IBC Solution

Innovation / Business Professionals / Challenge

IBC

PRODUCT

情報管理・品質管理 Information Management / Quality Control

システム情報管理 / 性能監視

System Answer® G3

マルチベンダー機器が混在した IT システムの稼働状態を、的確かつ詳細に把握できる監視・分析ツールです。誰でも簡単に、効率よく、高精度な情報を用いて分析をおこなうことができ、トラブル発生時の問題解決はもちろん、精度の高いキャパシティ計画を実現します。

従来の障害検知から

事前予防へ

一般的な監視システムの先を行く「自動分析」と「将来予測」を実装

純国産だからこその

質と早さ

OSS や海外製品では困難な有事の際のスピーディな対策支援や、お客様要望の製品化を実施

CX 監視 オプション

ユーザー端末からクラウドサービスまでのレスポンスを可視化することで、利用者の感じているレスポンス体感（Customer Experience = CX）を情報システムの運用担当者が視覚的に捉えることができます。

API オプション

G3 で取得した性能監視情報を、Word 形式で自動でレポート出力することができます。レポート作成工数を大幅に削減します。

将来予測オプション

キャパシティ予知 / 昨対比較 / 変動検知といった未来予測機能によって事前の予防対応を可能にし、システム障害を未然に防ぎます。

LOG OPTION

統合ログ管理をおこなうためのオプションです。各種ネットワークシステムの性能情報と、各機器が出力するシスログ、イベントログ、アプリケーションログ情報の一元管理が可能になります。

マルチテナント一元管理

System Answer G3 -XC (Xconnect)

サービス事業者様や、複数のお客様やシステムの管理をおこないたい場合などに、複数の System Answer G3 を一元管理できる製品です。

ネットワーク詳細調査

Progress | Flowmon

ネットフローを利用したトラフィック監視・分析・振る舞い検知をおこなう製品です。パケット解析と同様の視点による解析が短時間で実現可能です。

セキュリティ Security

脆弱性管理プラットフォーム

tenable Vulnerability Management

サーバー、ネットワーク、クラウド、ウェブアプリケーションなど、あらゆる IT 資産を可視化します。

クラウド型 WAF

攻撃遮断くん

情報漏えい、Web 改ざんなどを狙った攻撃を遮断することにより、Web セキュリティへの脅威から企業とユーザーを守るクラウド型の WAF 製品です。

クラウド型エンドポイント保護プラットフォーム

CROWDSTRIKE

クラウド型エンドポイント保護ソリューションは、最新の脅威に対する検知・防御だけでなく、侵入後の隔離まで対応いたします。

WAF 自動運用サービス

Waf Charm

AWS WAF / Azure WAF の自動運用サービスです。シグネチャ最適化技術を用いて、Web サイトごとにおすすめのシグネチャを判別して提供・自動運用します。

エンドポイントセキュリティ管理

ism CloudOne

標的型攻撃対策や内部不正防止に有効な、クラウド型 IT 資産管理ツールです。

セキュリティ保護

Web 改ざんチェック Cloud

独自の改ざん検知エンジンでWebサイトの改ざん有無を監視する SaaS 型セキュリティサービスです。

運用改善 Operational Improvement

総合的なコンフィグ管理

Net LineDancer

コンフィグ管理の自動化でネットワーク運用の負荷軽減と人為的エラーの根絶を実現し、ネットワーク管理コストを大幅に削減します。

運用自動化プラットフォーム

Kompira

アラート判断、エスカレーション、構成管理などの運用を自動化させるソリューション・サービスです。人的コストの削減とサービス品質の向上を実現します。

デジタル証明書 Digital ID

IoT セキュリティ基盤

kusabi

ブロックチェーン技術による電子証明システムと独自のデバイスプロビジョニング技術によって、ソフトウェアだけで IoT セキュリティ環境を実現します。

SSL 証明書

digicert

SSL サーバー証明書の取得にご利用いただけるクーポンをスピーディーにご提供します。デジサート・ジャパン合同会社の Excellent Partner であるため、クーポンを安価に購入することができます。

システム情報管理ソフトウェア

System Answer® G3

日々の業務でこんな課題はございませんか？

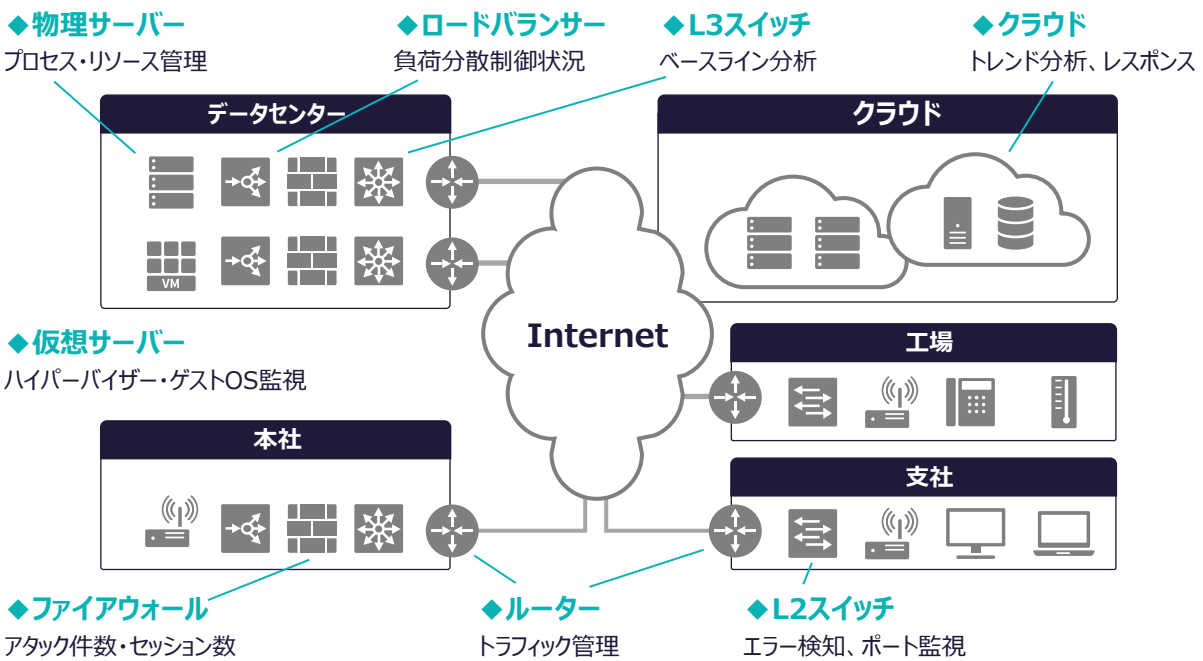
ひとつでも該当した場合は、System Answer G3 をご検討ください！
「現状の見える化」により今後どのようなことが必要か「最適解」を発見できます。

- 現場から「社内システムが遅い」と言われる
- 既存インフラを増強したいが 上層部がなかなか OK を出してくれない
- Microsoft 365 や VDI を導入してから NW のアクセスが遅くなったと感じる
- インフラにどのような負荷がかかっているか 実態が把握できていない

System Answer G3 を利用することで全体を把握

System Answer G3 は、さまざまなシステムの状態を正確かつ詳細に把握することができます。監視対象は、社内のネットワーク / サーバーからデータセンター、プライベートクラウド / パブリッククラウド、仮想環境まで多岐にわたります。各種機器の稼働状況や性能情報を収集することにより、システム全体を包括して一元監視することが可能となります。

ブラックボックス化している環境をクリアにして現状の「わかる化」をご支援いたします。



監視設定・分析・監視処理の自動化

1 分間隔データ収集・5 年分データ非圧縮保存

※お客様環境に依存します。

マルチベンダー機器対応

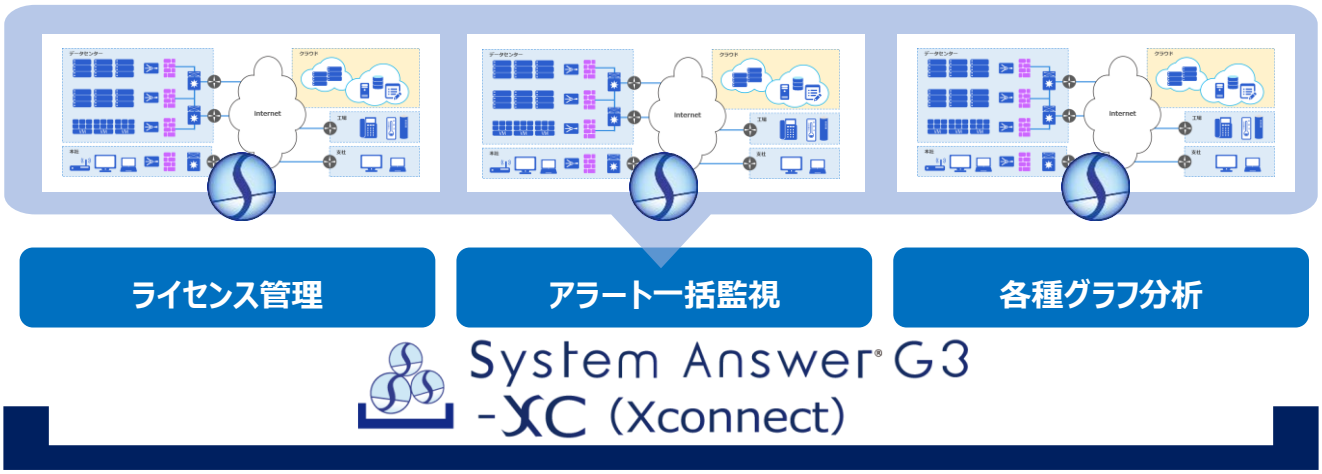
日本語 UI ・わかりやすい操作性

System Answer® G3 -XC

System Answer G3 - XC（Xconnect：クロスコネクト）は、複数の System Answer G3 を一元管理する機能です。各監視環境下で同一 IP アドレスが存在する環境であっても 1 システムで管理することが可能で、それぞれの G3 のアラートやライセンス管理も一元化できます。サービス事業者様や、複数のお客様やシステムの管理をおこないたい場合などにご活用いただけます。

System Answer G3 – XC の管理イメージ

System Answer シリーズのメリットを生かした大規模運用の構成を組むことができます。



特徴

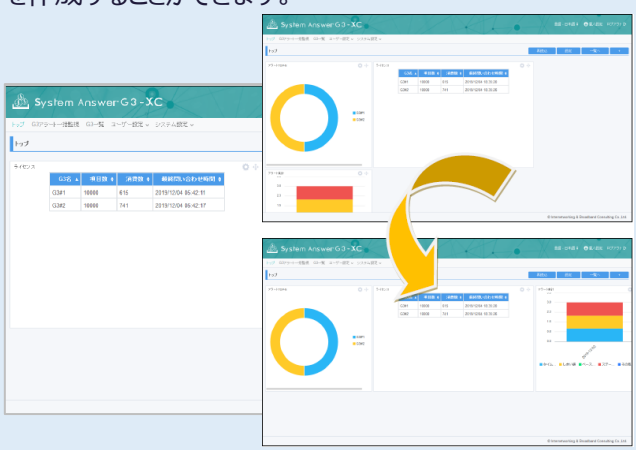
完全マルチテナント対応をしているため、MSP（運用管理）事業者様や複数システムを大規模に管理する必要のあるお客様の運用コストを大幅に削減します。XC はリモート監視にも効果を発揮します。

リモート G3 個別監視

管理配下にある、それぞれの G3 の「グループ」「ノード」「VMware」「機種ランキング」「項目ランキング」「イベント」「シスログ」「トラップ」などを表示できます。

使いやすい UI

XC と連携する G3 のアラート、ライセンス情報をウィジェットで設定、表示します。また、作成されたウィジェットは画面内に自由に配置可能で、見やすいダッシュボードを作成することができます。



将来予測オプション

情報システム障害の多くは回避することができる

IPA（独立行政法人 情報処理推進機構）が 2010 年から社会に影響を与え全国紙などに報道された情報システムの障害情報を集計している「情報システムの障害状況一覧」によると、2019 年後半における障害は 84 件（消費増税関連を除く）ありました。

https://www.ipa.go.jp/sec/system/system_fault.html

アイビーシーによる分析の結果、多くの情報システム障害は回避できた可能性がありました。

「将来予測」で 障害を回避できたもの	57件(68%)
人為的ミス / プログラムミス / その他	27件(32%)

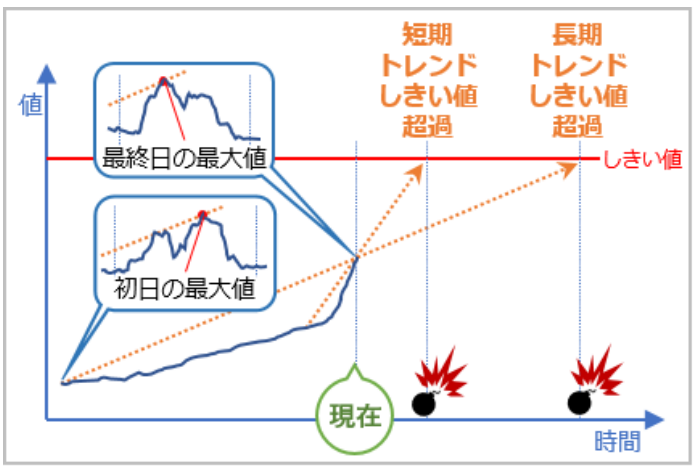
障害には様々なケースがありますが平均的な障害回復に必要となるコストは
数百万～数千万円となります。
また、障害による業務停止などの影響を鑑みた**機会損失額は数億円以上に及ぶ**ことも稀ではありません。金融システムや EC サイト / 決済サイトなどの障害は大きな社会的影響を及ぼします。

将来予測オプションは、「キャパシティ予知」「昨対比較」「変動検知」等の機能によって、将来的なシステムの障害を回避するためのオプションです。今まで過去のログ情報や監視データの収集・可視化・分析をもとにした事後対応が中心であったシステム運用のありかたをプロアクティブな事前対応に変え、運用にかかわる TCO を大幅に削減することが可能となります。

System Answer G3 は過去（ログ監視）から未来予測へ！

キャパシティ予知機能

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。ディスク容量やメモリー使用率などの傾向から、最大値やしきい値を超える時期を予測し、アラートを通知することで、リソース使用状況が限界となる 3 か月～ 1 年先のシステム障害を回避する対策を講じることができます。
キャパシティ予知機能では、サンプリングデータとして平均値や最大値を選択可能であり、サンプリング期間も長期、中期、短期などお客様リソース毎に任意の期間に設定可能ですので、高い精度の予測を実現します。

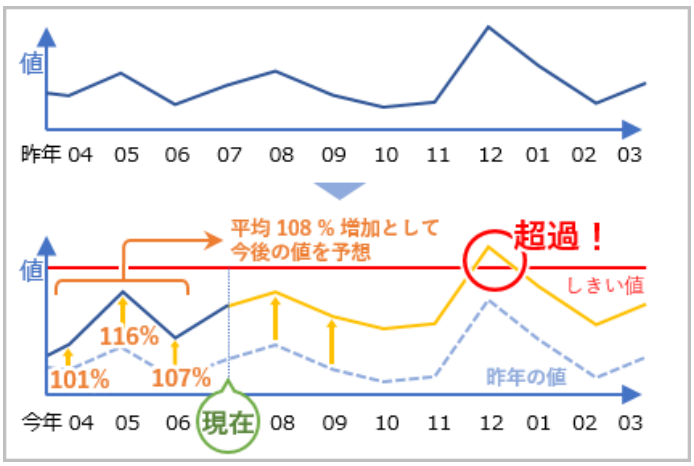


- しきい値を超えそうな 6 か月前 / 3 か月前 / 1 か月前にアラートを通知します。
- アラートには予測グラフが添付され、リソース枯渇時期を早期に的確に判断することができます。
- しきい値（デフォルトは 100 % になる日）やアラート発報のタイミングは、お客様ごと任意に設定可能です。

今年のピークはクリアできますか？ピークも安心して休めます！

昨対比較機能

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。主にお盆、年末年始などの将来の季節変動月において、リソースの最大値 / しきい値を超えないかを判断することができます。

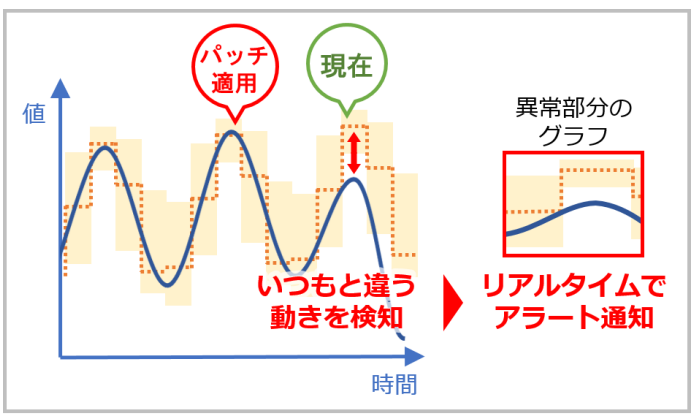


- 過去の対象データの開始月はお客様が任意に設定し、そこから 12 か月を昨年分として計算します。
- アラートには予測グラフが添付されます。
- 今年のピークを乗り切れるかどうか、早期に的確に判断することができます。

設定変更や本番リリースは人ではなく System Answer G3 が立ち会います！

変動検知機能

過去の性能データから周期性がある傾向を自動学習してベースラインを作成し、ベースラインから外れたイベントを検知すると、異常変動としてアラート通知します。
一般的な死活監視では、性能低下を検知することが難しく、障害としてアラートを通知できませんでした。そのためお客様などの利用ユーザーからクレームを受けて、初めて障害に気づくことになります。障害に気づいてから、原因特定さらに復旧までには相当の時間を要し、その間にお客様の離反や多額の売上機会損失を招くこととなります。
変動検知機能では、新システムリリースやソフトウェアの不具合などにより、急激なリソース上昇の変動も検知可能ですので、しきい値での監視では見過ごされていたサイレント障害に対しても有効に機能します。アラート検知後の処理をワークフロー化することで、設定変更や本番リリース時の運用担当者の立ち合いは不要となります。



- 平常時の状態把握、曜日や時間帯、イベントやキャンペーンによる突発的なリソース変化を予測することができます。
- ベースラインとしての学習対象から除外する曜日・日付（休日など）を、カレンダーから任意に設定可能です。
- 異常をアラートをとして検知させない曜日・日付も、カレンダーから任意に設定可能です。
- アラートには異常部分のグラフが添付され、どのようにいつもと違う動きをしたのか確認することができます。

CX 監視オプション

情シスのミッション『ユーザー満足度の向上』に貢献するために

働く場所の変化や DX 推進など、デジタル化を推奨する「クラウドファースト」への取り組みが進むに伴い、情報システムの運用に関する負担は増大しています。システム障害の原因となりうる箇所が、自社で保有しないインフラやサービスまでに及ぶようになりながら、より早期の検知・切り分け・復旧が求められるためです。

