ONLY

HUMANS

CAN

COUNTER

HUMAN-DRIVEN

THREATS.

https://www.cyberdefense.jp

CyberDefense

人間がもたらす脅威には、人間しか対処できない

サイバースペースの脅威がどのように変化しようとも、
サイバーディフェンス研究所には、それに対処できる人材がそろっています。
様々な分野で突出した専門性と高い倫理観を持つ最高のチームが
高品質な技術サービスで社会に貢献します。

サイバーディフェンスの強み

1 使命を持つ

サイバー空間の安全を守るという使命のもと、強烈な強みをもったサイバーセキュリティの専門家が結集したチーム、それがサイバーディフェンスです。サイバーディフェンスでは、全員が高い倫理観と強い社会貢献意識を持ち、サイバースペースの脅威に最前線で向き合っています。

2 攻撃に卓越する

高度な攻撃能力を持つ攻撃者。彼らによってもたらされる今日の脅威に立ち向かうためには、彼らと同様の視点と発想、彼らを上回る知識とスキルが必要です。真の攻撃を知るサイバーディフェンスなら、真の防御を実現できます。

3 攻撃者を逃がさない

サイバーディフェンスは、国内屈指のフォレンジック技術で攻撃に遭った組織におけるインシデントの原因究明、被害の極小化、攻撃者の封じ込めを強力に支援します。攻撃を 100% 防ぐことは不可能ですが、攻撃者の思い通りにはさせません。

4 サイバーセキュリティの未来を創造する

サイバーディフェンスのエンジニアは、現状のセキュリティ技術の常識や限界を疑い、より良い手法、斬新なアプローチが存在するという前提で課題に立ち向かいます。弛まぬスキルの研鑽と技術研究により、常識では不可能と考えられていることを可能にし、既製のツールやプロダクトの限界を超え、サイバーセキュリティの未来を切り拓きます。

5 お客様の期待を超越する

サイバーディフェンスは、常に中立的な立場で、お客様の課題と真摯に向き合い、高度な技術、ユニークな発想、アグレッシブなアプローチ、圧倒的なスピードと質の高いサービスで、お客様の期待を超越します。

サービス領域

セキュリティ診断
Penetration Test

フォレンジック調査
Forensics

トレーニング
Traning

事例紹介

国際機関から国内大手、ベンチャー企業まで
幅広くサイバーセキュリティのサポートをおこなっています。

INTERPOL
（国際刑事警察機構）

東南アジア地域におけるクリプトジャッキングへの対処を目的とした活動「Operation Goldfish Alpha」に貢献

INTERPOL
（国際刑事警察機構）

サイバー犯罪捜査演習に協力
ミッションの攻略を通じて、フォレンジック技術とサイバー犯罪捜査能力の向上に貢献

NEDO
（国立研究開発法人新エネルギー・
産業技術総合開発機構）

自動走行システム / 大規模実証実験へ参画
日米共同スマートグリッド実証事業へ参画

セキュリティ診断

脆弱性診断・ペネトレーションテスト

Penetration Test

エンジニアが思考する戦略的な擬似ハッキング

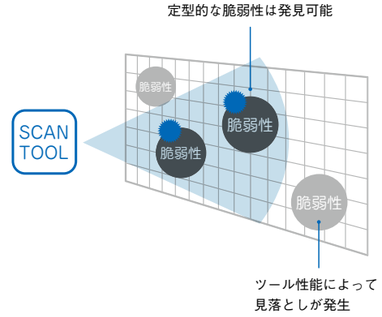
サイバーディフェンス研究所のセキュリティ診断（脆弱性診断・ペネトレーションテスト）は、高度な技術、豊富な経験、非凡な攻撃センスを併せ持つ一流のセキュリティエンジニアが実施します。

Web アプリケーションやネットワークはもちろん、組み込みデバイス、制御システム など様々なシステムを対象に、自動化されたツールに依存することなく、ハッカーの思考にもとづく戦略的なハッキングを行います。
スキャンツール主体の診断や、一般的なマニュアル診断とは一線を画する独自のアプローチにより、脆弱性の検出のみならず、企業経営、組織運営に潜在する真の脅威を明らかにし、診断対象となるシステムの安全な運用に貢献します。

