SECURING JAPAN'S SUPPLY CHAIN

AI駆動型リスクモニタリングで実現する ― 日本企業を守るリアルタイム・サプライチェーン脅威インテリジェンス

Pipeline株式会社
代表取締役社長
渡辺　アラン

www.ppln.co

PIPELINE 株式会社とは？

RiskSensorが日本セキュリティ大賞2025を優秀賞、AIでササプライチェーンのリスク可視化を革新Pipeline株式会社、
「**日本セキュリティ大賞2025**」セキュリティ運用支援部門を受賞

■ 審査員講評：園田 道夫 氏（NICT ナショナルサイバートレーニングセンター長）

今回、RiskSensorの受賞に際し、審査員である**国立研究開発法人情報通信研究機構（NICT） ナショナルサイバートレーニングセンター長・園田 道夫 氏**より、以下の評価をいただきました。

「PipelineのRiskSensorは、プロフェッショナルなセキュリティ知見をAIに統合し、企業外部に散在するリスクを高精度に可視化する点が非常に優れている。特に、サプライチェーンを含む全国規模の外部攻撃面データを蓄積・分析し、日本全体のサイバーリスクを評価する"国家レベルの基盤"を目指す構想は大いに期待できる。」

新たなサイバー脅威から日本企業を保護

監視対象 | WHAT WE MONITOR:
- ダークウェブフォーラムとマーケットプレイス
- ランサムウェアグループのコミュニケーション
- アンダーグラウンド脅威アクターコミュニティ
- 日本/APACを標的とした新たな攻撃キャンペーン

PIPELINE HORIZON – UNIT ZERO は、アジア太平洋地域における脅威情報リサーチと分析を専門とするチームです。

抽出情報 | INTELLIGENCE EXTRACTED:
- 脅威アクターの戦術・手法（TTPs）
- 貴業界を標的とした攻撃の早期警告
- 侵害の兆候（IOCs）
- サプライチェーン上の脅威パターン

