別紙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
第二次とりまとめ
（案）

平成２７年７月

目次

序章　・・・１

第１章　最近のサイバー攻撃に係る課題と対策例　・・・・２

第２章　具体的検討　・・・１２

第１節　C&C サーバ等との通信の遮断における有効な同意について　・・・１２

第２節　他人の ID・パスワードを悪用した
インターネットの不正利用への対処について　・・・１４

第３節　脆弱性を有するブロードバンドルータ
利用者への注意喚起について　・・・１６

第４節　DNS の機能を悪用した DDoS 攻撃に用いられている名前解決要求に
係る通信の遮断について　・・・２２

第３章　おわりに　・・・２５

（参考資料）

○　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

○　開催経緯

序章

情報通信技術の発展に伴い、昨今、巧妙化、複雑化するサイバー攻撃に対して、電気通信事業者が通信の秘密等に配慮した適切な対応を行うことが可能となるよう、総務省では、平成 25 年 11 月から「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」（以下「研究会」という。）を開催し、平成 26 年４月には優先的に対応すべき課題とそれぞれの課題の解決の方向性について、「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」（以下「第一次とりまとめ」という。）として公表した。インターネット・サービス・プロバイダ（ISP）等電気通信事業者においても、第一次とりまとめの整理を踏まえて、平成 26 年７月に「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「大量通信ガイドライン」という。）」[1]を改定する等、サイバー攻撃の脅威に対して官民が協働して対処に当たってきた。

近年、サイバーセキュリティを取り巻く環境は大きく変化している。政府においては、平成 26 年 11 月に政府全体のサイバーセキュリティ推進体制の強化に向けたサイバーセキュリティ基本法が成立し、これを受けて、我が国におけるサイバーセキュリティの司令塔機能を担う組織として内閣サイバーセキュリティセンター（NISC[2]）が設置されたところである。また、今回の取りまとめに向けた検討が開始された矢先である平成 27 年６月には、日本年金機構が標的型攻撃[3]と呼ばれるサイバー攻撃を受け、大量の年金加入者に関する情報が流出していたことが明らかになる等、サイバー攻撃が国民生活に与える影響の大きさが改めて浮き彫りになったと言える。

こうした中、研究会では、第一次とりまとめ以降に発生したサイバー攻撃の動向を踏まえ、電気通信事業者が通信の秘密等に配慮した適切な対応を行うことを可能とすることで、電気通信事業者がより能動的にサイバー攻撃に対処できるような取組について、技術的・制度的な観点から議論を行った。

本報告書は、研究会における議論や検討に基づき、それぞれの課題の解決の方向性について取りまとめたものである。今後、本報告書を参照し、電気通信事業者において、引き続き自主的に適正なサイバー攻撃への対処が行われることを期待する。

---

1 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から構成される「インターネットの安定的な運用に関する協議会」が策定及び改定。総務省はオブザーバーとして参加。

2 National center of Incident readiness and Strategy for Cybersecurity の略。

3 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。

第１章　最近のサイバー攻撃に係る課題と対策例

（１）C&C サーバ[4]等との通信の遮断について

第一次とりまとめにおいて、攻撃者が用意した C&C サーバ等の攻撃に係るサーバ（以下「C&C サーバ等」という。）に記録されたマルウェア感染端末の IP アドレスとタイムスタンプの情報に基づいて、マルウェア感染端末の利用者に注意喚起できるかについて整理した。本整理を踏まえ、平成 26 年７月[5]及び平成 27 年４月[6]には、ISP からインターネットバンキングに係るマルウェア感染端末の利用者に対して注意喚起が行われている。

これらの取組を通じてマルウェア感染を駆除する試みは一定の成果を上げているところであるが、本取組はあくまでも過去の通信履歴に基づいた注意喚起であるため、既に C&C サーバ等から攻撃の指令が行われ、利用者が何らかの被害を受けている可能性が高く、事後救済的な利用者保護にとどまっている。また、C&C サーバ等との通信は、通信が行われているという事実やその内容について利用者が認知できないままバックグラウンドで実行され、利用者に重大な被害をもたらすものである。そこで、利用者保護をより進める観点から、C&C サーバ等との通信による利用者の被害を未然に防止するために、ISP において、C&C サーバ等との通信が行われている時点を捉えた対策について検討する必要がある。

具体的には、ISP が C&C サーバ等の FQDN[7]のリストを保有している場合[8]において、ISP の DNS[9]サーバを通過する通信を検知し、名前解決要求に係る FQDN と、リストにある FQDN が一致する場合に当該名前解決要求に係る通信を遮断する手法が考えられる。

---

4 Command and Control サーバの略であり、外部から侵入して乗っ取ったコンピュータを多数利用したサイバー攻撃において、コンピュータ群に対して攻撃者からの指令を送り、制御を行うサーバコンピュータのこと。

5 http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000080.html

6 http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000092.html

7 Fully Qualified Domain Name の略。サブドメイン名及びドメイン名からなる文字列であり、ネットワーク上のコンピュータ（サーバ等）を特定するもの。

8 例えば、ISP において、第三者へ危害を与えることがないよう対策を施した端末を用意し、その端末をあえてマルウェアに感染させて挙動を観察し、攻撃者から C&C サーバ等と通信するよう指令が出た場合に、その FQDN を捕捉する等の手法が考えられる。

9 Domain Name System の略で、インターネット上のコンピュータ同士が通信する際に、通信相手を特定するためにドメイン名と IP アドレスを対応づける仕組みのことをいう。

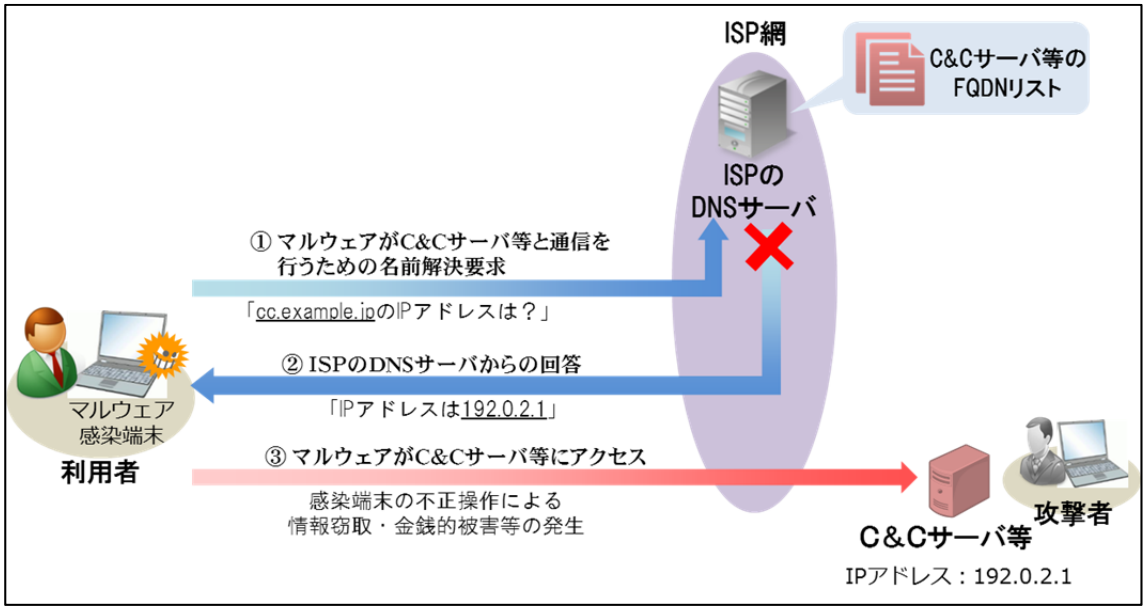

図１　C&C サーバ等との通信の遮断

一方で、ISP において、利用者が行う名前解決要求が C&C サーバ等との通信に係るものであるかどうかを検知する行為は、通信の秘密の侵害に該当することから、当該取組の実施に当たっては、通信の秘密に属する事項の利用について、あらかじめ利用者（当該 ISP のインターネット接続サービスの利用者）からの有効な同意を得ることが必要となる。この「有効な同意」に関して、運用上、既に契約をしている利用者から改めて個別の同意を得ることは困難であり、また、仮に個別の同意について呼びかけをしたとしても、利用者が当該呼びかけに気が付かなければ、個別に同意を得ることは難しく、結果的にマルウェア感染による被害を防止できないという結果となる。

