くらしの中に
総務省

サイバー攻撃対策と通信の秘密

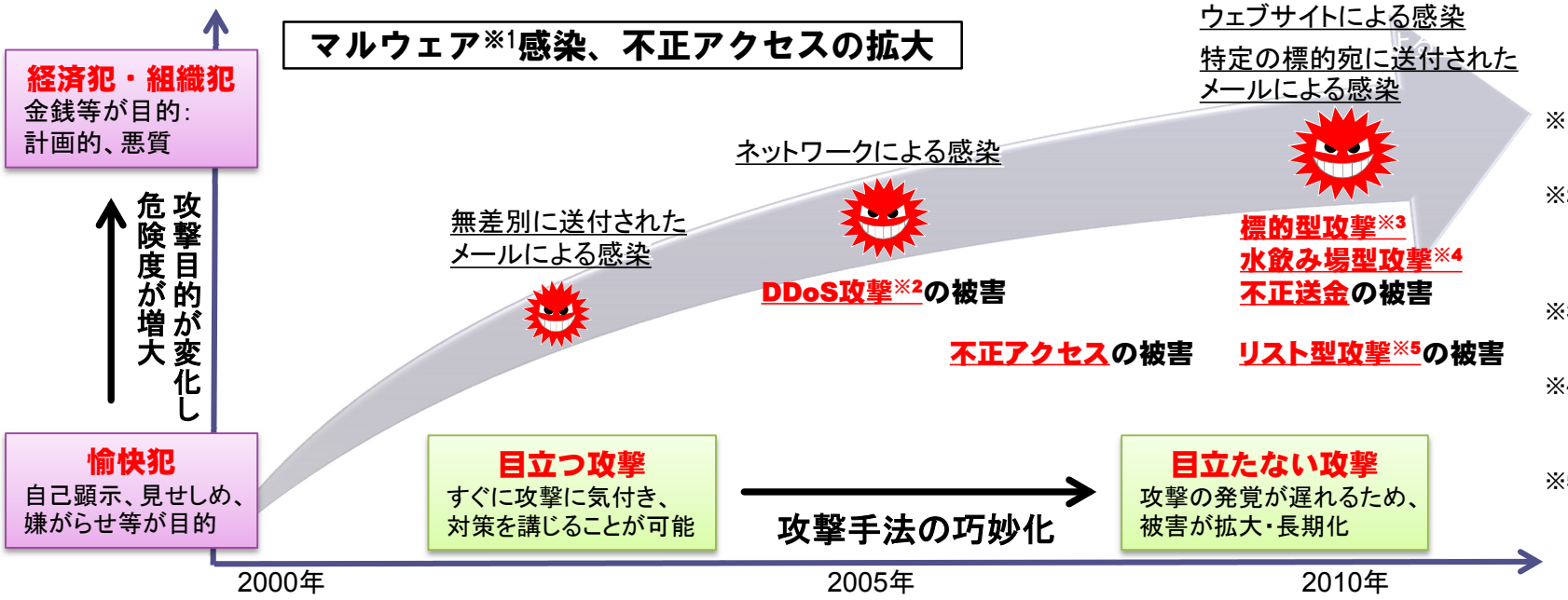
平成26年11月19日

情　報　流　通　行　政　局
情報セキュリティ対策室長

赤阪　晋介

情報セキュリティ上の脅威の増大①

インターネット等の情報通信技術は社会経済活動の基盤であると同時に我が国の成長力の鍵であるが、昨今、情報セキュリティ上の脅威が悪質化・巧妙化し、その被害が深刻化。



※1 マルウェア（Malware）：
Malicious softwareの短縮語。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。

※2 DDoS攻撃：
分散型サービス妨害攻撃（Distributed Denial of Service）のこと。多数の端末から一斉に大量のデータを特定宛先に送りつけ、宛先のサーバ等を動作不能にする攻撃。

※3 標的型攻撃：
機密情報等の窃取を目的として、特定の個人や組織を標的として行われる攻撃。

※4 水飲み場型攻撃：
標的組織が頻繁に閲覧するウェブサイトで待ち受け、標的組織に限定してマルウェアに感染させ、機密情報等を窃取する攻撃。

※5 リスト型攻撃
不正に入手した他者のID・パスワードをリストのように用いてWebサービスにログインを試み、個人情報の窃取等を行う攻撃。

最近のサイバー攻撃による被害の例

2011年10～11月・・・衆参両院のサーバやPCが情報収集型のマルウェアに感染していたことが報道。ID・パスワードが流出したおそれ（標的型攻撃）

2012年6月・・・国際ハッカー集団「アノニマス」により、財務省、国土交通省のウェブサイトが一時アクセスしづらい状態が発生（DDoS攻撃）

2012年9月・・・中国からのサイバー攻撃により、最高裁判所、文化庁等のウェブサイトが一時アクセスしづらい状態が発生（DDoS攻撃）

2013年1月・・・農林水産省のPCが遠隔操作型のマルウェアに感染し、TPPに関する機密文書が窃取されたおそれ（標的型攻撃）

2013年4月・・・宇宙航空研究開発機構（JAXA）に不正アクセスがあり、国際宇宙ステーションの運用準備参考情報、関係者メールアドレスが流出したおそれ（不正アクセス）

2013年4～8月・・・サイバーエージェントの運営するSNS「Ameba」がリスト型攻撃を受け、約24万件のメールアドレス等が流出したおそれ（リスト型攻撃）

2013年8～9月・・・共同通信等によるニュースサイト「47行政ジャーナル」が改ざんされ、サイト閲覧者にマルウェア感染のおそれ（水飲み場型攻撃）

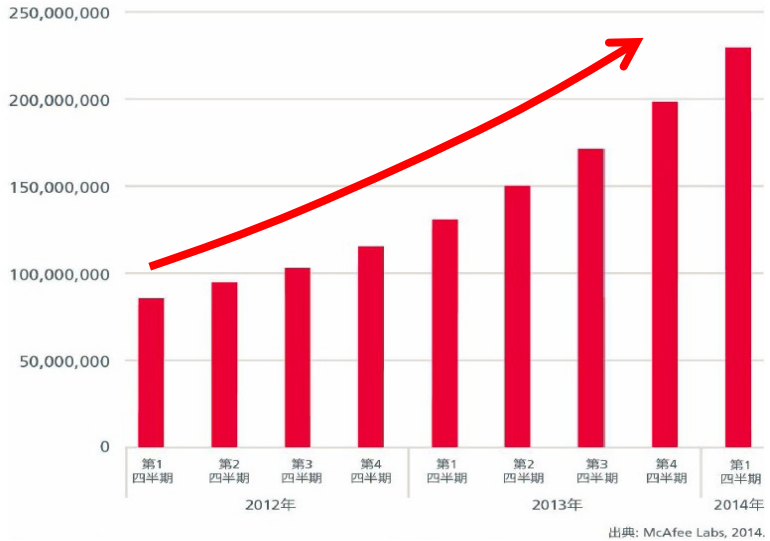
2014年9月・・・オンラインバンキングに係る不正送金事犯による2014年上半期の総被害額が約18億5,200万円で最高額を更新（不正送金）

2014年9月・・・法務省のサーバやPCに不正アクセスがあり、法務局の情報が流出したおそれ（不正アクセス）

2014年9月・・・JAL社内のPCがマルウェアに感染し、JALマイレージバンク会員の個人情報が約75万件流出したおそれ（標的型攻撃）

情報セキュリティ上の脅威の増大②

マルウェアの総数



マカフィーにおいて、１四半期で3,000万超の新種マルウェアを確認しており、
これまでデータベース上登録されたマルウェア数は２億件を突破

政府機関・重要インフラへの脅威件数等

24時間365日
（１分に１０回）

	2010年度	2011年度	2012年度	2013年度
センサー監視等による脅威件数※	約48万	約66万	約108万	約508万
センサー監視等による通報件数	181	139	175	139
不審メールに関する注意喚起の件数	118	209	415	381

	2013年度（括弧内は昨年度の数字）	主な内訳
重要インフラ分野からの情報連絡件数	153（110）	不正アクセス、DoS攻撃 121 ウイルスへの感染 7 その他の意図的要因 5

※ GSOC（政府機関・情報セキュリティ横断監視・即応調整チーム）により各府省等に置かれたセンサーが検知等したイベントのうち、正常なアクセス・通信とは認められなかった件数

nicterによる観測データ

年	年間総観測パケット数	観測IPアドレス数
2005	約　3.1億	約1.6万
2006	約　8.1億	約10万
2007	約　19.9億	約10万
2008	約　22.9億	約12万
2009	約　35.7億	約12万
2010	約　56.5億	約12万
2011	約　45.4億	約12万
2012	約　77.9億	約19万
2013	約128.8億	約21万

ダークネットセンサによる攻撃の観測数

国別ホスト数 Top 10

国名(国コード)	ホスト数	割合
中国(CN)	43,346	50%
韓国(KR)	6,384	7%
アメリカ(US)	4,861	6%
日本(JP)	3,083	4%
台湾(TW)	2,988	3%
ブラジル(BR)	2,376	3%
ロシア連邦(RU)	2,314	3%
香港(HK)	1,978	2%
インド(IN)	1,614	2%
タイ(TH)	1,422	2%

