Internet Week 2015
S9 ISPによる昨今のセキュリティ事案対応と通信の秘密のガイドライン

「電気通信事業者におけるサイバー攻撃等への対処と通信の秘密に関するガイドライン」の改定によるISPの新たな取組

2015年11月18日

北村 和広
Telecom-ISAC Japan ACTIVE業務推進WG 主査
エヌ・ティ・ティ・コミュニケーションズ株式会社

本セッションの説明内容

■目的

改定予定の「電気通信事業者におけるサイバー攻撃等への対処と通信の秘密に関するガイドライン」について、 改定により可能になったことを中心に説明します。

■目次

- Telecom-ISAC Japanの概要
- ISPにおけるサイバー攻撃への対処
  - -ACTIVEの取組概要
  - -これまでのガイドラインを踏まえてACTIVEで取り組んだこと
  - -脆弱性を有するブロードバンドルータ問題
- 今回のガイドライン改定後の新たな取組
  - -ガイドライン改定以前で制限されていたこと
  - -ACTIVEの新たな取組
    - ガイドラインの事例（マルウェア被害未然防止の取組）
  - -脆弱性を有するブロードバンドルータ問題
    - ガイドラインの事例（脆弱性を有するブロードバンドルータに対する注意喚起）

Telecom-ISAC Japan の概要

Telecom-ISAC Japanの概要

Telecom-ISAC Japan
Telecom Information Sharing and Analysis Center Japan

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(jpドメイン)」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
- 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

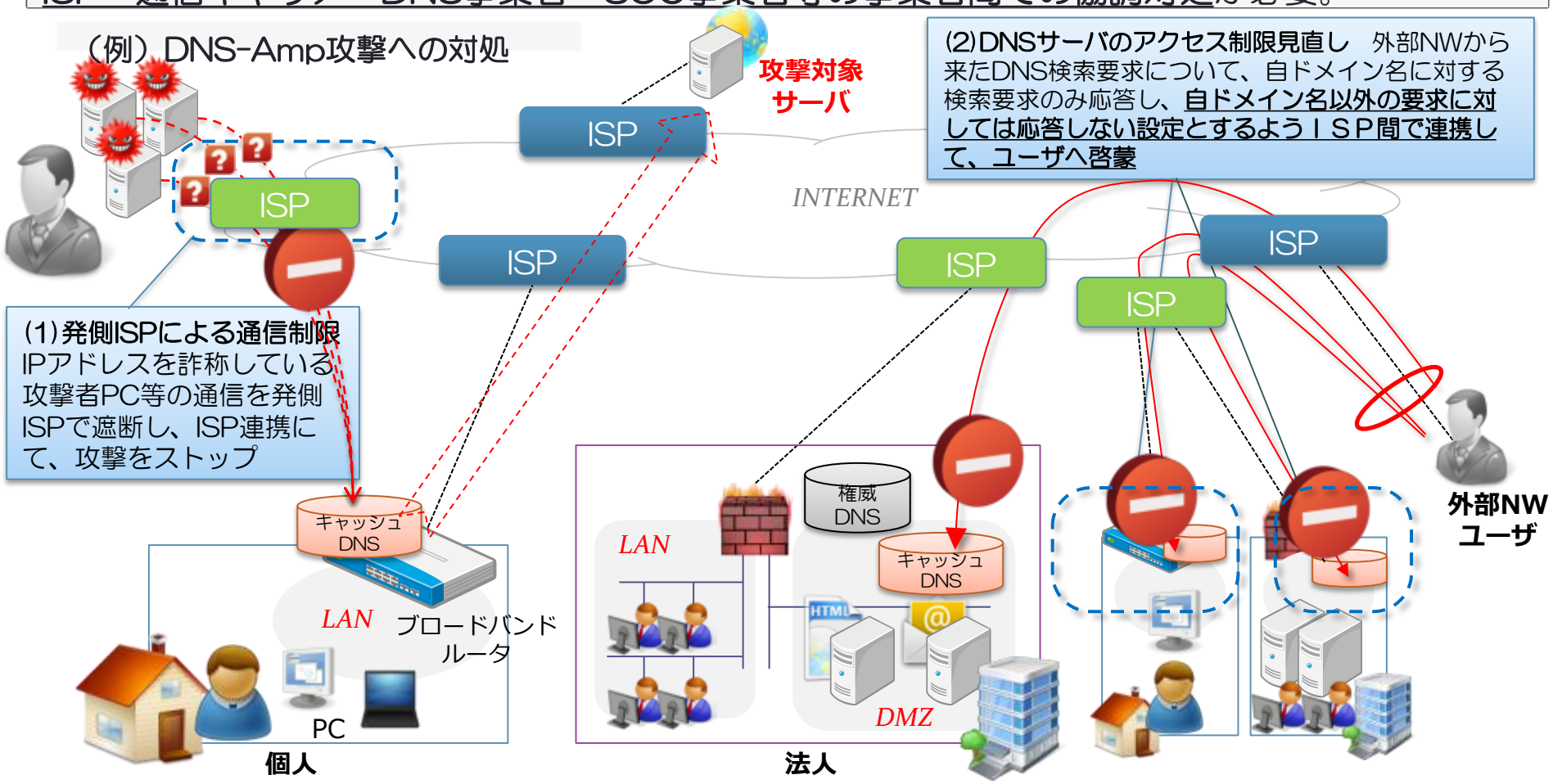
会員企業（2015年10月末現在）

緑文字はISP or 通信事業者を示す

会長：	飯塚　久夫
副会長：	KDDI株式会社、NTT コミュニケーションズ株式会社、一般財団法人日本データ通信協会
会員企業：(20)	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 、ビッグローブ株式会社 、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コムセキュリティ株式会社、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 株式会社ケイ・オプティコム
アライアンスメンバー：(11)	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 日本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：(5)	総務省、国立研究開発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処の必要性

昨今、大規模化・多様化し続けるサイバー攻撃に対し、組織単独での対応には限界がある。
ISP・通信キャリア・DNS事業者・SOC事業者等の事業者間での協調対処が必要。



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。

ＩＳＰにおけるサイバー攻撃への対処

ACTIVEの取組概要

マルウェアに関する官民連携事業（施策）

マルウェアの変遷

ボット

インターネットにつないだだけで、インターネット利用者の知らない間に感染するボットが主流

Drive-by-download

Webを見ただけで感染するWeb感染型マルウェアが台頭

より高度で多様なマルウェア

より高度で多様なマルウェアが次々と出現

対応方策の変遷

Cyber Clean Center

2006~2010年度

Cyber Clean Center ボット対策プロジェクト

RDB　2009~2011年度

マルウェア配布等危害サイト回避システムの実証実験

Advanced Cyber Threats response InitiatiVE

2013~2017年度

ACTIVE Advanced Cyber Threats response InitiatiVE

マルウェア感染防止・駆除の取組

2013~2014年度ACTIVE取組

ACTIVE（Advanced Cyber Threats response InitiatiVE）

総務省主管の国民のマルウェア対策支援プロジェクト

- 2013年11月1日開始
- 【目的】マルウェア感染の削減等により、安心・安全なインターネットの実現を目指す
- マルウェア感染防止から駆除まで一貫して取り組む総合的なマルウェア感染対策であり、官民連携により行う同様のプロジェクトは世界初の試み

http://www.active.go.jp

主な取組

マルウェア感染防止の取組

① マルウェア配布サイト等のURL情報をリスト化
② マルウェア配布サイト等にアクセスしようとする利用者に注意喚起
③ マルウェア配布サイト等の管理者に対しても適切な対策を取るように注意喚起

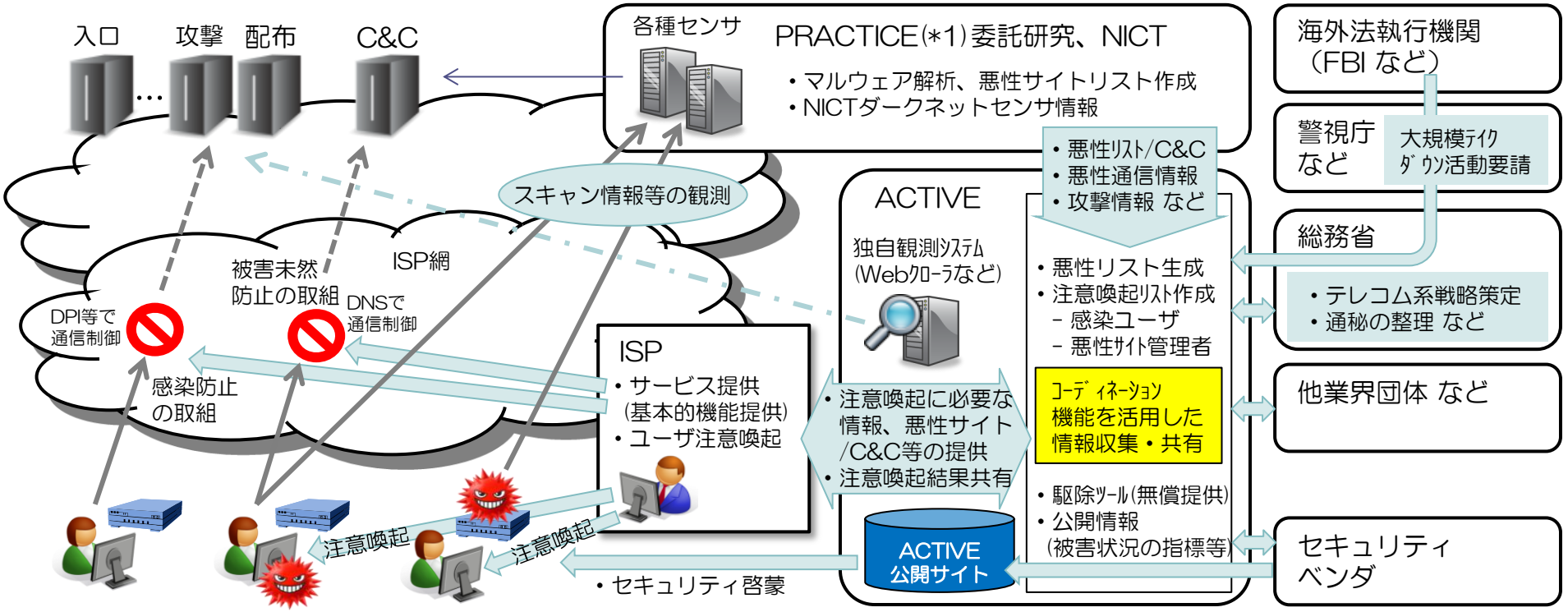
マルウェア駆除の取組

① マルウェアに感染した利用者のPCを特定
② 利用者に適切な対策を取るように注意喚起
③ 利用者は、注意喚起の内容に従いPCからマルウェアを駆除

2015年度ACTIVE取組

悪性サイトリストを用いた注意喚起　（★新規取組）
- マルウェア感染防止の取組（マルウェア配布サイト等をISP網で通信制御し、利用者へ注意喚起）
- ★ マルウェア被害未然防止の取組（C&Cサーバを ISPで通信制御。利用者へ対策を取るように注意喚起）
- 悪性サイト管理者への注意喚起

