コストダウンにつながる
クレジットカード番号を秘匿化する手段

2016年6月22日

株式会社MONET
代表取締役　前野 泰章

株式会社MONET　会社概要

社名	株式会社MONET（モネット）
所在地	〒101-0032　東京都千代田区岩本町2-16-5　TUCビル7F
設立	2002年12月
代表取締役	前野　泰章
パートナー覧	■販売パートナー 株式会社富士通ソーシアルサイエンスラボラトリ、株式会社日立ソリューションズ、株式会社ブライセン、日本情報システム株式会社、株式会社システム・ケイ、イアス株式会社、株式会社CMC Solutions、株式会社北斗システムジャパン、株式会社シティリバース ■RTPatch Embedded販売パートナー 株式会社日新システムズ、アイティアクセス株式会社、FORI I Inc. ■ソリューションパートナー タレスジャパン株式会社、アイベクス株式会社、株式会社ソフトエイジェンシー、株式会社セキュアブレイン ■コンサルティングパートナー グローバルセキュリティエキスパート株式会社 株式会社エムキュービック
主要取引実績	アイティアクセス株式会社、株式会社QUICK、クラリオン株式会社、ソフトバンク株式会社、株式会社東芝、東北インフォメーション・システムズ株式会社、株式会社セキュアブレイン、特種東海製紙株式会社、トレジャーデータ株式会社、株式会社日新システムズ、日本情報システム株式会社、パイオニア株式会社、パナソニック　システムネットワークス株式会社、株式会社日立システムズ、株式会社日立ソリューションズ、株式会社日立製作所、株式会社富士通ソーシアルサイエンスラボラトリ、防衛省、三菱UFJニコス株式会社、ライフカード株式会社、他　（順不同、敬称略）
参加団体	日本公認不正検査士協会 (ACFE)、Linuxビジネスイニシアチブ、日本カード情報セキュリティ協議会(JCDSC)

経済産業省の実行計画

経済産業省からクレジットカード取引における
セキュリティ対策の強化に向けた「実行計画」

ECサイトなどの非対面取引の場合（2018年3月まで）
対面取引の場合（2020年3月まで）

① クレジットカード番号の非保持化

or

② PCIDSSの準拠

重要データの保護手段

- **暗号化**
  - 重要データを、決まった規則（アルゴリズム）に従ってデータを変換する手法
    （第三者に盗み見られたり改ざんされない）

意味不明な文字列に変換

0123456789 ⇒ =opkm34tlZi1sd_xkzpa,sZXmWQ・・・・・

- **データ・トークナイゼーション**
  - 重要データを、形式を保持したまま**意味をなさない**別のデータ（トークン）に変換する手法

フェイク(fake)の文字列に置き換え

0123456789 ⇒ 2980314657

データ・トークナイゼーションの導入理由とターゲット

重要データ（例：クレジットカード番号）を別の文字列に置き換えて処理することで、実データ自体の漏洩を防御

【導入理由】

- 個人情報漏えい対策 (PII)
- 医療情報 (HIPPA)
- マイナンバー対策
- PCI DSS (Payment Card Industry Data Security Standard) → カード決済情報