このため、C&C サーバ等との通信の遮断について、どのような場合であれば、通信の秘密に属する事項の利用に対する利用者の「有効な同意」があると考えられるのか検討する必要がある。

（２）他人の ID・パスワードを悪用したインターネットの不正利用への対処について

昨今、攻撃者において第三者の ID・パスワードを悪用して他人になりすまし、各種ウェブサイト等にサイバー攻撃を行う事態が頻発している。

一般に、利用者がインターネットを利用する際には、その契約する ISP の認証サーバにおいて、正規の利用者であることの認証が行われている。主流の接続認証方式である PPPoE[10]認証においては、認証が成功すると、ISP から利用

10 Point-to-Point Protocol over Ethernet の略。主に利用者の認証や IP アドレスの割り当て等を行う PPP のプロトコルを、一般に LAN などで使用されている Ethernet の規格にお

者に IP アドレスが割り当てられ、利用者はインターネットを利用することができる。この PPPoE 認証の ID・パスワードは、通常、利用者が ISP との契約後、最初にインターネットの接続設定を行った際にブロードバンドルータに保存され、以降は利用者が当該認証を意識することなくインターネットを利用することが可能になっている。

この PPPoE 認証の ID・パスワードに関して、特定のブロードバンドルータに当該 ID・パスワードを窃取され得る深刻な脆弱性[11]があることが確認されている。当該脆弱性を突いてブロードバンドルータから PPPoE 認証の ID・パスワードを窃取し、これを悪用することで、IP アドレスを不正に取得することができ、発信者の特定を困難にした上で、リスト型攻撃[12]やソーシャル・ネットワーキング・サービス（SNS）を通じた詐欺行為、フィッシングメールの送付等の様々なサイバー攻撃等を行うことが可能となる。また、攻撃者が窃取した PPPoE 認証のパスワードを変更すれば、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想定される。

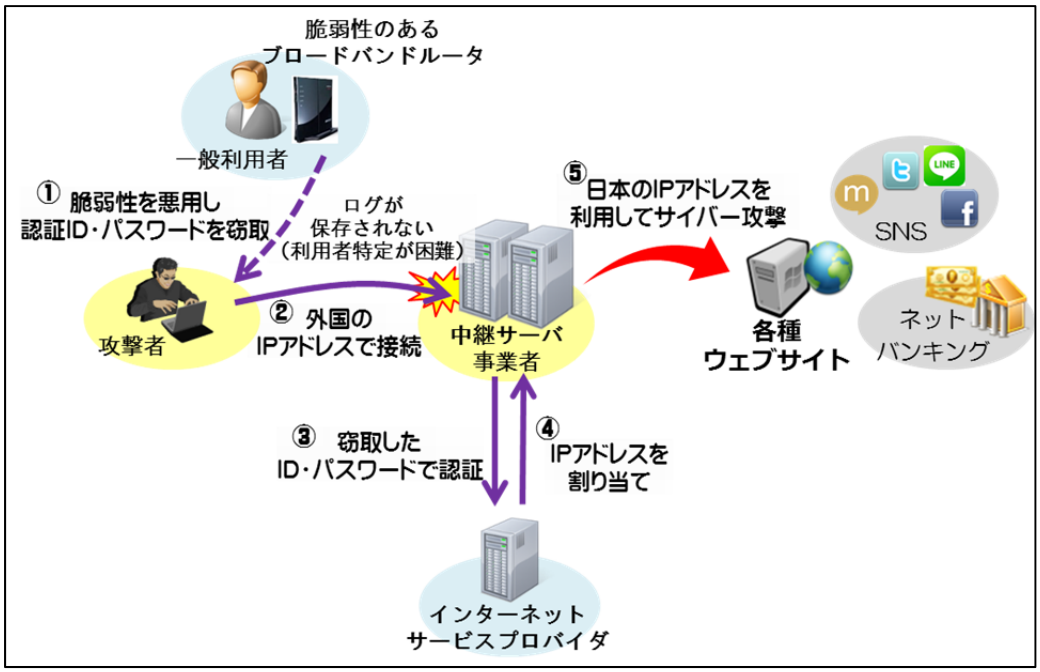

図２　他人の PPPoE 認証の情報を悪用したサイバー攻撃

いても利用できるようにするためのプロトコルをいう。

[11] 本ブロードバンドルータにおいては、

ⅰ 本来必要なアクセスコントロールが実施されておらず、インターネット側からブロードバンドルータの管理画面にアクセスが可能である、

ⅱ ルータの管理画面にログインするための ID・パスワードの初期設定が一律で平易なもの（例：ID、パスワードとも“admin”）である、

ⅲ ログイン後の管理画面において PPPoE 認証の ID・パスワードが暗号化されていない、

といった脆弱性を有しており、PPPoE 認証の ID・パスワードが容易に窃取可能であった。

[12] 何らかの手段により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様々なサイトにログインを試みることで、個人情報の閲覧等を行うサイバー攻撃。

このように、他人の PPPoE 認証の情報を悪用したインターネットの不正利用が行われると、正規の利用者のインターネット利用が阻害され、ひいては、ISP の電気通信役務の円滑な提供に支障を及ぼすおそれがあるため、対策を講じる必要がある。

具体的な対策としては、ISP において短時間に大量の認証要求が行われ、認証サーバにおいて異常を検知した際に、PPPoE 認証に係るログから、当該 ID に対して割り当てた IP アドレス等を分析することにより、同一の PPPoE 認証 ID に対して、短時間のうちに大量の認証要求が行われている、又は異なる地域に属する IP アドレスを割り当てている[13]等、PPPoE 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 に係るインターネット接続を切断し、当該 ID からの認証を一時的に停止した上で、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が考えられる。

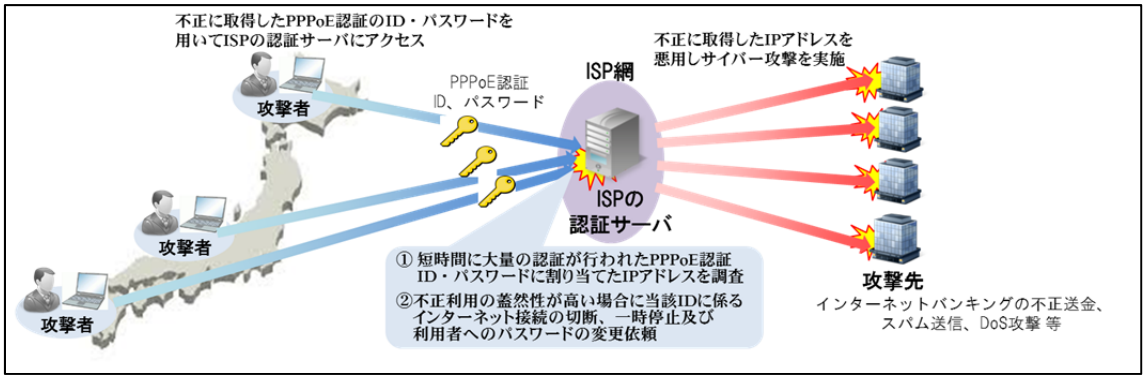

図３　他人の ID・パスワードを悪用したインターネットの不正利用への対処

（３）脆弱性を有するブロードバンドルータ利用者への注意喚起について

第一次とりまとめにおいて整理した DNSAmp 攻撃[14]等のリフレクション攻撃[15]に悪用され得る脆弱性や、上記（２）において記載した PPPoE 認証の情報を窃

---

13 短期間のうちに同一の ID に対して、北海道の範囲に属する IP アドレスや、鹿児島県の範囲に属する IP アドレスを割り当てていた場合等が考えられる。

14 小さなパケットを送るだけで、その何倍ものサイズにパケットを増幅（amplification）させる性質の攻撃を Amp 攻撃と呼び、DNS の仕組みを悪用したものについては DNSAmp 攻撃と呼ばれる。

DNSAmp 攻撃は、下記ｉの準備の下、下記 ii からⅳの一連の動作を繰り返し行うことによって、攻撃先に増幅されたパケットを何度も送り、大量のトラヒックを発生させる攻撃である。

