IBC アイビーシー株式会社

製造業様向け

工場内IT機器のあるべき監視

製造業DXの最適解

スマートファクトリーを実現する工場内IT機器のあるべき監視

製造業DXは、**ネットワーク**と**セキュリティ**が成功のカギ！

日本の製造業は、海外企業と比べてデジタル化が非常に遅れています。また、国内投資が増加する一方で、日本の大手製造業は海外での売上比率を伸ばし続け、現地法人に依存する傾向があります。このような背景から、経済産業省はDX（デジタルトランスフォーメーション）による製造機能の最適化と事業機会の拡大を目指し、**「ものづくりDX」「製造業DX」**を推進しています。

製造業のDXにおいて、その目指す姿として以下の3つが挙げられます：

・スマートファクトリー
・スマートプロダクト
・スマートサービス

まず実現すべき第一優先として、製造業の本命ともいえる**「スマートファクトリー」**があります。これは、データ活用による全体プロセスの最適化や、あらゆる生産工程の見える化を通じて工場生産の生産性向上を図るものです。

これまで工場内で完結していた機器・装置・設備（OT）の情報をネットワークで繋ぎ、そこから取得できる稼働・運用・品質などのデータを活用することで、低コスト・生産性向上・高品質化を目指すことが急務となっています。この「スマートファクトリー」を実現するためには、工場にある生産設備を制御するシステムと、本社の基幹システムを接続する**ネットワークがシームレスに繋がること**が重要です。

しかし、多くの製造現場ではそのネットワークに大きな課題があります。OT側のネットワークは、これまで外部と接続することを意識して設計されていなかったり、工場内を繋ぐネットワーク機器が購入時のままアップデートされていなかったりします。そのため、IT系のネットワークと接続する際にはセキュリティにも細心の注意を払わなければなりません。OTセキュリティの脅威の一つとして、**「外部ネットワーク経由のサイバー攻撃」**が最も大きな脅威とされています。

これらの脅威から自社を守り、シームレスなネットワーク接続を実現するためには、以下の対策が考えられます。

必須

- 境界分離＆一元管理
- 可視化＆監視

ネットワークインテグレーション
監視ツールの導入

やるべき

- ◎脆弱性管理
- ◎傾向把握
  ＆キャパシティ管理

脆弱性管理ツールの導入
分析型監視ツールの導入

安心

- ○データ分析
  ＆セキュリティ分析
- ○未知の脅威への対策

将来予測監視、リスク分析の実施
セキュリティ調査の実施

これらの対策の大きな課題とキーポイントとなるのが、
ネットワークと**セキュリティ**です。
それでは、これらの課題解決のためにはどうしたら良いでしょうか？

①-1 ネットワークの性能監視

必須

工場内と本社の情報系を繋ぐネットワーク。これらを一元管理し、ネットワーク全体の把握・管理に優れているのが、**System Answer G3** です。
System Answer シリーズは、アイビーシーが自社開発している**国産ソフトウェア**です。日本語UIで分かりやすく、直感的な操作ができ、自社エンジニアによるサポート（電話・メール対応）付ですので、専門的な知識がなくてもご活用いただけます！

なぜ System Answer G3 が選ばれるのか　～3つの強み～

検知から予防へ

一般的な監視システムは、異常の発生を**検知**し、調査や原因分析を行い、障害の迅速な対応を図る役割です。
System Answer では、監視で得た情報を自動分析することで**「将来予測」**を行い、**障害を予防**するための機能を実装しています。

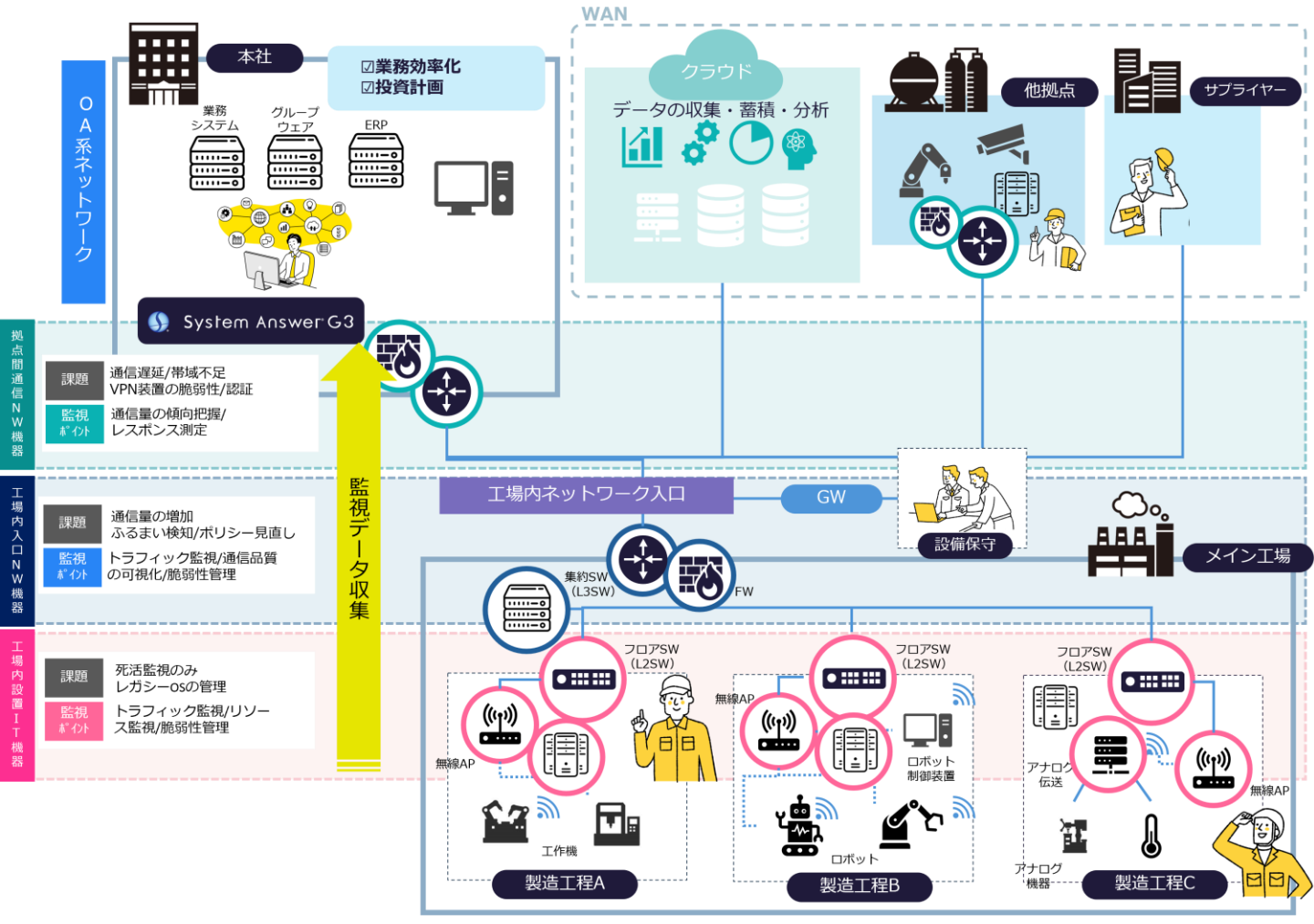
安定稼働を促進

IBCが20年間培った性能分析ノウハウを機能化した**「トラブルシューティングアシスタント」**が備わっており、お客様の障害復旧対応をサポートします。また、**「ダイナミックブックマーク（相関分析）」**をご活用いただくことで、潜在的な障害リスクの把握とその早期対策を実現します。

カスタマーサクセス

運用現場で**「本当に役立つ」**製品の開発を追及することが我々の誇りであり、プライドです。System Answer の**利活用支援**はもちろんのこと、お客様のシステム運用課題を解決する付加価値サービスをワンストップで提供しています。お客様に寄り添ったサービスを通し、システム運用業務の「成功」をサポートします。

