ITmedia エンタープライズ読者調査連動記事案のご案内

DX推進「デジタルリーダー」が知るべきハイブリッド／マルチクラウド時代のアタックサーフェス管理問題

2022年9月

タイアップ記事企画のご提案

DX推進「デジタルリーダー」が知るべきハイブリッド／マルチクラウド時代のアタックサーフェス管理問題

ITmedia エンタープライズの調査によると、読者の抱える脆弱性対策への課題が見えてきました。
エンタープライズ企業に対してどのようにデジタル化ソリューションの提案・訴求が最適か、調査結果をもとにしたタイアップ記事プランをご提案します。

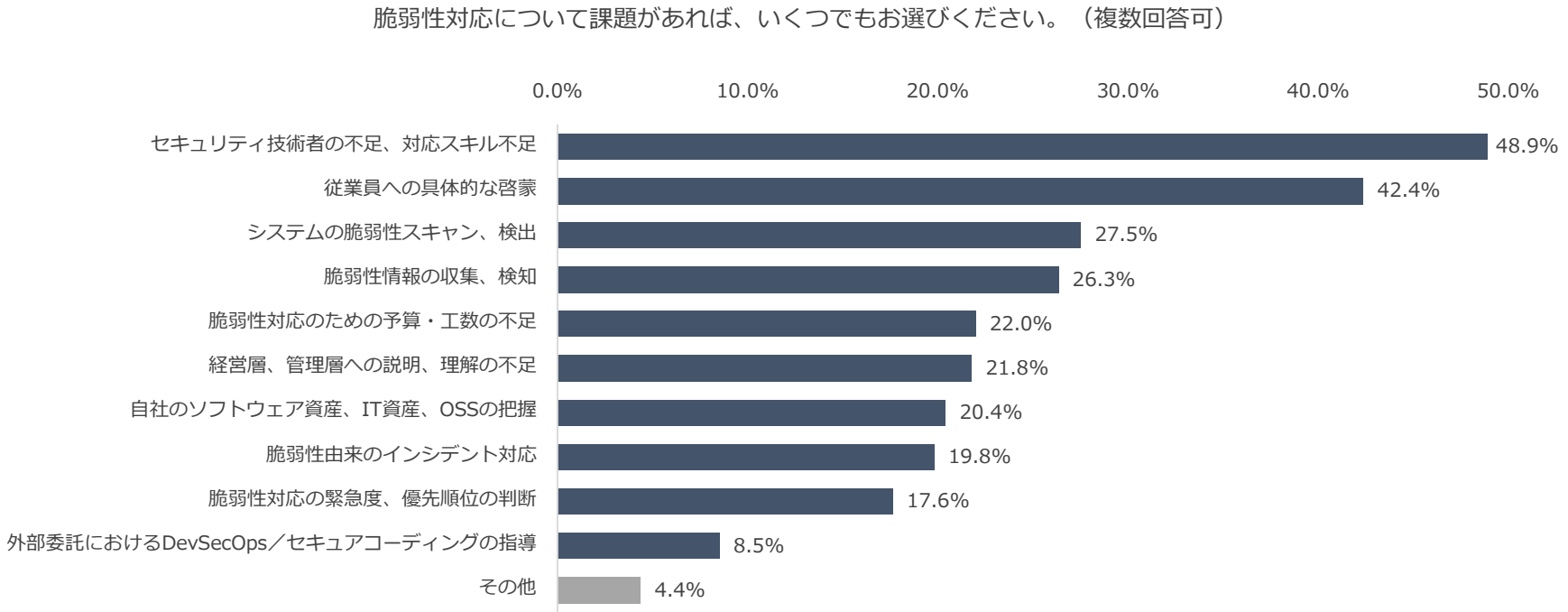
ITmedia エンタープライズでタイアップ記事をご実施頂ける場合、
本調査結果を貴社タイアップ記事中でご利用いただくことが可能です。

ITmediaエンタープライズ読者意識調査2022年3月「セキュリティ編」

■調査方法：ITmediaエンタープライズWebサイト上の自記式アンケート
■調査対象者：ITmediaエンタープライズ読者
■調査期間：2022年3月8日～2022年4月19日
■回答数：505件

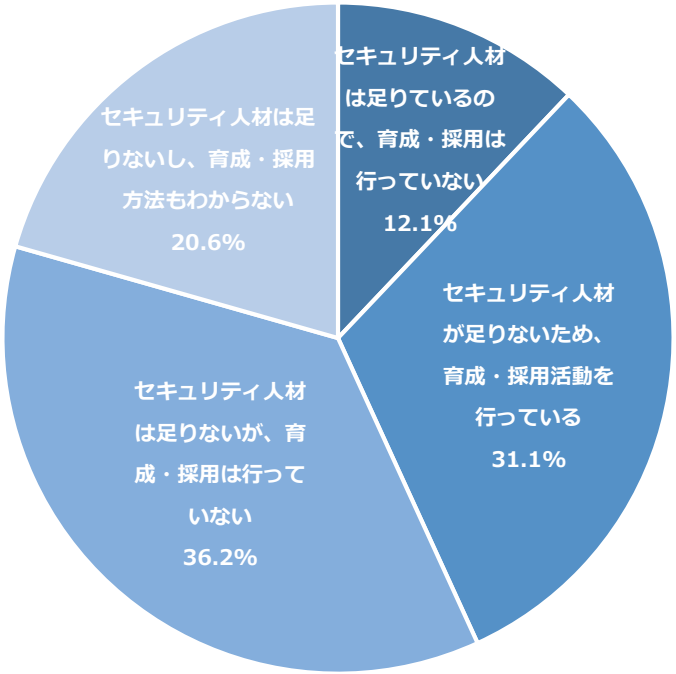
読者調査から読み取る読者の課題

読者の約半数は脆弱性対応に対して何らかの課題を抱えており、特にセキュリティ技術者の不足・スキル不足が顕著



読者調査から読み取る読者の課題

8割以上はセキュリティ人材は足りず、また育成・採用もできていない企業が多くを占める



読者を取り巻く背景

アタックサーフェス管理製品のリリースや、不足するセキュリティ人材を補う工夫をする企業が出てきている

攻撃者視点で脅威から保護 Microsoftが2つのセキュリティ製品を発表

Microsoftは、新たな脅威インテリジェンスと攻撃対象領域管理に向けたソリューション「Microsoft Defender Threat Intelligence」と「Microsoft Defender External Attack Surface Management」を発表した。


