Advanced Threat Protection

DR151026D

2015 年 12 月

Miercom

www.miercom.com

目次

要約

Miercom では、Symantec Advanced Threat Protection アプライアンス、Cisco SourceFire、FireEye 1310 製品を対象として、独立した第三者による検証を実施しました。

セキュリティ有効性テストでは、従来型、AET (Advanced Evasion Technique)、APT (Advanced Persistent Threat)、ボットネット、RAT、アクティブな脅威、悪質なドキュメントなど、複数のマルウェア脅威に対して検出機能とブロック機能を検証しました。

Symantec ATP ソリューションは、多様なマルウェア脅威を検出できることを実証しました。Symantec ATP ソリューションは 2 つの競合製品よりも 18% 以上優れた性能を示し、7 種類のマルウェアカテゴリのうち 6 種類に対して平均をはるかに上回る保護性能を発揮しました。

主な調査結果

- Symantec ATP のマルウェア検出率は、競合製品よりも 18.5% 高いものでした。
- 現在最も複雑な脅威とされる高度な回避技術に対する検出スコアは 100% です。これは競合ベンダーよりも 95% 高い数字です。
- レポートコンソールにはタイムラインビューが表示され、悪質なイベントを日付やカテゴリごとに簡単に追跡できます。

Symantec ATP ソリューションは、満足のいくマルウェア検出性能を示しました。特に、よく知られたマルウェアだけでなく、未知のマルウェアまで効果的に検出して駆除できる点が優れています。

Miercom
CEO
Robert Smithers

概要

セキュリティをめぐる問題の多くは、マルウェアがセキュリティ防御を突破する理由と手口に関連しています。その理由の 1 つは、悪質なコンテンツの大半が常に変化を遂げていることにあります。

シグネチャベースのウイルス対策、静的なセキュリティゲートウェイ、ファイアウォールテクノロジを回避するように図っているのです。

このレポートでは、アクティブで最も巧妙化が進んでいるマルウェアに対して Symantec ATP ソリューションがどのような対応を行ったかを示します。具体的には、複数のカテゴリを対象とした検出レベルについて、競合製品と比較しました。今回取り上げられたのは、Symantec ATP、Cisco SourceFire 侵入防止システム、FireEye セキュリティアプライアンスです。

Symantec ATP

シマンテックが提供するネットワークセキュリティソリューションです。これはハードウェアアプライアンスに導入することも可能ですし、本テストのように VMware ESXi 5.5 を使用した仮想マシンに導入することもできます。そのため企業環境にも迅速に導入することができます。次のような独自のツールを駆使して、実際の脅威に対する保護を提供します。

- Symantec Cynic はマルウェア分析サービスであり、悪質な可能性があるファイルを実行して多層にわたる調査を行い、高度な脅威とゼロデイ攻撃を検出します
- Symantec Insight はレピュテーションベースのテクノロジであり、履歴と普及度に基づいて不審なファイルを特定します
- Symantec Vantage はネットワークトラフィックをスキャンするテクノロジであり、エクスプロイト、悪質なファイル、ネットワーク攻撃を検出するとともに、環境内で現在感染中のエンドポイントを特定します
- Symantec DeepSight はインテリジェンスサービスであり、観測されたイベントに関する詳細情報を提供します

Symantec ATP は不審なファイルや URL データを迅速に収集して分類し、ビジュアル表示された調査機能を提供します。そのため、セキュリティアナリストはネットワークの脆弱性を迅速に修復して企業を安全に保護できます。このソリューションのテストでは、これらのツールを使用しています。ここでは、シミュレーションされた企業環境を実際に攻撃してみた結果を示します。

方法

今回の脅威検出評価のテスト方法は、悪質なコンテンツのネットワーク侵入をブロックするデバイスを対象とした、Miercom の一般的なセキュリティテスト手法に基づいています。

