

2026 年 10 月 29 日

口座情報へのサイバー攻撃に「能動的防御」は発動されるか ～能動的サイバー防御とサイバー対処能力強化法・整備法～

資産運用調査部 シニア研究員 重原 正明

1. はじめに

最近さまざまなシステムに対するサイバー攻撃が行われ、社会に混乱が生じている。そのような中、サーバーの貸し出し事業を行っているGMOインターネットグループが、FX口座情報など個人情報を含む自社サーバーへのサイバー攻撃に対し、能動的サイバー防御の実施を政府に緊急要請したと報じられている。

本レポートでは、この能動的サイバー防御と、その根拠法であるサイバー対処能力強化法（以下「強化法」）および同整備法（以下「整備法」）（注 1）について解説する。

2. 国によるサイバー攻撃への対応に関する法

強化法および整備法は、国家安全保障戦略に基づくものとして、2025 年 5 月に成立・公布された。強化法が基本的な対応の枠組みを示し、整備法がサイバー攻撃時の無害化措置や体制整備等、より実務的な事項を規定している。能動的サイバー防御は、整備法のほうに規定されている。

この 2 法の目的については、強化法第 1 条に「そのサイバーセキュリティが害された場合に国家及び国民の安全を害し、又は国民生活若しくは経済活動に多大な影響を及ぼすおそれのある国等の重要な電子計算機のサイバーセキュリティを確保する重要性が増大していることに鑑み、（中略）重要電子計算機に対する不正な行為による被害の防止を図ること」と記されている。具体的な対応としては、官民連携、通信情報の利用、アクセス・無害化措置の 3 点を挙げており、前 2 点は強化法に、最後のアクセス・無害化措置については整備法に記載されている。また官民連携とアクセス・無害化措置については 2026 年 10 月 1 日に施行されているが、通信情報の利用については 2027 年 11 月までに施行されることとされておりまだ施行されていない。

3. 官民連携については基幹インフラ事業者が中心

強化法に規定される官民連携は、電子計算機等のベンダーとともに、経済安全保障推進法上の特定社会基盤事業者（以下「基幹インフラ事業者」）との連携が中心となる。

基幹インフラ事業者は、「特定社会基盤事業を行う者のうち、その使用する特定重要設備の機能が停止し、又は低下した場合に、その提供する特定社会基盤役務の安定的な提供に支障が生じ、

これによって国家及び国民の安全を損なう事態を生ずるおそれ大きいものとして主務省令で定める基準に該当する者」(経済安全保障推進法(2022年6月施行)第50条抜粋)として規定された事業者である。エネルギー、水道、運輸、通信、金融、クレジットカード等の分野から特定社会基盤事業が設定されており、金融分野では銀行、信用金庫・農協等(系統金融)、証券(第一種金融商品取引業)、保険、証券取引所開設、プリペイドカード事業等が「特定社会基盤事業」とされている。特定社会基盤事業を営む全ての事業者が指定されている事業もあるが、金融機関の場合は、社会全体への影響という観点から、一定規模以上の事業者のみが指定されていることが多い。2026年7月1日現在の資料では、ネット銀行やネット証券の一部は含まれている。

強化法では、これら基幹インフラ事業者に対し、次のことを義務付けている。

- ・特定重要電子計算機を導入したときの、製品名等の事業所管大臣への届出
- ・特定重要電子計算機のインシデント情報やその原因となり得る事象を認知したときの、事業所管大臣および内閣総理大臣への報告

一方で、内閣総理大臣または事業所管大臣が重要電子計算機に用いられる電子計算機等の脆弱性を認知した場合には電子計算機等のベンダー等に対して情報提供し、対応方法を公表・周知するほか、基幹インフラ事業者が使用する特定重要電子計算機に用いられる電子計算機等に関連する脆弱性の場合には、事業所管大臣はその電子計算機等のベンダー等に対し、必要な措置を講ずるよう要請することとなっている。

(特定)重要電子計算機の定義については省略するが、大まかにはその機能の低下や停止が基幹インフラ事業者の基幹インフラ業務を妨げるものや特定の国家機密等を扱うものといえよう。

このほかにサイバーインシデント等に関する協議会の設置等も強化法に定められているが、電子計算機のベンダー等を除いた一般事業者とのサイバー関連情報の連携という意味では、基幹インフラ事業者がその中心になると考えられる。

