

2025年
8月

複数社協賛型デジタルイベント
セキュリティ



ITmedia Security Week 2025 夏

“侵入前提という言葉”を誤解してはいけない
「守りを固める」再点検ポイントと対策アプローチ

開催日 : 2025年8月25日(月)~9月1日(月)

申込締切 : セッションプラン最終締切 : 2025年7月28日(月)
リストプラン最終締切 : 2025年8月20日(水)

運営 : アイティメディア株式会社

ITmedia Security Week 2025 夏

主催メディア



会期

2025年8月25日(月)~9月1日(月)

申込締切日

セッションプラン最終締切：2025年7月28日(月)
リストプラン最終締切：2025年8月20日(水)

事前申込者数

約1,000名想定

想定視聴者属性

ユーザー企業の経営／経営企画、社内情シスのマネージャ／担当者、セキュリティ担当のシステムエンジニア、Slerなど

ご協賛プラン

- ・ プラチナプラン | 350万円
- ・ ゴールドプラン | 240万円
- ・ 全リストプラン | 240万円
- ・ セクションリスト | 200万円

過去開催実績

- <ITmedia Security Week 2025 冬>
- ・ お申込みページ▶[こちら](#)
 - ・ 開催報告書▶[こちら](#)

企画趣旨

“侵入前提という言葉”を誤解してはいけない 「守りを固める」再点検ポイントと対策アプローチ

サイバー攻撃が頻発する中、全ての組織が標的になり得ることに改めて危機感を強めている方も多いことでしょう。
特に2024年末から年始に多発したDDoS攻撃は記憶に新しいところです。

IoTボットネットが使われた一連の事件では、被害を受けるばかりか攻撃に加担するリスクもあることから、
機器の設定確認など「**基礎**」の**重要性**が指摘されました。

昨今は「侵入前提」という言葉も浸透していますが、これも言うまでもなく「備えが甘くなっている」という意味ではありません。
自社の責任範囲をはじめ、改めて**基礎を見直して**おくべきでしょう。

ITmedia Security Week 2025 夏では
「**侵入を防ぐ**」「**安全な状態を保つ**」**手段**を網羅。
「**再点検すべきポイント**」を徹底解説します。

※本内容は予告なく変更または実施を中止する場合がございます。あらかじめご了承ください。ご不明点等は営業担当までお問い合わせください。

“侵入前提という言葉”を誤解してはいけない「守りを固める」再点検ポイントと対策アプローチ

1. 「DXに走る日本企業、かつてないほどに高まるサイバーセキュリティリスク」	#DXとサイバーセキュリティリスク #サイバーセキュリティ経営 #サイバーセキュリティ体制構築・人材確保
2. 侵入、即アウトにならないためのゼロトラスト	#EDR #NDR #XDR #ネットワークセキュリティソリューション、#暗号関連全般 #認証系全般
3. “ID”こそが次の強化ポイントだ	#リスクベース認証 #IDaaS #ID管理・統制/特権ID管理/統合認証基盤/シングルサインオン
4. クラウドを守るために、平時のいま行うべきこと	#SaaS、PaaS、IaaSほかクラウド&セキュリティ関連全般
5. サイバーハイジーン向上のためのアタックサーフェス管理	#アタックサーフェスマネジメント（ASM） #VPNセキュリティ関連 #脆弱性マネジメント #レッドチーム
6. 次世代エンドポイント保護を実現せよ	#ディテクション&レスポンス #マルウェア検知ソリューション全般 #情報漏えい対策 #資産管
7. 脱PPAPの現在地	販売終了
8. ランサムウェア攻撃の入口対策～やった気で終わらず、攻めの視点で再確認～	#脅威エクスポージャー管理製品 #SOC #SOAR #脅威インテリジェンス
9. ランサムウェア攻撃の出口対策～待つだけでは本当の回復力は身に付かない～	#バックアップソリューション SOAR #SIEM #SOC #DLP（情報漏えい対策）製品全般
10. 組織の輪を乱す、内部不正を見逃すな	#UEBA #DLP #メールセキュリティ #フォレンジック #ログ管理 #ログ解析
11. 専用ゾーン	販売終了
12. “セキュリティ運用自動化”が組織全体を変える	#AIによるセキュリティ運用自動化 #SOAR #UEBA
13. 人任せにしないマネージドサービスの要件	販売終了 #MSP #MDR #SOC

※本内容は予告なく変更または実施を中止する場合がございます。あらかじめご了承ください。ご不明点等は営業担当までお問い合わせください。

概要

DXに走る日本企業、かつてないほどに高まるサイバーセキュリティリスク

世界中を混乱させてきたコロナ禍を境にわたしたちの生活様式はすっかり変わってしまいました。企業もより柔軟な働き方へのシフトを迫られています。国を挙げてDXが推進され、デジタルへの依存が深まっていくでしょう。デジタルが前提ともいえるポストコロナの「新常態」ではサイバーセキュリティのリスクがかつてないほど高まっており、サイバー事案が急増しています。さらにAIを悪用したサイバーセキュリティ攻撃も新たな段階に入ろうとしています。それはわたしたちの想像を遥かに超えたものとなるでしょう。直面するこのリスクをどのようにマネジメントし、有事にはどう対処して、説明責任を果たしていけばいいのでしょうか。

キーワード

DXとサイバーセキュリティリスク/サイバーセキュリティ経営/NIST2.0フレームワークを活用したセキュリティ体制の整備/AIを悪用したサイバーセキュリティ攻撃の激化/インシデント対応能力の作成・計画・運用/エンタープライズリスクマネジメント/サイバーセキュリティ体制構築・人材確保

視聴者の抱える課題

- デジタル前提の「新常態」でも持続的な成長を追求するにはサイバーセキュリティ施策の抜本的な見直しが求められている
- 事業部門主導でDXの取り組みが推進されているがサイバーセキュリティの構築・維持が懸念される
- サイバー事案が急増しているが、自社が攻撃された場合、迅速に復旧できるのか？ステークホルダーへの説明責任は果たせるのか？
- ランサムウェア攻撃を受けた場合、業務を優先して取り引きすべきか、事後の公表はどうする？
- 経営層のサイバーセキュリティに関する意識改革が上手く進められない
- 自然災害や事故への備えは全社を挙げて取り組んでいるが、サイバーセキュリティに関しては情報システム部門に任せきり
- サイバーセキュリティに関する専門人材が不足している

基調講演案

デジタル活用によるビジネスの変革（DX）や新しい働き方の実現するために不可欠なサイバーセキュリティの取り組みを企業の方からご紹介いただきます。

概要

侵入、即アウトにならないためのゼロトラスト

攻撃者が最も好むシステムとは、侵入しただけで全てのリソースにアクセスできるような境界防御モデルかもしれません。逆に言えば、侵入を許したとしても、個別のリソースにそれぞれ境界が用意され、ログインのためにはパスワードだけでない、複数の認証が行われるようなシステムであれば、侵入したとしてもより弱い企業に攻撃対象が移るかもしれません。これこそが、ゼロトラストのメリットです。

本セクションでは、「ゼロトラスト」をキーワードに、検討段階、導入段階において有効な製品を紹介するとともに、セキュリティ識者による移行期での防御ポイント、攻撃者の視点を紹介しつつ、組織におけるゼロトラストの理解度を高めるにはどうすれば良いのかを掘り下げ、ゼロトラスト導入を成功させる秘訣を明かします。

キーワード

EDR (Endpoint Detection and Response)、NDR、XDRなどディテクション&レスポンス) 系全般/ネットワークセキュリティソリューション全般
/ファイアウォール、IDS、IPS、セキュリティスイッチ、ルーター製品/セキュリティの仮想アプライアンス全般/VPNソリューション
/IDaaS (Identity as a Service)/BYOD/暗号関連全般（鍵管理も含む）/ゼロトラスト・ネットワーク構築系ソリューション全般/シフトレフト系/認証系全般

視聴者の抱える課題

- ゼロトラスト導入において、ノウハウが充実しつつある状況ながら、どのように自社にフィットさせていいかわからない
- 移行期におけるセキュリティが心配
- 実際に移行した組織において発生した「落とし穴」を知りたい

基調講演案

ゼロトラストに向かっている途中の、企業における状況を語っていただく。また、最終完成形の理想よりも、そこに向かうための第一歩として、どのような視点を持つのが重要かを語っていただく。加えて、ゼロトラストの導入のため、組織内でどういうメッセージを現場や経営層に向け発信するのがよいか、アドバイスをいただく。

概要

“ID”こそが次の強化ポイントだ

IDを“パスワード”という記憶情報のみに頼っていませんか。システムの“衛生管理”を考えれば、侵入される前にこそ、ID管理や認証機能を強化しておく必要があります。ID/パスワードは最も狙われる場所になりつつあります。フィッシングによるID/パスワードそのものの窃取だけでなく、認証した状態そのものを盗む専門の攻撃グループがサイバー裏社会で幅を利かせています。攻撃者の振る舞いを考えると、認証情報を盗むタイミングと不正侵入の時期が異なることも増え、「侵入経路は不明」と書かざるを得ない事例が増えてきています。これでは、顧客にも取引先にも説明責任が果たせません。本セクションでは、記憶だけに頼らない「多要素認証」や最新技術である「FIDO 2.0」「パスキー」などの認証技術を考えるとともに、これまで見過ごされがちだったアイデンティティ（ID）管理と統制を考えるきっかけを提供します。セキュリティの基礎でもあり、ゼロトラストでも重要な「アイデンティティ」に関わる最新技術を学んでみませんか。

キーワード

リスクベース認証/IDaaS（ポリシー決定ポイント（PDP）／ポリシー実施ポイント（PEP））/ID管理・統制/特権ID管理/統合認証基盤/シングルサインオン/FIDO対応製品／パスキー対応製品/ゼロトラストに関連するID/Active Directory関連ソリューション/認証に伴うログの管理

