

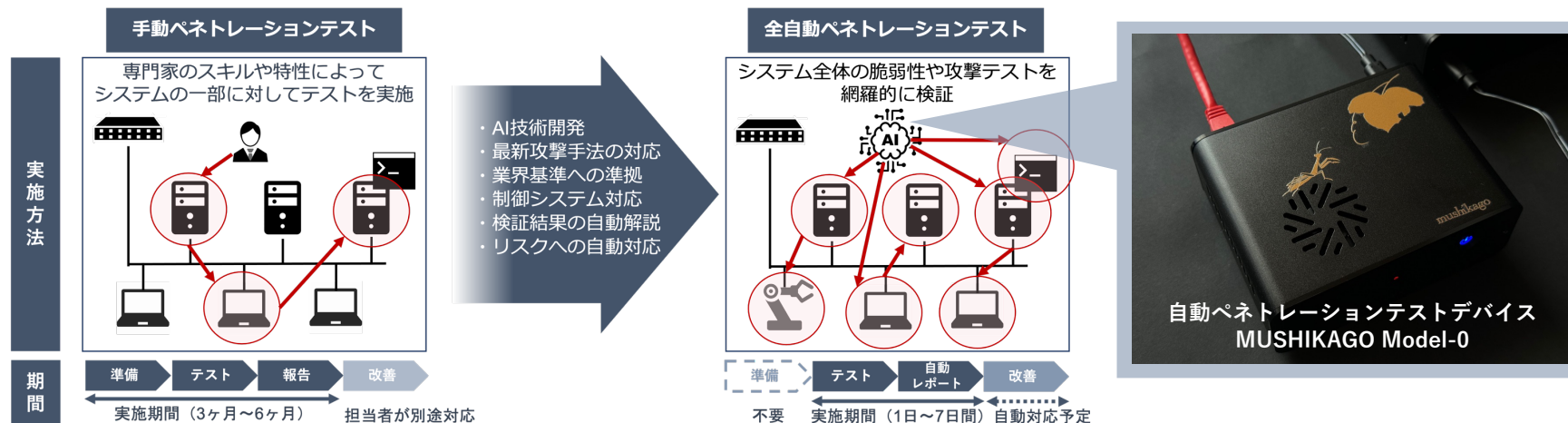
AI駆動のセキュリティ自動検証デバイス 「MUSHIKAGO」

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



会社概要

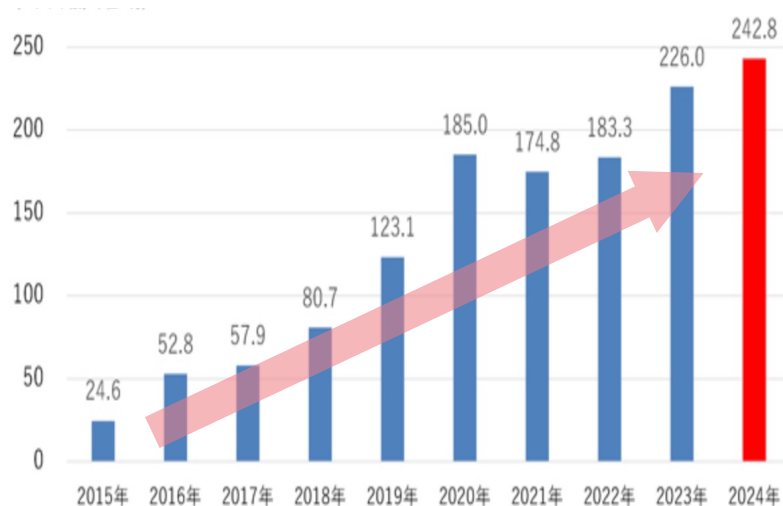
	Powder Keg Technologies 株式会社（東京都大田区蒲田）
設立	2021年9月（株式会社化 2023年6月）
資本金	2600万円（資本準備金含む）
代表	濱村 将人（はまむら まさと）
主要研究実績	- 世界最大のセキュリティの国際会議 Black Hat USAにて研究発表（2021年,2022年） - NEDO 研究開発型ベンチャー支援（NEP）事業に採択（2021年） - JETROスタートアップアクセラレーションプログラムに採択（2022年） - 内閣府「経済安全保障重要技術育成プログラム（先進サイバー）」に採択（2024年）



