完璧なGDPRプログラムの構築
Nuixの常時GDPR準拠へのアプローチ

Nuix Japan　日本代表　長谷 一生

nuix

アジェンダ

- Nuixのご紹介
- GDPRの概要
- Nuixの常時GDPR準拠のソリューションについて

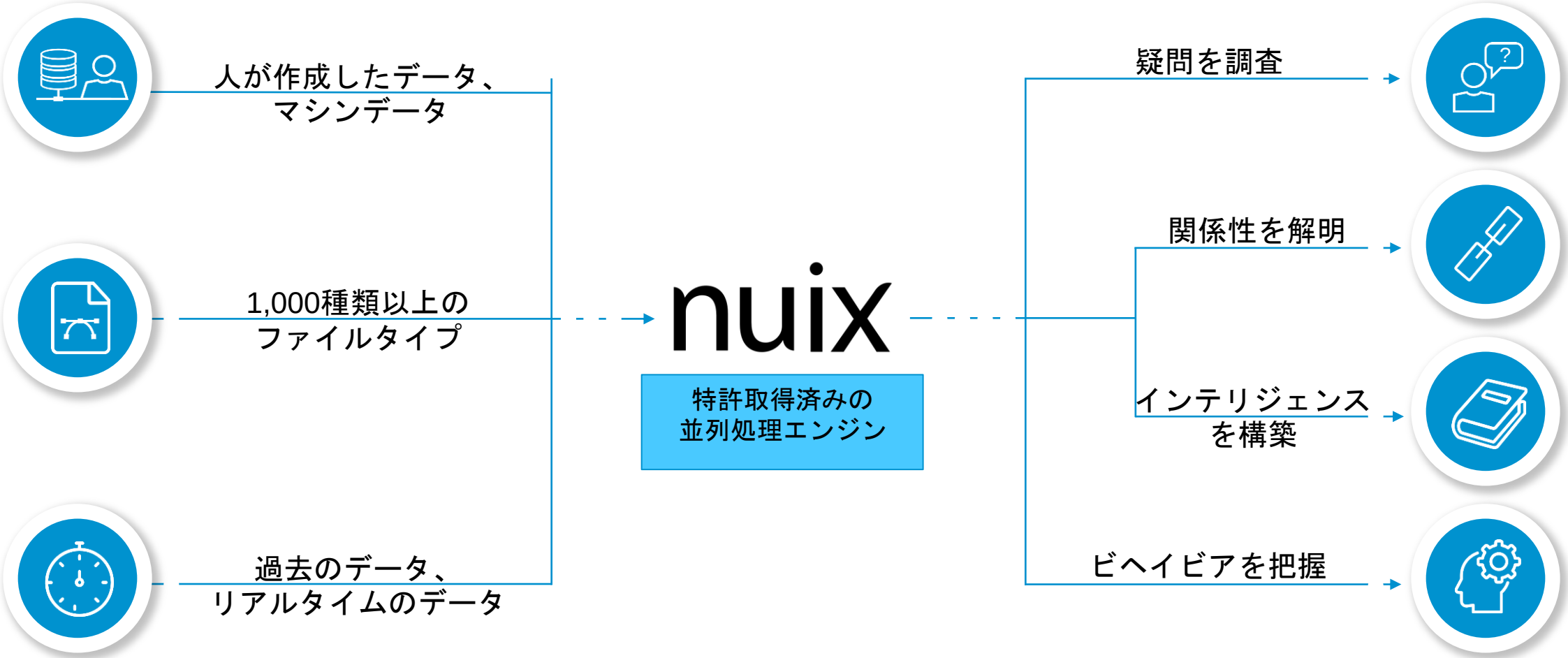
Nuixのご紹介

nuix

Nuixの概要

「 Nuixは、膨大な量のデータのDNAを理解するために開発されました。 Nuixのソフトウェアは、組織がセキュリティ、リスク、コンプライアンスへの脅威を予測、検知し、行動を取る必要のある重要な情報を特定します。」

Nuixは、お客様が膨大な量のデータを理解するお手伝いをします。



Nuixの製品領域

eDiscovery

調査

法執行機関

企業

セキュリティ

Ringtail

WR&A

A&I

ECC

Adaptive Security

Nuix Workstation/Engine

会社概要

財務の健全性

- 2000年にシドニーで設立
- 2006年に製品を商用化
- 2008年以降、黒字経営
- 過去5年以上に渡り、年平均40%の成長

優れた人材

- 世界中に約580名の従業員
- オーストラリア、ドイツ、インド、アイルランド、日本、ニュージーランド、シンガポール、イギリス、アメリカに事業拠点
- サイバーセキュリティ、情報ガバナンス、インテリジェンス、調査、法執行、電子証拠開示等の専門家

高い顧客満足度

- 世界中に2,000以上の顧客
- 2017年に250以上の新規顧客を獲得
- 70カ国以上に顧客とパートナー
- 主要な規制当局、法執行機関、諜報機関、監査法人、訴訟支援事業者、企業など

研究開発への継続的な投資

- 既存顧客や市場に対して新しい価値を提供
- 新たな課題の解決
- 2018年にRingtailを買収

世界中に2,000以上の顧客

監査法人

Deloitte. BDO BECHTLE Grant Thornton Kroll epiq KPMG FTI CONSULTING pwc EY

企業

AIRBUS SONY PICTURES Unilever SUPERVALU DUKE ENERGY UnitedHealth Group eir WPP vodafone HUAWEI

金融サービス

HSBC Freddie Mac AMERICAN EXPRESS AIG experian citi Westpac BARCLAYS

官公庁

IRS Inland Revenue Te Tari Taake 국세청 National Tax Service Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra HM Revenue & Customs EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES Llywodraeth Cymru Welsh Government DEPARTMENT OF COMMERCE UNITED STATES OF AMERICA Australian Government Department of Foreign Affairs and Trade European Commission

法執行機関

Police vaud canton de vaud Bundeskriminalamt AFP AUSTRALIAN FEDERAL POLICE Home Office U.S. DEPARTMENT OF HOMELAND SECURITY

法律事務所

ENSAFRICA DiscoverReady CONTACT Altep THOMSON REUTERS H5 FRONTEO LAW IN ORDER NELSON MULLINS

規制当局

SFC 證監會 Fair Trade Commission ASIC IBRC skkmigas Investment and Development Office Government of Ras Al Khaimah רשות ניירות ערך ISRAEL SECURITIES AUTHORITY

パートナー

Lighthouse eDiscovery MICROTECH INFINIGATE ... Adding Value to Distribution INGRAM MICRO ARINA SoftNet INDONESIA DLT shi SVA OPTIV

GDPRの概要

nuix

近年のEUでの調査

June 15, 2017

Report predicts banks under GDPR

Report urges banks to focus on breach levels of fines are exceedingly highs.

A new report is "conservatively" forecastin organisations are about to shell out €4.7 b GDPR comes into power thanks to data br currently have to declare.

