HITACHI

株式会社日立システムズ

今、組織が備えるべきサイバー脅威への対策をご提案
SHIELDグローバルインテリジェンスサービスのご紹介

グローバル＆セキュリティサービス事業グループ
セキュリティサービス事業部
セキュリティサービス・ソリューション本部
セキュリティサービス部
第二グループ

目次

1． SHIELDグローバルインテリジェンスサービスのご紹介

HITACHI

サービス概要

各国のセキュリティ情勢に精通した世界中のアナリストが分析した
脅威インテリジェンス／ぜい弱性情報／IoC情報をWebポータルで提供するサービス

脅威インテリジェンス情報	本サービスで提供している情報例として、サイバー犯罪に関わるセキュリティ侵害情報、諜報活動・政治的動機などによるセキュリティ侵害情報、これらの侵害に用いるマルウェア解析情報があり、**脅威に対する分析結果・回避策・関連情報**を提供します。
ぜい弱性情報	**既知・未知、および本サービス独自**に発見・検証した製品のぜい弱性情報を提供します。 ぜい弱性情報は**分析結果に加えて回避策やぜい弱性に関連した付随情報**も併せて提供します。
IoC情報 （Indicator of Compromise）	サイバー攻撃の**痕跡情報（マルウェアの通信先IPアドレス・ドメイン、ハッシュ値など）**を提供します。

主要な情報源

・専門アナリストによるHUMINT、オープンソース、ブラックマーケットからの情報
