インシデント対応プロセス再入門

SANS Institute
Technical Manager 上田 健吾
https://www.sans.org

自己紹介

SANS Institute

Technical Manager 上田 健吾（Kengo UEDA）

2000年にセキュリティベンチャー起業後、文部科学省 21世紀COE研究員（慶應義塾大学大学院 後期博士課程）を経て、2007年に野村総合研究所に入社。NRIセキュアテクノロジーズに出向し、銀行、生損保、クレジットカード業界をはじめ、セキュリティ監査、ペネトレーションテスト、フォレンジック、事故対応支援やコンサルティングなど、数多くのセキュリティ関連プロジェクトに参加。東京工業大学にて特定准教授として情報セキュリティの講義も担当。2021年6月より現業。

GSEC、GCIH、GWEB、GWAPT、CISSP、CISA、CISM、QSA、ASV、情報セキュリティ主任監査人など、セキュリティ系の資格を多数取得。IT雑誌、学会誌への寄稿や、ニュースへの出演経験、登壇経験も多数。業務を通して得られる最新の情報を展開。

不正アクセスの実態

令和2年に都道府県警察から警察庁に報告がなされた不正アクセス数

2,806件

2021年3月4日：
国家公安委員会、総務省、経済産業省：
「不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況」より

不正アクセスの実態

不正アクセス行為の動機

- 不正に経済的利益を得るため
- 顧客データの収集等情報を不正に入手するため
- 好奇心を満たすため
- 嫌がらせや仕返しのため
- オンラインゲームやコミュニティサイトで不正操作を行うため
- 料金の請求を免れるため
- その他

2021年3月4日：
国家公安委員会、総務省、経済産業省：
「不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況」より

