

Magic Lock Box

概要

2022年10月

株式会社システムデザイン

はじめに

現在多くの自動車で採用されている**スマートキー**は、その名の通りボタンを押さなくても、自動車のドアノブ等を触るだけで解錠できたり、エンジンをスタートし運転できたりと利便性が高い反面、その脆弱性を利用した **リレーアタック、コードグラバー** という手口で盗難が多発しています。国土交通省が「スマートフォンを利用し、自動車の施錠装置、イモビライザ、盗難発生警報装置を施錠・解錠することを可能とする」と発表したこともあり、**リレーアタック、コードグラバー** 防止にもなる、今回ご提案する仕組み **Magic Lock Box**（特許取得済み）を開発いたしました。

今回開発したものは、類似の他社製品と比較して、次のようなメリットがあります。

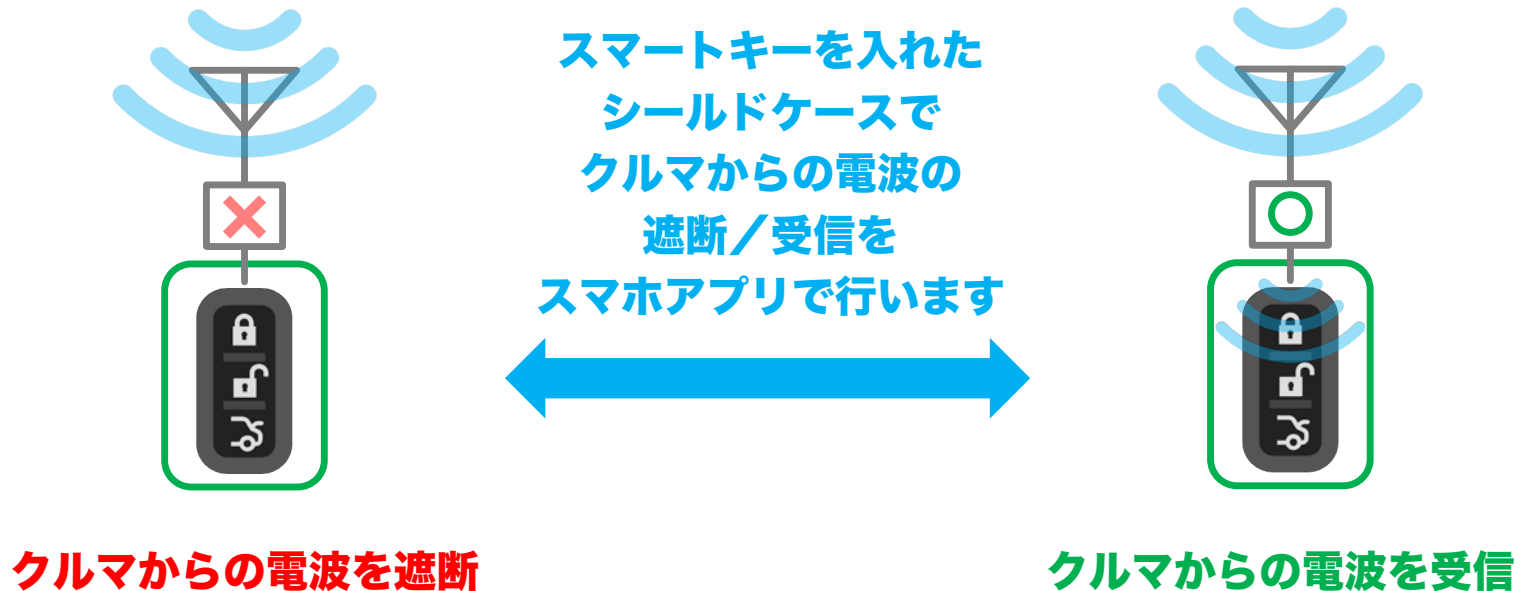
- ・ 自動車やスマートキーへの改造が不要
- ・ リレーアタック、コードグラバーによる盗難対策になる
- ・ 個人利用の場合には、利用時にネットワークに接続する必要がない
- ・ 複雑な仕組みを必要とせず、自動車メーカーを選ばない
- ・ 新車以外にも使用できる
- ・ 既存のカーシェア／レンタカー会社へのサービス提供が可能