【製造業での監視ポイント】



運用担当者も絶賛！

工場内でIT運用を始めるにあたり、「ITにはあまり詳しくない」という不安のある方にも、System Answer G3 は安心してご利用いただけます。

簡単導入	難しい監視設定も、豊富な監視テンプレートで自動登録が可能です。 また、安心の国内電話サポートも付随していますので、専門的な知識がなくてもすぐにご活用いただけます！
直感的な操作	System Answer G3 は当社が自社開発している国産ソフトウェアです。分かりやすい日本語のGUI（操作画面）で、説明書をイチから読まなくても直感的に操作いただけます！
評価レポート	当社独自の性能評価基準により、監視データをアップロードするだけで、監視項目の性能をA～Dランクで自動評価！評価結果をレポート出力できますので、工数をかけずに運用が可能です！

System Answer G3 を活用した 製造業の課題別解決策

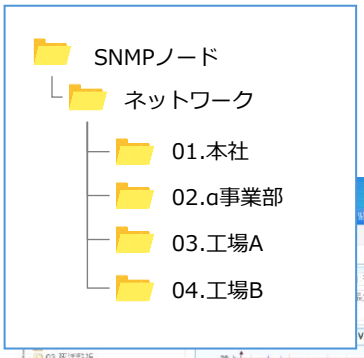
製造業ならではのいま起きている事象・悩みも System Answer G3 で即解決！

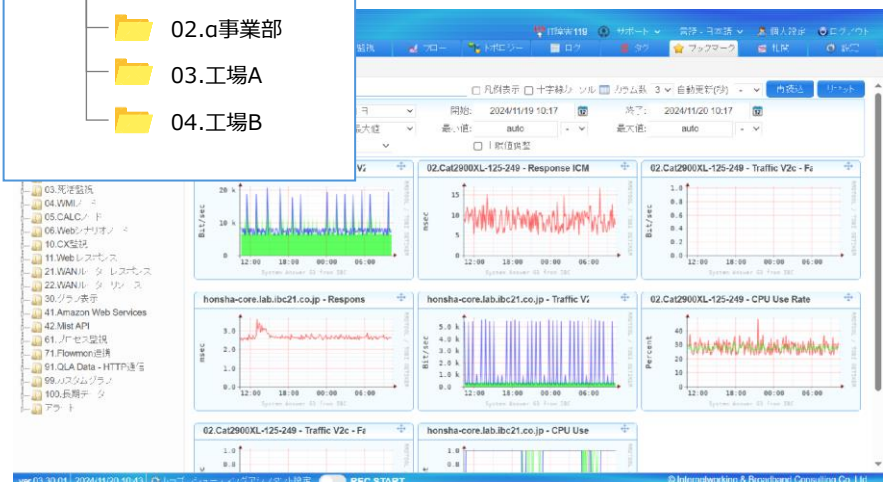
管理が分散

CADシステム、工程管理システムなどの基幹システムのほか、業務システムも乱立し、工場毎、本社管轄など、管理方法の違いから有事の際の切り分けが困難…

ブックマーク機能で、関連機器を横並びで分析したり、基盤環境の特性に応じて監視画面をカスタマイズし、重要拠点のトラフィック状況を1ページに集約して監視することで、一元管理が可能。
今まで時間も工数もかかっていた障害の切り分けも即時対応！

一元管理で工場拠点を含む
ネットワーク全体の把握





ボトルネックの把握

海外も含め拠点数が多く管理ができておらず、障害が起こっても、各拠点のどこがボトルネックになっているのかわからない…

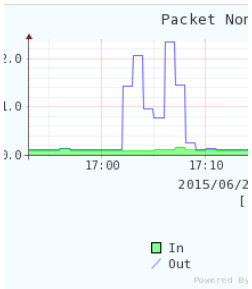
国内⇔国外、国内⇔国内の品質状況（トラフィック量やレスポンス状況）を一括管理し、ボトルネック個所を直ちに特定！
製造業特有の比較的大きく、特定時間に集中するパケット（CAD・工程管理システム）の数量を収集し周期性を把握することで、レスポンスの維持・向上に有効活用することができた。

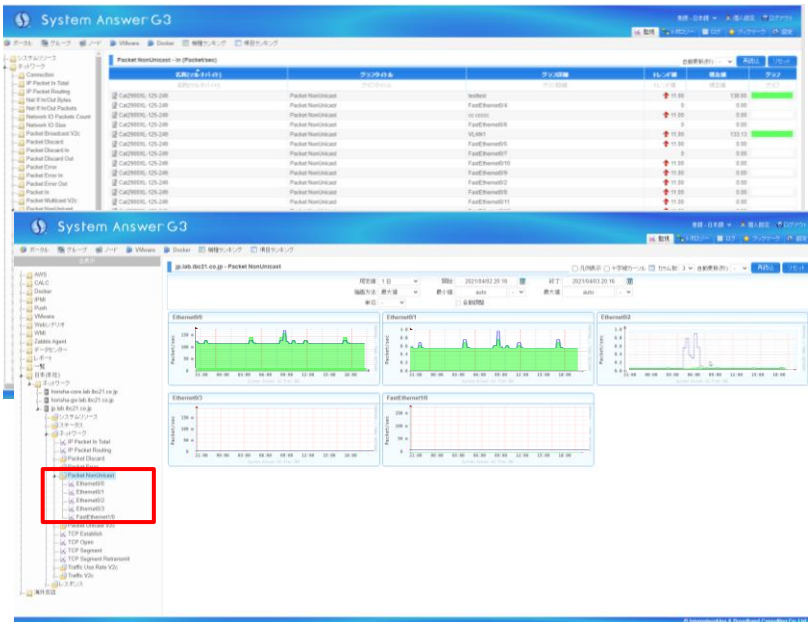
多拠点監視をリモートで実施

障害の検知からボトルネックの特定までを、現場まで行かずリモートで実施可能！

（障害検知～処置までの実例）

①障害検知（アラートメール）
↓
②G3 の管理画面から事象を確認
↓
③画面上からどのインターフェイスでリンクアップしているのかを確認
↓
④現場担当者へL3スイッチの抜線を指示
↓
⑤処置実施
↓
的確かつ早い指示で被害を最小限に抑えることができた





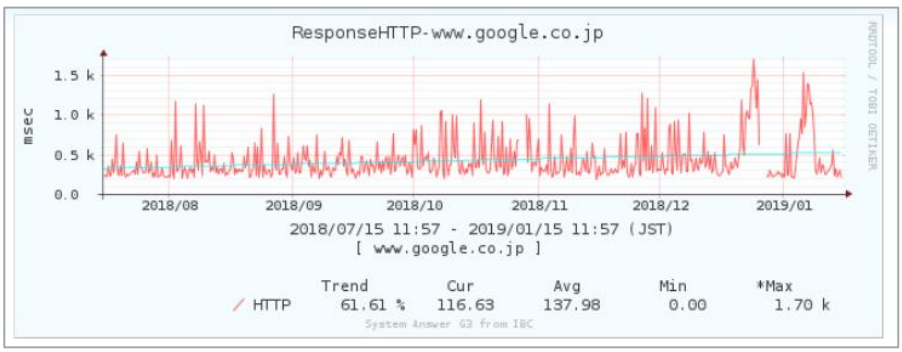
キャパシティ管理

工場の特性から各拠点現場から同時刻に一斉にアクセスが集中するときがあり、度々遅延が発生しており、最大負荷を想定した設備投資ができていない

ピーク時（始業時間、新たな生産ラインの稼働）の性能データも詳細かつ長期的に収集可能なため、将来的にどれぐらいのキャパシティが必要なのかといった分析ができ、ピーク時にも品質を落とすことのない最適で必要最低限の設備投資を実現。
最適なキャパシティ管理を行うことにより、現場の作業を第一優先としたシステム運用が可能。

分析ができる監視

5年分のデータを非圧縮で保存しているため、過去の傾向から、表示期間における増加率や減少率をグラフ上に傾向線を描画できます。
「将来的にいつ頃リソースが足りなくなるのか？」
「高負荷がかかるタイミングはいつなのか？」
といった運用上知りたかった情報が、ツール上で確認できます。
過度にもならず、不足もしない、適切な設備投資計画ができ、経営判断にも役立ちます！



