IPA NEWS vol.71 3月号

「IPA NEWS」はIPAの日々の活動をわかりやすくご紹介する広報誌です。

特集 リスクをしっかり理解し、安全に使うために

官民連携でAI利活用を加速！「AIセーフティ・インスティテュート」

- セキュリティのすゝめ 20〈Windows 10のサポート終了〉
  今年10月にWindows 10がサポート終了。
  移行はお早めに！
- IPAの最新情報をまとめてお届け！
  Hot & New Topics

IPA
デジタル基盤センター
デジタルエンジニアリング部
AIシステムグループ
グループリーダー

AIセーフティ・
インスティテュート
事務局
多賀和宏さん

特集

リスクをしっかり理解し、安全に使うために

官民連携でAI利活用を加速！「AIセーフティ・インスティテュート」

AI（人工知能）はさまざまな課題の解決に役立つと期待される一方で、ビジネスに実装するうえではリスクもあります。そこで、今回は官民が連携してAIの安全安心な活用を導く「AIセーフティ・インスティテュート（AISI）」に注目。日本のAI活用の現状とリスクを整理するとともに、AISIの役割や活動内容、安全なAI活用のポイントを紹介します。

15の府省庁・関係機関で構成される政府横断の組織

昨今のAI関連技術の進展は目覚ましく、優れた情報処理能力で人間に匹敵する知的作業が可能ともいわれるほどです。質問するだけで文章の要約やアイデア出しを瞬時に行う生成AIに触れた人もいることでしょう。個人レベルでは業務の生産性向上、企業活動では新たな価値創出やビジネスモデルの再構築など、大きなメリットが期待できます。

一方で、日本ではAI導入企業は約2割にとどまり、米国の4割とは大きな開きがあります（IPA「DX動向2024」）。企業が生成AIを用いたサービスを提供することに対し、誤情報の配信や拡散を不安視する人が約4割という調査結果（JIPDEC「デジタル社会における消費者意識調査2024」注1）があるほか、事業者からも機密情報の漏えい、偽情報の業務への悪影響、倫理や著作権に背いた情報の出力などを懸念する声が上がっています（JIPDEC／ITR「企業IT利活用動向調査2024」注2）。

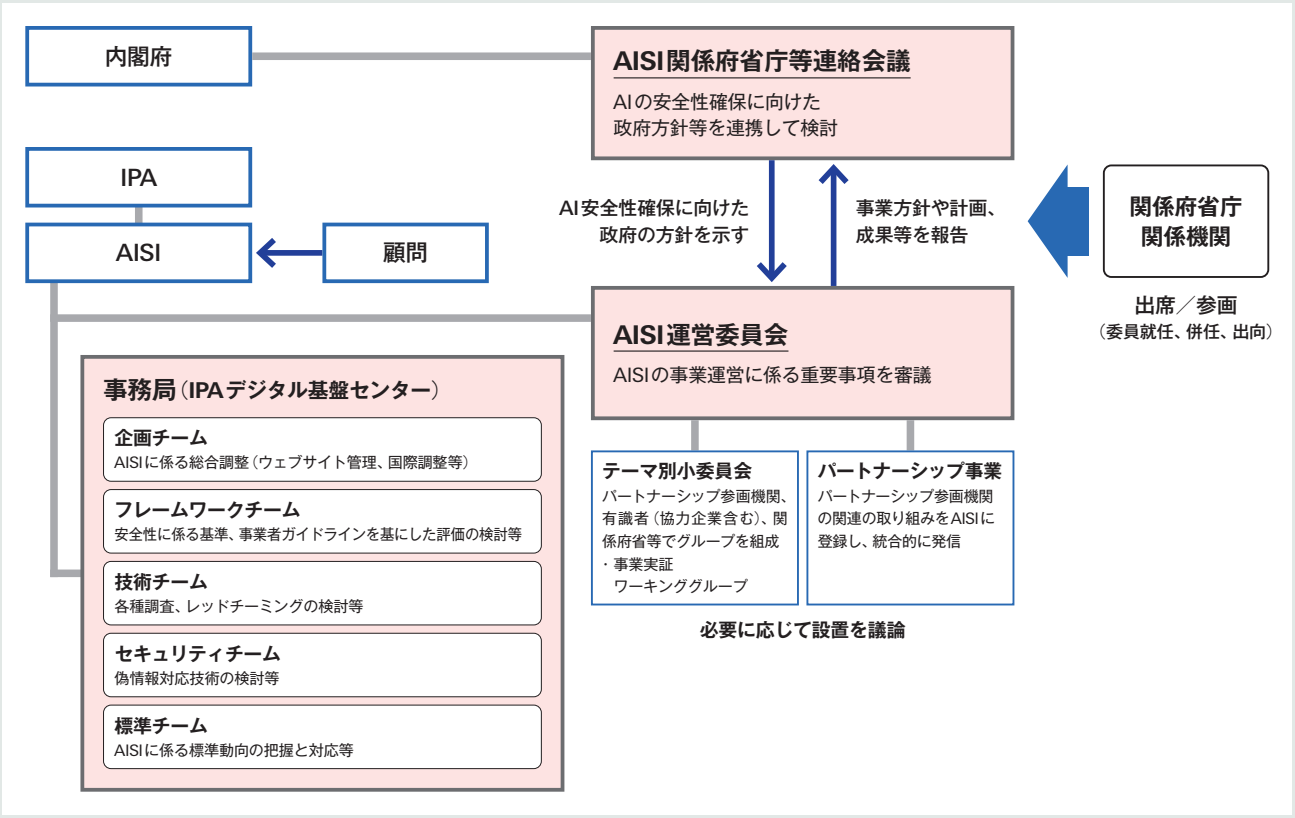
AI利活用について、こうしたリスクを低減すると同時に国際的な連携も図るべく、2024年2月に設立されたのが「AIセーフティ・インスティテュート」（以下、AISI：エイシー）です。10の府省庁と5の関係機関から成る政府横断の組織で、IPAに事務局が置かれています。AIの安全性確保を目的とした国レベルの組織としては、英国、米国に続く世界3番目の設立となりました。

