

「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

今、取得すべき国家資格はこれだ!!

「登録セキスペ」 メリット大解剖!

- データで読むITの今・未来
「プラス・セキュリティ人材」も資格を活用する傾向に!
- セキュリティのすゝめ 06〈サイバー攻撃のリスクはすべての企業にある〉
中小企業の被害事例とセキュリティ対策に学ぶ
- 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! ~ITパスポート試験編~

今、取得すべき国家資格はこれだ!!

「登録セキスペ」 メリット大解剖!

▶左から
株式会社京三製作所 信号事業部
運行システム部 主任
一般社団法人情報処理安全確保支援士会 理事
情報処理安全確保支援士(第000705号)
榊原 光一さん

日本電気株式会社
サイバーセキュリティ戦略統括部
セキュリティ実装技術グループ
プロフェッショナル
情報処理安全確保支援士(第002439号)
妹脊 敦子さん

IPA
IT人材育成センター
国家資格・試験部 登録・講習グループ
藁科 綾子さん

サイバー攻撃の脅威が高まり、すべての企業でセキュリティ対策が急務となっています。そこで中心的役割を果たすのが「情報処理安全確保支援士(登録セキスペ)」です。IPAの資格制度担当者と、企業内で登録セキスペとして活躍するお2人に資格制度の特徴や登録セキスペに求められる役割、仕事のやりがいなどを聞きました。

セキュリティ対策の「プロデューサー」役を担う

サイバー攻撃のリスクが増大する中、政府が「サイバーセキュリティ戦略」で打ち出しているように、企業には“DXとサイバーセキュリティの同時推進”が求められています。とはいえ、日本ではセキュリティ人材が不足しているのも事実。社員にセキュリティの知識・技能の習得を促したり、外部の専門家を活用したりすることも重要な施策といえます。

そこで注目されるのが、サイバーセキュリティの確保を支援する国家資格「情報処理安全確保支援士」です。IPAが実施する同試験(SC)の合格者か、SC合格と同等以上の能力を持つ人が所定の登録手

続きを行うことで資格保持できることから「登録セキスペ」とも呼ばれ、2016年10月の創設以降、登録者は約2万名に上ります。

IPA IT人材育成センター 国家資格・試験部の藁科綾子さんは、登録セキスペ制度の特徴として次の3点を挙げます。

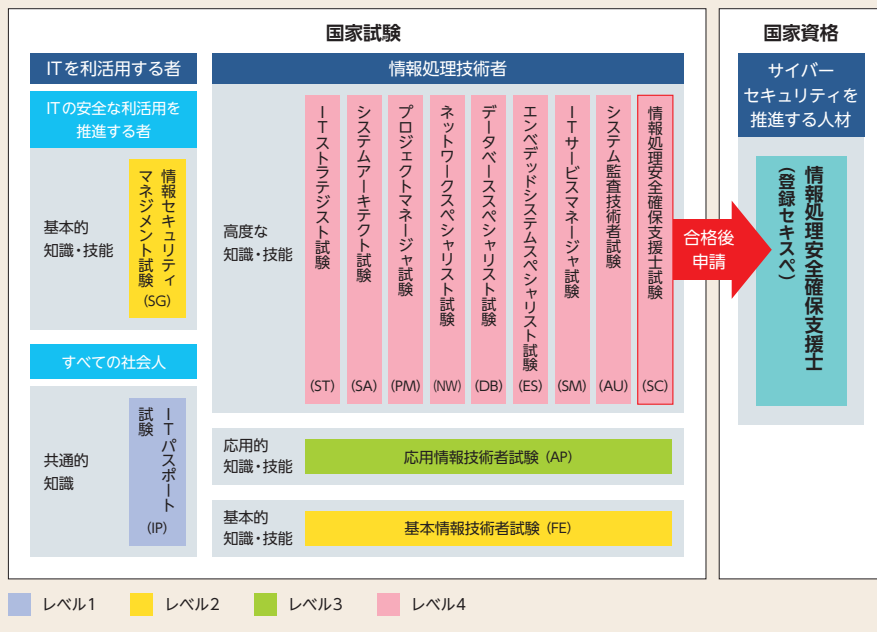
①**人材の質の担保**…「SCの難易度は高く、それゆえにセキュアな情報システムの企画、構築、運用保守までをトータルで支援できるという実力の証しとなります」と藁科さん。また、登録後も継続的な講習受講(有料)があり、最新の知識や技能を維持できることもポイント。今年3月からは、企業のDX推進に関してセキュリティ面の助言を行うための実践講習も新たに開設しています。

