CISCO
SECURE

XDR バイヤーズガイド

Extended Detection and Response 市場の製品のスムーズな選定に役立つガイド

cisco The bridge to possible

Extended Detection and Response (XDR) について

世界中で、さらに強固な セキュリティ対策が求められているのはなぜでしょうか。

今日のハイブリッド、マルチベンダー、マルチベクトル環境では、複雑さが最大の課題です。セキュリティチームは、統合に一貫性がない多数のツールで運用を実行し、拡大し続けるエコシステムを保護する必要があります。IoT とハイブリッドワークにより、攻撃対象領域が拡大しています。フィッシング、マルウェア、ランサムウェアは、毎年 2 倍、場合によっては 3 倍に増加しています。同時に、企業はかつてないほどのハイパーコネクティビティを体験しています。1 つの企業に対するセキュリティ侵害が、企業のサプライヤー、パートナー、顧客、さらにはあらゆる経済セクターに影響を与える可能性があります。

こうした新しい日常に、セキュリティレジリエンスが求められています。セキュリティレジリエンスとは、ビジネスが先例のない脅威や変化に耐え、かつ一層の強靭性をもって回復できるよう、あらゆる側面でビジネスの完全性を守ることです。今、セキュリティレジリエンスには、これまで以上の対策が求められています。

XDR の利点：

- マルチベンダー検出
- アラート疲れの軽減
- 生産性の向上
- セキュリティレジリエンス

ソリューション

脅威がますます高度化している今、自己完結型のポイント セキュリティ ソリューションを寄せ集めて構築した古い検出・対応モデルでは不十分です。ここで登場するのが XDR です。Extended Detection and Response（XDR）は、統合型のセキュリティインシデント検出および対応ツールです。XDR ソリューションはテレメトリを複数のセキュリティツールから自動的に収集して関連付け、分析を適用して悪意のあるアクティビティを検出し、脅威に対応して修復します。効果的な XDR ソリューションは包括的です。電子メール、エンドポイント、サーバー、クラウドワークロード、ネットワークなどのあらゆるベクトルにわたってデータを関連付け、最も高度な脅威に対してさえ、環境全体を可視化してコンテキストを提供します。

XDR を選ぶ理由

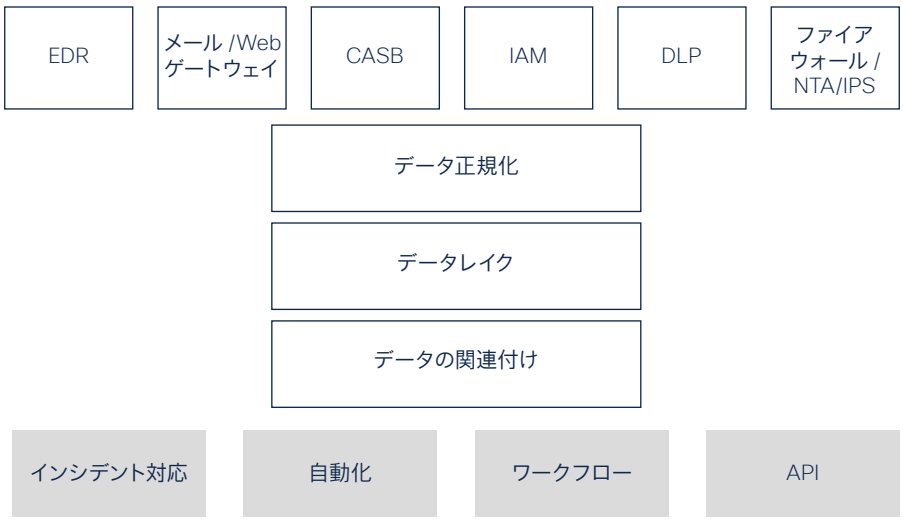
第一に、チームはイベントの関連付けとマルチベンダー検出により、ネットワーク、クラウド、エンドポイント、電子メールなどにかけて最も高度な脅威を検出できます。

第二に、チームが影響に基づいて脅威に優先順位を付けられるため、アラート疲れを軽減できます。

第三に、タスクの自動化によって生産性が向上するため、チームは SOC リソースをより効率的に使用できます。

第四に、組織はセキュリティギャップを埋め、実用的なインテリジェンスを通じて次に何が起こるかを予測することで、セキュリティレジリエンスを構築できます。

XDR 概念アーキテクチャ



適切な XDR に必要な 5 つの要素

1 優先順位が付けられた実用的なテレメトリを、必要なあらゆる分野で提供できる

大量のアラートを効率的にふるいにかけ、トリアージすることができますか?

