DIGITAL DEVELOPMENT SYSTEMS

DDS PARTNER EXECUTIVE CONFERENCE

全てに対応可能な万能認証基盤それが"Themis"
マガタマサービスとの連携で作る新しいビジネスインフラ

ビジネスチャンスはどこにあるか！貴社の為DDSは何をするのか?

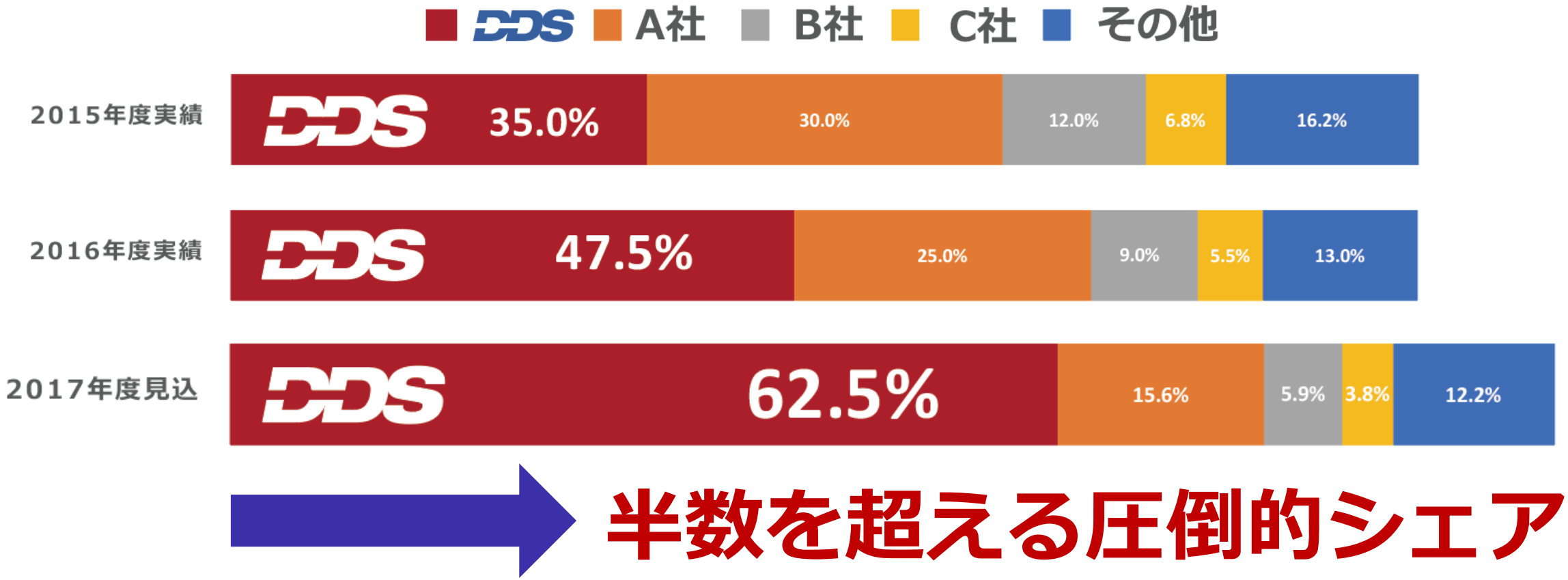
株式会社ディー・ディー・エス
専務取締役 久保統義

DDSの状況

急拡大する市場占有率

DDS PARTNER EXECUTIVE CONFERENCE

PC向け指紋認証シェア推移



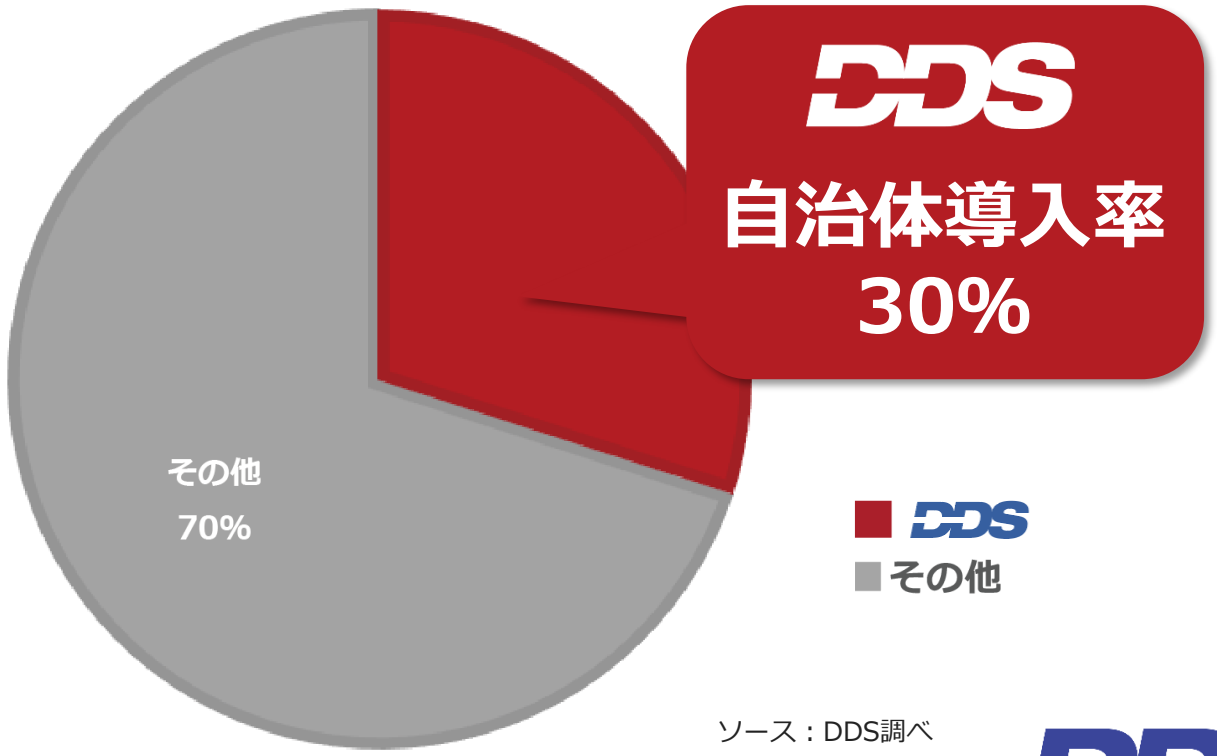
半数を超える圧倒的シェア

出典：富士キメラ総研『2017ネットワークセキュリティビジネス調査総覧』（2015年実績は『2016ネットワークセキュリティビジネス調査総覧』）

DDS DIGITAL DEVELOPMENT SYSTEMS

自治体 強靭性向上の結果

- 保守契約有：270自治体
- ライセンスのみ、またはスタンドアロン版利用：250自治体
- その他：1,221自治体



ソース：DDS調べ

東京大学との産学連携

DDS PARTNER EXECUTIVE CONFERENCE

2018年4月19日
日経産業新聞掲載

2018年（平成30年）4月19日（木曜日） 16
日経産業新聞

指紋認証 汗の穴で識別

Start Up
Innovation
Science

スマートフォン（スマホ）にも搭載され、広く知られる個人認証技術「指紋認証」。しかし、認識精度に限界があり、誤認や偽造などの懸念も指摘される。生体認証システムのディー・ディー・エス（DDS）と東京大学は指の汗が出る穴に着目し、精度を10倍以上高めることに成功した。読み取るセンサーのコストなど課題も残るが、個人認証の新たな手段として注目されそうだ。