視聴者の抱える課題

- いますぐできるセキュリティ強化策を知りたい
- パスワード管理を行えていない
- 従業員のパスワードが漏れている
- サービスにおいて多要素認証を提供できていない
- ゼロトラスト実現にあたりID管理／認証ソリューションを知りたい
- FIDO／パスキーなど最新の技術を知りたい
- IDaaSについてを知りたい

基調講演案

多要素認証を入口としつつ、その先にあるアイデンティティ管理／統制における重要なポイントを語る。ユーザー事例においては、社内でのアイデンティティ管理の実態や、B2C企業における利用者に見えるアイデンティティの状況など、実際の事例を語っていただく。

概要

クラウドを守るために、平時のいま行うべきこと

日本でも事業が完全に止まってしまいうレベルのインシデントが多発しており、クラウドセキュリティの本気度が事業存続の鍵となりつつあります。単なるソリューション導入に限らず、人による判断が重要な場合もあるでしょう。そのために必要なものを平時に用意するためには、全組織が一丸となる必要があります。当たり前となったクラウド利用には、抜けや漏れのないセキュリティが必要です。そのためには、攻撃を受けていないであろういまこそ、対策を進めるべき時です。本セクションでは、クラウドと自社システムを守るためのさまざまなソリューションの最新情報を学ぶとともに、いま最も必要な、優先度の高いソリューションを把握できる情報を集め、全員で組織のありたい姿により近づける手助けをします。

キーワード

SaaS/PaaS/IaaSほかクラウド＆セキュリティ関連全般（Office365などと連携する製品も含む）/セキュリティの仮想アプライアンス全般/SASE（Secure Access Service Edge）/SDP（Software Defined Perimeter）/SWG（Secure Web Gateway）CASB/CSPM/SSPM/暗号関連全般（鍵管理も含む）

視聴者の抱える課題

- ・ いま検討している、完了しつつあるクラウドシフトにおける「認識の穴」「システムの穴」に気が付くためのソリューションをここで知る。
- ・ 「視聴者が気が付いていないことに気が付ける」ことを目指す。
- ・ クラウドシフトのために組織が／CISOが考えるべきガバナンスや評価のための組織づくりへのヒントを提供する。

基調講演案

クラウドセキュリティが指すものが多種多様になっている状況で、特に中小規模の組織が優先度を高めて考えるべきクラウドセキュリティのイメージをつかめる講演を行う。

概要

サイバーハイジーン向上のためのアタックサーフェス管理

サイバーハイジーンとは、システムの「免疫力」を意味します。侵入後の対策だけでなく、侵入されないための健康維持が重要な時代となりました。この力を手に入れておけば、侵入された場合でも状況を把握し、対策が可能となるはずです。そのためにいま必要なのは、注目されているキーワードでもある「アタックサーフェス管理」でしょう。

「敵を知る」もさることながら、最も重要なことは「己を知る」こと。資産管理情報をセキュリティに活用し、「敵から見た己の姿」をコントロールできることが必要な時代です。攻撃を止めるためには、既に攻撃者は社内にまで到達していると考えることも必要です。その前提に立ったとき、必要なものはソリューションと、組織が一丸となりアタックサーフェスを意識することなのではないでしょうか。

絶対に侵入させない守り方から、広がる「アタックサーフェス」を理解することで、これをどう管理し、検知を行い、行動を止めていくかを考えてみましょう。

キーワード

アタックサーフェスマネジメント（ASM）/EDR／XDR / VPNセキュリティ関連/脆弱性マネジメント/メール対策製品/Web改竄対策/ペネトレーションテストサービス/レッドチーム

視聴者の抱える課題

- 次に何をすべきか悩む組織。アタックサーフェス管理というキーワードにピンときている、Security Week視聴者の中でもアンテナの高い視聴者層に満足される情報を提供する。
- 一度やられた組織など、現時点でどのような対策が取れるのか、先端事例を知りたい方に向ける

基調講演案

アタックサーフェスが意図せず広がり、管理ができていないという現状を把握するための情報を伝える。「見える化」を意識していないとこんなところに落とし穴がある、といった実例や、今後どのような心構えが必要なのかを、先端をウォッチする識者の目から伝える。

概要

次世代エンドポイント保護を実現せよ

サイバー攻撃の高度化はエンドポイントセキュリティを次なるフェーズへと進めています。これまではフィッシング対策製品やEDRをはじめとしたエンドポイント保護対策製品などを導入すれば「ひとまず安心」と考えられていたかもしれませんが。

しかしAIなどの発展に伴いサイバー攻撃の質と量が激化する今、EDRによる検知の回避といった高度な攻撃が進み、従来の防御策は通用しなくなってきています。こうした課題がある中、私たちは受け身の姿勢から脱却し、脅威を検知するための仕組みを多層的に整備するなど技術・組織の両面で積極的に整えていく必要があるでしょう。

エンドポイントセキュリティにおける喫緊の課題を明らかにし、これに向けた有効な対策を講じるための実践的な知識やノウハウを提供します。

キーワード

EDRやXDRなどxDR（ディテクション&レスポンス）系全般/マルウェア検知ソリューション全般（次世代アンチウイルス含む）/フィッシング対策製品全般/情報漏えい対策全般/資産管理系全般/ネットワークのマイクロセグメンテーション関連製品/BYOD

視聴者の抱える課題

- これまでウイルス対策ソフト導入（or EDR）とバックアップ程度しか対策をしていなかった
- 昨今の被害状況を見て不安だが何をすればいいか分からない
- エンドポイントデバイスの防御手法、脅威の検知手法を知りたい
- 情報漏えいをなんとしても防ぎたい
- 情報漏えいを防ぐためマイクロセグメンテーションを学びたい
- 社内にある資産を把握していない、脆弱性を把握していない
- 脆弱性が発表されても、なにをしていいのか分からない
- 脆弱性が発表されても、対象となる機器がどこにあるのか分からない
- フィッシングから利用者／組織を守る方法が分からない
- EDR導入後の運用に課題を持っている
- EDRを回避するようなサイバー攻撃にどう対処するべきか分からない

基調講演案

サイバー攻撃の高度化が進んでおり、従来のエンドポイントセキュリティ対策では通用しないケースが登場していることを事例を交えて説明していただき、これに対処するための実践的な知識やノウハウを提供する。

概要

脱PPAPの現在地

中央省庁は2020年、パスワード付きZIPファイルをメールに添付して送り、その直後にファイルを解凍するためのパスワードをメールで送る方式、いわゆる「PPAP」を廃止する方針を打ち出しました。これをきっかけに大手企業を中心に「脱PPAP」のブームが巻き起こり、一時期大きな話題を呼んだのは記憶に新しいでしょう。

あれから4年が過ぎましたが、企業の脱PPAPの進捗はどうなっているのでしょうか。また、依然としてPPAPを続ける企業のハードルとは何があり、PPAPの代替策として私たちはどのような手段を取るのがよいのでしょうか。本セクションは脱PPAPの現在地を明らかにします。

キーワード

脱PPAP

販売終了

視聴者の抱える課題

- PPAPの効果的な代替策を知りたい
- PPAPの代替策のメリット／デメリットをそれぞれ比較・検討したい
- PPAPをやめるべき理由を知りたい
- 従来の商習慣や取引先との関係性もあり、PPAPをやめられない
- PPAP問題についてあらためて知りたい

基調講演案

なぜPPAPが廃止されるようになったのか、その問題点を振り返りつつ、中央省庁の「PPAP廃止宣言」から4年たった今、企業における脱PPAPの進捗はどうなっているのか。効果的な代替策は何かをお話しいただく。

概要

ランサムウェア攻撃の入口対策～やった気で終わらず、攻めの視点で再確認～

ランサムウェア攻撃の脅威は激化していますが、その侵入経路についてはここ数年で大きな変化はありません。取引先などのサプライチェーンや電子メール経由、VPNの脆弱性、サービスアカウントの乗っ取りなどある程度はパターン化されています。

では、なぜ依然として被害は発生してしまうのでしょうか。それは自社システムの“穴”を「自分たちではふさぐことができている」とやった気になってしまっているからにほかなりません。この意識を改革するには、視点を変えて攻撃者の気持ちになって自社のウィークポイントを洗い出すのが重要でしょう。

多様な攻撃経路をあらためて整理し、ランサムウェア攻撃のプロセスを明らかにしたうえで、包括的に穴をふさぐための有効な対策を考えます。

キーワード

脅威エクスポージャー管理製品/攻撃対象領域管理（ASM）製品/脆弱性管理製品/ SOC / SOAR / SIEM / EDR製品全般/ XDR /アンチウイルスソフト製品全般（NGAVなど） / 脅威インテリジェンス/認証関連製品（IDaaS、特権ID管理） / CASB /ファイアウォール/ SWG（セキュアWebゲートウェイ） / SASEソリューション/ EPP（エンドポイント保護プラットフォーム）製品全般/メールセキュリティ製品全般

視聴者の抱える課題

- ランサムウェア攻撃の侵入経路のうち注意すべき箇所を知りたい
- どのような脆弱性からランサムウェア攻撃が実行されるのかを知りたい
- ランサムウェア攻撃の侵入から発覚までの攻撃プロセスを学びたい
- サプライチェーン経由でのランサムウェアの侵入を防ぎたい
- 従業員のITリテラシーを向上させたい
- サイバー攻撃に対処するセキュリティ人材が不足している、またはいない
- ランサムウェアをはじめとしたマルウェアの侵入を防ぎたい
- ランサムウェア攻撃を適切に検知したい
- ランサムウェアの被害を最小限にとどめたい

