平成 22 年度事前事業評価書

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　達成目標等

（１）達成目標

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実施することにより、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。

（２）事後事業評価の予定時期

事業終了後、平成 28 年度に事後事業評価を行う予定。

３　研究開発の概要等

（１）研究開発の概要

・研究開発期間

平成 23 年度～平成 27 年度（５カ年）

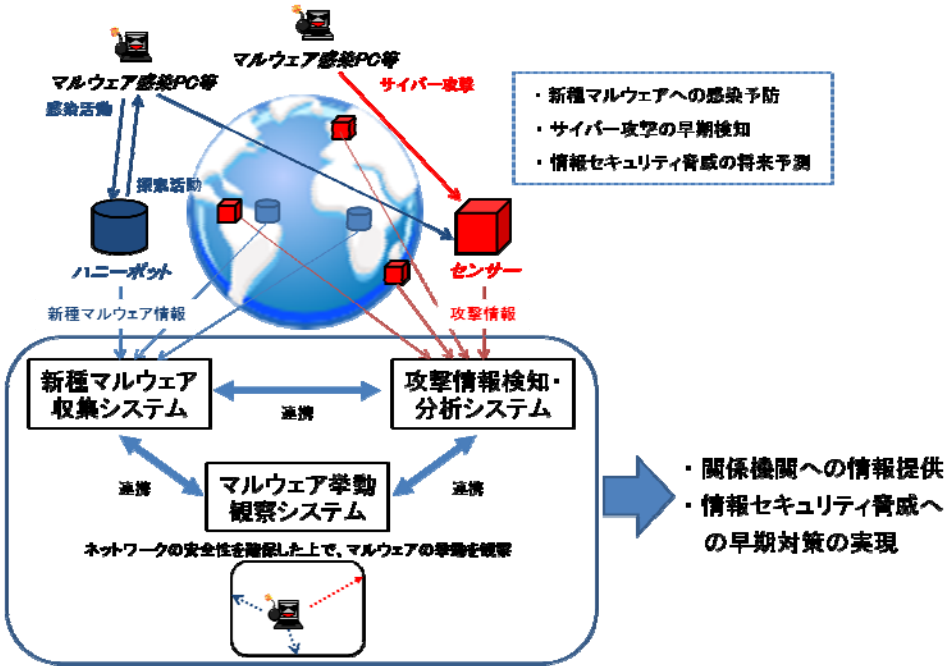
・想定している実施主体

インシデント対策事業者等

・研究開発概要

海外を含む複数の ISP、大学、研究機関等と連携して、各地にセンサーやハニーポットを設置することにより、全世界規模のマルウェア感染・攻撃状況等をリアルタイムで検知・分析し、情報セキュリティ脅威に対して迅速な対応を可能とする技術・手法を確立するため、クローラ技術等の応用による新種マルウェアを効果的・効率的に収集する技術、ネットワークに影響を及ぼすことなく、マルウェアを動作させ、その挙動を観察する技術、関係機関と連携することで迅速にインターネットユーザに対して、対策手法を周知する体制の確立に向けた研究開発を実施する。また、蓄積されたマルウェア感染・攻撃情報等を基に、将来における情報セキュリティ脅威を予測する技術の確立に向けた研究開発を実施する。

・研究開発概要図



・研究開発費

約 35 億円(うち、平成 23 年度要求額　7 億円)

（２）研究開発の必要性及び背景

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いる。2007 年４月にはエストニア、2009 年７月には米国及び韓国において大規模なサイバー攻撃が発生し、政府関係機関、金融機関等の主要機関のウェブサイトのサービスが長期間に渡って停止する事態となり、国民生活や経済活動に甚大な影響を及ぼしたところである。

一方、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。2009 年春には改ざんされたウェブサイトを経由して感染活動を行う Gumblar が出現し、世界的な感染活動を行った結果、我が国でも有名企業等のウェブサイト改ざん等の被害が発生し社会的に大きな反響を及ぼした。

なお、Gumblar による感染活動は現在も継続しており、効果的な対策が求められているところである。

これらの情報セキュリティ脅威の高まりに対応するため、新種マルウェアやサイバー攻撃の早期検知・対処体制の確立、また、高度化・巧妙化を続ける情報セキュリティ脅威の将来予測の技術基盤の確立が急務である。

また、サイバー攻撃先及び攻撃元のエリアが国境を越えた広域に跨る事例が増加し、被害規模も拡大傾向にある。これに効果的に対処するには、各国の協力体制強化が必要不可欠であり、民間では、早期の実施が不可能である。また、公共インフラであるインターネットの安全性の根幹に関わる問題への対策である点からも、国が率先して実施することが必要である。

