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
Training

事例紹介

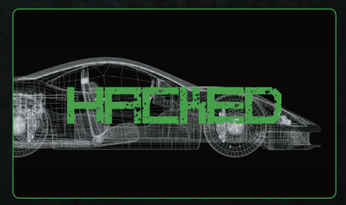
国際機関から国内大手、ベンチャー企業まで
幅広くサイバーセキュリティのサポートをおこなっています。

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

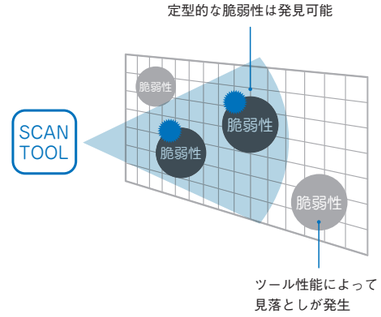
サイバーディフェンス研究所のセキュリティ診断（脆弱性診断・ペネトレーションテスト）は、高度な技術、豊富な経験、非凡な攻撃センスを併せ持つ一流のセキュリティエンジニアが実施します。

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。

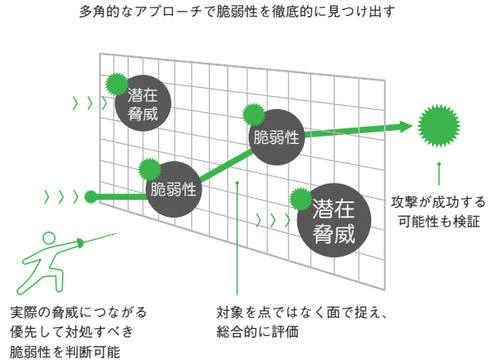
一般的なセキュリティ診断との比較

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

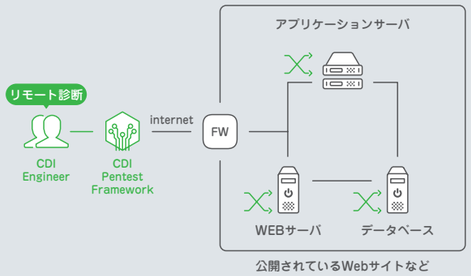
一般的なツールベースの脆弱性診断



サイバーディフェンス研究所の診断

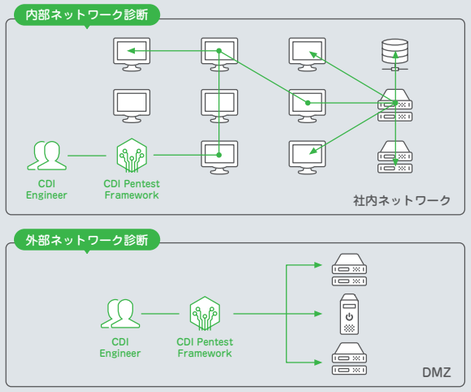


Webアプリケーション診断



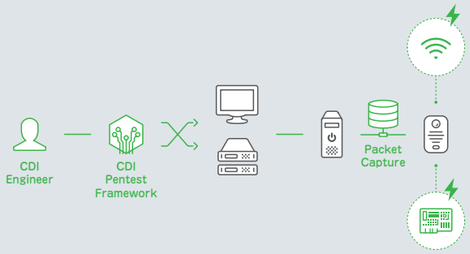
攻撃者と同様の思考、手法にもとづくペネトレーションテストにより、Web アプリケーションに潜む脆弱性と現実に起こり得る脅威を顕在化させます。
診断対象の特性を考慮し、様々な攻撃を戦略的に施行することにより、一般的な脆弱性診断サービスや Web アプリケーション脆弱性スキャナでは発見できない脆弱性までも徹底的に洗い出します。単なる脆弱性の検出にとどまらず、攻撃の成否、さらには、複数の脆弱性の組み合わせによる脅威の発現も検証します。

ネットワーク診断



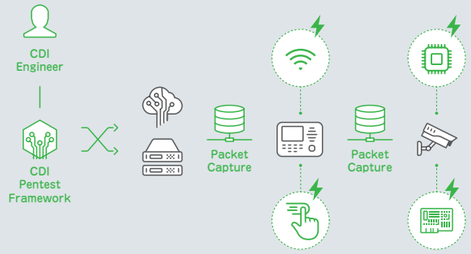
当社のネットワーク診断は、本物の攻撃に限りなく近い、実戦的なペネトレーションテストです。実際の攻撃と同様にネットワークを侵入対象とみなし、情報収集と侵入のプロセスを循環的に実行することで、ホスト単体のみならずネットワークの深層まで侵入し、対象ネットワークに潜む真の脅威を明らかにします。
独自のフレームワークが実現する高速な探索、検出した問題の自動蓄積、情報の一元管理により、複数名による攻撃試行のパフォーマンスを最大化。数千ホストを超える大規模環境が対象でも、圧倒的なスピードで攻略します。

