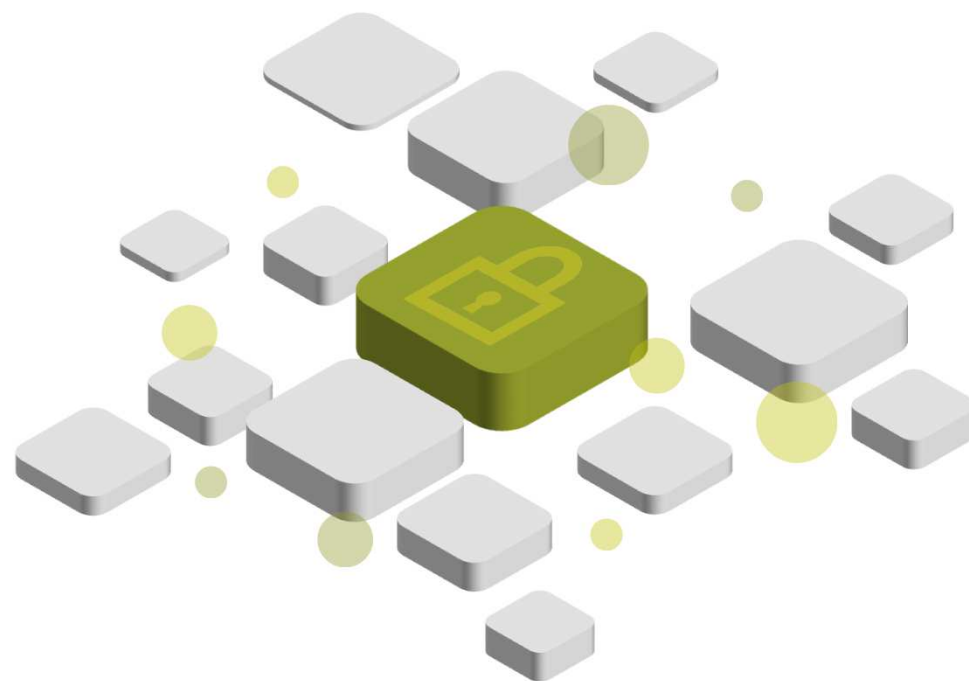


事業計画及び 成長可能性に関する説明資料

株式会社ZenmuTech | 2026年3月31日

東証グロース市場（証券コード：338A）

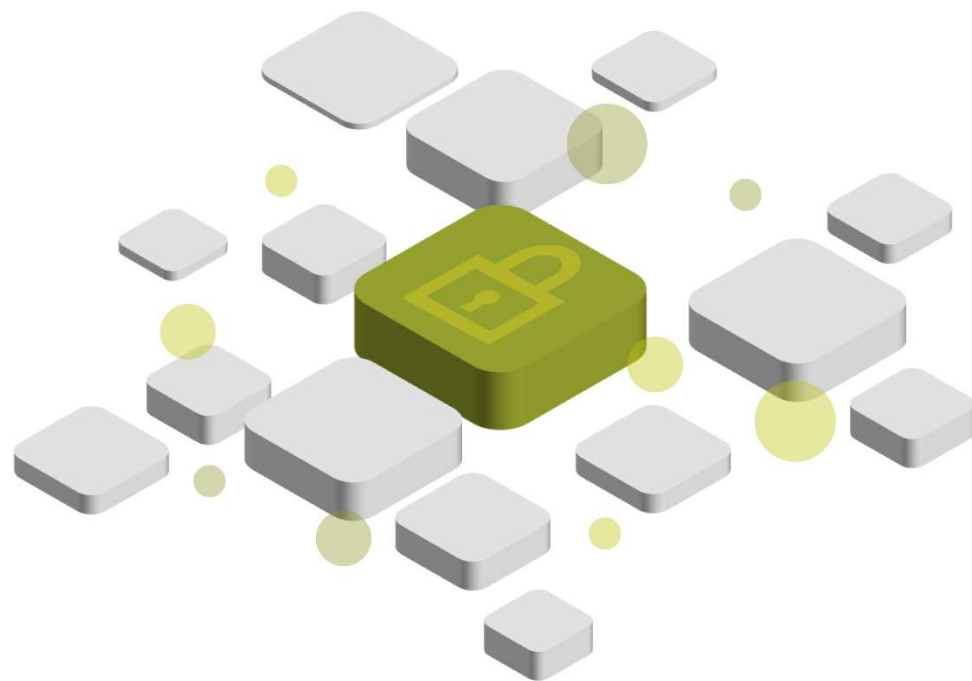


データはもっと自由になれる

ユーザーデータを分散させることで無意味化する「秘密分散」技術を活用したサービスをはじめ、「秘密分散」を基に発展させデータを秘匿化しながら活用できる「秘密計算」技術など、安心・安全からイノベーションを生み出していきます。

また、協業する企業のビジネスをよりスムーズに加速させ、マーケットに新しい機会を生み出し、働き方や暮らし方そのものをポジティブに変えていくことこそが、私たちの使命だと考えます。

1.会社概要



暗号化技術を応用した

秘密分散・秘密計算技術を活用した3つのソリューションを展開

第1軸：情報漏洩対策ソリューション

ZENMU Virtual Drive

データを無意味化しPCの利用を安全で快適にするセキュリティソフトウェア

第2軸：秘密分散ソフトウェア開発キット

ZENMU Engine

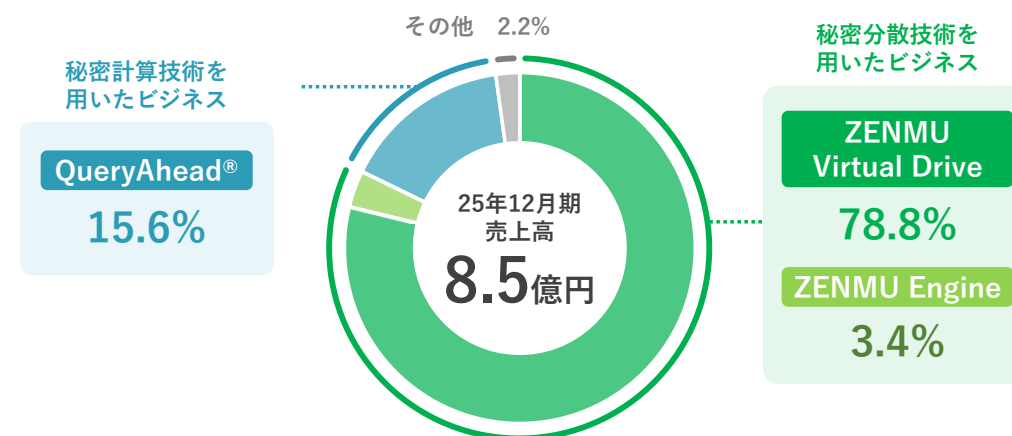
秘密分散技術をプロダクトやアプリケーションに組み込むためのソフトウェア開発キット

第3軸：秘密計算ソリューション

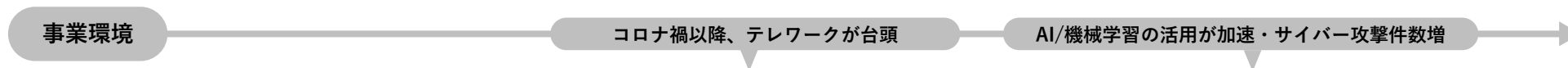
QueryAhead®

暗号理論などの専門知識不要で秘密計算技術を実用化するためのツール

会社名	株式会社ZenmuTech
設立	2014年3月4日
代表取締役社長	阿部 泰久
本社所在地	東京都中央区新川二丁目22番1号 いちご新川ビル5階
従業員数	36名（2025年12月31日時点）
資本金	43,435万円（2025年12月31日時点）
事業内容	秘密分散、秘密計算技術を活用したセキュリティソリューションの開発・販売



シンクライアント関連ビジネスで創業、PC向けセキュリティの知見を活かし秘密分散技術の事業化に着手
 大手企業各社とのパートナーシップを構築しながら、技術開発・サービス提供を行い事業基盤を構築、拡大



STEP

- 2015年
 - ✓ 秘密分散ソリューション事業化
- 2018年
 - ✓ 秘密分散処理モジュール「ZENMU Engine」の提供開始
- 2018年
 - ✓ 産業総合研究所と「秘密分散技術ZENMU-AONTに関する安全性評価」に関する共同研究開始

- 2019年
 - ✓ データ分散型仮想デスクトップソリューション「ZENMU Virtual Desktop」のサービス提供開始
- 2021年
 - ✓ 秘密計算データベースプラットフォーム「QueryAhead®」の提供開始
 - ✓ 「ZENMU Virtual Drive Enterprise Edition」のサービス提供開始

- 2023年
 - ✓ 株式会社AIST Solutionsから、AISolスタートアップとして認定
- 2025年
 - ✓ 東証グロース市場に上場

【今後の成長戦略】
 主力のZENMU Virtual Driveの安定成長
 +
 ZENMU Engine、QueryAheadの立ち上げによる更なる事業拡大

導入実績
 アライアンス

【導入実績】



導入数
 110,000アカウント

【販売代理店/ソリューションパートナー】



売上高	営業利益	経常利益	当期純利益
8.5億円 前年比+31.3%	1.4億円 前年比+88.3%	1.6億円 前年比+90.8%	1.5億円 前年比+98.6%
売上高CAGR	ZVDライセンス数※1	ZVD解約率※1,2	
54.2% (2022-2025年)	115,417 (2025年12期期末)	1.2% (2025年期末時点※)	

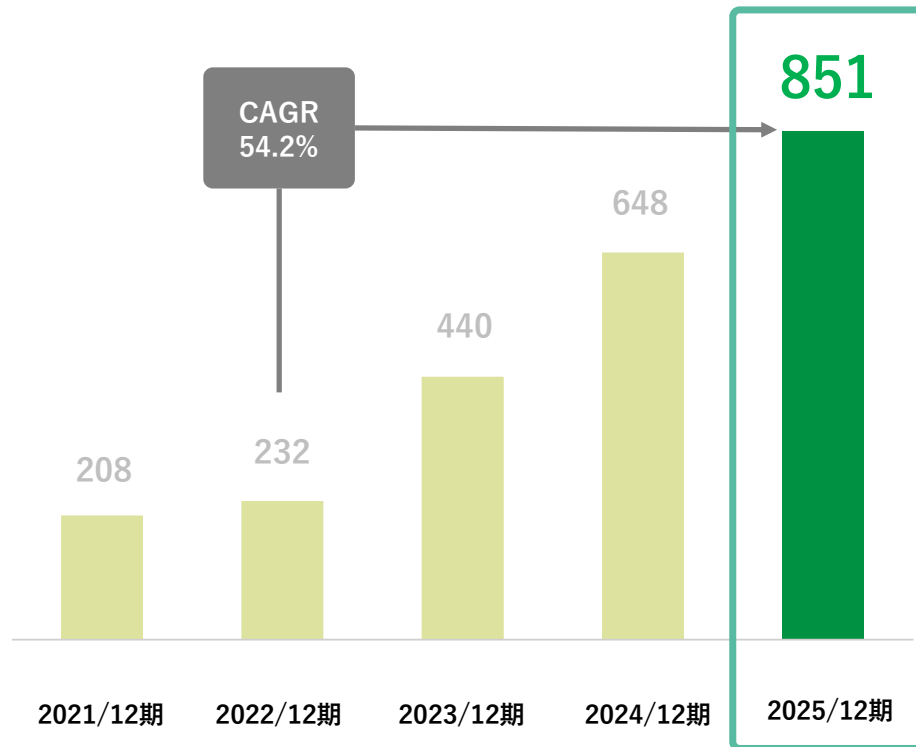
※1 「ZVDライセンス数」「ZVD解約率」について、従来「ライセンス数」「解約率」と表示していたものを名称のみ変更したもの

