アンラボ・セキュリティレター

Press Ahn

2014.2　Vol.02

11 のルールで APT 攻撃を防止せよ

APT 攻撃の現状と対策

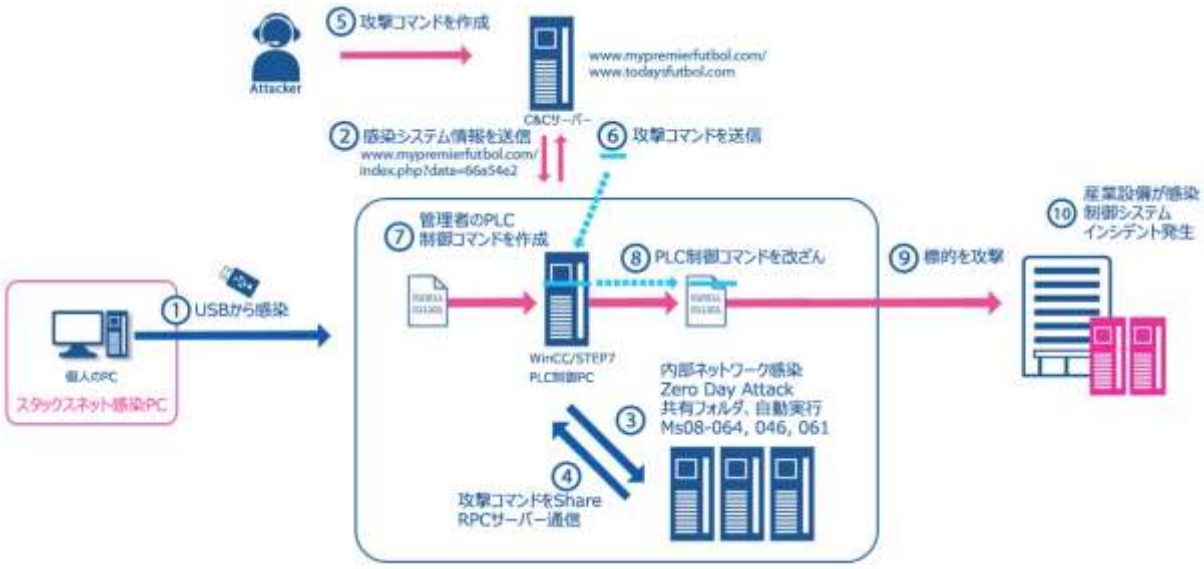
11 のルールで APT 攻撃を防止せよ

インターネットで繋がる世界は、網の目のように絡み合いながら益々複雑になっている。このような環境はマルウェアが生息・増殖するに最適な条件でもある。新年のご挨拶や結婚式の招待状、履歴書さえも電子メールやSNSを使って送付することが日常となっている今日、思わず開いたメールや常に使用していたSNSにマルウェアが潜んでいるとしたら…

インターネット環境が発達しユーザーが増えるほど、脆弱性の隙を狙うマルウェアもより巧妙になっていく。さらに不特定多数ではなく、特定の企業や組織、インフラ施設等が標的となり、ポイントアタックによる破壊力も想像を超える。今やセキュリティを知る人ならばしばしば目にする単語「APT」。2014年、進化したAPTによる対策の変化について確認する必要があるだろう。

APT の定義

2004年6月、韓国政府や企業の一線でPeepViewerというトロイの木馬に感染するケースがあった。韓国の情報筋によると6つの公共機関でPC64台と、民間企業のPC52台が感染されたという。手口としては電子メールで「ワークショップの概要とスケジュール、MDB」という添付ファイルを送信しマルウェア感染を試みたという。これは機密情報を奪取するために政府と民間企業を攻撃した韓国初のAPT攻撃事例として挙げられている。
以来、再び大規模なAPT攻撃が発生したのは2011年からだった。代表的なインシデントには同年4月に発生した農協のネットワークダウンがある。外部からの攻撃によって農協のネットワークシステムがダメージを被り、すべての業務がストップしてしまった。本件はアウトソーシングスタッフのノートパソコンがまずマルウェアに感染し、感染PCを介して内部システムに侵入する手法を使用した。攻撃者はP2Pプログラムにマルウェアを配布し、7ヶ月に渡ってモニタリングを続けながら攻撃のタイミングを図っていたことが分かった。

