2025年
5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 春

“自社の責任範囲”を自覚すれば、真に必要なことが見えてくる――
「今すぐ点検、着手すべきポイント」と「対策の具体像」

開催日　：　2025年5月26日(月)~6月2日(月)

申込締切　：　セッションプラン…2025年5月1日(木)
リストプラン　…2025年5月21日(水)

運営：アイティメディア株式会社

開催概要

ITmedia Security Week 2025 春

主催メディア	@IT atmarkIT / ITmedia エグゼクティブ / ITmedia エンタープライズ
会期	2025年5月26日(月)~6月2日(月)
申込締切日	セッションプラン…2025年5月1日(木) リストプラン　…2025年5月21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、SIer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 2024 秋 https://members08.live.itmedia.co.jp/library/NzcwODI%253D?group=SEC2024A

企画趣旨

“自社の責任範囲”を自覚すれば、真に必要なことが見えてくる――「今すぐ点検、着手すべきポイント」と「対策の具体像」

ランサムウェアをはじめサイバー攻撃が頻発している中、企業・組織には一層の対策強化が求められています。
ゼロトラスト、SASEといった概念、手段の認知度も上がり、取り組む企業も着実に増えています。
ただし、ビジネスも守るべきデータも各社各様。それが最新か否かではなく**「自社に最適か否か」を検討することが大切**です。

特に重要なのは丸投げにしない姿勢――
目的と責任分界点を自覚し、主体的にツールやサービスを使いこなすことでしょう。

ITmedia Security Week 2025 春では**「今すぐ見直すべき、着手すべきポイント」にフォーカスして各種対策の具体像を解説**。この春、「自社の責任範囲」を改めて意識しつつ「今の対策の在り方」を捉え直してみませんか。

※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。

テーマ

ゼロトラスト、SASEといった概念、手段の認知度が上がり、取り組む企業も着実に増えていますが、ビジネスも守るべきデータも各社各様です。それが最新か否かではなく「自社に最適か否か」を検討するため、各対策の具体像を解説します。

1. サイバーセキュリティリスクとマネジメント	#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. セキュリティを再構築するための“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. いま、最も狙われる「認証」を強化する	#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. 他社に後れを取らないためのクラウドセキュリティ	#SaaS、PaaS、IaaSほかクラウド＆セキュリティ関連全般
5. 「組織内の弱い部分を見つけられない」を解決する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. “二周目”のエンドポイントセキュリティ	#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 New!	#脱PPAP
8. 攻撃者の視点で侵入経路を再点検せよ～ランサムウェア攻撃における入口対策～	#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. レジリエンス強化で実現する生存戦略～ランサムウェア攻撃における出口対策～	#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. 人材不足、スキル不足を解決する「セキュリティ運用自動化」	#AIによるセキュリティ運用自動化 #SOAR #UEBA
11. マネージドサービス活用の勘所～セキュリティ運用を最適化せよ～	#MSS #MSSP #MDR #SOC
12. 「従業員/退職者の犯行を発見できない」を解決する内部不正対策 New!	**販売終了**LP #メールセキュリティ #フォレンジック #ログ管理 #ログ解析

※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。

テーマ1:サイバーセキュリティリスクとマネジメント

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、サイバー事案も急増しています。AIを悪用したサイバーセキュリティ攻撃は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/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

テーマ2:セキュリティを再構築するための“ゼロトラスト”

概要

「他社に取り残されない」を解決するゼロトラスト

ゼロトラストなどもう知っている、そして「あきらめた」という組織が少なくありません。しかし長期的な視野に立てば、ゼロトラストの考え方は確実にあなたの組織を強くし、攻撃者が最も嫌うシステムが作れることを忘れてはなりません。完全導入には時間がかかっても、少なくともいま検討すべき第一歩が、どの組織にも存在するはずです。同業他社、ライバル企業はもう、その一歩目を歩み出しているかもしれません。

本ゾーンでは、「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よいのかを掘り下げ、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

※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。

テーマ3:いま、最も狙われる「認証」を強化する

概要

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。

いま、最も狙われているのは、脆弱性だけでなく「認証情報」です。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。

本ゾーンでは、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

テーマ4:他社に後れを取らないためのクラウドセキュリティ

概要

抜け、漏れのないクラウドセキュリティを目指す

日本でも事業が完全に止まってしま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。クラウドサービス利用率が広がるいま、最も弱い設定をした企業から狙われていくでしょう。本ゾーンでは、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。また、クラウドを活用する上で必要なスキルを持つ人材をどのように確保し、育てるかについても重要なテーマとして取り上げていきます。

