

ブロードバンド サービス プロバイダーへのスパム ゾンビの影響の評価

はじめに

スパムは、以前は単なる迷惑なものと考えられていましたが、現在では、インターネット ユーザとブロードバンド サービス プロバイダーに影響を与える深刻な問題となっています。既知のウイルス、ワーム、およびトロイの木馬はマスコミに大きく取り上げられていますが、スパムはすべてのインターネット ユーザに直接または間接的に影響し、アンチウイルス ソフトウェア プログラムのような包括的なソリューションが存在しないため、より蔓延する悪質な脅威といえます。スパムは、大量の役に立たない不要なメッセージで E メールを受信箱をあふれさせるため、ユーザにとっては悩みの種となります。

迷惑や不都合の域を越えて、スパムはユーザとサービス プロバイダーの両方に実害を与えます。「フィッシング」詐欺により、ユーザが油断していると、クレジットカード番号やパスワードなどの重要な個人情報を盗まれ、金銭的な被害を受けるだけでなく、時間とプライバシーも失います。また、スパムは Distributed Denial-of-Service (DDoS; 分散型サービス拒否) エージェントなど、悪意のあるコード ウイルスを送信する可能性があります。サービス プロバイダーにとっては、スパムは E メール サーバに負担をかけ、正規の E メール メッセージの送信を遅延または阻害する要因となります。これにより、帯域幅が消費され、最終的に、サービス プロバイダーは、スパムによって埋もれてしまう正規のメールをサポートするため、コストを投入して容量を追加せざるを得なくなります。また、ユーザ アクティビティがスプーフィングされ、サービス プロバイダーがスパムの送信元としてブラックリストに載せられた場合、スパムがサービス停止の引き金になる可能性もあります。これは、市場へ深刻な影響を与えます。競争の激しい市場でのブロードバンド加入者獲得競争において、スパムの送信元としての評判は、サービス プロバイダーにとって非常に不利となります。

サービス差別化の機会

大半のユーザは、スパムの送信者をいかがわしい、または悪質と考えていますが、そのクレームはサービス プロバイダーに向けられます。「どこから送られるかが問題ではなく、スパムを止めてほしい」という反応が一般的です。Gartner Group の調査によると、74 パーセントの顧客が、Internet Service Provider (ISP; インターネット サービス プロバイダー) にスパムの問題を修正する責任があると考えています。E メールに対するフィルタリングおよびスパム対策テクノロジーの進歩は成長過程にあるにもかかわらず、一般的なホーム ユーザや中小・中堅企業ユーザは、サービス プロバイダーが E メールからのスパムの除去を保証することを期待しています。このようなユーザは、決して声なき多数派ではありません。PC Magazine によると、AOL だけで毎日 250,000 件のスパム関連の苦情が寄せられています。

スパムは、問題に適切かつ独創的に対処するサービス プロバイダーにとっては、ビジネス チャンスでもあります。スパムを存在させない ISP は、他の ISP 加入者の興味を惹くだけでなく、スパム対応サービスから新たな収益を生み出すこともできます。Gartner Group は、最新の調査報告書で次のように報告しています。

- スパムの受信数を減らすために、36 パーセントのユーザが ISP の切り替えを考えています。
- 24 パーセントものユーザが、スパムをブロックするためにお金を払ってもかまわないと考えています。

アンチスパム テクニカル アライアンスに対する期待

インターネット コミュニティは、サービス プロバイダーがスパムに対応することを期待しています。アンチスパム テクニカル アライアンスは、技術標準を開発し、スパム問題に対処するためにコミュニティ内の協力を促しています。サービス プロバイダーの業務を対象に、初期の推奨事項¹として、次のような提案をしています。

- 障害が発生したコンピュータ(ゾンビ)の検出と検疫
- Eメールの送信トラフィックへのレート リミットの実装
- 苦情報告システムの開発

スパム現象の評価

第一世代のスパム業者は、自分の E メール アカウントから数千～数百万の E メール メッセージを送信するという最も単純なアプローチを使用していました。サービス プロバイダー側も同様に単純な措置として、ユーザのブラックリストを作成し、苦情に対応しました。サービス プロバイダーは、メールの量、件名行とメッセージの分析、およびユーザの苦情に基づいてスパム業者を特定し、簡単に実行できる単純なポリシーを使用して、その業者をネットワークから除外しました。

