資料５－１

くらしの中に
総務省

政府における情報セキュリティ政策の動向について

平成27年1月16日
事　　務　　局

サイバーセキュリティ基本法(H26 11/6成立、11/12公布、H27 1/9全面施行)の概要

内閣

サイバーセキュリティ戦略の案の閣議請議

内閣総理大臣

戦略の案の作成

行政各部の指揮監督に関する意見具申

IT総合戦略本部

① 高度情報通信ネットワーク社会の形成に関する重点計画の作成、同計画の実施推進

② 上記のほか、同社会の形成に関する施策で重要なものの企画に関する審議、同施策の実施推進

※ 上記の実施推進のうち、府省横断的計画・関係行政機関の経費見積り方針・施策の実施に関する指針の作成、施策の評価を政府CIOに委任

本部長 ：官房長官
副本部長：国務大臣
本部員 ：国家公安委員会委員長、総務大臣、外務大臣、経産大臣、防衛大臣、上記以外の国務大臣のうち本部の事務を遂行するために特に必要があるとして総理が指定する大臣
有識者のうち総理が任命する者

戦略案の意見

重要事項について緊密連携

サイバーセキュリティ戦略本部

①サイバーセキュリティ戦略の案の作成及び同戦略の実施推進

② 国の行政機関及び独法における対策基準の作成及び同基準に基づく施策の評価(監査を含む。)その他の同基準に基づく施策の実施推進

③ 国の行政機関で発生したサイバーセキュリティに関する重大な事象に対する施策の評価(原因究明のための調査を含む。)

④ 上記のほか、次の事務

イ) サイバーセキュリティに関する重要施策の企画に関する調査審議

ロ) 同施策に関する府省横断的計画・関係行政機関の経費見積り方針・施策の実施に関する指針の作成、施策の評価その他の実施推進

ハ) 同施策の総合調整

本部に関する事務の処理を適切に内閣官房に行わせるために必要な法制の整備等
(情報セキュリティセンター[NISC]の法制化等)

資料等提供義務

勧告

勧告に基づく措置の報告聴取

国家安全保障会議

① 国家安全保障に関する外交政策及び防衛政策に関し、平素から機動的・実質的に審議

② 武力攻撃事態等への対処等の国防に関する重要事項に関し審議

③ 重大緊急事態への対処に関する重要事項に関し、集中して機動的かつ実質的に審議し、必要に応じて、政府がとるべき措置等について建議

戦略案の意見

我が国の安全保障に関する重要事項について緊密連携

資料等必要な協力の求め

情報の提供等の協力の求め

地方公共団体、独立行政法人、国立大学、特殊法人・認可法人であって本部が指定するもの、国内外の関係者との連絡調整を行う関係機関　等

地方公共団体

求めに応じるよう努める

各府省等

（参考）政府における情報セキュリティ政策の推進体制

平成26年の臨時国会で成立した「サイバーセキュリティ基本法」に基づき内閣に設置されたサイバーセキュリティ戦略本部を司令塔として、同本部事務局を担う内閣サイバーセキュリティセンター（NISC）の調整の下、関係省庁が連携した政府横断的体制を整備。

内閣　内閣総理大臣

IT総合戦略本部

高度情報通信ネットワーク社会の形成に関する施策を迅速かつ重点的に推進

緊密連携

サイバーセキュリティ戦略本部（平成27年1月9日　サイバーセキュリティ基本法により設置）

本部長　内閣官房長官
副本部長　情報通信技術（IT）政策担当大臣
本部員　国家公安委員会委員長
総務大臣
外務大臣
経済産業大臣
防衛大臣

閣僚が参画

遠藤　信博	日本電気株式会社代表取役執行役員社長
小野寺　正	KDDI株式会社代表取締役会長
中谷　和弘	東京大学大学院法学政治学研究科教授
野原佐和子	株式会社イプシ・マーケティング研究所代表取締役社長
林　紘一郎	情報セキュリティ大学院大学教授
前田　雅英	首都大学東京法科大学院教授
村井　純	慶應義塾大学教授

緊密連携

国家安全保障会議（NSC）

我が国の安全保障に関する重要事項を審議

（事務局）

内閣サイバーセキュリティセンター（NISC）

（平成27年1月9日　内閣官房組織令により設置）

内閣サイバーセキュリティセンター長
（内閣官房副長官補（事態）、国家安全保障局次長を兼務）

政府機関情報セキュリティ横断監視・即応調整チーム（GSOC）

協力

その他の関係省庁

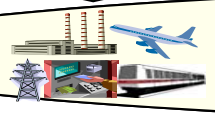
重要インフラ所管省庁
- 金融庁（金融機関）
- 総務省（地方公共団体、情報通信）
- 厚生労働省（医療、水道）
- 経済産業省（電力、ガス、化学、クレジット、石油）
- 国土交通省（鉄道、航空、物流）

