Atsumi & Sakai Newsletter
JAPAN
NEW YORK
LONDON
FRANKFURT
BRUSSELS
HO CHI MINH

September 2026
No. EID_004

Japan's New Cyber Incident Reporting Regime: What Foreign Cloud and Software Providers Should Review Before 1 October 2026

This article reflects laws, subordinate legislation and official materials published as of 28 September 2026.

Key takeaways

– From 1 October 2026, certain designated Japanese critical infrastructure operators must notify the government of the specified critical computers they use — including relevant computing resources provided through cloud services — and report cyber incidents on short reporting timelines. Foreign cloud and software providers are not direct incident-reporting entities merely by virtue of being providers.

– The regime attaches to what an operator uses, not what it owns: a cloud service hosted outside Japan can fall within scope, and, where notification is required, the service name and provider name go into a government filing (existing systems must be notified by 31 March 2027).

– The Act's supplier provisions (Article 42) reach suppliers outside Japan that supply covered computers, programs or services to persons in Japan: government vulnerability information, requests for remedial measures, and an effort-based duty to respond to requests for reports and materials.

– The first demands will come from customers, not the government: expect requests for notification data and renegotiation of incident-notification clauses and SLAs against rapid reporting timelines that the draft commentary interprets as "as soon as possible" for DDoS and three to five days from recognition for ransomware and other reportable incidents.

– Before 1 October: map exposure to the 258 designated operators, prepare notification data, review SLAs, document vulnerability-response (PSIRT) arrangements, and assign an owner for Japanese government contact.

1. Why this matters outside Japan

On 1 October 2026, the core notification and incident-reporting provisions of Japan's Act on Prevention of Harm Caused by Unauthorized Acts against Critical Computers (Act No. 42 of 2025) take effect. In the government's tentative English translation the statute is called the Cyber Response Capability Strengthening Act; in public debate it is better known as Japan's "active cyber defense" law.[1] The direct obligations fall on certain designated Japanese critical infrastructure operators. Foreign cloud and

[1] Act on Prevention of Harm Caused by Unauthorized Acts against Critical Computers (Act No. 42 of 2025) (the "Act"); Government of Japan, Cybersecurity Strategy (Cabinet decision, 23 December 2025), tentative English translation (the "Strategy"; for the official English names of the Act and the Related Laws Development Act, and the definition of "suppliers of computers" at n. 20).

software providers are nonetheless affected through three distinct channels, none of which requires a Japanese subsidiary or any physical presence in Japan.

First, the regime attaches to computers that a designated operator uses, not those it owns. Computing resources provided through a cloud service — even one hosted and operated entirely outside Japan — can fall within the "specified critical computer" framework, and, where notification is required, the service name and provider name will appear in the operator's statutory notification to the Japanese government. Second, the Act builds a vulnerability-response framework around "suppliers of computers" — a defined term that expressly reaches providers of services that make computers or programs available for another person's information processing, and thus cloud services — and provides that this framework also applies to suppliers located outside Japan where they supply covered computers, programs or services to persons located in Japan (Article 42).[2] Third, and in practice most immediately, designated operators facing statutory reporting deadlines measured in days are likely to translate those deadlines into contract amendments, security questionnaires and SLA renegotiations across their supply chains.[3] Providers that wait for a request from the government will find that the first demands arrive from their customers.

2. What takes effect — and what does not

For private companies, what takes effect on 1 October 2026 is the government-facing core of a much larger package: the obligation of certain critical infrastructure operators to notify the government of the important computers they use, and to report cyber incidents affecting those computers.[4] The core implementing cabinet order and the Reporting Order have been promulgated and will take effect on 1 October 2026; the commodity-product exclusion designation, the statutory designation of the applicable report forms, and the revised common reporting arrangement and Forms 1–3 were finalized on 15 September 2026. The detailed administrative commentary, however, remained pending as of this writing. Because it contains much of the practical detail discussed below, the final version should be consulted once published.[5]

Equally important for a foreign reader is what the regime is not. It is not a breach-notification law aimed at providers: no new filing obligation attaches to a foreign vendor as such. The communications-information provisions — the part of the law most often covered in the international press — enter into force on a separate date to be specified by cabinet order, no later than 23 November 2027, and are not the subject of this article.[6] And the access and neutralization powers that take effect on 1 October 2026 are

---

[2] Id.

