



# SecuAvail

## 会社説明資料

株式会社セキュアヴェイル (3042)

- I. 会社概要
  - II. 中間決算状況
  - III. 中期業績目標
  - IV. 企業価値向上に向けて
  - V. 成長戦略
-



# I. 会社概要

## 株式会社セキュアヴェイル

代表取締役 米今 政臣（よねいま まさおみ）

1961年6月5日（64歳）

愛媛県松山市出身

### 「経歴」

- ・外資系コンピュータメーカーにて営業として勤務
- ・大手インテグレーターにて営業管理職・事業立ち上げ
- ・株式会社セキュアヴェイル 設立（2001年8月） 代表就任
- ・株式会社キャリアヴェイル 設立（2017年5月）
- ・株式会社LogStare 設立（2020年8月） 代表就任

### （退任）

- ・株式会社セキュアイノベーション 2015年設立（社外取締役）
- ・株式会社インサイト （2018年買収 社外取締役）



会社名	株式会社セキュアヴェイル (英文表記：SecuAvail Inc.)
創業年月日	2001（平成13）年 8月 20日
代表者	代表取締役社長 米今 政臣（よねいま まさおみ）
証券コード	3042
従業員数（連結）	106名（2025年3月31日現在）
事業内容	コンピュータセキュリティの運用・監視・ログ分析サービス
本店所在地	〒530-0044 大阪府大阪市北区東天満1-1-19 アーバンエース東天満ビル
子会社	株式会社キャリアヴェイル 株式会社LogStare

## 当社の使命（ミッション）

お客様のシステムセキュリティを確保し、  
事業運営を安心して継続されるためのシステム運用支援者として、  
安全で役立つサービスを提供する会社として、  
末永くお付き合いいただける企業を目指してまいります。



<b>Security</b> セキュリティ（ソフト）マネジメント ネットワークの脅威から保護	<b>+</b>	<b>Availability</b> システム機器（ハード）マネジメント 安定したシステム稼働を継続
1 緊急セキュリティ対応 		5 障害復旧支援 
2 最新セキュリティ技術対応 		6 システム運用 
3 ログ管理/分析 		7 セキュリティ機器監視 
4 問い合わせ対応 		8 保護対象機器監視 

# 沿革

# SecuAvail

販売パートナー: アライドテレシス様、NECネクサソリューションズ様、NTTビズリンク様、キャノンITソリューションズ様、キャノンシステムアンドサポート様、KDD様、Coltテクノロジーサービス様、他……



 **NetStare**  
ファイアウォール運用・監視サービス『NetStare (ネッツステア) Ver.1.0』リリース

**SecuAvail**

コンピュータネットワークセキュリティとログ分析のサービスを提供する目的で設立



2003年  
1月  
現本社へ移転

2003年  
10月  
帝国ホテルタワーオフィスに東京ランチを開設

大阪証券取引所へ上場

2006年  
6月

NRIセキュアテクノロジー株式会社様と資本業務提携、主要な取引先となる。

2009年  
10月



2016年  
10月  
東京ランチを東京本部に改称。中央区の聖路加タワーに移転

東京証券取引所の市場区分再編に伴い、グロース市場へ移行

セキュリティエンジニアの派遣の完全子会社『(株)キャリアヴェイル』を設立

2017年  
5月

**CareAvail**

**LogStare**

2020年  
8月

セキュリティ運用監視基盤の開発及び販売の完全子会社『(株)LogStare』を設立

セキュリティエンジニアに代わって、システムトラブルやセキュリティインシデントの提示や原因、対処方法を示す生成AIのセキュリティ運用監視基盤の販売開始

2022年  
4月

2023年  
6月

病院向けランサムウェア攻撃の検知サービス「NetStare for Medicalシリーズ」、アマゾンAWSのクラウド型ログ分析・監視「LogStare For AWS」、その後は、Microsoft365対応「LogStare M365」、Boxログ分析及びGoogle Workspaceログ分析にも対応した商品群をリリースし、ゼロトラストにおけるサービスを拡充

2025年  
6月



# セキュアヴェイル創業ストーリー



セキュリティ運用サービスの将来性に着目

「創造・挑戦・信頼」を理念として  
2001年8月にセキュリティ専門として創業

SOCという言葉がない時代から  
24/365の運用監視サービスを提供

Log管理基盤プラットフォームを自社開発

2006年6月に上場（当時JASDAQ市場）

2008年 リーマンショック

ストックビジネス拡大へ（営業範囲拡大路線）

2017年 キャリアヴェイル設立

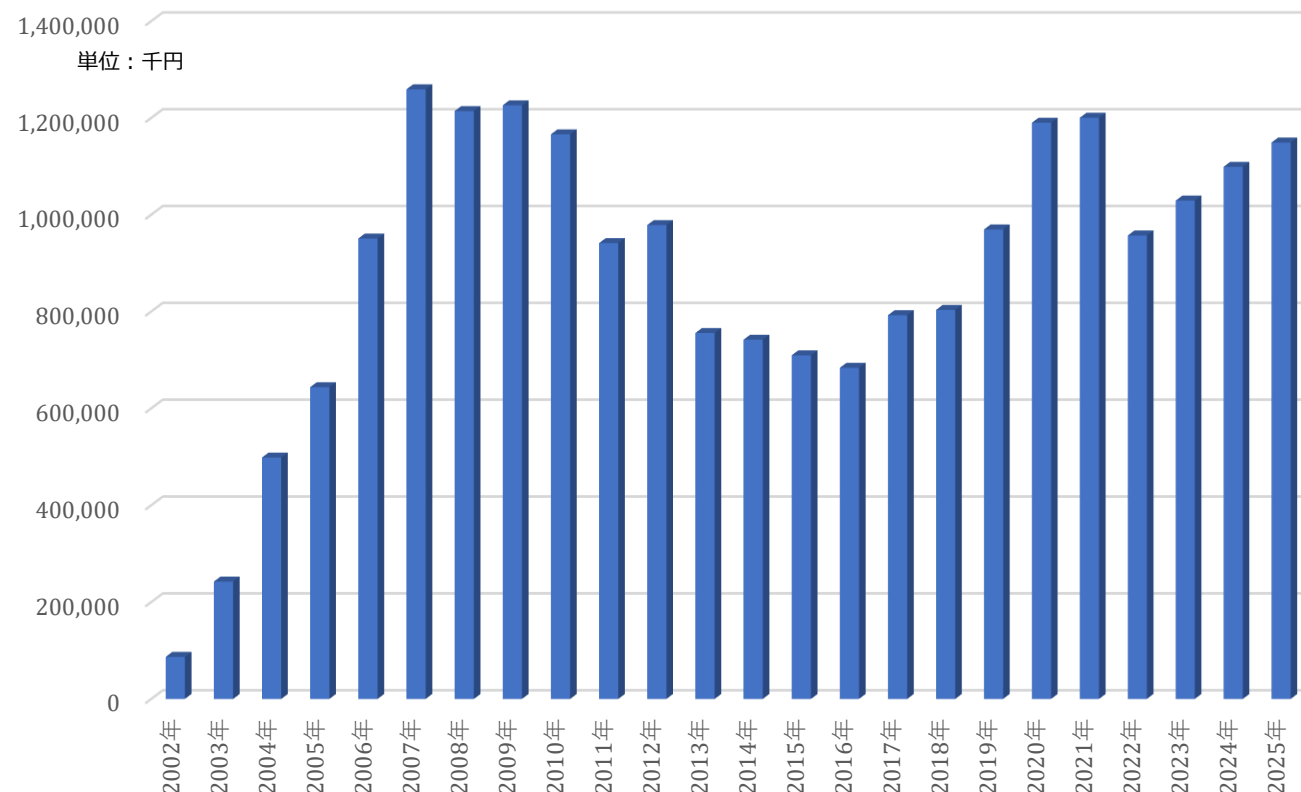
LogStare新バージョン開発スタート

2020年 コロナウィルス蔓延

2020年 LogStareル設立

Aiを活用した製品開発・販売へ  
何故、医療及び製造現場の市場開拓

売上高推移





当社グループの主たるビジネスである情報セキュリティ事業は、セキュリティ運用監視サービス「NetStare（ネットステア）」を主に展開する「株式会社セキュアヴェイル」、より付加価値の高いサービスを提供するため、「ユーザーの運用に役立つ」というサービスコンセプトの下に各種セキュリティ運用基盤の開発・販売を主たる事業とする「株式会社LogStare（ログステア）」の2社の事業部門から構成されております。

自社開発した各社のサービスの特徴が、グループとしての競争優位性を実現しています。

## 株式会社セキュアヴェイルの提供する



「NetStare®」とは、24時間365日体制でお客様のネットワークインフラを監視し、機器故障、通信障害、サイバー攻撃などをいち早く発見する、統合セキュリティ運用サービスです。SOC (Security Operation Center)とNOC (Network Operation Center)を融合させたプロフェッショナルサービスであり、日々のシステム監視やセキュリティ運用はもちろん、機器の設定代行、ログ分析・リスク分析、セキュリティポリシーの改善提案、ネットワークの脆弱性診断など、お客様のITセキュリティを総合的に支援する、業界でも数少ない自社開発による純国産のSOCサービスです。

## 株式会社LogStareの提供する



「LogStare」とは、システム監視、ログ管理、AI予測、すべての機能を1つのソフトウェアで実現する、次世代のマネージド・セキュリティ・プラットフォームです。

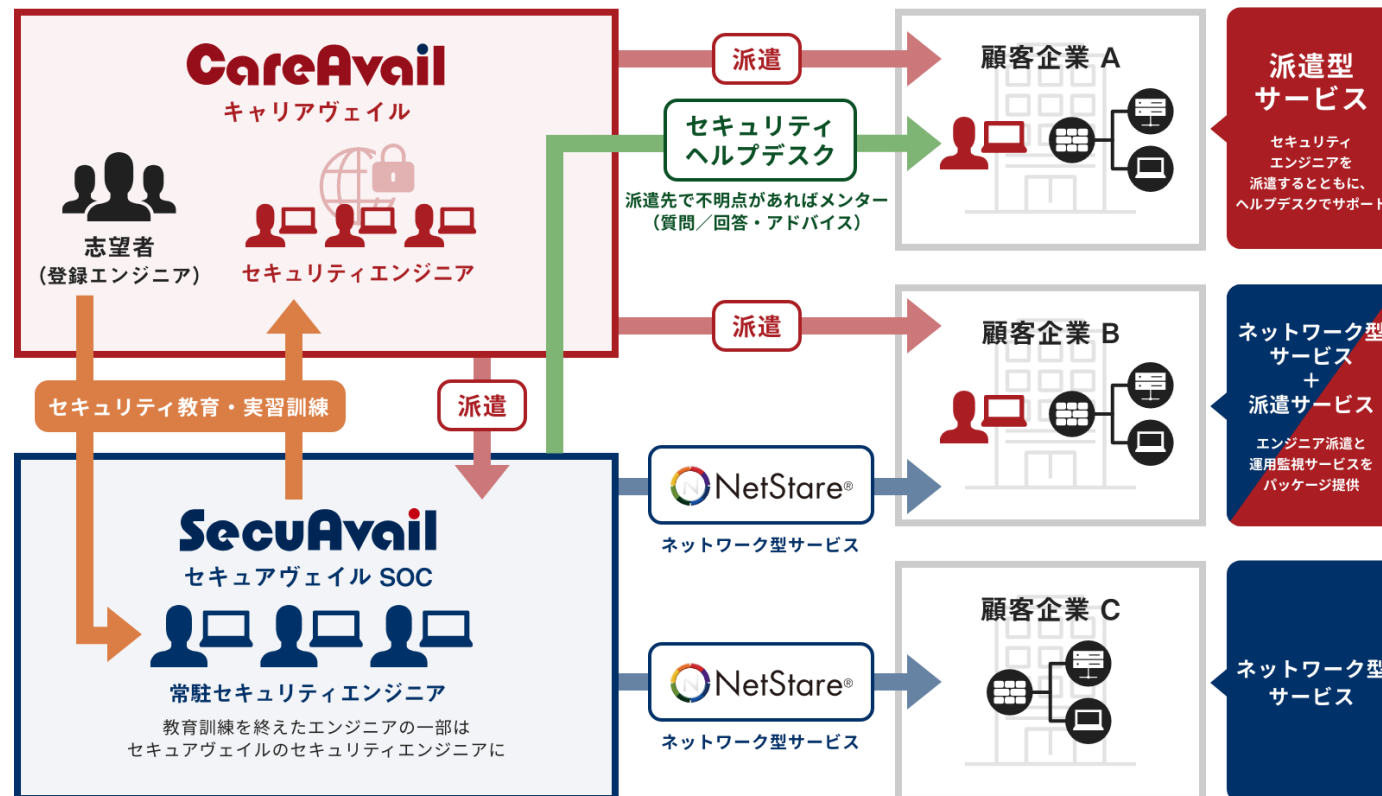
従来のセキュリティ運用ソフトは、システム監視とログ管理に分かれ、さらにレポート作成や将来予測のための分析ツールも別途必要となり、すべてを導入し適切に運用することは、お客様の大きな負担となっていました。「LogStare」は、セキュアヴェイルのSOCが実際に実務で使うレポートテンプレートが標準搭載されており、導入直後からすぐに使用できます。導入障壁・導入コストを最低限に抑え、多機能を1つのソフトウェアで実現し、かつクラウドで提供できることが、他社にはない強みです。

