

HPワークステーションでシステムセットアップを使用し、トラステッドプラットフォームモジュールを構成する。(スクリーンショットはHPからの許可を得て使用)

ハードウェアRoTの確立に関する問題は、誰もが完全に制御できる環境でデバイスが使用されることです。ハードウェアRoTを支えるファームウェアが侵入不可であるという完全な保証はありませんが、TPMに対する攻撃は、十分に困難なのでほとんどのケースで有効なセキュリティを提供します。

ブート時の完全性

ほとんどのPCとスマートフォンでは、**Unified Extensible Firmware Interface (UEFI)**が実装されています。UEFIはホストがOSを起動するためのコードを提供します。UEFIでは、さまざまなブート時の完全性チェックを強制できます。

セキュアブート

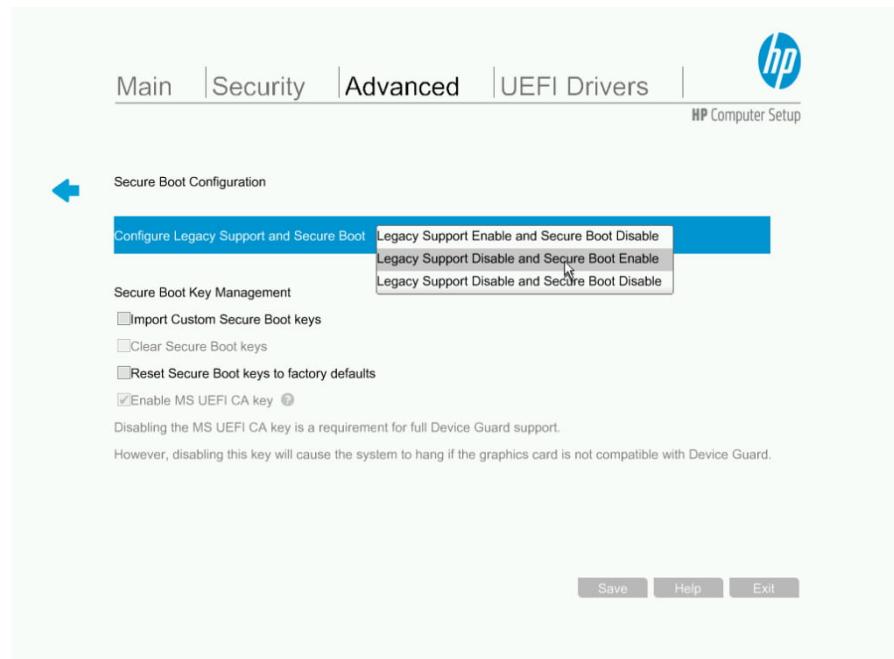
セキュアブートは、悪意のあるOSによるコンピューターのハイジャックを予防するために設計されています。UEFIは有効なOSベンダーからのデジタル証明書で構成されます。システムファームウェアは、保存された証明書を使ってオペレーティングシステムのブートローダーとカーネルをチェックし、OSベンダーがデジタル署名していることを確認します。これにより、マルウェア（または認可なくインストールされたOS）によって変更されたブートローダーやカーネルは使用できなくなります。セキュアブートはWindows (docs.microsoft.com/en-us/windows/security/information-protection/secure-the-windows-10-boot-process)と多くのLinuxプラットフォーム(wiki.ubuntu.com/UEFI/SecureBoot)でサポートされています。セキュアブートではUEFIが必須ですが、TPMは不要です。

メジャーブート

トラステッドブートまたは**メジャーブート**プロセスでは、ブートプロセスの各段階で、TPMのPCR (Platform Configuration Registers)を使用し、主要システムの状態データ（ブートファームウェア、ブートローダー、OSカーネル、重要なドライバー）のハッシュが変更されたかどうかをチェックします。これは通常、起動を防止することはできませんが、署名のないカーネルレベルのコードの存在を記録します。

ブート構成証明

ブート構成証明とは、信頼されるプロセスを介してTPMによって署名されたブートログレポートを、ネットワークアクセス制御サーバーなどのリモートサーバーに送信する機能です。ブートログを分析して、署名のないドライバーの存在などの侵入の兆候を確認することができます。必須の正常性ポリシーを満たさない場合や、構成証明レポートを受信しない場合は、ホストがネットワークにアクセスしないようにできます。



HPワークステーションのUEFIファームウェア設定プログラムを介してセキュアブートの設定を構成する。
(スクリーンショットはHPからの許可を得て使用)

ディスクの暗号化

フルディスク暗号化(FDE)とは、システムファイルやフォルダを含むドライブ（またはボリューム）のコンテンツ全体が暗号化されていることです。脅威アクターがドライブを別のホストOSに接続できる場合、OS ACLベースのセキュリティ対策は、非常に簡単に回避できます。ドライブ暗号化は、正しい暗号化キーと組み合わせなければドライブのコンテンツにアクセスできないようにすることで、このセキュリティ上の懸念を軽減します。ディスクの暗号化はHDD (Hard Disk Drive)とSSD (Solid State Drive)の両方に適用できます。

FDEでは、ドライブコンテンツの暗号化に使用するキーを安全に保管する必要があります。通常これはTPMで保管されます。TPMチップには、ディスク暗号化プログラム（Windows BitLockerなど）がキーを書き込めるセキュアなストレージエリアがあります。USBメモリを使うことも可能です（USBがブートデバイスオプションの場合）。セットアッププロセスの一部として、リカバリパスワードや鍵を作成します。これは、ディスクが別のコンピューターに移動した場合やTPMが損傷した場合に使用できます。



BitLockerドライブ暗号化を有効にする。(スクリーンショットはMicrosoftからの許可を得て使用。)

FDEの欠点の1つは、OSが暗号化操作を実行するため、パフォーマンスが低下することです。この課題は、暗号化操作がドライブコントローラーによって実行される**自己暗号化ドライブ(SED)**により緩和されます。SEDでは、一括暗号化に対称暗号のデータ/メディア暗号化キー(DEK/MEK: Data/Media Encryption Key)を使用します。またDEKを安全に保存するために、認証キー(AK: Authentication Key)やキー暗号化キー(KEK: Key Encryption Key)と呼ばれる非対称キーペアで暗号化します。AKの使用はユーザー/パスワードにより認証されます。これは、ユーザー/パスワードが、ドライブを復号化し、再暗号化する必要なく変更できることを意味します。SEDの初期のタイプでは、プロプライエタリメカニズムを使用していましたが、多くのベンダーは、Trusted Computing Group (TCG)によって開発された**Opalストレージ仕様**(nvmexpress.org/wp-content/uploads/TCGandNVMe_Joint_White_Paper-TCG_Storage_Opal_and_NVMe_FINAL.pdf)に基づいて開発するようになりました。

! 個々のドライブにパスワードを設定することは、数台以上のマシンが関与している場合には非常に困難であるため、企業では鍵管理相互運用プロトコル(KMIP: Key Management Interoperability Protocol)とハードウェアセキュリティモジュール(HSM: Hardware Security Module)を使用して、鍵のプロビジョニングを自動化することができます。[\(trustedcomputinggroup.org/wp-content/uploads/SWG_TCG_Enterprise-Introduction_Sept2010.pdf\)](http://trustedcomputinggroup.org/wp-content/uploads/SWG_TCG_Enterprise-Introduction_Sept2010.pdf)

USBとフラッシュドライブセキュリティ

研究者のKarsten Nohl氏が、BadUSBの論文(srlabs.de/wp-content/uploads/2014/07/SRLabs-BadUSB-BlackHat-v1.pdf)において、USBメモリなどの外部ストレージデバイスのファームウェア(そして潜在的にその他のファームウェアのタイプ)を悪用し、信じがたいツールキットを使用する脅威アクターが提示されています。ファームウェアをプログラムして、デバイスをキーボードなど別のデバイスクラスのように見せることができます。この場合、USBを挿入すると一連のキーストロークを注入したり、キーロガーとして動作させる可能性があります。また、ネットワーク機器のように動作するようにプログラムして、名前解決を破損し、ユーザーを悪意のあるウェブサイトにリダイレクトさせることも可能です。

