セキュリティインシデント分析コース
事前学習用資料

公益社団法人　私立大学情報教育協会

この資料の目的

インシデント分析コース受講にあたり
前提知識として確認しておいていただきたい内容を掲載

当日の演習を円滑に受講し、理解を深めることができる
（すべて必須の知識ではありませんが、
なるべく事前に確認して受講をお願いいたします）

公益社団法人　私立大学情報教育協会

メニュー

1. インシデント対応の基礎
    1. インシデントとは
    2. インシデントハンドリング
    3. 記録・報告書の作成
2. 受講の前に
3. 演習に必要な知識
    1. 環境やツールの紹介
    2. 脆弱性の概要

インシデント対応の基礎

インシデント対応の基礎

■ セキュリティインシデントとは

「情報システムの運用におけるセキュリティ上の問題として捉えられる事象」

・適切な情報管理が損なわれた状態
・機密性、完全性、可用性が脅かされ、
　業務に支障をきたす事象
・故意や過失、災害等、様々な要因による

インシデント対応の基礎

■ インシデントハンドリング

インシデント発生から解決までの一連の対応

step	内容	例
検知・連絡受付	• インシデント発生の連絡を受領	• ウィルス対策ソフトがマルウェア検知の警告を発していると連絡があった • 外部機関から、学内より不審な通信が発生していると連絡があった • USBメモリを紛失したと連絡があった
トリアージ	• 事実関係及び状況確認 • インシデントか否かの判断 • 対応の優先順位付け	• サイバー攻撃を受けている事実が確認された • 重要情報が外部へ漏れていることが確認された
インシデントレスポンス	• 対応方針の検討 • 被害の原因を取り除き、復旧	• 復旧可能性の確認 • 障害からの復旧 • セキュリティパッチの適用
報告・公表	• 被害状況や影響範囲に応じて組織内外に対して報告・公表	• サイバー攻撃の影響範囲を経営陣へ報告 • 個人情報漏えいの事実と被害範囲の公表
事後対応	• 報告書のとりまとめ • 振り返りの実施	• 事実確認の詳細を取りまとめ • 関係者での振り返りと今後の方針の決定

インシデント対応の基礎

■ タイムラインの記録の重要性

全体として何が起こったのかを俯瞰して把握する

・タイムライン作成の目的
  ・事実関係の正確な把握
  ・問題や課題の分析
  ・再発防止策の検討
  ・正確な報告や公表
  ・過失の証明等、事後の事実確認

・タイムラインへの記載事項
  ・時刻　・発生事象　・対応内容　など

インシデント対応の基礎

■ インシデント報告書

影響度や影響範囲を適切に把握・情報共有

・初動を行なった際の一次報告書
・詳細な調査を行なった二次報告書
・タイムラインの情報を元に事実関係を把握
・対外発表の際の根拠となる
・CISOへの報告を意識

インシデント対応の基礎

- 参考：代表的な外部からの連絡元となる組織

種類	目的 実施方法例
JPCERT/CC	インターネットを介して発生する侵入やサービス妨害等のコンピュータセキュリティインシデントについて、日本国内を対象とする報告の受付、対応の支援や助言等を、技術的立場から行う。
IPAサイバーレスキュー隊	サイバー攻撃の被害の発生が予見され、その対策の対応遅延が社会や産業に重大な影響を及ぼすと判断される組織等に対してエスカレーションや支援を行う
NISC （内閣サイバーセキュリティセンター）	監視活動により検知された脅威を分析した結果、攻撃が行われたと認識され、当該政府機関等において対応が推奨される事案について、通報を行う

