

# 情報セキュリティマネジメントセミナー 「事例に学ぶ 情報漏えい対策の高度化」



企業だけでなく、政府機関での被害が表面化している標的型攻撃や、組織内ユーザーや特権者などによる内部情報漏えいなど、その手法は多様化・巧妙化しています。これらへの対策の重要性についてはある程度認識されているものの、まだまだ十分な対策がなされているとは言えない状況です。

当セミナーでは、情報セキュリティマネジメントにおいて直面している課題に対し、現状の認識と、今から取り組める具体的な課題解決の手段やポイントを整理してまいります。

このようなお客様に  
特にオススメです！

- ・標的型攻撃について理解を深め、対策の必要性を見極めたい
- ・情報漏えいにてできるだけ早く気づく仕組みを作りたい
- ・セキュリティ事故発生時に組織が機能するためのポイントを知りたい

## セミナー概要

日時 2015  
**8/28** 金 14:00~16:55  
(13:30受付開始)

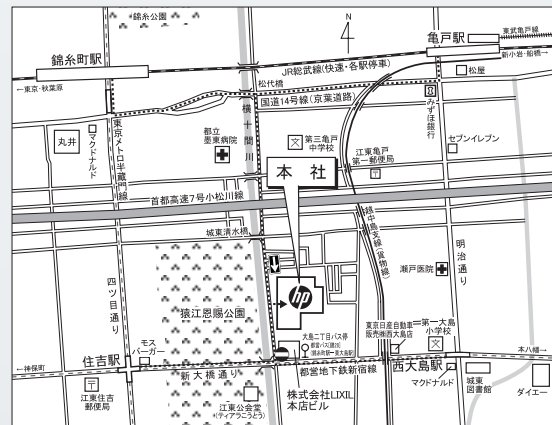
定員 50名

参加費 無料

会場 日本ヒューレット・パッカード株式会社  
大島本社  
〒136-8711 東京都江東区大島2-2-1

- アクセス
- ・都営新宿線・東京メトロ半蔵門線：住吉駅 A3出口徒歩7分
  - ・都営新宿線：西大島駅 徒歩8分
  - ・JR総武線：錦糸町駅南口 徒歩15分
  - ・JR総武線：東武亀戸線 亀戸駅 徒歩15分

共催 日本ヒューレット・パッカード株式会社  
SCSK株式会社



## お申し込み

URL 以下URLよりお申し込みください  
[http://www.scsk.jp/event/2015/20150828\\_3.html](http://www.scsk.jp/event/2015/20150828_3.html)

SCSK イベント

Search



## PROGRAM

14:00 ~ 14:05	開会挨拶
14:05 ~ 14:40	<p><b>ビッグデータ時代に必要なセキュリティ対策とは ～どこから始めるか～</b></p> <p>日本ヒューレット・パッカート株式会社 エンタープライズ・セキュリティ・プロダクツ統括本部 セキュリティソリューションコンサルタント 水野 令一</p> <p>今日の脅威は、攻撃者の多様化、悪質化、攻撃技術の巧妙化により、従来の手法では防ぎきれない状況となっています。新たな脅威に対し、可視化されたあらゆるデータを分析して、そこで生まれている脅威を把握できる技術が必要になります。内部に潜む脅威を可視化するセキュリティインテリジェンスを中心にHPセキュリティのポートフォリオをご紹介します。</p>
14:40 ~ 14:45	ショートブレイク
14:45 ~ 15:20	<p><b>いかにCSIRTを構築・運用するか ～有事に機能するCSIRTの作り方～</b></p> <p>SCSK株式会社 ITマネジメント事業部門 netXデータセンター事業本部 セキュリティサービス部 インテグレーション第二課 マネージャ 富田 洋康</p> <p>既にCSIRTを構築しているユーザ様から「継続的な運用が難しい」「有事に有効に機能するか不安」といったお話をよく伺います。このような背景から、本講演では、SCSKが保有する実績の中からCSIRTを運用していく上での課題・問題点を抽出し、「いかに運用を継続するか」「いかに有事に機能させるか」について、実際の事例を交えてご説明します。</p>
15:20 ~ 15:35	コーヒーブレイク
15:35 ~ 16:10	<p><b>情報漏えいリスクを低減するためのセキュリティマネジメント ～外部内部の脅威を早期発見するシステムの作り方～</b></p> <p>SCSK株式会社 ITマネジメント事業部門 netXデータセンター事業本部 セキュリティサービス部 インテグレーション第一課 マネージャ 青木 哲也</p> <p>外部からのサイバー攻撃や内部犯行などの不正アクセスによる情報漏洩のリスクが顕在化してきています。一方で内外からの脅威に対し、どのように対策をすることが効果的なのか、どこから着手すべきなのかを検討することは容易ではありません。本講演では、SIEMソリューションの豊富な導入実績をもとに、課題に対する解決策をご紹介します。</p>
16:10 ~ 16:15	ショートブレイク
16:15 ~ 16:50	<p><b>相次ぐ情報漏えいから企業を守る ～実際に標的型攻撃に使われたマルウェアを大解剖～</b></p> <p>SCSK株式会社 ITマネジメント事業部門 netXデータセンター事業本部 セキュリティサービス部 セキュリティサービス課 マネージャ 松村 卓也</p> <p>頻発する情報漏えい事故の多くに、既存の対策では検知することができないマルウェアが使われています。なぜ「検知できないのか」を実際に標的型攻撃に使われたマルウェアを解析することによって解説します。また、そのような現状において、現実的に有効な対策をご紹介します。</p>
16:50 ~ 16:55	閉会挨拶

※ 予告なくプログラム内容が変更される場合がございます。予めご了承ください。※ 記載されている製品/サービス名称、社名、ロゴマークなどは該当する各社の商標または登録商標です。  
※ 本セミナーの対象とならない方、同業他社の方はお断りさせて頂く場合がございます。予めご了承ください。



日本ヒューレット・パッカート株式会社  
エンタープライズ・セキュリティ・プロダクツ統括本部  
〒136-8711 東京都江東区大島2-2-1  
TEL: 0120-436-555  
e-Mail: HPEnterpriseSecurity-jpinfo@hp.com



SCSK株式会社  
ITマネジメント事業部門 netXデータセンター事業本部 セキュリティサービス部  
〒135-8110 東京都江東区豊洲3-2-20 豊洲フロント  
TEL: 03-5548-5428  
e-Mail: sys-info@ml.scsk.jp

※ 記載の内容は2015年7月時点のものです。