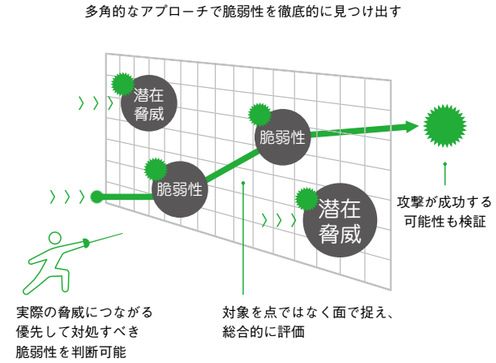
一般的なセキュリティ診断との比較

攻撃に卓越した人間が試行錯誤しながら診断し、脆弱性の組み合わせにより発現する潜在脅威も発見

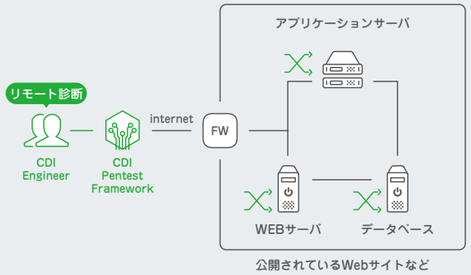
一般的なツールベースの脆弱性診断



サイバーディフェンス研究所の診断

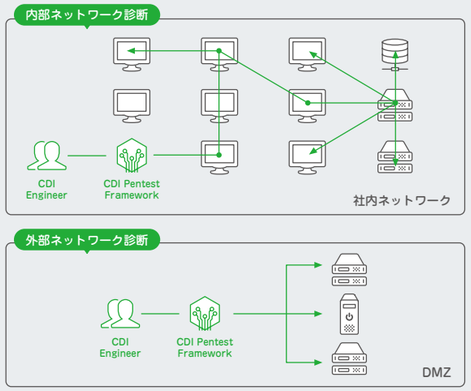


Webアプリケーション診断



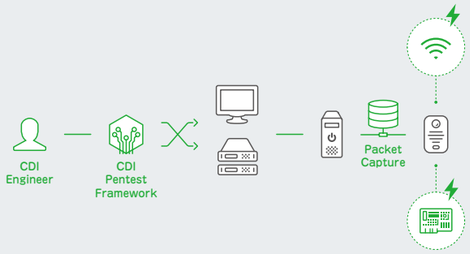
攻撃者と同様の思考、手法にもとづくペネトレーションテストにより、Web アプリケーションに潜む脆弱性と現実に起こり得る脅威を顕在化させます。
診断対象の特性を考慮し、様々な攻撃を戦略的に施行することにより、一般的な脆弱性診断サービスや Web アプリケーション脆弱性スキャナでは発見できない脆弱性までも徹底的に洗い出します。単なる脆弱性の検出にとどまらず、攻撃の成否、さらには、複数の脆弱性の組み合わせによる脅威の発現も検証します。

ネットワーク診断



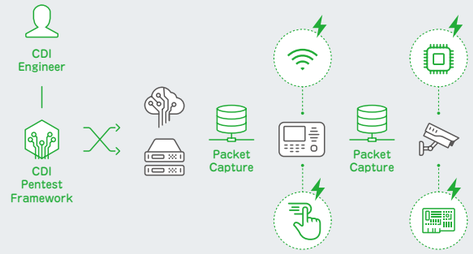
当社のネットワーク診断は、本物の攻撃に限りなく近い、実戦的なペネトレーションテストです。実際の攻撃と同様にネットワークを侵入対象とみなし、情報収集と侵入のプロセスを循環的に実行することで、ホスト単体のみならずネットワークの深層まで侵入し、対象ネットワークに潜む真の脅威を明らかにします。
独自のフレームワークが実現する高速な探索、検出した問題の自動蓄積、情報の一元管理により、複数名による攻撃試行のパフォーマンスを最大化。数千ホストを超える大規模環境が対象でも、圧倒的なスピードで攻略します。

