

PERSPECTIVE · 15 OCTOBER 2026

Japan, Cyber Emergency, and Truth

Dear CEO (of a Japanese company, or their customers),

Executive summary

- Japan has **not** declared a state of emergency. The word came from a ruling-party politician at a party meeting on 9 October 2026, and a foreign headline the same evening turned it into a declaration. The government's own notices ask and advise; none invokes emergency powers.
- **The wave of attacks is real and deserves board attention.** In September, 86 incidents were publicly disclosed, 37% more than in July, and shared providers carried single intrusions into hundreds of organisations at once.
- **These breaches are not distinctively Japanese.** The routes described by JPCERT/CC and the victims include known vulnerabilities, abused application interfaces and administrative functions, and malware on a contractor's PC. JPCERT/CC reports that the same attack servers also targeted web services provided outside Japan.
- **The lessons are concentration risk and thin layers of defence.** One cloud provider's ransomware reached 495 customers; one inquiry-handling service reached a securities house, a non-life insurer, a life insurer, a watchmaker and, through the broker, two regional banks.
- **Concentration risk needs statutory oversight of critical third parties.** Japan has no regime of the kind the EU and UK operate, and their lists are too narrow to catch the domestic concentrations that failed here.
- **Defence in depth and resilience should not wait for a domestic rulebook.** Operational resilience regimes abroad already describe what good looks like, and Japanese companies should not wait for the JFSA and others to write new rules on resilience.

The emergency was a headline rather than a declaration

On the morning of 9 October 2026, the Liberal Democratic Party's own 国家サイバーセキュリティ戦略本部, a party body, met to discuss the breaches. Its chair, Masaaki Taira, was Digital Minister and minister in charge of cyber security from October 2024 to October 2025. He said:

「サイバー空間の有事と言っていいと思います。サイバー空間の非常事態と言ってもいいと思いますので、これに対して政府を挙げて取り組む必要があると思います」

“I think we can call this a contingency in cyberspace. I think we can also call it an emergency in cyberspace, so the whole of government needs to address it.”

The party's own account, published on 14 October, quotes him more firmly: 「現在は非常事態、有事という状況」, “we are now in a state of emergency, a contingency”. Neither version describes an act of government.

That evening, Japan time, the Financial Times ran the headline “Japan declares cyber space emergency as attacks soar”. By 13 October the claim had passed through technology sites, a prediction-market account on X, The New York Times and translations in Eastern Europe that rendered it as a legal state of emergency. Most dropped the party attribution, and none of those that reported a declaration kept his “I think we can call”.

The government's own record is different. The statutory Cybersecurity Strategic Headquarters, chaired by the Prime Minister, has not met since 14 September 2026, when it met by circulation. On 8 October the National Cybersecurity Office convened ministries, where Toshiharu Furukawa, the Digital Minister, who also holds the cyber security portfolio, described the situation as 「大変、危急の状況」, “a very critical situation”. Between 7 and 13 October the Personal Information Protection Commission, the National Police Agency, the National Cybersecurity Office, the Financial Services Agency (JFSA), MIC, METI, MHLW, IPA, JPCERT/CC and NICT issued advisories. Each asks, advises or restates existing legal duties; none imposes a new obligation or invokes emergency powers.

Japanese law has no procedure for declaring a cyber emergency as such. Its general emergency powers, from an armed-attack or mass-casualty situation under the contingency laws to a police or disaster emergency proclamation, each need an act of the Cabinet or Prime Minister and the approval of the Diet, and none was used. The main provisions of the Active Cyber Defence laws came into force on 1 October 2026, including incident reporting and police and Self-Defence Forces access and neutralisation measures; none of them involves a declaration.

For boards, two conclusions follow: read the primary documents before the headlines, and treat the absence of a declaration as saying nothing about the size of the problem.

The attacks are real, and their scale has changed

Five of the largest figures below are confirmed thefts. The others are upper bounds of possible exposure, and some have since been withdrawn.

