



弊社取得済特許利用

世界77億人以上に貢献する  
「本人確認と認証情報管理」  
—スマホ紛失時自動安全対処システム—

開発中スマホ割符概要説明抜粋版  
です

2020年10月16日

# 会社概要



20年超の先進情報セキュリティ技術研究開発ノウハウで、人に優しいIT環境を実現したい

◎「**たくさんの人を幸せにしたい**」という揺るぎない創業理念

◎信頼の割符技術と複数取得済み特許をPRO向けから消費者を含めた広範な事業に活かすフェーズへ



創業	1994年8月(創業時は有限会社)
資本金	4233万円(2020年9月末時点)
役員及び正社員数	5名(監査役含め役員4名正社員1名)
事業内容	自社技術GFI電子割符®のライセンスに付帯する一切の事業等
参加団体	一般財団法人日本情報経済社会推進協会 (JIPDEC) 一般社団法人コンピュータソフトウェア協会(CSAJ) 秘密分散法コンソーシアム(SSS-C)、他



代表取締役社長 保倉 豊

代表取締役社長	保倉 豊(やすくら ゆたか)
生年月日	1968年8月14日
IT関係経歴	ECOM(電子商取引実証推進協議会:現JIPDEC)WGメンバーや理事等 秘密分散法コンソーシアム発起人・幹事、他
所属や論文等	情報処理学会、「電子割符」のデジタル社会への応用(川城三治共著)、 センサシステムと秘密分散技術(電子割符)による安全安心な社会基盤 システム(電気学会査読付き論文)、他

## 現状役員及び新任予定監査役紹介

### 川城三治(かわしろさんじ)

#### 技術及び知財担当取締役

旧通商産業省工業技術院電気試験所(現:産業技術総合研究所)IEC日本代表委員として国際標準化に貢献、Ecomで弊社代表保倉と出会い電子割符の必要性に賛同し合流。

### 山本直弘(やまもとなおひろ)

#### 経営全般担当取締役

弊社代表とは高校時代の同級生で弊社創業時から弊社事業全般の相談対応し、弊社代表が開発着手した電子割符の開発を陰ひなたなく応援。

### 船山雅史(ふなやままさし)

#### 2020年監査役就任予定

Citibank、HSBCを経て、公認会計士事務所を開設。弊社とはHSBC時代に富裕層業務での顧客情報保護に対する電子割符導入検討から、交流が深まった。

# 認証機関との提携認証



## 国際的観点

TUVラインランドグループ様とGFIは幅広い分野で相互協力していく事を確認し、2005年1月27日に2社提携証書に署名。これは、GFIが自社内部情報を自社電子割符技術を活用したシステムで保護し、BS7799とISMSを取得したことに起因。情報セキュリティ・マネジメントシステムに関連する規格に対し、弊社のBS7799-2(現:ISO27001)認証取得の事例を基にした規格開発協力や、電子割符技術の規格への組入れなどを視野に入れ、当該情報セキュリティ文化の国際普及に相互協力します。



<http://www.gfi.co.jp/>

認証書授与式当日写真 アジア グループ取締役副社長 K.K.ハインツ様 と GFI代表取締役社長 保倉豊  
関連参考:EU個人データ保護認証 代表的秘密分散技術(GFI電子割符®)を用いた世界発の事例  
[http://www.tuv.com/jp/japan/about\\_us\\_jp/press\\_2/news\\_1/newscontentjp\\_21163.html](http://www.tuv.com/jp/japan/about_us_jp/press_2/news_1/newscontentjp_21163.html)

※テュフ ラインランド グループは、グローバルに技術サービスを提供する世界有数の第三者認証機関です。

参考: <https://www.tuv.com/world/en/about-us/>



# IT環境の本人確認と認証

## 一人とITシステムの隔たり

開発中スマホ割符概要説明抜粋版  
です

- ①そもそも本人確認と認証とは
- ②人のとITシステムに横たわる溝
- ③人とシステムの結びつき
- ④結局責任主体は人なのだから
- ⑤認証情報管理事業の必要性