※2 2024年12月末～2025年12月末の1年間におけるZVDサブスク契約の解約ライセンス数 ÷ 2024年12月末時点でのライセンス数

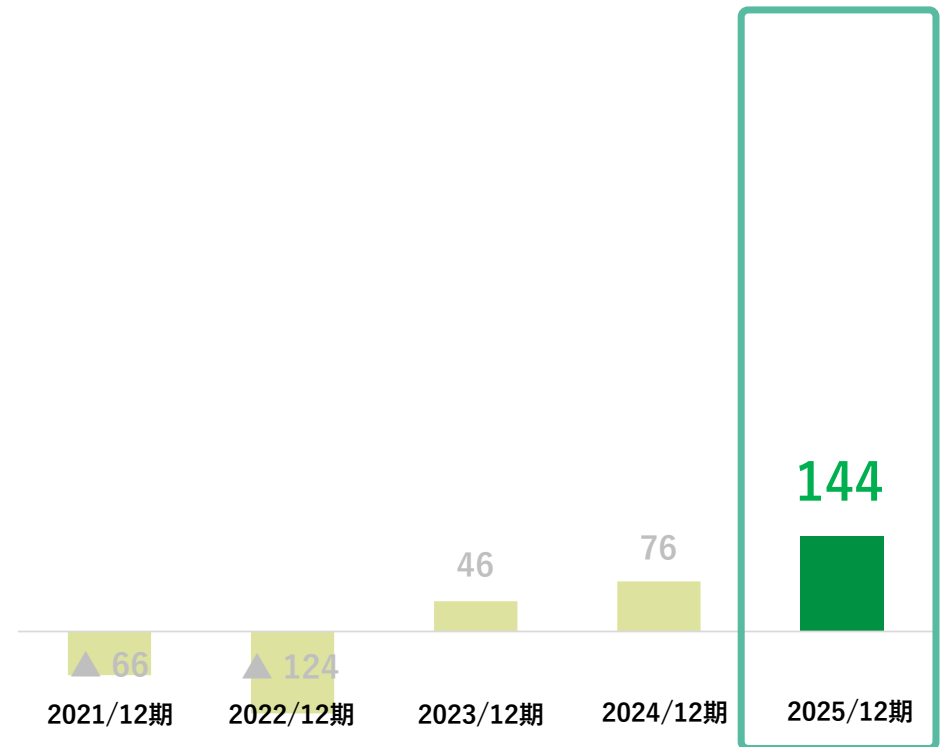
2025年12月期 業績ハイライト

売上拡大により2023年12月期から黒字化
2025年12月期も売上高前年比+31.3%、営業利益+88.3%と成長

売上高 (単位: 百万円)



営業利益 (単位: 百万円)



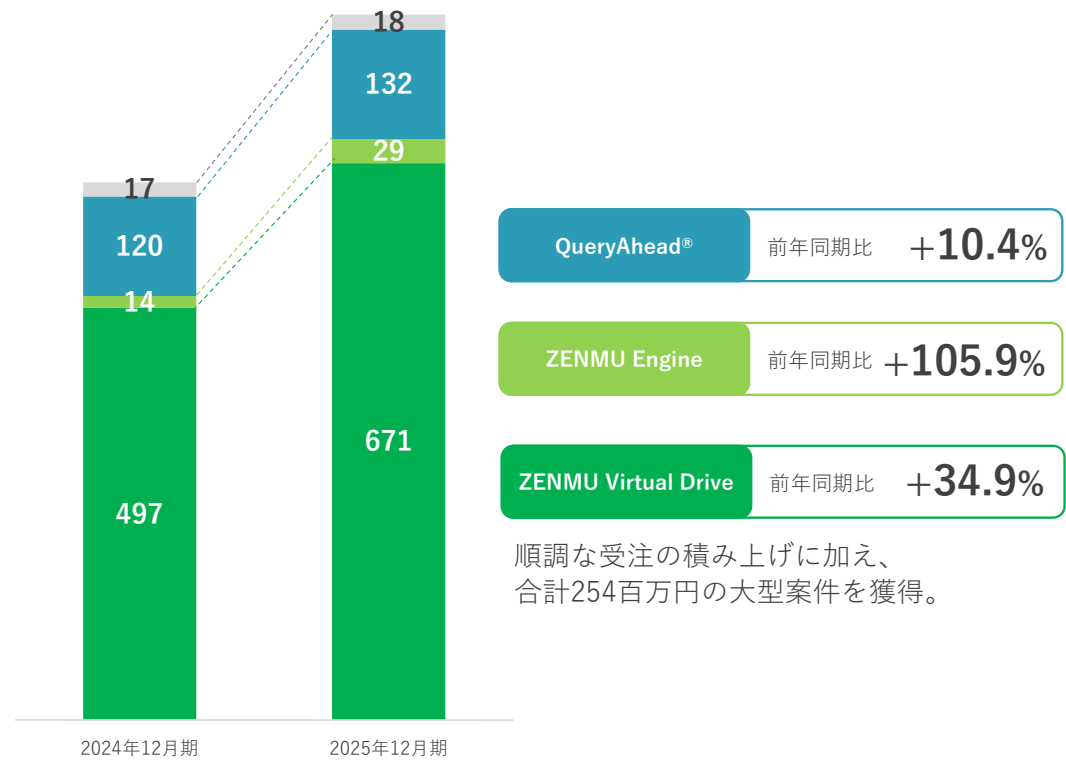
事業別売上高

主力の秘密分散ビジネスはZENMU Virtual Driveのサブスクリプション契約の順調な増加と大型案件の獲得により大きく増加、Zenmu Engineとあわせ+36.9%成長と全体を牽引。

事業別 売上高 (単位：百万円)

	2024年12月期	2025年12月期	増減率
秘密分散ビジネス	511	700	+36.9%
内訳) ZVD	497	671	+34.9%
Engine	14	29	+105.9%
秘密計算ビジネス	120	132	+10.4%
その他	17	18	+10.4%
合計	648	851	+31.3%

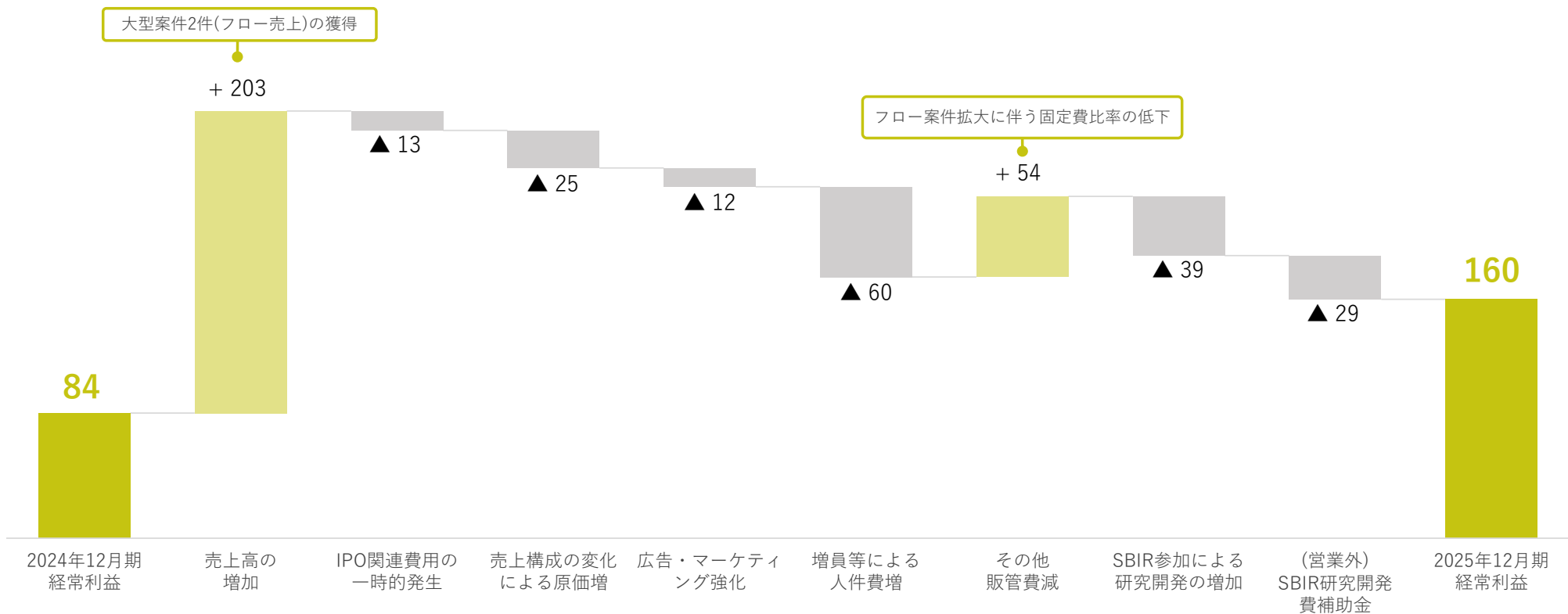
ソリューション別 売上高 (単位：百万円)



経常利益 増減分析



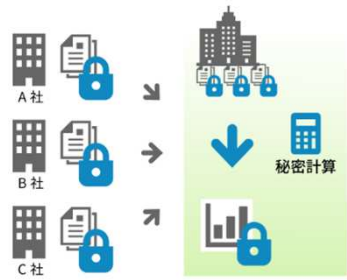
将来の成長に向けた人材・研究開発・認知度向上への投資を強化する一方、フロー案件の大幅な拡大に伴う売上増と固定費比率の低下により、経常利益は前期比+90.8%の大幅増益。

(単位：百万円)



2.事業内容と ビジネスモデル

秘密分散・秘密計算技術を活用した3つのソリューションを展開

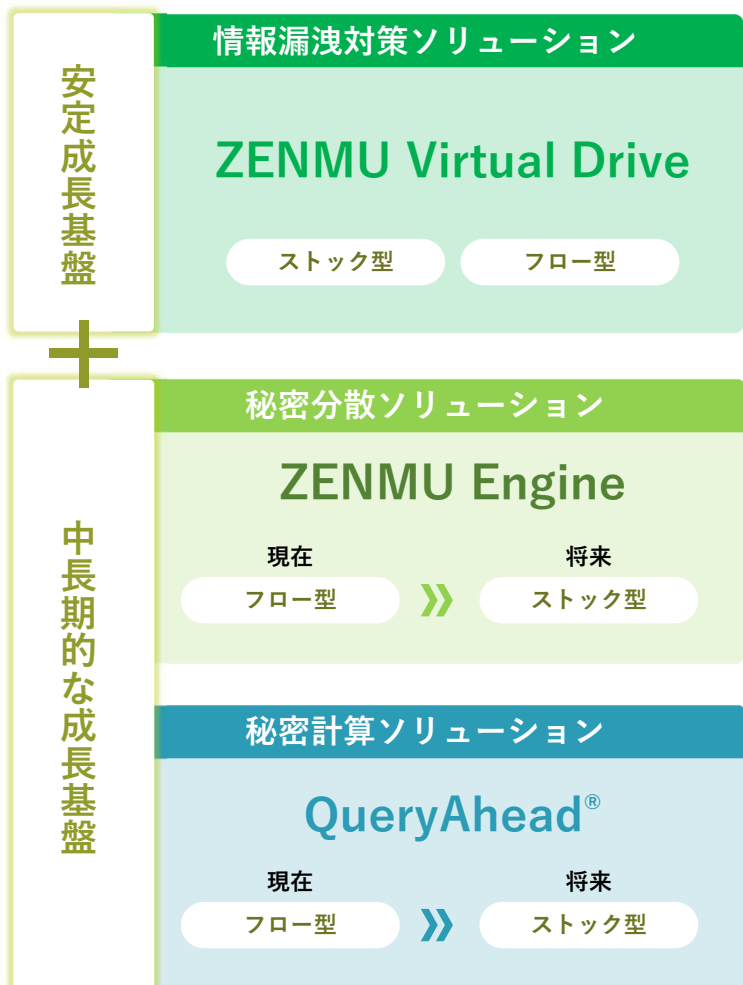
	秘密分散ビジネス		秘密計算ビジネス
ソリューション	<p>情報漏洩対策ソリューション</p> <p>ZENMU Virtual Drive (ZVD)</p>  <p>PCの利用を安全で快適にする セキュリティソフトウェア</p>	<p>秘密分散ソフトウェア開発キット</p> <p>ZENMU Engine</p>  <p>秘密分散技術をプロダクトや アプリケーションに組み込むためのSDK</p>	<p>秘密計算ソリューション</p> <p>QueryAhead®</p>  <p>専門知識不要で秘密計算をプロダクトや アプリケーションに組み込むツール</p>
売上高構成比 (2025年12月期)	78.8%	3.4%	15.6%

