記事

データが本当に復旧可能であることを証明するために、リーダーが答えるべき12の質問

ランサムウェア、内部脅威、運用上の障害は、もはや稀な事象ではなく、絶え間なく発生しています。それにもかかわらず、最も必要とされるときにデータの復旧が可能と言い切れる組織は少ないのが現状です。

こうした乖離が生じている理由は単純で、バックアップとスナップショットは入力データであり、復旧可能性は成果であるからです。

継続的なデータ保護、定期的なバックアップ、スナップショット、セキュリティ管理は必要ですが、それだけで、実際にプレッシャーがかかった状況でも迅速かつ正常に、そして適切な順序でシステムが復旧されることが保証されるわけではありません。多くの組織は、実際にインシデントが発生し、復旧を試みる際に初めてその不備に気づきますが、その時にはすでに手遅れになっています。

復旧可能性こそが、真のレジリエンスの尺度です。またこれは、攻撃や障害、人為的ミスによって問題が顕在化する前に、リーダーが厳格に検証できる (検証すべき) ものです。

以下の簡単な経営幹部向けチェックリストは、ツールやアーキテクチャーに関するものを除いた質問をまとめたものです。セキュリティの不備を早期に、まだ解決する方法があるうちに発見できるように構成されています。これらの質問に明確に回答できれば、今日の脅威やハイブリッドの実態に即した、復旧を優先する戦略の策定が可能になります。

「復旧可能」の厳密な定義

質問に入る前に、基準を明確にしておきます。

復旧可能とは、次の状態に復旧できることを意味します。

— ビジネスニーズに応じた**クリーンな復旧ポイント** (RPO)
— **ビジネスを存続させるのに十分な時間内** (RTO) (データだけでなく、優先サービスも対象)
— 適切な隔離および検証済みで、**すぐに再感染しない環境**

いずれか1つでも満たしていないと、レジリエンスは実効的な統制ではなく、単なる建前になってしまいます。

このチェックリストの使い方

初日から完璧な答えを出す必要はありません。目標は、まだ対応策があるうちに、問題点を早期に発見することです。

以下の質問を簡単な自己評価に活用してください。

— **緑色:** 文書化、テスト、および測定済み

— **黄色:** 部分的に実装済みまたは未検証

— **赤色:** 推定、不明、または「そう思われる」

赤色の回答には特に注意してください。そこが復旧時間やリスクにつながりやすい領域です。

保護の頻度 (復旧可能性の始点)

復旧の確実性は、自社が実際にどれだけのデータ損失を許容できるか、そして自社のデータ保護体制がその現実に対応できているかどうかを把握することから始まります。

1. **Tier-0およびTier-1サービスに求められるRPO (復旧ポイント目標) はどれくらいですか。それは理論上ではなく、実際に達成可能ですか。**
   RPOを暗唱できるチームは多くても、そのRPOを現行の保護モデルで、そして重圧下でも達成できることを検証したチームは少ないのが現状です。

2. **復旧ポイントは、影響を受ける数秒前のデータに復元できるほど細かく設定されているでしょうか。それとも、最後にスケジュールされたバックアップに復元されるのでしょうか。**
   攻撃やデータ破損が徐々に展開された場合、粗い復旧ポイントでは、許容できないデータ損失が発生する可能性があります。

3. **オンプレミス、クラウド、SaaSなどのさまざまなプラットフォームに一貫した復旧ポイント頻度を設定していますか。また、頻度が不足していると、リカバリ戦略にどのような影響があるでしょうか。**
   一貫性の欠如は、ハイブリッド環境ではよくある死角の1つです。ポリシーが異なるところに、保護のギャップが生じることがよくあります。

危険信号:

「Tier-0のRPOは把握していません」

「すべてのデータに、1つの標準的なバックアップポリシーを適用しています」

「クラウドワークロードは、別の方法で (しかも一貫性のない方法で) 処理されています」

不変性と隔離 (ランサムウェア時代に必須)

不変性は復旧用コピーの削除や暗号化を防ぐのに役立ちますが、それだけでは十分ではありません。隔離と運用規律によって、不変コピーが実際の攻撃に耐えられるかどうかが決まります。ほとんどの環境では、その両方が必要となります。