[3] Separately, the Critical Infrastructure Unified Standards, adopted by the Cybersecurity Strategy Headquarters on 31 July 2026 and scheduled to take effect on 1 October 2026, establish unified standards for government measures intended to promote cybersecurity across critical infrastructure. Part 3 identifies measures that sectoral standards should prescribe for operators, including assessment of supplier and contractor security, supply-chain risk management and cybersecurity requirements for the products and services they procure or use. That framework covers a different, though overlapping, population of operators from the designations discussed here. See National Cybersecurity Office, critical infrastructure materials. On 11 September 2026, the National Cybersecurity Office published the Guidelines for Developing Cybersecurity Standards for Critical Infrastructure (provisional translation), which provide detailed reference points for the sectoral standards described above and are scheduled to take effect on 1 October 2026. The previous guidelines for developing sectoral safety standards are scheduled to be abolished on the same date.

[4] The Act was passed on 16 May 2025 together with the Related Laws Development Act (Act No. 43 of 2025), as part of a package that also covers public-private information sharing, government acquisition and analysis of certain communications information, provision of analyzed threat information to the private sector, access and neutralization measures carried out by the police and Self-Defense Forces, and a new institutional structure centered on the National Cybersecurity Office (established 1 July 2025). See Cabinet Secretariat / Cabinet Office, overview materials. The Order for Enforcement of the Act (Cabinet Order No. 47 of 2026, promulgated 23 March 2026) and the Order on Reports of Specified Infringement Events etc. by Special Social Infrastructure Operators (promulgated 28 May 2026) (the "Reporting Order") are in force as of the effective date. A technical amendment to the Reporting Order was finalized on 31 August 2026 (public comment case no. 095260660), adjusting transitional treatment for certain operators newly designated following specified corporate or business succession events; it does not affect the core 1 October obligations discussed here.

[5] Designation of products excluded from the notification obligation, and designation of the forms for reports of specified infringement events, published in the Official Gazette of 15 September 2026 (joint notices nos. 1 and 2), both effective 1 October 2026. The draft administrative commentary on notifications of specified critical computers and reports of specified infringement events (public comment opened 15 July 2026) (the "Draft Commentary") remained pending in final form as of this writing.

[6] The Act, supra note 1.

powers of the Japanese state; the law does not authorize private "hack-back" by companies, Japanese or foreign.

3. Who bears the direct duties: your customers

The obligated entities are "special social infrastructure operators" (tokubetsu shakai kiban jigyosha): entities designated as critical infrastructure operators under Japan's Economic Security Promotion Act — 258 designated operators as of 1 July 2026, in sectors ranging from energy, transport and telecommunications to finance and broadcasting — that use one or more "specified critical computers," meaning computers whose compromise could stop or degrade the operator's designated critical equipment.[7] The test is use, not ownership: systems owned by group companies, systems located overseas, and third-party cloud services are all within the frame if the designated operator uses them for the covered business.

Nor is the category limited to the operational core. The draft commentary's candidate types include, among others, internet-facing systems assigned global IP addresses, authentication and authorization platforms, network control devices, repositories of credentials and configuration data, and systems that regularly feed data into critical equipment.[8] Foreign-provided identity platforms, VPN appliances, WAFs and cloud-hosted data stores can all sit inside these categories.

4. Notification: where your product name appears

Special social infrastructure operators must notify their sector regulator of each specified critical computer: newly introduced systems within four months of introduction as a rule, and systems already in use on 1 October 2026 by 31 March 2027. The statutory notification items include the product name and manufacturer name — and, for cloud services, the service name and provider name.[9] Not every component is notified: purpose-built systems and designated commodity products can fall outside the notification duty, and for non-appliance systems the notification focuses on the software stack rather than hardware — but a product excluded from notification does not necessarily fall outside the incident-reporting net.[10]

The practical consequence for a foreign vendor is visibility: if your software or cloud service is part of a designated operator's critical estate and notification is required, your name becomes part of the government-facing record of the covered components and services in that operator's critical environment. That record is intended to be operational, not merely static: the Basic Policy contemplates matching notification data against incident and vulnerability information and using the filed asset information to help target vulnerability information to affected operators; where a vulnerability is material to an operator's service, the sector regulator is expected to seek implementation of appropriate measures.[11] Expect customers to ask you, before the filing deadlines, for the statutory items — accurate product or service names and manufacturer or service-provider names — and, on a cooperative basis, for the identity of the relevant contracting entity within your group and for version and configuration information.

---

[7] Cabinet Office, designation status of specified social infrastructure operators under the Economic Security Promotion Act (as of 1 July 2026). The 15 current sectors are electricity, gas, oil, water, rail, trucking, shipping, ports, aviation, airports, telecommunications, broadcasting, postal services, finance and credit cards; a June 2026 amendment adds the medical sector, but that addition was not yet in force as of this writing.

[8] Draft Commentary, supra note 5.

