Vormetric
A Thales company

PCIDSSセキュリティフォーラム 2016

Vormetricの高速トークナイゼーション・暗号化機能を用いた情報漏洩対策

Vormetric,Inc. 東京オフィス

Vormetric

■Vormetric (ボーメトリック) 会社概要

2001年設立。
米国サンノゼ本社を拠点に北南米・アジア・欧州の21ヵ国でビジネス展開。

■製品

暗号化製品：ファイルサーバ・データベース・クラウド向け暗号化製品。

■顧客

1,500社以上の顧客、Fortune30社のうち17社がVormetric製品を採用。
連邦政府・金融企業・流通・製造業など多くの業種が顧客。

■日本

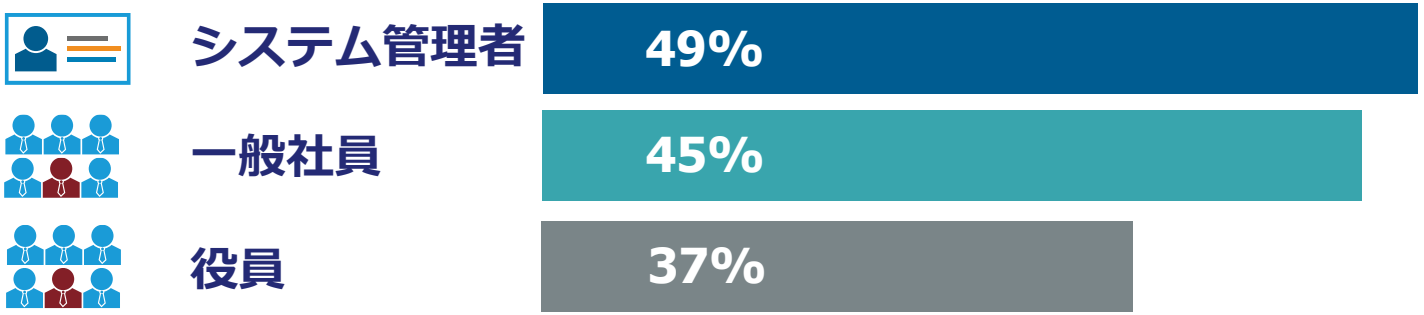
2015年3月 東京オフィス開設

Vormetric
A Thales company

内部犯行と情報漏洩

内部犯行による情報漏洩

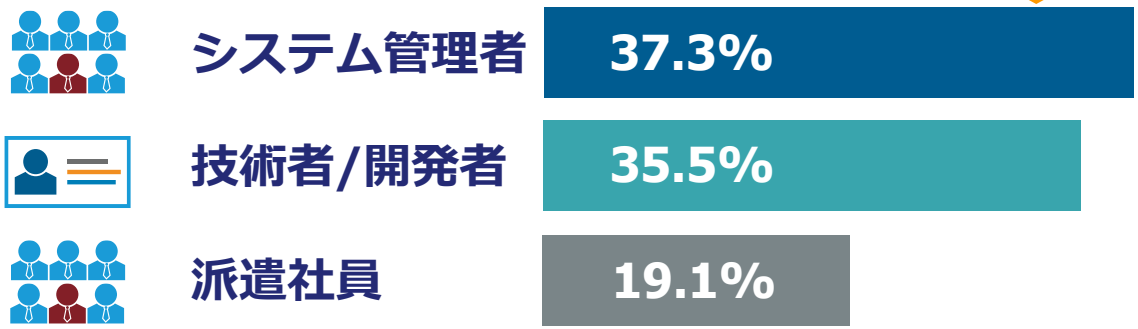
■IT部門は誰に対して脅威を感じているか？



※複数回答含む　※2016年 売上50億円以上の日本企業100社のIT部門に対するVormetric調査結果

■情報漏洩の犯人、その実態は？

システム管理者または技術系社員が
自分のスキルを使用し犯行に及ぶ



※IPA 組織内部者の不正行為によるインシデント調査より

漏洩した情報

■最近発生した国内の内部犯行による情報漏洩事件

日付	業種	漏洩データ数	漏洩したデータ
2016年　2月	金融関係	18万件	顧客情報
2015年12月	医療関係	10万件	健康保険証情報
2015年10月	地方自治体	18万件	住基/課税情報
2015年10月	人材関係	1.7万件	個人情報
2015年　9月	地方自治体	68万件	有権者情報等

データベースからの情報盗難が多い

■何が漏洩したのか？


顧客情報 52.6%


社内情報 15.8%


ID/パスワード 15.8%

※IPA 組織内部者の不正行為によるインシデント調査より

内部犯行の実態

■ **実態は**
・**アクセス可能なところから**データを盗んでいる。
・マルウェアや侵入に対する検知は行っていても**内部犯行に対する対策や検知**は？
・ログを取得していてもデータ自体は**盗むことが可能**。

故にその気になればいつでもデータを盗むことができてしまう。

■ **傾向: 犯行に及ぶ社員とその対象**
・一般社員は共有ファイルサーバ内のファイルを盗難。　(盗難データ数少)
・システム(DB)管理者はデータベース内のデータを盗難。(**盗難データ数多**)

■ **統計データには出てこない不正なアクセス**
システム管理者による管理者権限を利用したデータの閲覧。(盗難ではない)

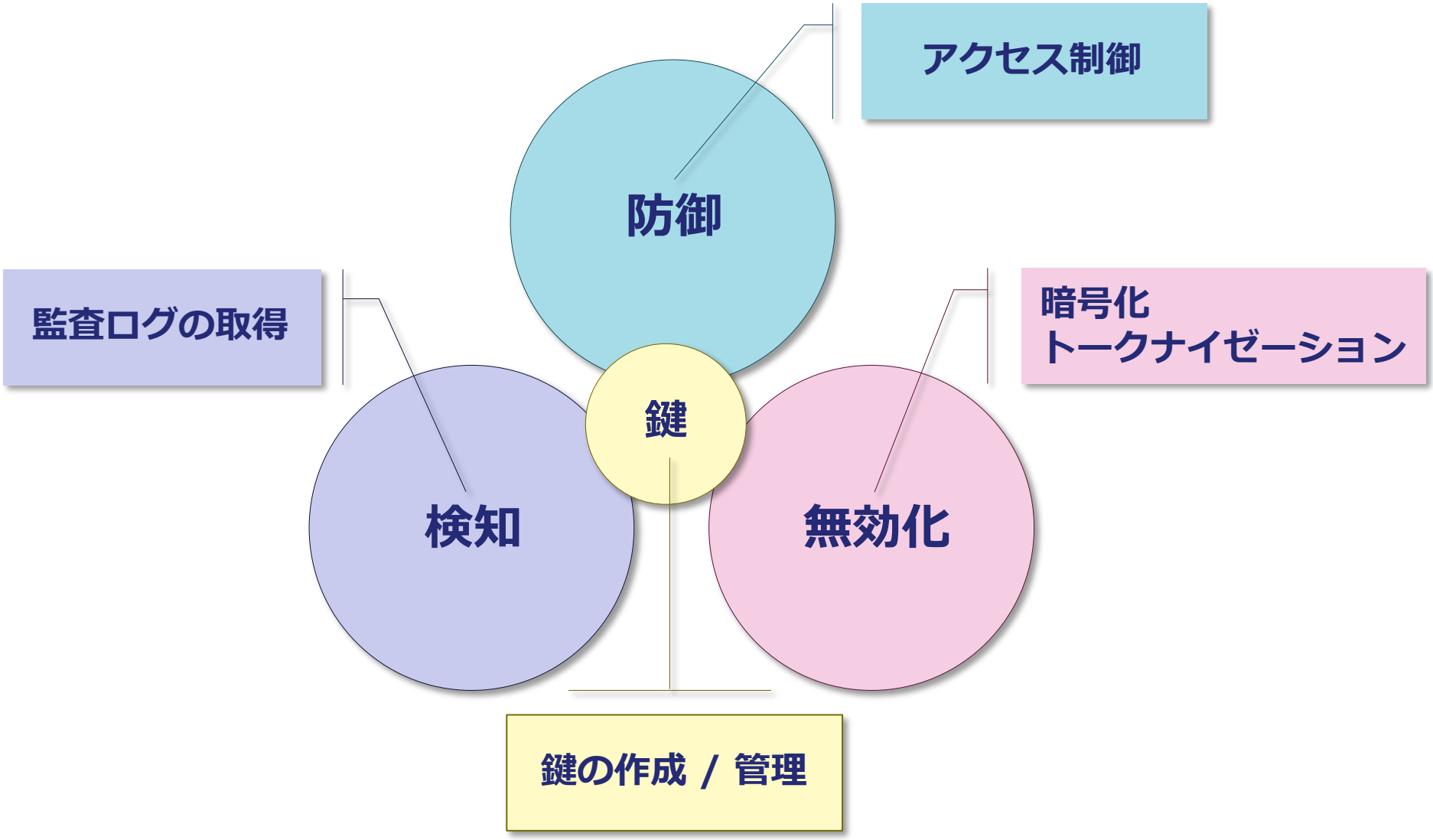
米国の展示会において某ベンダーがIT管理者に対してアンケートを実施。
「自分の管理者権限を用いてサーバ内の機密データを見たことがあるか？」

