Discover Protect Control

THALES
Building a future we can all trust

ハイブリッド環境のデータセキュリティ強化

2022年5月18日

Canon
キヤノンマーケティングジャパン株式会社

アジェンダ

1. サイバーセキュリティに関する脅威動向
2. 情報漏えいリスクと暗号化の必要性
3. データベースの透過暗号 デモ実演
4. 暗号化ソリューション、各種サービスのご紹介

最近のサイバー攻撃の状況を踏まえた経営者への注意喚起

■ 大企業・中小企業等を問わないランサムウェアによる被害の急増

新型コロナウイルス感染症の世界的な流行による経済の不安定化などにより、直接的に金銭を求める攻撃が急増している。特に、暗号化したデータを復旧するための身代金の要求に加えて、暗号化する前にあらかじめデータを窃取しておき、身代金を支払わなければデータを公開するなどと脅迫する、いわゆる**「二重の脅迫」を行うランサムウェア攻撃**の被害が国内でも急増しつつある。

ランサムウェア攻撃の深刻さを伺い知る上で参考になるセキュリティサービス企業による最近の調査結果の抜粋。

- 日本の IT セキュリティ担当者 200 人のうち、半数を超える52%が、この 1 年間で「ランサムウェア」によるサイバー攻撃を受け、データを暗号化されるなどの被害を受けたと回答。
  さらに、日本でランサムウェアの被害にあった組織のうち32%が、暗号化されたデータを復元するためのいわゆる「身代金」を犯行グループに実際に支払ったと回答。支払った額の平均は、110 万米ドル（約 1 億 1,400 万円）。

日本企業のランサムウェア被害額は 世界 2 位

金銭の支払いは犯罪組織に対して支援を行っていることと同義であり、また、金銭を支払うことでデータ公開が止められたり、暗号化されたデータが復号されたりすることが保証されるわけではない。さらに、国によっては、こうした金銭の支払い行為がテロ等の犯罪組織への資金提供であるとみなされ、金銭の支払いを行った企業に対して制裁が課される可能性もある。こうしたランサムウェア攻撃を助長しないようにするためにも、**金銭の支払いは厳に慎むべきものである**。

出典 ： 経済産業省「最近のサイバー攻撃の状況を踏まえた経営者への注意喚起」（2020年12月18日）

重要インフラ事業者へランサムウェアについて注意喚起

内閣サイバーセキュリティセンター (NISC) は、ランサムウェアによる被害が相次いで確認されているとして、重要インフラ事業者に対し、注意喚起を実施した。(2021年4月30日)
ランサムウェアを用いた攻撃が活発化し、データの暗号化や窃取といった被害が相次いで発生しており、重要インフラ事業者で被害が生じた場合は社会的な影響も大きいことから注意を呼びかけた。

■ 具体的対応策
(1) 【予防】ランサムウェアの感染を防止するための対応策
(2) 【予防】データの暗号化による被害を軽減するための対応策
(3) 【検知】不正アクセスを迅速に検知するための対応策
(4) 【対応・復旧】迅速にインシデント対応を行うための対応策

重要インフラ

- 情報通信
- 金融
- 航空
- 空港
- 鉄道
- 電力
- ガス
- 政府・行政サービス (地方公共団体を含む)
- 医療
- 水道
- 物流
- 化学
- クレジット
- 石油

チェックポイント

- 重要なデータに対する定期的なバックアップの設定を確認する。バックアップの検討に当たっては、ランサムウェア感染時でもバックアップが保護されるように留意する。例えば、ファイルのコピーを 3 個取得したうえで、ファイルは異なる 2 種類の媒体に保存、コピーのうち、1 個はクラウドサービスや保護対象のネットワークからアクセスできない場所等に保管するといった対策等を検討する。
- バックアップデータから実際に復旧できることを確認する。
- 公開された場合、実際に支障が生じるような機微データや個人情報等に対して、**特別なアクセス制御や暗号化** を実施する。
- システムの再構築を含む復旧計画が適切に策定できていることを確認する。

出典 ： NISC 「ランサムウェアによるサイバー攻撃に関する注意喚起」」 (2021年4月30日)

情報セキュリティ10大脅威 2022

昨年に引き続き、「ランサムウェアによる被害」が1位です。
国内企業や医療機関などを標的とした「二重脅迫型ランサムウェア」の被害が増えています。

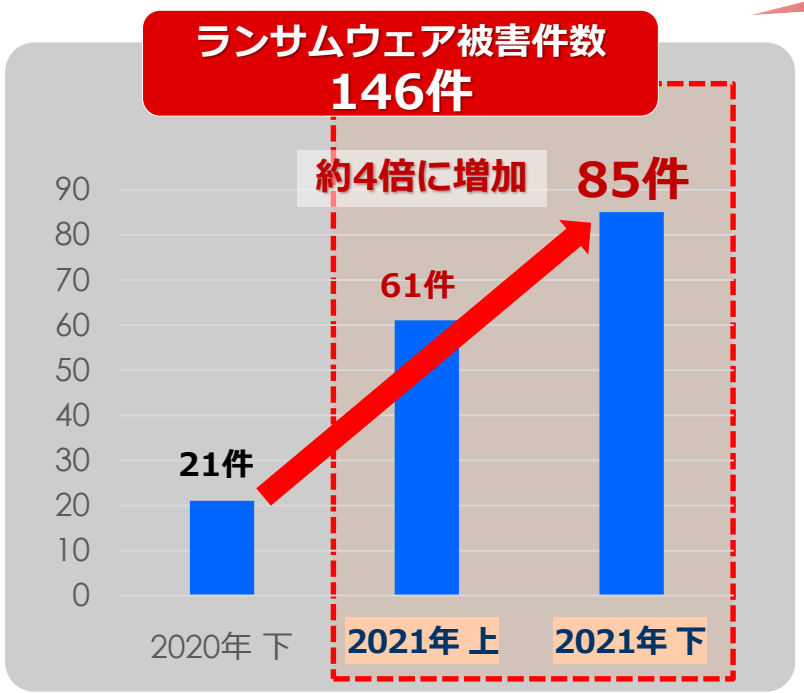
22年の順位	21年の順位		脅威となった攻撃や被害
1位	1位	→	ランサムウェアによる被害
2位	2位	→	標的型攻撃による機密情報の窃取
3位	4位	↗	サプライチェーンの弱点を悪用した攻撃
4位	3位	↘	テレワーク等のニューノーマルな働き方を狙った攻撃
5位	6位	↗	内部不正による情報漏えい
6位	10位	↗	脆弱性対策情報の公開に伴う悪用増加
7位	NEW		修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
8位	5位	↘	ビジネスメール詐欺による金銭被害
9位	7位	↘	予期せぬIT基盤の障害による伴う業務停止
10位	9位	↘	不注意による情報漏えい等の被害

出典 ： IPA 独立行政法人 情報処理推進機構 「情報セキュリティ10大脅威 2022」

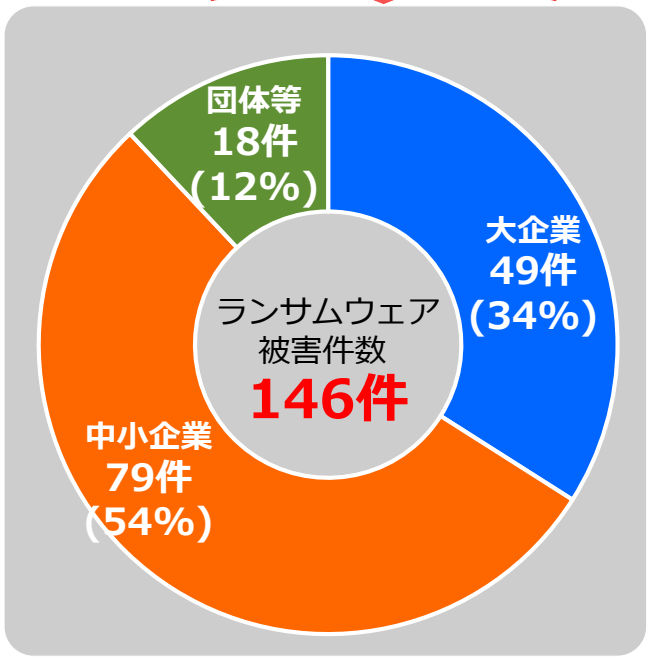
ランサムウェア被害の状況 (2021年)

