「防弾」ホスティングプロバイダー：サイバー犯罪インフラの防御網に生じた亀裂

成功しているサイバー犯罪者は、安全で発見されにくく、かつ復元力のあるインフラに依存しています。ネットワーク侵害、認証情報の窃取、ランサムウェア、さらには不正フォーラムでのデータの盗難や販売といったあらゆる事例の背後には、サイバー犯罪者の活動や身元の秘匿を可能にする安全なインフラが存在しています。

しかし、サイバー犯罪者にとって、自分の存在を気づかれずに、追跡されにくい状態を保ち続けることは、ますます難しくなっています。各国の政府、法執行機関、民間セクターの連携が進んだことで、オンライン上で匿名性を保つのが難しくなってきているのです。さらに、安全なインフラを自身で構築・維持するための高度なスキルや専門知識を持つサイバー犯罪者は、ほんの一握りしか存在しません。そのため、サイバー犯罪者は、このようなサービスを提供してくれる違法なインフラプロバイダーを探し出し、自身は被害者への攻撃や利益の獲得に専念できるようにしています。

「サイバー犯罪者のためのサービス（Cybercrime-as-a-service）」とは、さまざまな悪意あるサイバー行為者を支援する目的で発展してきたアンダーグラウンド市場を指します。この市場では、サイバー犯罪者がオンライン上の標的を攻撃するために利用する各種のツール、サービス、情報が、日々進化・拡大しながら取引されています。これからサイバー犯罪に手を染めようとする者が、ネットワークへのアクセス権を購入したり、セキュリティ対策を回避するためのツールを入手したり、被害者に使用して個人情報を盗むためのマルウェアを購入したりすることができます。防弾ホスティング（BPH）プロバイダーはこの犯罪エコシステムの一翼を担っており、サイバー犯罪者に対して安全なインフラを提供しています。重要なのは、1つのBPHプロバイダーが、世界中の何百人ものサイバー犯罪者による攻撃を可能にしているという点です。

「防弾」ホスティングプロバイダーとは？

簡単に言えば、防弾ホスティング（BPH）プロバイダーとは、サイバー犯罪者に対して、活動の拠点となる仮想または物理的なインフラをリースする業者です。BPHプロバイダーは、悪意あるアクター（サイバー犯罪者を含む）がインターネット上で違法なコンテンツをホストし、不正な活動を行うことを可能にする、特殊なタイプのインターネットインフラサービスです。

「防弾」という呼び方は、あくまでもマーケティング用語にすぎません。実際には、これらのサービスも他のインフラプロバイダーと同様に、妨害やサービス停止の対象となり得ます。しかし、BPHプロバイダーは、法執行機関やその他からのコンテンツ削除要請に応じることを拒み、被害者や利用者からの悪用に関する苦情、加入者からの要請通知も無視します。その結果、サイバー犯罪者は、通信、違法なフォーラムやウェブサイトの運営、マルウェアやフィッシング攻撃の実行、さらには資金洗浄といった行為を、運営者が法執行機関やその他の要請に応じて契約を打ち切る心配をすることなく続けることができるのです。

BPHプロバイダーは、自身がサイバー犯罪エコシステムの一部であることを認識した上で、金銭目的の深刻なサイバー犯罪を可能にしています。オーストラリアの組織やその顧客が被害を受けた重大なサイバーセキュリティインシデントでは、BPHプロバイダーを利用した犯罪者の関与が確認されています。これらの事件によって、ランサムウェアによる業務の妨害、データを使った脅迫、機微な情報の窃取といった被害が発生しています。

