AI駆動のセキュリティ自動検証デバイス「MUSHIKAGO」

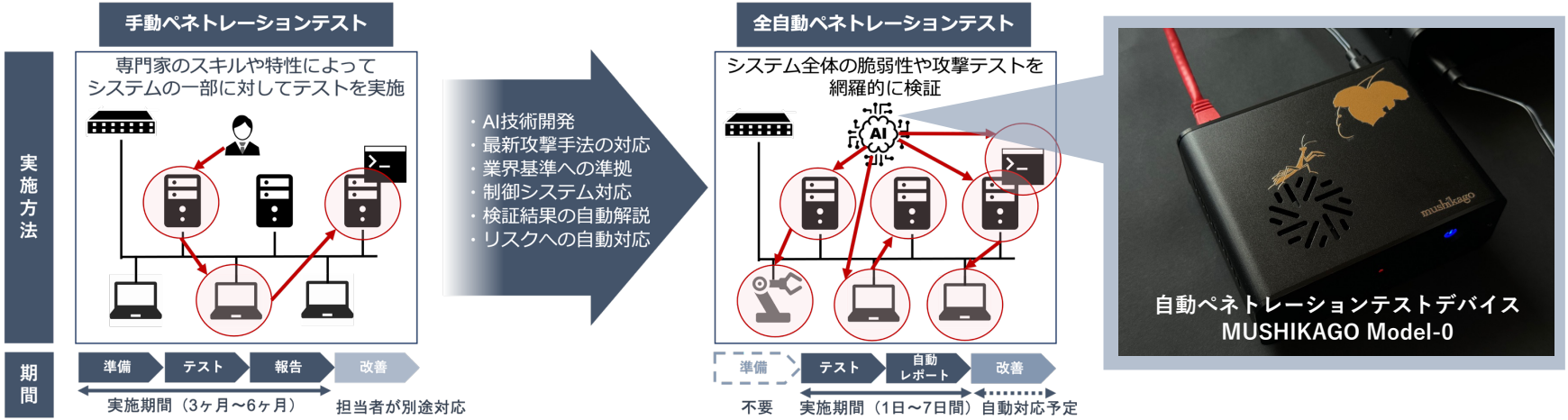
Powder Keg Technologies 株式会社
代表取締役　濱村将人

PowderKegTech

資料２

会社概要

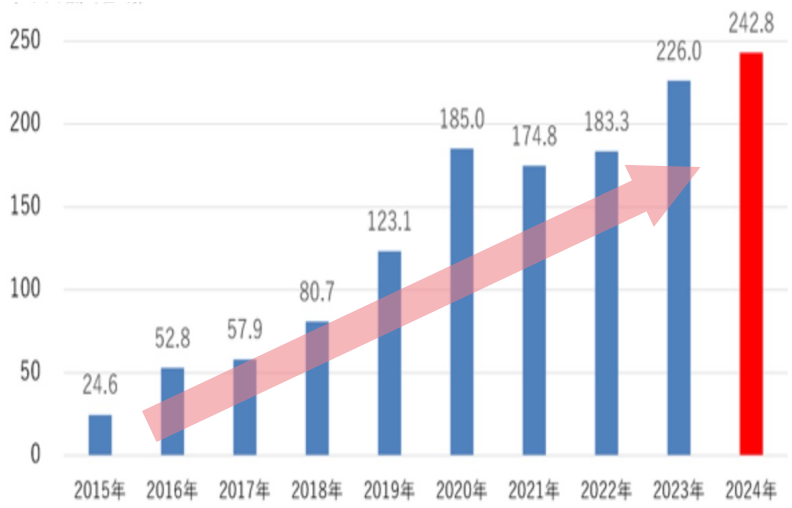
	Powder Keg Technologies 株式会社（東京都大田区蒲田）
設立	2021年9月（株式会社化 2023年6月）
資本金	2600万円（資本準備金含む）
代表	濱村 将人（はまむら まさと）
主要 研究実績	• 世界最大のセキュリティの国際会議 Black Hat USAにて研究発表（2021年,2022年） • NEDO 研究開発型ベンチャー支援（NEP）事業に採択（2021年） • JETROスタートアップアクセラレーションプログラムに採択（2022年） • 内閣府「経済安全保障重要技術育成プログラム（先進サイバー）」に採択（2024年）



Copyright © Powder Keg Technologies All Rights Reserved.

