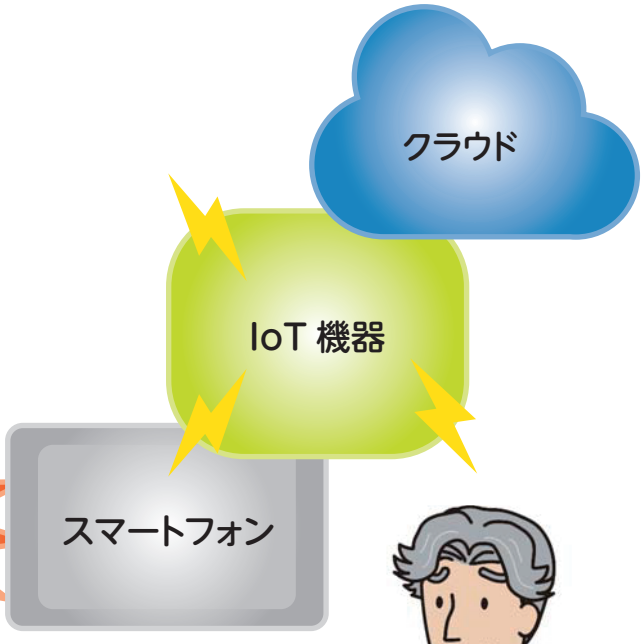
中小企業・小規模事業者の皆様へ

新 5分でできる！ 情報セキュリティ自社診断

最新動向への対応、できてますか？

脅威や攻撃の変化

IT環境の変化



取り返しのつかないことになる前に

あなたの会社のセキュリティ状況を

「5分でできる！自社診断」でチェック！

使用方法

診断編（次ページ）25問の質問に回答してください。

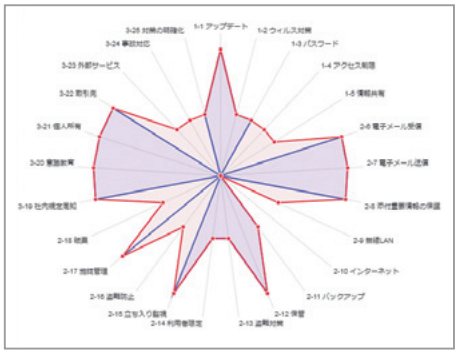
情報セキュリティ対策支援サイトでもオンライン診断できます。
https://security-shien.ipa.go.jp/learning/

回答結果をもとに採点し、対策を検討しましょう

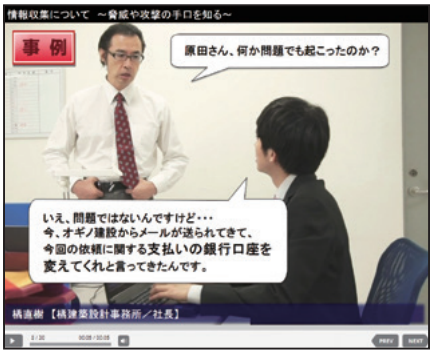
100点満点だった方	入門レベルのセキュリティ対策は達成です。ステップアップを検討しましょう。	「中小企業の情報セキュリティ対策ガイドライン」を参照して、情報セキュリティ対策の強化に取り組みましょう。
70～99点だった方	ほぼ、出来ていますが、部分的に対策が不十分な点があるようです。	小さな隙間から情報が漏えいすることもあります。100 点満点を目指しつつ、「中小企業の情報セキュリティ対策ガイドライン」を参照して対策の強化に取り組みましょう。
50～69点だった方	対策が行き届いていないところが目立ちます。	点数が低かった項目について「解説編」を参考に対策を検討し、「情報セキュリティハンドブック」を活用して周知しましょう。
49点以下だった方	いつ情報流出などの事故が起きても不思議ではありません。	「解説編」や「対策のしおり」「映像で知る情報セキュリティ」を利用して、分からなかった部分や点数が低かった項目を確認し、対策を施しましょう。

