\\ 危険度が点数でまるわかり //

最先端の サイバーリスク 可視化ツール とは？

近年、さらに危険度が増してきた、サイバーセキュリティの脅威や脆弱性

近年、サイバー攻撃の頻度や手口が巧妙化しており、企業にとってサイバーセキュリティ対策がますます重要になっています。少し前になりますが、2020年12月には、経済産業省が最近の攻撃の特徴と目的を整理し、経営者に対して、サイバーセキュリティの取組の一層の強化を促すことを呼びかけましたが、その後、サプライチェーン上での攻撃、ランサムウェアによる被害の増大、海外拠点を経由した攻撃などが顕著になっています。

このような背景から、サイバーセキュリティに関する知識を深め、事前対策から事後対応までのセキュリティ対策を徹底することが求められています。

【出典】最近のサイバー攻撃の状況を踏まえた経営者への注意喚起
https://www.meti.go.jp/press/2020/12/20201218008/20201218008.html

情報セキュリティ10大脅威の推移

2023年	10大脅威（組織）	2022年	2021年	2020年
1位	ランサムウェアによる被害	1位	1位↑	5位
2位 ↑	サプライチェーンの弱点を悪用した攻撃	3位↑	4位	4位
3位	標的型攻撃による機密情報の搾取	2位	2位	1位
4位 ↑	内部不正による情報漏えい	5位↑	6位	2位
5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	4位	3位New	圏外
6位 ↑	ゼロデイ攻撃	7位New	圏外	圏外
7位	ビジネスメール詐欺による金銭被害	8位	5位	3位
8位	脆弱性対策情報の公開に伴う悪用増加	6位↑	10位↑	14位
9位	不注意による情報漏えい等の被害	10位	9位	16位
10位 New	犯罪のビジネス化（アンダーグランドサービス）	圏外	圏外	圏外
圏外	予期せぬIT基盤の障害に伴う業務停止	9位	7位	6位

ランサムウェアは結果として被害となるので1位であろう

サプライチェーンの問題は脅威が高まっている

テレワークを狙う攻撃は対策が浸透してきた

脆弱性情報を利用した攻撃は上昇傾向

犯罪ビジネスが登場

【出典】情報処理推進機構「情報セキュリティ10大脅威」よりhttps://www.ipa.go.jp/security/vuln/10threats.html

① サプライチェーン上での攻撃パターンの急激な拡がり

攻撃者が利用する「攻撃起点」が中小企業を含む取引先や海外展開を進める企業の海外拠点にまで拡大しており、その影響がさらに大きくなっています。特に新型コロナウイルスの感染拡大に伴うテレワークの増加により、脆弱性が高まっている状況です。

② ランサムウェアによる被害の急増

暗号化されたデータを復元するために身代金を要求するランサムウェアによる被害が急増しています。さらに、攻撃者がデータを窃取し、身代金を支払わなければデータを公開すると脅迫する手法が一般的になっており、企業にとって深刻な問題となっています。

③ 海外拠点を経由した重要情報の窃取を狙った攻撃の深刻化

海外拠点と日本国内のシステムをつなげていることで、セキュリティ対策が不十分な海外拠点から日本に侵入されるリスクが高まっています。企業は、十分な対策を講じることが必要です。

いま、経営者に求められる
「サイバーセキュリティ対策と危機管理体制」の徹底

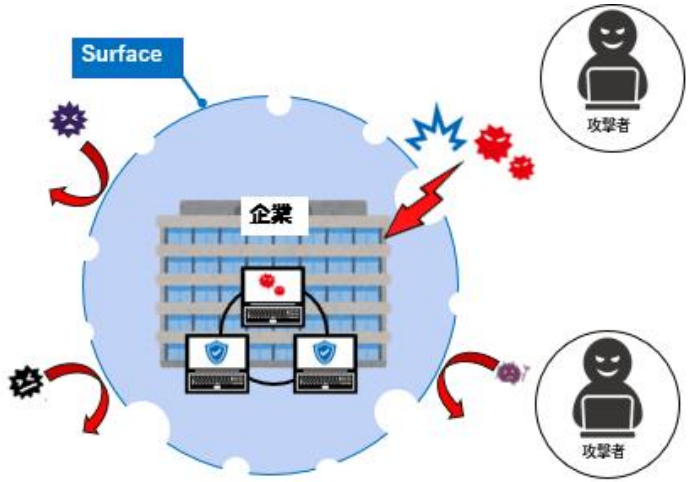
経営者には、サイバーセキュリティ対策についての迅速な判断と積極的な投資や、それを踏まえたグローバル・ガバナンスの構築、そして企業内での危機管理体制の整備が求められています。