・ダークウェブ、ディープウェブからの情報
・世界中の100人を超えるセキュリティ研究者が発見したゼロデイのぜい弱性情報

（※）本サービスで提供する一部の情報には英語が含まれます

HITACHI

本サービスの位置づけ

凡例
- サービス対象
- 非対称

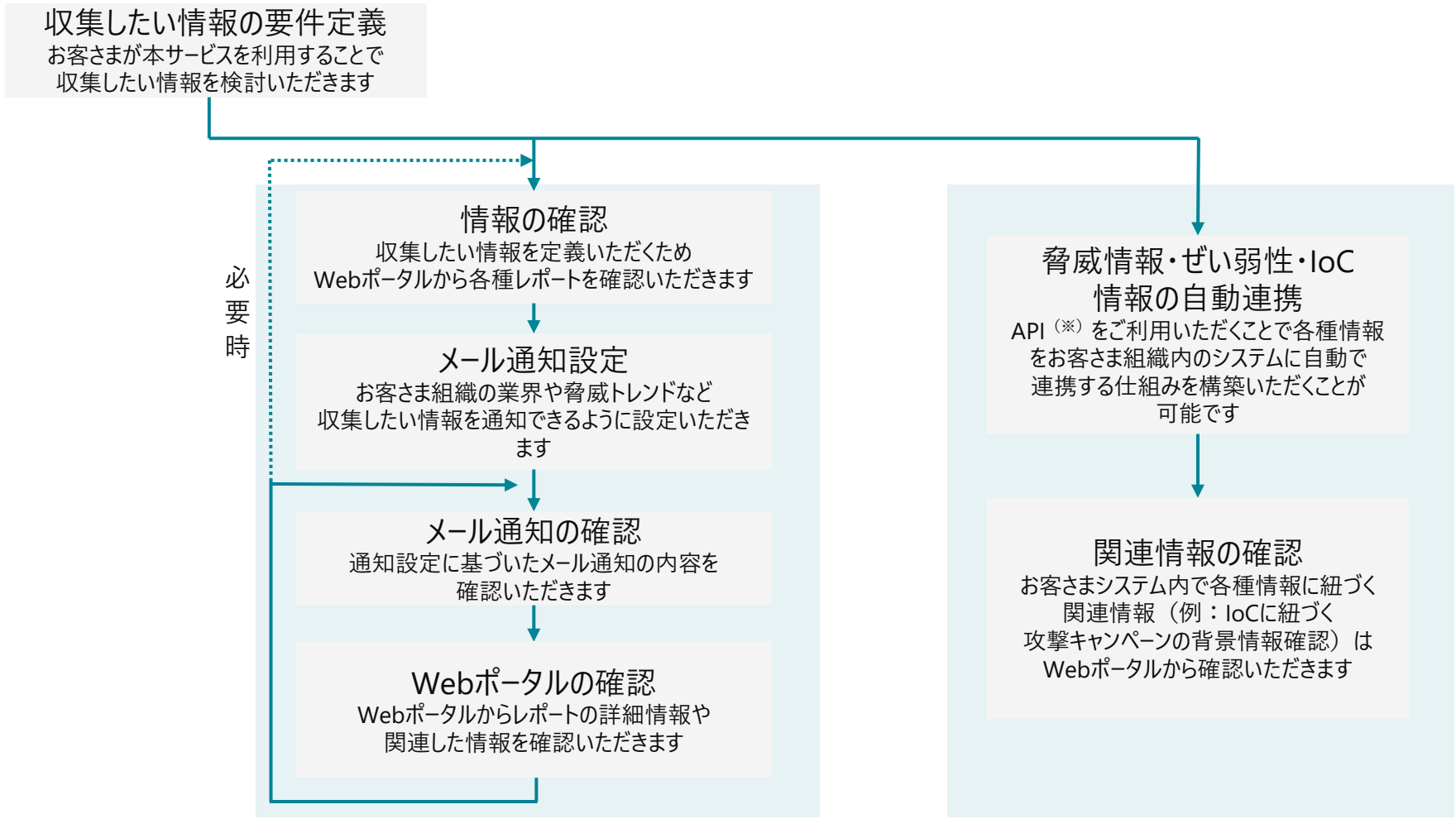
情報提供種別	戦術的インテリジェンス IoC（IPアドレス、URL、ハッシュ値など）の提供	運用的インテリジェンス 攻撃者のTTP、キャンペーン情報、攻撃アクター分析などの情報提供	戦略的インテリジェンス 地政学的リスク、業界の脅威トレンド、政策変化などの情報提供
提供方式	レポート提供型 人が読む前提のレポート形式での情報提供方式	マシン連携型（※） IoCなどをAPIをはじめとする手段で自動的にシステム連携する方式	検索型 情報ソースから効率的・効果的に必要な情報を検索する方式
情報収集ソース	OSINT 一般に公開されている情報源を収集・分析して得られるインテリジェンス	ダークウェブ・ディープウェブ 匿名性を前提としたWeb、検索エンジンにインデックスされていないWeb	HUMINT 人の行動や発言、関係性などを通じて得られる情報
運用スタイル	セルフサービス型 サービス、ツールを自組織のメンバーで利活用する運用スタイル	マネージド型 ベンダーが運用支援を含めて実施する方式	