警察庁から発表された2021年の「サイバー空間をめぐる脅威の情勢等について (速報版)」によると、国内でランサムウェアによる被害が企業・団体等の規模や業種を問わず急増しています。

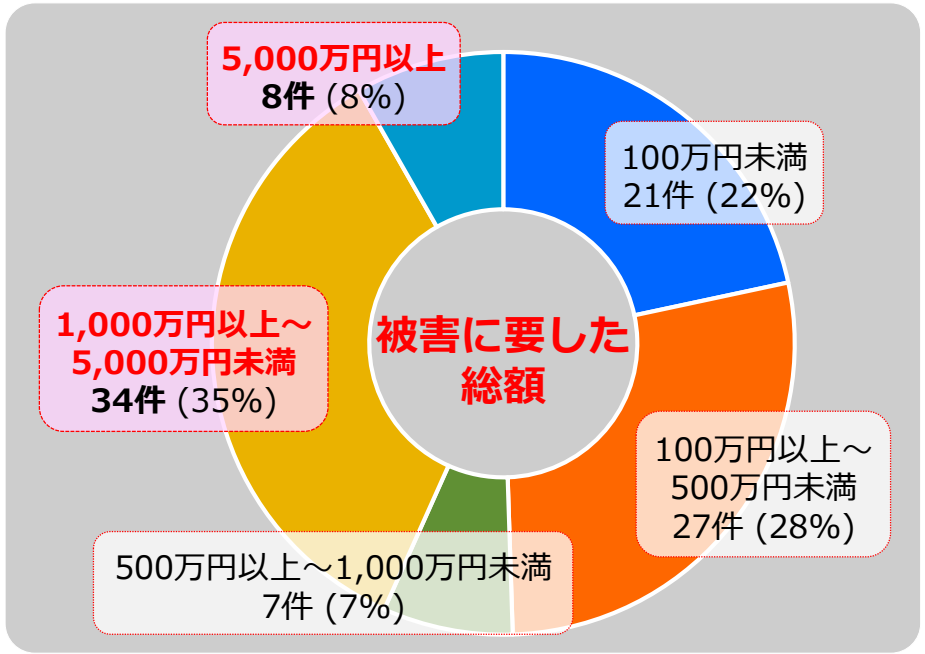
「二重脅迫型ランサムウェア」急増



企業・団体等におけるランサムウェア被害の報告件数



被害企業・団体等の規模別 報告件数

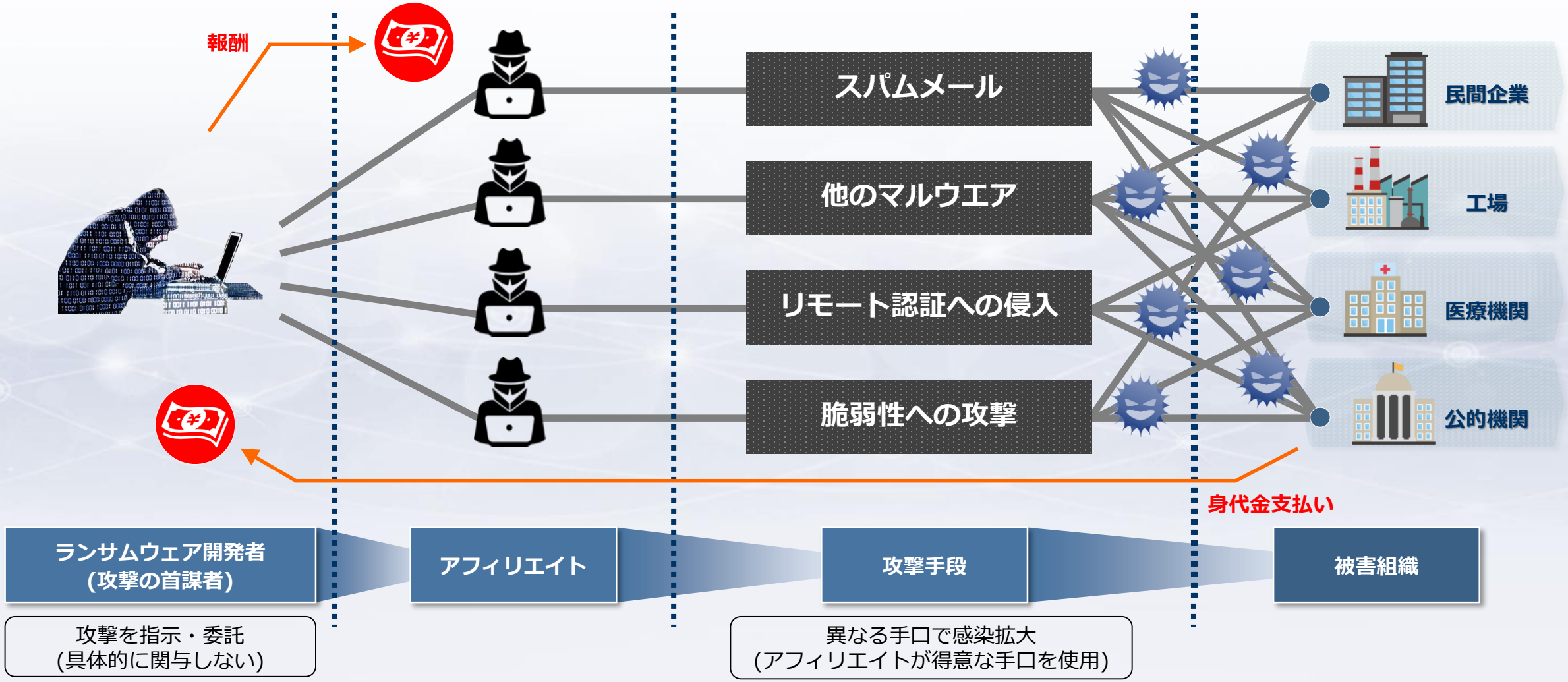


被害の調査・復旧に要した総額

出典 ： 警察庁「サイバー空間をめぐる脅威の情勢等について（速報版）」 2022年2月10日発表

サイバー犯罪のビジネスモデル (例)

RaaS (Ransomware as a Service) における首謀者とアフィリエイトの関係。



個人情報漏えい時の報告の義務化

2022年4月1日施行の令和2年改正個人情報保護法により、個人情報の漏えい等が発生した場合は個人情報保護委員会への報告及び本人への通知が義務化されました。

■ 報告義務が発生する4つのケース

① **要配慮個人情報が含まれる**個人データの漏えい等が発生し、又は発生したおそれがある事態
② 不正に利用されることにより**財産的被害が生じる**おそれがある個人データの漏えい等が発生し、又は発生したおそれがある事態
③ **不正の目的**をもって行われたおそれがある個人データの漏えい等が発生し、又は発生したおそれがある事態
④ 個人データに係る本人の**数が1000人を超える**漏えい等が発生し、又は発生したおそれがある事態

■ 報告を要しないケース

漏えい等が発生し、又は発生したおそれがある個人データについて、高度な暗号化等の秘匿化がされている場合等、「**高度な暗号化その他の個人の権利利益を保護するために必要な措置」が講じられている場合**については、**報告は不要**とされています。

● 原本データ

名前	住所	電話番号	クレジットカード番号
工藤 俊彦	茨城県水戸市宮町	0291982275	4012888888881881
横井 辰雄	神奈川県三浦市南下浦町松輪	0447713808	5105105105105100
西野 典子	広島県広島市西区山田新町	0828934448	378282246310005
上田 信長	埼玉県川越市三久保町	0496365387	38520000023237
浜崎 亜子	山口県山陽小野田市大須恵	0820993331	3566002020360505

