2024年度
10~12月

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

ITmedia Security Week 2024 秋

Security Week

脅威は待ってくれない！

セキュリティ人材不足を今度こそ解決できる「多彩なアプローチ」

開催日時：2024年11月25日(月)～12月3日(火)

セッションプラン最終締切：2024年11月1日(金)
リストプラン最終締切　　：2024年11月20(水)

SUMMARY

名称	ITmedia Security Week 2024 秋 脅威は待ってくれない！ セキュリティ人材不足を今度こそ解決できる「多彩なアプローチ」
主催	@IT atmarkIT / ITmedia エンタープライズ / ITmedia エグゼクティブ
開催日時	2024年11月25日(月)～ 12月3日(火)
申込締切	セッションプラン：2024年11月1日(金) リストプラン：2024年11月20日(水)
イベント形式	集合型オンラインセミナー
事前申込者数	約1,000名想定 ※過去開催の実績値に基づく想定値のため、実際には開催するテーマ数などに応じて前後する場合がございます

想定視聴者属性	経営者、経営企画の方、社内情報システムの運用・方針策定をする立場の方、企業情報システム部門の企画担当者、運用管理者、SIerなど
告知・集客	@IT atmarkIT / ITmedia エンタープライズ / ITmedia エグゼクティブ
テーマ	SECTION 1　：サイバーセキュリティリスクとマネジメント SECTION 2　：ゼロトラストセキュリティ SECTION 2-2：脱VPNって、本当にやる必要があるの？ SECTION 3　：クラウドセキュリティ SECTION 4-1：IT資産管理 SECTION 4-2：アタックサーフェス管理 SECTION 5-1：攻撃経路の再点検（攻撃事例） SECTION 5-2：攻撃のリカバリー SECTION 6-1：セキュリティ運用自動化 SECTION 6-2：マネージドサービス SECTION 7　：サイバーレジリエンスアワード
運営	アイティメディア株式会社

※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

脅威は待ってくれない！
セキュリティ人材不足を今度こそ解決できる「多彩なアプローチ」

セキュリティ事件・事故報道が相次ぐ中、企業の危機感は着実に高まっています。
ゼロトラスト、クラウドセキュリティの実装、改善に取り組む例も増えるなど、
対策を高度化することの重要性は着実に浸透していると言えるでしょう。
しかし同時に、企業を悩ませているのがセキュリティ人材の不足です。
「対策を強化したいが何から手を付けるべきか分からない」
「スキルが属人化しておりインシデント対応に時間がかかる」など、
課題の多くは「人」に根差しています。
無論、人材獲得・育成に時間が必要なことは言うまでもありません。
が、脅威が待ってくれるわけでもないのです。

――ITmedia Security Week 2024秋では人材不足問題にフォーカス。
あらゆる角度から現実的な解決策を紹介します。

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	New! 脱VPNって、 本当にやる必要があるの？	最近はVPN経由で社内ネットワークに侵入された話をよく聞く。今でもVPN装置を社員のリモートアクセスや関係企業との間の通信に使う企業があるが、本当にやめる必要があるのか。 やめるなら、何に切り替えればいいのだろうか。
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	New! IT資産管理	アタックサーフェイスマネジメントの入口となる「IT資産管理」を、物品管理だけではなくセキュリティの文脈から考え、どのような考え方で、何ができるかを探ります。
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。
5-1	New! 攻撃経路の再点検（攻撃事例）	サイバー攻撃の侵入経路が拡大する今、これを再点検し、“穴”を適切に埋めることが求められています。本ゾーンはフィッシングをはじめとした「人の脆弱性」などに根差した攻撃の事例を振り返りつつ、有効な対策を提案します。
5-2	New! 攻撃のリカバリー	ランサムウェアの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	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	マネージドサービス	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

基調講演 講師候補

※ご登壇をお約束するものではございません。

SECTION 2-1.　ゼロトラストセキュリティ

概要

「納得感とともにゼロトラストを実現せよ」

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、必要なスキルと考え方を紹介しつつ、セキュリティの有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。

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

基調講演 講師候補

※ご登壇をお約束するものではございません。

講演イメージ（共通）

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お話いただく。苦労している部分、変わった部分を語る事例を中心とした講演を想定。

