シスコのエグゼクティブ向け概要

2026 年 7 月

重要なインフラストラクチャの新たな運用モデル

AI 時代のサイバー防御に関するエグゼクティブ向け概要

目次

継続的な防御へのシフト

フロンティア AI モデルによって脅威の状況が根本的に変わりました。これらのシステムを使用すると、脆弱性の特定、エクスプロイトの作成、攻撃経路への連鎖がマシンスピードで可能になります。これは一時的なパッチの適用サイクルではありません。お客様の環境が侵害されるスピードを恒久的に変えてしまう変化です。

リスクを書き換える 2 つの力

01 パッチの適用サイクルをしのぐスピード

情報開示から実際の攻撃までの時間はすでに短くなりつつありました。フロンティア AI により、タイムラインが数時間に短縮されました。

02 参入障壁の消滅

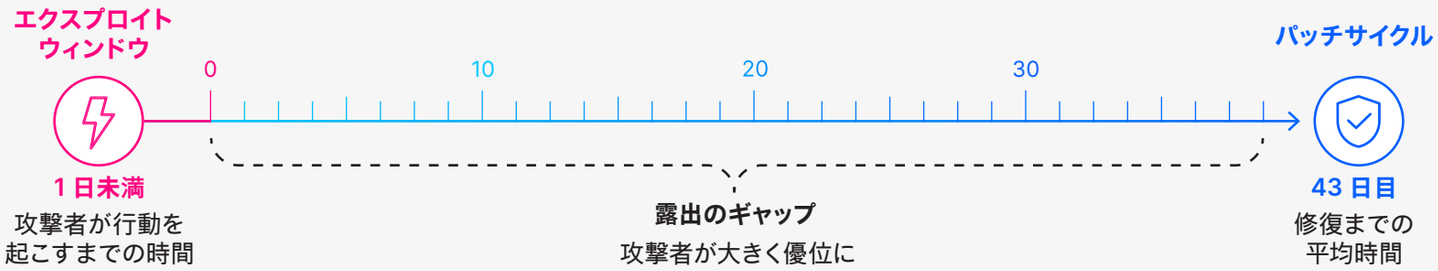
AI を活用すれば、スキルの低い攻撃者でも、国家規模のリソースが必要であった高度な手法を実行できるようになります。

これらの力の相乗効果：エクスプロイトが加速すると攻撃者が到達できる脆弱性の集合が拡大し、参入障壁が低くなると、その脆弱性を突くことができる攻撃者の集合が拡大します。機会の数、攻撃者の数、スピードが増加しています。

組織がこの新たな現実の防御に苦慮する2つの理由：パッチの適用やアップグレードによって保護することが不可能な老朽化したインフラストラクチャを抱えているうえに、インフラストラクチャのセキュリティを定期的な手動のイベントとして扱う旧態依然としたプロセスが残っています。

残存している従来のモデルは、強化、検証、メンテナンスから構成されていて、攻撃者がメンテナンス予定表の制約内で活動することが前提となっています。そのようなことはあり得ません。

データが浮き彫りにするこのアプローチのリスク：2025 年を見ると、高頻度で標的とされた脆弱性の 40% が、サポートが終了したシステムに関係するものでした。重大な脆弱性にパッチを適用するのに要した時間の中央値は、依然として 43 日でした。エクスプロイトのウィンドウ（情報が公開されてから攻撃手段として使用されるまでの時間）は、今や数時間です。その現実を見れば、43 日は遅れなどではなく、すべてを決定する要因です。