攻撃者優位

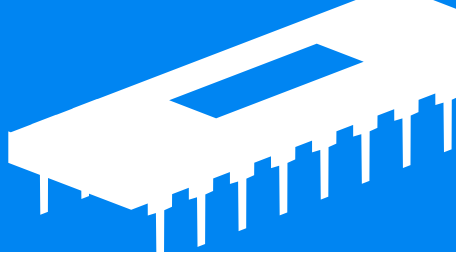
攻撃者

- ゼロデイ攻撃
- 最新技術
- 攻撃技術の販売
- ツール化
- ボットネット
- and so on…

防御側

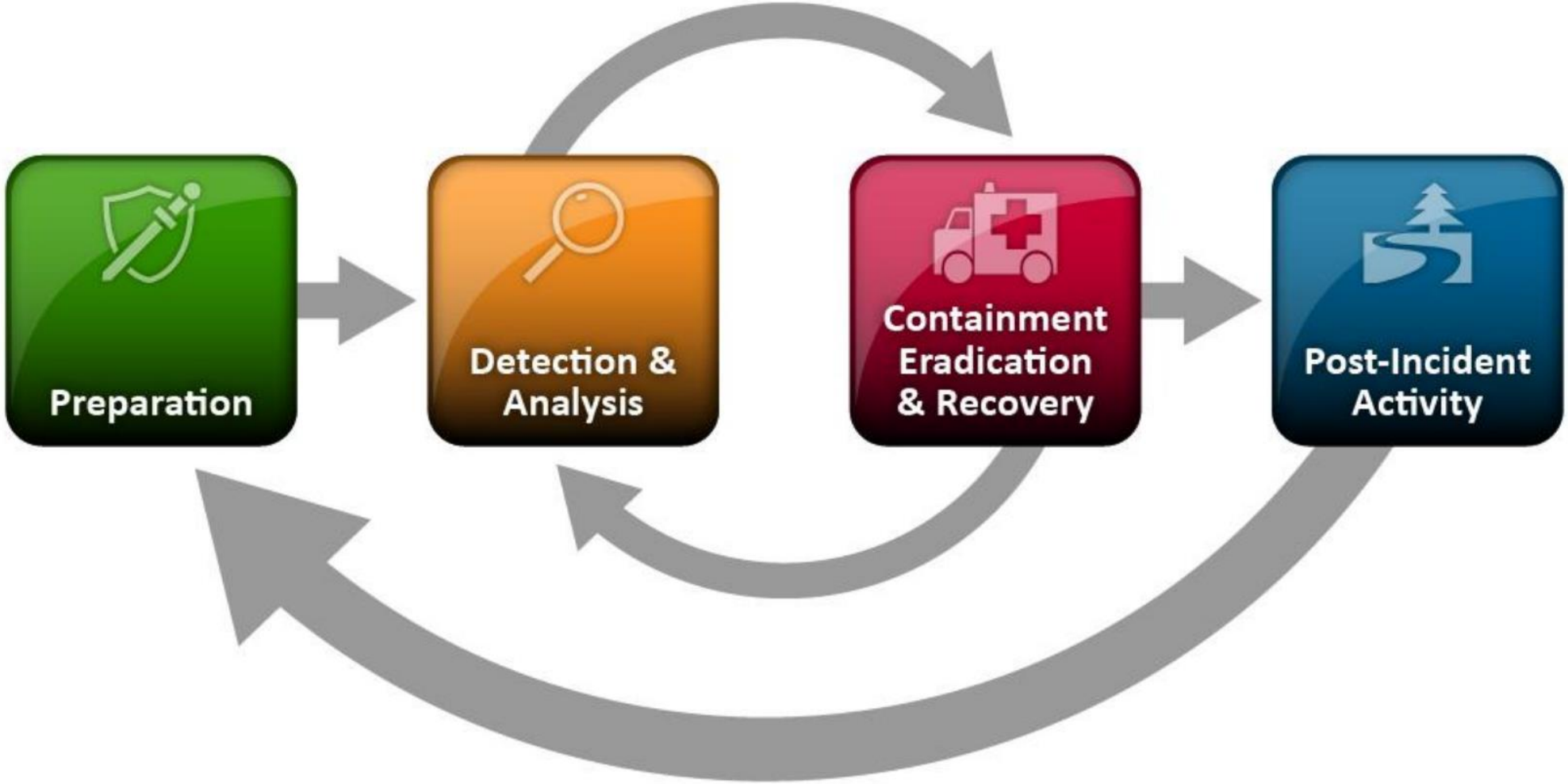
- 攻撃側の手口が分からない
- 事前対応が不十分
- パッチ配布後に対応
- 攻撃後にインシデント対応

必要なのは



早期発見・早期対策

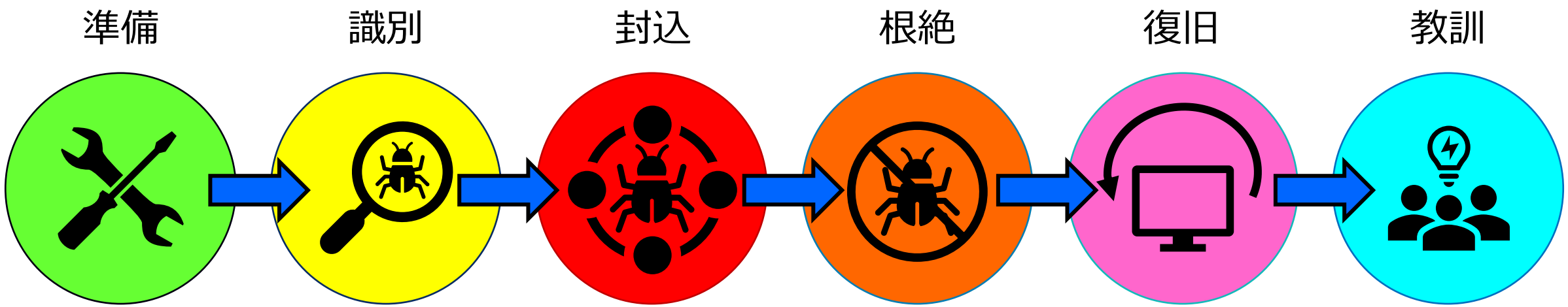
インシデントレスポンス



NIST: SP 800-61 Rev. 2, Computer Security Incident Handling Guide
https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