● 高度な暗号化 (AES-256)で変換されたデータ

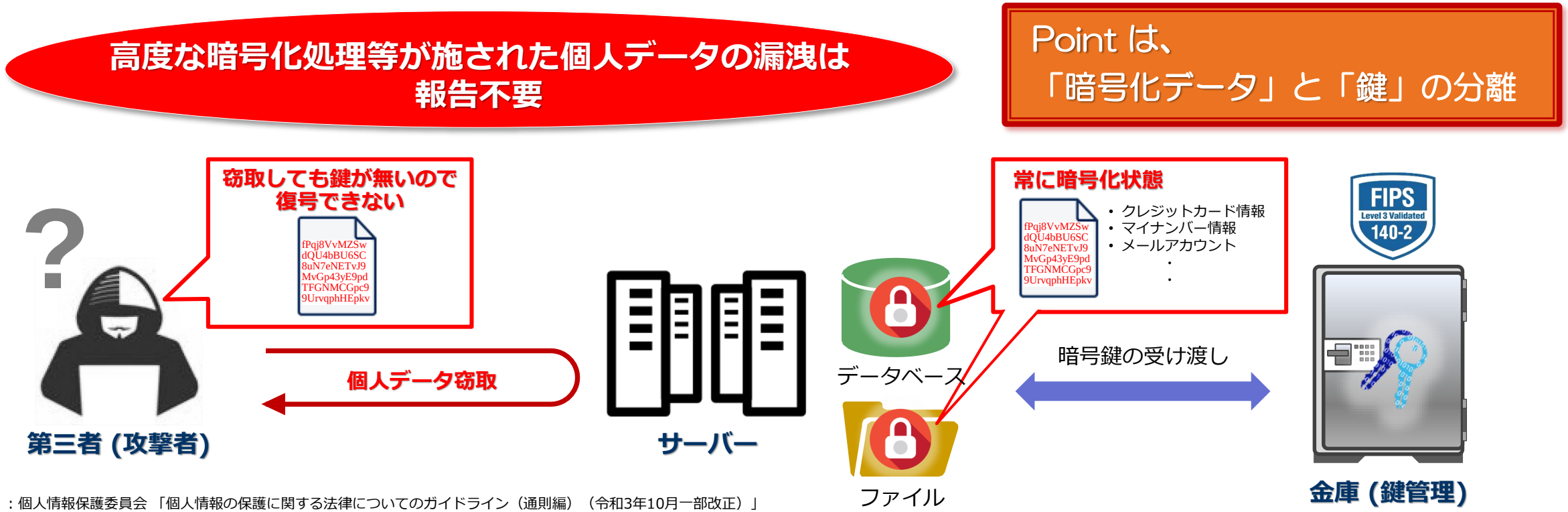
名前	住所	電話番号	クレジットカード番号
1YeV2KeUEN	2LyY1a++16y81oCE1riI1Yiy1Z6e16SK	kIAgIAAIJAQHBQ	BAABAggICAgICAgIAQgIA
1pia1IqlENiO	Yet16y81I15Wu1ZW41i51oWW1Yiy1b	AAQEBwcBAwgA	BQEABQEABQEABQEABQE
2JWP2be+E	1Yqz1YOG16y81Yqz1YOG1Yiy2JWP1b	DBACCAAAgQEC	AwcIAggCAgQGAwEAAAA
1Ii616SAENS	Yet2Ia611a+M176516y81Yiy1Ii51Im1	BgIGAAQBQMI	AAAgMAwgFAgAAAACAwc
rNWd1oWs1	+T16y81YG1YGB1bB2amN1YC/2be+1	WMDAAAgCAAkJA	UABQAwUGBgAAAgACAA

✤ AES (Advanced Encryption Standard) は、高度暗号規格として電子政府推奨暗号リスト (CRYPTREC) に登録されております。

報告及び通知義務の適用除外

個人情報の保護に関する法律についてのガイドライン (通則編) において、**「高度な暗号化その他の個人の権利利益を保護するために必要な措置」を講じた個人データ**は、報告を要しないとされています。

「第三者が見読可能な状態にすることが困難となるような**暗号化等の技術的措置としては、**適切な評価機関等により安全性が確認されている**電子政府推奨暗号リストや ISO/IEC 18033 等に掲載されている暗号技術が用いられ、それが適切に実装されていること**が考えられ」としています。



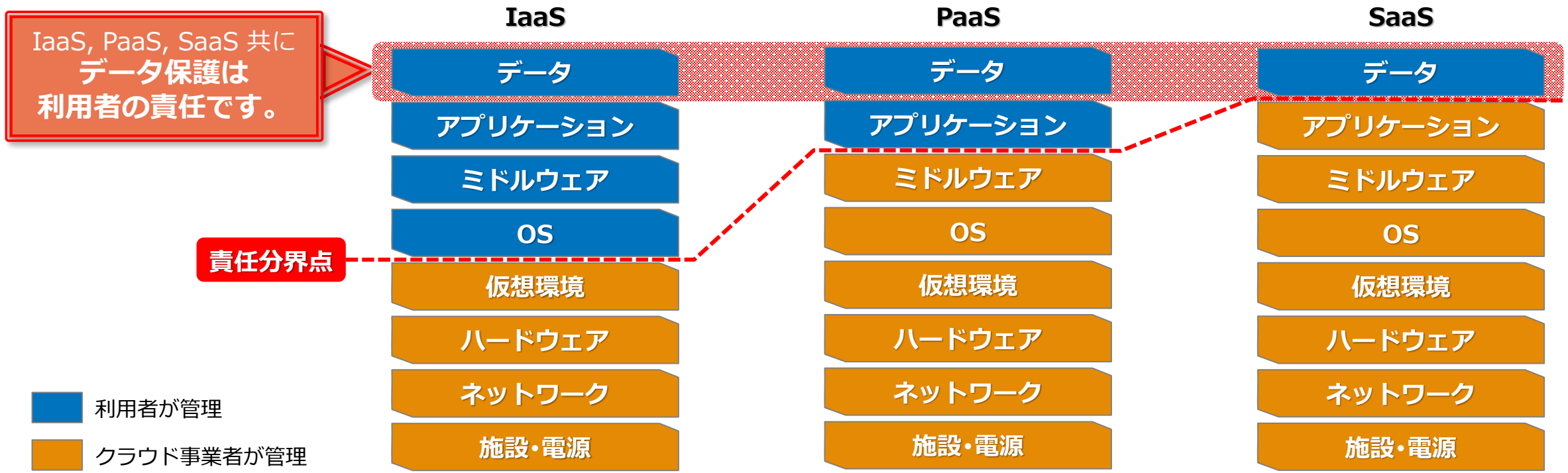
出典 ：個人情報保護委員会 「個人情報の保護に関する法律についてのガイドライン（通則編）（令和3年10月一部改正）」

クラウドからの情報漏えい、責任は誰に？

- **IaaSの責任分界点**
  仮想環境までの管理・責任をクラウド事業者が担います。
- **PaaSの責任分界点**
  OSとミドルウェアまでの管理・責任をクラウド事業者が担います。
- **SaaSの責任分界点**
  アプリケーションまでの管理・責任をクラウド事業者が担います。

第三者認証

IaaS, PaaS, SaaS 共に
データ保護は
利用者の責任です。



引用 ： 「クラウドサービス提供における情報セキュリティ対策ガイドライン（第3版）」

クラウドサービス利用に於ける暗号鍵の制御レベル

暗号化と鍵管理については、CCM (Cloud Control Matrix) のEKM-04において「鍵は (当該クラウドプロバイダの) クラウド内に保管するのではなく、クラウドの利用者または信頼できる鍵管理プロバイダが保管しなければならない。」とし、プロバイダではなく**利用者あるいは信頼できる鍵管理プロバイダが保管**することを推奨しています。

■ Cloud Security Allianceより提供されている「Cloud Control Matrix3.0.1」より

Control ID	Control Domain
EKM-01	暗号化と鍵管理: 権限付与
EKM-02	暗号化と鍵管理: 鍵生成
EKM-03	暗号化と鍵管理: 機密データの保護
EKM-04	暗号化と鍵管理: **鍵の保管とアクセス**

出典 ： Cloud Security Alliance「Cloud Control Matrix3.0.1」日本語版

CSP側で暗号鍵の管理		利用者側で暗号鍵の管理		
Cloud Native Encryption Service	Native Encryption with Tenant isolation	Bring Your Own Key (BYOK)	Hold Your Own Key (HYOK)	Bring Your Own Encryption (BYOE)
クラウドサービスプロバイダによる鍵管理。	利用者にて鍵を監視できるが、鍵はクラウドプロバイダにホスト。	利用者による鍵生成と管理。 鍵はクラウドプロバイダにホスト。 ✤ 利用者が生成した暗号鍵をクラウドプロバイダにホスト。	利用者による鍵のライフサイクル管理。(生成、保存、リキー、削除など) ✤ 利用者が保有する鍵管理サーバーで鍵のライフサイクル管理。	利用者が暗号化機能をクラウド上に展開。 ✤ 全て利用者にてコントロール。

