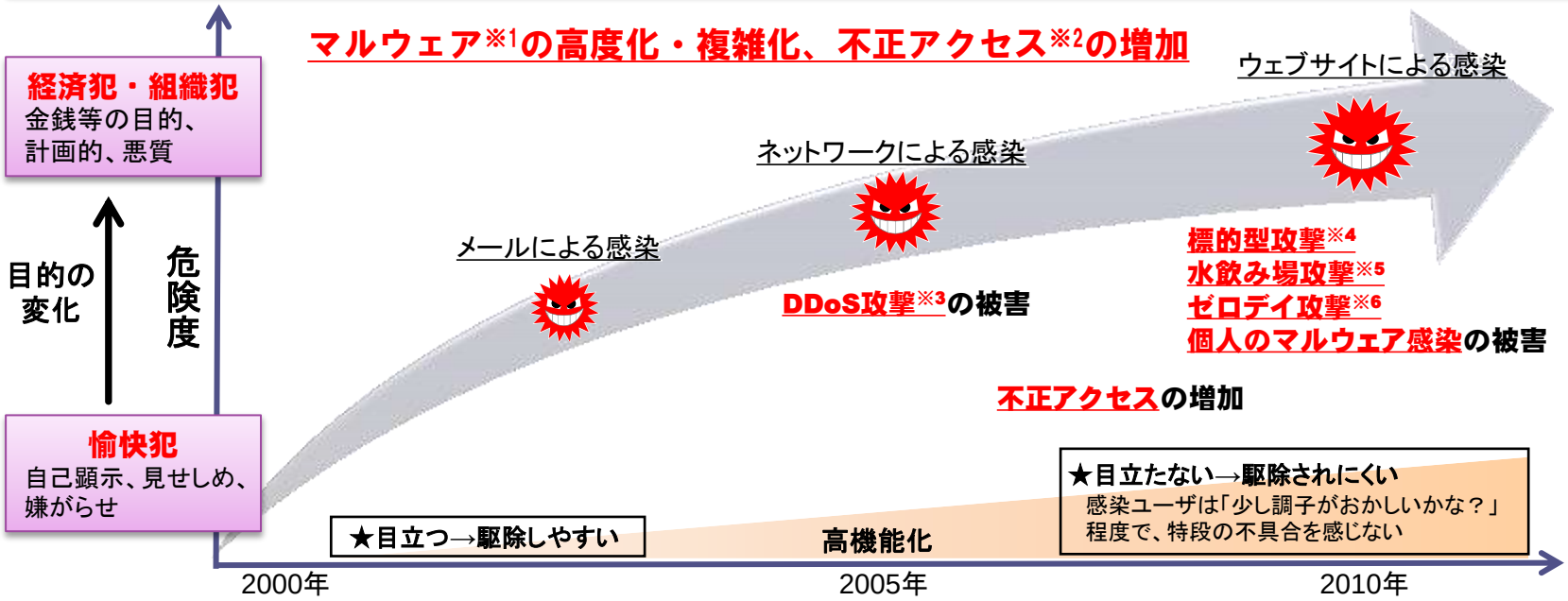
情報セキュリティ対策における「通信の秘密」について

平成26年7月

総務省　情報流行政局
情報セキュリティ対策室
課長補佐　平松　寛代

情報セキュリティ上の脅威の増大

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の多様化・悪質化により、その被害が深刻化。



※1 マルウェア（Malware）：
Malicious software の短縮された語。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 不正アクセス：
ID・パスワード等の識別符号により利用が制限・管理されている特定電子計算機に対し、ネットワークを経由して他人の識別符号を入力すること等により、本来は制限されている利用を可能にする行為。

※3 DDoS攻撃：
分散型サービス妨害攻撃（Distributed Denial of Service）のこと。多数のコンピュータ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。

※4 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、執拗かつ継続的に行われる攻撃。

※5 水飲み場攻撃：
攻撃対象組織が頻繁に閲覧するウェブサイト（水飲み場）で待ち受け、攻撃対象組織を狙ってマルウェア感染などをさせる攻撃。

※6 ゼロデイ攻撃：
脆弱性情報が判明してから修正プログラムが提供される前に行われる攻撃。

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パソコンが情報収集型のウイルス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）

