講演１

総務省における情報セキュリティ政策の最新動向

平成２７年３月１１日

情報流通行政局
情報セキュリティ対策室
本田　知之

最近のセキュリティトピック

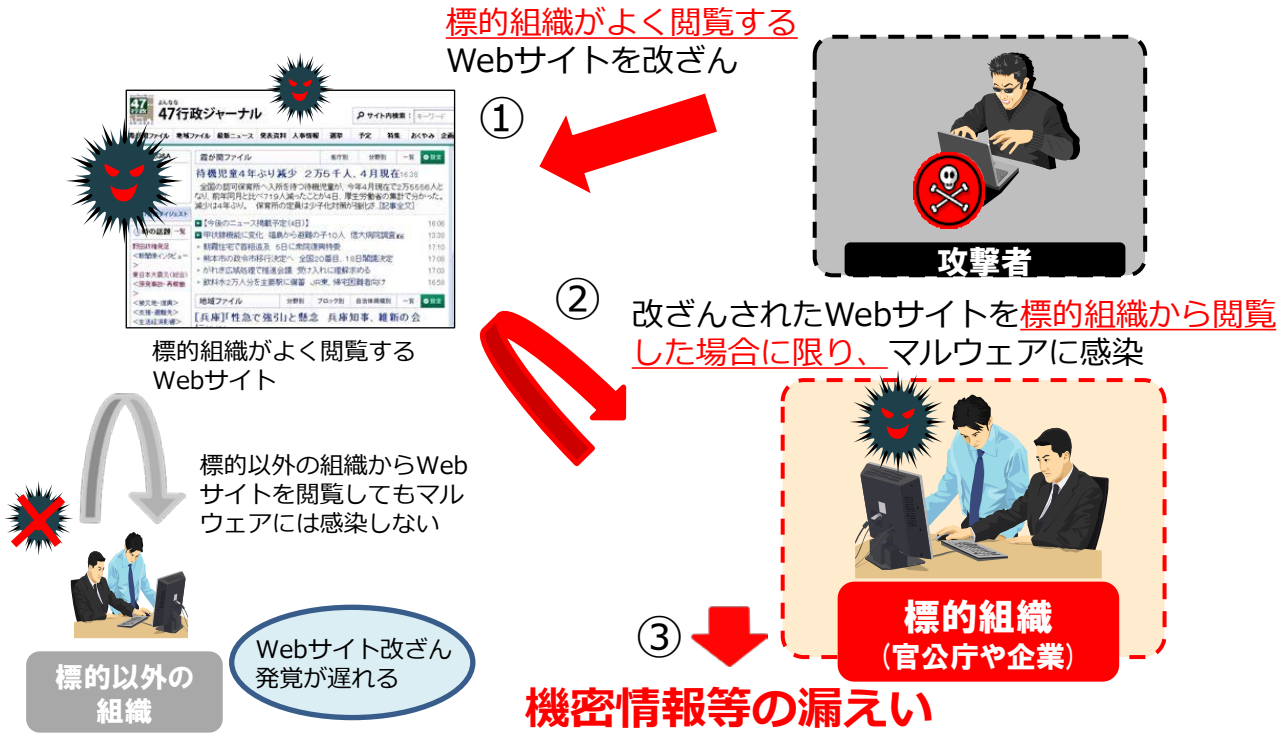
標的型攻撃（水飲み場攻撃）について

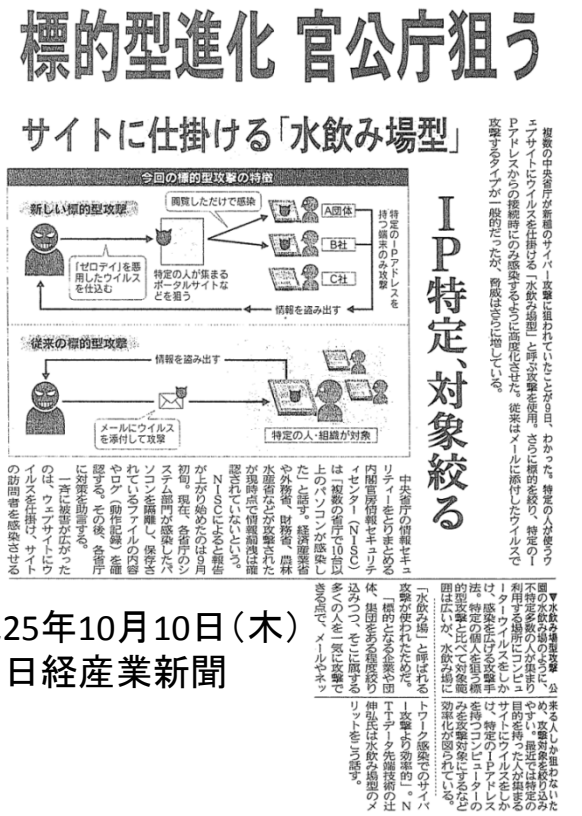
背景・経緯

- 昨今、**標的型攻撃**（特定の組織や個人を標的に複数の攻撃手法を組み合わせることで機密情報の窃取等を行う攻撃）**により、官公庁・民間企業等の機密情報が窃取される事態が頻発**。
- **標的型攻撃は日々巧妙化**しており、マルウェア添付メールによる攻撃も従来の「ばらまき型」から「やりとり型」へと進化しているほか、多くの人が閲覧するウェブサイトを改ざんしてマルウェアを仕掛け、標的とする組織のIPからアクセスがあった場合のみマルウェアに感染させる**「水飲み場攻撃※」など新たな攻撃が生み出されている**。
- 水飲み場攻撃については、平成25年8～9月に複数の新聞社で運営される有料ニュースサイト「47行政ジャーナル」が改ざんされ、経済産業省、財務省、農林水産省等の中央省庁の端末が感染している。

※ 水飲み場攻撃（Watering Hole Attack）：猛獣がオアシスなどに潜んで獲物を待ち伏せ、そこに水を飲みに集まってくる動物を狙って襲いかかるのになぞらえた名称

水飲み場型攻撃の事例




標的型進化 官公庁狙う

サイトに仕掛ける「水飲み場型」

IP特定、対象絞る

平成25年10月10日（木）
日経産業新聞

インターネットバンキングによる不正送金被害について

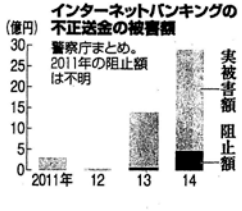
■ **インターネットバンキングによる不正送金被害が平成２５年６月以降急増**しており、**平成２６年一年間の被害額は約２９億円にのぼり、昨年一年間の被害額（約１４億円）を更新。**

■ 被害の主な原因は、コンピュータウイルス、フィッシング等により不正画面が表示され、インターネットバンキングのログインに関するＩＤ・パスワードが窃取されたことによるもの。

不正送金被害額の推移

期間	件数	被害額（実被害額）
H26	1,876件	約29億1000万円（約24億3600万円）
H25	1,315件	約14億 600万円（約13億3000万円）
H24	64件	約 4800万円（約 4800万円）

ネットバンク被害 最悪29億円



地銀や信金、狙われる 昨年

インターネットバンキングの口座から預金が不正に送金される被害は昨年1年間で1876件あり、被害額は約29億1千万円に上ることがわかった。前年より561件、約15億400万円多く、ともに過去最悪。地方銀行などの法人口座が狙われているという。

警察庁が12日、発表した。客がアクセスしたのを検知し、自動的に犯人側の口座に不正送金する「自立型ウイルス」によるとみられる被害も、国内で初めて確認したという。

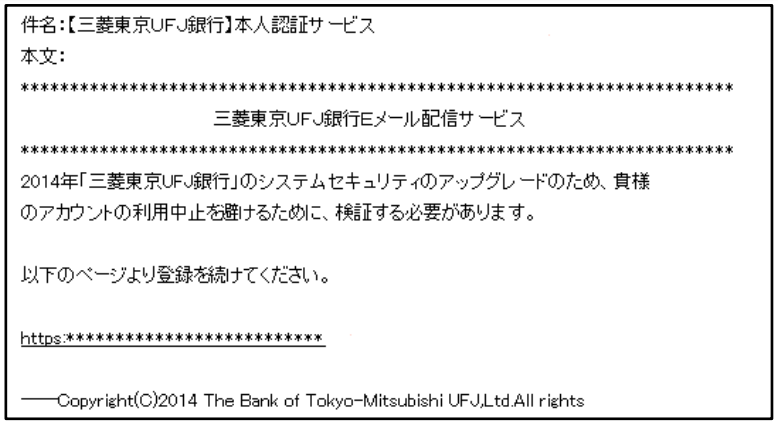
警察庁のまとめでは、被害が確認された金融機関は前年の32から102に増えた。金融機関の種別では、地銀・信用金庫・信用組合の被害額が約10億8500万円（前年比約8億8200万円増）で増加が目立った。口座の種別では、法人口座の被害額が約10億8800万円（同約9億9千万円増）で、このうち、地銀・信金・信組のものが約8億3700万円（同約7億9千万円増）を占めた。

犯人側の送金処理後に金融機関が水際で実害を防いだ「阻止額」も初めてまとめ、前年の約7600万円から、昨年は約4億7300万円に増えた。同庁は、事件で使われた口座と氏名や住所が同じ口座を凍結する▽法人口座の送金は客に事実関係を確認してから処理する――という取り組みが広がったためとみている。

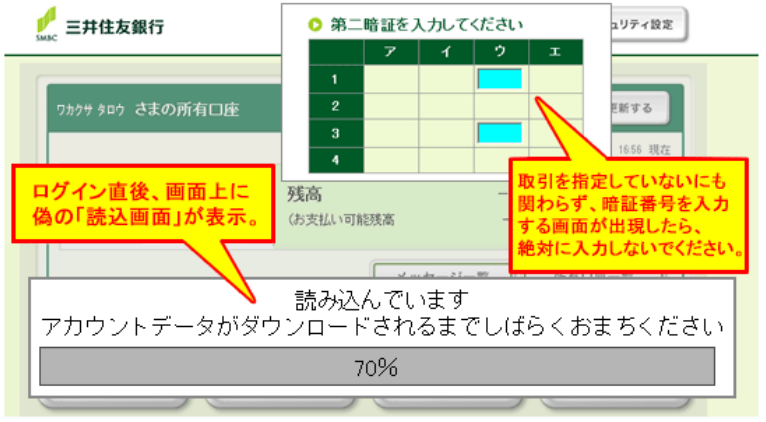
自立型ウイルスは、客のパソコンに感染し、客がパソコンでネットバンキングにアクセスすると自動的に犯人側の口座に不正送金する。客の操作画面に送金手続きの画面が表れないため、被害に気づきにくい。