SECTION 2-2.　脱VPNって、 本当にやる必要があるの？

概要

最近はVPN経由で社内ネットワークに侵入された話をよく聞く。
今でもVPN装置を社員のリモートアクセスや関係企業との間の通信に使う企業があるが、本当にやめる必要があるのか。
やめるなら、何に切り替えればいいのだろうか。

キーワード

＃脱VPN　＃ZTNA　＃SASE　＃UTM

視聴者の抱える課題意識

- なぜVPN装置でだめなのかが分からない
- セキュリティにコストをかけたくない

基調講演 講師候補

※2024年10月28日（月）に開催する「@IT NETWORK Live Week 2024 秋」の基調講演の再配信となります。

SECTION 3.　クラウドセキュリティ

概要

「インシデント多発中！ クラウドセキュリティが事業の明暗を分ける」

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。**
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

基調講演 講師候補

※ご登壇をお約束するものではございません。

講演イメージ（共通）

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想定。

SECTION 4-1.　IT資産管理

過去開催類似テーマ：エンドポイント

概要

「敵を知り、己を知れば、百戦危うからず」

――この言葉が、ITの文脈でも重要となっています。特にセキュリティにおいては、攻撃者は深く静かに侵入し、私たちの資産を改ざんし、盗み、破壊しようとします。セキュリティ意識は高まり、攻撃者の視点で考えるという手法は広まりつつありますが、自分の足元にあるシステムを、私たちは知らなさすぎるのではないでしょうか。
脆弱性が明らかになったとき、その影響を受けるのはどこの、誰の端末なのでしょうか。侵害を受けたとき、ネットワークのどの部分に脅威が含まれるのでしょうか。これまでは固定資産管理の視点でしかできていなかった「IT資産管理」を、セキュリティにも使うために必要なスキルと考え方、そしてソリューションはどのようなものでしょうか。
本ゾーンでは注目される「IT資産管理」をセキュリティ文脈で考え、必要な情報をまとめて得られる機会となるはずです。

キーワード

＃IT資産管理　＃脆弱性マネジメント　＃ユーザー管理　＃VPN　＃ネットワーク機器
＃Web改竄対策　＃アタックサーフェイスマネジメント

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

基調講演 講師候補

※ご登壇をお約束するものではございません。

講演イメージ（共通）

エンドポイントに関連する最新の脅威情報、及び中小企業がどのような対策を最優先で行うかを選択するため、必要となる前提情報を紹介する。各分野における専門家から、セキュリティに不慣れな方でもなにか一つは持ち帰れるよう、平易に分かりやすく解説する講演を想定。

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、すで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。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に向ける

基調講演 講師候補 ※ご登壇をお約束するものではございません。

講演イメージ（共通）

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講演を想定。

SECTION 5-1.　攻撃経路の再点検（攻撃事例）

概要

テレワークやクラウドサービスの普及によって企業のシステム環境はより広範になりました。
これに伴い、サイバー攻撃者たちの侵入経路についても多様化・複雑化が進んでいます。特に近年は、
サポート詐欺やソーシャルエンジニアリング攻撃などの「人の脆弱性」を突いた攻撃によって、サービスアカウントなどが窃取されて機密情報の漏えいにつながっています。
こうした高度な攻撃を防ぐためにもサイバー攻撃の経路を分析することは急務です。
本ゾーンはフィッシングをはじめとした電子メール経由の攻撃やVPNの脆弱性など発生しがちな攻撃事例を振り返りつつ、攻撃経路の再点検およびこれに有効な対策を解説します。

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意識

- サイバー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サイバー攻撃が実行されるのかを知りたい
- 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 講師候補

※ご登壇をお約束するものではございません。

講演イメージ（共通）

サイバー攻撃における侵入経路をあらためて整理し、攻撃事例などを基に今注意すべき脆弱性や攻撃を明らかにした上で有効な対策を紹介する講演を想定。

SECTION 5-2.　攻撃のリカバリー

過去開催類似テーマ：ランサムウェア

概要

ランサムウェア攻撃が激化する今、「攻撃を受けるかも」ではなく「必ずいつかランサムウェア攻撃被害に遭う」という前提で先んじて対策を講じることが重要です。こうした侵入前提の防御策を組み立てる上で忘れてはならないのがバックアップをはじめとした攻撃からのリカバリーでしょう。

