BBルータの脆弱性とサイバー攻撃の関係
～L社製BBルータ脆弱性事例を鑑み～
＋
VAWTRAK無効化作戦とISPs

2015/07/09

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
脆弱性保有ネットワークディバイス調査WG
西部 喜康 (NTTコミュニケーションズ)

Telecom-ISAC Japan
Telecom Information Sharing and Analysis Center Japan

BBルータの脆弱性とサイバー攻撃の関係
～L社製BBルータ脆弱性事例を鑑み～

本件、そこかしこで・・・・・
「西部君のライフワークだから」とか言われてる、
Mr.ルータ脆弱性西部が語ります(*^_^*)

Telecom-ISAC Japan
Telecom Information Sharing and Analysis Center Japan

概要

L社より、無線LANブロードバンドルータの一部にセキュリティ脆弱性があり、これにより利用者が設定したPPPoEの認証IDおよびパスワードが外部より取得される可能性があると、2012/5/16に情報公開がされ、5/24には、この脆弱性を改修したファームウェアが公開されました。

この脆弱性を悪用されれば、利用者のBBルータに対して外部からのアクセスが行われ、利用者のインターネット接続ID/パスワードが詐取されそれに起因するサイバー攻撃が行われる①、BBルータの設定が変更され利用者への不利益②が生じる恐れが懸念されました。

※ ①-1) 詐取したインターネット接続ID/パスワードを利用したインターネット接続（成りすましによる身元を隠ぺいした状態)上での各種サイバー攻撃
-2) 詐取したインターネット接続ID/パスワードを利用した詐取元利用者の契約情報の変更による金銭的被害の発生（追加メールアカウントの購入やVoIPオプションサービスの購入）
②-1) 通信の盗聴
-2) フィッシングサイトへの誘導

2012/05～06月には、悪意の第三者による大規模な国内インターネット上でのスキャン行為が実施され、本脆弱性を持つBBルータが特定され多くの利用者のインターネット接続ID/パスワードが詐取されたと判断できる事象が各ISPで観測された。

また、2013/03～04月以降、インターネット上で頻発している会員サービスサイトへのリスト型不正アクセス事案におけるAbuse対応において、その多くが①-1)による成りすまし接続が、その攻撃インフラとして使われていることが判明しているとともに、①-2)による利用者への被害の発生が判明している。

その後、本件に関わるサイバー攻撃、特に①-1)攻撃に基づく犯罪捜査が警察組織内で行われ、2014/02/13 および2014/11/19に、中継プロキシーサーバ事業者およびその一部構成員の一斉摘発が行われた。

2015/06/02 遂にL社により全国5紙上での社告(対ユーザ謝罪＆注意喚起)が掲載される。

悪用されたL社製ルータの脆弱性

保有していた3点の脆弱性を利用された攻撃によってPPPoE認証情報が詐取された

- L社製ルータ問題では、多くのNWデバイスに搭載されているWeb管理画面のID/パスワードが周知のもの、もしくは容易に推測可能であることを利用して、悪意のユーザがNWデバイス管理画面へ不正アクセスが行われた

■問題該当機種

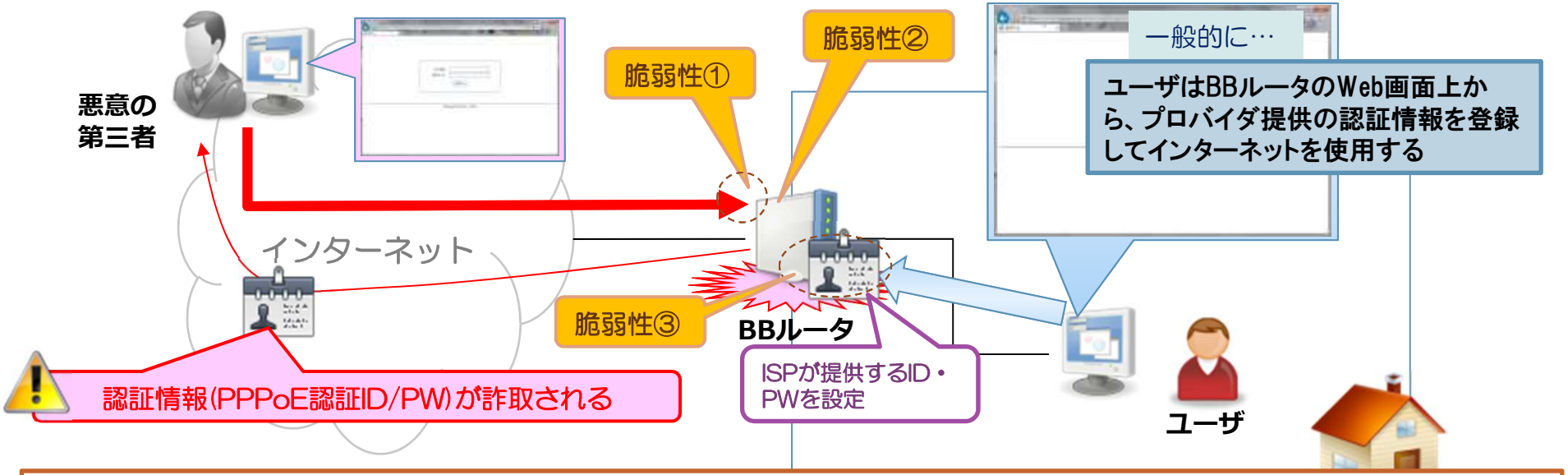
L社製「300Mbps無線LANブロードバンドルータ」 3機種

LAN-W300N/R
（2009年8月発売）

LAN-W300N/RS
（ 2011年7月発売）

LAN-W300N/RU2
（ 2010年2月発売）

3機種とも、
シリアルナンバーの末尾「B」
ファームウェアバージョン 2.17



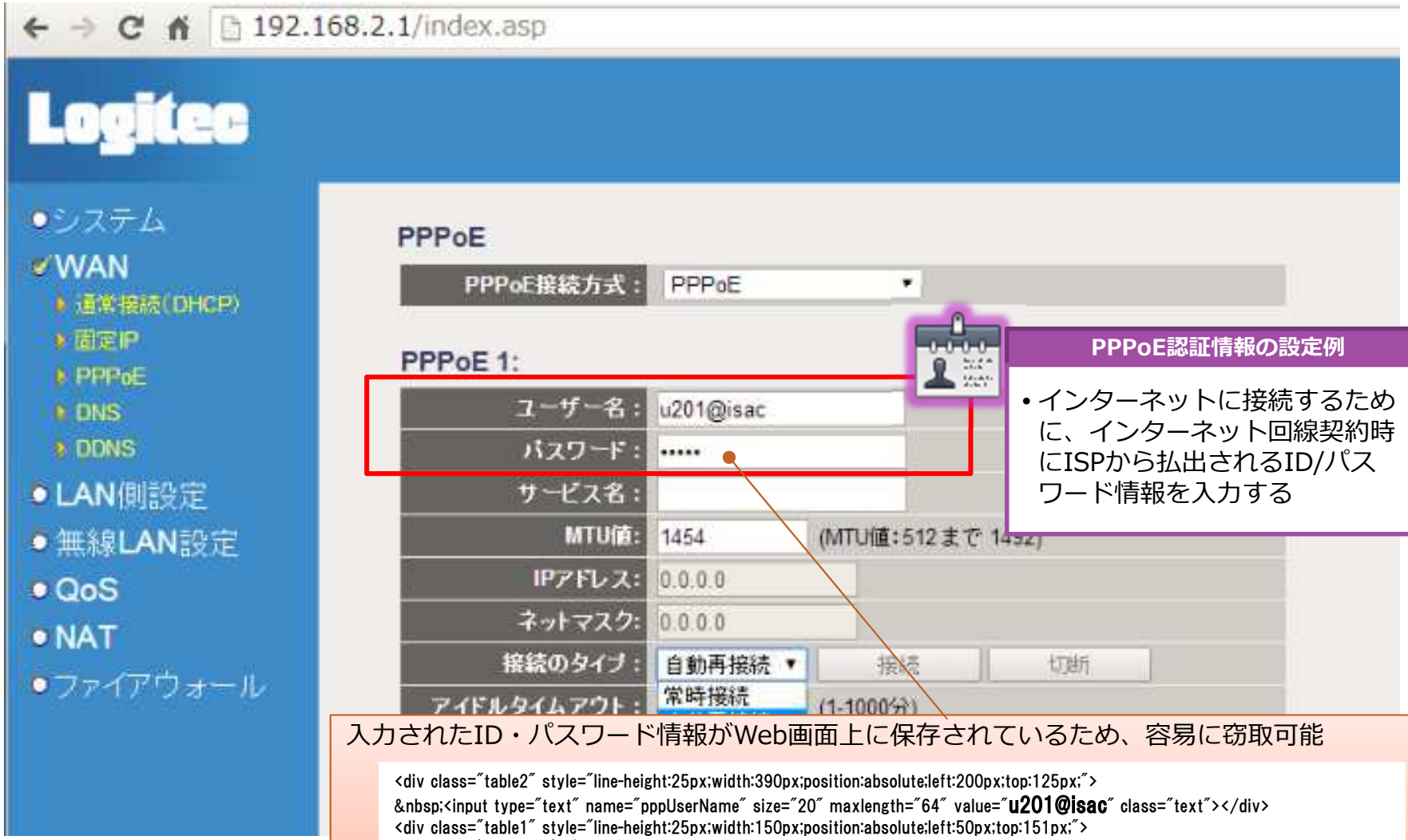
■L社ルータ問題の該当機種に実在するセキュリティ脆弱性

① **WAN(インターネット)側からBBルータ管理画面へアクセス可能**

② BBルータ管理画面の**初期ID/PWが"admin","password"のように平易**なもの

③ BBルータ管理画面上において、設定されているISP提供の**PPPoEアカウント(ID/PW)情報が容易に読み取り可能な状態(平文)**で保存されている

[参考]問題のルータ(LAN-W300N/R)のWeb管理画面例
PPPoE認証情報が容易に漏洩する状態になっていた



PPPoE認証情報の設定例

- インターネットに接続するために、インターネット回線契約時にISPから払出されるID/パスワード情報を入力する

入力されたID・パスワード情報がWeb画面上に保存されているため、容易に窃取可能

```
<div class="table2" style="line-height:25px;width:390px;position:absolute;left:200px;top:125px;">
 <input type="text" name="pppUserName" size="20" maxlength="64" value="u201@isac" class="text"></div>
<div class="table1" style="line-height:25px;width:150px;position:absolute;left:50px;top:151px;">
<script>dw(Password)</script> : 
</div>
<div class="table2" style="line-height:25px;width:390px;position:absolute;left:200px;top:151px;">
 <input type="password" name="pppPassword" size="20" maxlength="64" value="passw" class="text"></div>
```

[2013年4月～7月]
T-ISAC-J で把握した脆弱性ルータに関わるインシデント内容

悪意の第三者によるサイバー攻撃の発信元IP(インターネット接続)での利用

本年3月より各会員サービスサイトに対してリスト型攻撃が多数実施されていることが各会員サービスサイト運営企業やマスコミによって公表されている。
このリスト型攻撃において、悪意の第三者がインターネット接続に利用しているPPPoE認証ID/PWとして、L社製脆弱性保有BBルータ(もしくはその利用者)から詐取したPPPoE認証ID/PWが相当数利用されている。 ①-1)事案

詐取したPPPoE認証ID/PWへの攻撃(詐取された人への攻撃

詐取したPPPoE認証ID/PWを本来の持ち主が使えないようにするため、会員サイトに入りPPPoE認証PWを変更する行為が実施されている。①-2)事案
また、会員サイトにPPPoE認証ID/PWを利用して入り、オプションサービス(VoIP等)を購入し、本来の持ち主への金銭的負担をしいる行為も実施されている ①-2)事案

[2013年4月～7月]

脆弱性ルータに関わる攻撃被害発生状況(1/2) ①-1) 事案

投影のみ

※ 本数字はT-ISAC-Jへ報告があったもののみ

[2013年4月～7月]
脆弱性ルータに関わる攻撃被害発生状況(2/2) ①-2) 事案

投影のみ

※ 本数字はT-ISAC-Jへ報告があったもののみ

[2014年2月]
警察によるプロキシ業者(中都商事)の摘発

NHK NEWSWEB

2014年（平成26年）2月14日［金曜日］

トップページ ＞ 社会ニュース一覧 ＞ 中国の顧客に日本に不正接続させたか

ニュース詳細

中国の顧客に日本に不正接続させたか

2月13日 18時40分

東京・池袋のサーバー管理会社の社長ら２人が、不正に入手した他人のＩＤやパスワードを使って、中国国内の顧客に日本のインターネットに不正に接続させていたとして逮捕されました。
この会社のサーバーは、国内で起きた不正アクセス事件やサイバー攻撃に使われていて、警視庁で実態の解明を進めています。
２人は容疑を否認しているということです。

逮捕されたのは、東京・豊島区のサーバー管理会社「中都商事」の社長で、中国人の劉傳聞容疑者（３４）ら２人です。
警視庁によりますと、劉容疑者らは去年１０月、不正に入手した神奈川県内の男性のＩＤとパスワードを使って、中国の顧客に自分の会社のサーバーから日本国内のインターネットに接続させたとして、不正アクセス禁止法違反の疑いがもたれています。
この会社は、中国国内で顧客を募り、プロキシサーバーと呼ばれるインターネットへの接続を仲介するサーバーを通じて日本のインターネットに接続させるサービスを提供し

■ルーターの欠陥を悪用

今回、摘発されたサーバー管理会社(中都商事)は、一般家庭から盗まれたインターネットの接続IDとパスワードを使って、ネットに接続できるようにしていた。
この一般家庭からのID/PWの詐取は、今回のルータの脆弱性を悪用したものである。

プロキシ(代理)サーバー運営会社「中都商事」(東京都豊島区)の拠点で押収したパソコンなど＝13日午後、警視庁丸の内署（2014年02月13日 配信）【時事通信社】

(出典) NHK NEWSWEB

[2014年11月]
警察によるプロキシ業者の一斉摘発(大光・SUNテクノ)