# ①本人確認と認証とは

社会から本人と認められ社会的存在になること



人と人との信頼関係や「縁」が根底に存在します

## ②人とITシステムに横たわる溝

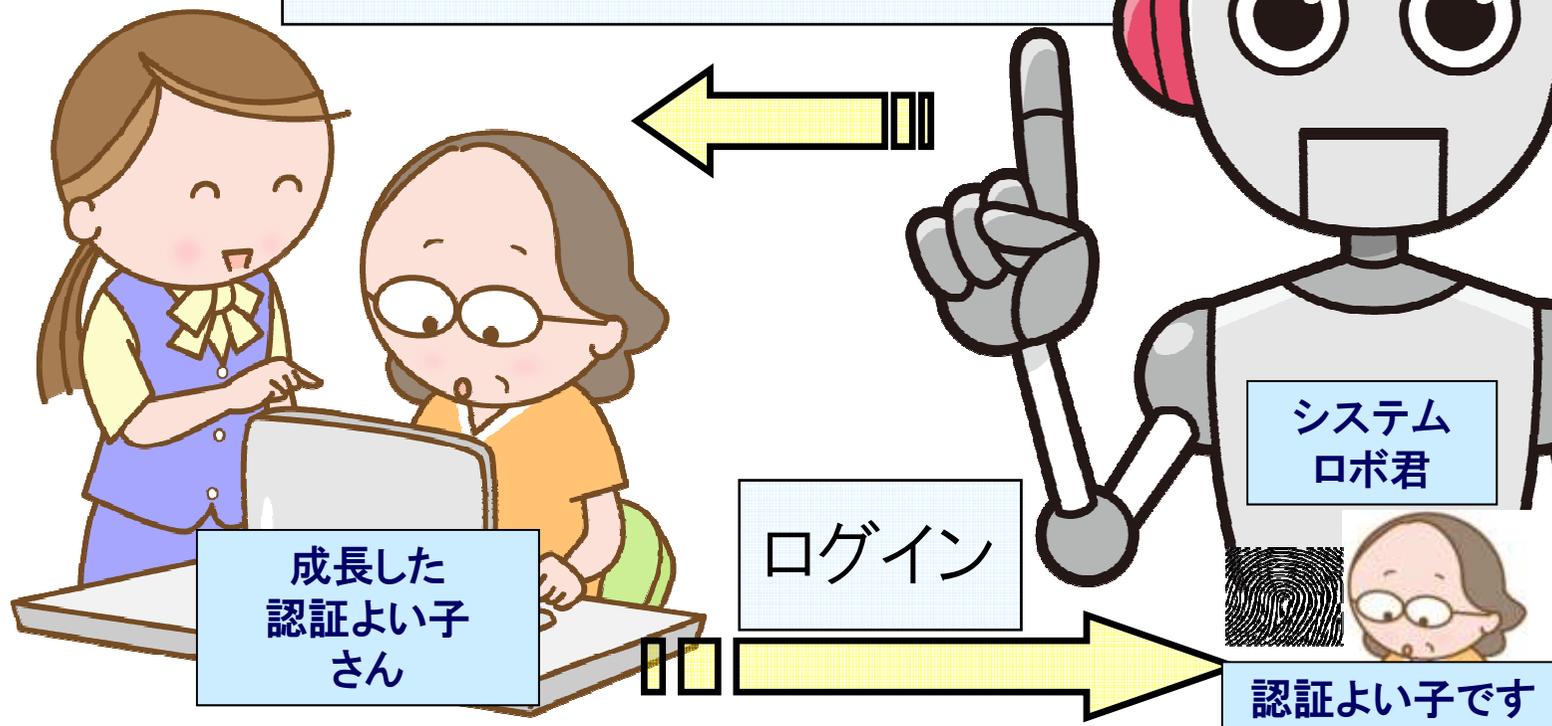


システムは単に人が決めたルール内で動く道具

あなたは認証よい子さんの  
ようですね(みなし)！  