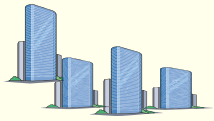
その他
- 文部科学省（セキュリティ教育）　等

協力

閣僚本部員5省庁

- **警察庁**（サイバー犯罪の取締り）
- **総務省**（通信・ネットワーク政策）
- **外務省**（外交政策）
- **経済産業省**（情報政策）
- **防衛省**（国の安全保障）


重要インフラ事業者等


政府機関（各府省庁）


企業


個人

総務省における主な情報セキュリティ対策予算（H26補正、H27当初）の概要

課題

標的型攻撃

標的型攻撃等の巧妙化するサイバー攻撃により、政府機関、民間企業等において機密情報漏えい等の被害が発生する事態が頻発。

個人のマルウェア感染

個人利用者においても、ウェブサイト等からのマルウェア感染により、ネットバンキングの不正送金などの実被害が発生。

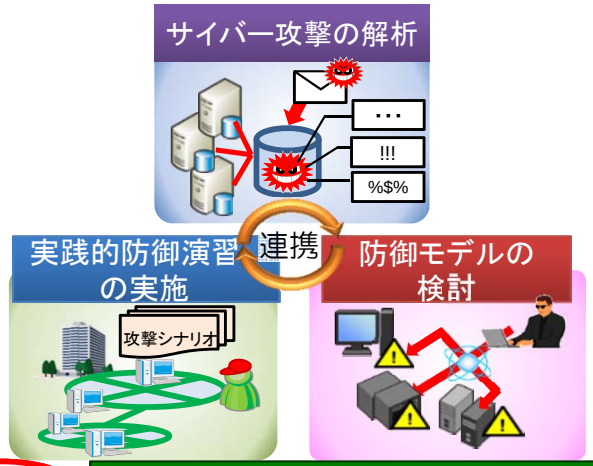
分散型サービス妨害攻撃（DDoS攻撃）

海外を主な発信源とするDDoS攻撃により、政府機関等のウェブサイトのアクセス障害やネットワークの輻輳が頻発。

対策

サイバー攻撃複合防御モデル・実践演習

標的型攻撃等の新たなサイバー攻撃の解析による実態把握、防御モデルの検討、官民参加型の実践的な防御演習の実施。【H27予定額】400百万円



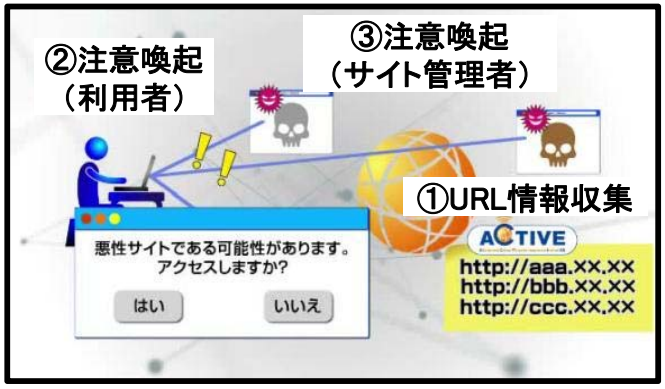
新規

新しい日本のための優先課題推進枠

M2Mセキュリティ実証事業

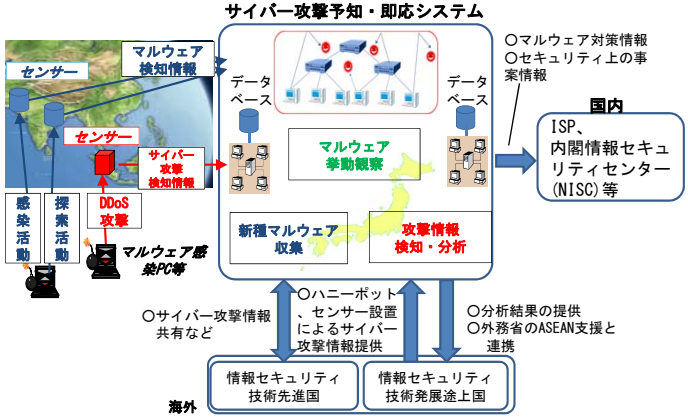
ICT環境の変化に応じた情報セキュリティ対応方策の推進事業

ISP等と連携し、インターネット利用者を対象に、マルウェア配布サイトへのアクセスの未然防止や利用者の行動特性に基づいた不正通信検知技術の開発など総合的なマルウェア感染対策を行うプロジェクト。【H27予定額】405百万円



