

ディスクの冗長性

ディスクリソースとストレージリソースは、冗長性に大きく依存します。バックアップではディスクで障害が発生する際に完全性が実現されますが、バックアップから復元するには、新しいストレージユニットのインストール、データの復元、システム構成のテストが必要になります。ディスクの冗長性により、サーバーは1つまたは場合によっては複数のストレージデバイスに障害が発生しても、引き続き作動できるようになります。

Redundant Array of Independent Disks (RAID)

ストレージシステムが**RAID (Redundant Array of Independent Disks)**として構成される場合、多くのディスクはお互いのバックアップとして機能し、信頼性とフォールトトレランスを高めることができます。1つのディスクに障害が発生しても、データが失われることなく、サーバーは引き続き機能できます。RAID Advisory Boardでは、0～6までのRAIDレベルを定義しており、各レベルはフォールトトレランス機能の実現方法がそれぞれ異なります。また、プロプライエタリのあるRAIDソリューションやネスト化されたRAIDソリューションもあります。最も一般的に実装されている種類のRAIDの一部を以下の表にリスト表示します。

RAIDレベル	フォールトトレランス
レベル1	ミラーリングとは、データが2つのディスクに同時に書き込まれ、冗長性を提供することです（ディスクの1つに障害が発生しても、データのコピーはもう1つのディスクにあります）。主な欠点は、ストレージ効率がたったの50%であることです。
レベル5	パリティを付加したストライピングとは、データが3つ以上のディスクに書き込まれますが、追加情報（パリティ）が計算されることを意味します。これにより、ディスクの1つを喪失してもボリュームは継続できます。このソリューションのストレージ効率はRAID 1よりも優れています。
レベル6	ダブルパリティまたは追加パリティストライプが付加されたレベル5では、デバイスを2台喪失してもボリュームは継続できます
ネスト化（0+1、1+0または5+0）	通常はRAIDセットをネスト化することで、パフォーマンスや冗長性が増します。例えば、一部のネスト化されたRAIDソリューションでは、1つ以上のディスクの障害をサポートできます。



RAIDレベル0はパリティのないストライピングを指します。データはいくつかのディスクにわたり、同時にブロックに書き込まれますが、冗長性はありません。これはパフォーマンスを向上できますが、ディスクの1つに障害が発生すると、障害はボリューム全体に及び、そこにあるデータは破損します。RAID 0の使用例はいくつかありますが、一般的にパリティのないストライピングはネスト化されたRAIDソリューションのパフォーマンスを向上させるためのみに実装されます。

マルチパス

RAIDはストレージデバイスの冗長性を提供しますが、**マルチパス**は、サーバーとストレージやRAIDアレイの間バスに重点が置かれます。ストレージシステムには、ある種のコントローラーを通じてアクセスできます。コントローラーはサーバーにローカルで取り付けられたディスクユニットに接続されている場合や、ストレージエリアネットワーク(SAN)内のストレージデバイスに接続されている場合があります。マルチパス入力/出力(I/O)により、コントローラーの冗長性やストレージデバイスへの複数ネットワークのバスが確保されます。

地理的な冗長性とレプリケーション

データのレプリケーションとは、1箇所以上の場所でデータの正確なコピーを維持する技術です。RAIDのミラーリングとパリティでは、ローカルストレージデバイス間でレプリケーションを実装します。データのレプリケーションはその他多くの状況で適用できます。

- ストレージエリアネットワーク(SAN) – ほとんどのエンタープライズストレージはSANとして構成されています。SANは、ファイバーチャネル、SCSI (Small Computer System Interface) またはInfinibandなどの技術が採用された高スピード光ファイバーストレージデバイスネットワークです。冗長性はSAN内で提供でき、またレプリケーションもWANリンクを使用してSAN間で実現できます。
- データベース – ほとんどのデータはデータベース内に格納されます。データベースは複数のサーバーやサイト間で複製されますが、複製間で一貫性を保つことが非常に重要になります。データベース管理システムにはさまざまな種類のレプリケーションを実装する専用ツールが搭載されています。
- 仮想マシン(VM) – 複数の場所で同じVMインスタンスがデプロイされる必要がある場合があります。これはVMのディスクイメージと構成設定を複製することで達成できます。

地理的分散

地理的分散は、お互いに物理的に離れているホットサイトやウォームサイトを複製するデータを指します。これは、自然災害によっていずれかの拠点のストレージが消失しても、データを保護できることを意味しています。またこれは、地理的冗長性（ジオリダンダンシー）とも呼ばれます。

非同期レプリケーションと同期レプリケーション

同期レプリケーションは、すべての複製に同時にデータを書き込むように設計されています。よって、すべての複製には常に同じデータがあるはずです。非同期レプリケーションでは、まずプライマリストレージにデータを書き込み、その後スケジュールされた間隔で複製にデータをコピーします。

非同期レプリケーションは、異なる地域からアクセスされる商品在庫リストのデータなど、複数の場所にあるデータの一貫性が求められるソリューションには適していません。複数の地域にあるデータセンター間の距離のため、多くの地理的冗長性のあるレプリケーションサービスは非同期レプリケーションに依存しています。場合によっては、ビジネスソリューションとして非同期レプリケーションの制限を回避することができます。例えば、オンラインショップは、その地域の倉庫の在庫のみを表示することもできます。

オンプレミスとクラウド

冗長性とレプリケーションによる高可用性は、特に複数のホットサイトとウォームサイトを構成する場合はリソースを大量に消費します。オンプレミスサイトの場合、地理的に分散された2つのホットサイト間で必要なストレージデバイスと高帯域幅、低レイテンシーのWANリンクをプロビジョニングすることは、多額のコストがかかる可能性があります。このコストは、クラウドを効率的に運用するCSPを信頼している場合、クラウドサービスの大きな推進要因の1つになります。クラウドサービスには、局所的および地理的な冗長性が組み込まれています。例えばクラウドでは地理的冗長性により、離れた2つの地域にあるデータセンター間のデータやサービスが複製できます。地震、ハリケーン、洪水など地域レベルで発生する災害は、複数のゾーンにまたがる可用性に影響を及ぼすべきではありません。

