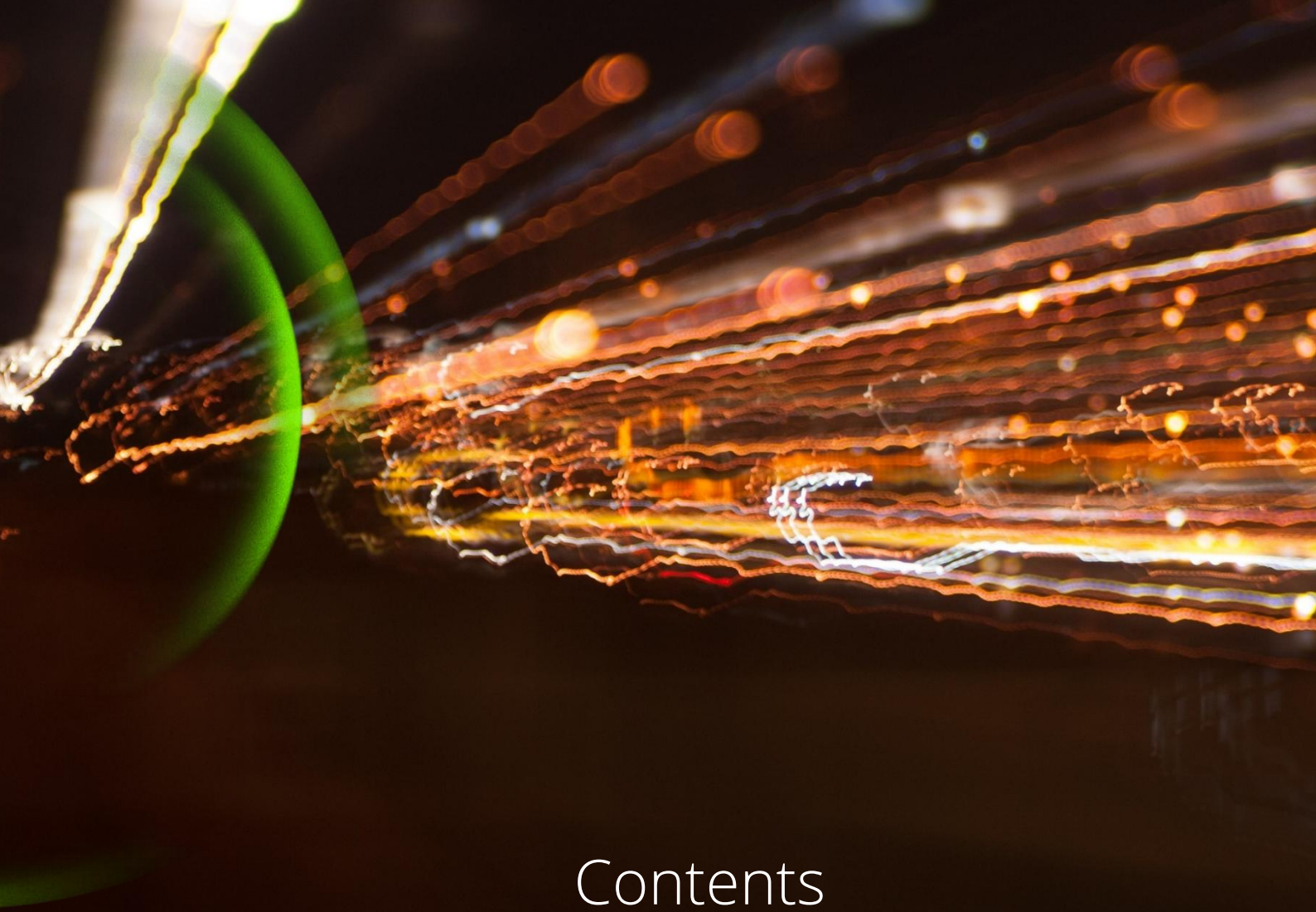
Deloitte.
デロイト トーマツ

Building Japan's cybersecurity workforce of tomorrow

Cyber talent reimagined



Contents

Introduction

Japan's cybersecurity landscape is under increasing pressure as the volume and sophistication of attacks surge dramatically. Japan has recently experienced several cyber breaches with attacks targeting infrastructure, government, and businesses.[1] New risks are also increasing with the spread of new technologies, such as generative artificial intelligence (AI).