（八木拓郎）

平成27年２月12日（木）
朝日新聞夕刊



銀行を騙り、アカウントの確認、アップデート等を名目に不正画面へと誘導するメールを送信

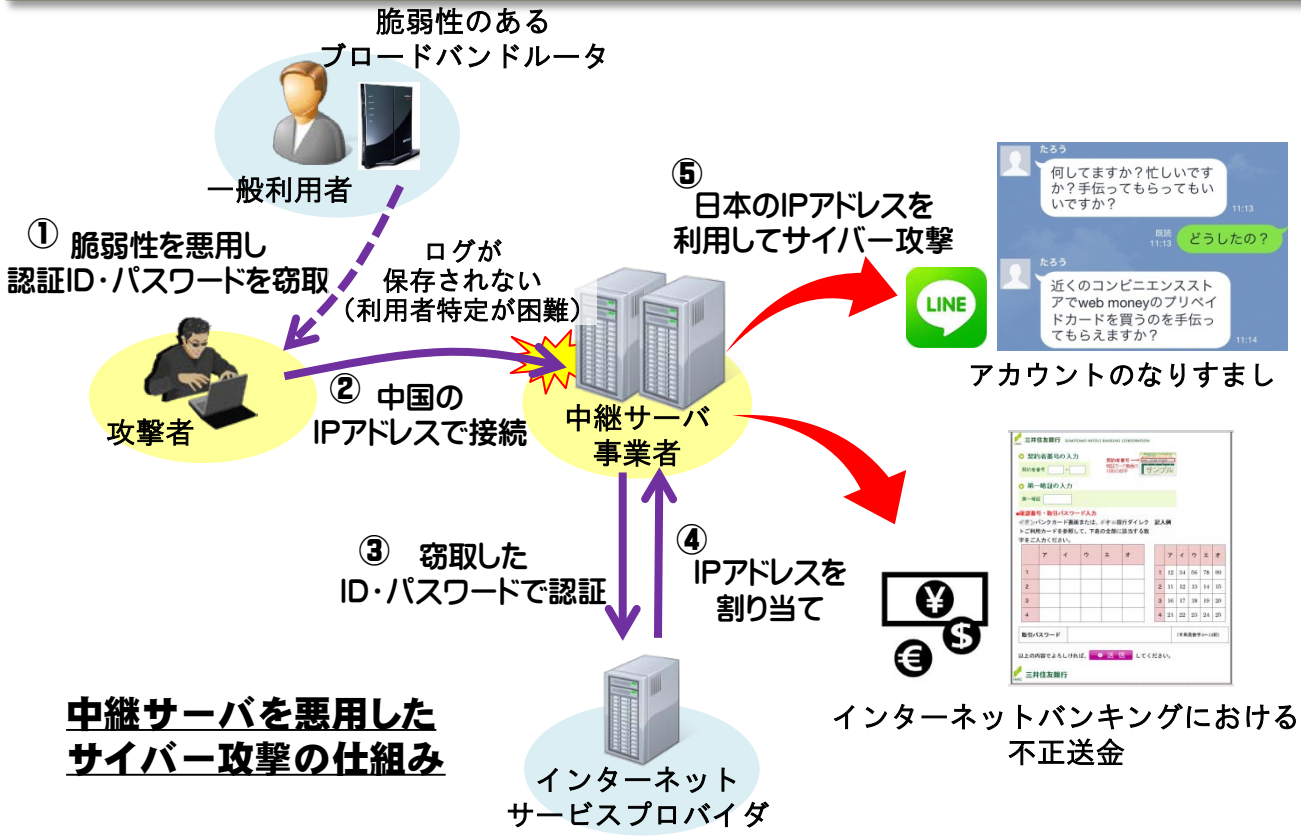


不正画面の例（三井住友銀行のサイトを模倣）

中継サーバ(プロキシサーバ)を悪用したサイバー攻撃について

背景・経緯

- インターネットユーザが利用する**特定のブロードバンドルータに脆弱性があり、PPPoE認証**（インターネットを利用するための認証）**のＩＤ・パスワードが第三者に大量に窃取**される事案が発生。
- 攻撃者は**窃取したＩＤ・パスワードと中継サーバを用いて、企業のサイト等にサイバー攻撃を実施**。無料通話アプリ「LINE」のアカウントなりすましによる電子マネーの詐取、インターネットバンキングにおける不正送金、リスト型攻撃等のサイバー攻撃に利用されたとされている。また、攻撃者が窃取したPPPoE認証のパスワードを変更し、正規の利用者がインターネットを利用できなくなる事態も発生している。
- 警視庁と１９道府県警の合同捜査本部は平成26年11月19日に中継サーバ運営業者を不正アクセス禁止法で一斉捜索。



**中継サーバを悪用した
サイバー攻撃の仕組み**

無線ルーターからID流出

中国向け中継サーバー 業者ら11人逮捕

不正接続容疑

ネット接続に使うID・パスワード流出の流れ

中国 / 中国の代理店 / ID・パスワードの情報提供者を紹介 / プロバイダー / 中継サーバー / ID・パスワードを使い不正アクセス / ID・パスワード流出 / 攻撃 / ネットバンキング / オンラインゲーム / ロジテック製ルーター転用者 / 日本

平成26年11月20日（木）
読売新聞

クラウド入力ＩＭＥについて

背景・経緯

- BaiduIME、Simeji、GoogleIMEといった**クラウド入力IME※はインターネット上のクラウドサーバと通信を行い、高精度な変換や顔文字、新語等の流行語の変換を実現**するため、ユーザの人気を博している。
- クラウド入力IMEは多くの**ユーザの変換結果をクラウド上で収集分析し、リアルタイムにIMEの辞書へ反映・活用できる効果の高い仕組みであることは事実**である。

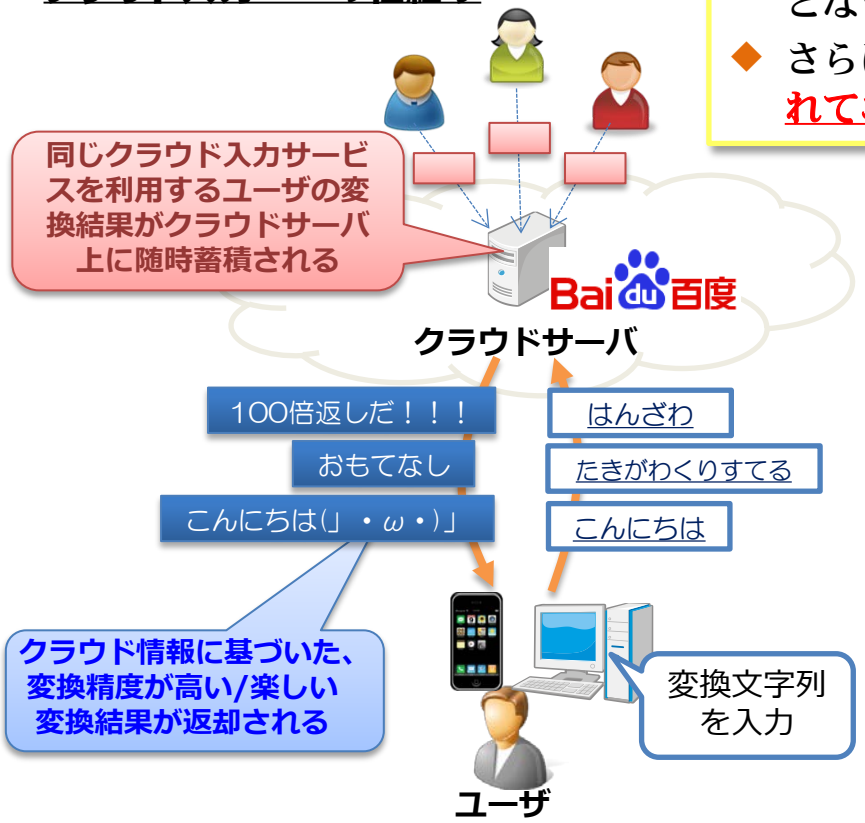
※ IME（Input Method Editor）：文字入力補助ソフト

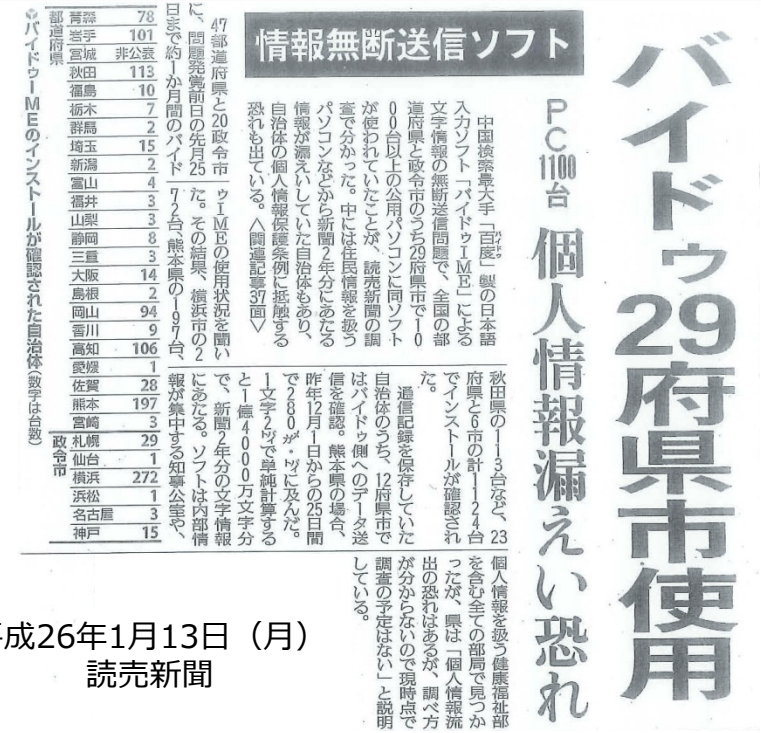
課題

- 以前のBaiduIME/Simejiは「クラウド入力機能」のデフォルト設定がオンとなっており、**クラウドへの情報送信に同意していない利用者が多く発生**。
- さらに、無料ソフトやレノボ社PCの一部に**BaiduIMEがバンドル（付属）されており、インストールの認識なく使う場合も**。

「サプライチェーン問題」

クラウド入力IMEの仕組み





バイドゥ29府県市使用

PC1100台 個人情報漏えい恐れ

情報無断送信ソフト

中国検索最大手「百度（バイドゥ）」製の日本語入力ソフト「バイドゥIME」による文字情報の無断送信問題で、全国の都道府県と政令市のうち29府県市で100台以上の公用パソコンに同ソフトが使われていたことが、読売新聞の調査で分かった。中には住民情報を扱うパソコンなどから新聞2年分にあたる情報が漏えいしていた自治体もあり、自治体の個人情報保護条例に抵触する恐れも出ている。〈関連記事37面〉

47都道府県と20政令市に、問題発覚前日の先月25日までの1か月間のバイドゥIMEの使用状況を聞いた。その結果、横浜市の272台、熊本県の197台、報が集中する知事公室や、秋田県の113台など、23府県と6市の計1124台でインストールが確認された。