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。

テーマ5:「組織内の弱い部分を見つけられない」を解決するアタックサーフェス管理

概要

攻撃者の“唯一”の出入り口、かつ“偏在”するアタックサーフェスを理解せよ

これまでのセキュリティ対策はその多くが「境界防御」に頼っていたといえます。社内、社外を明確に分けることで、対策のリソースを集中させることができました。しかしもはやこの区分けだけで組織を守ることは難しいのが現状です。標的型攻撃の侵入経路となる端末が1つでも陥落した場合、そこから侵入した脅威は境界防御では守ることができません。「敵を知る」もさることながら、重要なのは「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に必要なのは、ソリューションと、組織が一丸となって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。それには、大規模なインフラ改革を経営者に理解してもらう必要もあるでしょう。そのための準備は、早い方がいいはずです。

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、これを管理、検知し、行動を止めていく守り方に変える方法考えてみましょう。

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、本セミナー対象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。

※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。

テーマ6:“二周目”のエンドポイントセキュリティ

概要

“二周目”のエンドポイントセキュリティ

近年のサイバー攻撃の激化に伴い、企業でのIT資産管理製品やEDR製品などの導入が促進されました。ただ、このようなエンドポイント保護対策の強化が進んだことで新たな課題も生まれてきています。
例えば、企業が把握できていない“野良端末”やUSBといった資産管理および脆弱性の課題や、“アラート疲れ”といったセキュリティ運用における課題、EDRによる検知の回避を狙った“攻撃の高度化”といった課題は、エンドポイントセキュリティ対策がある程度進んでいる企業こそ頭を悩ませる問題でしょう。
このゾーンでは“二周目”に入ったエンドポイントセキュリティにおける課題を明らかにし、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

- アタックサーフェイスマネジメントが気になり始めた企業。その前に、IT資産管理ができているか？と考え始めた企業を含め、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指定なかった企業など。
- 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

New!

テーマ7:脱PPAPの現在地

概要

脱PPAPの現状と課題：企業の進捗と代替策の探求

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。本ゾーンは脱PPAPの現在地を明らかにします。

キーワード

PPAP

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

テーマ8:攻撃者の視点で侵入経路を再点検せよ
～ランサムウェア攻撃における入口対策～

概要

多様化するランサムウェア侵入経路への対策：攻撃者視点からの効果的な防御策

ランサムウェア攻撃における侵入経路の多様化・複雑化が進んでいます。取引先や子会社といったサプライチェーン経由や、電子メール経由のフィッシング、VPN製品の脆弱性、ソーシャルエンジニアリング攻撃によってサービスアカウントを乗っ取られるなど多様な攻撃経路を想定し、入口対策をしっかりと講じることが企業には求められています。

本ゾーンは実際に発生した攻撃事例を基に多様な攻撃経路を解説する他、侵入からランサムウェア攻撃を仕掛けるまでの攻撃プロセスを詳細に解説。攻撃者の視点に立って脆弱なポイントを明らかにすることで、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

※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。

テーマ9:レジリエンス強化で実現する生存戦略
～ランサムウェア攻撃における出口対策～

概要

ランサムウェア対策：企業のレジリエンス強化と出口対策の実践ガイド

ランサムウェア攻撃は明日にもあなたの企業を襲う可能性がある深刻な経営リスクです。特に昨今は、取引先や子会社などのサプライチェーン経由からシステムに侵入されて被害に遭うケースも度々聞くようになりました。つまり、あらゆる可能性を考慮して万が一被害に遭ったときにより迅速に事業を復旧できるようにデータバックアップや復旧、インシデント対応といったレジリエンス（強靭性）強化の仕組みを整えておく必要があるでしょう。

ただし「どうすればランサムウェアに強いレジリエンスを実現できるのか」「そもそもランサムウェアに強いレジリエンスとは何か」という問いはなかなか具体的には答えられない難しい問題です。そこで本ゾーンでは、ランサムウェアに強い企業・組織を解説。その上で“出口対策”の強化に役立つ知識やノウハウをお届けします。

