BITSIGHT

- 攻撃者から見たサイバーリスクの可視化 -

Bitsightご紹介資料

ASM(Attack Surface Management)

2026.8
ストリングアイル合同会社

STRINGISLE

Section 1

Bitsight

セキュリティ対策としてASMが注目されている背景

① 企業の攻撃対象領域が急速に拡大

・クラウドシフト，リモートワーク，SaaS乱立により「把握できていないIT資産」が増加
・シャドーIT，設定ミス，放置された資産やドメインなどが攻撃起点になりやすい

② ランサムウェアを含むサイバー攻撃の入口が「既知の脆弱性」に集中

・攻撃者のエコシステム化 (IAB対策)
・近年の侵入経路の多くが公開資産の脆弱性(VPN, Web, RDP 等)，EOL／未パッチシステム etc

③ ガバナンス・サプライヤー管理の要求の高まり

・経営層・監督官庁からの要求,説明責任
・他社から(へ)の要求(SCRM)
・費用対効果,プライオリティの明確化

IAB　: Initial Access Broker
　　企業への不正アクセス手段(侵入口)を調査、リスト化し，
　　ランサムウェア実行犯に販売する攻撃者の総称
SCRM: Supplier Chain Risk Management

効果（今までと何が変わるか）

●日々のセキュリティ運用でBitsightを活用することによる効果

BITSIGHT

●サイバー攻撃の「初期侵入リスク」の把握と軽減

・攻撃者目線で日々変動するセキュリティリスクの把握
・日々公表される脆弱性とIT資産を継続的にチェック
　Internetへ公開していない資産も含む （＊1）
・対策を行うべきリスクの優先度の判断
・管理対象外のIT資産,ドメインを検出
・暫定や抜本対策のアドバイス （＊2）

●インシデントやその予兆を早く発見 （＊1）

・侵害されている資産(マルウェア感染,遠隔操作など)を発見
・機密情報のインターネットへの漏洩
・認証情報(ID,パスワード) の漏洩,売買
・スパムメールの踏み台

●セキュリティガバナンスのチェックや指標(KPI)に活用

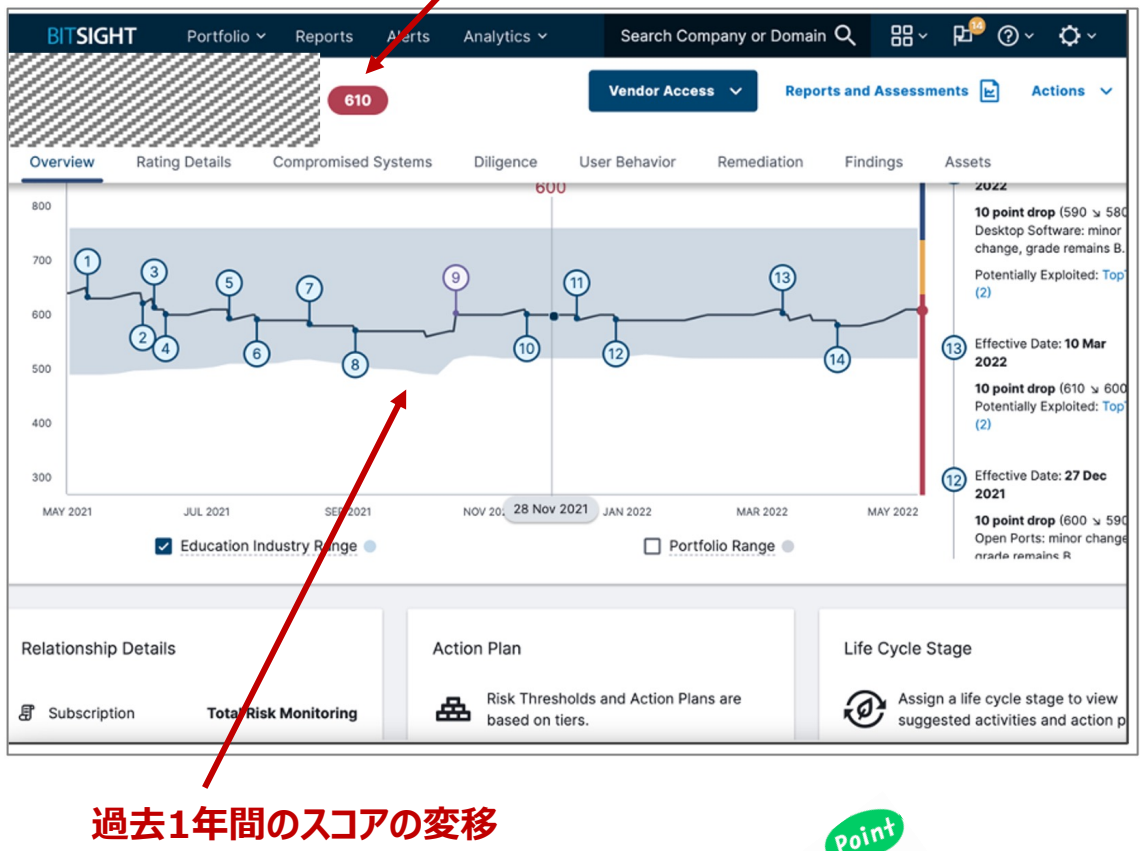
・スコア改善を中期的な目標に
・セキュリティガバナンスのチェック
・子会社,取引会社,海外拠点等のリスク把握と是正
・自社業界のセキュリティフレームワークとの差分チェック
・ステークホルダ(取引先,顧客,株主等)へのアピール,エビデンス