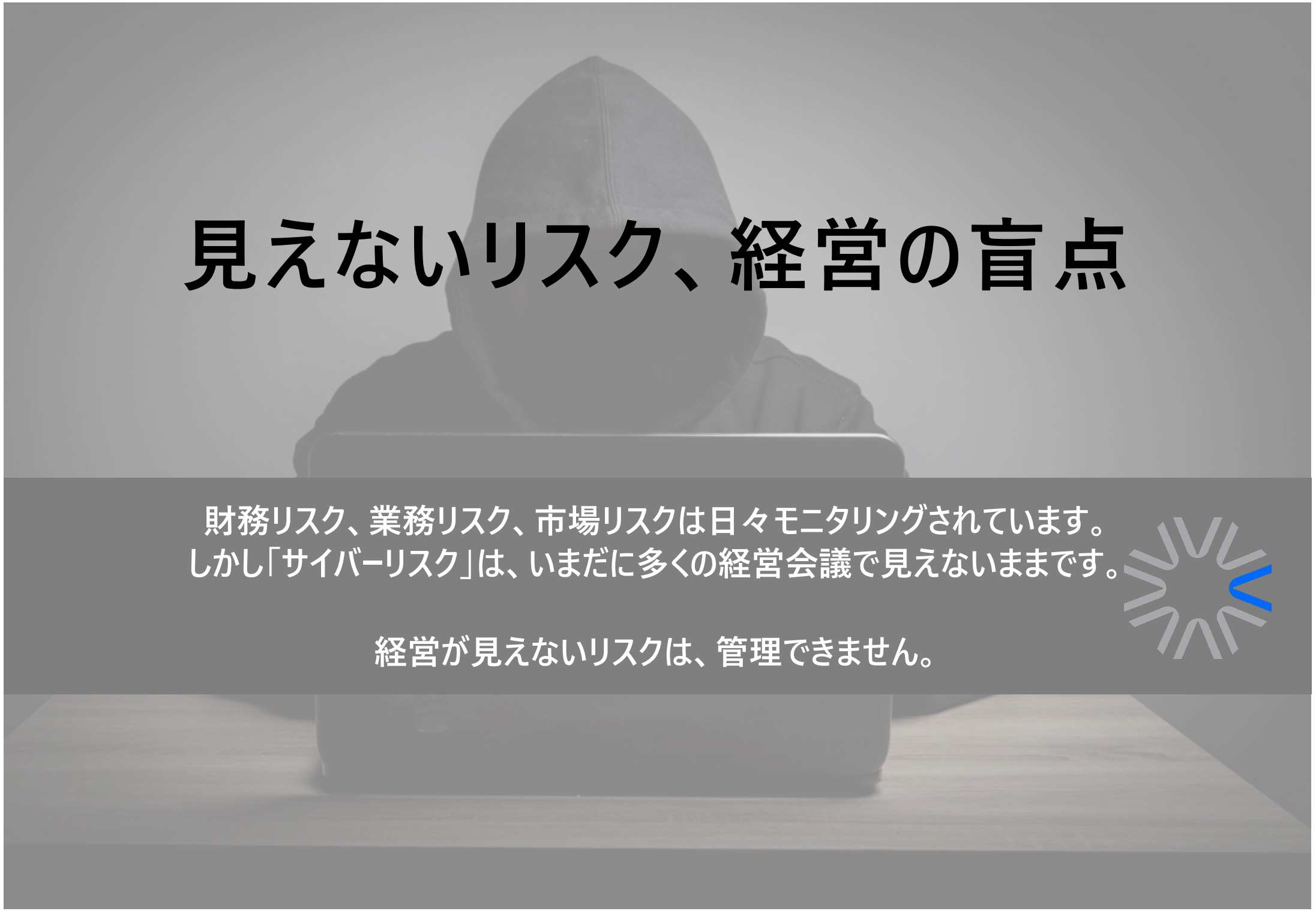
WE ARE PIPELINE HORIZON – UNIT ZERO

倫理基準 | ETHICAL STANDARDS:

✓ クライアント保護のための監視
✓ 脅威のパターンのみを抽出
✓ 責任ある開示

✗ 被害者のファイルは絶対にダウンロードしない
✗ 盗まれたデータを絶対に悪用しない
✗ 被害者にさらなる危害を加えない

www.ppln.co



見えないリスク、経営の盲点

財務リスク、業務リスク、市場リスクは日々モニタリングされています。
しかし「サイバーリスク」は、いまだに多くの経営会議で見えないままです。

経営が見えないリスクは、管理できません。

クリエイティブボックス株式会社・インシデント　8月16日2025年

クリエイティブボックス株式会社
デザインスタジオ
完全子会社

発生した事象：8月16日2025年

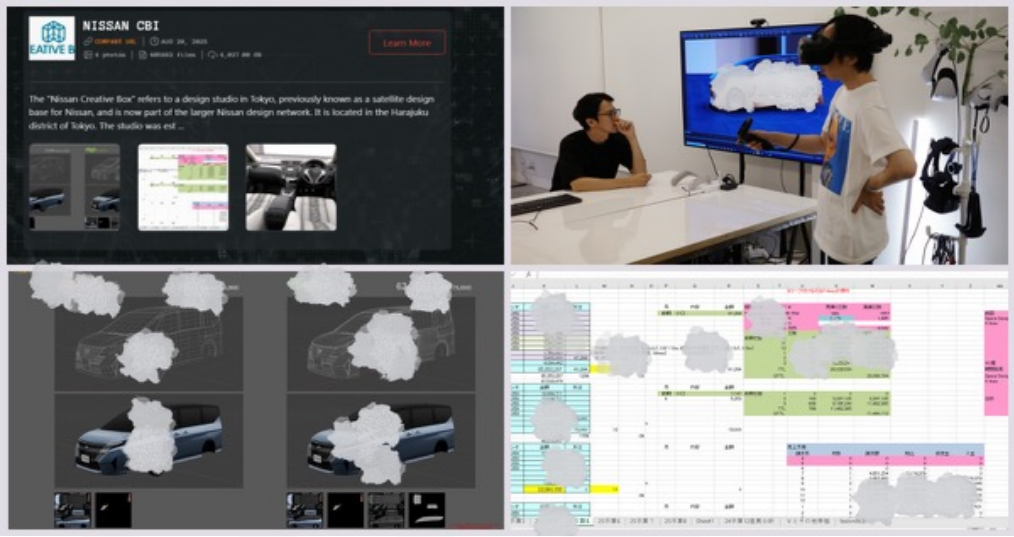
不審なアクセスを検知
↓ CBIが緊急対策を実行
↓ 警察へ通報
↓ 8月20日：脅威主体が侵害を公表
↓ 8月26日：日産が侵害を確認
↓ 手遅れでした

