情報漏えいやサイバー攻撃から個人データを守るソリューション

Vormetric, Inc. 東京オフィス
Country Manager
池田克彦
Tel: 03-6717-4483
E-Mail: kikeda@vormetric.com

うちの病院は大丈夫？

1. プライバシーマーク取得済み！

2. 信頼できるベンダーに任せてあるので・・

3. 個人情報を扱う基幹系はネットワーク
   分離しているので安心。

4. 国内に多数ある医療機関でハッカーは
   もっと大きなところを狙うはず・・

症例を伴う個人情報は１件５万円で
取引されている！

セキュリティ対策の基本 （総務省HPより）

必要な情報セキュリティ対策

組織や企業を脅かす情報セキュリティ上のリスクにはさまざまなものがあり、必要な情報セキュリティ対策も多様です。

例えば、組織や企業で発生する可能性のあるトラブルとそれぞれの情報セキュリティ対策には、以下のようなものがあります。

ウイルス感染

対策
- ウイルス対策ソフトの導入
- ソフトウェアの更新
- 危険なWebサイトのフィルタリング

不正侵入

対策
- パスワード管理
- ファイアウォールの導入
- 侵入防止システムの導入
- ソフトウェアの更新
- ログの取得と管理

情報漏洩

対策
- ファイアウォールの導入
- 顧客データなどの管理
- 資料、メディア、機器の廃棄ルールの徹底
- 無線LANのセキュリティ設定
- ユーザー権限の管理
- パスワード管理

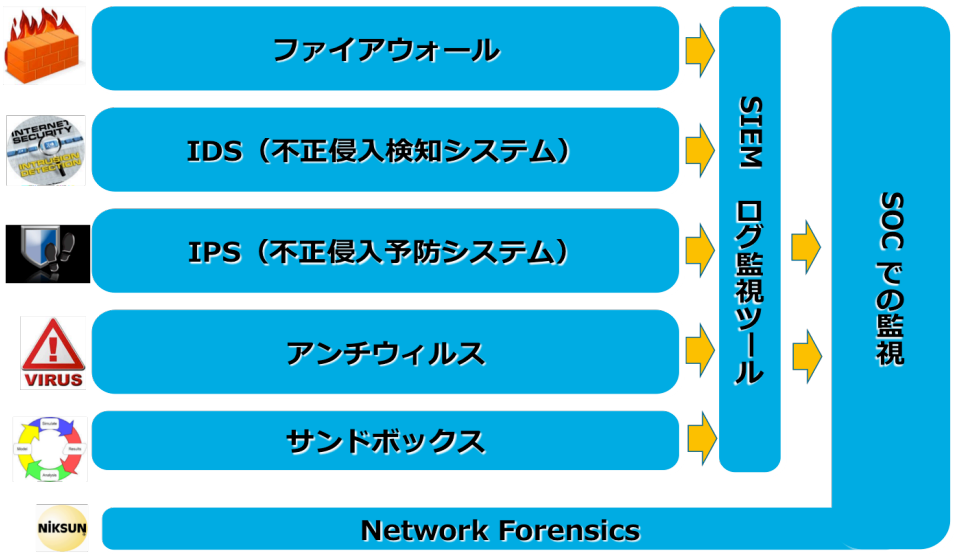
災害などによる機器障害

対策
- バックアップ
- 無停電電源装置の設置
- 設備の安全管理

理想的な！？　セキュリティ対策

- ポリシー策定
- 最新機材の導入
- SOC - セキュリティ監視
- CSIRT - 対応処置
- PDCAサイクル

CSIRT



SOC

それでも起こるインシデント

保険証情報10万人流出　名簿業者に 医療機関からか

2015/12/31付 | 日本経済新聞　朝刊 | 440文字 ［有料会員限定］

小 中 大　保存　印刷　リプリント

健康保険証の番号や加入者の氏名、住所など約10万３千人分の個人情報
していたことが30日までに、厚生労働省への取材で分かった。厚労省は病
機関から漏れた可能性があるとみて調査している。

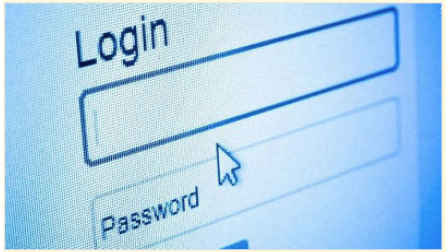
厚労省によると、流出したのは国民健康保険や企業の健康保険などに加
千人分の個人情報。健康保険証の番号や氏名、性別、住所、生年月日のほ
れているものもあった。

記載されていたのは2005年３月以前に生まれた人のデータ。対象は沖縄
に及び、大阪府の約３万７千人、奈良県の約２万５千人、滋賀県の約２万
国地方に集中していた。

後期高齢者医療制度の導入に伴って付与された番号がないことから、流

2016年05月06日 13時15分00秒

Gmail・Hotmail・Yahoo!などから2億7200万件のメールアドレスとパスワードが流



By Automobile Italia

GmailやHotmail、Yahoo!、そしてロシアで広く使われている「Mail.ru」などのウェブメールサービスから、**合計2億2700万件**というとてつもない
がセットになって流出していたことが判明しました。詳細は各サービスとも調査中とのことですが、気になった人は念のためパスワードを変更してお

Vormetric.com

個人情報漏洩事件・事故一覧（1ページ目 / 全294ページ）

2016/05/06 大手学習塾で個人情報が流出 - MT用プラグインにゼロデイ攻撃
2016/05/06 メルマガの誤送信でメールアドレスが流出 - 都港湾局
2016/05/02 エイベックス関連サイトに不正アクセス - 個人情報最大35万件が流出か
2016/05/02 5支店で顧客情報記載の書類紛失が判明 - 富士宮信金
2016/04/28 アサヒグループの3サイトで顧客情報の誤表示が発生
2016/04/28 家電通販サイト「デンキチWeb」へ不正アクセス - セキュリティコード含むクレカ情報流出
2016/04/28 オークファン子会社のB2B卸サイトに不正アクセス - 会員情報最大13万件が流出した可能性
2016/04/28 障害者福祉施設の利用者名簿を第三者へ誤送信 - 台東区
2016/04/27 旧奈良銀で扱った約300件の帳票が所在不明 - りそな銀
2016/04/27 マイナンバー含む扶養控除申告書が車上荒らしで盗難 - 鳥貴族FC加盟店
2016/04/25 J-WAVEに不正アクセス - ゼロデイ攻撃で個人情報が流出した可能性
2016/04/25 4支店で帳票約3万6000件の紛失が判明 - 十六銀
2016/04/25 ゴルフウェア通販サイトからクレカ情報が流出 - セキュリティコードも
2016/04/22 案内メール誤送信でメールアドレスが流出 - JAVADA
2016/04/21 日テレに不正アクセス - 最大43万件の個人情報が漏洩した可能性

山崎文明氏講演資料より

日本年金機構情報漏えい問題から学ぶ情報セキュリティ対策　2015年12月1日

1. 「高度な標的型攻撃」も対策の本質は変わらない
   - 不要なアプリケーションの削除
   - 確実な更新プログラム（修正パッチ）の適用
2. メールの運用を見直す
   - メールアドレスの推測を不可能に
   - 公開アドレスは別ドメインに
   - 偽装メールを不可能にするDMRACの普及
3. 最後の砦はホワイトリスト
   - EMET/Applockerなどの有効活用
4. データ中心セキュリティの適用
   - データの無価値化
     - トークナイゼーション/トランケーション
     - 暗号化