低い ← 暗号化と鍵管理に対する顧客の制御 → 高い

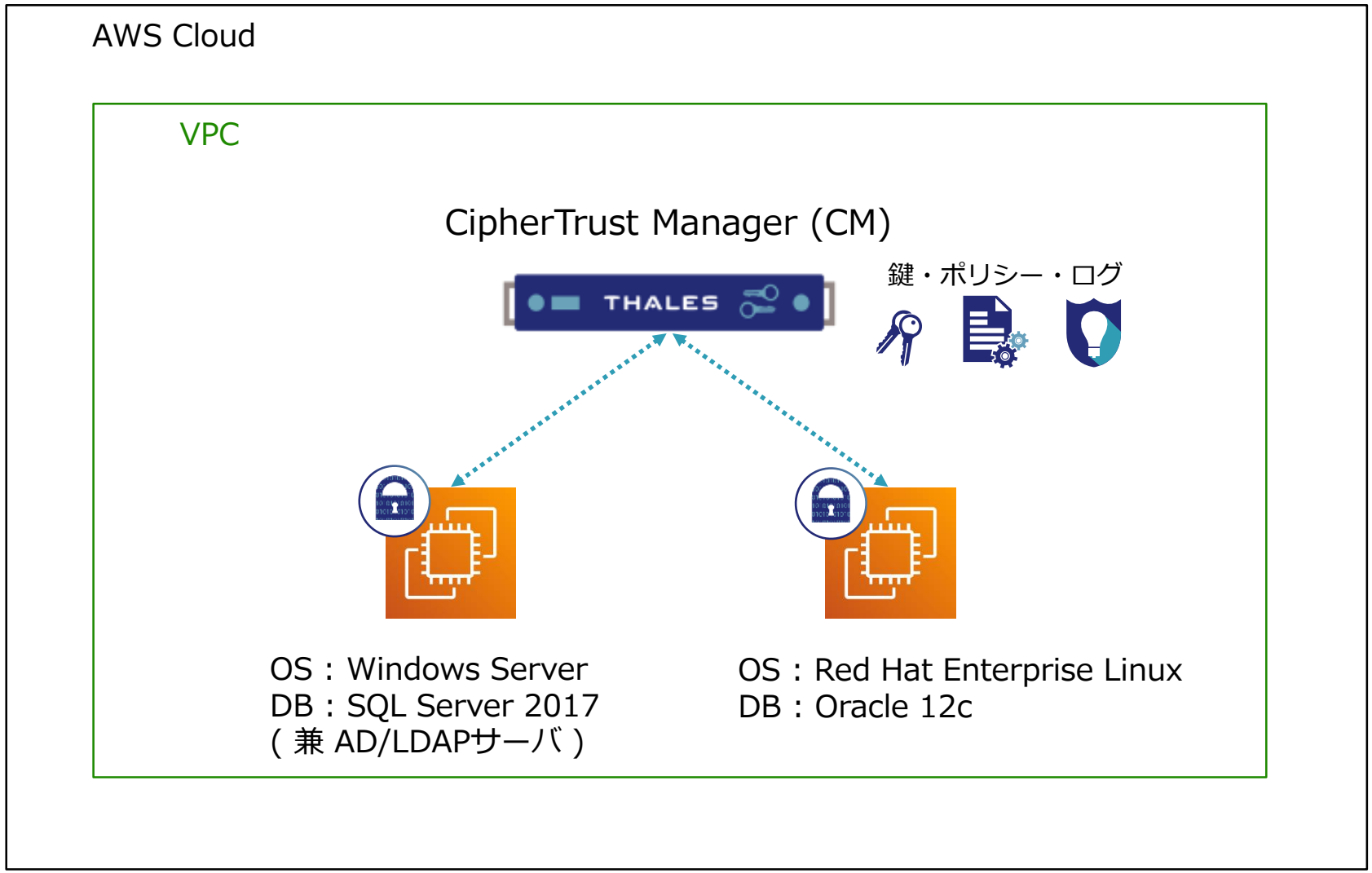
高度な暗号化と厳格な鍵管理でデータを保護

デジタル化が進むにつれ、企業が保有するデータはますます増加すると予測されています。
国内外の法令規定や情報セキュリティに関するガイドラインを基に、顧客情報や重要情報が保存されたデータベースやファイルシステムを中心に暗号化を実装することで、第三者による不正アクセスから情報漏えいを防ぐことができます。

暗号化データと鍵の保管場所を分離することで、

- **万が一情報が流出・漏えいしても、読み取れないため被害を最小限に抑えられる**
- **クラウドサービス提供事業者からデータを保護できる**
- **オンプレミスとクラウドの両方に、同様のデータガバナンスを適用できる**

データベースの透過暗号 デモ実演



お客様が抱えているデータセキュリティの課題

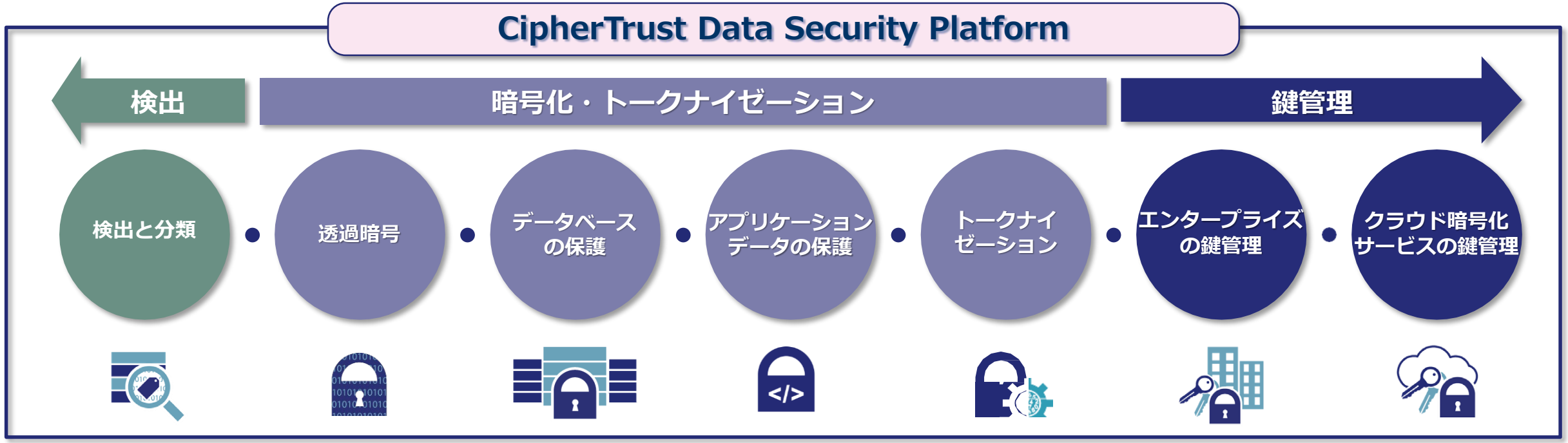
あなたの組織でデータセキュリティにこんな悩みを抱えていませんか？

1.	**データベースやファイルシステムに保存しているデータを保護したい** ✓ 大量に保存している重要なデータを秘匿化するには？ ✓ サイバー攻撃や内部不正から機密情報を守るには？ ✓ パブリッククラウドの保存データを暗号化するには？ 
2.	**データ利活用と保護対策を考えたい** ✓ 個人情報を暗号化および仮名化、匿名加工するには？ ✓ 保存データを組織全体で安全に利活用するには？ ✓ 暗号化によるパフォーマンス劣化を最小限にするには？ 
3.	**パブリッククラウド暗号化サービスの鍵管理を厳格にしたい** ✓ マルチクラウド環境で暗号鍵を一元管理するには？ ✓ 第三者による不正アクセスを防止するには？ ✓ 自社組織が独自に保有する鍵でデータを暗号化するには？ 