別の例としてO.MGケーブル(theverge.com/2019/8/15/20807854/apple-mac-lightning-cable-hack-mike-grover-mg-omg-cables-defcon-cybersecurity)があります。これは、普通のUSB-Lightningケーブルに十分な処理機能を詰め込み、アクセスポイントとキーロガーを実行できます。

改ざんされたデバイスには、一般的なUSBドライブやケーブルと区別できる視覚的な手掛かりがあることもあります、見つけ出るのは困難な場合もあります。ユーザーにリスクを警告し、出所が不明なデバイスをコンピューターやスマートフォンに決して接続しないように、アドバイスを繰り返す必要があります。デバイスを疑う場合、デバイスを接続する際に、サンドボックス化されたラボシステム(シープディップと呼ばれる場合があります)で注意深く観察してください。コマンドプロンプトのウィンドウやコマンドインターフェースの起動などのプロセス、レジストリや他のシステムファイルへの変更を確認します。



すべての攻撃が難解なものとはかぎりません。一般的なマルウェアに感染されたUSBスティックは、今でも非常に多く使用される感染要素です。ホストは必ず、USBデバイスが接続される場合に自動実行がされないように構成してください。USBポートは、ほとんどのタイプのホスト型侵入検知システム (Host Intrusion Detection System : HIDS) を使用してすべてまとめてブロックできます。

サードパーティのリスク管理

RoT (Root of Trust : 信頼の起点) は、ベンダーが適切に実装している場合にのみ信頼できます。ハードウェアとファームウェアの脆弱性とエクスプロイトは、サードパーティのリスク管理の必要性を示しています。サプライチェーンとは、商品とサービスの供給、製造、配送、納入に至るまでのエンドツーエンドのプロセスです。例えば、TPMを信頼できるようにするには、チップ製造業者、ファームウェア作成者、OEM小売業者、エンドユーザーへのデバイスの供給を担当する管理スタッフのサプライチェーンすべてが信頼できる必要があります。コンピューターのファームウェアを変更する時間とリソースがある人は、理論的には一種のバックドアアクセスを作成できるのです。同じことが、USBケーブルに至るまでのあらゆる種類のコンピューターまたはネットワークハードウェアに当てはまります。

コンピューター機器に信頼できるサプライチェーンを確立することは、基本的に、供給されようとしている資産に対して、脅威アクターに改ざんする時間やリソースを与えないことを意味します。



ほとんどのビジネスにとって、評判の高いOEMを使用することは、サプライチェーンの保護において最善の実践的な取り組みです。政府、軍事/セキュリティサービス、大企業は、より詳細な調査を行います。中古のマシンを使用する場合は特に注意が必要になります。

サプライヤーのリスクを評価する場合、次の2つのタイプの関係を区別することが役立ちます。

- ベンダー — 汎用的な商品やサービスを提供するサプライヤーで、場合によってはカスタマイズや直接的なサポートを行うこともあります。
- ビジネスパートナー — 2つの会社が共通の目標とマーケティング機会を非常に密接に共有する関係性を示します。

例えば、Microsoftは大手ソフトウェアベンダーですが、すべての潜在的な顧客と直接の関係を確立するのは実現不可能です。市場を拡大するために、OEM（相手先ブランド製造）やソリューションプロバイダーとパートナー関係を構築しています。Microsoftでは、証明書とパートナーのためのトレーニングのプログラムを実施し、製品サポートとセキュリティの認識を高めます。

サポートが終了したシステム

製造業者が製品の販売を終了すると、サポートや予備部品、アップデートの入手が制限される生産終了(EOL: End of Life)段階に入ります。サポート終了(EOSL: End of Service Life)システムとは、開発元やベンダーのサポートが終了したシステムのことです。EOSL製品は、セキュリティアップデートを受けることができないため、使用中の製品が残っている場合、重大な脆弱性を示すことになります。

例えばMicrosoftのサポートライフサイクルポリシーでは、Windowsの各バージョンに5年間のメインストリームサポートと5年間の延長サポートが提供されています（この期間中はセキュリティ更新のみ配信）。特定のWindowsバージョンのサポートステータスについては、support.microsoft.com/en-us/help/13853/windows-lifecycle-fact-sheetで確認できます。

ほとんどのOSベンダーとアプリケーションベンダーには同様のポリシーがあります。オープンソースのソフトウェアでもサポートが必要になります。ソフトウェアがしっかりと管理されている場合、開発グループはLTS (Long Term Support)のバージョンを指定します。その他のビルトやバージョンプランチはアップデートを受け取らないかもしれません。

また、オープンソースのプロジェクトと商用プロジェクトの両方が廃止される可能性もあります。企業がそのようなアバランチウェアに引き続き依存する場合は、その開発責任を負う必要があ

ります。ファームウェアやドライバーに既知の重大な脆弱性があり、修正に関してベンダーのサポートが得られる見込みがなくても市販され続けているアプリケーションやデバイス（特に周辺デバイス）がたくさんあります。この問題は、消費者向けのネットワークアプライアンスやIoTでも見られます。アプリケーションとデバイスのサプライヤーを利用するときは、製品の効果的なセキュリティ管理ライフサイクルがあることを確認することが重要です。

組織的なセキュリティ協定

誰もが基本的にあらゆるサービスや活動をサードパーティに委託できますが、こうしたサービスや活動の法的責任は委託できないことを覚えておいてください。そうしたサードパーティが行うサービスや活動に最終的な責任を負うのはあなたです。サードパーティがあなたのデータやシステムにアクセスできる場合、サードパーティの組織のセキュリティ違反（不正なデータ共有など）は事実上あなたの違反になります。セキュリティリスクの認識、義務の共有、契約上の責任の問題は、正式な法的契約書に記載することができます。一般的な契約書の種類は次のとおりです。

- **覚書（Memorandum of understanding : MOU）** — 連携業務の意図を表明する予備的または試行的な合意。MOUは通常、比較的非公式なものであり、拘束力のある契約として機能するものではありません。ですがMOUはほとんどの場合、両当事者が守秘義務を尊重するべきである旨が記される条項があります。
- **ビジネスパートナーシップ契約書（Business Partnership Agreement : BPA）** — ビジネスパートナーシップを確立する方法はたくさんありますが、ITで最も一般的なモデルは、大手IT企業（MicrosoftやCiscoなど）が再販業者やソリューションプロバイダーと締結するパートナー契約です。
- **秘密保持契約書（Non-disclosure agreement : NDA）** — 情報資産の保護に対する法的根拠。NDAは企業と従業員、企業と請負業者、企業と企業の間で使用されます。従業員または請負業者がこの契約を違反し、当該の情報を共有する場合、法的措置が取られる場合があります。NDAは、従業員や請負業者が雇用者の信頼を破ることを阻止するために有用です。
- **サービスレベル合意書（Service level agreement : SLA）** — サービスが提供される詳細な条件を定めた契約上の合意。
- **測定システム解析（Measurement systems analysis : MSA）** — シックスシグマなどの品質管理プロセスでは、定量化された解析方法を利用して、システムの有効性を判断します。これは、脆弱性や脅威の検知と対応などのサイバーセキュリティ手順に適用できます。MSAは、品質管理プロセスで使用されるデータ収集と統計手法を評価して、それらが堅牢であることを確認する手段です。これは、エンタープライズ企業や政府当局と提携する際の参加要件になる場合があります。

法的な合意は有効ですが、サプライヤー、ベンダー、請負業者がその合意に準拠できることを確認するのはあなた次第です。準拠できない場合、適切に訴訟を起こすことはできますが、相手が倒産する場合、相手の行動や不履行に対する責任はあなたが負うことになります。



