

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

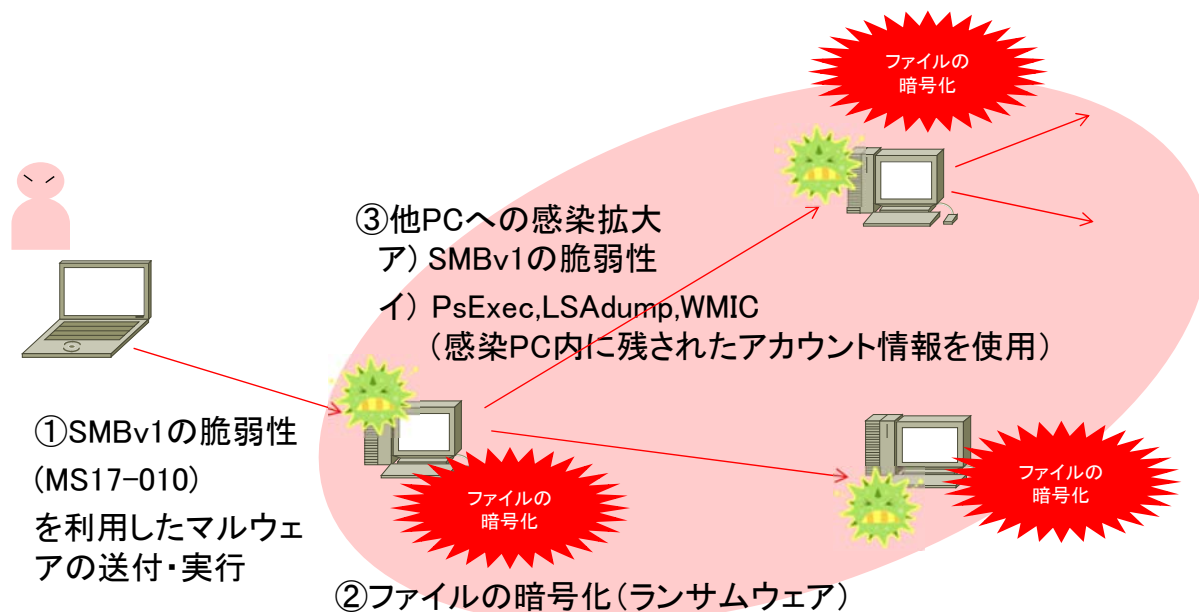
システムの脆弱性をついたインシデント(1)

- 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,秩父観光ナビ,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(びあ)
 - 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
 - ネットにつないた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

JVN iPediaの例 (https://jvndb.jvn.jp/)

最終更新日: 2019/07/16
現在の登録件数: 103230件
JVN iPedia
脆弱性対策情報データベース

JVN iPediaにようこそ
JVNに掲載される脆弱性対策情報のほか、国内外問わず日々公開される脆弱性対策情報のデータベースです。
ご利用されている製品の脆弱性対策情報の収集にご活用ください。具体的な活用方法については、[脆弱性対策情報データベース検索](#)

脆弱性対策情報データベース検索

お知らせ

JVN iPediaで注目されている脆弱性
集計期間: 2019/07/07 - 2019/07/13

- JVNDB-2019-000043
【ひかり電話ルーター/ホームゲートウェイにおける複数の脆弱性】
- JVNDB-2019-000045
【アクセス解析CDI An-Analyzer における複数の脆弱性】
- JVNDB-2019-005975
【Pulse Secure Pulse Connect Secure および Pulse Policy Secure

新着情報 RSS データフィード

最終更新日	データベース登録番号	タイトル	CVSSv3
2019/07/16	New JVNDB-2019-000048	WordPress 用プラグイン WordPress Ultra Simple Paypal	4.3 (低危)
2019/07/16	New JVNDB-2019-000047	サイボウズ Garoon における複数の脆弱性	4.9 (低危)
2019/07/16	New JVNDB-2018-015858	GitLab における入力検証に関する脆弱性	5.3 (低危)
2019/07/16	New JVNDB-2018-015857	GitLab EE におけるクロスサイトスクリプティングの脆弱性	5.4 (低危)
2019/07/16	New JVNDB-2018-015856	GitLab EE における認可に関する脆弱性	6.5 (低危)
2019/07/16	New JVNDB-2018-015855	GitLab CE/EE におけるサーバーサイドのリクエストフォージェリの脆弱性	7.7 (中危)