約60%のシステム管理者が「見たことがある」と回答。

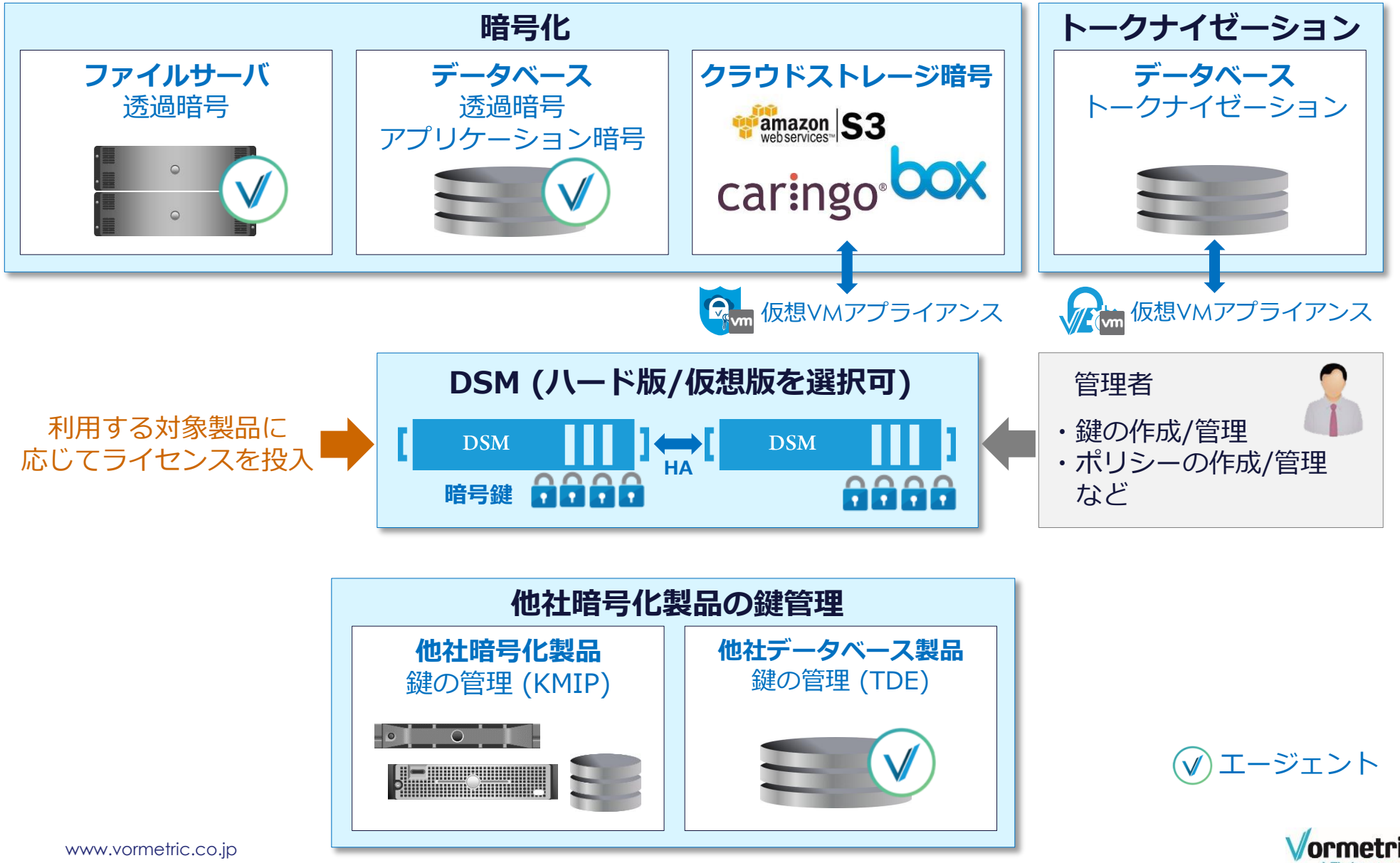
Vormetric
A Thales company

Vormetric 製品概要

Vormetric製品の主要機能



Vormetric製品 システム構成



DSM (Data Security Manager)

■DSMの役割

・鍵の作成/管理
・ポリシーの作成/管理
・ログ管理
・管理者による各コンポーネントの集中管理

※最小構成台数は2台より最大8台まで。(HA構成: Failover Cluster)

■DSMの種類

3タイプのDSMを提供。

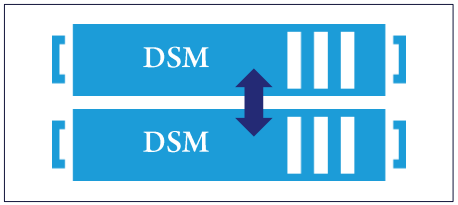
・仮想アプライアンス (FIPS Level1) : VMWare / Hyper-V / Amazon AMI
・ハードウェアアプライアンス (FIPS 140-2 Level 2)
・ハードウェアアプライアンス (HSM – FIPS 140-2 Level 3)

※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。

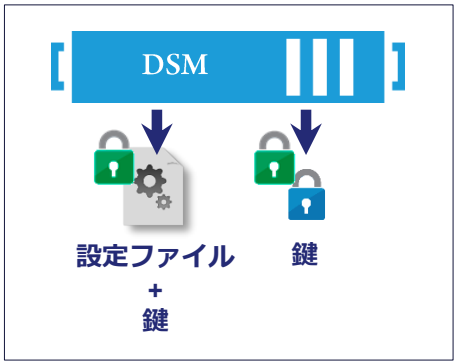
鍵の管理について

■鍵はDSMで一元管理

①鍵の作成・保管
・鍵はすべてDSM上で作成され、DSM内部に保管。
・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構成によって鍵は同期され、各DSM内に鍵を保管。
・Primary DSMの障害時はSlave DSM内の鍵が使用される。

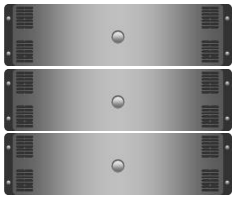


③鍵のバックアップ
・鍵を含むDSMの設定ファイルを外部のサーバへ定期バックアップ。
・鍵単体を外部へExport保管。
・バックアップファイルやExportした鍵ファイルはキーコードにより暗号化され、いずれもDSMの中でのみ復元可能。
・鍵のExport操作は鍵の名称含めDSM上のログに記録。

■運用においては
バックアップしたDSMの設定ファイルやExportした鍵を保管しているサーバやフォルダに対するアクセス制御や監査ログの取得を行っておくことも重要。

Vormetric製品 どのような暗号化が可能か ？

ファイルサーバやクラウド内の文書ファイルの暗号化



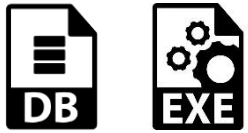
社員情報
01 鈴木
02 山田
03 佐藤

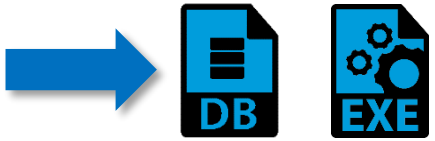
&3xHyｲﾟ
錣・喟ｼa
ﾃ脳ｨｷUｾ
虞↓!2k

透過暗号
ファイルを暗号化

クラウドストレージ暗号
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
実行ファイル等を暗号化

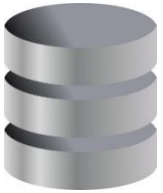
データベースカラムの暗号化

顧客名	カード番号
鈴木	1111-2222-3333-4444

顧客名	カード番号
鈴木	&3xHyｲﾟ錣・喟ｼa

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



顧客名	カード番号
鈴木	1111-2222-3333-4444

顧客名	カード番号
鈴木	2419-6457-7150-6319

トークナイゼーション
特定のカラムをトークン化
マスキング復号が可能

Vormetric
A Thales company

Tokenization

トークナイゼーション

トークナイゼーションのメリット

■技術面

・既存データベースのカラム改修は不要。
・組み込みがカラム暗号と比較して容易。
・マスキング機能によって表示内容の制御が可能。

暗号化 (データベースカラム暗号) の場合

氏名	カード番号
鈴木	1111-2222-3333-4444

→

氏名	カード番号
鈴木	w6ｶ｡ru?!PJQRMqｲ2ﾁﾀﾂ

・データ長が変わってしまう
・データタイプが変わってしまう
・既存プログラムの改修工数が大きい
・復号すると原本データが表示される

トークナイゼーション (トークナイズ)

氏名	カード番号
鈴木	1111-2222-3333-4444

→

氏名	カード番号
鈴木	2419-6457-7150-6319

・データ長は変わらない
・データタイプは同じ
・既存プログラムの改修工数は小さい

トークナイゼーション (デトークナイズ)

