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

PIPELINE 株式会社とは？

日本発のグローバルMSSプロバイダーとして、サイバーセキュリティ課題を解決します

国内企業のデジタル資産を保護します

日本セキュリティ大賞2024

この度は、「日本セキュリティ大賞2024」において
セキュリティ運用支援部門の大賞を賜り、誠に光栄です。
この受賞は、日々支えてくださるお客様やパートナー企業、
そして弊社チーム全員の尽力の賜物です。
特に、未活用だった情報資源を有効活用するための挑戦が
評価されたことを嬉しく思います。

今後も皆さまの信頼に応え、
より一層サイバーセキュリティの発展に貢献してまいります。

Pipeline株式会社　渡辺アラン

List of award-winning companies

日本電気株式会社、株式会社資生堂、舞鶴市、日本電気株式会社 サイバーセキュリティ戦略統括部、北海道地域情報セキュリティ連絡会、株式会社SYNCHRO、株式会社ストラテジア、サイバートラスト株式会社、ソフトバンク株式会社、アイシーエルシステムズ有限会社、日本サイバーセキュリティファンド1号投資事業有限責任組合

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

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

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。

倫理基準 | ETHICAL STANDARDS:

✓ クライアント保護のための監視	X 被害者のファイルは絶対にダウンロードしないでください
✓ 脅威のパターンのみを抽出	X 盗まれたデータを絶対に悪用しないでください
✓ 責任ある開示	X 被害者にさらなる危害を加えないでください

THEY HAVE
YOUR DATA
御社の大切なデータ
犯罪者の手元にあります。

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

QILIN

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

日本のサプライチェーンにおけるサイバー犯罪者
CYBERCRIMINALS IN JAPAN'S SUPPLY CHAIN

1. セキュリティ対策がなされていないサプライチェーン内の企業を狙い
2. ダークウェブで売り買いされている認証情報を取得
3. 既知の脆弱性にさらされているソフトウェアへマルウェアを展開
4. 機密情報の研究開発データを盗み、インターネット上へ流出させた

- サプライチェーンのセキュリティ対策の不備は日本経済、イノベーションに危機をもたらしている。
- 日本がセキュリティ対策がなされていない国家とみなされれば、同盟国や地域内での信頼を失い、取り返しのつかない危機となる恐れがある。

REAL DANGER

REAL DANGER

”ISO・脆弱性診断やりました”
“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”
“気にしてるけど何をすれば良い？”