2012年9月・・・ウイルスに感染したPCが第三者により遠隔操作され、掲示板に違法な書込みが行われたことでPCの所有者が誤認逮捕。（個人のマルウェア感染）

2012年10月・・・ウイルス感染により、ネットバンキングにログインした利用者のPCの画面に偽画面が表示され、ID・パスワードが窃取。これにより、数百万円の不正送金が発生。（個人のマルウェア感染、不正アクセス）

2013年1月・・・農林水産省のPCが遠隔操作型のウイルスに感染し、TPPに関する機密文書が窃取されたおそれがあることが報道。（標的型攻撃）

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

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。（ゼロデイ攻撃、水飲み場攻撃）

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」とは？

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。

「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。

※　「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。

「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。

○　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）

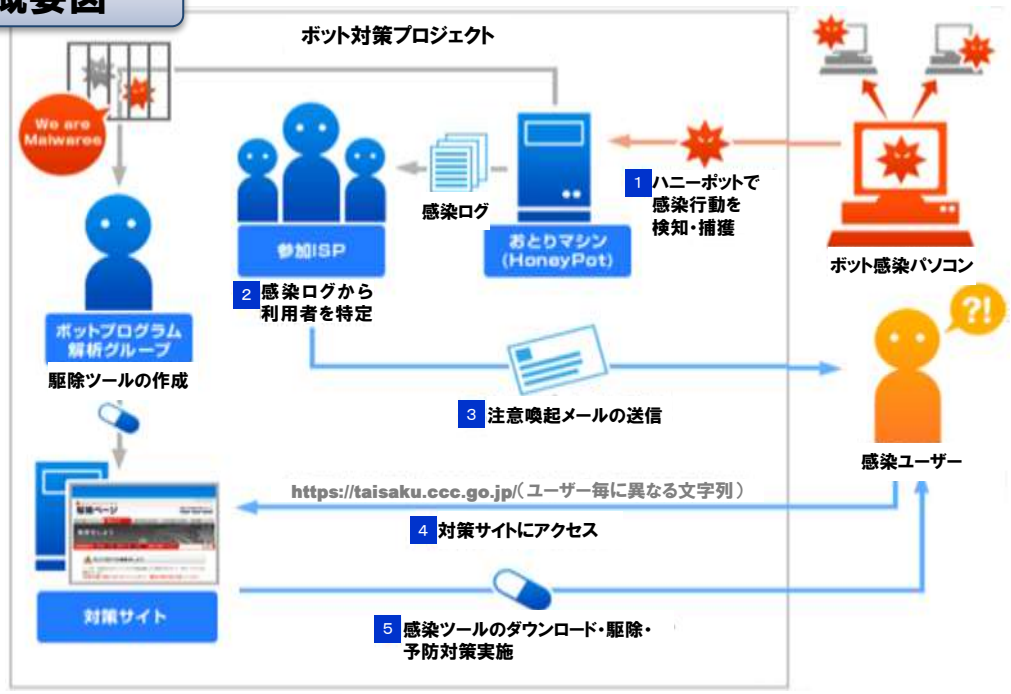
サイバークリーンセンター（CCC）について　－ボットウイルス対策プロジェクト－

○　平成18年12月より経産省との連携の下、情報セキュリティ関係機関のオールジャパン体制として「**サイバークリーンセンター（CCC）**」を組織し、サイバー攻撃の踏み台等となるボットウイルス撲滅に向けた取組を実施。

