Internet Week 2016
T7 プロが厳選！低予算でもできる効果あるセキュリティ施策

できるところから始める運用の備え

CSIRT研究家　山賀正人

山賀正人（やまが まさひと）

- CSIRT研究家
- フリーライター/コンサルタント
  - INTERNET Watch連載「海の向こうの“セキュリティ”」
- JPCERT/CC専門委員
- 日本シーサート協議会専門委員

- 略歴
  - 1994年から2001年まで千葉大学助手
  - 2001年から2006年までJPCERT/CCに勤務

はじめに

- 防御技術が進歩しても、攻撃者側が有利な状況は変わらない。
- 本気の攻撃者に狙われたら防ぎようがない。

- が、攻撃の多くは通りすがりの空き巣狙いなので、防ごうと思えば防げる。

- 防げるものは防ぎ、破られた場合には速やかに対応できるように!!

0. できるところから始めよう

「隗（かい）より始めよ」

《中国の戦国時代、郭隗(かくかい)が燕(えん)の昭王に賢者の求め方を問われて、賢者を招きたければ、まず凡庸な私を重く用いよ、そうすれば自分よりすぐれた人物が自然に集まってくる、と答えたという「戦国策」燕策の故事から》大事業をするには、まず身近なことから始めよ。また、物事は言い出した者から始めよということ。

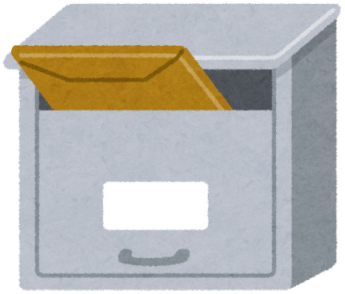
コトバンク「デジタル大辞泉」より

1. 外部からの通報窓口と社内連絡体制

- 深刻なインシデントの多くは外部からの通報により認知

[やるべきこと]
- 外部に公開しているメールアドレス、電話番号などの確認
- 意思決定者（経営層など）へのエスカレーションパスの確認
- 連絡体制が有効であるかを定期的に確認

など



（参考）セキュリティ関連の連絡先メールアドレス

- CSIRTコミュニティのメンバー一覧に掲載されている連絡先
  - FIRST https://www.first.org/members/teams
  - NCA　http://www.nca.gr.jp/member/
- whoisデータベースに登録された連絡先
- postmaster@ドメイン名
- RFC2142で紹介されているメールアドレス
  - abuse@ドメイン名、noc@ドメイン名、security@ドメイン名など
- root@ドメイン名、Administrator@ドメイン名など
- DNSのSOAレコードに登録されたメールアドレス

2. 濃淡をつける

- 「理想」を追い求めてもきりがない
  - 限られたリソース（予算、人手など）の中で、どこまでなら許容できるか
  - 許容したことによるリスクとその対策を考える

[やるべきこと]

例えば

- 機器ごとに調査分析（フォレンジクスなど）を優先するか復旧を優先するかをあらかじめ決めておく

3. 指差確認

- 多くのインシデントは「初歩的なミス」が原因

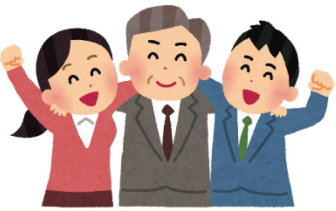
[やるべきこと]

- セキュリティ対策用の設備や機能が想定通りに動作しているかを確認
  - 設計通りに動いているか
  - マニュアル通りに運用されているか（そもそも運用可能なマニュアルか）
  - ログは確認しているか

  など
- 管理から漏れている機器やネットワークがないかを確認
  - 歴史的経緯で（なぜか）残っている機器やネットワーク
  - テスト用に立てられたまま放置されたサーバ
  - 勝手に立てられた無線LANのアクセスポイント
  - いわゆる「シャドーIT」など

4. 社内における信頼関係の構築

- いざという時のスムースな連携のためには信頼関係が必須
- 社内に敵を作ってはいけない



[やるべきこと]

- 経営層を含む関係者や関係部署との日常的な情報共有（定期的な会合など）
  - 平常時の活動の「見える化」にもつながる
- 「正直な報告」を促す空気の醸成
  - 失敗を正直に報告した者を褒める
  - いわゆる「標的型攻撃訓練」は開封率を見るのではなく、開封した者がルール通りに報告するか否かを見るべき

  など

5. コミュニティの力を借りる

- 適切な情報交換・情報共有
  経済産業省「サイバーセキュリティ経営ガイドライン」指示8参照
- 自組織単独では対応しきれないインシデント
  - 詳細な情報が公になりにくい標的型攻撃
  - リスト型攻撃

  など

[やるべきこと]

- 様々なセキュリティ関連コミュニティに積極的に加わり、様々な方たちとの意見交換を通じて信頼関係を構築し、日常的に情報交換するとともに、いざというときには相談相手になってもらえるように

コミュニティに参画する上での注意事項

- コミュニティとは他組織との信頼関係を構築するための「出会いの場」
- コミュニティを通じて「世の中」を良くすることが自組織のセキュリティ向上につながるという意識が必要

6. 訓練・演習

- 普段やってないことはいざという時にできるわけがない
- マニュアルの有効性の確認にも

[やるべきこと]

- まずは日常的に起きうる比較的軽微なインシデントへの対応訓練を重ねる
  - 広く使われているソフトウェアの脆弱性情報公開時の対応
  - 管理外の無線LANアクセスポイント発見時の対応

  など

まとめ

1. 外部からの連絡窓口と社内連絡体制
2. 濃淡をつける
3. 指差確認
4. 社内における信頼関係の構築
5. コミュニティの力を借りる
6. 訓練・演習

ご清聴ありがとうございました。

参考資料

- オープンガバメント・コンソーシアム「組織対応力ベンチマーク」
  https://ogc.or.jp/article/1525

  - 米国国立標準技術研究所(NIST)の定めたセキュリティインシデント対応ガイドライン「NIST SP800-61」をベースにしたチェックリスト
  - 現状把握と今後の改善に