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

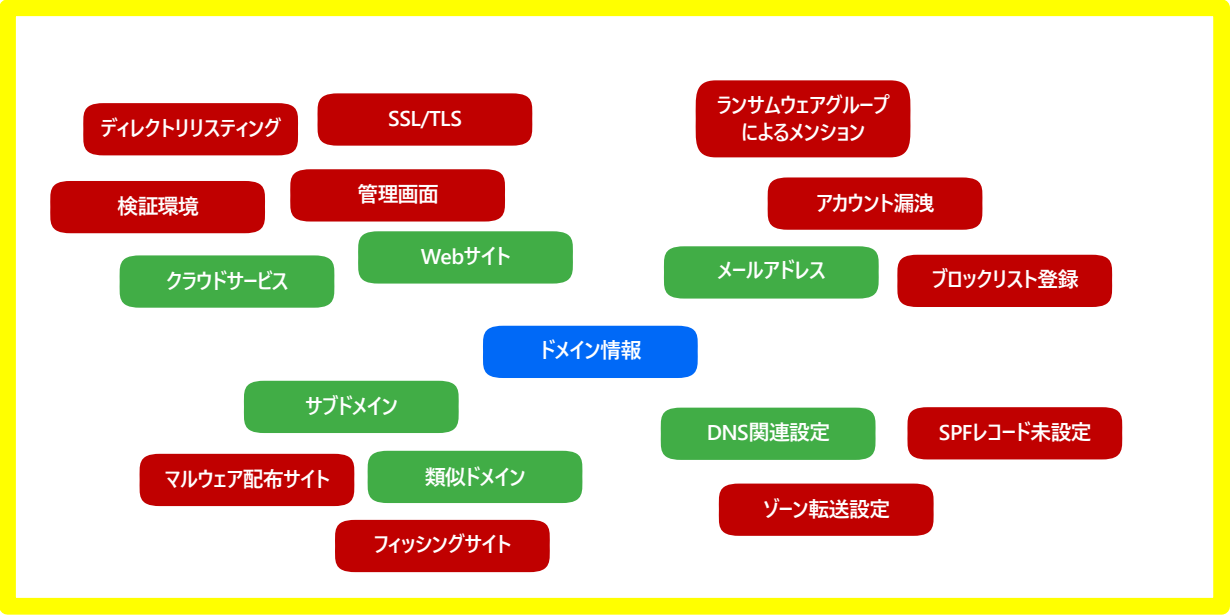
Risksensor ／ リスクセンサーです～

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。

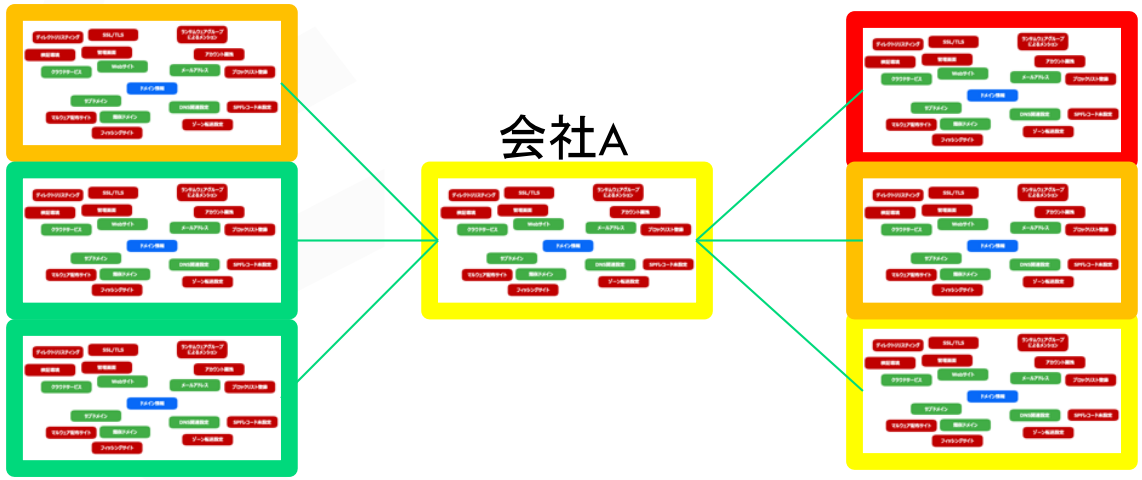
カテゴリ	スキャン項目例
データ漏洩	・ダークウェブ上でのアカウント情報の漏洩状況 ・機密データの外部公開状況
攻撃被害の兆候	・ランサムウェアグループによるメンション ・類似（フィッシング）ドメインの有無
Webアプリケーション	・管理画面の露出状況 ・検証環境の有無
メール関連設定	・SPF関連レコードなどの設定状況 ・ブロックリストへの登録状況
その他	・DNS関連レコードなどの設定状況 ・クラウドサービス関連画面の露出状況



Risksensor ／ リスクセンサーとは

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
   Enable Japanese enterprises to discover external threats across their supply chain before attackers do
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
   Prevent breaches through real-time visibility and actionable intelligence
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
   Provide a Japan-built platform aligned with Japanese business practices and regulatory environment



