

Produced by



Security Week

ITmedia Security Week 2024 夏

侵入前提時代、「自社にとっての対策高度化」に欠かせない
構成要素とロードマップ

開催日時：2024年8月26日（月）～9月2日（月）

申込締切：2024年6月14日（金）

SUMMARY

名称	ITmedia Security Week 2024 夏	視聴方法	無料登録制
主催	  	事前 申込者数	約1,000名想定
開催日時	2024年8月26日(月)～9月2日(月)	告知/集客	  
申込締切	2024年6月14日 (金)	運営	アイティメディア株式会社 セミナー運営事務局
イベント形式	集合型オンラインセミナー		

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。

PRODUCER'S COMMENT

侵入前提時代、「自社にとっての対策高度化」に欠かせない 構成要素とロードマップ

データ、システム資産、それらへのアクセスが社内外で入り乱れている今、侵入前提の仕組みは全ての企業組織にとって不可欠なものとなっています。

ゼロトラストという概念も浸透し、認証、クラウドセキュリティなど
昨今は各種構成要素への関心も改めて高まっているようです。

ただし、ビジネスや組織の在り方、それらの課題は各社各様。銀の弾丸はない以上、各社が「自社に最適化した仕組み」を吟味、実装することが不可欠です。

ITmedia Security Week 2024 夏は、

検知→対処をより確実化、迅速化するノウハウ、手段にフォーカス。

数ある課題の中でも「自社にとっての対策高度化」につながる最新情報をお届けします。

SECTIONS

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でしょうか。

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します。

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アイデンティティ管理／統制を考えます。

3 クラウドセキュリティ

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します。

4-1 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り、それをすり抜けたとしても検知し行動を止めることができる仕組みと、組織が持つ情報を管理、保護するための技術を手に入れましょう。

4-2 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く、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ります。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ます。

5 ランサムウェア対策のためのレジリエンス

ランサムウェア攻撃に対抗するための事前対策から、侵入を許した際の初動対応や封じ込め、バックアップ取得や復旧といった“出口対策”までを含めてサイバーレジリエンス能力の強化に役立つノウハウをお届けします。

6-1 セキュリティ運用（自動化） **New!**

人材不足に困る企業に対し、運用におけるさまざまな「自動化」手法を提案します。

6-2 セキュリティ運用（マネージドサービス） **New!**

マネージドセキュリティサービスに「セキュリティを丸投げ」するだけではその効果を最大限に発揮できません。本ゾーンは任せるべき部分と自社で実施する部分の切り分けなどをはじめ「上手な頼り方」を伝えます。

SECTION 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。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

#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

- 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？
- 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

SECTION 2-1. ゼロトラストセキュリティ

概要

「将来を見据えたゼロトラスト導入 その第一歩を踏み出す」

「ゼロトラスト」はパスワードを超え、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。

キーワード

#EDR

#XDR

#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

#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

SECTION 2-2. 多要素認証から始めるID管理・統制

概要

「アイデンティティとポリシーをもう一度捉え直す」

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。これはIDを「アイデンティティ」と正しく捉え、その扱いに関する「ポリシー」を考え直すことにつながるでしょう。

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

#多要素認証関連ソリューション

#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

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
- IDaaSについてを知りたい

SECTION 3. クラウドセキュリティ

概要

「2025年夏、クラウドセキュリティの焦点は」

クラウドが当たり前になった時代、そのセキュリティを考えることも当然の時代になりました。しかし、クラウドが指すイメージは広範なものとなり、どのセキュリティに取り組むべきか、フォーカスが定められない状況にあるかもしれません。

もはやクラウドセキュリティは遍在するレベルにまで達しようとしています。

そこで本ゾーンでは、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、**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 (鍵管理を含む)

視聴者の抱える課題意識

- いま検討中/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知りたい
- 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知りたい
- 「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

SECTION 4-1. エンドポイント対策&情報管理

概要

エンドポイント、そしてそこに含まれ、そこから見える情報の管理は引き続き組織の安全確保に重要なポイントとなっています。ウイルス対策ソフトを超え、EDRを活用している企業にとっては当たり前のように聞こえるかもしれませんが、それでもエンドポイントに起因するインシデントはあとを絶ちません。エンドポイントが侵入のきっかけにならずとも、弱い機器は横展開のターゲットとなり、自社に取っての最重要なデータが盗まれてしまう可能性があります。

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から、対策を考えていく必要があるでしょう。その第一歩として、**エンドポイントの対策をここでもう一度考え、さまざまな重要情報資産を守るための最新事情を知り、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) 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わからない
- 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わからない
- 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わからない
- フィッシングから利用者/組織を守る方法がわからない

