



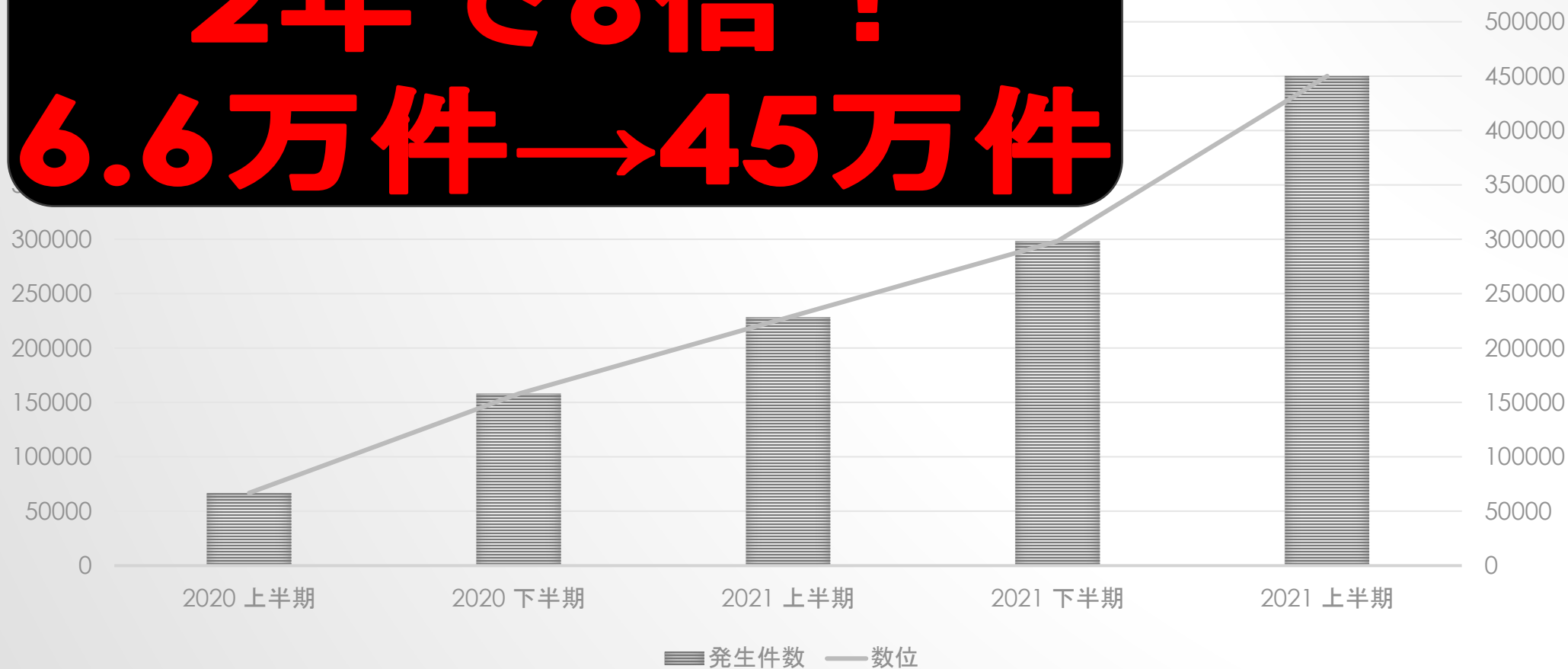
LYDSEC DIGITAL TECHNOLOGY

リーセックデジタルテクノロジー

セキュリティの話

フィッシング詐欺の発生状況（日本）

**2年で6倍！
6.6万件→45万件**



参照 : <https://www.antiphishing.jp/report/monthly>

ちなみに…

	発生件数
令和2年	309,178
令和3年	305,196
令和4年	<u>301,193</u>

交通事故
発生件数

情報漏洩件数（日本）

過去最高165件



フィッシング詐欺や情報漏洩対策？

ファイヤーウォール

**不正侵入の検知・防御
(IDS/IPS)**

**サーバー向け
ウイルス対策ソフト**

VPN

EPP

ID・パスワード管理

EDR

社員教育

ウイルス対策ソフト

それでも広がる被害。

多要素認証が必要では？

Amazon Web Services(AWS)、2024年半ばから多要素認証(MFA)が必須に

掲載日 2023/10/09 12:07

著者：後藤大地



AWS

サイバーセキュリティ

Amazon Web Servicesは、「[Secure by Design: AWS to enhance MFA requirements in 2024 | AWS Security Blog](#)」において、2024年半ば以降すべてのAmazon Web Services(AWS)の特権アカウントに多要素認証(MFA: Multi-Factor Authentication)の使用を義務付けると伝えた。



