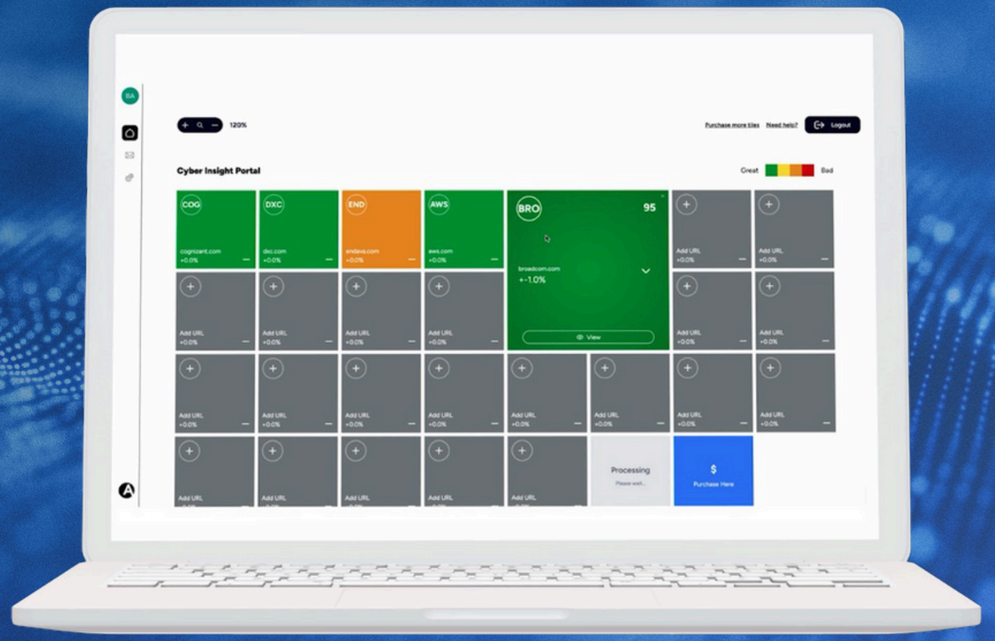
ビジネス視点のサイバーリスク管理を実現

Cyber Insight Portal
サイバー・インサイト・ポータル

SaaS型サイバーリスク管理プラットフォーム"Cyber Insight Portal (CIP)』が、その実現のための中核となります。
CIPは、御行グループ企業、投資・融資先、そして特に重要な取引先やサプライチェーン全体にわたるサイバーリスクを、継続的にモニタリングし可視化します。

視覚的コンセプト - タイル型ダッシュボード

CIPは、複雑なリスクデータを『タイル』と呼ばれるパネル形式で直感的に表示します。各タイルは1つの企業を表し、リスク状況をトラフィックライトプロトコル（TLP）に基づいた4色で示すため、一目でリスクレベルを把握できます。



Cyber Insight Portal の仕組みと主要機能：継続的なモニタリング、明確な洞察

① 継続的・自動化されたモニタリング

CIPは対象企業を継続的にモニタリングします。

リスクステータスは自動的に更新され、可視性を提供します。金融庁ガイドラインが求める『継続的なモニタリング』要件に直接対応するものです。

② 迅速な評価開始と広範なカバレッジ

CIPは対象企業のネットワークアクセスや許可を必要とせず、外部から合法的に実行されます。

これにより、迅速な初期評価（通常、5秒から72時間程度）が可能となり、インターネットに接続しているあらゆる企業、さらには二次請け以降のサプライヤまで、広範囲なモニタリングを実現します。

③ ビジネスインパクトへの焦点

分析結果はタイルに視覚的に表示され、IT専門家だけでなく、リスク管理、与信管理、経営層の方々にも理解しやすいように設計しています。

技術的なリスクを、事業継続性への潜在的な影響という観点から提示します。

④ 実用的なインテリジェンス

CIPはサイバーリスクに関する統一されたビューを提供し、サプライヤーのオン/オフボーディング、M&Aデューデリ、与信リスク評価、リスク低減策のためのリソース配分といった戦略的な意思決定を支援します。