4テラバイトが盗まれました
405,882ファイル
合計10日間

TLP:CLEAR | https://www.nikkei.com/article/DGXZQOUC262TW0W5A820C2000000/

日産クリエイティブボックスが最適なターゲットであった理由：

405,882 FILES | 4 TERABYTES | YEARS OF R&D



- ✓ 製造業／自動車業界
- ✓ Fortinet VPNの脆弱性が存在します
- ✓ 高価値知的財産：数百万ドル相当の車両設計
- ✓ 専門子会社
- ✓ データ漏洩のみ

日産自動車の公式声明：「漏洩したデータは、CBIの唯一の顧客である日産自動車のみに影響を及ぼします。お客様、契約業者、その他の企業様の情報は一切漏れておりません。」

サプライチェーンへの影響：
御社の設計パートナー、研究開発協力企業、および専門子会社において、修正されていない脆弱性のあるフォーティネットVPNをご利用の場合、直ちに危険に晒されます。Qilinは、御社のサプライチェーン内にある、まさにこうした高価値でセキュリティ対策が不十分な組織を標的としています。

日本のサプライチェーンを狙うサイバー犯罪者たち
CYBERCRIMINALS IN JAPAN'S SUPPLY CHAIN

攻撃の主な手口：

1. **防御の甘いサプライヤーを狙う** — セキュリティ対策が不十分な下請け企業を侵入口に
2. **認証情報をダークウェブで売買** — 取引先のIDやパスワードを悪用
3. **既知の脆弱性を悪用** — 未更新ソフトや古いシステムを標的に
4. **研究・開発データを窃取** — 機密情報を国外へ流出

サイバー攻撃がもたらすリスク：

- サプライチェーン全体が連鎖的に被害を受ける可能性
- 経済・技術・国家ブランドへの深刻な打撃
- セキュリティ対策が遅れると、**「日本全体が脆弱」**と見なされるリスク

REAL DANGER

REAL DANGER

”ISO・脆弱性診断やりました”
“気にしてるけど何をすれば良い？”
“中小企業のデータなんか狙われない”
“漏えいしても問題ない”

じゃ何が必要か？

✓外部からの継続的な可視性（攻撃者の視点）
Continuous external visibility (attacker‘s view)

✓ リアルタイムの脅威インテリジェンス統合
Real-time threat intelligence integration

✓ 日本のビジネスとサプライチェーンに特化
Japan supply chain specialization

✓ AIによる自動化と優先順位付け
AI-powered automation and prioritization

Risksensor ／ リスクセンサーです～

www.ppln.co

リスクセンサーとは

リスクセンサーの主なスキャン項目

リスクセンサーは、データ漏洩や攻撃被害の兆候など、脆弱性診断には通常含まれない内容もスキャンしています。
スキャン項目は現時点で50項目以上あり、その中でも代表的なものは次のとおりです。