40%

標的とされた脆弱性はサポートが終了したシステムに関係

パッチを適用することはできない。露出した状態が続く。

このギャップが非常に危険な理由：

出典：Talos 一年の総括および 2026 年 Verizon Data Breach Investigations Report

新しい運用リズム

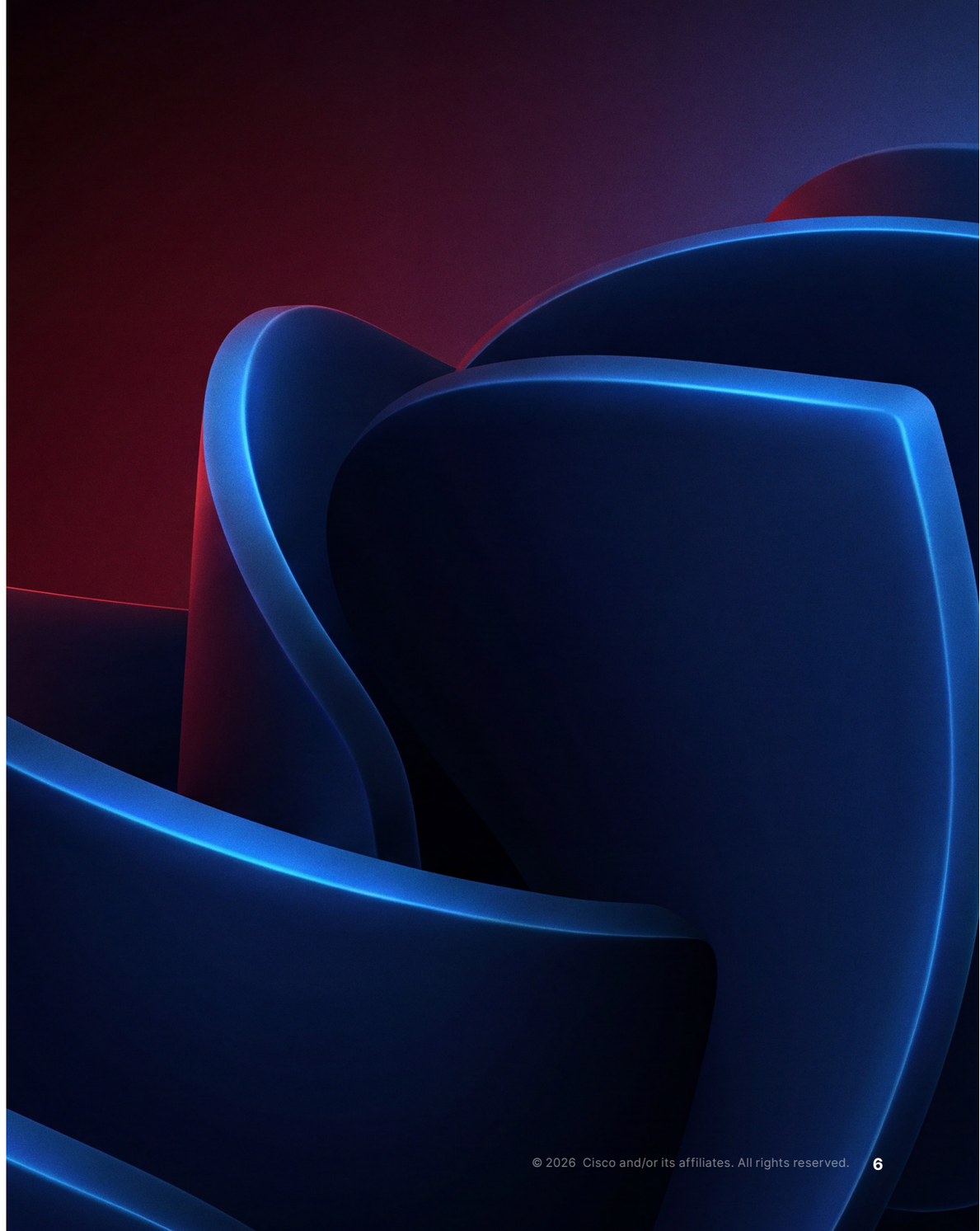
従来のプロセスやテクノロジーでは、AI 時代の脅威に先んじることはできません。今必要なのは継続的な運用のリズムです。パッチとアップグレードの頻繁かつ予測可能な周期での適用、保護できない資産の廃棄、年間を通じた露出の積極的な軽減が求められています。

このエグゼクティブ向け概要では、AI 時代に組織を保護するための実践的なステップとして、運用モデルの進化、インフラストラクチャのモダナイゼーション、セキュリティ態勢の強化を取り上げます。セキュリティ分野やネットワーク分野のリーダーと一緒に、これらの手順を確認してください。単一分野のみでのアプローチでは、不必要なリスクにさらされることになります。