基調講演案

ランサムウェア攻撃の侵入経路を整理。攻撃プロセスなどを詳細に解説することでどのポイントでどのような防御が有効かなど実践的な対策を語っていただく。

概要

ランサムウェア攻撃の出口対策～待つだけでは本当の回復力は身に付かない～

全ての企業がランサムウェア攻撃の標的になる危険がある今、バックアップをはじめとした侵入を前提にしたセキュリティ対策を講じることは必要不可欠でしょう。しかし最近ではバックアップを狙うランサムウェア攻撃も増えてきており、「バックアップを取っているから安全」と考えるのはむしろ非常に危険です。

「バックアップを取る」という受け身の対策を講じるだけにとどまらず「取得したバックアップをきちんとリストアできるかどうか」「事業復旧に向けた訓練を実施しているかどうか」など多岐にわたる備えをしてこそ、攻撃から回復できるのです。

ランサムウェア攻撃に強いレジリエンスを持った企業組織になるために何が必要か。“出口対策”の強化に役立つ知識やノウハウをお伝えします。

キーワード

バックアップソリューション/ SOAR/ SIEM / SOC / EDR製品全般/ XDR / SASEソリューション/ DLP（情報漏えい対策）製品全般

視聴者の抱える課題

- インシデント発生時の対応ノウハウが確立されていない
- ランサムウェアの被害を最小限にとどめたい
- ランサムウェアによって機密情報を窃取された後の対応が分からない
- ランサムウェア攻撃に遭った場合、被害状況を適切に把握したい
- ランサムウェア対策に有効なバックアップ手法について知りたい
- ランサムウェア被害後にデータおよびビジネスを迅速に復旧させる方法を知りたい

基調講演案

ランサムウェア攻撃におけるバックアップ戦略のポイントを、リストアや復旧訓練の勘所と合わせてお話しいただく。

概要

組織の輪を乱す、内部不正を見逃すな

脅威は外からやってくるもの、そう思い込みたいのは事実です。しかし、多くの企業で内部不正を発端とした事件が次から次へと報告されています。明確な悪意が内部から発生した場合、あなたの組織ではそれを見つけることができるでしょうか。これは本当に難しい課題です。

「1枚の割られた窓ガラスを放置することで、いずれ街が荒廃する」――この割れ窓理論は、組織の中でも起き得ます。従業員を監視してコントロールし、警告を与えるには、組織のポリシーとソリューションの力を活用し、どの程度ガバナンスを強めるかがポイントです。このセクションでは、組織の健康状態を維持するためのUEBA、DLP、メールセキュリティをはじめ、従業員が普段使うツールに対しどのような対策が打てるのかを考え、組織が一人称で考える力を手に入れるための知識を学びます。

キーワード

UEBA/DLP/メールセキュリティ/フォレンジック/ログ管理/ログ解析

視聴者の抱える課題

- 内部不正対策の仕組みを持っておらず、発見する術もない組織が、その第一歩を知りたい
- 万が一何かが起きた時、どこに聞いていいのかわからない

基調講演案

組織のポリシーをどうやって作るのか。また、不正を発見した時に組織としてどう警告するのか。具体例を示しながら講演していただく。

ご注意事項

※本セクションのご協賛プランはプラチナプラン・全リストプランのみとなります。

※本内容は予告なく変更または実施を中止する場合がございます。あらかじめご了承ください。ご不明点等は営業担当までお問い合わせください。

概要

“セキュリティ運用自動化”が組織全体を変える

セキュリティ人材不足は解決することはないかもしれませんが、今後もこれまで以上に熾烈な脅威がやってきます。平時の今こそ、攻めのセキュリティとして、AIや機械学習を基にした「運用の自動化」を、解決策としませんか。

運用の自動化は、もしかしたら経営層の方がそのメリットを把握しているかもしれません。現場も経営層も、向かう方向や理想は変わらないはず。それでも上手くいかない理由は、技術やソリューションだけでなく、コミュニケーションや組織作りなどにあるのかもしれません。

運用の自動化こそ、平時に考えておかねばなりません。AIによる補助や、脅威を発見したら対処、修復までを“ソリューションの助力”を基に、これまで以上に簡単に、確実な運用を考えるきっかけとして、このセクションでは、クラウド、オンプレミスで活用可能な、「自動化」をキーワードとした仕組みを中心に、最先端の情報を紹介します。また、運用に役立つスキルの付け方、その補助の仕方も考えていきましょう。

キーワード

AIによるセキュリティ運用自動化/SOAR (Security Orchestration, Automation and Response) / UEBA (User and Entity Behavior Analytics) / SIEM / XDR関連

視聴者の抱える課題

- 運用の手間がかかっている
- 運用がうまく回っていない／うまく回っているかどうかを判断できない
- 新たなサイバー脅威をカバーできない
- 専門知識を持つメンバーがいない
- 人材不足の問題を抱えている
- AIに関して興味がある

基調講演案

今のセキュリティ運用がシビアであり、1つの判断ミスが大きな影響を発生させるという現在の脅威を紹介しつつ、専門知識がなくても運用を回すためにはどのような考え方、ソリューションが必要かを専門家の視点から紹介する。「ソリューションだけじゃない」という課題をお話しいただく。

概要

人任せにしないマネージドサービスの要件

深刻化するセキュリティ人材不足の解消策として、運用監視やインシデント対応・封じ込め、セキュリティ強化の提案などさまざまな対策を外注するマネージドセキュリティサービスの有効性が注目されています。

ただ、マネージドサービスの効果を十分に得るためには、受け身の姿勢で全てを丸投げするのではなく、自組織に必要なセキュリティ要件を洗い出し、自分たちで対処すべき部分とアウトソースする部分を明確に分かることが重要です。ではその基準はどこにあるのでしょうか。マネージドサービスの上手な活用方法を基にセキュリティ運用を最適化するポイントを伝授します。

キーワード

MSS/MSSP/MDR/SOC

視聴者の抱える課題

- サイバー攻撃を防ぎたいが、ノウハウがない
- 自社が目指すべきセキュリティの全体像を描けない
- セキュリティ強化に向けてどのような製品を導入するのが適切か分からない
- セキュリティ運用を担う人材が不足している
- セキュリティ運用における知識や経験、ノウハウに乏しい
- セキュリティ運用に回すリソースが不足している
- インシデント発生時の対応ノウハウが確立されていない
- インシデントに遭った際、被害状況を適切に把握したい
- インシデント被害後にビジネスを迅速に復旧させたい
- マネージドセキュリティサービスを利用する際にどこからどこまでを任せるか（または自分たちで対応するか）を切り分けられない
- マネージドセキュリティサービスの選定ポイントや、機能と提供形態を知りたい
- マネージドセキュリティサービスに開示すべき情報を知りたい

基調講演案

マネージドセキュリティサービスを利用する上で、任せるべき部分と自社で実施する部分の切り分け、どのような情報を開示すればいいかなど、サービス利用時のポイントをお話いただく。

販売終了

2025年8月25日(月)		2025年8月26日(火)		2025年8月27日(水)		2025年8月28日(木)		2025年8月29日(金)		2025年9月1日(月)	
時間	枠 時間	セクション1: サイバーセキュリティリスクとマネジメント	セクション2:ゼロトラスト セクション3:アイデンティティ管理と統制	セクション4:クラウドセキュリティ セクション5:アタックサーフェス管理	セクション6:エンドポイントセキュリティ セクション7:販売終了	セクション8:ランサム（入口対策） セクション9:ランサム（出口対策） セクション10:内部不正	セクション11:専用ゾーン セクション12:セキュリティ運用自動化 セクション13:販売終了サービス				
10:00-10:40	40分	モーニングセッション1 (セクション1)	モーニングセッション2 (セクション2)	モーニングセッション3 (セクション4)	モーニングセッション4 (セクション6)	モーニングセッション5 (セクション8)	モーニングセッション6 (セクション11) 専用ゾーン				
10:50-11:20	30分	スポンサーセッション1-1 ご協賛企業決定 (セクション1)	スポンサーセッション2-1 ご協賛企業決定 (セクション2)	スポンサーセッション3-1 DAY3-4-S301 (セクション4) プラチナプラン限定枠	スポンサーセッション4-1 ご協賛企業決定 (セクション6)	スポンサーセッション5-1 DAY5-8-S501 (セクション8) プラチナプラン限定枠	スポンサーセッション6-1 DAY6-11-S601 (セクション11) 販売終了 専用ゾーン				
11:30-12:00	30分	スポンサーセッション1-2 ご協賛企業決定 (セクション1)	スポンサーセッション2-2 ご協賛企業決定 (セクション2)	スポンサーセッション3-2 DAY3-4-S302 (セクション4)	スポンサーセッション4-2 ご協賛企業決定 (セクション6)	スポンサーセッション5-2 DAY5-8-S502 (セクション8)	スポンサーセッション6-2 DAY6-11-S602 (セクション11) 専用ゾーン				
13:00-13:40	40分	基調講演1-1 (セクション1)	基調講演2-1 (セクション2)	基調講演3-1 (セクション4)	基調講演4-1 (セクション6)	基調講演5-1 (セクション9)	基調講演6-1 (セクション12)				
13:50-14:20	30分	スポンサーセッション1-3 ご協賛企業決定 (セクション1) プラチナプラン限定枠	スポンサーセッション2-3 ご協賛企業決定 (セクション2)	スポンサーセッション3-3 ご協賛企業決定 (セクション4) プラチナプラン限定枠	スポンサーセッション4-3 ご協賛企業決定 (セクション6)	スポンサーセッション5-3 ご協賛企業決定 (セクション8)	スポンサーセッション6-3 DAY6-11-S603 (セクション11) プラチナプラン限定枠				
14:30-15:00	30分	スポンサーセッション1-4 ご協賛企業決定 (セクション1)	スポンサーセッション2-4 ご協賛企業決定 (セクション2)	スポンサーセッション3-4 DAY3-4-S304 (セクション4)	スポンサーセッション4-4 ご協賛企業決定 (セクション6)	スポンサーセッション5-4 DAY5-9-S504 (セクション9)	スポンサーセッション6-4 ご協賛企業決定 (セクション12)				
15:10-15:50	40分	基調講演1-2 (セクション1)	基調講演2-2 (セクション3)	基調講演3-2 (セクション5)	基調講演4-2 (セクション6)	基調講演5-2 (セクション10)	基調講演6-2 (セクション13)				
16:00-16:30	30分	スポンサーセッション1-5 ご協賛企業決定 (セクション1)	スポンサーセッション2-5 ご協賛企業決定 (セクション3)	スポンサーセッション3-5 ご協賛企業決定 (セクション5)	スポンサーセッション4-5 DAY4-6-S405 (セクション6) プラチナプラン限定枠	スポンサーセッション5-5 DAY5-10-S505 (セクション10)	スポンサーセッション6-5 DAY6-12-S605 (セクション11) 販売終了				
16:40-17:10	30分	スポンサーセッション1-6 DAY1-1-S106 (セクション1)	スポンサーセッション2-6 ご協賛企業決定 (セクション3)	スポンサーセッション3-6 ご協賛企業決定 (セクション5)	スポンサーセッション4-6 DAY4-6-S406 (セクション6)	スポンサーセッション5-6 DAY5-10-S506 (セクション10) プラチナプラン限定枠	スポンサーセッション6-6 DAY6-13-S606 (セクション13)				

