アンラボ・セキュリティレター

# Press Ahn

2023.7　Vol.115

## ランサムウェアグループの新しいビジネスモデル、RaaS の最新動向は？

# ランサムウェアグループの新しいビジネスモデル、RaaS の最新動向は？

**RaaS (Ransomware as a Service) とは、サイバー犯罪者がランサムウェアの配布および管理に必要なツールとサービスを提供する新しいランサムウェアビジネスモデルを意味する。2015年に初めて知られたこのモデルは、構成員が役割を分担し収益を共有する形で組織化されており、活発な仮想通貨の使用と匿名性に支えられ、既存のランサムウェアよりさらに進化した恐喝手法を用いる。**

**RaaS モデルを利用すれば、ランサムウェア開発に関する専門知識が全くなくても、誰でもランサムウェア攻撃を通じて莫大な金銭的利益を得ることができる。このためランサムウェア攻撃はますます活発になっており、被害規模も大きくなっている。アンラボは最近、RaaS の運営構造と収益モデル、そして恐喝戦術を詳細に扱った「RaaS 動向報告書」を発行した。その内容を詳しく見てみよう。**


## RaaS の運営構造

RaaS は一般的にランサムウェア開発および RaaS 運営者と系列会社、初期侵入ブローカー (Initial Access Broker、IAB) が運営する。

まず、ランサムウェア開発者および RaaS 運営者は、ランサムウェア開発および RaaS の運営に使用されるツールとサービスを提供する。彼らは各自の役割を分担して被害組織との交渉、データリークサイトの管理、サイバー犯罪フォーラムで活動する代弁者、身代金支払いに対する処理、マネーロンダリングなどを担当する。

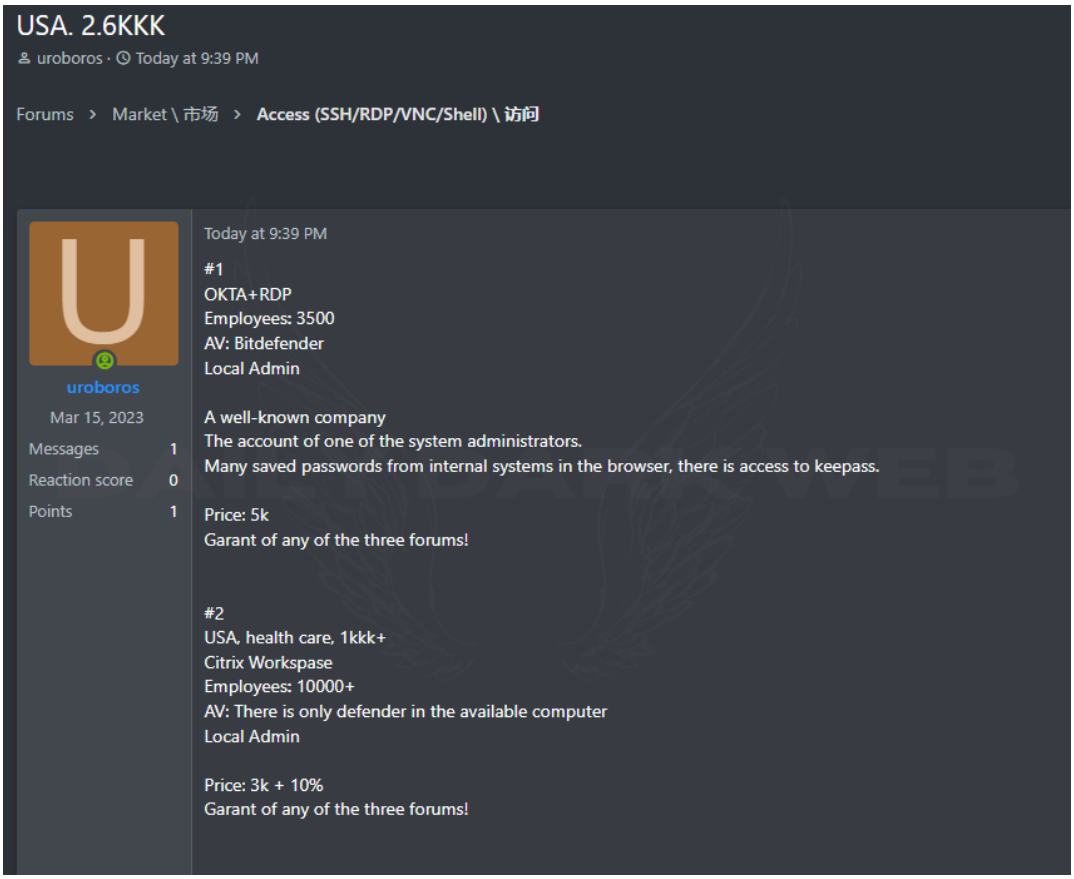
系列会社は実質的なランサムウェアの配布と攻撃を担当し、初期侵入に対する専門技術を保有した一人または多数で構成される。系列会社は侵入した組織内部に長期的または短期的に隠れ、ランサムウェアを流布および実行する。場合によっては暗号化する前にデータを流出することもある。流出したデータは身代金をつり上げる二重恐喝戦術に使われ、被害者が身代金を支払えばファイルを復号化する手続きを案内する。