本資料では **Magic Lock Box** に関して、その概要をご説明いたします。

Magic Lock Box とは

- ・スマートキーの弱点を利用した車両盗難（リレーアタック、コードグラバー）を防ぐことが可能
- ・クルマを改造する必要が無い
- ・車種を問わず、中古車にも簡単に設置可能で、既存のほぼ全ての車両に対応可能
- ・Bluetoothを利用した1対1の安全な暗号通信
- ・スマートフォン、Apple Watchによるドアの開閉が可能
- ・特許取得技術を利用しており、他社がマネできない
特許取得済み＝日本、台湾　特許出願中＝米国、欧州、中国、インド
- ・既存の車両管理システムとの連携が可能

Magic Lock Boxの仕組み



スマートキーの弱点を補完するために、スマートキーを入れるシールドケース（電波を遮断する箱）を用意し、電波の遮断／受信をスマホアプリで行うことにより、不必要な時にスマートキーが動作しないようにすることで、リレーアタックやコードグラバーを防ぐことができます。

Magic Lock Boxが対応しているキータイプ

スマートキー



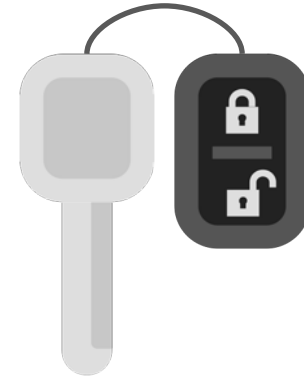
Magic Lock Boxに
入れるだけで
盗難対策！

キーレスキー
イモビライザー付き



イモビライザー機能は
そのまま
利便性アップ！

メタルキー
+ リモコン



利便性アップと
オプションリレー
により盗難対策！

商品説明

電波遮断機能を持つシールドケース（以下 ケース）を車内に設置して使用します。ケースを専用のスマホアプリに事前登録しておくこと、登録済みスマートフォンが近くにある時だけ電波遮断機能が停止し、スマホアプリの操作でケース内のスマートキーのボタンを押してドアを開閉する仕組みとなっています。

クルマとスマートキーの通信電波を遮断した状態で車内に保管するため、昨今車両盗難で多く用いられている「リレーアタック」を防止できます。

スマートフォンとケースはBluetoothで暗号通信を行い、スマートフォン1台で複数車両のスマートキーを代用可能です。そのためカーシェア、レンタカー、社用車の管理用途にも適しています。

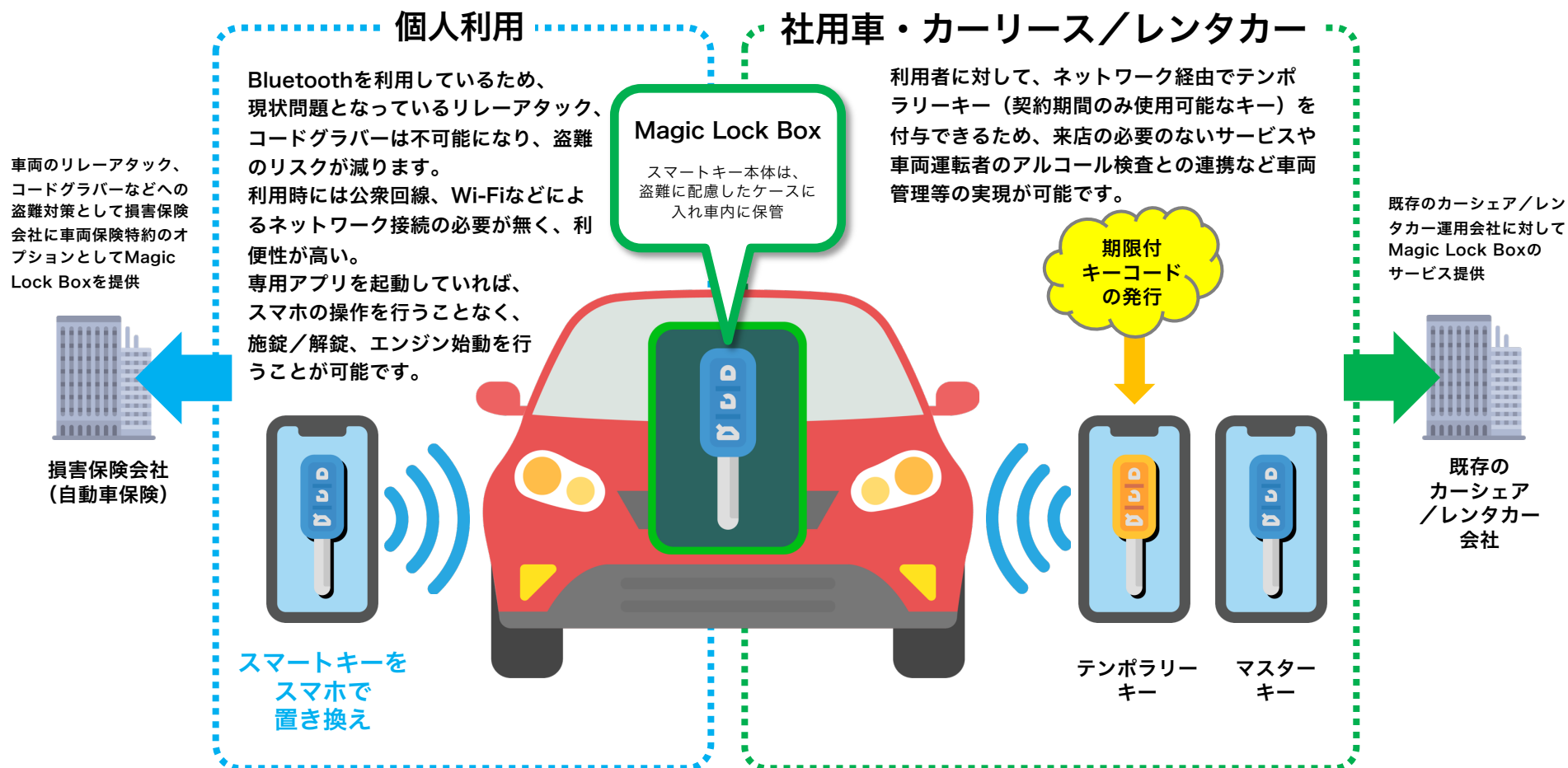
組み込みの際に車両改造も不要で、電池での動作にも対応。電源は車両から取ることもできます。

