令和6年度医療情報セキュリティ研修 及び
サイバーセキュリティインシデント発生時初動対応支援・調査等事業

【システム・セキュリティ管理者向け研修】
復習コース
～Networkセキュリティ編～

一般社団法人ソフトウェア協会

目的

【目的】

- 本研修では、システム・セキュリティ管理者を対象に、医療機関が直面するサイバー攻撃の脅威を具体的に理解し、実践的なセキュリティ対策を習得することを目的としています。
- 特に、基本的な研修であるため、わかりやすく、かつ実務に役立つ内容に焦点を当てています。

アジェンダ

【アジェンダ】
- サイバーセキュリティフレームワークの概要
- Networkセキュリティでの取り組み
- 特定
  - ネットワークの把握、シャドーITの排除、ネットワーク構成図や一覧表の作成方法、ネットワーク機器の脆弱性管理、ネットワーク機器の脆弱性修正（手順確立）
- 防御
  - ネットワーク機器の脆弱性修正、ネットワーク機器の資格情報の保護、データのバックアップ、安全なInternet接続、攻撃に対抗するためのネットワーク構成
- 検知
  - ネットワーク機器のSyslog
- ガバナンス
  - サイバーセキュリティサプライチェーンリスクの把握
  - サプライチェーンの正常性維持

サイバーセキュリティフレームワークの概要

- NIST（米国国立標準技術研究所）が策定した、組織のサイバーセキュリティリスク管理を体系的に行うためのフレームワーク
- 2024年2月にV2.0へバージョンアップ
- 幅広い組織に対応
- 新たな機能（ガバナンス）が追加

サイバーセキュリティフレームワークの概要

【特定（Identify）】
組織のシステムや、データなどの資産や取り巻く環境を把握し、それらがどのようなリスクにさらされているかを明確にする

【防御（Protect）】
組織の資産を保護するために、様々な技術的な対策を講じる

【検知（Detect】
サイバー攻撃やセキュリティインシデントを早期に検知するための監視システムやプロセスを構築する

【対応（Respond）】
サイバー攻撃が発生した場合に、迅速に対応し、被害を最小限に抑えるための計画と手順を確立する

【復旧（Recover）】
サイバー攻撃による被害から迅速に復旧し、事業の継続性を確保するための計画と手順を確立する

【ガバナンス（Govern）】
組織全体でサイバーセキュリティを管理、可視化する

Networkセキュリティでの取り組み

【特定（Identify）】
組織のシステムや、データなどの資産や取り巻く環境を把握し、それらがどのようなリスクにさらされているかを明確にする

- ネットワークの把握
- シャドーITの排除
- ネットワーク構成図や一覧表の作成方法
- ネットワーク機器の脆弱性管理
- ネットワーク機器の脆弱性修正（手順確立）

Networkセキュリティでの取り組み

【防御（Protect）】

組織の資産を保護するために、様々な技術的な対策を講じる

- ネットワーク機器の脆弱性修正
- ネットワーク機器の資格情報の保護
- データのバックアップ
- 安全なInternet接続
- 攻撃に対抗するためのネットワーク構成

Networkセキュリティでの取り組み

【検知（Detect）】

サイバー攻撃やセキュリティインシデントを早期に検知するため監視システムやプロセスを構築する

- ネットワーク機器のSyslog
- Syslogサーバーへの転送設定

Networkセキュリティでの取り組み

【ガバナンス（Govern）】
組織全体でサイバーセキュリティをどのように管理していくかを決める

- サイバーセキュリティサプライチェーンリスクの把握
- サプライチェーンの正常性維持

特定（Identify）

ネットワークの把握

- 防御対象の特定
  - 部門とベンダーの協力を得て、院内システムのネットワーク構成図を作成する
  - 院内で保有している診療継続に必要な、守るべき資産（サーバー、データー、バックアップ等）を、ネットワーク図にマッピングする
  - RDP接続の有無やSMBファイル共有の状況を把握する
  - 機器のメーカー、型番、OS、ファームウェアのバージョンを把握し、一覧表を作成する