一部の系列会社は単一の RaaS 組織と提携する傾向がある。しかし「Bassterlord」というニックネームを使用している人物とのインタビューによれば、系列会社はいろいろな RaaS と提携するケースがより多いことが確認された。この人物は一時レヴィル（Revil）、ランサム EXX（RansomEXX）、アバドン（Avadon）、ロックビット（LockBit）の系列会社と協力したことがある。

系列会社は収益を得るために一つではなく多数の RaaS と協力関係を維持する。これにより、特定の RaaS には多数の系列会社があり、系列会社ごとに使用する攻撃技術に差がある。したがって、セキュリティ企業は昔とは異なり、ランサムウェア攻撃に使われた技術（Tactics、Techniques、Procedures、TTP）を特定の RaaS と結びつけることに苦労している。

IAB は初期侵入に専門技術力を保有している人のことで、系列会社とは別に活動する。一部の RaaS は IAB と似た役割を果たす侵入テスターを別途募集することもある。RaaS の核心的な構成員として急速に定着している彼らは、多様なサイバー犯罪組織にネットワークアクセス権限を販売する。例えば、ランサムウェア系列会社は組織運営のためにネットワークへのアクセス権限を定期的に購入することが何よりも重要だ。最近の系列会社は直接攻撃対象を選定するよりは IAB からネットワークアクセス権限を購入する。

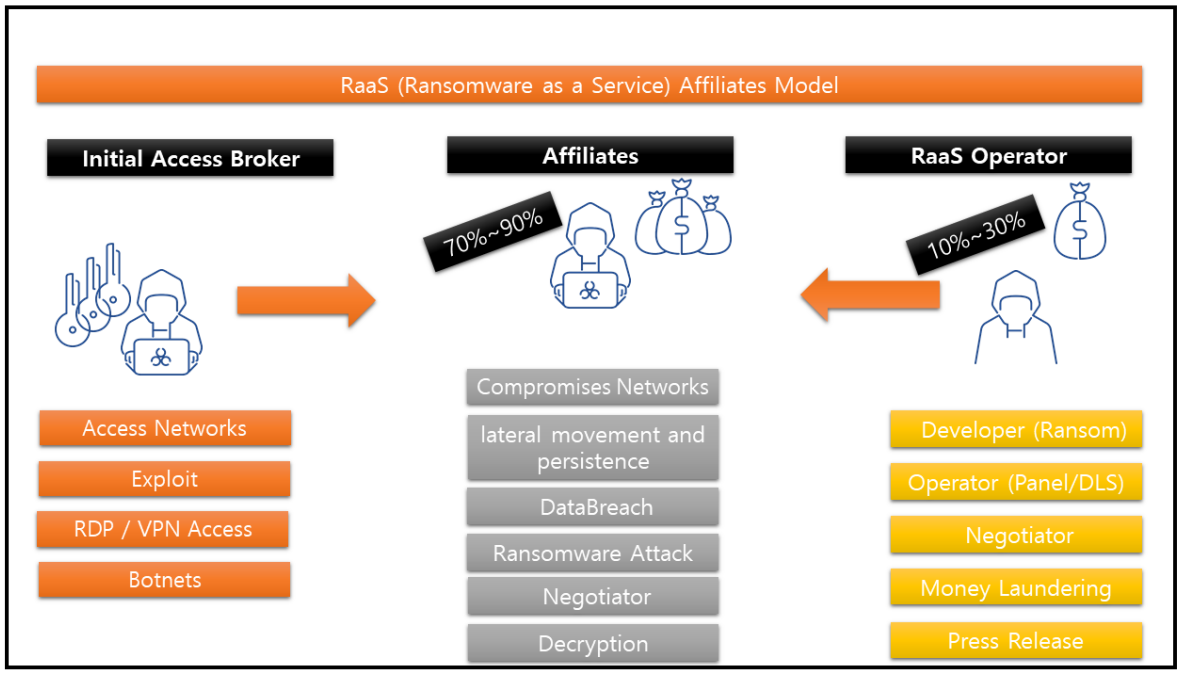
IAB は標的としたネットワークに侵入して長期的または短期的に隠れ、セキュリティ製品の使用およびサイバー攻撃被害保険加入有無の把握、RDP / VPN アクセス権限の収集、脆弱性、資格証明流出、ボットネット（Botnet）で使うマルウェアを流布したりもする。彼らは侵入後窃取した情報を利用してサイバー犯罪フォーラムに［図 1］のようにネットワークアクセス権限の販売文を掲示する。




