

レッスン21

物理的なセキュリティについて説明する

レッスン概要

ソーシャルエンジニアリング、ワイヤレスバックドア、モバイルデバイスによるデータ流出などの侵害のリスクはすべて、サイトの設計と運用において物理的なセキュリティが重要な考慮事項であることを示しています。ネットワークを導入している施設では、アクセス制御メカニズムが必要になり、火災などの人為的な災害や自然災害からの耐性がある必要があります。

レッスンの目的

このレッスンの内容は、以下のとおりです。

- 物理的なサイトのセキュリティ管理の重要性を説明する。
- 物理的なホストのセキュリティ管理の重要性を説明する。

トピック21A

物理的なサイトのセキュリティ 管理の重要性を説明する



対象試験範囲

- 1.2 与えられたシナリオに基づいて、可能性あるインジケーターを分析して攻撃のタイプを特定することができる
- 2.7 物理的セキュリティ制御の重要性について説明することができる

脅威アクターが施設に物理的にアクセスできる場合、不正なデバイスのインストールや、システムの破壊や中断、機密情報の取得を行うさまざまな機会がある可能性があります。よってセキュリティの専門家として、物理的な侵害からサイトを保護するために、アクセスと監視の制御の重要性について説明できる必要があります。

物理的なセキュリティ管理

物理的なアクセス制御は、特定の物理的なエリアや資産へのアクセスを制限し、監視するセキュリティ対策です。これにより、ビルや機器、サーバールーム、財務部や法務部のエリア、データセンター、ネットワークケーブル回線、重要な価値やセンシティビティがあるとされるハードウェアや情報があるその他のエリアなどへのアクセスを制御できます。物理的なアクセス制御を使用する場所を判断するには費用対効果分析が必要となり、保護される特定のデータの種類における規制やその他のコンプライアンス要件を考慮する必要があります。

物理的なアクセス制御は、ネットワークやオペレーティングシステムのセキュリティと同じアクセス制御の基本によって異なります。

- 認証 - アクセスリストと識別メカニズムを作成し、承認される人物が閑門を通過できるようにします。
- 許可 - 指定した出入口を通じてアクセスを管理できるようにリソースの周囲に閑門を設けます。
- アカウンティング - 出入口が使用された時間の記録を保存し、セキュリティ侵害を検知します。

物理的なセキュリティは、ゾーンの観点から考慮できます。各ゾーンは、独自の閑門によって分けられるべきです。閑門を通じた出入口は、1つまたは複数のセキュリティメカニズムによって管理される必要があります。各ゾーンは、進むごとに徐々に制限を強めるべきです。

サイトのレイアウト、フェンス、照明

既存の施設では、サイトのレイアウトに影響を与える余地はありませんが、コストと既存のインフラストラクチャの制約を考慮して、次の原則を使用してサイトを計画してみてください。

- 機器室などのセキュリティゾーンはできるだけ建物の奥深くに配置し、外壁、ドア、窓がないようにします。
- 物理的な空間には非武装地帯(DMZ)設計を使用します。ゲストがセキュリティゾーンのそばを通らないように、公共エリアを配置します。公共エリアのセキュリティメカニズムは、抑止を促すために良く見えるようにすべきです。

- サインや警告を使用して、セキュリティが厳密に管理されていることを強調します。基本的な「立ち入り禁止」サインのほか、家庭やオフィスでは、使用している警備会社の標識を配置している場合もあります。これにより侵入者が立ち入らないようにできる可能性があります。
- 逆に、セキュリティゾーンへの入口では控えめにするべきです。そのような地帯を保護するセキュリティメカニズムを侵入者が物色する機会を与えないようにします（またはそこにあるということすら知らないようにします）。**インダストリアルカモフラージュ**を使用して、価値の高い資産を保護する建物やゲートを目立たなくしたり、視認性の高いおとりエリアを作り、潜在的な脅威アクターを誘い出します。
- ゾーン間を通らなければならない行き来は最小限に抑えます。人の流れは、「横切ったり、間を行く」のではなく「入ったら出る」するようにすべきです。
- 出入りの激しい公共エリアの視認性を高めることで、ゲート、ネットワークアクセスポート、コンピューター機器の不正使用を妨害し、監視を簡素にできます。
- セキュリティゾーンでは、ディスプレイ画面や入力デバイスを通路や窓に向けて配置しないでください。あるいは、窓を通じて見ることができないように片側からしか見えないガラスを使用します。

バリケードと入口/出口

バリケードとは、アクセスを阻むものを指します。セキュリティシステムにおいては、完全に有効なバリケードはありません。例えば、壁は登ってくる可能性、ロックはピッキングされる可能性があります。バリケードの目的は、指定の出入口を通じて人々を通すことです。入口ごとに、認証メカニズムを設け、認証を受けた人のみが入れるようにします。有効な監視メカニズムにより、別の方法によるバリケードへの侵入の試みを確実に検知します。



テロ攻撃のリスクがあるサイトでは、ボラードやガイドポールなどのバリケードを使用し、車両が高スピードで建物に接近しないようにします。

フェンス

建物の外はフェンスで保護することができます。セキュリティフェンスは、分かりやすく（警備員が侵入の試みを見るように）、丈夫で（切断が困難になるように）、登ってこられないように（通常はフェンスを高くしたり、カミソリ有刺鉄線を使用するなどで対応可能）する必要があります。通常、フェンスは効果的ですが、建物が威嚇的に見てしまうのが欠点です。企業が、顧客や一般の人々を迎えるために使用している建物では、より慎重なセキュリティ対策を使用する場合があります。