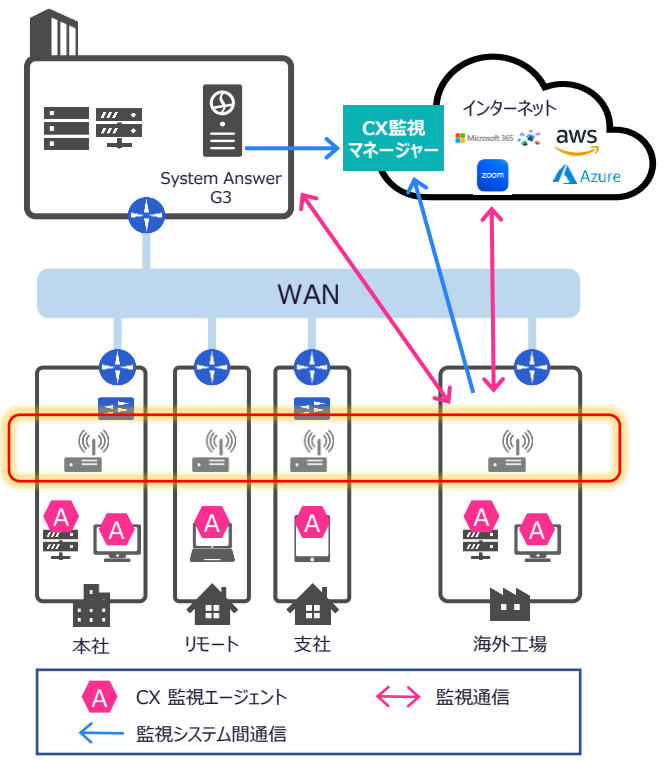
「CX 監視オプション」は、そんな課題を直観的に解決するために生まれた**ユーザー端末からクラウドサービスまでのユーザーのレスポンス体感を可視化する**オプションです。

カスタマーエクスペリエンス（CX）を視覚化する新機能

インターネット全体、拠点間の通信状態、全てのネットワークの監視をおこなう新たな監視体験

- “**なんとなく遅い**”原因を可視化
- 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**
- 通信遅延の早期検知、迅速なボトルネック特定を行い、**ネットワーク品質の向上**
- 問題の切り分けから復旧までの時間を短縮し、**TCO 削減**

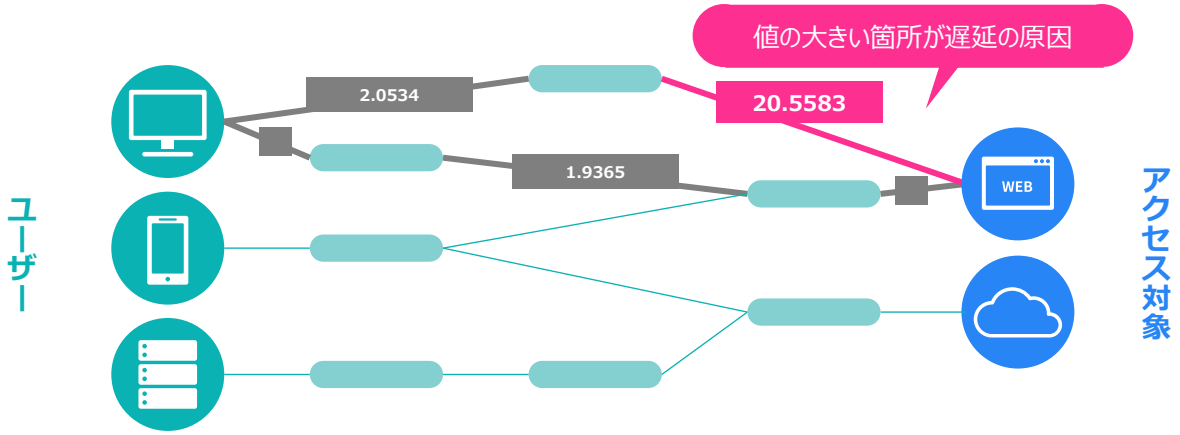
CX 監視オプション導入全体イメージ



CX 監視オプション導入イメージ

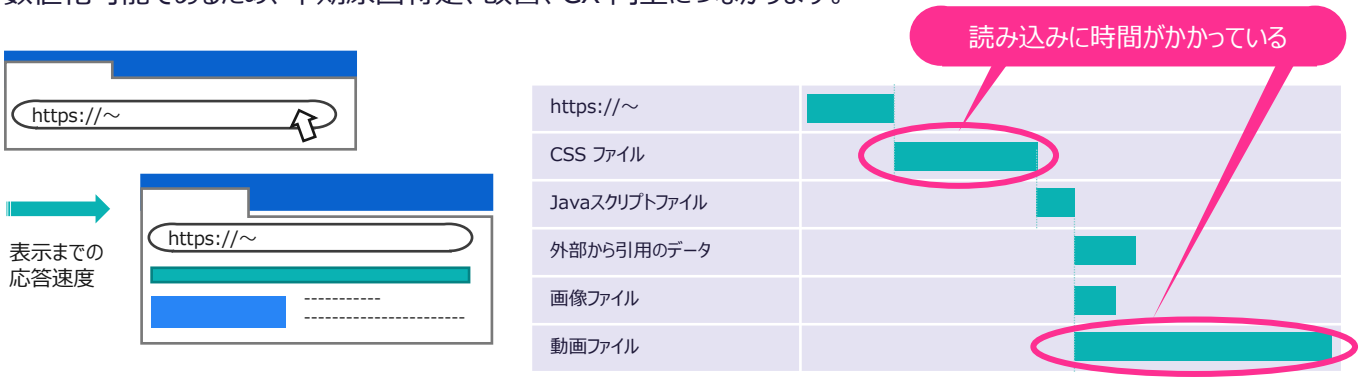
ネットワークパス表示機能

ユーザーが通信の異常（繋がらない、遅いなど）を感じた時に、その通信経路のパスと、応答値などの情報を表示します。設定した閾値よりも遅くなっている箇所は、通信経路のラインが赤く表示されます。



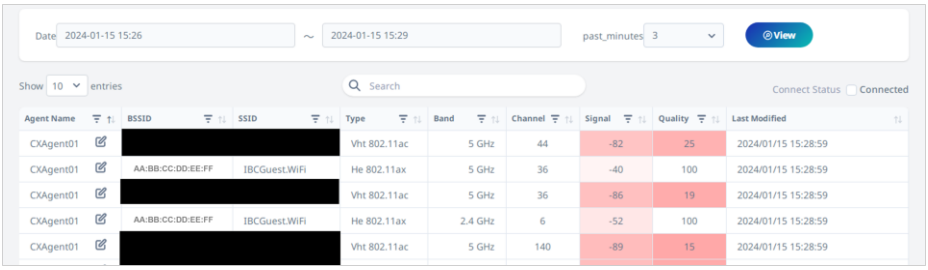
ページロード機能

指定した Web ページのすべてのドキュメントやコンテンツに対してダウンロードを実行し、その速度をチェックします。遅延状況をコンテンツ毎に確認できるため、「特定の画像の容量が大きい」「CDN が特定時間帯で遅い」などの原因の検証・特定が可能となります。また、クライアント環境から実行することでユーザーの体感するレスポンス速度をそのまま数値化可能であるため、早期原因特定、改善、CX 向上につながります。



無線通信状況モニタリング機能 ※Windows エージェント利用時のみ

Wi-Fi の通信状況（BSS 接続情報や信号強度）を管理できます。PC 端末を利用しているユーザーが接続している SSID の電波強度や、野良 SSID の影響度などを調査できます。
※ クライアント自身がクラウドへ情報を送るため、CX 監視エージェント（関連して NMAP、Chrome）のインストールが必要となります。



提供形態：System Answer G3 v03.28-00 より利用可能
提供価格：当社営業またはホームページの問い合わせホームまでお問い合わせください

LOG OPTION

Log Option は統合ログ管理をおこなうためのオプションです。各種ネットワークシステムの性能情報と、各機器が出力するシスログ、イベントログ、アプリケーションログの一元管理が可能になります。

統一されたフォーマットによる多種多様なログの管理

Log Option では、多種多様なログを収集方式にとらわれることなく、統一されたフォーマットで扱うことができます。

また、異なる種類のデータに同一の意味づけ（タグづけ）をおこなうことで、ログの形式の違いを吸収して扱うことができます。これによって、データの羅列でしかないログを人間が見てわかる形式に変換して、活用することが可能になります。

性能管理とログ管理の連携により、可用性と安全性を兼ね備えた安定的かつ効果的な IT システム運用が可能となります。

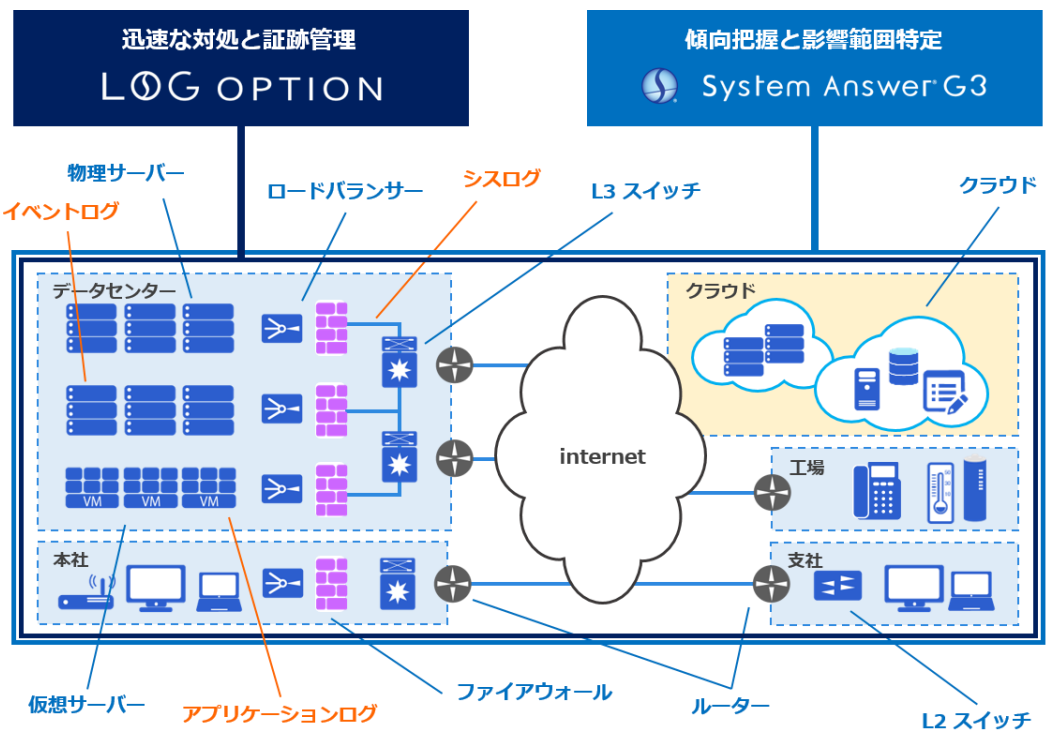
ログの管理機能

- 一元管理
- 長期・圧縮保管
- 保護機能
- セキュリティ強化
- アクセス制限
- PCI DSS/ISMS

機能一覧※一部抜粋

機能	概要	Log Option 対応機能
ログの検索・分析機能	収集したログに対する検索・分析をおこなう機能	検索機能 集計機能
リアルタイムアラート機能	異常を示すログを収集した際、アラートを挙げる機能	検知機能
定期レポート出力機能	ログ分析レポートを定期的に自動出力する機能	レポート機能

Log サーバー構築については、45ページをご覧ください。



Log Option の機能一覧

機能	概要	Log Option 対応機能
ログの一元管理機能	あらゆる箇所に点在するログを自動収集・一元管理する機能	ログ収集・保管機能
ログの保護機能	収集したログの暗号化、および保管ログに対する改ざんを検出する機能	ログ収集・保管機能
ログの長期・圧縮保管機能	収集したログをアクセス可能な形で圧縮・保管する機能	ログ収集・保管機能
ログ形式の吸収機能	異なるフォーマットのログに対して意味付け・タグ付けをおこない、横断的な検索・分析がおこなえるよう管理する機能	管理機能
ログに対するアクセス制限機能	グループ・ユーザーごとに、ログに対するアクセス許可・不許可を設定する機能	管理機能
ログの検索・分析機能	収集したログに対する検索・分析をおこなう機能	検索機能 集計機能
リアルタイムアラート機能	異常を示すログを収集した際、アラートを挙げる機能	検知機能
定期レポート出力機能	ログ分析レポートを定期的に自動出力する機能	レポート機能

System Answer シリーズとの連携

障害発生時には、原因箇所の迅速な特定と早期対応、そして的確な再発防止策の実施が求められます。そのためには、日頃からの性能監視による情報収集と影響範囲の特定、加えて該当システムに関する詳細なログ情報の管理が重要なポイントとなります。

System Answer シリーズ		+ LOG OPTION
性能監視 / リソース監視 性能・リソース情報を分析することで、早期の原因究明や根拠ある再発防止対策を提示。	**原因究明を迅速におこないたい** 障害発生時のアプリケーションログを把握しようとすると、該当サーバーに個別にログインする必要があり、原因究明に時間がかかる。	**詳細なログ取得** 各種機器のテキストログを取得し、一元管理。障害やセキュリティ事故発生時の詳細な証跡ログを把握し、迅速な復旧・対策が可能。
キャパシティ計画 CPU 、メモリー、ディスク情報などの性能情報をもとに将来予測をおこない、どの程度システムを増強すべきか、根拠ある対策を立案。	**具体的な対策を取りたい** 性能情報で全体的な傾向は把握できるが、アプリケーションレベルでの詳細な傾向が把握しにくい。	**豊富なログ収集** 各種サーバー / アプリケーションログを横断的に一元管理し、どのアプリケーションがリソースに影響を与えているかを分析して、計画立案が可能。
予防保守 性能情報の傾向を学習することで、サイレント障害の検知をおこない、トラブルを未然に防止。	**障害を予防したい** 性能監視だけでは把握しにくいアプリケーションの挙動の変化や、セキュリティ事故につながる不審なアクセス / 挙動を掴みたい。	**ログ分析による検知** ログの横断追跡によって「いつ誰が何をしたのか」を把握し、検知条件に合致したアラート通知も可能。障害や事故につながる挙動を早期に発見可能。
レポート 性能情報を簡単にレポート出力。システム全体の把握や、月次 / 週次レポートなどの報告書に活用。	**さまざまな脅威に対応したい** 性能監視では把握できないアプリケーションログを取得し、必要があれば取得結果を証跡レポートとして出力したい。	**集計レポート出力** 収集したログの集計結果を表やグラフで出力することができ、証跡として活用可能。また、その結果を月次や週次で定期的に自動出力が可能。(出力形式：PDF , HTML , CSV , XML)

Progress® Flowmon®

ネットワークフローを利用した、トラフィック監視・分析・振る舞い検知に特化したアプライアンス製品です。パケット解析と同様の視点による解析が「通信ログを残しつつ、短時間で実現可能」です。ユーザー単位やアプリケーション単位での通信状況を把握でき、直観的な GUI で、効率的かつ高速な解析を実現いたします。

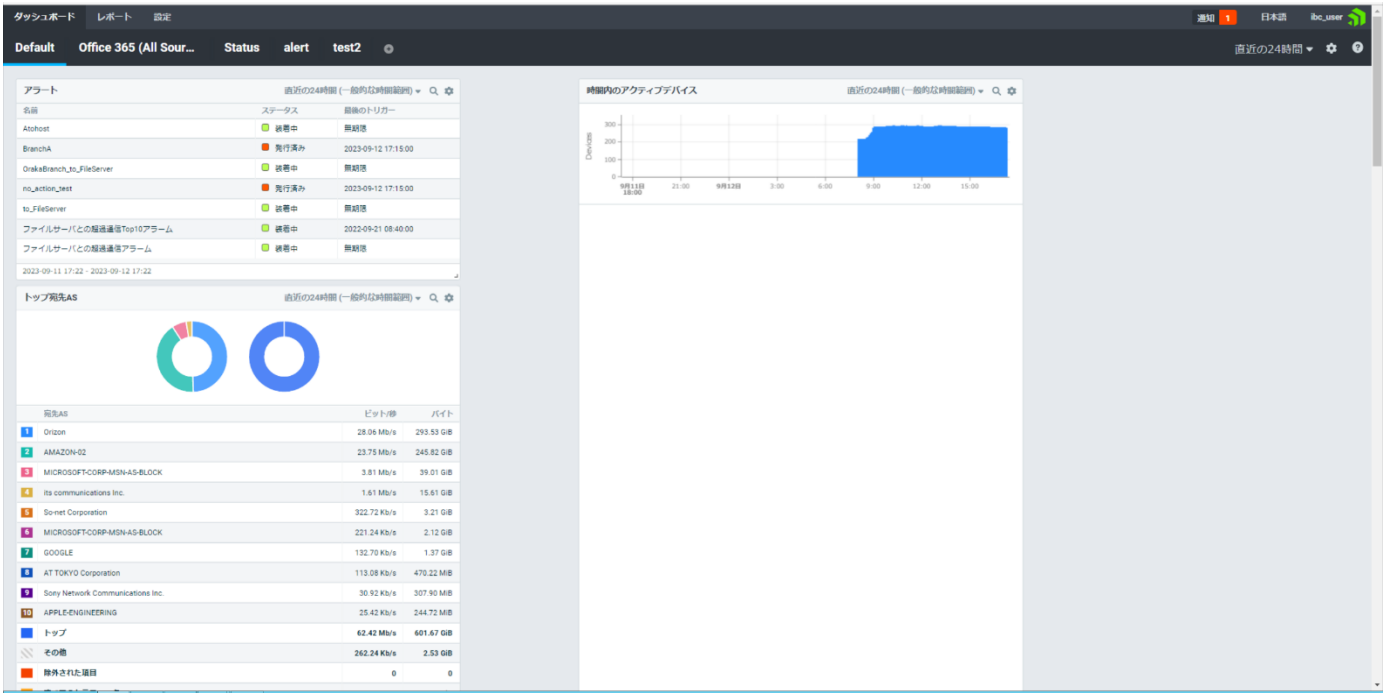
環境を選ばずに、ネットワークの状況を脅威も含めて可視化

- どこからどこへ通信が流れているのか？
- 誰が帯域を占有しているのか？
- どんなアプリを利用しているのか？
- 大事なデータのアクセスは？
- Web の使用状況は？
- 不正利用の対策は？

Flowmon（フローモン）によるネットワークフロー分析なら、誰が・いつ・どこで・何をしたかをすぐに把握することが可能です。帯域を占有しているユーザー（端末）を即座に発見し、原因を特定できます。

画面イメージ

ポートの種類ごとに色分けされた分かりやすい GUI のため、直感的にトラフィック量の分析が可能です。タイムスタンプつきで通信を可視化します。また、通信量の多い拠点 TOP10など、ユーザーの環境に応じた独自の分析画面を自由に構成することが可能です。



導入シミュレーション

ネットワークの可視化・次世代トラフィック解析にくわえ、振る舞い検知機能（オプションプラグイン）により、従来のパターンマッチングでは発見できなかった未知の脅威を可視化します。標的型攻撃対策やマルウェア感染端末の特定および不用意な行為の抑止に活用できます。

01. 監視・解析をしたい対象の選定

お客様の環境や目的に合わせて、トラフィックの分析をおこないたいエリアを決めます。Flowmon の特性上、既存のネットワーク環境を変更することなくトラフィック分析がおこなえます。

02. ログの収集・アラート検知

Flowmon の最適な構成により、フローログ（通信ログ）を収集します。今まで見えなかったネットワーク状況の可視化や、しきい値検知によるアラート発報から、社内規律保持を促せます。

