その対策で何を守れている？
リアルセキュリティから考える、
各種ソリューションの再整理

2016年11月21日

マクニカネットワークス株式会社
技術統括部プロダクト第４技術部
部長　高橋 峻

日本セーフネット株式会社（ジェムアルト株式会社）
アイデンティティ＆データプロテクション事業本部
セールスエンジニアアシスタントマネージャー　舟木 康浩

01

マクニカネットワークス

会社紹介

弊社概要


マクニカ新横浜本社


西日本支社

会社名　マクニカネットワークス株式会社
（株式会社マクニカ　100%出資）

設　立　2004年3月1日

本　社　横浜市港北区新横浜1-5-5

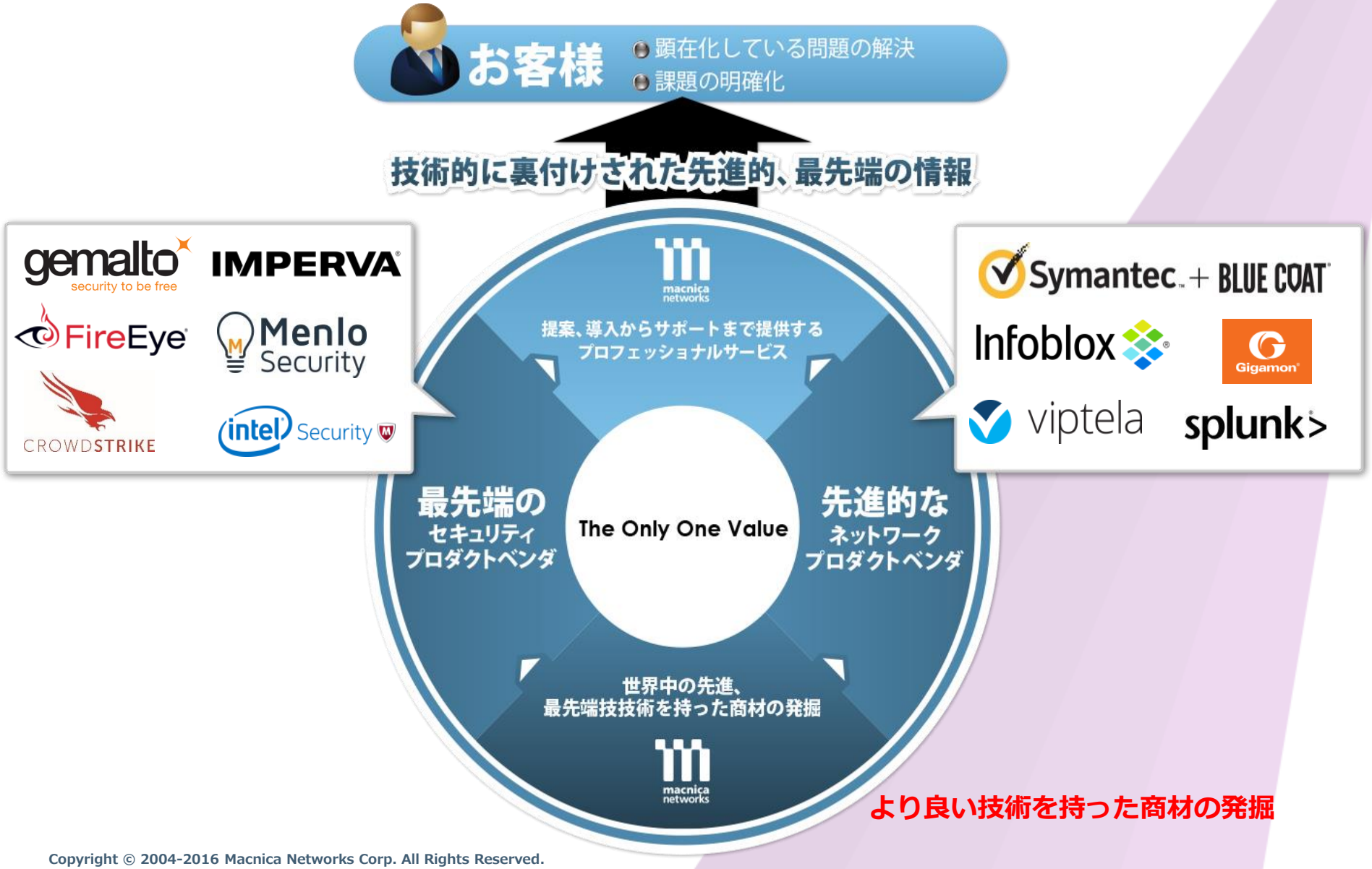
代表者　代表取締役社長　池田　遵

資本金　3億円

社員数　305名（2016年 3月31日現在）

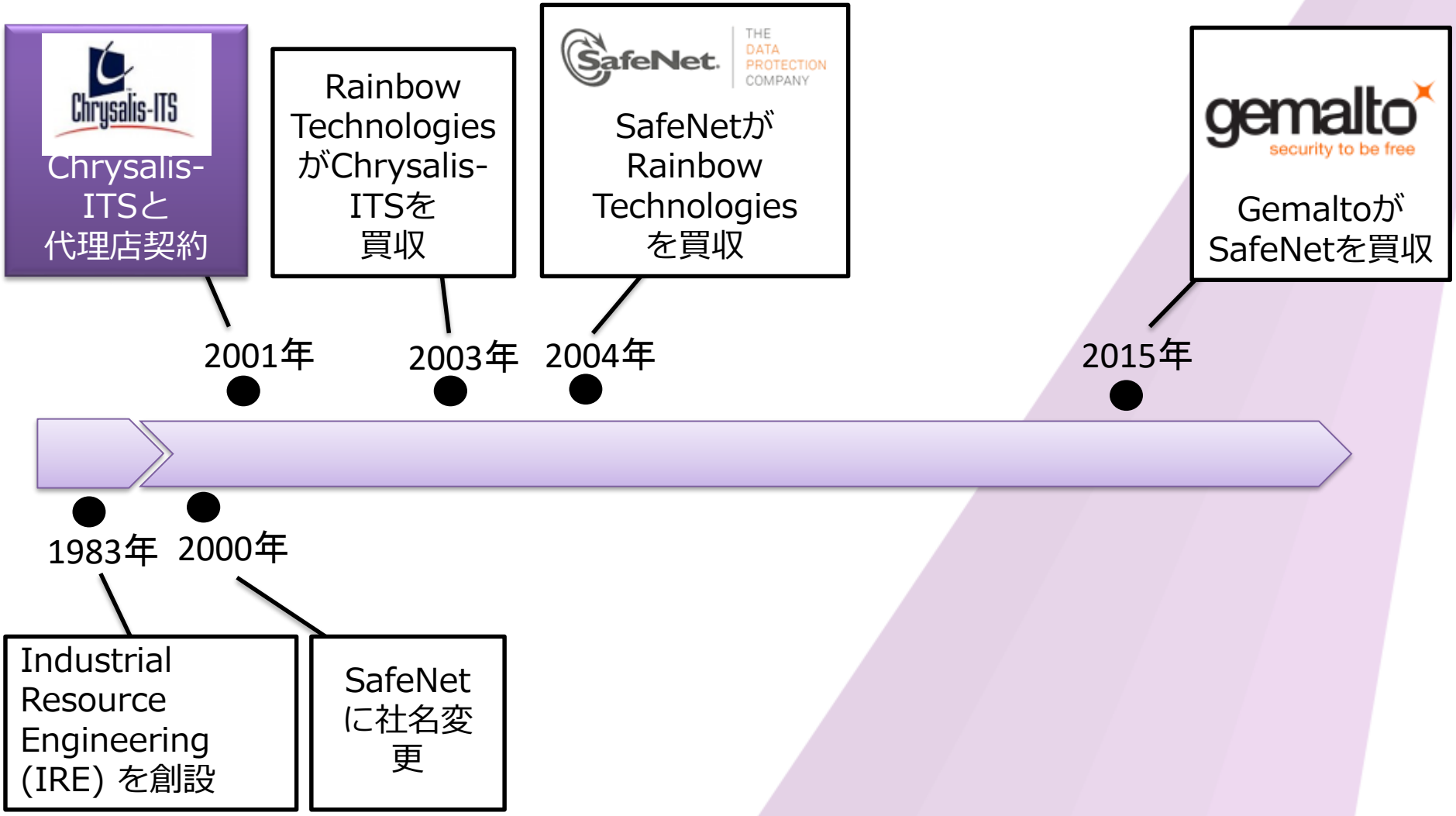
事業内容　企業向けネットワーク、コンピュータ及び情報通信システム関連ハードウェア・ソフトウェアの輸出入、開発、販売コンサルティング/保守・サービスにわたるITソリューションの提供