- 2014年2月に引き続き、11月20日、サーバー運営会社「大光」「SUNテクノ」に所属する中国人国籍の容疑者６人を逮捕。上記2社は約1500人分の認証情報を不正に取得
- 警察の調べでは両者のプロキシサーバを通じて、約4.5億円のネットバンキング不正送金が行われていた(2014年1～6月)ほか、企業の顧客情報(10万件)流出事件でも使用されていた

IDなど1500人分取得、摘発のサーバー2社　中国人に売る

2014/11/20 0:47

小 中 大　保存　印刷　リプリント　▼共有

インターネット接続を中継する「プロキシサーバー」の運営会社による不正アクセス事件で、警視庁が摘発した2社が、計約1500人分のIDやパスワードを不正に取得し、中国人の顧客に売っていたことが19日、同庁の調べで分かった。同庁はこれらのIDなどがインターネットバンキングの不正送金などに使われたとみている。

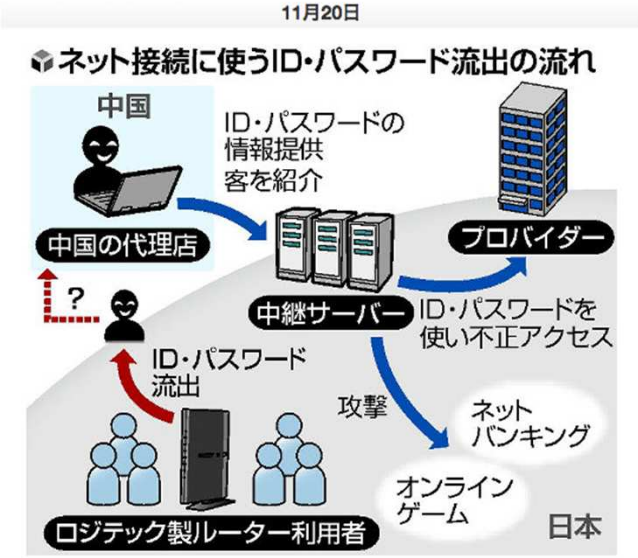
警視庁は19日、サーバー運営会社「大光」(東京・台東)の社長で中国籍の張徳育容疑者(30)＝東京都北区、「SUNテクノ」(東京・豊島)の元役員で中国籍の高志中容疑者(32)＝豊島区＝ら6人を不正アクセス禁止法違反容疑で逮捕した。同庁によると、6人はいずれも「分かりません」などと容疑を否認している。

警視庁によると、両社はIDなどをブローカーから不正に取得し、中国の代理店を通じて中国人顧客に1件あたり1700～5千円程度で販売していた。大光は少なくとも計8千万円、SUNテクノは計4600万円を得ていたという。

顧客は両社のプロキシサーバーを通じ、不正取得したIDやパスワードで日本の接続業者にアクセスしていた。

警視庁は今年1～6月に300件超、4億5千万円のインターネットバンキングの不正送金が両社のサーバーを通じて行われたとみている。携帯電話レンタル会社の顧客情報約10万件が流出した事件でも、大光のサーバー経由でシステムが攻撃されていたという。

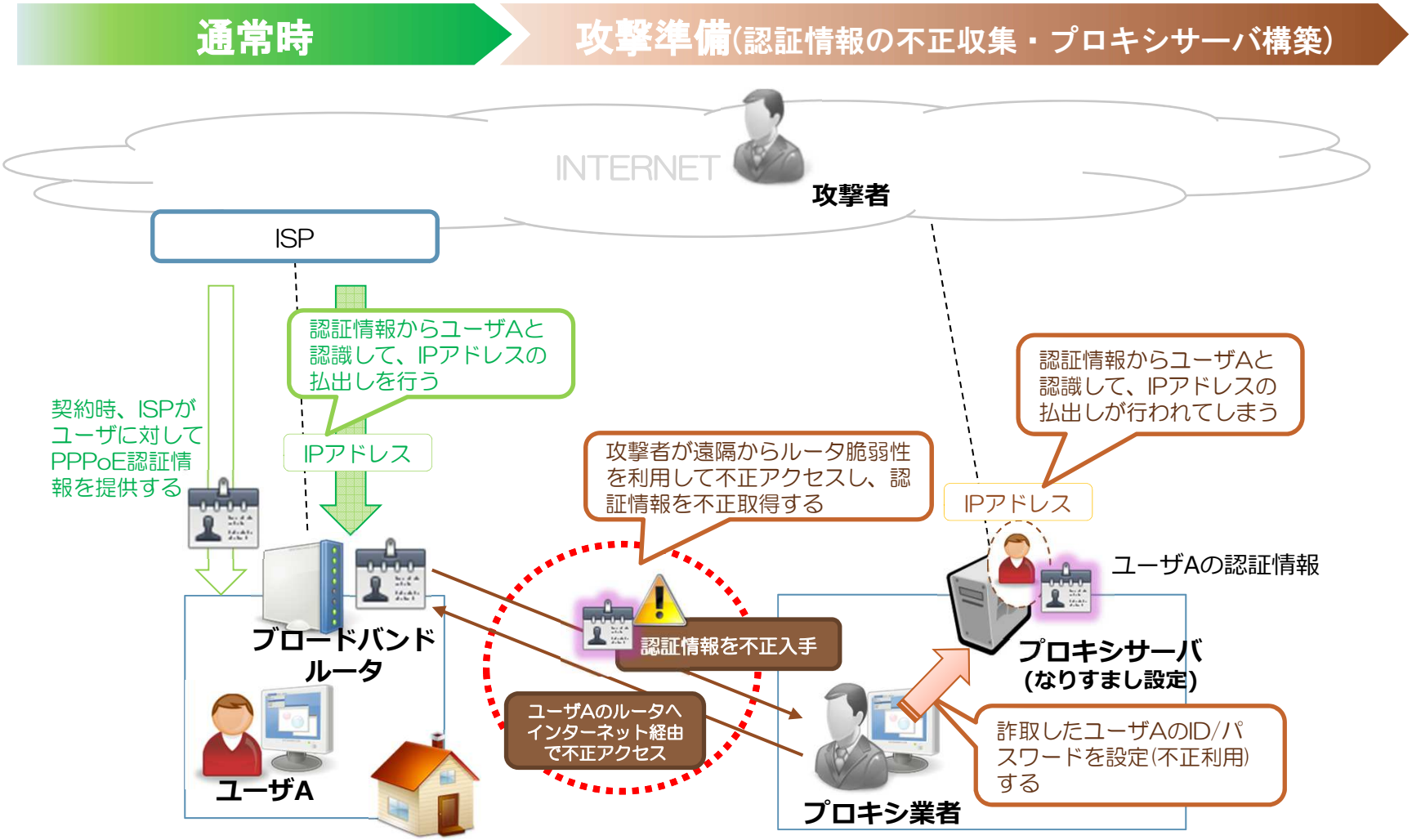
(出典) 日本経済新聞(11月20日)



(出典) KandaNewsNetwork

プロキシ業者が利用していた〝なりすまし回線〟の仕組み(1/2)
ユーザのPPPoE認証情報を不正取得してプロキシサーバを構築する

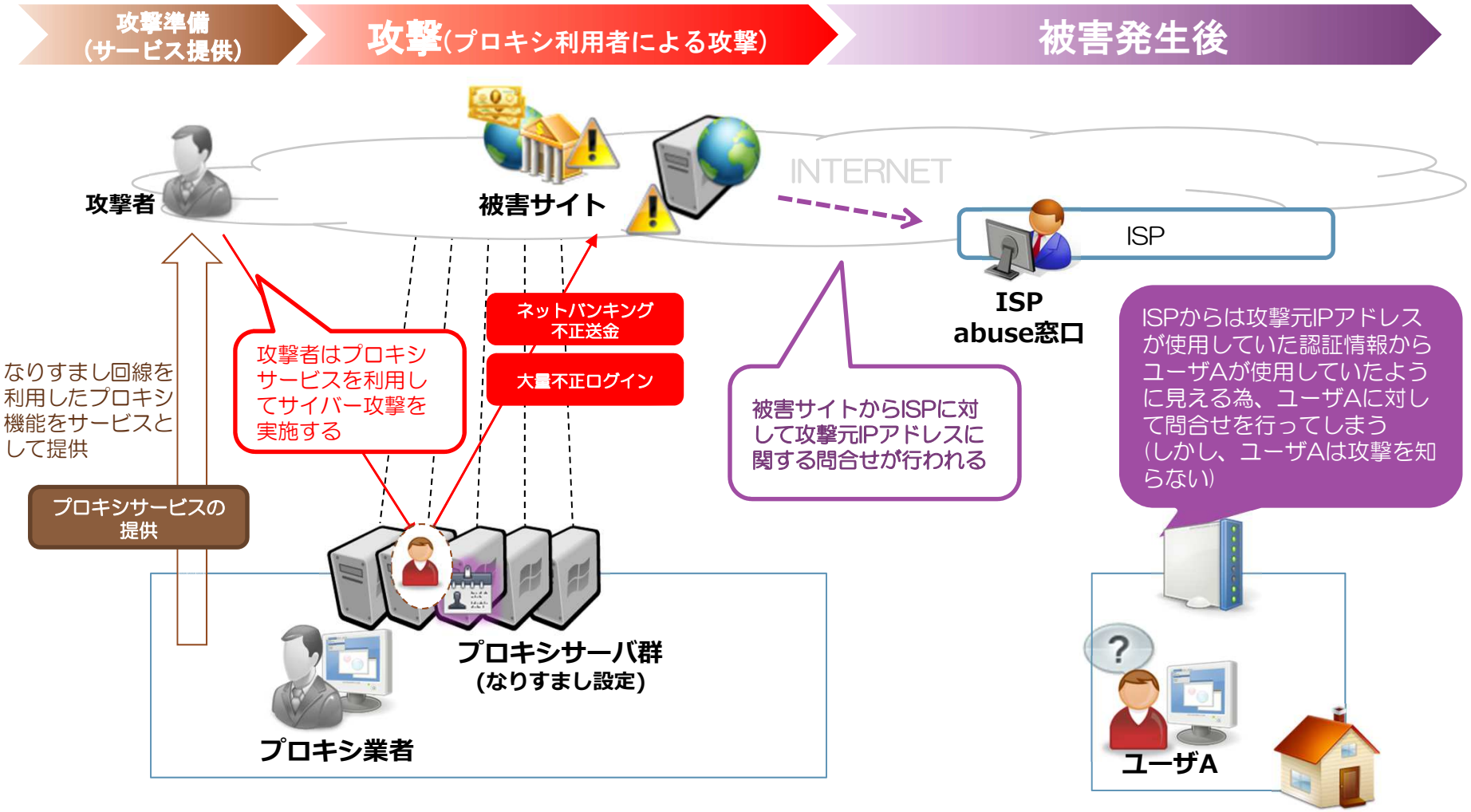
- プロキシ業者は被害ユーザのブロードバンドルータへ不正アクセスしてアカウントを詐取。詐取情報を利用してISPへインターネット接続(PPPoE認証)することで、被害ユーザになり済ました不正接続回線を構築



プロキシ業者が利用していた〝なりすまし回線〟の仕組み(2/2)

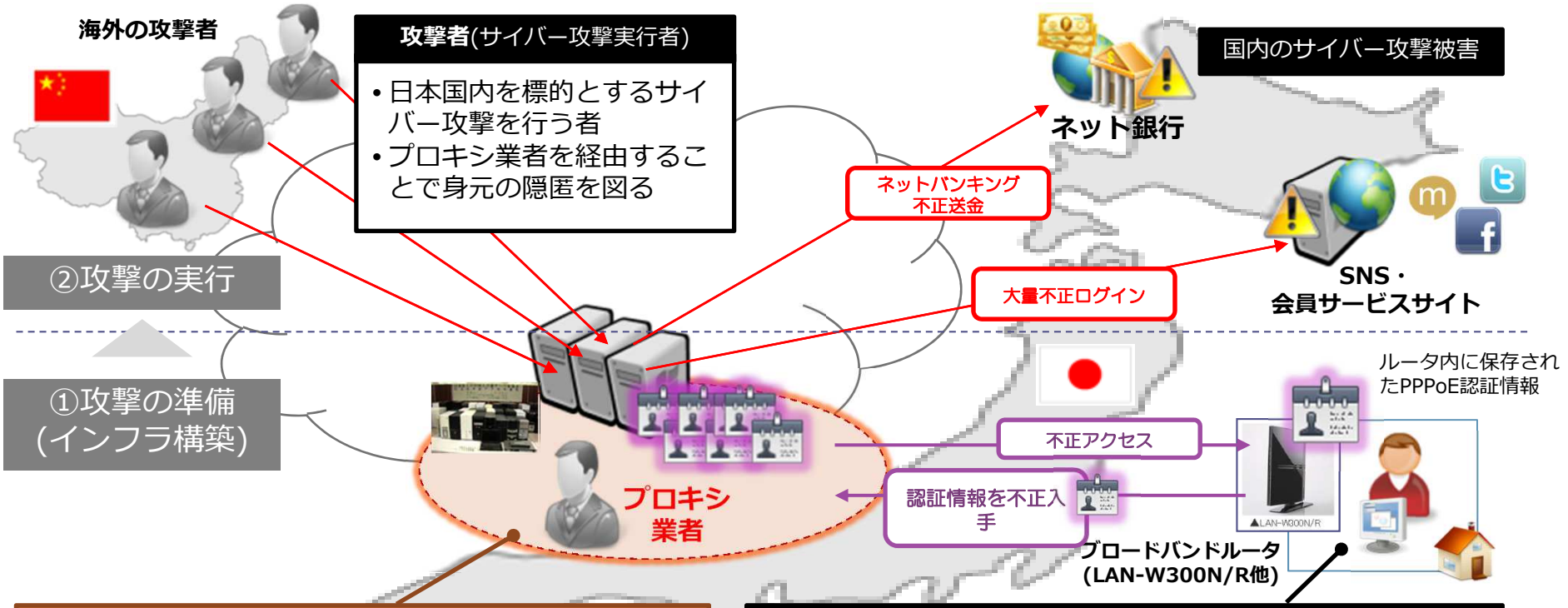
プロキシサーバを攻撃者向けにサービス提供する

- 被害ユーザになり済ました不正接続回線を大量に構築し、"プロキシサービス"として外部ユーザ(攻撃者)へ提供する。攻撃者は当サービスを利用し、身元隠匿しながらサイバー攻撃を行うことが可能
- サイバー攻撃の攻撃元IPアドレスを確認しても、被害ユーザの情報しか確認できず、攻撃者の追跡が困難