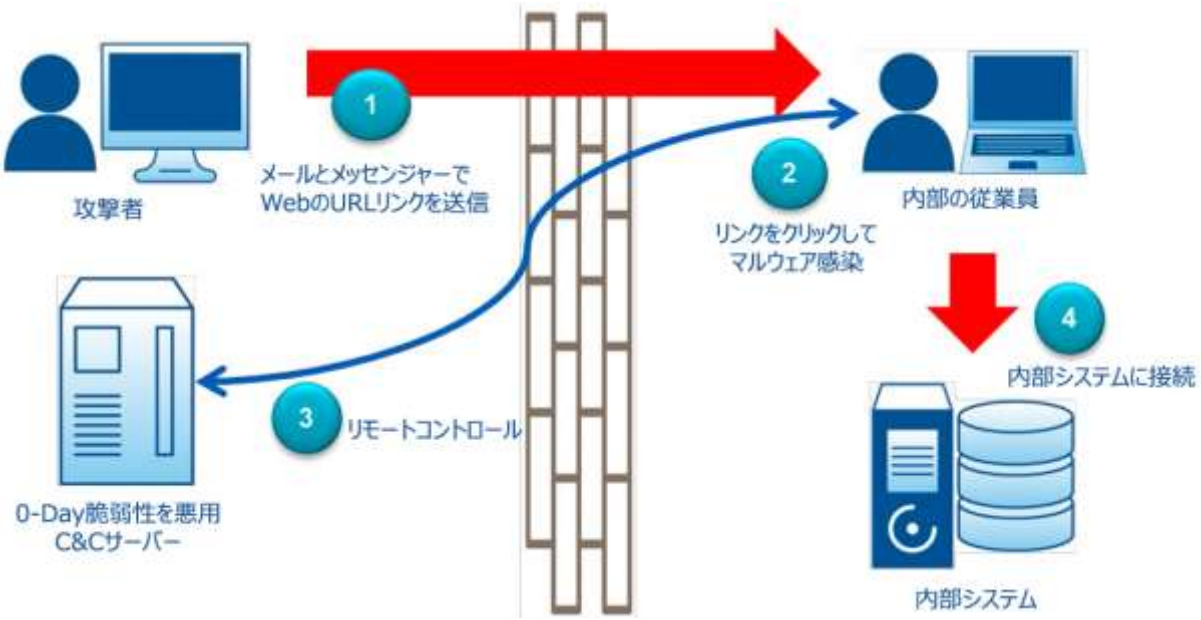


【図1】スタックスネット感染と動作メカニズム

続いてわずか3ヶ月後、7月には韓国の大手IT企業SKコミュニケーションズで3500万人ものユーザー情報が流出された事件が起こった。この時は無料のソフトウェアアップデートサーバをハッキングして、通常ファイルをマルウェアで改ざんした後に拡散させる方法を用いた。攻撃者はたった8日でDBの管理者権限を取得し、データを分割圧縮して外部に流出している。

その他代表的なインシデントとしては、2010年に発生したイラン原子力発電所のシステム破壊を目的としたスタックスネット（Stuxnet）がある。攻撃者はWindows OSに存在する既知の脆弱性とゼロデイ脆弱性を悪用してマルウェアを配布した。 2011年に報告されたDuquと2012年に発見されたFlameも、すべてイランの原子力発電所の情報収集を目的にして起こった標的型攻撃だった。

2010年1月にはGoogleの機密データを奪取するためのオペレーションAuroraが発生し、Googleのほか最先端のIT企業34社も攻撃を受けている。ここでもMicrosoft IEのゼロデイ脆弱性が悪用され、メールやメッセンジャーで悪意あるWebサイトに接続するリンクが配布された。



【図2】IT企業を攻撃したオペレーションオーロラ

2011年3月にはEMC/RSAのOTP（One Time Password）製品の機密情報を奪取しようとする試みがあった。標的を選定するため、ソーシャルネットワークを使って従業員の個人情報を確保した点から本格的なAPTとして知られている。Adobe Flash Playerのゼロデイ脆弱性を悪用した添付ファイルをメールで送信し、社会工学的手法で従業員のマルウェア感染を誘導した。