※セクション10「内部不正」のご協賛プランはプラチナプラン・全リストプランのみとなります。

※モーニングセッションおよび基調講演直後のスポンサーセッション枠は、「プラチナプラン限定枠」となります。

※スポンサー数に応じて、プログラムは適宜変更いたします。

デジタルイベント協賛予約システム



ご協賛企業様、代理店様から直接デジタルイベントへのご協賛をお申込みをいただけるようになりました！
申込可能な協賛枠や企業様のご協賛状況をリアルタイムで視覚的に確認可能です

ご予約はこちらから▶ https://techlive-itmedia.resv.jp/direct_calendar.php?direct_id=43

| ご協賛枠の予約受付完了までの流れ ※ 従来通り弊社営業担当経由でのご予約も可能です



| カレンダーの見方



① ご利用ガイド

- ご協賛を決定いただいたお客様
 - ・ 順次入稿シートをご案内いたしますので、今しばらくお待ちください。
- 仮押さえ有効期限について
 - ・ ステータスが仮押さえの枠の期限は、お申込みから14日間です。期限を超過すると枠は自動でキャンセルされます。
 - ・ ひとつのイベントにつき、予約者が同時に予約できるのは最大で3枠までとさせていただきます。
 - ・ 4枠目の予約を希望される場合は、すでに予約されている3枠のうち1枠をキャンセルしていただく必要があります。
 - ・ 他の企業様がお申込み、仮押さえをされる可能性があります。必要数だけの仮押さえをお願いいたします。
 - ・ 仮押さえから本予約へのステータス変更はシステム上でこなうか、お問い合わせフォームよりご連絡ください。
- キャンセルに関して
 - ・ キャンセルはお問い合わせフォームまでご連絡ください。担当者がご対応いたします。
 - ・ イベント企画書に掲載のキャンセル規定に基づき、キャンセル料が発生する場合がございます。
- 予約の変更に関して
 - ・ 予約完了後送られてくる予約受付メールに、URL、予約番号、確認コードの記載がございます。そちらからシステム上でこなうか、お問い合わせフォームよりご連絡ください。

	セッションプラン			リストプラン	
	ダイヤモンド	プラチナ	ゴールド	全リスト	セクションリスト
スポンサーセッション	●	●	●	—	—
専用ゾーン	●	—	—	—	—
全申込者リスト	—	想定1,000名	—	想定1,000名	—
協賛セクション申込者リスト	想定300名	想定350名	想定350名（上限450名）	想定350名	想定350名（上限450名）
セッションアンケート	●	●	●	—	—
視聴者リード	販売終了	●	●	—	—
事前アンケート結果	●	●	●	●	●
スポンサーロゴ掲載	●	●	●	●	●
資料配布	●	●	●	—	—
開催報告書	●	●	●	●	●
料金（すべて税別・グロス価格）	¥5,000,000-	¥3,500,000-	¥2,400,000-	¥2,400,000-	¥2,000,000-

※全申込者数および協賛セクション申込者数は想定値となります。

※モーニングセッションおよび基調講演直後のスポンサーセッション枠は、「プラチナプラン限定枠」となります。

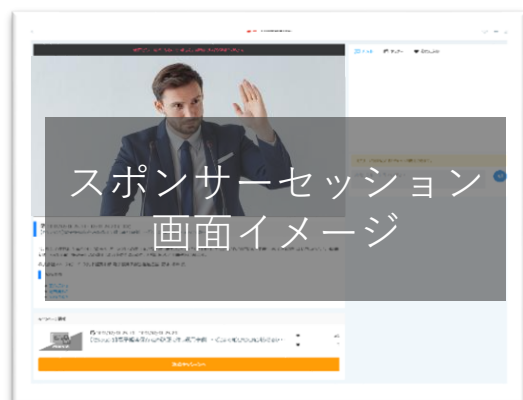
※セクション10「内部不正」のご協賛プランは、プラチナプラン・全リストプランのみとなります。

ご協賛メニュー詳細1



| スポンサーセッション

- 製品やサービスをPRできる。スポンサーセッション枠をご利用可能。



| 全申込者リスト

- イベントに申込みをされた全申込者のリード情報をご提供。
- ご提供情報：
名前・会社名・部署・役職・住所・電話番号・メールアドレス・業種・職種・役職クラス・従業員規模・年商規模・製品選定における関与など

| セクション申込者リスト

- 協賛セクション申込者のリード情報をご提供。
 - ご提供情報：
名前・会社名・部署・役職・住所・電話番号・メールアドレス・業種・職種・役職クラス・従業員規模・年商規模・関与など
- ※事前申込時に該当セクションを視聴希望としてチェックしている人(任意/申込時1カ所以上の視聴希望必須)のリストが納品対象です。

| セッションアンケート

- 貴社のセッション枠の時間内に独自のアンケートを実施。
- 単一回答・複数回答・自由回答の3種類を組み合わせる自由設定可能。
- アンケートボタンを押すと、ポップアップで表示。

※セッションアンケートの実施はLive配信時のみとなります

| 視聴者リード

- 貴社セッション視聴者のリード情報をご提供。
 - ご提供情報：
会社名・部署名・役職・電話番号・メールアドレスなどの名刺情報
- ※DL可能。
※アーカイブ開始後2日目までの視聴者リードが納品対象となります。

| 事前アンケート結果

- 事前登録時に製品選定における立場など（BANT情報）等も合わせてご提供。

※アイティメディア側で設定のため個別設定不可。

| スポンサーロゴ掲載

- イベントの集客サイトに貴社のロゴを掲載、貴社サイトへのリンクを設定可能。
- 講演間に表示する幕間スライドに貴社のロゴを掲載。

| 資料配布

- 貴社セッション内で視聴者に向けて資料の配布が可能。
- 配布点数：ご講演資料+3点まで
- PDFデータを送付いただきダウンロードリンクとするほか、貴社の指定外部リンクを設定することも可能。

| 開催報告書

- アイティメディアで一般来場者へアンケートを実施 集計結果を開催報告書として会期終了後にご提供。
- 個人情報は含まない集計データでの提供。

※画像はイメージです。

＼ダイヤモンドプラン協賛社限定／

ITmedia Security Week | 専用ゾーン

販売終了

タイムテーブル

ご留意事項

1. 専用ゾーンの企画

1. 集客サイト掲載用のゾーンタイトル・概要文の作成を含む

2. 基調講演の配信（40分間×1枠）と講演者1名のアサイン

1. ご協賛社さま自身でのアサインも可能。その場合の減額はありせん

2. 規定のスケジュールでのアサインが難しい場合は、弊社アサインで進行いたします

3. 弊社アサインの場合、講師謝礼が一定額を超える場合は別途申し上げます

3. スポンサーセッション配信（30分間×2枠）

1. 配信時間の変更など、仕様のカスタマイズは不可となります

2. 弊社スタジオでのLIVE登壇またはZoomでの事前収録となります

4. 専用ゾーン申込者リスト（300件想定、保証数ではありません）

1. ゾーン申込者、スポンサーセッション視聴者リストを提供いたします

2. 基調講演の視聴者リストの提供はありません

5. 集客サイトにてダイヤモンドスポンサーとして社名ロゴ掲載

ご提供内容

ご提供金額

お申込み締切

¥5,000,000-

2025年6月13日（金）

イベント 6日目の午前枠を専用ゾーンとしてご提供

※ご協賛状況によってタイムテーブルが変更になる場合がございます

時間	枠時間	
10:00-10:40	40分	モーニングセッション
10:50-11:20	30分	スポンサーセッション1
11:30-12:00	30分	スポンサーセッション2

基調講演

有識者によるご登壇。
ITmediaでアサインいたします。

ご協賛企業の
スポンサーセッション

スポンサーセッションにて、
ご協賛社独自のご講演をいただきます。

• 通常のスポンサーセッション枠と同様、視聴数は保証いたしません。

• 集客について

- 本専用ゾーンへの単独の告知などの集客施策は実施いたしません。
- 集客手段については弊社一任となります。

• 規定スケジュールでの進行が難しい場合は申込者数が減少する場合がございます。

• ご報告レポートはイベント全体の報告書のみとなります。
本プランの個別レポートや基調講演レポートのご提供はございません。

※金額はすべて税別・グロス価格

オプションメニュー1



| 貴社セッションmp4動画納品

- セッションありのプランにお申込み頂き、実際に配信した貴社のLIVEセッションの録画データを納品。
- mp4形式
- 配信時のままの状態となるため編集不可。

料金 **¥50,000**

| セッション収録サポート

- 30分のセッション動画の収録をサポート。
- 専用のプロ機材と収録会場を提供。
- オンラインでの収録も対応。
- 開催日の1.5カ月前までのお申込み必須。
- 講演者が2名以上の場合など、収録内容に応じて追加費用が発生する場合がございます。