中華プロキシ事案の登場人物と全体構成

摘発された事業者は攻撃者に対する「身元隠匿・中継の攻撃インフラ」を提供していた



プロキシ業者(=中都商事、大光、SUNテクノ等)

- 中国など海外の攻撃者に対し、プロキシ"サービス"を提供する事業者
- プロキシサービスのインフラに、被害ユーザから窃取したPPPoE認証情報を利用した「なりすまし回線」を大量に設置し、巨大な「身元隠匿プロキシ」を構築

被害ユーザ

- 問題のL社製ルータ(LAN-W300N/R他)を使用していたインターネット(NTT東西のFlet's)利用者
- プロキシ業者から行わる不正アクセスによってFlet's回線のPPPoE認証情報(認証ID/パスワード)が詐取される
- 認証情報を不正利用されていても、被害ユーザ自身の通信には影響が無い為、本人は気付かない

犯行手口

① プロキシ業者は被害ユーザのブロードバンドルータへ不正アクセスしてアカウントを詐取。詐取情報を利用してISPへインターネット接続(PPPoE認証)することで、被害ユーザになり済ました不正接続回線を構築

② ①の回線を大量に確保したインフラを構築し、「プロキシサービス」として提供。海外の攻撃者は当サービスを利用し、身元隠匿を図った上で、日本国内のWebサイトを標的としたサイバー攻撃を実施

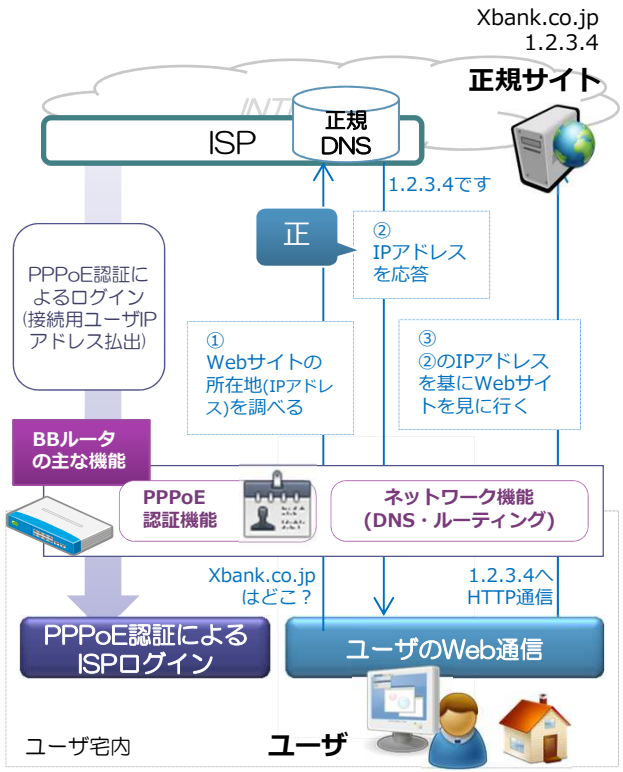
脆弱なルータによって発生し得る利用者不利益
ルータの脆弱性を狙った攻撃事案は既に顕在化している

- ブロードバンドルータ(以下、BBルータ)の脆弱性を突いた攻撃によって管理機能が乗っ取られてしまった場合、大きく①**情報漏洩**・②**フィッシング詐欺**というパターンの被害が発生し得る

通常時

◆**BBルータはWeb通信の為の2つの機能を具備**
- ✓**PPPoE接続機能:** ISPへログインしてIPアドレスの払出を受ける
- ✓**ネットワーク機能:** ユーザのWeb閲覧要求等に対して、**DNS(Webサイト所在地の検索)・ルーティング(Web通信を行うためのパケット転送機能)**等を行う

◆**上記機能は管理機能によって設定が行われる**
- ✓管理機能は専らWeb画面で操作できることが多い

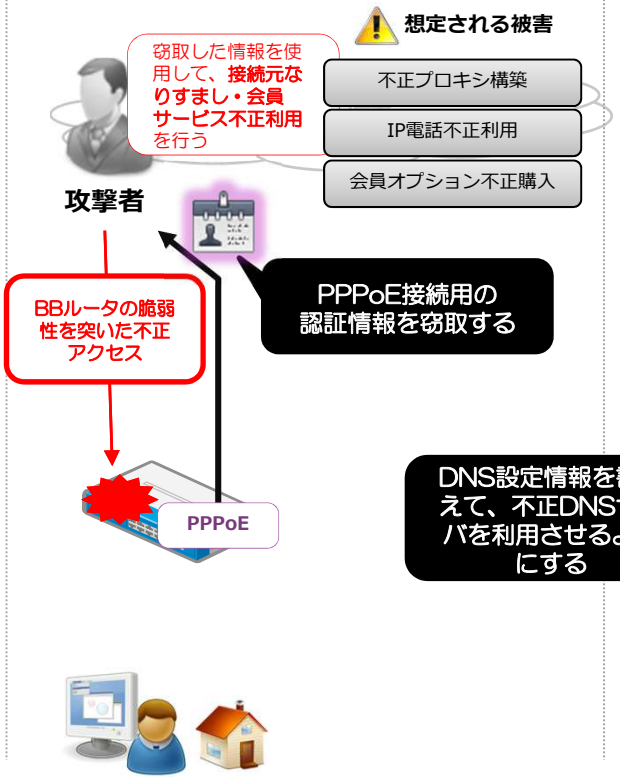


攻撃被害

パターン①: 情報漏洩

手口: 攻撃者が遠隔から脆弱性を利用して不正アクセスし、認証情報を不正取得する。認証情報はISPへの不正接続や会員サービスの不正利用に流用が可能

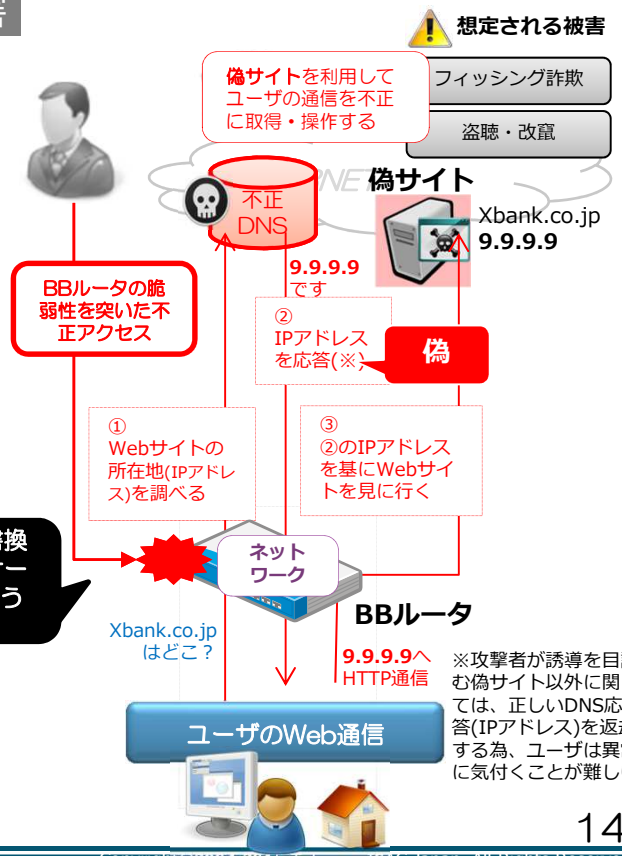
被害:
- 不正プロキシ業者問題
- IP電話高額請求問題
- メールオプション等不正購入



パターン②: フィッシング詐欺

手口: 攻撃者が遠隔から脆弱性を利用して不正アクセスし、ネットワーク(DNS)機能に関わる設定情報を書き換えてしまい、(ユーザが気付かない状態のまま)不正DNSを利用させる

被害:
- フィッシング詐欺
- 通信の盗聴・改ざん



※攻撃者が誘導を目論む偽サイト以外に関しては、正しいDNS応答(IPアドレス)を返却する為、ユーザは異常に気付くことが難しい

中華プロキシー斉摘発の影響

2014/11/19 警察当局による一斉摘発によって中華系プロキシー業者が摘発される。

それに連動するかのように、インターネット上でサービスしている各会員サービス事業者からのAbuse依頼（攻撃しているIPの調査や対応の依頼）の数が激減した。
※ 大手ISP ６社でのAbuse依頼数を合算

投影のみ

投影のみ

多くのサイバー攻撃・特にリスト型不正アクセス攻撃や
金融系不正送金事案がこのメカニズムの上で行われていた

詐取されたIDの利用停止処理の重要性

中華系プロキシー業者が一斉摘発され、その上で行われていたサイバー攻撃はなりを潜めた。しかしながら、

- 2012/05月以降、悪意の第三者に詐取されたインターネット接続ID/PWが消えてなくなったわけではない
  - 闇市場や悪意の第三者グループで流通している可能性が高い
  - 悪意の第三者がインターネット接続ID/PWを詐取可能な脆弱性を持ったBBルータはインターネット上に、現時点でも多数存在している。
    大半がL社製の該当製品であるが、他の製品も多数存在

- 詐取されたインターネット接続ID/PWの対処(利用不可)が非常に大事
- 脆弱性保有製品の対応や、今後発売される製品での対応が非常に重要

投影のみ

［補足資料1］
不正ログイン事案発生状況(2013年 総務省ほか発表)
(中華系プロキシーを攻撃インフラとして利用していたと思われるサイバー攻撃例)
※ ここで紹介する案件すべてが、中華系プロキシーを利用していたかは不明

[補足資料1]
不正ログイン事案発生状況(2013年 総務省ほか発表)

- 国家公安委員会,総務省,経産省は不正アクセス禁止法(第10条第１項)に基づき、毎年不正アクセス行為の発生状況を公表
- 平成25年(2013年)は平成24年の**約2.4倍 2951件**と不正ログイン件数が急増、そのほか「連続自動入力プログラムによる不正ログイン攻撃」が事業者から約80万件の報告があったという。リスト型攻撃手法による会員サイト等への不正ログイン攻撃が本格化していた状況が伺える

第１　平成25年中の不正アクセス禁止法違反事件の認知・検挙状況等について

平成25年中に都道府県警察から警察庁に報告のあった不正アクセス行為を対象とした。

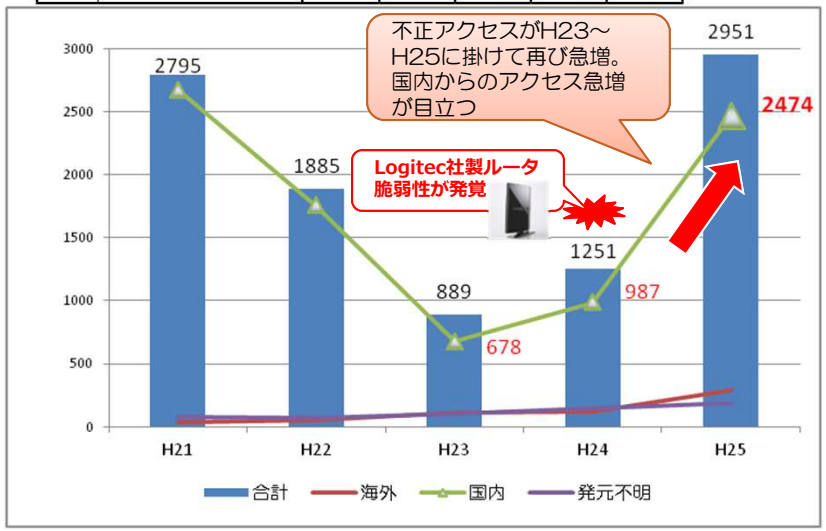
１　不正アクセス行為の認知状況

(1)　認知件数

平成25年中の不正アクセス行為の認知件数[注1]は2,951件で、前年と比べ、1,700件増加した。

表１－１　不正アクセス行為の認知件数の推移

区分＼年次	平成21年	平成22年	平成23年	平成24年	平成25年
認知件数	2,795	1,885	889	1,251	2,951
海外からのアクセス	40	57	110	122	289
国内からのアクセス	2,673	1,755	678	987	2,474
アクセス元不明	82	73	101	142	188



※グラフは上記資料 表1-1 のデータをもとに作成

「連続自動入力プログラムによる不正ログイン攻撃」による不正アクセス行為の状況

約80万件の「連続自動入力プログラムによる不正ログイン攻撃」による不正アクセス行為のうち、「約○件」など概数により報告されたものを除いた604,153件の状況は次のとおり。

１　アクセス元

海外からのアクセス	67,295
国内からのアクセス	437,959
アクセス元不明	98,899
計	604,153

２　被害を受けた特定電子計算機のアクセス管理者

一般企業	604,000
プロバイダ	153
計	604,153

３　警察が把握した経緯

アクセス管理者からの届出	600,750
発見者からの通報	3,272
その他	131
計	604,153

４　不正アクセス行為後の行為（※）

情報の不正入手	283,119
インターネットショッピングの不正購入	4,084
不明	316,950
計	604,153

（※）　各欄の件数は、「連続自動入力プログラムによる不正ログイン攻撃」による不正アクセス行為の被害を受けた事業者から、当該不正アクセス行為の後に行われた可能性のある行為として報告を受けたものである。

(出典) 総務省 不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況 別紙1

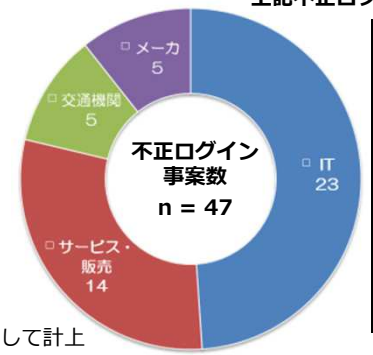
不正ログイン事案発生状況(2014年)