組み込み機器診断



近年急速に普及する IoT で注目の高まる組み込み機器のセキュリティ。機器の構成要素や機能仕様、運用設計を踏まえて攻撃観点を洗い出し、基板、シリアルコンソール、IC 単体、機器間通信、無線通信、Web インターフェース、ファームウェア解析など、物理層からアプリケーション層までの全てを対象とした擬似攻撃を行います。
規格書の調査や同等部品の調達から始め、電波暗室やリワークマシン等の各種専門設備を用いて実施する当社の診断は、あらゆる組み込み機器に対し、他に類をみない深く専門的なレベルでセキュリティ上の問題点を検証できます。

制御システムペネトレーションテスト



従来、その外部隔離性ゆえに、安全かつセキュアな環境と考えられていた制御システムにおいてもオープン化が進むことで、サイバー攻撃による被害報告が増加しています。
当社では、限られたテスト期間内に最大の成果をあげるべく、試験実施前に各種規格・ドキュメントの読み込みや情報収集を行い、脅威を分析した上で、最適な試験実施計画を策定します。その上で、制御システムにおいて最も重要な可用性を考慮しながら、制御システム特有の独自プログラムに対してもバイナリ解析や通信の可視化、実証ツールの開発を含む、より実戦的なテストを実施します。

フォレンジック調査

インシデント対応サービス

Forensics

セキュリティインシデントの原因と被害範囲を徹底究明

セキュリティインシデントの発生時に、初動対応の支援から本格的な調査、復旧支援と再発防止策のアドバイスまでを、ワンストップで支援します。
複雑化するサイバー攻撃の原因と被害範囲の究明には、経験豊富なフォレンジックエンジニアが必要不可欠です。当社のインシデント対応サービスは、サイバー犯罪捜査官を始めとした法執行機関の専門家へのトレーニング実績を持つフォレンジックのエキスパートが対応します。
さらに、マルウェア解析のエキスパート、攻撃者の視点、思考に精通したペネトレーションテスターなど、当社の能力を結集してインシデントの実態解明に臨みます。

ネットワーク全体の様々なエビデンスを統合的に解析

インシデント対応として、ログやマルウェアなどを個別に解析するだけでは、事象全体の把握が困難であり、結果として対応や判断を誤ってしまう可能性があります。
当社は、可能な限り正確に発生事象を把握すべく、調査すべきコンピュータやログ、マルウェアなど複数の情報を総合的に解析し、それらを時系列に分析することで攻撃の全容把握に努めます。

クライアントPC、サーバの調査

ディスクやメモリに残る不正ファイルやプログラム実行履歴などの痕跡から、攻撃手法や情報窃取の有無等を調査します。

ログ調査

ファイアウォールやプロキシサーバなどのログを調査します。クライアント PC やサーバの調査で判明した事項との相関分析も行います。

マルウェア解析

お客様が収集したマルウェアや、当社調査の過程で発見したマルウェアを対象に、動的解析または静的解析を実施します。

パケット解析

ネットワークパケットのデータを解析し、攻撃者がネットワーク侵入後にどのような活動を行ったかなどの分析を行います。

調査のアプローチ

フルフォレンジック

ディスク、メモリ、ログ、マルウェアなど、あらゆるエビデンスを総合的に解析します。情報の窃取や侵入が確実視されるケースにおいて、原因や被害範囲を究明します。

ファストフォレンジック

侵害が広範囲なインシデントに対する初動調査として推奨する方針です。限られた時間と予算の範囲で、多くのホストを調査し、被害概要を把握することを重視します。

脅威ハンティング

「既に侵入されている」前提で、より広範囲を能動的に調査します。
ネットワーク全体から攻撃の痕跡や進行中の攻撃を抽出し、攻撃を点ではなく面と捉えた分析や詳細調査範囲の絞込みを行います。

サービスフロー

まずはヒアリングさせていただき、想定される侵害内容や調査に着手するタイミング、期間や予算などに応じて、適切なフォレンジック調査方針をご提案します。

お問い合わせについて

インシデントが発生、もしくは、発生が疑われる場合など、お困りの際はすぐご連絡ください。事前契約不要で受付いたします。
インシデント対応における迅速な検討開始および調査着手は、事態の早期収拾に向けて極めて重要です。お気軽にお問い合わせください。
また、有事に備えた事前のご説明や秘密保持契約も承ります。

