A-4
「標的型攻撃への
セキュリティ対策」

文京学院短期大学
浜　正樹

標的型攻撃に対する
セキュリティ対策

方法論 [1]

1. 準備
2. 標的型攻撃の検出
3. 初期対応
4. 対応戦略の策定
5. 被害システムの複製
6. 被害・痕跡調査

方法論 [2]

7. セキュリティ対策の実施
8. ネットワーク監視
9. 復旧
10. 報告書の作成

セキュリティ対策の実装

応急措置

- C&Cサーバへの通信遮断
- パスワードの変更
- 被害PCの隔離

事後対策

- ネットワーク設計の改善
- ログ取得設定の改善
- Pass the Hash 対策
- ドメイン管理者利用時のアラート
- 利用ソフトウェアの検討