CipherTrust Data Security Platform

THALES

DXで浮上した
データセキュリティの課題と解決策

Canon

キヤノンマーケティングジャパン株式会社

本日のアジェンダ

1. デジタル社会とサイバー脅威の動向
2. 情報セキュリティと個人情報保護
3. データセキュリティソリューションのご紹介

データ・ドリブン・エコノミー時代へ

全てがデータでつながる時代を迎え、生活者の購買情報や交友関係、健康状態、位置情報にとどまらず、気候や交通などの社会環境に関する情報、企業の事業運営に関わる情報など、**あらゆる情報がデジタルデータとして捕捉**できるようになり、集められた情報は分析や予測に活用され、結果が現実社会にフィードバックされる時代を迎えました。
このように、リアルな世界から集めたデータが新たな価値を生み出し、あらゆる企業･産業･社会を変革していく一連の経済活動を『**データ・ドリブン・エコノミー**』と呼んでいます。

DXに終わりはない

DXの目的は、「**製品やサービス、ビジネスモデルを変革するとともに、業務そのものや組織、プロセス、企業文化･風土を変革し、競争上の優位性を確立すること**」であり、一過性の活動ではなく、その状態を維持できなければなりません。
ビジネス環境が常に変化し続けテクノロジーが進化し続ける中、競争優位性を維持するには企業が変化し続けなければならず、DXの取り組みに終わりはないと考えるべきです。
デジタル技術を活用した業務や、ビジネス変革という具体的なDXの実践による成果が、競争優位の源泉となっている状態を維持することに加えて、DXに向けた環境整備と企業内変革によって全社的な環境が整備され、誰もが意識することなくDXが推進されている状況をつくりあげていくことが求められます。

1 既存事業の継続的優位性の低下

漸進型イノベーション推進力
- デジタル技術やデータを活用して既存の事業や業務を高度化･変革する

2 ディスラプターによる業界破壊

不連続型イノベーション創出力
- デジタルを前提とした新規顧客価値や新たなビジネスを創出する

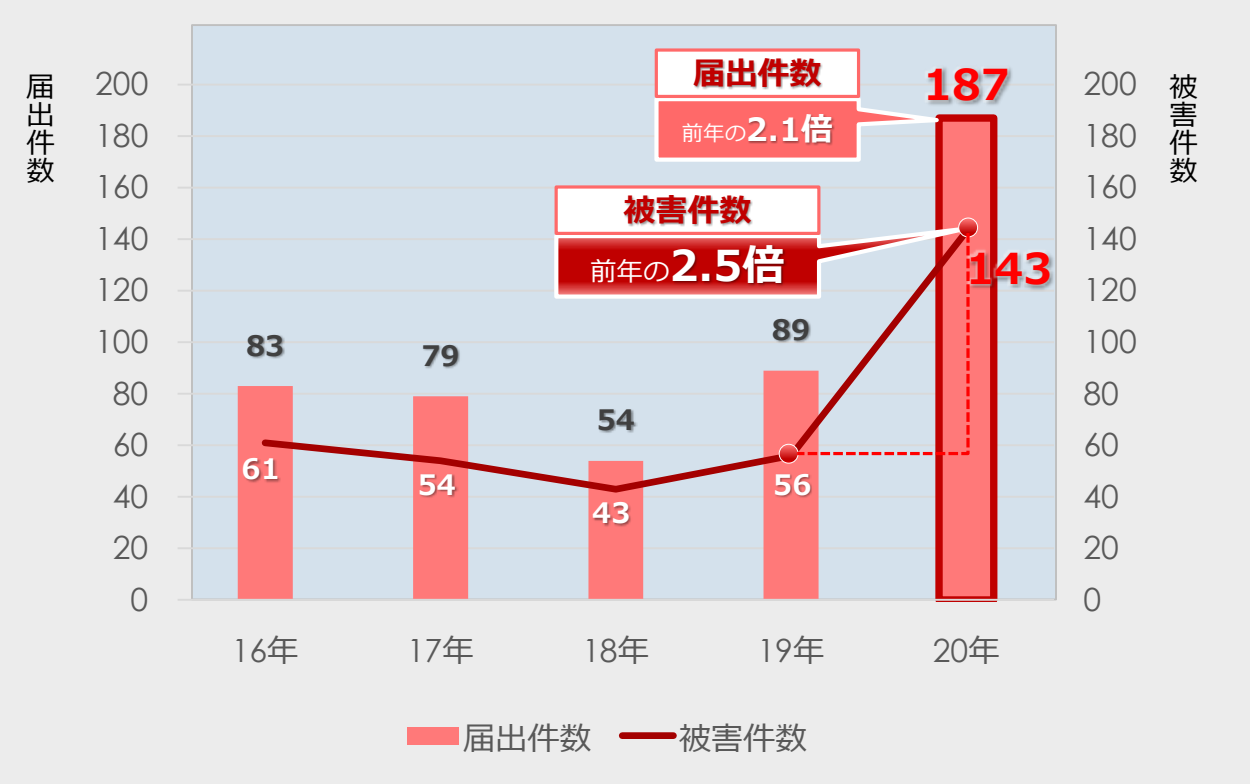
3 デジタルエコノミーによる構造変革

変化適応力
- 社会や市場のデジタル化など、時代の変化に適応する

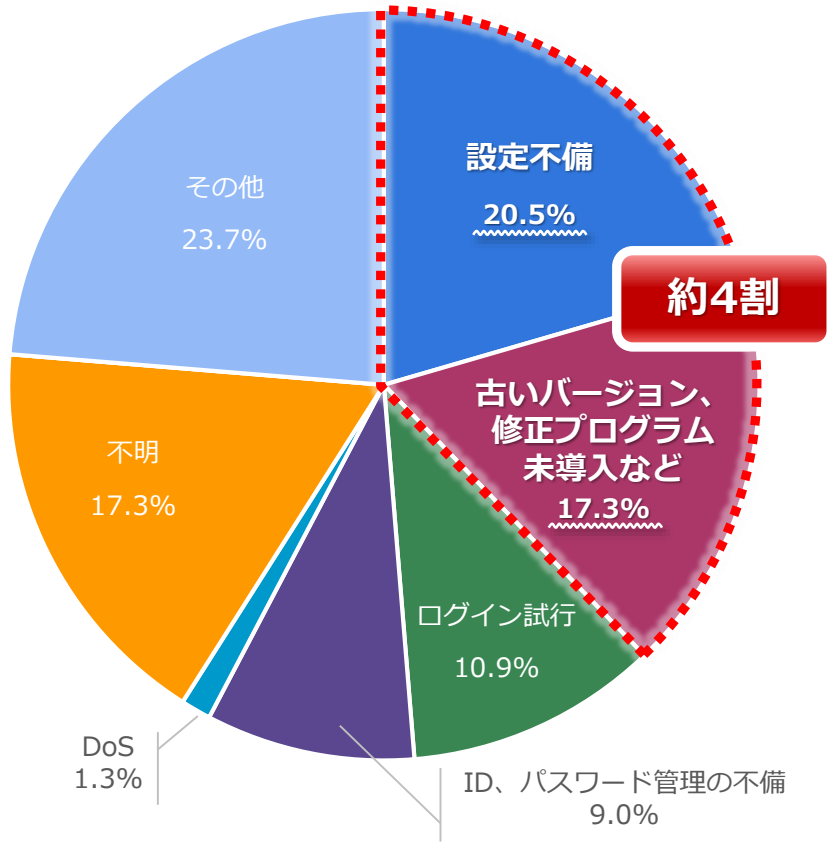
コンピュータ不正アクセス届出の推移

情報処理推進機構 (IPA) セキュリティセンターがまとめた「コンピュータウイルス・不正アクセスの届出状況」によると、2020年に寄せられた**不正アクセス届け出件数は前年の2.1倍**の187件でした。そのうち**被害があった届け出件数は前年の2.5倍**の143件となりました。

不正アクセス件数



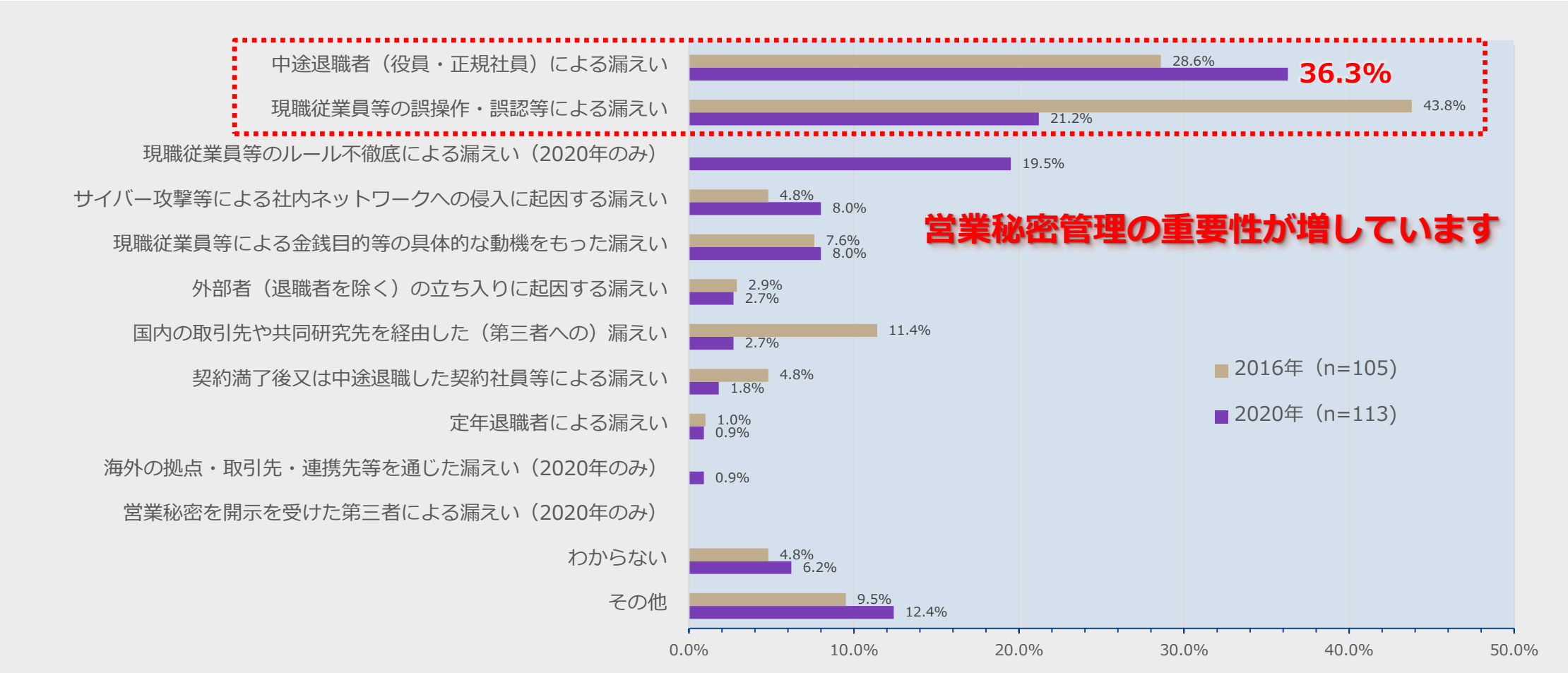
不正アクセス被害の原因別割合



出典 ： IPA 独立行政法人 情報処理推進機構 「コンピュータウイルス・不正アクセスの届出状況［2020年（1月～12月）］」

企業における営業秘密管理に関する実態調査2020

情報処理推進機構 (IPA)が公開した「企業における営業秘密管理に関する実態調査2020」によると、漏えいルートでは「中途退職者」による漏えいが増加し、**内部不正を原因とする情報漏えいは減少傾向にはない**ことが分かります。