攻撃者視点で脅威から保護　Microsoftが2つのセキュリティ製品を発表

Microsoftは、新たな脅威インテリジェンスと攻撃対象領域管理に向けたソリューション「Microsoft Defender Threat Intelligence」と「Microsoft Defender External Attack Surface Management」を発表した。

2022年08月04日 08時00分 公開　[山口開弘、ITmedia]

印刷 9 Share B! 2

「うちの企業は大丈夫」じゃ乗り切れない、防御を固めよう

この記事は会員限定です。会員登録すると全てご覧いただけます。

Microsoftは2022年8月2日（米国時間）、新たなセキュリティ製品として「Microsoft Defender Threat Intelligence」と「Microsoft Defender External Attack Surface Management」を発表した。

これらはサイバー攻撃者の活動に関する背景情報を提供し、ITインフラをロックダウンして攻撃対象領域（アタックサーフェス）を縮小する。

リアルタイムデータにアクセス可能な脅威インテリジェンスを提供

Microsoft Defender Threat Intelligenceは、サイバー攻撃者の活動や行動パターンを追跡するソリューションだ。これを利用することでコンテキストや洞察、分析に基づいて、攻撃者のインフラを発見して迅速な調査やレジリエンスを実現する。

同社のアンチウイルスソフト「Microsoft Defender」シリーズやSIEM（Security Information and Event Management）ソリューション「Microsoft Sentinel」などのセキュリティ製品にも脅威インテリジェンス機能は組み込まれているが、セキュリティシグナルに基づく同社のリアルタイムデータに直接アクセスできる点がMicrosoft Defender Threat Intelligenceの特徴だ。

Microsoft Defender Threat Intelligenceは、常にインターネットのトラフィックなど情報をマッピングし、サイバー攻撃者とその攻撃手法を理解するのに必要な情報を提供する。

IBMが“ハッカー企業”の買収計画を発表 ポートフォリオはどう強化されるか

IBMは、攻撃対象領域の調査に強みを持つRandoriの買収計画を発表した。企業におけるIT環境が複雑化し、攻撃対象領域が拡大していることから、これを支援するポートフォリオを拡充する予定だ。


IBMが“ハッカー企業”の買収計画を発表　ポートフォリオはどう強化されるか

IBMは、攻撃対象領域の調査に強みを持つRandoriの買収計画を発表した。企業におけるIT環境が複雑化し、攻撃対象領域が拡大していることから、これを支援するポートフォリオを拡充する予定だ。

2022年06月09日 08時00分 公開　[猫田奈美人、ITmedia]

印刷 3 Share B! 2

クラウド導入を無駄にしないためのクラウドセキュリティ戦略

この記事は会員限定です。会員登録すると全てご覧いただけます。

IBMは2022年6月8日（現地時間）、セキュリティ企業のRandoriを買収する計画を発表した。この買収によってIBMはハイブリッドクラウド戦略を推進し、AI（人工知能）を活用したセキュリティ製品及びサービスのポートフォリオ拡充を予定する。

同社は2020年4月にアービンド・クリシュナ氏が会長兼最高経営責任者（CEO）に就任して以降、AIを活用したEDR（Endpoint Detection and Response）製品を提供するReaQtaなど20社以上の企業を買収している。Randoriは2022年で4社目の買収企業だ。

ハッカー企業Randoriの買収で、IBMのポートフォリオはどう変わる？

IBMによれば、企業は投資額を増加させる一方で、サイバー攻撃を受ける可能性がある領域（攻撃対象領域：アタックサーフェス）の管理に苦慮している。クラウドやサードパーティーのサービス、IoTなどの利用が進み、67%の組織が過去2年間で外部からの攻撃対象領域が拡大したという。

ホワイトペーパー
基礎から分かるCIAM、顧客離れを防ぐ製品の選び方とは？
“保守期限切れ”でも機能するなら使う――IT機器の延命が好結果を生む理由

一般従業員にも「ホワイトハッカー教育」

企業のセキュリティ対策や教育はセキュリティ先任者や責任者への教育だけでは間に合わなくなりつつあるようです。非IT人材の一般従業員にもハッカーの攻撃手法をしっかり学ばせる組織が出てきました。


一般従業員にも「ホワイトハッカー教育」

企業のセキュリティ対策や教育はセキュリティ先任者や責任者への教育だけでは間に合わなくなりつつあるようです。非IT人材の一般従業員にもハッカーの攻撃手法をしっかり学ばせる組織が出てきました。

2022年07月01日 08時30分 公開　[猫 慎雄、ITmedia]

印刷 通知 11 Share B! 3

どうやってマルウェア攻撃って防ぐんだ？　答えはここから

この記事は会員限定です。会員登録すると全てご覧いただけます。

1カ月ほど前にGMOグループが全従業員約7000人に「ホワイトハッカー教育」を始めるとした新聞報道が話題になりました。見出しだけを見ると、従業員全員をホワイトハッカーに育成するのかと早合点したのですが、実際はもちろんそういうわけではありません。

GMOインターネット広報によると「GMOサイバーセキュリティ byイエラエ」が中心となって作成したホワイトハッカー研修プログラムを、GMOインターネットグループ全パートナー（従業員）約7000人全員受講予定」とのことです。研修対象にはもちろん、経理や人事などのIT部門の所属ではない従業員も含まれます。

GMOサイバーセキュリティ byイエラエ（旧イエラエセキュリティ）はホワイトハッカー集団によって設立された企業として知られていました。同社がGMOインターネットグループと資本業務提携を発表したのが2022年1月です。同社は所属するホワイトハッカーやその協力者らによる技術コミュニティーを強みとしているといいます。

