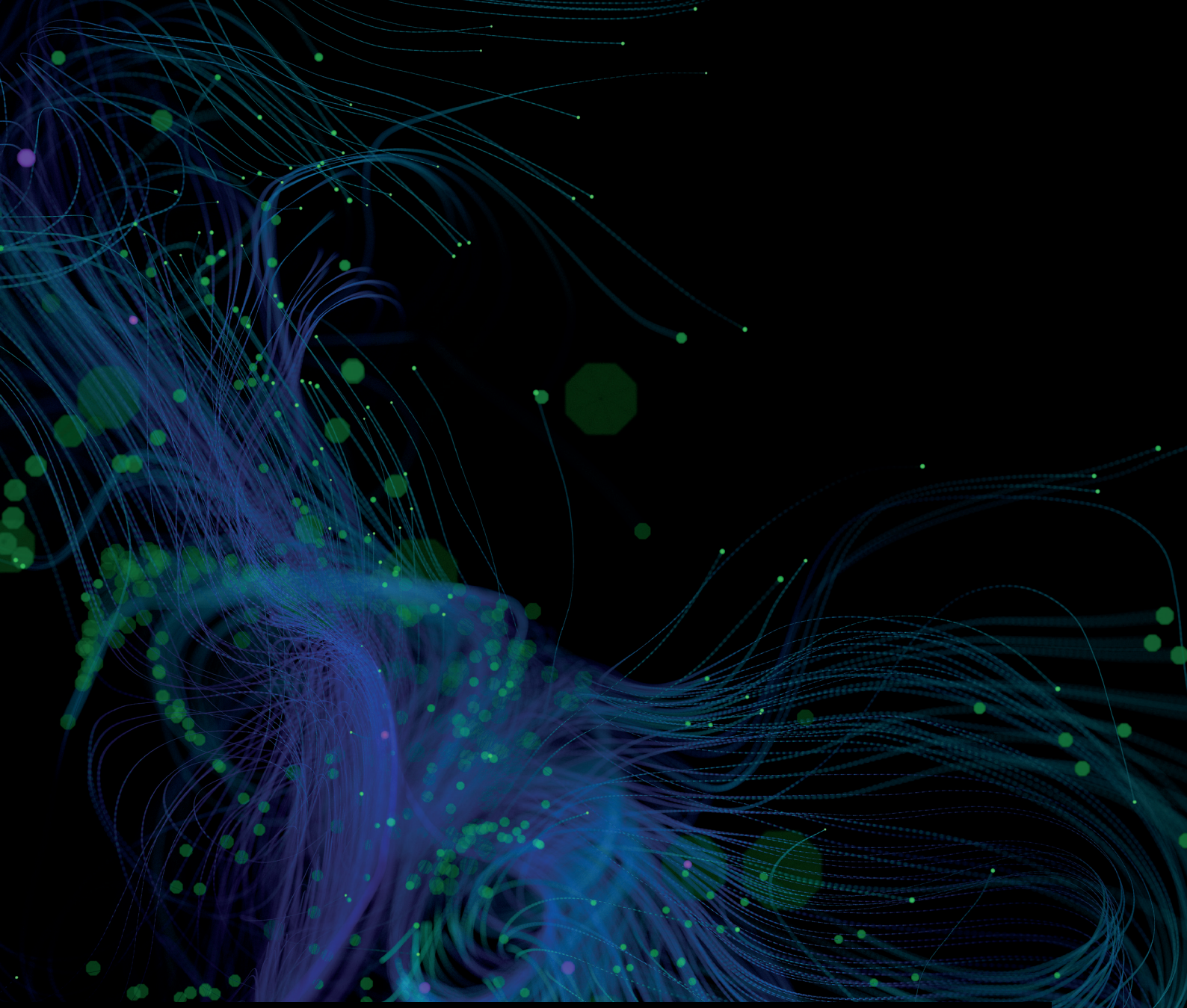


CylancePROTECT® スクリプト制御

機能紹介

CYLANCE

CylancePROTECT スクリプト制御が重要な理由

スクリプトはマルウェア配布の主要なメカニズムとなっています。2017 年に発表されたベライゾンのデータ侵害調査レポートでは、JavaScript がランサムウェアの主な配布経路（59%）であることが指摘されています。その理由は簡単です。悪意のあるスクリプトは、サイバー犯罪者が集う地下サイトで容易に入手可能だからです。また、セキュリティ製品の中にはスクリプトを検出するのが困難なものもあります。なぜなら、スクリプトはセキュリティ管理者も正当な目的で使用するものであり、スクリプトの正邪を判断するにはユーザーの意図を知る必要があるからです。

CylancePROTECT は、統合されたスクリプト制御機能を提供しています。この機能はマルウェア実行防止テクノロジーに基づくものであり、CylancePROTECT の優れた人工知能と機械学習を支援しています。この機能を利用することにより、管理者は自社環境において、いつ、どこで、どのようにスクリプトが使用されるかを制御できます。この機能を活用することによって、悪意のある攻撃者がマルウェア配布に利用する攻撃対象領域を縮小することができます。