カテゴリ	スキャン項目例
データ漏洩	・ダークウェブ上でのアカウント情報の漏洩状況 ・機密データの外部公開状況
攻撃被害の兆候	・ランサムウェアグループによるメンション ・類似（フィッシング）ドメインの有無
Webアプリケーション	・管理画面の露出状況 ・検証環境の有無
メール関連設定	・SPF関連レコードなどの設定状況 ・ブロックリストへの登録状況
その他	・DNS関連レコードなどの設定状況 ・クラウドサービス関連画面の露出状況

リスクセンサー（RiskSensor）技術は特許出願中です

AI駆動型リスクモニタリングで実現するリアルタイム・サプライチェーン脅威インテリジェンス

AI-DRIVEN REAL-TIME SUPPLY CHAIN THREAT INTELLIGENCE

1. 全国規模のデータ基盤を構築

全国の企業情報を安全に保管・分析するデータベースを整備

Building a nationwide data infrastructure to securely store and analyze corporate information

2. サプライチェーン全体を可視化

企業間のつながりを分析し、リスクスコアリングと脅威インテリジェンスを提供

Visualizing the entire supply chain to deliver risk scoring and threat intelligence

3. AIによるリスク理解の高度化

AIが脆弱性を自動分析し、組織のリスクを定量的に把握

Enhancing risk understanding through AI-driven vulnerability analysis

4. 対話型セキュリティAIエージェント

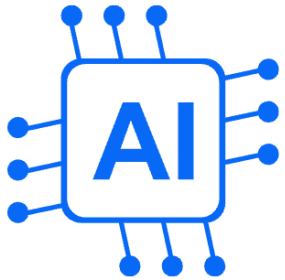
AIエージェントとの対話を通じて最適な対策を提示・支援

Interactive Security AI Agent that recommends and assists with optimal countermeasures

5. 日本の実情に即した国産プラットフォーム

法規制・商習慣・脅威動向に合わせた設計

Developed as a Japan-specific, domestically designed platform aligned with local regulations and threat landscape