レビュー アク ティビティ：

冗長性戦略

次の質問にお答えください。

1. MTDは可用性にどのように関連していますか？
2. エラスティシティとスケーラビリティの違いは何ですか？
3. 24時間を超える停電において冗長電源を確保するために必要な2つのコンポーネントは何ですか？
4. RAIDではどのようにフォールトトレランスをサポートしますか？

トピック20B

バックアップ戦略を実装する



対象試験範囲

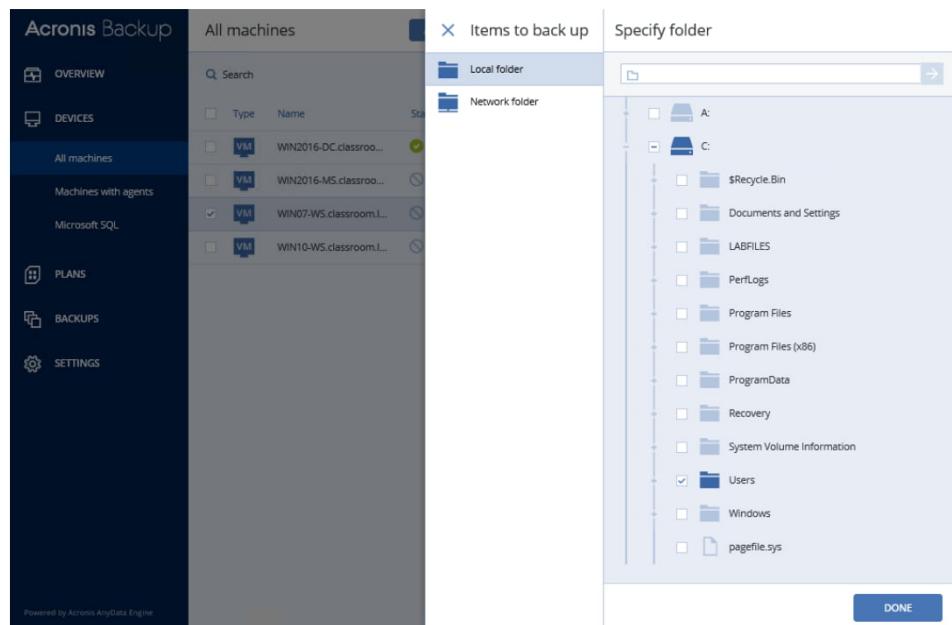
2.5与えられたシナリオに基づいて、サイバーセキュリティのレジリエンスを実装することができる

サイバーセキュリティプログラムは、重要なデータとシステム構成をバックアップし、復元するための有効で検証済みのシステムがなければ完全ではありません。あなたはセキュリティの専門家として、さまざまなシナリオに最適なバックアップの種類とメディアを選び、非永続性によって、よりセキュアなシステム構成を実現し、高可用性を維持する方法を説明できる必要があります。

バックアップと保持ポリシー

すべての事業継続計画と災害復旧計画は、何らかの種類の**バックアップ**を利用します。バックアップの実行とその頻度は、ポリシーに従って慎重に計画する必要があります。データの保持は、短期と長期の両面から検討する必要があります。

- 短期的には、頻繁に変更されるファイルは、バージョンコントロールの目的で保持する必要があります。短期的な保持は、マルウェア感染からの回復にも重要となります。例えば、月曜日にバックアップしたファイルが火曜日にウイルスに感染したとします。その後、ファイルをバックアップすると、月曜日に作成されたコピーは上書きされてしまいます。こうなると、感染していないファイルのバージョンを復元する方法はありません。短期的な保持は、最新のメディアセットが上書きされる頻度によって決まります。
- 長期的には、法的要件や会社のポリシー、業界標準を遵守するためにデータを保管する必要があります。最も古いセットを過ぎた特定のバージョンで保持する必要があるデータは、アーカイブストレージに移動する必要があります。



Acronis Backupを使用してバックアップを実行。(スクリーンショットはAcronisからの許可を得て使用。)

こうした理由のため、バックアップは特定の時点までさかのぼって保管されます。バックアップには、かなりの容量が必要になります。限りあるストレージ容量を有効活用するには、ストレージ管理ルーチンの導入が必要となります。これらを利用することで、必要な回復ウィンドウを十分にカバーしながら、バックアップストレージメディアに保存されているデータ容量を削減することが可能になります。回復ウィンドウは、事業継続計画に従い決定されたRPO（回復ポイントの目標）を基に定められます。高度なバックアップソフトウェアでは、特定の保持ポリシーに従い、メディアセットが上書きされるのを防ぐことができます。

Acronis Backupを使用してドメインコントローラーをバックアップ - [How Long to Keep] フィールドで保持期間を指定します。(スクリーンショットはAcronisからの許可を得て使用。)

バックアップの種類

エンタープライズのバックアップ操作をサポートするユーティリティには、保持ポリシーとメディアローテーションをサポートする機能があります。オリジナルデータをバックアップする場合、バックアップ方法は「完全」、「増分」、「差分」の3種類から選択できます。Windowsの場合、**完全バックアップ**には選択したすべてのファイルとディレクトリが含まれますが、増分/差分バックアップではファイルを含める前にアーカイブ属性のチェックが行われます。アーカイブの属性は、ファイルが変更されるたびにセットされます。これにより、バックアップソフトウェアはこの属性をチェックすることで、ファイルが変更されたかどうか、つまりコピーする必要があるかどうかを判断します。