商品構成



応用例

個人利用から社用車・カーリース／レンタカーまで利用することが可能です。

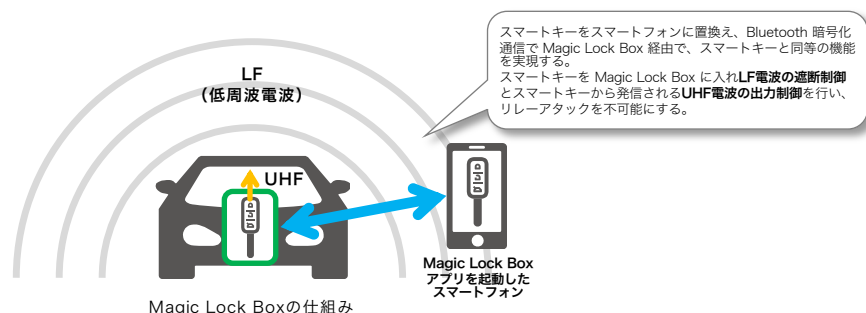
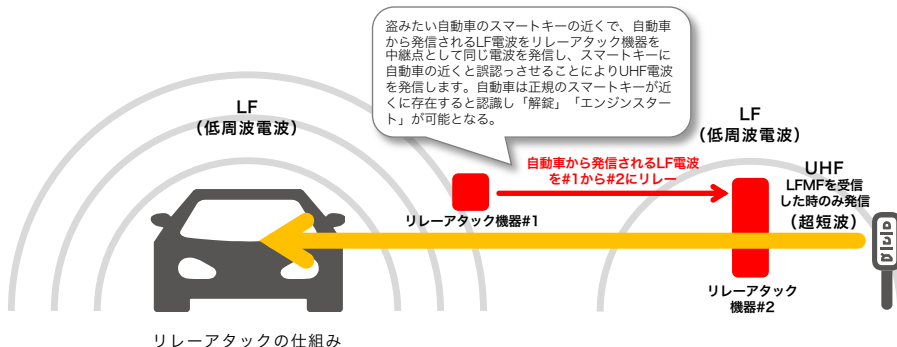
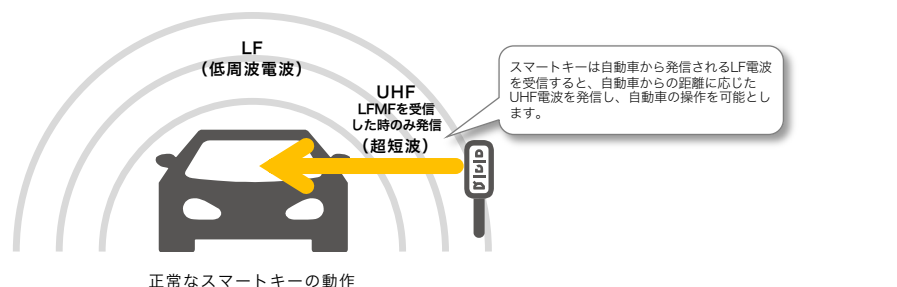


