

安心・安全な社会の実現に向けた本人 認証支援ソリューション：Trust Eye

Authentication Support Solution for Realizing Safe and Secure Society:
Trust Eye

● 坂藤英昭

● 豊嶋康司

● 吉田 聡

● 宇津木利章

あらまし

近年、ICTの発展とその普及により、個人・組織を問わず情報の取得、発信、活用などの機会が飛躍的に増加している。一方で、ICTはサイバー犯罪や国際テロなどの大規模かつ組織的な犯罪のインフラとしても利用され、治安における重大な脅威となっている。こうした中、富士通では世界中から最先端のソリューションを集め、お客様に最適な組合せと運用を統合的に提供するセキュリティ製品・サービスを早くから展開している。その一つである本人認証支援ソリューションTrust Eyeは、公的身分証の偽変造検証により、なりすましや偽装などの疑いのある不審者の発見や、公的身分証の不正利用の防止を可能とするサービスである。

本稿では、Trust Eyeの製品・サービスや認証技術の概要を紹介する。更に、公的身分証の高度活用や生体認証を活用した新たなビジネス創出に向けた取組み、および今後の展望について述べる。

Abstract

The recent development and diffusion of information and communications technology (ICT) has led to a dramatic increase in opportunities for acquiring, delivering and utilizing information, regardless of whether those activities are done by individuals or organizations. Meanwhile, ICT is also used as “infrastructure” for large-scale and systematic crimes such as cyber crimes and international terrorism, posing a significant threat to public security. In this situation, at an early stage Fujitsu started offering security products and services by gathering cutting-edge solutions from around the world to comprehensively provide the optimum combination and operation for each customer. Trust Eye, an authentication support solution, is a service that makes it possible to detect suspicious individuals using a falsified identity and prevent unauthorized use of public identification (ID) by authenticating such ID. This paper outlines the Trust Eye products, services and their authentication technology. In addition, it describes activities and future outlook for creating new businesses by making use of advanced utilization of public identification and biometric authentication.

まえがき

近年、ICTの発展とその普及は、インターネットに代表されるような新たな形態の情報の流れを生み出した。これにより、個人・組織を問わず情報の取得、発信、活用などの機会が飛躍的に増加している。一方で、ICTの進歩に伴い、サイバー犯罪や国際テロにおいて、大規模かつ組織的な犯罪インフラ（犯罪を助長し、または容易にする基盤）が構築され、治安における重大な脅威となっている。

このような背景から、2013年12月に閣議決定された「世界一安全な日本」創造戦略⁽¹⁾では、2020年オリンピック・パラリンピック東京大会を視野に入れ、地域の絆や連帯の再生・強化を図るとともに、新たな治安上の脅威への対策を含め、官民一体となった的確な犯罪対策により良好な治安を確保することで、「世界一安全な国、日本」を創り上げるとしている。また、2013年4月に改正された「犯罪収益移転防止法」^{(2),(3)}においても、金融機関などの本人確認、取引記録保存、および疑わしい取引の届け出などの義務を定めたマネーロンダリング対策を強化している。

しかし、本人確認は窓口による運転免許証や旅券（パスポート）などの公的身分証の原本また

はコピーの目視確認が主体であり、本物か偽物かの真正性確認は厳密には行われていないのが実情である。また「来日外国人犯罪の検挙状況（平成26年）」⁽⁴⁾によれば、旅券や在留カードなどの公的身分証の偽変造が近年増加している。

電子商取引やクラウドソーシング、クラウドファンディングにおけるサービスアカウントの発行においても、厳正な本人確認は行われていないことが多く、偽装の容易性やサービスアカウントの脆弱性も社会問題となっている。これらのことから、現状の本人確認方法では犯罪防止対策として不十分である（図-1）。

富士通が提供する本人認証支援ソリューションであるTrust Eyeは、こうした実情に着目した。すなわち、ICTを活用した公的身分証の真正性確認による窓口業務のセキュリティ強化、セキュアなIDカード発行、および認証に関わる本人情報の安心・安全な管理といった各種サービスを実現するパッケージソリューションである。