氏名	トークン番号
鈴木	2419-6457-7150-6319

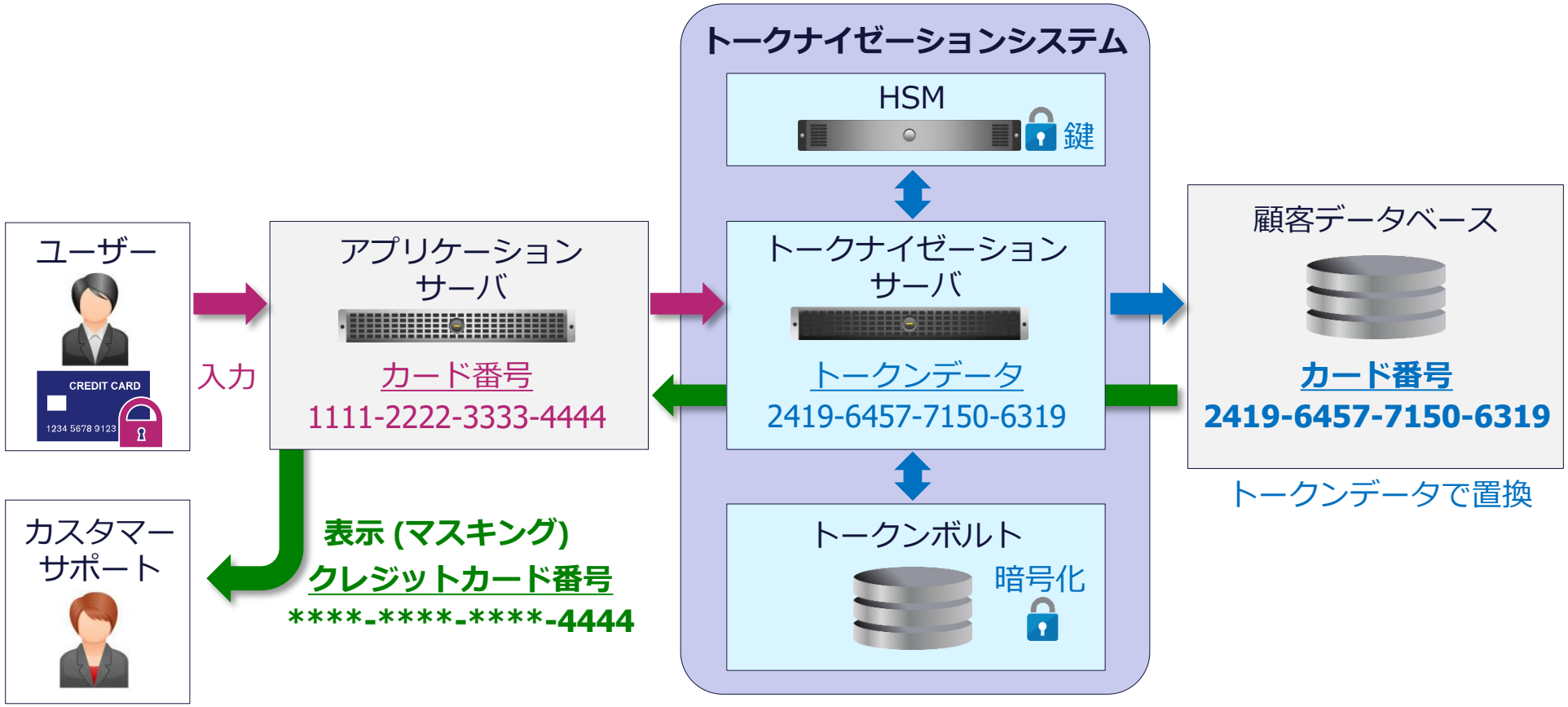
→

氏名	カード番号
鈴木	****- ****- ****-4444

・ユーザー別に表示内容を変更可能
・マスクデータからの復号は不可

一般的なトークナイゼーションの仕組み

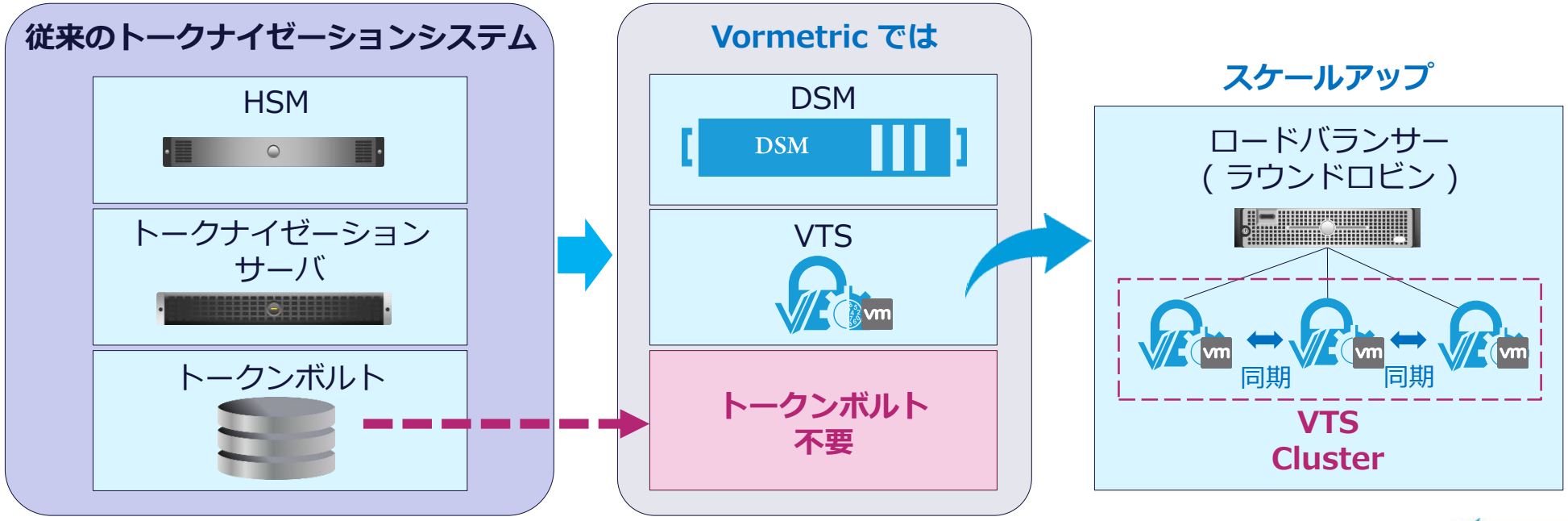
・指定されたデータをトークンデータで置き換え。
・既存のデータベースには置き換えられたトークンデータが保管される。
・原本データは暗号化されトークンボルトと呼ばれるデータベースに暗号化保存される。
・データの呼び出し時にマスキング機能を用いることもできる。



Vormetricトークナイゼーション (VTS) の特徴

(1) ボルトレス
・トークンボルトは不要。
・トークンボルト削減によるコスト削減・運用負荷の低減。
(PANなどの原本データやトークンデータはVTS内部には保管されない。)

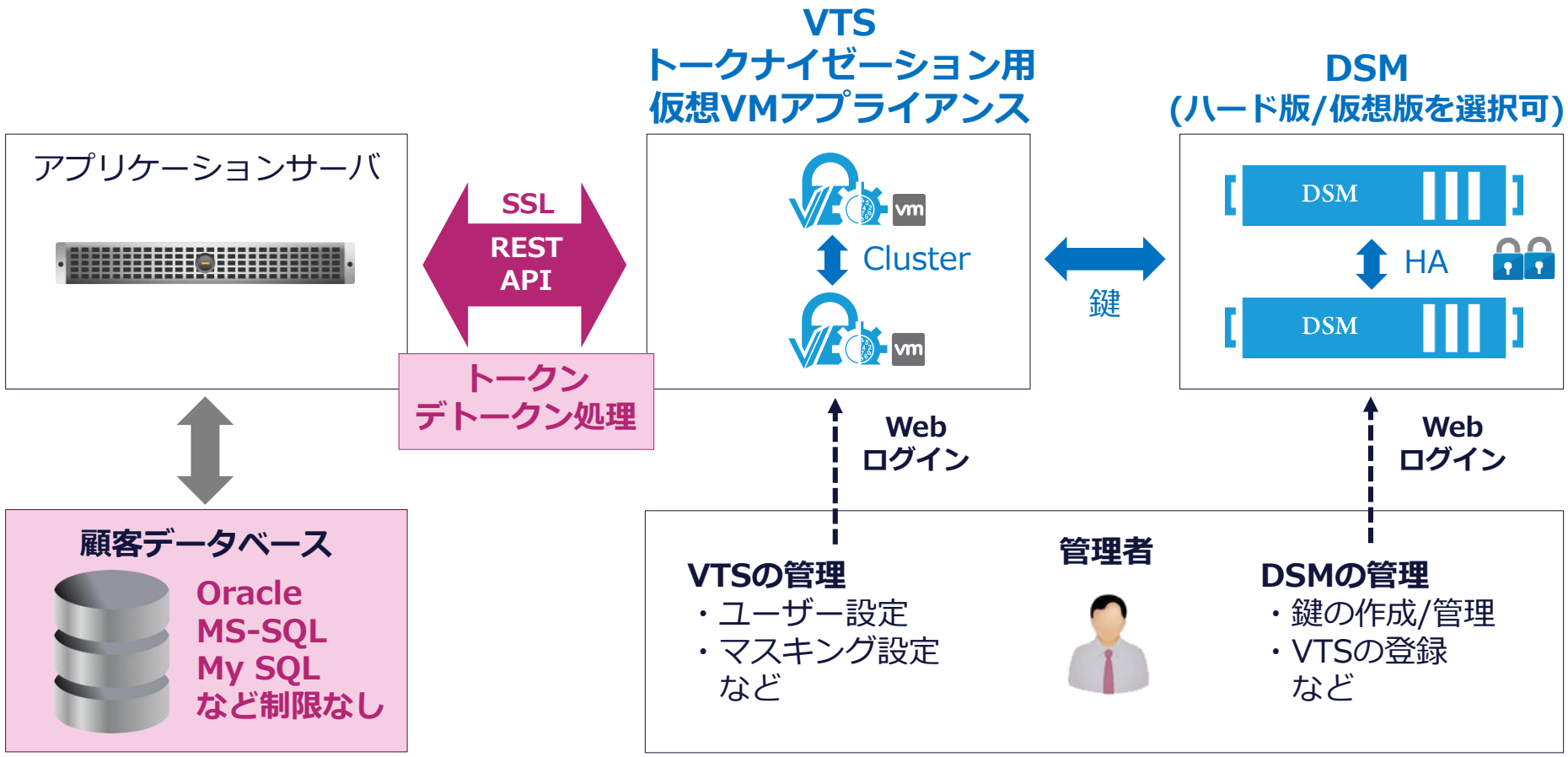
(2) パフォーマンス / 高可用性
・ボルトレスにより高パフォーマンスを提供。
・ロードバランサーとの連携で容易にスケールアップ、高可用性の構築が可能。
(稼働中のVTS Clusterへ新規VTSを追加するだけ。)