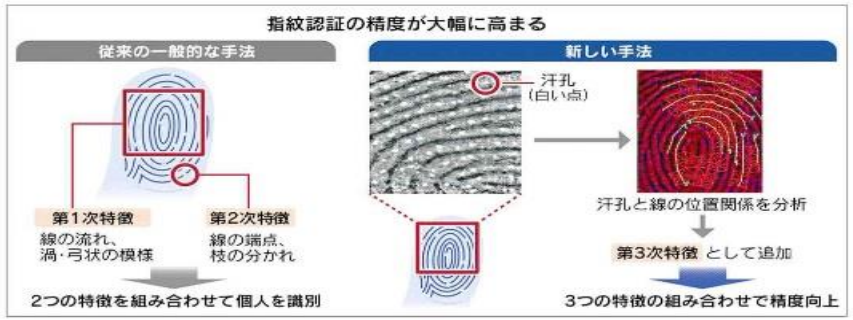
「従来の指紋認証は精度に限界がある。決済など様々な場面でスマホが使われるなか、より簡単で精度の高い個人認証技術が必要だ」。東京大学大学院の梅崎太造特任教授は、新たな指紋認証手法を開発した狙いを強調する。

現在の一般的な指紋認証は、複数の隆起した線（隆線）が集まって模様になった渦状紋などの「第1次特徴」と、線の分岐点や端点といった「第2次特徴」で個人を判別する。技術は確立されており、実績もある。

誤認や偽造も

しかし、スマホのセンサーのように読み取る面積が小さくなると、捉えられる特徴点が少なくなる。他人の指紋を登録者のものと誤って認識したり、偽造した指紋で認証を突破されたりといった懸念が指摘されてきた。

入室用の指紋認証機器といった大きなセンサーを使用する指紋認証では無作為に選んだ人がロックを解除できる確率は100万分の1程度とされる。一方、スマホでは5万分の1程度に低下するという。

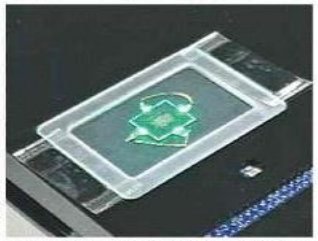


実際に米国のミシガン州立大学の研究グループは、指紋をインクジェットプリンターで偽造してスマホの認証を突破できると報告している。また、他人の指を本人のものと誤認してしまいスマホのロックを突破される危険性も報告されている。

DDSと東大が開発した技術は従来の2つの特徴に加えて、汗が出るための小さな穴である「汗孔（かんこう）」を“第3次特徴”として利用する。汗孔は個人によって位置関係が異なる。この汗孔同士の位置関係や線と汗孔の位置関係を判定基準に加えることで、精度を10倍以上に高めることができるという。

汗孔は隆線の中に数多く存在しており、スマホに搭載する小さなセンサーでも多くの特徴を捉えることが可能だ。ただ、現在の主流の静電容量式センサーでは十分な解像度がなく、小さな汗孔を検知できない。

スマホで活用、精度10倍に


指紋の「汗孔」を見られるセンサー

このため、DDSは新たなセンサーを開発した。薄いガラス板とイメージセンサー、発光ダイオード（LED）を組み合わせており、指の表面に光を当てて浸透率や反射率を利用して微細な隆線を読み取る。

検出部の大きさは縦6・6㍉×横4・8㍉で厚さも約0・6㍉と小さい。従来のセンサーは解像度が500ppi（1㌅あたりの画素数）程度だったが、新しいセンサーでは3000ppiまで高められるという。読み取った汗孔の位置関係から個人を認証できるソフトウエアも梅崎氏とDDSが開発した。

価格下げ課題

スマホに搭載される一般的なセンサーの価格は100～1000円程度とされる。新開発のセンサーはまだスマホに搭載できるほど安くはないが、今後は量産による価格低減で既存センサーと同程度まで下げられるとみる。スマホメーカーの採用を目指す。

さらに、将来は指をディスプレーに触れるだけで指紋認証できるようにして、ホームボタンのない機種にも対応できるようにしたい考え。スマホ以外でも自動車や住宅のカギなど様々な用途への展開を計画する。

生体認証には指紋認証のほか、静脈認証や顔認証、虹彩認証、音声認証など多くの技術がある。

このうち、DDSは新米アップルは「iPhone X」で3次元の顔認証技術、サムスン電子は「ギャラクシーS9」で顔認証と光彩認証を組み合わせた認証技術をそれぞれ採用している。これらは指紋認証に換わる認証技術として期待が高まっているが、現状では精度を疑問視する声も少なくない。

スマホ搭載のカメラは小型化を優先するため、生体認証に使うのに十分な精度が得られないケースもある。実際に「写真を本人と間違える」「双子の見分けがつかない」といったトラブルも報告されている。

精度が高いとされる静脈認証もセンサーの小型化が難しく、利用はATMなど一部に限られている。指紋認証は今後も様々な場面で利用されるのは間違いなく、汗孔を使った新技術に注目する企業も出てきそうだ。