# 人材サービス事業



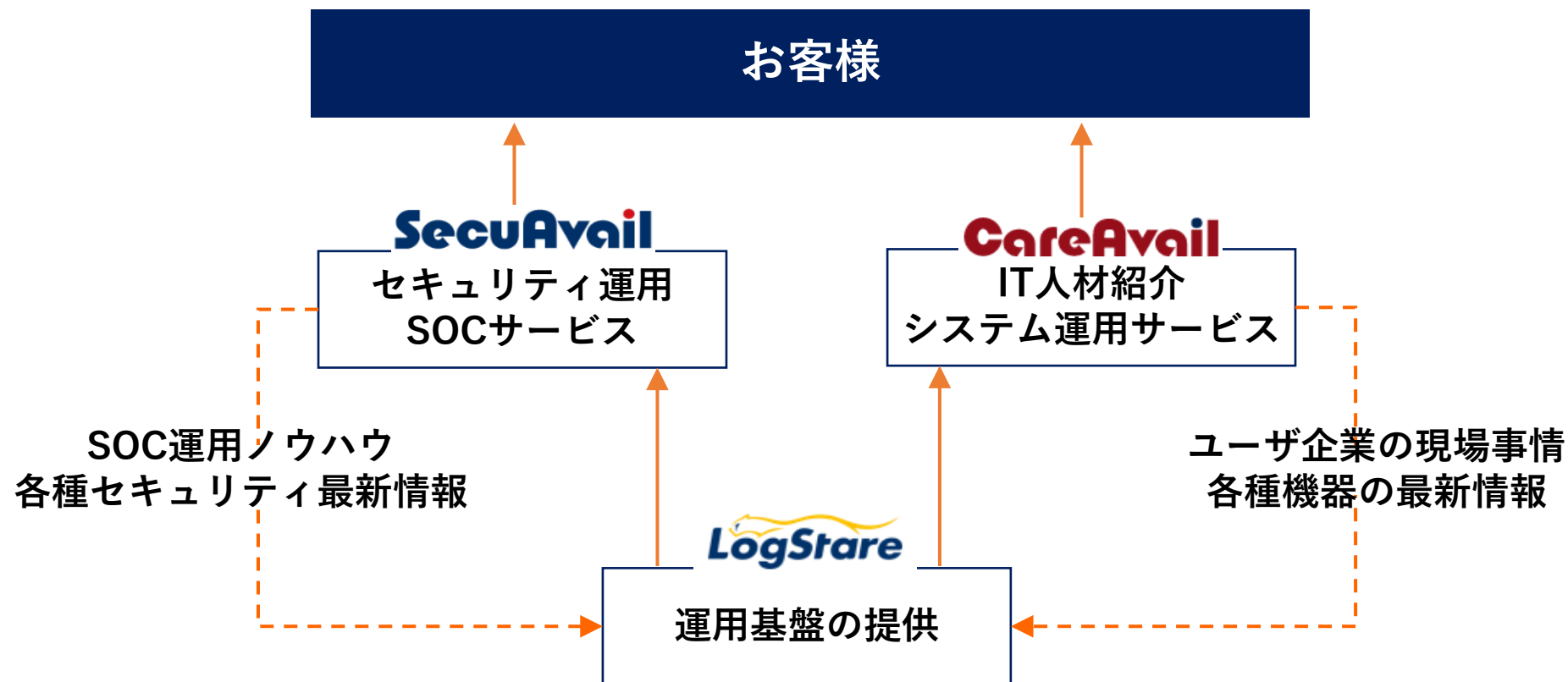
人材サービス事業は、連結子会社「株式会社キャリアヴェイル」を通じて、お客様への情報セキュリティエンジニア派遣を主としております。

効果的な情報セキュリティ対策を行うには、専門知識を有するプロフェッショナルの助力が必要であることから、情報セキュリティエンジニアを育成し、派遣することで、ネットワーク化の進行する社会の要請に応えるべく、情報セキュリティエンジニア不足に悩むお客様のニーズの獲得に取り組んでおります。



また、単に情報セキュリティエンジニアを派遣するだけでなく、上図のように情報セキュリティ事業の既存のお客様へ従来の運用監視サービスに、情報セキュリティエンジニア派遣サービスを合わせたハイブリッド型のビジネスモデルをご提案できることも他社にはない強みであると認識しております。

## セキュリティ運用に欠かせない現場の動向・情報が 常に最新に保たれる**垂直統合型ビジネス**





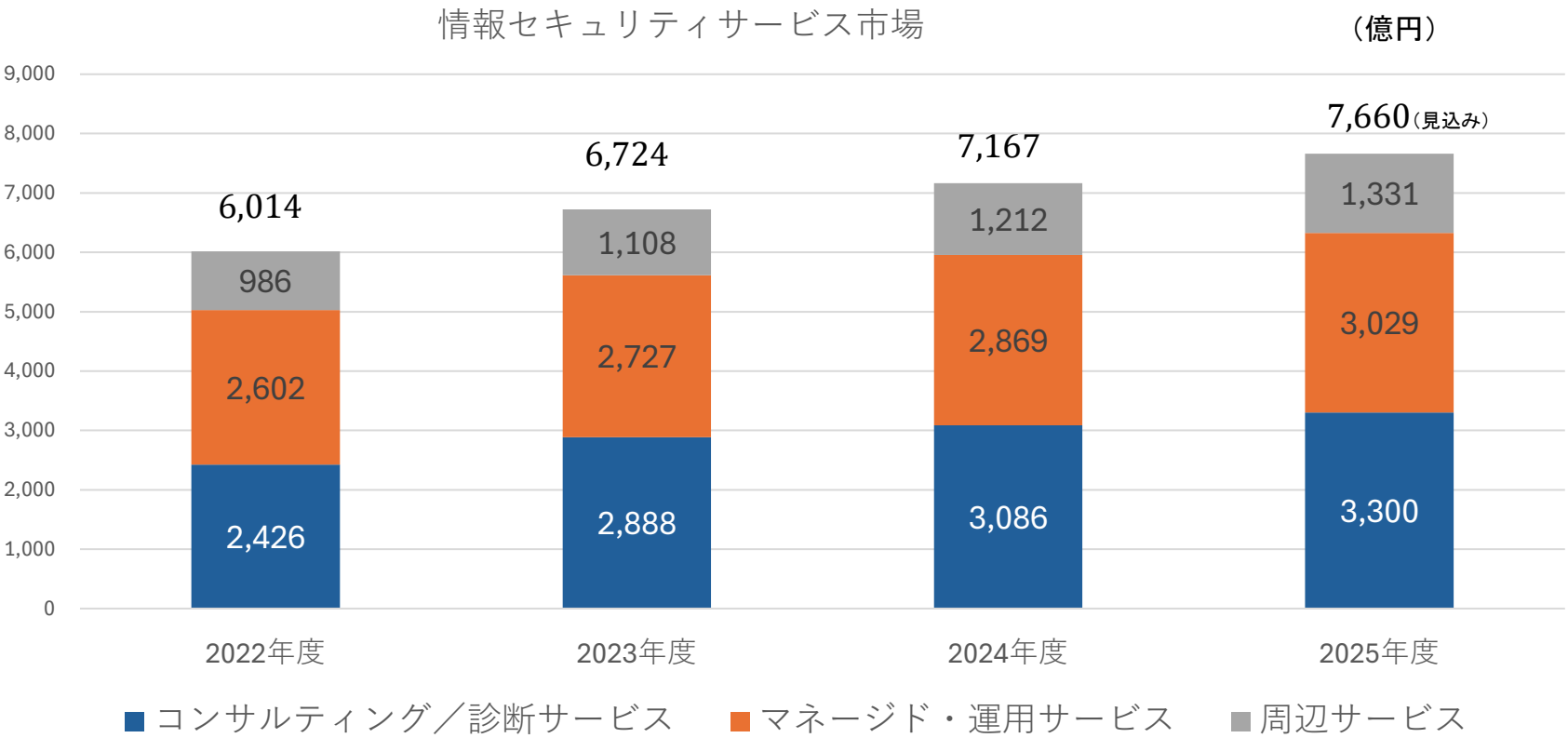
## II. 中間期決算状況

# 主たる事業の市場環境



情報セキュリティ市場の環境では、システムの脆弱性を突いたサイバー攻撃が後を絶たず、国内外の様々な企業で被害が発生しており、社会経済に与える影響は深刻化しています。

セキュリティインシデントや情報漏洩は年々増加傾向にあり、情報セキュリティ対策やログ管理の重要性が益々高まっております。



出所：JNSA調査研究部会「国内情報セキュリティ市場 2024年度調査報告」

# 連結決算損益書



(単位：百万円)

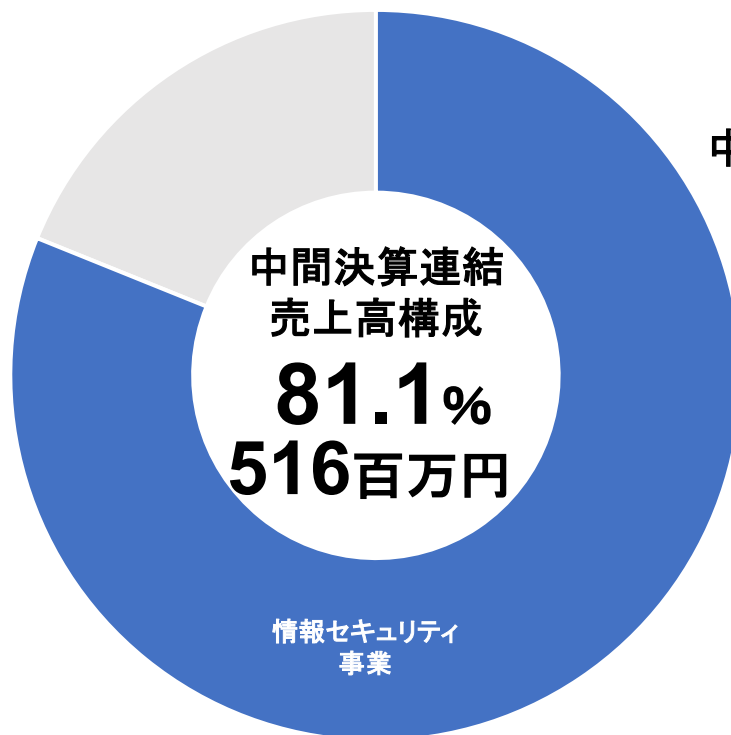
	2025年3月期 中間期実績	2026年3月期 中間期実績	対前期		2026年3月期		備考
			増減額	増減率	通期予想	予算に対する 実績進捗率	
売上高	465	636	171	36.9%	1320	48.3%	
売上原価	305	349	43	14.3%	736	47.5%	
売上総利益	159	287	127	80.1%	583	49.3%	
売上総益率	34.3%	45.1%	10.8%	-	44.2%	-	
販売費及び 一般管理費	211	239	28	13.2%	473	50.6%	
営業利益	△ 52	47	99	-	109	43.4%	
営業利益率	△11.2%	7.4%	18.7%	-	8.3%	-	
経常利益	△ 51	48	100	-	109	44.5%	
経常利益率	△11.1%	7.6%	18.7%	-	8.3%	-	
親会社株主に帰属する 当期純利益	△ 53	48	102	-	75	64.1%	
当期純利益率	△11.6%	7.6%	19.2%	-	5.7%	-	

# セグメント別実績



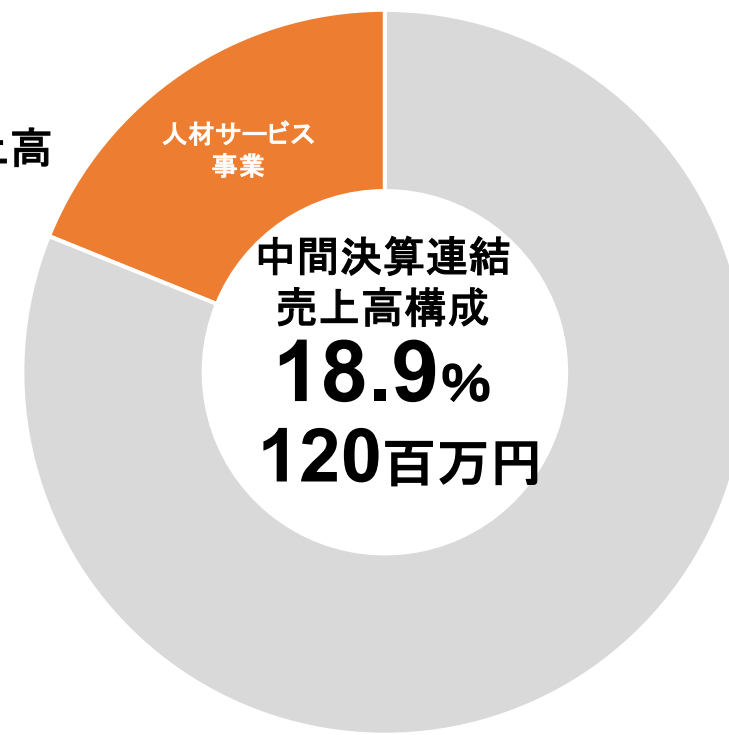
当社グループは、ネットワーク・セキュリティ運用・監視サービス及び各種セキュリティ運用基盤の開発・販売を主とする「**情報セキュリティ事業**」、情報セキュリティエンジニアを育成し派遣する「**人材サービス事業**」を展開しております。