セキュリティ強化

トークン化の導入により、監査の対象外になる

※該当システムが実データ自体を持たなくなる為

- PCIDSS要件3： 保存されるカード会員データの保護
  - 3.4 全ての保存場所でPANを読み取り不能にする

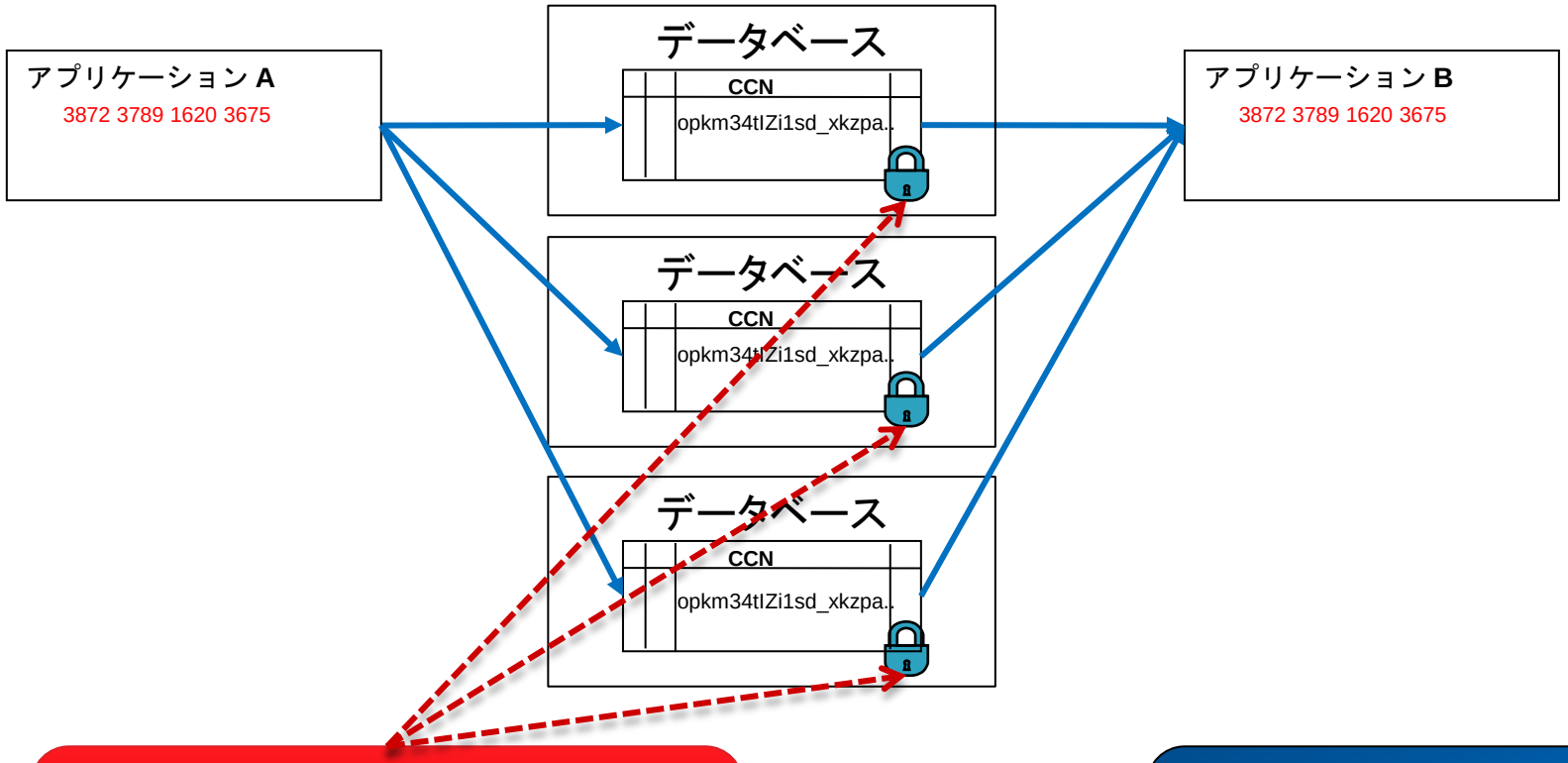
コストダウン（監査費用の削減）

【ターゲット】

- 金融 （銀行、証券会社、カード決済会社 etc.）
- 流通 （小売店、ネット販売 etc.）
- 旅行関連 （ホテル、エアーライン、旅行代理店 etc.）

一般的な暗号化とトークン化の処理位置

【暗号化】

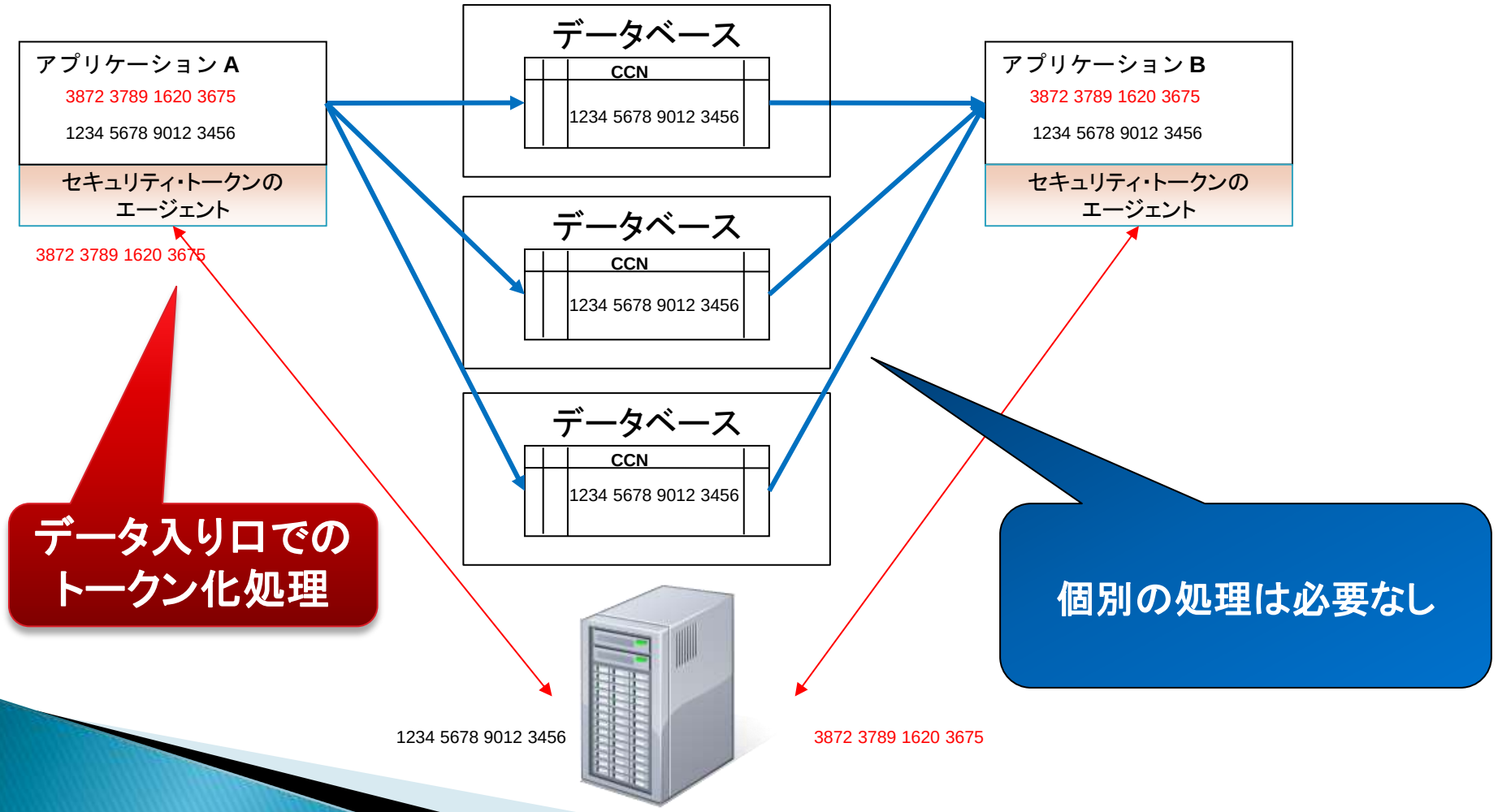


データベース/システム毎に<u>個別に</u>暗号化処理が必用

全てのデータベース/システムが暗号化機能を持っているとは限らない

一般的な暗号化とトークン化の処理位置

【トークン化】



データ・トークナイゼーションの手法

- 従来型のデータ・トークナイゼーション
  - ✓ダイナミック・モデル　（2000年頃の技術）
    - ✓ 元データを全て保管

    元データが来る毎に、トークンテーブルを参照して、登録済でなければ、新規にトークンデータを動的に生成して、登録済トークンテーブルに重複が無いか確認してトークンデータを返す。既に登録済であれば、該当のトークンデータを返す。

  - ✓事前生成型モデル　（2005年頃の技術）
    - ✓ 同じパターンのトークン化テーブルを事前に用意

    ありえる全パターンを網羅するトークン化テーブルを事前に生成
    （例えば、10億通りのクレジットカード番号があり得る場合は、10億に1対1に対応し、かつ、重複がないトークンテーブルを事前に生成する）

- 次世代型トークン
  - ✓ブロック化＋事前生成トークン化

    （Protegrity Vaultless Tokenization）

    小規模な事前生成型のトークンテーブルを複数用意して、AESなどのブロック暗号の内部で使用されるデータ置換えのロジックと複数のトークンテーブルを組み合わせることで、事前生成型の欠点を克服し、高速性、小リソース、容易なレプリケーション性、さらに高度な安全性も実現