（佐藤雅哉）

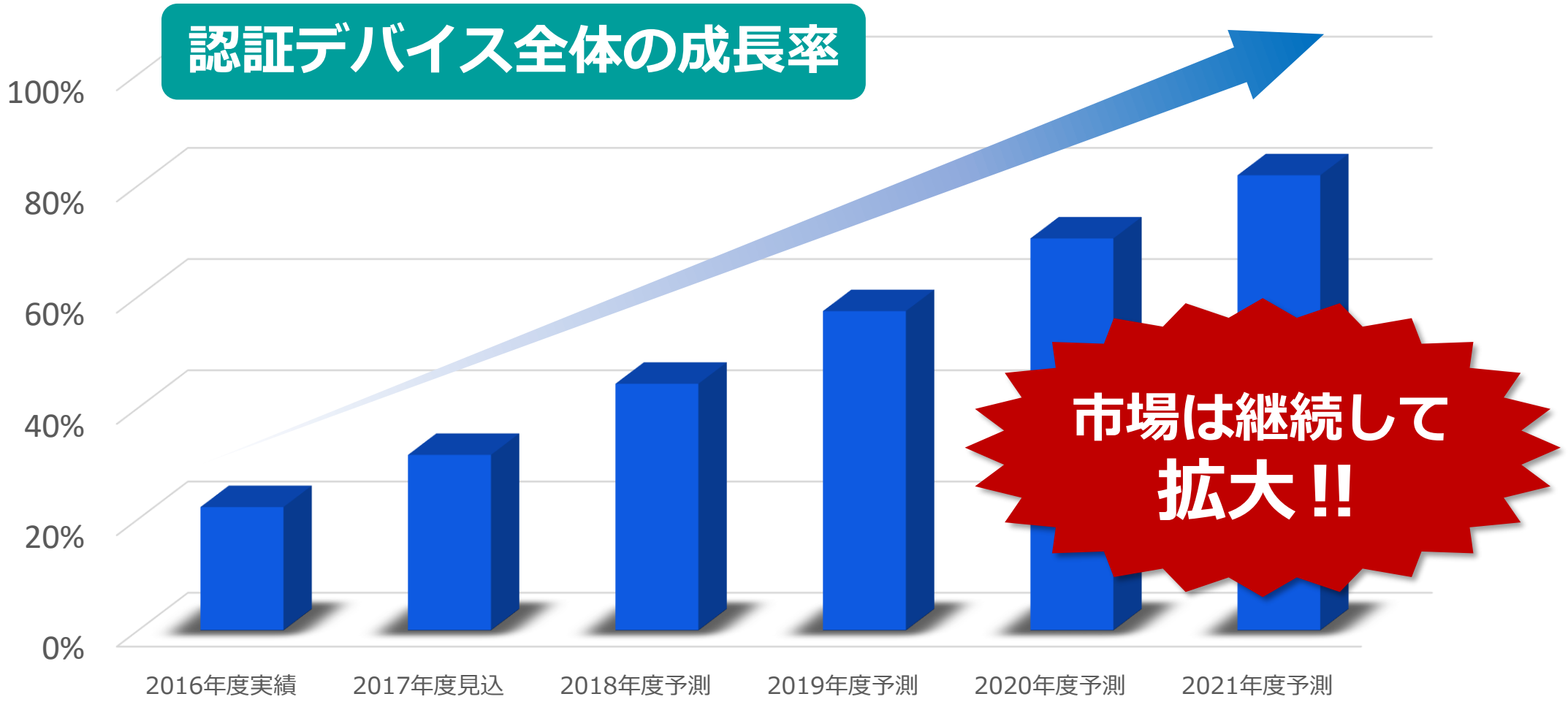
SiSOC TOKYO

DDS DIGITAL DEVELOPMENT SYSTEMS

認証市場の状況

拡大する認証市場

DDS PARTNER EXECUTIVE CONFERENCE



富士キメラ総研 『2017 ネットワークセキュリティビジス調査総覧 』の認証デバイス市場（ICカード、指紋・静脈・顔認証ツール、金額ベース）の2015年度を基準とした成長率を示した。