情報セキュリティ事業



**事業内容** ITセキュリティの運用監視サービス（NetStareシリーズ他）、運用監視基盤（ソフトウェア LogStare）の開発及び販売、その他関連機器の販売及びサービス

人材サービス事業



**事業内容** セキュリティエンジニアの育成及び人材派遣サービス

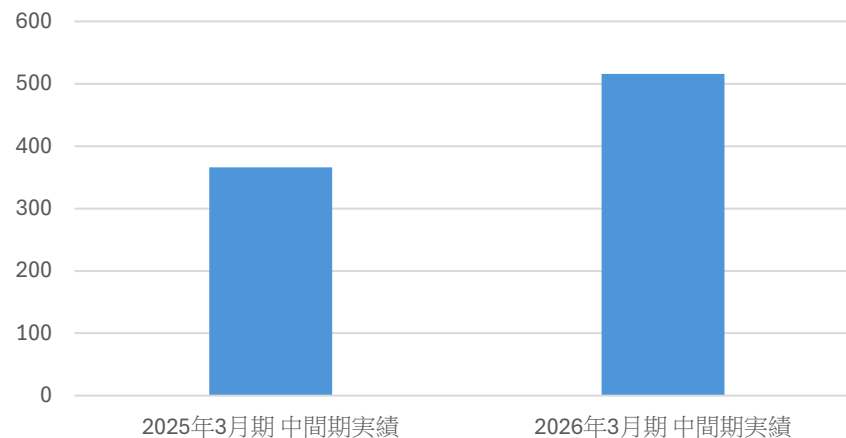
2026年3月期  
中間決算連結売上高  
**636百万円**



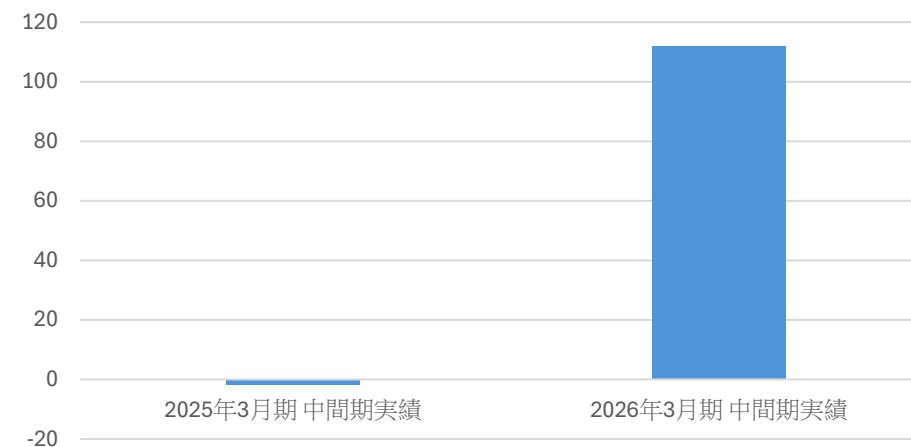
# セグメント別実績



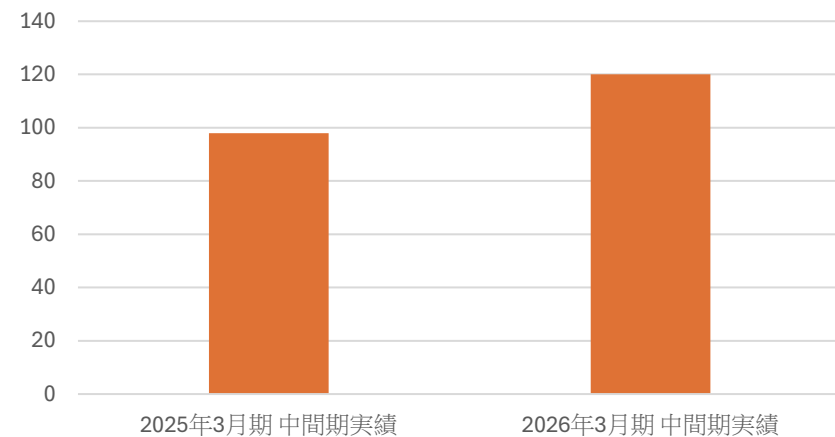
情報セキュリティ事業セグメント売上高



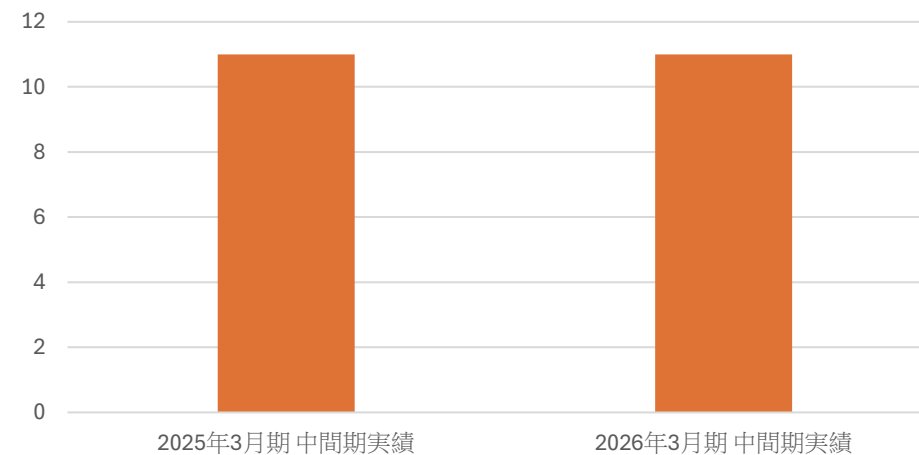
情報セキュリティ事業セグメント利益



人材サービス事業セグメント売上高



人材サービス事業セグメント利益





### III. 中期業績目標

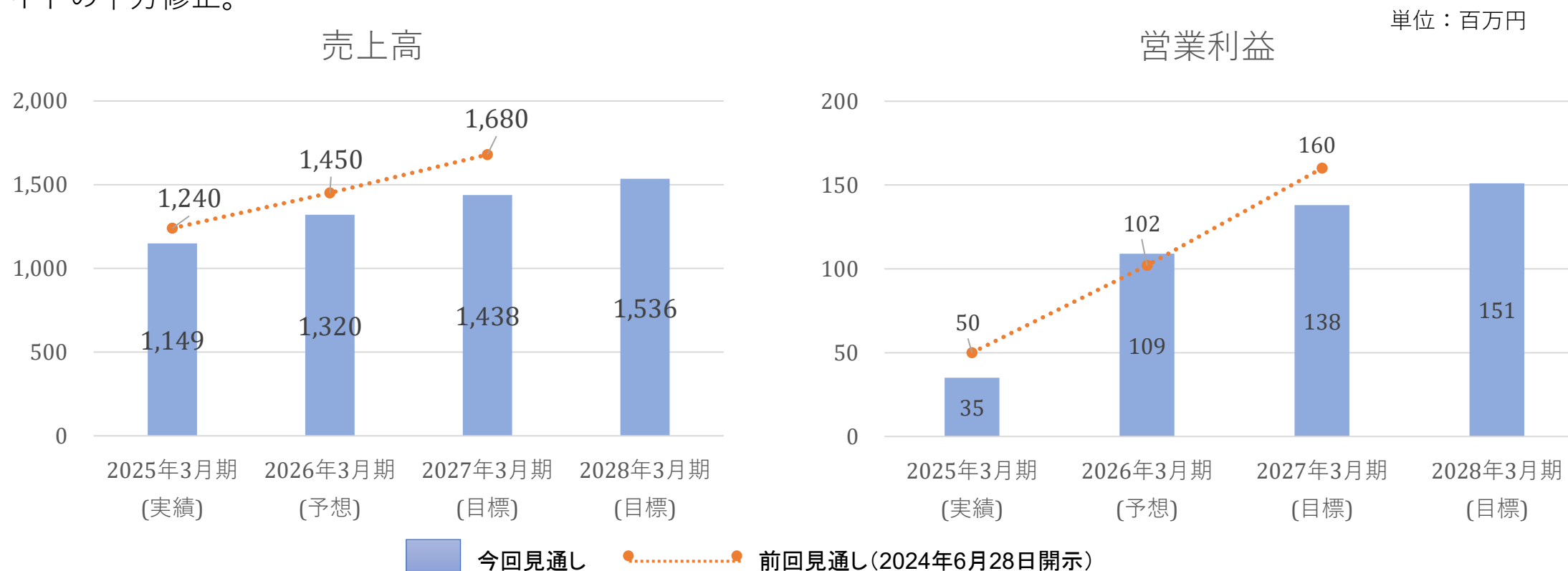
# 中期業績目標



業績予想につきましては、2026年3月期から2028年3月期にかけて、売上規模を16%アップさせるとともに、収益改善を図り、2027年3月期は売上高1,438百万円、営業利益138百万円、経常利益138百万円、また、2028年3月期は売上高1,536百万円、営業利益151百万円、経常利益151百万円を目標としています。

## 【前回資料（2024年6月28日開示）からの更新事項】

商談及び導入遅延により、2025年3月期予想1,240百万円が実績1,149百万円の下振れしたことを踏まえ、売上計画を1年スライドの下方修正。

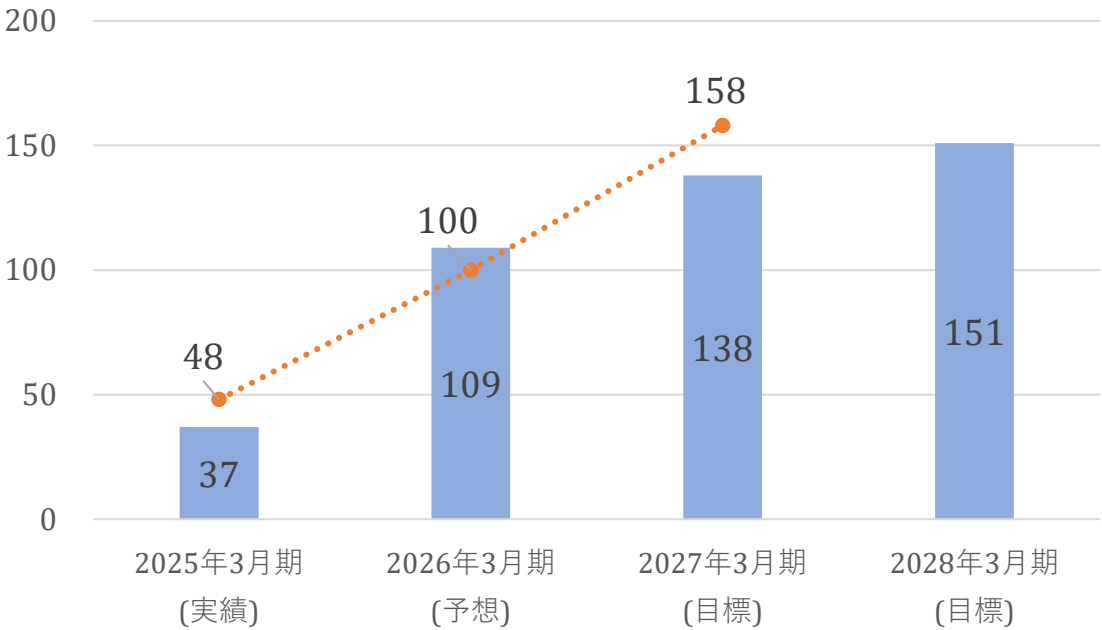


# 中期業績目標

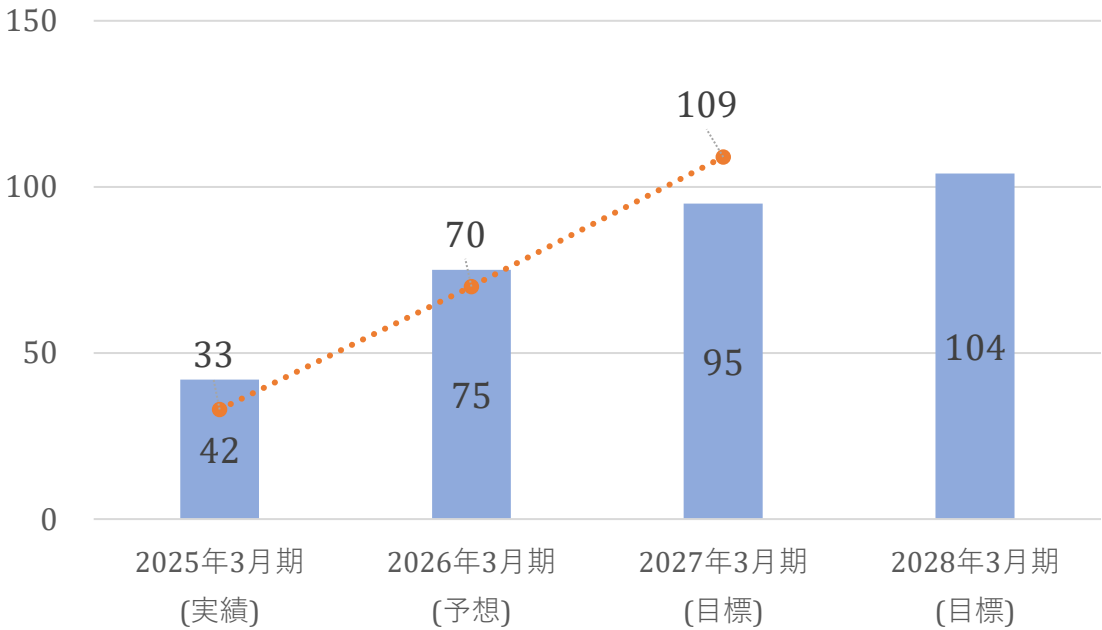


単位：百万円

経常利益



当期純利益



今回見通し      前回見通し(2024年6月28日開示)

