

2025年
3月

ITmedia Security Week 2025 冬

「危機感の解像度を上げる」「全社の理解を獲得する」ために

セキュリティ人材として持つべき
観点、言語、ノウハウ

開催日 : 2025年3月3日(月) ~ 3月11日(火)

申込締切 : セッションプラン…2025年2月7日(金)
リストプラン …2025年2月26日(水)



名 称	ITmedia Security Week 2025 冬 「危機感の解像度を上げる」 「全社の理解を獲得する」ために—— セキュリティ人材として持つべき観点、言語、ノウハウ	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
主 催 ・ 企 画	  	開催テーマ	・ セクション1 ：サイバーセキュリティリスクとマネジメント ・ セクション2 ：ゼロトラストセキュリティ ・ セクション3 ：アタックサーフェス管理 ・ セクション4-1：IT資産管理 ・ セクション4-2：クラウドセキュリティ ・ セクション5-1：攻撃経路の再点検（攻撃事例） ・ セクション5-2：攻撃のリカバリー ・ セクション6-1：セキュリティ運用自動化 ・ セクション6-2：マネージドサービス ・ セクション7 ：サイバーレジリエンスアワード
開催日	2025年3月3日(月)～ 3月11日(火)		
申込締切	セッションプラン…2025年2月7日(金) リストプラン …2025年2月26日(水)		
イベント形式	複数社協賛型デジタルイベント		
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、実際には開催テーマ数などに応じて前後する場合がございます	告知・集客	  
		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。

「危機感の解像度を上げる」「全社の理解を獲得する」ために **セキュリティ人材**として持つべき**観点、言語、ノウハウ**

ランサムウェアをはじめサイバー攻撃が頻発している今、
「侵入前提の対策」は必須となっています。
しかし、危機感を抱いていても対策の進め方が分からない、予算を確保できない
といったケースも多いようです。
事実、有効な対策を取る上では、技術面だけではなく、業務特性、費用対効果など、
技術以外の観点も不可欠です。
また、管理層、経営層の理解を得るためのコミュニケーション力も求められます。
手段は豊富にあっても有効に取り込めない真因は、実はそうした点にあるのではない
でしょうか。

——ITmedia Security Week 2025 冬では
「セキュリティ人材として持つべき観点」にフォーカス。
各セッションを通じて「危機感」の解像度を上げるとともに、
事業部門、管理層、経営層との共通言語となる情報源を提供します。

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「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	ゼロトラストセキュリティ	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、有識者に移行期での防御ポイントや攻撃者の視点などを解説していただく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。
3	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は到達している」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、インフラ改革も含めて考えます。
4-1	IT資産管理	アタックサーフェ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、何ができるかを学びます。
4-2	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。
5-1	攻撃経路の再点検（攻撃事例）	サイバー攻撃経路を再点検し“穴”を適切に埋めるためには、主要攻撃経路の分析や被害事例の収集が不可欠です。本ゾーンは「人の脆弱性」や「脱VPN」といったキーワードから入り口対策に有効なポイントを解説します。
5-2	攻撃のリカバリー	ランサムウェアインシデント発生時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”の強化に役立つ情報を提供します。
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（MSS）にセキュリティ対策を丸投げするだけでは、サービスの効果を最大限に発揮するのは困難です。本セクションはMSS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解説します。
New! 7	サイバーレジリエンスアワード	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きます。

| 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。

| 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？
- 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

| 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
- 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

| 講演イメージ（共通）

ビジネスの変革や新しい働き方の実現するために不可欠なサイバーセキュリティの取り組みを企業の方からご紹介いただくとともに、セクション1では専門家から急速に増しているサプライチェーンのセキュリティリスクについても最新動向を交え、解説いただく。

| 概要

「ゼロトラスト、現場から見るか、経営視点で考えるか」

現在の技術やインシデントの状況を考えると、「ゼロトラスト」に向かうという方向性になるのは間違いありません。

しかし、その道のりは長く陰しく「技術だけでなく、その考え方をいかに組織に浸透させるか」は、大きな課題の一つです。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、それらを取り扱う「人」の要素も重要です。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しつつ、「現場や経営層を含め、導入する「人」がどのようなスキルを必要とするのか」「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いいのか」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。