セキュリティ機能の評価

Symantec ATP 製品を次の観点から評価しました。

機能	説明	評価方法
検出	既知の脅威および従来型の脅威を特定する能力	割合（%）

テスト対象製品

シマンテック製品による脅威検出の有効性を、次の競合製品と比較調査しました。

シマンテック Advanced Threat Protection	Cisco SourceFire 侵入防止システム	FireEye セキュリティアプライアンス
バージョン 2.0.0.58	バージョン 5.4	バージョン 7.5.1
• Symantec Cynic のマルウェアデトネーションおよびグローバルインテリジェンスにより、ネットワーク内の悪質なコンテンツを検出 • Symantec Vantage により、ネットワーク侵入を検出 • Symantec Insight のレピュテーションベースによるセキュリティテクノロジが、既知の脅威とアクティブな脅威に対して警告 • Symantec DeepSight 受信トラフィックスキャナが、エンドポイントの脆弱性を検出	• 初期検出を回避するマルウェアの監視、保存、再呼び出しを繰り返し行う機能 • 侵入を試みるマルウェアの種類、脅威レベル、ふるまいを可視化 • 調査がインテリジェンスの強化につながり、今後の攻撃に備えてシステムリカバリを改善	• ファイアウォール、ウイルス対策、Web ゲートウェイ、侵入防止システムで見逃された脅威の検出 • データの盗難およびボットネットを発信トラフィックで防止 • 受信トラフィックおよび多階層の調査にさまざまな手法を適用 • リアルタイム処理の誤検知分析を搭載し、アクティブな脅威のデータベースを継続的に拡充して、電子メール経由のフィッシングを防止

セキュリティ脅威のサンプル

悪質なソフトウェアやマルウェアは、コンピュータまたはネットワークの運用を阻害したり、機密情報の収集を行ったり、コンピュータシステムへのアクセスを試みたりするソフトウェアです。これらのサンプルは Miercom のハニーポットで収集したものです。このテストのために複雑でリアルなマルウェアを準備しました。このセットには従来型のサンプルも含まれていますが、テストで焦点となったのは最も高度で最新のサンプルの検出です。

アクティブな脅威	外部のリソースと非公開のハニーポットから収集した、変化し続ける未知のマルウェア。これらのカスタマイズされた未検出サンプルと APT には、暗号化、ブラックパッケージ化、通常のトラフィックを使用するペイロードなど、ウイルス対策を回避する手法が組み込まれていました。
AET (Advanced Evasive Technique)	既知の回避手法を組み合わせて新たな攻撃を作成し、複数のレイヤーから同時に実行するネットワーク攻撃。コードは必ずしも悪質なものとは限りませんが、回避型の攻撃であるためアクセスを検出できないことが危険といえます。現在、ベンダー製品で認識している既知の回避手法は約 200 種類あります。AET では、いくつかの回避テクニックを組み合わせるだけで、新しいものを数百万種類も作り出すことができます。
APT (Advanced Persistent Threat)	人目につきにくい継続的な一連のコンピュータハッキングプロセスであり、多くの場合、特定の団体を標的とする人物によって実行されます。このマルウェアは通常、ビジネスまたは政治的な意図で企業や国家を攻撃します。APT は段階的なペイロードで構成される場合があります。これが有効化されると、攻撃者はリモートからコマンドラインでシェルにアクセスできるようになります。これらのペイロードはランダム化や回避テクニックにより隠蔽されていてウイルス対策を迂回します。テストで使用した既知の APT サンプルは、複数のソースから取得されたものです。
ボットネット	コマンドアンドコントロールという手法を使用する、相互に接続した通信プログラム。攻撃者からの指令やコマンドを中継者が受け取り、感染したすべてのホストに転送します。ボットネットは通常、スパムや DDoS（分散サービス拒否）攻撃で使用されます。このテストでは、高対話型ハニーポットで収集された Zeus および Citadel ボットネットの亜種を使用しました。