①-2 スマートファクトリーのネットワーク監視ポイント

本社・工場内のIT系ネットワーク全体を性能監視することで、ネットワーク全体の負荷状況の可視化ができます。

現状把握に基づく負荷予測

工場毎やライン毎の傾向把握が可能です。
今後、人数や機器数が増加した際、セッション数がどれぐらい増加するのかを予測できるため、事業計画に則した設備投資ができます。

本社
従業員数
150人

大阪工場
従業員数
100人

名古屋工場
従業員数
50人

導入事例Check

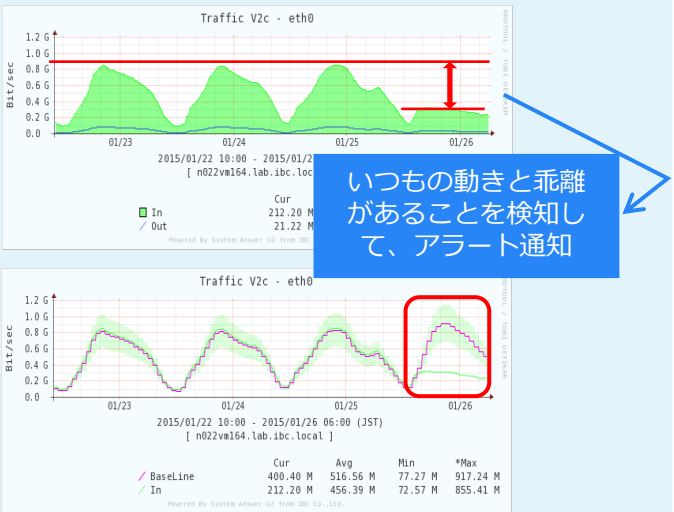
株式会社荏原製作所様

仮想環境の的確な利用状況把握により、適切なキャパシティプランニングを実現～ 利用率が低い仮想サーバーを洗い出し、余剰投資を回避 ～

「いつもと違う」サイレント障害検知

ベースライン監視にて、しきい値内でも、「トラフィックの傾向がいつもと異なる」ことを検知→アラート発報できます。

例えば、冗長構成の片側のルーターが不安定となっており、冗長構成が正常に機能していなかったことが判明することで、工場のライン停止などの障害が起きる前に検知→解決することができ、トラブルの事前回避に繋がります。
ネットワーク障害のために、生命線であるラインを止めることのない運用を実現します！



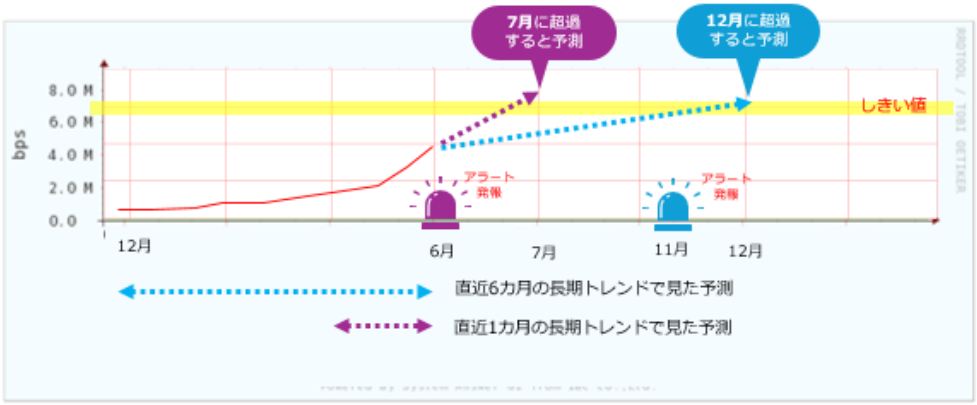
更に！ 将来を予測する監視

System Answer G3 の将来予測オプションで現状の把握、過去の履歴（ログ）だけでなく、将来を予測する監視ができます。

キャパシティ予知

障害は予知して対処する時代へ

将来、リソースが最大値やしきい値を超える状況を検知し、アラート通知をします。
障害が起きる前に「○カ月後にしきい値を超える！」とアラートを出してくれるため、将来来る障害のために予め対策を打ち、障害を未然に防ぐことができます。
System Answer G3 の将来予測オプションで**止めないラインを実現**することができます！



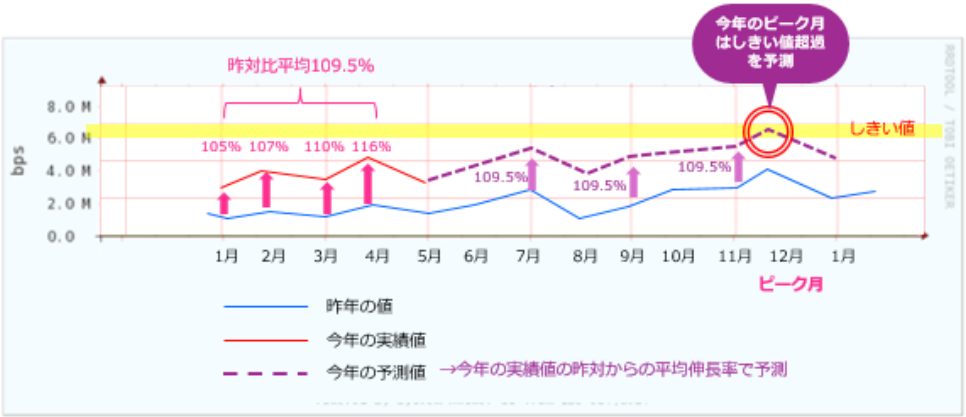
◆1 か月、3 か月、6 か月、1 年のトレンド値をもとに将来予測をおこないます。
◆最短 1 日からお客様指定の任意の期間を指定して、トレンド値をもとに将来予測をおこなえます。
◆しきい値を超えそうな、1 年前 / 6 か月前 / 3 か月前 / 1 か月前にアラートを通知します。

長期間のトレンド変化だけでなく、新システムのリリースや働き方の変化による短期間のトレンド変化にも柔軟に対応。サンプリング期間（短期・中期・長期）は任意に設定可能。

昨対比較

もうピーク時も怖くない

昨年の月別の実績値と今年の経過月の昨対平均倍率を算出し、掛け合わせることにより、将来月の予測値を算出します。この予測値がしきい値を超過する際に、アラートを通知します。ピーク月には24365体制で**疲弊していた運用から解放**されます！



◆ 過去の対象データの開始月はお客様が任意に設定し、そこから 12 ヵ月を昨年分として計算します。
◆ 月別の実績値として、最大値 / 平均値のどちらを利用するか任意に選択可能です。
◆ 今年のピークを乗り切れるかどうか、早期に的確に判断することができます。
◆ バッチ処理アラートとして月初に 1 回通知します。

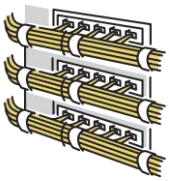
①-3工場内無線環境の高品質化に向けて

安心

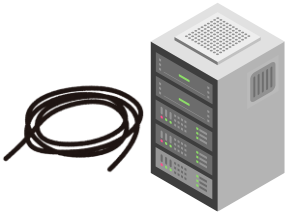
スマートファクトリー化に伴い、工場内には今後も無線の普及が予測されます。
工場内無線化の普及状況は、経済産業省の調査結果によると、従業員規模が大きい企業ほど積極的な傾向にあるようです。

無線化のメリット

ケーブル配線を最小限に！



機材配置の自由度



AGVなどモビリティの活用

無線化の課題

セキュリティ

コストの不透明感

安定/信頼/安全性

干渉に依る問題

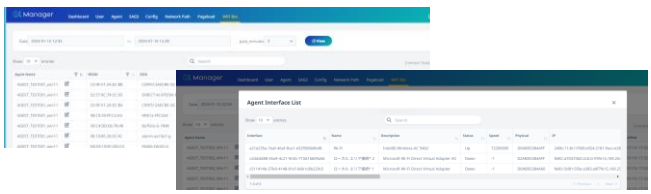
有線も無線も含め全てのネットワークを一元化し、柔軟に管理・運用していくことが必要