②**人材の見える化**…IPAは登録セキスペの検索サービスを提供しており、氏名や所属企業、勤務地、保有スキルなどの項目で人材を探ることが可能です。資格名称も独占使用できるため、多くの登録者が名刺に記載しています。

③**人材活用の安心感**…登録セキスペには秘密保持義務と信用失墜行為の禁止義務があり、違反すると罰則が科せられます。正しい倫理観を持つ人物を登録・資格継続することで、安心して活用できるわけです。

これら3つの要素を備えることで、登録セキスペはセキュリティ対策の「プロデューサー」としての活躍が期待されると藁科さん。「ビジネス戦略に基づいてセキュリ

図表 情報処理安全確保支援士試験 (SC) の位置付け



ティ対策を具体化したうえで、経営層と実務者層をつないだり、業務のデジタル化やDX推進をセキュリティの観点から支援する登録セキスペの重要性は今後ますます高まるでしょう」

登録後の継続的な講習でハイレベルな技量を維持

登録セキスペの妹脊敦子さんは日本電気株式会社(NEC)グループ全体のセキュリティ規程の策定、セキュアな開発を支援するツールの開発、インシデント対応など、社内外のセキュリティ施策に取り組んでいます。「NECはセキュリティに関する豊富な知見を蓄えており、安心・安全な製品・サービスを提供できることは競争力の源泉にもなっています」と妹脊さん。株式会社京三製作所に勤務する榊原光一さんも、業務上のニーズから会社の支援を受けて登録セキスペ資格を取得しました。同社は鉄道・交通信号やその制御システムなどの製造・販売を行っています。「社会インフラを支える会社として『安全と信頼』がモットーです。昨今のサイ

バー攻撃の脅威に対応すべく、さらに高度なセキュリティ体制の構築へ向けて取り組みを進めています」と榊原さん。ベンダーとユーザー企業という違いはあるものの、妹脊さんも榊原さんも登録セキスペの資格はDX時代の業務に必要という認識で一致しています。

資格取得後の講習について榊原さんは「セキュリティを包括的に勉強できるのがメリット」としつつ、「最新の対策を学べるので、知識や技量が陳腐化せず高いレベルを維持できます」と魅力を語ります。さらに「技術だけではなく、法律やガイドラインも勉強でき、得た知識は仕事でのリスクアセスメントでも役立っています」と妹脊さん。IPAの講習のほかに民間企業が実施する講習も受講でき、実機を使ってインシデント対応をシミュレーションできたことが大きな収穫になったとか。「攻撃手口の変化に伴い、セキュリティ対策も日々進化します。資格を取ったからと慢心せず、常にキャッチアップしていく姿勢が重要ですし、やりがいでもあります」という妹脊さんの

登録セキスペが社内が増えれば、企業価値向上にもつながる

言葉に、榊原さんも深くうなずきます。

また、榊原さんはIPAの藁科さんが登録セキスペの役割としてあげた「プロデューサー」役を現に担っています。「お客さまとベンダーの間を取り持つのも我々の仕事。自分自身が高度な知識を持っていることでベンダーと率直にやりとりでき、顧客価値を高めることができます。『さすが京三』という言葉が仕事の原動力です」と語る榊原さん。一方で、社内外へのセキュリティ啓発を推進し、リテラシー向上にも取り組んでいるそうです。

妹脊さんは「今やセキュリティと無縁でいられる人はいません。登録セキスペは多くの方に目指していただきたいですし、組織としても有資格者の拡大は企業価値の向上につながるはず」と訴えます。

資格取得を目指す人に対し、榊原さんは「いきなりSCに挑むのではなく、SG、FE、APなどの合格を経て挑戦するのがお勧め。セキュリティは、IPAのほかの試験区分でも必要となる知識なので応用が利きます」とアドバイス。資格保持者のコミュニティの場として、有志で構成される一般社団法人情報処理安全確保支援士会(以下、支援士会)の活動も活発に行われ、定期的に勉強会などが開催されています。支援士会の理事の立場から、「約400名の会員と情報交換ができ、人脈拡大も見込めます。登録後は支援士会にぜひ参加を!」と榊原さんはPRします。