インシデントレスポンス

SANS Incident Response 6 Primary Phases



SANS

準備

組織を知る

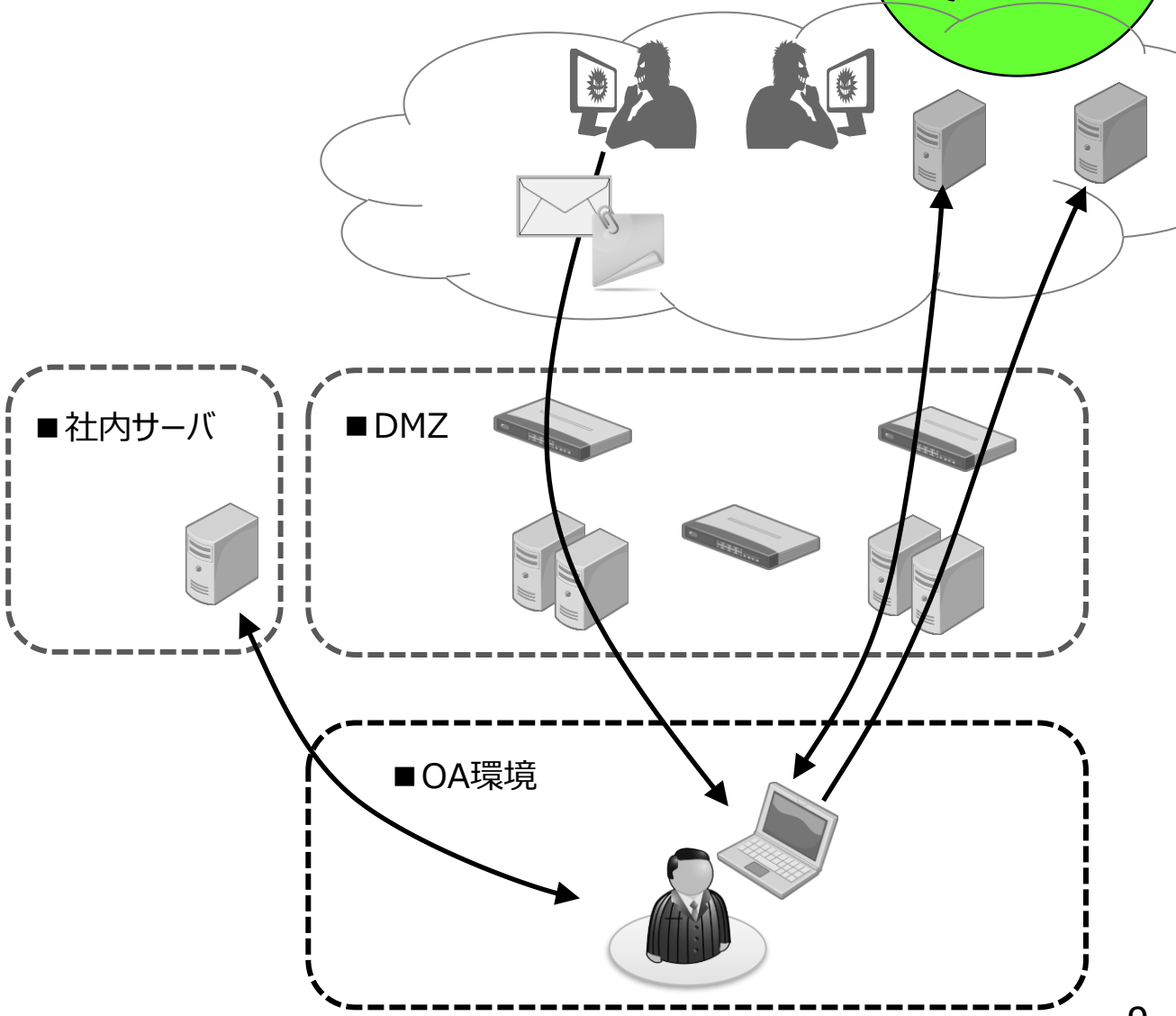
- ポリシーや手順

組織内IT環境の可視化

- ネットワーク
- エンドポイント
- データフロー

IT災害復旧計画

- バックアップ



識別

インシデントの検知

- FW/IDS、ホストのログ
- 異常な振る舞い
- 通報

検証

- インシデント？ 誤検知？

フォレンジック調査

