[Brief] Who Freezes the Money?

—Only private actors, at home and abroad, can freeze stolen funds. Japan's 66-item emergency package gives its authorities neither a procedure nor a legal basis to ask them

15 November 2026 | Japan Institute for Crisis Management | Miho Funayama | Reading time: about 7 minutes

> **Conclusion: the system that stops intrusion and the system that stops stolen funds are not connected. This is the fifth gap.**

A condensed edition of the full paper. **Independently adapted for readers outside Japan rather than directly translated.** The full text and all five figures are in the main article.

---

1 | What happened

4 November, France. Crédit Mutuel Arkéa (5.8 million customers, €211.5 billion in total assets) was subjected to a cyberattack and **more than €100 million was fraudulently transferred out of its own proprietary account.** Not customer accounts — the bank's own money.

> **An external contractor's platform** (outside supervision) → **the bank's proprietary account** (not customer accounts) → **converted into crypto** (where regulation reaches poorly) → **detected and traced by private parties** (not authorities)

The anomaly was first flagged by the blockchain investigator ZachXBT, **not by any authority.** The bank's communiqué states that part of the funds was **"blocked"** and that recovery is in progress. **Who stopped it, and by what route, has not been disclosed.**

October, Japan. GMO Internet's virtual private servers for automated FX trading were breached and login credentials for trading accounts stored on them were stolen. The Financial Services Agency issued an emergency notice to all FX operators on 22 October; on 27 October the Minister for Financial Services disclosed that five FX firms had reported customer losses.

The entry point is the same. Both were entered through a contractor or shared platform lying outside supervision.

---

2 | Who is supervised, and where attacks enter, do not coincide

The package's own text opens with this:

> In recent breach cases… many instances show that basic controls **at the organisation itself or at its contractors** were inadequate.

The recognition is there. No measure among the 66 items places an obligation on contractors. On 5 November, the day before the decision, Japan's National Cyber Office issued an advisory seeking "strengthened measures across the supply chain as a whole, including contractors." **But it was addressed to the contracting principal, and it ends "we ask that you undertake."**