国際連携によるサイバー攻撃予知・即応技術の研究開発

諸外国と連携してサイバー攻撃に関する情報を収集するネットワークを構築し、サイバー攻撃の発生を予知し即応を可能とする技術の研究開発及び実証実験。【H26補正予定額】200百万円



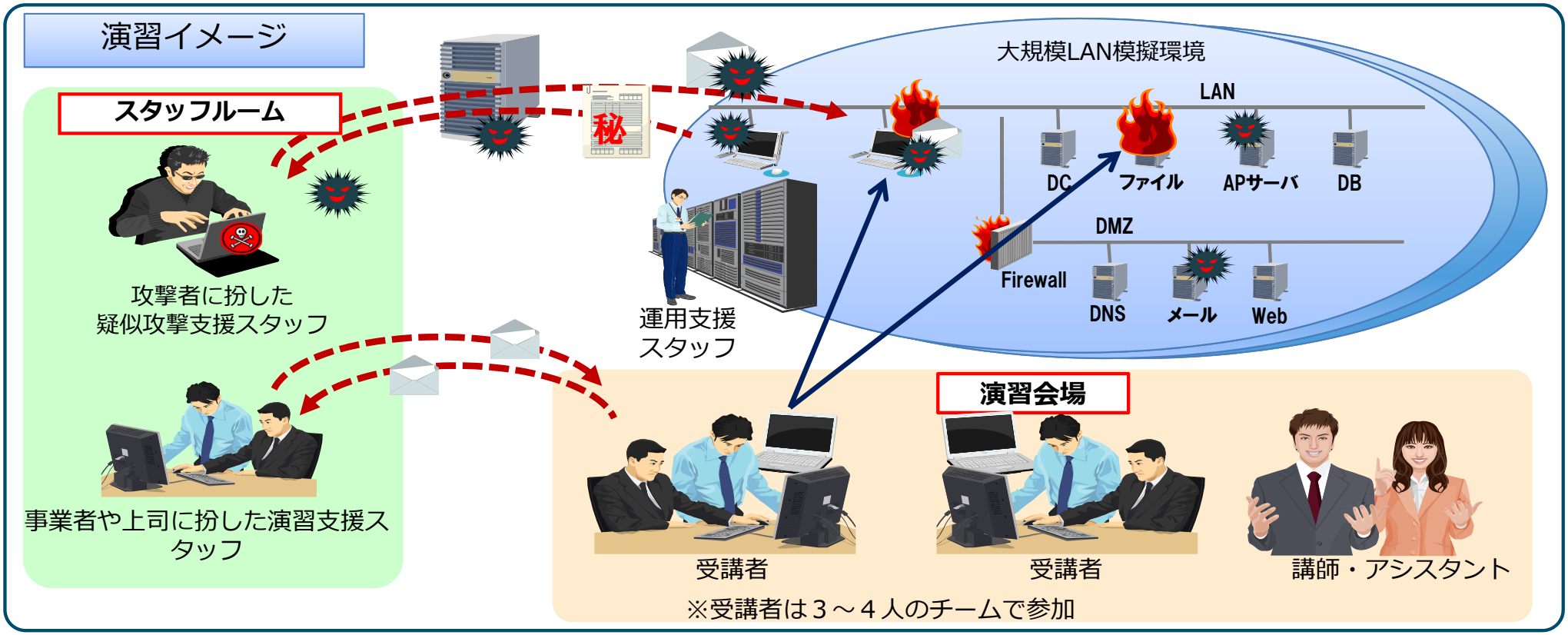
ICTの基盤である通信インフラの情報セキュリティを確保する横断的取組

IoT（Internet of Things）環境の本格的な到来により、今後の急速な普及が見込まれる機器間通信（M2M）について、M2Mの特徴に合致した通信プロトコル・暗号通信技術等の情報セキュリティ技術の開発・実証を実施。【H27予定額】150百万円

実践的サイバー防御演習（CYDER：CYber Defense Exercise with Recurrence）

- 官公庁・大企業等のLAN管理者のサイバー攻撃への対応能力向上のため、実践的なサイバー防御演習を実施。
- 職員数千人規模の組織内ネットワークを模擬した大規模環境による、官公庁を対象としたサイバー演習は国内唯一。
- LAN管理者の能力向上に寄与すると共に、演習で得られた知見を基に防御モデルを確立し広く展開していく予定。

概要図



実施状況

主に<u>官公庁・重要インフラ※事業者を対象</u>に平成25年度より演習を実施。平成26年度においては、官公庁並びに情報通信、金融、航空、鉄道、電力、地方自治体、医療、水道、物流、化学、クレジットカード、石油の12分野の重要インフラ事業者等から計62組織参加のもと計7回実施。