本ゾーンは、**ランサムウェアの侵入を万が一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”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意識

- 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 講師候補

※ご登壇をお約束するものではございません。

講演イメージ（共通）

サイバー攻撃からの復旧においてバックアップが果たす役割と効果を発揮する適切なバックアップ手法、この他、迅速にビジネスを復旧する上で企業組織としてどのような対応を取るべきかなどについての講演を想定。

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。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、確実な運用を考えてみませんか。
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

基調講演 講師候補

※ご登壇をお約束するものではございません。

講演イメージ（共通）

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講演を想定。

SECTION 6-2.　マネージドサービス

概要

セキュリティ人材不足が深刻化する中、サイバー攻撃に対抗するために、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に注目が集まっています。

十分なリソースをセキュリティ対策に割くことが難しい以上、マネージドセキュリティサービスを効果的に活用することが対策の鍵を握るわけですが、ただ「対策を丸投げ」するだけでは求める成果を得られないでしょう。
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「**失敗しないマネージドセキュリティサービスの使い方**」をお伝えします。

視聴者の抱える課題意識

- 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 講師候補

※ご登壇をお約束するものではございません。

講演イメージ（共通）

マネージドセキュリティサービスを選定中の方に向けて、どのような観点でサービスを選ぶべきかから、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までを伝える講演を想定。

SECTION 7.　サイバーレジリエンスアワード

アワードが目指すもの

「脅威は待ってくれない！サイバー攻撃による「深刻な被害」ゼロを目指して」

ITmedia Security Weekと一般社団法人サイバーセキュリティ連盟が共同で開催する「サイバーレジリエンスアワード 2024」は、インシデントを乗り越え、優れたセキュリティ対策を実施している企業を表彰すると同時に、最新のセキュリティ動向や技術を紹介します。他のセクションではアプローチが出来ない、セキュリティ対策に消極的な層に対し、サイバー攻撃の進化と新たな脅威を理解してもらい、対策強化の重要性を再認識していただくことを目指しています。

概要

2024年11月7日(木)に開催する「サイバーレジリエンスアワード2024」の特別編集版としてお届け。
表彰を受けたユーザ企業の事例講演を通じて、
サイバー攻撃の進化と新たな脅威を理解し、
対策強化の重要性を再認識する機会を提供いたします。
併せて最新のセキュリティ動向や技術を紹介します。

視聴者層のイメージ

基調講演 講師候補

※調整中
※2024年11月7日(木)開催の「サイバーレジリエンスアワード 2024」の講演動画の再配信を予定しております。
※講演は変更になる場合がございます。

講演イメージ

サイバー攻撃のインシデントを乗り越えた事例企業に、
いかにインシデントを乗り越え、その後どのような対策を施したのかをお話いただきます。

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

Day1 - Day6 Time table	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 脱VPNって、 本当にやる必要があるの？	SECTION 3 クラウド セキュリティ	SECTION 4-1 IT資産管理 SECTION 4-2 アタックサーフェス管理	SECTION 5-1 攻撃経路の再点検 （攻撃事例） SECTION 5-2 攻撃のリカバリー	SECTION 6-1 セキュリティ運用自動化 SECTION 6-2 マネージドサービス
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3	モーニングセッション4 **IT資産管理**	モーニングセッション5 **攻撃経路の再点検（攻撃事例）**	専用ゾーン 基調講演
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	スポンサーセッション 3-1	スポンサーセッション4-1 IT資産管理	スポンサーセッション5-1 攻撃経路の再点検（攻撃事例）	スポンサーセッション1
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	スポンサーセッション 3-2	スポンサーセッション4-2 IT資産管理	スポンサーセッション5-2 攻撃経路の再点検（攻撃事例）	スポンサーセッション2
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3-1	基調講演4-1 **IT資産管理**	基調講演5-1 **攻撃経路の再点検（攻撃事例）**	基調講演6-1 **セキュリティ運用自動化**
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	スポンサーセッション 3-3	スポンサーセッション4-3 IT資産管理	スポンサーセッション5-3 攻撃経路の再点検（攻撃事例）	スポンサーセッション6-1 セキュリティ運用自動化
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	スポンサーセッション 3-4	スポンサーセッション4-4 IT資産管理	スポンサーセッション5-4 攻撃経路の再点検（攻撃事例）	スポンサーセッション6-2 セキュリティ運用自動化
15:10〜15:50	基調講演1-2	基調講演2-2 *再配信 （脱VPN）	基調講演3-2 **中止予定**	基調講演4-2 **アタックサーフェス管理**	基調講演5-2 **攻撃のリカバリー**	基調講演6-2 **マネージドサービス**
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（脱VPN）	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管理	スポンサーセッション5-5 攻撃のリカバリー	スポンサーセッション6-3 マネージドサービス
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（脱VPN）	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管理	スポンサーセッション5-6 攻撃のリカバリー	スポンサーセッション6-4 マネージドサービス