Risksensor ／ リスクセンサー

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

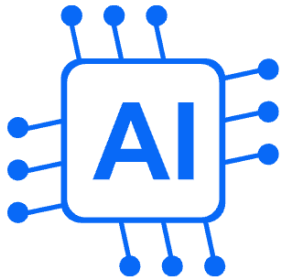
企業間のつながりを分析し、リスクスコアリングと脅威インテリジェンスを提供

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

サービス概要(1)サマリ版

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）

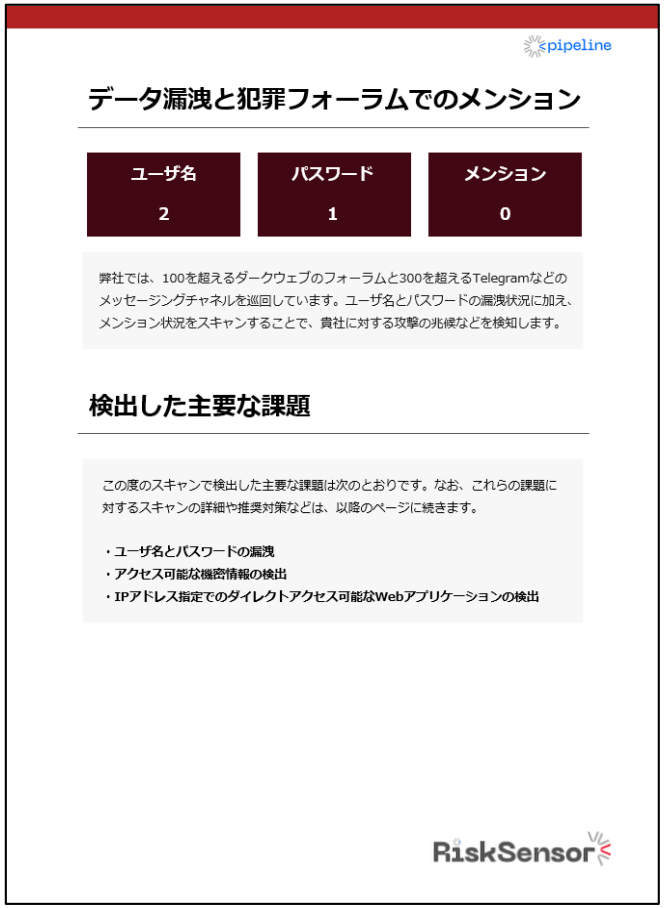
検出数	評価	カテゴリ	スキャン項目例
1/2	F	データ漏洩	・ダークウェブ上での機密情報の漏洩状況 ・機密データの外部公開状況
2/6	C	攻撃被害の兆候	・ランサムウェアグループによるメンション ・未確認かつ懐疑的なドメインの有無
4/8	D	Webアプリケーション	・管理画面の露出状況 ・検証環境の有無
1/2	D	メール関連設定	・SPF関連レコードなどの設定状況 ・ブロックリストへの登録状況
0/4	A	その他	・DNS関連レコードなどの設定状況 ・クラウドサービス関連画面の露出状況