[9] Reporting Order, supra note 4; Draft Commentary, supra note 5.

[10] For appliances (single-purpose devices), the hardware product and manufacturer are notified; for everything else, the notification covers the software stack (operating system, middleware, applications), with hardware and firmware not separately notified under this category. Purpose-built systems developed exclusively for one operator (or a group of affiliated operators) and not marketed generally can fall outside the notification duty, but a configured or customized commercial product does not thereby become "purpose-built," and commodity products are excluded only to the extent designated by the competent ministers. The final designation published on 15 September 2026 designates Microsoft Corporation's Windows and Windows Server for this exclusion. Beyond the statutory items, the Draft Commentary treats certain further information, such as version data, as desirable to submit where feasible rather than legally required. Draft Commentary and final designation, supra note 5.

[11] Basic Policy on preventing harm to critical computers (Cabinet decision, 23 December 2025).

5. Incident reporting: the clock your customers are on

When an operator recognizes a "specified infringement event" — a compromise of a specified critical computer's cybersecurity through malware, unauthorized access or business obstruction — or certain prescribed precursor events, it must report to its sector regulator and the Prime Minister. The ministerial order requires an initial report "promptly" after recognition; the draft commentary concretizes this as "as soon as possible" for DDoS incidents and within three to five days of recognition for ransomware and other incidents, with a detailed report due within 30 days. The final designation of 15 September 2026 assigns common Form 1 to DDoS incidents, Form 2 to ransomware incidents and Form 3 to other reportable incidents.[12] Three design features shape what customers will demand from providers.

– **Failed attacks can be reportable.** For certain particularly important categories of computers, defined precursor events must be reported even where the attack did not succeed — for example, where authentication held or malware was quarantined immediately.[13]

– **"Recognition" is a judgment, not an alert.** The clock starts when the operator can reasonably determine that a reportable event has occurred — a judgment that often depends on information sitting with a cloud provider, SOC or MSSP before it reaches the customer.[14]

– **Enforcement is indirect — and supplier-side requests are different.** The Act does not penalize the occurrence of an incident itself. Failure to make a required report can lead to a corrective order; breach of that order is punishable by a fine. A supplier asked for reports or materials under Article 42(4) is subject to a duty of effort to respond, not to those fines.[15]

The draft commentary itself tells operators to review, in peacetime, what their cloud providers' SLAs and terms of service actually promise about incident notification — which events are notified, through what channel, and how fast.[16] Providers should assume that Japanese critical infrastructure customers will read those clauses closely this autumn, and will ask for more than "promptly."

6. Article 42: the provisions that reach you directly

Separately from the operator-facing duties, the Act builds a vulnerability-response framework around "suppliers of computers" — a definition that covers those who supply computers or programs to be used in critical computers and expressly includes those who provide services enabling others to use computers or programs for information processing (Article 42(1)), language that squarely reaches cloud and SaaS providers, not only software licensors.[17] Under this framework, the government may provide vulnerability information to the supplier; the competent minister may request the supplier to take measures necessary to prevent harm where the vulnerability relates to a specified critical computer; and the authorities may seek reports and materials from the supplier, who is under a duty of effort to respond. The Act provides that these provisions also apply to suppliers located outside Japan where they supply computers, programs or relevant services to persons located in Japan (Article 42(6)).[18]

For suppliers located outside Japan, the Act's territorial reach turns on whether the covered computer, program or service is supplied to a person located in Japan. Separately, the substantive scope extends not

---

[12] Reporting Order, supra note 4; Draft Commentary and the report-form designation, supra note 5; National Cybersecurity Office, revised inter-ministerial arrangement on unified incident reporting and common Forms 1–3 (15 September 2026). Under the implementation structure, the Cabinet Office and other competent government bodies perform the relevant statutory functions under the Act, while the National Cybersecurity Office (NCO), located in the Cabinet Secretariat, provides government-wide cybersecurity coordination. See Basic Policy, supra note 11; National Cybersecurity Office, Overview.

[13] Draft Commentary, supra note 5.

[14] Id.

[15] If an operator fails to make a required Article 5 report or makes a false report, the competent minister may issue a corrective order under Article 6; breach of that order is punishable by a fine of up to JPY 2 million (Article 83). Failure to comply with an Article 9 request for reports or materials, or a false response, is punishable by a fine of up to JPY 300,000 (Article 84); these fines can also be imposed on the corporate entity (Article 86). A supplier asked to provide reports or materials under Article 42(4) is subject to a duty of effort to respond under Article 42(5), not to these fines. The Act, supra note 1.

[16] Draft Commentary, supra note 5.

[17] The Act and the Strategy, supra note 1.