本稿では、Trust Eyeの構成とコア技術、および新たなビジネス創出に向けた取組みについて述べる。

Trust Eyeの構成

Trust Eyeは、以下のパッケージ製品およびサー

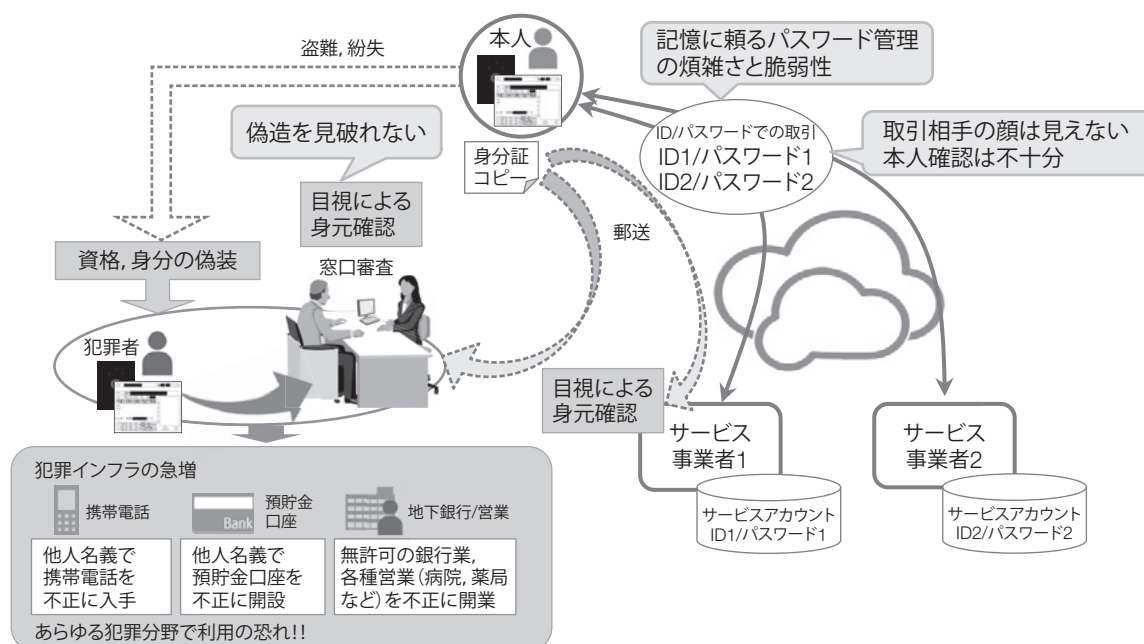


図-1 本人確認の現状

ビスから構成される（図-2）。

（1）Trust Eye for BASE

行政手続き、預貯金口座開設、携帯電話購入時など、窓口における本人確認に使用する公的身分証の真正性確認をPKI（Public Key Infrastructure：公開鍵基盤）を用いて認証し、偽変造の有無を検証するTrust Eyeのコアパッケージである。