Against this backdrop, the chronic shortage of highly skilled cybersecurity personnel further underscores Japan's cyber vulnerabilities. This shortfall is largely due to a combination of an aging population, an education system that has historically not prioritized practical IT skills, and a traditional corporate culture that

The regulatory environment is also tightening, with new cybersecurity frameworks demanding enhanced reporting, incident response capabilities, and governance structures. Organizations struggling with talent shortages find themselves increasingly exposed to compliance failures and regulatory penalties.

As digital transformation accelerates, this workforce gap will undoubtedly widen leaving the nation's critical infrastructure and businesses even more vulnerable.

A strategic imperative: Why this matters now

Japan is faced with a harsh reality – understaffed security teams cannot keep pace with increasingly sophisticated threat actors.

The cybersecurity threat landscape confronting Japan has intensified dramatically, with increased cyberattacks from state actors and criminals targeting infrastructure, government, and businesses. While businesses usually face ransomware and data theft, the government primarily sees cyber-espionage and attacks on critical infrastructure.

Despite the passage of the landmark Active Cyber Defense (ACD) law[2] in May 2025, aimed at modernizing government institutions and enhancing Japan's overall cybersecurity framework, the nation still struggles to manage security for its critical government systems, according to the government's Board of Audit report. The report identified 58 systems at 12 government agencies that had security gaps and lacked appropriate security measures.[3] This is happening during a surge in attacks. The government saw at least 447 incidents in 2024, more than double the prior year.[4]

Recent high-profile incidents underscore the human dimension of cybersecurity failures. Japan's cybersecurity workforce challenge has reached a pivotal moment that requires attention from business leaders, educational institutions, and the government. The nation faces a significant workforce gap with the shortage estimated at nearly 170,000 cybersecurity professionals.[5] According to ISC2, Japan experienced cybersecurity workforce growth in 2024 of 4% year-over-year. However, the skills gap expanded dramatically by 53.8%, showing demand is outpacing supply at an accelerating rate.[6]

Recognizing the need to develop its human resource capabilities, Japan has revealed various plans to expand its pool of cybersecurity personnel. In 2022, alongside the introduction of the ACD concept, the Ministry of Defense of Japan announced plans to more than quadruple its cyber defense personnel while increasing its overall staff dealing with cyberattacks to 20,000 by fiscal year 2027.[7]

In May 2025 the Ministry of Economy, Trade and Industry (METI) announced its target of increasing the number of Registered Information Security Specialists (RISSs). But the numbers underscore the challenge as only around 24,000 professionals as of April 2024 hold the Registered Information Security Specialist (RISS) national license – well below the government’s goal of 50,000 by 2030.[8]

Perhaps most concerning is the compound effect of all these challenges. As cyber threats grow more sophisticated and regulatory requirements expand, the workforce readiness gap widens further. Organizations cannot simply wait for the talent market to correct itself – this is a human capital challenge that threatens Japan’s digital sovereignty. Without immediate, coordinated action at the highest leadership levels, the risks to national security, economic resilience, and public trust will deepen.

Demographic shifts: The shrinking pipeline

Japan’s cybersecurity workforce challenge cannot be separated from its demographic realities – an aging society and a shrinking pool of young talent.

According to the Ministry of Internal Affairs and Communications, Statistics Bureau, as of 15 September 2025 the percentage of Japan's population aged 65 and over is 29.4%. This is the highest in the world among the 38 countries with a population of 40 million or more.[9] This is compounded by the percentage of Japan's working-age population (defined as those aged 15–64) being projected to drop to 52.9% by 2050.[10] This shrinking pool of working-age individuals puts pressures on traditional workforce development models. Recruiting fresh graduates into cybersecurity roles becomes increasingly difficult. Fewer young professionals are entering the job market precisely when cybersecurity demands are accelerating.

In addition to IT talent shortages, other industries face their own critical workforce needs. For example, healthcare, elderly care, and social services require significant human resources to support the growing elderly population. In essence, the aging society creates intense competition for skilled professionals across all sectors. Simultaneously, experienced IT professionals are reaching retirement age at an accelerated pace, taking decades of institutional knowledge with them. This creates a double burden: fewer new entrants to the workforce and accelerated departure of experienced professionals.

These demographic shifts affect cybersecurity recruitment and career pathways in multiple, compounding ways. Leaders would do well to understand and address these challenges, guiding their organizations to evolve to accommodate the dynamic, skills-based nature of cybersecurity work. Conventional career structures that were designed for a different era are likely no longer fit for purpose.