1. **ヒアリング・アドバイス**
   メールや電話によるヒアリングを行い、初動対応へのアドバイスを実施
2. **ご提案**
   目的に応じた調査範囲や項目を定義し、概算費用をご案内
3. **データ保全・授受**
   解析対象とするデータの保全と授受
4. **調査・解析**
   インシデント発生の原因や被害範囲、攻撃手法を調査
5. **報告書提出・報告会実施**
   調査結果報告書にもとづき報告会を実施
6. **対策支援**
   復旧支援や再発防止を目的とした対策の提案、助言、経過観察の支援

対応事例

- 標的型攻撃
- 外部からの侵入、情報漏洩
- マルウェア感染
- 不正な通信、アクセスの検知
- Web サイトの改竄
- 大量に発生した不審メールの送受信
- クラウド環境やスマートフォンで発生したインシデント
- 数千台を超える大規模環境で発生したインシデント

ツール　CDIRインシデント対応支援ツール

CDIR は、当社が独自に開発した、オープンソースのインシデント初動対応支援ツールです。自組織のインシデント対応にご活用ください。

CDIR-C データ収集用ツール

CDIR-C（Collector）は、調査対象端末の汚染や業務への影響を最小限に抑えながら安全にデータを収集するツールです。ファイルを実行するだけの簡単な操作で、事象把握に有用な情報を保全します。

CDIR-A データ解析用ツール

CDIR-A（Analyzer）は、CDIR-C で収集したデータを解析するツールです。インシデントの影響範囲と被害内容を迅速に把握することが出来ます。

トレーニング

セキュリティエキスパートの育成を目的とした実践的なトレーニング

護る力をその手に

サイバーディフェンス研究所は、ハッキング、フォレンジック、マルウェア解析などの教育サービスを提供しています。
トレーニングカリキュラムは、当社が実施するインシデントレスポンスや侵入テストのノウハウにもとづく実戦的な内容です。セキュリティエキスパートを目指す方から、高度な技術を習得したい方、サイバー犯罪捜査官など、様々な人材育成のニーズに応えます。

サイバー演習

ハッキング

セキュリティ診断

セキュア
コーディング

フォレンジック・
インシデント
レスポンス

マルウェア・
プログラム解析

Exploit Writing

プライベート・
カスタマイズ

受講モデル

アレンジご相談ください

教育の目的、現状のスキルレベル、目指すべきレベルなどを考慮し複数のコースを適切な順序で受講することで、効率的なスキルアップが可能となります。
CSIRT 要員のスキルアップ、サイバー犯罪捜査官の育成、セキュアな開発、運用を行うことのできるエンジニアの育成など目的に応じてトレーニングコースをアレンジします。

プライベートコース承ります

すべてのコースでプライベートトレーニングを承ります。自組織が体験したインシデントや実業務での課題などの質問をオープンに行うことが可能となり、より高い教養効果を期待できます。また、不特定多数の組織からの参加者との同時受講が望ましくないという場合もご相談ください。

お客様の指定する場所、会議室やセミナールームなどを使用したトレーニング開催も可能です。PC 含むトレーニング環境は、全て当社が用意いたします。

Traning

ハッキング

攻撃者の視点、思考を学ぶハンズオントレーニングです。
Web アプリケーションやネットワーク、ハードウェアに対して実際の攻撃を体験することによって、攻撃の仕組みを深く理解します。
ハードウェアを対象にしたコースでは、技術仕様に関する情報収集から、ロジック・アナライザ等を用いた通信の盗聴・解析、ファームウェアのダンプ、取得したファームウェアの解析まで、一連の技術習得を目的としており、チップオフやはんだ付けなども体験することができます。
セキュリティ管理者から、アプリケーションや組み込み機器、制御システムの開発に関与する技術者、法執行機関のフォレンジック担当者にとって有用な知識と実戦的な技術の獲得が可能です。

フォレンジック

インシデント対応やサイバー犯罪捜査に必要な技術を学ぶトレーニングコースです。一部のコースは法執行機関限定となります。
セキュリティインシデントやサイバー犯罪の初動対応から、様々な犯罪捜査のシーンを想定したハンズオンミッション、フォレンジック調査やマルウェア解析を少ないリソースでスピーディに行うために必要なサイバーインテリジェンスの活用まで、ハンズオンを通じて、より実戦的で効率的な調査・分析の手法を学ぶことができます。
コンテンツの企画・制作には、法執行機関で勤務経験のあるフォレンジックエンジニアが関与しており、警察をはじめ、全ての法執行機関のフォレンジック担当者の技術力向上に寄与します。