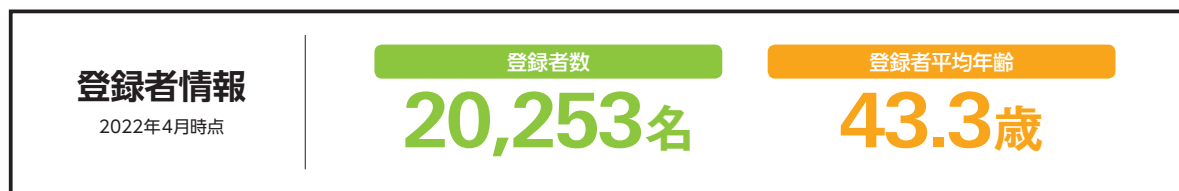
「DXとセキュリティ対策の両立や自身のスキルアップのため、登録セキスペや本制度を大いに活用していただきたいです」と最後に藁科さん。7月15日には本制度のオンライン説明会(無料)も実施予定。興味のある方はぜひご参加ください。



「プラス・セキュリティ人材」も資格を活用する傾向に！

本来業務と併せてセキュリティスキルが求められる人材（プラス・セキュリティ人材）も登録セキスへの資格を取得する動きが見られます。

2017～2022年登録者の登録申請書、現状調査票データより集計

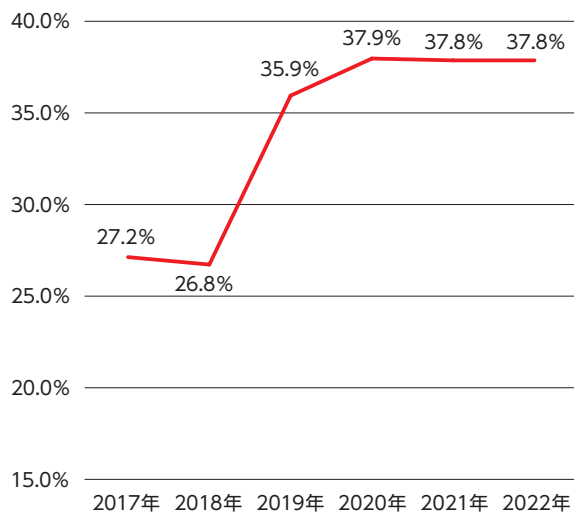


登録セキスへの所属企業（累計値）

n=18,423



非IT企業の割合の推移（登録年別）



ここ数年では、DXやシステムの内製化が進んでいることから、IT企業だけでなく非IT企業でも資格の活用が徐々に広がっています。また、セキュリティを専門としない業務従事者も資格を取得し、IT戦略・システムの企画、設計、運用等の

登録セキスへの担当業務（セキュリティ関連）

n=13,074（複数回答あり）

ITシステム・サービスのセキュリティ面での運用・管理	38.0%
セキュア設計・開発・構築・評価	36.6%
インシデント対応	25.9%
監視・情報収集	20.5%
サイバーセキュリティ対策機器の運用・保守	19.4%
サイバーセキュリティ管理体制のマネジメント	15.9%
サイバーセキュリティ管理体制の構築	15.8%
サイバーセキュリティに関する教育・人材育成	13.3%
セキュリティ技術及びサイバーセキュリティ対策に関する調査・研究	11.9%
脆弱性診断	11.5%
情報セキュリティ監査	9.0%
サイバーセキュリティに関する経営判断	3.6%
その他の業務	4.3%
サイバーセキュリティ関連業務に従事していない	27.7%

業務にセキュリティスキルを活かしている傾向が見られます。今後もDXの進展などによるプラス・セキュリティ人材のスキルアップの必要性とともに、資格のニーズが高まることが予想されます。

