「IP電話乗っ取りに関する検討」中間報告

2016年2月２４日

技術部会
ネットワーク ワークグループ

IP電話乗っ取りと高額請求の報道

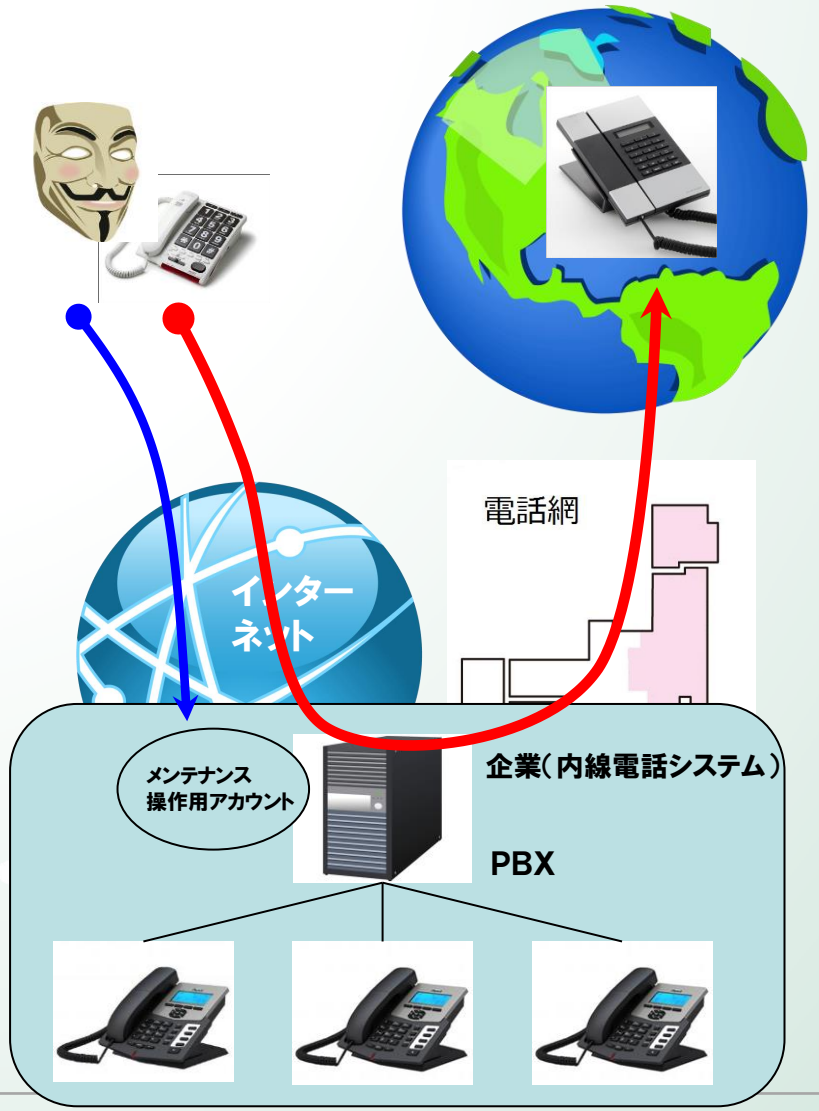
昨年、インターネット回線を使ったＩＰ電話が何者かに乗っ取られて国際通話を勝手に発信され、利用者が身に覚えのない高額の利用料を請求される被害が相次いでいる問題で、ＮＴＴ東日本と西日本は６日、被害額の一部を補償すると発表した。また被害拡大を防ぐため、これまで申し込みから数日間かかっていた国際通話の発信規制を、当日のうちに完了できるよう手続きを迅速化する。

補償対象となるのは、ＮＴＴに発信規制を申し込んでから完了するまでの間に発生した被害で計約１２０件、７１００万円前後。ＮＴＴ側の故障や不具合による被害ではないため、それ以外の通話料は請求するとしている。

この問題では、ＩＰ電話を内線電話として利用している事業者を中心に、何者かがソフトウェアのセキュリティの弱点を突いてインターネット経由で不正アクセスし、アフリカのシエラレオネなどに多数の国際通話を発信。被害額が５００万円に上るケースも出ている。

ＮＴＴによると、こうした内線機能を加えていない個人利用者などの被害は確認されていない。

ＩＰ電話の設定が、外部から遠隔操作される状態だったり、ＩＤやパスワードが初期設定のままだったりした利用者が被害に遭っており、ＮＴＴはセキュリティ対策の見直しを呼びかけている。



Copyright (C) 2016 JSSEC All rights reserved.