※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

Risksensor ／ リスクセンサー

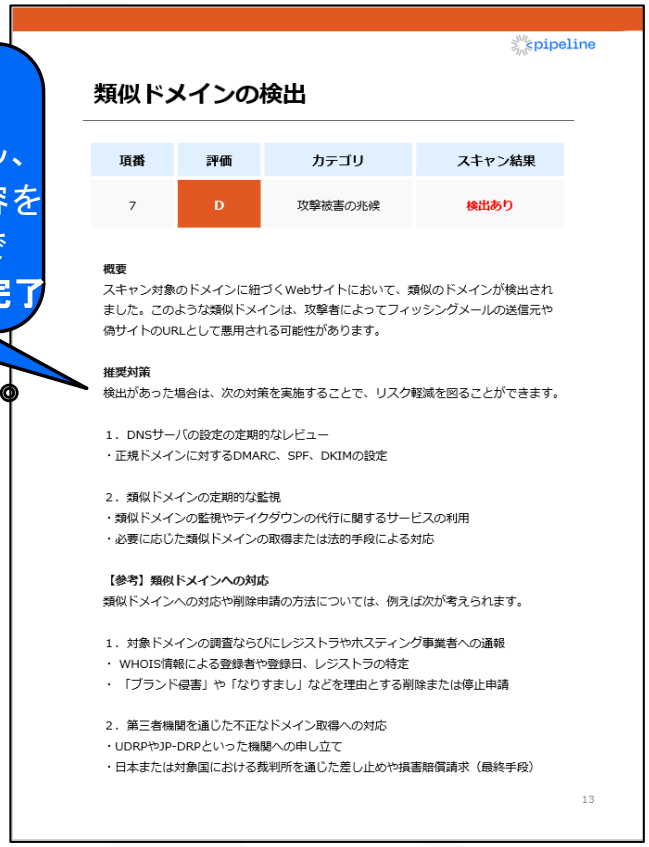
リスクセンサーサービス概要(2) フル版

M‥Management部分を実行することでセキュリティ性の向上が期待できる

サマリ版だけでは把握できないリスクの高い課題を把握及び対処・改善までの導線ご案内

推奨対策付き！
内部対処はもちろん、
外部提携先に本内容を
実行依頼するだけで
レポート**フォロー完了**

※実行リソース手配も可能◎



pipeline

類似ドメインの検出

項番	評価	カテゴリ	スキャン結果
7	D	攻撃被害の兆候	検出あり

概要
スキャン対象のドメインに紐づくWebサイトにおいて、類似のドメインが検出されました。このような類似ドメインは、攻撃者によってフィッシングメールの送信元や偽サイトのURLとして悪用される可能性があります。

推奨対策
検出があった場合は、次の対策を実施することで、リスク軽減を図ることができます。

1．DNSサーバの設定の定期的なレビュー
・正規ドメインに対するDMARC、SPF、DKIMの設定

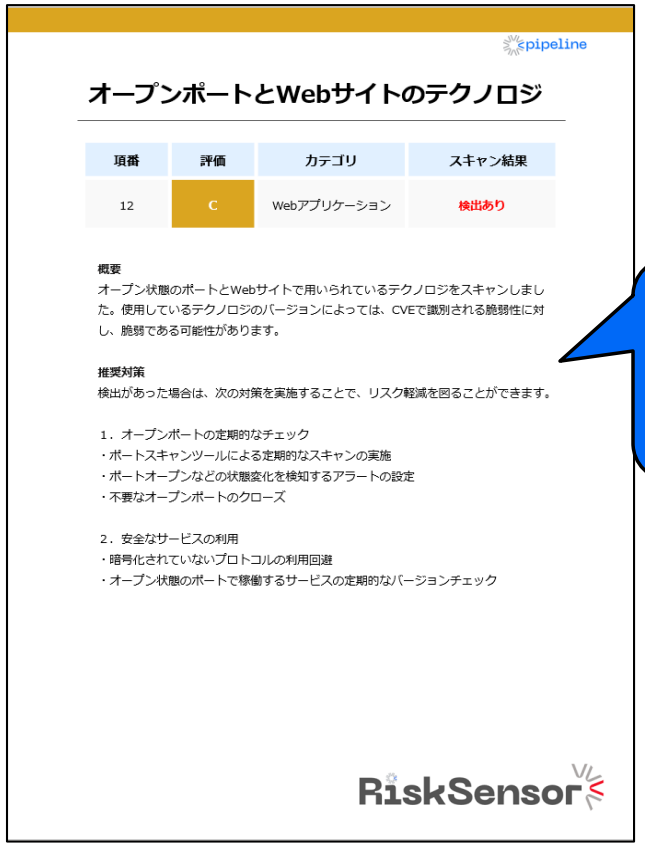
2．類似ドメインの定期的な監視
・類似ドメインの監視やテイクダウンの代行に関するサービスの利用
・必要に応じた類似ドメインの取得または法的手段による対応