Trust Eyeで扱える公的身分証を以下に示す。

- ・IC旅券
- ・IC運転免許証
- ・IC在留カード
- ・マイナンバー制度の個人番号カード（今後対応予定）

なお、本パッケージは、生体情報を活用したIC認証を実現する「生体IC認証」機能を有している（詳細は次章の「生体情報を活用した強じんなIC認証」を参照）。

（2）Trust Eye for ID

Trust Eyeで公的身分証の真正性を確認後、セキュアな入退出カードを発行するオプションパッケージである。

入退出カードのICチップには、生体情報と関連付けたID情報を記録しているため、本人以外の

カード利用を防止できる。なお、低コスト化したい場合は、ICチップの代わりに二次元バーコードも使用可能である。

（3）Trust Eye for GATE

セキュア入退出カードと自動ゲート装置を連携させるためのオプションパッケージである。

公的身分証で本人確認されたセキュア入退出カードとカード所持人の生体情報による厳正な本人認証を実現し、なりすましによる不正利用を防止できる。

Trust Eyeのコア技術

Trust Eyeの認証機能のうち、その特徴である二つのコア技術について解説する。

● PKIを活用した公的身分証の偽変造検証

公的身分証に組み込まれたICチップ内の電子署名を読み出し、PKIを利用して、身分情報の非改ざん性と発行者の真正性を検証する技術である。

旅券を例に偽変造検証の流れを以下に示す（図-3）。

- ①身分証に組み込まれたICチップ内のデータを読み込む。
- ②読み込んだ身分証の電子証明書を公開鍵で復号

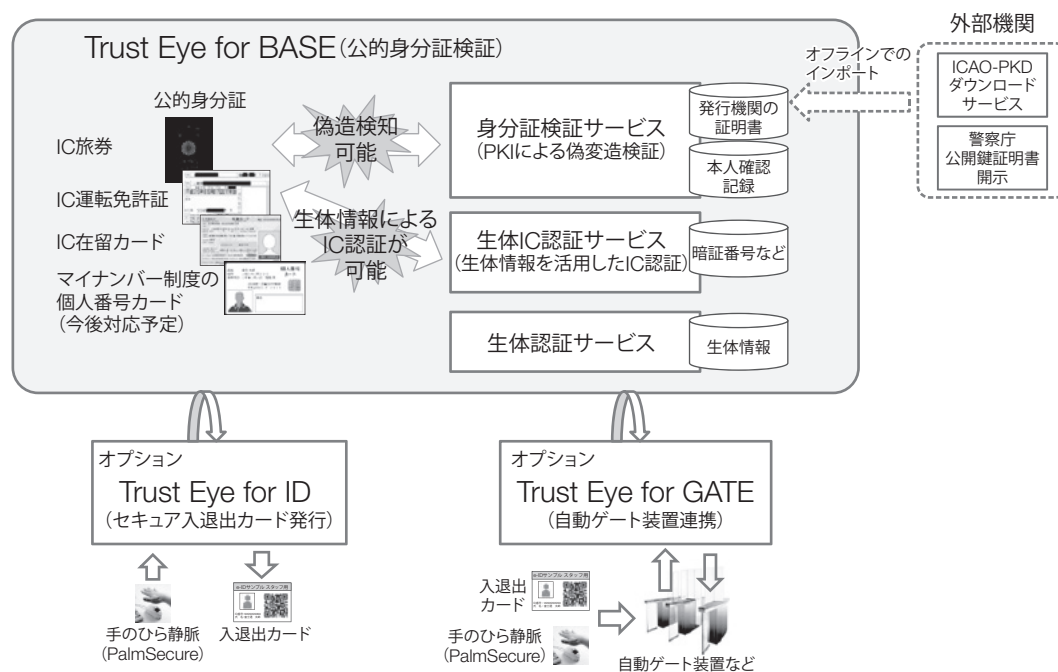