本サービスにて想定しているお客さま一例

・脅威インテリジェンスのサービスを**初めて活用しようと検討されているお客さま**
・脅威インテリジェンスを活用されているが、情報の分析を実施する**専門的な知識を持つ担当者の育成が難しいお客さま**

（※）マシン連携に該当する機能の利用はオプションサービスのご契約が必要です

本サービスの活用イメージのフロー



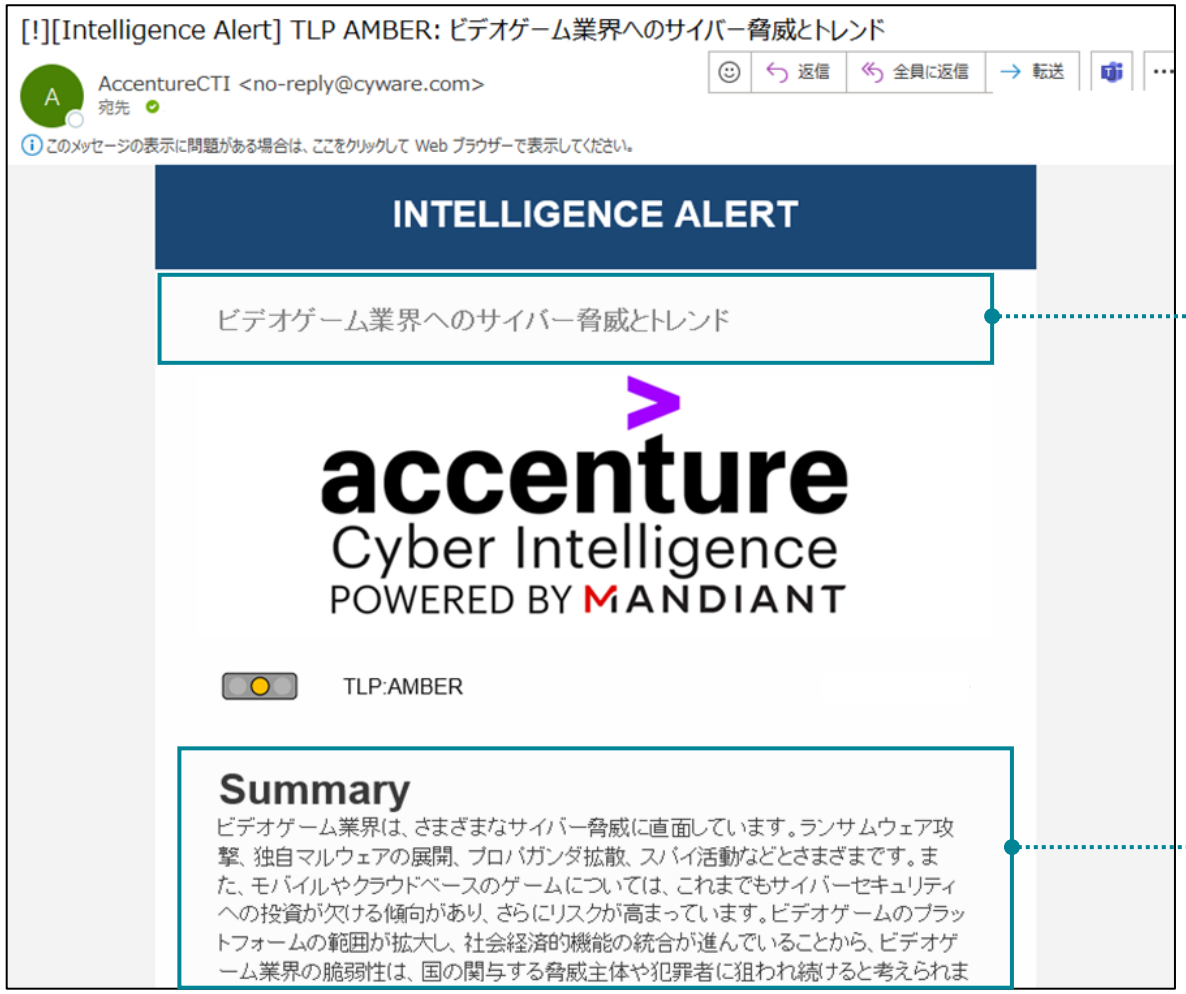
（※）APIのご利用にはオプションサービスのご契約が必要です

HITACHI

Webポータル画面

レポート一覧	レポートの内容	レポート周辺情報
脅威インテリジェンス、ぜい弱性情報などの一覧	各レポートの内容（概要、分析結果、回避策など）	各レポートのID・カテゴリなどの周辺情報

メール通知内容



タイトル

レポートのタイトル情報

レポート内容

メール本文から対象レポートの全文をご確認いただけます。なお、レポートに関連する情報を閲覧いただきたい場合は、Webポータルからご確認いただけます。

HITACHI

実用的な脅威インテリジェンス情報の提供

お客さまの適切な意思決定のサポートを目的として、さまざまな国やバックグラウンドを持つアナリストにより
検知、分析した脅威インテリジェンス情報をご提供します

グローバルな ネットワーク	・150人以上のインテリジェンスプロフェッショナルの集団 ・11か国に拠点があり、22か国の言語に対応できる人材を確保
経験豊富 アナリスト	インテリジェンスコミュニティや法執行機関での経験をもつインテリジェンスアナリスト・ マルウェア解析エンジニアなど豊富なバックグラウンドのアナリスト集団

【実用的な脅威インテリジェンスの特徴】

短期的～長期的な 脅威に関する情報提供	短期的な脅威から長期的な脅威にかかるまで、 あらゆる角度からの脅威についての分析結果をご提供します
脅威に関する 深い調査	技術的観点や地政学的観点など、さまざまな観点での対応経験を持つ セキュリティアナリストによる深い調査による情報をご提供します。
関連するIoC情報 の提供	脅威情報に関連する通信先URL、IPアドレス、ハッシュ値などの IoC情報をご提供します。

HITACHI

【短期的～長期的な脅威に関する情報提供】

短期的に対策が必要な情報のご提供

リアルタイムで発生した脅威に関する情報を提供
情報漏えい事案や攻撃アクターの動向などに関する情報を提供

〇情報提供例（レポート記事タイトル）

- 攻撃アクター「Anon-WMG」が自動車業界の大手企業へのネットワークアクセス情報を宣伝
- 重大なぜい弱性がQilinランサムウェア攻撃で悪用される
- Acreed Stealer の脅威の評価と検出