情報セキュリティ対策支援サイト
https://security-shien.ipa.go.jp/

中小企業が情報セキュリティ対策を「はじめる」、さらには「強化していく」ことを支援するサイトです。



■5分でできる！自社診断
25の質問に答えるだけで診断できる



■5分でできる！ポイント学習
自社診断の質問を1テーマ5分で学べる

■普及啓発コンテンツの提供
講習会や学習用に利用できる資料

診断項目	No	診断内容	チェック			
			実施している	一部実施している	実施していない	わからない
Part 1 基本的対策	1	パソコンやスマホなど情報機器の OS やソフトウェアは常に最新の状態にしていますか？	4	2	0	−1
	2	パソコンやスマホなどにはウイルス対策ソフトを導入し、ウイルス定義ファイル※1 は最新の状態にしていますか？	4	2	0	−1
	3	パスワードは破られにくい「長く」「複雑な」パスワードを設定していますか？	4	2	0	−1
	4	重要情報※2 に対する適切なアクセス制限を行っていますか？	4	2	0	−1
	5	新たな脅威や攻撃の手口を知り対策を社内共有する仕組みはできていますか？	4	2	0	−1
Part 2 従業員としての対策	6	電子メールの添付ファイルや本文中の URL リンクを介したウイルス感染に気をつけていますか？	4	2	0	−1
	7	電子メールや FAX の宛先の送信ミスを防ぐ取り組みを実施していますか？	4	2	0	−1
	8	重要情報は電子メール本文に書くのではなく、添付するファイルに書いてパスワードなどで保護していますか？	4	2	0	−1
	9	無線 LAN を安全に使うために適切な暗号化方式を設定するなどの対策をしていますか？	4	2	0	−1
	10	インターネットを介したウイルス感染やSNSへの書き込みなどのトラブルへの対策をしていますか？	4	2	0	−1
	11	パソコンやサーバーのウイルス感染、故障や誤操作による重要情報の消失に備えてバックアップを取得していますか？	4	2	0	−1
	12	紛失や盗難を防止するため、重要情報が記載された書類や電子媒体は机上に放置せず、書庫などに安全に保管していますか？	4	2	0	−1
	13	重要情報が記載された書類や電子媒体を持ち出す時は、盗難や紛失の対策をしていますか？	4	2	0	−1
	14	離席時にパソコン画面の覗き見や勝手な操作ができないようにしていますか？	4	2	0	−1
	15	関係者以外の事務所への立ち入りを制限していますか？	4	2	0	−1
	16	退社時にノートパソコンや備品を施錠保管するなど盗難防止対策をしていますか？	4	2	0	−1
	17	事務所が無人になる時の施錠忘れ対策を実施していますか？	4	2	0	−1
	18	重要情報が記載された書類や重要なデータが保存された媒体を破棄する時は、復元できないようにしていますか？	4	2	0	−1
Part 3 組織としての対策	19	従業員に守秘義務を理解してもらい、業務上知り得た情報を外部に漏らさないなどのルールを守らせていますか？	4	2	0	−1
	20	従業員にセキュリティに関する教育や注意喚起を行なっていますか？	4	2	0	−1
	21	個人所有の情報機器を業務で利用する場合のセキュリティ対策を明確にしていますか？	4	2	0	−1
	22	重要情報の授受を伴う取引先との契約書には、秘密保持条項を規定していますか？	4	2	0	−1
	23	クラウドサービスやウェブサイトの運用等で利用する外部サービスは、安全・信頼性を把握して選定していますか？	4	2	0	−1
	24	セキュリティ事故が発生した場合に備え、緊急時の体制整備や対応手順を作成するなど準備をしていますか？	4	2	0	−1
	25	情報セキュリティ対策（上記 1 ～ 24 など）をルール化し、従業員に明示していますか？	4	2	0	−1

※1 コンピュータウイルスを検出するためのデータベースファイル「パターンファイル」とも呼ばれます。
※2 重要情報とは営業秘密など事業に必要で組織にとって価値のある情報や顧客や、従業員の個人情報など管理責任を伴う情報のことです。

A 実施しているの合計点	B 一部実施しているの合計点	C わからないの合計点
点	点	マイナス(−) 点
A+B+C 合計		点

診断の後は次ページ以降を読んで対策を検討してください。

Part 1 基本的対策

No.1～5は企業の規模や形態を問わず、必ず対策していただきたい5項目です。いずれも一度やればよいものではなく、継続的な対策実施が欠かせないため、運用ルールとして社内に定着させる必要があります