マーケットトレンド

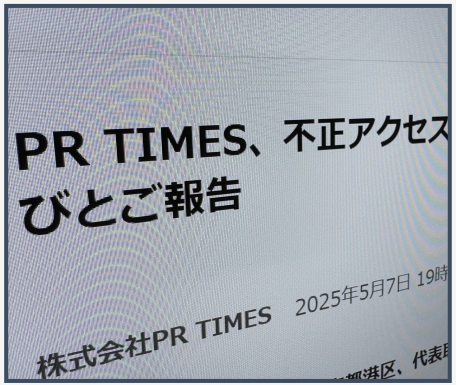
AIによるサイバー攻撃の高度化・攻撃数の増加



2025年に発生した国内被害事例

大手通信事業者（2025年4月）

被害：推定約 **400万件**



広報サービス企業（2025年5月）

被害規模：推定約 **90万件**

Copyright © Powder Keg Technologies All Rights Reserved.

現状の国内企業の対応

セキュリティ対策は、製品導入のみでは不十分。現状の可視化や検証が重要。

	現在の対応	課題
一般企業	セキュリティ対策製品の導入	・対策が**適切に機能しているか**分からない
先進企業	ホワイトハッカーによる検証	・テストが**属人的で網羅性に乏しい** ・実施範囲、期間が**スポットとなる**

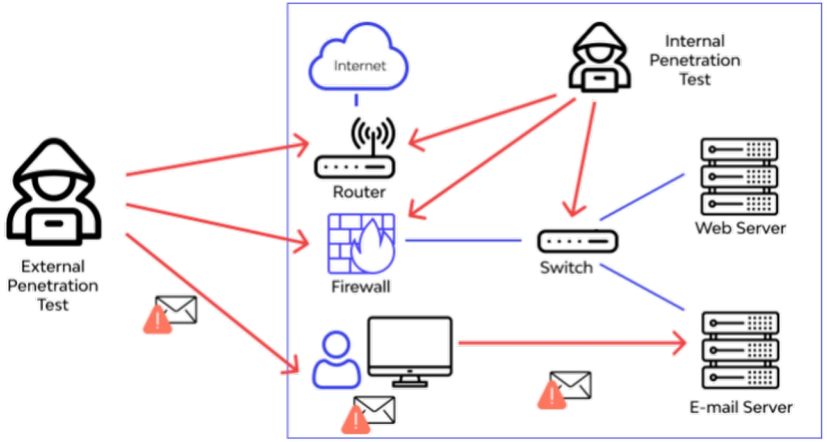
サイバーセキュリティ対策におけるPDCAサイクル

事案発生 → Plan（計画） → Do（対策導入） → Check（検証） → Action（修正）

Copyright © Powder Keg Technologies All Rights Reserved.

ペネトレーションテストとは？

実際のサイバー攻撃手法で、企業の対策の有効性を検証するテスト手法。



効果

- 既存対策の有効性把握
- ランサム感染時の想定被害の把握

課題

- 期間　（3ヶ月～6ヶ月）
- コスト（300万～数千万円/回）
- 属人性の高さ
- 網羅性の低さ

事前準備 → テスト実施 → 分析・報告 → 対策・改善

ペネトレーションテスト（約3ヶ月～6ヶ月）

Copyright © Powder Keg Technologies All Rights Reserved.

