ITmedia エグゼクティブ　@IT atmarkIT　ITmedia エンタープライズ

Security Week

ITmedia Security Week 2024 冬

「自社にとって必要なセキュリティ対策」の考え方、作り方
対策のポイント、手段を今改めて総点検

開催日時：2024年2月26日（月）～3月4日（月）
申込締切：2023年12月15日（金）

SUMMARY

名称	ITmedia Security Week 2024 冬
主催	ITmedia エグゼクティブ / ITmedia エンタープライズ / @IT atmarkIT
開催日時	2024年2月26日（月）～3月4日（月）
申込締切	2023年12月15日（金）
イベント形式	集合型オンラインセミナー
視聴方法	無料登録制
事前申込者数	約1,000名想定
告知/集客	ITmedia エグゼクティブ / ITmedia エンタープライズ / @IT atmarkIT
運営	アイティメディア株式会社　セミナー運営事務局

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。

Copyright © ITmedia Inc.

PRODUCER'S COMMENT

「自社にとって必要なセキュリティ対策」の考え方、作り方
対策のポイント、手段を今改めて総点検

ここ数年で企業のセキュリティ意識は向上し、その多くが対策強化に乗り出しています。
ゼロトラスト、SASEといった概念もある程度浸透し、実装する企業は着実に増えつつあるようです。
しかし、具体的な検討に入ると「自社の場合はどこから進めればいいのか」「どこに何を適用すればいいのか」
など、情報や理解が十分ではないことに気付くケースも多いのではないでしょうか。

ITmedia Security Week 2024 冬ではセキュリティ脅威の最新動向を紹介するとともに、
必要な仕組み、ポイントを基礎から総点検。
知識、対策のヌケ、モレを確認し、一歩前に踏み出せる知見をお届けします。

Copyright © ITmedia Inc.

CONTENTS

1	サイバーセキュリティリスクとマネジメント	デジタルが前提ともいえるウィズコロナの「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。直面するこのリスクをどのようにマネジメントしていけばいいのかを紹介します。
2-1	ゼロトラストセキュリティ	ゼロトラストをキーワードに、検討／導入段階において有効な製品を紹介しつつ、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することで組織のゼロトラスト導入を成功させる秘訣を明かす。
2-2	多要素認証から始めるID管理・統制	記憶だけに頼らない「多要素認証」「FIDO 2.0」「パスキー」などの認証技術とともに、これまで見過ごされがちだったID管理／統制を考える。シングルサインオンの次、ゼロトラストの前に考えるべき保護の方法とは。
3	クラウドセキュリティ	XDRやIDaaS、SASEをはじめとする、クラウドと自社システムを守るための製品を学ぶことで、クラウドにまつわるセキュリティを過不足なく実践するために必要な知見を手に入れ、ありたい姿により近づける手助けをする。
4	エンドポイント対策&情報管理	サイバー犯罪者のシステムへの侵入をできる限り防ぐためのソリューションを知る。例えそれをすり抜けたとしても検知できる仕組みと、組織が持つ情報を管理、保護するための技術を手に入れる。
5	ランサムウェアに打ち勝つサイバーレジリエンス	“サイバーレジリエンス”は総合力。本ゾーンではランサムウェア攻撃の“入口対策”に加え、脅威侵入時の初動対応や封じ込め、バックアップといった“出口対策”までを含めたノウハウをお伝えする。
6	アタックサーフェス管理	もはや社内／社外の区分だけで組織を守るのは難しい。攻撃を止めるには「既に攻撃者は社内に到達している」と想定する必要がある。広がるアタックサーフェスを管理し、攻撃者の行動をどう検知して止めるかを考える。

Copyright © ITmedia Inc.

CONTENTS 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で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。さらに国を挙げて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ウィズコロナの「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。直面するこのリスクをどのようにマネジメント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
＃エンタープライズリスクマネジメント（ERM）
＃インシデント対応能力の作成・計画・運用
＃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

視聴者の抱える課題意識

- 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？
- 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

Copyright © ITmedia Inc.

CONTENTS 2-1. ゼロトラストセキュリティ

概要

「ゼロトラストアーキテクチャの王道を進め」

「ゼロトラスト」はバズワードを超え、将来のあるべき姿として認識され始めました。いかにしてそのメリットを取り入れつつ、安全に「ゼロトラストアーキテクチャ」に移行するか。現実的な課題に対処するには、ゼロトラストの周辺にある最新技術を取り入れた各種製品を知るとともに、それらを組織がどう活用するかがポイントです。

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することで、組織の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

＃ゼロトラスト・ネットワーク構築系ソリューション全般　＃認証系全般　＃IDaaS (Identity as a Service)　＃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　＃IDaaS　＃VPN　＃セキュリティスイッチ、ルーター製品　＃BYOD　＃マネージドサービス全般　＃EDR　＃XDR

視聴者の抱える課題意識

- 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良いかわからない
- 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

Copyright © ITmedia Inc.

CONTENTS 2-2. 多要素認証から始めるID管理・統制

概要

「正しい認証とID管理／統制能力が組織と顧客を守る」

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。攻撃者が盗み出した情報を基にした不正侵入被害が後を絶ちません。顧客や従業員に対して「パスワードを使い回すな」と注意するにも限界があります。テクノロジーによるカバーが必須です。

本ゾーンでは、まず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IDの管理と統制を考えるきっかけを提供し、シングルサインオンの次、ゼロトラストの前に考えるべき保護の方法を知ることができます。まずは「多要素認証」の技術と展開を学び、IDをもう一度考えてみませんか。

キーワード

- ＃多要素認証関連製品
- ＃リスクベース認証
- ＃IDaaS (Identity as a Service)
- ＃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

視聴者の抱える課題意識

- 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

Copyright © ITmedia Inc.

CONTENTS 3. クラウドセキュリティ

概要

「クラウドセキュリティに穴はないか？」

クラウドのセキュリティレベルに、不安はないでしょうか。クラウドサービスにおける可視性、可観測性の確保や、設定ミスへの対応、アップグレードへの追従と確認など、クラウドサービスならではの“穴”が多く存在します。何も準備をしていなければ、攻撃者はその穴を的確に狙い、あなたのシステムや情報を丸裸にするかもしれません。

本ゾーンでは、XDRやIDaaS、SASEをはじめとする、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を学ぶことで、クラウドにまつわるセキュリティを過不足なく実践するために必要な知見を手に入れ、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）
＃CSPM：クラウドセキュリティ態勢管理
＃SSPM：SaaSセキュリティ態勢管理
＃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)
＃マネージドサービス全般
＃暗号関連全般（鍵管理も含む）
＃SASE
＃SORE
＃UEBA
＃SIEM

視聴者の抱える課題意識

- 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。

Copyright © ITmedia Inc.

CONTENTS 4. エンドポイント対策&情報管理

概要

「エンドポイント」は引き続き、企業にとってサイバー空間における最前線であり、侵入のきっかけになり得る場所です。メールやWeb、VPNなどの接点がどう進化するかは、サイバー犯罪者にとっても大きく注目されるところです。

引き続き、日本国内でもひっきりなしにインシデントが発生しております。組織は守るべき情報資産を把握すること、そして従業員とサイバー空間をつなぐエンドポイントにおける防御と検知を強化することで、あるべき対策を考えていく必要があります。本ゾーンでは、CSIRTをはじめとした組織構築のノウハウや最新の防御ソリューションを紹介するとともに、そのソリューションを100%有効に活用するための知識を学びます。

キーワード

＃情報漏えい対策全般
＃資産管理系全般／脆弱性管理系全般（SBOMなど含む）
＃ネットワークのマイクロセグメンテーション関連製品
＃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）
＃EDR、XDRなどxDR（ディテクション＆レスポンス）系全般
＃フィッシング対策製品全般
＃UEBA
＃BYOD

視聴者の抱える課題意識

- 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

※ご登壇をお約束するものではございません。 Copyright © ITmedia Inc.

