認定送信型対電気通信設備サイバー攻撃対処業務に関する政策評価

<table>
<tr><td>根拠法令</td><td>電気通信事業法（昭和 59 年法律第 86 号）第 116 条の２</td><td>評価実施時期</td><td>令和５年 12 月</td></tr>
<tr><td>事務・事業の目的</td><td colspan="3">本業務は、DDoS 攻撃等のサイバー攻撃への対処に取り組む電気通信事業者に対し、サイバー攻撃の送信元となるマルウェア感染機器などの情報を共有すること等によって、電気通信事業者によるサイバー攻撃への対処を支援・促進し、もって電気通信役務の円滑な提供を確保するとともにその利用者の利益を保護することを目的としている。</td></tr>
<tr><td>事務・事業の必要性等</td><td colspan="3">認定送信型対電気通信設備サイバー攻撃対処協会（以下「認定協会」という。）制度は、DDoS 攻撃（※）等のサイバー攻撃への対応を電気通信事業者が共同して行うことを促進するため、サイバー攻撃の送信元に関する情報の共有や、送信元が特定できない場合において送信元を特定するための調査研究等の業務を行う第三者機関を総務大臣が認定するものである。
（※）分散型サービス妨害攻撃（Distributed Denial of Service）。多数の機器から特定の宛先に大量のデータを送りつけることにより、当該宛先のネットワークやサーバを動作不能にする攻撃。

電気通信サービスの安定的提供に支障を及ぼす大規模な DDoS 攻撃等はますます増加しているところ、攻撃通信の受信側の電気通信事業者のみで通信ネットワークの障害に対応することは困難となっており、攻撃通信の送信側の電気通信事業者に対して迅速に情報提供を行い、電気通信事業者が相互に共同して攻撃通信の遮断や利用者への注意喚起等の対処措置を講じる必要がある。しかし、受信側の電気通信事業者が攻撃通信の送信側の電気通信事業者に個別に情報提供を行って対処を実現することは困難であるため、電気通信事業者によって構成される事業者団体が結節点となり、適時・適切に情報共有を行う必要がある。また、電気通信事業者においてサイバー攻撃に対する有効な予防策を講じていくためには、攻撃の送信元（発生源）の情報の活用が必要であり、そのためには、専門的な分析能力を備えた事業者団体において、通信情報を収集、分析・評価し、攻撃の送信元の特定のための調査研究を行い、その成果を電気通信事業者に対して共有する必要がある。加えて、複雑化しているサイバー攻撃に対して電気通信事業者が的確に対処するためには、最新のサイバー攻撃の傾向や防御策等に関する情報が有用であり、サイバー攻撃に関する様々な情報を取り扱う事業者団体から、広く電気通信事業者に対して情報提供を行う必要がある。
認定協会に対して情報提供を行うことができる要件を満たした電気通信事業者（特定会員）数は、制度開始当初から、主要な大手電気通信事業者を含む４社で推移している。
〇特定会員数の推移
<table>
<tr><td></td><td>平成 30 年度</td><td>令和元年度</td><td>令和２年度</td><td>令和３年度</td><td>令和４年度</td></tr>
<tr><td>特定会員数</td><td>４社</td><td>４社</td><td>４社</td><td>４社</td><td>４社</td></tr>
</table></td></tr>
</table>

評価の結果	電気通信役務の円滑な提供に支障を来すサイバー攻撃は、現在も引き続き複雑化・巧妙化が進んでおり、電気通信サービスの利用者にとっての脅威となっている。これまで認定協会においては、本業務として、参照性の高い攻撃事例に関する電気通信事業者への情報提供や、実際に大規模攻撃が発生した場合に備え、情報共有トライアル等の取組が行われており、これらを通じて電気通信事業者による共同したサイバー攻撃対処の実現に寄与している。 電気通信事業者がサイバー攻撃に的確に対処するためには、電気通信事業者が相互に連携、情報共有し、共同して対処に当たることが有効であるが、対処のために必要となる情報は機微性が高いため、円滑な情報共有を行うためには、それが個々の電気通信事業者との間で十分な信頼関係の築かれた、民間の事業者団体が主体となってなされる必要がある。また、サイバー攻撃への対処に当たる電気通信事業者への適切な支援を行うためには、その主体において、通信ネットワークや電気通信設備に関する専門的知見や、実態についても十分な知見を有していることが不可欠であるが、電気通信事業者により構成される認定協会においてはそのような知見が備わっている。 本業務は、法に規定された認定の要件を満たし、認定がなされた後は、当該事業者団体の有する設備等を活用して実施可能なものであり、国による業務への関与は必要最小限である。また、これまで本業務は、民間の設備や能力を活用することで、国費を投じずに実施できており、業務の実施状況等からも効率性が確保されている。 以上によれば、今後も、認定協会において、攻撃通信に関する受信側の電気通信事業者から送信側の電気通信事業者に対する情報共有業務、攻撃の送信元を特定するための調査研究業務、その他の情報提供を通じたサイバー攻撃に対処する電気通信事業者を支援する業務を引き続き実施していく必要があり、その妥当性も認められる。 他方、サイバー攻撃の複雑巧妙化・大規模化がますます進んでいることを踏まえると、より多くの電気通信事業者が本業務に参画することによって、さらに実効性のある対処を実現できると期待され、今後、本業務を一層活性化させるため、特定会員数の更なる増加に向けた検討等が必要である。
学識経験を有する者の知見の活用	本業務に係る制度の導入ないし改正に当たっては、学識経験者等で構成される研究会（「円滑なインターネット利用環境の確保に関する検討会」、「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会」、「電気通信事業ガバナンス検討会」等）で検討が行われ、その結果を踏まえて法令を改正している。
政策評価を行う過程において使用した資料その他の情報	□円滑なインターネット利用環境の確保に関する検討会 https://www.soumu.go.jp/main_sosiki/kenkyu/smooth_internet/index.html □電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会 https://www.soumu.go.jp/main_sosiki/kenkyu/denki_cyber/index.html □電気通信事業ガバナンス検討会 https://www.soumu.go.jp/main_sosiki/kenkyu/sd_governance/index.html

※　国からの指定等に基づき特定の事務・事業を実施する法人に係る規制の新設審査及び国の関与等の透明化・合理化のための基準（平成 18 年８月 15 日閣議決定）に基づく評価