Vormetricトークナイゼーション (VTS) の特徴

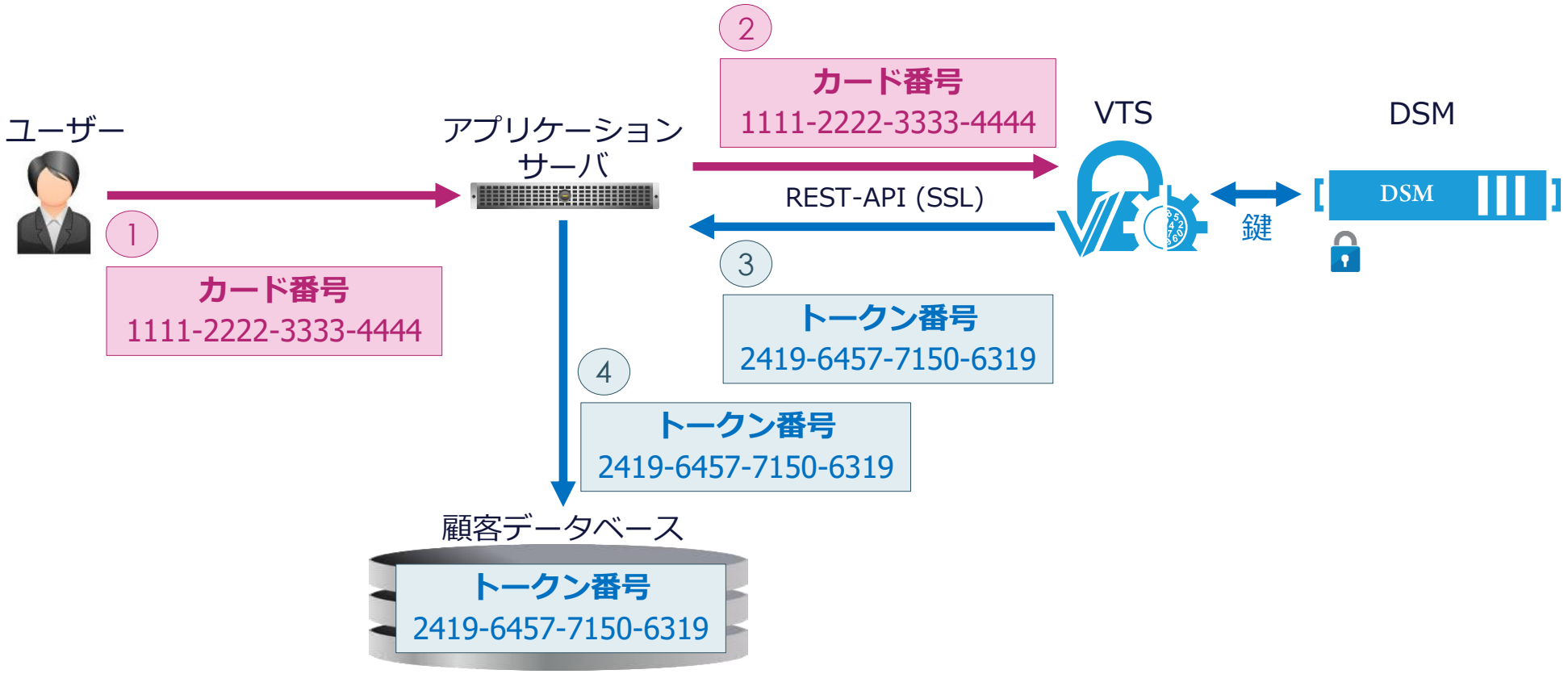
(3) 汎用性

・使用するデータベースの種類は問わない。
・REST-APIを用いた容易な組み込み。



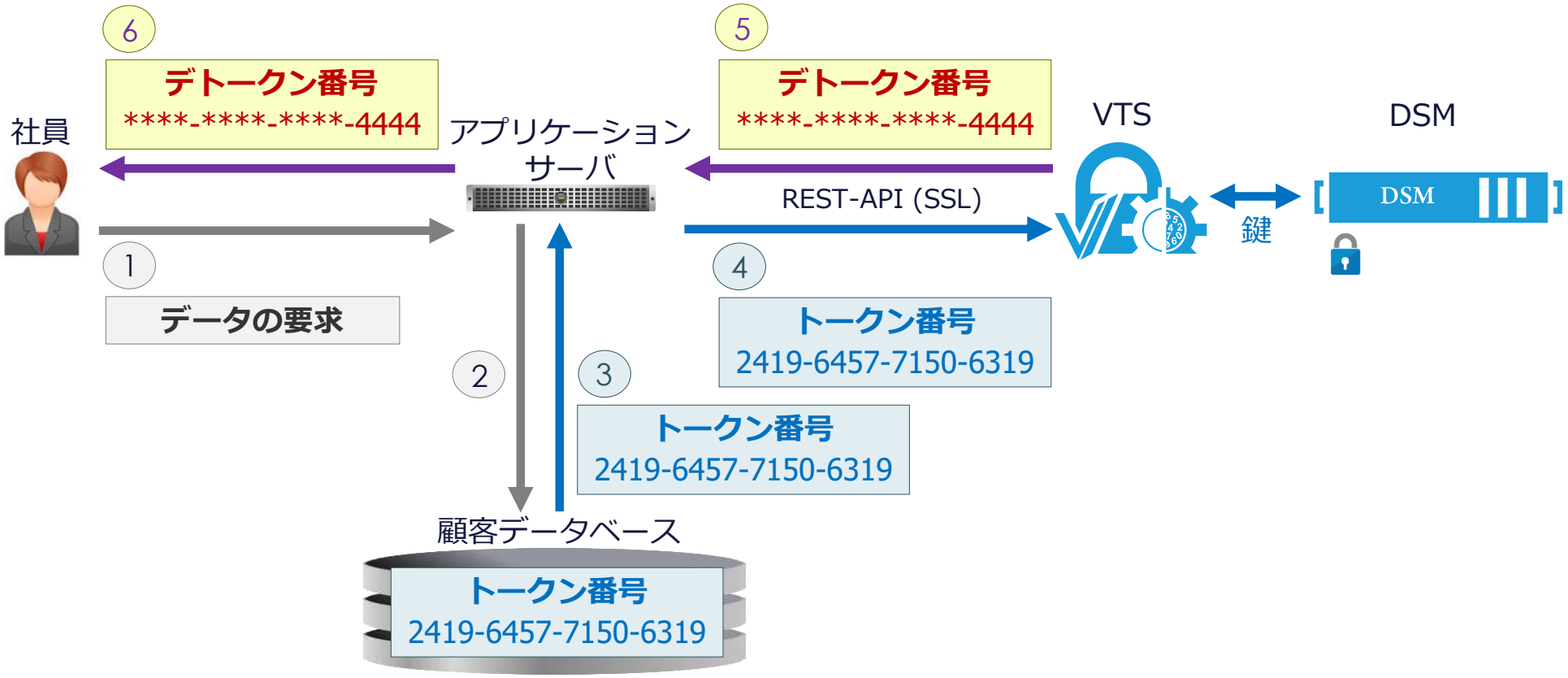
VTSによるトークナイズ

■トークナイズのワークフロー例



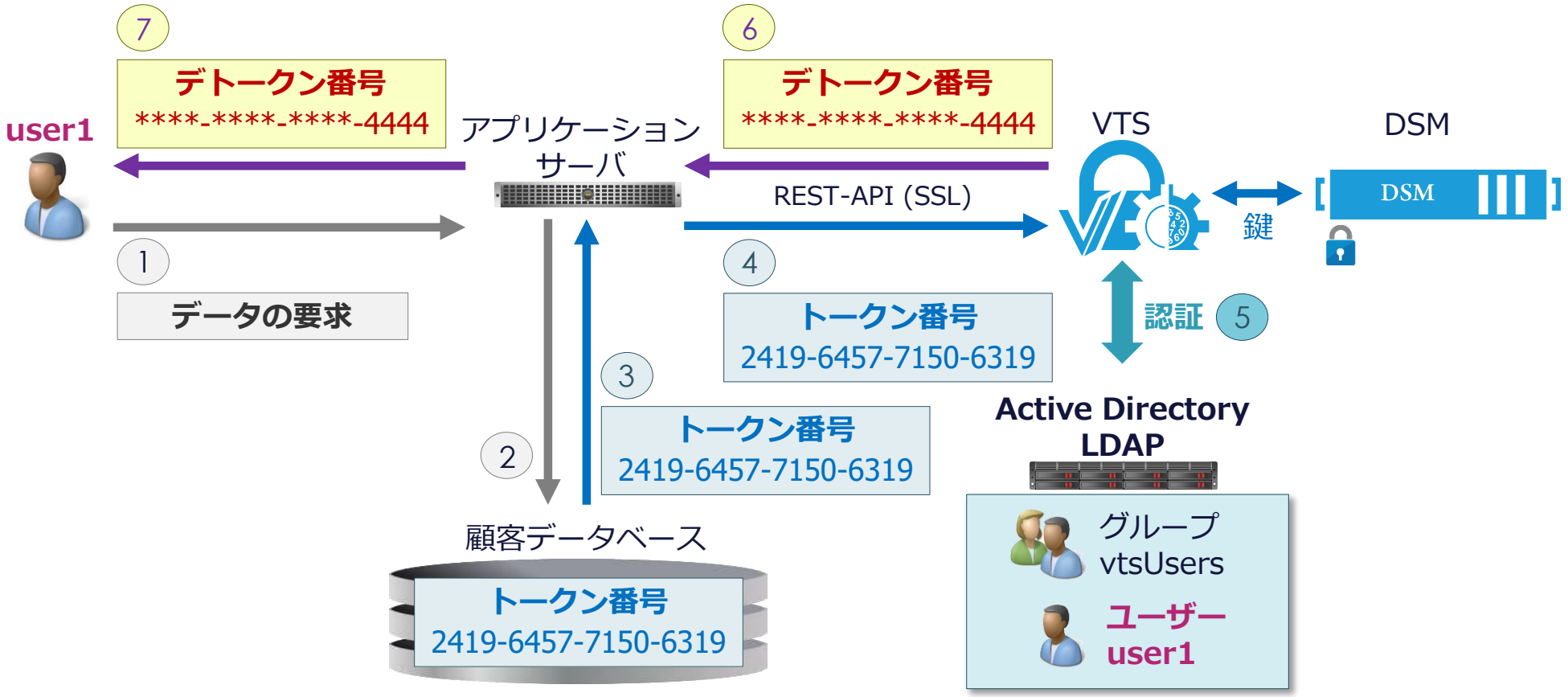
VTSによるデトークナイズ (復号)

