

法律上の位置づけ、報告時の留意事項、漏えい時の事業者の責任、私たちを取り巻く「サイバー」な出来事・・・

企業内部情報の漏えいリスクと その対応ポイント

～弁護士・実務専門家の視点から、企業内部情報の漏えいリスクについて詳細解説～

◆開催要領◆

<日 時> 2016年 4月 19日(火) 13:30～17:00

<会 場> 「企業研究会セミナールーム」(東京・麹町) 東京メトロ麹町駅より徒歩5分

講師

アンダーソン・毛利・友常法律事務所 弁護士 中崎 尚 氏

【講師略歴】 東京大学法学部卒。2001年弁護士登録、アンダーソン・毛利・友常法律事務所入所。2007年より Columbia University School of Law を修了、米国ワシントン D.C. の Arnold & Porter 法律事務所に勤務。2009年に復帰後は、インターネット法、IT法を中心に、知的財産権法、クロスボーダー取引など幅広い業務を提供。ソーシャルメディアやビッグデータをはじめとする IT 分野の論文、講演を数多くこなしている。

ソフトバンクテクノロジー(株) シニアセキュリティエバンジェリスト 辻 伸 弘 氏

【講師略歴】 1979年大阪府生まれ。セキュリティ・エンジニアとして、コンピュータの弱点を洗い出し修正方法を助言するペネトレーション検査などに従事している。自宅では、趣味としてのハニーポットの運用、侵入検知システム(IDS)による監視、セキュリティ情勢の調査および分析などを行っている。セミナー登壇多数の他、日経プラス10(BSジャパン)出演、「実践Metasploit」(オライリー)監訳、オンライン記事として、「セキュリティ・ダークナイト」(@IT)「セキュリティのトビラ」(マイナビ)などで執筆。

◆ご参加頂きたい方◆

情報システム・法務・監査部門の方、情報セキュリティ対策のご担当者

●受講料 ●1名(税込み、資料代含む)

一般社団法人 企業研究会 セミナー事務局宛

正会員	32,400円(本体価格30,000円)
一般	35,640円(本体価格33,000円)

申込書 FAX: 03-5215-0951

■参加要領

申込書はFAX、または下記担当者宛 E-mail にてお送り下さい。以下の当会ホームページからお申し込みいただけます。

後日(開催1週間～10日前までに)、受講票・請求書をお送りします。(https://www.bri.or.jp)

*よくあるご質問(FAQ)は当会ホームページにてご確認ください。([公開セミナー] → [よくあるご質問])

*お申込後のキャンセルはお受けしかねますので、ご都合が悪くなった場合、代理の方のご出席をお願いいたします。

*最少催行人数に満たない場合は、中止とさせていただきます。ありますので、ご了承ください。

■お申込・お問合せ先

一般社団法人企業研究会 セミナー事務局

担当) 鈴木 E-mail: a-suzuki@bri.or.jp

TEL: 03-5215-3550 FAX: 03-5215-0951

東京都千代田区麹町5-7-2 麹町M-SQUARE2F

161116-0313	2016.04.19	企業内部情報の漏えいリスクとその対応ポイント	
ふりがな 会社名			
住所	〒		
TEL		FAX	
ふりがな ご氏名		所 属 役 職	
E-Mail			
ふりがな ご氏名		所 属 役 職	
E-Mail			

※申込書にご記入頂いた個人情報、本研究会に関する確認・連絡および当会主催事業のご案内をお送りする際に利用させていただきます。

※申込書をご送信いただく際は、FAX番号をお間違えないようご注意ください。

4月19日(火)

於:東京・麹町「企業研究会セミナールーム」

【第1部】13:30 ~ 15:30

「特定個人情報の漏えい時のリスクとその対応ポイント」

1. 法律上の位置づけ
2. 事案発覚時に事業者が講じるべき措置
 - (1) 事業者内部における報告
 - (2) 被害の拡大防止
 - (3) 事実関係の調査、原因の究明
 - (4) 影響範囲の特定
 - (5) 再発防止策の検討・実施
 - (6) 影響を受ける可能性のある本人への連絡等
 - (7) 事実関係、再発防止策等の公表
3. 報告時の留意事項
 - (1) 報告の方法
 - ・主務大臣のガイドライン等において報告対象となる事案
 - ・報告する主務大臣等を直ちに特定できない事案
 - ・その他、番号法固有の規定に関する事案等の事案
 - (2) 報告の時期
 - (3) 報告書の様式
 - (4) 「重大事案」とは
 - (5) 「おそれのある事案」とは
 - (6) 特定個人情報保護委員会への報告を要しない場合
4. 漏えい時の、事業者の責任
 - (1) 法律上の罰則
 - (2) 行政対応
5. 事前整備の重要性
 - (1) 事案発覚後の対応を行う組織・体制の整備
 - (2) 事案の発見・兆候の把握
6. 最後に
 - (1) 特定個人情報の漏えいを起こさない情報管理体制整備のポイント
 - (2) 内部統制やモニタリング等 体制整備のポイント
～未然防止・起きてしまっても早期発見・早期解決する仕組み作り～
 - (3) ここまで対策してたら、大丈夫とみなされるレベル感はあるのか？
内部統制システム構築との関係で、問題と見なされないレベル感はあるか。

アンダーソン・毛利・友常法律事務所

弁護士

中崎 尚 氏

【第2部】15:30 ~ 17:00

「私たちを取り巻く「サイバー」な出来事」 ～忍び寄る影の実体と向き合うため～

ここ数年で私たちにとって「サイバー」という言葉がより身近になってきました。もはや、日常の一部になってしまったといっても過言ではないでしょう。

それにはもちろん便利であり人を幸せにする側面も多分にありますが一方でそれは見る方向を変えれば「便利な凶器」となります。

標的型攻撃、不正送金、身代金要求ウイルス、フィッシング、内部情報漏洩などなど。

サイバー空間の安全は今や交通安全や地域社会の安全と同様に多くの人々がそれぞれ意識を高め

力を合わせていかなければならなくなっています。今回は私が向き合ってきた脅威をデモを交えることでその実体を見ていただき、一緒に考える時間を過ごしましょう。

ソフトバンクテクノロジー(株) シニアセキュリティエバンジェリスト 辻 伸 弘 氏