- エビデンスの収集

封込

攻撃者の行動を止める

- 横展開、常駐化
- スコーピング

対応例

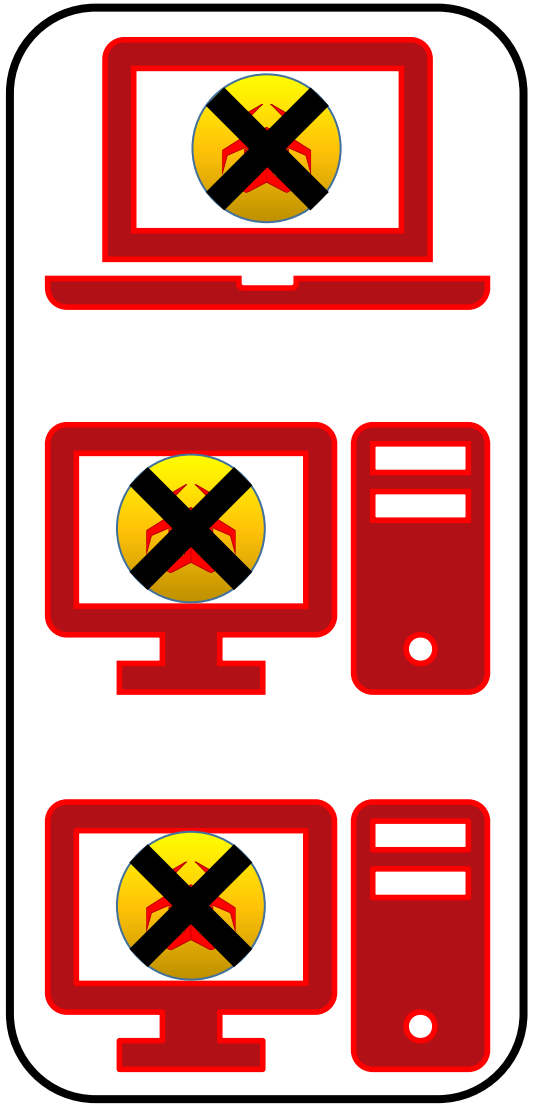
- 端末の隔離
- パッチの適用
- プロセス停止、アカウント削除
- ルータやFWでのフィルタリング
- DNSエントリの変更

根絶

攻撃者が残したものを駆除

対応例

- バックアップからの復旧
- 悪意あるプロセス、アカウントの削除
- 脆弱性診断
- ペネトレーションテスト
- 不正送金への対応
- 改ざんされたソースコードの復元



