資料1

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資料

当研究会第一次取りまとめを受けた「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」の修正の概要

2015年6月1日

一般社団法人日本インターネットプロバイダー協会
（JAIPA）
行政法律部会　部会長 木村　孝

ガイドラインの改定

- ２０１４年４月３日に公表された第一次取りまとめを受け、「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」（以下ガイドライン）の改定を行うべく、インターネットの安定的な運用に関する協議会*が開催された。
- ５回の検討を行い、７月１７日ガイドラインの第３版を決定し、７月２２日に報道発表を行った。

*構成員は以下のとおり
一般社団法人日本インターネットプロバイダー協会
一般社団法人電気通信事業者協会
一般社団法人テレコムサービス協会
一般社団法人日本ケーブルテレビ連盟
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
オブザーバー：総務省消費者行政課、情報セキュリティ対策室

主な変更点

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における有効な同意（ACTIVEでの活動）

- マルウェア配布サイトへのアクセスに対する注意喚起を行うに当たって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ことについては、一定の条件*を満たす場合には、契約約款に基づく事前の包括同意であっても、当該注意喚起を行うための通信の秘密に属する事項の利用についての有効な同意ということができる。（第一次取りまとめ　P20)

*　1.契約約款に同意した後も、随時同意内容を変更できること。同意内容に関わらずその他の提供条件が同一であること。2.契約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なされていること。3.注意喚起画面に同意内容を変更できること等の説明がされていること。

ガイドラインにおいて第2章　各論　第5条　３　その他の情報共有・情報把握について(2) レピュテーションDBの活用において、以下のように整理された。（P24）

個別の同意を取得していなくても、レピュテーションDBに基づい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を行う場合であって、その際、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、当該データベースが一定の正当性（目的の正当性、正確性、客観性　等）を有するものである場合には、契約約款に基づく事前の包括同意でも、次の条件（上述*）の下においては、当該注意喚起を行うための通信の秘密に属する事項の利用についての有効な同意ということができ、通信の秘密の侵害とならないと解される。

※　有効な同意の前提として、注意喚起を行う際のリストについて、「当該データベースが一定の正当性（目的の正当性、正確性、客観性　等）を有するものである場合」という条件を追記

２．新たなDDoS攻撃であるDNSAmp攻撃の防止（UDP５３番ポートブロック）

- 宛先の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には、正当業務行為として違法性が阻却されると考えられる。（第一次取りまとめ　P27）

ガイドラインにおいて　第2章　各論　第5条　大量通信等について1　攻撃通信への対応　(1) 大量通信等に係る通信の遮断　イ　事業者設備に支障が生じる場合　(カ)　として以下のように整理された。（P13）

通常想定されていないネットワーク外部からの問い合わせを受ける設定となっているブロードバンドルータ等を利用して、DNS等の通常のインターネットの機能を悪用し、大量通信等を発生させる攻撃（DNSAmp攻撃等。以下、「Amp攻撃等」と呼ぶ。）に対して、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、動的IPアドレス宛てであって、特定のポート番号に対して送信された通信のみを機械的に遮断することは通信の秘密の窃用等に当たりうる。

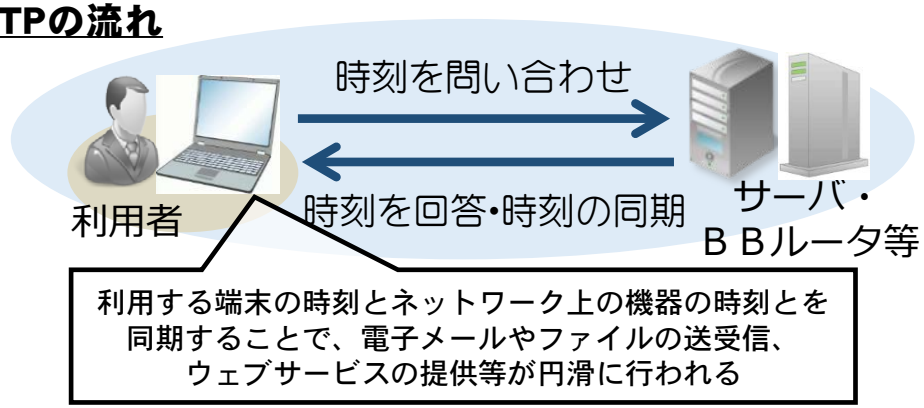
しかしながら、当該行為は、Amp攻撃等によりISPの通信設備が過負荷状態になることによるインターネットアクセスやメールの遅延等の発生を防止し、もって、インターネット接続役務等の電気通信役務の安定的提供を図るためのものであり、通常の通信環境下において、ブロックの対象となる、動的IPアドレス宛てであって、特定のポート番号に対して送信されるネットワーク外部からの通信は想定されず、侵害される通信の秘密も宛先IPアドレス及びポート番号のみと相当な限度で行われることから、正当業務行為として違法性が阻却されると考えられる