マルウェア駆除を案内する注意喚起
- 情報通信研究機構（NICT）のダークネットセンサ情報を用いた駆除の取組
- 業界全体の大規模テイクダウン活動



(*1) サイバー攻撃に関する情報を収集・分析の上、情報共有を行い、サイバー攻撃発生の予知・即応を可能とする技術を確立する総務省プロジェクト

マルウェア感染に関する注意喚起の概要（2015年度）

注意喚起分類	取組内容	感染経路(*1)			変遷
		Web	NW	他	
悪性サイトリストを用いた注意喚起	①マルウェア感染防止の取組 - マルウェア配布サイト等(*2)をISP網で通信制御し、利用者へ注意喚起 - 制御機器： DPI、Proxy、ツールバー（URL完全一致） - Webクローラを用いて、リストをACTIVE事務局で生成	○	―	―	拡大
	②マルウェア被害未然防止の取組 - C&Cサーバを ISPで通信制御。利用者へ対策を取るように注意喚起 - 制御機器： DNS（FQDN一致） ： DPI、Proxy（URL完全一致）	○	○	○	新規 (*3)
	③悪性サイト管理者へ注意喚起 - ①②のリストのうち国内のサイト管理者へ注意喚起	○	○	○	拡大
マルウェア駆除を案内する注意喚起	④ハニーポットを用いた駆除の取組 - Windows XPの脆弱性を狙うNW感染経由の攻撃が減少しているため、本取組は2014年度末に終了	―	○	―	終了
	⑤NICTダークネットセンサ情報を用いた駆除の取組 - 2014年度： 特定のマルウェアを対象に試行し、有効性を確認 - 2015年度： ④の取組後継として本格運用	―	○	―	拡大
	⑥業界全体の大規模テイクダウン活動 - 2014年度実績： Game Over Zeus - 2015年度実績： VAWTRAK	○	○	○	継続

(*1) Web： 悪性サイトへ通信して感染、 NW： NW経由で感染、 他：メール添付やUSB経由など
(*2) 入口サイト、中継サイト、攻撃サイト含む
(*3) 通信の秘密が整理された後に、取組み可能（業界ガイドライン策定後）

これまでのガイドラインを踏まえてACTIVEで取り組んだこと

ACTIVEにおける「通信の秘密」との関係（整理済）

総務省「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会」の公開資料抜粋　http://www.soumu.go.jp/main_content/000264105.pdf

（１）マルウェア感染防止の取組

① マルウェア配布サイトのURL情報をリスト化。
② マルウェア配布サイトにアクセスしようとする利用者に注意喚起。
③ マルウェア配布サイトの管理者に対しても適切な対策を取るよう注意喚起。

通信の秘密との関係

ISP等が、利用者がアクセスしようとするサイトのURLの情報を知得し、注意喚起を行うことについては、利用者の同意に基づいて行われており、通信の秘密の侵害にあたらない。

（２）マルウェア駆除の取組

① マルウェアに感染した利用者のPCを特定。
② 利用者に適切な対策を取るよう注意喚起。
③ 注意喚起の内容に従いPCからマルウェアを駆除。

通信の秘密との関係

① ACTIVE事務局が、マルウェア感染パソコンからハニーポットに来た通信における送信元IPアドレスを、当該IPアドレスの割当てを行っているISPに提供することは、ACTIVE事務局は当該通信を受信する一方当事者であり、通信の秘密の侵害にあたらないと考えられる。

② 上記ISPが、当該IPアドレスをどの契約者に割り当てたか顧客情報と突合し、該当契約者を割り出す行為は、マルウェア感染パソコンに対する現在の危難を避けるための緊急避難として、通信の秘密の侵害に係る違法性は阻却されると考えられる。

ACTIVEにおける「通信の秘密」との関係（整理済）

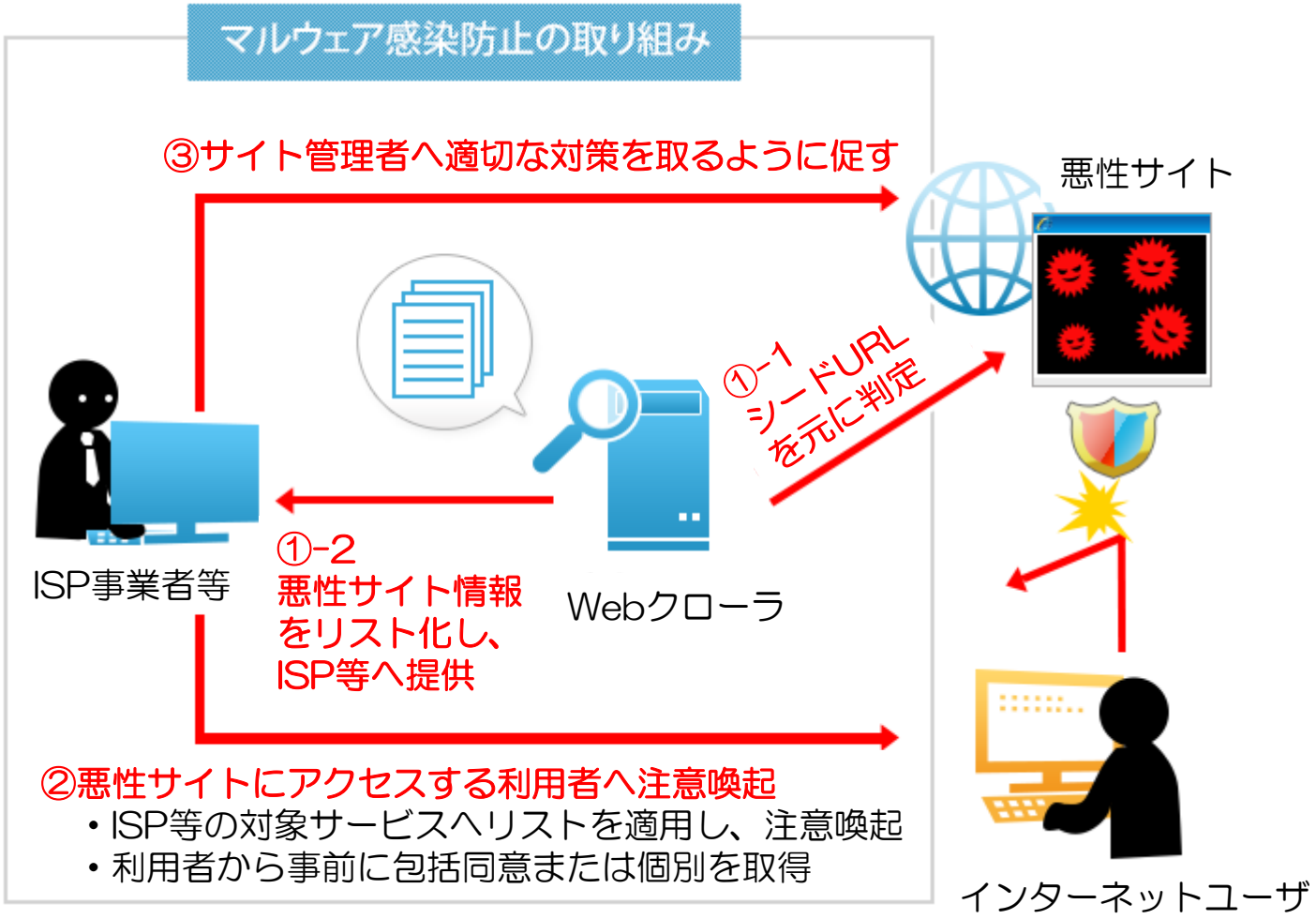
電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会
http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000074.html

- 研究会で整理された事項のうち、関係する内容（下表 1項と2項）についてはACTIVEの取組で実施。

	検討課題	通信の秘密との関係等の考え方
1	マルウェア配布サイトへのアクセスに対する注意喚起	利用者が、一旦契約約款に同意した後も、随時、同意内容を変更できる（オプトアウトできる）こと等を条件に、契約約款に基づく事前の包括同意であっても有効な同意と整理
2	マルウェア感染駆除の拡大	C&Cサーバに蓄積されている、同サーバとマルウェアに感染したPC等の端末に係る通信履歴からマルウェアの感染者を特定し、注意喚起を実施することは、当該端末が正常かつ安全に機能することに対する現在の危難を避けるための緊急避難として許容される
3	新たなDDoS攻撃であるDNSAmp攻撃の防止	利用者が設置しているブロードバンドルータ等のゲートウェイに対するインターネット側からの名前解決要求に係る通信を遮断することは、電気通信役務の安定的提供を図るための正当業務行為として許容される
4	SMTP認証の情報（ID及びパスワード）を悪用したSPAMメールへの対処	他人のID・パスワードを悪用して送信されるSPAMメールへの対処として、 当該IDの一時停止や、正規の利用者への注意喚起等を実施することは、電気通信役務の安定的提供を図るための正当業務行為として許容される