注：上記は、営業外損益、特別損益は見込んでいません。



## IV. 企業価値向上に向けて

資本収益性 2026年3月期第2四半期ROE4.0%であり低い状況である

(1) 現状分析

- 2024年3月期は投資有価証券売却益により一時的利益がでましたが、過去数年間は利益予算を未達成な状況が続いてきました。
- ROE8%達成するには、当期純利益1億円超(予算見込み)を達成しなければならない状況です
- 予算に対する各事業本部における責任の明確化、月次ベースでの具体策の計画と実行、評価、改善のPDCA進捗管理が不十分な状況です。

(2) ROE改善への取組み

- 収益力強化
  - 各サービスや商品の利益率を再度見直し、高収益事業体質へ変換する
- コスト構造改革
  - 原価構造を見直し及び固定費などの削減を継続的に実施する

ROEの推移



## 資本収益性2026年3月期第2四半期は、PBRは2.09倍ながら、同業他社に比べ低い状況である

### (1) 現状分析

- 2026年3月期第2四半期の自己資本比率は **78.0%**で、キャッシュリッチの状況ですが、資本に対する収益が同業他社に比べ低い状況であります
- 自己資本比率の高さ、キャッシュリッチ、ストックビジネスで安定した経営であることが十分にアピールできていません
- 安定性は評価されているが、成長性や将来性が株式市場に浸透しておらず、市場からの正当な評価(株価)につながっていません

### (2) PBR改善への取組み

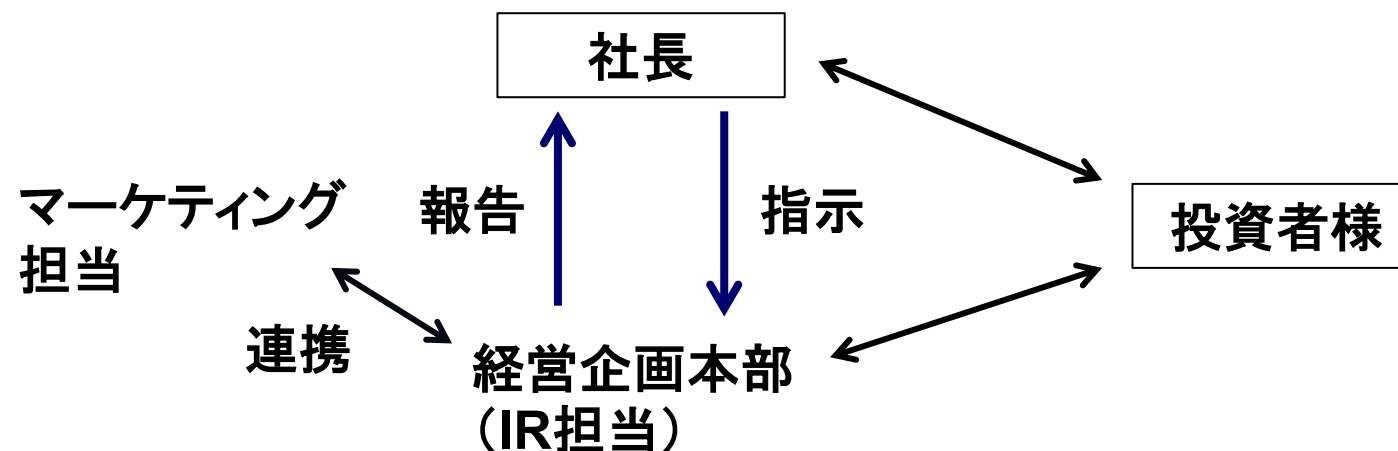
- IR・広報の強化
  - 財務の健全性だけでなく、その安定基盤を活かしてどのような成長戦略を描いているかを明確に示していきます
  - 継続的な収益基盤(解約率、LTVなど)を具体的な数値で示し、安定した将来キャッシュフローをアピールしていきます
- 中期経営計画の策定・公表
  - 明確な数値目標(ROE、売上高、利益率など)と戦略を盛り込んだ中期計画を策定し、株式市場との対話を深めてまいります



投資者様とのコミュニケーション向上に向けた情報開示、IR体制の整備に努めております。

現在の取組み

1. 決算説明会の実施(11/26 個人投資家向けのIRセミナー)
2. 英文開示
3. 資本コストや株価を意識した経営
4. 積極的なPR・IR活動、ラジオ番組出演予定(来年2月)、法人投資家への個別決算説明検討他
5. IR体制の整備



# 事業の取組み状況



パートナーとの提携を推し進め、ITセキュリティサービスに強みを持つ株式会社ブロードバンドセキュリティや医療DX事業を中心にサービス提供する株式会社メディカル・オーシャンと戦略的な業務提携を締結、医療分野や自治体・公共における新たな販路の開拓を図りました。結果として、新規パートナー開拓 年間9社獲得しました。

主力のセキュリティ運用監視サービス（SOCサービス）においては、医療機関向けサイバーセキュリティ対策サービス「NetStare for Medical」や自動車産業サプライチェーン向けサービス「NetStare for OT/IoT」の認知拡大・拡販に注力、また子会社LogStare（ログステア）では、BoxやGoogle Workspaceのログ分析などクラウド環境に対応した各種セキュリティ製品開発や運用基盤の強化を図りました。

新規顧客	<ul style="list-style-type: none"><li>✓ 新規パートナーとの戦略的提携（新たな業界で販売網の拡大）</li><li>✓ 地方自治体、公共、医療等セグメント向けストック型サービスの提供</li></ul>	<ul style="list-style-type: none"><li>✓ 新規サービスの企画・開発</li><li>✓ クラウド環境に対応したセキュリティ製品の開発</li><li>✓ 自社開発ソフトウェアのラインアップを拡充</li></ul>
既存顧客	<ul style="list-style-type: none"><li>✓ ストック型サービスの契約更新、アップセル</li></ul>	<ul style="list-style-type: none"><li>✓ グループ会社の持つサービスのクロスセル</li></ul>
	既存製品・サービス	新製品・サービス

従来から強みとしているストック型サービスであるセキュリティ運用監視サービス（SOCサービス）の新規契約獲得、契約更新を軸に、安定した収益基盤の確立に引き続き、取り組みました。