データセキュリティの解決策

(開発元)
THALES

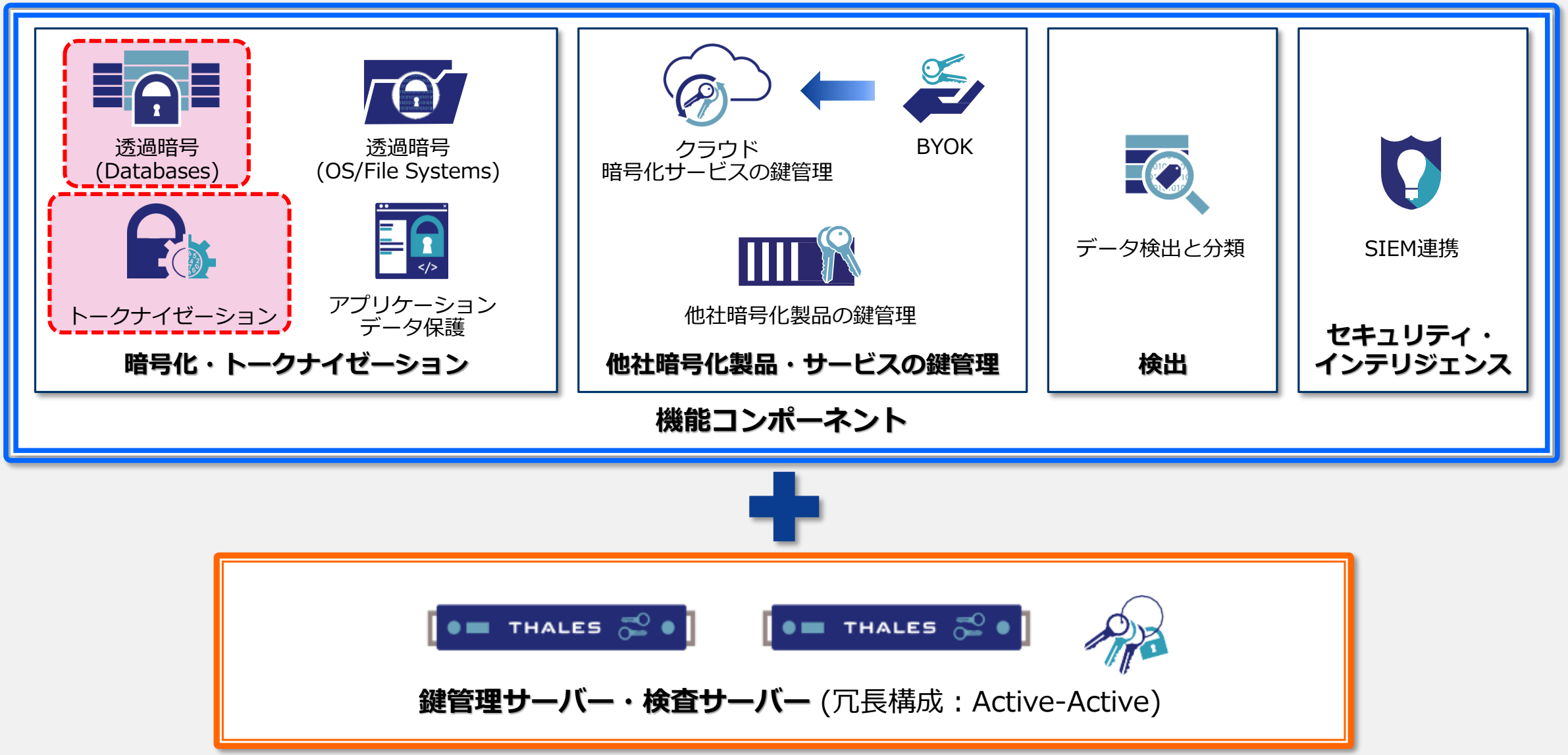
デジタルトランスフォーメーション (DX) の進展により、業種業態や企業規模を問わずパブリッククラウドサービスの利用が増加しております。情報系から基幹系まで多様なシステムでの利用が広がり、複数のクラウドサービスを使い分けるといったマルチクラウドの利用が一般的になりました。
このようにクラウド利用が進むと、保存されるデータの中には個人情報やセンシティブな情報も含まれるため、それらの情報を第三者から読み取れないように暗号化またはトークン化といった対策が必要になってきます。万が一情報が流出すると信頼を損なうだけではなく、損害賠償や訴訟問題へ発展し信用を大きく低下させてしまう可能性があります。
弊社は、重要なデータを守るため、国内外で導入実績のある Thales 社の統合データセキュリティプラットフォーム「**CipherTrust Data Security Platform**」をご提供しています。



「CipherTrust Data Security Platform」製品ラインアップ

鍵管理	**鍵管理サーバー・検査サーバー** 鍵管理とデータアクセスポリシーを一元化。	**CipherTrust Manager (CM)**
	クラウド暗号化サービスの鍵管理 IaaS/PaaS/SaaSクラウドプロバイダに対応し、 クラウドBYOKのライフサイクル管理を提供。	**CipherTrust Cloud Key Manager (CCKM)**
	他社暗号化製品の鍵管理 KMIP対応製品の暗号鍵を一元化。 TDE機能を備えたデータベース暗号鍵を一元化。	**CipherTrust KMIP Server** **CipherTrust TDE Key Management**
暗号化	**透過暗号** オンプレミス、クラウド、データベース、ファイル、 ビッグデータ環境のあらゆる場所でデータを暗号化。	**CipherTrust Transparent Encryption (CTE)**
	トークナイゼーション API連携でトークナイゼーション機能を提供。	**CipherTrust Tokenization (CT)**
	アプリケーションデータ保護 API連携で暗号化機能を提供。	**CipherTrust Application Data Protection (CADP)**
検出	**データ検出と分類** 機密データを検出、分類、保護機能を提供。	**CipherTrust Data Discovery and Classification (DDC)**

データセキュリティソリューション構成



透過暗号

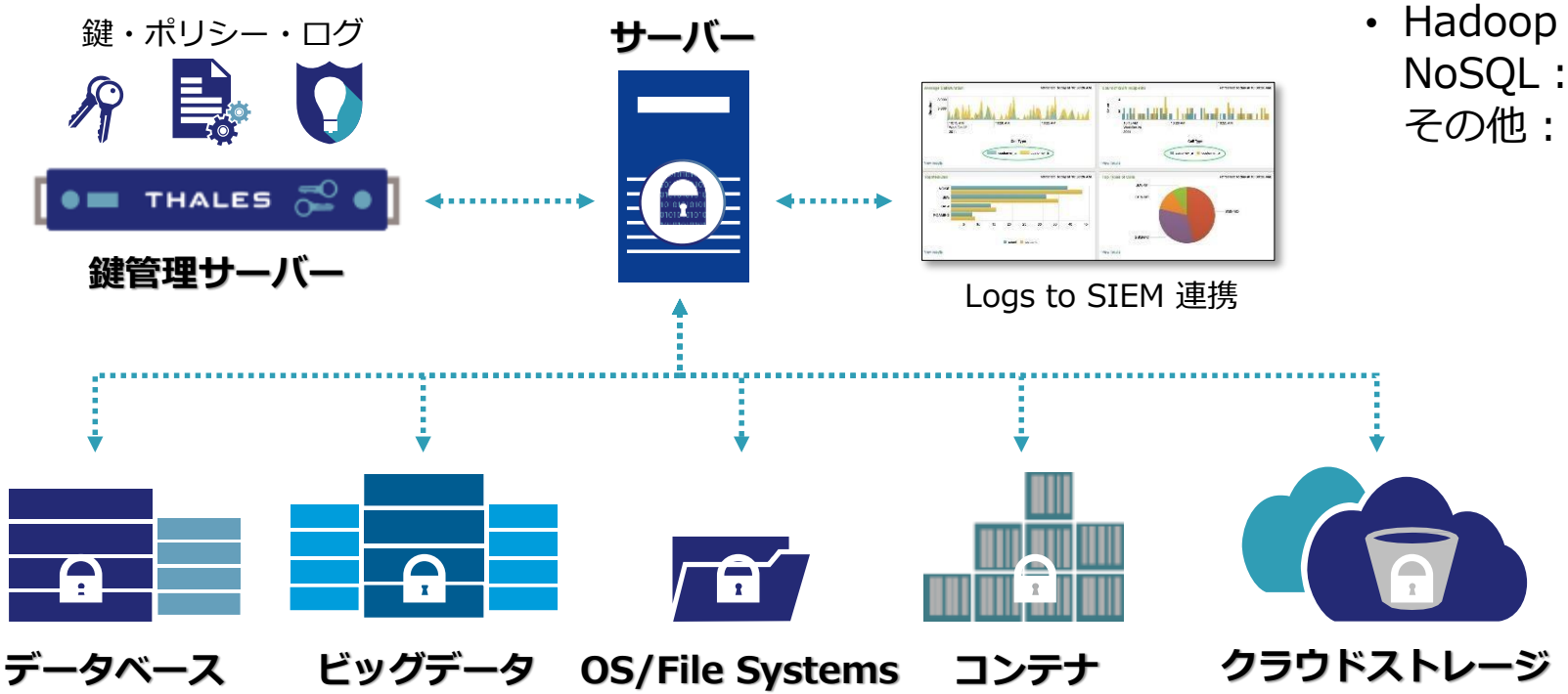
■ システム構成
- 鍵管理サーバー
- 透過暗号エージェント
  - ✤ FIPS 140-2 Level 1 認定