- 不正ログインに関するHP等公開情報を参考に、2014年度の主な不正ログイン発生事案の一覧を以下に示す
- 業界を問わず幅広い分野のWebサイトが攻撃されている中、利用者(会員)数が多いと見られる**SNS・ブログ、マーケティング(アンケート)、通信(ISP等)の会員サイト**の攻撃被害が目立つほか、金銭被害に繋がりやすい**ECサイト、ネットバンク**も被害が見られる

業種	発生日	被害企業	サービス名等	不正ログイン成功件数
メーカー	1/8	グレテックジャパン	GOM Player	不明
コミュニティ	1/21	NTTコムオンライン・マーケティング・ソリューション	Potora	323
ECサイト	1/22	スタイライフ	Stylife	24,158
通信	1/24	ニフティ	@nifty	165
交通機関	2/3	日本航空	JALマイレージバンク	65
SNS・ブログ	2/10	ミクシィ	mixiゲーム	370
SNS・ブログ	2/24	はてな	はてなのサービス	不明
SNS・ブログ	2/28	ミクシィ	mixi	165,972
通信	2/28	ソフトバンクモバイル	MySoftbank	344
交通機関	3/10	全日空	ANAマイレージクラブ	9
交通機関	3/16	東日本旅客鉄道	Suicaポイントクラブ	1万9千
金融	3/27	JCB	MyJCB	数百
金融	4/4	足利銀行	ネットバンク	15
メーカー	4/23	Panasonic	CLUB Panasonic	7万8361
通信	4/30	ソフトバンクモバイル	MySoftbank	724
通信	5/2	ソニーマーケティング	ソニーポイント	273
ECサイト	6月頃	楽天	楽天ダウンロード	不明
メーカー	6/9	任天堂	クラブニンテンドー	23,926
コミュニティ	6/10	ドワンゴ	niconicoアカウント	295,109
SNS・ブログ	6/11	ミクシィ	mixi	263,596
SNS・ブログ	6/12	LINE	LINE	3718
SNS・ブログ	6/20	はてな	はてなのサービス	2389
SNS・ブログ	6/23	サイバーエージェント	Ameba	38,280
マーケティング	6/26	Creative Planning & Promotion	CAPAT	11,502
メーカー	6/30	バンダイナムコ	バンダイナムコID	14,399
マーケティング	7/4	イード	あんぱら	15,092
メーカー	7/4	SEGA	SEGA ID	不明
コミュニティ	7/9	スクエア・エニックス	ニコッとタウン	4,748
金融	7/22	SBI証券	SBI証券Webサイト	不明
SNS・ブログ	7/25	GREE	GREE	39,500
金融	7/28	十八銀行	ネットバンク	不明
人材	7/30	Samurai Factory	Shinobiライティング	124
通信	7/30	NTTコミュニケーションズ	ポイントーク	1,265
ECサイト	8月頃	チケットぴあ	チケットぴあ	不明
ECサイト	8/13	良品計画	無印良品ネットストア	20,957
交通機関	8/18	東日本旅客鉄道	Suicaポイントクラブ	756
人材	9/8	リクルートホールディングス	リクルートID	9,749
交通機関	9/12	東日本旅客鉄道	My JR-EAST	21,400
ECサイト	9/23	良品計画	無印良品ネットストア	19
物流	9/26	ヤマト運輸	クロネコメンバーズWebサービス	10,589
物流	9/29	佐川急便	Webサービス	34,161
通信	9/30	NTTドコモ	docomoID	6,072
マーケティング	11/10	マーシュ	DSYTLE Web	108,185
マーケティング	11/11	GMOインターネット	infoQ	不明
マーケティング	11/22	バリューコマース	アプリス	2,821
金融	12/3	ライフカード	LIFE-WEB Desk	不明
マーケティング	12/24	キューデンインフォコム	ヒアコン	1,320

(データ参考) piyolog 2014年に発生した不正ログインインシデントをまとめてみた

上記不正ログイン事案(全47件)の業種別割合



IT	通信	6	12.77%
	SNS・ブログ	8	17.02%
	マーケティング	6	12.77%
	コミュニティ	3	6.38%
サービス・販売	ECサイト	5	10.64%
	人材	2	4.26%
	金融	5	10.64%
	物流	2	4.26%
交通機関	交通機関	5	10.64%
メーカ	メーカー	5	10.64%
	計	47 件	

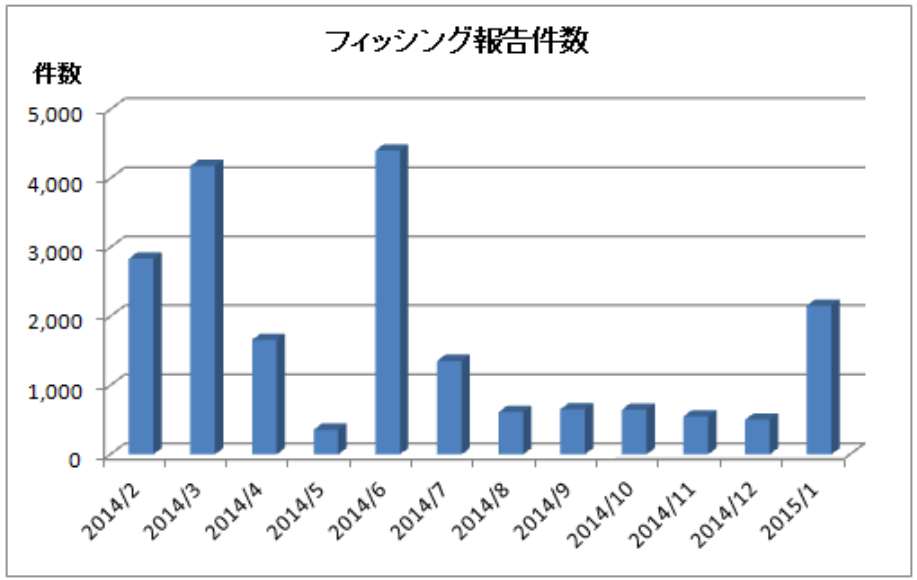
※注1 右記の事案数全47件は同一サービス上で発生した複数被害(例. ミクシィ)を別カウントとして計上
※注2 右記の業種別割合はあくまでWeb上からサンプル抽出した全47件を対象に割合を算出したものであり、必ずしも国内のWebサイト被害の全体傾向を表すものではない

[補足資料2]
三菱東京UFJ銀行フィッシング発生事案について
(中華系プロキシーを攻撃インフラとして利用していたと思われるサイバー攻撃例)
※ ここで紹介する案件すべてが、中華系プロキシーを利用していたかは不明

フィッシング被害発生状況（フィッシング協議会）

- 2014年8月以降、5～600件前後で推移していた報告件数が2015年1月に入り急増、前月の約4倍に及ぶ2156件まで増加。内訳として、約75%がオンラインゲーム関連であり、残り約25%が金融機関に関わるものであるという

フィッシング報告件数の推移



（参考） https://www.antiphishing.jp/report/monthly/201501.html

フィッシング報告事例(2014～2015)

日付		内容
2014年	1/8	[更新] 三菱東京UFJ銀行をかたるフィッシング
	1/16	大学などで使用されているWebメール(Risumail)アカウントを狙うフィッシング
	2/6	eoWEBメールをかたるフィッシング
	2/6	セゾンNetアンサーをかたるフィッシング
	2/17	[更新]ハンゲームをかたるフィッシング
	2/17	OMC Plus をかたるフィッシング
	2/20	更新ゆうちょ銀行をかたるフィッシング
	3/25	NCSOFTをかたるフィッシング
	4/1	ゆうちょ銀行をかたるフィッシング
	4/15	お名前.comをかたるフィッシング
	5/1	[更新]三井住友カードをかたるフィッシング
	5/8	スクウェア・エニックス(FINAL FANTASY XIV)をかたるフィッシング
	6/10	三菱東京UFJ銀行をかたるフィッシング
	6/16	りそな銀行をかたるフィッシング
	6/26	ウェブマネーをかたるフィッシング
	6/27	三井住友銀行をかたるフィッシング
	7/14	ODNをかたるフィッシング
	8/5	Yahoo! JAPANをかたるフィッシング
	8/19	[更新]セゾンNetアンサーをかたるフィッシング
	9/5	Club NTT-Westをかたるフィッシング
	10/7	Facebook をかたるフィッシング
	10/21	[更新] 三菱東京UFJ銀行をかたるフィッシング
	10/28	[更新] スクウェア・エニックス（ドラゴンクエスト X）をかたるフィッシ
	11/11	Club NTT-Westをかたるフィッシング
2015年	1/8	スクウェア・エニックス(ドラゴンクエストX)をかたるフィッシング
	1/23	三菱東京UFJ銀行をかたるフィッシング

（参考）https://www.antiphishing.jp/news/database/

2014年上半期までの不正送金被害状況(警察庁)

- 2014年上半期の被害額は**18億5200万円**に上り、2013年通年(661件、8億1000万円)の2倍以上に及ぶ過去最悪のペース
- 昨年と比して、特に**法人の被害が急増**しており、特に地銀の顧客である**中小企業の被害**が増えているものと見られている

2014年上半期不正送金事犯発生状況(警察庁)

平成26年上半期のインターネットバンキングに係る
不正送金事犯の発生状況について

1　平成26年上半期の発生状況

(1) 発生状況　１，２５４件　約１８億５，２００万円

期間	件数	被害額
H26上	1,254	約18億5,200万円 (約148万円/件)
H25下	1,098	約11億9,300万円 (約109万円/件)
H25上	217	約2億1,300万 (98万円/件)

(出典) 警察庁 広報資料 平成26年9月4日
https://www.npa.go.jp/cyber/pdf/H260904_banking.pdf

L社製ブロードバンドルータ脆弱性に関わるサイバー攻撃に対するISP業界の取組

Telecom-ISAC Japan
Telecom Information Sharing and Analysis Center Japan

L社ルータ問題に関する時系列経緯

投影のみ

第二期 本脆弱性撲滅への対応の実施(2013/05～)

脆弱性対応がとられていない該当製品への踏み込んだ対応

- 本脆弱性に対し、製品メーカ、ISP、セキュリティ団体から広く注意喚起が実施されているが、未だに脆弱性対策を実施していないと思われる該当製品を利用し続けているユーザが多数存在しており、サイバー攻撃のインフラとして悪用されているとともに、インシデントに巻き込まれている

- 外部からの観測とISP個別に持っているユーザ接続情報等を照らし合わせ脆弱性対応未実施の該当製品の利用者を特定し、注意喚起＆脆弱性対応のお願いをする
  → 本利用者特定は通信の秘密の該当項目であり、総務省 消行課の阻却判断が必要（NTTコミュニケーションズ / OCN の相談により、ユーザ保護の観点からの緊急避難として阻却事由の判断を頂く）

- 本事例に関しての公表を実施することで、利用者への更なる注意喚起と悪用者(サイバー攻撃者)への牽制

ユーザ特定による注意喚起 (2013/08~)

Telecom-ISAC Japanおよび本施策に対し賛同した会員ISPで、
① 本脆弱性の注意喚起および個別ユーザ対応を実施
- 2013/8/20~ 複数の会員ISP
- 2013/8/29 Telecom-ISAC Japan

で公表
② 個別ユーザ特定による対応の開始

Telecom-ISAC Japanおよび本施策に対し賛同した会員ISPで、
i) L社製脆弱性保有ルータをネットワーク側から調査を実施し　T-ISAC-Jで実施
ii) スキャン結果とISPが保有するユーザ接続情報を照らし合わせることで　ISPで実施
iii) 該当脆弱性保有ルータの利用者を特定し、　ISPで実施
iv) 特定した利用者に対し、手紙、電子メール等を利用して注意喚起を行う
とともに脆弱性対応をお願い　ISPで実施
脆弱性対応依頼 = ・ルータ ファームウェアのヴァージョンアップ
+ PPPoE認証ID / PW の変更

Telecom-ISAC Japan、会員ISP、製品メーカ(L社)との合意の下に本施策を実施

注意喚起による結果(2013/09~)

投影のみ

- ネットワーク側からの調査により2万弱（実施ISP=4社 合計）の利用者を特定
- 2013/9/24より各ISPより個別ユーザへの注意喚起を実施
- 各社による注意喚起の取り組みは対象数によるが、
  - メール、電話等での注意喚起で一定数以上の脆弱性対応を完了したのち、PPPoE認証PWの強制変更を実施し、ほぼ100%の脆弱性対応を完了
  - 2014/03/31時点で、NWサーチで数100レベルまでおとしたものの その後も地道に検索＞個別ユーザ注意喚起活動を実施し対象ユーザの低減化

2015/06/02 L社 社告掲載の動き

■ L社（ 2015/06/02 ）

L製300Mbps無線LANブロードバンドルータに関するお詫びとお知らせ

Logitec

対応情報 | 法人機向けサービス | サイトマップ | 採用情報 | RSS

製品・サービス | WEBストア "LOGITEC DIRECT" | データ復旧サービス | マニュアル(DL) | サポート(Q&A) | 会社

重要なおしらせ ≪ロジテック 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知らせ

2015/06/02
ロジテック株式会社

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知らせ

謹告掲載のご連絡

お詫びとお知らせ

お客様各位

平素より、格別のご厚情を賜り、厚くお礼申し上げます。
弊社製無線LANブロードバンドルータにおきまして、ファームウェア更新を実施されていない場合、外部からの不正アクセスを受けることにより、お客様のインターネット接続ID及びパスワード情報が流出し、犯罪行為に不正利用されるという事象が発生しております。
該当ルータをお持ちのお客様につきましては、改めてファームウェアが更新されているか確認いただき、アップデートいただくと同時に、インターネット接続IDもしくはパスワードの変更をお願い申し上げます。詳しくは弊社のHPへ誘導させていただきますので、弊社ホームページ又は警視庁ホームページをご確認ください。
ご愛用の皆様には、多大なるご迷惑をおかけしますことを深くお詫び申し上げますとともに、何卒ご理解ご協力を賜りますよう、よろしくお願い申し上げます。

二〇一五年六月二日
ロジテック株式会社

【対象商品】
製品名　300Mbps無線LANブロードバンドルータ
型番　LAN-W300N/R
LAN-W300N/RS
LAN-W300N/RU2
右記製品のシリアルナンバー（未定が「B」ファームウェアバージョンが「2.17」のもの