行動に向けた準備ができたら、シスコのアカウントチームが詳細なハンドブックを提供します。このハンドブックの目的は、この概要に記載されている情報に関する詳細な実務者レベルのガイダンスをネットワークチームとセキュリティチームに提供することです。

理論から実践へ：マシンスケールでの防御

フロンティア AI によって攻撃と防御が変化しつつありますが、変化は同等ではありません。Cloud Security Alliance 社のチーフアナリストである Rich Mogull 氏が最近のレポートで説明しているように、攻撃者には数字上の優位性があります。攻撃者はエクスプロイトする脆弱性を 1 つ見つけるだけで十分です。防御システムは、常にあらゆる攻撃者からすべてのリソースを保護する必要があります。従来のプロセスでは、この数字上の優位性を逆転することはできません。優位性を取り戻すには、コードの強化、パッチ適用の迅速化、大規模な環境での継続的な防御を可能にする運用モデルが必要です。



このモデルのシスコによる実用化

「

わずか 8 週間の間に、シスコのポートフォリオ全体にまたがる 18 億行のコードをスキャンしました。当社のセキュリティ研究チームが実施したとしたら、8 年を要していたはずです。私たちの取り組みはまだ始まったばかりです」

Anthony Grieco
シスコ、シニアバイスプレジデント兼
最高セキュリティおよびトラスト責任者

防御システムに必要なのは、強力な AI モデルへのアクセスだけではありません。AI のスピードと規模を再現可能なセキュリティ成果に結びつける専門知識と運用モデルが必要です、このアプローチは、シスコのセキュリティおよびトラストの組織によって、最初に自社環境で実証されました。フロンティア AI にセキュリティの専門知識と専任のリソースを組み合わせることで、脆弱性の検出と修正の迅速化、評価の再現性の向上、上流での防御が可能になりました。

- **検出と修正の迅速化：**シスコは Anthropic の Project Glasswing と OpenAI の Trusted Access for Cyber (TAC) に早期に参加することで、自社のポートフォリオ全体にフロンティア AI モデルを適用し、25 言語以上からなる 18 億行のコードを 8 週間で分析しました。この取り組みの結果、AI のスピードと規模を利用して実際の企業コードにおける脆弱性の検出と修復を迅速化する方法が明らかになりました。
- **評価の再現性の向上：**シスコは自社におけるこのセキュリティ エンジニアリングの取り組みを基に、Foundry Security Spec をオープンソース化しました。これは、エージェント型セキュリティ評価システムを構築するための実戦でテストされたブループリントです。防御システムにこのブループリントを適用すると、モデルやスタックに関係なく、ノイズの多いアラートから境界と優先順位がはっきりした検証可能な調査結果に移行することができます。
- **上流での防御：**シスコは、デフォルトでセキュリティを確保するルールを AI コーディングワークフローに組み込む Project CodeGuard を構築しオープンソース化しました。Foundry Security Spec と組み合わせることで、確認されたギャップを再利用可能なルールに転換でき、既知のバグクラスを実稼働環境に到達する前に排除できます。

重要なインフラストラクチャの新たな運用モデルの定義

組織が継続的な防御に移行する際に対象とすべき 3 つの側面 : 周期、モダナイゼーション、態勢を対象とする必要があります。

この継続的なモデルによる運用方法の変革 : パッチの適用が避難訓練ではなく継続的なリズムとなり、モダナイゼーションが単なるハードウェアの更新ではなくリスクの解消となり、動的なセキュリティ態勢によって侵害の影響範囲が縮小されます。

	古いアプローチ セキュリティを強化し、安全性を確認したら、そのまま運用し続ける	**Mythos 後のアプローチ** マシンスピードでセキュリティを強化し、安全性を確認したうえで、継続的に防御する
周期	12 ~ 24 か月ごとのメジャーアップグレード	継続的な CI/CD スタイルのリリース体制
モダナイゼーション	老朽化した機器、プロトコル、スクリプトを維持	安全性が確保できないものを継続的に排除
セキュリティ態勢	文書化されたリスク例外	露出の継続的な軽減と封じ込め