可視性の広さとインサイトの深さは、XDR の基本的な特徴です。高度な脅威の多くは、エンドポイントまたはネットワークを単体で攻撃するのではなく、電子メール、エンドポイント、ネットワーク、ID 管理、サンドボックス、ファイアウォールなど、さまざまなベクトルにわたり攻撃します。そのため、XDR の結果を通知し、環境全体で起こっている事態の包括的かつ完全な情報を提供できる、幅広いテレメトリと高いデータ品質を備えた XDR ソリューションが必要です。しかし、インサイトを収集するだけではなく、インシデントを管理することも同様に重要です。XDR が期待どおりの効果を実現するには、これらのインサイトに優先順位を付ける必要があります。リスクベースの優先順位付けを提供する XDR ソリューション（リスクが最大のインシデントを優先）を使用することで、本当に重要なインシデントに迅速に対応できます。また、XDR は次のステップの推奨事項も提示する必要があります。そうすることで、最善の行動方針について十分な情報に基づいた決断を下すことができます。

主な特徴と機能	関連する製品分野
・高い有効性と精度により誤検出によるノイズを最小化 ・環境全体のアラートを集約および関連付け	エンドポイントにおける検出と対応（EDR）
・継続的なリアルタイムのネットワーク監視	ネットワークにおける検出と対応（NDR）
・未知のマルウェアやその他の高度なネットワーク攻撃が検出された際に、コンテキストに合わせて優先順位付けされたアラートを生成する高度な分析	Extended Detection & Response（XDR）
・継続的なリアルタイムの 電子メール脅威モニタリングと、自動の修復優先順位付け	電子メールセキュリティ

ベンダーへの質問

- ご提案のソリューションは、すべての環境（エンドポイント、デバイス、ネットワーク）に対する可視性をどのように実現しますか?
- ご提案のソリューションは、インサイトをどのように提供しますか?ご提案のソリューションは、優先順位付けされたテレメトリを提供していますか?
- ご提案のソリューションは、ビジネスへの影響とリスクに基づいてどのように脅威の優先順位付けを行いますか?
- 検出にはどのタイプの脅威インテリジェンスが活用されていますか?そのインテリジェンスはどこで取得されますか?
- ご提案のソリューションで使用するデータソースをどのように検証していますか?
- この製品は、Wannacry、NotPetya、Turla などの高度な脅威にどのように対応しますか?

2 ベンダーや攻撃ベクトルを問わず、脅威の検出能力を集約

お使いの XDR ソリューションでは、 セキュリティへの投資を 1 つの連携したユニットとして動作させることができますか？

脅威がより高度になり、攻撃ベクトルの種類が増すにつれて、環境全体で一貫した検出を実現することがこれまでになく重要になっています。今日のセキュリティ チームは、セキュリティ環境と、グローバルサプライチェーン、攻撃者、防御システムから成るエコシステムの両方で、並外れたレベルの複雑さに対処しています。XDR ソリューションは、重大度と影響に基づいて検出内容を集約、相関付け、優先順位付けすることにより、チームの対応をサポートします。ただし、これを可能にするには、セキュリティスタックが連携して動作する必要があります。オープンかつ拡張可能でクラウドファーストの XDR ソリューションを選択することで、複雑なレイヤーを追加するのではなく、環境全体で統合された検出とイベント相関によるメリットを得ることができます。セキュリティスタックの各コンポーネントには、ネットワーク、電子メール、ファイアウォールなど、それぞれに固有の検出要素があります。それらを統合することで、さらに高度な検出が実現します。XDR は、潜在的な脅威の包括的なビューを提供するために、エンドポイント、ネットワーク、ファイアウォール、電子メール、ID、DNS の 6 つのテレメトリソースすべてを網羅する必要があることを考慮することが重要です。XDR ソリューションは、ネイティブのバックエンドからフロントエンドへの統合によって、セキュリティスタック全体と簡単に統合できる必要があります。これにより、ベンダーがポートフォリオを変更した場合や、ベンダーを切り替えた場合でもカバレッジの一貫性を保つことができます。最後に、セキュリティスタックの脅威検出機能を最適化するには、価値の高いローカルコンテキストを提供し、信頼できる正確な脅威インテリジェンスの判断を提示できる XDR ソリューションを検討する必要があります。