国別パケット数 Top 10

国名(国コード)	パケット数	割合
中国(CN)	1,214,956	37%
アメリカ(US)	555,109	17%
台湾(TW)	209,114	6%
ロシア連邦(RU)	142,925	4%
オランダ(NL)	122,770	4%
インド(IN)	95,948	3%
カナダ(CA)	94,760	3%
韓国(KR)	93,522	3%
フランス(FR)	89,051	3%
アイスランド(IS)	64,056	2%

攻撃の発出元（26年9月4日時点）

官民一体となった対策の必要性

昨今、サイバー攻撃はますます巧妙化・複雑化しており、攻撃により我が国の安全保障・危機管理に影響が及ぶだけでなく、ＩＣＴ利活用の基盤となる安心・安全なネットワーク環境が脅かされる事態が生じている。

とりわけ・・・

① **ウェブサイトを閲覧しただけで感染するマルウェアが出現するなど、気づかないうちにマルウェアに感染する危険が存在**

② **特定の組織や個人を標的にして、様々な手段を用いて執拗かつ継続的に攻撃を行うことにより機密情報を窃取する攻撃が発生**

③ **インターネット上想定されている正常な機能を悪用することにより、正常な通信と不正な通信の見分けがつきにくいような攻撃が発生**

サイバー攻撃が巧妙化・複雑化する中、一個人や一組織で対策を取るには限界が生じており、国として早急な対策を講じる必要がある。

政府における推進体制の機能強化（議員立法「サイバーセキュリティ基本法案」）

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

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

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

各府省等

総務省における主な情報セキュリティ対策予算の概要

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。

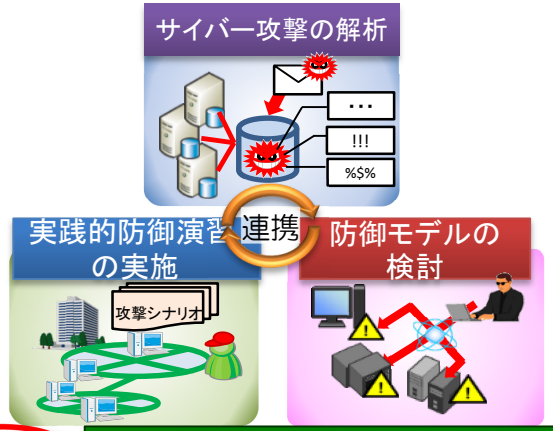
分散型サービス妨害攻撃（DDoS攻撃）

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。

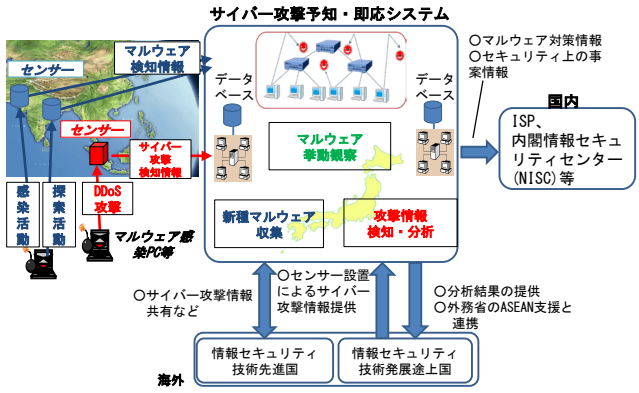


ICT環境の変化に応じた情報セキュリティ対応方策の推進事業

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。

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。



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。

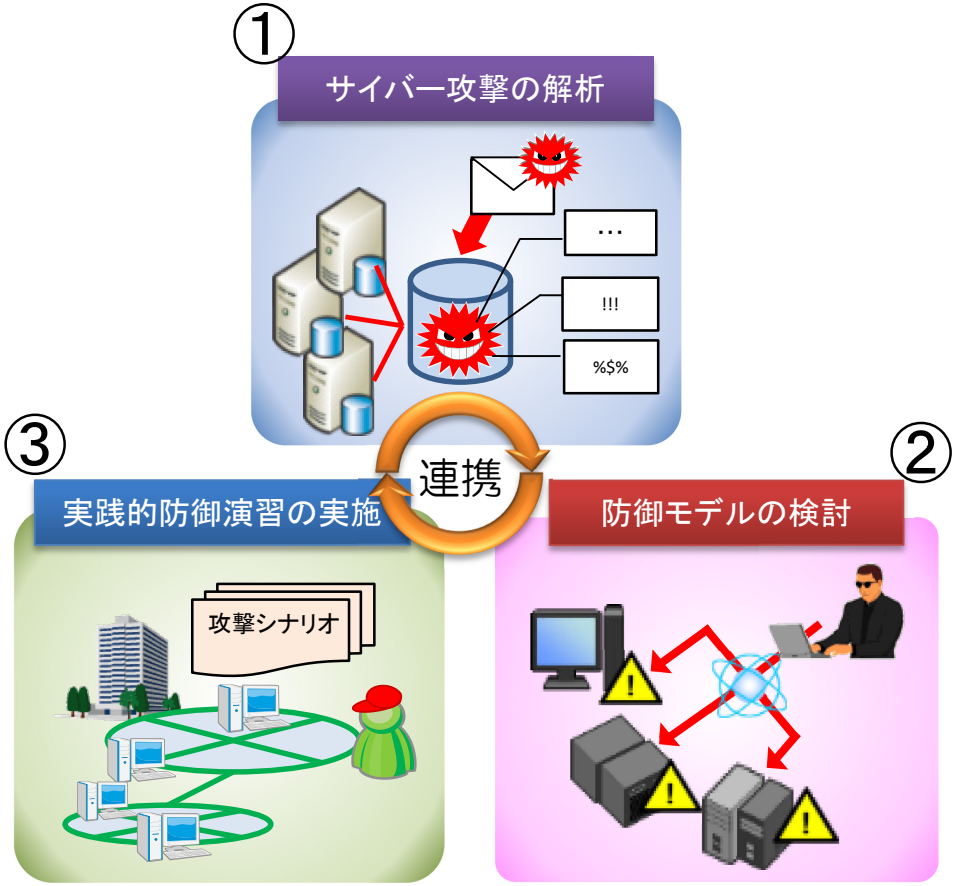
サイバー攻撃複合防御モデル・実践演習

新たなサイバー攻撃に対応可能な環境を実現するため、攻撃の解析及び防御モデルの検討を行い、官民参加型のサイバー攻撃に対する実践的な防御演習等を実施する。

施策概要

標的型攻撃に対応可能な環境を実現するための次の取組を実施。

① 官公庁・大企業のＬＡＮ環境を模擬した大規模実証環境による標的型攻撃の解析
② 標的型攻撃が発生した際の防御モデルの検討
③ 官公庁・大企業等のＬＡＮを模擬した環境による実践的な防御演習



