IPA news

vol.47
7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

サプライヤー&カスタマーの「良きパートナー」になる！

サクサク導入、バッチリ対策。中小企業の「IT」基本のキ

- データで読むITの今・未来
  SECURITY ACTION に大半の企業が信頼向上を期待
- IPAの最新情報をまとめてお届け！
  Hot & New Topics
- 目指せ！ 情報処理のエキスパート!!
  国家試験に挑戦！ ～情報セキュリティマネジメント試験編～

特集

サプライヤー&カスタマーの
「良きパートナー」になる！

サクサク導入、バッチリ対策。中小企業の「IT」基本のキ

中島康明さん

中小企業基盤整備機構経営支援部長。中小企業のIT化をあらゆる面からサポート。経営課題解決を情報提供、相談・診断、計画・立案、実行と4段階で支援。ウェブサイトから自社に適した問題解決アプリが見つけられる「ここからアプリ」が好評。https://ittools.smrj.go.jp/

江島将和さん

情報処理推進機構（IPA）セキュリティセンター企画部中小企業支援グループ研究員。「中小企業の情報セキュリティ対策ガイドライン」の改訂や「SECURITY ACTION」創設を担当。情報処理安全確保支援士実践講習講師／大学院講師／中小企業診断士

中小企業の代表的な課題は、「IT導入の遅れ」と「セキュリティ対策の甘さ」の2つ。これらの課題に万全の対策を講じる企業は、サプライヤーやカスタマーからも選ばれます。そのためのアプローチを探っていきましょう。

なかなか進まぬIT化とセキュリティ対策

「中小企業白書2018」によると、中小企業のITツールの利用状況は、Word、Excelなどの一般的なソフトでさえ十分利活用していると答えた企業はわずか6割弱。電子メールが5.5割、給与・経理業務のパッケージソフトが4割にとどまっています。この理由と対策について、中小企業基盤整備機構経営支援部長の中島康明さんはこう話します。

「中小企業の場合は、資金、人材不足によりITの導入が進んでいません。しかし今後、雇用の確保、コスト削減、売上の拡大のためにはITは不可欠です。そのためわれわれは、中小企業に対して、情報提供→相談・診断→計画・立案→実行と4段階でのキメの細かいサービスで、IT導入のサポートを行っています。最近では、『ここからアプリ（https://ittools.smrj.go.jp）』をリニューアル。課題を入力すると自社に有効なアプリが容易に探せるシステムも導入しました」

IT導入を進めている中小企業の中でも、特に対策が遅れているのが情報セキュリティ関連です。とはいえ、情報セキュリティについての意識が低いということではないと言います。

「中小企業は人的にも資金的にもギリギリのコストで会社を運営しています。業務に直接関係のない、お金を生まない分野にはコストをかける余裕がないため、どうしても情報セキュリティ対策は後回しになってしまうのです」（中島さん）

近年、情報セキュリティの重要性が叫ばれていますが、そもそもなぜセキュリティ対策が必要なのでしょうか。IPAセキュリティセンター企画部中小企業支援グループの江島将和さんは、大きく3つの必要性を指摘します（図表①参照）。

図表①　対策が必要な3つの理由

1. 脅威の増大

近年、セキュリティ犯罪が凶悪化し、ランサムウェアやビジネスメール詐欺など、金銭を狙う攻撃が増えている。

2. 社会的要請・法的責任の拡大

法律整備によって、対策を怠り、マイナンバー法や個人情報保護法などに違反すると法的に処罰されるようになった。

3. 取引先からの要請

委託先企業を踏み台にして発注元を狙う手口が頻発しているため、対策が甘い中小企業が選ばれなくなる恐れがある。

図表②　セキュリティ対策3つの落とし穴

1. 従業員任せ	現場のITに詳しい社員が気を利かせて対策を実施しているため、全社的に対策が進まないケースが散見。しかし本来は、人員や予算を適切に割り振るなど、経営者がリーダーシップをとるべき領域である。
2. 作りっぱなしで見直さない	セキュリティ対策のルールを作成したことで満足して、不便なルールであっても見直すことなく運用し続けている。サイバー攻撃の手口は日々進化していることもあり、対策ルールは適宜、見直すべきである。
3. 委託先の監督不備	自社では対策には取り組むが、委託先での対策は委託先任せ。しかし、委託先から情報漏えいすれば、委託元として監督責任を問われることになる。神奈川県庁の委託先でHDDが転売された事件は記憶に新しい。