■デトークナイズのワークフロー例



ユーザー認証

■2つのユーザー認証に対応
・VTSローカルユーザー認証。
・Active Directory/LDAPユーザー認証。



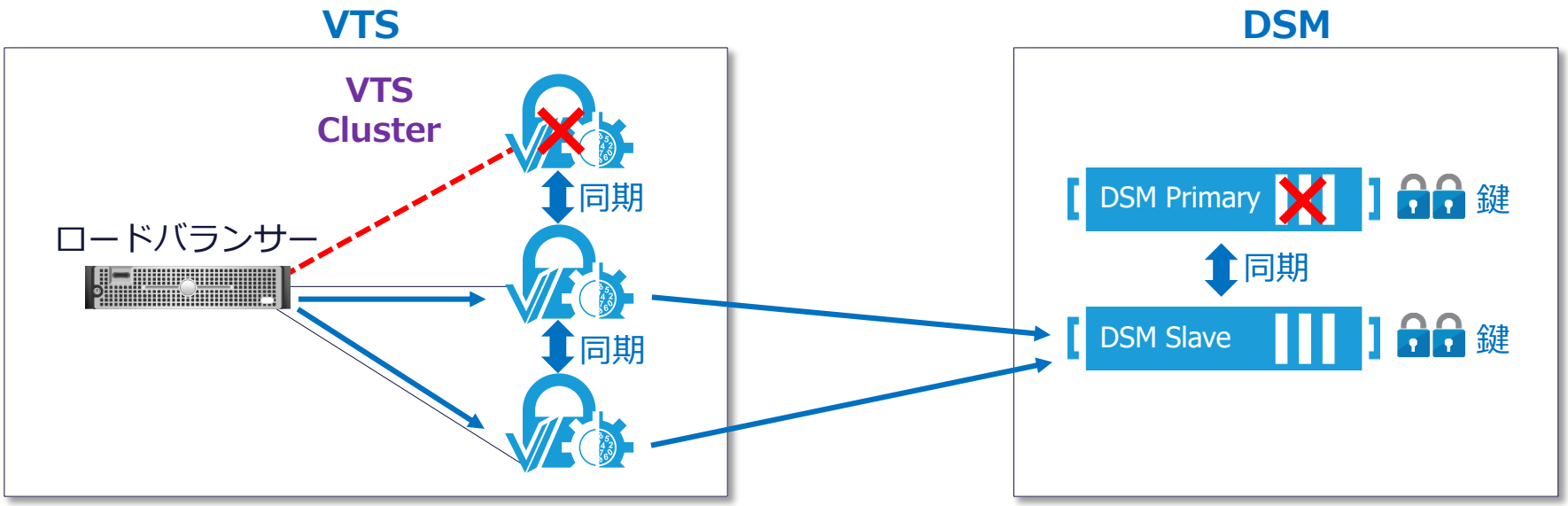
可用性

■トークナイゼーション(VTS)の可用性

・Cluster(Active-Active)構成による設定情報の同期。
・ロードバランサーを用いたVTS障害時の継続稼働。

■鍵の可用性

・DSM HA機能によるSlave DSMへの複製(鍵を含む全情報)。
・Primary DSMに障害時はSlave DSMの鍵を使用。
・Primary DSM復旧時はPrimary DSMに対して鍵通信を再開。



Vormetric
A Thales company

データベースの対策例

Vormetricのデータベースに対する不正対策は？

■Vormetricではどのような対策が可能か？

(1) 見せない
・トークナイゼーションで原本データを変換。
・デトークン(復号)時におけるマスキング。

(2) 盗ませない
・データベースファイルを透過暗号。
・Exportデータを透過暗号。
・データベースの実行ファイルを透過暗号。
・ftpなどのデータ転送を無効化。

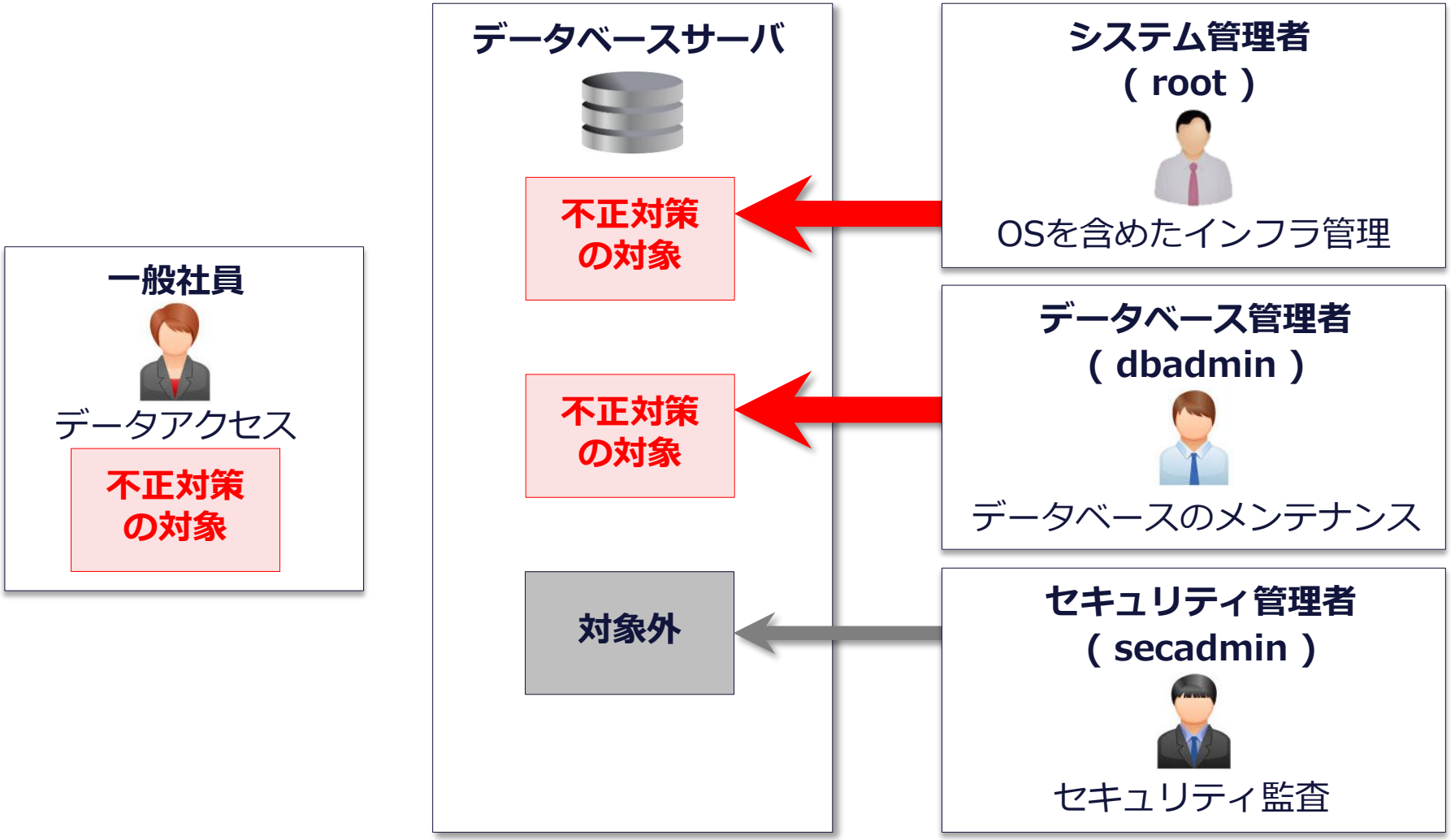
(3) 権限を悪用させない
・システム管理者による「鍵の悪用」を禁止。

今回の対策例で用いる製品群

トークナイゼーション　　透過暗号

データベースに対する不正対策

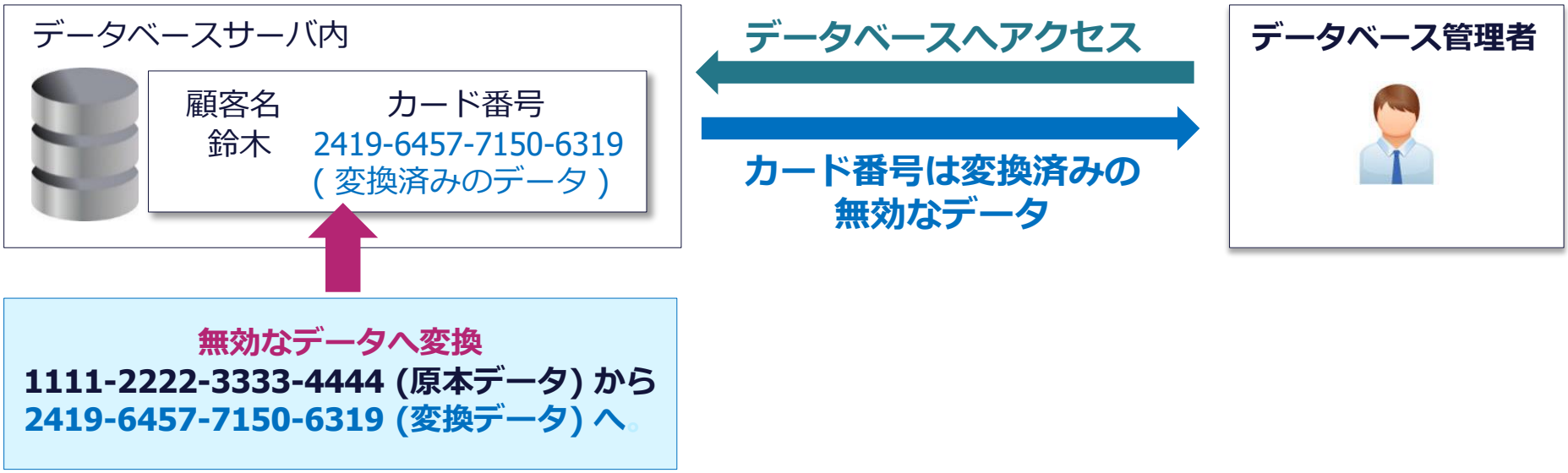
■不正対策の対象者(例)