■ 対応プラットフォーム
- Windows Server
- Red Hat Enterprise Linux
- SuSE Linux Enterprise Server
- Ubuntu
- IBM AIX

■ 対応データベース
- IBM DB2, MySQL, Oracle, SQL Server, Sybase 他

■ 対応アプリケーション
- Microsoft, Documentum, SAP, SharePoint, カスタムアプリケーション 他

■ 対応ビッグデータ
- Hadoop：Cloudera, Hortonworks, IBM
  NoSQL：Couchbase, DataStax, MongoDB
  その他：SAP HANA, Teradata



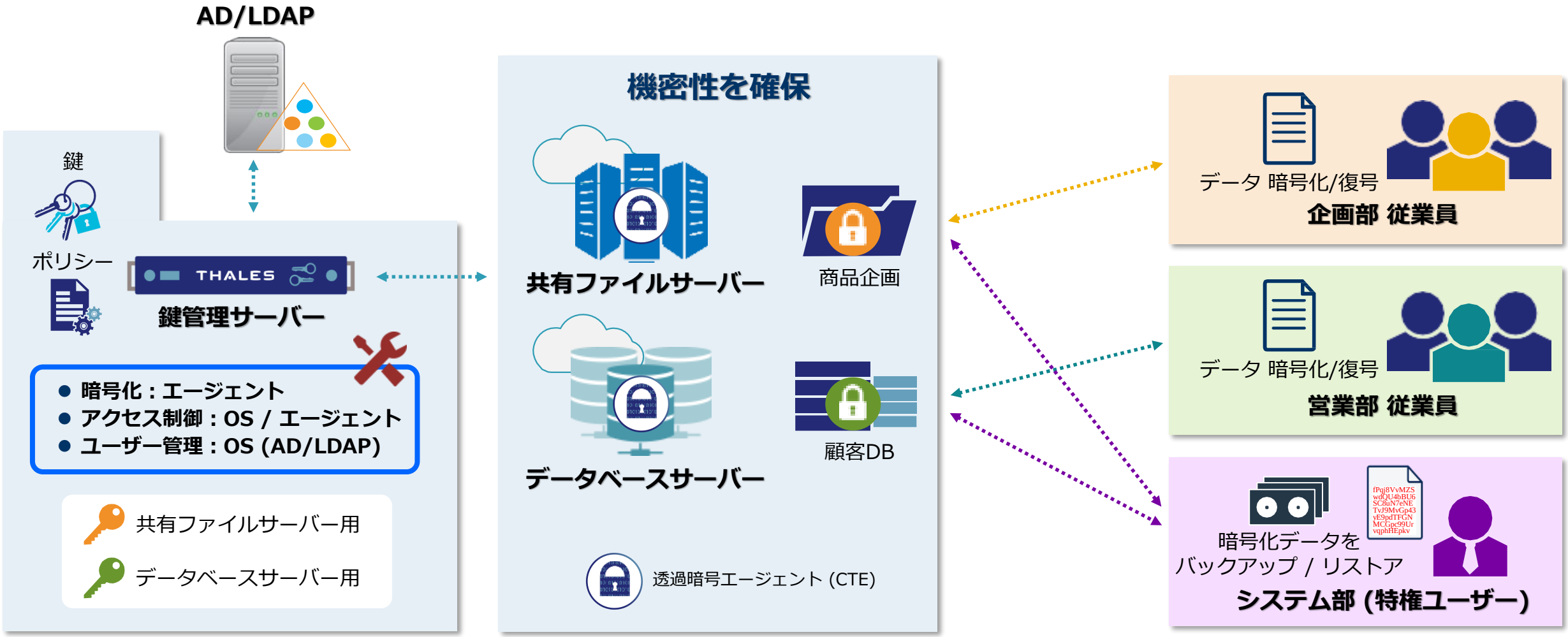
✤ オンプレミスと同様の暗号化システムをクラウド上に構築できます。

透過暗号 (オプション：自動暗号・Rekey)

透過暗号エージェント (CTE)

透過暗号 運用例

サーバー内のファイルは常に暗号化状態であり、権限を有した従業員のみデータの暗号化/復号が可能です。
特権ユーザーや第三者は復号権限がありませんので、データの中身を見れません。



トークナイゼーション ソリューション

■ システム構成
- 鍵管理サーバー
- トークナイゼーションサーバー(仮想アプライアンス)

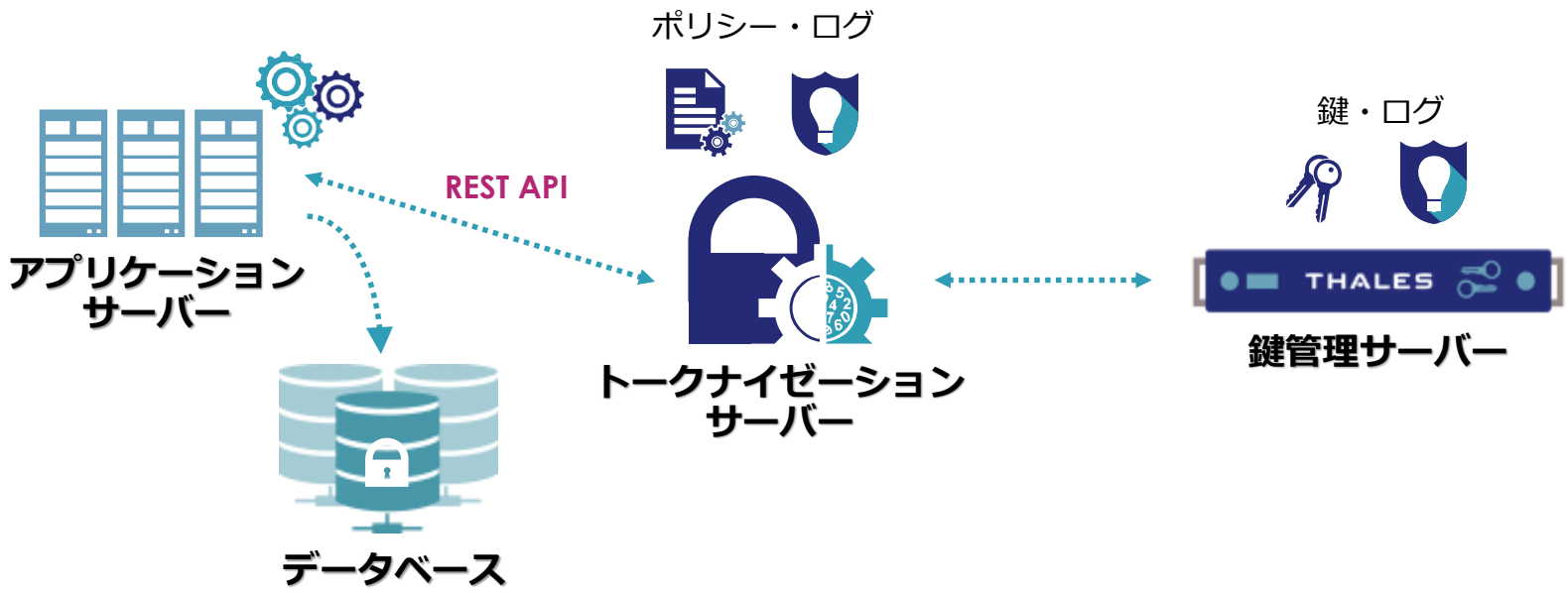
■ 提供形態
- Open Virtualization Format (OVA)
- International Organization for Standardization (ISO)
- Microsoft Hyper-V (VHD)
- Amazon Machine Image (AMI)
- Microsoft Azure Marketplace
- Google Cloud Platform

■ システム要件
- CPU：4個
- RAM：24GB(推奨)
- HDD：85GB以上

■ アプリケーション連携
- RESTful APIs

■ トークン化機能
- フォーマット保持トークン
- 指定された桁をマスキング (先頭、末尾など)
- 用途に即したテンプレートを生成

■ 開発ライブラリとAPI
- REST
- Java
- .NET



トークナイゼーション 運用例

データベースにはトークンデータが保存され、権限を有した従業員のみデータを復元 (原本に戻す) が可能です。
復元する際は、権限により原本データの一部をマスキング 「＊」(仮名化、匿名化) できますので、不正使用を防止できます。

