【富士通】

ダイナミックマップの流通に向けたデータセキュリティマネジメントの実現

SIP 課題間連携

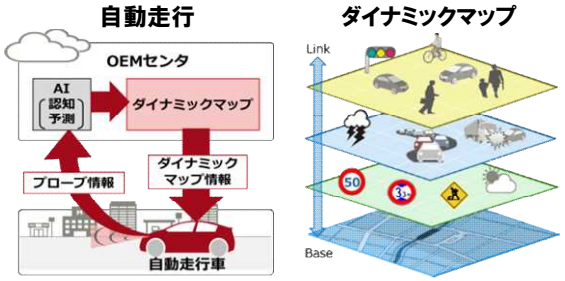
ダイナミックマップの流通においてデータのセキュリティを確保 ～データセキュリティマネジメント～

特長

- ✓ データが流出、拡散した場合にも第三者によるデータの不正利用を防止
- ✓ データを提供した後もデータ利用をコントロール可能
- ✓ 電子署名によるデータの真正性に加え、データ保有者の真正性を確認

本研究開発テーマの背景

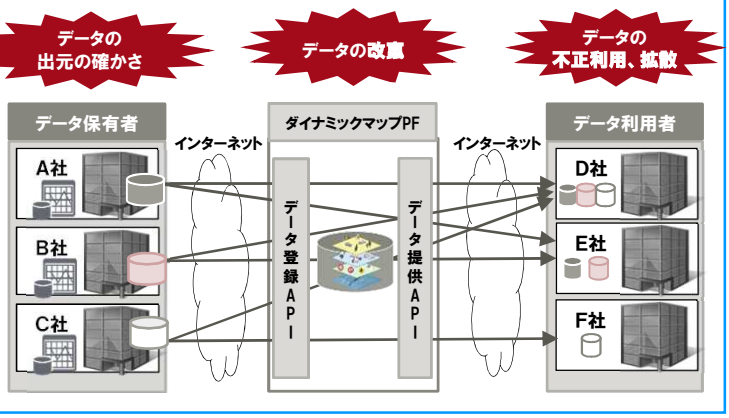
- ➢ 2016年度よりSIP/自動走行システムにおいてダイナミックマップを他分野、多用途に活用するための『ダイナミックマップサービスプラットフォーム』の調査・検討が始まりました。
- ➢ 本研究開発では、SIP/自動走行システム(ダイナミックマップサービスプラットフォーム)と連携し、ダイナミックマップを安心・安全に他分野、多用途に活用するために必要なセキュリティ技術の研究開発に取り組んでいます。



ダイナミックマップの流通に向けた課題

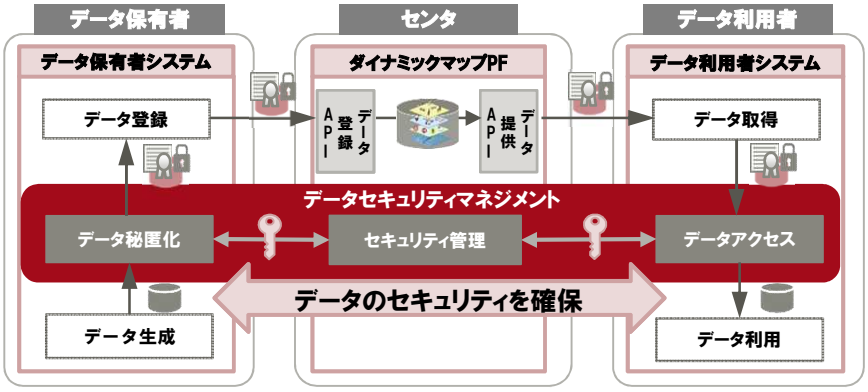
- ➢ ダイナミックマップの流通は、インターネットを介した多対多の取り引きとなる
- ➢ 取り引き相手のセキュリティレベルは様々である
- ➢ データ保有者、データ利用者の双方にとってセキュリティリスクが高く、不安も大きい

課題 データ保有者、データ利用者の双方にとって安心・安全な、ダイナミックマップを流通させる仕組みが必要



データセキュリティマネジメントの仕組みと機能

『データ秘匿化』、『データアクセス』、『セキュリティ管理』が連携する仕組みにより、ダイナミックマップの流通におけるデータのセキュリティ(機密性・完全性・真正性)を確保するレイヤとして機能します。