通信記録を保存していた自治体のうち、12府県市ではバイドゥ側へのデータ送信を確認。熊本県の場合、昨年12月1日からの25日間で2800ギガ・バイトに及んだ。1文字2バイトで単純計算すると1億4000万文字分で、新聞2年分の文字情報にあたる。ソフトは内部情

個人情報を扱う健康福祉部を含む全ての部局で見つかったが、県は「個人情報流出の恐れはあるが、調べ方が分からないので現時点で調査の予定はない」と説明している。

バイドゥIMEのインストールが確認された自治体（数字は台数）

都道府県		政令市	
青森	78	札幌	29
岩手	101	仙台	1
宮城	非公表	横浜	272
秋田	113	浜松	1
福島	10	名古屋	3
栃木	7	神戸	15
群馬	2		
埼玉	15		
新潟	2		
富山	4		
福井	3		
山梨	3		
静岡	8		
三重	3		
大阪	14		
島根	2		
岡山	94		
香川	9		
高知	106		
愛媛	1		
佐賀	28		
熊本	197		
宮崎	3		

平成26年1月13日（月）
読売新聞

インターネット上の無料翻訳ソフトについて

背景・経緯

■ 最近、インターネットの無料翻訳サービスにおいて、入力した文章や翻訳結果がネット上で誰でも見られる状態になっており、中央省庁や民間企業の業務メールなどの情報が流出した疑いが生じている。

■ これらの翻訳サービスについて、主要な言語から使用人口の少ない言語に至るまで多くの言語を取り扱っており、非常に便利なサービスであることは事実であるが、入力した内容について運営者に取得されている可能性がある。

・オンライン翻訳サイトをはじめ、主に**一般消費者向けにネット上で無料提供されている**、ウェブメールサービス、グループサービス、検索サービス、オンラインストレージ、データ転送、ソーシャルメディア、日本語文字入力補助（ＩＭＥ）等の**サービスについては、利用の際の情報管理について保証がないことが一般的**

・要機密情報はもちろん、メールも含め、情報をいったん外部に送信してしまうと、その後は情報の管理が及ばず、**第三者に見られるリスクがあるものと十分認識**し、送信内容や方法（暗号化など）について**細心の注意を払うことが必要**

平成27年2月20日付け内閣官房内閣サイバーセキュリティセンター発出
各府省庁への注意喚起文（抜粋）

ネット翻訳でメール流出

無料サイト 省庁、銀行情報

インターネットの特定の無料翻訳サイト㊟に入力した文章や翻訳結果が、ネット上で誰でも見られる状態になっていることが分かった。メガバンクの顧客情報のほか、中央省庁や自動車メーカーの業務メールなど、発信者を特定できるものだけで少なくとも30件の流出が確認された。入力内容などが公開されることが判明したのは、このサイトだけだが、気軽に使える無料翻訳サイトの利用方法については今後、影響が広がりそうだ。〈関連記事3面〉

この翻訳サイトは、グーグルやヤフー、エキサイトなどの大手サイトではないが、英語や中国語に対応しており、現地の企業関係者らが利用しているとみられる。翻訳したい文章や単語を入力画面に打ち込めば自動で翻訳され、最大3通りの訳文が表示される。一方、入力した文章や訳文は、本人が気付かないままネット上に公開され、本人は直接削除できない。

㊟無料翻訳サイト ネット上で日本語などを入力すると、外国語に翻訳してくれるサイト。外国語の種類はサイトによって異なる。日本語の翻訳は2000年頃から始まり、翻訳の精度は年々高まっているとされる。利用者数も増えており、大手のエキサイトの場合、13年度の国内利用者数は2510万人で、翻訳回数は5億7500万回に上った。

問題の翻訳サイト
「公開」のしくみ
入力
入力欄（参考例）
ジョン・スミス様
○○カンパニーの鈴木です。
極秘でお願いします。
当社は△△社の買収を検討しています。1億ドルと見積もっております。
英語 ○中国語 ○フランス語
翻訳
ネットに公開状態に
誰でも見られる

あるメガバンクでは昨年10月、インドネシアにある支店に宛てた、日系企業への100万件の融資をめぐる行内連絡メールが公開状態となった。現地の外国人行員が現地語に翻訳したという。今月18日に融資先企業の指摘を受け、この企業に陳謝した。

ある省庁の中堅幹部と、大手家電メーカーの社員とのメールのやりとりも公開された。メールには、この幹部の携帯電話番号や別の中堅幹部の実名などが記されていた。自動車メーカーでは、インドネシア現地法人への連絡メールなどが公開された。

この翻訳サイトを利用し、2013年1月頃に作成したメールの文面が公開されていることから、少なくとも2年以上、日本のメールなどがネット上に公開されていたとみられる。

このサイトの開設者とされる中国・重慶の中国人男性の連絡先に電話をすると、妻を名乗る女性が出て、「夫はいない。そのような会社はない」などと話した。

情報セキュリティー会社・ラックの西本逸郎・最高技術責任者の話「よく確認もせずに、この無料翻訳サイトを業務で使うのは論外だが、その他のサイトでも、翻訳した文章は運営会社側に渡っている。業務の機密などを取得している。頻繁にメールを翻訳するのは極力避けて、リスクを考えながら使うべきだろう」

平成27年2月20日（金）
読売新聞朝刊

要点

◆ これらのウェブサービスの利用に当たっては、サービスの運営者に**送信した内容を取得・分析されている可能性があることを認識した上で利用すること**。

ソニー・ピクチャーズ エンタテインメント　サイバー攻撃被害

● 概要

■　**平成26年11月下旬、ソニー・ピクチャーズエンタテインメント（SPE）にサイバー攻撃が行われ、従業員情報、公開前映画のデータ等の機密情報が流出**するという事件が発生。SPEが配給した金正恩第１書記暗殺をテーマにした映画「The Interview」の公開に対する抗議とみられている。

■　米国政府は北朝鮮による攻撃であると推測している。根拠として、過去の攻撃手法との類似性、利用PC言語、利用されたIPアドレスが北朝鮮のインフラと関連がある等としているが、明確な根拠データは開示されていない。

■　平成26年12月下旬には、今度は北朝鮮において、一時インターネットが利用できなくなる事態が発生。これについて、北朝鮮は米国が行ったと非難しているが、米国は関与を認めていない。

●主な報道（時系列）

年月日	概要
平成26年　6月	SPEが映画「The Interview」予告を公開。北朝鮮は同映画を非難。
11月24日	**SPEへ大規模なサイバー攻撃。未公開映画や従業員給与情報など流出。**
12月18日	米大統領報道官が「深刻な国家安全保障の問題」と発言。
12月19日	FBIがサイバー攻撃の北朝鮮の関与を断定。
12月20日	北朝鮮側は関与を否定する一方で、アメリカとの共同調査を提案。これに対して米国家安全保障会議（NSC）の報道官は、FBIの結論通り北朝鮮による攻撃に違いないとの認識を示す。
12月23日	**北朝鮮のインターネット接続障害が発生。**
平成27年 1月1日	**SPEへの攻撃は中国のIPアドレス経由であったとの報道。**
1月2日	北朝鮮への追加経済制裁を許可する米国大統領令。

The Interview

インタビュー番組の司会者とプロデューサーが、番組のファンである金正恩第一書記にインタビューを試みるコメディ映画

米国におけるサイバーセキュリティ情報集約のための新組織設立

●２０１５年２月１０日、米国はサイバー攻撃に関して連邦省庁間での情報共有・連携を改善するための新たな組織「**Cyber Threat Intelligence Integration Center (CTIIC)」の創設**を発表。

●関連する省庁ができるだけリアルタイムで脅威を認識できるよう、多様なサイバー脅威の「点と点をつなぐ」ことが目的。

●米国国家情報長官（Director of National Intelligence）の指揮下。

●約５０人体制。予算は約3, 500万ドル。

＜米国のインテリジェンス・コミュニティ＞

◆国家情報長官を頂点とする中央集権型の体制
◆6省15機関に跨がる組織。10万人規模

＜メンバー＞
・中央情報局（CIA）
・国防総省
　国防情報局（DIA）、国家安全保障局（NSA） 等
・司法省
　連邦捜査局（FBI）、連邦捜査国家保安部（NSS） 等
・国土安全保障省
　沿岸警備隊情報部（CGI）、情報分析・インフラ保護部 等
・エネルギー省
　不拡散・国家安全保障部 等
・国務省
・財務省

✔CTIICは、2003年に設立された、重要テロ情報の収集、共有等を目的とする「National Counterterroism Center」に倣うものとの位置づけ。

✔CTIICは、連邦議会の承認手続きを経ることなく、大統領命令によって創設される見込み。

米国における情報共有促進のための大統領命令（2015年2月13日）

●２０１５年２月１３日、ホワイトハウス主催により「サイバーセキュリティ及び消費者保護に関するホワイトハウス・サミット」を開催（於スタンフォード大学）。

●オバマ大統領がスピーチを行い、**民間部門におけるサイバーセキュリティに係る情報共有を促進するための大統領命令**を発表するとともに、同命令案に署名。

●同命令案により、民間部門における情報連携の促進、官民間の情報共有の向上、プライバシー及び市民の自由権の保護等を図る。

民間部門における情報連携の促進

◆情報共有及び分析組織（Information Sharing and Analysis Organizations (ISAOs)）の設立促進

民間企業間及び官民間の情報共有の中核としてのISAOs（NPO組織、協会組織、一企業等）。ISACsはISAOsの構成要素。

◆ISAOsのための共通的な任意基準の策定

DHSに対して、NPO組織の創設のために必要な財政負担を指示。

官民間の情報共有の向上

◆ISAOsとの情報共有規約締結のためのDHSの権限の明確化

DHS内のNCCICがISAOsと情報共有のための規約を締結するための枠組みを整備

◆サイバー脅威に係る機密情報への民間企業のアクセスの実現

サイバー脅威に係る機密情報を承認する連邦機関のリストにDHSを追加し、ISAOsによる機密情報へのアクセスを確保

強力なプライバシー及び市民の自由権の保護

ISAOsが遵守すべき任意基準の中に、データ最小化等のプライバシー保護措置を盛り込む。

将来の立法へ向けた道筋作り

民間企業にインセンティブを付与し、情報共有を促進するために不可欠な免責のための枠組みとしてISAOsという概念を作り、新たな立法への道筋を作る。

政府における情報セキュリティ政策動向（サイバーセキュリティ基本法）

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

戦略案の意見

重要事項について緊密連携

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

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

（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

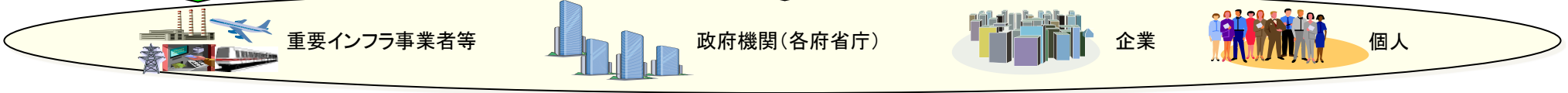
重要インフラ所管省庁
- 金融庁（金融機関）
- 総務省（地方公共団体、情報通信）
- 厚生労働省（医療、水道）
- 経済産業省（電力、ガス、化学、クレジット、石油）
- 国土交通省（鉄道、航空、物流）