ASM（Attack Surface Management）という考え方

攻撃者は、表面（Surface）の脆弱性を狙います。有名企業だから狙うのではありません。脆弱性が見えている個所をリスト化して、機械的に攻撃を試みます。

例：FWのコンソールポートが見えている、脆弱性パッチが当たっていない、
SSLの設定が甘い、など

自社を外から見ること、表面を整える事が重要です。



サイバーセキュリティ対策の第一歩として注目される「サイバーリスク可視化ツール」

ASMや体制づくりにおいて注目されているのが、セキュリティリスクを可視化し、リアルタイムで監視することができるサイバーリスク可視化ツール。ツールを使うことで、セキュリティリスクを点数（スコア）で把握でき、必要な対策を、優先順位をつけて迅速に行えるようになるので、強固なサイバーセキュリティ対策を図ることができます。

本書では、この最新のサイバーリスク可視化ツールについてわかりやすく解説して参ります。

【いままでのツールとここが違う】
最新のサイバーリスク可視化ツール　“6つの特徴”

セキュリティリスクの管理や対策の見直しが必要な企業にとって、セキュリティリスクを定量的に評価し、可視化できるサイバーリスク可視化ツールは救世主になるでしょう。ここでは、最新のサイバーリスク可視化ツールの特徴を6つご紹介いたします。

最新のサイバーリスク可視化ツール6つの特徴

① １日あたり800億超 膨大な量のデータを活用＆分析

② 測定できるリスクの範囲が大幅に拡大

③ 定量的で客観的なリスクスコアを算出

④ 自社およびグループ会社、サプライチェーン、同業他社に至るまでチェックが可能

⑤ 使いやすいUI（ユーザーインターフェース）

⑥ システムの追加、改変、インストール等が不要

①　1日あたり800億超　膨大な量のデータを活用＆分析

従来のサイバーリスク可視化ツールとの大きな違いの1つ目が、外部から収集された1日あたり800億超のイベント・データをはじめとする膨大な量のデータを活用し、わかりやすい定量的なセキュリティスコアとして確認できる点です。この新しいアプローチにより、自社のサイバーセキュリティの状態をより正確に把握し、改善策を策定することができます。

データ収集の量や範囲の拡大

インターネット上からさまざまな情報を収集します。これには、脆弱性スキャン結果、マルウェア情報、ネットワークトラフィックデータ、データ漏えい情報、ダークウェブ上の情報などが含まれます。

データ分析の精度の向上

収集された膨大なデータを分析し、セキュリティリスクに関連する情報を抽出します。機械学習や自然言語処理などの先進的な技術を用いて、関連性の高い情報を特定し、リスク評価に活用します。

自動的に情報を収集して解釈

インターネット上に公開されている情報を自動的に収集します。これには、企業のドメイン名、IPアドレス、DNS情報、メールレコードなども含まれます。この自動収集されたデータを解釈し、後述のセキュリティスコアに反映できます。

リアルタイムで情報提供

リアルタイムでデータを収集・分析し、セキュリティ状況について常に最新の情報で評価することができます。（例：最新でない脆弱性を含むプロトコルを利用していたためにスコアが減点されていた→新しいプロトコルを導入→セキュリティレベルが向上したためスコアが上昇）

②　測定できるリスクの範囲が大幅に拡大

2つ目は、従来のツールに比べてより広範囲のリスク要因を測定できるという点です。
以下に、評価できるリスクの一例をご紹介いたします。

脆弱性管理

企業が使用しているソフトウェアやシステムに存在する脆弱性のリスクを評価します。これには、未適用のパッチや、エンドポイント保護の不十分さなどが含まれます。

セキュリティポリシーと設定

企業のセキュリティポリシーおよびネットワーク、システム、アプリケーションの設定が適切に管理されているかどうかを評価します。

インシデントレスポンス

ウェブサイト、オンラインサービス、インターネット接続されたデバイスなどを対象に、インターネットから見える組織の外部表面に対する攻撃や脆弱性を評価・監視します。

ネットワークセキュリティ

企業のネットワークが適切に保護されており、不正アクセスやデータ漏えいのリスクを最小限に抑えているかどうかを評価します。

ウェブアプリケーションセキュリティ

企業が開発・運用しているウェブアプリケーションに関連するセキュリティリスクを評価します。これには、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）などの脆弱性が含まれます。