データベース管理者に対する対策

■データベース内のデータを無効化（ トークナイズ ）

見せない



トークナイゼーションを用いることで

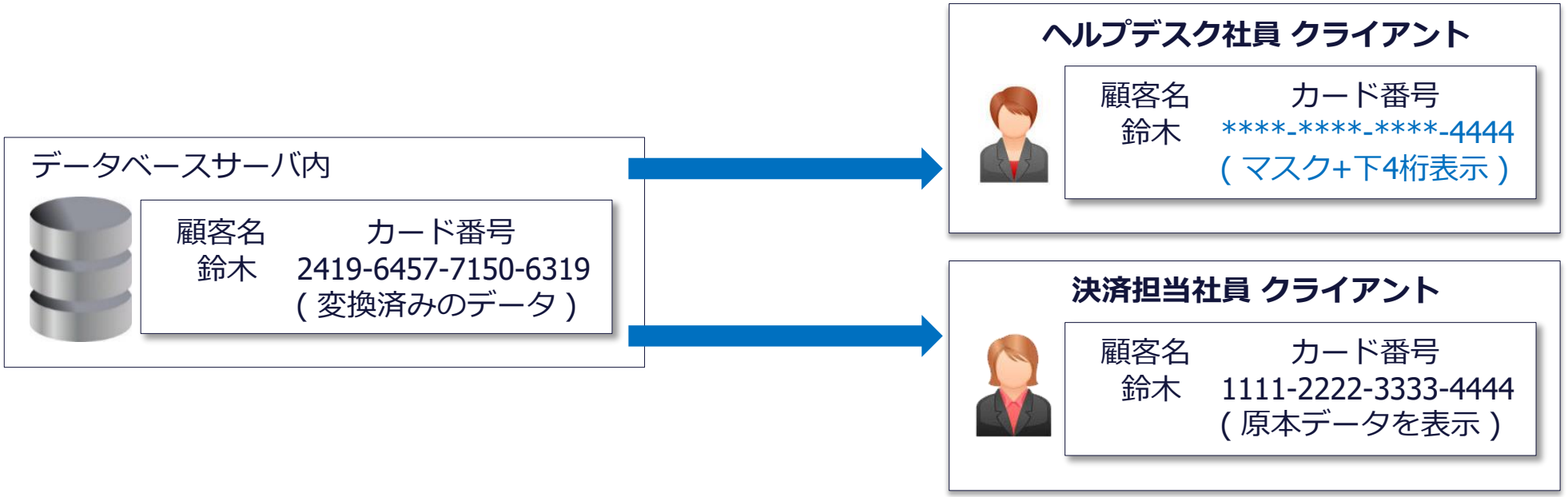
・データベースへ保存されるデータは変換後のランダムデータ。

例えデータベース管理者がデータを盗んでもカード番号は原本データではない。

一般社員に対する対策

■表示データを無効化（デトークナイズ）

見せない



トークナイゼーションのマスキング機能を用いることで

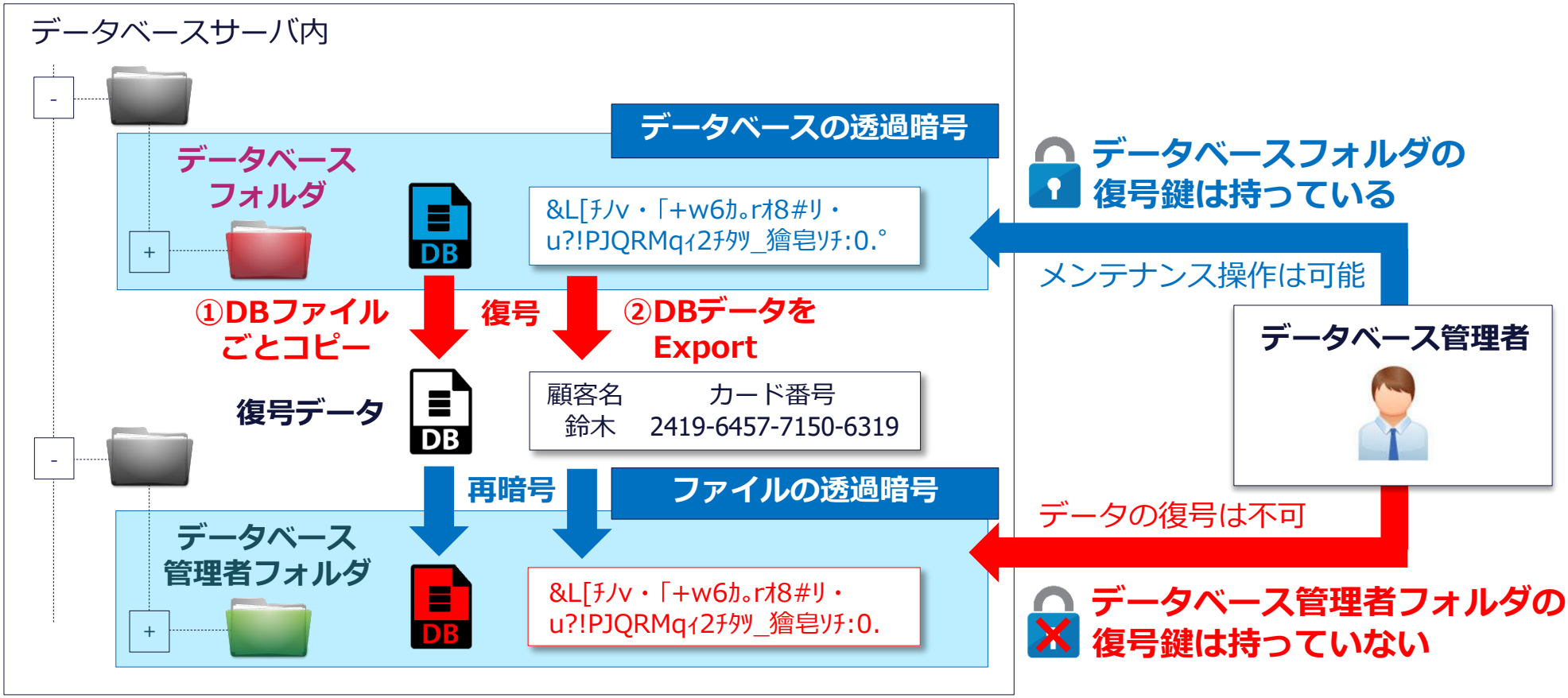
・原本データの表示が不必要な社員へはマスキングや下4桁のみ表示などの制御が可能。
・ユーザー/グループ単位でのマスキング設定が可能。

一般社員による機密データ/個人情報の持ち出しを対策。
（表示データの印刷やスマートフォンなどによる画面の写真撮影に対しても有効）

データベース管理者に対する対策

■データベースの透過暗号 + ファイルの透過暗号

盗ませない



データの盗難対策

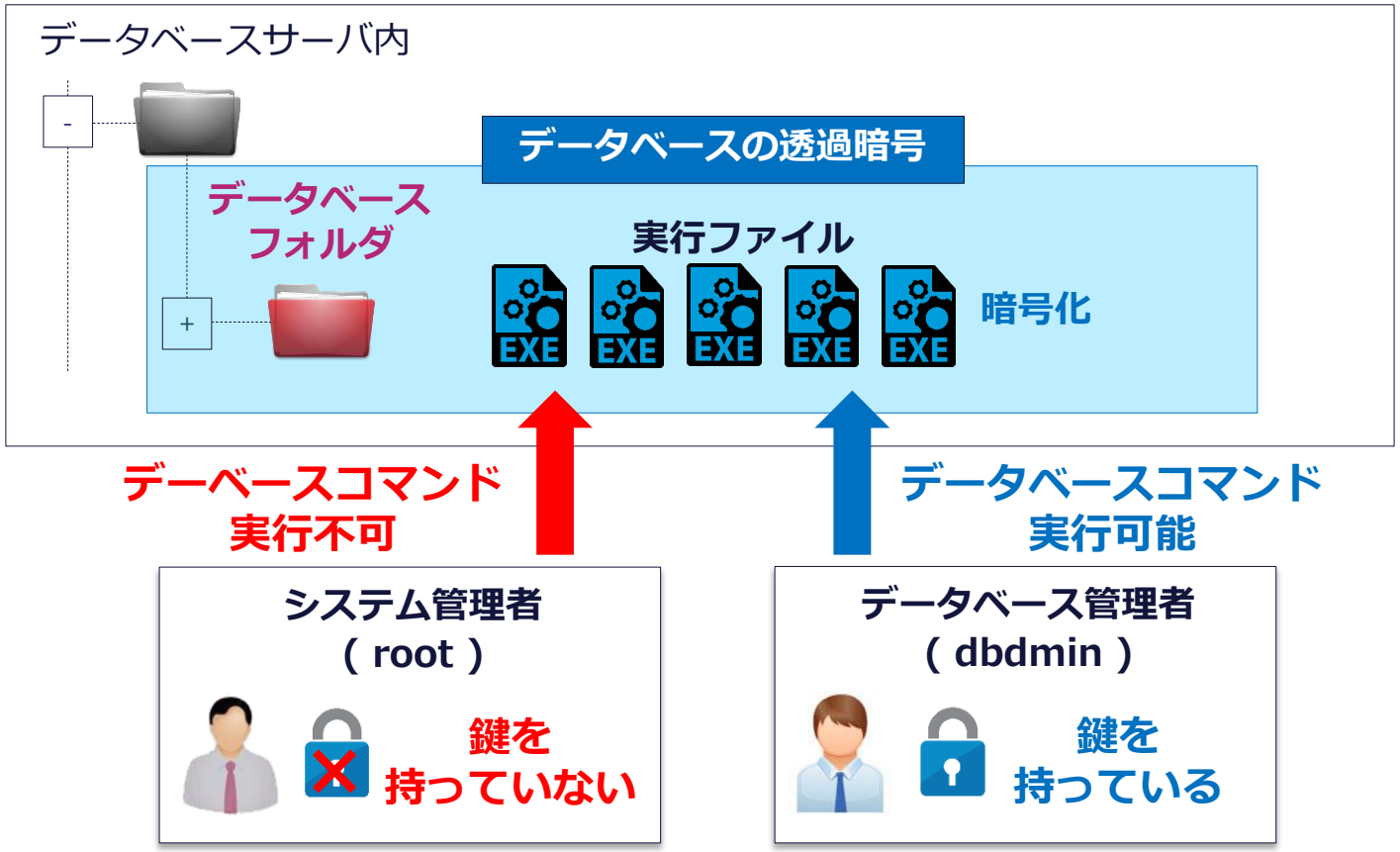
- 抽出データの書き込み時にファイルの透過暗号を用いて再暗号化、但し復号鍵は与えない。
- ①データベースファイルのコピー や ②データのExport(抽出) によるデータは復号不可。

