資料４

ICTサービス安心・安全研究会
個人情報・利用者情報等の取扱いに関するWG（第2回）

ISPにおける個人情報の取扱いの現状等

2015年2月5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） 会長補佐、行政法律部会長
ニフティ株式会社　経営戦略室　経営戦略推進部　担当部長
木村　孝

ISPにおける個人情報の取扱

- 第三者からの個人情報取得
- 社内の安全管理措置
- 委託先の管理

第三者からの個人情報取得

- 名簿業者からの個人情報の取得は、ISPではあまり例はないと思います。
- 販売代理店（取次代理店を含む）にISPが拡販を委託するに際し、販売代理店が自社独自のリストを用いて拡販活動を行うことはあります。
- FTTHなどのアクセス網事業者（ないしはその代理店、以下アクセス網事業者等）が、自社サービスの販売にあたって、ISPのサービスをセットで販売（ないしは取次）した場合に、アクセス網事業者等から、ISPに申込者の情報を提供してもらいます。
- ただし、これはサービスの利用にあたって必要なものとして同意を得ております。

社内の安全管理措置

- 多くのISPでは、安全管理措置として個人データへのアクセスへの制限、取扱場所や端末の隔離、スマートフォン、USBメモリなど機器の接続の制限、入退室記録の保存、カメラによる記録などは数年前から既に実施済みと思います。
- プライバシーマーク*を取得しているISPの場合、プライバシーマークに規定する安全管理措置が適用されます。
- 決済にクレジットカードを利用するISPは、PCI DSS**という基準の認定を求められています。
- 情報セキュリティマネジメントシステム(ISMS)の国際規格であるISO/IEC 27001の取得しているISPでは、個人情報を含めた情報セキュリティ全般についても厳しく管理しています。
- これらの基準では、個人情報を取り扱うシステムについて、サーバーや端末のログの定期的取得など、多数に及ぶ項目を定めており、この認定取得の結果、かなりの安全管理措置がとられております。
- 現在の電気通信事業における個人情報保護に関するガイドライン及び「ガイドラインの共通化の考え方について」(前回資料6)にある項目は既にほぼカバーされていると思われます。

*プライバシーマーク制度は、日本工業規格「JIS Q 15001個人情報保護マネジメントシステム－要求事項」に適合して、個人情報について適切な保護措置を講ずる体制を整備している事業者等を認定して、その旨を示すプライバシーマークを付与し、事業活動に関してプライバシーマークの使用を認める制度です。(JIPDECホームページより)

**PCI DSSは加盟店やサービスプロバイダにおいて、クレジットカード会員データを安全に取り扱う事を目的として策定された、クレジットカード業界のセキュリティ基準です。Payment Card Industry Data Security Standardsの頭文字をとったもので、国際カードブランド5社(American Express、Discover、JCB、MasterCard、VISA)が共同で設立したPCI SSC(Payment Card Industry Security Standards Council)によって運用、管理されています。(日本カード情報セキュリティ協議会のホームページより)

委託先の管理

- ISPはコンタクトセンター業務、出張サポート業務、印刷物発送業務などで、委託先に個人情報の取り扱いを委託する場合があります。
- このような委託先に対しては、個人情報保護に関する運営規定、管理規定を定め、定期的な監査を実施するなどして管理しております。また再委託、再々委託につきましても、委託と同様、再委託の相手方、業務内容、個人データの取扱等について、ISPのセキュリティ要求事項を遵守するべく、事前報告又は承認、定期的監査などの体制がとられています。
- 管理規定にはセンターの運営、管理、委託先スタッフの管理、教育、業務に必要な情報の取得、運用等の関連業務について詳細に規定しています。
- 委託先の個人情報安全管理措置のチェックリストには、機器の設置、管理、移動、メモリーの管理、保管、印刷の記録の保管、端末のパスワード管理、部屋への入退室管理（記録）など数十項目があります。
- 現在の電気通信事業における個人情報保護に関するガイドライン及び「ガイドラインの共通化の考え方について」（前回資料6）にある項目は既にほぼカバーされていると思われます。

