脅威インテリジェンスとAIを活用した積極的なサイバーセキュリティー保護対策とは？

オープンテキスト株式会社
ソリューションコンサルティング統括本部
サイバーセキュリティ　ソリューションコンサルティング部
シニアコンサルタント 髙萩華雪

オープンテキスト株式会社ご紹介

The Information Company

OpenText The Information Company

OpenTextは、ビジネスに不可欠な情報を強化・保護し、多種多様な業界・業種のお客様に情報の優位性をもたらします

30年以上に渡り企業のデジタル化を支える企業

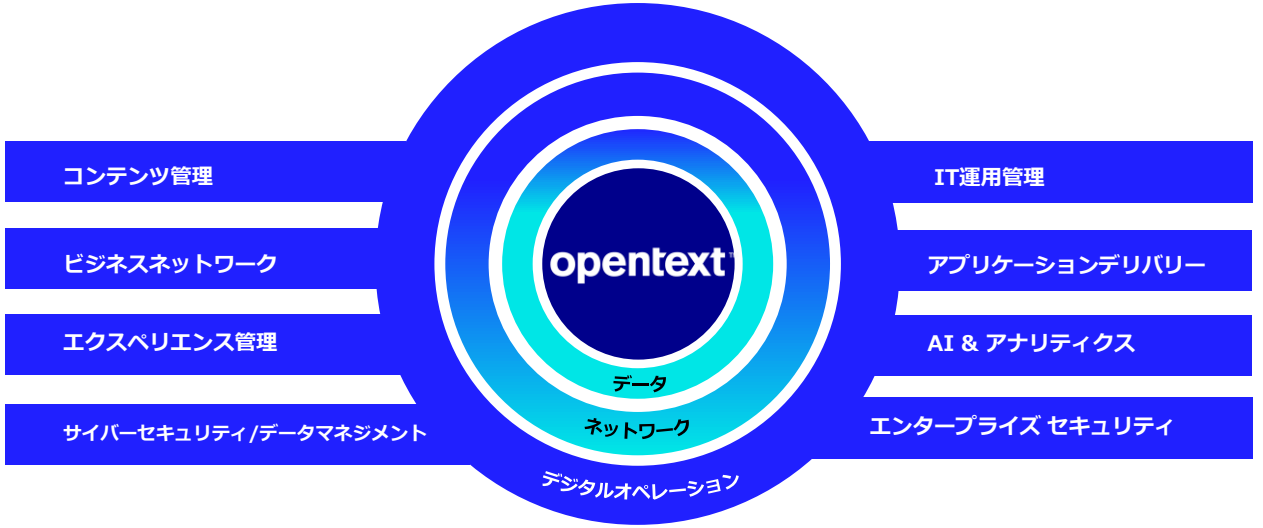
98社
Top100社の利用社数

125,000社
利用企業

2.3万人
従業員数

180カ国
事業展開

OpenTextのソリューションポートフォリオ



マイクロフォーカスとの統合でさらなる価値を提供*

*2023年1月31日（北米時間）にニュースリリース

OpenTextの事業領域＆ソリューション

オープンテキスト株式会社

情報＆デジタルコンテンツ管理

組織全体でビジネス文書やデータを一元的に管理、共有することで、情報の検索性が高まり、業務アプリとの連携による自動化が実現し、不適切な情報管理による漏洩リスクも解消されます。

主な機能

- 文書・コンテンツ管理
- プロセス自動化
- キャプチャ
- アーカイブ・記録管理
- 情報ガバナンス
- ERP/業務アプリケーション連携

デジタルエクスペリエンス

顧客、パートナー、従業員とのすべてのタッチポイントでデジタルエクスペリエンスを変革し、インタラクションを強化することで、生涯にわたる満足度を高め、持続的で価値の高い関係を構築します。

主な機能

- Webプラットフォーム
- メディア資産管理
- デジタルファックス
- 顧客インサイト/分析
- メッセージングAPI

ビジネスネットワーク

ビジネスエコシステムのコネクティビティを簡素化することで、サプライチェーン統合を変革し、将来にわたるスケーラビリティを確保し、コンプライアンスを高め、インサイトを活用できる強固な基盤を構築します。

主な機能

- B2B/EDI統合
- サプライチェーン最適化
- セキュアなコネクテッドエコシステム
- ハイブリッド統合プラットフォーム
- IoT管理

マイクロフォーカスエンタープライズ株式会社

データアナリティクス

大容量データへの同時実行処理に対してパフォーマンスを維持し、且つ、高度な分析を実現するための機械学習も搭載した柔軟性と拡張性をもったデータ分析に最適なプラットフォームを提供します。

