





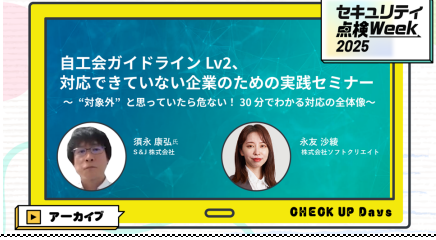



#01	#02	#03	#04
			
【KEYNOTE】 進化するサイバー脅威と日本企業が取るべきアクティブ防御戦略 ー 2025年上半期の最新動向と国内特有のリスク ー	【KEYNOTE】 生成AI時代の不安を解消！Microsoft 365 Copilot には、Microsoft 365 Business Premium + E5 Security がおすすめ！	【AD対策シリーズⅠ】 セキュアな Active Directory を運用するための第一歩 ～事業継続に本気で向き合う30分～	【AD対策シリーズⅡ】 NEW セキュアな Active Directory を運用するための第二歩 ～高度なセキュリティ設定と SOC のベストプラクティス～
KELA株式会社 Head of Pre-Sales 川崎 真 氏	日本マイクロソフト株式会社 コーポレートソリューション事業本部 SMB統括本部 セキュリティ本部 パートナーソリューションセールスマネージャー 浦崎 奈緒 氏	株式会社ソフトクリエイト サービス事業統括部 セキュリティサービス部 担当部長 尾崎 嘉一	株式会社ソフトクリエイト サービス事業統括部 セキュリティサービス部 主任SE 本山 裕大
本セッションでは、イスラエル発祥のダークウェブ脅威インテリジェンスの老舗ベンダー、KELAが収集・分析した最新の脅威インテリジェンスをもとに、こうした国内特有のリスク構造を踏まえた攻撃者の動きと、その対策としてのアクティブサイバーディフェンス（能動的防御）の実践方法を紹介します。	生成AIの業務活用には、利用者や情報システム管理者にとって「情報漏洩」「生成AIによるデータ学習」「設定ミスや悪用」など、さまざまな不安がつきものです。本セッションでは、Microsoft 365 Copilot と Microsoft 365 の先進的なセキュリティ機能を活用し、現状の運用を見直しながら、安心して生成AIを活用するための具体的なポイントを分かりやすく解説します。	Active Directory は企業のITインフラを支える重要な存在です。IT企業、金融業界、医療機関など、様々な業界で Active Directory はユーザー管理の効率化やセキュリティ強化に寄与しています。しかし運用の過程ではいくつかの課題が生じることもあります。例えば現在運用している Active Directory のセキュリティ対策は万全か不安に感じていませんか？また、アクセス制御のルールが適正かどうか、あるいは前任者の設定した内容が不透明という課題を抱えていませんか？本セミナーでは、実際に某病院で発生した Active Directory に関するランサムウェア感染のインシデントを取り上げ、その原因を詳しく解説します。	本講演では、AD 対策シリーズ第二弾として一般的な攻撃手法を交えながら、Active Directory のセキュリティの重要性と現状の課題について分かりやすく解説いたします。また、セキュリティ設定の診断や継続的な監視体制の構築といったソリューションを通じて、これらの課題をどのように解決できるかをご紹介いたします。