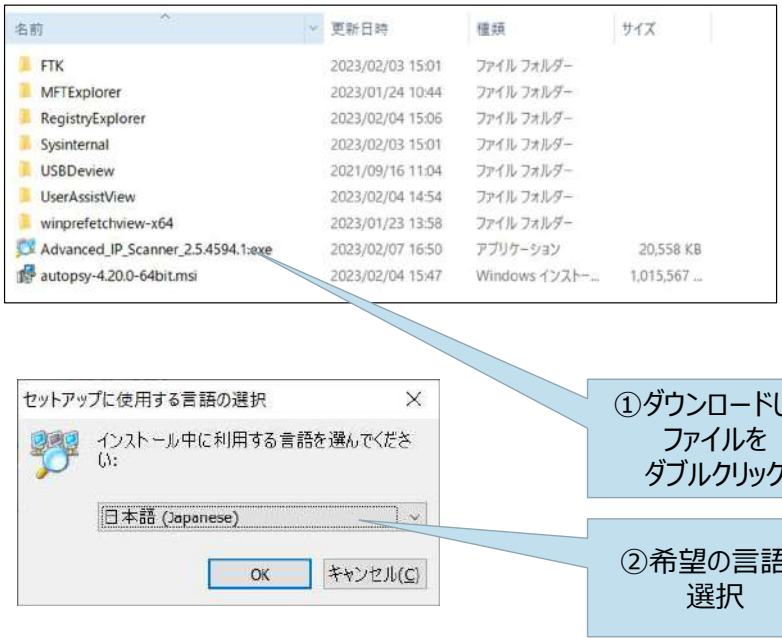
シャドーITの排除

- シャドーITとは
  - システム管理者の承認を得ずに「部門で独自に導入した機器やネットワーク等」
  - 保守目的で外部接続機器を設置するケースが散見される
- シャドーITの課題
  - 脆弱性対策が行われない可能性がある
  - 脆弱な推測しやすい ID/パスワードが使用される可能性がある
  - 接続元 IP アドレス制限が困難な、サポート期間が短い民生品が導入される可能性がある
  - 不要なポートが開いている、脆弱なプロトコルが使用される可能性が高まる
- 検出方法
  - セグメントごとにAdvanced IP Scanner でホストを検出する
  - ネットワーク構成図にない IP、ホストが存在した場合、ポートスキャンを実施し使用用途を調査する

ネットワーク構成図や一覧表の作成方法

- ベースとなる IP アドレスの調査
  - 無償ツールの活用「Advanced IP Scanner」
    https://www.advanced-ip-scanner.com/jp/help/
  - 調査したい IP アドレスの範囲を設定し、[スキャン] ボタンをクリックするだけで、指定したセグメントに接続されている機器の IP アドレスとコンピューター名の一覧が自動作成されCSV 形式でも保存できる
  - 同時に、Web サーバーや RDP の受け入れ状態、SMB ファイル共有などの外部に提供しているサービスが表示される