CONTENTS 5. ランサムウェアに打ち勝つサイバーレジリエンス

概要

ランサムウェアは今や事業継続を揺るがす深刻な経営リスクであり、大企業から中堅・中小企業まで全ての企業がいつこの被害に遭ってもおかしくありません。そのため企業は事業継続リスクで被ったダメージからいかにビジネスを迅速に復旧・回復させるかに焦点を置いた“サイバーレジリエンス”の能力を高める必要があります。

本ゾーンでは、ランサムウェア攻撃を防ぐ“入口対策”に加え、脅威の侵入に対する初動対応や封じ込め、ビジネスを迅速に復旧するための適切なデータバックアップ戦略など“出口対策”までを含めた“総合的なサイバーレジリエンス”獲得に向けた知識・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
- ＃SIEM/SOAR
- ＃SOC
- ＃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
- ＃DLP（情報漏えい対策）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意識

- 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
- ランサムウェア対策を自動化・高度化したい
- 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
- 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
- フィッシングやEmotetなどに対する従業員のITリテラシーが低い

※ご登壇をお約束するものではございません。 Copyright © ITmedia Inc.

CONTENTS 6. アタックサーフェス管理

概要

これまでのセキュリティ対策はその多くが「境界防御」に頼っていたと言えます。社内、社外を明確に分けることで、対策のリソースを集中す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。標的型攻撃の手法である1つの端末が陥落した場合、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。攻撃を止めるためには、境界の内部でも守れる仕組みが必要です。既に攻撃者が車内に潜んでいる可能性すらあるでしょう。

本ゾーンでは、「アタックサーフェス」の想定を広げ、社内で発生する攻撃の兆候を知り、それをどう止めるかを考えます。

キーワード

＃アタックサーフェス管理　＃EDR／XDR　＃VPNセキュリティ関連　＃脆弱性管理　＃メール対策製品　＃Web改ざん対策

視聴者の抱える課題意識

- 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

Copyright © ITmedia Inc.

TIME TABLE

セッション枠時間
モーニングセッション・基調講演：40分
スポンサーセッション：30分
パネルディスカッション：60分

	CONTENTS 1 サイバーセキュリティリスクとマネジメント	CONTENTS 2-1 ゼロトラストセキュリティ CONTENTS 2-2 多要素認証から始めるID管理・統制	CONTENTS 3 クラウドセキュリティ	CONTENTS 4 エンドポイント対策&情報管理	CONTENTS 5 ランサムウェア対策に打ち勝つサイバーレジリエンス	CONTENTS 6 アタックサーフェス管理	
10:00～10:40	モーニングセッション1	モーニングセッション2	モーニングセッション3	モーニングセッション4	モーニングセッション5	基調講演6-1	10:00～10:40
10:50～11:20	スポンサーセッション1-1	スポンサーセッション2-1 （ゼロトラストテーマ）	スポンサーセッション3-1	スポンサーセッション4-1	スポンサーセッション5-1	スポンサーセッション6-1	10:50～11:20
11:30～12:00	スポンサーセッション1-2	スポンサーセッション2-2 （ゼロトラストテーマ）	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	11:30～12:00
13:00～13:40	基調講演1-1	基調講演2-1 （ゼロトラストテーマ）	基調講演3-1	基調講演4-1	基調講演5-1	専用ゾーン1 基調講演6-2	13:00～13:40
13:50～14:20	スポンサーセッション1-3	スポンサーセッション2-3 （ゼロトラストテーマ）	スポンサーセッション3-3	スポンサーセッション4-3	スポンサーセッション5-3	スポンサーセッション6-3 （専用ゾーン）	13:50～14:20
14:30～15:00	スポンサーセッション1-4	スポンサーセッション2-4 （ゼロトラストテーマ）	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 （専用ゾーン）	14:30～15:00
15:10～15:50	基調講演1-2	基調講演2-2 （多要素認証テーマ）	基調講演3-2	基調講演4-2	基調講演5-2	ディスカッション1	15:10～16:10
16:00～16:30	スポンサーセッション1-5	スポンサーセッション2-5 （多要素認証テーマ）	スポンサーセッション3-5	スポンサーセッション4-5	スポンサーセッション5-5		
16:40～17:10	スポンサーセッション1-6	スポンサーセッション2-6 （多要素認証テーマ）	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	ディスカッション2	16:20～17:20

Copyright © ITmedia Inc.

CONTENTS

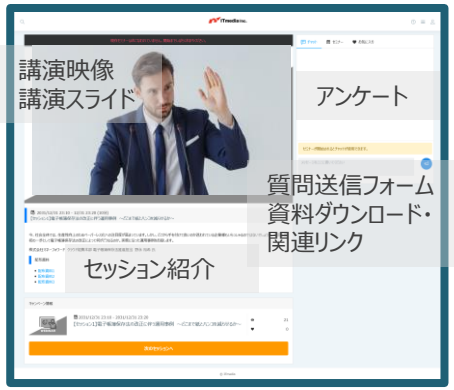
	1社限定！ プラチナスポンサー ＋ラウンドテーブル開催	1社限定！ 貴社テーマに関心の高い視聴者へ訴求可能！	貴社セッションを視聴した関心度の高い読者から、イベント全体の申込者まで幅広いリストを獲得可能！	協賛セクションのテーマに興味がある参加者へアプローチすることが可能！	スポンサーセッションの準備が難しい場合でも、多くのリストを獲得することが可能！	協賛セクションのテーマに興味がある視聴者のリストを獲得することが可能！	4社限定！ パネルディスカッションを通して、協賛社様の製品・サービスのPRに繋げる事が可能！
	ブラック	ダイアモンド	プラチナ	ゴールド	全リスト	セクションリスト	ディスカッション
スポンサーセッション Live配信＋アーカイブ	●	●	●	●	-	-	-
専用ゾーン	-	●	-	-	-	-	-
パネルディスカッション	-	-	-	-	-	-	●
セキュリティラウンドテーブル開催 （Security Week開催終了後）	●	-	-	-	-	-	-
スポンサーアンケート	●	●	●	●	-	-	-
全申込者リスト 想定1,000名	想定1,000名 ～申込者すべて	-	想定1,000名 ～申込者すべて	-	想定1,000名 ～申込者すべて	-	-
協賛セクション申込者リスト	想定350名	想定300名 ※追加オプションあり	想定350名	想定350名 ～450名（最大）	-	想定350名 ～450名（最大）	想定250名 ～450名（最大）
自セッションの 視聴者データ・レポートサイト	●	●	●	●	-	-	●
Security Week 申込者向けメール配信	2回配信	-	-	-	-	-	-
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）	￥7,000,000-	¥5,000,000-	¥3,500,000-	¥2,400,000-	¥1,800,000-	¥1,000,000-	￥2,500,000-

※集客人数は想定値となります。
※協賛セクション申込者リスト数はいずれのセクションも想定値ですが、セクション2-2（多要素認証テーマ）につきましては、他セクションよりもスポンサーセッション数が少ないため、特にセクション申込者リスト数が350名を下回る可能性がございます。

Copyright © ITmedia Inc.