ｉ　攻撃用 DNS サーバとして、あらかじめ公開 DNS サーバに対してある名前解決の問合わせがあった場合に増幅されたパケットを応答するものを用意し

ii　その後、送信元 IP アドレスを攻撃先 IP アドレスに詐称させて、一斉に利用者が設

取され得る脆弱性といった、サイバー攻撃につながり得る脆弱性を有するブロードバンドルータがインターネット上に数多く存在している。これらのブロードバンドルータを製造した事業者においても、脆弱性を修正するソフトウェアを公開する等、これを減少させるための一定の努力はなされているものの、現在もサイバー攻撃を発生させるのに十分な数がインターネット上に残されている。これらの脆弱性を有するブロードバンドルータを通じてリフレクション攻撃等の DDoS 攻撃や、PPPoE 認証の情報の窃取が行われると、ISP による電気通信役務の安定的提供等に支障が生じることとなる。

このような脆弱性を有するブロードバンドルータを通じたサイバー攻撃を未然に防止するためには、当該脆弱性を有するブロードバンドルータを調査した上で、積極的にこれを減少させる取組が必要となる。

これらのサイバー攻撃につながり得るブロードバンドルータにおいては、必要なアクセスコントロールが実施されておらず、インターネット側からの要求に対して、通常必要の無い応答を行ってしまうという脆弱性を有している。そこで、インターネット側からブロードバンドルータに対して名前解決要求等を行い、これに応答するブロードバンドルータを調査することで、応答のあったブロードバンドルータに関する情報に基づいて利用者を特定し、注意喚起を呼びかける手法が考えられる。

具体的には、①DNSAmp 攻撃等のリフレクション攻撃に悪用され得る脆弱性の有無を調査するため、一定の IP アドレスのレンジに対して網羅的に名前解決要求を行い、当該名前解決要求に対して IP アドレスの応答があった場合、又は②PPPoE 認証の情報を窃取され得る脆弱性の有無を調査するため、一定の IP アドレスのレンジに対して網羅的に HTTP のリクエスト[16]を行い、当該 HTTP リクエストに対してブロードバンドルータの管理画面にログインするための認証の要求があった場合において、応答等のあったブロードバンドルータの IP アドレス及びタイムスタンプの情報をもとに、ISP においてタイムスタンプ

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してインターネット側から名前解決要求を出し

iii　当該ブロードバンドルータ等のゲートウェイから、ISP の DNS サーバを経由して、当該攻撃用 DNS サーバに問合せをさせ

iv　当該攻撃用 DNS サーバから、問合せに対応して、上記 i の増幅されたパケット（問合せに係る通信量と比較して増幅された応答となっている。）を、ISP の DNS サーバを経由して、送信元として詐称された攻撃先 IP アドレスに送信する

（第一次とりまとめ 10 頁より）

[15] 送信元からの問い合わせに対して反射的に応答を返すように動作する機能（リフレクション機能）を持つ情報通信機器を悪用することで、問い合わせに対する反射された応答を攻撃先に送信するサイバー攻撃。

[16] 通信機器に保存されている html ファイルや jpeg ファイル等のコンテンツの取得要求を行うこと。

に示された日時分秒において当該 IP アドレスをどの利用者に割り当てたかを確認し、該当利用者を割り出すことで、メール等によって当該利用者に対して個別に注意喚起を行うことが考えられる。

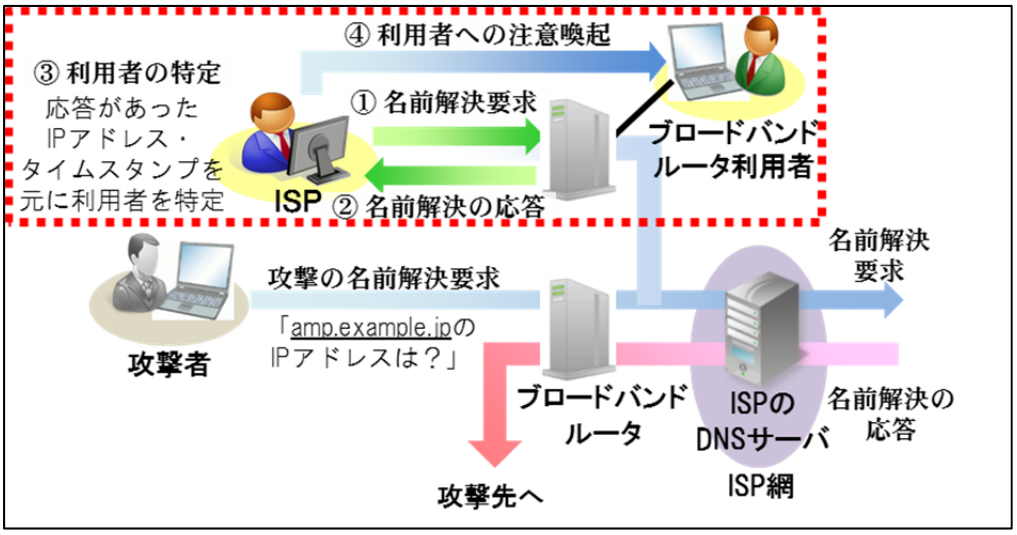

図４　脆弱性を有するブロードバンドルータの調査
（DNSAmp 攻撃等のリフレクション攻撃に悪用され得る脆弱性）

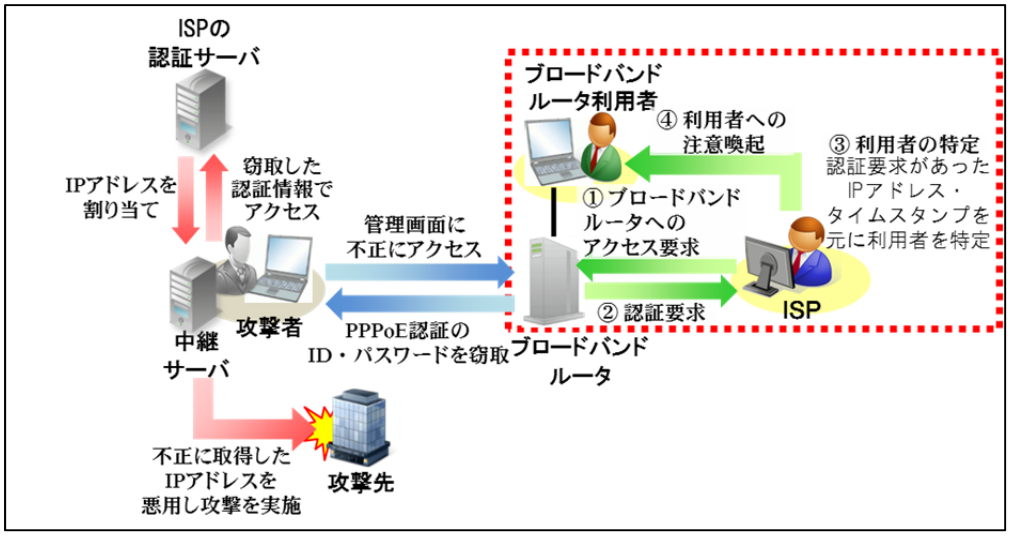

図５　脆弱性を有するブロードバンドルータの調査
（PPPoE 認証の情報を窃取され得る脆弱性）

（４）DNS の機能を悪用した DDoS 攻撃に用いられている名前解決要求に係る通信の遮断について

①　固定 IP アドレスを使用している通信機器を踏み台とした DNSAmp 攻撃への対処

第一次とりまとめにおいて、DNSAmp 攻撃に対処するため、インターネット側からの動的 IP アドレス宛てであって、UDP53 番ポートへの名前解決要求に係る通信の遮断について整理し、これを受けて、いくつかの ISP において実装

が進められているところである。本対策については、一定の有効性が認められるが、インターネット側から固定 IP アドレスを使用している通信機器に対して名前解決要求を行うことで攻撃を発生させるものも数多く発生しており、その対策について検討を行う必要がある。