RiskSensor

リスクセンサー（RiskSensor）技術は特許出願中です

Risksensor
リスクセンサー・レポートサービス

Risksensor = ASM ＋ TPRM + Darkweb調査 レポート

お客様からいただくのは**調査対象のドメイン(IPアドレス)情報**のみ　⇒　レポート排出

pipeline

総合評価（サマリー）

C　実施日：2025年1月1日　スキャン対象ドメイン：example.com

総合評価：C

今回のスコア（60/100）

0 Critical Notice 100

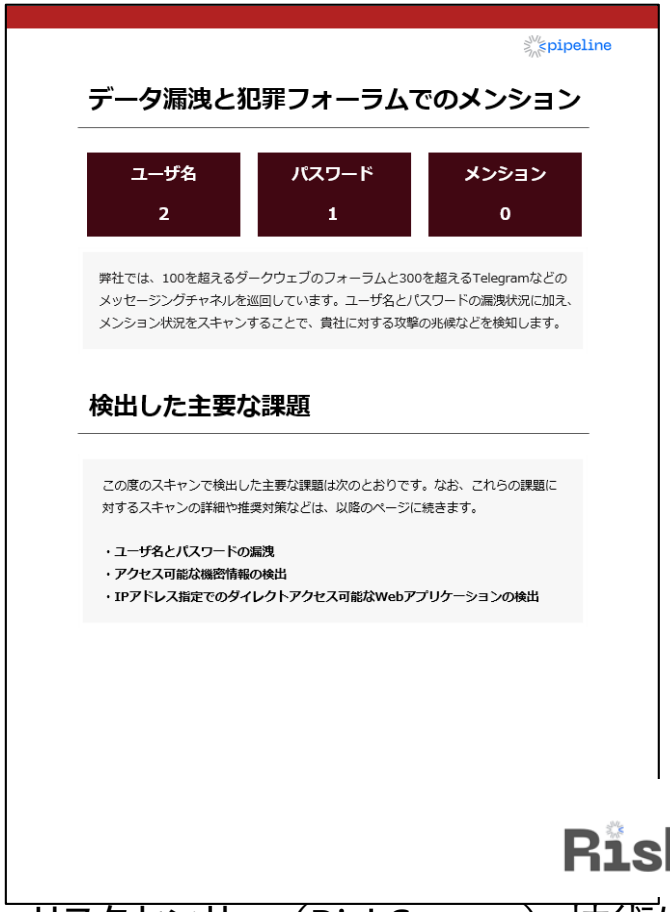
平均スコア（65/100）

検出数	評価	カテゴリ	スキャン項目例
1/2	F	データ漏洩	・ダークウェブ上での機密情報の漏洩状況 ・機密データの外部公開状況
2/6	C	攻撃被害の兆候	・ランサムウェアグループによるメンション ・未確認かつ懐疑的なドメインの有無
4/8	D	Webアプリケーション	・管理画面の露出状況 ・検証環境の有無
1/2	D	メール関連設定	・SPF関連レコードなどの設定状況 ・ブロックリストへの登録状況
0/4	A	その他	・DNS関連レコードなどの設定状況 ・クラウドサービス関連画面の露出状況

※リスク評価(5種）：A:Notice - B:Low - C:Medium - D:High - F:Critical
※平均スコア：RiskSensorご利用企業による初回レポート時のスコア平均

RiskSensor

3



pipeline

データ漏洩と犯罪フォーラムでのメンション

ユーザ名	パスワード	メンション
2	1	0

弊社では、100を超えるダークウェブのフォーラムと300を超えるTelegramなどのメッセージングチャネルを巡回しています。ユーザ名とパスワードの漏洩状況に加え、メンション状況をスキャンすることで、貴社に対する攻撃の兆候などを検知します。

検出した主要な課題

この度のスキャンで検出した主要な課題は次のとおりです。なお、これらの課題に対するスキャンの詳細や推奨対策などは、以降のページに続きます。

- **ユーザ名とパスワードの漏洩**
- **アクセス可能な機密情報の検出**
- **IPアドレス指定でのダイレクトアクセス可能なWebアプリケーションの検出**