脆弱性情報を活用したセキュリティ対策

- 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
- 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
- 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

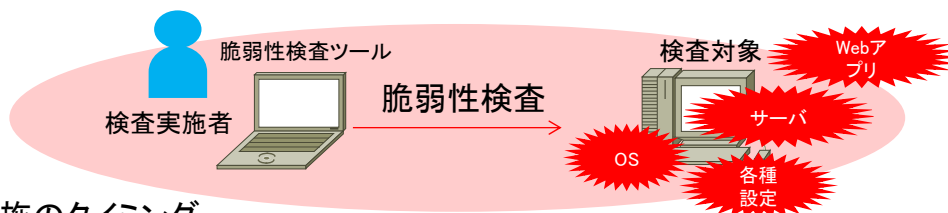
脆弱性の危険
度を確認

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。

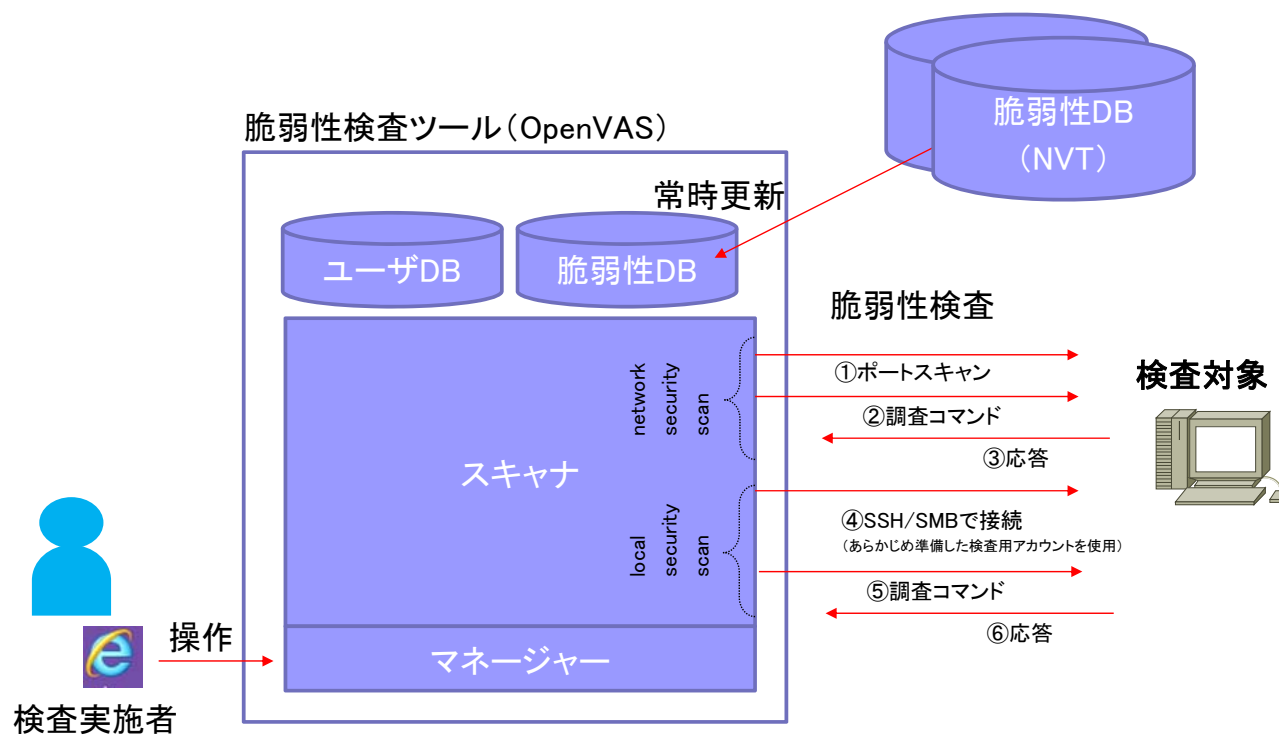


- 実施のタイミング
 - システム導入時
 - 運用開始後(PCI-DSSでは 四半期毎の実施を規定)
- 脆弱性検査の種類
 - システムセキュリティ検査
 - システムを構成するソフトウェア(OS, サーバ等)における既知の脆弱性の有無を検査
 - ウェブセキュリティ検査
 - ウェブサイトを構成するソフトウェア(PHP, CGI等)の脆弱性の有無を検査
 - 疑似侵入テスト(ペネトレーションテスト)
 - 攻撃者が実際に侵入できるかどうかを検査