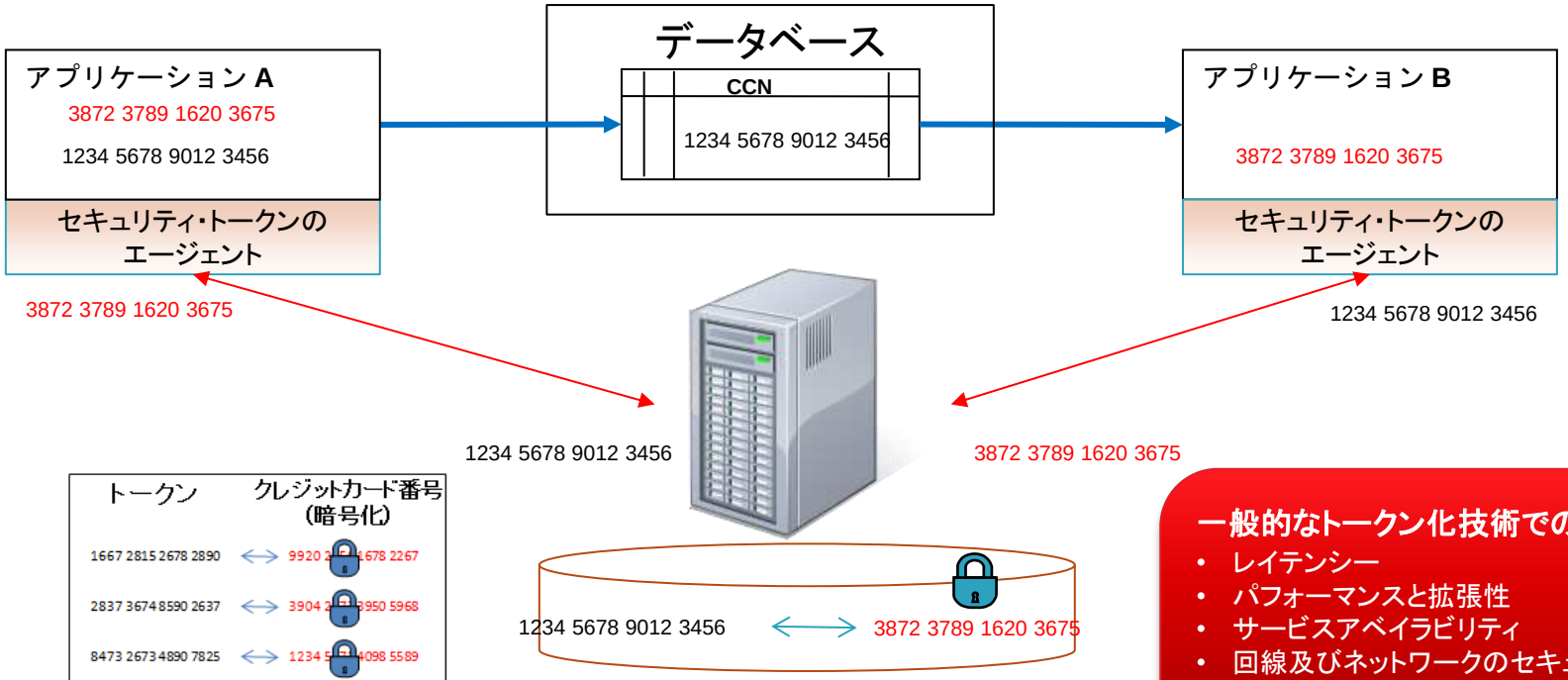
従来型データ・トークナイゼーションの問題点

- ●冗長化が困難
- ●負荷分散が困難
- ●リカバリの問題
- ●パフォーマンスの限界

- データ処理に限界
- クレジットカードのようなトランザクションに耐えられない

- ●拡張性が乏しい
  - ●複数拠点での運用が難しい
    （同期が困難なため、複数拠点での併用が非現実的）

従来型データ・トークナイゼーションとは



一般的なセキュリティ・トークン
(Vault-based Tokenization)

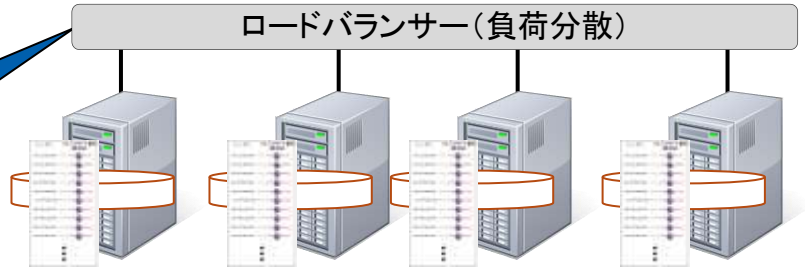
ダイナミック・モデル（動的型）
事前生成型モデル

データ量に応じた量のユニークなトークンが必要
→ 莫大なフットプリント

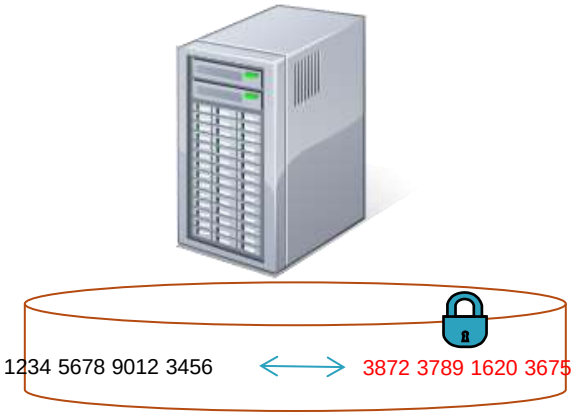
一般的なトークン化技術での懸念事項

- レイテンシー
- パフォーマンスと拡張性
- サービスアベイラビリティ
- 回線及びネットワークのセキュリティ
- トークン化サーバへのアクセス制御
- トークン化サーバ自体のデータセキュリティ
- トークン化の特性

冗長化が課題
- 負荷分散
- リカバリー
- 拡張性



データ・トークナイゼーション
Protegrity Protection Server のご紹介



一般的なセキュリティ・トークン
(Vault-based Tokenization)