Cultural and policy factors: Untapped potential

Underlying the talent shortage are cultural and policy issues that further complicate recruitment and retention efforts.

The gender gap in IT and cybersecurity represents a significant, untapped talent pool. Currently, women account for only 18.8% of IT engineers in Japan, below the OECD average of 20.6% and other key countries such as the United Kingdom at 22.8% and Australia at 21.7%.[11]

This perception of cybersecurity as a male-dominated field discourages potential female candidates from entering the industry. If organisations can rethink their talent sourcing models by implementing inclusive workplace policies, tailoring recruitment for women, and ensuring greater visibility for women in security leadership roles, there is a substantial opportunity to expand the talent pipeline.

Japan's more mature workers, many of whom are active beyond retirement age, also represent an untapped talent pool. Surveys indicate that approximately 80% of Japanese workers want to continue working after retirement. Of these, around 70% would like to stay with their current employer.[12] Although the Japanese government, through the revised Act on Stabilization of Employment of Elderly Persons[13] and various subsidy programs, is actively encouraging companies to improve senior employment in Japan, reskilling strategies to transition this demographic into digital roles seem to remain underdeveloped.

Across Japan, various workplace policies such as traditional Japanese lifetime employment models or hierarchical career ladders likely need to evolve. Younger workers want more flexibility, workplace satisfaction, and jobs with purpose. A 2025 survey found that only 24.4% of young people want to work for the same company until retirement, compared with 36.3% in 2015.[14] According to Gallup's 2026 State of the Global Workplace study, only 8% of Japanese workers report being engaged at work, among the lowest rates globally. In addition to poor levels of engagement, almost two in five workers in Japan are stressed, with 39% saying they experienced a lot of stress the prior day.[15] These engagement and stress challenges reflect deeper workplace satisfaction issues that affect cybersecurity roles as much as other professions. When the majority of workers feel disconnected from their work, organizations face significant challenges in attracting and retaining the passionate, committed professionals that effective cybersecurity operations require. Organizations that continue with traditional hiring and promotion practices may find themselves at a disadvantage in attracting younger cybersecurity talent. Cybersecurity professionals are often seeking roles with clear career progression paths that accommodate the dynamic and skills-based nature of cybersecurity work.

Unless these cultural dynamics and policy factors are addressed, efforts to expand the cybersecurity workforce will continue to fall short.

Beyond the numbers: Fit for the future

Building Japan's cybersecurity workforce of tomorrow requires a fundamental reimagining of how organizations identify, attract, develop, and retain security talent. Even if the numbers in the workforce gap can be reduced significantly through hiring university graduates, the new era of digital defence requires a cybersecurity workforce that has purpose and resilience.

The future workforce will likely have several core characteristics.

1. Mission-driven: The motivation for the profession should be rooted in societal impact. This drive – a shared desire to protect digital assets and society – is the primary factor for sustained motivation and effectiveness in a field facing continuous, high-stakes responsibility.

2. Diverse: To secure a digital landscape, the workforce must reflect it. Diversity across gender, age, background and geography is crucial to provide varied perspectives for anticipating varied attack vectors. It also ensures security solutions are comprehensive and inclusive.

3. Emotionally resilient: The cyber team should be given the appropriate support that prepares and allows them to function under pressure. This collective emotional resilience enables the workforce to operate effectively under pressure and rapid change that defines the threat landscape.

4. Digitally fluent: It is important for the workforce to be digitally fluent in various topics outside the cybersecurity basics. For example, newer areas such as automation, AI systems, and AI ethics.

5. AI-augmented: The workforce would gain from being augmented by AI, with organisations recognizing that AI tools augment rather than replace human expertise. The most effective approach combines AI's speed and scale with human creativity, contextual understanding, and ethical judgment.

This future-ready workforce calls for a systemic shift in how roles are designed, how people are developed, and how organizations engage with talent.

The path forward: Redesign, rethink, reimagine

Organizations in Japan should consider aligning cybersecurity career pathways with the real and evolving expectations of Japan's workforce. If cybersecurity can be framed as a career with purpose – maintaining national security, keeping society safe, and helping organisations and the economy to grow through digital trust – it can inspire a new generation. This may involve reimagining the entire talent architecture supporting the cybersecurity workforce. Organisations should look to address key challenges – the current workforce shortage, enhancing the employee experience, and the future talent pipeline.

The following ten recommendations do not claim to be exhaustive or to fully solve Japan's cyber talent shortage. Rather, they aim to address several core challenges and provide meaningful steps toward building a more robust cybersecurity workforce.