［図 1］IAB のネットワークアクセス権限の販売文（出典：@DailyDarkWeb）

IABs は主にアメリカと欧州連合（EU）、アジア太平洋諸国を対象に初期侵入してネットワークアクセス権限を確保する。アメリカ内の組織へのアクセス権限は他の国より高い価格で販売されており、銀行ドメインへのアクセス権限も他のドメインより高い。最近 10,000 ~ 160,000 ドル（約 144 万円 ~ 3,208 万円）で販売されていることがわかった。

前述の RaaS 構成員とその役割を図式化すると、[図 2] のようになる。

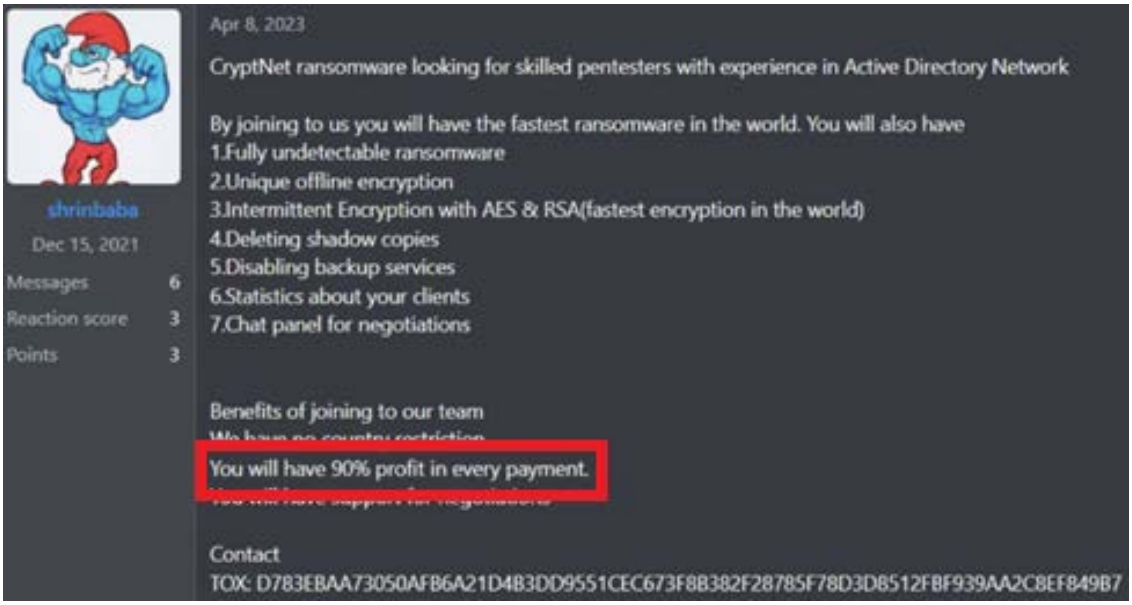



[図 2] RaaS 組織構成図

## RaaS の収益構造

RaaS はランサムウェア開発者および運営者がランサムウェアを作成すれば、系列会社がこれを流布する形だ。そのため、開発者と運営者が系列会社に収益の一部を割り当てる。

