開会のご挨拶:
KELA 事業概要と日本市場成長戦略
「能動的サイバー防御の未来をリードする」

廣川裕司
KELA株式会社 執行役員COO（最高執行責任者）
KELA Press Conference ｜ 2026年11月5日

2026 ©KELA K.K. | All rights reserved. | KELAcyber.com ULTRARED.ai SLINGscore.com

サイバーセキュリティを取り巻く環境の変化

- IT・セキュリティ・マター
- 国家安全・経営者・マター
- 全ての国民・一般人・マター

拡大し続けるサイバー攻撃被害

サイバー攻撃の年間被害額

2025年のGDPランキング(IMF)
Source: https://eleminist.com/article/4294

- 30.5兆ドル
- 19.2兆ドル
- 4.7兆ドル
- 4.187兆ドル
- 4.186兆ドル



2025年
サイバー犯罪被害額推定*1

10.5兆ドル（約1,650兆円）

2026年
サイバー犯罪被害額推定*2
11～12兆ドル（ 1,870兆円）



初期攻撃ベクトル	侵害あたりの被害額
サードパーティ・サプライチェーン侵害	**491万ドル（約7.4億円）**
認証情報の侵害	**467万ドル（約７億円）**
脆弱性の悪用	**424万ドル（約6.4億円）**

→ ランサムウェアによる年間被害額予測*3

2025年
570億ドル（約9兆円）
WW 約7500件、日本227件（約3%）

2026年
10ヶ月
＋31%ペース（約12兆円）
WW 9803件(11/4時点)

トップRAAS攻撃者：
WW:　Qilin 1666(17%), The Gentlmen 1081 (11%),　AKIRA　579 (6%)
日本：　The Gentlmen 21, Qilin 20,　SafePay 8, Everest 8

2031年
までに
2,750億ドル（約43兆円）

狙われたのか, 偶然ヒットしたのか



企業の場合は, **全体の**

70～90%

が偶然の結果

*1: Source: https://www.esentire.com/cybersecurity-fundamentals-defined/glossary/cybersecurity-ventures-report-on-cybercrime *2: Source: https://www.proxyrack.com/blog/global-cybercrime-report-2025/
*3: Source: https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/ *4: Source: https://www.ibm.com/jp-ja/reports/data-breach

KELA GROUP

2026 ©KELA Group | All rights reserved. | ULTRARED.ai

サイバーセキュリティで重要なこと
『脅威・リスクの管理』

- 何がリスク・脅威か？
- 何を守るか？
- どう守るか

サイバーセキュリティで重要なこと

- 何がリスク・脅威か？

  => 標的型攻撃(APT)、ランサムウェア、AI活用攻撃

- 何を守るか？

  => 知的財産、重要情報(顧客情報、データ）、事業そのもの

- どう守るか

  => NISTのCSF2.0(サイバーセクリティフレームワーク)
  に基づいた対応
  以前：AV ,Network→ 近年SASE, SIEM, EDR, MSS/MDR…
  受動的：Passive　→ 能動的：Active Cyber Defense(ACD)

脅威・リスクについて

2026年最新サイバー脅威は？

※IPA「情報セキュリティ10大脅威 2026

2025 順位		2026 順位	「組織」向け脅威
1	→	1	ランサム攻撃による被害
2	→	2	サプライチェーンや委託先を狙った攻撃
-		3	AIの利用をめぐるサイバーリスク
3	↘	4	システムの脆弱性を悪用した攻撃
4	↘	5	機密情報を狙った標的型攻撃
7	↗	6	地政学的リスクに起因するサイバー攻撃（情報戦を含む）
4	↘	7	内部不正による情報漏えい等
6	↘	8	リモートワーク等の環境や仕組みを狙った攻撃
8	↘	9	DDoS攻撃（分散型サービス妨害攻撃）
9	↘	10	ビジネスメール詐欺

Gartnerの予測に基づく20主要脅威・リスク
(4/14発表）

1.**サプライチェーン・サイバーリスクの拡大**:
委託先やサードパーティソフトウェアの脆弱性。
2.**AIエージェントのセキュリティリスク**:
自律的に行動するAIが悪用される新たな脅威。
3.**ランサムウェア攻撃**:
データ二重脅迫に加え、重要インフラを標的に。
4.**DDoS攻撃**:
サービス停止を狙った大規模・分散型攻撃。
5.**外部公開アプリケーション（API）の脆弱性攻撃**:
クラウド連携などを狙う。
6.**アイデンティティ（ID/パスワード）の侵害**:
認証情報窃取による不正アクセス。
7.**内部不正・情報漏えい**:
従業員による意図的または偶発的なデータ流出。
8.**偽情報・ディープフェイク攻撃**:
AI生成コンテンツを用いたソーシャルエンジニアリング。
9.**クラウド設定ミスと可視性不足**:
設定不備によるデータ暴露。
10.**未知の脆弱性（ゼロデイ）を突いた攻撃**:
セキュリティパッチ未公開の脆弱性を利用。