AI利活用のリスクは技術面と社会面がある

IPAデジタル基盤センター AIシステムグループのグループリーダー・多賀和宏さんは、AISIの立ち上げに関わり、現在は同事務局の業務を担当しています。

AI利活用のリスクについて、多賀さんは「さまざまなものがありますが、大きくは“技術的リスク”と“社会的リスク”に分けられるでしょう」と語ります。

図表　AISIの推進体制



技術的リスクとしては、AIが間違った出力をする誤回答、学習データの偏りによるバイアスの発生、事実に基づかない情報を合成するハルシネーションなどが挙げられます。「AIのしくみはブラックボックス化しており、誤回答の原因が不明なことも少なくありません。海外では、航空会社のチャットボットが間違った割引情報を示して搭乗客に迷惑をかけた事案や、ジャーナリストが裁判の訴状をAIで要約したところ、無関係な第三者の名前が盛り込まれたといった事案が起きています」

一方、社会的なリスクとして考えられるのは、プライバシーの侵害や社会活動への悪用などです。「生成AIの画像や動画、音声の合成機能を悪用した詐欺やディープフェイク動画などの拡散が懸念されます」と多賀さん。

AIを利用するうえでこうした多様なリスクを知ることがまずは重要ですが、それと同時にリスクの根絶＝ゼロリスクにこだわる必要はないと多賀さんは説きます。

「AI技術は日進月歩で進化しており、リスクそのものも常に変化しています。こうした状況ではリスクをゼロにすることは不可能といわざるを得ません。国際規格（ISO/IEC）でも、安全の定義を“許容できないリスクがないこと”としています。つまり、許容できる程度のリスクであれば安全とみなせるということです」

リスクの種類や特性、影響を把握したうえで、そのリスクが許容できるレベルかどうかを見極め、許容できないものには適切に対応することが求められます。「AIセーフティとは、そうしたAIガバナンスのあり方を指すもの。ビジネスへのAI実装においても現実的なスタンスではないでしょうか」

安全の定義は〝許容できないリスクがないこと〟

AIの安全性評価に関わる調査や基準を定める

では、どのようなリスクならば許容範囲といえるのか。リスクをどう評価すれば安全性を担保できるのか――。これを明らかにすることがAISIの使命のひとつです。「AIの安全性評価に関わる調査や基準、評価手法などを検討し、広く社会へ提供していくべく、AISIではさまざまな課題に取り組み、すでにいくつかの成果を上げています」と多賀さん。