「情報漏えいなどセキュリティ事故を起こすと、社会的信用の低下や顧客の喪失につながり、ひいては会社の存続自体が危ぶまれます。ゆえに、中小企業だからといって情報セキュリティ対策は必要ないとは言えません」

中にはサイバー攻撃の脅威を理解し、セキュリティ対策に乗り出している中小企業も存在しますが、自社だけではなかなかうまくいかないのが現状です。江島さんは、中小企業が陥りやすい落とし穴として「従業員任せ」「作りっぱなしで見直さない」「委託先の監督不備」の3つがあると話します（図表②参照）

セキュリティ事故の最新事情と最新手口

では現在、どのような情報セキュリティ事故が起こっているのでしょうか。

「ある会社で外部への不正な通信を検知し、サイバー攻撃が疑われました。実際に駆けつけて調べたところ、社員がウイルスに感染した自分のスマホを会社の無線LANに接続したことをきっかけに、外部との不正通信を行っていたことを突き止めました」（江島さん）

江島さんが図表①で指摘した通り、サイバー攻撃の手口は日々進化、巧妙化していることがわかるエピソードです。日常的に社員が個人スマホを会社に持ち込み、会社のWi-Fiに接続、使用しているというケースは少なくないでしょう。そうした職場では、どう対処すればいいのでしょうか。

「会社のセキュリティポリシーとして、個人スマホの接続の可否を決める必要があります。接続不可の場合は、社員に説明し、システム的に制限をかけます。接続可能な場合は、接続にあたってのルールを周知します」（江島さん）

江島さんによると、この事例はIPAが昨年から始めた「サイバーセキュリティお助け隊」で発見、対処したケースだといいます。この「お助け隊」とは、どのような施策なのでしょうか。

「『サイバーセキュリティお助け隊』とは、中小企業のサイバーセキュリティに関する悩みや、対策のニーズ、サイバー攻撃被害の実態を把握するとともに、サイバーインシデントが発生した際の地域における支援体制の構築などに向けた実証事業です」（江島さん）

2019年度は全国19府県8地域で実証実験的に実施し、1,064社の中小企業が参加、このうち727社にセンサーを設置して外部からのサイバー攻撃の観測を行いました。その結果、128件のインシデントを検出し、実際に攻撃を受けて情報漏えいが疑われる18社の中小企業に駆けつけ、支援を行いました。

「この事業を通して見えてきたのは、サイバー攻撃を受けている事実に気づいていない会社が多いということ。『ウチはサイバー攻撃なんてされてない』と油断する会社は多いのですが、そもそも攻撃を検知する仕組みがないから気づかないし、機器を設置していたとしても、社内に詳しい人がいないと使いこなせず、攻撃かどうか分析できません。お助け隊事業に参加することで初めてサイバー攻撃に気付き、情報セキュリティ対策の必要性を身をもってご理解いただいた会社も多くありました」（江島さん）

このほかIPAでは、セキュリティの専門家を派遣してセキュリティポリシー作りを支援するセキュリティマネジメント指導事業も行いました。

「この2つの事業は今年度（2020年度）も継続する予定です。経費の問題とともに、セキュリティ人材の不在で情報セキュリティ対策に踏み切れなかったという中小企業は、ぜひ活用していただきたいですね」（江島さん）

「SECURITY ACTION」で社会的信頼アップを！

情報セキュリティ対策の重要性は理解できたけれど、どこから手を付ければいいのか、どこまでやればいいかがわからないという中小企業も多いでしょう。そんな企業のため、IPAではセキュリティ対策自己宣言制度の「SECURITY ACTION」の活用を推奨しています。費用は一切かかりません。

「これまでセキュリティ対策に全く手を付けていなかったという中小企業でも、できるところから始めて一つ星→二つ星と段階的にステップアップできるような仕組み

一度のセキュリティ事故で会社の存続自体が危ぶまれる

図表③　SECURITY ACTIONと情報セキュリティ自社診断

SECURITY ACTIONは2段階の取り組み目標を用意。1段階目の「一つ星」は、1.OSやソフトウェアは常に最新の状態にしよう！ 2.ウイルス対策ソフトを導入しよう！などを含む「情報セキュリティ5か条」に取り組むことを宣言。2段階目の「二つ星」は、「5分でできる！情報セキュリティ自社診断」（画像）で自社の状況を把握した上で、「情報セキュリティ基本方針」を定め、外部に公開したことを宣言する。