ISPにおける通信履歴（通信ログ）の取扱い

- そもそも通信履歴とは？
- 接続履歴の用途
- ISPにおける接続履歴の保存、利用状況
- ISPにおける接続履歴保存の課題

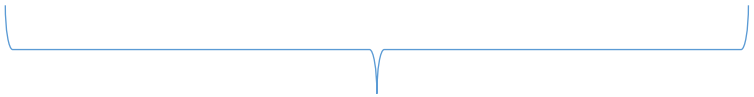
そもそも通信履歴とは？

- 通信事業者において、利用者の通信の履歴を記録するものです。
  - 電気通信事業における個人情報保護に関するガイドライン第23条では、以下のように定義されています。
  - 電気通信事業者は、通信履歴（利用者が電気通信を利用した日時、当該通信の相手方その他の利用者の通信に係る情報であって通信内容以外のものをいう。以下同じ。）については、課金、料金請求、苦情対応、不正利用の防止その他の業務の遂行上必要な場合に限り、記録することができる。
- 通信履歴には、接続履歴（接続認証ログ）とサーバーの利用ログ*があります。
- 以下、接続履歴について説明します。
- インターネット以外では、電話、IP電話の通話記録などがあります。
- 接続履歴内容は利用者IDと割り当てたIPアドレス、及び当該IPアドレスの利用開始日時・利用終了日時（タイムスタンプ）です。
- 通常はハードディスクの中に電子データとして記録されるが、画面に表示したり、紙として出力することも可能です。

*例としてはメールの送受信の記録やWebのアクセス履歴など

個々の接続認証ログの内容

ユーザーID	IPアドレス	認証結果	利用開始	利用終了	その他
ABC01234	123.123.123.123	OK	2014/08/31 11:52:00	2014/08/31 12:01:05	
CDE02345					



この部分をタイムスタンプといいます。

通常は利用開始の時刻順に記録が追加されていきます。
これは、実際のログを加工して見やすくしたイメージです。

IPアドレス

- インターネットの通信においては、端末（ホスト、サーバー）に割り当てられるIPアドレスを用いて、発信元と宛先の識別を行います。
- IPアドレスは、ISPにおいて通信開始時（認証成功時）に、利用者側の端末に割り当てられます。
- 一般利用者に割り当てられるIPアドレスは、動的IPアドレスといい、原則として毎回異なるIPアドレスとなります。
- 利用者に常に同じIPアドレスを割り当てる、固定IPアドレスという仕組みもありますが、追加料金がかかるので、通常は法人利用者やサーバー側でのみ用いられます。
- インターネット側においては、（通信の当事者である受信者側からは、）発信者の情報はIPアドレスしか分かりません。
- 一般利用者のIPアドレスは毎回異なるため、IPアドレスから実際の利用者を調べるためには、ISPの接続履歴を検索し、その時間帯に当該IPアドレスを割り当てられていたものを検索します。

接続履歴の用途

1. 課金
   - 接続認証の結果から通信開始時間と終了時間を記録し、そこから通信時間を算出し、従量制時間課金のデータとします。
   - 移動体通信で通信量（パケット）に上限値（例：月間2GB,4GBなど）がある場合には、毎回の通信量を記録し、累積結果が上限値を超えたときに制限を行うためのデータとします。
2. ユーザーサポート
   - 利用者に対し、自己の利用状況をインターネット上で参照できるよう提供します。
   - 利用者の身に覚えのない時間帯に利用がされていたという問い合わせがあった場合、調査します。
   - 利用者から、インターネットが利用できなかった、という苦情があったときに、何らかの問題などがあって当該利用者が実際できていたかどうか、接続実績の確認をとるデータとなることもあります。
   - 利用者による解約手続きが完了しておらず、利用者が解約したつもりでも月額課金がされ続けている場合があります。かなり経ってからそのことに気が付いた利用者から、利用していないことを理由に返金を求められた場合に、確認を行う場合もあります。
3. 設備管理
   - 年間の季節ごとの利用状況を把握し、適正な設備管理を行うために利用する場合もあります。

接続履歴の用途（2）

1. 情報セキュリティの確保
   - 不正アクセスや、不正アクセス目的で接続アカウントとパスワードの取得を試みるサイバー攻撃が行われた場合、大量の認証エラーが発生することもある。接続履歴にはエラーも記録されるので、それによりそのような攻撃を発見、確認します。
   - 端末がウイルスに感染した利用者に対し、ISP側から注意喚起を行うために接続履歴から利用者を調べます。（次ページ参照）
   - 新しく発見された脆弱性に基づく攻撃が過去にあったかどうか過去にさかのぼっての調査します。
2. 迷惑行為(Abuse*)の苦情対応
   - 迷惑メールを受信した被害者からの申告を受け、送信者に対し警告や利用停止などの措置をとるために利用者を特定するときにISP側で接続履歴を用います。（送信に使われたメールアドレスは通常詐称されているため）
   - ポートスキャン**などの苦情を受けた場合も同様です。
3. ファイル共有を悪用した著作権侵害対策
   - 著作権団体（権利者）からの申告に基づき、著作権を侵害した利用者に対し警告を行うに際し、権利者から連絡されたIPアドレスから利用者を特定するためにISP側で接続履歴を用います。