SPONSORED MENU

スポンサーセッション



スポンサーセッション枠をご活用いただけます。ご来社が難しい場合は動画データをご納品いただき、当日配信することも可能です。
※配信時のスポンサーセッションにはQ&Aコーナーが用意されており、講演に参加している視聴者はその場でテキストにて質問が可能です。（スポンサー様がQA実施を希望された場合のみ）

専用ゾーン

1社限定の特別プラン
スポンサーセッションを専用ゾーンで開催いたします。
編集部が貴社の訴求したいメッセージをお伺いし、ゾーン全体の概要やゲストセッション候補者のご提案・講演概要の企画をすることで、貴社テーマに関心の高い視聴者へ訴求することが可能です。

パネルディスカッション

＜テーマ1：エンタープライズ企業向け＞
そもそも侵入に気づけているか？　検知したら、脅迫されたら、その後はどうする？
エンタープライズ企業が知っておくべきインシデント対応の現実解（仮）
（読者実態、検知→対処を迅速に行える体制と手段の解説、コスト/スキルを考慮した現実的な対策法など）

＜テーマ2：中小企業向け＞
あの事件・事故は他人ごとではない。
どうする2023！？　脅威に巻き込まれないセキュリティジャーニーの描き方　（仮）
（読者実態、基礎的内容と最低限やるべきことをおさらい）

4社限定の特別プラン
協賛社様2社とアイティメディア編集部とゲスト講師のパネルディスカッション企画をアレンジメントいたします。編集部が選定したホットトピックを軸に協賛社様の製品やサービスのPRに繋げる事が可能です。テーマはご希望に応じて調整いたします。

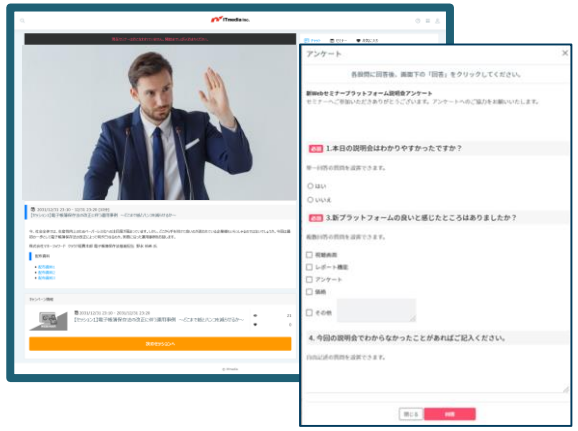
▼メニュー詳細
社数：1テーマにつき先着2社　※2社の協賛が付き次第実施決定。1社の場合は実施不可。
セッション時間：60分
出演者：4名（協賛社様2名、モデレーター：アイティメディア編集部1名、ゲスト1名）
事前申込者数：250名想定
備考：事前収録を想定

※画像はイメージです

Copyright © ITmedia Inc.

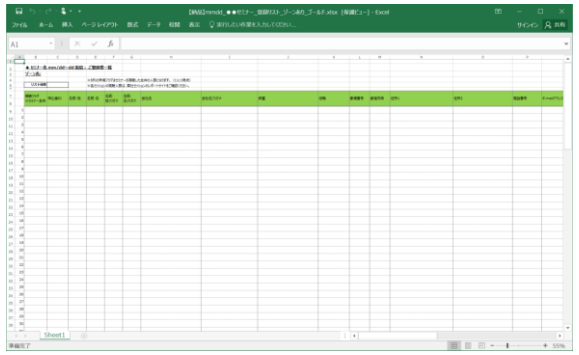
SPONSORED MENU

セッションアンケート



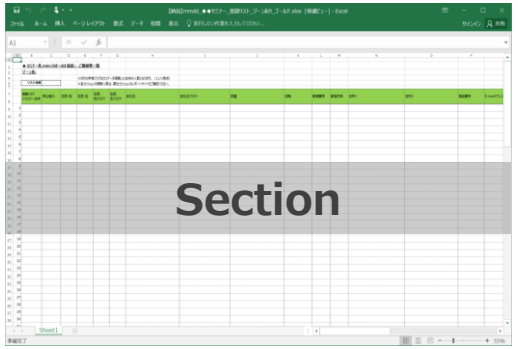
貴社のセッション枠の時間内に、独自のアンケートを実施頂けます。
※アンケートボタンを押すと、ポップアップで表示されます。
回答形式は単一回答、複数回答、自由回答の3種類を組み合わせて自由に設定頂けます。

全申込者リスト



全申込者の「会社名」「部署名」「役職」「電話番号」「メールアドレス」など、名刺情報をリストにてご提供します。
イベント終了後3～5営業日以内にExcelデータ形式にて納品いたします。

協賛セクション申込者リスト



協賛セクションの申込者の「会社名」「部署名」「役職」「電話番号」「メールアドレス」など、名刺情報をリストにてご提供します。
※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。

※画像はイメージです。

Copyright © ITmedia Inc.

SPONSORED MENU

視聴者データレポートサイト

セッションのレポートサイトをご提供します。
セッション視聴者の「会社名」「部署名」「役職」「電話番号」「メールアドレス」など、名刺情報もDL可能です。

申込者向けメール配信（ブラックスポンサー限定）

Security Week開催期間中、事前申込者を対象としたメール配信を2回行うことが可能です。
自社セッションの見どころのご紹介やアーカイブ視聴促進のためのご案内にご利用ください。

本サービスはブラックスポンサー限定で、会期中2回の配信が可能です。（配信タイミングはご相談となります）

原稿は貴社でご用意ください。
※ただし、特に内容指定がなければセッション情報をベースにして当社で作成代行も可

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（BANT情報）等も合わせて提供します。
見込み客の選別やアポイントを取るときの事前情報としてお役立てください。
※設問はアイティメディアが設定いたします。
個別設定はできません。

※画像はイメージです。

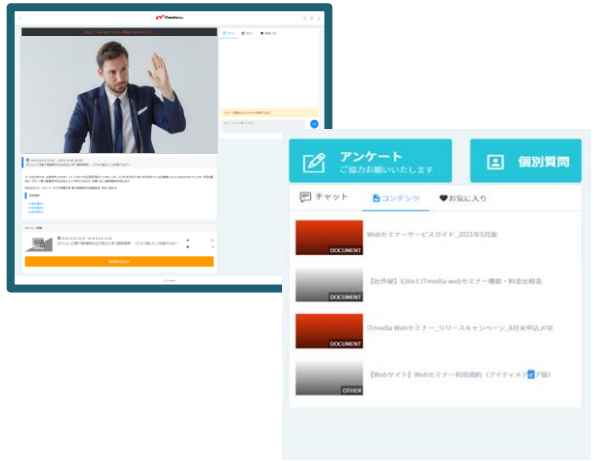
Copyright © ITmedia Inc.

SPONSORED MENU

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示し、
貴社サイトへのリンクを設定いたします。

配布資料



貴社セッション内で視聴者に向けて、
ご講演資料＋3点まで資料の配布が可能です。
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
に、貴社の指定外部リンクを設定することも可能です。

開催報告書

来場者へアンケート集計結果を開催報告書として会期終了後にご提供いたします。
開催報告書内は個人情報は含まない、集計データでのご提供となります。

※画像はイメージです。

Copyright © ITmedia Inc.

OPTION MENU

出展効果を最大化！
追加施策！

LIVEセッション録画データ納品

セッション動画を活用したい！

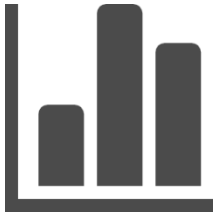
セッションがあるプランにお申込みいただき、LIVEでご登壇いただいた際に、配信した貴社のLIVEセッションの録画データをmp4形式で納品いたします。

※配信時のままの状態となるため、編集はありません。

5万円

納品リストへのABMデータ追加

納品リードから
効率的な案件発掘が可能！



アイティメディアのコンテンツ閲覧状況を分析して得た、各企業の導入検討状況を推察できるABMデータを納品リストに追加します。ABMデータで企業インテントを可視化することで、納品リードから効率的な案件発掘が可能です。

※データ集計作業のため、通常より1営業日遅れての納品となります。

詳細は右記URLよりご確認いただけます
go.itmedia.co.jp/l/291242/2022-10-19/2bvm1jn

20万円

セッション収録サポート

プロの機材で
手軽に動画の制作が可能！

アイティメディアがセッション動画30分の収録をサポートいたします。
プロ機材及び収録会場をご用意しますので、手軽に動画の制作が可能です.

▼備考
講演者のお顔＋資料スライドを同時収録します。
画面右上1か所に、肩書やテーマをテロップを入れていただけます。
オンライン収録も可能です。

18万円

※画像はイメージです。
※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）

Copyright © ITmedia Inc.