Product

専用デバイスを、オフィスなどのネットワークに接続するだけで、セキュリティリスクを自動検証する。

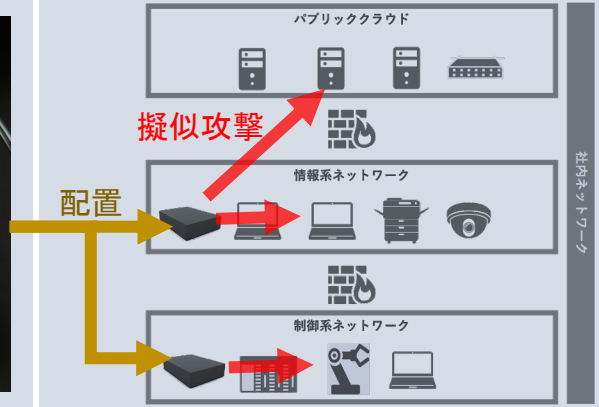
MUSHIKAGOとは

AIを利用したセキュリティ対策の自動検証デバイス

MUSHIKAGOの外観

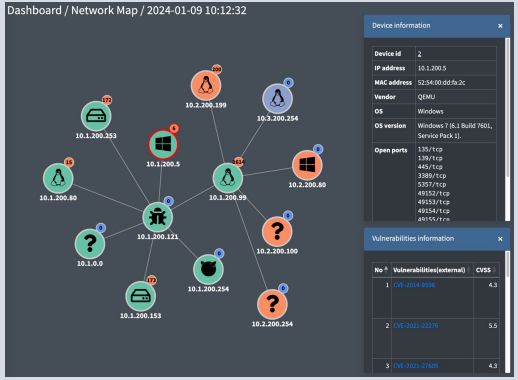
何をするのか

擬似的なサイバー攻撃を行うことで、社内のセキュリティ対策状況を検証



何ができるのか

社内端末の可視化、サイバー攻撃に遭った際の影響範囲の確認など

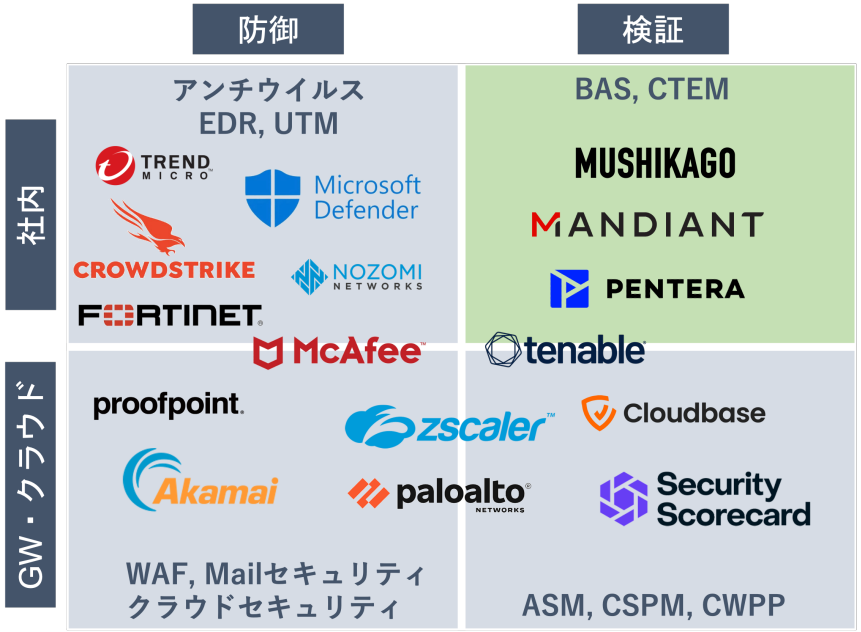


MUSHIKAGOの管理画面

Copyright © Powder Keg Technologies All Rights Reserved.

競合比較/優位性

国内にはAIで自動化できるプレイヤーは存在しない。海外競合製品はあるが、システムのみの提供で、初期設定に専門知識が必須。弊社ではハードウェアもセットで提供することでユーザ導入が圧倒的に簡単。