03.ネットワーク解析レポート作成

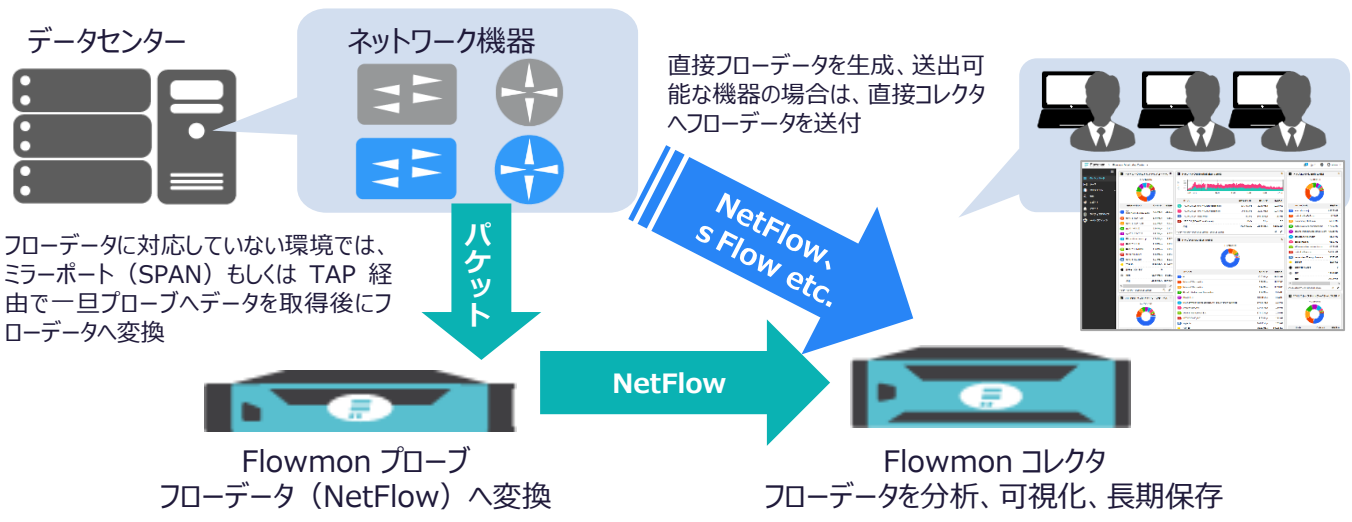
解析により、端末同士の会話やトラフィック量を把握できることから、帯域占有端末や使用率ランキングなどのレポートを作成します。
例）大阪拠点よりデータ転送量の多かった端末 Top 10 など

04.改善策のご検討

解析結果（レポート）は、キャパシティプランニングにご活用いただけます。また、望ましくないトラフィック通信の有無を確認できるため、不正利用対策にも有効です。

構成イメージ / 自動レポート機能

- ✓ PDF で出力可能（文言編集可能）、スケジュールを設定して自動でメール配信も可能
- ✓ 1 日、1 週間、1 ヶ月単位のレポート
- ✓ トップ N レポート、トラフィックレポート
  ex）通信量の多いトップ 10、特定ポートでフィルターなど



脆弱性管理プラットフォーム

tenable Vulnerability Management

Tenable Vulnerability Management は、組織の IT 資産の露出と脅威をサイバー攻撃の視点から監視し、クラウドベースで継続的に評価するサービスです。隠れた脆弱性を特定し、最も危険な脆弱性を最初に修正するための優先順位付けと、修復に必要な情報を一体化して提供します。

脆弱性管理の必要性と課題

順位	脅威	昨年順位
1位	ランサムウェアによる被害	1位
2位	サプライチェーンの弱点を悪用した攻撃	2位
3位	内部不正による情報漏えい等の被害	4位
4位	標的型攻撃による機密情報の窃取	3位
5位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	6位
6位	不注意による情報漏えい等の被害	9位
7位	脆弱性対策情報の公開に伴う悪用増加	8位
8位	ビジネスメール詐欺による金銭被害	7位
9位	テレワーク等のニューノーマルな働き方を狙った攻撃	5位
10位	犯罪のビジネス化（アンダーグラウンドサービス）	10位

※ 出典：情報処理推進機構（IPA）「情報セキュリティ10 大脅威 2024」

・第7位

ソフトウェアやハードウェア（機器類）の脆弱性対策情報の公開は、脆弱性の脅威や対策情報を製品の利用者に広く呼び掛けられるメリットがある。
一方で、攻撃者はその情報を悪用し、当該製品への脆弱性対策を講じていないシステムを狙って攻撃を行うことができる。近年では脆弱性関連情報の公開後に攻撃コードが流通し、攻撃が本格化するまでの時間もますます短くなっている。

定期的に脆弱性診断をしているが
対応状況の把握ができない

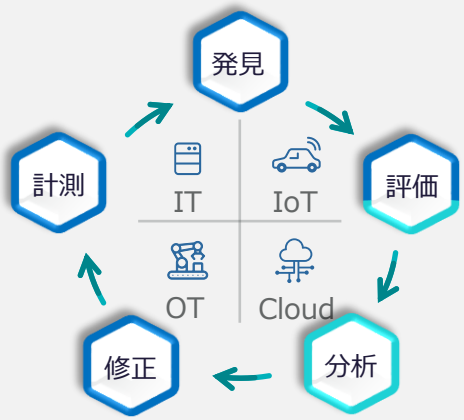
脆弱性診断対象となる
デバイスの把握が難しい

脆弱性診断結果に対する
優先順位づけがわからない

tenable Vulnerability Management による課題解決

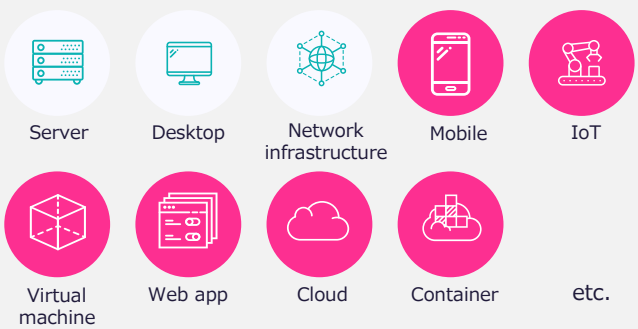
脅威へのアプローチ

脆弱性の悪用を未然に防ぐため、リスクの素早い特定と重要資産への修正の優先順位付けを支援する管理プロセスを提供します。



脆弱性状況の把握と管理が可能

オンプレミス、クラウド、コンテナ、Web アプリケーションなど、異なる資産のハイブリッド環境を一括管理し、高リスクな脆弱性を素早く識別します。



Exposure Management（露出管理）

Tenable 社が提唱する「Exposure Management（露出管理）」は、組織が IT 資産のサイバーリスクを効率的に理解し、対応するための戦略です。Web ブラウザを使用して、リスクのある資産の特定、対処策の参照、リスク状況の変化の追跡を正確に把握・管理することが可能です。

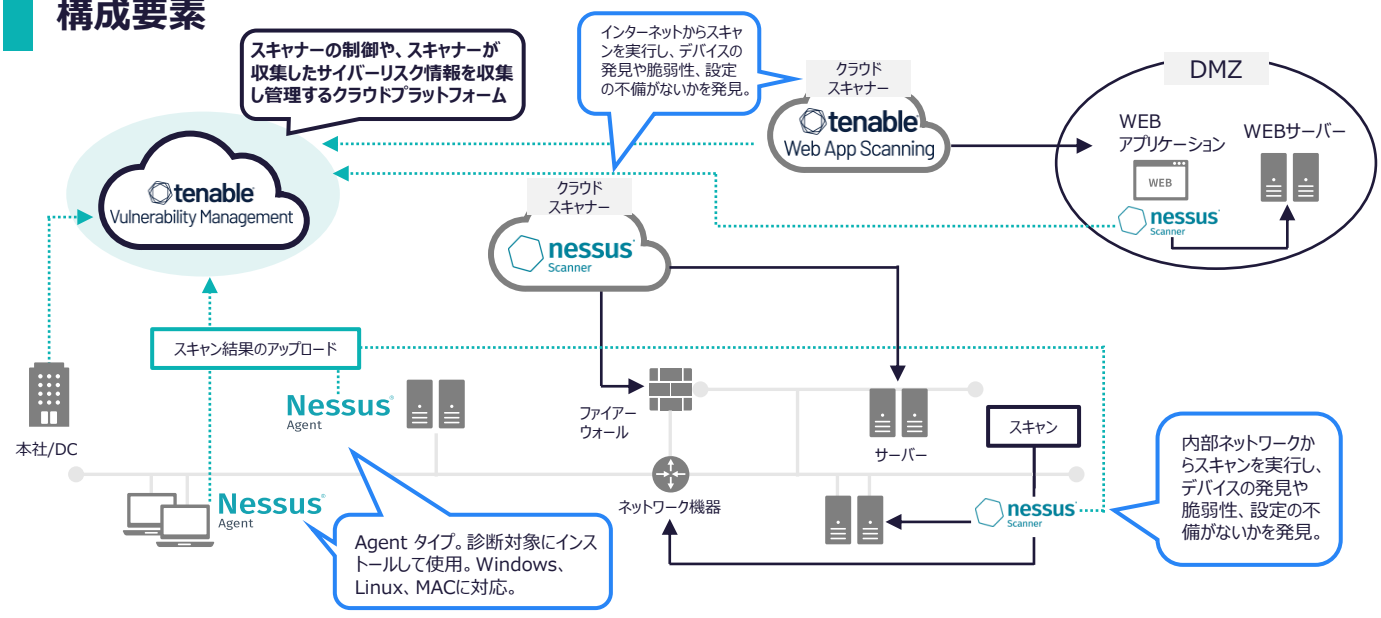
従来の脆弱性管理や資産管理

- 限定的な資産のみの把握
- 資産の不十分な発見
- IP ベースでの管理
- 可視化の間隔が長い
- 不十分な優先順位づけ
- 脆弱性情報だけにフォーカス
- 企業や組織全体のリスクが不明瞭

Exposure Managementによる解決

- 全資産を明確に識別してそれぞれのリスクレベルを評価
- 資産単位のリスクレベル、ビジネスインパクトなどをもとに優先順位を設定
- Web ブラウザのみで一元的なリスク評価が可能
- 定期スキャンにより継続的な監視、経過リスクに応じた危険性を追加判断
- コンプライアンスや業務規制（PCI DSS 準拠など）への評価要件に対応

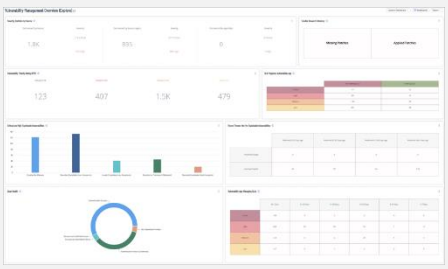
構成要素



tenable Vulnerability Management 機能特徴

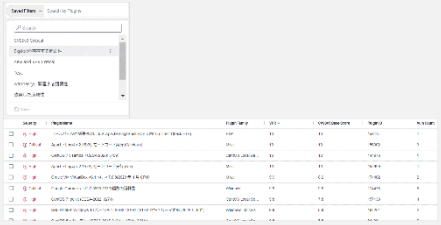
シンプルかつモダンな UI

不要な機能をそぎ落とし、シンプルかつ洗練された UI を提供。運用者に必要な UI へと継続的な開発、改善を実施します。



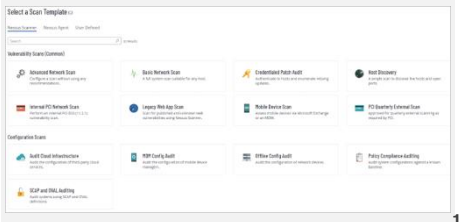
特定の脆弱性を調査

特定の脆弱性が組織内に存在しているかどうかを容易に確認可能。 CVE 番号やキーワード検索などのフィルタリングを用いて、調査したい脆弱性が存在しているかどうかを最新のスキャン結果に基づき可視化します。



スキャンテンプレート

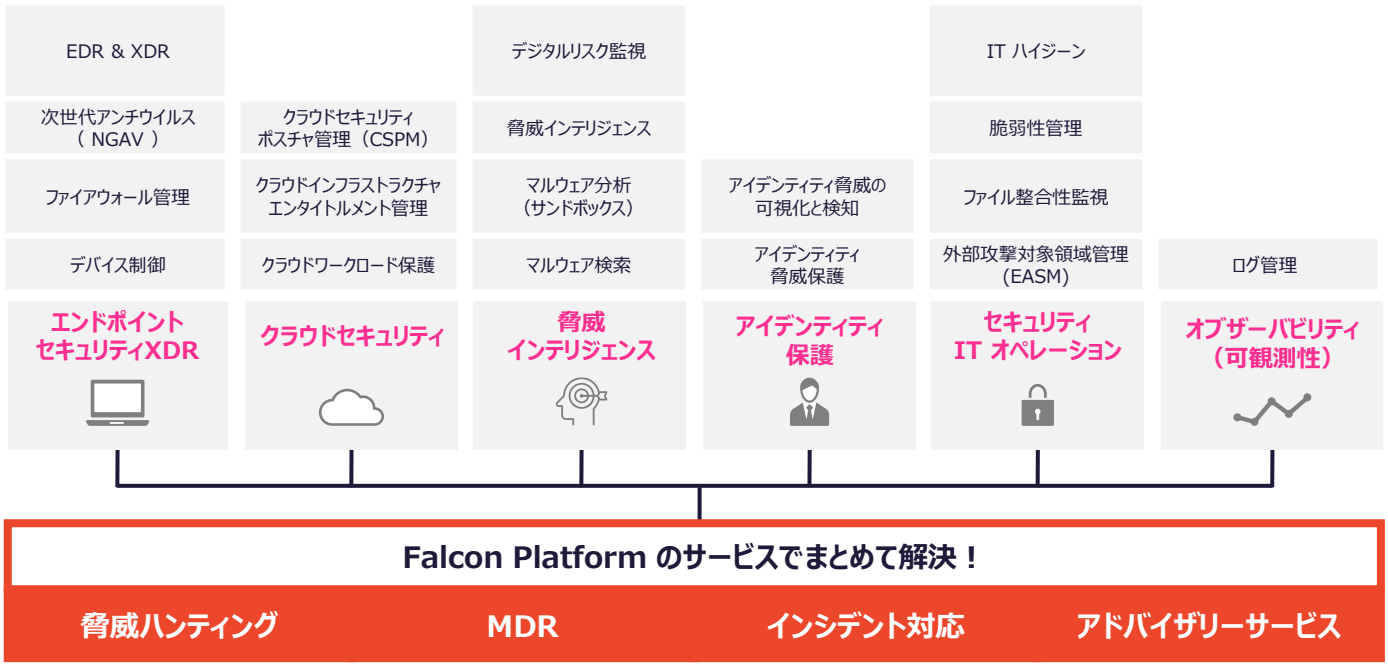
事前設定済みのスキャンテンプレートを使用すると、検証のためのスキャンを実施する前に、スケジュールに従って不良部分をスキャン、修復および提起することができます。



CROWDSTRIKE

リモートワークやクラウドサービスの利用拡大が進んでいる中で、昨今エンドポイントを狙うサイバー攻撃が高度化そして巧妙化していますクラウドストライクは、次世代アンチウイルス（NGAV）とエンドポイントでの検知と対応（EDR)、デバイス制御、脆弱性評価、IT 衛生管理が一体化された、クラウドで提供されるソリューションです。新しい攻撃手法対策として、セキュリティ侵害を効果的に検知・防御します。

1 つのプラットフォームで様々なセキュリティの課題を解決します



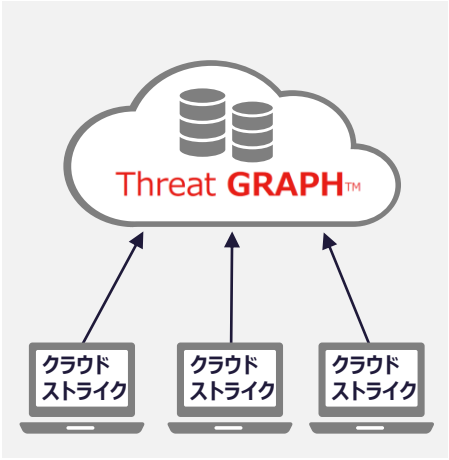
従来型と次世代型のアンチウイルスの機能の違い

	従来型アンチウイルス	次世代型アンチウイルス
新しい攻撃への対処能力向上（ファイルレス攻撃・正規のアプリケーションを悪用）	×	○ 定義ファイルで検出できない脅威への対応
リアルタイムな振る舞い分析による脅威の検出	×	○
検知時の詳細状況把握	× ファイル単体のみ	○ 侵入経路の特定、振る舞いの状況
定義ファイルの更新	必要 定期的な更新が必要	不要 定義ファイルなし
定期的なスキャン	必要 最新の定義ファイルによるスキャン	不要
端末の負荷	高負荷	低負荷
端末の対処機能	抜線等必要 ユーザーの負担あり	即時隔離可能 管理者側から可能

クラウドストライク を選ぶ理由

1 クラウドネイティブ：常に最新の脅威情報で防御

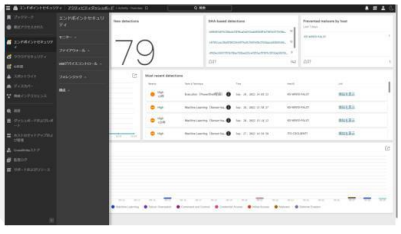
高度化、巧妙化する脅威に素早く対処するためには、最新の脅威情報をいち早く共有するためのプラットフォームが必要不可欠です。クラウドストライクはプラットフォームをクラウド化することで、全世界176 か国以上のユーザーからの膨大なログ(1日10億以上)をリアルタイムに収集・解析しています。これにより、最新の脅威からの素早い保護を実現しています。セキュリティ業界最大のクラウド分析プラットフォームである Threat Graph を利用することで、過検知・誤検知の少ない高精度な防御を実現することが可能となっています。



2 シングルエージェント：管理者と PC への負荷を大幅に軽減

次世代型アンチウイルス / EDR ほか様々なモジュールが、1つのエージェントとして機能し、エンドポイントがオフラインの時にも保護を提供します。軽量なエージェントであるので、エンドポイントの本来のパフォーマンスを妨げることなく監視を行い、然るべきタイミングで防御を実現します。
単一の機能を持つセキュリティ製品を複数導入する場合(マルチコンソール)と比べ、ブラウザのシングルコンソール上で管理が完結するため、管理者にとって運用、管理、機能拡張が簡単です。

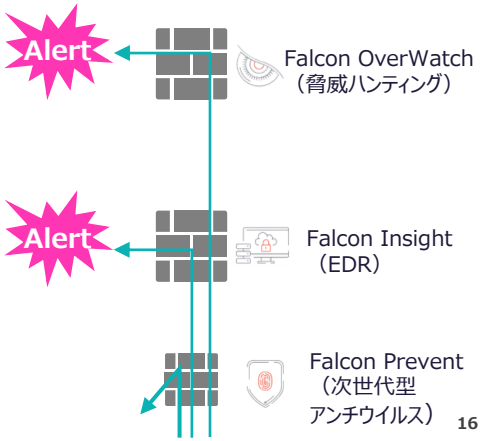
豊富なセキュリティソリューション



シングルコンソール

3 脅威ハンティング：セキュリティの専門家・プロによる 24 時間 365 日監視

次世代型アンチウイルス / EDR でも防御しきれない、さらに高度な侵入に対しては、いかに早く攻撃を検知するかが重要になります。
元 FBI やホワイトハッカーなど、セキュリティの専門家・プロが 24 時間 365 日体制で監視を行い、Threat Graph から解析された最新の脅威情報を基に高度な攻撃の検知、影響範囲の調査、対処法のアドバイスを行います。10 年以上の実績がありますが、脅威ハンティング由来の過検知、誤検知は今までで一回もございません。



クラウド型のIT資産管理ツール

ISM CloudOne

セキュリティ脅威から企業の端末を守る！

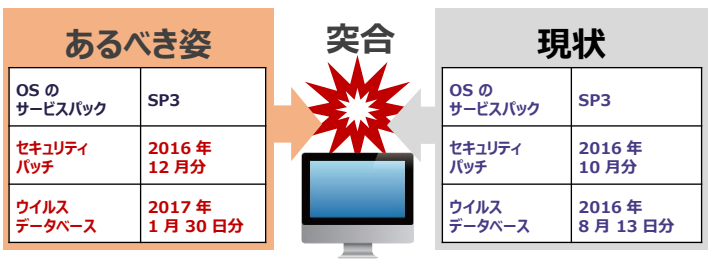
標的型攻撃対策や内部不正防止に有効なクラウド型 IT 資産 ＋ セキュリティ管理ツール。ロケーションフリーで、どこにいても管理対象すべてにポリシーの適用と脅威対策の実現が可能です。