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

Training

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。

受講モデル

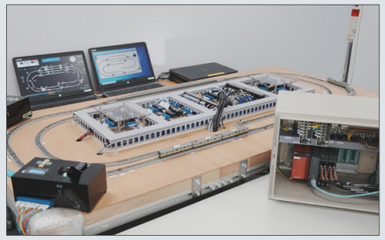
アレンジにも対応いたします

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。



【制御システムハッキングトレーニング】

仮想環境上に用意したトレーニング環境を用いて、独自プロトコルの解析や中間者攻撃による通信の盗聴と攻撃用パケットの生成と送信などの一連の流れをハンズオンで学習できるほか、模擬制御システムを用いた不正制御、監視値の改ざんなどを体験できるトレーニングコースです。
制御システムを対象とした攻撃者の思考にも踏み込むことで、より実践的な攻撃手法の洞察が可能になります。

Threat Intelligence

脅威リサーチ / コンサルティング

サイバーインテリジェンス活用の基盤構築を支援

脅威インテリジェンスツールの活用と導入をワンストップで支援

サイバーディフェンス研究所は、民間企業、重要インフラ事業者、各種政府機関、国際イベントのセキュリティチームなどを対象に、脅威インテリジェンスの活用を支援した実績を有します。

組織の目的および業務の内容を踏まえたサービスの選定、機能検証、連携のためのシステムの構築や機能拡張ツールの開発、チームへのトレーニング、高度な技術サービスの提供までをワンストップで支援することができます。

取扱製品例

Recorded Future®

サーフェスウェブやダークウェブなど 90 万以上の情報ソースをリアルタイムに収集・統合・分析できるインテリジェンスプラットフォーム。
特許取得済みの機械学習と自然言語処理及び AI を活用し、膨大な情報ソースの中から組織に関連する最新の脅威を可視化できるため適切で迅速なセキュリティオペレーションが実現可能。

VirusTotal

ファイルやウェブサイトが悪性であるか否かを検査することができるサービス。 有償版のサービスを利用することで、VirusTotal へアップロードされたファイルを 100 種類以上の検索演算子を緻密に検索、ダウンロードすることが可能となるほか、YARA ルールによるマルウェアのハンティング、IP やドメインに関連する悪意ある行為を過去に遡って分析することなどが可能。

オンデマンドリサーチサービス

安全保障上の脅威となるような人物、犯罪者、ハクティビスト、サイバー攻撃グループなどのアクティビティの把握、アトリビ ューションを目的とした情報収集・分析を代行いたします。
調査テーマに応じて、サイバーディフェンス研究所の OSINT アナリスト、リサーチャー、マルウェア解析者、フォレンジック アナリスト、ハッカーによるチームを構成し、テーラーメードの調査プランを検討・実行します。
主に、法執行機関、情報機関、防衛組織における情報分析活動を支援することを目的としたサービスです。

VirusTotalを活用したサイバー攻撃の動向分析基盤

THREAT LANDSCAPER

Threat Landscaper は、Virus Total と連携して機能する脅威分析ソリューションです。 Threat Landscaper を活用することで、日本で流行しているマルウェア、よく利用される脆弱性、TTPs の把握や、国家に帰属するアクターやランサムウェアグループに代表されるサイバー犯罪グループなど、様々な脅威アクターのアクティビティを継続的に追跡することが可能となり、防衛組織や法執行機関のリサーチチームや民間組織における脅威分析のパフォーマンスを向上させます。

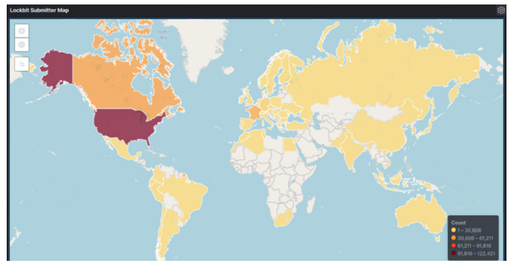
提供機能

J2 TRACKER

- VirusTotal に日本から投稿されたファイルの統計データを分析する
- ファイル形式の内訳や流行りのファミリ、よく使われる脆弱性、TTPs などを可視化し、日本の現状の脅威動向を把握する

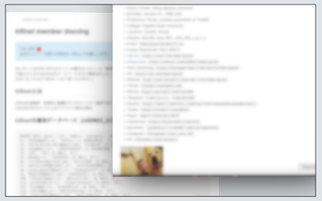
ACTOR TRACKER

- 指定したアクターやファミリの動向を追跡する
- 全世界から VirusTotal に投稿されたファイルを、アンチウイルスソフトの検知や Yara ルールによって精査する
- 対象のアクター
  - 中北露の APT グループ
  - ランサムウェアグループ