このサービス使えます

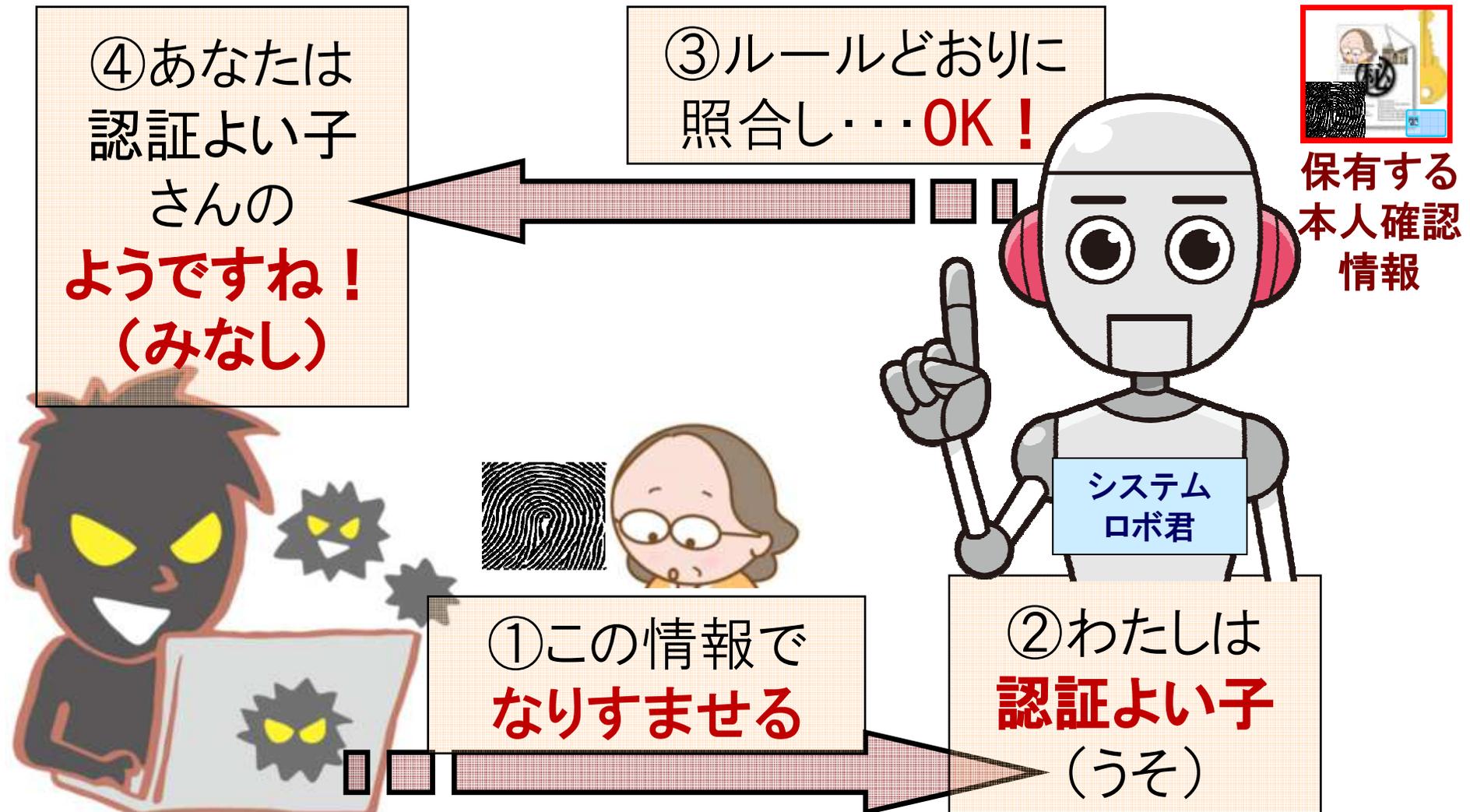


保有する  
本人を確認  
する情報



### ③人とシステムの結びつき

本人確認・認証情報悪用で**なりすまし**が可能



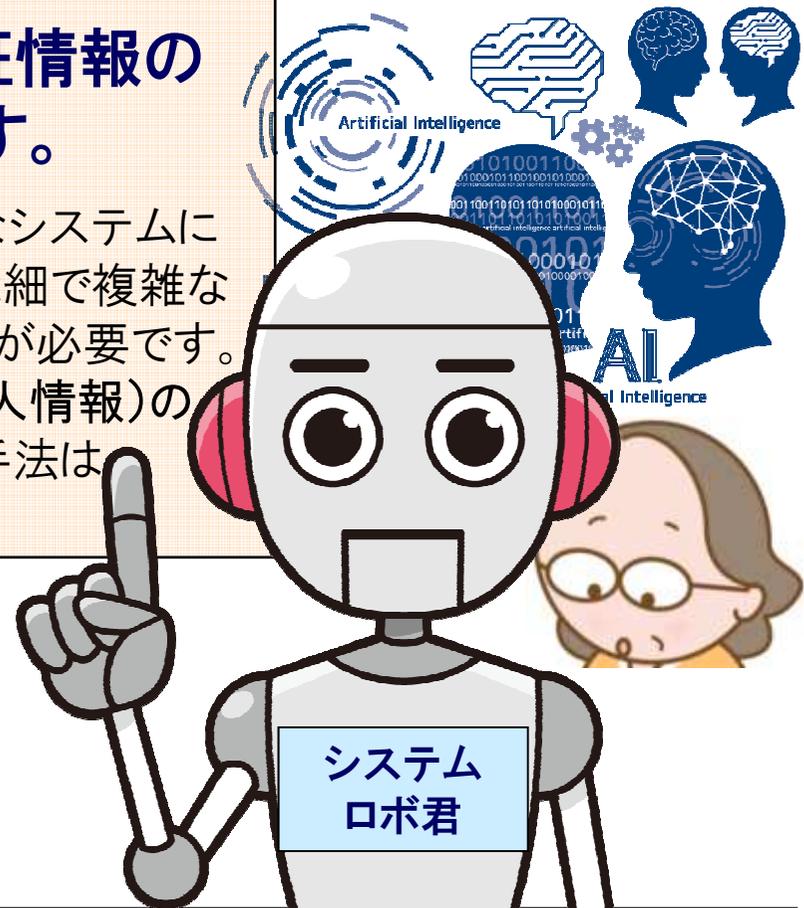
## ④結局責任主体は人なのです

システムは人間同士のような認証ができません

**まずは人間の皆さん、ご自身の認証情報の  
安全管理の徹底をお願いします。**

ITシステムは、AI等を利用してより人間らしく安全なシステムになろうとされていますが、人間同士の認証は非常に繊細で複雑な仕組みで容易に真似できませんし、更に多くの情報が必要です。