検討の目的

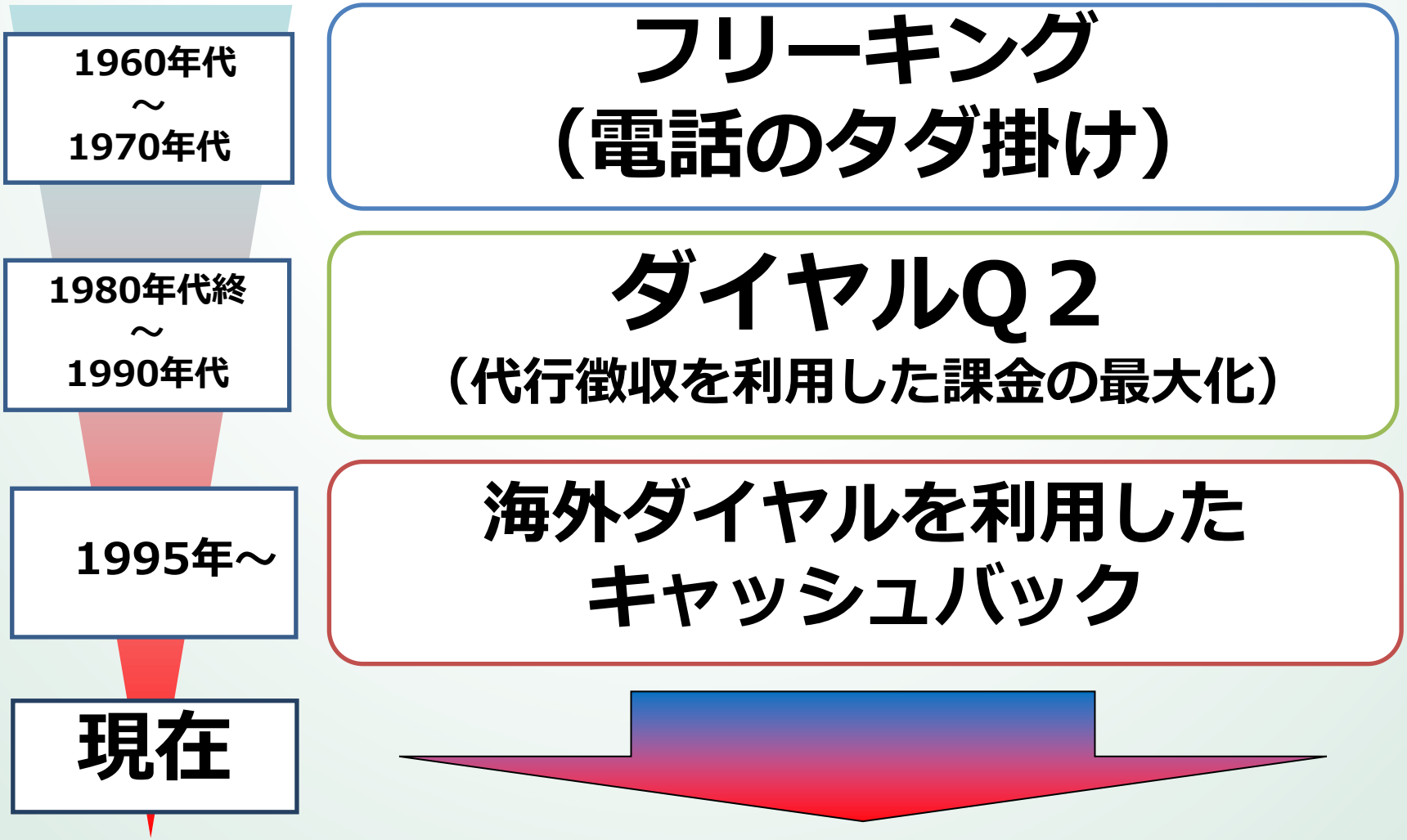
前のスライドの通り、インターネット回線を使ったＩＰ電話が何者かに乗っ取られて国際通話を勝手に発信され、利用者が身に覚えのない高額の利用料を請求される被害がある一方で、今後はスマートフォンを内線電話として登録・使用するケースも増加すると考えられるため、そのようなケースにおける不正利用についてネットワークワークグループにおいて検討を行う。

Copyright (C) 2016 JSSEC All rights reserved.

電話課金詐欺
～　古くて新しい問題 ～

Copyright (C) 2016 JSSEC All rights reserved.