※本稿は2022年5月30日版のメールマガジンに掲載したコラムの転載です。登録はこちら。

非セキュリティ人材にこそハッカー教育が必要な理由

一般的にホワイトハッカーと言うと、悪意ある攻撃者と同じように高いセキュリティの知識を持ち、防御策を講じられる高度なスキルを持つ人材というイメージがありますが、ここで話題になっている「ホワイトハッカー教育」は、単にホワイトハッカーを育成するプログラムというわけではないようです。

ご提案するタイアップ記事企画案

以上に基づいた企画案によるアウェアネス施策をご提案します。制作ではお客様の訴求ポイントを加味し決定いたします

仮題：

DX推進「デジタルリーダー」が知るべき、ハイブリッド／マルチクラウド時代のアタックサーフェス管理問題　～攻撃者の目はどこを見ているか～

記事の流れ

1. あらゆる業務がITソリューションを活用する状況において企業をサイバー攻撃から守るには、包括的な対策が重要になる。
2. アプリケーションやインフラ、物理的な装置やエンドポイントデバイス、外部サービスなど、個々の対策はあるが、リスク対策を考えるとポイントソリューションではなく、どう全体としてリスクを排除するかが課題となる。
3. 近年注目を集めるアタックサーフェス管理に焦点を当て、企業IT全体が孕むリスクがどこにあり、攻撃者がどのような思考で攻撃を試みるかを理解する必要がある。
4. 本記事では、ハイブリッド／マルチクラウド時代の企業ITシステムのがはらむセキュリティリスクを整理して問題を明確化し、現代的なセキュリティリスク管理の在り方を指南する。

キーワード　・アタックサーフェス管理・ホワイトハッカー・ペネトレーションテスト実施教育

セキュリティ関連記事の読者層

本施策のターゲット

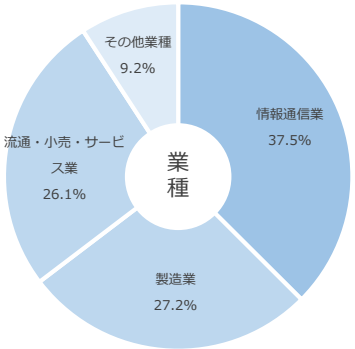
「脆弱性対策など」
に関心がある読者

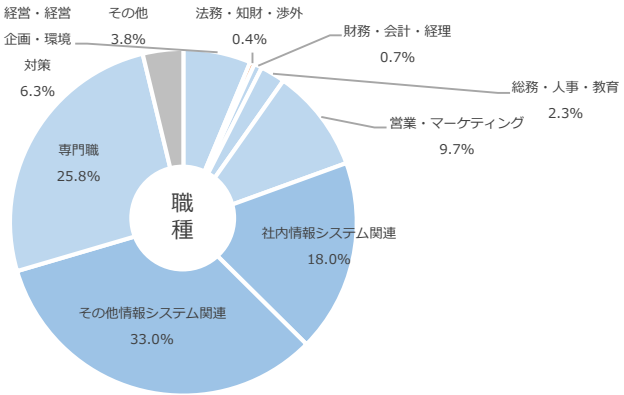
Intent

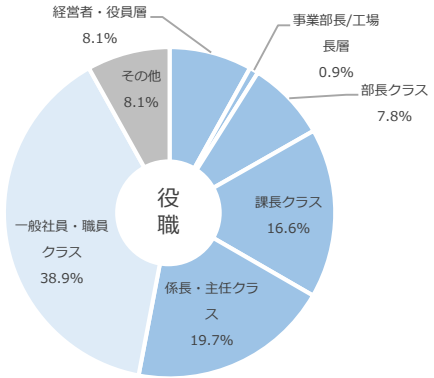
よく読まれている記事

- 「Windows 7」「Windows 8.1」もサポート終了へ、使い続けるとどれだけ危険？
- 任天堂、自社販売したWi-Fiルーターなどの利用中止呼び掛け　10年以上経過しセキュリティに問題
- iOS、macOSのセキュリティパッチ適用を　ゼロデイ脆弱性の修正あり　カーネルに問題発見
- ソフトウェア脆弱性管理の切り札、「sbom」はなぜ必要か?

Demographics







セキュリティ関連の出稿実績

ゼロトラスト時代のID管理　IDaaS選定に欠かせない3つのポイント

提供：HENNGE株式会社

IDaaSはコスト面だけでなく情報システム部門の負担軽減という意味でも魅力的だが、ノークリサーチの岩上氏は「導入を提言する際に強調すべき点は別にある」と指摘する。

その指摘から、“自社が本当に守りたいもの”を浮かび上がらせる方策と、情報システム部門が経営層や事業部門と距離を縮めるためのヒントが見えた。

実践企業3社の情シスが語る　「脱PPAP」を従業員と取引先から理解を得て進めるコツ

提供：HENNGE株式会社

「パスワード付きZIPファイルの添付」いわゆる「PPAP」からの脱却を目指す動きが民間企業の間で盛んになっている。

「脱PPAP」を実現した3社の情報システム部門担当者が集まり、実現までの道のりを本音で語り合った。

セキュリティ関連の出稿実績

“ゼロトラスト”は死んだ？　ノークリサーチ岩上氏に聞く「セキュリティの現在地と現実解」

提供：HENNGE株式会社

最近、「ゼロトラスト」という語をあまり聞かなくなったと感じる読者もいるだろう。ノークリサーチ岩上氏にその理由と背景を聞いたところ、システムへの侵入という最悪の事態を防ぐために今すべきことが明らかになった。

