

セキュリティ

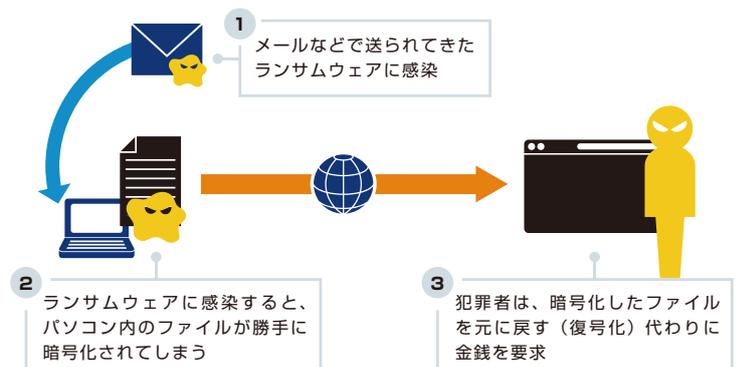
顧客対応力の強化

これだけは知っておきたい サイバー攻撃の種類

マルウェア(ランサムウェア)／標的型攻撃

ランサムウェアとは

勝手にファイルを暗号化し、その復号に身代金を要求する「ランサムウェア」と呼ばれるマルウェアが世界的に流行しているのをご存じでしょうか。すでに多くの企業が被害を受けており、一刻も早い対策が必要です。

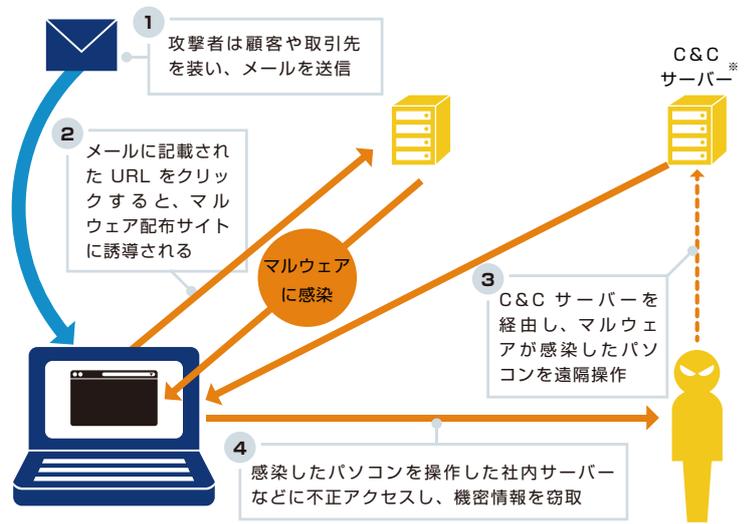


具体的な被害例

米国のある病院において、端末に感染したランサムウェアによってファイルが勝手に暗号化されるという事件が発生した。暗号化されたファイルは業務上極めて重要なファイルであり、業務への影響は極めて大きかった。病院は迅速に業務を再開するために、暗号化されたファイルの身代金として1万ドル以上を支払っている。

標的型攻撃とは

顧客や取引先を装い、マルウェアを感染させることを目的としたメールを送信するなどして社内に侵入し、遠隔操作により機密情報の窃取をはじめとする不正行為を行うのが標的型攻撃です。



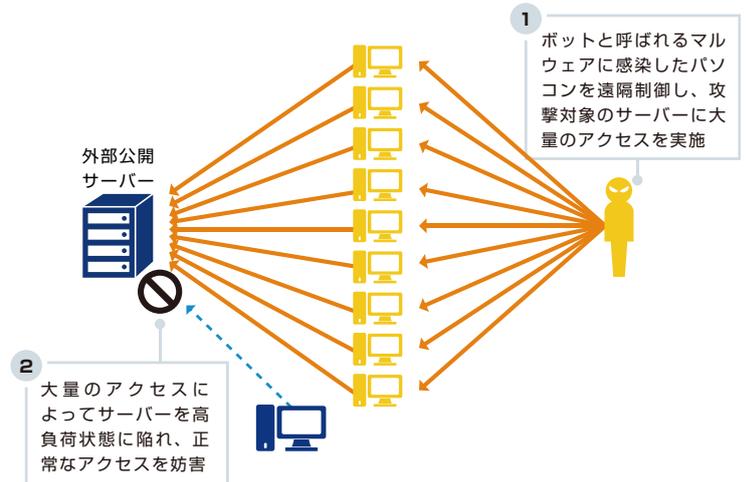
具体的な被害例

ある国立大学の非常勤職員のパソコンで標的型攻撃を目的としたメールを受信した。そのメールは以前からの知り合いであるかのように装い、添付ファイルを開くように誘導する内容であった。添付ファイルはマルウェアであり、これに感染したことで研究成果や公的機関や企業などに属する個人の情報が大量に漏えいした。

公開サーバーへのサイバー攻撃

DDoS 攻撃とは

インターネット上で公開されている Web サーバーなどに対し、大量のパソコンからアクセスし、正常なサービス提供を妨害する攻撃が DDoS 攻撃です。この攻撃を受けると外部からのアクセスが不可能な状態に陥り、たとえば EC サイトであれば機会損失などの被害が発生します。

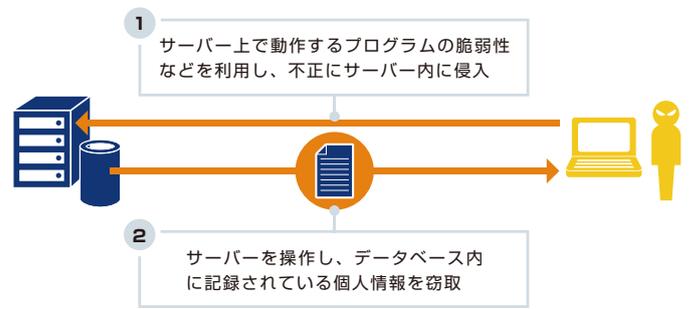


具体的な被害例

ある大手製造業の公式 Web サイトにおいて、1週間近くに渡って Web サイトが閲覧できない状況が発生した。同社は DDoS 攻撃が理由であることを公表、セキュリティ対策の強化などを行って復旧させた。この攻撃はハクティビスト(自分たちの主義主張を訴えるためにサイバー攻撃などを実施する個人や組織)が行ったものと考えられている。

Webサイトへの不正アクセス

脆弱性などを利用して外部から不正にサーバーを乗っ取り、顧客の個人情報などを盗む事件が続発しています。このような事態が発生すれば、ブランド価値の毀損や被害者への多額の賠償により、事業継続に大きな影響が生じかねません。一刻も早い対策が必要です。



具体的な被害例

2015年7月、10を超える団体や企業が相次いで不正アクセスの被害を公表した。その多くで情報漏えいの可能性があるとされており、サービスの停止や不正アクセスの原因となった脆弱性の修正といった対応を迫られることになった。また2015年3月には、複数の団体や企業が不正アクセスを受け、コンテンツを改ざんされるインシデントが発生している。

DDoS攻撃やサーバーへの不正アクセスを防ぐセキュリティソリューションとは
(http://www.ntt.com/bizon/s-7.html#id_3_2)

セキュリティ業務で課題をお持ちのお客さま

フリーダイヤル/ナビダイヤル回線から便利な機能まで、お客さまニーズに合わせた最適なソリューションをご提案いたします。



0120-106107

受付 9:30 ~ 17:00
時間 (土日祝日を除く)