DELL Technologies

ソリューション概要

# PowerProtect Cyber Recovery for Sheltered Harbor

重要な顧客データを保護し、米国の金融市場に対する消費者の信頼を維持する

## Sheltered Harbor の概要

2015 年に金融業界によって策定された Sheltered Harbor 標準には、米国の金融データを保護することを目的とした、サイバー レジリエンスおよびデータ保護に関する一連のベスト プラクティスと安全対策が盛り込まれています。本番環境やバックアップ システムを標的としたランサムウェア、データ破壊、窃盗などのサイバー脅威によって、消費者や企業の金融データが危険にさらされています。

米国の銀行、信用組合、証券会社に対するサイバー攻撃が成功すると、その金融機関の評判が落ち、米国の金融システムに対する消費者の信頼を損ない、世界的な金融危機を引き起こす可能性があります。

Sheltered Harbor は、重要な顧客口座記録やその他のデータを変更せずにデジタル ヴォールト内に分離することで、米国金融業界の安定性と金融機関のサイバー レジリエンスを強化します。金融機関のプライマリー システムまたはバックアップ システムがランサムウェアなどのサイバー攻撃やその他の事象によって侵害された場合でも、重要なデータを迅速にリカバリーできるため、顧客向けの重要な銀行業務の継続性を高め、世間からの信頼を維持することができます。

## Cyber Recovery の特長

デル・テクノロジーズは、Sheltered Harbor アライアンス パートナー プログラムに参加した初のソリューション プロバイダーであり、米国の金融機関向けに Sheltered Harbor 準拠のターンキー型データ保管ソリューションを開発してきました。

PowerProtect Cyber Recovery for Sheltered Harbor は、Sheltered Harbor によって承認された初のオンプレミス ターンキー型データ保管ソリューションです。このソリューションは、Sheltered Harbor 標準を実装する参加機関に対する製品の技術要件をすべて満たしています。

**データ ヴォールト**：参加機関またはサービス プロバイダーにより、重要なデータのバックアップが Sheltered Harbor 標準のフォーマットで毎晩作成されます。データ ヴォールトは暗号化され、変更することができません。また、金融機関のインフラストラクチャ（バックアップ、ディザスター リカバリー、その他のデータ保護システムなど）から分離されます。

**分離とガバナンス**：企業ネットワークから切り離された安全な分離環境により、適切な許可を受けていないユーザーが制限されます。また、データ コピーとエア ギャップの自動管理により、データの整合性、可用性、安全性、機密性が確実に維持されます。

**リカバリーと修復**：Sheltered Harbor のレジリエンス プランが開始されると、参加機関はデータをヴォールトから迅速にリカバリーし、銀行業務を最速で復旧して再開することができます。

### 課題：金融サービス業界に対するサイバー攻撃は世界的な金融危機を引き起こす可能性がある

あらゆる組織が、悪意のあるサイバー攻撃によりビジネスに及ぼされる深刻な影響を憂慮しています。それでも、97%の組織がデジタル トランスフォーメーションに向けた取り組みの中で機密データを使おうとしています [1]。データの価値を引き出すことに大きなメリットがあるからです。

しかし、機密データが悪用、破壊、公開されると、重大なリスクも生じます。マルウェアとランサムウェアは進化を続けており、攻撃は増加傾向にあります。Symantec の 2019 年インターネット セキュリティ脅威レポートによると、企業を対象としたランサムウェア攻撃は 2019 年に 12%増加し、全ランサムウェア感染の 81%を占めています [2]。また、Ponemon Institute の最新レポートによると、2020 年の全データ侵害の 52%が悪意のある攻撃によって発生したものであり、わずか 5 年で 30%増加しています [3]。

さらに、攻撃者の戦術やツールも進化しています。これらの検出はほぼ不可能になっており、攻撃の防止もますます困難になっています。サイバー犯罪の戦術も進化を続けています。Verizon の『2020 年度データ漏洩/侵害調査報告書』によると、内部関係者が関わっているサイバー攻撃はわずか 3 年で 25%から 30%に増加しています [4]。

Accenture の『2019 年サイバー犯罪コスト調査レポート』によると、米国金融業界のサイバー犯罪による損害額は過去 3 年間で最多となっています [5]。こうした状況が重なって最悪の脅威が生じており、全世界の金融市場が対処を余儀なくされています。

Sheltered Harbor は 2015 年に業界主導の非営利イニシアティブとして設立され、米国の金融機関が顧客データの侵害や通常の銀行業務の中断を引き起こすサイバー攻撃のリスクを低減できるよう支援しています。Sheltered Harbor のエコシステムは、参加機関（米国の銀行、信用組合、証券会社、資産管理者）、全米の事業者団体、ソリューション プロバイダー、サービス プロバイダーで構成されており、金融セクターの安定性とサイバー レジリエンスの強化に取り組んでいます。