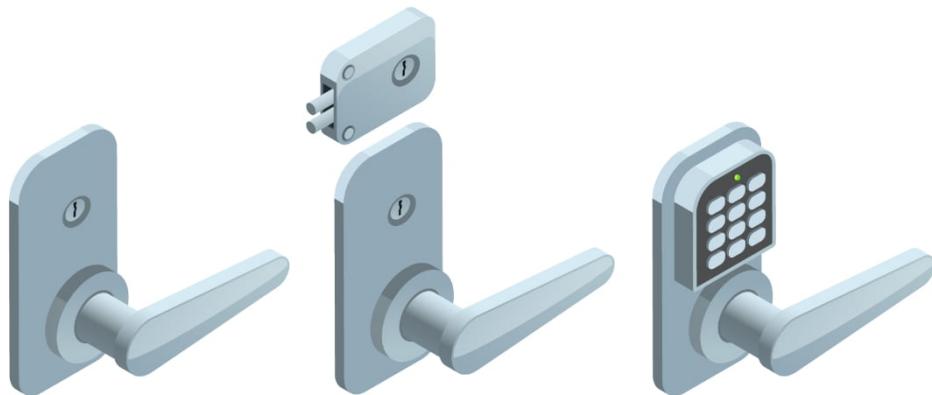
照明

防犯用照明は、建物が夜間に安全で保護されていると周知させるために極めて重要です。しっかりと設計された照明は、特に公共エリアや駐車場などの閉鎖空間で人々が安心できるようにします。また防犯用照明は、侵入をより困難にして抑止の役割も果たし、監視（カメラまたは警備員）を容易にします。照明の設計では、全体的な光源レベル、特定の面やエリアの照明（カメラが顔認証を実行できるようにするなど）を考慮し、影になる部分やまぶしすぎる部分がないようにする必要があります。

ゲートとロック

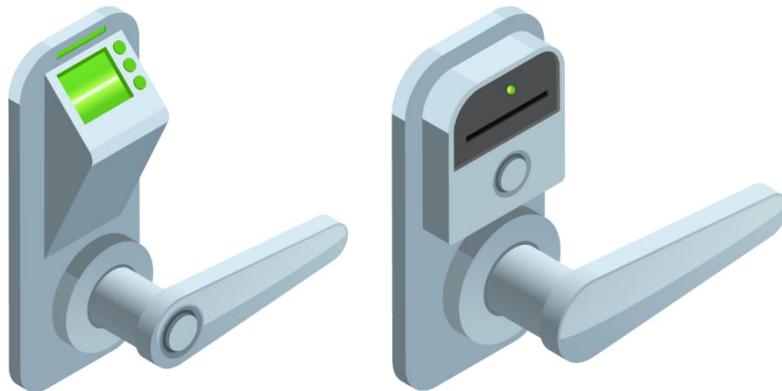
ゲートのセキュリティを確保するには、ロックを取り付ける必要があります。セキュアなゲートとは通常、ユーザーによる閉鎖・施錠に依存しない自己閉鎖および自己施錠式のものです。ロックには以下のような分類があります。

- 従来型 - 従来型のロックは、鍵を使用しないとドアの取っ手が動作しないというものです。より高価なものほど、ピッキングに対する防御力に優れています。
- 電子錠 - 鍵を使用してではなく、電子キーパッドにPINを入力することで動作するロックです。この種のロックは、暗号錠または文字合わせ錠、キーレスロックとも呼ばれます。スマートロックは、磁気スワイプカードを使用するか、ワイヤレスキーフォブやスマートカードなどの物理的なトークンの存在を検知する[近接型リーダー](#)を使用して解錠できます。



ロックの凡例 - (左から右) 標準的なロック、デッドボルト錠、電子キーパッドロック。
(画像 : user macrovector © 123RF.com)

- 生体認証 - ロックは生体認証スキャナーに統合できる場合があります。



生体認証親指指紋スキャナーロックとトークンベースのキーカードロックの凡例。
(画像 : user macrovector © 123RF.com)

マントラップ

シンプルなドアやゲートを入室メカニズムに使用する場合の主な問題は、ロックのピッキングに対して脆弱であるほか、入退室した人の正確な記録ができないことです。複数の人が同時にゲートを通過する場合や、次の人のためにドアを開けておく場合、入室許可のない人が許可されている人の後ろから「テールゲート」して入る場合があります。こうしたリスクは、**ターンスタイル**（一度に1人のみ入れるゲートの種類）を取り付けて、低減できます。もう1つのオプションは、ゲートにある種の監視を設けることです。セキュリティが重要で、コストが問題ではない場合、アクセス制御玄関ホールまたはマントラップを導入することができます。**マントラップ**とは、ゲートが、別の閑門で保護されている閉鎖された空間に繋がっている場所を指します。

ケーブルロック

ケーブルロックは、デバイスのシャーシのセキュリティスロットに取り付けられます。サーバーのシャーシには、金属製ループとKensington製セキュリティスロットの両方が付いている可能性があります。シャーシをラックやデスクに固定するだけでなく、セキュリティスロットの位置により、ケーブルを外さずにシャーシを開くことができなくなります。