Advanced IP Scanner インストール方法



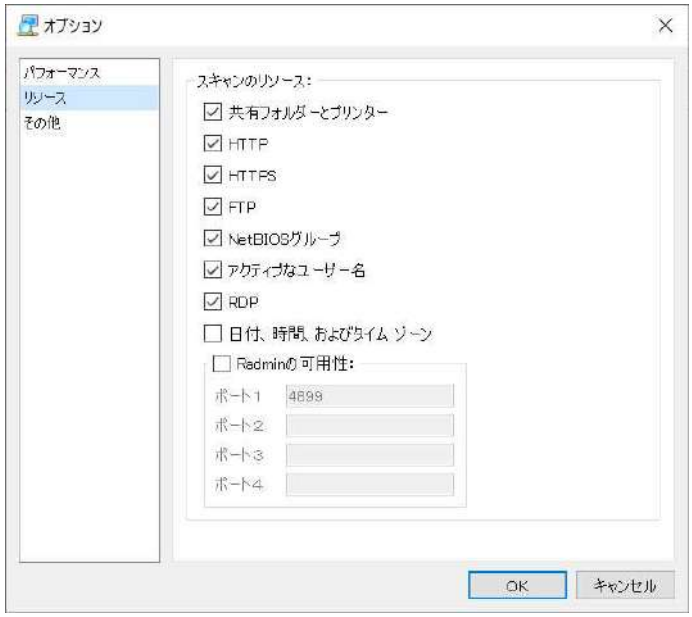
①ダウンロードしたファイルをダブルクリック

②希望の言語を選択

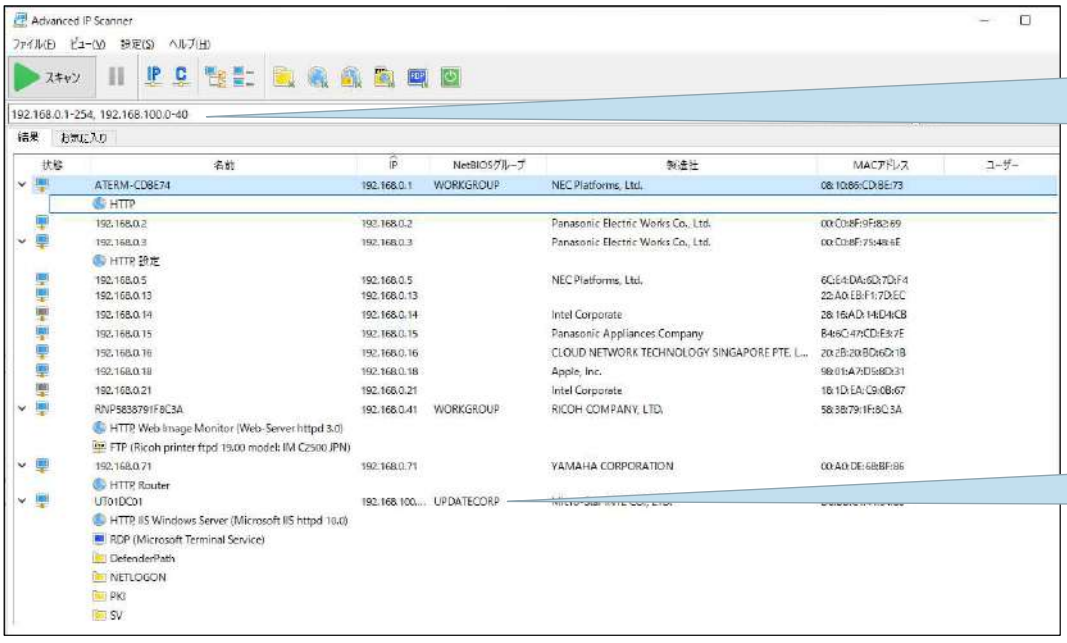
③実行を選択するとインストールなしで、すぐに実行できる

Advanced IP Scanner のオプション

- 以下のポートの有無を調査します
  - 共有フォルダーとプリンター
  - HTTP
  - HTTPS
  - FTP
  - NetBIOSグループ（ドメインやワークグループ名）
  - アクティブなユーザー名
  - RDP
- 検索結果の保存形式
  - html
  - xml
  - csv