| 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

| キーワード

- EDR、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

| 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いて、苦勞している部分、変わった部分を語る事例講演を想定。加えて、ゼロトラストアーキテクチャに移行するために、組織内で現場や経営層に向けてどういうメッセージを発信すべきかのアドバイスをいただく。

| 概要

「全員が意識し、攻撃可能な“表面”を把握せよ」

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。

| 視聴者の抱える課題

- 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が、組織として次に何をすべきか悩んでいる
- 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

| 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

| 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に必要な情報を伝える。「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、といった事例や、今後どのような心構えが必要なのかを、アタックサーフェス管理の先端をウォッチする識者の目から伝える。

| 概要

「可視化から見直すIT資産管理」

サイバー攻撃者は深く静かにシステム侵入し、IT資産を改ざんし、盗み、破壊しようとします。この現状を踏まえると、「自社にとって重要な資産とは何か」「重要資産を適切に管理できているかどうか」「重要資産が万が一盗まれたときトラッキングできる仕組みを整えているかどうか」など考えるべきことは山ほどあります。

本セクションはセキュリティの文脈から、セキュリティ担当者や総務担当者だけでなく、ITを利用する現場や経営者の立場で「IT資産管理」を考えます。

| 視聴者の抱える課題

- 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

| 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
- アタックサーフェスマネジメント

| 講演イメージ（共通）

IT資産管理ができている企業とできていない企業で、例えばランサムウェアなどのマルウェアが社内に侵入した場合にどのように見え方が変わるのかを、攻撃事例から解説いただく。また、資産管理を強化する上で、組織内でどのように上司と連携すべきかという視点でも解決する。

| 概要

「クラウドセキュリティの重要性を説明できますか？」

「クラウド利用にはセキュリティが必須」—その当たり前のようなことを、新人や現場、経営層にどう説明したらいいのでしょうか。簡単のように見えて、説明するにはかなりのスキルが必要です。技術だけでなく、それぞれの立場を理解し、言葉を変える必要もあります。もしかしたら、それこそが今最も必要とされるクラウドセキュリティのスキルなのかもしれません。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に取り組む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で用意するには、全組織が一丸となる必要があります。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ます。

| 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。

| 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）

| 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。

| 概要

「攻撃の入り口、守れていますか？」

サイバー攻撃の侵入経路が多様化・複雑化する今、これを再点検し、“穴”を適切に埋めることは企業にとって急務となっています。特にサイバー攻撃の主要な侵入経路は電子メールから、VPN機器へと変化している中、企業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」を突いた攻撃への対処に加え、「脱VPN」を視野に入れた新たなセキュリティシステムを構築する必要があります。

本セクションは、攻撃経路の再点検してサイバー攻撃の入り口対策を講じたい企業に向け、主要攻撃経路の分析や被害事例を踏まえて、効果的な情報を提供するセクションです。

| 視聴者の抱える課題

- 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

| キーワード

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

| 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します。

| 概要

「侵入前提の出口対策」

サプライチェーン全体を狙ったランサムウェア攻撃被害が大きな話題を集めています。今や規模にかかわらず全ての企業が被害に遭う前提で対策を講じることは不可欠だと言えるでしょう。そして侵入前提の対策の要となるのがバックアップです。

本セクションは、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など“出口対策”に焦点を絞ったセクションを予定しています。

| 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

| 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

| 講演イメージ（共通）

“出口対策”に焦点を絞り、サイバー攻撃やインシデントにおける初動対応や封じ込め、調査、バックアップなどのポイントを解説。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を伝えます。

| 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。

本セクションでは、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に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。

| 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

| 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

| 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。

| 概要

「マネージドセキュリティサービスの賢い使い方」

セキュリティ対策に十分なリソースを割けない昨今、運用監視や、ネットワーク隔離・封じ込めといったインシデントの初期対応、セキュリティ強化提案などの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（MSS）の需要が高まっています。

