

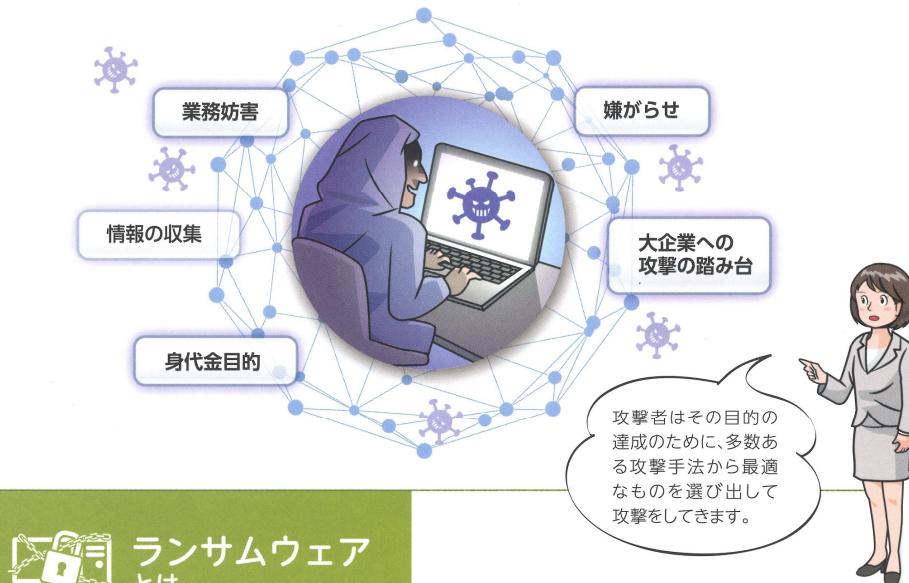
サイバー攻撃は目的・手法ともに多様化

「能力の誇示」から 「アンダーグラウンドビジネス」へ

サイバー攻撃の手段は標的型攻撃だけではありません。

また、その目的も、かつては「いたずら」や「能力の誇示」が主なものでしたが、ネット

ワーク化の進展と情報の価値向上により、「金銭目的」や「特定の組織活動の妨害」など「アンダーグラウンドビジネスとしての活動」に変わりつつあります。



ランサムウェアとは

PCのロックやファイルの暗号化により使用不能にした後で、元に戻すこと引き換えに「**身代金(Ransom)**」を要求する**不正プログラム**。ランサムウェアによって暗号化されてしまうと、攻撃者にしか解除できません。

ランサムウェアはメールに添付されるファイルやメール本文に記載されたURLリンク先のWebサイトから侵入してきます。

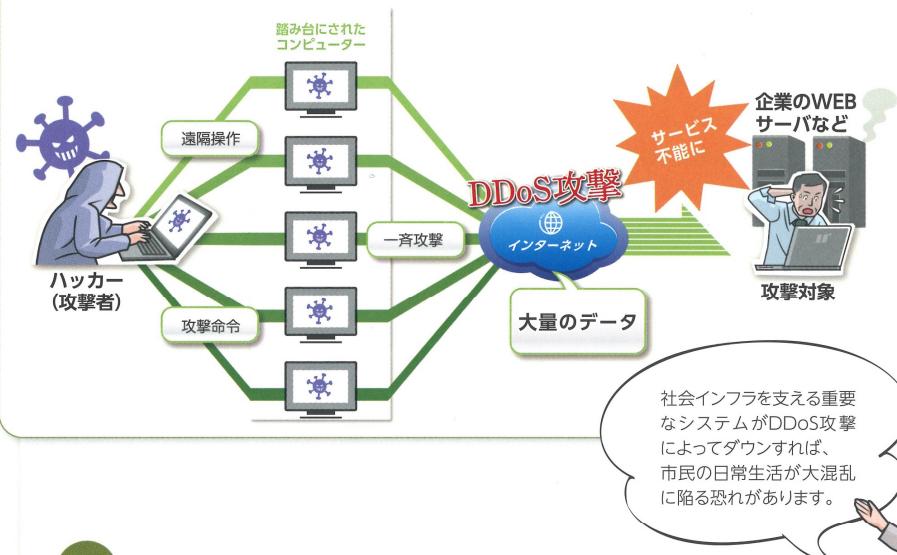


ランサムウェアの画面イメージ

DDoS攻撃とは

ネットワークを通じた攻撃手法の一種で、インターネット上の公開システムへ処理負荷を与える(例:極めて多大なリクエストを一斉に送信する)ことで、**システム機能停止**を狙った攻撃です。

通常のDDoS攻撃は、攻撃者が乗っ取った複数のパソコンを不正に操作し、これらのパソコンから標的のサーバーに対して大量のリクエストを送り付けます。最近ではパソコンだけでなく、監視カメラやテレビなどインターネットにつながるデジタル情報家電も攻撃に利用されます。



事例 サイバー攻撃による被害事例

攻撃を受けた時期	被害企業・団体	概要
2015年5月～6月	公的機関外郭団体	標的型メール攻撃によりPCがマルウェアに感染し、約125万件の個人情報・年金情報が漏えいした。
2015年9月	中央省庁、大手企業	日本の大手企業、中央官庁がDDoS攻撃によりウェブサイト閲覧ができない状態になった。 (ハッカー集団「アノニマス」による攻撃とみられる)
2017年3月	自治体サイト 独立行政法人サイト	サイトに悪意のあるプログラムが設置され、クレジットカード情報やメールアドレス等の個人情報が窃取された可能性。 (Apache Struts 2 の脆弱性を悪用)
2017年5月	全世界	ランサムウェアによるサイバー攻撃。 (Windowsの脆弱性をついたランサムウェアはWannaCryと呼ばれるものの亜種であると考えられる) 日本でも自治体、病院、企業、個人で被害が確認されている。

(公開情報を基にインテリリスク総研作成)