Vormetric A Thales company

システム管理者に対する対策

■実行ファイルを無効化

盗ませない



システム管理者(root) には使わせない

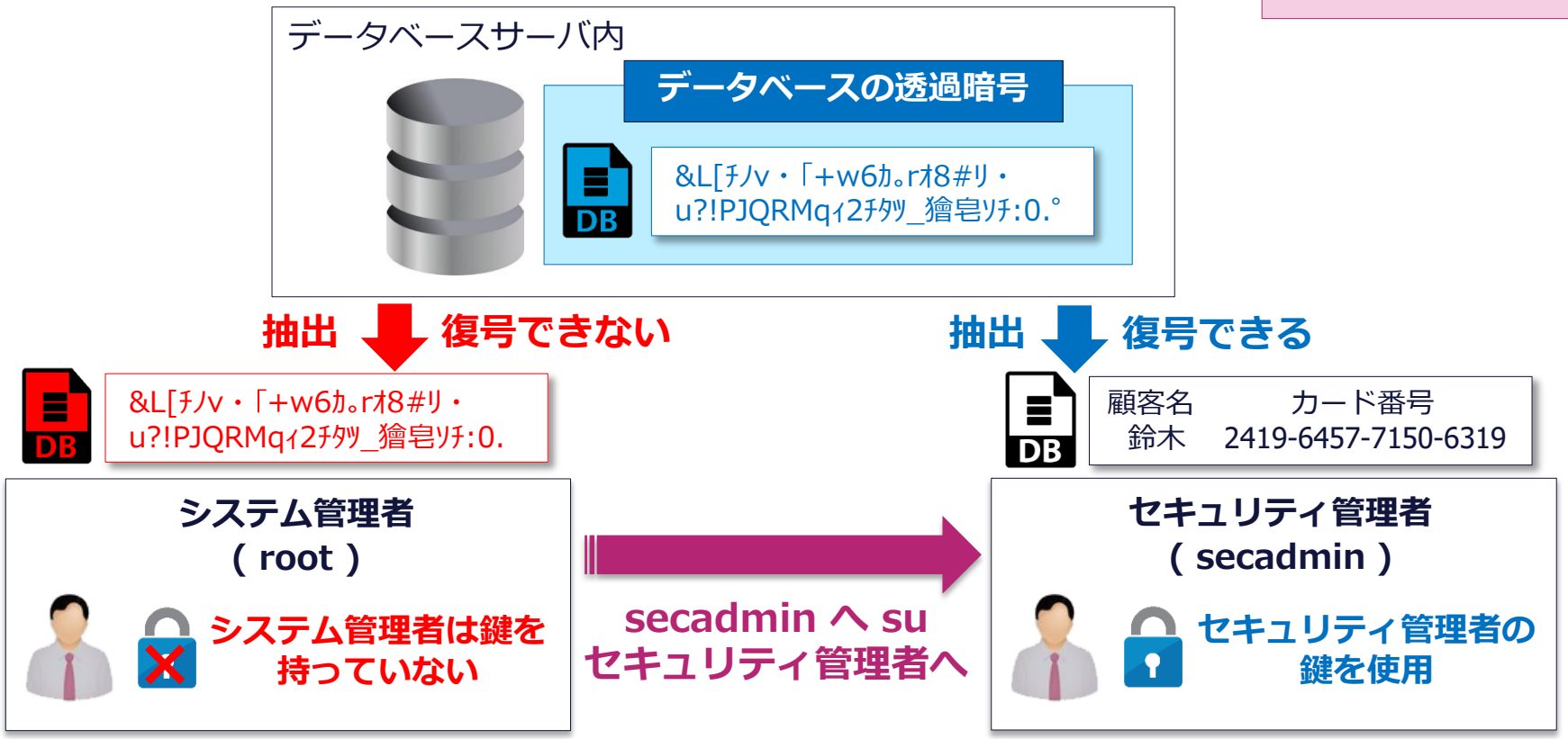
・実行ファイルは暗号化済。

・鍵を持たないシステム管理者はデータベースのコマンド類を実行することはできない。

システム管理者への対策

■対策前「なりすまし」例

対策前



システム管理者(root) によるデータの盗難

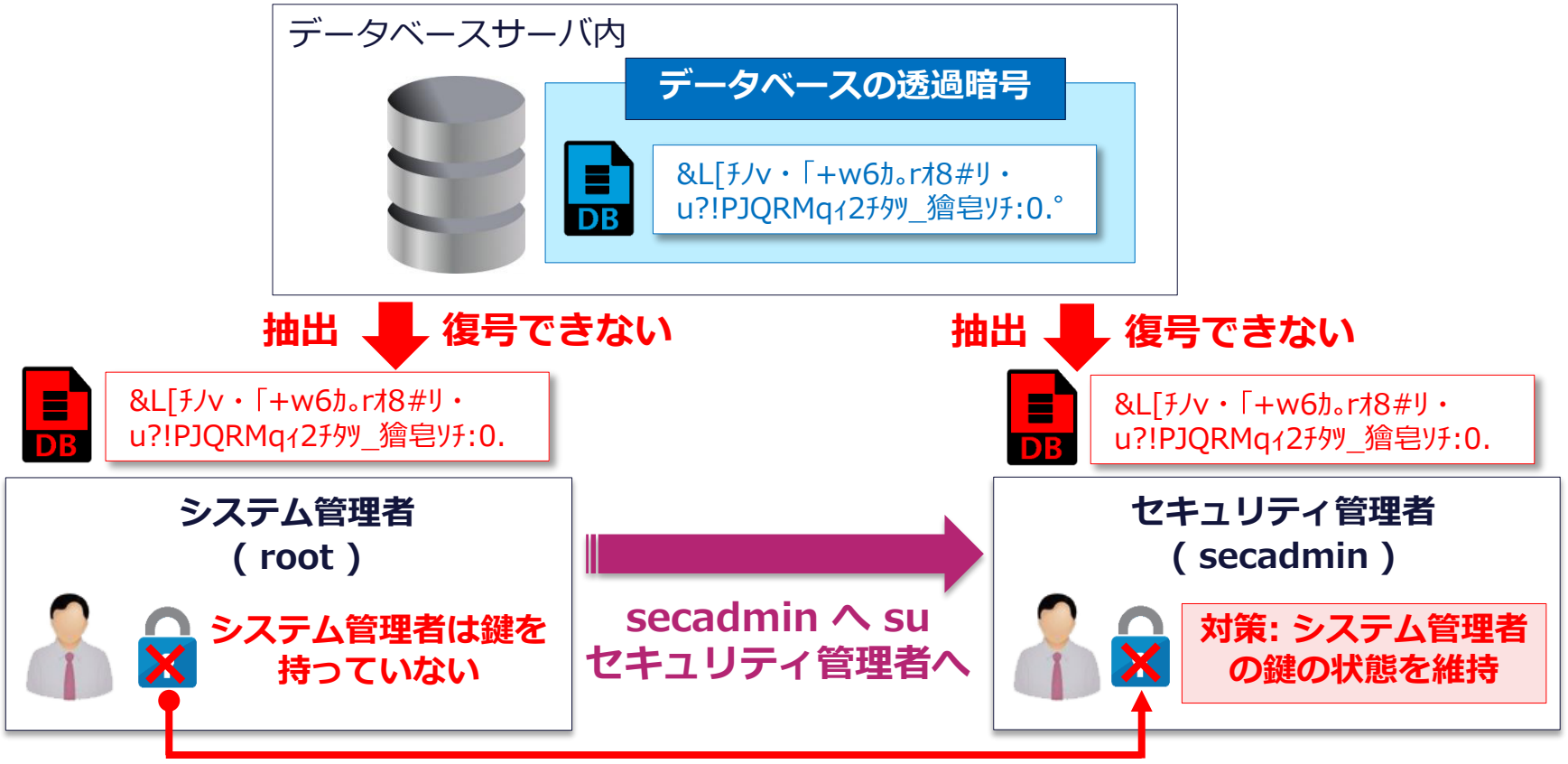
・システム管理者(root)は鍵を所有していない。

・但し “su” を実行し鍵を持つセキュリティ管理者(secadmin)としてデータを盗めてしまう。

システム管理者への対策

■対策後「なりすまし」を禁止

権限を悪用させない



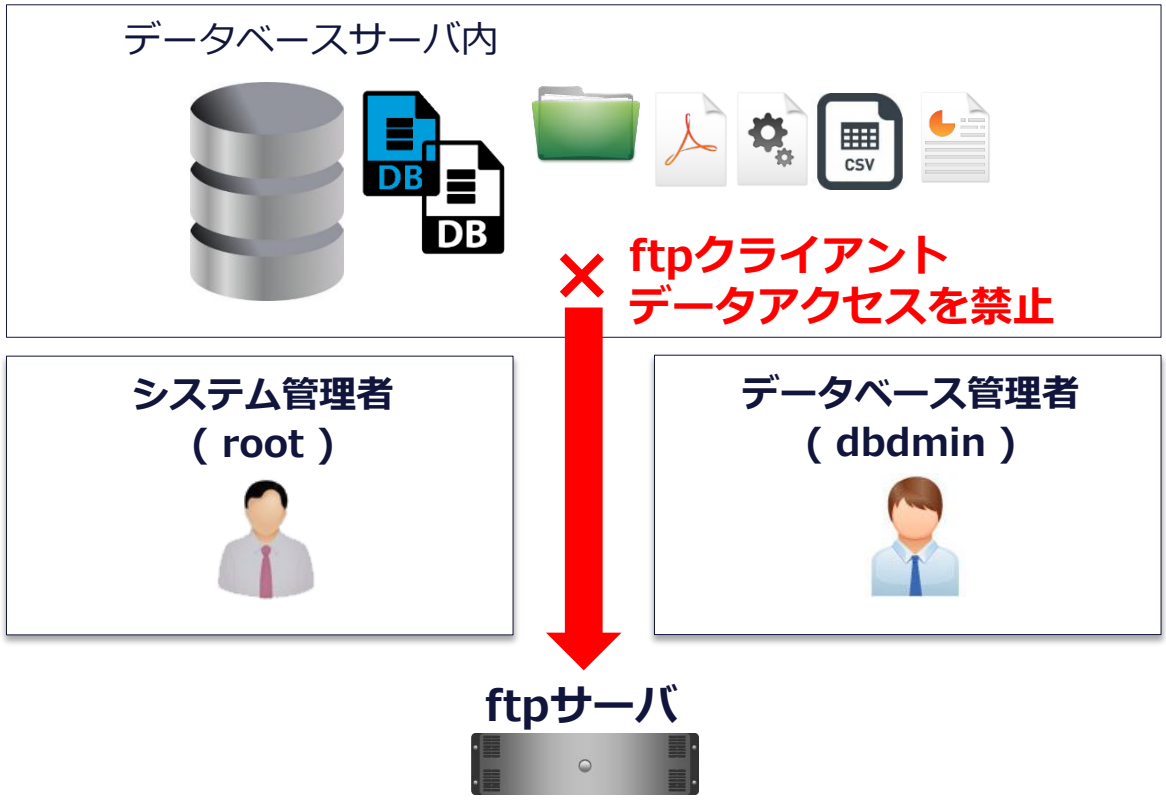
Vormetric の「なりすまし」対策

・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ため鍵の悪用を禁止できる。

システム管理者 / データベース管理者に対する対策

■アクセス制御

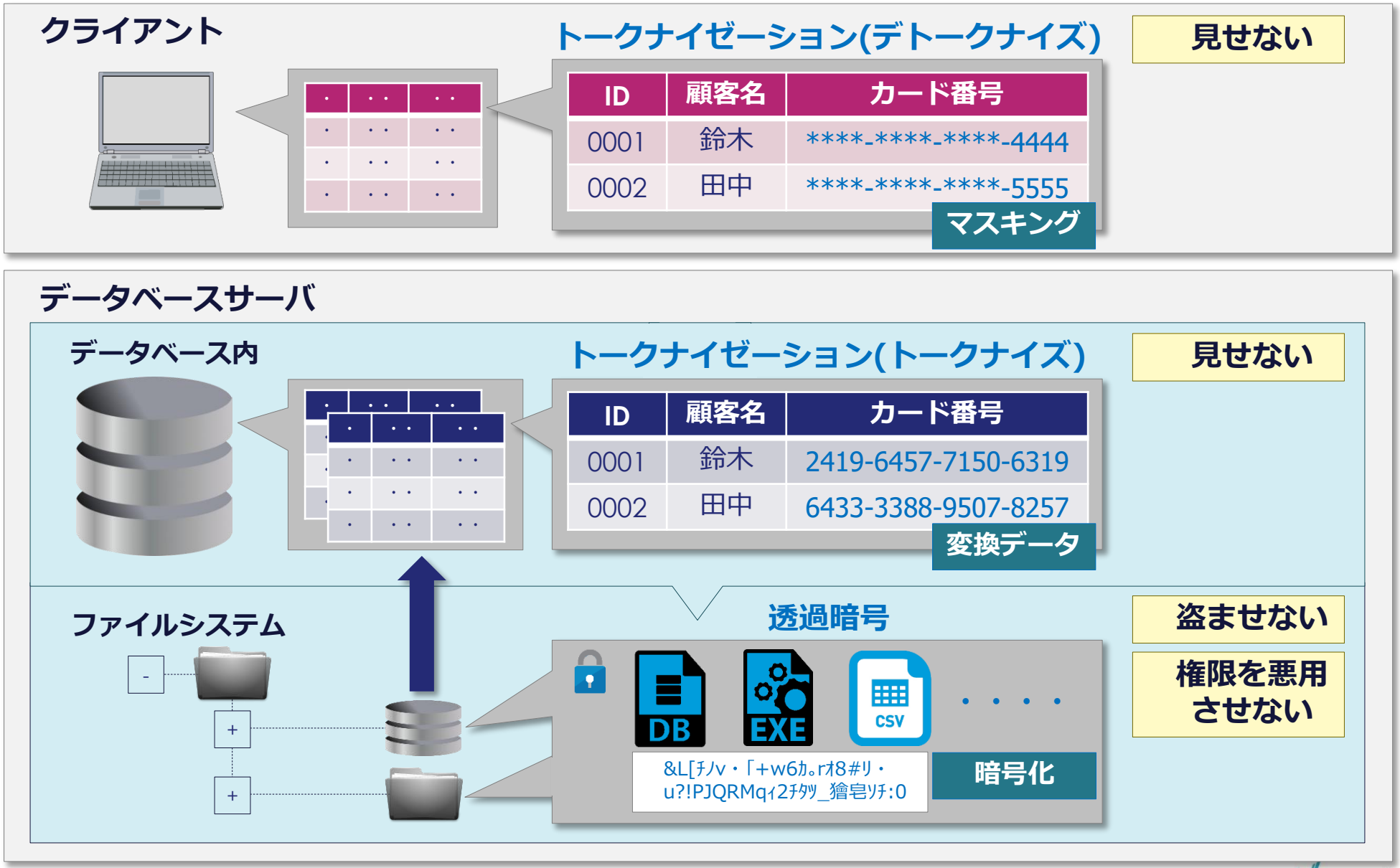
盗ませない



データ転送を禁止

・アクセス制御機能を用いてftpクライアントのデータアクセスを制御。
・例えば、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させることが可能。

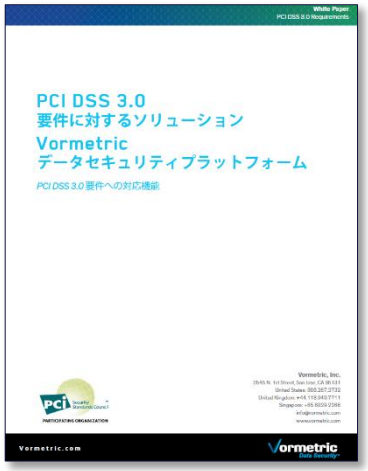