SECTION 4-2. アタックサーフェス管理

概要

「拡大するアタックサーフェス—攻撃者の選択肢を狭めよ」

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することができました。しかしもはやこの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、すでに攻撃者は社内にも到達していると考えることも必要です。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管理 (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改ざん対策

#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、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向ける

SECTION 5. ランサムウェア対策のためのレジリエンス

概要

ランサムウェア攻撃が増加し、攻撃手段が多様化する今、「万が一侵入されたら」ではなく「侵入される」という前提で防御を組み立てることが必須となっています。このためには自社の“サイバーレジリエンス”能力をいかに高めるかが鍵となるでしょう。

本ゾーンは、ランサムウェア攻撃に対抗するための事前対策から、侵入を許した際の初動対応や封じ込め、適切なデータバックアップ取得やビジネスの復旧といった“出口対策”までを含めて**サイバーレジリエンス能力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

#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

#SASEソリューション

#EPP製品全般

#DLP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
- ランサムウェア攻撃に遭った場合、被害状況を適切に把握したい
- 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
- ランサムウェアに対する従業員のITリテラシーが低い

SECTION 6-1. セキュリティ運用（自動化）

概要

「セキュリティ人材不足を解決する「運用自動化」の極意」

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、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や機械学習を基にした「運用の自動化」を解決策としませんか。

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、確実な運用を考えませんか。本ゾーンでは、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。

キーワード

AIによるセキュリティ運用自動化

SOAR

UEBA

SIEM

XDR関連

視聴者の抱える課題意識

- 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

SECTION 6-2. セキュリティ運用（マネージドサービス）

概要

セキュリティ人材の不足が深刻化している今、十分なリソースをセキュリティ運用に充てるのは一部の大企業を除いて困難です。多くの中堅・中小企業は限られたリソースをやり繰りして激化するサイバー攻撃に立ち向かっているのが実態でしょう。こうした企業の強い味方として注目を集めているのが、セキュリティ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です。最近のサービスは従来の運用監視といった業務に加えて、インシデント対応や封じ込め、セキュリティ強化の提案といった包括的な支援を提供しています。

しかしこれに胡坐をかき「セキュリティを丸投げ」するだけでは適切なセキュリティ対策は得られません。**本ゾーンはサービスの選定ポイントや、任せるべき部分と自社で実施する部分の切り分けなどをはじめとした「上手な頼り方」を伝えます。**

視聴者の抱える課題意識

- 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
- 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
- セキュリティ運用における知識や経験、ノウハウに乏しく、リリース不足
- 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
- 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
- セキュリティ運用を担う人材が不足している
- 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

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

SECTION1-5の タイムテーブル	SECTION 1 サイバーセキュリティ リスクとマネジメント	SECTION 2-1 ゼロトラストセキュリティ	SECTION 2-2 多要素認証から始める ID管理・統制	SECTION 3 クラウドセキュリティ	SECTION 4-1 エンドポイント対策 &情報管理	SECTION 4-2 アタックサーフェス管理	SECTION 5 ランサムウェア対策 のためのレジリエンス	SECTION 6-1 運用自動化	SECTION 6-2 マネージドサービス	SECTION6の タイムテーブル
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 (ゼロトラスト)	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	モーニングセッション4 (エンドポイント)	モーニングセッション4 (エンドポイント)	モーニングセッション5	専用ゾーン 基調講演	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)	スポンサーセッション2-1 (ゼロトラスト)	スポンサーセッション 3-1	スポンサーセッション4-1 (エンドポイント)	スポンサーセッション4-1 (エンドポイント)	スポンサーセッション 5-1	スポンサーセッション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)	スポンサーセッション2-2 (ゼロトラスト)	スポンサーセッション 3-2	スポンサーセッション4-2 (エンドポイント)	スポンサーセッション4-2 (エンドポイント)	スポンサーセッション 5-2	スポンサーセッション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)	基調講演2-1 (ゼロトラスト)	基調講演3-1	基調講演4-1 (エンドポイント)	基調講演4-1 (エンドポイント)	基調講演5-1	基調講演6-1 (運用自動化)	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)	スポンサーセッション2-3 (ゼロトラスト)	スポンサーセッション 3-3	スポンサーセッション4-3 (エンドポイント)	スポンサーセッション4-3 (エンドポイント)	スポンサーセッション 5-3	スポンサーセッション6-1 (運用自動化)	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)	スポンサーセッション2-4 (ゼロトラスト)	スポンサーセッション 3-4	スポンサーセッション4-4 (エンドポイント)	スポンサーセッション4-4 (エンドポイント)	スポンサーセッション 5-4	スポンサーセッション6-2 (運用自動化)	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)	基調講演2-2 (多要素認証)	基調講演3-2	基調講演4-2 (アタックサーフェス)	基調講演4-2 (アタックサーフェス)	基調講演5-2	基調講演6-2 (マネージドサービス)	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)	スポンサーセッション2-5 (多要素認証)	スポンサーセッション 3-5	スポンサーセッション4-5 (アタックサーフェス)	スポンサーセッション4-5 (アタックサーフェス)	スポンサーセッション 5-5	スポンサーセッション6-3 (マネージドサービス)	16:20~17:20	
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)	スポンサーセッション2-6 (多要素認証)	スポンサーセッション 3-6	スポンサーセッション4-6 (アタックサーフェス)	スポンサーセッション4-6 (アタックサーフェス)	スポンサーセッション 5-6	スポンサーセッション6-4 (マネージドサービス)		