マクニカネットワークスのミッション



より良い技術を持った商材の発掘

15年以上の販売・サポート実績



サイバーセキュリティに特化し、攻撃を受ける前に、予測的かつ先回りした防御システムの構築を強力にサポート

セキュリティ研究センター
センター長

政本 憲蔵

主任技師

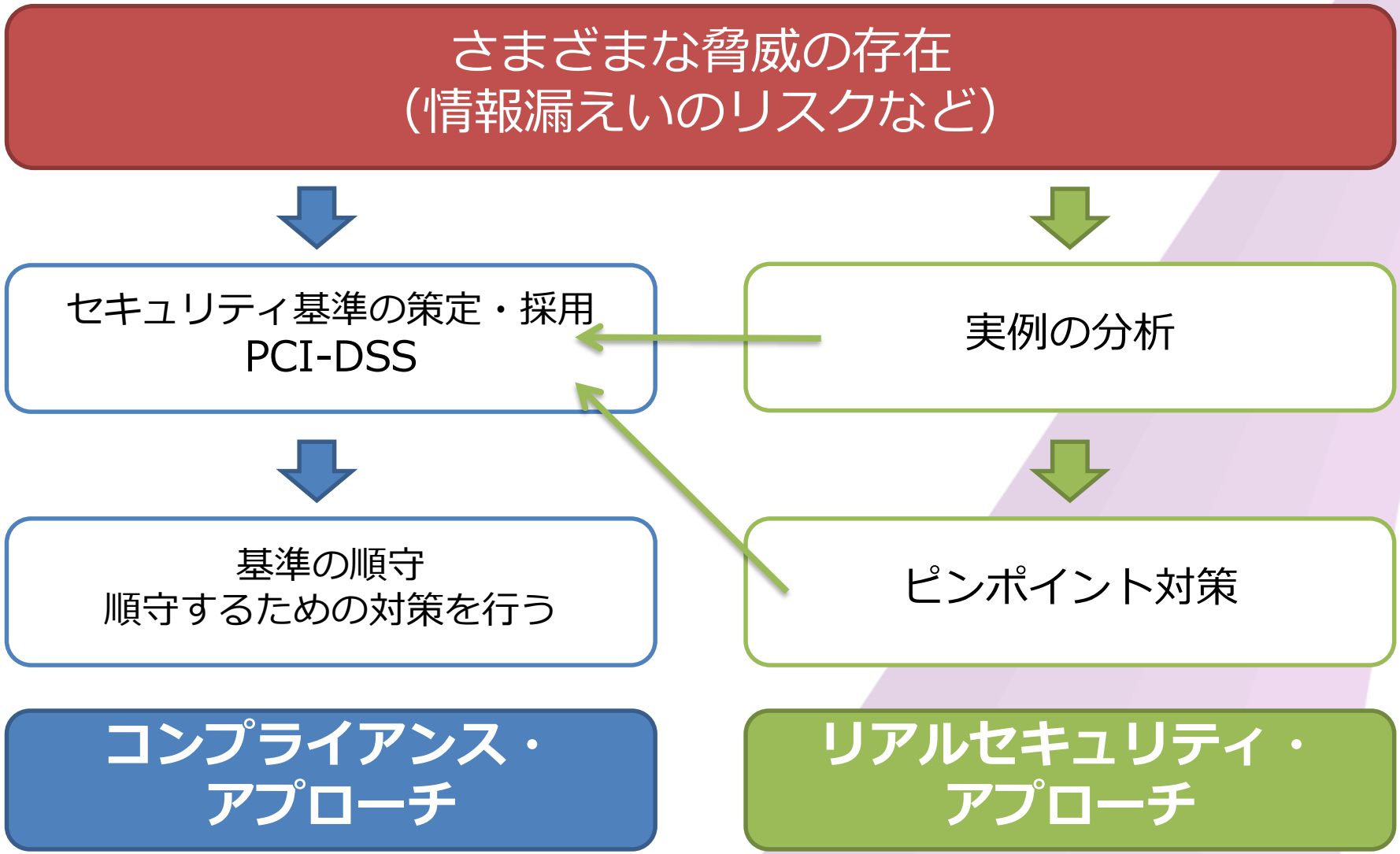
凌（しのぎ） 翔太

- **脅威インテリジェンス(※)の蓄積と発信**
- **海外の最先端セキュリティ技術の発信**

※インテリジェンスとは、高度化する脅威の情報を集めて分析し、未来にやってくる脅威を検知するために予測的で先回りした策略を講じるセキュリティ対策のこと

02

昨今の脅威とセキュリティ対策

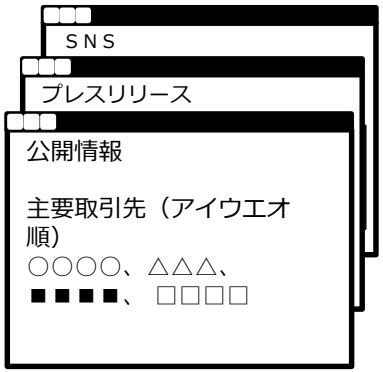


標的型攻撃（外部脅威）

内部不正

標的型攻撃のフロー　Cyber Kill Chain

インターネット

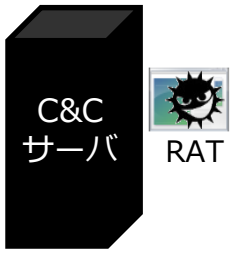


①偵察

SNS、公開情報などからターゲットの情報を収集する

②武器化

マルウェアの作成およびC&Cサーバを構築する



企業A

③配送

メール、Web経由でマルウェアを被害者に送る

④攻撃

被害者がドキュメントを開くと脆弱性が突かれる

⑤インストール

RATが常駐する

RAT：リモートアクセスツール

⑥遠隔操作

RATがC&Cサーバ上の命令を実行する

⑦侵入拡大

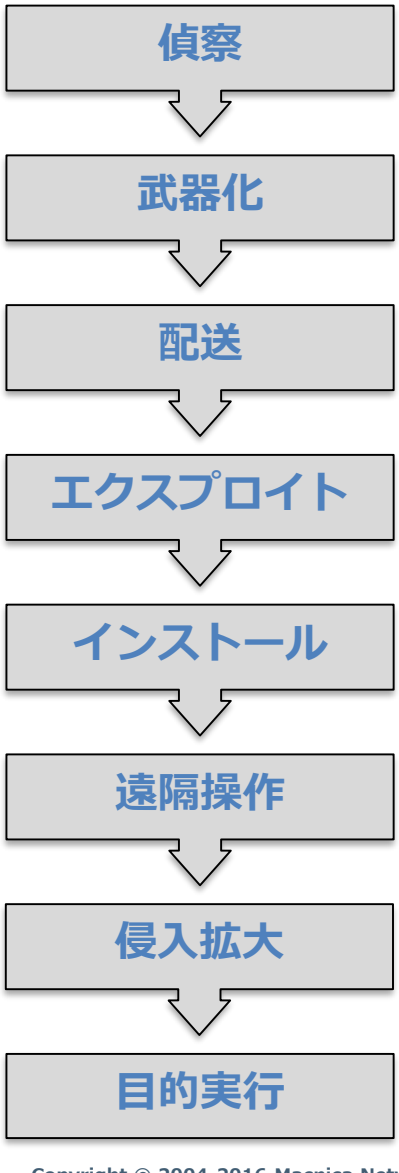
他の端末に侵入する

⑧目的実行

機密情報をC&Cサーバにアップロードする

脆弱性を突くドキュメント

- 強い目的意識
- 高い能力
- 豊富な資金