スマートカードとUSBに対する物理的攻撃

電子錠のパスキーとして使用されるスマートカードの中には、クローニング攻撃やスキミング攻撃に対して脆弱なものがあります。

- **カードのクローニング** – これは、既存のカードのコピーを1つまたは複数作ることを指します。暗号で保護されていない、紛失したり、盗難されたカードは物理的に複製される可能性があります。カードを紛失した場合は、そのカードを停止して新しいカードを発行できるように、直ちに報告してください。攻撃が実行された場合は、疑わしい場所や時間にカードが使用されたことで判明する可能性があります。
- **スキミング** – これは、偽装カードリーダーを使用してカードの詳細を取得し、それをプログラムで複製することを指します。一部の近接型カードでは、脅威アクターが自分の身元を隠せる携帯型RFIDリーダーに認証情報を非常に簡単に送信することができます。ATMマシンなどの公共のリーダーに取り付けられたスキマーは検出が困難な可能性があります。

これらの攻撃は通常、暗号処理を実行するのではなく、トークンを転送する「スマートではない」スマートカードのみをターゲットにできます。銀行が発行した、EMV (Electron、MasterCard、Visa) と呼ばれるスマートカードも、互換性のために保持されている磁気ストライプを通じて、脆弱になる可能性があります。



カードのクローニングとスキミングからリスクを評価する場合、「スマートカード」には多くの種類があることを認識する必要があります。例えば、公共交通機関の支払いカードとして使用されている古いMIFAREクラシックカードは、脆弱な暗号化実装を使用しているため、簡単に複製できます。暗号処理されていない非接触型カードを使用する入室システムの構築もまた脆弱性があります([youtube.com/watch?v=cxxnuofREcM](https://www.youtube.com/watch?v=cxxnuofREcM))。TPMのような暗号プロセッサを実装するMIFARE EVまたはEMVスマートカードの複製は、不可能であると考えられます。

悪意のあるUSB充電ケーブルとプラグも大きな問題になっています。カードスキミングと同様に、空港などの場所にある公共の充電ポートを利用する場合があります。**USBデータブロッカー**では、スマートフォンやラップトップが充電ポイントに接続される場合に、あらゆるデータの転送を防ぐことにより、こうしたジユースジャッキング攻撃を低減できます([zdnet.com/article/this-cheap-gadget-can-stop-your-smartphone-or-tablet-being-hacked-at-an-airport-hotel-or-cafe](https://www.zdnet.com/article/this-cheap-gadget-can-stop-your-smartphone-or-tablet-being-hacked-at-an-airport-hotel-or-cafe))。

警報システムとセンサー

施設のセキュリティを設計する際、非常口、窓、昇降口、格子など、不正使用される可能性がある入口のセキュリティについて考慮する必要があります。侵入を防ぐための鉄格子、ロック、警報を設置できます。また、つり天井やダクトなど上下の経路も考慮してください。警報には、主に次の5種類があります。

- 回路 - 回路ベースの警報は、警報の種類に応じて、回路が開いたり閉じたりするときに鳴ります。ドアや窓が開いたり、フェンスが切断されることにより作動する場合があります。開回路の警報は回路が切断されると無効になるため、閉回路の警報の方がより安全になります。
- 動作検出 - 動きに基づく警報は、部屋などのエリア（検出器の感度と範囲によって定義）内の動きによってトリガーされる検出器に接続されています。こうした検出器のセンサーは、マイクロ波無線の反射（レーダーに類似）または熱源の動きを検知するパッシブ赤外線方式(PIR)のいずれかになります。
- ノイズ検出 - マイクが拾う音によってトリガーされる警報です。最新のAI分析と特殊な音の識別により、このタイプのシステムでは誤検知の傾向がかなり低くなります。
- 近接型 - RFIDタグ（無線ICタグ）とリーダーを使用して、エリア内でタグ付けされたオブジェクトの動きを追跡できます。これは、誰かが機器を持ち出そうとしているかどうかを検知するための警報システムのベースにすることができます。
- 脅迫状態 - この種の警報は、従業員が脅威にさらされる場合に手動でトリガーされます。この種の警報は、ワイヤレスパンダント、隠しセンサーまたはトリガー、DECTハンドセットまたはスマートフォンなどさまざまな方法で実装できます。また一部の電子ロックでは、通常時のアクセスコードとは別に、脅迫状態時のコードをプログラムできます。これにより、ゲートが開きますが、脅迫状態にある中でロックが操作されたことをセキュリティ担当者に警告できます。

通常、回路ベースの警報は、境界および窓やドアでの使用に適しています。これらは、ロックメカニズムを正しく使用せずにゲートが開かれたり、指定した時間よりも長く開いたままになっている場合に有効です。動作検出は、頻繁に使用されないスペースへのアクセスを管理する際に役に立ちます。脅迫状態警報は、公共エリアでその場にいる従業員にとって有用になります。警報は単にアラート音を鳴らしたりする場合や、モニタリングシステムに接続される場合があります。多くの警報は、地元の警察署やサードパーティのセキュリティ会社に直接繋がっています。無音警報装置は、可聴警報を鳴らさずに、セキュリティ担当者に警告します。

