

レッスン19

リスク管理の概念を要約する

レッスン概要

企業が1つ以上の脆弱なビジネスプロセスを運用している場合、重要なデータの開示、変更、損失、破壊、または中断が発生したり、顧客へのサービスが失われたりする可能性があります。そのようなセキュリティインシデントから発生する即時的な経済損失とは別に、結果がどうであれ企業の評判は低下してしまいます。銀行が、パートナーと繋がっているトレーディングフロアを1時間でも失うと、組織の主な機能（取引）ができなくなるため、巨額の損失が発生する可能性があります。よって、ネットワークやその他のITシステムを計画する際には、リスク管理を実行して、脅威と脆弱性を評価する必要があります。

リスクの分析は、組織でセキュアな環境を確保するための重要な役割を担っています。ネットワークコンポーネント、ハードウェア、人材に損害をもたらす可能性がある特定のリスクを評価し、特定することで、脅威の可能性を緩和し、損失や法的責任を回避するための正しい是正措置を確立できるようになります。

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。

- リスク管理プロセスと概念を説明する。
- ビジネスインパクト分析の概念を説明する。

トピック19A

リスク管理プロセスと概念を説明する



対象試験範囲

5.4|リスク管理プロセスと概念を要約する

ほとんどの組織には、コンプライアンス要件を満たし、ビジネスを保護するための正式なリスク管理ポリシーとプロセスがあります。こうしたポリシーとプロセスは通常、フレームワークによって実施され、全体的なプロセス内の要因や手順を説明する標準用語があります。重要な評価に参加できるように、リスク管理の主な概念を要約できるようになる必要があります。

リスク管理プロセス

リスク管理とは、企業が顧客にサービスを提供するために必要不可欠な機能に対する脆弱性と脅威を特定し、評価し、緩和するためのプロセスです。このプロセスは、次の5つの段階で実行できます。

1. 任務上必要不可欠な機能を特定する - リスクを緩和するには多額の費用がかかる可能性があるため、集中的に対応することが重要になります。効果的なリスク管理では、任務上必要不可欠な、実行されないとビジネス全体が稼働しなくなる可能性がある機能に重点を置く必要があります。このプロセスの一部には、こうした機能をサポートする重要なシステムと資産の特定が含まれます。
2. 脆弱性を特定する - 機能やワークフローごとに（最も重要なものから開始）、システムと資産を分析し、影響を受けやすい脆弱性や弱点を発見し、一覧にします。
3. 脅威を特定する - 機能やワークフローごとに、脆弱性の利用や悪用、または誤ってトリガーする可能性がある脅威のソースと脅威アクターを特定します。
4. ビジネスインパクトを分析する - 脅威によってセキュリティインシデントとして脆弱性がアクティブになる可能性と、そのインシデントが重要なシステムに与える影響は、リスクの評価に使用される要素になります。インパクトと可能性を分析する方法には、定量的分析と定性的分析があります。
5. リスク対応を特定する - リスクごとに、考えられる対策を特定し、セキュリティ制御を追加するためのコストを評価します。ほとんどのリスクではある種の緩和が必要になりますが、特定のリスクの種類やレベルにはより適切なそれ以外の対応がある可能性があります。

ビジネスプロセスや脅威ごとに、存在するリスクの度合いを評価する必要があります。リスクの算出は複雑ですが、主な2つの変数は可能性とインパクトになります。

- 発生の**可能性**とは、認識される脅威のプロバビリティ（確率）です。
- **インパクト**とは、セキュリティインシデントとして認識される場合のリスクの重度です。これは、資産の価値や、資産が危険にさらされる場合の中止のコストなどの要因によって決まる場合があります。

リスク管理は複雑で、企業や機関の規模、規制やコンプライアンスの要件が異なるため、その扱いは大きく異なります。ほとんどの企業では、NISTのリスクマネジメントフレームワーク(RMF)またはISO 31Kなどのフレームワークに基づいて、**エンタープライズリスク管理(ERM)**ポリシーと手順を制定します。これらの法的要件やフレームワークのコンプライアンス要件は多くの場合、リスク制御の自己評価(RCSA)として整備されています。また組織では、外部当事者とプロセスの先導を契約する場合がありますが、この場合は、リスク制御の評価(RCA)と呼ばれます。

RCSAは、リスクと、そうしたリスクを緩和する制御の効果を特定するためにステークホルダーによって行われる内部プロセスです。RCSAは多くの場合、各部門のマネージャーのアンケートやワークショップを通じて実行されます。RCSAの結果はレポートになります。最新のRCSAレポートは、外部の監査プロセスに不可欠になります。

リスクの種類

一般的なリスクの種類は、特定の脅威や脆弱性のシナリオから生じるものとして特定できます。

外部

外部の脅威アクターは、はっきりと目に見えるリスクのソースの1つです。また、サイバー攻撃よりも広範な脅威を考慮する必要があります。新型コロナ感染症のパンデミックなどの自然災害では、広範囲に広がる配置転換に対応できるITシステムとワークフローが必要であることを示しています。最も重大な種類のインパクトは、人命の損失や致命的な傷害に繋がる可能性のあるものです。命と安全に対する最も明らかなリスクは、自然災害、人為的災害、火事などの事故から発生します。

内部

内部リスクは、組織が所有し管理する資産とワークフローから発生します。内部リスクをレビューする際、そうしたリスクが悪意のあるもの、偶発的なもの、または悪意のないものとして分類できることを覚えておくことが重要です。内部脅威には、一時的なアクセス許可を付与された請負業者が含まれます。