Consult Hyperion, which commissioned Al

BUSINESS

Google Faces Record EU Antitrust Fine

Penalty could reach as high as 10% of annual revenue, which was more than $90 billion in 2016

JUNE 16, 2017

report is "conservatively" forecasting that ean finance organisations are about to

E.U. Fines Facebook $122 Million Over Disclosures in WhatsApp Deal

MAY 18, 2017

TalkTalk hit with record fine over cyber attack

OCTOBER 15, 2016

GDPRをめぐるさまざまな動き

EUデータ新規制 100社調査

国内企業 8割が対応未了

対象情報精査に時間

GDPRは厳しい対策を企業に求める

商品やサービス

EUの居住者

個人情報

企業

取得 情報の収集そのものに同意を得る

活用 情報を域外に持ち出すことにも同意が必要

削除 個人の求めに応じ、データを削除できる仕組み

管理 データ保護責任者の設置

EU GDPRの次はクッキー法

当事者以外が通信データを処理するのは原則禁止

通信会社など 同意なく処理してはならない

通信データ

文章・音声・画像など

通信当事者

通信当事者

eプライバシー規則案のポイント

原則	通信の当事者以外が、メッセージの文面や通信情報などの通信データを処理することを原則禁止する
規制の対象	メッセージ事業者にも
クッキー規制	サイトの閲覧するクッキードルを高く
制裁金	最大で2000での年間総いずれか高と同じ)
日本企業への影響	EUの拠点ら、EU向提供してい

通信の秘密保護 強

個人情報移転、日本承認へ

EUデータ規制で欧州委

ホテル予約システムで情報漏洩、プリンスなど多数被害

科学&新技術　BP速報

2018/6/28 18:00

保存　共有　印刷　その他

日経XTECH 日経クロステック

ホテル予約システムを提供する仏ファストブッキングは2018年6月26日、フランスにある同社の管理サーバーが不正アクセスを受け、顧客であるホテルの予約情報や予約システムで決済に使われたクレジットカード情報が漏洩したと発表した。日本国内では400施設以上のホテルが該当し、合計で32万5717件の情報が漏洩した。

同社は、顧客である国内ホテルの英語や中国語などで宿泊予約できる外国人向け予約サイトを運営していた。各ホテルが独自で運営する予約サイトは影響を受けていない。

不正アクセスを受けたのは、18年6月15日と6月17日の2回。6月15日の攻撃では、国内380施設のホテルの予約情報20万5137件が漏洩した。予約情報は、利用者の名前、住所、メールアドレス、予約ホテル名、チェックイン/チェックアウト日が含まれる。一方、6月17日の攻撃では、国内189施設のホテルの予約時に決済に使われたクレジットカード情報（カード番号や有効期限、名前など）が12万580件漏洩した。両方の攻撃を受けたホテルは168施設。

同社は影響を受けるホテル施設名を明らかにしていない。ただ6月26日には、プリンスホテル（グループ内43施設）のほかに、セルリアンタワー東急ホテルやホテルニューオータニ大阪、ホテルモントレ（グループ内20施設）、リッチモンドホテル（3施設、運営はアールエヌティーホテルズ）が情報漏洩を発表している。

EU GDPR: 先ずは理解から

nuix

Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now

1 **Awareness**
You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.

2 **Information you hold**
You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit.

3 **Communicating privacy information**
You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

4 **Individuals' rights**
You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

5 **Subject access requests**
You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

6 **Lawful basis for processing personal data**
You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.

7 **Consent**
You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard.

8 **Children**
You should start thinking now about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity.

9 **Data breaches**
You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

10 **Data Protection by Design and Data Protection Impact Assessments**
You should familiarise yourself now with the ICO's code of practice on Privacy Impact Assessments as well as the latest guidance from the Article 29 Working Party, and work out how and when to implement them in your organisation.

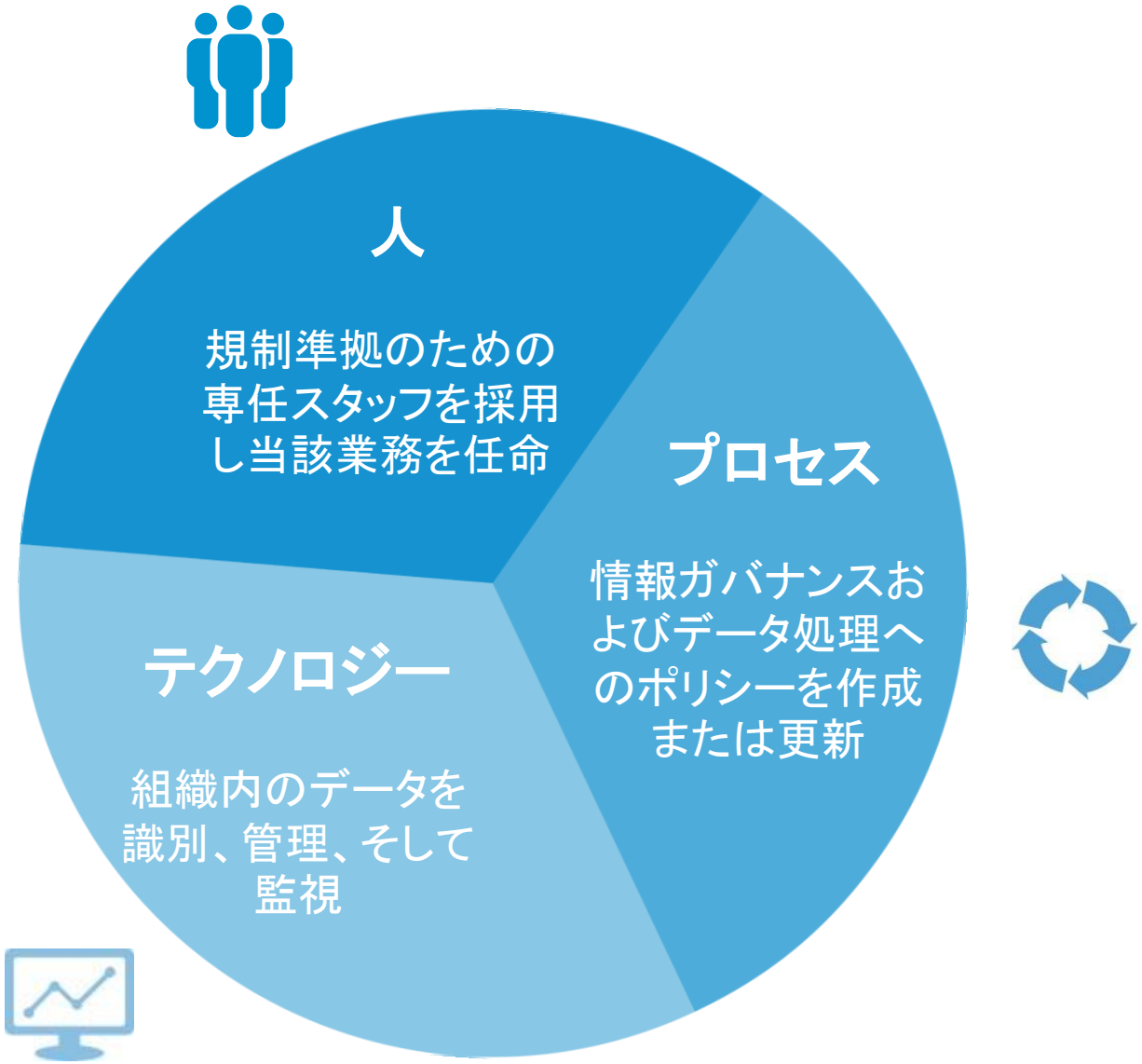
11 **Data Protection Officers**
You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements. You should consider whether you are required to formally designate a Data Protection Officer.