Protegrityデータ・トークナイゼーション

Protegrity トークン化 テクノロジ

－ Vaultless Tokenization （データ蓄積なし）－

元データ（リアルな情報）とトークンデータ（フェイクな情報）の対応データ（Vault-base）を持たない

ブロック化された変換テーブルのみ

（Vaultless トークン技術）

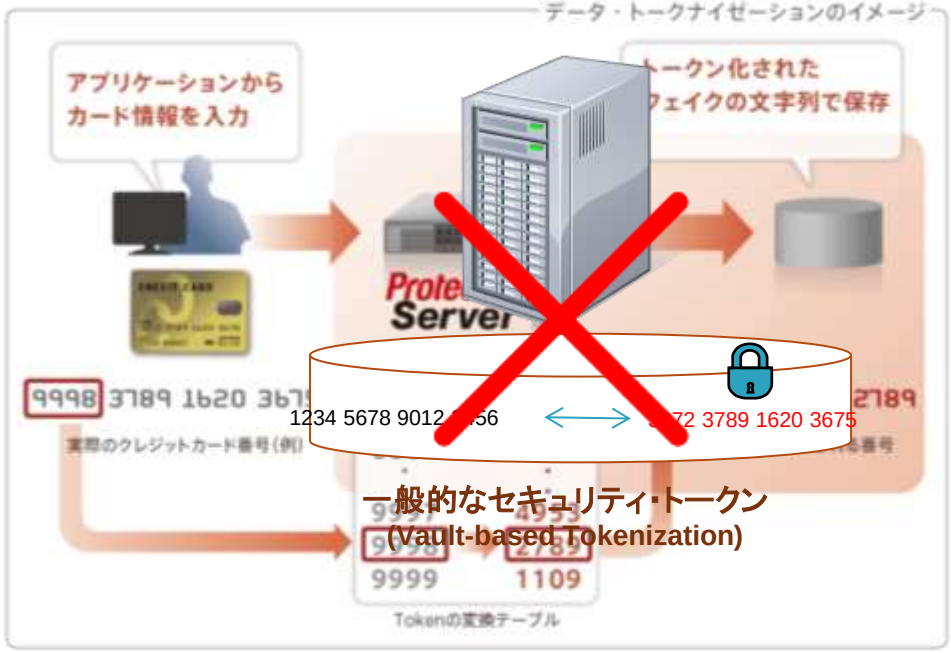
- 拡張性
- 可用性
- 高パフォーマンス

200,000 tokens / 秒を実現

一般的なトークン化のパフォーマンス

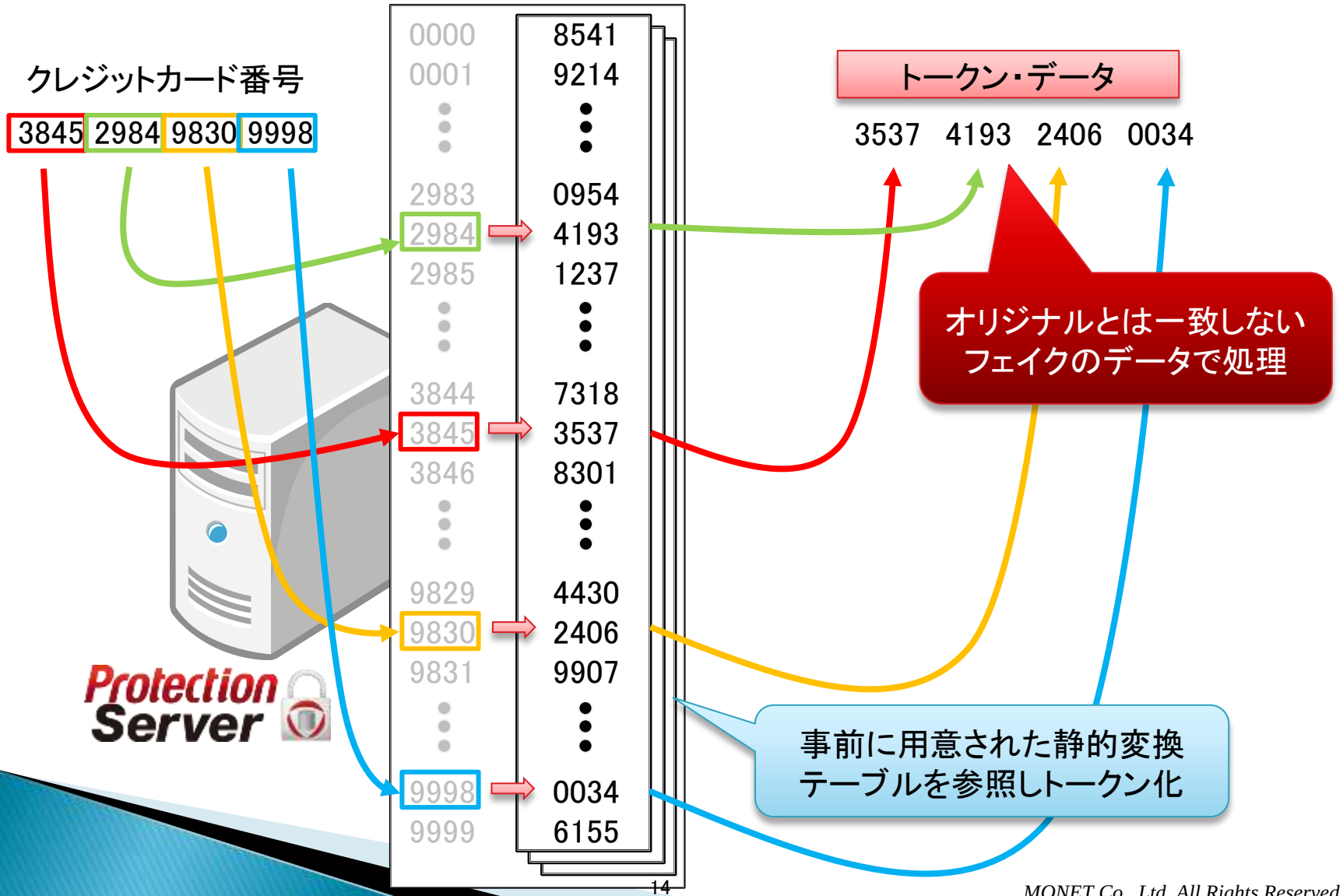
5 tokens / 秒（外部でトークナイゼーション化）

5,000 tokens / 秒（社内でトークナイゼーション化）



Protegrityデータ・トークナイゼーション

– Vaultlessの仕組み –



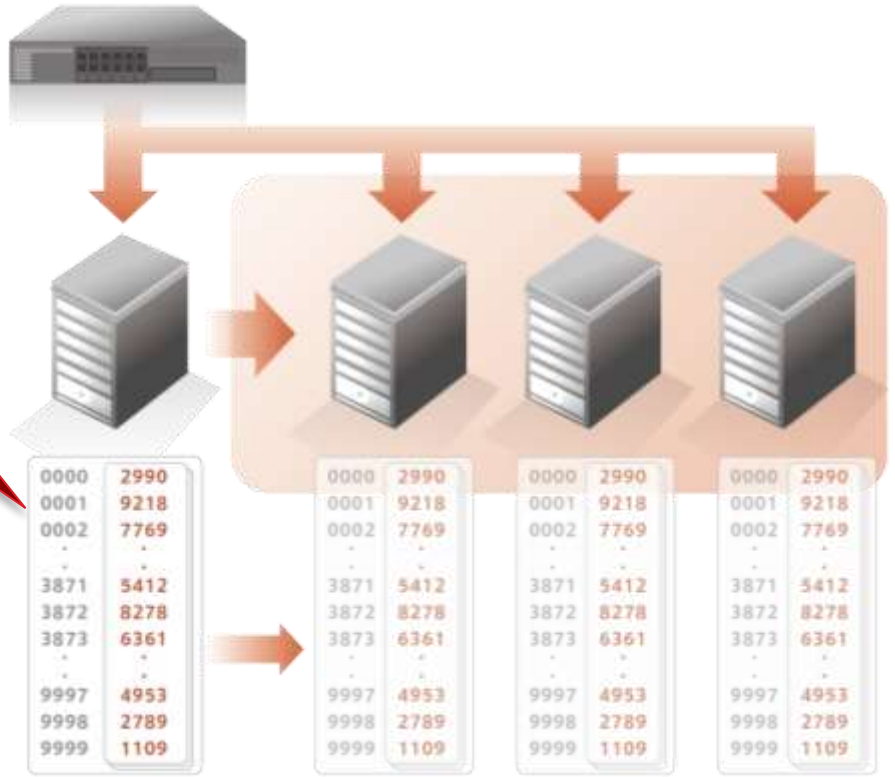
Protegrityデータ・トークナイゼーション
– 拡張性 –

静的変換テーブルをコピーするだけで2台目、3台目の複製が可能です

※導入後の拡張が容易

静的変換テーブルのメリット
- 同期の必要がない
- 静的変換テーブルを事前にコピーすることで拡張が容易
- 障害発生時のレプリケーションが必要ない

※ 静的変換テーブルはAES（256ビット）で暗号化



Protegrityデータ・トークナイゼーション

多様なデータ形式への対応

クレジットカード番号のような数列だけではなく、会員番号などに使用されるアルファベットと数字の組み合わせ・Eメールアドレスなど様々なデータ形式に対応しています。

	元データ	トークンデータ
クレジットカード（数字）	3872 3789 1620 3675	8278 2789 2990 2789
日付（日付）	10/30/1955	12/25/2034
Eメールアドレス（アルファベット＆数字、記号による区分と挿入）	taro@hanako.com	empo@svtien.snk
電話番号（数字+記号による区分と挿入）	03-5809-3188	54-7653-2941
クレジットカード（数字、最終4文字のみ変更なし）	3872 3789 1620 3675	8278 2789 2990 3675
クレジットカード（マスクがけ、最初の6文字は表示）	3872 3789 1620 3675	3872 37## #### ####
Unicode	安全	xM2EcAQ0LVtQ
バイナリーデータ	Protegrity	0xA2EA9C9BC53D77BA7F8E85C124296BF3