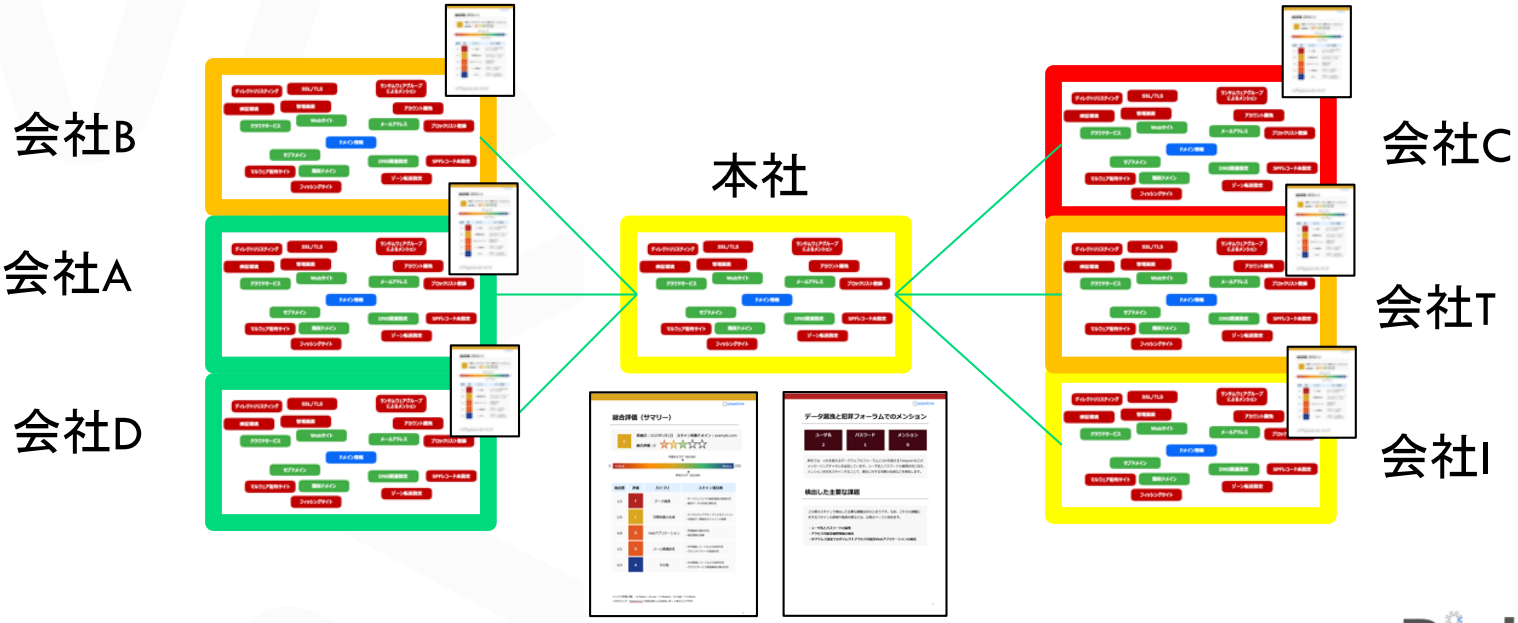
RiskSensor

リスクセンサー（RiskSensor）技術は特許出願中です

Risksensor ／ リスクセンサー特徴

日本のサプライチェーンに特化した、AI駆動型の リアルタイム外部脅威インテリジェンスプラットフォーム

1. 日本企業がサプライチェーン全体の外部脅威を 攻撃者より先に発見できるようにする
2. リアルタイムの可視性と実用的なインテリジェンスで 侵害を予防する
3. 日本の商習慣と規制環境に適合した 国産プラットフォームを提供