12 **International**
If your organisation operates in more than one EU member state (ie you carry out cross-border processing), you should determine your lead data protection supervisory authority. Article 29 Working Party guidelines will help you do this.

ico.
Information Commissioner's Office

ico.org.uk

EU GDPR: 重要となる3つの要素



企業が、GDPRに準拠するために回答できなければならない重要な質問事項:

1. どのような個人情報を保有しているのか？
2. どこにそのデータは保管されているのか？
3. 誰がそのデータに責任を持っているのか？
4. お客様の情報を保護していますか？

GDPR データ識別子

EUのデータ保護条令(Data Protection Directive: 95/46/EC)は、個人情報を以下のように定義:

「個人情報」とは、自然人(データ主体)を特定できるあるいは特定しうるために関係するすべての情報を意味します。特定しうる個人とは、直接的あるいは間接的に特定される人であり、特にその人の物理的、生理的、精神的、経済的、文化的そして社会的地位の一つまたは複数により特定されます。

Personal Identifiable Information (PII: 個人を特定しうる情報) とは、直接的あるいは間接的を問わず自然人を特定しうるいかなる情報。

Sensitive Personal Information (SPI: 注意を要する個人情報) とは、その個人に関係した、民族的出身、政治的信条、宗教、哲学の信条、心身の健康状態、性的指向、犯罪歴(容疑または確定)、指紋、顔認証、網膜認証などの遺伝的データを含む。

PII
名前
住所
メールアドレス
モバイルデバイス ID
GPS 位置情報
銀行口座情報
社員ID
IPアドレス

SPI
民族的出身
政治的信条
宗教、哲学の信条
心身の健康状態
性的指向
犯罪歴 (容疑または確定)
遺伝的データ 例: 指紋、顔認証、網膜認証、その他

プライバシー規制要件

データプライバシー は、情報マネジメントの成長領域であり、企業の責任であり、GDPRのような規制で拍車がかかっています。

- 通知を受ける権利
- アクセスする権利
- 修正する権利
- 消去する権利
- 情報の処理を制限する権利
- データを移動する権利
- 異議を唱える権利
- 自動的に意思決定やプロファイリングをされない権利

規制要件とデータ主体からの請求は、個人を保護する目的で設計されています。

GDPRと分類

企業は以下の質問に答えながら、自社のデータに対して大規模な分類を実行しなければなりません。

- どのような個人を特定しうる情報をファイルで持っているのか？
- どこにそれは保存されているか？
- どのようなセキュリティレベルが必要か？
- 誰がアクセス可能か？
- どのようにそのデータは利用されるのか？
- そのデータを利用するための承諾を得ているか？

Nuixは、GDPRを熟知しています

Nuixは、貴社のGDPR対応を支援します。

- 大規模のデータセットに対するプロセッシングと情報開示の実績
- お客様に透明性とインテリジェンスをもって自社のデータに対する識別、管理、監視を実現
- 企業が自社を守り、将来を実現する方法を一変させます。
- 前進するアプローチでのプロセスやポリシーを構築するための基礎を養成

Nuixの常時GDPR準拠ソリューション

nuix

GDPRの課題とNuix活用によるお客様の対応

GDPR

見つけ出す

- どのようなGDPRコンテンツを探すのか？
- どこにそのコンテンツはあるのか？
- 誰がそれにアクセスできるのか？
- 権限、彼らはアクセスできるのか？

理解

- ようやく、業務データの大きさや規模を把握しました。
- アクセス請求、情報の自由、忘れられる権利にどのように対応したら良いのか？

行動

- いかに素早く情報漏洩通知を行えば良いのか？
- いかに業務プロセスとしてアクセス請求に対応するのか？
- いかに情報漏洩を特定し、72時間以内に対応できるか？
- どのように規制に合致した適切な情報ガバナンスを保証できるか？

nuix

識別：データマッピングと検出

- GDPRに関連したコンテンツをファイルから特定（メタデータだけでなく）
- 1000種医女のファイルタイプをサポート; ペタバイトのデータを処理; 構造化データ/非構造化データ/アーカイブストレージを処理

管理：把握と分類

- どこに存在してもすべてのGDPRデータへの完全な可視性を提供
- 完璧なデータ分析で、GDPRデータに対して誰が、何を、いつ、そしてそれらの関係性を解明
- データのライフサイクルを管理し、企業インフラストラクチャー内の適所での存在を保証
- 冗長、古い、また些細なデータを分類して季節の管理
- 構造化/非構造化データとエンドポイントデータを関連づけ、直ちに識別し対応

監視：リアルタイムでイベントに対応

- GDPRに識別されたドキュメントを監視し保守するためのインフラストラクチャーを構築
- 高度な技術を活用し、人が生成した情報にアクセス、把握し、行動
- 発生後72時間以内にデータ漏洩を報告
- 大惨事のシナリオを演習でき、リスクを把握
- データを暗号化し監視し、アラート、ソースの破棄（忘れられる権利）、権限の更新