出典 ： IPA 独立行政法人 情報処理推進機構 「企業における営業秘密管理に関する実態調査 2020」

サイバー攻撃による被害事例

経営に大きな影響を及ぼすセキュリティ事件･事故が急増

2021年5月14日時点

2021年4月 ： 大手ゼネコンのグループ会社 サイバー攻撃を受け機密情報が流出

- 海外グループ会社がサイバー攻撃を受け、機密情報が流出した可能性
- 一部を闇サイトで公開し、金銭要求される

2021年4月 ： 光学機器大手の米子会社 サイバー攻撃を受け機密情報が闇サイトで公開

- アメリカの子会社がサイバー攻撃を受け、機密情報などが流出した可能性
- 盗まれた情報が闇サイトに公開される

2021年5月 ：センサー機器大手 サイバー攻撃を受け個人情報が流出した可能性

- サイバー攻撃を受け、海外支店関係者の個人情報が流出した可能性
- 闇サイトで公開、情報の買い取りを要求される

2021年5月 ：印刷機器大手 サイバー攻撃を受け情報の一部が流出した可能性

- サイバー攻撃を受け、米国子会社が利用していたファイルサーバーから情報の一部が流出した可能性
- 情報が外部に公開される

2021年5月 ：POS (販売時点情報管理) システム大手 サイバー攻撃を受け金銭要求

- フランスやドイツなど欧州4拠点でサイバー攻撃を受け、情報を盗み取られた可能性
- 金銭を要求するメールが送りつけられる

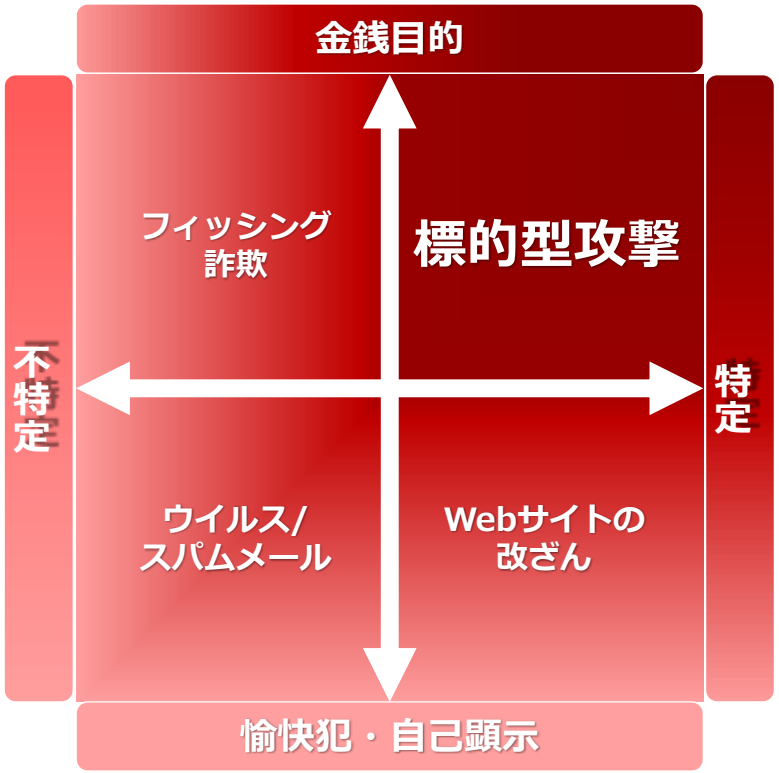
日本企業を狙うサイバー攻撃が拡大

サイバー攻撃の主体

サイバー攻撃は何らかの意図をもった者が、その目的を達成するために使う手段です。

攻撃主体	攻撃手法
サイバー犯罪組織	個人情報やクレジットカード情報などを盗み、その情報をマネタイズすることで資金を得るタイプの組織を指す。
反社会的組織	企業から機密情報や個人情報など、世間に公表されては困るような情報を何らかの形で搾取し、金銭を要求する。
産業スパイ	ライバル企業などの情報システムに侵入し、機密情報や知的財産をターゲットに活動する。 ソーシャルエンジニアリングや標的型攻撃などを駆使して情報を搾取する。
テロリスト	社会通念では理解しがたい信念を持ち、自分たちの要求を通すためにあらゆる手段を使って国家や組織に脅しをかける。
内部犯行	会社への恨みや金銭目的からライバル企業へデータ提供を行うなど。
愉快犯	趣味や知的好奇心、技術検証など、悪意の伴わない迷惑行為が特徴で、多くは個人の趣味の延長として行われる。

攻撃目的の変化



あらゆる企業・組織が、身代金要求型サイバー攻撃の標的に

情報セキュリティ対策の考え方

企業や組織で管理する紙文書や電子データ、情報システム等を「情報資産」と呼びます。これまで多くの場合、情報資産はオフィスの中で管理されておりましたが、テレワークの普及によって情報資産はインターネット上を流れ、持ち運びが容易なノートパソコン等で利用されるようになりました。そのため、**ネットワーク上での通信の盗聴や改ざん、ウイルス感染、紛失、破壊等の脅威にさらされ、情報漏えいなどの事故発生につながるリスク**が高まっております。

情報セキュリティは、**情報のライフサイクルを通じて情報のCIAを確保**する取り組みです。それは、企業活動の基本となる資産である情報を守ることであり、企業活動が健全に行われることを確保するための努力に他なりません。
情報セキュリティ対策は情報を取り扱う過程に関わる全て (技術、人、組織、物理の4領域) において確実に実施されなければなりません。

技術 	ウイルス対策ソフトやファイアウォールなどの正しい配置と運用による防御、 ならびに常時監視、定期チェックによる検知・発見
人 	従業員一人ひとりの規則遵守 (コンプライアンス)、判断、目配り気配り、運用と管理
組織 	ルール作り、ルールを守る取り組み、ルールが守れるPDCA
物理 	オフィスへの入退室・施錠管理、PCなど情報機器やUSBメモリ・紙などの記録媒体の管理 (移動・輸送・廃棄も含めた管理)

情報セキュリティを確保するには

企業における情報セキュリティは、**各組織が保有する情報資産を守るにあたって自ら責任を持って確保**すべきものであり、
情報セキュリティポリシーは、各組織が事業内容に応じて自主的に策定するものです。
予め、情報セキュリティを確保するための**方針、体制、対策などを包括的に定めた文書を策定**しておくことが重要です。

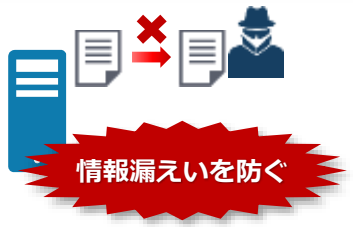
情報セキュリティ対策 (例)

- ■ 経営者層
  - 組織としての体制の確立
    - 迅速かつ継続的に対応できる組織内体制の構築 (CSIRT)
    - 予算の確保と継続的な対策実施
    - セキュリティポリシーの策定
  - 情報リテラシーや情報モラルの向上
    - コンプライアンス教育の徹底、罰則の周知
    - 退職時に秘密保持契約締結
- ■ セキュリティ担当者
  - 被害の予防 / 対応力の向上
    - 情報の管理とルール策定
    - セキュリティ教育・インシデント訓練
    - サイバー攻撃に関する情報収集
- ■ システム管理者
  - 被害の予防 / 早期発見
    - セキュアなシステム設計
    - アクセス制御･データの暗号化
    - ネットワーク分離
    - ネットワーク監視･防御
    - 操作履歴やシステムログの取得と継続的な監視
    - 影響調査および原因の追究、対策強化
- ■ 従業員、職員
  - 情報リテラシーの向上
    - セキュリティ教育の受講
  - 被害を受けた後の対応
    - CSIRTへ連絡
- ■ 委託元組織
  - 被害の予防
    - 業務委託や情報管理における規則の徹底
    - 信頼できる委託先、取引先の選定
    - 委託先からの納品物の検証
    - 契約内容の確認
    - 委託先組織の管理
  - 被害を受けた後の対応
    - 影響調査および原因の追究、対策の強化
    - 被害への補償
- ■ 委託先組織
  - 被害の予防
    - セキュリティの認証取得 (ISMS、Pマーク、ISMAP等)
    - 各種ガイドラインを基に情報セキュリティ対策実施
  - 被害を受けた後の対応
    - 委託元への連絡

公的機関が発行しているガイドライン等を活用
「サイバーセキュリティ経営ガイドライン Ver2.0」
https://www.meti.go.jp/policy/netsecurity/downloadfiles/guide2.0.pdf

✣ 経済産業省が独立行政法人情報処理推進機構（IPA）とともに策定

C 機密性 (Confidentiality)