電話課金詐欺の歴史と傾向の遷移



Copyright (C) 2016 JSSEC All rights reserved.

フリーキングの時代

1960年代のアメリカでは、初期の電話課金詐欺がさかんに行われるようになる。所謂「フリーキング」と呼ばれる行為で、電話システムをだまして不正に無料で電話をかける事である。

手口としては、当時のAT&Tの電話接続方式の仕様を逆手にとったもので 2600MHz のトーン信号を利用する。この信号は、電話線が待機状態を示す信号であり、電話呼出しを行っている間に、トーン信号を電話線に発信すると電話線は待機状態になる。次に、繋ぎたい電話番号を規定の周波数で発生させると、相手に電話がるという仕組みになっている。この通話は、接続方式の仕様が同じ海外に対する接続も可能であり、それらの逸話も残されている。

1970年代になると、この詐欺に利用される装置（電話接続をシミュレーションする装置）である「ブルーボックス」が紹介され、それを自作するユーザが現れた。また、この装置の完成品がアンダーグランドで販売されるようにもなり広がりを見せた。

フリーキングで実現できる、地域網のハッキングを元に地域から世界へと次々に接続を行うビジョンは、後のハッカー文化の形成に多大な影響を与えて行く事になる。

Blue Box at the Powerhouse Museum

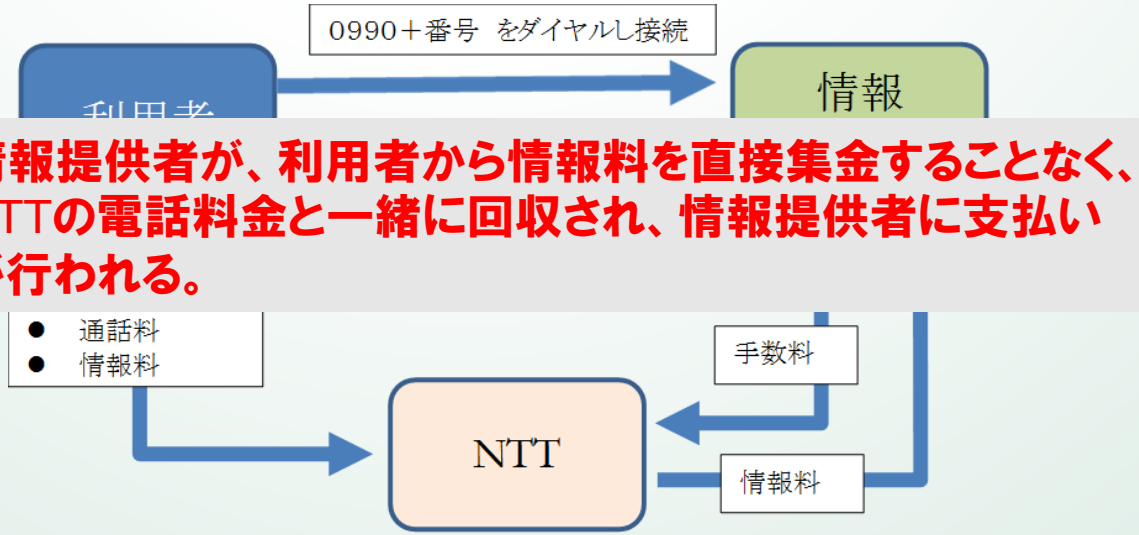
Copyright (C) 2016 JSSEC All rights reserved.

画期的だった「ダイアルQ２」

分割化前の日本電信電話株式会社（以下NTT）により1989年7月10日に開始された「ダイヤルQ2」は「電話による有料情報サービスの情報料金を、電話料金と一緒に回収するサービス」として開始された。サービス開始当初、NTT側はニュースやテレフォン相談のような一般サービスに利用されることを想定していたが、ほどなく成人向け情報提供業者が目をつけアダルト番組等を提供するようになる。

これらの背景があり、爆発的に利用が拡大すると援助交際目的の利用が次第に増え、少年非行や未成年相手の買春の温床になるなどし、また、若年者が長時間利用したことによる数十万円から数百万円 という高額な情報料が発生したために、利用料金請求が高額となりトラブルになるなど社会問題化した。

この後、世論を重く見た NTTは、情報提供事業者の電話回線の利用企画書をより厳しくチェックし、当初の利用企画書内容と異なる事業内容の番組の回線利用（ツーショットダイヤル）を提供している事業者のQ2回線利用契約を更新しないといった規制に乗り出した。



Copyright (C) 2016 JSSEC All rights reserved.