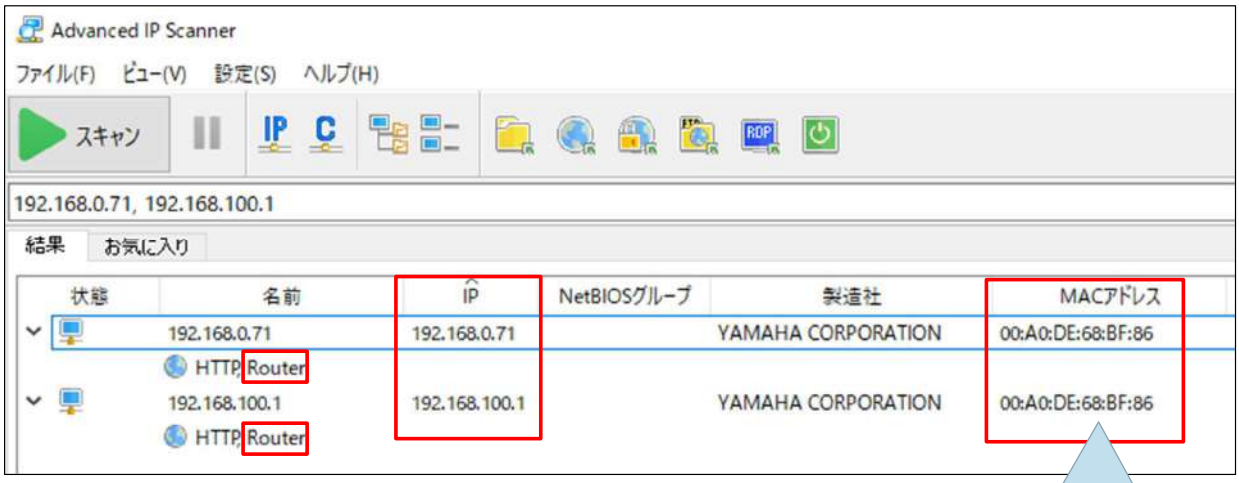
Advanced IP Scanner の実行例



調査したい IP、アドレスの範囲を入力してスキャンボタンをクリック
192.168.0.1-254,
192.168.100.0-40

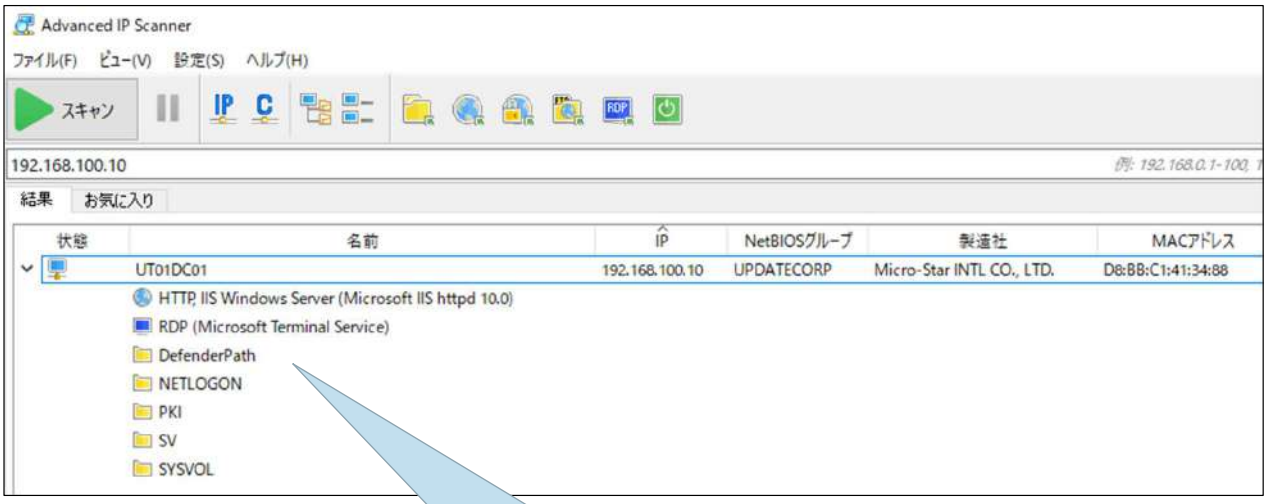
ドメインやワークグループなども表示される

ルーターの場合



MACアドレスが同じなので、
192.168.0.71が含まれるセグメントと
192.168.100.1が含まれるセグメント
をルーティングしているのが分かる

ドメインコントローラーの場合



アイコンをクリックすると、Web サイト
やフォルダが表示され、確認が可能

ネットワーク機器の脆弱性管理

- インターネットと接続しているネットワーク機器の脆弱性管理
  - インターネット側の攻撃者から、ネットワーク機器の脆弱性を悪用されると、院内ネットワークに侵入される恐れがある
  - ネットワーク構成図をもとに、部門、ベンダーの協力を得て、脆弱性情報の入手先、脆弱性修正の基準、脆弱性修正の手順を平常時に策定しておく
- RDP 接続や SMB ファイル共有の管理
  - RDP 接続はランサムウェアに悪用されるため、推測されにくいID/パスワードの利用を確認する
  - SMB ファイル共有はランサムウェアによって暗号化されるため、アクセス制御されているかを確認し、Everyone などは原則禁止する

ネットワーク機器の脆弱性修正（手順確立）

- 脆弱性修正手順書の作成をベンダーに依頼する
  - 脆弱性修正プログラムのダウンロード場所
  - ダウンロードした修正プログラムの完全性チェックのための Hash の検証方法
  - 修正プログラムの適用方法
  - 動作テストの実施方法
  - 不具合発生の場合、設定情報のバックアップからの切り戻し方法

ネットワーク機器の脆弱性修正（手順確立）

- 動作テストの内容（ベンダーと検討する）
  - 設定情報の確認
    （IPアドレス、サブネットマスク、ゲートウェイアドレス、アクセス制御リスト等）
  - ping、traceroute、ポートスキャン等による、ネットワークの到達性や接続性
  - 冗長構成、負荷分散を行っている場合、通常運用の影響を考慮しながら、障害テストを実施する
  - 時刻同期、SNMP、Syslog などの運用設定も確認する
  - 設定情報のバックアップが正常に取得できるか確認する

防御（Protect）

ネットワーク機器の脆弱性修正

- 現状構成の設定情報のバックアップを取得する
  - 平時に現在の構成における設定情報のバックアップを取得する
  - 設定情報のバックアップ取得に関するルールを策定する（いつ、誰が、どのような手順等）
- 脆弱性の修正
  - 作成された手順書に従い脆弱性の修正を実施する
  - 動作テストも忘れずに実施し、問題なければ設定情報のバックアップの取得を実施する