4. 能動的サイバー防御はサイバー通信情報監理委員会の承認のもと、警察と自衛隊が行う

一方、整備法による能動的サイバー防御は、具体的には警察と自衛隊のサイバー対応担当者が、内閣府に置かれる独立性を有する機関であるサイバー通信情報監理委員会の承認のもとに行う(緊急の場合は事後承認も認められる)「アクセス・無害化措置」のことを指す(以下本レポートでは、能動的サイバー防御は「整備法によるアクセス・無害化措置」を意味するものとする)。

警察については「サイバー攻撃又はその疑いがある通信等を認めた場合であって、そのまま放置すれば、人の生命、身体又は財産に対する重大な危害が発生するおそれがあるため緊急の必要がある」(警察官職務執行法(警職法)第6条の2)場合に対応が行われる。対応としては攻撃に関わっているサーバー等の管理者に対する措置の命令のほか、自ら措置を行うこともできる。自衛隊に関しては、国外からの特に高度で組織的なもので、自衛隊が出動すべき要件がある場合に、対応の対象は限られる。

攻撃を受けた側の防御措置にとどまらず、攻撃に利用されているサーバー等(第三者に乗っ取られている場合も含めて)に対して対応を迫るところが一般に「能動的」と称される理由であ

る。

5. 能動的サイバー防御は基幹インフラ事業者でない金融機関への攻撃に対しても発動されるか

能動的サイバー防御の発動の判断においては、警察の場合であれば「そのまま放置すれば、人の生命、身体又は財産に対する重大な危害が発生するおそれがある」と判断されるかどうか重要な鍵となる。

能動的サイバー防御は警察等の判断により発動されるものである。口座乗っ取り等のサイバーインシデント発生の通報は、判断材料の一つとなろうが、それだけで警察等が能動的サイバー防御に乗り出すとは限らない。能動的サイバー防御は（特に緊急の場合）管理者の了解なしに攻撃に関わっているサーバーに手を入れたり、通信を遮断したりすることにもなりかねない。これは攻撃側のサーバーにも善意の利用者がいる可能性等を考えると、簡単にできることではない。

ただ、事業者が基幹インフラ事業者かどうか、という点は、能動的サイバー防御の発動に際して必ずしも絶対的な判断基準とする必要はないと筆者は考えている。基幹インフラ事業者は、社会全体の維持（言い換えると経済安全保障）の意味では重要であり、強化法や整備法の目的である経済安全保障の観点からも重点を置くべき対象ではあるが、犯罪の捜査や個人の財産の保護という面では必ずしも絶対的な区分ではないように思われる。また、例えば病院システムへのハッキング等、人の生命、身体又は財産に影響を与えるシステムは他にもある。

社会全体のシステム維持のための連携体制整備と、犯罪対応とは分けて考えてよいのではないかと筆者は思う。

6. 個人レベルでネットリテラシーを高めつつ、今後の議論を見守ろう

サイバー犯罪の横行に対して、個人レベルでできる対策はいくつかある。パスワードを使い回さない、二段階認証等セキュリティの高い本人認証方式の採用、さらには口座の適正な分散やオフラインでの取引記録の保存も対応の選択肢に入るだろう。偽メールへの対応等も含め、ネットリテラシーの向上は、資産運用にインターネットが不可欠となりつつある現在、資産形成・資産運用の上でも重要なことである。

今回のネットワーク関連企業の要請に対し、国からどのような判断が下るかわからないが、今後事例が積み重ねられていく中で、一定の基準が作られていくこと、またサイバー攻撃への対応の蓄積が進んでいくことを期待したい。

以 上

【注釈】

1) 強化法の正式名称は「重要電子計算機に対する不正な行為による被害の防止に関する法律」、整備法の正式名称は「重要電子計算機に対する不正な行為による被害の防止に関する法律の施行に伴う関係法律の整備等に関する法律」である。

【参考文献】

・内閣官房国家サイバー統括室・内閣府政策統括官（サイバー安全保障担当）（2026）「サイバー対処能力強化法及び同整備法について」

https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo_torikumi/pdf/setsumeir810.pdf

・経済産業省（2026）「特定社会基盤事業者として指定された者」（令和8年7月1日現在）

https://www.cao.go.jp/keizai_anzen_hosho/suishinhou/infra/doc/infra_jigyousya.pdf