既存顧客との契約継続、更にはアップセル、クロスセルの取引拡大に向けて、顧客フォローに技術スキルを保有する担当者を加えるなどの体制で差別化を図っております。



## V.重点施策

## 4つのコア戦略

当社の成長実現のため以下の4点をコア戦略としております。

1  
戦略

「基幹商品の**サービスレベル向上**」

既存顧客の満足度を向上し契約の継続を図ってまいります。

2  
戦略

「既存顧客へ**営業リソースを集中**」

顧客単価向上のためにシステム更改の獲得と提供サービスの範囲を拡張してまいります。

3  
戦略

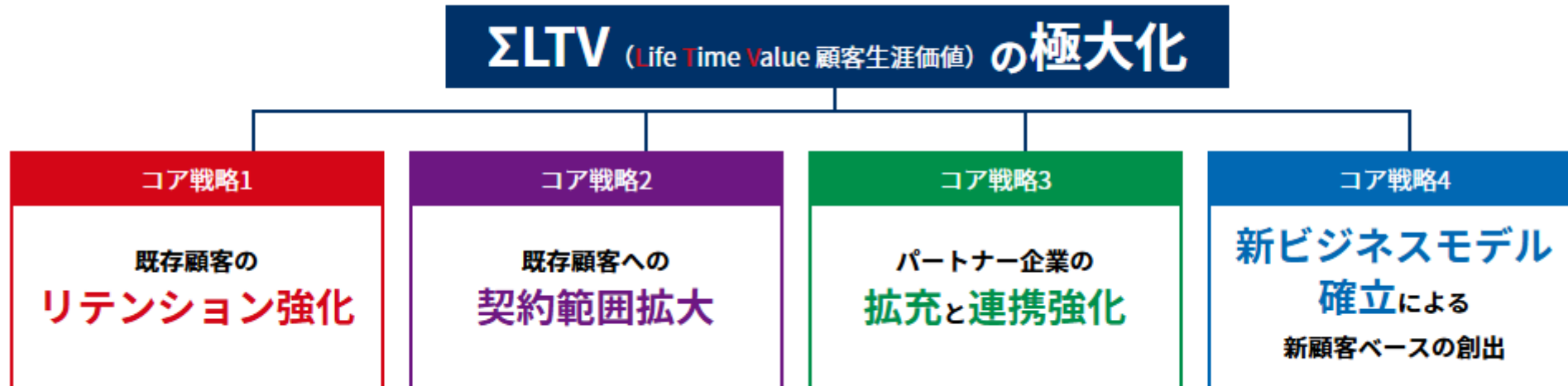
「パートナー企業の**拡充と連携強化**」

新規顧客の効率的獲得のため既存パートナーの販促支援・営業支援を積極的に実施してまいります。

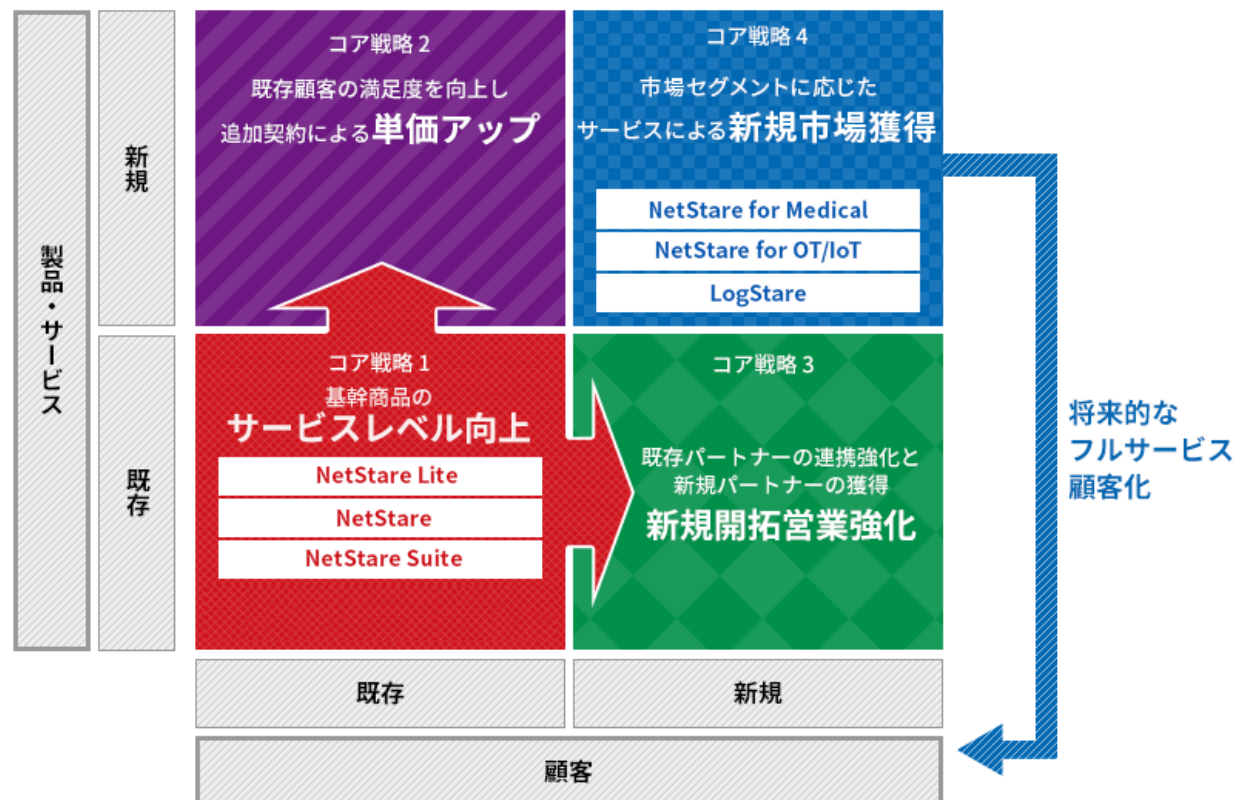
4  
戦略

「**新ビジネスモデル確立**による新たな顧客ベースの創出」

新規顧客・新規パートナー獲得のためグループ各社と連携し顧客ニーズに応える提案を進めてまいります。

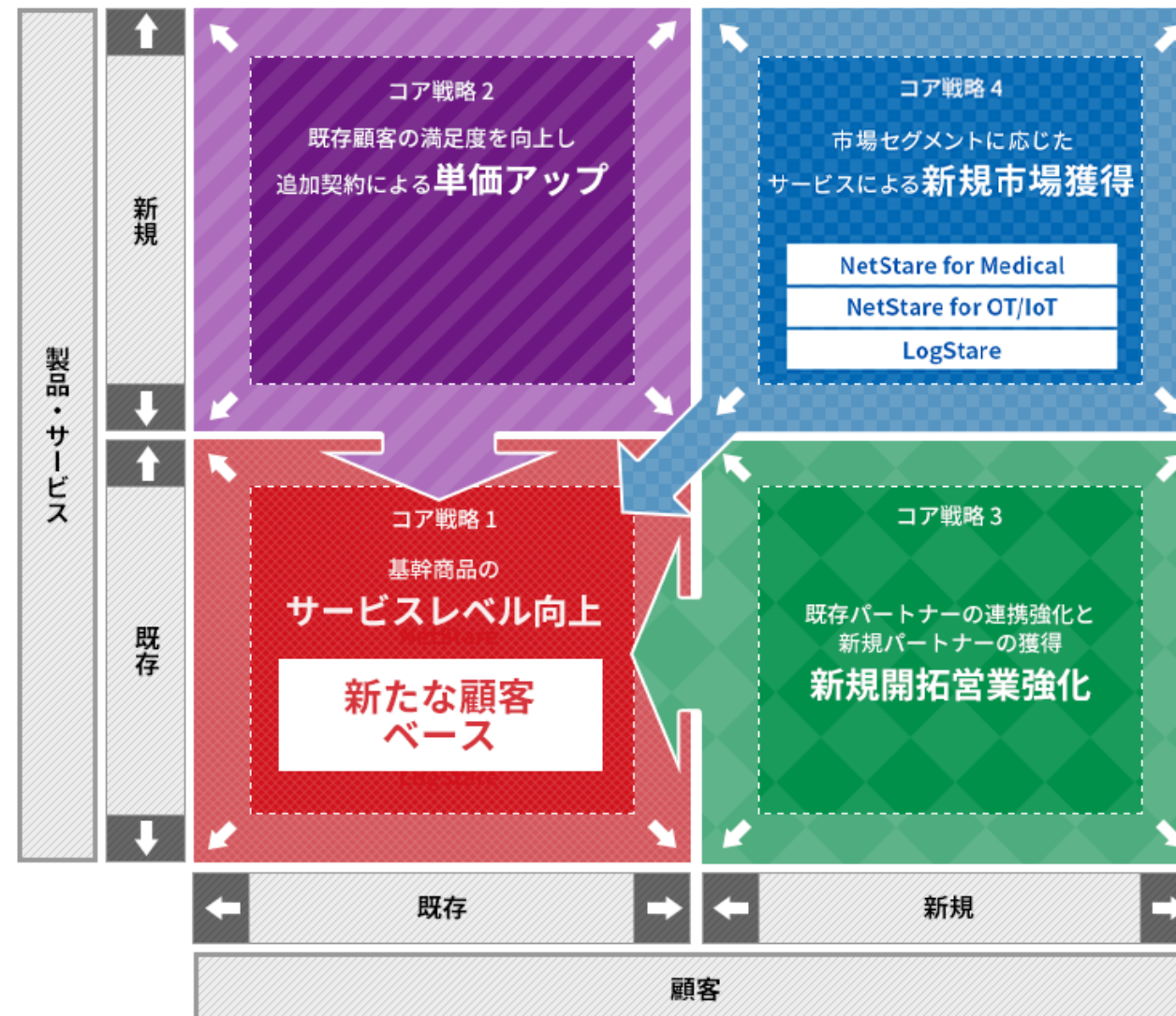


## コア戦略の流れ



成長戦略の実現による顧客基盤の拡大

# 成長に向けた重点施策



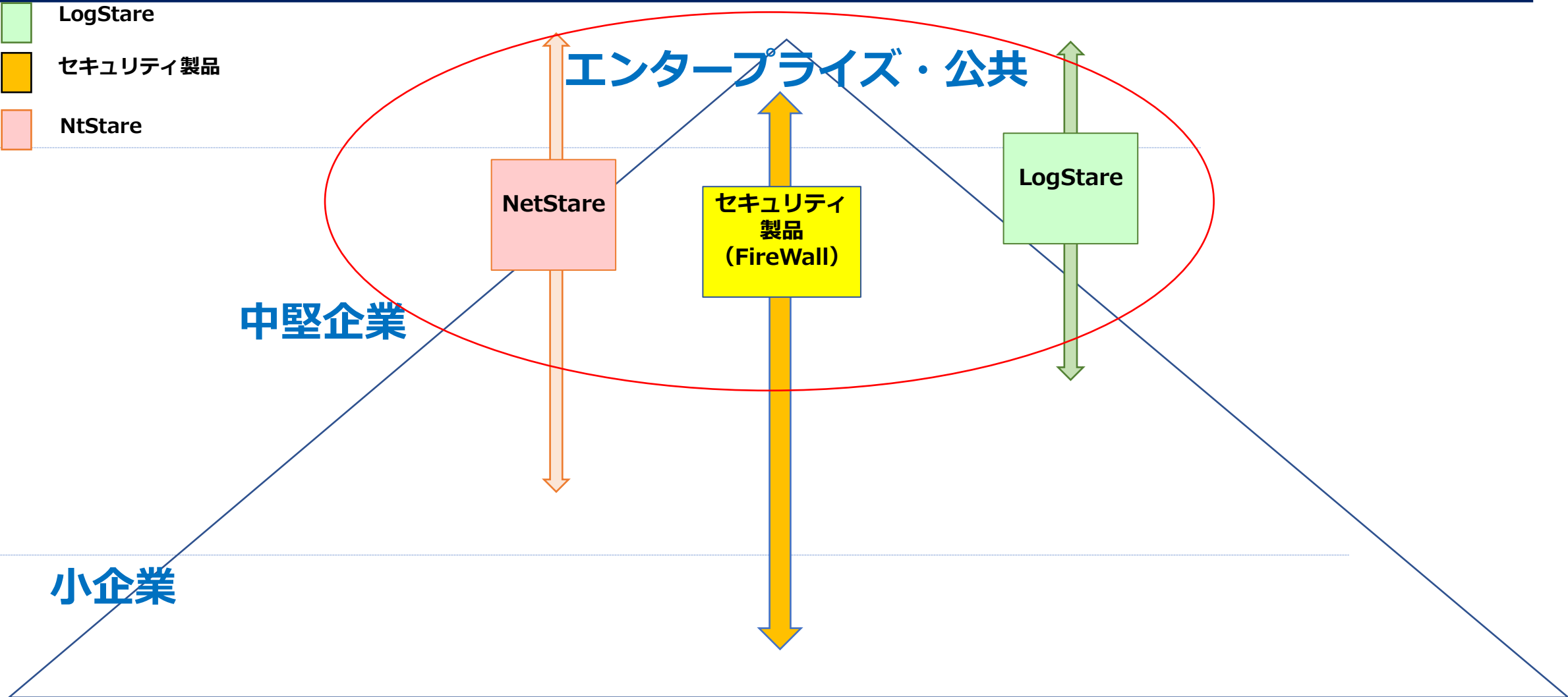




## VI.製品戦略

# 創業期ターゲット（2001～2010頃）

SecuAvail



# ターゲット (2010~2020)

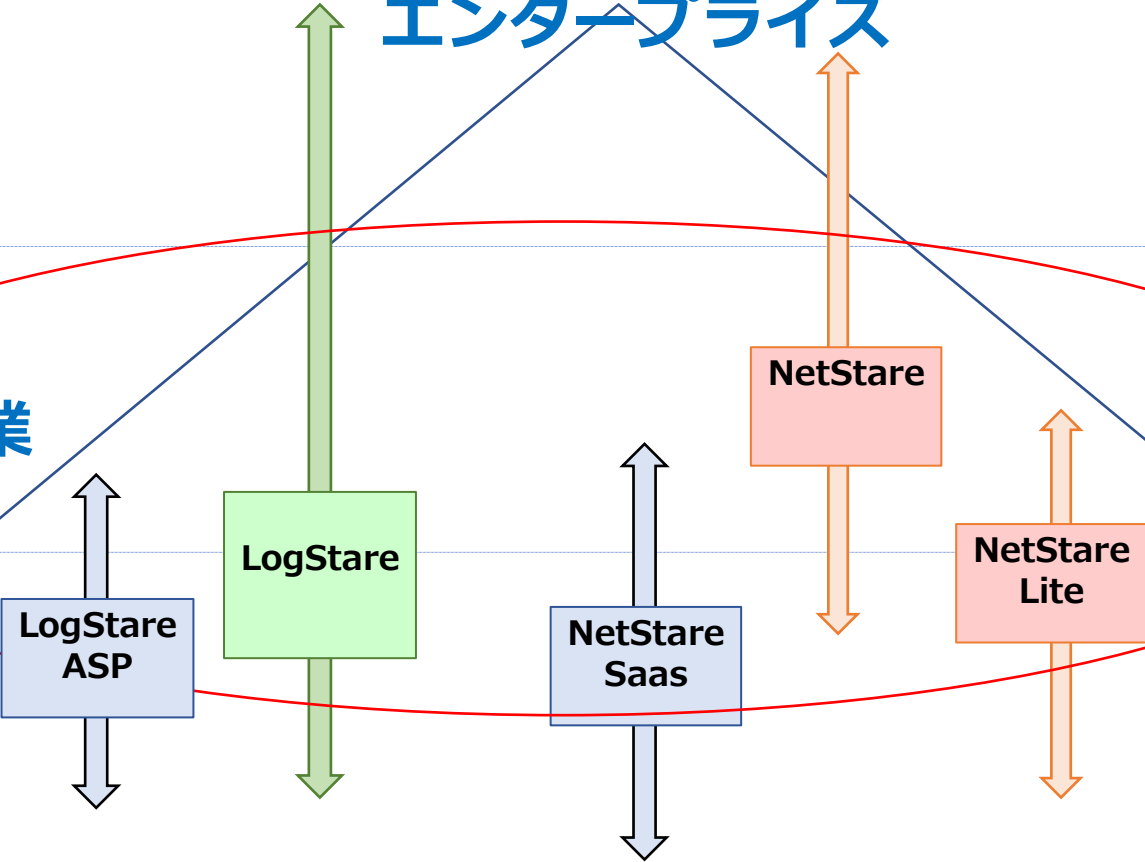
SecuAvail

- ソフトウェア製品
- クラウドサービス
- NetStare

エンタープライズ

中堅企業

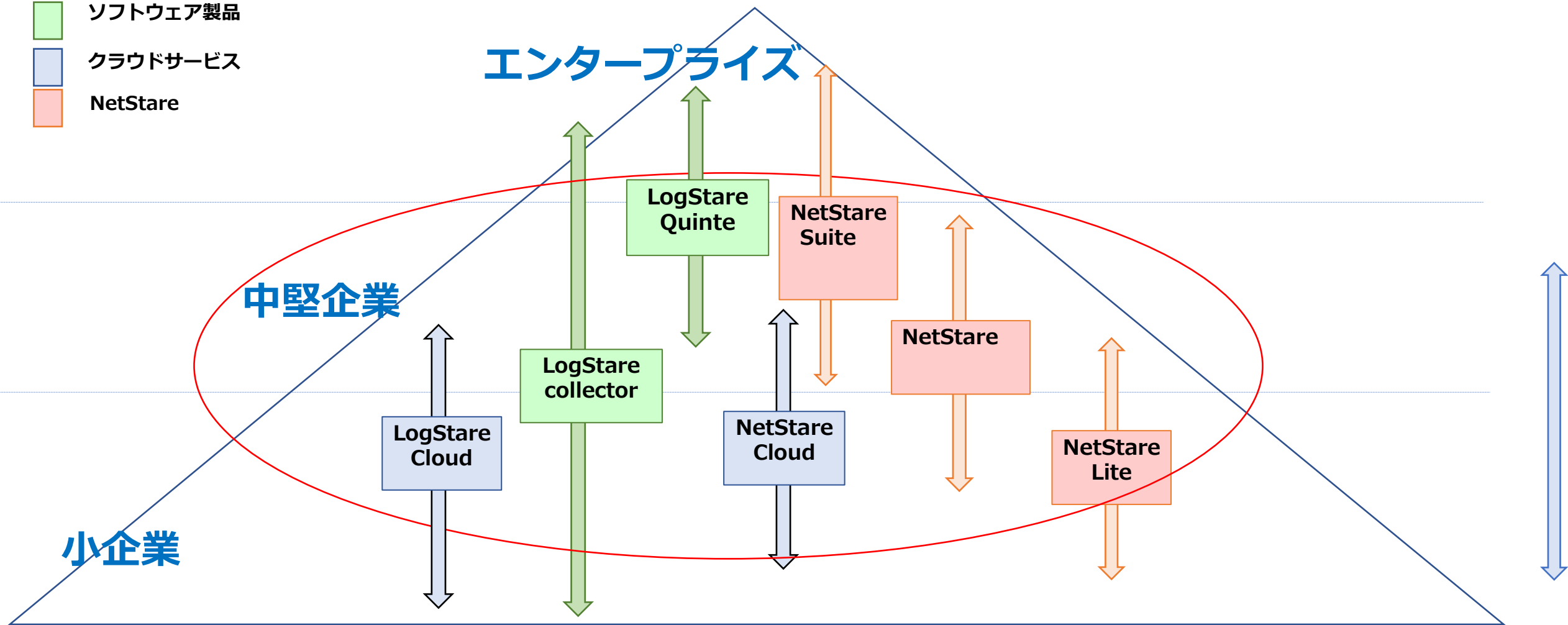
小企業



# ターゲット (2021~2020)

SecuAvail

- ソフトウェア製品
- クラウドサービス
- NetStare



1. 次世代ファイアウォール監視運用支援サービス

NetStare Suite

NetStare

NetStare Lite

NetStare Cloud

2. ランサムウェア攻撃検知サービス  
(Windowsサーバログ監視)