文科省経由での連絡もあり得る・・・？

受講の前に

サイバー攻撃に関する法や倫理

■ 様々な法に関係する情報セキュリティ

	刑事法	行政法	民事法
規制方式	国家機関による刑罰権行使	所轄の大臣が事業者を監督	個人の自由意思が優先（私的自治の原則）
違反・侵害の効果	刑事罰	助言、勧告、命令など	損害賠償、差止請求
主な法律・規定	刑法、不正アクセス禁止法、公認会計士法などの守秘義務規定	個人情報保護法、特定電子メール法、特定商取引法、電気通信事業法、e-文書法、電子署名・認証法	民法、著作権法、不正競争防止法、会社法（内部統制制度）
備考	刑事罰は人権保証の観点から、最後の手段	日本に存在する多くの法律が行政法に属する。命令違反は刑事罰の対象となり得る	法律上の明文はないが、人格権を根拠にした場合にも差し止めや損害賠償請求が可能

サイバー攻撃に関する法や倫理

■ 法律に抵触した後のリスク（社会人）

懲戒処分の区分	ペナルティ
懲戒解雇	解雇となり退職金の全部または一部が不支給 失業保険が制限され、再就職も困難
論旨解雇	退職届の提出を勧告し依願退職
降格	役職、職位、職能資格等を引き下げ
出勤停止	1か月未満程度の就労禁止（無給）
減給	賃金から一方的に一定額を差し引く
譴責（けんせき）	書面での反省（顛末書、報告書）
戒告（かいこく）	口頭での反省

悪用行為による法律抵触は懲戒解雇の可能性がある

サイバー攻撃に関する法や倫理

- 法律に抵触した後のリスク（学生）

懲戒処分の区分	ペナルティ
退学・除籍・抹籍	修学の権利を剥奪し学籍関係を一方的に終了
停学	一定期間、教育課程の履修及び課外活動を禁止
譴責（けんせき）	口頭及び文書により注意

悪用行為による法律抵触は退学の可能性がある
また、懲戒処分は就職や転職に大きく影響する

誓約書について

- 法令の遵守と十分な理解を担保するため、誓約書への署名をお願いしている

情報セキュリティの演習（攻撃手法の学習や手法の理解を含むなど）への参加は、誓約書に署名し提出することが参加条件となる

■ 誓約書の主な記載内容
・得られた知識の利用制限　・違反時の訴追の可能性
・違反によって生ずる損害の賠償責任帰属
・授業／研修実施組織規則違反時の処罰　　など

演習に必要な知識

環境やツールの紹介

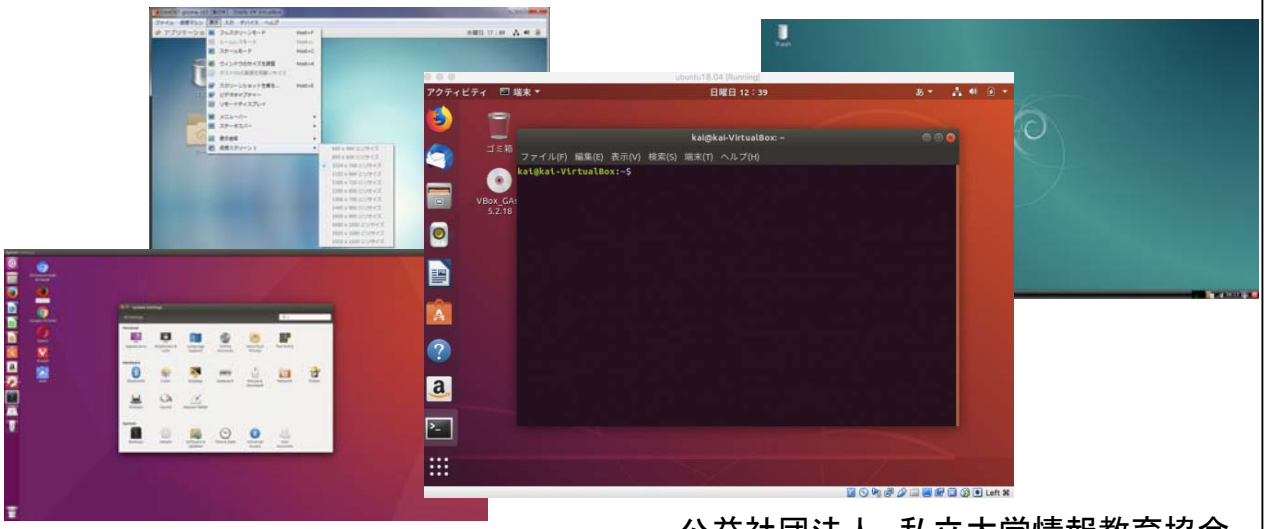
- サイバーレンジとは
  - 実世界を模した仮想システム環境
  - 実際に使われている機器やアプリケーション
  - 本物のマルウェア