RaaS 運営者は通常、身代金の 10 ~ 30% を受け取り、残りは企業ネットワークへの不正アクセスおよびランサムウェアの配布を実行する系列会社が受け取る。この割合は系列会社が身代金をどれだけ多く稼ぐかによって変わることもある。比較的最近知られているクリプトネット (CryptNet) の RaaS 組織はサイバー犯罪フォーラムの広告で、運営者は身代金の 10%だけを受け取り、90% を系列会社に分配すると明らかにした。これは一般的な RaaS の利益分配率とは少し異なり、新規 RaaS 組織が多数の系列会社を確保して勢力を拡張しようとする意図であると推定される。




[図 3] サイバー犯罪フォーラムのクリプトネット RaaS 広告 (出典: zerofox.com )

系列会社は実際にランサムウェア攻撃のすべての部門を担当し、身代金の 70 ~ 90% を受け取る。一部の系列会社はランサムウェア攻撃時に売上高が高い組織を優先順位に指定したり、特定産業群のデータを好んだりする。例えば、医療機関や最先端技術を保有している企業のデータは、販売時に大きな収益を得ることができるため、攻撃の対象となりやすい。結局、ランサムウェアグループが特定の産業群を狙って攻撃する理由は、その産業群で収益を得る可能性が高いためだ。

## RaaS の恐喝方法

ランサムウェア攻撃に対する対応としてバックアップと復旧プロセスがアップグレードされ、攻撃者たちはファイルの暗号化だけでこれ以上身代金を受け取ることが難しくなった。したがって、攻撃者たちはデータを武器化し始め、これを二重恐喝戦術と呼ぶ。二重恐喝戦術は攻撃者がデータを暗号化する前、被害組織または高位経営陣の敏感な情報を選別し流出した後、これを公開 / 販売すると脅迫して身代金を受け取ったり、その金額をつり上げたりするための手法だ。一部の RaaS 組織はランサムウェアを配布せずにデータだけを流出して脅迫するデータ強奪グループに変貌することもあり、カラクルト (Karakurt) グループが代表的な例だ。

また、攻撃者は電気、水道、行政といった社会基盤施設の重要インフラを侵害し、DDoS 攻撃を加える三重恐喝戦術も使用する。これを通じて攻撃者はユーザーがサービスを正常に利用できないようにした後、復旧するという条件で身代金を要求する。

その後、四重恐喝戦術も登場したが、これは流出したデータを単にランサムウェアのデータ流出サイト (Data Leak Sites、DLS) に掲示するレベルにとどまらず、ランサムウェアのセキュリティインシデントやデータ流出関連の内容を被害組織の顧客、ビジネスパートナーまたは競合他社に積極的に知らせる。これは被害組織の評判を脅かして身代金を受け取ろうとする目的だ。

## RaaS の動向

サイバー犯罪グループ間の関係は、非常に急速に変化する。系列会社は実力のある他のサイバー犯罪グループの人材を雇用し、収益配分率が良く支援ツールとサービスを惜しみなく提供する多数の RaaS と協業することもある。一部の最上位組織は法執行機関の監視が強化されれば運営を中断し、新しい名前にブランドを変更する。

ランサムウェア攻撃の大部分は特定対象を直接攻撃するのではなく、IAB が販売しているネットワークアクセス権限の中から攻撃に成功した後に身代金を受け取ることができそうな組織のネットワークアクセス権限を購入する。主な攻撃対象としては、北米地域に位置する一般企業および大企業であり、法執行機関の追跡や監視を避けるために他の地域または小規模な組織を狙うケースも増加している。この他に IAB またはサイバー犯罪組織が流布したエモテット (Emotet)、クアックボット (QakBot)、アイスド ID (IcedID)、ピカボット (PikaBot) のような既存のマルウェア感染を初期侵入経路として使用し、ランサムウェア攻撃を遂行することもある。

### (1) ロックビット (LockBit)

ロックビットは 2023 年 1 月から 5 月末まで 450 箇所を越える被害者リストを掲示した最も活動的なランサムウェアグループだ。2019 年に初めて報告され、100 社を超える系列会社を保有している。ロックビットランサムウェアは速い暗号化速度とセキュリティツール回避機能などを系列会社に貸し、医療、教育、慈善、社会サービス部門に所属した組織は攻撃標的にしないというのが特徴だ。これと関連して、今年 1 月にロックビットの系列会社がカナダのトロント所在のある小児病院を攻撃した際、ロックビットは侵害行為に対して謝罪し無料で復号化ツールを提供した。