マルチパーティ

マルチパーティリスクとは、有害事象が複数の組織に影響を及ぼすことを指します。マルチパーティリスクは通常、サプライヤーとの関係から発生します。重要なイベントによりサプライヤーや顧客に中断が発生すると、自身の組織が被害を受けることになります。これらは多くの場合、波及効果として説明されます。例えば、5本の指に入るお得意様の1つが、データ侵害のために廃業する場合、自身の会社もかなりの収益を失うことになります。こうしたサプライチェーンの関係にある組織は、チェーンを通じたサイバーセキュリティの認識と能力を向上させることに関心を寄せています。

マルチパーティの関係の観点から**リスク評価**がどのように変化するかを示す例として、もともとラップトップで使用するためのワイヤレスアダプターを製造している会社について考えてみましょう。もともとの使用では、ファームウェアのアップグレードプロセスのセキュリティは重要ですが、人命や安全には何の影響もありません。ですが同社では、車載電子システムを接続するアダプターを供給する新しい契約を取り付けました。同社には知らされていなかった車載システムの設計における弱点により、脅威アクターは侵害されたワイヤレスアダプターのファームウェアを使用して、車両の制御システムに影響を及ぼすことができるようになります。これでアップグレードプロセスの完全性には、安全面におけるインパクトができ、リスクは遥かに高くなります。

知的財産(IP)の盗難

知的財産(IP)とは、組織が所有する商業的価値のあるデータです。これは、小売用の著作物（ソフトウェア、著作物、映像、音楽）、製品のデザインや特許を意味します。IPデータが流出する場合、商業的価値の多くが失われます。強力な法的保護のない地域では、損失からの回復は非常に困難になります。

ソフトウェアコンプライアンス/ライセンシング

ソフトウェアのインストールに条件を課すエンドユーザー使用許諾契約書(EULA)の条件に違反すると、コンピューターの所有者に多額の罰金が科せられる可能性があります。ライセンスの問題は、ユーザーが変更管理の承認なく、ソフトウェアをインストールするシャドーITから発生する可能性が最も高くなります。ネットワークインベントリ管理スイートでは、各ホストでのソフトウェアのインストールをレポートし、購入したライセンスのシート数に関連付けることができます。仮想化とクラウドが関連する場合は特に、ライセンシングモデルも複雑になる可能性があります。各製品に対する特定のライセンス条件について、管理スタッフを指導することが重要になります。

レガシーシステム

レガシーシステムは、セキュリティアップデートを受けることがなくなり、システムの保守とトラブルシューティングを行うための専門知識が不足するため、リスクの原因になります。

定量的リスク評価

可能性とインパクトを評価するためにリスク分析を実行するには、定量的と定性的の2つの方法があります。



定量的リスク評価は、各リスク要因に具体的な価値を割り当てる目的としています。
(画像提供：© 123RF.com)

定量的リスク評価は、各リスク要因に具体的な価値を割り当てる目的としています。

- **単一損失予想(SLE)** - リスク要因が1回発生する場合の損失金額。これは、**資産の価値に暴露係数(EF)**を掛けて算出されます。EFは、資産の価値に対する損失割合です。
- **年間予測損失額(ALE)** - 年間を通じて損失する可能性のある金額です。これは、**SLE**に**年間発生率(ARO)**を掛けて算出されます。

資産の価値は、その物的価値だけを指すのではないことを認識することが重要です。その他の主な2つの考慮事項として、危険にさらされる資産に関連する直接コスト（ダウントIME）と、その結果として生じる企業の評判などの無形資産のコストがあります。例えば、サーバーには数百ドルの物的コストがかかる場合があります。そのサーバーが盗まれると、回復または交換されるまで営業できないことで発生するコストは、数千ドルに及ぶ可能性があります。また、中断している間は、注文ができなかったり、注文を充足できないため、顧客が別のサプライヤーを探し、何千件もの売上損失と信用が失われる可能性があります。

定量的リスク評価の問題は、こうした価値を決定し、割り当てるプロセスが複雑で、時間がかかることです。割り当てられた価値の正確度も、過去のデータがなくては判断することが困難です（多くの場合、主観的な推測に基づいています）。ですが、時間の経過とともに経験を積むと、このアプローチによって資産とリスクに関する詳細で洗練された記述が得られ、セキュリティ経費を正当化して優先順位を付けるための適切な基盤として使用できるようになります。

定性的リスク評価

定性的リスク評価では、定量的アプローチの複雑さを避け、重要なリスク要因の特定を重視します。定性的アプローチでは、どのリスク要因が重要かという人々の意見が求められます。資産とリスクはシンプルなカテゴリーに分けられます。例えば、資産は「交換不可」、「高価値」、「中価値」、「低価値」として分類でき、リスクは一度限りまたは反復的、プロバビリティ（確率）は「クリティカル」、「高」、「中」、「低」と分類できます。

もう1つのシンプルなアプローチとして、ヒートマップまたは「信号機」インパクトマトリックスがあります。リスクごとに、単純な「赤」、「黄」、「緑」のインジケーターを各列に入れ、リスクの重度、その可能性、制御コストなどを示すことができます。このアプローチは単純ですが、セキュリティを向上させるためにどの部分に尽力すべきかが一目で分かるようになっています。

リスク要因	影響	ARO	管理コスト	全体的なリスク
旧バージョンの Windows クライアント				
訓練されていないスタッフ				
ウイルス対策ソフトウェアなし				