警備員とカメラ

通常、監視は境界のゲートの安全を強化するために設計された第2層のセキュリティになります。監視では、周辺エリアやセキュリティゾーン内に焦点が当てられる可能性があります。保護対象場所の前や周囲に、（武器を携行して、あるいは携行せずに）警備にあたる人員を配置するという方法があります。警備員は、重要なチェックポイントを監視し、身元確認を行ないアクセスを許可または却下し、物理的な入場を記録します。視覚的な抑止力としての効果もありますし、各自の知識と直感に従ってセキュリティ侵害の可能性に対応することもできます。警備員が目に見えるところに配備されることは、非常に有効な侵入の検知と抑止のメカニズムですが、それに応じて高額になります。また、警備員が適格性資格を与えられないため、特定のゾーン内に警備員を配置することができない場合もあります。記録します。警備員のトレーニングと適正審査は必要不可欠になります。

CCTV（クローズドサーキットテレビジョン）は、各ゲートや地帯に個別の警備員を管理するよりもコストのかからない監視方法ですが、設備がすでに施設に配備されていない場合は、コストがかかります。これもまた有効な抑止策です。もう1つの大きな利点は、動きとアクセスが記録できることです。警備員の配備と比べる場合の主な欠点は、応答時間が長くなることと、カメラのフィードを監視するために配備される職員が不足している場合、セキュリティが危険にさらされる可能性があることです。



サーバールームを監視するために導入されたCCTV。(画像 : Dario Lo Presti © 123rf.com)

CCTVネットワークのカメラは通常、同軸ケーブルを使用してマルチプレクサに接続されています。マルチプレクサは、1台または複数のスクリーンにカメラからの画像を表示でき、オペレーターはカメラ機能を制御したり、テープやハードドライブに画像を記録できます。最近のカメラシステムでは、通常のデータケーブルを使用してIPネットワークにリンクされている可能性があります。



制御の種類を考慮する場合、警備員は攻撃を検知し、防止するために行動できるので、予防制御となります。カメラは検知的制御だけです。

カメラシステムとロボット工学では、AIと機械学習を使用して、スマートな物理的なセキュリティを実装します(theverge.com/2018/1/23/16907238/artificial-intelligence-surveillance-cameras-security)。

- **動作認識** - カメラシステムは、歩行識別技術で構成されている場合があります。これは誰かがカメラの監視範囲内で動き、その動きのパターンが既知の許可された個人と一致しない場合、システムでアラートを生成できることを意味します。
- **オブジェクト検知** - カメラシステムでは、サーバーの消失や壁のポートに接続された不明なデバイスなど、環境への変化を検知できます。
- **ロボット警備員** - 監視システム（と場合によっては兵器システム）は、自立型ロボットに全般的または部分的に取り付けることができます(switch.com/switch-sentry)。
- **ドローン/UAV** - ドローンに取り付けられたカメラでは、地上のパトロールよりも広範囲を網羅できます(zdnet.com/article/best-security-surveillance-drones-for-business)。

受付とIDバッジ

監視において最も重要な部分の1つは、身元確認に関するポリシーです。これには、どのような対応が特定の状況で適切であるか、またソーシャルエンジニアリング攻撃を打破する役に立つかが説明されています。従業員に通達し、理解されるようにする必要があります。身元確認とは、さまざまな接触状況の全体を指します。例：

- IDバッジを持たない、または付き添いなしで移動する訪問者の身元確認を行う。
- 従業員（職位に関係なく）が不便に感じることになっても、ゲートで適切な認証を完了するよう主張する。
- 侵入者や警備員が武装している場合がある。従業員の安全と現地の法律の遵守は、会社の他のリソースを保護するための必要性との間でバランスを取る必要があります。

従業員にとって、自分の行動が同意した、期待されている行動基準に準拠していると分かっていれば、このような状況でセキュアな行動をとる方がはるかに簡単です。

受付と訪問者の記録

各ゲートの受付にあるアクセスリストには、入室が許可されている人物が記載されています。電子錠では、アクセスの試みを記録できます。また受付では行動を手動で記録できます。最低限のレベルで、入退室のシートを使用して承認を受けたアクセスを記録できます。訪問者の記録要件は組織によって異なりますが、少なくとも名前と所属する会社名、日付、入退室の時間、訪問の理由、組織内での窓口を含めるべきです。

2人体制による完全性/制御

セキュリティの高いゾーンの受付では、常に少なくとも2人のスタッフが配置されている可能性があります。これにより、入室管理の完全性が確保され、内部脅威のリスクが軽減されます。

IDバッジ

名前と（場合により）アクセス権情報を記載した写真付きのIDバッジは、建物のセキュリティ対策の基本です。建物内のセキュリティなエリアを移動する人物は必ずIDバッジを着用し、着けていない者には身元確認を求める必要があります。色分けにより、バッジにアクセスが許可されているゾーンを明確にすることができます。

レビューアク ティビティ：

物理的なサイトのセキュリティ管理

次の質問にお答えください。

1. 抑止の役割を果たしている物理的なサイトのセキュリティ管理は何ですか？
2. サイトのセキュリティにおける近接型リーダーの用途は何ですか？
3. モバイルカメラの監視の2つの主なオプションは何ですか？
4. ジュースジャッキングを低減する物理的なセキュリティシステムは何ですか？

トピック21B

物理的なホストのセキュリティ 管理の重要性を説明する



対象試験範囲

2.7 物理的セキュリティ制御の重要性について説明することができる
4.1 与えられたシナリオに基づいて、適切なツールを利用して組織のセキュリティを評価することができる (データのサニタイズのみ)