ORGANISATION	WHAT HAPPENED	SCALE, AS DISCLOSED
IDC Frontier (SoftBank group)	Ransomware on its IDC F Cloud from 7 October	495 corporate and local-government customers affected; on 14 October it reported no data leak from customer servers and recovered snapshot backups for 194 customers
Nissui Logistics	Hosted on IDC F Cloud	Shipping and receiving halted at all 17 centres from 7 October; partial restart on 9 October
JR East, View Card, JR Kyushu	External email-delivery services on IDC F Cloud	About 2.06m, 4.03m and 1.3m records at risk; on 15 October all three reported that no leak had occurred
Scala Communications (i-ask)	Inquiry-handling service accessed 2 to 3 October	Data of Daiwa Securities (about 110,000 customers), Sampo Japan, Orix Life and Citizen possibly taken; Shikoku Bank and Iwate Bank affected through Daiwa
Arcadia (SpeeCAN RAIDEN)	Municipal alert-mail service, intrusion detected 11 October	Up to about 3.14m email addresses possibly exposed; servers stopped from 13 to 15 October
Medley (@link)	Medical-institution system suspended on 14 October	Up to 787 medical institutions potentially affected
Daiichikosho (Big Echo)	Malware on a PC at contractor Nippon Columbia Group, 1 to 2 October	About 8.72m records possibly exposed
Adventure (skyticket)	Servers accessed 2 to 4 October	About 14.64m records leaked
Monogatari (Yakiniku King)	App membership system, access confirmed 2 October	10.79m users' data leaked
Times Car (Times Mobility, Park24 group)	Intrusion detected 25 September	About 6.6m accounts taken, with identity-document images for about 1.6m
Bookoff	Membership data taken 4 to 6 October	6.43m records leaked, including password hashes
Lawson	Lawson ID accessed 12 to 14 September, identified 7 October	2.16m records leaked

These figures overlap and measure different things, so they must not be added together. The counts of incidents show the change more reliably. TrendAI counted 86 publicly disclosed incidents in September, 37% more than in July, and more in the first nine months of 2026 than in the whole of 2025. Tokyo Shoko Research counted ten leaks of more than one million

records by listed companies by 5 October, against six in all of 2025. No authority or victim has named a threat actor for any of the major incidents.

On the surface that was attacked, these victims look like their peers abroad

JPCERT/CC describes four attack patterns behind the wave: scanning for known vulnerabilities and misconfigurations, abuse of application interfaces (some found by analysing public smartphone apps), exploitation of a Metabase SQL injection flaw (CVE-2026-72898) on the US list of known exploited vulnerabilities since 11 August 2026, and web shells. On 15 October it added that the attackers used AI for vulnerability scanning and interface attacks, and that the same attack servers also targeted web services provided outside Japan. Where victims have disclosed the route, it was abuse of administrative functions, abuse of an in-app display mechanism, an unauthorised login to an administrative site or malware on a contractor's PC.

None of these is a Japanese weakness. BeatQuantum has measured the external security posture of 17 organisations caught up in the wave and of 51 comparable firms in Europe, North America and Asia. On web-facing posture, the surface this wave exploited, the Japanese victims cannot be told apart from their peers. Their email posture trails the peers; no victim has named email as the route in, but it is worth fixing. The results are available on request.

The external surface therefore does not explain the scale of this month's damage. We see two causes: concentration of shared services, and too few layers between an intruder and the data.

Concentration risk turned single intrusions into a national story

The incidents with the widest reach came through shared providers. IDC Frontier's ransomware reached 495 customers, from a food-logistics company to prefectural websites and railway email systems. Scala Communications' inquiry-handling service carried one intrusion into the data of a securities house, a non-life insurer, a life insurer and a watchmaker, and through the broker to two regional banks. From 13 October, Arcadia's municipal alert-mail service and Medley's system for medical institutions have added local authorities and up to 787 clinics and hospitals. Each customer had done its own procurement diligence, and nobody held a view of the aggregate.

That aggregate view is what critical third-party regimes exist to provide. Under the EU's Digital Operational Resilience Act, the European Supervisory Authorities oversee designated providers directly, each through a Lead Overseer. On 18 November 2025 they designated 19: cloud providers, telecoms and data-centre operators, market-data and financial-software firms, and integrators, including Tokyo-headquartered NTT DATA. HM Treasury designated

four in the UK from 13 July 2026: the Irish and Luxembourg entities of Microsoft, Google Cloud and Amazon Web Services, and Oracle's UK company.

Japan has no equivalent. Its only direct regime for technology providers is narrow: a July 2026 amendment will require firms that supply custody systems to crypto-asset exchanges to notify the JFSA in advance. A government expert panel proposed in January 2026 that data centres and cloud services be brought within economic-security law, but the proposal was left out of the amendment enacted in June. The Economic Security Promotion Act screens the critical equipment that 258 designated infrastructure operators in 15 sectors install, and the contractors they entrust to maintain it, for the risk of interference from abroad. Since 1 October 2026 the Active Cyber Defence regime has obliged the same operators to report incidents affecting their critical systems. Neither designates or supervises the providers on which many firms depend at once. The JFSA can demand reports from, and inspect, a bank's contractors, one bank at a time.