Linuxではファイルアーカイブ属性をサポートしていません。その代わりに変更の有無の確認には、日付スタンプを使用します。

完全バックアップ、増分バックアップ、差分バックアップの種類

次の表は、3種類のバックアップ方法をまとめたものです。

タイプ	データ選択	バックアップ/復元時間	アーカイブ属性
完全	前回いつバックアップされたかに関係なく、選択されたすべてのデータ	長い/短い（1つのテープセット）	クリアされる
増分	新しいファイルと、前回のバックアップ以降に変更されたファイル	短い/長い（複数のテープセット）	クリアされる
差分	すべての新しいファイルと、前回の完全バックアップ以降に変更されたファイル	中間/中間（最高2つのテープセット）	クリアされない



差分バックアップと増分バックアップ、復元操作。

使用する方法を決定する要因は、復元にかかる時間と、バックアップにかかる時間になります。バックアップが毎営業日に実行されると仮定する場合、**増分バックアップ**ではその日に変更されたファイルのみが含まれますが、**差分バックアップ**では、前回の完全バックアップ以降に変更されたすべてのファイルが含まれます。増分バックアップでは、バックアップ時間が節約できますが、システムを復元しなければならない場合に時間がかかる可能性があります。システムは前回の完全バックアップと、その後に行った各増分バックアップから復元される必要があります。差分バックアップシステムでは、復元が必要となるときに2つのテープセットのみを使用します。



差分バックアップと増分バックアップを組み合わせることはできません。完全バックアップをベースに、差分バックアップと増分バックアップのどちらか1つを使用することが推奨されます。

コピーバックアップ

ほとんどのソフトウェアは、コピーバックアップ機能も備えています。コピーバックアップは、テープのローテーションシステムに関係なく行われるため、アーカイブ属性に影響しません。

スナップショットとイメージ

スナップショットは、開いているファイルの問題を回避する方法です。バックアップを検討しているデータが、SQLデータ、またはExchangeメッセージングシステムなどのデータベースの一部である場合、そのデータはおそらく常に使用されています。多くの場合、コピーベースのメカニズムでは、開いているファイルのバックアップはできません。ファイルとデータベースを閉じなければ、コピーベースのシステムは機能しません。スナップショットは、ファイルシステムによって管理されるデータのある時点のコピーです。バックアッププログラムでは、ライブデータではなくスナップショットを使用して、バックアップを実行できます。Windowsの場合、**ボリュームシャドウコピーサービス(VSS)**によってNTFSボリュームにスナップショットが提供されます。これらはSunのZFSファイルシステムと、一部のLinuxエンタープライズディストリビューションでもサポートされます。

The screenshot shows the Acronis Backup software interface. On the left, there's a sidebar with navigation links: Overview, Devices, Plans, Backups, Settings (Administrators, Agents, Licenses, SAN storage, Storage nodes), System settings, and Tape management. The 'System settings' link is highlighted. The main panel has tabs for 'System settings' and 'Volume Shadow Copy Service (VSS)'. The 'Volume Shadow Copy Service (VSS)' tab is active. It contains several configuration options:

- Use VSS when taking snapshots:** A toggle switch between 'No' and 'Yes'. 'Yes' is selected.
- Automatically select snapshot provider:** A radio button selected.
- Use Microsoft Software Shadow Copy provider:** An unselected radio button.
- Enable VSS full backup:** An unselected checkbox.
- VSS notifications:** A note explaining VSS notifies VSS-aware applications about the backup start to ensure data consistency.

At the bottom right of the main panel is a 'SAVE' button.

Acronis BackupでVSSを設定。（スクリーンショットはAcronisからの許可を得て使用。）

通常は、仮想システムマネージャーでVMのスナップショットまたはクローンコピーが作成できます。スナップショットは、元のVMに接続されたままになりますが、クローンされたイメージが作成された時点から、クローンは別のVMになります。

イメージバックアップは、OSインストールを複製することで作成されます。これは、物理的なハードディスクまたはVMの仮想ハードディスクのいずれかから実行できます。**イメージング**により、サードパーティのソフトウェア、パッチ、構成設定を再インストールすることなく、すみやかにシステムを再デプロイできます。ユーザーデータファイルはすぐに古くなるため、通常、システムイメージにはこれらのファイルは含めないようにしてください。

バックアップストレージに関する問題

バックアップされ、アーカイブされたデータは、ライブデータと同様に安全に保管される必要があります。データバックアップには、ソースと同じ機密性と完全性に関する要件があります。また、独自の可用性の要件があります。通常バックアップメディアは、他のサーバーやネットワーク機器と一緒に建物の限られた場所に保管することで、窃盗やスヌーピングから物理的に保護されます。多くのバックアップソリューションでは、メディアが窃盗された場合に、データの機密性を確保するために暗号化が使用されます。

オフサイトストレージ

ライブデータとバックアップセットの両方を危険にさらす可能性のあるイベントを考慮する必要があります。火災、地震、洪水などの自然災害が発生する場合、組織はデータのバックアップをオフサイトで保管していない限り、データのバックアップがないままになる可能性があります。距離の考慮とは、さまざまな災害シナリオを想定して、どのくらいの距離のオフサイトにバックアップを保存する必要があるかを計算することです。メディアは災害による損害を受けないように十分に遠くに保存する必要がありますが、他方でメディアにアクセスするために回復操作が遅くなりすぎないようにしてください。

必要な帯域幅をサポートできるネットワークがない場合、オフサイトメディアは、物理的にオンラインに移動し（オフサイトメディアの予備セットがない場合、データはこの時点でかなりのリスクにさらされています）、最新のバックアップを実行して、オフサイトストレージに再び移動する必要があります。これを行うための困難さや費用とは別に、データの運搬にはデータの機密性とセキュリティの問題があります。近年、高帯域幅インターネットと大容量のクラウドストレージプロバイダーは、オフサイトバックアップソリューションをはるかに手頃な価格で簡単に実装できるようにしています。

オンラインバックアップとオフラインバックアップ

オンライン/オフサイトに関する考慮事項のほか、オンラインバックアップとオフラインバックアップの間の区別にも注意する必要があります。オンラインバックアップシステムでは、管理者がデバイスを運んで接続したり、バックアップメディアをロードしたりすることなく、バックアップや復元操作をすぐに実行できます。オフラインバックアップは、ホストから切断し、手動で接続する必要があります。