ただMSSは非常に便利ですが、全ての対策を丸投げできるかということそうではありません。

本セクションは選定基準や、任せるべき部分と自社で実施する部分をどう切り分けるかなど、MSSの賢い使い方・有用性をお伝えするセクションです。

| 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

| キーワード

- マネージドセキュリティサービス
- MDR
- MXDR

| 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をお伝えします。

| 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」

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的としてセクションです。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。

※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 2025」の再配信になります

| 視聴者層のイメージ



| サイバーレジリエンス事例紹介

※調整中

※2025年2月18日(火)開催の「サイバーレジリエンスアワード 2025」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。

同時お申込みがお得！▶ [パッケージプラン](#)はこちら

| 概要

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。

| 事例紹介イメージ

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。

タイムテーブル

		3月3日（月）	3月4日（火）	3月5日（水）	3月6日（木）	3月7日（金）	3月10日（月）	3月11日（火）		
時間	枠 時間	サイバーセキュリティ リスクとマネジメント	ゼロトラスト セキュリティ	アタックサーフェス管理	・ IT資産管理 ・ クラウドセキュリティ	・ 攻撃経路の再点検 （攻撃事例） ・ 攻撃のリカバリー	・ セキュリティ運用自動化 ・ マネージドサービス	サイバーレジリエンスアワード		
10:00-10:40	40分	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 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 販売終了 スポンサーセッション1 専用ゾーン スポンサーセッション2	時間	枠 時間	
10:50-11:20	30分	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）		13:00-13:05	5分	開会あいさつ アワード趣旨説明
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 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）		13:05-13:30	25分	授賞式
13:00-13:40	40分	基調講演1-1	基調講演2-1	基調講演3-1	基調講演4-1 IT資産管理	基調講演5-1 攻撃のリカバリー	基調講演6-1 セキュリティ運用自動化	13:30-14:10	40分	サイバーレジリエンス 事例講演
13:50-14:20	30分	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 攻撃のリカバリー	スポンサーセッション6-1 セキュリティ運用自動化	14:20-14:50	30分	スポンサーセッション7-1
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 IT資産管理	スポンサーセッション5-4 攻撃のリカバリー	スポンサーセッション6-2 セキュリティ運用自動化	15:00-15:30	30分	スポンサーセッション7-2
15:10-15:50	30分	基調講演1-2	基調講演2-2	基調講演3-2	基調講演4-2 クラウドセキュリティ	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	15:40-16:10	30分	スポンサーセッション7-3
16:00-16:30	30分	スポンサーセッション1-5	スポンサーセッション2-5	スポンサーセッション3-5	スポンサーセッション4-5 クラウドセキュリティ	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	16:20-16:50	30分	スポンサーセッション7-4
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 クラウドセキュリティ	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	16:50-16:55	5分	閉会あいさつ
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 クラウドセキュリティ	スポンサーセッション5-7 攻撃のリカバリー	スポンサーセッション6-5 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枠】各日のスポンサーセッション1枠目、3枠目、5枠目

ご協賛メニュー

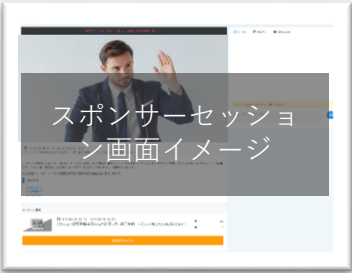
	専用ゾーンプラン	プラチナ	ゴールド	全リスト	セクションリスト
	ダイヤモンド				
スポンサーセッション Live配信＋アーカイブ	●	●	●	-	-
専用ゾーン	●	-	-	-	-
全申込者リスト	-	想定1000名	-	想定1000名	-
協賛セクション申込者リスト	想定300名	想定350名	想定350名（上限450名）	-	想定350名（上限450名）
セッションアンケート	販売終了	●	●	-	-
視聴者データ・レポートサイト	●	●	●	-	-
事前アンケート結果	●	●	●	●	●
スポンサーロゴ掲載	●	●	●	●	●
資料配布	●	●	●	-	-
開催報告書	●	●	●	●	●
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-

※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。



| 専用ゾーン

- 1社限定特別プラン
- スポンサーセッションを専用ゾーンで開催。
- 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。
- 貴社テーマに関心の高い視聴者へ訴求可能。