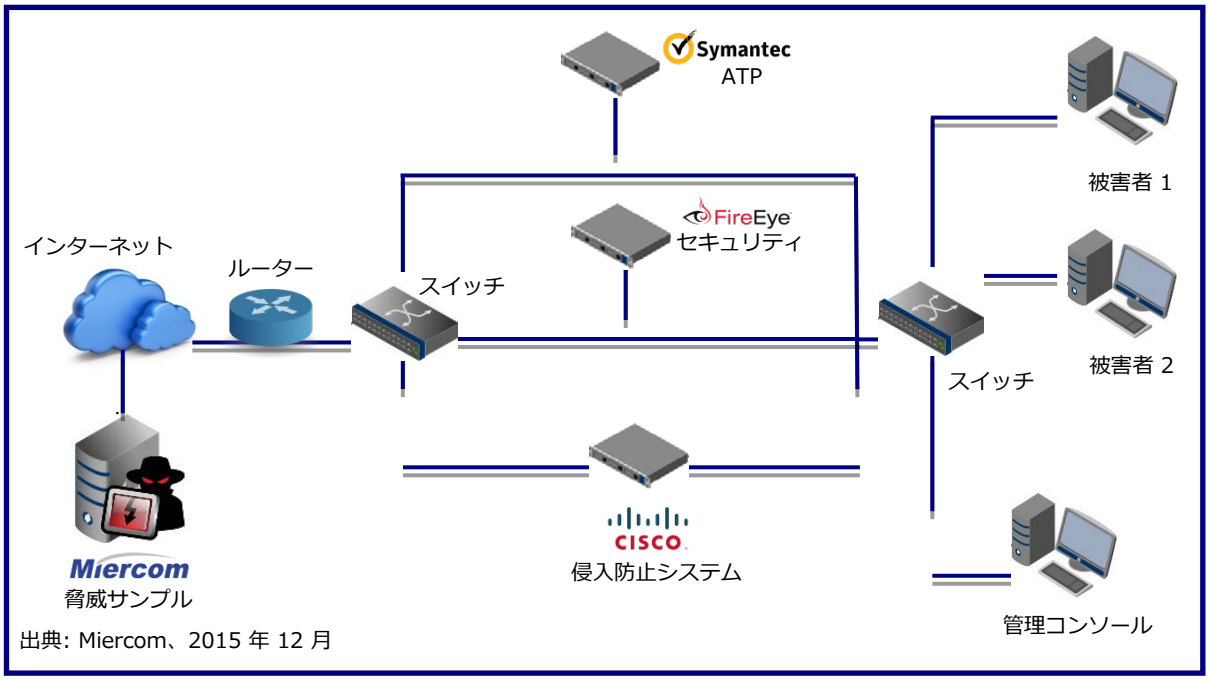
従来型	サンプルには、活動期間が 30 日以上にわたる既知のマルウェアの亜種が数百種類含まれています。これらマルウェアは、主にウイルスとワームで構成されています。
悪質な文書	これらのサンプルは、既知のマクロウイルスが含まれる Microsoft Office 文書（Word、PowerPoint、Excel ファイル）と、各種のウイルスや APT やワームが含まれる PDF ファイルを組み合わせたものです。
RAT	RAT (Remote Access Threat) は、正常で使用可能であることを装う悪質なコードです。多くの場合、他の正当なソフトウェアの中に偽装されて組み込まれています。被害に遭ったホストで RAT がアクティブ化されると、そのホストを完全にリモートで制御できるようになります。

テストツール

Miercom では、業界をリードするテストツール、スクリプト、データベースを独自に組み合わせることにより、現実に即した強力で包括的なテスト環境を用意しました。高度な脅威検出に関する当社の調査から得られたサンプルも、シマンテックおよび競合他社による今回のテストの対象となりました。

テストパートナー

テスト環境図



出典: Miercom、2015 年 12 月

現実の環境をシミュレーションするため、マルウェアは実際にインターネットから複数の外部ソースを通して収集しました。これらの手法には、Symantec ATP およびその他の DUT（テスト対象デバイス）の背後にある保護されたネットワーク内からの http、https、FTP ファイル初期化などがあります。悪質なサンプルは通常のレイヤー 3 ネットワークルーターを経由して DUT に直接送り、ローカル LAN に到達する前に徹底的に調査しました。テスト環境としては、FireEye 1310、Cisco Source Fire、Symantec ATP を、ESXI 5.5 サーバーでホスティングされる事前構成済みの仮想マシンに設定しました。DUT は、攻撃対象となるマシンで構成されるレイヤー 2 ネットワークスイッチに接続しました。

テスト環境構成

アプライアンスの設定は、管理コンソールで提供されているすべてのセキュリティ関連カテゴリを検出し、利用可能な防御をすべて利用するようにしました。どの製品もデフォルト設定で使用しました。