※その他事業 売上比率2% 既存取引先、ユーザー向けにシンククライアント関連サービスを提供

秘密分散・秘密計算技術を活用した3つのソリューションを展開

	秘密分散ビジネス		秘密計算ビジネス	売上高構成比 (2025年12月期)
ソリューション	情報漏洩対策ソリューション ZENMU Virtual Drive	秘密分散ソフトウェア開発キット ZENMU Engine	秘密計算ソリューション QueryAhead®	
フロー型 収益	<ul style="list-style-type: none"> ✓ 買い切りライセンス 	<ul style="list-style-type: none"> ✓ SDK買い切りライセンス ✓ OEM商品を開発する際のコンサルティングや開発支援 	<ul style="list-style-type: none"> ✓ 試用ライセンスの販売契約 ✓ PoCや実証研究などの受託役務 	53.4%
ストック型 収益	<ul style="list-style-type: none"> ✓ ライセンス利用に伴う保守契約 ✓ ライセンス契約と保守契約、アップデート対応が一体となったサブスクリプション契約 	<ul style="list-style-type: none"> ✓ ライセンス利用に伴う保守契約 ✓ OEM商品の売上に伴うロイヤリティ契約 		46.5%

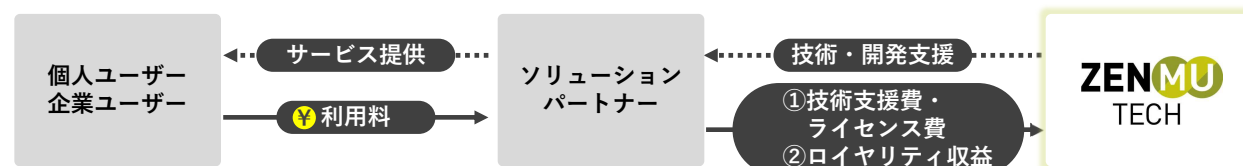
※その他事業 売上比率2% 既存取引先、ユーザー向けにシンクライアント関連サービスを提供



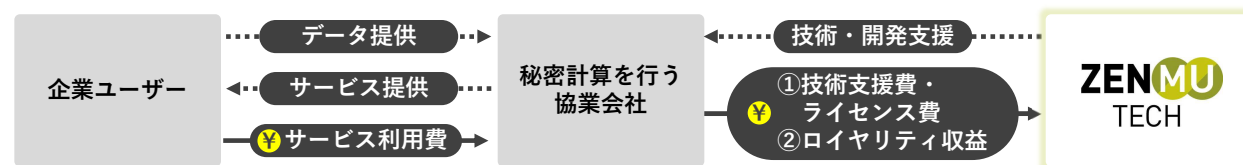
システム更新などのPC買い替え時に、販売代理店による間接販売で導入を拡大、サブスクリプション収益を獲得
※要望があればOEM商品開発のための当社の技術者によるコンサルティング費用発生



ZENMU Engineを各社の製品・サービスに組み込むプログラムとして外部提供、オープンイノベーションを通じて新事業・新サービスを協創、ロイヤリティ収益を獲得



PoCや受託開発などで協業会社による事業化支援を実施しつつ
将来的には協業会社からロイヤリティ収益獲得

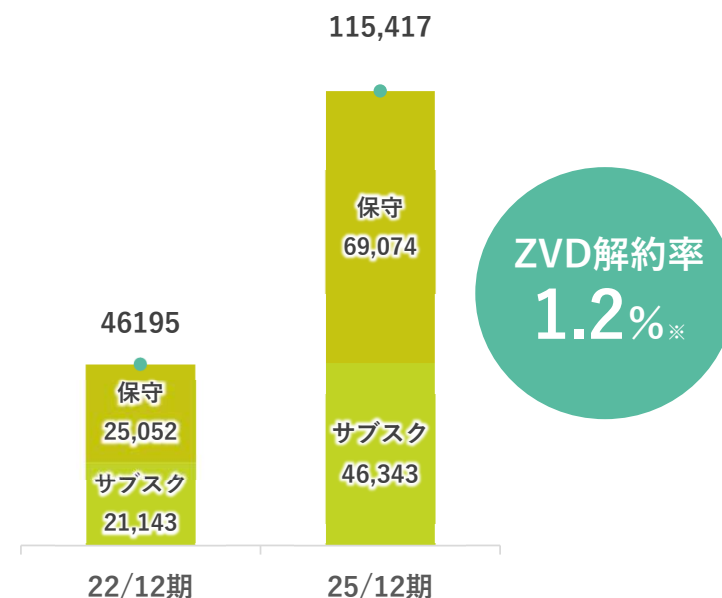


秘密分散技術によりPC内のデータを無意味化して分散、
分散片が揃った時のみPC上にデータが復元
既存のソリューションにかわる情報漏洩対策

ZENMU-AONTにより1kbの分散片を外部保存するだけでPC内のデータを無意味化
通信環境への依存度が高い従来ソリューションに対し、オフラインや低速環境でも
PCを快適に使用可能



ZENMU Virtual Drive ライセンス数



データ保護ができる

PC紛失の際にも、本人や管理者が分散ファイルへのアクセス停止をおこなうことPCへのアクセス防止が可能

働く場所に依存せず
快適に仕事ができる

分散片はスマホやUSBメモリーでも同期可能なので、ネットワーク環境に頼らずオフラインでも安定して利用可能

管理者負担が軽く
コストも低減

重厚なサーバーやネットワークが不要なので、管理者の負担が軽く導入、運用のコストも縮小

企業規模に依存しない

FAT-PC形式で対応可能で導入、運用のコストが低いので小規模企業でも導入可能

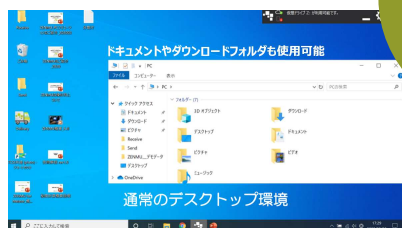
短期間で
利用開始が可能

ポリシー設定のみで、導入決定から1ヶ月程度で利用可能

※24年12月末～25年12月末の1年間におけるZVDサブスク契約の解約ライセンス数 ÷ 2024年12月末時点でのライセンス数

秘密分散技術によりPC内のデータをPCとクラウドに分散、分散片が揃った時のみPC上にデータが復元

分散片が揃った時のみPC上にデータが復元

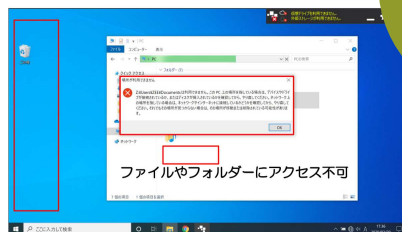


クラウド上の分散ファイルと合わせてデータを復元



PCの紛失・盗難時にはユーザー本人または社内管理者がクラウド上の分散片へのアクセスを遮断

分散片が揃わないとPC上では何も見えない状態



未接続時、PC内には無意味な分散ファイルのみ

- ✓ クラウドに保存する分散片のサイズは1kbと小さく、低速通信環境やクラウドへのアクセス集中時でも影響をうけない

競合するVDIやデータレスPCは画面転送やファイルの転送を行うため通信量が大きく通信回線やサーバーの状況によってパフォーマンスが低下

- ✓ 紛失・盗難後、PCが回収できた場合にはクラウド側へのアクセスを再開することで元のデータをそのまま利用可能

PCにデータ消去指示を送る遠隔消去ツールは成功率に課題。また、消去後の復元も不可能

- ✓ クラウドへのアクセスログから紛失・盗難中の不正アクセスの有無自体を把握可能

情報漏洩がなかったことの証明が可能

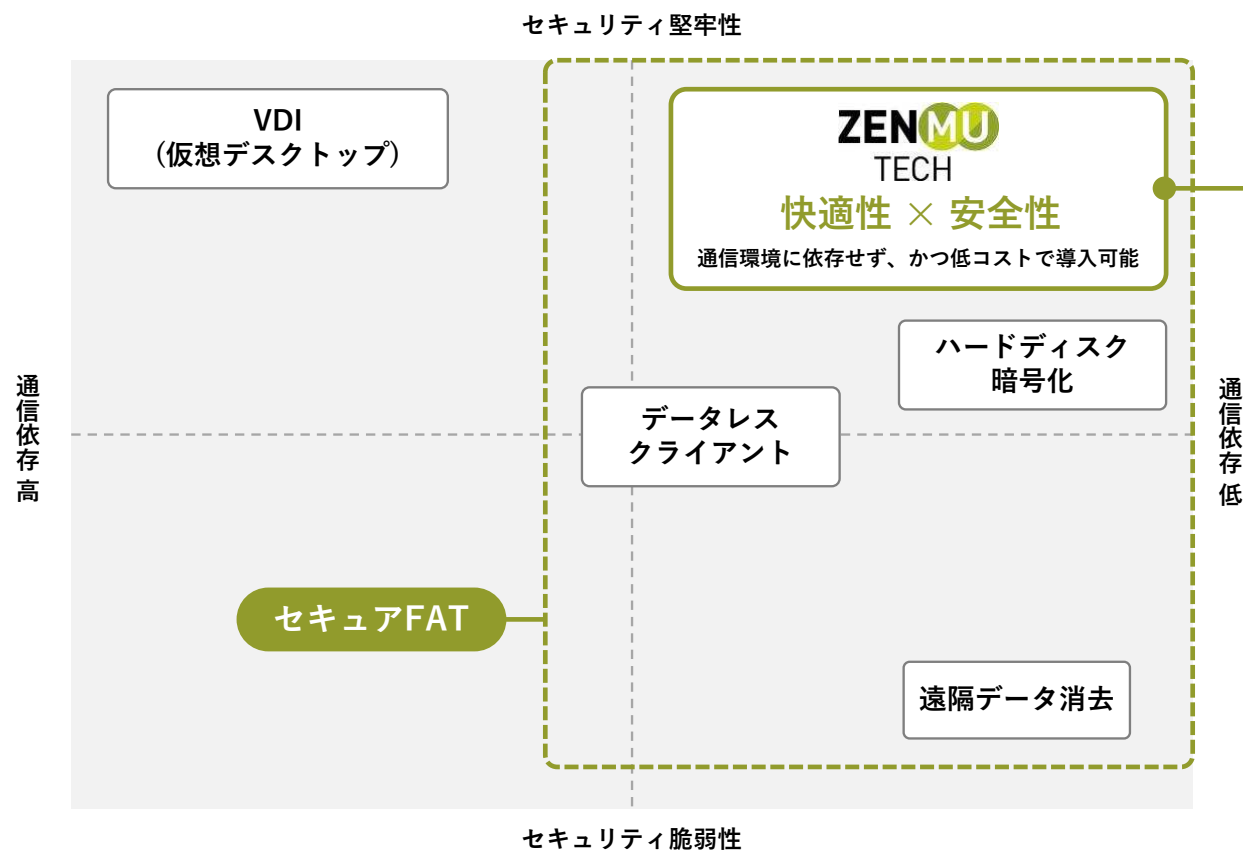
コロナ禍以降のリモートワークの拡大、定着にともない業務用PC持出時のセキュリティ対策への需要も拡大
従来のPC向け情報漏洩対策ソリューションの課題に応えるセキュアFATに需要が高まる



※VDI：デスクトップ環境を仮想化してサーバー上に集約したものであり、利用者はシンクライアントPCからネットワークを通じてサーバー上の仮想マシンに接続し、デスクトップ画面を呼び出して操作する。

※シンクライアント：企業などの情報システムにおいて、ユーザーが使うPC等のクライアント端末に必要最小限の処理をさせ、ほとんどの処理をサーバー側に集中させることでソフトウェアやデータなどの資源を管理します。

「ZENMU Virtual Drive」はVDIのデメリットを解消 且つ、通信依存度の低さからなる快適性と低コスト、安全性を両立



✓ 快適性

AONTの特性を活かし1kbの分散片のみクラウド上に保存。通信速度やサーバーの処理能力に依存せずに利用できるため低速環境やネットワークのアクセス集中による影響を受けにくい

✓ 安全性

秘密分散技術によりデータを無意味化してPC内とクラウドに分散保管するため、クラウドの接続をロックすればPC内のデータは無意味なものとなり、盗難・紛失時も情報漏洩を防ぐことができる