ロックビットランサムウェアは被害組織の情報と流出データを販売する四重恐喝戦術を使用する。系列会社になるためには、多様なアンダーグラウンドハッキングフォーラムのプロフィールリンクと他の RaaS の提携証明による技術能力および以前に遂行した攻撃に関する証拠が必要だという。

**(2) アルフ V (ALPHV)**

2021 年末に初めて報告された「ブラックキャット (BlackCat)」とも呼ばれるアルフ V (ALPHV) は、高性能およびメモリ安全性によって人気が高いラスト (Rust) 言語を使用して最初のランサムウェアを開発した。そのランサムウェアは昔のダークサイド (DarkSide) とブラックマター (BlackMatter) ランサムウェアをブレンドしたものと推定される。

このランサムウェアグループは、セキュリティツールを無効化して分析機能を迂回する。電気、ガス、上水道などの重要インフラと医療、製造、金融、法律、専門サービス産業を対象に攻撃する。

二重恐喝戦術を使う彼らは最近、被害組織に対する脅迫のレベルが高くなった。例えば、高位経営陣の不正や企業の秘密資料を公開して身代金を要求するやり方だ。系列会社は身代金の支払い規模によって多様な収益割合で受け取る。例えば、身代金が 150 万ドル、300 万ドル、300 万ドル以上の場合、系列会社が受け取る収益割合はそれぞれ 80%、85%、90% と異なる。

**(3) レヴィル (REvil)**

2019 年に初めて登場したレヴィルは、ガンドクラブ (GandCrab) をブレンドしたバージョンだ。現在は存在しないダークサイドグループとも関連があると推定される。2021 年 7 月、レヴィルの提携会社のうち 1 社がカセヤ (Kaseya) という企業が開発したシステム管理およびモニタリングツールのゼロデイ (Zero Day) の脆弱性を悪用し、全世界 30 箇所余りの MSP (Managed Service Provider) と彼らが管理する企業 1,000 社以上のネットワークを損傷させた。

この攻撃により 2022 年 1 月、アメリカはロシア政府を圧迫して RaaS 構成員の一部を逮捕した。瓦解したと思っていたレヴィルは 2022 年 5 月、中断されたデータ流出サイトに被害組織が再び掲示され復活した。レヴィルは身代金を支払う条件が整った組織を狙い、特に売上高の高い産業群を中心に攻撃する。レヴィルを代表する人物は「Unknown」というニックネームを使うことが知られており、現在は行方がわからない状態だ。

**(4) ブラックバスタ (BlackBasta)**

2022 年 4 月に初めて知られたランサムウェアグループのブラックバスタ (BlackBasta) は二重恐喝戦術を使用し、クアックボット (QakBot) のマルウェアでシステムを感染させてアクセス権限を得る系列会社を利用して多数の組織に被害を与える。一部のセキュリティ会社と研究員たちは、ランサムウェアグループのコンティ (Conti) が瓦解した後に派生したグループと推定している。また、「カーバナック (Carbanak)」とも知られている、金銭的動機を持つサイバー犯罪ギャングである FIN7 とも関連している。彼らは主に建設、運送および関連サービス、通信、自動車部門などの産業群を狙っている。

**(5) ロイヤル (Loyal)**

ロイヤル (Loyal) は 2022 年 9 月に初めて発見され、多様な感染経路の中で SEO (Search Engine Optimization) ポイズニング (Poisoning) 攻撃で感染した事例が多かった。SEO ポイズニングはマルウェア流布先を検索サイトの上位に配置し、そのサイト訪問者にランサムウェアを流布する攻撃方式だ。ロイヤルはランサムウェアを流布する前にレッドライン (RedLine) やアースニフ (Ursnif) のようなマルウェアでシステムを感染させて必要な情報を獲得する。医療、製造、通信など重要なインフラを備えた産業群を重点的に攻撃し、今年 4 月末にはアメリカのテキサス州ダラス市を攻撃して都市インフラを麻痺させた。

**(6) バイスソサエティ (Vice Society)**

2021 年に初めて知られたバイスソサエティ (Vice Society) は、ランサムウェアを自主的に開発する前までハローキティ (Hello Kitty) やツェッペリン (Zeppelin) などさまざまなランサムウェアを使用した。多様な産業群を対象に攻撃したが、アメリカの教育業界を中心に攻撃したため、教育部門だけを標的にしたと誤解されたりもした。バイスソサエティは二重恐喝戦術を使い、比較的大きな金額の身代金を要求すると知られている。