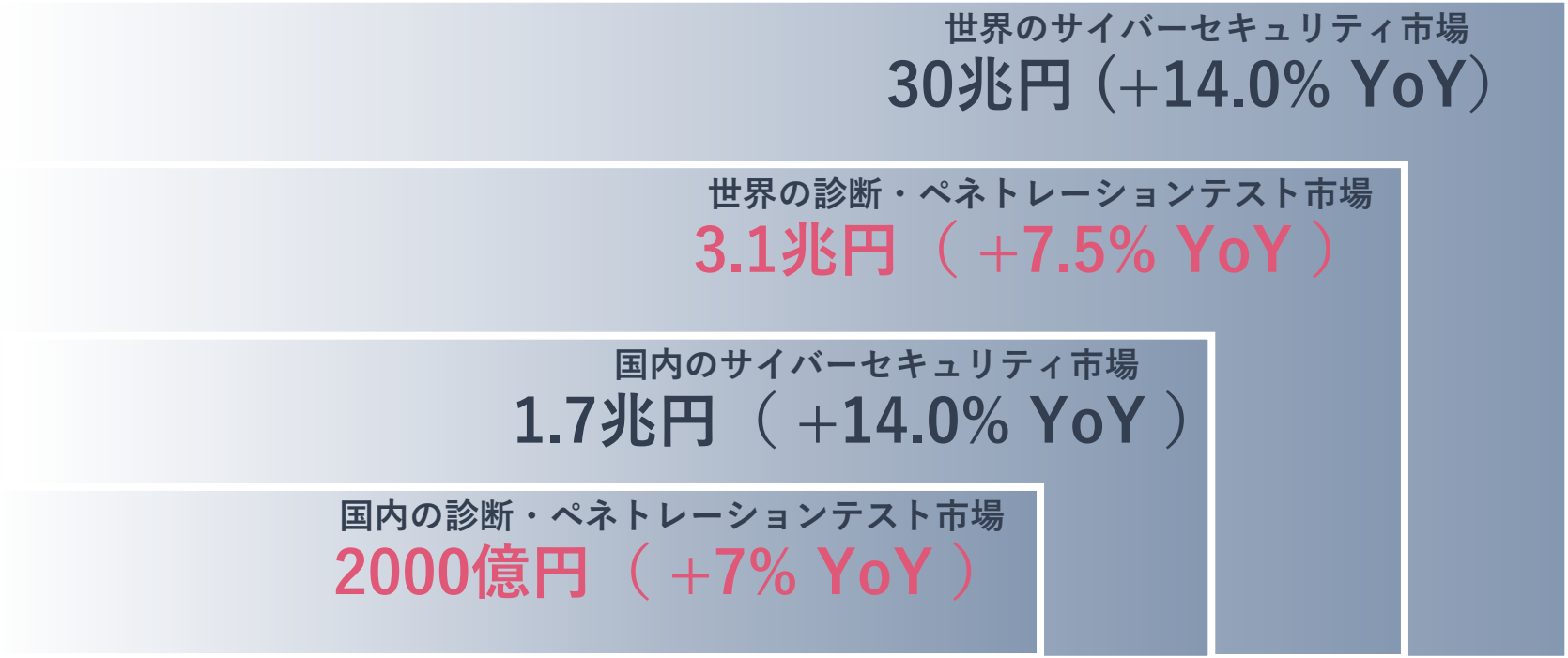
	MUSHIKAGO	MANDIANT	PENTERA
国	日本	米国	イスラエル
導入容易さ	◎	△	△
機能	○	◎	○
価格	¥¥	¥¥¥¥	¥¥¥

運用とセットで導入をすることで
導入の容易さを実現

Copyright © Powder Keg Technologies All Rights Reserved.

Market

サイバーセキュリティ市場及び診断市場は国内外で高い成長性が期待できる。

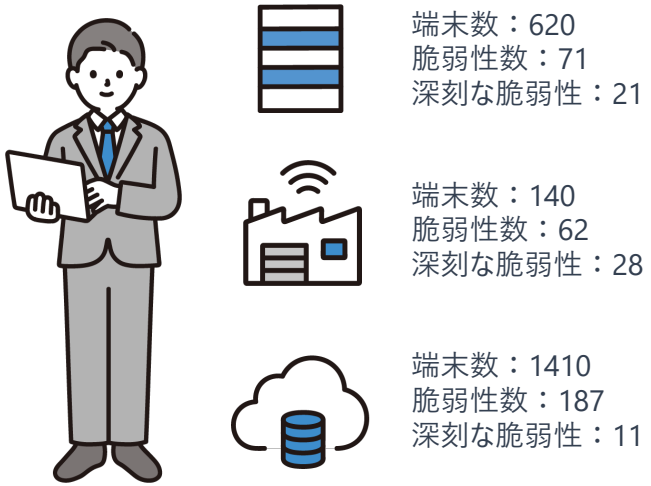


Copyright © Powder Keg Technologies All Rights Reserved.

検証に関する国内状況

Copyright © Powder Keg Technologies All Rights Reserved.