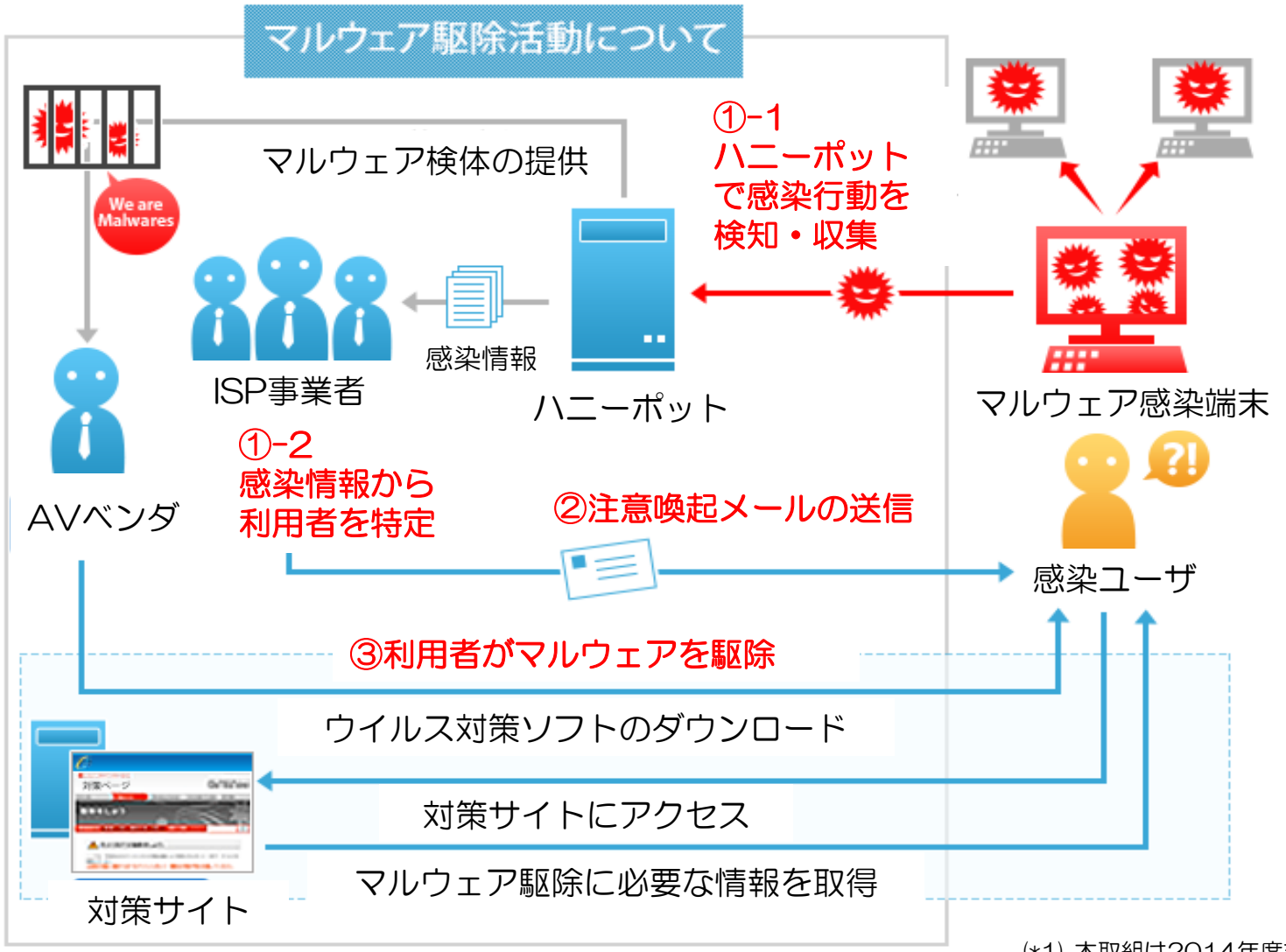
ACTIVEにおけるマルウェア感染防止の取組

マルウェア感染防止の取り組み
- 各社の対象サービスに対して、利用者から事前に包括同意または個別の同意を取得



ACTIVEにおけるマルウェア駆除の取組

マルウェア駆除の取り組み

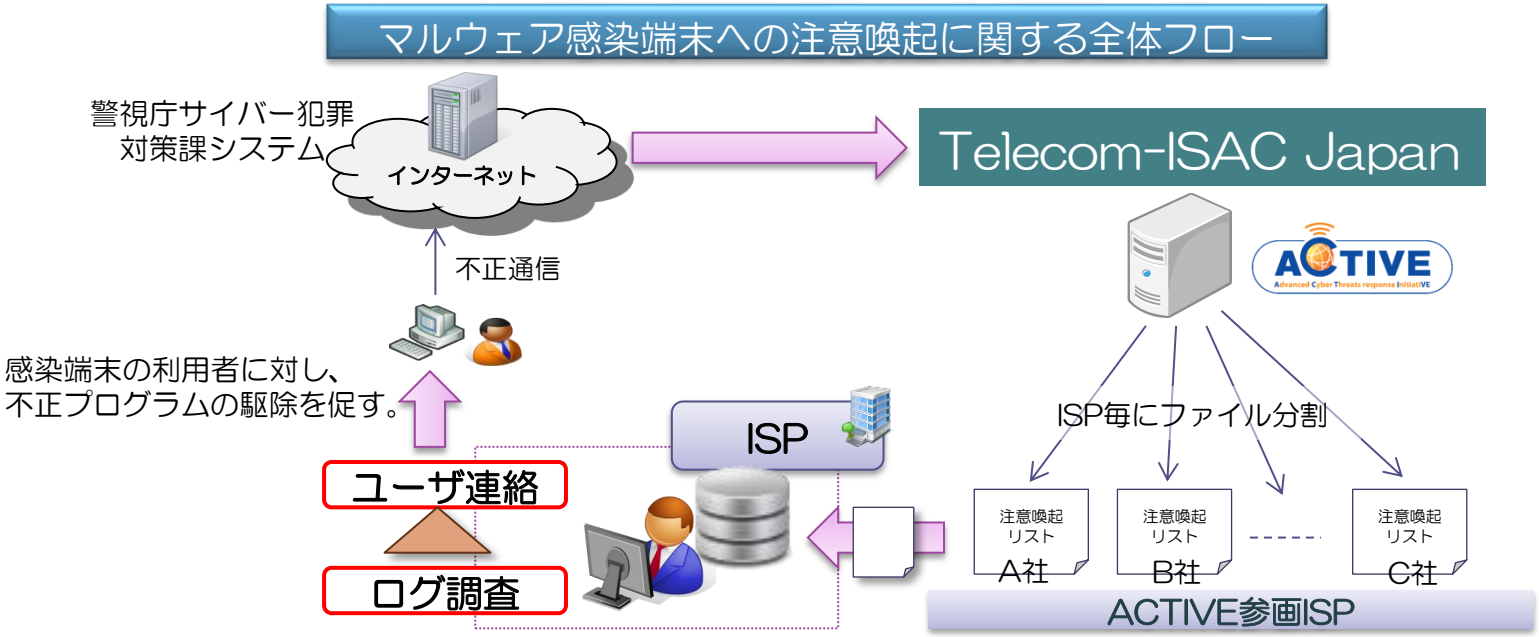


(*1) 本取組は2014年度末に終了

業界全体の大規模テイクダウン活動

①目的
警視庁等の他組織・団体からの要請に基づく大規模テイクダウン活動に参画することで、マルウェア感染端末の撲滅を目指す。

②実施概要
インターネットバンキングに係るマルウェア（Game Over ZeusやVAWTRAK）に関する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実績の活用により、参画ＩＳＰ事業者に対して感染者に関する情報提供を行う。また、複数の参画ＩＳＰ事業者から利用者への注意喚起を実施した知見を最大限に活用することで、より多くのＩＳＰ事業者の参加による注意喚起が可能となるよう取り組む。



ACTIVEの注意喚起スキームを有効活用することで、効率的な情報提供を実現。
インターネットバンキングマルウェアの駆除に貢献する。

業界全体の大規模テイクダウン活動
警察情報によるGame Over Zeus駆除について

インターネットバンキング不正送金に使用されるマルウェア「Game Over Zeus」が世界的に蔓延している状況に対し、**米国連邦捜査局（FBI）及び欧州刑事警察機構（ユーロポール）**が中心となり、日本を含む協力国の法執行機関と連携した大規模なボットネットテイクダウン作戦が行われている。本作戦では犯行者が使用する関連サーバの押収と共に、より多くの感染端末の特定・注意喚起を行うことでマルウェア駆除・感染端末の減少を目指している。

(出典)
http://www.fbi.gov/news/stories/2014/june/gameover-zeus-botnet-disrupted

(出典)
http://www.npa.go.jp/cyber/goz/

作戦の内容

- C&Cサーバ・中継サーバのテイクダウン
- テイクダウンしたC&Cサーバ上で感染端末からの通信を観測し、当該ユーザへの注意喚起を行う。

業界全体の大規模テイクダウン活動
警察情報によるGame Over Zeus駆除について

2014年6月3日、警察庁がFBI及びユーロポールのボットネット駆除作戦に参加する旨公表。

- FBI及びユーロポールが中心となって、国際的なネットバンキングマルウェア、Game Over Zeus（GOZ）の感染駆除作戦を決行し、日本も参加。
- 本作戦は、関連サーバを押収し、当該ネットワークの管理者を起訴するとともに、より多くの感染端末を特定し、プロバイダ等を通じて感染端末の利用者に対して不正プログラムの駆除を促し、感染端末の減少を目指すもの。
- FBIによれば、感染端末は世界で約100万台存在し、そのうちの20%（約20万台）が日本に存在。

当時の情報を整理すると以下の通り。

- 警察庁は本作戦に参加するため、各都道府県警察を通してISPに対して以下を依頼。
  ① ISPによる特定のドメイン（.ruドメイン）へのアクセスの遮断
  ② GOZの2次プロキシとなっている感染端末※のテイクダウン
  ※世界で約4,000台存在し、その約800台が日本に存在。
- FBIが把握した感染端末の情報はUS-CERTを通じてJPCERT/CCに提供され、JPCERT/CCから各ISPに対して利用者への注意喚起の依頼が行われる予定。

業界全体の大規模テイクダウン活動
警察情報によるGame Over Zeus駆除について

警察庁・総務省およびTelecom-ISAC Japanにおける調整の結果、JPCERT/CCや警察など複数の関係者からISP各社に連絡を行うことは負担が大きいと判断し、Telecom-ISAC Japanが主管するACTIVEにて本案件の窓口・とりまとめを行う次第となった。

ISP各社の対応内容

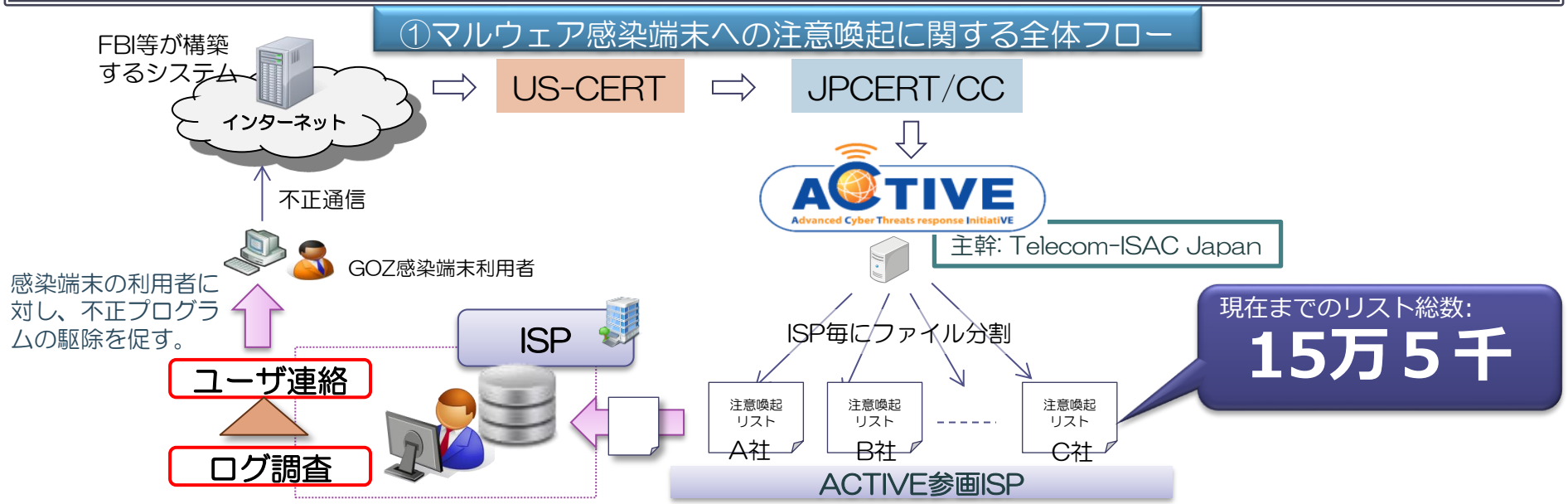
① **マルウェア感染端末への注意喚起について**

JPCERT/CCからの情報をTelecom-ISAC Japanが窓口として一元的に受け取ったのち、総務省「ACTIVE」のデリバリラインを活用して各ISPに対して情報提供を行う。情報を受け取った各ISPにおいて対処を実施して頂く。

② **2次プロキシとなっている感染端末（約800台）のテイクダウンについて**

各ISPにおいて各都道府県警からの依頼に基づき、各社の判断で必要な対応がとられているが、必要に応じてTelecom-ISAC Japanでも個別に対応の相談を受け付ける。

①マルウェア感染端末への注意喚起に関する全体フロー



ACTIVEの注意喚起スキームを有効活用することで、効率的な情報提供を実現
インターネットバンキングマルウェアの駆除に貢献

業界全体の大規模テイクダウン活動
警察情報によるGame Over Zeus駆除について

インターネットバンキングに係るマルウェア（Game Over Zeus）に関する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、国内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。

リスト配布先：　１４の協力先に配布

	1回目	2回目	3回目	4回目	合計
JPCERT/CC からの受領数	1,320	19,482	46,718	88,001	155,521
ISP	1回目	2回目	3回目	4回目	小計
１４協力先への送付合計	839	13,028	31,725	58,647	104,239
	1回目	2回目	3回目	4回目	合計
JPCERT/CC　への返却数	481	6,454	14,993	29,354	51,282
T-ISAC-J　での対応率	63.6%	66.9%	67.9%	66.6%	67.0%

複数のISP事業者に対し、４回にわたり情報提供を行い、合計104,239の感染端末情報を提供

業界全体の大規模テイクダウン活動
警察情報によるVAWTRAK駆除について

インターネットバンキングの不正送金被害は、昨年（2014年）で1,876件、
被害額は約２９億円と過去最悪を記録、その手口に用いられるウイルスもますます悪質・巧妙化。
そこで、感染端末のウイルス駆除をはじめとする各種取組みを実施。