✓ 低コスト

クラウド基盤のサービスのため、サーバーの新規購入や設計・構築費用等は一切不要
自社開発であるため海外製品と比べライセンスも相対的に安価

「ZENMU Virtual Drive」はVDIのデメリットを解消
 且つ、通信依存度の低さからなる快適性と低コスト、安全性を両立

プロダクト	VDI (シンククライアント)	データレスクライアント	ZENMU Virtual Drive
概要	サーバー上でデータを処理、保存し 手元の端末に画面転送	PC内でデータを処理するが データはサーバー上に保存	PC内でデータを処理し PCとクラウドに分散保管
安全性	データは端末上には一切存在しない	データはPC上に残らないが、 キャッシュが残る場合もある	PC内には 無意味な分散ファイルのみ
操作の快適性 パフォーマンス	画面転送のため通信量が大きく 通信環境およびサーバーの処理能力に 左右される。サーバーへのアクセス 集中などによりパフォーマンス低下	処理は通常のPCとほぼ同等、 データの読み書きは通信環境に依存	通常のPCとほぼ同等 サーバー等外部との接続は 1kbの分散片のみ
1ユーザー あたりの費用	オンプレで年額250,000円程度 クラウドで年額50,000~100,000円程度	年額10,000~25,000円程度、 他にサーバーコストも必要	年額 21,600円
通信環境への 依存度	通信環境のない場所では 利用できない	基本的に通信環境のない場所では 利用できない	通信環境に依存しない オフラインでも利用可能

A社

VDI下のパフォーマンスに大きな不満、
業種柄、移動が多くネットワーク品質に左右される余地が大きい
→ 導入後の利用者アンケートはおおむね好評、現在2万4,000ライセンスまで拡大

導入前

× グループ各社で業務内容、業務用アプリが異なるため必要な性能に応じたVDI環境の設定が必要。煩雑かつコストの制約から対応に限界

× 業務・拠点の関係で小刻みな移動が多く、VDIのセッション切れで時間ロスが大きい

× パフォーマンスに対する潜在的な不満がある



導入後

✓ 端末のセキュリティコスト削減
VDIサーバーも移行完了時には撤廃の方針

✓ 移動時の起動や操作の点で従来より
パフォーマンス向上、
ユーザアンケートでは9割が評価

✓ VDI同等のセキュリティを確保しながら、
パフォーマンスは改善

自社開発の秘密分散技術「ZENMU-AONT」をソフトウェア開発キット（SDK）※1として提供
秘密分散技術を他社のプロダクトやアプリケーションに組み込むことが可能

セキュリティやコストの問題を解決する
新たなソリューションを開発して
使用又は販売したい



DEVELOPER

SDKとしての提供価値

- ✓ 開発時間の短縮
- ✓ 品質や開発コスト

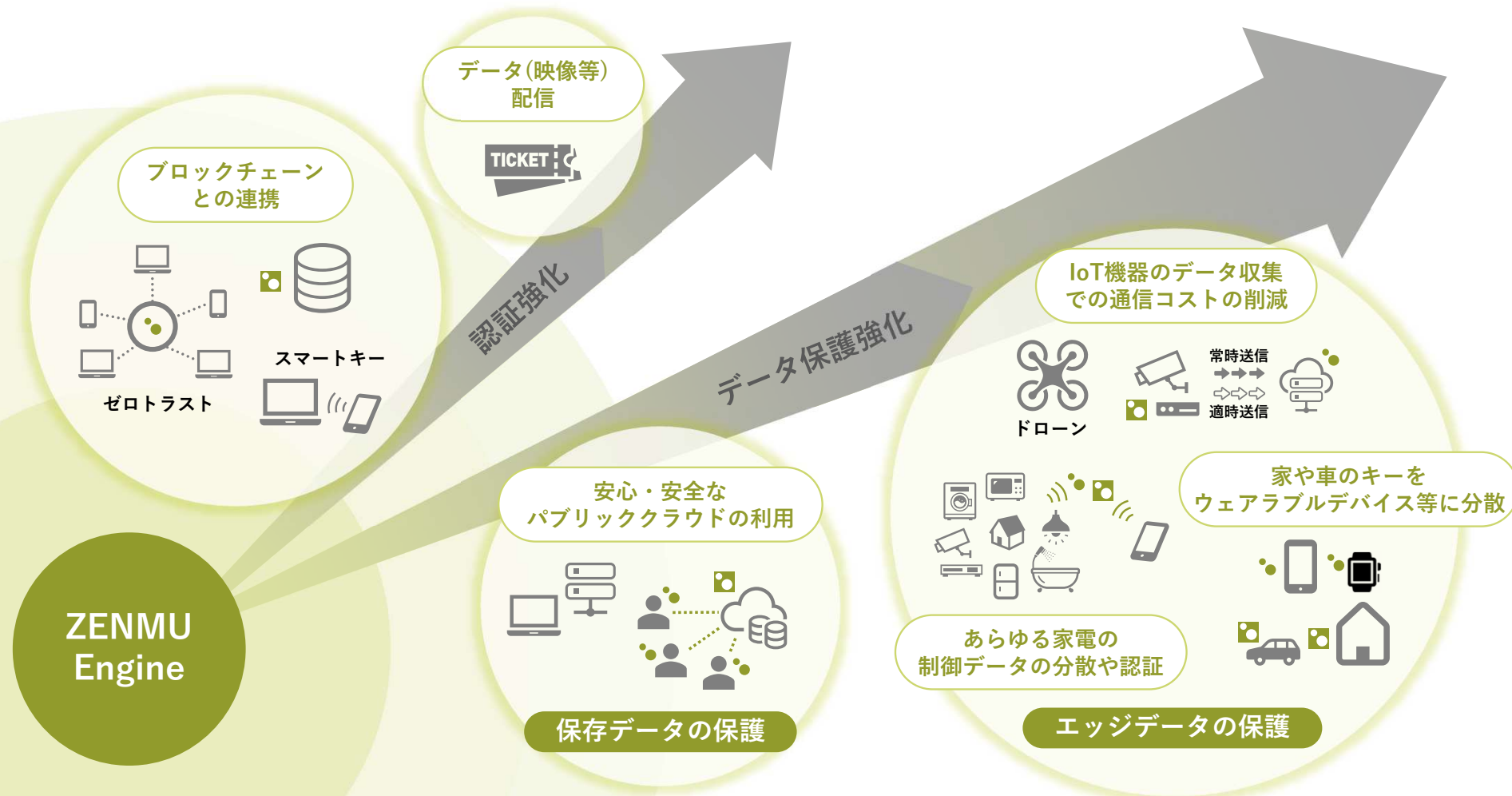
ZENMU-AONTを組み込むメリット



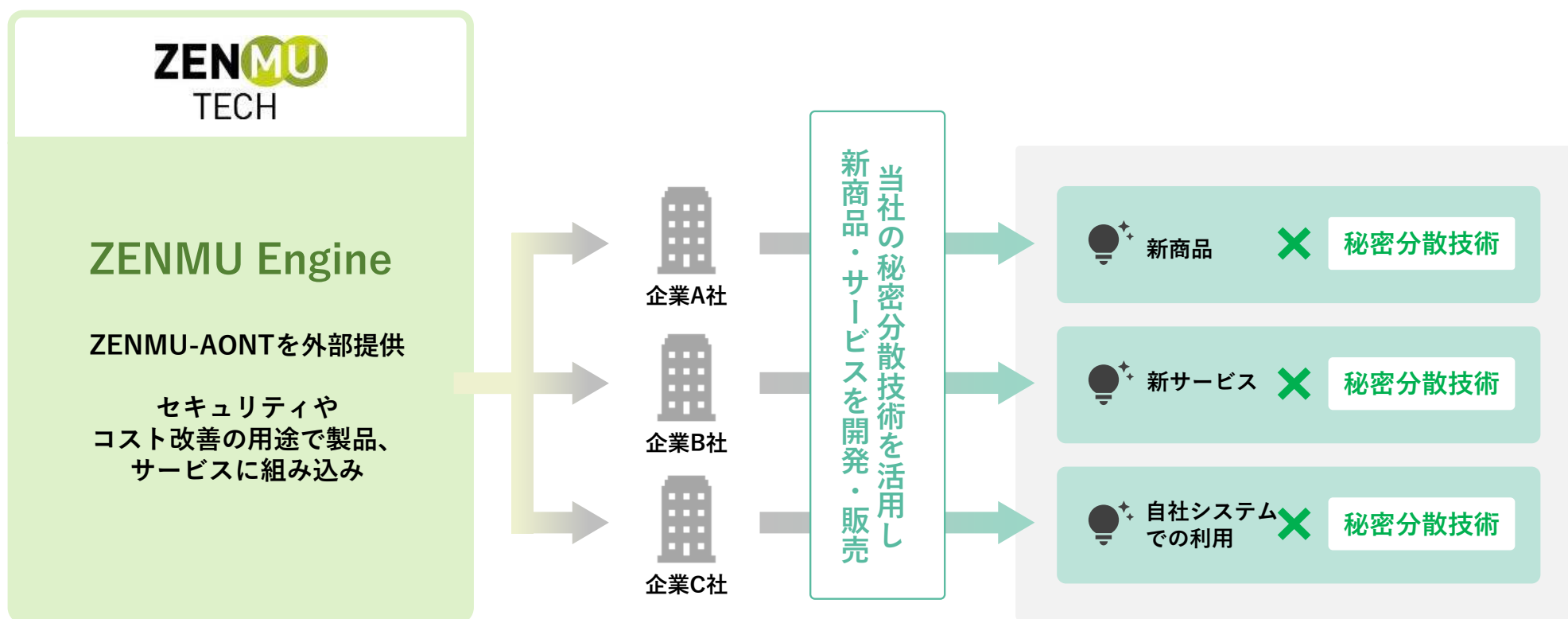
ZENMU Engineを組み込むだけで
秘密分散機能を実装

ひとかたまりで保管、通信する暗号化に対して分散（小さく分割）することで
セキュリティ課題だけでなく保管、通信上の課題にもアプローチが可能

※1 特定のシステムに順応したソフトウェアを開発するために必要なプログラムなどをパッケージ化したもの。



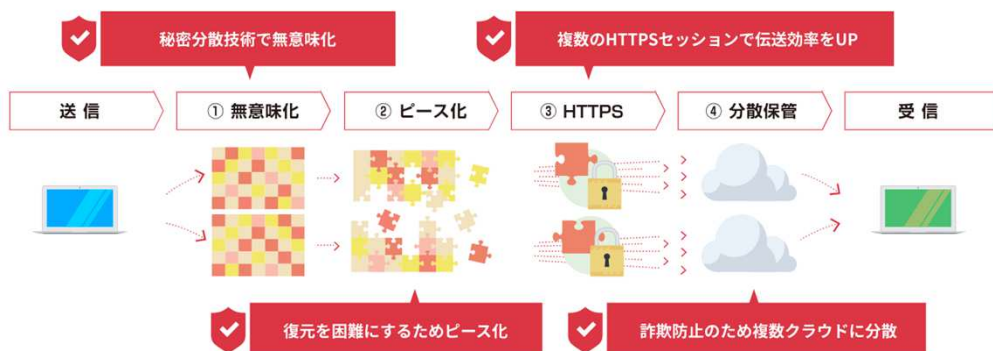
ZENMU-AONTを利用しセキュリティ課題やセキュリティコストを改善するソリューションを創出
販売収益からロイヤルティを獲得





日立システムズ グローバルセキュア転送サービス

秘密分散を含めた4重のセキュリティ技術で
高価な専用線を必要とせず安心な拠点間転送を実現



海外の製造・開発拠点などへの図面・CADデータ転送を
安全かつ容易に。クラウドストレージへのセキュリティ
面での不安解消や物理輸送や高価な専用回線に代わりコ
スト削減にも効果



日立システムズ 秘密分散フォービデオ

監視カメラ映像を安全にクラウドに分散保管、
カメラの稼働状況を24時間365日体制で監視



プライバシー含む撮影データを安全にクラウドに分散保管

ZENMU-AONTを用いた暗号化とは別のアプローチでセキュリティ課題を解決し市場拡大への貢献を図る



車載データ保護・
管理

市場ポテンシャル

約**173**億ドル^(※1)

2030年(世界市場)
※スマートキー



ブロックチェーンと
様々なコンテンツの
組み合わせ・管理

市場ポテンシャル

約**2,520**億ドル^(※2)

2034年(国内市場)



防犯カメラ内データ
の保護

市場ポテンシャル

約**4,362**億円^(※3)

2030年(国内市場)



ドローン内の
データ保護

市場ポテンシャル

約**9,054**億円^(※4)

2028年(国内市場)

※1：TechNavio.「自動車用スマートキーの世界市場」

※3：矢野経済研究所「2025年度 監視カメラ／画像解析システム市場の実態と展望」

※2：マーケットリサーチセンター「ブロックチェーンの日本市場（2026年～2034年）」

※4：インプレス総合研究所「ドローンビジネス調査報告書2024」

アライアンスパートナーであるネクストウェア株式会社と株式会社アイ・ロボティクスと共に、ドローンや移動型ロボットに搭載する技術「インテグリティ・ドローン」の技術検証を推進