リスクセンサー（RiskSensor）技術は特許出願中です

RiskSensor Guardian

リスクセンサー・ガーディアンサービス

サイバー緊急時に押せる安心パッケージ

🚨もしもの時、すぐに助けを呼べる仕組みを。

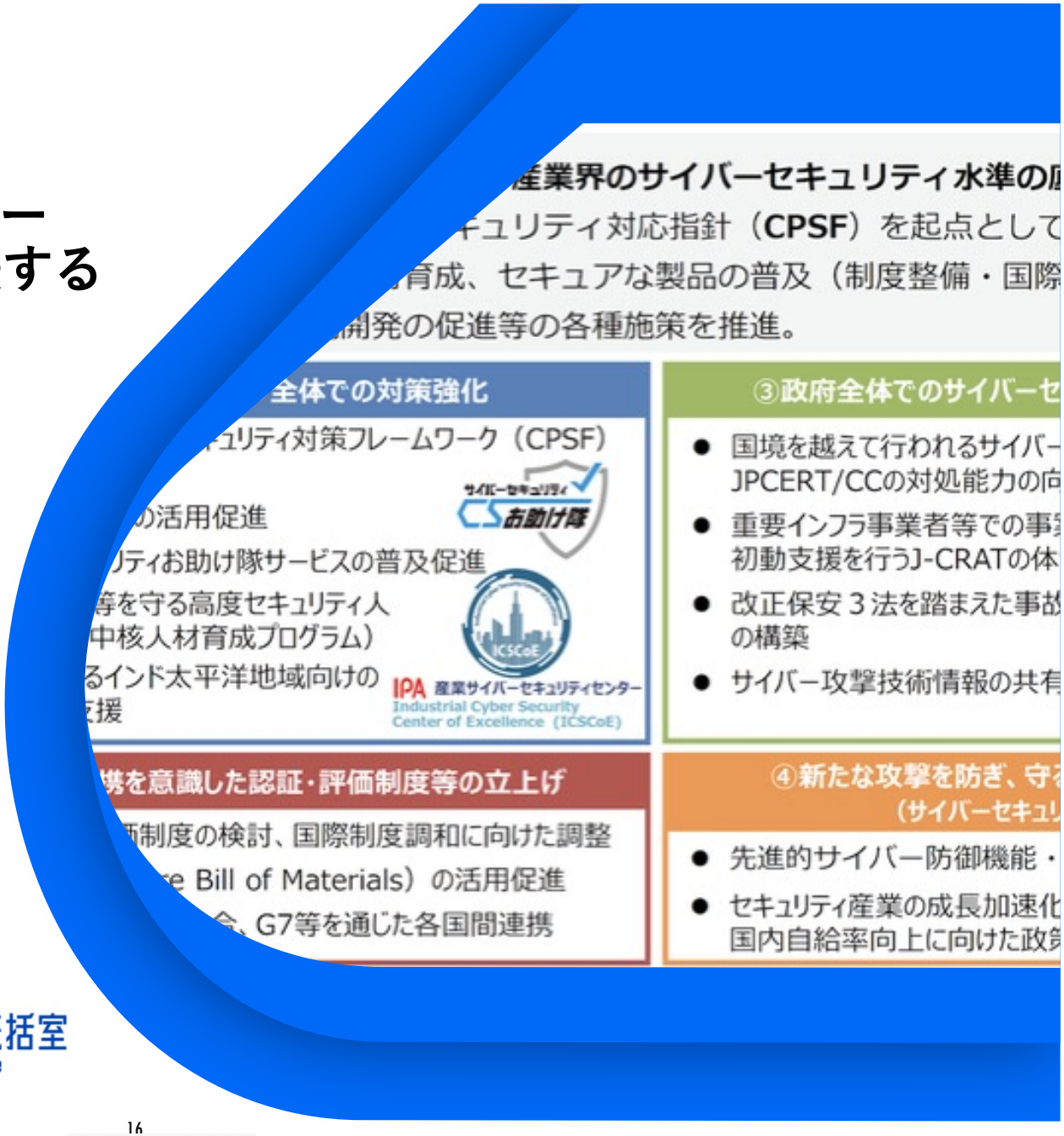
検知 → **分析** → **対応** → **改善**

- 年間契約内で利用できる **ワンタイム緊急対応サポート**
- **専門アナリストが即時リモート対応**（初動から封じ込めまで）
- **実際のIRチームが直接支援** ― 技術調査・報告・提言を実施
- **72時間以内に報告書提出**（原因分析・再発防止策含む）

本サービスはリスクセンサー年間パッケージに含まれる安心保証オプションです。

Risksensor ／ リスクセンサー
コンプライアンス対応を支援する

- 外部可視化とコンプライアンス保証をつなぐ。
- 検出されたリスクをSTAR-1／JC-STAR管理項目にマッピング。
- ビジネス影響度に基づくリスク分析のエビデンスを自動生成。
- パートナーが事前アセスメントや継続的準備チェックを提供可能。
- IPAのICSリスク評価モデルに基づくアプローチ。
- 資産重要度 × 脅威レベル × 脆弱性レベル = 動的リスクスコア。
- 技術的な結果をビジネス影響度に変換。