中期的な視点でのサマリ情報のご提供

ランサムウェア事案や特定地域のハクティビスト活動などについて
週次などでサマリした情報をご提供

〇情報提供例（レポート記事タイトル）

- 中南米サイバー脅威隔週レポート: 2025年5月21日～6月4日
- 2025年NATOサミットを狙うサイバー活動 (隔週レポート): 2025年6月4日～17日
- ウクライナ戦争の影響について: 2025年3月～5月

長期的な視点における脅威の分析

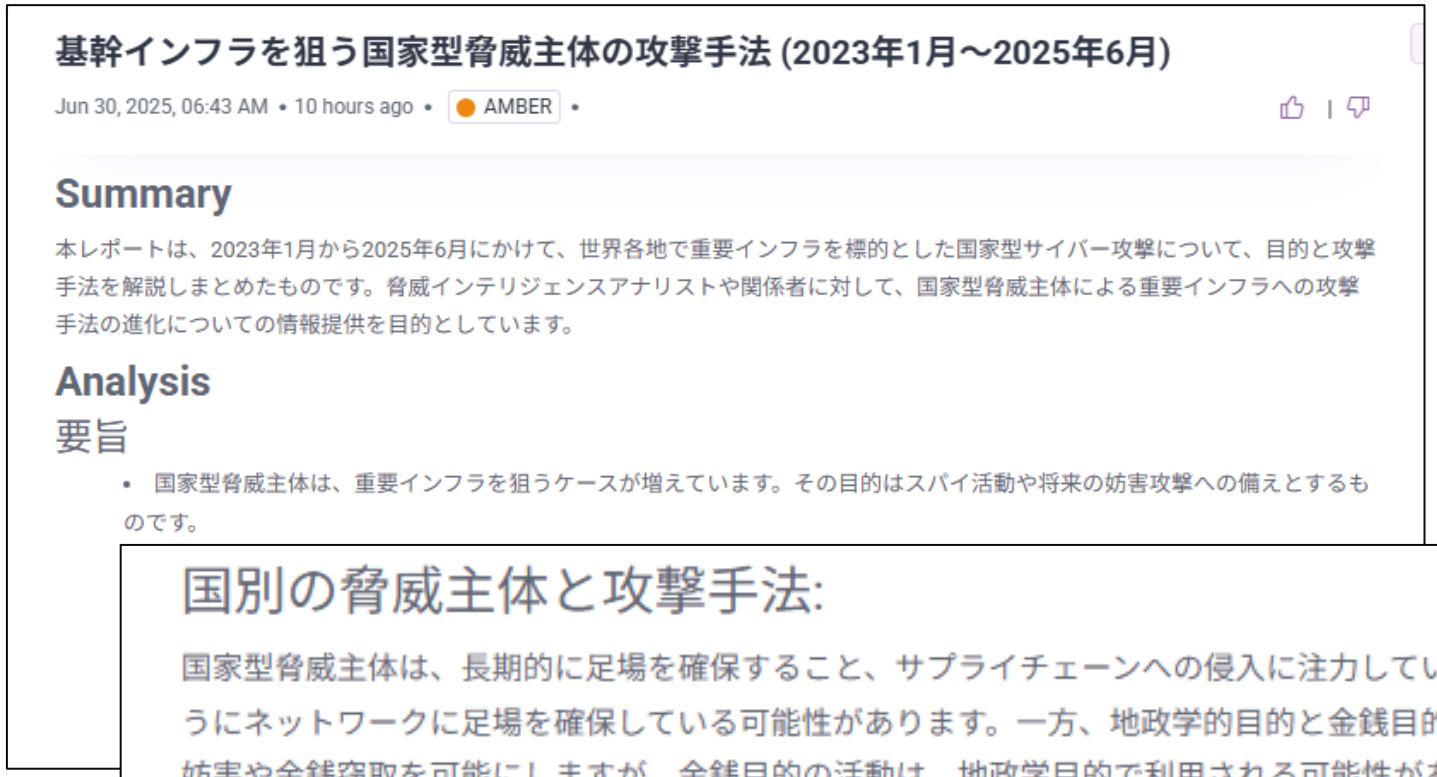
業界、地域、攻撃グループなどのさまざまな対象を
長期的な目線で分析した情報をご提供

〇情報提供例（レポート記事タイトル）

- 基幹インフラを狙う国家型脅威主体の攻撃手法 (2023年1月～2025年6月)
- 業界別の脅威: 医療機器
- 日本、サイバー先制攻撃を認める法律を成立

HITACHI

【脅威に対する深い調査】
【レポート例（抜粋）】


基幹インフラを狙う国家型脅威主体の攻撃手法 (2023年1月～2025年6月)

