

OUCH!

コンピュータ利用者のためのマンスリー・セキュリティ・awareness・ニュースレター

電話攻撃と詐欺

はじめに

サイバー犯罪者と聞いてまず思い浮かぶのは、おそらくパソコンの画面越しに、インターネット上で高度な攻撃を仕掛けている悪の首謀者ではないでしょうか。確かに現代のサイバー犯罪者は、メールやインスタントメッセージといったテクノロジーを悪用しますが、彼らが被害者を騙す手段の一つとして、電話も使用しています。電話による攻撃には2つの大きな利点があります。1つ目は、メールとは違い、通話を監視することで攻撃を検知し、阻止するセキュリティ技術が少ないということ。2つ目は、電話越しだとより感情を伝えやすいため、被害者が騙される確率が高まるということです。こうした電話による攻撃を検知し、阻止する方法について学びましょう。

電話攻撃はどのように仕掛けられるのか

まず、電話攻撃を仕掛ける攻撃者が、何を目的としているのかを理解する必要があります。彼らは大抵あなたの金銭やパソコンに保存された情報、またはパソコンへのアクセス権（もしくは全て）を狙っています。攻撃者はあなたを騙して、自分がやりたいことをあなたにやらせることで、この目的を達成します。攻撃者は緊急事態が発生しているかのように装い、世界中の人々に電話をかけます。彼らはあなたに恐怖を感じさせ、パニック状態に陥れようとします。そうすることであなたは物事を正確に判断できなくなり、ミスを起こしやすくなります。よくある攻撃例をいくつか挙げます。



攻撃者は、政府の課税部門や徴税サービスを提供する企業の職員を騙り、滞納している税金があるという内容の電話をかけます。今すぐに税金を支払わなければ逮捕されるとほめかし、電話越しにクレジットカードで税金を支払うよう強要します。これは詐欺の手口であり、多くの税金関連の部署は、電話やメールによる通知を一切しません。税金に関する公的な通知は、通常の郵便で送られます。



攻撃者は、Microsoft社のテクニカルサポート部門に所属する人物を騙り、あなたのパソコンがウイルスに感染していると説明します。説得に成功すると、ソフトウェアの購入を強要したり、あなたのパソコンへのリモートアクセスの許可を執拗に求めたりします。Microsoft社は、あなたの自宅に電話をかけるようなことはしません。



銀行口座が凍結されており、復活させるにはこれから伝える番号に電話をかける必要があるという内容の、自動音声メールのメッセージがあなたに届きます。実際に電話をかけると、身元証明を求める自動応答システムにつながり、様々なプライベートな質問をされます。この電話はあなたが利用している銀行からのものではなく、攻撃者が詐欺を目的として、あなたが話す情報を全て録音しているに過ぎません。

自分の身を守る

電話攻撃に対する最大の防御はあなた自身です。次のことを心がけてください。



誰かがあなたに電話をかけ、緊急事態であることを匂わせ、何かをするようせがんできた場合は、疑う気持ちを強く持つようにしましょう。最初は電話の内容に問題が無いように思えても、次第に雲行きが怪しくなってきたと感じたら、いつでも“いいえ”と言い、会話を止めることができます。



かかってきた電話が攻撃であると強く感じたら、単純に電話を切りましょう。電話が正当なものであるか確かめたい場合は、電話をかけてきた組織（銀行など）のウェブサイトを確認し、カスタマーサポートに直接電話をかけてみましょう。そうすることで、相手が正当な組織であることを確認できます。



電話をかけてきた人物の電話番号を信用してはいけません。攻撃者は大抵、電話番号をなりすますことで、正当な組織から、もしくはあなたが住んでいる地域と同じ市外局番から電話をかけているように見せかけています。



電話をかけてきた攻撃者に、一時的なパソコンの操作を許してはいけません。さもないと、ソフトウェアをダウンロードするよう誘導されてしまいます。これは攻撃者がパソコンをウイルス感染させる際に用いる常套手段です。



個人的に知らない人物から電話がかかってきた場合は、直接留守番電話につながるようにしましょう。そうすることで、知らない人物からかかってきた電話の内容を、余裕をもって調べることができます。多くの電話機で設定できるさらに良い方法は、デフォルトでこの機能が有効になる、「おやすみモード」を設定することです。

電話による詐欺や攻撃は、増加傾向にあります。攻撃を検知し、阻止するための最善の防御はあなた自身であることを、覚えておいてください。

リソース

身元情報、プライバシー、& オンラインセキュリティに関する消費者向けの情報：

<https://www.fsa.go.jp/ordinary/chuui/chuui.html>（日本：金融庁）

<https://www.consumer.ftc.gov/topics/privacy-identity-online-security>（米国：連邦取引委員会）

ゲストエディタ

ジェン・フォックス氏は、ALL COVERED社のシニアセキュリティコンサルタントとして、セキュリティ啓発、ソーシャルエンジニアリング、そしてリスクアセスメントの各サービスを提供しています。TWITTER (@j_fox) でも情報を発信しています。



リソース

消費生活相談窓口（日本）：

<http://www.caa.go.jp/consumers/damage/measures/>

電話による詐欺の報告窓口（米国内）：

<https://www.ftccomplaintassistant.gov/#crnt>

ソーシャルエンジニアリング：

<https://www.sans.org/u/Fi5>

OUCH!はSANS Security Awareness プログラムによって発行され、Creative Commons BY-NC-ND 4.0 licenseに従って配布されます。このニュースレターを再配布し、もしくは啓発資料としてご利用いただけますが、コンテンツの改変は認められません。翻訳その他に関しては、www.sans.org/security-awareness/ouch-newsletter までお問合せください **Editorial Board:** Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley | **Translated By:** 内山 貴之, 時田 剛