※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。

【プラチナプラン限定の枠】各日のスポンサーセッション1枠目、3枠目、5枠目

※タイムテーブルは適宜変更の可能性がございます

SPONSORED MENU

	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!	協賛セッションのテーマに興味がある参加者へアプローチ可能!	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可能!	協賛セッションのテーマに興味がある視聴者のリストを獲得可能!
	ダイヤモンド	プラチナ	ゴールド	全リスト	セッションリスト
スポンサーセッション Live配信+アーカイブ	●	●	●	-	-
専用ゾーン	●	-	-	-	-
パネルディスカッション	-	-	-	-	-
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	-
協賛セッション申込者リスト	想定300名	想定350名	想定350名 ~450名 (最大)	-	想定350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	●	●	●	-	-
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-	¥1,800,000-	¥1,000,000-

※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。
 ※協賛セッション申込者リスト数はいずれのセッションも想定値ですが、セッション2および6につきましては、
 他セッションよりもスポンサーセッション数が少ないため、特にセッ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。

SCHEDULE

申込締切 2024年6月14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 2024年7月下旬



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週間前程度）。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8月26日(月)～9月2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。

SPONSORED MENU

スポンサーセッション



御社の製品やサービスをPRできる、スポンサーセッション枠をご利用いただけます！

機能：セッションアンケート・セッション紹介・質問送信フォーム・資料DL・関連リンク

全申込者リスト

イベントに申込みをされた、全申込者の名刺情報のリストをお渡しします。

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
納期：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

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いたします。

※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。

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いたします。

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いただけます。

※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に設定いただけます。
※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。

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）等も合わせて提供いたします。
※設問はアイティメディアが設定で個別設定不可。

スポンサーロゴ掲載

イベントの集客サイトに、貴社のロゴを掲示し、貴社サイトへのリンクを設定いたします。

資料配布

貴社セッション内で視聴者に向けて、資料の配布が可能です。

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

アイティメディアで一般来場者へアンケートを行っており、その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。

※個人情報は含まない、集計データでの提供です。

SPONSORED MENU

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。

OPTIONS

リード情報×主催アンケート回答情報付与

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！

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いたします。
※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

■納品イメージ

会社名	従業員規模	セキュリティ対策、いま 本当に必要なこと	サブライフェーン夜型に びびらない、新たな商機	クラウド&ゼロトラスト	エンドポイント対策&脅威 管理	企業名	職位	変化	「課長以 上の役職 者の有無」 フラ グ	「等入予 定1年以内 の有無」 フラ グ	「新規シ ステム等 入目的の 有無」 フラ グ	「職歴値
8												
9	総合警備保障 (株)	06.5000人以上	●	●	●							
10	エヌ・ティ・ティ・データ先端技術株式会社	05.1000人～5000人未満	●	●	●	エヌ・ティ・ティ・データ						
11	西日本電信電話株式会社 東海支店	05.1000人～5000人未満	●	●	●	西日本電信電話 (株)						
12	株式会社デンソー	05.1000人～5000人未満	●	●	●							
13	株式会社三井住友銀行	06.5000人以上	●	●	●	(株) 三井住友銀行						
14	SCSK株式会社	06.5000人以上	●	●	●	SCSK (株)						
15	昭和産業株式会社	05.1000人～5000人未満	●	●	●	昭和産業 (株)						
16	タカサン乳業株式会社	05.1000人～5000人未満	●	●	●							
17	株式会社TMI	06.5000人以上	●	●	●							

通常のリード情報

アンケート回答
情報付与

■納期

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期はイベントによって異なります

料金 **20万円**

リード カスタム納品サービス

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いたします！

■納品イメージ



■備考

対応可能ツールはお問い合わせください。

※Lead Brizzy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

■納期

閉幕後6-8営業日後
※納期はイベントによって異なります

件数	料金
～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

※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)

OPTIONS

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いたします。
※mp4形式
※配信時のままの状態となるため、編集はありません。