例えば、2024年9月に、安全性の観点を示した「AIセーフティに関する評価観点ガイド」と、攻撃者の目線でAIシステムにおける弱点を浮き彫りにして修正・堅牢化するための「レッドチーミング手法ガイド」を公開しました（両ガイドの詳細はウェブ限定記事へ）。

また、米国NIST（国立標準技術研究所）の「AIリスクマネジメントフ

レームワーク（AI-RMF）」を日本語に翻訳して公開。さらに、経済産業省と総務省が2024年4月に公表した「AI事業者ガイドライン（第1.0版）」と、AIリスクマネジメントフレームワークを比較し、対応関係を日米相互に確認する「日米クロスウォーク」の結果も公開しています。

「AI事業者ガイドライン」はAI利活用にまつわる既存の複数のガイドラインを統合し、事業者の自主的な取り組みを支援する指針を改めて示したもの。AIシステムを開発する事業者である「AI開発者」、AIシステムを製品やサービスに組み込んで事業展開する「AI提供者」、AIシステムやAIサービスを事業利用する「AI利用者」と、立場を3つに分類し、AIに関するリスクや対応方針をわかりやすくまとめているのが特徴です。

「このガイドラインの米国版ともいうべきものがAIリスクマネジメントフレームワークです。両者を比較することで、日米のAIガバナンスの相互運用性の向上に役立つでしょう。共通点は日本のガイドラインに準拠すればよいですし、相違点は米国仕様に手当てすれば、日本企業の米国展開が効率的に進められると考えました」

海外のAISIと意見交換しくみづくりでも連携

このほか、AISIではさまざまな国・地域のAIセーフティ機関との連携を進めています。「いまやビジネスに国境はありません。日本企業が海外でAI技術を展開していく場合、日本のみならずその国の基準も満たす必要があります。国ごとにルールや制度が違うと事業者の負担が大きくなるため、海外のAISIと意見交換しながらしくみづくりでも連携することは大きな意義があると考えています」と多賀さんは言います。

前述のように、米国を筆頭に各国と個別折衝を進める一方で、2024年5月のAIソウル・サミット（韓国）、11月のAISI国際ネットワーク会合（米国）などの国際会議にも積極的に参加。2025年2月にフランスで開催されるAIアクションサミットにも参加し、各国との議論や連携のさらなる活性化を期待しています。

ここで紹介したAISIの成果はいずれも下記AISIのウェブサイトで公開しています。ぜひアクセスしてみてください。

AISIでは人材を募集中。チャレンジングな環境が魅力

多賀さんは、AISIのさらなる活動の拡大に意欲を示します。

「日本におけるAIセーフティのハブとして、企業や大学・研究機関と協力し、情報集約や連携を図ることもAISIの役割のひとつ。そこで、民間企業との連携を目的とした事業実証ワーキンググループを設置し、業界特有の基準やツールづくりなど、さらに議論を深掘りしていく予定です。また、独立行政法人などとの連携強化を図るパートナーシップ事業も引き続き推進していきます」

AIの安全性について議論する中で日本のプレゼンスを高めたい

国際的な観点でも、日本のプレゼンスを高めていきたいと抱負を語ります。「AIの安全性について議論をしていく中で日本の強みを生かせるポイントを探り、明確化していきたいと考えています」

安全安心なAIの利活用に向けたサポートにAISIが力を注ぐことで、日本のAIシステムの普及・拡大が見込まれます。AI関連の技術革新や市場開拓が進めば、日本の産業の競争力強化にもつながっていくことでしょう。

「業界や業種別のAIリスク対策を確立・洗練させ、より具体的な手順まで落とし込んだ対応など、事業者の皆さんにいっそう役立つ情報発信をしていきたいですね。目の前の課題感にフィットする、より解像度の高い成果の創出を目指します」

そのためにも人材を拡充したいと多賀さん。国内外のAI利活用の最前線で、技術的な知見を生かした議論に参画できる点はAISIで働くことの魅力といえるでしょう。「グローバルに活躍したい」「AI分野で能力を発揮したい」といった人は、ぜひ注目を。

「チャレンジングな仕事ができるので興味がある方はぜひお問い合わせください。企業に在籍している方の出向も多くあります。経営者の方にとっては、人材育成の一環としてもご検討いただければ」と多賀さん。人材募集は下記AISIウェブサイトで行っています。

