IP Meeting 2015
IW2015セッション総括！
「セキュリティ」

2015/11/20

JPCERT/CC 分析センター
中津留 勇

「セキュリティ」

攻撃とその対策を知る

- 標的型攻撃の現状と対策 2015 ～知らなかったでは済まされない。～
- あなたの身近で起きているサイバー攻撃 2015

インシデント対応体制を整備する

- 150分で分かるセキュリティ対応できる組織にする10のコツ
- CSIRT時代のSOCとのつき合い方 2015
- インシデントに備えて ～上手なログの扱い方～

経営者とセキュリティ技術者をつなぐ

- 企業経営のためのセキュリティ ～基礎と勘所～

暗号化の未来

- SSL/TLSはどうなっていくのか

攻撃とその対策を知る

標的型攻撃の現状と対策 2015 ～知らなかったでは済まされない。～

- Emdivi にかかわる一連の攻撃活動
- 完全な防御は不可能という前提にたった対策が必要
  - 侵入後の攻撃者の行動、JPCERT/CC からの連絡

あなたの身近で起きているサイバー攻撃 2015

- ハクティビズム、ランサムウェア、Webサーバの脆弱性
- 悪意のある広告、スマホアプリ、SNS スパム、ばらまき型
- 明日からはじめる対策の第一歩

インシデント対応体制を整備する

150分で分かるセキュリティ対応できる組織にする10のコツ

- Ten Strategies for Becoming a World-Class CSOC
  http://www.mitre.org/node/21436
- SOC を活用できなかった例

CSIRT時代のSOCとのつき合い方 2015

- 外部　SOC、自社 SOC、SIEM それぞれのカバー範囲
- 正しく付き合う、アウトソースの判断の重要性

インシデントに備えて ～上手なログの扱い方～

- 昨年はデータ保全、今年はログ

経営と SSL/TLS

企業経営のためのセキュリティ ～基礎と勘所～

- 経営者のための情報
  - サイバー攻撃全般、マイナンバー
- 経営者と話す人、経営に関わるようになってきた技術者

SSL/TLSはどうなっていくのか

- SSL/TLS の昨今
  - Let’s Encrypt ベータテスト中
- HTTP/2, QUIC, TLS 1.3

今年の「セキュリティ」セッション

サイバー攻撃対応熱

その裏？で進む大きな変化

来年もお楽しみに！