E-Globaledge Corporation
イーグローバレッジ株式会社

Controller-Based Encryption
＝ *RAID Board*を用いた 暗号化ソリューションのご紹介 ＝

E-Globaledge Corporation
CS Dept.

2019/05

データセキュリティーを取り巻く市場

E-Globaledge Corporation

- 暗号化ストレージソリューション
  - ストレージ導入全体の中で、今後大きな割合を占める予想
  - 既に一部市場では、調達の要求要件に
    - 医療系、金融、Eコマース、政府、保険、国防
- データセキュリティーとプライバシー保護を義務付ける法の整備
  - 個人情報保護法 (2003年制定)
  - 金融商品取引法(J-SOX法) (2008年以降実施)
  - 欧州連合一般データ保護規則 (2018年制定)
- サイバー犯罪の高度化
  - データ保護は喫緊の課題

保存データの暗号化は、
今後のセキュリティー戦略上の重要な要素に

Microsemi a Microchip company

FutureScape 2019 @ IDC 2018/10/30発表 oration

IDC FutureScape 2019

Prediction 9: By 2022, 50% of servers will encrypt data at rest and in-motion; over 50% of security alerts will be handled by AI-powered automation; and 150M people will have blockchain-based digital identities.

Business & IT Impact	✓ Pervasive encryption will be implemented by system ✓ Blockchain identity rollouts are nascent, complex ✓ Automated incident response will be accelerated by expanding attack surface
Guidance	✓ Press your vendors for their encryption platform timeline ✓ Work with blockchain consortia/communities to build verified ID projects ✓ Develop/refine more holistic risk and ROI models for deploying automated responses

Source: www.brighttalk.com IDC webinar 10/30/2018

暗号化ソリューションの実装方法

E-Globaledge Corporation

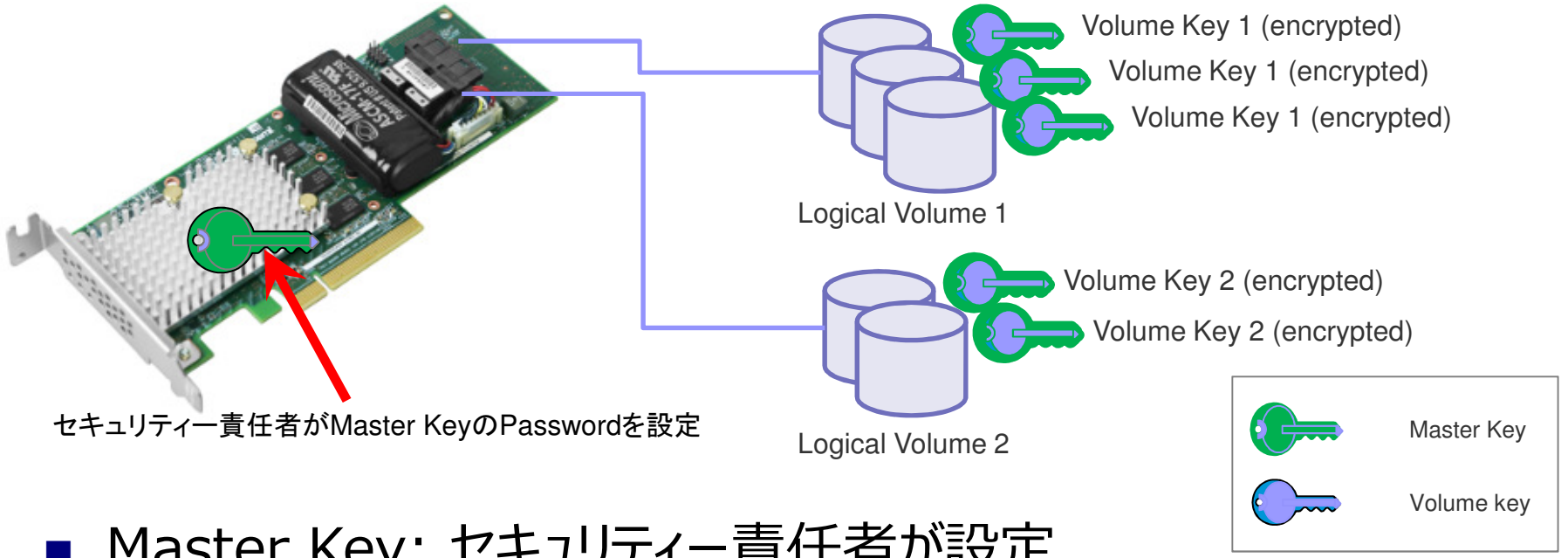
- ソフトウェアベース (SW)
  - アプリケーションまたはドライバ内のホストプロセッサのリソースを利用して暗号化
- 自己暗号化ドライブ (SED)
  - メディアに記録されているデータに対し、ハードウェア内のストレージデバイス自体で暗号化
- コントローラベース (CBE)
  - I/OコントローラまたはRAID on Chip(RoC)内で暗号化

