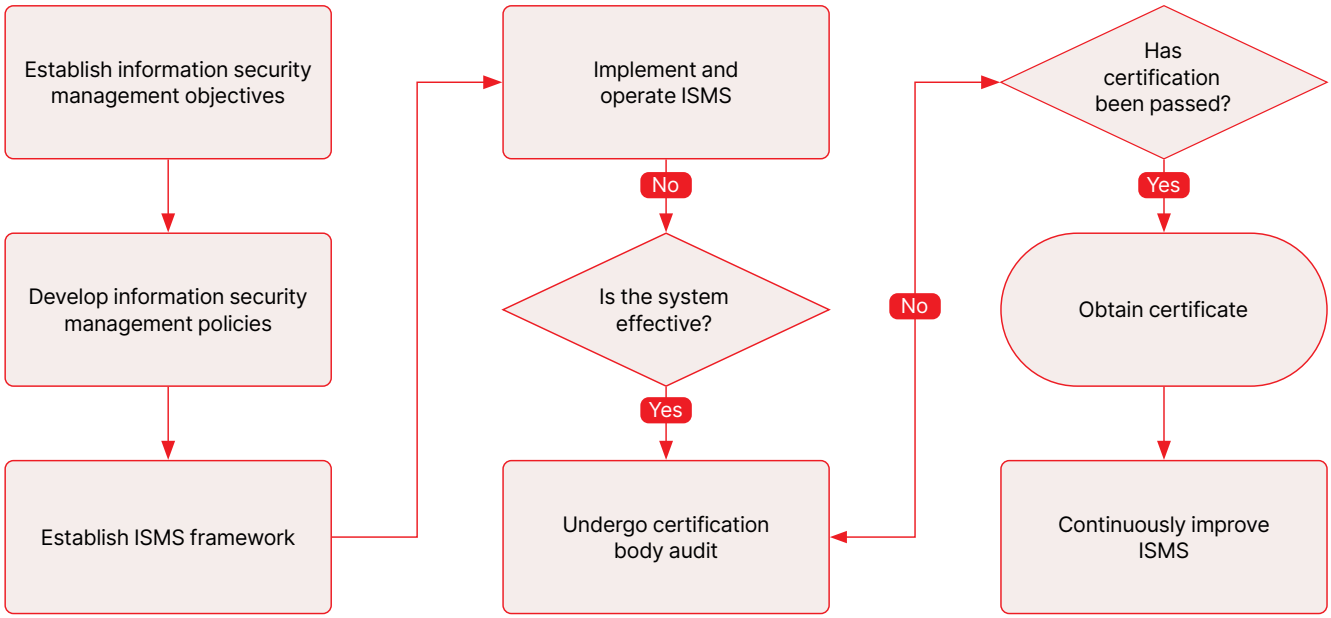
(SaaS) and AI technologies, emerging security techniques like AI-powered operations and AI monitoring/protection are progressively replacing traditional manual data centre management models, achieving collaborative defense through "human+technology" integration. Management measures involve establishing comprehensive policies to regulate employee conduct, balancing business growth with security controls. For instance, explicit operational rules govern employee password management and device access permissions.

H3C systematically advanced its ISMS certification in accordance with the ISO/IEC 27001 standard (see Figure 10). The process began by defining the certification scope, encompassing core business operations and information systems throughout headquarters and global branches, while identifying and classifying information assets including hardware, software, data and intellectual property. Subsequently, a comprehensive assessment evaluated potential threats and vulnerabilities in cybersecurity, data protection and personnel management domains, providing quantitative analysis to inform countermeasures development.

Based on the assessment results, H3C developed an integrated strategy encompassing physical, network, data and personnel security, closely aligned with corporate strategy. The company established a comprehensive ISMS framework and documentation system, clearly defining security responsibilities for each department and position. During implementation, security levels and operational efficiency were continuously enhanced through company-wide training and regular system inspections.

To validate the effectiveness of the system, H3C regularly conducts internal audits and management reviews, promptly addressing identified issues. After the system matured, the company successfully passed a third-party on-site audit and obtained ISO/IEC 27001 certification. Since then, H3C has continuously optimized its ISMS, actively addressing security challenges posed by emerging technologies, such as cloud computing and big data, thereby providing robust safeguards for digital transformation.

Figure 10: H3C ISO/IEC 27001 certification process



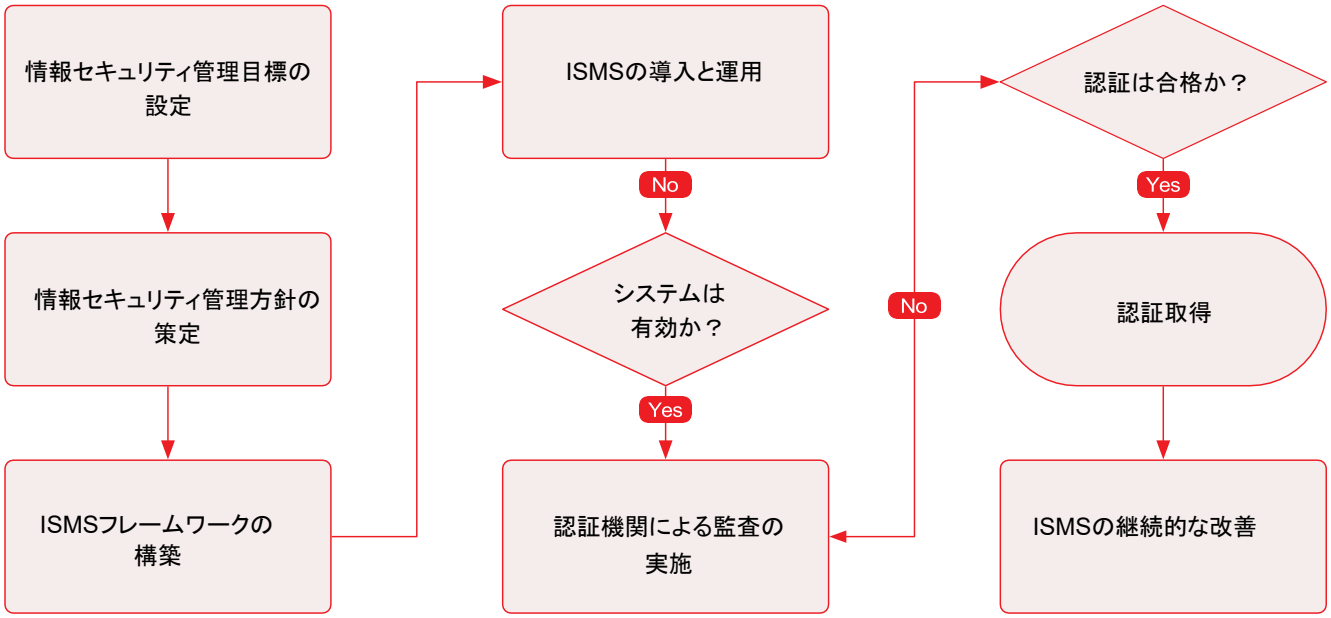
用やAIによる監視・保護といった新たなセキュリティ技術が，従来の手動によるデータセンター管理モデルに徐々に取って代わり，「人間＋テクノロジー」の統合による協調的な防御を実現しています。経営管理策には，従業員の行動を規制するための包括的なポリシーの策定，事業成長とセキュリティ管理のバランスのとれた取り組みが含まれます。例えば，従業員のパスワード管理やデバイスへのアクセス権限は，明確な運用ルールによって規定されています。

H3Cは，ISO/IEC 27001規格に準拠し，ISMS認証を体系的に取得しました（図10参照）。認証プロセスは，本社およびグローバル支店全体のコアビジネスオペレーションと情報システムを網羅する認証範囲の定義から始まり，ハードウェア，ソフトウェア，データ，知的財産などの情報資産を特定・分類しました。続いて，サイバーセキュリティ，データ保護，人事管理の各領域における潜在的な脅威と脆弱性を包括的に評価し，対策策定のための定量分析を行いました。

評価結果に基づき，H3Cは企業戦略と密接に連携した，物理的セキュリティ，ネットワークセキュリティ，データセキュリティ，人事セキュリティを網羅する統合戦略を策定しました。包括的なISMSフレームワークと文書化システムを構築し，各部門および役職におけるセキュリティ責任を明確に定義しました。導入期間中は，全社的な研修と定期的なシステム検査を通じて，セキュリティレベルと運用効率を継続的に向上させました。

システムの有効性を検証するため，H3Cは定期的に内部監査とマネジメントレビューを実施し，特定された問題に迅速に対応しています。システムが成熟した後，同社は第三者機関によるオンサイト監査に合格し，ISO/IEC 27001認証を取得しました。それ以来，H3CはISMSを継続的に最適化し，クラウドコンピューティングやビッグデータといった新興技術がもたらすセキュリティ上の課題に積極的に取り組み，デジタルトランスフォーメーションのための強固な保護策を提供しています。

図 10: H3CのISO/IEC 27001認証プロセス



Effectiveness of H3C's ISO/IEC 27001 certification

Market access enhancement: Forging a global trust passport

ISO/IEC 27001 certification has become a "passport" for H3C to break through international market barriers, with its global recognition effectively strengthening trust among overseas customers. Beyond serving as a bidding and compliance tool, the certification translates into tangible competitive advantages by reinforcing H3C's credibility in the global marketplace.