「日本版ボットネットテイクダウン作戦」として展開

※日本独自で大規模なボットネット（ウイルスのネットワーク）をテイクダウンする初の取組みとなった。

ISP各社の対応内容

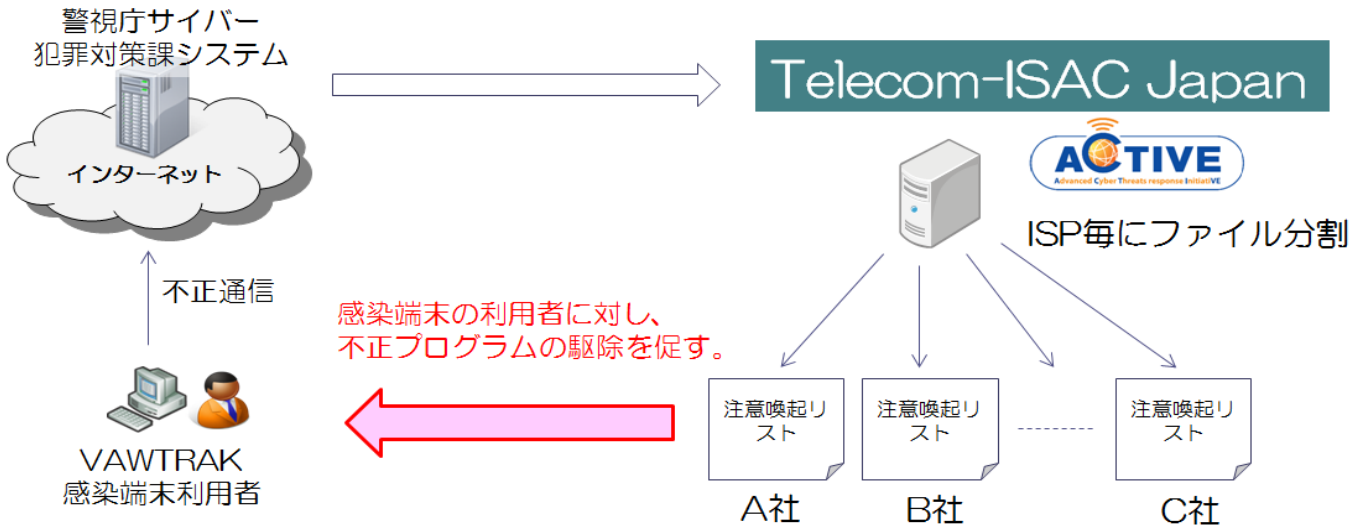
① **マルウェア感染端末への注意喚起について**

警察からの情報をTelecom-ISAC Japanが窓口として一元的に受け取ったのち、総務省実証事業「ACTIVE」のデリバリラインを活用して各ISPに対して情報提供を行い、情報を受け取った各ISPにおいて対処を実施。

② **感染端末のテイクダウンについて**

情報を受け取った各ISPにおいては、各社の判断で必要な対応がとられているが、必要に応じてTelecom-ISAC Japanでも個別に対応の相談を受け付け。

マルウェア感染端末への注意喚起に関する全体フロー



業界全体の大規模テイクダウン活動
警察情報によるVAWTRAK駆除について

インターネットバンキングに係るマルウェア（ VAWTRAK ）に関する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、国内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。

リスト配布先：　１６の協力先に配布

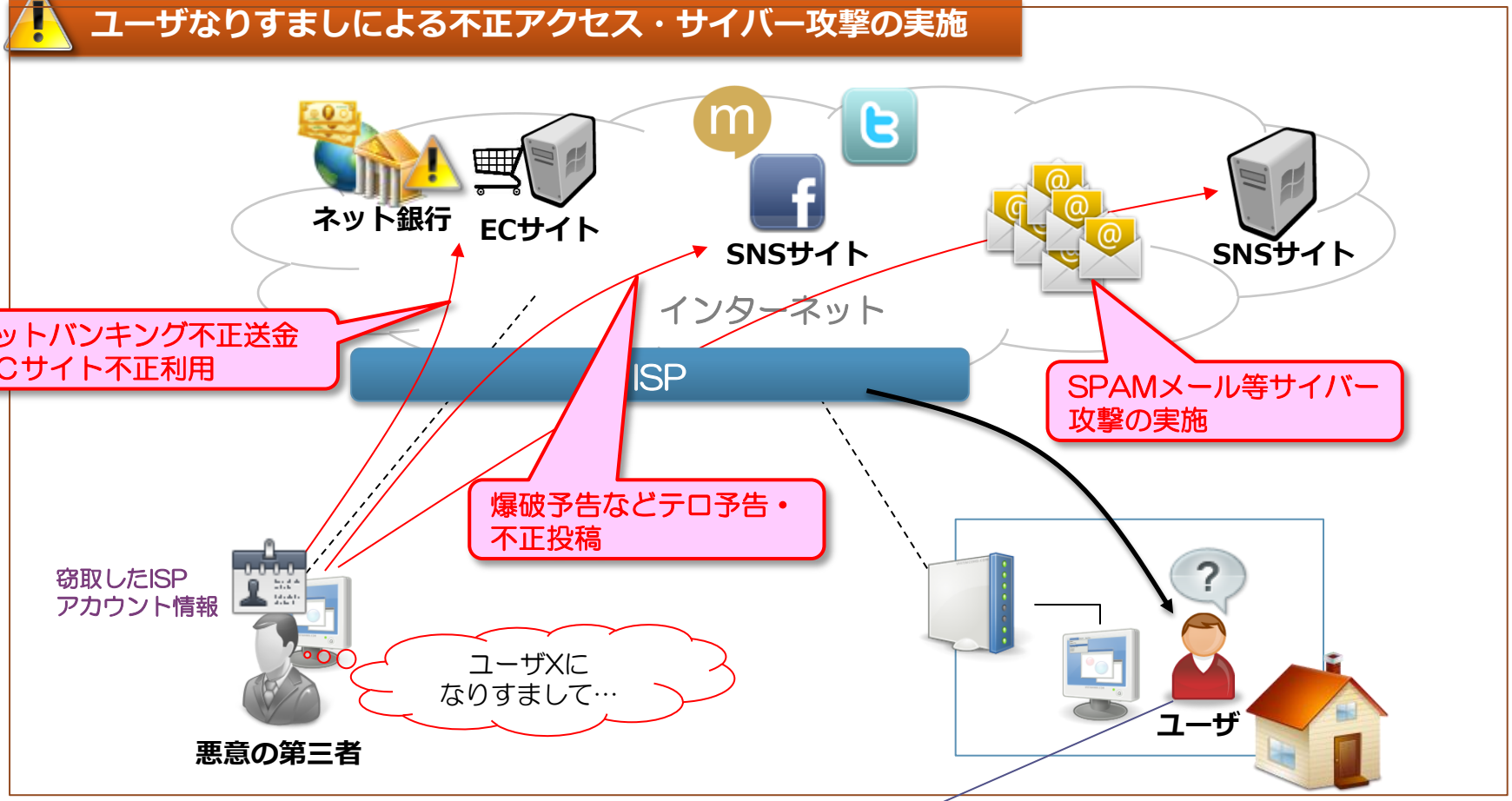
	合計
警視庁からの受領数	43,565
ISP	合計
１６協力先への送付合計	33,196
	合計
警視庁への返却数	10,369
T-ISAC-J　での対応率	76.2%

複数のISP事業者に対し、情報提供を行い、合計33,196の感染端末情報を提供

脆弱性を有するブロードバンドルータ問題

脆弱性を有するブロードバンドルータ問題
発生した被害事案①

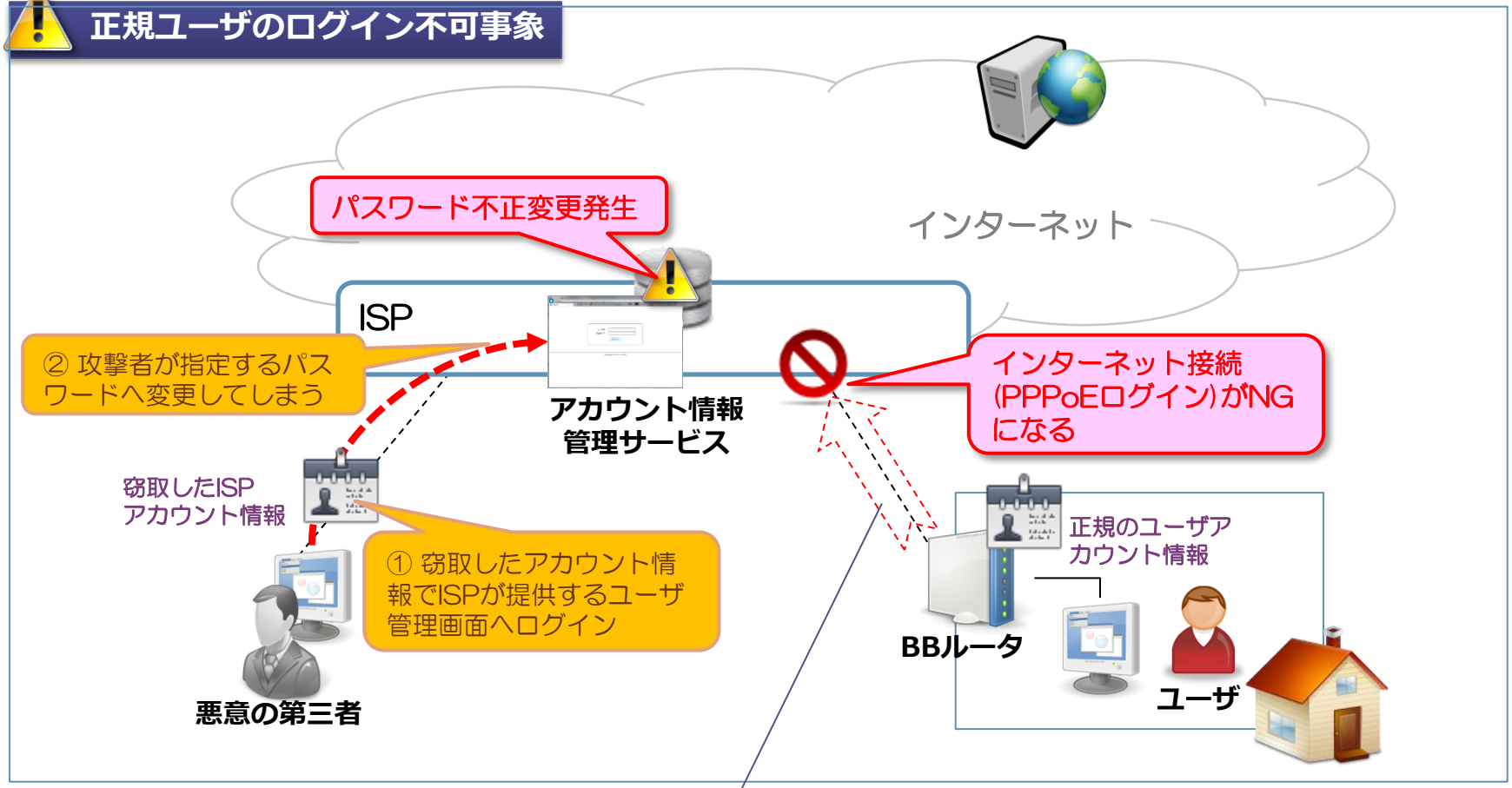
窃取したアカウント情報を利用することにより、攻撃者は別ユーザになりすますことができる。
なりすましは様々なサイバー攻撃の温床となり、攻撃者にとって隠れ蓑になる。