逆に言うと、サービスプロバイダーになる場合には、締結する契約の要件とパフォーマンス基準に準拠できることを確認する必要があります。

レビュー アク ティビティ： セキュアなファームウェア

次の質問にお答えください。

1. NAC構成証明のためにTPMはどのように使用されますか。
2. コンピューターやモバイルデバイスが紛失や盗難に遭う場合に、OSで強制されるファイルアクセス制御が十分ではないのはなぜですか。
3. フルディスク暗号化を実施する際、TPMはどのように使用されますか。
4. 悪意のあるファームウェアコードの脅威に対して使用できる対応策は何ですか。
5. 連携して作業を行うことに同意する2社に最適な相互運用性契約書は何ですか。
6. 特定のパフォーマンス基準を確実にするための相互運用性契約書は何ですか。

トピック12B

エンドポイントセキュリティを実装する



対象試験範囲

3.2与えられたシナリオに基づいて、ホストまたはアプリケーションのセキュリティソリューションを実装することができる。

ホストハードウェアの完全性は、そこで実行されるOSとアプリケーションソフトウェアの構成が弱い場合、あまり役に立ちません。あなたはセキュリティプロフェッショナルとして、構成ベースラインの作成、ホストがそれらのベースラインに準拠していることの確認、エンドポイント保護セキュリティエージェントの実装を支援することがよくあります。

ハードニング

オペレーティングシステムやアプリケーションをセキュアな構成にするプロセスは**ハードニング**と呼ばれます。システムのハードニングをすることで、システムのアクセスと機能も制限される可能性があるため、システムのセキュリティを強化する際は、その用途を念頭に置くことが重要です。ハードニングの必要性は、特定の状況でのアクセス要件と使いやすさに対してバランスが取れていなければなりません。

特定の役割で機能するOSの場合、通常はOSとアプリケーションソフトウェアがその役割を実行できるようにセキュアな構成を適用するための、標準的な一連の手順があります。要件の多くは、構成ベースラインテンプレートを介して自動適用できます。基本原則は機能性を最低限にすることです。システムでは、正当なユーザーが必要とするプロトコルとサービスのみが実行され、それ以外は実行されないようにするべきです。これにより、潜在的な攻撃対象領域は減ります。

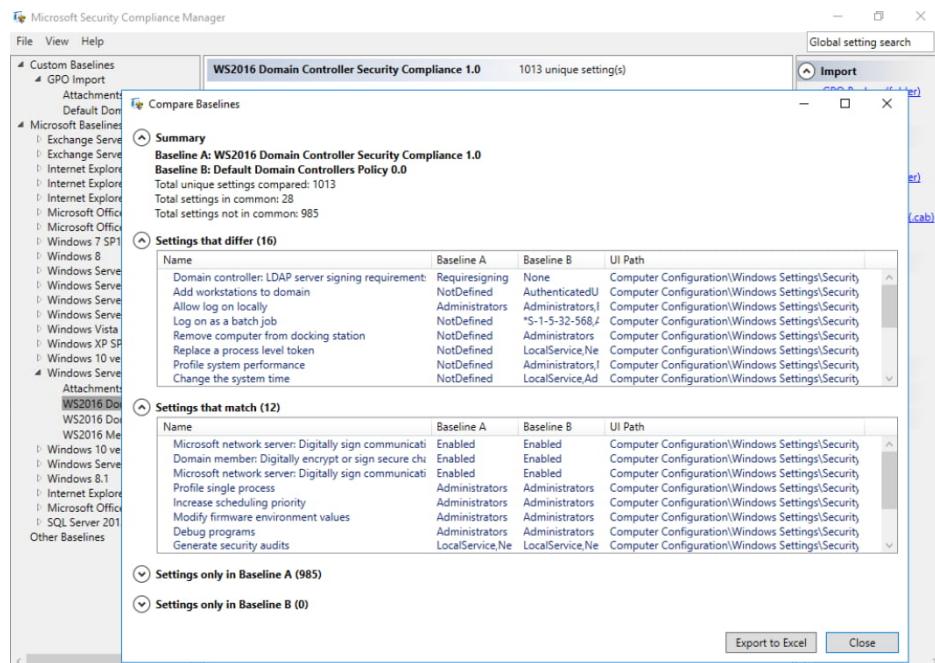
- インターフェイスはネットワークへの接続を提供します。中には、インターフェイスが1つ以上あるマシンもあります。例えば、有線および無線のインターフェイスやモデムインターフェイスがある場合があります。中には、管理ネットワークインターフェイスカードがあるマシンもあります。これらのインターフェイスが不要な場合、使用しないだけではなく、明確に無効にしてください。
- サービスでは、さまざまな種類のアプリケーションに機能のライブラリを提供します。一部のサービスでは、OSとインストール済みのアプリケーションのローカル機能をサポートします。他のサービスでは、クライアントからサーバーアプリケーションまでのリモート接続をサポートします。使用しないサービスは無効にしてください。
- アプリケーションサービスポートを使用すると、クライアントソフトウェアではネットワークを介してアプリケーションに接続できます。リモートアクセスが不要な場合は、ファイアウォールで無効にするか、ブロックしてください。サーバーに規格外ポートが構成されている場合もあるので注意してください。例えば、HTTPサーバーは、80ポートではなく8080ポートを使用して構成されている場合があります。逆に、マルウェアではオープンポートを介して規格外データの送信を試みる場合があります。侵入検知システムは、ネットワークデータが期待されるプロトコル形式に対応していないことを検知する必要があります。
- 永続ストレージでは、アプリケーションによって生成されたユーザーデータと、キャッシュ済みの認証情報を保持します。ディスク暗号化はデータのセキュリティにとって不可欠です。自己暗号化ドライブを使用すれば、すべての保存データを常に安全に保管できます。

また、各デバイスにメンテナンスサイクルを設定し、実行している特定のソフトウェア製品に関する新しいセキュリティの脅威と対応について絶えず最新情報を得ることも重要です。

ベースラインの構成とレジストリの設定

デスクトップクライアント、ファイルおよびプリントサーバー、DNS (Domain Name System)、アプリケーションサーバー、ディレクトリサービスサーバー、ならびにその他各種システムごとに個別の構成ベースラインがあります。Windowsでは、構成設定はレジストリに保存されます。Windowsドメインネットワークの場合、ドメインに参加している各コンピューターは、1つ以上のGPO (Group Policy Objects)からポリシー設定を受領します。こうしたポリシー設定は、コンピューターが起動するたびにレジストリに適用されます。ホストが一元管理され、承認済みのアプリケーションとサービスのみを実行する場合、セキュリティに関するレジストリ値を変更する理由は比較的少ないはずです。レジストリを変更する権限は、最小限の特権に基づいてユーザーとサービスアカウントにのみ発行してください。ホスト型侵入検知システムは、疑わしいレジストリのイベントを警告するように構成できます。

ベースラインからの逸脱のレポートとは、ホストの実際の構成をテストして、その構成設定がベースラインテンプレートと一致していることを確認することを意味します。Windowsネットワークでは、Microsoft Baseline Security Analyzer (MBSA)ツールがセキュリティ構成の検証に一般的に使用されていました。MBSAとその他のMicrosoftレポートツールは、Security Compliance Toolkit (docs.microsoft.com/en-us/windows/security/threat-protection/security-compliance-toolkit-10)に置き換わりました。



セキュリティコンプライアンスマネージャーを使用して、本番GPOの設定をMicrosoftのテンプレートポリシー設定と比較する。(スクリーンショットはMicrosoftからの許可を得て使用。)