SECURITY ACTION
セキュリティ対策自己宣言

SECURITY ACTION
セキュリティ対策自己宣言

になっています（図表③参照）。宣言企業は順調に増え、現在では9万件を超えています」（江島さん）。

中島さんも「アイデアとしてとてもユニークな取り組み。簡単でわかりやすいし、無料だから取り組みやすいという点が素晴らしい。あとは取り組むことで得られるメリットが認知されればさらなる拡大が期待できます」と評価しています（※SECURITY ACTIONのメリットや期待に関してはP.5を参照）。

IPAの施策を利用してセキュリティアップを！

車の両輪としてIT化とセキュリティ対策を推進

中小企業では生産性向上やさまざまな経営課題解決のほか、新型コロナウイルスの影響によるテレワークやオンライン会議の増加などを受け、今後ますますITやIoTの導入を迫られるでしょう。

「われわれとしても、ITの導入・活用を強力に支援しているところですが、同時にサイバー攻撃の危険性や情報セキュリティ対策の重要性についても周知する必要に迫られています。しかし具体的対策については専門外。だからこそ、セキュリティ関係に膨大な知見とノウハウを持つIPAとともに、車の両輪のように、中小企業のIT化とセキュリティ対策を迅速に進めたいと考えています」（中島さん）

情報セキュリティ対策にお悩みの企業は、SECURITY ACTIONやお助け隊などが心強い味方となります。ぜひ活用しましょう。

SECURITY ACTIONを活用した企業の声

リカザイ株式会社（製造業／一つ星宣言）　経営管理統括部長　**有賀成一**さん／管理部総務課　**石沢真樹子**さん

――なぜ活用しようと思ったのですか？

まずお客様から、情報セキュリティ対策をしているか、確認の問い合わせがあったこと。また、過去にサイバー攻撃を受け、当社のウェブサイトが改ざんされたことも大きいです（有賀さん）

――具体的にどのような対策を実施しましたか？

もともと社長と私でセキュリティ管理の下地は整備できていたので、一つ星の条件の「5か条」はほぼ全部満たしていました。ですので1ヶ月程度で一つ星のマークをダウンロードできました（石沢さん）

―― SECURITY ACTION活用のメリットは？

新しく導入したファイヤーウォールのおかげでサイバー攻撃をブロックできていること。また、社員の情報セキュリティの意識が向上したことを実感しています。さらに、当社は情報セキュリティに対してしっかり取り組んでいるというPRになることが大きなメリットですね（有賀さん）

――今後はどのような取り組みをする予定ですか？

IPAからいただいたDVDを教材として、社員に情報セキュリティの重要性や具体的な対策について説明しているのですが、今後は定期的に実施していこうと思っています（有賀さん）