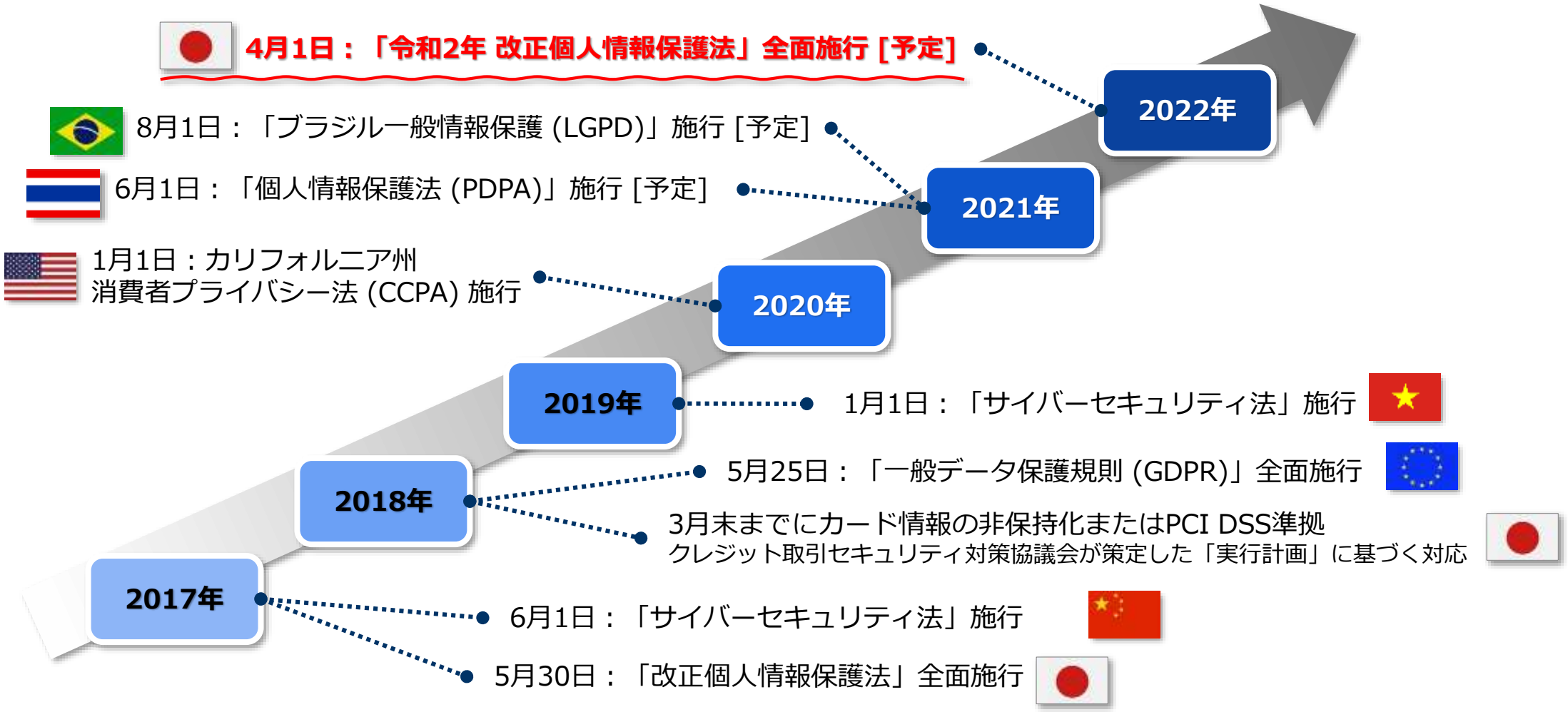


I 完全性 (Integrity)

A 可用性 (Availability)

各国のプライバシー保護規制・ガイドライン

世界各国で、個人データなどの自国外・地域外への移転を規制する「**越境移転規制**」と「**データローカライゼーション**」の導入が加速しています。



個人情報保護法改正「いわゆる3年ごと見直し」

2022年4月1日施行

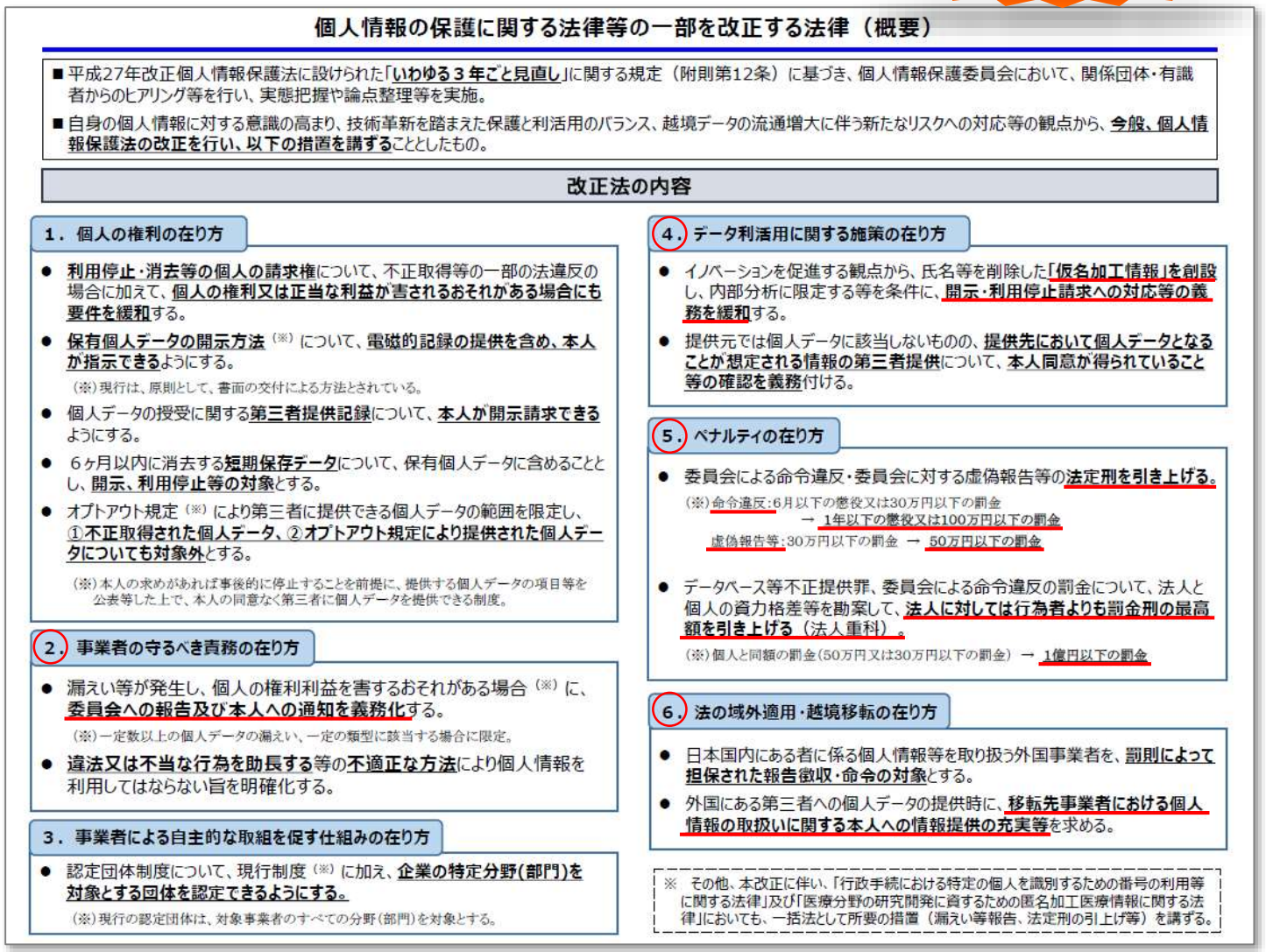
2020年(令和２年)３月10日に第201回通常国会に提出された「**個人情報の保護に関する法律等の一部を改正する法律案**」は、2020年(令和２年)６月５日の国会において**可決、成立**し、2020年(令和２年)６月12日に公布されました。改正法の施行は一部を除き、公布後２年以内となります。

データ活用が加速

仮名加工情報の創設

《 メリット 》

- 利用目的の変更の規定が適用されなくなる
- 利用目的の変更の範囲に制限がなくなる
- 漏えい等の場合の個人情報保護委員会への報告義務がない（勧告･命令の場合を除く）
- 開示、訂正等、利用停止等の請求に対応する必要がなくなる
- 安全管理措置に関し滅失、毀損の防止を図る必要がなくなる。



個人情報の保護に関する法律等の一部を改正する法律（概要）

■平成27年改正個人情報保護法に設けられた「いわゆる３年ごと見直し」に関する規定（附則第12条）に基づき、個人情報保護委員会において、関係団体･有識者からのヒアリング等を行い、実態把握や論点整理等を実施。

■自身の個人情報に対する意識の高まり、技術革新を踏まえた保護と利活用のバランス、越境データの流通増大に伴う新たなリスクへの対応等の観点から、今般、個人情報保護法の改正を行い、以下の措置を講ずることとしたもの。

改正法の内容

1．個人の権利の在り方

- 利用停止･消去等の個人の請求権について、不正取得等の一部の法違反の場合に加えて、個人の権利又は正当な利益が害されるおそれがある場合にも要件を緩和する。
- 保有個人データの開示方法（※）について、電磁的記録の提供を含め、本人が指示できるようにする。
  （※）現行は、原則として、書面の交付による方法とされている。
- 個人データの授受に関する第三者提供記録について、本人が開示請求できるようにする。
- ６ヶ月以内に消去する短期保存データについて、保有個人データに含めることとし、開示、利用停止等の対象とする。
- オプトアウト規定（※）により第三者に提供できる個人データの範囲を限定し、①不正取得された個人データ、②オプトアウト規定により提供された個人データについても対象外とする。
  （※）本人の求めがあれば事後的に停止することを前提に、提供する個人データの項目等を公表等した上で、本人の同意なく第三者に個人データを提供できる制度。

2．事業者の守るべき責務の在り方

- 漏えい等が発生し、個人の権利利益を害するおそれがある場合（※）に、委員会への報告及び本人への通知を義務化する。
  （※）一定数以上の個人データの漏えい、一定の類型に該当する場合に限定。
- 違法又は不当な行為を助長する等の不適正な方法により個人情報を利用してはならない旨を明確化する。

3．事業者による自主的な取組を促す仕組みの在り方

- 認定団体制度について、現行制度（※）に加え、企業の特定分野(部門)を対象とする団体を認定できるようにする。
  （※）現行の認定団体は、対象事業者のすべての分野(部門)を対象とする。

4．データ利活用に関する施策の在り方

- イノベーションを促進する観点から、氏名等を削除した「仮名加工情報」を創設し、内部分析に限定する等を条件に、開示･利用停止請求への対応等の義務を緩和する。
- 提供元では個人データに該当しないものの、提供先において個人データとなることが想定される情報の第三者提供について、本人同意が得られていること等の確認を義務付ける。

5．ペナルティの在り方

- 委員会による命令違反･委員会に対する虚偽報告等の法定刑を引き上げる。
  （※）命令違反：6月以下の懲役又は30万円以下の罰金 → 1年以下の懲役又は100万円以下の罰金
  虚偽報告等：30万円以下の罰金 → 50万円以下の罰金
- データベース等不正提供罪、委員会による命令違反の罰金について、法人と個人の資力格差等を勘案して、法人に対しては行為者よりも罰金刑の最高額を引き上げる（法人重科）。
  （※）個人と同額の罰金（50万円又は30万円以下の罰金） → 1億円以下の罰金

6．法の域外適用･越境移転の在り方

- 日本国内にある者に係る個人情報等を取り扱う外国事業者を、罰則によって担保された報告徴収･命令の対象とする。
- 外国にある第三者への個人データの提供時に、移転先事業者における個人情報の取扱いに関する本人への情報提供の充実等を求める。

※ その他、本改正に伴い、「行政手続における特定の個人を識別するための番号の利用等に関する法律」及び「医療分野の研究開発に資するための匿名加工医療情報に関する法律」においても、一括法として所要の措置（漏えい等報告、法定刑の引上げ等）を講ずる。