NetStare RW

NetStare RW appliance

3. エンドポイントセキュリティサービス

NetStare EDR : Aurora (旧Cylance) Managed Service  
: With Secure Managed Service

4. ネットワークセキュリティサービス

NetStare NDR : FortiNDR Managed Service

NetStare IDS : 不正侵入検知監視サービス

5. VPN接続監視と脆弱性管理サービス

NetStare Remote

6. Web Application FireWall 運用支援サービス

NetStare WAF : F5 BIG-IP ASM Managed Service

LogStare Collector  
ログステア コレクター



LogStare Reporter  
ログステア レポーター



LogStare Quint  
ログステア クイント



LogStare M365  
ログステア エムサンログ



業種・業界向けサイバーセキュリティソリューション

1. 病院向けサイバーセキュリティ対策 NetStare for Medical

2. 製造業向けサイバーセキュリティ対策 NetStare for OT/IoT

3. 中小企業向けランサムウェア攻撃検知アプライアンス NetStare RW appliance



セキュリティ診断サービス

1. FW診断

2. プラットフォーム診断 / Webアプリケーション診断



- ✓ **令和4年度診療報酬改定において、400病床以上の保険医療機関について「安全管理ガイドライン」に基づき、診療録管理体制加算の要件に、非常時に備えたサイバーセキュリティ対策の整備に係る要件が追加**
- ✓ **令和5年3月に医療法施行規則第14条の一部を改正し、医療機関（病院、診療所、助産所）に対し、医療情報システムのサイバーセキュリティを確保するための必要な措置を講じることが追加（同年4月に施行）**
- ✓ **令和5年6月に厚生労働省は、医療機関等が患者の電子カルテなどの医療情報を適切に管理するための必要な措置として「医療情報システムの安全管理に関するガイドライン第6版」（以下「安全管理ガイドライン」という。）を公表**
- ✓ **令和5年6月医療法第25条第1項の規定に基づく、立入検査要綱の項目に、サイバーセキュリティ確保のための取組状況をチェックする項目が追加（サイバーセキュリティ対策チェックリスト）**

医療機関の管理者が遵守すべき事項への位置づけ

第16回 健康・医療・介護情報利活用検討会医療等情報利活用ワーキンググループ（令和5年3月23日）資料2-2改

健康・医療・介護情報利活用検討会医療等情報利活用ワーキンググループでの議論を踏まえ、下記のとおり、サイバーセキュリティの確保を医療機関の管理者が遵守すべき事項に位置づけた。

改正概要・対応の方向性

- 医療法施行規則第14条第2項を新設し、病院、診療所又は助産所の管理者が遵守すべき事項として、サイバーセキュリティの確保について必要な措置を講じることが追加する。
- 令和5年3月10日公布、4月1日施行
- 「必要な措置」としては、最新の「医療情報システムの安全管理に関するガイドライン」（以下「安全管理ガイドライン」という。）を参照の上、サイバー攻撃に対する対策を含めセキュリティ対策全般について適切な対応を行うこととする。
- 安全管理ガイドラインに記載されている内容のうち、優先的に取り組むべき事項については、厚生労働省においてチェックリストを作成し、各医療機関で確認できる仕組みとする。
- また、医療法第25条第1項に規定に基づく立入検査要綱の項目に、サイバーセキュリティ確保のための取組状況を位置づける。

○医療法施行規則（昭和二十三年厚生省令第五十号）

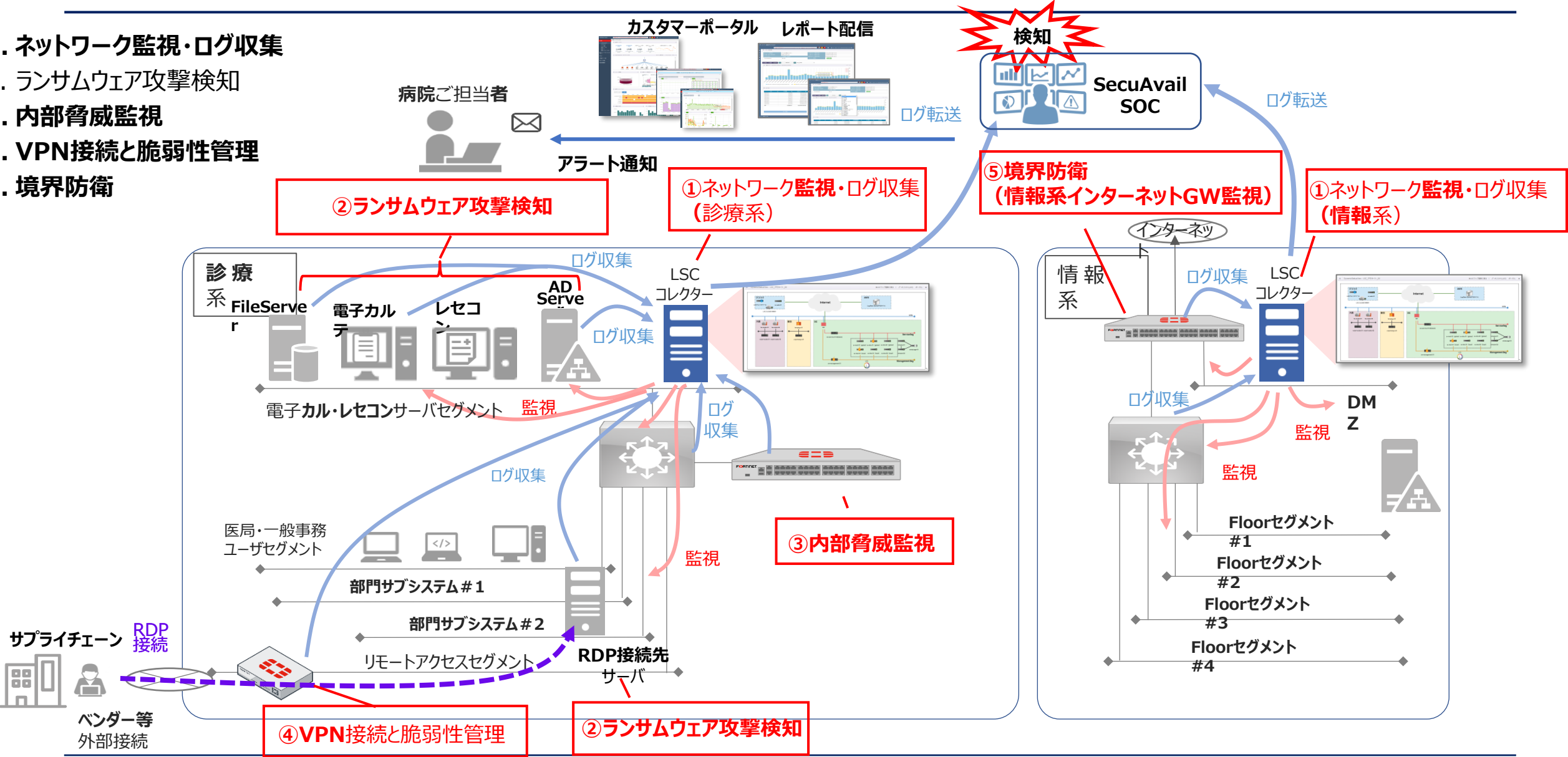
第十四条（略）

2 病院、診療所又は助産所の管理者は、医療の提供に著しい支障を及ぼすおそれがないように、サイバーセキュリティ（サイバーセキュリティ基本法（平成二十六年法律第百四号）第二条に規定するサイバーセキュリティをいう。）を確保するために必要な措置を講じなければならない。

※ 下線部を新設。

NetStare for Medical < 5つの対策 >

- 1. ネットワーク監視・ログ収集
- 2. ランサムウェア攻撃検知
- 3. 内部脅威監視
- 4. VPN接続と脆弱性管理
- 5. 境界防衛







## ガイドラインの構成（3-ステップ2 セキュリティ対策の立案①）

ステップ 2

- ステップ1で収集・整理した情報に基づき、工場システムのセキュリティ対策方針を策定する。

ステップ2-1	セキュリティ対策方針の策定【3.2.1】	ステップ1で整理したゾーンとこれに紐づく業務、保護対象、想定脅威に対して、業界や個社の置かれた環境に応じ、重要度・優先度を設定する。
ステップ2-2	想定脅威に対するセキュリティ対策の対応づけ【3.2.2】	どのようなセキュリティ対策が対応づけられるのか整理する。脅威に対応するためには物理面、システム構成面どちらか一方でなく双方の対策が重要となるため、参照されたい。