Contact Us

Support ▼

My Account ▼

Sign In

Create an AWS Account

Products

Solutions

Pricing

Documentation

Learn

Partner Network

AWS Marketplace

Customer Enablement

Events

Explore More



多要素認証とは？

多要素認証とは、2つ以上の異なる要素を用いて、デバイスやツールなどのログイン認証を行うことです。

- ①「本人の特徴」-生体認証等
- ②「本人のみ知っていること」-パスワード等
- ③「本人のみ持っている」-IDカード等
- ④「本人の行動」-場所等

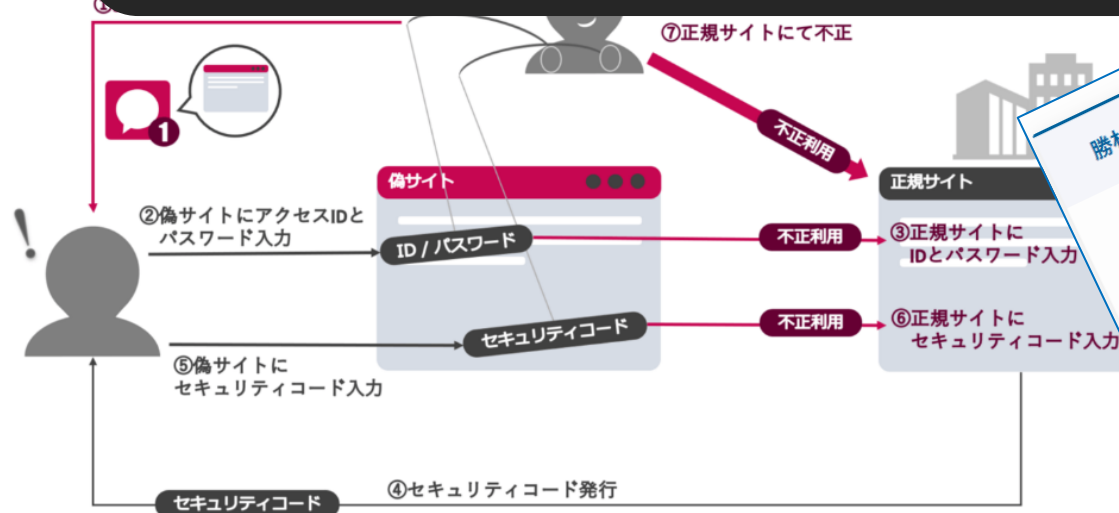
4要素から2つ以上の方法を用いて行います。ひとつのログイン情報だけではログインできないため、不正ログインやなりすましへの効果が高いセキュリティ方法です。