Protection Serverとは

トークン化だけでなく、暗号化も含めた以下データセキュリティを実現します。

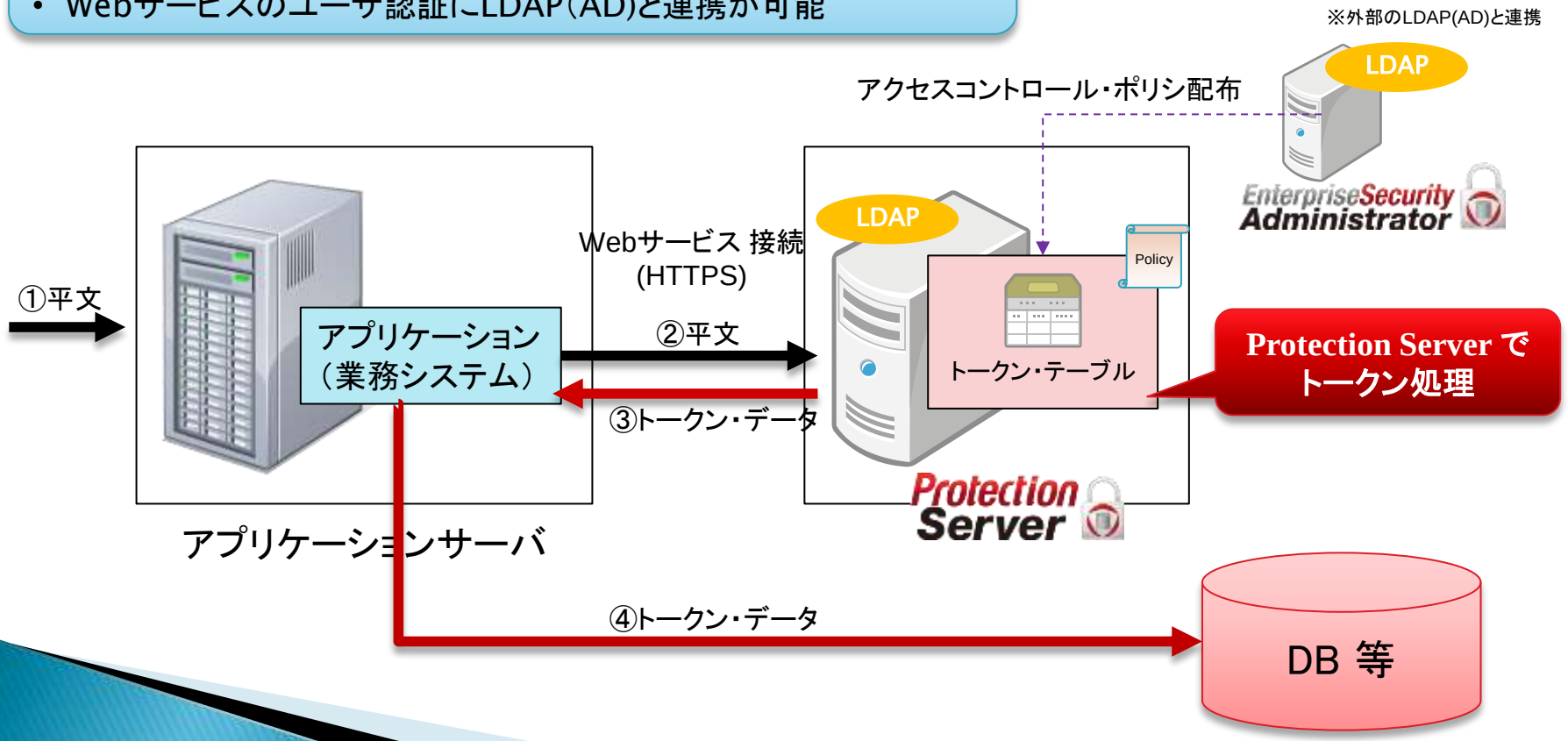
手法	詳細	オリジナルデータ（例）	変換後データ（例）
トークン化		5511 3092 3993 4975	8278 2789 2990 2789
暗号化		Protegrity	0xA2EA9C9BC53D77BA7F 8E85C124296BF3
	DTP2 ※Protegrity社が開発したデータ形式	Protegrity123	cGkKMjRIEP123
	CUSP ※AES-128 [z/OS]のケース	Protegrity	0x1D95BEFC71590AA7B5
アクセスコントロール	ユーザ毎でのデータ アクセス制御	—	—
ハッシュ	HMAC-SHA1	Protegrity	0x0153DE6D5B43A0C38F 8359643775F4D6D18FCD13
マスキング		4537432557929840 4537432557929840	453743******9840 ----43255792----

Protegrity Protection Server構成例 -推奨構成-

アプリケーションサーバとProtection Serverを Webサービス（SOAP-XML、REST-JSON）で接続

注意点： アプリケーションの改修が必要

- トークン化に伴う負荷が、アプリケーションサーバに掛からない
- 負荷分散／Protection Serverの拡張が容易に可能
- Webサービスのユーザ認証にLDAP(AD)と連携が可能