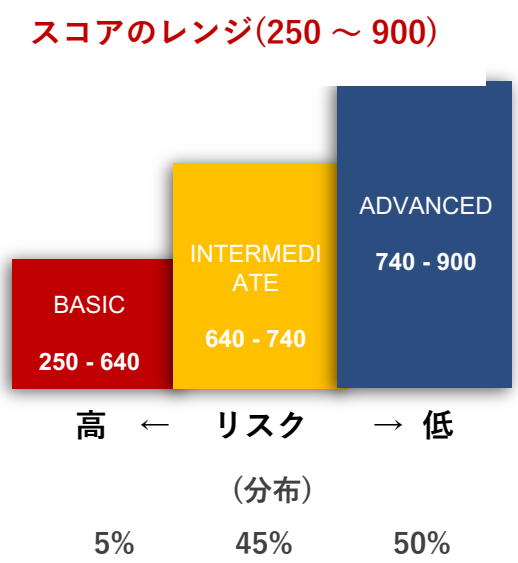
（＊1） ASMの中でBitsightの強みです
（＊2） 弊社のアドバイザリーサービスを含みます

ASM「Bitsight」

● Bitsight(ビットサイト)とは

Internetの様々な情報を収集・分析し,企業のセキュリティリスクを**攻撃者目線で可視化**するサービス(SaaS)です。





Internet上のデータだけで可視化するため、ログの送信やセンサー設置などの企業側での作業は一切不要です。

Bitsight会社紹介

● Bitsight Technologies, Inc.

・本社：米国ボストン（111 Huntington Ave, Suite 400, Boston, MA 02199）
・CEO：John Clancy

● 主要数値・実績（2026年5月）

・モニター組織数（可視化企業数） **4,000万社以上**
・プラットフォーム上のアクティブ組織数 **75,000組織以上**
・顧客数 **3,500社以上**
　- Fortune 500企業に採用（Bitsight公式サイトの表記）
・特許取得数 75件以上
・日次処理サイバーイベント 5,400億件以上／常時スキャンIPアドレス 40億
・Forrester Wave™ Cybersecurity Risk Ratings Platforms, Q2 2026 で Leader に選出
・Gartner® Magic Quadrant™ for Cyber Threat Intelligence Technologies 2026 で Visionary に選出

● 経緯

・2011年 ボストンにて設立。セキュリティレーティング（格付け）分野を創出
・2013年 世界初の "Security Rating Services（SRS）" をリリース
・2014年 世界最大シンクホールの AnubisNetworks を買収
・2021年 **Moody's による2.5億ドル（約270億円）の投資とパートナーシップ**
　VisibleRisk 買収
・2022年 ThirdPartyTrust 買収（第三者リスク管理／2022年8月発表）
・2024年 **Cybersixgill 買収（1.15億ドル・脅威インテリジェンス／ダークウェブ）**
・2025年 Brand Intelligence／Cyber Risk Command Center を提供開始
・2026年 Security Posture Management 提供開始、John Clancy が CEO 就任

BITSIGHTソリューション
外部に公開しているデジタルエコシステム全体におけるセキュリティリスクへ優先的に対処

https://www.bitsight.com/jp

可視化の結果 (詳細)

● 可視化が可能な項目(リスクベクター)を以下に示します。

①侵害の状況 (Compromised Systems)

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

②ユーザに関するリスク(User Behavior)

	Risk Vector	意味
1	File Sharing	インターネットで共有されている機密情報
2	Exposed Credentials	搾取・公開された認証情報

③公開情報(Public Disclosures)

	Risk Vector	意味
1	Security Incidents /Breaches	公開されたインシデント情報
2	Other Disclosures	その他の開示情報