それぞれフェーズに対し、多層的な防御

サンドボックス
プロキシ、メールセキュリティ
エンドポイントセキュリティ

データ保護（暗号化、トークン化）

標的型攻撃（外部脅威）

内部不正

不正のトライアングル

～ドナルド・R・クレッシー　（1919-1987）～

①機会

不正行為の実行を可能ないし容易にする客観的環境
（見つからずに不正ができる認識を持つ）

EX)・容易に情報にアクセスできる
・不正をしてもバレないことを知っている

②動機

不正行為を実行することを欲する主観的事情
（他人に打ち明けられない何かがある）

EX)・借金を抱えている
・不正を犯すことで利益を得られる

③正当化

不正行為の実行を積極的に是認しようとする主観的事情
（自分を納得させて不正に踏み切る）

EX)・不当な評価をされているから仕返しして当然だ
・他の人もやっているから自分がやっても大丈夫

どれか一つの要素を切り崩す必要性

①機会

不正行為の実行を可能ないし容易にする客観的環境
（見つからずに不正ができる認識を持つ）

- 複数人でチェックをする業務フローにする
- アクセス権限を適切に割り振る
- アクセスログを取得する
- サーバルームに入るときは必ず２人で行う
- 監視カメラを設置する

②動機

不正行為を実行することを欲する主観的事情
（他人に打ち明けられない何かがある）

- 上司が悩み相談に乗ってあげる
- 組織内の円滑なコミュニケーションを図る
- 担当者を定期的に変える

③正当化

不正行為の実行を積極的に是認しようとする主観的事情
（自分を納得させて不正に踏み切る）

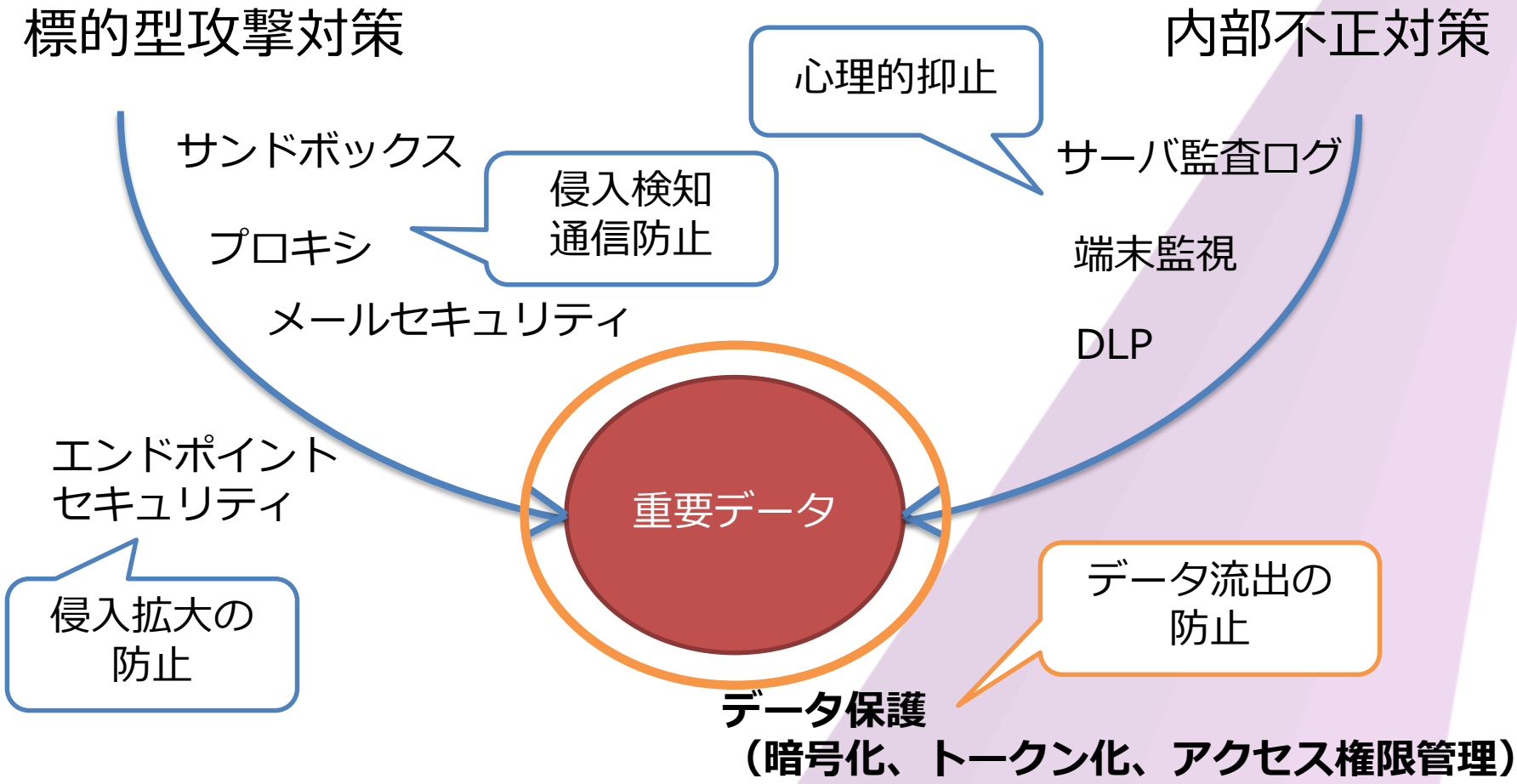
- やったら大変なことになることを教える（教育）
- 適正な評価（尊重）
- 上司との信頼関係を築く
- うらまれないようにする