注1　https://www.jipdec.or.jp/news/pressrelease/20240418.html
注2　https://www.jipdec.or.jp/news/pressrelease/20240315.html

- **【ウェブ限定記事】AISIが公開している「評価観点ガイド」と「レッドチーミング手法ガイド」の詳細はこちら…**
  https://www.ipa.go.jp/about/ipanews/ipanews202503.html#specialissue_weblimited
- **AISIのウェブサイトはこちら…**
  https://aisi.go.jp/

そのまま使っているとセキュリティリスクが増大！

今年10月にWindows 10がサポート終了。移行はお早めに！

一部製品はサポート継続。使用OSの種類をチェック

2025年10月14日（米国時間）、マイクロソフト製OS「Windows 10」のうち、「Home and Pro」「Enterprise and Education」「IoT Enterprise」がサポート終了を迎えます（一部製品を除く。詳しくはウェブ限定記事へ）。

サポート終了後はOSのセキュリティ更新プログラムが提供されず、セキュリティのリスクが増大するため、後継製品や代替製品への移行が欠かせません。また、OS上で動くサードパーティ製ソフトウェアもサポート終了が見込まれるので、それらも併せて対処しましょう（図表を参照）。

まず自分が使っているOSの種類を確認し、サポート終了対象製品であれば後継製品や代替製品への移行を計画し、サポートが終了するまでの間に移行しましょう。その際は個人・企業それぞれで行う対策があります。個人で行う対策は以下のとおりです。

①端末スペックの再確認……使用端末が後継や代替のOSに対応できるか確認しましょう。例えばWindows 11に移行する場合、CPUやメモリ、ストレージ以外にもさまざまなシステム要件が必須とされ、注意が必要です（詳しくはウェブ限定記事へ）。

②ソフトの対応性の確認……OS上で使用しているソフトウェアについても後継や代替のOSで動作するか確認を。また、後継OSをWindows 11とする場合、インターネットエクスプローラーやワードパッドなど一部機能が廃止されるので、そうした点も留意しておきましょう。移行時のアクシデントに備えてデータのバックアップを取ることもお勧めです。

旧端末を廃棄する際は情報漏えいに万全の注意を

次に企業で行う対策です。

①余裕を持った移行計画の策定……予算の確保に時間がかかったり、サポート終了直前は買い替え需要に供給が追いつかなかったりすることも懸念されます。予算措置と併せて余裕のある調達スケジュールを検討しましょう。

②社内周知……OSの移行について社内の利用者へ早めに周知し、混乱を最小限に抑えましょう。

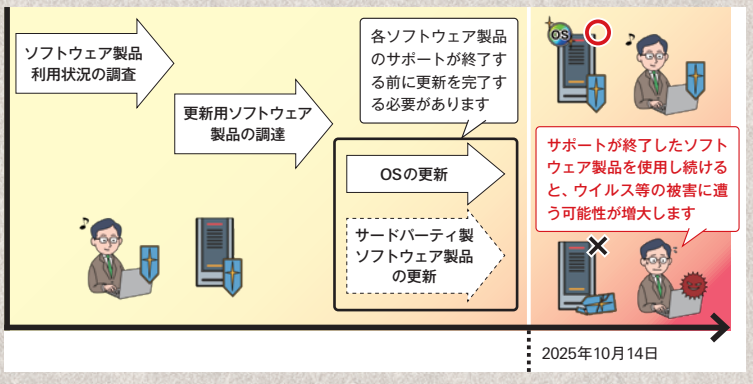
③端末スペックの再確認……個人向けの対策と同様です。情報システム部門だけでなく、事業部門で調達した端末も漏らさず確認してください。

④ソフトの対応性の確認……情報システム部門だけでなく、事業部門で導入したソフトウェアも確認を。特に社内システムや独自開発のソフトウェアは、OSのアップグレードやブラウザの変更により正常に動作しなくなるおそれもあるため注意が必要です。

⑤端末の廃棄……端末の更新後、旧端末を廃棄する際は情報漏えいのないよう十分配慮しましょう。削除ツールによる完全削除やストレージの物理破壊など、対策の徹底が求められます。

個人、企業のいずれもサポート終了直前に慌てることのないよう、余裕を持った移行の計画を立てることを心がけてください。

Windows 10のサポート終了に向けた各種ソフトウェア製品の更新計画例



＋ 対策のポイント ＋

1. サポート終了OSはセキュリティリスクが高いため後継・代替製品へ移行
2. 移行では端末スペックやソフトの対応性を確認
3. 余裕ある移行計画を立て、早めの準備を心がける