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）



総務省における情報セキュリティ政策動向

我が国における情報セキュリティ推進体制

総務省

情報流通行政局情報セキュリティ対策室

- ◆ **サイバー空間の根幹であるネットワークを防護**する観点から、攻撃の検知・予防、ウイルス感染対策等を推進
- ◆ 組織の標的型攻撃対策や個人ユーザのウイルス感染防止等のユーザ対策を推進

……（独）情報通信研究機構（NICT）【ネットワークセキュリティ分野における基盤的な研究開発を推進】

……（一財）日本データ通信協会 テレコム・アイザック推進会議 【通信事業者等間の情報共有及び連携を促進】

外務省

大臣官房情報通信課

- ◆ サイバー政策担当大使を設置し、**国際連携強化のための取組**等を実施

経済産業省

商務情報政策局情報セキュリティ政策室

- ◆ 電力・ガス等の**制御システムやソフトウェア・機器**等のセキュリティ対策を推進

……（独）情報処理推進機構（IPA）
【個人・組織の各種相談窓口、普及啓発を実施】
（H26.7～ サイバーレスキュー隊）

……（一社）JPCERTコーディネーションセンター
【各国CERT※の連携窓口として、攻撃情報の収集等を実施】
※CERT：Computer Emergency Response Team

内閣官房 内閣サイバーセキュリティセンター（NISC）

- ◆ 基本戦略の立案及び関係省庁との総合調整
- ◆ GSOCを運用し、政府ネットワークの監視等を実施

※ GSOC:政府機関情報セキュリティ横断監視・即応調整チーム（Government Security Operation Coordination team）

防衛省

運用企画局 サイバー攻撃対処・情報保証企画室

- ◆ サイバー空間における**自衛隊の能力・態勢強化に向けた取組**の推進
- ◆ サイバー防衛隊（約100人体制）を設置（H26.3～）

……技術研究本部【自衛隊のネットワーク防御のための研究開発を推進】

警察庁

長官官房審議官（サイバーセキュリティ担当）
生活安全局情報技術犯罪対策課、警備局警備企画課

- ◆ **サイバー犯罪・サイバー攻撃の取締り**等を推進

重要インフラ※所管省庁（５省庁１３分野）

※ 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

金融庁（金融）、**総務省**（**情報通信、地方公共団体**）、厚生労働省（医療、水道）、国土交通省（航空、鉄道、物流）、経済産業省（電力、ガス、クレジット、石油、化学）

総務省における情報セキュリティ政策動向（予算プロジェクト）

総務省における情報セキュリティ対策の概要

2020年東京五輪等の安心・安全な開催も見据え、国内で多角的な情報セキュリティ対策プロジェクトを実施するとともに、得られた成果の国際展開を推進することで、「サイバーセキュリティ立国」実現に貢献。

○ 現在、ネットワークの防護、ユーザの情報セキュリティ対策強化の観点から、ISP事業者との連携も図りつつ、以下のプロジェクト等を実施中。

組織に対する情報セキュリティ対策

官公庁、重要インフラ事業者等の組織を対象として、実践的サイバー防御演習「CYDER」を実施（平成25年度～、平成27年度予定額：400百万円）

個人に対する情報セキュリティ対策

一般のインターネット利用者等の個人を対象として、主要なISP事業者と連携してマルウェア感染防止プロジェクト「ACTIVE」を実施（平成25年度～、平成27年度予定額：405百万円）

国際連携の推進

ASEAN諸国等との国際連携によるサイバー攻撃予知・即応プロジェクト「PRACTICE」を実施（平成23年度～、平成26年度補正予算額：200百万円）

○ 今後は、2020年東京五輪等の開催も見据え、IoT（Internet of Things）の本格的な普及等、ICT環境の変化に対応した情報セキュリティ対策を推進。

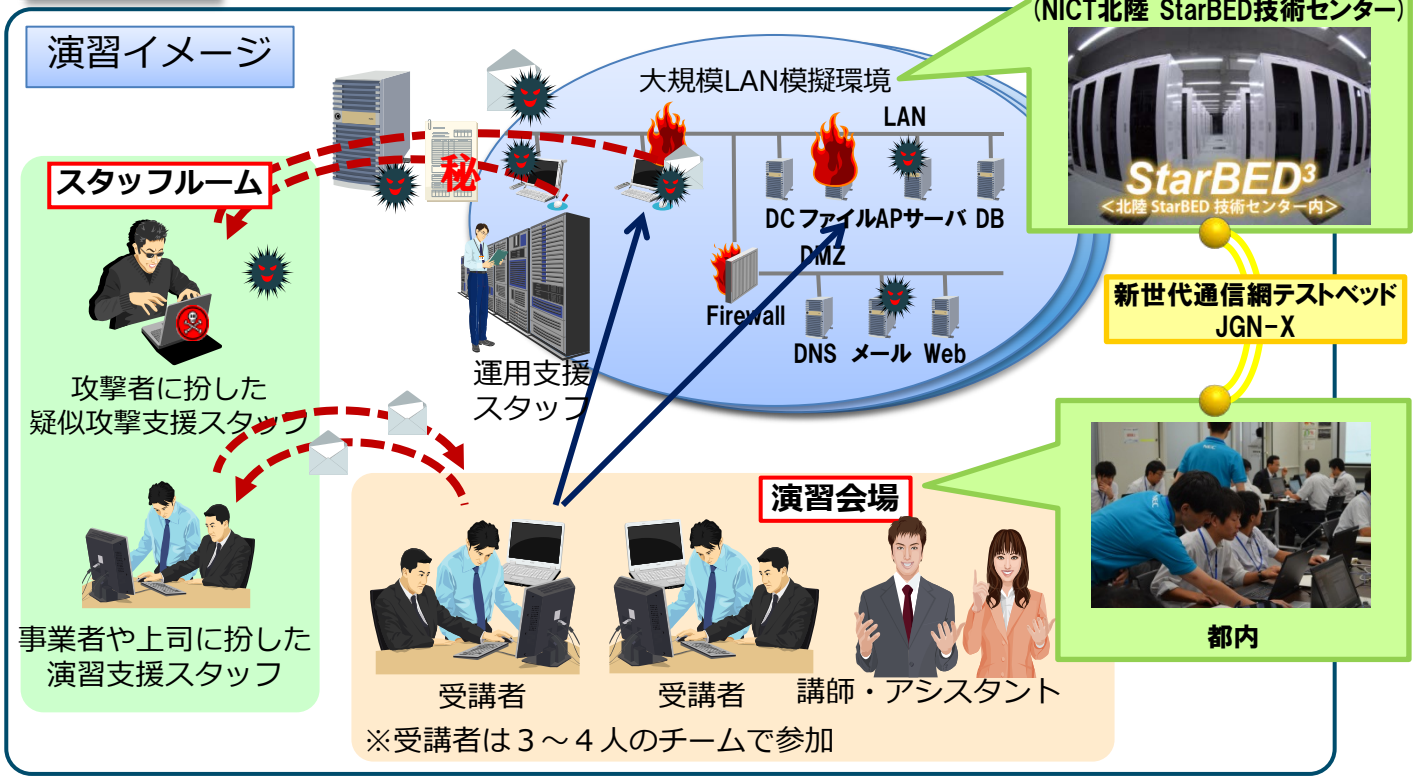
M2Mにおける情報セキュリティ対策

※M2Mセキュリティ実証事業
（平成27年度新規、平成27年度予定額：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



平成26年度の特徴

- ✓ **参加組織数が増加**
  ３３組織（H25） → **６２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。

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

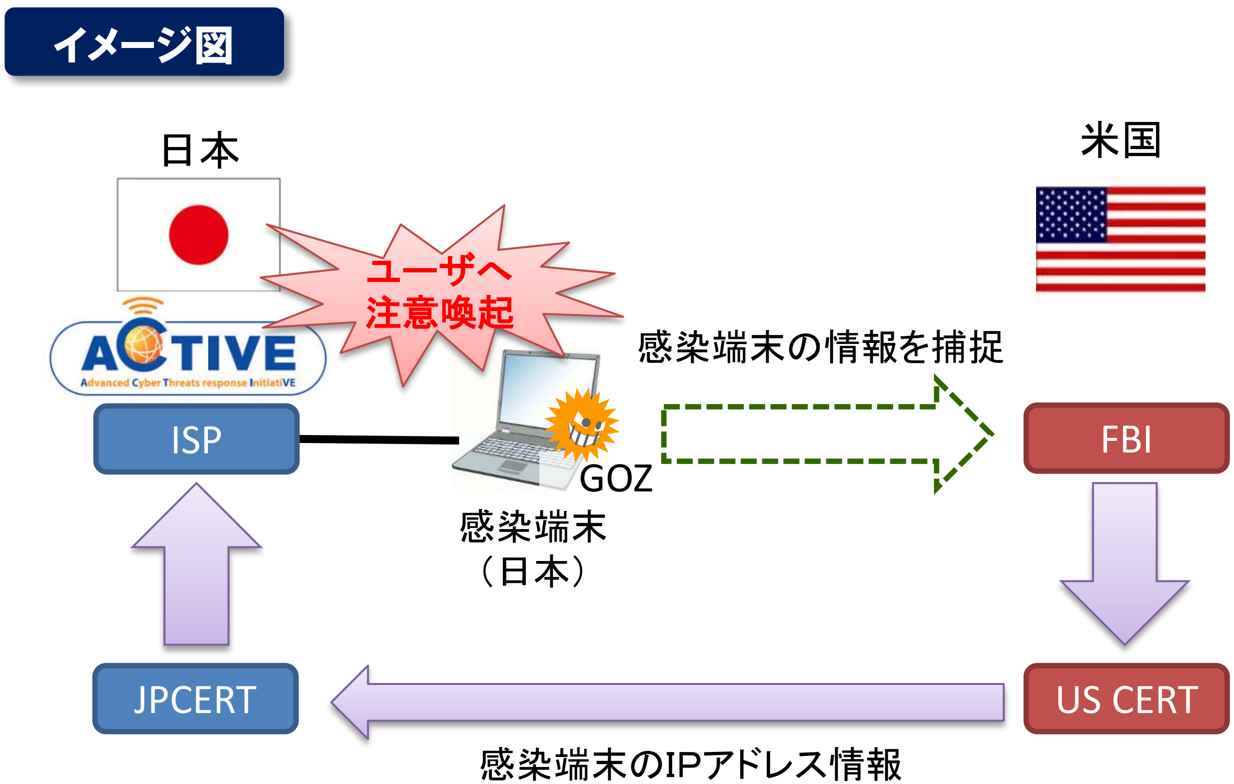
① マルウェア配布サイトのURL情報をリスト化。
② マルウェア配布サイトにアクセスしようとする利用者に注意喚起。
③ マルウェア配布サイトの管理者に対しても適切な対策を取るよう注意喚起。

