

## アクロニスが Google の VirusTotal のパートナーシップにより、 機械学習ベースの Acronis PE Analyzer を誰もが使用可能に

～サイバープロテクションのリーダーが保存場所に左右されないデータ保護を実現～

※本リリースは 2018 年 12 月 18 日に米国で発表された[プレスリリース](#)です。

[サイバープロテクション](#)と[ハイブリッドクラウドソリューション](#)のグローバルリーダーであり、[今年 15 周年](#)を迎えたアクロニスは、本日、ML（機械学習）ベースのマルウェア検知エンジン Acronis PE Analyzer を VirusTotal に統合することを発表しました。Google 傘下の VirusTotal は、疑わしいファイルや URL を分析する無料のオンラインサービスです。ウイルス、ワーム、トロイの木馬などの悪意のあるコンテンツをすばやく検出できます。

アクロニスの AI（人工知能）ベースのマルウェア対策機能に最後に追加された Acronis PE Analyzer エンジンは、革新的な機械学習モデルを使用して、あらゆる種類の Windows PE マルウェアを検知する機能を備えています。実行ファイル形式のマルウェアは、今も Windows オペレーティングシステムに対する主要な脅威となっていて、世界各地のセキュリティベンダーのレポートに記載されているように、年々着実に拡大しています。AV-TEST などのセキュリティソフト評価機関では、各種のトロイの木馬、バックドア、ランサムウェア、クリプトジャッカーなどの新しいマルウェアのサンプルを、1 日あたり約 400,000 個登録しています。

アクロニスの機械学習モデルのベースとなるのは、[勾配ブースティング決定木（Gradient Boosting Decision Tree）](#)にいくつかのニューラルネットワークモデルを組み合わせたものです。このモデルを使用して、さまざまな静的特性に基づきこれらの脅威に関する「ポートレート」ファイルが作成されます。機械学習ベースの検知モデルは、モデル自体が小型であり、かつ有効性を備えているため、非常に高速です。また、機械学習モデルはインターネットに接続する必要がなく、独立して動作可能であり、定期的に更新しなくても高い検知率を実現できます。

VirusTotal と統合するまで、スキャナは、AMTSO (Anti-Malware Testing Standards Organization) が規定したテスト基準に従う独立系のセキュリティ研究所から認定されるか、個別のレビューを受ける必要がありました。AMTSO のメンバーであるアクロニスは AV-TEST にこのエンジンを送付し、そこで、Acronis PE Analyzer が PE マルウェアの検知に有効であり、ごく低い誤検知率であるという評価を受けました。

アクロニスが 2019 年にリリースする予定の Acronis PE Analyzer は、新しいサイバープロテクションスイートのコンポーネントとして開発されました。アクロニスでは、VirusTotal の使用によって生成された分析情報を基に、リリース日まで Acronis PE Analyzer を継続的に強化していきます。そして新しいスイートのリリース後も、VirusTotal コミュニティに付加価値を提供できるよう、検知エンジンを引き続き改善してまいります。

アクロニスのテクノロジーオフィサーである[オレグ・メルニコフ（Oleg Melnikov）](#)は次のように述べています。「データプロテクションの本質は、データに対する脅威が進化する速度に応じて、根本から変わります。バックアップデータを狙う悪意のある攻撃が実効性を持たないよう、ソリューションによって防止する必要があります。アクロニスがプロアクティブな防御技術の開発に投資してきたのは、このためです。当社の使命は、あらゆるデータを保護することです。セキュリティ業界全体が Acronis PE Analyzer の検知機能の恩恵を受けるようにするには、機械学習ベースのエンジンを VirusTotal に組み込むのが最善の方法だと考えています」

アクロニスは2018年始めに、ランサムウェア対策ソリューションのAcronis Active Protectionの拡張に合わせて、AIベースのテクノロジーを導入しました。このランサム対策テクノロジーは、Acronis Backup や Acronis True Image など、アクロニスのセキュアなバックアップソリューションに統合されていて、ゼロデイのランサムウェア攻撃をリアルタイムで検知および遮断する機能を備えています。最近では、クリプトマイニングマルウェアを防止できるよう拡張されました。

## アクロニスについて

アクロニスは、革新的な[バックアップ](#)、[ランサムウェア対策](#)、[ディザスタリカバリ](#)、[ストレージ](#)、[企業向けファイル同期・共有ソリューション](#)によって、[サイバープロテクション](#)と[ハイブリッドクラウドストレージ](#)の標準を確立します。[AIベースのActive Protectionテクノロジー](#)、[ブロックチェーンベースのデータ証明](#)、独自の[ハイブリッドクラウドアーキテクチャ](#)により強化されたアクロニスの製品は、物理、仮想、クラウド、モバイルのワークロードおよびアプリケーションを含む、あらゆる環境のあらゆるデータを保護します。

アクロニスは[2003年にシンガポールで設立され](#)、現在世界中で500万人以上の個人ユーザーと、[世界のトップ企業100社のうち79社を含む](#)50万社以上の企業に信頼されています。

## 【本件に関する報道関係者のお問い合わせ先】

アクロニス・ジャパン株式会社 広報担当

TEL: 03-4572-2542 Email: [Media\\_jp@acronis.com](mailto:Media_jp@acronis.com)

株式会社 TYO パブリック・リレーションズ（広報代行）担当 山口・福島・後藤

TEL : 03-5413-4670 Email : [acronis@tyopr.jp](mailto:acronis@tyopr.jp)

Acronis®は米国、およびその他の国における Acronis International GmbH の登録商標です。ここに記載されるその他すべての製品名および登録／未登録商標は、識別のみを目的としており、その所有権は各社にあります。