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

※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。

テーマ10:人材不足、スキル不足を解決する「セキュリティ運用自動化」

概要

運用自動化の重要性を理解せよ

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。しかし、今後もこれまで以上に熾烈な脅威がやってきます。攻めのセキュリティとして、AIや機械学習など新しい技術を駆使した「セキュリティ運用の自動化」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。それでもうまくいかない理由は、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。
このゾーンでは、脅威を発見したら対処、修復までを、AIによる補助や“製品の助力”を基に、これまで以上に簡単で確実な運用を考えるきっかけを提示します。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

※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。

テーマ11:マネージドサービス活用の勘所～セキュリティ運用を最適化せよ～

概要

マネージドセキュリティサービスの活用法：自社対応とアウトソースの最適なバランス

セキュリティ人材不足の深刻化に伴い、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といった包括的な対策をアウトソースするマネージドセキュリティサービスが注目を集めています。

効果的にマネージドサービスを活用するには単に「丸投げ」ではなく、セキュリティ業務をどこから内製で対応し、どこまでをアウトソースするかを定めることが大事ですが、これは自社の状況によって異なるため簡単ではありません。

本ゾーンはマネージドサービスに任せるべき業務と自社で実施すべき業務の基準に始まり、セキュリティ運用を最適化するため秘訣をお伝えします。

キーワード

MSS/MSSP/MDR/SOCなど

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

※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。

New!

テーマ12:「従業員/退職者の犯行を発見できない」を解決する内部不正対策

概要

組織内の“割れ窓”をなくす――内部不正を検知し、警告せよ

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み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」――割れ窓理論といわれるこのストーリーは、組織の中でも起き得ることです。従業員を監視しコントロールすること、警告を与えること。そこには、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。

このゾーンでは、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

販売終了

※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。

タイムテーブル

時間		2025年5月26日(月) 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	2025年5月27日(火) セクション2:ゼロトラスト セクション3:多要素認証	2025年5月28日(水) 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	2025年5月29日(木) 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:脱PPAP	2025年5月30日(金) 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）	2025年6月2日(月) セクション10:セキュリティ運用自動化 セクション11:マネージドサービス	
10:00-10:40	40分	モーニングセッション1 **サイバーセキュリティリスクとマネジメント**	モーニングセッション2 **ゼロトラスト**	モーニングセッション3 **クラウドセキュリティ**	モーニングセッション4 **エンドポイントセキュリティ**	モーニングセッション5 **ランサムウェア攻撃（入口対策）**	モーニングセッション6 **専用ゾーン**	
10:50-11:20	30分	スポンサーセッション1-1 ※プラチナプラン限定枠	スポンサーセッション2-1 ※プラチナプラン限定枠	スポンサーセッション3-1 ※プラチナプラン限定枠	スポンサーセッション4-1 ※プラチナプラン限定枠	スポンサーセッション5-1 ※プラチナプラン限定枠 **販売終了**	スポンサーセッション6-1 専用ゾーン **販売終了**	
11:30-12:00	30分	スポンサーセッション1-2	スポンサーセッション2-2	スポンサーセッション3-2	スポンサーセッション4-2	スポンサーセッション5-2	スポンサーセッション6-2 専用ゾーン	**2025年6月3日(火)**
13:00-13:40	40分	基調講演1-1 **サイバーセキュリティリスクとマネジメント**	基調講演2 **ゼロトラスト**	基調講演4 **クラウドセキュリティ**	基調講演6 **エンドポイントセキュリティ**	基調講演8 **ランサムウェア攻撃（入口対策）**	基調講演10 **セキュリティ運用自動化**	基調講演12-1 内部不正
13:50-14:20	30分	スポンサーセッション1-3 ※プラチナプラン限定枠	スポンサーセッション2-3 ※プラチナプラン限定枠	スポンサーセッション3-3 ※プラチナプラン限定枠	スポンサーセッション4-3 ※プラチナプラン限定枠	スポンサーセッション5-3 ※プラチナプラン限定枠	スポンサーセッション6-3 ※プラチナプラン限定枠	スポンサーセッション7-1 ※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	スポンサーセッション2-4	スポンサーセッション3-4	スポンサーセッション4-4	スポンサーセッション5-4	スポンサーセッション6-4	スポンサーセッション7-2
15:10-15:50	40分	基調講演1-2 **サイバーセキュリティリスクとマネジメント**	基調講演3 **多要素認証**	基調講演5 **アタックサーフェス管理**	基調講演7 **脱PPAP**	基調講演9 **ランサムウェア攻撃（出口対策）**	基調講演11 **マネージドサービス**	**販売終了**
16:00-16:30	30分	スポンサーセッション1-5 ※プラチナプラン限定枠	スポンサーセッション2-5 ※プラチナプラン限定枠	スポンサーセッション3-5 ※プラチナプラン限定枠	スポンサーセッション4-5 ※プラチナプラン限定枠	スポンサーセッション5-5 ※プラチナプラン限定枠	スポンサーセッション6-5 ※プラチナプラン限定枠	スポンサーセッション7-3 ※プラチナプラン限定枠
16:40-17:10	30分	スポンサーセッション1-6	スポンサーセッション2-6	スポンサーセッション3-6	スポンサーセッション4-6	スポンサーセッション5-6	スポンサーセッション6-6	スポンサーセッション7-4
17:20-17:50	30分	スポンサーセッション1-7	スポンサーセッション2-7	スポンサーセッション3-7	スポンサーセッション4-7	スポンサーセッション5-7	スポンサーセッション6-7	スポンサーセッション7-5

