CTC セキュリティサミット 2022

ハイブリッドクラウド時代の“モダンセキュリティ”

主催　伊藤忠テクノソリューションズ株式会社

7/7（木）

14:00 - 17:00

概要

2021年セキュリティインシデント（事件・事故）の被害が増加・甚大化しています。被害が甚大化することで、被害拡大の防止、復旧作業、原因の解明や改善などに、想像以上の時間やコスト、対応が必要となります。また、損害賠償への発展や社会的信用が失墜し顧客離れ、ユーザー離れにもつながるかもしれません。

セキュリティインシデントが発生する要因・原因は、ハイブリットクラウド化、DX、テレワーク、IoT、AI、自動化など積極的にIT技術を取り入れたものの、セキュリティに対する意識・知識・経験や、セキュリティ対策・体制などセキュリティの確保ができていなかったことが考えられます。

今どのような対応ができて、これからどのような手を打つべきか、ハイブリッドクラウド時代の“モダンセキュリティ”についてご紹介します。

このような方におすすめ

- 組織のゼロトラストのあるべき形と現状のギャップを確認し対策に役立てたい
- 企業内の異なる立場（一般ユーザー、開発者、運用者）に適したセキュリティ対策をしたい
- 脅威情報をどのように取得して、いかに自社に活用すべきかを知りたい
- EDR製品導入後の運用課題に対して、ベンダーとSIerのサービスの違いを確認したい
- 大企業の4割でサイバー対策不安あり。外部から見える自社の弱点を把握し対策を講じたい
- セキュリティ事故発生後の復旧と回復について対策の疑問・悩みを解決したい
- セキュアなクラウドネイティブ環境をどう実現するのか、SIerと共に対策を検討したい

お問い合わせ

伊藤忠テクノソリューションズ株式会社　CTCセキュリティサミット事務局

mrc-info@ctc-g.co.jp

www.business-on-it.com/event/ctc-security-summit

CTC Challenging Tomorrow's Changes

CTC セキュリティサミット 2022

プログラム

CTC セキュリティサミット 2022

ハイブリッドクラウド時代の“モダンセキュリティ”

14:00-14:30

All about CTCのセキュリティ

マネージドサービス企画・推進事業部　事業部長　金子 長寛

14:30-14:50

米政府のゼロトラスト成熟度モデルから紐解く、最新セキュリティ動向

サイバーセキュリティサービス部　ソリューション課　課長　萩原 聡

ゼロトラストはキーワードが先行して「どこまでやればゼロトラスト？」とお悩みの方も多いのではないでしょうか。米国では政府機関向けにゼロトラスト移行方針が示され、その動きは民間企業へも広がりつつあります。本セッションでは、米政府が採用するゼロトラストのあるべき形（To-Be）と現状（As-Is）を分析する手法である「ゼロトラスト成熟度モデル」を解説しつつ、組織の現状とあるべき形のギャップを埋める方法についてもご紹介します。

14:50-15:10

情報戦を制する！　～ ハイブリッドクラウド時代の脅威ベースアプローチ ～

サイバーセキュリティサービス部　レジリエンス課　エキスパートエンジニア　東 拓央

企業インフラがハイブリッドクラウドへ移行するとともに、テレワーク化等の推進等により企業の環境の変化が進み、今までの手法では対処困難な新たな脅威に対して、迅速なの対応が求められる時代となっています。新たな脅威をより早く察知して対処するために、公知の情報だけでなくダークウェブも含めた広大な情報元から自社の脅威につながる情報を見つけ出し、セキュリティ対策へ活用する、脅威ベースアプローチに注目が集まっています。本セッションでは、脅威インテリジェンス情報を用いて、サイバー攻撃から自社を効率的に守るために必要な手段についてご紹介します。