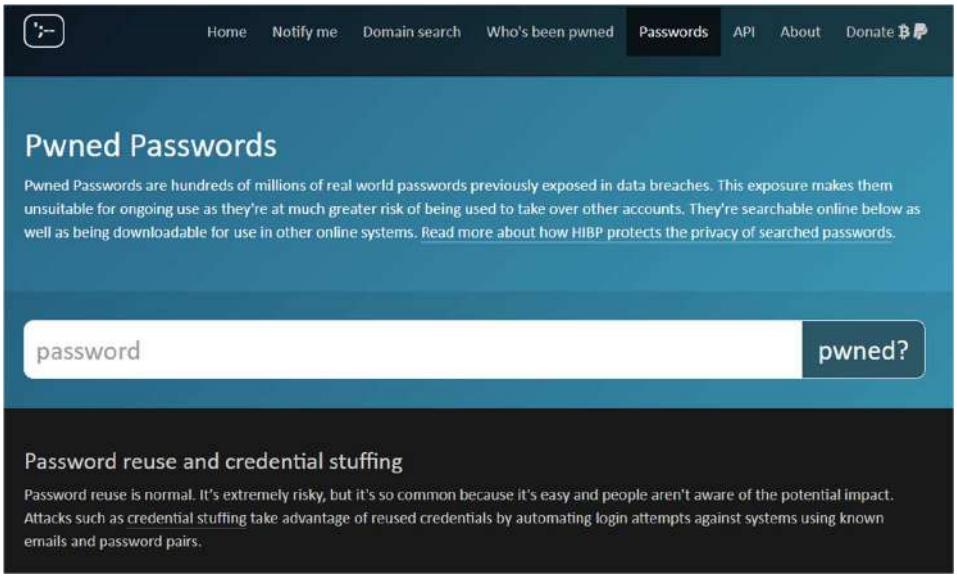
ネットワーク機器の資格情報の保護

- 推測されやすい資格情報の特徴
  - ID：
    組織名01、組織名02、Administrator、Admin、root
  - パスワード：
    P@ssw0rd、pass、1qaz2wsx
- Firewall、VPN装置、ルーターの資格情報の保護
  - ID：
    Admin などの共通 ID を使用させない
    ベンダーを含め接続者全員のIDをユニークにする
  - PW：
    出荷時設定のパスワードは必ず変更する
    長いパスフレーズの使用を強制する
    https://haveibeenpwned.com/Passwords 等で定期的に漏洩のチェックを行う

実際の攻撃で試行されたパスワードリスト

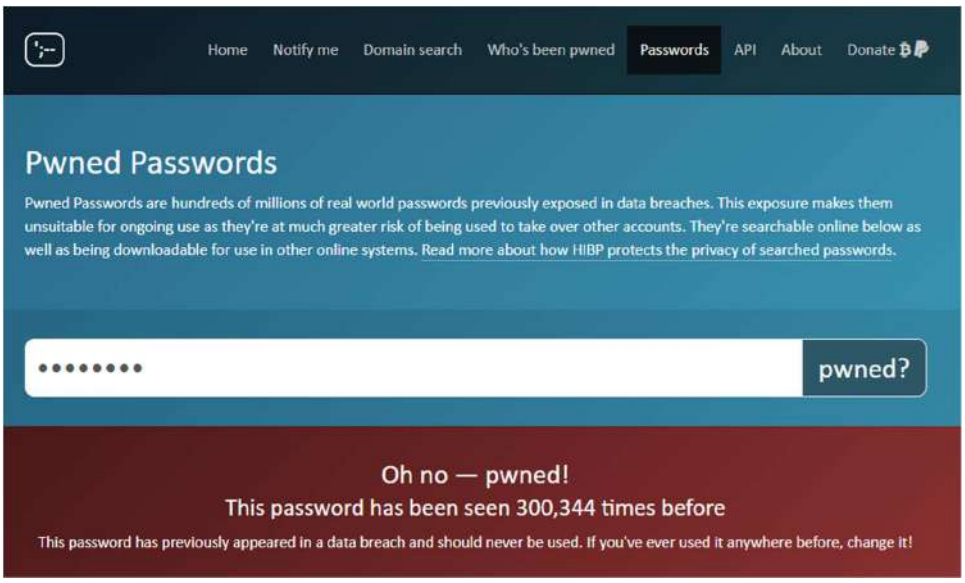
P@ss2020	!qaz@WSx4	1q2w3e1q3e2w	!QAZxsw2	12345678
P@ssw0rd	123456	Passw0rd5	!QAz@wsx1	p@ssword0101
P@ssword	123Abc!	!@12QWqwASas	P@$$w0rd1	Welcome2020!
p@ssword	P@ssw0rd@2020	qwe123QWE	1qaz!@#$	Admin@321
P@SSw0rd	Pass@word	!qaz@WSX4	!QAZ2wsx	!Qaz@wsx3
p@ssw0rd	P@SSw0rd2022!	PassworD123	!QAZ@Wsx3	1qazxsw2@20
P@ss0wrd	P@ssw0rd0	!qaz@wsx3	!qaz@Wsx2	qwe123!@#
P@ss2021	Password@1234	1qazxsw2@22	!QAZ@Wsx4	P@ssw0rd123456
P@ss2022	pa$$w0rd	!qaz@wsx	abc!@#	admin#DSC2022
!qaz@WSx1	p@ssword01	P@$$W0RD	1234	admin@321
admin#DSC2020	Pa$$wOrd12	P@ssw0rd@2023	1q2w3e4rT	!qaz@WSX1
admin#DSC	!QAZ@wsx	P@ssword1	!@#123admin	Password888$
P@ssw0rd123456	!QAZ@WSX3	1q2w3e4r5T	!Qaz@wsx	1qazxsw2+
P@ssw0rd--	!Qaz@wsx1	1qaz2wsx	!password1	admin@123
!QAz@wsx3	Password$1	!QAZ@Wsx	Pa$$word	123qwe!@#
P@ss@1234	P@ssw0rd@2019	!QAZ@wsx4	Qwe123!@#	Aa@12356
admin	!qaz@Wsx4	Passw0rz	!@123qwsazx	P@ssword1234
Zaq123	!QAZ@wsx3	P@ssw0rd123	123456a!	!P@ssw0rd
Pass@2022	P@ssw0rd1	@dmin123	1qaz@WSX	Passw0rd1