国際電話へ・・・

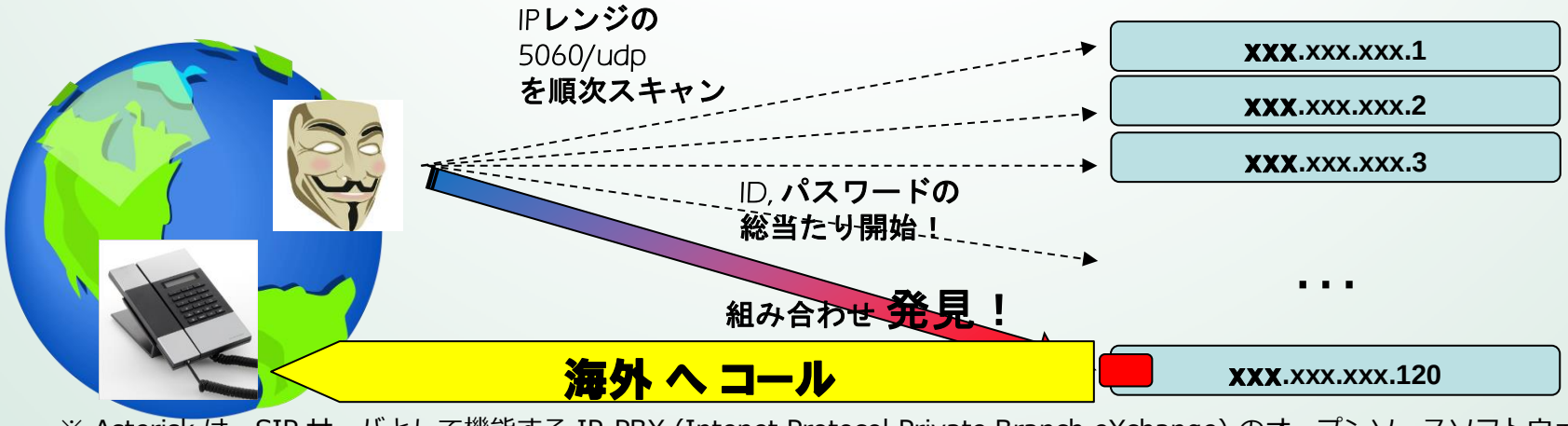
1995年になると、NTTがさらに規制を強化したため、残留していたアダルト系情報コンテンツは ***課金に国外への通話を発生させた際の着信国側の通信会社からの払戻を利益とする国際電話回線を利用するような状況*** や、パソコン通信の普及（モデムを使用したインターネット接続）に付随するダイヤルアップ接続の電話番号をダイヤルQ2番号に書き換えてしまうソフトウェアを知らないうちにダウンロードさせて、ダイヤルQ2番号に接続させる行為等が発生した。

海外ダイヤルを利用した
キャッシュバック

Copyright (C) 2016 JSSEC All rights reserved.

IP-PBX (Asterisk の事例)

- 2010年12月に、IPA から「不適切な設定で Asterisk を利用した場合に発生し得る不正利用に関する注意喚起」が発表された。
- 攻撃者は、SIP の通信で使用される 5060/udp パケットをインターネットの広い範囲に送信し、応答した SIP サーバに対して IP 電話の発信に必要な ID, パスワードを特定するための総当たりアタックを行って有効な組み合わせを探すもの。
- IPA では、Asterisk を運用しているユーザが高額な国際通話料を請求される事例を複数確認している。



※ Asterisk は、SIP サーバとして機能する IP-PBX (Intenet Protocol Private Branch eXchange) のオープンソースソフトウェア

Copyright (C) 2016 JSSEC All rights reserved.

