IP53Bと通信の秘密との関係について

平成26年11月20日

総務省　総合通信基盤局
電気通信事業部　消費者行政課
課長補佐　戸取謙治

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（IP53B関連箇所）

現状

■ 昨今、情報通信技術の発展とともに、DDoS攻撃やマルウェアの感染活動などサイバー攻撃が巧妙化・複雑化しており、社会経済活動におけるICTの急速な普及とも相まって、情報セキュリティへの脅威やリスクが深刻化している状況にある。

■ サイバー攻撃に対するこれまでの取組は次のとおり。

・ DDoS攻撃※1等の大量通信への対処

→ 電気通信役務の提供に影響を与える大量通信について、業界の自主基準としてガイドライン※2を策定し、遮断等を実施

※1 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
※2 「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」（平成19年「インターネットの安定的運用に関する協議会」策定）

課題

○ 新たなDDoS攻撃であるDNSAmp攻撃※の防止（IP53B）

※ 予め、公開DNSサーバに対して、ある名前解決の問い合わせがあった場合には大量のパケットを応答するような仕掛けをしておき、送信元IPアドレスを攻撃先IPアドレスに詐称して、当該公開DNSサーバに問い合わせを行い、攻撃先IPアドレスに対して大量のパケットを送信するDDoS攻撃

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

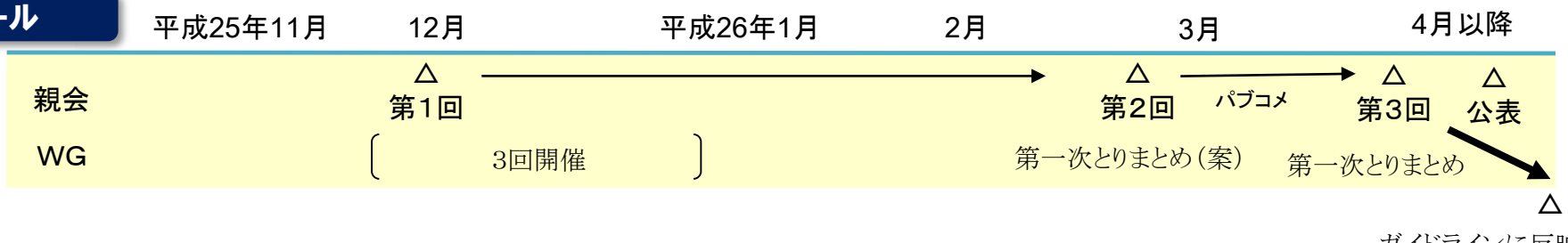
＜本会合＞

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

＜WG＞

宍戸　常寿	東京大学大学院法学政治学研究科教授
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
森　　亮二	弁護士
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

スケジュール



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」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。**

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。

通信の秘密の侵害の該当性について

1.「通信の秘密」該当性

「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。

※ 東京地裁判決H14.4.30は、「電気通信事業法第104条の「通信の秘密」には、通信の内容のほか、通信当事者の住所・氏名・電話番号、発受信場所、通信の日時・時間・回数なども含まれると解する。」と判示している。

2.「侵害行為」該当性

通信の秘密を侵害する行為は、以下の3類型に大別されている。

- ○ **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り得る状態に置くこと」
- ○ **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」

3. 通信の秘密の侵害に該当しない場合

○ 通信当事者の同意がある場合、「通信当事者の意思に反しない利用」であるため侵害に当たらない。

注 同意の取り方について・・・約款等による事前の包括的合意については、①約款の性質になじまない、②同意の対象が不明確、との理由により、一般的には有効な同意と解されていない。（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・第二次提言から抜粋）

通信の秘密の侵害が許容される場合

4. 通信の秘密の侵害が許容される場合： 違法性阻却事由がある場合

(1) 正当防衛、緊急避難に該当する場合

正当防衛の要件（急迫性等）、緊急避難の要件（危難の現在性等）を満たす場合。典型的には、通信施設に対する攻撃に対応したり、人の生命身体に対する危険を避けたりするために通信の秘密を侵すことが必要な場合等が挙げられる。