販売終了

| 全申込者・協賛セッション申込者リスト

- 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。

| セッションアンケート

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

| 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。
- 講演間に表示される幕間スライドに貴社のロゴを掲載。

| 資料配布

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

| 開催報告書

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

※画像はイメージです。

スポンサーセッション協賛社限定！
主催：アイティメディア編集部 特別協賛：スポンサー企業様

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

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

※登壇者は最大4名までとなります

ご提供内容

- セッション内容企画
- 有識者のアサイン（1名）
- ITmedia主催デジタルイベント内での配信（60分）
- セッション視聴者リード情報のご提供

タイムテーブルイメージ

例：セッションスポンサー協賛＋パネルディスカッションの場合

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）

※イベントによってタイムテーブルは異なります

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。

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。

販売終了

ご協賛価格

本企画のご協賛価格：¥1,500,000-

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。
（オプション単体でのお申込みはできません）
- 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。

お申込締切：通常締切（開幕2か月前）と同日

スポンサーセッション協賛社限定！

主催：アイティメディア編集部 特別協賛：スポンサー企業様

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

パネルディスカッション動画 | 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
- 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
- 動画内の登壇者の見え方：長テーブルに並んで着席を想定
- 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

販売終了

オプションメニュー

| 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/291242/2024-04-30/2czfbvx>

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）

オプションメニュー

| セッション動画活用リード獲得

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

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

料金 **¥300,000～**

| レポート記事配信（ターゲットヘブッシュ型で配信）

- 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。

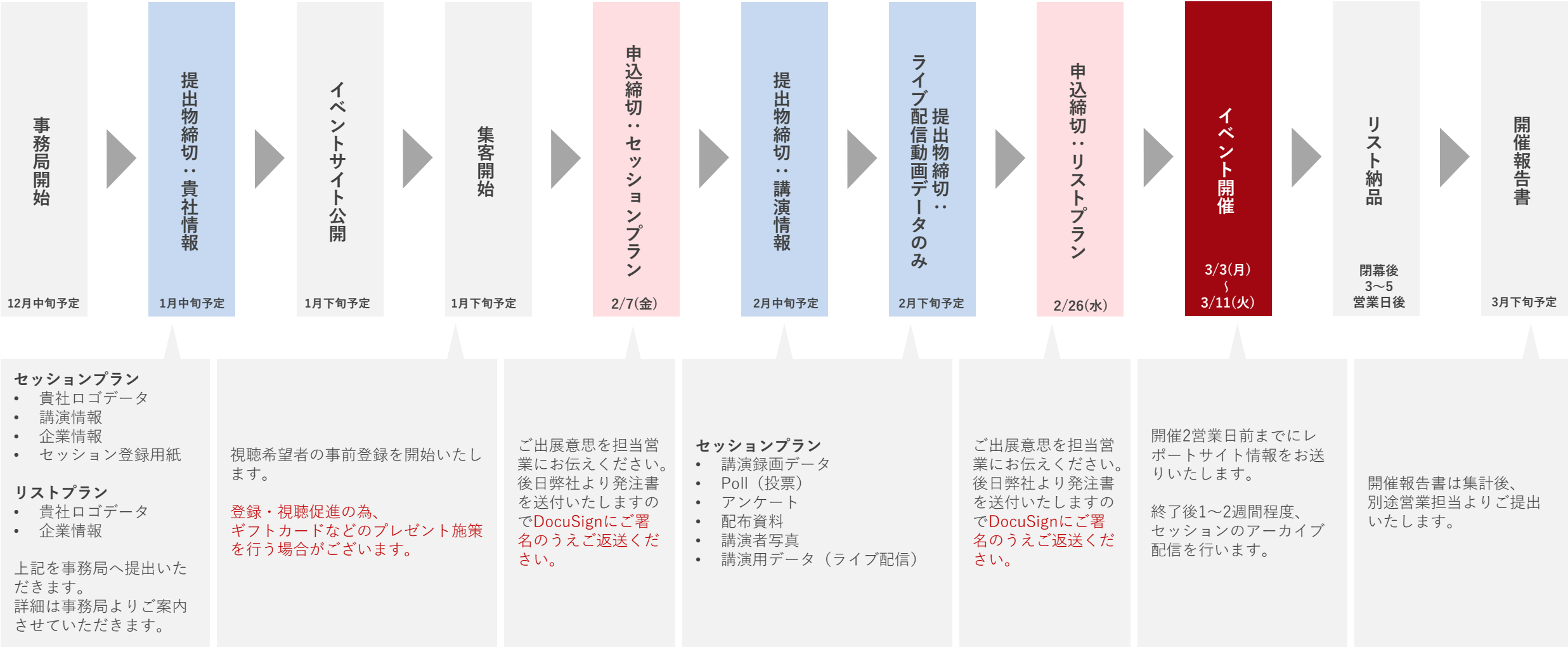
詳細：<https://go.itmedia.co.jp/l/291242/2024-08-05/2d122lq>