料金 **¥200,000~**

| リード情報×主催アンケート回答情報付与

- 視聴者の課題感などを収集している主催者アンケートの回答情報を、納品リードに付与して納品。
- リードフォロー時の参考情報としてお役立てください。

詳細：<https://go.itmedia.co.jp/l/291242/2024-04-30/2czfbw2>

料金 **¥200,000~**

| 納品リストへのABMデータ追加

- アイティメディアのコンテンツ閲覧状況を分析し、各企業の導入検討状況を推測できるABMデータを納品リストに追加するサービス。
- ABMデータによって企業の意図を可視化し、効率的な案件発掘が可能。
- データ集計作業のため、通常より1営業日遅れての納品。

詳細：go.itmedia.co.jp/l/291242/2022-10-19/2bvm1jn

料金 **¥200,000**

| リード カスタム納品

- イベントで入手したリードをMAツールへ直接納品や、貴社フォーマットにあわせて加工して納品。
- 弊社パートナーのデータ連携ツールを介してリード情報を納品。

詳細：<https://go.itmedia.co.jp/l/291242/2024-04-30/2czfbvy>

リード件数によって料金は変動

料金 500件~ **¥100,000~**

| ブランディング施策

- イベント告知サイトに貴社情報を追加で掲載し、ブランディング施策として活用可能。
- 通常より大きく会社ロゴの表示。
- ショート動画(1分以内を推奨、最長2分まで)の埋め込み。
- フローティングバナー情報掲載。

詳細：<https://go.itmedia.co.jp/l/291242/2024-04-30/2czfbvy>

料金 **¥500,000**

| アフターフォローセミナー

- 貴社の訴求と読者の関心に合わせた企画を編集部が設計し、アイティメディアが集客・配信までサポート。
- パネルディスカッションや30分のセッション動画の収録も可能。
- プロ機材と収録会場を提供。

詳細：<http://go.itmedia.co.jp/l/291242/2022-01-30/281s4xh>

料金 **¥2,500,000**

| テレマーケティング

- イベント終了後、獲得したリードに対して所定の件数分コールを実施。
- 効果的に実施することで高い反響率と顧客獲得効果が望める。
- 最低実施件数：50件~
- 期間：3~4週間（250件の場合）
- 1000件以上は不可。

料金 **¥75,000~**

※オプションのみでのお申込みはできません（すべて税別・グロス価格）

オプションメニュー2



セッション動画活用リード獲得

- 講演動画や資料をTechTargetジャパン／キーマンズネットに転載するサービス。
- セミナー後も継続的な【属性＆件数を保証したリード獲得】が可能。

詳細：<https://go.itmedia.co.jp/l/291242/2024-06-14/2czswgv>

料金 **¥300,000～**

レポート記事配信（ターゲットヘプッシュ型で配信）

- 貴社のセッションを基にタイアップ記事を作成し、閲覧者属性を指定してHTMLメールで配信。（アーカイブ掲載あり）
- 業種、職種、企業名など狙いたいターゲット属性をターゲティングして貴社セッション内容をお届け
- 条件：セッションありプランにご協賛

詳細：<https://go.itmedia.co.jp/l/291242/2024-06-04/2czqsvy>

タイアップ プッシュ ターゲティング & ABM 15,000通～

料金 **¥1,000,000～**

レポート記事掲載（広範に読者を記事へ誘導）

- 貴社のセッションを基にタイアップ記事を作成
- DX関心層が多く閲覧しているメディア横断でタイアップ記事へ誘導
- 記事掲載メディア：イベント主催メディア
- 条件：セッションありプランにご協賛

詳細：<http://go.itmedia.co.jp/l/291242/2024-06-04/2czqsty>

DXメディア横断 PV保証タイアップ 4,000PV保証

料金 **¥1,200,000**

セッションパンフレット作成（IT・ビジネス関連）

- 貴社のセッションをパンフレットとして制作し、印刷用データ（PDF/x）を納品
- 取材内容はタイアップ記事広告としてメディアにも掲載（2,000PV保証）
- 読者への認知獲得も狙える
- 条件：セッションありプランにご協賛

詳細：<http://go.itmedia.co.jp/l/291242/2024-06-04/2czqsvn>

DXメディア横断 PV保証タイアップ 2,000PV保証
パンフレット制作（PDF/x納品）

料金 **¥1,200,000**

CM動画放映スポンサープラン

- 各基調講演(主催者セッション)開始前の待機時間に、視聴者に対して貴社支給動画を放映。
- イベント視聴者に対して、映像と音声を活用して自社サービスを繰り返し訴求することで製品やサービスの認知度向上につながります。

詳細：<https://go.itmedia.co.jp/l/291242/2024-08-05/2d122lq>

料金 **¥300,000**

パネルディスカッションパッケージ コンテンツ二次利用

- 弊社にお任せいただいたパネルディスカッションパッケージで作成したコンテンツを主催イベントに再利用。
- 通常30分間のスポンサーセッション枠を2枠ご提供。過去制作した60分間のコンテンツをそのままお届け。
- 新規でコンテンツ制作を行わずに更なるリード獲得が可能。

詳細：<http://go.itmedia.co.jp/l/291242/2024-04-17/2czbqt5>

※価格・割引率はご協賛イベントによって変動いたします。

料金 **¥3,000,000**

※オプションのみでのお申込みはできません（すべて税別・グロス価格）

／スポンサーセッション協賛社限定／

ITmedia主催デジタルイベント特別企画 | パネルディスカッション

販売終了

ご提供内容	- セッション内容企画 - 有識者のアサイン（1名） - ITmedia主催デジタルイベント内での配信（60分） - セッション視聴者リード情報のご提供	タイムテーブルイメージ 例）セッションスポンサー協賛＋パネルディスカッションの場合 ※イベントによってタイムテーブルは異なります 基調講演1 スポンサーセッション1（30分間） スポンサーセッション2（30分間） スポンサーセッション3（30分間） スポンサーセッション4（60分間） スポンサー企業様の通常講演 スポンサーセッションにて、貴社独自のご講演をいただきます。 パネルディスカッション企画 有識者、アイティメディア編集部と、貴社のご登壇者様を交えたディスカッション企画に登壇いただきます。
登壇者構成	- スポンサー企業様1名 - 有識者1名 - アイティメディア編集部1名 ※登壇者数は原則3名、最大4名 ※4名の場合はオプション費用が発生 ※5名以上は不可	
仕様	- 収録形態：事前収録のみ可（LIVE登壇は不可） - 事前収録スタジオ：アイティメディア スタジオ@麹町 - 動画内の登壇者の見え方：長テーブルに並んで着席 - オプション ※下記2点以外のオプションはご実施いただけません 1. 動画へのテロップ挿入の作業：20万円（税別グロス）→アジェンダの提示・登壇者の肩書 2. 動画納品：5万円（税別グロス）	
ご実施条件	1. セッション付きプランを定価にてお申込ください。 2. ディスカッション枠の配信枠は配信日の最終枠を予定しております。 ※他のスポンサー企業様のご協賛状況により、ディスカッションの枠の講演順を調整する場合がございます。	
ご留意事項		- 通常のスポンサーセッション枠と同様、視聴数は保証しておりません - 本パネルディスカッション枠への単独の告知などの集客施策は実施いたしません - ご報告レポートはイベント全体の報告書のみとなります。本プランの個別レポートのご提供はございません
お申込締切		通常締切（開幕2か月前）と同日
ご協賛価格		¥1,500,000-

※オプションのみでのお申込みはできません（すべて税別・グロス価格）

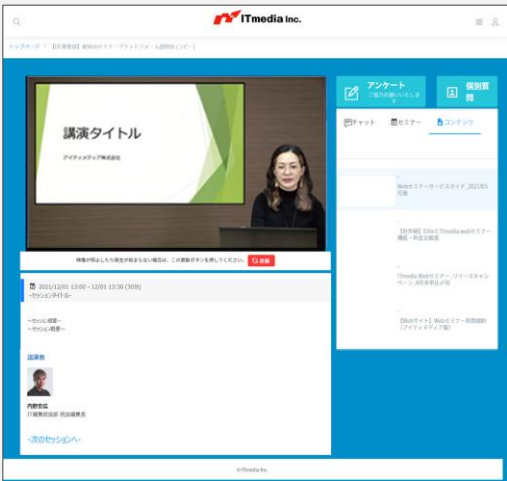
セットプランのご紹介

イベントで配信したセッション動画を二次展開し、さらなるリード獲得にご活用いただけます

本イベント
セッション登壇付きプラン

スポンサーセッションを通じて、当該テーマで情報収集中の読者に対し貴社メッセージを訴求いただけます。

▼スポンサーセッション配信画面イメージ



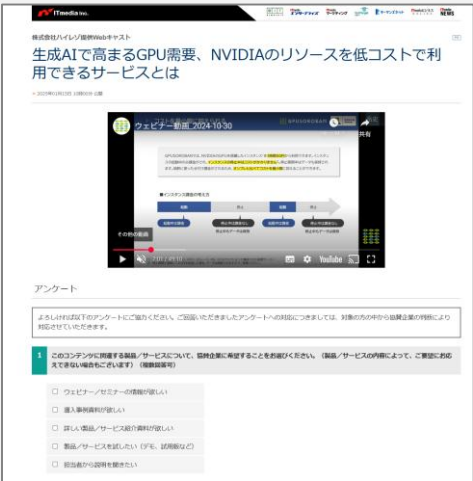
セッション動画活用
リード獲得

本イベントご講演動画1本＋貴社ご所有の関連コンテンツ1～2本を弊社メディア内に掲載し、閲覧者のリードを提供します。（マスク化して設置し、閲覧時に個人情報提供の承諾を取得）

