

6学期講義

Network Security Introduction

総合情報学科

ISMSによる対策(5) - Do編

- 導入Phase
 - セキュリティシステムの導入/構築
 - 適切な設定 (default設定の変更、不要service停止)
 - 脆弱性の解消 (修正patch, updateの適用)
 - 必要に応じたアクセス制御
- 運用Phase
 - Security Policyの周知徹底とセキュリティ教育
 - 脆弱性対策 (最新情報の収集とupdateの適用)
 - 異動/退社社員のフォロー (権限の見直し、削除)

Default設定は危険

- 初期設定は (悪意ある人達に) 広く知られている
 - 例) 管理画面/管理ツールへの初期 ID & Password
- 購入時の設定を変更せずに利用するのは危険
 - 「変更しなければ機器が使用不可」とすべきだが...
- Internet上に接続されたNetwork機器を探す手段なんてない？
 - 実は広く出回っている... (警告目的、悪意の情報共有?!)
 - 検索エンジン：SHODAN

Default設定は危険



Give me your
default passwords.


Right now.

twitter

**Default Pass DBさんからの、短くてタ
を受信しましょう!**

Twitterは豊富なリアルタイム情報の宝庫です。Twitter
題の情報が飛び交っています。今すぐ参加して@pass

登録する>

 SMS で更新を受け取るためには、あなたの地域でのロー



@passdb

passdb

EPiServer AB EPiServer Commerce:
admin/store
<http://tinyurl.com/4bmjboh>
#password

検索エンジン SHODAN

- SHODAN - Computer Search Engine
- Google等と何が違う？
 - Googleは「Webページ」が対象
 - SHODANは「IT機器のBanner(バナー)」を対象
- Bannerとは?
 - 見出し、垂れ幕、軍旗など



何が得られる

- サーバのBannerから機器情報を取得
⇒ IP camera, FAX(複合機), インフラ制御システムなど
- 集約して、検索可能に

Shodan Exploits Scanhub Maps Blog Membership Register Login

SHODAN Search

EXPOSE ONLINE DEVICES.

WEBCAMS. ROUTERS.
POWER PLANTS. IPHONES. WIND TURBINES.
REFRIGERATORS. VOIP PHONES.

TAKE A TOUR FREE SIGN UP

Popular Search Queries: **default password** - Finds results with "default password" in the banner; the named defaults might work!

DEVELOPER API 105 LEARN MORE FOLLOW ME

SHODAN記事

- Googleでは分からないインターネット裏情報を引き出す「SHODAN」
<http://ascii.jp/elem/000/000/779/779119/>
- 複合機や家電の不要な公開サーバーは「SHODAN」で発見を、IPAが利用法を指南
http://internet.watch.impress.co.jp/docs/news/20140228_637532.html
- 検索サービスSHODANを使うと何が見えるのか？
<http://itpro.nikkeibp.co.jp/article/COLUMN/20140610/562887/>

何ができる

- とある機器のBannerを調べる
 - 対象機器の機種名とメーカーが判明
 - メーカー/機種名 ⇒ Default passwordを得る
⇒ 同一機器を購入すれば誰でも知ることができる
- SHODANでnetに接続されている当該機器を検索
 - Default passwordで不正アクセス！
 - Default passwordのままだと、不正侵入できてしまう！

恐れられている

- インフラの攻撃に使われる懸念ありと警告
- SCADA: Supervisory Control and Data Acquisition
 - 産業用制御システムの一つ
 - 上下水道、石油/ガスのパイプライン、送電/通信網など
- 一部のシステムは検索できてしまう...
 - 攻撃者によるインフラ攻撃を支援することに

ISMSによる対策(6) - Check編

- 監視と評価
 - 異常検知、不正アクセス検知
 - 脆弱性検査 / 監査
- Policy遵守に関する自己点検
 - 情報セキュリティ対策Benchmarkによる自己診断
 - IPA: 組織の情報セキュリティ対策自己診断テスト
<http://www.ipa.go.jp/security/benchmark/>
- 情報セキュリティに関する第三者監査

ISMSによる対策(7) - Check編

- セキュリティ事故への対応 = インシデントレスポンス (Incident Response)
- **緊急時対応計画**を策定、これを基に適切に対応
- 注意点
 - 被害状況と被害範囲の調査、二次災害防止の対策
 - 原因特定、再発防止策の策定
 - 対応内容を時系列に記録、報告書とする。
必要があれば公的機関等への各種届出を
 - 必要なら対応窓口を設け、正確な情報の提供を実施

