サイバーセキュリティ概論

林隆史
新潟大学工学部情報工学科
会津大学

全体安全と結果安全

ポリシー

プロジェクトマネジメントと課題管理

ライブラリとプロトコル

ネットワークとソフト

変化への対応

サイバーテロ

サイバー演習

情報共有

人手不足

情報セキュリティの全体安全と結果安全

- 弱点があれば、そこからアタック（可用性、完全性、気密性などの毀損）
- どこにも弱点をつくらないことが理想
- 方法はどうであれ、結果が大事
- 多面的アプローチが必要

ポリシー

セキュリティポリシー

- 何を守るべきかを明確化
- 優先順位を明確
- 判断基準

個別のポリシー

- より上位のポリシーを具体化
- 手順とは違う

ポリシーの変更

- 要注意

ポリシーの変更

ポリシーの緩和

- 「これくらい」が危険
- ポリシーのベースとなっている考え方が大事
- ポリシーの根拠も可能なかぎり文書化
- 悪影響はすぐには出ない　から　こわい

ポリシーの強化

- 安全になったという誤解を与えないことが大事
- 例外が問題
- 例外は列挙して明示

変更理由と変更前

- 変更理由は明示
- 変更前のものは消さずに残す（消し線など）

ポリシー、PDCA、マイルストン、PM

- ポリシーは必要に応じて変える
- スタンダードは変わる
- PDCAは、ただまわしても無意味
- いつまでに何をどうして行うのか
- PDCAで積み残したものの課題管理
- マイルストン未達成課題の管理
- プロジェクトマネジメント
  - セキュリティで最重要
  - システムの設計・構築でも最重要

プロジェクトマネジメントと課題管理

プロジェクトマネジメントは重要
- マイルストン
- PDCA
- 課題管理

保留課題は保留であって消滅課題ではない

課題管理は重要
- 課題管理の

解決した課題を課題管理表から消してはいけない
- 履歴
- どういう内容で「終結」させたか

過去の課題管理は有用

終結課題

いつでも参照できるようにしておく

再燃することがある

類似の問題への対応

対応方法に問題があったことがわかることもある

- Malicious patch

ライブラリとプロトコル

古いものは問題がある

- メンテナンス
- 脆弱性への非対応
- 残存バグ
- 作られたときの暗黙知はもはや有効ではない

新旧バージョン

- 利用側（呼び出し側）と被利用側のずれ
- 一つのアプリケーションで新旧を利用していることも
  - 関数Aは新バージョン、関数Bは旧バージョン（それぞれ別ライブラリ）

残存バグ

それ自体は脆弱性要因にならなくても、他との組み合わせで脆弱性の原因となる可能性

新たな別の問題の原因となることがある

セキュリティパッチとの組み合わせで問題となる可能性も

ライブラリとプロトコル

膨大な数

古いものを新しいもので置き換えることが必要

Global Environment for Network Innovations のような取り組みが必要

ネットワークとソフトを一体で考えることが必要

ネットワークとソフト

別々に考えていてはセキュリティは確保できない

ネットワークとソフトを合わせてセキュリティ対策

無駄な伝送、無駄な処理、無駄なコピーの削減

疎結合によるセキュリティ向上

- 可用性
- 機密性
- 完全性

変化への対応

- システムもネットワークもソフトも変わる
- SKYPEはもはやIP電話ではない
- メールの送信者認証
- 認証基盤
- Sendmail の終了
- Delegateは？

サイバーテロ

- 一般生活に関わる部分への対応が必要
- 従来のテロ対策は管理下にあるシステム
- Advanced Persistent Threat の標的は特別な対象とは限らない
- 防御は困難だが必要
- 代替できるか？

サイバー演習

避難訓練

- 判断、行動の再確認
- 想定外の確認、課題抽出

実際に起きたときに、慌てたり興奮しないようにできるか

防災訓練との相違点

- 五感で感じ取りにくい
- 人為的な被害なので、対策の裏をかかれる可能性がある

想定外(?)

- ネットワーク切断したとたんにファイル消去
- 探知作業を検知した動作
- テキスト＋インタプリタ
- パッチ
- BIOS
- ブート領域

情報共有

様々なシステム

オフラインになった状態

IPAの「新たな情報セキュリティ早期警戒パートナーシップの 基本構想」 2016.3

SAMACソフトウェア辞書とJVN iPeida連携　2016.4

情報を知ってから対策までの時間

対策もれ

- Openssl Heartbleedのあとの秘密鍵

人手不足

- 技術者の偏在
- 情報の偏在
- 人がいなくても守らないといけない
- どうすればいいのか

最後に

- やるべきとわかっていることは多い
- やるべきとわかっていないこともあるが、わかっていないことばかりよりはずっと良い
- 一つずつ進めていく
- 個々ではできないとあきらめない