低コストで有効なセキュリティ対策とは

1. まずは基本の徹底
   - パスワード（✗デフォルト　✗使い回し
   - 適切なアクセス管理とデータ保管の見直し
     - Admin、DBAにすべての権限を与えていないか
     - 機密データの保管場所とアクセス管理
   - ソフトウェアは常に最新に更新しているか
   - ログの管理は短時間でも日々目を通す
2. 最新機器を導入するその前に、無償の機能を徹底活用
   - EMET
   - Applocker
   - 偽装メールを不可能にするDMRAC
3. データ中心セキュリティの適用
   - データの無価値化
     - トークナイゼーション/トランケーション
     - 暗号化

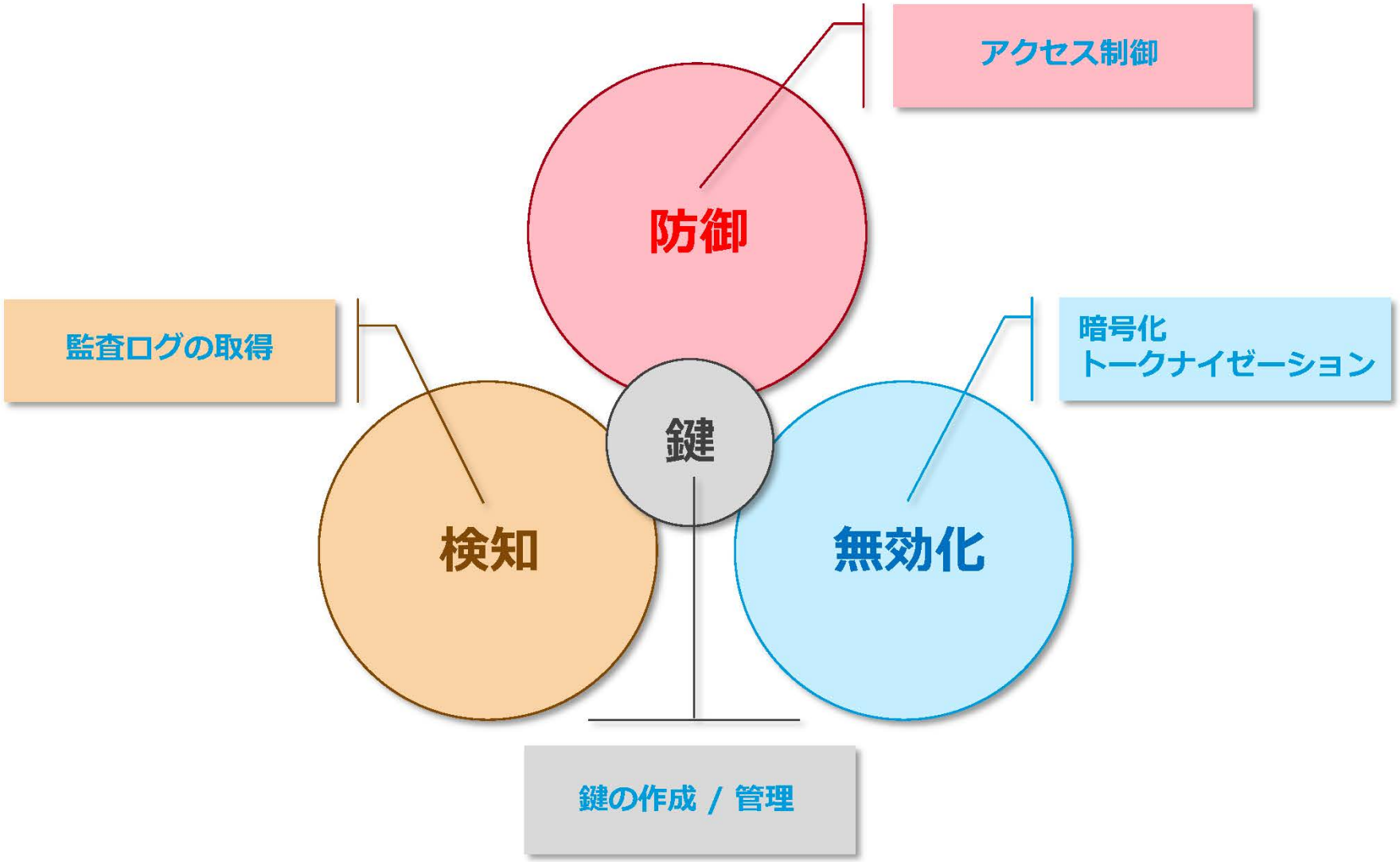
データ中心セキュリティ対策とは

1. 侵入は100%阻止できない
   - データを無価値化することにより進入時の被害を最小限に抑えることができます。
2. 侵入検知・防御に係るコストは膨大
   - 防御系システム、運用監視は際限のない投資
   - データ中心セキュリティは機密情報に対して「暗号化」と「アクセス管理」で守るため対象が限定できるため低コストで高い導入効果を得ることができます。。
3. データ中心セキュリティ
   - アクセス管理による防御
   - 暗号化、トークン化によるデータの無価値化
   - データへのアクセス証跡を可視化

Vormetric 製品概要

Vormetric.Inc 東京オフィス

Vormetric製品の主要機能



Vormetric製品 暗号化できる対象は？

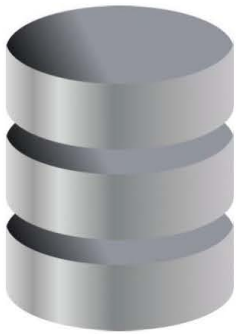
Vormetric

アプリケーション暗号
トークナイゼーション

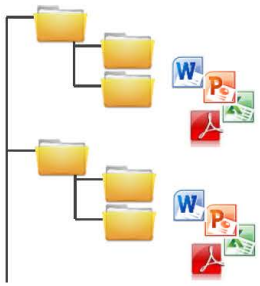
透過暗号

クラウドストレージ暗号

データベース



ファイルサーバ



クラウド

ORACLE
PostgreSQL
Microsoft SQL Server
MySQL
mongoDB
その他

solaris
suse
AIX
redhat

amazon web services S3
box
caringo

Vormetric製品 システム構成

クラウドストレージ暗号

amazon web services S3

box

caringo

クラウドストレージ用
仮想VMアプライアンス

エージェント

管理者

Web
ログイン

・鍵の作成/管理
・ポリシーの作成/管理
・監査ログ　など

対象に応じて
ライセンスを投入

DSM (ハード版/仮想版を選択可)

DSM　HA　DSM

暗号鍵

他社暗号化製品
鍵の管理 (KMIP)

トークナイゼーション用
仮想VMアプライアンス

他社データベース製品
鍵の管理(TDE)

ファイルサーバ暗号

データベース暗号

トークナイゼーション

DSM (Data Security Manager)

■DSMの役割

・鍵の管理
・ポリシーの管理
・ログ管理
・管理者による集中管理

※HA構成が可能です。(推奨)