- 組織論
  - 不正をさせない企業文化の創造
    - 適正な人事評価制度
    - 適正な労働環境
    - 社内コミュニケーションの活性化など
- システム論
  - 抑止：必ずばれる仕組みを作り、周知する
    - 監査ログ（重要データへのアクセスのログ取得）
    - 権限の分掌（2人以上でのアクセスが必要）
  - 防止：重要なデータを取り出せないようにする
    - データ保護（暗号化、トークン化）
    - アクセス権限管理

03

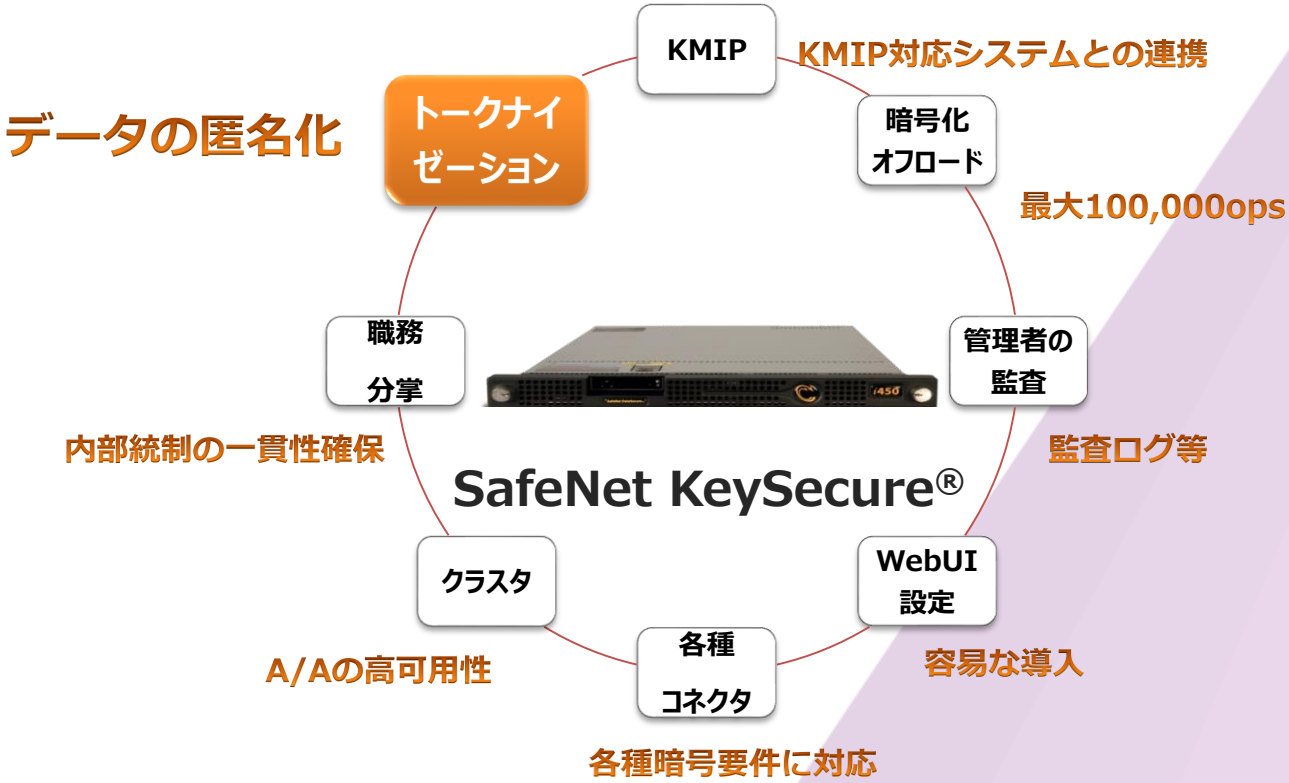
脅威への対策まとめ

- どちらも狙いは「重要データ（カード情報、顧客情報、機密情報など）」
- 多層的な対策アプローチは必須



暗号＋鍵管理＋職務分掌=KeySecure

業界初のHSMベースのマルチプラットフォーム対応
暗号化・内部統制アプライアンス



04

データ保護対策製品のご紹介

- **デジタルセキュリティ分野で世界をリード**
  - UICC（ユニバーサル集積回路）カードやSIMカード、バンキングカード、トークン、電子パスポート、電子IDカード等の組み込みチップ
  - 暗号化技術＆認証技術
- **会社情報**
  - 本社所在地：Amsterdam, The Netherlands （オランダ）
  - 最高経営責任者（CEO）：Philippe Vallée
  - 売上高（FY2014）：25億ユーロ
  - 営業利益（FY2014）：3億8,300万ユーロ
  - 従業員数：約14,000名(46カ国)
  - **特許件数：110件以上（2014年)**