テレワーク従業員のスマホ、PCの守り方はこう変わる 管理のシンプル化を目指すには？

提供：エムオーテックス株式会社、SB C&S株式会社

事業継続のために急場しのぎでテレワーク環境を構築した企業がセキュリティリスクにさらされている。対策を強化するには抜本的な見直しと管理のシンプル化が必要だ。

セキュリティ関連の出稿実績

サイバー攻撃を受けてからじゃ遅い　今から企業が取り組むべきこととは？

提供：クラウドストライク株式会社

「アクセスブローカー」と呼ばれるサイバー犯罪者を起点にしたマルウェア攻撃が近年増加している。企業はこれにどう対抗すべきか。本稿は認証情報を標的にしたサイバー攻撃の実態と危険性を明らかにし、アイデンティティー保護に特化したセキュリティ対策を解説する。

スキだらけのクラウドに襲い掛かる脅威　ビジネスのためのセキュリティ戦術とは

クラウドストライク株式会社

コロナ対策やビジネススピードの向上を目指してクラウド移行を推進する企業が増えている。同時にクラウドセキュリティを講じることは必要不可欠だが、そもそもクラウドセキュリティとは何なのか。そして適切なクラウドセキュリティとはどのような対策なのか解説する。

セキュリティ関連の出稿実績

激化するランサムウェアをはじめとしたマルウェア攻撃になぜ「特権ID管理」が有効か？

提供：エンカレッジ・テクノロジ株式会社

ランサムウェアをはじめとしたマルウェア被害を報告する国内企業が増加する中、脅威の侵入を防ぐエンドポイントの保護は重要だが、侵入後を想定したセキュリティ対策も求められている。これに向けて特権ID管理が果たす役割を解説する。

これまでの定石は通用しない　IT部門から“見えづらい”環境のセキュリティをどう守る？

提供：トレンドマイクロ株式会社

サプライチェーン攻撃に関する被害報告が相次いでいる。サイバー攻撃者の標的が大企業だけでなく中小企業といったサプライチェーン関連企業にも拡大し、企業規模を問わず適切なランサムウェア対策が必要だ。

セキュリティ関連の出稿実績

「人手もコストもかけられない」企業でも容易に導入可能なEDRとは

提供：フォーティネットジャパン合同会社

サイバー攻撃が激化し、規模を問わずさまざまな企業が被害を受ける中、どのような対策をすべきか。「もはや予防措置だけでは不十分」という認識からEDRの導入を検討するものの、人材不足や運用負担の大きさを理由に諦めていないだろうか。

ランサムウェアに対する日本企業の“脆弱さ”　改善の鍵を握る3つのポイント

提供：クラウドストライク株式会社

ランサムウェア攻撃は今や企業にとって事業継続を脅かす重大リスクとなっている。被害増加の背景には何があるのか。そこから見えたランサムウェア対策のポイントとは。

セキュリティ関連の出稿実績

Webアプリケーション開発者に寄り添う次世代WAFの実力を探る

提供：フォーティネットジャパン合同会社

Webアプリケーションを狙うサイバー攻撃の高度化は、機械学習機能を組み込んだbotによる同時多発攻撃などとどまるところを知らない。従来のWAFでは防ぎ切れない攻撃にどのように立ち向かうべきなのか。

エンドポイントセキュリティ実現のポイント

提供：富士通株式会社

テレワークが進む中、エンドポイントにおけるセキュリティリスクへの対処が多くの企業の課題になっている。新しいタイプの脅威も登場する中で、ポストコロナ時代における新しいセキュリティ対策を紹介する。

セキュリティ関連の出稿実績

コストゼロから始められるセキュリティ強化ツールはどこまで「使える」か

提供：ジャスミー株式会社

忙しい「ぼっち情シス」が、今以上に仕事を増やすのは不可能に近いだろう。今ある環境で手間をかけずにテレワーク従業員の情報漏えい対策と就労管理を実現するというJasmy Secure PCは、ぼっち情シスを救う神の手になるだろうか。実際の使い勝手を見ていく。

いまセキュリティにプラットフォームが必要な理由

提供：クラウドストライク株式会社

サイバー攻撃の高度化が止まらない。企業はさまざまなセキュリティ製品を導入してきたが、新たな製品を追加し続けるのではなくプラットフォームで防御するという発想に転換する必要がある。

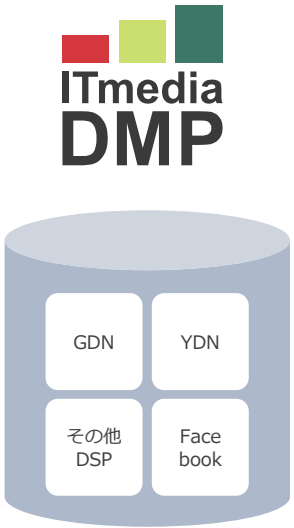
タイアップ記事メニューについて

1. 掲載イメージ
2. タイアップ記事のパターン
3. 当社タイアップ記事の特徴
4. 読者調査から見る、タイアップ記事制作のポイント
5. **【広告メニュー】**読者の課題を明らかにする読者調査とタイアップ記事のメニュー
6. **【広告メニュー】**読者の関心データに基づいた、大量PV保証型タイアップ記事メニュー
7. **【広告メニュー】**タイアップ記事でのアウェアネスからリード獲得まで行うメニュー
8. 記事制作スケジュール
9. キャンセル規定
10. 媒体規定