（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。

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。



ネットバンキング不正送金

ウイルス駆除、日米欧連携

FBIが対策プログラム

「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「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1億ドル以上という。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、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

情報セキュリティ関係のASEANとの国際連携

地理的・経済的に密接に関連するアジア太平洋地域連携を重視

● **日・ASEANサイバーセキュリティ協力に関する閣僚政策会議**（2013年9月東京にて）
- セキュリティをテーマとする日・ASEANで初の閣僚レベルの会議
- 我が国からは、次のプロジェクトによる協力を提案

①JASPER(Japan-ASEAN Security Partnership)

i）PRACTICE：我が国及び連携国に設置したセンサーにて、サイバー攻撃発生の予兆を検知するためのプロジェクト

ii)DAEDALUS：連携国内のPCからのウィルス感染が疑われるトラフィックが観測された場合に、連携国に警告を送付するプロジェクト

②ASEANサイバーセキュリティ人材育成イニシアティブ

● **日・ASEAN情報セキュリティ政策会議**
- 2009年に第１回を開催し、2014年10月7日・8日、第7回を東京で開催。
- 閣僚政策会議での議論の具体化を議論。

PRACTICE連携国		DAEDALUS連携国	
・タイ	2013年2月～	・ミャンマー	2013年10月～
・マレーシア	2013年3月～	・ラオス	2013年11月～
・インドネシア	2013年5月～	・インドネシア	2013年11月～
・フィリピン	2014年1月～	・フィリピン	2013年12月～
・シンガポール	2014年3月～	・マレーシア	2014年3月～

連携国拡大の働きかけ

ASEANにおけるサイバー脅威の認識共有、情報交換のための基盤として活用

ASEANサイバーセキュリティ人材育成イニシアティブ

① JICA専門家派遣
- 2014年７月から２年半、インドネシアに派遣
- ASEAN各国のニーズに合わせた研修を企画・立案

② CYDER（実践的サイバー防御演習）の海外展開
- ASEAN域内でのCYDER演習実施の検討

政府職員のサイバー攻撃等への対応能力の強化

M2Mにおける情報セキュリティの確保について

背景

- IoT社会の本格的到来により、これまでインターネットに接続されていなかったモノ・システムがネットワークに接続されることで**サイバー空間の外延が拡大し、新たなサイバー空間上の脅威が発生しうる**。
- **2020年におけるIoT対応製品は約250億台**（うち、PC、スマートフォン、タブレット以外の端末が過半数）、**市場規模は約2,630億ドル**と予想（Gartner社）されている。

課題

- これらの拡大領域に対してどのような脅威がどの程度のリスクで存在するかについて、十分な検討がなされていない。
- 成長が見込まれるIoT産業において、国際競争力の強化とセキュリティの確保を両立させる通信技術の確立及びその活用の枠組みの検討が必要。

解決の方向性（案）

［脅威とリスクの分析・検証の実施］

○ 生じうる脅威について、IoTの特性や従来の通信機器との関係性を勘案しながら検討する。
○ 脅威に対するリスクや実現可能性はどの程度か検討するとともに、実環境を用いた検証を合わせて行う。
○ 脅威とリスクを分析した上で何を防護すべきか、対策を講じるべき対象の絞り込みを行う。

［産業競争力を確保する情報セキュリティ技術の確立］

○ 脅威・リスク分析の結果を踏まえ、対策が必要となるM2Mシステムについて、IoTの制約条件を加味した情報セキュリティ技術要件及びM2Mのライフサイクル（設計・配備・運用・廃棄）を考慮したセキュリティ運用要件を策定し、ガイドライン化する。
○ 策定したガイドラインについては、複数の民間企業の参加の元で共通的に活用する官民連携の枠組みを検討することで、M2Mにおけるセキュリティの確保を競争領域とせず、サービスへのイノベーションへの加速化を促す。

（参考）M2Mにおける情報セキュリティ技術上の課題

今後の活用が見込まれるM2Mについては、M2MのIP化、端末のスペック、利用拡大等に起因する様々な情報セキュリティ上の課題が存在している。

① M2MのIP化に起因する実装上の課題

M2Mは従来、インターネットに接続しない（非IP）環境下での活用が主であったが、昨今**インターネット（IP）への接続が増え、外部接続に伴う情報セキュリティ上の脅威**が生じている。

ビル管理

具体的脅威

カメラの映像を外でも確認できるようインターネットに接続した結果、攻撃者が外部から特定のコードを実行することで、管理権限を乗っ取り、映像の窃取・改ざんが可能に

・その他、大学の複合機に保存されたデータがインターネット上で閲覧できることが判明（平成25年11月）

課題①

M2Mのインターネット接続（IP化）に伴う設定・運用に関する基準が必要

② M2M端末のスペックに起因する課題

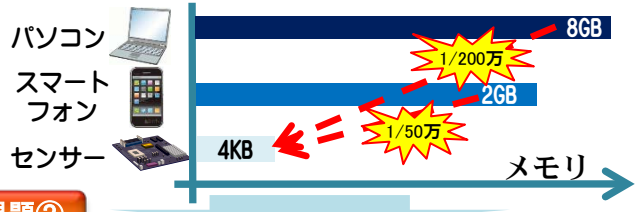
M2M端末のうち、センサーやウェアラブル端末等は小型化が重視される都合上、**機器の処理能力が極端に低く、大容量のデータの受信が困難であるため、情報セキュリティ対策が困難**である。

防災

具体的脅威

センサーには、情報を送信する権限があることを確認する認証機能がなく、攻撃者によるセンサー情報の破壊・改ざんが可能に

しかし、センサーはＰＣやスマートフォンと比較して、**数十万～数百万分の一の処理能力しかなく**、認証に必要な**大容量の暗号通信の処理が困難**



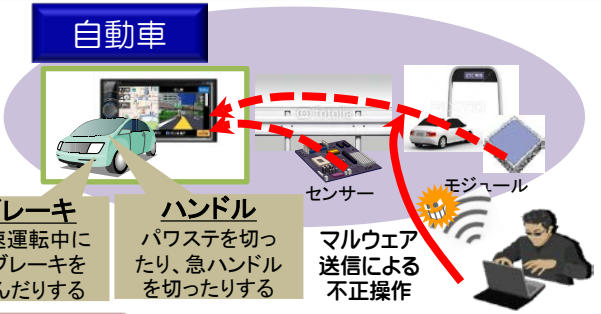
課題②

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が必要

③ M2Mの利用拡大に起因する課題

M2Mは今後自動車や家電等の高額の製品にも用いられる見込みであるが、これらの製品において**情報セキュリティ対策が十分でない場合、製品の回収・買い換え等膨大な社会経済的損失が発生**しうる。

自動車



具体的脅威

カーナビゲーションやＥＴＣ等での通信における設定の不備を悪用してマルウェアを送信することで車内システムに侵入し、外部からの自動車の操作が可能に。

脅威への対処として、ソフトウェア更新によるセキュリティ寿命の延伸が考えられるが、現状、**Ｍ２Ｍにおけるアップデートの通信プロトコルが存在しない**

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

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

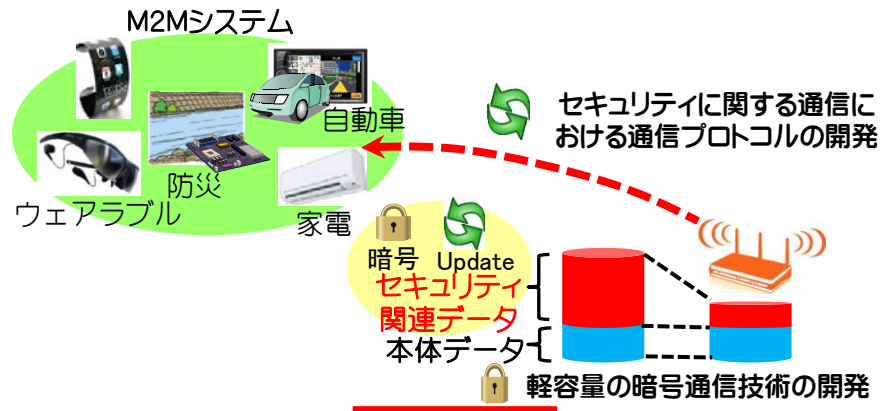
② M2Mにおける省エネ・省リソースでセキュアなデータ通信を可能とし、かつM2M端末における長期間のセキュリティ品質の確保を可能とする暗号通信技術及び通信プロトコルの開発

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

無線LAN（Wi-Fi）の安全な利用に関する周知啓発

■ 電波の有効利用の観点から、携帯電話ネットワークから無線LANへのオフロード（通信の迂回）を推進するため、Wi-Fiの安全利用に関する周知啓発を実施。

■ 具体的には、Wi-Fiの安全な利用に関する周知啓発テキストを作成し、総務省ホームページ（「国民のための情報セキュリティサイト」）にて公表するとともに、一般利用者、自治体等を対象にセミナー等を実施。

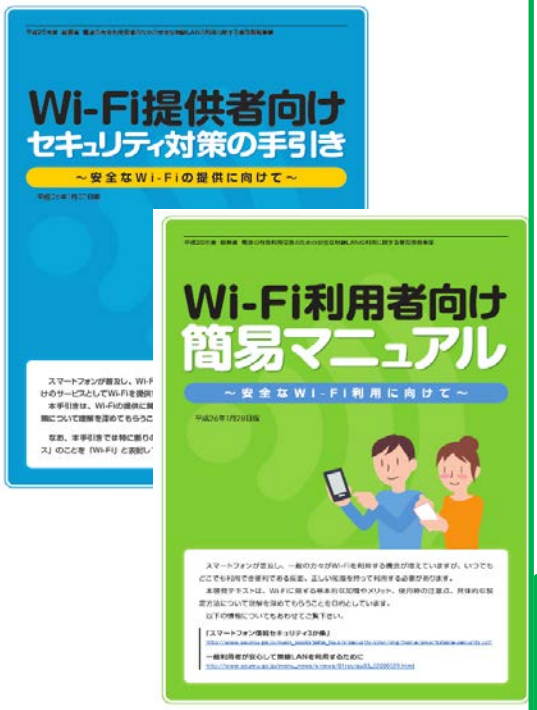

空港無線ＬＡＮ 無防備

送信メール丸見え

利便性優先 成田など暗号化せず

注意事項の浸透 不十分

Wi-Fiに関する情報セキュリティ上の懸念



Wi-Fiの安全な利用に関する
周知啓発テキスト

http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/wi-fi.html

- アクセスポイントのSSIDなどを確認することで、自分が意図したアクセスポイントに正しく接続しているか確認する。
- アクセスポイントが適切な暗号化方式に対応していることを確認する。
- ID、パスワードやクレジットカード番号等の大事な情報を入力する際はSSL（※）を利用しているサイトかを確認する。