マーケットトレンド

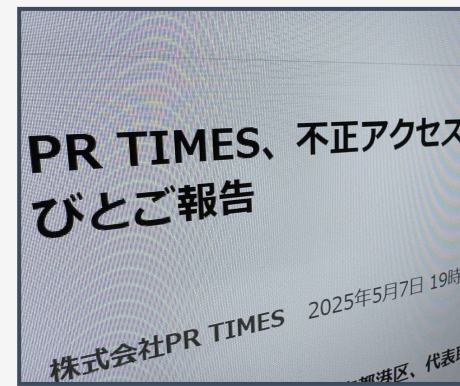
AIによるサイバー攻撃の高度化・攻撃数の増加

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**

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。

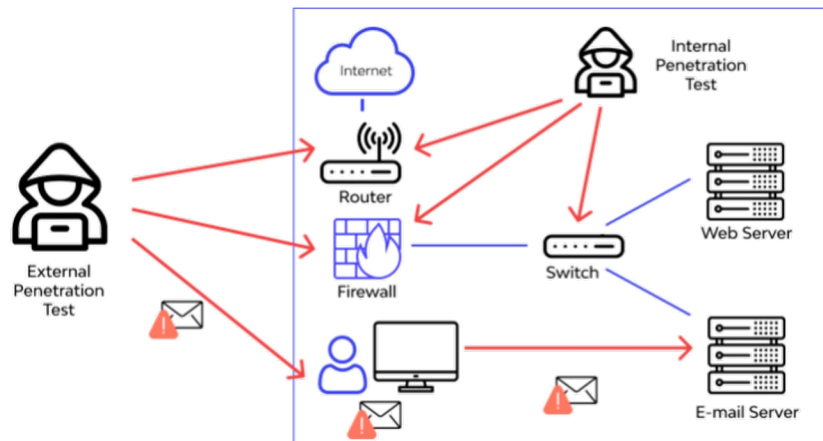
	現在の対応	課題
一般企業	セキュリティ対策製品の導入	・ 対策が 適切に機能している か分からない
先進企業	ホワイトハッカーによる検証	・ テストが 属人的で網羅性に乏しい ・ 実施範囲、期間が スポット となる

サイバーセキュリティ対策におけるPDCAサイクル



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)