※　NTPAmp攻撃（ネットワーク上の機器の時刻を同期させるためのプロトコルであるNTPの仕組みを悪用して、問い合わせに対して何十、何百にも増幅した通信を発生させ、ネットワークを輻輳させる攻撃。次ページ参照）等についても、同様の対処が必要であることから、DNSAmp攻撃以外についても、同様の整理が成り立つものについて、適用できるような記載を追加

NTPAmp攻撃について

・・・ネットワーク上の機器の時刻を同期するための仕組み（NTP）を悪用したリフレクション攻撃

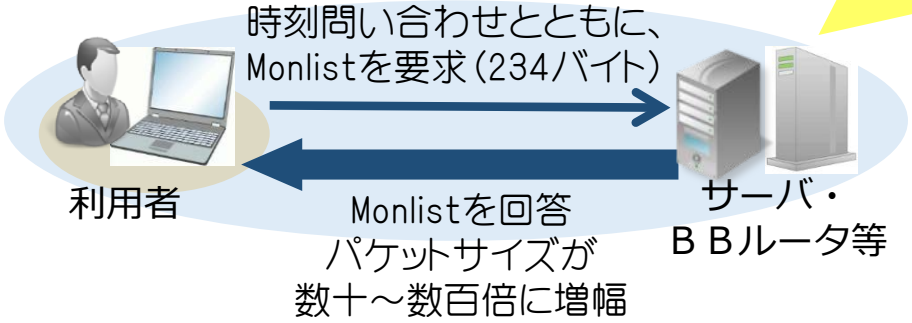
通常のNTPの流れ



※ NTP（Network Time Protocol）：ネットワーク上にある機器において、各機器が持つ時計の時刻を同期させる仕組み

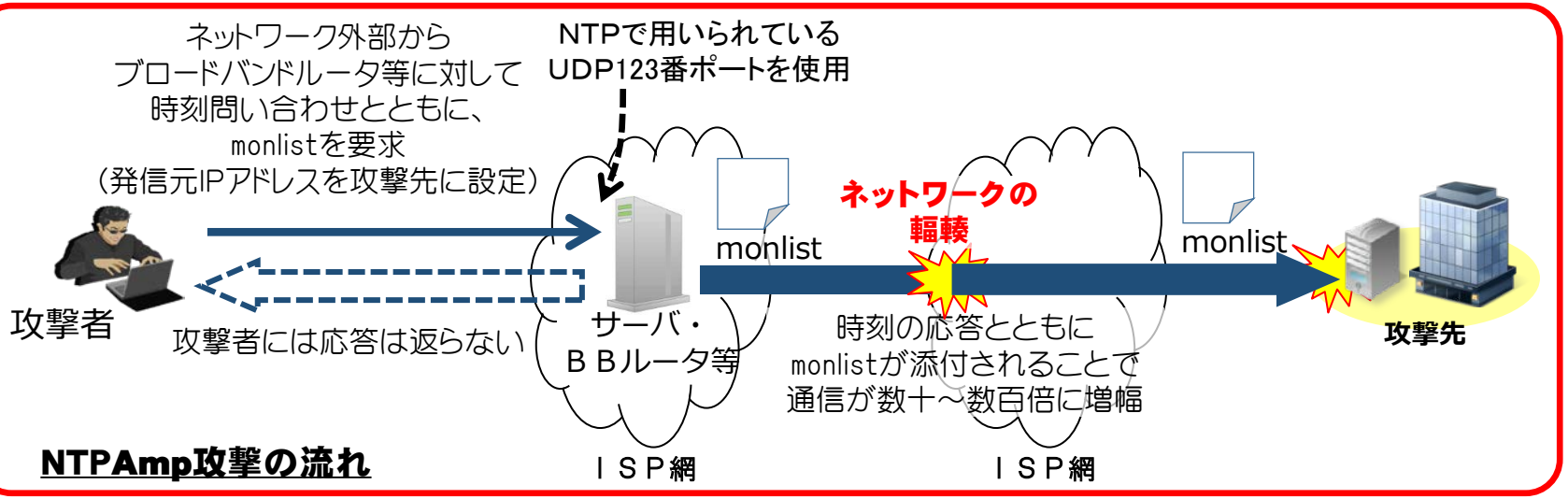
NTPの Monitoring機能

ネットワーク機器においては“monlist”（過去にNTPの通信を行った端末のIPアドレスのリスト（最大600台分））を有している



※　通常は通信機器のNTP機能をモニタリングするために用いるコマンド

ＮＴＰのこれらの機能を悪用



※ブロードバンドルータにおいては、通常、外部からの時刻の問い合わせに応答する必要はないが、多くのルータでこの設定がオンになっており、攻撃者においてこれを攻撃に悪用している

３．SMTP認証の情報を悪用したスパムメールへの対処（対策１）

- 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、メールアドレス及びSMTP認証のIDを分析することにより、スパムメールが一のSMTP認証のIDを用いて送信されているにもかかわらず、当該認証の発信元IPアドレスが瞬時に別の国や地域に移動している等、SMTP認証のID・パスワードの不正利用の蓋然性が高いもの について、当該IDからのSMTP認証を一時停止するとともに、そのID・パスワードを不正に利用されている利用者に対し、個別に連絡を取り、パスワードの変更を依頼することは、正当業務行為として違法性が阻却されると考えられる。（第一次取りまとめ　P30）

ガイドラインにおいて　１　迷惑メール等　(4) SMTP認証の情報を悪用した迷惑メールへの対処　(ナ)　として以下のように整理された。（P21　）

しかしながら、これらの行為は、正規の利用者以外の者が不正に電気通信役務を享受することを防止するとともに、SMTP認証のIDを不正に利用した迷惑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に行うものであり、侵害される通信の秘密もSMTP認証の発信元IPアドレス、タイムスタンプ、メールアドレス及びSMTP認証のIDのみと相当な限度で行われることから、正当業務行為に当たり違法性が阻却されると考えられる。