パッチ管理

オペレーティングシステム、ソフトウェアアプリケーション、ファームウェアの実装は脆弱性から完全に解放されることはありません。脆弱性が特定されるとすぐに、ベンダーは修正を試みます。同時に、脅威アクターは悪用を試みます。自動脆弱性スキャナーは、オペレーティングシステムやさまざまなサードパーティ製ソフトウェアアプリケーションやデバイス/ファームウェアに足りないパッチの検出に有効です。しかし、スキャンが有効なのは、不足するパッチを適用するための効果的な手順が整っている場合のみです。

家庭用ネットワークや小規模のネットワークの場合、ホストは、自動更新するように構成されます。これは、自動的にパッチを確認してインストールすることを意味しています。主要なOSやアプリケーションソフトウェア製品は、セキュリティ問題に対するベンダー提供の修正に関しては十分にサポートされています。ですが企業ネットワークの場合はこの種の自動展開に注意する必要があります。アプリケーションやワークフローに対応しないパッチにより可用性の問題が発生する可能性があります。また、複数のアプリケーションが同じホストでクライアントの更新を実行する場合、パフォーマンスと管理の問題も発生する可能性があります。例えば、OSの更新のほか、セキュリティソフトウェア、ブラウザ、Java、OEMドライバーなどの更新がある可能性があります。これらの問題は、エンタープライズパッチ管理スイートを導入することで緩和できます。MicrosoftのSystem Center Configuration Manager (SCCM)/Endpoint Manager (docs.microsoft.com/en-us/mem/configmgr)はベンダー固有ですが、その他にもサードパーティ製アプリケーションや複数のOSをサポートするよう設計されているものがあります。

またパッチ操作のスケジュールを立てることが難しい場合があります。特に重要なシステムにとってパッチの適用が可用性のリスクである場合です。脆弱性の評価により、不足しているパッチの問題を継続的に強調する場合は、パッチ管理の手順をアップグレードしてください。問題が特定のホストのみに影響している場合、侵害インジケーターである可能性があるため、より詳しく調べる必要があります。

またレガシーシステム、プロプライエタリシステム、一部のIoTデバイスなど、強固なセキュリティ管理プランのないベンダーからのシステムでは、パッチ管理が困難になる場合があります。こうしたシステムにすぐにパッチが利用できない場合は、補完制御、またはその他のリスク低減対策が必要になります。

エンドポイント保護

ハードニングにおけるその他の重要なステップは、マルウェア脅威の自動検知と予防にエンドポイント保護を構成することです。ホストベース/エンドポイント保護スイートやエージェントは、これまでも何度も繰り返し登場しています。個々のソフトウェアツールやプロテクションスイートは、複数の機能を兼ね備えていることが多いため、実行される機能の対比を考慮することが重要です。

ウイルス対策（アンチウイルス）(A-V)／マルウェア対策

第1世代のウイルス対策（アンチウイルス）(A-V)ソフトウェアは、既知のウイルスのシグネチャベースの検知と防止を特徴としています。「A-V」製品では、ウイルスとワームだけでなく、トロイの木馬、スパイウェア、PUP (Potentially Unwanted Program : 潜在的に望ましくないプログラム)、クリプトジャックなどの一般的なマルウェア検知が実行できるようになりました。「A-V」ソフトウェアは依然として重要ですが、シグネチャベースの検知は、データ侵害の防止には不十分であると広く認識されています。

ホスト型侵入検知/防止システム(HIDS/HIPS)

ホスト型侵入検知システム(HIDS)では、ログとファイルシステムの監視を通じて脅威検知を行います。HIDSはさまざまな機能とさまざまな形式で利用できます。一部には防御機能があるものもあります(HIPS)。ファイルシステムの完全性の監視では、シグネチャを使用して、OSシステムファイル、ドライバー、アプリケーション実行ファイルなどの管理されているファイルイメージが変更されているかどうかを検知します。また、ポートとネットワークインターフェイスを監視し、HTTPやFTPなど特定のアプリケーションによって生成されたデータとログも処理します。

エンドポイント保護プラットフォーム(EPP)

エンドポイント保護は通常、ローカルホストで実行されるエージェントに依存します。複数のセキュリティ製品が複数のエージェントにインストールされている場合（ウイルス対策用、HIDS用、ホスト型ファイアウォール用など）、競合を引き起こしシステムパフォーマンスに影響を与え、多数のテクニカルサポートインシデントとセキュリティインシデントの誤検知を引き起こす可能性があります。エンドポイント保護プラットフォーム(EPP)は、マルウェア/侵入の検知と防止を含む複数のセキュリティタスクを実行する単一のエージェントですが、ホストファイアウォール、Webコンテンツフィルタリング/セキュアな検索とブラウジング、ファイル/メッセージの暗号化などの他のセキュリティ機能も実行します。

データ損失防止 (DLP : Data Loss Prevention)

多くのEPPは、DLPエージェントが含まれます。これは、特権的なファイルの識別や、クレジットカード番号など、プライベートや機密を保持すべき文字列を特定するためのポリシーで構成されています。エージェントでは、許可なくデータがメッセージにコピーまたは添付されないようにポリシーを適用します。

エンドポイント保護の展開

特定の製品は機能と実装の詳細が大きく異なりますが、エンドポイント保護を実装するための一般的なタスクには次のものがあります。

1. エージェントソフトウェアと更新をすべてのデスクトップに配信するように管理システムを構成する。これには、アクセス許可とファイアウォール設定を構成する必要があります。
2. ポリシーを割り当てるために、ホストを適切なグループに割り当てます。例えば、クライアントエンドポイントには、サーバーとは全く異なるセキュリティ要件があります。脅威が検出された場合、即座にクライアントを隔離する予防的な仕組みは適切かもしれません。重要なサーバーに対してこれを自動的に行うと、ネットワーク全体の機能連鎖的に損失してしまう可能性があります。
3. さまざまなホストグループ構成設定をテストし、予想される脅威の範囲が検知されるようになります。
4. 監視ダッシュボードを使用して、すべてのネットワークホストでステータスを確認する。検知イベントとは別に、エージェントが無効されていたり存在しない場合にアラートが表示されるべきです。

次世代エンドポイント保護

EPPが主にシグネチャベースで検知と防止を行うのに対して、自動応答による次世代エンドポイント保護は、エンドポイント観測データと指標のロギング、および行動と異常ベースの分析に重点を置いています。

EDR (Endpoint Detection and Response)

EDR (Endpoint Detection and Response) 製品の目的は、初期実行を阻止することではなく、侵害に対するリアルタイムおよび履歴の可視性を提供し、単一のホスト内にマルウェアを封じ込め、ホストを元の状態に修復することを容易にすることです。EDRという用語は、Gartnerのセキュリティ研究者Anton Chuvakinによって作られました。Gartnerでは、セキュリティ・スイート内のEPP機能(gartner.com/en/documents/3848470)とEDR機能の両方に関する「マジック・クアドラント」レポートを毎年作成しています(gartner.com/en/documents/3894086/market-guide-for-endpoint-detection-and-response-solution)。

以前のエンドポイント保護スイートがオンプレミス管理サーバーに報告していたのに対し、次世代のエンドポイントエージェントは、クラウドポータルから管理され、人工知能(AI)と機械学習を使用してユーザーとエンティティの動作分析を実行する可能性が高くなります。これらの分析リソースは、セキュリティサービスプロバイダーが提供するものの一部となります。



*Managed Detection and Response (MDR)*は、ホストされたセキュリティサービスのクラスであることに注意してください(digitalguardian.com/blog/what-managed-detection-and-response-definition-benefits-how-choose-vendor-and-more)。

次世代ファイアウォール統合

分析に基づく次世代ウイルス対策製品は、次世代ファイアウォールによって提供される境界およびゾーンのセキュリティと組み合わされる可能性があります。エンドポイントで脅威を検知することで、ファイアウォールポリシーを自動化し、境界で隠れチャネルをブロックし、エンドポイントを隔離して、ホスト間のラテラルムーブメントの使用によるマルウェアのリスクを緩和できます。この種の機能については、同期されたセキュリティに関するSophosのホワイトペーパー (sophos.com/en-us/lp/synchronized-security.aspx)で詳細に記載されています。