診断編　NO.1　脆弱性対策

OSやソフトウェアは常に最新の状態にする

OS やソフトウェアを古いまま放置していると、セキュリティ上の問題点が解決されず、それを悪用したウイルスに感染してしまう危険性があります。お使いの OS やソフトウェアには、修正プログラムを適用する、もしくは最新版を利用するようにしましょう。

対策例 Windows　Updateを実施する(WindowsOSの場合)、Adobe Flash Player・Adobe Reader・Java実行環境などの利用中のソフトウェアを最新版にするなど。

情報セキュリティ対策に役立つツール
MyJVNバージョンチェッカ

パソコンにインストールされているソフトウェア製品（ウェブブラウザや動画再生ソフトなど）のバージョンが最新であるかを簡単な操作でチェックできるツールです。MicrosoftのWindows Updateと併せて、ソフトウェア製品のバージョンアップを行う習慣を身に付けましょう。

「MyJVNバージョンチェッカ」
http://jvndb.jvn.jp/apis/myjvn/

診断編　NO.2　ウイルス対策

ウイルス対策ソフトを導入し適切に利用する

ID・パスワードを盗んだり、遠隔操作を行ったり、ファイルを勝手に暗号化するウイルスが増えています。ウイルス対策ソフトを導入し、ウイルス定義ファイル(パターンファイル)は常に最新の状態になるようにしましょう。

対策例 ウイルス定義ファイルが自動更新されるように設定する、統合型のセキュリティ対策ソフトの導入を検討するなど。

診断編　NO.3　パスワード管理

強固なパスワードを使用する

パスワードが推測や解析されたり、ウェブサービスから流出した ID・パスワードが悪用されたりすることで、不正にログインされる被害が増えています。パスワードは「長く」、「複雑に」、「使い回さない」ようにして強化しましょう。

対策例 パスワードは英数字記号含めて10文字以上にする、名前、電話番号、誕生日、簡単な英単語などはパスワードに使わない、同じID・パスワードをいろいろなウェブサービスで使い回さないなど。

診断編　NO.4　機器の設定

共有設定を見直す

データ保管などのウェブサービスやネットワーク接続した複合機の設定を間違ったために、無関係な人に情報を覗き見られるトラブルが増えています。無関係な人が、ウェブサービスや機器を使うことができるような設定になっていないことを確認しましょう。

対策例 ウェブサービスの共有範囲を限定する、ネットワーク接続の複合機やカメラ、ハードディスク（NAS）などの共有範囲を限定する、従業員の異動や退職時に設定の変更（削除）漏れがないように注意するなど。

診断編　NO.5　情報収集

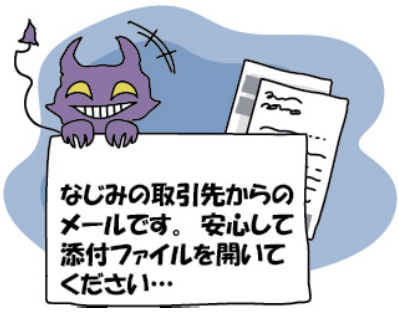
脅威や攻撃の手口を知り、対策に活かす

取引先や関係者と偽ってウイルス付のメールを送ってきたり、正規のウェブサイトに似せた偽サイトを立ち上げて ID・パスワードを盗もうとする巧妙な手口が増えています。脅威や攻撃の手口を知って対策をとりましょう。

対策例 IPAなどのセキュリティ専門機関のウェブサイトやメールマガジンで最新の脅威や攻撃の手口を知る、利用中のインターネットバンキングやクラウドサービスなどが提供する注意喚起を確認するなど。

Part 2 従業員としての対策

No.6～18は従業員として注意すべき項目です。重要情報を日々扱っていると慣れによる人為的ミスが発生しやすくなります。また、脅威の形が日々変化しているので、油断しないように注意する必要があります。



診断編　NO.6　電子メールのルール

身に覚えのない電子メールは疑ってみる

電子メールに添付されたファイルを開いたり、電子メール本文中に記載されたURLリンクをクリックしたりすることでウイルス感染する事故が続いています。身に覚えのない電子メールの添付ファイルやURLリンクへのアクセスに気をつけましょう。