【図3】EMC/ RSAで発生したインシデント過程

2012年2月CNNは、シリア政府が反政府人物を監視する目的でマルウェアを配布したと暴露した。アンダーグラウンドに公開されたDarkComet RATでマルウェアを作成し、メールの添付ファイル、偽のYoutube、skypeからマルウェアを配布したことが分かった。このマルウェアには主にシリア、イスラエル、サウジアラビア、レバノンなどのPCが感染した。

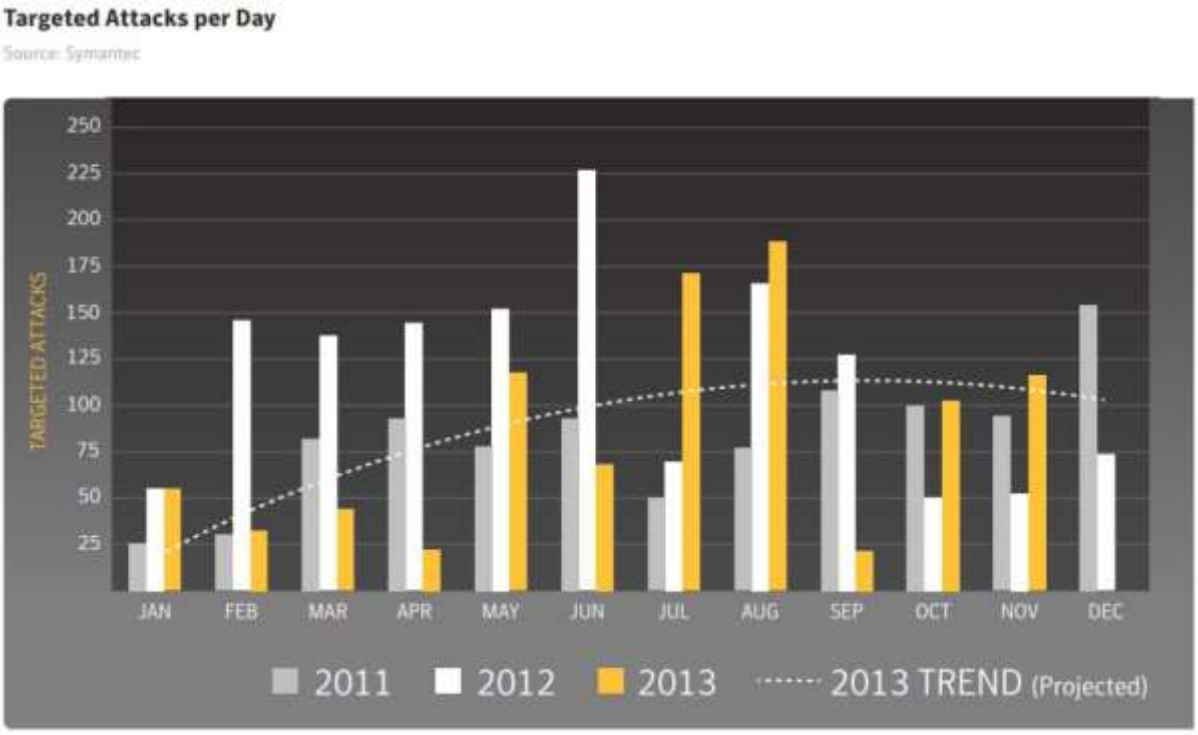
2013年はAPT攻撃がさらに猛威をふるい、1月オペレーション「Red October」が東ヨーロッパと中央アジアの国家機関をハッキングする事件が発生した。このマルウェアは政府や研究機関などを標的に、高度な攻撃を仕掛けたという。さらに2月にはニューヨーク・タイムズ、ウォール・ストリート・ジャーナルなど米国の主要メディアが以前ハッキングの試みがあったと発表し、その黒幕を中国の「APT1」と報道して話題になった。3月にはインドのハッカー集団オペレーションhangoverが近隣諸国の政府機関をハッキングする事件が発生したり、韓国では放送局や金融機関など6社のネットワークがダウンするサイバーテロが発生していた。
4月、国際ハッカー集団「Winnti」が韓国を始めとするアメリカ、日本など30カ国以上のオンラインゲーム会社を攻撃し、6月にはNetTravelerが世界40カ国350の機関を攻撃したことが分かった。続いて9月には、小規模なサイバー傭兵隊「Icefog」と中国に拠点を置くハッカー集団「Hidden Lynx」が韓国と日本の政府機関や企業を対象に攻撃を仕掛け、その実体が明るみに出た。12月にはG20首脳会談の直前、中国のハッカー集団「Ke3chang」が、欧州5カ国の外交部長官のコンピュータをハッキングした事件が報道されたこともあった。

