長期休暇で注意すべきセキュリティ

概要

春の入社シーズンや、年末年始・お盆等の長期連休は、ウイルス感染などの事故が発生しやすい時期です。

このような時期に発生しやすい事故と対処法についてご案内します。

どのようなリスクがあるか

- マルウェア感染したパコソンの持ち込み
  長期連休のため、自宅にパソコンを持ち帰ったり、今まで他で使っていたパソコンを新たに持ち込んだりするなど、社外でマルウェア感染したパソコンを、社内 LAN に接続したことにより、他のパソコンにも感染が拡大するケースが報告されています。

  連休明けの最初には、最新のパターンにてウイルスチェックを行われることをお勧めします。

- Windows Update されていないパソコンの持ち込み
  長期連休の間に Windows の更新がリリースされる場合も多くあります。
  連休中は使用していなかったパソコンや、インターネットに接続していなかったパソコンが、更新されないままネットワークに接続され、脆弱性の影響を受けてマルウェアに感染するケースが報告されています。

  連休明けの最初には、Windows Update を実施されることをお勧めします。

- データの持ち出し・持ち帰り
  連休中に、USB メモリやクラウドストレージサービス等のデータをコピーし、自宅で仕事をするケースなどがあります。
  USB メモリの紛失、クラウドストレージ設定の誤り等で、データが外部に流出する可能性があります。

  持ち出す必要がある場合は、パスワードや指紋等で暗号化された USB メモリを利用するなど、セキュリティ対策を検討してください。

- 不審なメールの受信
  昨今、実在する企業などを装った不審なメールに関する相談が多く寄せられています。メールの添付ファイルを開いたり、本文中の URL にアクセスしたりすることで、ウイルスに感染したり、フィッシングサイトに誘導されたりしてしまう可能性があります。

  連休明けの最初には、メールが溜まっていることが想定されますので、誤って不審なメールの添付ファイルを開いたり、本文中の URL にアクセスしないように注意してください。

NetStable のログにも注意

上記のように、長期連休等の際には、セキュリティ事故等につながりかねないことから、NetStable で検出されるログにも注意してください。

普段の傾向と違うシグネチャが検出された場合、送信元・受信先 IP アドレスの端末や機器を調査し、きちんと発生原因を追及されることをお勧めします。

まとめ

- 長期連休明けにはマルウェア感染のリスクが高まる
- 連休明けにはウイルスチェック・Windows Update 等をする
- NetStable で検出されるログの変化にも注意する