■DSMの種類

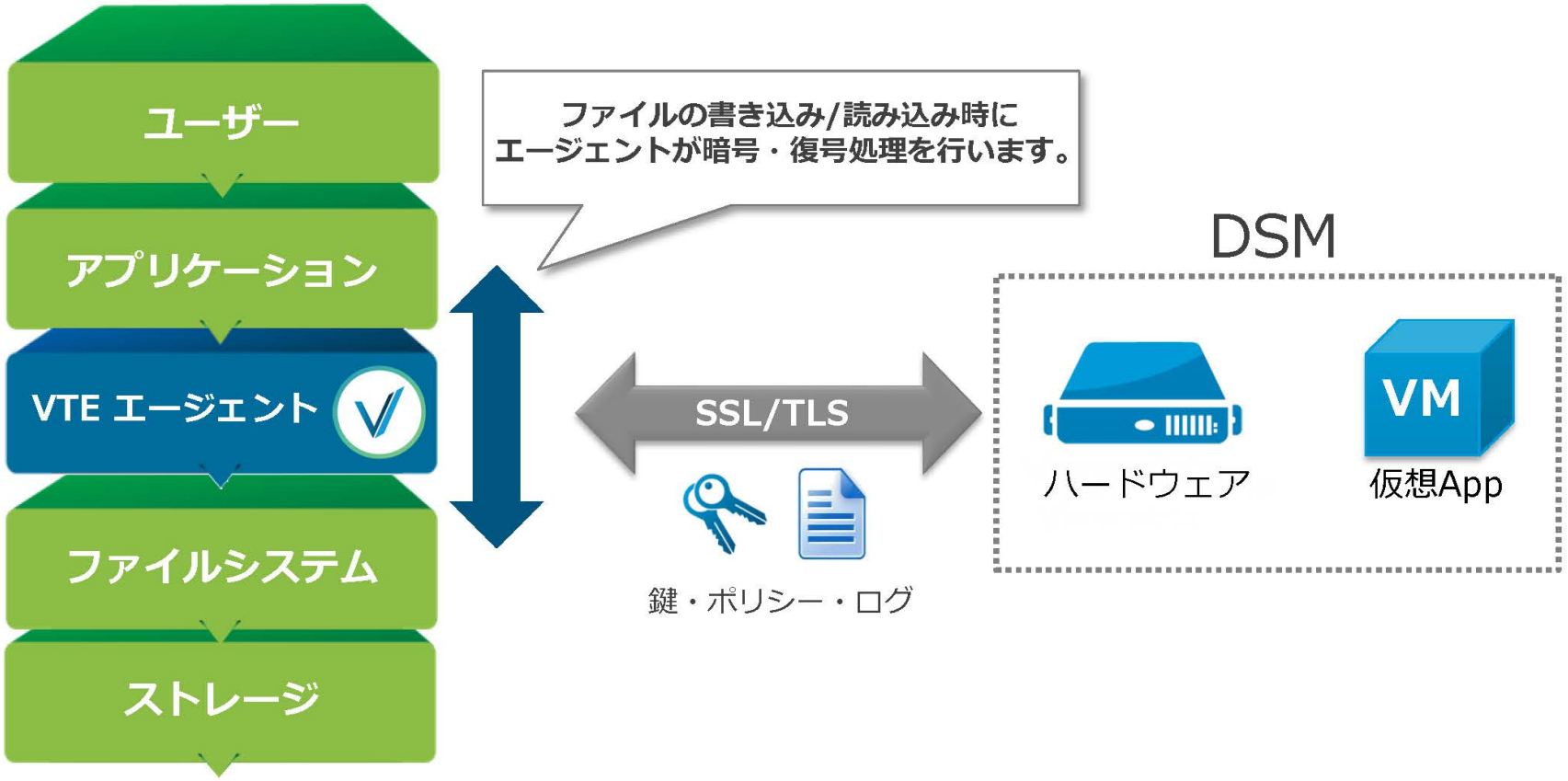
3タイプのDSMを提供しています。

・仮想アプライアンス
・ハードウェアアプライアンス (FIPS 140-2 Level 2)
・ハードウェアアプライアンス (HSM – FIPS 140-2 Level 3)

※FIPS
Federal Information Processing Standardの略。
アメリカ合衆国の連邦政府機関が軍事以外の用途で購買・利用する情報・通信機器が満たすべき技術標準を定めた規格。
暗号・セキュリティ関連の標準の例として、FIPS 46(DES)、FIPS 140(暗号モジュールのセキュリティ要件)、FIPS 197(AES)などがある。

