A-2.
システムの脆弱性の点検と対策

明治大学
服部　裕之

公益社団法人　私立大学情報教育協会

セッションの目的

サイバー攻撃の事前対策として有用な、
脆弱性検査について学び、体験する

↓

自組織のシステム的な脆弱性を発見し、対策がとれる

メニュー

1. 脆弱性検査について
   - ✓ システムの脆弱性をついたインシデント事例
   - ✓ 公開されている脆弱性情報
   - ✓ 脆弱性検査とツール
2. 実習
3. 事例紹介

1. 脆弱性検査について

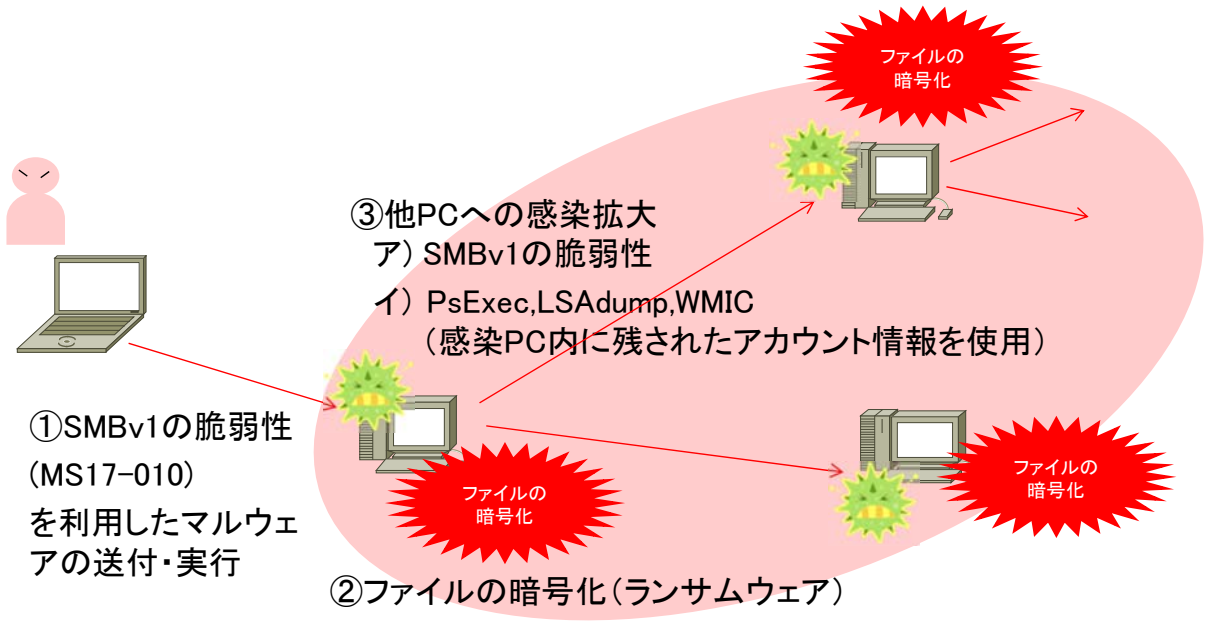
システムの脆弱性をついたインシデント(1)

- WordPressの脆弱性(2017-2)
  - 認証されていないユーザーによるWebページの改ざんが可能
  - 被害
    - 福井県立病院HP,群馬県HP,秩父観光なび,丸川五輪相HP等
      1週間で国内700以上のサイトが改ざん被害
- Apache Struts2の脆弱性(2017-3)
  - リモートから任意のコードが実行可能
  - 被害
    - B.LEAGUEチケットサイト（ぴあ）
      - 14万件（氏名、住所、電話番号、ID、パスワード 等）
    - 都税クレジットカード支払いサイト（トヨタファイナンスGMOペイメントゲートウェイ）
      - 36万件（クレジットカード情報等）
    - 国際郵便マイページ（日本郵便）
      - 2万件（メールアドレス等）
- WannaCry(2017-05)、Petya(2017-06)
  - SMBv1にリモートから任意のコード実行可能な脆弱性
  - 被害
    - ネットにつないだだけでランサムウェアに感染、PC上のファイルが暗号化被害。
    - 世界150ヶ国、30万件以上で被害

システムの脆弱性をついたインシデント(2)