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

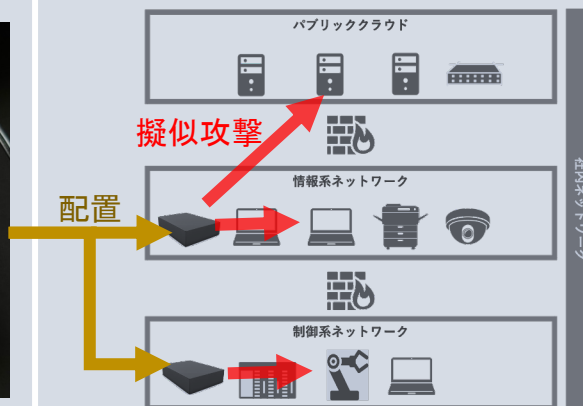
AIを利用したセキュリティ対策の自動検証デバイス



MUSHIKAGOの外観

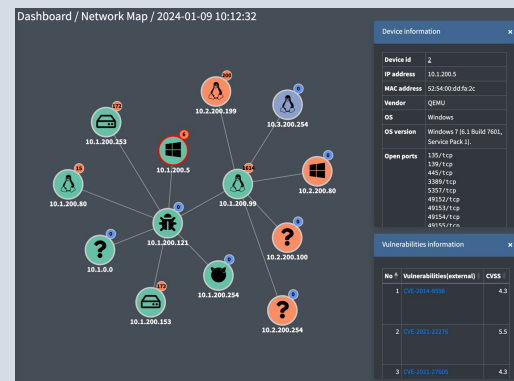
何をするのか

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

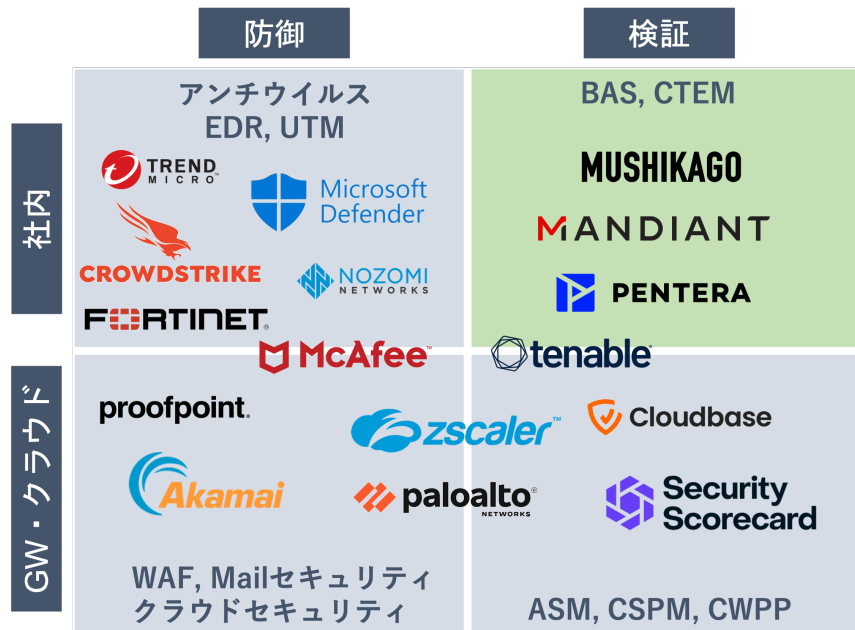
社内端末の可視化、サイバー攻撃に遭った際の影響範囲の確認など



MUSHIKAGOの管理画面

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

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。

世界のサイバーセキュリティ市場
30兆円 (+14.0% YoY)

世界の診断・ペネトレーションテスト市場
3.1兆円 (+7.5% YoY)

国内のサイバーセキュリティ市場
1.7兆円 (+14.0% YoY)

国内の診断・ペネトレーションテスト市場
2000億円 (+7% YoY)

検証に関する国内状況

検索

日本経済新聞

朝刊・夕刊 LIVE Myニュース 日経会社情報 人事ウオッチ NIKKEI

トップ 速報 ビジネス マーケット 経済 国際 オピニオン もっと見る

この記事は会員限定記事です 今月の閲覧：残り1本

金融庁、地銀に「疑似サイバー攻撃」 テストで対応力診断

経済 + フォローする

2024年10月8日 20:25 [会員限定記事]

保存

金融庁は金融機関にサイバー攻撃対策の強化を促す。2024事務年度（7月～25年6月）中に一部の地域金融機関に疑似的なサイバー攻撃を実施してセキュリティ体制を検証するテストを実施する。金融機関向けの新たな指針も策定し、業務委託先も含めた

読売新聞 オンライン 朝刊記事 紙面ビューアー 社説 English

三すべて | トップ 速報 社会 政治 経済 スポーツ 国際 地域 科学・IT エンタメ・文化 ライフ 受験・就活 ヘルプ

ホーム > ニュース > 政治

サイバー防御能力向上へ自治体に「ペネトレーションテスト」...総務省、来春にも

2024/11/18 15:00

スクラップに追加

総務省は、地方自治体のサイバー防御能力向上のため、自治体の情報システムに疑似的な攻撃を仕掛ける「ペネトレーションテスト（侵入テスト）」を来春にも行う。人口規模別に全国6程度のモデル自治体を選定し、結果や対応策を全国で共有する。

総務省は、地方自治体のサイバー防御能力向上のため、自治体の情報システムに疑似的な攻撃を仕掛ける「ペネトレーションテスト（侵入テスト）」を来春にも行う。人口規模別に全国6程度のモデル自治体を選定し、結果や対応策を全国で共有する。

侵入テストのイメージ

ハッカー役（セキュリティ事業者）

疑似サイバー攻撃（人口規模別に6自治体程度）

自治体システム

弱点や脆弱性の検証

総務省が結果を検証報告書・事例集作成

全国の自治体に共有へ

侵入テストは、個人情報の流出などで甚大な影響が予想される人口規模として、都道府県や政令市、中核市などを念頭に置いたモデル自治体で行う。対象自治体は、同省が意向を確認した上で抽出する方針で、政府が年内の成立を目指す2024年度補正予算案に関連経費を計上する方向で調整が進んでいる。

