ENTRUST
SECURING A WORLD IN MOTION

TOP 5 REASONS

NSHIELD HSMをAZUREに使用する5つの理由

1 Azure内のデータは、ユーザの責任

責任共有モデルが示すように、クラウドサービスの提供方法にかかわらず、データは常にユーザ（企業）の責任です。

	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)
ユーザの責任	データ	データ	データ
	アプリケーション	アプリケーション	アプリケーション
	ランタイム	ランタイム	ランタイム
	ミドルウェア	ミドルウェア	ミドルウェア
	O/S	O/S	O/S
プロバイダーの責任	仮想化	仮想化	仮想化
	サーバ	サーバ	サーバ
	ストレージ	ストレージ	ストレージ
	ネットワーキング	ネットワーキング	ネットワーキング

出典：https://gallery.technet.microsoft.com/Shared-Responsibilities-81d091

2 増え続けるデータ漏洩

個人を特定できる情報（PII）を含む顧客情報の漏洩の報告数は、2018年に1億9,760万件から4億4,650万件へと大幅に増加し、これは、126%の増加率を意味します。報告された漏洩のうち、件数を公表しているものが半分にとどまっていることを踏まえると、実際の漏洩件数はさらに多いものと考えられます。

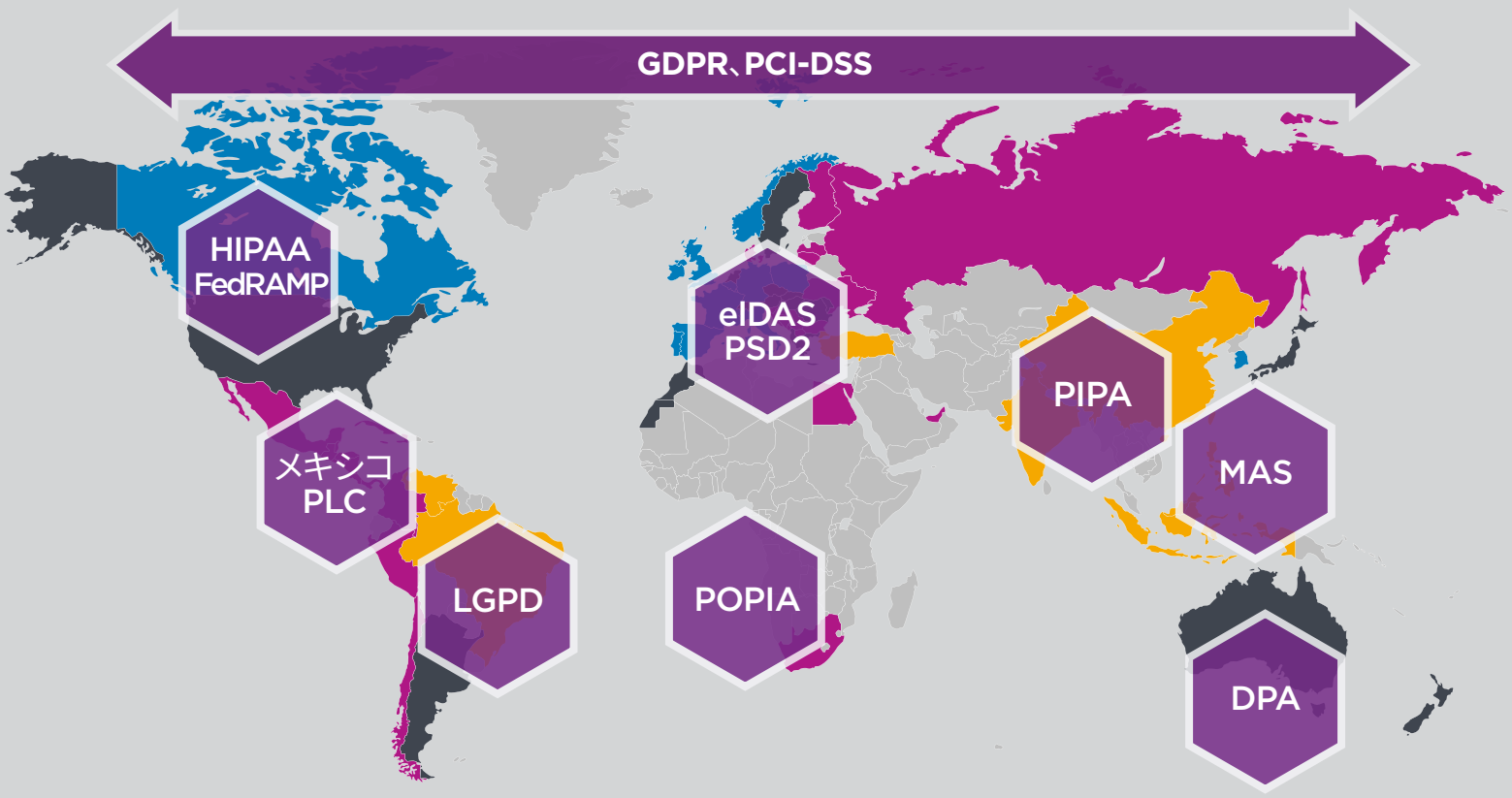
2018年に顧客データの漏洩件数が126%急増

1億9,760万件 → 4億4,650万件

出典：Identity Theft Resource Center www.idtheftcenter.org/2018-data-breaches