これらを用いた**実践的演習環境**

今回は基礎的な内容の演習を行います。詳細な手順書を別途用意しますので、
環境に不慣れな方も安心してご参加ください。

環境やツールの紹介

- LINUX…オープンソースのOS
  - サーバ環境で広く利用
  - 様々な種類（ディストリビューション）が存在
  - スマートフォンからスーパーコンピュータまで多くのデバイスで利用



環境やツールの紹介

- 主要なコマンド

コマンド	内容	使用例
cat	ファイルの内容の閲覧	**cat [filename]** filenameの内容の閲覧
cp	ファイルやディレクトリのコピー	**cp [filename] [directory]** filenameをdirectory配下にコピー **cp –r [directory1] [directory2]** directory1の内容をすべてdirectory2としてコピー
mv	ファイルやディレクトリのの移動、名前の変更	**mv [filename] [directory]** filenameをdirectory配下に移動 **mv [filename1] [filename2]** filename1の名前をfilename2に変更
rm	ファイルやディレクトリの削除	**rm [filename]** filenameの削除 **rm –r [directory]** directoryの中身ごと削除
ls	ファイルやディレクトリの情報を表示	**ls –la** 現在のディレクトリのすべてのファイルの詳細を表示 **ls –laR** サブディレクトリも含めたすべてのファイルの詳細を表示
pwd	現在のディレクトリ（カレントディレクトリ）の表示	**pwd** 現在のディレクトリを絶対パスで表示
cd	ディレクトリの移動	**cd /usr/home** /user/homeに移動 **cd** 自分のホームディレクトリに移動
grep	ファイル中の文字列を検索	**grep abc *.txt** 現在のディレクトリの.txtが付くファイルからabcという文字列がある行を検索して表示

環境やツールの紹介

■ 主要なコマンド

コマンド	内容	使用例
last	直近のログイン履歴を確認	**last** 最近ログインしたユーザを新しい順に表示
lastlog	全てのユーザの最終ログイン時の情報を表示	**lastlog** 全ユーザの最終ログイン情報を表示。一度もログインしていないユーザは**Never logged in**と表示される
more	ファイルの内容を1画面ずつ止めながら表示	**cat** [filename] filenameの内容を1画面ずつ表示 スペースキーで1画面先に進む。**/abc**で文字列abcを含む行を検索するなどサブコマンドによる操作が可能。
head/ tail	ファイルの内容を先頭だけ/末尾だけ表示	**head** [filename] filenameの内容の最初の10行を表示 **tail –n 20** [filename] filenameの内容の最後の20行を表示
sudo	rootユーザの権限でコマンドを実行する	**sudo** [command] commandをroot権限で実行 パスワードが必要な場合、一定時間内は2回目以降の入力は省略される

「｜」(パイプ)の利用について
パイプは、コマンドの出力結果を別のコマンドに渡すことができます。
(使用例)**$ more log.txt | grep apache** log.txtの内容から、apacheを含む部分を1画面ずつ表示させる

標準の出力結果が非常に多いものなどから目的の内容を探し出す際などに便利に使えます。

環境やツールの紹介

■ nmap

ポートスキャンなど、ネットワークの状態を確認できるツール

Nmapによるポートスキャンコマンドの例:
nmap –F [対象のIP/URL]

```
root@attacker:~# nmap -F company.example.com

Starting Nmap 7.60 ( https://nmap.org ) at 2019-01-15 15:37 JST
Nmap scan report for company.example.com (10.76.22.98)
Host is up (0.00017s latency).
Not shown: 97 closed ports
PORT     STATE    SERVICE
22/tcp   filtered ssh
80/tcp   open     http
8080/tcp filtered http-proxy
```

