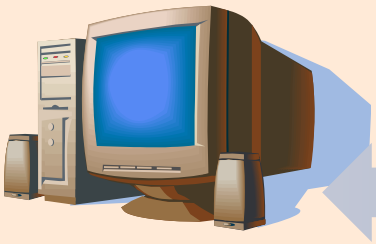
サイバーセキュリティだより

発行 ： 愛媛県警察本部生活安全部サイバー犯罪対策課

令和元年
6月20日
Vol. 31

ランサムウェアの拡散に悪用されるWindowsリモートデスクトップサービス

被害の例



WindowsのRDP（リモートデスクトッププロトコル）を使っている端末（ポート番号3389）

① ツール等を使用してネットに接続しているRDPのポート番号が開いているパソコンを探索。

② RDP経由でリモートデスクトップサービスの脆弱性を利用した攻撃を行う。
※攻撃にパスワード等を必要としない

③ 攻撃対象のパソコンで自動的に、ランサムウェアなどの不正なプログラムが実行される。

攻撃者

要注意

◆ リモートデスクトップサービスを利用しているWindows(Windows7 SP1、Windows Server 2008 SP2、Windows Server 2008 R2 SP1)の場合は、パスワードを設定していても、攻撃者にマルウェアを感染させられてしまいます。

対策

◆ 対象のWindowsを使用している場合は、直ちにマイクロソフトから提供されている対策プログラムをインストールする。

◆ リモートデスクトップサービスが不要な場合は無効にする。

◆ リモートデスクトップサービスを利用する必要がある場合は接続可能なIPアドレスを限定したり、バーチャルプライベートネットワーク（VPN）を利用して接続する。

◆ 適切なパスワードを設定し、パスワード入力を複数回間違った際のアカウントロックを設定する等セキュリティポリシーを強化する。

相談窓口

愛媛県警察本部生活安全部サイバー犯罪対策課 TEL089-934-0110