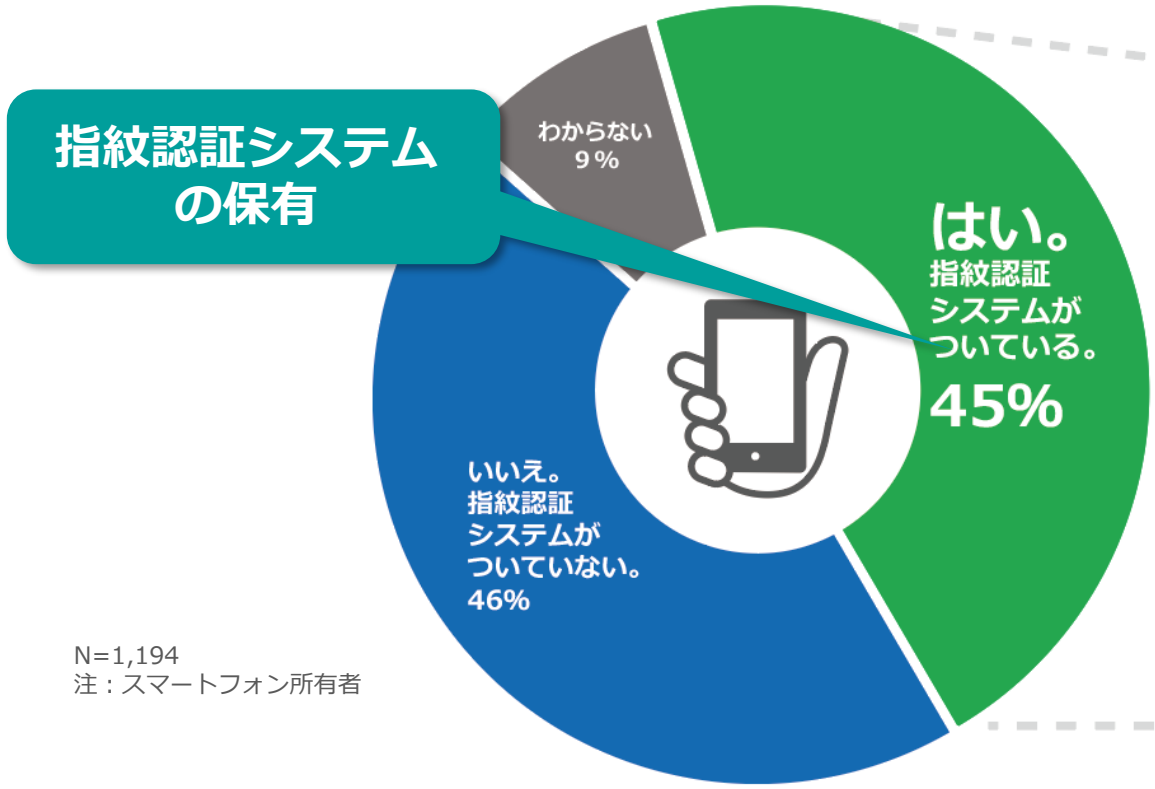
DDS DIGITAL DEVELOPMENT SYSTEMS

スマートデバイスでの生体認証

DDS PARTNER EXECUTIVE CONFERENCE

回答者の45%が指紋認証機能がついた携帯電話を所有しており、そのうち2/3がロック解除やモバイル決済等の認証に利用している。

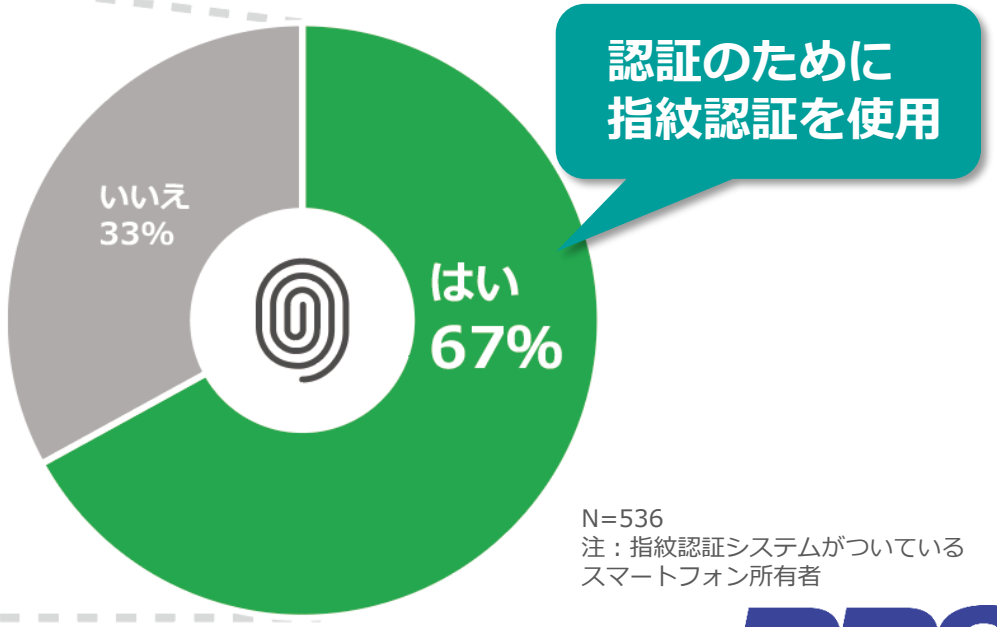
使用しているスマートフォンに指紋認証システムはあるか？（日本）



N=1,194
注：スマートフォン所有者

本人認証※1のために指紋認証を使用したことはあるか？（日本）

※１スマートフォンのロック解除・モバイル決済時など



N=536
注：指紋認証システムがついているスマートフォン所有者

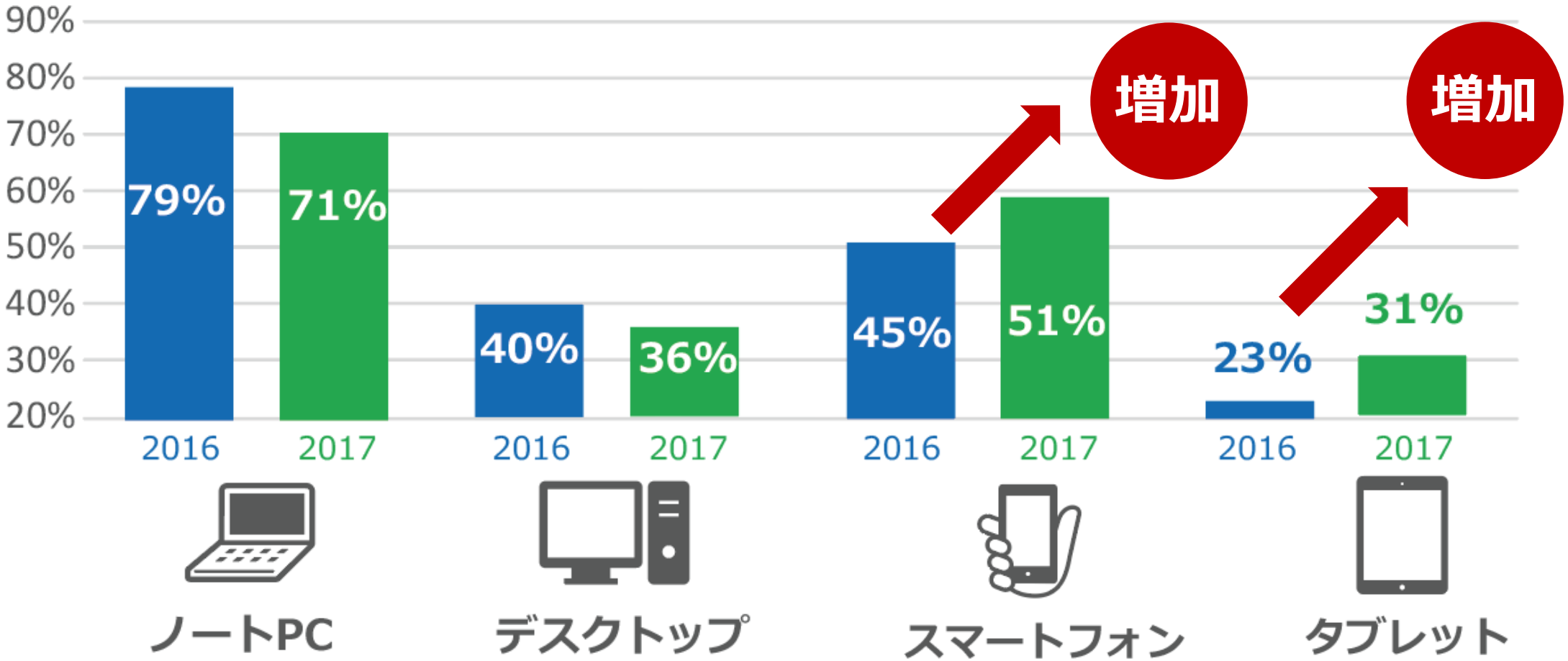
出典：デロイトトーマツ「世界モバイル利用動向調査2017」より抜粋・加筆

DDS DIGITAL DEVELOPMENT SYSTEMS

使われるデバイスの変化

DDS PARTNER EXECUTIVE CONFERENCE

所有しているもしくは利用できるデバイスは？（日本/経年）※複数回答



出典：デロイトトーマツ「世界モバイル利用動向調査2017」より抜粋・加筆

DDS DIGITAL DEVELOPMENT SYSTEMS

改正個人情報保護法

◆**個人情報保護法**
『改正個人情報保護法』（2017年5月30日全面施行）
◆**自治体**
『自治体情報システムの強靭性の向上』
◆**医療**
『医療情報システムの安全管理に関するガイドライン』
◆**金融**
『PCIデータセキュリティ基準』『FISC安全対策基準』
◆**文教**
『教育情報セキュリティポリシーに関するガイドライン 』

改正個人情報保護法

① 個人情報を**取得・利用**する時のルール
⇒個人情報を取得した場合は、その利用目的を本人に通知、又は公表すること（あらかじめ利用目的を公表している場合を除く。）