④サービスやアセットのセキュリティ実装,運用の正しさ(Diligence)

	Risk Vector	意味
1	SPF Domains	メールセキュリティ(SPF)
2	DKIM Records	メールセキュリティ(DKIM)
3	TLS/SSL Certificates	暗号化通信の電子証明書
4	TLS/SSL Configurations	暗号化通信の実装方法
5	Open Ports	危険なサービス(ポート)の観測
6	Web Application Headers	Webコンテンツの実装の問題
7	Patching Cadence	脆弱性とその運用の問題
8	Insecure Systems	危険なシステム
9	Server Software	サーバの問題
10	Desktop Software	デスクトップの問題
11	Mobile Software	モバイルの問題
12	DNSSEC	DNSセキュリティ(DNSSEC)
13	Mobile Application Security	モバイルアプリの問題
14	Web Application Security	Webアプリのセキュリティ
15	Domain Squatting	不正目的のドメイン取得

ライセンス,費用,付加サービス

●ライセンスと費用は都度お問合せください

●弊社はライセンスのご提供だけでなく、日々の運用業務をサポートします。（現在,数社に実施中）

(例)
・Bitsightで日々変動する貴社のリスクを監視します。リスク発見には対処方法アドバイスを含めて通知します。
特に緊急を要するインシデントの予兆や発生については即時通知します。
・発見されたリスクの暫定/根本的改善方法のアドバイザリーを行います。
・グループ会社/サプライヤーのリスクマネジメント運用業務の策定支援を行います。
・改善に向けた定例MTGを開催します。

Section 2

Bitsight CTI (別ライセンス)

Bitsight Cyber Threat Intelligence

Bitsightと合わせてCTIをご契約いただき、より高度なセキュリティ運用を実現されるケースが増えています

Bitsight Cyber Threat Intelligence(CTI)

Cyber Threat Intelligence(CTI)は，脅威情報と言われるもので，ASMの得意とするその企業の表層からリスクを検知するだけでなく，ダークウェブやアンダーグラウンドマーケットと言われる攻撃者が活動する領域から脅威情報を収集し,検索を可能とします。
世界中の企業，MSSP，政府機関や法執行機関で活用されています。

これにより，セキュリティチームに対して調査能力を与え、アクション可能な洞察を得られるようにすることで、データ侵害の防止、ブランド保護、リアルタイムでの調査や不正アクセスの早期検知、アタックサーフェスの最小化を支援します。

Bitsight Cyber Threat Intelligence(CTI)

主な特長

自動化された脅威インテリジェンス収集

- サーフェスウェブやダークウェブ各所のフォーラム、チャット、マーケットプレイス、SNS グループなどを自動巡回し、インテリジェンスを収集 (1 日あたり複数回巡回)
- AI と機械学習を活用し、ノイズの多いデータから意味のある脅威インテリジェンスを抽出、レピュテーション付けし、より意味合いの高いものにフォーカスした調査が可能