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(Windows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)
 - Kali 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

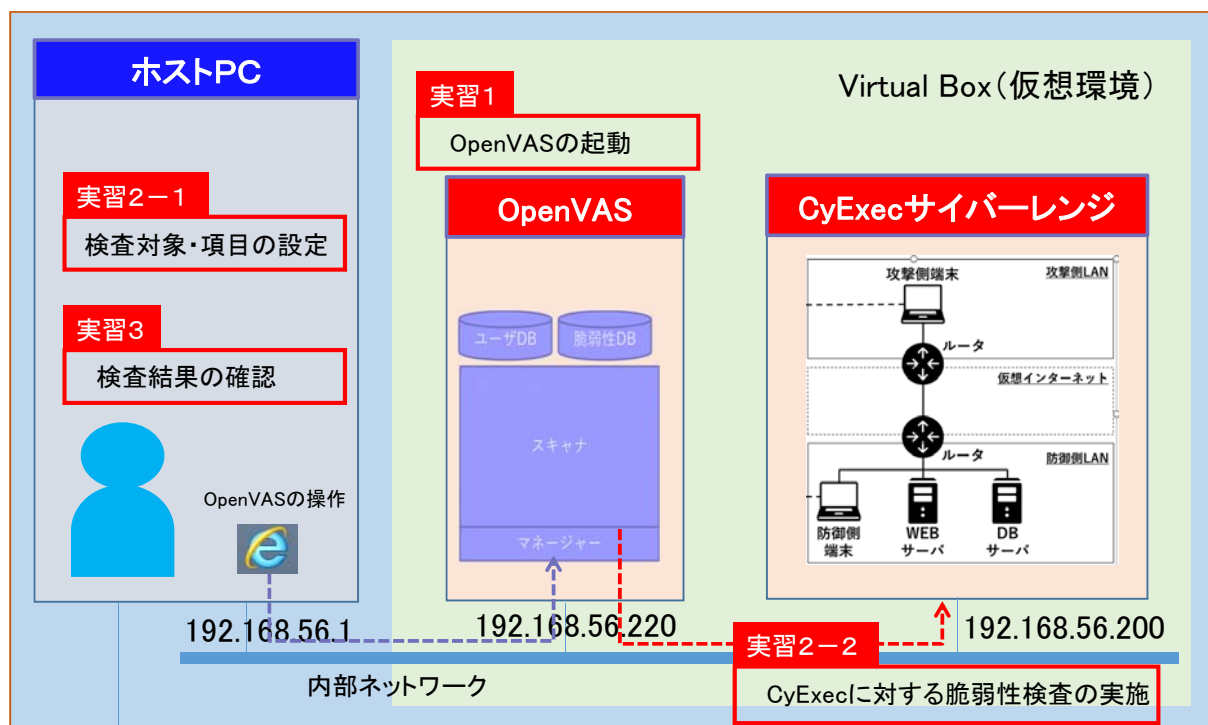
- Full and fast (default)
 - 開いているポートに対する標準的な脆弱性の検査。但し被検査機器にダメージを与えない項目のみ。
- Full and fast ultimate
 - 開いているポートに対する脆弱性の検査。サービス停止やシャットダウンを伴う可能性がある。
- Full and very deep
 - 開いているポートに対する脆弱性の検査に加え、脆弱性DB (NVT) に掲載されている全ポートに対して脆弱性を検査。但し被検査機器にダメージを与えない項目のみ。
- Full and very deep ultimate
 - 開いているポートに対する脆弱性の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



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。

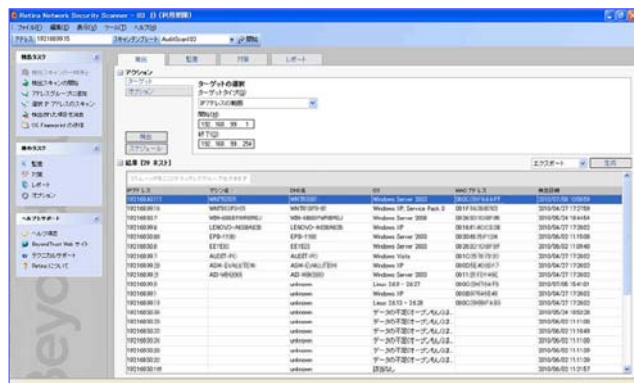
□ 運用後(不定期)