※ 機能が停止すると社会経済活動に多大な影響を及ぼすおそれがある、国民生活及び社会活動に不可欠なサービスを提供している社会基盤。全13分野。

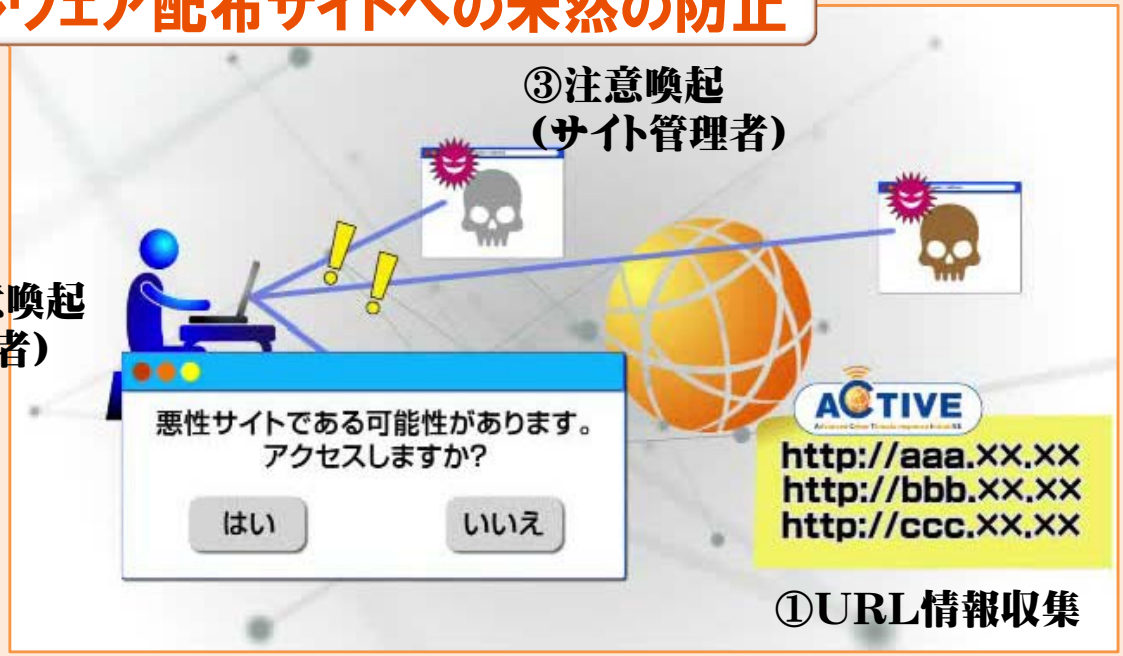
ACTIVE（Advanced Cyber Threats response InitiatiVE）

○ ACTIVEは、インターネットサービスプロバイダ（ISP）等との協力により、インターネット利用者を対象に、マルウェア配布サイトへのアクセスを未然に防止する等の実証実験を行う官民連携プロジェクト。平成25年11月から開始。