第三者リスク

サプライチェーン内のベンダーやパートナー企業のセキュリティリスクを評価し、全体的なリスクを把握します。

暗号化の適用

企業が適切な暗号化技術を使用して、データの機密性と完全性を維持しているかどうかを評価します。

③ 定量的で客観的なリスクスコアを算出

注目の3点目は、測定したリスク要因を複合的・総合的に分析することで、サイバーセキュリティリスクを客観的かつ定量的な「セキュリティスコア」として算出することができる点です。このアプローチにより、自社のサイバーセキュリティの状態をより正確に把握し、現在必要な改善策について優先順位を付けて策定することができるようになります。

さらに、このスコアは定期的に更新されるので、リアルタイムのリスク情報に基づいた評価も可能になります。また、競合企業との比較も容易になるため、現在セキュリティは業界内のどのあたりのレベルにあるのかを把握したうえで改善に取り組むことができます。以下は、スコアリングに関する特徴をご紹介いたします。

スコアリングシステム

複数のセキュリティ評価項目を基に、セキュリティスコアを●●●ポイントのような分かりやすい形式で数値化するスコアリングシステムが注目を集めています。スコアが高いほど、セキュリティ対策が適切でリスクが低いことを示します。このシステムにより、従来の主観的な評価に依存することなく、客観的な基準でセキュリティ状況を把握できます。

さまざまな視点からスコアを算出

インフラストラクチャー、脆弱性、構成管理、ポリシー遵守など、さまざまなセキュリティ関連のデータを収集・分析し、定量的なセキュリティスコアを算出します。これにより、自社の打つべき対策を明確にすることができます。

（例：バージョンが古く脆弱性がありセキュリティスコアが低い→パッチを適用することで脆弱性を解決→スコアが向上）

業界内や同業他社とのスコア比較

業界内の平均スコアとの比較もできるので、自社のセキュリティスコアが業界平均と比べて高いのか低いのか、現在のポジションを把握することができます。もちろん、目指すべき業界のトップクラスのスコアも把握できますし、先行する同業他社のセキュリティ対策やリスク管理のベストプラクティスを参考にして、自社のセキュリティ強化に取り組むこともできます。

時系列データの分析

セキュリティスコアを時間経過とともに追跡し、改善のトレンドを分析することができます。これにより、セキュリティ対策の効果を評価し、継続的な改善が促されます。過去のデータを参照することで、セキュリティ対策の効果や問題の発見・解決にかかる時間を把握することができ、セキュリティレベルの向上に役立ちます。

進捗の追跡とトレンド分析

セキュリティスコアの履歴データを利用して、セキュリティ対策の進捗を追跡し、トレンドを分析することができる機能も重要です。改善の効果を確認し、継続的なセキュリティ強化につながります。

④　自社およびグループ会社、サプライチェーンに至るまでチェックが可能

4点目は自社だけでなく、グループ会社、サプライチェーン、サードパーティのセキュリティリスクも評価することができる点です。これにより、今まで以上に広い範囲でセキュリティ状況の把握が可能になります。

グループ会社全体での評価

自社のみならず、グループ会社のセキュリティスコアを評価し、セキュリティリスクを把握することができます。これにより、グループ全体のセキュリティ状況を監視し、効果的なリスク管理と対策の実施が可能となります。

サプライチェーン全体での評価

サプライチェーン内のベンダーやパートナー企業のセキュリティリスクも評価することができます。これにより、サプライチェーン全体のリスクを把握し、ベンダーやパートナー企業と連携してセキュリティ対策を強化することができます。

サードパーティの評価

サードパーティ（ベンダー）のセキュリティリスクを評価する機能も重要で、サプライチェーン全体のリスクを把握し、適切な対策を講じることができます。サードパーティのセキュリティリスクが企業全体のリスクに影響を与えるため、適切な情報共有や協力体制を構築することが重要です。

⑤　使いやすいUI（ユーザーインターフェース）

5点目は、簡単かつ正確にセキュリティ状況を把握するために重要な「使いやすいUI」についてです。最新のセキュリティツールは直感的で使いやすいUI設計を採用し、セキュリティ対策において重要な整理された情報をわかりやすく表示。専門家だけでなく一般のユーザーにも馴染みやすく、継続的な活動を支えます。