- Oracle WebLogic Serverの脆弱性(2018-1, 2019-04)
  - リモートから任意のコードが実行可能
  - 被害
    - 仮想通貨採掘ソフト（XMRig）の実行
    - ランサムウェアへの感染、内部ネットワークへの拡大
- Drupalの脆弱性(2018-3)
  - リモートから任意のコードが実行可能
  - 被害
    - 米サンディエゴ動物園など、世界数百サイトで，仮想通貨採掘ソフト(Coinhive)が仕込まれていた
- Mirai(2016)
  - IoT機器(家庭用ルータ、Webカメラ等）の脆弱性（主に初期パスワード未変更に起因）
  - 被害・加害
    - Miraiに感染した個々のIoT機器が、DNSサーバへのDDoS攻撃元としてボット化
    - Twitter, Netflix, PayPal, PlayStation Network等が被害を受ける

【参考】WannaCry, Petya 感染の仕組み



公開されている主な脆弱性情報

- CVE – Common Vulnerabilities and Exposures
  - https://cve.mitre.org/
  - 個別製品の脆弱性識別番号 。MITRE社（非営利団体）が運営。
- JVN – Japan Vulnerability Notes
  - https://jvn.jp/
  - JPCERT/CC, IPAの共同運営。CVEとも連携。
- JVN iPedia – 脆弱性対策情報データベース
  - https://jvndb.jvn.jp/
  - IPAが運営。JVNやNVD(NIST)とも連携。

CVE識別番号 (CVE-ID)	JVNのID（識別番号）	JVN iPediaのID（登録番号）	脆弱性関連情報のタイトル
CVE-2007-5000	JVN#80057925	JVNDB-2007-000819	Apache HTTP Server の mod_imapおよびmod_imagemapにおけるクロスサイトスクリプティングの脆弱性
CVE-2008-0006	JVN#88935101	JVNDB-2008-001043	X.Org Foundation製Xサーバにおけるバッファオーバーフローの脆弱性
CVE-2008-3271	JVN#30732239	JVNDB-2008-000069	Apache Tomcatにおいて権限のないクライアントからのリクエストが実行されてしまう脆弱性
CVE-2008-5382	JVN#70599814	JVNDB-2008-000079	アイ・オー・データ製HDL-Fシリーズにおけるクロスサイトリクエストフォージェリの脆弱性

https://www.ipa.go.jp/security/vuln/CVE.html

JVN iPediaの例 （https://jvndb.jvn.jp/）

脆弱性情報を活用したセキュリティ対策

1. 情報の収集と絞り込み
   - 脆弱性情報から、自組織のシステムに関連する情報を抽出

2. 脆弱性の危険度（深刻度）を確認
   - CVSS値、攻撃状況の確認

   ※ CVSS値：Common Vulnerability Scoring System値
   - 脆弱性の深刻さを客観的に評価する値（最大10.0）
   - CVSS値7.0～8.9は重要レベル、9.0～10.0は緊急レベルの脆弱性を意味する

   （例）CVE-2017-0145(WannaCryが利用した脆弱性）のCVSS = 9.3

3. 自組織システムへの影響を分析
   - リスクの評価
     - 脆弱性の深刻度 ⇔ 対象システムの重要性 → 緊急対応？ 後で対応？

脆弱性情報の収集 と 絞り込み → 脆弱性の危険度を確認 → 自組織への影響を分析 → 脆弱性への対応

脆弱性検査

- サイバー攻撃による被害を未然に防ぐ為、既知の脆弱性情報を元に、自システムの脆弱性の有無を検査すること。

- 実施のタイミング
  - システム導入時
  - 運用開始後（PCI-DSSでは 四半期毎の実施を規定）

- 脆弱性検査の種類
  - システム セキュリティ検査
    - システムを構成するソフトウェア(OS, サーバ等)における既知の脆弱性の有無を検査
  - ウェブ セキュリティ検査
    - ウェブサイトを構成するソフトウェア(php,CGI等)の脆弱性の有無を検査
  - 疑似侵入テスト（ペネトレーションテスト）
    - 攻撃者が実際に侵入できるかどうかを検査