*RFC2142においては、「公共における不適当なふるまい」と定義されています。
**インターネット上のホストの開いている通信ポートを探す、侵入などの予備的行為をさします。

接続履歴の用途（3）ウイルス感染者への警告

1. ACTIVE*の場合
   - **ACTIVEのマルウェア駆除活動に際し、感染ユーザーの特定のために、ISPにおいて接続履歴を参照します。**
2. ネットバンキングに関わる不正アクセスを行う国際的なボットネットテイクダウン対応
   - **2014年夏に行った「インターネットバンキングに係るマルウェアへの感染者に対する注意喚起の実施」**などがあります。**
3. フィッシングサイトや不正中継サーバーとなっている場合
   - **ウイルスに感染した結果、利用者が意図せず、ISP利用者の端末がフィッシングサイトや不正中継サーバーとなっていることがあります。そのような場合にも当該ユーザーの特定のために接続履歴を参照します。**

*総務省は2013年10月に、複数のインターネット・サービス・プロバイダ（ISP）事業者やセキュリティベンダー等の事業者と連携し、国内のインターネット利用者を対象に、マルウェアの感染防止と駆除の取組を行う官民連携プロジェクトを開始することを発表しました。このプロジェクトがACTIVE（Advanced Cyber Threats response InitiatiVE）です。詳細は https://www.active.go.jp/

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

接続履歴の用途（4）法律に基づく対応の場合

1. プロバイダ責任制限法に基づく発信者情報開示の場合
   - プロバイダ責任制限法第4条に基づき、接続プロバイダが発信者を割り出すためには、権利を侵害されたとする申出者からIPアドレスとタイムスタンプの情報を得て、接続履歴からその時間に当該IPアドレスを利用していた利用者を検索します。
2. 刑事訴訟法等に基づく令状に対応する場合
   - 刑事訴訟法等に基づき発せられた差押令状により、同様に指定されたIPアドレスを当該タイムスタンプ時に用いていた利用者を検索します。

接続履歴の用途(5)その他の場合

1. インターネット上における自殺予告の書き込みに際し、人命保護の観点から緊急に対応する必要がある場合
   - 掲示板の書き込みを見た人からの通報を受け、警察の依頼でISPが接続履歴から利用者を特定し、警察官が利用者をISP登録住所に訪問することで自殺を防止できた事例が多数存在します。
   - インターネット上の自殺予告事案への対応に関するガイドライン (2005.10)で規定しています。
2. 障害対応
   - 障害の影響範囲の推定のために、過去の同じ時期にログインしていた利用者数を調べたりします。インターネット電話などの場合は相互接続で相手の呼との照合を行います。

ISPにおける接続履歴の保存、利用状況

- JAIPA加盟のISPにおいては、接続履歴を保存していないところはない模様です。
- 保存期間は各社により異なります。接続履歴は通信の秘密に当たるため、各社業務上必要最小限の保存期間を設定しています。例：利用後　月単位で、2ヶ月間、3ヶ月間、6ヶ月間、1年程度など。
- 典型的な例は利用月から3ヶ月間だが、6ヶ月保存している社も多くあります。
- 理由としては、利用者からの問い合わせに対応するなどのためです。
- 課金以外の利用にあたっては、その都度必要な部分のみを抽出して利用します。
- 保存期間については、各社ばらばらで判断するより、ある程度の目安があったほうが良いと考えます。

ISPにおける接続履歴保存の課題

- 接続履歴の保存装置（ストレージ）は高速かつ高信頼性なものが求められるため高価です。
- 接続履歴の保存自体よりも、特定の利用に関わる記録を抽出するためのソフトウェア開発や抽出自体の人的作業の負担が大きいと言われています。（接続履歴は、全利用者のものがひとつのデータにまとめてあるため、データサイズが非常に大きく、専用のソフトウェアがないと、抽出に時間がかかります。例：2日間とか）