#05	#06	#07	#08
			
【AD対策シリーズⅢ】 NEW ADセキュリティ最終ステップ！ 診断＆監視で実現する鉄壁のADセキュリティの作り方	【ASM/攻撃者目線対策】 複雑化するIT環境！ ～御社の情報資産を守るASM運用の第一歩～	【Web脆弱性診断】 もしもの前に！ インシデント事例から学ぶ脆弱性診断の効果	【Microsoft 365】 そのポリシー、本当に効いてる？ 今すぐ確認したい条件付きアクセスポリシーの落とし穴
株式会社ソフトクリエイト サービス事業統括部 セキュリティサービス部 担当部長 尾崎 嘉一	株式会社ソフトクリエイト サービス事業統括部 セキュリティサービス部 担当部長 尾崎 嘉一	株式会社ソフトクリエイト サービス事業統括部 セキュリティサービス部 技師補 永友 沙綾	ネクストリード株式会社 (Next Read, Inc.) クラウドサービス本部 業務執行役 成田 翔 氏
サイバー攻撃がますます巧妙になる中、Active Directory (AD) や社内システムのセキュリティ対策はできていますか？「今の対策で本当に大丈夫？」「どこに注意したらいいの？」と感じている方にぴったりの講演です。本シリーズの締めくくりとして、AD を中心とした最新のセキュリティ事情や、よくあるトラブル事例、今日から始められる対策のポイントをわかりやすく解説します。	企業のIT環境が複雑化し、情報漏洩やダークウェブでの被害が増加する中、ASM（攻撃対象領域管理）による外部公開資産の可視化と、限られた情シスリソースで実現できる最新セキュリティ運用のポイントをわかりやすく解説します。	近年多発するサイバー攻撃や情報漏えいの多くは、脆弱性診断の実実施や見落としが原因です。本ウェビナーでは、実際のインシデント事例をもとに、もしもの前に、「なぜ脆弱性診断が必要なのか」「PF診断やWebアプリ診断で何ができるのか」をSler視点で分かりやすく説明します。診断計画の立て方や、負担を抑えて効果的に実施するポイントも併せてご紹介いたします。	本セミナーでは、こうした「条件付きアクセスポリシーの盲点」に焦点を当て、設計・設定時の見落としやすいポイント、そして運用面での継続的な見直しの重要性について説明します。また、技術的・運用的な制約から完全な設計が難しい場合でも有効な、ログ分析やアラート監視を組み合わせた補完的アプローチについてもご紹介いたします。条件付きアクセス ポリシーは強力なセキュリティ機能である一方、その有効性を保つためには高度な設計力と定期的な点検が欠かせません。セミナーを通じて、貴社のポリシーが実際のリスクに対して適切に機能しているかを再確認し、運用改善のヒントになれば幸いです。

#09	#10	#11	#12
			
【プラットフォーム診断】 NEW プラットフォーム診断で強固な基盤をつくる ～サービス基盤の安全を支えるための運用とは～	【外部公開資産】 攻撃者の視点とダークウェブ情報で守る ～ SCSmart (SLING) による外部リスク総点検～	【自工会/部工会ガイドライン】 自工会ガイドラインLv2、対応できていない企業のための実践セミナー	【SASE】 リモートアクセスを見直そう！ SSL-VPNの動向と新時代のSASEを学ぶ
株式会社ソフトクリエイト サービス事業統括部 セキュリティサービス部 主任SE 本山 裕大	KELA株式会社 Account Executive 川副 沙也加 氏	S & J 株式会社 セキュリティプロフェッショナルサービス部 須永 康弘 氏	株式会社ソフトクリエイト アカウント営業統括部 シニアエキスパート 朝倉 裕太
システムの基盤となるOSやミドルウェアの管理はできていますか。攻撃者はシステムの脆弱性について内部への侵入を試みることがありますが、システムの基盤の脆弱性も例外ではありません。定期的なパッチ適用ができていないか、また、既知の脆弱性が所管しているサーバー・機器に潜んでいないかというのは事前に確認しておくことが重要になります。本講演では、実際の攻撃事例を交えながら、基盤部分のセキュリティ意識の重要性について分かりやすく解説します。	攻撃者は企業の外部に露出した資産だけでなく、ダークウェブ上の漏洩情報や資格情報も利用して侵入を試みます。本セッションでは、SCSmart (SLING) を活用し、外部資産の可視化とダークウェブ監視を組み合わせた総点検手法、継続的監視、そして伴走型支援による運用改善方法をご紹介します。	自工会セキュリティガイドラインの適用対象や背景を解説し、未対応のリスクや今すぐ始めるべき対策を紹介します。124項目の要求事項の全体像と初動ポイントを30分で効率的に学べる内容です。本講演は、以下の二部構成となります ■第一部(約15分) あなたの会社も対象です！自工会/部公開セキュリティガイドライン ■第二部(約13分) 自工会セキュリティガイドラインを早期かつ効果的に押さえる具体的な方法とは？	最近、「SSL-VPNはもう危ないかも…」という声が多く聞かれるようになりました。特に、既存製品をご利用中の企業では、2026年に一部機種をサポート終了が予定されており、今後の対応に悩む声が増えています。本セミナーでは、数多くの企業課題を解決してきた営業スペシャリストと、構築を担当するエンジニアが、それぞれの視点から皆様の疑問にお答えします。リモートアクセスの基本 なぜ今「SASE」への移行が注目されているのか 実際のプロジェクト事例を交えた解説、今すぐ移行できない場合の現実的な対策 SSL-VPNの今後に不安を感じている方、SASEへの移行を検討中の方にとって、実践的なヒントが得られる内容です。