OPTION MENU

出展効果を最大化！
追加施策！

セッション動画 活用リード獲得

もっと自社コンテンツを見た人のリードがほしい！

セミナーにご掲載いただく講演動画や製品資料をTechTargetジャパン／キーマンズネットに転載。ご準備いただいたコンテンツをそのまま活用し、セミナー終了後にも手間なく【属性＆件数を保証したリード獲得】を継続実施していただけます。

詳細はこちら
http://go.itmedia.co.jp/l/291242/2022-09-02/2bfy1tr

30万円~

行動履歴 ターゲティングタイアップ

もっとサービスを知ってほしい！
理解を深めてほしい！

読者の記事閲覧履歴を基に「興味・関心」の高い人を貴社タイアップ記事へ誘導します。読者の行動データを外部サービスへ連携し拡張配信を行うことで、アイティメディアに訪れたことが無くても、同じ「興味・関心を持つ人」を捕捉することでリーチを広げます。

※本メニューは、ライブ/オンデマンド配信、録画データ等を視聴しながら要点をまとめるものです。別途取材は行いません。

詳細はこちら
https://go.itmedia.co.jp/l/291242/2022-09-09/2bjcm9g

150万円

アフターフォローセミナー

獲得したリードを
ナーチャリングしたい！

編集部が貴社の訴求メッセージと読者の関心を掛け合わせた企画を設計。講師のご提案・アサインから、集客(60名)・配信までITmediaがサポート致します。ご希望により、編集部や基調講演講師とのパネルディスカッションも可能です。

詳細はこちら
http://go.itmedia.co.jp/l/291242/2022-01-30/281s4xh

230万円

全申込者リスト納品

全申込者リスト納品

ダイアモンドプランの納品リストを、全申込者リストに変更いただけます。貴社の専用ゾーン視聴者だけでなく、イベントに参加登録をした全員のリストで、より多くのリード獲得が可能です。

100万円

※画像はイメージです
※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）

Copyright © ITmedia Inc.

＼追加施策で効果を最大化！／

オプションメニュー ｜ リード情報×主催アンケート回答情報付与

New!

リード情報と主催アンケートの回答情報を紐づけることで、

興味関心や課題感がより深く可視化できるのでフォローしやすい！

【メニュー詳細】

- お申込みいただいたプランに沿って納品されるリード情報に、主催アンケートの回答情報を付与して納品
（＝納品リードの中で、回答情報が付与されるリード／されないリードが発生します）

- **セミナーにご協賛いただいているお客さまのみお申込み可能**

納品データサンプル　※画像はイメージです

【納品タイミングについて】

- **リード情報** ｜セミナー閉幕日の3-5営業日後に納品
- **アンケート回答情報** ｜セミナー閉幕日の2-3週間後を目途に追って納品

※アンケート回答情報の納品タイミングは、セミナーによって異なります
※アーカイブ配信期間中もアンケートの回答を受付けるため、アーカイブ配信終了後にデータ精査のうえ納品いたします

お申込締切：セミナー開幕日前日まで

ご提供価格（税別・グロス価格）：**30万円**

＼追加施策で効果を最大化！／

オプションメニュー ｜ リード カスタム納品サービス

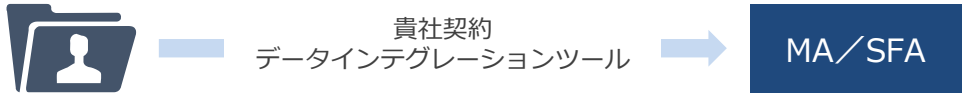
New!

MAツールなどへの直接納品や、貴社フォーマットにあわせたリードデータの加工に対応
リード加工の手間なく、すぐにフォローが可能です！

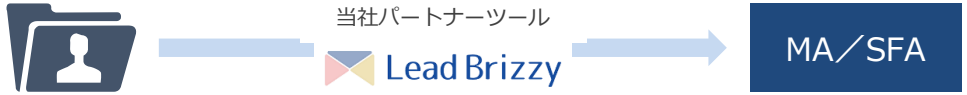
納品フロー イメージ

パターン1：**貴社フォーマットに合わせてリード情報を加工して納品**

パターン2：**貴社利用のデータ連携ツールを介してリード情報を納品**



パターン3：**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**



※本サービスのご利用には一定の条件がございますので、詳細はお問い合わせ下さい

実施料金（税別グロス）

セミナーで納品する総リード数に応じて一律の金額設定となります

- ～500件：**10万円**
- 500～1,000件：**15万円**
- 1,000件以上：**20万円**
- 3,000件以上：**30万円**

納品タイミング

閉幕後6-8営業日後
※加工内容によって前後する場合がございます

お申込み締切

セミナー閉幕日まで

備考

- 対応可能なツールは下記の通りです
  - パターン1、2：お問い合わせください
  - パターン3：Marketo、Hubspot、salesforce、Pardot、Hot Profile
- パターン2、3で「Lead Brizzy」をご利用の場合は下記を必ずご確認ください
  - 株式会社Brizzy提供の「Lead Brizzy」を弊社が代理店としてご提供いたします。別途、株式会社Brizzyとの間で、申込書の取り交わし、利用規約への同意などが別途必要となります
  - 初期設定を代行する場合、1案件あたりオプション費用50,000円を頂戴します
- ご希望の納品形態や詳細については営業担当にお申し付けください

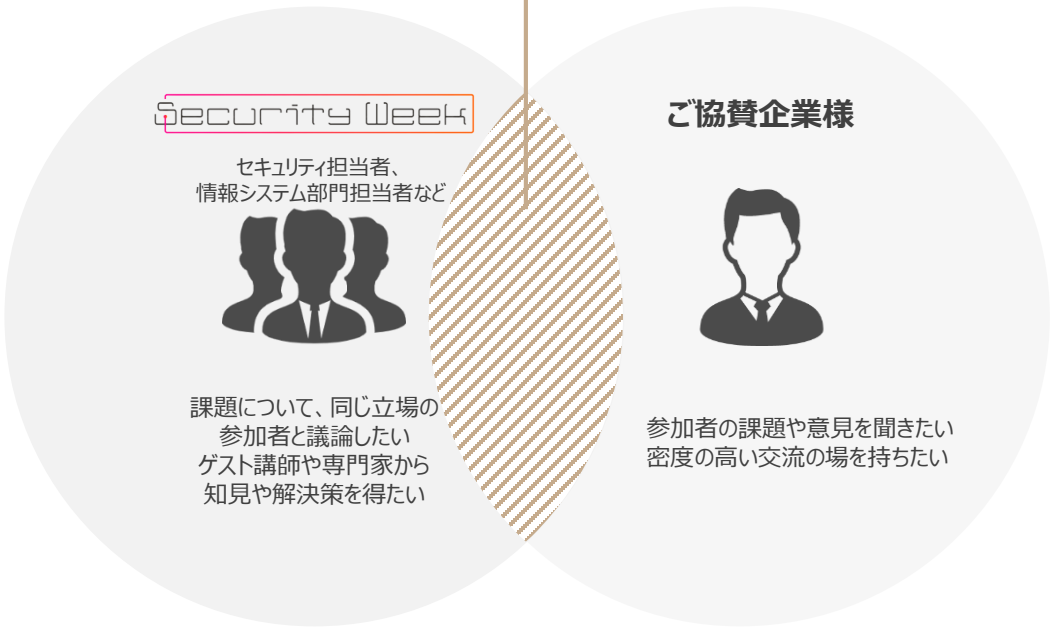
Copyright © ITmedia Inc.

ブラックスポンサー限定

SPONSORED MENU ラウンドテーブル

企画概要

イベント参加者と直接コミュニケーションを行える場として、
SecurityWeek終了後に招待者限定ラウンドテーブルを開催いたします。



ご協賛メリット

ラウンドテーブル

交流

- ディスカッション、懇親会を通じて、**交流・関係構築**をすることができる
- 訪問等、**次回提案に向けたファーストコンタクト作り**をすることができる

商品開発

- 購入する側視点での**ニーズ・シーズを得る**ことができる

販売戦略

- 開発中の**商品やサービスなどに対する意見をクローズドな空間で得る**ことができる

Copyright © ITmedia Inc.