主な機能

- データサイエンスプラットフォーム
- 分析ツール
- 分析API

- 統合型分析プラットフォーム

サイバーセキュリティ

様々なセキュリティ脅威を未然に防ぎます。高度な脅威を迅速に検出・対応し、ビジネスの中断させることなく、ハイブリッド環境向けのセキュリティア分析で、変化のスピードに合わせてセキュリティ体制を進化させます。

主な機能

- エンドポイントネットワークセキュリティ
- 脅威インテリジェンス
- デジタルフォレンジック

- アプリケーションセキュリティ
- データプライバシー/プロテクション
- セキュリティオペレーション(SIEM, UEBA, SOAR)
- IDおよびアクセス管理
- バックアップ、リカバリ

デジタル運用管理

統合されたAIベースのコンポーザブルソリューションの採用により、ITインフラストラクチャ管理を最適化し、デジタル運用を効率化することで、ITパフォーマンスを向上させながら、クラウドコストの抑制や、運用の統合化を実現します。

主な機能

- ITSM（サービスマネジメント）
- ハイブリッドクラウド管理
- 運用のオーケストレーション、自動化
- IT資産管理
- イベントおよびパフォーマンス管理
- データセンター自動化
- ネットワーク運用管理

アプリケーションデリバリ管理

AI/MLを採用し、バリューストリーム管理、DevOps、アジャイルアプリケーション開発の戦略立案からリリースまでを一貫し、エンタープライスレベルの高品質のソフトウェア開発をスピーディーにサポートする環境をご提供します。

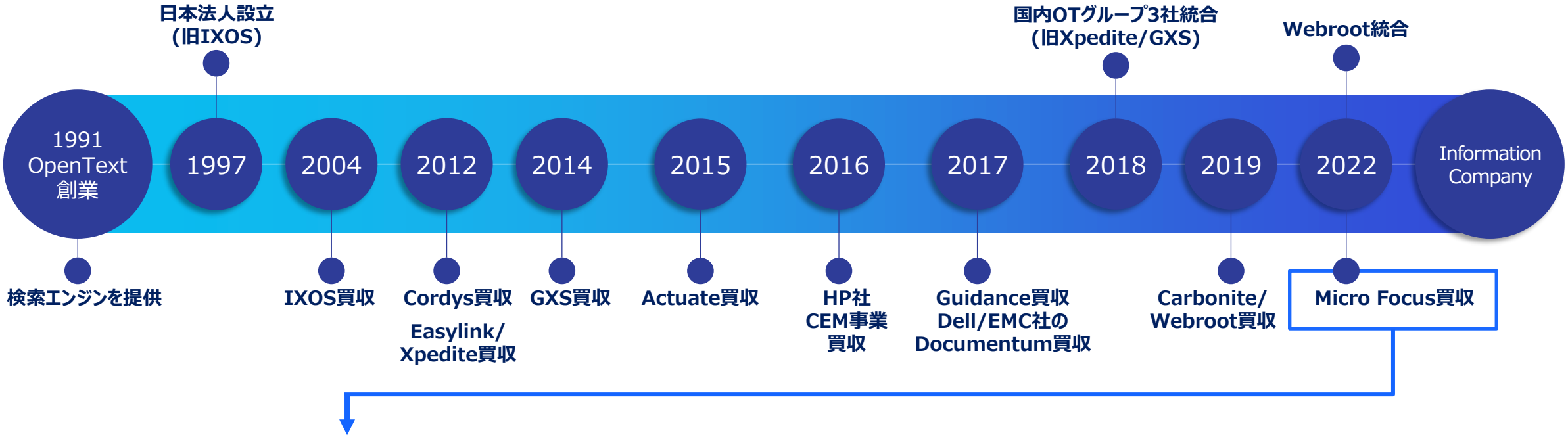
主な機能

- バリューストリーム管理
- アプリケーション機能テスト
- パフォーマンステスト
- アプリケーション戦略
- アプリケーションライフサイクルマネジメント、品質ガバナンス
- アプリケーションデリバリ
- リリースコントロール、管理
- デプロイメント自動化

