脆弱性保有ブロードバンドルータ状況調査

2013年11月28日

Telecom-ISAC-Japan　ステアリングコミッティ運営委員
ソフトバンクBB株式会社
松隈　純

Telecom-ISAC Japan
Telecom Information Sharing and Analysis Center Japan

ブロードバンドルータに深刻な脆弱性

Telecom-ISAC Japan
Telecom Information Sharing and Analysis Center Japan

Telecom-ISAC Japan 2012/07/30
2012/09/24 更新

【注意喚起】ロジテック製ルータの脆弱性、
および、利用者が行うべき必要対策

情報通信基盤の安心・安全を確保するために活動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(所在地:東京都港区、会長:飯塚久夫(NECビッグローブ株式会社)、以下、Telecom-ISAC Japan)は、インターネットの安定運用に関わる事象の検出および対処に取り組んでおります。

I. 概要

ロジテック株式会社(以下、ロジテック)より、「ロジテック 300Mbps無線LANブロードバンドルータ」の一部において、セキュリティに脆弱性があることが判明」したと5月16日に、そして、「セキュリティを強化したファームウェア」を公開したと5月24日にアナウンスがありました。

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) に関するお詫びとお願い
http://www.logitec.co.jp/info/2012/0516.html?lnk_id=out_oshirase_20120516_2_2

「この脆弱性により、インターネット接続に必要な「PPPoEの認証ID」および「PPPoEの認証パスワード」が外部より取得される可能性」があることから、インターネットの安全な利用に及ぼす影響の大きさを鑑みて、Telecom-ISAC Japanでは、この脆弱性に関する注意喚起をいたします。該当ルータの利用者は以下の対策を全て実行することを強く推奨いたします。