オンラインシステムの方が高速ですが、オフラインバックアップの方がセキュリティは高まります。例えばクリプトランサムウェアのケースを考慮してみてください。バックアップシステムが感染したホストに接続されている場合、ランサムウェアがバックアップを暗号化して、使用できないようにします。一部のクリプトランサムウェアは、クラウドアカウントへのアクセスとクラウドストレージの暗号化を試みるように構成されています(f-secure.com/v-descs/articles/crypto-ransomware.shtml)。



3-2-1ルールでは、2つのメディアタイプで3つのデータコピーを作成し、コピーの1つはオフライン・オフサイトで保管される必要があります。

バックアップメディアの種類

バックアップ操作では、さまざまなメディアのタイプが使用できます。各タイプには多かれ少なかれ、特定のシナリオに適しているメリットとデメリットがあります。

ディスク

個別のリムーバブルハードドライブはSOHOネットワークバックアップに最適な低成本オプションですが、自動化されたエンタープライズバックアップソリューション内で使用するには、十分な容量や柔軟性がありません。

ネットワーク接続ストレージ(NAS)

NAS（ネットワーク接続ストレージ） アプライアンスとは、Windows File Sharing (SMB)やFTPなどの一般的なネットワークプロトコルでRAIDストレージを利用するようにする、特別に構成されたサーバーの種類です。NASアプライアンスは、IPアドレスを介してアクセスされ、バックアップはファイルレベルで行われます。NASは、SOHOバックアップにおけるもう1つの優れたオプションですが、単一デバイスとして、オフサイトオプションは提供されません。通常はオンライン状態で運用されるため、クリプトランサムウェアに対しても脆弱性があります。

テープ

デジタル**テープ**システムは、数テラバイトのストレージ要件がある組織にとって人気の選択です。テープのコスト効率は非常に高く、メディアローテーションシステムがあれば、テープをオフサイトに運搬できます。最新世代のテープでは、カートリッジあたり10～12テラバイト、または圧縮で最大約30TB保存できます。テープの主な欠点は、ディスクベースのソリューションと比較すると、特に復元操作に時間がかかることです。

ストレージエリアネットワーク(SAN)とクラウド

RAIDアレイまたはテープドライブ/オートローダーは、直接接続ストレージとして、通常は**Serial Attached SCSI (SAS)**経由で、サーバーがバックアップデバイスを収容します。直接接続ストレージのスケーラビリティには限界があるため、多くの場合、企業やクラウドのストレージソリューションでは、サーバーで取り扱うファイルシステムオブジェクトと、実際のストレージメディアの構成との間の抽象化レイヤーとして**ストレージエリアネットワーク(SAN)**を使用することがよくあります。NASではストレージへのファイルレベルのアクセスを使用しますが、SANはブロックレベルのアドレス指定に基づいています。SANでは同じネットワーク内でRAIDアレイとテープシステムを組み込むことができます。SANではレプリケーションを通じてオフサイトストレージを実現できます。

復元順序

サイトで制御不能の機能停止が発生する場合、理想的な状況は、処理が代替サイトに切り替えられ、サービスを中断することなく機能停止を解決できることです。代わりとなる処理サイトが利用できない場合、メインのサイトはできる限りすぐにオンラインに戻し、サービス中断を最低限に抑える必要がありますが、これは、そのプロセスを大急ぎで行うということではありません。データセンターやキャンパスのネットワークなどの複雑な施設は、慎重に設計された**復元順序**に従って再構築が必要があります。制御されていない方法でシステムをオンラインに戻す場合、電源の問題がさらに発生したり、さまざまなアプライアンスとサーバー間の依存関係が満たされていないため、ネットワーク、OS、またはアプリケーション層で問題が発生したりする深刻なリスクがあります。

非常に一般的な復元順序は次のとおりです。

1. 電力供給システム（系統電力、配電ユニット [PDU]、UPS、予備発電機など）を有効にし、テストします。
2. スイッチインフラストラクチャ、その後にルーティングアプライアンスとシステムを有効にし、テストします。

3. ネットワークセキュリティアプライアンス（ファイアウォール、IDS、プロキシ）を有効にし、テストします。
4. 重要なネットワークサーバー（DHCP、DNS、NTP、ディレクトリサービス）を有効にし、テストします。
5. バックエンドとミドルウェア（データベースとビジネスロジック）を有効にし、テストします。データの完全性を確認します。
6. フロントエンドのアプリケーションを有効にし、テストします。
7. クライアントのワークステーションとデバイス、クライアントブラウザアクセスを有効にします。

非永続性

システムを回復する場合、本番環境を再構築する際にマルウェアやバックドアなどの障害からのアーティファクトが削除されているようにする必要があります。これは、非永続性を持つように設計されている環境で容易にできます。**非永続性**とは、特定のインスタンスが処理機能に関して完全に静的であることを意味します。データはインスタンスから分離されているため、構成に問題が発生することなく「新規の」コピーと交換できます。非永続性を確保するためのメカニズムはさまざまあります。

- スナップショット/既知の状態に戻す - これはシステム状態を保存したもので、インスタンスに再適用できます。
- 既知の構成にロールバック - 物理的なインスタンスはスナップショットをサポートしていない可能性がありますが、Windows System Restoreなど、ベースラインシステム構成を回復する「内部」メカニズムがあります。
- ライブブートメディア - もう1つのオプションは、ローカルの読み取り/書き込みハードディスクにインストールするのではなく、読み取り専用ストレージからメモリに起動するインスタンスを使用することです。