【図4】2013年の主なAPT攻撃ケース

APT 攻撃の様相

攻撃対象の拡大

コンピュータの使用環境が発達することにより、政府機関や各企業では業務の自動化システムを導入している。ほとんどの業務はもちろんのこと機密書類でさえも、電子文書などのデータ形式でファイルサーバに保存することが一般的である。これは標的型攻撃が増加しやすい環境なのだ。
かつては主に政府や軍事機関のみ攻撃対象と見なされていたが、今は経済的に付加価値の高いデータを保有しているハイテク企業を含む民間企業にまで攻撃対象が拡大した。
特に韓国と日本は金融、放送、オンラインゲーム会社なども攻撃の対象となっている。



【図5】標的型攻撃の増加傾向（参考資料：シマンテック）

対象	目的
政府機関	- 政府機関の機密文書を奪取 - 軍事機密文書を奪取
インフラ産業施設	- サイバーテロ活動 - 産業インフラ動作不能
情報通信業者	- 最先端の技術資産を奪取 - オリジナル技術の機密情報を奪取
メーカー	- 企業の知的資産を奪取 - 企業の営業秘密を奪取
金融業者	- 社会金融システムの動作不能 - 企業の金融資産情報を奪取

高度化された攻撃手法

Webやソーシャルネットワークの発達は、標的の個人情報を容易に収集できるようにした。収集された個人情報をベースに、標的にカスタマイズされた社会工学的手法を開発し、攻略の成功率を高めているのである。EMC/RSAインシデントも、内部の従業員に採用情報の関連メールを装って送信したことから起こった。

さらにマルウェアの作成と脆弱性開発技術の発展は、セキュリティ製品の検知バイパスとAPT攻撃の成功率を高めることに貢献した。

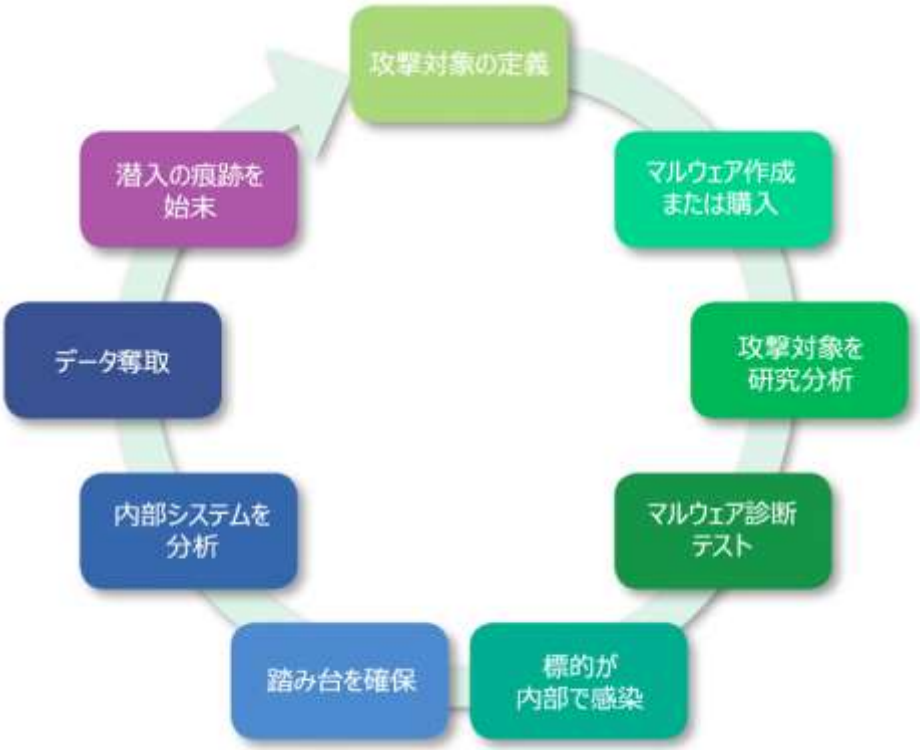
マルウェアはセルフアップデートやセキュリティ製品の無力化など、多数の機能を持つファイルを組み合わせることもある。脆弱性に関しては一般的なソフトウェアの様々な脆弱性やゼロデイ脆弱性を悪用している。