DXとサイバーセキュリティの両立に 登録セキスへ制度を活用しましょう！

中小企業の被害事例とセキュリティ対策に学ぶ

❗ 予算や人員に限られる中、「人」に焦点を当てる

IPAは今春、「2021年度中小企業における情報セキュリティ対策の実態調査報告書」と併せて、中小企業のインシデント被害や対策への取り組みなどの事例(61件)をまとめた事例集を公開しました。ここではその中の3件に注目し、セキュリティ対策の教訓を探ります。

①マルウェア感染やランサムウェア攻撃で大きな痛み(建設業・石川・従業員数101~300名)

この会社は、過去に社内のパソコンがマルウェアに感染したりランサムウェア攻撃を受けるなどして復旧に多大な費用と時間を費やしたため、セキュリティ対策に高い関心を寄せています。対策に割く予算や人員に限られる中、同社が焦点を当てたのは「人」でした。従業員に対し、継続的な周知活動でセキュリティリテラシーの向上に努めているのです。また、IPAが公開

する情報を参考に社内の情報管理規定も整備。業務委託先にもセキュリティ対策の徹底を求めるなど、実効性の高い施策を効率よく行っています。

❗ 管理の甘さから多くの企業サイトに脆弱性が

②ホームページへの不正アクセスを機に対策(サービス業・兵庫・従業員数5~20名)

この会社では外部のホームページ作成・管理サービスを利用していたところ、権限管理に隙があったことからホームページに不正アクセスされてしまいました。「自分たちのような小規模な会社がセキュリティ被害に遭うはずがない」と思い込んでいたということで、そこに油断があったといえそうです。早速、IDやパスワードは容易に推測できないものに変更し、関連会社ごとに個別に設定。さらに、IPアドレスの制御、システムアップデートの義務付けなど対策を強化しました。管理の甘さから自社ホームページに脆弱性







を招く企業は多々あります。IPAが公開する「安全なウェブサイトの作り方」なども参考に安心・安全なホームページ運用を心掛けましょう。

③退職者が社内の機密情報を不正持ち出し(卸売業・東京・従業員数6~20名以下)

元従業員が退職前に大量にファイルダウンロードして持ち出し、痛手を被ったこの会社。トラブルが発生してから機密情報の漏えいを防ぐ社内規定を新たに設けました。また、情報資産管理・画面記録などでログやデバイスを管理するシステムも導入し、従業員にとっても身の潔白を証明できる環境を構築。さらに、中小企業庁「IT導入補助金」の活用により低負担でシステムを導入することができました。

中小企業の多くは、被害に遭ってから対策を講じているのが実情です。すべての企業がサイバー攻撃のリスクに直面している今、これらの事例を他人事ととらえず、自社のセキュリティ対策の向上のために役立てましょう。

事例から得る学びと教訓

 マルウェア感染&ランサムウェアの被害	▶▶▶  従業員のリテラシーを向上させることで、省資源でも大きな効果を見込むことができる！
 ホームページへの不正アクセス	▶▶▶  「規模の小さい会社は狙われない」という思い込みを捨て、対策を強化することが大切！
 退職者による機密情報の持ち出し	▶▶▶  社内の情報セキュリティ対策の拡充が重要。従業員の潔白を証明する手段としても有効！

+ 対策に有効なIPAのツール +

- 1 社内のルールづくりに「中小企業の情報セキュリティ対策ガイドライン」^{※1}
- 2 従業員の意識啓発に「映像で知るセキュリティシリーズ」^{※2}
- 3 内部不正の防止に「組織における内部不正防止ガイドライン 第5版」^{※3}
- 4 セキュリティの考慮に「安全なウェブサイトの作り方」^{※4}

※1 <https://www.ipa.go.jp/security/keihatsu/sme/guideline/index.html>

※2 <https://www.ipa.go.jp/security/keihatsu/videos/index.html>

※3 <https://www.ipa.go.jp/security/fy24/reports/insider/index.html>

※4 <https://www.ipa.go.jp/security/vuln/websecurity.html>

もっと詳しく知りたい方は… <https://www.ipa.go.jp/security/fy2021/reports/sme/index.html>

Hot & New Topics

サイバーセキュリティ対策の実践事例を検索できるツールを公開

IPAは、「サイバーセキュリティ経営ガイドライン[※]」に記載の「重要10項目」の実践をサポートする検索ツール「プラクティス・ナビ」を公開しました。本ツールは、これまでPDFで公開していた「サイバーセキュリティ経営ガイドラインVer 2.0実践のためのプラクティス集」の第2章・第3章の内容を拡充・ウェブコンテンツ化したもので、新たに検索機能を追加しました。