日本法人情報

オープンテキスト株式会社

1991年に創業し、日本法人は1997年に設立
本社の買収した様々な会社のソリューションを日本でも提供可能
代表取締役社長：三浦 デニース
国内所在地：東京都千代田区丸の内1-8-3丸の内トラストタワー本館18F



マイクロフォーカスエンタープライズ株式会社

2017年9月 Micro FocusによるHewlett Packard Enterprise ソフトウェア事業を統合
2023年1月31日 OpenTextによるMicro Focusの買収完了
代表取締役社長：三浦 デニース
国内所在地：東京都千代田区丸の内1-8-3丸の内トラストタワー本館18F

本日の講演の流れ

1．脅威インテリジェンスとは何か

2．脅威インテリジェンス情報はどのように作られるか

3．　BrightCloud脅威インテリジェンスの活用

4．脅威インテリジェンスの活用 - ArcSight

１．脅威インテリジェンスとは何か

NIST SP800-150による定義

NIST SP 800-150とは

米国国立標準技術研究所（NIST）のNIST SP 800-150はサイバー脅威情報共有に関するガイドラインで、2章サイバー脅威情報共有の基本の中で脅威情報、脅威インテリジェンス、脅威インテリジェンスレポートという用語が定義されています。

NIST Special Publication 800-150 "Guide to Cyber Threat Information Sharing", Chris Johnson et al. 2016

米国国立標準技術研究所（NIST） 、NIST SP 800-150 サイバー脅威情報共有ガイド

ダウンロードリンク：
http://dx.doi.org/10.6028/NIST.SP.800-150

用語の定義:脅威情報とは

脅威情報

“組織が脅威から身を守るため、またはアクターの活動を検出するのに役立つ可能性のある、脅威に関連する情報”

脅威情報	NIST SP 800-150 2章の説明
インジケーター	攻撃が差し迫っている、または現在進行中である、または侵害がすでに発生している可能性があることを示唆する技術的なアーティファクトまたは観測可能なもの。
戦術、技術、手順（TTP）	アクターの行動を表す戦術、技術、手順についての記述。
セキュリティアラート	アドバイザリ、セキュリティ情報、脆弱性ノートとも呼ばれ、現在の脆弱性、エクスプロイト、およびその他のセキュリティ問題に関する簡潔で、通常は人間が読める技術的な通知。
脅威インテリジェンスレポート	一般に、アクター、TTP、標的となるシステムや情報の種類、および組織の状況認識を高めるその他脅威関連情報を記載したドキュメント。
ツール構成	脅威情報の自動収集、交換、処理、分析、および使用をサポートするツール (メカニズム) の設定と使用に関する推奨事項。

用語の定義:脅威インテリジェンスとは

脅威インテリジェンス

“意思決定プロセスに必要なコンテキストを提供するために、集約、変換、分析、解釈、または強化された脅威情報”

脅威インテリジェンスレポート

“一般に、アクター、TTP、標的となるシステムや情報の種類、および組織の状況認識を高めるその他脅威関連情報を記載したドキュメント”

OpenTextは大規模に脅威インテリジェンス情報を収集し、脅威インテリジェンスサービス**BrightCloud™ Threat Intelligence**を提供しています。