この例では、80番ポートがopenしているのが確認できる。
22番のfilteredは、ファイアウォールなどネットワーク上の障壁でポートが遮られている状態を指す

環境やツールの紹介

■ ssh

通信内容を暗号化できるリモートアクセスプログラム

```
# ssh [ アカウント名 ]@[ ホスト名 ]
```

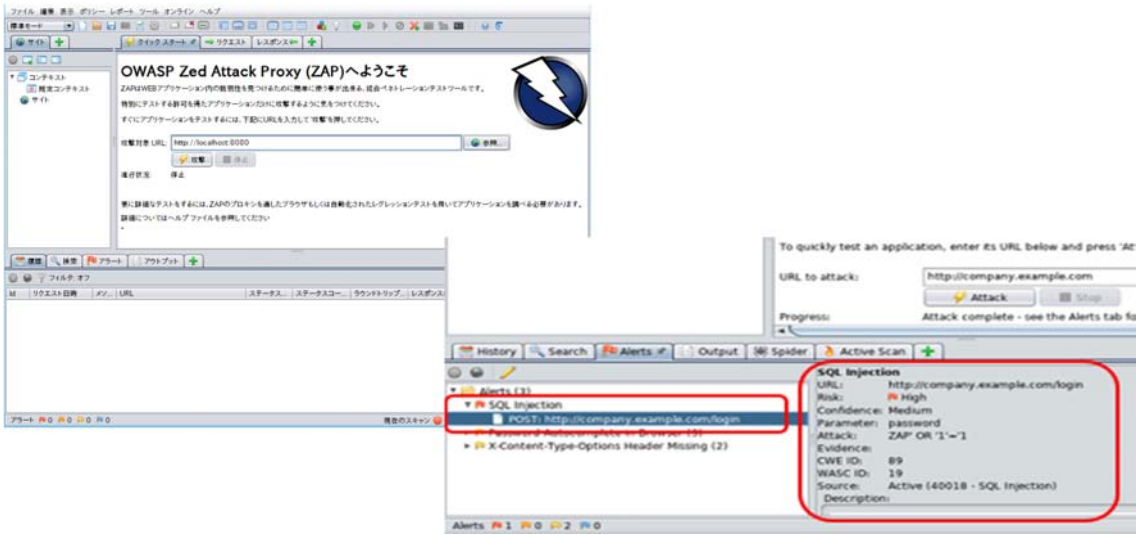
```
root@attacker:~# ssh backdoor@company.example.com
The authenticity of host 'company.example.com (10.76.22.98)' can't be establishe
d.
ECDSA key fingerprint is SHA256:Z6e/yRxhHrwHhYQto3lcN/J6K0YPD+GQTxwMTxm/y9A.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'company.example.com,10.76.22.98' (ECDSA) to the list
 of known hosts.
backdoor@company.example.com's password:
Welcome to Ubuntu 18.04.1 LTS (GNU/Linux 4.15.0-43-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
```

