アンカーテクノロジーズ株式会社
Anchor Technologies, Inc.

〒150-0002
東京都渋谷区渋谷2丁目19番15号 宮益坂ビルディング
https://anchor-u.com

Anchor
Technologies

アンカーテクノロジーズ株式会社 Anchor Technologies, Inc.

会社概要
OUTLINE

IT関連製品・サービスを幅広く提供

セキュリティ強化・データ分析等をサポートする
IT関連製品・サービスを国内最安水準で、幅広く提供します。

1
製品販売事業
◇セキュリティ
◇データ復旧
◇データ分析

2
セキュリティ関連
教育事業

3
セキュリティ診断
・調査事業

4
コンサルティング
事業

5
システム開発事業

当社の特徴

国内最安水準

広告宣伝やプリセールス、各種固定資産等にかかるコストのために、メーカーが設定する希望価格をはるかに上回る価格が多くなっています。

当社では、各種コストを最大限スリム化することによって国内最安水準の価格を実現しています。

選べる各種特典

お取引の際、毎回１％のお値引きを適用、又はご購入額の１％相当をギフト券でご担当者の方に進呈します。

さらに、別組織様をご紹介いただいた場合は、紹介した方、紹介された方の双方に1％のギフト券を進呈します。

豊富なラインナップ

当社では、世界中で高いシェアを誇るメジャーな製品から、逆にまだあまり認知されていないマイナーな製品まで、幅広く販売できるよう、日々取り扱いを拡充しています。

新たに製品の取り扱いをご提案いただいた方には、特典の付与がございます。

Anchor Technologies

会社名	アンカーテクノロジーズ株式会社（Anchor Technologies, Inc.）
代表取締役	阿部　里美
本社	〒150-0002 東京都渋谷区渋谷2丁目19番15号 宮益坂ビルディング TEL (03)6897-6281(代) E-Mail: sales.tech.gu@anchor-u.com URL: https://anchor-u.com/
事業内容	1.製品販売事業（セキュリティ・データ復旧・データ分析） 2.セキュリティ関連教育事業 3.セキュリティ診断・調査事業 4.コンサルティング事業 5.システム開発事業
加盟団体等	デジタル・フォレンジック研究会（IDF） 一般社団法人ソフトウェア協会（SAJ） 日本カード情報セキュリティ協議会（JCDSC）

事業内容
BUSINESS

Product 製品販売事業

セキュリティ

データ復旧

データ分析

リバースエンジニアリング

IDA Pro
フラッグシップライセンスのIDA Proに代表されるIDAシリーズ（IDA Pro、IDA Home、IDA Teams）と各種Decompiler（x86、x64、ARM、PowerPC他）は、長年逆アセンブル&デバッガソフトとして多くの解析者に愛用されています。マルウェア解析や自社開発製品の耐タンパ性試験等のために活用されます。

Binary Ninja
逆アセンブラ、デコンパイラ、デバッガーとしての機能を持つ、非常にコストパフォーマンスに優れたバイナリ解析ソフトです。Windows版、Mac版、Linux版それぞれ別々に購入する必要がなく、いずれのOS上でも動作します。デコンパイラも別途オプション購入不要で、標準で利用可能です。

JEB
逆アセンブル、デコンパイル、デバッグ等の機能を有するリバースエンジニアリングソフトです。特にデコンパイル機能が充実しており、Dalvik、Java、x86、x64、ARM、ARM64、MIPS、MIPS64、RISC-V、S7 PLC Block、WebAssembly、Ethereum 等、多種に対応します。難読化されたAPKのデコンパイルも可能です。

脆弱性診断・侵入テスト

insightVM
組織内のIT資産の脆弱性を継続的に監視するためのソリューションです。対象のIT資産と最新の脆弱性情報とを突合させて、各々のリスクを数値化し、対応を優先度付けします。クライアント端末のほか、NW機器、IoTデバイス等に加えて、AWS、Azure、GCPといったIaaSのセキュリティチェックも可能です。

metasploit Pro
ペンテストツールとして長年多くの組織に利用されてきたOSS、metasploit frameworkの高機能商用版です。NW機器、サーバー、仮想マシン、OS、Webアプリ等に対するペンテストが可能です。GUIによる操作が可能で、簡単にご利用いただけます。Android、組込Linux、IoTの検証にも対応します。

Burp Suite
Webアプリケーションのセキュリティテストを行うための統合プラットフォームです。無償版のCommunity Edition、リリース後の精緻な手動テストをサポートするProfessional Edition、対象を継続的に自動的に診断しSecDevOpsをサポートするEnterprise Editionの3種類のプランがあります。

AppScan
Web アプリケーションおよびモバイルアプリケーションの脆弱性の診断・検出を行う、脆弱性診断ツールです。動的解析機能を有するAppScan Standard、静的解析機能を有するAppScan Source、組織的な診断を支援するAppScan Enterprise、SaaSモデルのAppScan on Cloud、合計4種類のご用意があります。

Vex
純国産のWebアプリケーション脆弱性検査ツールです。導入～運用までのサポート体制が整っており、レポート作成機能をはじめ日本語サポートが充実しています。Webサイト特性や利用者のスキルに合わせて、自動巡回機能、手動巡回機能、画面遷移図ベースでわかりやすいシナリオマップ機能の3つを使い分けて診断を行うことが可能です。

Cobalt Strike
攻撃者によるネットワーク内の行動を再現して対策に活かすために用いられる、ペネトレーションテスト用のツールキットで、特にシステム侵入後の情報窃取や横展開のための各種機能を提供します。対象マシンにBeaconを配置し、C2通信、各種コマンド実行、キーロギング、特権昇格等、多くのことを実行可能です。