KELA

最大サイバー脅威は？

① 最大の脅威：ランサムウェア（不動の1位）

•11年連続で最重要脅威
•日本企業への攻撃件数も増加（前年比＋42%）

なぜ最も危険か

•事業停止（＝売上直撃）
•データ公開（二重恐喝）
•サプライチェーン全体に波及 👉 **もはやIT問題ではなく「経営停止リスク」**

② 次に危険：サプライチェーン攻撃（連鎖型リスク）

•取引先・委託先を踏み台に侵入
•日本企業は特に影響を受けやすい構造

ポイント

•自社が強くても意味がない「最も弱い1社」から崩れる
👉 **“自社防御”から“エコシステム防御”へ**

③ 2026年の本質的変化：AIサイバーリスク（新たな主戦場）

2026年に初めてトップ10脅威にランクイン

3つの側面

1.AIを使った攻撃
・フィッシングの高度化（ほぼ見抜けない） ・マルウェア自動生成

2 AIそのものへの攻撃
•モデル汚染、・プロンプト攻撃

3. AIの誤用リスク
機密情報の入力 → 情報漏えい

👉 **AIにより「攻撃の質 × スピード × 規模」が一気に上昇**

■ エグゼクティブサマリー

👉 2026年のサイバー脅威は
「AIにより最適化・拡大化されたランサムウェア経済圏」
これに対して企業が取るべき戦略は：
👉 **Reactive （事後対応）**

→ **Active（事前制御）への転換**

KELA会社・事業概要と沿革

KELAグループと日本事業沿革　(2019年にKELA株式会社設立)

KELAグループはカンパニー制度のもと、**事業会社KELA Research & Strategy, Ltd.**をはじめ、**UltraRed, Ltd.**と **Sling, Ltd.** の３社、
地域会社 KELA株式会社等で構成されています。但し、日本・APAC市場では　KELA株式会社がグループ各社全てのソリューションを統合、
市場に提供するSingle Point of Contactという形態を踏襲中。

日本事業の歩み

「見えない脅威を可視化し、攻撃を未然に防ぐ。」

2009
KELA
創業

2015
包括的な
サイバー脅威
インテリジェンス
プラットフォーム
完成

2019
外部アタックサーフェス
管理（EASM）や
侵害・攻撃シミュレーション
（BAS）テクノロジー
分野で成長
日本法人設立

2022
サードパーティ
リスク管理（TPRM）
やデジタルリスク
保護サービス
（DRPS）に
ビジネスを拡大

2023
生成AIや継続的な
脅威エクスポージャ
管理（CTEM）の
導入を開始

2025・2027～
KELA GROUP
AI エージェント活用、 C2 Hunting開始
ACD統合パッケージ、ACRD経営管理ダッシュボード
AI powered CTEM投入HIVE,Decoy・Deception、Crimson…
➡ **次世代ACD対応へPIOFA/IOFCへ**

日本事業「第二成長」フェーズ突入

能動的サイバー
ソリューションを
進化・充実

主要なソリューション　CTI　EASM　BAS　DRPS　TPRM　GenAI

アクティブディフェンスを支援するKELA Group

エンドツーエンドをカバーする脅威インテリジェンスプラットフォームが
インテリジェンスのライフサイクルをトータルにサポートします。

「見えない脅威を可視化し、攻撃を未然に防ぐ。」



SLING

サプライチェーンリスク対応

お客様のグループ企業取引先を含めたネットワーク構成要素のセキュリティリスクを診断。システムと連携して、脅威アラートやリアルタイムのリスク評価、最適なリスク軽減策の案を行い、アタックサーフェスリスクを最小化します。

『仲間を知る』
サードパーティリスク管理

KELA GROUP

ACD『能動的サイバー防御』
攻撃を未然に防ぐ

『敵を知る』
ダークウェブ脅威インテル

KELA

KELAの革新的な サイバー脅威インテリジェンスプラットフォーム



- 匿名性を確保しながら、ダークネットの情報から具体的な脅威や標的、トピック、犯罪グループの行動を リアルタイムに調査・分析
- 組織の重要な資産を守るためにダークネットのサイバー空間を監視