直感的で使いやすいUI

セキュリティ対策をはじめとする継続的な取り組みが求められるテーマにおいては、使いやすさも極めて重要な要素です。最新のツールは直感的でわかりやすいUI設計で、セキュリティの専門家だけでなく、一般のユーザーにも馴染みやすく、使いやすい仕様になっています。

整理された分かりやすい情報表示

セキュリティスコアや各評価項目に関連する詳細情報が整理されてわかりやすく表示されますので、問題の特定や優先順位付けが容易になり、企業は効果的な対策を計画・実行することができます。

⑥ システムの追加、改変、インストール等が不要

最後は、システムの追加、改変、インストール等が不要で、外部からのデータ収集によりセキュリティリスクを評価できる点です。クラウド上でツールを稼働させることで、迅速かつ簡単にセキュリティ状況を把握することができます。

追加のハードウェアやソフトウェアが不要

従来のセキュリティリスク管理ツールには、専用のハードウェアやソフトウェアを用意する必要がありましたが、クラウドベースのサービスであるため、追加のハードウェアやソフトウェアの導入が不要です。そのため、専門知識や追加の設備投資が必要なく、セキュリティリスク管理システムの構築や導入にかかる時間やコストを削減することができます。

導入の簡単さ

追加のハードウェアやソフトウェアの導入が不要であるため、導入が簡単です。また、既存のインフラストラクチャーを変更することなく導入が可能なため、セキュリティリスク管理システムの構築や導入にかかる時間やコストを削減することができます。管理者はブラウザーを開いてアクセスするだけで、セキュリティリスク情報を収集し、分析することができます。

最新の環境での稼働

クラウド上で動作するため、常に最新の環境で稼働しています。そのため、セキュリティリスク管理システムを自社で運用する場合に発生する、システムのアップグレードやメンテナンスにかかる時間やコストを削減することができます。また、クラウド上での動作により、管理者は常に最新の機能やセキュリティアップデートを利用することができます。

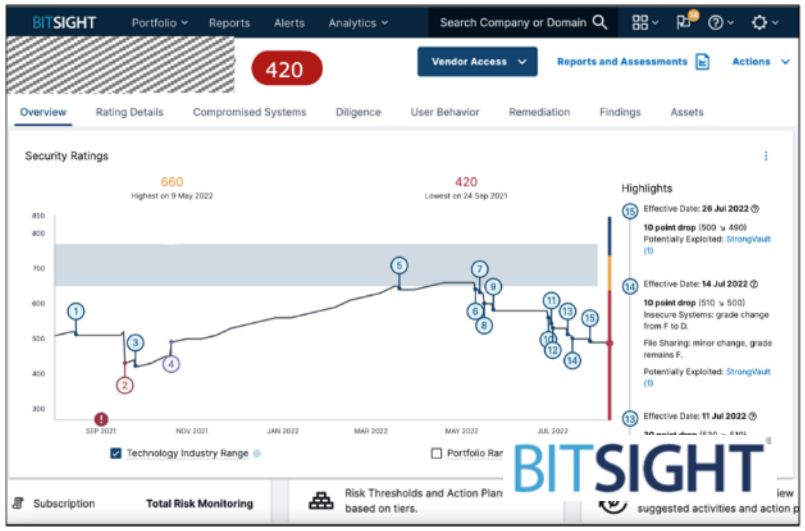
最新のサイバーリスク可視化ツール BITSIGHT（ビットサイト）とは？

ASMサービスの決定版 BITSIGHT

BITSIGHTは、セキュリティリスク評価のための総合的なプラットフォームです。企業やサードパーティリスクの監視、脆弱性管理、サイバー保険の下でのリスク管理などの機能があり、膨大なデータを分析することでセキュリティの問題を素早く特定し、リスク管理を支援できます。

ユーザーフレンドリーなダッシュボードやビジュアル化されたリスク評価の結果など、可視化された情報を提供することで、ユーザーが迅速かつ正確に問題を特定し、対応できるようになっています。さらに、サプライチェーンリスクの監視に特化した機能を備えており、サードパーティのリスクに対しても高い精度で評価できる点が特徴的です。