GDPR：Nuixによる7つのプロセス

ステージ 1: 個人情報のパターンを識別

ステージ 2: データマッピングの開発

ステージ 3: 情報の監査を実施

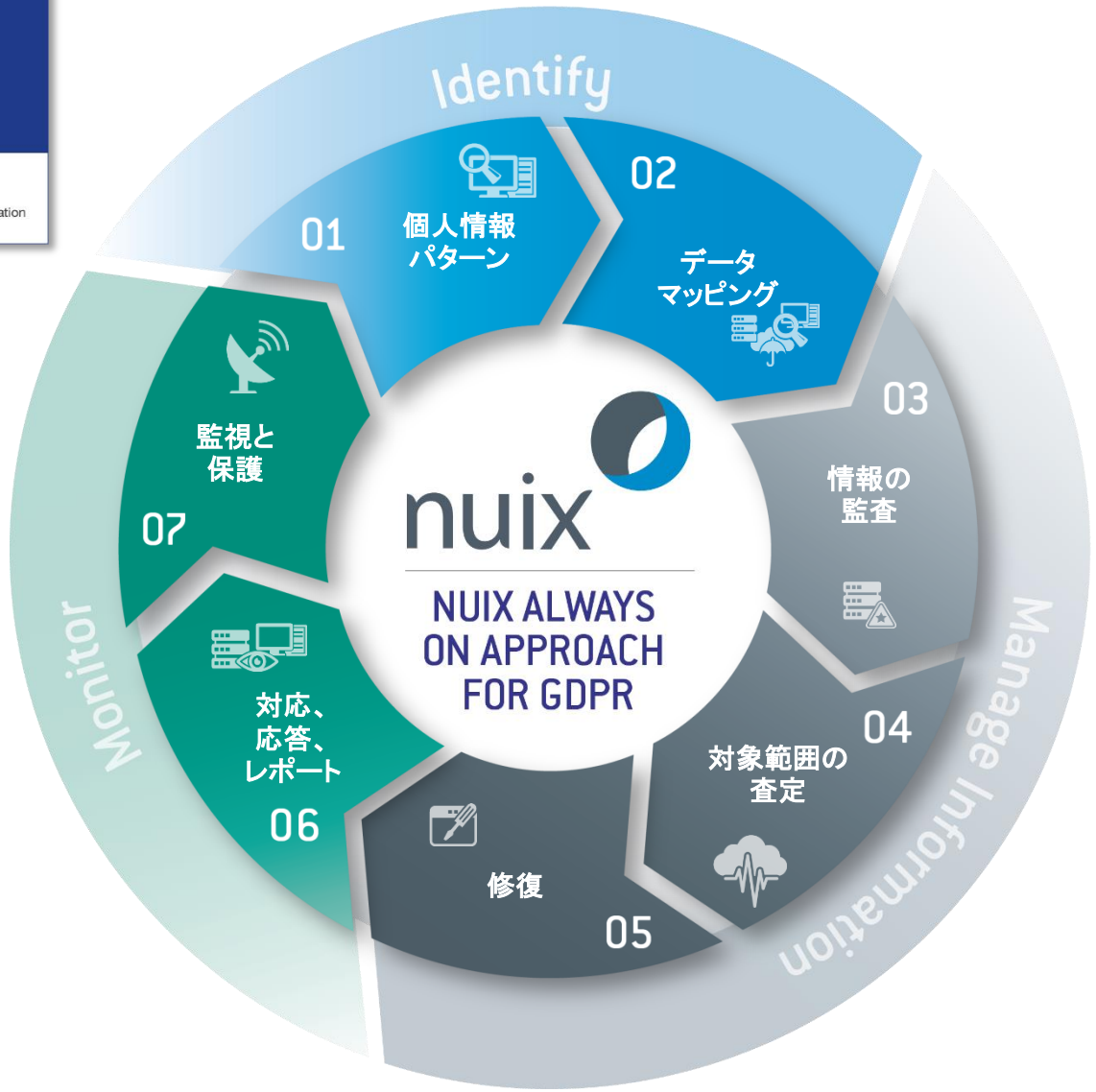
ステージ 4: 対象範囲の査定

ステージ 5: 修復の適用

ステージ 6: 対応、応答、レポート

ステージ 7: 常時保護の導入

GDPR：Nuixによる７つのプロセス - ステージ1



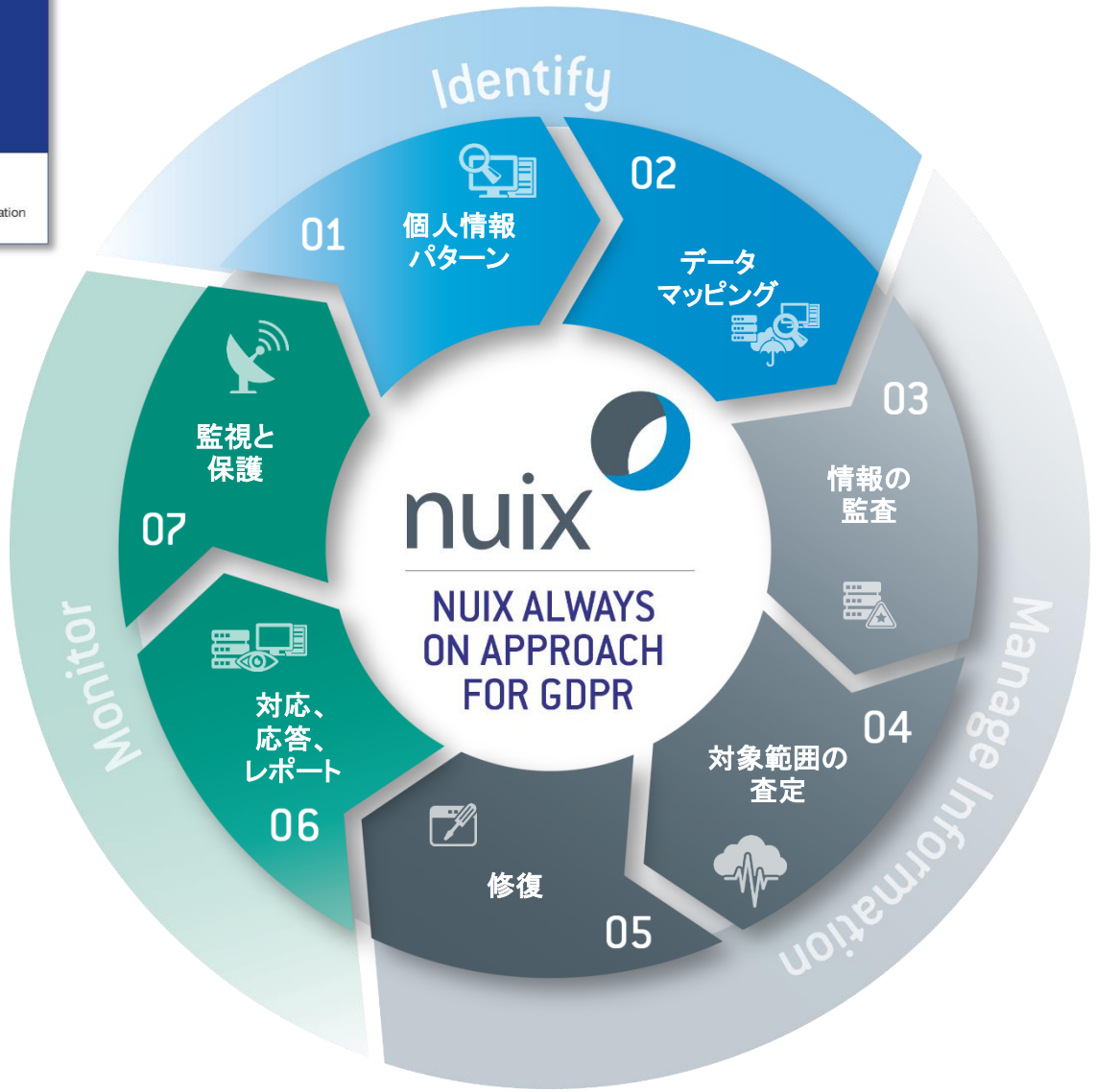
ステージ 1: 個人情報のパターンを識別

- ❑ データポリシー/GDPRポリシーをレビューし、それらが正しくかつ適切にアップデートされていることを確認
- ❑ プロセッシングの検索ルールを開発

データにNuixのパラレルプロセッシングを実行し、

- ❑ サンプルデータセットのデータパターンを確認し、GDPR識別要件に適応した文字列を策定
- ❑ PIIや他のGDPR関連文字列を判別するパターン識別の実体を構築し、検証