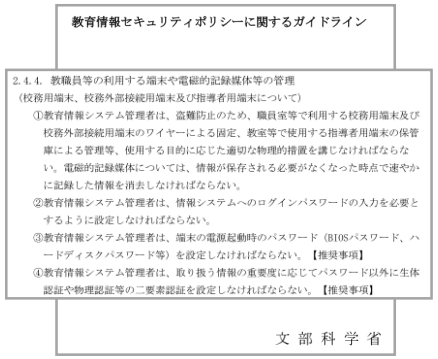
② 個人情報を**保管**する時のルール
⇒情報の漏えい等が生じないように安全に管理すること

③ 個人情報を**他人に渡す**時のルール
⇒個人情報を本人以外の第三者に渡すときは、原則として、あらかじめ本人の同意を得ること

④ 個人情報を**外国にいる第三者に渡す**時のルール

⑤ 本人から個人情報の**開示を求められた**時のルール
⇒本人からの請求に応じて、個人情報を開示、訂正、利用停止等すること

文　教


教育情報セキュリティポリシーに関するガイドライン

2.4.4. 教職員等の利用する端末や電磁的記録媒体等の管理
（校務用端末、校務外部接続用端末及び指導者用端末について）
①教育情報システム管理者は、盗難防止のため、職員室等で利用する校務用端末及び校務外部接続用端末のワイヤーによる固定、教室等で使用する指導者用端末の保管庫による管理等、使用する目的に応じた適切な物理的措置を講じなければならない。電磁的記録媒体については、情報が保存される必要がなくなった時点で速やかに記録した情報を消去しなければならない。
②教育情報システム管理者は、情報システムへのログインパスワードの入力を必要とするように設定しなければならない。
③教育情報システム管理者は、端末の電源起動時のパスワード（BIOSパスワード、ハードディスクパスワード等）を設定しなければならない。【推奨事項】
④教育情報システム管理者は、取り扱う情報の重要度に応じてパスワード以外に生体認証や物理認証等の二要素認証を設定しなければならない。【推奨事項】

文 部 科 学 省

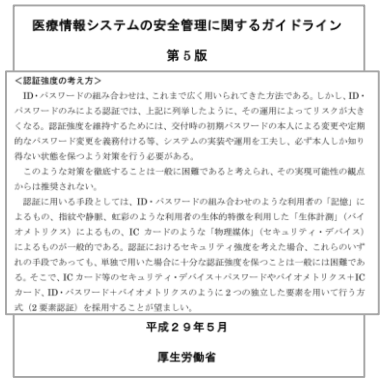
金　融


PCI Security Standards Council

Payment Card Industry（PCI）
データセキュリティ基準

要件とセキュリティ評価手順
バージョン 3.2
2016 年 4 月

医　療


医療情報システムの安全管理に関するガイドライン

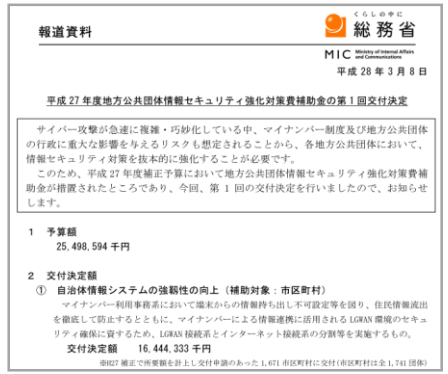
第５版

＜認証強度の考え方＞
ID・パスワードの組み合わせは、これまで広く用いられてきた方法である。しかし、ID・パスワードのみによる認証では、上記に列挙したように、その運用によってリスクが大きくなる。認証強度を維持するためには、交付時の初期パスワードの本人による変更や定期的なパスワード変更を義務付ける等、システムの実装や運用を工夫し、必ず本人しか知り得ない状態を保つよう対策を行う必要がある。
このような対策を徹底することは一般に困難であると考えられ、その実現可能性の観点からは推奨されない。
認証に用いる手段としては、ID・パスワードの組み合わせのような利用者の「記憶」によるもの、指紋や静脈、虹彩のような利用者の生体的特徴を利用した「生体計測」（バイオメトリクス）によるもの、IC カードのような「物理媒体」（セキュリティ・デバイス）によるものが一般的である。認証におけるセキュリティ強度を考えた場合、これらのいずれの手段であっても、単独で用いた場合に十分な認証強度を保つことは一般には困難である。そこで、IC カード等のセキュリティ・デバイス＋パスワードやバイオメトリクス＋IC カード、ID・パスワード＋バイオメトリクスのように２つの独立した要素を用いて行う方式（2 要素認証）を採用することが望ましい。

平成２９年５月

厚生労働省

自 治 体


報道資料

総務省
MIC Ministry of Internal Affairs and Communications
平成 28 年 3 月 8 日

平成 27 年度地方公共団体情報セキュリティ強化対策費補助金の第１回交付決定

サイバー攻撃が急速に複雑・巧妙化している中、マイナンバー制度及び地方公共団体の行政に重大な影響を与えるリスクも想定されることから、各地方公共団体において、情報セキュリティ対策を抜本的に強化することが必要です。
このため、平成 27 年度補正予算において地方公共団体情報セキュリティ強化対策費補助金が措置されたところであり、今回、第 1 回の交付決定を行いましたので、お知らせします。

1　予算額
25,498,594 千円

2　交付決定額
① 自治体情報システムの強靱性の向上（補助対象：市区町村）
マイナンバー利用事務系において端末からの情報持ち出し不可設定等を図り、住民情報流出を徹底して防止するとともに、マイナンバーによる情報連携に活用される LGWAN 環境のセキュリティ確保に資するため、LGWAN 接続系とインターネット接続系の分割等を実施するもの。
交付決定額　16,444,333 千円
※H27 補正で所要額を計上し交付申請のあった 1,671 市区町村に交付（市区町村は全 1,741 団体）

働き方改革にも生体認証

DDS PARTNER EXECUTIVE CONFERENCE

事業主が労働時間の適正な把握の為、講ずべき措置

○使用者は、労働者の労働日ごとの始業・終業時刻を確認し、適正に記録すること

（１）原則的な方法

・ 使用者が、自ら現認することにより確認すること

・ タイムカード、ＩＣカード、パソコンの使用時間の記録等の客観的な記録を基礎として確認し、適正に記録すること

（２）やむを得ず自己申告制で労働時間を把握する場合

① 自己申告を行う労働者や、労働時間を管理する者に対しても自己申告制の適正な運用等ガイドラインに基づく措置等について、十分な説明を行うこと

② 自己申告により把握した労働時間と、入退場記録やパソコンの使用時間等から把握した在社時間との間に著しい乖離がある場合には実態調査を実施し、所要の労働時間の補正をすること