注意喚起

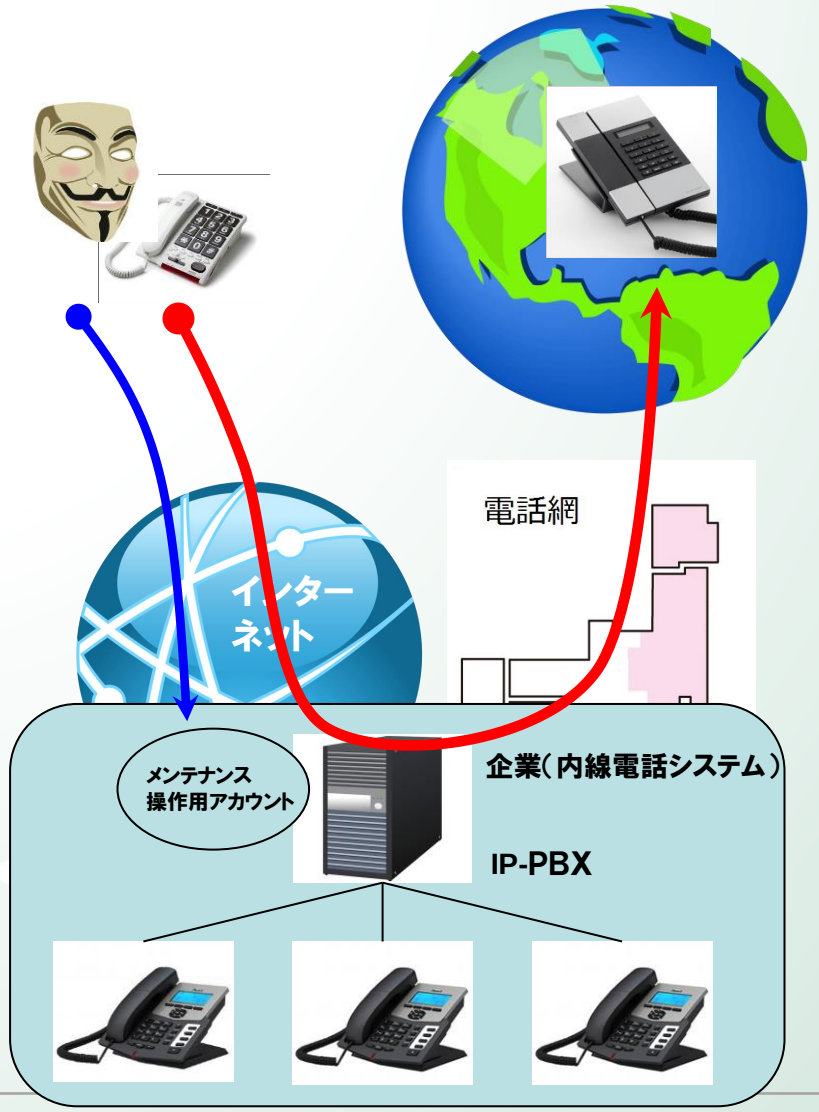
海外ダイヤルによる被害については、これまで総務省並びに各電話会社から何度も注意喚起が行われています！

Copyright (C) 2016 JSSEC All rights reserved.

2015年の IP電話 乗っ取り

- 管理画面やSIPサーバを不正に操作され国際電話をかけられた。
  - IP-PBX はインターネットに公開状態だった
  - 管理者の初期ID・パスワードがそのままだった
  - PSTN （公衆交換電話網）接続のある IP-PBX であった

電話帳や通話記録と言った情報漏えいの可能性



Copyright (C) 2016 JSSEC All rights reserved.

新たな被害の可能性

海外通話以外の、新たな被害の可能性

- ●情報の漏洩
- ●なりすまし

【情報漏洩】

- 通話履歴
- 電話帳が統合されている場合など、
  - 取引先等の電話番号、部署・担当者名など
  - 社内の部署・ユーザー名と電話番号やメールアドレスなど

【なりすまし】

- IP-PBX を乗っ取った企業を騙って、電話の送受信を行うなど

Copyright (C) 2016 JSSEC All rights reserved.

対策

- 発信制限
  - 海外通話の全面禁止（電話会社に依頼）
  - 発信のフィルタリング
    - 番号登録制
      - 海外取引先の番号を申告してもらい、登録番号へのみ発信可
    - 発信端末、もしくはユーザ、あるいは両方の登録制
      - 海外に発信可能な端末もしくはユーザあるいは両方を登録し、それ以外からの発信を禁止
- IP-PBX
  - ネットワークの見直し
    - IP-PBX のネットワーク的な位置
    - 接続方法
  - 管理者および一般アカウントの制限強化
    - パスワードの強化
    - ログ監視、不審な電話が登録されていないかなど
  - システムの定期的な監査