（※）SSL（Secure Socket Layer）：
インターネット上でデータを暗号化して送受信する仕組みのひとつ。

テキストにおいて、Wi-Fi利用に伴う危険性や
取るべき情報セキュリティ対策等について解説

所要経費

平成26年度当初予算額　０．３億円
平成27年度当初予算案　０．２億円

公衆無線LAN利用に関する情報セキュリティ意識調査

項目	日本人	訪日外国人
調査背景	総務省では2020年オリンピック・パラリンピックの東京開催を見据えて、観光立国を推進する観点から、関係省庁、関係団体とも協力しつつ、公衆無線LANの整備促進に取り組んでいる。公衆無線LANは外出先等で高速な回線を利用できる点で便利である一方、盗聴、なりすましといったセキュリティ上の懸念もあり、正しい知識を持って利用する必要がある。 総務省では、日本の公衆無線LANの安心安全利用の観点から、公衆無線LANに期待される要件や現状の改善点の検討に資するため、訪日外国人及び日本人に対し、公衆無線LANの利用状況や情報セキュリティに係る意識及び対策状況について調査を実施。		
調査方法	Webアンケートによる調査		
調査期間	平成26年11月14日～21日	平成26年11月12日～25日	
調査対象	＜共通条件＞ 直近1年間に日本（東京都、神奈川県、千葉県、埼玉県の1都3県）を観光目的で訪れ、 かつ自分の端末でインターネット接続をした人（1都3県居住者を除く）		
	①「日本人観光客」200人 上記条件を満たしかつ普段スマホ・タブレット端末で、 日常的に公衆無線LANを利用している ②「自宅利用の日本人」200人 上記条件を満たしかつ普段スマホ・タブレット端末で、 自宅のみで無線LANを利用している	上記条件を満たしかつ普段スマホ・タブレット端末で、 日常的に公衆無線LANを利用している 「訪日外国人」660人 （アメリカ：214人、イギリス：217人、中国：229人）
調査事項（設問）	・公衆無線LANサービスの利用状況、満足度、利用に当たっての情報収集の有無、公衆無線LAN利用に係る脅威の理解度、情報セキュリティ対策状況、公衆無線LANサービスの改善点、今後利用したい通信手段　等		

＜調査結果の表記に係る注意事項＞

・「公衆無線LAN」は「公衆無線LANサービス」「Wi-Fi」と記載している場合があります。　・アクセスポイントは「AP」と記載しています。

・ ユーザIDは「ID」、ログインパスワードは「PW」と記載しています。

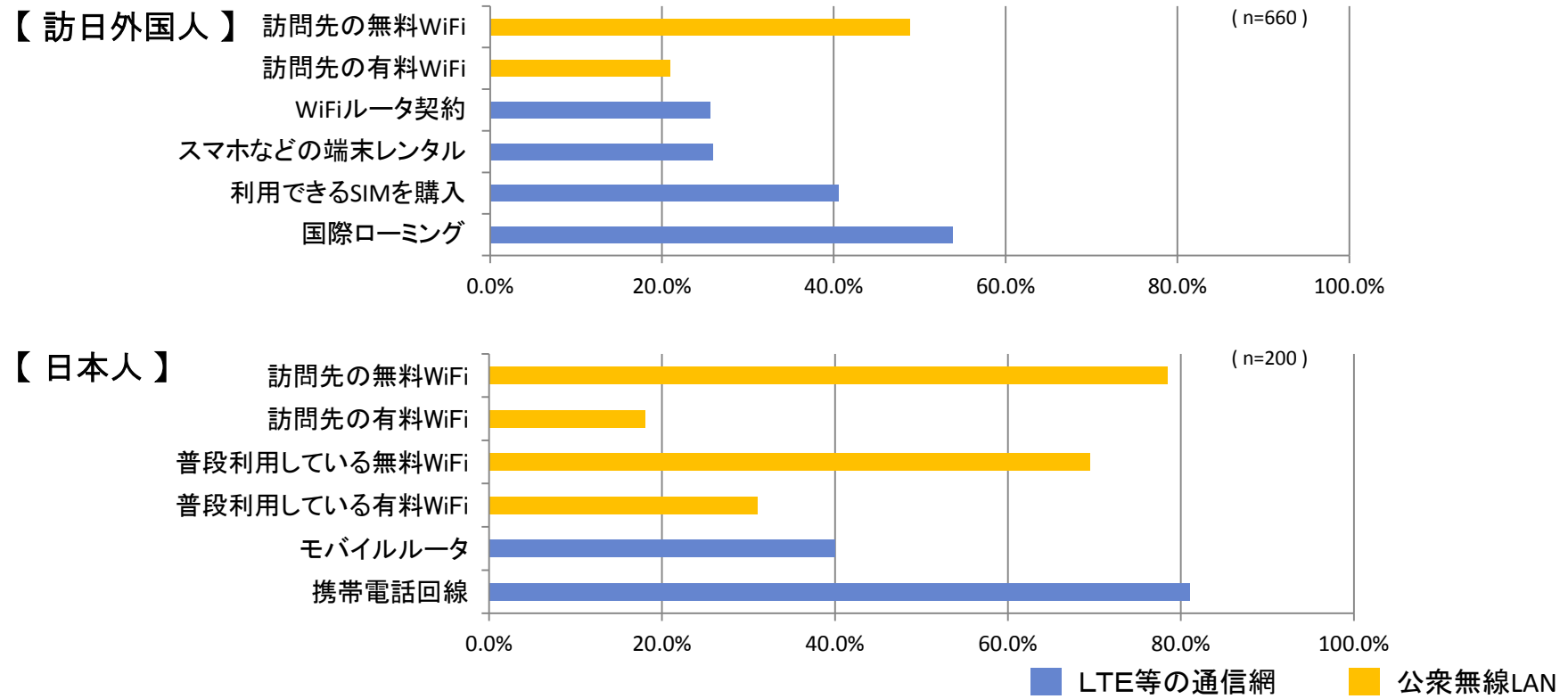
公衆無線LAN利用に関する情報セキュリティ意識調査　結果概要①

Point　1：
観光先で利用するインターネット接続手段として公衆無線LANが重要な通信手段となっている。

- 訪日外国人・日本人観光客が観光先で利用するインターネット接続手段にとして、公衆無線LANは携帯電話回線と並ぶ利用手段ととらえられており、今後も重要な通信手段と考えられる。
- 公衆無線LANでは無料の利用比率が高い。

■ 観光先で利用するインターネット接続手段について

※複数回答可



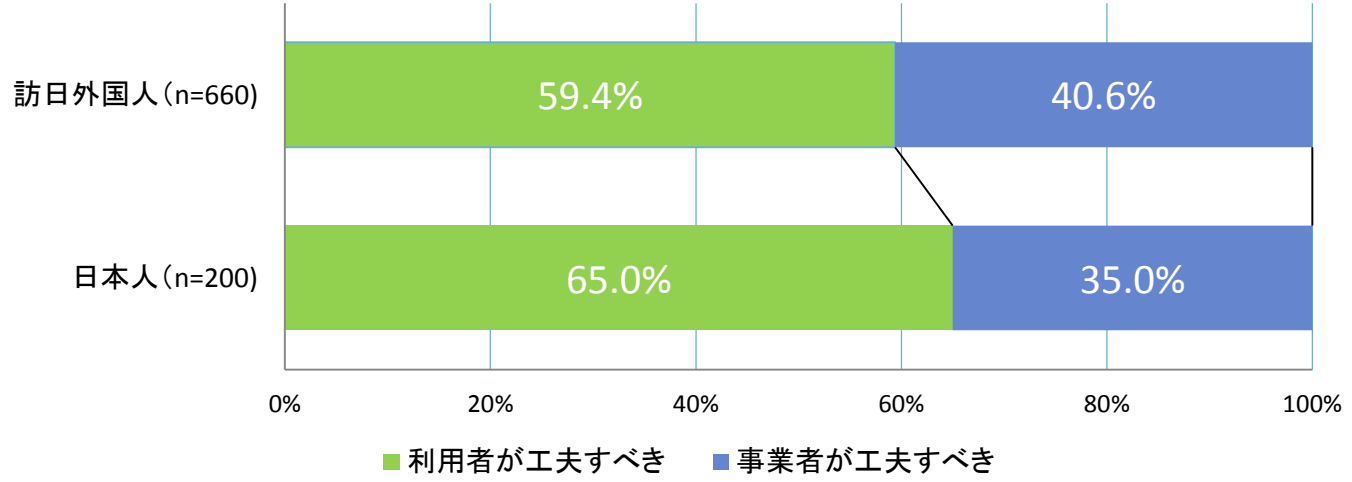
公衆無線LAN利用に関する情報セキュリティ意識調査　結果概要②

Point　2：
無料公衆無線LANの情報セキュリティ対策はユーザが行うべきと考えている人が多いが、3割以上のユーザは無料でも事業者側が対策すべきと考えている。

■ セキュリティを担保すべき当事者について

- 訪日外国人、日本人観光客を問わず、無料サービスでは利用者であるユーザが情報セキュリティ対策を行うべきという考えが半数以上を占めている。
- 一方、3割を超えるユーザが無料サービスにおいても事業者が工夫すべきと考えており、事業者に安全への取組を期待していることがわかる。