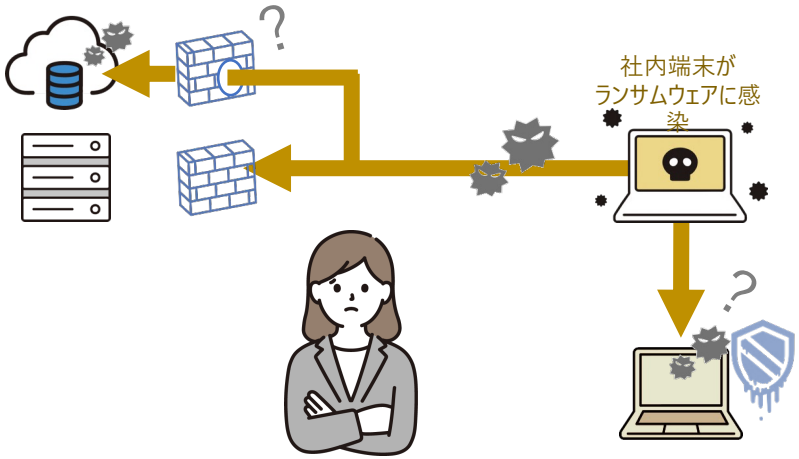
事例１　大手スーパーマーケット

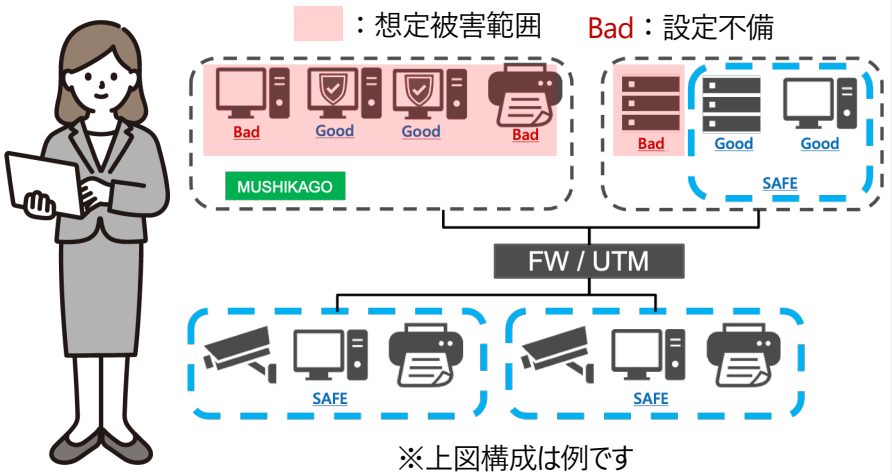
Before	After
・各拠点の端末数や脆弱性が把握できておらず、どのようなセキュリティリスクがあるのか分からない。 	・各拠点のデバイスが可視化され、端末数、脆弱性数、深刻なセキュリティリスクの有無等が簡単に把握できるようになった。  ※記載数値は例です

Copyright © Powder Keg Technologies All Rights Reserved.

事例２　金融系IT企業さま

Before	After
・社内のセキュリティ対策や設定が、適切に機能しているかわからない。 ・もしランサムウェアに感染したら、どこまで影響が出るかのか把握したい。	・MUSHIKAGOでペネトレーションテストを行うことで、導入対策の有効性や設定不備を把握できるようになった。 ・社内PCと同じ環境に繋いでテストを行うことで、ランサム感染発生時の想定被害範囲が把握できるようになった。