ISMSによる対策(8) - Act編

- 事故の発生によって、Security Policy(SP)の不備が見つかる
 - Security Policyの見直し、改善点を検討
- セキュリティ監査 / 評価 ⇒ 結果に基づき、改善提案
 - Security Policy等へfeedback

情報セキュリティ対策 ⇒ 終わりのないプロセス

ISMSのサイクル (技術的対策 + 組織/運用管理対策)の

継続実施が重要

利用者の心得

規則を知り、それを遵守する

- 情報セキュリティ上の脅威とその対策を知る
⇒ ニュース等で日頃情報収集するのは重要
- 「自分は大丈夫...」 「これぐらいは...」 は通用しない
- Securityは最も脆弱な部分からほころびる
 - 自分が最弱点(ほころび)にならないよう努力する

Weakest link

The chain is no stronger than its weakest link.

その鎖の強さは、最も弱い環によって決まる。



One of Principles for Security

引用: <http://mgmt600.wordpress.com/2010/10/07/the-weakest-link/>

<http://theindependent.sg/blog/2013/08/08/free-speech-is-only-as-strong-as-your-weakest-link/>

利用者の心得

規則(ポリシー)は万能ではない！

- 以下の場合、上司やSystem/Network管理者に報告・相談
 - Security Policyで明確なルールがない事例
 - ルールが遵守しにくい場合
- そして「以下の対応」も大切
 - 禁止されていることを“してしまった”場合

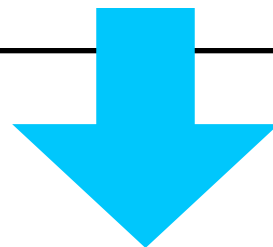
あきらめてはならない！

Securityに
100%はない



攻撃者は最弱点
から忍び寄る

「できること」を
しっかり実施する



多くの不正行為を退けることになる

あきらめてはならない！

「できること」をしっかりと実施する

- Operating SystemのUPDATE (patch 適用)
- Applications / 言語処理系 の UPDATE
- Anti-Virusのパターンfile のUPDATE と Scan実行
- Firewallの利用 (設定)
- Web browserの設定

あきらめてはならない

サイバー・ノーガード戦法

2005年5月26日の記事

>> 某大手サイトの「4つのやりません宣言」 驚天動地の発表

某大手サイトが昨日「4つのやりません」を公言した。

このサイトでは第三者から攻撃を受けて下記のような事態が発生した。

- ・ サイトが改ざんされて、閲覧者にウイルスをばらまく状態になったのを知っていながら数日間放置
- ・ メールアドレスが多数漏洩
- ・ サイト閉鎖、システム入れ替えして再開

今回の事件に対して某大手サイトでは「4つのやりません宣言」を発表した。

- ・ 過失は認めません
- ・ サイトを見てウイルス感染した被害者へは補償しません
- ・ サイトからメールアドレスを漏洩してしまった被害者へは補償しません
- ・ 原因については公表しません

引用: <http://scan.netsecurity.ne.jp/article/2005/05/26/15940.html>

あきらめてはならない サイバー・ノーガード戦法

2005年5月26日の記事

これは今回のことだけでなく、将来に向けても同様のことを公言したようなものである。

- ・ 第三者から攻撃を受けて問題がおきても自社の過失は認めません
- ・ サイト利用者に被害が発生しても補償しません
- ・ メールアドレスを含むサイト利用者情報が漏洩しても補償しません
漏洩した情報はなんであっても個人情報ではないと言い張ります

しかもその理由が「当社は被害者だから」というのは開いた口がふさがらない。

我々は被害者であり悪くない、悪いのは攻撃者！

漏えいさせてしまった企業も十分な対策を
行っていなかったという点では**加害者**

引用: <http://scan.netsecurity.ne.jp/article/2005/05/26/15940.html>

サイバークロスカウンター

6ヶ条の対応

1. 「適切」なセキュリティ対策を実施。

某大手サイトは自社のセキュリティ対策を「適切」と表現していた。どのようなものが「適切」なのかは筆者の理解の範疇ではないが、結果論からいうと少なくとも第三者に悪意ある行動を許容するおおらかさをもったセキュリティ水準ということなのであろう。

2. 攻撃を受けたら被害防止よりも犯人特定を優先した行動をとる。

情報が漏洩してもそれは個人情報ではないと言い張る立場をより明確にする。

3. IPAと警察に連絡して「被害者」という立場を明確にする。

4. 「4つのやりません宣言」を発表し、なにもなかったようにサービスを再開する。

5. 犯人を捕まえられなくても批難を受けないように、セキュリティ業界の有名人に協力を要請する。

6. 数ヶ月たってほとぼりがさめたら、完全になにもなかったことにする。

セキュリティ業界の有名人には謝礼を払うが、「最高」のセキュリティ対策を構築、維持する費用に比べたら格安である。

信用消失は損害ではない

理由：**Priceless**だから...