出典 ：個人情報保護委員会 「個人情報の保護に関する法律等の一部を改正する法律案」（令和２年６月12日）公布

保護すべき情報とリスク軽減策

個人データや機密データを取り扱う企業は、そのデータをビジネスで活用するだけでなく情報漏えい等のセキュリティインシデントから守らなくてはなりません。
コンプライアンス要件を満たすデータ保護対策を示します。

遵守要件		保護対象例	データ保護対策
改正個人情報保護法	個人を識別できるもの	• 本人の氏名、住所、電話番号、生年月日、電話番号、メールアドレスなど • 本人の氏名を組み合わせて個人が特定できる情報 • 特定の個人を識別できる音声や画像、映像情報	• 暗号化 • トークン化 • マスキング • アクセス制御 • 監査･検知
	個人識別符号	• マイナンバーやパスポート番号、基礎年号番号、運転免許証番号、住民票コード、健康保険証番号など公的な番号 • DNA配列や顔、容姿、虹彩、声紋、静脈、挙動の特徴、指紋	
GDPR	個人データ	• 本人の氏名や所在地、識別番号、メールアドレス 、IPアドレス、Cookie、GPSなどの情報、クレジットカード情報、パスポート情報、身体的、生理学的、遺伝子的、精神的、経済的、文化的、社会的固有性に関して識別され得る情報	• 暗号化 • トークン化 • マスキング • アクセス制御 • 監査･検知
PCI DSS	クレジットカード情報	• プライマリアカウント番号 (PAN)、カード会員名、有効期限、サービスコード	• 暗号化 • トークン化 • マスキング • アクセス制御 • 構成管理 • 監査･検知

クラウド環境においてもコンプライアンスは必須

経営者が認識する必要のある「3原則」と「重要10項目」

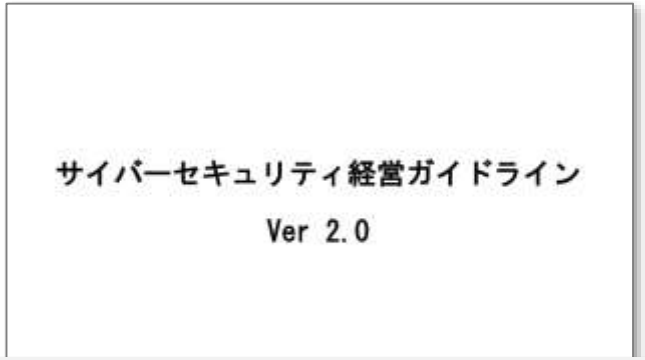
「**サイバーセキュリティ経営ガイドライン Ver2.0**」は、経営者がサイバー攻撃から企業を守るための理念や行動を記したガイドラインのこと。**経営者が認識すべきサイバーセキュリティに関する原則（3原則）**や、**トップダウンで取り組むべき項目（重要10項目）**などで構成されています。

■ 経営者が認識すべき3原則

1. 経営者は、サイバーセキュリティリスクを認識し、リーダーシップによって対策を進めることが必要
2. 自社は勿論のこと、ビジネスパートナーや委託先も含めたサプライチェーンに対するセキュリティ対策が必要
3. いついかなる場合においても、サイバーセキュリティリスクや対策に係る情報開示など、コミュニケーションが必要

■ サイバーセキュリティ経営の重要10項目

1. セキュリティリスクの認識と組織全体での対応方針の策定
2. セキュリティリスク管理体制の構築
3. セキュリティ対策のための資源確保
4. セキュリティリスクの把握とリスク対応に関する計画の策定
5. セキュリティリスクに対応するための仕組みの構築
6. セキュリティ対策においてPDCAサイクルを実施する
7. インシデント発生時の緊急対応体制をつくる
8. インシデント被害発生時の復旧体制の整備
9. サプライチェーン全体の対策と状況把握
10. 情報入手と情報共有およびその有効活用



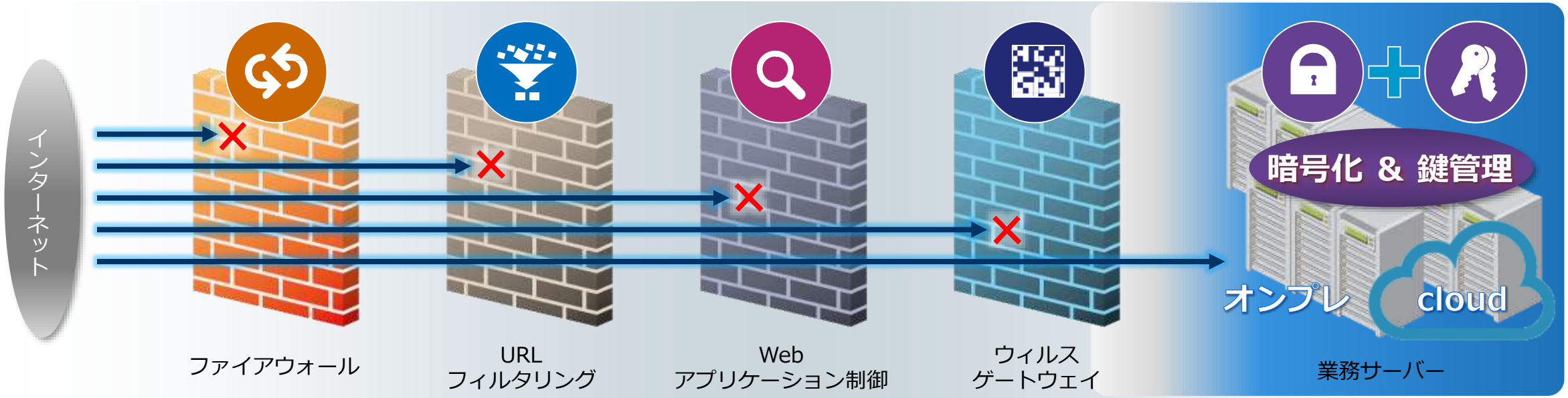
セキュリティ対策の実施をコストと捉えるのではなく、将来の事業活動・成長に必須なものと位置づけ、投資として捉えることが重要です。

出典 ：経済産業省が公開した資料「サイバーセキュリティ経営ガイドライン Ver.2.0［平成29年11月16日］」

高度化・長期化する攻撃「防ぎ切れない」を前提に

企業では、さまざまなインシデントが毎日のように発生しています。しかも攻撃は日々高度化し、情報セキュリテイ対策はこれまでの防御型では防げないものが数多くみられます。情報セキュリテイ担当者は、日々発生するインシデントに対応していかねばならない時代に直面しています。

Step1	Step2	Step3	Step4	Step5
境界防御	ウイルス対策ソフト	脆弱性対応	ネットワーク可視化	暗号化＆鍵管理



ネットワーク・アプリケーションによるセキュリティ対策

データセキュリティ対策

お客様が抱えているデータセキュリティの課題

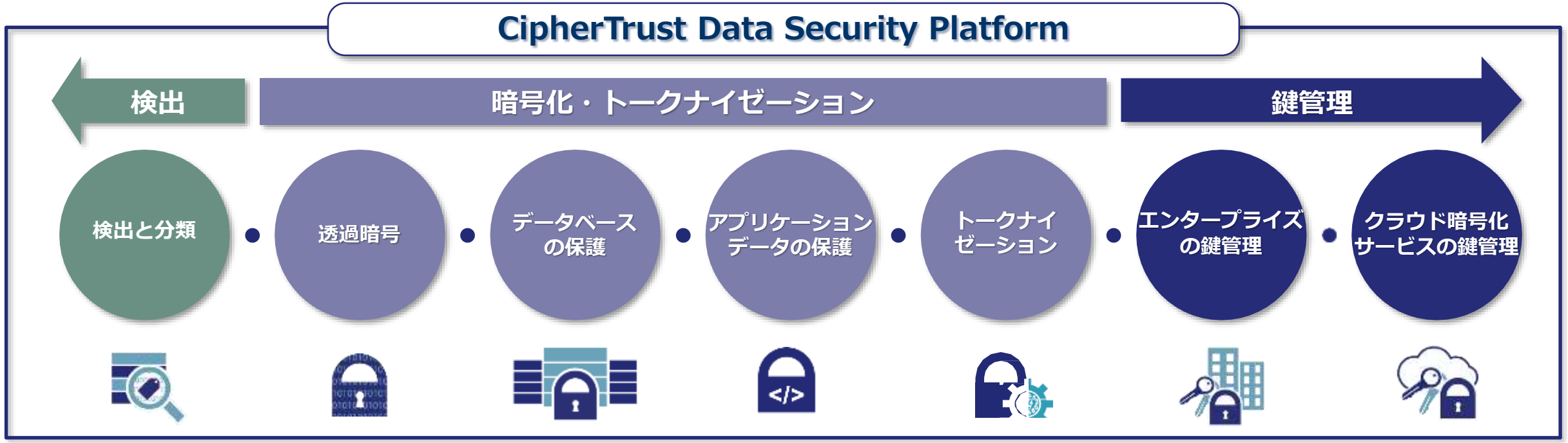
あなたの組織でデータセキュリティにこんな悩みを抱えていませんか？

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ーに対応し、 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

DXを支える
データセキュリティ基盤

鍵管理サーバー・検査サーバー 機能・特徴

■ 機能・特徴

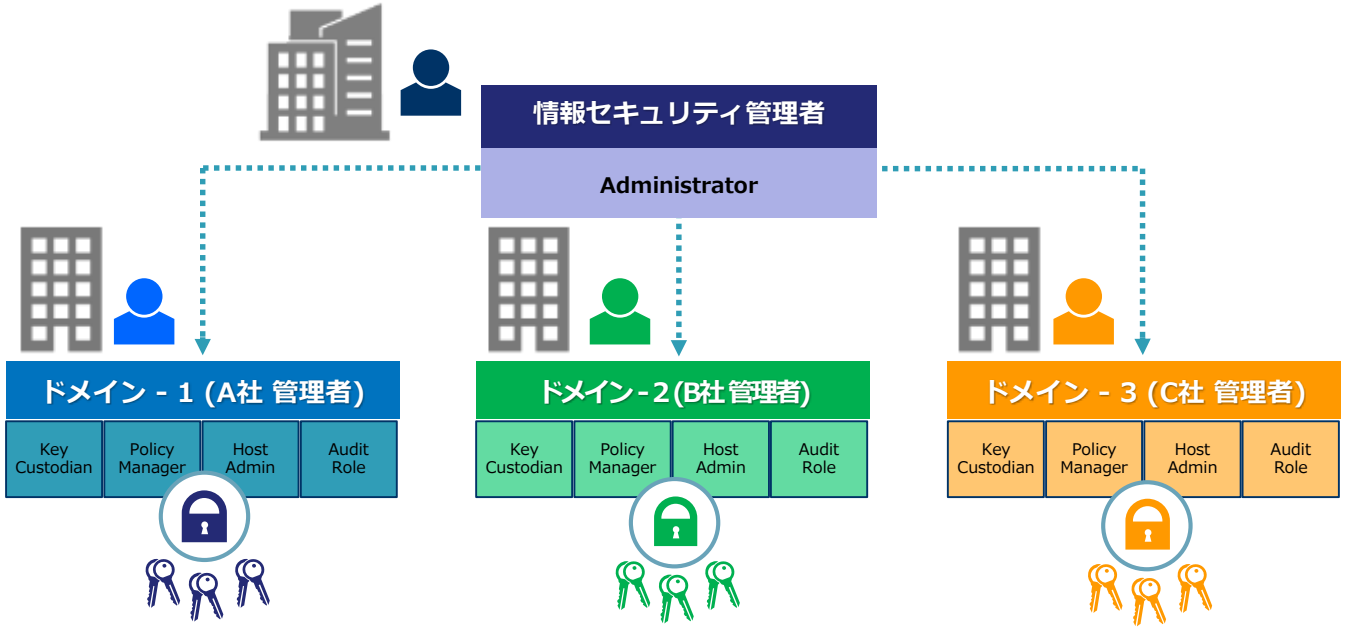
- 鍵の生成、ローテーション、廃棄、インポート/エクスポートなど鍵の管理を簡素化
- クラウド暗号化サービスを含め、他社暗号化製品の鍵を一元管理
- 鍵とポリシーに対するロールベースのアクセス制御
- 職務分掌が可能なマルチテナンシーをサポート
- 物理アプライアンスまたはソフトウェアアプライアンスにて鍵を安全に保管
- 鍵と暗号化操作に対する監査ログを取得
- 管理機能を自動化してプログラムによる暗号化機能を提供 (REST API)