- 【ウェブ限定記事】Windows 10のサポート対応製品と後継OS移行時の留意点はこちら
  https://www.ipa.go.jp/about/ipanews/ipanews202503.html#security_weblimited
- Windows 10のサポート終了に伴う注意喚起についてはこちら
  https://www.ipa.go.jp/security/security-alert/2024/win10_eos.html

IPAの最新情報をまとめてお届け！

Hot & New Topics

DX先進事例をスマートに検索できるサイトを公開

デジタルトランスフォーメーション（DX）の事例を効率的に検索、閲覧できるウェブサイト「デジタル事例データベース」を公開しました。

本データベースでは、「DX銘柄選定企業レポート」などに掲載された100以上の事例を閲覧できます。業種や事業規模、所在地のほか、取り組み理由、取り組み内容、結果などデータ項目を揃えた形で事例データを保持しているため、ご自身の組織が参照したい項目をキーにして事例を探したり、比較したりすることができます。今後も事例を随時掲載し、企業や組織の皆様からの投稿依頼も受け付けていきます。

参考になりそうな先進事例を見つけて、DXをスマートに進めませんか？

https://case-studies.ipa.go.jp/

●「デジタル事例データベース」の画面

制御システムに対するリスク分析の事例を公開

制御システムは、重要インフラや産業システムの基盤となるシステムです。これまでは外部ネットワークから隔離された構成が一般的でしたが、近年では、生産性や品質などの向上のため、制御システムが外部サービスに接続する事例が増えています。そこで今回は新たに、外部サービスから攻撃者が制御システムに侵入する脅威を想定してリスク分析を行った事例を公開しました。

本事例は「制御システムのセキュリティリスク分析ガイド」の別冊として「事例2：社外サービスと接続した制御システムに対するリスク分析」と題して公開中です。事業者の皆様、本事例を参照してリスク分析に取り組んでみませんか？

https://www.ipa.go.jp/security/controlsystem/riskanalysis.html

●「事例2：社外サービスと接続した制御システムに対するリスク分析」

未踏会議2025 MEET DAYを開催します

3月9日(日)に、「未踏会議2025 MEET DAY」を東京ミッドタウン・ホールで開催します。突出したIT人材の発掘・育成事業として2000年にスタートした未踏事業。その魅力を多くの人に伝える年次イベントである「未踏会議」は今回で11回目の開催となり、未踏修了生たちによる50以上もの展示ブースや、トークセッションなどを用意しています。

今回は第一線で活躍する未踏修了生と吉本興業の芸人さんが共演し、生成AIや量子コンピューティングといった最新技術をテーマにトークを繰り広げます。未踏事業を楽しく知っていただく本イベントに、ぜひご来場ください。