例：人命救助のための基地局に係る位置情報の救助機関への提供

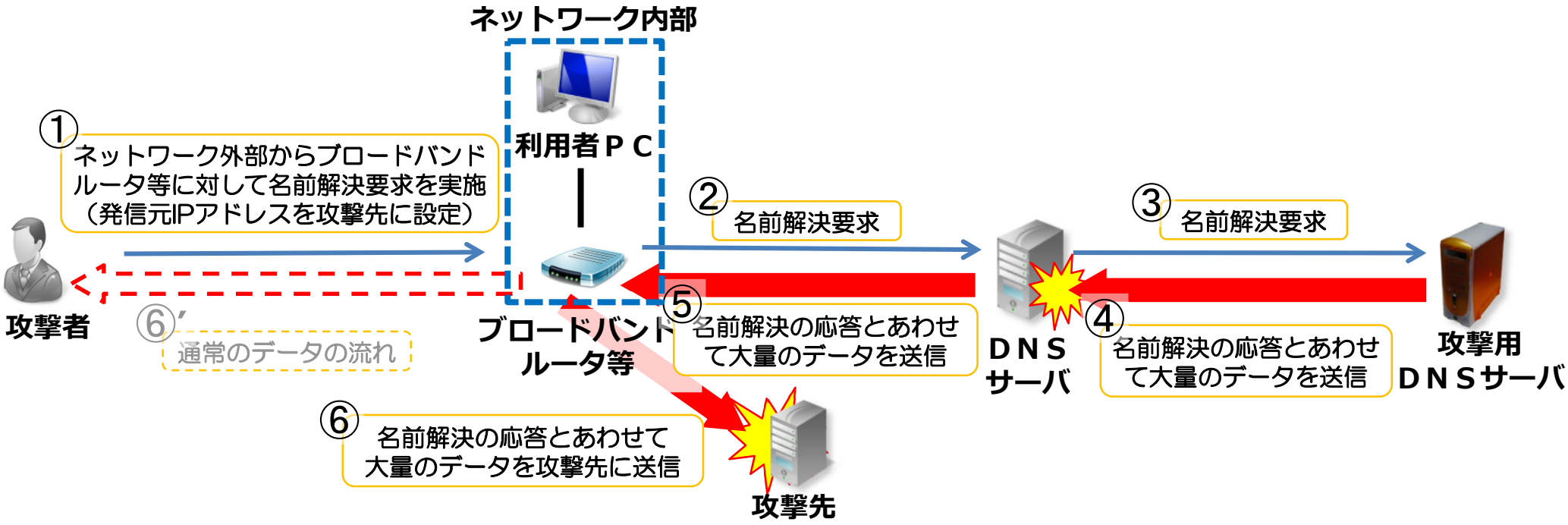
(2) 正当業務行為に該当する場合

電気通信事業者としての業務を遂行するために必要な場合であって、目的の正当性、行為の必要性、手段の相当性を満たすことが必要。典型的には、課金やシステム整備のために必要な場合において、最低限度で通信の秘密を侵す行為は、当該条件を満たすと考えられる。

例：帯域制御（特定のアプリケーションによる通信が過度に帯域を圧迫している場合、当該アプリケーションによる通信量を制限）

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）
DNSAmp攻撃の防止について

■ 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(IP53B)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（平成26年4月4日公表）
DNSAmp攻撃の防止について

論点と整理

新たなDDoS攻撃であるDNSAmp攻撃の防止

（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（IP53B）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

（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」後の状況について

【サイバーセキュリティ2014（平成26年7月10日情報セキュリティ政策会議決定）抜粋】

1「強靱な」サイバー空間の構築

④サイバー空間の衛生

（ヌ）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、「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」のとりまとめを踏まえ、ISPなど電気通信事業者等において、関係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支援するとともに、今後も必要に応じ、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。

【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（平成26年7月22日公表）抜粋】

第2章　各論

第5条　大量通信等について

（カ）【考え方】

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