引用: <http://scan.netsecurity.ne.jp/article/2005/05/26/15940.html>

さらに続く心得

1. 所属組織の情報や機器を、許可なく持ち出さない
2. 私物のPCやProgramを、許可なく組織内に持ち込まない
3. 所属組織の情報や機器を、未対策のまま放置しない
4. 所属組織の情報や機器を、未対策のまま廃棄しない
5. 個人に割り当てられた権限を、第三者に貸与/譲渡しない
6. 業務上知り得た情報を公言しない
7. 情報漏えいの可能性がある場合には速やかに関係者に報告

情報セキュリティ対策とは

- 「明確な悪意」または「過失」により発生しうる
“望ましくない行為”に対して、必要な対策を実施すること
- 直接的な保護対象 ⇒ 情報やシステム。
 - ただし、それらを扱うのは人間 ⇒ **人間も対象**
- 今後も「**終わりのない戦い**」が続くことになる
- **システムと利用者そして管理者**の3つのstake holderによる行動が重要で「あった」(過去形)
 - 今日、ICT機器の普及により利用者 = 管理者となりつつある
 - 管理者が行っていたことを、利用者が実施する必要あり

知る・守る・続ける

- 「知る」

- IT Riskなどの情報を冷静に理解し知る

- 「守る」

- 安全にInternetを利用し、情報Security上の脅威から身を守る

- 「続ける」(これが大切)

- 情報セキュリティ対策を情熱を持って続ける



引用: <http://www.nisc.go.jp/security-site/logo.html>

国民を守る情報セキュリティサイト

知る
安心・安全・便利な
インターネット環境を構築するための
ポイントを「知る」こと。

守る
情報セキュリティ上の脅威から、
身を「守る」こと。

続ける
移り変わる情報セキュリティ上の
脅威に対して
対策を「続ける」こと。

情報セキュリティ対策
のエッセンスを端的に
伝えるキャッチフレーズ
「知る・守る・続ける」
をご利用ください。

知る 守る 続ける
情報セキュリティ
対策キャンペーン
— 平成24年10月 —
知る セキュリティ

Web: <http://www.nisc.go.jp/security-site/index.html>

Securityで何か困ったらまず見てほしいWebページ

IPA: 情報処理推進機構

<http://www.ipa.go.jp/security/>

The screenshot shows the IPA website's security section. The header includes the IPA logo and navigation links like 'HOME', '情報セキュリティ', 'ソフトウェア・エンジニアリング', 'IT人材育成', '情報処理技術者試験', '未読', and 'オープンソフトウェア'. The main content area features a 'クイックアクセス' (Quick Access) section with links to various security resources, a '5分でできる!' (Can be done in 5 minutes!) section for security point learning, and a '情報セキュリティ対策' (Security Measures) section with links to various security measures. The footer includes a 'お問い合わせ' (Contact Us) link.

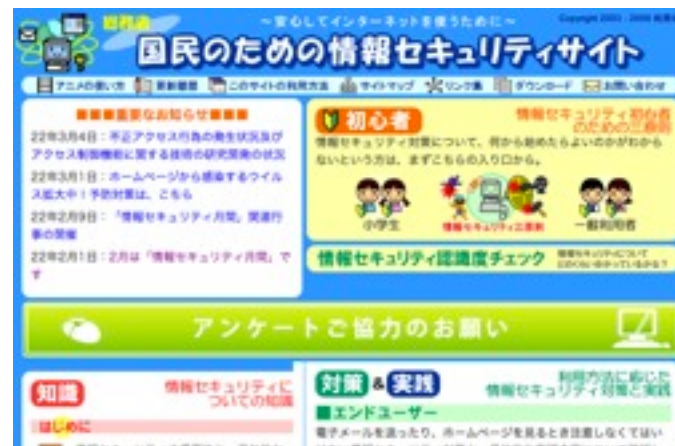
JPCERT/CC

<http://jpcert.jp/>

The screenshot shows the JPCERT/CC website. The header includes the JPCERT/CC logo and the text '安全・安心なIT社会のための、国内・国際連携を支援する' (Supporting domestic and international cooperation for a safe and secure IT society). The main content area features a '注意喚起' (Alert) section with a list of recent security alerts, a '情報提供' (Information Provision) section with links to various security information, and a '脆弱性関連情報' (Vulnerability Related Information) section with links to various vulnerability information. The footer includes a 'お問い合わせ' (Contact Us) link.