○ 総合的なマルウェア感染対策を官民連携により実施するプロジェクトは、世界初。

ACTIVE（Advanced Cyber Threats response InitiatiVE）の取組

マルウェア配布サイトへの未然の防止



① マルウェア配布サイトのURL情報をリスト化。

② マルウェア配布サイトにアクセスしようとする利用者に注意喚起。

③ マルウェア配布サイトの管理者に対しても適切な対策を取るよう注意喚起。

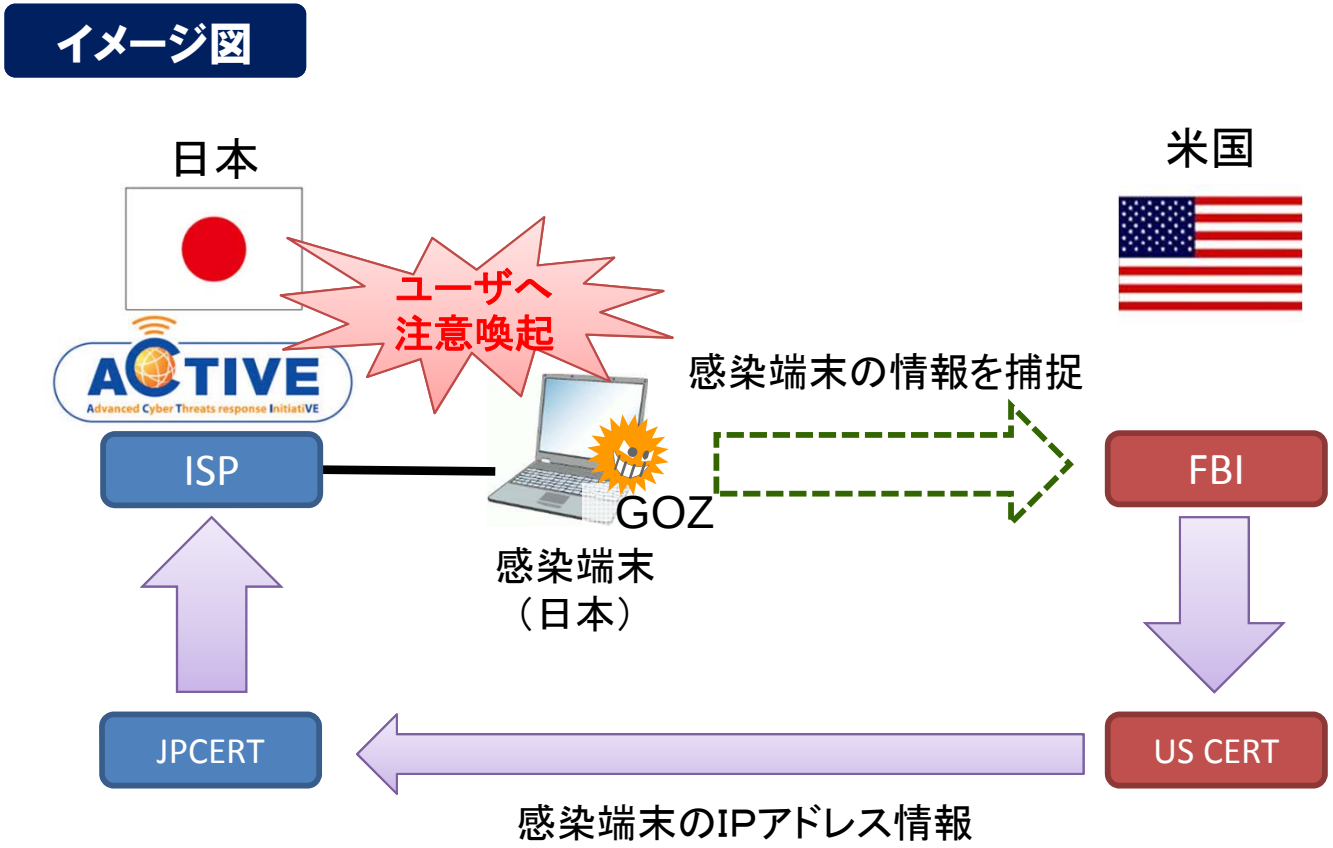
上記のほか、マルウェアに既に感染している利用者に対する注意喚起など、総合的なマルウェア感染対策を実施。

国際的なマルウェア駆除作戦へのACTIVEの活用

○ インターネットバンキングの不正送金等を行うマルウェア「Game Over Zeus（GOZ）」が世界的に蔓延しており、日本国内にも約20万台の感染端末が存在していることが判明。これを踏まえ、平成26年6月より米国連邦捜査局（FBI）、欧州刑事警察機構（ユーロポール）が中心となり、GOZの駆除作戦を展開。

○ ACTIVEを活用し、日本国内のGOZの感染者（IPアドレスベースで約10万台）に対する注意喚起を実施。

イメージ図



「GameOver Zeus」の感染のしくみ

攻撃者　サーバー　ウイルス　PC　ID、パスワード

ネットバンキング不正送金

ウィルス駆除、日米欧連携

FBIが対策プログラム

警察庁は3日、インターネットバンキングの不正送金被害を防ぐため、米国や欧州の捜査当局と連携し、2011年から全世界で猛威を振るうコンピューターウイルスの駆除に乗り出したことを明らかにした。米連邦捜査局（FBI）が最大100万台あるとみられる感染したパソコンの情報を集約する。

連携するのは日米欧など12カ国。欧州刑事警察機構（ユーロポール）に対策本部を置き、警察庁も職員を派遣した。日本の捜査当局が欧米とのウイルス駆除に参加するのは初めて。

警察庁によると、このウイルスは「GameOver Zeus（GOZ）」と呼ばれ、感染するとネットバンキングのIDやパスワードを抜き取る。被害は推計1億円以上という。ウイルスに感染したパソコンの約2割（最大20万台）が日本国内にあるとみられ、警察庁はホームページ（HP）に情報を掲載した。

GOZは、ほかの同種ウイルスに比べ、感染したパソコンの特定が困難だった。FBIが、新たに開発した対策プログラムで感染パソコンをあぶり出し、集約。FBIからパソコンの住所に当たるIPアドレスの提供を受けた各国捜査当局が、国内にあるとみられ、警察プロバイダーに連絡するなどして、利用者にウイルス駆除を促す。