https://www.ipa.go.jp/jinzai/mitou/mitoukaigi/

● 未踏会議2025 MEET DAY

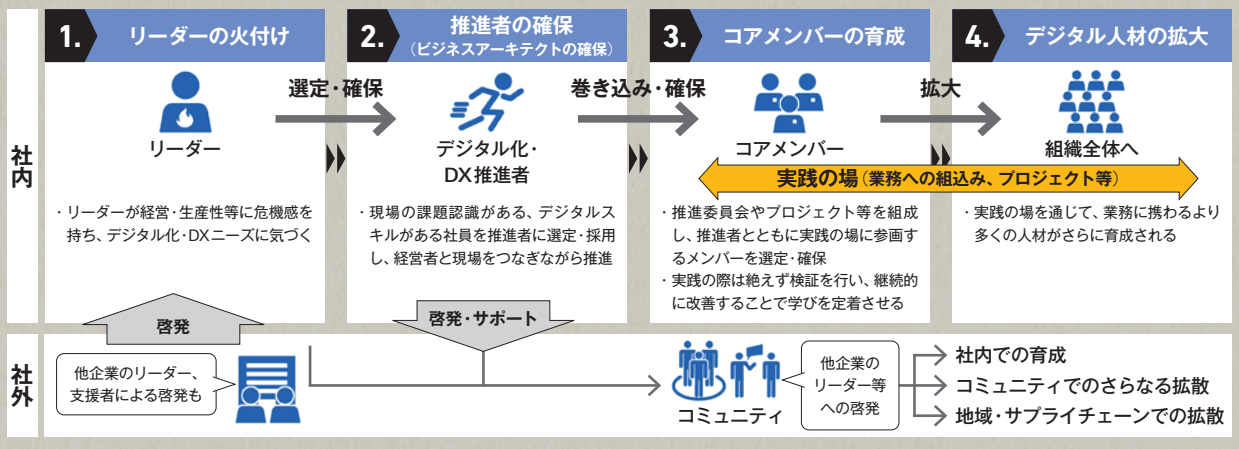
Just Information

「デジタル人材育成モデル」のご紹介

デジタルトランスフォーメーション(DX)を推進する企業はデジタル人材をどのように確保し、育成しているのでしょうか。IPAでは複数の企業に取り組みの全体像についてヒアリングし、共通する部分を抽出してモデル化した「デジタル人材育成モデル」を公開しています。

本モデルでは、デジタル化・DX推進において、主にビジネスアーキテクト(BA)の役割を担う人材を内部で育成・確保することが重要とし、実務を通じたデジタル人材育成の進め方を、図のとおり4ステップで示しています。デジタル人材育成をこれから進める企業の皆様に、ぜひご活用いただければ幸いです。

https://www.ipa.go.jp/jinzai/skill-transformation/model.html



発行日　令和7年3月

独立行政法人情報処理推進機構
〒113-6591 東京都文京区本駒込二丁目28番8号　文京グリーンコートセンターオフィス

URL●https://www.ipa.go.jp/

目指せ！ 情報処理のエキスパート!!

国家試験に挑戦！ ～ITパスポート試験編～

ITパスポート試験（iパス）は、IT社会で働くすべての社会人が備えておくべきITに関する基礎的な知識が証明できる国家試験です。

問1　ストラテジ系【令和6年度・問34】

顧客の特徴に応じたきめ細かい対応を行うことによって，顧客と長期的に良好な関係を築き，顧客満足度の向上や取引関係の継続につなげる仕組みを構築したい。その仕組みの構成要素の一つとして，営業活動で入手した顧客に関する属性情報や顧客との交渉履歴などを蓄積し，社内で共有できるシステムを導入することにした。この目的を達成できるシステムとして，最も適切なものはどれか。

ア　CAEシステム　　**イ**　MRPシステム　　**ウ**　SCMシステム　　**エ**　SFAシステム

問2　マネジメント系【令和6年度・問40】

アジャイル開発に関する記述として，最も適切なものはどれか。

ア　開発する機能を小さい単位に分割して，優先度の高いものから短期間で開発とリリースを繰り返す。
イ　共通フレームを適用して要件定義，設計などの工程名及び作成する文書を定義する。
ウ　システム開発を上流工程から下流工程まで順番に進めて，全ての開発工程が終了してからリリースする。
エ　プロトタイプを作成して利用者に確認を求め，利用者の評価とフィードバックを行いながら開発を進めていく。

問3　テクノロジ系【令和6年度・問94】

企業において情報セキュリティポリシー策定で行う作業のうち，次の作業の実施順序として，適切なものはどれか。

a　策定する責任者や担当者を決定する。
b　情報セキュリティ対策の基本方針を策定する。
c　保有する情報資産を洗い出し，分類する。
d　リスクを分析する。

ア　a→b→c→d　　**イ**　a→b→d→c
ウ　b→a→c→d　　**エ**　b→a→d→c

正解：問1 エ　問2 ア　問3 ア

IPAとは

**独立行政法人情報処理推進機構（IPA）は、経済産業省所管の政策実施機関です。
デジタル基盤の構築・提供、デジタル人材の育成、
サイバーセキュリティ対策の普及促進などの事業に取り組んでいます。**

●「IPA NEWS」最新号の公開をお知らせするメール配信サービスをご提供しています。お申込み、配信先の変更・配信停止につきましてはウェブページをご覧ください。

IPAニュース　検索

https://www.ipa.go.jp/about/ipanews/index.html

●「IPA NEWS」アンケートはこちら

IPA 独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan

VEGETABLE OIL INK
リサイクル適性Ⓐ この印刷物は、印刷用の紙へリサイクルできます。
R70 古紙パルプ配合率70％再生紙を使用