15:10-15:30

レガシーSOCからモダンSOCへ　～ CTC-SOCのサイバーセキュリティ監視システムのアップグレード事例 ～

サイバーセキュリティサービス部　SOC運営課　主任　平賀 辰樹

CTCセキュリティオペレーションセンタ（CTC-SOC）は、2021年7月に、セキュリティ監視基盤をオンプレミス型のSIEMから、クラウドネイティブSIEMである「Microsoft Sentinel」に刷新しました。Microsoft Sentinel に移行した理由やクラウドネイティブSIEMならではの特長、インシデント検知の仕組み、監視・運用の課題、SOARの実装事例など、モダンSOCにアップグレードした CTC-SOC のサイバーセキュリティ監視システムの構築・運用の裏側を惜しみなくご紹介します。

15:30-15:40

休憩（アンケート）

お問い合わせ　伊藤忠テクノソリューションズ株式会社　CTCセキュリティサミット事務局

mrc-info@ctc-g.co.jp　www.business-on-it.com/event/ctc-security-summit

CTC Challenging Tomorrow's Changes

プログラム

CTC セキュリティサミット 2022

ハイブリッドクラウド時代の“モダンセキュリティ”

15:40-16:00

EDR を正しく理解して導入・運用していますか？　～ EDR を120%活用するヒント ～

サイバーセキュリティサービス部　SOC運営課　**課長　宮崎 孝之**

マルウェアによるサイバー攻撃の巧妙化、複雑化、およびコロナ禍によってリモートワークを採用する企業も増え、EDR製品を導入する企業も急激に増えています。従来のウイルス対策製品とは違い、EDR 製品は名前の通り、”検知”と”対応”が必要です。検知したアラートを分析・判断し、結果によってはプログラムの強制終了やネットワークからの隔離が求められます。しかもアラートはいつどこで発生するかわかりません。このような EDR 製品導入後に陥る運用上の課題、およびその解決のためのヒントをご紹介します。

16:00-16:20

脆弱性診断のいま、これから

サイバーセキュリティサービス部　アセスメント課　**課長　中島 嗣晶**

ITシステムの多様化・複雑化が進む中、『脆弱性診断』の重要性は増すばかりです。しかし「十分な診断ができてない」、「診断結果の活用に関して課題がある」といった声をよく聞きます。システム開発・リリースサイクルが短くなる現在、脆弱性診断にも高速化・効率化と同時に高い専門性と品質の維持が求められています。本セッションでは、これまでの脆弱性診断の提供実績を踏まえて、いま／これからの時代において脆弱性の把握・対策にどう向き合い取り組むべきかお伝えします。

16:20-16:40

クラウドからエンドポイントに先手必勝のCybersecurity Mesh

サイバーセキュリティサービス部　サービスインテグレーション課　**課長　瀧本 正人**

クラウドシステムのDX活用や、リモートワークの促進で企業内でコントロールできた情報資産（PC、サーバなど）が企業外に分散されています。それに伴い、情報資産の管理やセキュリティパッチの適用、脆弱性の放置など浮き彫りになった課題をサイバーセキュリティメッシュアプローチを用いて解決します。広範囲に分散した資産を守る、サイバーセキュリティメッシュサービスをご紹介します。

16:40-17:00

セキュアなクラウドネイティブ環境を実現するための勘所について

マネージドサービス企画・推進事業部　クラウドネイティブ推進部　**事業部長代行 兼 部長　池永 直紀**

Kubernetesやクラウドネイティブ技術を活用したシステム創りへのニーズは年々高まってきています。その一方で、セキュリティ観点はこれまでのバーチャルマシンを中心としたシステムとは異なる、新たな考慮ポイントや観点が必要となります。
本セッションでは、NIST SP800-190のポイントを解説しながら、セキュアなクラウドネイティブ環境をどのように実現すべきかの構成例とそのアプローチ方法をご紹介します。

お問い合わせ　伊藤忠テクノソリューションズ株式会社　CTCセキュリティサミット事務局

mrc-info@ctc-g.co.jp　www.business-on-it.com/event/ctc-security-summit

CTC Challenging Tomorrow's Changes