市場課題

産業領域や物流領域における有翼型・マルチコプター型の無人航空機であるドローンの活用の用途の広がり

災害時の情報収集等に警察・消防でもドローンや自律移動型ロボットの導入が推進される^(※1)

ドローン、ロボットの機体には、自律移動用のプログラムや飛行経路の情報、撮影したデータ等の機密情報を多数含んでおり、予期せぬ落下等の事故による情報漏洩のリスクがある

ZENMU Engine活用による解決



秘密分散ソリューションを組み込むことでドローンのデータを瞬時に無意味化し情報漏洩を防止

橋梁、一般住宅、大規模建造物などの点検用途での商用化・実用化がより一層進んでいく

- ✓ 各社が展開するドローン事業への展開
- ✓ 国内外の航空機メーカー、ドローン運用業者、自動運転業界、防衛装備業界などへの提案

※1 警視庁「国家公安委員・警察庁防災業務計画」第1-2多様な情報収集手段の整備

秘匿性の高いデータを秘密分散により分割、無意味化したまま計算
暗号技術や秘密計算の専門知識を持たずともアプリケーションに
組み込んで利用することが可能



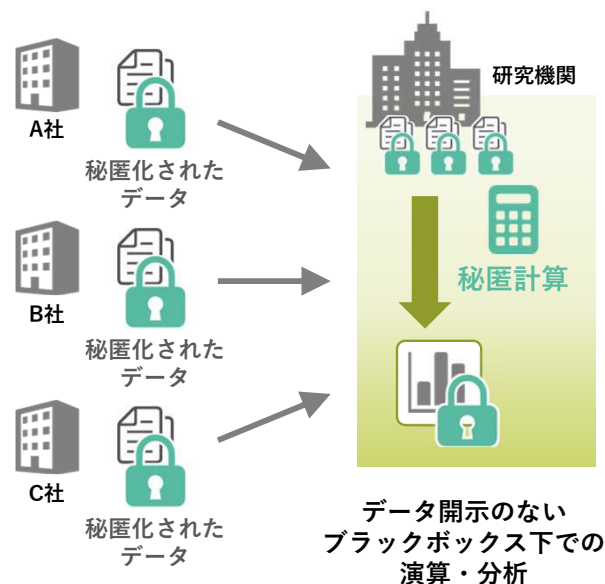
産業技術総合研究所と
共同で研究開発

データ活用における課題

- ✓ 個人情報など秘匿性の高いデータの利活用の促進がハードルが高く進まない
- ✓ 他企業協業によるイノベーションをしたいが、機密データの情報共有がボトルネック
- ✓ 秘匿性の高いデータを第三者が分析する際に、漏洩や改ざんのリスクが発生



QueryAhead®によるソリューション



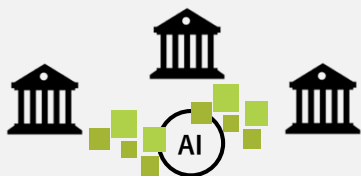
暗号化したデータを
復号することなく
計算処理を実行

暗号技術などの専門知識は不要
PythonとSQLでクエリー可能

社内でのデータ利活用から
外部組織との連携まで
幅広い用途で利用

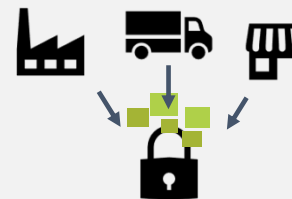
AI・機械学習の活用に伴い、複数の企業などから大量の機密データを一か所に集めて活用
新サービス創出による売上拡大や研究開発、製造コストの改善に寄与することでマネタイズを図る

適用領域の一例



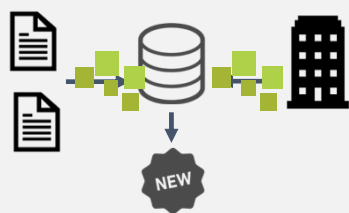
金融・不動産

各銀行が持つ取引データを秘匿化したまま不正検知AIモデルを構築し、共同利用することで業界全体で不正防止を進めることが可能
不動産分野では互いに情報を伏せたまま秘匿マッチングなどに期待



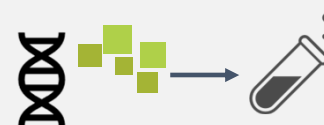
製造・物流

サプライチェーンを構成する企業全体に秘密計算を適用し、各社の機密は維持したまま、企業をまたいでボトルネックを可視化し、購買、製造、物流の多岐にわたって最適化することにより競争力を向上させる



材料開発

個別のデータを秘匿化したまま企業間を越えたデータ連携を行いAIによる実験モデルの精度を向上。
開発期間を大幅に加速しコスト改善や競争力向上につなげる



ヘルスケア

個人情報を含んでいるDNA情報や疾病情報などを各医療機関、製薬会社等とデータを秘匿化したまま共有、分析することで、より最適な創薬や医療サービスが提供できる可能性

3.競争優位性の源泉

社会課題を解決する
秘密分散/秘密計算技術

データの保護に関する社会課題

社会のニーズ サイバー攻撃による被害は年々増加

課題 より高度なセキュリティが求められる時代に



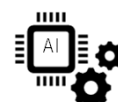
サイバー攻撃関連の通信数(※1)

2014年 約241億 ▶ 2023年 約6,197億

データの利活用に関する社会課題

社会のニーズ AI・機械学習の活用が加速

課題 精度向上のために膨大なデータを使った学習が必要



世界の生成AI市場規模(※2)

2022年 約1.2兆円 ▶ 2030年 約14.2兆円

🔒 従来の、鍵を用いた暗号技術情報漏えい対策



内部不正や人的ミスによりパスワードなどの鍵とともに暗号化した重要情報が漏えいする事態も



分析、利用時には復号（元のデータを復元）する必要があるためセキュリティリスクが生じる

従来型の暗号技術に代わるセキュリティ技術が求められている

※1：NICT「NICTER観測レポート2023」を基に作成

※2：経済産業省 中部経済産業局「兆しレポート テーマ：生成AIを活用した働き方改革の兆し」

	従来の暗号技術	ZenmuTechの取り組み
データの保存時の保護	○ <ul style="list-style-type: none">✓ 従来から暗号化によりデータを保護してきた領域✓ パスワードなどの暗号鍵が流出した場合などに解読されるリスクを排除できずセキュリティ上の課題や運用の負担となっている	<ul style="list-style-type: none">✓ 秘密分散技術でデータ自体を分割した状態で保管や転送をすることで暗号鍵の管理を不要にしセキュリティリスクや運用負担を改善✓ 分割する（小さくする）ことで保存や通信のコストなどの課題にもアプローチ
データの転送時の保護	○	
データの処理時の保護	× <ul style="list-style-type: none">✓ 暗号化したままでは閲覧や計算はできずデータを復元する必要があり漏洩や改ざんのリスクが生じてしまう	<ul style="list-style-type: none">✓ 秘密分散技術を応用してデータを秘匿化したまま計算する秘密計算技術を研究、事業化へ取り組む

※高機能暗号…従来の暗号技術に対して、機能が追加・向上される等の優位性を主張する暗号技術、および、従来の暗号技術では困難であった事象を解決できる等の新規機能を有することを主張する暗号技術
2023年3月 CRYPTREC 暗号技術調査ワーキンググループ「CRYPTREC 暗号技術ガイドライン（高機能暗号）」

新発想のセキュリティ

サイバーセキュリティ技術は「防ぐ」から「無意味化」へ

ZenmuTech特許取得

自社開発
独自の秘密分散アルゴリズム
「ZENMU-AONT」

独自
技術



元データ

現状

通常の暗号化



暗号化された「元データ」を保存

- 暗号は、鍵をパスワードに変えて管理
- 管理するのは、不確実性の高い人間
- 忘れる、使いまわす、盗まれる、解かれる

復元



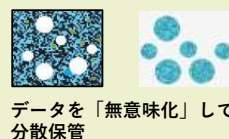
暗号鍵の漏えい、解読などにより、元データが解読されるリスクがある

課題

- ✓ 情報漏洩のおそれ
- ✓ パスワードは増え続けることで管理が難しくなり、同一のパスワードを使い回す懸念

進化

秘密分散

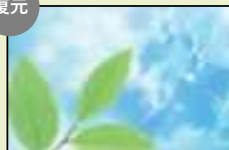


データを「無意味化」して分散保管

- 暗号化した上で、鍵ごと無意味なデータに分散管理
- 分散した無意味なファイルが揃わないとデータが復元しない

2つを重ねて初めて復元

復元



データの無意味化で、元データが解読されるリスクなし

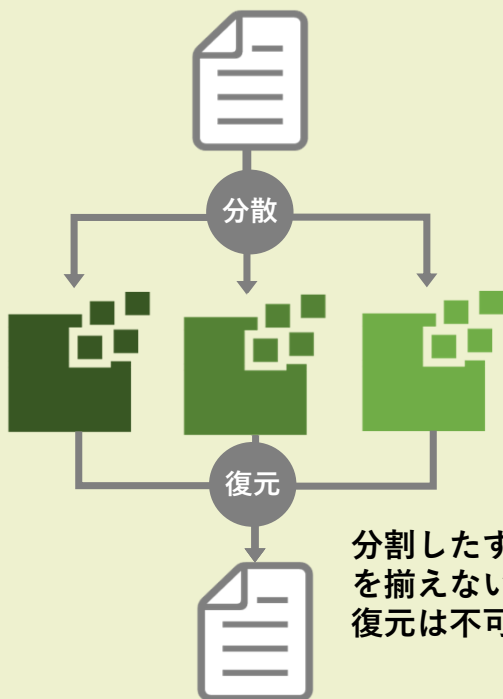
解決

- ✓ データの分散片が保管されているデバイスの紛失や盗難されても、管理者が分散片へのアクセスを停止することでデータ復元は不可能
- ✓ 社外へのPCの持ち出しやリモートワーク等の際、紛失・盗難時の有効な対策になり得る

分割前後でデータの総量が変わらないAONT方式を採用し、分散片の小サイズ化、高速化をさらに追求
低速通信環境や記憶容量の少ないデバイスでも利用が可能

当社

All or Nothing Transformation方式



分割したすべての分散片を揃えないと元データの復元は不可能

特徴

- ✓ 分散片がすべて揃わないと復元できないためより厳格なセキュリティ性を持つ
- ✓ 分散後の総データ量は元データとほぼ同じ。また、分散片のサイズ比を任意に設定可能（元データ100に対し99:1や33:33:33:1など）
- ✓ しきい値分散と比較して分散・復元の処理速度は高速であり、分散片の一方を小さくすることで通信などに適した運用が可能

独自技術

自社開発
独自の秘密分散アルゴリズム
「ZENMU-AONT」

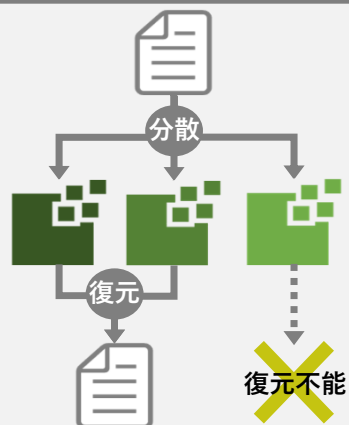
- AONTの特徴である分散片の小ささを更に追及、最小32バイトまで可能
→ 低速通信環境やエッジデバイスでも利用が可能
- 分散片をより小さくすることで処理速度も更に向上
- 安全性についても理論的検証を実施

技術としての競合状況 ～有力な競合のいないニッチな技術領域～

秘密分散技術の中ではAONT方式は後発かつ非主流派の理論

主流である「しきい値分散方式」の技術をもつIT大手企業もあるが当社が主力とするPC向けには不向き

主流派 しきい値（閾値）分散方式



あらかじめ定めた任意の数（＝しきい値）の分散片を揃えることで元データの復元が可能
例) 2/3、3/4...など

特徴

- ✓ ◎分散片の一部がなくとも復元可能
→重要データのBCP（事業継続計画）
DR（災害復旧）に適している

- ✓ ×分散片一つ一つのサイズは
元データとほぼ同じ
例.3分散すると総データ量は元の約3倍
保存や転送、処理時間が増加

例：3個に分散したうち
2個揃えれば復元可能

必ず3つ以上に分散、それぞれの
保管や復元など運用の煩雑さ



しきい値分散方式の特性により総
データ量は増加するため、保存や
転送に負担
PCやモバイルデバイスなどには
不向きな方式

大手IT企業などを中心に
2000年代初め頃から研
究、製品化、普及せず

参入障壁

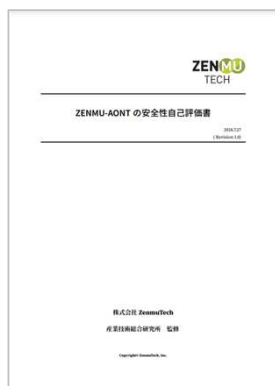
暗号理論の一分野である秘密分散、その中でも主流でないAONT方式について有力な研究者や企業は限定的