1. ファームウェアのバージョンアップ
2. ルータ管理画面のパスワード変更
3. PPPoEの認証パスワード変更
4. ルータの再設定

ユーザ自身による対策が必要

自社製品なら何とかなるんだけど・・・

対策促進のために・・・

脆弱性を放置したままの
該当機器接続ユーザを特定し注意喚起

「通信の秘密」に抵触

対策促進のために・・・

脆弱性を放置したままの

該当機器接続元への注意喚起

脆弱性を悪用した
インシデントが発生！！

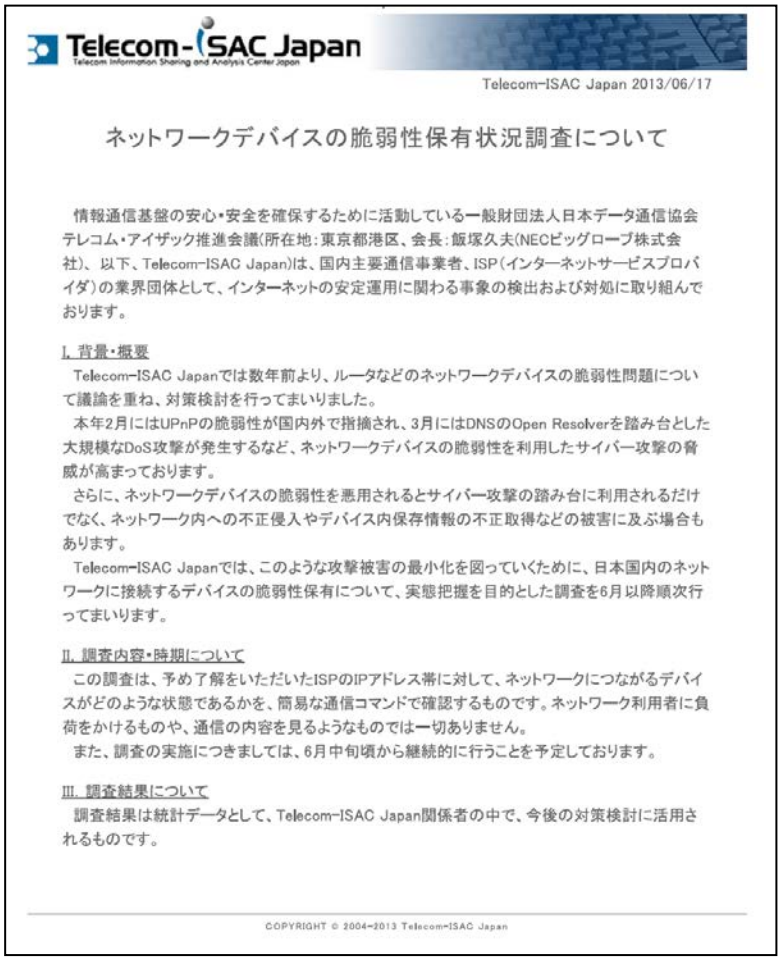
「通信の秘密」に抵触

インシデントが発生していることを踏まえ・・・

脆弱性を放置したままの
該当機器接続ユーザを特定し注意喚起

ユーザ保護による通信の秘密抵触に対しての阻却事由により可能（全ISPに適用）

Telecom-ISAC-Japanが調査実施
該当機器利用者へのアクションは各社判断



Telecom-ISAC Japan
Telecom Information Sharing and Analysis Center Japan

Telecom-ISAC Japan 2013/06/17

ネットワークデバイスの脆弱性保有状況調査について

情報通信基盤の安心・安全を確保するために活動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(所在地:東京都港区、会長:飯塚久夫(NECビッグローブ株式会社)、以下、Telecom-ISAC Japan)は、国内主要通信事業者、ISP(インターネットサービスプロバイダ)の業界団体として、インターネットの安定運用に関わる事象の検出および対処に取り組んでおります。

I. 背景・概要

Telecom-ISAC Japanでは数年前より、ルータなどのネットワークデバイスの脆弱性問題について議論を重ね、対策検討を行ってまいりました。

本年2月にはUPnPの脆弱性が国内外で指摘され、3月にはDNSのOpen Resolverを踏み台とした大規模なDoS攻撃が発生するなど、ネットワークデバイスの脆弱性を利用したサイバー攻撃の脅威が高まっております。

さらに、ネットワークデバイスの脆弱性を悪用されるとサイバー攻撃の踏み台に利用されるだけでなく、ネットワーク内への不正侵入やデバイス内保存情報の不正取得などの被害に及ぶ場合もあります。

Telecom-ISAC Japanでは、このような攻撃被害の最小化を図っていくために、日本国内のネットワークに接続するデバイスの脆弱性保有について、実態把握を目的とした調査を6月以降順次行ってまいります。

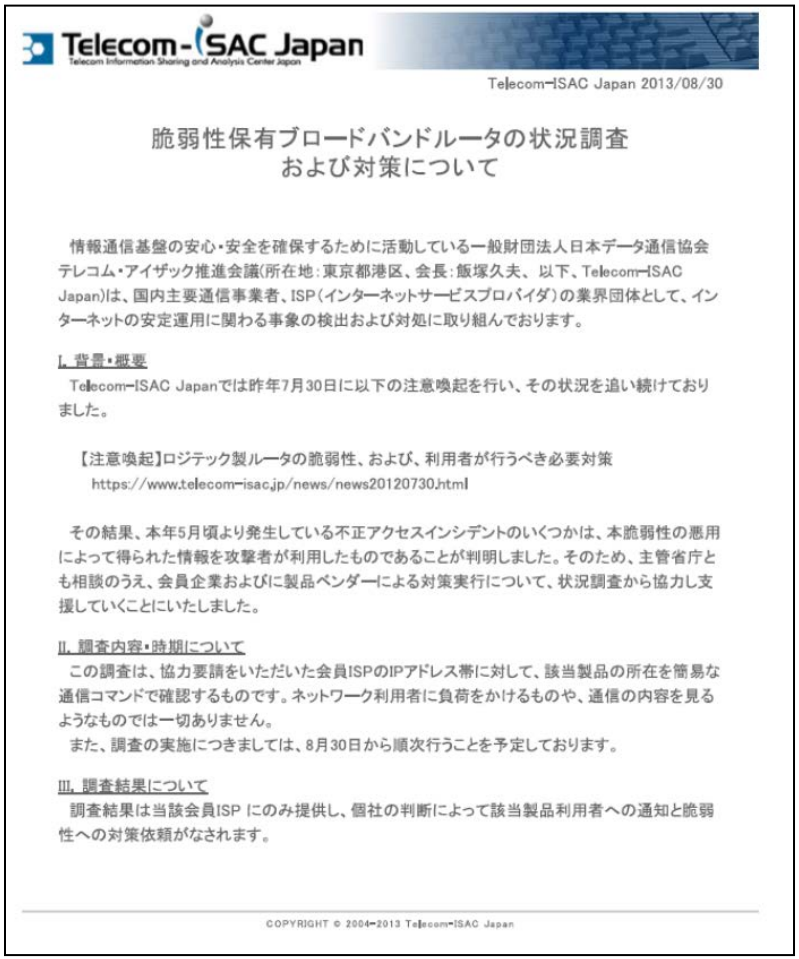
II. 調査内容・時期について

この調査は、予め了解をいただいたISPのIPアドレス帯に対して、ネットワークにつながるデバイスがどのような状態であるかを、簡易な通信コマンドで確認するものです。ネットワーク利用者に負荷をかけるものや、通信の内容を見るようなものではー切ありません。