データネットワークと同様に、サイト内のホストのセキュリティを確保するには、境界防御は十分ではありません。セキュリティシステムでは、境界が危険にさらされる可能性があるリスクだけでなく、インサイダーの脅威にも対応できる必要があります。コンピューター室やデータセンターなどのセキュアなエリアを保護するための追加制御を導入する必要があります。

環境的なセキュリティにより、ホストの過熱による可用性へのリスクを最小限に抑えます。またすべてのサイトでは、機密性の高いデータ残余が暴露のリスクにさらされないようにするために、機器や書類の有効な破棄手順が必要になります。

セキュアなエリア

セキュアなエリアは、一般的なオフィスのエリアよりも高いレベルのアクセス保護で重要な資産を保管するために設計されています。ネットワークインフラストラクチャの最も脆弱なポイントは、通信室またはサーバールームです。この部分には、可能な限り最も厳格なアクセス制御と監視を適用する必要があります。同様の対策は、データセンターへのアクセスの強化にも適用されます。

セキュアなキャビネット/エンクロージャ内に機器を取り付けることにより、インサイダー攻撃と境界セキュリティメカニズムを突破した攻撃を低減できます。購入時点で、鍵式のロックまたは電子錠が装備されているものもあります。



鍵式のロックを備えたラックキャビネット。(画像提供: © 123RF.com)

一部のデータセンターには、別の企業が所有する機器のラックが含まれる可能性があります（コロケーション）。こうしたラックはケージ内に設置できるため、技術者は、自社のサービスやアプライアンスを収容するラックにのみ物理的にアクセスできます。



コロケーションケージ。（画像：© Chris Dag、CC BY 2.0 flickr.com/photos/chrisdag/865711871で共有）

エアギャップ/非武装地帯

エアギャップホストは、あらゆるネットワークに物理的に接続されていないホストです。このようなホストは通常、セキュアなエンクロージャ内に収容したり、接続されているメディアデバイスを検証したりするなど、厳格な物理的アクセス制御も備えています。

セキュアなエリア内のエアギャップは、非武装地帯と同じように機能します。それは侵入を厳密に監視する高価値資産の周囲にある何もないエリアのことです。ホスト周囲の物理的なスペースにより、あらゆるネットワークから切断されるだけでなく、資産への不正なアプローチの試みを簡単に検出できます。セキュリティポリシーにより、許可されていないコンピューティングホストやストレージメディアがDMZに持ち込まれないようにするべきです。

金庫と金庫室

携帯デバイスやメディア（バックアップテープや暗号化キーを格納するUSBメディアなど）は金庫に保管されている可能性があります。金庫は、鍵やダイヤル錠を使用する場合がありますが、電子錠メカニズムが使用されている可能性があります。金庫はさまざまな国際的な格付けスキームに対し、その内容の特定の金銭的価値に応じてランク付けています。また、煙や炎、水の浸透（消化器の使用による）に対する一定レベルの保護を提供する耐火性金庫があります。

金庫室は、ドリルや爆弾など物理的な方法による不正侵入に対するセキュリティが強化されている部屋です。金庫室は高額ですが、商用CAのルートサーバーなど、安全性の高いエアギャップを施す必要があるミッションクリティカルな資産には必要と見なされる場合があります。

保護されたディストリビューションとファラデーケージ

物理的にセキュアなケーブルネットワークは、保護されたケーブルディストリビューションまたはPDS (Protected Distribution System)と呼ばれます。主なリスクは2つあります。

- 侵入者は、盗聴機器を（タップにより）ケーブルに接続する可能性があります。
- 侵入者はケーブルを切断する可能性があります（サービス拒否）。

堅牢なPDSは、すべてのケーブルが密閉された金属製導管の中に配線され、定期的な目視点検の対象になるものです。低グレードオプションでは、導管に異なる素材（プラスチックなど）が使用されます。もう1つのオプションは、ケーブルの導管内に警報システムを取り付け、侵入が自動的に検知できるようにすることです。

通信機器は、**ファラデーケージ**と呼ばれるシールドされたエンクロージャ内に設置することができます。ケージは帯電した導電性メッシュで、信号がエリアに入り出るのをブロックします。電磁信号の漏えいによる傍受のリスクはUS DoDが調査し、信号をシールドする方法としてTEMPEST (Transient Electromagnetic Pulse Emanation Standard)を策定しました。

暖房、換気、空調

環境的な制御により、オーバーヒートなどの機器の機械的な問題による可用性の損失を低減できます。建物の制御システムは、建物のさまざまな部分に最適な作業環境を維持します。多くの場合、頭字語**HVAC (暖房、換気、空調)**が、こうしたサービスを説明するために使用されます。HVACでは、温度センサーと水蒸気検知センサー（湿度を計測）を使用します。

 ポータブルモニターを使用して、HVACの温度と湿度のセンサーが正しい数値を返していることを確認します。

コンピューター室やデータセンターの場合、温度制御された環境は通常、温度20～22°C (68～70°F)、相対湿度50%に保たれています。機器によって1時間あたりに生成される熱は、イギリス熱単位(BTU)またはキロワット(KW)で測定されます。1 KWは3412 BTUです。空調システムの冷却要件を計算するには、室内のすべての機器のワット数（照明を含む）に3.41を掛けて、1時間あたりのBTUを算出します。サーバールームに人が常駐している場合（ほとんどの場合可能性は低い）、1人につき400 BTU追加してください。空調のBTUレーティングはこの合計値を超えている必要があります。