重要10項目の実践手順や、セキュリティ担当者の悩みを解決するための対策、考え方など、企業の実例に基づく参考情報が簡単に検索できるため、マネジメント層がサイバー攻撃への対策強化に着手する際の情報収集などに活用できます。

※サイバー攻撃から企業を守るために経営者が認識すべき「3原則」と、CISO等に指示すべき「重要10項目」をまとめたガイドライン

<https://www.ipa.go.jp/security/economics/practice/>
<https://www.ipa.go.jp/security/fy30/reports/ciso/index.html>



● プラクティス・ナビ



「DX実践手引書 ITシステム構築編」改訂版を公開

本書は、DX推進に向けたITシステム構築のためのガイドです。国内のDX先進事例の調査結果をもとに、DX実現に求められるITシステムと技術要素群を整理し、その全体像を「スサノオ・フレームワーク」として示しています。

改訂版では、この要素群にセキュリティ要素を追加しました。独自アプリケーションのクラウド上での構築や、外部サービス・APIとの連携などDXに求められるセキュリティの考え方を整理しています。

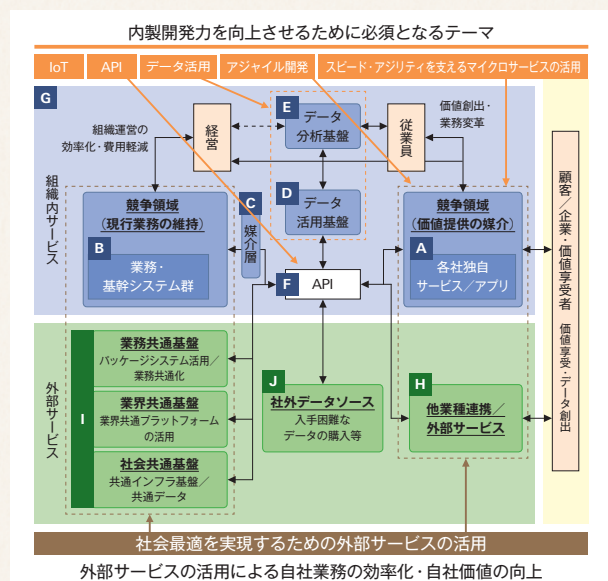
また、継続的にDXを推進している企業の事例を参考に、「変革規模」と「組織成熟度[※]」の指標を定義しました。変革規模に応じた組織成熟度への取り組みを行うことで、継続的なDX推進が可能になります。

※経営体制・環境準備・IT人材や技術力などの要素の達成度



https://www.ipa.go.jp/ikc/our_activities/dx.html#section7

● あるべき IT システムを実現する技術要素群 「スサノオ・フレームワーク」



「組織における内部不正防止ガイドライン」第5版を公開

本書は、内部不正による情報セキュリティ事故防止のためのガイドラインです。5年ぶりとなる今回の改訂では、テレワークの普及による新しい働き方への移行や、雇用・人材の流動化の加速、個人情報保護法、不正競争防止法などの法改正を踏まえ、新たに必要となる対策・強化すべき対策を追加しました。また、経営リスクを具体化して経営者へのメッセージをより強化しています。

今版では、営業秘密の漏えいの原因に多い「中途退職者」への対策や、役職員の人権・プライバシーに配慮しながらAIによるふるまい検知機能などを内部不正対策に適用するための措置についても提示しています。付録の対策状況の簡易チェックシートやQ&Aとの併用で対策の強化が期待できます。



<https://www.ipa.go.jp/security/fy24/reports/insider/index.html>

● 改訂のポイント

▶ テレワークの普及に伴う対策

オンラインストレージやクラウド等の外部サービスの利用拡大に合わせて、それらの技術・運用面での対策、テレワークを行う従業員等の教育、テレワーク中の内部不正に対応できるログ・証拠の取得といった幅広い対策を示しています。