To maximize the certification's value, H3C has adopted supporting measures such as introducing proprietary high-performance business processing chips, dedicated core software systems, and partnering with internationally renowned security organizations and manufacturers like Microsoft, Kaspersky and Commtouch to deliver comprehensive, reliable and stable security protection solutions. The company also prioritizes certification from joint venture institutions to ensure broader international acceptance. An interviewee explained: "The ISO/IEC 27001 is internationally recognized. In theory, after obtaining certification, as long as the certificate is recognized, it can be used abroad." They added: "H3C usually seeks ISO/IEC 27001 certification from joint venture institutions, as foreign clients recognize certificates issued by overseas institutions and joint venture institutions." Ultimately, the trust transmitted by the certification is continuously converted into business growth momentum for H3C globally.

Internal management optimization: Boosting operational efficiency

The certification has optimized H3C's internal management model by serving as a baseline for information security compliance, helping the company systematically identify and address vulnerabilities in its security protection framework. More importantly, it provides a robust justification for advancing internal information security initiatives, effectively balancing the tension between security controls and business development. This has significantly reduced internal implementation resistance and operational costs.

As one interviewee noted: "ISO/IEC 27001 certification helps us systematically identify and address gaps while strengthening weak areas. At the same time, it provides a basis for advancing information security work. When promoting security controls, resistance is inevitable, especially when security conflicts with business operations. Having the support of laws, regulations and compliance certifications significantly reduces the difficulty of internal implementation. So, the biggest help of ISO/IEC 27001 and other system certifications is to enable us to better promote information security work and implement control requirements internally." The interviewee added that for enterprises with weak foundations, the certification can also assist in conducting risk analysis, process monitoring and resolving other management issues, which remains valuable. Additionally, the certification clarifies cross-departmental security responsibilities, facilitating secure information sharing on cross-departmental projects and laying a solid foundation for efficient project advancement.

H3CのISO/IEC 27001認証の有効性

市場アクセスの強化：グローバルな信頼のパスポートの構築

ISO/IEC 27001認証は，H3Cにとって国際市場への進出における「パスポート」となり，その世界的な認知度は海外顧客からの信頼を効果的に強化しています。入札やコンプライアンスツールとしての役割にとどまらず，この認証はH3Cのグローバル市場における信頼性を高めることで，具体的な競争優位性へと繋がっています。

認証の価値を最大限に引き出すため，H3Cは独自の高性能ビジネス処理チップや専用コアソフトウェアシステムの導入，Microsoft，Kaspersky，Commtouchといった国際的に著名なセキュリティ企業やメーカーとの提携など，包括的な信頼性と安定性を備えたセキュリティ保護ソリューションを提供するための様々な施策を講じています。また，国際的な認知度を高めるため，合弁機関からの認証取得も優先的に行っています。あるインタビュー対象者は，「ISO/IEC 27001は国際的に認知されています。理論的には，認証を取得すれば，その認証が認められる限り，海外でも使用できます」と述べています。彼らはさらに，「H3Cは通常，合弁機関からISO/IEC 27001認証を取得しています。これは，海外の顧客が海外機関や合弁機関が発行する認証を高く評価しているためです」と述べました。最終的に，この認証によって得られる信頼は，H3Cのグローバルな事業成長の原動力へと継続的に転換されています。

内部管理の最適化：業務効率の向上

この認証は，情報セキュリティコンプライアンスの基準として機能し，H3Cの内部管理モデルを最適化しました。これにより，同社はセキュリティ保護フレームワークにおける脆弱性を体系的に特定し，対処することが可能になりました。さらに重要なのは，内部情報セキュリティイニシアチブを推進するための強力な根拠を提供し，セキュリティ管理と事業開発の間の緊張関係を効果的にバランスさせることです。これにより，内部における導入抵抗と運用コストが大幅に削減されました。

あるインタビュー対象者は次のように述べています。「ISO/IEC 27001認証は，弱点を体系的に特定し，対処するとともに，弱点を強化するのに役立ちます。同時に，情報セキュリティ活動を推進するための基盤となります。セキュリティ対策を推進する際には，特にセキュリティと業務運営が衝突する場合，抵抗は避けられません。法律，規制，コンプライアンス認証の支援があれば，社内での導入の難しさは大幅に軽減されます。したがって，ISO/IEC 27001をはじめとするシステム認証の最大のメリットは，情報セキュリティ活動をより効果的に推進し，社内で管理要件を実装できるようになることです。」このインタビュー対象者はさらに，基盤が弱い企業にとって，認証はリスク分析，プロセス監視，その他の管理課題の解決にも役立ち，依然として価値があると付け加えました。加えて，認証は部門横断的なセキュリティ責任を明確化し，部門横断的なプロジェクトにおける安全な情報共有を促進し，効率的なプロジェクト推進のための強固な基盤を築きます。

Business development upgrade: Expanding high-value security consulting services

The certification has empowered H3C to expand its business boundaries by leveraging its accumulated security expertise to offer high-value security consulting services. With nearly two decades of experience in cybersecurity, H3C has integrated Hewlett Packard Enterprise Company's professional consulting team and experience to build mature methodologies, advanced tools and a team of seasoned security consulting specialists.

As a leading vendor with a comprehensive ICT product portfolio, H3C boasts experts throughout networking, back-up storage, disaster recovery, applications and middleware – beyond security technical advisers. This enables it to deliver integrated consulting services covering network, cloud, mobile, application, data, and IoT security. The certification has created new cooperation opportunities in this area, as one interviewee explained: "Our company's service department actually assists clients in establishing management systems. For example, the technical services department helps clients build system frameworks for ISO Standards and domestic standards. This also represents a valuable cooperation opportunity brought about by certification."

The case of Hangzhou DPtech Technologies Co., Ltd.

DPtech is a leading enterprise in China's full-scenario cybersecurity sector and was listed on the ChiNext board of the Shenzhen Stock Exchange in April 2019. DPtech embarked on its ISO/IEC 27001 information security management system certification journey in 2015. The company consistently upholds its mission of "making networks simpler, smarter and more secure", focusing on core domains including cybersecurity, data security, industrial control security and application delivery. After more than a decade of dedicated development, the company has established a service network spanning critical industries, including government, telecommunications, power and energy, finance and public security, becoming a vital security force in the digital transformation of various sectors. In 2024, the company delivered outstanding operational performance, achieving operating revenue of RMB 11.548 billion, a year-on-year increase of 11.68%. Net profit attributable to shareholders of the listed company reached RMB 1.612 billion, a 27.26% year-on-year increase. Net cash flow from operating activities amounted to RMB 3.282 billion, surging 160.69% year-on-year. The company demonstrated high-quality development in scale expansion and profitability, showcasing its competitive resilience and growth potential within the cybersecurity industry.

Drivers behind DPtech's ISO/IEC 27001 certification

Market access needs: Meeting bidding requirements and international market requirements

Fulfilling market access needs is a core driver for DPtech's certification. As a company deeply engaged with the cybersecurity industry, DPtech's primary clients are concentrated in critical sectors such as government, telecommunications, finance and power/energy. In bidding for high-value projects in these industries, clients not only assess product performance but also attach great importance to suppliers' own security management and service guarantee capabilities. Developed international markets, in particular, impose extremely strict and complex compliance requirements on information security management, such as the Cybersecurity Law and the Data Security Law. ISO/IEC 27001 certification, as an internationally recognized information security management standard, has become a mandatory prerequisite for market access. As one interviewee stated: "In project bidding, many leading enterprises and operators require us to obtain ISO/IEC 27001 certification. To meet international market requirements, and comply with domestic and foreign regulations, DPtech has obtained ISO/IEC 27001 certification for the sales of network security products related to overseas markets."