スマート工場化の進展に伴い、ネットワークを使用する機器が増加するため、工場全体を見据えたネットワーク環境の再整備が必要

System Answer G3 の **CX監視オプション**で、工場内無線環境もユーザー目線でモニタリングできます！

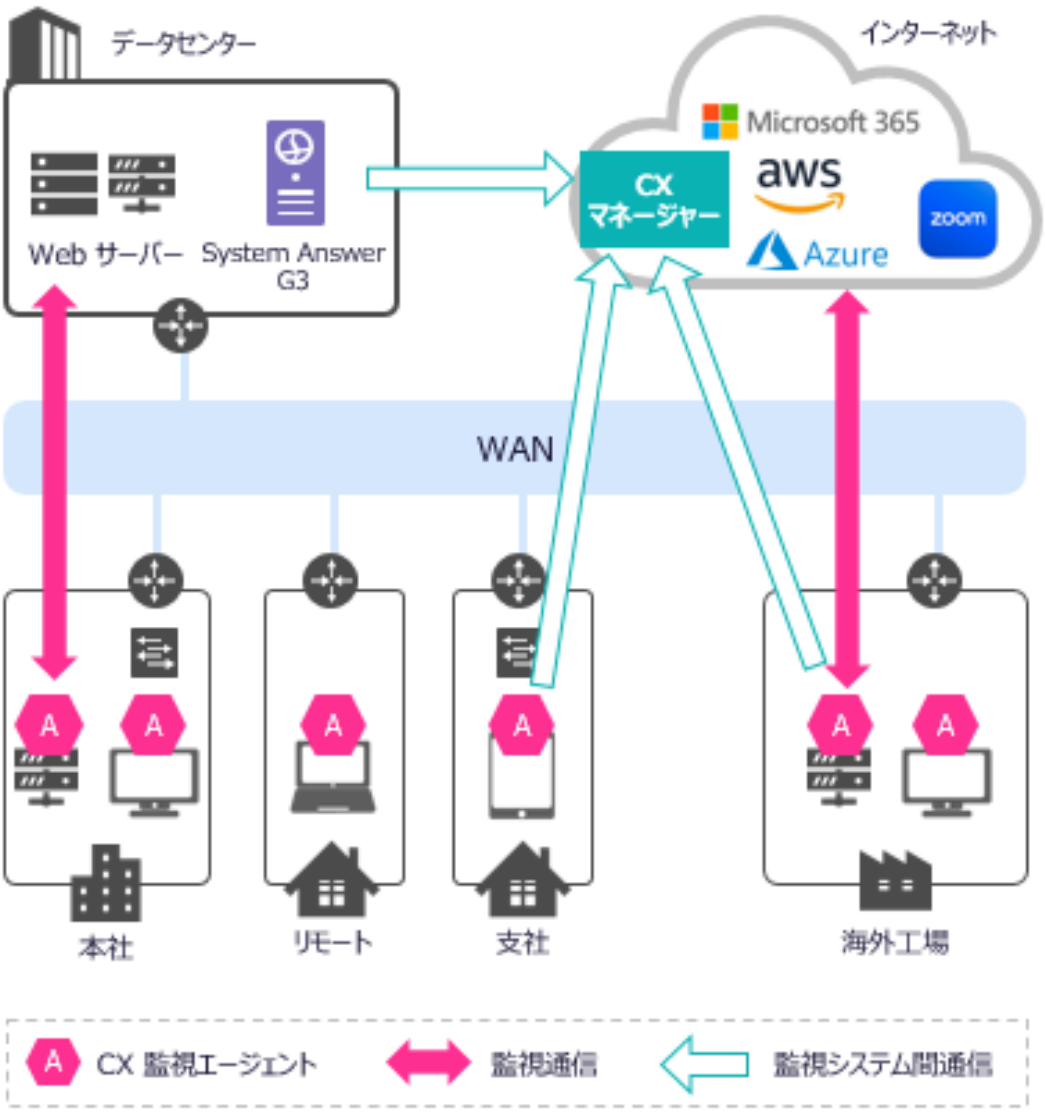
CX（カスターマーエクスペリエンス）監視オプションは、アプリケーションやサービスのパフォーマンスをユーザー視点で監視する仕組みです。。ユーザーの満足度に影響をおよぼすパフォーマンスの問題を迅速に検知・対処ができ、 WiFiの受信状況もユーザーの端末単位でモニタリング可能です。

Point! 無線トラブル時の**「ユーザー証跡」**が分かる



Windowsエージェントを導入した端末では、無線の受信状況をモニタリング可能です。接続しているSSID （Wi-Fi接続に必要なネットワーク名）だけでなく、情報アップロードのタイミングで端末が受信しているSSIDの情報を確認できます。　これにより、PC端末を利用しているユーザーが接続して欲しいSSIDの電波強度が弱くないか、いわゆるノラSSIDの影響度を調査できます。
また、無線用ネットワークシステムの画面上でも分からなかった、「どのホストがどの無線APに繋がったか」が確認できるため、**想定外の場所のAPに接続している端末も特定**できます。

CX監視オプション導入イメージ図



CX監視オプションの導入目的とその効果

01

ユーザー視点のサービスレベルを把握し顧客満足度の向上を図る

02

通信遅延の早期検知、迅速なボトルネック特定を行い、ネットワーク品質向上を図る

03

通問題切り分けから復旧までの時間を短縮し、TCO削減を図る

CX監視オプション詳細はこちらから→

①-4 通信トラフィックの可視化

やるべき

拠点ごとの通信量を知りたい等、ネットワーク管理に必要な要件を網羅的に満たすためには、ネットワークの詳細調査に特化したFlowmonと連携することで、詳細な性能分析とフロー解析を一括管理しシステムのオブサーバビリティを実現します。

SNMP 稼働状況・障害予兆の把握

情報管理 / 性能監視ソフトウェア

System Answer® G3

抜群の操作性で、誰でも直感的にネットワークやサーバー機器の現状を把握することが可能です。長期および短期の傾向を的確に把握することで、障害の前兆を見逃しません。

特徴 障害検知、監視対象機器の負荷、トラフィック量（通常 / ピーク / 平均）の把握が可能

課題 通信内容（ユーザー単位やアプリケーション単位）の把握まではできない

Netflow /sFlow ネットワークの詳細調査

フロー分析、振る舞い検知

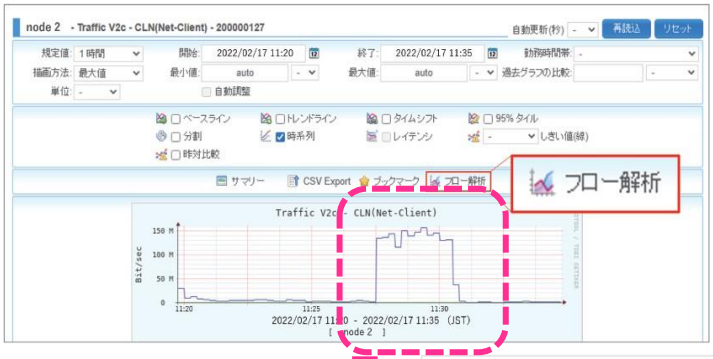
Progress® | Flowmon

フロー分析によって、より高度なセキュリティ対策、詳細なネットワーク調査を行うことができます。レポート機能も充実しています。

特徴 発生したトラフィックの通信内容（ユーザー単位やアプリケーション単位）の把握が可能

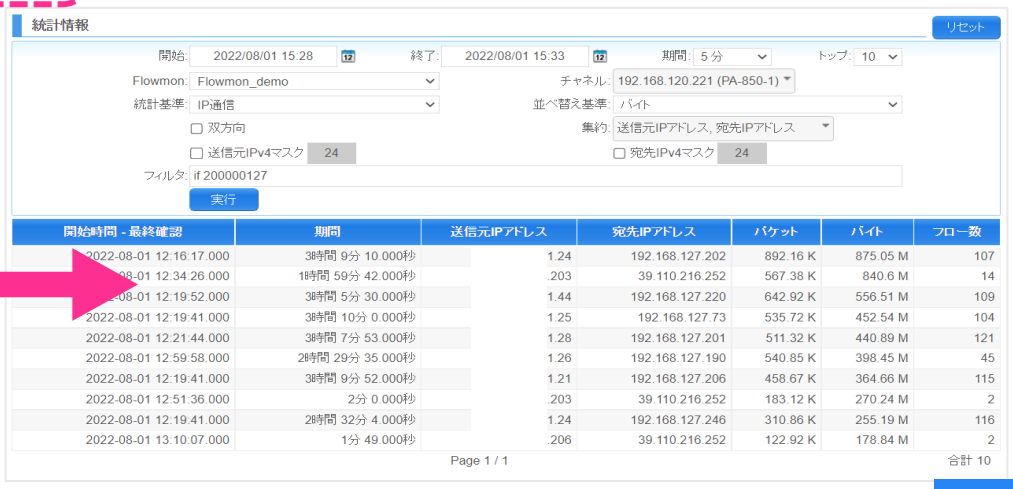
課題 障害検知、監視対象機器の負荷などインフラ環境の負荷、リソース状況などの把握まではできない

