

平成 22 年度事前事業評価書要旨

政策所管部局課室名：情報流通行政局 情報セキュリティ対策室

評価年月：平成 22 年 8 月

1 政策（研究開発名称）

国際連携によるサイバー攻撃予知・即応技術の研究開発

2 研究開発の概要等

近年、大規模なサイバー攻撃が世界各国で発生し、国際的な問題となっており、これらサイバー攻撃の原因となるマルウェア※の感染手法は高度化・巧妙化を続けており、また、新種マルウェアの発生数も急激に増加している。

そのため、平成 23 年度から平成 27 年度の 5 か年において、感染手法が多様化するマルウェア※を効果的・効率的に捕獲するシステム(ハニーポット)と、攻撃手法が多様化するサイバー攻撃を広範囲に検知・分析するシステムを構築し、高度化・巧妙化を続ける情報セキュリティ脅威への迅速な対応実現に向けた研究開発を行い、将来の情報セキュリティ脅威を予測する技術的基盤を確立して、安心・安全な ICT 利用環境を実現する。

※コンピュータウイルス等の「悪意あるソフトウェア」の総称。

3 政策効果の観点及び分析等

専門家・有識者から構成される「情報通信技術の研究開発の評価に関する会合」及びその下に設けられた評価検討会（平成 22 年 7 月）において、外部評価を実施し、以下の分析を行った。

観点	分析
有効性	本研究開発は、政府、ISP、ソフトウェアベンダー、情報通信機器ベンダー、研究機関等の連携によって実施し、「新種マルウェアによる感染の予防」、「大規模なサイバー攻撃の早期検知・迅速な対処」、「情報セキュリティ脅威の将来予測に基づく予防的対処」を可能とする技術的基盤を実現することで、現在懸念されているサイバー攻撃やマルウェア等の情報セキュリティ脅威に関する被害を軽減することが可能と考えられる。これにより、国民が安心・安全にインターネットを利用できる環境の整備が実現され、社会・経済活動の発展に寄与することが期待される。 よって、本研究開発には有効性があると認められる。
効率性	本研究開発の技術の実現により、一回当たり約 100 億円のサイバー攻撃による機会損失を減らすことが可能と考えられ、投入される費用に見合った効果が得られると認められる。また、本研究開発の実施に当たっては、政府、ISP、ソフトウェアベンダー、情報通信機器ベンダー、研究機関等が連携することによって、最新の情報セキュリティ脅威に係る情報を広く共有する体制を構築するとともに、これら情報セキュリティ関係者が適切な役割分担を行う体制で基盤的技術の確立に向けた研究開発を実施することとしている。 よって、本研究開発には効率性があると認められる。
公平性	ICT の利活用が社会活動に広く浸透した現在では、多くの企業や一般ユーザが情報セキュリティの脅威にさらされており、誰もが被害者と成り得る。そのため、サイバー攻撃やマルウェア等の情報通信における情報セキュリティ脅威の被害軽減に資する本研究開発の成果は、広く社会に還元される公平性の高いものである。
優先性	大規模なサイバー攻撃事例が世界各国で発生している事例や、新種マルウェア Gumblar により、多くのウェブサイトが改ざんされた事例等、国内外において、情報セキュリティインシデントによる被害が数多く発生している。また、情報セキュリティインシデント数は増加する傾向にあり、このような事態に、一刻も早く対処するためには、本研究開発の実施が必要である。 よって、本研究開発の優先性があると認められる。

4 政策評価の結果

高度化・巧妙化を続ける情報セキュリティ脅威への対応に際しては、関係主体による能動的な取組が必要であるが、本研究開発の実施によって「新種マルウェアによる感染の予防」、「大規模なサイバー攻撃の早期検知・迅速な対処」、「情報セキュリティ脅威の将来予測に基づく予防的対処」を可能とする技術的基盤が実現され、政府、ISP、ソフトウェアベンダー、情報通信機器ベンダー、研究機関等における取組の更なる充実が期待される。

その結果、現在、社会問題となっている情報セキュリティインシデントによる被害の軽減に資することから、国民が安心・安全にインターネットを利用することが可能となると考えられる。

よって、本研究開発には、有効性、効率性、公平性、優先性があると認められるため、平成23年度予算において、「国際連携によるサイバー攻撃予知・即応技術の研究開発」として所要の予算要求を検討する。