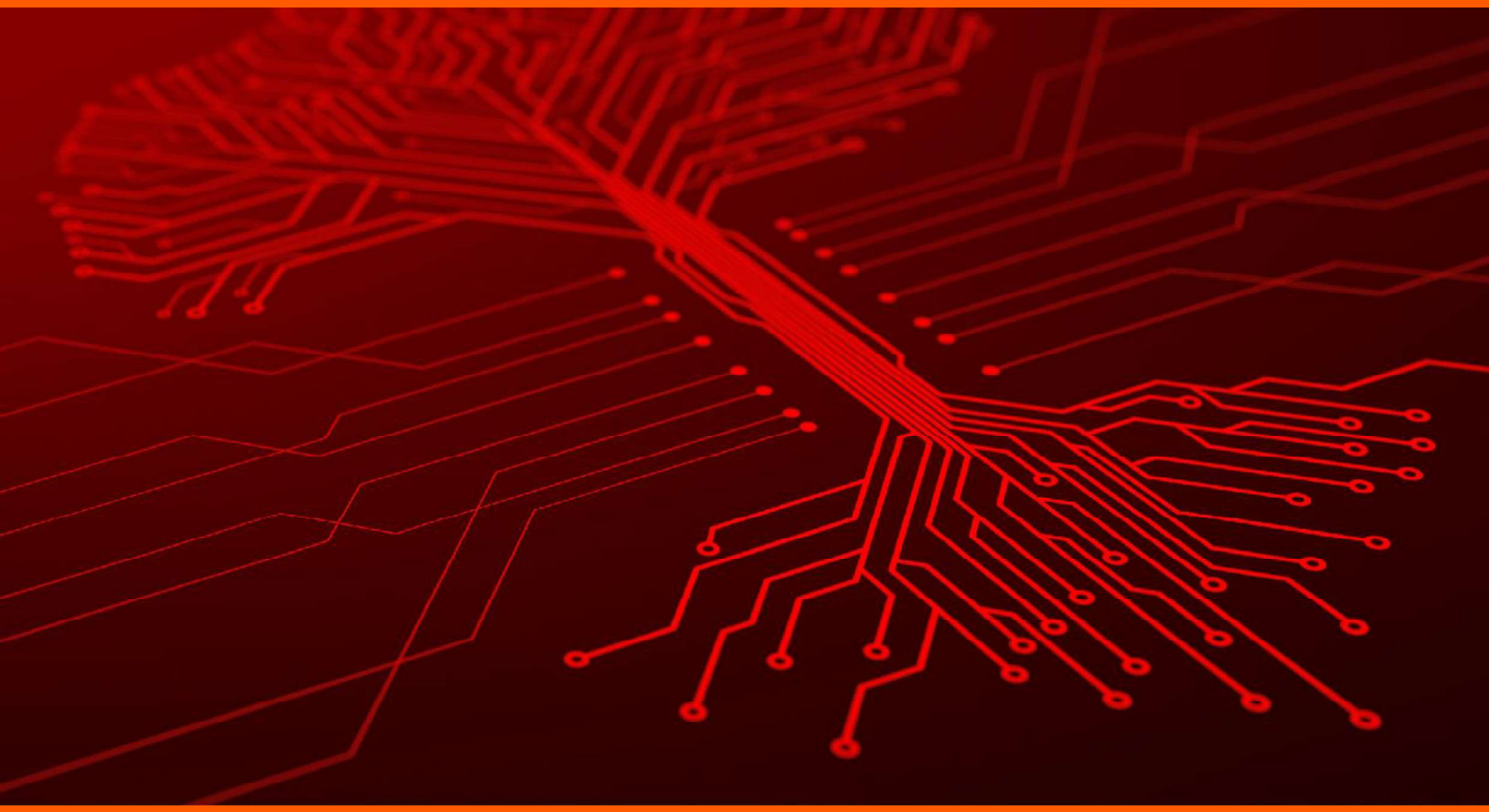
KnowBe4
Human error. Conquered.