【参考】類似ドメインへの対応
類似ドメインへの対応や削除申請の方法については、例えば次が考えられます。

1．対象ドメインの調査ならびにレジストラやホスティング事業者への通報
・ WHOIS情報による登録者や登録日、レジストラの特定
・ 「ブランド侵害」や「なりすまし」などを理由とする削除または停止申請

2．第三者機関を通じた不正なドメイン取得への対応
・UDRPやJP-DRPといった機関への申し立て
・日本または対象国における裁判所を通じた差し止めや損害賠償請求（最終手段）

13



pipeline

オープンポートとWebサイトのテクノロジ

項番	評価	カテゴリ	スキャン結果
12	C	Webアプリケーション	検出あり

概要
オープン状態のポートとWebサイトで用いられているテクノロジをスキャンしました。使用しているテクノロジのバージョンによっては、CVEで識別される脆弱性に対し、脆弱である可能性があります。

推奨対策
検出があった場合は、次の対策を実施することで、リスク軽減を図ることができます。

1．オープンポートの定期的なチェック
・ポートスキャンツールによる定期的なスキャンの実施
・ポートオープンなどの状態変化を検知するアラートの設定
・不要なオープンポートのクローズ

2．安全なサービスの利用
・暗号化されていないプロトコルの利用回避
・オープン状態のポートで稼働するサービスの定期的なバージョンチェック

RiskSensor

被害に繋がった場合の
リスク内容は多面的に
記載しているので
見直しのきっかけに

記載内容：対象ドメインの評価＋漏洩情報＋詳細リスクや推奨対策

Risksensor ／ リスクセンサー

- NISCをはじめ関係省庁との連携の下、**産業界のサイバーセキュリティ水準の底上げに向けた施策を企画・実行**。Society 5.0におけるセキュリティ対応指針（**CPSF**）を起点として、実践的なガイドラインの整備、**中小企業の支援**、人材育成、セキュアな製品の普及（制度整備・国際連携）、サイバー攻撃被害企業への対処支援、研究開発の促進等の各種施策を推進。

①サプライチェーン全体での対策強化

- サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）の具体化・実装
- 経営ガイドラインの活用促進
- サイバーセキュリティお助け隊サービスの普及促進
- 重要インフラ等を守る高度セキュリティ人材の育成（中核人材育成プログラム）
- 日米欧によるインド太平洋地域向けの能力構築支援

サイバーセキュリティ お助け隊

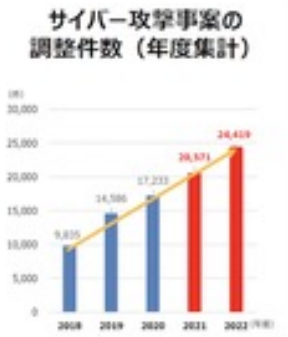
IPA 産業サイバーセキュリティセンター
Industrial Cyber Security Center of Excellence（ICSCoE）

②国際連携を意識した認証・評価制度等の立上げ

- IoT適合性評価制度の検討、国際制度調和に向けた調整
- SBOM（Software Bill of Materials）の活用促進
- QUAD上級サイバー会合、G7等を通じた各国間連携

③政府全体でのサイバーセキュリティ対応体制の強化

- 国境を越えて行われるサイバー攻撃へのJPCERT/CCの対処能力の向上
- 重要インフラ事業者等での事案発生時の初動支援を行うJ-CRATの体制強化
- 改正保安３法を踏まえた事故調査体制の構築
- サイバー攻撃技術情報の共有促進



④新たな攻撃を防ぎ、守るための研究開発の促進（サイバーセキュリティ産業振興）

- 先進的サイバー防御機能・分析能力の強化
- セキュリティ産業の成長加速化、製品/サービスの国内自給率向上に向けた政策検討

私たちの未来のために
RISKSENSOR.AI – FOR OUR FUTURE