情報漏えいに対する新たな考え方
Gemaltoの提唱する3ステップアプローチ

データの暗号化

PCIDSS要件3
機密データ保護

厳重な鍵管理

PCIDSS要件3
鍵管理

ファイルサーバ

仮想マシン

認証とアクセス制御

PCIDSS要件8
アクセス制御/他要素認証

アプリケーション

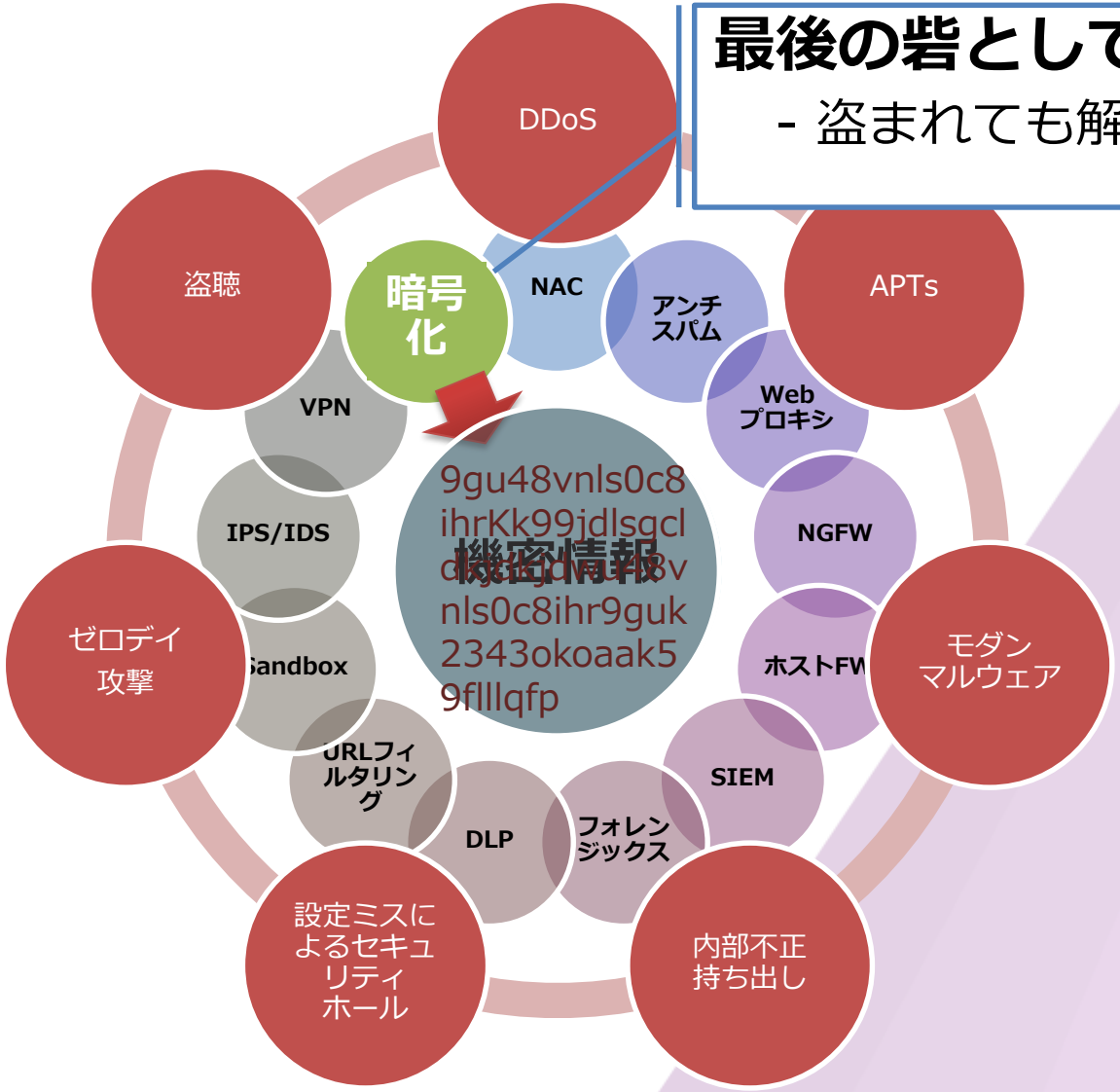
SaaS Apps

3

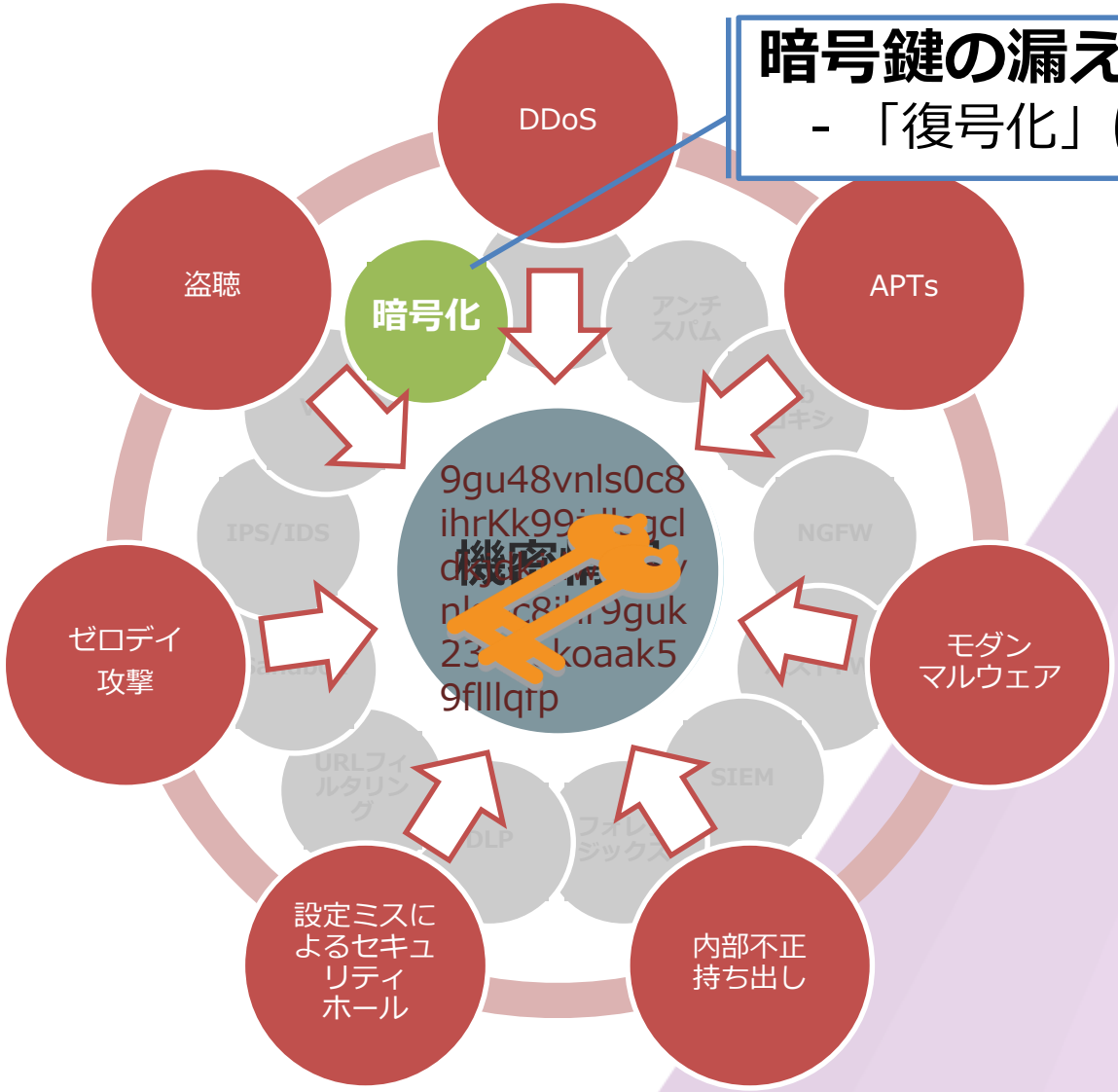
暗号化＋鍵管理の重要性

最後の砦としての暗号化

- 盗まれても解読不可を実現



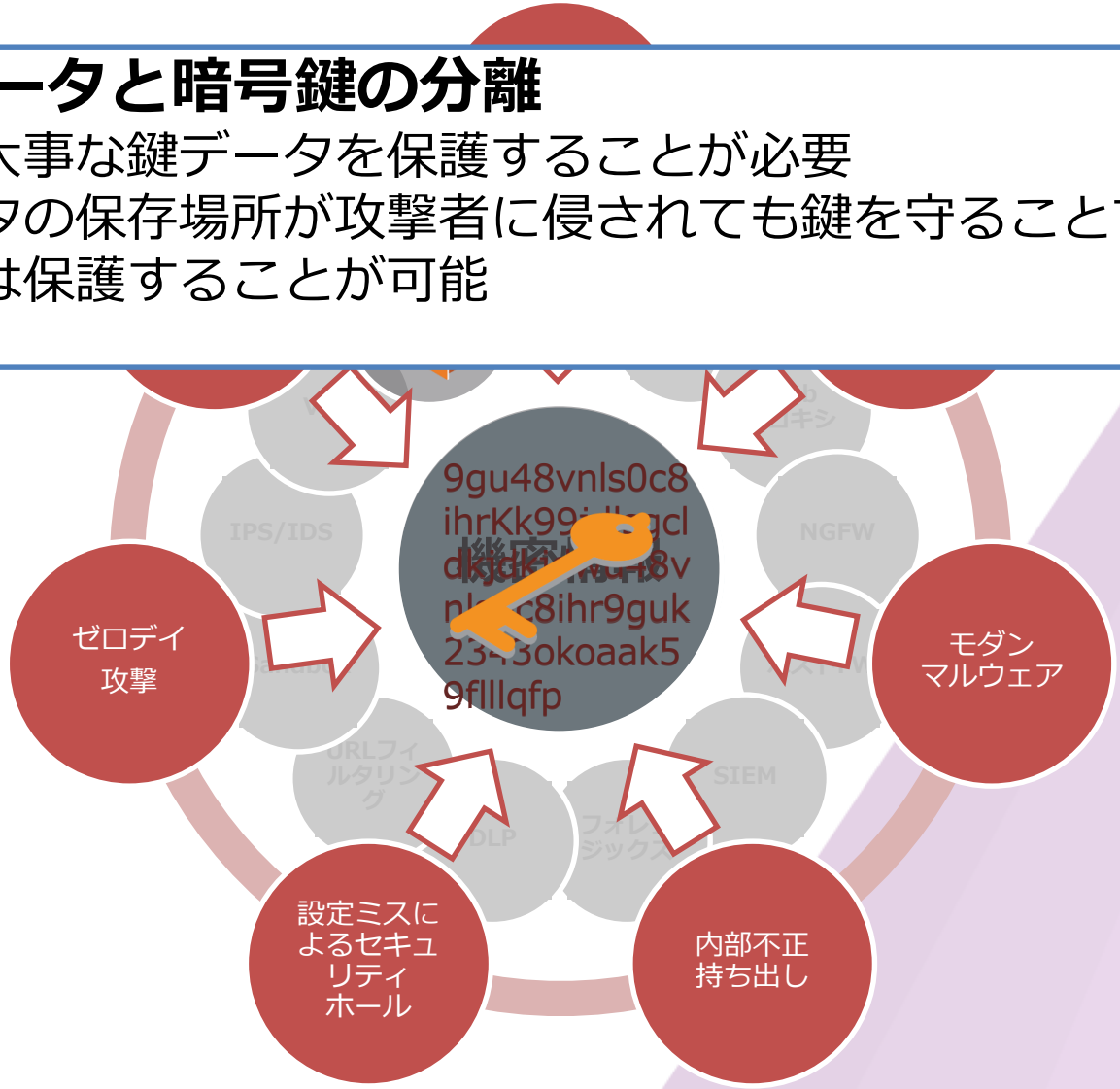
ソフトウェアだけでは防げない



gemalto
security to be free

暗号データと暗号鍵の分離

- 最も大事な鍵データを保護することが必要
- データの保存場所が攻撃者に侵されても鍵を守ることで「機密データ」は保護することが可能



1. F/Wの導入の適切な設定
2. パラメータの適切な設定
3. カード所持者データの保護
4. ネットワーク転送における暗号化
5. アンチウイルスの導入と更新
6. システムの開発とメンテナンス
7. 必要最小限のデータアクセス権限
8. 各個人へのID付与
9. 機密情報への物理アクセス制御
10. 機密情報アクセスの監視