**(7) プレイ (Play)**

ランサムウェアグループのプレイ（Play）は、2023 年 2 月にアメリカのカリフォルニア州オークランド市を攻撃した。オークランド市は都市インフラが麻痺して非常事態宣言を出したが、その内容が記事化されてランサムウェアグループのプレイが大衆に知られるようになった。一部のセキュリティ会社と研究員は、「ランサムウェアグループのハイブ（Hive）」と連携していると推定した。プレイも多様な産業群を対象に攻撃を遂行し、被害を受けた組織はラテンアメリカに多数分布している。

### (8) クロップ（Clop)

ランサムウェアグループのクロップ（Clop）は 2019 年 2 月、「TA505」というサイバー犯罪組織による大規模なスピアフィッシングキャンペーンを開始して知られた。最近、ゴーエニウェア（GoAnywhere）MFT のゼロデイ（Zero Day）脆弱性を使って 130 箇所以上の組織にデータ流出およびランサムウェアによるセキュリティインシデントを起こした。2021 年にインターポールの国際捜査により一部系列会社が逮捕されたが、現在まで瓦解せず活動中だ。

## 結語

このように RaaS はランサムウェアの開発 · 流布に必要な技術とインフラを提供することで攻撃の難易度を下げて効率性を高める。その結果、RaaS は近年急激に増加しており、ランサムウェア攻撃はますます精巧になっている。ランサムウェア攻撃者は初期侵入戦術と技術を整備し、攻撃対象選択時にどの国の対象を攻撃すればより大きな収益を得ることができ、どのデータが盗む価値があり、脅迫レベルと強度はどう調節するべきかなど、ランサムウェア攻撃戦略に対するノウハウを得ている。ランサムウェア攻撃者の目標はただ一つ、大金を稼ぐことだ。

皆が懸念しているように、人工知能（AI）技術および自動化されたツールと開発で、さらに多くの攻撃が発生する可能性もある。サイバー犯罪者たちはエンドポイント保護ソリューションを回避し、完全に迂回するために合法的なドライバを悪用した高級回避技術を具現化している。多様な恐喝戦術が利益を創出しており、間欠的暗号化の出現と Windows や Linus などプラットフォーム間ランサムウェアが増加している。多数の系列会社が登場し、彼らが使用する攻撃技術が多様化し、ランサムウェア攻撃によるセキュリティインシデントを調査する際に特定ランサムウェアと結びつけることは容易ではない。

ランサムウェアの被害は企業と個人の両方に深刻な脅威として作用する。ランサムウェア攻撃を受ければ、金銭的な損失だけでなく評判にも打撃を受け得る。ランサムウェア攻撃より先に備えることが最も必要な予防措置であり、ランサムウェア攻撃を防止するためには強力なセキュリティソリューションを導入し、社員たちのセキュリティ認識を向上させる教育を実施しなければならない。また、バックアップを定期的に行ってデータ損失を防止することが何よりも重要だ。サイバー脅威インテリジェンスサービスはランサムウェア攻撃者に対する情報と知識を提供し、組織の先制的な対応に役立つ。

http://jp.ahnlab.com/site/main.do

http://global.ahnlab.com/site/main.do

http://www.ahnlab.com/kr/site/main.do

**アンラボとは**

株式会社アンラボは、業界をリードする情報セキュリティソリューションの開発会社です。
1995年から弊社では情報セキュリティ分野におけるイノベーターとして最先端技術と高品質のサービスをご提供できるように努力を傾けてまいりました。今後もお客様のビジネス継続性をお守りし、安心できるIT環境づくりに貢献しながらセキュリティ業界の先駆者になれるよう邁進してまいります。
アンラボはデスクトップおよびサーバー、携帯電話、オンライントランザクション、ネットワークアプライアンスなど多岐にわたる総合セキュリティ製品のラインナップを揃えております。どの製品も世界トップクラスのセキュリティレベルを誇り、グローバル向けコンサルタントサービスを含む包括的なセキュリティサービスをお届け致します。

AhnLab

〒108-0014 東京都港区芝4丁目13- 2 田町フロントビル3階 | TEL: 03-6453-8315 (代)