計画年数

5か年計画（平成25年度～29年度）

所要経費

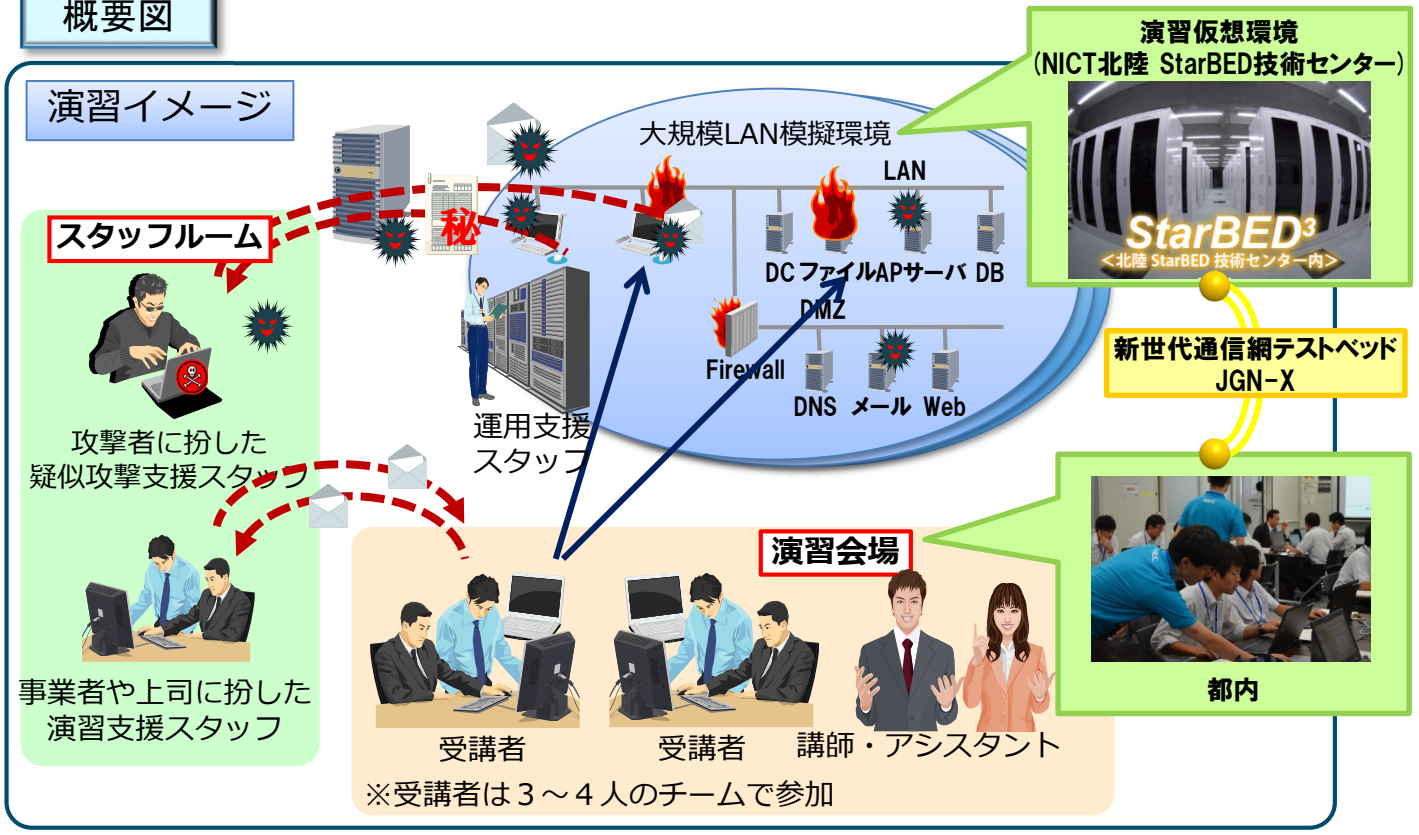
平成26年度当初予算　4．5億円

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

（サイダー：サイバー 防御 反復演習）

- 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



平成26年度の特徴

- ✓ **参加組織数が増加**
  ３３組織（H25） → **５４組織**
- ✓ **重要インフラ分野が拡大**
  ４分野（H25） → **１２分野**
- ✓ **新規シナリオの追加**
  水飲み場型攻撃に対応
  （H25：標的型メール攻撃）

平成26年度の実施スケジュール

開催回	開催日
第1回	H26/10/21(火), 22(水)
第2回	H26/10/23(木), 24(金)
第3回	H26/11/10(月), 11(火)
第4回	H26/11/12(水), 13(木)
第5回	H26/11/17(月), 18(火)
第6回	H26/11/25(火), 26(水)
第7回	H26/12/11(木), 12(金)

演習参加者

主に**官公庁・重要インフラ※事業者を対象**に演習を実施。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の参加のもと実施予定。

※ 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。

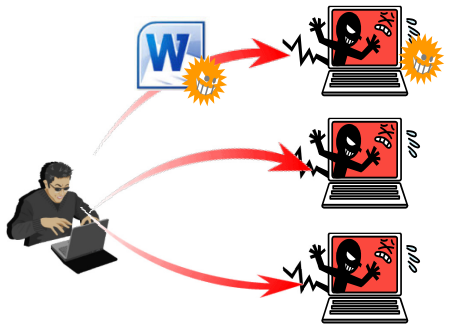
国民のマルウェア感染による被害の拡大

我が国において、利用者のPC内部の情報を窃取したり、PCを遠隔から不正に操作したりする有害なソフトウェア（マルウェア）の感染が拡大しており、インターネットバンキングの不正送金などの金銭的被害が増加している。

主なマルウェア感染手口

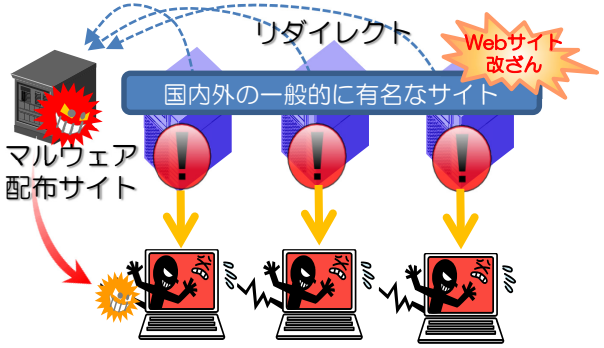
メールを経由した感染

マルウェアを仕込んだファイル（Word文書等）をメールに添付して送り、ファイルを開くと感染。



Webを経由した感染

Webサイトにマルウェアを仕込み、当該Webサイトにアクセスすると感染。



マルウェア感染により、様々な被害が発生

マルウェア感染による主な被害事例①

不正送金被害 昨年超す

ネットバンキング 1~5月14億円

インターネットバンキングのIDとパスワードが盗まれ、口座から現金が不正に抜き取られる被害が、今年1月から5月9日までに約14億1700万円に上ったことが15日、警察庁のまとめで分かった。すでに過去最悪だった昨年1年間の約14億600万円を上回った。地方の金融機関で法人口座が狙われる事例が目立つ。

ネットバンキング被害の流れ

地方の法人口座、標的

被害に遭った金融機関は昨年の32から58に増え、うち47が地銀や信金、信組などだった。法人口座の被害が昨年の約9800万円から約4億8千万円に急増。地方の小規模な金融機関で、セキュリティー対策に手が回りにくい中小企業の口座が狙われている可能性がある。

法人口座から現金を不正に引き出すには、IDとパスワードのほか、銀行がユーザーに発行する電子証明書を入手する必要がある。警察庁によると、ユーザーのパソコンから電子証明書を盗み出したり、ユーザーになりすましたりするタイプのウイルスが出回っている可能性があるという。

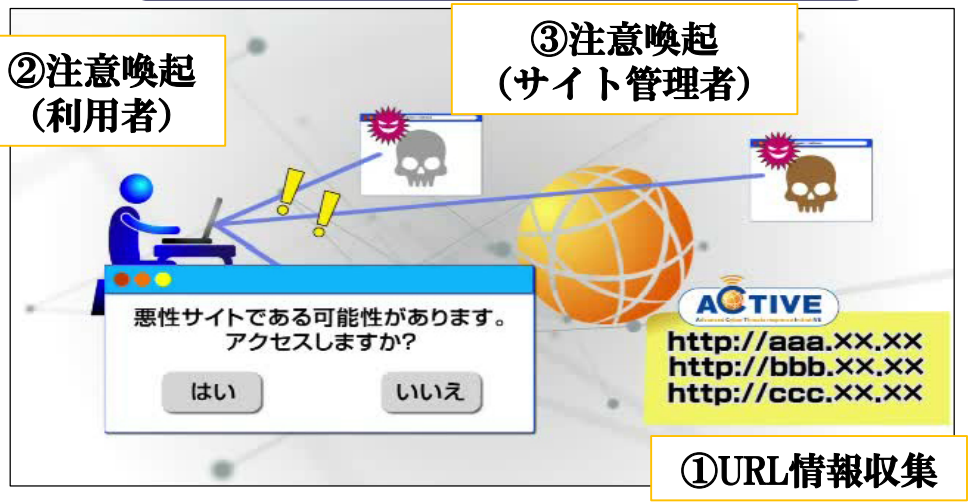
一方、不正送金に絡んで全国の警察が摘発した件数は、昨年の34件（68人）から47件（74人）に増えた。しかし大半は口座の不正売買や、不正送金を受けた口座から現金を引き出す役割で、犯行グループでは末端とみられる。IDやパスワードを実際に盗み出したり、送金を指示したりする中枢部には捜査が及んでいない。