▼コンテンツ紹介画面



▼コンテンツ閲覧画面
（動画の場合）



※詳細は[こちら](#)をご覧ください。

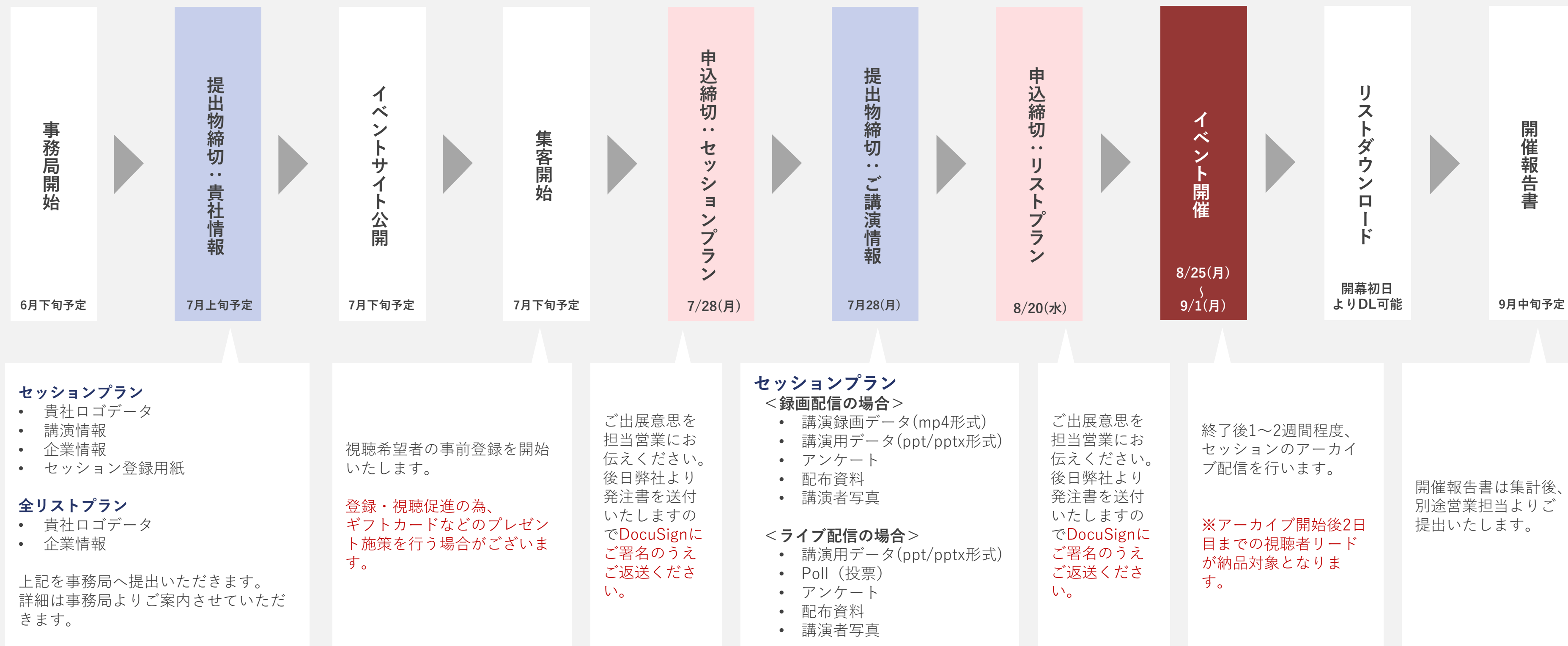
【例】

プラン名	プラチナプラン	セッション動画活用リード獲得
リード提供数	1,000件想定 ※イベントによって変動します	100件 ※ユーザー企業限定
料金（税別・グロス価格）	¥4,500,000-	

お申込みからの流れ



下記スケジュールは目安になります。状況によって変更になる可能性があり、開催決定後に確定したスケジュールをイベント事務局よりご連絡いたします。



※本内容は予告なく変更または実施を中止する場合がございます。あらかじめご了承ください。ご不明点等は営業担当までお問い合わせください。

| キャンセル料につきまして

以下の条件のいずれかに該当する場合、キャンセル料が発生しますので、ご了承ください。

発注書取り交わし後のキャンセル
登録用紙提出後のキャンセル
事務局案内開始後のキャンセル

その場合のキャンセル料は以下の通りです。

開催日41日前までのキャンセル : 契約金額の50%
開催日40日以内のキャンセル : 契約金額の100%

ただし、上記キャンセル料を超える実費（会場キャンセル料、講師アサインキャンセル料など）が発生する場合には、その追加費用も含めたキャンセル料を請求いたします。

| 消費税につきまして

企画書のプランは税別表記のため、消費税は別途申し受けます。

| 配信プラットフォームにつきまして

会場構成、運用システム等を含む配信プラットフォームは、都合により変更する場合がございます。

| オンラインでのセミナー配信リスクにつきまして

ライブ配信は常にリスクが伴います。以下にリスクを明示するとともに、当社の対策を記載いたしますので、予めご了承のほどよろしくお願いいたします。

リスク1：インターネット回線およびインターネットサービスプロバイダーにおける障害

映像・音声ともに落ちてしまう可能性があります。
直ちにバックアップPCおよびバックアップ回線での配信に切り替えます。

リスク2：ライブストリーミングプラットフォームにおける障害

配信中にバッファをためておくことで、ユーザー環境によって映像の途切れや音声途切れる現象を軽減します。
障害対策として常にバックアップ配信ができるようにシステムを冗長化していますが、万が一配信プラットフォームが落ちた場合は視聴者にメールにて配信停止のお詫びを送付し、後日オンデマンド版を案内いたします。

リスク3：電源障害

映像・音声ともに落ちてしまう可能性があります。
バックアップPCから配信停止のお詫びをアナウンスし、後日オンデマンド版をご案内いたします。

リスク4：機材障害

映像・音声ともに配信が中断（停止）する場合がございます。
直ちにバックアップPCおよびバックアップ回線での配信に切り替えます。

リスク5：視聴側における障害

- 総視聴者数に対し、視聴不良報告数が10%未満の場合
視聴者側の環境に起因する可能性が高いので、問い合わせに対して個別対応いたします。
- 総視聴者数に対し、視聴不良報告が10件単位で確認された場合
配信停止のお詫びをアナウンスし、後日オンデマンド版をご案内いたします。