Jun 30, 2025, 06:43 AM • 10 hours ago • AMBER •

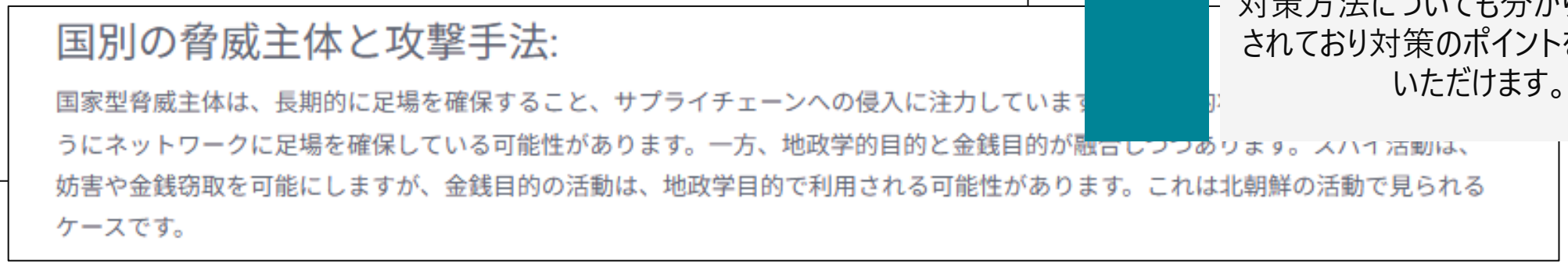
Summary

本レポートは、2023年1月から2025年6月にかけて、世界各地で重要インフラを標的とした国家型サイバー攻撃について、目的と攻撃手法を解説しまとめたものです。脅威インテリジェンスアナリストや関係者に対して、国家型脅威主体による重要インフラへの攻撃手法の進化についての情報提供を目的としています。

Analysis

要旨

- 国家型脅威主体は、重要インフラを狙うケースが増えています。その目的はスパイ活動や将来の妨害攻撃への備えとするものです。


国別の脅威主体と攻撃手法:

国家型脅威主体は、長期的に足場を確保すること、サプライチェーンへの侵入に注力しています

うにネットワークに足場を確保している可能性があります。一方、地政学的目的と金銭目的が融合しつつあります。スパイ活動は、妨害や金銭窃取を可能にしますが、金銭目的の活動は、地政学目的で利用される可能性があります。これは北朝鮮の活動で見られるケースです。