平成26年5月16日（金）
日本経済新聞

ACTIVE（Advanced Cyber Threats response InitiatiVE）について

■ 平成25年11月から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（ACTIVE）を開始。

（１）マルウェア感染防止の取組



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。

（２）マルウェア駆除の取組

① マルウェアに感染した利用者のPCを特定。
② 利用者に適切な対策を取るよう注意喚起。
③ 注意喚起の内容に従いPCからマルウェアを駆除。

計画年数

5か年計画（平成25年度～29年度）

所要経費

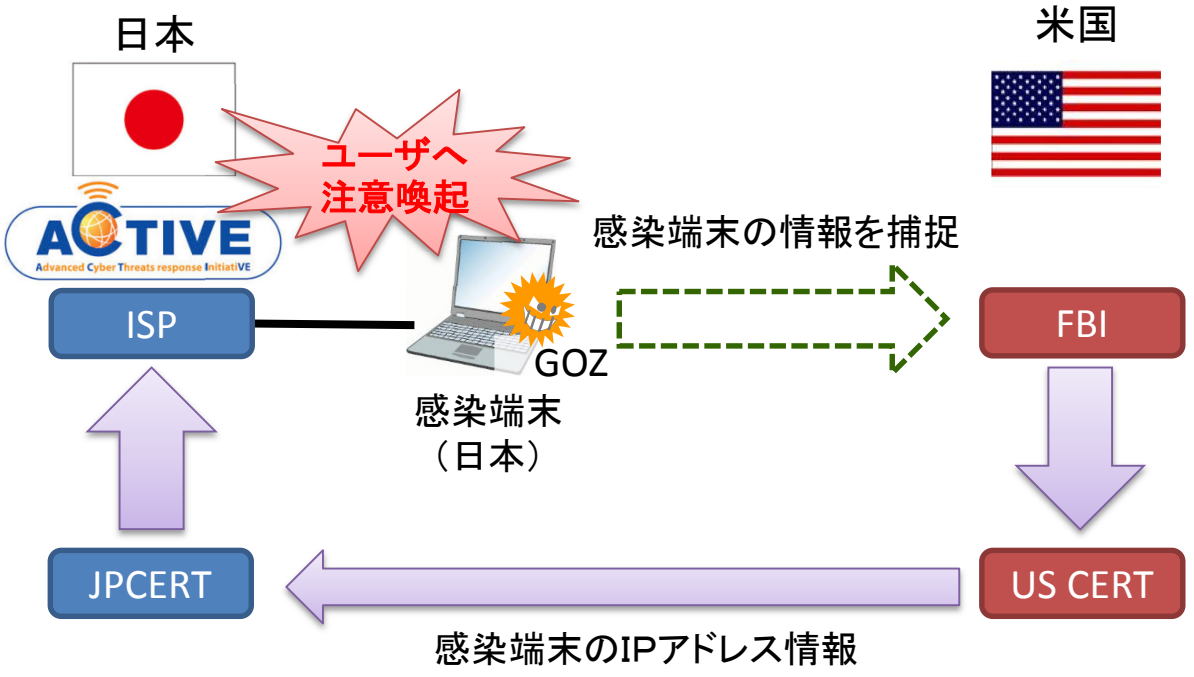
平成26年度予算額　３．５億円

国際的なマルウェア駆除作戦へのACTIVEの活用について

○ 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の感染者に対する注意喚起を実施。

イメージ図



ウイルス駆除、日米欧連携

FBIが対策プログラム

ネットバンキング不正送金

「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

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「Game Over 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「Game Over 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」に変貌するのが特徴。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手口が主流だ。

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の予知・即応技術の研究開発（PRACTICE）」について

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分散型サービス妨害攻撃（DDoS攻撃）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発生の予兆を検知し・迅速な対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。

実施内容

研究開発

サイバー攻撃の予兆解析技術の開発

- センサーを通じて収集・集約したサイバー攻撃情報の類似性・局所性・時系列性について自動的に分析し、既存のマルウェアの情報を除去することにより、未知のマルウェアによる攻撃の予兆を検知する技術を確立。
- DNSAmp攻撃を捕捉する環境を構築し、DNSAmp攻撃の予兆を検知する技術等を確立。

予兆情報の提供

攻撃情報の提供

実証実験

情報の提供・共有・即応体制の構築

- 予兆検知技術により得られた攻撃情報をもとに、リアルタイムにISP及びセキュリティベンダにアラート情報を提供するシステムを構築し、ISP間で迅速に対処する体制を整備。

早期警戒情報

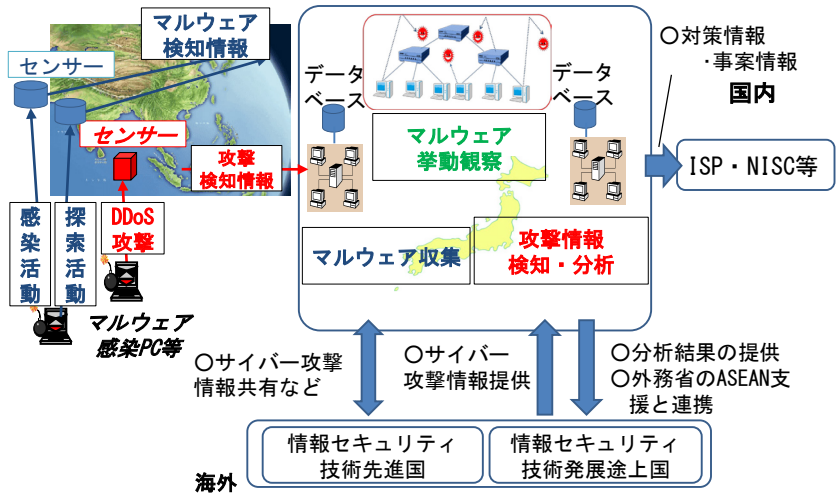
ISP・セキュリティベンダ等に提供

国際連携

諸外国との連携による情報共有

- ASEAN諸国等にセンサーを設置し、国外のサイバー攻撃情報を収集。
  現在シンガポール、フィリピン、インドネシア、モルディブ、タイ、マレーシアと連携。

施策イメージ



○ 計画年数 ・・・ 5年計画（平成23年度～平成27年度）

○ 予 算 額：平成２６年度当初予算 ３．０ 億円

M2Mにおける情報セキュリティ上の脅威の具体例

複合機の事例

日本の大学等において複合機をインターネットに接続した結果、複合機に保存されたデータがインターネット上で誰でも閲覧できる設定となっていることが判明。

複合機ネットワーク公開状態

東大など3大学

学生ら264人分個人情報

住民票や答案

初期設定変更せず

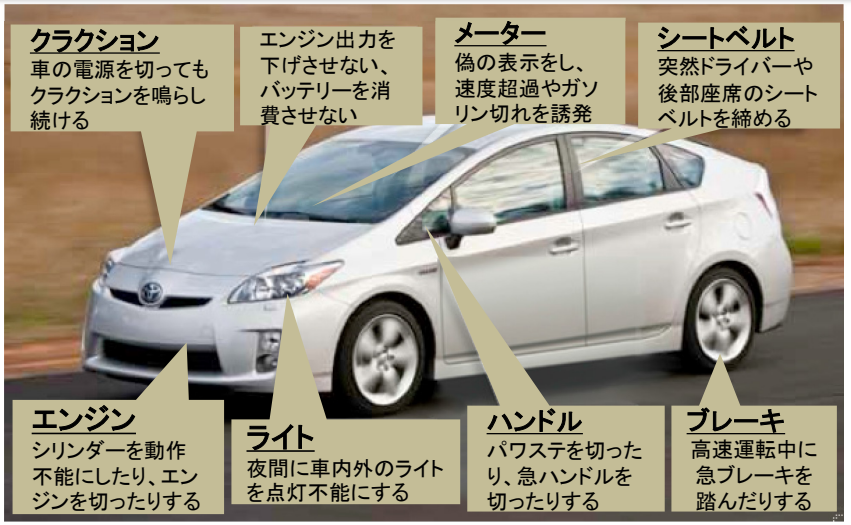
平成25年11月7日（木）
読売新聞

ウェアラブル機器の事例

米国において、無線通信機能を持つペースメーカーやインシュリンポンプに認証機能が存在せず、外部からのなりすましにより、これらの医療機器の電源の操作が可能であることが明らかにされた。

自動車の事例

ハッカーの世界的なイベント「DefCon」の２０１３年大会において、トヨタプリウスの内部ネットワーク（ＣＡＮ）をハッキングし、ハンドルやブレーキに関わるクリティカルなコントロール権限を奪うことが可能であることが実演された。



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。

課題に対する施策の方向性

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

施策概要

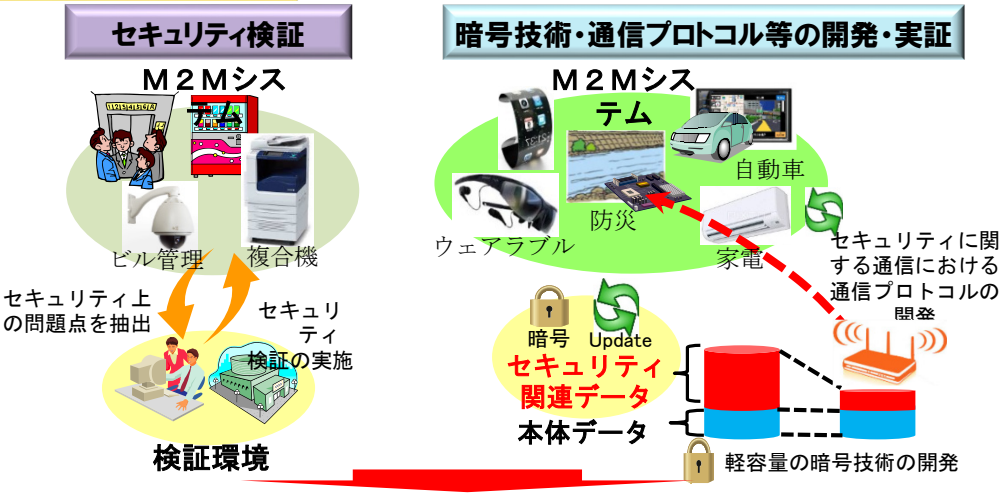
① 検証環境による情報セキュリティ検証を通じた、Ｍ２Ｍの設定・運用におけるセキュリティ基準の策定

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

① Ｍ２Ｍのセキュリティ検証環境を用いて、ビル管理等の既存のシステムに対するセキュリティ上の問題点の検証を行い、Ｍ２Ｍの設定・運用時のセキュリティ基準を策定する。