出発点：3 つの優先事項

変革は 3 つの優先事項から開始：ビジネスを支える復元力のあるインフラストラクチャの運用、老朽化したインフラストラクチャへの対処、全体的なセキュリティ態勢の強化から始めます。これらの優先領域の概要と、開始する際にチームに行う質問について説明します。

1. 運用モデルの進化による復元力の高いインフラストラクチャの実現

パッチ適用はもはや定期的なプロジェクトではなく、継続的な取り組みです。数字を見るとこのシフトの必然性がわかります。修正量が増加している一方でメンテナンスウィンドウは減少していて、デバイスごとの手動のプロセスではそのギャップを埋めることができません。その遅れを攻撃者がエクスプロイトするのです。これに対する解決策は予測可能な自動化された周期です。自動化によって量をこなすことができるため、エンジニアはデバイスごとの実行ではなく、判断に時間を使うようになります。次に、この周期を強制できるようにします。つまり、インターネットに向けた露出を数日以内にクローズし、次のウィンドウで次の階層をクローズするように、露出の階層ごとに修復 SLA を設定します。

チームに対する質問：

- 露出の階層ごとに見た場合、アドバイザリから検証済みのクローズまでに要する時間の中央値は現在どのくらいですか。
- 手動のまま残っている手順はどれですか。

2. インフラストラクチャのモダナイゼーション

サポート対象外の資産には、どの対策でも相殺できないリスクが伴っています。新たな脆弱性が発生してもパッチは提供されません。ベンダーが保守しなくなったものを修復することはできず、封じ込めるか廃止することしかできません。モダナイゼーションの目的が更新ではなくリスクに基づく廃止であり、ビジネスケースのベースが機器の経過年数ではなく露出とライフサイクルデータであるのはこれが理由です。パッチ適用、確認、セグメントへの分割、検証が可能な 単一のアーキテクチャを標準とします。次に、セキュリティ要件として資金を提供し、露出度の高い資産から順次対処します。

チームに対する質問：

- サポート終了日を過ぎている資産や終了日が迫っている資産はいくつありますか。
- それらの資産は何に接続されていますか。もう 1 年間維持するためのコストはどのくらいですか。