被害サイト等から問合せを受けたISPは不正アクセス元IPアドレスを基にユーザに対して問合せを行うが、ユーザ(アカウント窃取被害者)はサイバー攻撃の事実を知らない

脆弱性を有するブロードバンドルータ問題
発生した被害事案②

既に不正アカウント窃取によって、以下のような事件が発生してしまっている。



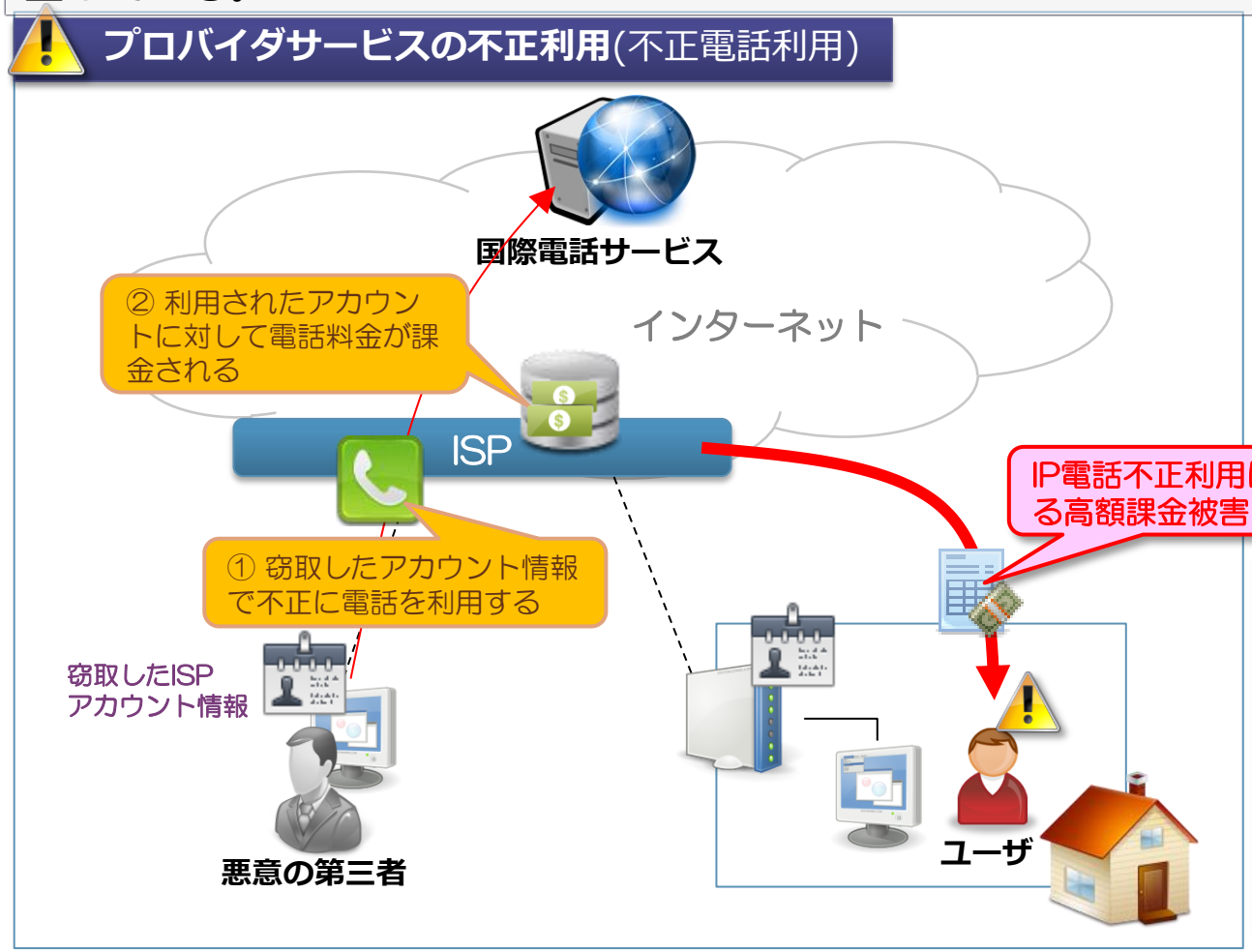
意図せずネット接続がNGとなり、ユーザはISPへ問合せを行う。
※ただし、既に確立済みPPPoEセッションが不正変更後もそのまま残っているケースもあり、不正変更に気づかないユーザも多い。

ユーザ問合せによって、アカウント不正窃取事象が発覚した。

脆弱性を有するブロードバンドルータ問題
発生した被害事案③

ログイン不可事象ばかりではなく、アカウント情報窃取によって金銭被害につながる事件も発生している。

プロバイダサービスの不正利用(不正電話利用)




OCN

2013年6月20日

第三者による不正なIP電話利用にご注意ください

お客さま各位

平素は、OCNサービスをご利用いただき、誠にありがとうございます。

OCNドットフォンおよびOCNドットフォンオフィスにおいて、お客さまのIP電話用のIDとパスワードを第三者が流用し「かけた覚えのない国際通話料金」が発生している、という事例が確認されています。

お客さまにおかれましては、ご利用のIP電話対応機器において必要のないインターネットからのアクセスを許可しない、第三者が容易に推察できないようIDやパスワードを設定する等の対策を行ってください。

なお、お客さま保護の観点より、NTTコミュニケーションズのIP電話から一部の国/地域への発信を一時的に規制させていただく場合がございますのでご了承ください。

また、着信国際通話をご利用にならないお客さまは、国際電話利用休止の付加サービス(無料)を利用することで、国際電話への発信をできないよう規制することも可能です。

「OCNドットフォンの国際電話利用休止についてはこちら

「OCNドットフォンオフィスの国際電話利用休止についてはこちら

NTTコミュニケーションズ株式会社

OCNなど一部のISPでは、実際に不正なIP電話利用の事件が発生しており、アカウント窃取事案との関連が強く疑われる。

(出典) OCN 第三者による不正なIP電話利用にご注意ください
http://www.ocn.ne.jp/voip/announce/20130620.html

脆弱性を有するブロードバンドルータ問題に関するリリース

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）に関するお詫びとお願い
2013年８月20日掲載

Logitec

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) | 会社案内

重要なおしらせ ＜ 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

2013/ 8/20
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願い

＜更新のお知らせ＞ 2014.9.30
お問い合わせ窓口を更新いたしました。

お客様各位

平素は格別のご高配を賜り、厚く御礼申し上げます。

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(LAN-W300N/R, LAN-W300N/RS, LAN-W300N/RU2 ※2013年8月15日現在販売終了済)のセキュリティ脆弱性につきまして、当社ホームページにおいて、該当ルータのファームウェア更新のご案内をさせていただいております。
本ファームウェア更新を実施していない場合、外部からの不正アクセスを受ける等の可能性がございます。該当ルータをお持ちのお客様におかれましては、改めてファームウェアが更新されているか、下記の手順にてご確認いただき、アップデートをいただきますようお願い申し上げます。

また、お客様がご契約されているインターネットサービスプロバイダから、同様の内容が直接お客様の元へご案内がある場合がございます。その場合も下記の手順にて、お使いのルータのファームウェアのバージョンのご確認ならびにアップデートをいただきますようお願い申し上げます。

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、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。

敬具

－ 記 －

■対象製品
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

LAN-W300N/R　LAN-W300N/RS　LAN-W300N/RU2

シリアルナンバー 末尾が「B」
ファームウェア バージョン2.17

■確認と更新の手順

1. 型番とシリアル番号の確認方法
本体側面のカバーを外すと、シールに型番、対象S/N(シリアルナンバー)が記載されています。

くわしくはこちらをご確認ください。(http://qa.elecom.co.jp/faq_detail.html?id=4111&category=5&page=1)

（出典） http://www.logitec.co.jp/info/2013/0820.html

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
2013年８月30日掲載

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一切ありません。
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。

（出典） https://www.telecom-isac.jp/news/news20130830.html

脆弱性を有するブロードバンドルータ問題に関するリリース

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
2013年８月20日掲載

News Release　NTT Communications

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[*1]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[*2]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[*3]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が、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）

NTT コミュニケーションズ株式会社　広報室
NTT Communications Corporation　Public Relations Office
〒100-8019　東京都千代田区内幸町 1-1-6
1-1-6 Uchisaiwai-cho, Chiyoda-ku, Tokyo 100-8019, Japan
Tel [03]6700-4019 International +81 3 6700 4019

（出典）　http://www.ntt.com/release/monthNEWS/detail/20130820.html

NTT Communications　Global ICT Partner
Innovative. Reliable. Seamless.

脆弱性を有するブロードバンドルータ問題に関するリリース

「 OCN認証ID・パスワード流出、Ｌ社製ルーターの脆弱性を突かれた可能性」
INTERNET Watch 2013年８月20日掲載

2015/11/6 OCN認証ID・パスワード流出、ロジテック製ルーターの脆弱性を突かれた可能性 -INTERNET Watch

INTERNET Watch

ニュース

OCN認証ID・パスワード流出、ロジテック製ルーターの脆弱性を突かれた可能性

該当3機種の利用者は、OCN会員に限らずファームウェア確認を

（2013/8/20 13:10）

NTTコミュニケーションズ株式会社（NTT Com）は20日、インターネット接続サービス「OCN」の固定回線ブロードバンド会員（OCN 光、OCN ADSL）を対象に、利用しているブロードバンドルーターのセキュリティ調査をリモートで実施すると発表した。脆弱性のあるルーター製品を使っている会員を割り出し、NTT Comが個別に連絡してルーターのファームウェア更新と、接続認証用パスワードの変更を求める。

OCNでは6月、第三者によるOCN認証ID・パスワードの不正利用が確認されていたが、その流出元が、ロジテック株式会社製の無線LANルーターである可能性が高いことが判明したという。該当する製品は、2009年発売のIEEE 802.11n/b/g対応無線LANルーター「LAN-W300N/R」、その簡易包装版である「LAN-W300N/RS」、同ルーターとUSB無線LANアダプターのセット「LAN-W300N/RU2」の3製品。2013年8月15日現在、販売は終了している。

「OCN認証ID」とは、OCN会員がPPPoEやダイヤルアップなどでインターネット接続する際の認証に用いられるもので、ウェブメールなど各種ウェブサービスへのログインに普段使用する、メールアドレスを用いたIDとは別のものだ。ブロードバンド会員であれば、回線開通後にブロードバンドルーターにOCN認証ID・パスワードを設定したまま、以降、目にしていないという人も少なくないと思われる。

このOCN認証IDのパスワード変更機能などを提供する会員向けウェブサーバーにおいて6月21日～25日、2000件以上のOCN認証IDに対して不正ログイン試行があり、そのうち756件で不正ログインに成功され、パスワードを変更されるという被害が発生していた（本誌2013年6月26日付関連記事を参照）。

NTT Comによると、その被害を受けた会員にヒアリング調査したところ、上記3製品の利用者という点がほぼ共通していることが判明。それら無線LANルーターに設定されていたOCN認証ID・パスワードが、同ルーターの脆弱性を突かれて外部から窃取された可能性が高いと判断した。

該当3機種の利用者は、OCN会員に限らずファームウェア確認を

3製品の脆弱性は、ルーターのアクセス制限に不備があり、インターネット側からルーターの管理ページにアクセスされてしまうというもの。ルーターに設定されているPPPoEの認証IDや認証パスワードなどのISP接続情報が、攻撃者によって取得されたり、変更される可能性がある。

この脆弱性についてはすでに2012年5月の時点で公表されており、ロジテックでは脆弱性を修正したファームウェアを公開。また、これを突いた攻撃活動も確認されているとして、独立行政法人情報処理推進機構セキュリティセンター（IPA/ISEC）や一般社団法人JPCERT/CCコーディネーションセンター（JPCERT/CC）でも注意喚起を行っていた（本誌2012年5月25日付関連記事を参照）。

ロジテックでは今回、8月20日付であらためて3製品の脆弱性について告知し、ファームウェアのバージョン確認・更新を呼び掛けている。NTT Comでも、同社からの連絡を待たずに脆弱性の確認を行いたいOCN会員に対して、ロジテックのウェブサイトを参照するよう案内している。また、今回はOCN認証ID・パスワードの流出元ということでNTT Comがセキュリティ調査を実施するわけだが、他のISPの会員であっても3

（出典） http://internet.watch.impress.co.jp/docs/news/20130820_611788.html

「ＯＣＮ不正アクセス、無線ルーターの脆弱性が原因か 」
NIKKEI ITpro 2013年８月21日掲載

OCN不正アクセス、無線ルーターの脆弱性が原因か

2013/8/22 6:30

保存 印刷 リプリント 共有

NTTコミュニケーションズは2013年8月20日、インターネット接続サービスの「OCN」で756件の接続パスワードが不正に変更された原因は、無線LANブロードバンドルーターの脆弱性である可能性が高いことが判明したと発表した。該当する製品を使用しているユーザーを調査し、ファームウエア更新を呼びかける。

同社は2013年6月26日、OCNにおいて、インターネット接続用の認証パスワード756件が不正に変更されたと発表した。契約者以外の第三者が、OCNの認証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。調査の結果、ロジテックが過去に販売した無線LANブロードバンドルーターの脆弱性を突いた可能性が高いことが判明したという。

