資料1

国際通話不正利用の現状と対策（IP電話＋PSTN）

平成27年7月6日

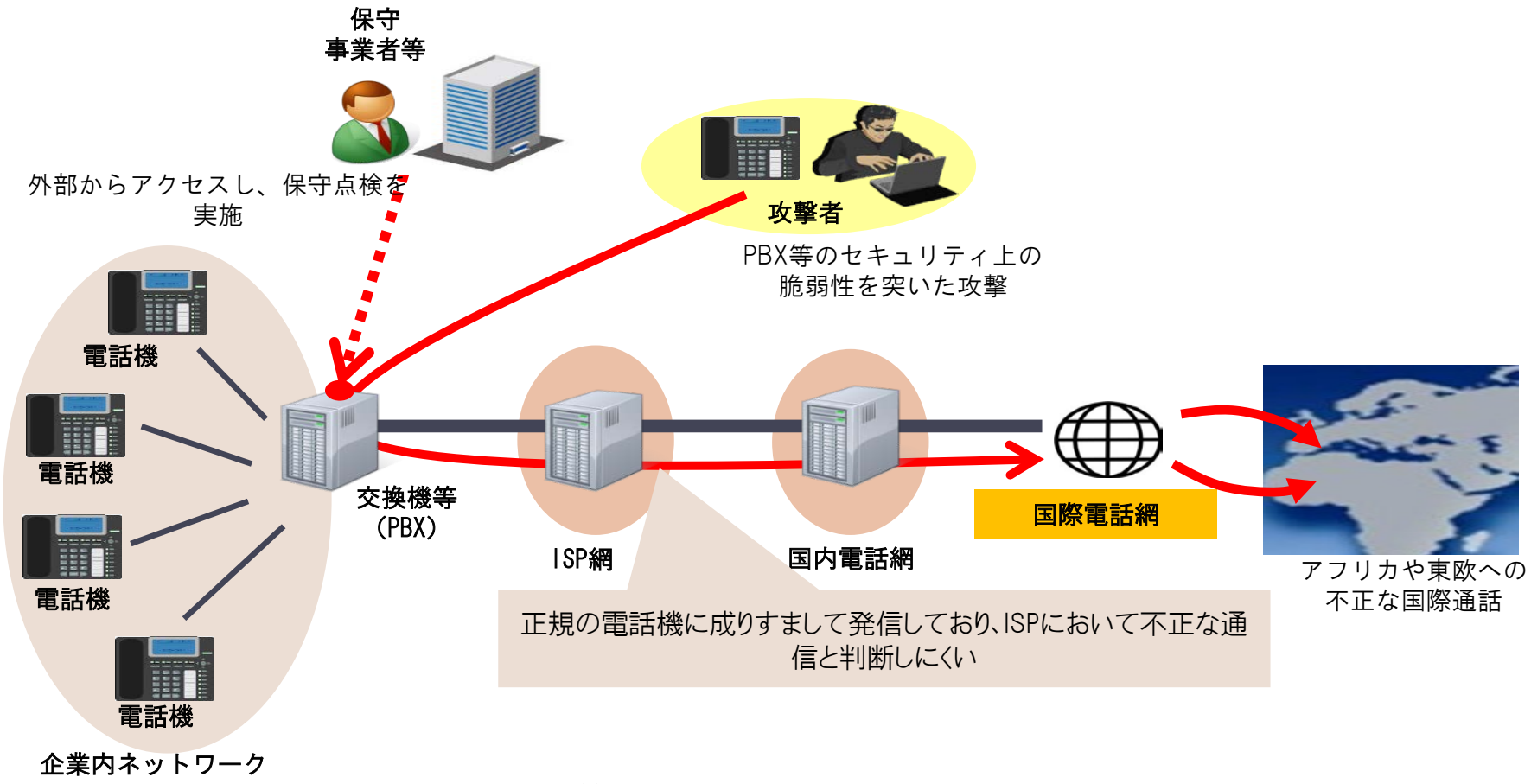
NTTコミュニケーションズ株式会社
土沼恒之

Agenda

1　Telecom-ISAC Japanの調査結果（WG資料）
（なりすましによるＩＰ電話等の不正利用について）
2　国際不正利用の概要
3　事業者の取組むべき対策
4　NTTComの取組みの紹介
5　電気通信業界で取組みたいこと

なりすましによるIP電話等の不正利用について 1/2

■ IP電話等を利用する際にインターネットに接続している通信機器の中に、外部から保守や管理を行う目的でネットワーク外部からのアクセスを許可しているものがあり、そこからセキュリティ上の脆弱性（平易なID・パスワードの設定等）を突かれ、第三者が正規の利用者になりすまして任意に国際電話を発信可能にしたと考えられている。