※本内容は予告なく変更または実施を中止する場合がございます。あらかじめご了承ください。ご不明点等は営業担当までお問い合わせください。

@IT

“ビジネスを変革する” ITエキスパートのための技術専門メディア

■ 媒体資料

<https://go.itmedia.co.jp/l/291242/2020-10-14/tlw6gn>

■ URL

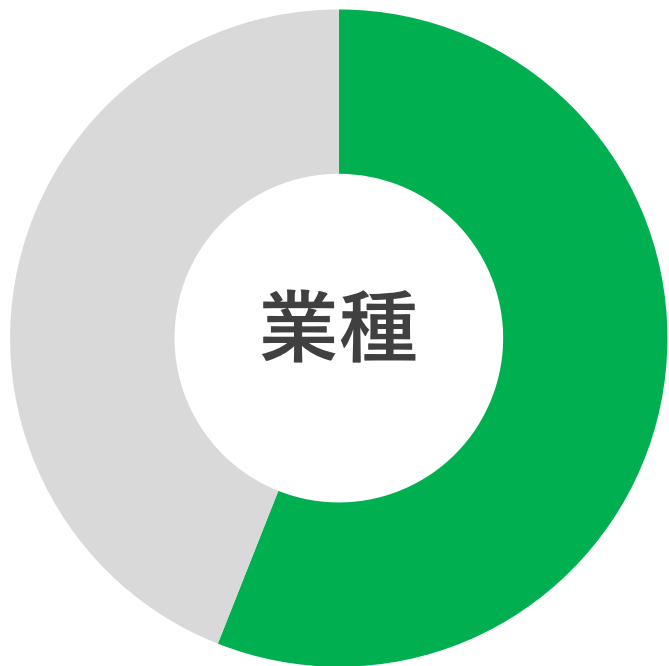
<https://atmarkit.itmedia.co.jp/>

■ PV

約770万 PV/月 約390万 UB/月 ※2024年1月実績

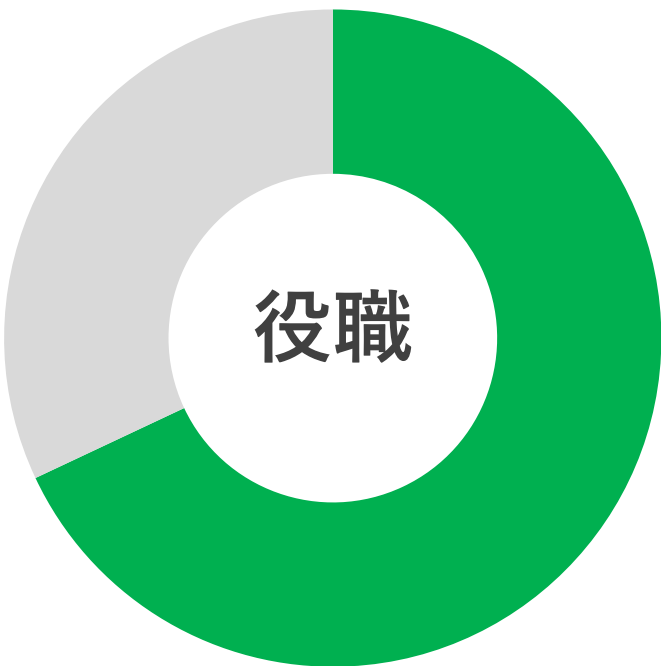
■ メルマガ配信数

約54万通



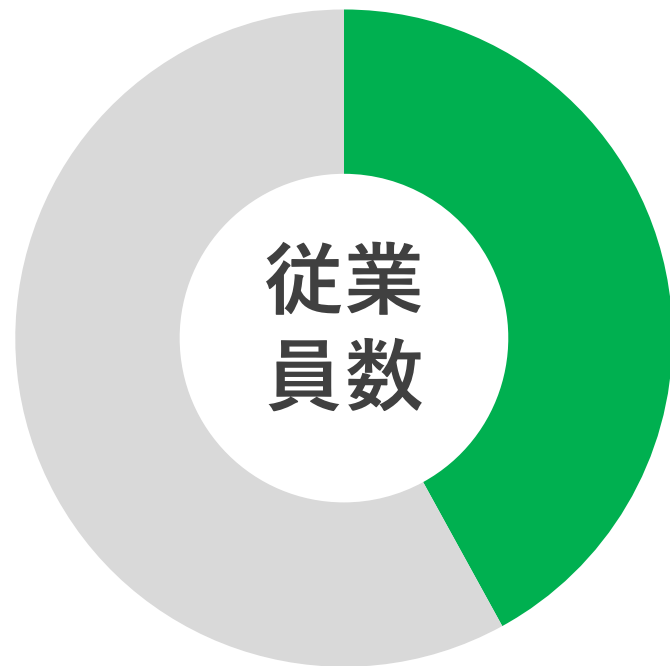
ユーザー企業 約**56%**

主な内訳：IT関連35.5%,製造業29%



係長クラス以上 約**60%**

主な内訳：係長クラス21.2%,部長クラス20.6%



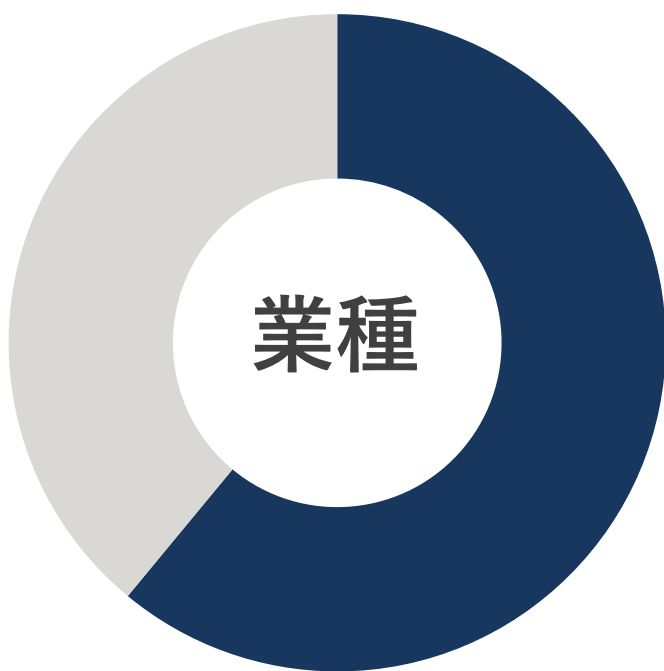
1000人以上 約**41%**

主な内訳：1000人～ 5000人未満18.4%,
5000人以上24%

ITmedia エンタープライズ

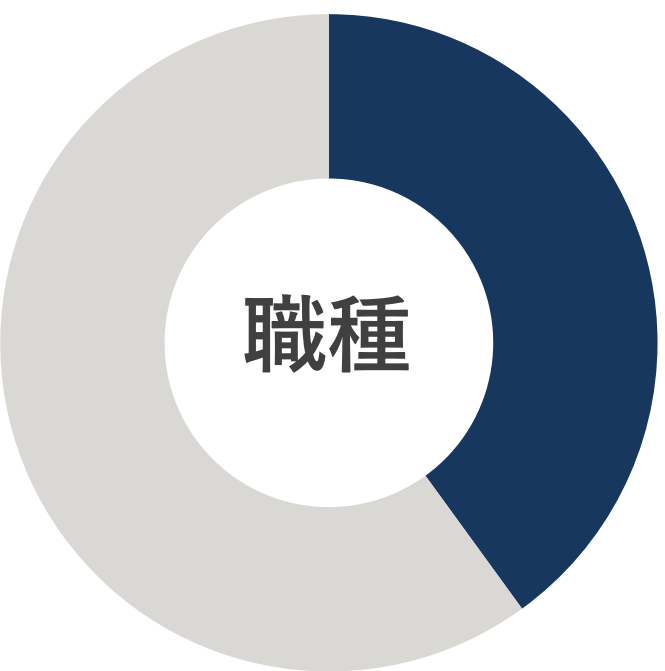
ビジネスを革新するIT部門向け実践情報サイト

■ターゲット読者	主に大企業でIT戦略の企画立案、導入システムの運用管理を担うIT担当者
■URL	https://www.itmedia.co.jp/enterprise/
■PV	約122万 PV/月 約73万 UB/月 ※2024年2月実績
■メルマガ購読数	約24万通