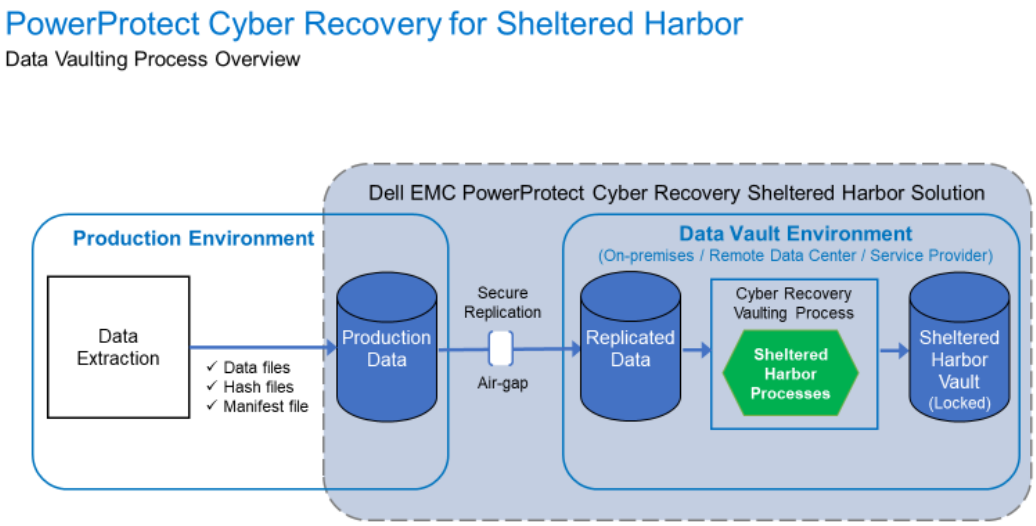
従来のディザスター リカバリーとビジネス継続性は、自然災害や人為的災害の発生後に業務機能を完全に復旧させるために必要なものです。一方、Sheltered Harbor は、標的型の高度なサイバー攻撃を受けた後に、すべてのリカバリー手順を継続しつつ、基本的な銀行業務を再開するために必要なデータを、整合性を維持しながら直ちに使用できるようにすることを目的としています。


文書番号：H18199

## Dell EMC PowerProtect Cyber Recovery for Sheltered Harbor：金融機関の最も重要なデータを保護するための堅牢なサイバー レジリエンス

デル・テクノロジーズは、Sheltered Harbor アライアンス パートナー プログラムに参加した初のソリューション プロバイダーです。Sheltered Harbor の承認を受けた当社のソリューションは、Dell PowerProtect Cyber Recovery をベースとしています。これは、組織の最も重要なデータをランサムウェアなどのサイバー攻撃から保護するソリューションであり、ほぼ 5 年にわたって市場をリードしてきました。

Sheltered Harbor 仕様に準拠するために、Cyber Recovery のヴォールト アーキテクチャが拡張され、アーカイブの生成と安全なリポジトリーのプロセスを実行できるようになっています。抽出された Sheltered Harbor データは本番環境に保存され、その後、論理的にエア ギャップで隔離された専用の接続を介してヴォールト環境に安全に複製されます。保存ロックなどのその他の手順はヴォールト環境で実行されます。




企業ネットワークとバックアップ システムから物理的に分離された専用の環境を構築することで、Sheltered Harbor の参加組織が保護する必要がある重要なデータ セットを標準化されたフォーマットで保存できます。これにより、顧客向けの基本的な銀行業務を迅速に再開できます。導入の評価は数か月もかからず数週間で完了し、また Sheltered Harbor 仕様を確実に満たすことができます。

## 要約

Dell EMC PowerProtect Cyber Recovery for Sheltered Harbor は、迅速でコスト パフォーマンスと効率性に優れ、完全に承認されたソリューションを参加機関に提供します。各機関が Sheltered Harbor 仕様を満たすために、ワンオフのヴォールトを独自に構築する必要はありません。銀行、信用組合、証券会社は、Sheltered Harbor 標準を実装する場合、完全に承認およびサポートされた、デル・テクノロジーズのターンキー型データ保管ソリューションを使用できます。

Sheltered Harbor の参加組織は、PowerProtect Cyber Recovery for Sheltered Harbor を選択することで、ヴォールトベースの成熟したテクノロジーを利用するメリットが得られ、緊急の導入ニーズにも安心して対応できるだけでなく、将来のデータ保管要件に対応するための足掛かりを築くことができます。参加機関は存続のための道筋を確保でき、米国の金融システムに対する世間からの信頼を維持することができます。

出典：

1. 『2019 Thales Data Threat Report』：www.thalessecurity.com/DTR
2. 『2019 Symantec Internet Security Threat Report』：https://www.symantec.com/security-center/threat-report
3. Ponemon Institute, LLC、『2020 年情報漏えい時に発生するコストに関する調査』：https://www.ibm.com/jp-ja/security/data-breach
4. Verizon、『2020 年度データ漏洩/侵害調査報告書』：https://enterprise.verizon.com/ja-jp/resources/reports/dbir/
5. Accenture、『2019 年サイバー犯罪コスト調査レポート』：https://www.accenture.com/jp-ja/insights/security/cost-cybercrime-study