多要素認証のメリットは？

なりすましを激減させることができます。

社内・社外360° でセキュリティが確保できます。

2020年2月6日 10:19



ワンタイムパスワード
成功率8割をうたう恐るべし

LYDSEC DIGITAL TECHNOLOGY

リーセックデジタルテクノロジー

多要素認証ソリューション

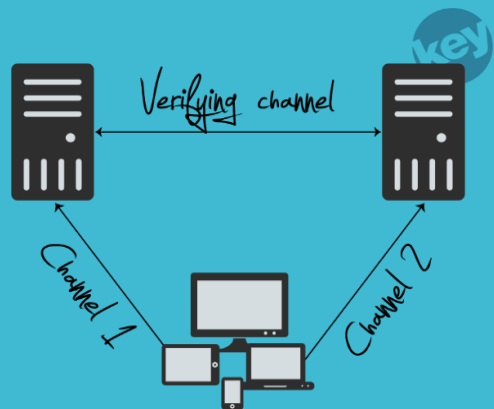


多要素認証ソリューション：キーパスコ

KYPASCOの特徴は？
キーパスコ

「KEYPASCO は色々な要素をご用意しておます。」

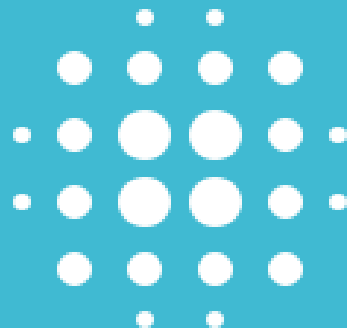
2チャンネル認証



デバイスフットプリント



リスクエンジン



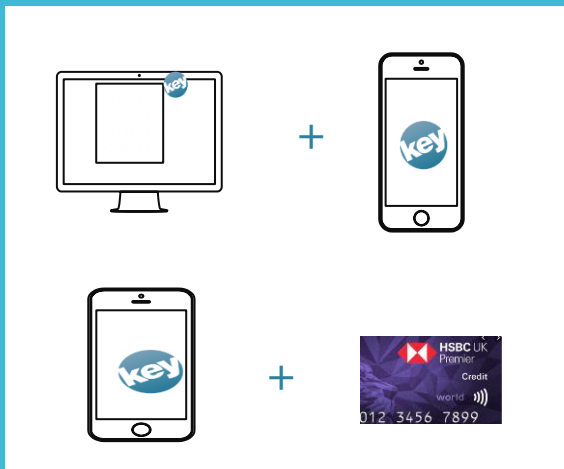
ジオロケーション



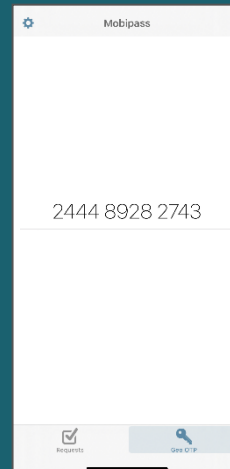
時間管理



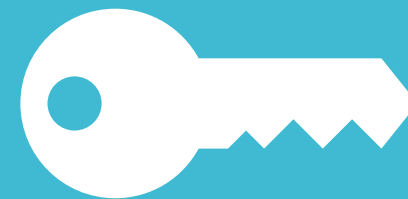
プロキシ

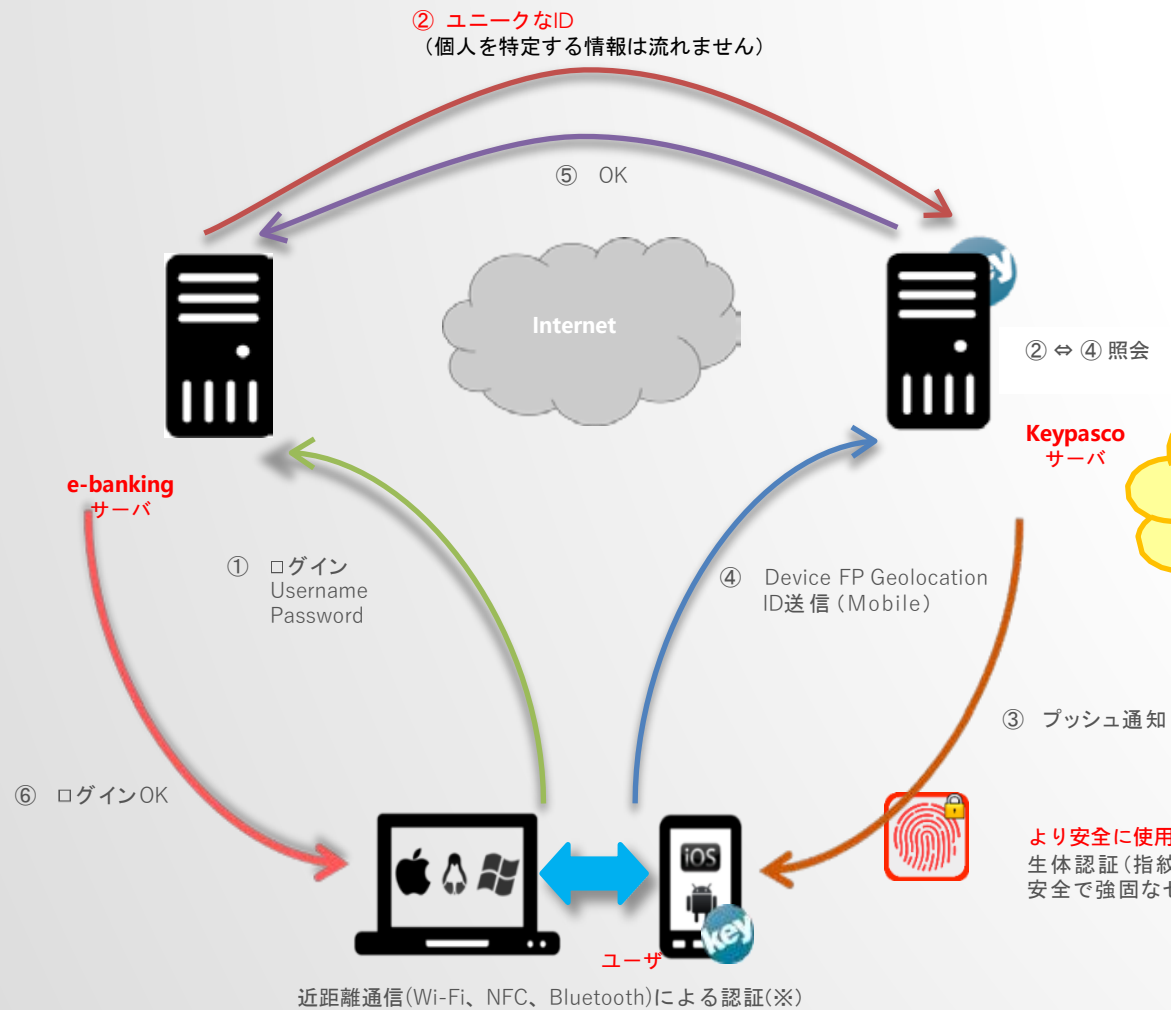


ワンタイムパスワード



分散型 PKI Sign



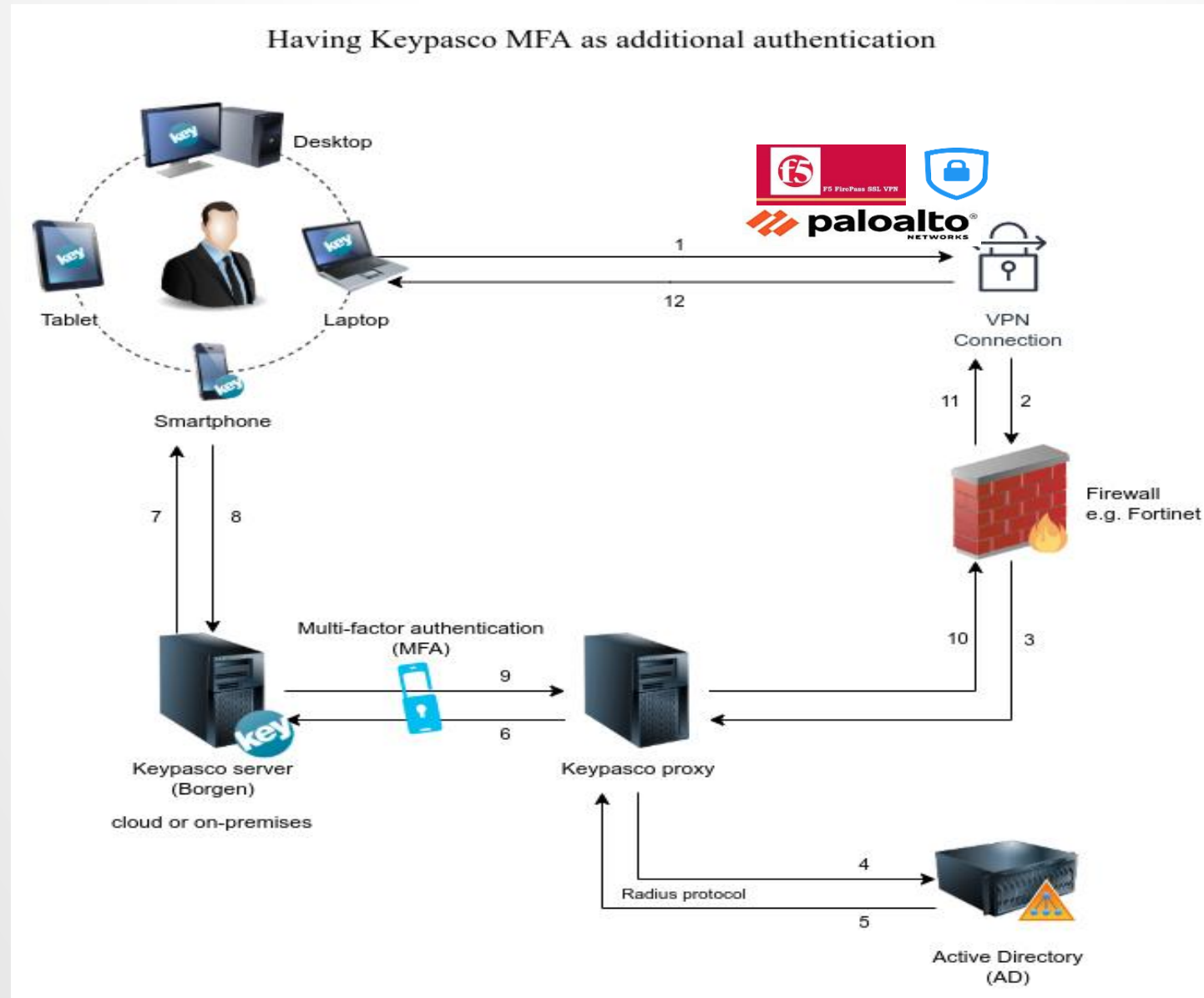


- ① e-bankingのサイト(例)へログイン (Username、Pasword入力)
 - ② e-bankingサーバは、ログイン情報をもとに、登録済みのユニークなIDをKeypascoサーバに送信
(※個人を特定する情報は流れません)
 - ③ Keypascoサーバは認証済みのユーザのモバイル端末にプッシュ通知を送信
 - ④ 認証済みのユーザのモバイル端末からDevice FP、Geolocation IDを送信
 - ⑤ Keypascoサーバは、登録済みのユニークなIDと、④の情報を照会。正規のログインかどうかを判断。