主な特徴と機能	関連する製品分野
・エクスプロイトベースのメモリインジェクション攻撃など、エンドポイント実行プログラムの異常な動作を検出してブロック ・MITRE ATT&CK マッピングで侵害の指標（IoC）を判断 ・ファイルレピュテーションをモニタリングして、脅威をエントリポイントで検出および隔離 ・環境内の OS 脆弱性を特定し、管理者がリスクに基づいて修復に優先順位を付けられるようにし、攻撃対象領域を削減	エンドポイントにおける検出と対応（EDR）、脆弱性管理
・高度な分析により、未知のマルウェア、データ漏えいやポリシー違反などの内部脅威、その他の高度な攻撃を迅速に検出 ・信頼度の高いアラートでネットワーク攻撃をリアルタイムで検出	Extended Detection & Response（XDR）、ネットワークにおける検出と対応（NDR）
・レピュテーション フィルタリングによる迷惑メールの検出とブロック ・ソーシャルエンジニアリング、なりすましなどの詐欺型の電子メール攻撃を特定して保護	電子メールセキュリティ

ベンダーへの質問

- ご提案の XDR プラットフォームでは、弊社の既存の投資をいくつ活用できますか？
- ご提案の XDR プラットフォームは、ベンダーに関係なく弊社のソリューションと互換性がありますか？
- ご提案のソリューションは、すぐに互いに統合できますか？
- ご提案の検出テクノロジーは、市場の他のテクノロジーと比べてどのように優れていますか？
- ご提案のソリューションは、どのような種類の脅威の検出に役立ちますか？アラートは MITRE ATT&CK フレームワークにマッピングされますか？

3 脅威対応の的確さとスピードの向上に貢献

脅威を特定したら、 どれくらいの速さで自信を持って対応できますか？

ネットワーク、エンドポイント、メール（およびその他の多くの要素）から得られたインサイトが統合されると、発生している事象、その進行状況、脅威の修復に必要な手順について、より正確に理解できます。脅威の影響と範囲を 1 ヵ所から確認し、1 ～ 2 回のクリックでアクションを実行できることが理想です。効果的な XDR は、ホストの隔離や、すべての受信トレイからの悪意のある電子メールの削除など、ネイティブな対応および修復機能を備えています。時間の経過とともにチームがセキュリティを進化させることができるように、XDR にはカスタム対応措置を容易に作成し、自動化できる機能も必要です。

主な特徴と機能	関連する製品分野
・侵害されたエンドポイントの脅威に迅速に対応	エンドポイントにおける検出と対応（EDR）
・ネットワークの問題やインシデントの根本原因を数秒で特定して切り分け	Extended Detection & Response（XDR）、ネットワークにおける検出と対応（NDR）
・リアルタイムのクリックタイム分析により、悪意のある Web サイトをすばやくブロック	電子メールセキュリティ

ベンダーへの質問

- 製品はどのような対応措置を備えていますか？
- 1 つの場所で XDR ソリューションを使用してエンドポイントで修復を実行し、他の場所に拡張することはできますか？
- 製品は、対応を可能にする既存のセキュリティツールとどのように統合できますか？
- ご提案のソリューションは、どのように修復を加速しますか？
- 脅威のアラートから修復までの対応時間はどのくらいですか（例：フィッシング攻撃の場合）？