漏洩したパスワードの検索サイト



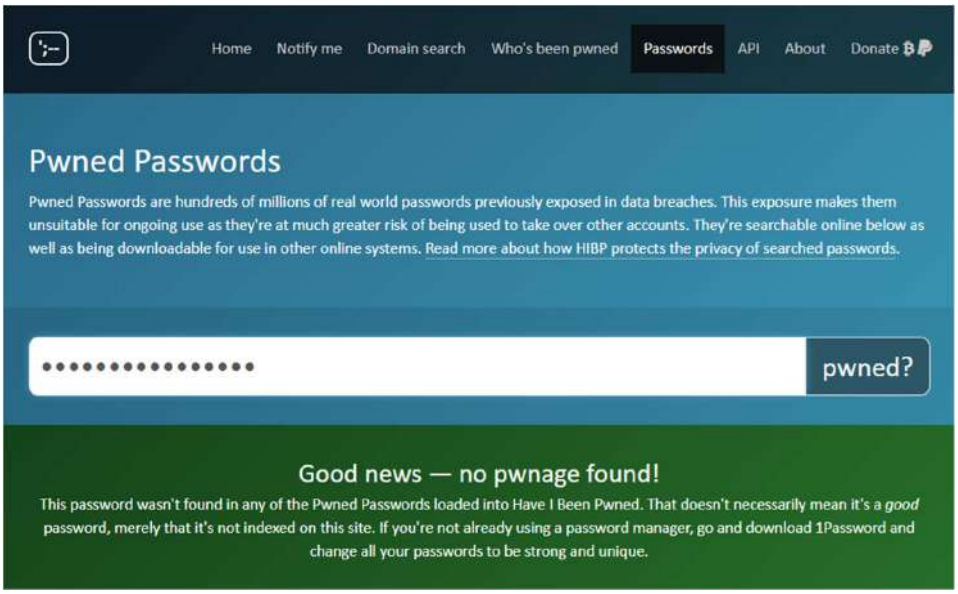
- 過去に攻撃を受けたクラウドシステムやWebサイトから漏洩したパスワードの検索サイト
- 6億1,300万件のパスワードDBを保有
- FBIや英国政府などと協力し、漏洩したパスワードのデータベースとAPIを提供

漏洩したパスワードの検索サイト



- 漏洩したパスワードの場合

漏洩したパスワードの検索サイト



- 漏洩していない場合

データのバックアップ

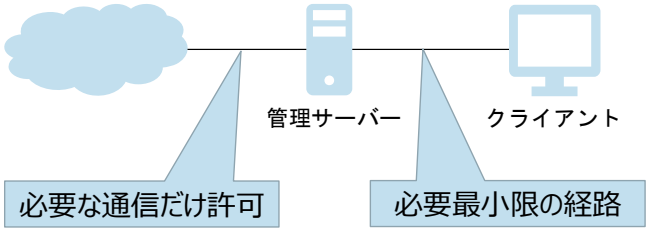
- 3-2-1ルール
  - ３つのバックアップコピー
  - ２つの異なるメディアに保存
  - １つのバックアップコピーはオフサイトに保管
    - 多要素認証による不正アクセスの防止
    - 通信経路でのデータの暗号化
    - Firewall等による不必要な通信の遮断
    - 接続元制限
    - 接続時間制限