料金 **¥300,000**

※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。





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」
開催日時	2024年11月25日(月)～12月2日(月) ※12月16日(月)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
主催	@IT、ITmedia エンタープライズ、ITmedia エグゼクティブ
全申込者数	1,244人
視聴者数	863人
申込みページ	https://members08.live.itmedia.co.jp/library/NzcwODl%253D?group=SEC2024A
開催報告書	http://go.itmedia.co.jp/l/291242/2024-12-23/2d1r3dt



- arcserve Japan合同会社
- 株式会社エーアイセキュリティラボ
- Exabeam Japan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
- 株式会社カスペルスキー
- Cato Networks株式会社
- 株式会社CyCraft Japan
- 株式会社サイバーセキュリティクラウド
- サイバーリーズン合同会社
- 株式会社JALインフォテック
- S k y 株式会社
- ゴーホージャパン株式会社
- Tanium合同会社
- デジタルアーツ株式会社
- 東芝ITサービス株式会社
- 日本ブルーフポイント株式会社
- BlackBerry Japan株式会社
- 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
- 株式会社マクニカ
- 株式会社ラック

モーニング セッションおよび 基調講演	【モーニングセッション1】 2030年問題への処方箋 ――持続可能な次世代サプライチェーン統制の 要諦 NRIセキュアテクノロジーズ株式会社 DXセキュリティプラットフォーム事業本部 本部 長 足立 道拡 氏 ※本講演は過去の再放送です。 講演内容は配信当時（2024年8月26日）の情報となります。	【モーニングセッション2】 MIXIにおけるゼロトラストの取り組み ～これまでとこれから～ 株式会社MIXI 執行役員 CISO セキュリティ室長 亀山 直生 氏 ※本講演は過去の再放送です。 講演内容は配信当時（2023年3月1日）の情報となります。	【基調講演3-1】 繋ぐ楔と断ち切る楔 株式会社インターネットイニシアティブ 根岸 征史 氏 SBテクノロジー株式会社 辻 伸弘 氏 piyokango 氏
	【基調講演1-1】 セキュリティ専門家が語る今更ながらの情報セ キュリティ対策の基本 楽天グループ株式会社 セキュリティエンジニア 原子 拓 氏	【基調講演2-1】 ゼロトラストで万事解決？ 「信頼性ゼロ」にならないために 京姫鉄道合同会社 代表社員CEO アニメ「こうしす！」脚本・監督 井二 かける 氏	【基調講演3-2】 セキュリティ芸人の解説付きお笑いネタ & エンジニアを楽しむ極意 セキュリティ芸人 アスースン・オンライン 氏
	【基調講演1-2】 現実に即したサイバーレジリエンス ～チェックリスト依存からの脱却と実践的アプ ローチ～ 株式会社Armoris 取締役専務 CTO／一般社団法人金融ISAC アドバ イザー兼CTO 鎌田 敬介 氏	【モーニングセッション3】 コンピュータ技術とサイバーセキュリティにお ける日本の課題、人材育成法および将来展望 独立行政法人 情報処理推進機構（IPA） サイバー技術研究室 登 大遊 氏 ※本講演は過去の再放送です。 講演内容は配信当時（2023年11月29日）の情報となります。	【モーニングセッション4】 エンドポイントを守るために気にすべきこと 株式会社川口設計 代表取締役 川口 洋 氏 ※本講演は過去の再放送です。 講演内容は配信当時（2024年8月29日）の情報となります。