掲載イメージ

ITmedia エンタープライズ
TOPページ・各記事ページ

DSPやGDNなど
メディア外部のアドネットワーク



タイアップ記事

※イメージです。掲載位置を保証するものではありません。

タイアップ記事プランのポイント

訴求内容に応じた記事コンテンツを制作　豊富な掲載実績をもとに最適な企画をご提案いたします

▼記事コンテンツ例

有識者インタビュー・対談	調査結果とインサイト	イベントレポート	製品・サービス紹介	開発担当者インタビュー	導入事例
•業界の第一人者・識者に、いま企業が直面するビジネス環境の変化や課題についてお聞きしソリューションに沿って広く問題提起と課題感の醸成を狙う	•貴社の調査データ、またはITmediaで実施した調査結果と得られたインサイトを解説することで、客観的な数値や傾向をもって問題提起することで、客観的な根拠に基づいた説得力のある訴求が可能	•各種イベントやセミナーの発表内容や資料を記事化しイベント参加者以外にも広く訴求するレポート記事。イベントのアーカイブ化と幅広いターゲット層へのリーチを図る	•ソリューションについてインタビューし、課題の提起と、その解決策としての製品訴求を行う。 •製品・サービスの認知拡大、ブランド理解促進	•ソリューション開発担当者様へ、開発経緯やソリューションを取り巻く環境のリアルタイムな分析などをインタビュー。ソリューションに対する立体的な理解を喚起 •製品・サービスの認知拡大、ブランド理解促進	•実際にソリューションを導入しているユーザー企業に、導入に至る経緯や課題感、導入後の改善点をインタビュー。 •製品・サービスの認知拡大と、具体的な活用シーンの提示と検討導入への動機づけを狙う

※識者のアサインには別途アサイン費を頂戴する場合がございますので予めご了承下さい。
※あくまで一例です。ご要望に応じて貴社独自の企画案をご提案いたしますので、お気軽にお問合せ下さい。

※ITmedia エンタープライズに掲載するタイアップ記事に限り、ITmedia エンタープライズが実施した読者調査の結果を記事内で無償で利用することが可能です。詳しくは営業担当へお問合せください。

当社タイアップ記事の特徴

読者のことを最もよく知る編集者による企画・編集

日々メディアで配信しているニュース記事を執筆・編集しているメディア編集者がその知見を活かし、読者の理解を促しエンゲージメントを高めるコンテンツをご提案。制作作業に最後まで携わります。

効果的な読者導線

アイティメディアが有する数多くのサイト特性を生かした広告や、
「ITmedia DMP」に蓄積されている読者の行動データを活用したオーディエンス拡張配信などを組み合わせ、効率的な読者の閲覧を獲得します。