２．脅威インテリジェンス情報はどのように作られるか

弊社BrightCloudの例

膨大な脅威情報を分析

４０億以上

IPv4、IP6
アドレス履歴

１０億以上

カテゴリ分類された
ドメイン数

430億以上

検証されたURL数

３８０億以上

ファイルの振る舞い
履歴データ

9500万以上

センサー数

32 PB

管理下にある
データ容量

脅威情報分析のエコシステム

1 収集　2 分析・分類　3 公開

クローラーやハニーポットなどの専用の
アクティブセンサーとパッシブセンサー

WEBROOT by opentext
BrightCloud by opentext
opentext | EnCase

インターネットセンサネットワーク

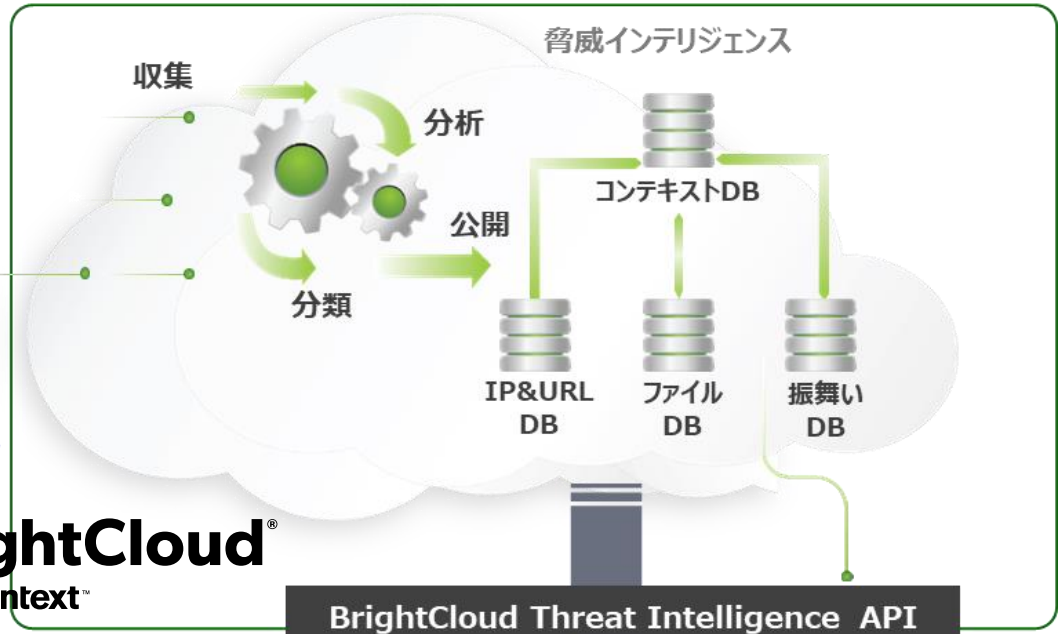
グローバル脅威データベース

Webroot法人ユーザ
（4000万以上）

BrightCloud OEMユーザ
(7800万以上)