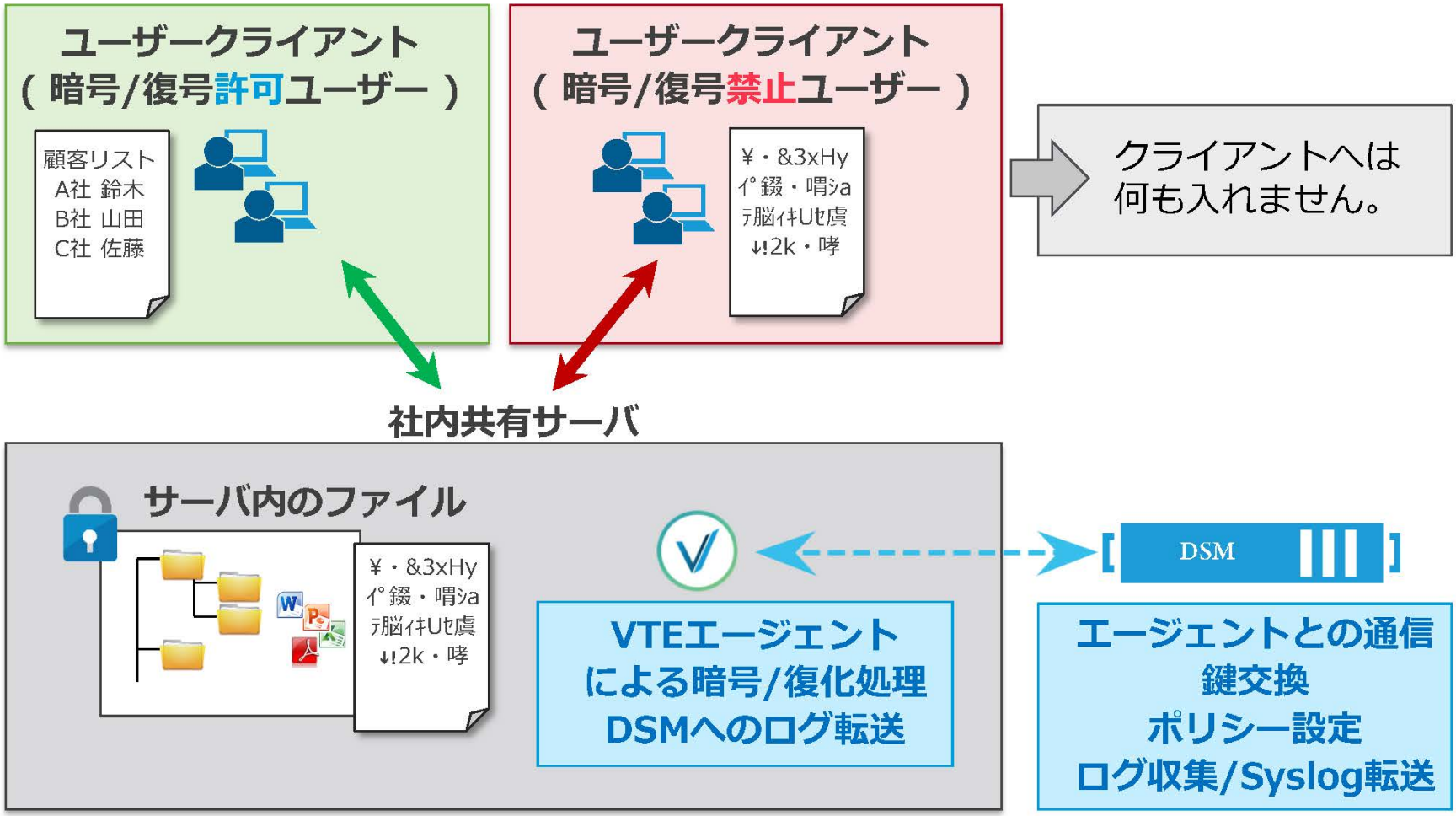
Vormetric製品を用いた対策例
ファイルサーバ

透過暗号 (VTE) エージェント



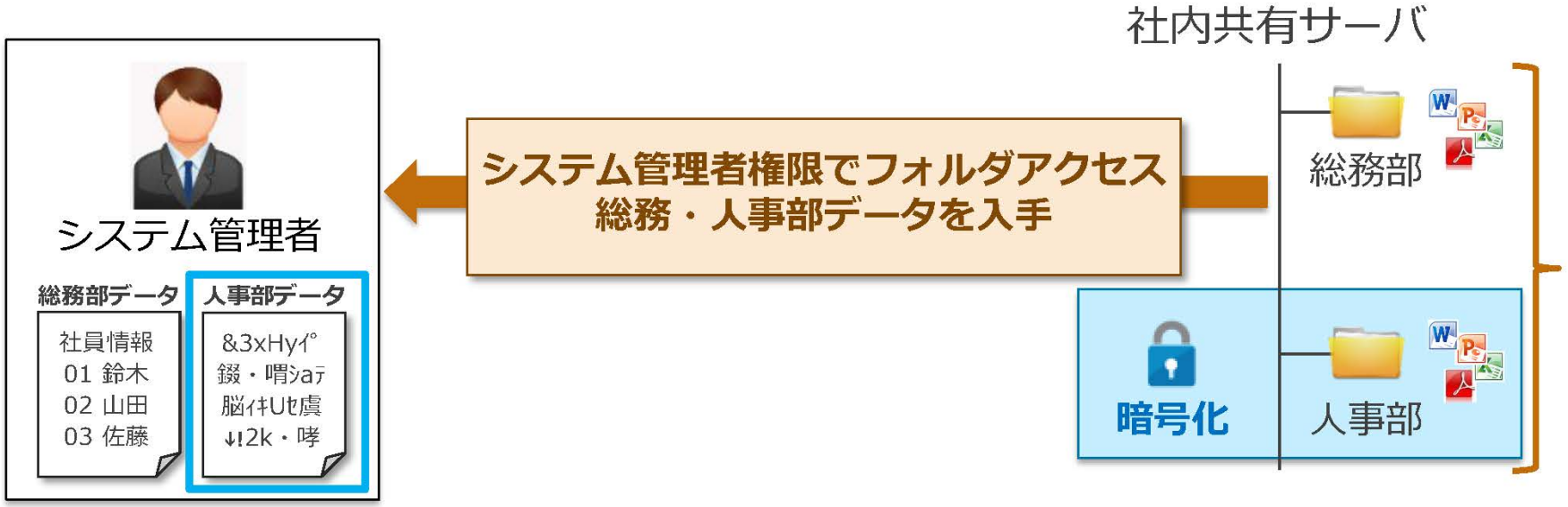
透過暗号（VTE）の構成例

・煩雑な暗号化を容易に実現します。
・ユーザーに対して暗号化/復号化されていることを意識させません。



内部犯行対策

人事部フォルダはVormetricによって暗号化されてるためシステム管理者でもデータ内部を読み取ることはできません。



システム管理者へ暗号/復号権限を与えない場合も

- ファイルのプロパティデータ(作成者など)は暗号化しても維持されます。
- アクセス権の操作など、システムメンテナンスへの影響は与えません。

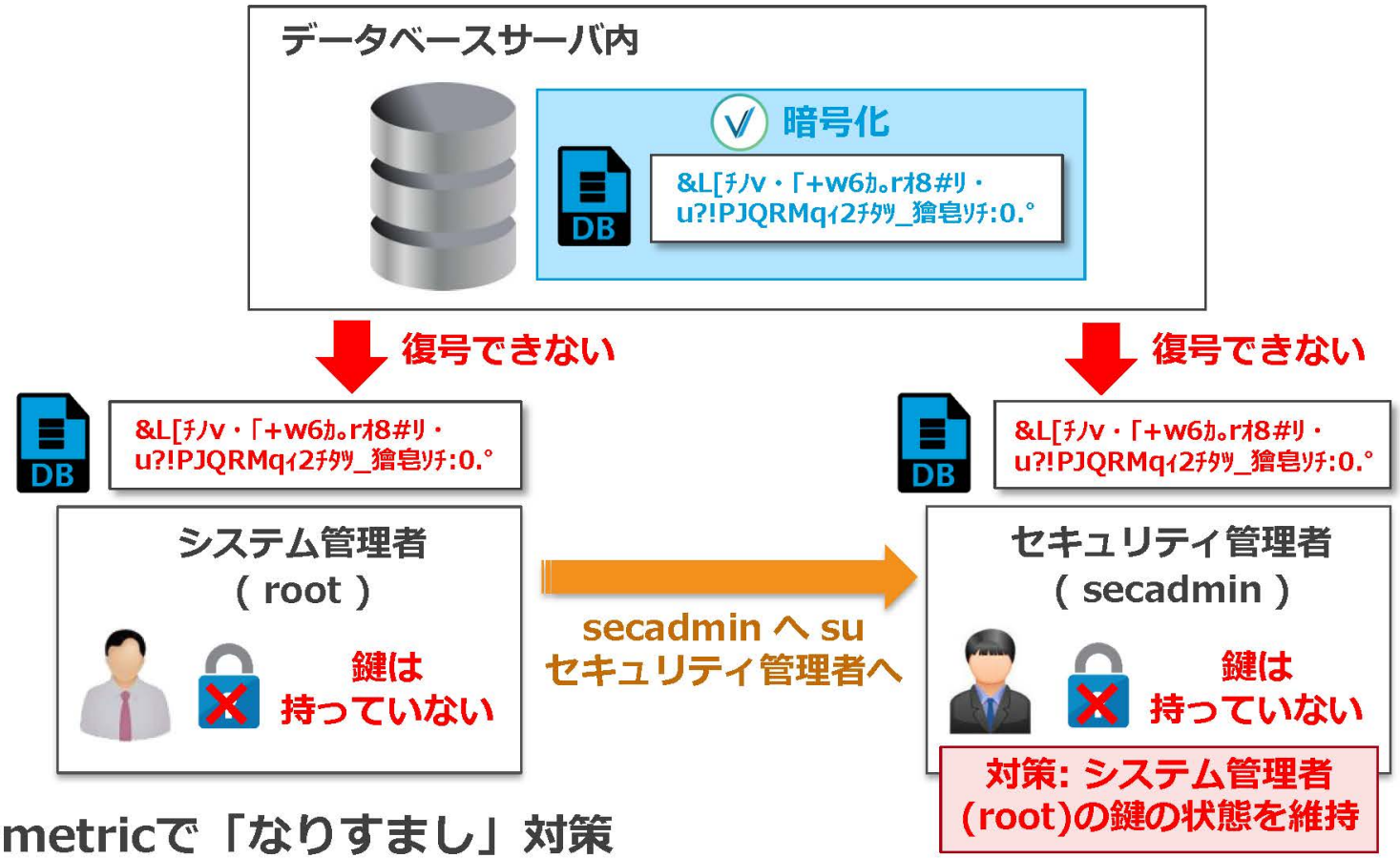
システム管理者がデータ内部を見る必要が無いならば
システム管理者に復号権限を与えないということも情報漏洩対策の一つ。