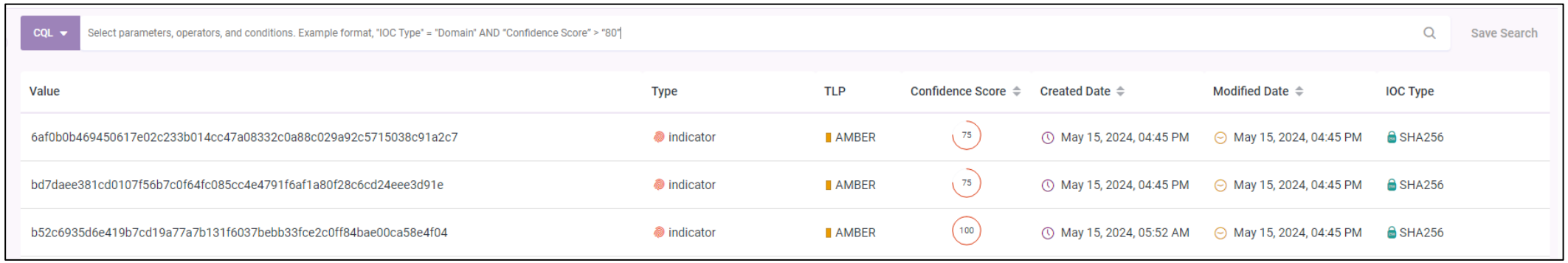
概略

世界各国の重要インフラは国家型サイバー攻撃グループにおいての主な標的の一つです。

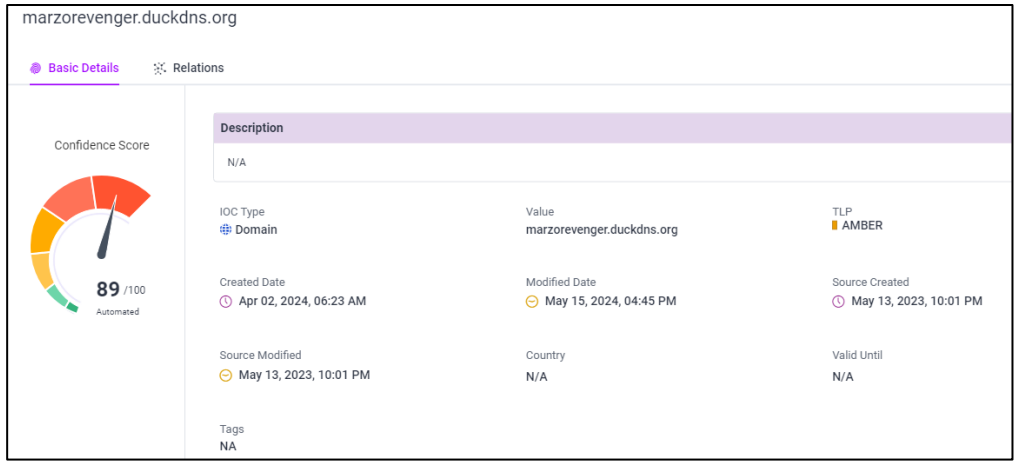
国別に行われている攻撃内容や攻撃の目的などの情報を分かりやすく説明しています。

重要インフラに対するサイバー攻撃の対策方法についても分かりやすく説明されており対策のポイントを迅速把握いただけます。

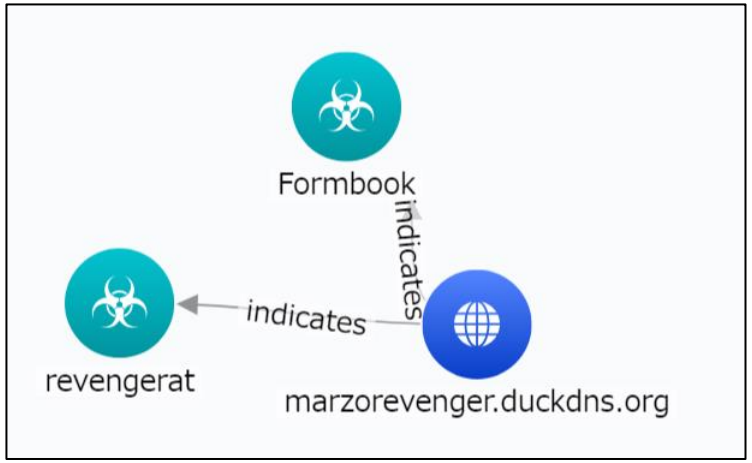
【関連するIoC情報の提供】



一覧画面　IoCなどの関連情報の一覧を確認できる画面



IoC 詳細画面　IoCの信頼性スコアや最初・最後に確認された日時情報などを提供



関連性情報　IoCに関連するマルウェアや攻撃者、攻撃事案などとの関連性（リンク）情報を提供

HITACHI

豊富なぜい弱性情報のご提供