② ウェアラブル機器や自動車といった今後の普及が見込まれるＭ２Ｍシステムについて、機器の処理能力等に制約がある中でも実装が可能で、かつ長期間のセキュリティ品質が確保できる暗号通信技術及び通信プロトコルの開発・実証を行う。

施策イメージ



M2Mの情報セキュリティ技術の確立による安心・安全なM2M利用環境の実現

サイバー攻撃への対処における通信の秘密との関係について

サイバー攻撃への対処における通信の秘密との関係について

- サイバー攻撃への対策を実施するにあたっては、攻撃に係る通信に関する情報の取得・利用が必要となる場合があり、「通信の秘密」について留意することが必要。
- 「通信の秘密」の保護は、個人の私生活の自由を保護し、個人生活の安寧を保障する（プライバシーの保護）とともに、通信が人間の社会生活にとって必要不可欠なコミュニケーション手段であることから、憲法上の基本的人権の一つとして、憲法第21条 第2項において保障されているもの。
- 日本国憲法の規定を受け、電気通信事業法において、罰則をもって「通信の秘密」を保護する規定が定められており、電気通信事業法上「通信の秘密」は厳格に保護されている。

通信の秘密について

日本国憲法

第２１条　２　検閲は、これをしてはならない。**通信の秘密は、これを侵してはならない。**

電気通信事業法

（秘密の保護）

第４条　**電気通信事業者の取扱中に係る通信の秘密は、侵してはならない。**

※　「通信の秘密」とは、①個別の通信に係る通信内容のほか、②個別の通信に係る通信の日時、場所、通信当事者の氏名、住所・居所、電話番号などの当事者の識別符号、通信回数等これらの事項を知られることによって通信の意味内容を推知されるような事項すべてを含む。

第１７９条　電気通信事業者の取扱中に係る通信（第１６４条第２項に規定する通信を含む。）の秘密を侵した者は、２年以下の懲役又は１００万円以下の罰金に処する。

２　電気通信事業に従事する者が前項の行為をしたときは、３年以下の懲役又は２００万円以下の罰金に処する。

３　前２項の未遂罪は、罰する。

「通信の秘密」とは？

「侵す」の意味

＜侵害の３類型＞

一般に、通信の秘密を侵害する行為は、通信当事者以外の第三者による行為を念頭に、以下の３類型に大別。

【知得】

積極的に通信の秘密を知ろうとする意思のもとで知得しようとする行為

【窃用】

発信者又は受信者の意思に反して利用すること

【漏えい】

他人が知り得る状態に置くこと

ここにいう、知得や窃用には、機械的・自動的に特定の条件に合致する通信を検知し、当該通信を通信当事者の意思に反して利用する場合のように機械的・自動的に処理される仕組みであっても該当し得る。

通信の秘密が侵害されない又は侵害が許容される場合

①通信当事者の「同意」がある場合

②正当防衛、緊急避難、正当業務行為等の違法性阻却事由がある場合

通信の秘密に関する同意についての基本的な考え方

通信当事者の同意がある場合には、通信当事者の意思に反しないため、通信の秘密の侵害に当たらない。もっとも、以下の理由から、契約約款等に基づく事前の包括同意のみでは、一般的に有効な同意と解されていない。

① 約款は当事者の同意が推定可能な事項を定める性質であり、通信の秘密の利益を放棄させる内容はその性質になじまない

② 事前の包括同意は将来の事実に対する予測に基づくため対象・範囲が不明確となる

（平成22年5月総務省「利用者視点を踏まえたICTサービスに係る諸問題に関する研究会（※）」第二次提言より）

※ 総務省主催の研究会として平成21年4月から開催。

通信の秘密侵害に関する違法性阻却事由についての基本的な考え方

○ 緊急時に行われる対策については、一般的に、正当防衛、緊急避難（※）の要件を満たす場合には通信の秘密の侵害について違法性が阻却される。

※「緊急避難」として違法性が阻却されるためには、①現在の危難の存在、②法益の権衡、③補充性の全ての要件を満たすことが必要。
「正当防衛」として違法性が阻却されるためには、①急迫不正の侵害に対して、②自己又は他人の権利を防衛ために、③やむを得ずした行為であること、の全ての要件を満たすことが必要。

○ 常時行われる対策については、急迫性、現在の危難といった要件を満たさないものと思われるため、正当業務行為（※）に当たる場合には違法性が阻却される。

※ 電気通信事業者による通信の秘密の侵害行為が正当業務行為となる場合については、実務上の運用事例を通じて一定の考え方が整理されてきている。これまでに正当業務行為が認められた事例は、ア．通信事業者が課金・料金請求目的で顧客の通信履歴を利用する行為、イ．ISP がルータで通信のヘッダ情報を用いて経路を制御する行為等の通信事業を維持・継続する上で必要な行為に加え、ウ．ネットワークの安定的運用に必要な措置であって、目的の正当性や行為の必要性、手段の相当性から相当と認められる行為（大量通信に対する帯域制御等）といったものが挙げられる。こうした事例の根底にある基本的な考え方は、国民全体が共有する社会インフラとしての通信サービスの特質を踏まえ、利用者である国民全体にとっての電気通信役務の円滑な提供という見地から正当・必要と考えられる措置を正当業務行為として認めるものである。

（平成22年5月総務省「利用者視点を踏まえたICTサービスに係る諸問題に関する研究会」第二次提言より）

ACTIVE(Advanced Cyber Threats response InitiatiVE)と通信の秘密との関係

■ 平成25年11月から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(ACTIVE)を開始。

(1)マルウェア感染防止の取組

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。

通信の秘密との関係

ISP等が、利用者がアクセスしようとするサイトのURLの情報を知得し、注意喚起を行うことについては、利用者の同意に基づいて行われており、通信の秘密の侵害にあたらない。

(2)マルウェア駆除の取組

① マルウェアに感染した利用者のPCを特定。
② 利用者に適切な対策を取るよう注意喚起。
③ 注意喚起の内容に従いPCからマルウェアを駆除。

通信の秘密との関係

① ACTIVE事務局が、マルウェア感染パソコンからハニーポットに来た通信における送信元IPアドレスを、当該IPアドレスの割当てを行っているISPに提供することは、ACTIVE事務局は当該通信を受信する一方当事者であり、通信の秘密の侵害にあたらないと考えられる。

② 上記ISPが、当該IPアドレスをどの契約者に割り当てたか顧客情報と突合し、該当契約者を割り出す行為は、マルウェア感染パソコンに対する現在の危難を避けるための緊急避難として、通信の秘密の侵害に係る違法性は阻却されると考えられる。

サイバーセキュリティに関する政府戦略について

【サイバーセキュリティ戦略（平成25年6月10日情報セキュリティ政策会議決定）抜粋】

3. 取組分野

（1）「強靱な」サイバー空間の構築

④サイバー空間の衛生

潜在型のマルウェアの挙動等について、高度かつ迅速に検知するための技術開発等を行うとともに、サイバー攻撃の複雑・巧妙化などサイバー空間を取り巻くリスクの深刻化の状況等を踏まえ、**情報セキュリティを目的とした通信解析の可能性等、通信の秘密等に配慮した、関連制度の柔軟な運用の在り方について検討**する。

【サイバーセキュリティ2013（平成25年6月27日情報セキュリティ政策会議決定）抜粋】

Ⅱ 具体的な取組

1「強靱な」サイバー空間の構築

④サイバー空間の衛生

（ノ）情報セキュリティ目的の通信解析の可能性等関連制度の柔軟な運用の在り方の検討（総務省）

総務省において、**情報セキュリティを目的とした通信解析の可能性等、通信の秘密等に配慮した、関連制度の柔軟な運用の在り方について、**可能な範囲で速やかに**一定の結論を得る**よう、サイバー攻撃の実態、これに対する現行の取組状況等の実態把握に努めるとともに、情報セキュリティを目的とした通信解析における課題の洗い出し等を行う。

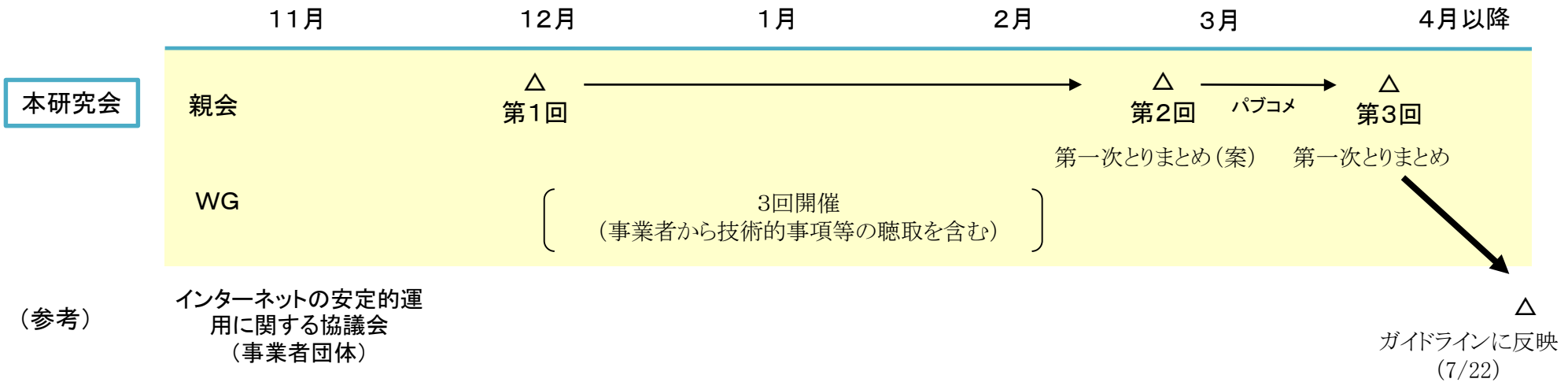
電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会