製品の配備

Symantec Advanced Threat Protection	Cisco SourceFire 侵入防止システム	FireEye セキュリティアプライアンス
TAP モードでの導入	**インラインでの導入**	**TAP モードでの導入**
• 送受信パケット情報の監視 • リアルタイム保護なし • トラフィックと悪質なデータを、管理コンソールで受動的に監視 • 攻撃が発生しない限り、対応は行わない	• システムをネットワークのデータパス上に配置して、トラフィックを分析 • リアルタイム保護 • 悪質でないトラフィックの基準を逸脱したトラフィックを記録 • トラフィックを本来の送信先に転送するか検疫するかを判断	• 送受信トラフィックのパケット情報を監視 • リアルタイム保護なし • トラフィックと悪質なデータを、管理コンソールで受動的に監視 • 攻撃が発生しない限り、対応は行われない

Symantec ATP は TAP モードで導入されました。これはトラフィックを監視する受動的なアプローチです。一方、インライン導入は、センサーをネットワークパスに直接配置してトラフィックを調査するものです。TAP モードではリアルタイムの保護を実現できません。また、攻撃がすでに発生していない限り、対応は行われません。

攻撃対象の環境

テスト時には、VMware ESXi リリース 5.5 でホスティングされた仮想マシンが、攻撃を受けるコンピュータとして保護の対象となります。これらの仮想マシンは、悪質なサーバーからの攻撃にさらされました。サーバーから攻撃対象のマシンにサンプルを転送したのち、セキュリティ製品のログファイルを確認しました。ログファイルでは、サンプルの検出有無、ダウンロードを最初にリクエストしてから検出までにかかった時間、セキュリティ製品が攻撃の検出後に修復ステップを実行する場合にはその詳細を確認しました。

結果の概略

セキュリティ有効性テストでは、各ユニットが実際の脅威をどれだけ正確かつ明確に短時間で検出できるかを検証しました。市場には多様なセキュリティ製品が存在します。そのため、検出率の他に、製品が提供するリスク緩和策や企業環境への導入のしやすさも重要です。

	シマンテック
検出	92.1%

検出

Symantec ATP は、92.1% のマルウェア検出率を示しました。競合製品より少なくとも 18.5% 高い値です。検出率が特に高かったマルウェアは、AET、APT、ボットネット、従来型、RAT でした。特に注目すべきことは、AET と APT の検出率が 100% ということです。これらの高度な回避型および持続型のマルウェアは、現在最も問題となっている脅威だからです。競合製品の AET カテゴリでのスコアは、著しく低いものでした。

フォレンジックレポート

レポートインターフェースは使いやすいものです。すべての脅威を時間、名前、送信先で分類したリストが自動的に提供されました。ダッシュボードのタイムライン機能では、検出された脅威に関する大量の情報が発生日時に沿って整理されて表示されます。そのため、攻撃の追跡が容易になります。

