

『NTT R&D 情報セキュリティ
シリーズ』第3弾!!

インシデントに対応するのはアナタ自身!

事例で学ぶ セキュリティ運用技術・インシデント対応技術

中～大規模企業をモデルに、インシデント(セキュリティ被害)が発生した場合の対応を時間軸に沿って具体的に解説し、実践的な知識と技術を身につける『事例で学ぶセキュリティ運用技術・インシデント対応技術』を6月20日(火)に刊行いたします。貴紙誌読者・サイト閲覧者への本書ご紹介を是非ご検討いただきたくお願い申し上げます。

サーバーへの不正侵入! 迅速に対応できますか?

情報システム/ネットワークをセキュア(安全)に運用することは企業の責務

企業・組織が社会に貢献し、健全に運営されるためには、所有・提供する情報システム/ネットワークがセキュアに運用されることがその企業・組織の責務です。

インシデントを未然に防止するための、あるいは被害を早期に検知して影響を局限化するためのインシデントマネジメントの重要性とその具体的項目、手順を伝授します。

問題形式で具体的な対策法を身につける

第1章では架空企業で起きるインシデントを時間軸に沿って問題/解答方式で解説しました。ただ読むだけでなく自分で対策を考えることで、実践的スキルを体得することができます。インシデントに対する1つひとつのアクションの選択が、新たなインシデントを発見できる場合もあれば、逆に新たなインシデントを発生させるきっかけにもなるという例も、解説から読み取ることができます。

事前に準備できるセキュリティ対策もある

第2章では対策ミーティングの召集と連絡体制、アウトソースしている会社への対応、証拠保全とログファイルの精査の仕方など、インシデントが起こってから具体的なセキュリティ対策のポイントを確認します。対策マニュアルの作成や連絡フローは事前に用意できます。また、インシデントの兆候を解説することで、未然に防ぐための運用体制の構築法も身につけることができます。

本書概要



書名: 事例で学ぶセキュリティ運用技術・インシデント対応技術

著者: NTT 情報流通プラットフォーム研究所

判型・ページ数: B5判、144ページ

定価: 2,520円(税込)

ISBN: 4-7561-4764-X

発行・発売: 株式会社アスキー

『NTT R&D 情報セキュリティシリーズ』は、セキュリティやEコマースなどの情報流通基盤の研究開発を行っている「NTT 情報流通プラットフォーム研究所」の研究成果である、NTTグループ内で使われるセキュリティ人材育成のテキストをもとに作成しました。既刊に『事例で学ぶ OS・アプリケーションセキュリティ』、『最新 暗号技術』があります。

目次

第1章 事例研究

前提条件/ 主な登場人物

事例1 インシデント発生

事件発生;2003年8月19日0:52 現地調査;2003年8月19日1:47 一時対応;2003年8月19日2:12 対策チームの解散;2003年8月19日2:37

事例2 対応組織の編成

コールセンタの混乱;2003年8月19日9:00 原因調査1;2003年8月19日9:45 連絡体制構築;2003年8月19日9:55 NOCからのメール;2003年8月19日10:00 対策ミーティング;2003年8月19日10:30 構築業者の告発;2003年8月19日12:05 告発の内容;2003年8月19日13:00 原因調査2;2003年8月19日13:00 業者への措置;2003年8月19日14:12 暫定対処;2003年8月19日15:00

事例3 実環境での調査

IRTへの移行準備;2003年8月20日13:00 攻撃兆候に対する調査;2003年8月21日9:30 証拠保全としてのイメージの複製;2003年8月22日9:30 システムファイルの精査;2003年8月22日13:00 ユーザの挙動調査;2003年8月22日19:00 ログファイルの精査;2003年8月23日9:30 不審なファイルの検索;2003年8月25日9:30 インシデント報告会議;2003年8月30日10:30 教訓一覧

第2章 運用技術と知識

技術 Topic1 組織的対応の必要性

組織的対応の必要性/ インシデント対応の種類/ インシデント対応手順/ 組織内での対応/ 事後のための事前準備/ 関係組織への連絡について

技術 Topic2 インシデントを発見するために必要な準備

ログの取扱い/ システムで使用するファイル・コマンドの完全性

技術 Topic3 システム改ざんの痕跡とその発見方法

不審なファイルの設置/ ファイル属性の変更/ 設定変更

技術 Topic4 ログイン情報の改ざん

侵入者の確認(last および who コマンド)/ ログの改ざん

コラム1 Nimda の事例

コラム2 Forensics ツールを利用した保全

コラム3 Computer Forensics の法的側面

コラム4 個人情報漏えい

コラム5 セキュリティ関連情報の収集について

コラム6 ネットワーク監査手順(Nessus 操作手順)

Nessus の構成 ターゲットの指定 スキャン結果の保存

検査前の準備 検査スタート 事前準備

監査項目の選択 スキャン結果の確認 解析時の注意点

コラム7 ファイアウォールログの解析ポイント