新しいインスタンスや交換インスタンスを自動的にプロビジョニングする場合、自動化システムでは、次の2種類のマスター作成手順のうちの1つを使用できます。

- マスターイメージ - これはOS、アプリケーション、パッチがすべてインストールされ、構成されたサーバーインスタンスの「ゴールド」コピーです。これはテンプレートを使用するよりも速いのですが、イメージを最新に保つことはテンプレートを更新するより多くの作業が必要になる場合があります。
- テンプレートから自動構築 - マスターイメージと同様、これはインスタンスのビルト手順です。ソフトウェアでは、マスターイメージを保管するかわりに、テンプレートの手順に従ってインスタンスを構築し、プロビジョニングできます。

レジリエンス戦略を自動化するもう1つの重要なプロセスは、構成検証を提供することです。このプロセスでは、回復ソリューションが各層（ハードウェア、ネットワーク接続、データレプリケーション、アプリケーション）で機能するようにします。インシデントと災害復旧の自動ソリューションには、主要なインジケーターのダッシュボードがあり、観察用データからRPOとRTOのコンプライアンスなどの指標を評価することができます。

レビュー アク ティビティ： バックアップ戦略

次の質問にお答えください。

1. 定期的なWindowsのバックアップジョブの種類で、アーカイブ属性を消去しないものは何ですか？
2. VSSでは、どのようにバックアップソリューションを支援しますか？
3. 次の記述は正しいですか、誤りですか？バックアップメディアはオンラインにできますが、オフラインになります。
4. あなたは、数十テラバイトのデータをホストする数十基のアプリケーションサーバーのバックアップ要件について、ある企業にアドバイスをしています。この企業では、短期バックアップのオンライン可用性と、オフサイトのセキュリティメディア、長期的なアーカイブストレージが必要になります。クラウドソリューションは使用できません。この要件に最適なオンプレミスストレージソリューションの種類は何ですか？
5. 重大なインシデントからサイトを回復する場合、テストされた復元順序に従わない場合のリスクは何ですか？

トピック 20C

サイバーセキュリティレジリエンス戦略を実装する



対象試験範囲

- 2.1 エンタープライズ環境におけるセキュリティコンセプトの重要性を説明することができる
- 2.5 与えられたシナリオに基づいて、サイバーセキュリティのレジリエンスを実装することができる
- 5.3 組織のセキュリティに関するポリシーの重要性について説明することができる

効果的なサイト管理とサイバーセキュリティのレジリエンスは、変更制御と構成管理に依存します。この重要な文書が最新に保たれていない場合、インシデントや障害発生時の対応は混乱し、エラーが生じて、時間を失うことになります。

サイバーセキュリティプログラムの一環として、脅威アクターにとって物事を困難にする技術を実装できるようになる必要があります。多層防御と制御の多様化は、耐性のあるシステムを設計する上で重要になります。偽装と阻害の戦術により、攻撃のコストが増すため、攻撃を抑止できます。

構成管理

対応と復旧管理とは、インシデントや障害の対応と復旧のために作成した一連のポリシー、手順、リソースを指します。これらの管理は、サイバーセキュリティにとって不可欠ですが、大規模に供給することはますます困難になっています。効果的な対応と復旧は、サイトレベルでITシステムがどの程度整備されているかによって大きく異なります。変更や構成の管理を制定する有効な組織的ポリシーが無ければ、対応と復旧ははるかに困難になります。

構成管理では、ICTインフラストラチャの各コンポーネントが文書化された特性から逸脱していない、信頼できる状態にあるようにします。**変更制御**と**変更管理**により、こうしたコンポーネントへの変更によるサービスの中止のリスクを減らすことができます。

ITIL®は、ITサービスの提供に関するベストプラクティス活動とプロセスをまとめた、良く知られた書籍群です。ITILでは、構成管理は次の理解を基に実践されています。

- **サービス資産**とは、ITサービスの供給に貢献するモノ、プロセス、人を意味します。
- 構成アイテム(CI)は、サービスを提供するために使用する特定の管理手順を必要とする資産です。各CIは、何らかのラベル（理想的には標準命名規則を使用）によって識別されている必要があります。CIはそれぞれの属性と関係性により定義され、構成管理データベース(CMDB, Configuration Management Database)で管理されます。
- **ベースライン構成**は、デバイス、VMインスタンスまたはその他のCIが構成される設定のテンプレートで、継続的に一致している必要があります。また監視しているレベルとの比較用に、サーバーが達成したスループットなどのパフォーマンスベースラインも記録できます。
- CMS（構成管理システム）は、CIとその関係性に関する情報を収集、保存、管理、更新、表示するツールとデータベースです。これらの情報は、小規模ネットワークではスプレッドシートやダイアグラムにキャプチャされますが、企業のCMSでは専用アプリケーションを使用しています。
- ネットワーク要素間の複雑な関係を理解するには、ダイアグラムに表すのが一番です。ダイアグラムを使用して、ビジネスワークフロー、論理的(IP)と物理的なネットワークポロジー、ネットワーククラックレイアウトにCIがどのように関わっているかを示すことができます。単にダイアグラムを作成するだけではありません。図は常に最新に保つ必要があります。

資産管理

資産管理プロセスでは、組織にあるすべての重要なシステム、コンポーネント、デバイス、インベントリにあるその他の価値のあるオブジェクトを追跡します。これには、こうした資産に関する情報の収集と分析も含まれるため、従業員はより多くの情報に基づいて変更を行ったり、資産を扱ってビジネス目標を達成できるようになります。

資産の追跡・管理を効率化するために、多くのベンダーがさまざまなソフトウェアスイートやハードウェアソリューションを提供しています。資産管理データベースは必要なだけの情報を格納するように構成できますが、種類やモデル、シリアル番号、資産ID、設置場所、ユーザー、価値、サービス情報などが一般的です。

 ある程度の構成 (CI) が必要な資産に焦点を当てています。組織には、家具などの構成要件がない資産も多く存在します。

資産の識別と標準命名規則

有形資産は、デバイスに付けられたバーコードラベルや無線周波数ID (RFID)タグ（または、単にID番号）により識別できます。RFIDタグとは、資産データでプログラミングしたチップを内蔵したタグです。スキャナーの範囲内にある場合、チップは有効になり、スキャナーに信号を送ります。スキャナーでは、デバイスの場所を更新するよう管理ソフトウェアにアラートします。この方式では、管理ソフトウェアで資産だけでなくデバイスの場所も追跡できるため、窃盗をより困難にします。