３．SMTP認証の情報を悪用したスパムメールへの対処（対策２）

- SMTP認証のID・パスワードの不正取得それ自体を防ぐために、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、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のアカウントハッキング である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認証を止めることで、SMTP認証のID・パスワードの不正取得を防ぐことは、正当業務行為として違法性が阻却されると考えられる。（第一次取りまとめ　P31）

ガイドラインにおいて　１　迷惑メール等　(4) SMTP認証の情報を悪用した迷惑メールへの対処　(二)　として以下のように整理された。（P21　）

当該行為は、正規の利用者以外の者が不正に電気通信役務を享受することを防止するとともに、SMTP認証のID・パスワードの不正取得から生じ得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に行うものであり、侵害される通信の秘密も、認証の発信元IPアドレス、タイムスタンプ、認証回数、認証間隔のみと相当な限度で行われることから、正当業務行為に当たり違法性が阻却されると考えられる。

４．マルウェア感染駆除の拡大

第三者から提供されたマルウェア感染端末情報（IPアドレス及びタイムスタンプ）と契約者の接続ログを突合し、当該感染端末を保有している契約者を特定した上で、当該加入者に対して注意喚起

C&Cサーバ等がテイクダウンされた場合において、当該C&Cサーバ等に蓄積されている、C&Cサーバとマルウェアに感染したコンピュータ等の端末（以下「マルウェア感染端末」という。）との間の通信の履歴のうち、マルウェア感染端末に係るIPアドレス及びタイムスタンプを基に、ISPにおいて、タイムスタンプに示された時刻において当該IPアドレスをどの利用者に割り当てたか確認して、該当利用者を割り出し、メール等によって個別に注意喚起を行うこと

ガイドラインにおいて第2章　各論　第5条３　その他の情報共有・情報把握について　(1) 踏み台端末や攻撃中継機器への対処　(ﾉ)　第三者から提供されたマルウェア感染端末情報（IPアドレス及びタイムスタンプ）と契約者の接続ログを突合し、当該感染端末を保有している契約者を特定した上で、当該加入者に対して注意喚起を行うことができるか、として以下のように整理された。(P23)