System Answer G3で着目したトラフィックグラフから［フロー解析］をクリックするだけで通信の内訳を表示します。



ノード、インターフェース、時間が引き継がれてフロー検索があっという間にできます！

ここからフロー解析をすると



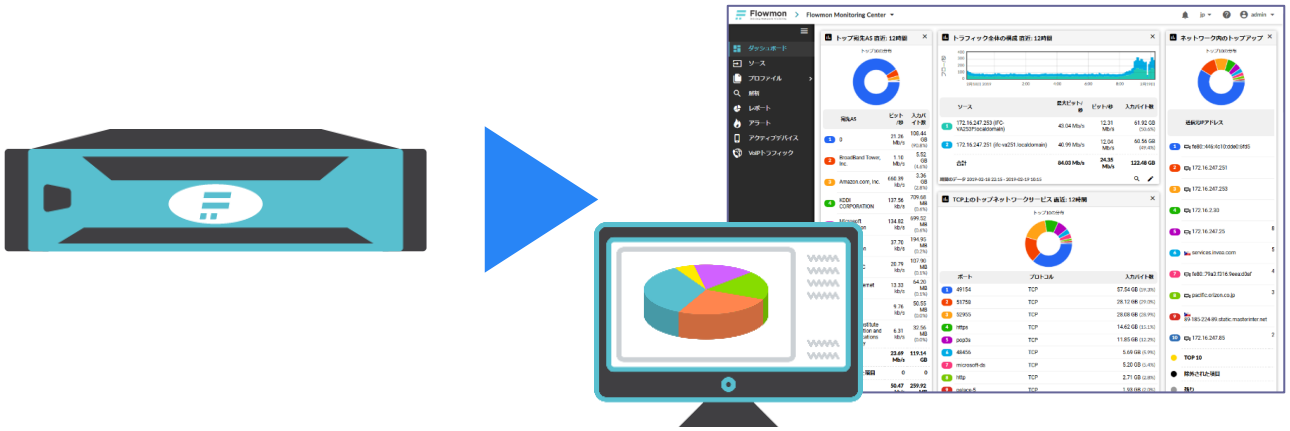
開始時間 - 最終確認	期間	送信元IPアドレス	宛先IPアドレス	パケット	バイト	フロー数
2022-08-01 12:16:17.000	3時間 9分 10.000秒	1.24	192.168.127.202	892.16 K	875.05 M	107
2022-08-01 12:34:26.000	1時間 59分 42.000秒	.203	39.110.216.252	567.38 K	840.6 M	14
2022-08-01 12:19:52.000	3時間 5分 30.000秒	1.44	192.168.127.220	642.92 K	556.51 M	109
2022-08-01 12:19:41.000	3時間 10分 0.000秒	1.25	192.168.127.73	535.72 K	452.54 M	104
2022-08-01 12:21:44.000	3時間 7分 53.000秒	1.28	192.168.127.201	511.32 K	440.89 M	121
2022-08-01 12:59:58.000	2時間 29分 35.000秒	1.26	192.168.127.190	540.85 K	398.45 M	45
2022-08-01 12:19:41.000	3時間 9分 52.000秒	1.21	192.168.127.206	458.67 K	364.66 M	115
2022-08-01 12:51:36.000	2分 0.000秒	.203	39.110.216.252	183.12 K	270.24 M	2
2022-08-01 12:19:41.000	2時間 32分 4.000秒	1.24	192.168.127.246	310.86 K	255.19 M	116
2022-08-01 13:10:07.000	1分 49.000秒	.206	39.110.216.252	122.92 K	178.84 M	2

Page 1 / 1 合計 10

更に

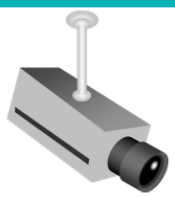
Flowmon ADS なら不正な通信（振る舞い）を自動でキャッチアップ

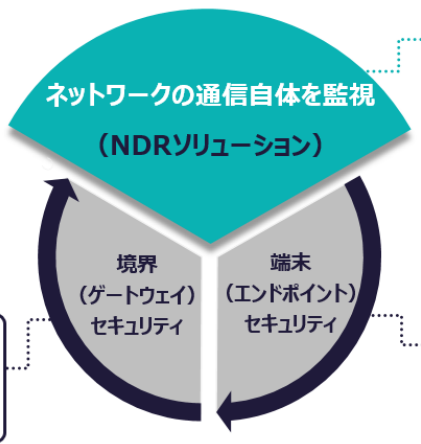
- いつ・誰が・どこへ・何をしたのかを記録（標準機能）
- おかしな挙動（振る舞い）を監視
- 上記の度合い（イベント）に応じてアラートで通知
- 該当者（送信元）や影響範囲（宛先）を特定
- 該当者の過去の動きを調査（録画の巻き戻し）



ADS（Active Defense System：自動防衛システム）とは…

「ネットワークの監視カメラ」がコンセプト





NDR ソリューションとして、
ゲートウェイをすり抜けた脅威
（標的型攻撃・マルウェア）への対策や、
ポリシー違反通信の監視・抑制・
証跡管理が可能

ゲートウェイですべて防ぐのは難しい

例）ファイアウォール
IDS / IPS

エンドポイント製品は管理が大変

例）アンチウイルス
SNMP 監視

Progress® Flowmon®

詳細な機能や特長はこちらから »

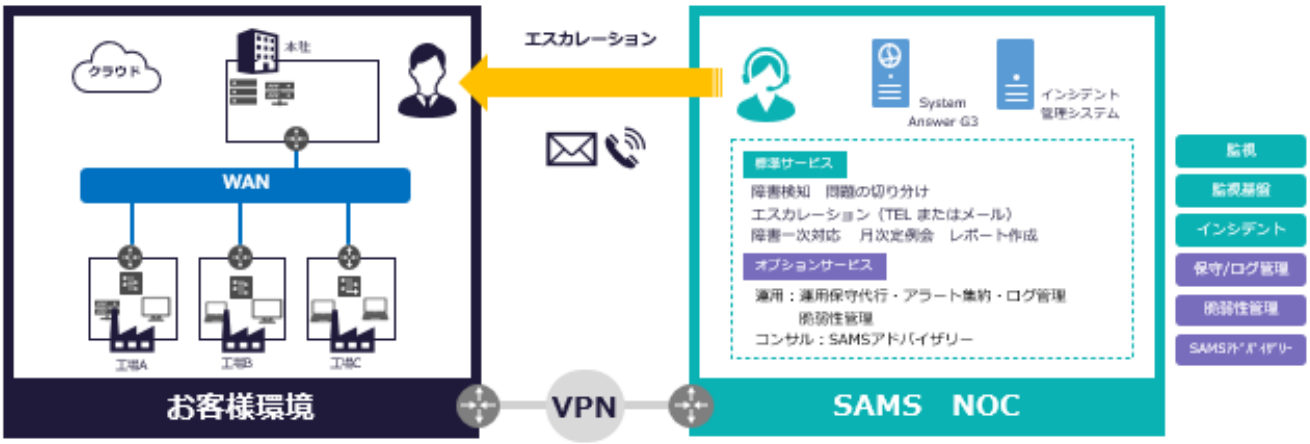
①-5 監視のアウトソース　SAMS

製造DX化に向けて、システム構築の目途はついたが、**運用に不安**が残る・・・。
そんなお悩みもアイビーシーにおまかせください！

24 時間 365 日の環境下で、監視基盤からのアラートをもとに**問題の切り分け**から**障害対応**までを**エンジニアが対応**いたします。自動音声やAIではないので、有事にこそ必要な、正確な事態の把握と迅速で的確な対応が可能となります。また、システムの稼働状況報告と安定稼働に向けた改善を、毎月のレポート形式でご提示いたします。