IP電話等の不正利用の仕組み

なりすましによるIP電話等の不正利用についての各社の被害状況 2/2

被害状況（取扱注意）

※　平成27年6月22日（月）時点

■　全体的な傾向として、従来より一定の頻度で不正利用による被害が発生しているものの、報道にあったような直近で大規模な不正利用は、事業者横断的に発生しているものではなく、局所的な被害に留まっている模様。

- 本年３月及び４月に特定の事業者のPBXを導入している利用者において、不正利用による被害が８０件程度発生。（A社、B社）※ さらに当該事業者が提供するPBXのうち、特定の型番の利用者に被害が集中している模様
- １か月に５～１０件程度の頻度で発生。（C社）
- １か月に５件程度の頻度で発生。（D社）
- 昨年に４０件程度発生（E社）
- 2か月に1件程度の頻度で発生（F社）
- ここ数年被害は発生していない（G社・H社・I社）

被害額

■　本年の被害が総額数千万円程度にのぼる通信事業者もある。利用者の被害額は１件あたり数万円～数百万円程度。

被害の傾向

■　IP電話の被害はやや減少傾向にある一方で、PSTN（固定電話網）への攻撃が増加傾向にある。

■　法人利用者（特に中小企業）における被害が中心で、個人利用者への被害は比較的少ない。

被害の原因

■　PBXに不正アクセスが行われ、SIPサーバのIDとパスワードが窃用された。

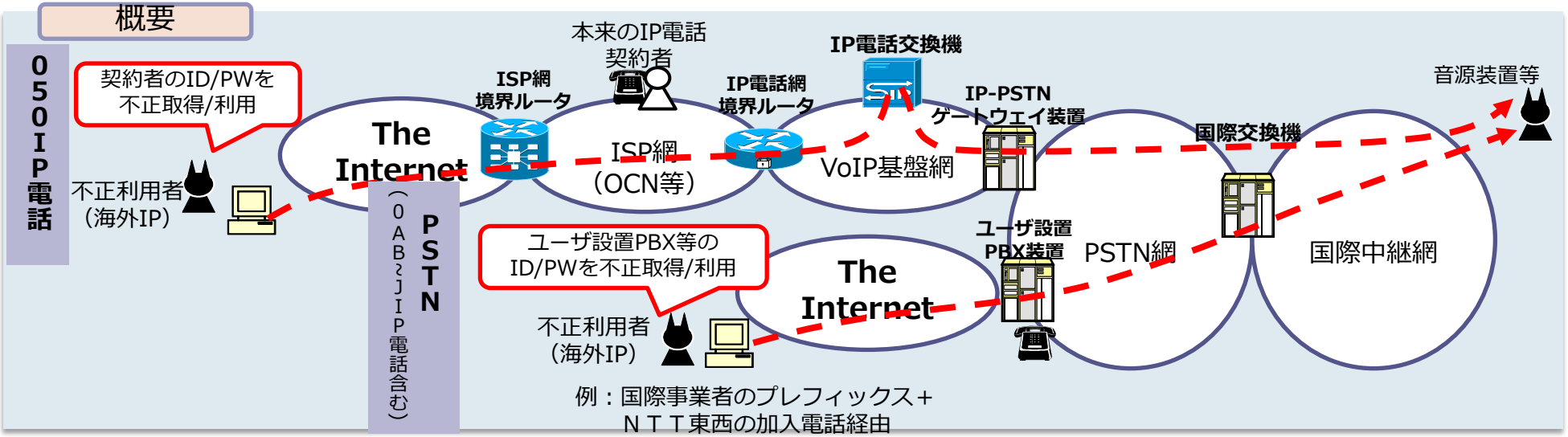
■　PBXに不正アクセスが行われ、任意の端末を組織内の端末になりすまされた、もしくは、特定の番号にかけた場合に国外に転送するよう設定された。

■　利用者サポートとして、ウェブ上でSIPサーバのID・パスワードの案内をしており、そこからID・パスワードが窃用された。

■　また、今回報道になっているケースは特定の事業者の特定の型番にPBXに何らかの脆弱性があったものと推測されるが、事業者において調査中であり、詳しい原因までは分かっていない。