opentext フォレンジックユーザ

BrightCloud by opentext



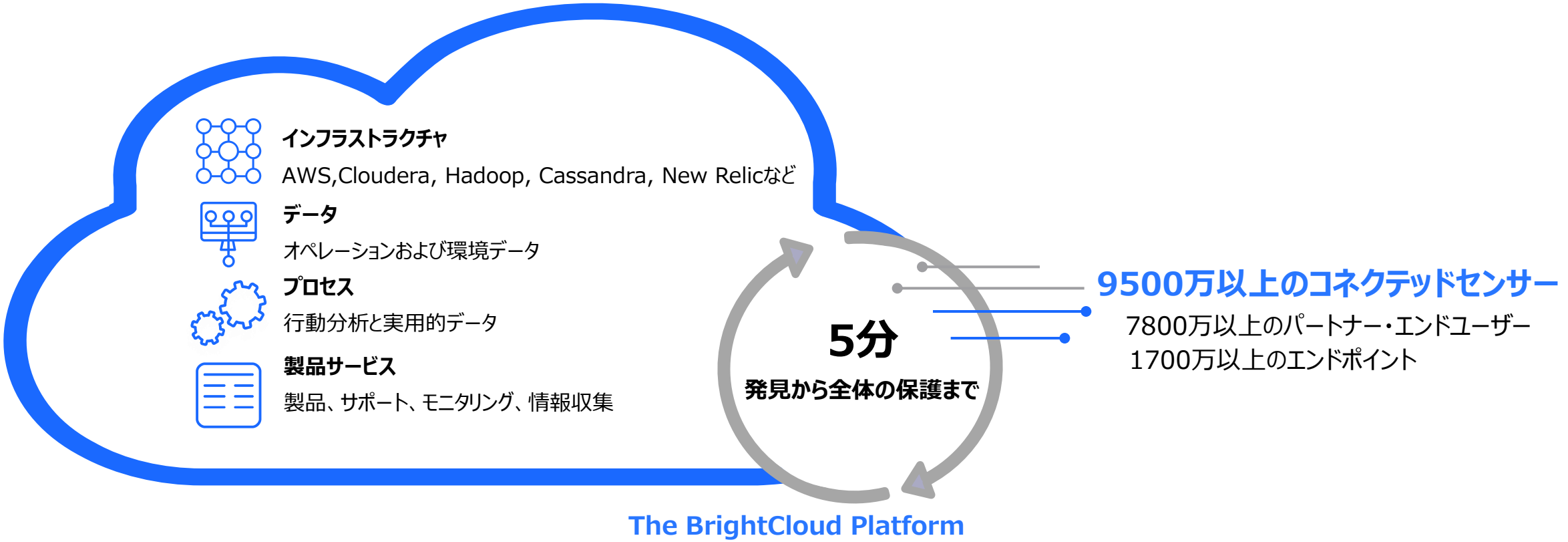
4 フィードバック

40万社以上 世界中の法人ユーザー	9500万以上 センサーネットワーク
16,000社以上 MSPパートナー	7800万以上 OEMユーザー

OEM products Customers

BrightCloud™ プラットフォーム

膨大な脅威情報を僅か5分で分析完了するプラットフォームを構築
AWS上にHadoopでプラットフォームを構築、常時稼働



アナリストによる分析、情報追加も並行して実施
さらにSNSのフィード情報、他社から買い入れた脅威情報も投入

OpenText Cybersecurity 2024年版脅威インテリジェンスレポート

本日ご紹介したBrightCloud™ Threat Intelligence Platformとその分析チームの知見はOpenText Cybersecurityの年次脅威インテリジェンスレポートにも生かされています。

2024年は世界中の企業や個人のお客様、テクノロジーベンダーが多層セキュリティアプローチを強化するための実用的な脅威インテリジェンスに関するインサイトをご紹介しています。

本会場で冊子版を配布している他、下記のサイトより無償ダウンロード可能です。ぜひご覧ください。

https://gateway.on24.com/wcc/eh/4366600/lp/4685713/japanese-opentext_2024-threat-report

2024年版脅威インテリジェンスレポートの一部をご紹介

- 多層防御戦略を導入したサイバーレジリエンスは、サイバー犯罪を取り巻く現状における最良の防御策

- Webroot SecureAnywhere、Webroot Security Awareness Training、Webroot DNS Protectionによる三層の保護をすべて導入したユーザーは、デバイスのマルウェア感染率が平均30.7%低下

- マルウェアの添付ファイルを含む電子メールの数は2023年に大幅に増加し、2022年のデータから35%上昇、地政学的な紛争と騒乱の他、生成AIにる悪意のあるコードと電子メールコンテンツの記述が容易になったという理由も考えられる。

- 最も狙われやすい業種は昨年に引き続き製造業

- ランサムウェアの支払い額の中央値が約20万ドルに急増(昨年は7万ドル)