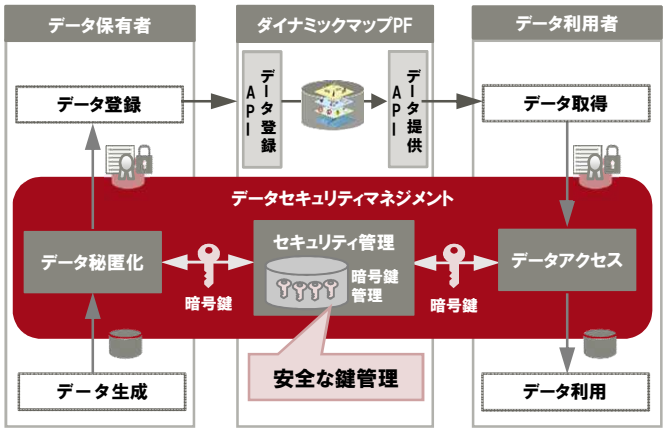
構成要素	主な機能
データ秘匿化	・データの暗号化(鍵取得) ・データへの電子署名付与
セキュリティ管理	・暗号鍵管理(生成～廃棄) ・デジタル証明書管理 ・データ保有者の真正性確認 ・アクセス制御 ・証跡管理
データアクセス	・データの改竄検知 ・データの復号(鍵取得)

【富士通】

ダイナミックマップの流通に向けたデータセキュリティマネジメントの実現

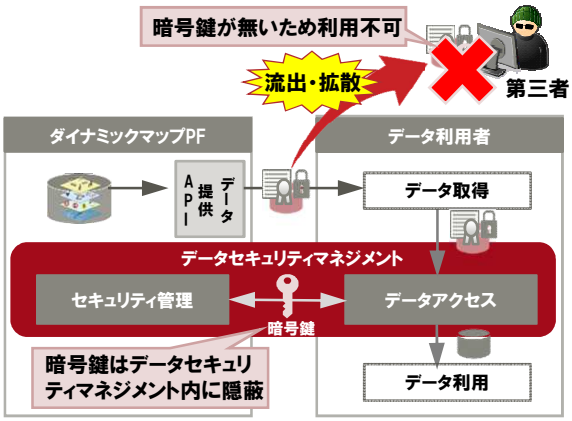
効果① 安全な鍵管理の仕組み

【従来】
データ保有者が暗号鍵を生成、配布
【効果】
データセキュリティマネジメントが暗号鍵のライフサイクルマネジメントに基づいた安全な暗号鍵の生成～廃棄を実施



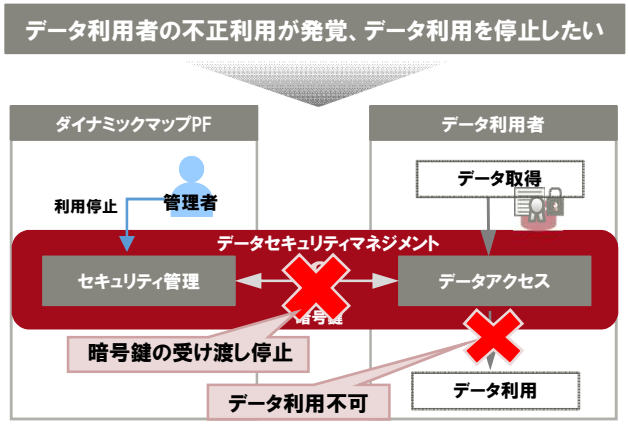
効果② データ流出、拡散時の不正利用を防止

【従来】
データと暗号鍵の両方が流出、拡散した場合、第三者による不正利用が発生
【効果】
暗号鍵はデータセキュリティマネジメント内に隠蔽しているため、データ流出、拡散時の第三者による不正利用を防止



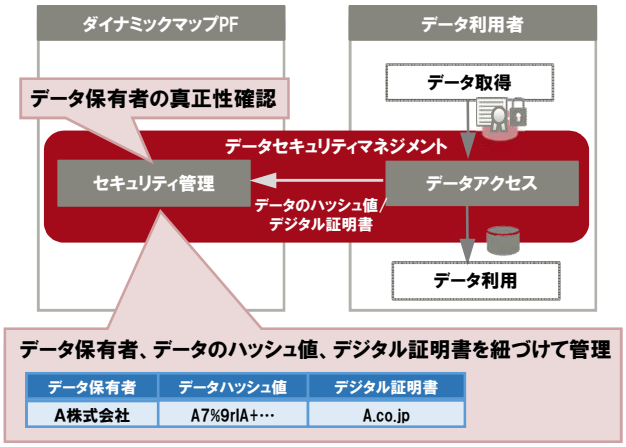
効果③ データ提供後もデータ利用をコントロール

【従来】
データ提供後はデータ利用をコントロールできない
【効果】
データ利用時に暗号鍵を取得するため、データ提供後でもデータ利用をコントロール可能



効果④ データ保有者の真正性を確認

【従来】
電子署名によりデータの真正性は確認可能
【効果】
データの真正性に加え、データ保有者の真正性も確認可能



実施状況

- 2016年度～2017年度は、脅威/リスク分析を実施、ダイナミックマップPFのセキュリティ要求事項を策定。
- 2018年度は、セキュリティ要求事項(データ保護)を実現するデータセキュリティマネジメントのアーキテクチャ、機能仕様、インターフェース仕様の検討とプロトタイプによる有用性の検証/評価に取り組んでいます。

スケジュール

- 本研究開発の成果は、SIP/自動走行システムに提供、ダイナミックマップのセキュリティ強化に役立てられます。
- 将来、他分野のデータ流通PFへの展開を目指します。