In our view, Japan's concentration risk will not be addressed until it has effective statutory oversight of critical third parties. We would go further: the EU and UK lists are not good enough. Each sees a provider only through the services it supplies to its own financial sector, and DORA exempts providers whose services go only to financial entities active in a single member state. A domestic cloud such as IDC Frontier, which markets itself as a sovereign cloud, will never appear on them, and nor will an inquiry-handling service, a municipal alert-mail service or a system for medical institutions. These are the concentrations that failed this month. **The list must be wider and longer, and each jurisdiction must draw it around its own economy, across all sectors rather than finance alone.**

Defence in depth and resilience cannot wait for a domestic rulebook

Some intrusions ran for weeks before discovery: Lawson's systems were accessed from 12 to 14 September and the breach was identified on 7 October. Others were found within a day, by which time millions of records had already left. The notices do not say whether stored data was encrypted, and skyticket and Bookoff held passwords only as hashes. Several do show that an intruder who reached the application or its administrative functions could read customer records in bulk. Layers behind the application, such as segmentation, monitoring of bulk reads, encryption under keys the application cannot freely use, and retention limits, reduce what each intrusion yields. The National Cybersecurity Office's advisory now asks firms to hold less, delete what they no longer need, encrypt what they keep and watch for bulk retrieval.

Resilience is the second requirement. IDC Frontier has recovered snapshot backups for 194 of its 495 affected customers; the others depend on backups of their own. Nissui Logistics restarted part of its operation two days after the attack and expects all sites to return to normal next week, on servers outside IDC Frontier. The question each affected firm now faces is one that operational resilience regimes abroad ask in advance: which services matter most to customers, how long can each be disrupted before the harm becomes intolerable, and can the firm stay within that limit through a severe but plausible disruption at a provider it does not control.

The JFSA set out its approach to operational resilience in an April 2023 discussion paper, wrote it into its supervisory guidelines for major banks that June, and added cybersecurity guidelines covering third parties in October 2024. All of it is principles-based. Most of this month's victims, from car sharing to karaoke and restaurant chains, fall outside financial regulation altogether. Japanese firms do not need to wait for the JJFSA to turn principles into rules. The UK's PRA SS1/21, in force since March 2022 and fully phased in since March 2025, Australia's CPS 230, in force since July 2025 and explicit about material service providers, and DORA already describe what good looks like. Any firm can adopt the discipline voluntarily: identify important business services, set impact tolerances, map the third parties behind each service, and test against severe but plausible scenarios.

Five questions for the board this quarter

1. Which of our important services depend on a provider that also serves many other firms, and what happens to us if that provider is encrypted tomorrow?
2. Do we hold our own restorable backups of data hosted by every critical provider, and when did we last restore from them?
3. If an attacker were inside our customer database for three weeks, what would tell us, and how much could they read?
4. Which contractors hold or process our customer data on their own devices and services, and what assurance do we have over them?
5. Have we set an impact tolerance for each important service, and could we stay within it through a provider failure of the kind seen this month?

What concerns us most

Our concern lies with the political reluctance to take a hard stance against the concentrations that matter, rather than with the headlines. A handful of shared providers now sit beneath the services on which whole economies run, and the oversight built around them covers few

providers and stops at national and sectoral borders. Left unaddressed, that reluctance could eventually do lasting damage to countries and to the world that depends on them.

Errors and omissions are expected in this article. I had to use AI for the Japanese text and its interpretation. Please be gentle, if I got it wrong.

Yours sincerely,

Santosh Pandit

Founder, BeatQuantum

[BeatQuantum.com](https://beatquantum.com) | [SantoshPandit.com](https://santoshpandit.com) | contact@santoshpandit.com