対策例 不審な電子メールの添付ファイルを安易に開かない、URLリンクに安易にアクセスしない、不審な電子メールの情報を社内に共有するなど。

診断編　NO.7　電子メールのルール

宛先の送信ミスを防ぐ

電子メールや FAX の送り先を間違えて、他人に情報が漏えいしてしまう事故が続いています。電子メールや FAX は送り先を十分確認するようにしましょう。また、電子メールアドレスを誤って他人に伝えてしまうことも情報漏えいになります。複数の送り先に送信する際には、送り先の指定方法を十分に確認するようにしましょう。

対策例 電子メールやFAXを送る前に送信先を再確認する、電子メールはTO・CC・BCCを使い分けて指定するなど。

診断編　NO.8　電子メールのルール

重要情報を送信する時は保護する

重要情報を電子メールで送る場合は、電子メールの本文に書き込まず、文書ファイルなどに記載してパスワードで保護した後、メールに添付します。パスワードはその電子メールには書き込まず、電子メール以外の手段で通知することが必要です。

対策例 重要情報は文書ファイルに書いてパスワードで保護する、パスワードはあらかじめ決めておくか、携帯電話のショートメッセージサービス（SMS）などの別手段で知らせるなど。

診断編　NO.9　無線LANのルール

無線LANの盗聴や無断使用を防ぐ

適切なセキュリティ設定がされていない無線 LAN は、通信内容を読み取られたり、不正に接続されて犯罪行為に悪用されたりする被害を受ける可能性があります。無線 LAN の盗聴対策や無断使用を防止するようにセキュリティ設定をしましょう。

対策例 強固な暗号化方式（WPA2-PSK）を選択する、パスフレーズ（暗号化キー）は長くて推測されにくいものを使用するなど。

診断編　NO.10　インターネット利用のルール

インターネットを介したトラブルを防ぐ

悪意のあるウェブサイトやセキュリティ上の問題があるウェブサイトを閲覧することでウイルス感染する可能性があります。また、SNS や掲示板へ悪ふざけした画像を投稿したり秘密情報を勝手に掲載して会社に被害を及ぼすことがあります。業務でのインターネット利用を制限する仕組みやルールにより、被害を防止することが必要です。

対策例 インターネットの利用ルールを作る、SNSの利用ルールを作る、Webフィルタリング機能を導入することでシステム的にインターネットの利用を制限するなど。

診断編　NO.11　バックアップのルール

バックアップを励行する

故障や誤操作、ウイルス感染などにより、パソコンやサーバーの中に保存したデータが消えてしまうことがあります。このような不測の事態に備えて、バックアップを取得しておきましょう。

対策例 重要情報のバックアップを定期的に行う、バックアップは別の場所に保存するなど。

診断編　NO.12　保管のルール

重要情報の放置を禁止する

机の上に放置された情報は、誰かに持ち去られたり、盗み見られたりする危険にさらされています。関係者以外が見たり、触れたりすることができないように、重要情報は放置せず、管理する必要があります。保管場所を定め、作業に必要な場合のみ持ち出し、終了後に戻すことを励行するようにしましょう。

対策例　机の上をきれいにする、重要書類は鍵付き書庫に保管するなど。

診断編　NO.13　持ち出しのルール

重要情報は安全な方法で持ち出す

重要情報を社外へ持ち出す場合、思わぬ盗難にあったり、うっかり紛失したりすることがあります。ノートパソコンやスマートフォンの利用にあたってパスワードの入力を求めるように設定したり、データファイルを暗号化するなどの対策を事前に行うことで、盗難や紛失の際に情報を簡単に読み取られることができないようにしましょう。

対策例　重要情報の持ち出しは許可制にする、ノートパソコン・スマートフォン・USBメモリなどはパスワードロックをかける、荷物を放置しないなど。

診断編　NO.14　事務所の安全管理

機器を勝手に操作させない

パソコンを使用した作業の途中でそのまま席を離れたり、パスワードなしでログインできるパソコンなど、誰でも操作できる状態のパソコンは、不正に使用される可能性があります。不正使用からパソコンを守るための対策を行いましょう。

対策例　離席時にパソコンをロックする、退社時にパソコンをシャットダウンし、他人がパソコンを使うことを防ぐなど。

診断編　NO.15　事務所の安全管理

見知らぬ人には声をかける

関係者以外の事務所への立ち入りを制限しなければ侵入されてしまい、情報を盗み取られる危険性があります。特にサーバーや書庫・金庫など、重要な情報の保管場所の近くには無断で立ち入りができないようにしましょう。