特長1　国内・海外拠点のマルチデバイスを一元管理

社内ネットワークだけでなく、外出先や海外など利用環境を問わず、PC / スマートデバイスを一元管理することができます。

特長2　脆弱性を自動で診断、すぐに是正

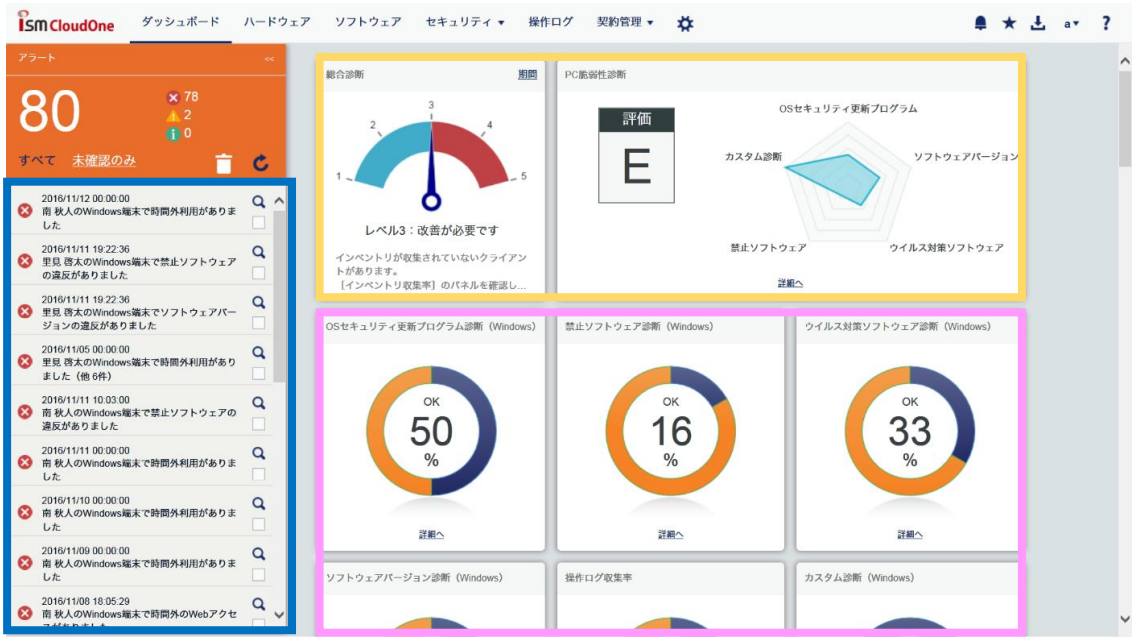
日々変わるセキュリティ脅威に対して、「理想のセキュリティポリシー」を毎日更新し、管理端末の現状と突き合わせて自動で診断。NG項目はユーザー側で是正できます。



特長3　ふるまい検知で未知の脅威にも対抗

ウィルス対策ソフトでは防げない未知の脅威のふるまいを検知し、情報漏えいを未然にブロックします。

必要な情報・問題点が一目でわかるダッシュボード



違反行為や問題点を
アラートで表示

企業全体の
セキュリティレベルを 5 段階
で評価

操作ログアラートや
OS のパッチ更新状況
などを個別にグラフ化

日本語・中国語・英語に対応

かんたん操作で管理工数を削減する、充実の機能

- 自動脆弱性診断
- 操作ログ取得
- 外部デバイス制御
- ふるまい検知
- URL フィルタリング
- ハードディスク暗号化
- IT 資産管理
- スマートデバイス管理
- グローバル対応

無料で！

30 日間の**トライアル実施中！**

自社のセキュリティ状態を
チェックしてみませんか？

何度でも！

eラーニングの受講ができます！

ご購入前の評価および運用後の教育
としてご活用いただけます。

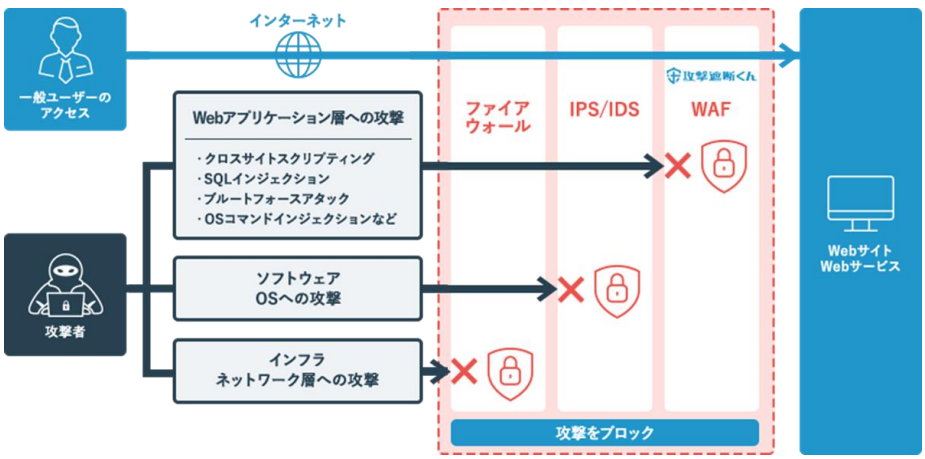
クラウド型 Web Application Firewall

攻撃遮断くん

セキュリティ技術者不要で新たな脅威に瞬時に対応 ！クラウド型 WAF

Web セキュリティ対策の重要度が増す中、「攻撃遮断くん」は、あらゆる Web システムに導入可能な、独自開発のクラウド型 WAF（Web Application Firewall）サービスです。

WAF は、SQL インジェクションやクロスサイトスクリプティング（XSS）をはじめとした不正侵入による情報漏えいや Web サイト改ざんなどを防ぐファイアウォールです。
WAF は、従来の FW（ファイアウォール）や IDS / IPS では防ぐ事ができない攻撃にも対応します。



- Web サービスからの **個人情報の窃取**
- サービス妨害攻撃による **サービスの停止**
- Web サイトの **改ざん**
- Web サービスへの **不正ログイン**
- 対策情報の公開に伴い公知となる **脆弱性の悪用**

重大な脅威を WAF で対策 攻撃遮断くん

「攻撃遮断くん」は、クラウド型の WAF（Web Application Firewall）製品です。情報漏えい、Web 改ざん、サーバーダウンを狙った Web サイトや Web サーバーへの攻撃を遮断することにより、Web セキュリティへの脅威から企業とユーザーを守ります。クラウド型のため、保守・運用に一切手間をかけることなく、24 時間 365 日の高セキュリティを実現します。また、業界で唯一の ”サイバー保険” を付帯しています。

公開サイトの数が多くて、対策するサイトを決めることが難しい。

あらゆる Web システムに導入可能

他社の WAF では導入が困難な高トラフィックの Web サービスにも対応する独自開発のクラウド連動型 WAF を提供。

すべての公開サイトを対策すると、予算が膨大になるのではと不安。

クラウド型 WAF 唯一の定額制

Web サイト数やトラフィック量の増加に関わらず一定額でご利用いただけるプランを提供。

自社での WAF 運用が難しい。日本語のサポートを受けたいので、海外製品では不安。

国産だからできる 万全のサポート体制

24 時間 365 日の技術サポート体制で個別カスタマイズにも柔軟に対応。

サービスラインナップ

サーバセキュリティタイプ

1. 様々な環境での導入が可能
クラウド型（SaaS）のため、各社様のクラウド環境（IaaS）に対応しております。

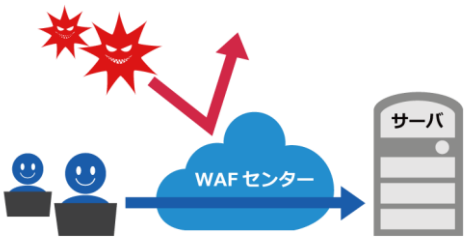
2. サービスへの影響なし
通信はクラウド上の攻撃遮断くん監視センターとのログのみとなるため、障害発生時にもお客様側のサービスに影響しません。

サーバーに攻撃遮断くんのエージェントをインストールして、アクセスログ / システムログをクラウド上の監視センターに送ります。クラウド上で攻撃の判定をし、遮断命令を出してサーバーを攻撃から守ります。

Web / DDoS セキュリティタイプ（WAF + DDoS 対策）

1. ネットワーク構成変更やサーバー停止は不要
担当者様の作業は DNS の切り替えだけ。簡単に導入が可能です。

2. DDoS 対策機能（DDoS セキュリティタイプ）
WAF では防御できない DoS / DDoS 攻撃を、お客様ネットワークより上位のネットワーク側で検知、軽減します。



SaaS / クラウドの形で提供するタイプ。お客様のシステムに変更を加えることなく、DNS を切り替えるだけで簡単に導入可能です。WAF センターを経由して、正規のアクセスはそのまま通し、不正なアクセスは WAF センターで遮断します。

重大な脅威を WAF で対策

WAF では防御できない DoS / DDoS 攻撃を、お客様ネットワークより上位のネットワーク側で検知、軽減することにより、サーバーやネットワーク機器、インターネット回線までを含めた防御が可能です。

お客様ネットワークに最適化したポリシー

サービス開始前に防御対象ネットワークのトラフィックを学習、分析します。その結果から防御ポリシーを設定することで、精度の高いクリーニングを実現します。

不正なトラフィックを選択的に遮断

トラフィックのモニタリングを実施し、異常を検知した場合はお客様サーバーやネットワーク宛のすべての通信をアンチ DDoS システムへ引き込みます。そこで通信の精査と不正なトラフィックのクリーニングを実施し、正常な通信だけをお客様サーバーやネットワークへ転送します。

◆防御できる DoS / DDoS 攻撃の代表例

・TCP
　（Syn flood, Ack flood, Fins flood, Fragments）
・HTTP GET / POST Flood
・HTTP Slow Attack Protection
・ICMP（Unreachable, Echo, Fragments）
・Connection Exhaustion
・Ping of Death
・TCP 不正フラグ

※ セキュリティ上、一部のみ公開しています。

AWS WAF / Azure WAF 自動運用サービス

WafCharm

WAF 自動運用サービス WafCharm とは、煩雑な AWS WAF / Azure WAF /Google Cloud Armor のルール運用を最適化させる WAF 自動運用サービスです。WafCharm を利用することで、専任のセキュリティエンジニアを必要とすることなく、各クラウドプラットフォームのWAFを効率的に運用をすることが可能になります。
ユーザー登録と WAF 設定情報を WafCharm に登録するだけのわずか 2 ステップで AI × ビックデータにより Web サイトごとにお勧めのシグネチャを判別して提供・自動運用します。

WAF 運用の課題

ルール作成

最適なルールの作り方がわからない

防御力が高く、アプリケーションの妨げにならないルールを作る専門知識がなくて困ってる。

網羅性

適用したルールで防げているか不安

決められた制限の中で設定したルールで網羅性が担保されているか不安。

アップデート

新規脆弱性への対応は？

新規の脆弱性が発見された場合に、すぐに攻撃方法を理解し適切なルールを作成する余裕が無い。

誤検知

誤検知対応はどうしたら良い？

運用開始後に誤検知した場合の対応方法が分からない。

WafCharm の 3 つの製品コンセプト

より強力な防御を

AWS / Azure 環境にベストな本格 WAF を提供

1. お客様ごとに最適な防御
- 最適シグネチャを自動選択※1
- カスタマイズ可能
- シグネチャの新規作成可能

2. 数百ものシグネチャでより強力に
- ルール 10 個※1では漏れる可能性も
- 漏れたものは数百におよぶシグネチャで再マッチング
- 再マッチングで攻撃認定したものは Blacklist に自動登録

楽に

AWS WAF / Azure WAF を手放しで自動運用

1. 導入も運用も楽に
- 専用機器設置や DNS 切り替え不要
- 自動で最適なルールを選択
- ルールを自動変更しない場合は、固定することも可能

2. 新たな脆弱性への対応不要
- ルール 10 個※1では漏れる可能性も
- セキュリティリサーチャーが監視
- 新規シグネチャを迅速に作成
- 作成したシグネチャを適用

安心して

日本のお客様を熟知した安心の日本語サポート

1. 何か困ったらサポートへ
- 日本人による日本語サポート
- 24 時間 365 日の技術サポート
- 継続率 99 % を誇るサポート※2

2. AI でカバーできない領域は人によるサポートで安心
- 誤検知対応
- ルールの手動入れ替え
- カスタマイズにも柔軟に対応

※1 aws waf classicの場合
※2 攻撃遮断くんの実績

AI × ビックデータによる WAF 自動運用 = WafCharm

ビックデータ	×	AI
国内 1,000 社、12,000 サイト以上の企業情報を守ってきたデータ		Web サイトごとにピッタリの防御方法を判別して自動運用

料金プラン (税抜)

無料トライアル	ビジネスプラン	エンタープライズ
30 日間 **無料**	**112,000** 円 / 月 ～	**192,000** 円 / 月 ～

◆料金詳細 / 機能比較		無料トライアル	ビジネスプラン	エンタープライズ
月額料金 A + B + C	(A) Web ACL / WAF policy 利用料金 ※1	30 日間無料	12,000 円	12,000 円
	(B) プラン料金 (Web リクエスト数) ※2	30 日間無料	**100,000 円** (1,000 万件まで)	**180,000 円** (1 億件まで)
	(C) Web リクエスト数 追加料金	30 日間無料	900 円 / 100 万件	**400 円 / 100 万件**
シグネチャの自動適用 (AWS WAF、Azure WAF ともに)		○	○	○
メールサポート		○	○	○
手動ルール入替		○	○	○
24 / 7 サポート		-	○	○
シグネチャカスタマイズ		-	○	○
Web サイト改ざん検知機能			○	○
静的 Blacklist や Whitelist の即時反映 ※3			○	○
シグネチャ再マッチングによるブラックリストの 5 分毎更新 ※3			○	○

お得！

※1 Web ACL / WAF policy のご利用料金は日割り課金です。ご利用の Web ACL / WAF policy ごとに計算致します。
※2 Web リクエストは WafCharm の 1 アカウント単位で合算されます。
※3 AWS 版のみの対応となります。別途 AWS WAF / Azure WAF/Google Cloud Armorの利用料金が掛かります。詳しくはこちらをご確認下さい。
AWS : https://aws.amazon.com/jp/waf/pricing/ Azure : https://azure.microsoft.com/ja-jp/pricing/details/web-application-firewall/
Google : https://cloud.google.com/security/products/armor

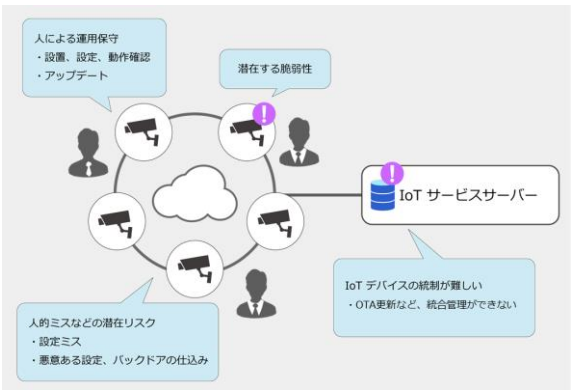
IoT の設計から開発、量産、運用まで
一貫性のあるセキュリティ対策のための証明書を提供

kusabi のコンセプトは、さまざまなデバイスに最適な情報セキュリティの 3 要素である CIA を兼ねた証明書鍵（デジタル ID）を提供することです。ブロックチェーン技術を電子証明サービスに応用し、各デバイスごとにユニークな証明書鍵で論理的保証を得る仕組みにより、従来の機密性（Confidentiality）、完全性（Integrity）、可用性（Availability）に加え、真正性（Authenticity）も提供します。

kusabi の『信用』が実現する 3 つの不要

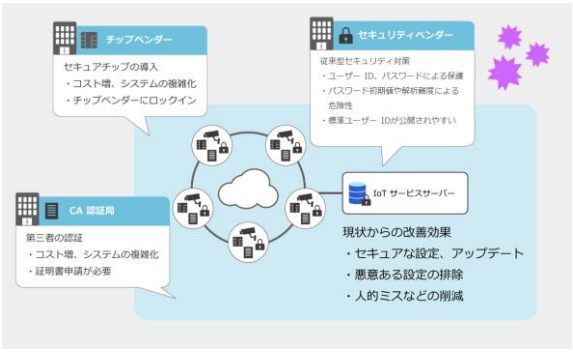
セキュリティの現状

現在の IoT セキュリティ対策は、既存の PC セキュリティ対策（ID、パスワード）を踏襲した手法が多く見受けられます。
しかし、IoT のビジネスユースケースではデバイスが主役であるため、従来のセキュリティ対策では不都合が生じることも多々あります。
多様性が前提の IoT では、ワクチンそのものが流用しにくいため、対策が困難です。膨大なデバイスの統制自体がリスク要因であり、統制から漏れてしまったデバイスが、社会インフラを破壊してしまう可能性も十分にあります。



現状の解決策と新たな課題

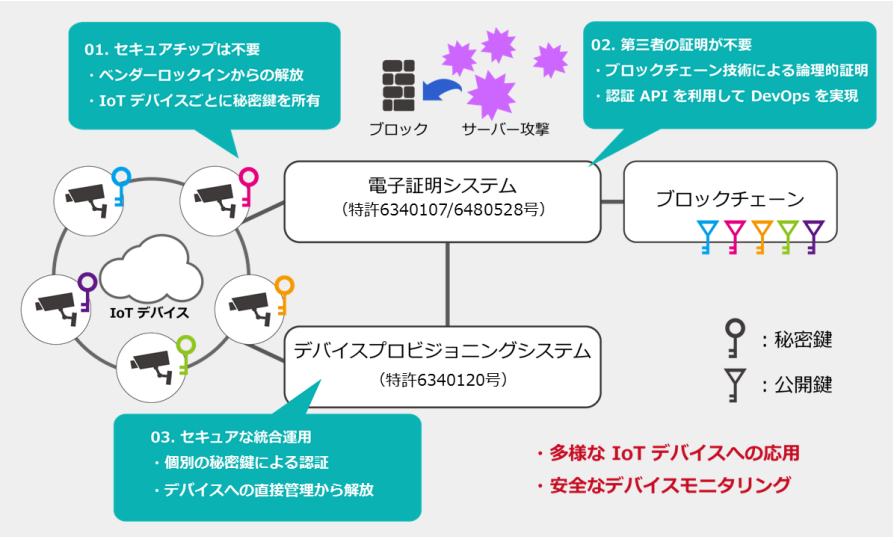
深刻化する IoT セキュリティ対策として、専用チップと CA（認証局）によるセキュリティモデルが注目されています。セキュリティとしては有効な施策ですが、製造コストおよび運用コストに対する投資を考慮する必要があります。また、専用チップのベンダー依存が高まるため、調達面など製品開発での課題や考慮点が増えます。
さらには、大量のデバイスから CA（認証局）へ問い合わせが集中することにより、トラフィック障害が発生することも想定されます。



NEXT：kusabi モデルによる課題解決▶

kusabi モデルで実現する IoT デバイスの課題解決

kusabi モデルでは、ブロックチェーン技術による電子証明システムと、独自のデバイスプロビジョニング技術による新たな発想の鍵を採用することで、ブロックチェーンや PKI（公開鍵暗号基盤）、API を活用した電子証明鍵によるセキュリティ対策を実現します。
これにより、デバイス進化への柔軟な対応やコスト削減が可能になり、さらにソフトウェアにより実現しているため、さまざまな環境への適用やデバイスへ活用することができます。