ウイルス対策の対応

オンアクセス型のアンチウイルス・スキャナーや侵入防御システムは、プロセスやスクリプトが実行されるタイミングを特定し、その呼び出しを傍受（またはフック）して最初にコードをスキャンすることで機能します。コードが既知のマルウェアのシグネチャと一致するか、ヒューリスティックプロファイルに一致するマルウェアのような動作を示す場合、スキャナーは実行を阻止し、ホストファイルに対して設定されたアクション（消去、隔離、削除など）の実行を試みます。アラートがユーザーに表示され、アクションは記録されます（管理者への警告が生成される場合もあります）。マルウェアは通常、ベンダー独自の文字列を使用して、場合によってはCME (Common Malware Enumeration)識別子によってタグ付けされます。これらの識別子は、マルウェアの症状や手法を調査するために使用することができます。これにより、システムが完全に修復されたことを確認したり、その他のシステムが感染したかどうかを特定したりできます。また、攻撃や発生を繰り返さないためには、感染源を追跡し、確実にブロックすることが重要です。

高度なマルウェアツール

マルウェアは、自動スキャナーによる検知を回避できることがよくあります。SIEMや侵入検知のログを分析することで、疑わしいネットワーク接続が判明したり、ユーザーがホスト上で説明のつかないアクティビティや挙動を観察することができます。このような症状を特定しても、AVスキャナーまたはEPPエージェントが感染を報告しない場合は、高度なツールを使用してホストのマルウェアを分析する必要があります。

高度な分析と検知のユーティリティは多数ありますが、ほとんどの技術者の出発点は [Sysinternals](https://docs.microsoft.com/en-us/sysinternals) (docs.microsoft.com/en-us/sysinternals)です。

サンドボックス

サンドボックスは、信用できないホストやアプリを分離された環境で隔離し、テストを実施するテクニックです。サンドボックス環境は、ホスト環境とのインターフェイスを意図的に制限します。サンドボックスに送られたファイルの分析には、ファイルが悪質なものかどうか、サンドボックス外で実行された場合には特定のシステムにどのように影響しうるか、外部ファイルやホストとの間にどのような依存関係があるなどの判断が含まれます。サンドボックスは、マルウェアが現在の構成でどのように存在しうるかに依拠するだけでなく、サンドボックスにさまざまな異なる環境を適用できるため、従来のマルウェア対策ソリューションよりも多くの機能を提供します。

レビュー アク ティビティ： エンドポイントセキュリティ

次の質問にお答えください。

1. セキュリティ強化された構成とは何ですか。
2. 次の記述は正しいですか、誤りですか？ Microsoftのオペレーティングシステムとアプリケーションのみでセキュリティのパッチが必要になります。
3. ウイルス対策ソフトウェアは、マルウェアの存在を報告しますが、マルウェアを自動的に削除できません。影響を受けたファイルの場所のほか、システムを手動で修復するため必要な情報は何ですか。
4. エンドポイントセキュリティソリューションについて中規模の会社と相談しています。クラウドベースの分析プラットフォームには、シグネチャの更新に依存するオンプレミスソリューションに比べてどのような利点がありますか。
5. データの抜き取りに使用されたプロセスが疑わしいのですが、そのプロセスがウイルス対策ソフトウェアによってマルウェアとして識別されない場合、最も役に立つのはどのタイプの分析ツールですか。

トピック12C

組み込みシステムのセキュリティ のリスクについて説明する



対象試験範囲

2.6組み込みシステムおよび専用システムがもたらすセキュリティ上の影響について説明することができます

ネットワーク内の明らかなコンピューティングホストだけでなく、組み込みシステムのセキュリティも考慮する必要があります。組み込みコンピューティング機能は、家庭用電化製品や専門の監視および制御システムで使用されており、これらのデバイスを識別して保護する方法を認識することが重要です。

組み込みシステム

組み込みシステムは、特定の専用機能を実行するようにデザインされた完全なコンピューターシステムです。これらのシステムは、点滴速度計内のマイクロコントローラーのように小型のものから、水処理工場を管理する制御デバイスのネットワークのように大型で複雑なものまでさまざまです。組み込みシステムは静的環境として特徴付けることができます。PCは動的環境です。ユーザーは、プログラムやデータファイルの追加／削除、新しいハードウェアコンポーネントの追加、オペレーティングシステムのアップグレードなどを実行できます。静的環境では、このような頻繁な変更は可能でもなければ必要でもありません。

静的な環境は通常、保護も防御も簡単なため、セキュリティの観点からはこれが理想的です。しかし、静的な環境には独自のリスクがあります。静的環境は多くの場合、セキュリティ管理者にとってブラックボックスです。WindowsなどのOS環境とは違い、セキュリティ問題の特定と修正のサポートはほとんどない可能性があります。

コスト、電源、コンピューターの制約

組み込みシステムは通常、プロセッサ能力（コアとスピード）、システムメモリ、永続ストレージに関する制約があります。コストは重要な要素です。デバイスは多数使用される可能性があり、極めて予測可能な処理ワークロード用に設計されているため、コンピュータリソースを過剰に供給する明確な理由はなく、ユニットあたりの価格を可能な限り低く抑えることができます。

コンピュータリソースを判断するその他の要素は電源です。多くの組み込みデバイスではバッテリーが使用され、セルを交換せずに何年も実行する必要がある場合があります。これは、処理を可能な限り最小限に抑える必要があることを意味します。

暗号化、認証、暗黙の信用の制約

コンピュータリソースが不足しているということは、組み込みシステムが、コンピューターネットワークで広く使用されている暗号化の識別と認証技術に不向きであることを意味します。しかし、組み込みシステムがこれらのネットワークを介してアクセスしやすくなるにつれて、機密性、完全性、可用性を確保するために暗号プロセッサを使用する必要があります。これは、そのような大きな処理リソースを必要としない暗号の開発を促しています。

PCハードウェアの場合、RoTはTPMによってハードウェアレベルで確立されます。この明示的なトラストアンカーがない場合、ネットワークは暗黙の信用モデルを使用する必要があります。暗黙の信用とは、ネットワークに追加されたすべてのデバイスが、正当な管理者によって追加され、引き続き操作されていることを前提として、信用されていることを意味します。組み込みTPMが広く採用されるまで、組み込みネットワークは境界セキュリティモデルに依存する必要があります。

ネットワークと通信範囲の制約

コンピューティング機能を最小限に抑えることは、ネットワーク接続の選択にも影響を及ぼします。コンピューターとスマートフォンのネットワークで使用するために開発されたWiFiと4G/5Gの規格は電力を大量に消費するアンテナを使用して、データレートと通信範囲を最大化し、さらに通信を暗号化する処理を行います。組み込みシステムのネットワークでは、高い信頼性と低レイテンシーを備えた少量のデータの電力効率の高い転送に重点を置いています。

組み込みシステムの論理コントローラー

組み込みシステムは通常、**PLC (Programmable Logic Controller)**で実行されるファームウェアに基づいています。これらのPLCは、一部のデスクトップPCとは異なるハードウェアとコンポーネントから構築されています。

SoC (System on Chip)

デスクトップコンピューターのシステムアーキテクチャでは、マザーボードを介してリンクされた、一般的なCPUに加え、その他のさまざまなプロセッサ、コントローラー、システムメモリを使用します。**SoC (System on Chip)**とは、これらのすべてのプロセッサ、コントローラー、デバイスが1つのプロセッサダイ（またはチップ）で提供される設計です。このタイプのパッケージはスペースを節約し、通常は電力効率が高いため、組み込みシステムで一般的に使用されます。

Raspberry Pi (raspberrypi.org)と**Arduino** (arduino.cc)はSoCボードの例で、最初は教育用ツールとして考案されたものですが、現在は産業用アプリケーションとハッキングに幅広く使用されています。