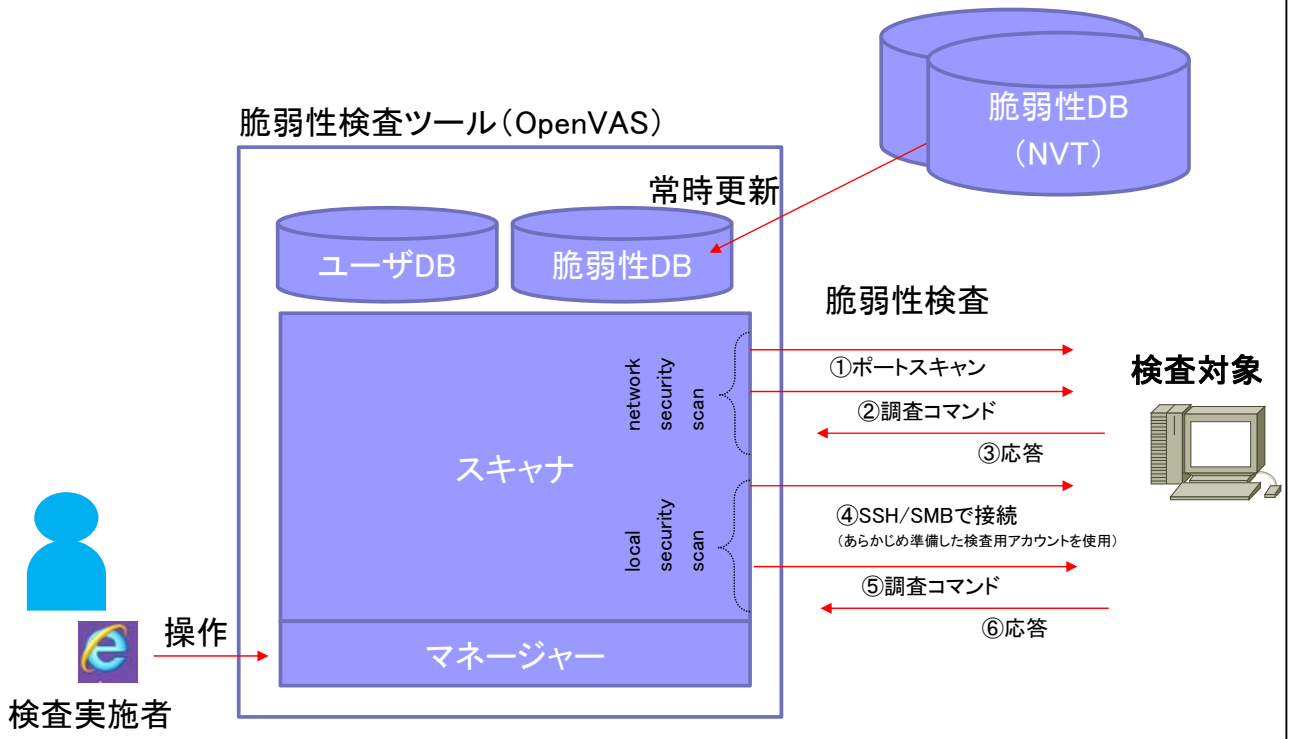
脆弱性検査ツールの例（無償版）

- システム セキュリティ検査
  - Vuls
    - 脆弱性関連情報の収集と検知を自動化する脆弱性検知ツール
    - SSHで接続し検査対象の内部から検査を実施。検査対象はLinux/FreeBSD系サーバ
    - https://vuls.io/en/
  - OpenVAS
    - Nessusを元にしたオープンソースな脆弱性検知ツール
    - ネットワーク経由の検査。検査対象をポートスキャンし、ネットワーク的な脆弱性を検査さらに、SSH(Linux系)/SMB(Widows系)で接続し検査対象の内部から検査可能
    - 検査対象は、Linux/Windows系サーバ
    - http://www.openvas.org/

- ウェブ セキュリティ検査
  - OWASP ZAP
    - 「クロスサイトスクリプティング」「SQLインジェクション」など、WEBアプリケーションの代表的な脆弱性の診断が可能
    - https://www.owasp.org/index.php/Main_Page

- 疑似侵入テスト（ペネトレーションテスト）
  - Kari Linux
    - 250を超えるペネトレーションテスト用ソフトウェアがインストールされたLinux
    - https://www.kali.org/