FBIはGOZに感染したパソコンのネットワークを管理していたロシアに居住歴のある男（30）を指名手配。ネットワーク壊滅を目指す。

手口多様化で被害拡大

インターネットバンキングの不正送金をめぐっては、手口が多様化し、国内でも被害が急拡大している。

今回、問題になっているウイルス「GameOver Zeus（GOZ）」は、2011年9月に出現が確認された。感染すると、銀行の正規のログイン画面を装った偽画面が表示され、入力したIDやパスワードなどの情報を盗まれる。

これまでのウイルス攻撃は、司令塔に当たるサーバーから発信されることが多かったが、GOZは感染パソコン同士がネットワークを構築し、大量の迷惑メールを送信するなど「攻撃者」に姿を付けて利用者を偽サイトに誘導し、IDやパスワードを入力させる「フィッシング」が主流だった。最近はウイルスに感染させ、利用者が正規サイトで入力した情報を盗み出すのが特徴。感染拡大を防ぎにくいという。

ネットバンキングを狙う手口は多様化している。従来はメールを送り付けて利用者を偽サイトに誘導し、IDやパスワードを入力させる「フィッシング」が主流だった。最近はウイルスに感染させ、利用者が正規サイトで入力した情報を盗み出すのが特徴。感染拡大を防ぎにくいという。

今年の国内の不正送金被害は、5月9日までで約14億1700万円。大手銀だけでなく地域金融機関も標的になり、過去最悪だった2013年を既に上回った。GOZによる被害額がどの程度かは判明していないが、メガバンク担当者は「次々に新種ウイルスが登場しており、対策が追いつかない」と話している。

平成26年6月4日（水）
日本経済新聞

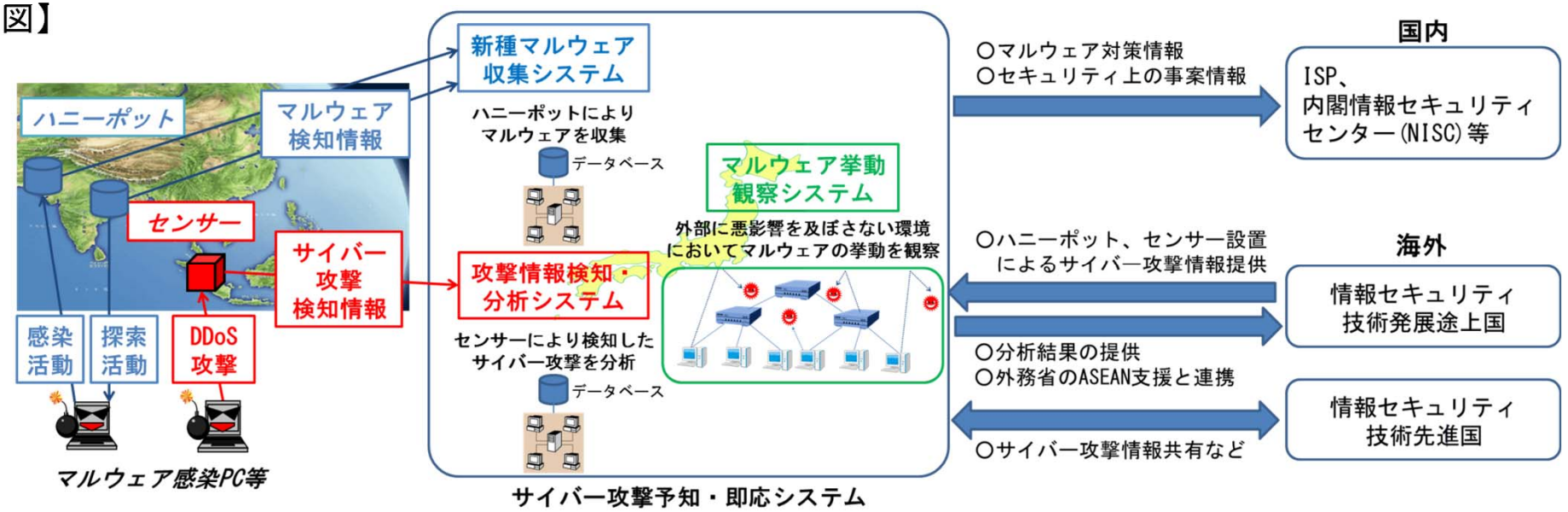
国際連携によるサイバー攻撃予知・即応技術の研究開発

プロジェクト略称：PRACTICE, Proactive Response Against Cyber-attacks Through International Collaborative Exchange