Vormetric製品を用いた対策例
データベース

データベースの対策例 システム管理者への対策

システム管理者の「なりすまし」を禁止

権限を悪用させない



Vormetricで「なりすまし」対策

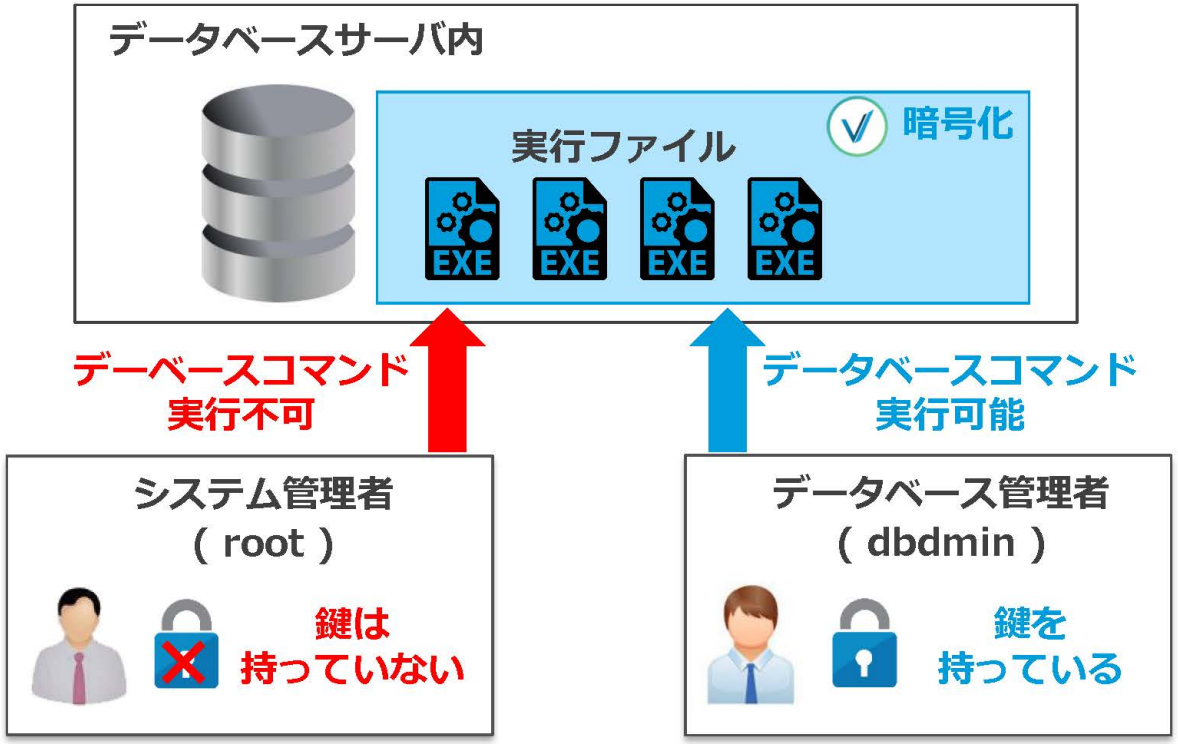
元のユーザーの鍵の状態を維持。

どのユーザーへ変更しても鍵は持てない。データの盗難を防止。

データベースの対策例 システム管理者に対する対策

実行ファイルを無効化

使わせない



システム管理者(root) には使わせない

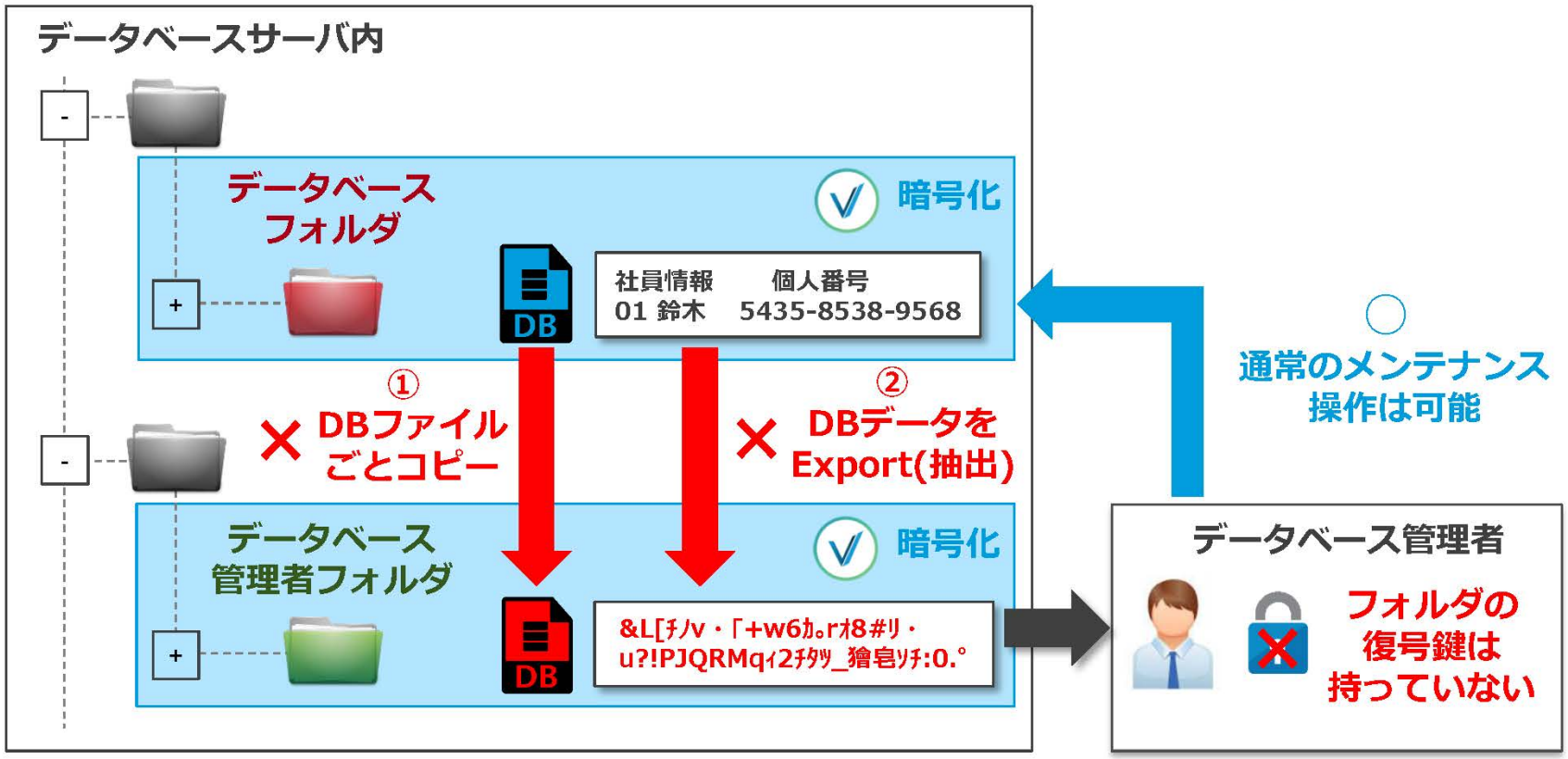
実行ファイルが暗号化されているため、システム管理者はデータベースの各種コマンドは実行できない。