事例紹介

Killnetメンバーに関する調査



親ロシアのハッカーからなるハクティビスト集団「Killnet」のメンバーを特定した。

5th INTERPOL Digital Security Challenge

現実に活動中のランサムグループを中心とした違法サイトとその運営者・協力者を特定した。

その他活動実績

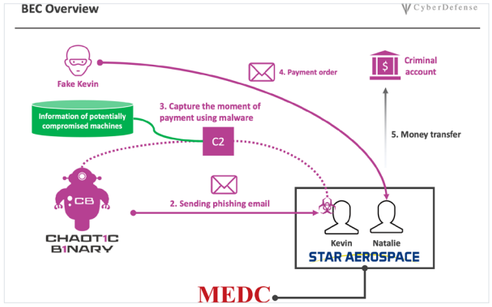
コンサルティングによる課題解決の支援や最新技術の研究

サイバー犯罪捜査演習「Digital Security Challenge」

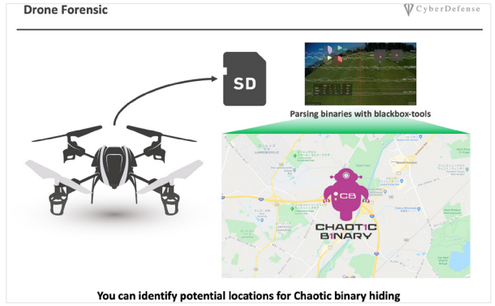
サイバーディフェンス研究所は、インターポールに加盟している各国の警察のサイバー犯罪捜査官向けの演習の企画開発、運営に協力しました。

メモリフォレンジックやマルウェア解析、HW のリバースエンジニアリングといった高度な解析技術が求められる問題だけでなく、被害企業へのヒアリングといった現実の犯罪捜査で行われる捜査を組み込むなど緻密に作り込まれた演習環境を作成し、実践的なフォレンジック技術とサイバー犯罪捜査能力の向上に寄与しています。

過去の演習例



世界的な航空宇宙企業がサイバー犯罪グループからフィッシング攻撃を受けたことを発端とする BEC の一連の調査を行うというシナリオを用意。

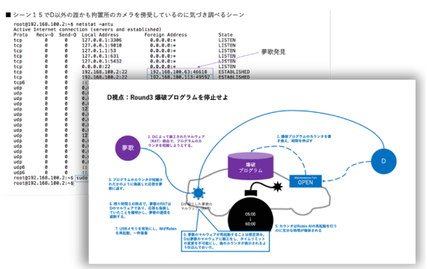


鹵獲したドローンに対するログの抽出やリバースエンジニアリングを必要とする高難易度な問題も作成。

メディア監修

サイバーディフェンス研究所は、ドラマや映画、漫画といったメディアにおけるハッキングシーンおよびサイバー攻撃に関する技術監修にも多数携わっています。

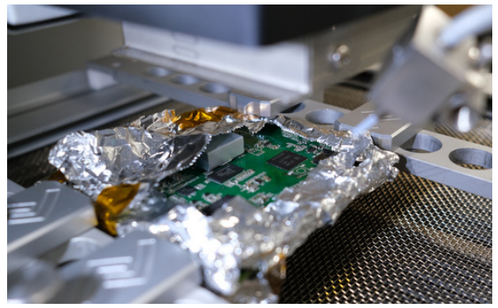
- TBS 系列ドラマ「ブラッディ・マンデイ」
- TBS 系列ドラマ「CODE：M コードネーム ミラージュ」
- Amazon ビデオ「フェイス - サイバー犯罪特捜班」
- 映画「恋する寄生虫」
- TBS 系列ドラマ「インビジブル」
- テレビ朝日系列ドラマ「科捜研の女 2022」
- 芳文社「解体屋ゲン」



技術ブログ「DARK MATTER」

サイバーディフェンス研究所には、「最新の技術や仕組みに対する飽くなき関心」や「より良い解決方法を探求する姿勢」といった優れたハッカーに必要とされる能力を遺憾なく発揮できる環境が整っており、当社のセキュリティエンジニアは日頃から様々な技術の調査・研究を行っています。