まずは、お預かりしている皆さんの認証情報(個人情報)の安全管理をがんばらねば！不正攻撃者の手法は日々高度化・巧妙化しています。



**不正攻撃の第一歩は、認証情報の不正取得です。**



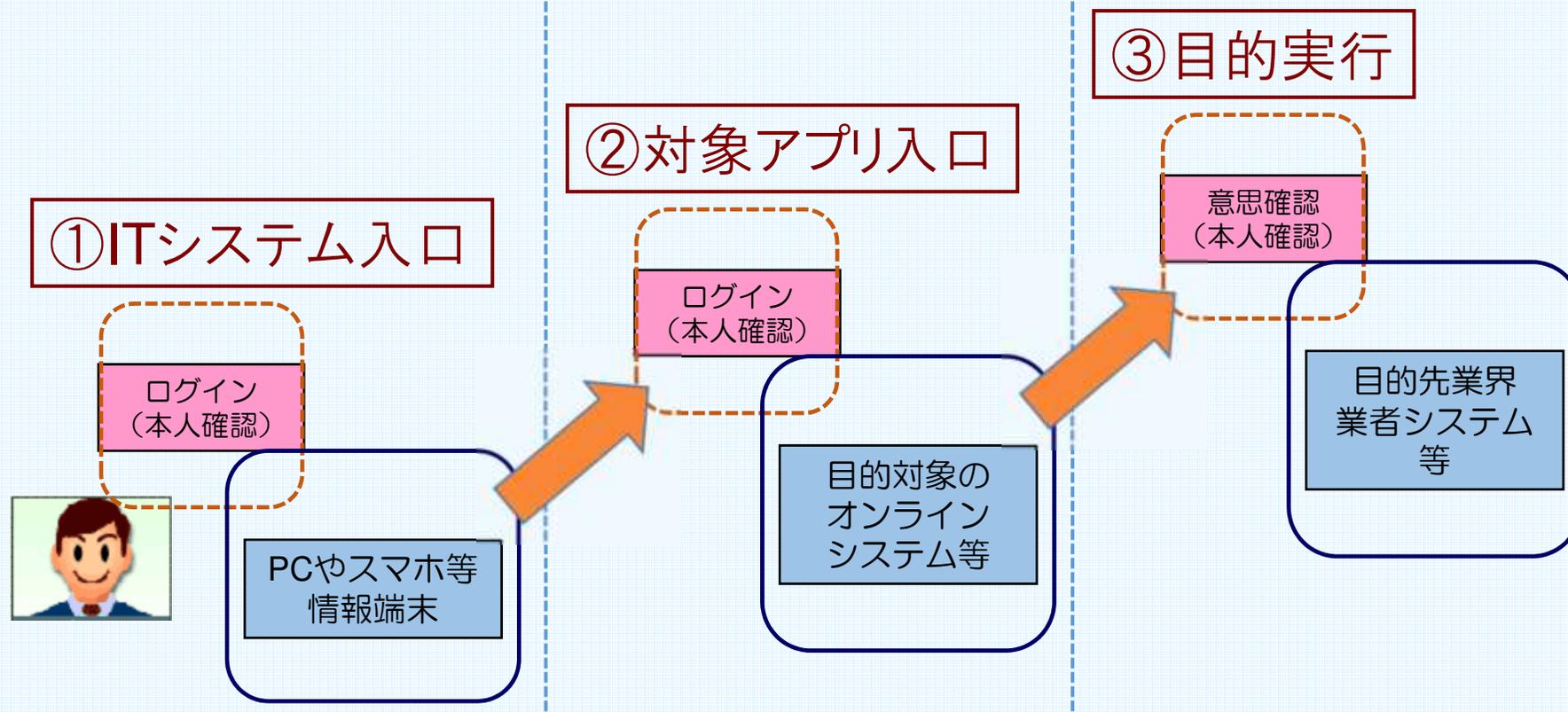
# ID/PASSや認証情報管理 —IT弱者でも簡便で安全に—

開発中スマホ割符概要説明抜粋版  
です

- ①本人確認のタイミング概念図
- ②割符なら盗まれても大丈夫
- ③今までにないセキュリティ事業
- ④開発中スマホ割符特徴