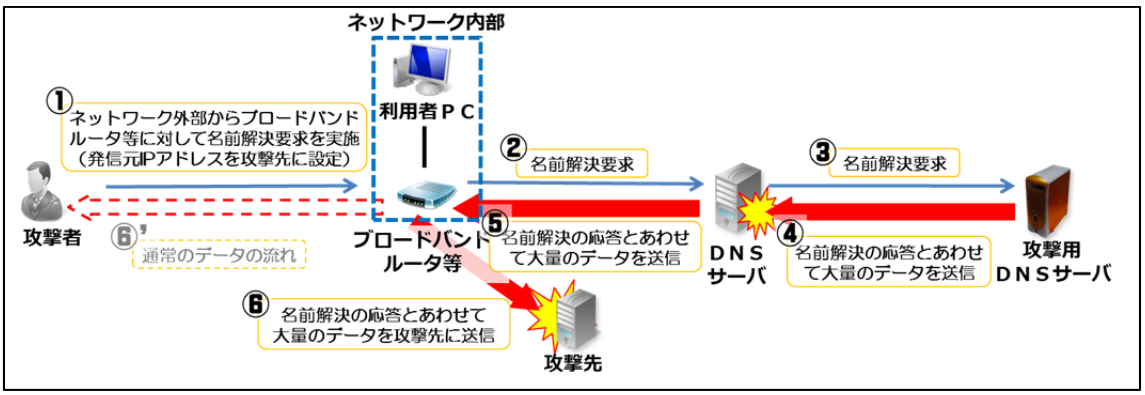

図６　DNSAmp 攻撃（第一次とりまとめ 11 頁より）

②　新たな DDoS 攻撃であるランダムサブドメイン攻撃への対処

上記①に記載のとおり、第一次とりまとめにおいては、DNS 等のインターネット上の正常な機能を悪用した DDoS 攻撃の手法の一つである DNSAmp 攻撃への対策について整理したところである。このような DNS の機能を悪用した新たな DDoS 攻撃として、最近では、ランダムサブドメイン攻撃[17]と呼ばれる DDoS 攻撃が発生しており、国内の観測網においても本攻撃と思われるパケットを多数観測[18]している。DNS の機能を悪用したこの攻撃は、マルウェア感染活動による DDoS 攻撃と異なり、正常な通信と不正な通信の見分けがつきにくいため、従来のマルウェア感染駆除や感染防止の取組では対応ができないという問題がある。

ランダムサブドメイン攻撃は、下記ｉからiiiの一連の動作を繰り返し行うことによって、権威 DNS サーバ[19]及び ISP の DNS サーバに大量の名前解決要求の処理を発生させる攻撃である。

ｉ　攻撃者は、攻撃対象のドメインのサブドメイン部分にランダムな文字列を付与した上で、一般のインターネット利用者が設置しているブロードバンドルータ等インターネット接続のゲートウェイに対して名前解決要求を出し【図７の①部分】

17 DNS 水責め攻撃とも呼ばれる。
18 JPCERT/CC インターネット定点観測レポート（2014 年 4 月～6 月）
19 あるドメイン名に対する IP アドレス等の情報を管理している DNS サーバをいう。

ii　当該ブロードバンドルータ等のゲートウェイはISPのDNSサーバを経由して攻撃対象のドメインの情報を有する権威DNSサーバに問い合わせを行い【図７の②及び③部分】

iii　問い合わせを受けた当該権威DNSサーバは、存在しないサブドメインに関する名前解決要求に対して、問い合わせのあったドメインに対応するIPアドレスが存在しない旨の回答を行うことになる【図７の④及び⑤部分】

この一連の攻撃が、複数のゲートウェイに対して大量に行われることで、権威DNSサーバに大量の問い合わせが集中して負荷が生じ、権威DNSサーバが応答不能になる[20]とともに、ISPのDNSサーバにおいても、権威DNSサーバからの回答待ちが多数発生することで名前解決要求が滞留し、ISPのDNSサーバが応答不能になる等多大な影響が発生する。

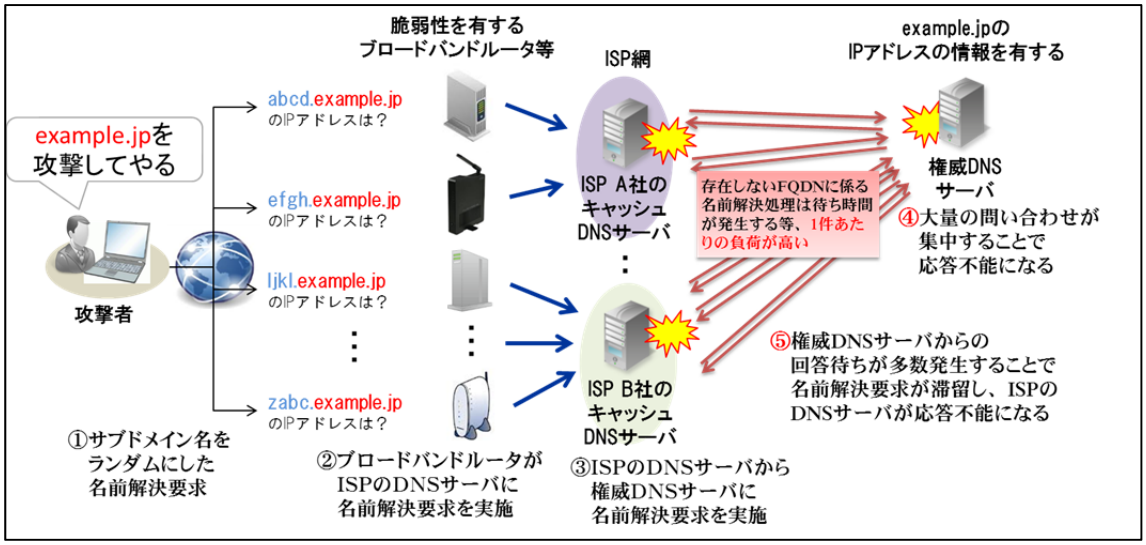

図７　ランダムサブドメイン攻撃

ランダムサブドメイン攻撃によるものと見られるDDoS攻撃の影響により、国内の複数のISPにおいてインターネットアクセス等に遅延が発生したという報告があり、ある大手ISPにおいては、平成26年度に171回発生しており、攻撃に利用されたDNSサーバが、約16時間にわたって高負荷になり、名前解決の遅延が発生するなど、利用者の電気通信役務利用を妨げている状況にある。ISPによるインターネット接続役務等の電気通信役務を安定的に運用するためには、このような攻撃への対策を検討する必要がある。

[20] 存在しないサブドメインに関する名前解決要求については、権威DNSサーバにおける処理に時間を要するため、大量の問い合わせが集中することで権威DNSサーバの負荷が高まり、最終的に権威DNSサーバが応答不能になる。

③　攻撃に対する対策の方向性

DNS の仕組みを悪用した攻撃に係る通信については、外形上正常な通信と不正な通信との見分けがつきにくく、攻撃に係る通信のみを個別に遮断することが困難であるところ、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に係る通信の遮断については、通常のインターネット利用への影響が考え難いことから、第一次とりまとめにおいてこれを整理したところである。

しかしながら、上記①のとおり、固定 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を通じた DNSAmp 攻撃や、新たな DDoS 攻撃であるランダムサブドメイン攻撃も数多く発生しており、これへの対策を講じる必要がある。対策の検討にあたり、固定 IP アドレスを使用している通信機器については、動的 IP アドレスを使用している通信機器と異なり、通常の利用においてインターネット側からの名前解決要求を受けることも想定され、これを一律に遮断することは適当ではないと考えられる。

こうした中、DNSAmp 攻撃やランダムサブドメイン攻撃に用いられている名前解決要求に係るドメイン名（FQDN）を捕捉し、リスト化する対策手法が確立[21]されたことから、ISP の DNS サーバを通過する通信を検知し、名前解決要求に係る FQDN と、リストにある FQDN が一致する場合に当該名前解決要求に係る通信を遮断する手法が考えられる。