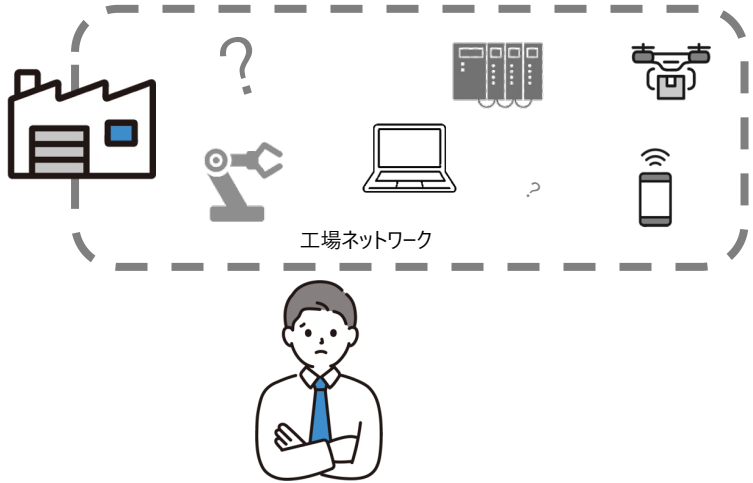


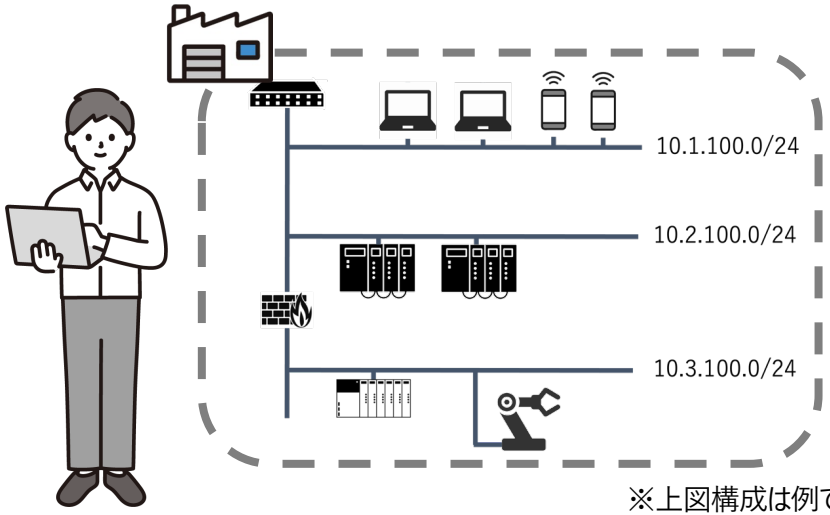
※上図構成は例です

Copyright © Powder Keg Technologies All Rights Reserved.

事例３　自動車部品工場さま

Before	After
・工場内のネットワークに何が接続されているのか把握できていない。 ・工場ネットワークへのセキュリティ対策を提案されているが、現時点でどの程度リスクがあるのか、必要最低限の対策は何なのか把握したい。	・MUSHIKAGOで工場ネットワークに接続された端末やIP体系を可視化でき、適切に管理できるようになった。 ・工場ネットワークの現状を正確に把握できるようになり、必要な対策や、設定が明確となった。

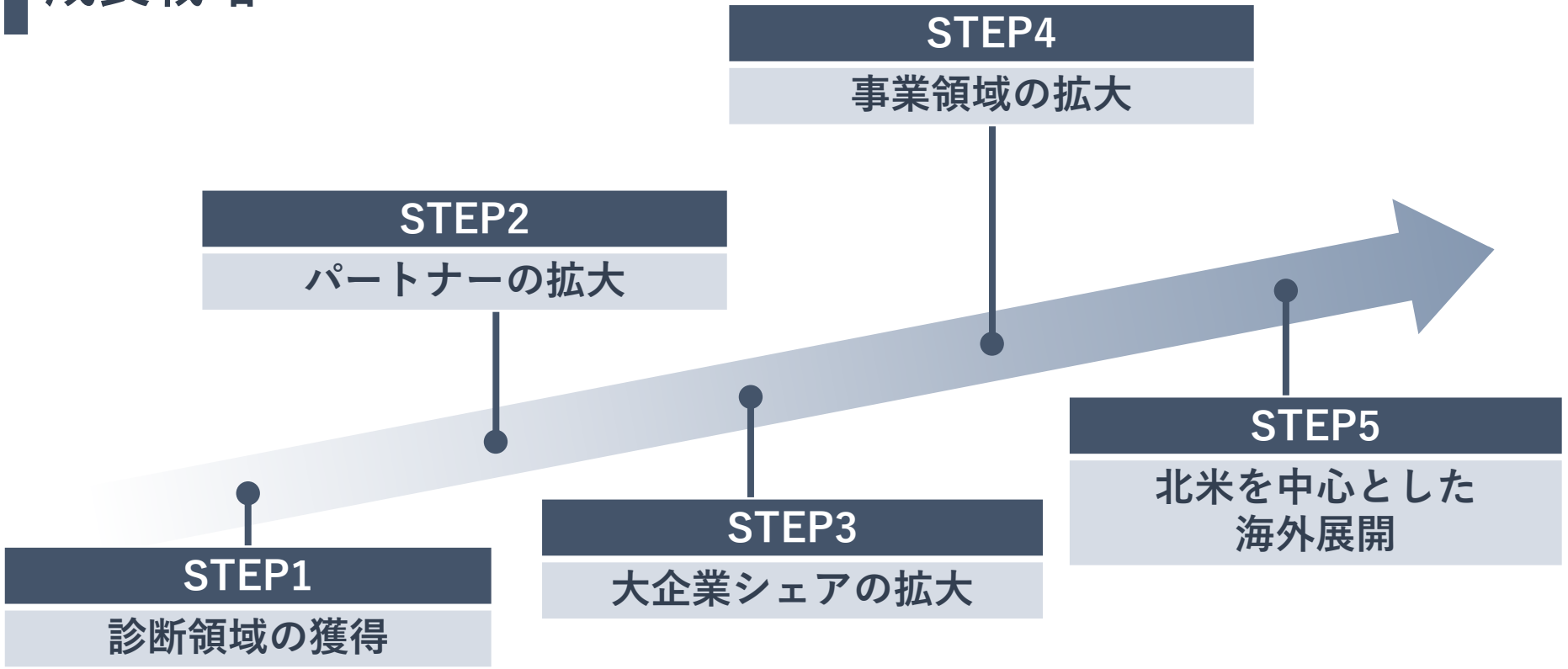




※上図構成は例です

Copyright © Powder Keg Technologies All Rights Reserved.