Protegrity Protection Server構成例③（追加参考情報）

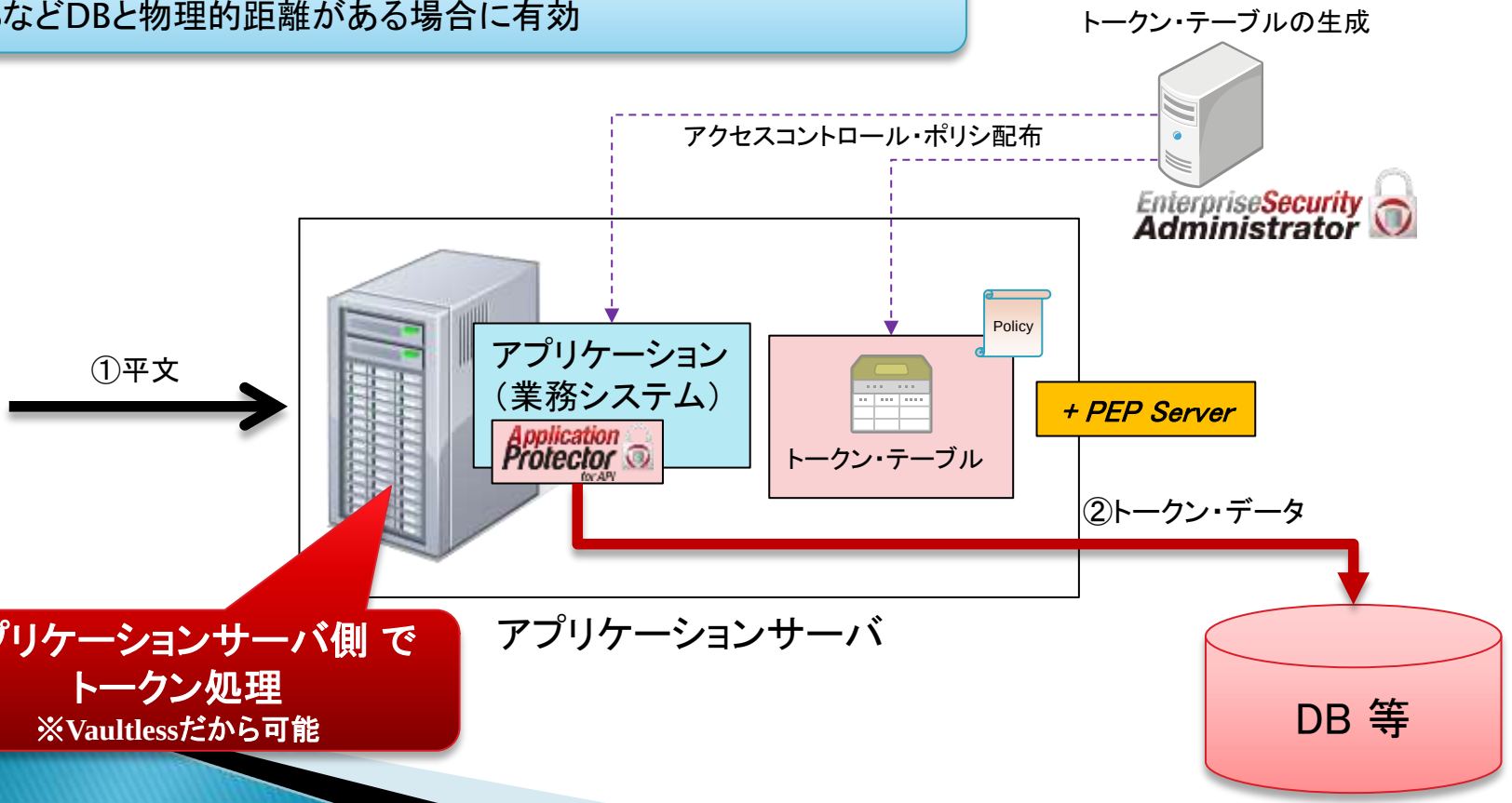
アプリケーションサーバ内に、トークン・テーブルを実装

アプリケーションサーバ内で、データ・トークナイゼーション化を行う

Application Protectorが必須

注意点： アプリケーションの改修が必要

・データ入力時に、オンメモリでトークン化をすることが可能な構成
・POSなどDBと物理的距離がある場合に有効



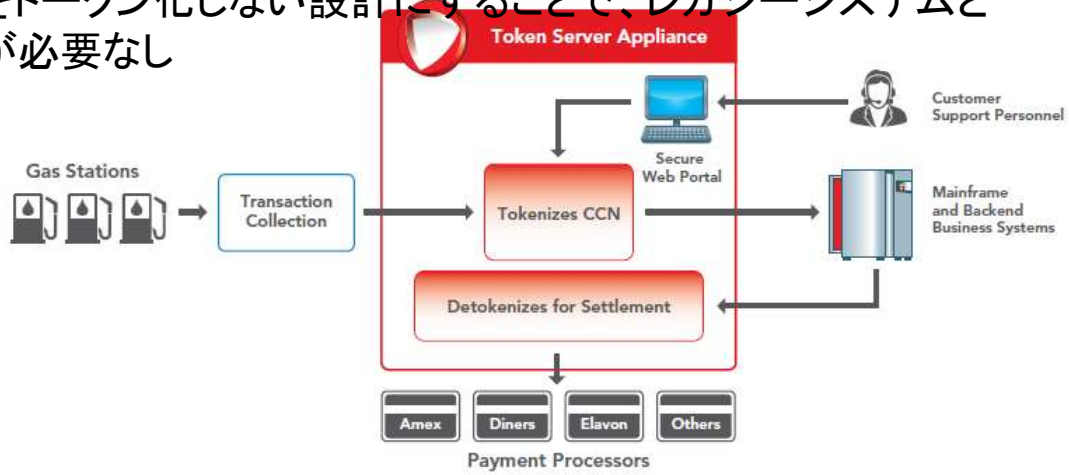
アプリケーションサーバ側 で トークン処理
※Vaultlessだから可能

Protegrity Protection Server 導入実績

- ✓ 大手石油会社 Preem（スウェーデン）

- ➢ 目的：
  クレジットカード番号のトークン化
  システムの変更を最小限にし、メインフレームをPCIの監査対象外にする
  支払決済が高度な処理速度と拡張可能を持つ
  カスタマーサポートチームは通常通りに決済システムに入力できるようにする

  ガソリンスタンドから収集された取引データは暗号化状態で保存される。
  クレジットカード番号はトークン化される。
  クレジットカード番号の最初の6桁をトークン化しない設計にすることで、レガシーシステムとの連携を可能にし、システム変更が必要なし



Protegrity Protection Server 導入実績

- ✓ 大手石油会社A（米国）

- ➢ 目的：
  クレジットカード番号をトークン化することで、データウェアハウス及び、関連する他のシステムをPCI DSSの監査対象外にする。

  Protegrity Protection Serverの導入により、対象となるシステムをPCI DSSの監査対象から除外することで、監査期間を7ヶ月から3.5ヶ月への短縮を実現。

  ワークフローの前段部もトークン化することで、他のシステムもPCI DSSの監査対象外にする計画を推進中。

Protegrity Protection Server 導入実績

- ✓ 大手リテールストア（米国）

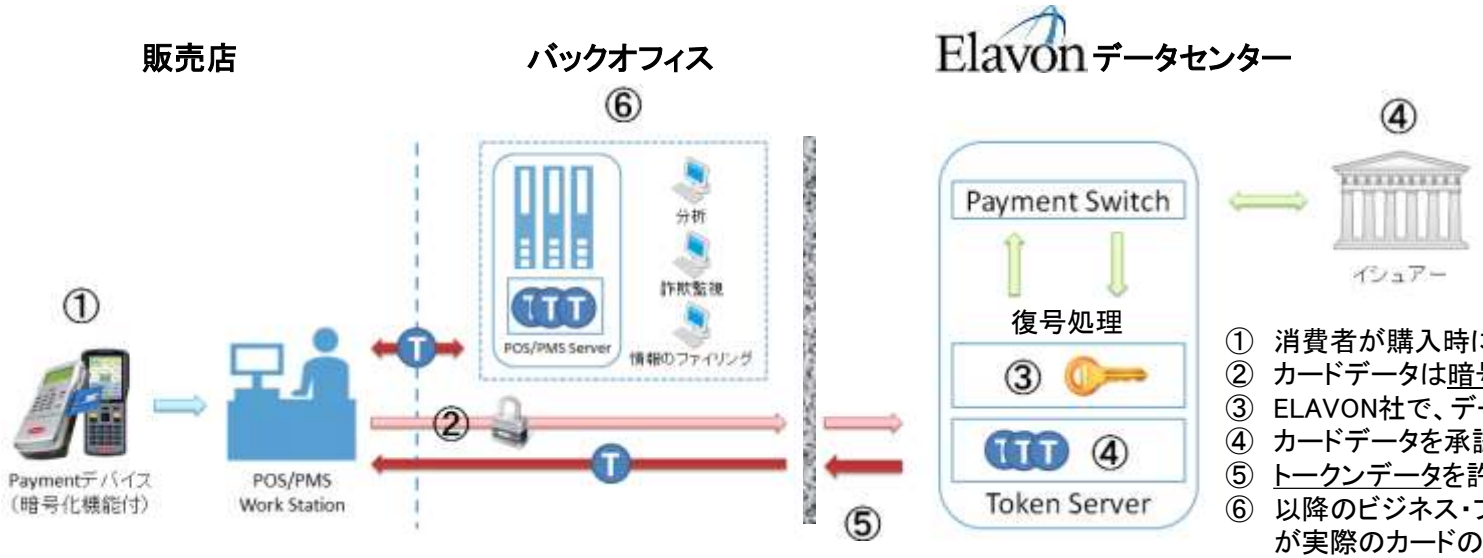
- ➢ 目的：
  導入済みのProtegrity暗号化製品から、トークン化への移行。

  各小売店舗からアーカイブまでの”End to End Encryption”を実現する、Protegrity社のデータ暗号化製品を利用していました。
  その後、Protegrity Protection Serverを検証し、好結果が認められたことから、Protegrity社に全暗号化データの復号処理を含むトークン化の依頼がありました。

Protegrity Protection Server 導入実績

- ✓ Elavon社（米国）

- ➢ 目的：
  カード決済に伴うセキュリティの確保
  運用効率の改善
  高速なトークン化、コスト削減



① 消費者が購入時にカードを提示
② カードデータは暗号化されELAVON社に送信
③ ELAVON社で、データ・ペイロードを復号化
④ カードデータを承認のためイシュアーに送信
⑤ トークンデータを許可応答とペアでPOSに返信
⑥ 以降のビジネス・プロセスでは、トークンデータが実際のカードのデータの代わりに、POS/PMSサーバに格納され使用される

※Elavon社は、米国で第4位の規模を持つ決済プロセス企業です。世界中で100万以上のロケーションでの決済を、年間20億件以上取り扱っています。

Protegrity Protection Server 導入実績

大手石油会社（米国）	使用されるクレジットカード情報は、様々なプロセスを経て最終的に決済されます。ファイルでの処理を受け取るメインフレームがあり、あるプロセスにおいては、決済会社に処理を送ります。 Protegrity社が開発したファイルゲートウェイとProtegrity Protection Serverを組み合わせにより、クレジットカード情報が入った状態でのファイルの遣り取りを可能にしました。このファイルゲートウェイ内部では、ファイル発行時にクレジットカード情報をトークン化し、メインフレームで処理を行います。トークン化されたクレジットカード情報が処理されることで、このメインフレームはPCI DSSの監査対象外となりました。 支払いプロセスのルートにおいては、このファイルはメインフレーム外で非トークン化されます。このお客様は、簡単に利用でき、且つ、このメインフレームで30分以内に処理出来るトークン製品を探していました。
大手リテールストア（米国）	eコマースビジネスを開始するにあたり、クレジットカード番号を含む全てのビジネスプロセスを防御するために、Protegrity社のProtection Serverを導入しています。 全てのクレジットカード番号をトークン化するために導入されました。
中堅保険会社（米国）	このお客様は、多くの拠点及びグループからバッチ処理の要求を受けています。このバッチ処理はトークン化されて受け渡されます。ソーシャルセキュリティ番号がトークン化された後、極秘データはアクセス不可能となり、プロセスを通して防御されます。
大手クレジットカード発行会社（米国）	取り扱われるデータは複数のソースからテラデータのデータウェアハウスに格納されます。データはETLによって管理されます。この企業ではデータを部署ごとに分析しています。（使用パターン、プロモーション、詐欺の確認など） これらすべての分析では、実際のクレジットカード番号は必要としていません。このためカードデータをトークン化して最後の4桁のみを実データと紐付け分析する手法をとっています。 この企業では内部からのカード情報漏洩対策と、PCI DSS準拠を目的としてProtegrity社のデータ・トークナイゼーションを導入しました。