③ 使用者は労働者が自己申告できる時間数の上限を設ける等適正な自己申告を阻害する措置を設けてはならないこと。さらに36協定の延長することができる時間数を超えて労働しているにもかかわらず、記録上これを守っているようにすることが、労働者等において慣習的に行われていないか確認すること

出典：厚生労働省・都道府県労働局・労働基準監督署
「労働時間の適正な把握のために使用者が講ずべき措置に関するガイドライン」

DDS DIGITAL DEVELOPMENT SYSTEMS

DDS PARTNER EXECUTIVE CONFERENCE

全てに対応可能な万能認証基盤それが"Themis"

マガタマサービスとの連携で作る新しいビジネスインフラ

2018

DDSは何をやるのか？

DDS
DIGITAL DEVELOPMENT SYSTEMS

Universal Authentication Themis

magatama

で、DDSは何を提供できるのか？

DDS DIGITAL DEVELOPMENT SYSTEMS

多要素認証基盤の提供

DDS PARTNER EXECUTIVE CONFERENCE

認証要素をAND/ORで指定可能

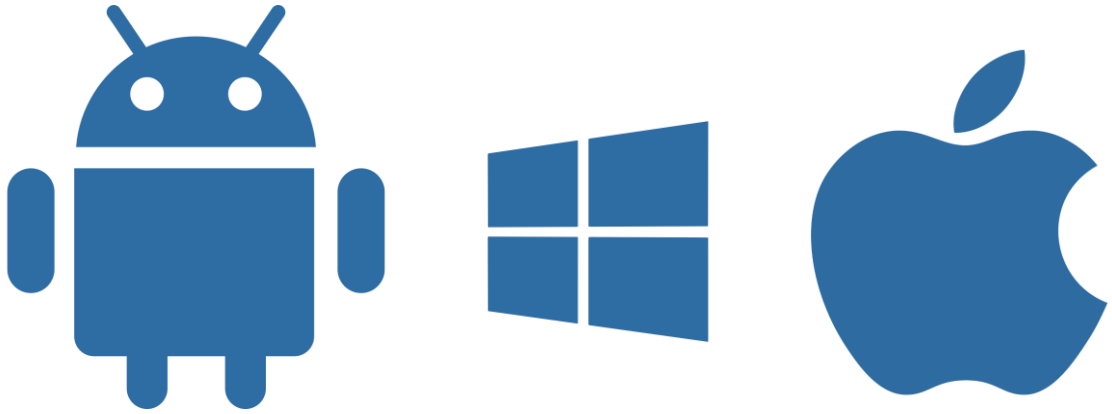
- 指　紋
- PC内蔵 指紋認証
- 顔
- てのひら 静　脈
- 指　静　脈
- IC カード
- ワンタイム パスワード
- テンポラリ パスコード
- パスワード

