

2013年8月20日

## OCN 認証 ID・パスワードの不正利用防止に向けた セキュリティ上の脆弱性があるブロードバンドルータの 利用調査および対策の実施について

NTT コミュニケーションズ（略称：NTT Com）は、インターネット接続サービス「OCN」において、ご契約者以外の第三者によるインターネット接続用の認証 ID・パスワード<sup>\*1</sup>の不正利用を防止するため、2013年8月20日から2013年10月31日までの間、OCN をご利用のお客さまを対象に、セキュリティ上の脆弱性が判明している特定のブロードバンドルータをご利用されている方の調査を実施します。本調査により当該機器のセキュリティ脆弱性が確認されたお客さまには、NTT Com より個別にご連絡し、ファームウェアの更新と認証パスワードの変更をお願いしていきます。

### 1. 背景

NTT Com の OCN においては、2013年6月26日に発表したとおり、ご契約者以外の第三者が、インターネット接続時に必要な OCN 認証 ID・パスワードを不正に利用してアクセスし、認証パスワードを変更する事象が発生しました。この原因について調査した結果、ロジテック株式会社より過去に販売された無線 LAN ブロードバンドルータの特定機器<sup>\*2</sup>におけるセキュリティ上の脆弱性により、機器に設定された OCN の認証 ID・パスワードを外部から取得された可能性が高いことが判明しました。

NTT Com は、これまで OCN をご利用のお客さまに対して認証パスワードの定期的な変更とブロードバンドルータのファームウェア更新をお願いしてきましたが、このような状況を踏まえ、不正利用防止を徹底するため、OCN をご利用のお客さまを対象にセキュリティ上の脆弱性が判明している該当のブロードバンドルータのご利用に関する調査を実施するとともに、当該機器の利用が確認されたお客さまには不正利用防止に向けた対応を個別にお願いすることとしました。

### 2. 調査および対策の概要

NTT Com は、OCN 光・ADSL をご利用のお客さまを対象に、セキュリティ上の脆弱性により認証 ID・パスワードが外部から取得される可能性があるブロードバンドルータの利用状況について調査<sup>\*3</sup>を実施します。セキュリティ上の脆弱性があるブロードバンドルータを利用されている可能性のあるお客さまには、個別にご連絡し、当該機器のファームウェア更新と認証パスワードの変更をお願いしていきます。

これまで、お客さまがご利用の宅内機器のセキュリティ上の脆弱性に対して調査を行い、お客さま個別に対策措置を取ることができておりませんでした。今回、お客さまのより安心安全なインターネット利用のため、インターネットサービスプロバイダー（ISP）としては国内で初めて本対策を実施することとしました。

### 3. 調査期間

2013年8月20日（火）～2013年10月31日（木）

#### 4. お客さまへのお願い

セキュリティ上の脆弱性が確認されたブロードバンドルータをご利用されているお客さまに対しては、2013年8月以降、NTT Com より順次ご連絡しますので、ご案内に従って認証パスワードの変更と当該機器のファームウェア更新を実施いただきますようご協力をお願いいたします。また、NTT Com からの連絡を待たずに、ご利用の機器の脆弱性を確認し対策を実施されたいお客さまにつきましては、以下のロジテック社ホームページよりご確認をいただき当該機器のファームウェア更新を実施いただきますようお願いいたします。

※ファームウェアの更新方法（ロジテック社ホームページ）

<http://www.logitec.co.jp/info/2012/0516.html>

<本件に関するお客さまからのお問い合わせ先>

インターネットセキュリティ担当

電話番号：0570-783-609

受付時間：午前10時-午後6時

※年末年始除く

- \*1：OCNのインターネット接続時に必要なID・パスワードであり、通常、お客さま宅内に設置したブロードバンドルータに設定して利用します。本認証ID・パスワードはOCN ID（メールアドレスを利用して各種WebサービスにログインできるID・パスワード）とは異なるため、2013年7月24日に発表している「OCN IDのサーバーへの不正アクセス」の事象と本件は関係ありません。
- \*2：ロジテック製300Mbps無線LANブロードバンドルータ(LAN-W300N/R、LAN-W300N/RS、LAN-W300N/RU2)。
- \*3：インターネット側から簡易な通信コマンドをブロードバンドルータに送信し、その応答からセキュリティ上の脆弱性があるかを確認する調査です。お客さまがご利用のインターネット通信に負荷をかけたり、お客さまのブロードバンドルータにログインすることはありません。また、OCN認証ID・パスワードを見ることも一切ありません。なお、本調査は、国内の主要なISPにより構成され、情報セキュリティインシデント情報を収集・分析し、業界内で共有することを目的としている「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」と協力して行います。