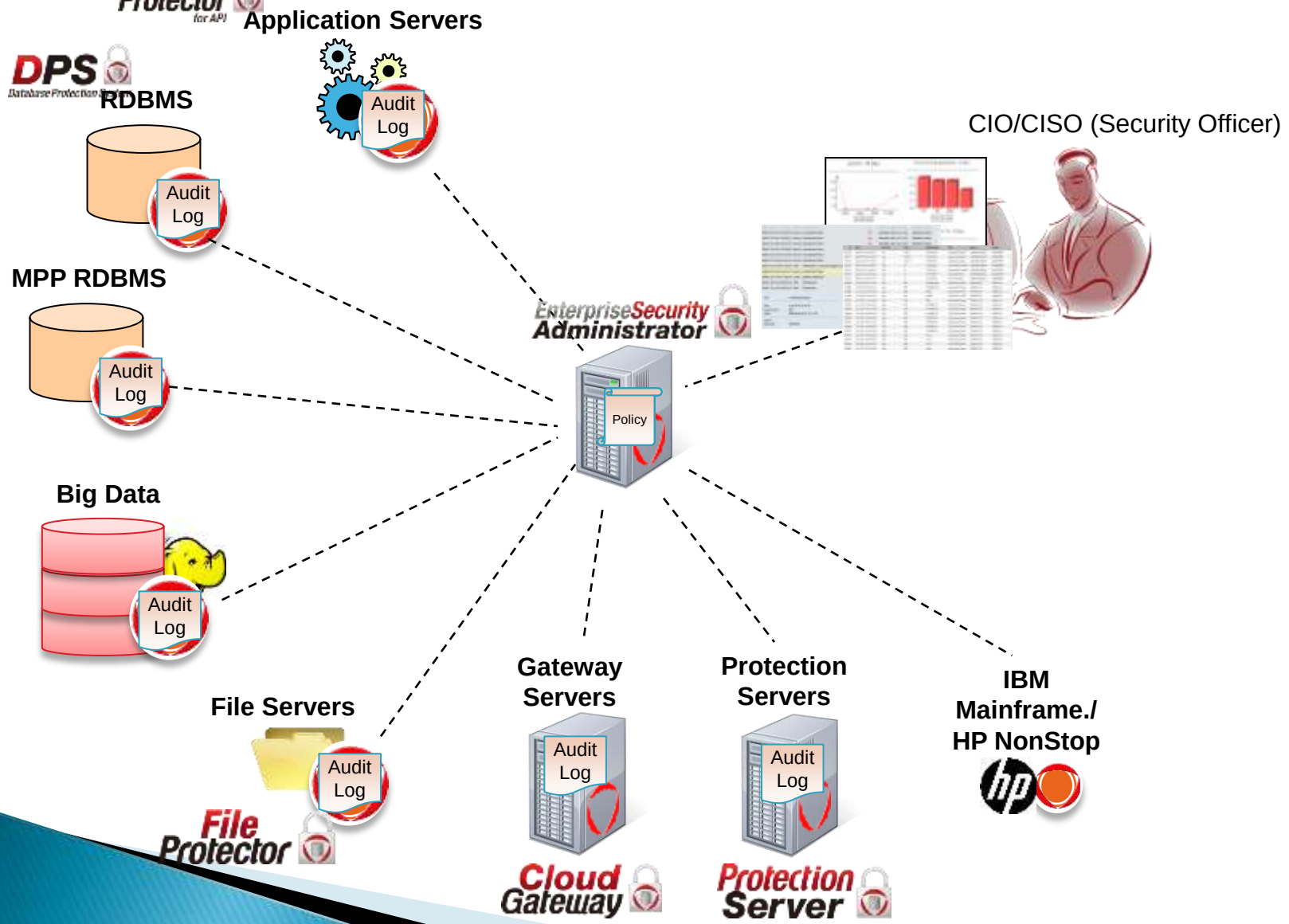
※一部抜粋

Protegrity 製品導入実績

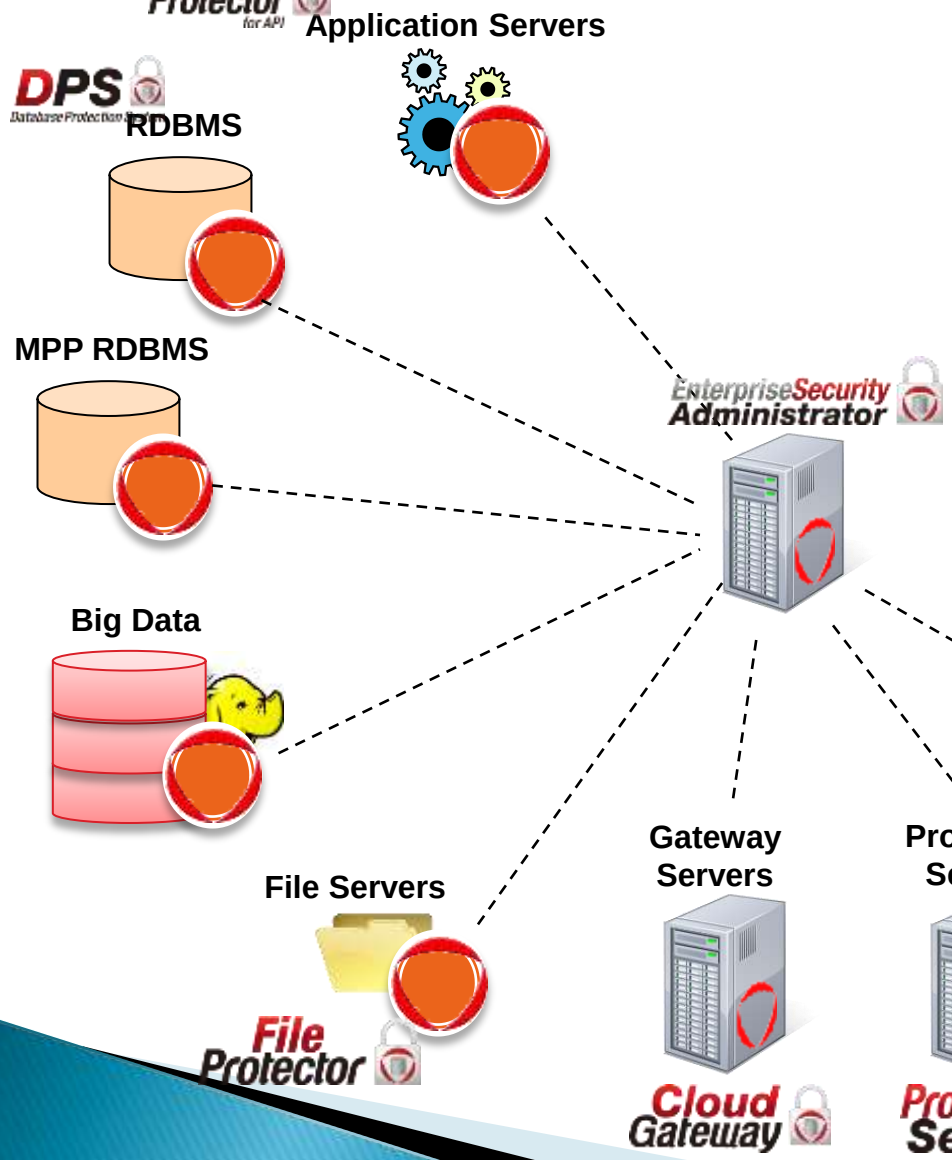
米国大手リテールストア	USDA：アメリカ合衆国農務省
Lowe‘s：米国第2位の住宅リフォーム・チェーン	Cabela‘s：米国大手アウトドア通信販売専門店
GAP：米国大手製造小売業	Coop Italia：イタリア大手スーパー
Safeway：米国第2位のスーパーマーケット	First American Financial：米国大手金融会社
Best Buy：世界最大の家電量販店	GE Commercial Finance：GEキャピタル金融事業
Limited Brands：世界第4位の大手衣料専門店	Independence Blue Cross：米国大手保険会社
Lufthansa：欧州第2位、世界でも十指に数えられる大手航空会社	Kaufland：ドイツ大型スーパーマーケット
Southwest Airlines：米国で第6位、世界で8位の大手航空会社	State Compensation Insurance Fund：米国大手ファウンダー
ARC（Airlines Reporting Corporation）：大手航空会社と旅行代理店の間で航空券販売に関わる決済を請け負う企業	Union Pacific：米国最大規模の鉄道会社
CH Bank：中国大手銀行	Visa Argentina：VISAカードアルゼンチン