スパム業者は、ただちにオープン メール プロキシを使用した新しい方法に切り替えました。オープン メール プロキシは、どのようなネットワーク アドレスからの接続も受け入れるサーバであり、他のネットワーク アドレスからは事実上見えない媒介として機能します。受信者(および介在するネットワーク インフラストラクチャ)からは、スパム メッセージは、メール プロキシから発生しているように見えるため、送信者の正体を効果的に隠すことができます。サービス プロバイダーは、スパムを送信している既知のメール サーバについて、2 番目のブラックリストを作成して対応しました。サーバのブラックリストに対して、スパム業者は、スパム ゾンビというより高度な攻撃方法を開発しました。

スパム業者は、保護されていないコンピュータにトロイの木馬プログラムを感染させ、リモート コマンドによって大量のユーザが意図せずにスパム攻撃を開始するようにしました。このような攻撃には、DDoS 攻撃に似た特徴があります。多数のマシンからの攻撃により、攻撃の送信元を特定したり、正規のユーザを混乱させることなく有効な修正措置を実行したりするのが困難または不可能になります。

ゾンビ: 悪用された PC

スパム ゾンビは、これまでに開発されたスパム送信方法のうちで間違いなく最も悪質なものです。現在のブロードバンド ネットワークは、特にゾンビの影響を受けやすくなっています。これは、多くのユーザがネットワークに常時接続し、スパム業者がセキュアではないコンピュータを検出して攻撃する機会を与えているためです。

ゾンビは重大な問題であり、この問題は拡大しつつあります。業界の専門家は、ブロードバンド ネットワークで感染した PC の割合は少なくとも 1 パーセントであり、10 パーセントの可能性もあると推定しています(ゾンビ メカニズムの詳細については、図 1 の「ゾンビによる攻撃方法」を参照)。

¹「Antispam Technical Alliance Technology and Policy Proposal」Version 1.0、2004 年 6 月 22 日

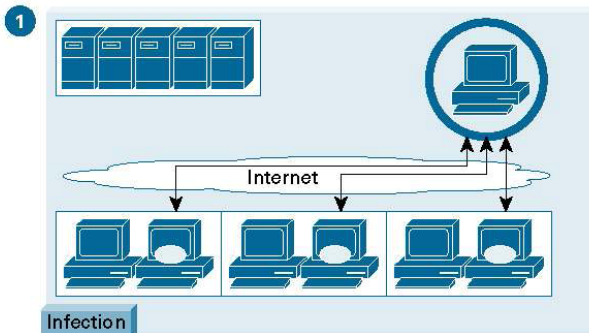
送信元でのスパム ゾンビのブロック

既存のスパム防止メカニズムに負荷をかけて回避する方法として、スパム業者がスパム ゾンビを選択していくにつれて、インターネット コミュニティは、悪影響を軽減するための新たな戦略を開発して対処する必要に迫られています。ブロードバンド サービス プロバイダーは、ブラックリスト、メッセージ テキスト分析、フィルタリングといった既存のスパム防止テクノロジーを使用して、スパムメッセージがメール サーバに届いた時点でフィルタリングし、削除することはできます。しかし、ブロードバンド サービス プロバイダーが必要としているのは、ゾンビにより生成された E メール メッセージがブロードバンド アクセス ネットワークから送信され、指定されたメール サーバに到達するのを防ぐ効果的なソリューションです。このようなソリューションを使用すれば、スパム業者にとって重要なスパム ゾンビの配布を阻止できます。スパム攻撃は、IP アドレスを頻繁に変更する多数の送信元から発生します。