※詳細は弊社ホームページ
(http://www.logitec.co.jp/info/2015/0516.html)
又は警視庁ホームページ
(http://www.keishicho.metro.tokyo.jp/haiteku/haiteku_hotsuan500.htm)をご確認ください。

【お問い合わせ窓口】
ロジテック株式会社　お客様相談室
電話番号：0120-741-422
受付時間：10時から12時、13時から18時
（月曜日～土曜日（祝日営業）※夏期、年末年始特定休業日を除く）

※お客様から一ご提供いただきました個人情報は、本件の目的以外には使用いたしません。

（※）無線LANブロードバンドルータの設定用ID／パスワードのみ（プロバイダーとの認証を行う際に利用されるインターネット接続ID／パスワード）であり、ネットバンキングやオンラインショッピングで用いられるID／パスワードとは関連のないものです。

弊社といたしましては、さらなるご案内を行い、今後も継続的にファームウェアの更新をお客様にお願いするとともに、インターネットサービスプロバイダ事業者様とも連携をとりながら、誠心誠意取り組んで参ります。

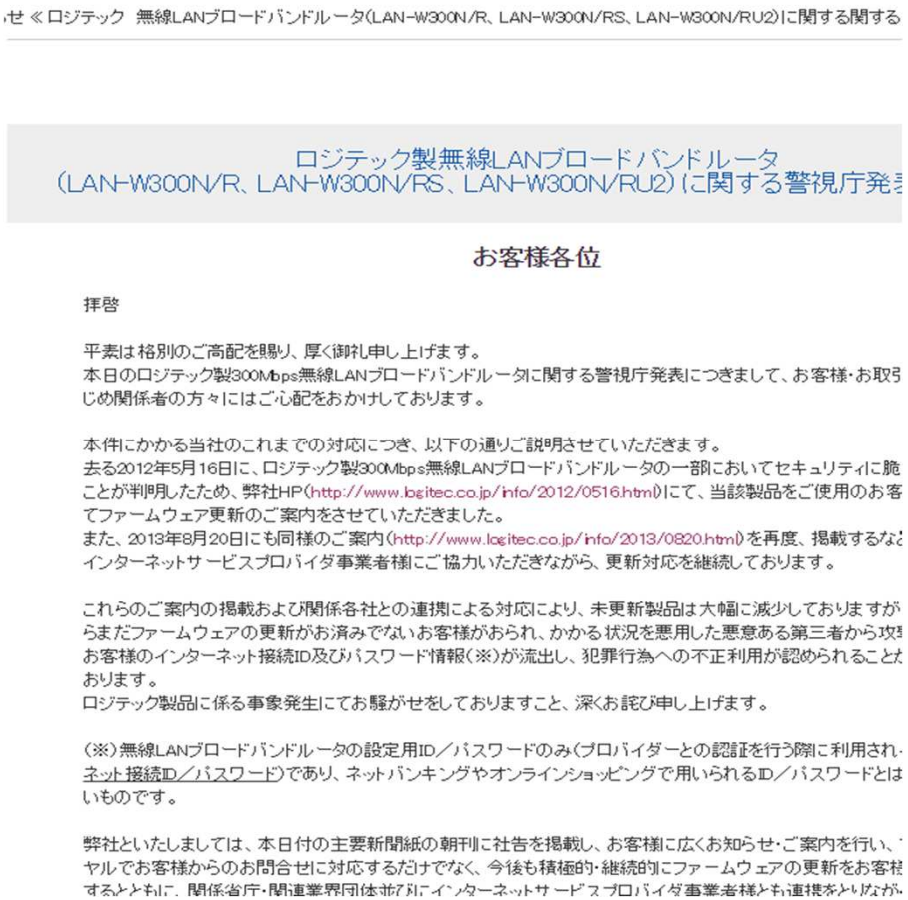
なお当該製品については2013年8月に既に販売を終了しております。

お客様に大変ご迷惑をおかけしますことをお詫び申し上げるとともに、品質管理につきまして今後一層の強化に努めてまいります。何卒ご理解とご協力を賜りますようお願い申し上げます。

(出典)
http://www.logitec.co.jp/info/2015/0602_01.html

■ 警視庁（ 2015/06/02 ）

L製無線LANブロードバンドルータに関する警視庁発表について



≪ロジテック 無線LANブロードバンドルータ(LAN-W300N/R、LAN-W300N/RS、LAN-W300N/RU2)に関する関する

ロジテック製無線LANブロードバンドルータ
(LAN-W300N/R、LAN-W300N/RS、LAN-W300N/RU2)に関する警視庁発表

お客様各位

拝啓

平素は格別のご高配を賜り、厚く御礼申し上げます。
本日のロジテック製300Mbps無線LANブロードバンドルータに関する警視庁発表につきまして、お客様・お取引
じめ関係者の方々にはご心配をおかけしております。

本件にかかる当社のこれまでの対応につき、以下の通りご説明させていただきます。
去る2012年5月16日に、ロジテック製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
ことが判明したため、弊社HP(http://www.logitec.co.jp/info/2012/0516.html)にて、当該製品をご使用のお客
てファームウェア更新のご案内をさせていただきました。
また、2013年8月20日にも同様のご案内(http://www.logitec.co.jp/info/2013/0820.html)を再度、掲載するなど
インターネットサービスプロバイダ事業者様にご協力いただきながら、更新対応を継続しております。

これらのご案内の掲載および関係各社との連携による対応により、未更新製品は大幅に減少しておりますが
らまだファームウェアの更新がお済みでないお客様がおられ、かかる状況を悪用した悪意ある第三者から攻撃
お客様のインターネット接続ID及びパスワード情報(※)が流出し、犯罪行為への不正利用が認められることと
おります。
ロジテック製品に係る事象発生にてお騒がせをしておりますこと、深くお詫び申し上げます。

(※)無線LANブロードバンドルータの設定用ID／パスワードのみ(プロバイダーとの認証を行う際に利用され
ネット接続ID／パスワード)であり、ネットバンキングやオンラインショッピングで用いられるID／パスワードとは
いものです。

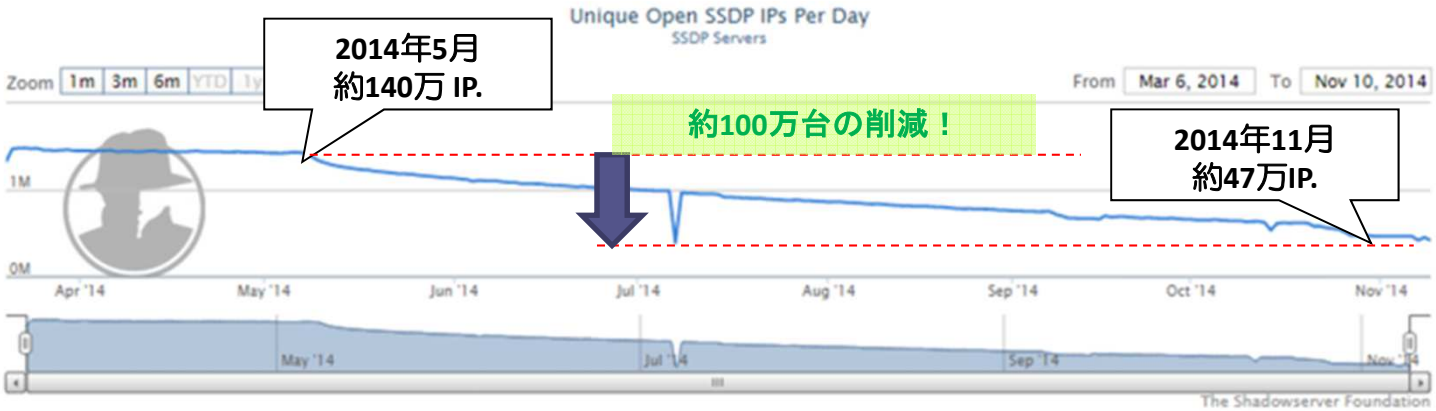
弊社といたしましては、本日付の主要新聞紙の朝刊に社告を掲載し、お客様に広くお知らせ・ご案内を行い、
ヤルでお客様からのお問合せに対応するだけでなく、今後も積極的・継続的にファームウェアの更新をお客様
するとともに、関係省庁・関連業界団体並びにインターネットサービスプロバイダ事業者様とも連携をとりなが

(出典)
http://www.logitec.co.jp/info/2015/0602_02.html

別件ですが・・・通信事業者が管理するNW機器に対する脆弱性を通信事業者がやると・・・・・

- 2014年当初よりSSDPに関する脆弱性を保有した一部の機器がインターネット上に大量存在することが確認
  2014年5月よりインシデント発生前に対策版のファームウェアの準備がサプライヤ側で行われた
- 2014年8月の米国ホスティング会社への攻撃発生時、会員ISPから事案発生に関する情報連絡が行われた際、機器サプライヤへ情報共有を行い、対策版ファームウェアの展開を促すことで早期対策の実施に繋がる結果となった
- 最終的には、2014年10月より強制対応が実施された

外部観測情報から見る脆弱性ルータ数の削減状況



(出典) https://ssdpscan.shadowserver.org/stats/ssdp_jp.html

※ 6か月という機関で100万台近くの数の脆弱性対応が完了
該当機器のSSDPに関する脆弱性は消失

BBルータの現状
(インターネット接続ID/PWの詐取の観点)

調査の結果から見る脆弱性BBルータの現状

ここ２～３年の傾向として、他人から詐取した認証ID (PPPoE認証ID/PW)でインターネット接続を行い、その接続環境から各種サイバー攻撃(リスト型攻撃等)をしている事案が多数見受けられている。

投影のみ

2013年2月に逮捕者が出た中都商事事案に代表される脆弱性保有L社製該当ルータから詐取したPPPoE認証ID/PWを悪用したサイバー攻撃は各種団体による対応により減少していると思われるが、L社製該当ルータ以外の所有者のPPPoE認証ID/PWを悪用したサイバー攻撃事案が報告されはじめている。

- **Logitec該当製品以外からの詐取行動が起こっていると推測される**
  WAN側からアクセス可能でL社製該当製品でないもの(万オーダ)も、脆弱なID/PWによって管理機能へのアクセスが可能な状態にあるものと推測できる
- **WAN側からのアクセスせずにBBルータへのアクセスを行う攻撃手法が存在**
  - **クロスサイトリクエストフォージェリ(CSRF)攻撃**
  - **脆弱なWiFi経由の管理画面不正アクセス**

家庭用BBルータの脆弱性がサイバー攻撃者に攻撃インフラを提供している現状がある

WAN側アクセス可能なホストは万オーダ

ログイン画面(401応答)を示す機器は万オーダ (全国換算値)存在する。
当該機器らはWAN側へ開放していることを意味する。これの多くはL社と同様にWeb管理画面を持つBBルータ等NW機器であるとみられる。

応答有無	code	応答数(割合)	全国換算
HTTP応答有			
	200 OK		
	301 Moved Permanently		
	302 Found		
	400 Bad Request		
	401 Unauthorized		
	403 Forbidden		
	404 Not Found		
	その他		
HTTP応答無			
調査対象アドレス総数			

取扱注意
(投影のみ厳守)

投影のみ

※( )内の数値は総アドレス数に対する割合を示す

※2013/08 測定

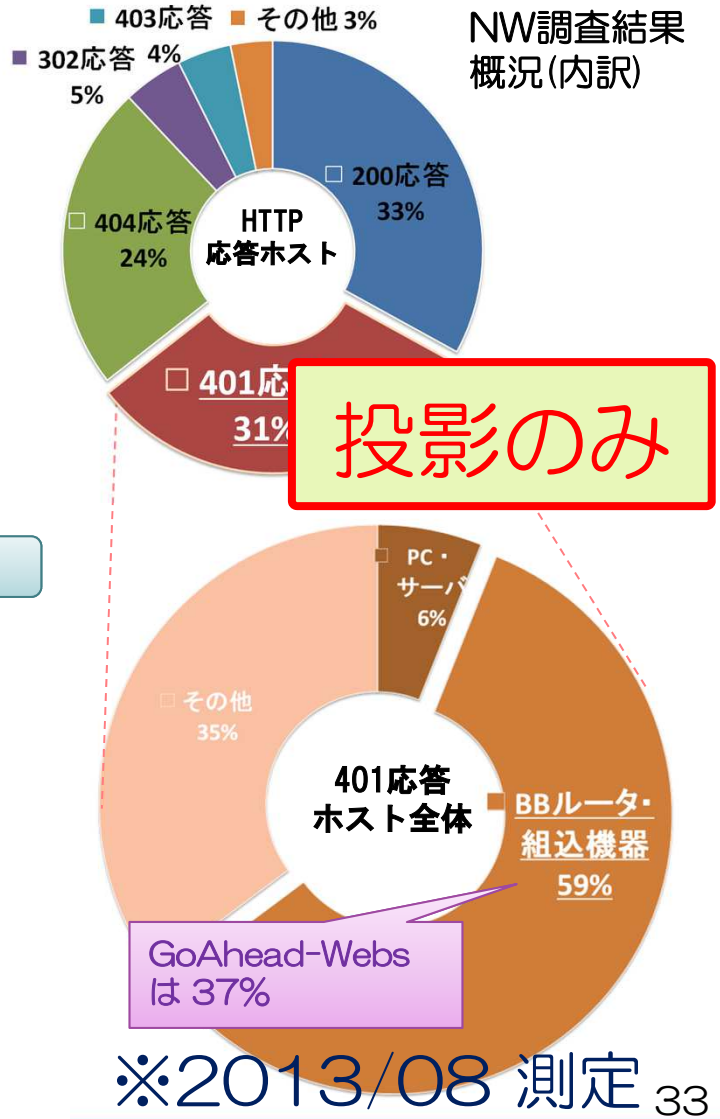
NW調査結果から見られるNWデバイスの現状

■ユーザ認証画面が外部公開されているNWデバイス機器が多い

- HTTP応答ホストとして、Webサイト公開を行っている200応答ホストに続いて、ユーザ認証を行う401応答ホストの割合が目立つ。
- 401応答ホストの内訳をみると、GoAhead-Websなど組込系Webサーバソフトウェアの特徴が見られるホストが多く占めており、BBルータ等管理Web画面を持つNW機器が該当することが推測される。