図-2 Trust Eye パッケージ製品およびサービスの構成

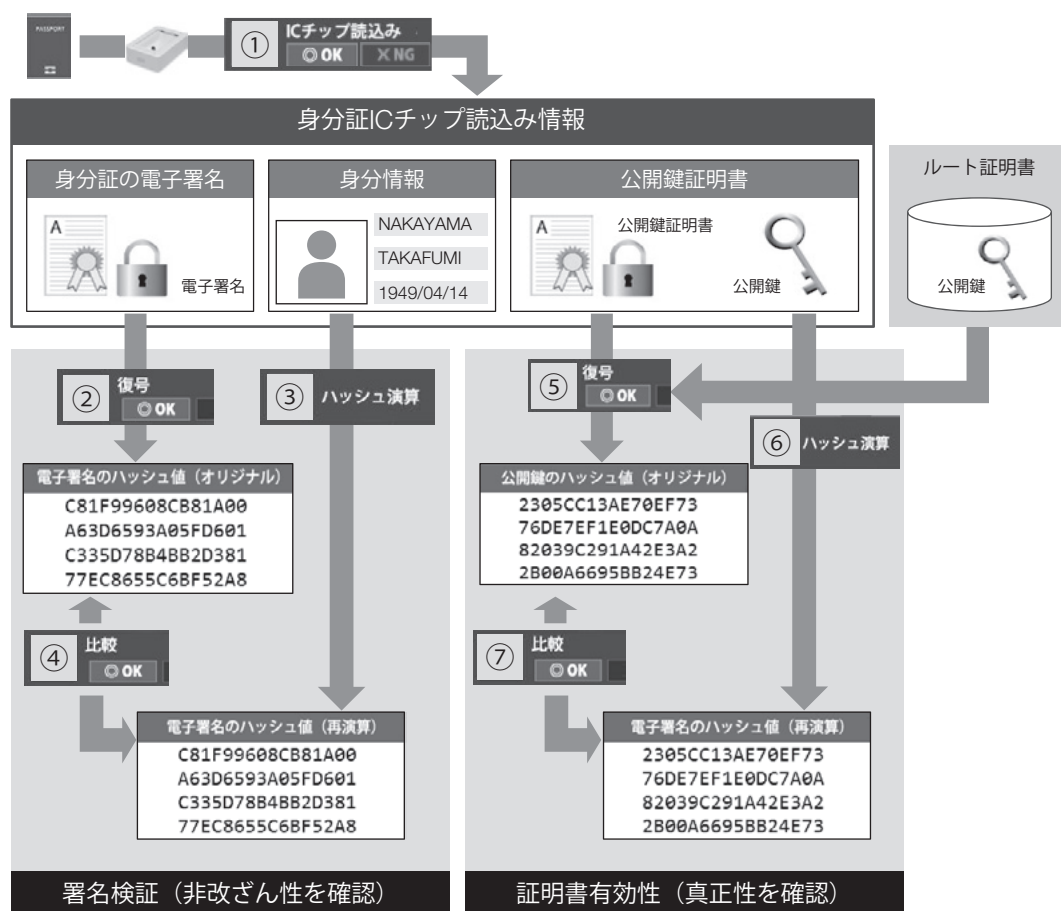


図-3 偽変造検証の流れ

し、身分情報のハッシュ値を求める。復号できない場合、電子署名に不正の疑いがある。

③読み込んだ身分証の身分情報を再度ハッシュ演算して、ハッシュ値を求める。

④②と③で求めたそれぞれのハッシュ値を比較する。ハッシュ値が一致しない場合、身分情報が改ざんされた疑いがある。

⑤発行機関より取得したルート証明書で公開鍵証明書を復号し、公開鍵のハッシュ値を求める。復号できない場合、公開鍵証明書に不正の疑いがある。

⑥公開鍵を再度ハッシュ演算して、ハッシュ値を求める。

⑦⑤と⑥で求めたそれぞれの公開鍵のハッシュ値を比較する。ハッシュ値が一致しない場合、公開鍵証明書が改ざんされた疑いがある。

公開鍵暗号方式では、秘密鍵で暗号化された情報は、秘密鍵とペアである公開鍵でしか復号でき

ないという性質を利用する。公開鍵で復号できるということは、公開鍵のペアである秘密鍵で暗号化されたものであるということである。公的身分証の発行機関において、秘密鍵を適切に管理して盗難・漏えいから守り、かつ適切な暗号強度を確保していれば、PKIによる検証で偽変造を100%見極めることができる。

● 生体情報を活用した強じんなIC認証

公的身分証のICチップ読み取り時に暗証番号（例：運転免許証のPINコード）を入力する代わりに、富士通の生体認証である手のひら静脈認証（Palm Secure）を用いる技術である。生体情報を活用した強じんなIC認証の仕組みを図-4に示す。