信号機のインパクトグリッド。

FIPS 199 (nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf)では、機密性、完全性または可用性の侵害が組織全体に及ぼすインパクトに基づいて、情報システムにセキュリティ分類(SC)を適用する方法について説明しています。潜在的なインパクトは次のように分類できます。

- 低 - 資産への損害や損失またはパフォーマンスの損失は低い（重要な機能は引き続き機能する）。
- 中 - 資産やパフォーマンスに大きな損害や損失がある。
- 高 - 多大な損害や損失、または1つ以上の重要機能が実行不能になる。

リスク管理戦略

定量的分析または定性的分析の結果は、固有リスクの尺度になります。固有リスクは、あらゆる種類の緩和策が試される前のリスクのレベルです。

理論的には、セキュリティ管理や対策は、各リスク要因に対処するために導入します。問題は、セキュリティ管理が高額になる可能性があることなので、リスクに関連するコストと管理にかかるコストのバランスを取る必要があります。リスクを排除することは不可能です。代わりに組織が受容できるレベルのリスクになるまでリスク要因を緩和することを目標にしてください。リスク管理の全体的なステータスは、リスク体制と呼ばれます。リスク体制は、どのリスク対応オプションを特定し、優先順位を付けるかを示します。例えば、次の優先順位を特定できます。

- セキュリティ管理を導入し、リスクを低減するための実証可能な取り組みを行うための規制上の要件。リスク管理を義務付ける法律と規制の例には、SOX、HIPAA、グラム・リーチ・ブライリー法、国土安全保障法、PCI DSS規則、その他のさまざまな個人データ保護措置が含まれます。
- 脅威の可能性にかかわらず、高価値資産。
- 高い可能性の脅威（高ARO）。
- 脅威の可能性を増す手順、機器、またはソフトウェア（レガシーアプリケーション、ユーザートレーニング不足、古いソフトウェアバージョン、パッチが未適用のソフトウェア、不要なサービスの実行、監査手順を講じていないなど）。



定量的アプローチの場合、導入したセキュリティ管理によって生じる損失の削減に基づき、新しいROIを計算することでセキュリティ投資対効果(ROI)を決定できます。ROIの計算式は次のとおりです。 $[(ALE - ALE_m) - \text{ソリューションのコスト}] / \text{ソリューションのコスト}$ 。ALEは管理導入前のALEで、ALE_mは管理導入後になります。

リスク緩和（または修復）は、リスク要因への暴露またはリスク要因の影響を減らすための全体的なプロセスです。脅威や脆弱性への暴露を減らす対策を導入している場合、それは**リスク抑止（または低減）**となります。リスク低減とは、リスクインシデントの可能性を減らしたり、コストを抑えられること（または両方）ができる管理を指します。例えば、火災が脅威の場合、サイトでの可燃物の使用を厳しく制御するポリシーにより可能性を減らすことができ、警報とスプリンクラーのシステムは、インシデントを（できれば）小さなエリアに封じ込めることで影響を減らすことができます。もう1つの例は、オフサイトのデータバックアップがあります。これは、サーバーが火災によって破壊された場合の修復オプションを提供します。

リスク回避とリスク移転

回避とは、リスクを含むアクティビティを止めることを意味しています。例えば、ある企業が在庫を管理するための社内アプリケーションを開発し、その販売を試みるとしています。アプリケーションを販売している間に、さまざまなセキュリティの脆弱性が発見され、苦情や法的措置の脅威が発生する場合、企業ではソフトウェアのセキュリティを維持するためのコストは収益に見合わないと判断し、販売を中止する可能性があります。当然ですが、これでは既存の顧客にかなりの不快感を与えるでしょう。多くの場合、回避は信用が得られるオプションではありません。

移転（または共有） は、保険会社または責務を明確に定めるサプライヤーとの契約など、サードパーティにリスクを割り当てるることを意味しています。例えば、企業はeコマースサイトの社内メンテナンスを停止し、サービスをサードパーティに委託できます。サードパーティは詐欺やデータの窃盗の責任を負います。特定のサイバーセキュリティの保険やサイバー責任の補償範囲では、データ侵害やDoS攻撃から生じる罰金や責任から保護されます。



このようなケースでは、明らかなリスクを移転することは比較的簡単ですが、会社の評判に対するリスクは残っていることに注意してください。安全ではないeコマースアプリケーションを使用したことにより、顧客のクレジットカードの詳細が盗まれる場合、顧客は、名目上のセキュリティに関する責任があなたにあるか、サードパーティにあるかということは気にかけません。また、この方法で法的責任が完全に移転される可能性は低いです。例えば保険の条件では、ベストプラクティスのリスク管理が実装されていることが要求される可能性があります。

リスク受容とリスク選好

リスクをゼロまで減らすことはできないため、リスク体制の一部は、残っているリスクの管理に関与します。

リスク受容

リスク受容（または容認）は、リスクのレベルがコストをかける根拠にはならないため、または対策が導入される前に避けられない遅延が生じるため、対策が講じられていないことを意味します。この場合、リスクを無視するのではなく、監視を続ける必要があります。

残留リスクとリスク選好

固有リスクが緩和する前のリスクであるのに対し、**残留リスク**とは、特定の緩和、移転または受容の対策が適用された後の可能性と影響です。リスク選好とは、どのレベルの残留リスクが許容できるかについての、戦略的評価です。リスク選好の範囲は広範に及びます。リスク受容が単一システムの範囲であるのに対し、リスク選好はプロジェクトまたは機関全体の範囲になります。リスク選好は規制とコンプライアンスによって制約されています。