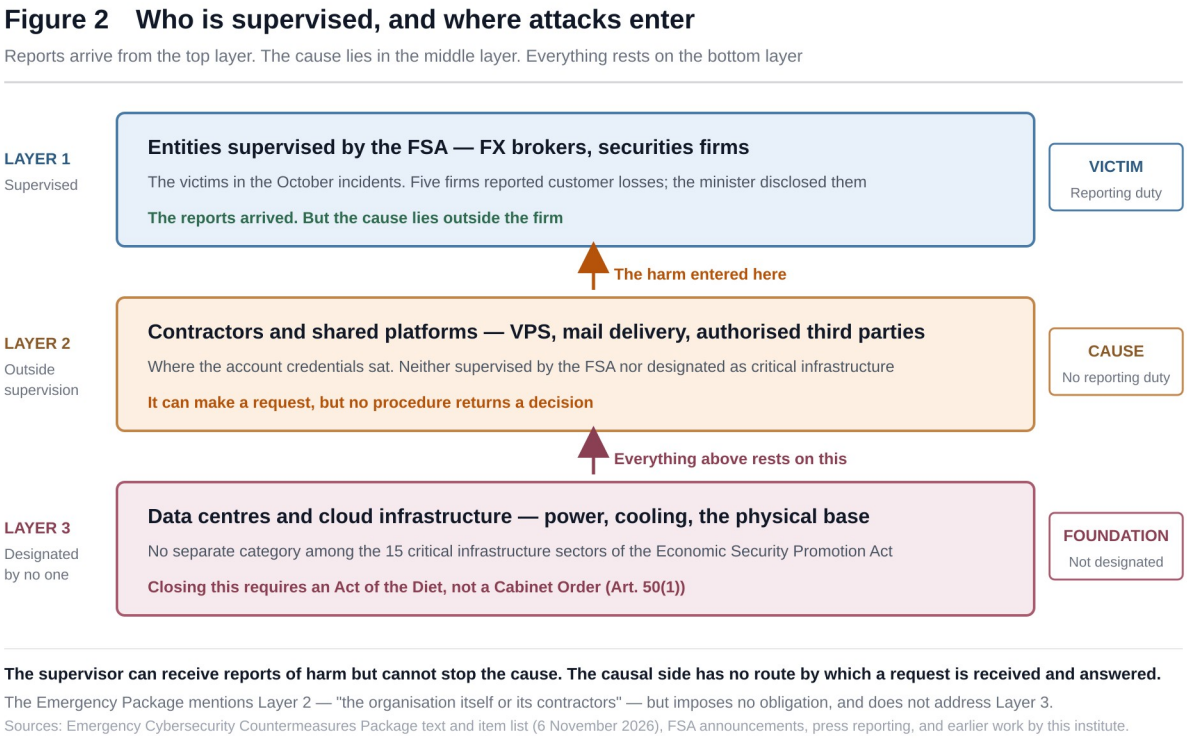


Figure 2: Reports arrive from Layer 1. The cause lies in Layer 2. Everything rests on Layer 3.

On 6 November the FSA published "A Request to Users of Financial Institutions." **The party addressed is the user, and what is asked is self-protection.**

On Layer 3. The package committed to "carry out the necessary institutional arrangements" for telecommunications carriers, but for cloud providers went no further than "encouraging them to join a consultative council." Data centres as facilities — power, cooling, physical protection, siting — are not addressed. **Cloud is treated as a service, not as a facility.** In the UAE in March 2026, an attack on data centres took down **two banks and payment applications** (this institute's "Four-Layer Frame: Failure Cases and Countermeasures"; that was a physical attack, and this paper does not discuss physical attacks on Japan). Finance sits on this layer. **Whether cloud and data centres fall within the institutional arrangements the Ministry of Internal Affairs and Communications is pursuing for carriers is the immediate branching point.**

---

3 | Scoring the Emergency Package (adopted 6 November, 66 items)

Four pillars — basic controls, information collection and analysis, response to attacks, victim support — across 66 items, with approximately ¥10 billion from contingency reserves (¥2bn AI inspection, ¥4.1bn police, ¥3.8bn Digital Agency). **The published breakdown is entirely capacity-building on the government side.** Separately, and **outside the package text**, the Prime Minister instructed that amendment of the Cyber Response Capability Enhancement Act be considered, with extension to domestic communications among the options.

Were the four gaps closed?

Only the fourth (speed) shows partial progress — A2B attacks are named, but minimum standards for public APIs remain untouched. **The first (scope) is acknowledgement only**, with no designation and no obligation. **The second (timing) runs in a different direction**: amendment arose outside the

text, with domestic communications entering the options. **The third (procedure) runs in reverse**: the outreach team is specified as the National Cyber Office "making contact proactively," and the special page opened two days after the decision lists only existing contact points. **The sixth (extortion) is not addressed: the words "ransom" and "ransomware" appear nowhere.**

---

4 | The new gap — who stops the stolen money?

What the package set out to stop is **the circulation of information** (study of suppressing access to sites carrying leaked data). What the French case required was **the stopping of money.** For crypto, the police item list contains "crypto-asset tracing" — **but that is investigative capacity, not a channel.**

Figure 4 Who can freeze funds — a map of authority

Institutions down the side, functions across the top. Only private actors occupy the "immediate freeze" column. No public body does

Institution	Incident intake	Supervision	Investigation	Fund tracing	Immediate freeze
National Cyber Office (NCO) Coordinating body. Neutralisation and takedown	○	△	×	×	×
Financial Services Agency Supervises financial firms only, not their contractors	○	○	×	×	×
National Police Agency Procuring crypto-tracing equipment. FFF preserves logs	○	×	○	△	×
Japan's FIU (National Police Agency) Collects suspicious transaction reports. Separate from the NCO	△	×	△	○	×
Crypto-asset exchanges (private) Only funds passing through their own books. Nothing prompts them	×	×	×	○	△
Stablecoin issuers (foreign private firms) Can freeze immediately on the major chains. No channel to ask them	×	×	×	○	○
No public body occupies this column. Every actor that can is private The problem is not that nobody can stop it, but that Japan has no route for asking those private actors				→	

Key ○ can do it △ limited or voluntary × cannot

Tether reports cumulative involvement in roughly US$4.4 billion of frozen assets across more than 2,300 cases (as of April 2026). The Emergency Package defines none of the following: a route by which an exchange notifies the authorities, a route by which the authorities ask a private actor to freeze, or a procedure connecting FIU data with cyber incident information. This is "Gap 5 — Money."