# ①本人確認のタイミング概念図

現行一般的ITサービスの場合2～3回の本人確認がある



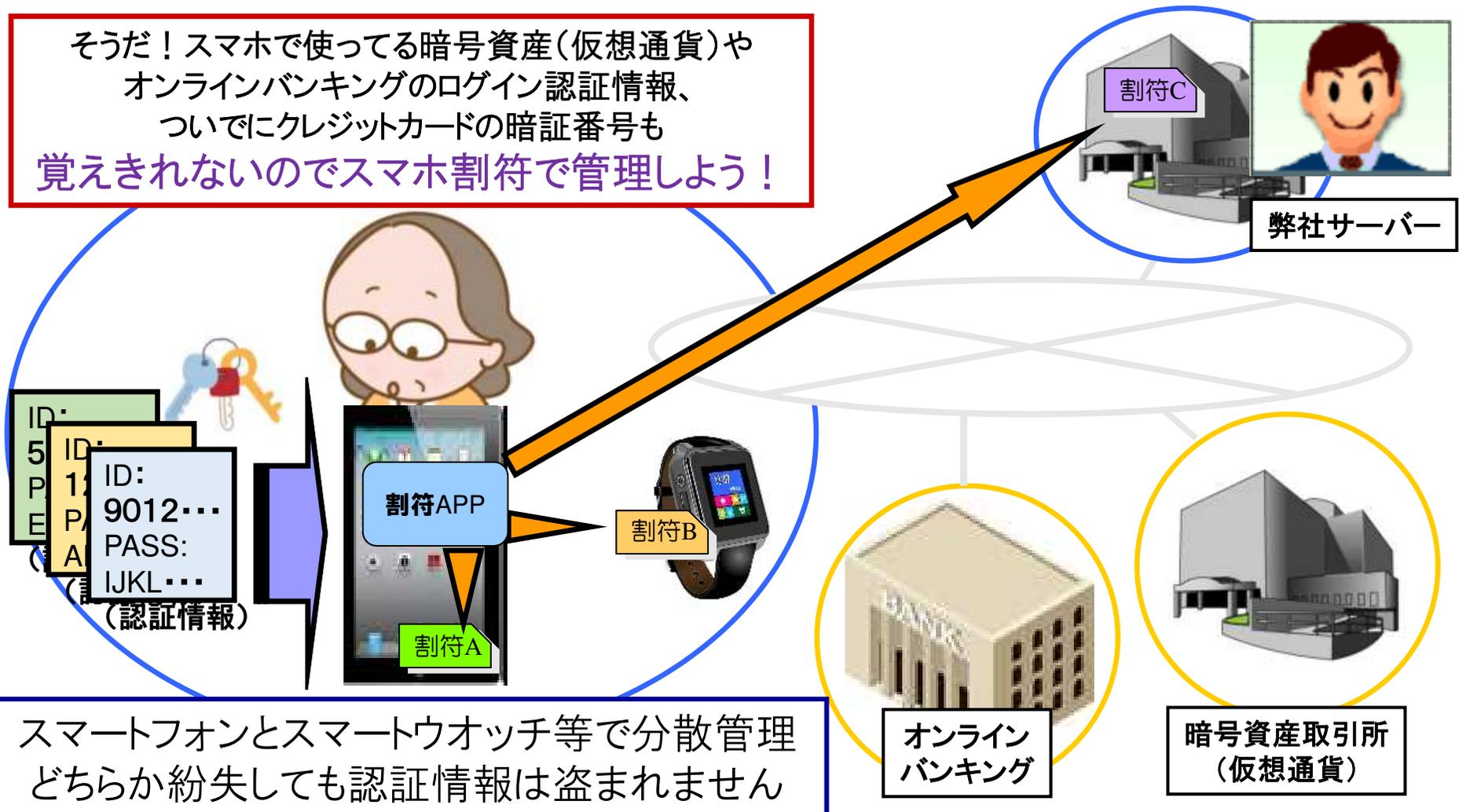
仮に2回であってもID/PASSの数は4つ。  
専用機器を用いた認証等もありますが、  
多くの場合その器機を用いる際にも本人確認があります。

## ②割符なら盗まれても大丈夫



GFIスマホ割符は機密情報を自動割符化&分散管理

そうだ！スマホで使ってる暗号資産(仮想通貨)や  
オンラインバンキングのログイン認証情報、  
ついでにクレジットカードの暗証番号も  
覚えきれないのでスマホ割符で管理しよう！