物理アプライアンス

仮想アプライアンス

鍵管理サーバー 兼 検査サーバー

FIPS 140-2 認定



マルチドメイン機能

透過暗号 ソリューション

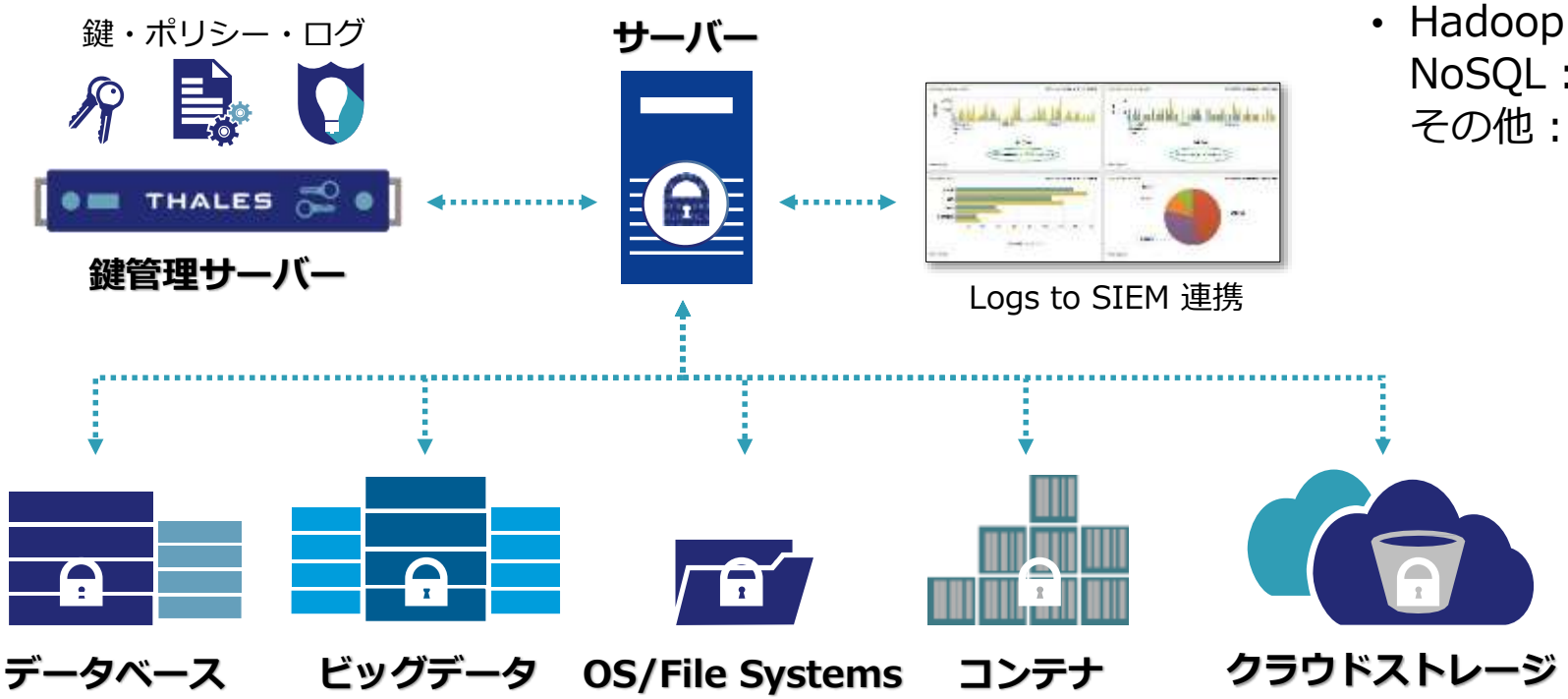
■ システム構成
- 鍵管理サーバー
- 透過暗号エージェント
  - ✤ FIPS 140-2 Level 1 認定

■ 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)

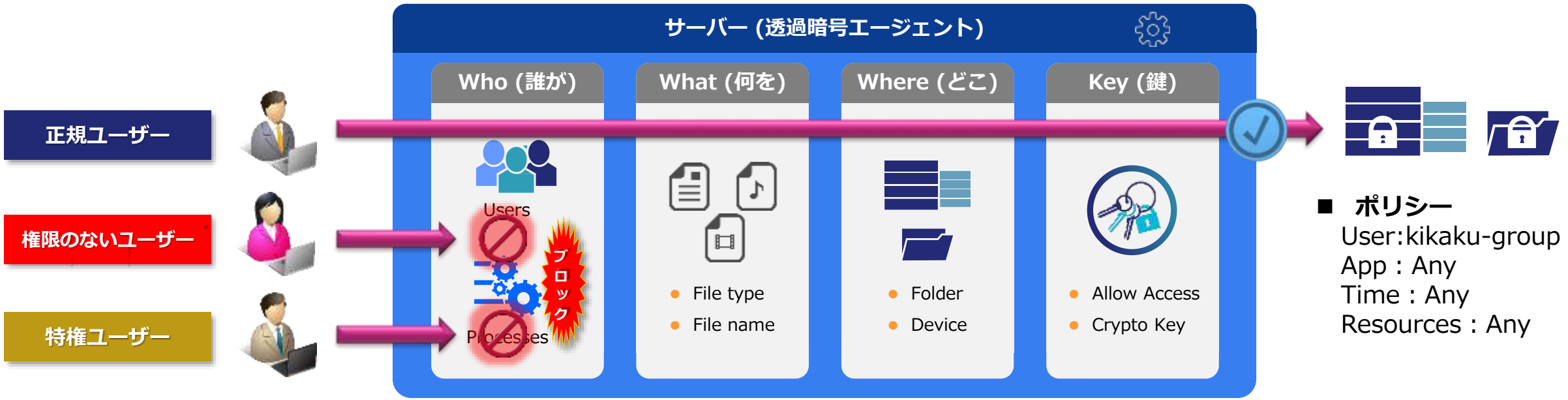
透過暗号 機能・特徴

■ 機能・特徴

- サーバー内のファイルやデータベースに対して自動的 (透過) に暗号化します
- 構造化データ、非構造化データを暗号化します (ファイルの種類を問わない)
- AES-NI (Advanced Encryption Standard New Instruction) にて暗号化と復号を高速化します
- クライアントPCに特別なソフトウェアは不要です
- 既存のファイルシステムやデータベース、アプリケーションの変更が不要です
- ユーザーやグループ情報、アクセス権などは LDAP/ActiveDirectory と連携します
- 「だれが」「何を」・・といった操作を全てログに記録します

《 Security-Policy 》

	Permit (アクセス権：許可)
	Deny (アクセス権：拒否)
	ApplyKey (暗号化/復号)
	Audit (監査ログ)

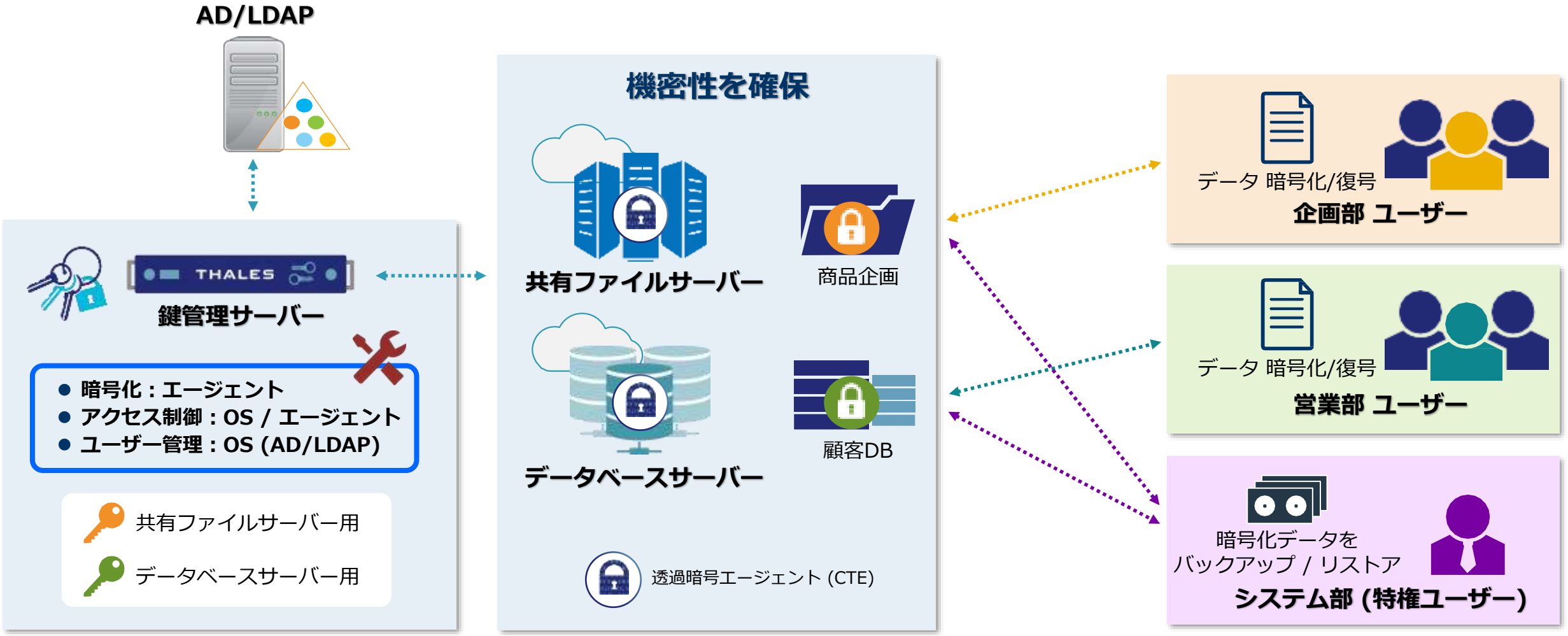


■ **ポリシー**
User:kikaku-group
App : Any
Time : Any
Resources : Any

✤ 特権ユーザーによる機密情報への不正アクセスを排除

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、権限を有したユーザー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)