11. システムの定期的なテスト
12. 内部統制の見直し

PCIDSS要件に対する ソリューションご紹介

要件3：HSMの導入メリット



gemalto
security to be free

「鍵」に対する物理/論理セキュリティの提供

- 必要最小限のシステムが特定の場所にある鍵にアクセス
- 物理的盗難対策

「鍵」の利用に対する監査

- 誰がいつアクセスしたか

安全な「鍵」の生成

- ハードウェア乱数生成機能を利用した鍵生成

「鍵」を利用した処理のオフロード

- 専用に設計されたHSM内部で高速に安全に鍵を利用した処理を実行
- 暗号/復号だけでなく多数のAPIを用意(PIN認証等)

第3者認定済

- FIPS140－2L3
- PCI-HSM

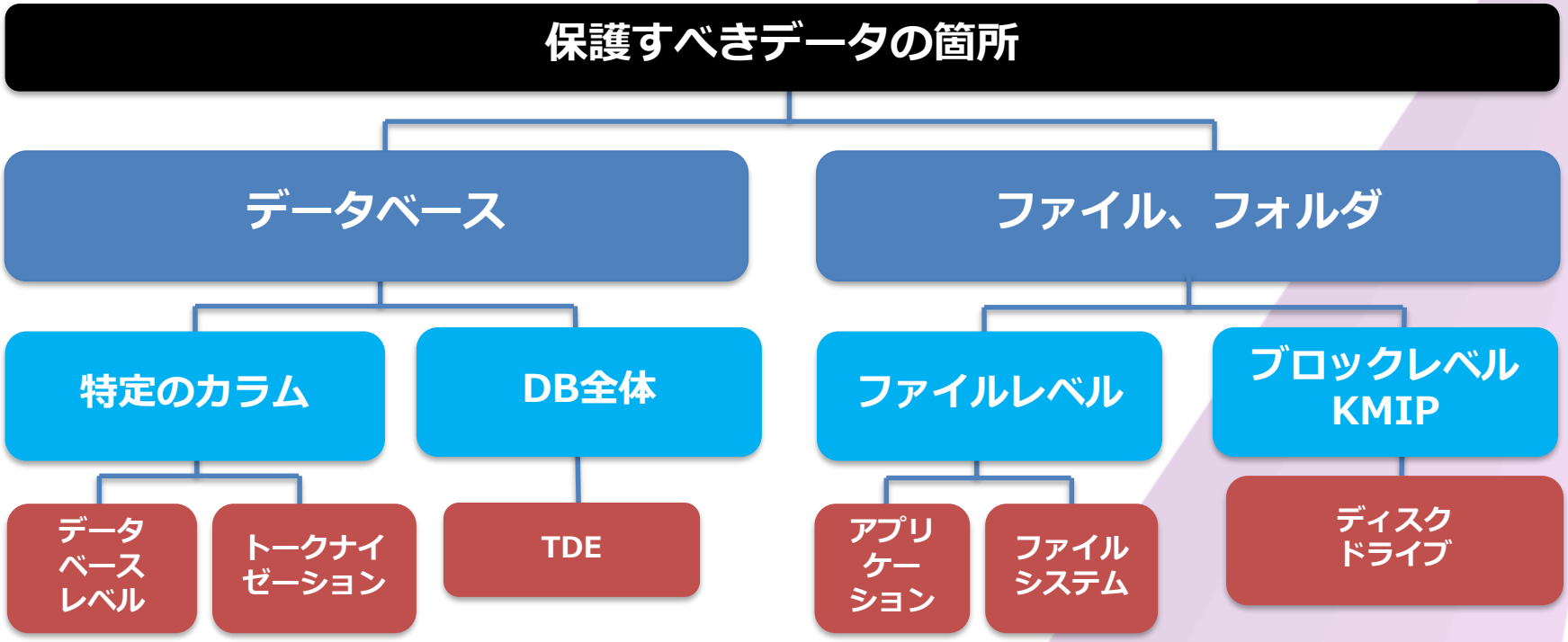
HSMの種類

gemalto
security to be free

汎用HSM Lunaシリーズ	• 標準の暗号API(PKCS,CAPI/CNG,JCE/JCA等）サポート • PKI、DB暗号, SSL等の様々なアプリケーション環境下で利用
決済系HSM EFT	• ICカード発行、金融決済関連アプリケーションに特化 • PCI HSM認定取得 • **P2PE/DUKPT**
（暗号）鍵管理HSM KeySecure	トークナイゼーションご紹介