制御リスク

制御リスクは、時間が経つにつれ、セキュリティ管理の効果がどの程度低下したかを示す尺度です。例えば、ウイルス対策でシグネチャに基づいてマルウェアを適切に検知できるようになったとしても、脅威アクターがコードの難読化を行えば効果が低下します。また制御リスクは、固有リスクの緩和においてまったく効果がなかったセキュリティ管理を指す場合もあります。これは、リスク管理が継続的なプロセスであり、継続的な再評価と再優先順位付けが必要であるという点を示しています。

リスク認識

ビジネスのステークホルダーに各リスクシナリオを理解してもらうために、資産の所有者が原因と結果を明確に把握できるように表現する必要があります。DoSの場合、どのようにリスクが発生し、結果として誰に対するどのようなアクセスが拒否されるのか、ビジネスに対する影響はどうのようなものであるかを、わかりやすい言葉で説明する必要があります。例：公開されているWebサイトへの悪意のある行為やハッキング行為の結果、サイトが過負荷状態になり、クライアントが注文アカウントにアクセスできなくなります。この結果、長期間における売上の損失、多額の収益減の可能性があります。

リスクの登録は、リスク評価の結果を分かりやすい形式で示す文書です。リスク登録は、インパクトと可能性の評価、特定日、説明、対策、所有者/エスカレーションルート、および状況の列を持つ、先に示したヒートマップリスクマトリックスに似ているかもしれません。また、リスクの登録は一般的に散布図として表されます。散布図でインパクトと可能性はそれぞれ座標軸であり、プロット点は、プロットされたリスクの性質に関する詳細情報を含む凡例に関連付けられています。リスクの登録はステークホルダー（役員、部長、上級技術者）間で共有され、全員が管理するワークフローに関連するリスクを理解できるようにすべきです。

レビュー アク ティビティ：

リスク管理プロセスと概念

次の質問にお答えください。

1. 複数の当事者に関するリスクを評価する場合、ビジネスまたはワークフローのどのエリアを調べる必要がありますか？
2. シャドー ITに起因するリスクの種類は何ですか？
3. 特定の機能や資産への特定の脅威のためにリスクの定量的計算を行う際に使用できる指標は何ですか？
4. 全体的な予算の観点から、セキュリティ管理の選択を決定する要因は何ですか？
5. 保険の加入によって得られるリスク緩和オプションの種類は何ですか？
6. リスクの登録とは何ですか？
7. 管理リスクとは何ですか？

トピック19B

ビジネスインパクト分析の概念を説明する



対象試験範囲

5.4!リスク管理プロセスと概念を要約する

ビジネスインパクト分析では、組織を動かすワークフローとそれを支える重要な資産やシステムを文書化することで、リスク評価に反映させます。主な指標では、こうしたシステムで耐えることができるダウンタイムを定量化します。あなたはセキュリティの専門家として、頻繁にこの種の分析の作成を依頼されます。

ビジネスインパクト分析

ビジネスインパクト分析(BIA)は、さまざまな脅威シナリオで発生する可能性がある損失を評価するプロセスです。例えば、DDoS攻撃により、eコマースポータルが5時間停止する場合、ビジネスインパクト分析では、過去のデータに基づき、実行されなかった注文と、顧客が別のサプライヤーに永久に移動したことによる損失を定量化できます。DoS攻撃の可能性は、年率ベースで評価し、コスト面における年間インパクトを判断できます。その結果、負荷分散や管理されたDDoSの緩和などのセキュリティ管理が、投資する価値があるかどうかの評価に必要な情報が得られます。

BIAではリスクが特定され、事業継続計画(BCP)では、組織が何らかの有害事象に直面した場合に重要なワークフローを維持できる制御やプロセスが特定されます。



用語オペレーション継続計画(COOP)は、同じ種類の活動が、企業ではなく政府機関によって行われる場合を指します。

任務上必要不可欠な機能

任務上必要不可欠な機能(MEF)は、保留できない機能です。これは、組織ができる限り継続的に機能を実行できる必要があり、サービスの中止がある場合、任務上必要不可欠な機能がまず復旧されなければならないことを意味します。



ビジネスまたはMEFのサポートしますが、それ自体は重要ではない機能は、主なビジネス機能(PBF)と呼ばれます。

任務上必要不可欠な機能の分析は、一般的に次の4つの主要な指標によって管理されます。

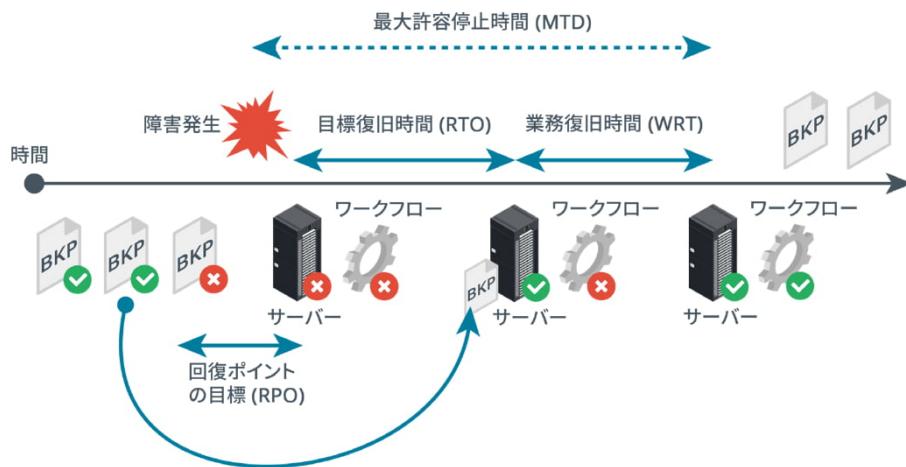
- **最大許容停止時間(MTD)**は、回復不可能な経営破綻を招くことのない、最大限譲歩できる業務中断の最長時間です。各ビジネスプロセスでは、重要な機能の場合は数分から数時間、緊急の機能の場合は24時間、通常の機能の場合は7日など、独自のMTDを設定できます。MTDは企業やイベントによって異なります。各機能は、複数のシステムと資産によってサポートされる場合があります。MTDでは、システム所有者と資産所有者が運用を再開するのに必要な復旧時間の上限を設定します。例えば、医療機器を専門に扱う組織では、かなりの在庫を備えているため、生産資材が3か月間入荷しなくても存在できます。3か月後には資材が不足し、製品を製造できなくなり、破綻する可能性があります。この場合、MTDは3か月になります。