 - ⑥ Keypascoサーバによって正規のログインが承認されると、ユーザーはe-bankingのサイトにログイン可能
- ※ 認証済みの端末を持って席を離れた際に悪意ある人がPCに対して不正にログインを試みても、認証済みの端末が近くにならないため、ログイン不可能

- ・ 認証された端末からログインが行われた場合：ログイン可能
- ・ 認証されていない端末からログインが行われた場合：ログイン不可能

「KEYPASCO は簡単に導入可能」

プロキシモデル



LYDSEC DIGITAL TECHNOLOGYは、どんな会社？
リーセックデジタルテクノロジー

「LYDSEC DIGITAL TECHNOLOGY社は、
多要素認証ソリューションの専門会社です。」

**2012
本社台湾**

**R&D
スウェーデン**

**利用業界
10+**

**ユーザー数
1000万+**

**特許 (国数)
5(16)**

**特許証書
63**

**Global
Awards
8**



Keypasco 各賞一覧

1. フロスト&サリバン2014年新製品イノベーションリーダーシップ賞
受賞：セキュアな多要素認証ソリューション
2. APICTA 2014 Merit Awards in Lydsec Bao for Securely Managing Accounts：金融分野
3. Red Herring Europe 2016年アワード：同社の「Keypasco Multi-Factor Authentication」がイノベーションと健全なビジネスモデルであることを示す賞
4. 2016 Contactless & Mobile Awardsを受賞：ペイメントセキュリティ／Keypasco PKI Sign機能
5. インターネットセキュリティプロバイダー・オブ・ザ・イヤー2017
GDSの最も革新的な多要素認証技術
6. AWS Cloud Challenge 2019 トップテン
7. 2019 Taipei Startup Demo Day Awardを受賞しました：レインメーカーとミスター・ポピュラー・フォー・イノベーション