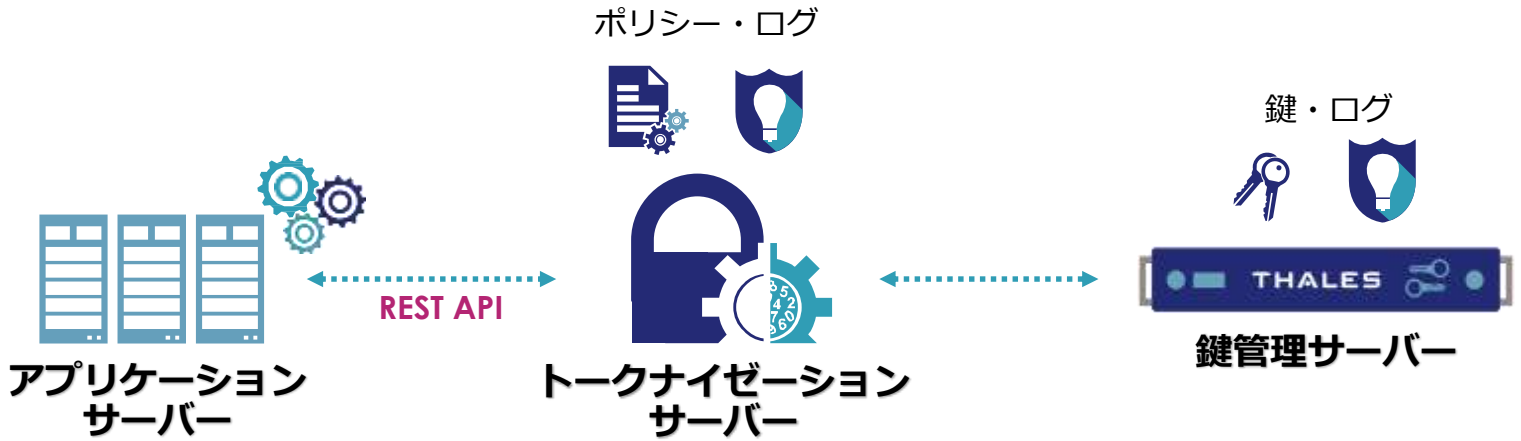
■ 提供形態
- Open Virtualization Format (OVA)
- International Organization for Standardization (ISO)
- Microsoft Hyper-V (VHD)
- Amazon Machine Image (AMI)
- Microsoft Azure Marketplace
- Google Cloud Platform

■ システム要件
- CPU：4個
- RAM：32GB(推奨)
- HDD：80GB

■ 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 機能・特徴

■ 機能・特徴

- 桁数とデータ型式を保持した状態で原本データを秘匿化(無価値化)します
- カード番号や電子メールアドレスなどの英数字に加え、住所や氏名などのマルチバイト文字にも対応します
- 復元する際は、テンプレート設定にて指定した桁をマスキングできます
- RESTful API で連携します
- 高パフォーマンス (単体エンジン性能：約30万トークン/秒)を実現します
- クラスタ構成による容易なスケールアップで、高可用性を実現します

【 原本データ】

ID	氏名	住所	Tel	E-Mail
1	山田太郎	東京都中央区東日本橋2-15	03-9060-9913	masaichi.sakurai@abcde.co.jp
2	佐藤花子	千葉県市原市山木2-18	04-0098-4336	ryuuichi.miyaji@fghij.co.jp
3	吉田次郎	神奈川県平塚市虹ケ浜4-13-15	046-197-8241	shigeru.yamawaki@klmno.co.jp

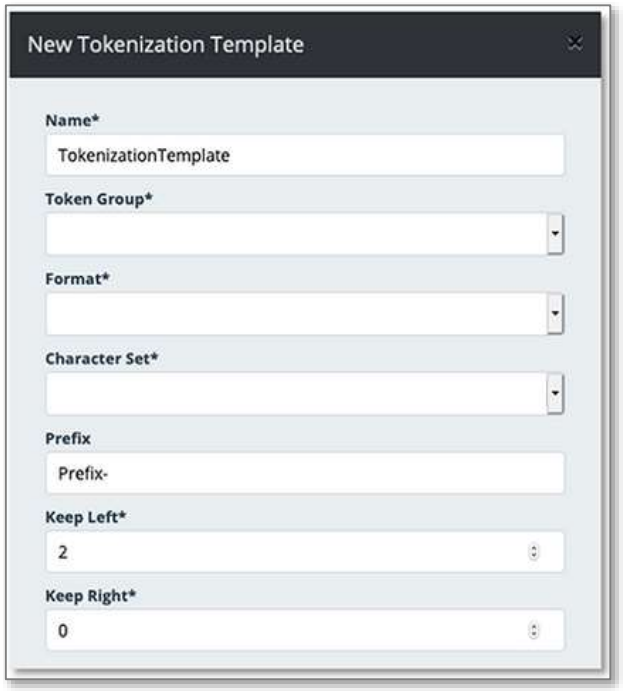
トークナイズ

デトークナイズ

【 トークンデータ】

ID	氏名	住所	Tel	E-Mail
1	欅亥整壱	桃供鍍仲奥狗桃乳翻況3-26	14-0171-0024	nbtbjdij.tblvsbj@bcdef.dp.kq
2	弓弛竜湿	占蓉肩師厳師惨黙3-29	15-1109-5447	szvvjdij.njzbkj@ghijk.dp.kq
3	惨惑妄樺	秦那戦肩弊栂師廿コ瀬5-24-26	157-208-9352	ibsvlp.tfljnpup@qrstuv.dp.kq

✤ フォーマット保持暗号化 (FPE：Format Preserving Encryption)



トークンテンプレート設定画面

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、権限を有したユーザーのみデータを復元 (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

無価値化

トークナイゼーション サーバー

データベース

THALES

鍵管理サーバー

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

CREDIT CARD

ファイナンス部 ユーザー

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

CREDIT CARD

マーケティング部 ユーザー

クラウド暗号化サービスの鍵管理 ソリューション

■ **システム構成**
- 鍵管理サーバー
- CipherTrust Cloud Key Manager (CCKM)
  仮想アプライアンス

■ 提供形態
- Open Virtualization Format (OVA)
- Microsoft Hyper-V (VHD)
- Amazon Machine Image (AMI)
- Microsoft Azure Marketplace

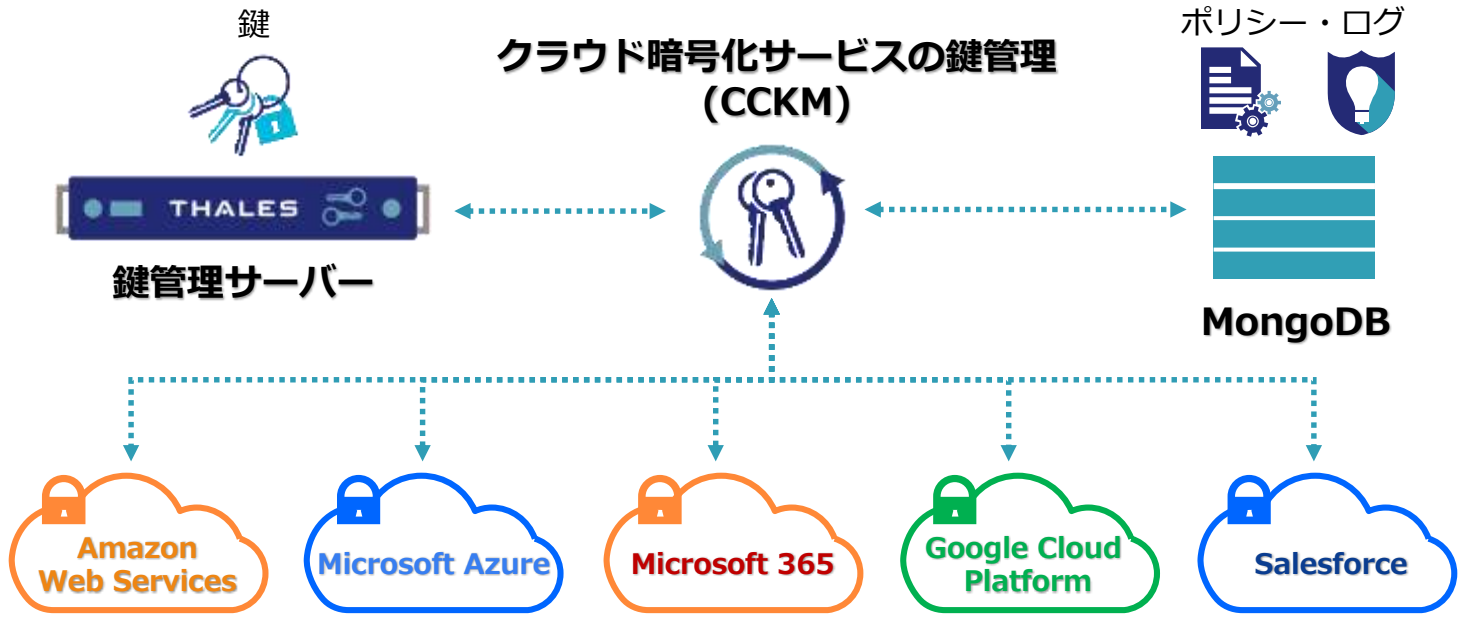
■ システム要件
- CPU：4個
- RAM：16GB(推奨)
- HDD：100GB

✣ MongoDBはお客様にてご用意ください。
(ご参考：MongoDB)
- CPU：4個
- RAM：16GB(推奨)
- HDD：250GB

■ **サポート対象のパブリッククラウドサービス**

[IaaS and PaaS]
- Amazon Web Services
- Microsoft Azure、Microsoft Azure Stack
- Google Cloud

[SaaS]
- Microsoft 365
- Salesforce.com、Salesforce Sandbox



クラウドサービスの責任共有モデル

クラウドサービスにおいては、利用者が責任を持つ範囲とクラウドサービスプロバイダ (CSP) が責任を持つ範囲を明確に区分し、それぞれが責任を果たすために必要な対策を実施することでサービス全体のセキュリティを保ちます。
クラウドサービスのセキュリティの考え方のベースとなるのが責任共有モデルです。
IaaSの場合、OSより上位のレイヤーでのセキュリティ対策は、利用者が実施する必要があります。

