Produced by 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 春

生成AIで攻撃が進化・拡大――
「自社を守る仕組み」の確認点とアップデートのポイント

開催日時：2024年5月27日(月)～6月3日(月)
申込締切：セッションプラン最終締切　2024年4月26日（金）
リストプラン最終締切　2024年5月22日（水）

SUMMARY

名称	ITmedia Security Week 2024 春
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5月27日(月)～6月3日(月)
申込締切	セッションプラン最終締切：2024年4月26日（金） リストプラン最終締切：2024年5月22日（水）
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。

PRODUCER'S COMMENT

生成AIで攻撃が進化・拡大――
「自社を守る仕組み」の確認点とアップデートのポイント

およそ全てのビジネスがデジタル前提となり、システム／データとそれらへのアクセスが
社内外で入り乱れるようになった中、企業には自社を守る「今に即した仕組み」が求められています。

特に昨今はランサムウェア、サプライチェーン攻撃などに加え、生成AIも新たな攻撃手段・対象となり、
ChatGPTのアカウントがダークウェブで売買される、
生成AIでマルウェアを生成するといった問題が既に起きています。
攻撃自体が進化、拡大する中、対策を常に確認、アップデートし続けることが一層強く求められているのです。

ITmedia Security Week 2024 春では「侵入前提で守る仕組み」の確認点を総ざらい。
「今、不可欠な視点」を提供します。

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す。
2-2	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。
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	ランサムウェア対策のためのレジリエンス	ランサムウェア被害からの復旧に向けたサイバーレジリエンス能力の強化を実現するために、サイバー演習事例や組織構築事例などを通して役立つ知識やノウハウをお届けします。
6	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。

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（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

- 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

「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。
本セクションでは、「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　＃マネージドサービス全般

＃ファイアウォール　＃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　＃シフトレフト系

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. 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――“既に社内に潜む攻撃者”も想定せよ」

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。現在はもはや、この区分だけで組織を守るのは難しい状況です。攻撃を止めるには「既に攻撃者は“社内”にまで到達している」と想定することも必要です。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、止める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（マネジメント）　＃EDR／XDR　＃VPNセキュリティ関連　＃脆弱性管理（マネジメント）

＃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
- 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

SECTION 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。
本セクションでは、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）
＃マネージドサービス全般
＃暗号関連全般（鍵管理を含め）
＃IDaaS（Identity as Service）
＃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）
＃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。

SECTION 4. エンドポイント対策&情報管理

概要

エンドポイントのないシステムは存在しません。そして、エンドポイントの防御なくしてシステムや組織、企業を守ることはできないはずです。さまざまな視点でのセキュリティが存在しますが、それらはエンドポイント防御の延長線上で考えていくことが、理解の第一歩になるでしょう。脅威は今も、エンドポイントから内部に入り込み、情報資産を奪っていきます。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提供します。

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

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連日のように世間を騒がしています。大企業から中堅・中小企業まで企業規模を問わずこの攻撃のターゲットとなる今、「脅威の侵入は防げない」という前提で、ビジネスやシステムの回復力を高める“サイバーレジリエンス”能力が高い組織やシステム、仕組みづくりが急務となっています。
本セクションは、万が一にランサムウェアの侵入を許した場合に備え、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”までを含めた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サイバー演習事例などを通してお伝えします。

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
- 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. 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。
本セクションでは、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

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

SECTION 2-1
ゼロトラストセキュリティ

Section1,3,4,5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	Section2のタイムテーブル	SECTION 2-2 アタックサーフェス管理	SECTION 3 クラウドセキュリティ	SECTION 4 エンドポイント対策&情報管理	SECTION 5 ランサムウェア対策のためのレジリエンス	SECTION 6 多要素認証から始めるID管理・統制	Section6のタイムテーブル
10:00～10:40	モーニングセッション1	10:00～10:40	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	販売終了	10:00～10:40
10:50～11:20	スポンサーセッション1-1	10:50～11:20	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	販売終了	10:50～11:20
11:30～12:00	スポンサーセッション1-2	11:30～12:00	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	販売終了	11:30～12:00
13:00～13:40	基調講演1-1	13:00～13:40	基調講演2-1 （アタックサーフェステーマ）	基調講演3-1	基調講演4-1	基調講演5-1	基調講演6-1 （多要素認証テーマ）	13:00～13:40
13:50～14:20	スポンサーセッション1-3	13:50～14:20	スポンサーセッション2-3 （アタックサーフェステーマ）	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6-1 （多要素認証テーマ）	13:50～14:20
14:30～15:00	スポンサーセッション1-4	14:30～15:00	スポンサーセッション2-4 （アタックサーフェステーマ）	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6-2 （多要素認証テーマ）	14:30～15:00
15:10～15:50	基調講演1-2	15:10～15:40	基調講演2-2 （アタックサーフェステーマ）	基調講演3-2	基調講演4-2	基調講演5-2	販売終了	15:10～16:10
16:00～16:30	スポンサーセッション1-5	15:50～16:20	スポンサーセッション2-5 （アタックサーフェステーマ）	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	販売終了	16:20～17:20
16:40～17:10	スポンサーセッション1-6	16:30～17:00	スポンサーセッション2-6 （アタックサーフェステーマ）	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		
		17:10～18:10	スポンサーセッション2-6 （アタックサーフェステーマ）					