20年以上のサービス提供実績があり、世界中の幅広いぜい弱性の情報収集源としてご利用いただけます

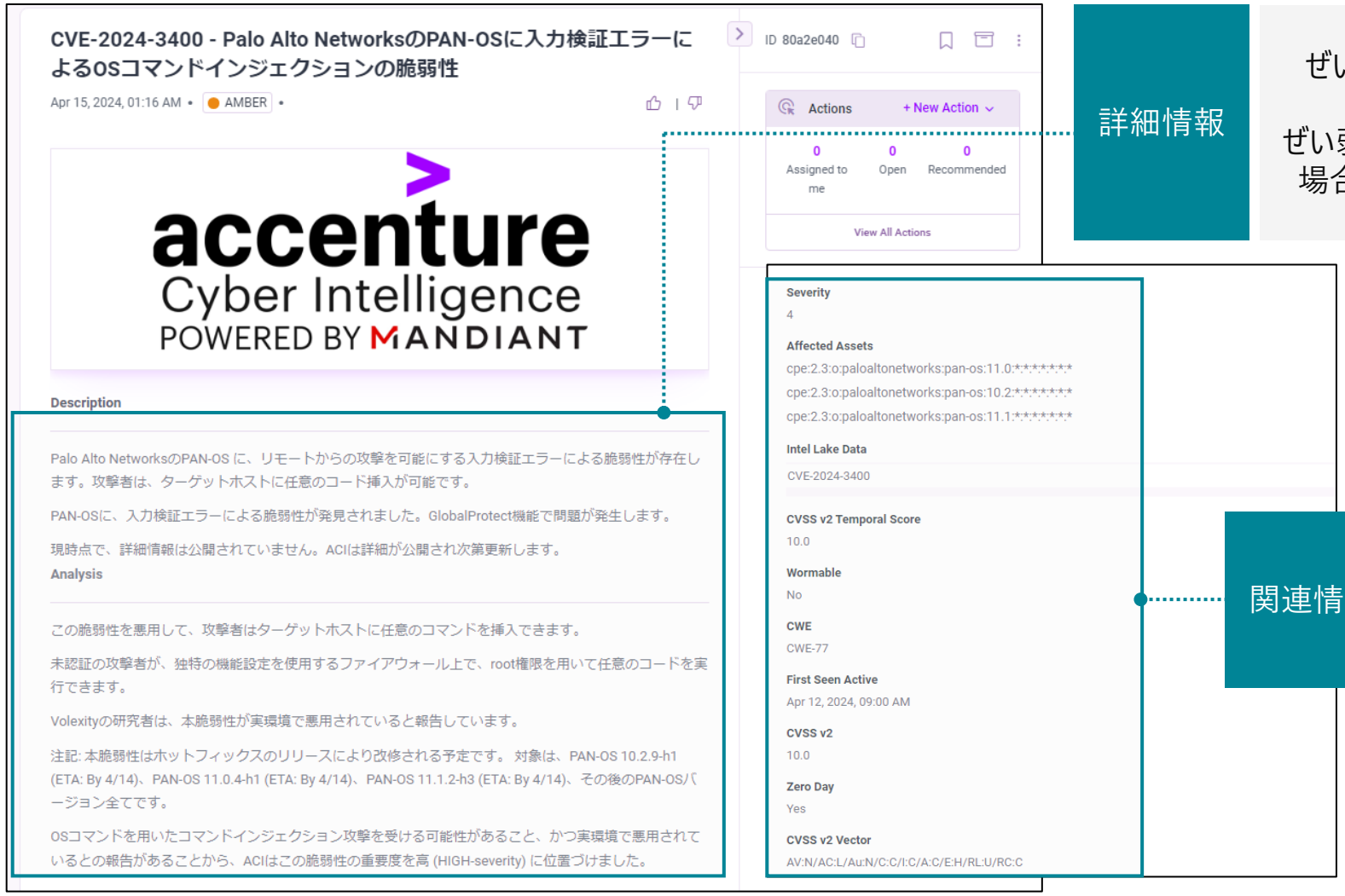
豊富なぜい弱性情報提供	・毎年1万件を超えるぜい弱性情報の提供実績 （提供実績：2023年 14,000件、2022年 11,000件、2021年 10,000件以上）
幅広い製品への対応	本サービス独自情報を含む7,000組織以上の製品、および 10万件以上のぜい弱性情報の提供

【ぜい弱性情報の特徴】

ぜい弱性の詳細情報をご提供	アナリストが分析した情報や回避策などの情報に加えて、周辺情報（情報ソース、CVSS値、影響を受ける製品、ゼロデイ有無、など）も含めて情報をご提供します。
システム連携に適した情報形態	ぜい弱性情報はCVE（ぜい弱性の識別子）ごとの情報提供であり、 また影響・対策バージョンもCPE形式（製品の識別子）となっているため、 システム連携に適した提供形態です。