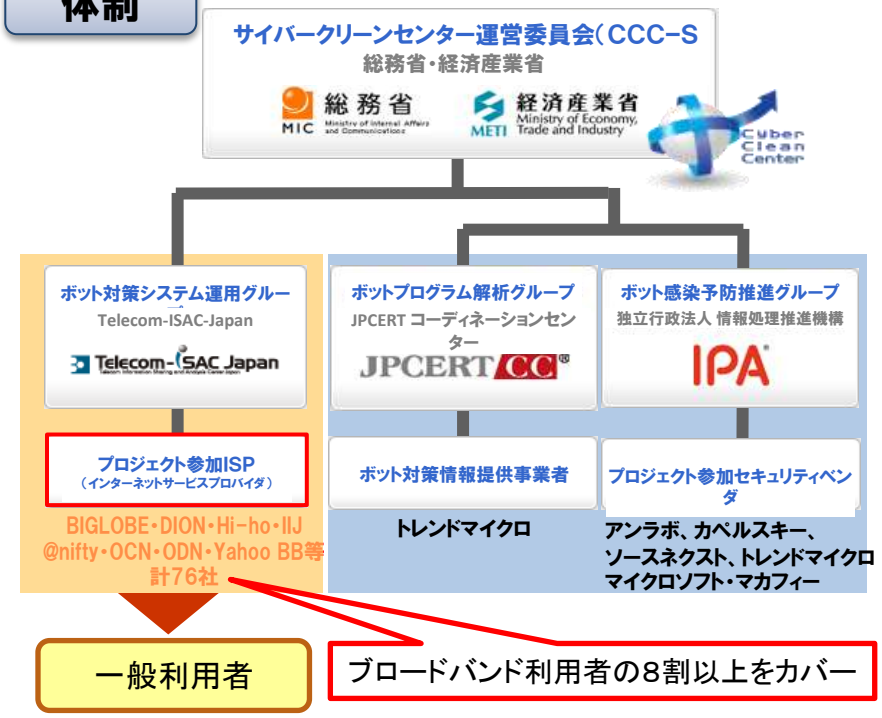
○　ボットウイルス感染者に対して参加ISP（76社）が注意喚起を実施し、ウイルス駆除、Windows Update等の対策実施を勧奨。

○　ウイルス駆除ツールをウェブサイトで提供し、インターネット利用者の自発的なウイルス駆除等の実施をサポート。

概要図



体制



通信の秘密との関係

①　CCCの事務局が、ボットウイルス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（ダイナミックIPアドレス）を参加ISP（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

⇒CCCの事務局はボットウイルス感染パソコンからの**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　参加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こと

⇒**ボットウイルス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。

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。

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。

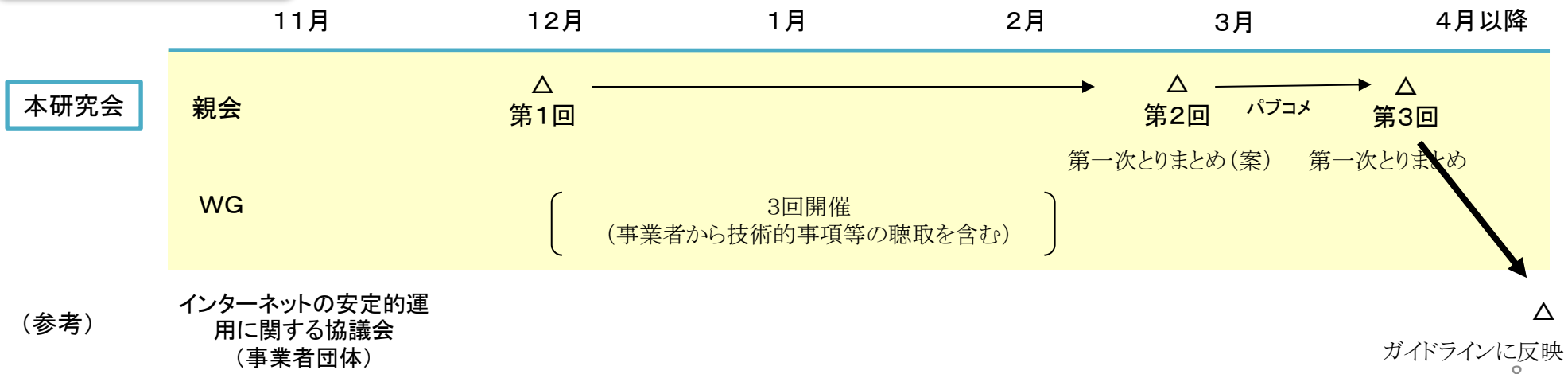
電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会