ピックアップカテゴリ

最前線で戦う現役エンジニアによる実戦的なトレーニング

Exploit Writing

実戦的な Exploit 技法を学ぶための上級コースです。セキュリティプロフェッショナルを対象に、効果的な脆弱性の発見や攻撃コードの作成に必要となる知識と技術を学びます。
Binary Exploitation Fundamentals では、メモリ破壊の脆弱性を利用したリモートからのシェル起動という一連のプロセスを通じ、攻撃者視点で Binary Exploitation の考え方に触れて頂きます。
脆弱性攻撃の古典的なシナリオの把握から、総合演習では様々な手法や考え方を組み合わせたフルスクラッチでの Exploit 開発を体験することができます。

マルウェア・プログラム解析

実際のサイバー攻撃に使用された検体などを題材として、実戦的なマルウェア解析技術を習得するためのコースです。
マルウェア感染が疑われるインシデントが発生した際の対処方法や、モニタツールによる動的解析では解析できないような、マルウェアが潜在的に有する機能や通信プロトコルを解析する際に必要となるリバースエンジニアリング技術について学ぶことで、実戦的なマルウェア解析技術を習得することを目的とします。

計画的にセキュリティ技術者を育成しようとする組織にとって、数日から数ヶ月の学習や業務体験が、必ずしも実務能力の獲得に至らないことが課題となっています。サイバーディフェンス研究所は、ある日突然セキュリティ業務に放り込まれた方から、既に高度なスキルを身につけられた方まで、幅広い層のセキュリティ業務の従事者が、楽しみながら必要な知識やテクニックを獲得・維持できる、継続的な自学自習の仕組みを作り、組織の能力向上に寄り添います。

研究開発

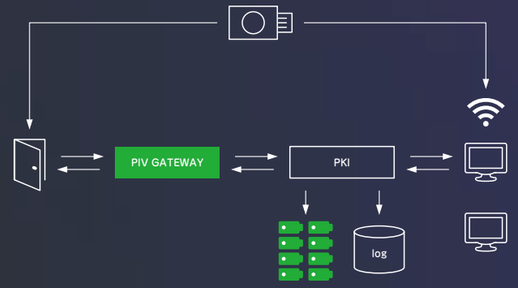
サイバー空間の安全を守る、その使命感にもとづき、私たちは既存のサービスに固執せず、
自由な研究開発に取り組んでいます。
様々な領域のプロフェッショナル達が集うサイバーディフェンス研究所では、
一見すると実現困難な新しいアイデアであっても、驚異的なスピードで具現化してしまいます。

MONSTRO

エージェントレスの大規模環境向け調査用プラットフォームです。
数千を超えるホストから収集したアーティファクトに、高速処理かつ自動解析を施し、Web ブラウザでの深堀調査を可能にします。インシデントレスポンスの効率化や、スレットハンティングでの活用が見込まれます。

PIV GATEWAY

サイバー空間だけでなくフィジカル空間も含めたアクセスコントロールの仕組みです。IT における認証・認可やアカウント管理に加え、ドアの入退制御による物理的なゾーニングまで、一元的な管理を可能にします。NIST や FIPS 等の各種規格に準拠します。



MAGURO

現役のトップクラス CTF プレイヤーが運営するオンライン CTF サイトです。組織の人材育成を支援します。自組織に密かに存在するセキュリティエンジニアを発掘できるかもしれません。

CyberDefense

社名	株式会社サイバーディフェンス研究所
所在地	〒101-0062　東京都千代田区神田駿河台2-5-1 御茶ノ水ファーストビル5 階
資本金	100,000,000 円
加盟団体	特定非営利活動法人デジタル・フォレンジック研究会 Nippon CSIRT Association（NCA） Forum of Incident Response and Security Teams（FIRST） 等
認証	ISMS（ISO/IEC27001）

TEL
03-5843-9015（代表）

E-MAIL
sales@cyberdefense.jp

公式 Twitter
https://twitter.com/cyberdefense_jp

ハッキング Blog
https://io.cyberdefense.jp