

営業秘密・個人情報の漏洩(サイバー攻撃を含む)対策として検討すべき 情報管理体制・社内規程の見直しと従業員教育のポイント

～不正競争防止法、営業秘密管理指針、秘密情報の保護ハンドブック、個人情報保護法のガイドライン等、最新情報を踏まえて～

●日 時● 2017年 11月 21日(火) 13:00～17:00

●会 場● 東京・麹町『企業研究会セミナールーム』

講 師 牛島総合法律事務所 パートナー弁護士 影島 広泰 氏

【略歴】一橋大学法学部卒業、03年弁護士登録、牛島総合法律事務所入所。ITシステム・ソフトウェアの開発・運用、個人情報・プライバシー、ネット上のサービスや紛争に関する案件を中心に活躍中。実務視点のわかり易い講義に定評がある。日本経済新聞社「企業法務・弁護士調査」2016年情報管理部門において「企業が選ぶランキング」2位。裁判所ウェブサイトで公開された最新判例の判決文を自動的に分析してTwitterに投稿するBot(プログラム)を提供 (@kageshima)。約25万ダウンロードのiPhone/iPad人気アプリ「e六法」開発者。「法律家・法務担当者のためのIT技術用語辞典」(商事法務)、「個人情報保護法と企業実務」(清文社)、「情報漏洩事案の類型別 分析と対策」(月刊ザ・ローヤーズ 2014年5月号(ILS出版)等、著書・論文多数。

◆ 開催にあたって

企業の競争力の源泉となる営業秘密や個人情報の漏洩が後を絶たず、また、特定企業を狙った標的型攻撃メールをはじめサイバー攻撃も増加しており、多くの企業にとって情報管理体制の見直しが喫緊の課題となっています。

本セミナーでは、昨今の状況を受けて改正や改訂が相次いだ情報管理に関する法律、指針、ガイドライン等の要点を整理し、企業に求められる法的義務を明らかにします。更には、現行の情報管理体制の見直しを検討する際に有効な社内規程のサンプル、従業員教育のポイント等を紹介し、営業秘密・個人情報の漏洩対策として企業が講じるべき対応策について、ケーススタディも交えながら実践的に解説していきます。

《詳細は裏面をご覧ください》

●受講料● 1名(税込み、資料代含む)

正会員	33,480円	本体価格 31,000円
一般	36,720円	本体価格 34,000円

- 正会員の登録の有無など、よくあるご質問(FAQ)は、当会ホームページでご確認いただけます。(〔TOP〕→〔公開セミナー〕→〔よくあるご質問〕)
- お申込み後(開催日1週間～10日前までに)受講票・請求書をお送り致します。
- お申込み後のキャンセルは原則お受け致しかねますので、ご都合が悪くなった際は、代理出席をお願い致します。
- 最少催行人数に満たない場合ほか、諸般の事情により開催を中止させていただく場合もございます。
- 本申込書をFAXでお送りいただく際は、ご使用のFAX機の使用法(0発信の有無など)をご確認の上、番号をお間違えないようご注意ください。

一般社団法人企業研究会

担当：上島 E-mail kamijima@bri.or.jp
〒102-0083
東京都千代田区麹町5-7-2 麹町M-SQUARE 2F
TEL 03-5215-3516 FAX 03-5215-0951

申込方法 ホームページからのお申込みが便利です。https://www.bri.or.jp

企業研究会セミナー

検索

*セミナーの最新情報もご覧いただけます。

171606-0302(※)		2017.11.21	
申込書 情報管理体制・社内規程の見直しと従業員教育のポイント			
会社名	フリガナ		
住所	〒		
TEL		FAX	
ご氏名	フリガナ	所属 役職	
Eメール			

【個人情報の利用目的】お客様の個人情報は、お申込受付後のご連絡やご請求等を行うため、また、ダイレクトメールの発送等、当会主催の各種事業をご案内するために利用させていただきます。