事業展開の強化：高付加価値セキュリティコンサルティングサービスの拡充

H3Cは，今回の認証取得により，長年培ってきたセキュリティ専門知識を活かし，高付加価値セキュリティコンサルティングサービスを提供することで，事業領域を拡大することができました。サイバーセキュリティ分野で20年近い経験を持つH3Cは，ヒューレット・パッカード・エンタープライズ（HPE）の専門コンサルティングチームと経験を統合し，成熟した手法，高度なツール，そして経験豊富なセキュリティコンサルティングスペシャリストチームを構築しました。

包括的なICT製品ポートフォリオを持つリーディングベンダーとして，H3Cはセキュリティ技術アドバイザーだけでなく，ネットワーク，バックアップストレージ，災害復旧，アプリケーション，ミドルウェアなど，あらゆる分野の専門家を擁しています。これにより，ネットワーク，クラウド，モバイル，アプリケーション，データ，IoTセキュリティを網羅する統合コンサルティングサービスを提供することが可能となっています。今回の認証取得は，この分野における新たな協力機会を生み出しました。あるインタビュー対象者は次のように述べています。「当社のサービス部門は，顧客の管理システム構築を支援しています。例えば，技術サービス部門は，ISO規格や国内規格に準拠したシステムフレームワークの構築を支援しています。これは，今回の認証取得によってもたらされた貴重な協力機会の一つです。」

杭州 DPtech Technologies Co., Ltd.の事例

DPtechは，中国のフルシナリオサイバーセキュリティ分野をリードする企業であり，2019年4月に深圳証券取引所のChiNext市場に上場しました。DPtechは2015年にISO/IEC 27001情報セキュリティマネジメントシステム認証の取得に着手しました。同社は，サイバーセキュリティ，データセキュリティ，産業制御セキュリティ，アプリケーション配信などのコア領域に注力し，「ネットワークをよりシンプルに，よりスマートに，より安全にする」という使命を一貫して堅持しています。10年以上にわたる献身的な開発を経て，同社は政府，通信，電力・エネルギー，金融，公共安全などの重要産業にまたがるサービスネットワークを構築し，さまざまな分野のデジタル変革において重要なセキュリティ勢力となっています。2024年には，同社は優れた業績を上げ，営業収益は前年比11.68%増の115億4,800万元を達成しました。上場企業の株主に帰属する純利益は16億1,200万元に達し，前年同期比27.26%増となりました。営業活動による純キャッシュフローは32億8,200万元となり，前年同期比160.69%増と大幅に増加しました。同社は規模拡大と収益性において質の高い発展を遂げ，サイバーセキュリティ業界における競争力と成長の可能性を示しました。

DPtechのISO/IEC 27001認証取得の要因

市場参入ニーズ：入札要件と国際市場ニーズへの対応

市場参入ニーズへの対応は，DPtechの認証取得における重要な要因です。サイバーセキュリティ業界に深く携わる企業として，DPtechの主要顧客は政府，通信，金融，電力・エネルギーといった重要分野に集中しています。これらの業界における高額プロジェクトの入札において，顧客は製品性能だけでなく，サプライヤー自身のセキュリティ管理能力とサービス保証能力も重視します。特に先進国市場では，サイバーセキュリティ法やデータセキュリティ法など，情報セキュリティ管理に関して極めて厳格かつ複雑なコンプライアンス要件が課されています。国際的に認められた情報セキュリティ管理規格であるISO/IEC 27001認証は，市場参入の必須条件となっています。あるインタビュー対象者は，「プロジェクト入札において，多くの大手企業や通信事業者からISO/IEC 27001認証の取得を求められています。国際市場の要求に応え，国内外の規制を遵守するため，DPtechは海外市場向けネットワークセキュリティ製品の販売に関してISO/IEC 27001認証を取得しました」と述べています。

Internal management needs: Fuelling digital transformation

Driving the continuous optimization of internal management and supporting digital transformation is a long-term driver for DPtech. ISO/IEC 27001 aligns with the company's internal demand for digital transformation security. With the development of the company's business, DPtech wants to achieve several things: establish a comprehensive protection mechanism covering technology, management and personnel, mitigate risks such as network attacks, reduce data breaches, and dynamically adapt to evolving threats through regular audits and optimizations. DPtech views ISO/IEC 27001 certification not as an end goal but as a starting point. Through post-certification periodic audits and continuous improvement mechanisms, DPtech is able to regularly review and refine its security policies and processes, dynamically adapting to the evolving cybersecurity threat landscape.

This culture of continuous improvement is highly consistent with DPtech's core values of "innovation, integrity, contribution and sharing". An interviewee emphasized: "It is essential to dynamically adapt to the evolving security demands of digital transformation. During this process, the ability to identify risks must be established, with the ISO/IEC 27001 standard serving as a key reference." He added: "In terms of self-demand, DPtech wants to dynamically adapt to its own security needs in digital transformation. DPtech aims to establish a comprehensive protection mechanism that covers technology, management and personnel. It also seeks to mitigate risks such as network attacks, and strengthen security defenses, reduce data breaches, dynamically adapt to changes in threats through regular audits and optimizations, and finally, support security needs in digital transformation."

DPtech's ISO/IEC 27001 certification status

DPtech's IT department fully manages the ISO/IEC 27001 certification process (see Figure 10). This department centrally coordinates all aspects of the enterprise information security certification, playing a core leading role throughout the entire life cycle – from preparatory work prior to certification, coordination and communication during the certification process, and post-certification maintenance and optimization. To ensure comprehensive information security throughout all corporate operations, the ISO/IEC 27001 certification encompasses every business department, including marketing, R&D and technical support. Whether safeguarding customer information during marketing campaigns, protecting core technological assets in R&D, or maintaining user data confidentiality in technical support, all aspects are integrated into the certification management system, achieving full coverage of information security management.

Certification's key control areas cover four core links: development security, supplier security, project management security, and application and network security. Specifically, for development security, the company holds Capability Maturity Model Integration (CMMI) Level 5 certification, deploys virtual desktops for development-process data protection, and adopts Product Life Cycle Management (PLM) and Enterprise Resource Planning (ERP) systems to secure internal system development. For supplier security, it signs security/confidentiality agreements and conducts on-site supplier audits. For project management security, it follows relevant specifications to enforce security requirements and standardizes operations via information systems. For application and network security, it deploys firewalls, Intrusion Prevention Systems (IPS), situational awareness systems and bastion hosts for isolation, protection and auditing, while conducting regular system security tests and local/off-site back-ups of critical data.

During the process of pursuing ISO/IEC 27001 certification, DPtech also encountered several challenges. The most prominent challenge was balancing the relationship between information security and work efficiency, as well as between investment and value output. This issue significantly influenced the company's decision-making.

社内管理ニーズ：デジタルトランスフォーメーションの推進

社内管理の継続的な最適化とデジタルトランスフォーメーションの推進は，DPtechにとって長期的な推進力となっています。ISO/IEC 27001は，デジタルトランスフォーメーションにおけるセキュリティに関する同社の社内ニーズに合致しています。DPtechは事業の発展に伴い，いくつかの目標達成を目指しています。それは，技術，経営，人材を網羅する包括的な保護メカニズムの構築，ネットワーク攻撃などのリスク軽減，データ漏洩の削減，そして定期的な監査と最適化を通じて進化する脅威への動的な適応です。DPtechはISO/IEC 27001認証を最終目標ではなく，出発点と捉えています。認証取得後の定期監査と継続的改善メカニズムを通じて，DPtechはセキュリティポリシーとプロセスを定期的に見直し，改善することで，進化するサイバーセキュリティの脅威環境に動的に対応しています。

この継続的改善の文化は，DPtechのコアバリューである「革新，誠実，貢献，共有」と非常に合致しています。あるインタビュー対象者は，「デジタルトランスフォーメーションに伴うセキュリティ要求の進化に動的に対応することが不可欠です。このプロセスにおいて，リスクを特定する能力を確立する必要があり，ISO/IEC 27001規格はその重要な参照点となります」と強調しました。同氏はさらに，「DPtechは，デジタルトランスフォーメーションにおける自社のセキュリティニーズに動的に対応していくことを目指しています。技術，管理，人材を網羅する包括的な保護メカニズムの構築を目指し，ネットワーク攻撃などのリスクを軽減し，セキュリティ防御を強化し，データ漏洩を削減し，定期的な監査と最適化を通じて脅威の変化に動的に対応し，最終的にデジタルトランスフォーメーションにおけるセキュリティニーズをサポートすることを目指しています」と述べました。