GDPR：Nuixによる７つのプロセス – ステージ２



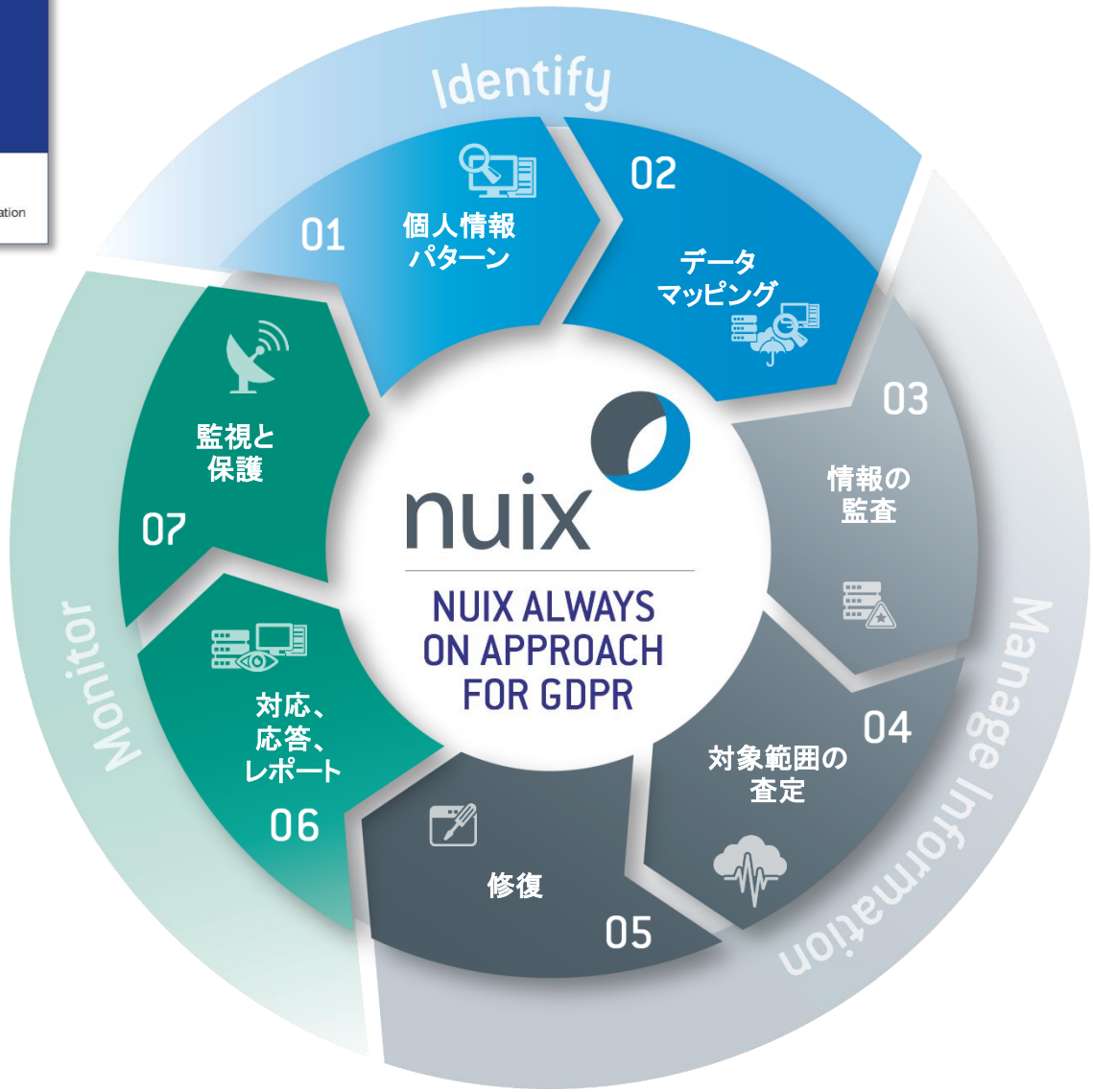
ステージ 2: データマッピングを開発

すべてのデータ領域に対して潜在的に個人情報を含んでいる可能性のあるデータリポジトリを特定し分類

- ❑ サードパーティデータ
- ❑ クラウドストレージ
- ❑ NAS / SAN ストレージ
- ❑ エンドポイントデータ
- ❑ モバイル
- ❑ マルチメディア