Day7 Time table	SECTION 7 サイバーレジリエンス アワード
13:00〜13:15	開会挨拶 アワード趣旨説明
13:15〜13:30	授与式
13:30〜14:10	事例講演7-1
14:20〜14:50	スポンサーセッション **開催中止**
15:00〜15:30	スポンサーセッション 7-2
15:40〜16:10	スポンサーセッション 7-3
16:20〜16:50	スポンサーセッション 7-4
17:00〜17:40	事例講演7-2
17:40〜17:45	閉会挨拶

※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

お申込み受付を終了いたしました

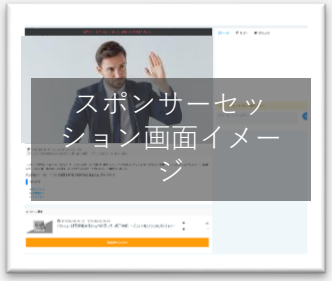
	1社限定！ 貴社テーマに関心の高い視聴者へ訴求可能！	貴社セッションを視聴した関心度の高い読者から、イベント全体の申込者まで幅広いリストを獲得可能！	協賛セクションのテーマに興味がある参加者へアプローチ可能！	スポンサーセッションの準備が難しい場合でも、多くのリストを獲得可能！	協賛セクションのテーマに興味がある視聴者のリストを獲得可能！
	ダイヤモンド	プラチナ	ゴールド	全リスト	セクションリスト
スポンサーセッション Live配信＋アーカイブ	●	●	●	-	-
専用ゾーン	●	-	-	-	-
スポンサーアンケート	●	●	●	-	-
全申込者リスト 想定1,000名	●	● （全申込者）	-	● （全申込者）	-
協賛セクション申込者リスト	想定300名～上限400名	想定350名	想定350名～上限450名	-	想定350名～上限450名
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。
※協賛セクション申込者リスト数は想定値です。特にセクション2および6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
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。

SPONSORED MENU

｜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名刺情報のリストをご提供
■ 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
■ 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

■ 協賛セクション申込者の名刺情報のリストをご提供
■ 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

■ 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

｜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。

SCHEDULE

申込締切

セッションプラン：2024年11月1日(金)
リストプラン　　：2024年11月20(水)

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

セッションの講演者情報、講演タイトル、貴社ロゴデータ等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10月23日(水)　※予定

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。登録・視聴促進の為、インセンティブを使用する場合がございます。

開催準備

2024年11月上旬頃

配布資料・視聴者向けセッションアンケート設問・動画納品など**講演に関する情報**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致します。

開催

2024年11月25日(月)～12月3日(火)

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**事前申込者リスト**をご提出致します。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致します。

上記スケジュールは目安であり、状況によって変更になる可能性がございます

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。
- 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 **¥180,000~**

｜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。
- セミナー閉幕日の3-5営業日後に納品するリード情報に、アンケート回答情報を付与したうえで納品いたします。
- 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金額は変動

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

~~¥2,450,000~~

料金 **¥2,300,000**

｜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）

OPTIONS

｜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：go.itmedia.co.jp/l/291242/2024-06-14/2czswgv

料金 **¥300,000~**

｜タイアップ プッシュ ターゲティング & ABM

- 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。
- 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

料金 **¥1,300,000~**

｜DXメディア横断 PV保証タイアップ

- 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

10,000PV保証 ~~¥1,900,000~~

料金 **¥1,700,000**

｜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。
- 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