Are you sure you want to continue connecting (yes/no)?に
yesと入力することで対象に接続。

環境やツールの紹介

■ OWASP ZAP

Webアプリケーションの脆弱性などに関する診断ツール

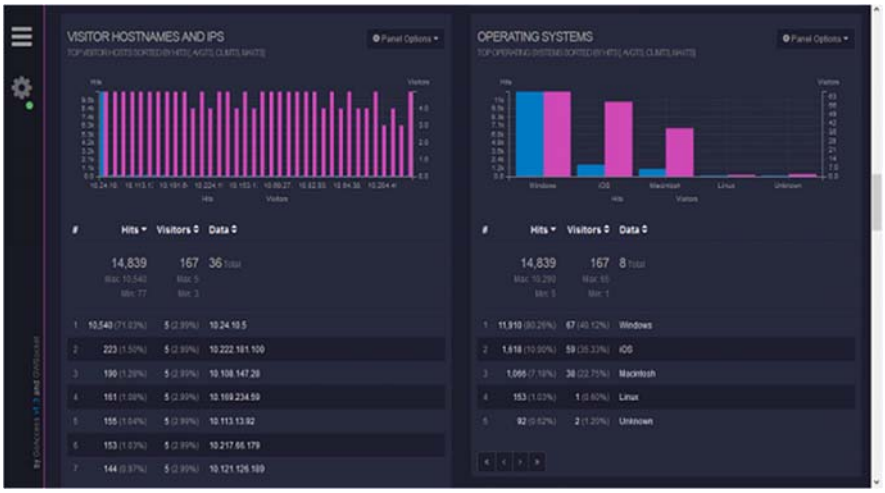


脆弱性の種類や、攻撃する方法の例などが確認できる

環境やツールの紹介

- GoAccess

リアルタイムにWebのログを解析できるツール



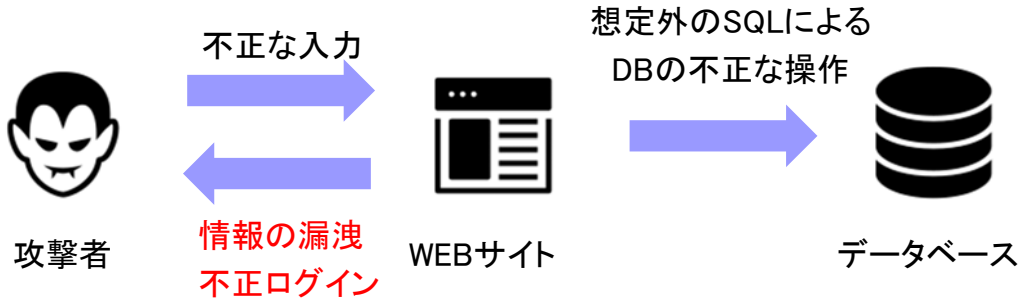
不自然にアクセスの多いIPアドレスなどを確認できる

演習で扱う脆弱性

SQLインジェクション

■ SQLインジェクションの概要

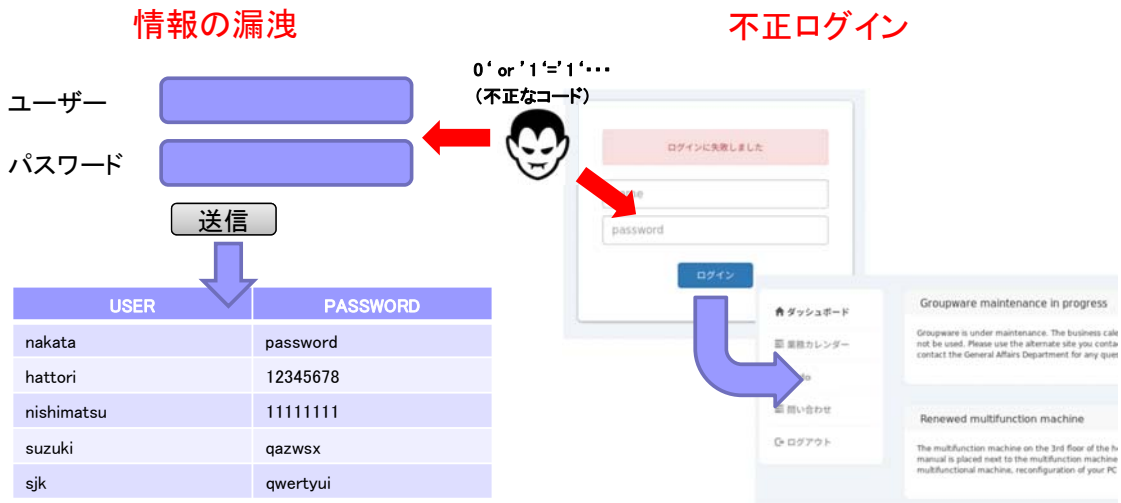
入力されたデータにより、SQL文の内容を意図的に変更させる攻撃手法



SQLインジェクション

■ SQLインジェクションの影響

意図しないデータが表示されたり、不正にログインされてしまう



USER	PASSWORD
nakata	password
hattori	12345678
nishimatsu	11111111
suzuki	qazwsx
sjk	qwertyui