DPtechのISO/IEC 27001認証取得状況

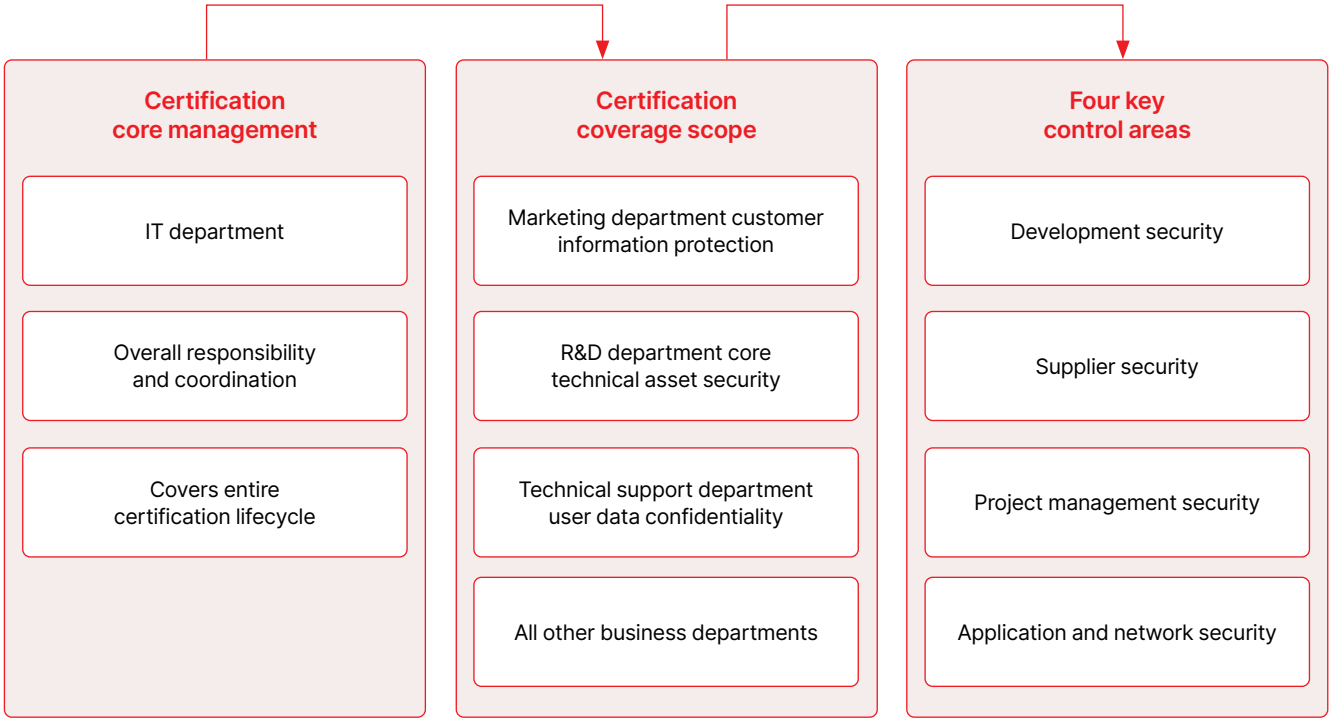
DPtechのIT部門は，ISO/IEC 27001認証プロセスを全面的に管理しています（図10参照）。この部門は，企業情報セキュリティ認証のあらゆる側面を一元的に調整し，認証前の準備作業から，認証プロセス中の調整とコミュニケーション，認証後の維持管理と最適化に至るまで，ライフサイクル全体を通して中心的な役割を担っています。企業活動全体における包括的な情報セキュリティを確保するため，ISO/IEC 27001認証は，マーケティング，研究開発，テクニカルサポートを含むすべての事業部門を対象としています。マーケティングキャンペーンにおける顧客情報の保護，研究開発における基幹技術資産の保護，テクニカルサポートにおけるユーザーデータの機密保持など，あらゆる側面が認証管理システムに統合され，情報セキュリティ管理の完全な網羅を実現しています。

認証の主要な管理領域は，開発セキュリティ，サプライヤーセキュリティ，プロジェクト管理セキュリティ，アプリケーションおよびネットワークセキュリティという4つの主要なリンクを網羅しています。具体的には，開発セキュリティに関して，同社は能力成熟度モデル統合（CMMI）レベル5の認証を取得し，開発プロセスデータの保護のために仮想デスクトップを導入し，社内システム開発のセキュリティ確保のために製品ライフサイクル管理（PLM）および企業資源計画（ERP）システムを採用しています。サプライヤーセキュリティに関しては，セキュリティ／機密保持契約を締結し，サプライヤーのオンサイト監査を実施しています。プロジェクト管理セキュリティに関しては，関連仕様に準拠してセキュリティ要件を徹底し，情報システムを通じて業務を標準化しています。アプリケーションおよびネットワークセキュリティに関しては，ファイアウォール，侵入防御システム（IPS），状況認識システム，および隔離，保護，監査のためのバスティオンホストを導入し，定期的なシステムセキュリティテストと重要データのローカル／オフサイトバックアップを実施しています。

ISO/IEC 27001認証取得の過程で，DPtechはいくつかの課題にも直面しました。最も大きな課題は，情報セキュリティと業務効率，そして投資と価値創出のバランスを取ることでした。この問題は，同社の意思決定に大きな影響を与えました。

Take protecting core R&D assets as an example. To ensure the security of these assets, the company implemented virtual desktops for management. However, the application of virtual desktops had a slight negative impact on R&D work efficiency. To address this issue, the company conducted in-depth research and analysis, implementing a differentiated solution. For the R&D department, while ensuring the security of core assets, the company continuously optimized the performance and user experience of virtual desktops to minimize the impact on R&D efficiency. For other departments, core asset protection relied more on robust management practices and a limited number of necessary technical measures. This approach ensured information security while maximizing work efficiency throughout all departments, achieving a balance between information security and operational productivity.

Figure 11: DPtech's ISO/IEC 27001 certification status



The effectiveness of DPtech's ISO/IEC 27001 certification

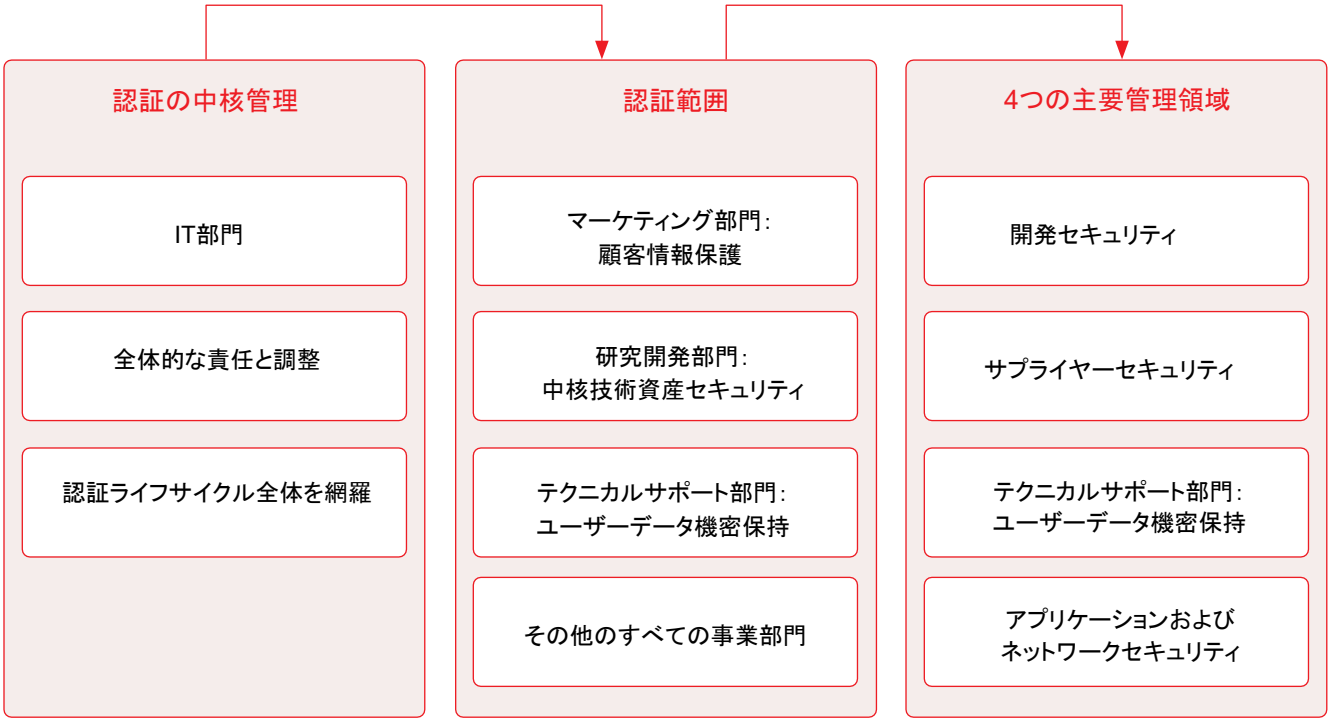
Commercial value elevation: Gaining the competitive edge in market competition

At the commercial level, ISO/IEC 27001 certification has brought significant competitive advantages to DPtech. On one hand, it meets domestic and international market compliance requirements for corporate information security management, helping mitigate operational security risks. On the other hand, it strengthens customer trust, enhances the company's attractiveness in market competition, and lays a solid foundation for business expansion. Obtaining this certification allows DPtech to directly enter high-end markets and significantly improve its market competitiveness. As one interviewee noted: "Chinese enterprises have ISO/IEC 27001 certification, which is very helpful for the credibility of products and solutions, as well as for enhancing market competitiveness."