2．国際不正利用の概要（NTTコムの事例）

- 2010年ごろからユーザ端末の脆弱性に付込んだ不正アクセス型の国際電話不正利用が発生。
- 不正利用者は主にアフリカや東欧等の通話料が高額な国へ架電。
- 事業者側からは『正常な通話』としか見えない。（「不正利用」か否か区別がつかない）



不正利用が生じる主な要因

①端末機器の仕様に瑕疵がある場合　ex）A社、L社

②端末機器の取扱説明書に不備がある場合　ex）I社、R社

} 特定の端末機器に集中的に被害が発生

③利用者自身のセキュリティ対策に不備がある場合

} どの端末機器でも被害が発生し得る

利用者設備にセキュリティの穴があれば、何らかの方法でID/パスワードは盗まれる

<u>電気通信事業者だけで不正利用が発生しないようにする抜本的な対策は難しい</u>

- ◆IP電話やPBXのID/パスワードは**お客様の管理**に委ねられ、完全な盗難防止が不可能。
- ◆家庭用インターネットを利用するIP電話では、お客様のIPアドレスが動的に変わることなどから、発信時のIPアドレス等で**不正を判別することは完全には不可能**。

3.事業者の取組むべき対策（検討中の例）

通信事業者における対策（例）

次のような対策の組合わせが有効と考えられる

- 利用者に向けてＨＰ掲載等による利用環境の確認、セキュリティ対策の強化等のお願い
- 利用者からの申請を受けて国際電話の利用を休止
- 国際電話をしばらく利用していない利用者について、同意を得て国際電話の利用休止
- 不正利用の宛先となる国/地域を公表し、利用者側の端末での発信制限を促す
- 国際電話の料金が急激に高騰した場合、利用者へ国際電話の利用の有無確認と利用休止の勧奨
- 利用者と連絡がとれず緊急の場合、一時的に利用の休止を行い、事後に通知を行う
- 特定の番号帯に同時多発的に発信が行われた場合、特定の国／地域宛の発信を一時的に規制
- 海外の特定のIPアドレスから同時多発的な攻撃時に、そのIPアドレスからSIP認証要求の遮断

機器メーカにおける対策（例）

- 不正利用が行われた際に、速やかな脆弱性診断とそれを踏まえたソフトウェアの更新
- 汎用的なソフトウェアを使用している場合における、脆弱性情報の共有

４.NTTComの取組みの紹介（はじめに）

◆NTTComの考える不正利用抑止の考え方

１．不正利用者の検挙

⇒被害者自身に警察へ被害届を実施して頂く必要有り

２．端末機器の仕様や取扱説明書で一層のセキュリティ強化

⇒但し、端末機器や取扱説明書に瑕疵を認識しつつ出荷しているベンダーはいない
　また、お客様自身の使い方で発生し得るのでベンダーでも対応に限界はある

３．啓蒙活動

⇒NTTComはNTT東と連携して国内で初めて不正利用の注意喚起の報道発表を実施
⇒ホームページトップの「お知らせ」に注意喚起を常設（昨年3月ソフトバンクが先行開設したものに追随）
- 不正利用が確認されたケースの紹介（主な発信先の国/地域掲載）
- お客様側で必要な対策の紹介
- NTTComの対策紹介（不正利用時に一時的に発信規制を行う場合があること等）
- 国際電話を利用しない場合の利用休止の申出先をサービス別に分かり易く掲載
- 以上の内容は適宜更新

（参考）2010年＆2012年：JAIPAとも連携して注意喚起の報道発表を実施
　　2013年：TCAを中心に５つの業界団体から注意喚起の報道発表を実施

４．被害の早期検知＆被害額の抑止

⇒平時と比べ短期間で急激に国際料金が高騰した際に利用者へ利用状況の確認

通信事業者が出来る対応

上記４の取組みに関して、NTTComでは電気通信事業法第４条（通信の秘密の保護）＆第121条（役務提供義務）を踏まえつつ、消費者保護の観点から約２年前から導入し、実績を挙げている３つの取組みを紹介します。