モーニング セッションおよび 基調講演	【基調講演4-1】 セキュリティ対策におけるIT資産管理の重要性 フリー株式会社 常務執行役員CISO 茂岩 祐樹 氏	【モーニングセッション5】 守井のセキュリティ対策向上委員会 ～脆弱性と設定不備と時々ゼロデイ～ 株式会社レオンテクノロジー 代表取締役社長 守井 浩司 氏 ※本講演は過去の再放送です。 講演内容は配信当時（2024年5月30日）の情報となります。	【基調講演6-1】 組織で考えるべきセキュリティ人材の育て方 ーAIに振り回されない運用支援に必要なことー 大阪大学 D3センター 教授, CISO 猪俣 敦夫 氏
	【基調講演4-2】 Security Talk Café ～セキュリティというレッドオーシャン 専門性が高い“だけ”の人はなぜ組織で生き残れないのか？～ 株式会社ドラゴン・ラボラトリーズ 代表取締役 人事実践家科学研究会 常任理事、 千葉商科大学客員講師 等 堀口 卓志 氏	【基調講演5-1】 攻撃者はどこから侵入してくるのか？ システムや人の守るべき弱点とは 株式会社トライコーダ 代表取締役 上野 宣 氏	【基調講演6-2】 あなたの会社のセキュリティシステムは誰のもの？～人材育成とMSSの相関関係を語ります GMOあおぞらネット銀行株式会社 執行役員 テクノロジー＆プロセッシンググループ長 金子 邦彦 氏
	株式会社Armoris 取締役専務 CTO 一般社団法人金融ISAC 専務理事兼CTO 鎌田 敬介 氏 アイティメディア株式会社 編集局 統括編集長 内野 宏信 アイティメディア株式会社 ITmedia エンタープライズ編集部 田淵 聖人	【基調講演5-2】 ランサムウェアの脅威を逆手に取れ！ 実例から学ぶ迅速な復旧と防止策 システムガーディアン株式会社 代表取締役 加藤 登志典 氏	