まとめ (トークナイゼーション+透過暗号で機密データを保護)



PCIDSS3.0 への適用

PCIDSS 要件	内 容	Vormetric の対応項目
2	システムパスワードおよび他のセキュリティパラメータにベンダ提供のデフォルト値を使用しない	2
3	保存されるカード会員データを保護する	3.3 / 3.4 / 3.4.1 / 3.5 / 3.6
4	オープンな公共ネットワーク経由でカード会員データを伝送する場合、暗号化する	4.1
7	カード会員データへのアクセスを、業務上必要な範囲内に制限する	7.1 / 7.1.1 / 7.1.2 / 7.1.3 / 7.1.4 / 7.2
8	システムコンポーネントへのアクセスを確認・許可する	8.2 / 8.2.1 / 8.7
9	カード会員データへの物理アクセスを制限する	9.8.2
10	ネットワークリソースおよびカード会員データへのすべてのアクセスを追跡および監視する	10.1 / 10.2 / 10.3 / 10.4.1 / 10.5 / 10.6

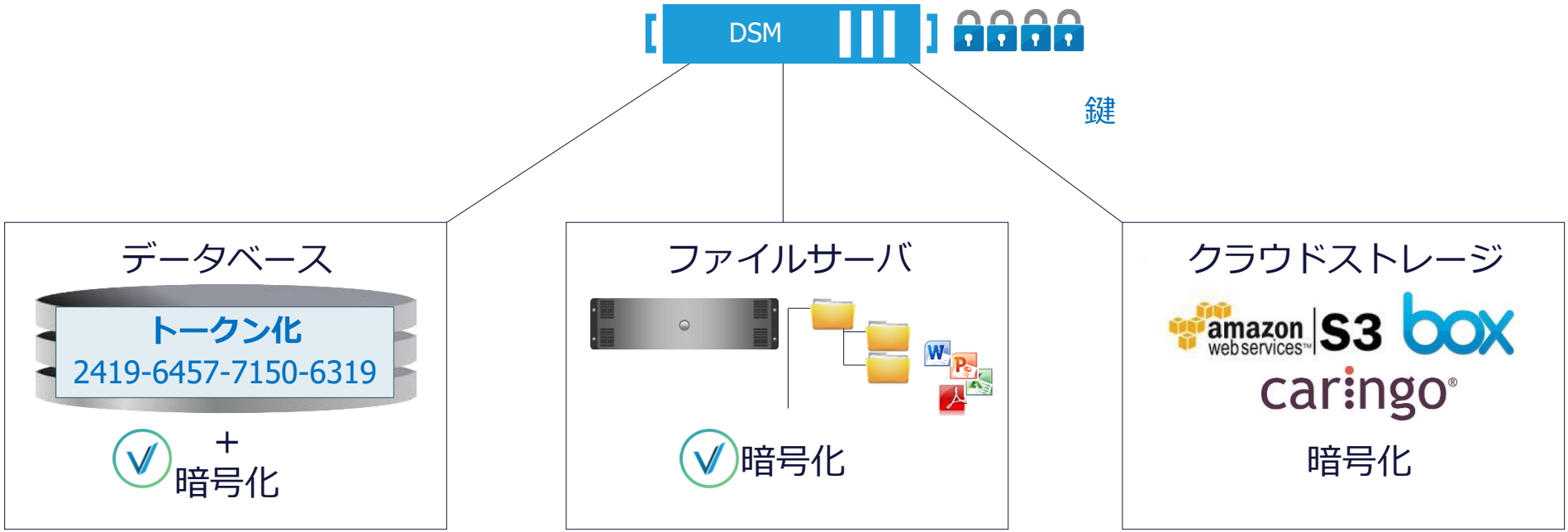
詳細な内容は以下よりダウンロードできます。
http://www.vormetric.co.jp/resources/
PCI DSS 3.0 ホワイトペーパー (日本語)



Vormetricでさらにセキュアに

■ **保護対象を拡張**

・ファイルサーバやクラウドに対しても透過的に暗号化を適用可能。
・鍵やポリシーはDSMで一元管理。



Thank you

http://www.vormetric.co.jp

Vormetric
A Thales company