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

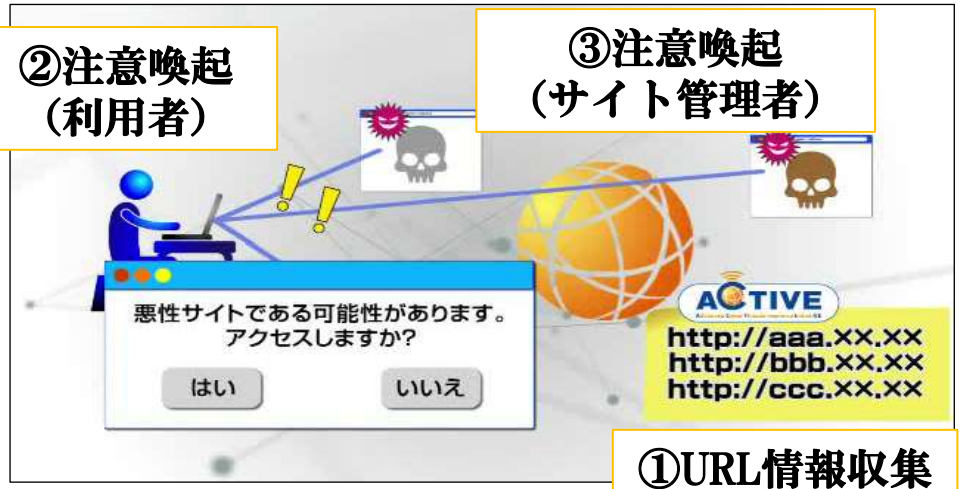
スケジュール



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

■　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

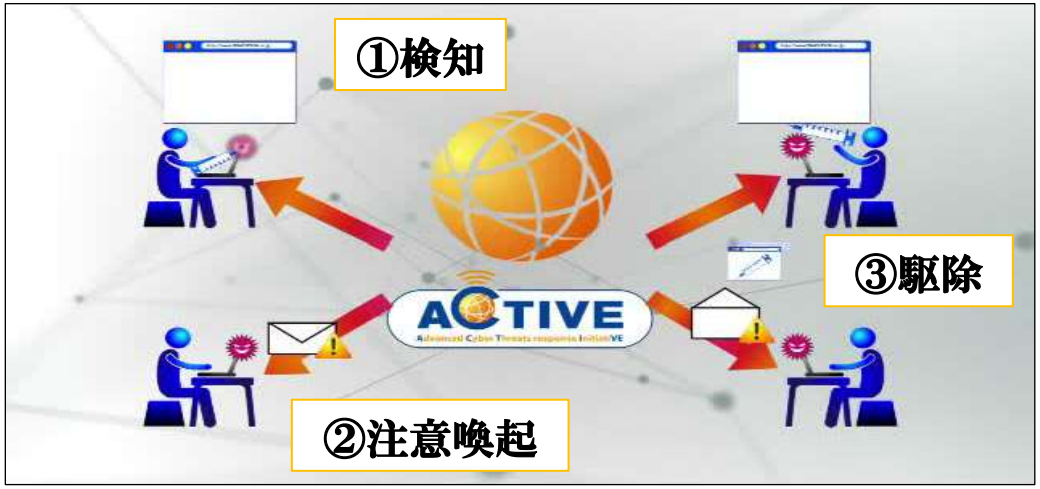


① マルウェア配布サイトのURL情報をリスト化。

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



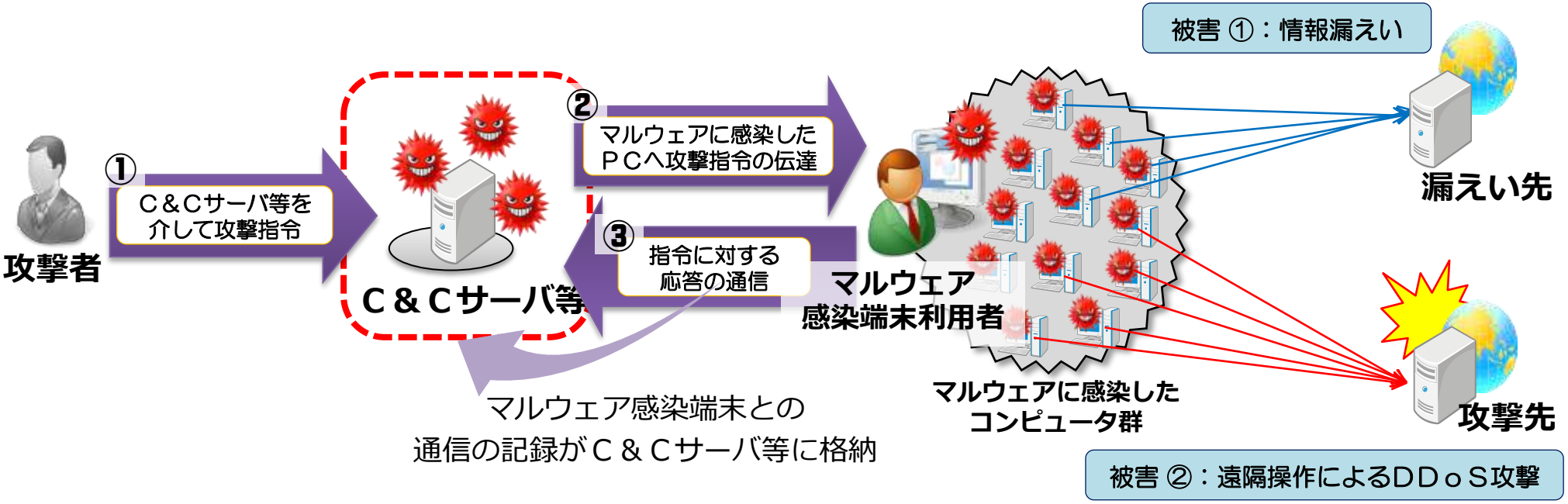
① マルウェアに感染した利用者のPCを特定。

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。

