移動中のデータセキュリティの確保できていますか？

ITおよびセキュリティの意思決定者を対象としたグローバル調査では、ネットワーク上の移動中データのセキュリティに関する深刻な懸念とその対応策が明らかになりました。

5つの主な調査結果

あなたの組織ではどうですか？

01 ネットワーク上の移動中データを暗号化しない危険性に対する認識が不十分

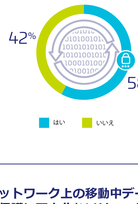
注目すべき点：

- **42%**の回答者が、移動中データを暗号化していない、または暗号化しているかどうかわからないと答えています。
- そのうち、32%が閉域ネットワークまたはプライベートネットワークを使用していると回答し、29%が暗号化は必要ないと回答しています。

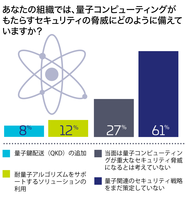
その意味：

- 移動中データに対するサイバーセキュリティの脅威の程度を十分に理解していない可能性があります。
- ソリューションプロバイダー組織は、クライアントよりもクライアントのリスクを認識しています。サービスプロバイダーの93%が、ネットワークデータを暗号化する必要があると考えているのに対し、顧客は29%にとどまっています。

あなたの組織では、データネットワーク上の移動中データを暗号化していますか？



ネットワーク上の移動中データの保護に不十分なソリューションが多用されている



02 ネットワーク上の移動中データの保護に不十分なソリューションが多用されている

注目すべき点：

- **69%**が、移動中データの暗号化にファイアウォールを使用していると答えています。
- ネットワーク上の移動中データを保護するために、専用のハードウェア暗号化アプライアンスを使用している企業はわずか23%です。

その意味：

- 専用の暗号化アプライアンスのパフォーマンスとセキュリティ上の利点（デュアル機能デバイスのペナルティとの比較）に対する認識が不足しています。
- 多くの企業がIPSecを使用していますが、これは時代遅れのプロトコルで、低オーバーヘッド、低遅延を必要とする高帯域幅ネットワーク向けに設計されていません。

03 頻繁なパッチ適用とデバイス交換を避けるには、専用の暗号化ソリューションがより良い選択肢である

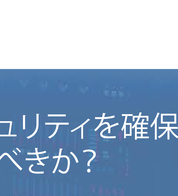
注目すべき点：

- **70%**の回答企業が、セキュリティの更新を確実にするために、現在も頻繁にソフトウェアパッチを適用しています。
- **47%**の回答者が、自社のソリューションではセキュリティ要件の変化に対応するために、定期的なデバイスのアップグレードが必要であると答えています。

その意味：

- 専用の暗号化ソリューションを使用することで、組織はコンプライアンスを確保し、コストと時間のかかるパッチ適用やアップデートの必要性を減らすことができます。

あなたの組織では、進化する標準やサイバー脅威によって必要となる暗号化プロセスの変更に、どのように対応していますか？



あなたの組織では、量子コンピューティングがもたらすセキュリティの脅威にどのように備えていますか？

04 量子コンピューティングのサイバー脅威とクリプトアジリティ（暗号の俊敏性）の重要性

注目すべき点：

- **73%**が、量子は脅威であると認識しているにもかかわらず、61%がポスト量子世界に対する戦略をまだ策定していません。

その意味：

- 意思決定者は、現在暗号化によって保護されているデータが、量子コンピューティングが現実のものとなっても確実に保護されるようにするためのソリューションを検討し始めています。暗号化戦略には、ポスト量子暗号に対応したクリプトアジャイルなソリューションを組み込むべきです。

05 移動中データに最大限のセキュリティを適用するために重要な「用意すべきもの」

注目すべき点：

- 大半の回答者が、セキュリティ面をネットワーク機能から分離することに価値があると考えています。
  86%が、ネットワーク暗号化ソリューションを採用する際、暗号鍵マテリアルの品質に関する問題が重要または非常に重要であると考えています。

その意味：

- 意思決定者は、移動中データの効果的なセキュリティには、機能の分離と暗号鍵のセキュリティ確保の両方が必要であると認識しています。

セキュリティ製品（バンドルされたデュアル機能デバイスではない）を評価する際、ネットワーク暗号化ソリューションの機能の分離はどの程度重要ですか？

暗号鍵マテリアルの品質に関する問題はどの程度重要ですか？

移動中データのセキュリティを確保するためには何をすべきか？

セキュリティ、IT、ネットワーキングの各チームが協力して、最新のネットワークアーキテクチャにおけるパフォーマンス、セキュリティ、予算の要件を満たす最適なソリューションを提供する必要があります。DevSecOpsのベストプラクティスに集中することから始めましょう。

専用の暗号化
最大限のセキュリティとネットワークパフォーマンスを実現

独立性
ネットワークレイヤに依存しないポリシーベースのデータ保護

データとネットワークの保護
エンドツーエンドの認証付き暗号化

セキュアな暗号鍵
暗号鍵のセキュアな管理と保管

一元化されたシステム
シンプルで信頼性の高い導入と管理

クリプトアジリティ
デザインインのクリプトアジャイルなプラットフォーム

タレス高速ネットワーク暗号化ソリューションについて詳しく見る

レポート全文を読む：移動中データにおけるセキュリティの弱点（英語版）

各種フォロー：

THALES
Building a future we can all trust

> cpl.thalesgroup.com/ja <

お問い合わせ：すべてのオフィスの所在地と連絡先情報につきましては、cpl.thalesgroup.com/ja/encryption/contact-usをご覧ください。