【無料Wi-Fiにおけるセキュリティ対策をすべき当事者調査】



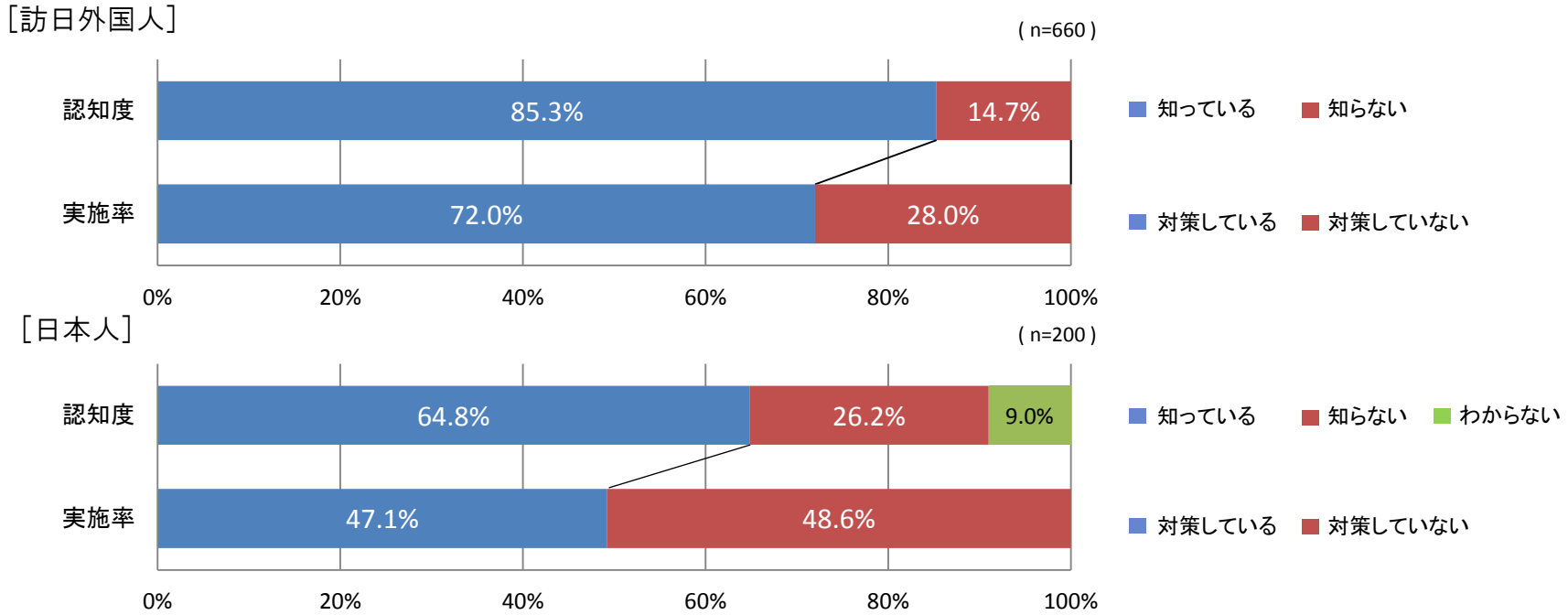
公衆無線LAN利用に関する情報セキュリティ意識調査　結果概要③

Point　3：
公衆無線LAN利用時の脅威について、一定の認知はされているものの、対策の実施については低い傾向にある。特に日本人についてその傾向が強い。

■ 公衆無線LAN利用時の脅威認知度と対策の実施率

- 公衆無線LAN利用時の脅威（盗聴/なりすまし/悪意のアクセスポイントやサイトへの接続）について、認知度と対策の実施率を調査した。訪日外国人・日本人観光者ともに認知度にくらべ実施率は大きく低下することがわかった。
- 特に日本人観光客は、認知度と実施率の乖離が大きく、対策の実施率が5割を切るなど、十分な対策がなされていない実態が明らかになった。

【公衆無線LAN利用時の脅威（盗聴／なりすまし／悪意のアクセスポイントやサイトへの接続）認知度及び実施率】



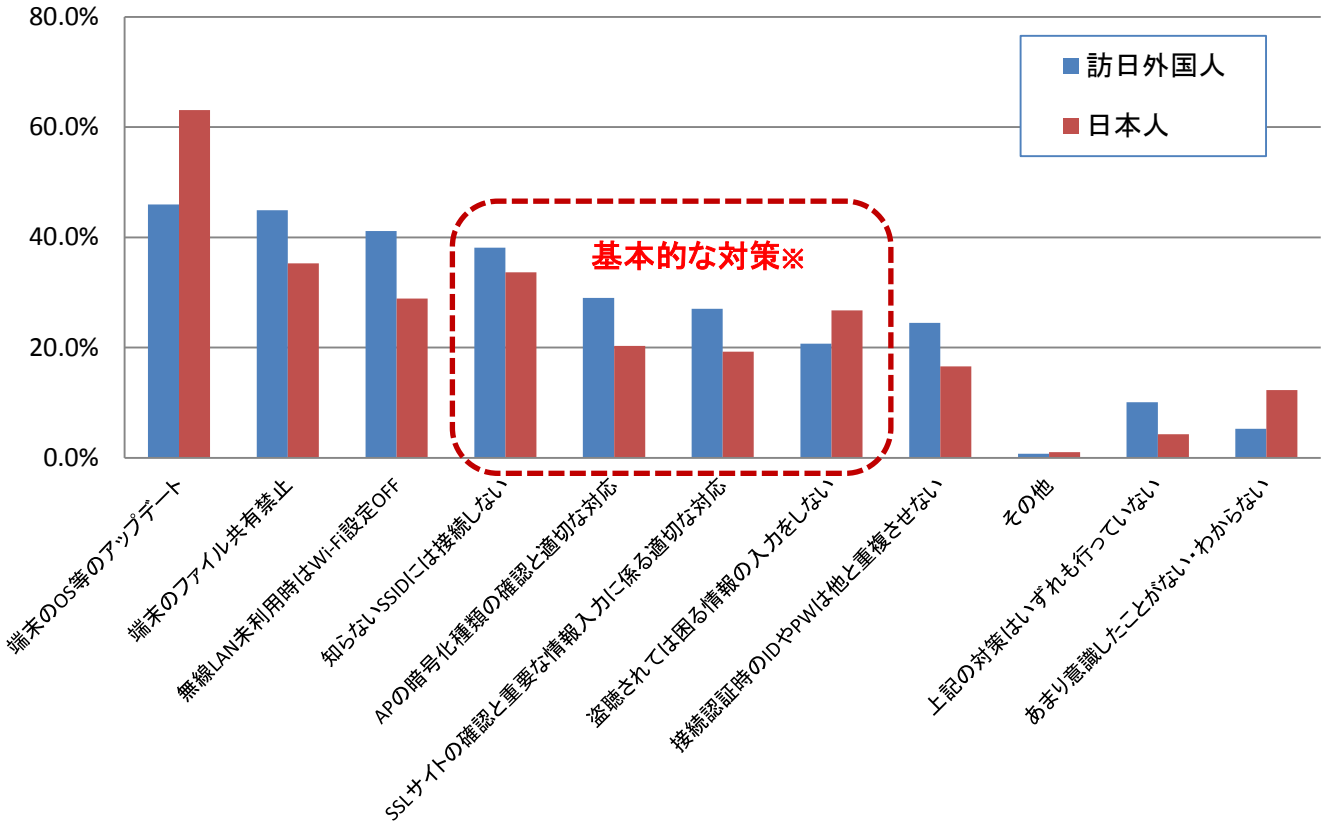
公衆無線LAN利用に関する情報セキュリティ意識調査　結果概要④

Point　4：
公衆無線LAN利用時の具体的なセキュリティ対策について、基本的な対策の実施率が2～3割と著しく低い。

■ 公衆無線LAN利用時における具体的な対策の実施率 （詳細版：3-3）

- 公衆無線LAN利用時の具体的な対策は訪日外国人・日本人とも傾向は比較的類似しているが、多くの項目で日本人の方が実施率が低い。
- 日本人において、端末のOS等のアップデートは一定程度なされているが、公衆無線LAN利用時の基本的な対策の実施率は2～3割と著しく低いことが明らかとなった。

【公衆無線LAN利用時に実施していた情報セキュリティ対策】



総務省における情報セキュリティ政策動向（制度的検討）

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」を侵害する場合とは・・・？

○ ＩＳＰが従量制の課金を行うため、利用者の通信データ量を調査する行為
○ ＩＳＰが自社の設備投資等の検討のため、自社を流れる通信量を調査・記録する行為
○ ＩＳＰがDDoS攻撃の発信元を調べる行為、また、DDoS攻撃を遮断する行為
○ ＩＳＰがマルウェアに感染者に注意喚起を行うため、ＩＰアドレスとタイムスタンプから利用者を特定する行為

⇒ 全て「通信の秘密」を侵害する行為！

＜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。

ただし、違法性阻却事由がある！

通信の秘密が侵害されない又は侵害が許容される（違法性が阻却される）場合とは・・・

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。また、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。

※「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。
「正当業務行為」として違法性が阻却されるためには、①目的の正当性、②行為の必要性、③手段の相当性の全ての要件を満たすことが必要。

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

概要

- DDoS攻撃やマルウェア感染活動等サイバー攻撃が巧妙化・複雑化する中で、電気通信事業者が通信の秘密等に配慮しつつ、新たな対策や取組を講じていくことが可能となるよう、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ついて検討を行うことを目的として開催。（消費者行政課及び情報セキュリティ対策室の共同事務局。）
- 平成25年11月より検討を開始し、**平成26年4月4日にはこれまでの議論を取りまとめた「第一次とりまとめ」を公表**。「第一次取りまとめ」の内容を踏まえ、平成26年7月22日に事業者団体「インターネットの安定的運用に関する協議会」において「電気通信事業者における大量通信等への対処と通信の秘密に関する ガイドライン」を改定。

構成員

＜親会＞

（座長）	佐伯　仁志	東京大学大学院法学政治学研究科教授
（座長代理）	宍戸　常寿	東京大学大学院法学政治学研究科教授
	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
	木村　たま代	主婦連合会
	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
	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　主管研究員
	藤本　正代	富士ゼロックス（株）パートナー／情報セキュリティ大学院大学客員教授
	森　亮二	英知法律事務所　弁護士

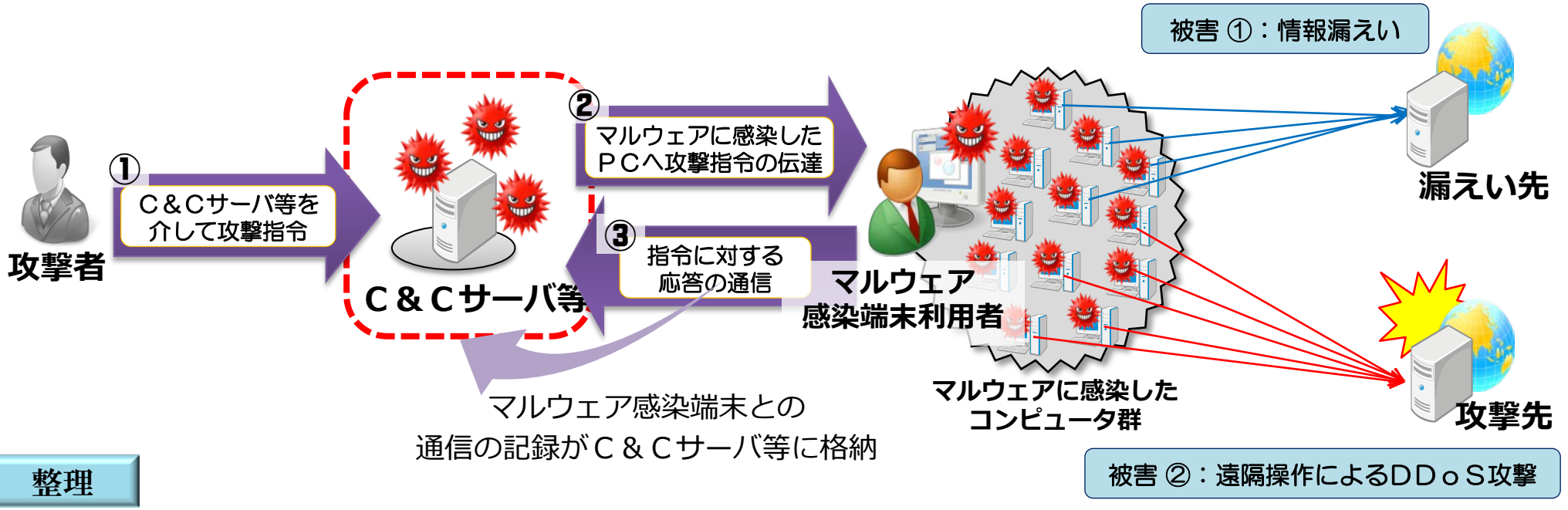
＜WG＞　WGにおいて、専門的な観点から詳細な検討を実施。

（主査）	宍戸　常寿	東京大学大学院法学政治学研究科教授
（主査代理）	森　亮二	英知法律事務所　弁護士
	衛藤　将史	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任研究員
	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
	齋藤　衛	株式会社インターネットイニシアティブ　サービスオペレーション本部　セキュリティ情報統括室長
	丸橋　透	ニフティ株式会社　法務部長
	村主　亘	ソフトバンクテレコム株式会社　お客様相談室