これまでAPT攻撃の主な手法は、電子メールの添付ファイルを利用していた。以前は添付ファイルが実行可能ファイル形式であったが、最近は電子文書の形式に変化しつつある。韓国の場合は無料ソフトウェアの自動更新機能とファイル共有プログラムを悪用するケースが増加している。

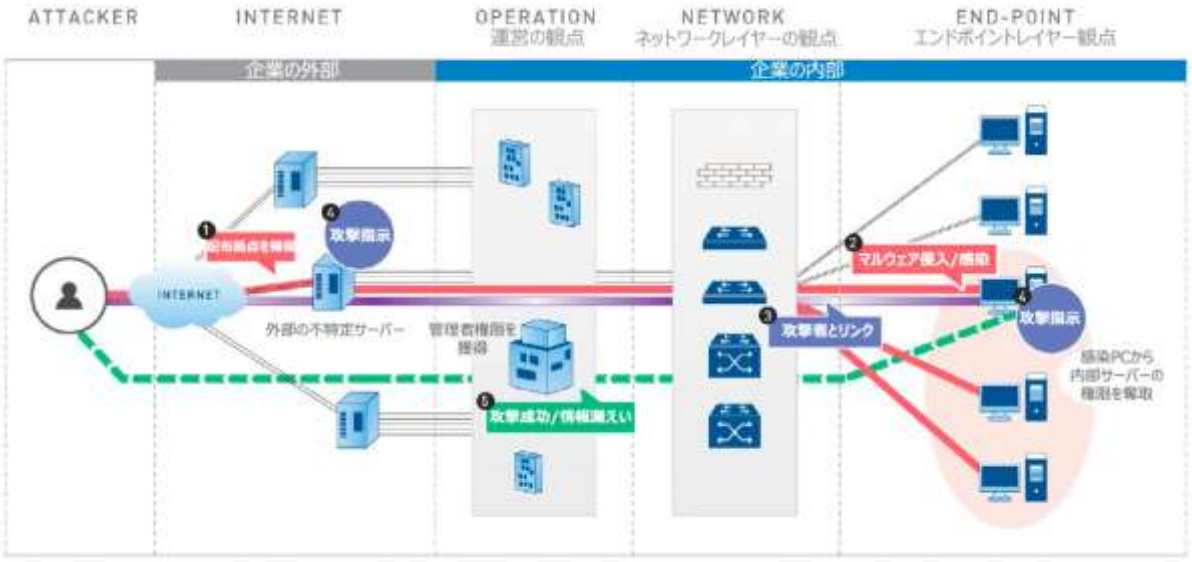
APT 攻撃対応策

攻撃手法

APT攻撃はまず標的を定義することから始まる。標的が決まると、対象に合わせてマルウェアを作成及び購入する。以降は標的について研究しながら内部からの感染を試みると同時に、社会工学的手法を駆使した標的型攻撃が実行される。一旦内部感染に成功すると拠点を確保したも同然で、攻撃者は感染対象を踏み台してC&Cサーバーと接続する。接続後はC&Cサーバーを介してリモートコントロールや攻撃命令を指示することができる。これにより内部データを奪取し、潜入の痕跡を消してから密かに標的から離脱するのである。