3. セキュリティ態勢の強化

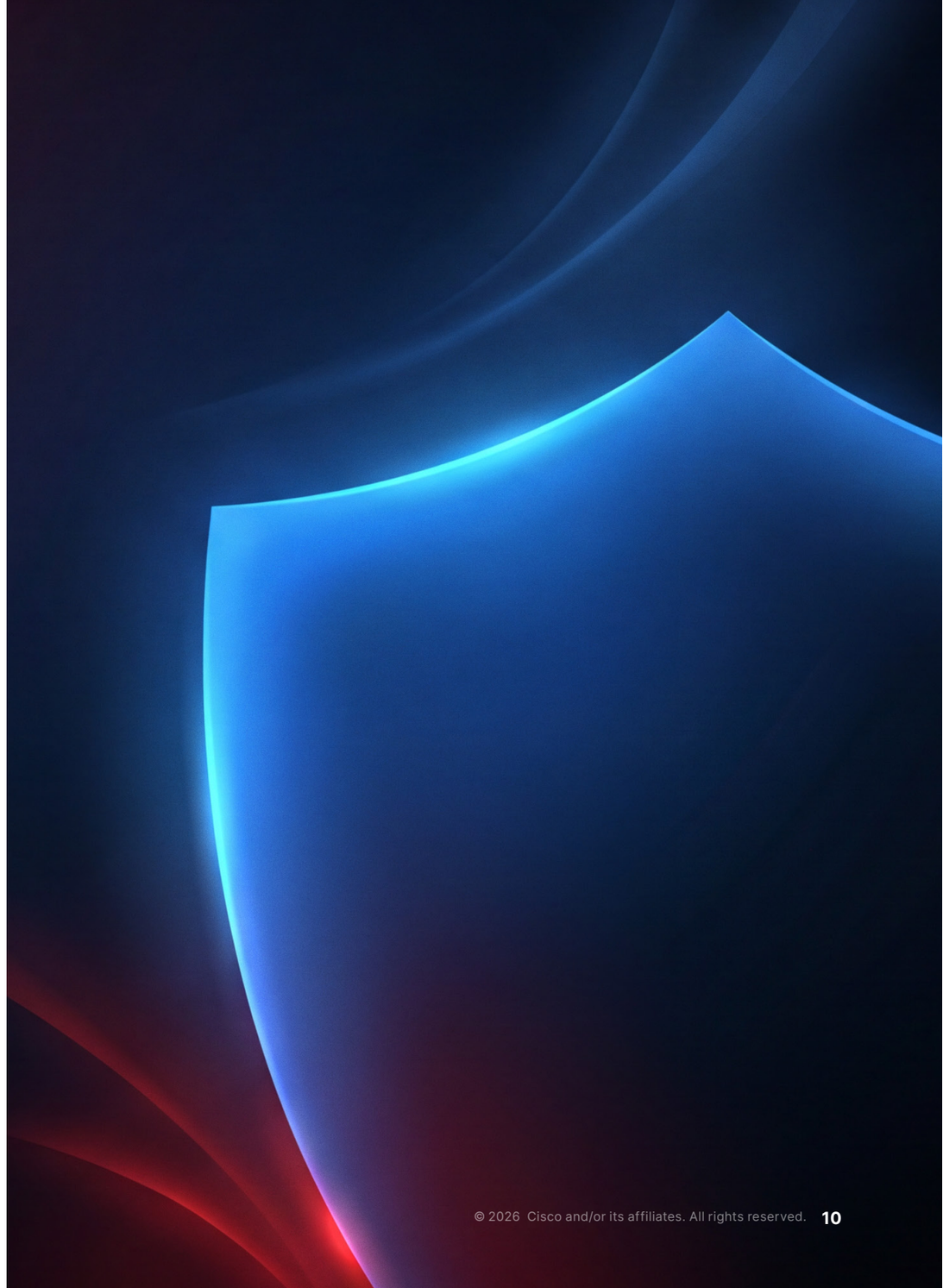
攻撃者は、AI を活用することで、マシンスピードで脆弱性を連鎖させ、インフラストラクチャをリスクにさらすことができるようになりました。露出した資産を保護することで、攻撃対象領域を縮小します。環境をセグメントに分割して侵害を封じ込め、その影響範囲を限定します。アイデンティティの隠れたギャップを解消し、エスカレーションを防ぎます。攻撃のスピードが人間のチームを上回っているため、SOC にはそのスピードに追従できる可視性、自動化、エージェント型 AI ワークフローが必要です。

これらの対策はこれまでになかったものではありませんが、その緊急性はこれまでになかったものです。これらの対策を今導入することが、現在の限られた高度な攻撃者だけでなく、近い将来に出現する攻撃者に対しても先手を打つための鍵となります。

チームに対する質問：

- 今攻撃者が足がかりを確保したとしたら、封じ込めを行う前に攻撃経路をどこまで移動できますか。
- それはどのようにして知ることができますか。
- どのくらいの速さで対応できますか。

これら 3 つの優先項目を設定すると、技術的な戦略から、ビジネスの実行と成功の測定に焦点が移ります。



成功の測定と予算の確保

重要な項目を測定してビジネスリスクを中心に投資を構成することで予算を確保します。

成功の測定

- アドバイザリからクローズまでの時間を追跡。 露出の階層ごとに測定します。
- 資産の最新化状況を測定。最新のリリースを実行している環境の割合を追跡します。
- 修復のサービスレベル契約（SLA）を適用。脆弱性そのものの数ではなく、階層ベースのサービスレベル契約に焦点を当てます。
- 取締役会に提出できる証拠を保管。 コンプライアンス記録、修復タイムライン、資産のステータスを監査人やサイバー保険会社がいつでも把握できるようにします。
- エージェントによる作業について説明責任を明確化。 結果として生じたすべてのアクションについて、監査と復旧を可能にし、人間のオーナーを指名します。