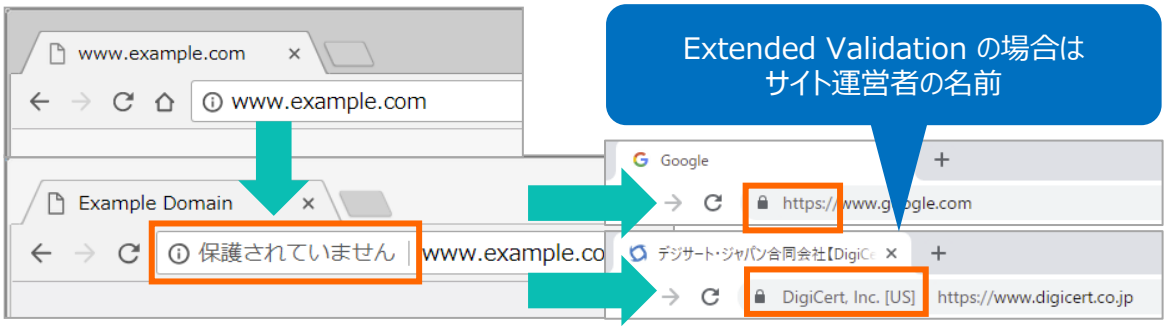
kusabi モデルと従来の IoT セキュリティの比較

		kusabi モデル	専用チップ ＋ CA（認証局）モデル
プレイヤー	チップベンダー	【不要】kusabi の電子証明システムを活用（環境構成により）	【必須】生産段階で出荷予定台数分の専用チップのハードウェアモジュールに鍵を書き込む
	CA（認証局）	【不要】kusabi の電子証明システムを活用	【必須】出荷段階で上記のハードウェアモジュールの鍵を使用してデバイス単位に電子証明書を発行および管理
	IoT デバイスベンダー	【必須】kusabi のデバイスプロビジョニングシステムの API を活用した起動・初期化プログラムを組み込む	【必須】CA 提供の PKI ライブラリによる起動ならびに初期化プログラムを組み込む
	インテグレーター	【必須】kusabi のデバイスプロビジョニングシステムの API を用いたエッジサーバーを提供	【任意】チップベンダー・ CA ・セキュリティベンダーのオーケストレーターとして存在
コスト		kusabi のライセンス費用のみ	チップベンダー・ CA ・セキュリティベンダーの各プレイヤーごとにライセンス費用が発生
汎用性		インテグレーターにてユーザーごとにカスタマイズしたシステムを提供可能	チップベンダー・ CA ・セキュリティベンダーの各プレイヤーによる提供システム（サービス）にロックインされる

digicert®

Web サイトは HTTPS がスタンダードな時代に突入

2018 年 7 月から国内市場シェア 52 % ※ の Chrome で、HTTP サイトは警告が表示されています。そのため、できるだけ早く、自社サイトの HTTPS 化を進める必要があります。

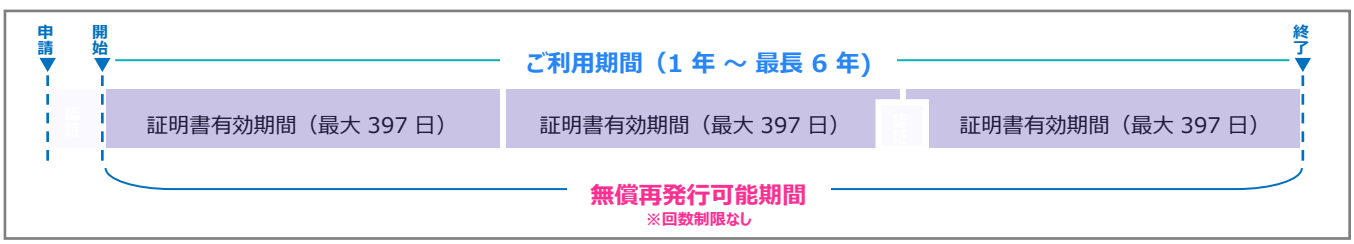


※出典元：StatCounter（2017/8 ～ 2018/8） http://gs.statcounter.com/browser-market-share

いま選ぶなら、常時 SSL + EV SSL 証明書

公共無線 LAN の普及や Google による HTTPS サイトの SEO 優遇方針の発表などの動きを背景に、Web サイト全体を SSL / TLS 化して保護する「常時 SSL 化」がトレンドとなっています。
EV SSL 証明書による常時 SSL 化で暗号化通信はもちろん、サイト全ページのアドレスバーで緑色表示＋運営団体名表示が可能です。Web サイトの身元がサイト利用者に明確に伝わり、大きな安心感を与えるとともに、なりすましサイトやフィッシング詐欺の抑止策としても効果的です。

複数年プランで SSL 証明書の利用を長期的にお得に！



◆1 年～ 6 年までの複数年プランから選択が可能です。長期であるほどお得になります。
◆各プランの料金は基本的にお申し込み時のお支払いとなるため、OV / EV 証明書の予算管理が長期間を見据えた 1 度で済み、毎年の稟議や予算を設ける必要がありません。
◆利用期間が終わる前に複数年プランの延長や、プラン延長時に FQDN 追加も可能です。
※バウチャー利用のプラン延長は有効期間の 90 日前から可能です。追加の場合は、プラン延長時に追加料金が必要です。
◆OV / EV 証明書の有効期間は利用期間中、業界共通の最大 397 日の有効期間内で設定が可能です。
※ Web サーバー等へ証明書の入れ替え（再インストール）作業が必要です。
◆必要に応じて期間内であれば証明書を何度でも再発行・有効期間の調整が可能です。
※御社のタイミングで証明書の入れ替え（再インストール）する時期の調整ができます。

SERVICE

運用サービス
レポーティング（性能評価レポート）
定例会によるITライフサイクル支援
定期メンテナンス等の各種運用代行

アセスメントサービス
IBC-PAS（遅延調査/改善支援/トラブルシュート）
IBC-SAS（脆弱性診断、セキュリティリスク調査）
IT障害119（IT障害解決支援）

監視サービス
IBCのノウハウが集約された最適な
監視手法で24時間365日安定稼働を実現

保守サービス《IBC Care》
保守一次窓口から、脆弱性のパッチ適用まで
まるっとお任せ

クラウドインテグレーション
既存環境を考慮し、全体最適を実現
環境変化に柔軟に対応可能で、ビジネスを
阻害しないプラットフォームを提供

ネットワークインテグレーション
LAN、Wi-Fi、SD-WAN、SASEなど最新の
トレンドを踏まえ、ユーザーのニーズに合わせて
将来を見据えた環境をマルチベンダーで提供

次世代 MSP サービス

SAMS

IT 管理者の皆様
こんなお悩みありませんか？

エンドユーザーからの原因不明のトラブル

- Web 会議が繋がらない
- Wi-Fi が遅い
- 拠点から繋がらない

セキュリティ対策

- 脆弱性パッチ対応が多く、対応できない
- 事故が発生した場合の相談先が分からない

運用支援が欲しい

- 日々の運用に手が回らない
- トラブルが発生しても原因と対応が分からない

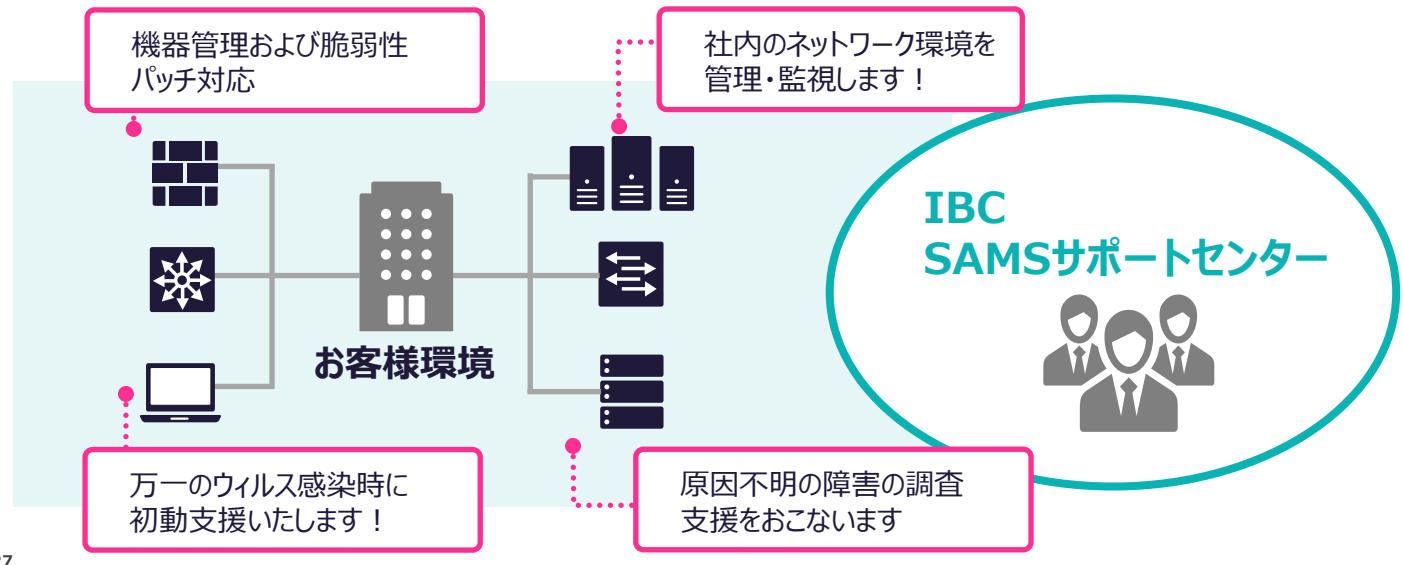
相談先が多数

- 機器購入先に相談しても、明確な回答が得られない
- 海外製品なので調査時間がかかる

IT よろず相談をお受けします！

SAMS サービス

ITのお困りごとのご相談をお受けします！
些細なことでもOK！まずはご相談ください！



SAMS 関連ソリューション

SAMS運用代行サービス

即時検知
24 時間 365 日体制で
即時対応が可能

障害復旧支援
1 次対応から障害対応の
レポート作成までを代行

コスト削減
自社管理ではなく
サービス利用によりコスト削減

System Answer シリーズ

システム監視ご要望

・予防保守　・アラート一次受け
・問題の最適な切り分け

性能レポート

性能情報を可視化し

・稼働状況レポート
・設備計画レポート

コンサルティング

当社技術員が

・障害の原因究明
・改善提案

IT 障害 119 レスキュー

IT 障害が発生した際などの突発的なお困り事に対して、原因究明や技術的な支援を実施するサービスです。また、今後の IT インフラをどうしていくべきかをご検討される際のご相談窓口を提供し、将来的に障害を発生させないインフラ環境を目指すことを目的としています。

24 / 365 受付対応
Web 会議などによるヒアリングを行い、事象の調査を実施

どなたでもご利用可
21 年間で培った運用・分析ノウハウを持ったプロが対応

セキュリティ
セキュリティインシデントの初動対応支援

SAMS　性能評価レポートサービス

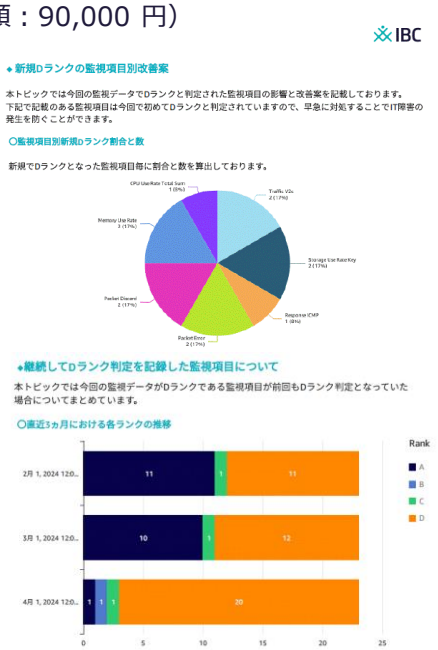
SAMS / System Answer G3 にて蓄積したデータを月次分析サービス（月額：90,000 円）

データ収集

System Answer G3 および SAMS にて収集したデータを IBC へ定期送付（バッチ）

分析・解析

グラフレポートではなく、数値的根拠より分析した結果、診断結果を表示
Dランク～Aランクでの解析結果を月次で表示。
定常的にリスクの高いものから、リスクが上がってきた機器を即時判断可能（3か月傾向分析）



IT 障害を解決するコンサルティングサービス

IT 障害 119 レスキュー

21 年間培った運用・分析ノウハウや知見を活かし、IT 障害を解決するコンサルティングサービスをご提供

ネットワークシステムの性能監視に長年携わってきた性能分析のノウハウを活かし、 IT 障害が発生した際などの突発的なお困り事に対して、原因究明や技術的な支援を実施するサービスです。また、今後の IT インフラをどうしていくべきかをご検討される際のご相談窓口を提供し、将来的に障害を発生させないインフラ環境を目指すことを目的としたコンサルティングサービスです。

日々の業務でこんな 課題 はございませんか？

- NW遅延やシステム障害が発生したが、切り分け方法が分からず、解決に時間がかかってしまった
- IT インフラの専任担当者がおらず、専門家の見解やサポートを受けながら適切な対応を行いたい
- セキュリティインシデントが発生した際、何から手を付ければいいか分からない
- 根本原因が分からないまま自然復旧した事象があり、いつ再発するか不安である

ひとつでも該当した場合！

ぜひ IT 障害 119 レスキュー をご検討ください。
弊社がお悩み解決のご支援をいたします。

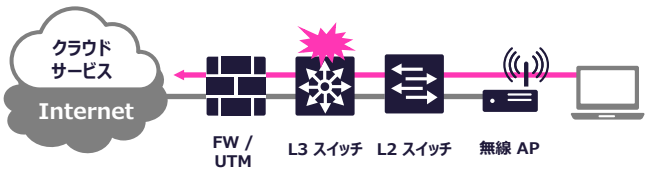
よくあるお悩みとサービス活用例

根本原因が分からないまま自然復旧

ネットワーク機器導入後のドキュメント更新ができておらず、どのような構成になっているのかわからない。トラブルが発生した際にも、構成が不明で最新のコンフィグ情報も無い状況であるため、原因の切り分けができない。

運用・分析ノウハウを元にトラブル原因を迅速に切り分け！

トラブルが発生した際、Web 会議などによるヒアリングを行い、事象発生箇所やタイミング、ログの内容から原因切り分けをし、迅速なトラブル解決に貢献します。



サービス内容

障害の切り分けから被疑箇所の洗い出しを 24 時間 365 日、無償にて提供する緊急障害対応支援サービスです。全てのお客様が対象となります。G3 ご利用中のお客様は、G3 の画面上にある「119」ボタンからの受付も可能です。

	IT障害119レスキュー	
対象	全てのお客様	System Answer シリーズ及び SAMSご利用中のお客様
受付方法	専用フォーム	専用フォーム/電話（※）
時間	受付：24/365 対応：24/365	
緊急対応	初動対応 ーWeb会議によるヒアリング/状況把握 ー被疑箇所の洗い出し ー本調査方針の報告	
本調査	必要に応じて別途見積	
費用	最大2日間までは無償で対応	

※専用受付フォーム：https://system-answer.com/contact/it119_contact/
電話番号は、ユーザー様専用フォーム上に記載されております。

24 / 365 受付対応

障害時に 24 / 365 受付・対応

Web 会議などによるヒアリングを行い、事象の調査を実施

どなたでもご利用可

21 年間で培った運用・分析ノウハウを持ったプロが対応

セキュリティ

セキュリティインシデントの初動対応支援

障害時の切り分け支援・脆弱性情報の提供・パッチ適用サービスをワンストップで提供

IBC Care サービス

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？

- 専任の保守要員がいない。機器の運用ができていない。
- コンフィグの管理ができていない。ネットワークに詳しくない。
- 脆弱性情報の取得や対応まで手が回らない。
- 保守連絡先を一本化したい。ひとり情シスで業務過多。

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。

窓口対応
導入機器に対する一般的な問合せ窓口対応を行います。

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。御見積作成。

ライセンス更新
ライセンスの確認から、ご要望に応じて適用まで行います。

障害調査
ログの調査、リリースノートの確認などの調査を行います。

メーカー対応
ソフトウェア起因の障害の場合、メーカーへのエスカレーションを行います。

代替機手配
ハードウェア障害の場合、メーカーへ連絡のうえ、代替機の手配を行います。

脆弱性管理
注目!!

脆弱性情報の入手、緊急パッチ適用を行います。

コンフィグ管理
注目!!

適用したパッチ情報や送付頂いた設定情報を管理します。

注目!! …UTM管理において最も重要な項目。一般的な保守サービスにはない、アイビーシーならではのメニューです！

アイビーシーは、お客様環境を把握し最適化する**性能分析サービス**・将来を見据えた最適なネットワークインフラを構築する**インテグレーションサービス**・導入後の機器保守を行う **IBC Care サービス**・24 時間365日監視でシステムの安定稼働および障害対応をサポートする **SAMS** の 4 つのソリューションで、お客様のニーズに合わせた最適なソリューションを提供します。

Q&A

アイビーシー の提供する **・IBC Care** **・IT 障害 119 レスキュー** **・SAMS アドバイザリー** のサービスの違いは何ですか？	**IBC Care** は、個別機器に対する保守サービスメニューです。 **IT 障害 119 レスキュー**は、障害被疑個所の切り分けを行う、緊急障害対応支援メニューです。 **SAMS アドバイザリー**は、IT インフラ全体を包括的に見た上で、障害発生状況の確認 ～ 改善対処まで実施する技術支援メニューです。
もともと別ベンダーから導入した FortiGate を、IBC Care で見てもらえますか？	はい。ライセンス・ソフトフェア保守・ハードウェア保守を含めて弊社経由で契約いただければ対応可能です。
IBC Care の購入単位は何年 / 何か月ですか？	メーカーのライセンス・保守契約の年数に応じた期間となります。

自社の抱えるリスクを可視化する

セキュリティリスク分析『V-Sec』

攻撃者に狙われるサプライチェーン

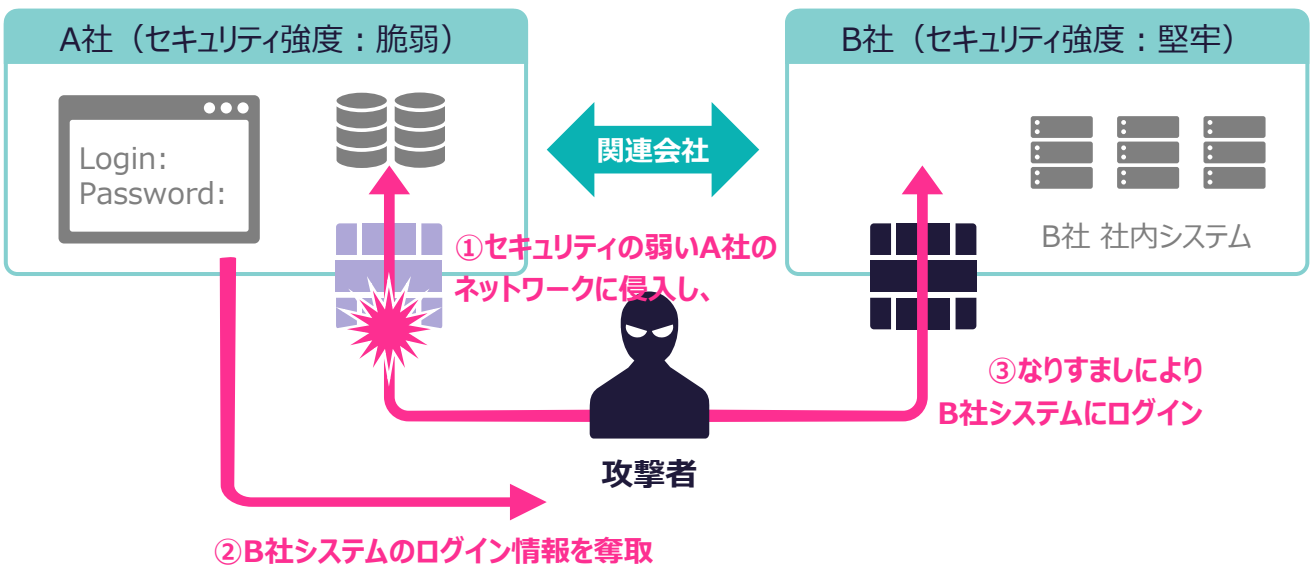
IPAの公開する「情報セキュリティ10大脅威 2024」において**「サプライチェーンの弱点を悪用した被害」**は2位にランクインしており、6年連続6回目の選出になっています。