また、調査の実施につきましては、6月中旬頃から継続的に行うことを予定しております。

III. 調査結果について

調査結果は統計データとして、Telecom-ISAC Japan関係者の中で、今後の対策検討に活用されるものです。



Telecom-ISAC Japan
Telecom Information Sharing and Analysis Center Japan

Telecom-ISAC Japan 2013/08/30

脆弱性保有ブロードバンドルータの状況調査
および対策について

情報通信基盤の安心・安全を確保するために活動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(所在地:東京都港区、会長:飯塚久夫、以下、Telecom-ISAC Japan)は、国内主要通信事業者、ISP(インターネットサービスプロバイダ)の業界団体として、インターネットの安定運用に関わる事象の検出および対処に取り組んでおります。

I. 背景・概要

Telecom-ISAC Japanでは昨年7月30日に以下の注意喚起を行い、その状況を追い続けておりました。

【注意喚起】ロジテック製ルータの脆弱性、および、利用者が行うべき必要対策
https://www.telecom-isac.jp/news/news20120730.html

その結果、本年5月頃より発生している不正アクセスインシデントのいくつかは、本脆弱性の悪用によって得られた情報を攻撃者が利用したものであることが判明しました。そのため、主管省庁とも相談のうえ、会員企業およびに製品ベンダーによる対策実行について、状況調査から協力し支援していくことにいたしました。

II. 調査内容・時期について

この調査は、協力要請をいただいた会員ISPのIPアドレス帯に対して、該当製品の所在を簡易な通信コマンドで確認するものです。ネットワーク利用者に負荷をかけるものや、通信の内容を見るようなものではー切ありません。