３．BrightCloud脅威インテリジェンスの活用

BrightCloud脅威インテリジェンスサービス、Webrootエンドポイントプロテクション

BrightCloud®
by opentext™

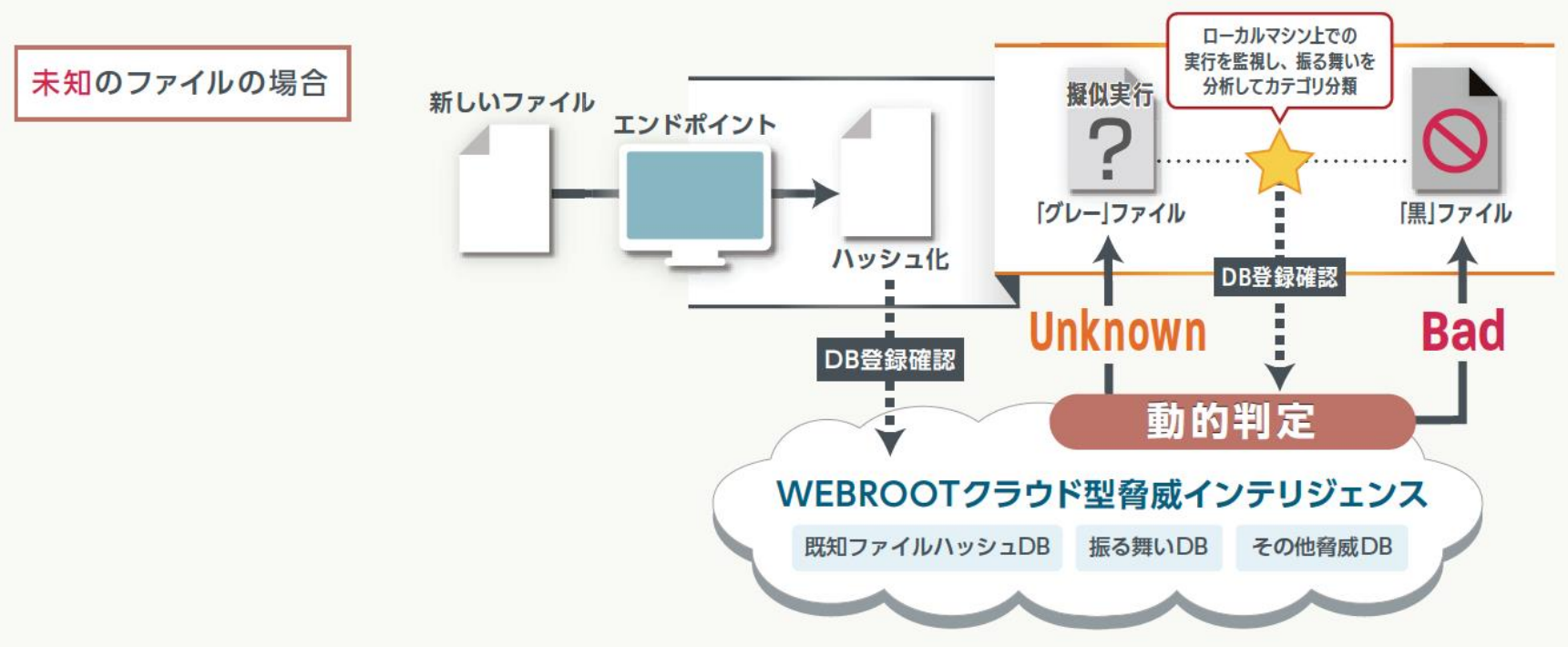
脅威インテリジェンスサービスBrightCloud™のサービスラインナップ

サービス名	内容
Web Classification & Reputation	数十億のWebページに対するコンテンツの分類と独立した評価スコアを提供し 顧客を不必要で安全でないサイトから守ります。
IP Reputation	リスクの高いIPアドレスを動的に公表しInbound/Outboundのトラフィックを保護します。
Real Time Anti-Phishing	サイト接続のタイミングでリアルタイムに分析し高度なフィッシング攻撃を検知します。
File Reputation	ダウンロードされたファイルの評価情報を動的に提供、既知の悪意あるファイル情報および ホワイトリスト情報を提供しマルウェアの侵入を阻止します。
Streaming Malware Detection	ダウンロードの過程でパケット上のPEヘッダーの情報を組み立て、ファイルの評価情報を 動的に提供、既知の悪意あるファイル情報およびホワイトリスト情報を提供。ダウンロード 自体を阻止します。
Threat Insight	Web/IP/ファイルのレピュテーションから悪意ありと判断した理由を提供します。

SOCでの利用、製品へのセキュリティ組み込みなどユースケースに応じて選択いただけます。

定義ファイル不要の次世代セキュリティ、Webroot Business Endpoint Protection

- 脅威判定にBrightCloud™を利用する他、コネクテッドセンサーとしても機能
- PC上のパターンファイルが不要なアンチウィルスソフト
- 未知のファイルのハッシュ値をBrightCloudプラットフォームに問い合わせ、ゼロデイ攻撃にも対応
- フットプリントが小さく、PCに負荷をかけないアンチウィルスソフト
- クラウド上の管理コンソールで集中管理、アンチウイルスサーバの構築・管理が不要



４．脅威インテリジェンスの活用

- SIEM/脅威分析/SOARソリューション OpenText ArcSight

Arcsight Intelligence/cyDNA x Galaxy脅威インテリジェンス

ArcSight SIEM/脅威分析/SOARソリューション OpenText ArcSightの製品から一部をご紹介

リアルタイムの脅威検出 (ArcSight ESM)

業界をリードする相関エンジンを利用して、脅威に関連するイベントを迅速に処理し、アナリストに警告します

振る舞い分析 (ArcSight Intelligence)

ルールフリーの異常検出により、変化する状況や新たな脅威に動的に適応し、とらえどころのない攻撃を未然に防ぎます。

脅威アクターのシグナル分析 (ArcSight cyDNA)