4. **少なくとも1つの復旧用コピー (不変であり、かつ本番環境のIDおよびネットワークから隔離されているもの) を保持していますか。**
   攻撃者が本番環境にアクセスするのと同じ経路で復旧データにアクセスできる場合、不変性だけでは十分ではない可能性があります。

5. **不変性は設計段階から適用されていますか。それとも、管理者IDが侵害されると保持や削除の保護が変更される可能性がありますか。**
   多くのインシデントの根本原因は、マルウェアではなく、認証情報にあります。復旧管理では、こうした現状を考慮する必要があります。

6. **攻撃者が最初にリカバリデータを標的にした場合、攻撃者がこちらのリカバリパスを発見、暗号化、妨害することを防ぐものとして、どのようなものがありますか。**
   この質問では往々にして、「隠すことがセキュリティ」という前提が今日の脅威戦術には通用しないことが露呈します。

> **有益な考え方**
>
> 攻撃者はこちらの環境を把握しないという前提で復旧を設計しているなら、それは既に時代遅れです。

テストの規律 (復旧は、テストによって有効になる)

未検証の復旧計画は、気づかないうちに失敗するのではなく、組織が最も重圧を受ける状況下で失敗します。

7. **現実的な規模でTier-0アプリケーションの復旧テストを最後に実施したのはいつですか。また、復旧にかかる時間を測定しましたか。**
   小規模かつ部分的なテストでは、実際の復旧シナリオの複雑さが反映されません。

8. **バックアップの完全性と復元用資産を、必要になる前に定期的に検証していますか。**
   インシデント発生時にバックアップデータの破損が発覚すると、技術的な問題がビジネス上の危機へと発展します。

9. **本番環境に再接続する前に、フォレンジック検証のために隔離された環境に復元することは可能ですか。**
   復元は、迅速に行うことはもちろん、正常に行う必要があります。

> **厳しい現実**
>
> リハーサルを行っていない復旧は、即興劇となります。

ID管理と復元の優先順位 (復旧時間を決める要素)

復旧時間は、ストレージやインフラストラクチャだけで決まるわけではありません。多くの場合、IDシステム、アクセス制御、不明確な優先順位などの影響を受けます。

10. **データ保護および復旧管理は、多要素認証、最小権限、役割の分離によって保護されていますか。また、ADやIAMが侵害された場合でも、耐障害性のある管理体制になっていますか。**
    IDシステムが停止すると、復旧権限も失われてしまうことが少なくありません。

11. **Tier-0サービスの復元手順書は作成済みですか。また、その手順書はテスト済みですか。**
    ID、ネットワーク、DNS、コアプラットフォーム、データが、デフォルトで同時にオンラインに戻るわけではありません。順番は重要です。

12. **不変コピーから最も重要なアプリケーションをどれだけ迅速に復元できますか。また、データ取得時間だけでなく、サービス提供までの時間を遅らせる依存関係は何ですか。**
    経営幹部は障害を、ファイルの消失ではなく、機能の喪失と捉えています。復旧計画は、そうした現状を反映したものでなければなりません。

チェックリストから行動へ

この評価は、自己採点を目的としたものではありません。重要なのは、リスクを最も早く軽減できるところに注力することです。

具体的な次のステップ:

— **上位3つの赤色の回答**を特定し、それぞれに明確な担当者を割り当てます。

— **復旧テストの定期的なサイクル**を確立し、約束ではなく、成果を公表します。

— 攻撃者がこちらの環境を把握していることを前提として、**敵対的な状況下**での復旧策を設計します。

復旧可能性は、新たなツールを購入したり、新たなチェックボックスにチェックを入れたりすることで証明できるものではありません。重要なデータを既知のクリーンな状態に、かつ測定されたサービス開始目標時間内に、繰り返し復元できることで証明されます。

詳細はこちら

HPE.com/data

HPE.comにアクセス

今すぐチャット

a00155955JPN

HEWLETT PACKARD ENTERPRISE

hpe.com