

第三者の不正アクセスによる電話利用について (ご注意)

2015年6月29日
日本電気株式会社
スマートネットワーク事業部

第三者の不正アクセスによる電話利用について

最近の報道記事等で取り上げられております「IP電話の乗っ取り」の事例のとおり、お客様がご利用中の電話システムへの不正アクセスにより、第三者が利用者になりすまして電話を不正に利用している事例が確認されております。

これらは、インターネットに直接接続した電話システムの設定不備を突いた「なりすまし」が原因です。

弊社IP-PBX・ビジネスホン※は、基本的にインターネットに接続して初期設定のまま利用するシステムではございません。

お客様におかれましては、ご利用中のIP-PBX・ビジネスホンの保守会社に設定状況を確認いただき、十分なセキュリティ対策をご依頼いただけますよう、お願いいたします。

※ UNIVERGE SVシリーズ / APEXシリーズ、および UNIVERGE Aspireシリーズ

【参考】総務省 お知らせ「第三者によるIP電話等の不正利用に関する注意喚起」(2015年6月12日)

http://www.soumu.go.jp/menu_kyotsuu/important/kinkyu02_000191.html

想定される主な不正利用のケース

[ケース1]

IP-PBX・ビジネスホンの追加ダイヤルイン外線アクセス機能、ISDNサブアドレス着信機能、ボイスメールの内線転送機能を悪用

[ケース2]

インターネット経由でIP-PBX・ビジネスホンにアクセスし、内線電話になりすまし

[ケース3]

IP電話機等接続端末に設定されているID・パスワードを悪用

主な対策

ご利用中のIP-PBX・ビジネスホンの保守会社にご相談の上、設定状況の確認、以下の対策を依頼いただけますようお願いいたします。

- IP-PBX・ビジネスホンの設定を確認し、不要な外線着信の有無を確認するとともに、適切な設定を行う。
- 外線着信を追加ダイヤルイン外線アクセス、ボイスメールの内線転送に利用している場合、「利用者のパスワード」および「管理者のパスワード」を第三者に推測されにくいパスワードに変更するとともに、定期的にパスワードを変更する。
- 外線着信からIP-PBX・ビジネスホン経由で国際電話等への発信接続(タンデム接続)の設定を規制する。
- IP電話機等接続端末のID・パスワードを第三者に推測されにくいパスワードに変更するとともに、定期的にパスワードを変更する。
- 定期的に通話ログを確認し、不正利用の有無をチェックする。

Orchestrating a brighter world

世界の想いを、未来へつなげる。

未来に向かい、人が生きる、豊かに生きるために欠かせないもの。
それは「安全」「安心」「効率」「公平」という価値が実現された社会です。

NECは、ネットワーク技術とコンピューティング技術をあわせ持つ
類のないインテグレーターとしてリーダーシップを発揮し、
卓越した技術とさまざまな知見やアイデアを融合することで、
世界の国々や地域の人々と協奏しながら、
明るく希望に満ちた暮らしと社会を実現し、未来につなげていきます。

Empowered by Innovation

NEC