リスク・スコアリング・ロジックを適用し、よりインテリジェントな意思決定と修復の優先順を把握

GDPR：Nuixによる７つのプロセス – ステージ３



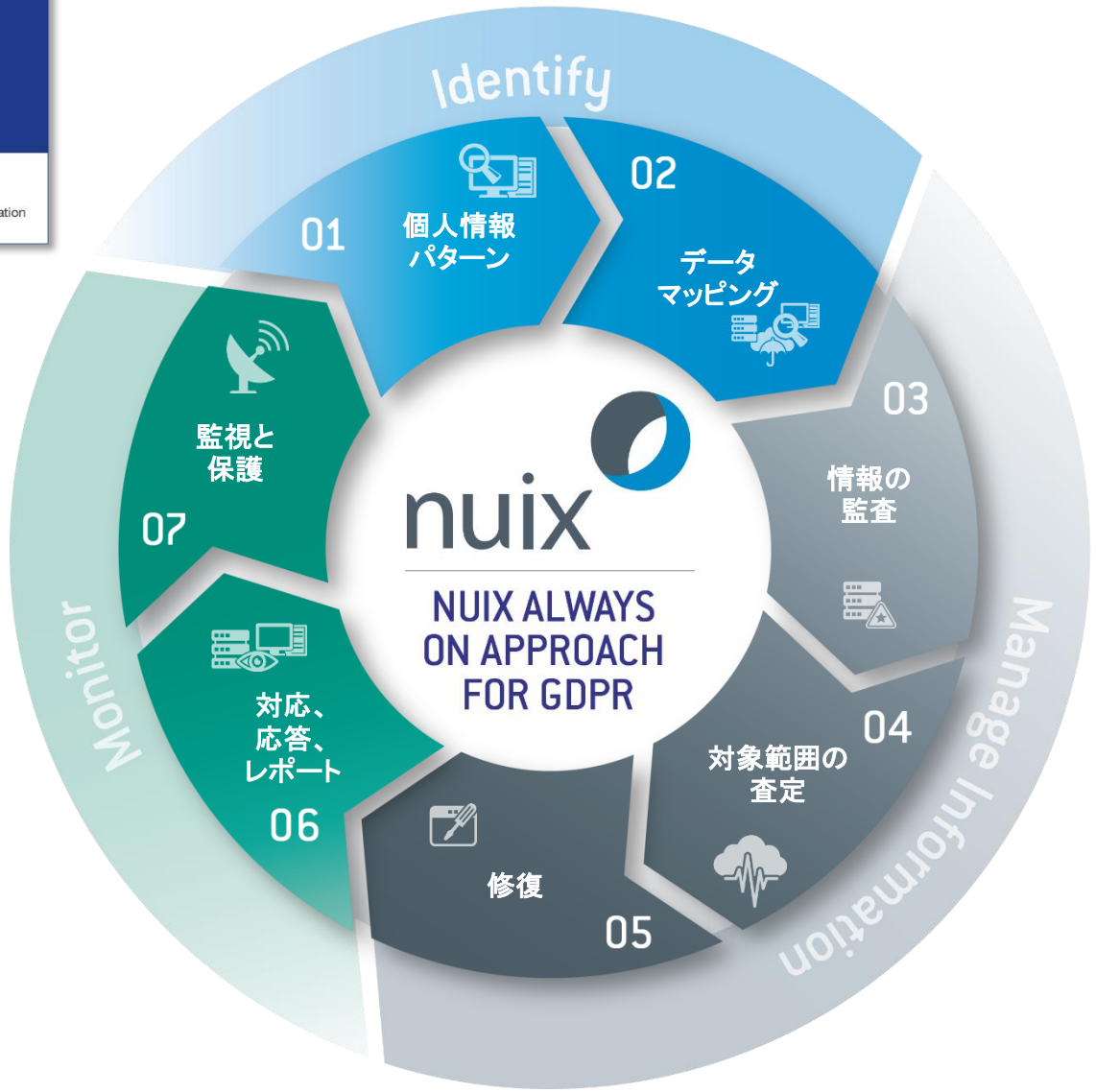
ステージ 3: 情報監査を実施

Nuixを導入し環境設定を行い、データリポジトリとエンドポイントの調査が行えるよう、レビューや修復機能を活用

収集したデータへの詳細な段階的プロセッシングの基準：

- ❑ リスク
- ❑ 緊急性
- ❑ 稼働率
- ❑ サイズ

GDPR：Nuixによる７つのプロセス – ステージ４

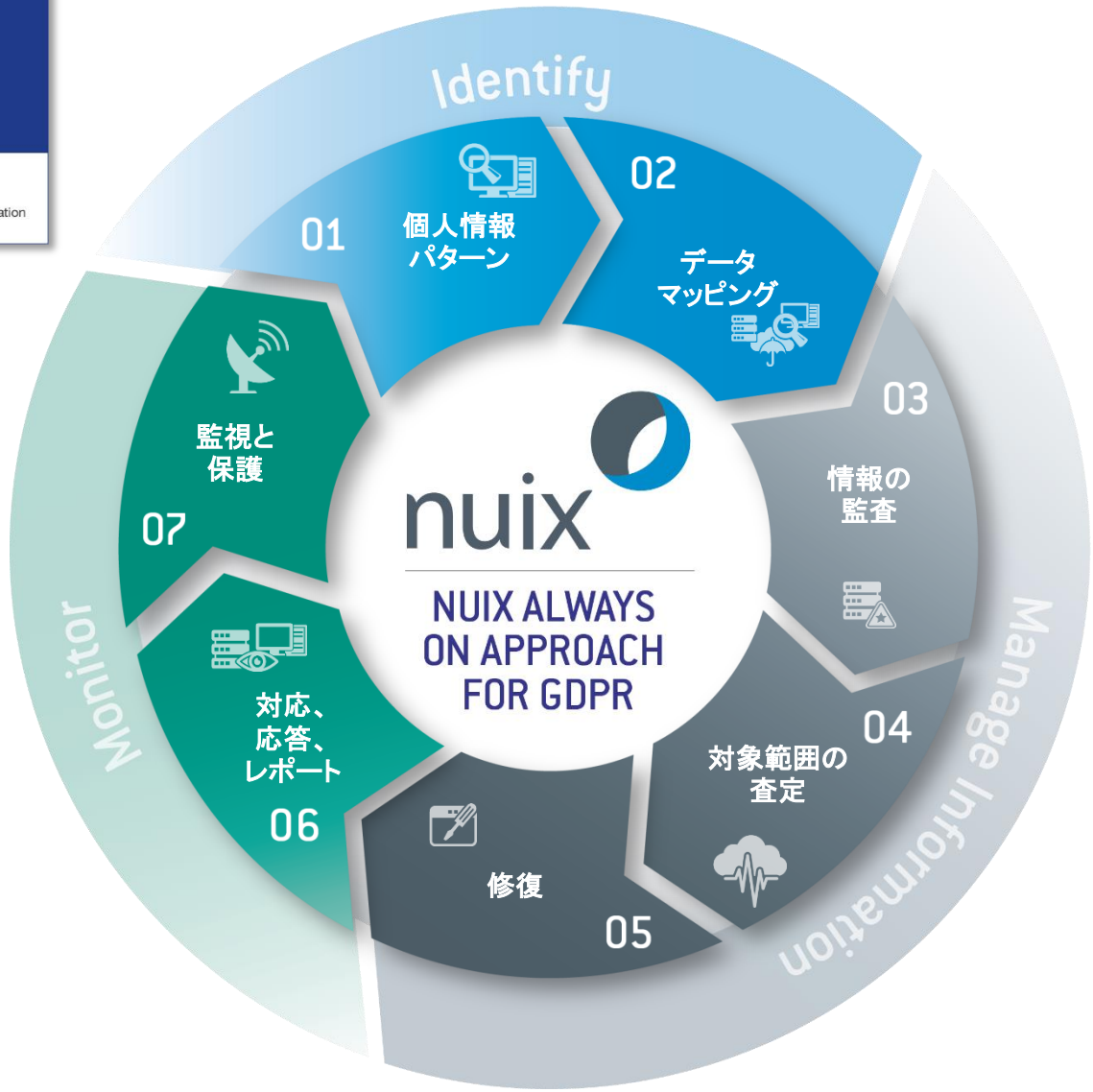


ステージ 4: 対象範囲の査定

Nuixで作成されたデータエビデンスや情報の透明性を活用：

- ❑ データ管理者とともにインデックス化されたデータをレビューし自動分類のルールを作成
- ❑ アクションプランを決定
  - ❑コンプライアンス違反への調査や原因を修復するプロセスを文書化
  - ❑忘れられる権利や情報の自由の権利等に対応するためのプロセスを整理
- ❑ 最適なストレージ環境を定義
- ❑ 詳細なマイルストーン
- ❑ 修復の手順に同意