デジタルイベント協賛予約システム

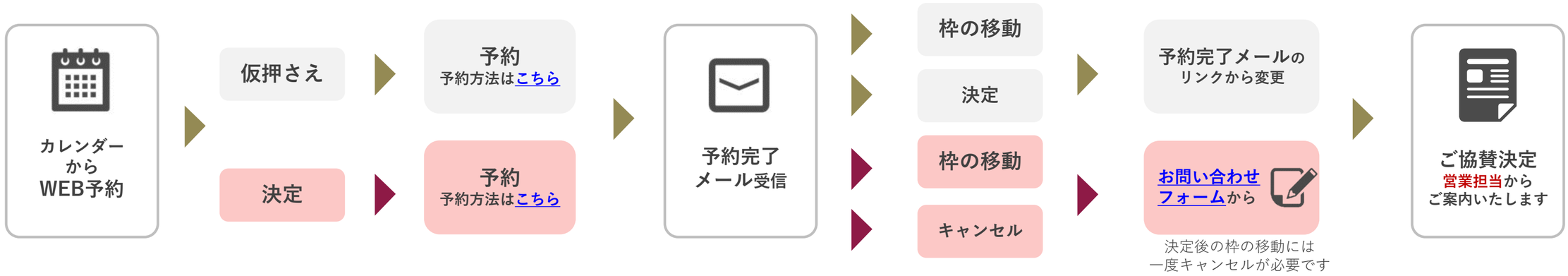
ご協賛企業様、代理店様から直接デジタルイベントへのご協賛をお申込みをいただけるようになりました！

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=23

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

ⓘ 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おこなうか、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おこなうか、お問い合わせフォームよりご連絡ください。

ご協賛メニュー

	ダイアモンド	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　Live配信＋アーカイブ	●	●	●	-	-
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（上限450名）
セッションアンケート	●	●	●	-	-
視聴者リード	●	●	●	-	-
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-**

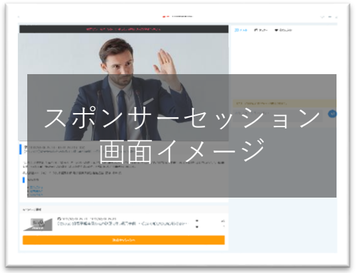
販売終了

※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。

ご協賛メニュー詳細

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種類を組み合わせて自由に
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。

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。

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ご提供。

※画像はイメージです。

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/291242/2024-04-30/2czfbvv

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（ターゲットへプッシュ型で配信）

- 貴社のセッションを基にタイアップ記事を制作し、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制作
- 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）

オプションメニュー

＼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

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
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。
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） **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。 **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。
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-