自社ではまかないきれない部分の運用をアウトソースしてみてはいかがでしょうか？
月額サービスですので、簡単に始められます。

■SAMSサービス提供イメージ



お客様の必要な範囲内でのカスタマイズが可能で、月額サービスにて監視がスタートできます。
監視規模（ホスト数）・インシデント件数（最小5インシデント～）・オプション有無を選択いただけます。

運用アウトソースサービス SAMS の詳細はこちらから→

活用アイディア

アウトソースだけでなく、IBCは監視にかかわるサービスメニューを多数取り揃えております。国産メーカーだからこそ実現する充実のサポート体制を活用したを自社の運用に取り入れ監視運用を成功させている製造業様の活用アイディアをご紹介します。

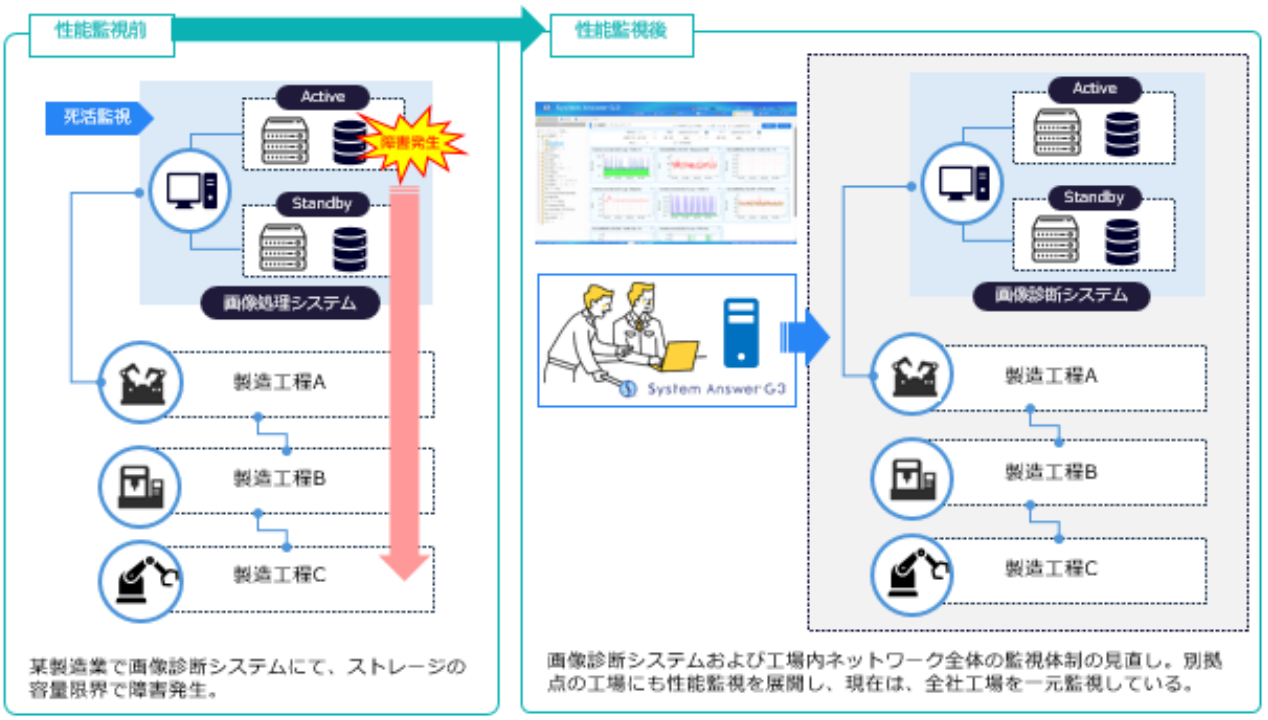
日本農産工業株式会社 様

ツールの良さはもちろんのこと、サポートの良さも実感したため、System Answer だけでなく、ツールをより活用するために、定期的にオンサイトで支援が受けられる運用支援サービスも採用。今後もアイビーシー社の力を借りつつ、自社にノウハウを貯めていきながら、より良いシステム運用を目指していく。

①-6 製造業の課題解決事例

以下は、某製造業様での課題解決事例です。
画像診断システムにて、ストレージの容量限界による障害が発生。冗長構成をとっていたため、死活監視しかしておらず、障害に気づいたのは、画像診断システムから工場のネットワーク全体に影響が出て、全ての製造ラインが止まってしまった後であった。復旧まで数日を要し、その損害規模は数億円に及んだ。

本障害をきっかけに、**性能監視や分析の必要性を痛感**し、監視自体の見直しを実施。障害発生前は、死活監視のみでリソース情報などの性能情報の取得は行っていなかったため、画像処理システムおよび工場内ネットワーク全体の監視体制を見直し、性能監視や分析に特化したSystem Answer G3をご採用。当該工場だけでなく、別拠点の向上にも性能監視を展開し、現在は、全社工場を一元監視している。



IBCなら工場ネットワークと工場セキュリティのどちらもおまかせ！
貴社のスマートファクトリーを実現します！！

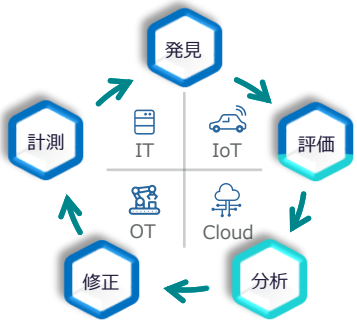
② セキュリティの解決策

これまで工場内部で閉じていたOT系ネットワーク。外部に接続することがないため、サポート切れOSなど脆弱性のあるソフトや機器がそのまま使われているケースも多いのではないでしょうか？このままの状態で、情報系ネットワークに接続したら、OT系のネットワークの弱点を突いたサイバー攻撃により、工場の稼働停止に追い込まれてしまう、とうことも起きかねません。また、サイバー攻撃の足掛かりとしてサプライチェーンを利用したセキュリティ事故も多発しており、今まで工場と直接やりとりをしてきたサプライチェーンの管理も必要となるなど、ひとくちに「スマートファクトリー」といっても、現場の皆様には頭のいたい課題が山積みなのではないでしょうか？

やるべき

脆弱性管理をいち早く行いたい
Tenable One

「保有している資産を把握して、脆弱性管理をいち早く行いたい！」という方には、脆弱性管理ソリューション（ツール）を導入することで、資産の整理と可視化から、サイバーリスクの可視化、攻撃経路の分析まで行うことができます。



安心

業界のガイドラインに準拠したリスク分析をしたい
セキュリティリスク分析　V-Sec

情報セキュリティを組織的な活動ととらえ、ネットワーク（技術的）対策だけではなく、各業界のガイドラインに準拠したガバナンスやマネジメント等の観点から、多面的なセキュリティリスク分析を行うアセスメントサービスです。結果はレポート形式でわかりやすく明示し、さらなる対策強化に向けたアクションまでご提案します。

安心

外部からの攻撃対象となり得る箇所を知りたい
OSINT調査　Discovery

OSINT（オープンソースインテリジェンス）技術を用いた調査です。「OSINT（オシント）」とは、元々は諜報や軍事活動の分野での概念で、ありとあらゆる情報をかき集めそれらの情報を分析する技術をサイバーセキュリティの分野に応用したものが「OSINT調査」と呼ばれるものです。企業情報をハッカー目線で収集し、脆弱性の予測および監視をします。

必須

煩わしい機器の更新管理をなんとかしたい
ネットワークインテグレーション

機器導入後のファームウェアのアップデートが実施されていない状況で運用されている実状があり、機器の脆弱性を悪用され、不正アクセスやランサムウェアによる被害が拡大しています。情報セキュリティ 10 大脅威 2025では「システムの脆弱性を突いた攻撃」が3位に浮上。IBCでは、機器の入替・チューニング・更新管理といったインテグレーションサービスを提供しています。