脆弱性が確認されたロジテックの300Mbps無線LANブロードバンドルータ（ロジテックの発表資料より引用）

脆弱性のある製品はロジテックの300Mbps無線LANブロードバンドルータで型番がLAN-W300N／R、LAN-W300N／RS、LAN-W300N／RU2、シリアルナンバー末尾が「B」でファームウエアがバージョン2.17のもの。確認と更新の手順はロジテックのWebサイトに掲載している。

NTTコミュニケーションズでは8月20日からユーザーの調査を行い、該当する製品を使用しているユーザーには個別に連絡しファームウエア更新とパスワードの変更を依頼する。

（ITpro 高橋信頼）

［ITpro 2013年8月21日掲載］

（出典） http://www.nikkei.com/article/DGXNASFK2102B_R20C13A8000000/

今回のガイドライン改定後の新たな取組

ガイドライン改定以前で制限されていたこと

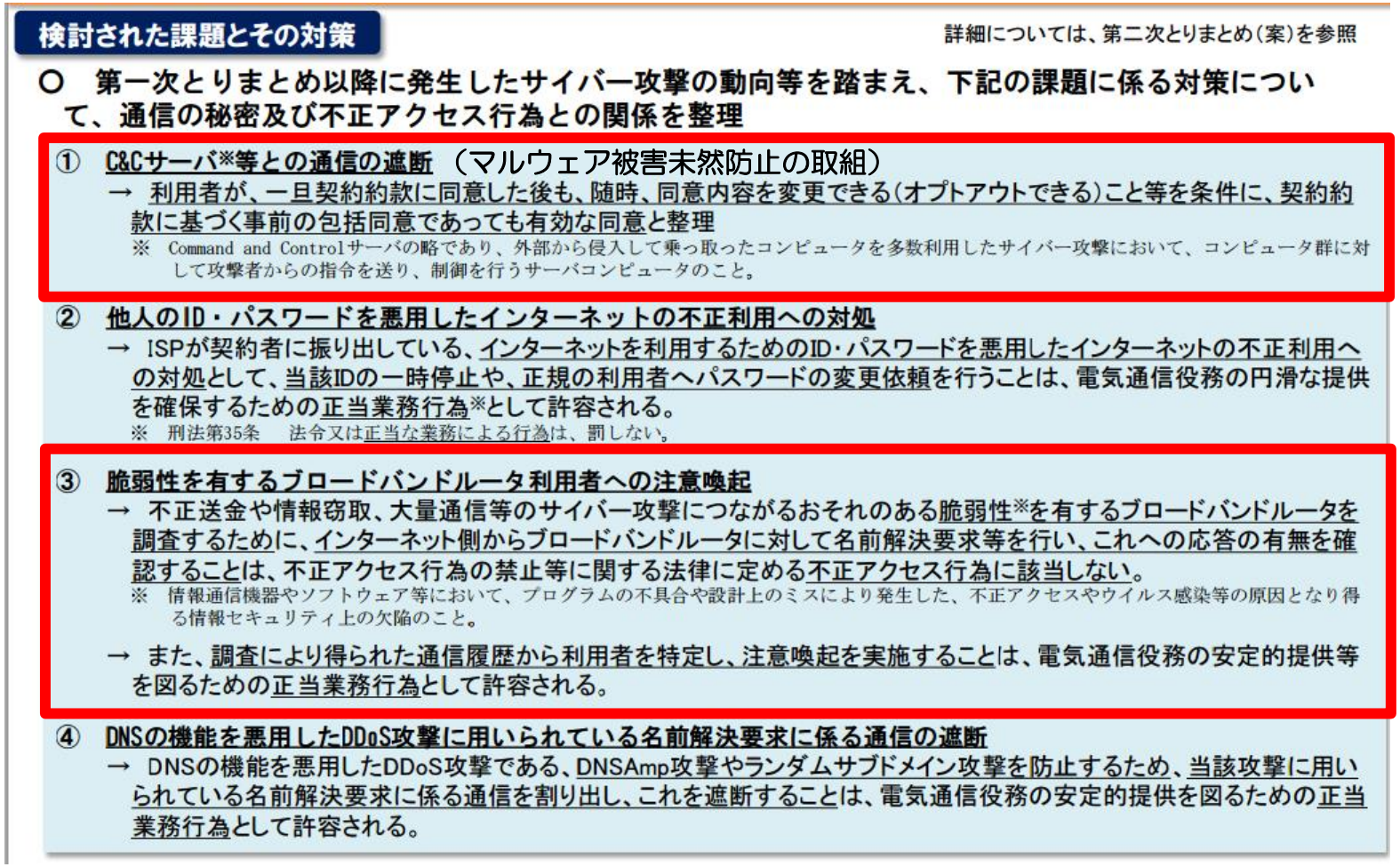
ガイドライン改定以前で制限されていたこと

- マルウェア感染による利用者への被害を防止するため、C&Cサーバ等へのアクセスの遮断を行って良いか、整理されていない。

- 不正送金や情報窃取、大量通信等のサイバー攻撃につながるおそれのある脆弱性を有するブロードバンドルータを調査するために、インターネット側からブロードバンドルータに対して名前解決要求等を行い、これへの応答の有無を確認していいか、整理されていない。
  また、調査により得られた通信履歴から利用者を特定し、注意喚起を実施してよいか、整理されていない。

今回ご紹介のサイバー攻撃と「通信の秘密」との関係

総務省「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会第二次とりまとめ（案）」概要の公開資料抜粋
http://www.soumu.go.jp/main_content/000369166.pdf



検討された課題とその対策

詳細については、第二次とりまとめ(案)を参照

○　第一次とりまとめ以降に発生したサイバー攻撃の動向等を踏まえ、下記の課題に係る対策について、通信の秘密及び不正アクセス行為との関係を整理

①　C&Cサーバ※等との通信の遮断（マルウェア被害未然防止の取組）

→　利用者が、一旦契約約款に同意した後も、随時、同意内容を変更できる(オプトアウトできる)こと等を条件に、契約約款に基づく事前の包括同意であっても有効な同意と整理

※　Command and Controlサーバの略であり、外部から侵入して乗っ取ったコンピュータを多数利用したサイバー攻撃において、コンピュータ群に対して攻撃者からの指令を送り、制御を行うサーバコンピュータのこと。

②　他人のID・パスワードを悪用したインターネットの不正利用への対処

→　ISPが契約者に振り出している、インターネットを利用するためのID・パスワードを悪用したインターネットの不正利用への対処として、当該IDの一時停止や、正規の利用者へパスワードの変更依頼を行うことは、電気通信役務の円滑な提供を確保するための正当業務行為※として許容される。

※　刑法第35条　法令又は正当な業務による行為は、罰しない。

③　脆弱性を有するブロードバンドルータ利用者への注意喚起

→　不正送金や情報窃取、大量通信等のサイバー攻撃につながるおそれのある脆弱性※を有するブロードバンドルータを調査するために、インターネット側からブロードバンドルータに対して名前解決要求等を行い、これへの応答の有無を確認することは、不正アクセス行為の禁止等に関する法律に定める不正アクセス行為に該当しない。

※　情報通信機器やソフトウェア等において、プログラムの不具合や設計上のミスにより発生した、不正アクセスやウイルス感染等の原因となり得る情報セキュリティ上の欠陥のこと。

→　また、調査により得られた通信履歴から利用者を特定し、注意喚起を実施することは、電気通信役務の安定的提供等を図るための正当業務行為として許容される。

④　DNSの機能を悪用したDDoS攻撃に用いられている名前解決要求に係る通信の遮断

→　DNSの機能を悪用したDDoS攻撃である、DNSAmp攻撃やランダムサブドメイン攻撃を防止するため、当該攻撃に用いられている名前解決要求に係る通信を割り出し、これを遮断することは、電気通信役務の安定的提供を図るための正当業務行為として許容される。

ACTIVEの新たな取組

ガイドラインの事例（マルウェア被害未然防止の取組）

ガイドラインの事例（マルウェア被害未然防止の取組）

【ガイドラインに記載されている事例】

- あるISPにおいて、マルウェア感染による利用者への被害を防止するため、契約約款に基づく事前の包括同意に基づき、C&Cサーバ等へのアクセスの遮断を行うとともに、遮断を行った契約者に対して、メールによりC&Cサーバ等との通信の遮断を行ったことや端末のマルウェア駆除が必要であること、遮断を望まない場合は変更が可能であること等を周知した。

マルウェア被害未然防止の取組

遮断を望まない場合は変更が可能であること等を連絡（オプトアウト）

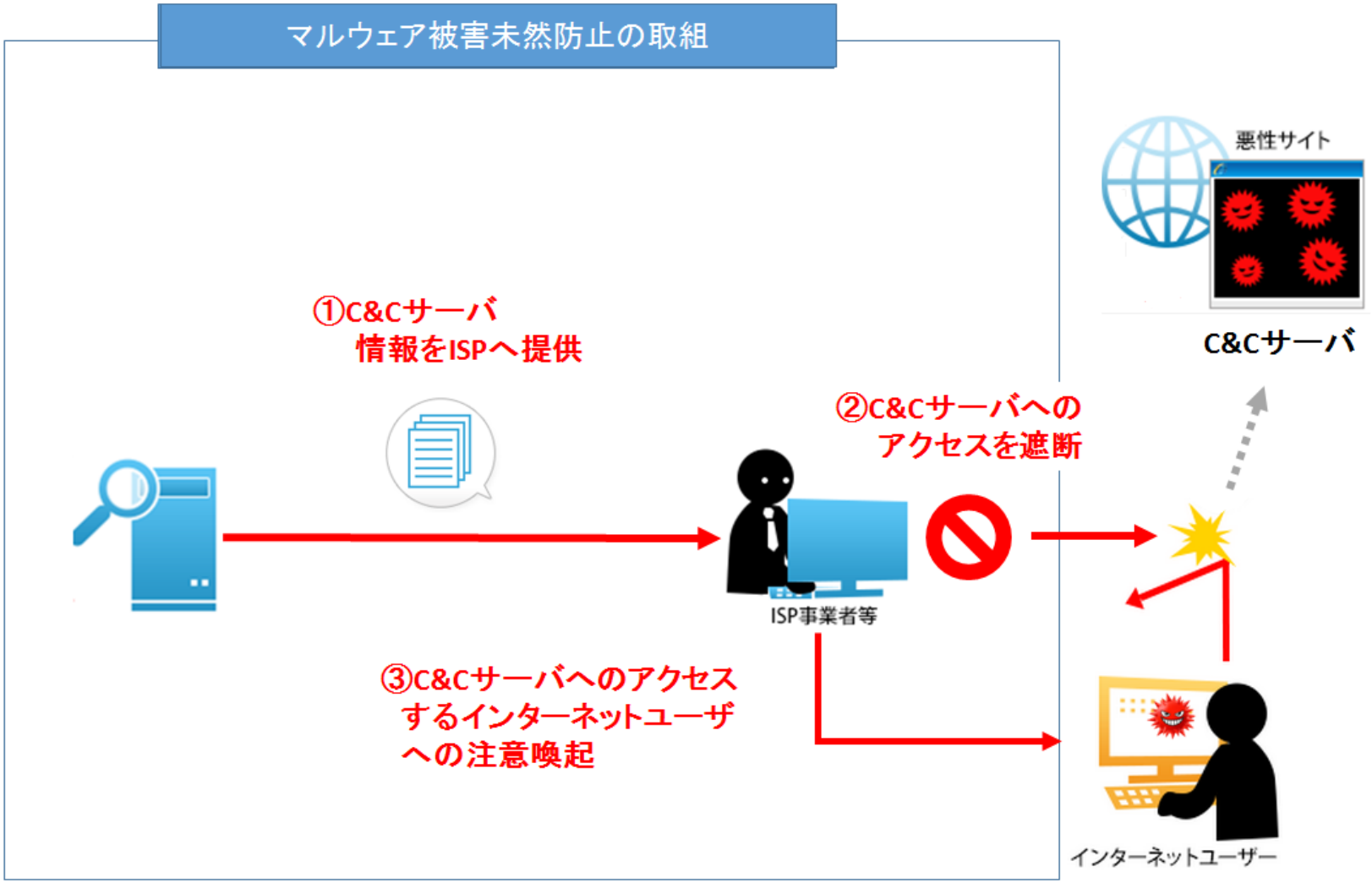
① C&Cサーバ等のFQDN情報・URL情報をリスト化
② C&Cサーバ等にアクセスしようとする利用者の通信を遮断
③ メールによりC&Cサーバ等との通信の遮断を行ったことや端末のマルウェア駆除が必要であることを連絡。