BITSIGHTを利用することで、サイバーセキュリティを強化し、ビジネスリスクを最小限に抑えることができます。



サイバーリスクの可視化サービスで有名な BITSIGHT社 が開発

BITSIGHT社 とは？

2022年 3月時点

●モニター組織数 4,000 万＋
　(4,000万以上の組織のリスクを可視化)
●顧客数 2400+
　フォーチュン1000の20%、30カ国120以上の政府機関、
　世界のサイバー保険会社の50%を含む
●特許取得数 32
●従業員数 500+
●米国司法省が企業のサイバーリスク評価に活用
–
2011年 ボストンにて設立
2011年 アルゴリズム・方法論の特許取得
2013年 世界初“Security Rating Services(SRS)”リリース
2014年 世界最大シンクホールのAnubisNetworksを買収
2021年 Moody’sによる約270億円の投資とパートナーシップ、
　　Visible Risk買収

【HP】https://www.bitsight.com/

詳細 (リスクベクター)

BITSIGHT

サイバーセキュリティリスクにさらされる脆弱性や影響の一例です。
これは攻撃者が知り得る情報でもあります

①侵害されたシステム(Compromised Systems)

・ボットネット感染:Botnet Infections
・スパムメールの発信や中継:Spam Propagation
・マルウェア感染:Malware Servers
・高リスクの通信:Unsolicited Communications
・悪用される可能性のあるホスト:Potentially Exploited

②実装の正しさ(Diligence)

・SPF・DKIM・SSL Certificates・SSL Configurations・Open Ports・Web Application Headers
・Patching Cadence (パッチの適切な運用)・Insecure Systems・Server Software・Desktop Software
・Mobile Software
・DNSSEC
・Mobile Application Security
・Domain Squatting (不正目的のドメイン取得)

③ユーザーの行動(User Behavior)

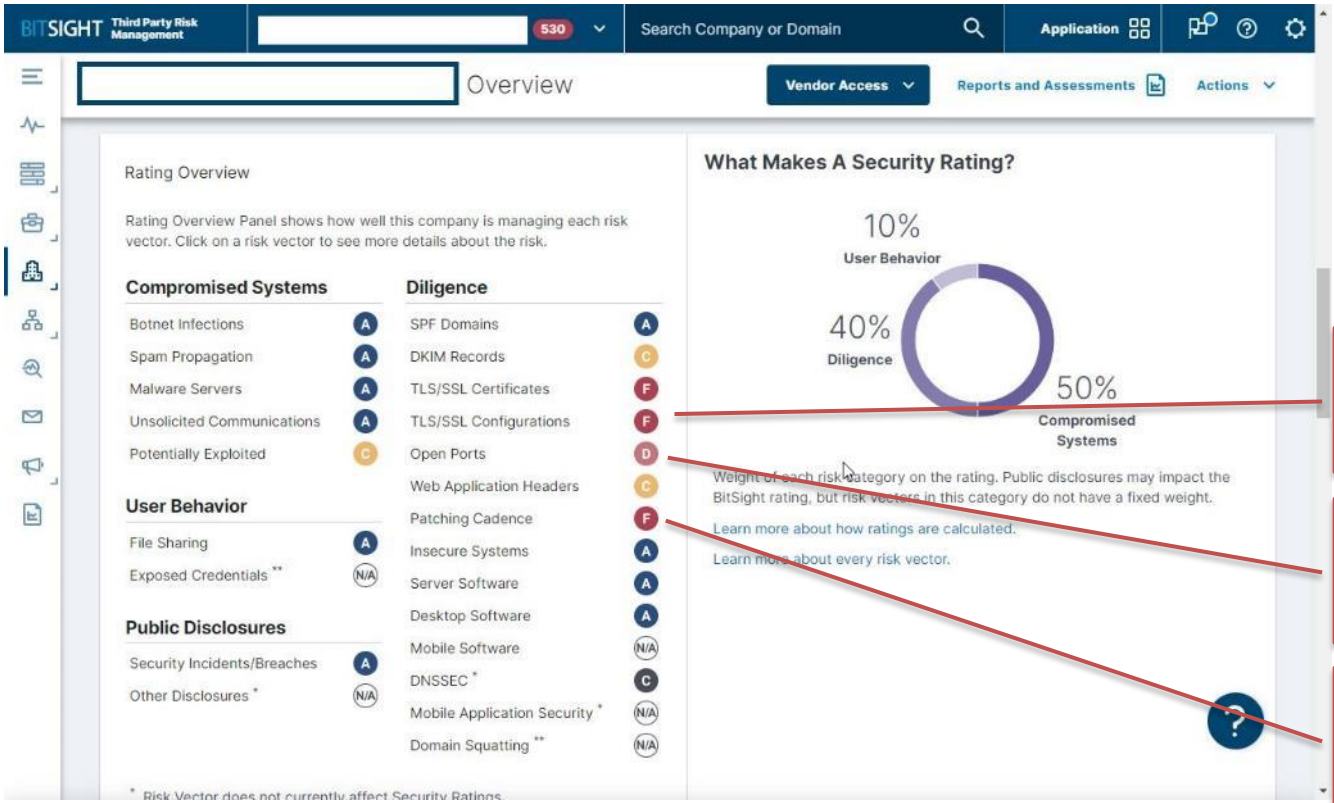
・File Sharing:BitTorrentで共有されているファイル情報
・Exposed Credentials :搾取・公開された認証情報