②-1 脆弱性管理ソリューション　Tenableとは？

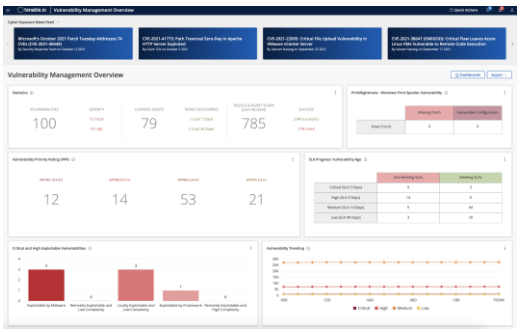
やるべき

スマートファクトリー実現のために、工場内もシステムの侵害につながりうるソフトウェアの弱点や設定上の不備を見つけ、早期対策をすることでセキュリティインシデントの発生を予防することが求められます。
しかし、増え続ける脆弱性の数、人手不足、リスク分析と対応優先の順位付けの難度から手作業による管理には限界があります。
サイバーセキュリティ管理の先駆者である Tenable社の Tenable VM (Vulnerability Management) は、資産管理から定期的な観測まで一気通貫で管理することができます。

脆弱性の数

新たに公開される脆弱性の数は年々増え続けているから、情報についていけない。
2021年：約21,000件
2022年：約23,000件
（1年で2,000件増）

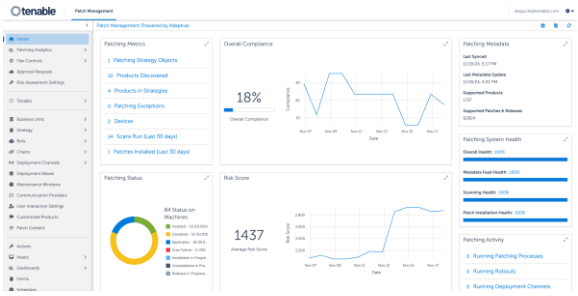
クラウドベースによる脆弱性管理の自動化で、漏れることなくシステムの**脆弱性情報を自動で収集**可能



人出不足

情報系の管理だけでも手一杯だったのに、OT系も管理するのは大変。新たにセキュリティの専門知識を持ったSE を確保することは難しい…

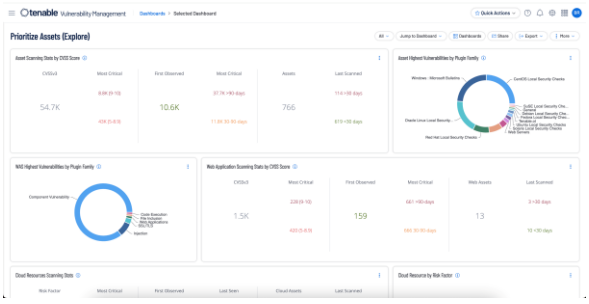
脆弱性の検知履歴と滞在期間（リスク）の把握し、膨大な脆弱性情報を**リアルタイムに管理 / 把握**が可能



リスク分析

膨大な脆弱性の中から、自社に大きな影響を及ぼす（リスクの大きい）ものを分析し、優先順位付けをするなんてできない…

緊急性の高い脆弱性の早期発見し、脆弱性の**脅威 / 緊急性が高い脆弱性を早期発見 / 対応**が可能



Tenableでできること

- 緊急性 / 脅威が高い脆弱性の絞り込み
- 脆弱性の検知履歴と滞在期間（リスク）の把握
- SLA（サービスレベルアグリーメント）の策定
- 資産の重要度付け ASSET CRITICALITY RATING
- 脆弱性管理の自動化

アイビーシーの Tenable サービス

Tenable社のMSSP（マネージドセキュリティサービスプロバイダー）であるアイビーシーに任せて安心のサービスをご提供しています。

日本語サポートサービス

メールによるtenableの操作方法などの機能に関するお問い合わせを日本語で対応します。

＜受付対応時間＞
9:00～12:00
および13:00～17:00
（土日祝、年末年始、IBCの休日を除く）

運用支援サービス

導入後の定期的なフォローアップサービスをご提供。
現場でのSE育成の場としてもご利用いただけます。

- 検出した脆弱性に対するレクチャー
- お客様の運用に合わせた使用/活用方法のレクチャー
- 運用の中でのQ＆A
- 画面を見ながらのクイック分析

Tenable 導入事例 ： シチズン株式会社 様

サイバー攻撃の被害にあう可能性や確率を削減することができ、より強固なセキュリティ体制を整備することができた…

②-2 セキュリティ分析 V-Sec

安心

V-Secはセキュリティ対策上の不備を指摘するだけではありません。お客様がセキュリティ強化に向けたアクションにスムーズに移行するための情報を提供いたします。また、お客様のご要望に応じて、セキュリティリスク分析V-Sec（Visualization Security）の結果に基づいた、セキュリティ強化実装に関しても総合支援が可能です！

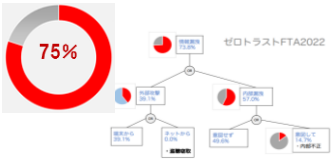
15万円

お試しプラン

V-Sec IC

内容 現状レポート
情報漏洩発生確率の分析

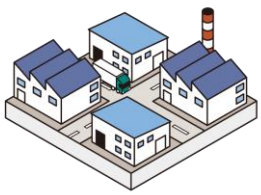
目的 本調査前のセキュリティリスクチェックにより、現状の情報漏洩発生確率を数値化し確認



120万円

Standardプラン（1拠点）

V-Sec FA



内容 管理者へのヒアリングとネットワーク図による現状の対策確認
＜報告内容＞
脆弱性可視化・現状課題・強化の方向性・推奨セキュリティ対策のご提案

目的 工場におけるサイバー・フィジカル・セキュリティ対策ガイドラインに準拠した調査を実施し、企業のネットワークおよびマネジメント等における脆弱性やリスクレベルを分析

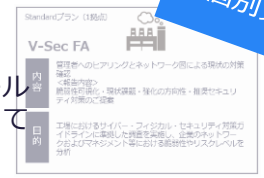
個別見積

Standard（複数拠点）

V-Sec FA+SS

内容 現場担当者へのヒアリングによる業務現場実態調査

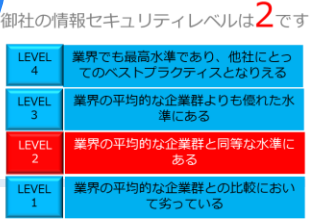
目的 現場のルール遵守状況や業務とルールの乖離を調査分析。業務負担となっているルールの見直し等も検討



報告書の特徴

V-Secは自社の情報セキュリティリスクについて経営陣に把握していただくことを目的にしています。したがって、ビジュアル表現にこだわり直感的理解できるような報告書になるように工夫しています。

総合評価



想定リスクシナリオ

現状対策評価

- 情報セキュリティマネジメントについてはポリシーの整備やインシデント管理体制等の整備に課題が存在します。
- 御社のオペレーションレベルの情報セキュリティは、システム的な対策の整備・運用において、今後のレベルアップが推奨されます。

対策選択肢の提示

②-3 企業情報モニタリング Discovery

安心

AI テクノロジーを活用した OSINT 技術に加え、エンジニアによるハッカー視点での、ダーク Web への漏えい情報を含む外部公開情報の収集・調査を行う独自の監視サービスです。

インシデントの監視および報告

セキュリティインシデントの持続的監視で、タイムリーに対応
・盗まれた資格情報
・公開された社内ドキュメント
・漏洩したソースコード
など

コンプライアンスの準拠と脆弱性予測

本番環境に害を与えない安全な外部スキャンと脆弱性予測
・Web サイトのセキュリティ
・期限切れのドメインと証明書
・PCIDSS 準拠状況
など

外部からの攻撃対象を予測

ハッカー目線で外部からの攻撃対象領域を監視
・API と Web サービス
・保有する Web サイト
・ドメインと SSL 証明書
など

簡易調査（PoC）	簡易レポート、情報漏洩の発生有無の調査、脆弱性診断（Critical、High）	**100**万円～
本調査	詳細レポート、情報漏洩の詳細情報報告、脆弱性診断（Critical、High、Medium）	**個別見積**