SQLインジェクション

■ SQLインジェクションの攻撃例

select * from 社員テーブル where 社員番号='〇〇';　…(式1)

式1は、「社員テーブルから社員番号が〇〇のデータを取ってきてください」
という命令のSQL文です。「〇〇」の部分には外部から指定した社員番号が入ります。

しかし、〇〇の部分に　0’ or ‘1 ‘= ‘1　と入力されてしまうと・・・

select * from 社員テーブル where 社員番号= ‘0’ or ‘1’ = ‘1’;　…(式2)

となります。
式2では、検索条件にあたるwhere部分がすべて「真」になってしまい、
すべてのデータを検索対象としてしまいます。

ファイルアップロード機能の不備

■ ファイルアップロードの不備の概要

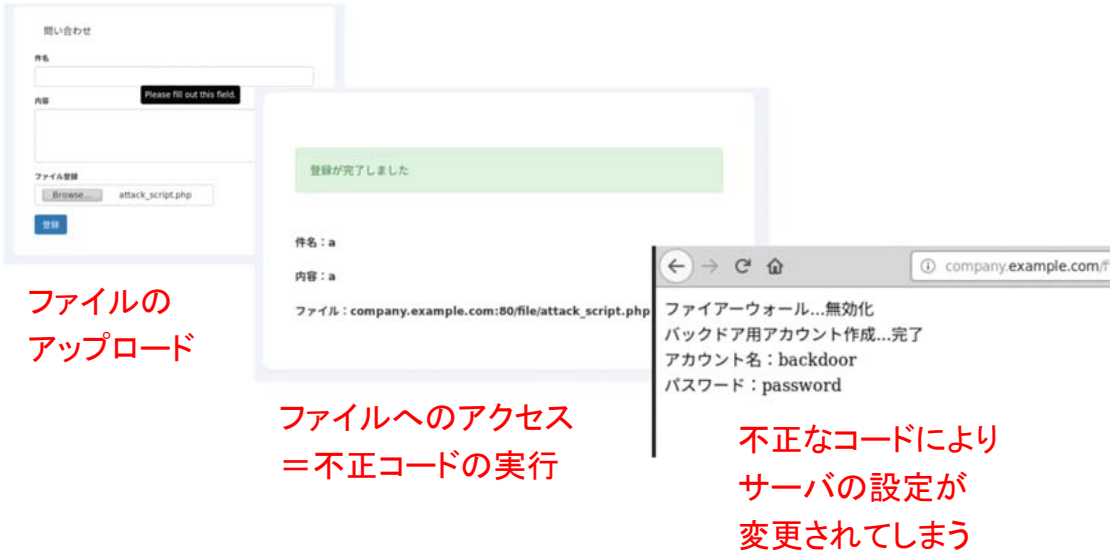
不正なコードを記述したファイルをアップロードし、
そのまま実行できてしまうことで意図しない動作が発生