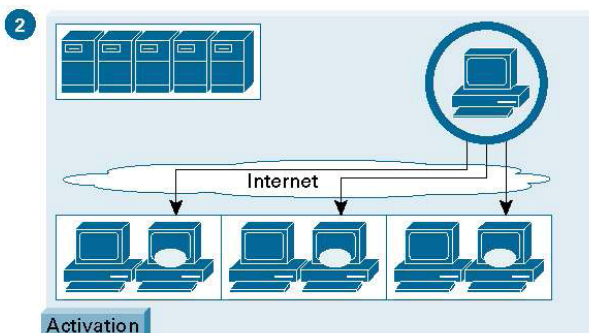
図1 ゾンビによる攻撃方法

How Zombies Attack

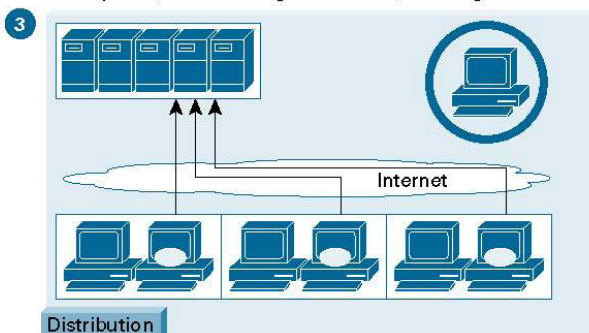
A virus or Trojan horse enters the personal computer in one of numerous ways such as e-mail attachments, improperly secured Internet ports, or operating system flaws. When the zombie infects the target computer, it sends a notification message to the spammer and remains dormant until activated.



When a sufficient number of zombies are in place, the spam controller initiates a spam campaign by first activating the zombies with a wake-up command. The command includes the content of the spam e-mail and a separate list of target addresses for each zombie.



Each zombie then initiates the bulk e-mail transfer to its addresses by acting as a simple mail transfer protocol (SMTP) relay. A large number of spam zombies are used to stage a coordinated campaign of spam distribution. In most cases, individual users are unaware of the presence of the zombie during all phases of the operation. After the distribution phase, the zombie goes inactive, awaiting a new command.



スパム ゾンビは、1つの「スパム活動」を送信元とするメッセージを、膨大な数のゾンビソースから送信する方法を導入しているため、メールサーバでの特定が困難です。ブラックリストや統計に基づく阻止などの従来の方法は効果がありません。テキストパターン検出方法により、このような攻撃を最終的には検出できますが、コンピュータリソースでこのような詳細なメッセージ分析を行うと、作成された攻撃のサイズに直接比例して、メールサーバの処理速度も低下します。

ゾンビ動作の送信元となるブロードバンド ネットワークでの攻撃の識別が可能になれば、防御の拡張も効果的に行えます。また、ネットワーク内のすべてのトラフィックをトランスパアレントにモニタし、ブロードバンド リソースのパフォーマンスやアベイラビリティに影響を与えることなく、スパム ゾンビを効率的に識別および阻止できるソリューションを使用すれば、インターネット コミュニティで、悪質なゾンビの配布を遮断する新たな方法となります。

Cisco Service Control を使用したスパム ゾンビへの対処: 科学捜査的アプローチ

ゾンビによるスパムに対抗する最も効果的なアプローチは、原因となる当事者、つまりスパムを送信している PC を特定することです。感染したマシンが特定されると、サービス プロバイダーはそのマシンを検疫(ネットワーク アクセスを拒否)して、ネットワークを保護し、ネットワーク ユーザに感染を通知することで修正措置を実行できます。

スパムの送信元は、どのようにして特定されるのでしょうか。ゾンビは送信元の正体を隠すことができますが、ネットワーク使用パターンに特徴的な「フィンガープリント」を残します。高度な Cisco® Service Control ソリューションのネットワークに対する洗練された科学捜査的アプローチを使用すれば、これを読み取ることができます。スパム ゾンビの弱点は、スパム活動の一部として生成される SMTP セッションの数です。シスコシステムズがサービス プロバイダーのお客様に対して行ったさまざまなテストでは、ゾンビ攻撃をリアルタイムで特定するネットワーク ルールの開発は、技術的には実現可能であり、高度な信頼性も備えられることが証明されています。