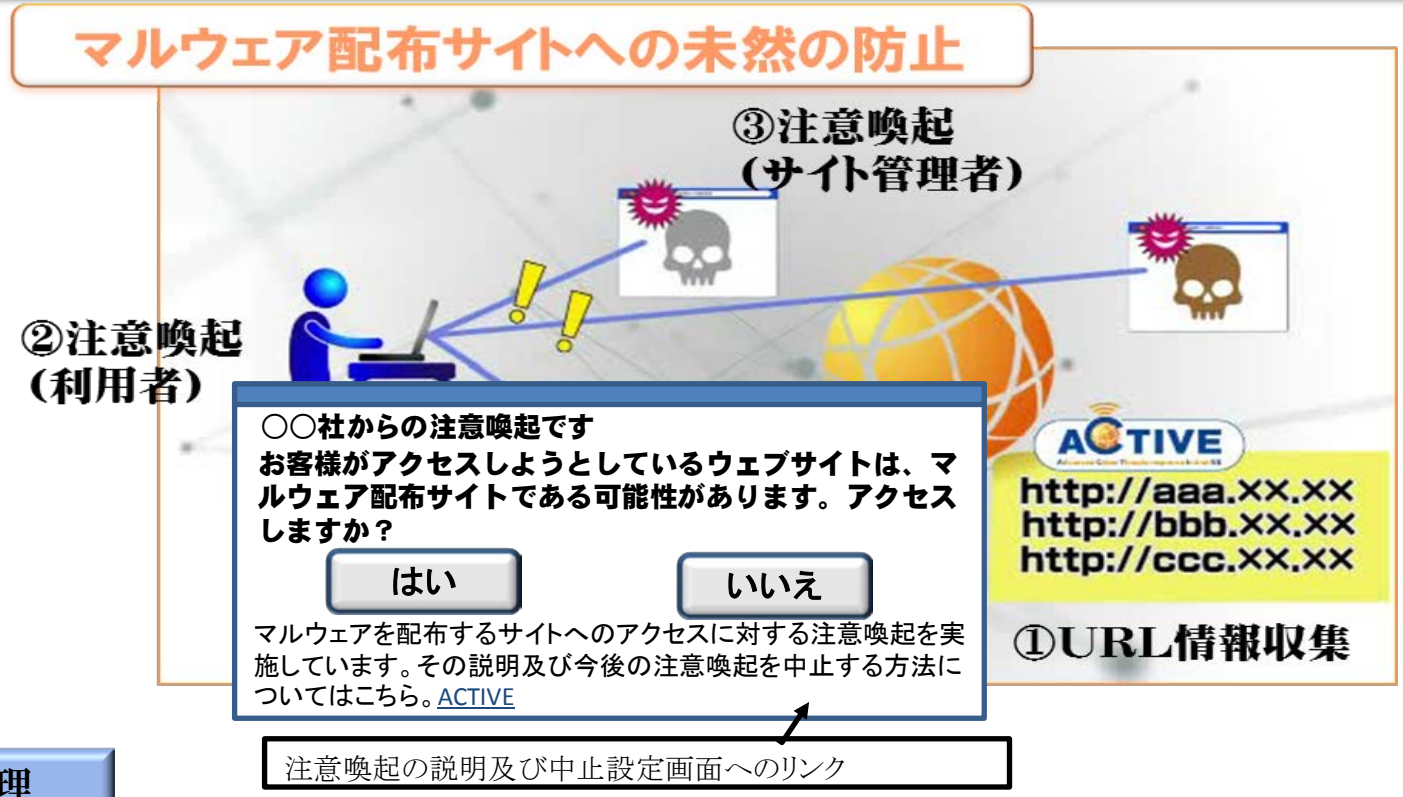
当該行為については、マルウェアの感染による当該端末が正常かつ安全に機能することに対する現在の危難を避けるための緊急避難として、違法性が阻却される