- **目標復旧時間(RTO)**は、災害後に、個別のITシステムがオフラインのままになる時間です。これは、問題があることを特定し、復旧を実行（バックアップからの復旧や、代替システムへの切り替えなど）するまでにかかる時間を表します。
- 業務復旧時間(WRT)。システム復旧に続き、ビジネス機能が再び完全にサポートされるように、さまざまなシステムを再統合し、全体的な機能をテストして、システムユーザーに変更や異なる業務実施方法を伝えるための作業がある可能性があります。



RTO+WRTはMTDを超えてはなりません！

- **回復ポイントの目標(RPO)**は、時間で測定される、システムで許容される損失データ量です。つまり、ウイルスによってデータベースが破壊された場合、RPOが24時間であれば、データベースが感染する以前の24時間まで（バックアップコピーから）データを回復できることを意味します。



任務上必要不可欠な機能を管理する指標。（画像提供：© 123RF.com）

例えば、見込み顧客データベースでは、数時間または数日分のデータの損失に耐えることができる場合があります（通常、営業担当者は誰に連絡したかを覚えていて、データを手動で再入力できます）。逆に、注文処理はより重要であると見なされる場合があります。それは損失により、注文を失ったことになり、ウェブ受注や、会計や注文充足の記録など、コンピュータシステムを通じてのみ開始される処理を取り戻すことが不可能な場合があるためです。

MTDとRPOにより、重要なビジネス機能を判断し、適切なリスク対策を特定できるようになります。例えば、RPOが日数で測定される場合、簡単なテープバックアップシステムで十分です。RPOがゼロの場合や分数や秒数で測定される場合、より高額なサーバークラスター・バックアップと冗長構成が必要になります。

重要なシステムの特定

任務上必要不可欠な機能や主なビジネス機能の復元性をサポートするには、重要なシステムの特定を実行することが不可欠です。これは、ビジネスプロセスとそれをサポートする資産のインベントリを収集することを意味しています。資産の種類には次が含まれます。

- 人（従業員、訪問者、サプライヤー）。
- 有形資産（ビル、家具、機器、機械〔工場〕、ICT機器、電子データファイル、紙面文書）。
- 無形資産（アイデア、商業的評判、ブランドなど）。
- 手順（サプライチェーン、重要な手順、標準業務手順書）。

任務上必要不可欠な機能の場合、コンポーネント間の依存関係の数を減らすことが重要です。依存関係は、ビジネスプロセス分析(BPA)を機能ごとに実行することで特定できます。BPAでは次の要因が特定できるはずです。

- 入力 - 機能を実行する情報のソース（遅延される場合や順序が狂った場合のインパクトを含む）。
- ハードウェア - 処理を実行する特定のサーバーやデータセンター。
- 機能をサポートする従業員とその他のリソース。
- 出力 - 機能によって作成されたデータやリソース。
- プロセスフロー - 機能が実行される方法のステップバイステップの説明。

单一障害点

各ITシステムは、サーバー、ディスクアレイ、スイッチ、ルーターなどのハードウェア資産によってサポートされています。依存関係を減らすとは、システム設計でそうしたデバイスが**单一障害点(SPoF)**になることから生じる種類の弱点を簡単に取り除けることを意味します。SPoFは、それが破損しているか利用できない場合にワークフロー全体が機能しなくなる原因となる資産です。SPoFは、冗長なコンポーネントをプロビジョニングすることにより緩和できます。資産の信頼性の指標により、いつ、どの程度の冗長性が必要なのか判断できます。サービス可用性に関する主なKPIの一部は次のとおりです。

- **平均故障時間(MTTF)**と**平均故障間隔(MTBF)**は、製品の予想寿命を表します。MTTFは、修復不可能な資産に使用されるべきです。例えば、ハードドライブはMTTFで説明できますが、サーバー（ハードドライブを交換することで修復可能）はMTBFで説明できます。ですが多くの場合、MTBFが無差別に使用されています。ほとんどのデバイスでは、故障は寿命の早い段階または遅い段階で発生する可能性が高く、いわゆる「バスタブ曲線」を形成します。

MTTF/MTBFを使用して、システムに必要な資産の冗長性の量を判断できます。障害が発生した場合、冗長システムは別の資産にフェイルオーバーし、引き続き通常通りに運用できます。また、障害が発生する可能性の計算にも使用できます。