不正なコードが記述された
ファイル

ファイルアップロード機能の不備

■ ファイルアップロードの不備の影響

ファイアウォールの無効化や、不正なアカウント作成など様々な影響



ファイルの
アップロード

ファイルへのアクセス
＝不正コードの実行

不正なコードにより
サーバの設定が
変更されてしまう

脆弱性への対策

■ どのような対策ができるか

・システム的な対策
・セキュアなコーディング
・脆弱性を発見する

いくつかの対策・予防策などが考えられます。
これらの脆弱性に有効な対策を調べてみてください。

参考：用語集

用語	読み	意味
C&Cサーバ	シーアンドシーサーバ	「C&C」は「Command And Control」の略。攻撃者が感染した端末上のマルウェアに遠隔操作 のための指令を送るサーバのこと。「C2サーバ」と呼ばれることもある。
CISO	シーアイエスオー	「Chief Information Security Officer」の略。組織の最高情報セキュリティ責任者。
CSIRT	シーサート	「Computer Security Incident Response Team」の略。 情報セキュリティに関わるインシデントに対処する組織。自組織のインシデント(事件や 事故のこと)に対処する以外にも、インシデント情報、脆弱性情報、攻撃予兆情報の収集・分析、対応方針や手順の策定などを行う。
CVE	シーブイイー	「Common Vulnerabilities and Exposures」の略。共通脆弱性識別子。CVEは、個別製品中の 脆弱性を対象として、米国政府の支援を受けた非営利団体のMITRE社が採番している識別子である。脆弱性検査ツールや脆弱性対策情報提供サービスの多くがCVEを利用している。
DMZ	ディーエムゼット	「DeMilitarized Zone」(非武装地帯)の略。 インターネットのような攻撃の危険を伴う外部ネットワークと、内部ネットワークの中間に置か れる領域。外部向けWebサーバなどを配置する。
DoS攻撃	ドスコウゲキ	「DoS」は「Denial of Service」の略。DoS攻撃の手法は大きく二つに分けられ、サーバに負荷をかけることによって、コンピュータ資 源やネットワーク資源を提供できない状態にさせる攻撃と、コンピュータやネットワーク機器の 脆弱性を悪用し機能を停止させる攻撃がある。
Drive-by Download	ドライブバイダウンロード	Webブラウザなどを介して、ユーザに気づかれないようにマルウェアなどをダウンロードさせる攻撃手法のこと。
Exploit	エクスプロイト	コンピュータ関連のソフトウェアやハードウェアの脆弱性を利用した悪意ある行為のために書かれた、スクリプトまたはプログラムのこと。
IDS	アイディーエス	「Intrusion Detection System」の略。侵入検知システムと呼ばれる。ネットワーク上に流れる パケットを監視し、攻撃や不正アクセスの兆候を検知して管理者に通報するシステムの総称。
IPA	アイピーエー	「Information technology Promotion Agency, Japan」(情報処理推進機構)の略。経済産業省所管の独立行政法人。日本の情報化社会の発展に寄与するため、情報セキュリティ対策の強化、社会全体を支える情報処理システムの信頼性向上、IT人材育成の戦略的推進に取り組んでいる。

参考：用語集

用語	読み	意味
IPS	アイピーエス	「Intrusion Prevention System」の略。侵入防止システム。外部との通信を監視して不正なアクセスを検知し、自動的にブロックする機能を備えたシステムの総称。
IOC	アイオーシー	「Indicator of Compromise」の略。セキュリティ侵害の証拠や痕跡のこと。例えば、攻撃者のIPアドレス、マルウェアのハッシュ値、通信先のドメインなど。 IOCとシステムのログなどを突合することで、サイバー攻撃の被害に遭っているシステムを洗い出すことが可能になる。
JPCERT/CC	ジェーピーサートコーディネーションセンター	「Japan Computer Emergency Response Team Coordination Center」の略。 インターネットを介して発生する侵入やサービス妨害などのコンピュータセキュリティインシデ ントについて、日本国内を対象とする報告の受け付け、対応の支援、発生状況の把握、手口の分析、再発防止のための対策の検討や助言などを、技術的な立場から行う、特定の政府機関や企業に属せずに独立した中立の組織。
JVN	ジェーブイエヌ	「Japan Vulnerability Notes」の略。 日本で使用されているソフトウェアなどの脆弱性関連情報とその対策情報を提供し、情報セキュ リティ対策に資することを目的とする脆弱性対策情報ポータルサイト。JPCERT/CCと情報処理推 進機構(IPA)が共同で運営している。
NISC	ニスク	「National center of Incident readiness and Strategy for Cybersecurity」の略。内閣サイバーセキュリティセンターのこと。
PoC	ポック	「Point of Contact」の略。組織内外からの情報セキュリティに関する報告や依頼などを受け付ける統一的な窓口の連絡先の こと。インシデントレスポンス分野では、主に「Point of Contact」の略として用いられる。 または、「Proof of Concept」の略。 新しい概念や理論、原理、アイディアの実証を目的とした検証のこと。情報セキュリティ分野に おいては、何らかの脆弱性を悪用した攻撃が実際に有効であることの検証、または検証するため のプログラムを指すこともある。
SOC	ソック	「Security Operation Center」の略。 外部からネットワーク機器やサーバ類を常時監視し、サイバー攻撃の検出と分析、対応策のアド バイスを提供する組織、企業のこと。SOCを提供する企業をSOCベンダという。