DDS DIGITAL DEVELOPMENT SYSTEMS

マルチデバイス認証基盤の提供

DDS PARTNER EXECUTIVE CONFERENCE

デバイスを選ばない認証基盤



Universal Authentication Themis

magatama

DDS DIGITAL DEVELOPMENT SYSTEMS

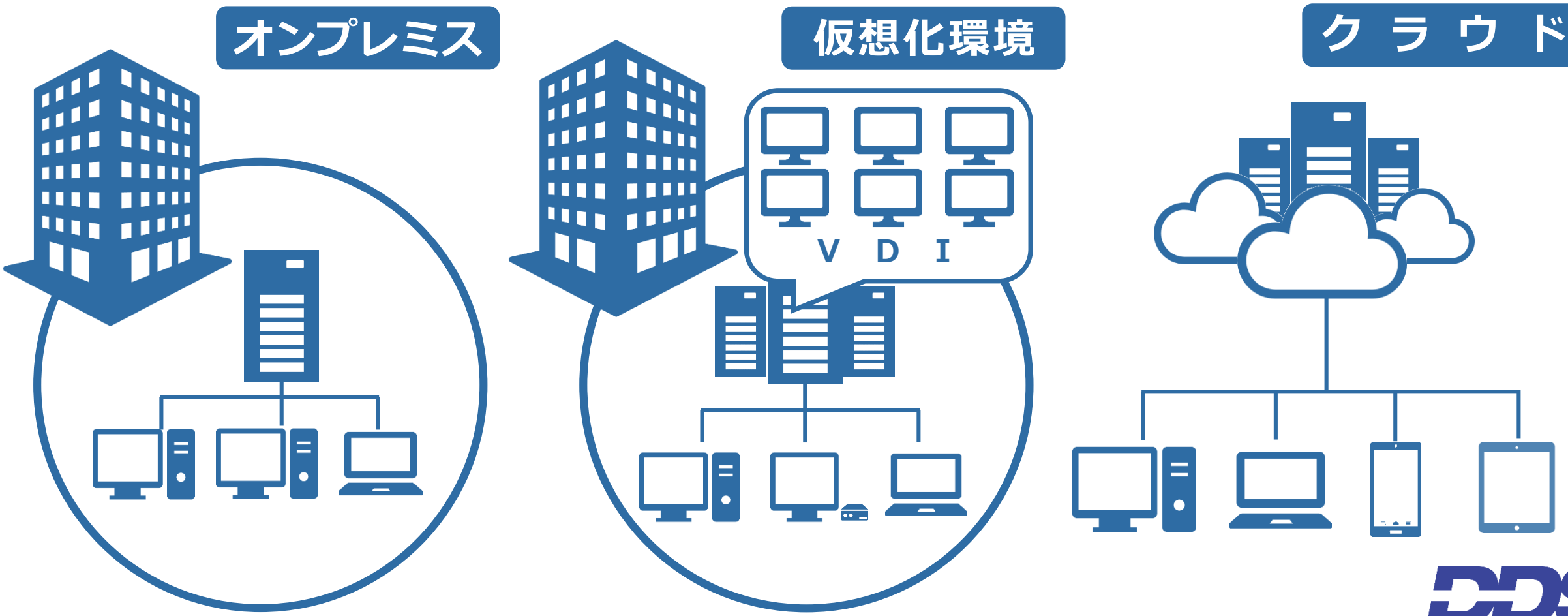
マルチ環境認証基盤の提供

DDS PARTNER EXECUTIVE CONFERENCE

環境を選ばない認証基盤

Universal Authentication Themis

magatama



DDS DIGITAL DEVELOPMENT SYSTEMS

Universal Authentication Themis

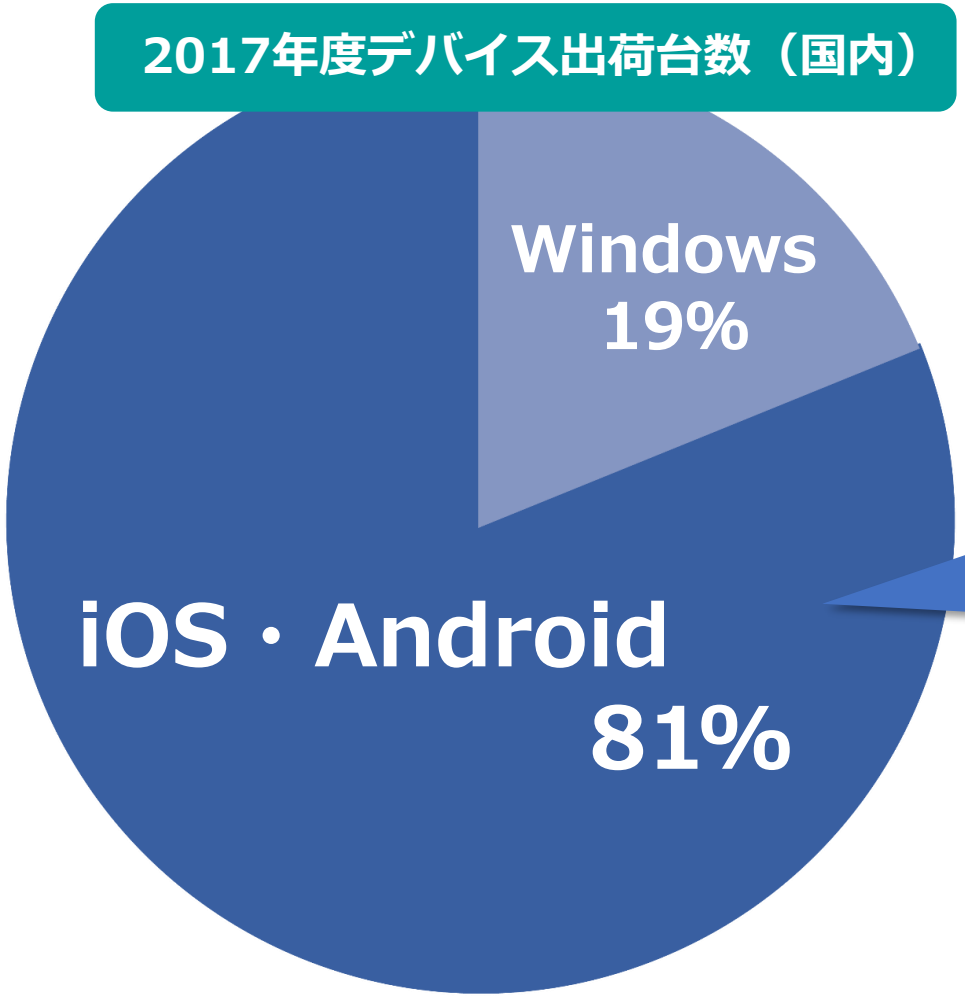
magatama

で、提供するBlue Ocean

DDS DIGITAL DEVELOPMENT SYSTEMS

今回 創られるBlue Ocean

DDS PARTNER EXECUTIVE CONFERENCE



Windows 1025.3万台に対し

新たに
4,128万台※の市場

※17年国内出荷台数
内訳：タブレット 870万台 スマートフォン 3,258万台

出展：MM総研株式会社 https://www.m2ri.jp/news より抜粋加筆

DDS DIGITAL DEVELOPMENT SYSTEMS

Universal Authentication Themis

magatama

ご拡販に際してDDSからの支援

DDS DIGITAL DEVELOPMENT SYSTEMS

トレーニングの無償提供

DDS PARTNER EXECUTIVE CONFERENCE

Universal Authentication Themis

magatama

営業トレーニング

技術トレーニング

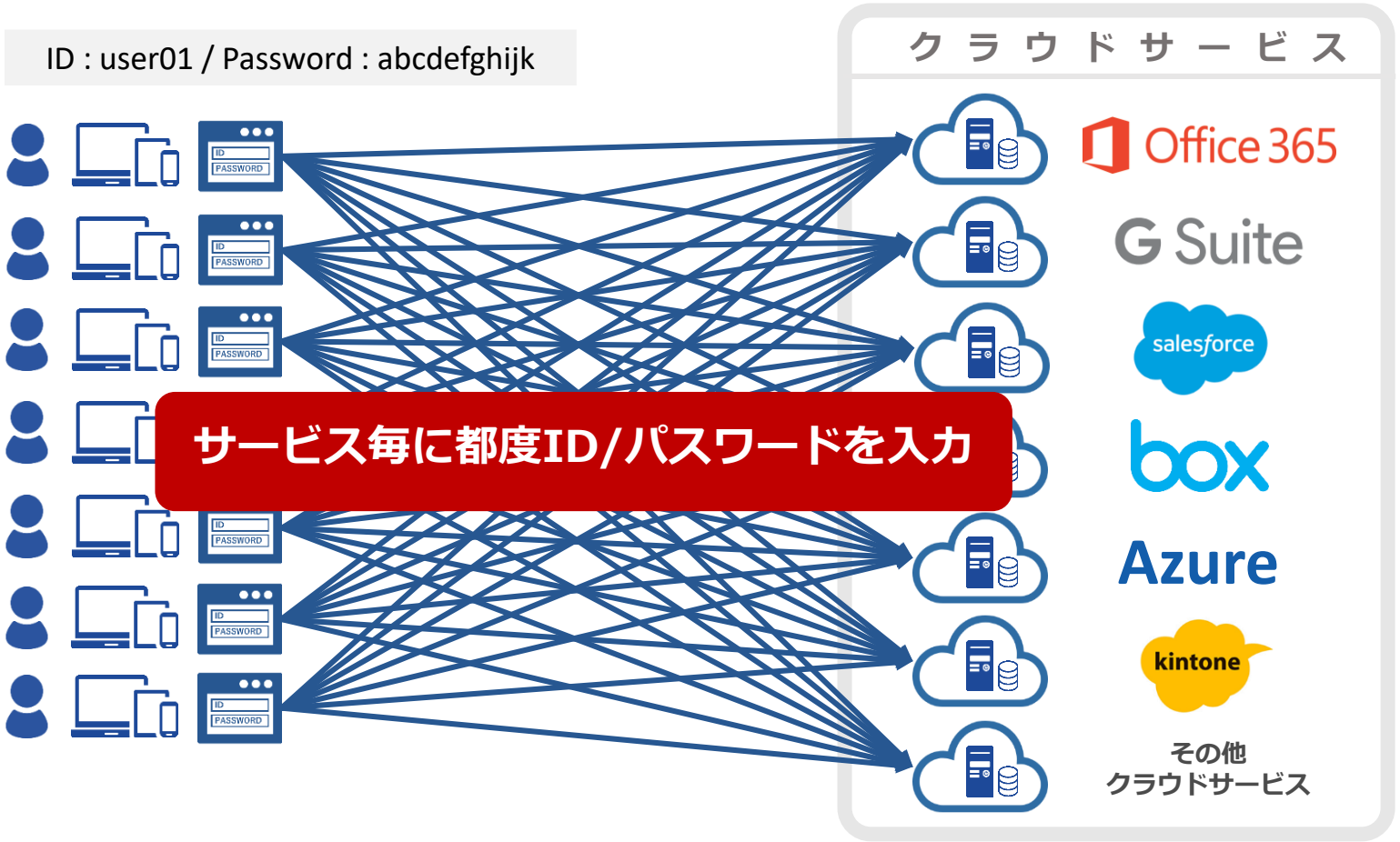
→ 無償提供いたします

DDS DIGITAL DEVELOPMENT SYSTEMS