References

1. KSB/ANN, 「サイバー空間の有事」自民党がサイバー防御の会合開催, 9 October 2026.
<https://news.ksb.co.jp/ann/article/16953985>
2. Liberal Democratic Party, サイバーセキュリティ有事に対峙, 14 October 2026.
<https://www.jimin.jp/news/information/214364.html>
3. Financial Times, “Japan declares cyber space emergency as attacks soar”, 9 October 2026 (archived).
<http://web.archive.org/web/20261010162655/https://www.ft.com/content/2d4333d1-8119-44a4-a5a5-2ee9ef2544fa>
4. KSB/ANN, inter-ministerial meeting and Minister Furukawa’s remarks, 8 October 2026.
<https://news.ksb.co.jp/ann/article/16951387>
5. National Cybersecurity Office, Cybersecurity Strategic Headquarters meetings.
<https://www.cyber.go.jp/council/cs/index.html>
6. National Cybersecurity Office, 不正アクセスによる漏えい等の事案を踏まえた対応について, 9 October 2026.
<https://www.cyber.go.jp/pdf/press/taiou.pdf>
7. National Cybersecurity Office, 不正アクセスによる漏えい等の事案を踏まえた各機関による注意喚起等について, 14 October 2026. <https://www.cyber.go.jp/news/20261014.html>
8. Cabinet Office and National Cybersecurity Office, サイバー対処能力強化法等の施行について, September 2026.
<https://www.cao.go.jp/cybersecurity/pdf/sekousetsume.pdf>
9. JPCERT/CC, 直近で相次いでいる国内組織における不正アクセスに関する注意喚起 (JPCERT-AT-2026-0030), 8 October 2026, updated 9 October. <https://www.jpccert.or.jp/at/2026/at260030.html>
10. JPCERT/CC Eyes, web API attacks, 15 October 2026.
https://blogs.jpccert.or.jp/ja/2026/10/web_api_attacks.html
11. NIST National Vulnerability Database, CVE-2026-72898. <https://nvd.nist.gov/vuln/detail/CVE-2026-72898>
12. IDC Frontier, fifth report on unauthorised access, 14 October 2026.
<https://www.idcf.jp/news/topics/20261014001>
13. Nissui, third notice on the Nissui Logistics system failure, 14 October 2026.
<https://www.nissui.co.jp/news/20261014.html>
14. JR East, notice on the external email-delivery service, 9 October 2026, updated 15 October.
https://www.jreast.co.jp/press/2026/20261009_ho02.pdf
15. View Card, notice of 15 October 2026. <https://www.jreast.co.jp/card/news/pdf/20261015.pdf>

16. JR Kyushu, notice of 15 October 2026.
https://www.jrkyushu.co.jp/common/inc/news/newtopics/__icsFiles/afieldfile/2026/10/15/202691015_mail_address_access.pdf
17. Daiwa Securities, timely disclosure, 5 October 2026. <https://ssl4.eir-parts.net/doc/8601/tdnet/2891437/00.pdf>
18. Arcadia, SpeeCAN RAIDEN notice, October 2026. <https://www.arcadia.co.jp/info/4076>
19. Medley, timely disclosure on @link, 14 October 2026.
<https://www.release.tdnet.info/inbs/140120261014550839.pdf>
20. Lawson, 第三者による不正アクセスに伴う個人情報漏えいに関するお詫びとお知らせ, 8 October 2026, updated 13 October. https://www.lawson.co.jp/contents/cont07/1533174_3310.html
21. Reuters via NBC News, “South Korea and Japan are buffeted by hacks as AI lowers bar for cybercriminals”, 9 October 2026. <https://www.nbcnews.com/world/asia/south-korea-japan-are-buffeted-hacks-ai-lowers-bar-cybercriminals-rcna602464>
22. Tokyo Shoko Research, large-scale personal-data leaks by listed companies, October 2026. https://www.tsr-net.co.jp/data/detail/1203305_1527.html
23. European Supervisory Authorities, list of designated critical ICT third-party providers, 18 November 2025.
https://www.esma.europa.eu/sites/default/files/2025-11/List_of_designated_CTPPs.pdf
24. HM Treasury, “UK financial system strengthened with new safeguards for major technology providers”, 10 July 2026. <https://www.gov.uk/government/news/uk-financial-system-strengthened-with-new-safeguards-for-major-technology-providers>
25. Financial Services Agency, Bills submitted to the 221st Diet session (Financial Instruments and Exchange Act and Payment Services Act amendment), 2026. <https://www.fsa.go.jp/common/diet/221/index.html>
26. Cabinet Secretariat, expert panel on economic security legislation, recommendation outline, 16 January 2026. https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/r8_dai14/teigenkosshi_6.pdf
27. Financial Services Agency, ディスカッション・ペーパー オペレーショナル・レジリエンス確保に向けた基本的な考え方, April 2023. <https://www.fsa.go.jp/news/r4/ginkou/20230427/02.pdf>
28. Financial Services Agency, 金融分野におけるサイバーセキュリティに関するガイドライン, 4 October 2024.
<https://www.fsa.go.jp/news/r6/sonota/20241004/20241004.html>
29. Prudential Regulation Authority, SS1/21 Operational resilience: Impact tolerances for important business services, March 2022. <https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/supervisory-statement/2021/ss121-march-22.pdf>
30. Australian Prudential Regulation Authority, CPS 230 Operational Risk Management.
<https://www.apra.gov.au/standards/cps-230>

Company figures are taken from each organisation’s own notice; full sources are in the companion research report.