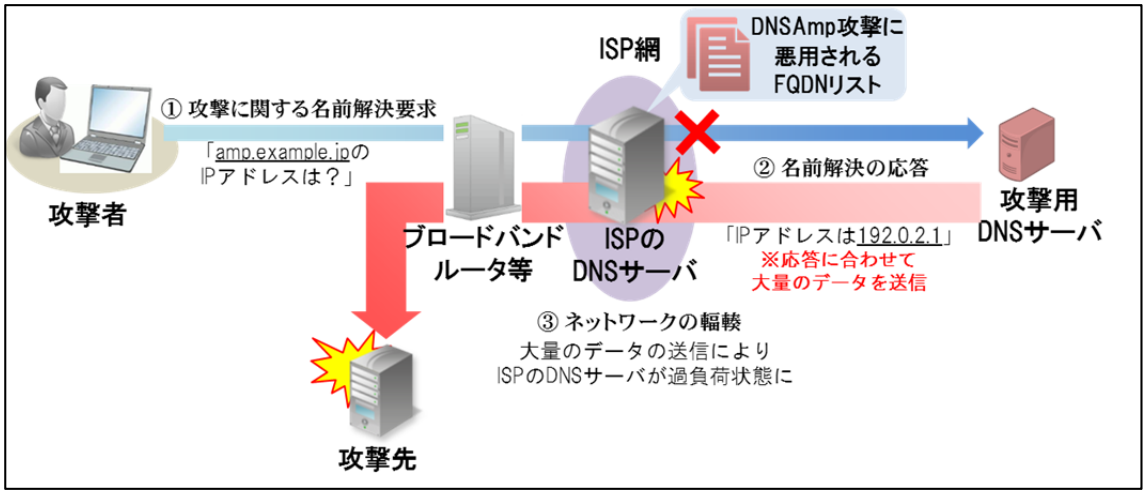

図８　DNSAmp 攻撃に用いられている名前解決要求に係る通信の遮断

[21] 攻撃に係る通信を発生させないよう対策を施したオープンリゾルバ（※）の脆弱性を有する DNS サーバを用意して監視下に置き、当該 DNS サーバに対して攻撃に係る通信が送信された際に、当該通信を解析することで、どの FQDN が攻撃に悪用されているか、攻撃先がどこか等を把握することができる。

※　オープンリゾルバ：通信機器の不適切な設定やデフォルト設定の不備等により本来必要なアクセスコントロールが実施されていないため、インターネット上のどこからの要求であっても応答を返してしまう状態にある脆弱性のこと。

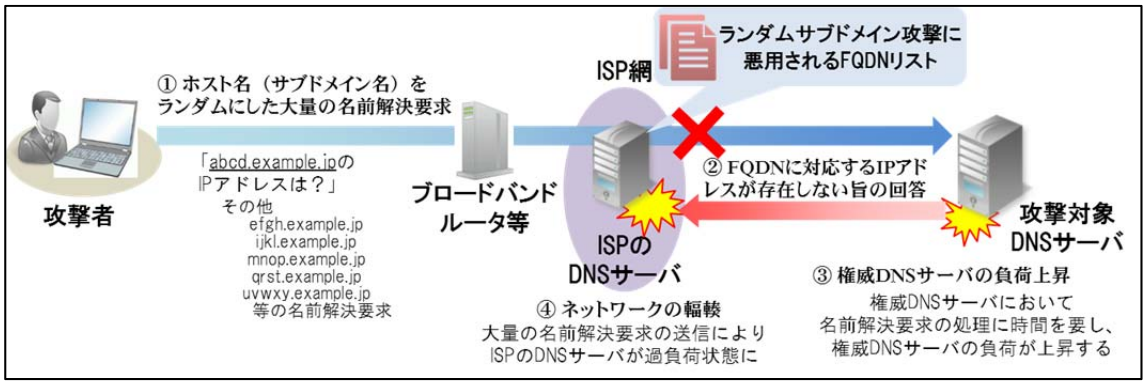

図９　ランダムサブドメイン攻撃に用いられている名前解決要求に係る通信の遮断

第２章　具体的検討

第１章に記載した最近のサイバー攻撃に係る課題と対策例に基づき、当該対策例と通信の秘密等との関係について以下のとおり検討を行った[22]。

第１節 C&C サーバ等との通信の遮断における有効な同意について

（１）対策の概要及び問題の所在

C&C サーバ等の FQDN が判明している場合において、感染者が情報窃取や金銭的被害等の深刻な被害を受けることを防ぐとともに、感染者を踏み台にした新たな攻撃の発生を防ぐため、ISP が自社 DNS サーバを通過する利用者のアクセスに係る FQDN を検知し、C&C サーバ等の FQDN の名前解決要求に係る通信を遮断することが考えられる。

この点、C&C サーバ等へのアクセスに対する遮断を行うに当たって利用等される通信の宛先 FQDN は、通信の構成要素であり、通信の秘密の保護の対象であることから、通信の宛先 FQDN を検知した上で、該当するアクセスを遮断することは、利用者の有効な同意がない限り、通信の秘密の窃用等に該当し、通信の秘密の侵害となる。

通信の秘密についての同意は、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おらず、個別の同意でなくてはならないと解されている。しかしながら、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いては、一定の要件の下で契約約款による事前の包括同意で許容されると整理したところ、本件においても、利用者の被害防止のため、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を行う。

（２）有効な同意についての考え方

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としては、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こと、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ことが挙げられる。なお、理由②を補足すると、同意の対象・範囲が不明確となることにより、利用者に不測の不利益が生じることに問題意識がある[23]。

これを C&C サーバ等へのアクセスに対する遮断についてみるに、理由①と

---

[22] 通信の秘密についての基本的な考え方は、第一次とりまとめ 15 頁以下参照。

[23] 第一次とりまとめ 19 頁及び総務省「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（平成 22 年５月）12 頁より。

の関係では、一般的・類型的に見て、ISP が C&C サーバ等へのアクセスに対する遮断を行うに当たって、通信の秘密に当たる情報のうち必要最小限度の事項（通信の宛先 FQDN）のみを機械的・自動的に検知した上で、該当するアクセスを遮断することは、マルウェア感染による被害拡大を防止し、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、ブラウザ経由の注意喚起画面を表示させることができないために遮断を実施するものであるから、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得るため、契約約款の性質になじまないとまでは言えない。

なお、マルウェア配布サイトへのアクセスに対しては注意喚起を実施する一方、本件対策では直ちに遮断を実施することとなるが、C&C サーバ等との通信はブラウザを介さず、ブラウザ経由の注意喚起画面を表示させることができないことから遮断を実施するものであり、遮断が許されるのは当該通信の性質を考慮したものである点について留意が必要である。

理由②との関係では、利用者が、いったん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、当該契約約款の内容及び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、並びにそれらについて利用者に相応の周知が図られている場合には、契約約款による包括同意当時において予測し得なかった事情が将来生じた場合についても、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と考えられる。

この点、本件対策において、遮断を希望しない者に対しては別の DNS サーバを使用するなど、オプトアウトができるような対応を行うことにより、利用者が、いったん契約約款に同意した後も、随時、同意内容を変更でき（設定変更でき）、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契約内容とした上、アクセスの遮断並びに遮断を望まない利用者は随時同意内容を変更できる（設定変更できる）こと及びその方法について利用者に相応の周知が図られている場合には、契約約款による包括同意当時において予測し得なかった事情が将来生じた場合についても、随時、利用者が同意内容を変更することができると言えることから、将来、利用者が不測の不利益を被る危険を回避できる。利用者に対する相応の周知の方法としては、ウェブサイトへの掲載等を行うとともに、利用者に対するメールの送付等により、マルウェア感染駆除の注意喚起をするとともに、遮断の実施、随時同意内容を変更できる（設定変更できる）こと及びその方法等について個別の説明をすることが考えられる。

したがって、上記の要件を満たす場合、本件対策について、契約約款に基づく事前の包括同意であっても、当該遮断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考えられる。

上記の契約約款においては、少なくとも以下のような内容を規定すべきと考えられる。

＜契約約款に記載すべき事項＞

・　検知を行うこと

（例）検知を行う

・　C&C サーバ等へのアクセスに係る通信の検知の目的

（例）利用者が C&C サーバ等とアクセスしようとする場合には、そのアクセスを遮断するため

・　検知の時期

（例）利用者が、インターネット上のサーバに対するアクセス要求をした際

・　検知の対象となる情報の範囲

（例）利用者のアクセス要求に係る FQDN について

・　事後的に同意内容を変更できる（設定変更できる）こと

（例）当該検知等は、利用者が設定変更を申し出た場合、中止できる

なお、C&C サーバ等へのアクセスに対する遮断を行うに当たって取得した通信の秘密に当たる情報（通信の宛先 FQDN）を本件対策以外のために利用することは、同意の範囲を越えることとなるため、通信の秘密の窃用となり、通信の秘密を侵害することとなる。

第２節 他人の ID・パスワードを悪用したインターネットの不正利用への対処について

（１）対策の概要及び問題の所在

不正送金や情報窃取、大量通信等のサイバー攻撃につながるおそれのある、PPPoE 認証の情報を悪用した不正なインターネット利用を防止するためには、短時間に大量の認証要求が行われ、認証サーバにおいて異常を検知した際に、PPPoE 認証に係るログから、当該 ID に対して割り当てた IP アドレス等を分析することにより、同一の当該 ID に対して通常の利用では想定されない短時間のうちに大量の認証要求が行われている、又は当該認証に対して割り当てている IP アドレスが瞬時に別の地域に移動している等、PPPoE 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 に係るインターネット接続の切断、当該 ID からの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が考えられる。