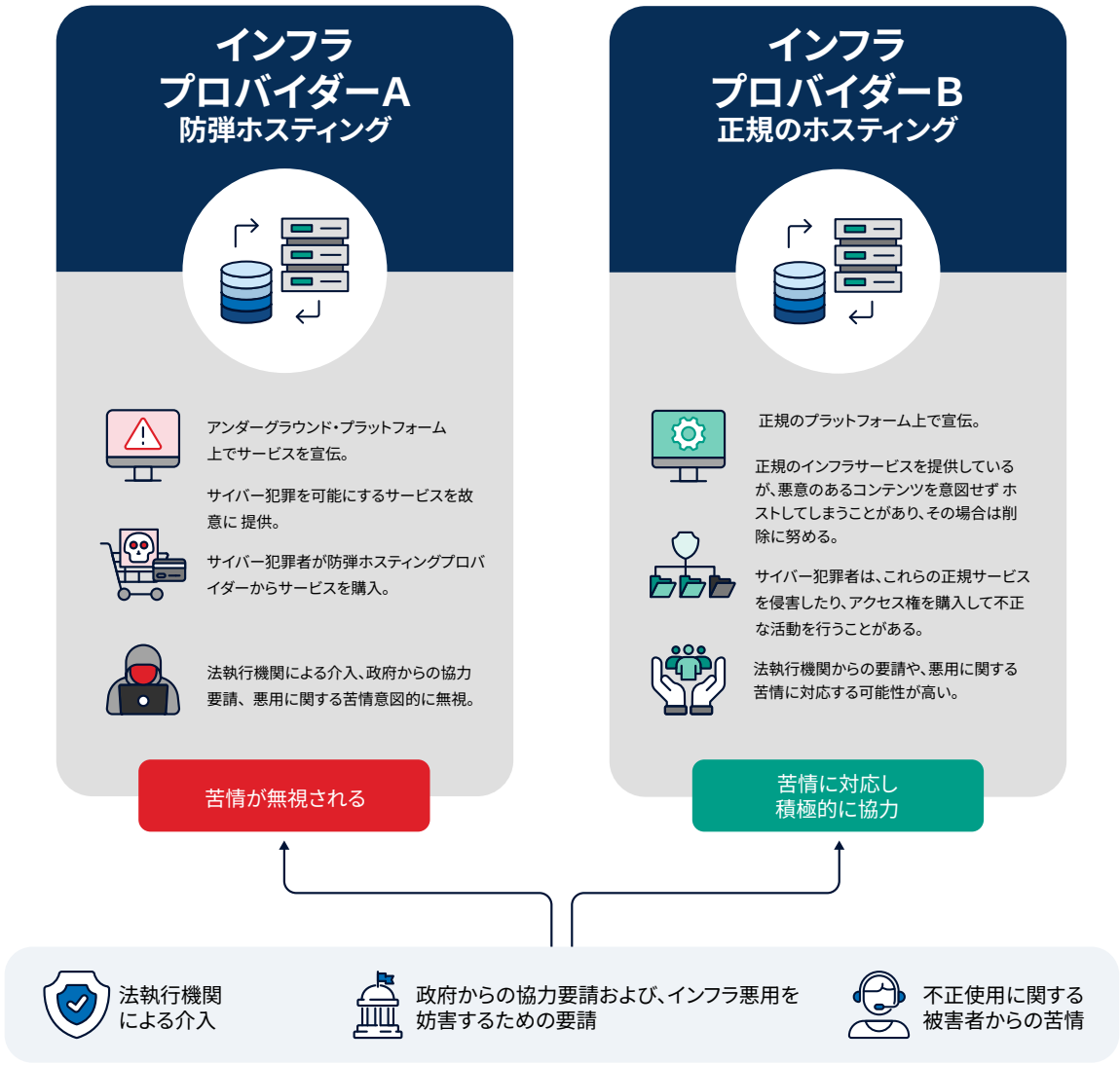
アンダーグラウンドフォーラムに掲載された防弾ホスティングプロバイダーの広告例：

BPHプロバイダーの仕組みとは？

BPHプロバイダーのビジネスモデルは、事業者によって異なります。最も一般的なやり方は、サイバー犯罪者にIPアドレスを貸し出し、複雑なネットワークスイッチ手法を用いて、所在地や身元、活動内容を秘匿するというものです。多くの場合、BPHプロバイダーは、他の正規のホスティングプロバイダーやデータセンター、インターネットサービスプロバイダー（ISP）から、IPアドレスやサーバーを再販またはリースの形で取得しています。こうした「上流」のプロバイダーは、自社のインフラがBPHプロバイダーを通じて「下流」のサイバー犯罪者に提供されていることに気づいていない場合があります。

BPHプロバイダーは、顧客の身元が特定されにくくなるよう、自社のネットワークやシステムの構成を巧妙に設計しています。たとえば、彼らは、顧客の活動に関連付けられたインターネット上の識別子（割り当てられたIPアドレスやドメイン名など）を頻繁に変更します。このような手法により、アクターや顧客が特定の時点で使用していたIPアドレスとインシデントを結びつけることが難しくなり、防御側や調査機関による対応が妨げられます。さらに、BPHプロバイダーは、悪意あるサイバー行為の調査や防止に関する正式な制度が存在しない、または極めて緩やかな国にインフラを設置していることがよくあります。

防弾ホスティングプロバイダーは、正規のインフラプロバイダーとどのような点で異なるのか？



BPHプロバイダーを標的にすることで、サイバー犯罪の脅威はどう変化するのか

BPHプロバイダーは、一度に数百から数千ものサイバー犯罪者の活動を阻止するための貴重な機会となります。。さまざまなサイバー犯罪者やその他の悪意あるサイバーアクターは、犯行を容易にする手段としてこれらのサービスを利用しており、削除要請や悪用に関する苦情が寄せられても、活動が秘匿されていて継続できると信じています。

しかし、法執行機関、政府機関、民間セクターが連携し、既知のBPHプロバイダーからのインターネット通信をあらかじめ遮断するなどの防御的措置を講じることで、こうした違法なインフラプロバイダーを対象に、その活動を妨害しています。こうした取り組みによって、オーストラリアおよび同盟国のネットワークに接触するサイバー犯罪の件数を減らすことが可能になります。また、正規の「上流」インフラプロバイダーやISPが、意図せずBPHプロバイダーにインターネット接続や安全なインフラを提供してしまっている場合もあります。

BPHプロバイダーは、「サイバー犯罪者のためのサービス」のエコシステムにおけるインフラ提供者の一つにすぎません。これらのサービスは、サイバー犯罪者の活動を積極的に支援し、正当な捜査や対応を意図的に妨害することで、オーストラリアにおけるサイバー犯罪の脅威を助長し、長期化させています。BPHプロバイダーに対して措置を講じることで、こうしたサービスの脆弱性や、それを利用する悪意あるサイバーアクターの実態が明らかになります。