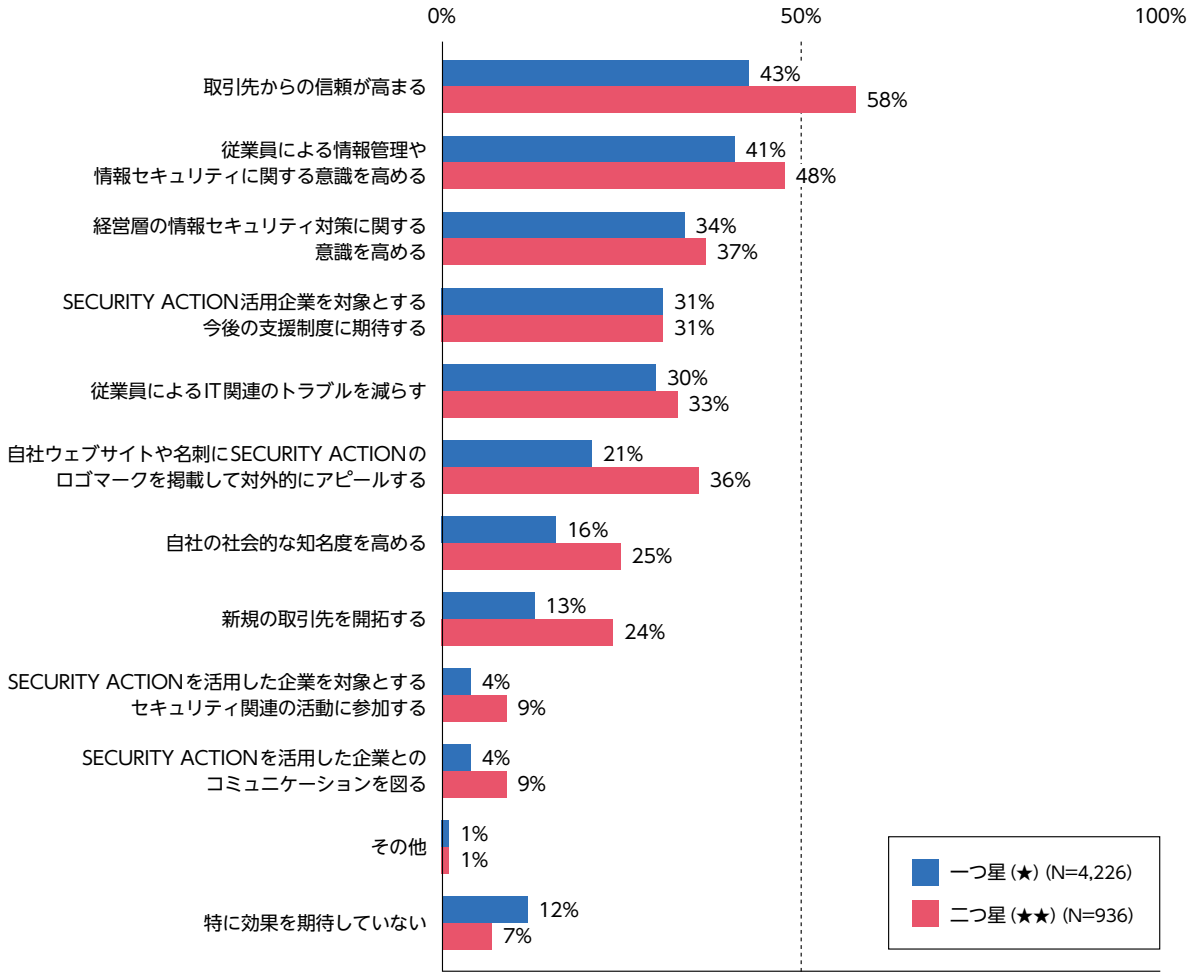
サイバー攻撃の手口は年々悪質化、巧妙化しています。最近はコロナ対策でオンラインツールの使用機会も増えましたし、一つ星宣言で終わりにせず、常に対策を続けていこうと思っています（石沢さん）

SECURITY ACTIONに大半の企業が信頼向上を期待

SECURITY ACTIONを活用する企業は9万社。期待する効果は「取引先からの信頼」が1位。社内の情報セキュリティ意識の向上にも期待。

※SECURITY ACTION宣言事業者数96,365件（一つ星83,628件、二つ星12,737件）2020年6月11日時点
※「2018年度 SECURITY ACTION宣言事業者における情報セキュリティ対策の実態調査」報告書の掲載データをもとに編集部で作成

取り組み目標別 SECURITY ACTIONに期待する効果



「SECURITY ACTION で自己宣言をしたことで、どのような効果を期待しているか」を「取り組み目標」別にみると、二つ星は一つ星と比べ、ほとんどの項目において、効果を期待している割合が高い。特に、「取引先からの信頼が高まる」、「新規の取引先を開拓する」、「自社の社会的な知名度を高める」、「SECURITY ACTION のロゴマークを掲載して対外的にアピールする」の割合の差が大きく、対外的な効果を期待していることがうかがえる。

SECURITY ACTIONの活用で、対外的な信頼度と社内セキュリティ意識の向上を図りましょう！

IPAの最新情報をまとめてお届け！

HOT & NEW TOPICS

IPAとNTT東日本が「シン・テレワークシステム」を無償開放

新型コロナウイルスに関する政府の緊急事態宣言や在宅勤務への社会的要請を受け、IPAとNTT東日本は、今年4月にシンクライアント型VPNテレワークサービスの実証実験システム「シン・テレワークシステム」を共同で構築しました。