@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

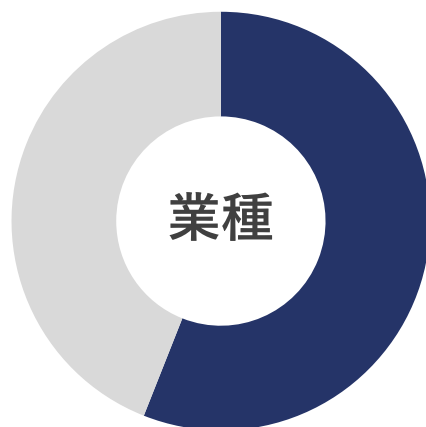
<https://atmarkit.itmedia.co.jp/>

■ PV

約770万 PV/月 約390万 UB/月 ※2024年1月実績

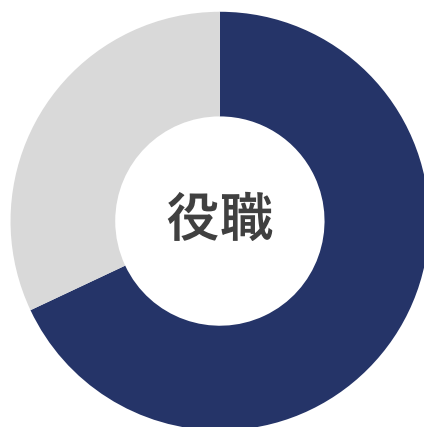
■ メルマガ配信数

約54万通



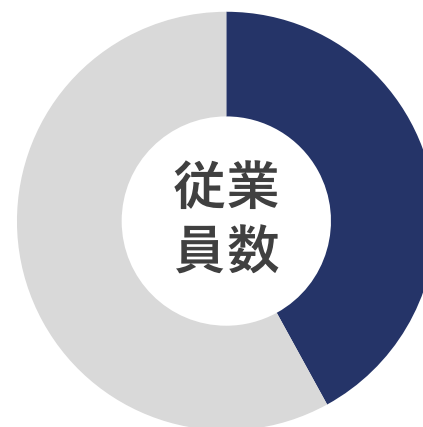
ユーザー企業 約**56%**

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%



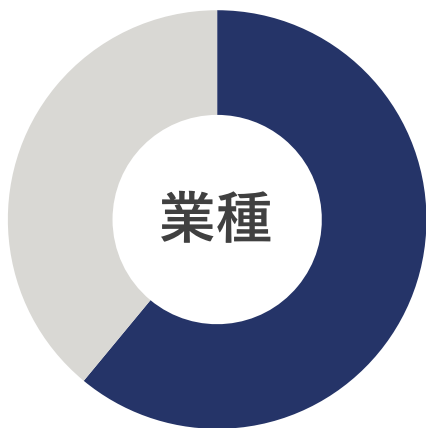
1000人以上 約**41%**

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

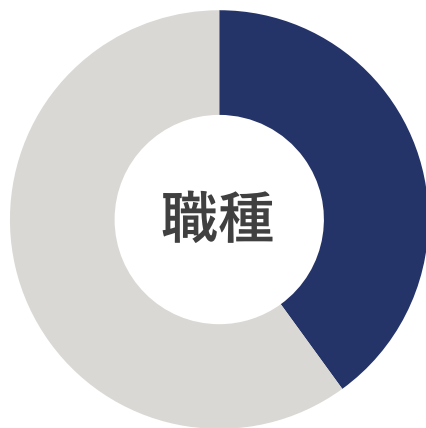
ビジネスを革新するIT部門向け実践情報サイト

■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



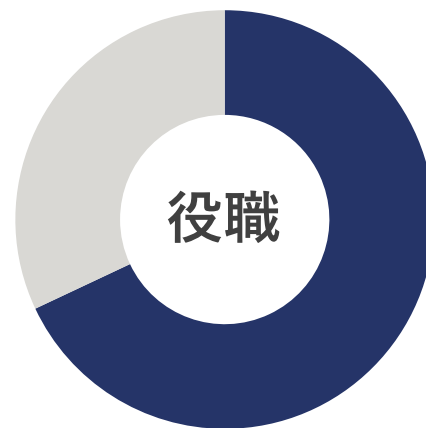
ユーザー企業 約**61%**

主な内訳：製造業37.9%, 商社・流通・サービス業27%



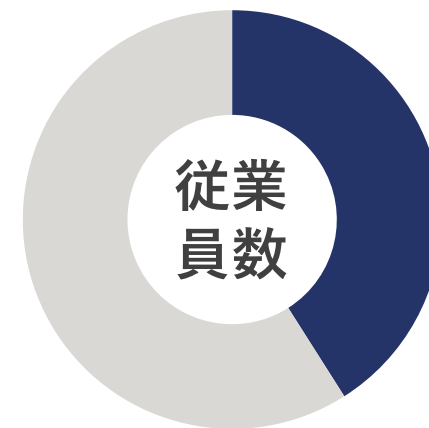
情シス及び
経営・経営企画 約**40%**

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%**

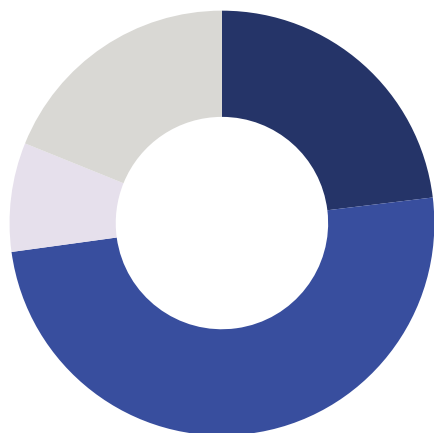
主な内訳：1000人～5000人未満20.3%,
5000人以上20.6%

ITmedia エンタープライズ

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