テストで判明したシステムの脆弱性などの知見は、報告書や事例集などにまとめることを想定しており、小規模自治体を含めた全国の自治体の対応力の底上げを図りたい考えだ。

情報システムの強化には、組織内部での自己診断や、外部による侵入テストなどの点検を繰り返すことが不可欠だが、地方自治体では人材や予算が慢性的に不足している。同省によると、昨年4月時点で情報セキュリティに関する内部・外部の審査を実施した自治体の割合は、都道府県

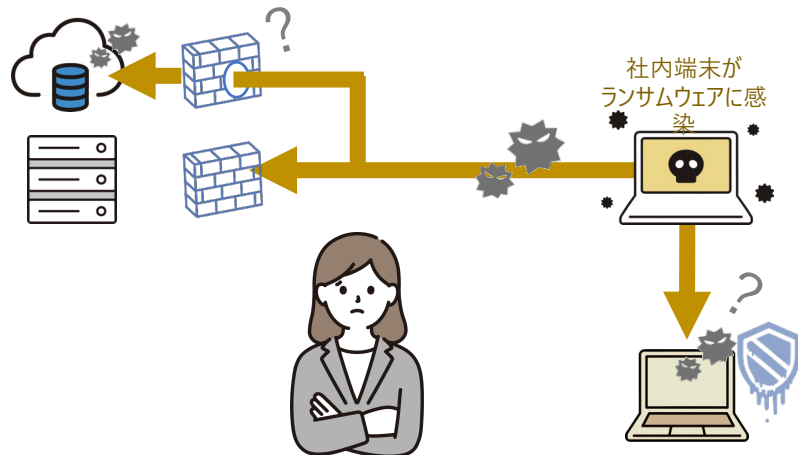
事例 1 大手スーパーマーケット

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。   端末数：620 脆弱性数：71 深刻な脆弱性：21  端末数：140 脆弱性数：62 深刻な脆弱性：28  端末数：1410 脆弱性数：187 深刻な脆弱性：11 ※記載数値は例です

事例 2 金融系IT企業さま

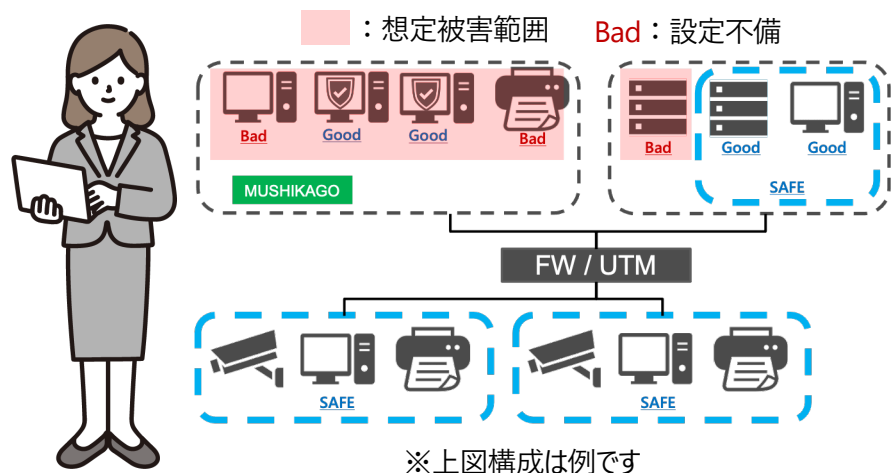
Before

- ・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のか把握したい。



After

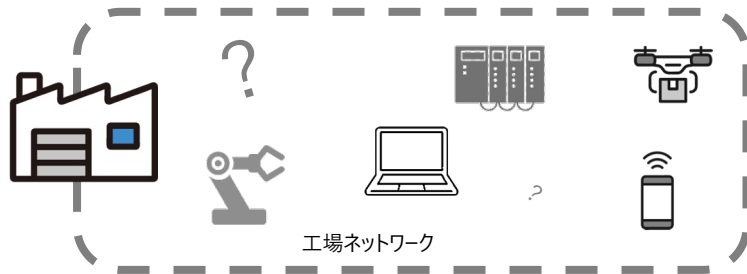
- ・MUSHIKAGOでペネトレーションテストを行うことで、導入対策の有効性や設定不備を把握できるようになった。
- ・社内PCと同じ環境に繋いでテストを行うことで、ランサム感染発生時の想定被害範囲が把握できるようになった。