METI Ministry of Economy, Trade and Industry

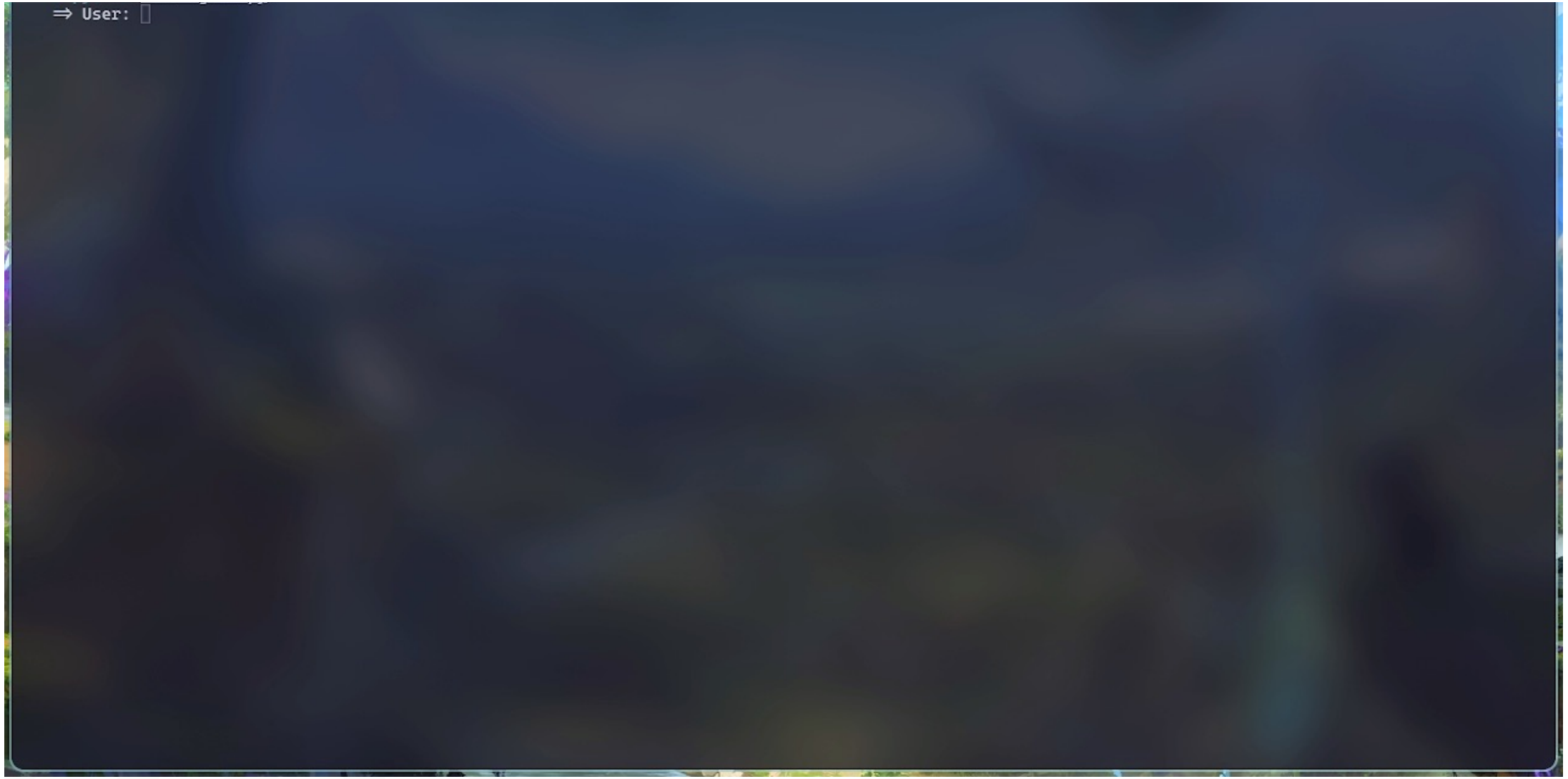
国家サイバー統括室 National Cybersecurity Office

JC-STAR IPA ISO CIS MITRE ATT&CK

RiskSensor.ai

AI駆動型リスクモニタリングで実現する ― 日本企業を守るリアルタイム・サプライチェーン脅威インテリジェンス

RiskSensor




私たちの未来のために
WWW.PPLN.CO — FOR OUR FUTURE
HELLO@PPLN.CO