Source: compiled from the Emergency Package text and item list, the general framework of each scheme, and press reporting. Non-public channels cannot be excluded.

Figure 4: No public body occupies the "immediate freeze" column. Every actor that can is private.

(In this brief, "funds" means money taken from the victim by the attack — property the victim organisation held itself, or assets it held for customers — not the attacker's war chest. "Exit" means where those funds were converted. This differs from the established security term "exit control," which concerns preventing information from leaving.)

Actors able to stop it exist. Stablecoin issuers can freeze addresses immediately for the tokens they issue on the major chains; Tether reports cumulative involvement in roughly **US$4.4 billion across more than 2,300 cases.** But it is **a foreign private company**, it acts on **informal requests** from US authorities, and it is being sued over their lawfulness.

The problem is not that nobody can stop it. It is that Japan's authorities have no procedure and no legal basis for asking those who can. The gap has two shapes and one measure will not close

both. **Domestically, supervisory power exists but no procedure does. Internationally, there is no channel at all.**

Japan already has the precedent. In 2024, roughly ¥48.2 billion in bitcoin left DMM Bitcoin — **and the intrusion began with an employee of Ginco, the contractor managing the wallets.** The business improvement order that followed, under Article 63-16 of the Payment Services Act, **was addressed to DMM Bitcoin.** A statutory duty to manage contractors does exist, at **Article 63-9 (Guidance to Contractors)** — **but its addressee is also the exchange. The law is built to make the principal supervise the contractor.**

---

5 | Recommendations (five items, no new organisation)

#	Recommendation	Verification point
1	**Designate shared digital infrastructure by statutory amendment.** Bring cloud, data centres and cable landing stations within reporting duties. Article 50(1) of the Economic Security Promotion Act enumerates covered businesses in the body of the statute and does not delegate to Cabinet Order, so **this gap cannot in principle be closed by an emergency package.** Include wider scope in the legislative review the Prime Minister ordered	2027 ordinary Diet session
2	**Add a "receive and respond" function to the outreach team.** The decision stays with government; the requesting party is told the outcome, confidentially if necessary	Operating rules (within November)
3	**Design access suppression and domestic communications intelligence together with their oversight.** Condition on strengthening the Oversight Commission; extension to domestic communications is not advisable before controls on foreign-related intelligence are shown to work	On introduction of the bill
4	**Set the procedure and legal basis for stopping funds, separately for domestic and foreign counterparts** (the empty column in Figure 4). **Domestic** — write the exchange-notification and freeze-request procedure into supervisory documents (**achievable without new legislation**, as an exercise of existing powers over registered providers), and connect FIU data to cyber incident information. **Foreign** — decide who asks the issuer, and on what basis (today the operative route is an informal US request). Conditions follow the eight criteria in the predecessor paper	End of March 2027
5	**Adopt a national policy on extortion-type attacks.** A ransom payment reporting scheme (Australian model: within 72 hours), formalised support for firms that refuse, and published after-action reviews	2027 ordinary Diet session

---

Notes on sources and limits

Principal quotations were collated against **the final version** of the package — the version whose title does not carry "(draft)" and which is dated 6 November 2026. That the words "ransom" and "ransomware" never appear was also confirmed there, though equivalent expressions cannot be entirely excluded. The amount and entry point in the French case are unestablished; this brief uses a participant's statement, "more than €100 million." No public information shows that the compromised platform was housed in a data centre, and this brief does not assert it. Issuers' freezing records come

from trade media. Figure 4 is the author's compilation from public sources; non-public channels cannot be excluded. **Freezing by an issuer reaches only assets that have an issuer, so Recommendation 4's foreign limb does not reach Bitcoin or Ether.**

This brief does not assess the vulnerability of any particular financial institution, and does not discuss physical attacks on Japan. The question is not "will Japanese banks be attacked?" but **"does the same entry point and the same exit exist in Japan, and if so, who stops them?"**

For the full source list, please see the references in the main article.

Full article: Who Freezes the Money? — Japan Institute for Crisis Management

https://inst-ds.org/?p=2411

Japanese original: https://inst-ds.org/?p=2375

© 2026 Japan Institute for Crisis Management This brief may be reproduced and distributed freely for policy discussion and citation. Please state the source (publisher and date of publication).