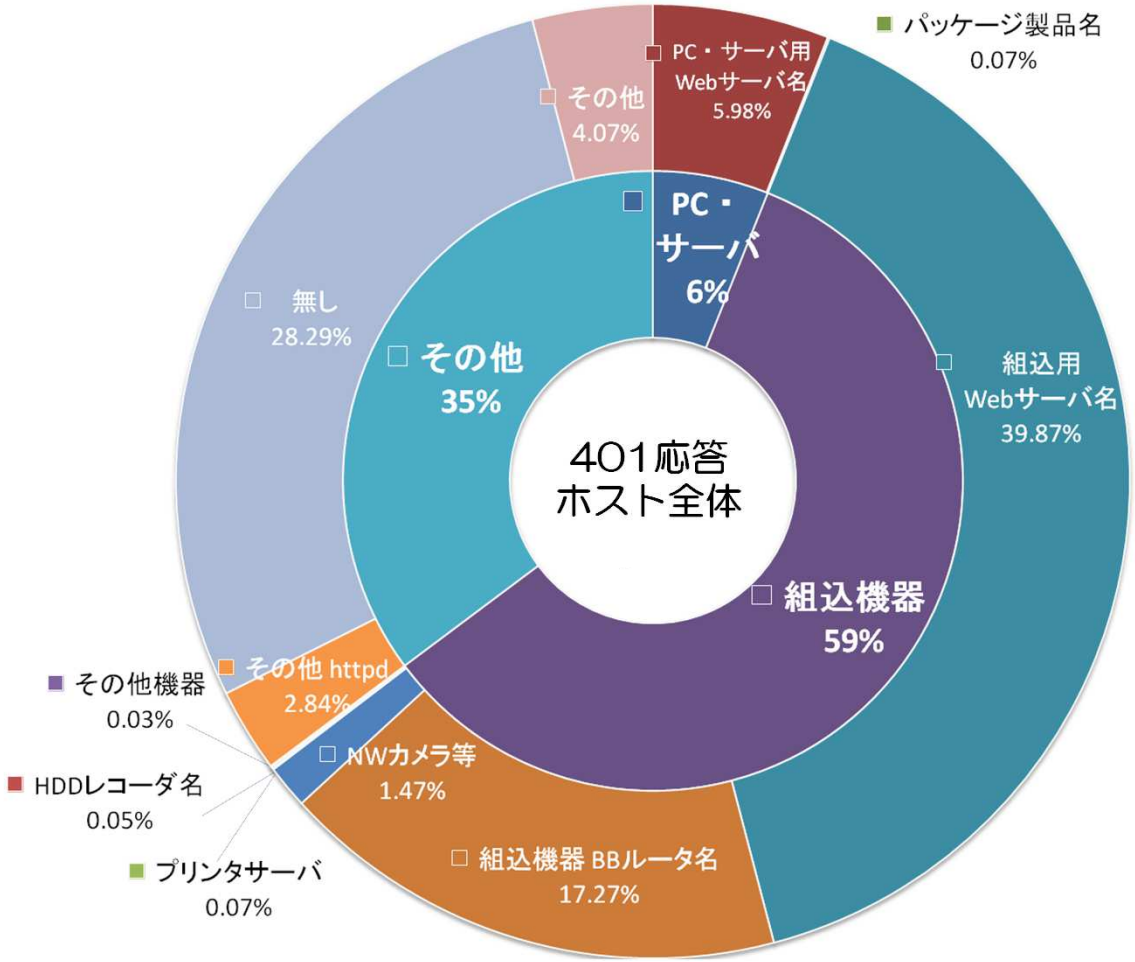
■401認証ホストの脆弱性追加調査の必要性

- 401認証画面がオープンになっている機器は全国換算で万オーダに上る。その中にはL社ルータと同様に、WAN側から推測容易な値(admin／password)等でログインできるなど、脆弱性を保有したNW機器が存在することが予想されるが、詳細についてはさらなる追加調査が必要である。



401応答機器の多くはBBルータ

401応答ホストの内訳として、PC・サーバ系server値を一定数確認した一方で、GoAhead-Websを中心に主に組込機器に使用されるWebサーバソフトウェアがより多く観測された。BBルータをはじめ、NWカメラ・プリンタサーバ等NWデバイスが主なものと推測される。

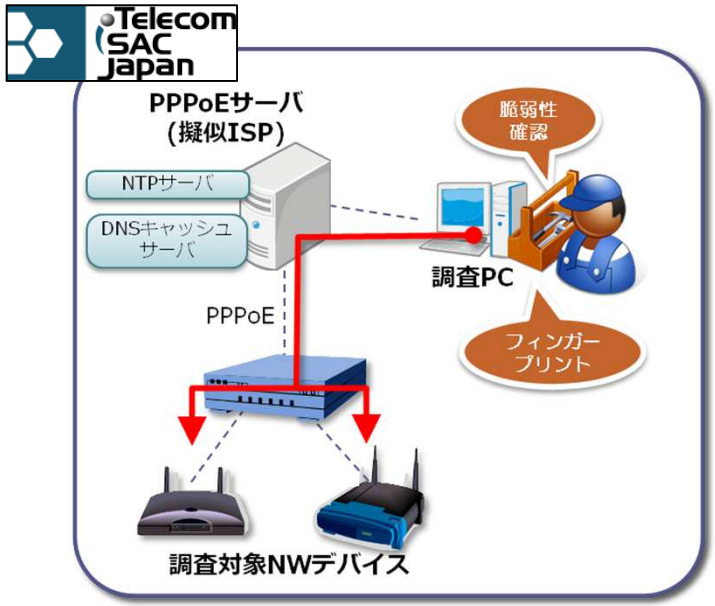


HTTP server値の例(抜粋)

	server値	数
PC・サーバ系	Apache系	投影のみ
	Microsoft-IIS系	
	lighttpd* (lighttpd)	
	thttpd* (thttpd)	
	Boa* (Boa)	
	mini_httpd*	
組込機器系	GoAhead-Webs	
	(A社ルータ)	
	(C社ルータ)	
	(B社ルータ)	
	GR-HTTPD Server	
	(I社ルータ)	
	(F社NWカメラ)	
	IPCamera-Web	

2013/12 売れ筋BBルータの調査結果(1/2)

T-ISAC-Jでは赤坂環境にてローカルの疑似環境を利用したBBルータの実機詳細調査を実施。



項目		該当機種 数	(%)
Web(HTTP)管理画面の認証脆弱性有り		**1**	(2.2)
(内訳)	WANからWeb管理画面アクセス可能	1	(2.2)
	脆弱な管理者デフォルトID/PWDを利用	33	(71.7)
	PPPoEアカウントの暗号化保存無し	20	(43.5)
SSDP(UPnP)機能に関する脆弱性有り		**3**	(2.2)
(内訳)	SSDP応答あり	6	(13.0)
	Description情報取得可能	3	(6.5)
	SOAP-IFアクセス可能	1	(2.2)
Amp攻撃の踏み台脆弱性有り		**1**	(2.2)
(内訳)	DNS(オープンリゾルバ)	1	(2.2)
	NTP	0	(0.0)
	SNMP	0	(0.0)
	CHARGEN	0	(0.0)
全調査対象機種		**46**	(100)

- L社以外のWAN側からWeb管理画面(HTTP)へアクセスできる機種は現状発見せず
- **脆弱な管理者デフォルトID/PWDを持つ機種は 33機種**(71.7%)**も存在**
- **PPPoEアカウント情報を暗号化せずに平文で保存する機種は20機種**(43.5%)

調査結果(Web画面認証)(1/3)

- L社製ルータ問題で知られるLAN-W300N/Rのみ、**WAN側からのWebアクセス**が可能であった
- 他ルータにおいても、**推測容易なID/パスワードの利用**、**パスワードの平文保存**が確認されている。もしポート開放等の理由によって第三者にアクセスされた場合、容易にログイン可能であり注意が必要といえる

機種名	WANからのWeb画面閲覧	デフォルトのWeb画面認証ID/パスワード		PW平文保存
		root	(無し)	-
		admin	password	無
		(認証なし)	(認証なし)	-
		admin	admin	有
		admin	admin	有
		admin	(ユーザ設定必須)	無
		admin	password	有
		admin	password	有
		admin	password	有
		au	1234	有
		admin	(ユーザ設定必須)	無
		root	(無し)	有(Manual時)
		root	(無し)	有(Manual時)

投影のみ

調査結果(Web画面認証)(2/3)

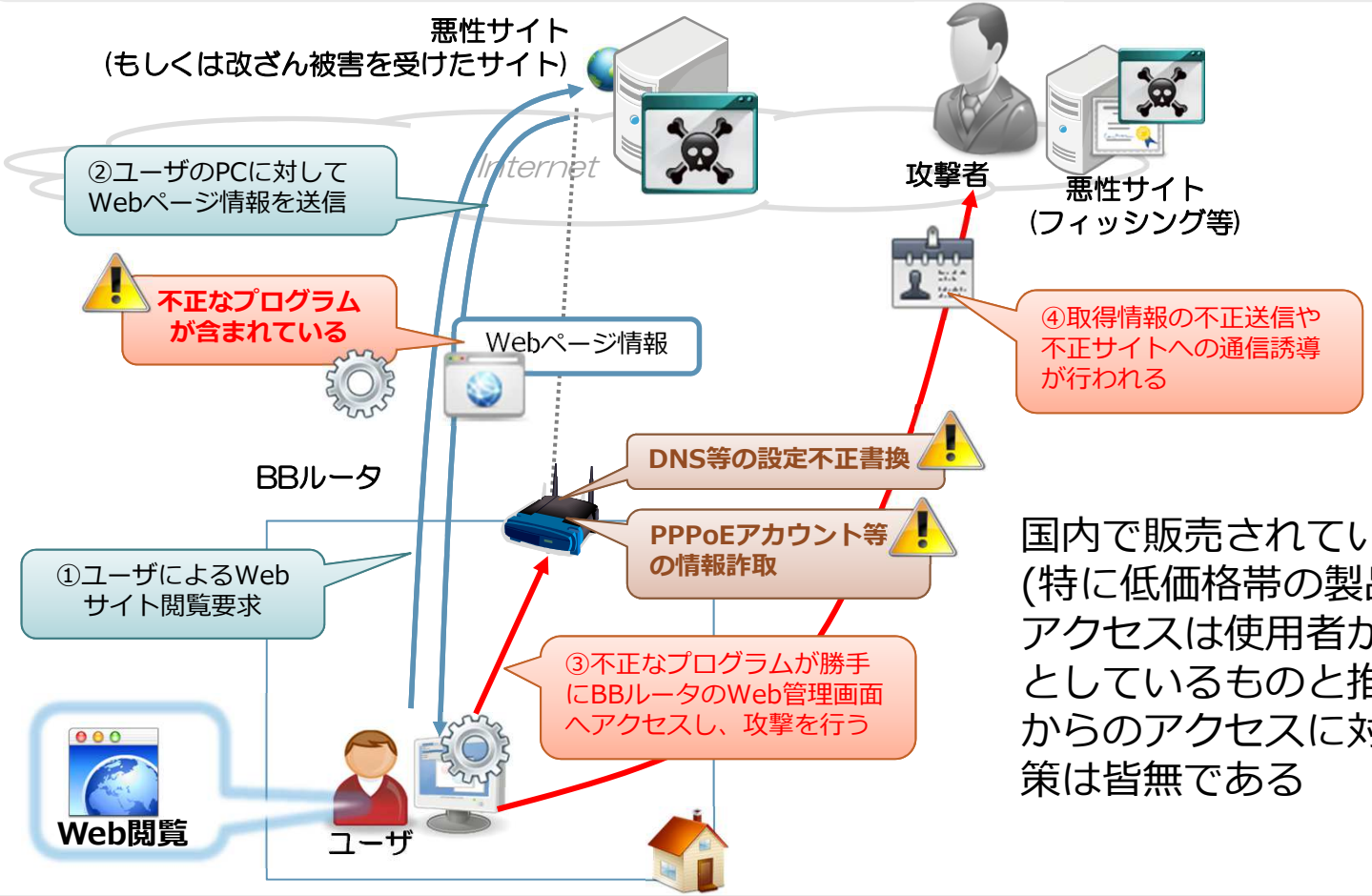
機種名	WANからのWeb画面閲覧	デフォルトのWeb画面認証ID/パスワード		PW平文保存
投影のみ		admin	password	有
		admin	admin	有
		admin	admin	無
		(ツール利用のため不明)	(ユーザ設定)	無
		(認証なし)	(認証なし)	有
		(認証なし)	(認証なし)	有
		(認証なし)	(認証なし)	有
		admin	password	無
		admin	password	無
		admin	password	無
		admin	password	無
		admin	password	無
		admin	password	無
		root	(無し)	有
		root	(無し)	無

調査結果(Web画面認証)(3/3)

機種名	WANからのWeb画面閲覧	デフォルトのWeb画面認証ID/パスワード		PW平文保存
投影のみ	不可	root	(無し)	無
	不可	root	(無し)	無
	不可	root	(無し)	無
	不可	root	(無し)	無
	不可	user	(ユーザ設定)	無
	不可	admin	(無し)	無
	不可	admin	password	無
	不可	admin	(ユーザ設定)	無
	不可	admin	(ユーザ設定)	無
	不可	admin	(ユーザ設定)	無
	不可	admin	(ユーザ設定)	無
	不可	admin	(ユーザ設定)	無
	不可	admin	(ユーザ設定)	無
	不可	admin	(ユーザ設定)	無
	不可	admin	(ユーザ設定)	無
	不可	root	(無し)	無
	不可	(ユーザ設定)	(ユーザ設定)	無
	不可	(認証なし)	(認証なし)	無

境界を越える不正設定変更の攻撃(CSRF)

クロスサイトリクエストフォージェリ(CSRF)攻撃は、ユーザが不正に細工されたWebサイトを閲覧した際にユーザ側のPC端末に意図しない不正な操作を行わせる攻撃である。



国内で販売されているBBルータの大半(特に低価格帯の製品)は、LAN側からのアクセスは使用者からのアクセスを前提としているものと推測されるが、LAN側からのアクセスに対するセキュリティ対策は皆無である

本攻撃手法を利用することで、攻撃者は外部から侵入することなくユーザ宅内のBBルータ等への不正アクセスを実現できる。この結果、ユーザ側には **DNS設定不正書換による通信の不正誘導、外部向けポート公開による外部からの不正侵入・BBルータ内の情報詐取**といった被害が発生する可能性がある。

まとめ

- **サイバー攻撃インフラを構築するための接続ID/PWの詐取**

国内NW中に存在する家庭用ブロードバンドルータから、インターネット接続ID/PWを詐取することは非常に簡単。

NW調査(2013年夏)

数万規模で、ネットワーク側から管理画面に入れるBBルータが存在(しかもID/PWが平易)

実機調査(2013年～)

2013~2014年に家電量販店で購入できるBBルータにおいて・・・・・・

ネットワーク側から管理画面に入れるBBはなかったが・・・・・・

管理画面のID/PWは平易(4～6パターン) … CSRF などには引っかかる・・・

国内インターネットではサイバー攻撃インフラを攻撃者に提供して・・・・・ます(ー_ー)!!