su も禁止されているためデータベース管理者になることもできない。

データベースの対策例 データベース管理者に対する対策

データファイルを無効化

盗ませない



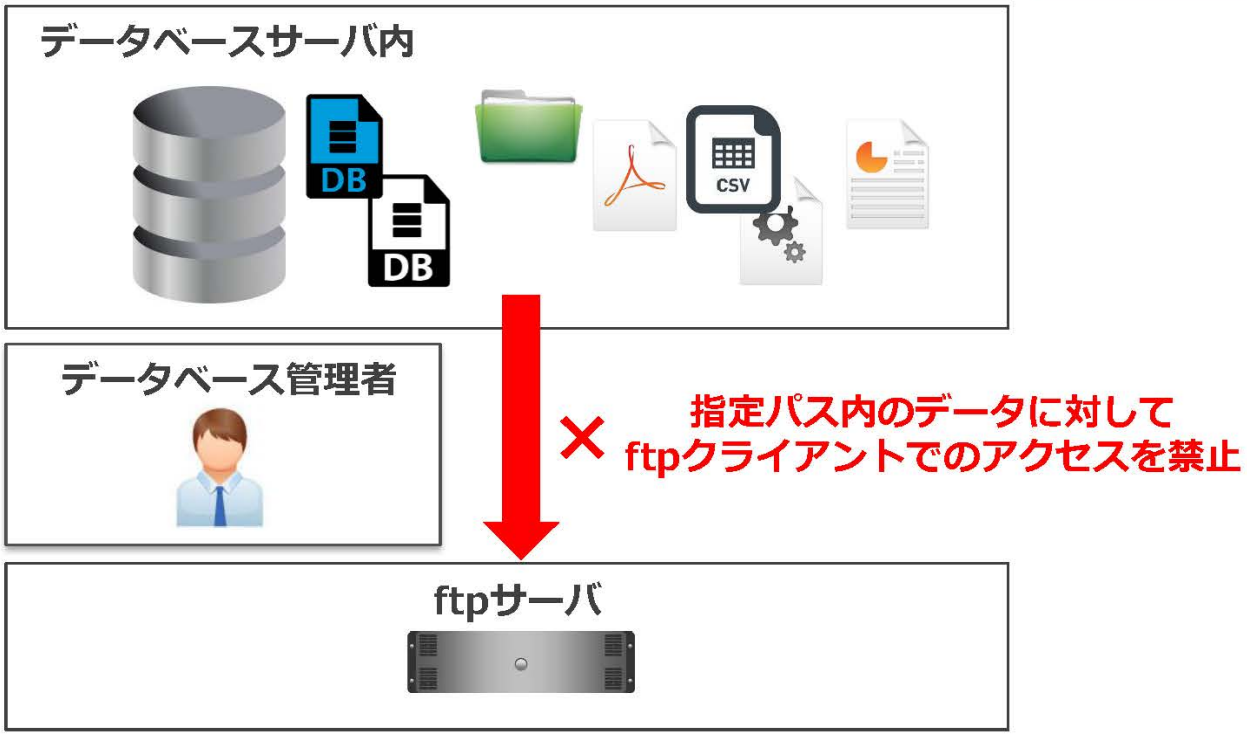
データベース管理者に対する防御

データベース管理者フォルダの復号鍵を与えないことで、
①データベースファイルのコピーや②データのExport(抽出)を無効化。

データベースの対策例 データベース管理者に対する対策

データベース管理者によるftp転送の禁止例

盗ませない



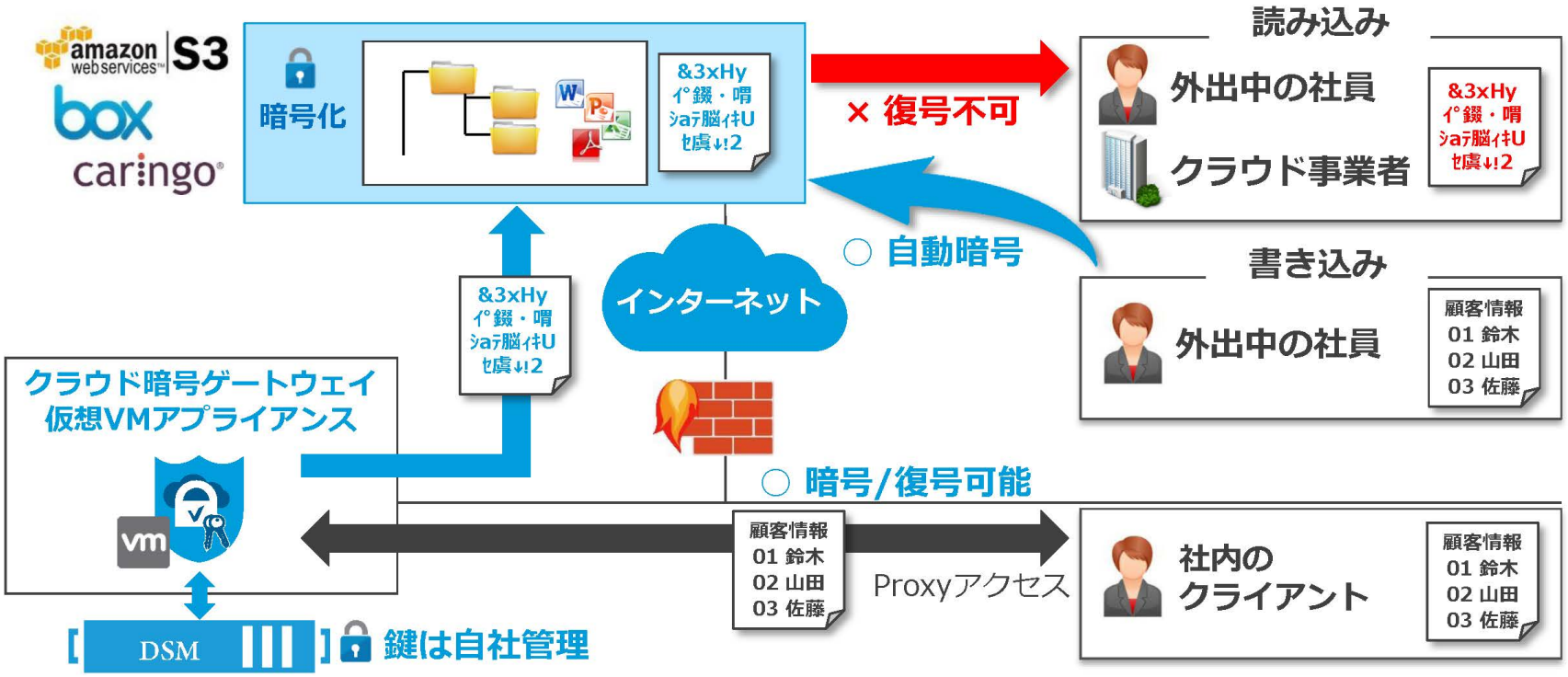
データ転送を禁止

特定ユーザーが実行する特定プロセス(ftpなど)に対して、指定したパス内にあるデータへのアクセスを禁止する。

Vormetric製品を用いた対策例
クラウドストレージ

クラウドストレージの対策例

外部からのファイルアクセスを無効化

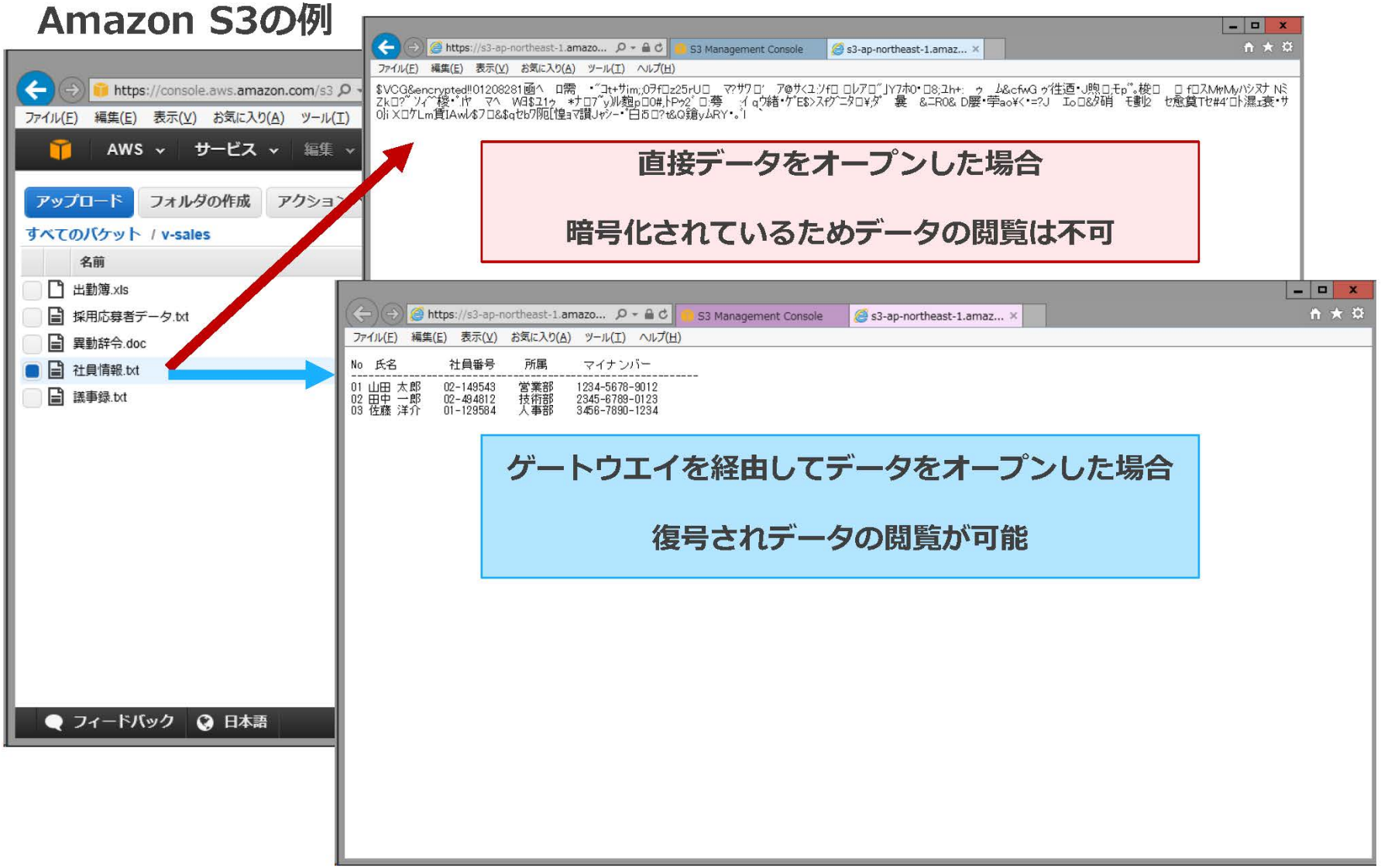


クラウドストレージの暗号化による防御

外出中の社員は社内のアプライアンスを経由しなければ復号はできない。
外出中に社員がアップロードするデータはアプライアンスによって自動検知されて暗号化される。