PVの保証

PV数を保証するメニューをご用意。キャンペーンの数値目標にコミットします。また、一度掲載期間が終了したタイアップ記事に読者誘導を再開することも可能です。

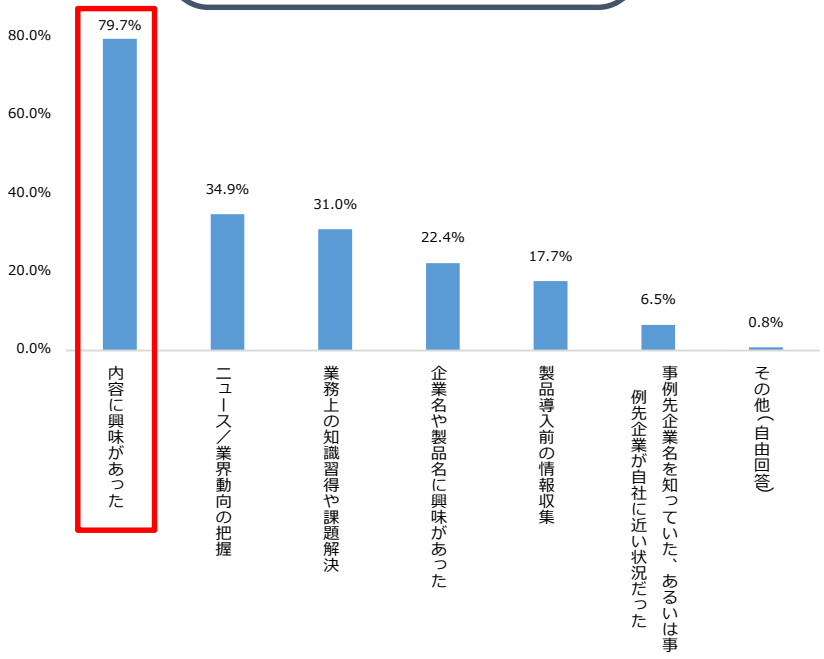
詳細なレポーティング

掲載期間終了後には閲覧レポートをご提供しますので、キャンペーンを適正に評価し、次回施策への活用が可能です。

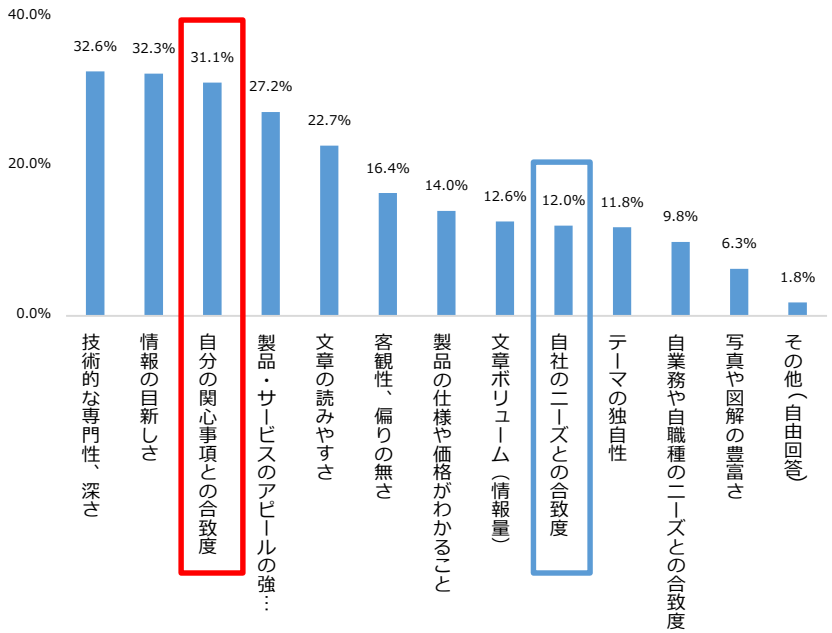
読者調査から見る、タイアップ記事制作のポイント

読者は企業名や製品名よりも**内容**を重視。会社のニーズより**読者自身のニーズとの合致度**を訴求するのがポイント

広告記事を閲覧した理由



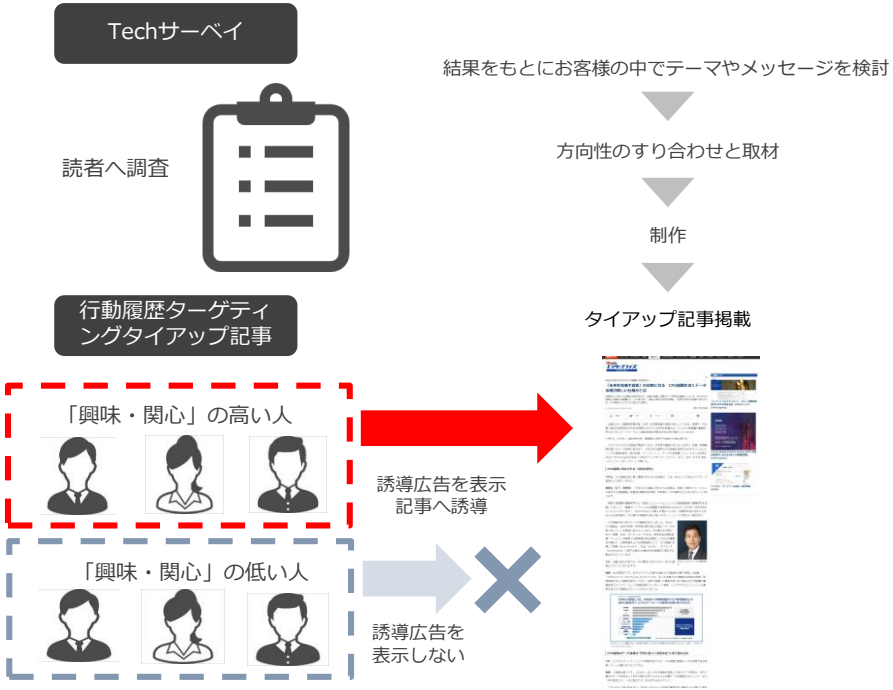
広告記事の満足／不満足の理由



読者調査2021年10月「広告記事（PR記事）の利用について」1423件

読者の課題を明らかにする読者調査とタイアップ記事のメニュー

- 読者調査を実施した結果をもとにタイアップ記事を制作。読者はどんな課題を持っているのか、どんなメッセージを出せば効果的かを見極め



実施料金

~~220万円~~ → 195万円（グロス税別）※特別価格

メニュー

提供メニュー①	**Techサーベイ**
定価	50万円（税別）
保証回答数	200件
想定回答収集期間	想定2週間～1か月
設問	最大10問　流し込み シングル、マルチ、テキストボックス　（必須／任意設定可能）
納品物	回答ローデータ ※回答データの成型および個人情報の取得・納品は行いません ※回答結果の二次利用可
備考	アンケートページへの誘導方法はお任せ頂きます。回答インセンティブを付けて実施いたします。インセンティブの内容は一任頂きます。
提供メニュー②	**5000PV保証 行動履歴ターゲティングタイアップ記事 「セキュリティ」関連コンテンツ関心者**
定価	170万円（税別）
保証PV数	5,000PV
掲載期間	最短1週間～想定2ヶ月（保証PVを達成次第終了）
メニュー	タイアップ記事　1本制作 約3000～4000字、図版3点以内（取材あり） 閲覧レポート（PV,UB,閲覧企業等）
制作期間	約1か月～1.5か月

読者の関心データに基づいた、大量PV保証型タイアップ記事メニュー

- 読者の行動データをもとに興味・関心の高い人だけを誘導するタイアップタイアップ記事
- 読者の行動データ（記事閲覧履歴）を元に「興味・関心」を特定「興味・関心」の高い人だけをタイアップへ誘導

「興味・関心の高い人」を中心に認知度を向上

興味・関心の高い人のみに誘導広告を表示するため、興味・関心を持つ人を中心に認知度を向上させる効果が期待できます。

アイティメディアへ訪れたことがない人へもアプローチ

読者の行動データを外部サービスへ連携。拡張配信を行うことで、アイティメディアに訪れたことのない、
同じ「興味・関心を持つ人」を外部メディアで捕まえる事が可能に。読者のリーチが広がります。

実施料金	
~~300万円~~ → 240万円（グロス税別）※特別価格	

メニュー	
提供メニュー	行動履歴ターゲティングタイアップ記事
保証形態	PV保証
保証PV	20,000PV
掲載期間	最短1週間～想定2ヶ月（保証PV達成次第終了）
仕様	タイアップ記事　1本制作 約3000～4000字、図版3点以内（取材あり） コンテンツ掲載費含む 閲覧レポート（PV,UB,閲覧企業等）

- キーワードは自由に選定可能ですが、弊社内でのUB数が10万UBを下回る場合、調整をお願いする場合がございます。
- 本サービスは、オーディエンスの拡張配信及び、外部メディアを利用したプランとなります。
- 外部メディアの利用先はアイティメディアが内容に応じて、最適な配信先を選択します（指定出来ません）
- 誘導原稿はアイティメディアが準備いたします（事前の確認・指定はできません）
- 誘導広告は保証PV達成次第、掲載を停止いたしますが、最低1週間は掲載を保証いたします。