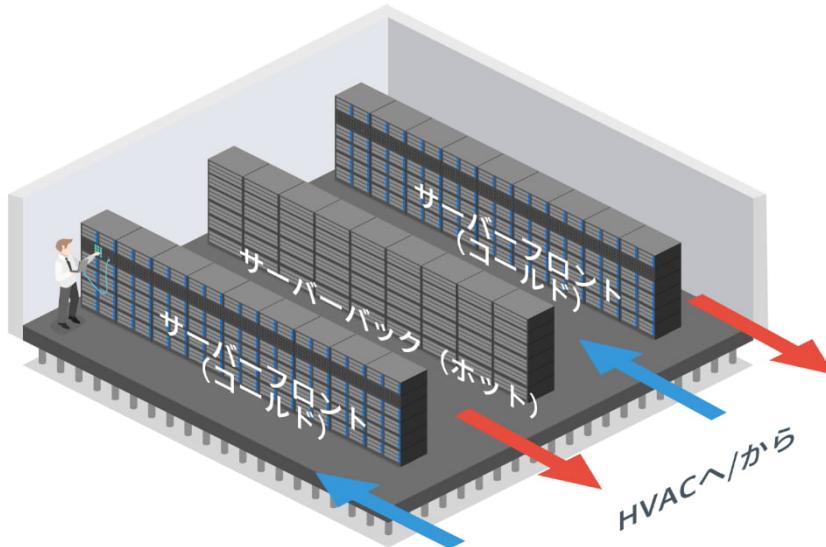
 一部のデータセンター（特にGoogleによって運営されるもの）では、高温（約26°C/80°Fまで）に対応できます。これにより、エネルギーコストを大幅に節約できます。また最新の電子機器はこの温度で信頼性が高いことが証明されています。

HVACシステムによって作られた正圧も、ほこりなどの汚染物質を施設から出します。HVACシステムのフィルターはほこりが溜まるので、定期的に交換する必要があります。空調システムを使用する場合、定期的に検査・保守されているようにします。システムには、従業員に問題を警告するためのアラームが装備されている場合があります。ミッションクリティカルなシステムではバックアップの空調システムが必要な可能性があります。

 サーバールームはストレージスペースとして使用すべきではありません。箱や使用していない機器を箱に入れて置かないでください。また、プリンターなどの熱やほこりが発生する不要なデバイスは設置しないでください。

ホット/コールドアイル

データセンターやサーバールームは、サーバーまたはラックの空気の流れを最大限にするように設計されるべきです。複数のラックを使用する場合、サーバーの前面と背面が対面するようではなく、背中合わせになるように配置し、サーバー群からの暖気が別のサーバー群の空気取り入れ口に向かわないようにします。これは**ホットアイル/コールドアイル配列**と呼ばれます。ホットアイルからコールドアイルへの空気の漏れを防ぐには、ラックの隙間を空のパネルで埋め、ストリップカーテンや遮断シートでラックの上や間のスペースを覆います。



ホットアイル封じ込め設計 - 冷気は空調から床下やラック周辺を循環し、暖気はラックの間から天井スペース（プレナム）を通じて熱交換器に引き込まれます。この設計では、暖気は天井またはラック間の床スペースから漏れないことが重要です。（画像提供：© 123RF.com）

ケーブルはケーブルタイまたはダクトで固定し、通路を横切らないようにします。ケーブルはフリーアクセス床を使用して通すのが最適です。ケーブルをプレナムスペースに通す場合は、難燃性であることを確認し、データ信号を妨害（電磁妨害[EMI]）する可能性のある電気ケーブルや蛍光灯などの電源への接近を最小限に抑えるようにします。また、空調システムが正常に機能するように、プレナムに十分なスペースを確保する必要があります。ケーブルでエリアを埋めるのは最善ではありません。



干渉を減らすには、データ/ネットワークケーブルを電源ケーブルと並行して配置しないでください。EMIが問題の場合、シールドケーブルを取り付けます。または、銅ケーブルをEMIの影響を受けにくい光ファイバーケーブルに交換します。

火災の探知と消火

健康と安全に関する法律では、火災を探知して消火するために組織が導入する必要があるメカニズムが定められています。火災安全の基本事項には次が含まれます。

- はっきりと示された非常口と、定期的にテスト、練習される緊急避難手順。
- 防火壁やドアでエリアを区分し、火事が急激に広がらないようにする建物の設計。
- 煙/火災自動検知システムと手動で操作できる警報。

消火システムは、火の三角形に基づいて機能します。火の三角形とは、火災が発生するには、熱と酸素、可燃物が必要になるという原則に基づいています。これらの要素の1つを排除することで、消火（防火）できます。米国（およびほとんどの国）の場合、火災は燃料となる可燃物に従って、NFPA（全国防火協会）システムでクラスごとに分けられます。消火器にはさまざまなタイプがあり、それぞれのタイプは、特定の火災のクラス向けに設計されています。特に、クラスCの消火器はガスベースの消火剤が使用され、他のタイプの消火器は適さない電気ショックのリスクがある場所で使用できます。



ヨーロッパの分類システムでは、漏電による火災はクラスEになります。

施設には、頭上にスプリンクラーシステムが導入されている場合もあります。ウェットパイプスプリンクラーは自動的に機能し、熱によってトリガーされ、水を放出します。ウェットパイプシステムは常に高圧で水を貯めているため、パイプが破裂したり、偶発的にトリガーされたりするリスクがあり、また実際に火災が発生する際に損害の原因になる場合があります。部屋が水浸しになるとによる損害を最小限に抑えることができる、ウェットパイプシステムの代替システムがいくつかあります。