CBEモデル唯一の商品は、
Microsemi製 SmartRAID3162-8i /e

暗号化ソリューションの実装別の比較 obaledge Corporation

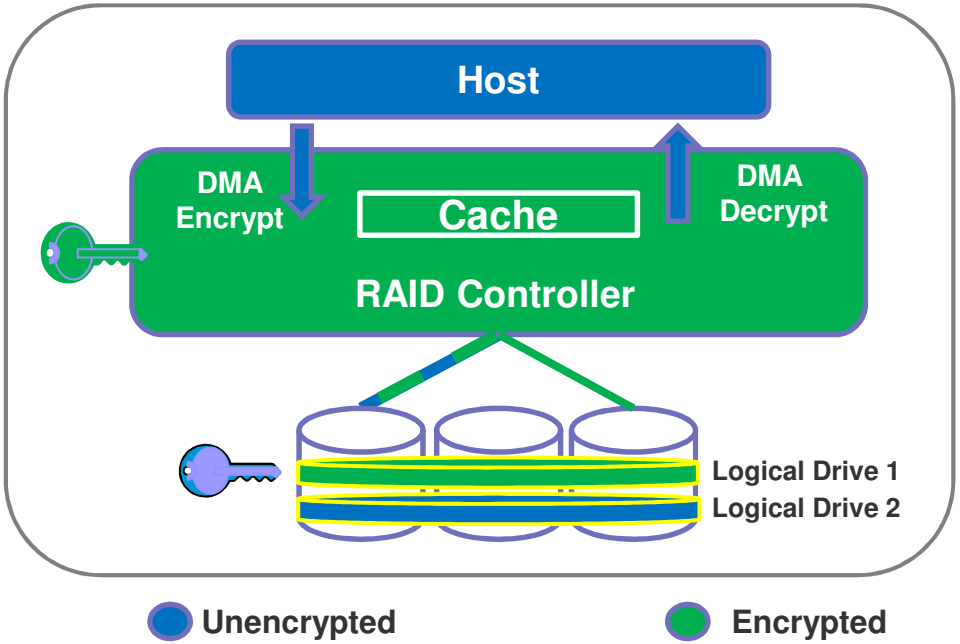
	ソフトウェア (SW)	自己暗号化 (SED)	maxCrypto コントローラーベース (CBE)
データ移動無しでの暗号化	○		○
暗号化キーの更新	○		○
ボリューム単位の暗号化選択	○		○
特定の論理ボリュームに対する暗号消去	○		○
サーバーやアプリケーションへの影響	**	○	○
対応メディアに依存しない暗号化	○		○
メディア数によるパフォーマンスへの影響	制限アリ	○	○
OSやアプリケーションへの依存		○	○
プラットフォームに依存しない一貫した性能			○
暗号化データ経路の確保 (ケーブル、エキスパンダー、キャッシュなど)	○		○
ファームウェア更新のロック		○	○
ストレージが増えた場合の費用増	可変	大	小

コントローラベースの暗号化



- Master Key: セキュリティー責任者が設定
  - 仮にRAIDボードが壊れた場合は、設定済みのMaster Keyを交換用のRAIDボードに設定すればOK
- 暗号化設定： HII, OffLineツール, GUI, CLIから設定可能
- 暗号化は論理RAIDボリューム単位で設定可能
- データへのホストアクセスを維持しながら暗号化が可能

maxCryptoの特長



- XTS AES 256bit インライン暗号方式
- 論理ブロックアドレス指定(LBA)毎の調整で、ブルートフォースデコードが防止
- RAIDコントローラー上のキャッシュで暗号化
- キー更新ライフサイクルポリシーをサポート
- コントローラ交換及び暗号化対応コントローラ間のドライブ移動をサポート

まとめ

- セキュリティーを向上
  - メディアタイプを問わずデータを安全化
  - コントローラードライブ間の情報抜き取りを防止
  - MasterキーとVolumeキーの2段階で暗号化
  - RAIDコントローラ上のキャッシュで暗号化

- 優れた柔軟性
  - 既存データはそのまま、暗号化が可能 (ボリュームも継続利用可能)
  - 特殊ドライブ(暗号化ドライブ)を使わず暗号化の導入が可能
  - OSやアプリケーションに関係なく64論理ドライブまで暗号化可能
  - 暗号化によるパフォーマンス低下を極小化