[18] The Act, supra note 1.

only to software currently used in critical computers but also to software with a high probability of future use in them.[19] A foreign provider with meaningful business in Japanese infrastructure, finance or telecom sectors cannot conclusively determine today which of its products will be treated as within scope — but it can, and should, assess its readiness on the assumption that Article 42 may become relevant to some of them.

This statutory framework is complemented by an existing statutory supplier duty and related soft-law guidance: since July 2025, the amended Basic Act on Cybersecurity has imposed on suppliers of information systems a duty of effort to support their users' cybersecurity (Article 7(2)), and in March 2026 METI and the National Cybersecurity Office published the Guidelines on the Roles of Cyber Infrastructure Providers — available in an English excerpt and expressly covering cloud services, embedded software and firmware, and software components. In substance, the Guidelines describe the peacetime posture — a functioning PSIRT, current product-composition data, rapid patch and advisory channels — that allows a provider to respond to an Article 42 request without crisis improvisation.[20]

7. What to review before 1 October 2026

For a foreign cloud or software provider, the pre-deadline review is less about new legal filings — there are none for the provider itself — and more about being ready for two waves: customer demands now, and possible government requests later.

1. **Map your Japanese exposure.** Identify customers among the 258 designated operators (and group companies serving them), and which of your products or services could plausibly sit in the specified-critical-computer categories.

2. **Prepare the notification data customers will request.** The statutory items first — accurate product or service names and manufacturer or service-provider names — organized so that a customer can meet the four-month window or the 31 March 2027 deadline; decide separately how to handle requests for group contracting-entity details and for version and configuration information.

3. **Re-examine incident-notification clauses and SLAs.** Expect requests for defined notification triggers, a first-notice window aligned with the customer's rapid initial-report clock, 24/7 contact points, log retention and production, and forensics cooperation — including shared-responsibility boundaries in cloud offerings.

4. **Stand up (or document) the vulnerability-response machinery.** A reachable PSIRT or security contact for Japanese authorities and customers, disciplined tracking of product composition (including OSS components), and established patch and advisory processes — the substance behind an Article 42 response.

5. **Designate an owner for Japanese government contact.** Article 42 requests may be addressed to the supplier directly, including outside Japan. The response duty is one of effort rather than penalty-backed compulsion, but a non-response would be visible to the Japanese authorities handling the request — decide now which legal entity and which team responds, and with what language capability. The Basic Policy also contemplates delegating some supplier-facing vulnerability-information and coordination functions to IPA, JPCERT/CC and NICT, so providers should ensure that contacts arriving through established vulnerability-coordination channels can be routed internally to the appropriate legal and security teams.[21]

6. **Track the final administrative commentary.** The commodity-product exclusion, the statutory designation of the applicable report forms, and the revised inter-ministerial arrangement and common Forms 1–3 were finalized on 15 September 2026. The administrative commentary remained

[19] METI and National Cybersecurity Office, Guidelines on the Roles of Cyber Infrastructure Providers (31 March 2026; English excerpt available) (the "Guidelines"), § 5.7(2).

[20] Id. The Guidelines set out expectations across six areas: secure development and supply; software supply-chain management, including SBOM practices; vulnerability handling; organizational capability; stakeholder cooperation; and customer-side secure procurement. Section 5.7 expressly explains how this framework relates to Article 42. Neither the Act nor the Guidelines imposes a blanket SBOM mandate; the Guidelines treat SBOM as recommended practice rather than a universal legal requirement. Press release: METI.

[21] Basic Policy, supra note 11.

pending as of this writing. Its final version may still affect practical points that matter to vendors — including how the appliance/software distinction is applied and the practical interpretation of the precursor-event categories.[22]

7. **Watch the new information-sharing council.** A public-private council under the Act is scheduled to be launched on 1 October 2026, with infrastructure operators and computer and software suppliers expected to participate as private-sector members — a channel worth monitoring for foreign providers with significant Japanese infrastructure business.[23]