ハードウェア資産と、アカウントや仮想マシンなどのデジタル資産に対する**標準命名規則**により、環境の一貫性をより高めることができます。これは、エラーを簡単に見つけることができ、スクリプト化によって簡単に自動化できることを意味しています。命名戦略により、管理者がCMDBやネットワークディレクトリの任意の時点で、特定のリソースや場所のタイプや機能を特定できるようにする必要があります。各ラベルは、ホストとDNS名の規則に従うようにしてください (support.microsoft.com/en-us/help/909264/naming-conventions-in-active-directory-for-computers-domains-sites-and)。ID属性と同様に、有形資産やデジタル資産の場所と機能は属性タグとフィールドまたはDNS CNAMEおよびTXTリソースレコードを使用して記録できます。

インターネットプロトコル(IP)スキーマ

IPアドレススペースのサブネットへの分割は、慎重に計画し、インターネットプロトコル(IP)スキーマで文書化されるべきです。一貫したアドレス割当法を使用することにより、ファイアウォールアクセス制御リスト(ACL)の適用とセキュリティ監視の実行が容易になります(tools.cisco.com/security/center/resources/security_ip_addressing.html)。また、設定エラーが発生する可能性が減り、検知しやすくなります。各サブネット内で、スキーマは手動または静的割り当てに確保されたIPアドレスと、DHCPで割り当てるアドレスプールを区別するべきです。**IPアドレス管理(IPAM)**ソフトウェアスイートを使用して、IPの使用を監視できます。

変更制御と変更管理

サービス管理基準では、変更を要求することと、変更を承認することで、サービス制御を全体的な変更管理プロセス内で別の手順として区別しています。

変更制御

変更制御プロセスを使用して、計画・制御された方法で変更を要求したり、承認したりできます。変更要求は通常、何かを修正する必要が生じた場合や、何かが変更された場合、現在のプロセスやシステムに改善の余地がある場合などに作成されます。変更の必要性は多くの場合、組織への変更を余儀なくされる「リアクティブ（対応的な）」と、内部で積極的に変更に取り組む「プロアクティブ（主体的な）」のどちらかになります。また変更是、潜在的な影響やリスクレベル（重大、重要、軽微、標準など）に応じて分類することもできます。標準的な変更管理プロセスでは、変更の必要性や理由、変更の実施方法を変更要求(RFC)書に記載し、承認申請を行います。

提出されたRFCは、適切な役職者により審査され、影響を受ける利害関係者にその内容が通知されます。標準/軽微な変更は主任や部長レベルで処理できますが、重大/重要な変更は個別のプロジェクトとして扱い、変更諮問委員会(CAB)の承認を受ける場合があります。

変更管理

変更の実施は、依存コンポーネントへの影響などを考慮したうえで慎重に計画するべきです。重大/有意な変更は最初に試験導入してください。すべての変更是、有害な影響や不測の問題が生じた場合に備えて、ロールバック（修復）プランを準備しておく必要があります。また、変更対象のITシステムに依存する事業部門のワークフローに悪影響が及ぶと思われる場合は（システムのダウントIMEなど）、特に慎重に計画しなければなりません。ほとんどのネットワークでは、メンテナンス期間を事前にスケジュールすることでダウントIMEを管理しています。変更の実施後は、その影響を評価し、プロセスを検証して今後の変更管理プロジェクトに役立つ成果を特定して文書に記録してください。

サイトの復元力

エンタープライズレベルのネットワークでは多くの場合、サイトレベルで復元できるようになっています。代替の処理サイトまたは復旧サイトは、同じ（または同様の）サービスレベルを提供できる場所になります。代替の処理サイトは常に利用可能で使用できますが、復旧サイトは設定に時間がかかり、緊急時にのみ使用できます。

オペレーションは、以前のサイトがオンラインに戻るまで新しいサイトにフェールオーバーするように設計されています。フェールオーバーは、冗長なコンポーネント、デバイス、アプリケーション、サイトが、障害が発生した資産の機能を迅速かつ効率的に引き継ぐようにする手法です。例えば、ロードバランサーでは、ロードバランサーの背後にある1つ以上のサーバーまたはサイトで、障害が発生したり、応答に時間がかかる場合に、フェールオーバーを実施します。ロードバランサーがこれが検知すると、代わりとなる処理サーバーやサイトに受信トラフィックをリダイレクトします。よってロードバランサープールにある冗長サーバーにより、サービスの中斷が無いように、または最小限に抑えられます。

サイトの復元はホット、ウォームまたはコールドとして説明されます。

- **ホットサイト**はほぼ即時にフェールオーバーできます。これは一般的に、サイトが既に組織内の所有物で、デプロイできる状態であることを意味しています。例えばホットサイトは、ライブデータセットで常に更新されており、いつでも使用できるコンピューター機器を備えた建物で構成されている場合があります。
- **ウォームサイト**はホットサイトに似ていますが、最新データセットをロードする必要があるという要件があります。
- **コールドサイト**は設定にさらに時間がかかります。コールドサイトは、リース契約が締結されており、必要に応じて機器を何でも設置できる、何もない建物である場合があります。

この規模で冗長性を実現するのは明らかに膨大なコストがかかる可能性があります。多くの場合、サイトはサービスプロバイダーからリースされますが、全国規模の緊急時の場合は、サービスの需要が供給を上回る可能性があります。もう1つのオプションは、企業が相互支援を提供できるように相互協定を結ぶことです。これはコスト効率は高いですが、計画と準備が複雑になります。

また他にも、何かの複製を作成するとそのリソースを適切に保護する複雑性が倍になるという問題があります。メインコピーに適用されるものと同じセキュリティ手順を、冗長サイト、スペアのシステム、バックアップデータにも適用する必要があります。