FPGA (Field Programmable Gate Array)

マイクロコントローラーとは、専用の命令セットから順次操作を実行できる処理ユニットです。命令セットは製造時にベンダーによって決定されます。マイクロコントローラーで実行するソフトウェアは、こうした命令（アセンブリ言語）に変換される必要があります。多くの組み込みシステムが比較的単純ですが反復的な操作を実行するため、必要な命令のみを実行するようにハードウェアコントローラーを設計する方が効率は高くなります。この例として、イーサネットスイッチで使用される特定用途向け集積回路(ASIC)があります。ですがASICは設計に費用がかかり、イーサネットスイッチなどの1つの用途のみで機能します。

FPGA (Field Programmable Gate Array)は、この問題を解決するコントローラーのタイプです。コントローラーの構造は、製造時には完全に設定されていません。エンドカスタマーが特定のアプリケーションを実行するためにデバイスのプログラミングロジックを構成できます。

リアルタイムオペレーティングシステム(RTOS)

多くの組み込みシステムでは、点滴流量計や流量弁などの時間に大きく依存するタスクを実行するデバイスを作動させます。このようなデバイスを実行するカーネルまたはオペレーティングシステムは、デスクトップコンピューターやサーバーを実行するOSより安定性と信頼性が大幅に高くななければなりません。組み込みシステムは通常、再起動やクラッシュを容認せず、マイクロ秒以内の許容誤差で予測可能な応答時間が必要となります。そのため、これらのシステムでは多くの場合、**リアルタイムオペレーティングシステム(RTOS)**と呼ばれる、異なる設計技術を用いたプラットフォームが使用されます。RTOSは、できる限り攻撃対象領域を小さくするように設計する必要があります。RTOSはCVEやエクスプロイトの影響を受ける可能性があります。

組み込みシステム通信に関する考慮事項

組み込みシステムは歴史的に、プロプライエタリなベンダー通信技術を使用していました。技術が向上し、ITネットワークとの緊密な統合がさらに重要になる中、標準化された通信技術の使用が拡大しています。

OT (Operational Technology)ネットワーク

産業アプリケーションのケーブルネットワークはOT (Operational Technology)ネットワークと呼ばれます。これらは通常シリアルデータプロトコルか産業用イーサネットのいずれかを使用します。産業用イーサネットは、リアルタイムで確定的な転送向けに最適化されています。このようなネットワークでは、ベンダーが開発したデータリンクとネットワークプロトコル、専用アプリケーションプロトコルが使用される場合があります。

携帯ネットワーク

携帯ネットワークにより、携帯電話やスマートフォンをサポートする同じシステム上で長距離通信が可能になります。これは、携帯モ뎀の機能を実行するベースバンドプロセッサにちなむで、**ベースバンド無線**とも呼ばれています。ベースバンド無線技術は次のようにいくつかあります。

- ナローバンドIoT (NB-IoT)- これは、LTE (Long Term Evolution)または4G携帯規格の低電力バージョンを指します。信号は通常の携帯より少ない帯域幅を占有します。これは、データレートが制限されていること (20 ~ 100kbps) を意味しますが、ほとんどのセンサーでは、大規模なデータ転送ではなく、小さなパケットを低レイテンシーで送信する必要があります。また、ナローバンドの方がより透過力が大きいため、トンネルや建物の奥深くなど、通常の携帯接続が不可能なアクセスできない場所での使用に適しています。
- LTEマシンタイプ通信(LTE-M)- これは別の低電力システムですが、より高い帯域幅 (最大約1Mbps) をサポートします。

まだ完全に標準化されていませんが、NB-IoTとLTE-Mの両方は、5Gネットワークと互換性があるように設計されています。これは、NB-IoTとLTE-Mは5Gの信号を妨害せず、5G用に開発されたタワーリレーを使用できることを意味しています。それらはより高いデータレートをサポートする可能性がありますが、レイテンシーと信頼性がより重要な考慮事項になる傾向があります。

LTEベースのセル無線では、**SIM (subscriber identity module)**カードを識別子として使用します。SIMは他のサプライヤーのタワーリレーの使用を許可するローミング付きで、携帯電話プロバイダーによって発行されます。リムーバブルカードは組み込みに適したフォームファクターではありませんが、eSIMにはシステムボードまたはSoC設計のチップと同じ機能が組み込まれています。

エンドポイントと基地局間と、インターネットルーターへのバックホール内におけるフレームの暗号化は、ネットワークオペレーターの責任になります。無線区間の暗号化は、携帯電話の標準化団体である3GPPで考案された暗号化スキームで行われます。バックホールのセキュリティは通常IPSecを使用して実施されます。組み込みシステムでは、追加のセキュリティとしてアプリケーション層の暗号化を使用できます。

Z-WaveとZigbee

Z-WaveとZigbeeは、主にホームオートメーションに使用されるワイヤレス通信プロトコルです。両方とも、低エネルギー電波を使用してメッシュネットワークを構築し、1つのアプライアンスから別のアプライアンスへの通信を可能にします。**Z-Wave**の場合、デバイスはネットワークを拡張するリピータとして構成することができますが、コントローラデバイスとエンドポイントの間で通過できる「ホップ」は4つに限られています。Z-Waveでは900 MHzまでの周波数を使用します。

ZigbeeはZ-Waveと同じ用途で、オープンソースの競合技術として登場しました。Zigbeeアライアンスは、様々な技術や規格の認証プログラムを運営しています。Zigbeeは2.4 GHz周波数帯を使用します。高い周波数の使用により、Z-Waveと比べると通信範囲は劣るもののデータ帯域が広くなっています。ただし、他の2.4 GHz無線通信の干渉を受けるリスクも高くなっています。Zigbeeは単一ネットワーク内で多数のデバイスをサポートできるほか、デバイス間の通信におけるホップ制限もありません。

Z-WaveとZigbeeの両方で通信暗号化が使用されています。主な脅威は再ペアリング攻撃と不正なデバイスによるものになります。再ペアリング攻撃では、脅威アクターがあるデバイスをネットワークから強制的に切断し、それが再接続を試みることにより、ネットワークキーを見ることを可能にします。[\(checkpoint.com/press/2020/the-dark-side-of-smart-lighting-](https://checkpoint.com/press/2020/the-dark-side-of-smart-lighting/)

[check-point-research-shows-how-business-and-home-networks-can-be-hacked-from-a-lightbulb](#))。ユーザーが不正なデバイスをネットワークに接続する場合、システムはアプリケーションレベルのセキュリティ依存して、デバイスがスマートハブ、アラームまたはドアエントリ装置などのさらに価値の高いターゲットを侵害しないようにします。

産業用制御システム

産業用システムには、ITシステムとは異なる優先順位があります。多くの場合、危険な電気機械部品が関わるため、安全性が最も重要な優先事項になります。また産業プロセスでは、機密性よりも可用性と完全性が優先され、CIA（機密性、完全性、可用性）トライアドとは逆にAIC（可用性、完全性、機密性）トライアドになります。

ワークフローとプロセス自動化システム

産業用制御システム (ICS : Industrial Control Systems) では、ワークフローとプロセス自動化のメカニズムを提供します。これらのシステムは、電力会社、水道会社、医療サービス、通信、国家安全保障サービスなどの重要なインフラで使用される機械を制御しています。1つのサイト内でプロセス自動化を管理するICSは通常、分散制御システム (DCS : Distributed Control System)と呼ばれます。