- ドライパイプ - 凍結が起こり得る場所で使用されます。他の場所でスプリンクラーがトリガーされた場合にのみ、水がシステムのこの部分に入ります。
- プレアクション - プレアクションシステムは、警報がトリガーされる場合のみ水が充てんされ、熱が上がると散布されます。これにより、偶発的な放水やパイプの破裂を防ぎ、スプリンクラーが作動する前に手動で火を封じ込める時間を与えます。
- ハロン - ガスベースのシステムで、電気システムを短絡させず、残留物を残さないという利点があります。数年前までは、ほとんどのシステムはハロン1301が使用されていました。ハロンはオゾン層を破壊するため、その使用がほとんどの国で禁止されましたかが、すでに取り付けてあるものは多くの場合交換されておらず、引き続き合法的に使用できます。
- クリーンエージェント - ハロンの代替品は「クリーンエージェント」と呼ばれます。こうしたガスは環境に優しいだけでなく、人にとっても無害と考えられています。例えばINERGEN (CO_2 、アルゴン、水素の混合)、FM-200/HFC-227、FE-13などがあります。ガスは、周辺の酸素濃度を枯渇させますが（人間にとて危險なレベルにはなりませんが）、冷却効果があります。 CO_2 も使用できますが、混んでいる場所での使用は安全ではありません。

セキュアなデータ破棄

物理的なセキュリティ管理では、データライフサイクルの破棄段階も考慮する必要があります。メディアのサニタイズと残余の削除とは、ハードドライブ、フラッシュドライブ/SSD、テープメディア、CD、DVD ROMを破棄する前、または別の用途で使用する前に、中のデータを削除することを指します。書類も安全に破棄する必要があります。データ残余は、メディアを破壊するか、ページすること（機密情報は削除しますが、メディアは再利用のためにそのまま残すこと）で、対処できます。

サニタイズへのアプローチの1つに、メディアを破壊して使用できなくなることがあります。物理的な破壊のオプションはいくつかあります。

- 焼却 - 焼却は、メディアのサニタイズ用に設計された焼却炉で行う限り、すべてのメディアのタイプに有効な方法になります。一般的の焼却炉では、残余が出る可能性があります。
- シュレッディングおよびパルピング - ほとんどのメディアはシュレッダーにかけることができます。書類の場合、シュレッダーは紙面を裁断する残余サイズによってランク付けされます。レベル1は12mmの長片で、レベル6は0.8x4mmの小片になります。裁断された残りを、水を使ってパルプにするか、焼却することで、さらなる保護対策を講じることになります。オフィスで使用するシュレッダーの中には、光学メディアを破棄できるものがあります。工業用シュレッダーでは、ハードドライブやフラッシュドライブが破棄できます。

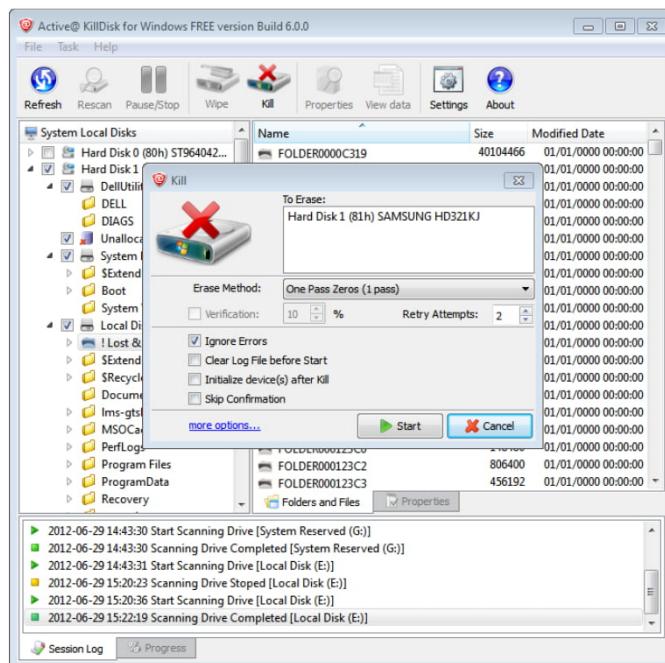
- 粉碎 - ハードドライブをハンマーで叩いても、驚くほど大量のデータが回復可能のまま残るため、この方法は、工業用機械で実施されるべきです。
- 消磁 - ディスクを強力な電磁石にさらし、データを保存しているディスク表面の磁気パターンを破壊します。SSD、フラッシュメディア、光学メディアは消磁できません。ハードディスクドライブのみ消磁できます。

施設のコスト面により、物理的な破壊はサードパーティに委託される可能性があります。信頼できるサービスプロバイダーを使用し、各メディアアイテムがどのようにサニタイズされたかの詳細なインベントリと破壊証明書を取得することが重要です。

データサニタイズのツール

磁気タイプのハードディスクから削除されたファイルは、完全に消去されてはいません。そのセクターは書き込み可能なものとしてマークされ、そこに含まれるデータは新しいファイルが追加されたときに初めて削除されます。同様に、標準のWindowsフォーマットツールを使用した場合も、ファイルへの参照が削除され、すべてのセクターが使用可能なものとしてマークされるだけです。