- 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



Microsoft Office のセキュリティ更新 - 2017年7月 - 3213537 Excel 2013

更新	更新	更新	更新	更新
62564	成功	62563	成功	62562
62561	成功	62560	成功	62559
62558	成功	62557	成功	62556
62555	成功	62554	成功	62553
62552	成功	62551	成功	62550
62549	成功	62548	成功	62547
62546	成功	62545	成功	62544
62543	成功	62542	成功	62541
62540	成功	62539	成功	62538
62537	成功	62536	成功	62535
62534	成功	62533	成功	62532
62531	成功	62530	成功	62529
62528	成功	62527	成功	62526
62525	成功	62524	成功	62523
62522	成功	62521	成功	62520
62519	成功	62518	成功	62517
62516	成功	62515	成功	62514
62513	成功	62512	成功	62511
62510	成功	62509	成功	62508
62505	成功	62504	成功	62503
62502	成功	62501	成功	62500
62499	成功	62498	成功	62497
62496	成功	62495	成功	62494
62493	成功	62492	成功	62491
62488	成功	62487	成功	62486
62485	成功	62484	成功	62483
62482	成功	62481	成功	62480
62479	成功	62478	成功	62477
62476	成功	62475	成功	62474
62473	成功	62472	成功	62471
62470	成功	62469	成功	62468
62467	成功	62466	成功	62465
62464	成功	62463	成功	62462
62461	成功	62460	成功	62459
62458	成功	62457	成功	62456
62455	成功	62454	成功	62453
62452	成功	62451	成功	62450
62449	成功	62448	成功	62447
62446	成功	62445	成功	62444
62443	成功	62442	成功	62441
62440	成功	62439	成功	62438
62437	成功	62436	成功	62435
62434	成功	62433	成功	62432
62431	成功	62430	成功	62429
62428	成功	62427	成功	62426
62425	成功	62424	成功	62423
62422	成功	62421	成功	62420
62419	成功	62418	成功	62417
62416	成功	62415	成功	62414
62413	成功	62412	成功	62411
62410	成功	62409	成功	62408
62407	成功	62406	成功	62405
62404	成功	62403	成功	62402
62401	成功	62400	成功	62399
62396	成功	62395	成功	62394
62393	成功	62392	成功	62391
62388	成功	62387	成功	62386
62385	成功	62384	成功	62383
62382	成功	62381	成功	62380
62379	成功	62378	成功	62377
62376	成功	62375	成功	62374
62373	成功	62372	成功	62371
62370	成功	62369	成功	62368
62367	成功	62366	成功	62365
62364	成功	62363	成功	62362
62361	成功	62360	成功	62359
62358	成功	62357	成功	62356
62355	成功	62354	成功	62353
62352	成功	62351	成功	62350
62349	成功	62348	成功	62347
62346	成功	62345	成功	62344
62343	成功	62342	成功	62341
62340	成功	62339	成功	62338
62337	成功	62336	成功	62335
62334	成功	62333	成功	62332
62331	成功	62330	成功	62329
62328	成功	62327	成功	62326
62325	成功	62324	成功	62323
62322	成功	62321	成功	62320
62319	成功	62318	成功	62317
62316	成功	62315	成功	62314
62313	成功	62312	成功	62311
62310	成功	62309	成功	62308
62307	成功	62306	成功	62305
62304	成功	62303	成功	62302
62301	成功	62300	成功	62299
62296	成功	62295	成功	62294
62293	成功	62292	成功	62291
62288	成功	62287	成功	62286
62285	成功	62284	成功	62283
62282	成功	62281	成功	62280
62279	成功	62278	成功	62277
62276	成功	62275	成功	62274
62273	成功	62272	成功	62271
62270	成功	62269	成功	62268
62267	成功	62266	成功	62265
62264	成功	62263	成功	62262
62261	成功	62260	成功	62259
62258	成功	62257	成功	62256
62255	成功	62254	成功	62253
62252	成功	62251	成功	62250
62249	成功	62248	成功	62247
62246	成功	62245	成功	62244
62243	成功	62242	成功	62241
62240	成功	62239	成功	62238
62237	成功	62236	成功	62235
62234	成功	62233	成功	62232
62231	成功	62230	成功	62229
62228	成功	62227	成功	62226