事例 3 自動車部品工場さま

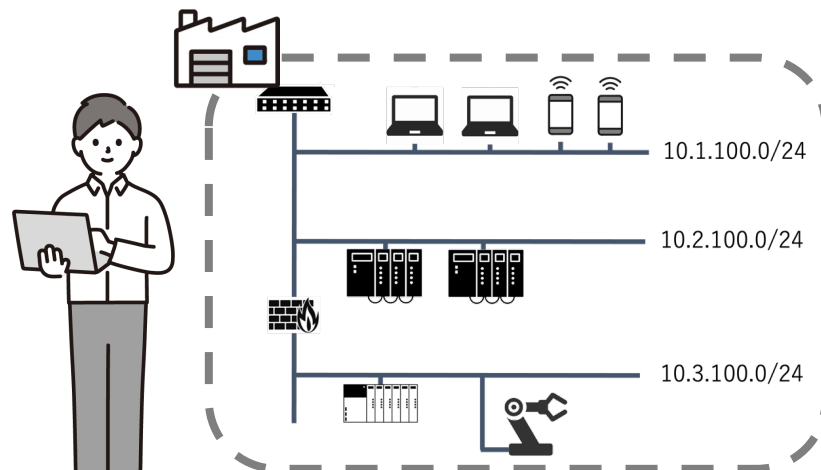
Before

- ・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。



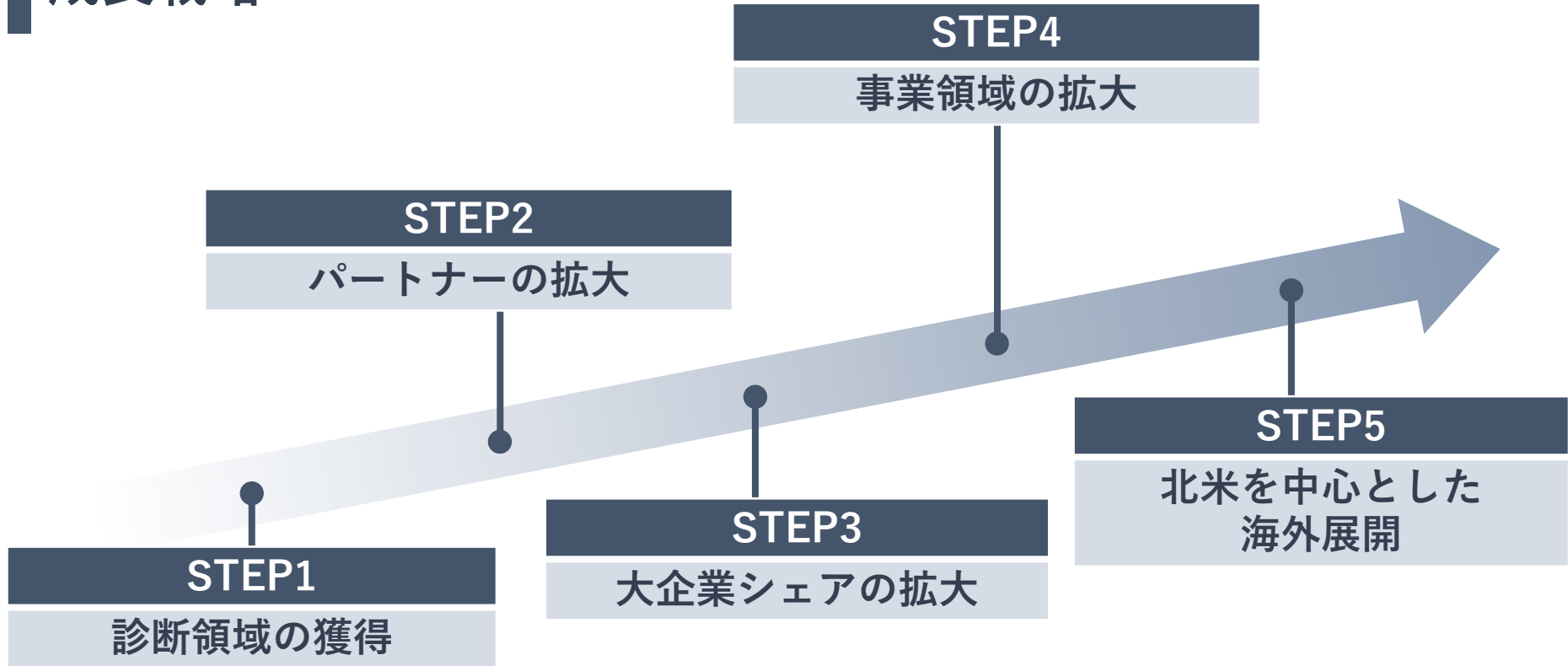
After

- ・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

成長戦略



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。



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してほしい。

■ 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 of 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。