- MTBFは、合計の時間を障害の数で割ることで計算されます。例えば、50時間稼働するデバイスが10台あり、そのうちの2台に障害が発生した場合で、修復時間を考慮しない(0時間)とすると、MTBFは $250\text{時間}/\text{障害}(10*50)/2$ になります。
- 同じテストで、故障するまでに2台が25時間稼働した場合のMTTFの計算は、合計稼働時間をデバイスの数で割ったものであるため、 $(8*50+2*25)/10$ となり、結果は45時間になります。

- **平均復旧時間(MTTR)**は、システムが完全に動作するように復元するために、災害の修正にかかる時間の尺度です。またこれは、「交換」や「回復」までの平均時間として説明できます。この指標は、全体の目標復旧時間(RTO)を判断する上で重要になります。



NISTは、耐性とIT緊急時対応計画のガイド(SP800-34)を公開しており、nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdfで入手できます。

災害

事業継続の観点から言えば、災害は任務上必要不可欠な機能への脅威となり得るイベントです。例えば、プライバシーの侵害は深刻なインシデントですが、ビジネス機能への直接の脅威ではない可能性があります。データセンターを破壊する地震は、災害レベルのイベントになります。災害対応には、インシデント対応と同じ原則と手順の多くが関わりますが、より大規模になります。

内部と外部

内部の災害は、悪意のあるアクティビティまたは従業員や請負業者（会社や組織内で存在が認められている人やもの）によって偶然に発生するものです。また内部の災害には、火災を引き起こす配線などのシステムの欠陥も含まれます。一方、外部の災害イベントは、アクセス権限のない脅威アクターによって引き起こされます。外部の災害には、公共サービスの中止やサプライチェーンへの影響など、より広範な環境的影響や社会的影響を通じて、組織に影響を及ぼす災害が含まれます。

人為的

人為的な災害イベントは主な原因が人によるものであるイベントです。破壊的なサイバーセキュリティインシデント以外の一般的な例には、テロ、戦争、公共物破壊、環境汚染、放火が含まれます。また、電源や通信のケーブルを切断するなどの偶発的な人為的災害もあります。

環境的

環境的災害または自然災害は、人の力では防ぐことのできない災害です。環境的災害には、河川や海の氾濫、地震、暴風雨、病気などが含まれます。自然災害は、予測できる場合（洪水や暴風雨の被害を受けやすい地域の場合など）と、予測できない場合があるため、計画が難しい可能性があります。



ほとんどの自然災害と環境的災害は、人的または人工的なことに起因している可能性があります。例えば、ダムが適切に管理されていないために氾濫が起こったり、山火事は、放火や電力インフラの整備不良が原因である可能性があります。

サイトのリスク評価

サイバーセキュリティは一般的に経済的な影響を及ぼしますが、サイトの安全性は生命や資産に影響を及ぼす可能性があります。サイトのリスク評価では、次の種類の要因への露呈を評価します。

- 地震や洪水、火災などの災害イベントによるリスク。こうしたイベントは、自然に発生するか、人為的原因がある可能性があります。
- 電気、水道、交通など公共サービスの中止によるリスク。こうしたリスクは、地理的に孤立したサイトで高くなります。
- オンプレミスの電気機械システムや化学薬品による健康と安全へのリスク。

災害復旧計画

災害復旧計画(DRP)には、災害レベルのイベントの後に、システムやサイトを稼働できる状態に回復するために従う特定の手順を記述します。DRPでは次を達成するべきです。

1. 自然災害と人為的災害のシナリオ、システム保護措置を特定する。計画では、リスク（災害が発生する可能性と組織への影響の可能性の組み合わせ）とコストを考慮する必要があります。

組織が経済的に活動不能になる災害復旧計画を実装する意味はありません。ビジネスケースは、回復対策のコストとダウンタイムのコストを比較して作成します。一般的に回復計画は、ダウンタイムのコストを超えないようにすべきです。

2. 災害への対応に必要なタスク、リソース、責任の所在を特定する。
 - 行動に対する責任者は？連絡方法は？対応できない場合は？
 - 一番重要な機能は？最初に尽力すべき箇所は？
 - 利用可能なリソースは？事前に購入して、在庫を持つべきか？災害により、供給の可用性に影響するか？
 - 通常稼働の再開へのタイムスケールは？
3. 災害対策手順と状況の変化に対応する心構えについて担当者をトレーニングする。

災害復旧計画では、システムの回復だけでなく、生命と安全に影響を及ぼすインシデントについて通知する必要があるステークホルダーを特定する必要があります。安全に関連するインシデント、または刑事事件について警察、消防署、または建物の検査官に通知する法的要件があります。サードパーティのデータや個人データが紛失または盗難される場合、データの対象者に通知する必要がある可能性があります。災害によりサービスに影響がある場合、修復までの時間と実施できる代替手段の手配について顧客に知らせる必要があります。

機能復旧計画

災害は極端で（願わくば）まれなイベントであるため、回復計画がどれほど効果的または機能的であるかを評価することは非常に困難です。回復計画の機能性を評価する方法は主に4つあります。

- ウォークスルー、ワークショップ、オリエンテーションセミナー - 災害復旧チームメンバーに基本的な認識とトレーニングを提供するためによく使用されます。これらの演習では、DRPやその他の計画の内容と計画で概説されている役割と責任について説明します。
- 机上演習 - スタッフは、実際に災害の状態を作り出したり、何かを適用または変更したことなく、災害発生時と同じ手順を「代行」します。これらは簡単にセットアップできますが、上手くいかない可能性があることや完了するまでにかかる時間などの実用的な証拠は提供しません。
- 機能演習 - シミュレーション環境でシナリオベースのアクティビティを実行することで、従業員がDRPを検証できるアクションベースのセッションです。
- フルスケール演習 - 実際の状況を反映したアクションベースのセッションです。こうした演習はオンラインで行われ、可能な限り実際の機器と実際の人材を使用します。多くの場合、フルスケール演習は公共機関によって行われますが、地元の組織の参加が求められる可能性があります。