※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」の枠となります。
【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

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	-	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350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	●	●	●	●	-	-	●
Security Week 申込者向けメール配信	2通配信	●	-	-	-	-	●
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-

お申込み受付を終了しました

お申込み受付を終了しました

お申込み受付を終了しました

※集客人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」の枠となります。
※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およびセクション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、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。

SCHEDULE

申込締切
セッションプラン最終締切：2024年4月26日（金）
リストプラン最終締切：2024年5月22日（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4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5月27日(月)～6月3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。

ご協賛メニュー　詳細

スポンサーセッション Live配信＋アーカイブ

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頂けます！

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・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頂けます。

※単一回答、複数回答、自由回答の3種類を組み合わせて自由に設定頂けます。
※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。

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、集計データでのご提供です。

ご協賛メニュー　I　　詳細2（特定プラン向け）

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

ブラックスポンサー限定 申込者向けメール配信

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

ご協賛メニュー　I　　オプション1

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致します。
※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

■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　**30万円**

リード カスタム納品サービス

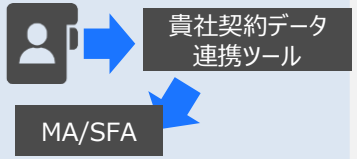
イベントで入手したリードをMAツールへ直接納品や、
貴社フォーマットにあわせて加工して納品します！

■納品イメージ

パターン1

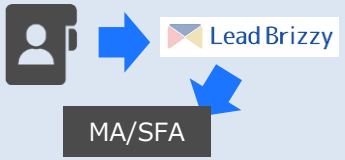
貴社フォーマットに合わせてリード情報を加工して納品

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※

■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

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**

※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）

ご協賛メニュー　I　　オプション2

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カ月前までのお申し込みとなります。

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/291242/2022-09-09/2bjcm9g

料金 ~~170万円~~➡ **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 ~~245万円~~➡ **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～
期間　3~4週間（250件の場合）
※1000件以上は不可

料金 **70万5千円~**

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）

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。

お申込み受付を終了しました

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、懇親会を通して、**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

ブラックスポンサー
限定

SPONSORED MENU ラウンドテーブル

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
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）
規模	8～9名想定 参加者：最大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）

お申込み受付を終了しました

※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。

ブラックスポンサー
限定

SPONSORED MENU ラウンドテーブル

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	参加者[illegible]
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[illegible]	ご来場者様[illegible]ケーションの場[illegible]ご活用ください
順次解散	

お申込み受付を終了しました

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	

PAST EVENTS

タイトル	ITmedia Security Week 2023 冬 本当に「自社にマッチする仕組み」になっていますか？ 主体的判断に欠かせない情報源と、各種手段の生かし方
日時	2023年11月27日（月）～ 12月4日（月） ※12月18日までアーカイブ配信
全申込者数	1,287
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、株式会社アシスト、株式会社アシュアード、Ivanti Software株式会社株式会社インターナショナルシステムリサーチ、株式会社imperva japan、ウィズセキュア株式会社、Veeam Software Japan株式会社株式会社エーアイセキュリティラボ、Exabeam Japan株式会社、SCSK Minoriソリューションズ株式会社、SBテクノロジー株式会社NRIセキュアテクノロジーズ株式会社、NTTデータ ルウィーブ株式会社、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、クラウドストライク合同会社、Cloudbase株式会社、サイバーリーズン合同会社、株式会社JSOLJamf Japan合同会社、Ｓｋｙ株式会社、株式会社セールスフォース・ジャパン、SentinelOne Japan株式会社、TC3株式会社テクマトリックス株式会社、デジサート・ジャパン合同会社、東芝ITサービス株式会社、トレンドマイクロ株式会社Netskope Japan株式会社、パスロジ株式会社、バリオセキュア株式会社、株式会社日立製作所、フォーティネットジャパン合同会社freee株式会社、株式会社マクニカ、メンロ・セキュリティ・ジャパン株式会社、Ridgelinez株式会社
申込みページURL	https://v2.nex-pro.com/campaign/60341/apply

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。

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