ULTRARED

お客様の組織にとっての最優先事項や実用的なサイバーセキュリティの課題を特定することができます。
ULTRA REDの技術をご利用いただくことで、エクスターナル・アタックサーフェス管理（EASM）、サイバー脅威インテリジェンス（CTI）、自動侵入・攻撃シ

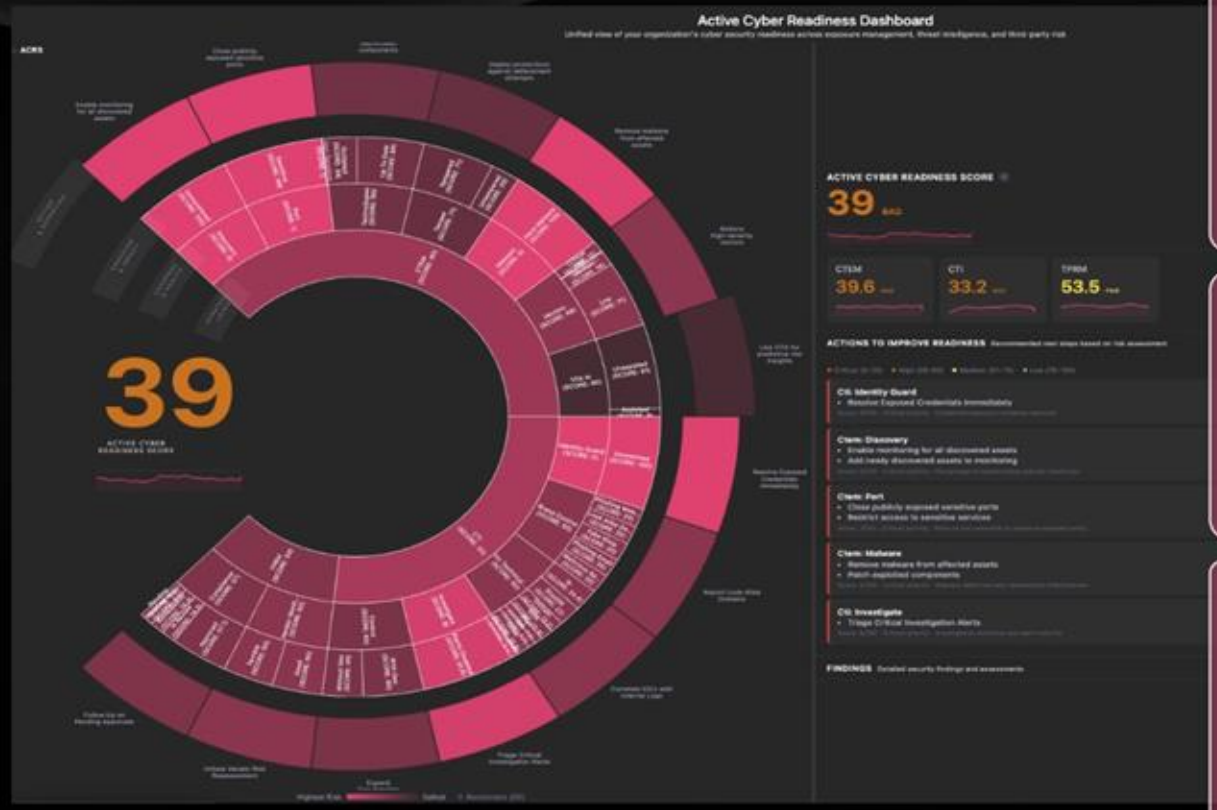


『己を知る』
外的アタックインタフェイス管理

KELAは、企業がこれまで弱かった「攻撃者視点」を、データと実例で補完し受動防御（Passive)から能動防御（Active)への転換を現実的に実現します。

アクティブサイバー経営管理ダッシュボード
Active Cyber Readiness Dashboard

組織として積極的サイバー防御の準備態勢としての基盤整備状況を可視化しアクションへマップ



CTI
サイバー脅威インテリジェンス
受動的脅威インテリジェンスと
サイバー攻撃者側を監視
Cyber Threat Intelligence

CTEM
継続的脅威エクスポージャー管理
攻撃者視点と攻撃者思考で，お客様環境
のエクスポージャーを深層解析
Continuous Threat Exposure Management