成長戦略



Copyright © Powder Keg Technologies All Rights Reserved.

海外展開戦略

サイバーセキュリティ製品はローカライズ不要。日本で実績を築いた後、積極的に海外展開を推進します。

Copyright © Powder Keg Technologies All Rights Reserved.

国産セキュリティ製品普及にあたっての課題と要望

課題

■ 実績重視の商習慣

国内の商習慣として、製品の採用判断が企業ブランドや過去実績に強く依存しているため、実績の乏しいスタートアップは導入が進みにくい。サイバーセキュリティ領域においては特に顕著であり、国内発の新興企業が参入・成長しにくい状況。

負の循環：

■ 海外依存の常態化

国産製品のシェアが低い領域では、積極的な投資や導入が滞り、スタートアップや国内企業が研究開発に取り組む機会が限られている。その結果、新しい選択肢が生まれにくく、海外製品の選択・導入が常態化し、国内シェアの多くを海外に依存する状況が続いている。

要望

■ 公共/防衛事業等での優先調達

行政機関や防衛関連の調達において、国産のセキュリティ製品や、先進技術を保有するスタートアップのサービスを、一定割合優先して調達することで、実績を確保する基盤を作ってほしい。

■ 研究開発支援

K Program（経済安全保証重要技術育成プログラム）のようなプロジェクトに、先進技術を保有するスタートアップも参画可能な仕組みを整えることで、市場が未発達の技術についても、積極的に研究開発に取り組むことが可能になる。

Copyright © Powder Keg Technologies All Rights Reserved.

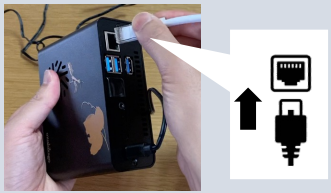
Appendix

Copyright © Powder Keg Technologies All Rights Reserved.