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予定）

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



第一次とりまとめ（平成26年4月4日公表）における論点

① ACTIVEの普及展開

- マルウェア配布サイトへのアクセスに対する注意喚起における有効な同意取得のあり方

② マルウェア感染駆除の拡大

- C&Cサーバ※に蓄積されている通信履歴に基づくマルウェア感染者の特定及び注意喚起の実施

※ 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。

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の遮断の実施

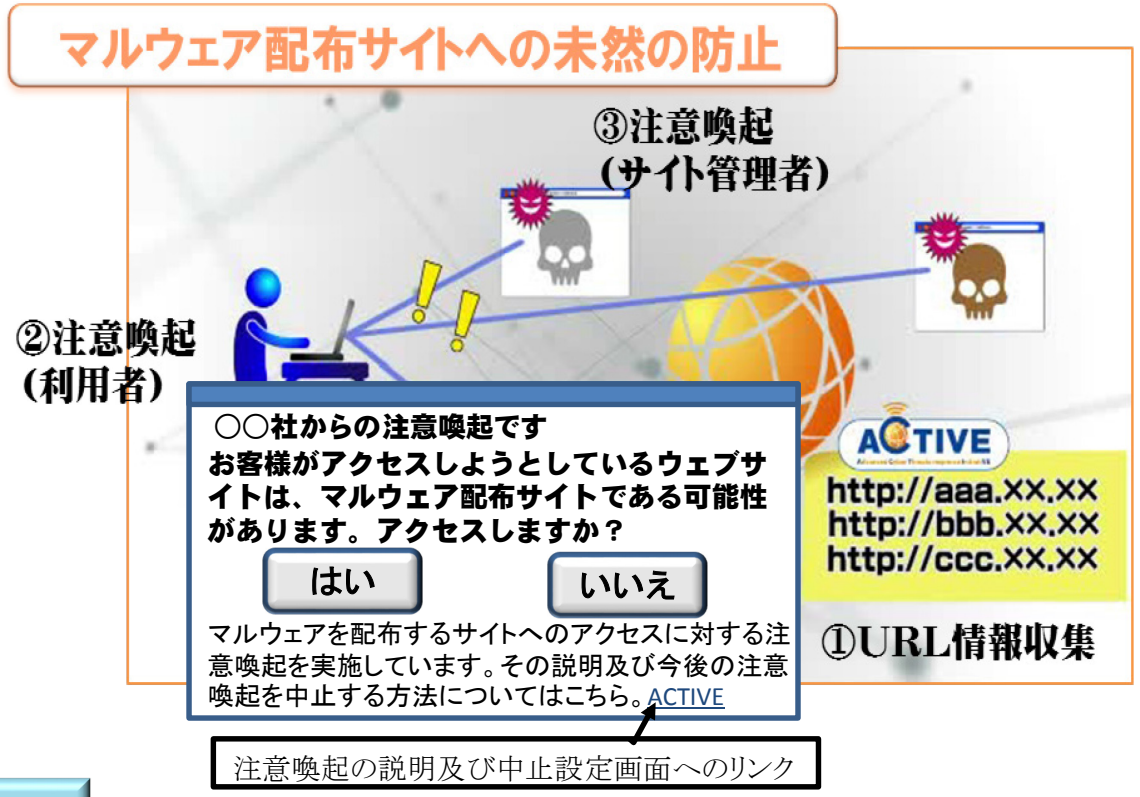
④ SMTP認証の情報（ID及びパスワード）を悪用したスパムメールへの対処

- SMTP認証ID・パスワードの不正利用の蓋然性が高いアカウントの一時停止や、正規の利用者への注意喚起の実施
- SMTP認証のID・パスワードのハッキング攻撃の蓋然性が高いものについて、当該IPアドレスからのSMTP認証の拒否の実施

課題① ACTIVE(Advanced Cyber Threats response InitiatiVE)の普及展開

論点

■ 利用者がマルウェア配布サイトにアクセス(閲覧)しようとする場合に、ISPがアクセスに係るIPアドレス又はURLを検知し、そのアクセスに対して注意喚起画面を表示することについて、利用者の同意を得て行うとして、どのような場合に通信の秘密に属する情報(アクセス先IPアドレス又はURL)の利用についての有効な同意と言えるか。



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。

整理

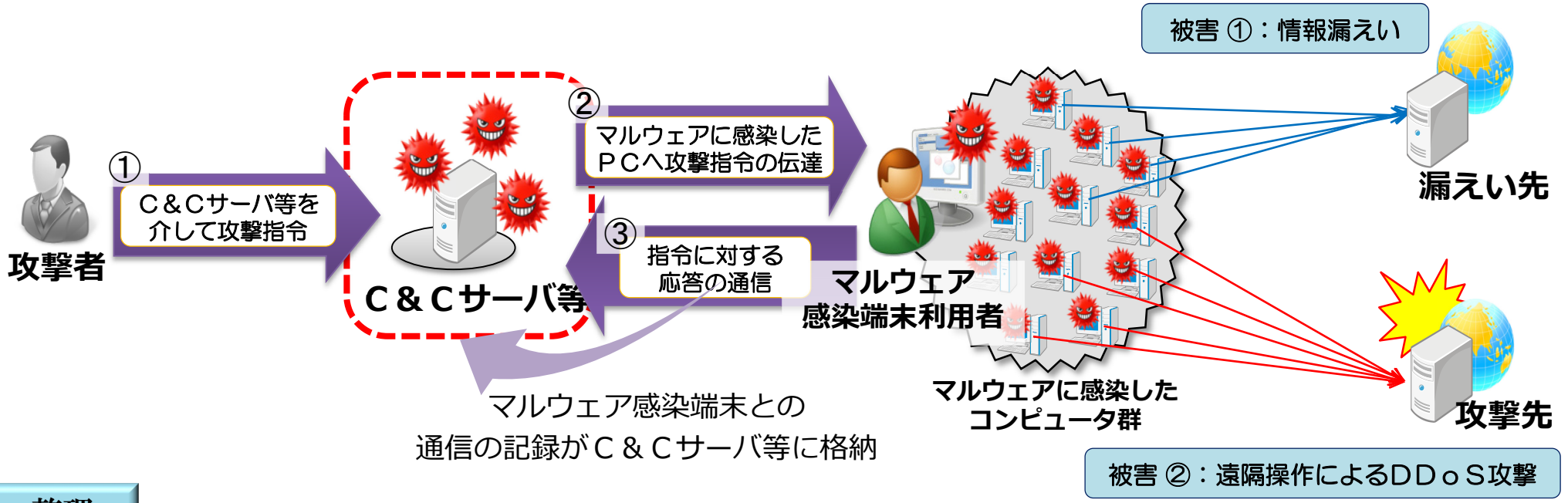
■ 次の3条件を満たせば、個別の同意ではなく、約款に基づく包括的な同意であっても有効な同意ということができる。

1 利用者が、約款に同意した後も、**随時、同意内容を変更できる**契約内容であること
2 約款の内容や随時同意内容を変更できることについて**相応の周知が図られている**こと
3 注意喚起画面に、**注意喚起の趣旨や随時同意内容を変更できること等の説明がされている**こと

課題②　マルウェア感染駆除の拡大について

論点

■　C&Cサーバ（Command and Controlサーバ）がテイクダウンされた場合、当該サーバに蓄積されているマルウェア感染端末との通信履歴のうち、IPアドレス及びタイムスタンプをもとに、ISPにおいて、当該時刻に当該IPアドレスを割り当てた利用者を割り出し、メール等により個別の注意喚起することは、通信の秘密との関係上どのように整理が可能か。



整理

■　以下のことから、どの利用者に、当該時刻に当該IPアドレスを割り当てたか確認した結果を、当該者への注意喚起以外の用途で利用しない場合には、**緊急避難として違法性が阻却される**