GDPR：Nuixによる７つのプロセス – ステージ５

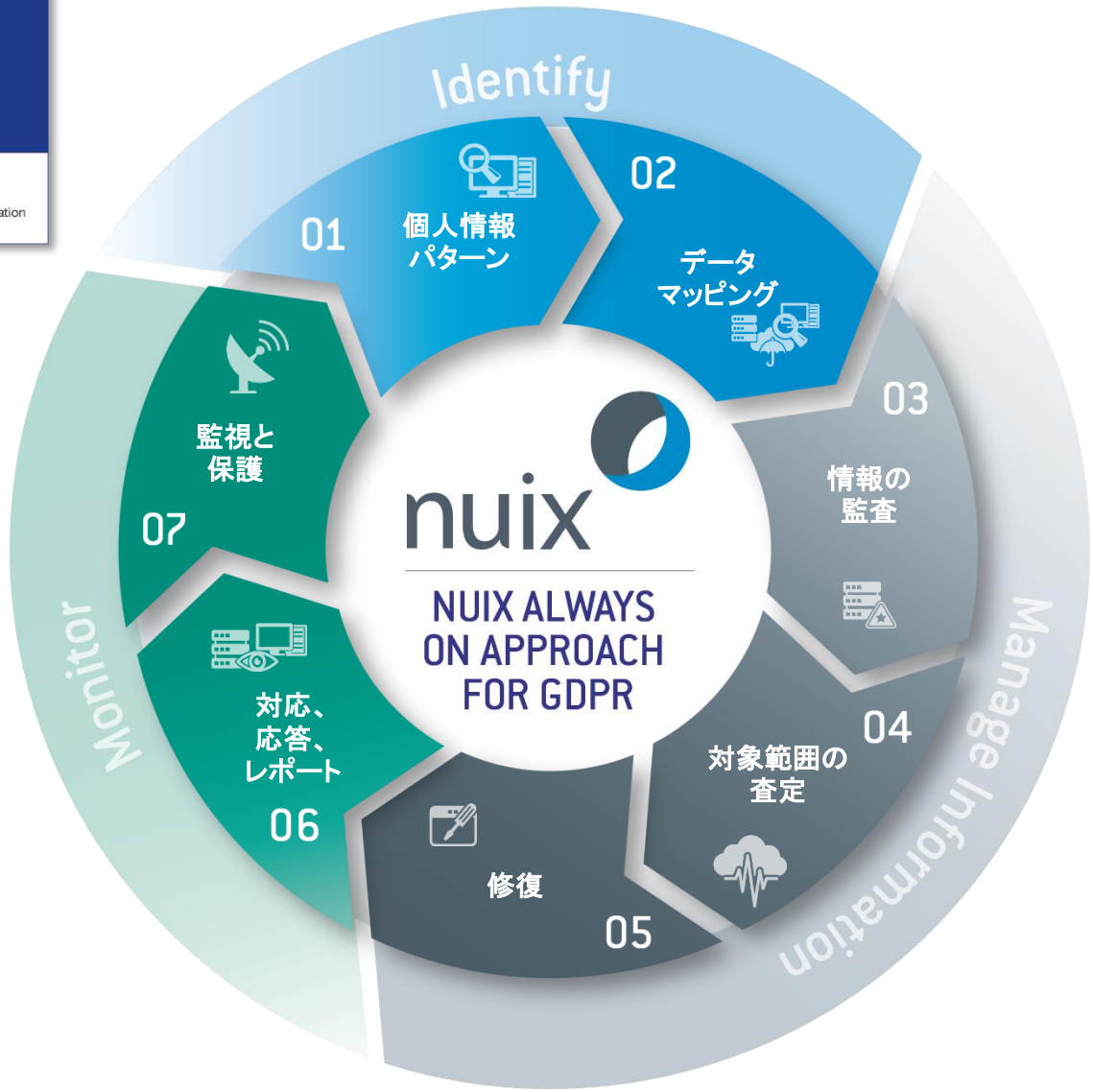


ステージ 5: 修復の適用

組織のポリシーと実践を更新したら、Nuixを活用し修復を実行し、適用前に最終的にクリーンアップを行う。

- ❑ 以下の内容を含むデータ修復：
  - ❑ 期限切れのコンテンツの削除
  - ❑ 管理責任者の任命
  - ❑ 機密情報の移動
  - ❑ データの保護と暗号化
  - ❑ アクセス権限
- ❑ ポリシーとプロセスの更新を通知
- ❑ 権限の再設定の承諾
- ❑ 差分のインデックスを通し、新しい情報を定期的に監査

GDPR：Nuixによる７つのプロセス – ステージ６

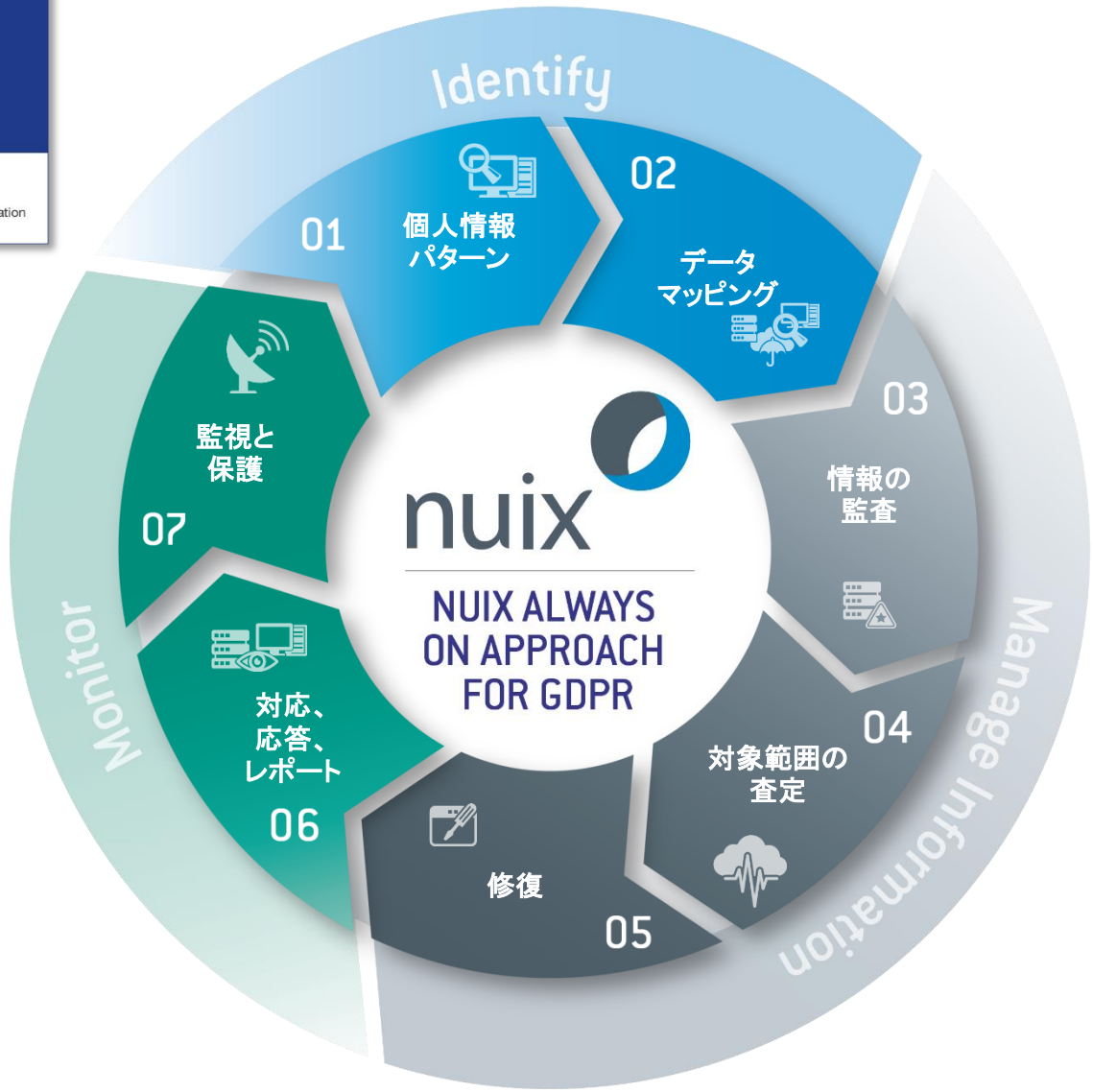


ステージ 6: 対応、応答、レポート

継続的に環境を評価し、規制当局や主体からのリクエストに対応：

- ❑ アクセス請求や忘れられる権利に対応
- ❑ 規制当局の要求に応答
- ❑ GDPR当局へ情報漏洩をレポート
- ❑ 情報漏洩と対象データについて、自社のデータ保護責任者や取締役会にレポート