対策例　事務所で見知らぬ人は事務所に入れない、受付を設置するなど。

診断編　NO.16　事務所の安全管理

機器・備品の盗難防止対策を行う

ノートパソコンやタブレット端末、USB メモリなどは手軽に持ち運べる便利さがある反面、盗難や紛失の危険性も高くなっています。利用しない場合は、施錠可能な引き出し等に保管するなどの対策を講じましょう。

対策例　退社時に机の上のノートパソコンやタブレット端末、備品（CD、USBメモリ、外付けハードディスクなど）を引き出しにしまうなど。

診断編　NO.17　事務所の安全管理

オフィスの戸締まりに気を配る

最終退出者と退出時間の記録を残すことは、最終退出者による施錠の責任意識を向上させることにも役立ちます。施錠と退出記録の管理をしましょう。

対策例　鍵の管理を徹底する、最終退出者は事務所を施錠し退出の記録（日時、退出者）を残すなど。

診断編　NO.18　情報の安全な処分

重要情報は復元できないように消去する

重要情報が記載された書類をゴミ箱にそのまま捨てると、関係者以外の目に触れてしまい、重大な漏えい事故を引き起こすことがあります。また、電子機器・電子媒体に保存された情報は、ファイル削除の操作をしても復元される恐れがあります。重要情報を廃棄する場合は、シュレッダーや消去用ソフトウェアを利用するなど、媒体ごとに適切な処分をしましょう。

対策例　書類は細断する、電子データは消去ソフトを利用する、物理的に壊してから処分する、専門業者に消去を依頼するなど。

情報セキュリティ対策に役立つツール

対策のしおり

情報セキュリティ上の様々な脅威への対策をテーマ別にわかりやすく解説した小冊子シリーズです。IPA のホームページからダウンロード (PDF) もできます。

「対策のしおり」
https://www.ipa.go.jp/security/antivirus/shiori.html

Part 3 組織としての対策

No.19～25は組織としての方針を定めた上で、実施すべき対策です。情報セキュリティのルールは明文化して社内で共有することにより、従業員の意識を高めるようにしましょう。

診断編　NO.19　守秘義務の周知

従業員に守秘義務について理解してもらう

従業員の守秘義務や機密保持について就業規則などで定められていることもありますが、どのような情報が秘密なのか、何をしたらいけないのかなどを、従業員に明確に説明しましょう。

対策例 採用の際に守秘義務について説明する、守秘に関する覚書を交わす、秘密としている情報を具体的に示すなど。

診断編　NO.20　従業員教育

従業員に情報セキュリティ教育を行う

日々の仕事では常に様々な情報を取り扱いますが、日常的であるがゆえに管理の意識がつい疎かになりがちです。従業員に対し繰り返し意識付けを行うことが有効です。

対策例 情報管理の大切さや関連する法令などを説明する、定期的な研修の機会を設けるなど。

診断編　NO.21　私物機器の利用

個人所有端末の業務での利用可否を決める

個人所有のパソコンやスマートフォンを業務で使用する場合、管理が行き届かず、セキュリティの確保が難しくなります。個人所有端末の業務利用の可否や業務利用のルールを定めましょう。

対策例 個人所有パソコン、スマートフォンの業務利用を許可制にする、業務利用する場合のルールを決めるなど。

診断編　NO.22　取引先管理

取引先に秘密保持を要請する

取引先が情報の内容から判断して「当然秘密にしてくれるだろう」という一方的な期待は禁物です。取引先に機密情報を提供する場合には、それを機密として取り扱ってもらうことを明確にすることが必要です。

対策例 秘密保持や具体的な対策を明記した契約や覚書を交わす、情報セキュリティ対応方針を公表している取引先を選定する、取引先の情報セキュリティ対策を確認するなど。

診断編　NO.23　外部サービスの利用

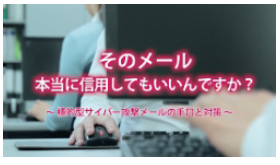
信頼できる外部サービスを使う

クラウドサービスなど外部サービスをコスト優先で選んでしまうと障害等でサービスが利用できなくなっても、補償を受けられない場合もあります。外部サービスを利用する場合は、性能や信頼性、補償内容など十分に吟味しましょう。