SPONSORED MENU ラウンドテーブル

ブラックスポンサー限定

セキュリティラウンドテーブル 企画概要

主催	ITmedia エグゼクティブ　ITmedia エンタープライズ　@IT atmarkIT
開催時期	ITmedia Security Week 開催終了後4週間以内に開催想定（随時調整）
開催規模	8～9名想定 一般参加者：最大5名～6名想定 ゲストスピーカー 1名 モデレーター（ITmedia 編集部）1名 協賛企業様　ご担当者様　1名
ご招待方法	SecurityWeek申込者のうち、役職等の特定の条件で選定をした方をご招待
会場	アイティメディア株式会社　セミナールーム想定（調整中）
形式	ディスカッション形式ラウンドテーブル　＋　懇親会（軽食、ドリンク提供予定）

※企画、ゲストアサイン、当日の運営、会場費、懇親会費等を含みます。
※懇親会の開催は必須とさせていただきます。
※企画内容、ゲストにより謝礼が別途追加になる可能性がございます。
※外部会場での実施をご希望の場合、会場費、懇親会費は実費精算のため参加者数、お部屋によって変動する可能性がございます。
※通訳、撮影収録などは含まれておりません。
※新型コロナウイルス感染症の状況により、延期または中止の可能性があります。

【キャンセル規定】開催日の41日前まで：50%　開催日の40日以内：100%
※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。

Copyright © ITmedia Inc.

SPONSORED MENU ラウンドテーブル

ブラックスポンサー限定

当日の開催スケジュールイメージ

時間	分	内容	詳細
9:30-10:00	30	受付	参加者受付
10:00-10:15	15	開会挨拶/自己紹介	来場者同士の立場などを紹介
10:15-10:35	20	ゲスト講演	ゲストに講演いただきます
10:35-11:45	70	ディスカッション	モデレーターITmedia 編集部
11:45-12:00	15	貴社プレゼンテーション	参加者にPRしたい事項をお伝えいただきます
12:00-13:00	60	懇親会	軽食とドリンクの提供※ご参加可能な方のみ
13:00-		順次解散	-

ご協賛者様の当日のご対応

受付開始45分前	協賛社様ご集合 プレゼン環境確認（チェック）ディスカッションの流れ、最終すり合わせ
来場者受付～本番	ディスカッション席には貴社より1名参加可能。ご担当者など他の方も数名ご同席可能です
懇親会	ご来場者様とのコミュニケーションの場としてご活用ください
順次解散	

進行フロー・想定実施スケジュール

Security Week 開催1.5ヶ月前	開催1ヶ月前	開催2～3週間前	Security Week 開催日	開催5営業日後	開催1週間後	開催4週間後
ラウンドテーブル 企画内容のご相談	企画概要・講師案の ご提出	講師への登壇 打診・調整	Security Week 開催 セッションご登壇	SecurityWeek 参加者リスト ご納品	ラウンドテーブル 招待対象者の選定ご 招待開始	**ラウンドテーブル 開催**
テーマ設定のため、ターゲット層や訴求内容についてお伺いします。		講師へのラウンドテーブル登壇依頼を行います。 ※講師決定まで時間がかかる場合がございます。		プラチナスポンサー（全リスト）のご納品となります。	ご招待者を選定し、 イベント運営事務局より 対象の方にご招待をお送りいたします	

Copyright © ITmedia Inc.

SCHEDULE

申込締切	2023年12月15日（金）	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が送付されますのでDocuSignにご署名のうえご返送ください。
告知準備		セッションのご講演者情報、ご講演タイトル、貴社ロゴデータなどと合わせてご提出いただく、 **セッション登録用紙を事務局へご提出**ください。
告知開始	2023年1月中旬	事務局にて、イベント告知サイトをオープンいたします。 同時に視聴希望者の事前登録も開始いたします。
開催準備		**配布資料・視聴者向けセッションアンケート設問・動画納品の場合のご講演データなどを事務局にご提出**ください。開催2営業日前までにレポートサイト情報もお送りいたします。
開催	2024年2月26日（月）～3月4日（月）	ライブ講演いただく場合は、事務局よりご案内する時間までにアイティメディアの スタジオ受付にお越しください。
レポート		会期終了**3～5営業日以内に事前申込者のリストをご提出**いたします。 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。※予定 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。

Copyright © ITmedia Inc.

PAST EVENTS

【モーニングセッション1】
医療情報企業に学ぶ セキュリティ対策を推進する勘所――経営と現場を動かす方法は？
メディカル・データ・ビジョン株式会社 渡邊 幸広 氏

【モーニングセッション2】
DXで変化するデジタル環境とゼロトラスト
ニューリジェンセキュリティ株式会社 仲上 竜太 氏

【モーニングセッション3】
クラウドのセキュリティガバナンス確立に必要なCCoEの役割
大日本印刷株式会社 和田 剛 氏

【モーニングセッション4】
古くて新しいサプライチェーンのセキュリティ問題、実のところどうすればよいか
イー・ガーディアングループ 徳丸 浩 氏

【モーニングセッション5】
DXを妨げるデータ侵害のシナリオとシフトレフト
株式会社アスタリスク・リサーチ 岡田 良太郎 氏

【基調講演1-1】
セキュリティ対策、今までの考え方でいいですか？～TOPPANが実践するセキュリティ対策事例～
凸版印刷株式会社 池田 望 氏

【基調講演1-2】
組織固有のリスクを踏まえたサイバーセキュリティ強靭化方策
前内閣参事官 結城 則尚 氏

【基調講演2-1】
ペネトレーションテストを技術観点、運用観点、組織観点で3倍美味しく活用するメソッド
日本セキュリティオペレーション事業者協議会 阿部 慎司 氏

【基調講演2-2】
Security Talk Cafe ～特別篇～ 現役医師が語る 医療現場のサイバーセキュリティのリアル
誠馨会 千葉中央メディカルセンター 大谷 俊介 氏

【基調講演2-2】
Security Talk Cafe ～特別篇～ 現役医師が語る 医療現場のサイバーセキュリティのリアル
株式会社Armoris／金融ISAC 鍵田 敬介 氏

【基調講演3-1】
クラウドサービス上の機密情報を攻撃者は如何にして奪取するのか
株式会社トライコーダ 上野 宣 氏

【基調講演3-2】
脅威と人の変化と不変
株式会社インターネットイニシアティブ 根岸 征史 氏

【基調講演3-2】
脅威と人の変化と不変
SBテクノロジー株式会社 辻 伸弘 氏

【基調講演3-2】
脅威と人の変化と不変
piyokango 氏

【基調講演4-1】
今見直したいエンドポイントの穴
株式会社川口設計 川口 洋 氏

【基調講演4-2】
攻撃者エコシステムから考えるエンドポイントセキュリティの軍拡競争
株式会社リチェルカセキュリティ 黒米 祐馬 氏

【基調講演5-1】
セキュリティインシデントにどう備えるか - 組織に求められる対応力、初動対応
国立研究開発法人情報通信研究機構 盛合 志帆 氏

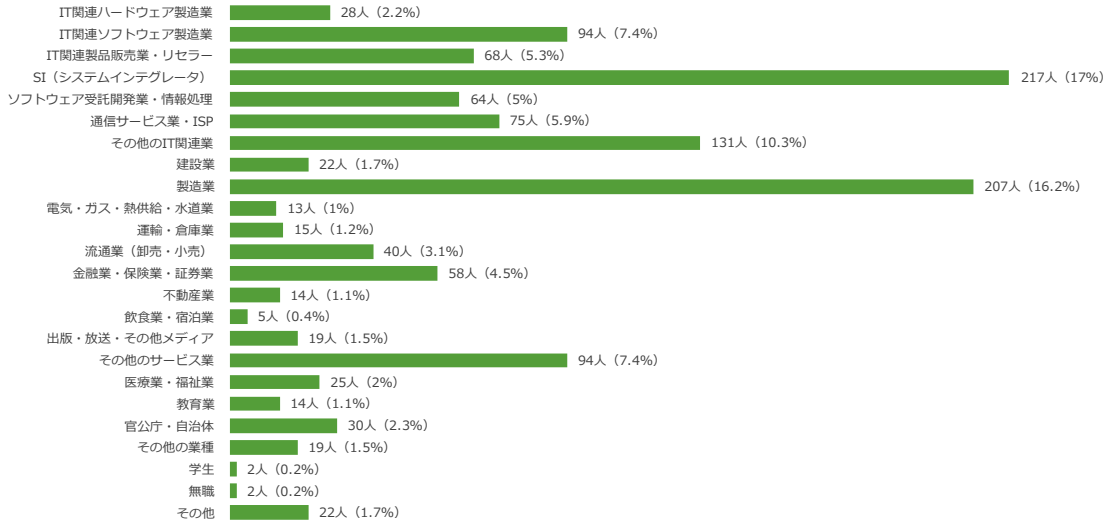
【基調講演5-2】
現場とともに危機に備える――住友化学が実践する工場とオフィスのサイバーレジリエンス強化
住友化学株式会社 門田 あおい 氏