「**現在の危難の存在**」：C&Cサーバによる制御が行われている場合には、端末に対する法益侵害が顕在化・継続している。

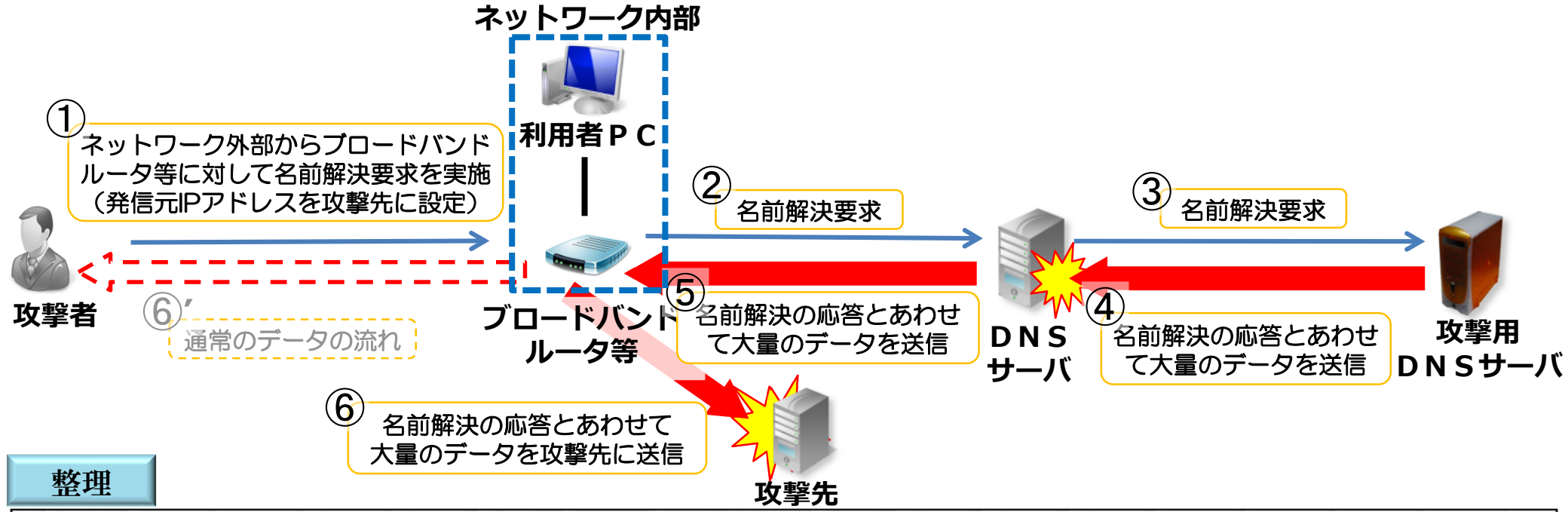
「**法益の権衡**」：本件対策により避けようとする害（マルウェアに感染している状態）に対して、侵害される通信の秘密は、IPアドレスとタイムスタンプを該当利用者を割り出す限度で利用するのみである。

「**補充性**」：感染端末の利用者に対する個別の注意喚起以外の方法でマルウェア駆除の目的達成に有効な手立てが考えがたい。

課題③　新たなDDoS攻撃であるDNSAmp攻撃の防止（１）

論点

■ DNS Amp攻撃を未然に防止するため、ISPのネットワークの入り口又は出口において、そこを通過する全ての通信の宛先IPアドレス及び宛先ポート番号を常時確認して、動的IPアドレス宛であってUDP53番ポートに対して送信された通信を割り出し、これをブロックすることは、通信の秘密との関係上どのように整理が可能か。



整理

■ 以下のことから、本件対策は、宛先IPアドレス及びポート番号を確認した結果をDNSAmp攻撃の防止以外の用途で利用しない場合は、**正当業務行為として違法性が阻却される**

「**目的の正当性**」：本件対策は、ISPのDNSサーバが過負荷状態となることによる、インターネットアクセスやメール送信遅延等の発生を防止し、もってインターネット接続役務等の安定的提供を図るためのものである。

「**行為の必要性**」：他の部分での対策は困難である一方、本件ISP網の入口・出口での対策は可能かつ必要である。

「**手段の相当性**」：侵害される通信の秘密は、宛先IPアドレス及びポート番号のみであること等から、検知・確認結果を本件対策以外の用途で利用しない場合は、通信の秘密侵害の程度は相対的に低く、またこのような通信をブロックすることは通常のインターネット利用への影響は考え難い。

課題③　新たなDDoS攻撃であるDNSAmp攻撃の防止（２）

－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における議論のポイント－

【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の検討資料より一部抜粋】

○　DNSAmpによるDDoS攻撃を未然に防止するためには、①の部分で、その引き金である、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検知してブロックすることが有効である。

※　①以前に、仕掛けをしている公開DNSサーバのすべてを発見して対応を講ずることは非現実的であるから、この部分での対応は困難。②～⑤での対応については、ISPのDNSサーバ上の通信の挙動等を仮にモニタリングしたとしても、ISP側からみると、ISPのDNSサーバを経由する通信は、名前解決要求が行われる際の正常な通信の挙動と区別がつかない上に、その発信元も詐称された者からの通常の通信に見え、一概に不正な通信とは認識できないこと等から、この部分での遮断等の対応は困難。

○　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ブロックするためには、ISPの網の入り口又は出口において、管理下の動的IPアドレスレンジ向けに入ってくる通信を検知し、UDP53番ポートに入ってくる通信のみ遮断する必要がある。

※　攻撃が成功するとISPのDNSサーバが影響を受けることから、被害のインパクトが大きいため、一度攻撃が発生すると事後的にそれを速やかに鎮静化することは困難である。さらに、ブロードバンドルータ等には通常通信ログが残っていないことから、攻撃者の事後追跡も困難であり、そのため、DNSAmpによるDDoS攻撃を未然に防止するためには、すべての通信の宛先IPアドレス及びポート番号を常時確認して、該当する通信をブロックする必要がある

○　上記の措置を講ずるために確認する通信の秘密は、宛先のIPアドレス及びポート番号のみであり、これを機械的に確認して、動的IPアドレス宛てであってUDP53番ポートに対して送信された通信を検知すれば足りる。

※　他方、通信の宛先のポート番号がUDP53番ポートであっても宛先のIPアドレスが固定IPアドレスである通信については、利用者がインターネットアクセスの際に通常利用することとなるISP自身のDNSサーバ（同サーバには固定IPアドレスが割り当てられている。）への名前解決要求や、利用者が設置した固定IPアドレスを割り当てられたDNSサーバへの名前解決要求等、ブロックすべきではない通信が存在するため、慎重な対応が必要。

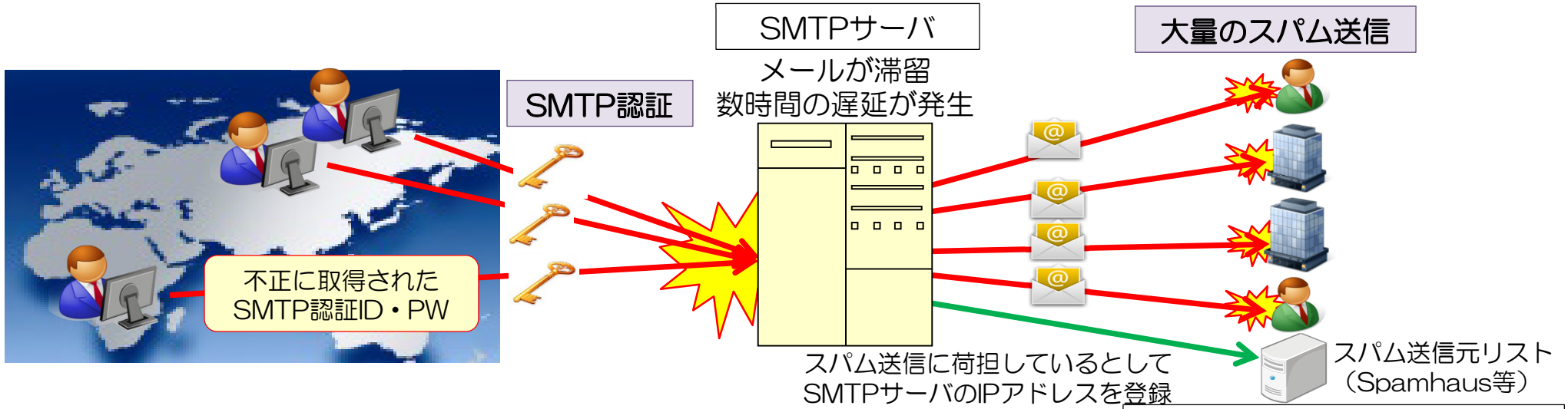
○　なお、通常の通信環境下においては、動的IPアドレスに対するインターネット側からの名前解決要求は想定されない。

○　②～⑤の部分では、正当な通信との区別が困難であり、対応を講じることは難しいこと、また、そもそも、DNSAmpによるDDoS攻撃の発生を事前に予測することは困難である上に、一度攻撃が発生すると事後的にそれを速やかに鎮静化することは困難であること等から、**現時点では、①の部分での対応として、すべての通信の宛先IPアドレス及びポート番号を常時確認して、該当する通信をブロックする本件対策を講ずる以外に、有用な手段は見当たらない**。

課題④　SMTP認証の情報を悪用したスパムメールへの対処[対策１]