④公開情報(Public Disclosures)

・Security Incidents:発生したセキュリティ事故
・Other Disclosures:その他の開示情報

リスクベクターの可視化の例

BITSIGHT



TLS/SSLの証明書や
設定が良くない

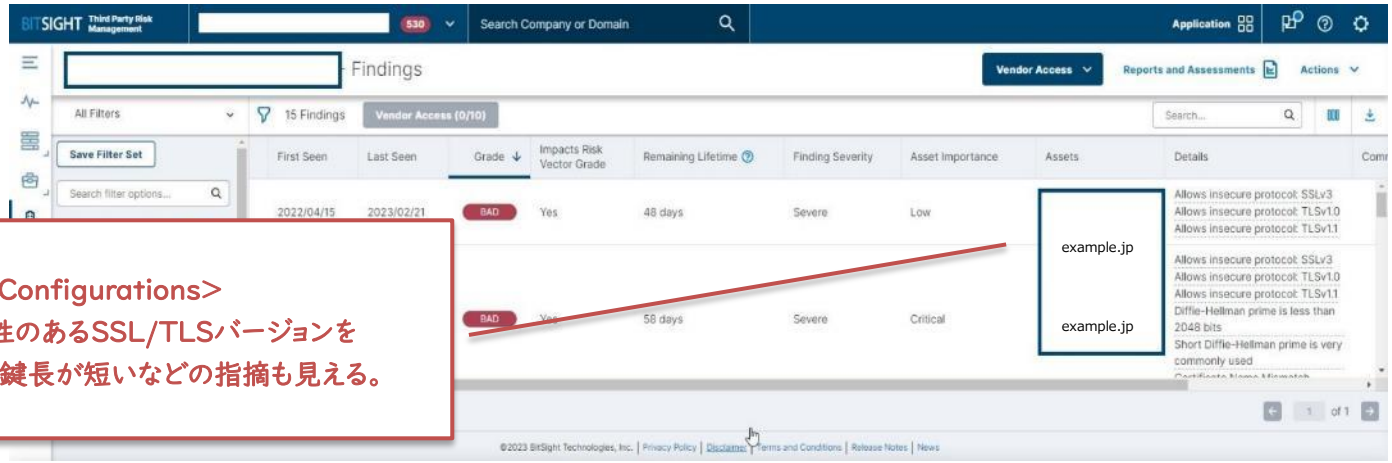
不要なポートが
開いているのでは？

パッチが当たっていない

詳細な可視化の例

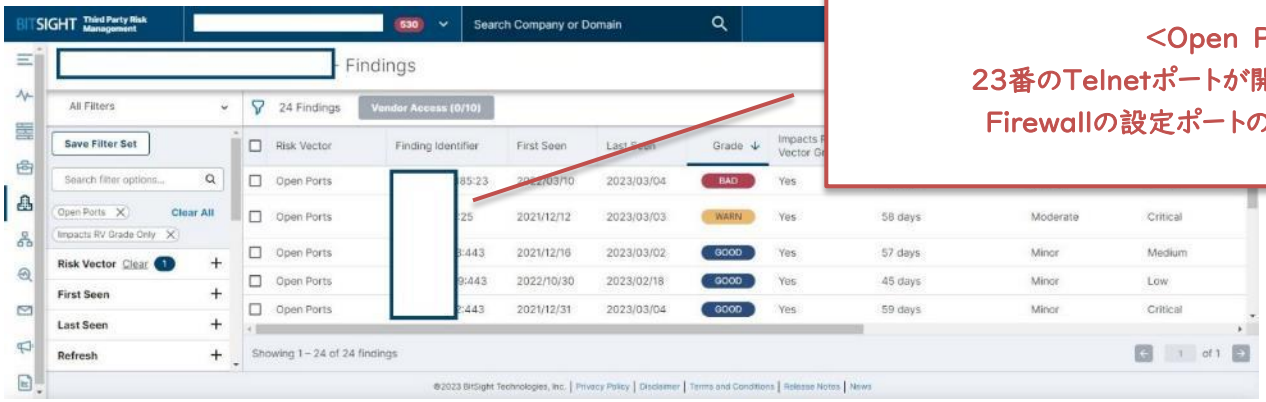
BITSIGHT

TLS/SSL Configurations



<TLS/SSL Configurations>
そのWEBサーバが脆弱性のあるSSL/TLSバージョンを
許容していることが分かる。鍵長が短いなどの指摘も見える。

Open Ports



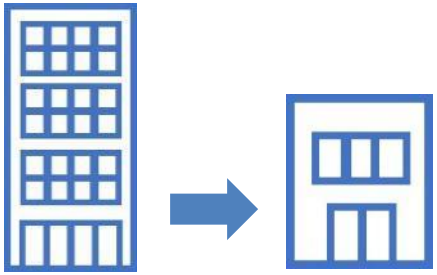
<Open Ports>
23番のTelnetポートが開いている事が見える。
Firewallの設定ポートの閉め忘れの可能性。