○目的：
近年、被害が拡大しているサイバー攻撃（分散型サービス妨害攻撃、マルウェアの感染活動等）に対処し、我が国におけるサイバー攻撃のリスクを軽減。

○概要：
国内外のインターネットサービスプロバイダ（ISP）、大学等との協力によりサイバー攻撃、マルウェア等に関する情報を収集するネットワークを国際的に構築し、諸外国と連携してサイバー攻撃の発生の予兆を検知し即応を可能とする技術について、その研究開発及び実証実験を実施。

【イメージ図】



○マルウェア：コンピュータウイルスのような有害なソフトウェアの総称。

○DDoS（Distributed Denial of Service）攻撃：分散型サービス妨害攻撃。多数のPCから一斉に大量のデータを特定宛先に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。

○ハニーポット：故意に外部からの進入を容易にした囮のネットワーク機器。マルウェアの感染活動等の検知を目的にネットワーク上に設置。

国際連携の状況

○　平成23年11月、「第4回日・ASEAN情報セキュリティ政策会議」において、ASEAN各国に連携を呼びかけ。
○　平成24年3月には、サイバー攻撃の予知のための研究開発の協力について、米国と合意。
○　その他、インドネシア、モルディブ、タイ、マレーシア、フィリピン、シンガポールとの間で連携中。
○　現在、欧州諸国、インド等と連携に向けて協議中。

M2Mにおけるセキュリティ上の脅威への対策（M2Mセキュリティ実証事業）

■ M2Mは今後市場規模の大きな成長が見込まれ（2018年度の市場規模１兆円超）るとともに、その利活用シーンも拡大していくことが見込まれる（2020年には300～500億超のデバイスがインターネットに接続され、うち過半数がM2M関係）。

■ 一方、M2Mにおいては情報セキュリティ上の課題も数多く存在しており、これらの情報セキュリティ上の脅威に対して対策を講じることにより、脅威から生じる様々な社会経済的混乱を防ぐ必要がある。

M2Mの情報セキュリティを確保するために必要となる情報通信技術の開発・実証を実施する。

課題

課題①

M2Mのインターネット接続（IP化）に伴う設定・運用に関する基準の不備

課題②

センサー等の処理能力の低いM2M機器にも処理可能な軽量な暗号通信技術の不備

課題③

M2M端末のソフトウェア更新により長期間セキュリティを確保できる仕組みが必要

① 情報セキュリティ検証を通じた、M2Mにおけるセキュリティ基準の検討

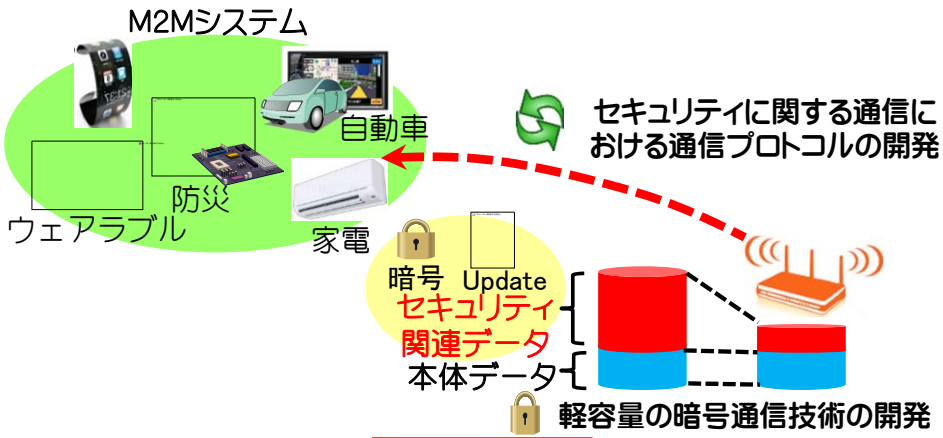
② M2Mにおける省エネ・省リソースでセキュアなデータ通信を可能とし、かつM2M端末における長期間のセキュリティ品質の確保を可能とする暗号通信技術及び通信プロトコルの開発

施策概要

① セキュアなＭ２Ｍシステムの設定・運用のあり方について検討を行う。

② Ｍ２Ｍにおけるリソースの制約に適合した、省エネ・省リソースでセキュアなデータ通信を可能とし、かつＭ２Ｍシステムに必要な長期間のセキュリティ品質管理を可能とする通信プロトコル及び暗号通信技術について、国際展開も見据えた開発・実証を行う。