この点、ISP の認証サーバに記録されたタイムスタンプ及び PPPoE 認証の ID は、通信の構成要素として通信の秘密の保護の対象であるから、これら

を分析し、不正利用の蓋然性が高い ID に係るインターネット接続の切断、当該 ID からの認証を一時停止し、正規の利用者へパスワードの変更依頼を行うことは、通信の秘密の窃用等に該当する可能性がある。もっとも、違法性阻却事由がある場合には、例外的に通信の秘密を侵すことが許容されることになるところ、本件対策は、正当業務行為の要件を満たすと考えることはできないか検討する。

（２）正当業務行為該当性

①　目的の正当性

本件対策の目的は、ISP において、正規の利用者に対して電気通信役務を円滑に提供するとともに、通信事業を維持・継続するため、正規の利用者以外の者が正規の利用者になりすまし、不正に電気通信役務を享受することを防止することにより、電気通信役務の円滑な提供を確保することにあるから、目的の正当性を認めることができると考えられる[24]。

②　行為の必要性

通常の利用では想定されないような短時間で大量の認証要求が一の PPPoE 認証の ID を用いて送信されている場合や、当該認証に対して割り当てている IP アドレスが瞬時に別の地域に移動している場合[25]には、当該 PPPoE 認証の ID・パスワードが不正に利用されている蓋然性が高い。

このため、認証サーバにおいて異常を検知した際に、当該サーバに記録された PPPoE 認証の ID に対して割り当てた IP アドレス、タイムスタンプ及び PPPoE 認証の ID を分析することにより、上記の特徴を有する PPPoE 認証の ID を特定した上で、当該 ID に係るインターネット接続の切断、当該 ID からの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、上記目的との関係で、行為の必要性を肯定できると考えられる。

---

24 正規の利用者に対して電気通信役務を提供することは、電気通信事業者において「電気通信役務の円滑な提供の確保」（電気通信事業法（昭和五十九年十二月二十五日法律第八十六号）第一条参照）という目的の達成に期待されるものといえ、そのため、正規の利用者以外の者が正規の利用者になりすまし、不正に電気通信役務を享受することを防止することは、正当業務行為における目的の正当性として認めることができると考えられる（正当業務行為に関する基本的な考え方について、第一次とりまとめ 17 頁及び第二次提言 14 頁、57 頁参照）。

25 ある大手 ISP において、平成 26 年８月から平成 27 年２月までに不正アクセスが行われた IP アドレスの割り当てに係る ID についてみると、本来の ID の契約者住所（都道府県単位）とは異なる地域からの接続割合は、約 82％であった。

③　手段の相当性

分析する通信の秘密は、認証サーバにおいて異常を検知した際に、当該サーバに記録された PPPoE 認証の ID に対して割り当てた IP アドレス、タイムスタンプ及び PPPoE 認証の ID のみであるから、分析の結果を本件対策以外の用途で利用しない場合であって、当該 ID に係るインターネット接続の切断、当該 ID からの認証の一時停止についても、正規利用者がパスワードを変更する等、不正利用の危険が解消されるまでの間に限られる場合には、手段の相当性も認められる。

④　まとめ

以上から、本件対策は、分析の結果を本件対策以外の用途で利用しない場合であって、当該 ID に係るインターネット接続の切断、当該 ID からの認証の一時停止についても、正規利用者がパスワードを変更する等、不正利用の危険が解消されるまでの間に限られる場合には、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３節 脆弱性を有するブロードバンドルータ利用者への注意喚起について

（１）対策の概要及び問題の所在

前述のとおり、電気通信役務の安定的提供等に影響を及ぼし得るブロードバンドルータの脆弱性には主に２通りが考えられる。具体的には、①リフレクション攻撃に悪用され得る脆弱性（オープンリゾルバ等）と、②ISP の ID・パスワードを不正窃取されるおそれのある脆弱性（前掲脚注 11 参照）である。

各ブロードバンドルータにおける当該脆弱性の修正が迅速に行われれば、DNSAmp 攻撃をはじめとするリフレクション攻撃をより前段階から防ぐことが可能となるとともに、ISP の認証 ID・パスワードを悪用し、不正ログインを行ったなりすましによる個人情報の漏えい、金銭窃取等の被害の発生等を防止することができる。

そこで ISP 又は ISP の委託を受けた事業者団体等において、ネットワーク上におけるブロードバンドルータに対して名前解決要求又は HTTP リクエストを実施することにより、脆弱性を有するブロードバンドルータを調査することが考えられる[26]。

---

[26] なお、事業者団体等が ISP の委託を受けて代表して調査を実施し、調査により判明した該当する IP アドレス及びタイムスタンプを、当該 IP アドレスの割当てを行っている ISP に提供するスキームも考えられるところ、このような行為については、調査を行った事業者団体等は、当該通信を送信した一方当事者であるから、これらを他の ISP に提供することは、通信の秘密の侵害に当たらないと考えられる（これらは、通信当事者間で共有されている情報であり、その秘密性を当事者間で相手に委ねているため、第三者への関係で、

この点について本件対策は、インターネット上に存在するブロードバンドルータに対して、脆弱性を調査する情報を実際に送信し、それにより得られる応答をもとに、当該ブロードバンドルータに脆弱性があるかどうか調査するもの[27]であり、ブロードバンドルータにおけるプログラムの瑕疵や設定上の不備に着目して、ブロードバンドルータの管理者が意図していない利用を行うものであるから、不正アクセス行為の禁止等に関する法律（以下「不正アクセス禁止法」という。）に定める不正アクセス行為に該当するかについて検討が必要となる。

また、ISP において、調査により判明した IP アドレス及びタイムスタンプ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し、利用者に注意喚起する行為について、通信の発信元 IP アドレス及びタイムスタンプは、通信の構成要素として通信の秘密の保護の対象であることから、ISP において、当該 IP アドレス及びタイムスタンプを基に、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すことは、通信の秘密の窃用等に該当する可能性がある。もっとも、違法性阻却事由がある場合には、例外的に通信の秘密を侵すことが許容されることになるところ、本件対策は、正当業務行為の要件を満たすと考えることはできないか検討する。

（２）不正アクセス禁止法との関係について

①　不正アクセス禁止法について

現代社会においては、ネットワークを通じて様々な社会経済活動が営まれている。これらのネットワークを通じた社会経済活動における安全の確保は、ネットワークを通じてコンピュータを利用する者が誰であるかを正しく識別するアクセス制御機能[28]に対する信頼に立脚している。サイバー攻撃等により、アクセス制御機能に対する信頼が損なわれる事態になれば、ネットワークを通じた社会経済活動の健全な発展が阻害されるおそれがある。そこで、アクセス制御機能に対する社会的信頼を確保して、犯罪の防止及び電気通信に関する秩序の維持を図り、もって高度情報通信社会の健全な発展に寄与することを目的として、不正アクセス禁止法において、アクセス制御機能の社会的信頼を害する不正アクセス行為等について、罰則をもってこれを禁止している[29]。

一方当事者の同意により秘密性が解除されるためである。)。

27 ポートスキャンとも呼ばれる。

28 利用権者等を ID・パスワード等の識別符号により識別し、識別符号が入力された場合にのみその利用を認めることとするコンピュータの機能（下記④参照）。

29 不正アクセス行為の禁止等に関する法律

（不正アクセス行為の禁止）

② 「不正アクセス行為」の意義

不正アクセス行為とは、特定電子計算機[30]に他人の識別符号又はアクセス制御機能による特定利用[31]の制限を免れる情報若しくは指令を入力することで、アクセス制御機能による特定電子計算機の特定利用の制限を免れて、その制限されている特定利用をし得る状態にさせることである[32]。（不正アクセス禁止法第２条第４項）

③ 「識別符号」の意義

識別符号とは、特定電子計算機の特定利用をすることについて、当該利用権者等を他の利用権者等と区別して識別することができるように付さ

第３条　何人も、不正アクセス行為をしてはならない。

（罰則）

第 11 条　第３条の規定に違反した者は、３年以下の懲役又は 100 万円以下の罰金に処する。

30 電気通信回線に接続している電子計算機をいう。

不正アクセス行為の禁止等に関する法律

（定義）

第２条　この法律において「アクセス管理者」とは、電気通信回線に接続している電子計算機（以下「特定電子計算機」という。）の利用（当該電気通信回線を通じて行うものに限る。以下「特定利用」という。）につき当該特定電子計算機の動作を管理する者をいう。