セキュリティ点検Week 2025 おかわり配信 - PROGRAM

(#13-#24)

<div>#13</div> <div></div> <div>【経営層へのセキュリティ報告】 原理原則から考える経営陣へのセキュリティ対策状況の報告ポイント</div> <div>S & J 株式会社 取締役 SOCエバンジェリスト 石川 剛 氏</div> <div>ランサムウェアに対して基準やガイドライン対応では、最初から対策の抜け漏れが発生してしまいます。また、「横並びのセキュリティ対策をしている」とこと、「対策が充分である」ということは、全く違っています。本Sessionではランサムウェアの被害事例を用いて、急所を抑えた対策ポイントを解説します。</div>	<div>#14</div> <div></div> <div>【標的型メール訓練】 社員の意識を変える！ 効果的な標的型メール訓練とセキュリティ教育とは</div> <div>株式会社ソースボッド 営業部 サービス営業チーム 綱川 慧 氏</div> <div>本セッションでは、訓練や教育の重要性を改めて整理するとともに限られた予算・リソースでも標的型メール訓練と情報セキュリティ教育の効果最大化する方法をご紹介します。 ※ 情報セキュリティ教育サービスの SPC Leak Detection は SPC Literacy+ へ名称変更しております。</div>	<div>#15</div> <div></div> <div>【ID管理】 クラウド時代の認証： IDaaSで実現する安全・効率的なパスワード管理</div> <div>システムワークスジャパン エンジニアリング事業部 事業部長 湯浅 圭介 氏</div> <div>近年、クラウドサービスの利用増加に伴い、企業や個人が管理すべきID・パスワードの数は急増しています。その結果、利用者のパスワード管理コストが増大し、使い回しや弱いパスワードの設定によるパスワード漏洩リスクが深刻化しています。こうした課題に対し、IDaaS (Identity as a Service) によるSSO (シングルサインオン) の導入が有効です。本講演では、これらの技術を活用した安全かつ効率的な認証基盤の構築方法について解説します。</div>	<div>#16</div> <div></div> <div>【CSIRT】 CSIRTの必要性和現場での役割</div> <div>S & J 株式会社 営業部パートナーグループ 志摩 大輔 氏</div> <div>サイバー攻撃への対応は、ITスキルだけの問題ではなく、組織力の問題です。IT部門主導でCSIRTを立ち上げ、全社を巻き込んだ連携体制を構築することが、現実的で持続可能な対策に繋がる気付きをお伝えします。</div>
<div>#17</div> <div></div> <div>【Microsoft 365】 Copilot って便利だけど…その前に知っておきたい“データの話”</div> <div>AvePoint Japan株式会社 営業部 チャネル営業グループ リードエグゼクティブ 小澤 正弘 氏</div> <div>株式会社ソフトクリエイト クラウドソリューション統括部 クラウドビジネス部 主任 東田 航大</div> <div>Copilot、使ってみると本当に便利ですね。翻訳や議事録作成、ちょっとした調べものまで、業務のいろんな場面で活躍してくれます。でも、ちょっと待ってください。その Copilot、どんなデータを使って答えているか、考えたことがありますか？</div> <div>このセミナーでは、「データの鮮度って何？」「古い情報を使うとどうなるの？」といった、普段あまり意識しないことについてご紹介します。</div>	<div>#18</div> <div></div> <div>【ID管理】 クラウド時代だからこそ Entra ID でまとめて楽ちん管理 ～ゼロトラストで最新脅威に備える統合ID管理術～</div> <div>株式会社ソフトクリエイト クラウドソリューション統括部 クラウド技術部 課長代理 柳澤 佑紀</div> <div>本ウェビナーでは、Microsoft Top Partner Engineer Award 2025 受賞エンジニアが登壇し、最新の脅威動向を始め、なぜ Entra ID が良いのか、シングルサインオンや多要素認証 (MFA)、条件付きアクセスなどの具体策をわかりやすく紹介し、セキュリティ強化と管理効率化を両立するヒントをお届けします。最新のセキュリティ対策に関心のある方、Entra ID 導入を検討中の方はぜひ御覧ください。