Another interviewee elaborated on the bidding benefits: "Using the ISO/IEC 27001 certification in bidding processes provides clear and direct benefits: it helps reduce operational risks and

例えば，コアとなる研究開発資産の保護について考えてみましょう。これらの資産のセキュリティを確保するため，同社は管理部門向けに仮想デスクトップを導入しました。しかし，仮想デスクトップの導入は研究開発業務の効率に若干の悪影響を及ぼしました。この課題に対処するため，同社は綿密な調査と分析を行い，差別化されたソリューションを導入しました。研究開発部門においては，コア資産のセキュリティを確保しつつ，研究開発効率への影響を最小限に抑えるため，仮想デスクトップのパフォーマンスとユーザーエクスペリエンスを継続的に最適化しました。その他の部門においては，コア資産の保護は，より頑健な管理手法と必要最小限の技術的対策に重点を置きました。このアプローチにより，全部門において情報セキュリティを確保しつつ業務効率を最大化し，情報セキュリティと業務生産性のバランスを実現しました。

図 11: DPtechのISO/IEC 27001認証取得状況



DPtechのISO/IEC 27001認証の有効性

商業的価値の向上：市場競争における優位性の獲得

商業レベルでは，ISO/IEC 27001認証はDPtechに大きな競争優位性をもたらしました。一方では，企業情報セキュリティ管理に関する国内外の市場コンプライアンス要件を満たし，運用上のセキュリティリスクの軽減に貢献しています。他方，この認証は顧客の信頼を強化し，市場競争における企業の魅力を高め，事業拡大のための強固な基盤を築きます。DPtechはこの認証を取得することで，ハイエンド市場に直接参入し，市場競争力を大幅に向上させることができます。あるインタビュー対象者は，「中国企業はISO/IEC 27001認証を取得しており，これは製品やソリューションの信頼性を高め，市場競争力を向上させる上で非常に役立っています」と述べています。

別のインタビュー対象者は，入札におけるメリットについて次のように詳しく説明しました。「入札プロセスにおいてISO/IEC 27001認証を活用することで，明確かつ直接的なメリットが得られます。運用リスクの低減と顧客からの信頼向上に貢献します。」さらに，「ISO/IEC

enhances customer trust." He added: "ISO/IEC 27001 qualifications help enterprises obtain more orders." As the interviewee summarized: "Certification enhances customers' trust in the enterprise, making it more attractive in the market and beneficial for business expansion."

Internal management optimization: Improving the information security management system

Obtaining ISO/IEC 27001 certification has promoted a comprehensive and in-depth optimization of DPtech's ISMS. From management model transformation to risk prevention enhancement, and from employee awareness upgrading to process institutionalization, the system has achieved a leap from fragmented management to systematic governance. This has significantly improved the overall level of the company's information security work and laid a solid foundation for business development.

Key elements of progress have included:

Management model upgrade: From reactive response to proactive prevention

The certification has driven a fundamental transformation in DPtech's information security management approach: moving from the previous "reactive firefighting" model to an "active prevention" model, and evolving management processes from "disjointed and arbitrary" to "systematic and standardized". By establishing a comprehensive ISMS and processes, the efficiency and effectiveness of information security management have been significantly enhanced.

One interviewee recalled: "Before certification, our information security efforts were relatively passive and fragmented, lacking clear standards and a systematic framework. After the problem arose, a system and process were developed to address it, lacking initiative and systematic problem-solving. After reviewing various practices, we recognized that the ISO/IEC 27001 framework is more comprehensive, helping to address issues in a systematic manner and move away from the previous scattered and inconsistent approaches." They added: "After certification, the company's management approach has become more standardized and structured... Risk control objectives are now clearer, and process-driven operations have effectively kept risks under control."

Risk prevention enhancement: Clearer objectives and targeted protection

ISO/IEC 27001 certification has helped DPtech establish a risk-driven management approach. As a result, DPtech has clarified the goals and priorities of information security management through the certification system. Targeted protection measures have been established for the company's core information assets, enabling timely detection and response to various security incidents, thereby minimizing security breach-related losses.

Prior to certification, unregulated information security management posed hidden risks to the company. As one interviewee noted: "After certification, the company's risk control objectives have become clearer, and process-driven operations are now effectively managing risks." This systematic risk management approach has significantly reduced the impact of potential security threats on business operations.

Employee awareness improvement: Building a solid human defence line

Through training and awareness-raising activities during the certification process, employees' information security awareness has been greatly enhanced, transforming them from a "weak link" into a "security defence line" for the company. Employees now consciously abide by the ISMS in daily work and proactively identify and mitigate security risks, further reducing the company's overall information security risks.

One interviewee pointed out: "Before certification, employees had weak security awareness, such as using weak passwords and inadequate confidentiality of personal information." To consolidate the awareness

27001認証は，企業がより多くの受注を獲得するのに役立ちます。」と付け加えました。インタビュー対象者は，「認証取得は企業に対する顧客の信頼を高め，市場における企業の魅力を向上させ，事業拡大に有益です。」と結論付けました。

内部管理の最適化：情報セキュリティマネジメントシステムの改善

ISO/IEC 27001認証の取得は，DPtech社のISMS（情報セキュリティマネジメントシステム）の包括的かつ徹底的な最適化を促進しました。管理モデルの変革からリスク予防の強化，従業員の意識向上からプロセスの制度化に至るまで，システムは断片的な管理から体系的なガバナンスへと飛躍的に進化しました。これにより，同社の情報セキュリティ業務全体のレベルが大幅に向上し，事業発展のための強固な基盤が築かれました。

主な進展要素は以下のとおりです。

管理モデルのアップグレード：事後対応型から予防型へ

認証取得は，DPtechの情報セキュリティ管理アプローチに根本的な変革をもたらしました。従来の「事後対応型」モデルから「予防型」モデルへの移行，そして「断片的で恣意的」だった管理プロセスから「体系的で標準化された」プロセスへの進化です。包括的なISMSとプロセスを確立することで，情報セキュリティ管理の効率性と有効性が大幅に向上しました。

あるインタビュー対象者は次のように述べています。「認証取得前は，情報セキュリティへの取り組みは比較的受動的で断片的であり，明確な基準や体系的なフレームワークが欠如していました。問題が発生してから対処するためのシステムやプロセスを開発していましたが，主体性や体系的な問題解決能力が欠けていました。様々な実践事例を検討した結果，ISO/IEC 27001フレームワークはより包括的であり，問題を体系的に解決し，従来の散漫で一貫性のないアプローチから脱却するのに役立つと認識しました。」彼らはさらに，「認証取得後，当社の経営アプローチはより標準化され，体系化されました。リスク管理の目標がより明確になり，プロセス主導型の運用によってリスクを効果的に管理できるようになりました」と述べました。

リスク予防の強化：目標の明確化と的を絞った保護

ISO/IEC 27001認証は，DPtechがリスク主導型の経営アプローチを確立する上で役立ちました。その結果，DPtechは認証制度を通じて情報セキュリティ管理の目標と優先順位を明確にしました。企業の中核となる情報資産に対して的を絞った保護対策が確立され，様々なセキュリティインシデントをタイムリーに検知・対応できるようになり，セキュリティ侵害による損失を最小限に抑えることができました。

認証取得前は，規制のない情報セキュリティ管理が企業に潜在的なリスクをもたらしていました。あるインタビュー対象者は，「認証取得後，当社のリスク管理の目標がより明確になり，プロセス主導型の運用によってリスクを効果的に管理できるようになりました」と述べています。この体系的なリスク管理アプローチにより，潜在的なセキュリティ脅威が事業運営に与える影響が大幅に軽減されました。

従業員の意識向上：強固な人的防衛線の構築

認証取得プロセスにおける研修と啓発活動を通じて，従業員の情報セキュリティ意識は大幅に向上し，これまで「弱点」であった従業員が，企業にとっての「セキュリティ防衛線」へと変貌を遂げました。従業員は現在，日々の業務においてISMS（情報セキュリティマネジメントシステム）を意識的に遵守し，セキュリティリスクを積極的に特定・軽減することで，企業全体の情報セキュリティリスクをさらに低減させています。

あるインタビュー対象者は，「認証取得前は，従業員のセキュリティ意識が低く，脆弱なパスワードの使用や個人情報の機密保持の不徹底などが見ら

improvement, DPtech has embedded internal processes and policies into platforms such as PRM, ERP and CRM, institutionalizing workflows to ensure all employees follow standardized procedures. The interviewee confirmed: “Both management and R&D staff have demonstrated enhanced security awareness.”