安全な Internet 接続

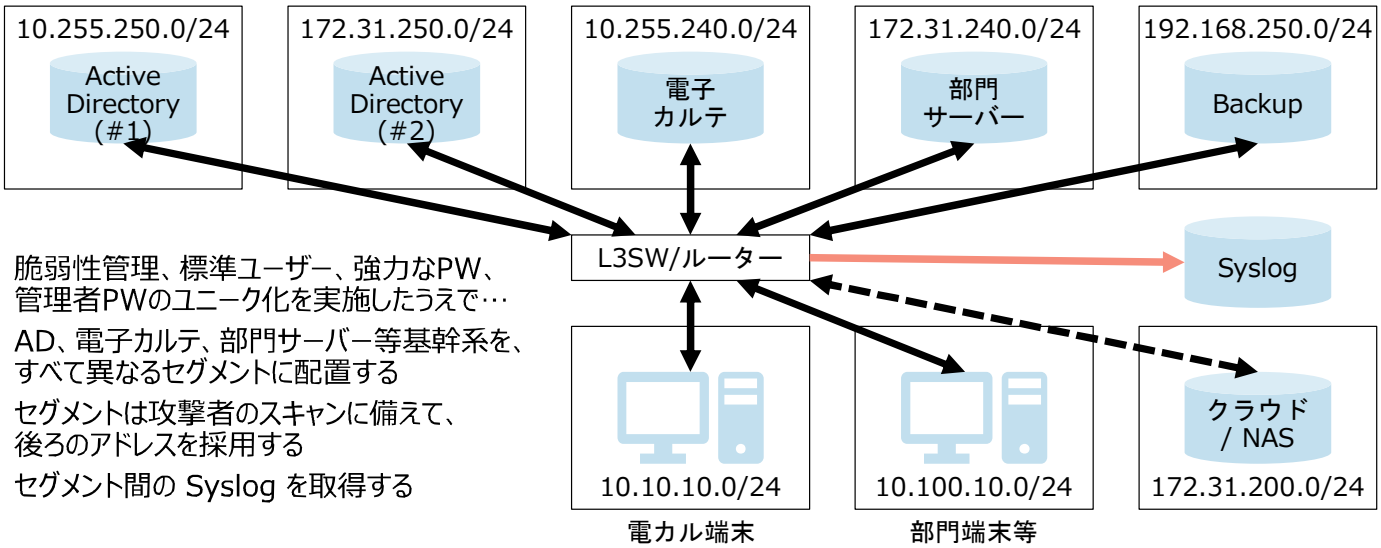
- 安全なメール設定
  - 病院の法人メールアドレスがフィッシングメールに悪用されないようにする
  - メールセキュリティを強化するために、DMARCに対応したメール配信サービス（プロバイダー）を選択し、そのサービスのガイドラインに従って SPF、DKIM、DMARCの設定を行う
    - SPF：送信元メールサーバのIPアドレスが正当なものかどうかを判別
    - DKIM：メールに電子署名することで、 送信者なりすましと改ざんを検証
    - DMARC：SPF、DKIMの認証失敗時の処理を DNS で公開し、受信サーバーに指示
  - フリーメールを利用されている場合は、法人メールアドレスへの移行を推奨
  - 長いパスフレーズや、多要素認証等による認証の強化を実施

安全な Internet 接続

- 不正サイトの名前解決をしない DNS の採用
  - ウイルス配信サイトや、フィッシングサイトの名前解決をしない無償サービスを採用する
  - Quad9、Cloudflare、OpenDNS などがある
- ウイルス対策ソフト（HIS 系も同様です）
  - ウイルス対策ソフトは、定義ファイルの更新だけでなく、エンジンの更新も行う
  - 完全スキャンは、最低でも週1回以上実施する
  - 管理サーバーがある場合、必要最小限の経路設定、必要な通信だけ許可



攻撃に対抗するためのネットワーク構成



- 脆弱性管理、標準ユーザー、強力なPW、管理者PWのユニーク化を実施したうえで…
- AD、電子カルテ、部門サーバー等基幹系を、すべて異なるセグメントに配置する
- セグメントは攻撃者のスキャンに備えて、後ろのアドレスを採用する
- セグメント間の Syslog を取得する