ICSは、PLCを組み込んだプラント機器や装置で構成されています。PLCは、OTフィールドバスのシリアルネットワークか産業用イーサネットのいずれかを介して、弁、モーター、サーチットブレーカーなどの機械部品を操作する作動装置（アクチュエータ）や、温度などのローカルな状態を監視するセンサーにリンクされています。PLCの出力と構成は、1つ以上の**ヒューマンマシンインターフェイス(HMI)**によって実行されます。HMIはローカルコントロールパネルまたはコンピューティングホストで実行しているソフトウェアの場合があります。PLCはコントロールループ内で接続され、プロセス自動化システム全体は、コントロールサーバーによって管理できます。もう1つの重要なコンセプトは、**データヒストリアン**です。これは、コントロールループによって生成されるすべての情報のデータベースです。

監視制御とデータ取得 (SCADA : Supervisory Control and Data Acquisition)

SCADA (Supervisory Control and Data Acquisition)システムは、大規模でマルチサイトのICSでの、コントロールサーバーの代わりになります。SCADAは通常、一般的なコンピューターでソフトウェアとして実行され、フィールドデバイスと呼ばれる、組み込みPLCを使用するプラントの機器や装置からデータを収集し、管理します。SCADAでは通常、携帯電話や衛星などのWAN通信を利用して、SCADAサーバーとフィールドデバイスを接続します。

ICS/SCADAアプリケーション

このタイプのシステムは産業の多くの分野で使用されています。

- エネルギーとは、発電と配電を指します。より広い意味では、上下水道や交通網などを含む公共サービスです。
- 産業とは、特に危険な高圧炉、プレス、遠心分離機、ポンプなどを含む、原材料の採掘および精製のプロセスを指します。
- 製作と製造とは、コンポーネントを作成し、それらを製品に組み立てるのを指します。組み込みシステムは、鍛造、ミル、組立ラインなどの自動化された生産システムを制御するために使用されます。これらのシステムは非常に高い精度で作動する必要があります。
- ロジスティクスとは、工場内または顧客への配送のために、製造または組み立てられた場所から必要な場所に物品を移動させることを指します。組み込みテクノロジーは自動化された輸送およびリフトシステムと、コンポーネント追跡用センサーの制御に使用されます。
- 設備とは、サイトや建物の管理システムを指し、通常は自動化された暖房、換気、および空調 (HVAC : Heating, Ventilation, and Air Conditioning) 、照明、セキュリティシステムを操作します。

ICS/SCADAは歴史的にITセキュリティに関係なく構築されてきましたが、特にネットワーク環境で動作する場合は、保護するためにセキュリティ管理を強制する必要性についての認識が高まっています。



組み込みシステムにおける有名な攻撃の例に、*Stuxnet*ワーム(wired.com/2014/11/countdown-to-zero-day-stuxnet)があります。これは、イランの核燃料プログラムによって使用される遠心分離機に損害を与えるために、Windows PCで実行されるSCADA管理ソフトウェアを攻撃するために設計されました。NISTの特別刊行物800-82には、ICSとSCADAにセキュリティ管理を実装する場合の推奨事項が記載されています(nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf)。

モノのインターネット

モノのインターネット(IoT)という用語は、センサー、ソフトウェア、ネットワーク接続が装備されたアプライアンスとパーソナルデバイスのグローバルネットワークを表すために使用されます。このコンピューティング機能によって、これらのデバイスが相互に、またはコンピューターサーバーなど従来のシステムと通信し、データの交換を可能にします。これは「マシンツーマシン (M2M : Machine to Machine)」通信と呼ばれます。それぞれの「モノ」は、オペレーティングシステムやコントロールシステム内に組み込まれた一意のシリアル番号またはコードにより識別され、既存のインターネットインフラストラクチャ内で直接、または仲介者を通して相互運用することができます。IoTネットワークは通常、次のタイプのコンポーネントを使用します。

- ハブ/制御システム - IoTデバイスでは通常、Z-WaveまたはZigbeeネットワーキングを促す通信ハブが必要になります。また、IoTデバイスの多くはヘッドレス、つまりユーザー操作のインターフェースを持たないため、制御システムも必要です。これは音声コントロールを装備したスマートハブや、スマートフォン/PCアプリである可能性があります。
- スマートデバイス - IoTエンドポイントでは、遠隔操作できるスマート電球やテレビインターフォンなどの機能を実装します。これらのデバイスは、悪用に脆弱な可能性が高いコンピューティング、ストレージ、ネットワーク機能を実装しています。ほとんどのスマートデバイスではLinuxまたはAndroidカーネルを使用します。スマートデバイスはミニコンピューターを効果的に実行しているため、Webアプリケーションやネットワーク機能に関連する一部の標準的な攻撃に対して脆弱です。カメラやマイクなどの一体型周辺機器は監視を容易にするため危険にさらされる可能性があります。
- ウエアラブル - スマートウォッチやブレスレット型/ペンダント型のフィットネスマニターや眼鏡など、一部のIoTデバイスはアクセサリーとして設計されています。現在競合している技術は、FitBit、Android Wear OS、Samsung Tizen OS、Apple iOSをベースにしたもので、それぞれ独自のアプリエコシステムを確立しています。
- センサー - IoTデバイスは、温度、光量、湿度、圧力、近接度、動き、ガス/化学物質/煙、心拍数/呼吸数など、あらゆる種類のものを測定する必要があります。これらは熱電対/サーミスタ、赤外線検出器、誘導性セル、光電性セル、容量性セル、加速度センサー、ジャイロスコープなどとして実装されます。

ホームオートメーション製品は多くの場合、ベンダー固有のソフトウェアとネットワーキングプロトコルを使用します。組み込みデバイスと同様に、セキュリティ機能の文書化が不十分である可能性があるため、ベンダーのパッチ管理/セキュリティ対応プロセスが不十分である可能性があります。IoTデバイスが住宅用に設計されている場合、デフォルト設定が弱い可能性があります。最小限の構成で「機能」するように設定されている場合があります。顧客が決して講じない、デバイスを保護する推奨手順がある可能性があります。

設備の自動化に特化したシステム

専用システムとは、特定の目的や用途で組み込みシステムやIoTデバイスを使用することを指します。

ビルオートメーションシステム(BAS)

オフィスとデータセンターの**ビルオートメーションシステム (BAS)**、「スマートビルディング」には、物理的なアクセス制御システムだけでなく、暖房、換気、および空調(HVAC)、防火、電力、照明、エレベーターおよびエスカレーターを含めることができます。これらのサブシステムは、PLCと、温度、気圧、湿度、部屋の占有率などを測定するさまざまなタイプのセンサーによって実装されます。これらのシステムに影響する一般的な脆弱性には次が含まれます。

- バッファーオーバーフローなどのPLCのプロセスとメモリの脆弱性。これらは、自動化管理プロトコルで悪意を持って作成されたパケットを処理することで発生する可能性があります。ビルオートメーションでは、BACnetまたはDrynetなどの専用ネットワークプロトコルを使用します。
- アプリケーションコード内の平文の認証情報や暗号化キーの使用。
- システムの構成と監視に使用されるグラフィカルWebアプリケーションインターフェイスを介したコードインジェクション。これは、クリックジャッキングやクロスサイトスクリプティング(XSS)などのJavaScriptベースの攻撃を実行するために使用できます。

これらのシステムの制御を使用して、ある種のDoSまたは身代金要求を実行できる可能性があります（例えばデータセンター内のHVAC制御を中断することを考慮してください）。ですが、Target社のデータ侵害のように、目的は自動化と監視のシステムから企業データネットワークにアクセスする可能性が高く、サプライヤー企業からアクセスできる可能性があります (krebsonsecurity.com/tag/fazio-mechanical)。

スマートメーター

スマートメーターでは、電気、ガス、または水の使用状況のレポートを継続的に更新してサプライヤーに提供し、手動による検査の必要性を減らします。ほとんどのメーターは、サプライヤーとの通信に携帯データネットワークを使用し、スマートアプライアンスとの統合にZigBeeなどのIoTプロトコルを使用します。