マルウェア感染者の特定・注意喚起に対する研究会における論点及び整理

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。

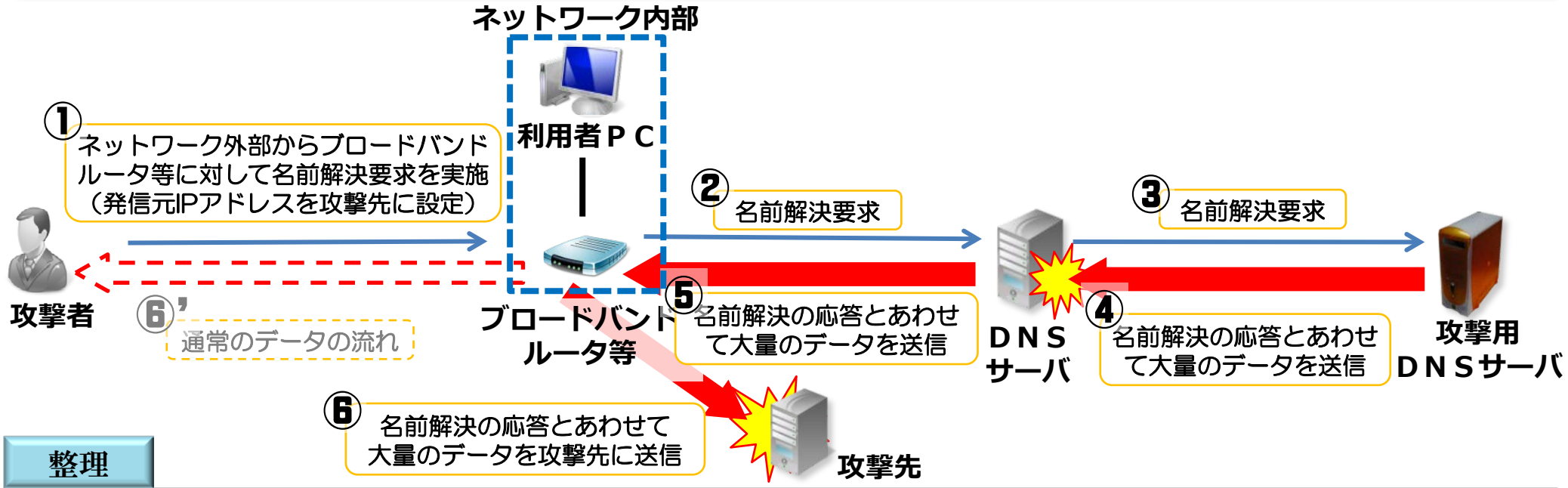
「**法益の権衡**」：本件対策により避けようとする害（マルウェアに感染している状態）に対して、侵害される通信の秘密は、IPアドレスとタイムスタンプを該当利用者を割り出す限度で利用するのみである。

「**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。

DNSAmp攻撃の防止に対する研究会における論点及び整理

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。

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。

「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」 http://www.soumu.go.jp/main_content/000283608.pdf
「電気通信事業者における大量通信等への対処と通信の秘密に関するガイドライン」（大量通信ガイドライン） http://www.jaipa.or.jp/other/mtcs/guideline_v3.pdf

安全・安心な情報通信ネットワークの確保に向けて今後検討すべき制度的課題

今後の安全・安心な情報通信ネットワークの確保に向けては、主に次の取組について検討が必要ではないか。

主な検討事項（案）

○ **C&Cサーバとの通信に対する対策の検討**

- 第1次取りまとめにおいて、テイクダウンしたC&Cサーバに蓄積された通信履歴等に基づくマルウェア感染者の特定及び注意喚起の実施について整理したところであるが、C&Cサーバとの通信のような、利用者がその内容について了知し得ないまま、重大な損害を被るおそれがある通信に対して、ISPにおいてより前段階での対策が取れないか。

○ **リフレクション攻撃の踏み台等の脆弱性を有したブロードバンドルータに対する対策の検討**

- 第1次とりまとめにおいて、DNSAmp攻撃を防止するための特定の通信の遮断について整理したところであるが、これらのリフレクション攻撃の踏み台となるブロードバンドルータは存置されたままであることから、攻撃のリスクを低減させる観点から、これらの脆弱性を有するブロードバンドルータに関して、ISPにおいて利用者の特定及び注意喚起が出来ないか。

○ **PPPoE認証の不正利用に対する対策の検討**

- 昨今、不正に窃取されたPPPoE認証を用いて、インターネットバンキングによる不正送金や迷惑メールの送付、SNSでのなりすまし等が行われていることから、ISPにおいてPPPoE認証の不正利用を防ぐための対策が取れないか。

情報セキュリティ アドバイザリーボードにおける検討

2014年11月に成立したサイバーセキュリティ基本法を踏まえ、次期サイバーセキュリティ戦略の策定等も見据え、今後取り組むべき課題について、情報セキュリティ アドバイザリーボードにおいて検討を実施。

情報セキュリティ アドバイザリーボード（親会）

【目的】

情報セキュリティの推進に当たり、短期的及び中長期的に講ずべき対策や既存の取組の改善などの方向性について幅広い観点から助言を行うとともに、情報セキュリティに係る諸問題への対応について、必要に応じて提言をとりまとめるために開催。

【構成員】（敬称略）

（座　　長）	徳田　英幸	慶應義塾大学 環境情報学部 教授
（座長代理）	林　紘一郎	情報セキュリティ大学院大学 前学長・教授
	飯塚　久夫	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 会長
	岡村　久道	国立情報学研究所 客員教授・弁護士
	宮地　充子	北陸先端科学技術大学院大学 情報科学研究科 教授
（顧　　問）	小野寺　正	KDDI株式会社 代表取締役会長

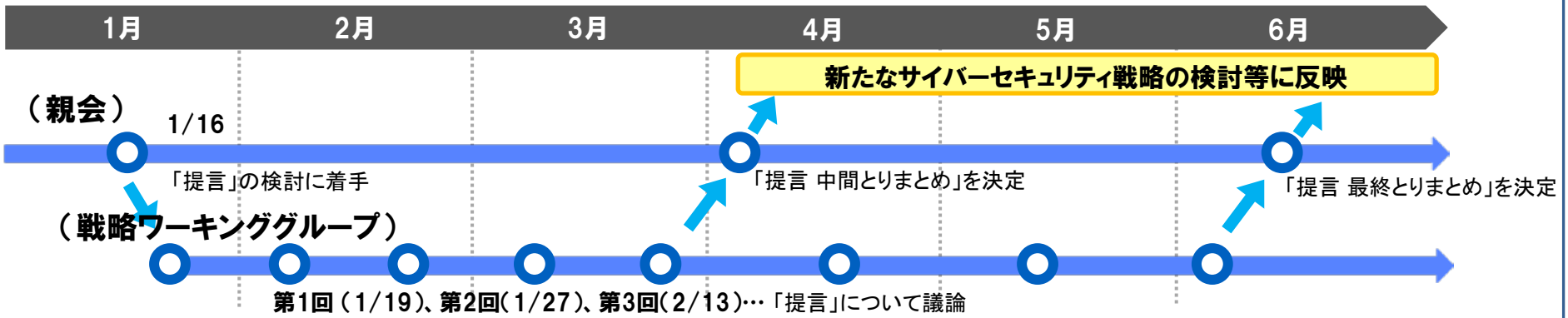
戦略ワーキンググループ

（主査）　中尾　康二
KDDI情報セキュリティフェロー／
NICT ネットワークセキュリティ研究所
主管研究員

通信事業者、放送事業者、ベンダー、学識経験者等から構成

2015年1月、情報セキュリティ アドバイザリーボードの下に新たに戦略ワーキンググループを設置し、今後取り組むべき課題についての「提言」とりまとめに向けて集中的に議論。

スケジュール



戦略ワーキンググループにおける検討の論点（概要案）

背景

○ 2014年、我が国全体のサイバーセキュリティ推進体制の機能強化等に向けたサイバーセキュリティ基本法が成立。

○ 今後、IoT環境の本格的到来等、ICT環境の大きな変化が想定。

○ 2012年ロンドン五輪では多数のサイバー攻撃が発生。2020年東京五輪に備えたサイバーセキュリティ対策が必須。

○ サイバーセキュリティ対策の実施に当たっては、経済発展への貢献も念頭に置くことが必要。

論点（案）

上記の背景を踏まえ、戦略ワーキンググループにおいては、以下の１～５の各項目について検討を実施することが考えられるのではないか。

１．通信ネットワークの防護

昨今、脆弱性のあるルータ・サーバ等を悪用したリフレクション型のDDoS攻撃の急増を始めとして、通信ネットワークの安定運用を脅かす情報セキュリティ上の脅威が深刻化している。制度と実際の対策の両面から、こうした情報セキュリティ上の脅威への対策を検討する。

２．新たな情報セキュリティ上の脅威への対応

IoT環境の本格的な到来により今後M2Mの急速な普及が見込まれているが、M2Mにおける情報セキュリティ上の脅威の全体像は十分に把握されていない。M2M等における情報セキュリティ上の脅威の動向を把握するとともに、機器メーカ等との連携を含め、その対策を検討する。

３．事業者間連携の強化

情報セキュリティ上の脅威への対応のため、情報共有の推進等、事業者間における連携強化策を検討する。特に、通信事業者内のみではなく、通信事業者と情報セキュリティベンダや放送分野をはじめとした重要インフラ事業者等の関連組織との連携の在り方について、試行的な取組の実施も含めて検討する。

４．東京大会の開催に際しての対応

2020年オリンピック・パラリンピック東京大会の開催に直接影響を与えうる情報セキュリティ上の脅威について、脅威分析・リスク分析等を実施するとともに、東京大会に向けて立ち上げが想定されるCERTとの連携を含め、その対策を検討する。

５．その他

上記以外の取組等についても検討する。

（例）国際連携の展開、人材育成、研究開発の推進、
地方創生に資する情報セキュリティ対策、
サプライチェーンリスクへの対応

ご清聴ありがとうございました