行動履歴ターゲティングタイアップ誘導イメージ

ターゲット・オーディエンス＋類似ユーザー誘導することで掲載効果UP

本施策のターゲット

「●●●」
に関心がある読者

ITmedia DMPで
オーディエンスを抽出

ITmedia DMP

①ターゲティング誘導

「興味・関心の高い読者」に絞って、
アイティメディアの各メディアから誘導

タイアップ記事

②外部サービスでリターゲティング

ITmedia DMPで抽出した**「興味・関心者」**を
DSPやGDNで**リターゲティングして誘導**

オーディエンスを連携

GDN
YDN
その他
DSP
Face
book

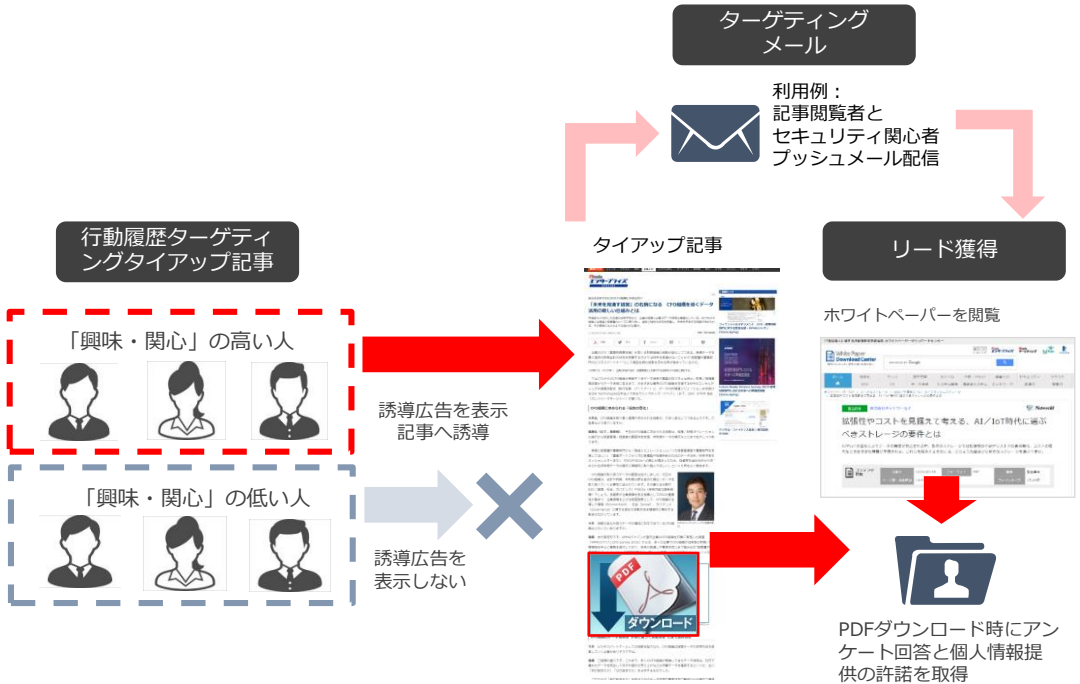
③類似ユーザーに拡張

オーディエンス拡張機能を利用し、**より多くの**
「興味・関心者」をタイアップ記事へ誘導

※DSP・SSPを利用する場合は、独自のホワイトリストを利用し、面の安全性を確保しています

タイアップ記事でのアウェアネスからリード獲得まで行うメニュー

➢ リード獲得とアウェアネス向上施策をワンパッケージにした、
『セキュリティ』に関心のある読者への訴求に最適な施策



実施料金

~~240万円~~ → 200万円（グロス税別）※特別価格

メニュー

提供メニュー①	**LeadGen. Segmentサービス**
定価	基本料10万円＋リード料40万円（税別）
保証リード数・属性	50件　属性保証：エンドユーザー（IT関連業除く）
掲載期間	想定2ヶ月（保証リード数を達成次第終了）
入稿期間	約2週間～1カ月
必要コンテンツ数	ホワイトペーパー2本以上
提供メニュー②	**5000PV保証 行動履歴ターゲティングタイアップ記事 「セキュリティ」コンテンツ関心者**
定価	170万円（税別）
保証PV数	5,000PV
掲載期間	最短1週間～想定2ヶ月（保証PVを達成次第終了）
メニュー	タイアップ記事　1本制作 約3000～4000字、図版3点以内（取材あり） 閲覧レポート（PV,UB,閲覧企業等）
制作期間	約1か月～1.5か月
提供メニュー③	**ITmedai エンタープライズ　ターゲティングメール**
定価	行動履歴データ利用単価50円×4,000通　定価20万円（税別）
配信数	4,000通保証

【補足】LeadGen. Segment サービス概要

ターゲットリードを大量・確実に獲得

キャンペーン設計	▶	リード獲得	▶	リード納品・活用

ターゲット属性

業種職種、従業員数など、納品対象となる属性を設定

掲載コンテンツ

リード獲得に利用するコンテンツの内容と本数を確認

保証件数

ご予算、ターゲット属性、コンテンツ数に応じて、保証件数を設定

ターゲットに向けてメールなどで貴社コンテンツをオファー

ホワイトペーパーや編集タイアップを閲覧

コンテンツダウンロード／閲覧時にアンケート回答と個人情報提供の許諾を取得

獲得したリードは管理サイトからダウンロードできます（日次更新）

【補足】リード獲得／提供の仕組み

※ サービスによっては、週1回または隔週の納品になる場合もございます。

タイアップ記事制作スケジュール

想定スケジュール

掲載までのスケジュールはお申込み後別途ご案内いたします。詳細については各営業担当にお問い合わせください。

※「制作～校正」の期間中には初校・再校・念校が含まれます。念校では“再校時にご依頼いただいた修正内容が反映されているかどうか”の最終確認を行っていただきます。

ご注意事項

・制作した記事広告の著作権は、当社および制作スタッフ（ライター、カメラマンなど）に帰属します。
・印刷物でのご利用は二次利用費が発生いたしますので、利用をご希望される場合は、担当営業までお問合わせ下さい。
・著名人のアサインや、遠方への取材などが必要な場合は、別途料金を頂戴いたします。
・お申し込み後、広告主様の都合で合意いただいた内容から大きく変更を行う場合、以下の追加費用が発生する場合がございますのでご了承ください。