復旧

業務活動を再開

- 最終判断は経営層による

システムの再構築が最良

- できない場合もある
- 再構築した上で脆弱性診断は必須
- 短期的対策後に本格対応をすることも

業務時間外に復旧

- 注意深く監視することが可能

教訓

報告書にまとめて情報共有

- セキュリティ基盤の改善
- 事故直後は関係者の意識が高い

フォローアップレビューミーティング

- 影響が薄れていくことを軽減
- 導入した対策、改善したポリシー
- 再び侵害されたらどうなるか
- 30日後、60日後、90日後など

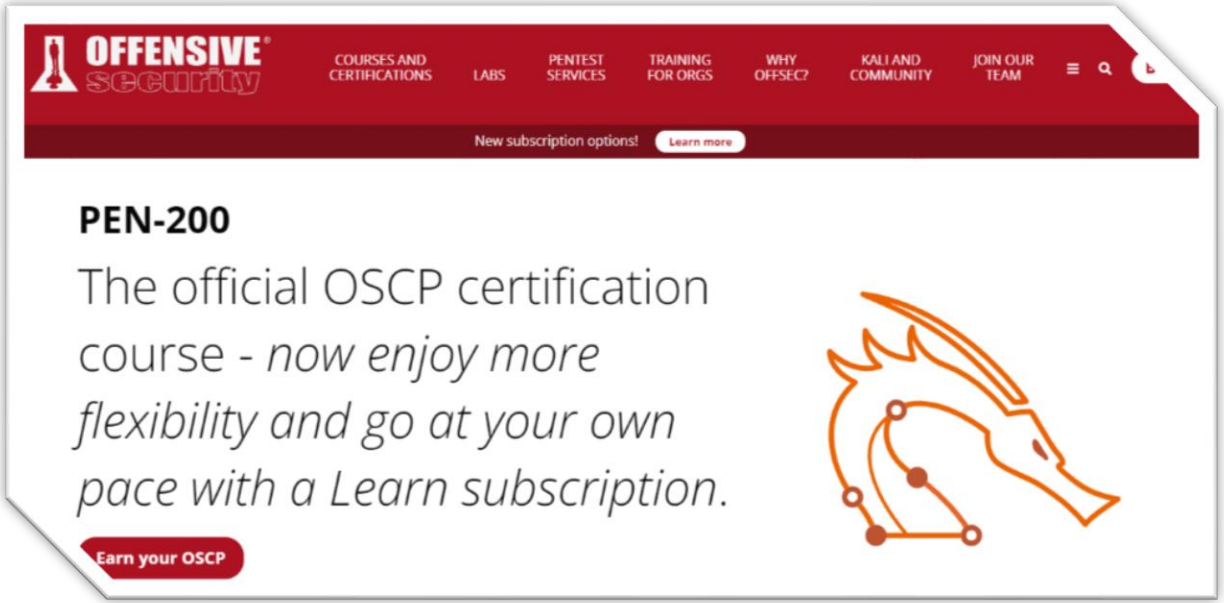
セキュリティ人材育成

インシデント対応技術者の人材育成が必要とされている

トレーニング選定

- 業務に適合した内容であること
- 体系立った内容であること
- 実践的な内容であること
- 復習可能な教材があること
- 定評、実績あるトレーニングであること
- 身につけた能力を評価・測定できること

トレーニング選定



プロフェッショナルの育成

SANS Institute
(SysAdmin, Audit, Network, Security)

SANS

- SANS本部：米国メリーランド州
- 情報セキュリティトレーニング、認定資格、調査研究におけるグローバルリーダー
- 第一線の専門家による講義・高品質のマテリアル
- 単なる知識の習得ではなく実務的なスキルを習得
- 多様なラーニングフォーマット（オンライン、対面、プライベート開催等）

SANS Overview

1989	• リサーチ及び教育機関として設立
117,000	• のべ11万人以上の資格保持者
40,000	• 年間4万人以上のセキュリティ専門家を育成
500	• 500以上の組織・政府機関と提携
65	• 65以上のトレーニングコースを提供
35	• 35以上の認定資格（GIAC）

SEC504：Hacker Tools, Techniques, Exploits and Incident Handling

- 攻撃者のねらいとその手口を詳細に理解し、それを踏まえて、脆弱性の発見と侵入検知の実践的な経験を養います。成果として、総合的にインシデントハンドリングを行えるようになることを目標としています。

Day1 インシデントレスポンスとコンピュータ犯罪の調査

•インシデントレスポンスとデジタル調査の両方の重要な要素を検討します。いくつかのインシデントから情報を得て、ビジネス運営とセキュリティの両方にとって重要な目標と結果を検討します。

Day2 情報収集、スキャン、列挙手法

•攻撃者のツールや技術を理解し、ターゲット組織を偵察するための方法を学び、最初の侵害の弱点に関する情報を開示・特定します。次に攻撃者が特権的なアクセスを得るためのスキャン技術を掘り下げていきます。

Day3 パスワード攻撃と不正アクセス

•簡単なパスワード推測攻撃から始め、アカウントロックアウトなどの防御システムを回避する効果的なプロセスを採用するために攻撃者が採用しているテクニックを調査します。

Day4 外部からの攻撃とDrive-By攻撃

•Metasploitなどを使用して、システムを侵害する技術を調査します。また、Drive-By攻撃や水飲み場攻撃などについて取り上げ、攻撃者がどのようにしてエクスプロイトやシステム侵害ツールを作成するかを調べます。

Day5 回避と侵入後の攻撃

•侵害が終わった後の攻撃者のステップを検証します。侵入検知を回避したり、攻撃者が踏み台を経由して移動したりする方法、組織内のシステムスキャンおよび情報資産探索のための手法を学びます。

Day6 Capture the Flag

•グループでチームを組んで、Windows、Linux、IoT、クラウドなどを対象に、スキャン、エクスプロイト、ポストエクスプロイトのタスクを行います。現代のネットワークを再現した環境の中で、コース全体で学んだ技術を再確認します。

受講対象者

- セキュリティ担当者
- システム管理者
- インシデントハンドリング担当者
- システムアーキテクト
- セキュリティ関係者
- ペネトレーションテスター

効果

- インシデントハンドリングの理解
- 攻撃者の手口とその防御
- ハッキングツールと技術
- 最新の攻撃ベクトル
- 攻撃からの復旧

Demonstration

SEC504:

Hacker Tools, Techniques, Exploits and Incident Handling

THANK YOU

上田 健吾（Kengo Ueda）
japan@sans.org / https://www.sans.org

@sansinstitute.japan
@SANS_JAPAN_TEAM