販売終了

※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）

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致します。

事務局開始	提出物締切：貴社情報	イベントサイト公開	集客開始	申込締切：セッションプラン	提出物締切：講演情報	申込締切：リストプラン	イベント開催	リストダウンロード	開催報告書
3月下旬予定	3月下旬予定	4/16(水)予定	4月下旬予定	5/1(木)	4月中旬～5月上旬予定	5/21(水)	5/26(月)～6/2(月)	開催初日よりDL可能	6月下旬予定
セッションプラン • 貴社ロゴデータ • 講演情報 • 企業情報 • セッション登録用紙 **リストプラン** • 貴社ロゴデータ • 企業情報 上記を事務局へ提出いただきます。詳細は事務局よりご案内させていただきます。	視聴希望者の事前登録を開始いたします。 登録・視聴促進の為、ギフトカードなどのプレゼント施策を行う場合がございます。	ご出展意思を担当営業にお伝えください。後日弊社より発注書を送付いたしますのでDocuSignにご署名のうえご返送ください。	**セッションプラン** **＜録画配信の場合＞** • 講演録画データ(mp4形式) • 講演用データ(ppt/pptx形式) • アンケート • 配布資料 • 講演者写真 **＜ライブ配信の場合＞** • 講演用データ(ppt/pptx形式) • Poll（投票） • アンケート • 配布資料 • 講演者写真	ご出展意思を担当営業にお伝えください。後日弊社より発注書を送付いたしますのでDocuSignにご署名のうえご返送ください。	終了後1～2週間程度、セッションのアーカイブ配信を行います。	開催報告書は集計後、別途営業担当よりご提出いたします。

※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。

ご留意事項

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が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。