施策イメージ



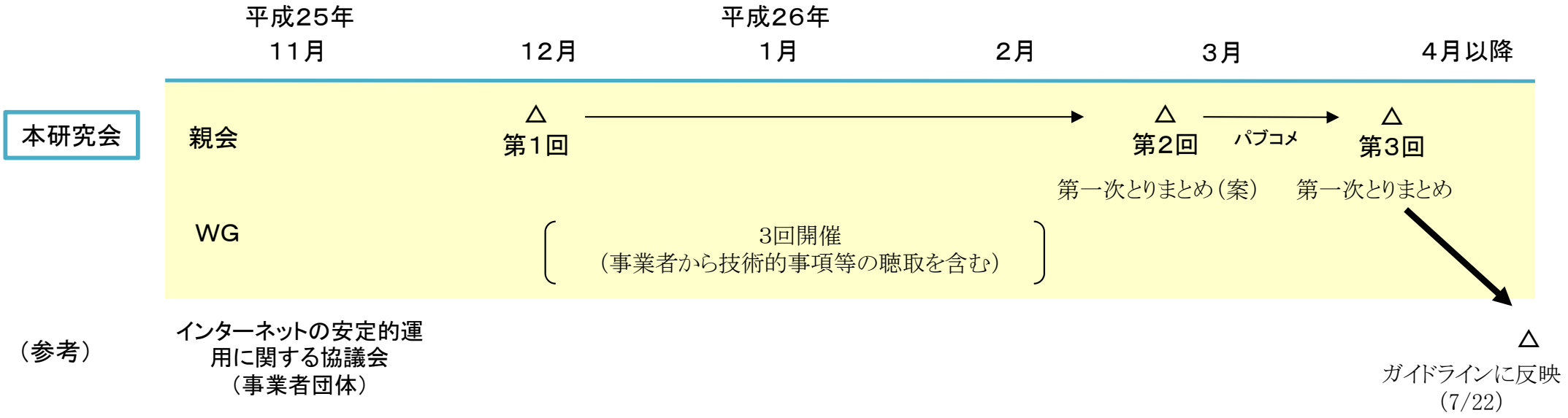
M2Mの情報セキュリティ技術・基準の確立による安心・安全なM2M利用環境の実現

構成員

＜本会合＞　（本会合の下にWGを設置し、事業者から技術的事項の聴取も含め検討を実施）

佐伯　仁志	東京大学大学院法学政治学研究科教授
宍戸　常寿	東京大学大学院法学政治学研究科教授
森　　亮二	弁護士
藤本　正代	情報セキュリティ大学院大学客員教授
中尾　康二	独立行政法人情報通信研究機構　ネットワークセキュリティ研究所　主幹研究員
木村　たま代	主婦連合会
木村　孝	一般社団法人日本インターネットプロバイダー協会
小山　覚	一般財団法人日本データ通信協会 テレコム・アイザック推進会議

スケジュール



「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 第一次とりまとめ」（平成26年4月4日公表）について

整理のポイント

最近のサイバー攻撃の動向を踏まえ、下記の対策に関し、通信の秘密との関係を整理

① ACTIVEの普及展開
→ 利用者が、一旦契約約款に同意した後も、随時、同意内容を変更できる（オプトアウトできる）こと等を条件に、契約約款に基づく事前の包括同意であっても有効な同意と整理

② マルウェア感染駆除の拡大
→ C&Cサーバ※1に蓄積されている、同サーバとマルウェアに感染したPC等の端末に係る通信履歴からマルウェアの感染者を特定し、注意喚起を実施することは、当該端末が正常かつ安全に機能することに対する現在の危難を避けるための緊急避難※2として許容される。

※1　Command and Control serverの略。マルウェアに感染してボットと化したコンピュータ群（ボットネット）に、情報漏えいやデータ破壊等に係る指令を送り、制御の中心となるサーバ。

※2　刑法第37条　自己又は他人の生命、身体、自由又は財産に対する現在の危難を避けるため、やむを得ずにした行為は、これによって生じた害が避けようとした害の程度を超えなかった場合に限り、罰しない。ただし、その程度を超えた行為は、情状により、その刑を減軽し、又は免除することができる。

③ 新たなDDoS攻撃であるDNSAmp攻撃の防止
→ 利用者が設置しているブロードバンドルータ等のゲートウェイに対するインターネット側からの名前解決要求に係る通信を遮断することは、電気通信役務の安定的提供を図るための正当業務行為※として許容される。

※　刑法第35条　法令又は正当な業務による行為は、罰しない。

④ SMTP認証の情報（ID及びパスワード）を悪用したスパムメールへの対処
→ 他人のID・パスワードを悪用して送信されるスパムメールへの対処として、当該IDの一時停止や、正規の利用者への注意喚起等を実施することは、電気通信役務の安定的提供を図るための正当業務行為として許容される。