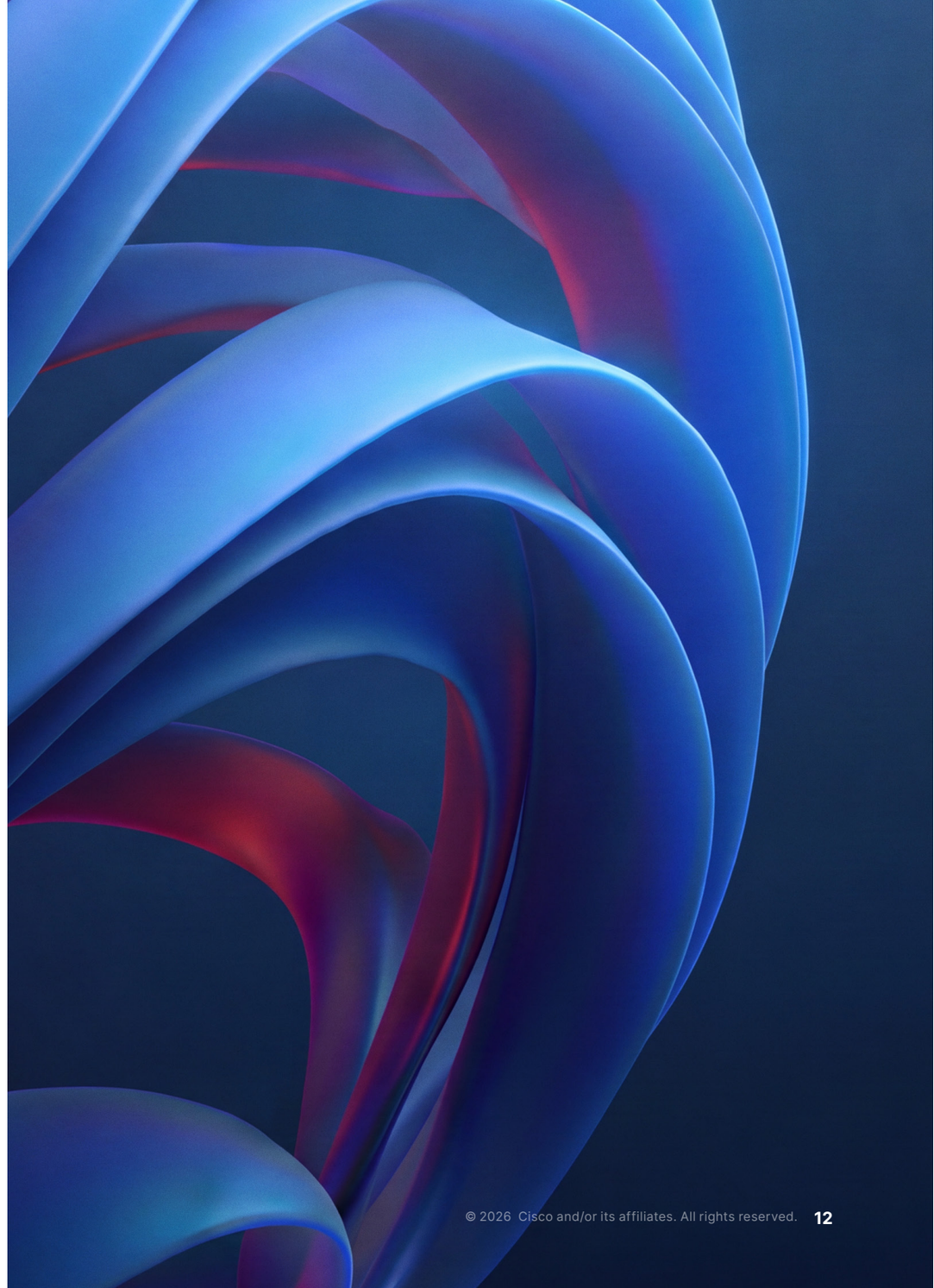
新しいモデルへの資金の提供

- 支出に順序を設定。モダナイゼーションの各段階を予算サイクルに関連付け、露出の多い資産から順に対処します。
- 適時に支出。ファイナンスを活用すると計画外の資金を予測可能な支払いに変換できます。
- セキュリティ要件として構成。 脅威に応じて期限が決まります。これはビジネス上の必須項目であり、やったほうがよいという項目ではありません。
- 運用能力の確保に資金を提供。サービスとパートナーのために予算を確保することで、要員を増やすことなくチームの取り組みを拡大します。