IDPの立ち上げ支援

DDS PARTNER EXECUTIVE CONFERENCE

複数のクラウドサービス利用において、ユーザーはログイン時に都度ID/パスワードを入力する必要があります。



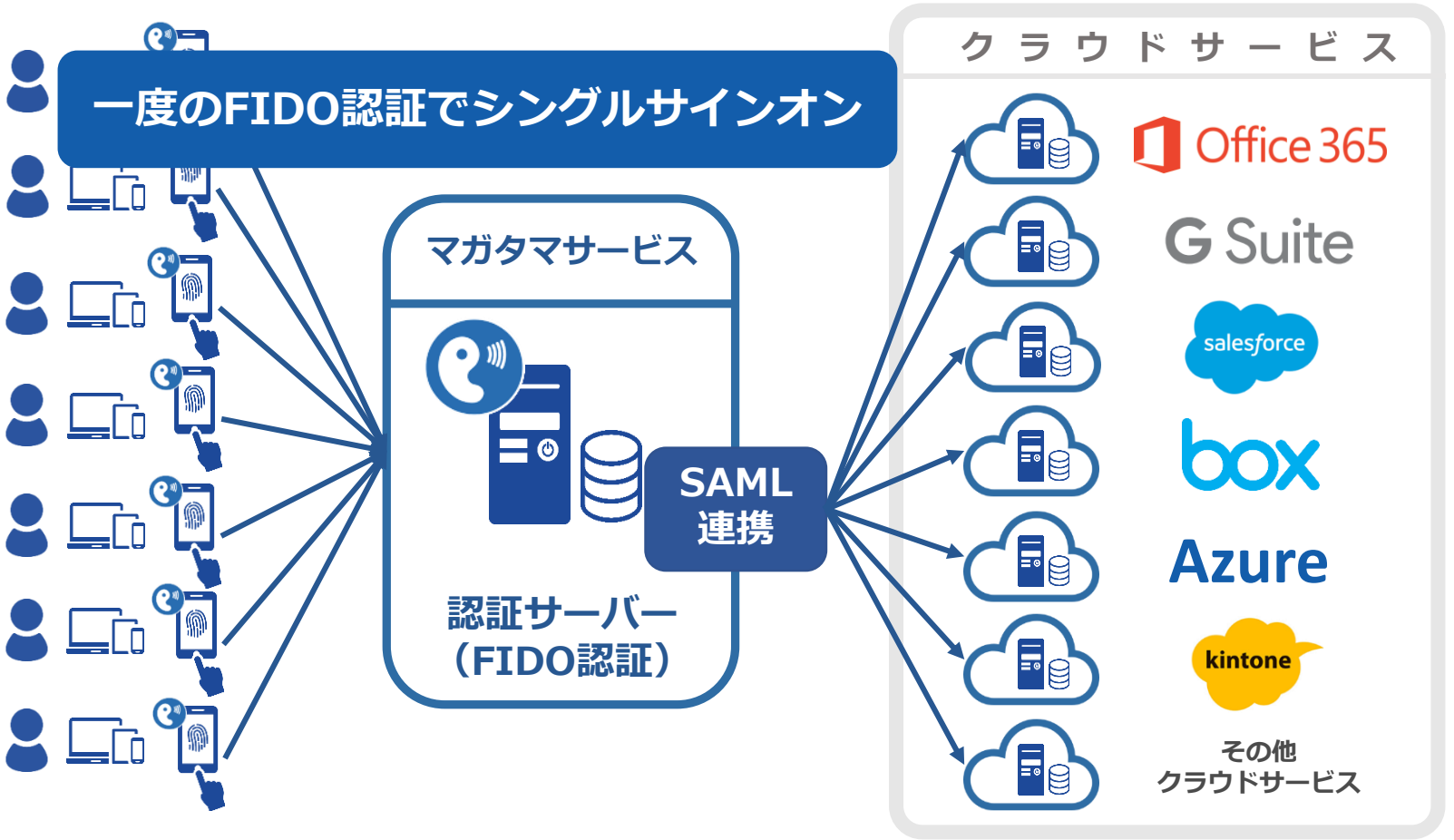
また、社内ではユーザーアカウントの**登録・削除作業に追われ管理に手間**がかかります。

DDS DIGITAL DEVELOPMENT SYSTEMS

IDPの立ち上げ支援

DDS PARTNER EXECUTIVE CONFERENCE

貴社Idpサービスを開始することで、クラウドサービスへのアクセスを集約し、認証を一手に引き受けることができます。



fido ALLIANCE

FIDO対応の認証サーバーであれば、**セキュリティも利便性も向上します。**

DDS DIGITAL DEVELOPMENT SYSTEMS

販促補助金のご提供

DDS PARTNER EXECUTIVE CONFERENCE

貴社でThemis及びマガタマサービスの
販売促進を行っていただいた場合

Universal Authentication Themis　magatama

販促費用の6割をDDSが負担

総額５００万円をご用意

→ 営業担当へご連絡ください

DDS DIGITAL DEVELOPMENT SYSTEMS

本日のまとめ

本日のポイント

DDS PARTNER EXECUTIVE CONFERENCE

Themis＋マガタマサービスで理想の認証基盤が実現します

万能認証基盤Themisとクラウド本人認証マガタマサービスを組み合わせれば、
社内からの認証も、社外からのマルチデバイスによる認証も一元管理。
Active Directoryとの連携はもちろん、多要素認証対応で、認証要素の追加も
簡単だから、導入後もサスティナブルに運用可能。

Universal Authentication Themis

magatama

いつでも・どこでもセキュアに働ける安心をお客様へ提案しませんか？

DDS DIGITAL DEVELOPMENT SYSTEMS

ご静聴ありがとうございました