タイトル	ITmedia Security Week 2023 秋 脅威から守る「一連の仕組みとフロー」にどう位置付け、どう生かすか セキュリティ対策の全体観と各種ツールの生かし方
日時	2023年8月28日（月）～ 9月1日（金）　※9月17日までアーカイブ配信
全申込者数	1,278
主催	@IT、ITmedia エンタープライズ、ITmedia エグゼクティブ
協賛 （※50音順）	株式会社IIJグローバルソリューションズ、株式会社アウトソーシングテクノロジー、arcserve Japan合同会社、アクロニス・ジャパン株式会社、株式会社アシュアード、AvePoint Japan株式会社、株式会社インターネットイニシアティブ、Veeam Software Japan株式会社、ヴイエムウェア株式会社、株式会社エーアイセキュリティラボ、SB C&S株式会社、NECフィールディング株式会社、エムオーテックス株式会社、オープンテキスト株式会社、クラウドストライク合同会社サイバーリーズン合同会社、株式会社JALインフォテック、ジョーシス株式会社、Ｓｋｙ株式会社、株式会社ソリトンシステムズ、タレスDISジャパン株式会社、テクマトリックス株式会社、東芝ITサービス株式会社、トレンドマイクロ株式会社日本プルーフポイント株式会社、Netskope Japan株式会社、パロアルトネットワークス株式会社、株式会社日立ソリューションズ、株式会社日立製作所、株式会社ベリサーブ、株式会社マクニカ、ルーメン・テクノロジーズ株式会社
申込みページURL	https://v2.nex-pro.com/campaign/57934/apply

Copyright © ITmedia Inc.