最初の 90 日間

今すぐ承認できるアクション項目を 5 つ紹介します。最初に完全なプログラムを設計する必要はありません。それぞれのアクション項目には次のアクション項目を簡単にする効果があります。

1. **露出のアセスメントを開始。**所有しているもの、脆弱性のあるもの、サポート対象外のもの、リスクにさらされているものを示す最新の優先順位付けされた一覧を用意します。これは、信頼できる共有情報源として利用できます。
2. **露出の階層ごとに修復の SLA を設定。**インターネットに向けた露出や重大度の高い露出を数日以内にクローズし、次のウィンドウで次の階層をクローズすることをコミットし、その結果をレポートします。このポリシーを決定することで、継続的な防御が実現します。
3. **周期を確立。**変更ウィンドウと事前承認用のテンプレートを標準化することで、パッチ適用が例外ではなく日常的な保守となるようにします。
4. **モダナイゼーションの第 1 段階となるターゲットを特定。**露出が最も多いサポート対象外の資産を特定し、交換に必要な資金を最優先で提供します。露出、ライフサイクルデータ、将来のビジネスニーズをビジネスケースのベースとします。モダナイゼーションは、将来にわたって使用できるよりセキュアなインフラストラクチャを導入する機会です。
5. **AI 時代の対応についての机上訓練を実施。**エッジの脆弱性をエクスプロイトしてマシンスピードで水平方向に移動する攻撃者をシミュレーションすることで、対応における各チームの連携を図ります。



シスコのサポート

シスコとその信頼できるパートナーが、この新たな現実に対処できるようお客様を支援します。シスコはパートナーとともに、これらすべての領域にわたって、お客様の組織を支援するプロフェッショナルサービスを提供します。その 1 つが、インフラストラクチャの強化に向けた 3 段階の構造化アプローチを提供するシスコの Resilient Infrastructure サービスです。

運用モデルの進化による復元力の高いインフラストラクチャの実現

2026 年 7 月以降、シスコは事前に通知した固定スケジュールでリリースを実施します。チームが重要なウィンドウ 2 つに同時に対処しなくて済むよう、ずらしたスケジュールとします。各アドバイザリをお客様の資産にマッピングし、重大度スコアだけではなく露出も考慮してランク付けを行い、修正が適用されたことを確認します。パッチやアップグレードをまだ展開できない場合は、ランタイムシールドを使用することでダウンタイムなしで資産を保護できます。

インフラストラクチャのモダナイゼーション

シスコは、露出したサポート対象外のシスコ資産を把握するためのいくつかの方法に加え、インフラストラクチャを強化し、さらなるセキュリティ保護を可能にするための推奨事項を提示します。最新のインフラストラクチャによる更新を検討する場合、シスコは、ネットワーク自体にセキュリティを融合したセキュアなネットワークアーキテクチャを推奨します。これにより、アイデンティティファーストのセグメンテーション、共通のポリシー、分散型の適用が可能になります。その過程を後押しするために、計画外の支出に対処するファイナンスオプションが Cisco Capital によって提供されます。

セキュリティ態勢の強化

シスコは攻撃経路全体を保護します。まず、人間、マシン、AI エージェントの各エンティティにわたってアイデンティティが管理されます。これはエージェントが増加するにつれてますます重要になる相違点です。次に、セグメンテーションが適用され、侵害が発生した際に水平方向の移動が封じ込められます。さらに、AI が量をこなしアナリストが的確に判断できるようにすることで、検出と対応がマシンスピードに加速されます。

次のステップ

行動に向けた準備ができたら、シスコのアカウントチームに問い合わせ、この概要を実行に移すための支援を依頼してください。お客様の組織とその課題に特化した詳細な計画とアセスメントを提示することで、お客様のプロセスを支援します。

シスコパートナーも素晴らしいリソースです。パートナーの能力はさまざまであるため、強みがお客様の環境に適合したパートナーを選択してください。シスコパートナーハブにアクセスして、最適なパートナーを見つけてください。