- **脆弱性対応は非常に高コスト！**

サイバー攻撃の多くは既知のソフトウェア脆弱性を利用して攻撃してきます。
絶えず言われることですが、ソフトウェア最新化は重要かつ効果的です。

-製品利用者との接点を持つことが重要

利用者にリーチできない、リーチできても対応してもらえない！

-特にNW側から脆弱性対応ファームウェアを送り込れば効果は絶大！

-国内外製品メーカとの連携は不可欠！セキュリティに関する情報共有を！

製品メーカによっては、何が問題であるか理解するが結構困難！

ISPの皆様へのお願い

警察庁のサイバー犯罪対策のHP等でインターネット利用者が取り組むべき対策とされているのは．．．．

■ ウイルス対策ソフトを導入する
■ パソコンのＯＳや各ソフトウェアを最新の状態にする
■ パスワード等の利用では多要素認証を利用する
■ 不審な入力画面等発見した場合はさわらない

- これらは基本的に、インターネット利用における端末(PC / スマホなど)での対策です。
- しかしながら、攻撃者が利用する脆弱性は端末だけではなくネットワーク接続機器全般に及びます。

利用者に対して以下を啓発して頂きたい

端末利用に関して

■ ウイルス対策ソフトを導入する
■ パソコンのＯＳや各ソフトウェアを最新の状態にする
■ パスワード等の利用では多要素認証を利用する
■ 不審な入力画面等発見した場合はさわらない

NW機器

■ NW機器ソフトウェア(ファームウェア)を最新の状態にする
■ 管理画面へのlogin ID / PW を工場出荷時から利用者固有のものに変更する
■ 不審なNW / NW機器(WiFiなど)を利用しない

VAWTRAK無効化作戦とISPs

本報告内容は、総務省プロダクトであるACTIVEで
実施されているものです。
総務省様やACTIVEプロジェクトメンバーが話すべきですが
通りすがりの西部が語ります
(；ー_ー)

Telecom-ISAC Japan
Telecom Information Sharing and Analysis Center Japan

概要

2014年5月、トレンドマイクロ社よりインターネットバンキングユーザを対象に攻撃する「VAWTRAK」の検出数増加の注意喚起が行われた。同社の調べでは2014年1～6月期に日本国内で約2万台の感染が確認されており、これは同時期に検出されたオンライン銀行詐欺ツールの約66%にあたる。警察庁発表の情報では同時期の不正送金被害額が約18億5200万円（前年比9倍）となっており、一部報道ではVAWTRAKによる被害がその大半を占めるとの見方がされた。

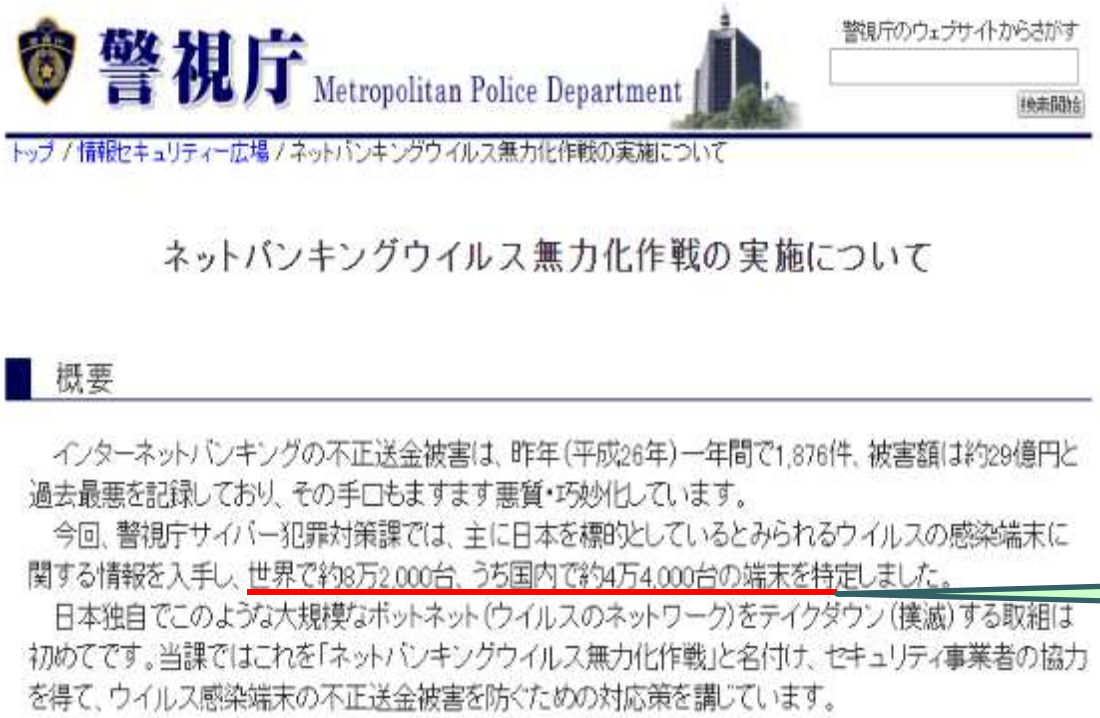
その後、2015年4月10日の警視庁発表時点では世界で約8万2,000台（うち国内で約4万4,000台）の感染端末が特定されており、ネットバンキングウイルス無力化作戦として総務省、Telecom-ISAC Japanおよび通信事業者が連携しての対応策が講じられている。

問題のVAWTRAKはWebサイト，メール添付ファイル，フリーウェアからの感染が確認されており以下の特徴を持っている。
・PC上に保存されているユーザ情報の窃取
・偽画面による秘密情報（ID，パスワード，証明書等）の窃取、および不正送金の実施
・ターゲット情報および偽画面表示用データの自動取得

更なる被害拡大を防止するため、インターネットバンキング利用者は本情報を確認の上、ウイルス対策ソフト等の利用による感染確認、駆除の実施が望まれる。

経緯

- 2014年5月トレンドマイクロ社の注意喚起として、VAWTRAKの標的として日本を拠点とする銀行4行とクレジットカード会社5社が設定され、感染者の9割以上が日本であると報告された。同年9月には標的が日本国内の銀行17行、クレジットカード会社20社に急増したことが確認され、日本が重点攻撃対象と見られた。
- 2015年4月10日、警視庁よりネットバンキングウイルス無力化作戦として、世界で約8万2,000台（うち国内で約4万4,000台）の感染端末を特定した事実とそれらを撲滅する取り組みについて発表された。本作戦の一環として、総務省およびTelecom-ISAC Japanら通信事業者が中心となり、ACTIVEを通じた対応（感染者への注意喚起，駆除依頼）が行われている。



警視庁 Metropolitan Police Department

警視庁のウェブサイトからさがす

検索開始

トップ / 情報セキュリティー広場 / ネットバンキングウイルス無力化作戦の実施について

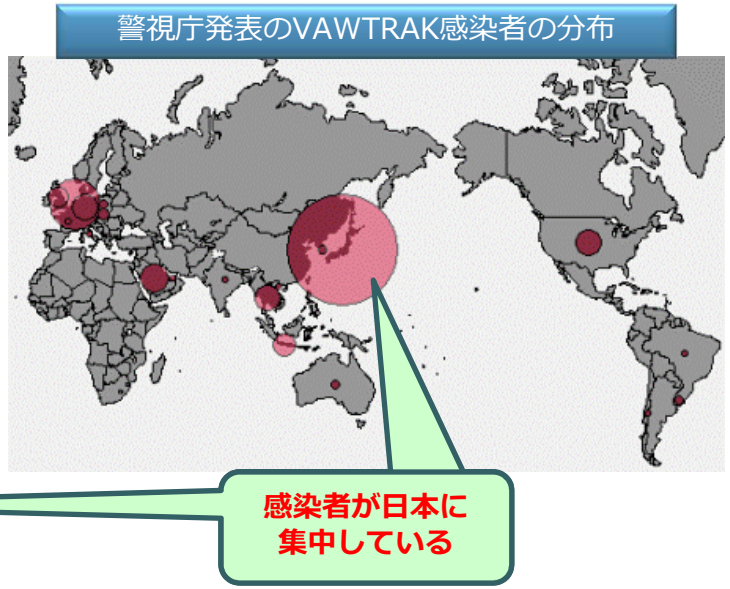
ネットバンキングウイルス無力化作戦の実施について

概要

インターネットバンキングの不正送金被害は、昨年（平成26年）一年間で1,876件、被害額は約29億円と過去最悪を記録しており、その手口もますます悪質・巧妙化しています。

今回、警視庁サイバー犯罪対策課では、主に日本を標的としているとみられるウイルスの感染端末に関する情報を入手し、世界で約8万2,000台、うち国内で約4万4,000台の端末を特定しました。

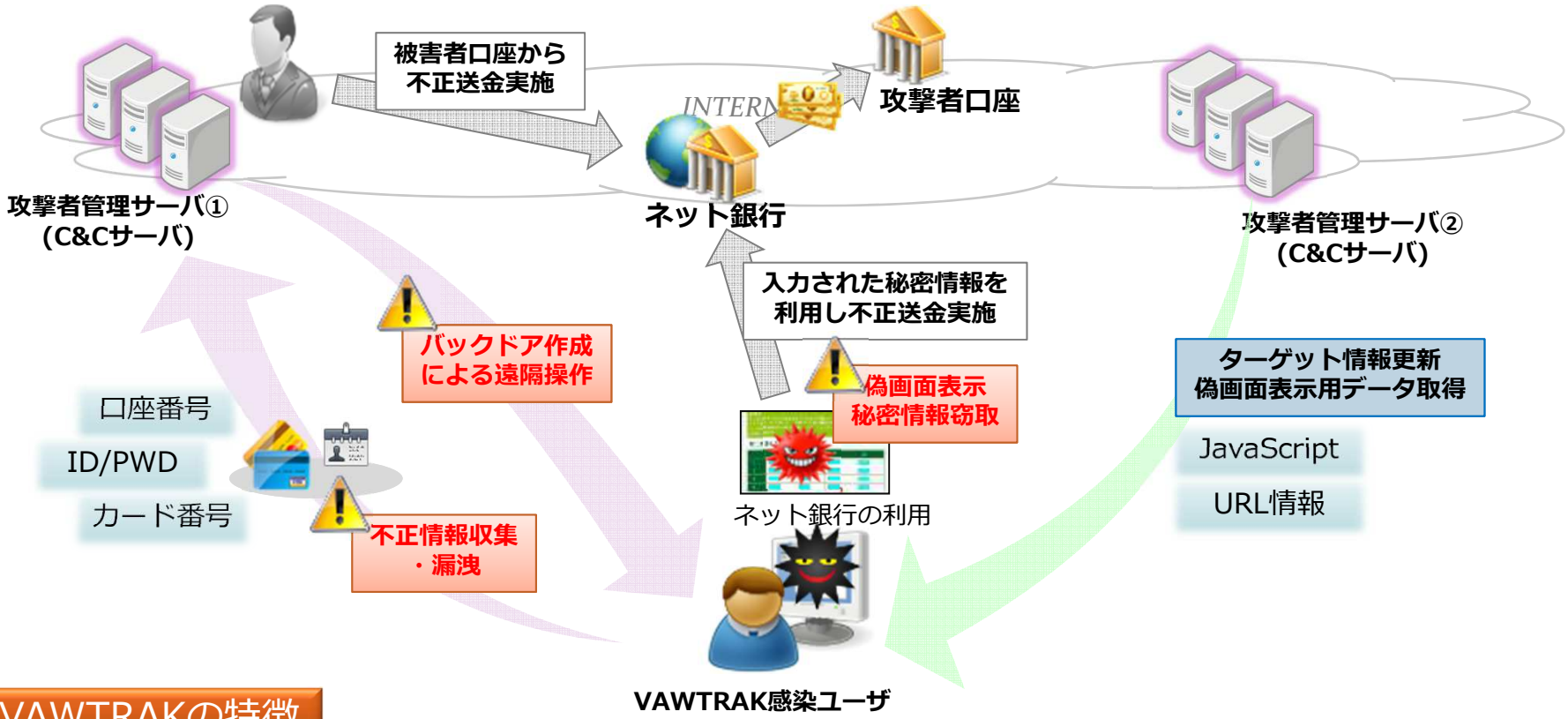
日本独自でこのような大規模なボットネット（ウイルスのネットワーク）をテイクダウン（撲滅）する取組は初めてです。当課ではこれを「ネットバンキングウイルス無力化作戦」と名付け、セキュリティ事業者の協力を得て、ウイルス感染端末の不正送金被害を防ぐための対応策を講じています。



（出典）
http://www.keishicho.metro.tokyo.jp/haiteku/haiteku/haiteku504.htm

VAWTRAKの脅威　動作概要

- VAWTRAKはインターネットバンキングの個人情報を狙うネットバンキングウイルスであり、感染端末内の不正な情報収集や偽画面表示、不正送金等の機能を持っており、ユーザに対して金銭被害も含めた大きな被害を与え得る。



VAWTRAKの特徴

- PC上に保存されているユーザ情報の窃取
- 偽画面による秘密情報（ID,パスワード等）の窃取および不正送金の実施
  ⇒送金処理に必要な認証情報の入力を促す画面を表示しワンタイムパスワードでの対策を回避
- ターゲット情報および偽画面表示用データの自動取得