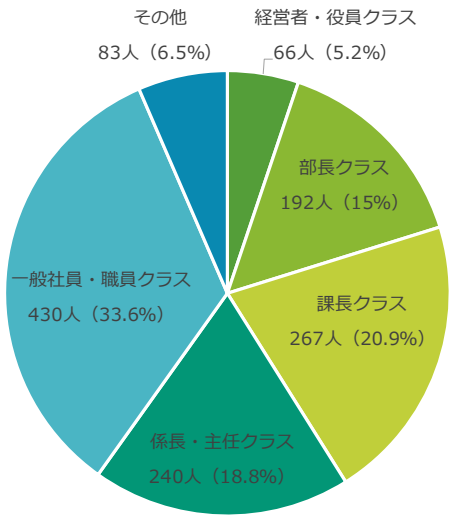
PAST EVENTS

業種

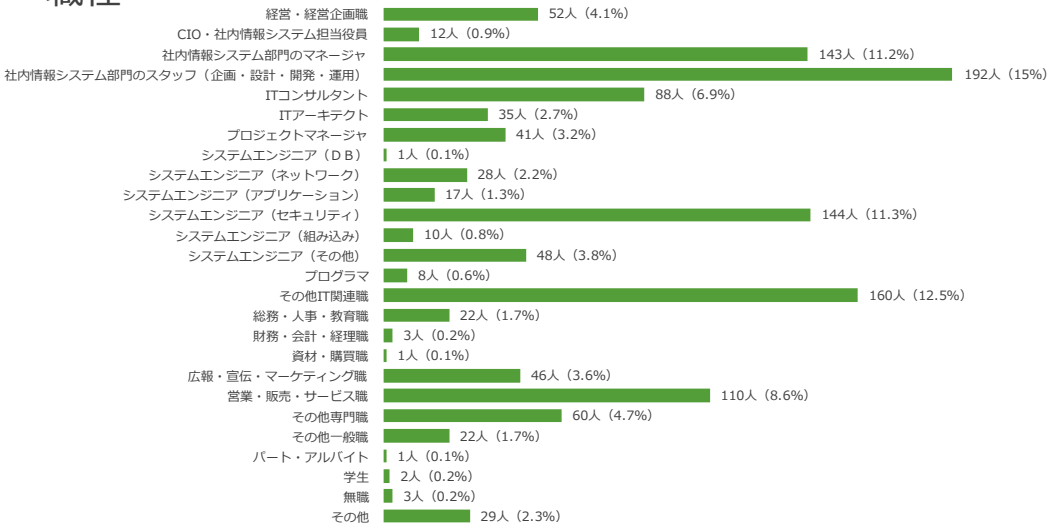


N=1278

役職

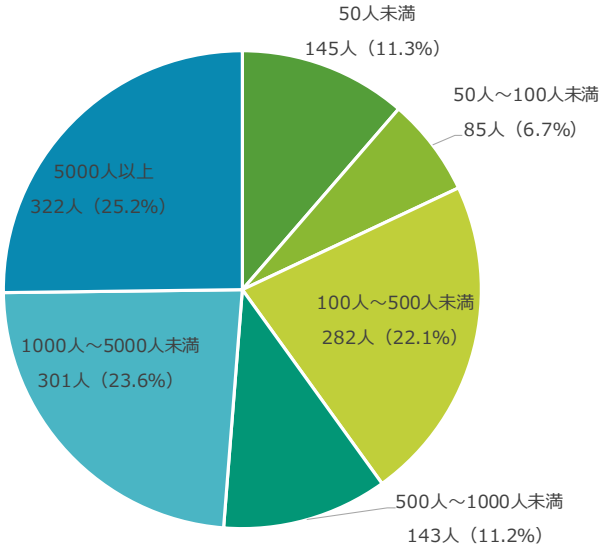


職種



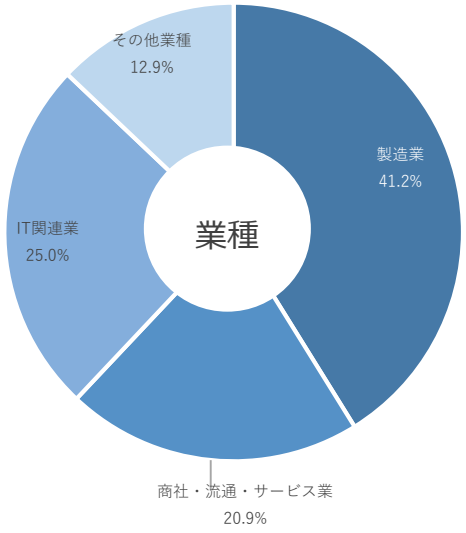
N=1278

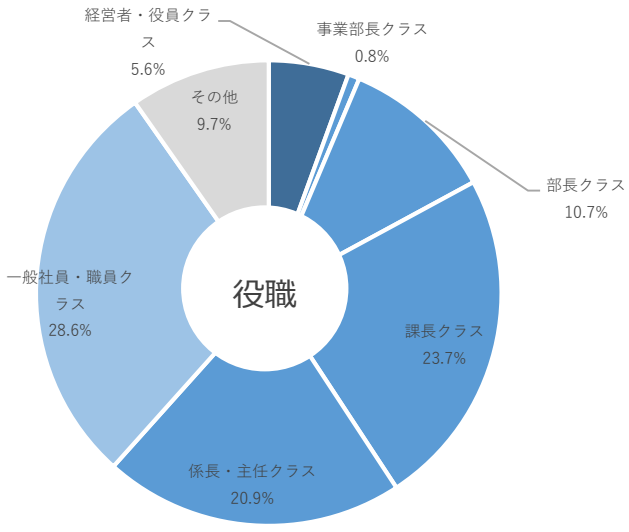
従業員規模

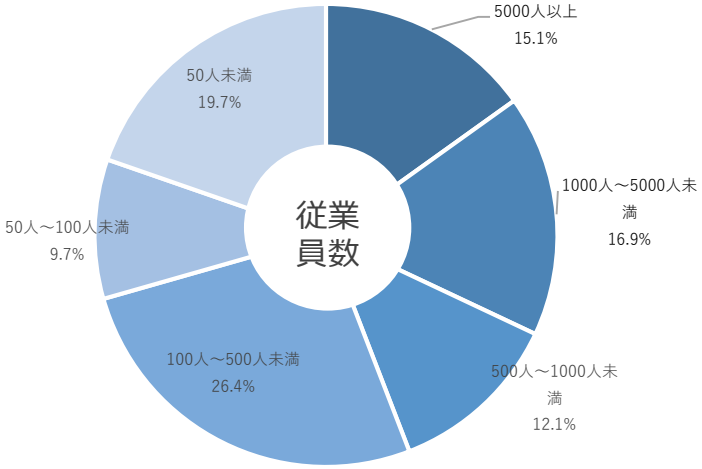


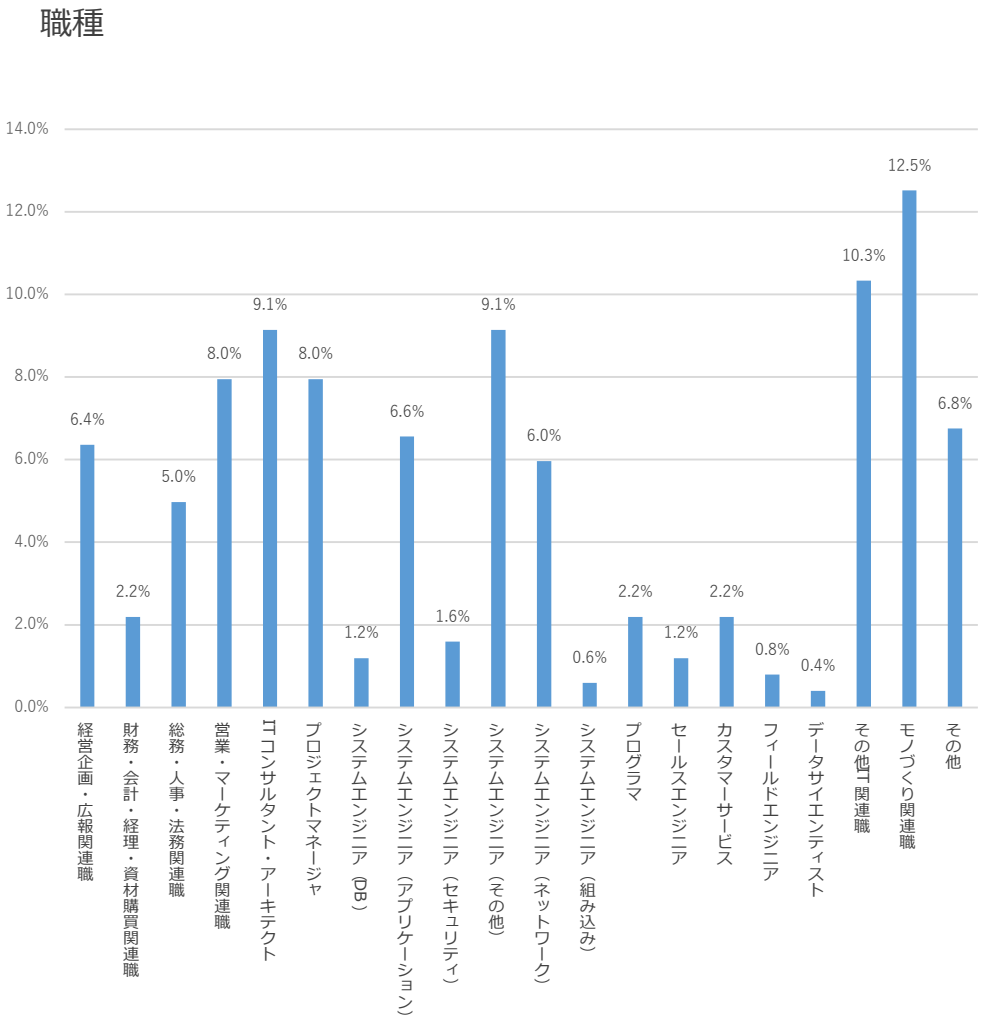
Copyright © ITmedia Inc.

MEDIA GUIDE 読者属性





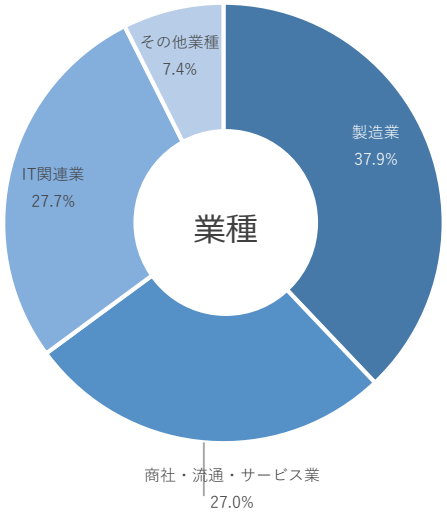


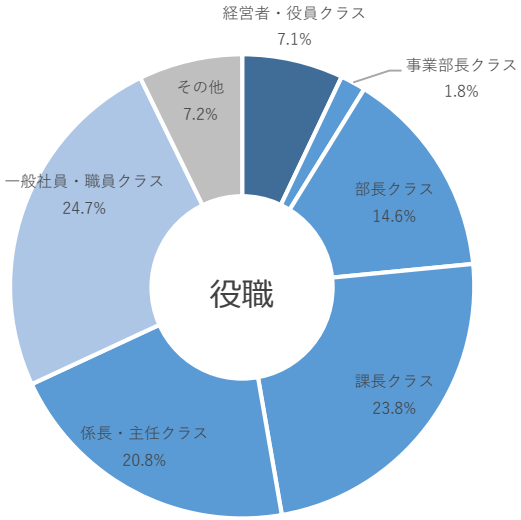


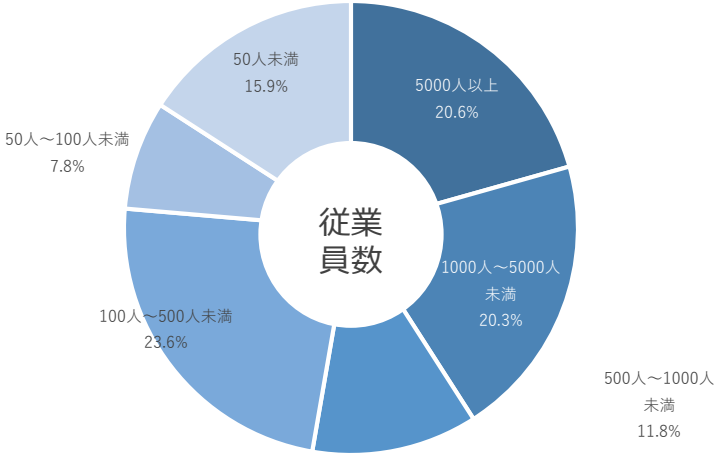
Copyright © ITmedia Inc.