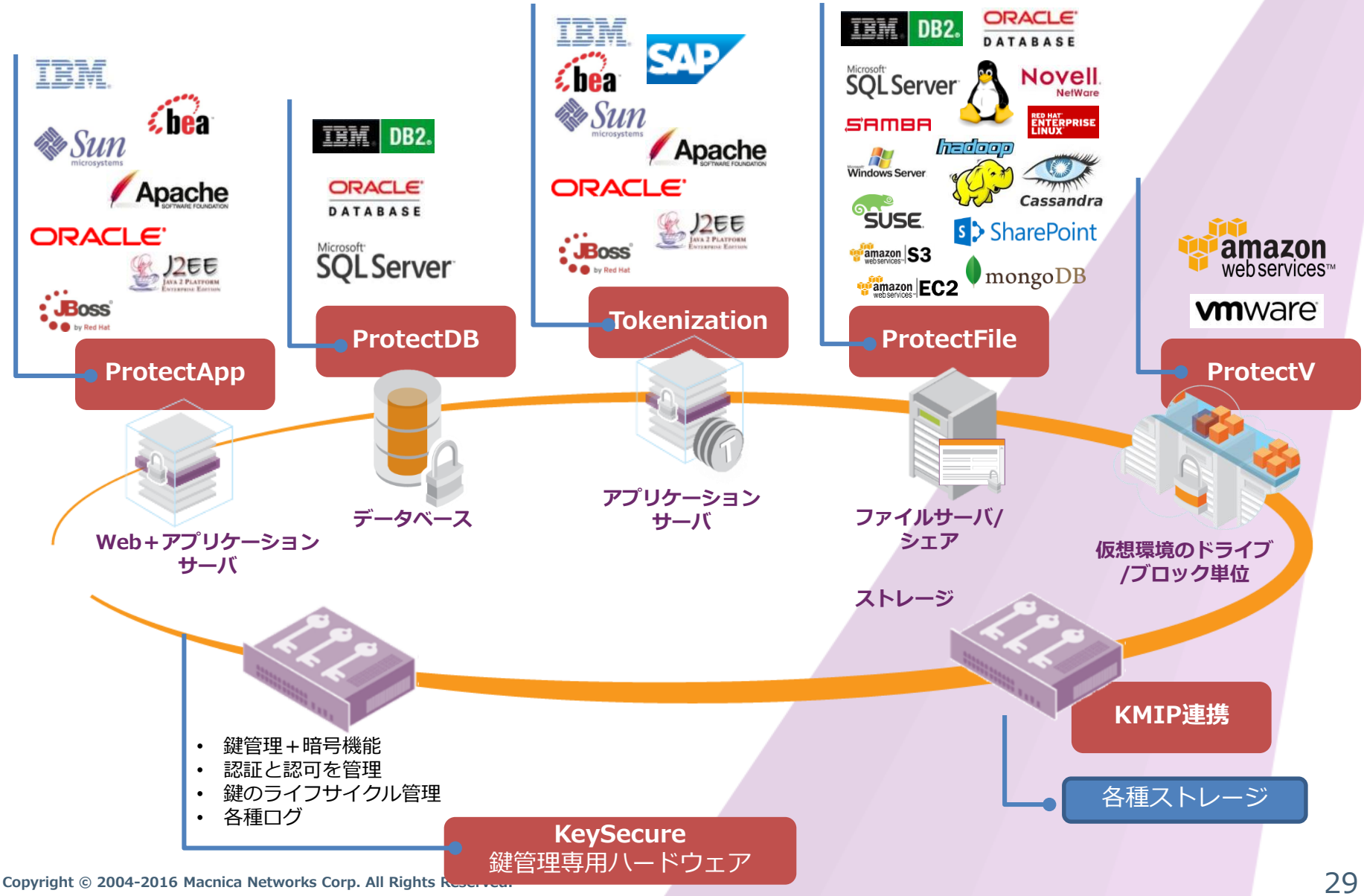
SafeNet KeySecure の提供範囲
あらゆるお客様システムをサポート