料金 **5万円**

セッション動画活用リード獲得

セミナーの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し、セミナー後も継続的に属性&件数を保証したリード獲得を行うことができるサービスです。

詳細：
<http://go.itmedia.co.jp/l/291242/2022-09-02/2bfy1tr>

料金 **30万円~**

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するオプションです。専用のプロ機材と収録会場を提供し、手軽に動画制作ができます。講演者のお顔と資料スライドを同時に収録し、画面右上に肩書やテーマのテロップを入れることも可能です。オンラインでの収録も対応しています。
※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 **18万円**

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です。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となります。
※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：go.itmedia.co.jp/l/291242/2022-10-19/2bvm1jn

料金 **20万円**

行動履歴ターゲティングタイアップ

読者の行動データを活用して、興味のある人を貴社のタイアップ記事に誘導し、拡張配信によって同じ興味を持つ人々にリーチするサービスです。このメニューは、ライブやオンデマンドの配信や録画データを活用して要点をまとめ、別途の取材は行いません。

詳細：<https://go.itmedia.co.jp/l/291242/2022-09-09/2bicm9g>

料金 **150万円**

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・配信までサポートします。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であり、プロ機材と収録会場を提供しますので、手軽に動画制作ができます。

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

料金 **230万円**

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致します。効果的に実施することで、高い反響率と顧客獲得効果が期待できます。

- 最低実施件数：50件~
- 所要期間：3~4週間（250件の場合）

※1000件以上は不可

料金 **7万5千円~**

セッションパンフレット作成

貴社セッションを元にオリジナルのパンフレットを制作し、印刷用データを納品。データを営業資料としてセミナーや展示会での配布にご利用頂けます。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し、読者への認知獲得も行います。

詳細：<http://go.itmedia.co.jp/l/291242/2023-12-15/2cycg7h>

料金 **120万円**

※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）

PAST EVENT



タイトル	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
日時	2024年2月26日（月）～ 3月4日（月） ※3月18日までアーカイブ配信
全申込者数	1,110名
視聴者数	666名
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)	arcserve Japan合同会社、株式会社アウトソーシングテクノロジー、アクロニス・ジャパン株式会社、株式会社アシュアード、イーセットジャパン株式会社、Veeam Software Japan株式会社、ウィズセキュア株式会社、株式会社エーアイセキュリティラボ、SBテクノロジー株式会社、株式会社NSD、NTTデータルウィーブ株式会社、オープンテキスト株式会社、キヤノンマーケティングジャパン株式会社、クラウドストライク合同会社、Cloudflare Japan株式会社、Sysdig Japan合同会社、ジョーシス株式会社、S k y 株式会社、ゼットスケラー株式会社、ソニービズネットワークス株式会社、ソフォス株式会社、Tanium合同会社、株式会社DTS、テクマトリックス株式会社、デジタルアーツ株式会社、テナブルネットワークセキュリティジャパン株式会社、日本アイ・ビー・エム株式会社、日本マイクロソフト株式会社、ニュートン・コンサルティング株式会社、Netskope Japan株式会社、日鉄ソリューションズ株式会社、フリー株式会社、ベーステクノロジー株式会社、株式会社ベリサーブ、HENNGE株式会社、マイクロフォーカスエンタープライズ株式会社
申込みページ URL	https://members07.live.itmedia.co.jp/library/NjQyMDE%253D?group=sec240226
開催報告書	http://go.itmedia.co.jp/l/291242/2024-03-27/2cz456d

CAUTIONS

①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。

発注書の取り交わし後のキャンセル
登録用紙の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 : 50%
開催日40日以内のキャンセル : 100%

②消費税につきまして

消費税は別途申し受けます。

③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。

④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

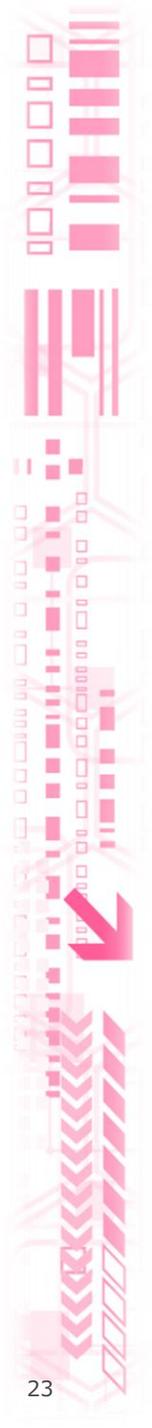
映像・音声ともに落ちてしまう可能性があります。
バックアップPCから配信停止のお詫びをアナウンスし、後日オンデマンド版をご案内いたします。

●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ため、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。



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