脆弱性検査ツールの構成（OpenVAS）



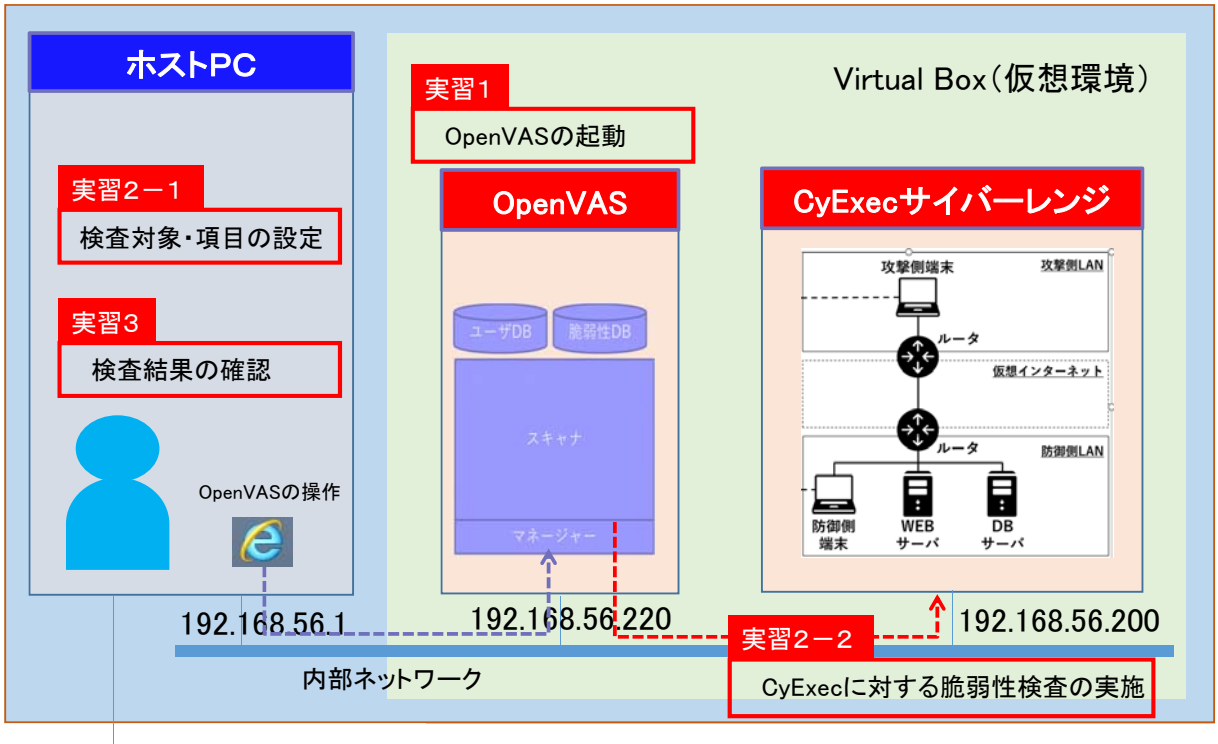
検査可能な項目

- スキャンレベルの設定
  - Full and fast (default)
    - 開いているポートに対する標準的な脆弱性の検査。但し被検査機器にダメージを与えない項目のみ。
  - Full and fast ultimate
    - 開いているポートに対する脆弱性の検査。サービス停止やシャットダウンを伴う可能性がある。
  - Full and very deep
    - 開いているポートに対する脆弱性の検査に加え、脆弱性DB（NVT）に掲載されている全ポートに対して脆弱性を検査。但し被検査機器にダメージを与えない項目のみ。
  - Full and very deep ultimate
    - 開いているポートに対する脆弱性の検査に加え、脆弱性DB（NVT）に掲載されている全ポートに対して脆弱性を検査。サービス停止やシャットダウンを伴う可能性がある。

- 例：Full and fastの検査項目
  - Brute force attacks
    - ncrack(オンライン パスワード クラッキング ツール)によるテスト
    - phrasen/drescherによるテスト
  - Gain a shell remotely
  - Buffer Overflow
  - etc.

2. 実習

実習概要


ホストPC
実習2－1
検査対象・項目の設定
実習3
検査結果の確認
OpenVASの操作
実習1
OpenVASの起動
Virtual Box（仮想環境）
OpenVAS
ユーザDB
脆弱性DB
スキャナ
マネージャー
CyExecサイバーレンジ
攻撃側端末
攻撃側LAN
ルータ
仮想インターネット
ルータ
防御側LAN
防御側端末
WEB サーバ
DB サーバ
192.168.56.1
192.168.56.220
192.168.56.200
実習2－2
CyExecに対する脆弱性検査の実施
内部ネットワーク
PC教室LAN