TPRM
サードパーティリスク管理
サードパーティ及びサプライチェーン
のリスク評価
Third Party Risk Management

3 YEAR ASPIRATIONAL GOAL

2028年末までに3年で狙うゴール

GOAL 01

事業規模3倍を狙う

ACV Booking（新規案件受注）

YoY 30% 成長

Renewal Booking（更新案件受注）

> 80%

業界トップの成長を狙う！

（受注・売上）

GOAL 02

組織強化と拡大

人員体制（陣容）

20人体制 ➔

50人規模

パートナービジネス

13社 ➔ 50社以上

MSSP & 2Tier Distribution加速

CTI/ASM/CTEM/TPRMの

最大パートナーエコモデル確立

GOAL 03

市場ポジション

ACD

（能動的サイバー防御）

における確固たる

トップベンダー

ポジションの確立

3 YEAR ASPIRATIONAL GOAL

2028年末までに3年で狙うゴール

GOAL 01

事業規模3倍を狙う

ACV Booking（新規案件受注）

YoY 30% 成長

Renewal Booking（更新案件受注）

> 80%

業界トップの成長を狙う！

（受注・売上）

GOAL 02

組織強化と拡大

人員体制（陣容）

20人体制 ➔

50人規模

パートナービジネス

13社 ➔ 50社以上

MSSP & 2Tier Distribution加速

CTI/ASM/CTEM/TPRMの

GOAL 03

市場ポジション

ACD

（能動的サイバー防御）

における確固たる

トップベンダー

ポジションの確立

ON TRACK!!!　組織：30人越え 6xEnt, 3 x Partner, SE/PM/CSM

パートナー 増大(新規：SB C&S様、富士通様、日立ソリューション様など）・プログラム強化

GROWTH STRATEGY

KELA株式会社の事業成長戦略 = ５本の成長戦略施策を行使=

01

Strategic Account

戦略顧客・大型案件に注力

成功ストーリーを確立（ハイタッチ営業）

主要インダストリーのトップ2-3企業への浸透を図る

02

Partner Leverage

パートナー事業でスケール

既存パートナーの活性化と新規パートナー開拓

2Tier Dist., SIer, MSSP, Referral 等を駆使し日本全国SBM含めた対応

03

Pipeline Expansion

需要創出と案件5倍化

1年以内でのターゲット達成

マーケティング・SDR・パートナー協業による抜本的需要喚起と案件の拡大を図る

04

Org Reinforce

組織の強化・人材育成

優秀な人材採用と組織力の向上

営業・SE・エキスパート・アナリスト・リサーチャ等の採用＋GPTW文化醸成

05

Ops Excellence

業務改善・効率的成長

データドリブンな意思決定

サイバーセキュリティーのトップ企業としての高効率事業モデルを確立、協業拡大を図る

TRARED.ai
2026 ©KELA Group | All rights reserved. | ULTRARED.ai

15

GROWTH STRATEGY

KELA株式会社の事業成長戦略 = ５本の成長戦略施策を行使=

01

Strategic Account

戦略顧客・大型案件に注力

成功ストーリーを確立（ハイタッチ営業）

主要インダストリーのトップ2-3企業への浸透を図る

【実績・進捗】

- 3/7 ACDパッケージACRD発表
- 6つインダストリーチーム発足
- 7/29 AI powered CTEM発表

02

Partner Leverage

パートナー事業でスケール

既存パートナーの活性化と新規パートナー開拓

2Tier Dist., SIer, MSSP, Referral 等を駆使し日本全国SBM含めた対応

【実績・進捗】

- SB C&Sほか5社以上パートナー様と新規契約締結
- 7/27 SOC発足、支援強化

03

Pipeline Expansion

需要創出と案件5倍化

1年以内でのターゲット達成

マーケティング・SDR・パートナー協業による抜本的需要喚起と案件の拡大を図る

【実績・進捗】

- 2月よりIn-house SDR発足
- Pipe額 x 4.5倍に拡大

04

Org Reinforce

組織の強化・人材育成

優秀な人材採用と組織力の向上

営業・SE・エキスパート・アナリスト・リサーチャ等の採用＋GPTW文化醸成

【実績・進捗】

- SE/PM/CSM 人員倍増！
- 営業部門は3倍化
- 東京本社新橋移転(50+人 capacity)
- 大阪オフィス開設

05

Ops Excellence

業務改善・効率的成長

データドリブンな意思決定

サイバーセキュリティーのトップ企業としての高効率事業モデルを確立、協業拡大を図る

【実績・進捗】

- SOC発足で営業支援高速化
- Training/POCで価値訴求加速
- Flexible Pricing(User単位 EA等)

2026 ©KELA Group | All rights reserved. | ULTRARED.ai

KELAGROUP

KELA ULTRARED SLING

Thank You

www.kelacyber.com/ja

2026 ©KELA Group | All rights reserved.