４.国際電話不正利用に関する取組の紹介①

ＩＰ電話/ＰＳＴＮ共通

国際電話の料金が急激に高騰した場合に、利用者へ利用状況の確認を行う
なお、連絡が取れない場合は一時的に国際電話の利用休止を実施し、利用者には事後連絡

【平常時】国際電話料金の異常値の定期的な検針

◆事業者として将来の料金回収業務に影響が生じることへの予防措置

【異常検出時】通話先を不正利用時の『規制対地リスト』と照合

◆規制対地リストは、お客様からの不正利用情報を基に、役務提供義務とのバランスを図り作成

・政府機関に関わるような重要な通信がほぼ無い地域であることを確認
・人命に関わるような重要な通信がほぼ無い地域であることを確認
・その国への一定期間内の総トラヒック

【深堀調査】契約者の国際利用状況の確認

◆お客様の当該国への通話料金の確認
◆発側のIPアドレスの確認【IP電話のみ】

【対処】以上により同時多発している状況を総合的に勘案し、不正利用の蓋然性が高い場合であって、複数連絡をしても確認が取れないときは、一時的に利用休止を実施し、利用者には事後連絡

◆連絡が取れない場合は、『消費者保護ガイドライン』の趣旨に準じ複数回連絡を試みる

※連絡が取れないのは、
（個人：就寝中や１ｃｈ利用のため不正利用中により話中となる
法人：退社してオフィスは無人）というケースが多い。

◆契約約款では「不正利用が発生時は、利用休止措置を取る」ことを規定している

導入して約２年間この取組みにより正当な呼を誤って止めたことはない
※連絡が取れず止めたことについても、理由を説明することで理解は得ている

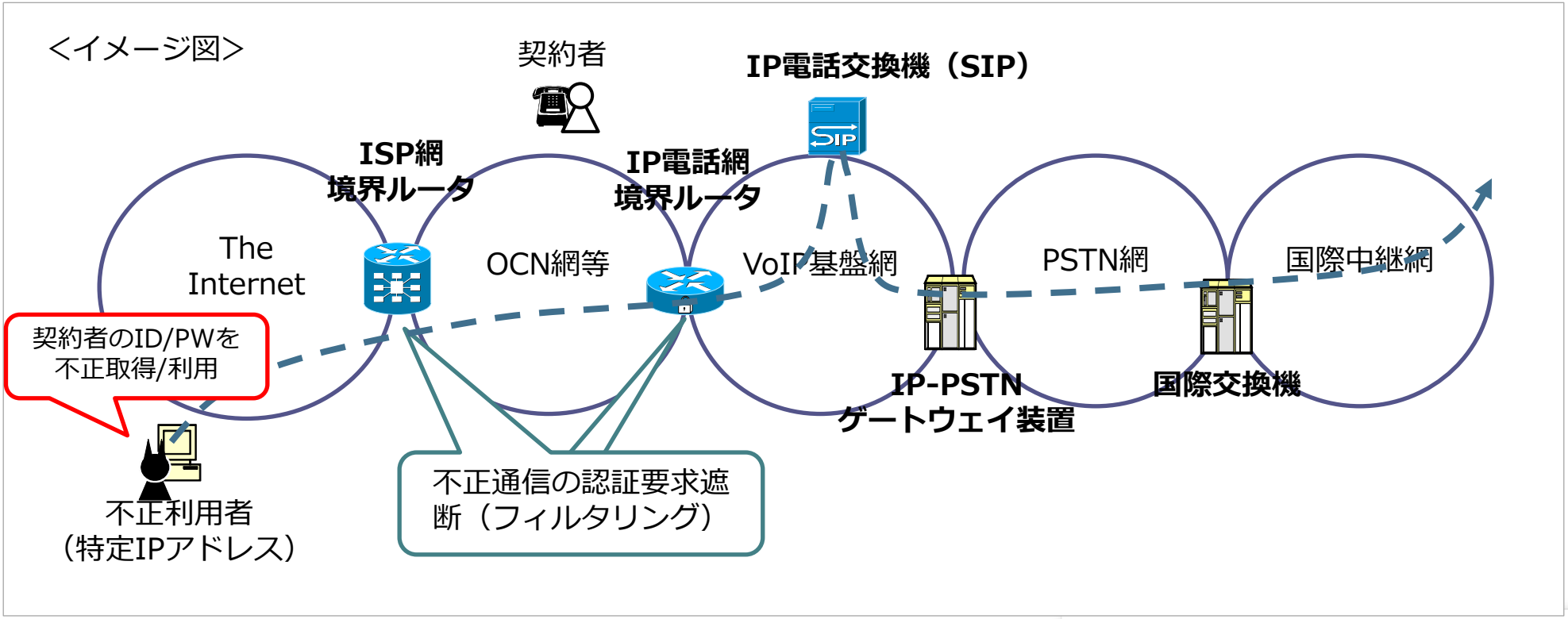
Global ICT Partner
Innovative. Reliable. Seamless.