マルウェア被害未然防止の取組背景

- 近年、バンキングトロージャンに代表される、金融資産や個人情報を大量窃取するといった、実害を及ぼすマルウェアが広く拡散
- これらのマルウェアには、単独で動作するのではなく、外部にあるC&Cサーバから指令を受け、様々な動作するマルウェアが多数存在
- また、これらのマルウェアはユーザーの操作・意図に関係なくC&Cサーバと通信を行うため、ユーザーがその動作を認識することが難しい
- マルウェアの高度化に伴って、アンチウィルスソフトによるマルウェアの駆除が困難になってきており、被害を軽減するための新たな方策が求められる

ACTIVEの概要（マルウェア被害未然防止の取組）

マルウェア被害未然防止の取組
- 各社の対象サービスに対して、利用者から事前に包括同意または個別の同意を取得

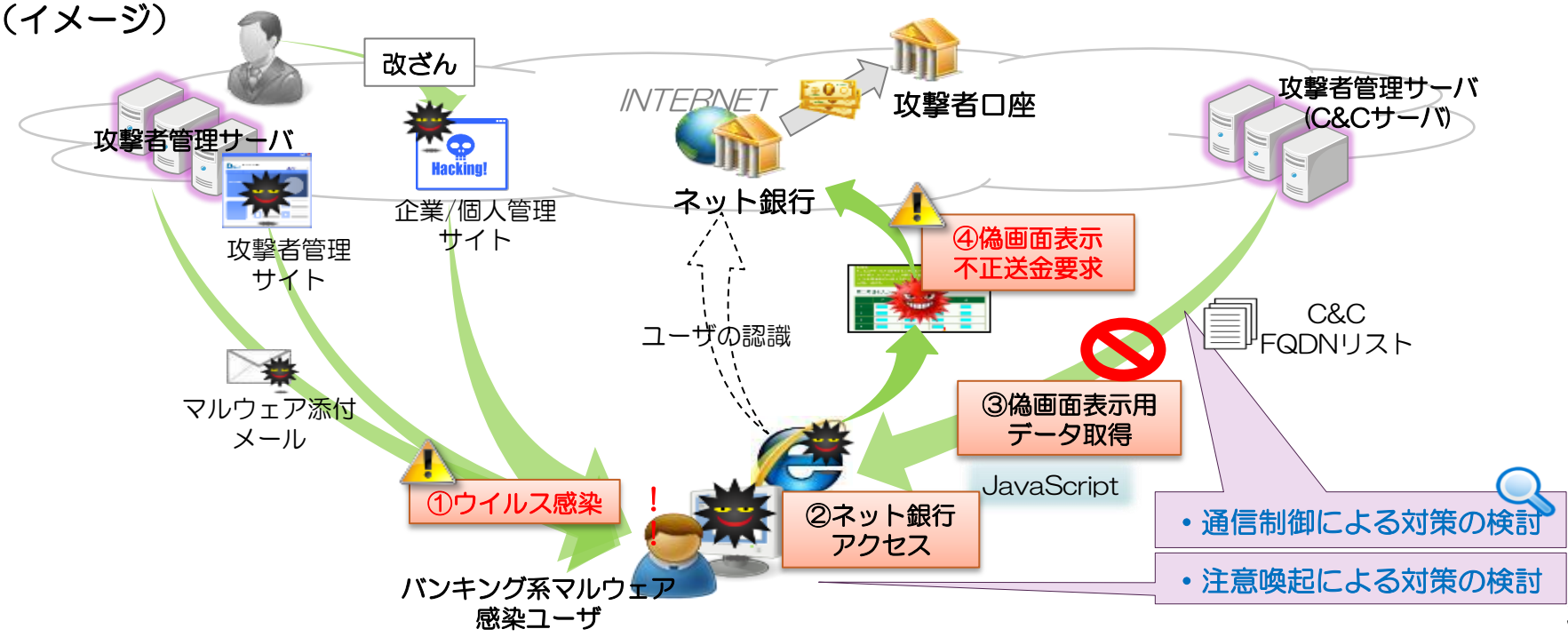


ACTIVEの概要（マルウェア被害未然防止の取組）

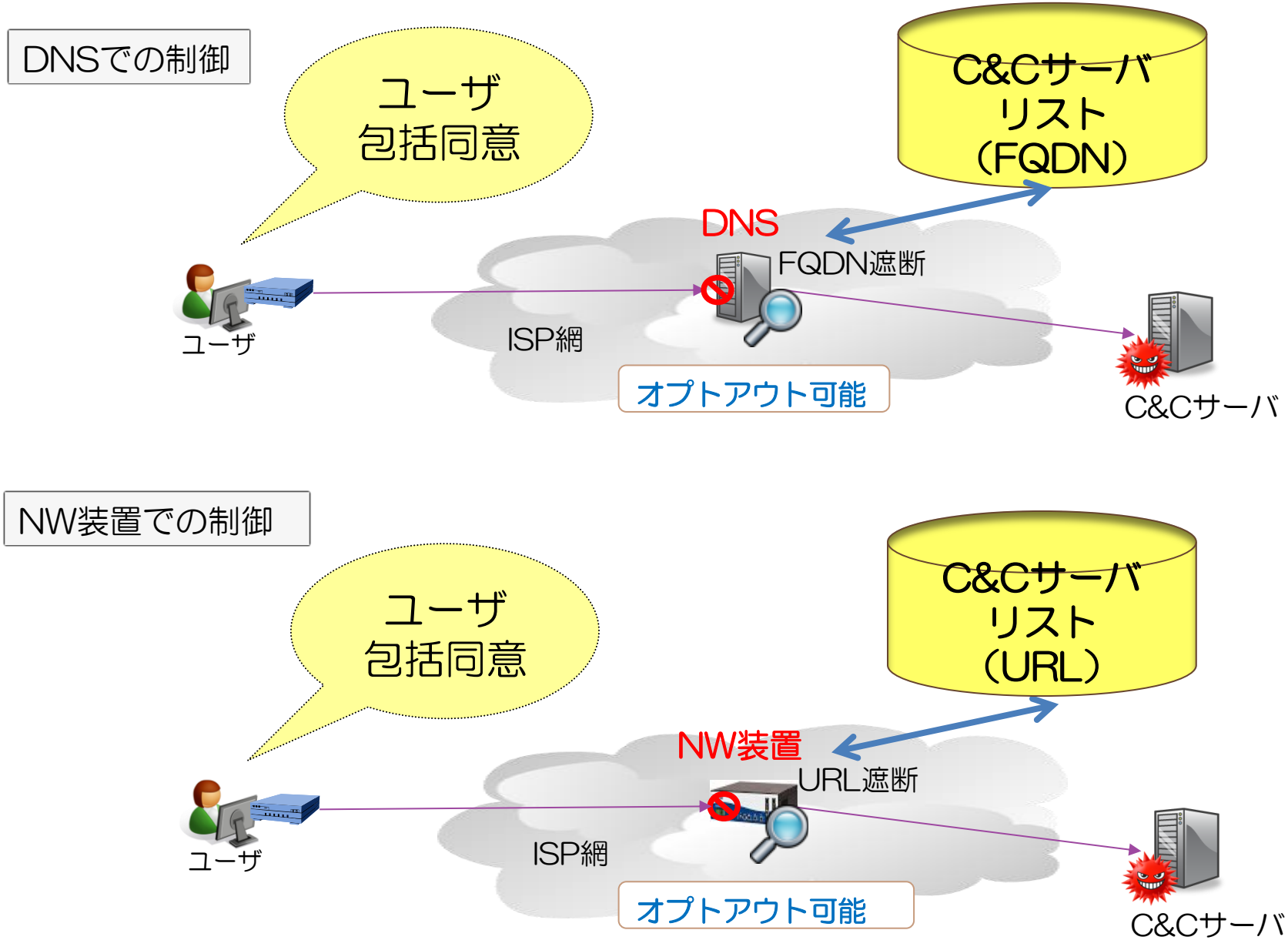
インターネットバンキングによる不正送金被害等に代表されるように、マルウェアに感染した端末はC&Cサーバの指令を受けて個人情報を窃取される他、サイバー攻撃の攻撃基盤としても利用されている。C&Cサーバとの通信はウェブブラウザを経由せず、またその通信においては独自の通信プロトコルを利用する場合が多いため、URLをもとにウェブブラウザで注意喚起する方法が取りにくいことが考えられ、新たな枠組みの検討が必要となる。

① C&Cサーバとの通信の対策として、注意喚起・通信制御等の具体的取組としてどのようなものがあるか検討（DNS方式、DPI／Proxy方式など。普及可能な包括同意＋オプトアウトを考慮）
② ①の場合におけるシステムやC&Cサーバ情報の収集手法等の技術的検討や効率的な運用について検討
③ 本取組について通信の秘密との整理が付いた場合には、整理内容を踏まえて、参加事業者において試験的な検証を実施

C&Cサーバとの通信に関する調査（イメージ）



マルウェア被害未然防止の取組（実装イメージ）



包括同意の取り方等の詳細

参考資料「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会 第二次とりまとめ」より抜粋

第1節　C&Cサーバ等との通信の遮断における有効な同意について

⑵有効な同意についての考え方

1. ISPがC&Cサーバ等へのアクセスに対する遮断を行うに当たって、通信の秘密に当たる情報のうち必要最小限度の事項(通信の宛先FQDN)のみを機械的・自動的に検知した上で、該当するアクセスを遮断することは、マルウェア感染による被害拡大を防止し、安全なインターネットを確保するためのものであり、インターネットの通常の利用者であれば、これらの事項について許諾することが想定し得るため、契約約款の性質になじまないとまでは言えない。

2. 本件において、遮断を希望しない者に対しては、その他の提供条件が同一であることを前提に、別のDNSサーバを使用するなど、オプトアウトができるような対応を行うこと、また利用者が、一旦契約約款に同意した後も、随時、同意内容を変更でき(設定変更でき)、同意内容の変更の有無にかかわらず、その他の提供条件が同一である契約内容とした上、アクセスの遮断並びに遮断を望まない利用者は随時同意内容を変更できる（設定変更できる）こと及びその方法について利用者に相応の周知が図られている場合には、契約約款による包括同意当時において予測し得なかった事情が将来生じた場合についても、随時、利用者が同意内容を変更することができると言えることから、将来、利用者が不測の不利益を被る危険を回避できる。

3. 利用者に対する相応の周知の方法としては、ウェブサイトへの掲載等を行うとともに、利用者に対するメールの送付等により、マルウェア感染駆除の注意喚起をするとともに、遮断の実施、随時同意内容を変更できる（設定変更できる）こと及びその方法等について個別の説明をすることが考えられる。

上記要件を満たす場合、契約約款に基づく事前の包括同意であっても、通信の秘密に属する事項の利用についての有効な同意と考えられる。

＜契約約款に記載すべき事項＞
検知を行うこと、検知の時期、検知の対象となる情報の範囲、事後的に同意内容を変更できる（設定変更できる）こと

包括同意の例

コンピュータ通信網（HOTCN）サービス契約約款

（利用の制限）
第＊＊条当社は、特定の地域等との通信が第三者によって不正に使用されていると判断された場合には、その地域等との通信の全部又は一部の利用の制限又は中止する措置をとることがあります。

