事　業　評　価　書

政策所管部局課室名　総合通信基盤局電気通信事業部データ通信課

評価年月　平成１７年７月

１ 政策	電気通信事業分野におけるサイバー攻撃対応演習
２ 達成目標等	**（１）達成目標** サイバー攻撃等によるインターネットの機能不全（以下「インシデント」という。）に対応するための人材育成及び緊急対応体制の検証を行い、インターネットの安全性・信頼性の向上を図り、利用者が安心・安全にインターネットを利用できる環境を実現する。
	（２）必要性及び背景 インターネットは、国民の社会経済活動を支えるインフラとして定着し、その重要性が高まる一方で、特に近年、ネットワークに接続しただけで感染してしまうウイルスや特定のプログラムに感染した多数のコンピュータから一斉に攻撃が行われる事案が発生している。 こうしたインシデントの広域化や組織的攻撃により、個々の電気通信事業者のみでは対応できなくなっており、事業者間及び事業者と行政との間で連携してセキュリティ対策を講じることのできる人材や協力体制の強化が求められている。 「次世代 IP インフラ研究会　第二次報告書」（平成 17 年 7 月、総務省）においても、インシデント事案の広域化や組織的攻撃の増加という最近の傾向にかんがみ、事業者をまたがる総合的な演習の必要性を提言しており、また、「情報セキュリティ基本問題委員会　第 2 次提言」（平成 17 年 4 月、ＩＴ戦略本部）においても、演習等を通じて高度なＩＴスキルを有する人材を育成すべきと提言されており、「経済財政運営と構造改革に関する基本方針２００５」（平成１７年６月）等の各種政策提言においても、「安心・安全の取組みを推進する」こととされている。 サイバー攻撃対応演習を行うためには、電気通信事業者、通信機器メーカ、情報家電メーカ等の複数の主体が参画した大規模で実環境に近い演習環境の構築が必要となるが、こうした演習環境の構築には民間事業者のみではリスクが高いことから、サイバー攻撃対応のための演習環境を国が主導して構築し、速やかに演習を実施する必要がある。
３ 事業概要等	**（１）事業概要** サイバー攻撃等によるインシデントに対応するため、実環境に近い演習環境を構築し、 ⑴セキュリティの専門家による実行可能な攻撃方法と攻撃による損害の程度 ⑵攻撃発生後の緊急対応体制が実際に機能するか否か 等について検証を実施し、高度なＩＴスキルや調整力を有する人材を育成するとともに、事業者間及び事業者と行政との間の緊急対応体制を強化する。