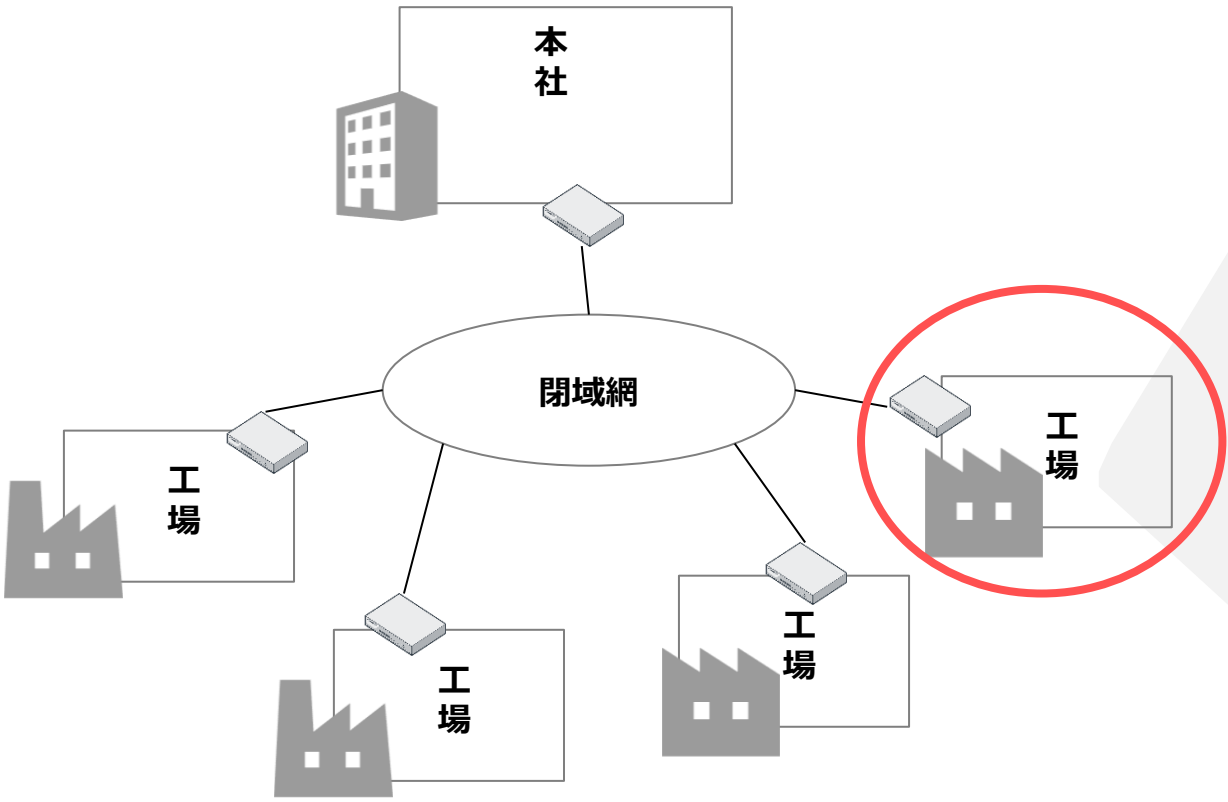
### （1）システム構成面での対策

#### ① ネットワークにおけるセキュリティ対策（例）

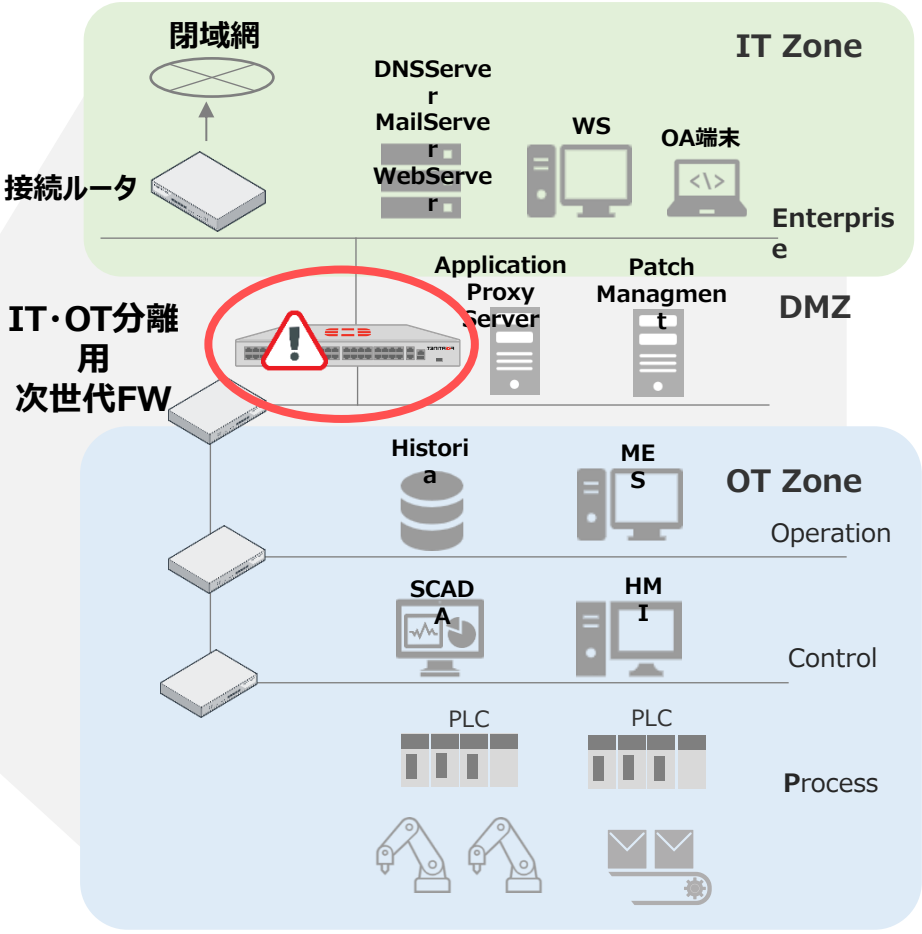
対策項目	セキュリティ強度ごとの対策		
	最低限	中	高
構成分割	－	VLAN等による論理ドメイン細分	物理ドメイン分割
接続機器制限	－	IP、MAC制限	+ 接続機器の論理証明 + 接続機器の信頼性確保
内部秘匿	－	NAT、ステルス	不正通信防止（ゲートウェイ）
通信データ制限	送信元／宛先制限（FW）	+ 通信電文種別制限、 + 電文内容解析・異常検知（IDS）	+ 電文内容解析・ 異常通信遮断（IPS）
利用者制限	不要ユーザ削除、パスワードポリシー策定	+ 個人ID認証（1要素認証）	+ 多要素認証
通信監視・制御	－	通信状況可視化・監視（NDR）、 異常検知（IDS）	+ 異常通信遮断 （IPS、フィルタリング）
構成管理	－	接続機器管理・可視化	+ 機器内の構成管理・可視化
脆弱性対策	脆弱性情報収集	+ 脆弱性診断、侵入可否検査 + 回避策	+ ソフトウェア更新 （セキュリティパッチ適用） [or 仮想的な対策（IPS、仮想パッチ等）]
ログ取得	機器内ログ取得 （処理負荷への影響を考慮）	+ IDSログ連携	+ ログ分析の仕組み整備

※ 表は例示であり、内容について個社や業界に応じて精査が必要な場合がある。

サービス対象拠点と構成イメージ



IT・OT分離による不正侵入防御構成イメージ





## By LogStare

### （1）クラウド対応



クラウドファースト、クラウドネイティブと言った考え方が普及するにつれBoxやMicrosoft 365、グーグル、AWSのパブリッククラウドサービスの企業導入が進み、利便性が増す一方、マルチクラウド化による管理ツールのサイロ化、運用業務の煩雑化が避けて通れない課題となっています。LogStareは各種クラウドサービスのセキュリティを向上させるログ分析機能を開発し、企業のIT運用担当者のセキュリティ運用業務を支援します。各クラウドサービスの利用者のセキュリティ対策に好評です。さらに24時間365日監視のNetStareサービスを組み合わせれば、かなりのリスク抑制に有効と考えます。

### （2）生成AI



「LogStare」に生成AIを活用したログ分析機能を搭載  
従来LogStareが得意としているログの収集・正規化・レポート作成の自動化に加え、新たに生成AIによるログレポートのインサイトを提供することで、SOC (Security Operation Center) の業務効率と成果を最大化。企業の意思決定を強力にサポートします。





# 製品戦略 (NetStare 24時間365日 セキュリティサービス)

**SecuAvail**

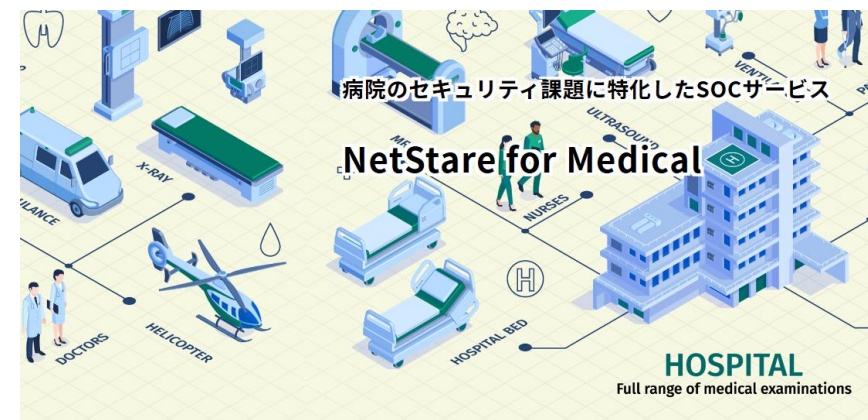


アウトソーシングサービス  
アウトソーシングサービス

By **SecuAvail**

## (1)「NetStare for Medical」

病院などの医療機関のサイバーセキュリティ対策に特化したセキュリティ運用(SOC)サービスです。  
近年被害が深刻化しているサプライチェーン攻撃やランサムウェア攻撃への対策など、病院が直面している課題や、病院規模・予算に応じて5つのサービスから必要な対策を選択いただけます。



ネットワーク監視  
/ログ収集



ランサムウェア  
検知



内部脅威監視



VPN接続と  
脆弱性管理



境界防御



# 製品戦略 (NetStare 24時間365日 セキュリティサービス)

自動車産業のサプライチェーンを守るSOCサービス

NetStare for OT/IoT

**SecuAvail**

## (2)「NetStare for OT/IoT」

近年、自動車産業におけるサイバー攻撃による被害が深刻化しており、「NetStare for OT/IoT」は自動車産業サプライチェーンを守るためのセキュリティ運用(SOC)サービスです。

自工会/部工会  
サイバーセキュリティ  
ガイドライン対応

### 7つのサイバーセキュリティ対策ラインナップ



## (3)「ランサムウェア攻撃検知アプライアンス」

Active DirectoryやファイルサーバーなどWindowsサーバーの監査ログを監視し、独自の検知ロジックでランサムウェアの侵入・潜伏を検知、被害の拡大を防ぎます。

エージェントレスなので、既存環境への閉胸が極小、専用サーバーやOS調達の手間もなくスピード導入可能、置くだけでランサムウェア攻撃対策が実現する小型アプライアンスです。



### 導入例

ランサムウェア攻撃検知アプライアンスは、標的型メールなどから容易に組織内に侵入し徐々に被害を広げるランサムウェアの行動を、独自のロジックでログから探し出します。

お客様環境には小型アプライアンスを設置するだけ。エージェントレスでログ収集できるので既存環境に影響を与えません。

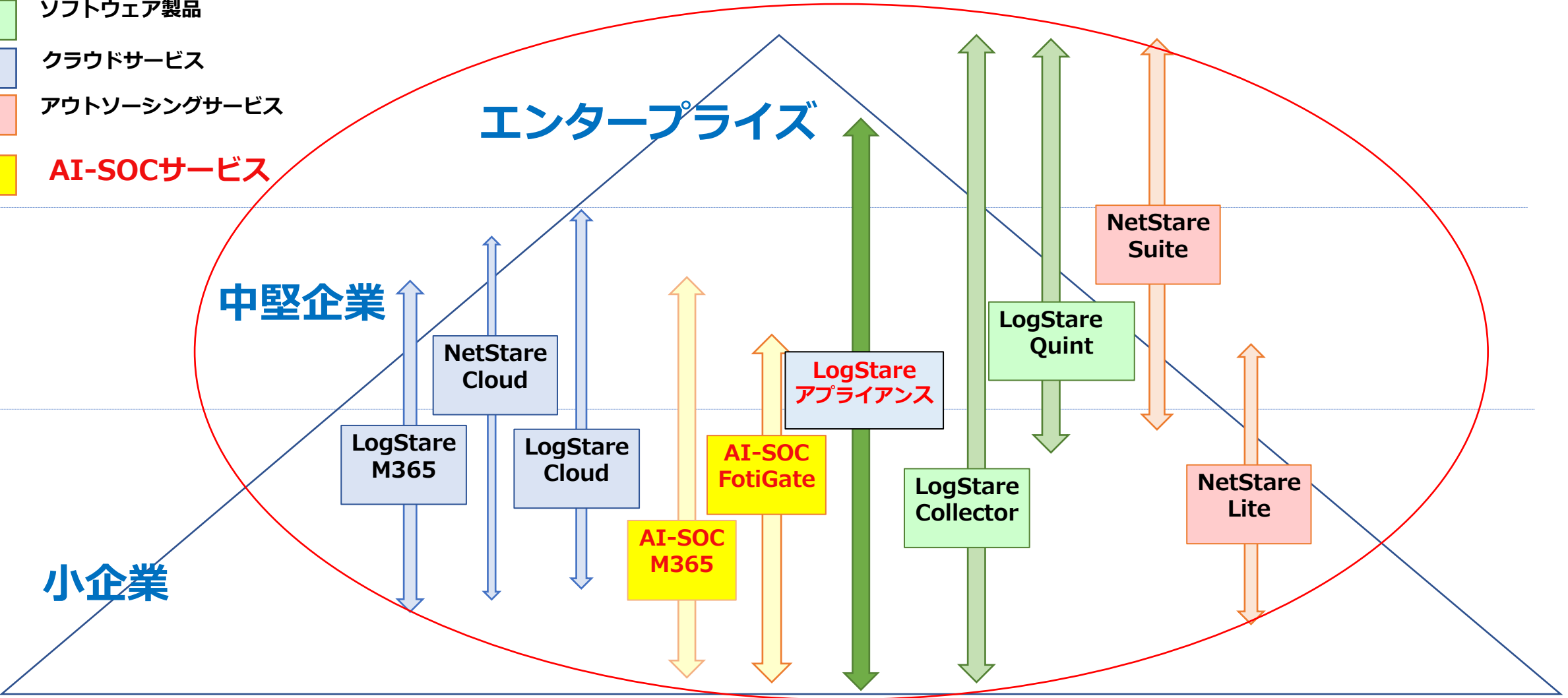
収集したログは24時間365日有人対応のSOC (Security Operation Center) に転送し解析するので、ランサムウェア検知時の対応をSOCに相談することも可能です。





# ターゲット (2025～)

- ソフトウェア製品
- クラウドサービス
- アウトソーシングサービス
- AI-SOCサービス



新規リリースサービス

Microsoft 365の“運用上のリスク”をAIが監視  
クラウド時代の新しいSOCサービス

AI-SOC for Microsoft 365

powered by NetStare

『AI-SOC for Microsoft 365』はMicrosoft 365の利用状況をAIが監視し、セキュリティリスクの高い事象を検知してアラートする次世代のSOC (Security Operation Center) サービスです。SOC黎明期から25年にわたって培ったセキュアヴェイルのログ分析のノウハウをAIに継承し、Microsoft 365の監査ログからアカウント乗っ取りの可能性、外部からの不正アクセスによる侵入、アクセス権の不備による情報流失のリスクなどを検知してアラート通知します。

従業員のアカウントが不正使用された!?

重要ファイルが世界中に公開された!?

退職者が重要ファイルをダウンロードした!?

管理者権限を悪用された!?

人手では見逃しがちなリスクを  
AI-SOCが代わりに監視  
クラウド活用の安心と効率が向上します

👍 1ユーザー月額50円、AI-SOCだから実現できるサービス価格

👍 いざという時は24/365の有人窓口への質問もOK

👍 より高度なSOCやログ分析サービスに柔軟に拡張できる

© SecuAvail Inc. www.secuavail.com

AI-SOC powered by NetStare

3つの標準サービスでIT管理者のセキュリティ運用を支援

🔔 アラート ... アカウント乗っ取りや外部からの不正アクセスなど、セキュリティインシデントの兆候を見つけたら直ちに通知します。

📊 月次レポート ... 1ヶ月間の監査ログの分析レポートを提出。Microsoft 365の利用状況や隠れたリスクが分かります。

👤 ヘルプデスク ... 必要に応じて24/365有人窓口でアラートの内容や対応方法について質問できます。

Microsoft 365  
Officeアプリケーション  
Share Point / One Drive  
Teams etc...