（３）関連する政策、上位計画・全体計画等

○　関連する主要な政策：政策 10「情報通信技術の研究開発・標準化の推進」

○　新成長戦略～「元気な日本」復活のシナリオ～（平成 22 年６月　閣議決定）

同戦略において、科学・技術・情報通信立国戦略の一つとして、「大規模サイバー攻撃への対応」が記載されている。

○　国民を守る情報セキュリティ戦略（平成 22 年５月　情報セキュリティ政策会議決定）

同戦略において、「マルウェアへの感染対策等を強化するため、（中略）情報セキュリティ脅威の収集解析システム等の充実や、利用者・ISP 等への情報提供を通じたネットワーク等の情報セキュリティ対策を強化する。加えて、国際的な連携を推進する。」とあり、マルウェア対策等の充実・強化等を図ることとされている。

○　情報セキュリティ 2010（平成 22 年７月　情報セキュリティ政策会議決定）

同計画において、「ISP と協力してサイバー攻撃に関わる情報収集ネットワークを構築し、サイバー攻撃の事前防止・早期対策に向けた枠組みの構築を検討する。」とされている。

４　政策効果の把握の手法

（１）事前事業評価時における把握手法

当該事業の企画・立案に当たっては、外部専門家・外部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、本研究開発の必要性、技術の妥当性、実施体制の妥当性、予算額の妥当性等について外部評価を行い、政策効果の把握を実施した。

（２）事後事業評価時における把握手法

本研究開発終了後には、達成目標である「安心・安全な ICT 利用環境の整備」、「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の実現に際し、各技術・対処の実用化の状況について、主にセンサー、ハニーポットの設置数、新種マルウェアの検知数、情報セキュリティ脅威のトレンド等に係る関係者への情報提供回数（情報セキュリティインシデントレポート発行枚数等）をもとに検証・評価を行う。

５　政策評価の観点及び分析

（１）有効性の観点からの評価

マルウェアによる感染被害、また、マルウェアに感染した PC に起因するサイバー攻撃等による被害を減少させるためには、PC 上の脆弱性をねらって次々に現れる新種マルウェアを早期に発見・解析し、その結果のウィルス対策ソフトへの迅速な反映等が有効である。爆発的に出現する新種マルウェアへの対応が困難になりつつある状況下において、クローラ技術等を応用して新種マルウェアを能動的に収集する技術を確立することは、「新種マルウェアによる感染」予防を推進する手法として有効と考えられる。

また、ボットネットを悪用した大規模なサイバー攻撃の発生を早期に検知して迅速な対応を講じるためにはボットネット活動を監視することが効果的であるが、ボット感染 PC による有害な通信を遮断する安全な状態で監視を行う手法が確立されていない。このため、ボット感染 PC による有害な通信のみを遮断する技術を開発し、ボットネット監視手法を確立するこ

とは、サイバー攻撃発生を検知する一つの手法として有効と考えられる。

さらに、新種マルウェアには、既存マルウェアを基として改変された亜種が多く含まれている。それら亜種の変遷等の解析によって、将来におけるマルウェア変遷の方向性を把握することが可能になることが期待される。

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。

（２）効率性の観点からの評価

本研究開発の技術の実現により、一回当たり約 100 億円(注)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。

（注）平成 21 年７月に韓国で発生したサイバー攻撃による被害額は 363 億～544 億ウォン（約 27～41 億円）と報告されている。(韓国の現代経済研究院)　日本の GDP は韓国の 3～4 倍程度であることを考慮すると、同サイバー攻撃が日本で起きていた場合、約 100 億円以上の被害が起きた計算になる。

（３）公平性の観点からの評価

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。

なお、情報処理分野やソフトウェア分野におけるセキュリティ向上に向けた取組についても国費による支援が行われている。ICT に関するセキュリティ対策の推進に際しては、情報処理分野、ソフトウェア分野、情報通信分野における対策を総合的に実施することが必要であり、本研究開発も国が取り組むべき課題である。

（４）優先性の観点からの評価

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。

6　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ことから、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。

7　政策評価の結果の政策への反映方針

評価結果を受けて、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。

8　学識経験を有する者の知見の活用に関する事項

「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、「従来の受動的な対処のみでは不十分であり、本施策を実施し、新種マルウェアを能動的に収集する技術の確立等により、Gumblar 等の新たな脅威に対抗することは重要性が非常に高い」との評価を得た。このような有識者からの評価を本評価書の作成に当たって活用した。

9　評価に使用した資料等

○ 新成長戦略～「元気な日本」復活のシナリオ～（平成 22 年６月　閣議決定）
http://www.kantei.go.jp/jp/sinseichousenryaku/sinseichou01.pdf

○ 国民を守る情報セキュリティ戦略（平成 22 年５月　情報セキュリティ政策会議決定）
http://www.nisc.go.jp/active/kihon/pdf/senryaku.pdf

○ 情報セキュリティ 2010（平成 22 年７月　情報セキュリティ政策会議決定）
http://www.nisc.go.jp/active/kihon/pdf/is_2010.pdf