インターネットバックボーン上の脅威を検出、定義、コンテキスト化して、攻撃パターンと脅威アクターの属性の高度な認識を行います。

ArcSightシリーズ製品を導入いただければ、ライセンス料無償で

SOAR機能（ArcSight SOAR）も利用可能です。

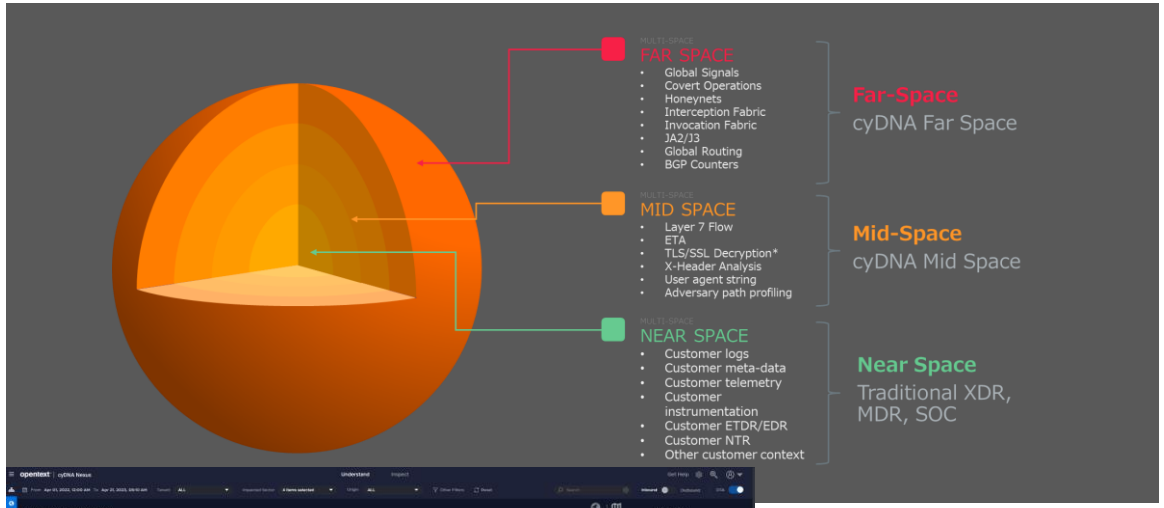
opentext™

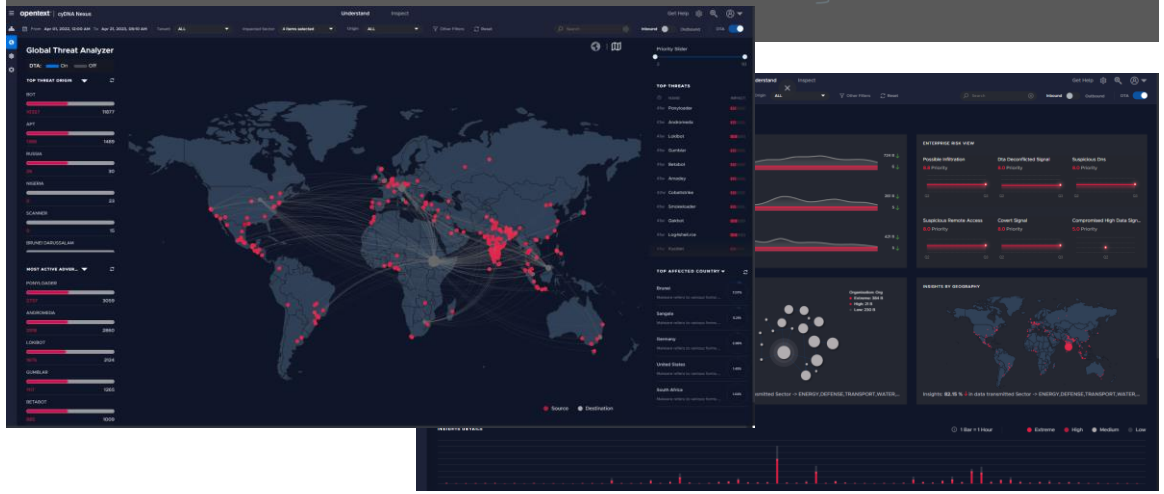
Arcsight Galaxy cyDNA

SaaSベースのグローバルシグナル分析、重要インフラ組織向けの脅威分析プラットフォーム

主な機能・特徴

- **SaaS ベースのグローバルシグナル分析**
  - インターネットバックボーンのBGPネットワーク上のAS局を伝播する脅威アクターの行動を分析
  - 悪意のあるインターネットトラフィックを検出
  - Galaxy脅威インテリジェンスを活用
  - 可能性のある敵対者パターンへのマッピング
  - 早期警告アルゴリズムによる将来の攻撃の監視・準備
- 迅速なエンドツーエンド （レイヤー 4）信号可視性
- セキュリティ監視能力の範囲と到達距離を拡張