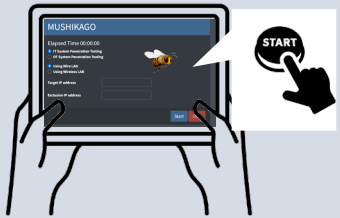
Appendix　製品利用のステップ

- 検査対象ネットワークに製品接続・IP アドレス設定を行うだけで、利用可能。
- IPでの疎通可能であれば、右図（1）-（4）横断的にテストすることが可能。

STEP1　設置・接続

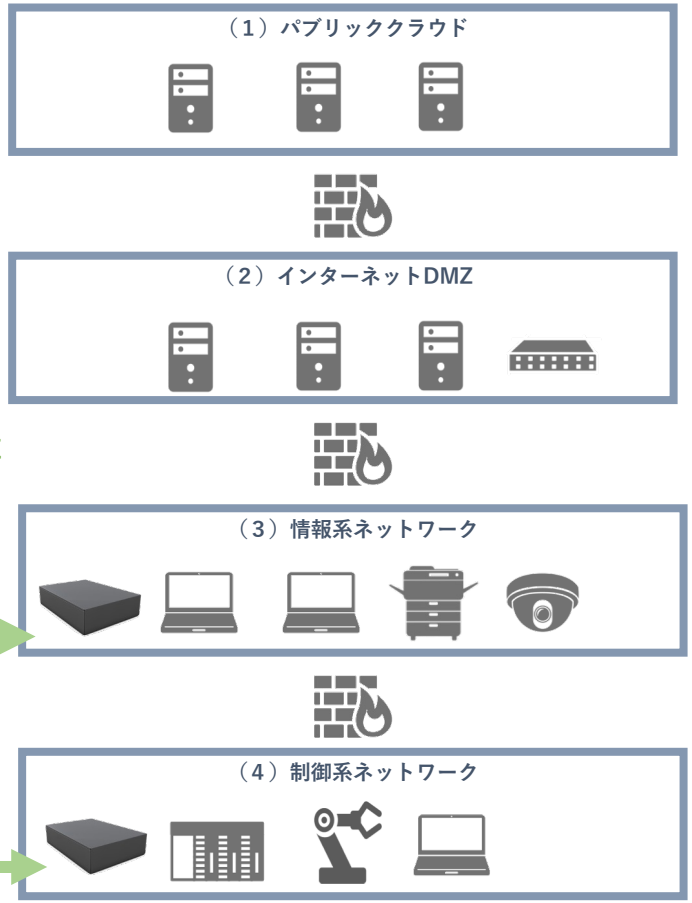


STEP2　設定・実行



STEP3　結果確認

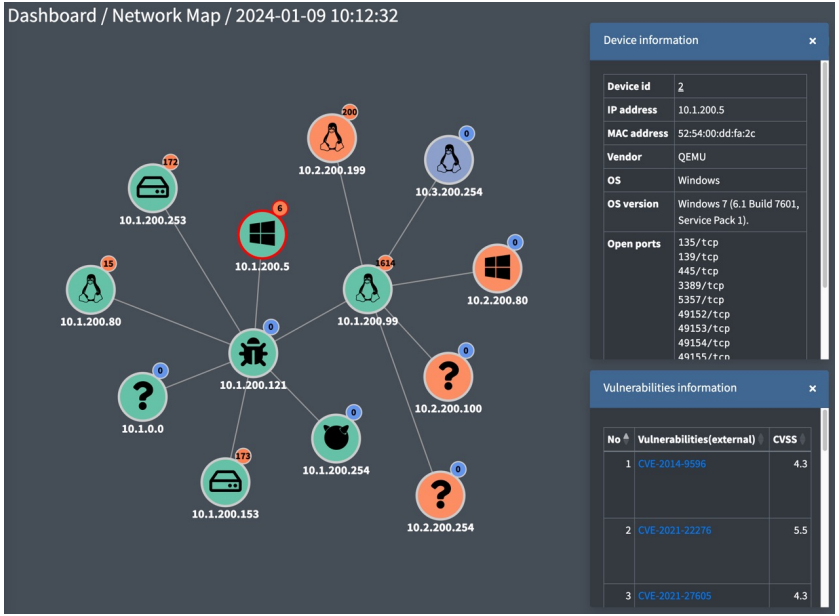
配置



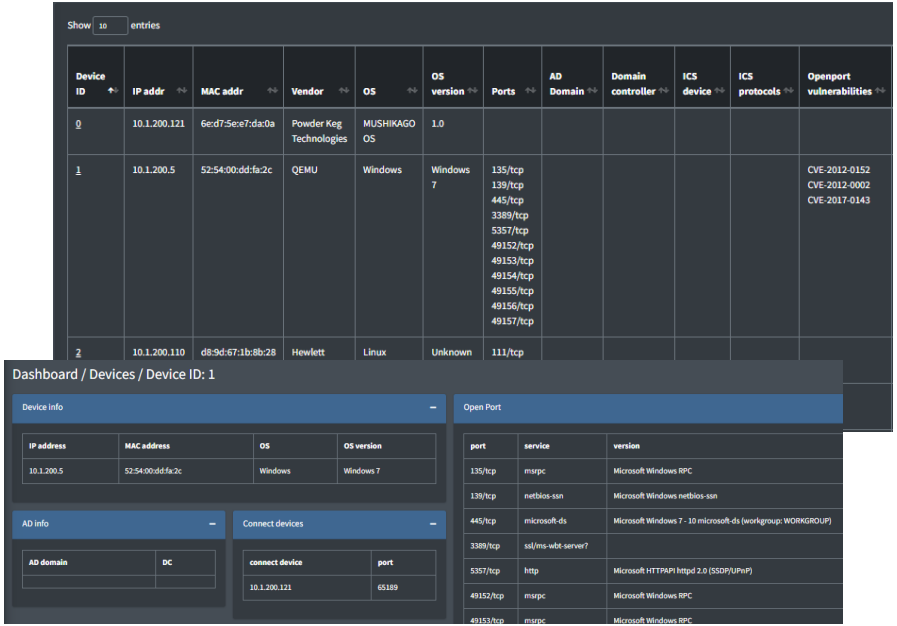
Copyright © Powder Keg Technologies All Rights Reserved.

Appendix デバイスの可視化画面

検出したデバイス情報の一覧や詳細をリアルタイムで確認可能。



ネットワークマップの表示



デバイスの一覧と詳細画面

Copyright © Powder Keg Technologies All Rights Reserved.

Appendix 自動レポート出力

検査内容・検査結果は、PDF,CSV形式でレポートとしてダウンロード可能

ペネトレーションレポート

脆弱性診断レポート

Copyright © Powder Keg Technologies All Rights Reserved.