参考資料（リレーアタック防止）

リレーアタック防止の概要

リレーアタックでは、自動車から発信されるLF電波を受信して、遠方にあるスマートキーに特殊な送信機を使って中継し、スマートキーに自動車の近くと誤認させることにより、スマートキーはLF電波に反応してUHF電波で自動車に返答を送ります。

そうすると自動車は正規のスマートキーが近くにあると認識し、ロック解除やエンジンを始動することも可能となります。



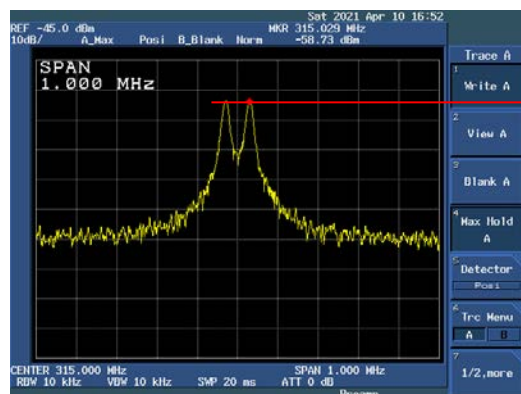
Magic Lock Boxでは、スマートキーを電波シールドボックスに入れ自動車内に設置し、自動車とスマートキーの通信を、スマートフォンからの操作で必要に応じて遮断することにより、リレーアタックを行うことができなくします。

参考資料（コードグラバー防止）

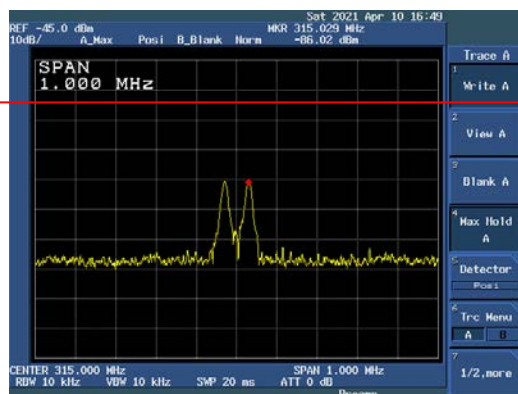
コードグラバー防止の概要

スマートキーは自動車から発信されるLF（低周波電波）を受信し、これを基に自動車とのUHF（超短波）で通信を行っています。コードグラバーは、スマートキーと自動車との通信時にスマートキーから発信されるUHF電波をコピーし、同じ内容の電波を発信することにより、自動車に正規のスマートキーと誤認させています。

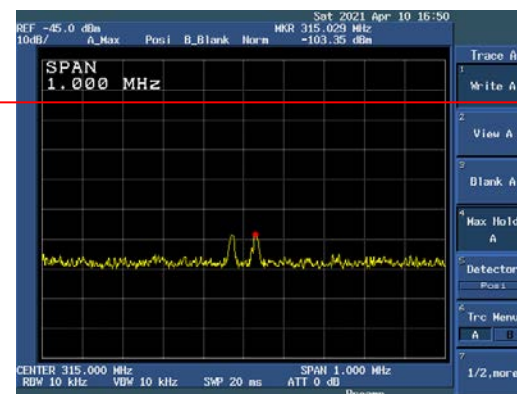
Magic Lock Boxでは、これを防ぐためにスマートキーを自動車内の電波シールドボックスに入れ、LF電波による通信の有効／無効とUHFの電波強度を制御（特許取得済）することによりスマートフォンでスマートキーと同等の利便性を享受できることを実現しています。この技術を応用して自動車内に設置した電波シールドボックス内のスマートキーから発信されるUHF電波を減衰させることにより、自動車の外でスマートキーからの電波を受信することを困難にしコードグラバーで使用される機器で、スマートキーからの電波を受信することを防止します。



通常のスマートリモコンから発信される電波の強さ



Magic Lock Box セキュリティ設定 弱
電波の強さはセキュリティ無しに比べて約1/500



Magic Lock Box セキュリティ設定 強
電波の強さはセキュリティ無しに比べて約1/50000

スマートリモコンから
発信される電波の強さ