サイバーセキュリティの置き薬

2019年
第7号

ソフトウェアの脆弱性を狙った攻撃等に注意を

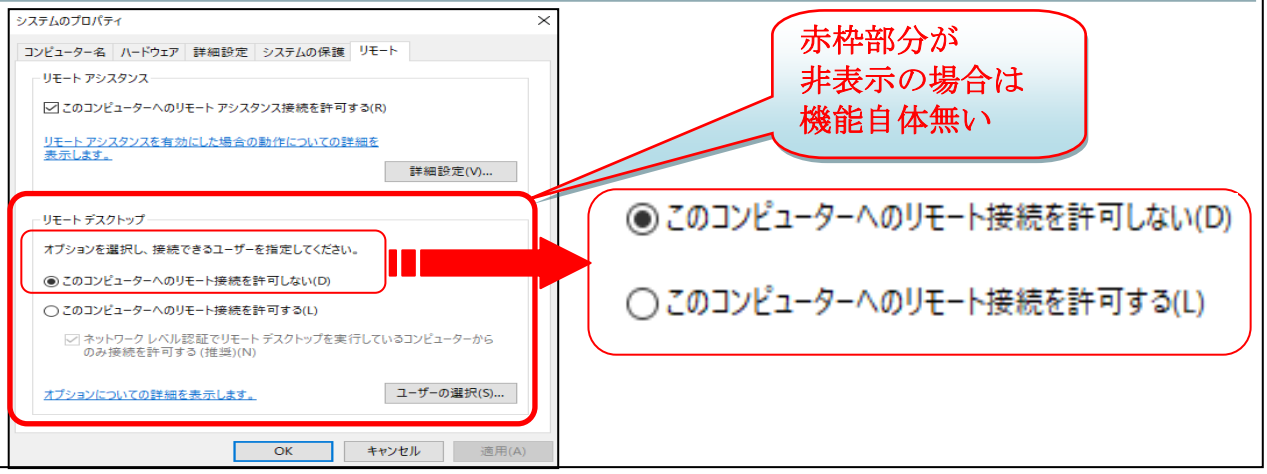
Check! リモートデスクトップサービスを標的としたアクセスが増加

リモートデスクトップサービスは、スマホ・タブレット・パソコンからMicrosoft Windows®をネットワーク経由で操作することができる機能です。マイクロソフト社は5月15日、リモートデスクトップサービスの脆弱性に対する修正プログラムを公開しました。

●脆弱性による被害を受けると

PCのユーザアカウントが乗っ取られ、ランサムウェア等の不正なプログラムが実行されるなど、PCを不正に操作されてしまいます。

●機能の利用状況については、「システムのプロパティ」の「リモート」タブを確認



参照：@Police「https://www.npa.go.jp/cyberpolice」

【ワンポイントアドバイス】

- OSを最新の状態にしましょう。
- リモートデスクトップサービスが不要な場合は許可しない。
- ユーザ名やパスワードは推測されにくいものにしましょう。

Check! ウェブブラウザ「Firefox」に危険度最高の脆弱性、既に攻撃を確認

ウェブブラウザ「Firefox」の脆弱性が確認され、「Firefox 67.0.3」と「Firefox ESR 60.7.1」より前のバージョンに影響があります。

●脆弱性を悪用されると

システムのクラッシュやユーザが悪意あるウェブページにアクセスするとPCを乗っ取られる恐れがあります。

【ワンポイントアドバイス】

- Firefoxのバージョンを最新のものにアップデートしましょう。