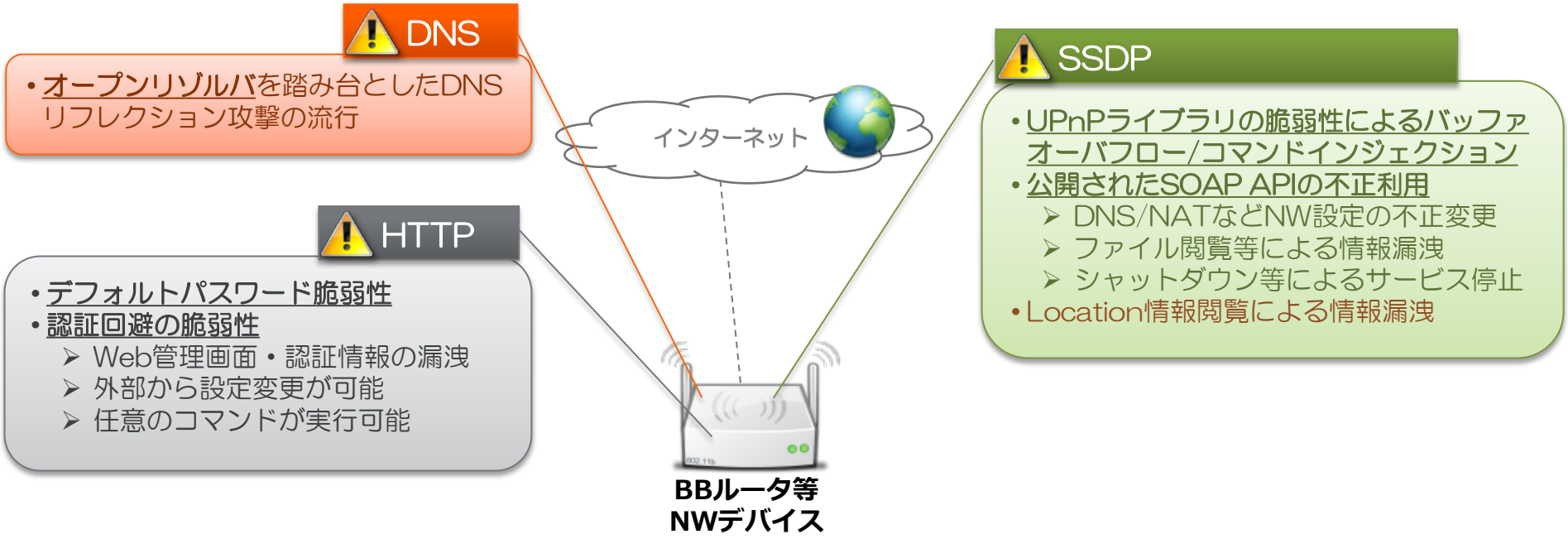
また、調査の実施につきましては、8月30日から順次行うことを予定しております。

III. 調査結果について

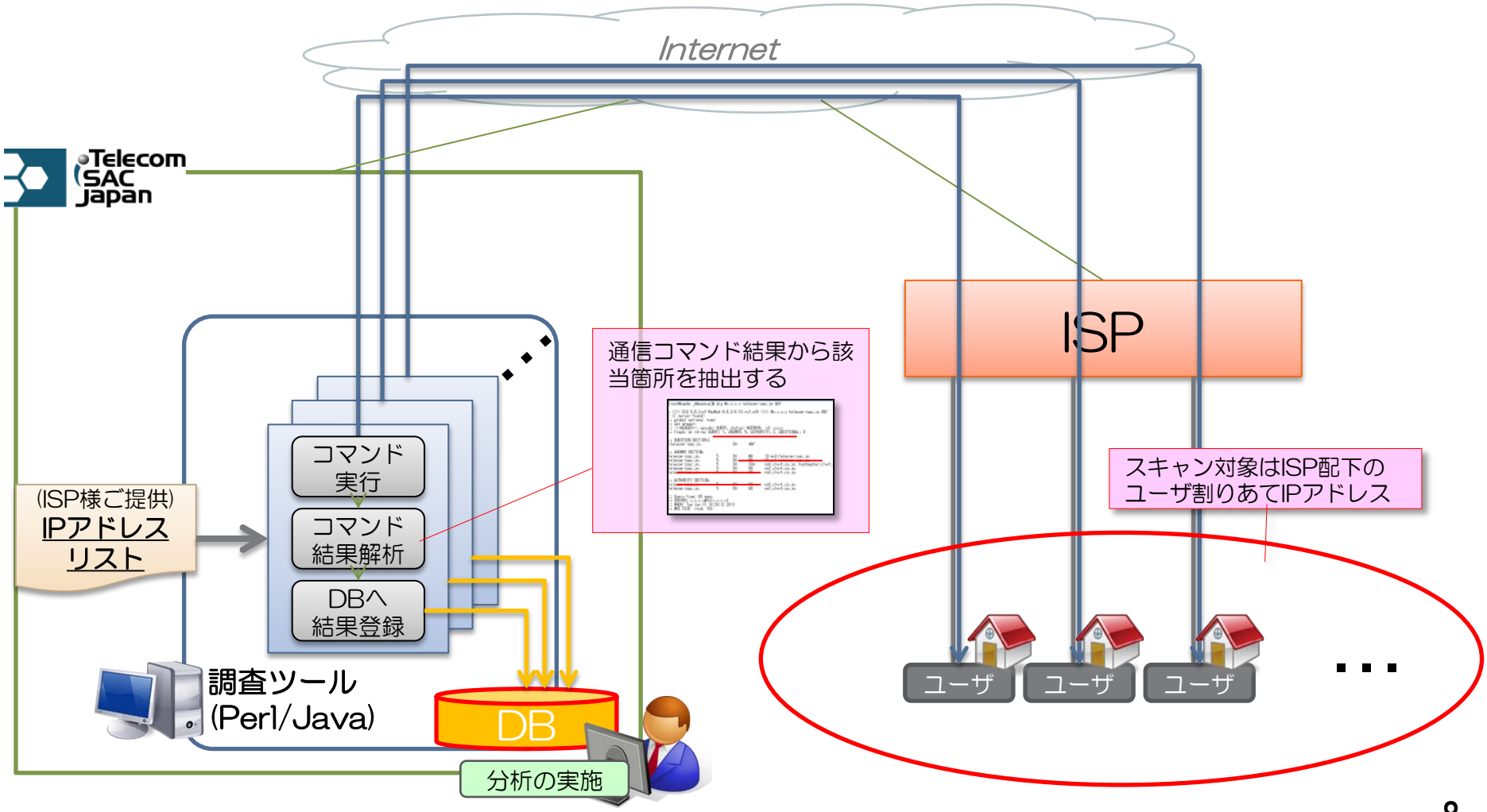
調査結果は当該会員ISP にのみ提供し、個社の判断によって該当製品利用者への通知と脆弱性への対策依頼がなされます。

調査対象プロトコル

セキュリティ情勢、サイバー攻撃状況等を鑑み HTTP、DNS、SSDPを選定



調査ネットワーク構成概要



今後について・・・

機器脆弱性による危険性は
今後も存在する

実態把握ができる仕組み
利用者への注意を促す仕組み

End of slides