MEDIA GUIDE 読者属性

ITmedia エンタープライズ



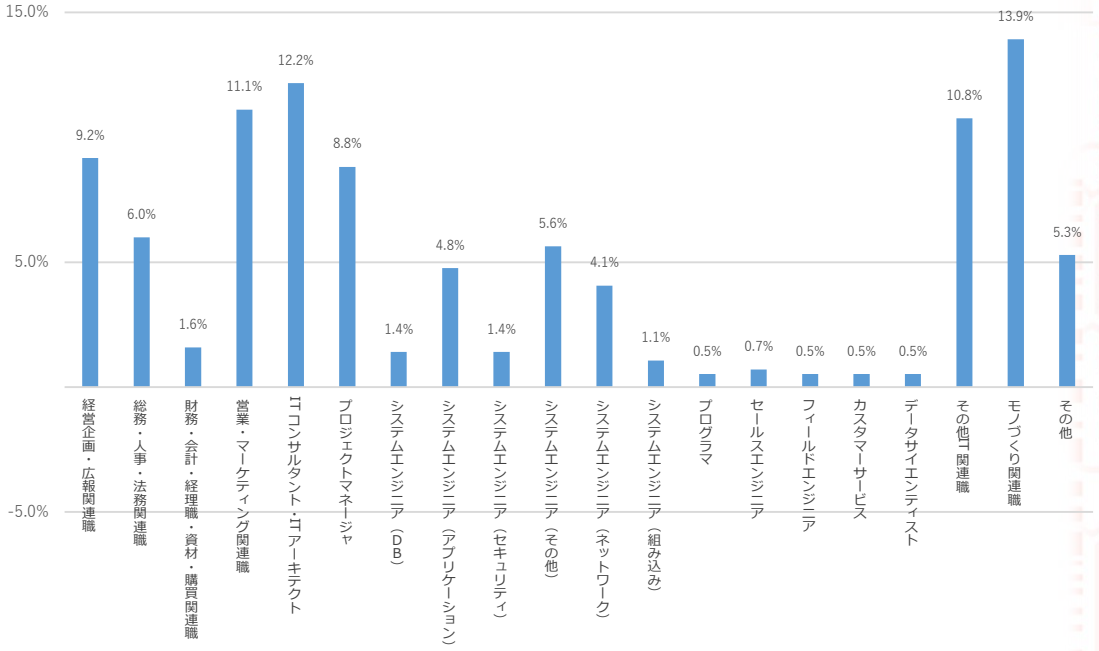




閲覧企業上位

- パナソニックホールディングス株式会社
- 株式会社エヌ・ティ・ティ・データ
- ソニーグローバルソリューションズ株式会社
- 楽天グループ株式会社
- 株式会社リコー
- キヤノン株式会社
- 株式会社デンソー
- 株式会社野村総合研究所
- 日鉄ソリューションズ株式会社
- TIS株式会社
- アマゾンウェブサービスジャパン合同会社
- セイコーエプソン株式会社
- 株式会社ミスミグループ本社
- 株式会社本田技術研究所
- 日本オラクル株式会社
- 日産自動車株式会社
- 東京大学
- シャープ株式会社
- 本田技研工業株式会社
- 凸版印刷株式会社
- 株式会社きんでん
- マツダ株式会社

職種

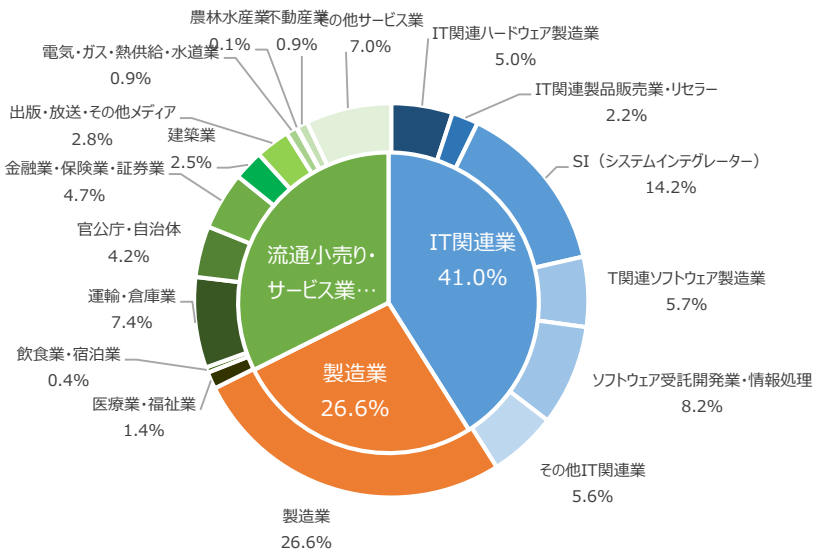


Copyright © ITmedia Inc.

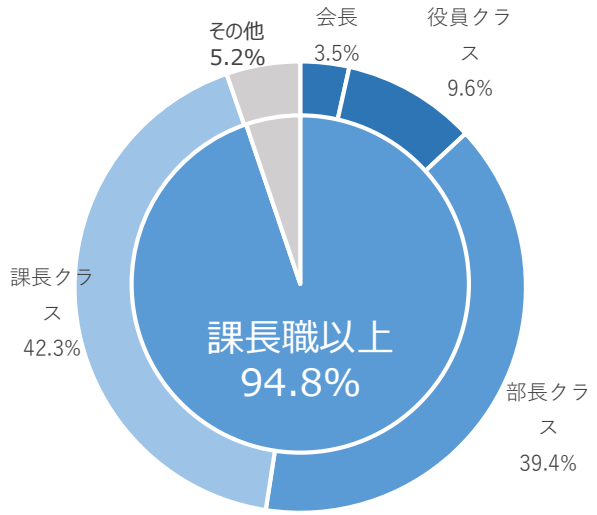
MEDIA GUIDE 読者属性

ITmedia エグゼクティブ

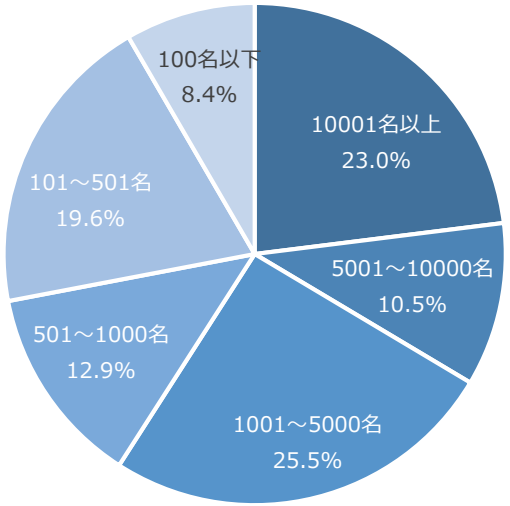
業種



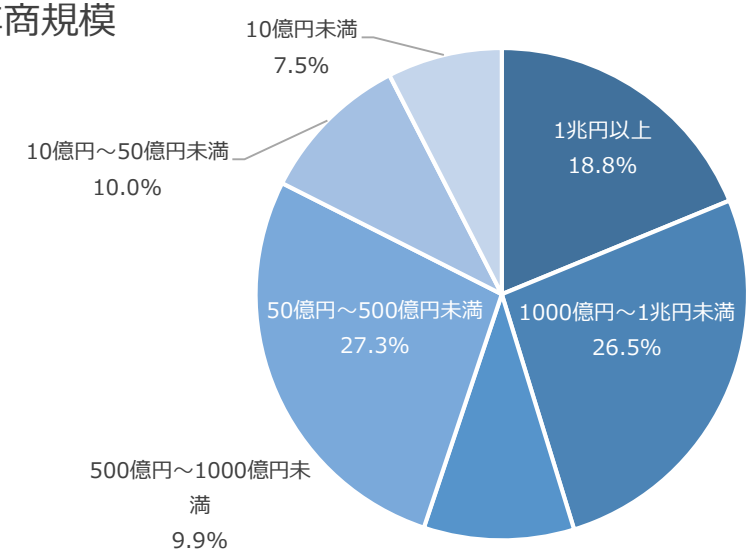
役職



従業員数



年商規模



Copyright © ITmedia Inc.

CAUTIONS

キャンセル料につきまして

申込書受領後または事務局案内開始後のキャンセルは、下記のキャンセル料が発生いたします。予めご了承下さい。

・開催日41日前まで　　：50%
・開催日40日以内　　：100%

消費税につきまして

消費税は別途申し受けます。

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
ネクプロは高精細な映像、音声を届ける仕組みを搭載し、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ぎ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５：視聴側における障害
総視聴数に対する単独（10%以下）の視聴不良はそれぞれ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。
10件単位で同様の症状がみられる（現場でご報告いただいた）場合は、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。

Copyright © ITmedia Inc.

Security Week

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13F
MAIL : sales@ml.itmedia.co.jp

Copyright © ITmedia Inc.