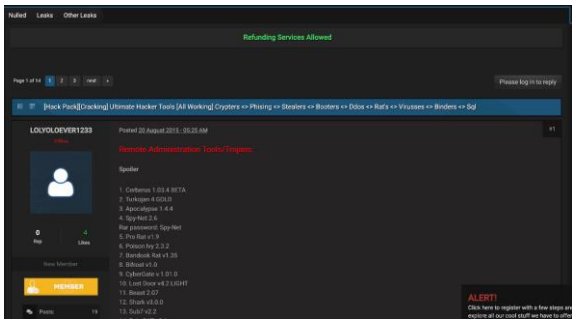
本調査を行う前に、リスクの高い脆弱性の有無や情報漏洩の可能性の有無を簡易的に診断することが可能です。
PoC の結果をもとにして本調査の実施をご検討いただけます。

Discoveryによるインシデント検出事例

未公開の脆弱性情報の流出
一部上場　建設企業

ハッキングの議論もされる掲示板サイトにて対象企業の未修正の脆弱性情報が攻撃ツールと共に売買されている。
公式サイトなどで脆弱性を発見した後に、自ら攻撃するのではなく手法自体を売買することで収益を得る犯罪グループも存在しています。

未公開の脆弱性情報と攻撃ツールのセット販売を発見



従業員のメールアドレス設定流出
一部上場　小売業

Discoveryによる調査期間中に従業員の電話番号やメールアドレスとパスワードのセットがダークマーケット上で『パスワードセレクション』としてリスト販売されていることを発見

メールアドレスとパスワード情報がダークwebにて販売されていることを発見

Phone	Email	Password
********	margaret.razor@example.org	Dublin18
********	rojer.wilhelmsen@example.org	Hallo2021
********	tina.d.ross@example.org	Hockey3
********	ramil.fondeo@example.org	ramilfondeo
********	ramil.fondeo@example.org	385055055ff53e34932667423124772 79
********	rojer.wilhelmsen@example.org	9e995610a1eaaf79fae5d3889cc0725 4
********	tina.d.ross@example.org	7f85055b7267489c5ce5127e98f957b0 1

②-4 ネットワークインテグレーションのご紹介

必須

「工場の監視の前に、工場内のネットワークを見直したい」という方には、
ネットワーク / サーバーインフラの新規導入の際のお悩みをIBCが一気通貫でサポートいたします！

創業以来20年以上、日本のネットワークに携わってきたIBCが、その蓄積したインフラ環境の分析・解析ノウハウをもとに、小規模から大規模まで、高信頼・高可用なネットワークおよびクラウドを設計・構築します。お客様のお悩みに寄り添い、システムの構築から“攻めのIT”提案まで、幅広くご支援します。

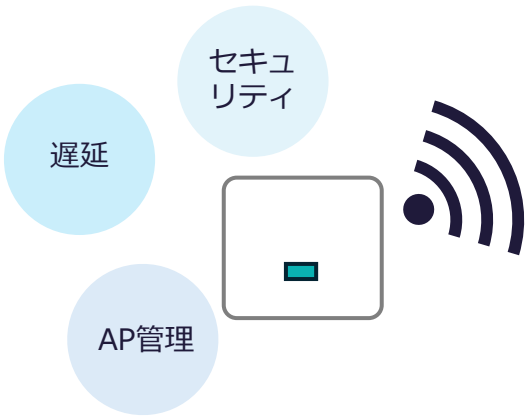
ファイアウォール / インターネットゲートウェイ構築サービス

アセスメントによるゲートウェイ / ファイアウォールの性能劣化状況の可視化→分析、ボトルネックポイントの見直し検討、機器の入れ替えやチューニングなどによる改善を行います。

無線LAN構築サービス

- Wi-Fi 導入規模
- 情報システム部の体制
- 支店や工場など、拠点における対応可否
- 将来に向けた事業の拡張要件
- セキュリティポリシーとの整合性
- 障害発生時の対応

に応じて最適なソリューションを提供



IBCネットワークインテグレーションの製品群

IBCでは多種多様な製品群をを取り扱っており、お客様の課題・ご要望に対応した最適なソリューションをご提供いたします。

ネットワークインフラ	LAN / WAN	ルーター L2 / L3 スイッチ	Cisco / Fortinet / YAMAHA / Apresia、他
		次世代ネットワーク	Fortinet / Cisco DNA / Zscaler/ CATO
	無線 LAN	無線 AP コントローラー	Juniper / Cisco / Aruba / Apresia
		認証サーバー	ソリトンシステムズ / HCNET
		PoE スイッチ	Juniper / Cisco / Aruba / Apresia
	ネットワークセキュリティ	ファイアウォール UTM	Palo Alto / Fortinet / Juniper
		エンドポイントセキュリティ 次世代アンチウイルス、 EDR/MDR	CrowdStrike

サーバーインフラ	OS	MS-Windows / Linux
	仮想基盤	VMware / Hyper-V
	VDI	VMWare Horizon / Xen Desktop / SKYDIV Desktop Client
	NAS	NetApp / ISILON
	ウイルス対策	Symantec / トレンドマイクロ
	バックアップ	アクロニス / Arcserve
クラウド構築	AWS	Amazon（仮想アプライアンスの設置）
	Azure	マイクロソフト（AD 移行、ファイルサーバー移行）

注目！

IBC Care

煩わしいUTMの更新管理もこれで解決！

IBC Care は、アイビーシーで導入したネットワークインフラ機器に対して、保守一次窓口、障害時の切り分け支援、脆弱性情報の提供、パッチ適用、コンフィグ管理等を行う保守サービスです。

こんなお悩みはございませんか？

そんなお悩みを **IBC Care** が解決します。

ネットワークシステムの性能監視に長年携わってきた
アイビーシーのエンジニアが、障害の切り分け支援から
機器保守まで、お客様に代わり対応します！

サービス提供内容

IBC Care サービスは、 メーカーのソフトウェア保守・ハードウェア保守に加え、以下の内容を提供します。当面は Fortinet 社の FortiGate シリーズおよび PaloAlto 社の PA シリーズを対象とします。

カテゴリ	業務項目	提供内容
保守	問合せ窓口対応	導入機器に対する問合せ窓口対応
	ライセンス更新	ライセンスの確認 / 適用
	保守管理	ソフトウェアサポート期限に関する情報の提供
	ソフトウェアに起因する障害における調査	ログの調査、リリースノートの確認、メーカーへのエスカレーション
	ハードウェア故障に対する代替機の手配	機器故障時における交換スケジュールの調整、交換手配
運用	脆弱性対応	脆弱性情報の入手、緊急パッチ適用
	コンフィグ管理	パッチ適用時や送付頂いたコンフィグの管理

IBC Care サービス詳細はこちらから→

多拠点監視、キャパシティ管理、障害予測・早期対応など、製造業で必要とされる情報システムの運用において優れている System Answer シリーズは多くの製造業者様へ導入されています。

事業のDXを支える

ダイキン工業株式会社　様

事業の DX を支える、IT インフラの健全性を獲得！
System Answer G3 の導入から今日に至るまで、長期休暇明けのトラブルは一度も発生することなく…実現できている。

OSSからのリプレイス

マックス株式会社　様

OSSからリプレイス。
直感的に操作できるだけでなく、充実したメーカーサポートやサービスで運用業務工数の大幅削減も実現！

拠点・建屋ごとの管理

あすか製薬ホールディングス株式会社　様

ブックマーク機能を活用して、拠点・建屋ごとに管理。現場からの連絡も、その建屋のグラフを確認して異常の有無や問題の発生したタイミングが一目で判明！

BTmonitor時代から

株式会社タツノ　様

BTmonitor時代から、IBCの性能監視ツールを利用！
本社内、工場内のネットワーク機器、物理サーバーに仮想サーバーと、インフラ全体の性能監視ツールとして活用の幅を広げている。

資料ダウンロード

本書でご紹介した以外にも様々なソリューションを取り扱っております。
こちらのページ↓からダウンロードが可能です。

IBC アイビーシー株式会社

本　社　〒104-0033
東京都中央区新川1-8-8　アクロス新川ビル8F

西日本事業所　〒532-0003
大阪府大阪市淀川区宮原4-1-14　住友生命新大阪北ビル3F

お問い合わせ

03-5117-2780

info@ibc21.co.jp