➡ **公開サーバと同じレベルの対策**

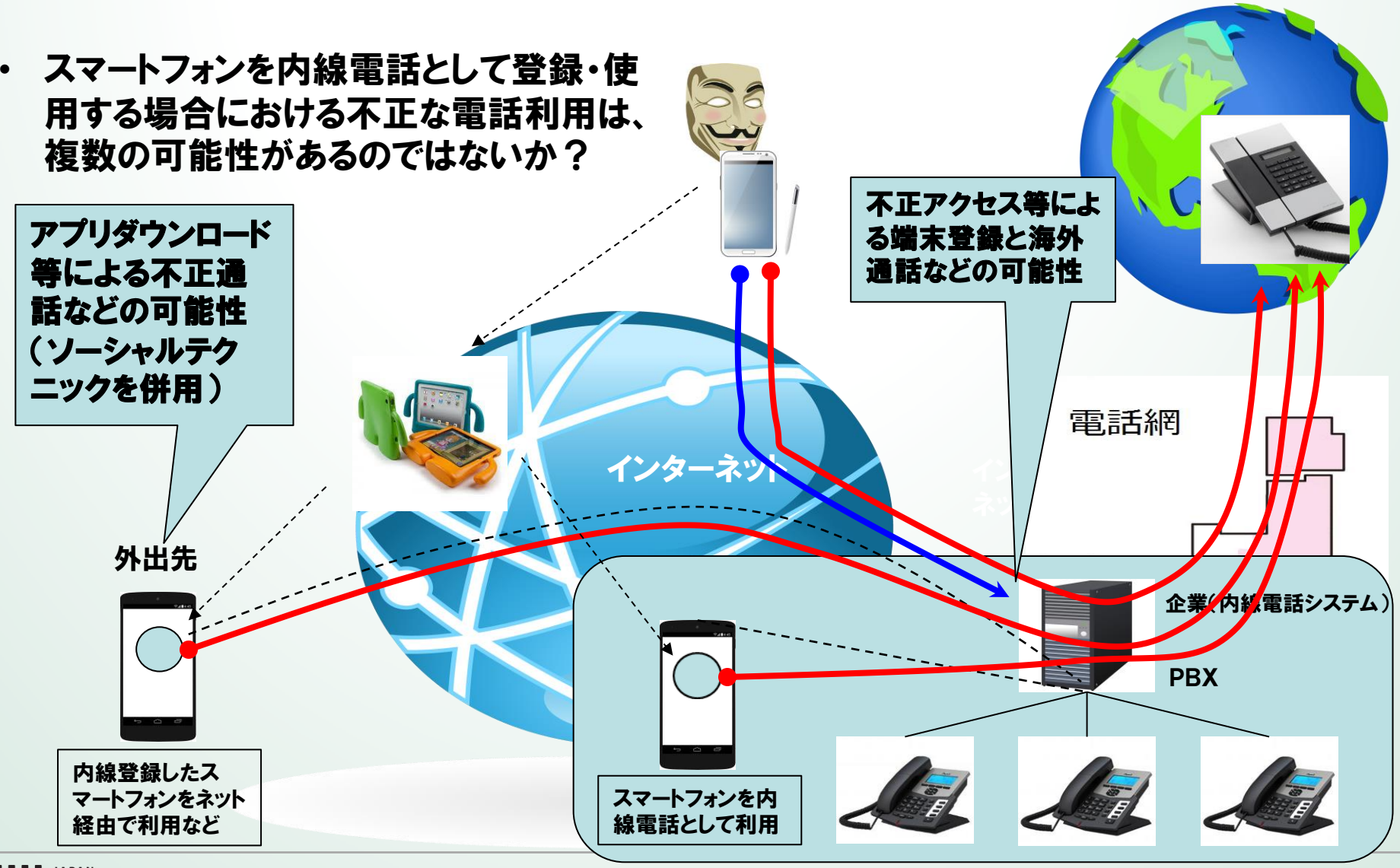
Copyright (C) 2016 JSSEC All rights reserved.

(BYOD)
モバイルワーキング時代の
内線電話

Copyright (C) 2016 JSSEC All rights reserved.