</div>	<div>#19</div> <div></div> <div>【Microsoft 365】 Copilot から始める セキュアなAI業務改革 ～認定トレーナーが語る、情シス担当者の不安を解消するセキュリティと運用手法の学び方～</div> <div>株式会社ソフトクリエイト クラウドソリューション統括部 クラウドサクセス部 課長代理 武井 絵理</div> <div>セキュリティへの不安を Copilot で払拭し、AI導入のポイントから利活用までを実践的に学べる、現地開催オンラインのワークショップを本セミナー限定で特別にチラ見せします。Microsoft 365 Copilot、および Copilot Chat の基本機能と業務活用例を紹介しながら、導入時に気になる情報漏洩対策やアクセス制御に関する不安に対して、Microsoft 365 が提供するセキュリティ機能 (Entra ID など) を交えながら、Microsoft 認定トレーナーが解説します。</div> <div>AI導入を検討中の方はもちろん、まずは情報収集から始めたい方にもおすすめの30分セッションです。ぜひこの機会に、AI活用とセキュリティの両立について理解を深めてください。</div>	<div>#20</div> <div></div> <div>【AI】 AIの種類、AIのPoCサービス、AIの安全性についての学び</div> <div>株式会社ソフトクリエイト 事業推進本部 製品開発部 課長代理 大和 祐介</div> <div>AIの利活用が進むにつれ、AIのセキュリティについても考える必要があります。AIのセキュリティはかなり大雑把な言葉で、実際にはAIの種類に応じた対策や対応が必要となります。本セッションでは、AIの種類について振り返りを行い、各種AIの得意な点、不得意な点を明確にした上で、それぞれのセキュリティについて掘り下げてみたいと考えております。</div>
<div>#21</div> <div></div> <div>【AI】 安全な生成AIプラットフォーム</div> <div>株式会社ソフトクリエイト 事業推進本部 製品開発部 主任SE 小野 力</div> <div>生成AIの業務活用には、安全な環境整備が第一歩となります。本セッションでは安全な生成AIって何？ という所からスタートし、安全な生成AIの利用に必要なプラットフォームについて掘り下げていきます。最後に当社で提供している「Safe AI Gateway」の簡単な商品紹介もさせていただきます。 ※ 本講演の内容は上期時点の情報に基づいております。</div>	<div>#22</div> <div></div> <div>【情報漏洩】 情報漏洩リスクは組織の中にも外にも存在している デジタル時代の重要データの守り方</div> <div>Sky 株式会社 ICTソリューション事業部 システムサポート部 山下 柚香 氏</div> <div>情報のデジタル化が当たり前になり、企業や組織は重要な情報をデジタル形式で保管することが一般化しています。サイバー攻撃者からして見れば、それらは価値のある格好の標的であり、情報を窃取するための手口も巧妙化しています。 また、組織の内部にも、情報を不正に持ち出す内部不正のリスクや、人為的なミスによって漏洩するリスクが存在。 組織内外にどのようなリスクがあり、データを守るためにどのような対策が必要なのか、本セミナーでご紹介します。</div>	<div>#23</div> <div></div> <div>【ID管理】 ゼロトラスト実践の第一歩： ID管理の重要性和国産ソリューションの選択</div> <div>エクスジェン・ネットワークス株式会社 マーケティング部 部長 前田 祐一郎 氏</div> <div>ゼロトラストが注目される中、その実践において最も重要な「起点」となるのがID管理です。本ウェビナーでは、ID・認証管理の専門企業であるエクスジェン・ネットワークスが、ゼロトラストの考え方とID管理の関係をわかりやすく解説。 オンプレミス型ID管理ソフトウェア「LDAP Manager」と、クラウド型IDaaS「Extic」の特長と活用シーンを紹介し、業界のセキュリティガイドラインとの関連も踏まえながら、現実的かつ効果的なゼロトラストの第一歩をご提案します。</div>	<div>#24</div> <div></div> <div>【不正アクセス対策】 セキュリティガイドライン遵守のための不正遮断ソリューション</div> <div>エクスジェン・ネットワークス株式会社 Device Security 営業部 部長 植松 卓 氏</div> <div>製造、医療、文教関連を筆頭に、業界ごとのセキュリティガイドラインが出され、対策の強化が求められています。本セミナーでは、業界ごとのガイドラインを進めるための共通ポイントを解説し、対策の底上げにつながり、簡単に導入できるシステム「L2Blocker」をご紹介します。</div>