Addressing the talent shortage

1. Embracing automation and AI: Automation and AI represent perhaps the most significant opportunity for organizations to address cybersecurity workforce constraints while simultaneously improving security effectiveness. Forward-thinking organizations invest in both people and technology, creating integrated human-AI teams that leverage complementary strengths. For example, AI-augmented security operations enable smaller teams to scale their impact. AI handles the routine tasks and highlights the critical issues that require human judgment. Japan's Ministry of Defense announced in July 2024 that it also plans to utilize AI to augment cybersecurity capabilities.[16] This approach can address immediate workforce constraints while building long-term capabilities for any organization.

2. Upskilling: The rapidly evolving nature of cybersecurity threats requires professionals to continuously update skills and adapt to new challenges. It is vital that organizations consider investment in comprehensive upskilling programs to enhance the capabilities of their existing cybersecurity workforce. This includes establishing structured talent development programs that offer continuous learning opportunities, certifications, and mentorship programs.

3. Reskilling: Reskilling employees from other parts of the business or from other industries can also help to expand the workforce. For example, professionals from finance roles could bring risk assessment expertise, manufacturing engineers possess operational technology insights crucial for industrial cybersecurity, and former military personnel offer discipline and crisis management. These professionals often possess the analytical thinking, attention to detail, and problem-solving capabilities that translate effectively to cybersecurity roles with appropriate training and support.

4. Hybrid talent models: Organizations can alleviate pressure on overstretched cybersecurity teams by adopting hybrid talent models that blend internal staff with external resources. By outsourcing certain functions to specialized providers, organizations can free internal teams to focus on strategic initiatives and high-priority threats. This approach not only reduces burnout and improves retention but also provides access to diverse expertise and 24/7 coverage that may be impractical to maintain solely with in-house personnel.

Enhancing the employee experience

5. Hiring practices: Cybersecurity encompasses diverse roles beyond just technical hacking, including strategy, privacy compliance, incident response, and risk analysis. Organizations can strengthen their workforce by recognizing that effective teams may include lawyers, incident responders from healthcare, and critical thinkers from varied backgrounds. This may require moving away from rigid, cybersecurity exam-based recruitment towards flexible, skills-based pathways for employment including bootcamps or apprenticeships. It may be that one-size-fits-all employment contracts are no longer suitable. In addition, inclusive hiring practices targeting women, mid-career professionals, retirees, and hiring in regional cities such as Sapporo or Fukuoka, can expand the workforce while attracting candidates from non-traditional sectors.

6. Recruitment marketing: Once organizations have rethought their hiring practices, how do they effectively attract the right talent? Modern recruitment marketing strategies can expand the talent pipeline by repositioning cybersecurity careers as dynamic, mission-critical roles offering societal impact and intellectual challenges. Rather than technical job descriptions that emphasize required credentials, effective recruitment narratives could highlight diversity and inclusion, career growth opportunities, critical problem-solving, and the meaningful work of protecting digital infrastructure. Social media campaigns, employee advocacy programs, and authentic storytelling about cybersecurity professionals' daily experiences can reshape public understanding of cybersecurity careers as exciting, meaningful, and accessible to professionals from varied backgrounds.

7. Talent retention: Retention strategies should address the unique aspects of cybersecurity work that contribute to stress and turnover. Organizations that implement performance evaluation and compensation systems suitable for cybersecurity personnel – with set career progression paths – demonstrate commitment to employee development and retention. Creating career paths beyond purely technical roles, such as dual career tracks that recognize leadership on one track and technical mastery on another, can remove the pressure to lead in order to be promoted. Continuous learning such as access to training platforms and certification support can help build internal capabilities and reduce external recruiting pressure.

8. Flexible working and wellbeing: Flexible work arrangements and remote working enable organizations to access broad talent pools while accommodating diverse lifestyle preferences. Remote work capabilities allow recruitment beyond geographic constraints, tapping into international expertise and professionals preferring locations outside major cities. This flexibility is particularly appealing to younger professionals and women valuing work-life balance. In security operations, with the constant pressure of threat response and high-stakes decisions, providing flexibility and mental health support can help attract and retain talent that may have otherwise been driven away.