同法人の公開する「サイバーセキュリティ経営ガイドライン」では、**「経営者が認識すべき3原則」**、**「サイバーセキュリティ経営の重要10項目」**のいずれにも、サプライチェーンに関する記述がされており、サプライチェーンにおけるセキュリティ対策はますます重要になっています。

攻撃者であるハッカーは、セキュリティの強固な大企業ではなく、**比較的セキュリティの脆弱な中小のサプライチェーン企業を経由**して大企業を狙います。

順位	組織向け脅威
1	ランサムウェアによる被害
2	サプライチェーンの弱点を悪用した被害
3	内部不正による情報漏えい等の被害
4	標的型攻撃による機密情報の窃取
5	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）

引用： IPA「情報セキュリティ10大脅威 2024」



セキュリティリスクに対する適切な対策と自社の状況の可視化

「サイバーセキュリティ経営の重要10項目」の最初のステップとして、**「サイバーセキュリティリスクの認識、組織全体での対応方針の策定」**が挙げられています。効果的かつ投資対効果の高いセキュリティを実現するための第一歩としてリスクアセスメントにより組織内部のリスクを可視化することが重要です。

セキュリティツールの導入だけでなく、社内規定の見直しや社員教育は実施できていますか？

- **個々のセキュリティリスクの分析と対策すべき優先順位の設定**
- **セキュリティにまつわる規定や運用フローの見直し**
- **費用対効果を考えたセキュリティ対策の立案**

セキュリティリスク分析 V-Sec とは？

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。

V-Sec トライアル

お試しプラン

内容	現状レポート、情報漏洩発生確率
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

V-Sec スタンダード

1 拠点向け

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
目的	各業界の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

V-Sec プレミアム

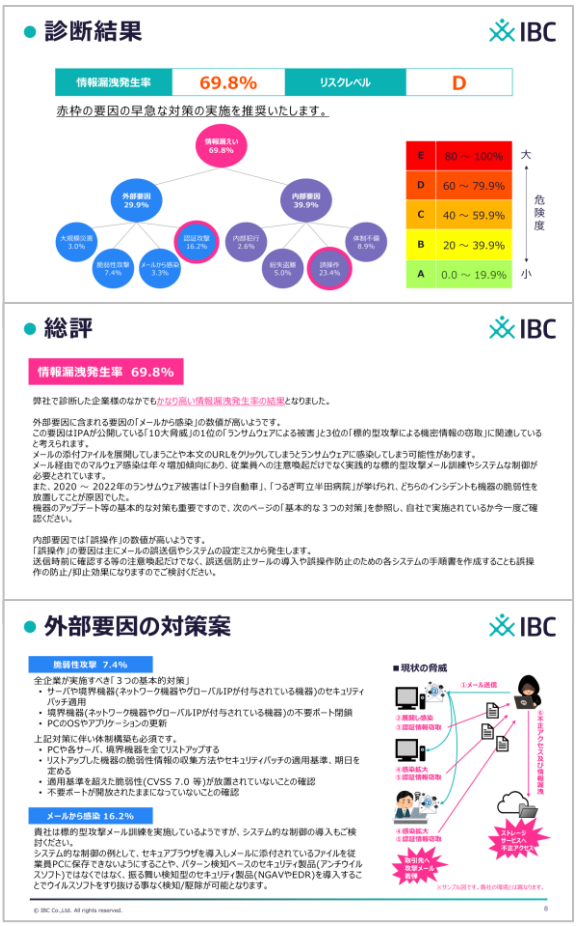
複数拠点向け。スタンダード＋下記

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現場業務とルールとの乖離を調査分析。業務負担となっているルールの見直し等も検討

レポートサンプル （抜粋 / 数値および内容はサンプルです）

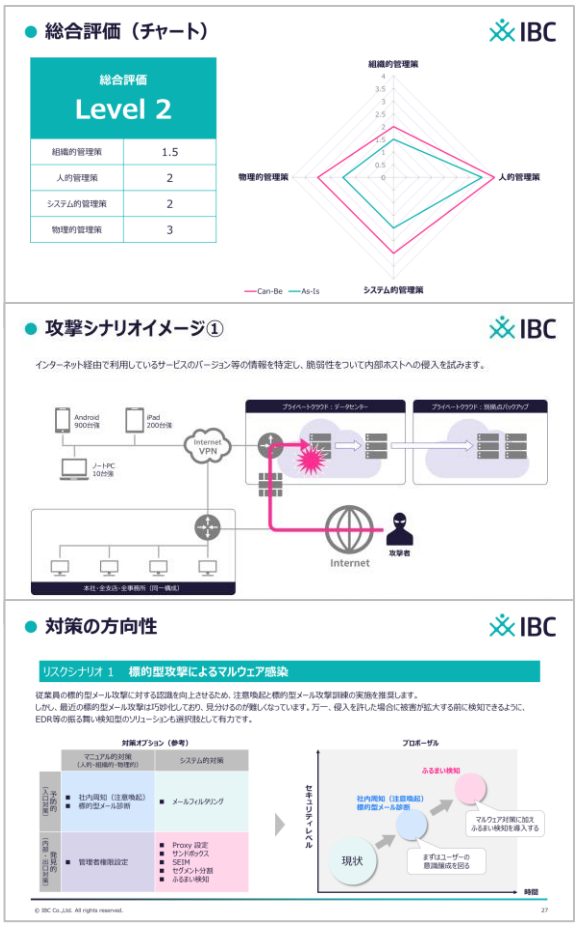
V-Sec トライアル

情報漏洩発生確率と対策ポイントを記載します。



V-Sec スタンダード

より具体的な攻撃シナリオや、対策方針を記載します。



企業情報をモニタリングする

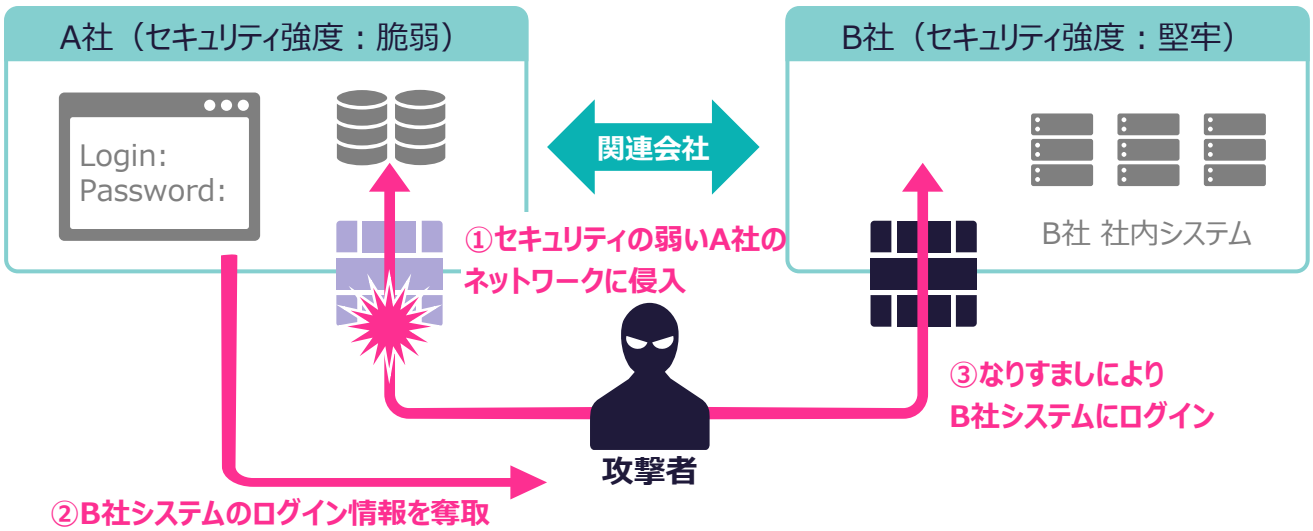
OSINT 調査『Discovery』

攻撃者に狙われるサプライチェーン

IPA の公開する「情報セキュリティ 10 大脅威 2024」において**「サプライチェーンの弱点を悪用した被害」**は 2 位にランクインしており、6 年連続 6 回目の選出になっています。さまざまな規模の企業が存在するサプライチェーンにおいて、大企業と中小企業では**セキュリティ対策への投資にギャップ**があることがしばしば見受けられます。
攻撃者であるハッカーは、攻撃が成立する確率の高い、**セキュリティ対策が手薄な中小企業**への侵入を試みます。

順位	組織向け脅威
1	ランサムウェアによる被害
2	サプライチェーンの弱点を悪用した被害
3	内部不正による情報漏えい等の被害
4	標的型攻撃による機密情報の窃取
5	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）

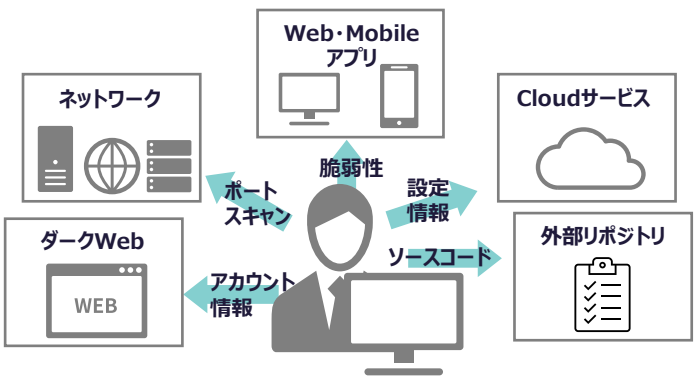
サプライチェーンのネットワークを利用した攻撃



ハッカーは、直接侵入が難しいセキュリティの強固なターゲット組織に対し、**比較的セキュリティ対策が手薄な取引先や子会社（＝サプライチェーンの弱点）などを経由**することで、ターゲット組織へと侵入します。つまり、自社のセキュリティ対策が不十分であることは、関係会社のセキュリティを脆弱な状態にしてしまうことに繋がります。セキュリティ対策は自社のみの問題ではなく、対外的にも重要な要素になっています。

公開情報による情報収集

ハッカーは、公開されている様々な情報を収集し攻撃の準備をします。公開情報には、ホームページやSNSアカウントなどの容易にアクセスができるものから、ダークWebで取引されている**「実際の攻撃手法」**や**「正規のユーザ情報」**なども含まれます。
意図していない情報の公開や、漏えいしているユーザ情報などは、**設定の変更**等で対策可能な



ものもあります。企業の中に存在する「攻撃者を侵入しやすくさせてしまう隙」を潰しておかなければ、攻撃者から目を付けられやすい状況が続き、いずれは攻撃の餌食となってしまいます。各種公開情報の把握とそれらへの対策は急務です。

企業情報モニタリング Discovery とは？

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

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。

簡易調査（PoC）

内容　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）

本調査

内容　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）

レポートサンプル　（抜粋 / 数値および内容はサンプルです）

簡易調査


1. Discovery PoC 簡易レポート

本調査レポートは「企業情報モニタリング Discovery」の PoC 簡易レポートとなります。
正式調査を実施する前の事前調査資料として作成するものであり、全ての脅威情報や詳細情報を掲載するものではありません。脅威度として Critical/High リスク判定された事例のみを抽出して正式調査時に報告されるであろう内容の参照物としてご利用ください。
また、正式調査時には Medium リスク以下の報告や、具体的な漏洩情報と脆弱性予測の詳細情報の取得が実施されます。

2. Web

2.1. 脆弱性 Critical Risk レベル

本調査レポートは「企業情報モニタリング Discovery」の PoC 簡易レポートとなります。
いくつかの Web サイトではライブラリや CMS のバージョンが古いことが観測されています。
Web サイトや Web サービスに構築されている古いコンポーネントは将来的な脆弱性の発現や、攻撃者グループからの侵害ポイントとなる恐れがあります。

3. Mobile

3.1. 脆弱性 Critical/High Risk レベル

本調査レポートは「企業情報モニタリング Discovery」の PoC 簡易レポートとなります。
いくつかのモバイルアプリではライブラリや暗号プロトコルが古いことが観測されています。
Mobile アプリに構築されている古いコンポーネントは将来的な脆弱性の発現や、攻撃者グループからの侵害ポイントとなる恐れがあります。

本調査


2. Web

2.1. 脆弱性 Critical Risk レベル

2.1.1. www.example.edu

Vulnerable URL: www.example.edu

予測される脆弱性の数：9

この AI 主導のスコアは、アプリケーションとその環境から収集されたデータに基づいています。ディスカバリダッシュボードで利用可能な設定ミスに加えて、スコアは、侵入テストで検出される可能性のある悪用可能なセキュリティの脆弱性の数を予測します。スコアは、相互に関連する 3 つの要素で構成されています。

アプリの魅力

毎日のユーザー数、機密データの処理または処理、チェーン攻撃への影響の可能性が含まれます。

スコアは、侵入テストの優先順位を上げるためにのみ提供されます。スコアは毎週更新されます。スコアに直接影響を与える方法はありません。

月間の標的型攻撃の推定数：7

この AI 主導のスコアは、企業とアプリケーションに関して収集された OSINT データに基づいています。スコアは、公開されている情報に基づいて、アプリケーションに対する標的型攻撃の可能性を予測します。スコアは、相互に関連する 3 つの要素で構成されています。

会社の魅力

業界、場所、顧客と従業員の数、メディアの言及、特許、財務が含まれます。

スコアは、侵入テストの優先順位を上げるためにのみ提供されます。スコアは毎週更新されます。スコアに直接影響を与える方法はありません。

フィンガープリント ソフトウェア：

Drupal 8.7.0

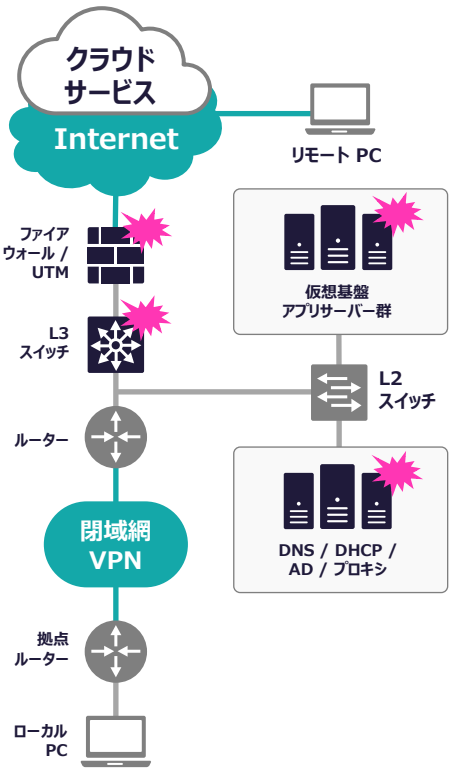
フィンガープリントされた CMS バージョンは古く、公に知られている脆弱性に対して脆弱です。最新バージョン 8.9.0 に緊急に更新します。

CVSSv3.1	CVE-ID	CWE-ID	References
8.7 High	CVE-2019-6539	CWE-20	https://www.drupal.org/sa-core-2019-002 https://www.cybersecurity-help.cz/vdb/SB2018101801
8.5 High	Not Assigned	CWE-434	https://www.drupal.org/sa-core-2019-013 https://www.cybersecurity-help.cz/vdb/SB2018101801

IBC-PAS

新型コロナウイルス感染症の流行し生活様式の変化に伴い、システムの利用方法や負荷状況が以前とは大きく変化しています。たとえば、リモートワークや Web 会議の急増により、システムやネットワークに想定外の負荷が発生し、十分なサービスを提供できない状況に陥ってしまうことがあります。そこで、IBC 性能アセスメントサービス「IBC-PAS」では、ネットワークシステムの性能監視に長年携わってきた経験豊富なエンジニアによる分析をおこない、お客様の ICT インフラの安定稼働を実現します。

ネットワークトラブルの原因として多いこと



リモートアクセスやクラウド利用が増えてから通信が遅い・途切れる

特定の時間帯に不安定になる

オンライン会議のみ調子が悪い

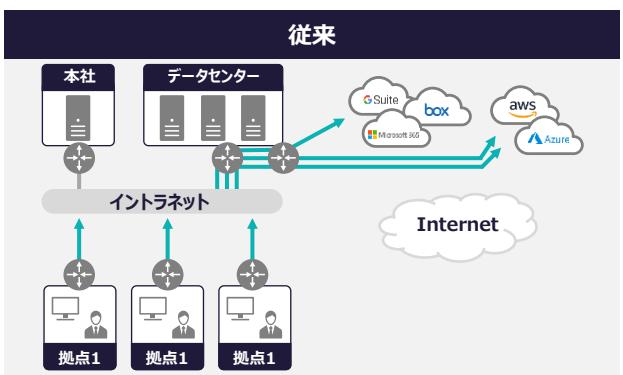
クラウドサービスの応答が遅くなる

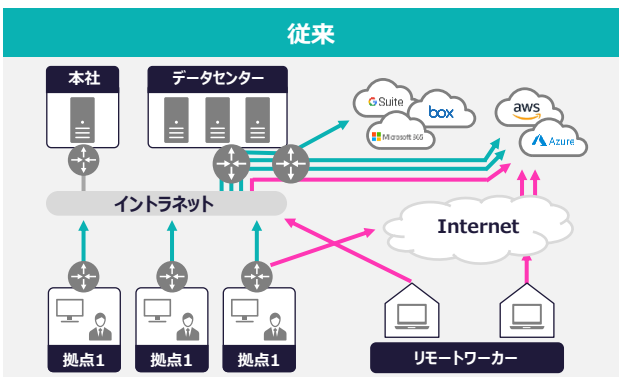
サーバーやネットワークは稼働しているのになぜ？

例えば
- 想定していなかったアクセス追加によるインフラリソースの逼迫
- パケットロスやエラーによる遅延

ICT システムを取り巻く環境の変化と課題

ワークスタイル変革・コロナ禍における企業内コミュニケーション手段の変化に伴い企業のネットワーク環境が大きく変化しています。





課題

- Microsoft 365、box、G suite 利用時の通信レスポンスが遅い
- AWS、Azure 利用時の通信レスポンスが遅い
- Web 会議利用時の音声や画面表示が不安定

要求事項

インフラ環境（ネットワーク、クラウド、サーバーなど）の稼働状況やパフォーマンスの見える化による課題の把握と対策を実施したい

アセスメントサービス

ネットワークシステムの性能監視に長年携わってきた経験豊富なエンジニアが、客観的な立場からお客様の ICT ステムの性能分析をおこなうサービスです。System Answer G3 で個別のシステムを分析するだけでは気づかない、他システムとの比較や相関など、システム全体を俯瞰したうえで分析をおこなった結果を報告します。

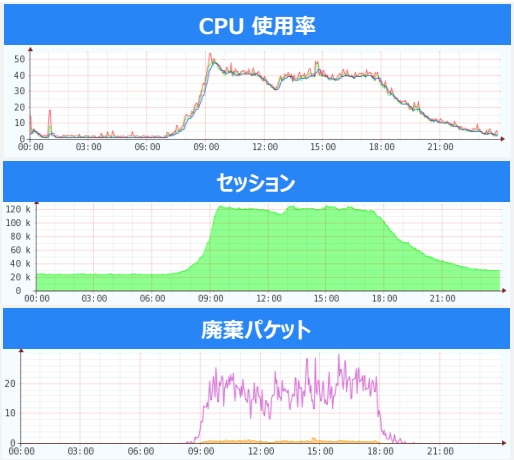
【特長】

- 事前打合せによる的確な評価
- ツールの利用により、人手による情報収集が不要
- マルチベンダー環境に精通したエンジニアによる客観的な分析
- 現状報告だけでなく、システム改善や運用改善まで提案