8. Timeline

Date	Event
16 May 2025	Act passed by the Diet (promulgated 23 May 2025), together with the accompanying Related Laws Development Act (Act No. 43 of 2025).
1 July 2025	National Cybersecurity Office (NCO) established; suppliers' duty of effort to support users' cybersecurity added to the Basic Act on Cybersecurity (Art. 7(2)).
23 Dec. 2025	Basic Policy on preventing harm to critical computers adopted by Cabinet decision; new Cybersecurity Strategy adopted the same day.
23 Mar. 2026	Implementing cabinet order promulgated (Cabinet Order No. 47 of 2026).
31 Mar. 2026	Cyber Infrastructure Provider Guidelines published by METI and the NCO (Japanese, with an English excerpt).
28 May 2026	Ministerial order on notifications and incident reports by special social infrastructure operators promulgated.
July–Aug. 2026	Draft administrative commentary, draft report forms and draft designation of excluded commodity products released for public comment in July; the respective comment periods closed between 17 and 25 August 2026.
11 Sep. 2026	National Cybersecurity Office published the Guidelines for Developing Cybersecurity Standards for Critical Infrastructure (effective 1 October 2026; previous guidelines abolished the same date).
15 Sep. 2026	Final commodity-product exclusion designation and statutory report-form designation published in the Official Gazette (effective 1 October 2026); revised inter-ministerial reporting arrangement and common Forms 1–3 published.
1 Oct. 2026	Notification and incident-reporting obligations take effect. Government access/neutralization powers under the Related Laws Development Act also take effect (government powers only). A new public-private information-sharing council is scheduled to be launched the same day.

[22] Supra note 5.

[23] Cabinet Office, materials on implementation of the public-private cooperation provisions (December 2025); National Cybersecurity Office materials indicating the launch of the new public-private council on 1 October 2026.

Date	Event
31 Mar. 2027	Deadline to notify specified critical computers already in use on 1 October 2026.
By 23 Nov. 2027	Communications-information provisions to enter into force on a separate date to be specified by cabinet order, no later than 23 November 2027.

9. Closing observation

Japan's new regime does not deputize foreign providers as reporting entities, and it should not be read as one more mandatory breach-notification law on the global compliance map. Its effect on providers is structural: it can hardwire the identity of suppliers into government filings, gives Japanese ministers a named statutory route to those suppliers, including qualifying suppliers located outside Japan, and puts in-scope critical infrastructure customers on a reporting clock that only works if their providers move first. Providers that approach the new regime as a contract-hygiene and vulnerability-readiness exercise will be better positioned for 1 October. Those that do not will encounter the regime through an urgent customer email.

Where the data behind these systems sits — and which foreign governments can lawfully reach it — raises separate questions of data sovereignty and government access under Japanese law, which we will address in a forthcoming article.

This article is based on materials publicly available as of the date stated above. The Draft Commentary cited above remained subject to change upon finalization; please consult the final text once published.

Author

Yuka Daimon
Partner
E: yuka.daimon@aplaw.jp

Contacts

E-mail: cpg_emergingindustries@aplaw.jp

If you would like to sign up for A&S Newsletters, please fill out the sign-up form.
Back issues of our newsletters are available here.

Atsumi & Sakai is a multi-award-winning, independent Tokyo law firm with a dynamic and innovative approach to legal practice; it has been responsible for a number of ground-breaking financial deal structures and was the first Japanese law firm to create a foreign law joint venture and to admit foreign lawyers as full partners. Expanding from its highly regarded finance practice, the Firm now acts for a wide range of international and domestic companies, banks, financial institutions and other businesses, offering a comprehensive range of legal expertise.

Atsumi & Sakai has an outward-looking approach to its international practice, and has several foreign lawyers with extensive experience from leading international law firms, providing its clients with the benefit of both Japanese law expertise and real international experience.

We are the only independent Japanese law firm with affiliated offices located in New York, London, Frankfurt, Brussels and Ho Chi Minh City which, together with our Tokyo office, Osaka affiliated office and Fukuoka affiliated office, enables us to provide real-time advice on Japanese law to our clients globally.

Atsumi & Sakai

www.aplawjapan.com/en/

Tokyo Head Office
Fukoku Seimei Bldg. (Reception: 16F)
2-2-2 Uchisaiwaicho, Chiyoda-ku, Tokyo 100-0011 Japan

Osaka Affiliate Office
Nakanoshima Festival Tower 16F,
2-3-18 Nakanoshima, Kita-ku, Osaka City, Osaka 530-0005 Japan

Fukuoka Affiliate Office
Tenjin Bldg. 10F
2-12-1 Tenjin, Chuo-ku, Fukuoka-shi, Fukuoka 810-0001 Japan

New York Affiliate Office
1120 Avenue of the Americas, 4th Floor, New York, New York 10036

London Office
85 Gresham Street, London EC2V 7NQ, United Kingdom

Frankfurt Affiliate Office
Barckhausstraße 1 (8th Floor), 60325 Frankfurt am Main, Germany

Brussels Office
CBR Building
Chaussée de la Hulpe 185, 1170, Brussels, Belgium

Ho Chi Minh Office
10F, The NEXUS building
3A-3B Ton Duc Thang Street, Sai Gon Ward, Ho Chi Minh City, Vietnam