○　想定している実施主体

民間等

○　実施期間

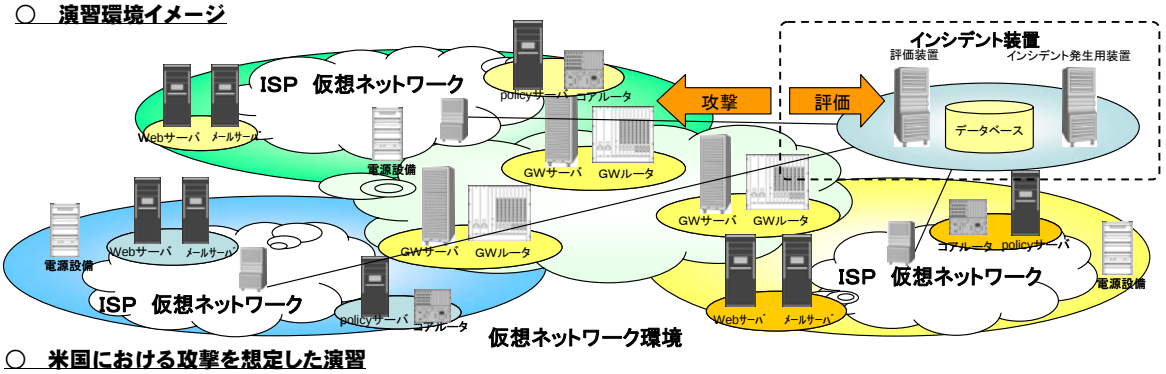
平成１８年度～平成２０年度

○　総事業費

予定総事業費　約１５億円（うち、平成１８年度要求額　５．０億円）

○　事業概要図

○　演習環境イメージ



○　米国における攻撃を想定した演習

演習名称	実施時期	実施主体	演習の概要
The Day After	1996年3月	国防総省（DARPA）	行政、大学、情報インフラ関係者による机上演習。攻撃の発生を想定して複数のシナリオを用意し、以下の演習プロセスを実施。
Eligible Recover	1997年6月	国家安全保障局（NSA）	NSAのスタッフが「実際に」攻撃を実施し、電力や電話のシステムを切断する方法等を模索し、システムの脆弱性を検証。
Digital Pearl Harbor	2002年7月	Gartner、米海軍大学	セキュリティ専門家が電力、通信インフラ、インターネット、金融サービスについて実行可能な攻撃方法と攻撃による損害を検証。
Livewire	2003年10月	国土安全保障省（DHS）	通信、エネルギー、金融、地方自治の分野について、攻撃発生後の緊急対応体制が実際に機能するかを検証。

	（２）関連する政策、上位計画・全体計画等 ○「e-Japan 戦略Ⅱ」（平成１５年７月　ＩＴ戦略本部）の「Ⅲ．新しい IT 社会基盤の整備　２．安全・安心な利用環境の整備」において、「情報セキュリティを確保し、不正アクセス、（中略）その他の不正行為に対処するための対策を推進」及び「情報セキュリティ全般に関する十分な知識・技術を有する専門家を育成」することとされている。 ○「u-Japan 政策」（平成１６年１２月　総務省）の「情報ネットワークの脆弱性克服」において、「サイバーテロや災害・停電等により機能が停止しやすいという脆弱性を内包したネットワークはシステミックリスクにさらされており、その運用上、適切なセキュリティ対策を施すなど、十分な危機管理を行う必要がある。」こととされている。 ○「情報セキュリティ基本問題委員会　第２次提言　～我が国の重要インフラにおける情報セキュリティ対策の強化に向けて～」（平成１７年４月　ＩＴ戦略本部）の「第５章　実現のための行動計画」において、「毎年度ごとにテーマを決めた「総合的訓練・演習」の企画・実施」や「演習・訓練及びセミナー等を通じた、高度なＩＴ人材の育成」が挙げられている。 ○「経済財政運営と構造改革に関する基本方針２００５」（平成１７年６月　経済財政諮問会議）において、「ＩＴ戦略の推進」のための取組として、「官民における統一的・横断的なセキュリティ対策を推進する。」、「ネットワーク分野について、２０１０年までにユビキタスネット社会を実現するために、「u-Japan 政策」を推進する。」及び「ＩＴを活用した安心・安全への取組を推進する。」こととされている。 ○「次世代 IP インフラ研究会　第二次報告書　～「情報セキュリティ政策２００５」の提言～」（平成１７年７月　総務省）において、「事業者をまたがる総合的な演習の必要性」が提言されている。
４　政策効果の把握の手法	○　総務省の「次世代 IP インフラ研究会」（座長：東京大学名誉教授　齊藤忠夫）において、学識経験者、電気通信事業者、メーカ等が参加し、情報セキュリティに関する課題や政策支援の在り方について検討し、これを活用して政策効果の把握を行った。