日本政府の取り組み

- 内閣官房情報セキュリティセンター (NISC)
 - 国民を守る情報セキュリティサイト - <http://www.nisc.go.jp/security-site/>
- 総務省
 - 国民のための情報セキュリティサイト - http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/
- 経済産業省
 - Check PC! - <http://www.meti.go.jp/policy/netsecurity/checkpc/>



Securinaが消えた

2009年02月12日 12時10分00秒

経済産業省、ニューアイドル「セキュリーナ」を起用してパソコンのセキュリティ対策を呼びかけ



常時接続環境がどんどんと整っていき誰もが簡単にネットに接続できるようになって、コンピュータウイルスや不正アクセス、フィッシング詐欺などに出会う危険性が高くなっています。そんな現状を危惧して、経済産業省がパソコンやモバイルのセキュリティ対策を呼びかけています。キャンペーンに起用されたのはニューアイドルの「セキュリーナ」。最初に見たときは目を疑いましたが、これぐらい目を引けば対策呼びかけにはちょうどいいかもしれません。

Web: http://gigazine.net/news/20090212_securina/

おわり

Network Security Firewall

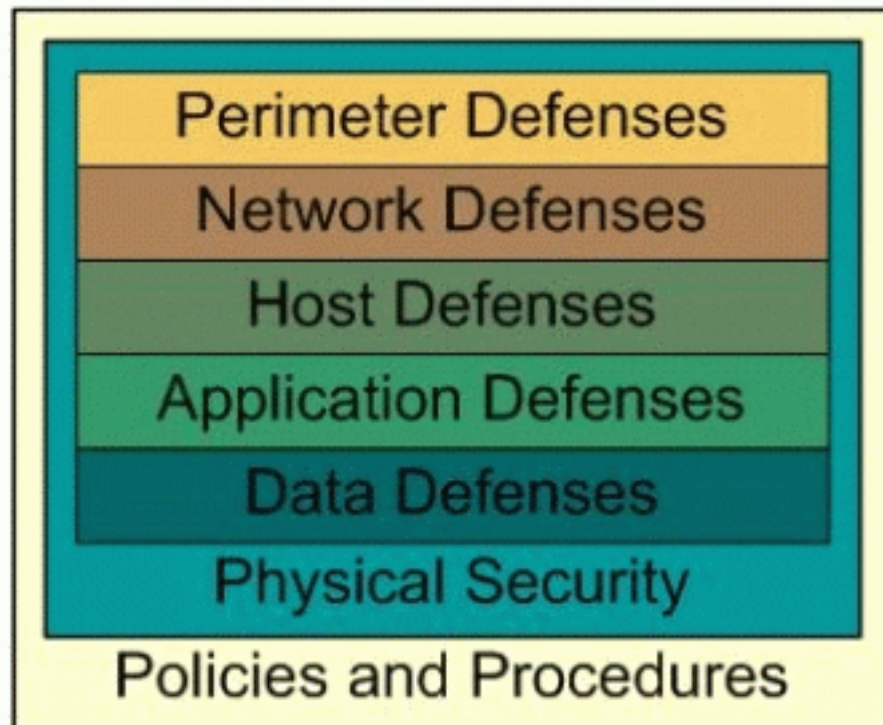
総合情報学科
セキュリティ情報学コース

Firewallは～ではない!

- Crackerの侵入を防ぐものではない
- Virusの感染を防ぐものではない
- インストールさえすればよい. ものではない

Network通信の制御を行うシステム
多層防御(Defense in Depth)における1部品

Defense in Depth



- Physical security
- Access control (biometrics)
- **Firewall** (DMZ, packet filter)
- Virtual Private Network (VPN)
- Authentication (password, PIN, etc...)
- Intrusion Detection System (IDS)
- Anti Virus software
- Logging and Auditing
- Security through obscurity

引用: Microsoft|TechNet, Security Content Overview,
[http://technet.microsoft.com/en-us/library/
cc767969.aspx](http://technet.microsoft.com/en-us/library/cc767969.aspx)

Wikipedia, Defense in depth,
[http://en.wikipedia.org/wiki/
Defense_in_depth_\(computing\)](http://en.wikipedia.org/wiki/Defense_in_depth_(computing))