- 図右上のBackupサーバーのデータバックアップを取得する環境が、常時オフラインによるNASへのデータバックアップの場合は、手動でデータバックアップを取得する
- 攻撃は深夜、早朝が多いので、日中のデータバックアップ取得を検討する（接続時間制限の検討）
- データバックアップ取得後、NASの電源はOFFにし、LANケーブルも抜いておく

検知（Detect）

ネットワーク機器のSyslog

- 考え方
  - 攻撃を受けた場合、攻撃元や情報漏洩の有無を判断するには Syslog が極めて重要
  - Firewall、VPN装置 のメモリ上だけでなく、外部の Syslog サーバーに転送設定する
  - 攻撃が長期にわたる可能性があることから、保存期間としては、半年以上を目安にする
  - 継続的なモニタリングを実施し、不正アクセス等の異常な事象が発生していないか監視する
- 設定 （ベンダーと相談してください）
  - Firewall、VPN装置、ルーターの設定に従う
  - Syslogサーバーでログが転送されてきているか確認する
    - 確認できない場合、Syslog クライアントの送信元インターフェースとの疎通を確認する
    - ネットワーク経路上、Syslog が使用する通信ポートが止まっていないか確認する（TCP/UDP 514）
  - ログの時刻を確認する（時刻同期の確認）

Syslogサーバーへの転送設定例

製品	Web GUI	CLI
Cisco ASA	Configuration > Device Management > Logging > Syslog Servers	logging host <interface_name> xx.xx.xx.xx
FortiGate	ログ＆レポート > ログ設定	config log syslogd setting set status enable set server "xx.xx.xx.xx" end
YAMAHA ルーター	管理タブ 保守 > SYSLOGの管理	syslog host xx.xx.xx.xx

- 場合によっては、転送設定だけでなく、事前にロギングを有効にしなければならないものもあります。
- メーカー、機種、バージョンによって設定方法が異なりますので、ベンダーの方に相談をしてください。

ログの種類、重大度（Severity）

ログの種類
アクセスログ
イベントログ
トラフィックログ
認証ログ
システムログ
エラーログ

重大度（Severity）
Emergency
Alert
Critical
Error
Warning
Notification
Information
Debug

- ログの継続的なモニタリング方法とともに、詳細については、ベンダーの方に相談をしてください。

ガバナンス（Govern）

サイバーセキュリティサプライチェーンリスクの把握

- サイバーセキュリティサプライチェーンリスクの把握
  - VPN による医療機器等への保守接続、地域連携、事業者等、サプライチェーンのリスク把握が必要である
  - 各接続先の協力を得て、先方のネットワーク機器のメーカー、型番、OS、ファームウェアのバージョンを把握し、一覧表を作成する
  - ネットワーク機器の脆弱性管理の主体を把握し、責任分界点を明確化する
  - サプライチェーン間の接続手順（RDP、SMBファイル共有など）を把握する

サプライチェーンの正常性維持

- サプライチェーンの正常性維持を契約として求める必要
  - 契約にない項目は、ベンダーの債務にならない
  - 調達仕様書は、抽象的な記述ではなく、具体的な要件を記述する

悪い例	良い例
○○ガイドラインに準拠すること	○桁以上のパスワードにすること
○○セキュリティを強化すること	脆弱性情報の定期的な提供を求める （例：１ヶ月毎）
万全なサポート体制を整備すること	脆弱性修正のための手順書を作成すること

  - 場合によっては、専門家に相談する

サプライチェーンの正常性維持

- ネットワーク接続するベンダーに、都度、接続申請を求める
  - 接続元組織名
  - 接続元責任者名
  - 接続元担当者
  - 接続方法及び接続元 IP アドレス
  - 接続経路
  - 使用機器
  - OS、アプリケーションの名称
  - OS、アプリケーションの脆弱性最終更新日時
  - ウイルス対策ソフト
    定義ファイル、エンジン更新日時
  - 接続目的と接続日時
  - 接続元の正常性の保証表明
  - 保守の場合、作業内容、完了報告

まとめ

- サイバーセキュリティフレームワークの概要
- Networkセキュリティでの取り組み
- 特定
  - ネットワークの把握、シャドーITの排除、ネットワーク構成図や一覧表の作成方法、ネットワーク機器の脆弱性管理、ネットワーク機器の脆弱性修正（手順確立）
- 防御
  - ネットワーク機器の脆弱性修正、ネットワーク機器の資格情報の保護、データのバックアップ、安全なInternet接続、攻撃に対抗するためのネットワーク構成
- 検知
  - ネットワーク機器のSyslog
- ガバナンス
  - サイバーセキュリティサプライチェーンリスクの把握
  - サプライチェーンの正常性維持

ありがとうございました。