2当社は、アクセスしただけでマルウェア（不正かつ有害な動作を行う、悪意を持ったソフトウェア）に感染させる可能性の高いウェブサイト（以下「マルウェア配布サイト」）に関して、当社設備で必要な範囲において通信（アクセス先IPアドレス又はURL）を検知し、当社が指定する悪性サイトリスト作成管理団体から提供される悪性サイトリストに基づき、（コンピュータ通信網サービス）契約者がアクセスしようとするウェブサイトが、マルウェア配布サイトである場合には、その接続要求に対して、その通信を一時停止し、注意喚起を行うため、当該通信の制限をすることがあります。

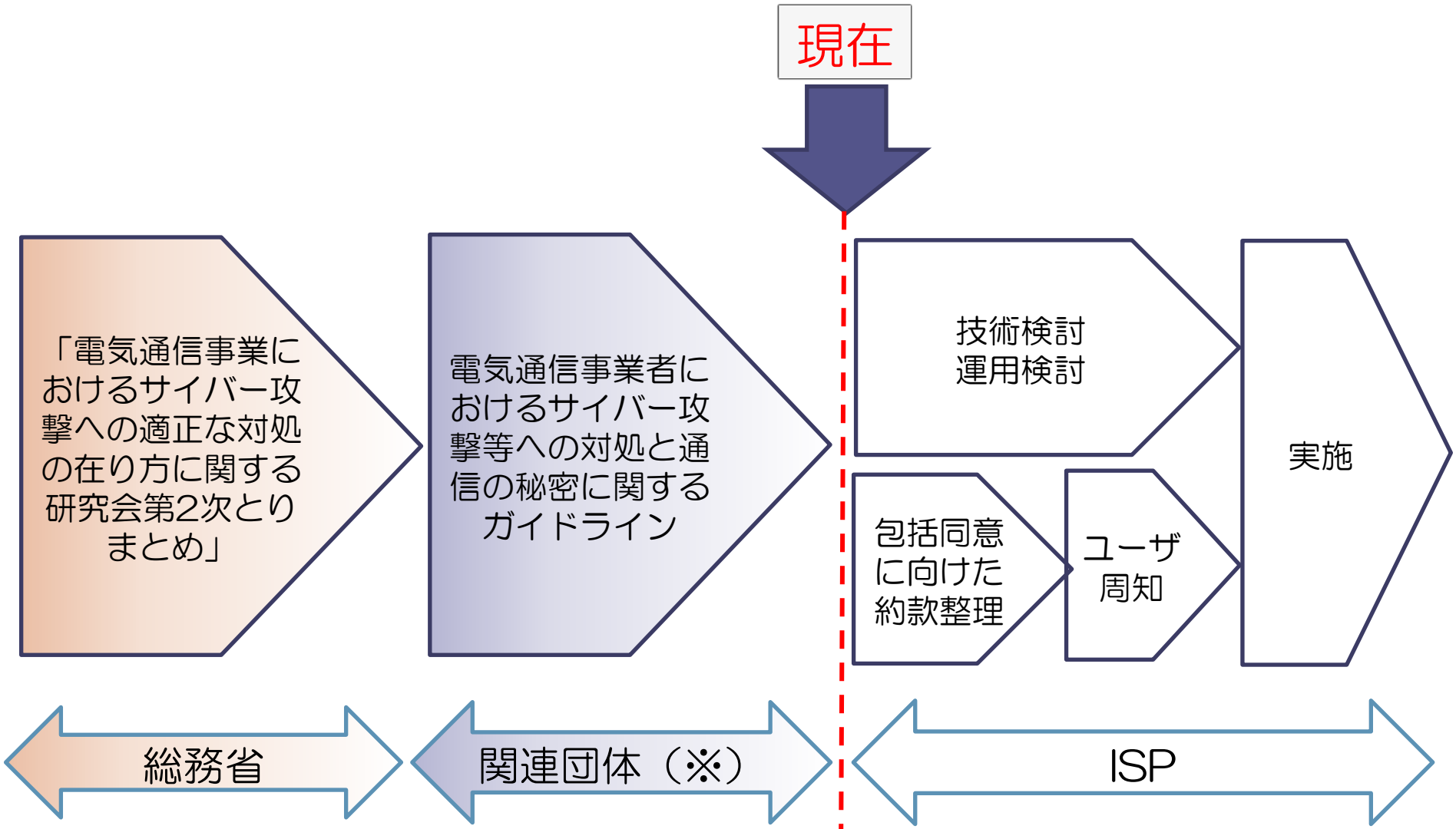
3当社は、外部から侵入して乗っ取ったコンピュータを多数利用したサイバー攻撃において、コンピュータ群に指令を送って制御するサーバコンピュータ（以下「C&Cサーバ等」）へのアクセスに係る通信に関して、当社設備で必要な範囲において通信（宛先FQDN）を検知し、当社が指定するC&Cサーバ等リスト作成管理団体から提供されるC&Cサーバ等リストに基づき、（コンピュータ通信網サービス）契約者が、インターネット上のサーバに対するアクセス要求をした際に、C&Cサーバ等とアクセスしようとする場合には、そのアクセスを遮断し、当該通信の制限をすることがあります。

4　第2項及び第3項の規定により、（コンピュータ通信網サービス）契約者の利用に何らかの不利益が生じた場合であっても、当社はその一切の責任を負わないものとします。

5当社は、当社の電気通信設備（これに付属する設備を含みます。）を不正アクセス行為から防御するため必要な場合、サービスの全部又は一部の利用を中止する措置を取ることがあります。

（利用制限の解除等）
第＊＊＋１条（コンピュータ通信網サービス）契約者は書面等による請求により、前条（利用の制限）第2項及び第3項による、当該制限（検知及び一時停止等又は遮断）の措置を解除することができるものとします。

マルウェア被害未然防止の実施流れ



（※）
一般社団法人日本インターネットプロバイダー協会
一般社団法人電気通信事業者協会
一般社団法人テレコムサービス協会
一般社団法人日本ケーブルテレビ連盟
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

脆弱性を有するブロードバンドルータ問題

ガイドラインの事例
（脆弱性を有するブロードバンドルータに対する注意喚起）

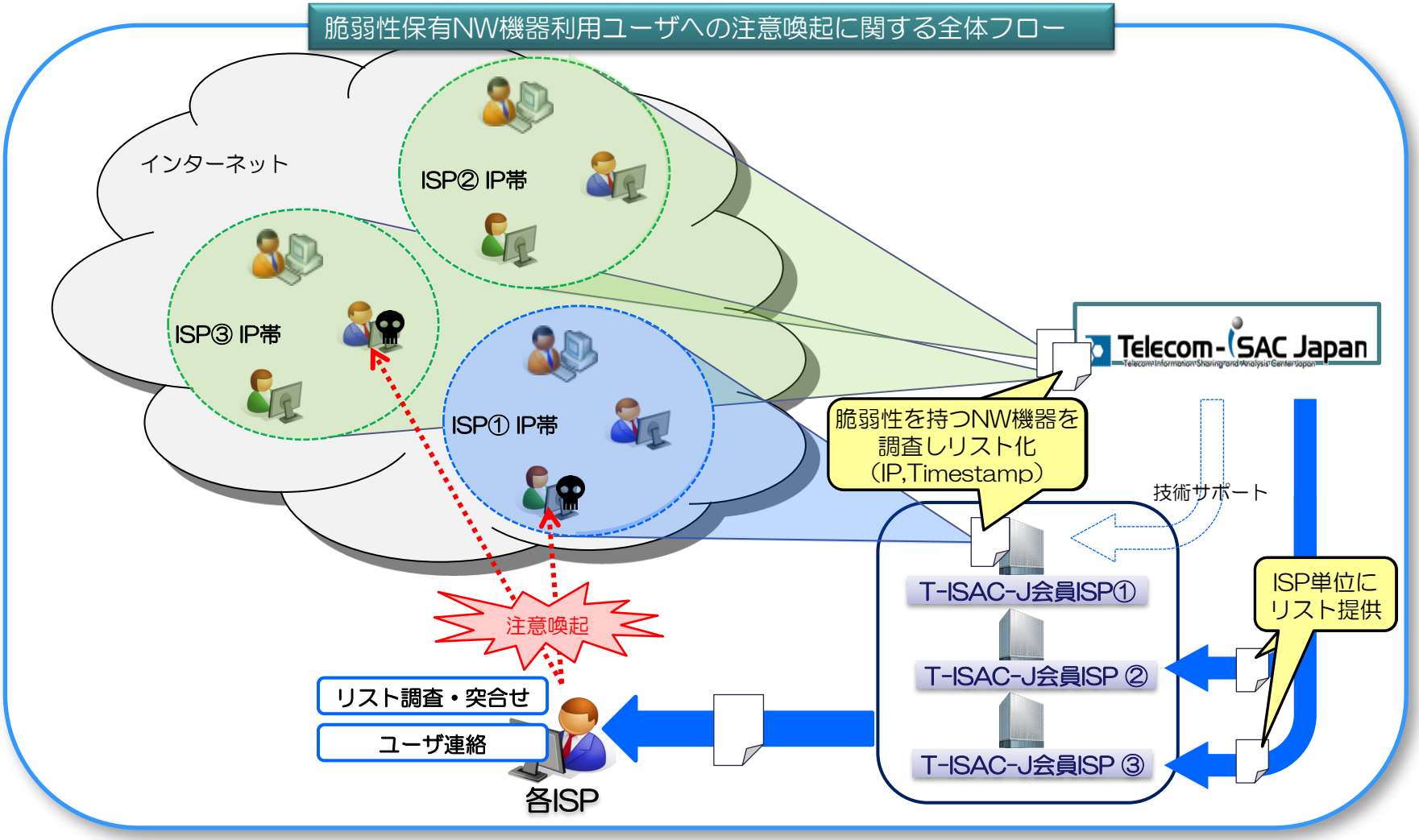
ガイドラインの事例（脆弱性を有するブロードバンドルータに対する注意喚起）

【ガイドラインに記載されている事例】

・事業者において、リフレクション攻撃に悪用されうる脆弱性やPPPoE認証の情報を窃取され得る脆弱性を有するブロードバンドルータについて調査を行い、当該ブロードバンドルータに関する情報（IPアドレス及びタイムスタンプ）を、当該IPアドレスを管理しているISPに提供した。各ISPにおいて、提供のあったIPアドレス及びタイムスタンプの情報を基に、タイムスタンプにおいて示された時刻において当該IPアドレスをどの契約者に割り当てたか確認して、該当契約者を割り出し、メール等によって個別に注意喚起を行い、ファームウェアの更新等を依頼した。

脆弱性を有するブロードバンドルータに対する注意喚起

ISP事業者自身またはT-ISAC-J等の外部団体がリスト化した情報を元に、脆弱性を持つNW機器を利用しているユーザへ注意喚起の実施が可能



まとめ

- 「電気通信事業者におけるサイバー攻撃等への対処と通信の秘密に関するガイドライン」の改定により、サイバー攻撃に関する下記の課題に係る対策について、通信の秘密及び不正アクセス行為との関係が整理された

  - C&Cサーバ等との通信の遮断
    ⇒ 利用者が、一旦契約約款に同意した後も、随時、同意内容を変更できる（オプトアウトできる）こと等を条件に、契約約款に基づく事前の包括同意であっても有効な同意と整理

  - 脆弱性を有するブロードバンドルータ利用者への注意喚起
    ⇒ 不正送金や情報窃取、大量通信等のサイバー攻撃につながるおそれのある脆弱性を有するブロードバンドルータを調査するために、インターネット側からブロードバンドルータに対して名前解決要求等を行い、これへの応答の有無を確認することは、不正アクセス行為の禁止等に関する法律に定める不正アクセス行為に該当しない。
    ⇒ また、調査により得られた通信履歴から利用者を特定し、注意喚起を実施することは、電気通信役務の安定的提供等を図るための正当業務行為として許容される。

- 今後は、上述の対策がISPで実施できるため、ISPがサイバー攻撃からの被害を軽減することが可能となり、利用者への安全・安心なインターネット環境を提供することができる

ご清聴有難うございました