本システムは、多くの方々が同時に、かつ迅速にテレワークシステムを利用できるようにするためのもので、専用ソフトウェアをインストールすることで自宅のパソコンから職場などで使用するパソコンのデスクトップ環境の操作を可能にします。リモートデスクトップ接続は、暗号化された通信経路であるSSL-VPNを用いているためセキュリティ面でも安全です。本システムは、実証実験として無償開放しています。

https://telework.cyber.ipa.go.jp/news/

● シン・テレワークシステム概念図

2019年度未踏スーパークリエータが決定！

「2019年度未踏IT人材発掘・育成事業」において、17名を未踏スーパークリエータに認定しました。

2019年度は、いちごの受粉作業を自動で行い安定生産を可能にするロボットの開発や、ソフトウェア開発の作業コストを軽減するソースコードの自動修正ツールの開発、生体情報向けの秘密計算プラットフォームなど産業界への貢献が期待されるプロジェクトのほか、高精度な動画テロップを自動生成するモバイルアプリ、VR空間において実在感を保ったまま食事が体験できるシステムの開発など新たな価値を提供するプロジェクトなどで高い成果を上げました。

https://www.ipa.go.jp/jinzai/mitou/2019/20200528.html

■ **虫媒に代わるいちごの自動受粉ロボットシステムの開発**

［**ミツバチによる受粉の課題**］

- 一般的に授粉で用いられるセイヨウミツバチの価格が高騰している
- 外来種であるため生態系に悪影響を及ぼす可能性が高い　など

［**解決策**］

- ミツバチに代わっていちごの授粉作業を行うロボットシステム
- 専用のアタッチメントと授粉アルゴリズムによりミツバチの動きを再現する


ミツバチをロボットに置き換える


開発したロボットシステム

DX推進の実態調査報告書を公開

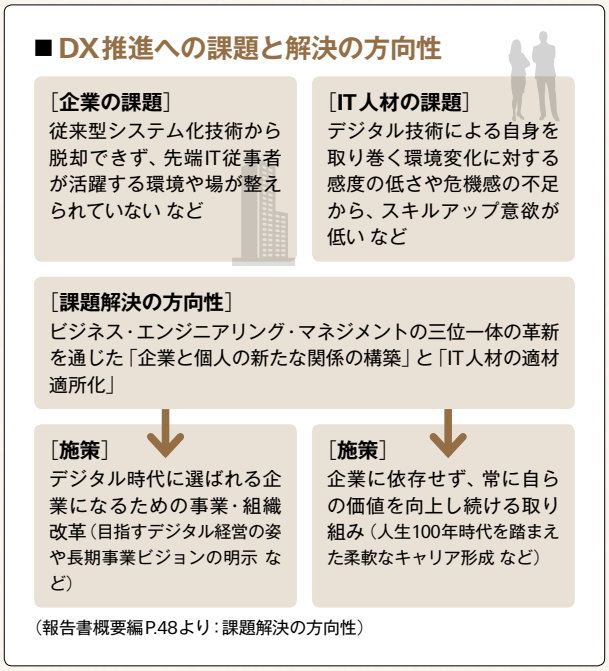
IPAが行った「デジタル・トランスフォーメーション（DX）推進に向けた企業とIT人材の実態調査」によると、国内においてはいまだ多くの企業でDXが進んでいないことがわかりました。

報告書では、その背景にある本質的な課題を、デジタル時代に向けた企業の方向性や、個人としてのあるべき姿が描けていないことと分析し、その課題解決の方向性を示しています。