3. 事例紹介

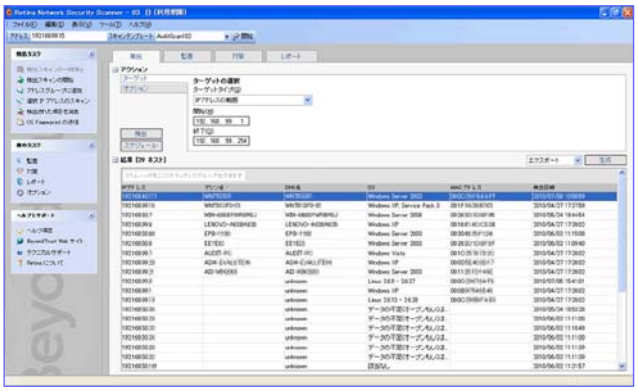
明治大学における脆弱性検査

脆弱性検査の対象機器

- インターネットから接続可能な機器（レベル3機器）
  - 申請時
    - NW管理部門は申請機器に対し、脆弱性検査を実施。
    - 申請者は、発見された脆弱性への対応を行う。
    - NW管理部門は、脆弱性への対応確認後、申請機器をインターネットから接続可能となるよう、FWやDNSの設定を行う。
  - 運用後（不定期）
    - 稼働中の機器に対し、申請時と同様の脆弱性検査を行う。

脆弱性検査ツール

- BeyondTrust Network Security Scanner
  - 攻撃コードを実行することなく高精度な診断が可能
  - 日本語レポート出力可能



発見される主な脆弱性（申請時）

- 脆弱性のあるOS,アプリケーション
  - バージョンアップで対応
- アカウント管理
  - 弱いパスワード
- 弱い暗号方式
  - SSLv2, v3　3des-cbc, aes128-cbc　MD5,　SHA-1
- 不必要な情報の公開
  - ディレクトリ、バージョン番号、管理者用情報
- 不要なポート、不要なサービス
  - SMB

➢ 実のところ、最近はOS,ミドルウェアの自動アップデートがされていることが多く、脆弱性検査にひっかかることはほとんどない

➢ 特に、脆弱性検査だけを見るとWindowsServerの方が優秀で、ほとんどの場合指摘事項は無し

脆弱性検査の課題（運用開始後）

- 事務的な負担
  - 検査スケジュールの事前調整
  - 各検査対象機器のイベント管理
    - レポート送付⇒対処報告
    - 検査スケジュール変更要望、再チェック要望への対応
  - クラウド。事前の申請や時間指定への対応
  - 集計作業
- サポートの負担
  - 発見された脆弱性への対処方法に関するサポート
- 寡黙なPCへの対応
  - pingに応答しないPCは、そもそも電源が入っていない可能性がある
  - tarpitやハニーポット
- ブロードバンドルータの存在
  - ブロードバンドルータの背後にあるPCの脆弱性チェックは不可
- Linuxディストリビュータによる脆弱性対応
  - ディストリビュータが行う脆弱性対応と、検査で発見された脆弱性との一致確認の手間がかかる
- 誤検知
  - バージョン誤り
- 脆弱性が発見された場合の緊急措置
  - 対処されるまでの間、マシンのアクセスレベルを変更するか？

脆弱性検査の効果（運用開始後）

- 管理者の意識・技術の向上
  - 最新セキュリティ事情の再学習のきっかけに
- 機器の棚卸
  - （インターネットからの接続が）不要になった機器の洗い出し
- 運用開始後の変更作業へのフォロー
  - 検査通過後に行った変更（別ポートの開放やサービスの追加等）をチェック

⇒ 定期的な脆弱性検査は必須

参考文献

1. 「脆弱性対策の効果的な進め方（実践編）第二版」,IPA, 2019.2
https://www.ipa.go.jp/files/000071660.pdf

2. 「脆弱性対策の効果的な進め方（ツール活用編）」,IPA, 2019.2
https://www.ipa.go.jp/files/000071584.pdf

セキュリティ インシデント 分析コースのまとめ

A-1. サイバー攻撃と防御・インシデント対応

- SQLインジェクション攻撃による情報漏洩
- 痕跡調査
- インシデント報告書の作成

・脆弱性を抱えたシステムのリスクを理解
・サイバーレンジを用いた演習の有用性

自組織でのCSIRT要員育成に！
CyExecを自校でご利用になりたい方はご連絡ください

A-2. システムの脆弱性の点検と対策

- サイバー攻撃の事前対策として有用な、脆弱性検査
- 脆弱性検査の活用事例紹介

・日々報告される新たな脆弱性
・脆弱性の発見→攻撃実行までの時間は短い

自組織システムの脆弱性の早期把握、対策の実施を！