▶ 退職者関連対策

内部不正への抑止力として有用なシステムのログ収集・解析とその注意点、秘密保持契約や誓約書の提出を拒否することを想定した対策など、雇用終了の際の対策の強化について示しています。

▶ ふるまい検知等の新技術活用に伴う対策

役員保護のための適切な設定ができるシステムを選定し、人手による判断と組み合わせるなどで説明責任を果たすといった運用を示しています。

※上記の各項目については、関連する法令をもとに注意点を追記し、コンプライアンスに問題が生じないように配慮しています。

Just Information

基本情報技術者試験 (FE) と情報セキュリティマネジメント試験 (SG) がいつでも受験可能になります！



これまで年2回(上期・下期の一定期間) CBT方式にて実施していたこれらの試験区分は、2023年4月から通年試験となる予定です。これによって受験者は都合のよい時期・日時を選択して受験できるようになります。また、試験時間の短縮によって受験者の利便性が高まります。

基本情報技術者試験 (FE) ……………ITに関する基本的な知識・技能を評価するための国家試験。

情報セキュリティマネジメント試験 (SG) ……………組織の情報セキュリティ確保に貢献し、脅威から継続的に組織を守るための基本的な知識・技能を評価するための国家試験。

● 各試験の変更内容

試験区分	変更前		変更後		変更後の出題範囲
FE	午前試験 (小問)	試験時間: 150分 出題数: 80問 解答数: 80問	科目A試験 (小問)	試験時間: 90分 出題数: 60問 解答数: 60問	現在の午前試験に準じる。
	午後試験 (大問)	試験時間: 150分 出題数: 11問 解答数: 5問 ※選択問題あり	科目B試験 (小問)	試験時間: 100分 出題数: 20問 解答数: 20問 ※選択問題なし(全問必須)	
SG	午前試験 (小問)	試験時間: 90分 出題数: 50問 解答数: 50問	科目A・B試験 (小問)	試験時間: 120分 ※2科目まとめて実施	科目A: 現在の午前試験に準じる。 科目B: 現在の午後試験に準じる。
	午後試験 (大問)	試験時間: 90分 出題数: 3問 解答数: 3問		出題数: 60問 解答数: 60問	

詳しくはこちら ▶ https://www.jitec.ipa.go.jp/1_00topic/topic_20220425.html

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2年度10月・問18】

UX (User Experience) の説明として、最も適切なものはどれか。

- ア 主に高齢者や障害者などを含め、できる限り多くの人が等しく利用しやすいように配慮したソフトウェア製品の設計
- イ 顧客データの分析を基に顧客を識別し、コールセンターやインターネットなどのチャネルを用いて顧客との関係を深める手法
- ウ 指定された条件の下で、利用者が効率よく利用できるソフトウェア製品の能力
- エ 製品、システム、サービスなどの利用場面を想定したり、実際に利用したりすることによって得られる人の感じ方や反応

問2 マネジメント系【令和2年度10月・問47】

システム障害が発生した際、インシデント管理を担当するサービスデスクの役割として、適切なものはどれか。

- ア 既知の障害事象とその回避策の利用者への紹介
- イ システム障害対応後の利用者への教育
- ウ 障害が発生している業務の代行処理
- エ 障害の根本原因調査

問3 テクノロジ系【令和2年度10月・問97】

公開鍵暗号方式では、暗号化のための鍵と復号のための鍵が必要となる。4人が相互に通信内容を暗号化して送りたい場合は、全部で8個の鍵が必要である。このうち、非公開にする鍵は何個か。

- ア 1
- イ 2
- ウ 4
- エ 6

正解：問1エ 問2ウ 問3ウ

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。
IT社会の課題解決や産業の発展につながる指針を示し、情報セキュリティ対策・DXの普及促進や、優れたIT人材を育成するための活動に取り組んでいます。

- 「IPA NEWS」定期送付のお申込み、送付先の変更は、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 spd-ipanews@ipa.go.jp



- 「IPA NEWS」アンケートはこちら

- 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/>

本誌に記載の製品名、サービス名などは、IPAまたは各社の商標もしくは登録商標です。
誌面に掲載しているQRコードは、cookieによりアクセス状況、簡易位置情報を取得します。制作の参考情報とするため、これらを外部に公表することはありません。