標準のHDDのサニタイズ方法は、上書きと呼ばれます。これは、ドライブのファームウェアツールまたはユーティリティプログラムを使用して実行できます。最も基本的なタイプの上書きはゼロフーリングと呼ばれ、各ビットを単にゼロに設定します。単一パスのゼロフーリングでは、専門のツールで読み取ることができるパターンを残すことができます。よりセキュアな方法は、最初にすべてゼロのパス、次にすべて1のパス、そして3番目のパスの疑似乱数パターンでコンテンツを上書きすることです。一部のシークレットサービスエージェンシーでは、3回以上のパスが要求される場合があります。パスによって、上書きが完了するまでかなりの時間がかかる場合があります。



データワイピングソフトウェアActive KillDisk。
(スクリーンショットはLSoft Technologies, Inc.の許可を得て使用)



セキュアなファイルまたはディスクの消去をサポートするツールの例には、[Sdelete](#) ([Sysinternals docs.microsoft.com/sysinternals](#)の一部) とDarikのBoot and Nuke ([dban.org](#))、ここに表示されるActive KillDiskサイトが含まれます。

セキュア消去(SE)

2001年より、SATAとSerial Attached SCSI (SAS)仕様に**セキュア消去(SE)**コマンドが追加されました。このコマンドは、ドライブ/アレイユーティリティまたはhdparm Linuxユーティリティを使用して呼び出すことができます。HDDの場合、**ゼロフィーリング**の単一パスを実行します。

SSD、ハイブリッドドライブ、一部のUSBドライブとフラッシュメモリカードの場合、デバイスは、使用できる場所がどこかを、ドライブコントローラーのウェアレベリング(wear-leveling)ルーチンを使用してデバイスにアクセスするソフトウェアプロセスと通信するため、上書き方法は信頼できません。

SSDでは、SEコマンドはすべてのブロックを空とマークします。ブロックとは、eraseコマンドが対象とする、フラッシュメディアの最小単位です。その後ドライブファームウェアの自動ガベージコレクターが、時間とともに各ブロックの実際の消去を実行します。このプロセスが完了していない場合は（進捗状況の指標はない）、残余回復のリスクがありますが、それには専用ハードウェアでチップを分析するために、デバイスからチップを取り外す必要があります。

インスタントセキュア消去(ISE)

自己暗号化ドライブ(SED)のHDDとSSDは別のオプションをサポートし、2012年よりSATA基準とSASの基準で制定されたSANITIZEコマンドを呼び出して、**暗号化消去**を実行します。ドライブベンダーは、これをインスタントセキュア消去(ISE)として実装します。SEDを使用すると、ドライブのすべてのデータはメディア暗号化鍵で暗号化されます。eraseコマンドが発行されるとメディア暗号化鍵が消去され、データは回復不可能になります。FIPS140-2またはFIPS140-3の認証により、暗号化の実装が強固であることが保証されます。

 デバイスのファームウェアで暗号化がサポートされない場合、ソフトウェアのディスク暗号化製品を使用してからキーを破棄して、SEを使用すれば、ほとんどの機密性の要件が満たせるはずです。

レビューアク ティビティ：

物理的なホストのセキュリティ管理

次の質問にお答えください。

1. 保護されているホストへのコンピューター、ネットワーク、ストレージのあらゆる種類の不正な接続を防止することを説明しているポリシーはどれですか？
2. 「ホットアイル」と「コールドアイル」はどこで使用されますか。またその目的は何ですか？
3. ケーブル配線の保護を実施するために使用されるセキュリティ管理は何ですか？
4. オンサイトのバックアップテープの安全性を確保するために使用できる物理的なセキュリティデバイスは何ですか？
5. HDDメディアとSSDメディアの両方と互換性があり、高速動作で、メディアを再利用可能な状態に保つという要件をすべて満たすサニタイズソリューションは何ですか？
6. USBドライブに適していない、物理的に破壊するメディアサニタイズ方法は何ですか？

レッスン21

概要

アクセス、監視、環境的保護、セキュアなデータ破棄における物理的なセキュリティ管理の重要性について説明できる必要があります。

物理的なセキュリティ管理を実装する際のガイドライン

物理的なセキュリティ管理を実装またはアップグレードする際は次のガイドラインに従います。

- 可能な場合、サイトをゾーンとして設計し、該当する場合にはインダストリアルカモフラージュ、DMZ、エアギャップ、金庫室、金庫を使用して、最もセキュアな領域のアクセス制御と監視を最大化します。
- フェンス、バリケード/ボラード、ロック（物理的、電子的、生体認証）を使用して、サイトの境界とアクセスポイントを保護します。スマートカードを使用する場合、クローニング/スキミングが困難なタイプを使用します。
- 警備員、CCTV、ロボット警備員、ドローン/UAVを使用してサイトを監視し、有効な照明を使用して監視を最大化します。
- 警報システム（回路、動きベース、近接型、脅迫状態）を導入して、侵入を検知します。
- 完全性のための2人体制による管理の重要性を考慮し、警備員、受付、IDバッジを使用してアクセスを承認します。
- 温度と湿度の管理、センサー、ホット/コールドアイルの施設の設計、火災検知と消火システムを使用してコンピューティングリソースの環境的なセキュリティを確保します。
- 物理的な破壊またはデータサニタイズ方法のいずれかを使用して、メディアやデバイスを処分する際に残余の削除を確実に実施します。