主流のしきい値分散方式について技術蓄積のある大手企業の関心は応用技術である「秘密計算」（後述）に関心が移っている

当社の特許等によるブロックにより権利侵害を迂回した新規開発が必要

AONT方式を新たに採用して、新規開発するよりも当社のZENMU Engineを利用したほうが経済的合理性（開発期間の短縮、品質・機能）が高い。

産業技術総合研究所の監修のもとZENMU-AONTの安全性自己評価書を作成 共著論文としてまとめ、査読付きの国際学会でも発表



2018年7月27日 産業技術総合研究所監修のもと安全性自己評価書を作成

評価方法

- ✓ Anand Desaiによる攻撃モデルを用いて計算量的安全性※を評価
- ✓ 単に理論上の安全性だけではなくソフトウェアとしての実装実現性と実用性についても評価

結論

理論面と実装面の両方において十分な安全性を有し実用的な方式である

監修コメント

ZENMU-AONT は通常想定される利用形態において安全であるものと判断できる
(産業技術総合研究所サイバーフィジカルセキュリティ研究センター 首席研究員 花岡悟一郎博士)

- ✓ 2019年にはZENMU-AONTのアーキテクチャおよび理論的安全性検証等を産業技術総合研究所との共著論文「An Extended CTRT for AES-256」として発表
- ✓ 暗号・情報セキュリティに関する国際会議であるThe 20th World Conference on Information Security Applications (WISA2019)においてBest Paper Awardを受賞



※計算量的安全性 = 暗号の解読や署名の偽造などを計算問題として定式化し、これを解く最も効率のよいアルゴリズムの計算量をもって暗号の安全性の評価尺度とする。暗号解読に必要な計算量が利用できる計算機の能力に比較して膨大であり、現実的時間では実行不可能である場合に計算量的に安全と考えるもの

暗号化や秘密分散により秘匿化されたデータを復号・開示せずに
演算・分析し必要な結果だけを得ることが可能

産業技術総合研究所と
共同で研究開発

現状の課題



- ✓ 企業同士がデータを共有するには機密性の高いデータの取得と共有が障壁
- ✓ 大量のデータを使う場合や、複数企業から学習データを提供される場合、あるいは個人情報などの慎重な取り扱いが必要な場合には、データを一カ所に集めることは大きなリスク

秘密計算技術による解決

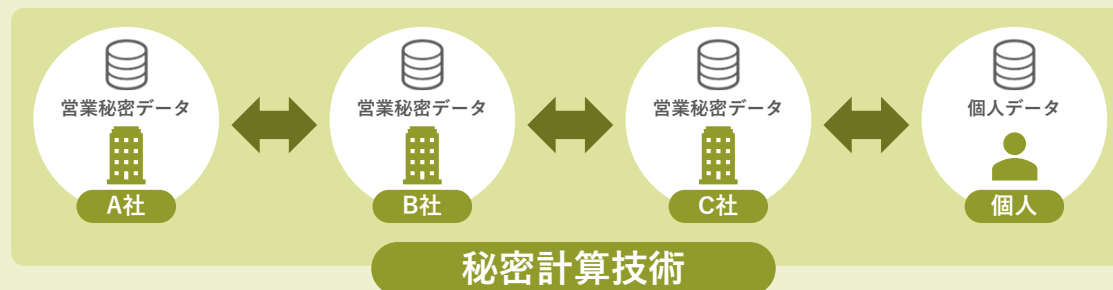
個別化医療

EVインフラ
最適化

金融
不正検知

ものづくり・
物流最適化

電力消費の
見える化

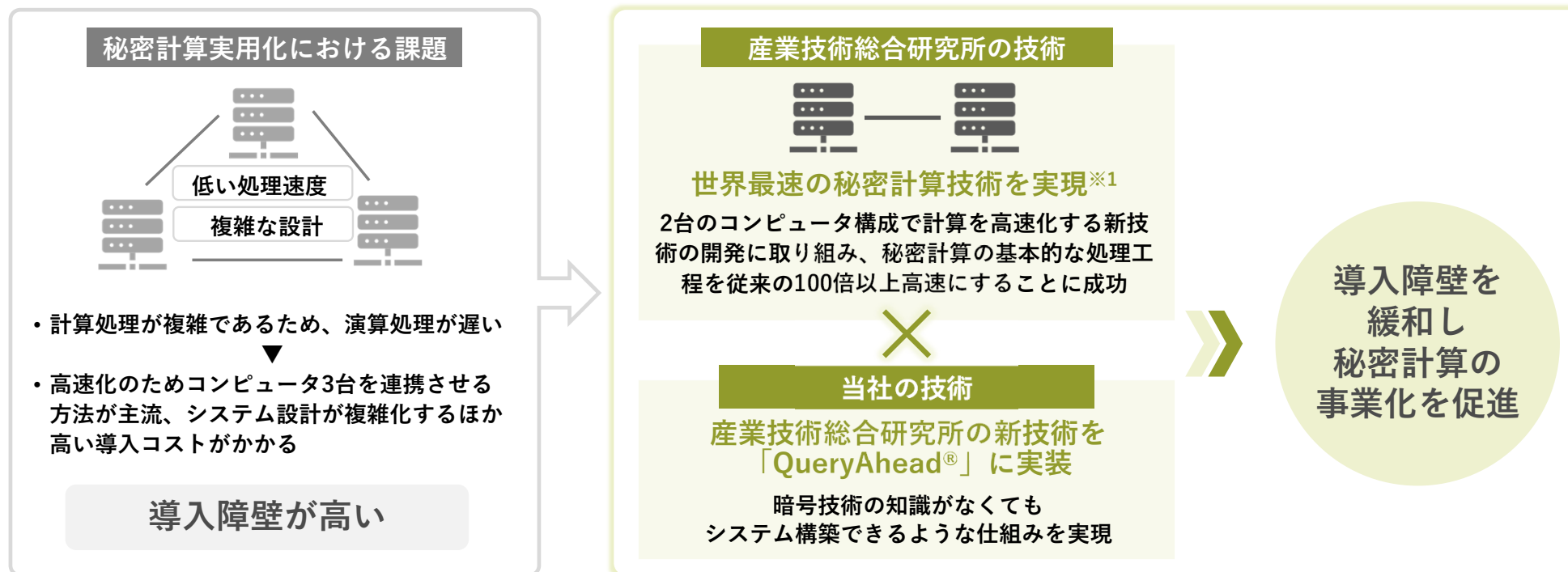


暗号化や秘密分散によって秘匿化したまま計算

- ・ 複数の金融機関の取引情報を結合することによる不正取引検知の精度向上
- ・ ゲノム情報や診療情報を安全に解析することによる創薬やオーダーメイド医療への活用
- ・ 複数の企業を横断し1社単独では困難なサプライチェーン全体の効率化



産業技術総合研究所の新技术 × 当社の秘密分散技術事業化の実績を活かし秘密計算技術の実用化を目指す



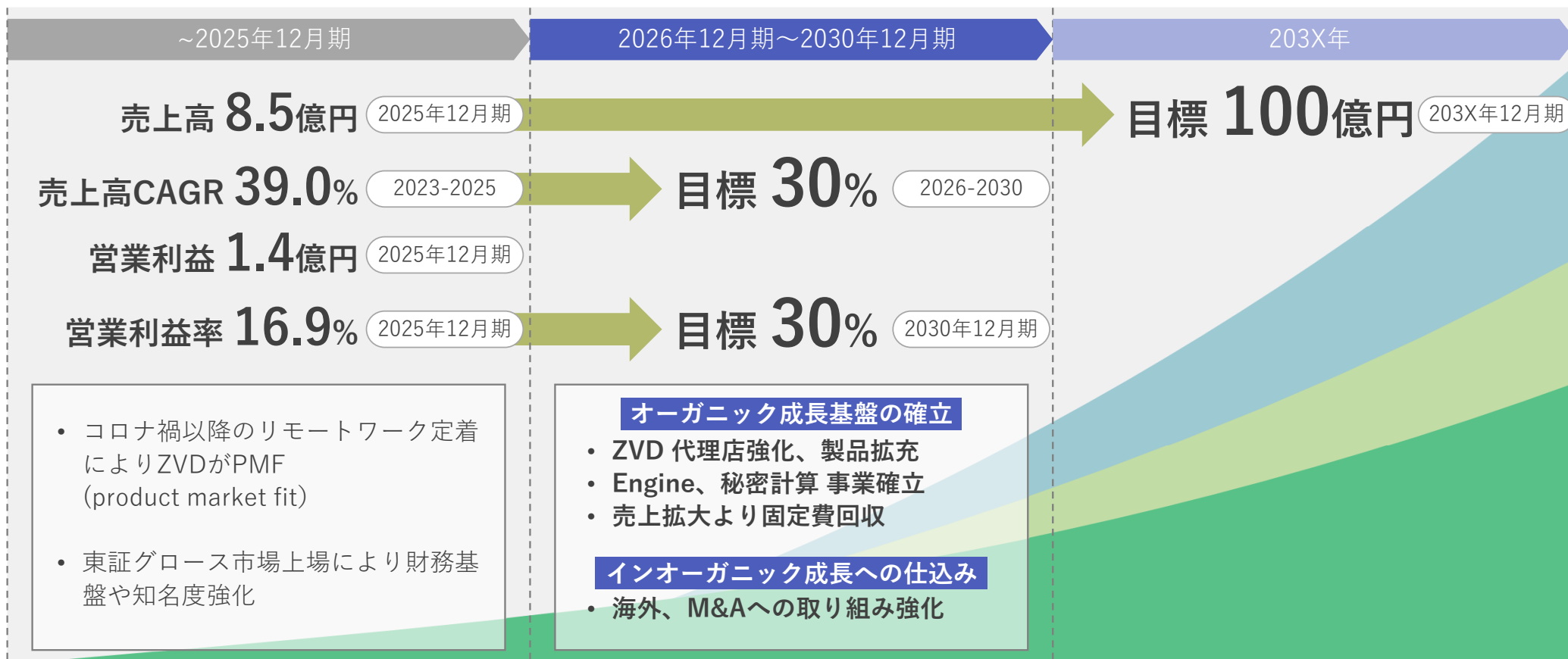
*1: 計算サーバが2台における特定の場合に、世界最速の計算速度を達成した。(詳細はこちらの論文で発表している。Nuttapong Attrapadung, Goichiro Hanaoaka, Takahiro Matsuda, Hiraku Morita, Kazuma Ohara, Jacob C. N. Schuldt, Tadanori Teruya, and Kazunari Tozawa. 2021. Oblivious Linear Group Actions and Applications. In Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security (CCS '21). Association for Computing Machinery, New York, NY, USA, 630–650. <https://doi.org/10.1145/3460120.3484584>)

4.成長戦略

中期成長目標“triple 30 Plan” **2030年12月期 売上年平均成長率30% x 営業利益率30%**

2030年12月期までの中期目標 **売上高CAGR（年平均成長率）30% × 営業利益率 30%**

オーガニック成長を加速させるとともに、インオーガニック成長への施策に取り組み、長期目標では売上高100億円企業を目指す



短期的にはZENMU Virtual Driveによる収益基盤を形成、中長期的には、ZENMU Engine、秘密計算によるサービス充実化を図り、事業領域の拡大と持続的成長を目指す