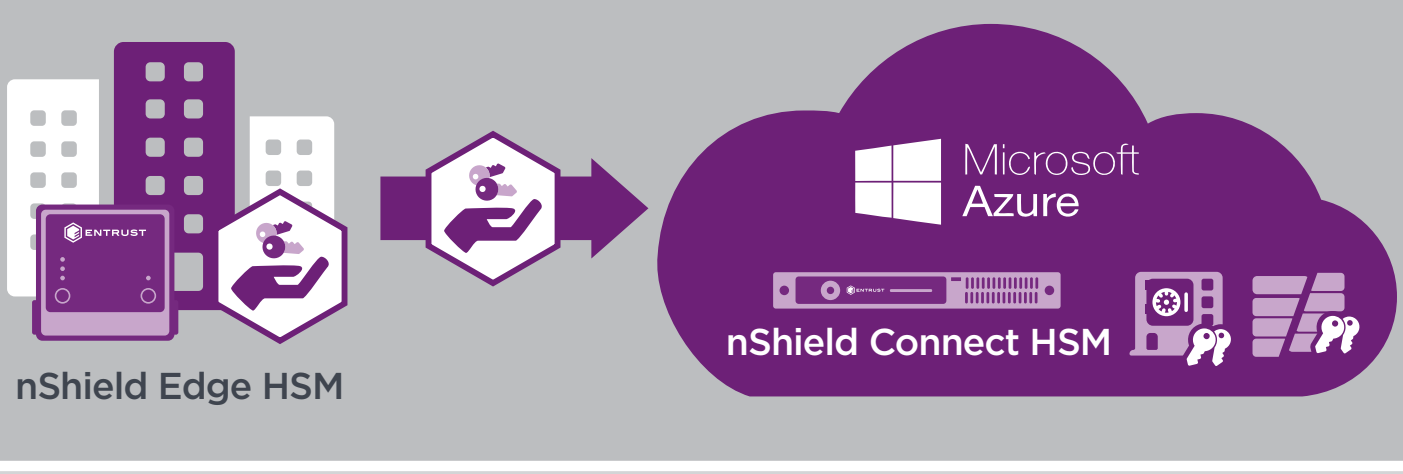
3 必要不可欠なコンプライアンス要件の遵守

プライバシー規制が次々と世界中で施行されているため、企業はより大きな責任と義務を負うこととなり、違反した場合には重い罰金が科せられます。nShield®ハードウェア・セキュリティ・モジュール（HSM）を使用することで、ベストプラクティスを確実に採用することができます。



4 鍵の利用権限を自社で維持

Bring Your Own Key（BYOK：独自の鍵の持ち込み）により、暗号鍵を使用して、クラウド内のデータを安全に制御および保護することができます。オンプレミスで独自の鍵を生成すると、鍵はクラウド内のHSMへ安全に転送されます。Azureはその鍵を使用してアプリケーションとデータを保護しますが、それらを閲覧したり悪用したりすることはできません。



5 クラウドに信頼の基点を追加

nShield HSMは強力な耐タンパ環境内で安全な暗号処理、鍵の生成や保護、暗号化、鍵管理などを可能にし、以下を実現します。

- 安全なアプリケーションプラットフォームを構築するためのさらなるセキュリティ層
- 暗号化操作と鍵の分離
- スマートカードによる強力なユーザ認証
- 二重管理と権限分散の施行
- 認定された高パフォーマンスの鍵生成
- 強力な暗号処理の高速化とオフロード
- FIPS 140-2認定取得

「*Bring Your Own Key with Entrust and Microsoft Azure*」動画をご覧ください

詳細は下記URLをご覧ください。
entrust.com/ja/HSM

ENTRUST
SECURING A WORLD IN MOTION