情報セキュリティ心理学

1．はじめに
- 人を騙すことは、神話の時代からあり、必ずしも悪いことではなかった
- 情報セキュリティ分野では、1987 年 12 月に BITNET でクリスマスツリーを表示するトロイの木馬が出現し、全登録メールアドレスに送付したため、ネットワークが混乱
- サイバー攻撃では利用者権限を盗取できれば、ネットワークに正規権限でアクセスできる

2．セキュリティインシデントの実態

2.1 調査等からみるインシデントの実態
- Verizon Business 調査：　97%は中程度以下の管理で防御可能。2001 年の米国 DoD 調査も同じ
- 防御の仕組みに問題？　高度な攻撃は少ない

2.2 インシデントに対するマスコミ報道の特徴
- 発生確率、重要度とは必ずしも一致しない
- 2009 年 新型インフルエンザ騒動が典型

2.3 高度なサイバー攻撃はないのか？
- Stuxnet 等の高度なものは勿論存在する

3．ソーシャルエンジニアリングとは？

3.1 ソーシャルエンジニアリングの特徴と種類

3.2 ソーシャルエンジニアのバイブル
- R.B.チャルディーニ「影響力の武器」 人間の６つの脆弱性

3.3 ソーシャルエンジニアの実例

4．セキュリティ分野への心理学の適用

4.1 安全・安心／信頼について
- 安全で安心、・・・　危険であり不安を感じる

4.2 内部犯行者の分析
- CMU MERIT ⇒ Insider Threat

4.3 セキュリティ教育への心理学の援用

4.3.1 集合教育

4.3.2 集合・業務連携教育

4.3.3 利用者への模擬訓練・教育

4.4 ソーシャルエンジニアリングへの総合的対応
- Purdue 大学 CERIAS の机上研究
- 名古屋大・富士通の振り込め詐欺実証実験

5．終わりに