対策例 利用規約や補償内容、セキュリティ対策などを確認して事業者を選ぶなど。

情報セキュリティ対策に役立つツール

映像で知る情報セキュリティ



情報セキュリティ上の様々な脅威と対策が学べる映像コンテンツです。10 分前後のドラマやデモンストレーションを通じて情報セキュリティを学べます。YouTube「IPA チャンネル」でも公開中です。組織内研修等でご利用ください。

「映像で知る情報セキュリティ」
https://www.ipa.go.jp/security/keihatsu/videos/

診断編　NO.24　事故への備え

事故発生に備えて事前に準備する

実際に事故が起きてからだと、冷静に対応する余裕がなくなってしまいます。また、対応が後手に回り、それが原因でさらに深刻な事態になりがちです。報道されるセキュリティ事故などを参考に「もし、同じことが自分の会社で起きたら・・・」を想定して、誰がいつ何をするのかをまとめておきましょう。

対策例　重要情報の流出や紛失、盗難があった場合の対応手順書を作成し、従業員に周知するなど。

診断編　NO.25　ルールの整備

情報セキュリティ対策をルール化する

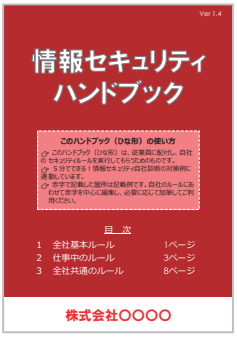
経営者が情報セキュリティ対策に関する方針を決めていたとしても、それを具体的なルールとして明文化していなければ、従業員は都度経営者の指示を仰がなければなりません。従業員が自らルールに従って行動できるように、「企業としてのルール」をまとめて明文化し、従業員がいつでも見られるようにしておく必要があります。

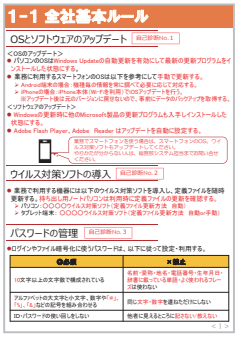
対策例　情報セキュリティ対策として、診断シート項目のNo.1から24までをルール化して社内で共有する、一度決めたルールでも問題があれば改善するなど。

解説編で例示した対策の前提は以下のとおりです。
■経営者（代表者）が対策方針を直接指示・確認することができる
■従業員全員が顔見知りである
■複雑な設定を必要とするサーバーやネットワーク機器を自社所有していない
・電子メールやのホームページは外部サービスを利用するなどのように、インターネットに直接接続しているサーバーを自社所有していない
・市販のアプリケーションソフトだけを利用しているなどのように、自社で独自に開発したアプリケーションソフトはない

自社診断の後は社内ルールの周知に取り組もう！

中小企業の情報セキュリティ対策ガイドライン付録の「情報セキュリティハンドブック（ひな形）」を自社のルールに合わせて編集し、全従業員に配付するなどして一人ひとりが実施すべき対策の周知に取り組んでください。自社診断で100点満点が取れるよう組織全体のレベルアップを図りましょう。





情報セキュリティハンドブック（ひな形）
https://www.ipa.go.jp/security/keihatsu/sme/guideline/

情報セキュリティ対策の取り組みを外部にアピールしよう！

「SECURITY　ACTION」は中小企業自らが、情報セキュリティ対策に取組むことを自己宣言する制度です。「5分でできる！情報セキュリティ自社診断」を実施し、「情報セキュリティ基本方針」を定め、公開することで２段階目の「二つ星」を使用することができます。

Check!!
☑ 5分でできる！
情報セキュリティ自社診断

Check!!
☑ 情報セキュリティポリシー
（基本方針）

SECURITY ACTION ★★
セキュリティ対策自己宣言

SECURITY ACTION 二つ星
https://www.ipa.go.jp/security/security-action/

IPA 独立行政法人情報処理推進機構
セキュリティセンター

〒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
TEL 03-5978-7508　FAX 03-5978-7546
E-mail isec-pr-nw@ipa.go.jp　URL https://www.ipa.go.jp/security/

VEGETABLE OIL INK
この印刷物は植物性油インキを使用しています。
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。
定価：47円（税別）
2019.3.19 Version 5.0