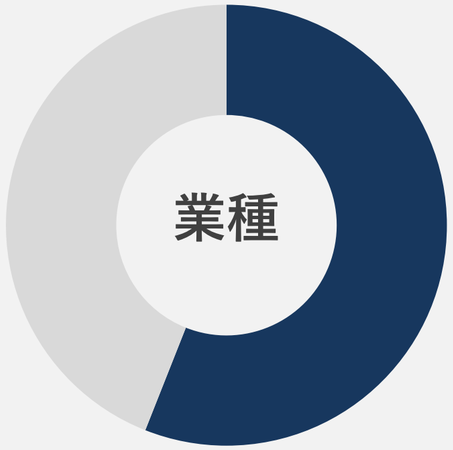
リスク５：視聴側における障害

- 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。

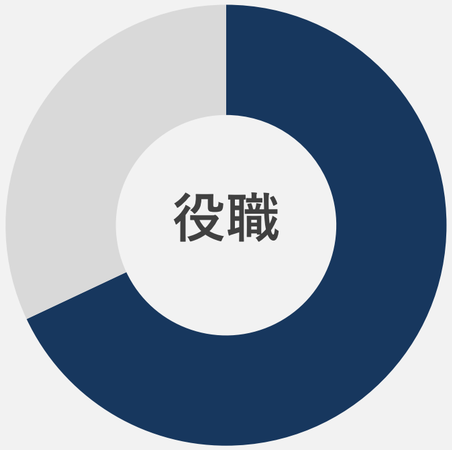
@IT
“ビジネスを変革する” ITエキスパートのための技術専門メディア

■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



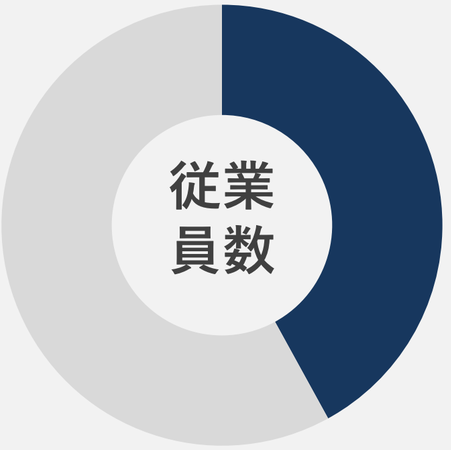
ユーザー企業 約**56**%

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

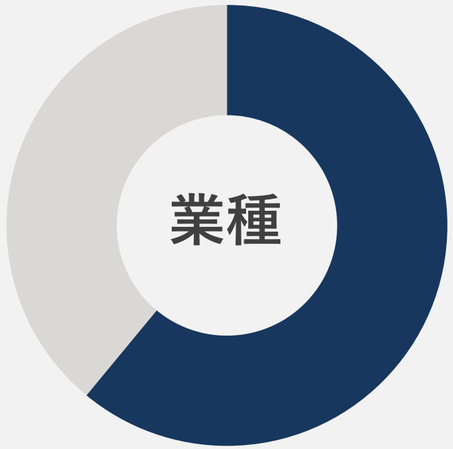
ビジネスを革新するIT部門向け実践情報サイト

■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/

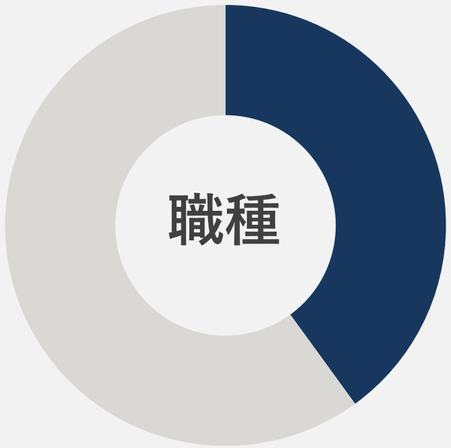
■ PV　約122万 PV/月　約73万 UB/月　※2024年2月実績

■メルマガ購読数　約24万通



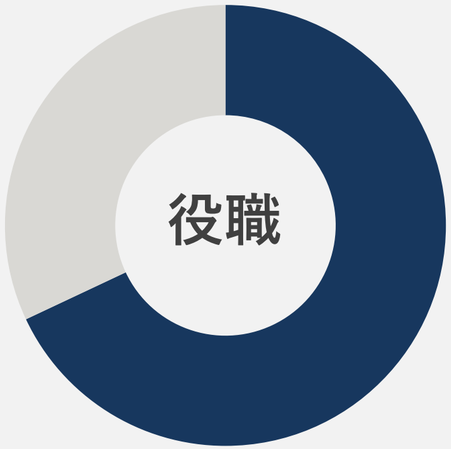
ユーザー企業 約**61**%

主な内訳：製造業37,9%,商社・流通・サービス業27%



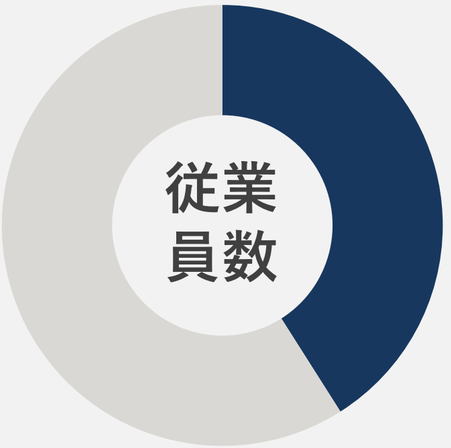
情シス及び
経営・経営企画 約**40**%

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%



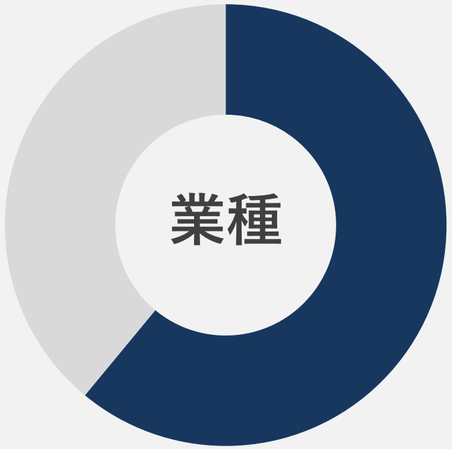
1000人以上 約**41**%

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

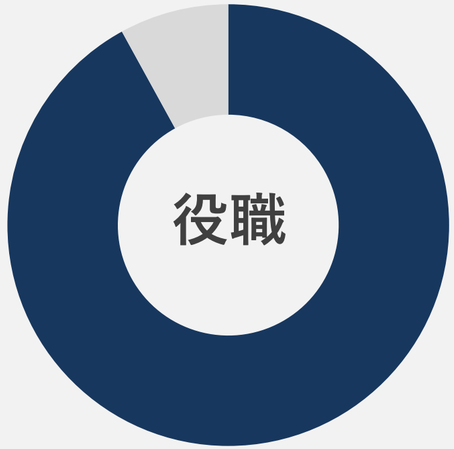
企業の明日を変えるエグゼクティブとCIOのためのコミュニティー

■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



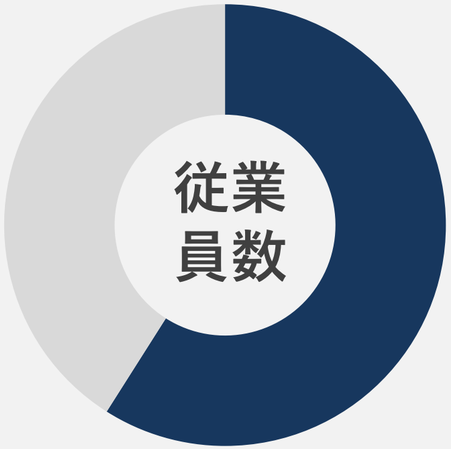
ユーザー企業 約**61**%

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