Appendix

Appendix 製品利用のステップ

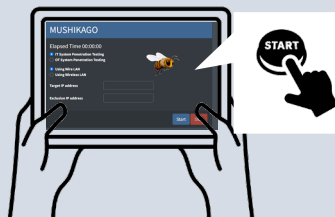
- 検査対象ネットワークに製品接続・IP アドレス設定を行うだけで、利用可能。
- IPでの疎通可能であれば、右図（１） - （４）横断的にテストすることが可能。

STEP1 設置・接続



配置

STEP2 設定・実行



STEP3 結果確認



（１）パブリッククラウド



（２）インターネットDMZ



（３）情報系ネットワーク

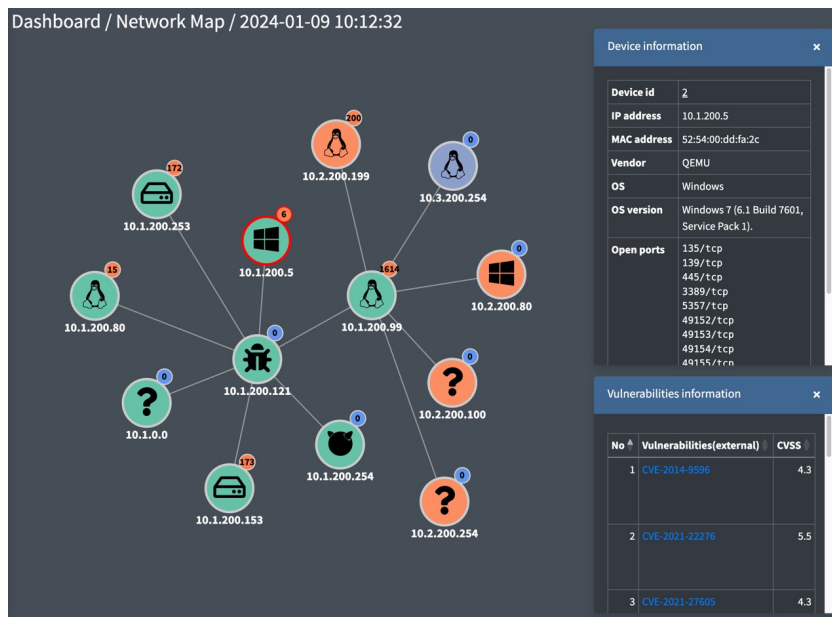


（４）制御系ネットワーク



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

Show 10 entries

Device ID	IP addr	MAC addr	Vendor	OS	OS version	Ports	AD Domain	Domain controller	ICS device	ICS protocols	Openport vulnerabilities
0	10.1.200.121	6e:d7:5ee7:da:0a	Powder Keg Technologies	MUSHIKAGO OS	1.0						
1	10.1.200.5	52:54:00:dd:fa:2c	QEMU	Windows	Windows 7	135/tcp 139/tcp 445/tcp 3389/tcp 5357/tcp 49152/tcp 49153/tcp 49154/tcp 49155/tcp 49156/tcp 49157/tcp				CVE-2012-0152 CVE-2012-0002 CVE-2017-0143	
2	10.1.200.110	d8:9d:67:1b:8b:28	Hewlett	Linux	Unknown	111/tcp					

Dashboard / Devices / Device ID: 1

Device info

IP address	MAC address	OS	OS version
10.1.200.5	52:54:00:dd:fa:2c	Windows	Windows 7

AD info

AD domain	DC

Connect devices

connect device	port
10.1.200.121	65189

Open Port

port	service	version
135/tcp	mrpc	Microsoft Windows RPC
139/tcp	netbios-ssn	Microsoft Windows netbios-ssn
445/tcp	microsoft-ds	Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
3389/tcp	sslmis-wait-server?	
5357/tcp	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp	mrpc	Microsoft Windows RPC
49153/tcp	mrpc	Microsoft Windows RPC

デバイスの一覧と詳細画面

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