

サイバーセキュリティ経営ガイドラインから紐解く標的型攻撃対策 ～セキュリティソリューションの連携による高度標的型攻撃対策～

参加費
無料

昨今、多くの情報漏えい、とりわけ標的型攻撃の事例が話題となっています。単に最新のセキュリティソリューションを導入していても攻撃を完全に防げないのが現状であり、皆様頭を悩まされている事と思います。

対策として多層防御によって防御力の向上を図り、侵入を前提とした検知機能や運用体制を整える必要があることは理解しつつも、どこから手をつければよいか分からず、手をこまねいている組織も多いのではないのでしょうか。

昨年末に経済産業省によって公開されたサイバーセキュリティガイドラインを切り口に、システム全体として如何に防ぎ、如何に検知するか、複数のソリューションを結合したサイバーセキュリティ対策の一例をご紹介します。

開催概要

開催期日	2016年7月27日(水) 13:20 ~ 16:50 (受付開始13:00~)
開催場所	A P 東京八重洲通り 東京都中央区京橋1丁目10番7号 KPP八重洲ビル7階 ・JR東京駅八重洲中央口 徒歩6分 https://www.tc-forum.co.jp/kanto-area/ap-yaesu/ya-base/
参加費	無料 (事前登録制)
定員	50名 (申込締切: 定員になり次第締め切らせていただきます)
主催/協賛	主催: ニッセイ情報テクノロジー株式会社 協賛: マカフィー株式会社 マクニカネットワークス株式会社 デジタルガーディアン株式会社 アズビルセキュリティフライデー株式会社

アジェンダ

※講演内容詳細については裏面をご覧ください

13:00 (開場)	受付開始
13:20 (開始)	セミナー開催のご挨拶
	講演 1: サイバーセキュリティ経営ガイドラインにおける技術対策について サイバーセキュリティ対策を効果的に進める「脅威対策ライフサイクル」のご説明
	講演 2: ITシステム内部に侵入したサイバー攻撃活動を見える化する「VISUACTシリーズ」 攻撃者が改竄を施せないパケットシーケンスを解析してログを生成し見える化を実現
	講演 3: マルウェアによるデータのハイジャックをブロックする最新DLPソリューション 標的型攻撃などの外部脅威から重要なデータを守るために何をすべきか
	講演 4: スモールスタートではじめるログ分析～VISUACT・DigitalGuardianとともに～ 導入経験から得た知見を元に、各社様製品を活用したSIEM実装例をご紹介します
	講演 5: 総括 (統合的セキュリティ対策における事例紹介) 複数のソリューションを用いた統合的なセキュリティ対策のご紹介
16:50 (終了)	質疑応答・アンケート記入

お申込サイト: <http://www.sbbit.jp/eventinfo/36140>

お問い合わせ: ニッセイ情報テクノロジー株式会社 ITソリューション営業本部 梅木(ウメキ)・塩崎(シオザキ)
Tel. 03-5532-3044 Mail. security_info@nissay-it.co.jp

ご記入いただいた個人情報は、ニッセイ情報テクノロジー、マカフィー、デジタルガーディアン、マクニカネットワークス、アズビルセキュリティフライデーからのご案内(当社主催のイベント・セミナー、製品・サービスのご案内、アンケート等へのご協力のお願い、お客様層の分析、各種統計資料の作成)で使用させていただきます。その他の目的で使用する場合には、必ず個人情報を提供していただいた本人の同意のもとに使用します。各社の個人情報保護方針については各社サイトをご確認ください。

<http://www.nissay-it.co.jp/company/policy.html>, <http://www.mcafee.com/jp/index.html>, <https://digitalguardian.com/ja>, <http://asf.azbil.com/jp/>, <http://www.macnica.net/>

プログラム	
13:00 (開場)	受付開始
13:20～13:30	セミナー開催のご挨拶 ニッセイ情報テクノロジー株式会社 ITソリューション営業本部 生駒 勝治
13:30～14:00	サイバーセキュリティ経営ガイドラインにおける技術対策について 経済産業省サイバーセキュリティ経営ガイドラインに記載されている技術対策のポイントと、対策を効果的に進めるコンセプトとして「脅威対策ライフサイクル」を説明致します。サイバー攻撃の被害を最小限にするため、インシデントレスポンスにおいて経営層・現場担当に共通して重要な、素早く、的確な判断と対策を実現する運用モデルもご紹介致します。 マカフィー株式会社 セールスエンジニアリング本部 櫻井 秀光 氏
14:00～14:40	ITシステム内部に侵入したサイバー攻撃活動を見える化する「VISUACTシリーズ」 内部ネットワークに侵入したマルウェアは、長期間見つからずに活動し続けることを重視するためWindowsネットワークに紛れて活動します。またイベントログの消去などの隠ぺい工作も行います。「VISUACTシリーズ」は、攻撃者が改竄を施せないパケットシーケンスを解析してログを生成し、内部ネットワークにおける活動を見える化します。 アズビルセキュリティフライデー株式会社 営業部 内田 秀和 氏
14:40～14:50	休憩
14:50～15:30	マルウェアによるデータのハイジャックをブロックする最新DLPソリューション データを守る「最後の壁」としてのDLPが再び注目を集めています。ランサムウェア等によるデータのハイジャックに対し、DLPの有効性が認められたためです。標的型攻撃などの外部脅威から重要なデータを守るために何をすべきかについて、DLPという視点でお話しします。 デジタルガーディアン株式会社 石井 靖彦 氏
15:30～16:10	スモールスタートではじめるログ分析～VISUACT・DigitalGuardianとともに～ 高度化するサイバー攻撃への対策として、侵入を前提とした発見型対策ソリューション“SIEM”の必要性が広く認知されるようになりました。しかし導入に向けてのフロー、効果のイメージがわからない方も少なくないのではないのでしょうか？ 本セッションでは、マクニカネットワークスが導入経験から得た知見を元に、各社様製品を活用したSIEM実装例をご紹介します。 マクニカネットワークス株式会社 技術統括部 プロダクト第2技術部 第1課 岡地 紘 氏
16:10～16:40	総括（統合的セキュリティ対策における事例紹介） 標的型攻撃への対策として、今まで様々なソリューションを検討し、自社に不足しているものを導入してきました。しかし、本当に必要なソリューションを導入し、またその有効活用ができているのでしょうか。セキュリティアセスメントを通じた、お客様のセキュリティ対策状況の客観的分析及び必要なセキュリティ対策を見つける方法と、一例として本日ご紹介した複数のソリューションを用いた統合的なセキュリティ対策をご紹介します。 ニッセイ情報テクノロジー株式会社 インフライノベーション事業部 ビジネスイノベーション室 小澤 賢一朗
16:40～16:50 (終了)	質疑応答・アンケート記入