監視システム

物理アクセス制御システム (PACS : Physical Access Control System) は、監視対象のロック、侵入者アラーム、**ビデオ監視**のネットワークです。PACSは、ビルオートメーションシステムの一部として実装することも、それ自体で別のシステムとして実装することもできます。施設への物理的なアクセス、または単にビデオ監視システムへのアクセスを取得することは、脅威アクターにその他の攻撃を開発する多くの機会を与えます。ビルオートメーションと同様に、PACSは外部サプライヤーによってインストールされ、管理される可能性が高いです。これにより、連邦政府機関のPACSに関する米国政府説明責任局の2014年のレポートで強調されるように、リスクと脆弱性の評価から除外される可能性があります (gao.gov/assets/670/667512.pdf)。

物理的なセキュリティシステムでは、監視にネットワークカメラシステム (CCTV : Closed-Circuit TeleVision) を使用します。残念ながら、一部のメーカーのカメラシステムには、脅威アクターが侵入の記録を防止したり、カメラを乗っ取って独自の監視を実行したりすることを許可する深刻な脆弱性が多数あることが判明しています。これらの問題は、エンタープライズモデルではなく、安価な消費者向けシステムに影響を与える傾向がありますが、どちらの場合でも、セキュリティ監視および修復サポートサービスが有効であることを示すためにサプライヤーを評価する必要があります。

ITに特化したシステム

プリンターやVoIP (Voice over IP)機器など、オフィスネットワーク内にインストールされている専用システムもあります。これらのシステムは、セキュリティ監視手順によって見過ごされてはなりません。

複合機(MFP)

最新の印刷デバイス、スキャナー、ファックスマシンのほとんどにはハードドライブと最新のファームウェアが搭載されており、コンピューターに接続したり、ネットワークを介したりせずに行使用できます。多くの場合このような印刷/スキャン/ファックス機能は、1台のデバイスで実行され、**複合機(MFP)**と呼ばれます。画像やドキュメントは安全に削除されるまで、これらすべてのマシンから高い頻度で復元できます。また、より機能性が高く、ネットワーク接続されたプリンターやMFPは、残りのネットワークを攻撃するための中継地点として使用されることがあります。これらのマシンにも独自のファームウェアが搭載されており、最新のパッチと更新が適用される必要があります。

VoIP (Voice over IP)

VoIP (Voice over IP)エンドポイントとメディアゲートウェイの両方を実装するために、さまざまな種類の組み込みシステムが使用されています。エンドポイントは、個々のハンドセットまたは会議端末にできます。メディアゲートウェイは、電話および携帯ネットワークとの統合を実装するために、個別のファームウェア/OSを使用する場合があります。



これらのデバイスがインターネットに直接接続される場合、フィンガーブリンティングアプリやWebサイト (shodan.io/explore/tag/voip または shodan.io/explore/tag/printer など) を使用して、パッチが適用されていない脆弱性を調べることができます。IoTやICSのデバイスにはいくつものShodanクエリがあります。

TOP COUNTRIES	RESULTS
	439,759
	Netherlands, Amsterdam
	United States
	China
	Hong Kong
	Germany
	France

TOP ORGANIZATIONS	RESULTS
Leaseweb USA	28,337
Cogent Communi...	15,481
Peg Tech	15,348
China Unicom Lia...	13,953
Amazon.com	9,321

New Service: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

HTTP/1.1 400 Bad Request
Content-Type: text/plain; charset=utf-8
Connection: close

400 Bad Request

HTTP/1.1 400 Bad Request
Server: nginx
Date: Sun, 09 Aug 2020 11:49:07 GMT
Content-Type: text/html
Content-Length: 158
Connection: close

```
<html>
<head><title>400 Bad Request</title></head>
<body>
<center><h1>400 Bad Request</h1></center>
<hr><center>nginx</center>
```

ポート9100（未加工印刷データ用TCPポート）上でプローブに対応するサイトのShodan検索結果。

車両とドローンに特化したシステム

自動車および無人航空機(UAV)やドローンには、エンジン、電力系統、ブレーキ、着陸、サスペンション/安定性を制御する最新電子工学が使用されています。近年の車両は、ナビゲーションやエンターテイメントシステムのほか、車両の自動化システムがハンドル操作やブレーキを制御できるドライバーアシストや自動運転機能を備えている可能性が高まっています。また、施錠、アラーム、エンジン始動ロックのメカニズムも同システムの一部となる可能性が高くなっています。

います。こうしたサブシステムはそれぞれ、電子制御装置(ECU)として実装され、1つ以上のコントローラーエリアネットワーク(CAN)のシリアル通信バスを介して接続されています。主な外部インターフェイスはOnboard Diagnostics (OBD-II)モジュールです。OBD-IIは複数のCANバスのゲートウェイとしても機能します。

CANバスは、イーサネットと同じように作動し、セキュリティ対策がほとんど講じられずに設計されました。ECUは、ブロードキャストとしてメッセージを送信するので、同じバスにある他のすべてのECUで受信されます。送信元アドレスやメッセージの認証の概念はありません。悪意のあるデバイスをOBD-IIポートにアタッチできる脅威アクターは、CANバスに対してDoS攻撃を実行し、車両の安全を脅かすことができます。また、自動車のナビゲーションやエンターテイメントシステムの携帯機能を介すなどして、CANバスに遠隔でアクセスする方法もあります (wired.com/2015/07/hackers-remotely-kill-jeep-highway)。車両の中には、車載WiFiを実装しており、攻撃対象領域がさらに広がっているものもあります。

医療デバイスに特化したシステム

医療デバイスは、さまざまな攻撃に対して脆弱な可能性がある一連のシステムです。これらの装置の使用は、病院やクリニック内だけに限られたものではなく、心臓モニター／除細動器やインシュリンポンプなどのポータブル機器も含まれることを認識することが重要です。安全対策が講じられていない通信プロトコルと同様に、こうしたデバイスの制御システムの多くは、新しいOSバージョンで機能するためのソフトウェア更新コストが高額で、患者サービスに支障が出るため、サポートのないバージョンのオペレーティングシステム (Windows XPなど) で実行されています。医療デバイスとサービスに対する攻撃の目的には次があります。

- 侵害されたデバイスを使用して、保護されるべき医療情報(PHI)を盗むことを目的として、医療データを保存するネットワークに侵入する。
- 医療機関のサービスを停止させると脅し、身代金を要求する。
- 投与量や機器の設定を改ざんし、患者を殺害または負傷させる（またはそのように脅す）。

組み込みシステムのセキュリティ

セキュリティシステムを設計する場合、組み込みシステムを見落としてはなりません。次の方法は、そのような環境におけるリスクを低減するために使用できます。

ネットワークのセグメント化

ネットワークのセグメント化はネットワークセキュリティの中核原則の1つです。静的環境へのネットワークアクセスは、ホストソフトウェアからデバイスへのファームウェアアップデートや管理制御の適用、およびデバイスからホストソフトウェアへのステータスや診断情報の報告のみに限定されるべきです。この制御ネットワークは、ファイアウォールやVLANを使用して企業ネットワークから分離させてください。

SCADAなどの環境では、管理ソフトウェアで古いオペレーティングシステムが必要になる場合があるので、ホストのセキュリティ保護は特に困難になります。ネットワークのセグメント化を通じてこれらのホストを他のホストから隔離し、エンドポイントセキュリティを使用することで (USBデバイスの接続を阻止すること) で、マルウェアに感染したり、ネットワークのエクスプロイトに晒されないようにできます。

ラッパー

組み込みシステム転送中のデータのセキュリティを強化する1つの方法は、IPSecなどのラッパーを使用することです。脅威アクターや送信をスニッフィングする者に明らかにされる唯一のものは、トンネルエンドポイントを表すIPSecのヘッダーだけです。これは、トラフィックが信頼できないネットワークを経由するときに信頼できるネットワーク間のトラフィックを保護する場合や、同じネットワーク上の信頼できるノード間のトラフィック保護する場合に有効です。