Conclusions and recommendations

Conclusions

Certification serves as the core credential for enterprises to gain market access and secure competitive advantage.

In tendering processes for projects within critical sectors such as government, telecommunications, finance, and power and energy, ISO/IEC 27001 certification has evolved from a supplementary advantage to an essential qualification or core evaluation criterion. For DPtech, this certification grants eligibility to compete in high-end markets while dismantling international trade barriers. It demonstrates to overseas clients that its information security management aligns with global standards, paving the way for business expansion worldwide.

H3C, meanwhile, leverages this certification alongside its Tier 3 Cybersecurity Protection Level certification to meet stringent data protection requirements in regions such as the EU and South-East Asia. Its strategic choice of Norwegian certification bodies operating in China, coupled with regionally tailored TÜV qualifications, further enhances the international credibility of its certifications, directly driving growth in overseas orders. Both enterprises demonstrate that certification serves as a strategic foundation for winning client trust and capturing market share in digital trade.

ISO/IEC 27001 and its certification drive systematic upgrades to corporate information security management models.

ISO/IEC 27001 has enabled both enterprises to transition from a reactive, firefighting management approach to establishing a proactive, systematic framework for prevention. At the enterprise level, DPtech centralized certification efforts in all business departments under its IT division, achieving comprehensive information security coverage. H3C established a dedicated information security department and formed cross-departmental working groups, with strategic decisions overseen by the President’s Office, creating an efficient top-down management structure that clarifies departmental responsibilities and reduces communication overhead.

Regarding processes and technology, DPtech integrates security requirements throughout the entire business lifecycle via CMMI5 virtual desktops and PLM/ERP systems, while balancing security and efficiency according to the distinct needs of R&D versus non-R&D departments. H3C has introduced AI-driven operations, AI monitoring and protection technologies to replace traditional approaches, forming a collaborative defence system combining human expertise with technological capabilities. Notably, H3C’s actual security management standards now exceed certification benchmarks. These certifications primarily validate and enhance the effectiveness of existing frameworks, reflecting the forward-thinking strategic positioning of mature enterprises.

れました」と指摘しました。意識向上を確固たるものにするため，DPtechはPRM，ERP，CRMといったプラットフォームに社内プロセスとポリシーを組み込み，ワークフローを制度化することで，全従業員が標準化された手順に従うようにしました。インタビュー対象者は，「経営陣と研究開発部門の両方で，セキュリティ意識の向上が見られました」と述べています。

結論と提言

結論

認証は，企業が市場参入を果たし，競争優位性を確保するための重要な資格となります。

政府，通信，金融，電力・エネルギーといった重要セクターにおけるプロジェクトの入札プロセスにおいて，ISO/IEC 27001認証は，付加的な利点から，必須の資格または主要な評価基準へと進化しました。DPtechにとって，この認証はハイエンド市場での競争資格を得ると同時に，国際貿易障壁の撤廃にもつながります。また，海外の顧客に対し，同社の情報セキュリティ管理がグローバルスタンダードに準拠していることを証明し，世界的な事業拡大への道を開きます。

一方，H3Cは，この認証をティア3サイバーセキュリティ保護レベル認証と併せて活用し，EUや東南アジアなどの地域における厳格なデータ保護要件を満たしています。中国で事業を展開するノルウェーの認証機関を戦略的に選択し，地域に合わせたTÜV認証を取得することで，認証の国際的な信頼性をさらに高め，海外からの受注増加に直接的に繋げています。両社は，認証が顧客の信頼獲得とデジタル取引における市場シェア拡大のための戦略的な基盤となることを示しています。

ISO/IEC 27001とその認証は，企業の情報セキュリティ管理モデルの体系的なアップグレードを推進します。

ISO/IEC 27001は，両社が事後対応型の危機管理アプローチから，予防のための積極的かつ体系的なフレームワークの構築へと移行することを可能にしました。企業レベルでは，DPtechはIT部門傘下の全事業部門における認証取得活動を一元化し，包括的な情報セキュリティを実現しました。H3Cは，情報セキュリティ専門部署を設立し，部門横断的なワーキンググループを組織しました。戦略的な意思決定は社長室が監督し，部門の責任範囲を明確化し，コミュニケーションの負担を軽減する効率的なトップダウン型の経営体制を構築しました。

プロセスとテクノロジーに関しては，DPtechはCMMI5仮想デスクトップとPLM/ERPシステムを通じて，ビジネスライフサイクル全体にわたってセキュリティ要件を統合し，研究開発部門と非研究開発部門のそれぞれのニーズに応じてセキュリティと効率性のバランスを取っています。H3Cは，従来の手法に代わるものとして，AIを活用した運用，AIによる監視，保護技術を導入し，人間の専門知識と技術力を融合させた協調的な防御システムを構築しました。特筆すべきは，H3Cの実際のセキュリティ管理基準が認証基準を上回っていることです。これらの認証は，既存のフレームワークの有効性を検証・強化するものであり，成熟した企業の先見的な戦略的ポジショニングを反映しています。

The value of ISO/IEC 27001 and its certification extend beyond compliance assurance to encompass business empowerment and brand building.

Information security management capabilities have evolved from a supporting role to a value-creating driver. DPtech leveraged ISO/IEC 27001 to strengthen protection of core R&D assets and enhance supplier security controls, thereby boosting the competitiveness of its products and solutions, achieving significant revenue growth in 2024. H3C, meanwhile, transformed its certification practices into external security consulting services. Capitalizing on its full-stack ICT product line advantages, it provides ISO/IEC 27001 certification consulting to clients, creating a new business growth point. Furthermore, both enterprises bolstered client trust through certification: DPtech met domestic and international compliance requirements to mitigate operational risks, while H3C enhanced global brand influence by building digital trust. ISO/IEC 27001 and its certification are vital pillars for corporate digital transformation and high-quality development.

Recommendations

Elevate information security management to the corporate strategic level.

Organizations should integrate ISO/IEC 27001 certification into their long-term development strategy, with senior management spearheading implementation and coordinating resource allocation to ensure information security management is planned and executed in tandem with business development. Only by embedding security capabilities as a core organizational competency can sustainable, differentiated advantages be established amid increasingly fierce digital competition.

Establish a continuous improvement mechanism to proactively adapt to technological evolution and business changes.

Certification is not the end goal, but rather the starting point for enhanced management. Enterprises should establish routine review and optimization mechanisms to proactively address security challenges that emerging technologies such as cloud computing and AI pose. Concurrently, through continuous staff training and cultural development, security awareness must be embedded within the organization's DNA, thereby constructing a security governance framework that effectively defends against risks while flexibly supporting business innovation.

Unlocking the derivative value of ISO/IEC 27001 and its certification to drive the transformation of security capabilities.

Enterprises must proactively unlock the business-enabling value of ISO/IEC 27001 and its certification. Technology-driven companies may follow the example of H3C by transforming certification practices into external services, such as security consulting and system architecture development, thereby cultivating new revenue streams. Product-driven enterprises can draw inspiration from DPtech by leveraging ISO/IEC 27001 to enhance R&D and supply chain security, thereby boosting product competitiveness. Furthermore, by capitalizing on the international credibility of certification, they can expand into overseas markets, propelling information security management from a cost centre to a value-creating hub and injecting momentum into high-quality corporate development.

ISO/IEC 27001とその認証の価値は，コンプライアンス保証にとどまらず，ビジネスの強化とブランド構築にも及びます。

情報セキュリティ管理能力は，支援的な役割から価値創造の原動力へと進化を遂げました。DPtechはISO/IEC 27001を活用し，コアとなる研究開発資産の保護強化とサプライヤーセキュリティ管理の向上を図ることで，製品・ソリューションの競争力を高め，2024年には大幅な収益成長を達成しました。一方，H3Cは認証業務を外部セキュリティコンサルティングサービスへと転換しました。フルスタックICT製品ラインの強みを活かし，顧客向けにISO/IEC 27001認証コンサルティングを提供することで，新たな事業成長の足がかりを築きました。さらに，両社とも認証を通じて顧客からの信頼を強化しました。DPtechは国内外のコンプライアンス要件を満たすことで運用リスクを軽減し，H3Cはデジタル信頼の構築を通じてグローバルブランドの影響力を高めました。ISO/IEC 27001とその認証は，企業のデジタルトランスフォーメーションと高品質な開発にとって不可欠な柱です。

提言

情報セキュリティ管理を企業戦略レベルに引き上げる。

組織は，ISO/IEC 27001認証を長期的な開発戦略に組み込むべきです。経営陣が主導して導入を推進し，リソース配分を調整することで，情報セキュリティ管理が事業開発と連携して計画・実行されるようにする必要があります。セキュリティ能力を組織の中核的な能力として組み込むことによってのみ，ますます激化するデジタル競争の中で持続可能で差別化された優位性を確立できます。