論点

■　他人のSMTP認証のID・パスワードを悪用したスパムメールの送信を防止するため、サーバの負荷が急増し警告が出た場合、メールサーバに滞留したメールに係るSMTP認証の発信元IPアドレス、タイムスタンプ、メールアドレス、SMTP認証IDを分析することにより、SMTP認証ID・パスワードの不正利用の蓋然性が高いものについて、利用者への注意喚起や一時認証停止を行うことは、通信の秘密との関係上どのように整理が可能か。



整理

■　以下のことから、本件対策は、滞留したメールに係る、SMTP認証の発信元IPアドレス、タイムスタンプ、メールアドレスの確認結果をスパムメール対策以外の用途で利用しない場合は、**正当業務行為として違法性が阻却される**

「**目的の正当性**」：本件対策は、SMTP認証のIDを不正に利用したスパムメールの大量送信によってSMTPサーバの負荷が急増することにより生じるメールの遅延等を防止し、もって電気通信役務の安定的運用を図るためのものである。

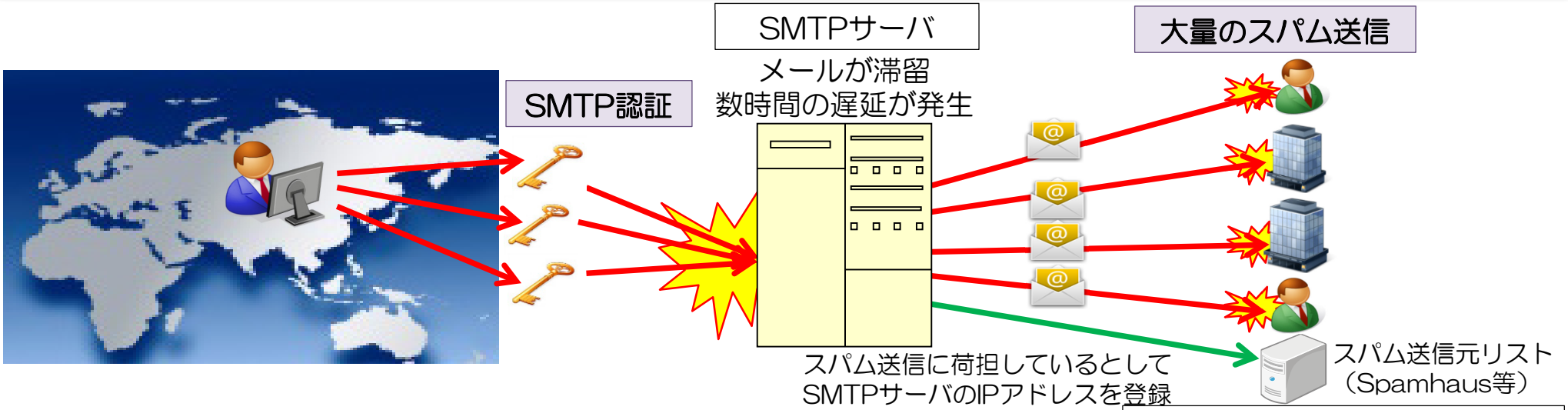
「**行為の必要性**」：不正利用の蓋然性が高いSMTP認証IDを特定した上で、当該IDからのSMTP認証を一時停止するとともに正規の利用者に注意喚起を行うことは必要。

「**手段の相当性**」：侵害される通信の秘密は、滞留したメールに係るSMTP認証の発信元IPアドレス、タイムスタンプ、メールアドレスのみであり、検知・確認結果を本件対策以外の用途で利用しない場合は、侵害の程度は相対的に低い。

課題④　SMTP認証の情報を悪用したスパムメールへの対処[対策2]

論点

■　他人のSMTP認証のID・パスワードを悪用したスパムメールの送信を防止するため、大量のSMTP認証の失敗が発生し警告が出た場合、SMTP認証に係るログから認証の発信元IPアドレス、タイムスタンプ、認証回数、認証間隔（頻度）を分析し、SMTP認証のID・パスワードのハッキング攻撃の蓋然性が高いものについて、当該攻撃期間中、当該IPアドレスからのSMTP認証を止めることは、通信の秘密との関係上どのように整理が可能か。



整理

■　以下のことから、本件対策は、SMTP認証の発信元IPアドレス、タイムスタンプ、認証回数、認証間隔（頻度）の確認結果をスパムメール対策以外の用途で利用しない場合は、**正当業務行為として違法性が阻却される**

「**目的の正当性**」：本件対策は、SMTP認証のID・パスワードの不正取得にから生じうる大量通信等の弊害を防止し、もって正規の契約者に対する安定的な電気通信役務の提供を確保するためのものである。

「**行為の必要性**」：ID・パスワードのハッキング攻撃の継続を放置すれば、SMTP認証IDの不正取得が生じうることから、それを阻止するために当該IPアドレスからのSMTP認証を阻止することは必要。

「**手段の相当性**」：侵害される通信の秘密は、認証の発信元IPアドレス、タイムスタンプ、認証回数、認証間隔（頻度）のみであること等から、検知・確認結果を本件対策以外の用途で利用しない場合は、侵害の程度は相対的に低い。

「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」について

対応に係る整理のポイント

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。

2020年東京五輪に向けて

2020年のICT環境の変化を見据えた情報セキュリティ対策を推進し、東京五輪等の安心・安全な開催に貢献。

2012年ロンドン五輪での経験

◆ ロンドン五輪では、大会を標的としたサイバー攻撃が多数発生。

・大会期間中、オリンピックのウェブサイトに対して約2億回の悪意のあるアクセスや、1秒間に1.1万アクセスにも及ぶDDoS攻撃が発生。

・開会式会場の電力供給監視制御システムに対するサイバー攻撃があるとの事前情報に基づき、制御システムをネットワーク制御から手動制御に切換。

2020年東京五輪に向けた取組

◆ 東京五輪が開催される2020年にはIoT（Internet of Things）の広がりなどICT環境の大きな変化が想定。DDoS攻撃の踏み台となり得るネットワーク接続機器の爆発的な増加が見込まれるなど、新たな攻撃の出現を見据えた情報セキュリティ対策が必要。

◆ このようなICT環境の変化を見据え、安心・安全な東京五輪の開催に向けて、

・サイバー攻撃への対応体制の強化（サイバー攻撃の発生状況や発生の予兆に関する情報の事業者や関係機関等での共有や、サイバー攻撃に対する共同対処の在り方の検討等）

・新たな分野の情報セキュリティ上の課題解決（新技術の普及とともに登場する新たなデバイスやサービスを踏まえ、例えば機器間通信（M2M）等へのサイバー攻撃に対する対策手法の研究開発や実証等）

等の取組を促進。

ルーター攻撃 ネット障害

480万世帯、一時不通

家庭用を標的

インターネットに複数の端末をつなげられる家庭用ルーターを悪用する新たなサイバー攻撃があり、ネットが利用できなくなる通信障害が今春以降、多発していることが分かった。少なくとも480万世帯が通信障害の影響を受けており、総務省は悪用されるルーターの利用者に対し、ソフトを更新するよう呼び掛けている。〈関連記事34面〉

この攻撃は「DNSアンプ攻撃」と呼ばれ、大量にデータを送りつけてサーバーを使えなくするDDoS攻撃の一種。

一部の家庭用ルーターが、本来受け付けない外部からの通信に応答してしまう弱点を悪用し、攻撃者がそのルーター経由でプロバイダーのサーバーにデータを送ると、データが数十倍に増幅される。これを繰り返してサーバーに過大な負荷を与え、ネット利用を一定期間できなくさせる。高度な技術を必要としないため、初心者ハッカーの腕試しではないかとみられている。

今年5月末以降、この攻撃による通信障害を明らかにしたプロバイダーは、ジュピターテレコム（JCOM、東京都千代田区、利用者282万世帯）、ケイ・オプティコム（大阪市、150万世帯）、アルテリア・ネットワークス（東京都港区、56万世帯）、DTI（渋谷区、非公表）などがある。このほか昨年8月には、NTTコミュニケーションズ（千代田区）が運営する最大手の「OCN」（815万世帯）でも、約40分間にわたってネット利用ができなくなった。

民間団体の調査によると、悪用される弱点を持つルーターなどは国内に約54万台あり、うち9割は家庭用とみられる。ルーター大手のバッファロー（名古屋市）が昨年に出荷した一部製品にも弱点があり、同社がソフト更新を呼び掛けている。

この攻撃を受け、総務省は今年4月、プロバイダーが通信を遮断しても電気通信事業法に違反しないとする見解をまとめた。

サイバー攻撃に詳しい中京大の鈴木常彦教授（ネットワークセキュリティー）は「攻撃者が弱点のあるルーターを一斉に攻撃すると、日本中のネットをダウンさせることも可能だ。深刻な脅威で、ほかの利用者に迷惑をかける恐れがあり、利用者は早急に更新すべきだ」と指摘している。

ルーター インターネットで通信する際、パソコンやタブレット、スマートフォンなど複数の端末を同時に接続できる機器。無線電波を発する無線LANルーターなどがあり、家庭用は数千円から2万円程度で販売されている。

平成26年8月2日（土） 読売新聞