料金 **¥1,200,000**

※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）

CAUTIONS

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%

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

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。

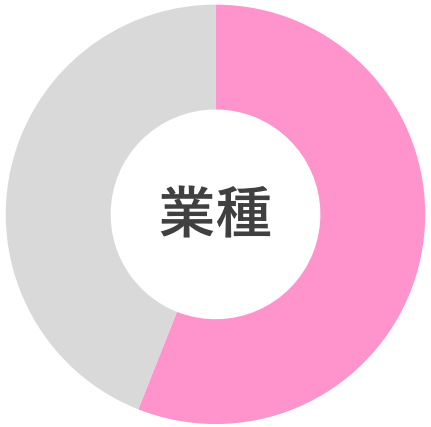
PAST EVENT

タイトル	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
日時	2024年8月26日(月)～ 9月2日(月)　※2024年9月17日(火)までアーカイブ配信
対象	経営者、経営企画の方、社内情報システムの運用・方針策定をする立場の方、企業情報システム部門の企画担当者 運用管理者、SIerなど
全申込者数	1,658名
視聴者数	1,082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、アクロニス・ジャパン株式会社、イーセットジャパン株式会社、株式会社インターネットイニシアティブ、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 C&S株式会社、SBテクノロジー株式会社、NTTコミュニケーションズ株式会社、エムオーテックス株式会社、エントラストジャパン株式会社、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、KDDI株式会社、サイバーリーズン合同会社、GMOサイバーセキュリティbyイエラエ株式会社、シスコシステムズ合同会社、ジョーシス株式会社、Ｓｋｙ株式会社、ソフトバンク株式会社、Tanium合同会社、株式会社ＤＴＳ、東京エレクトロン デバイス株式会社、東芝ITサービス株式会社、トレンドマイクロ株式会社、日本マイクロソフト株式会社、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PFU、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、フォーティネットジャパン合同会社、ペンタセキュリティ株式会社、マイクロフォーカスエンタープライズ株式会社、メンロ・セキュリティ・ジャパン株式会社
申込みページURL	https://members05.live.itmedia.co.jp/library/NzMxMjQ%253D?group=SEC2024SMR
開催報告書	https://go.itmedia.co.jp/l/291242/2024-09-25/2d19t94