（参考）「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）

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

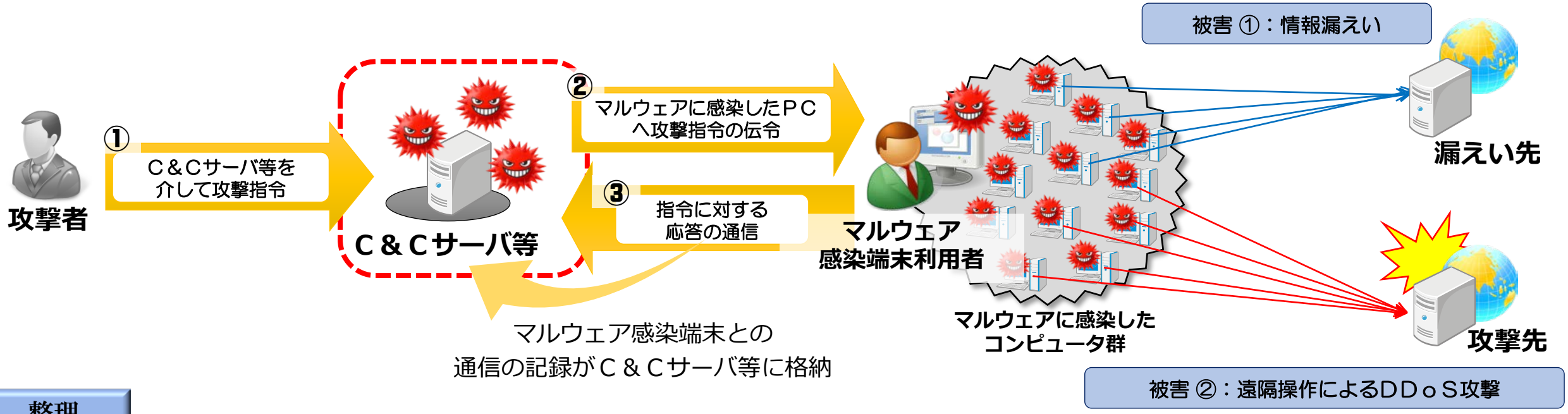
■ 次の3条件を満たせば、個別の同意ではなく、約款に基づく包括的な同意であっても有効な同意ということができる。

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

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。

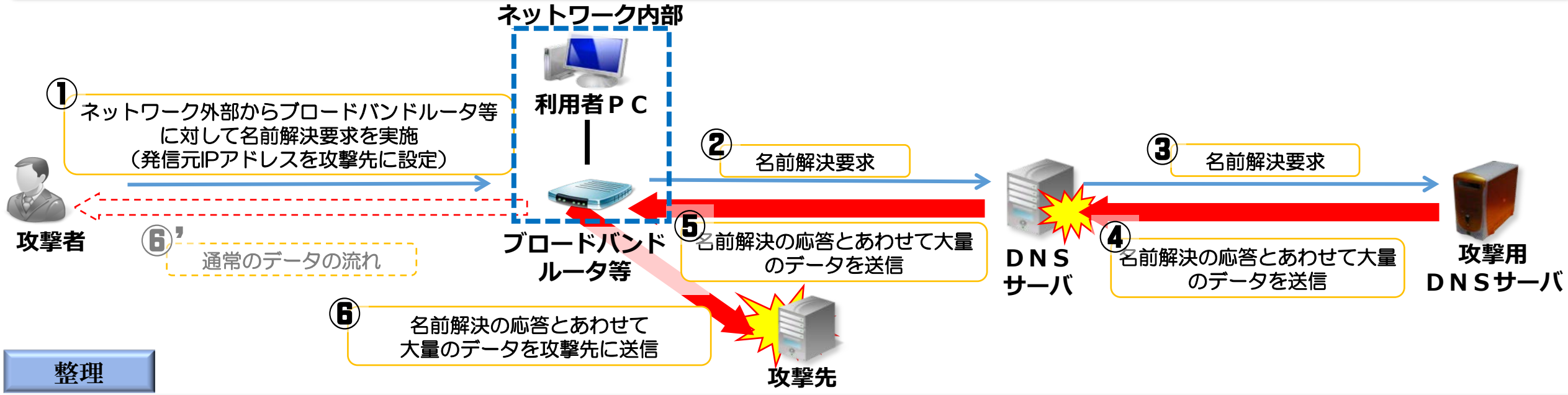
「**補充性**」：感染端末の利用者に対する個別の注意喚起以外の方法でマルウェア駆除の目的達成に有効な手立てが考えがたい。