4 脅威調査の結果を集約し、ユーザー体験を合理化できる

脅威の検出、対応、修復は、単一のインターフェイスから管理できますか？

XDR ソリューションを評価する際は、セキュリティアナリストのエクスペリエンスを考慮することが重要です。セキュリティチームはすでに多くの管理を担当しています。数十のツールと大量のコンソールによって、チームに負担をかける必要はありません。そのため、複数のセキュリティツールとデータソースにわたるセキュリティデータの統一されたビューを提供することで、アナリストが脅威をより迅速かつ効果的に検出して対応できるように設計された XDR ソリューションをお勧めします。これにより、ワークフローが合理化され、セキュリティインシデントの調査と修復に必要な時間と労力を削減できます。XDR ソリューションは、すべての脅威ベクトルとアクセスポイントをカバーする完全なライフサイクルダッシュボードを提供する必要があります。また、MITRE ATT&CK などの仕組みを用いて脅威ハンティングを促進し、経験の浅いメンバーでも仮説主導型の脅威ハンティングが実行でき、次に何が起こるかを把握し備えられるようにする必要があります。考慮すべきもう 1 つの要素は、設計がアナリストのエクスペリエンスに与える影響です。XDR ソリューションによって生産性を高め、検出、調査、対応の主要機能に関連する意思決定時間を短縮し、初心者から中級者のアナリストがセキュリティ運用における高度なタスクを実行できるようにする必要があります。そのためには段階的な情報開示によってより優れたコンテキストを提供し、潜在的な脅威の範囲と深刻度をすばやく判断できるようにする必要があります。

主な特徴と機能	関連する製品分野
・すべての脅威ベクトルとアクセスポイントをカバーする完全なライフサイクルダッシュボードを提供 ・ITOps、SecOps、NetOps にまたがる統合ツールセットを提供 ・統合された場所からデータ、分析、自動化にアクセスおよび管理	Extended Detection & Response (XDR)

ベンダーへの質問

- ご提案のソリューションは、当社のチームの脅威ハンティングをどのように支援できますか？
- ソリューションは、SOAR や SIEM ソリューションなどの既存のセキュリティテクノロジーとどのように統合できますか？
- ご提案の XDR を使用すると、脅威の影響や侵害の範囲を把握し、単一のインターフェイスから 1 回のクリックで措置を講じられますか？
- ご提案のソリューションは、システム / サブシステムへのアクセスのすべてまたは一部を承認されたグループおよび個々のユーザーに制限することによる、ロールベースのセキュリティがサポートされていますか？
- 弊社で使用する既存のすべてのセキュリティテクノロジーからのテレメトリを一元化して分析できますか？
- ご提案のソリューションでインシデント対応ワークフローを合理化し、全体的な調査時間を短縮できますか？

5 生産性を高め、セキュリティ態勢を強化できる機会を提供する

ご提案の XDR ソリューションで、オーバーヘッドを減らしながら、脅威の検出と対応の効率を向上させることは可能ですか？

企業のセキュリティレジリエンスを構築するための重要な要素は、自動化とオーケストレーションです。セキュリティスタッフには、完了すべき重要なタスクがあります。セキュリティの脅威に直面した場合に、複雑な人力の、反復的なワークフローに時間を費やす必要はありません。重要なワークフロー（アラートの検出、関連付け、優先順位付け、対応措置の迅速な実行など）を自動化することによって生産性を向上させる XDR ソリューションは、ライフサイクル全体でチームを解放します。効果的な XDR ソリューションは、明確な判断とアクションを可能にする調査を実現し、アナリストがポリシーと手順に従って自動化された一貫した方法で対応できるようにすることで、対応にかかる平均時間を短縮します。これは、セキュリティチームがより戦略的でプロアクティブなセキュリティタスクに時間とエネルギーを投資し、企業のセキュリティ体制をさらに強化できることを意味します。

主な特徴と機能	関連する製品分野
・普及率の低い脅威を含む自動エンドポイント脅威ハンティング ・管理者はカスタムの侵害インジケータ（IoC）を作成してスキャン可能	エンドポイントにおける検出と対応（EDR）
・動作分析主導のインサイトによる予測的なネットワーク脅威修復	Extended Detection & Response（XDR）、ネットワークにおける検出と対応（NDR）
・電子メールの脅威修復の自動優先順位付け	電子メールセキュリティ

ベンダーへの質問

- サードパーティとの統合で、ベンダーが API を変更した場合に自動化スクリプトに影響は出ませんか？
- ご提案のソリューションは、クラウドベースのワークロードとの間の監視をどのようにサポートできますか？
- ご提案の XDR ソリューションを使用するために環境を変更したり、新しいテクノロジーを導入したりする必要はありますか？
- ご提案の XDR ソリューションは、サードパーティのセキュリティテクノロジーとの事前構築済みですぐに利用できる統合を提供していますか？
- ご提案の XDR ソリューションで、インシデントの調査と解決に必要なアナリストの時間を短縮できますか？
- ご提案の XDR ソリューションは、レジリエンスを構築するためにポリシー管理に向けた情報を提供しますか？

