管理者必須！　これだけ情報漏洩対策ポイント

当たり前のように起きてしまう事しか起きていない！情報漏洩の対策は、ごく当たり前の事をするだけで対策出来ます。知らなかった、悪意なかった…しかし事件が発生したら、どんな事情であっても漏洩は漏洩です。まず知る事からはじまります。

■ 研修のねらい

具体的事例に置き換えて研修を進めます。なぜ対策するのか？様々な立場から考えます。

1．攻撃が最大の防御から考えることで、情報・漏洩・対策が基礎３部構成になります。

2．徹底的に体感する実践研修は、ロープレ・実例・シミュレーションの３構成になります。

3．漏洩する出口を発見認知することから、弱点部分の問題解決、対策案を知って頂きます。

■ 対　象

ミドルマネジメントを対象とします。守るためには、手法を知ることからはじまります。
経営幹部だけを対象とした研修内容のアレンジも対応します。最低限の事を知って下さい。

■ プログラム

●基礎研修（１日）

コンセンサス・研修守秘義務について
オリエンテーション・研修の狙いと目的
　携帯冊子の情報漏洩これだけチェックを使用
1．情報とは？
　情報の基礎、プライバシーの範囲、機密情報
2．漏洩とは？
　なぜ漏れるのか？単純発生する問題、
　プロセス
3．対策とは？
　出口発見、起こりにくい仕組み、逆トラップ
応用シュミレーション
　漏洩実例からグループ討論・発表（刑事編）
まとめ：理解度チェック・質疑応答
　ゴール：漏洩対策のポイントがわかること

●実践研修（１日）

コンセンサス・研修守秘義務について
　オリエンテーション・研修の狙いと目的
1．ロールプレイング
　五感から感性を高めることで、情報感度アップ！
2．実例ケーススタディ
　技術的手法 vs 人的手法から考える対策とは？
3．攻撃的手法から学ぶ防衛術
　ソーシャルエンジニアリングのワナとは？
応用シュミレーション
　身近な事例でグループ討議、発表（クレーム編）
まとめ：理解度チェック・質疑応答
　ゴール：漏洩対策のセンスがわかること

■ 講師料・依頼条件など

１日研修：２０万円。（消費税別）。※双方向での研修になりますので１５名までに致します。受講者によっては研修内容の調整が必要です。基礎から実践研修に進めることで、より深く理解出来ます。自ら考えることで、実践的な対策案が見えてきます。

■ 講師よりひとこと

情報漏洩対策は、現状の漏洩パターンを知ることからはじまります。新入社員むけのインターネット利用者講習～トップマネジメントが最低限知らないと重大な問題に発展することまで、人に焦点をあてた研修が中心です。まず知るべきことを知っていただきたいです。毎月のコンサルティング型研修メニュー（月１回・半日１５万円×６ヶ月間）もご用意しております。抜き打ちチェックを研修と同時に進めることで理解浸透が早くなります。

■ 講師プロフィール ■

新倉　茂彦（Shigehiko Niikura）1969年生まれ

有限会社ティーシーニック　代表取締役

■ 専門分野

◎セミナー講師　　◎IT・情報システム　　◎新規事業

■ 得意業界

◇インターネット　　◇法人向けサービス業　　◇学校・教育

■ 経　歴

イベント関連の仕事で手配・管理・調整・折衝等のコーディネーターを現場で１２年経験。
その後、コンピュータネットワークセキュリティの論理的分野と物理的セキュリティ分野で経験を積み、リスクマネイジメントの観点から現在は情報セキュリティ分野で活動中。
情報漏洩対策に独自思考と現実的なバランスを折衷することに集中し、情報セキュリティ対策のさらなる追求を目指し、漏洩対策を大学院で研究。
攻撃が最大の防御をポリシーに、情報を狙う側の思考を折り込んだ防衛術を追求する。
・国内旅行業務取扱主任者／国際パフォーマンス研究所パフォーマンスアドバイザーコース修了

■ コンサルティング実績

（１）コンサルティング…情報漏洩対策の総合提案・導入・実施／インターネットにおける情報漏洩対策／ソーシャルエンジニアリング手法を用いた抑止対策／顧客で起こった問題の相談・解決・提案／顧客に起こりうる事前対策・提案
（２）セミナー啓蒙の講師…カスタマイズしたセミナー企画・立案・講師
（３）物理セキュリティ…集中統合管理のネットワークカメラ企画･提案･導入／ネットワークカメラの活用・販売方法の企画・提案・導入／物理セキュリティ・入退室管理対策／物理データ破壊対策
（４）ネットワークセキュリティ…ネットワーク環境の整備・導入／ネットワーク上の漏洩対策
（５）企画提案…情報漏洩対策の企画・提案・実施・導入／新規事業の立ち上げ

■ セミナーテーマ

「情報漏洩これだけ！対策」「インターネット基礎講習」「実例！丸見え個人情報」他

■ PR・特記事項

中間に立つコーディネータ役として、技術的対策と非技術的対策の相反するギャップを調整、実行する。常に問題意識持ち “なぜだろう？” から物事を考え、別な角度からも物事を見て多角的に考える事を重視し、そこから代替案を提供。なによりも知的好奇心がとても重要と考えます。得意な事は、新しい事をゼロから構築し、まとめあげること。現在、多摩大学大学院ＭＢＡで情報漏洩対策のモラルを研究中。