Building the future talent pipeline

9. School education: One approach to addressing future talent pipeline challenges is to rethink cybersecurity education from foundational levels. If high schools do not currently have formal cybersecurity foundational learning, it could be a missed opportunity to engage younger students. Integrating foundational cybersecurity concepts into school education curricula can spark early interest and build awareness among the next generation. Subjects such as digital literacy, online safety, and cybersecurity basics can help drive interest in cybersecurity careers and contribute to a sustainable talent pipeline.

10. Policy reforms: Policy reforms could help to address structural barriers in Japan's cybersecurity talent pipeline. For example, reforming the RISS certification model to increase accessibility and reduce expensive certification costs can lower entry barriers for aspiring professionals. Although Japan's Ministry of Economy, Trade and Industry will introduce a system that exempts individuals with specific practical experience from attending the training required at the time of license renewal, it will not significantly reduce the initial certification costs.[17] Additionally, continuing to revise current policies such as the Specified Skilled Worker program[18] to include cybersecurity can help to accelerate workforce development.

Conclusion: The call to action

Japan's cybersecurity landscape is characterized by a rapidly expanding threat environment and a pressing need for skilled professionals. Despite efforts to scale up the cybersecurity workforce, demand continues to outpace supply and the workforce gap is growing. This cybersecurity workforce challenge will likely define Japan's digital future – it is a societal imperative.

Addressing this gap requires innovative approaches. Various stakeholders, including government agencies, educational institutions, and private sector organizations, would benefit from collaborating to develop a future-focused national strategy that addresses the workforce shortage – now and into the future. This may involve redesigning, rethinking, and reimagining the entire talent architecture supporting the cybersecurity workforce.

Looking ahead, Japan could realize a future where the cybersecurity workforce is mission-driven and motivated by societal impact; diverse across gender, age, and geography; emotionally resilient; digitally fluent; and AI-augmented.

The ten recommendations presented offer actionable pathways forward, though they represent starting points rather than complete solutions. Successfully addressing Japan's cybersecurity talent shortage will require sustained commitment, adaptive strategies, and willingness to challenge conventional approaches.

Japan can build a more cybersecure future based on digital trust – where companies can strive for growth, society can be safe online, and national security is maintained. Japan has a history of leading in innovation – now it has the opportunity to lead in the way it develops and empowers the people who protect the nation.

It’s time to secure Japan’s digital future. The nation’s safety depends on it.

Let's talk

Authors and contributors

Authors

Karen Grieve
Director
Deloitte Services Pty Ltd
kagrieve@deloitte.com.au

Asako Iwanaga
Managing Director
Deloitte Tohmatsu Cyber LLC
asako.iwanaga@tohmatsu.co.jp

Key contributors

Eric Leo
Director
Deloitte Services Pty Ltd
eleo@deloitte.com.au

Hideyuki Namiki
Manager
Deloitte Tohmatsu Cyber LLC
hideyuki.namiki@tohmatsu.co.jp

Nicole Scoble-Williams
Partner, Global Future of Work Leader
Deloitte Tohmatsu Consulting LLC
nscoble-williams@tohmatsu.co.jp

Kentaro Sonoda
Specialist Leader
Deloitte Tohmatsu Cyber LLC
kentaro.sonoda@tohmatsu.co.jp

Key contacts

Yuichiro Kirihara
Partner, Japan Cyber leader
Deloitte Tohmatsu Cyber LLC
ykirihara@tohmatsu.co.jp

Asako Iwanaga
Managing Director
Deloitte Tohmatsu Cyber LLC
asako.iwanaga@tohmatsu.co.jp

Endnotes

1. Walter Sim, "Hit by wave of online attacks, Japan shifts to 'active cyber defence'," *The Straits Times*, 20 January 2025.

2. The House of Representatives, Japan, ***サイバー安全保障を確保するための能動的サイバー防御等に係る態勢の整備の推進に関する法律案*** [in Japanese], 16 May 2025.

3. The Japan Times, "12 Japan agencies found vulnerable to cyberattacks," 14 September 2025.

4. Rika Kimura, "Audit finds 16% of Japan government IT systems unprepared for attack," *Nikkei Asia*, 13 September 2025.

5. ISC2, *Employers Must Act as Cybersecurity Workforce Growth Stalls and Skills Gaps Widen*, 10 September 2024.

6. Ibid.

7. Japan Ministry of Defense, *Defense Buildup Program*, [Provisional Translation as of 14 March 2023], pp. 11-12.

8. Ministry of Economy, Trade and Industry, "*Study Group for Promoting the Development of Cybersecurity Talent Compiles and Announces Its Final Report*," press release, 14 May 2025.