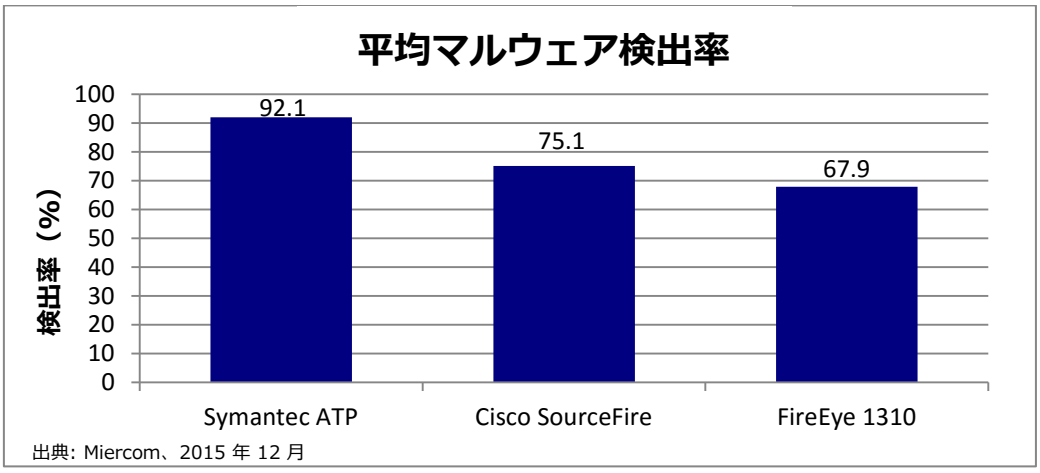
マルウェア検出機能の競合製品比較

説明

マルウェア検出機能とは、悪質なサンプルと悪質でないサンプルが混在した中から、悪質なソフトウェアの存在をどの程度正確に警告するかを示します。

競合製品の結果

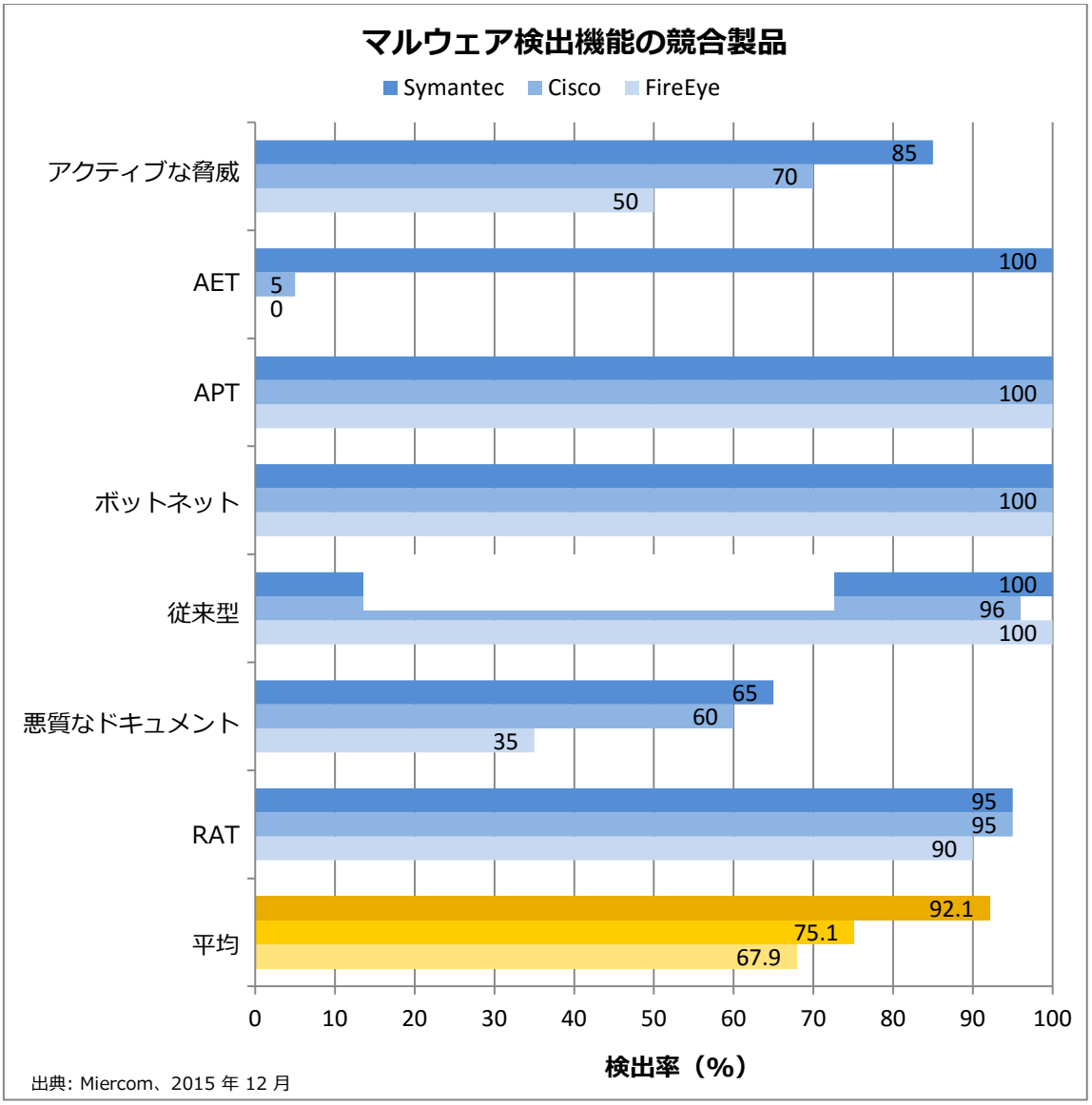
次のグラフは、テストを実施したサンプルセット内の各マルウェアカテゴリに対して検出されたサンプルの平均の割合を表しています。検出は、正常なトラフィックも混在するサンプルセットから特定できたサンプル数として定義されます。