当社の技術ブログ「DARK MATTER」では、それらの活動の一端を公開しています。

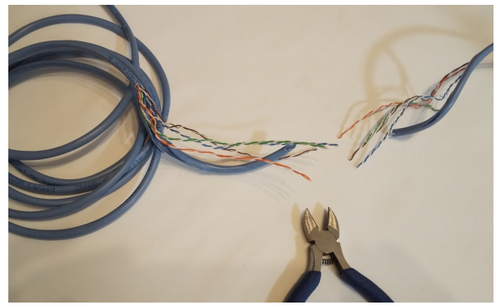


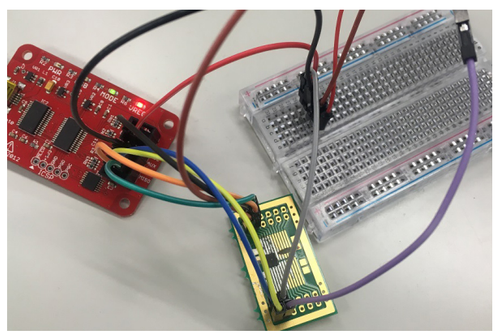
「デバイスの初期化で個人情報は完全に削除できるのか」

初期化済みの体表温度計を対象に、基板から eMMC と呼ばれるフラッシュメモリを取り外してファームウェアイメージを解析したところ個人情報が残存していることを確認。

「LAN ケーブルをニッパーで切断し５秒でネットワークに侵入・盗聴できるか実験してみた」

ネットワークを構成する大きな要素である LAN ケーブルからネットワークへ侵入し、通信を盗聴されるリスクを周知するために行った実験。





「BusPirate を用いて SPI 接続するフラッシュメモリを手動で読み出す」

デバイスをサポートする ROM ライターが無いケースに備え手動で読み出すための実験。ハードウェアから小型の SPI フラッシュメモリを取り外し、BusPirate と flashrom コマンドでデータの抽出を試みた。

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、私たちは既存の技術や手法に固執せず、
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は、新しいアイデアを驚異的なスピードで具現化し、実用可能性を検証します。

PIV GATEWAY™

サイバーディフェンス研究所は、様々なシステムに対する膨大なペネトレーションテスト・ハッキング試験の経験から、最優先のセキュリティ対策は「認証・認可の強化」であると確信し、NIST や TCG (Trsuted Computing Group) などの国際標準規格をベースに堅牢な認証・認可の仕組みを自社開発しました。

パスワードレス化と認証認可の統合によって、ユーザーの利便性と管理コストを最適化しながら、ゼロトラストの思想に基づくデバイスとユーザーの真正性検証、認証、認可を真にセキュアに実装したソリューション、それが PIV GATEWAY ™ です。

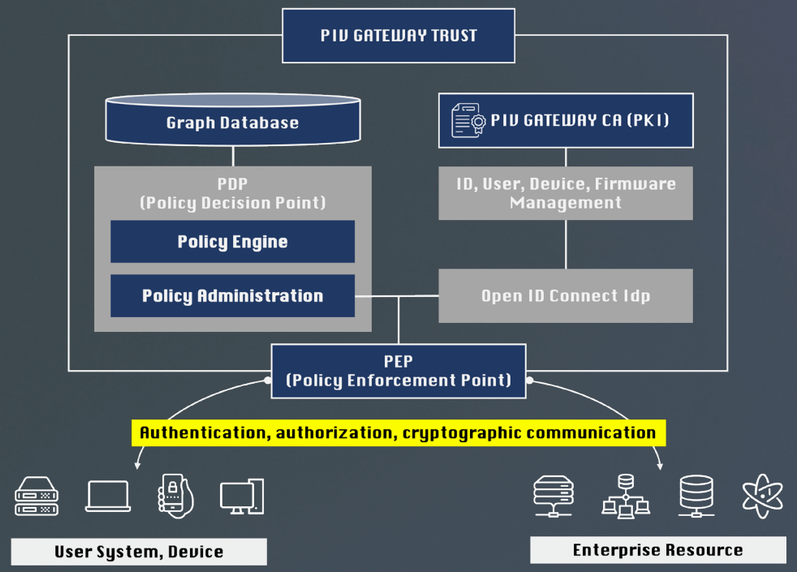
主要機能

PIV GATEWAY CA

認証局基盤のテンプレートを提供することで、NIST SP800-63B AAL3 レベル相当の認証基盤を容易に導入・運用できます。
FIPS 140-2 Level3 認証済 HSM（ハードウェアセキュリティモジュール）を用いてセキュアに鍵を保護します。

PIV GATEWAY TRUST

認証 / 認可を統合管理します。ヒト（ユーザー）とモノ（デバイス）両方の真正性を検証することでゼロトラストの根幹であるアクセス制御（PEP, PDP）を実現します。
NIST SP800-162（属性ベースアクセス制御）を参照実装しています。



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 Computer Security Incident Response Team Association
Forum of Incident Response and Security Team（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