クラウドストレージへの適用例

Amazon S3の例



Vormetric製品の特長

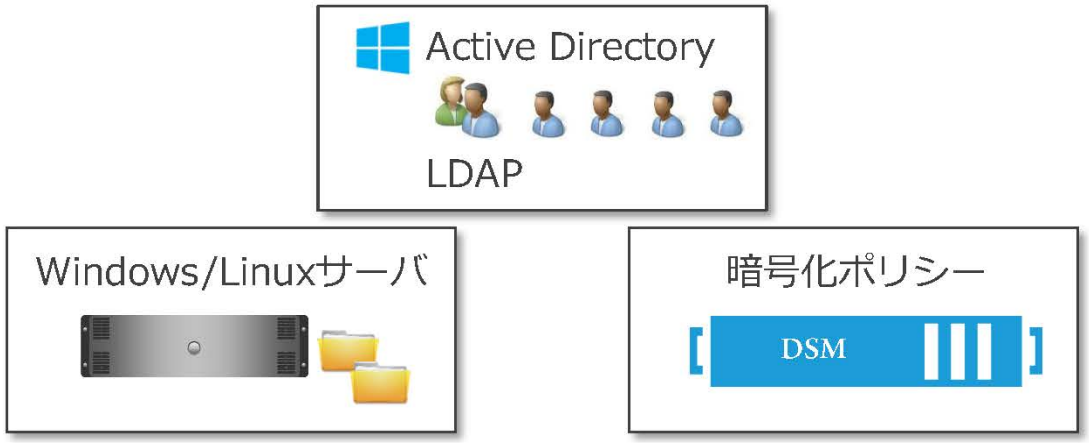
暗号化製品は運用管理が難しい？

暗号/ポリシー設定

1.Web GUIを用いた分かり易い設定画面。
2.鍵の作成も鍵の名称を入力するだけで作成可能。
3.暗号化用フォルダのような専用フォルダは不要。既存フォルダを利用可能。
4.利用ユーザーに暗号化されていることを意識させない。

認証サーバとの連携

1.ポリシーはActive DirectoryやLDAPといった認証サーバと連携可能。
2.人事異動時もActive Directoryの操作だけでポリシーの変更操作は不要。※
※既存のWindowsフォルダアクセス権をドメイングループでコントロールしている場合。



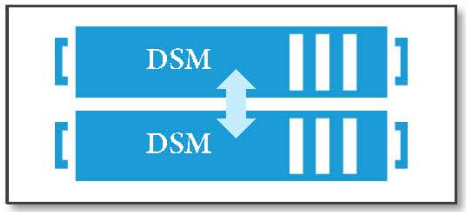
鍵の管理は？

鍵は重要

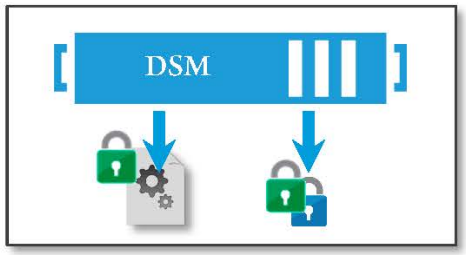
1.鍵を紛失した場合はデータの復号ができなくなる。
2.鍵の紛失には「物理的な紛失」と「トラブルによる鍵の取得障害」がある。
3.鍵を盗まれると情報漏洩を招く恐れがある。