レビューアク ティビティ： ビジネスインパクト分析の概念

次の質問にお答えください。

1. システムの復元力（レジリエンス）を低下させる可能性が最も高い要因は何ですか？
2. 次の記述は正しいですか、誤りですか？RTOは、単一のシステムまたは資産内の問題を特定して解決するために必要な時間を表します。
3. MTBFで測定されるのは何ですか？
4. 机上演習とは何ですか？
5. 災害復旧計画を作成する上で、演習が重要な部分であるのはなぜですか？

レッスン19

概要

リスク管理、ビジネスインパクト分析、災害復旧計画のプロセスと指標について説明できる必要があります。

リスク管理のガイドライン

リスク管理評価を支援する場合は、次のガイドラインに従います。

- MTTF/MTBFやMTTRなどの指標を使用して、ワークフローを分析し、任務上必要不可欠な機能(MEF)と主なビジネス機能(PBF)やそれらをサポートする資産を判断します。
- 内部と外部、環境的、人為的、サイト固有のリスク評価、マルチパーティ、ソフトウェアライセンス/コンプライアンス、知的財産(IP)の盗難、レガシーシステムを考慮し、脅威と災害発生のシナリオを特定します。
- MEFIに優先順位を付け、ビジネスインパクト分析を実行して、SLE、ARO、ALEなどの指標を使用して、さまざまな脅威と災害シナリオに固有のリスクの可能性と影響を判断します。
- 機能や重要なシステムごとにMTD、RTO、RPOを定義し、これらの目標を達成するリスク緩和手法（抑止、回避、移転、または受容）を適用します。
- リスク要因と対策を、ステークホルダーが理解しやすいようにヒートマップを使用してリスク登録に要約します。
- 現行のリスク監視を実行し、残留リスクと制御リスクを判断します。
- 機能的なDRPを確立し、テストして、災害レベルのイベントに効果的に対応できるようにします。

レッスン20

サイバーセキュリティレジリエンスを実装する

レッスン概要

サイバーセキュリティレジリエンスとは、脅威アクターが侵入に成功しても、機密性、完全性、可用性への影響が限定的になることを意味します。ストレージ、電源、ネットワークシステムにおける冗長性の実現、効果的なバックアップ手順、サイトの復元、変更制御と構成管理における有効な手順は、可用性を高く保つうえで必要不可欠になります。

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。

- 冗長性戦略を実装する。
- バックアップ戦略を実装する。
- サイバーセキュリティレジリエンス戦略を実装する。

トピック20A

冗長性戦略を実装する



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

リスク評価とビジネスインパクト分析の出力により、価値のあるビジネスプロセスが特定されます。こうしたプロセスでリスクを低減するには、ITシステムやそれらをサポートするビジネスシステムの障害に対する耐性を高めて対応します。冗長性のある電源、ネットワーク、ストレージシステムになるようにシステムを設置し、構成できるようにする必要があります。

高可用性

耐性のあるシステムの主な特性の1つは**高可用性**です。可用性とは、システムがオンラインになっている時間の割合で、指定した期間（通常は1年間）で測定されます。可用性に直接関連するのはダウンタイムで、これはシステムが利用できない時間です。最大許容停止時間(MTD)指標では、特定のビジネス機能の可用性の要件を示しています。高可用性は通常、24x7（1日24時間、1週間に7日間）、または24x365（1日24時間、1年間365日）と大まかに説明されます。重要なシステムの場合、可用性は99%や、最大99.9999%として説明されます。

可用性	年間ダウンタイム(hh:mm:ss)
99.9999%	00:00:32
99.999%	00:05:15
99.99%	00:52:34
99.9%	08:45:36
99%	87:36:00

ダウンタイムは、予定に沿ったメンテナンス時間と、期間中の計画外の停止の合計です。

システムの可用性とはプロセス全体を指しますが、サーバーや個別のコンポーネントのレベルの可用性も指します。

スケーラビリティ（拡張性）とエラスティシティ（弾力性）

高可用性とは、システムが必要の急速な増加に対応できることでもあります。こうした特性は、スケーラビリティとエラスティシティと呼ばれます。スケーラビリティとは、同様の費用比率内で需要を満たすためにリソースを増やす機能を指します。これは、サービスの需要が2倍になんて、コストは2倍より多くならないことを意味しています。スケーラビリティには2種類があります。

- スケールアウトは、既存のリソースに並行してリソースを追加することです。
- スケールアップは、既存のリソースのパワーを増やすことです。

エラスティシティは、リアルタイムかつオンデマンドで変更を処理するシステムの能力を指します。高いエラスティシティを有するシステムでは、需要が急増しても、サービスやパフォーマンスの喪失が生じません。

フォールトトレランスと冗長性

障害が発生しても同じ（またはほぼ同じ）レベルのサービスを提供し続けることができるシステムは、**フォールトトレランス**であるとされます。多くの場合、フォールトトレランスは、重要なコンポーネントと単一障害点に**冗長性**を持たせることで達成できます。冗長コンポーネントは、システムの通常の機能にとって不可欠ではありませんが、システムで別のコンポーネントの障害から回復できるようにするものです。