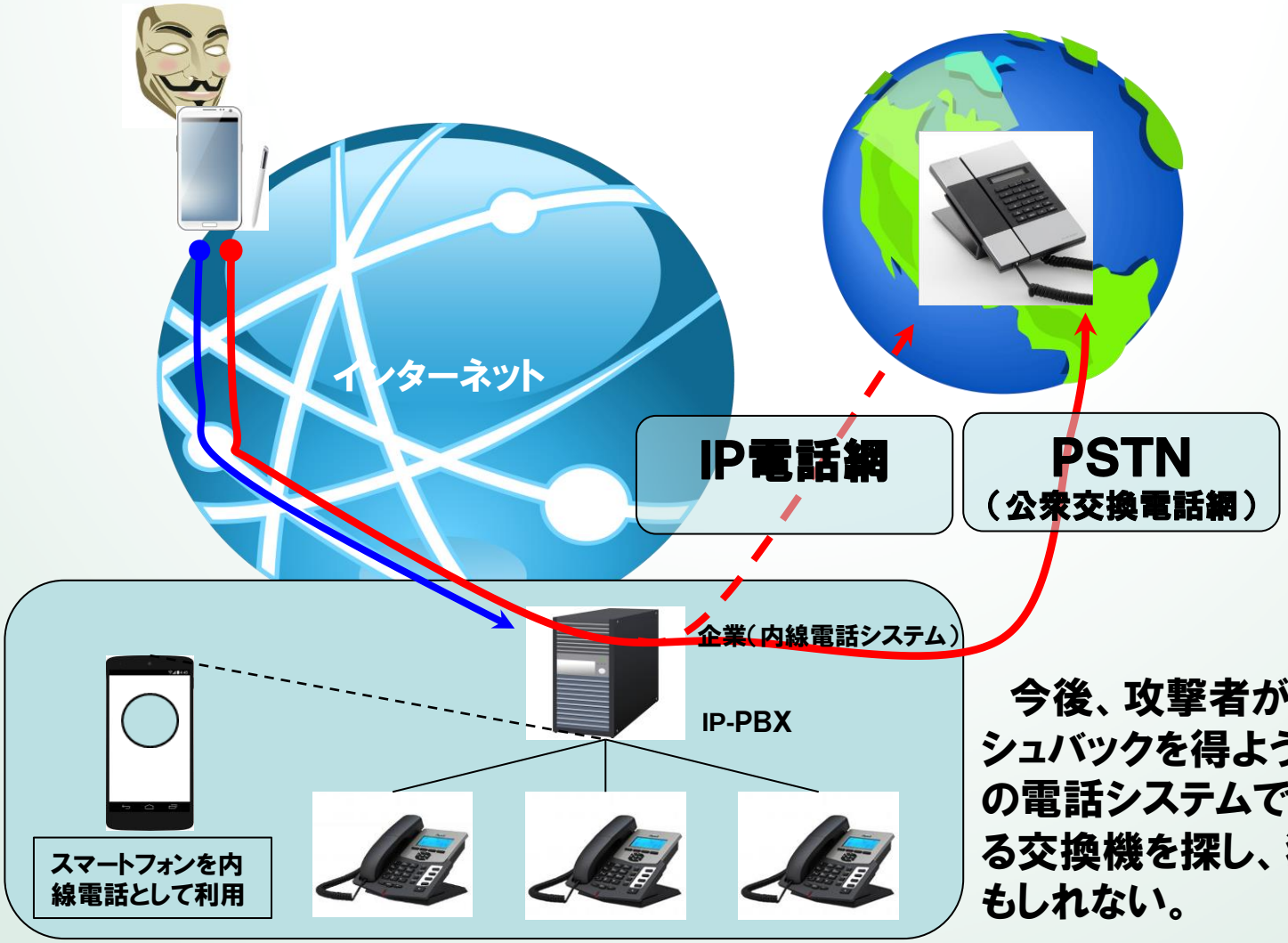
スマートフォン・タブレット等の内線登録

- スマートフォンを内線電話として登録・使用する場合における不正な電話利用は、複数の可能性があるのではないか？



Copyright (C) 2016 JSSEC All rights reserved.