技術革新とビジネスの変化に積極的に適応するための継続的改善メカニズムを確立しましょう。

認証は最終目標ではなく，管理強化の出発点です。企業は，クラウドコンピューティングやAIなどの新興技術がもたらすセキュリティ上の課題に積極的に対処するために，定期的なレビューと最適化のメカニズムを確立する必要があります。同時に，継続的な従業員研修と文化開発を通じて，セキュリティ意識を組織のDNAに根付かせ，リスクから効果的に防御しつつ，ビジネスイノベーションを柔軟に支援するセキュリティガバナンスフレームワークを構築する必要があります。

ISO/IEC 27001とその認証の派生価値を解き放ち，セキュリティ能力の変革を推進しましょう。

企業は，ISO/IEC 27001とその認証が持つビジネス促進価値を積極的に活用していく必要があります。技術主導型企業は，H3Cの事例に倣い，認証取得プロセスをセキュリティコンサルティングやシステムアーキテクチャ開発といった外部サービスへと転換することで，新たな収益源を創出できるでしょう。製品主導型企業は，DPtechの事例を参考に，ISO/IEC 27001を活用して研究開発とサプライチェーンのセキュリティを強化し，製品競争力を高めることができます。さらに，認証の国際的な信頼性を活用することで，海外市場への進出が可能となり，情報セキュリティ管理をコストセンターから価値創造のハブへと転換させ，質の高い企業発展に弾みをつけることができます。

Reference list

1. Abeliansky, A. L., & Hilbert, M. (2017). Digital technology and international trade: Is it the quantity of subscriptions or the quality of data speed that matters. Telecommunications Policy, 41(1), 35-48.

2. Al-Karaki, J.N., Gawanmeh, A. & El-Yassami, S. (2022). GoSafe: on the practical characterization of the overall security posture of an organization information system using smart auditing and ranking. Journal of King Saud University, 3(6), 3079-3095.

3. Blum, B. S., & Goldfarb, A. (2006). Does the internet defy the law of gravity? Journal of international economics, 70(2), 384-405.

4. Boubakri, S., Guillaumin, C., & Silanine, A. (2019). Non-linear relationship between real commodity price volatility and real effective exchange rate: The case of commodity-exporting countries. Journal of Macroeconomics, 60, 212-228.

5. Chernozhukov, V., Chetverikov, D., Demirer, M., Duflo, E., Hansen, C., & Newey, W. K., & Robins, J. (2018). Double/debiased machine learning for treatment and structural parameters. The Econometrics Journal, 21(1), 1-68.

6. China Standardization Newsletter (2023), available at: https://sesec.eu/wp-content/uploads/2025/03/SESEC-V-Newsletter-January-February-2025.pdf

7. Corbett, C. J., & Kirsch, D. A. (2001). International diffusion of ISO 14000 certification. Production and operations management, 10(3): 327-342.

8. Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. The TQM Journal, 33 (7), 76–105.

9. Dionysiou, I. (2011). An investigation on compliance with ISO/IEC 27001 in Cypriot private and public organizations. International Journal of Services and Standards, 7 (3), 197-234.

10. Guo, S., Ahmad, K., & Khan, N. U. (2024). Natural resources, geopolitical conflicts, and digital trade: Evidence from China. Resources Policy. 90, 104708.

11. Milner, H. V. (2006). The digital divide: The role of political institutions in technology diffusion. Comparative Political Studies, 39(2), 176-199.

12. Podrecca, M., Culot, G., Nassimbeni, G., & Sartor, M. (2022). Information security and value creation: The performance implications of ISO/IEC 27001. Computers in Industry, 142, 103744.

13. Podrecca, M., & Sartor, M. (2023). Forecasting the diffusion of ISO/IEC 27001: a Grey model approach. The TQM Journal, 35(9), 123-151.

14. Rezaei, G., Ansari, M., Memari, A., Zahraee, S.M. & Shaharoun, A.M. (2014), A heuristic method for information scaling in manufacturing organizations. Jurnal Teknologi, 69(3), 87-91.

参考文献

1. Abeliansky, A. L., & Hilbert, M. (2017). デジタル技術と国際貿易：重要なのは加入者数か，それともデータ速度の質か．電気通信政策，41(1)，35-48.

2. Al-Karaki, J.N., Gawanmeh, A. & El-Yassami, S. (2022). GoSafe: スマート監査とランキングを用いた組織情報システムの全体的なセキュリティ態勢の実際的な特性評価について．キングサウード大学紀要，3(6)，3079-3095.

3. Blum, B. S., & Goldfarb, A. (2006). インターネットは重力の法則に反するのか？国際経済学ジャーナル，70(2)，384-405.

4. Boubakri, S., Guillaumin, C., & Silanine, A. (2019). 実質商品価格変動と実質実効為替レートの非線形関係：商品輸出国の事例．マクロ経済学ジャーナル，60，212-228.

5. Chernozhukov, V., Chetverikov, D., Demirer, M., Duflo, E., Hansen, C., & Newey, W. K., & Robins, J. (2018). 治療パラメータと構造パラメータのための二重バイアス/バイアス除去機械学習。計量経済学ジャーナル，21(1)，1-68.

6. 中国標準化ニュースレター (2023)，入手先: https://sesec.eu/wp-content/uploads/2025/03/SESEC-V-Newsletter-January-February-2025.pdf

7. Corbett, C. J., & Kirsch, D. A. (2001). ISO 14000認証の国際的普及。生産および運用管理，10(3)：327-342.

8. CCulot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). ISO/IEC 27001情報セキュリティマネジメント規格：文献レビューと理論に基づく研究課題。TQMジャーナル，33(7)，76-105.

9. Dionysiou, I. (2011). キプロスの民間および公共機関におけるISO/IEC 27001準拠に関する調査．国際サービス・標準ジャーナル，7(3)，197-234.

10. Guo, S., Ahmad, K., & Khan, N. U. (2024). 天然資源，地政学的紛争，そしてデジタル貿易：中国からの証拠．資源政策，90，104708.

11. Milner, H. V. (2006). デジタルデバイド：技術普及における政治制度の役割。比較政治学研究，39(2)，176-199.

12. Podrecca, M.，Culot, G.，Nassimbeni, G.，Sartor, M. (2022). 情報セキュリティと価値創造：ISO/IEC 27001のパフォーマンスへの影響．産業におけるコンピュータ，142，103744.

13. Podrecca, M.，Sartor, M. (2023). ISO/IEC 27001の普及予測：グレーモデルアプローチ．TQMジャーナル，35(9)，123-151.

14. Rezaei, G.，Ansari, M.，Memari, A.，Zahraee, S.M.，Shaharoun, A.M. (2014). 製造業における情報スケーリングのためのヒューリスティック手法．技術ジャーナル，69(3)，87-91.

15. Vastag, G. (2004). Revisiting ISO 14000 diffusion: A new “look” at the drivers of certification. Production and Operations Management, 13(3), 260-267.

16. Wu, W., Shi, K., Wu, C. H., & Liu, J. (2021). Research on the impact of information security certification and concealment on financial performance: Impact of ISO 27001 and concealment on performance. Journal of Global Information Management (JGIM), 30(3), 1-16.

17. Zhu, Q., & Zhou, X. (2024). Regional differences and dynamic evolution of digital trade: Data from China. Applied Economics, 56(31), 3722-3740.

15. Vastag, G. (2004). ISO 14000普及の再検討：認証の推進要因に関する新たな視点．生産および運用管理, 13(3), 260-267.

16. WWu, W., Shi, K., Wu, C. H., & Liu, J. (2021). 情報セキュリティ認証と情報隠蔽が財務業績に与える影響に関する研究：ISO 27001と情報隠蔽が業績に与える影響．グローバル情報管理ジャーナル (JGIM), 30(3), 1-16.

17. Zhu, Q., & Zhou, X. (2024). デジタル貿易の地域差と動態的進化：中国のデータ．応用経済学, 56(31), 3722-3740.

About ISO

ISO (International Organization for Standardization) is an independent, non-governmental international organization with a membership of 176* national standards bodies. Through its members, it brings together experts to share knowledge and develop voluntary, consensus-based, market-relevant International Standards that support innovation and provide solutions to global challenges.

ISO has published more than 26 200* International Standards and related documents covering almost every industry, from technology to food safety, to agriculture and healthcare.

For more information, please visit **www.iso.org**.