参考：用語集

用語	読み	意味
SSL/TLS	エスエスエル/ティーエルエス	「Secure Socket Layer/Transport Layer Security」の略。インターネット上でデータを暗号化して送受信する方法のひとつ。TLSはSSLをもとに標準化させたもの。
WAF	ワフ	「Web Application Firewall」の略。Webアプリケーションの脆弱性を悪用した攻撃からWebアプリケーションを保護するセキュリ ティ対策の一つ。
可用性	カヨウセイ	情報管理における「可用性」とは、許可されたユーザが必要な時に情報および関連する情報資産に確実にアクセスできることをいう。
完全性	カンゼンセイ	情報管理における「完全性」とは、情報そのものやその情報の処理方法の正確さが完全であること。
機密性	キミツセイ	情報管理における「機密性」とは、許可されたものだけが情報にアクセスできることをいう。
Sandbox	サンドボックス	「National center of Incident readiness and Strategy for Cybersecurity」の略。内閣サイバーセキュリティセンターのこと。
脆弱性	ゼイジャクセイ	アプリケーションは開発過程における考慮漏れなど様々な要因によって、欠陥を持つことがある。脆弱性はその欠陥の一種で、例えば情報漏洩の原因となるなど、特に情報セキュリティに影響を与えるものである。セキュリティホールと呼ばれることもある。
セキュリティインシデント	セキュリティインシデント	コンピュータの利用や情報管理、情報システム運用管理に関してセキュリティ上の脅威となる事象や、業務に影響を与えたり、情報セキュリティを脅かすしたりする事件や事故のこと。
トリアージ	トリアージ	検知または通報された内容が、インシデントであるかどうかを判断し、対応する優先順位を決定すること。
バックドア	バックドア	攻撃者が侵入に成功したシステムに対して、再度侵入するために仕掛けたプログラムのこと。
ファイアウォール	ファイアウォール	PCやネットワークを、外部からの不正な侵入から保護するための機器やシステムのこと。

参考：用語集

用語	読み	フォレンジック意味
フォレンジック	フォレンジック	インシデントが生じた場合に、原因究明に必要な機器やデータなどを収集・分析し、当該インシデントの事象の調査および証拠の取得を行う技術のこと。
ポートスキャン	ポートスキャン	ネットワークに接続しているコンピュータに対して、他のコンピュータからの通信を受け取る状態となっているポート番号とアプリケーション(サービス)を探索すること。攻撃者が、攻撃を行うための事前調査として実施することがある。
マルウェア	マルウェア	不正かつ有害に動作させる意図で作成された悪意のあるソフトウェアや悪質なコードの総称。
ランサムウェア	ランサムウェア	マルウェアの一種で、感染したPCをロックしたりファイルを暗号化したりすることによって使用 不能にしたのち、元に戻すことと引き換えに「身代金」(ransom)を要求するソフトウェアの こと。
ログ	ログ	Cやサーバの稼働状況の記録や、ネットワーク機器上に残る通信の記録のこと。

おわりに

演習を通して

・具体的な操作を体験することで、インシデント対応の訓練とする

・一般的なインシデント対応の流れを体験し、自身の環境での対応手法を考察するきっかけとする

・サイバーセキュリティ教育の現状を体験し、教育・学習環境の整備を検討する際の参考とする

様々な部署・立場の方々に有益となるような内容を検討して参ります。
ご協力をよろしくお願いいたします。

公益社団法人　私立大学情報教育協会