MEDIA GUIDE

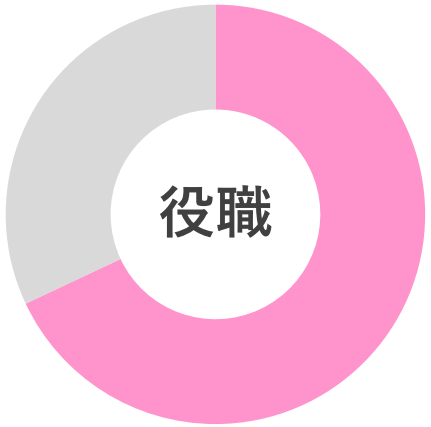
“ビジネスを変革する” ITエキスパートのための技術専門メディア

■媒体名　@IT
■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



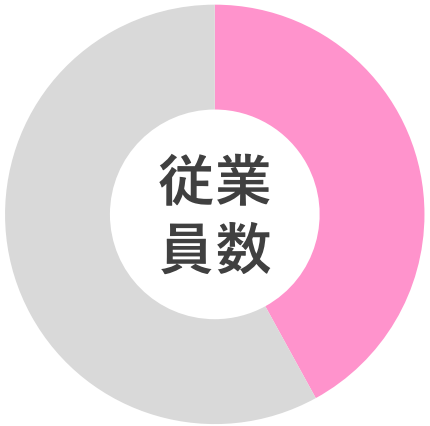
ユーザー企業 約56%

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%



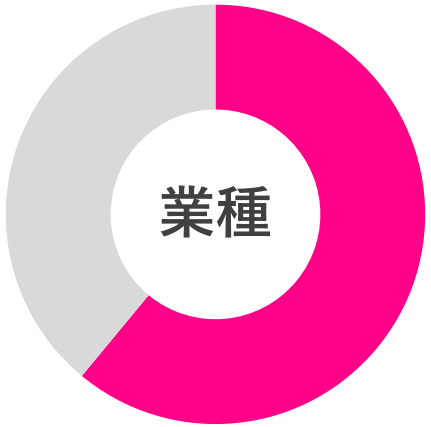
1000人以上 約41%

主な内訳：1000人～5000人未満18.4%,
5000人以上24%

MEDIA GUIDE

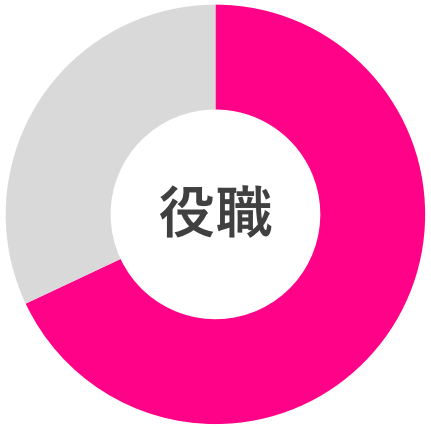
ITによってビジネスを革新するビジネスリーダー向け実践情報サイト

■媒体名　ITmedia エンタープライズ
■URL　https://www.itmedia.co.jp/enterprise/
■ PV　約122万 PV/月　約73万 UB/月　※2024年2月実績
■メルマガ配信数　約24万通



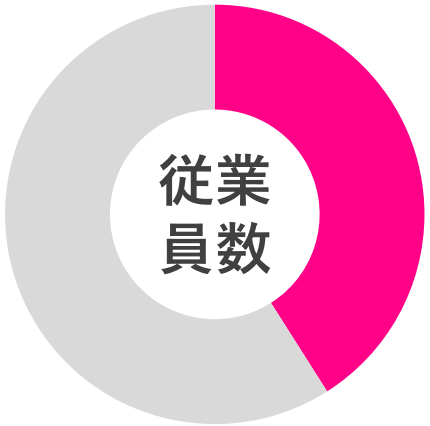
ユーザー企業 約61%

主な内訳：製造業37,9%,商社・流通・サービス業27%



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%



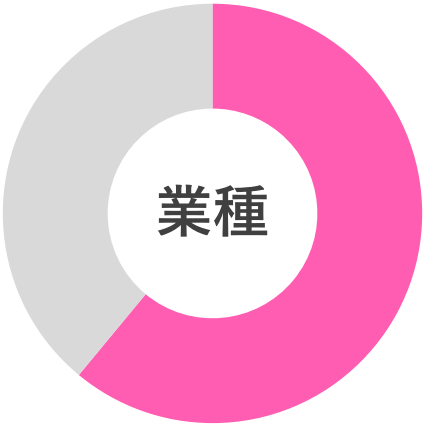
1000人以上 約41%

主な内訳：1000人～5000人未満20.3%,
5000人以上20.6%

MEDIA GUIDE

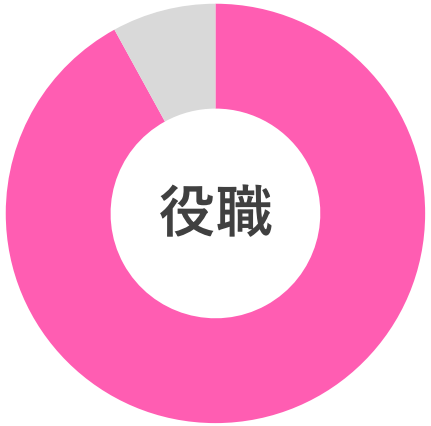
企業の明日を変えるエグゼクティブとCIOのためのコミュニティー

■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



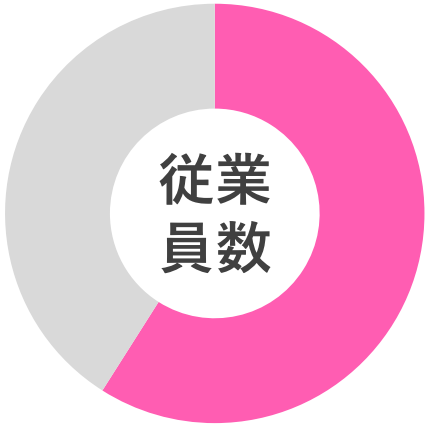
ユーザー企業 約61%

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%

メールでのお問い合わせ

mail：sales@ml.itmedia.co.jp
アイティメディア株式会社 営業本部

デジタルイベントの最新情報はこちら
https://promotion.itmedia.co.jp/plan