包括的なサイバーセキュリティーソリューション

リスクを軽減し、信頼を維持し、事業中断を最小限にして、レジリエンスを高める

既知および未知の脅威を特定し、防御する

Fortify by opentext™

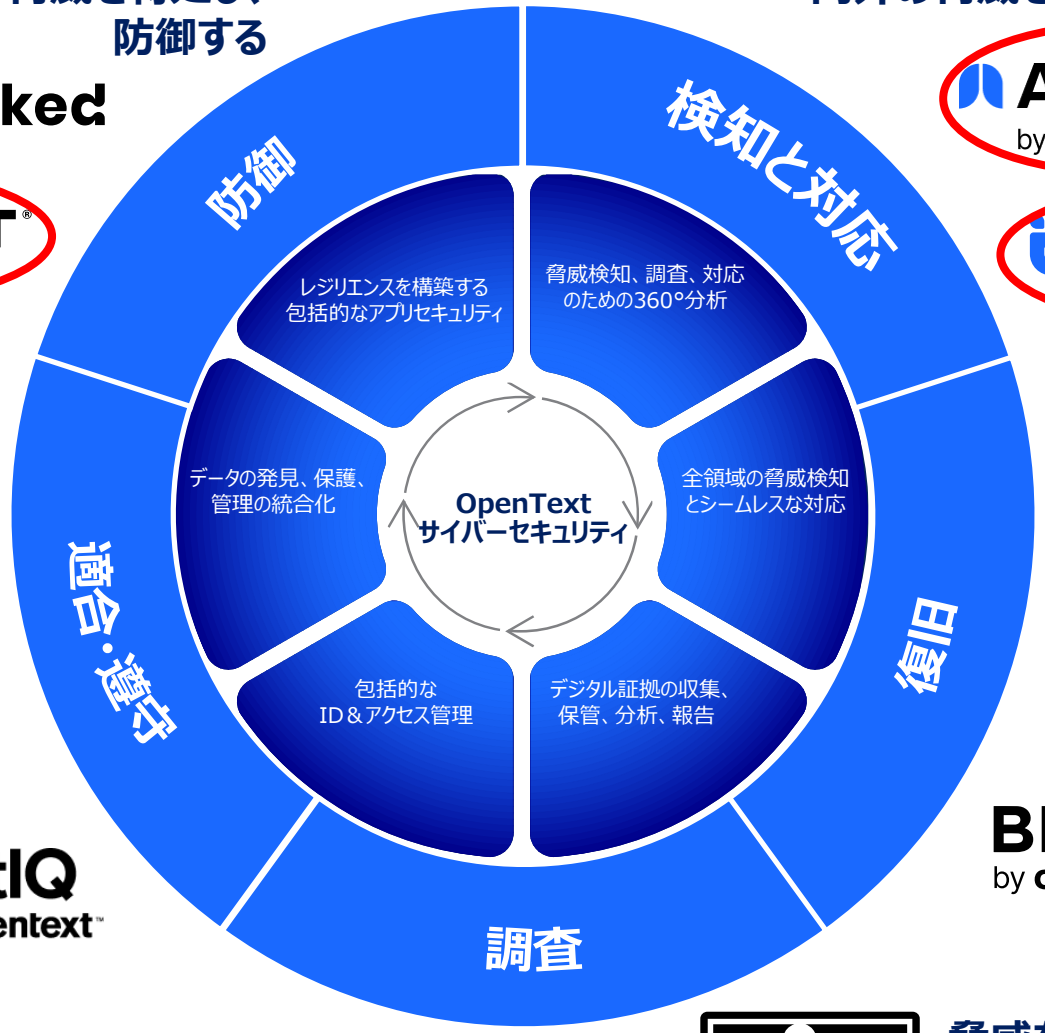
debricked by opentext™

WEBROOT® by opentext™

内外の脅威を迅速に検知し、対応する

ArcSight by opentext™

BrightCloud® by opentext™



情報セキュリティ、規制、業界標準を遵守する

Voltage by opentext™

NetIQ by opentext™

ダウンタイム、データ損失、リスクを最小化するための迅速な修復および復旧

CARBONITE® by opentext™

Availably

opentext™ | Data Protector

BRICATA® by opentext™

本日は赤丸で囲まれた製品についてご紹介させていただきました。

EnCase® by opentext™

脅威を調査・分析し、その範囲と影響を解明する

opentext™

opentext™

最後までご視聴頂き
ありがとうございました。

twitter.com/opentext

linkedin.com/company/opentext

opentext.com