Cisco XDR

XDR はセキュリティレジリエンスに不可欠な要素

今の時代に確実なのは、「すべてが不確実」ということです。そのため企業は、財務からサプライチェーンまで、ビジネスのあらゆる側面でレジリエンスを高めるべく投資を続けています。しかし、セキュリティレジリエンス、つまり脅威や混乱からビジネスを保護し、変化に自信を持って対応することで企業を強化する能力への投資がなければ不十分です。

XDR は、ビジネスのセキュリティレジリエンスを実現するために不可欠な要素です。XDR を適切に活用することで、セキュリティチームが影響によって脅威に優先順位を付け、脅威をより早く検出し、対応を迅速化できるようになり、セキュリティ体制を強化できます。自動化とオーケストレーション機能によってこのプロセスが促進され、セキュリティチームが最も重要なことに集中できるようになります。

統合型アプローチの価値

50%
データ侵害のリスクと
コストの削減

90%
インシデントごとの
分析作業の削減

90%
セキュリティの
効率性向上

85%
攻撃の滞在時間の
短縮

出典：Cisco SecureX の Total Economic Impact（総合的な経済効果）2021 年 7 月

Cisco XDR で簡素化されたセキュリティ運用

シスコは、市場で最も包括的なセキュリティポートフォリオで XDR ソリューションをリードしています。シスコでは、将来のセキュリティニーズを予測し、市場で最も包括的なセキュリティポートフォリオの作成に積極的に投資してきました。ベンダーとベクトルを問わずコンポーネントを統合することで、効果的なセキュリティを簡素化し、すべてのチームがアクセスできるようにしました。シスコは、XDR アプローチの構築が 1 つのプロセスであると考えています。また、お客様のチームがポイントソリューションで過飽和状態にある業界の、その場しのぎの修復による悪循環から抜け出すことを望んでいます。Cisco XDR によって、検出から対応までの最短経路を最小限の負担で発見することを目指しています。

SOC エキスパートが SOC エキスパートのために設計した Cisco XDR は、セキュリティ オペレーションを簡素化し、セキュリティアナリストが最も高度な脅威に対してプロアクティブに対応し、レジリエンスを維持できるように支援します。シスコのソリューションはオープンで拡張性が高く、クラウドファーストです。そのため既存のセキュリティ投資を活用し、環境全体でセキュリティ検出能力を統合できます。

シスコでは、お客様のアセットを保護することに真剣に取り組んでいます。シスコもお客様の顧客であるためです。シスコは Cisco Security Cloud を通じて、セキュリティレジリエンスを目指す過程でお客様のパートナーになりたいと考えています。Cisco Security Cloud は、次に何が起こるかにかかわらずエコシステム全体を保護するために役立つオープン セキュリティ プラットフォームです。包括的なセキュリティの力をぜひ体験してください。