今夏には、AIサジェスト機能を実装予定です。

TLP評価ごとの根拠・影響・外部評価について

グリーン（低リスク）

概要	厳格な脆弱性管理やマルウェア対策が機能しており、サプライチェーンや保険審査でも高く評価されやすい。
根拠	公開サーバやネットワーク設定に深刻な問題がほぼなく、脆弱性管理やパッチ適用が行き届いている状態。マルウェア感染や流出情報、危険なポートの放置などが見られない（または極めて少ない）。
影響	データ侵害・セキュリティインシデントに遭遇する確率が著しく低い。「レッド」に比べて10倍程度、侵害確率が低いと想定しており、今後の分析対象企業（利用者）増加(n>15,000）に伴って相関データを示すことができると考えられる。
外部評価	深刻な脆弱性がほぼ検出されていないことから、外部（金融機関、信用情報機関、保険会社等）から見てもセキュリティ状況の良い会社と評価される可能性が高い。

イエロー（中低リスク）

概要	比較的安全ではあるが、いくつか修正すべきリスクの課題が散見される可能性がある。
根拠	比較的リスクは低いが、「グリーン」よりはやや懸念点がある。深刻ではないものの、いくつかの中程度の深刻度の脆弱性や設定不備など（ex. 古いSSL/TLS設定、未更新のWebアプリケーションなど）が検出されている可能性が高い。
影響	重大な問題を抱えているレベルではないため、定期的な脆弱性対策や設定見直しによって「グリーン」への改善が比較的容易。
外部評価	外部から見ても依然として「セキュリティ水準はまずまず」と判断されることが多いが、「グリーン」と比べて注意が必要な分野が散見される。

アンバー（中リスク）

概要	リスクが中程度からやや高めで、懸案事項を放置し続けると「レッド」になるため早急な改善が必要。
根拠	「イエロー」に比べ、明確な懸念点や未対応の脆弱性が増えている状態（深刻な脆弱性が複数存在している、長期間放置されているなど）。「脆弱なプロトコルの継続利用」「公開サーバの一部が古いソフトウェアを使用」「ダークウェブ上で漏洩した可能性があるクレデンシャルの検出」など攻撃者が付け入る余地が見受けられる。
影響	セキュリティ侵害に遭遇するリスクが有意に高まると考えられる。
外部評価	外部から見た際に、早期の対策が必要と判断されやすく、信用リスクや保険料増加リスクが生じる可能性が高まる。

レッド（高リスク）

概要	リスクが最も高く、深刻な問題や過去の事故痕跡が多い。
根拠	深刻度の高い脆弱性やインシデントの痕跡が多数検出されている可能性が高い。過去の漏洩事故歴、既知の重大脆弱性の長期放置、不正アクセス・マルウェア感染の継続など、外部から見ても危険度が高い兆候が散見される。
影響	最優先でセキュリティ改善が必要なレベル。
外部評価	外部からは「ビジネス上の大きなリスク要因」と受け止められやすく、取引先からの契約を見直されるなど厳しい対応を取られる可能性がある。

Cyber Insight Portal でのサイバーリスク解析・評価について

① ドメインを入力

ドメインは、対象企業特定のための一意の識別子として用いているだけで、ドメイン以下のウェブサイトだけを診断しているわけではない。

② 対象企業の特定とIT資産リスト生成

分析対象企業とIT資産との紐付けは、外部データベース（常に更新されているため、帰属精度は高まり続けている）によってマッピングされる。

③ 評価対象データ取得

IT資産リストに基づき非侵入手法および外部データプロバイダからのデータ取得。

保険会社や信用格付機関が既に用いている手法や、攻撃者がインターネット探索で用いているのと同等の手法によって収集したデータも含む。

カスタマイズにより、分析対象企業から提供されるデータセットも含めての分析可能。

④ 解析・評価

評価の基盤は、法規制等で基準となる技術的対応および組織的対応に加え、外部脅威を含めた３つのリスク要因に基づいて分析する。

問題ごとに外部データプロバイダーの提供するデータベース（ユーザー増加に伴い、自社データベースも増加）と付き合わせて統計上の偏差値のような指標を計算し、類似規模の組織の平均（小規模事業者の場合、大規模事業者に対してIT資産の少ないことから問題の絶対数も少なくなる。

このことで相対的に評価が高くなることを回避するために、外部データベースによる組織規模ごとのサイズ正規化を行う）から値を測定。

⑤ 評価結果の表示

客観的なセキュリティ要素を点数化し、時間経過や環境変化に伴うダイナミックな評価を行う。バックエンドでは脆弱性を修正できるだけの情報は揃っている。