31 電気通信回線を通じて行う情報処理（インターネットへの接続、電子メールの受信、ウェブサイトの閲覧等）をいう（前掲脚注 30 参照）。

32 不正アクセス行為の禁止等に関する法律

（定義）

第２条

４　この法律において「不正アクセス行為」とは、次の各号のいずれかに該当する行為をいう。

一　アクセス制御機能を有する特定電子計算機に電気通信回線を通じて当該アクセス制御機能に係る他人の識別符号を入力して当該特定電子計算機を作動させ、当該アクセス制御機能により制限されている特定利用をし得る状態にさせる行為（当該アクセス制御機能を付加したアクセス管理者がするもの及び当該アクセス管理者又は当該識別符号に係る利用権者の承諾を得てするものを除く。）

二　アクセス制御機能を有する特定電子計算機に電気通信回線を通じて当該アクセス制御機能による特定利用の制限を免れることができる情報（識別符号であるものを除く。）又は指令を入力して当該特定電子計算機を作動させ、その制限されている特定利用をし得る状態にさせる行為（当該アクセス制御機能を付加したアクセス管理者がするもの及び当該アクセス管理者の承諾を得てするものを除く。次号において同じ。）

三　電気通信回線を介して接続された他の特定電子計算機が有するアクセス制御機能によりその特定利用を制限されている特定電子計算機に電気通信回線を通じてその制限を免れることができる情報又は指令を入力して当該特定電子計算機を作動させ、その制限されている特定利用をし得る状態にさせる行為

れる符号のことをいう[33]。（不正アクセス禁止法第２条第２項）

④　「アクセス制御機能」の意義

アクセス制御機能とは、特定電子計算機の特定利用を自動的に制御するために、当該特定利用に係るアクセス管理者によって付加されている機能であって、当該特定利用をしようとする者により当該機能を有する特定電子計算機に入力された符号が当該特定利用に係る識別符号であることを確認して、当該特定利用の制限の全部又は一部を解除するものをいう[34]。（不正アクセス禁止法第２条第３項）

⑤　本件対策における検討

本件対策は、ブロードバンドルータに対して、名前解決要求又は HTTP リクエストを行うことにより、当該ブロードバンドルータがインターネット側からのこれらの問合せに対して名前解決の結果又は HTTP レスポンスを応答するか確認するものである。

当該行為が不正アクセス禁止法第３条において禁止されている不正アクセス行為に該当するか検討すると、本件対策において当該ブロードバン

---

33 不正アクセス行為の禁止等に関する法律
（定義）
第２条
２　この法律において「識別符号」とは、特定電子計算機の特定利用をすることについて当該特定利用に係るアクセス管理者の許諾を得た者（以下「利用権者」という。）及び当該アクセス管理者（以下この項において「利用権者等」という。）に、当該アクセス管理者において当該利用権者等を他の利用権者等と区別して識別することができるように付される符号であって、次のいずれかに該当するもの又は次のいずれかに該当する符号とその他の符号を組み合わせたものをいう。
一　当該アクセス管理者によってその内容をみだりに第三者に知らせてはならないものとされている符号
二　当該利用権者等の身体の全部若しくは一部の影像又は音声を用いて当該アクセス管理者が定める方法により作成される符号
三　当該利用権者等の署名を用いて当該アクセス管理者が定める方法により作成される符号

34 不正アクセス行為の禁止等に関する法律
（定義）
第２条
３　この法律において「アクセス制御機能」とは、特定電子計算機の特定利用を自動的に制御するために当該特定利用に係るアクセス管理者によって当該特定電子計算機又は当該特定電子計算機に電気通信回線を介して接続された他の特定電子計算機に付加されている機能であって、当該特定利用をしようとする者により当該機能を有する特定電子計算機に入力された符号が当該特定利用に係る識別符号（識別符号を用いて当該アクセス管理者の定める方法により作成される符号と当該識別符号の一部を組み合わせた符号を含む。次項第一号及び第二号において同じ。）であることを確認して、当該特定利用の制限の全部又は一部を解除するものをいう。

ドルータ（特定電子計算機）に対して送信する情報は、ドメインに対応する IP アドレスの回答を求めるコマンド（名前解決要求）や、ルータに保存されている管理画面のデータの取得を求めるコマンド(HTTP リクエスト)であるから、「識別符号」や「アクセス制御機能による特定利用の制限を免れる情報又は指令」には該当しない。

また、名前解決の結果や HTTP レスポンス（要求されたコンテンツの取得には認証が必要である旨の応答を含む。）を応答することについては、その特定利用（リクエストに対する応答）が識別符号を用いて利用権者を識別することにより制限されていない、すなわちアクセス制御機能により制限されているとは言えないため、当該ブロードバンドルータに対して名前解決要求や管理画面の取得の要求を行い、それに対して応答が返ってきたとしても、不正アクセス禁止法に定める「アクセス制御機能により制限されている特定利用をし得る状態にさせ」ているとは言えない。

したがって、本件対策は、不正アクセス禁止法第３条において禁止されている不正アクセス行為には該当しない。

なお、PPPoE 認証の情報を窃取され得る脆弱性を有するブロードバンドルータの調査に関して､HTTP リクエストの応答としての認証の要求に対して、ID・パスワードを推測して入力する場合には、不正アクセス行為に該当し得ることに留意する必要がある。

（３）通信の秘密との関係について（正当業務行為該当性）

①　目的の正当性

本件対策を実施する目的は、リフレクション攻撃に悪用され得る脆弱性を有するブロードバンドルータを利用した DNSAmp 攻撃等の DDoS 攻撃によって、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の遅延等の発生を防止するとともに、インターネット接続時の PPPoE 認証 ID･パスワードの不正利用を防止することにより、正規の利用者以外の者が正規の利用者になりすまし、不正に電気通信役務を享受することを防止[35]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等を図るためのものであり、その目的に資するため、当該ブロードバンドルータを特定するために調査し、当該ブロードバンドルータの利用者を特定することは、目的の正当性が認められると考えられる。

②　行為の必要性

リフレクション攻撃は、ブロードバンドルータの脆弱性を突いて行われ

[35] 前掲脚注 24 参照

るものであり[36]、各ブロードバンドルータにおける攻撃に悪用され得る脆弱性の修正が行われれば、リフレクション攻撃をより前段階から防ぐことが可能となることからすると、本件対策は、大量攻撃一般に対する有効な対処策となる。

また、外部から ISP の PPPoE 認証 ID・パスワードが窃取可能な状態となっているブロードバンドルータの脆弱性については、当該 ID・パスワードが窃取されることにより、不正アクセス等におけるなりすましのツールとして悪用され、個人情報漏えいや金銭窃取等の被害が発生するおそれがある。このように、当該ブロードバンドルータを使用する利用者は、インターネット接続時に使用する PPPoE 認証 ID・パスワードを窃取され得る危険にさらされており、これらの ID・パスワードがなりすましに悪用されるおそれがあることから、不正な電気通信役務の享受を防止するため、本件対策を行う必要がある。

この点、脆弱性を有するブロードバンドルータの製造事業者においても、脆弱性が発見された際に広く周知や注意喚起等を図るなど一定の対策[37]は行っているものの、インターネット利用者の多くは、自らサイバー攻撃による被害を受けたことを認識しない限り、ソフトウェアのアップデート等具体的な行動には移りにくいと考えられるため、インターネット等を通じた一般的な注意喚起ではブロードバンドルータにおける脆弱性の修正を実現することは困難である。

そこで、本件対策についてみると、調査して得られた当該ブロードバンドルータの IP アドレス及びタイムスタンプを基に、当該時刻において当該 IP アドレスをどの利用者に割り当てたかを確認し、該当利用者を割り出し、注意喚起をすることは、上記目的との関係で、行為の必要性を肯定できると考えられる。

③　手段の相当性

上記対策を講ずるに当たって侵害される通信の秘密は、ISP 等が行った名前解決要求又は HTTP リクエストに応じて自動的に返信された通信に係る送信元 IP アドレス及びタイムスタンプのみであり、確認した結果を本件対策以外の用途で利用しない場合には、手段の相当性も認められる。