4.国際電話不正利用に関する取組の紹介②

ＩＰ電話のみ

特定のIPアドレスから同時多発的に不正利用が行われている場合、当該IPアドレスからの呼接続要求を遮断（IPフィルタリング）

◆発側のIPアドレスが平常時と明白に異なる場合に、当該IPアドレスからの接続を遮断



４.国際電話不正利用に関する取組の紹介③

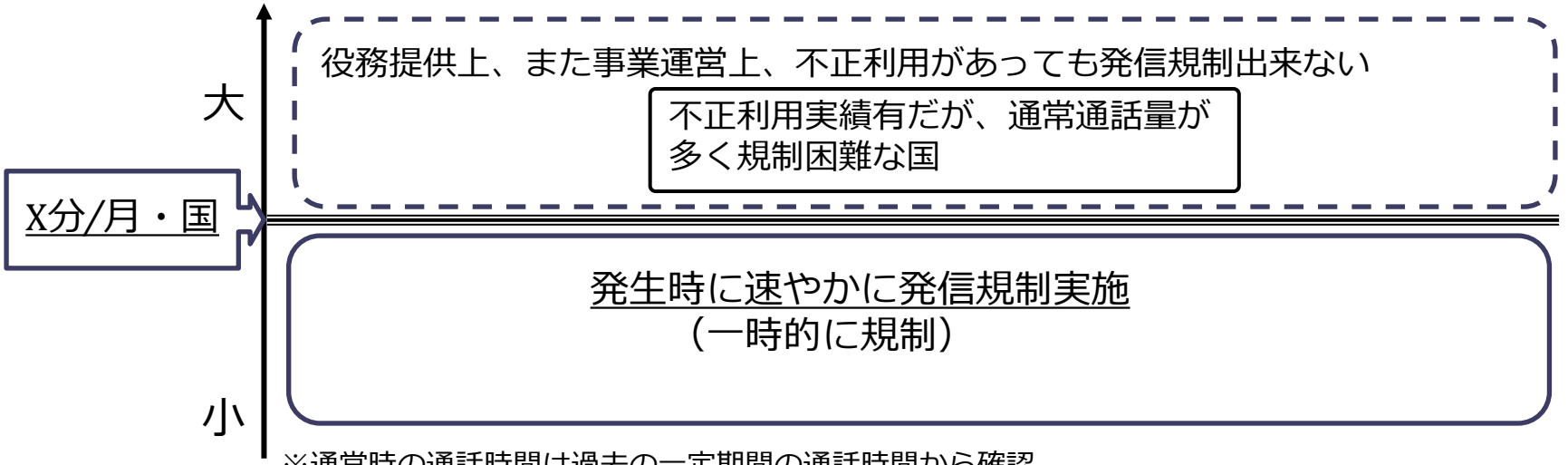
ＩＰ電話/ＰＳＴＮ共通

特定の国に同時多発的に発信が行われた場合、当該国宛の発信を一時的に規制

◆発信規制は、特定の対地のみ識別するものであり、個々の通信先を識別するものではない
- 攻撃先の着信番号を頻繁に変える攻撃は少なくない
- 「通信の秘密」の侵害程度を鑑み、通信先の国番号のみ識別している

} ので、国単位で規制している

◆発信規制国は、公表しないポリシーとしている



※通常時の通話時間は過去の一定期間の通話時間から確認

前述の規制対地リストに該当し、更に平常時におけるその国宛の発信通話時間が一定の基準（「月X分」や「数コール/日」等）に満たない場合であって、同時多発的な発信が行われる等の緊急性が高いときは、その国宛ての発信規制を実施する

NTT Communications Global ICT Partner Innovative. Reliable. Seamless.

5.電気通信業界で取組みたいこと

◆不正利用対地情報の相互共有

- 事業者により不正利用対地に差分が見られる
- 事業者間で不正利用対地情報を共有して予見性を高めることは重要

◆不正利用対地リストの契約者限定周知

- 契約者のみが閲覧できるポータルサイト等で周知

◆攻撃日時（特に時間帯）情報の共有

- 主に攻撃される時間帯を事業者間で共有することにより共通対策を講じる