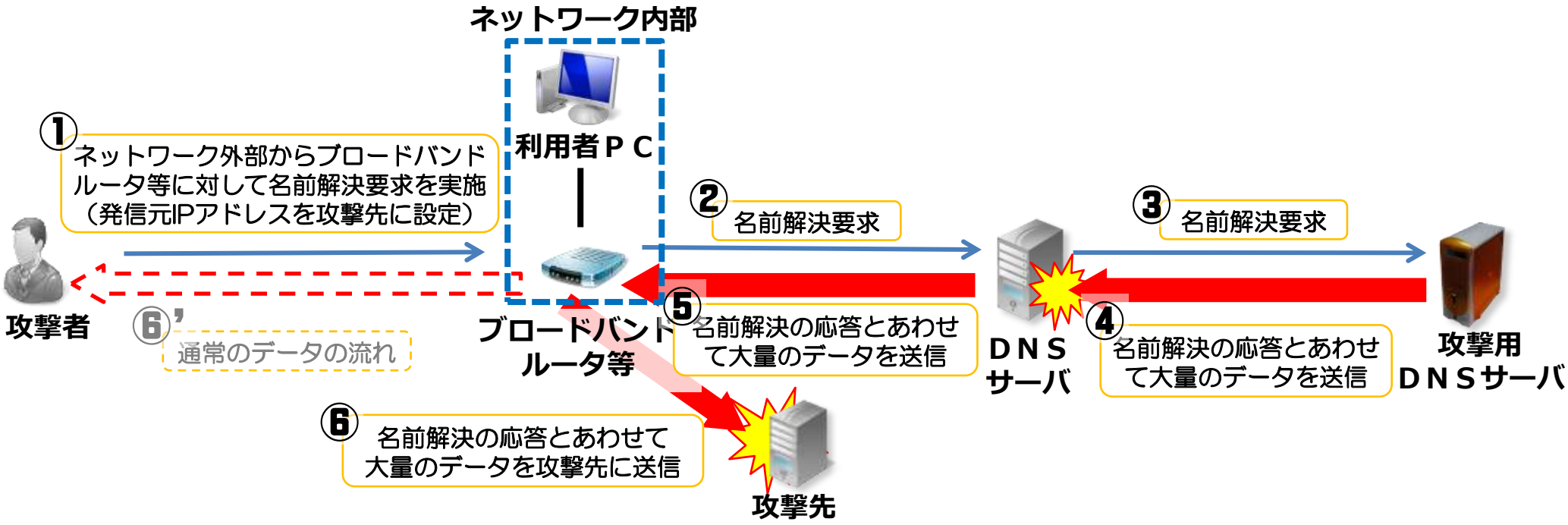
課題②　マルウェア感染駆除の拡大について

■　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。



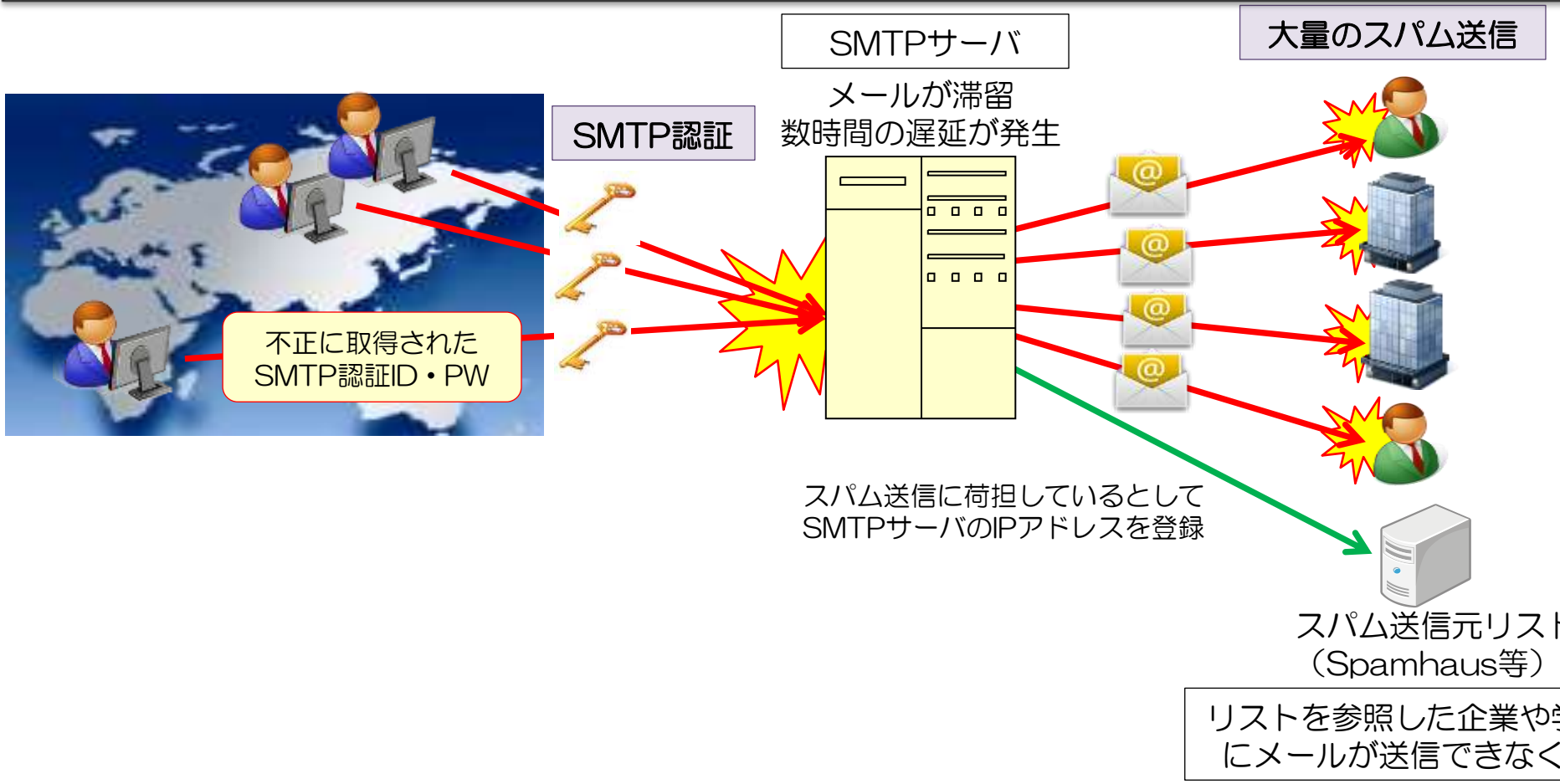
課題③　新たなDDoS攻撃であるDNSAmp攻撃の防止

■　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。



課題④　SMTP認証の情報を悪用したスパムメールへの対処

■　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、SMTPサーバの不可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、一時認証停止や利用者への注意喚起を行うことは、通信の秘密との関係上どのように整理が可能か。



「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。

「第一次とりまとめ」 具体的事例 ①
マルウェア配布サイトへのアクセスに対する注意喚起

論点と整理

（論点）

○ 通信の秘密に関する同意は、契約約款等に基づく事前の包括同意のみでは、一般的には有効な同意と解されていない

○ しかしながら、ACTIVEプロジェクトに参加する利用者が拡大し、マルウェア感染の防止を進めるために、契約約款に基づく事前の包括同意であっても、一定の条件の下においては、有効な同意ということはできないか

（検討・整理）

○ 契約約款等に基づく事前の包括同意のみでは、一般的には有効な同意と解されていない理由

① 契約約款は当事者の同意が推定可能な事項を定める性質のものであり、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（利用者に不測の不利益が生じることが問題）