公的身分証を識別する管理番号に関連付けた暗証番号と生体情報の初回登録以降は、公的身分証の管理番号と所有者本人の生体情報でICチップを読み込むため、従来の暗証番号の入力は不要となる。また、暗証番号の保存・管理は、情報の所有

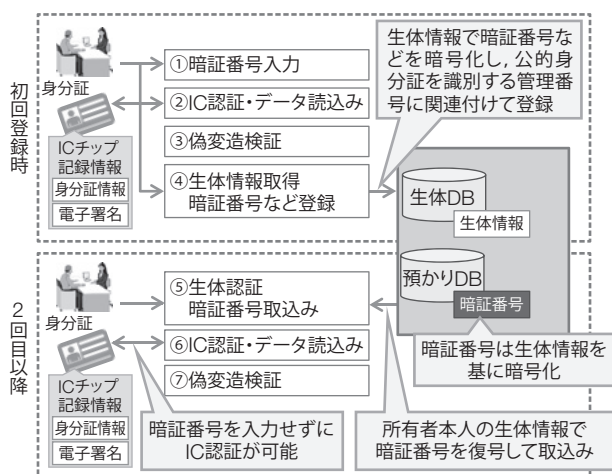


図-4 生体情報を活用したIC認証

者である本人の生体情報より生成した暗号鍵で暗号化・復号するため、安心・安全に記録・保管される。これにより、本人の記憶や記録に頼った暗証番号管理の脆弱性に対するセキュリティ強化や利便性の向上に寄与する。

図-4に沿ってIC認証の流れを説明する。

(1) 初回登録時の流れ

- ① 公的身分証のICチップの読み込みに使用する暗証番号を入力する。
- ② 入力した暗証番号でIC認証を行い、ICチップ内に記録されている各種情報を読み込む。
- ③ ICチップから読み込んだ各種情報により、公的身分証の偽変造検証を行う。
- ④ 検証に問題がなければ、身分証所有者の生体情報を取得し、生体情報から生成した暗号鍵で暗証番号を暗号化したあと、公的身分証を識別する管理番号に関連付けてデータベースに登録する。

(2) 2回目以降の流れ

- ⑤ 公的身分証所有者の生体情報による生体認証で本人認証を行い、公的身分証を識別する管理番号に関連付けられている暗証番号を復号して取り込む。
- ⑥ 取り込んだ暗証番号でIC認証を行い、ICチップ内に記録されている各種情報を読み込む。
- ⑦ ICチップより読み込んだ各種情報により、公的身分証の偽変造検証を行う。

なお、生体情報には揺らぎがあり、取得の度に同一の情報とはならないため一意性を確保できず、これまでは暗号鍵生成には利用できなかった。

Trust Eyeでは、複数登録されている同一人物の生体情報の中から、常に一意となる生体情報を検出できる仕組みを生体認証処理に実装することで問題を解決している。

ビジネスにおける利用シーン

本章では、実際のビジネスにおけるTrust Eyeの代表的な利用シーンを紹介する。

(1) 窓口業務での確実な本人確認

Trust Eyeの基本的な利用シーンであり、本人確認を必要とする窓口業務において、身元を証明する公的身分証の偽変造検証による真正性確認を行うことで、資格・身分を偽装したなりすましによる不正利用や不審者の発見を可能とし、より確実な本人確認を必要とする業務を支援する。

具体的には、以下の本人確認を行う窓口業務での利用が想定される。

- ・金融機関の窓口での預貯金口座開設
- ・通信機器販売店でのデータ通信機器・携帯電話などの契約
- ・本人確認を要するチケット購入
- ・企業などでの外国人雇用
- ・ホテル宿泊
- ・マイナンバー制度における個人番号カードの受取り
- ・郵便局などでの荷物の受取り