冗長電源

すべての種類のコンピューターシステムでは、作動するために安定した電源が必要になります。電圧スパイクやサージなどの電気的事象はコンピューターやネットワークアプライアンスのクラッシュの原因となり、**ブラウンアウト**や停電による電源喪失は機器の機能停止につながります。電源管理とは、機器をこういったトラブルから保護するための対策が講じられており、システムとネットワークが中断なく稼働し続けるか、迅速に回復できる状態を意味します。

デュアル電源

エンタープライズクラスのサーバーやアプライアンスエンクロージャでは、冗長性のために2つ以上の電源ユニット(PSU)を搭載している可能性があります。ホットプラグ対応PSUは、（障害発生時に）システムの電源を落とさずに交換できます。

管理された配電ユニット(PDU)

ラック、ネットワーククローゼット、またはサーバールームに系統電力を供給する電力回路は、設置されたすべての機器の負荷容量に加えて、拡張の余地を十分に満たす必要があります。したがって、サーバールームへの回路は通常、家庭用またはオフィス用の回路よりも容量が大きくなります（13アンペアではなく、30または60アンペアなど）。こうした回路は、**配電ユニット(PDU)**を経由する場合もあります。これらには、電力信号を「クリーン」にする回路が付いており、スパイク、サージ、ブラウンアウトに対する保護を提供し、無停電電源装置(UPS)と統合できます。管理されたPDUでは、負荷とステータスの報告、ソケットへの電源のオンとオフ、またそれを特定の順序で実行するなどのリモート電源モニタリング機能をサポートしています。

バッテリーバックアップと無停電電源装置(UPS)

バッテリーバックアップを使用すれば、電力が失われた場合でも、その容量に応じて数分から数時間システムを稼働させることができます。バッテリーバックアップは、ディスクドライブやRAIDアレイなど、コンポーネントレベルでのプロビジョニングが可能で、電力損失時にキャッシュされた読み取り/書き込み処理を保護できます。システムレベルでは、停電（完全に電源を喪失した状態）時には**無停電電源装置(UPS)**が稼働し、一定時間給電を行います。デスクトップPCであれば数分、エンタープライズシステムであれば数時間とさまざまです。最もシンプルなUPSは、バッテリー式と充電回路、バッテリーから供給されたDC電圧からAC電圧を生成するインバーターで構成されます。

UPSによって許可される時間は、予備発電機などの代替電源にフェールオーバーするのに十分な時間である必要があります。代替電源がない場合でも、少なくともUPSが稼働している間に管理者はサーバーやアプライアンスを安全にシャットダウンし、ユーザーはファイルをセーブし、OSは適切なシャットダウンドルーチンを実施することができます。

発電機

バックアップ発電機では、多くの場合数日間建物全体に電源を供給できます。ほとんどの発電機では燃料にディーゼル、プロパンまたは天然ガスを使用します。ディーゼルとプロパンの場合、主な欠点は安全な保管になります（またディーゼルの保存期間は18か月～2年になります）。天然ガスの場合は、自然災害が発生する場合の、ガスの供給の信頼性が問題になります。またデータセンターでは、太陽熱や風力、地熱、水素燃料電池、水力などの再生可能なエネルギー源に投資しています。再生可能なエネルギーを使用できることは、新しいデータセンターに最適なサイトを判断するうえで重要な要因になります。TeslaのPowerpack (tesla.com/powerpack)などの大規模バッテリーソリューションは、バックアップ発電機に代わるもの提供できる可能性があります。データセンターのすべてのバッテリー資源を、電力貯蔵用のマイクログリッドとして使用する新技术もあります([scientificamerican.com/article/how-big-batteries-at-data-centers-could-replace-power-plants/](https://www.scientificamerican.com/article/how-big-batteries-at-data-centers-could-replace-power-plants/))。

 UPSは、コンピューターサービスの中止から保護するために常に必要になります。バックアップ発電機は電源障害に対応できるだけの速さでオンラインにすることはできません。

ネットワークの冗長性

ネットワークもまた、単一障害点となってサービスに重大な支障をきたす可能性のある重要なりソースです。

ネットワークインターフェイスカード(NIC)チーミング

ネットワークインターフェイスカード(NIC)チーミングまたはアダプターチーミングとは、サーバーに複数のNICまたは複数のポートを使用したNIC、もしくはその両方が導入されていることを意味します。各ポートは、個別のネットワークケーブルに接続されています。通常の操作では、これにより高帯域幅のリンクが提供できます。例えば、4つの1GBポートでは、全体で4GBの帯域幅を提供します。1つのケーブル、または1つのNICに問題が発生した場合でも、3GBにはなりますが、ネットワーク接続は引き続き機能します。

 システムがパールトレントであるためには、高い帯域幅が機能にとって重要であってはなりません。

スイッチングとルーティング

ネットワークのケーブリングは、ネットワークの一部に障害が発生した場合でも、他の部分の動作が維持されるよう、さまざまなスイッチやルーター間でマルチパス対応しておく必要があります。

 複数のスイッチングパスでは、STP (スパニングツリープロトコル) を使用して、ループを防ぐ必要があります。

ロードバランサー

NICチーミングでは、アダプターレベルでロードバランシングを実現します。ロードバランシングとクラスタリングはサービスレベルでも実現できます。

- ロードバランシングのスイッチでは、利用可能なサーバー間でワークロードを分散します。
- ロードバランシングのクラスターでは、複数の冗長サーバーでデータとセッションの情報を共有し、1つのサーバーから別のサーバーへのフェイルオーバーがあっても一貫したサービスを維持できます。