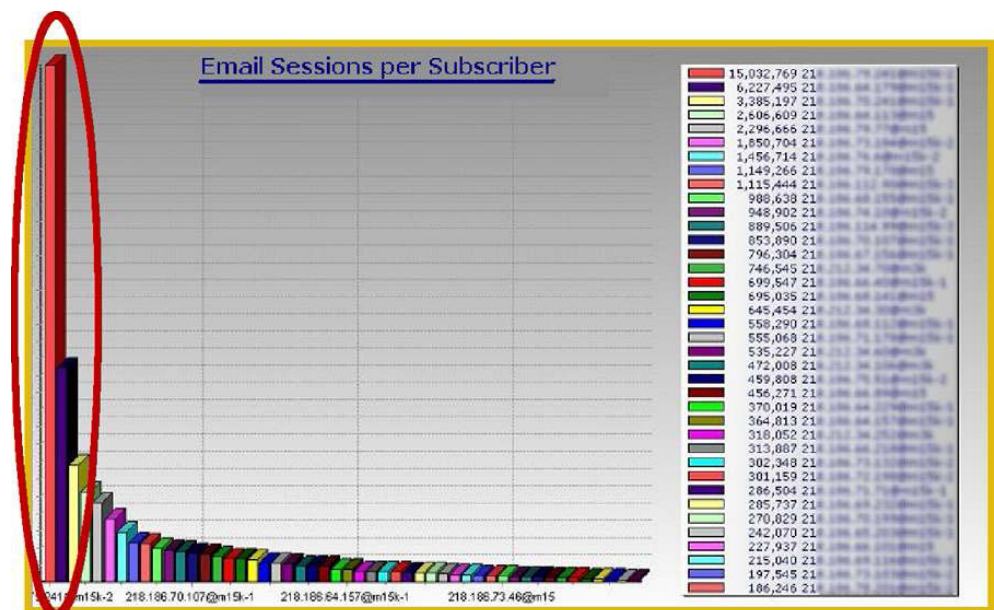
ゾンビ スパムの送信元を特定するには、ネットワークトラフィック モニタリングおよび次の主要な機能を備えたネットワーク エレメントが必要です。

- **詳細なパケット インスペクション:** パケットに対する詳細な検査を実行して、SMTP メール プロトコル フローへのネットワーク パケットの分類を行います。これにより、加入者が生成した SMTP トラフィックの種類を正確に把握して、ゾンビ メール トラフィックに存在する疑わしいパターンを特定できます。
- **フローおよび加入者ステータスの維持:** 特定のパケット フローが SMTP プロトコルに基づくとは判断された場合、特定の加入者によって生成されたこのようなフローの合計数を追跡します。これにより、ゾンビ パターンを示す、つまり多数の受信者にメールを配信しようとする不適切な数のセッションを生成する加入者を特定できます。
- **E メール トラフィックの宛先ベースによる分類:** ゾンビ メール トラフィックと正規の E メールを区別するために、個々の加入者が一定の期間に使用する宛先メール サーバの数を追跡します。これにより、正規のアクティビティ (ISP 独自のメール サーバまたは少数のオフネット サーバの使用) と、ゾンビ アクティビティ (多数のオフネット サーバの使用) を区別できます。
- **E メールおよび HTTP アプリケーションのトラフィック制御:** レート リミットまたはブロッキング、および加入者に障害が発生したことをプロアクティブに通知する HTTP リダイレクト機能を使用することで、緩和プロセスを自動化するソリューションを作成し、ゾンビ トラフィックを制御します。
- **パフォーマンスを考慮した設計:** アプリケーション トラフィックの視覚化と制御を維持し、負荷がかかっているトラフィック ストリームの管理を専門に行うことで、疑わしい E メール スパムにただちに対応します。このネットワーク エレメントがないと、大量のトラフィックがネットワークに送信された場合、E メール スパムを管理するソリューションの機能に障害が発生します。

レイヤ 4 ~ 7 の詳細なパケット インスペクションと、「ステータス」を維持する機能は、スパム ゾンビによって生成されたネットワーク トラフィックの異常を識別するための強力な手段です。ソリューションがステータスを維持できないと、このような異常を検出するのが困難になります。ステータスの追加により、たとえば 1000 個の 1 KB メッセージが、1000 個の独立したセッションか、1 つの 1 MB

メール セッションかをソリューションで区別できます。ステートレス ソリューションでは、パケットの集計は可能ですが、それが多数の小さいセッションか、1 つの大きいセッションかを簡単に区別することはできません。さらに、Cisco Service Control ソリューションは、複数のログインにおける加入者ステータスを追跡することで、スパム ゾンビ アクティビティが複数の加入者ブロードバンド セッションで行われた場合、または異なる IP アドレスを使用している場合でも、それらを識別できます。サービス プロバイダーは、ステートフルなアプリケーションおよび加入者認識機能により、特定の加入者からのスパム ゾンビ アクティビティを迅速に識別して、その E メール送信をブロックすることができます。また、システムからゾンビの感染を除去できるサイトに感染した加入者をリダイレクトできます。