---

36 リフレクション攻撃等に悪用され得る脆弱性を有するブロードバンドルータは、ネットワーク上に数十万台存在するのに対して、DNSAmp 攻撃等では、そのうち数百台を利用することで攻撃に必要な通信量を発生させ得るとの調査結果がある。

37 ブロードバンドルータ製造事業者のホームページ上において、機器のソフトウェアに脆弱性が発見された際、当該脆弱性を修正するためのソフトウェアを公開するなどしており、利用者に対して脆弱性の公表及びブロードバンドルータのソフトウェアの更新等を周知している。

④　まとめ

以上から、本件対策は、確認した結果を本件対策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４節　DNS の機能を悪用した DDoS 攻撃に用いられている名前解決要求に係る通信の遮断について

（１）対策の概要及び問題の所在

DNSAmp 攻撃やランダムサブドメイン攻撃を防止するため、ISP の網内の DNS サーバにおいて、ISP の自社 DNS サーバに過負荷を生ずることとなる名前解決要求[38]に係る通信を遮断することが考えられる。そのため、DNS サーバを通過するすべての名前解決要求に係る FQDN を常時確認して、上記攻撃に用いられている名前解決要求に係る通信を割り出し、これを遮断することが考えられる。

名前解決要求に係る FQDN は、通信の構成要素として通信の秘密の保護の対象であるから、これらを常時確認し、上記攻撃に用いられている名前解決要求に係る通信を検知し、遮断することは、通信の秘密の窃用等に該当する。もっとも、違法性阻却事由がある場合には、例外的に通信の秘密を侵すことが許容されることになるところ、本件対策は、正当業務行為の要件を満たすと考えることはできないか検討する。

（２）　正当業務行為該当性

①　目的の正当性

DNSAmp 攻撃やランダムサブドメイン攻撃を防止する措置は、ISP において、自社の DNS サーバに過負荷が生ずることにより、インターネットアクセスやメール送信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、目的の正当性を認めることができると考えられる。

②　行為の必要性

DNSAmp 攻撃は、前掲脚注 14 にある手法を用いて、攻撃先に増幅されたパケットを何度も送ることで、大量のトラヒックを発生させる攻撃であり、ランダムサブドメイン攻撃は、第１章（４）②にある手法を用いて、権威

[38] ランダムサブドメイン攻撃は、権威 DNS サーバを標的とすることが多く、攻撃の過程において ISP の DNS サーバに大量の処理を行わせるものであるため、本件対策では、ISP の自社 DNS サーバに過負荷を生ずることとなる名前解決要求に関する検討を行う。

DNS サーバ及び ISP の DNS サーバに大量の名前解決要求の処理を行わせる攻撃である。

このような DNS の仕組みを悪用した DDoS 攻撃への対処に関して、第一次とりまとめで整理したとおり、インターネット側からの動的 IP アドレス宛てであって、UDP53 番ポートへの名前解決要求に係る通信の遮断については一定の有効性が認められるが、固定 IP アドレス向けの攻撃通信も多く[39]、その点の対応を行う必要がある。

一方、ISP の DNS サーバでの対処に関して、DNSAmp 攻撃に使用される FQDN については、一定の攻撃に使われている FQDN を事前に把握することが可能な場合があり、ランダムサブドメイン攻撃に使用される FQDN については、機械的に生成された FQDN のパターンを攻撃の兆候として検知することにより、事前に把握することが可能な場合がある。これらの場合には、ISP の網内の DNS サーバにおいて、DNSAmp 攻撃に使用される FQDN 又はランダムサブドメイン攻撃に使用される FQDN の名前解決要求に係る通信を遮断することで DNSAmp 攻撃、ランダムサブドメイン攻撃を防止することができる。

以上から、これらの攻撃を防止するために、すべての名前解決要求の FQDN 情報を常時確認して攻撃に係る通信を遮断することは、上記目的との関係で、行為の必要性を肯定できると考えられる。

③　手段の相当性

本件対策を講ずるに当たって侵害される通信の秘密は、名前解決要求に係る FQDN 情報のみであり、これを機械的・自動的に確認して、攻撃に用いられる名前解決要求の FQDN を検知しブロックする限度であるから、その確認結果を本件対策以外の用途で利用しない場合であれば、通信の秘密の侵害の程度は相対的に低いということができる。また、通常の利用者が、ブロックの対象となる FQDN に対して名前解決要求を行うことは想定されない[40]ため、このような通信をブロックすることによる通常のインターネット利用への影響は考え難く、以上によれば、手段の相当性についても肯

---

[39] ある ISP において、2014 年 3 月に発生したリフレクション攻撃の際の IP アドレスを調査すると、攻撃に使われた IP アドレス総数 138 件の内訳は、企業の管理する IP アドレス(固定)49 件、大学が管理する IP アドレス(固定)23 件、個人等が管理する IP アドレス(固定)5 件、ISP が管理する IP アドレス(固定)24 件、ISP が管理する IP アドレス(動的)37 件であり、固定 IP アドレスが多数を占めている。

[40] DNSAmp 攻撃においては、攻撃に使用されている FQDN、ランダムサブドメイン攻撃においては、実在しない FQDN である必要があるため、正規のドメインであるホワイトリストとの照合や目視確認等をすることにより、正常な通信を遮断することがないリストを作成しておかなければならない。

定することができると考えられる。

④　まとめ

　以上から、本件対策は、確認した結果を本件対策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３章　おわりに

本研究会では、第一次とりまとめ以降に発生したサイバー攻撃の動向を踏まえた優先的に対応すべき課題とその対策について、通信の秘密の観点及び不正アクセス行為の観点から検討し、一定の整理を行った。

今後は、第一次とりまとめと同様に、ISP など電気通信事業者等において、本報告書における整理を踏まえ、大量通信ガイドラインの改定など具体的な取組が行われることを期待する。

また、サイバー攻撃についてはその手口や手法が絶えず高度化・巧妙化していることから、これらの情報通信技術等の変化に対応できるよう、今後とも官民の連携と適切な役割分担のもと、必要な検討を進めることで、サイバー攻撃に機動的に対応していくことが重要である。

なお、本研究会では IP 電話等の不正利用への対策についても一定の整理を行った。これを踏まえ、総務省において、平成 27 年７月７日に、通信事業者団体に向け、不正利用の実情を踏まえながら、適切な対応を適宜行うことを求める要請が行われており、各電気通信事業者等において、引き続き、適切な対応を行うとともに、必要に応じ、大量通信ガイドラインの改定等の取組が行われるものと期待する。

（参考資料）

○　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

・　構成員

（座長）	佐伯（さえき） 仁志（ひとし）	東京大学大学院法学政治学研究科教授
（座長代理）	宍戸（ししど） 常寿（じょうじ）	東京大学大学院法学政治学研究科教授
	木村（きむら） 孝（たかし）	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（きむら） たま代（たまよ）	主婦連合会
	小山（こやま） 覚（さとる）	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（なかお） 康二（こうじ）	国立研究開発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（ふじもと） 正代（まさよ）	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（もり） 亮二（りょうじ）	英知法律事務所　弁護士

・　ワーキンググループ構成員

（主査）	宍戸（ししど） 常寿（じょうじ）	東京大学大学院法学政治学研究科教授
（主査代理）	森（もり） 亮二（りょうじ）	英知法律事務所　弁護士
	衛藤（えとう） 将史（まさし）	国立研究開発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（きむら） 孝（たかし）	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（こやま） 覚（さとる）	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（さいとう） 衛（まもる）	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（まるはし） 透（とおる）	ニフティ株式会社　理事（法務・渉外担当）（兼） 法務部長
	村主（むらぬし） 亘（わたる）	ソフトバンク株式会社　お客様相談室

○　開催経緯

＜電気通信事業におけるサイバー攻撃への適正な対処のあり方に関する研究会＞

・　第４回（平成 27 年７月６日）

－　第二次とりまとめ（案）について

－　第三者による IP 電話等の不正利用への対策について

＜ワーキンググループ＞

・　第４回（平成 27 年６月１日）

－　「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」第３版の改定について

－　第一次とりまとめの内容の事業者における実装について

－　サイバーセキュリティ上の新たな課題について

・　第５回（平成 27 年６月 30 日）

－　第二次とりまとめ（案）について

－　第三者による IP 電話等の不正利用への対策について

＜第二次とりまとめ（案）に対する意見募集の実施＞

（平成 27 年７月 18 日～８月 10 日）