		戦略	主な施策
短期	<p>情報漏洩対策ソリューション</p> <p>ZENMU Virtual Drive</p>	<p>VDI共存戦略により商談機会創出</p> <p>大企業のPC買替、システム見直しによりZVDシェア拡大</p>	<ul style="list-style-type: none"> ✓ 大企業中心にアプローチ ✓ 自社直販とSierなど販売代理店網を拡大し販売力を強化 ✓ カスタマーサクセス活動によるリテンションとアップセル
中長期	<p>秘密分散ソリューション</p> <p>ZENMU Engine</p>	<p>アライアンス戦略強化により事業を拡大</p> <p>OEMプロダクト群の形成</p>	<ul style="list-style-type: none"> ✓ 既存アライアンスにおいて、ドローンや車載データ、監視カメラ、AIなどの成長分野においてZENMU Engineの活用を進める ✓ アライアンスパートナー数の拡大 ✓ 秘密分散技術の特性を活用したOEMプロダクト群の形成
	<p>秘密計算ソリューション</p> <p>QueryAhead®</p>	<p>AI、機械学習の加速とともに事業を拡大</p> <p>海外事業展開</p>	<ul style="list-style-type: none"> ✓ 産総研との共同研究による認知度向上への取り組み ✓ 第三者によるQueryAheadの安全性証明を検討 ✓ QueryAhead® のPaaSソリューション転換によるPLG ✓ 秘密計算適用領域へのアプローチ

販売代理店の拡充：代理店のポジショニングにあわせた販売シナリオ

800万人以上の国内VDIユーザーに対し現時点での
ZENMU Virtual Driveのユーザー数は約1%と獲得余地は大きい

国内の全ホワイトカラー
2,700万人^{※1}

国内VDIユーザー数
802万人^{※2}

ZENMU Virtual Drive
ユーザー数
11万人^{※3}

対 VDI市場戦略（置き換え、共存戦略）

置き換え

引き続きPCライフサイクル管理を強みとするSierとの連携を強化。
コスト、利便性などVDIとの比較優位性を訴求

共存

新たにVDI、DaaSの販売実績の大きいSierとの連携を開拓。
VDIのメリットはそのままに併用による付加価値を提案

対 非VDI市場戦略

中小向け、士業事務所向け提案

中小企業向け、会計事務所特化など、特色をもった中堅Sier、
販売会社を軸にコストや導入のしやすさを訴求

※1：労働力調査（令和5年総務省）の基づく全就労者数と国勢調査（令和2年）に基づくホワイトカラー比率から推計。

※2：VDIユーザー数:2024年実績値 2025年6月IDC市場予測資料

※3：2025年12月現在、買い切りライセンスによる保守契約を含む

VDIおよびDaaSとの併用を前提とした廉価版「ZLE」と 大企業のBCP需要に応える「ディザスタリカバリオプション」を新たにリリース

課題

VDIの利用方式として従来の主流であるハードディスク(HDD)を内蔵しないシンクライアント端末での利用から、通常のPCで利用するケースが増加傾向。ユーザーがローカルにデータを保存できるため利便性は高い一方で、PCの紛失・盗難時の情報漏洩リスクが懸念。

2025年2月から新製品「ZENMU Virtual Drive Limited Edition」を月額500円で提供開始
VDI及びDaaS利用中のユーザー向けVDI利用と併用を前提とした新たな提案

ZENMU Virtual Drive Limited Edition (ZLE)

- ✓ VDI・DaaSの利用環境で、Windows PCのローカルに保管したデータを保護
- ✓ VDI・DaaSとの併用に必要な機能に絞り込み、安価で提供

PCの更新タイミングに限られない導入機会を創出

課題

自然災害の発生やAWS東京リージョンへの依存によるシステム停止リスクの高まり、企業の事業継続計画への対応強化の要求を背景に、高可用性と冗長性を備えたIT環境の重要性が高まっている。

「ZENMU Virtual Drive ディザスタリカバリ オプション」は、大規模災害時にお客様の接続先を大阪リージョンに振り向け、継続的な利用を可能に



マルチリージョン

金融系など大企業からの需要に対応、有償OPとしてアップセル

協業・提携によるPC向けトータルソリューション化

他社のセキュリティ製品との同時利用や共同販売によるタッチポイント創出、総合的なセキュリティ実現を図る

マルチOS、マルチデバイス/クラウド対応

現行のWindows PC向けだけでなく macOSやPC以外のスマートフォン・タブレットなどデバイスの種類を選ばず利用可能なサービスの開発を検討

PC領域

非PC領域 (スマートフォン、タブレット等)

Windows OS

メイン市場として引き続き製品強化に注力

① 連携製品の拡大によるトータルソリューション化

デバイス管理、バックアップ、認証など他社のセキュリティ製品との同時利用により総合的なセキュリティを実現を図る

macOS

② ZVD Mac版の開発を検討

広告、ITなどの需要に対応

その他

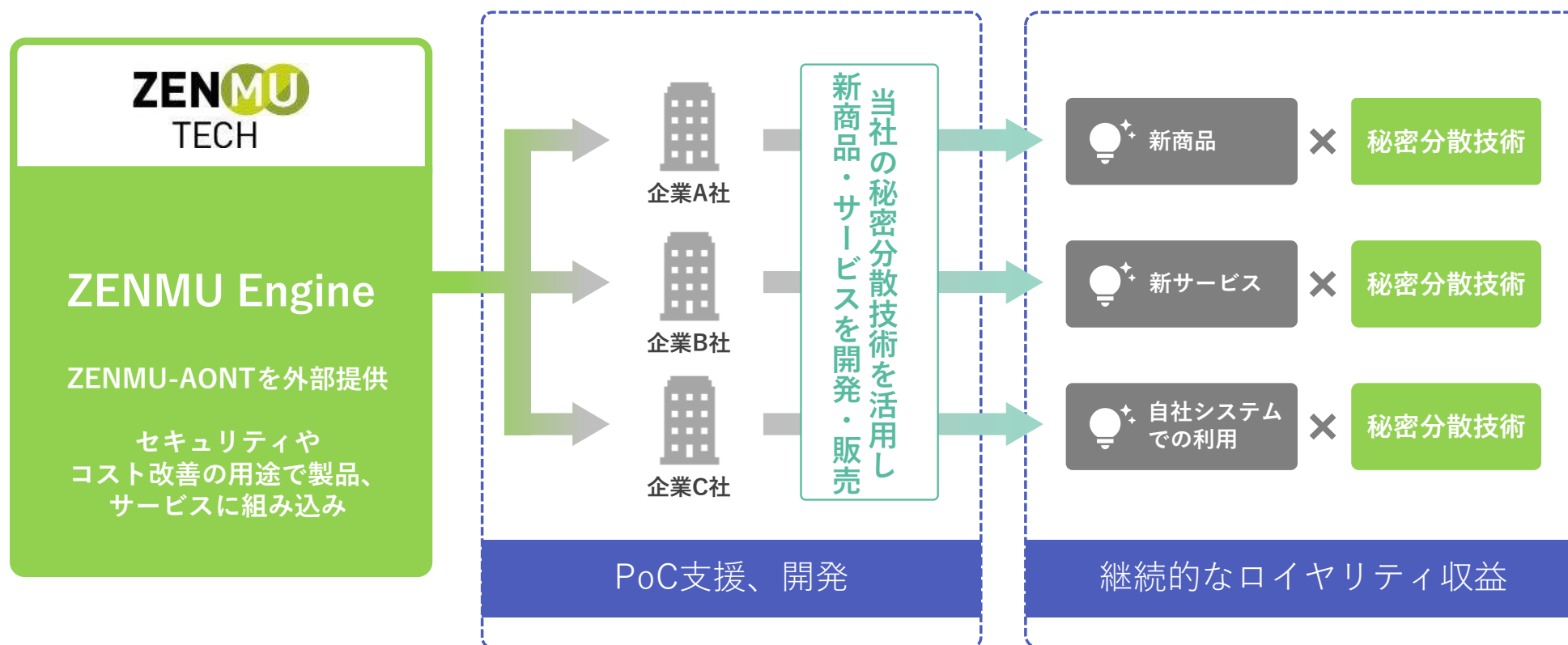
(Linux、Chrome OS等)

③ クラウドデータ保護製品の開発

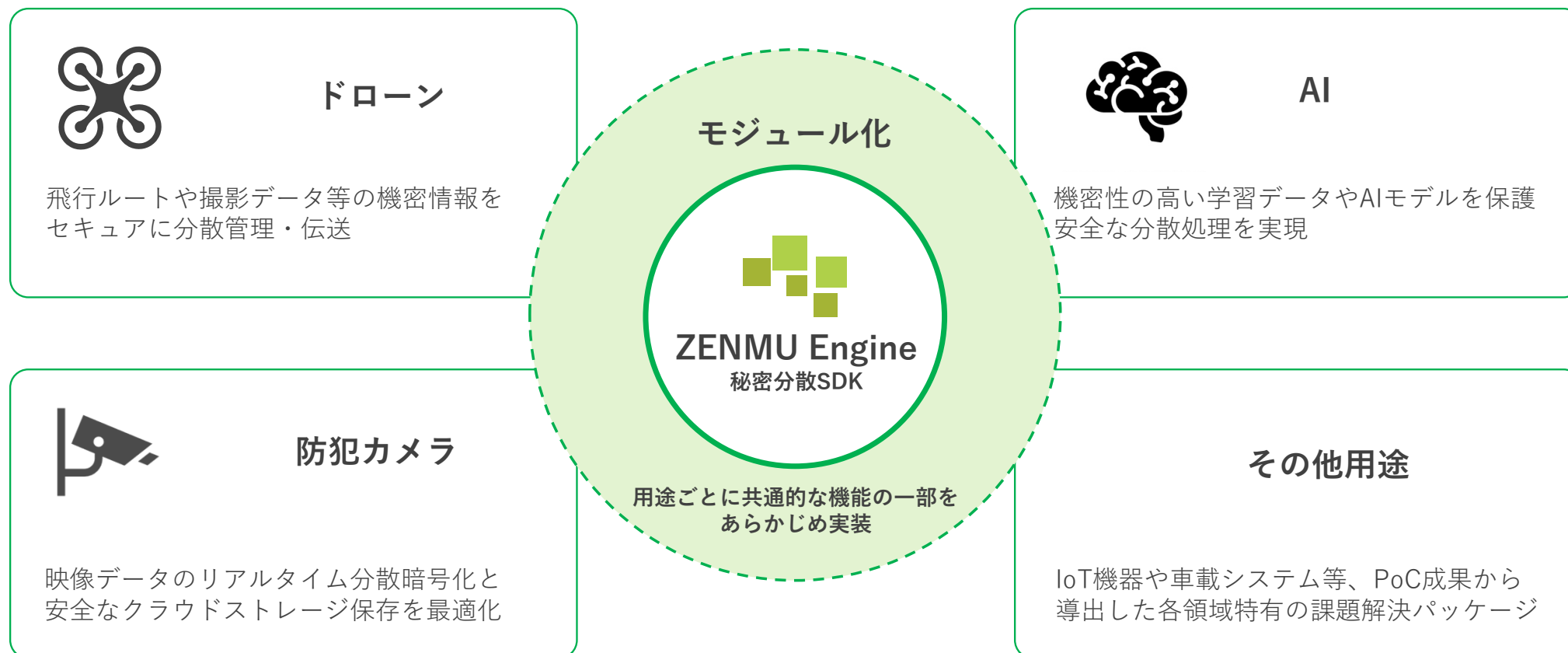
PC内ではなくクラウド側のデータを秘密分散で保護する製品の開発に着手。

ブラウザベースで秘密分散、復元に対応させることでプラットフォームを選ばずPCだけでなくスマートフォンやタブレットでも同じデータに接続可能なマルチデバイス対応を実現