# ホワイトペーパー

# Root Causes of Ransomware
# ランサムウェアの根本的原因

Roger A. Grimes著

## はじめに

ランサムウェアは、世界がこれまでに直面した最大のサイバーセキュリティ上の脅威の1つであると言えます。世界中のサイバーセキュリティの専門家が最も懸念することのトップとしてランサムウェアをリストアップしていますが、それには妥当な理由があります。 第一に、ランサムウェアの急増は全世界に及び、その手法は巧妙化し続けています。さらに、小規模から超大規模まで組織の規模に関係なく、何万もの組織が攻撃を受けています。これらの攻撃は、私たちの生活を支える医療施設、石油パイプライン、食品製造の複合企業、警察署、さらには都市全体に被害を与えています。

オーストラリアに本拠を置くマルウェア対策ソリューションプロバイダーである Emsisoft 社は、2020年だけでも世界で180億ドルの身代金が支払われ、総コストは数千億ドルに上ると述べています。(https://blog.emsisoft.com/en/38426/the-cost-of-ransomware-in-2021-a-country-by-country-analysis/)
また、米国サイバーセキュリティ調査会社である Cybersecurity Ventures 社は、ランサムウェアの被害額は2021年に200億ドル、2031年には2650億ドルにまで拡大すると推定されています。(https://cybersecurityventures.Com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/)

では、ランサムウェアに対してどう立ち向かえば良いのでしょうか。その第一の対策としては、ランサムウェアがどのようにデバイスや組織を攻撃するかを理解することです。さらに、デバイスや組織に存在する脆弱性を見極め、そのリスクを組織のすべてのメンバーが各自の問題として認識することが重要になっています。

ランサムウェア対策の鍵は、ランサムウェアの本質を理解することです。ランサムウェアそれ自体は、私たちが抱えている本当の問題ではないのです。ランサムウェアが引き起こす本当の問題は、そこから生まれる最終的な結果であることを認識することです。つまり、ランサムウェアがどのようにして皆さんの環境に最初に入り込み、特権アクセスを得て、システム内に侵害していったかが問題の真の根源です。踏み台となる最初のアクセスがなければ、ランサムウェアによって皆さんの環境を侵害されることはありません。言い換えれば、踏み台となる攻撃を防御できれば、最終結果として発生した業務の中断や損害を引き起こすことはないのです。別の言い方をすれば、もしあなたが魔法の杖を振って、ランサムウェアを退治したとしても、ランサムウェアの侵入を可能にする脆弱性があなたの環境にあれば、**あなたの環境には重大なサイバーセキュリティのリスクが残っているのです。あなたの組織を標的とするハッカーやサイバー攻撃者は、依然としてあなたの環境に侵入することが可能です。**例えば、リモートバッドドアに攻撃をかけるトロイの木馬などを使って、依然として侵入することは可能です。また、キーロガーのトロイの木馬の攻撃者にとっては有効な手段です。文字通り、サイバーセキュリティの脅威の1つを取り除いたとしても、ランサムウェアを仕掛ける攻撃者は、脆弱性があれば、そこを踏み台に侵入することができるのです。ここには、組織的な脆弱性も含まれます。また逆に言えば、ランサムウェアが環境に侵入する可能性のある脆弱性を取り除けば、ランサムウェアだけでなく、同じ脆弱性を利用する可能性のあるあらゆるサイバーセキュリティの脅威のリスクに対応することが可能になります。

ランサムウェアに立ち向かうには、ランサムウェアやマルウェアだけではなく、攻撃者が最初の踏み台として使用する攻撃手段を特定し、これを排除することが不可欠です。本ホワイトペーパーでは、ランサムウェアがほとんどの環境にアクセスするために使用する最も一般的なルートエクスプロイト（発生原因となった攻撃）の方法について探求していきます。

## ハッカーやマルウェアが利用するルートエクスプロイト（発生原因となった攻撃）の方法

悪意のあるハッカーやマルウェアプログラムが、脆弱なデバイスや環境を攻撃するために使用できるルートエクスプロイトの方法は、基本的に9つあります。以下にその9つの方法を列記します。

- プログラミングバク（パッチ利用可または不可）
- ソーシャルエンジニアリング