多くの企業にとって、最もコスト効率の良いソリューションは、処理とデータのストレージをクラウドに移行することです。

多様化と多層防御

通常多層化されたセキュリティは、**多層防御**を実現するため、サイバーセキュリティのレジリエンスを向上していると見なされます。これは、脅威アクターがシステムを完全に侵害するには、制御が多様化された複数のセキュリティ制御を突破しなければならないということを意味しています。こうした層により、攻撃対象領域の可能性を抑え、攻撃を抑止または防止する可能性を高めることができます。また少なくとも攻撃を検知して、手動の介入で防止できるようになります。

技術と制御の多様化

多層防護と並んで、**多様化**による（あるいは多様性を伴う）セキュリティという概念があります。技術の多様化とは、オペレーティングシステム、アプリケーション、コーディング言語、仮想化ソリューションなどが入り混じる環境を指します。制御の多様化とは、制御の層はさまざまな制御機能（防止、検知、是正、抑止）を持つ、異なるクラスの技術制御や管理制御と組み合わせるべきであることを意味しています。

マーケティング部のアランに、ある代理店からの新しい広告用掲示板へのキャンペーンのデザインが含まれるUSBスティックが送られたというシナリオについて考えてみましょう。多層防御がなければ、アランは朝自分のデスクにあったUSBスティックを、あまり深く考えずにノートパソコンに差し込んでいた可能性があります。その時点から侵入に対して脆弱になる可能性があります。このシナリオでは、代理店、ポスト、アランのデスクなど、脅威アクターがメディアを改ざんする機会がたくさんあります。

さまざまなセキュリティ管理をデプロイすることで確立される多層防御により、このシナリオに内在するさまざまなリスクを低減できます。

- ユーザートレーニング（管理的制御）により、メディアを誰もいないデスクに置きっぱなしにしたり、前もってスキャンせずにコンピューターシステムに差し込んではならないことを学びます。
- ノートパソコンのエンドポイントセキュリティ（技術的制御）により、メディアのマルウェアをスキャンし、自動的にアクセスをブロックできます。
- ノートパソコンのUSBポートに差し込むセキュリティロック（物理的制御）により、キーを要求しないメディアの接続を防止し、最初に認証確認を実行るようにします。
- アランのユーザー アカウントを制限するアクセス許可（技術的制御）により、マルウェアが実行されないようにできます。
- 暗号化し、デジタル署名したメディアを使用（技術的制御）することで、改ざんの試みを防止したり、特定したりできます。
- ノートパソコンが危険にさらされる場合、侵入検知とログ/アラートシステム（技術的制御）により、マルウェアがネットワーク上で拡散されることを検知し防止できます。

ベンダーの多様化

複数の種類の制御を導入するのと同様に、ベンダーの多様化を活用することによる利点も考慮するべきです。ベンダーの多様化とは、セキュリティ管理がさまざまなサプライヤーから提供されることを意味します。単一ベンダーのソリューションは、相互運用性が高く、トレーニングとサポートの費用を節約できるため、多くの組織にとって魅力的な選択肢になります。以下はそのデメリットの例です。

- クラス最高のパフォーマンスではない — あるベンダーは有効なファイアウォールソリューションを提供するかもしれません、バンドルされたマルウェアスキャンの有効性は低い可能性があります。
- 複雑性の低い攻撃対象領域 — 単一ベンダーのソリューションでは、サプライヤーのコードにある1つの脆弱性が、複数のアプライアンスをリスクにさらす可能性があります。脅威アクターは、制御と潜在的な弱点を容易に特定できるようになります。
- イノベーションの欠如 — 単一ベンダーに依存することにより、組織はそのベンダーのソリューションに信頼を置きすぎるようになり、新しいアプローチを意欲的に調査し、テストしなくなる可能性があります。

暗号の多様化

この概念は、アルゴリズムの選択や暗号化の実装にまで及ぶことができます。ブロックチェーンベースのIAM(ibm.com/blogs/blockchain/2018/10/decentralized-identity-an-alternative-to-password-based-authentication)などの方法を導入したり、推奨暗号化スイートとしてAESの代わりにChaChaを選択する(blog.cloudflare.com/it-takes-two-to-chacha-poly)ことで、脅威アクターは新しい攻撃方法を開発しなければならなくなります。

偽装と阻害の戦略

多くの場合、サイバーセキュリティの実践は非対称戦争と説明され、防御側がすべての攻撃に勝ち、常時準備が整っているようにする必要があります。脅威アクターは、攻撃するときを選ぶことができ、勝たなければいけないのは1回のみです。一部のサイバーセキュリティ戦術は、攻撃のコストを上げることで、その非対称性を減らすことを目的にしています。これは、脅威アクターが攻撃の計画をするときでさえ、より多くのリソースを投入する必要があることを意味しています。

アクティブディフェンスとは、脅威アクターと関わることを意味しますが、これはさまざまな方法で解釈できます。アクティブディフェンスの1つのタイプには、罠や餌の役割を果たすおとり資産の展開が含まれます。本番環境の資産では難しい、ベースラインのトラフィックと正常な動作を正確に制御できるため、脅威アクターがおとりリソースとやり取りする際の侵入を検知することがはるかに容易になります。

ハニーポット、ハニーネット、ハニーファイル

ハニーポットは、攻撃戦略やツールを分析したり、攻撃の試みを早期に警告したりするため、または実際のコンピューターシステムから注意をそらすおとりとして、脅威アクターをおびき寄せるために設定されたコンピューターシステムです。また、内部の不正、スヌーピング、悪用を検知するためにも使用できます。ハニーネットはおとりネットワーク全体を指します。これは、実際のネットワークとして設定したり、エミュレーターを使用してシミュレートできます。