62225	成功	62224	成功	62223
62222	成功	62221	成功	62220
62219	成功	62218	成功	62217
62216	成功	62215	成功	62214
62213	成功	62212	成功	62211
62210	成功	62209	成功	62208
62207	成功	62206	成功	62205
62204	成功	62203	成功	62202
62201	成功	62200	成功	62199
62196	成功	62195	成功	62194
62193	成功	62192	成功	62191
62188	成功	62187	成功	62186
62185	成功	62184	成功	62183
62182	成功	62181	成功	62180
62179	成功	62178	成功	62177
62176	成功	62175	成功	62174
62173	成功	62172	成功	62171
62170	成功	62169	成功	62168
62167	成功	62166	成功	62165
62164	成功	62163	成功	62162
62161	成功	62160	成功	62159
62158	成功	62157	成功	62156
62155	成功	62154	成功	62153
62152	成功	62151	成功	62150
62149	成功	62148	成功	62147
62146	成功	62145	成功	62144
62143	成功	62142	成功	62141
62140	成功	62139	成功	62138
62137	成功	62136	成功	62135
62134	成功	62133	成功	62132
62131	成功	62130	成功	62129
62128	成功	62127	成功	62126
62125	成功	62124	成功	62123
62122	成功	62121	成功	62120
62119	成功	62118	成功	62117
62116	成功	62115	成功	62114
62113	成功	62112	成功	62111
62110	成功	62109	成功	62108
62107	成功	62106	成功	62105
62104	成功	62103	成功	62102
62101	成功	62100	成功	62099
62096	成功	62095	成功	62094
62093	成功	62092	成功	62091
62088	成功	62087	成功	62086
62085	成功	62084	成功	62083
62082	成功	62081	成功	62080
62079	成功	62078	成功	62077
62076	成功	62075	成功	62074
62073	成功	62072	成功	62071
62070	成功	62069	成功	62068
62067	成功	62066	成功	62065
62064	成功	62063	成功	62062
62061	成功	62060	成功	62059
62058	成功	62057	成功	62056
62055	成功	62054	成功	62053
62052	成功	62051	成功	62050
62049	成功	62048	成功	62047
62046	成功	62045	成功	62044
62043	成功	62042	成功	62041
62040	成功	62039	成功	62038
62037	成功	62036	成功	62035
62034	成功	62033	成功	62032
62031	成功	62030	成功	62029
62028	成功	62027	成功	62026
62025	成功	62024	成功	62023
62022	成功	62021	成功	62020
62019	成功	62018	成功	62017
62016	成功	62015	成功	62014
62013	成功	62012	成功	62011
62010	成功	62009	成功	62008
62007	成功	62006	成功	62005
62004	成功	62003	成功	62002
62001	成功	62000	成功	61999
61996	成功	61995	成功	61994
61993	成功	61992	成功	61991
61988	成功	61987	成功	61986
61985	成功	61984	成功	61983
61982	成功	61981	成功	61980
61979	成功	61978	成功	61977
61976	成功	61975	成功	61974
61973	成功	61972	成功	61971
61970	成功	61969	成功	61968
61967	成功	61966	成功	61965
61964	成功	61963	成功	61962
61961	成功	61960	成功	61959
61958	成功	61957	成功	61956
61955	成功	61954	成功	61953
61952	成功	61951	成功	61950
61949	成功	61948	成功	61947
61946	成功	61945	成功	61944
61943	成功	61942	成功	61941
61940	成功	61939	成功	61938
61937	成功	61936	成功	61935
61934	成功	61933	成功	61932
61931	成功	61930	成功	61929
61928	成功	61927	成功	61926
61925	成功	61924	成功	61923
61922	成功	61921	成功	61920
61919	成功	61918	成功	61917
61916	成功	61915	成功	61914
61913	成功	61912	成功	61911
61910	成功	61909	成功	61908
61907	成功	61906	成功	61905
61904	成功	61903	成功	61902
61901	成功	61900	成功	61899
61896	成功	61895	成功	61894
61893	成功	61892	成功	61891
61888	成功	61887	成功	61886
61885	成功	61884	成功	61883
61882	成功	61881	成功	61880
61879	成功	61878	成功	61877
61876	成功	61875		

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！