図 2 加入者単位の異常な数の E メール セッションを特徴とするゾンビ攻撃



加入者単位の E メール セッションのサービス コントロール分析

Cisco Service Control を使用したスパムからのネットワークの保護

スパム業者がより高度なテクノロジーに移行するのと同様に、サービス プロバイダーもそれに対応する必要があります。レイヤ 3 デバイスは、効果的な防御を実装するためのインテリジェンスとスピードを備えていません。攻撃を識別して、ネットワークを保護し、加入者に通知できるアプリケーション対応の強力なネットワーク デバイスが必要です。Cisco Service Control の高度なテクノロジーを使用すると、サービス プロバイダーは、コストをかけてインフラストラクチャを整備しなくても、ゾンビによって生成されたネットワーク上のスパムの量を大幅に削減できる市販ツールを利用できます。

また、Cisco Service Control ソリューションは、ステートフルかつ詳細なパケット インспекションにより、サービス プロバイダーにスパム防止用の強力なツールを提供します。Cisco Service Control ソリューションは、スパムを識別し、ネットワークを保護して、加入者に通知するのに必要なインテリジェンスとスピードを備えています。

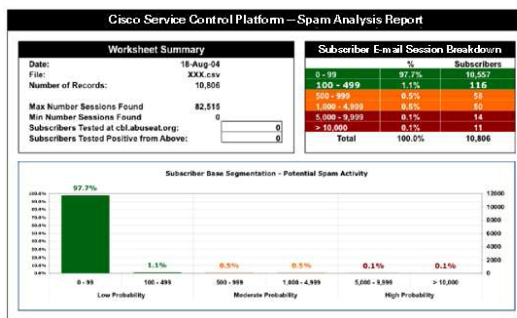
- スпам ゾンビへの対処には、アプリケーションと加入者の両方に対応したソリューションが必要です。Cisco Service Control ソリューションは、ルータやスイッチなどのレイヤ 3 デバイスよりも高度な方法で、トラフィックをモニタおよび分析します。さらに、ステータスを維持および管理する包括的な機能により、スパム ゾンビ アクティビティの検出と緩和を迅速かつ効率的に自動化できます。
- スпам ゾンビへの対処には、マルチギガビットのワイヤ スピードで動作し、帯域幅のボトルネックを生成せずに、現在のような大量のトラフィックを処理できるソリューションが必要です。Cisco Service Control ソリューションは、この基準を満たしています。

Cisco Service Control は、3 段階のアプローチを使用して、ゾンビに効果的に対処できます。

- **ゾンビ マシンの識別:** Cisco Service Control ソリューションは、早い段階でゾンビ攻撃の特性を検出できます。多くの場合、対象となるスパム メッセージ数のごく一部である、最初の数千のメッセージが送信された段階で検出できます。
- **ゾンビ マシンの検疫による攻撃からのネットワークの保護:** 疑わしいトラフィック パターンが識別された場合、被害を最小限に抑える処理をただちに実行する必要があります。迅速なレポートにより、ネットワーク管理者は、攻撃の早い段階で介入することが可能になり、ネットワークを通過するスパムの量を制限できます。
- **修正措置を実行するためのユーザへの通知:** 感染した PC のユーザは、感染に気づいていません。したがって、そのユーザのマシンから発生したゾンビ攻撃を停止するだけでなく、加入者が修正措置を実行できるようにただちに通知する必要があります。この通知を行うと、サービスの優位性がただちに示されることになるため、サービス プロバイダーにとって、上級レベルのサービスを加入者に提供する機会となります。

図 3 お客様のケース スタディ: シスコのブロードバンド スпам制御ソリューションの価値

スパム分析レポートのサンプル



Zombie Fingerprints

In conjunction with several of its service provider customers, Cisco identified several distinctive patterns indicative of zombie attacks. By monitoring these patterns for service provider customer during a typical 24-hour period, Cisco discovered the following:

- 1 percent of subscribers generated more than 1000 SMTP sessions
- 0.1 percent generated more than 10,000 sessions (refer to graph)

To validate the suspected spamming activity, Cisco then compared the list of high SMTP session users to published spam listings. Many of the +1000 group—and virtually all the +10,000 group—were listed as major spammers.