(2) 生体認証と連携した入退室管理

Trust Eyeのオプション機能を使用して公的身分証を活用した確実な本人確認によるセキュアなIDカード発行と、生体認証を活用した厳正な本人認証を組み合わせることで、IDカード所有者本人以外は入退出できない安心・安全な入退室管理を支援する。

具体的には、以下の本人認証を行う入退室管理での利用が想定される。

- ・スポーツイベント会場、関連施設などへの入退出（ボランティアなど）
- ・国際首脳会議会場や政府関連施設など重要施設への入退出
- ・公共施設、イベント会場などへの入退場
- ・社会インフラ施設（電力、ガス、水道など）への入退出

新規ビジネスへの取組みと期待効果

これまで述べたTrust Eyeの機能や利用シーンを踏まえ、新規ビジネスの創出にチャレンジしている。

ここでは、国際的なスポーツイベントにおけるTrust Eye導入検討と期待効果について述べる。本事例では、不特定多数かつ一時的なニーズへの対応として、国内外のボランティア、外国人訪問者への適用を検討している。

ボランティアの活用にあたっては、短期間に国内外から多数の人を受け入れ、大会を安心・安全に運営するために、受入れ時における公的身分証によるボランティア参加者の身元確認、および大会期間における生体情報を活用した厳正な本人認証を的確かつ効率的に行うシステムが求められる。Trust Eyeを導入することで、安価で確実性の高いシステムを短期間で構築できる。

外国人訪問者に対しては、入国時の登録データ、または旅券情報と生体認証を組み合わせ、日本滞在時の身分証（IDカード）を発行すれば、滞在中の保護や治安維持に役立つほか、長期宿泊やレンタルサービス、免税品などの取引における、より確実な本人確認にも活用できる。

Trust Eyeがもたらす新たな可能性

2016年1月から施行される「マイナンバー制度」

の段階的な利用拡大に伴い、行政だけでなく民間企業でも様々な取組みが必要となる。特に個人番号カードの利活用においては、行政機関や民間企業のコスト削減に加え、セキュリティリスク対策として、富士通が提唱する統合認証基盤（ID統合や生体認証データバンク）とTrust Eyeの組合せがもたらす価値は大きい（図-5）。今後も富士通内にとどまらず、行政機関や民間企業、個人に向けTrust Eyeの適用拡大を進めていく所存である。

Trust Eyeを活用した新たなビジネスの可能性について、以下で考察する。

(1) 災害発生時の行政対応

災害時において、公的身分証を紛失したり暗証番号を忘れたりした場合でも迅速に被災者の本人確認ができ、医療や救援物資の援助、被災証明書の発行やその後の管理までを正確・確実に実施できる。