機密性を確保

No.	カード番号	有効期限	性	名	住所	電話番号
1	8054894463027059	73/51	維鶴	嬰潅	稗黛喬詑阪惇敬圧度漬5-3-9	59-5178-4378
2	7888717189088957	42/64	愈暢	恥幾	噸壌蝋蕪寡姻鯖聾坤掃姉4-1-6	89-9401-8431
3	1507143438470031	31/31	斑約	揚卯	痢燭銚爾陽贋窪塔棲2-7-4	618-046-9484
・						
・						

トークンデータ

ポリシー

トークナイゼーション サーバー

データベース

無価値化

THALES

鍵管理サーバー

鍵 (トークン用)

トークンデータを バックアップ / リストア

システム部 (特権ユーザー)

No.	カード番号	有効期限	性	名	住所	電話番号
1	4012888888881881	03/25	山下	秀一	東京都新宿区市谷田町1-2-3	03-3606-2873
2	5105105105105100	10/22	渡部	英幸	東京都足立区古千谷本町1-2-3	03-3539-6582
3	3566002020360505	07/24	岡部	優香	東京都府中市本宿町1-2-3	042-308-1948
・						
・						

原本データ

ファイナンス部 従業員

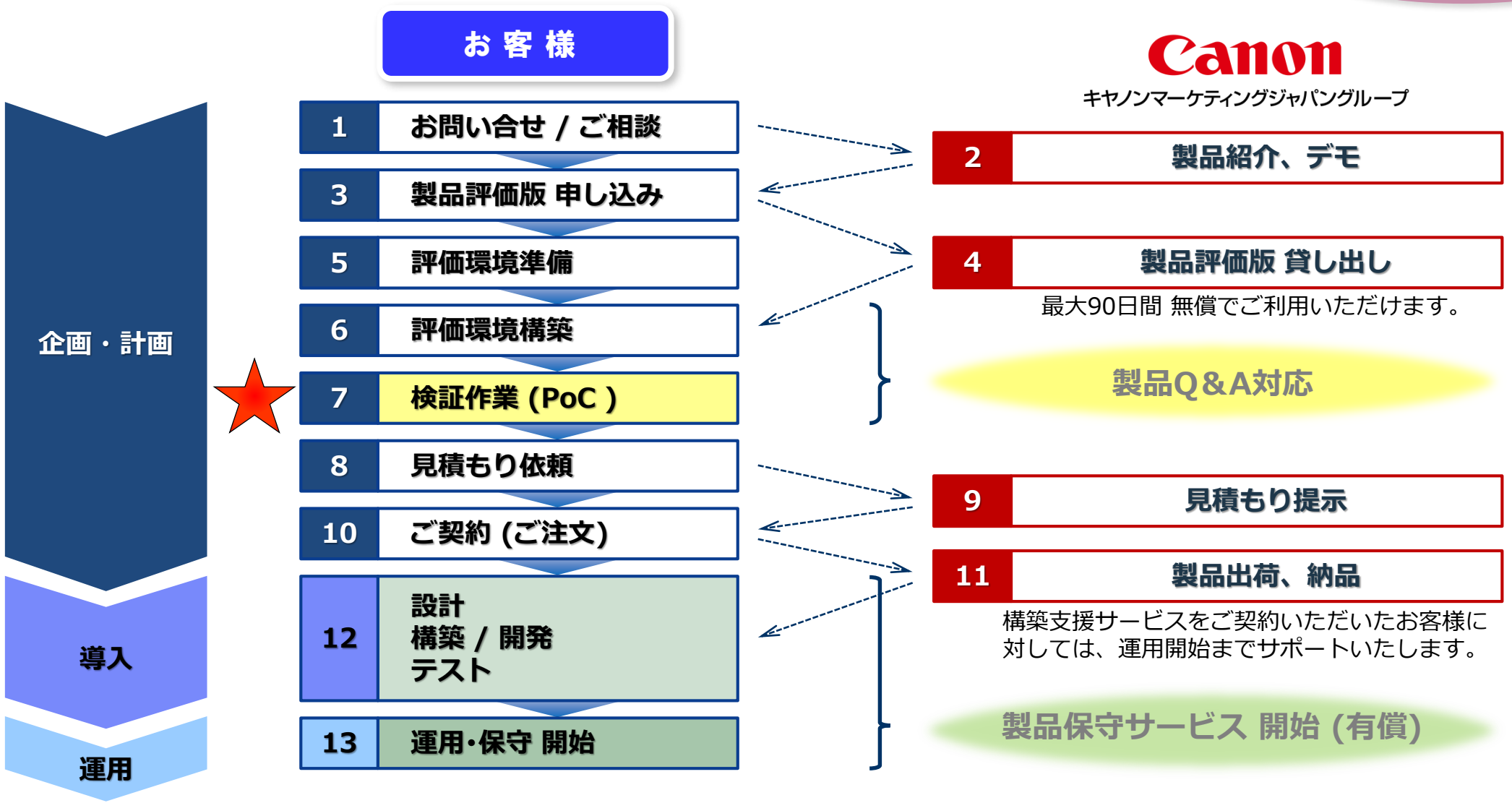
No.	カード番号	有効期限	性	名	住所	電話番号
1	401288**********	**/**	山下	**	東京都新宿区市********	**-****-****
2	510510**********	**/**	渡部	**	東京都足立区**********	**-****-****
3	356600**********	**/**	岡部	**	東京都府中市********	***-***-****
・						
・						

原本データ ＋ マスキング

マーケティング部 従業員

導入ステップ

評価版貸出



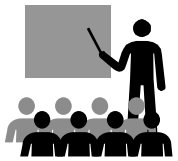
PoC : Proof of Concept (概念実証) の略称です。

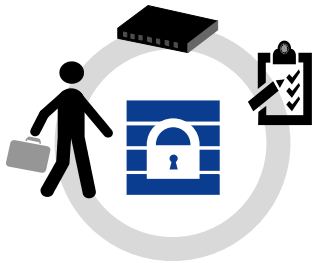
構築サービス・構築ステップ

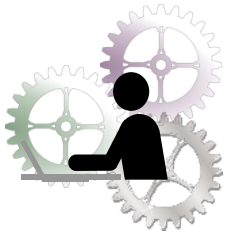
事前検討段階から設計、構築、保守に至るまで一貫したサービスを提供します。
『簡単』『迅速』『既存システムの影響最小限』といった点に軸足を置いた製品です。

一般的に運用フェーズに持っていくまでに約1ヶ月を要します。

Week 1	Week 2	Week 3	Week 4+
ご契約・キックオフ	設計	構築・テスト	運用・保守
▪ 目的・ご要件の確認 ▪ 現状環境の確認 ▪ 実装形態の確認 ▪ スケジュールの確認	▪ 構成設計 ▪ システム設計 ▪ 設計レビュー	▪ CipherTrust導入 ▪ 初期設定 ▪ カスタム設定 ▪ テスト・チューニング ▪ 管理者向け教育	▪ システム管理・監視 ▪ 継続的なチューニング ▪ バックアップ/リストア 保守開始
プロフェッショナルサービス			保守サービス