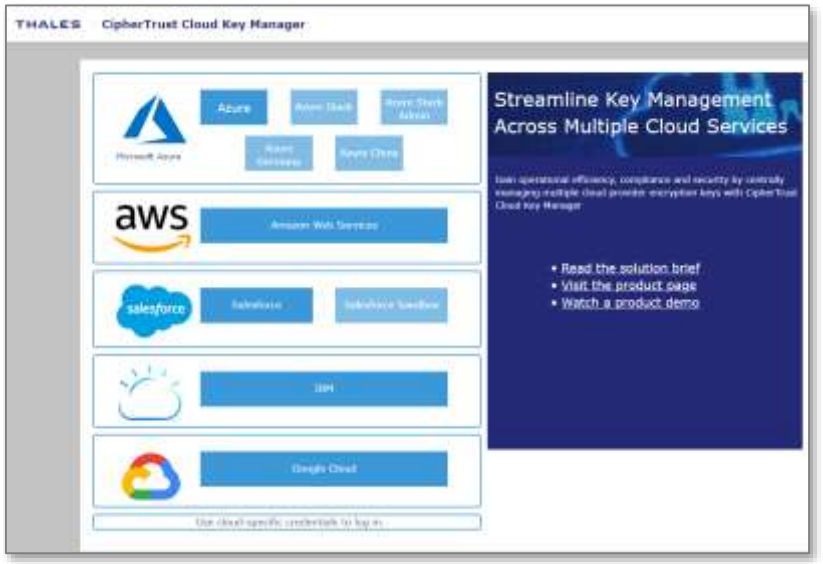
第三者認証

・・・・・

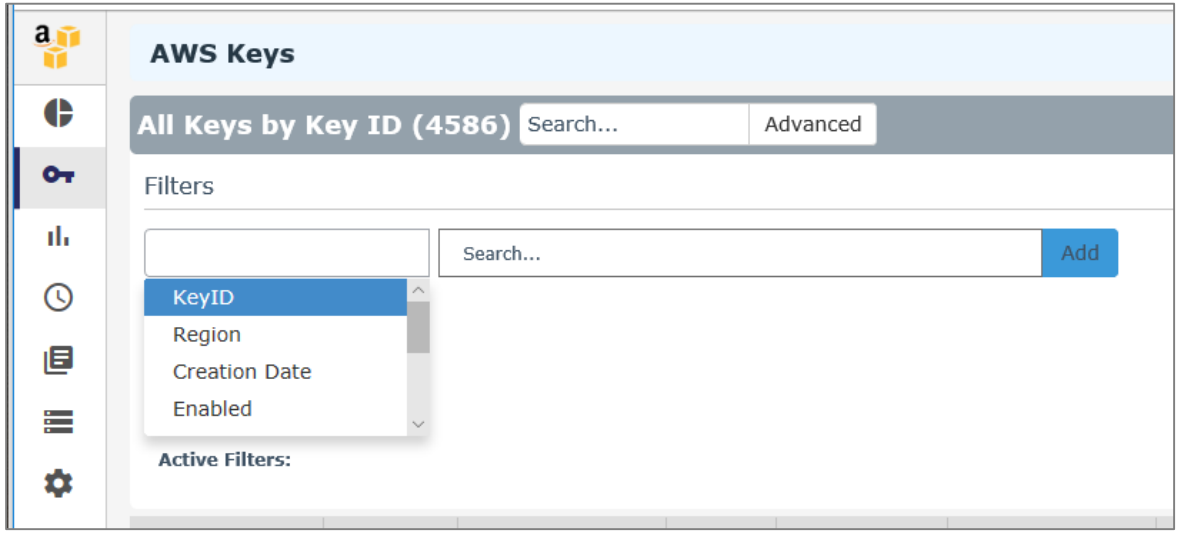
クラウド暗号化サービスの鍵管理 機能・特徴

■ 機能・特徴

- 自社で鍵を保管することにより、クラウド環境でも安全にデータを保護します
- オンプレミスとクラウド、更にはハイブリット環境で高度な暗号化と鍵管理を実現します
- 複数のクラウド暗号化サービスの暗号鍵を一元管理できます
- 管理者に対して統一した管理画面UIを提供します
- 鍵のバックアップ、ローテーションといったライフサイクル管理を実現します
- ユーザー側の暗号鍵を使用できます (BYOK)
- 鍵に関する各種操作を監査ログとして収集します



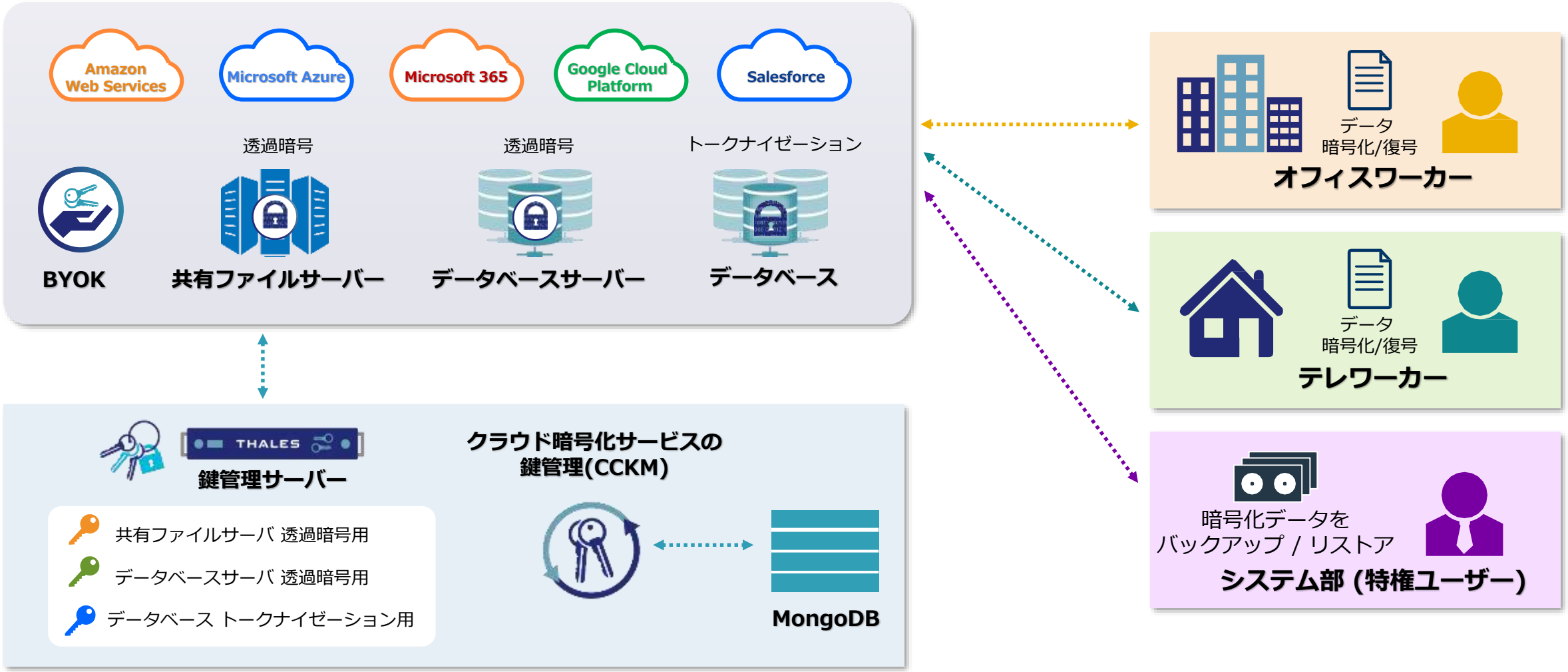
クラウド暗号化サービスの鍵管理 (CCKM)
トップ画面



クラウド暗号化サービスの鍵管理 (CCKM)
鍵生成画面

クラウド暗号化サービスの鍵管理 運用例

サーバー内のファイルは常に暗号化状態であり、権限を有したユーザー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。



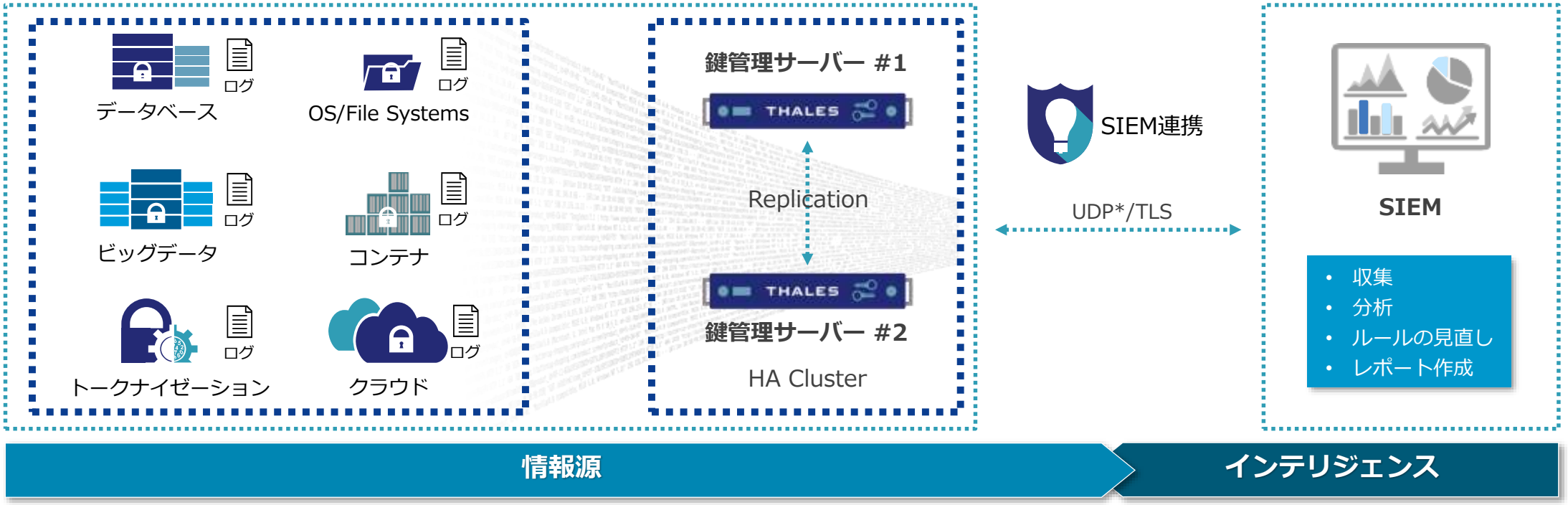
セキュリティインテリジェンス ソリューション

■ システム構成
- 鍵管理サーバー
- 各機能コンポーネント
- サードパーティのSIEM

■ ログフォーマット形式
- Common Event Format (CEF)
- Log Event Extended Format (LEEF)
- RFC5424*
- Plain Message