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

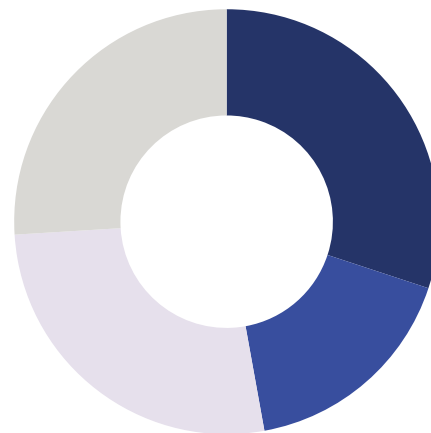
2024年度のIT関連予算の増減



■ 増加 ■ 同程度 ■ 減少 ■ 不明

IT関連予算増加の企業 約**23%**

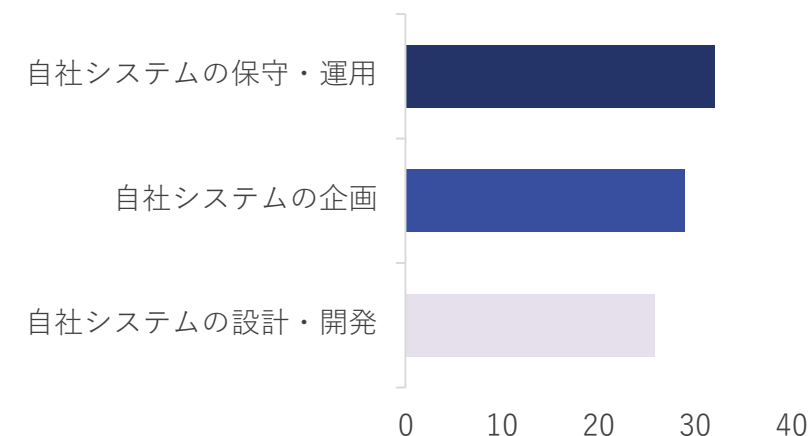
DXに向けた戦略の策定と実行



■ 実行中
■ 戦略策定済みで準備中
■ 予定はあるが未着手

DXに向けた戦略を策定・実行中 約**74%**

読者の業務内容

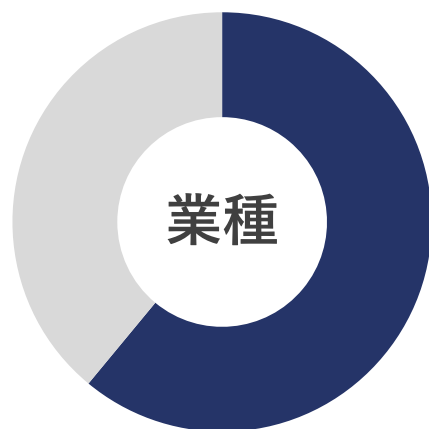


自社システムの企画、設計・開発、
保守・運用に携わる 約**30%**

ITmedia エグゼクティブ

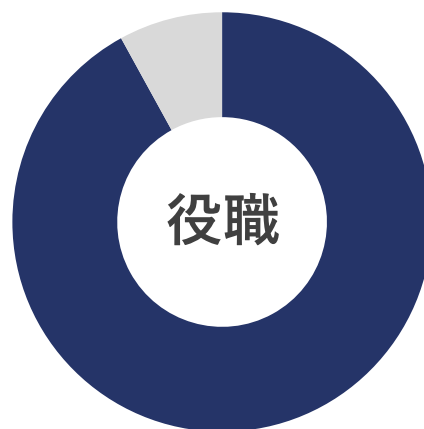
企業の明日を変えるエグゼクティブとCIOのためのコミュニティ

- 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



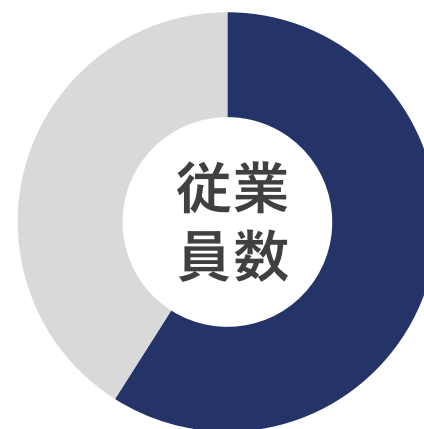
ユーザー企業 約**61**%

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%

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・音声ともに配信が中断（停止）し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中断（停止）し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・音声ともに配信が中断（停止）する可能性があります。
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。

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>