GDPR：Nuixによる７つのプロセス – ステージ７

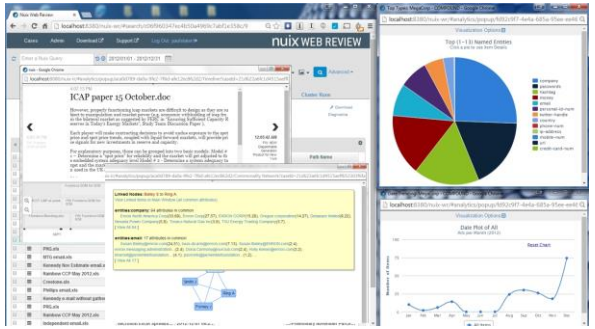


ステージ 7: 常時保護の導入

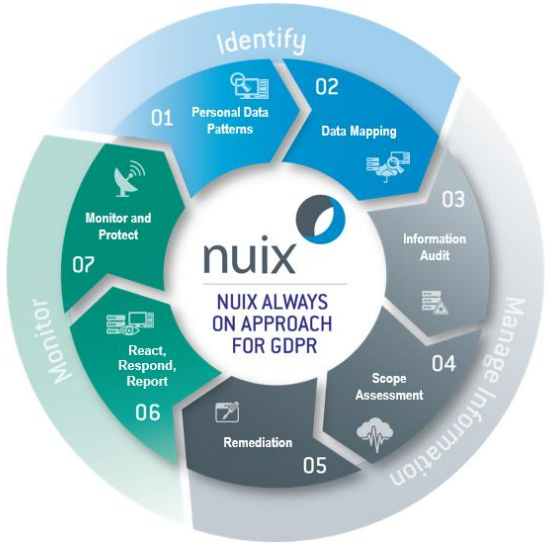
Nuixを導入し、常時監視を確立するプロセスを開発し適用：

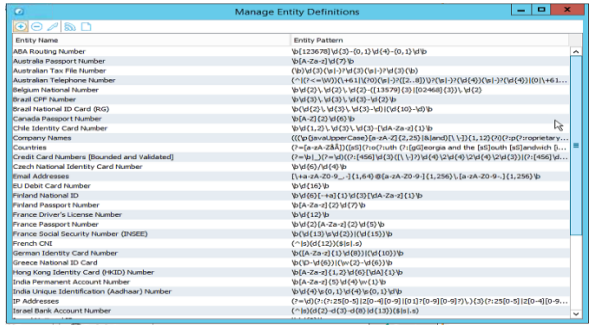
- ❑ 情報漏洩の報告
- ❑ エスカレーションの決定
- ❑ 潜在的な攻撃経路の発見
- ❑ データの持ち出しを把握
- ❑ 行動に着手

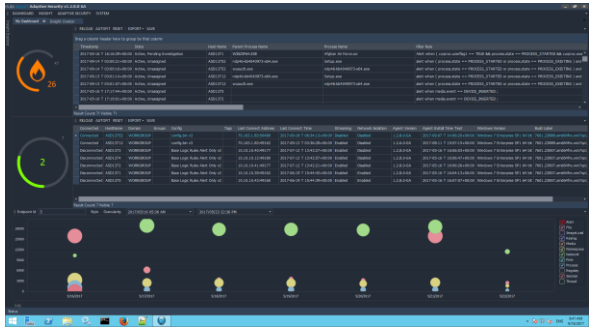
GDPR：Nuixによる７つのプロセス – レビュー

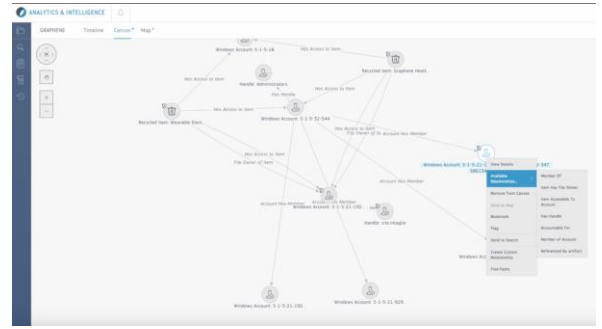


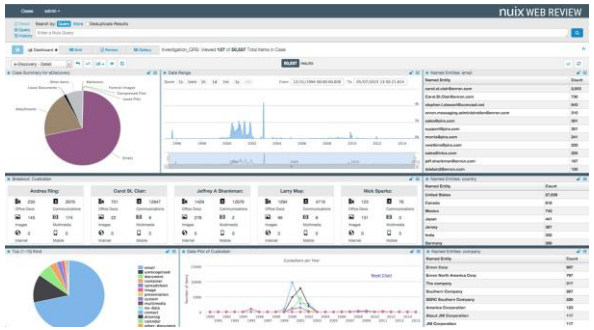
Nuixのテクノロジーにより、データプライバシー 、
フォレンジック、GDPRコンプライアンスを、より
シンプルに管理できます。

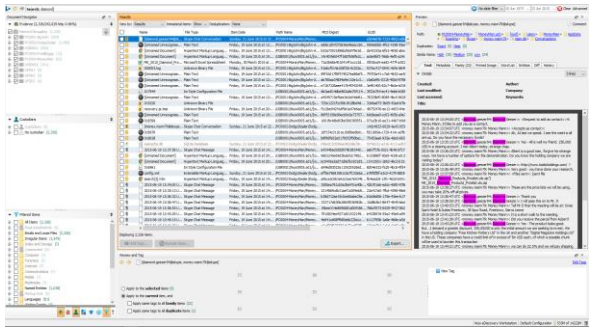












GDPR：まとめ

- GDPRは、貴社の情報ガバナンスをより上手く管理する機会となります。
  - 国内での個人情報や機密情報の保護、内部不正調査にも適用できます。
- 貴社がGDPR準拠となるための要件を理解する必要があります。
- GDPR対策を成功に導くための主要なステップに対する具体的なアクションプランが必要となります。
- **Nuixのソフトウェアが貴社のGDPR対応をサポートします。**

更に詳細は:

- nuix.com/jp/gdpr
- nuix.com/blog
- twitter.com/nuix
- facebook.com/nuixsoftware
- linkedin.com/company/nuix
- youtube.com/nuixsoftware


nuix
Simple. Powerful. Precise.