HITACHI

【ぜい弱性の詳細情報をご提供】



詳細情報

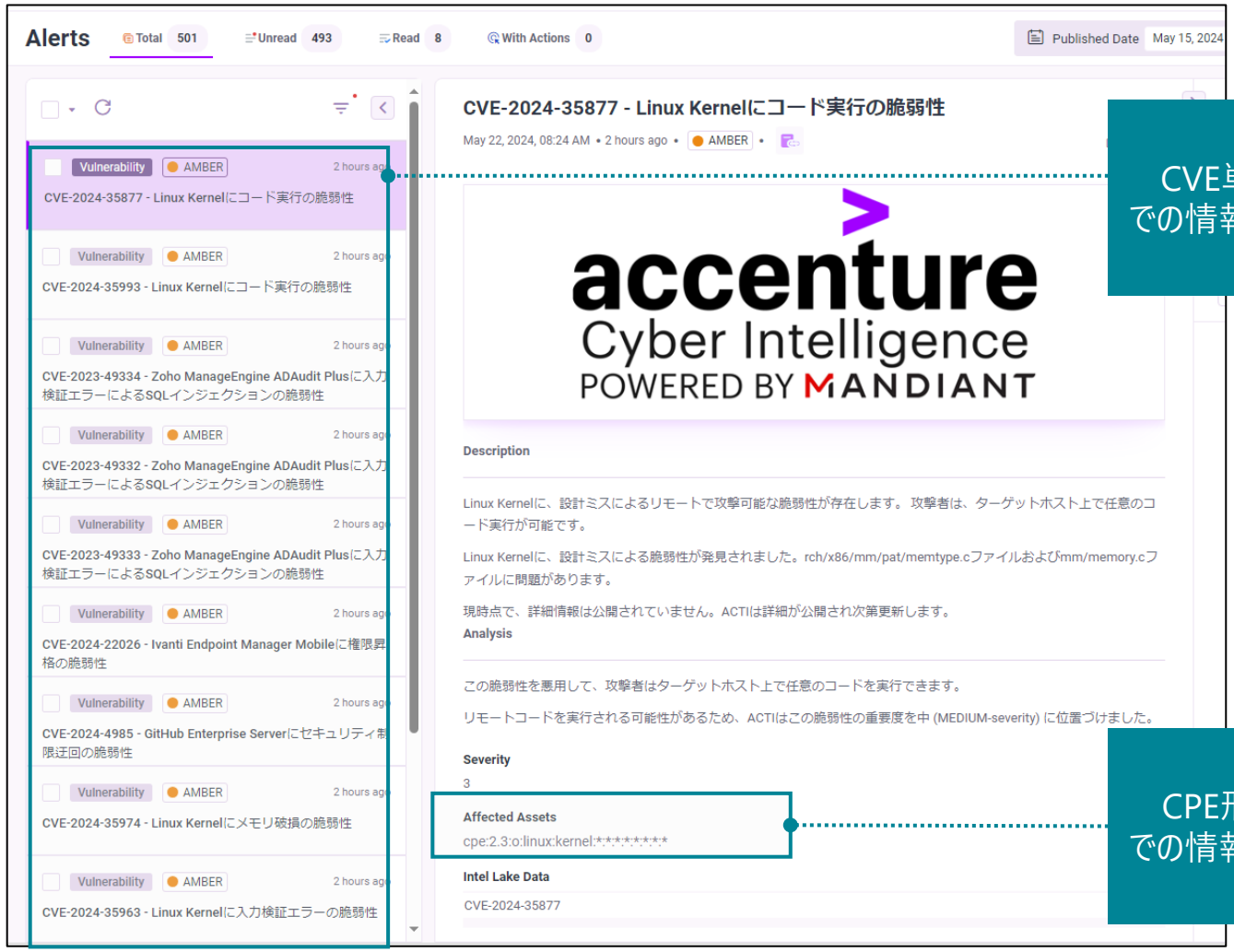
ぜい弱性についてアナリストが詳細に分析した情報を提供します。
ぜい弱性の内容から、そのぜい弱性を悪用された場合の影響などについての詳細を提供します。

関連情報

CVSS値、ゼロデイの有無、
ぜい弱性の悪用が確認された
日時などの関連情報も合わせてご提供

HITACHI

【システム連携に適した情報形態】



CVE単位
での情報提供

ぜい弱性情報は、CVE（ぜい弱性の識別子）ごとの情報提供です。ぜい弱性毎に影響を受ける製品およびバージョンの管理がしやすくシステム連携に適した形態となっています。

CPE形式
での情報提供

CPE（製品およびバージョンの識別子）ごとの情報提供です。膨大な量の社内製品および社内製品バージョンのぜい弱性をシステム的に管理するために適した情報形態です。

HITACHI

サービスメニュー

#	サービス区分	必須/選択	サービスメニュー	内容
1	基本サービス	必須 （#1～#3 のいずれかの 契約が必須）	ポータルアクセス	・ポータルアクセスが可能なライセンス ・ポータルアクセスは25名まで
2			APIアクセス	APIアクセスが可能なライセンス
3			ポータルアクセスおよび APIアクセスのハンドル	・ポータルアクセスとAPIアクセスが可能な バンドルライセンス ・ポータルアクセスは25名まで
4	オプション サービス	選択	追加ポータルアクセス	ポータルアクセスについて1名分のアカウント追加 が可能なライセンス

HITACHI

サービス開始までの流れ

導入実績

サービス販売実績	20社以上 ※2025年7月時点
導入企業様の業種	金融業、情報通信業、製造業、官公庁など多数

・本資料に記載されている会社名および商品名は、各社の商標または登録商標です

HITACHI