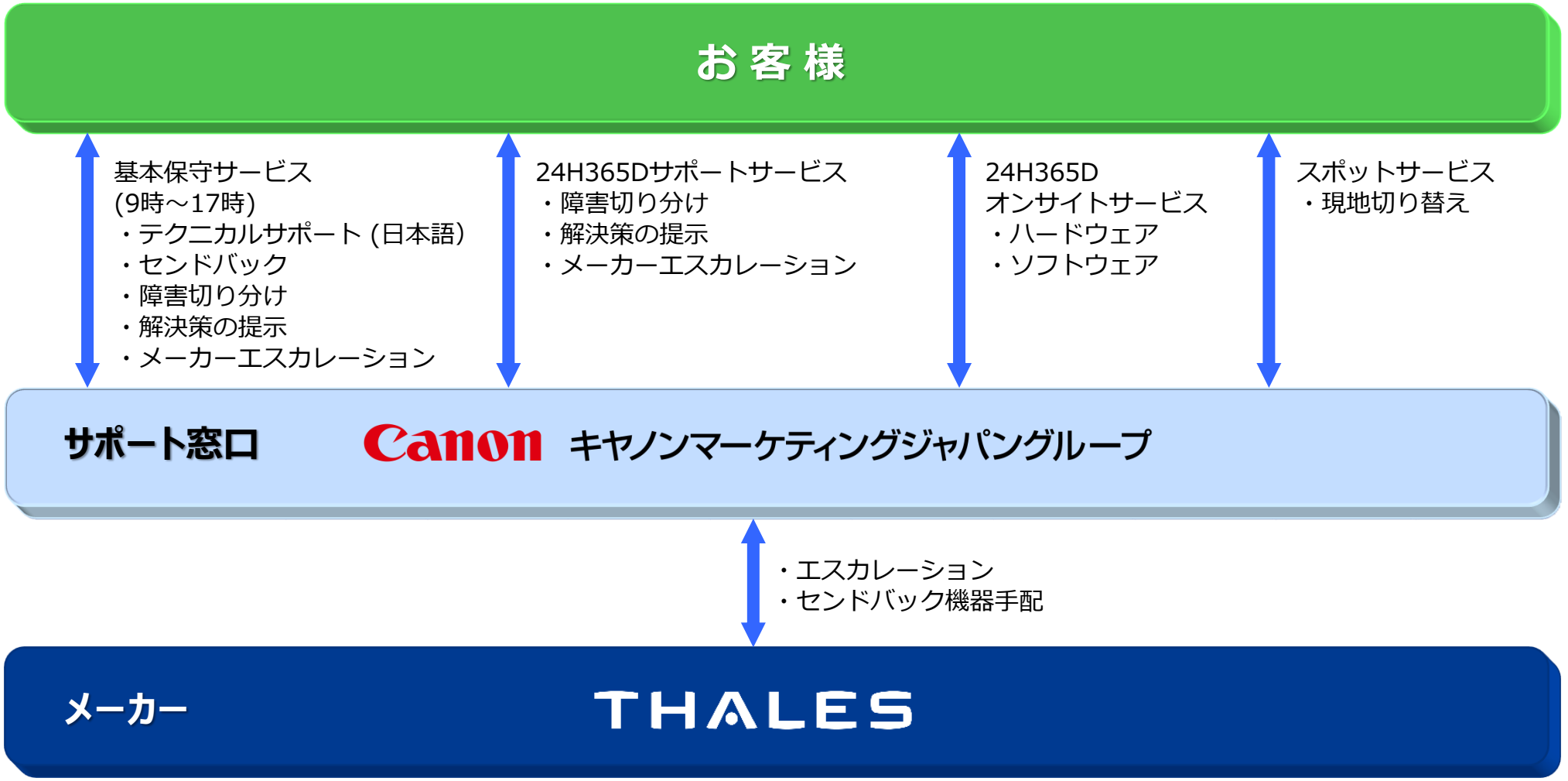




※ 構築サービスをご希望のお客様は、弊社担当営業までお問合せください。

保守サービス・体制のご紹介

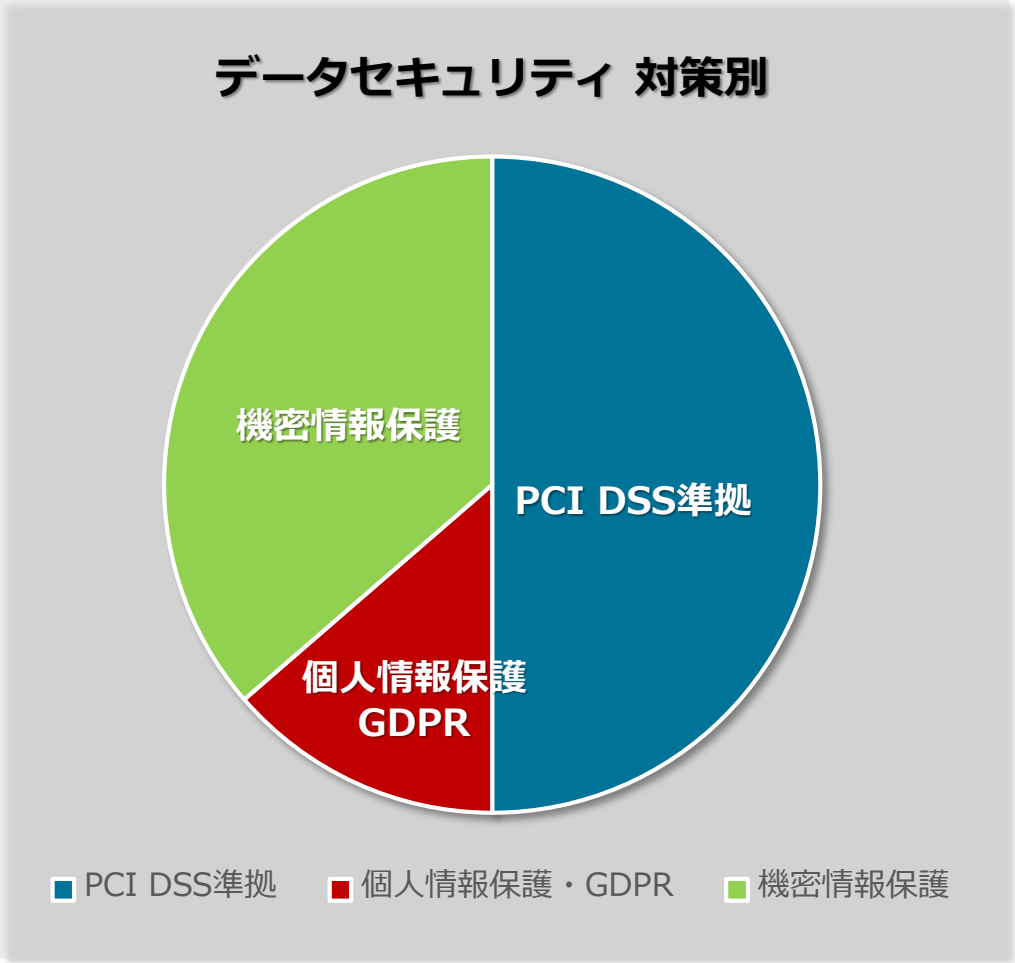
■ メーカー保守と連動し、キヤノンITSが各種サービスの1次窓口を提供します



主な導入実績

「CipherTrust Data Security Platform」は、業種業態を問わず多くのお客様にご利用いただいております。

業種・事業内容	対象システム
金融 (決済代行)	決済システム
金融 (決済代行)	決済システム
情報・通信 (決済代行)	決済システム
情報・通信 (決済代行)	決済システム
運輸	ファイルサーバー
アパレル	会員情報システム
総合小売	決済システム
ブロードバンドIP通信サービス	決済システム
エネルギー	決済システム
機械、エレクトロニクス、情報・通信	決済システム
情報・通信	クラウドストレージ
医療・介護	ファイルサーバー
自治体 (長野県)	ファイルサーバー
エレクトロニクス	ファイルサーバー
情報・通信	ファイルサーバー
食料品	ファイルサーバー
自治体 (東京都)	ファイルサーバー
情報・通信 (決済代行)	決済システム
情報・通信 (決済代行)	決済システム
運輸	ファイルサーバー
アミューズメント	DBサーバー・業務サーバー
自動車	ファイルサーバー・DBサーバー



重要情報を安全に保管

情報セキュリティ対策に取り組むことは、「企業の信頼構築」に繋がります。

高度な暗号化によるデータ保護

- AES256暗号化アルゴリズムでデータを暗号化
- 暗号鍵のライフサイクル管理を自動化
- マスキングによる柔軟なデータ保護
- ファイルやデータベースの種類を問わず暗号化

アクセス制御

- アクセス権限の最小化 (AD/LDAP連携＋独自)
- 暗号化/復号の権限設定
- 従来と変わらない操作性
- アクセス履歴を記録 (SIEM連携)

CipherTrust Data Security Platform

堅牢な暗号鍵管理

- FIPS 140-2 L1/L3 認定
- クラスタリング構成で高可用性を実現
- クラウド暗号化サービスの鍵を一元管理
- オンプレミス、クラウド、ハイブリッド環境に対応

コンプライアンス遵守

- 個人情報保護法
- 一般データ保護規則 (GDPR)
- ペイメントカード業界データセキュリティ基準 (PCI DSS)
- NISTセキュリティ基準　など

ご視聴ありがとうございました。

Canon キヤノンマーケティングジャパン株式会社

セキュリティソリューション企画本部

セキュリティソリューション企画部

ご相談・お問い合わせはこちら

https://cweb.canon.jp/it-sec/solution/data-security-platform/