CylancePROTECT スクリプト制御の仕組み

CylancePROTECT スクリプト制御は、スクリプトの実行を担うスクリプトインタープリターにスクリプト制御機能を注入し、環境内で実行されるスクリプトを監視して防御することによって、デバイス上で悪意のあるスクリプトが実行されるのを防止します。エージェントは、スクリプトが実行される前に、スクリプトとスクリプトパスを検出できます。

CylancePROTECT スクリプト制御の使用方法

CylancePROTECT スクリプト制御に対して設定されたポリシー（警告またはブロック）に応じて、エージェントは、スクリプトの実行を許可またはブロックします。

警告モード

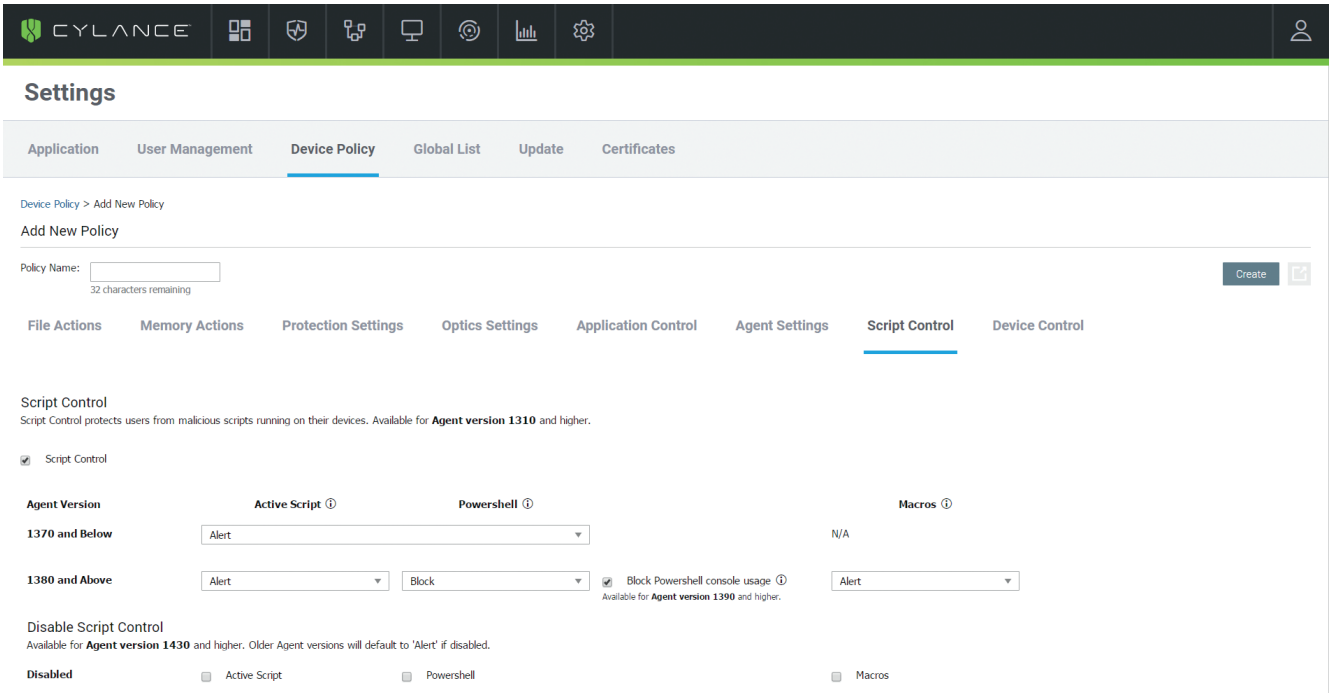
すべてのスクリプトの実行を許可し、スクリプトの実行時に警告します。

管理者は、最初は警告モードで CylancePROTECT スクリプト制御を有効にして、環境で実行されているすべてのスクリプトを監視および観察することをお勧めします。

遮断モード

すべてのスクリプトを遮断します。承認されたスクリプトについては、「これらのフォルダー（とそのサブフォルダー）のスクリプトを承認する」オプションを使用して実行を許可できます（上の情報を参照）。

管理者が環境内で実行されているすべてのスクリプトについて十分に把握したら、設定を遮断モードに変更して、指定したフォルダーからのみスクリプトの実行を許可できます。



Cylance コンソールからスクリプト制御を有効にするには、**「設定」 ->「デバイスポリシー」 ->「スクリプト制御」**に移動して「スクリプト制御」をオンにします。「スクリプト制御」は、警告モードまたは遮断モードで利用できます。

CylancePROTECT スクリプト制御は、PowerShell および Active Scripts をサポートしています。

- PowerShell では、Agent バージョン 1310 以降が必要です
- Active Script では、Agent バージョン 1340 以降が必要です
- Microsoft Office マクロでは、Agent バージョン 1380 以降が必要です