フォレンジック

Passware
Passware Kit Forensicは、これまで多くの利用実績を持つプロ仕様のパスワード解析ソフトです。フルディスク暗号（Bitlocker等）、アプリケーションファイル（Officeソフト、PDF等）をはじめとする各種パスワードを解析します。また、Passware Kit Mobileでは、iPhoneやAndroidのパスコードを解析します

Elcomsoft
GPUによる解析高速化、複数マシンによる分散処理（クラウドコンピューティングにも対応）等が可能なパスワード解析ソフトDesktop Bundle、スマホ・タブレットのデータ取得、バックアップPWの解析、暗号化バックアップの復号等が可能なMobile Bundle、そしてそれら機能をすべて持つPremium Bundleのご用意があります。

Blade
フォレンジックイメージ、物理/論理ディスク、携帯電話、バイナリダンプ等といったデータソースから、データカービングにより削除ファイルを復元します。Intelli-Carveという独自技術を使用した高度なデータ復元エンジンを搭載し、特殊なファイル形式のものも含め、高速かつ正確に復元します。

NetAnalysis
ウェブブラウザの証拠データ抽出・分析のための専用フォレンジックツールで、多種多様なウェブブラウザに対応しています。NetAnalysisに付帯するHstExは、削除されたブラウザ履歴やキャッシュデータを復元します。Windows、macOS、Linux、Android、iOSの各種ブラウザに対応しています。

Arsenal Recon
次の解析用ソフトを含む、フォレンジックのためのパッケージソフト群です。ハイバネーションファイル解析、レジストリ解析等の各領域において、他ソリューション以上の解析能力を有します。Arsenal Image Mounter/Hibernation Recon/Registry Recon/ HBIN Recon/Hive Recon/ODC Recon

OSForensics
データ保全、ハッシュ値検証、インデックス検索等の基本的な機能から、各種ファイルやBitlocker等のパスワード解析、ディスクイメージのマウント、VSS解析、RAID再構築等の機能も有する、コストパフォーマンスに長けた統合型フォレンジックソフトです。年間ライセンスと買い切りライセンスの両方のご用意があります。

F-Response
ネットワーク上のPC（Windows、Linux、Apple OSXに対応）やクラウドサービス（Azure、AWS、Gsuite、Onedrive等に対応）にエージェントレスかつ読み取り専用でアクセスしてデータを収集することができる、リモートフォレンジックツールです。同時接続数などによらない価格体系で、コストパフォーマンスに長けています。

OSINT

Maltego
調査対象のIPやDNS名等をもとにインターネット上の各種データ群を収集し、それらの相関を1つのUIでグラフィカルに表示します。ユーザーが別途契約する商用サービスで提供されるデータや、組織内のログ等を取り込むことも可能です。これにより、犯罪行為、サイバー攻撃等の全容解明を手助けします。

VirusTotal Enterprise
マルウェア検査等を行うVirusTotalの有償版。VT Intelligence、VT Graph、VT Hunting、VT APIといったプレミアムサービスが提供されます。VT Intelligenceは、各種データ（ファイル、ドメイン、URL、IP等）に対する高度な検索エンジンで、脅威に関する詳細情報が得られます。

GreyNoise
セキュリティチームが脅威を適切に特定し、優先順位をつけ、ブロックすることを支援するCTIソリューションです。特定の脆弱性やCVEを狙ったトレンドの攻撃を特定することを支援します。また、SIEMやSOAR等と連携して使用することで、誤ったアラートの削減や、アラートへの迅速な対応が可能になります。

その他

SCADAfence
インダストリアルIoT/OTネットワークにおける資産の可視化・管理のためのプラットフォームです。独自の通信プロトコル内部の解析技術により、マルウェア侵入、不正操作、誤操作等を検知します。IEC62443やNIST CSFといったセキュリティ基準への適合状況を評価することも可能です。

Chronicle Security Operations
統合ログ管理のためのChronicle SIEM、セキュリティ自動化対応のためのChronicle SOAR、脅威情報の収集・分析のためのThreat Intelligenceの3つで構成される最新のクラウドネイティブ スイートです。Googleならではの速度、スケール、インテリジェンスを活用してサイバー脅威の検出・調査・対応を行うことが可能です。

Service サービス

セキュリティ関連教育

- SANS、CISSP CBKトレーニング、セキュアEggs、EC-Council、インシデント対応トレーニング、フォレンジックトレーニング、脆弱性診断トレーニング、ペネトレーションテストトレーニング、および各種ツールトレーニングを提供しております。

コンサルティング

- セキュリティ組織構築・強化支援、セキュリティ水準成熟度評価、法規制・ガイドライン準拠支援、セキュリティ関連規程類の策定・改定支援、BPR（ビジネスプロセス・リエンジニアリング）支援等のコンサルティングサービスを提供しております。

セキュリティ診断・調査

脆弱性診断・侵入テスト

Web アプリケーション・スマホアプリ・サーバ・ネットワークといった資産を対象とした脆弱性診断に加えて、組織を対象にした脅威ベースのペネトレーションテスト（TLPT）を実施しております。

フォレンジック調査

スマートフォン・PC・クラウドサービスを対象にしたフォレンジック調査サービスを提供しております。ランサムウェア等のマルウェア感染、不正アクセス、職員による内部不正等の調査に対応します。

システム開発

- SFA・CRM・RPA等の各種業務システムの開発・導入支援、iOS・Android向けアプリの開発、クラウド環境設計等を受託しております。