また、デジタル化のみに閉じずさまざまな変革に取り組む際の「考えるヒント」を、24のパターンで整理し、併せて公開しました。

https://www.ipa.go.jp/ikc/reports/20200514_1.html

https://www.ipa.go.jp/ikc/reports/20200514_2.html



（報告書概要編P.48より：課題解決の方向性）

Just Information

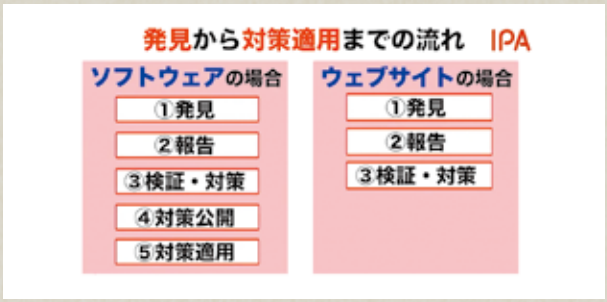
脆弱性発見者の心得を学ぶ動画シリーズ「脆弱性発見・報告のみちしるべ」公開中

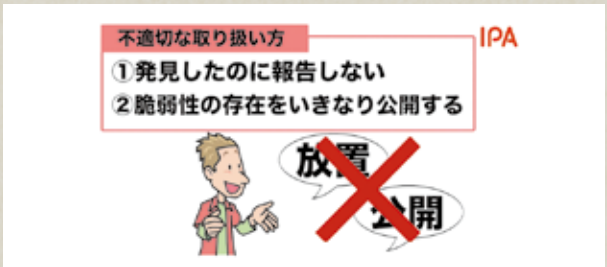
ソフトウェアなどに脆弱性が発見された場合、開発者への速やかな情報共有と、開発者による対策の実施が求められます。その際、脆弱性発見者が情報の取り扱いを誤ると、脆弱性が放置されたり、攻撃を受けたりするリスクが高まります。

本動画は、脆弱性発見者に求められる対応・心構えを学ぶための教育コンテンツで、脆弱性情報の適切な取り扱い方や注意点などを紹介しています。これから情報セキュリティを学ぶ方の自己学習や、教育機関での教材に活用いただけます。

「脆弱性発見・報告のみちしるべ」全8編（1編あたり1～3分）

1. 脆弱性という言葉知っていますか？
2. 脆弱性情報とは？
3. 実は諸刃の剣？ 脆弱性情報の2つの側面
4. やってはいけない！ 脆弱性情報の取扱い
5. 脆弱性の発見から対策実施までの流れ
6. 発見時の注意点～発見者に求められる心構え～
7. 報告時の注意点～発見者が知っておくべきこと～
8. 情報セキュリティ早期警戒パートナーシップ





脆弱性　みちしるべ　検索

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！ ～情報セキュリティマネジメント試験編～

情報セキュリティマネジメント試験は、情報セキュリティ管理に関する基礎知識を問う国家試験です。

問1　【平成28年秋・問21】

情報の“完全性”を脅かす攻撃はどれか。

ア　Webページの改ざん
イ　システム内に保管されているデータの不正コピー
ウ　システムを過負荷状態にするDoS攻撃
エ　通信内容の盗聴

問2　【令和元年秋・問18】

WPA3はどれか。

ア　HTTP通信の暗号化規格
イ　TCP/IP通信の暗号化規格
ウ　Webサーバで使用するディジタル証明書の規格
エ　無線LANのセキュリティ規格

問3　【平成30年秋・問37】

JIS Q 27001：2014（情報セキュリティマネジメントシステム－要求事項）に基づいてISMS内部監査を行った結果として判明した状況のうち，監査人が指摘事項として監査報告書に記載すべきものはどれか。

ア　USBメモリの使用を、定められた手順に従って許可していた。
イ　個人情報の誤廃棄事故を主務官庁などに、規定されたとおりに報告していた。
ウ　マルウェアスキャンでスパイウェアが検知され，駆除されていた。
エ　リスクアセスメントを実施した後に、リスク受容基準を決めた。

正解：問1 ア　問2 エ　問3 エ

IPAの事業領域

おかげさまで創設50周年

情報セキュリティ対策の実現
- 社会を守る
- 対策を促す
- 安全を担保する

IT人材の育成
- サイバーセキュリティ人材を育てる
- ITイノベーション人材を磨き上げる
- IT人材の知識・スキルを認定する

IT社会の動向調査・分析・基盤構築
- IT社会の動向調査・分析、情報発信
- データ利活用を促進する
- IoT製品・システムの安全性・信頼性を確保する
- スキル変革の推進
- 地域における取り組みの支援

「IPA NEWS」送付先の変更・送付中止は、下記のメールアドレスにご連絡くださいますようお願い致します。
メール　**pr-inq@ipa.go.jp**

IPAのSNS公式アカウント、メールニュースの配信登録はこちら
https:www.ipa.go.jp/

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