企画/提案→検証→開発→販売というパイプラインの拡大、スピードアップのため採用や専任化により体制を強化



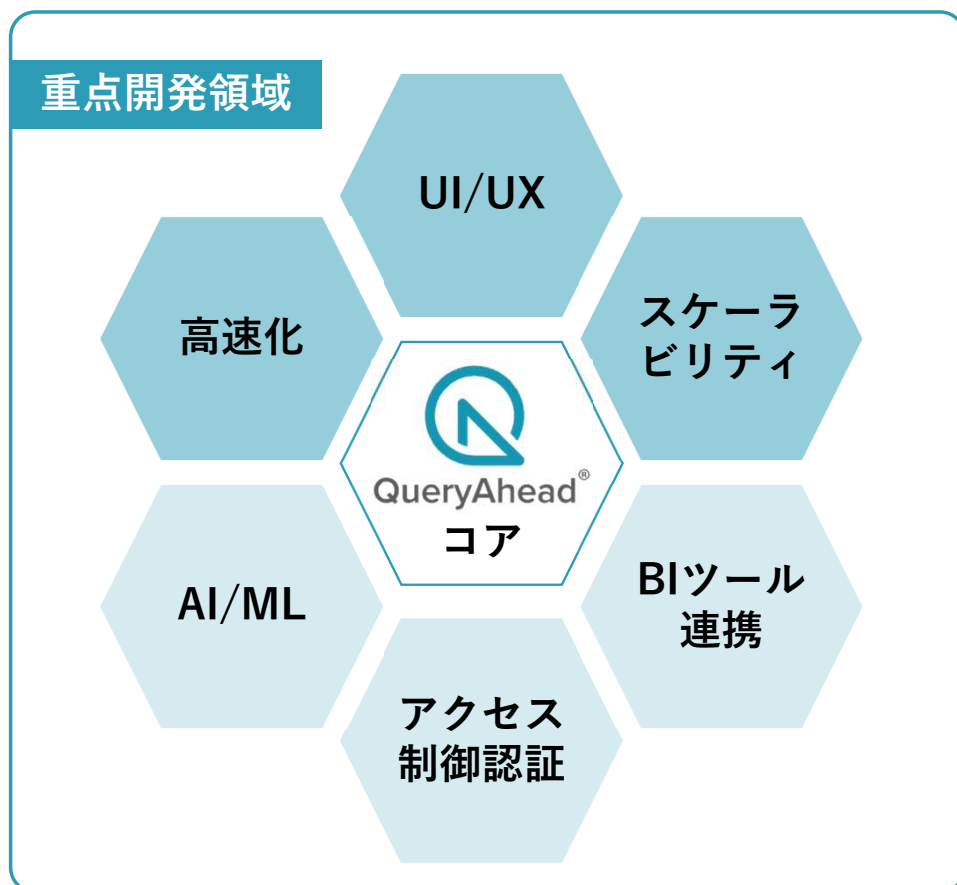
Engineの単体提供に加えて、これまでのPoCから抽出した各領域の課題、用途に応じた共通的な機能の一部を加えたモジュール化を行うことでお客様側での製品開発期間の短縮、コストの大幅削減を実現



プロジェクトの性質上、非公開の案件も相当数が進捗しており、
イノベーション創出への萌芽が着実に現れ始めている

	プロジェクト	概要	企画/準備	実証	契約	プリサービス	リリース予定
Engine	<ul style="list-style-type: none"> セキュリティソリューション開発 	文教、自治体向けソリューションのセキュリティ強化					2026 RevoWorks ZENMU-Storage
Engine	<ul style="list-style-type: none"> ファイル転送ソリューション開発 	複数のパートナーとデータ転送や共有サービスのセキュリティ強化					2026
Engine	<ul style="list-style-type: none"> ドローンプロジェクト 	データ転送、保管に関するセキュリティ強化					2026
Engine	<ul style="list-style-type: none"> AIプロジェクト 	AIで利用するデータについてセキュリティと利便性を両立					2026
Engine	<ul style="list-style-type: none"> 医療系プロジェクト 	医療分野のDXに対して安価なセキュリティ基盤の提供					2026

機能強化とビジネス開拓に並行で取り組む。リピート案件を中心とした受託収益を確保しながら商用サービス化に向けてアライアンスを開拓



Development

回帰や次元圧縮といった人工知能や機械学習を用いたプライバシーデータの活用需要が高いため、これらに対応するモジュール開発をさらに充実させるとともに、ビッグデータの高速な秘密計算処理を実現するシステムリファインメントをプライオリティとする

Collaboration

安全性の担保、最先端技術の導入と普及、世界トップレベルの学会への発信といったあらゆるフェーズにおいて産総研との協業をさらに深化させ、グローバルで価値創出が可能なソリューションを開発していく

Business

豊富な国プロ参画の経験・知見をベースに国家安全保障におけるデータセキュリティ戦略に貢献していくとともに、市場における着実な社会実装、価値創出をさらに具現化し、官民共創のロールモデル確立を追求していく

Gov（国）プロジェクト関連の受託案件（フロー収益）中心の売上からPaaS化「収益・市場・導入」のボトルネックを解消し、継続的な成長基盤を構築する。

現状の課題



収益構造

売上の8割強が「国プロ案件」等の労働集約型ビジネス。エンジニアリソースが開発に拘束される「売り切り型（フロー）」であり、収益の予測と積み上げが困難。



市場の限界

オンプレミス志向のままでは導入先が金融・医療などの「超規制業界」に限定されやすい。クラウドが主流（71%）である世界の秘密計算市場の成長セグメントを取り込めていない。



導入障壁

専用環境構築やデータ移動が必要であり、リードタイムが長期化。顧客が手軽に試せない。

QueryAhead as a Service

期待される効果



スケーラビリティ

汎用ソリューションとしてのサブスクリプション（継続課金）モデルへ移行し、安定的かつ継続的な成長基盤を構築（ARR み上げ）。



成長セグメントにフィットさせTAMの最大化

世界市場のボリュームゾーンへ適合
データウェアハウスとの連携を容易にし
可用性を向上。



導入最適化（Product-Led Growth）

無料トライアル→小規模PoC→本番採用」のPLG（Product-Led Growth）ファネルを確立し、顧客獲得効率を向上。

情報セキュリティ市場は海外のシェアが大きいいため、今後は米国等への海外展開も見据え、事業化へ向けて積極的な投資を行う予定。各地域において市場調査段階、展示会の出展やパートナー開拓を実行中。

欧州(EU)

- ✓ GDPRによる個人情報に関する厳しい保護規制
→ 制約下での利用について秘密計算に商機
- ✓ 今後の市場調査を検討

北米(USA)

- ✓ 2022年から展示会出展など
市場調査、パートナー開拓を推進

APAC

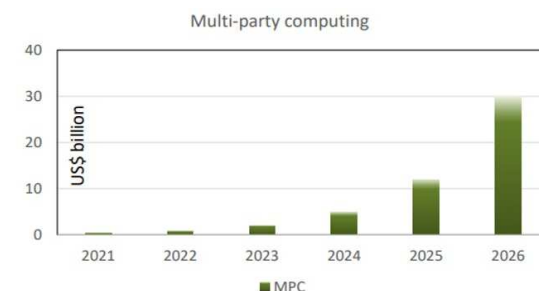
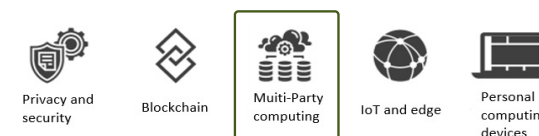
- ✓ DXが進みAPACのHQが集中する
シンガポールへの進出を検討
- ✓ 台湾では電子企業等向けに
Engine紹介のため展示会出展も検討

※ CONFIDENTIAL COMPUTING CONSORTIUM 「Common Terminology for Confidential Computing」

世界市場規模

2024年 160-180億ドル ➡ 2026年(推定) 520-540億ドル

当社が採用する
「Multi-party computing」領域の市場規模



2026年3月、リアルタイム・ビッグデータ解析プラットフォームを提供する台湾のBigObject Inc. と、機密データを安全に活用しながら高性能なデータ分析を可能にするプラットフォームの実現に向け戦略的協業を目的とした覚書（MOU）を締結。



パートナー

BigObject社（台湾）

独自のインメモリ技術を活用した超高速なビッグデータ分析やエッジコンピューティング領域に強みを持つテクノロジー企業。スマートマニュファクチャリングや金融分野で豊富な実績を持ち、本提携を通じて高度なセキュリティ領域へ事業を拡大。








台湾のデータ活用政策

データ駆動型社会とAI推進の加速

デジタル発展部（moda）の主導によるオープンデータ政策や「台湾AI行動計画」のもと、医療やスマートシティ分野でのデータ利活用が強力に推進中。データの積極活用と強力なプライバシー保護の両立が国家的な急務となっており、本協業の技術が強く求められてる。



マテリアルズ・インフォマティクス（AIや機械学習、ビッグデータを活用して新材料探索を高速化・効率化するデータ駆動型の研究手法）を中心に複数のPoCが進行中

	プロジェクト	概要	企画/準備	実証	契約	プリサービス	リリース予定
Query Ahead®	• Gov（国）プロジェクト	量子コンピュータ、インフラ領域におけるプライバシーデータ利活用					2026～2027
Query Ahead®	• 民間プロジェクト(MI)	マテリアルズ・インフォマティクス分野における先進的なデータ利活用					2026
Query Ahead®	• 民間プロジェクト(金融)	金融機関向けのプライバシーデータ利活用					2028
Query Ahead®	• 台湾BigObject	BigObjectの知見、ネットワークをもとに製造、金融、ヘルスケア領域でのデータ基盤構築をはかる					2026～2027

IPOの調達資金は、下記項目への充当を計画

項目	2025年12月期	2026年12月期	2027年12月期	目的
採用費 および人件費	計画 45百万円 実績 39百万円	計画 130百万円	計画 236百万円	将来の成長事業と位置付けるQueryAheadによるOEMサービスの拡大により中長期での事業領域の拡大及び成長に向け、数学、暗号理論等に通じたエンジニアや事業企画やビジネス立ち上げの経験を有す者など高度な人材を確保することに充当する目的であります。

リスク情報

当社の事業展開その他に関するリスクについて、主な事項を記載しております
その他のリスクは、有価証券届出書の「事業等のリスク」をご参照ください

項目	主要なリスク	リスクの概要	可能性	影響度	対応方針
事業環境	技術革新、事業環境の変化による競争力の相対的な低下	技術革新への対応の遅れや、市場環境の急速な変化、競合のより優れた技術の台頭	高	高	技術開発及び各研究機関との研究成果の各種学会、カンファレンス等での発表、各種メディアへの情報発信などの取り組みにより、当社製品及びサービスの競争力の維持向上に努めております。
	特定事業への依存に係るリスク	主力サービスであるZVDに関する売上高の割合が高く、これを含めた秘密分散事業の売上構成は2025年12月期において82.2%と依存度が高くなっております	低	高	ZENMU Engineを用いたOEMの強化や、秘密分散技術を応用させた秘密計算ソリューションの研究開発を進める等、特定サービスへの依存低下を進めております。
会社組織	人材の育成・確保に係るリスク	当社が属する情報セキュリティ分野においては、特に専門的な技術を持ったエンジニアや業界・技術に通じた営業担当者の獲得は難しい状況にあります。そのため、適切な人材を十分に確保できず、あるいは優秀な人材が社外へ流出した場合には、当社の経営戦略の遂行上、影響を及ぼす可能性があります。	中	高	積極的に優秀な人材の採用、育成に注力し、従業員の働きやすさを重視したりリモートワーク等の業務環境の整備によるワークライフバランスの確保や従業員のウエルビーイング（健康かつ健全な心と身体である状態）の維持向上の推進を図ることで、人材の定着に努めております。

項目	主要なリスク	リスクの概要	可能性	影響度	対応方針
その他	知的財産権に係るリスク	秘密計算データソリューション「QueryAhead」では産業技術総合研究所の開発したソースコード（※1）について同研究所の子会社として知財および共同研究の管理を行う株式会社AIST Solutionsから許諾を得て使用しております。	低	高	当該ソースコードの使用については2091年12月31日までの使用許諾契約を締結済みであり、また、秘密計算の処理自体は当該ソースコードに依存することなく実現しているものであることから、当社の事業及び業績に影響を及ぼす可能性は限定的であるものと考えております。 また、同研究所との共同研究契約を通じて、秘密分散技術、秘密計算技術の双方について理論面での高度化を継続的に図っており、同研究所との協力関係の維持および強化について今後も取り組んでいく方針です。

※1 「ソースコード」

コンピュータへの指示や一連の処理手順などをプログラミング言語によって表記したものを。

QueryAheadにおける産総研が開発した「秘匿シャッフルプログラム」ソースコードはデータを秘匿化したまま大ききの順番に並べる機能を担っており、最大値、最小値を求める、等の処理を実現しています。

本資料の取扱いについて

本資料には、将来の見通しに関する記述が含まれています。これらは当該記述を作成した時点における情報に基づいて作成されています。これらの記述は、将来の結果を保証するものではなく、リスクや不確実性を内包しています。その結果、将来の実際の業績や財務状況は、将来予想に関する記述によって明示的または暗黙的に示された将来の業績や結果の予測とは大きく異なる可能性があることをご留意ください。

これらの将来展望に関する表明の中には、様々なリスクや不確実性が内在します。すでに知られたもしくは、未だに知られていないリスク、不確実性その他の要因が、将来の展望に関する表明に含まれる内容と異なる結果を引き起こす可能性があります。

また、本資料に含まれる当社以外に関する情報は、公開情報等から引用したものであり、かかる情報の正確性、適切性等について当社は何らの検証も行っておらず、またこれを保証するものでもありません。

当資料のアップデートは、今後、毎年1回、3月頃を目途として開示を行う予定です。次回は2027年3月を予定しております。