gemalto
security to be free



SafeNet KeySecure＋鍵管理ソリューション
あらゆるお客様環境のデータを保護可能

gemalto
security to be free



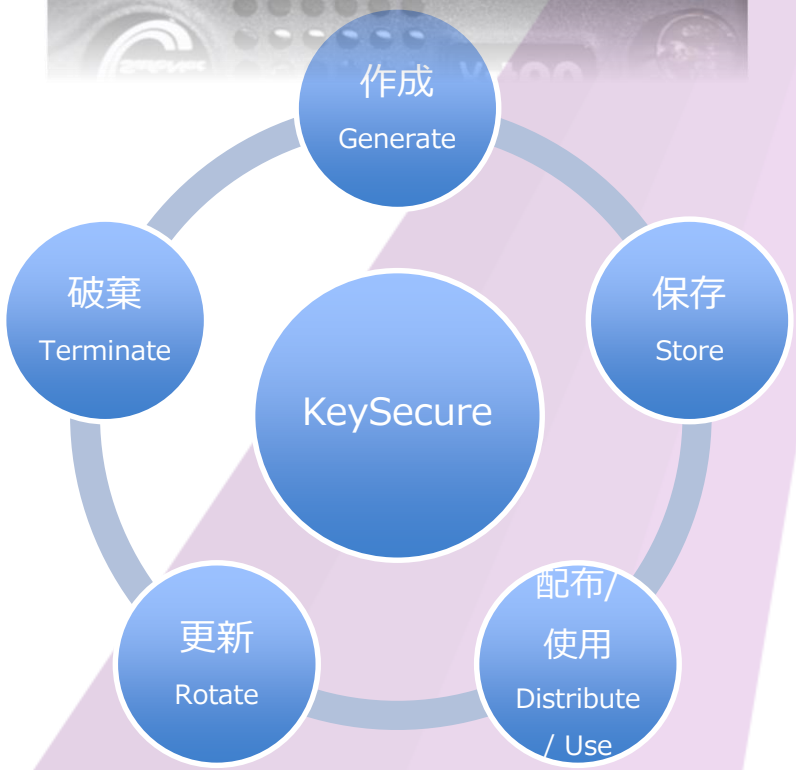
KeySecureによる鍵管理

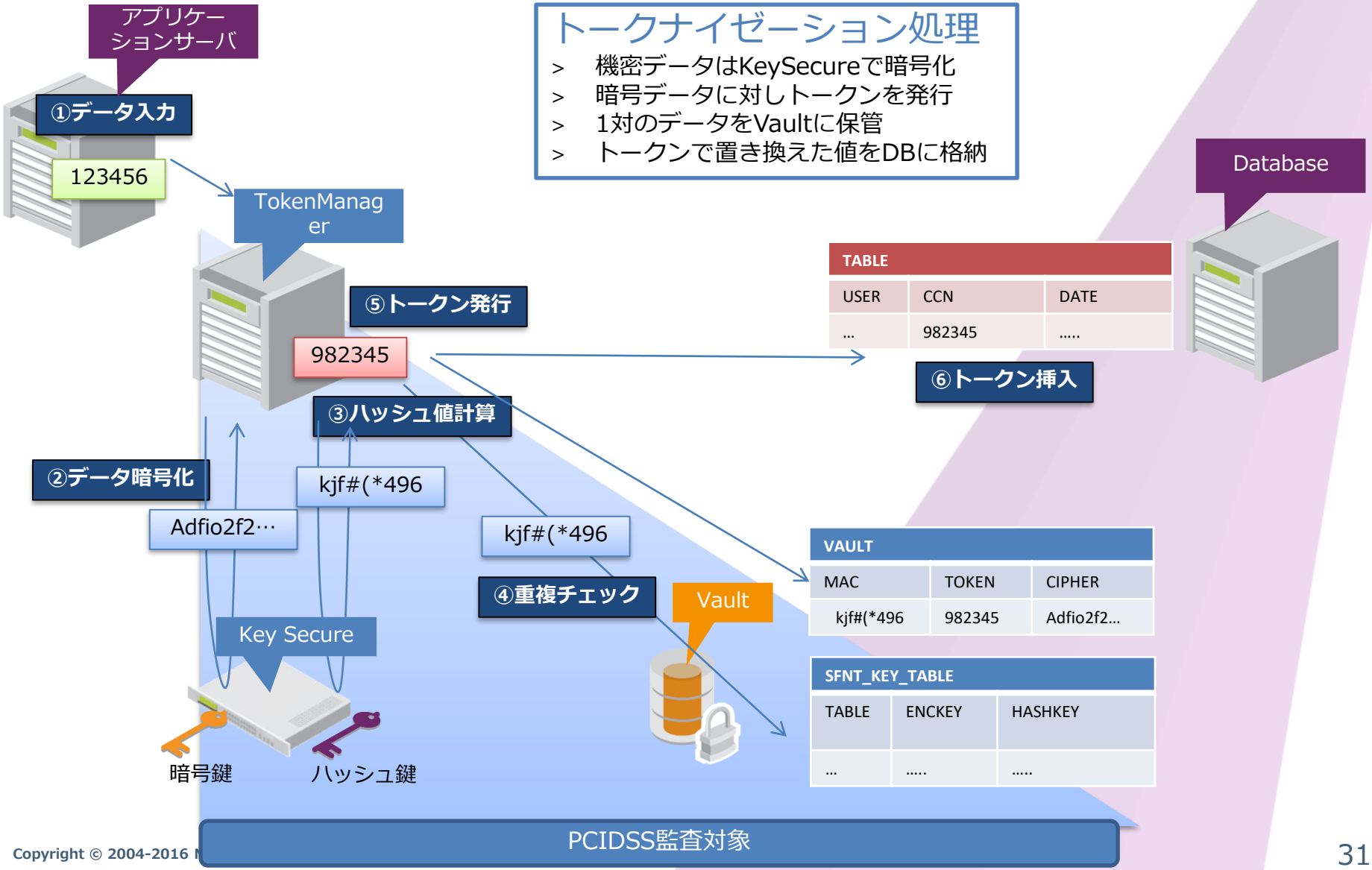
エンタープライズにおけるすべての鍵を管理

- 鍵の集中管理を自社で実現
- 最大100万個の鍵を管理（クラスタ単位）
- クラスタにより高可用性サポート
- 仮想アプライアンス用意(ESXi,AWS)

各種コネクタ(暗号用ソフトウェア)を用意

- SDK
- ファイル暗号/復号
- カラム単位DB暗号/復号
- トークナイゼーション
- KMIPサポート





トークナイゼーション処理

> 機密データはKeySecureで暗号化
> 暗号データに対しトークンを発行
> 1対のデータをVaultに保管
> トークンで置き換えた値をDBに格納

トークナイゼーション導入にあたり
製品機能検討事項例

検討事項	GTO機能
トークナイゼーションシステム構成	以下それぞれのコンポーネントを提供することでお客様要件に応じた柔軟なシステム構成が可能 TokenManager(トークン/デトークン提供するSW) KeySecure(HSM) Vault(トークン格納DB)
HSM機能	FIPS140-2 L3相当のハードウェアアプライアンスを提供
	FIPS140-2 L1相当の仮想アプライアンスを提供
トークンフォーマット	各種トークンフォーマットをサポート
	お客様カスタムフォーマット追加可能
トークン発行機能	Luhnチェックサポート
	トークン重複チェックサポート
デトークン機能	サポート
Vaultの選定	システム要件に応じてOracle、MSSQL、MYSQL、Casandraから選択
	Vaultless(デトークン利用なし）サポート
トークンマネージャインターフェース	WEBサービス(SOAP,REST)、API(JAVA,.NET)をサポート
パフォーマンス要件	マルチスレッドサポート、トークン化/デトークン化ともバッチ処理APIを提供
鍵変更	Key Rotation(新規鍵利用)とReKey(過去のデータを新規鍵で暗号化)をサポート
ログ	TokenManager、KeySecureともSyslogサポート
	KeySecureはAuditログ機能サポート(ログ改ざん検知機能サポート)
監視	SNMPトラップ
冗長構成	各種コンポーネントを必要に応じて冗長構成可能
	KeySecureクラスタサポート
	TMの冗長構成
	Vaultの冗長構成(ご利用されるDBの機能を利用)
トークナイゼーションシステム導入実績	国内での実績有
HSM導入実績	国内でPCIDSS対応、個人情報暗号、ストレージ暗号等の汎用利用で実績有
クラウドサポート	仮想アプライアンス版KeySecureはAWSで利用可能であり、すべてのコンポーネントをAWS上に構築可能

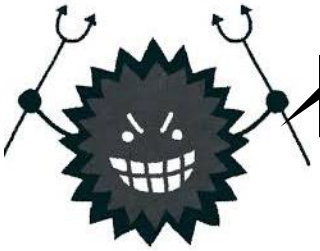
即時の対策が必要なシステム
ファイル暗号化-Protect File

暗号ポリシー

透過的に
各ファイルに
アクセス可能

指定したユーザ/
グループ/プロセス
以外権限なし

暗号/復号



権限なし

参照不可

特定のフォルダ内の
ファイル暗号化指定
各ユーザの権限設定

Windows/Linux

バックアップ/リストア

運用担当者

バック
アップは
許可

macnica networks

ご清聴ありがとうございました。

Thank you.