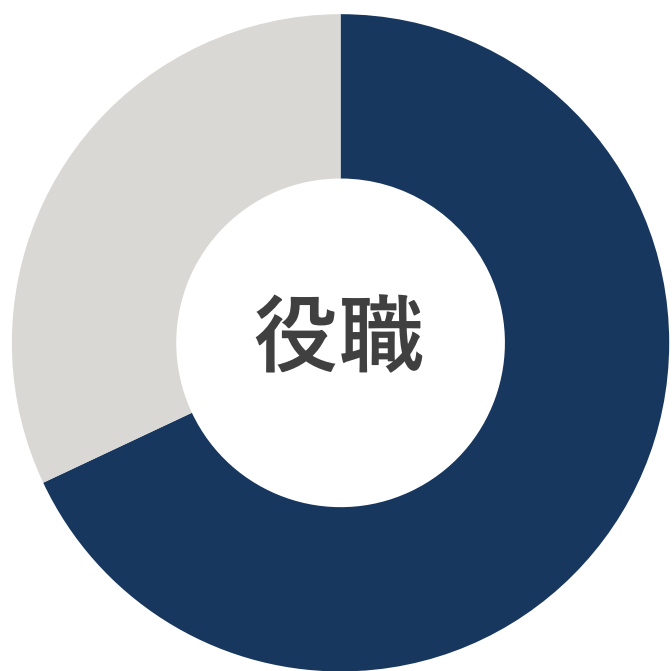
ユーザー企業 約**61**%

主な内訳：製造業37.9%, 商社・流通・サービス業27%



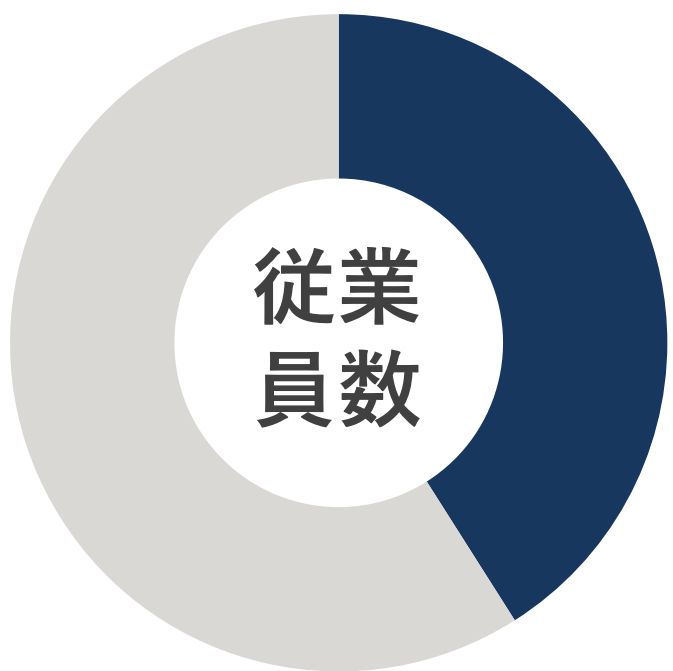
情シス及び
経営・経営企画 約**40**%

主な内訳：社内情報システム(CIO/マネージャ) 8.3%
経営・経営企画7.6%



係長クラス以上 約**68**%

主な内訳：課長クラス23.8%, 部長クラス14.6%



1000人以上 約**41**%

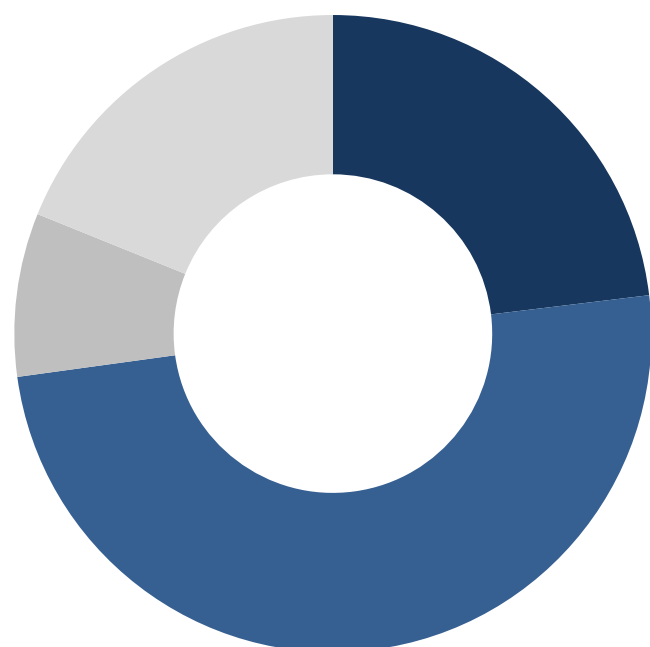
主な内訳：1000人～ 5000人未満20.3%,
5000人以上20.6%

ITmedia エンタープライズ

参考：ITmedia エンタープライズ読者調査 2024年4月 「IT戦略編」

詳細はこちら：<https://go.itmedia.co.jp/l/291242/2023-06-09/2cwt3qx>

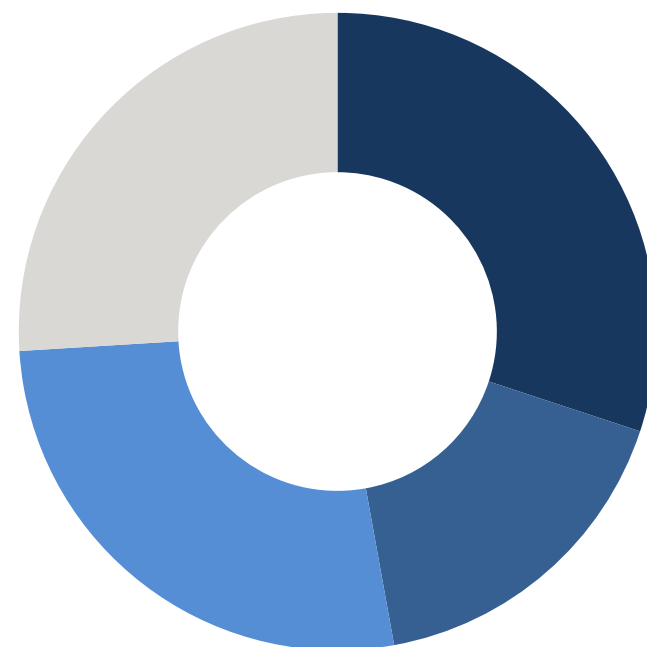
2024年度のIT関連予算の増減



■ 増加 ■ 同程度 ■ 減少 ■ 不明

IT関連予算増加の企業 約**23%**

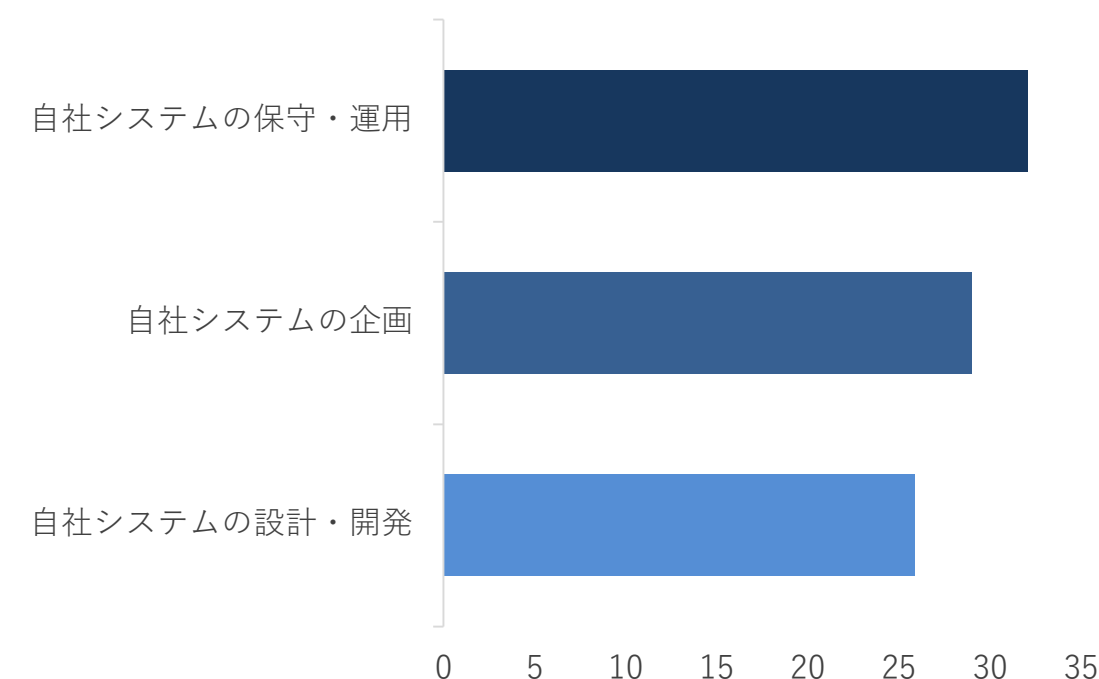
DXに向けた戦略の策定と実行



■ 実行中
■ 戦略策定済みで準備中
■ 予定はあるが未着手
■ 予定がない・携わる立場にない

DXに向けた戦略を策定・実行中 約**74%**

読者の業務内容



自社システムの企画、設計・開発、
保守・運用に携わる 約**30%**

ITmedia エグゼクティブ

企業の明日を変えるエグゼクティブとCIOのためのコミュニティ

■ 媒体資料

<https://go.itmedia.co.jp/l/291242/2020-10-14/tlw6gs>

■ URL

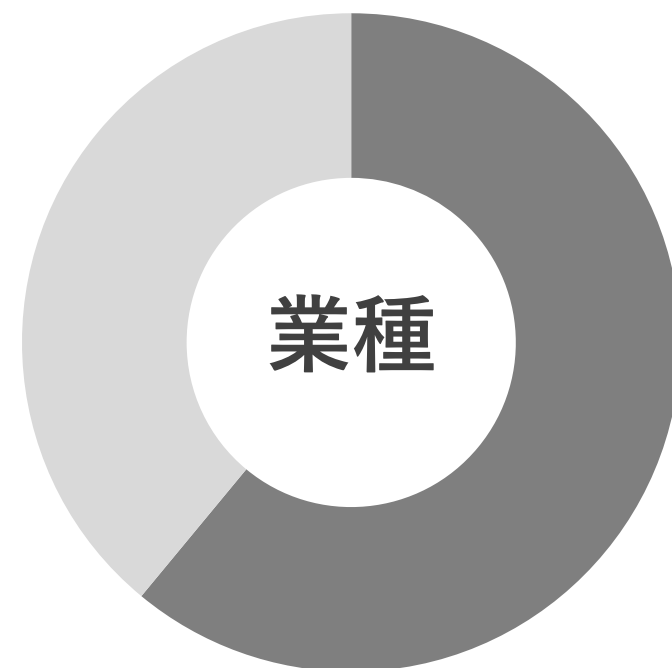
<https://mag.executive.itmedia.co.jp/>

■ 会員数

約9,700名 ※2024年4月実績

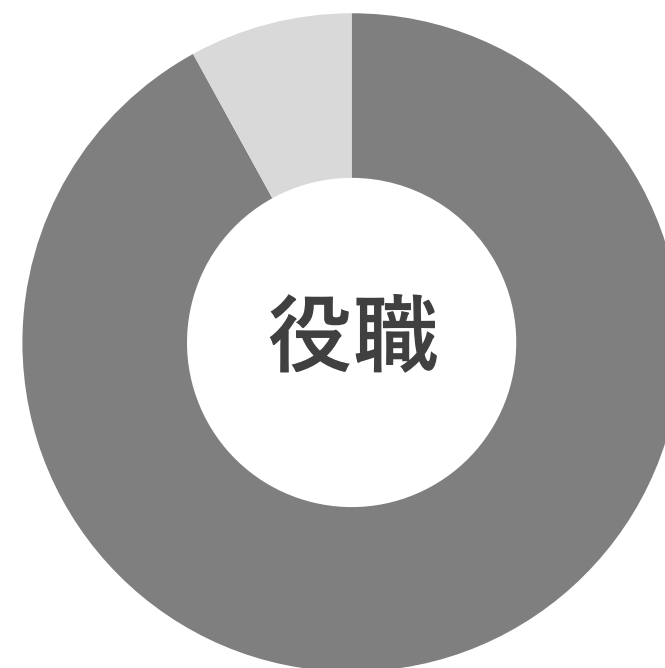
■ 年齢層ボリュームゾーン

40-50代



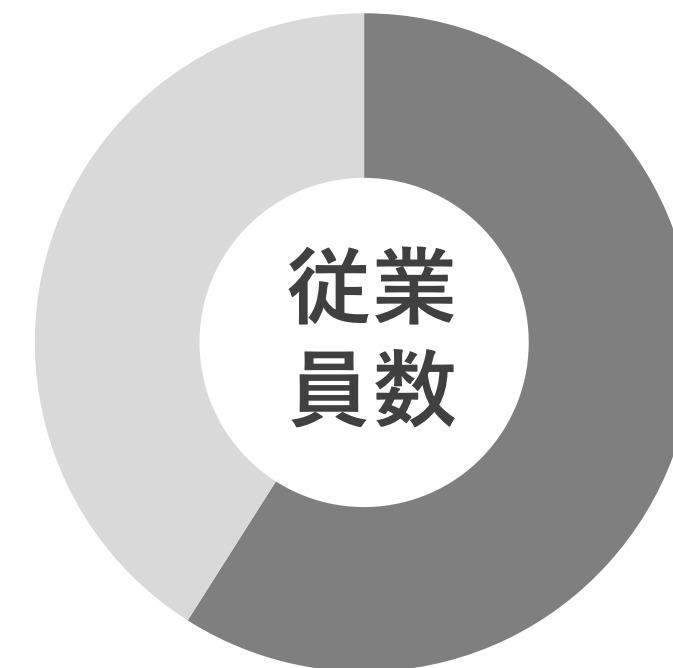
ユーザー企業 約**61**%

主な内訳：製造業約27%, IT関連業約41%



課長クラス以上 約**92**%

主な内訳：部長クラス以上約38%, 課長クラス以上約92%



1000人以上 約**59**%

主な内訳：1001～5000人約26%,
10001人以上約23%

デジタルイベントに関するお問い合わせ

アイティメディア株式会社 営業本部

〒102-0094

東京都千代田区紀尾井町3-12 紀尾井町ビル

（受付：13F）

<https://promotion.itmedia.co.jp/contact>

デジタルイベントの最新情報は[こちら](#)