・初校の出し直し：¥300,000
・念校以降の修正：¥100,000
・再取材のご要望についてはご相談下さい。 ※全て税別・グロス

キャンセル規定

広告商品の発注書受領後、広告主様のご都合でキャンセルを行う場合は、下記の料率でキャンセル料を申し受けます。

商品			キャンセル料金	主な対象商品（下記以外の商品はお問合せ下さい）
ディスプレイ広告、メール広告			入稿締切期日まで：50% 入稿締切期日以降：100%	各種ディスプレイ広告、メール広告
記事企画 Special（タイアップ記事広告）			初校提出前まで：広告料金（制作費、掲載費、誘導費を含む一式）の50% 初校提出以降：広告料金（制作費、掲載費、誘導費を含む一式）の100%	期間保証型タイアップ PV保証型タイアップ
リードジェン	件数保証型	リード獲得	キャンペーン開始前まで：広告料金（基本料金＋リード料金）の50% キャンペーン開始後：広告料金（基本料金＋リード料金）の100%	LeadGen. Basic / Segment ITmedia リサーチ
		制作オプション	初校提出前まで：広告料金（制作料金）の50% 初校提出以降：広告料金（制作料金）の100%	LG. Segment オプション 編集タイアップ制作 LG. Segment オプション ホワイトペーパー制作
		その他オプション	キャンペーン開始前まで：広告料金（オプション料金）の50% キャンペーン開始後：広告料金（オプション料金）の100%	LG. Segment オプション アンケートカスタマイズ LG. Segment オプション テレマーケティング
	期間保証型	ホワイトペーパー	キャンペーン開始前まで：広告料金の50% キャンペーン開始後：広告料金の100%	TechFactory 期間保証型LGサービス
		タイアップ	初校提出前まで：広告料金の50% 初校提出以降：広告料金の100%	TechFactory 期間保証型LGサービス
	長期リード獲得サービス		申込み金額の半額費消まで：広告料金（リード料金）の50% 申込み金額の半額費消以降：なし	LeadGen. Segment 長期利用プラン

媒体規定

広告の掲載につきまして
・広告の掲載可否（掲載中の掲載停止の可否を含みます）につきましては、アイティメディア株式会社が広告掲載基準に基づき判断し決定いたします。
・掲載された広告およびリンク先の内容についての一切の責任は、広告主が負うものとします。
・同ページに複数の広告が掲載される場合、同業種競合調整はいたしません。ご了承ください。

広告掲載基準

1．掲載に関する基本基準
（1） 弊社及び弊社の運営するサイトの信頼と品位を損なう表現・内容を含む広告は掲載しません。
（2） 法令、政令、省令、条例、条約、業界規制等に違反する表現、内容を含む広告は掲載しません。
（3） 虚偽、誇大、もしくは誤認、錯誤される恐れのある表現・内容を含む広告は掲載しません。
（4） 以下の類を含む、公序良俗に反する表現・内容を含む広告は掲載しません。
・人権を侵害する恐れのある表現・内容
・名誉毀損、プライバシーの侵害、信用毀損、誹謗中傷、その他不当な業務妨害となる恐れのある表現・内容
・非科学的、迷信に類するもので、消費者を惑わせたり不安を与える恐れのある表現・内容
・宗教信仰による布教活動を目的としている表現・内容
・暴力、賭博、麻薬、売春などの犯罪行為を肯定、美化した表現・内容
・醜悪、残虐、猟奇的で不快感を与える表現・内容
・性的に露骨、わいせつ、セクハラに該当するおそれのある表現・内容
・風紀を乱し、犯罪を誘発するおそれのある表現・内容
・賭博行為および投機等、射幸心を著しく煽る恐れのある表現・内容
（5） 消費者を混乱させる恐れのある表現・内容を含む広告は掲載しない。
（6） 団体・個人の氏名、肖像、写真、談話、商標、著作物などを無断で使用している恐れ、または権利侵害のある恐れのある表現・内容を含む広告は掲載しません。
（7） 広告内容及びリンク先に関し運営者が不明、または責任所在が明らかでない広告は掲載しません。
（8） その他、弊社が不適当と判断した表現・内容を含む広告は掲載しません。
（9） 個人サイトの広告は掲載しません。

2．掲載の停止
（1） 掲載開始後に以下の事由が生じた場合、アイティメディアは広告掲載を停止することがあります。なお、アイティメディアは、本項目に基づく掲載停止に関し、広告主に対し何らの責めを負うものではありません。
① 広告に含まれるリンク先サイトが、アイティメディアの責によらない理由によりデッドリンクとなっているとき
② 広告に含まれるリンク先サイトがウイルスに侵された等、何らかの不具合が発生した場合
③ 掲載を継続することにより第三者もしくはアイティメディアに損害が生じる恐れがある、または第三者もしくはアイティメディアの信用を損なう恐れがあるとアイティメディアが判断したとき
④ 法令・業界規制等の改定、その他の掲載後に生じた事情の変更により、広告の内容が広告掲載基準に違反することとなったとアイティメディアが判断したとき
⑤ 広告掲載規準に違反すると、アイティメディアが判断したとき
（2） 前項目（1）に基づき掲載停止した期間における広告主の広告掲載料の支払い義務は、免除されないものとします。

3．掲載の中断
（1） 掲載開始後に以下の事由が生じた場合、アイティメディアは広告掲載を中断します。
① 火災、停電、天災地変、戦乱等の非常事態、インターネットトラフィックの過大等の不可抗力により広告配信サーバ又は広告配信システムが故障し、または機能不能となった場合
② 広告配信サーバ又は広告配信システムの定期または緊急の保守・点検を行う場合
③ 第三者によるハッキングやクラッキング、不正アクセス等、アイティメディアの責に帰すことのできない事由により広告配信サーバ又は広告配信システムに障害が生じた場合
④ その他アイティメディアが広告配信サーバまたは広告配信システムの一時的な中断が必要と判断した場合
（2） 前項目に基づく中断により、広告主の申込条件通りに広告掲載が不可能になった場合、または掲載された広告からリンク先への接続ができない場合等、広告掲載契約における当社の義務を履行できない事象が生じた場合におけるアイティメディアの義務は、可能な限り、当該事象を治癒することに限定されるものとします。また、当該事象がアイティメディアの故意または重大な過失によることが明らかである場合を除き、アイティメディアは当該事象に起因する広告主の損害について一切責任を負わないものとします。