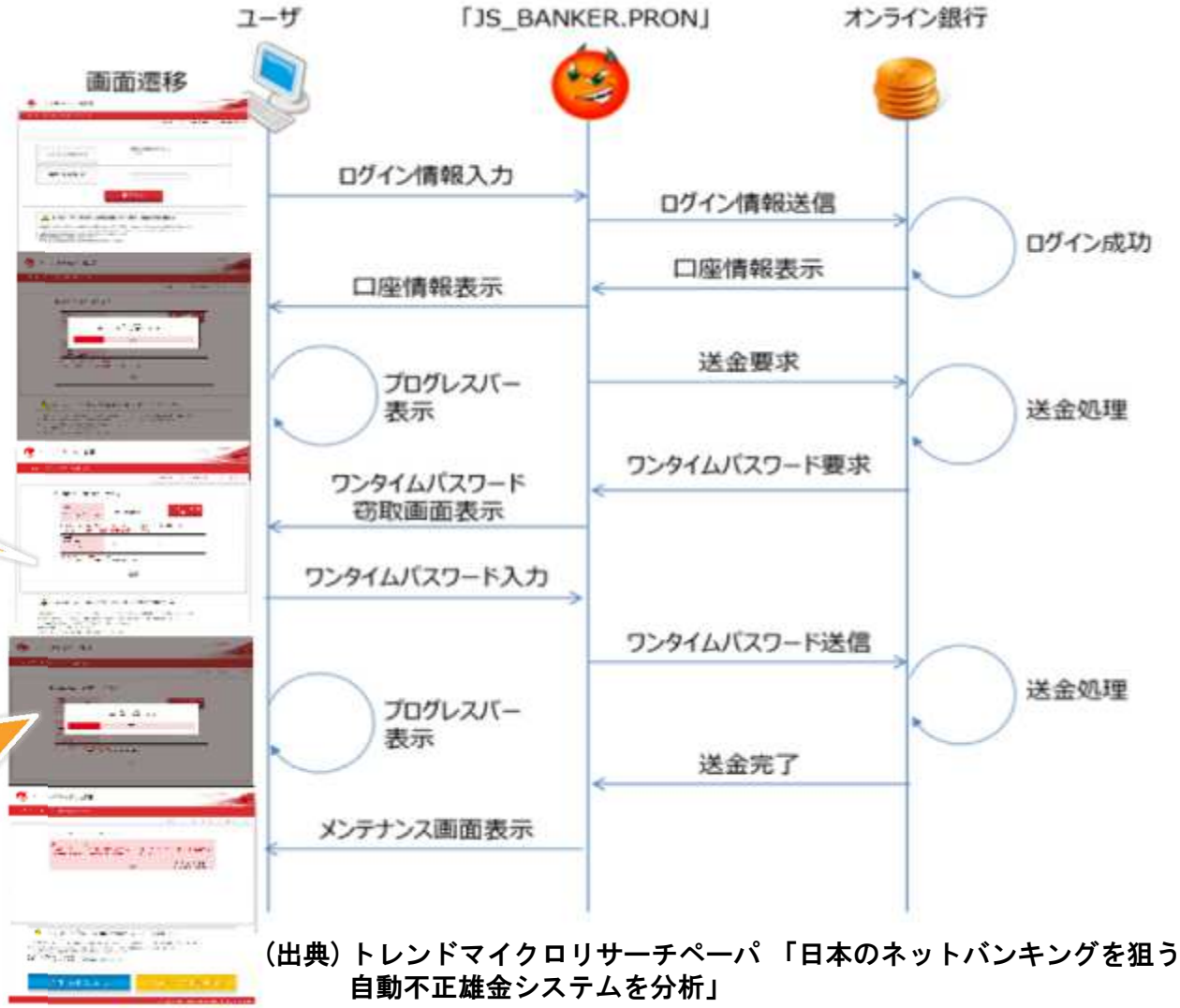
VAWTRAKの脅威

偽画面による不正送金時の画面遷移フロー

- VAWTRAKは送金処理に必要な情報を窃取する偽画面とプログレスバーを交互に表示させることで、感染端末利用者の気づきを阻害しワンタイムパスワード等の二要素認証を突破する仕組みとなっている。

追加の認証情報が必要になると情報入力を促す別の偽画面を表示
※ワンタイムパスワード以外でも「生年月日」「多段認証」の入力を促す偽画面が確認されている

画面遷移時にプログレスバーが表示されるのがVAWTRAKの最大の特徴



（出典）トレンドマイクロリサーチペーパ 「日本のネットバンキングを狙う自動不正雄金システムを分析」

T-ISAC-JおよびACTIVEでの協力活動

- Telecom-ISAC Japanは総務省と連携し、警視庁から提供される感染端末情報からACTIVEを通じてVAWTRAKに感染している利用者へ注意喚起を行っている。

（出典）
http://www.soumu.go.jp/main_content/000352800.pdf

まとめ

- 2014年5月、トレンドマイクロ社よりインターネットバンキングユーザを対象に攻撃する「VAWTRAK」の検出数増加の注意喚起が行われた。同社発表の2014年1～6月期の日本国内感染台数と、警察庁から発表された同時期の不正送金被害額（約18億5200万円[前年比9倍]）の関係から、一部報道ではVAWTRAKによる被害がその大半を占めるとの見方がされた。
  2015年4月10日には警視庁よりネットバンキングウイルス無力化作戦として、特定されている感染端末とそれらを撲滅する取り組みについて発表された。

- VAWTRAKは以下の特徴を持ち、感染端末内の不正な情報収集や偽画面表示、不正送金等を行うことでユーザに対して金銭被害も含めた大きな被害を与え得る。
  ・PC上に保存されているユーザ情報の窃取
  ・偽画面による秘密情報（ID，パスワード，証明書等）の窃取、および不正送金の実施
  ・ターゲット情報および偽画面表示用データの自動取得

- 投影のみ

- Telecom-ISAC Japanはネットバンキングウイルス無力化作戦の一環として、総務省および通信事業者と連携し、ACTIVEを通じた感染者への注意喚起を行っている。

［参考］

VAWTRAK作戦発表を受けたメディア等の動き

■ 警視庁発表後、各メディアでの報道が続いた

時刻	メディア	タイトル	URL
9:46	時事通信社	感染PC、国内外8万2千台＝被害防止でウイルス無力化―ネット銀不正送金・警視庁	http://headlines.yahoo.co.jp/hl?a=20150410-00000028-jij-soci
10:12	日本経済新聞	警視庁、不正送金ウイルス無力化　民間とプログラム開発	http://www.nikkei.com/article/DGXLASDG09HA2_Q5A410C1MM0000/
10:25	47news	新種ウイルス感染の端末８万台超　ネット銀の不正送金被害	http://www.47news.jp/CN/201504/CN2015041001001161.html
11:03	産経WEST	新種ウイルス感染８万台超　ＭＩＴＢ攻撃でネット銀不正送金　石川の女性被害確認　警視庁、駆除呼び掛け	http://www.sankei.com/west/news/150410/wst1504100038-n1.html
11:46	NHK NEWSweb（首都圏）	ネットバンキングに新ウイルス	http://www3.nhk.or.jp/shutoken-news/20150410/3892021.html
11:48	毎日新聞	新種ウイルス:ワンタイムパスワード無効化…感染８万台超	http://mainichi.jp/select/news/20150410k0000e040191000c.html
12:07	NHK NEWSweb	不正送金の新種ウイルス ＰＣ８万台余感染	http://www3.nhk.or.jp/news/html/20150410/k10010043791000.html
12:44	朝日新聞デジタル	ワンタイムパスワードでも被害　不正送金の新ウイルス	http://www.asahi.com/articles/ASH4B2VCCH4BUTIL005.html?iref=comtop_6_01
13:08	TBS（JNN）	国内外８万２０００台のパソコン、新種ウイルスに感染	http://headlines.yahoo.co.jp/videonews/jnn?a=20150410-00000038-jnn-soci http://news.tbs.co.jp/newseye/tbs_newseye2465842.html
13:40	テレビ朝日	不正送金ウイルス　国内外“8万台以上”のPCが感染	http://news.tv-asahi.co.jp/news_society/articles/000048165.html
13:59	東京新聞	不正送金　新ウイルス　８万台感染　無力化作戦　動きだす	http://www.tokyo-np.co.jp/s/article/2015041090135913.html

［参考］

VAWTRAK作戦発表後のTwitter上の反応

- Twitter上でも警視庁発表以降、HPを参照するツィートが相次いでおり、本作戦への関心が伺える

(出典)
https://twitter.com
http://realtime.search.yahoo.co.jp/

[参考] 総務省HP(4/10 14:00)

マルウェアへの感染者に対する注意喚起の実施

総務省
MIC Ministry of Internal Affairs and Communications

ご意見・ご提案 English Google™カスタム検索 サイト内
ここに検索語句を入力

総務省トップ > 広報・報道 > 報道資料一覧 > 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

報道資料

平成27年4月10日

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

近年、コンピュータのマルウェア※感染を原因とするインターネットバンキングの不正送金被害が増加し続けており、これを踏まえて、我が国においてインターネットバンキングに係るマルウェアの駆除作戦が行われます。
総務省は本作戦に協力し、「官民連携による国民のマルウェア対策支援プロジェクト（プロジェクト名：Advanced Cyber Threats response InitiatIVE(略称「ACTIVE」)」を通じた感染者への注意喚起を実施します。
※マルウェア：悪意のあるソフトウェアの総称であり、コンピュータに感染することによって、不正送金や情報窃取などの遠隔操作を自動的に実行するプログラムのこと。

1 経緯等

近年、インターネットバンキングを通じた不正送金事案が多発しており、昨年一年間の被害総額が前年の被害額を上回る等、その被害も拡大傾向にあります。
不正送金事案の多くはコンピュータへのマルウェア感染が原因であり、これらの不正送金事案への対策として、警視庁においてインターネットバンキングに関するマルウェア（VAWTRAK）の駆除作戦の実施について発表がありました。
本作戦により、感染端末の特定が可能になることから、総務省は安心・安全なネットワーク環境の実現を図るため、本作戦への協力として、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連携し、当省が実施しているプロジェクト「ACTIVE」を通じて、当該マルウェアに感染している利用者への注意喚起を行います。

2 実施内容

本作戦において得られた当該マルウェアへの感染端末に関する情報を元に、「ACTIVE」の取組を活用して、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、国内インターネット・サービス・プロバイダ（ISP）事業者に対して感染者に関する情報提供を行い、各ISP事業者から利用者への注意喚起を実施します。（別紙参照）

<関係情報>

○ ネットバンキングウイルス無力化作戦の実施について（警視庁発表資料）
http://www.keishicho.metro.tokyo.jp/haiteku/haiteku/haiteku504.htm

連絡先

情報流通行政局情報流通振興課
情報セキュリティ対策室
（担当：堀川課長補佐、本田係長）
電話：03-5253-5749（直通）
FAX：03-5253-5752

(出典) http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000092.html

[参考] Telecom-ISAC Japan(4/10 14:00)
インターネットバンキングに係るマルウェア（VAWTRAK）感染端末利用者に対する注意喚起について

Telecom-ISAC Japan
Telecom Information Sharing and Analysis Center Japan

2015/04/10

インターネットバンキングに係るマルウェア(VAWTRAK)感染端末利用者に対する注意喚起について

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。

インターネットバンキングの不正送金被害は、昨年(平成26年)一年間で1，876件、被害額は約29億円と過去最悪を記録しており、その手口もますます悪質・巧妙化しています。不正送金被害の多くはコンピュータへのマルウェア(不正なプログラム)感染によるものです。今回、警視庁サイバー犯罪対策課において、主に日本のインターネットバンキングを標的としているとみられるマルウェア「VAWTRAK」の感染端末に関する情報を入手したことから、当該マルウェアを駆除する作戦を発表しています。

本作戦の実施に当たり警視庁より総務省並びにTelecom-ISAC Japanに対し協力の依頼があったことを受け、Telecom-ISAC Japanでは総務省と連携し、平成25年11月1日より実施している「官民連携による国民のマルウェア対策支援プロジェクト(ACTIVE)」の取り組みを活用して、ACTIVEに参加する国内ISP事業者に対して感染端末に関する情報を提供し、当該マルウェアに感染している端末利用者への注意喚起に協力することと致します。

(出典) https://www.telecom-isac.jp/news/news20150410.html

[参考] ACTIVE(4/10 14:00)
インターネットバンキングに係るマルウェア（VAWTRAK）感染端末利用者に対する注意喚起について

ニュースリリース

ホーム › Activeについて › ACTIVEからの最新のお知らせ › ニュースリリース › インターネットバンキングに係
対する注意喚起について

ニュースリリース 2015/04/10

インターネットバンキングに係るマルウェア（VAWTRAK）感染端末利用者に対する注意喚起について

総務省、複数の国内インターネット・サービス・プロバイダ（ISP）事業者、およびセキュリティベンダ等の事業者は、国内のインターネット利用者を対象に、 マルウェア駆除の注意喚起をする等の実証実験を行う官民連携プロジェクト（ACTIVE: Advanced Cyber Threats response InitiatiVE）に取り組んでおります。

インターネットバンキングの不正送金被害は、昨年（平成26年）一年間で1,876件、被害額は約29億円と過去最悪を記録しており、その手口もますます悪質・巧妙化しています。不正送金被害の多くはコンピュータへのマルウェア（不正なプログラム）感染によるものです。今回、警視庁サイバー犯罪対策課において、主に日本のインターネットバンキングを標的としているとみられるマルウェア「VAWTRAK」の感染端末に関する情報を入手したことから、当該マルウェアを駆除する作戦を発表しています。

本作戦の実施に当たり警視庁より協力依頼があったことを受け、平成25年11月1日より実施しているACTIVEの取組を活用して、ACTIVEに参加する国内ISP事業者に対して感染端末に関する情報提供を行い、各ISP事業者から当該マルウェアに感染している端末利用者への注意喚起を実施します。

(出典)
http://www.active.go.jp/active/news/release/entry-231.html

ご静聴ありがとうございました。

nishibe@telecom-isac.jp
(y.nishibe@ntt.com)