※一部抜粋

Protegrity データ・セキュリティ プラットフォーム



Protegrity データ・セキュリティ プラットフォーム



- Enterprise Security Administrator (ESA)
  - セキュリティポリシーの集中管理
  - ソフトウェア・アプライアンスとして提供
  - 強固、HA構成、バックアップ及びレストアー機能
- Data Protectors
  - Enforcing data security policy close to the data store
  - 各拠点でのアージェントとして配置
  - 多種多様のカバー:
    - AIX, HPUX, Linux, Solaris, Windows, z/OS
    - Teradata, Oracle, Netezza, Greenplum, DB2, UDB, MSSQL, Hadoop
    - C/C++, Java, .NET, Cobol
    - IBM Mainframe, HP NonStop
  - ソフトウェア・アプライアンスとして提供: Web Services, Gateway

Protegrity社紹介

Protegrity社は、米国コネチカット州スタンフォードで1996年に設立されました。

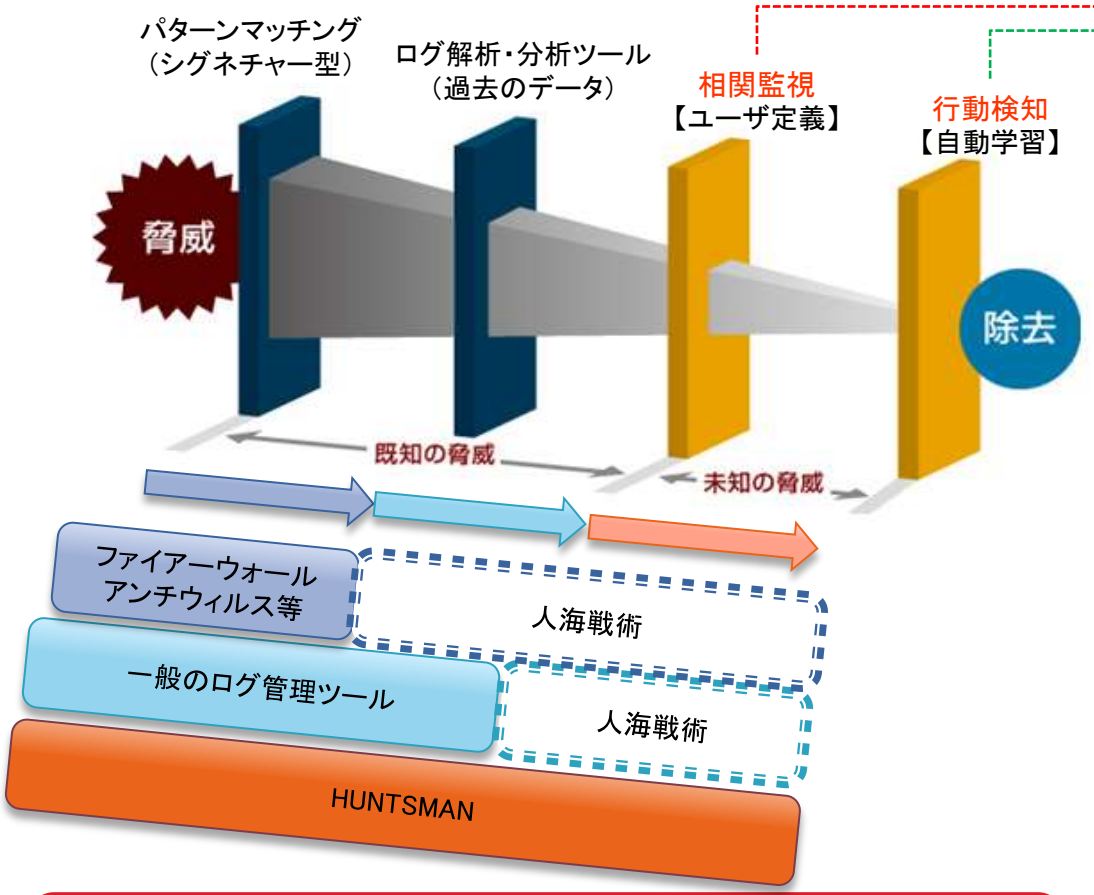
米国金融ヘッドクォーターの集うスタンフォードを中心に各重要セキュリティ・ソリューションを提供・展開しております。

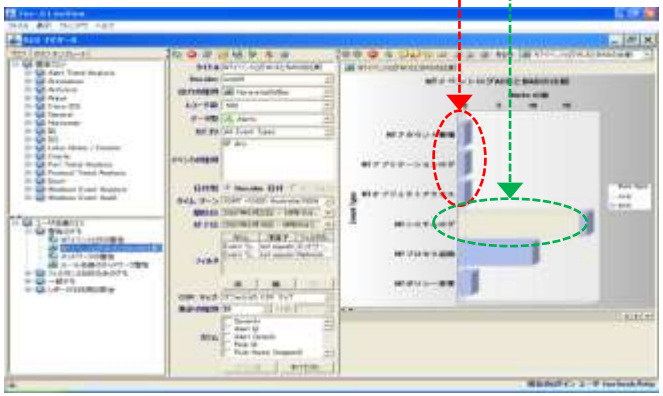
欧米では、PCIDSSに基づくセキュリティ・ソリューションの提供を中心に行っており、主要銀行、大手小売店から、大手ECサイト、大手アパレルなどへの導入実績もあり、Hadoopやクラウドサービスへのセキュリティを含めたトータル・セキュリティ・ソリューションを提供しています。

http://www.protegrity.com

【余談】ログベースの統合監視ソフトウェア

未知の脅威(内部犯行・標的型マルウェア対策)には行動検知(B.A.D)が有効





HUNTSMANの優位性

行動検知による不正監視対策
Behavioral Anomaly Detection
(振る舞いによる検知)技術を実用化
※特許を取得

リアルタイム性の実現
既存の技術では不可能な
高度な情報セキュリティの要求に応える

一般的なログ管理ツールでは、『未知の脅威』の事象が発生した場合、
人海戦術で対応せざるを得ない

想定外の問題・脅威の発見が可能

「File Watch」「Directory Watch」機能により、
ファイル変更、ディレクトリー変更の監視が可能。(要件11.5)

PCI DSS向けのテンプレートが存在します

日時計（sun dial）のシンボルに示される「文字盤」は、真理（ゆるぎなき価値基盤）を表し、偏りなき目で事実を捉える姿勢を意味します。そして、「針」は「方角」と「時」を表し、現在の位置と向かうべき方向を指し示し、時代をリードする取り組みを意味しています。

MONETは、お客様のビジネスにおける事実の認識を支援し、時代をリードする独創的・先進的なソリューションの提供を通じてお客様に貢献することをミッションとしております。

お問い合わせ先
株式会社MONET（モネット）
ソリューション事業部
URL：www.monetz.com
E-mail：sales@monetz.com