現状の可視化 | **迅速な問題把握** | **サービスレベルの向上** | **キャパシティ計画の立案**

レポートイメージ

System Answer G3 に蓄積されたデータを分析し、稼働状況報告や改善提案のレポートをスポットまたは定期で作成します。システムの余裕度や性能を把握することで ICT システムを可視化し、安定稼働、予防保守、適切な設備計画の策定に活用いただくことができます。



性能アセスメントに活用するソリューション

ソリューション名称	System Answer G3	Flowmon
貸出機材イメージ		
ソリューション概要	■マルチベンダー環境のICTシステム全般（ネットワーク、サーバー・仮想基盤、クラウド）に対応した「障害予防対策監視ソリューション」です。 ■障害検知を目的に利用される一般的な監視ソリューションと異なり、収集・蓄積した詳細監視データを自動分析（将来予測・変動検知・相関分析など）し、障害発生前の未然防止を促進できることが特徴です。 ■1,000社以上の導入実績があり、公共・文教・医療・社会インフラ・キャリア・民需など様々なお客様のICTシステム安定稼働に貢献しています。	■ネットワークフローを利用した、トラフィック監視・分析・振る舞い検知に特化したアプライアンス製品です。 ■パケット解析と同様の視点による解析が「通信ログを残しつつ、短時間で実現可能」です。 ■ユーザー単位やアプリケーション単位での通信状況を把握でき、直観的な GUI で、効率的かつ高速な解析を実現いたします。 任意 ※トラフィック解析まで行う場合には必要となります。

IBC セキュリティアセスメントサービス

IBC-SAS プラットフォーム脆弱性診断サービス

情報処理推進機構（IPA）が毎年発行している情報セキュリティ 10 大脅威 2025 において、脆弱性にかかわる脅威として「サプライチェーンや委託先を狙った攻撃」、「システムの脆弱性を突いた攻撃」、「機密情報等を狙った標的型攻撃」などがランクインしました。

脆弱性管理の必要性　IPA「情報セキュリティ 10 大脅威　2024」

順位	脅威	昨年順位
1位	ランサム攻撃による被害	1位
2位	サプライチェーンや委託先を狙った攻撃	2位
3位	システムの脆弱性を突いた攻撃	7位
4位	内部不正による情報漏えい等	3位
5位	機密情報等を狙った標的型攻撃	4位
6位	リモートワーク等の環境や仕組みを狙った攻撃	9位
7位	地政学的リスクに起因するサイバー攻撃	-
8位	分散型サービス妨害攻撃（DDoS攻撃）	-
9位	ビジネスメール詐欺	8位
10位	不注意による情報漏えい等	6位

※ 出典：情報処理推進機構（IPA）「情報セキュリティ10 大脅威 2025」

- 第2位「ビジネス上の繋がり」を悪用した攻撃は、自組織の対策のみでは防ぐことが難しいため、関係組織も含めたセキュリティ対策が必要な脅威と言える。また「ソフトウェア開発の繋がり」を悪用した攻撃もまた脅威であり、対策が必要である。
- 第3位 ソフトウェアやハードウェアの脆ぜい弱性対策情報の公開は、脆弱性の脅威や対策の情報を製品の利用者に広 く呼び掛けられるメリットがある。一方で、攻撃者はその情報を悪用し、脆弱性対策を講じていない当該製品を使用したシステムを狙って攻撃を行うおそれがある。近年では脆弱性関連情報が公開されるとすぐに攻撃コー ドが流通し、攻撃が本格化するまでの時間がますます短くなっている。
- 第5位 特定の組織（企業、官公庁、民間団体等）を狙う攻撃のことであり、機密情報等を窃取することや業務妨害を目的としている。攻撃者は社会の変化や働き方の変化に合わせて攻撃手口を変える等、標的とする組織の状況に応じた巧みな攻撃手法で機密情報等を窃取しようとする。

よくある脆弱性診断の課題

診断開始までの
リードタイムが長く対応が遅れている

報告内容の品質に差があり
提供ベンダーを変更したい

コスト改善を図りたいが
ベンダーの良し悪しが判断できない

➡ **IBC では、複数の専門事業者と連携し、お客様のニーズにあった診断サービスを提供しています。**

プラットフォーム脆弱性診断（マニュアル診断）

- パッチ適用状況
- 脆弱な設定
- 不要なサービス
- 容易なパスワード
- 不要なアカウント

プラットフォーム診断項目

No.	診断項目	概要	
		調査・確認事項	主な脅威
1	ホストの存在確認	対象サーバの存在を確認 主にICMPパケットを利用	ICMPレスポンス状況によっては、攻撃者に攻撃の糸口を与える可能性あり
2	ポートスキャン (TCP/UDP全ポート)	対象サーバのオープンポート確認	不正侵入・攻撃を行う前の事前調査として動作しているサービス状況が判明
3	不要と思われるサービス の稼働	サービスの動作状況確認	不要なサービスの動作は、攻撃者に攻撃の糸口を多く与える可能性あり
4	稼働中のサービスからの 情報取得	稼働しているサービスのバナー情報等を取得	動作しているプログラムの特定等により、攻撃に利用される可能性あり
5	OSやアプロケーションソフトウェアの既知の脆弱性	OSのバージョンやセキュリティパッチの適用状況等を確認	既知の脆弱性を利用したコマンドの実行やサービス妨害攻撃を受ける可能性あり
6	脆弱なパスワード設定	認証を伴うサービスに対して容易に推測可能なパスワードが設定されていないか確認	なりすましにより不正にシステムにアクセスされる可能性あり
7	脆弱性の知られている CGIスクリプトの存在	CGIスクリプトの存在確認及びバージョンなどを確認	既知の脆弱性を利用したコマンドの実行やサーバの内部情報を取得される可能性あり
8	アカウントポリシーの調査	アカウントロックアウト値などを取得できた場合設定値の妥当性を評価	設定値に不備がある場合、パスワード推測攻撃が容易になったり、攻撃の成功確率が上がる可能性あり
9	各種サービス(FTPサービス、SSHサービス等)の既知の脆弱性	各種サービスにおいて脆弱性の報告されている古いバージョンのソフトウェアが稼働していないか確認	既知の脆弱性を利用したコマンドの実行やサービス妨害攻撃を受ける可能性あり
10	サービス運用妨害(DoS) の可能性	サービス運用妨害攻撃を実施できる可能性があるか確認	提供しているサービスが停止または、アクセスが困難になる可能性あり
11	サーバ設定上の問題	サーバ設定(書込権限やアクセス制御設定等)がセキュリティ的に妥当であるか確認	セキュリティ的に不備がある設定の場合、不正侵入等の攻撃に利用される可能性あり
12	プライベートアドレス漏洩	対象ホストからの応答にプライベートアドレス等が含まれていないか確認	システムの内部ネットワーク情報が漏えいすることにより、不正侵入等の攻撃に利用される可能性あり
13	DNSゾーン転送の可否	DNS ゾーン転送を不特定のホストに許可しているか確認	ドメイン内に存在すると思われるホストと利用用途を容易に特定することが可能となり攻撃対象が多くなる
14	DNS再帰的問い合わせ の可否	DNS再帰的問い合わせを許可している設定か確認	許可している場合、DNSサーバの不正利用や他のサーバを攻撃する DDoS 攻撃に利用される可能性あり
15	DNS ダイナミックアップデートの可否	DNS レコードをアップデート可能な設定であるか確認	任意のレコード追加により悪意あるサイトに利用者を誘導することが可能
16	メール不正中継の可否	メールサーバのメール中継の設定状況を確認	不正中継が可能な場合、スパムメールの送信などに利用される可能性あり
17	メールサーバによるユーザ情報漏えい問題	メールサーバでユーザに許可しているコマンドやサーバの応答等を確認	コマンドの応答結果により登録されているユーザー情報を特定され、パスワード推測攻撃に利用される可能性あり
18	Web サーバ上のデフォルトコンテンツの存在	システム導入時にインストールされるデフォルトコンテンツが存在するか確認	デフォルトコンテンツに脆弱性があった場合、それを利用した不正侵入や攻撃に利用可能な情報を取得される可能性あり
19	不要なファイルの存在	不要なファイルが公開されていないか確認	ファイルの情報から、攻撃者に攻撃の糸口を多く与えてしまう
20	Proxy 設定の不備	Proxy サーバの設定がセキュリティ的に妥当であるか確認	セキュリティ的に不備がある設定の場合、ほかのシステムを攻撃する際の踏み台として利用される可能性あり
21	不適切な SSL サーバ証明書の利用	SSL サーバ証明書を取得して信頼できる証明書であるか確認	SSL サーバ証明書に不備がある場合、サーバの実在証明ができず、利用者が悪意ある偽のサーバに誘導されても判断がつかず、偽のサーバに情報を送信してしまう可能性あり
22	エラーメッセージによる情報漏えい	エラーメッセージが返るようなリクエストを送りエラーメッセージにサーバ内部情報等が含まれていないか確認	サーバ内部情報等が含まれている場合、取得した情報を不正侵入等の攻撃に利用される可能性あり
23	ワーム感染の有無	既にワームに感染していないかを確認	攻撃や不正侵入、サービス妨害に利用されている可能性あり
24	バックドア検出	バックドアが既に仕組まれていないかなど様々な項目を確認	バックドアがある場合、すでに不正にシステムを利用されている可能性あり

IBC セキュリティアセスメントサービス

IBC-SAS Web アプリ脆弱性診断サービス

情報処理推進機構（IPA）が毎年発行している情報セキュリティ 10 大脅威 2025 において、脆弱性にかかわる脅威として「サプライチェーンや委託先を狙った攻撃」、「機密情報等を狙った標的型攻撃」、「システムの脆弱性を突いた攻撃」などがランクインしました。

脆弱性管理の必要性 IPA「情報セキュリティ 10 大脅威 2025」

順位	脅威	昨年順位
1位	ランサム攻撃による被害	1位
2位	サプライチェーンや委託先を狙った攻撃	2位
3位	システムの脆弱性を突いた攻撃	7位
4位	内部不正による情報漏えい等	3位
5位	機密情報等を狙った標的型攻撃	4位
6位	リモートワーク等の環境や仕組みを狙った攻撃	9位
7位	地政学的リスクに起因するサイバー攻撃	-
8位	分散型サービス妨害攻撃（DDoS攻撃）	-
9位	ビジネスメール詐欺	8位
10位	不注意による情報漏えい等	6位

※ 出典：情報処理推進機構（IPA）「情報セキュリティ10 大脅威 2025」

- 第2位「ビジネス上の繋がり」を悪用した攻撃は、自組織の対策のみでは防ぐことが難しいため、関係組織も含めたセキュリティ対策が必要な脅威と言える。また「ソフトウェア開発の繋がり」を悪用した攻撃もまた脅威であり、対策が必要である。
- 第3位 ソフトウェアやハードウェアの脆ぜい弱性対策情報の公開は、脆弱性の脅威や対策の情報を製品の利用者に広く呼び掛けられるメリットがある。一方で、攻撃者はその情報を悪用し、脆弱性対策を講じていない当該製品を使用したシステムを狙って攻撃を行うおそれがある。近年では脆弱性関連情報が公開されるとすぐに攻撃コードが流通し、攻撃が本格化するまでの時間がますます短くなっている。
- 第5位 特定の組織（企業、官公庁、民間団体等）を狙う攻撃のことであり、機密情報等を窃取することや業務妨害を目的としている。攻撃者は社会の変化や働き方の変化に合わせて攻撃手口を変える等、標的とする組織の状況に応じた巧みな攻撃手法で機密情報等を窃取しようとする。

よくある脆弱性診断の課題

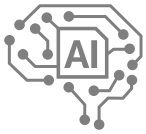
診断開始までの
リードタイムが長く対応が遅れている

報告内容の品質に差があり
提供ベンダーを変更したい

コスト改善を図りたいが
ベンダーの良し悪しが判断できない

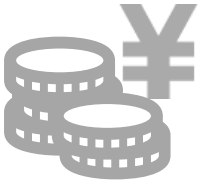
IBCは、AIプラットフォーム（Immuni Web）を利用した脆弱性診断サービスを提供

Web アプリ脆弱性診断（AIプラットフォーム+セキュリティスペシャリストによる診断）



AIがサイト全ページをスピーディーに診断

最新攻撃を自動学習(12h毎)セキュリティ専門家が結果を確認



圧倒的に優れたコストパフォーマンス

Web アプリ診断項目一覧

診断項目
OWASP Top10
CWE/SANS Top25
OWASP TestingGuide v4
WEB サーバテスト（PCIDSS/GDPR）
SSLテスト（PCIDSS/GDPR）

	OWASP Top 10 の診断項目詳細
1	アクセス制御の不備
2	暗号化の失敗
3	インジェクション
4	安全が確認されない不安な設計
5	セキュリティの設定ミス
6	脆弱で古くなったコンポーネント
7	識別と認証の失敗
8	ソフトウェアとデータの整合性の不具合
9	セキュリティログとモニタリングの失敗
10	サーバーサイド・リクエスト・フォージェリ

以下のガイドラインに準拠し、脆弱性診断を実施

国際セキュリティガイドライン
NIST SP 800-115 Technical Guide to Information Security Testing and Assessment
PCI DSS Information Supplement: Penetration Testing Guidance
FedRAMP Penetration Test Guidance
ISACA’s How to Audit GDPR

報告書イメージ


7.1. Cleartext Storage of User Information

Vulnerability CWE-ID: CWE-312: Cleartext Storage of Sensitive Information

Vulnerability CVE-ID: Not Assigned or Unknown

Risk Level: MEDIUM

CVSSv3 Base Score: 4.4 [CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N]

脆弱性の詳細:
モバイルアプリケーションは、現在のユーザーの ID をプレーンテキストで「userid.dat」および「authid.dat」ファイル内に保存しています。
これらのファイルは、アプリケーションのプライベートデータディレクトリに保存されます。これにより、ルート化されたデバイス（またはマルウェア）のスーパーユーザー権限を持つ攻撃者がディレクトリとそのファイルにアクセスしてトークンを取得し、そのトークンを権限ユーザーとして API の呼び出しで使用できるようになっています。

脆弱性の再現:
以下は、アプリケーションのプライベートデータディレクトリの「files」ディレクトリにある「userid.dat」ファイルの内容です。

Step 1 / Screenshot:

修正方法:
絶対に必要ではないデータをデバイスに保存しないことを推奨します。
保持する必要がある機密情報については、暗号化を使用し、生成された暗号化キーを KeyStore などの安全な場所に保存することを検討してください。

CWE-312: Cleartext Storage of Sensitive Information とは？
ソフトウェアがアプリケーション内に保存されている機密情報に適切な暗号化を使用していない場合、攻撃者はデバイスにアクセスして機密データを抽出することが可能です。

CWE（Common Weakness Enumeration）共通脆弱性タイプ一覧
発見された脆弱性がどのような攻撃手法により活用されるのかを示します。脆弱性の修正方法を知る際に役立ちます。

CVE(Common Vulnerabilities and Exposures)共通脆弱性識別子
発見された脆弱性の共通番号を表示します。脆弱性の修正方法を知る際に役立ちます。

CVSS（Common Vulnerability Scoring System）共通脆弱性評価システム
発見された脆弱性がどの程度危険であるかをCritical,High,Middle,Lowの4種類で評価します。

脆弱性の詳細
発見された脆弱性がどのようなものであるか説明します。

脆弱性の再現
発見された脆弱性が誤検出でないことを確認するため、再現方法を示します。

スクリーンショット
発見された脆弱性の再現方法をキャプチャします。

修正方法
発見された脆弱性の修正方法を示します。

脆弱性によるリスクの説明
発見された脆弱性によるリスクに関して記述します。

※ Immuni Web以外のWebアプリ脆弱性診断サービスも提供しております。
複数の専門業者と連携し、お客様のニーズにあった診断サービスを提供しておりますので、是非ご相談ください。

IBC-SAS ログ解析サービス（年間）

パロアルトネットワークス社　次世代ファイアウォール PA シリーズで収集したログをもとに、解析をおこなうサービスです。PA シリーズのレポート機能をさらに深堀りし、お客様環境に即したレポートをご提示します。毎月分析をおこなうことにより、問題点・改善方法の早期把握を実現します。

よくあるお悩み

- ログの内容を解析するノウハウがない
- ログ情報を活用できていない
- ログ解析に工数がかかっている
- 脆弱性の具体的な対応方法を知りたい
- 脆弱性対策をタイムリーに実施できない
- 脆弱性の分析をおこないたいが ノウハウがない

サービスの特徴

実績豊富なエンジニアが PA シリーズの詳細な分析をおこないます。毎月の分析により、セキュリティ強化を実現します。

リスク状況の可視化

- 情報漏洩の可能性を検出
- マルウェア感染の可能性を検出
- インシデント対象サーバーの洗い出し

具体的対策の提案

- 検出した脆弱性に関する分析
- PA 本体の脆弱性対応に関する情報提供

セキュリティ品質の保持

- 前月比較で傾向を把握
- 新規インシデントに対して迅速に対応

サービスの流れ

01 ログ情報のご提出（過去 1 か月分）

02 弊社で分析（約 2 週間）

03 報告会開催および ログ解析レポート提出

価格　月額 ￥ 400,000 ～

※ 1 年間のご利用を前提とした金額です。詳細はお問い合わせください。

ログ解析サービス結果 / レポート例

ログ情報をもとにした分析結果をレポートとしてご提供いたします。レポートでは、現状の設定状況とあわせて、お客様環境に則した推奨設定をご案内いたします。

インシデント件数サマリー

■ インシデント種類、重要度別件数

	Critical	High	Medium	Low	Informational
Vulnerability	8 件	30 件	3,879 件	23,230 件	4,232,454 件
Antivirus	0 件	0 件	172 件	0 件	0 件
Wildfire	0 件	0 件	1,649 件	0 件	0 件
Anti-Spyware	0 件	0 件	70 件	0 件	64,294,448 件

■ 総評

本件の解析対象期間 2019 / ×× / ××-2019 / ×× / ×× について、Vulnerability にて Critical 判定が 3 種類（8 件）、High の判定が 6 種類（30 件）ございました。

いずれも対象のソフトウェアを利用していない、もしくは、最新の状態であれば影響を受けません。念のため、ご確認いただくことを推奨いたします。

また、Vulnerability 以外の Antivirus 、Wildfire 、Anti-Spyware においても、全体的に Web サービスを対象とした脅威の検知・マルウェアに関連するトラフィックが多く見受けられました。