○ 「マルウェア配布サイトへのアクセスに対する注意喚起」について、上記①、②に関し次のとおり整理

① 通信の秘密に当たる情報のうち必要最小限度の事項（アクセス先IPアドレス又はURL）のみを機械的・自動的に検知した上で、該当するアクセスに対して注意喚起画面等を表示させるのは、安全なインターネットアクセスを確保するためのものであり、インターネットアクセスサービスの通常の利用者であれば、その限りにおいてこれらの事項が利用されることについて許諾することが想定しうるため、契約約款の性質になじまないとまでは言えない

② **契約約款による包括同意であっても、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（設定変更できる）契約内容であって、そのことについて利用者に相応の周知が図られており、注意喚起画面等においても説明されている場合には、随時、利用者が同意内容を変更することができることから、将来、利用者が不測の不利益を被る危険を回避できる。**

以上から、上記の方法により注意喚起画面等を表示させる場合、**以下の条件の下で有効な同意があると理解される**

ア 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契約内容であって、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同意内容の変更の有無にかかわらず、その他の提供条件が同一であること

イ 当該契約約款の内容及び事後的に同意内容を変更できることについて、利用者に相応の周知が図られている

ウ 注意喚起画面等においても、本件注意喚起対策の説明に加え、本件対策を望まない利用者は、随時、同意内容を変更できること及びその方法が説明されている

「第一次とりまとめ」 具体的事例 ②
マルウェア感染駆除の拡大

論点と整理

（論点）

○ C&Cサーバがテイクダウンされた場合、当該サーバとマルウェア感染端末との通信の記録のうち、端末のIPアドレス・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確認し、個別に注意喚起することは、緊急避難の要件を満たすと考えられるか

（検討・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と考えられる

- C&Cサーバと端末が通信している記録がある場合、端末が正常かつ安全に機能することについて「現在の危難が存在」していること、
- 本件対策により避けようとする害と侵害される通信の秘密の間に「法益の権衡」が認められること、
- 他の方法では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という「補充性」が認められること

「第一次とりまとめ」 具体的事例 ③
新たなDDoS攻撃であるDNSAmp攻撃の防止

論点と整理

（論点）

○ ISP網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アドレス及びポート番号を常時確認して、動的IPアドレス宛てであってUDP53番ポートに対する通信を検知しブロックすることは、正当業務行為に該当すると考えられるか

（検討・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と考えられる

- 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との「目的の正当性」が認められること
- DNSAmp攻撃に係る通信のうち、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り、「行為の必要性」が認められること
- 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ことから、「手段の相当性」も認められること

「第一次とりまとめ」 具体的事例 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

論点と整理

○ 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には、SMTP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認証のIDを分析することによる対策が必要と考えられる。

さらに、SMTP認証の高いID・パスワードの不正取得それ自体を防止するには、大量のSMTP認証の失敗が発生し警告が出た場合、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)を分析することによる対策が必要と考えられる。

○ このような対策については、

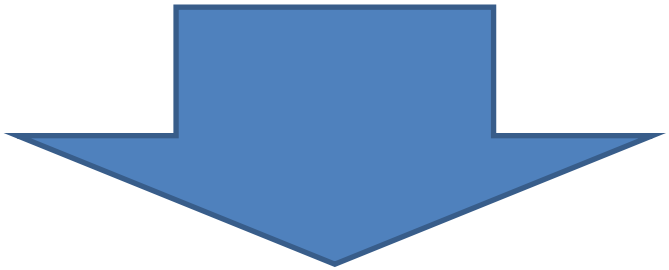
・ 不正利用の蓋然性の高いID・パスワードからのSMTP認証を一時停止するとともに、当該ID・パスワードの利用者に個別に連絡をとりパスワードの変更等を依頼すること[対策1]

・ 特定のIPアドレスからSMTP認証の失敗が短期間に大量に発生している等アカウントハッキング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認証をとめること[対策2]

のいずれも、**それぞれ「目的の正当性」「行為の必要性」「手段の相当性」の観点から考慮して、正当業務行為として違法性顔阻却される**と考えられる。

今後・・・

- ✓ 情報セキュリティの世界はいたちごっこ、ますます技術的に高度化
- ✓ 法律の運用者にとってみれば、ますます分からない世界
- ✓ でも、社会的に重要な問題を解決していきたいという気持ちは同じ



お願い

- **何かあれば、まずは個別にご相談ください。**
- **起きている現象について、なるべく分かりやすく教えてください。**
- **最初から諦めないでください。**