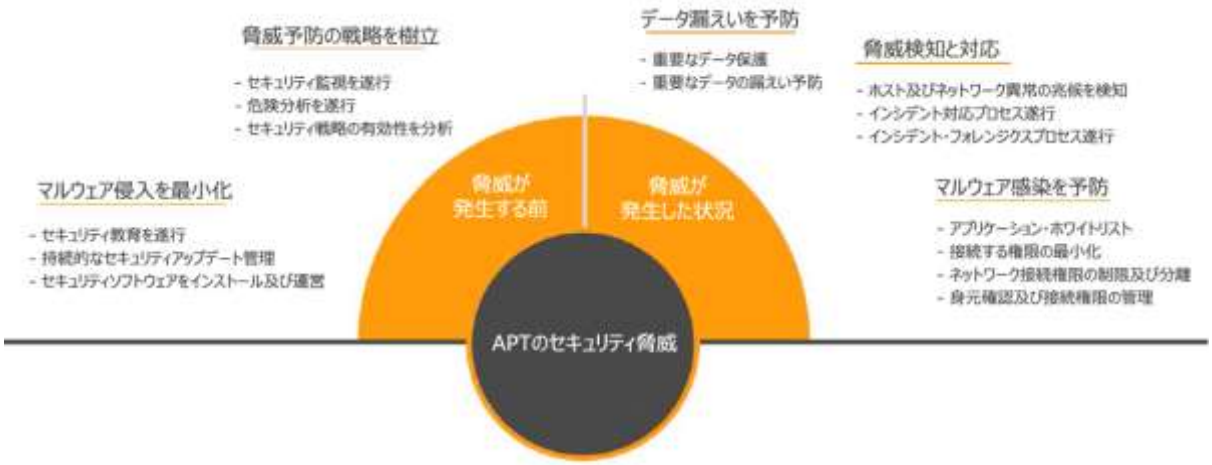
【図6】APT攻撃のライフサイクル



【図7】APT攻撃のタイムライン

APTの総合的な対応策

セキュリティ上の脅威に対応するためには危機管理ベースのセキュリティポリシーを策定することが必要だ。またセキュリティホールを可能な限り縮小し、攻撃を効率的に検知するために深層対応（Defense in Depth）戦略を打ち立て新たな脅威が出現した際、迅速に対応するためセキュリティ・インテリジェンス（Security Intelligence）を確保すべきだ。脅威の発信ポイントは内部の従業員である場合が多いので、定期的なセキュリティ教育も非常に重要といえる。



【図8】 APT攻撃に対応するためのセキュリティ戦略

APT攻撃を事前に予防するためには以下の事項を遵守しなければならない。

<APT攻撃を予防するためのシステム強化>

1. すべてのOSとWebアプリケーション及び関連サーバーは最新バージョンを維持し、セキュリティパッチを適用する。
2. WSUS（Windows Server Update Services）で最新セキュリティパッチをインストールする。
3. すべてのシステムはアンチウイルスソフトウェアをインストールし、ウイルス対策管理サーバーでモニタリングする。
4. すべてのOSから使用しないユーザーアカウントを無効にするか削除する。
5. HSM（Host Security Monitoring）適用後、モニタリングすると共に定期的に分析する。
6. ターミナルサーバーでは共用アカウントを削除し、保存されたアカウント情報とパスワードをすべて削除する。
7. ターミナルサーバーでは業務目的別にアカウントを作成し、ログイン記録を作成・管理する。
8. データベースのxp_cmdshell Procedureを削除し、関連ファイルxplog70.dllを削除する。
9. データベース情報は暗号化して管理し、Webサーバーで暗号化してデータベースに送信する。
10. WebサーバーはSSL（Secure Socket Layer）をアクティブにする。
11. WindowsのイベントログおよびIISのWebログは統合し、ログ管理サーバーで管理する。

<APT攻撃検知のためのネットワーク制御>

1. バックボーンスイッチでは、ホワイトリストとブラックリストを二重ポリシーに設定・管理する。
2. 企業の外部ネットワークから内部にアクセスする際、IPSec VPNまたはSSL VPNを使用する。
3. IPSec VPN、またはSSL VPNに接続するたびに発生するすべてのVPNログを別途管理する。
4. VPNアカウントは業務目的別に作成し、権限も区分して適用する。
5. 企業内部のアウトバウンドパケットに対するフィルタを適用する。
6. 企業内部のHTTP通信は、すべてWebプロキシを通過するように運営・管理する。
7. 企業内ではファイル共有サービスではなく、SFTPまたはSCP（Secure Copy）のみ使用する。
8. NIDS同様のNSM（Network Security Monitoring）をフルタイムで運営・管理する。
9. NIDSイベントおよびセッション全体のデータとパケット全体を保存・分析する。
10. 業務領域別にネットワークを分離し、それぞれの業務領域ごとにファイアウォールをインストールして管理する。
11. システム、ネットワーク及びデータベースなどのIT管理部門は、一般的な業務領域と別途区分する。

http://www.ahnlab.co.jp

http://global.ahnlab.com

http://www.ahnlab.com

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

〒101-002 東京都千代田区外神田4-14-1 秋葉原ＵＤＸ ８階北 | Tel：03-5209-8610 (代)