リアルタイムアラート

- ドメイン名、企業名、ブランド名、取締役名などに関連するインテリジェンスが検出されれば即時に通知

攻撃者(脅威アクター)のプロファイリング

- 脅威アクターの行動履歴や発言傾向、利用するツールなどを整理しプロファイリングを支援

SOAR/SIEM との連携

- 主要 SIEM ソリューションや SOAR ソリューションとのインテグレーションも可能
- 自動レスポンスやリスク分析の効率化を支援

Section 3

Appendix

CSF2.0とBitsightの対応

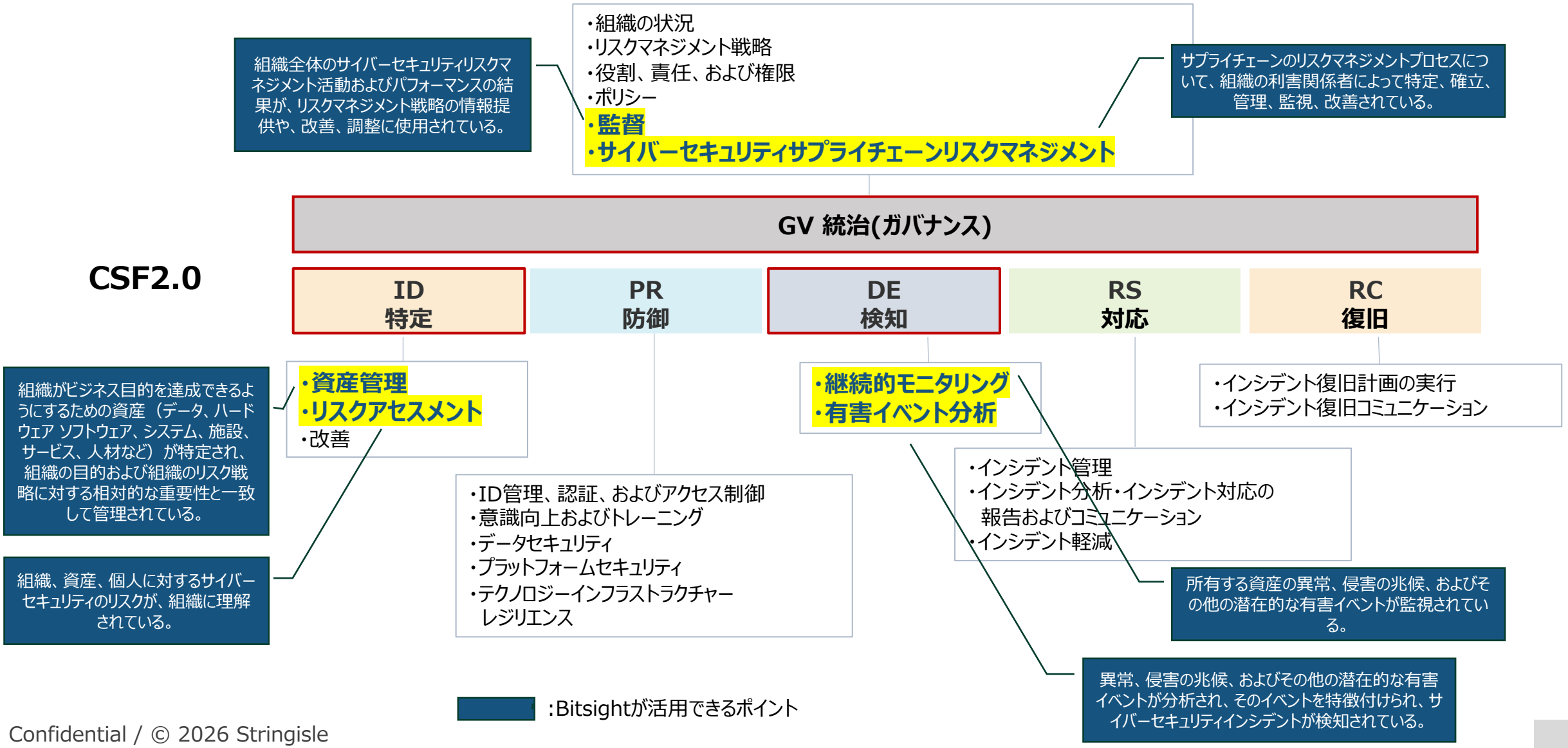
CSF (Cybersecurity Framework) は、アメリカ国立標準技術研究所（NIST）が提供している、組織や団体がサイバーセキュリティリスクを管理し、強化するためのガイドラインです。(最新はCSF 2.0) 。
企業や団体のセキュリティ対策として最も参考とされているもので、下記6つのエリアで定義されています。

CSF2.0

・ガバナンス（GV）：組織のサイバーセキュリティリスクマネジメント戦略、期待、ポリシーが確立され、伝達され、監視されている。
・特定（ID）：組織の現在のサイバーセキュリティリスクが理解されている。
・防御（PR）：組織のサイバーセキュリティリスクを管理するための保護策を使用されている。
・検知（DE）：潜在的なサイバーセキュリティ攻撃および侵害が発見され、分析される。
・対応（RS）：検出されたサイバーセキュリティインシデントに関して措置が講じられる。
・復旧（RC）：サイバーセキュリティインシデントの影響を受けた資産および運用が復旧される。

CSF2.0とBitsightの対応

CSF2.0においてBitsightを効果的に活用できるポイントを以下に示します。
ASMの中でもBitsightは多くの機能を有していますので、ASMと比較しより広い範囲で活用可能です。



Section 4

ASM比較

The Forrester Wave™: Cybersecurity Risk Ratings Platforms, Q2 2026

https://www.forrester.com/report/the-forrester-wave-tm-cybersecurity-risk-ratings-platforms-q2-2026/RES192714

Bitsightのデモやご提案,お見積りのご相談は下記までお問合せください。

ストリングアイル合同会社

contact@stringisle.com

〒819-0168
福岡県福岡市西区今宿駅前1丁目15番18号
マリブ今宿シーサイドテラス３階

www.stringisle.com

Services
- Security services
- SI /Project management /PMO
- Customer success
- IT platform
- IT education

Office
- Fukuoka
- Yokohama

- Since 2020 -