（参考）「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）

③ 新たなDDoS攻撃であるDNSAmp攻撃の防止

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。

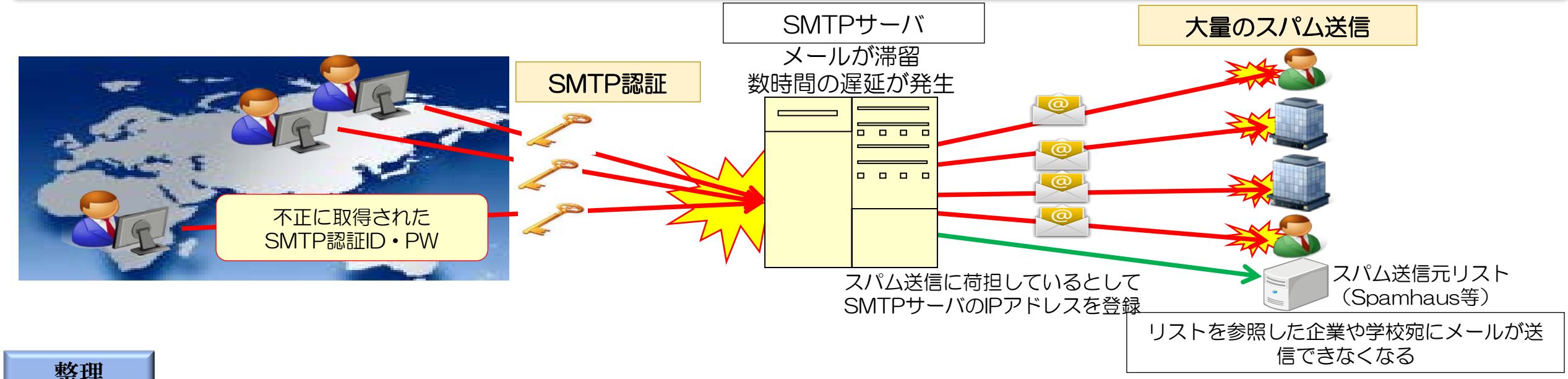
「**行為の必要性**」：他の部分での対策は困難である一方、本件ISP網の入口・出口での対策は可能かつ必要である。

「**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。

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。

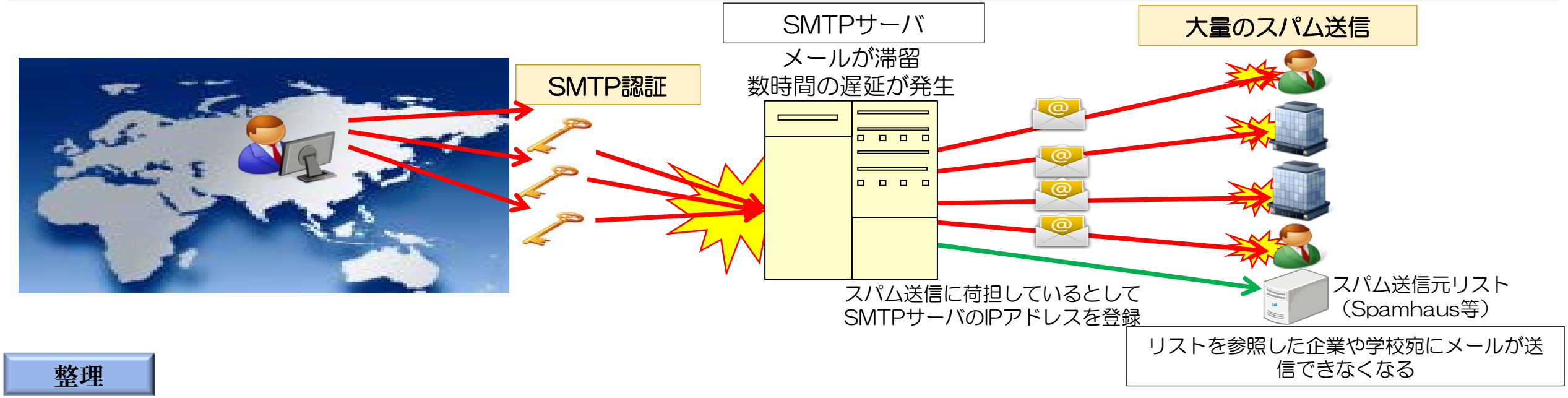
「**手段の相当性**」：侵害される通信の秘密は、滞留したメールに係るSMTP認証の発信元IPアドレス、タイムスタンプ、メールアドレスのみであり、検知・確認結果を本件対策以外の用途で利用しない場合は、侵害の程度は相対的に低い。

（参考）「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）

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。