ハニーポットまたはハニーネットを導入することにより、組織はセキュリティシステムを向上できるようになりますが、脅威アクターがハニーポットシステムを分析して、ネットワークの構成方法や保護方法についてかなり多くのことを学習できるというリスクがあります。多くのハニーポットは、マルウェアの脅威やソフトウェアの悪用、スパマーによるオープンリーメールシステムの悪用について調査するセキュリティ研究者によって設定されます。これらのシステムは通常、インターネットに完全公開されています。本番ネットワークでは、ハニーポットはDMZか、(インサイダーの脅威を探るためにハニーポットが使用される場合に) プライベートネットワークの中の分離されたセグメントに配置される可能性があります。これにより、早期警告ができ、脅威アクターが特定のセキュリティゾーンに侵入できたかどうかの証拠が得られます。セキュリティチームは、攻撃の出所を突き止め、組織から脅威を完全に根絶するためにより総合的な手順を取ることができます。

ハニーポットまたはハニーネットは、ハニーファイルの概念（役に立つと思わせて、実際はフェイクであるデータ）と組み合わせることができます。こうしたハニーファイルは追跡可能にできるため、脅威アクターによって持ち出されると、再利用や悪用の試みが追跡できるようになります。

例えば、ある組織が重要な財務記録を見せかけた、無効な意味のないデータのデータベースを作成するとします。この偽装戦略には、本番環境に挿入したパンくずリスト(breadcrumbs)が含まれており、脅威アクターをスプーフィングされた「戦利品」へと巧妙に導くことができます(fidelissecurity.com/threatgeek/deception/breadcrumbsintelligent-deception)。データベースは防御の低いサブネットの裏に配置され、脅威アクターがこの役に立たないデータを持ち出すように仕向けています。また脅威アクターを特定することにより、組織はアトリビューション戦略を講じることもできます。アトリビューションとは、組織が脅威アクターの役割と、攻撃インテリジェンスとして使用された方法を公開することを意味します。

阻害戦略

もう1つのアクティブディフェンスの種類では阻害戦略を使用します。これには悪意のある脅威アクターによって使用される難読化戦略が一部採用されています。その目的は、攻撃コストを上げ、脅威アクターのリソースを耗殺することです。阻害戦略の例には次のようなものがあります。

- 偽のDNSエントリを使用して、存在しない複数のホストをリスト化します。
- 複数のおとりディレクトリや動的に生成されたページがあるWebサーバーを構成して、スキャンのスピードを低下させます。
- ポートトリガーやスプーフィングを使用して、ホストがポートスキャンを検知する場合に、**偽装テレメトリー**データを返します。これにより、複数のポートが開いていると偽って報告されるため、スキャンのスピードを低下させます。テレメトリーとは、リモートスキャンによって返されるあらゆるタイプの測定やデータを指します。同様の偽装テレメトリーを使用して、例えば使用していないIPアドレスを使用していると報告できます。
- DNSシンクホール**を使用して、疑わしいトラフィックを、分析ができるハニーネットなどの別のネットワークにルーティングします。

レビュー・アクティビティ：

サイバーセキュリティレジリエンス戦略

次の質問にお答えください。

1. あなたは、お客様のために構成管理の基本事項についてのホワイトペーパーを準備しています。すでに、「ダイアグラム」、「標準命名規則」、「インターネットプロトコル(IP)スキーマ」の見出しへを作成しました。CompTIA Security+の対象範囲に基づいてペーパーを作成する場合、含めるべきもう1つのトピックは何ですか？
2. 文書化されたIPスキーマを持たない場合のリスクは何ですか？
3. 組織的なポリシーにおいて、変更について制定する2つの概念は何ですか？
4. サイトの復元力（レジリエンス）レベルについて話し合う際に使用される用語は何ですか？
5. あなたは、エグゼクティブチームのサイバーセキュリティレジリエンスのための多様化戦略に関する要約を準備しています。「技術」、「暗号」、「制御」に関するセクションは準備できました。他に追加する必要があるトピックは何ですか？
6. 偽装ベースのサイバーセキュリティレジリエンス戦略では、どのように脅威アクターに偽装テレメトリを返すことができますか？

レッスン20

概要

冗長性、バックアップ、構成/変更管理、多様化、偽装を使用して、サイバーセキュリティレジリエンスを向上できるようになる必要があります。

サイバーセキュリティレジリエンスを実装する際のガイドライン

以下はサイバーセキュリティレジリエンスを実装するためのガイドラインです。

- 構成管理システムを設定して、以下の項目を最新の状態に保つようにします。
 - 標準命名規則とラベリングを使用して資産を追跡する棚卸表。
 - 各構成アイテムのベースライン構成情報。
 - ワークフローとネットワークに記載された資産の間の関係を表示するダイアグラム。
- ワークフローや資産への変更が変更制御と変更管理のプロセスによって管理されるようにします。
- バックアップ戦略を作成し、復元順序が完全にテストされるようにします
 - さまざまなデータ資産のRPOと回復ウインドウを判断する。
 - データをコンピューティング機能から区別し、回復時に非永続性を確保する。
 - ストレージ要件、オンサイト/オフサイト要件、オンライン/オフラインストレージ要件（ディスク、テープ、NAS、SAN）を満たすメディアを選択する。
 - 完全/増分/差分スキームを実装し、メディアストレージの制限に対応する。
- リスク評価を使用して、高可用性要件がある資産を特定し、冗長性によりこの要件を満たします。
 - 障害から回復するためのホットサイト、ウォームサイト、コールドサイトのリソース。
 - 電源に耐性を持たせるためのデュアル電源、PDU、PSU、発電機。
 - ネットワークに耐性を持たせるためのNICチーミング、複数パス、ロードバランシング。
 - ストレージに耐性を持たせるためのRAIDとマルチパスI/O。
- リスク評価とインパクト分析を使用して、技術、制御、ベンダー、暗号の多様化で、耐性を向上させることができるかどうか特定します。
- 脅威の認識とリスク評価により、おとり/ハニーポット資産、偽装テレメトリなどの偽装とアクティブディフェンス戦略により耐性を向上することができるかどうか判断します。