CylancePROTECT スクリプト制御の詳細については、このナレッジベースの記事を参照してください。

FAQ

スクリプト制御の仕組みについて教えてください。

スクリプト制御は、スクリプトの実行を担うスクリプトインタープリターに注入されて、環境内で実行されるスクリプトを監視して防御します。インタープリターに注入されることで、エージェントはスクリプトが実行される前にスクリプトとスクリプトパスを検出できます。スクリプト制御に対して設定されたポリシー（警告またはブロック）に応じて、エージェントはスクリプトの実行を許可または遮断します。

CylancePROTECT スクリプト制御は、どのような種類のスクリプトを検出できますか？

CylancePROTECT スクリプト制御の検出機能は、エージェントのバージョンに応じて異なります。

- PowerShell - Agent 1310 以降
- Active Script - Agent 1340 以降
- Microsoft Office マクロ - Agent 1380 以降

Active Scripting とは何ですか？

CylancePROTECT スクリプト制御では、エージェントは Windows Script Host（WSH）で実行される 2 種類の Active Scripting エンジン（VBScript、JScript）を検出できます。WSH は言語から独立したスクリプト実行ホストであり、目的のスクリプトエンジンを起動することによってスクリプト実行環境を提供します。この場合、スクリプトエンジンとは、VBScript と JScript の Active Scripting エンジンを指します。WSH は GUI モード（wscript.exe）、コマンドラインモード（cscript.exe）のいずれかで実行されます。WSH の詳細については、Microsoft の KB 188135 を参照してください。

PowerShell ISE で実行されるスクリプトが検出されないのはなぜですか？

CylancePROTECT スクリプト制御は、PowerShell インタープリターで実行される PowerShell スクリプトのみを検出します。PowerShell ISE のインタープリターで実行されるスクリプトは検出されません。

CylancePROTECT スクリプト制御は、ブラウザーベースのスクリプトに対する防御機能を備えていますか？

いいえ。CylancePROTECT スクリプト制御は、デバイスのオペレーティングシステム上でネイティブに実行されるスクリプトのみを検出します。

CylancePROTECT スクリプト制御で発生する [*COMMAND*] イベントとは何ですか？

PowerShell が**「遮断」**に設定されており、**「PowerShell コンソールの使用を遮断します」**が有効になっている場合、PowerShell コンソール（またはワンライナーコマンド）の実行はブロックされ、ログに記録されます。実行が試みられたコマンドは、ファイルパス／ファイル名フィールドにレポートされます（最大 250 文字）。

CylancePROTECT の PowerShell 用スクリプト制御を「警告」に設定した場合、PowerShell コンソールの使用を把握できますか？

いいえ。PowerShell コンソールの使用を把握し、それをブロックするには、PowerShell を**「遮断」**に設定し、**「PowerShell コンソールの使用を遮断します」**を有効にする必要があります。

CylancePROTECT の PowerShell 用スクリプト制御は、ワンライナーのスクリプトに対する保護機能を備えていますか？

はい。PowerShell が「遮断」に設定された場合、PowerShell コンソールへのアクセスもデフォルトでブロックされます。承認されたスクリプトは、コマンドコンソール（cmd）で -F パラメータを使用して実行できます。それ以外については、PowerShell コマンド（ワンライナー）のいかなる実行もポリシーに基づいてブロックされます。

例：c:\temp\approved\sample.ps1 が承認された スクリプト（ポリシーの除外フォルダーで指定）である場合、コマンドコンソール（cmd.exe）で「Powershell -F c:\temp\approved\sample.ps1」と入力することによってこのスクリプトを実行できます。

JScript と JavaScript は同じものですか？

いいえ。JScript と JavaScript は似た機能を持っていますが、スクリプトエンジンが異なります。CScript または WScript を通じて実行される JScript と JavaScript のスクリプトは、CylancePROTECT スクリプト制御によって検出され、アクション（警告または遮断）が適用されます。Web ブラウザーを通じてこれらのスクリプトが実行された場合、CylancePROTECT スクリプト制御はそれを検出せず、アクションが適用されることもありません。

Microsoft Office マクロについて

Visual Basic for Applications（VBA）を使用して、Office ドキュメント（Word、Excel、PowerPoint など）の中にコードを埋め込むことができます。Microsoft Office マクロはこの機能を使用しています。マクロの主な目的は、スプレッドシート内のデータ操作やドキュメントのテキストの書式設定など、一連の決まった操作を簡略化することです。ただし、マルウェアの作成者は、マクロを使用してコマンドを実行することでシステムを攻撃します。システム操作を試みる Microsoft Office マクロは、悪意のあるアクションであると見なされます。CylancePROTECT のエージェントは、マクロによって実行され Microsoft Office 製品の外部に影響する、悪意のあるアクションを検出します。

ヒント：Microsoft Office 2013 以降、マクロはデフォルトで無効になっています。ほとんどの場合、Office ドキュメントのコンテンツを表示するために、マクロを有効にする必要はありません。信頼できるユーザーから受け取ったドキュメントである場合のみ、また、マクロを有効にする適切な理由がある場合のみ、マクロを有効にします。それ以外の場合、マクロは常に無効にしてください。

Cylance Japan 株式会社
〒100-6510
東京都千代田区丸の内 1-5-1　新丸の内ビルディング 10F
www.cylance.co.jp
03-6386-0061 (代表)

201803-FF003