9. Statistics Bureau of Japan, ***統計からみた我が国の高齢者*** [in Japanese] (Statistics on Japan's elderly population), 14 September 2025, p. 1.

10. National Institute of Population and Social Security Research, *Population Projections for Japan (2023 revision): 2021 to 2070*, 2023, p. 25.

11. Human Resocia Co., Ltd., "***ITエンジニアの女性比率、日本は18.8%でOECD加盟国中17位、ITおよびSTEM分野卒業者の女性比率は、OECD最下位と将来の女性活躍が危惧される結果に*** [in Japanese]", press release, 7 March 2025.

12. Ministry of Health, Labour and Welfare of Japan, *The Employment Policy Study Group Report: Building an Inclusive Labour Market for All Backgrounds*, August 2024, p. 13.

13. Ministry of Health, Labour and Welfare of Japan, *Age of the 100-Year Life – Current State of Employment Measures for the Elderly*, March 2023.

14. The Tokyo Chamber of Commerce and Industry, ***2025年度 新入社員意識調査 集計結果*** [in Japanese], 21 April 2025, p. 4.

15. Gallup, *State of the Global Workplace: 2026 Report*, April 2026.

16. Ministry of Defense, ***防衛省ＡＩ活用推進基本方針*** [in Japanese], July 2024, p. 8; Ministry of Defense, Press Conference by Defense Minister Kihara [Ministry of Defense Basic Policy on Promoting the Utilization of AI], 2 July 2024.

17. Ministry of Economy, Trade and Industry, "*Study Group for Promoting the Development of Cybersecurity Talent Compiles and Announces Its Final Report*," press release, 14 May 2025; Information-technology Promotion Agency, Japan (IPA), ***講習の目的と概要 | デジタル人材の育成*** [in Japanese], 25 September 2025.

18. Ministry of Foreign Affairs Japan, "Japan is looking for Specified Skilled Workers," accessed 14 October 2025.

Deloitte.
デロイト トーマツ

Deloitte Tohmatsu Group (Deloitte Japan) is a collective term that refers to Deloitte Tohmatsu Group Japan LLC, which is the Member of Deloitte Asia Pacific Limited and of the Deloitte Network in Japan, and firms affiliated with Deloitte Tohmatsu Group Japan LLC that include Deloitte Touche Tohmatsu LLC, Deloitte Tohmatsu LLC, Deloitte Tohmatsu Tax Co., and DT Legal Japan. Deloitte Tohmatsu Group is known as one of the largest professional services groups in Japan. Through the firms in the Group, Deloitte Tohmatsu Group provides professional services in accordance with applicable laws and regulations. With more than 20,000 people in over 30 cities throughout Japan, Deloitte Tohmatsu Group serves a number of clients including multinational enterprises and major Japanese businesses. For more information, please visit the Group's website at www.deloitte.com/jp.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("Deloitte Global"), its global network of member firms, and their related entities (collectively, the "Deloitte organization"). Deloitte Global and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. Deloitte Global and each of its member firms and related entities are liable only for their own acts and omissions, and not for those of one another. Deloitte Global does not provide services to clients. Please see www.deloitte.com/about to learn more.
Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of Deloitte Global. Members of Deloitte Asia Pacific Limited and their related entities, each of which is a separate and independent legal entity, provide services from more than 100 cities across the region, including Auckland, Bangkok, Beijing, Bengaluru, Hanoi, Hong Kong, Jakarta, Kuala Lumpur, Manila, Melbourne, Mumbai, New Delhi, Osaka, Seoul, Shanghai, Singapore, Sydney, Taipei and Tokyo.

Deloitte provides leading professional services to nearly 90% of the Fortune Global 500® and thousands of private companies. Our people deliver measurable and lasting results that help reinforce public trust in capital markets and enable clients to transform and thrive. Building on its 180-year history, Deloitte spans more than 150 countries and territories. Learn how Deloitte's approximately 460,000 people worldwide make an impact that matters at www.deloitte.com.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited ("Deloitte Global"), its global network of member firms, or their related entities (collectively, the "Deloitte organization") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of Deloitte Global, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. Deloitte Global and each of its member firms, and their related entities, are legally separate and independent entities.

Member of
Deloitte Touche Tohmatsu Limited

IS 669126 / ISO 27001

BCMS 764479 / ISO 22301

Please see here for the scope
of IS/BCMS certifications
https://www.bsigroup.com/clientDirectory