8. 最も革命的なインターネットセキュリティカンパニー - スカンジナビア2020"

2022 SELECT USA サイバーセキュリティ部門1位



特許一覧

5つの特許はすべて米国、日本、台湾、韓国で対応しています。そのうちのいくつかは、EU、中国、シンガポールで承認されています。合計16カ国、63件の特許証書を取得。

1. Device Fingerprint and two-channel authentication method: 2チャンネル構造により、ユーザー自身のデバイスをユニークな認証デバイスとして使用。Security by Your own device
2. Proximity: ユーザー自身のデバイスを近接させることで、ユニークなIDとしてセキュリティを強化する。Internet of Things
3. Central stored PKI solution: デバイス FP で保護されたモバイルアプリに配布される復号化された半分のプライベートキーのみ使用。PKI on open platform without distributed credentials
4. Dynamic URL: 複数のICPと複数のIDP（IDプロバイダ）が同じクライアント/アプリで利用できる動的で柔軟なURLをサポートする認証構造です。
Security on your terms
5. Key Management and System: キー管理とシステム デバイスの固有値で保護された暗号化された半分のプライベートキーのみをモバイルアプリに配布。 Split PKI private key

ご質問

デモ

LYDSEC DIGITAL TECHNOLOGY は
多要素認証ソリューションに自信が御座います。

是非、皆様のお話をお伺いさせていただきます。

Lydsec Digital Technology Japan 株式会社

担当：青柳

Mail: Aoyagi@lydsec.com