シマンテックの平均マルウェア検出率は、競合製品を上回りました。Cisco SourceFire と比べて 18% 以上、FireEye と比べて 26% 以上高い数字です。

これらのマルウェア検出結果は、さらにカテゴリごとに分けられました。これにより、特定のマルウェアについて各製品がどれだけ検出できるのかが分かります。アクティブな脅威、AET、APT などのマルウェアは、他のマルウェアよりも深刻な脅威と考えられます。これらは高度に複雑なうえに回避型かつ持続型であるため、企業にとって最も深刻なマルウェアです。

次のページのグラフでは、平均検出率およびマルウェア種類ごとの検出率を、競合製品と比較して示しています。



さまざまなマルウェアを混在したトラフィックを送信したところ、シマンテック製品は最高水準の検出率を示しました。特に、最も複雑な脅威である、アクティブな脅威、AET、APT については最高の検出率です。Cisco 製品や FireEye 製品と比べて 95% 以上の数字でした。シマンテックの平均検出率は、競合製品と比べて少なくとも 18.5% 高い値を示しました。

TAP モードの場合、検出されたサンプルは各製品のコンソールで確認できました。シマンテック製品ではすべてのカテゴリのマルウェアに対して最高の検出率が確認され、AET と APT は 100% の検出率を記録しました。

フォレンジックレポート

説明

将来に向けた予防措置をとるためには、脅威分析が不可欠です。収集したデータの追跡、定量化、分析が的確に実行できれば、企業ネットワークへの侵入を試みる最新型で最も蔓延している脅威に対する備えを強化することができます。レポートインターフェースは、情報の詳細度と使いやすさで評価しました。

結果

悪質なファイルや URL の送信元と送信先が表示されるため、ユーザーは Web ベースの脅威とファイルベースの脅威を簡単に見分けられます。脅威を種類と名前によって分類したリストが作成され、ファイルパスも提供されました。さらに、その脅威に関連すると考えられる他の悪質なインシデントの情報も提供されました。タイムライン機能では、脅威が発生した時刻をユーザーがビジュアル表示で追跡できます。また、全世界およびローカルでの拡散状況などのコンテキスト情報や、攻撃元に関する DeepSight 情報も提供されます。

公正なテストに関する通知

このレポートで取り上げた製品のベンダー全社に対しては、テストの実施前、実施中、実施後において、テスト結果について意見を述べて製品の性能を実証する機会が付与されました。Miercom が公開調査でテストを実施した製品のベンダーが調査結果に異議を持つ場合には、無償で再テストを実施して製品の性能を実証する機会が付与されます。

どのベンダーも、自社で性能を実証して Miercom に示すことができます。新しいデータがあれば、Miercom はこれらの結果を更新します。

Miercom について

Miercom は主要な業界誌などの出版物で数百件のネットワーク製品分析を公開しています。Miercom は紛れもなく、トップクラスの独立系製品テストセンターであるという評価を受けています。

Miercom が提供する非公開のテストサービスには、競合製品分析や個別製品の評価などがあります。Miercom は Certified Interoperable™（相互運用性認定）、Certified Reliable™（信頼性認定）、Certified Secure™（安全性認定）、Certified Green™（環境認定）などの総合的な認定とテストプログラムを扱っています。また、製品の有用性と性能を評価する Performance Verified™（パフォーマンス検証）プログラムで製品を評価することもできます。これは業界で最も徹底的であり、信頼されている評価プログラムです。

このレポートの使用について

このレポートに記載したデータは正確を期すようあらゆる努力を行っていますが、誤りや見落としが発生する可能性があります。また、このレポートに記載した情報は各種テストツールに基づいたものであり、その精度については当社の管理外にあります。さらに、このドキュメントはベンダーからの説明に基づいており、それに対して Miercom では妥当な検証を行っていますが、100% 確実であるかどうかまでは検証できません。

このドキュメントは Miercom から「現状有姿」で提供するもので、このレポートに記載された情報の正確性、完全性、有用性、適合性については、黙示的にも明示的にも、いかなる保証、表明、約束はいたしません。また、それに関して直接または間接を問わず、いかなる法的責任も負いません。