Vormetricでは

①鍵の保管
・鍵はすべてDSM内に格納。
・鍵の内部を見ることはDSM管理者であっても不可能。



②鍵の可用性
・HA構成によってそれぞれのDSM内に鍵を格納。
・プライマリーDSMの障害時はバックアップDSM内の鍵を使用。

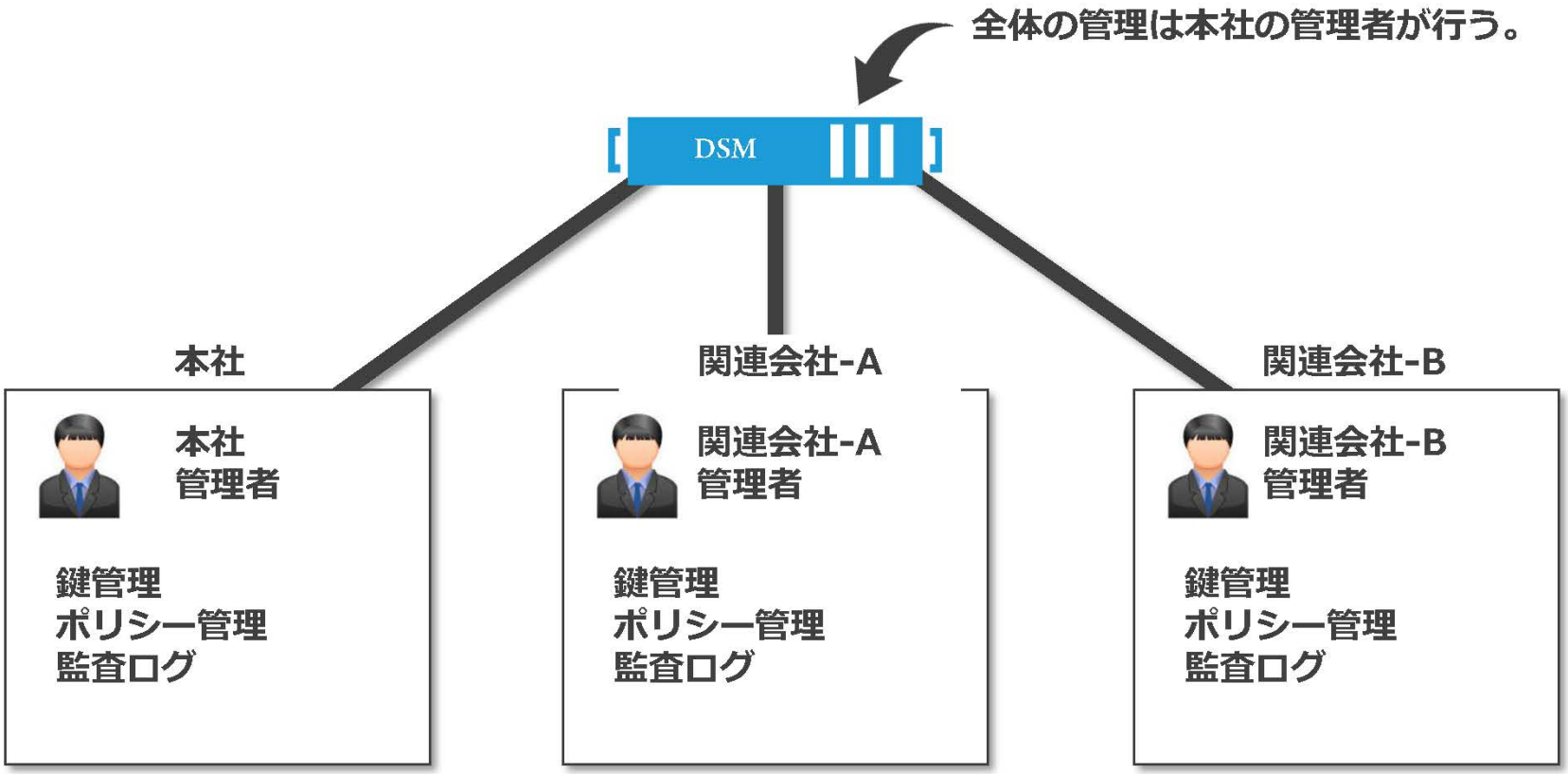


③鍵のバックアップ
・鍵も含んだDSMの設定を定期バックアップ可能。(ファイルは暗号化)
・鍵を外部へExportし保管可能。
(Exportされた鍵ファイルは キーコードにより暗号化)
・いずれもDSMの中でのみ復元可能。

テナント単位で運用管理を分散

マルチテナント機能

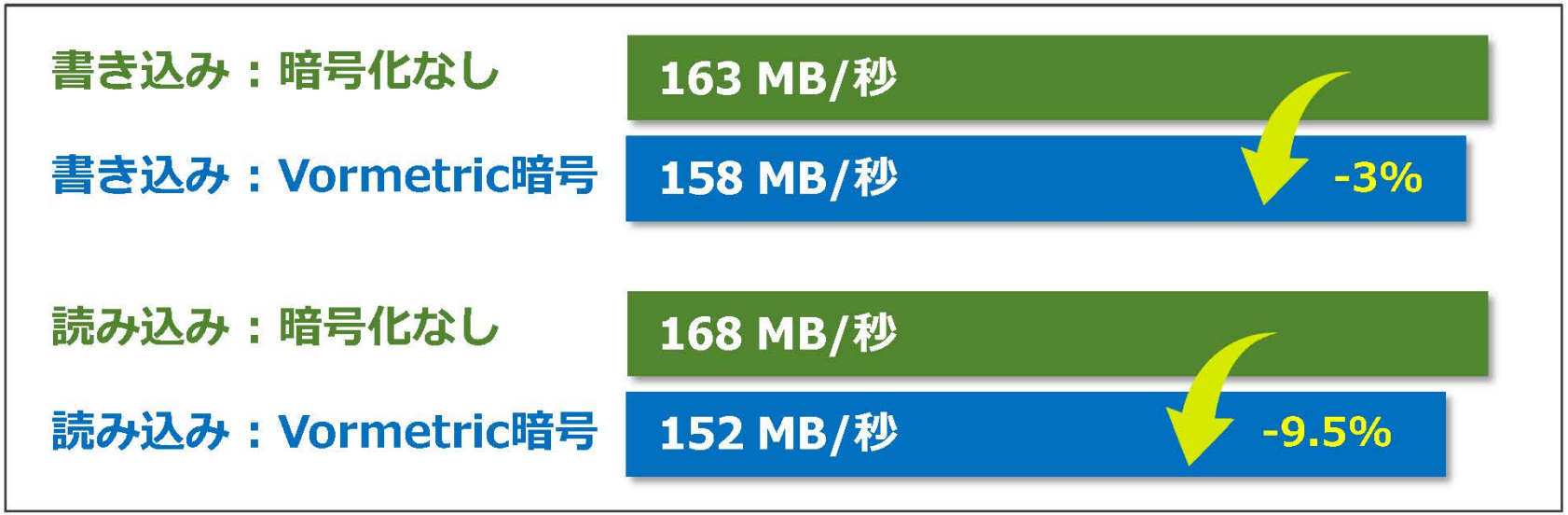
DSMのマルチテナント機能を使用することで、関連企業単位や部門単位で運用管理を分散させることが可能。



パフォーマンスは？

暗号化のボトルネックを解消

2008年にインテルが発案した暗号/復号の高速化技術、
AES-NI (Advanced Encryption Standard New Instructions)を用いることで
暗号/復号のパフォーマンスが大幅に改善。



テスト環境
・Windows2012r2 サーバ (intel Corei7 / 3.4GHz / 2 socket, 4 core / 4GB RAM / AES-NI対応)
・vShpere5.0 Guestサーバ
・テストドライブは起動ドライブとは別のものを使用 (VMプロビジョニングはシックEager Zeroed)

テスト方法
・1GBファイルの読み込み / 書き込みを3回実施し平均値を取得

Vormetric製品 どのような暗号化が可能か ？

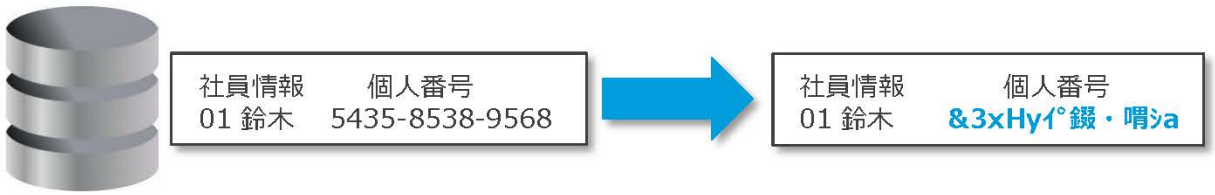
ファイルサーバ内の文書ファイルの暗号化

透過暗号
ファイルを暗号化

データベースファイルの暗号化

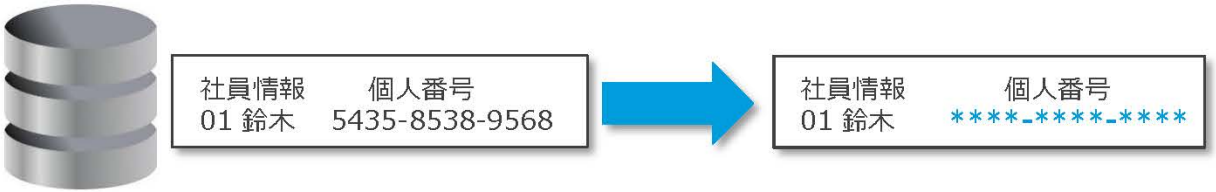
透過暗号
データベースファイル
や実行ファイルを暗号化

データベースカラムの暗号化



アプリケーション暗号
特定のカラムを暗号化

トークナイゼーション



トークナイゼーション
特定のカラムをトーク
ン化してマスキング

透過暗号 (VTE) エージェント

■ファイルサーバ上で稼働し、以下の役割を持っています。

(1) DSMとの通信

・鍵の要求取得 / ポリシー情報の要求取得
・イベントのロギング / DSMに対するステータスの提供

(2) 適用処理

・対象フォルダ (Guard Points) に対する鍵 / ポリシーの適用
・対象リソースのモニター (暗号化 / 復号化、アクセス制御)

■サポートプラットフォーム

・HPUX 11iv2～11iv3
・Solaris 10～11.2
・Red Hat / CentOS 5.5.5～7.1
・SUSE Linux Enterprise Server (SLES) 11～12
・AIX 5.3～7.1
・Windows 2003～2012

※詳細は別途お問い合わせ下さい。