クラウドtoクラウドで監査ログ収集

業務利用  
管理者  
お客様環境

SecuAvail AI-SOC  
ログ収集・保管  
ログ分析  
アラート判定  
アラート通知  
レポート作成

アラートメール  
月次レポート  
ヘルプデスク

オペレーター (24/365)

AI-SOCのアドバイザーコメントで初動対応に迷わない

ただアラートやログレポートをメール通知するだけではありません。  
25年のSOCノウハウを継承したAI-SOCがセキュリティアナリストの視点でログを分析してアドバイザーコメントを記載。管理者の判断業務を支援します。  
セキュリティの専門知識がなくても対応に迷いません。

アドバイザーコメントの例

ログ分析レポートの例

サービス	価格 (月額)
AI-SOCサービス費用	¥50/ユーザー
ログ長期保管オプション	¥20/ユーザー
ログ分析調査/アドバイザー	¥10/ユーザー
ログ分析ポータルオプション	¥200/ユーザー

※別途初期費用 ¥50,000 が掛かります ※標準のログ保管期間は1か月間です  
※標準で利用のMicrosoft 365ユーザー数と専任のオペレーターが必須です  
※30ユーザー以上での契約をお願いします ※最低の契約期間1年以上、年一様払いとさせていただきます

販売パートナー

SecuAvail 株式会社セキュアヴェイル  
www.secuavail.com  
大阪市北区東天満1-1-19 アーバンエース東天満ビル

SOCサービス

※本資料に掲載の価格は2025年1月時点の価格です  
※価格の情報は予告なく変更されることがあります  
※記載されている製品名は各社の登録商標または商標です

## 最近、PR発表から

報道機関各位

令和 7 年 11 月 13 日

株式会社セキュアヴェイル（東証グロース 3042）

代表取締役社長 米今政臣

SecuAvail

NEWS RELEASE

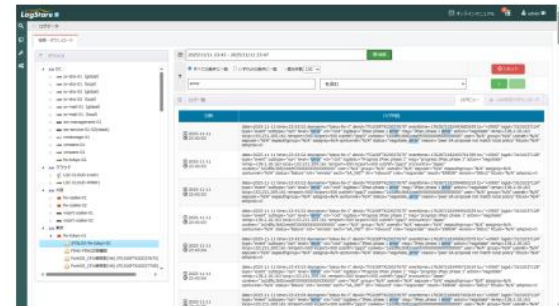
セキュアヴェイルグループ企業の LogStare が”置くだけで使える”  
統合ログ管理アプライアンスを提供開始

IT セキュリティの専門企業、株式会社セキュアヴェイル（本社：大阪市北区、代表取締役社長：米今政臣、東証グロース：3042、以下セキュアヴェイル）のグループ会社である株式会社 LogaStare（以下 LogStare）が、置くだけで簡単にログ管理が始められる統合ログ管理アプライアンス「LSC アプライアンス」の提供を開始しました。

LogaStare が独自開発する統合ログ管理ソフトウェア「LogStare Collector（ログステア コレクター）」をマイクロサーバーにインストールした状態で出荷、従来のソフトウェア版に付帯したサーバー調達や OS インストールの手間を削減し、専任の IT 運用担当者が不在の中小規模オフィスでの手軽なセキュリティ運用装置として活用が見込まれます。



LSC アプライアンス イメージ



ログはキーワード検索や正規表現による検索が可能

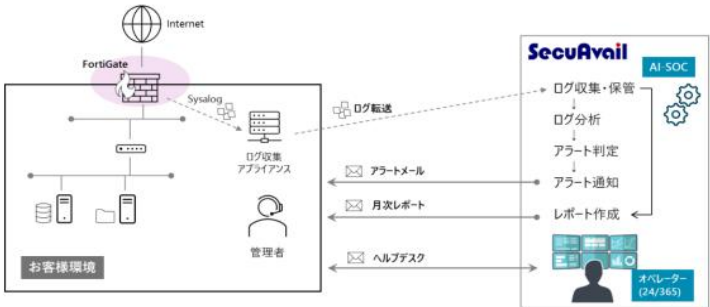
## セキュアヴェイル、AI を活用した FortiGate 向けセキュリティ運用サービス『AI-SOC』を月額 9800 円で提供開始

IT セキュリティの専門企業、株式会社セキュアヴェイル（本社：大阪市北区、代表取締役社長：米今政臣、東証グロース：3042、以下セキュアヴェイル）は、創業より 25 年にわたって提供する SOC サービス（セキュリティ運用サービス）の運用経験とグループ会社である株式会社 LogStare が開発した AI ログ分析機能を活用し、小規模ネットワーク向けの FortiGate シリーズの運用に特化した SOC サービス『AI-SOC for FortiGate』の提供を 12 月 1 日より開始します。

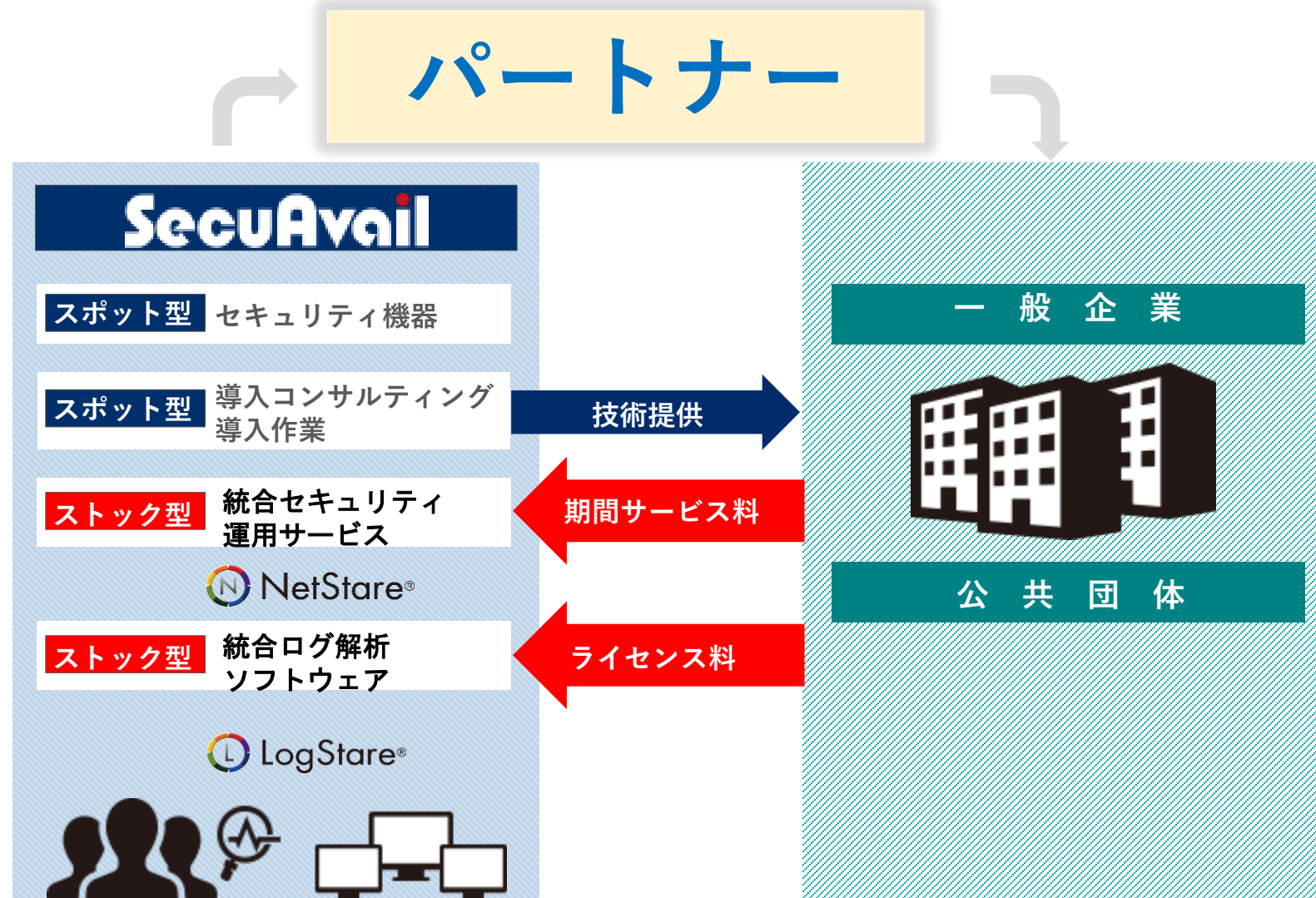
昨今は企業の大小に関わらず業務アプリケーションなどでのクラウドサービスの利用や、サプライチェーンネットワークによる企業間の情報交換のための相互接続など、インターネットのビジネス活用は不可欠です。一方でランサムウェア感染などのセキュリティ事故が多発し情報漏えいや事業停止などの影響を受けているのも実状です。しかし中小企業や医院・クリニックなどでは専任の情報担当者やセキュリティ担当者が置けず、IT ベンダーに依頼しセキュリティ対策に取り組むものの自社のネットワーク干渉の把握や確認もままならず、外部からのセキュリティ侵害、内部不正利、新しい脆弱性への対応などのセキュリティ運用が後手になっている企業がほとんどです。

セキュアヴェイルは創業時から 25 年にわたって提供する SOC サービスの運用基盤とログ分析やアラートのノウハウを AI に継承した『AI-SOC for FortiGate』の提供を 2025 年 12 月 1 日より開始します。

セキュアヴェイル FortiGate の豊富な運用実績と LogStare の AI 機能を有効活用し、月額¥9,800 という低価格での提供を実現。FortiGate の全通信を分析し、外部からの不正アクセスや内部からの不正通信による情報漏えいの可能性などを検知してアラートします。さらに FortiGate の OS のバージョンアップもオプションで提供します。

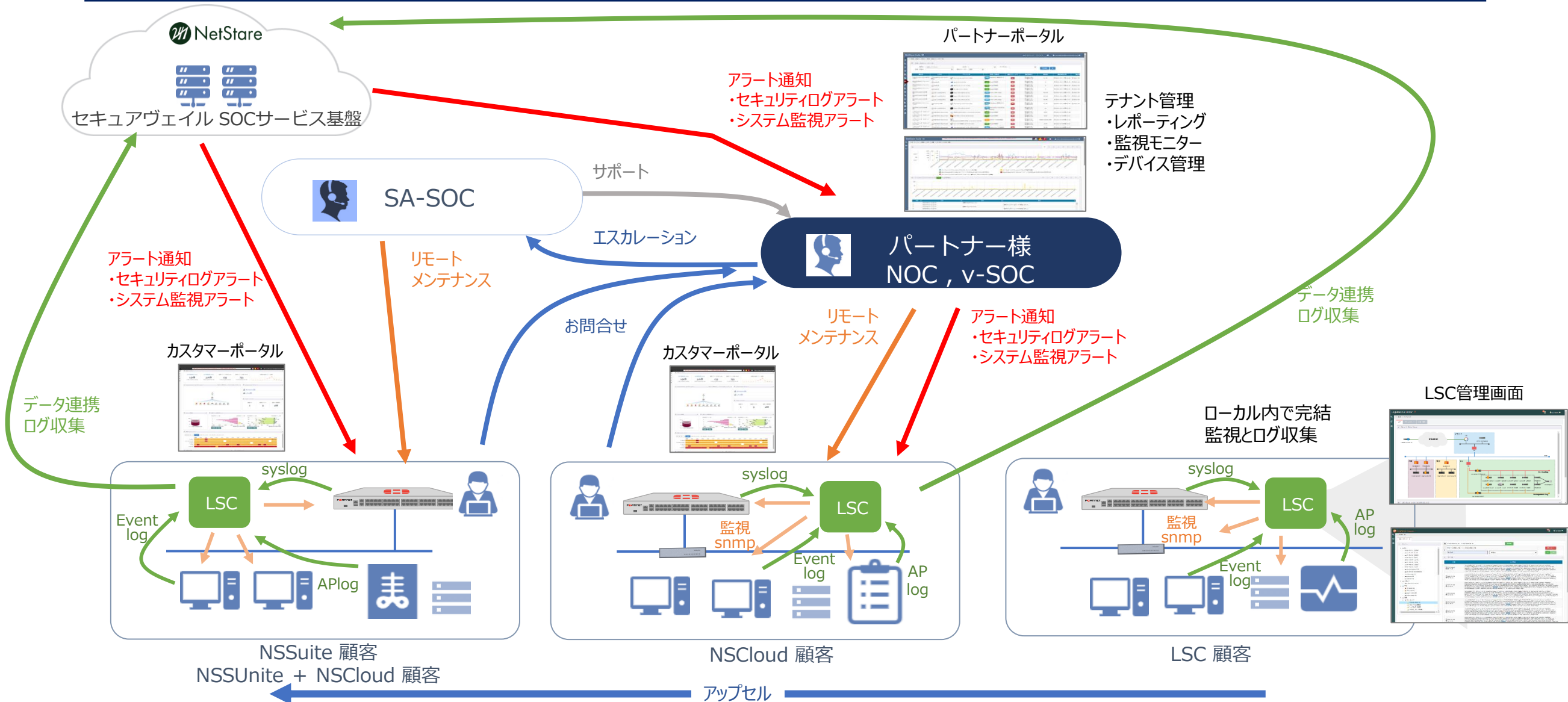


# 「ストック型ビジネス」を拡大。



# サービス提供構成

SecuAvail



本資料には、当社グループに関する見通し、将来に関する計画、業績目標などが記載されています。これらの将来の見通しに関する記述は、将来の事象や動向に関する当該記述を作成した時点における仮定に基づくものであり、実際には今後の様々な要因によって、予想数値と異なる可能性があります。





安心の見える化 - **SEC**urity for the fut**URE** -

# SecuAvail