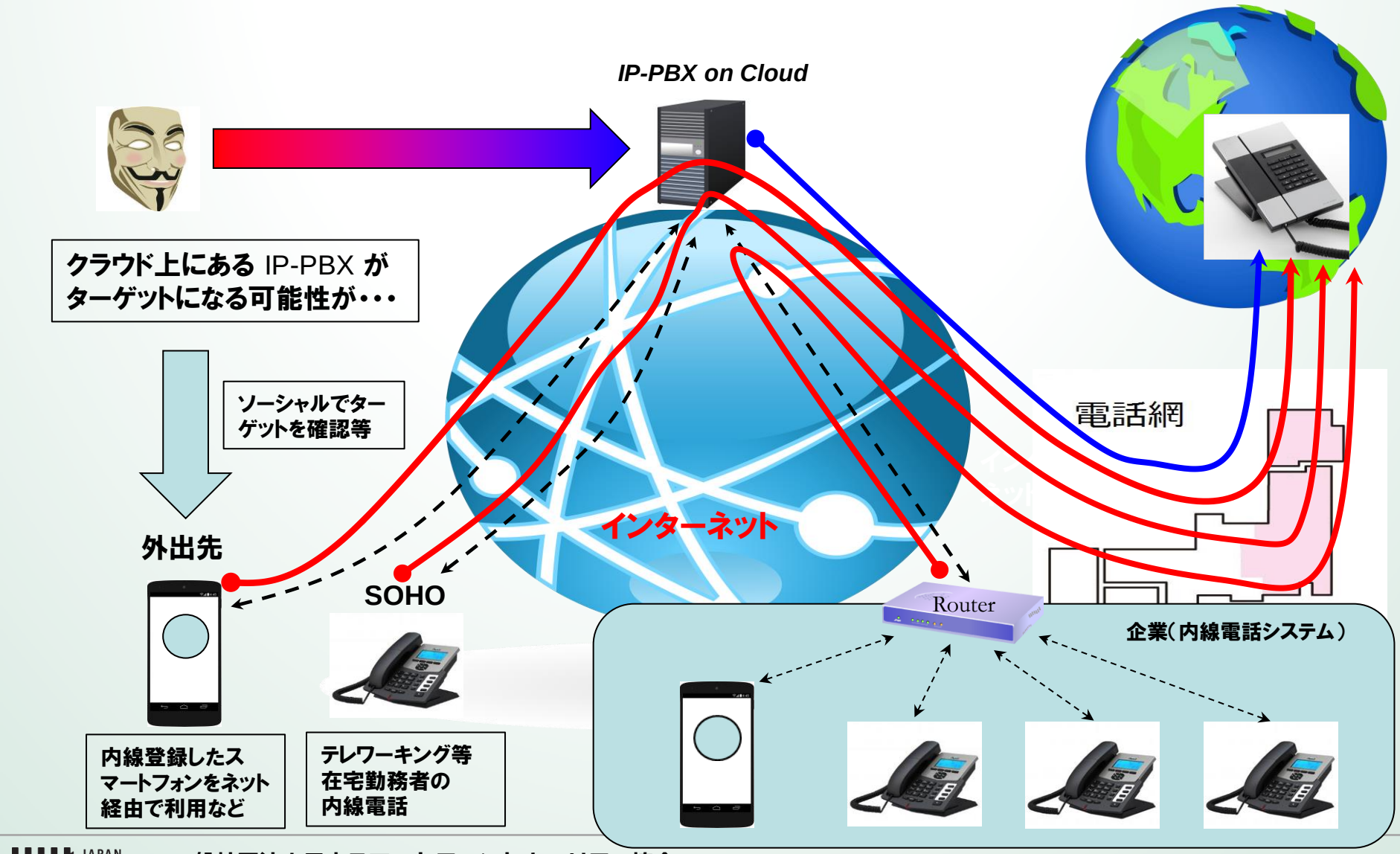
IP電話（050）では対策が進んでいます



今後、攻撃者が海外通話のキャッシュバックを得ようとした場合、企業の電話システムで PSTN 接続のある交換機を探し、狙うようになるかもしれない。

Copyright (C) 2016 JSSEC All rights reserved.

IP-PBX はクラウドへ



Copyright (C) 2016 JSSEC All rights reserved.

対策

- 基本的には「発信制限」,「IP-PBXの管理」
- セキュリティログをきちんと把握して、アタックの兆候を掴み適切に管理してゆく
- ユーザに対するソーシャル的なアタックについての注意喚起及び教育
  - SNS等で電話番号が送られてきても、安易に電話しない
  - フィッシングメールに注意する
  - 他
- スマートフォンアプリへの注意
  - 信頼性のあるアプリか判断する必要がある。
  - 通話が必要なアプリか判断する。
  - 例えば、Android の ACTION_CALL だと CALL_PHONE パーミッションが必要だが、ACTION_DIAL だとCALL_PHONE パーミッションがいらない。これは、前者が自動的に電話を掛けるのに対して、後者だとユーザが最終的に通話ボタンを押して電話を掛けるため。後者のような実装のアプリでは、ユーザがきちんとダイヤルする電話番号を認識する必要がある。
  - SIPフォンは、例えば Android で言う CALL_PHONE パーミッション無しでも通話が可能なので注意

Copyright (C) 2016 JSSEC All rights reserved.

以上

Copyright (C) 2016 JSSEC All rights reserved.