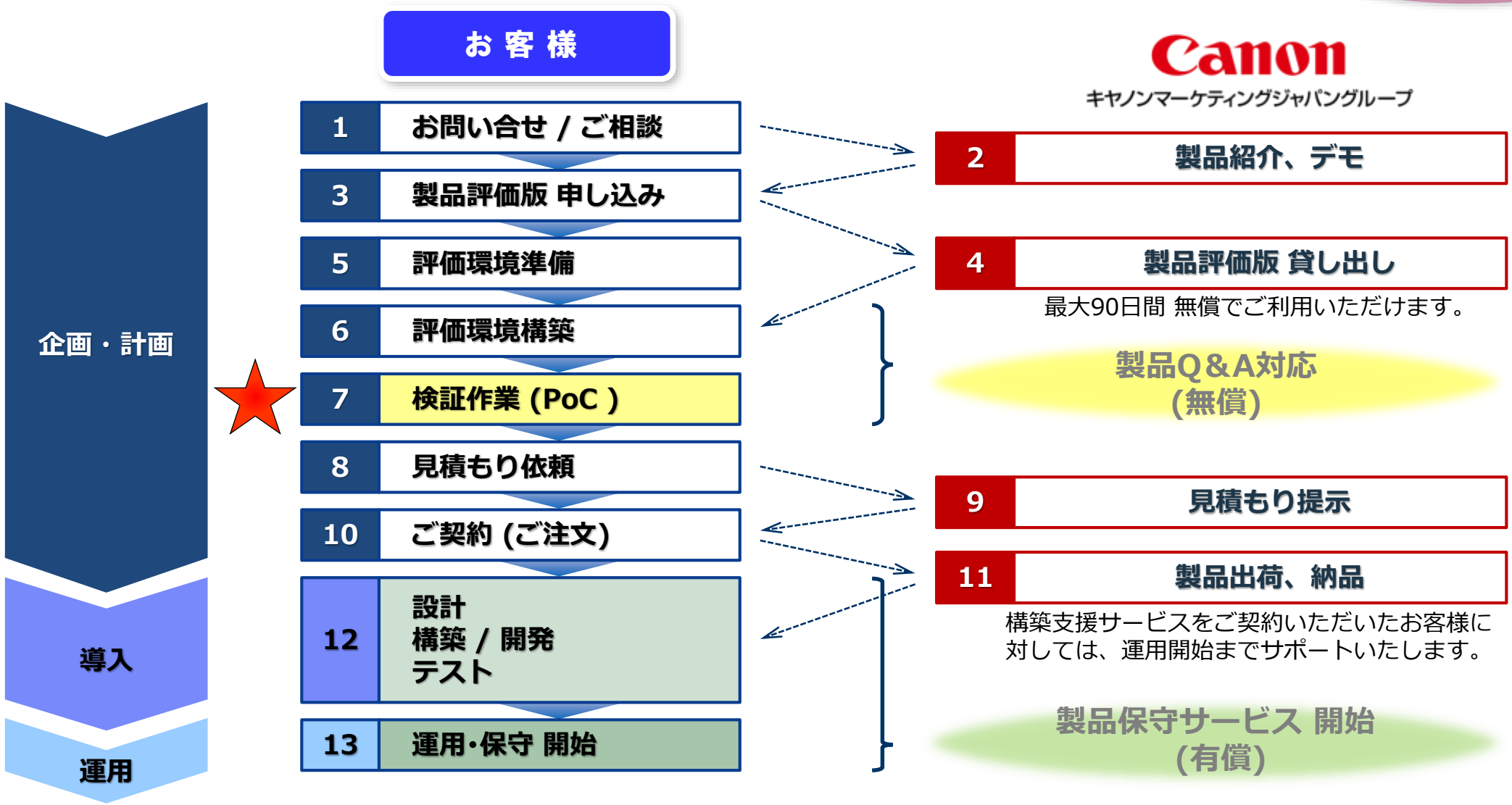
✤ =デフォルト

■ 連携可能なSIEM
- Splunk
- HP ArcSight
- IBM Qradar
- LogRhythm
- McAfee
- FireEye



導入ステップ

評価版貸出

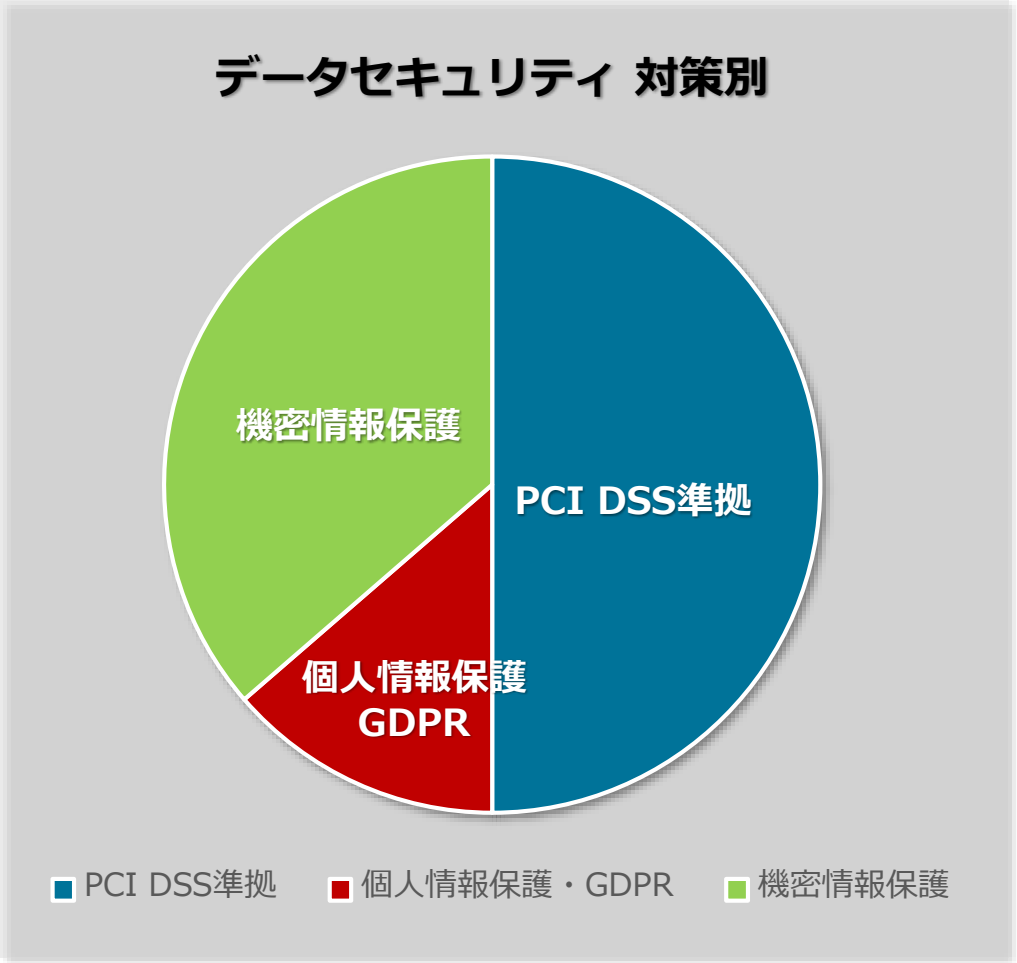


PoC : Proof of Concept (概念実証) の略称です。

主な導入実績

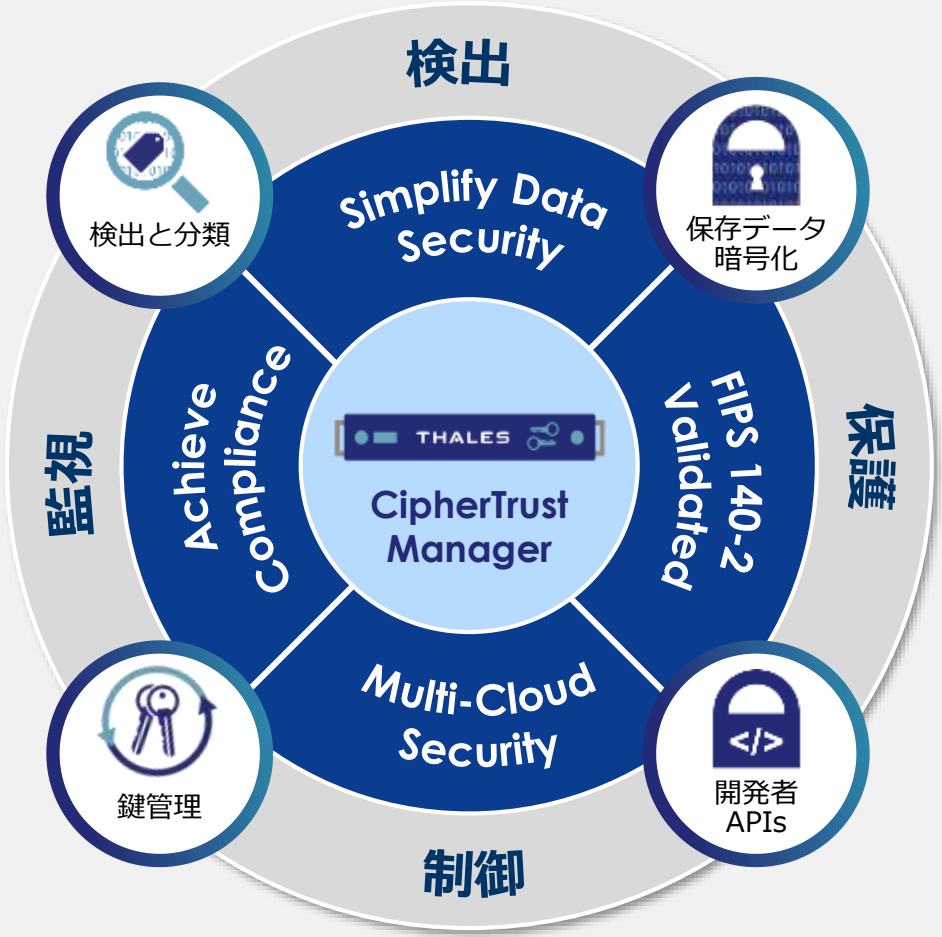
「CipherTrust Data Security Platform」は、業種業態を問わず多くのお客様にご利用いただいております。

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



データセキュリティソリューション

CipherTrust Data Security Platform



THALES

高セキュリティ・高可用性を実現

- FIPS 140-2 L1/L3 認定
- クラスタリング構成で高可用性を実現

マルチ環境のセキュリティを実現

- ハイブリッド環境で利用可能
- クラウド暗号化サービスの鍵を一元管理

コンプライアンス要件に対応

- 機密データを検出、分類、保護
- データプライバシーとセキュリティ規制に対応

ご視聴ありがとうございました。

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商品企画部

ご相談・お問い合わせはこちら

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