将来のセキュリティ運用を今すぐ構築する準備はできていますか？

Cisco XDR の詳細

主な XDR 要素と機能

XDR ベンダーとの会話の際のクイック リファレンスとして、この表 (9 ~ 10 ページ) を使用してください。

主な要素	主な機能	対応するシスコ製品
優先順位が付けられた実用的なテレメトリを、必要なあらゆる分野で提供できる	・完全に管理可能な組み込みの Endpoint Detection and Response(EDR)、プロアクティブな脅威ハンティング ・脆弱性の迅速な特定、リスクのスコアリング、優先順位付け、修復を可能にする統合されたリスクベースの脆弱性管理	Cisco Secure Endpoint
	・継続的なクラウドアクティビティ分析 ・動作モデリングと機械学習アルゴリズムを含む高度な分析 ・統合された可視性と集約された実用的なインテリジェンスを実現する、セキュリティ インフラストラクチャ全体の単一ビュー	Cisco XDR
	・リアルタイムのクリックタイム分析による高度なアウトブレイクフィルタ	Secure Email
ベンダーや攻撃ベクトルを問わず、脅威の検出能力を集約	・実行中プログラムの異常な動作の実行時の検出およびブロック ・エンドポイントで高度な OS クエリをリアルタイムで実行する機能 ・MITRE ATT&CK フレームワークにマッピングされる組み込みの脅威ハンティング	Cisco Secure Endpoint
	・コンテキスト (ユーザー、デバイス、場所、タイムスタンプ、アプリケーション) を含む高精度のアラートにより、クラウド全体の攻撃をリアルタイムで検出 ・確認済みの検出結果による脅威の検出と分離 ・NDR で不正なエンティティを検出し、エンドポイントの検疫を自動化 ・外部ホストと通信する内部ホストの検出 ・より効果的なフォレンジック調査に向けてすべてのクラウドトランザクションの完全な監査証跡を提供 ・ポートフォリオ内の他の XDR ソリューションとの組み込みの統合 ・サードパーティのソリューションと組み込み、事前パッケージ、カスタムのいずれかの統合機能によって統合し、結合されたバックエンドアーキテクチャと一貫したエクスペリエンスを実現 ・クラウド、エンドポイント、ネットワーク、アプリケーションにわたる、他のテクノロジーとの組み込みの統合 (他のサードパーティテクノロジーを含む)	Secure Network Analytics および Cisco XDR
	・スパム対策、URL 関連の保護と制御、高性能ウイルススキャン、アウトブレイクフィルタ、ドメイン機能のレピュテーションスキャン ・エグゼクティブに向けられた BEC 攻撃を阻止する偽装電子メール検出 ・自動化されたマルウェア分析およびサンドボックス分析	Secure Email
脅威対応の的確さとスピードの向上に貢献する	・幅広い顧客ベースに向けたグローバル セキュリティ オペレーション センター (SOC) からプールされた脅威インテリジェンスとインサイトを活用して、常時オンの保護にアクセス	すべての Cisco Secure 製品

主な XDR 要素と機能

主な要素	主な機能	対応するシスコ製品
脅威対応の的確さとスピードの向上に貢献(続き)	・幅広い顧客ベースに向けたグローバル セキュリティ オペレーション センター（SOC）からプールされた脅威インテリジェンスとインサイトを活用して、常時オンの保護にアクセス	すべての Cisco Secure 製品
	・すべてのエンドポイント アクティビティを継続的に監視し、実行時の異常な動作を検出およびブロック	Cisco Secure Endpoint
	・プライバシーとデータの整合性を損なうことなく、暗号化されたトラフィックの脅威を特定して隔離 ・1 つの場所から「対応」ワークフローをトリガー ・セキュリティ製品のデータソースからのコンテキスト認識と、API を介した Talos® およびサードパーティソースからのグローバルな脅威インテリジェンスを集約した脅威対応 ・フォレンジックインシデント調査のケースブックの作成	Cisco XDR
	・潜在的に悪意のあるリンクのリアルタイム分析による、URL ベースの脅威に対する永続的な保護 ・リアルタイムの Talos® モニタリング、分析、脅威インテリジェンスの継続的な活用による、未知の脅威や突然の変化の特定	Secure Email
脅威調査の結果を集約し、ユーザー体験を合理化できる	・グローバルインテリジェンスを単一のビューで収集して関連付け、脅威の調査を迅速化 ・カスタムの対応アクションを作成して対応時間を短縮 ・複数のデータソースからの情報補完を自動化し、脅威インテリジェンスを補強	Cisco XDR
生産性を高め、セキュリティ態勢を強化できる機会を提供する	・普及率の低い実行ファイルの自動識別と脅威分析 ・カスタム IoC を作成して、エンドポイントの展開全体で侵害後のインジケータをスキャンする機能	Cisco Secure Endpoint
	・動作モデリング、多層機械学習、グローバル脅威インテリジェンス ・ネットワークに追加された新しいデバイスを自動的に分類 ・XDR ソリューションとの統合により、あらゆる脅威ベクトルとアクセスポイントを自動化	Secure Network Analytics および Cisco XDR
	・動的レピュテーション分析を自動的にトリガーし、電子メール マルウェアの発生場所、影響を受けたシステム、マルウェアの動作を可視化 ・修復インサイトに基づいて受信メールと送信メールの両方に対応	Secure Email
	・一般的なユースケースと連携した事前構築済みのワークフローによるルーティーン作業の自動化 ・セキュリティチーム間でのプレイブックの共有 ・他のセキュリティ ポートフォリオ ソリューションからのアラートの自動トリアージと優先順位付け	Cisco XDR

米国本社
Cisco Systems, Inc.
San Jose, CA

アジア太平洋地域本部
Cisco Systems (USA), Pte. Ltd.
Singapore

ヨーロッパ本社
Cisco Systems International BV アムステルダム、
オランダ