5　政策評価の観点及び分析	○　有効性 　インシデントの広域化や組織的攻撃の発生という最近の傾向を踏まえ、①実行可能な攻撃方法とシステムの脆弱性の有無、攻撃による損害の程度を検証するとともに、②攻撃発生後の緊急対応体制が実際に機能するか否か等を検証することにより、インシデントが発生した場合に事業者間及び事業者と行政との間の緊急対応体制や連携を強化することができ、加えて、演習を通じて、高度なＩＴスキルや調整能力を有する人材を育成することが可能であることから、社会インフラとしてのインターネットの安全性・信頼性を確保する上で有効である。 　また、本施策は、e-Japan 重点計画に掲げる「世界最高水準の高度情報通信ネットワークの形成」、「すべての国民がＩＴのメリットを享受できる社会の実現」、「高度情報通信ネットワークの安全性・信頼性の確保」に大きく寄与するものである。 ○　効率性 　サイバー攻撃に際して、電気通信事業者、通信機器メーカ、情報家電メーカ等の各主体における対応能力が向上すると同時に、演習を通して高度なＩＴスキルや調整能力を有する人材を育成することが可能なことから、社会経済に寄与し十分投資に見合うと考えられる。 　また、本施策の実施に当たっては、電気通信事業者、通信機器メーカ、情報家電メーカ等の複数の主体が連携して実施するものであり、実施計画面からみても効率的な実施が可能である。 ○　公平性 　本施策により、事業者間及び事業者と行政との間において、迅速かつ効率的なサイバー攻撃対応が可能になることにより、インターネットの安全性・信頼性の確保が可能となり、国民の多くが安心・安全なインターネットを享受できる環境が実現することから、その政策効果は広く国民一般に公平に分配される。 ○優先性 　インシデントの広域化や組織的攻撃の増加という最近の傾向にかんがみると、既に発生している攻撃や今後発生しうる攻撃に対応するため、速やかに対応を図る必要がある。 　「情報セキュリティ基本問題委員会　第２次提言」（平成１７年４月　ＩＴ戦略本部）においても、「日々増大していく脅威に対する重要インフラにおける情報セキュリティ対策強化は喫緊の課題であり、可及的速やかに実施に移していくことが必要である」と指摘されており、本施策について優先的に取り組む必要がある。 　また、「経済財政運営と構造改革に関する基本方針２００５」（平成１７年６月　経済財政諮問会議）においても、「ＩＴを活用した安心・安全への取組を推進する。」こととされており、優先して実施すべき施策である。

	○　社会的な影響 本施策は、高度なＩＴスキルや調整力を有する人材を育成し、事業者間及び事業者と行政との間の緊急対応体制を強化すること等により、重要な社会経済活動の基盤であるインターネットの安全性・信頼性の向上に資するものであり、社会経済に大きなインパクトを与えるものである。
６　政策評価の結果	本施策の実施は、サイバー攻撃等によるインターネットの機能不全に対応するため人材育成及び緊急対応体制の検証を行うことにより、インターネットの安心・安全な利用環境を実現に大きく寄与するものである。加えて、本施策は、民間事業者のみでは推進しがたいものであることから、高度情報通信ネットワーク社会の形成に必要な政府の取組みとして適切である。
７　政策評価の結果の政策への反映方針	平成１７年度実績評価においては、情報通信分野における情報セキュリティ対策に関する今後の取組みの方向性として、情報通信ネットワークの安全性及び信頼性の確保を図ることがあげられており、予算要求等を講じていく必要があるとの評価を行っている。 これらの評価結果を受け、平成１８年度において、「電気通信事業分野におけるサイバー攻撃対応演習」として所要の予算を要求する。
８　学識経験を有する者の知見の活用に関する事項	○　「次世代 IP インフラ研究会」（座長：東京大学名誉教授　齊藤忠夫）の下に、「セキュリティＷＧ」を設置し、学識経験者、電気通信事業者、メーカ等が参加し、情報セキュリティ確保に係る課題や政策支援の在り方等を検討し、これを活用して政策効果の把握を行った。
９　評価に使用した資料等	○　e-Japan 戦略Ⅱ（平成１５年７月　ＩＴ戦略本部） http://www.kantei.go.jp/jp/singi/it2/kettei/030702ejapan.pdf ○　u-Japan 政策（平成１６年１２月　総務省） http://www.soumu.go.jp/s-news/2004/041217_7_bt2.html ○「情報セキュリティ基本問題委員会　第２次提言　～我が国の重要インフラにおける情報セキュリティ対策の強化に向けて～」（平成１７年４月　ＩＴ戦略本部） http://www.bits.go.jp/itso/kaigi/kihon/teigen/pdfs/2teigen_hontai.pdf ○　経済財政運営と構造改革に関する基本方針２００５（平成１７年６月　経済財政諮問会議） http://www.keizai-shimon.go.jp/cabinet/2005/decision0621.html ○　次世代 IP インフラ研究会第二次報告書（平成１７年７月　総務省） http://www.soumu.go.jp/s-news/2005/050707_2.html