引き続き、万が一に備え推奨設定で運用いただくことをお勧めいたします。

インシデント詳細（Vulnerability）

No	重要度	件数	脅威 ID	名称	CVE 番号	詳細	送信元 IP	宛先 IP	コメント
1	critical	5	38598	Android Stagefright Library Overflow Vulnerability	2015-3864 2015-1538 2015-1539 2015-3824 2015-3826 2015-3827 2015-3828 2015-3829	Android の Stagefright（メディア再生サービス）ライブラリにて細工された MP4 ファイルを処理する際に、オーバーフローを引き起こす脆弱性	157.205.xxx.xxx (JP) 183.79.xxx.xxx (JP) 209.85.xxx.xxx (US) 40.107.xxx.xxx (US)	211.8.xxx.xxx (JP)	2015 年に発見された Android バージョン 6 以前の問題。また、ベンダーによってはパッチがリリースされている。 Android の OS バージョン別シェア (https://developer.android.com/about/dashboards/)では、対象端末は全体の 29.5 % (2019 年 1 月現在)。 そのため、現時点ではやや危険性は低い。 業務で Android 端末利用をしている場合、アップデートを推奨する。
2	critical	2	37057	Microsoft Schannel Remote Code Execution Vulnerability	2014-6321	Microsoft の S チャンネル（セキュリティパッケージ）において、細工されたパケットを処理する際に、ヒープオーバーフローが生じる脆弱性	10.10.xxx.xxx 10.10.xxx.xxx	117.18.xxx.xxx (AU) 192.229.xxx.xxx (US)	修正ファイルリリース済。 また、Windows 10 には影響しない。 必要に応じて、対応を推奨。
3	critical	1	38092	Microsoft OpenType Font Parsing Code Execution Vulnerability	2015-2459	Microsoft の OpenType（フォントフォーマット）において、細工された OTF ファイルを処理する際に遠隔でのコード実行を可能とする脆弱性	59.106.xxx.xxx (JP)	10.10.xxx.xxx	修正ファイルリリース済。 PoC が存在し、実際の攻撃も確認されているため、クライアント OS のアップデートがおこなわれていない場合、対策が必要。

ネットワークインテグレーション

IBC-Integration インターネットゲートウェイ構築サービス

こんなお悩みはありませんか？

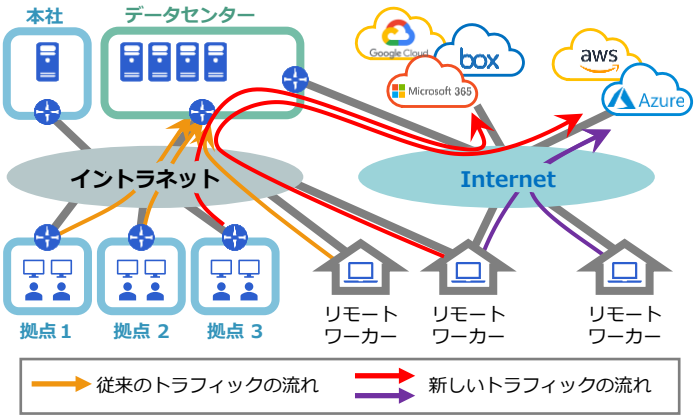
リモートアクセスやクラウド利用が増えてから
- 動作が重たい、途切れる
- 特定の時間帯に不安定になる
- オンライン会議の調子が悪い
- クラウドサービスの応答が遅い

どこが問題なのか わからない

大幅なネットワーク変更には時間と費用がかかる

現状の構成で問題ないかどうか判断できない

昨今のクラウドシフトによるアクセス先の変化や、コロナ禍の影響で一気に加速したテレワークシフトにより、トラフィックの流れが大きく変わりました。これまでのイントラネット主体での接続の流れから、インターネット環境にある Microsoft 365 などのクラウドサービスへの接続や、自宅やサテライトオフィスからのテレワーク接続が大幅に増えています。
それにともない、従来のネットワーク構成においてボトルネックとなるポイントが発生するようになりました。

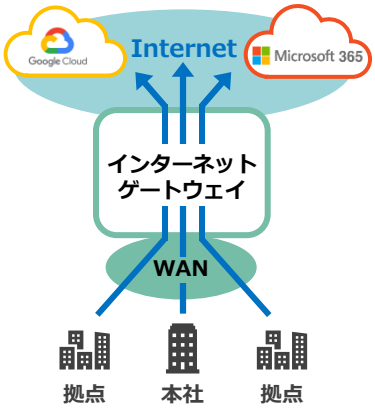


ネットワーク構成の変化

トラフィックの流れの変化にあわせ、さまざまなネットワーク構成のパターンが登場しました。管理工数、コスト、セキュリティなどを検討し、自社に一番合った構成を選ぶ必要があります。

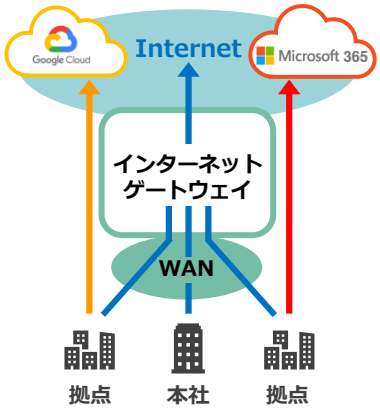
センター集中型
従来型のイントラネットのみで構成

インターネットへの通信がセンター側へ集中しているのでセキュリティ統制や管理がしやすい一方、インターネット回線が混雑したり、ファイアウォール / プロキシの負荷が増大する。



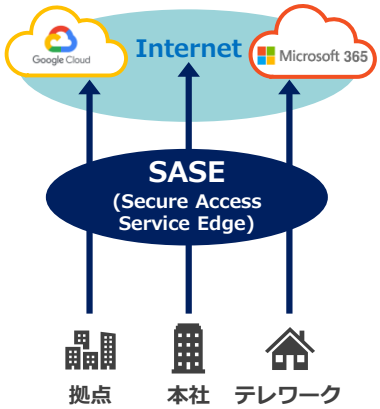
ローカルブレイクアウト型
アクセスが分散した構成

許可されたアプリケーションは別経路へ迂回する。回線混雑を避けられる一方、拠点からインターネットへ直接接続するためセキュリティリスクがある。



フルインターネット型
すべてクラウド上で提供する構成

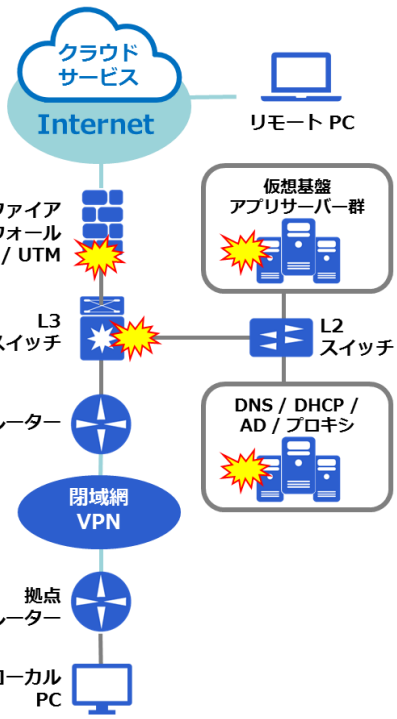
自宅や外出先からクラウドサービスを利用する際も安全にアクセスすることが可能。オフィスからのアクセスでも、適切に SASE の機能を使うことでセキュリティを保つことができる。

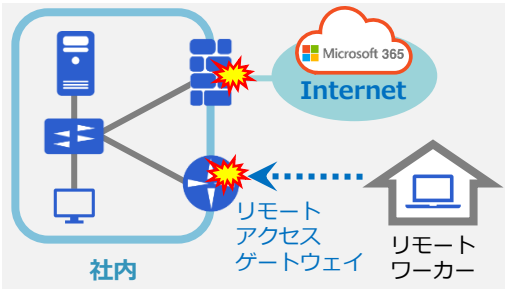


お客様のご要件にあわせて、適切な製品選定、構築、導入後の運用までご支援します。

事前検証 方式検討 → 要件定義 → 基本設計 詳細設計 → 設定 構築 → 運用・保守 サポート

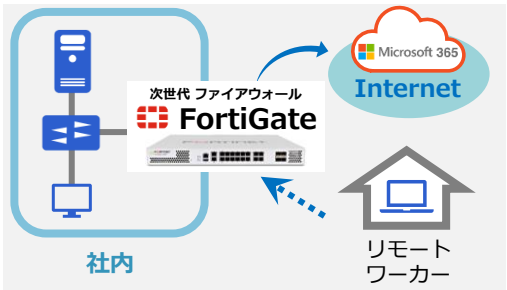
実際の構築事例





◆お客様のお悩み

- リモート接続、インターネット接続の性能劣化（原因不明）
- リモートアクセスゲートウェイの保守切れ
- 既存装置のスペック不足が一因となり、VDI 系通信や LAN 内の通信遅延が発生



◆ご提案と対応

- 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
- 次世代ファイアウォール（FortiGate）へのリプレイスご提案
- リモートアクセスゲートウェイの統合
- FortiGate を選定することで、パフォーマンスの向上に加え、UTM 機能の拡張等のセキュリティ強化を実現

ボトルネックポイント見直しの流れ

ネットワークにおける課題や問題点を解決するためのポイント

設計性能	用途需要	端末数 社員数	アプリケーション	サービス
機器性能	CPU 負荷 メモリー	セッション数	フロー数	処理遅延
	機器機能	破棄パケット	トラフィック	ルーティング
環境性能	品質	回線帯域	遅延	サーバー応答

お客様では解決できない課題や第三者目線での現状調査、アセスメント等の要望について、性能分析に長年携わってきた経験豊富なエンジニアによる、分析サービス(IBC-PAS)で解決します。

ネットワークインテグレーション

IBC-Integration

ログサーバー構築サービス

なぜ今、「統合ログ管理」なのでしょうか。リモートワークによるネットワーク構成の変更ログや各種クラウドサービスの利用ログ、勤務実態の把握のためのパソコンの利用ログ、各種サーバーや業務システムへのアクセスログなど、あらゆる場面でログを取得し統合的に管理する必要があります。

現状、ログは個別（システムごと）の管理にとどまっていることがほとんどでしょう。ですが、「有事の際にそれぞれのログを見に行く」という運用はシステム管理者の工数が膨大となり現実的ではありません。単純なセキュリティインシデントが発生した場合でも、点在しているさまざまなログを確認し、統合的に分析し、状況を判断することが求められます。

ログ監視
迅速な対処と証跡管理

ログ取得、分析、検知

性能情報、運用改善レポート

性能監視
傾向把握と影響範囲特定

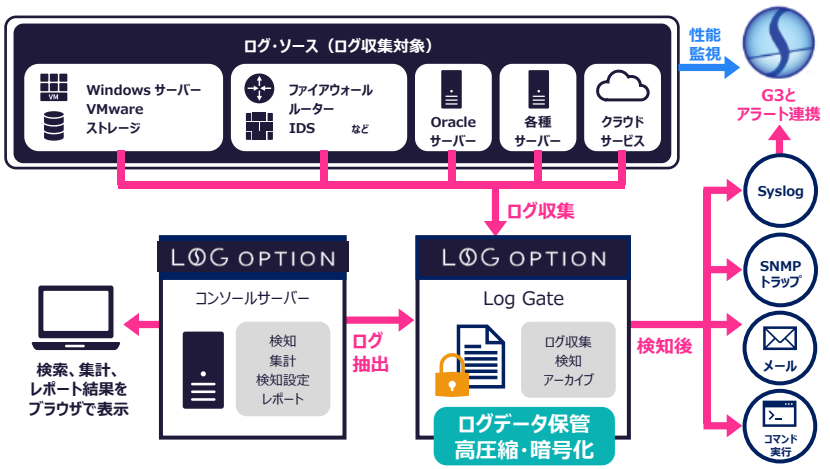
高度なセキュリティ対策に対応するには、サイバー攻撃対策、情報漏えい対策、内部不正対策などが求められます。これらの実現のためには、各機器が出力する**ログ情報**（シスログ、イベントログ、アプリケーションログなど）の一元管理に加えて、各種ネットワークシステムの**性能情報**の把握も必要となります。

System Answer G3 LOG OPTION

System Answer G3 の詳細はこちらから！

システム性能監視ツール System Answer G3 のオプション製品である「Log Option」は、多種多様なログを統一されたフォーマットで扱うことができる統合ログ管理ツールです。異なる種類のデータに同一の意味づけ（タグづけ）をおこなうことで、ログの形式の違いを吸収して扱うことができ、データの羅列でしかないログを人間が見てわかる形式に変換して活用することが可能になります。

収集	検知
受信機能 Syslog / FTP（S）/ SNMP / 共有フォルダ **ログ送信・取得機能** Agent / EventLogCollector / SecureBatchTransfer	・ポリシーに合致したログのアラート ・複合的な条件付けによるログの検知設定が可能
保管	**検索・集計・レポート**
・ログの圧縮保存、高速検索 ・ログの改ざんチェック ・ログに対する意味付け（タグ付け） ・ログの暗号化保存 ・保存期間を経過したログを自動アーカイブ ・ログの保存領域管理機能	・複数ログの横断追跡と高度な絞込み ・インデックスによる大量ログの高速検索 ・グラフによるログのサマリー表示 ・レポート（HTML / PDF / CSV / TXT / XML）の自動メール通知



価格例	ログ収集性能	ライセンス価格（年額）			
エントリー版（ET）	100 行 / 秒	初年度	600,000 円	次年度以降	100,000 円
ワークグループ版（WG）	1,000 行 / 秒		900,000 円		150,000 円
スタンダード版（ST）	2,000 行 / 秒		1,920,000 円		320,000 円

※ 他のモデルについてはお問い合わせください。

IBC-Integration 無線 LAN 構築サービス

こんなお悩みはありませんか？

無線 LAN 環境の
- **接続が突然切れる**
- **セキュリティ対策が不安**
- **時間帯によって繋がりにくい**
- **アクセスポイントの管理が複雑**

どこが問題なのか わからない

大幅なネットワーク変更に は時間と費用がかかる

現状の構成で問題ないか どうか判断できない

無線 LAN 通信の規格は 3 ～ 5 年程度で改訂されており、最新のものほど通信速度が速く、セキュリティ対策も向上していますので、定期的に最新規格に対応した機器へリプレイスする必要があります。リプレイス直後はサイトサーベイのデータをもとに快適な電波環境で利用できることが多いのですが、しばらくすると繋がりにくくなったり、通信が遅くなったりする事象が発生しやすくなります。
無線 LAN 環境構築の際には、このような通信不安定を極力発生させないことに加え、管理工数、コスト、セキュリティなどを考慮する必要があります。

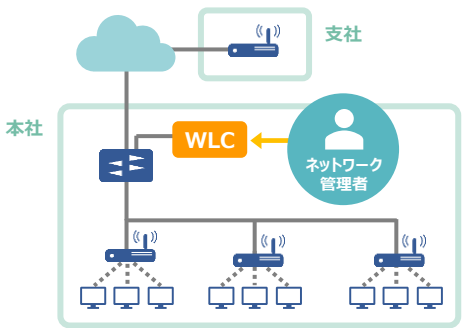
世代	策定年	規格名	最大通信速度
第 1 世代	1997 年	IEEE 802.11	2 Mbps
第 2 世代	1999 年	IEEE 802.11a	54 Mbps
		IEEE 802.11b	11 Mbps
第 3 世代	2003 年	IEEE 802.11g	54 Mbps
第 4 世代 (Wi-Fi 4)	2009 年	IEEE 802.11n	600 Mbps
第 5 世代 (Wi-Fi 5)	2013 年	IEEE 802.11ac	6.9 Gbps
第 6 世代 (Wi-Fi 6)	2019 年	IEEE 802.11ax	9.6 Gbps
第 6 世代 (Wi-Fi 6E)	2020 年	IEEE 802.11ax	9.6 Gbps

アクセスポイントの管理方法の変化

無線 LAN の普及にともない、アクセスポイント（AP）の管理方法も従来の AP 1台 1台を個別で設定する「FAT AP 型」からより効率的な「無線 LAN コントローラー型」や「クラウドサービス型」に進化しました。

無線 LAN コントローラー型

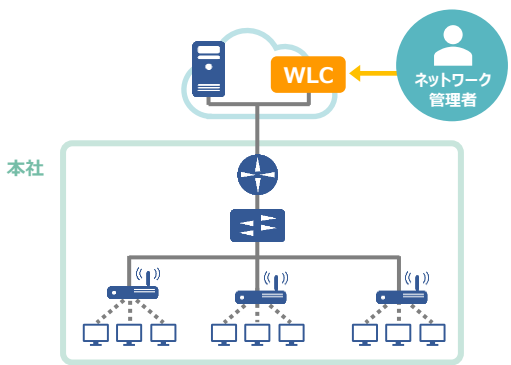
本社に設置した WLC（Wireless LAN Controller）の操作だけですべての AP 設定が完結する。



安全性	◎	性能	◎	管理性	○
拡張性	△	価格	高		

クラウドサービス型

クラウドサービス上に WLC と認証サーバーを設置する。



安全性	○	性能	○	管理性	○
拡張性	○	価格	中		

お客様のご要件にあわせて、適切な製品選定、構築、導入後の運用までご支援します。

事前検証 方式検討 → 要件定義 → 基本設計 詳細設計 → 設定 構築 → 運用・保守 サポート

導入検討時のポイント

◆ セキュリティ：盗聴や不正アクセスを防ぐ強固な認証と暗号化ができるか

IEEE802.1X/EAP 認証には様々な種類がありますが、実際によく使用されている方式は TLS と PEAP です。

EAP-TLS 認証		PEAP 認証	
セキュリティ強度が高い。 相互に電子証明書を発行するため、電子証明書の発行および管理負担とコストがかかる。		クライアント証明書の管理の必要がなく（ユーザー ID と証明書のハイブリッド認証）手軽な一方、ユーザー名とパスワードが盗まれた場合、不正アクセスされる危険性がある。	
セキュリティ強度	◎	セキュリティ強度	○
端末側の認証	電子証明書	端末側の認証	ID / パスワード
サーバー側の認証	電子証明書	サーバー側の認証	電子証明書

◆ 管理効率：本社や支店、工場などに散在する多数の無線 AP を設定・監視できるか

- FAT AP 型　：家庭や小規模なオフィスで使用する場合
- 無線 LAN コントローラー型　：大手企業の大規模インフラを管理する場合
- クラウドサービス型　：店舗数が多い場合や、アプライアンスの保守の手間を省きたい場合

◆ 通信品質：電波干渉などの通信状況不安定による業務効率低下を防止できるか

- 設置前、設置後のサイトサーベイ
- 負荷分散、電波出力、チャネルの自動調整
- 適切なセグメンテーション

メーカー比較

Aruba Networks
無線 LAN コントローラーの老舗。オンプレ型のメリットである安定性 / 信頼性がある。バージョン管理と認証機能の柔軟な設定が可能な大型エンタープライズ向けソリューション。

Cisco
クラウド型無線 LAN のデファクトスタンダード。クラウド型サービス《Meraki》は導入負担やログ取得など管理負担の軽減とサイジングが不要で、手軽に導入が可能な多店舗展開向けソリューション。

Juniper
クラウド型サービス《MIST》は AI「Marvis」を搭載しており、無線 LAN 運用で人が苦労していた部分を代行。クラウド型でありながらアクセスポイントのファームウェアのバージョン指定・管理が可能で、検証コストを削減しながら安定性を向上できる。

ファイルサーバー

ファイル管理のサーバーレス化
物理劣化を気にせず運用が可能なクラウド基盤への移行

膨大な量のデータが保存されているファイルサーバーは、経年変化や利用ユーザーの増加によるレスポンスの変化が如実にあらわれ、業務効率を左右する大きな問題です。

働き方改革によるリモートワークも増加する中、ファイルサーバーをクラウド上に構築することで、社内外問わず同じ環境を実現することが可能になります。

パッケージ名		Point
	ファイルサーバー構築パッケージ	物理サーバーを置きたくない
	【オプション】認証基盤サービス（PaaS）	新規 Active Directory を構築し、連携させたい
	【オプション】認証基盤サービス（IaaS）	既存 Active Directory と連携させたい
	【オプション】障害復旧サービス	DR 対策をおこないたい
	【オプション】ファイルバージョン管理サービス	ファイルバージョン管理をおこないたい（VSS 機能）

IBC
アイビーシー株式会社

東京本社 | 〒104-0033 東京都中央区新川1-8-8 アクロス新川ビル8F
tel.03-5117-2780　fax.03-5117-2781

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
tel. 06-7653-1014　fax. 06-7177-0542

URL | https://www.ibc21.co.jp/
https://system-answer.com/

20250115 v1.0