営業秘密・個人情報の漏洩(サイバー攻撃を含む)対策として検討すべき 情報管理体制・社内規程の見直しと従業員教育のポイント

● プログラム ●

- 解説 -

■講師 牛島総合法律事務所 パートナー弁護士 影島 広泰氏

13:00

I. 情報漏洩事件をめぐる近時の傾向と情報管理体制見直しの必要性

- (1) 営業秘密の漏洩 ~製造技術、研究データ、顧客情報等の持ち出し
- (2) 個人情報の漏洩 ~管理ミス、誤操作/サイバー攻撃・システムからのデータ漏洩
- (3) サイバー攻撃 ~標的型攻撃メール、ランサムウェアなど
- (4) 裁判例で考える情報管理の法的義務

II. 営業秘密を保護するための法律、指針、ハンドブックと実務対応

- (1) 不正競争防止法の再確認 ~営業秘密を満たす3要件から罰則まで
- (2) 「不正競争防止法」改正(2016年1月1日施行)のポイント
 - ・「未遂行為」への罰則と具体例、第3次取得者以降への処罰の拡大、罰金刑の上限引き上げ
 - ・犯罪収益の任意的没収規定の導入、営業秘密侵害品の譲渡・輸出入等に対する差止請求、等
 - ・改正法について、役員・従業員へ周知しておくべきこと
- (3) 「営業秘密管理指針(2015年1月全面改訂)」のポイント
 - ・「ベストプラクティス」から、「法的保護を受けるために必要な最低限の水準の対策を示すもの」への改訂
 - ・秘密管理措置の具体例(紙媒体、電子媒体、媒体が利用されない場合、他)
 - ・改訂版管理指針よりも対応が甘かった場合の社内体制見直しの必要性
- (4) 「秘密情報の保護ハンドブック(2016年2月公表)」のポイント
 - ・情報管理に関する「ベストプラクティス」としての役割(法律、指針、ハンドブックの関係)
 - ・ハンドブックに記載の「従業員等」「退職者等」「取引先」「外部者」それぞれに向けた対策
- (5) 法律、指針、ハンドブックを踏まえた社内規程(サンプル)と実務対応
 - ・前提となる情報資産の洗い出しとその方法、社内の組織体制の整備、従業員への周知
 - ・「秘密情報管理規程」、「文書管理規程」、「個人情報取扱規程」といった様々な規程の整理の仕方
 - ・退職後の競争禁止条項の有効性(有効性が認められる/認められない可能性が高い規程とは)

III. 個人情報の漏洩を防止するための法律、ガイドラインと実務対応

- (1) 個人情報保護法における「安全管理措置」の要点 ~ガイドラインとQ&Aを踏まえて
 - ・安全管理措置(組織的、人的、物理的、技術的)の内容と講ずべき手法
 - ・委託先の選定基準、委託先における個人データ取扱状況の把握、委託契約に盛り込むことが望まれる事項
 - ・委託先の監督において実務的に注意したいポイント(再委託、漏洩の際の損害賠償の定め)
- (2) 法律、ガイドラインを踏まえた社内規程(サンプル)と実務対応

IV. サイバー攻撃に対する現実的な対応【ケーススタディによる考察】

- (1) 標的型攻撃メール
 - ・その巧妙な手口(ウィルス感染から情報流出の発覚、公表に至るまで)
 - ・標的型攻撃を避けるための重要情報の取扱い
 - ・万が一標的型攻撃にあってしまった時の対応(事前に全従業員に徹底しておくべきこと)
- (2) ランサムウェア
- (3) 「サイバーセキュリティ経営ガイドライン」に基づいた対応

V. 情報管理に関わる体制・ルールの見直しと従業員教育のポイント

- (1) 情報管理に関わる体制・ルールの見直し
 - ・モニタリングの強化、機器・メディアの持ち込み禁止と入出制限の徹底、対応専門部署の新設
 - ・誓約書・秘密保持契約書の見直しと整備
 - ・私物の携帯電話・スマホを業務利用するための社内ルール(BYODルール)、等
 - ・情報漏えい時の対応規程
- (2) 効果的な従業員教育のポイント
 - ・経営陣・従業員への意識改革(会社が被る被害額、従業員に対する処分、株主代表訴訟の実例の啓発)
 - ・問題意識を持たせる系統的かつ継続的な教育訓練、教育ツール・カリキュラム・マニュアルの作成
 - ・標的型攻撃メールの見分け方(製品の問合せ、セキュリティの注意喚起、取材申込、就職活動の問合せ)、等

17:00