

【テーマ】

～もはや防御は不可能～

講師が目の当たりにした事故から分かる問題と
インシデント対応に必要な対策とは？

【講師】

株式会社神戸デジタル・ラボ

取締役 セキュリティソリューション事業部長

兵庫県警サイバーセキュリティ対策アドバイザー

三木 剛

【講義内容】

1. インターネットの歴史
2. 日本を取り巻く脅威
3. 直近ニュースとなったインシデント
4. 私が目の当たりにした事件
5. 脅威≠リスク
6. セキュリティ対策の全容
7. リスク分析による優先順位
8. 喫緊の課題（体制と教育）
9. メール訓練のススメ
10. サイバーセキュリティ経営ガイドライン

～もはや防御は不可能～
講師が目の当たりにした事故から分かる問題と
インシデント対応に必要な対策とは？

(株) 神戸デジタル・ラボ

取締役 サービス推進本部長

(兼) セキュリティソリューション事業部長

三木 剛

兵庫県警サイバーセキュリティ対策アドバイザー

を取り巻く脅威

サイト改ざん

不正アクセス

不正送金

負荷攻撃

標的型攻撃

攻撃手法が多様化しており、企業、個人として
どこまで対策すべきか頭を抱えている・・・

% of Attacks

Applications

95%

5%

NIST

% of Dollars

10%

90%

インシデントレスポンス体制構築のステップ

体制構築に必要な 4 ステップ

STEP4 専門チーム(CSIRT)の構築

STEP3 情報セキュリティ委員会の設置

STEP2 インシデント対応訓練

STEP1 インシデント対応マニュアルの作成

CSIRT ... Computer Security Incident Response Team
コンピュータ・セキュリティに関する事故が発生した場合に、実際に対応に当たるチーム
外部組織との連携を行うこともある