スマートフォンとスマートウォッチ等で分散管理  
どちらか紛失しても認証情報は盗られません



# 補足資料

- ①スマホ割符有識者評価抜粋
- ②スマホ割符市場供給の流れ
- ③自己情報コントロール権 **開発中スマホ割符概要説明抜粋版**  
**実現概念図** **です**
- ④電子割符利用の意義
- ⑤GFI電子割符®技術外部評価
- ⑥GFI電子割符®関連確認概要
- ⑦GFI電子割符®個人情報法等確認
- ⑧GFI電子割符®はAONTの特性も持ちますが

# ① スマホ割符有識者評価抜粋



弊社取得済特許利用

—各有識者様ご了承の下、開発中デモをご覧いただき頂戴しましたコメントの**要旨抜粋**をご紹介します—

## 弁護士 牧野剛様

タブレット、携行型情報端末の顧客情報等を割符化することは、個人情報保護法的にも一般データ保護規則(GDPR)の観点からも極めて有用であると考えます。

## 弁護士 影島広泰様

日常業務では通信環境に依存せずにデータを利用できる一方で、万が一端末を紛失したときにも情報が漏えいしないという、「いいとこ取り」のソリューションであるといえます。

さらに、例えば、データを3つの割符に分割し、うち2つの割符で復元できるよう設定しておけば、万が一端末を喪失したり破壊されたりしたとしても、残った2つの割符からデータを復元することができますので、業務継続も図ることができます。

## グローバルコンサルティングファーム パートナー 大洞健治郎様

スマホ割符のデモを拝見し、以下の点が大変画期的であると思いました。

- ①各デバイスに保存されるデータ自体は無意味化された断片となり、デバイス単体の盗難が発生しても情報を読み取られない点
- ②他のデバイスとの距離が離れることでデータが自動消去される点
- ③1つのデバイス上のデータが消失しても、他の複数デバイスのデータにより消失したデータを復元可能なセーフガードが存在する点

また、ユーザが操作を行う必要もなく、すべて自動で分割・復元処理が行われている点も素晴らしいと思います。従来のデータセキュリティやネットワークセキュリティとは異なる発想で、技術的安全管理措置と物理的安全管理措置とを融合させたソリューションと言えるのではないのでしょうか。

注1:有識者各位評価全文についてご関心のある方は、GFIまでお問合せください。

注2:本資料及び評価等は、あくまでGFI電子割符(R)に実装された技術処理による特性を根拠とするものです。

# ⑤GFI電子割符®技術外部評価

## 東京大学

電子割符セキュリティ強度調査報告書 2001年12月20日

電子割符は、秘密情報を分割して安全に伝送(または記録)する目的に開発された符号化法(およびそれを実現するためのソフトウェア)である。秘密情報である平文Sをn個の割符に分割符号化し、n個の割符が全部そろえば、平文Sが複合できるが、n-1個以下の割符からは平文Sの情報が漏れないように工夫されている。(注:通常非公開資料)

