Mehr Licht!
More Photonics for Intelligence

#C20

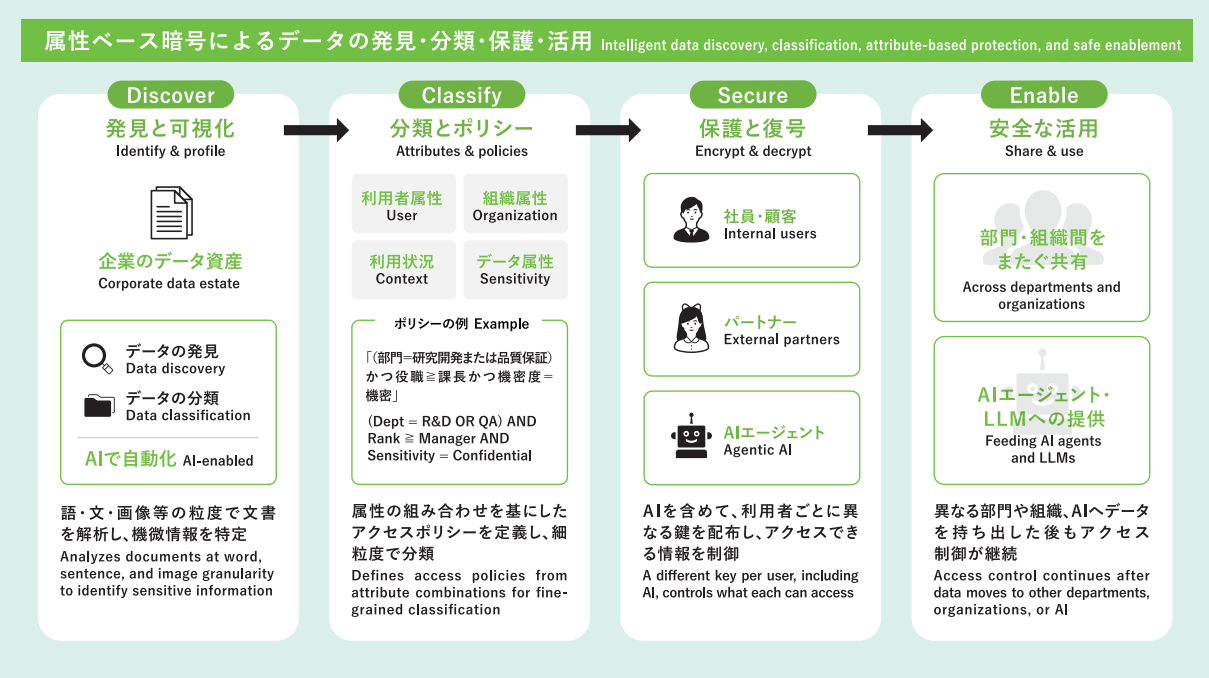
#サイバーセキュリティ#DX・AX（デジタル変革）#AI倫理・責任あるAI

AI時代のゼロトラストデータセキュリティ

暗号文に埋め込んだ条件を満たす属性の鍵だけに復号を許しデータ単位のアクセス制御を実現します

技術課題・ゴール

サイバー攻撃高度化とAI利活用拡大で守るべきデータは増え続けます。境界防御中心のゼロトラストは侵入後のデータを守れず、データ層制御も鍵保有者にファイル全体を見せるか否かの二択です。属性ベース暗号はアクセス条件を暗号文に埋め込み、条件を満たす属性の鍵で復号を許します。形式や保存・転送問わず保護し、漏洩時の影響を最小化します。AIエージェントも人と同ポリシー下に置き安全な利活用と導入拡大を後押しします。



技術ポイント

要素技術

・アクセスポリシーを暗号文に埋め込み、条件を満たす属性の鍵保有者のみ復号可能とする方式。AND/OR条件による複合ポリシーの定義・即時変更可能

・複数の独立した認証局が属性と鍵を分散管理するマルチオーソリティ方式。単一の管理主体に依存せず、組織をまたいだ権限管理を実現

市中技術差異点

・開示先がN人でも暗号文は1個で足り、従来の公開鍵暗号でN個必要だった暗号文をN分の1に削減。鍵の所持ではなく属性で復号範囲を判定

・属性ベース暗号を用いたゼロトラスト・データセキュリティ製品として業界初。AIエージェント・RAGのデータアクセス制御とPQC対応設計

適用ビジネス/ユースケース

金融

銀行や保険会社が顧客情報を含む審査書類を支店・本部・監査法人と共有する際、AIが文書を自動分類してポリシーを付与。与信分析を行うAIエージェントは許可された属性の範囲しか復号できず、対象外データの学習や外部流出を防ぎます。

出展組織

NTT Research, Inc.

関連情報URL

https://ntt-research.com/scale-academy/
https://ntt-research.com/ntt-research-launches-scale-academy-and-new-quantum-safe-security-platform/