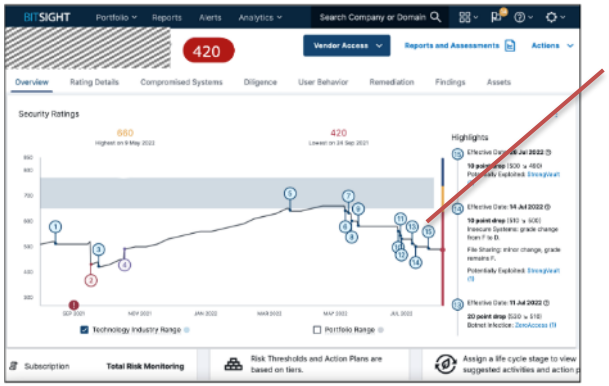
BITSIGHT の活用場面

BITSIGHT

自社や自社のグループ会社はもちろん、
サプライヤーや新規取引先を可視化して評価もできる

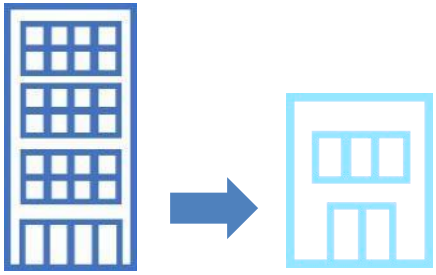
サプライヤーの可視化・評価

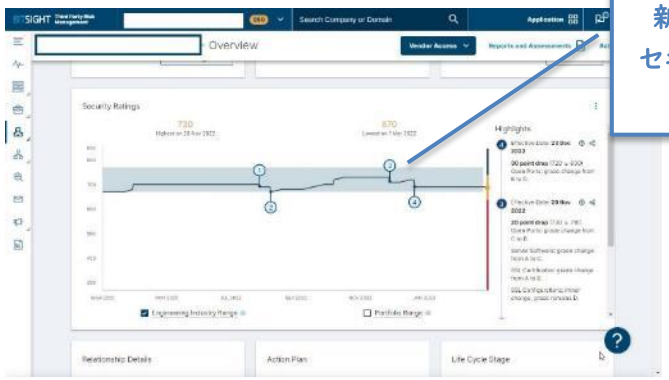




サプライヤーには、具体的に改善ポイントを伝えて是正を促そう。

新規取引先（第3者）





新規取引を開始するにあたり、セキュリティ面は問題無さそうだ。

最新のサイバーリスク可視化ツール「BITSIGHT」
より詳しい資料のご提供、無料相談受付中

BITSIGHT

こちらをクリックで

メールで
お問い合わせ

または、お問い合わせ先メールアドレスまで
seibu-web-market@seibu-denki.co.jp

最後までお読みいただきありがとうございました。
無料相談やより詳しい資料もご用意がございますので
お気軽にお申し付けください。