栃木県警察サイバー対策センター
TOCHIGI POLICE
CYBERCRIME CONTROL CENTER

正規ツールがサイバー攻撃に悪用されています!!
～LotL攻撃（Living off the Land攻撃）への対策～

近年、サイバー攻撃において、

LotL（Living off the Land）攻撃

という手法が増加しています。

LotL（Living off the Land）攻撃とは？

「LotL（Living off the Land）攻撃」とは、攻撃者がマルウェアや不審なツールを持ち込むのではなく、既にシステム内に存在する正規のツールや機能（PowerShell、コマンドプロンプト、リモートデスクトップ等）が悪用されるサイバー攻撃のことです。

※　Living off the Landとは、「その土地にあるもの（既存の資源）を利用して生活する」という意味であり、LotL攻撃は、日本語で「自給自足型攻撃」、「環境寄生型攻撃」と訳されます。

2023年5月、米国家安全保障局（NSA）や米国サイバーセキュリティ・インフラセキュリティ庁（CISA）などは、中国政府が支援するハッカー集団「Volt Typhoon（ボルト タイフーン）」による米国の重要インフラや軍事拠点に対するLotL攻撃を公表し、注意喚起を実施しました。

LotL攻撃によって想定される被害

- ○　長期間の情報窃取
- ○　システムの完全掌握
- ○　ランサムウェアの展開

対策のポイント

① **権限管理（アカウント権限の最小化）**
　管理者権限を付与する範囲を限定する

② **業務で使用しない不要な機能の無効化**

③ **ＥＤＲの導入**
　ＥＤＲ（端末上のプログラム実行等を記録し、不審な挙動を捕捉する製品）によって、実行されたコマンド等の「振る舞い」を監視・分析

④ **従業員に対する教養**
　「不審なメールの添付ファイルやリンクを開いてしまう」といった従業員の些細な行動がサイバー攻撃のきっかけとなるケースは少なくありません
　従業員個々のセキュリティ意識を高めることも重要な対策です
　警察では、企業でのセキュリティ講話を実施しています

「怪しいファイルやマルウェアがない＝安全」といった常識は、もう通用しません!!