ゾンビのないネットワークの利点

ブロードバンド サービス プロバイダーは、長年にわたりスパムに対処してきましたが、成功の程度はさまざまです。ゾンビの出現は、圧力の多い業界での新たな問題と見ることもできますが、効果的な防御策を実装することで、次のような具体的な利点ももたらします。

- **市場での差別化:** ブロードバンド サービスの選択肢が多数ある場合、サービスの差別化がますます重要になります。ネットワーク上のスパムを削減するプロアクティブなステップを実行することにより、ISP は独自の強力な位置付けを確保し、競合他社との差別化を行うことができます。

- **IP ブラックリストに対する防御:**ISP の顧客の多くが感染し、ゾンビ攻撃に関わっている場合、他社は、対象 ISP の IP アドレス範囲全体のブラックリストを作成し、すべての正規ユーザがリモート E メール トランザクションを開始するのを効果的に阻止します。そのため、自社のサービスが停止した場合、加入者ロイヤルティが失われ、顧客の解約率が向上する可能性があります。
- **加入者ロイヤルティの構築:**ISP は、ゾンビ感染の被害者である加入者に対して、迅速な通知、オンライン ヘルプ、およびプロアクティブな顧客サポートを提供することにより、顧客ロイヤルティを高めることができます。
- **販売機会:**通知プロセスは、アンチウイルス ソフトウェアやファイアウォールなど、上級レベルのセキュリティ サービスとセキュリティ製品を加入者に提供する機会でもあります。
- **帯域幅の回復:**ネットワークを通過するスパムの量が少なくなると、加入者が使用できる帯域幅が増え、設備投資の必要がなくなります。ただし、この利点は、送信元または送信元の近くでスパムを停止するソリューションにのみ当てはまります。ユーザの PC で動作するスパム フィルタは、ユーザに表示されるスパムの量を削減しますが、帯域幅の解放を行うことはできません。

Cisco Service Control がプロバイダーに提供するスパム制御以外の機能

Cisco Service Control は、スパム キラーとしての強力なアプリケーションの域を越えて、さまざまなネットワーク管理機能をサービス プロバイダーに提供します。Cisco Service Control は、アプリケーションの種類とプライオリティに基づいてネットワーク帯域幅を最適化し、不要なアップグレードをなくすことでコストを削減します。これにより、加入者全体のパフォーマンスを向上させます。Cisco Service Control ソリューションは、ハードウェアおよびソフトウェアで構成され、ネットワークの使用状況をリアルタイムでモニタおよび分類する、プログラム可能なネットワーク エlementを導入しています。Cisco Service Control プラットフォームは、ブロードバンド サービス プロバイダーが加入者の識別、アプリケーションの分類、パフォーマンスのサービス レベル保証の適用、プロバイダーのトランスポートで行われる IP サービスの測定と課金を実行できるようにする、包括的なソリューションです。

Cisco Service Control ソリューションの主な機能は、次のとおりです。

- アプリケーションおよび加入者ごとにトラフィックを確実かつ正確に分類する機能を提供します。
- プログラム可能なソリューションであるため、ネットワーク セキュリティに対する新たな脅威に適応し、拡張することができます。
- すべての分類がリアルタイムで実行され、キャリアグレードの構成でギガビット ライン レートをサポートする、優れた機能を提供します。
- インテリジェントかつトランスペアレントなネットワーク オーバーレイの展開に必要なネットワークの再設定が最小限で済むため、プロバイダーは、追加投資を最小限に抑え、複数のサービスでソリューションを償却できます。

Cisco Service Control テクノロジーを使用すると、ブロードバンド オペレータは、ネットワーク リソースの効率的な管理、ネットワーク パフォーマンスの向上、運用コストの削減、および新しいブロードバンド サービスの開発が可能になります。

©2007 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、およびCisco Systemsロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における登録商標または商標です。本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(0704R)

この資料に記載された仕様は予告なく変更する場合があります。



シスコシステムズ株式会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先(シスコ コンタクトセンター)

<http://www.cisco.com/jp/go/contactcenter>

0120-092-255 (通話料無料)

電話受付時間：平日10:00～12:00、13:00～17:00

お問い合わせ先