*March 2026

ISO Website: www.iso.org
ISO newsroom: www.iso.org/news
ISO videos: www.iso.org/youtube

Follow @isostandards on social media

ISOについて

ISO（国際標準化機構）は，176*の各国標準化団体が加盟する独立した非政府国際機関です。会員団体を通じて，専門家が知識を共有し，イノベーションを支援し，地球規模の課題解決に貢献する，自主的かつコンセンサスに基づく市場適合性の高い国際規格を開発しています。

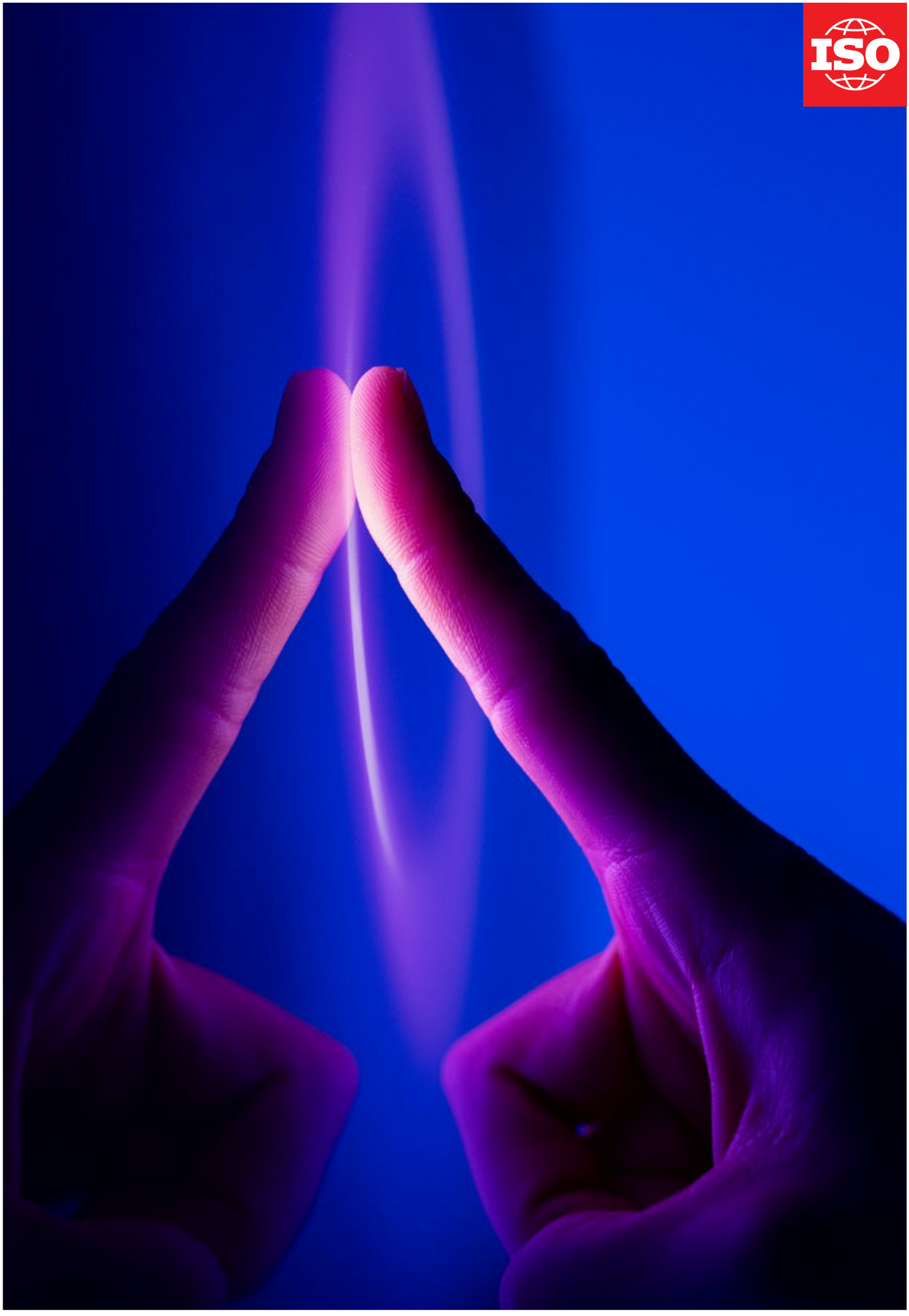
ISOは，テクノロジーから食品安全，農業，医療に至るまで，ほぼすべての産業分野を対象とする26,200*を超える国際規格および関連文書を発行しています。

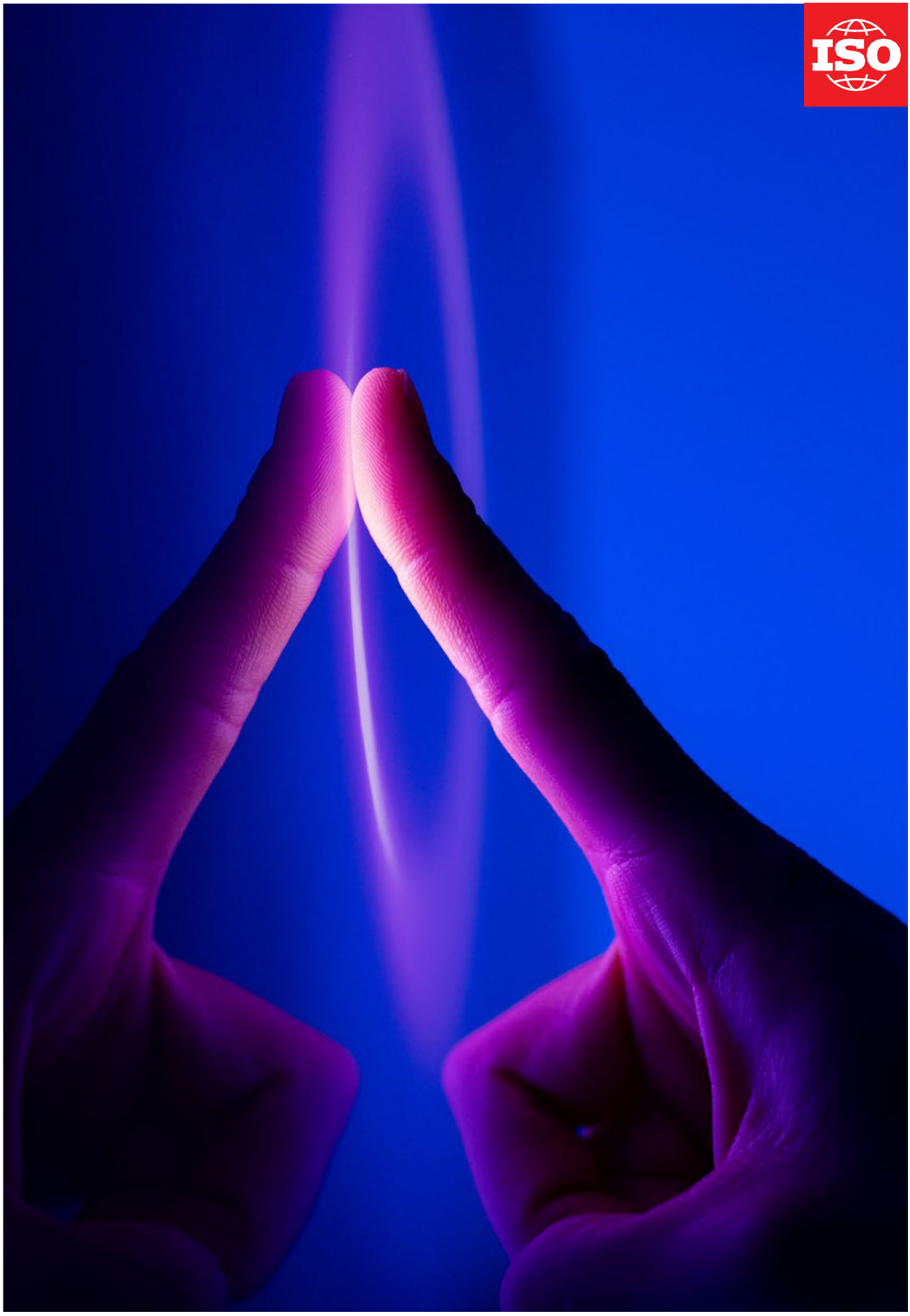
詳細については，**www.iso.org** をご覧ください。

*2026年3月現在

ISO Website: www.iso.org
ISO newsroom: www.iso.org/news
ISO videos: www.iso.org/youtube

Follow @isostandards on social media





International Organization for Standardization

ISO Central Secretariat
Chemin de Blandonnet 8
1214 Geneva, Switzerland

We care about our planet.
（私たちは地球環境を大切にしています。）
This brochure printed on recycled paper.
（このブロシュアは再生紙を使用しています。）

ISBN 978-92-67-11450-7

本文書は経済産業省の委託事業の成果です。

iso.org