(2) 公的機関における防犯対応

幼稚園、学校、病院、役所などでは、部外者による敷地内への侵入を防止することで、誘拐、盗撮などによる犯罪の防止を安価・確実に実現できる。

(3) 医療福祉分野への適応

高齢者や要介護者については、徘徊、投薬、救急搬送時の病状伝達から災害時の要援護者対応、更には年金の不正受給問題などに的確に対処できる。

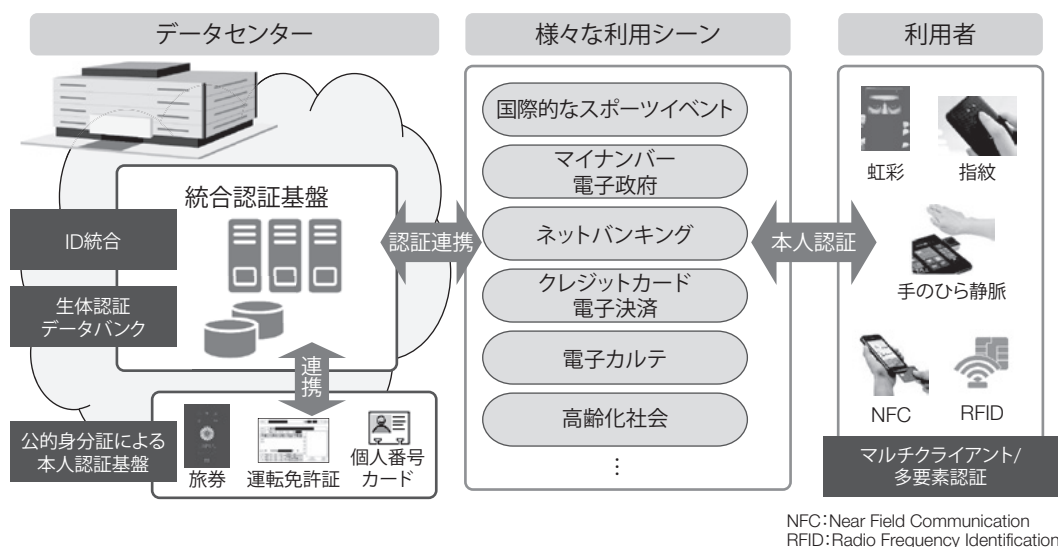


図-5 統合認証基盤が実現するスマートな社会

(4) 邦人保護の高度化

これまで国内情報とは別に管理されてきた海外の邦人情報は、外務省と自治体がシームレスに情報連携できるようになる。このため、在外における紛争時などにおいて迅速な邦人確認が可能となり、緊急脱出などの事務手続きを大幅に省力化できる。また、旅券所持の煩わしさと紛失などのリスクを軽減できる。

このように、Trust Eyeを継続的に発展させることで、様々な分野で新規ビジネスの創出が期待できる。

もちろん、こうした高度なサービスが、国や行政機関によって一元的に管理されることに懸念がないわけではない。新たなサービス提供者には、高い倫理性、公平性、公正性、更に堅牢なセキュリティなどが要求されるためである。こうした難しい要求事項を、国民の誰もが安心・安全に簡単に実現できる技術を提供することは、富士通の重要なミッションと考える。

む す び

本稿では、FUJITSU Security Initiative⁽⁵⁾における「共通/業務アプリケーション（認証、アクセス制御、ID管理）」に関連するTrust Eyeの概要、

新たなビジネス創出に向けた取組み、および今後の展望について述べた。

今後もICTを活用してより良いサービスをお客様に届け、安全で豊か、かつ持続可能な社会づくりに貢献するパッケージソリューションの開発に力を注ぎたい。

参考文献

- (1) 「世界一安全な日本」創造戦略。
<http://www.kantei.go.jp/jp/singi/hanzai/kettei/131210/honbun.pdf>
- (2) 警察庁など：犯罪収益移転防止法。
<https://www.npa.go.jp/sosikihanzai/jafic/pdf/leaf20130401.pdf>
- (3) 総務省：犯罪収益移転防止法の概要～平成25年4月1日以降の特定事業者向け資料～。
http://www.soumu.go.jp/main_content/000256683.pdf
- (4) 警察庁：来日外国人犯罪の検挙状況（平成26年）。
https://www.npa.go.jp/sosikihanzai/kokusaisousa/kokusai/H26_rainichi.pdf
- (5) 富士通：FUJITSU Security Initiative。
<http://jp.fujitsu.com/solutions/safety/security-initiative/>

著者紹介



坂藤英昭 (さかとう ひであき)

(株)富士通パブリックソリューションズ
第二ソリューション統括部 所属
現在、パッケージソリューション開発
全般および自治体ビジネスに従事。



吉田 聡 (よしだ さとし)

(株)富士通パブリックソリューションズ
現在、富士通セキュリティイニシアティブ
センターに出向中。
Trust Eyeを含むソリューションの企画・拡販に従事。



豊嶋康司 (とよしま こうじ)

(株)富士通パブリックソリューションズ
第二ソリューション統括部 所属
現在、Trust Eyeの企画・拡販に従事。



宇津木利章 (うつぎ としあき)

(株)富士通パブリックソリューションズ
第二ソリューション統括部 所属
現在、Trust Eyeなどのパッケージ
開発に従事。