## 産業技術総合研究所(下記参考URL公開情報抜粋)

GFI電子割符(R)の安全性評価について 縫田光司 2015年11月03日

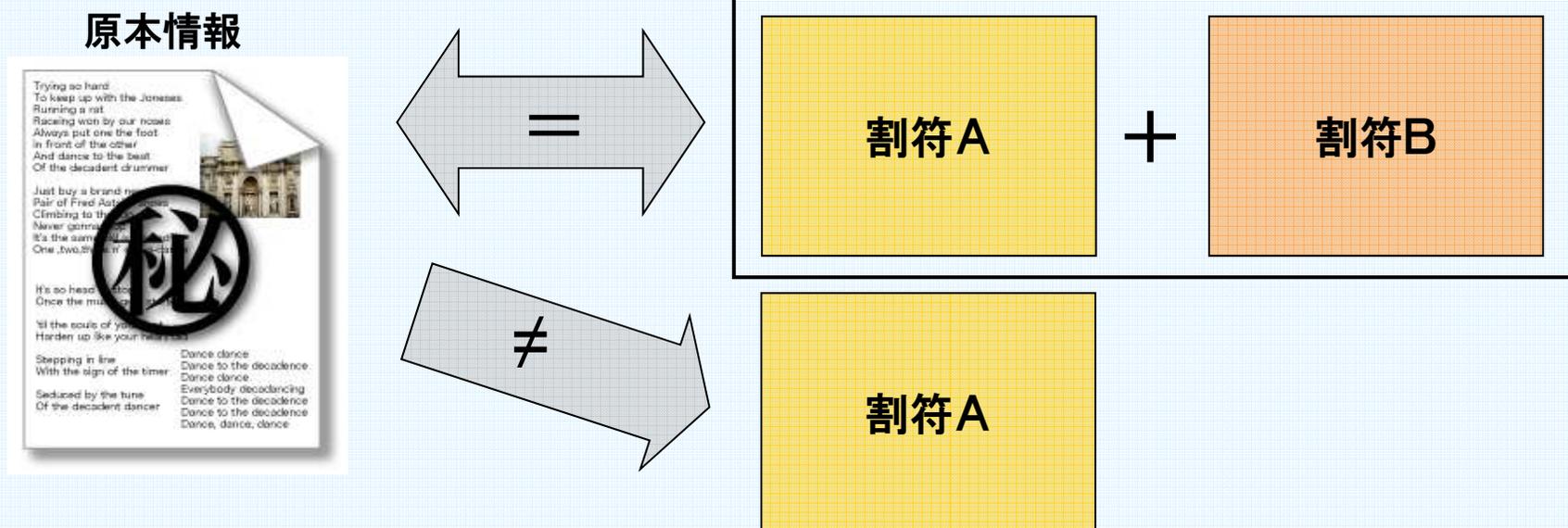
通常の暗号技術の標準的安全性レベルである「80bit安全性」では、暗号の解読が2の80乗(およそ10の24乗)通りの全数探索と同程度以上に困難であることを要求している。一方、現時点での安全性評価では、例えば、攻撃者が3個ある割符ファイルのうち一つのみを入手した状態で元データを完全に復元できる可能性について、およそ10の105,000乗通りの場合の数から正解を言い当てるのと同程度に困難であるとの見積もりを得ている。(中略)現時点での安全性評価で得られる内容に限るならば、十分な**情報理論的安全性**を持っていると考えられるレベルにある(中略)当該技術の安全性はこうした**技術標準化の検討に値する水準**にあるものと期待できると考える。

参考:「産総研様との共同研究の第二期結果概要報告」,[2015.12.26] [http://www.gfi.co.jp/01news20151226\\_393.html](http://www.gfi.co.jp/01news20151226_393.html)

注意喚起: GFIの継続した外部評価等の機能を期待する場合には、正しく「GFI電子割符®が実装されている商品・サービス」を選択ください。

# ⑧GFI電子割符®とAONT理論の関係

産総研様の「GFI電子割符(R)の安全性評価について」の調査報告の際、一部の割符の不足も許さない(n,n)型割符の場合、GFI電子割符®はAONT理論に極めて近い特性を持つので、AONT特性も踏まえた報告の打診ありましたが、



弊社技術は安全性を落とさずに(k,n)型の機能も保有しているため、利用者様の  
錯誤を未然防止すべく、AONT理論の特性を持つ記述は削除いただきました。

仮にAONT理論を安全性背景に持つ場合で、ファイル消失等に対し、  
リカバリー可能とするには、AONT理論の想定外の分割ファイルのコピー保存等  
を行なう実装が必要で、そこにセキュリティリスクが発生することが予見できます。  
厳格なn,n型に加え安全なリカバリーも可能な、GFI電子割符®をご利用ください。



<http://www.gfi.co.jp/>

GFI創業理念:「たくさんの人を幸せにしたい」