

6学期講義

Network Security Introduction

総合情報学科


Open Source Vulnerability Database (OSVDB)


- Open source projectとして作成された脆弱性情報DB
- Black Hat & DEFCON conferenceで構想発表
- 2004年3/31に公開
- Twitterでも情報公開 (<http://twitter.com/OSVDB>)

OSVDB	Search OSVDB	Browse	Vendors	Project Info	Help OSVDB!	Sponsors	Account	Download DB
--------------	------------------------------	------------------------	-------------------------	------------------------------	-----------------------------	--------------------------	-------------------------	-----------------------------

The Open Source Vulnerability Database

OSVDB is an independent and open source database created by and for the community.
Our goal is to provide accurate, detailed, current, and unbiased technical information.
The database currently covers **70,234** vulnerabilities, spanning **31,811** products from **4,735** researchers, over **46** years.

Latest OSVDB Vulnerabilities 		
71283	Disclosed: 2011-03-24	Group-Office Admin User Creation CSRF
71282	Disclosed: 2011-03-24	Avaya IP Office Manager TFTP Request Handling DoS

Sponsors
 **LAYERED[®]**
TECHNOLOGIES

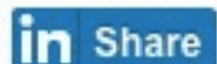
Will not return

Home > Vulnerabilities



OSVDB Shut Down Permanently

By [Eduard Kovacs](#) on April 07, 2016



56



5



The maintainers of the Open Sourced Vulnerability Database (OSVDB) announced this week that the project will be shut down permanently due to the lack of support from the industry.

“As of today, a decision has been made to shut down the Open Sourced Vulnerability Database (OSVDB), and will not return. We are not looking for anyone to offer assistance at this point, and it will not be resurrected in its previous form,” Brian Martin, aka Jericho, one of the leaders of the OSVDB project, said in a [blog post](#).

“This was not an easy decision, and several of us struggled for well over ten years trying to make it work at great personal expense. The industry simply did not want to contribute and support such an effort,” Martin added.

OSVDB

Everything is Vulnerable

脆弱性探索(Exploit)行為 (1/2)

- 脆弱性を探す行為
 - 誰がする？
⇒ セキュリティ専門家(White hat) or 攻撃者(Black hat)
- その際の成果物 ⇒ “Exploit code”
 - 脆弱性の存在を証明、悪用可能にするProgram
 - **利点:** 脆弱性の危険度や影響範囲を検証可能に
⇒ 脆弱性の修正に不可欠
 - **問題点:** 悪用の懸念
⇒ Malware, 攻撃ツールの「部品」となる

悪用事例: Hotfix report, エクスプロイト・コード,
<http://www.hotfix.jp/archives/word/2003/word03-13.html>

公開のジレンマ

- Mailing listや掲示板で“Exploit code”を公開
- その是非について議論がある
 - 利点 (white hat目線)
様々な環境での脆弱性検証 (影響範囲の特定)
 - 問題点 (black hat目線)
Code公開 ⇒ Codeを改変、攻撃ツールを作成
 - 攻撃Code公開 ⇒ 脆弱性悪用攻撃を誘発、拡散
- 良心に基づく行為が、攻撃ツールを生むというジレンマ
- しかし、攻撃ツールはいずれ出回る。なので利点をとるべき、
という意見

脆弱性届出制度

- Exploit codeの公開について
 - 基本：当事者間以外には非公開にすべき
 - 個人がメーカに脆弱性を報告してもメーカが対応しない場合がある
そこで当該脆弱性の危険性を証明するexploit codeを公開し、
修正対応を迫るということが行われていた (対応への圧力をかける)
- 脆弱性届出制度
 - 公的機関が脆弱性情報を受け付け、メーカと対応を協議、
また適切なタイミングで脆弱性情報を公開するといった仕組み
 - 危険を伴うような脆弱性情報の公開を防ぎたい
 - 受付機関: IPA、調整機関 JPCERT/CC
 - メーカが対応しなくても調整開始から45日以内に脆弱性情報は公開

ソフトウェア脆弱性届出制度、2004年7月8日から運用開始, 45日以内の公表に,
<http://journal.mycom.co.jp/news/2004/07/07/004.html>

ゼロデイ攻撃 (Zero day attack)

- 一般に広く知られていない脆弱性、または対策用patchが公開されていない脆弱性を突いた(狙った)攻撃
- Zero-dayとは、脆弱性への対策(patch, new versionのsoftware)が公開された日を1st dayとし「それ以前」の状態であることを意味する
- つまり「ゼロデイ攻撃 ⇒ 防御が困難な攻撃」
- なぜzero-day (0-day) attackが可能なのか?
 - PoC code or Exploit codeが脆弱性情報公開前に流通 / 漏えい
 - Exploit codeは、undergroundで共有/売買
⇒ Black marketの存在 (Crackerの動機変容)

IPA, 修正プログラム提供前の脆弱性を悪用したゼロデイ攻撃について, (2010/01/22),

<http://www.ipa.go.jp/security/virus/zda.html>

人為的な脆弱性

- 人間は、かならずミスをする
 - 情報漏えい事案の原因の多くは人間
- 攻撃原因の多くは、人間に起因
 - 紛失、盗難
 - P2Pアプリケーションを経由した漏洩
 - 誤公開、誤送信、誤設定
 - 内部犯行 (転/退職者、恨みなど)

ソーシャルエンジニアリング (Social Engineering)

Social Engineering

- 非技術的な方法で機密情報やPasswordを取得
 - 別名: **Human Hacking** (社会的動物である人間を攻略)
 - 「最も安全なComputerは電源を切っているComputerだ」
⇒ だがSocial Engineeringはもっともらしい口実を駆使し、組織内部の誰かを口説き、Computerの電源を入れさせることだってできる！
 - さまざまな事例
 - 例1) 電話での聞き出し (嘘、なりすまし)
 - 例 2) Shoulder hacking / Phishing / fake Anti-Virus software
 - 例3) 社内に来る掃除人、保険販売員、自販機補充者による情報漏洩
 - 例4) Dumpster Diving, Scavenging
 - 例5) Data Salvage

中古HDDは宝の山



- 中古HDD
データが未消去の
まま販売されている
- eBayで販売されてい
るUsed HDDの40%に
個人情報や企業情報
が残っていた

URL: http://www.computerworld.com/s/article/9127717/Survey_40_of_hard_drives_bought_on_eBay_hold_personal_corporate_data?taxonomyId=19&pageNumber=1&taxonomyName=Storage

HDDからのData削除

捨てる前に「データの完全削除」が必要

「ゴミ箱に入れて空にする」では不十分

⇒ 「データ復旧」製品・サービスで復元できてしまう

- 中古HDDからの個人情報漏えいを防ぐ方法 (2009/03/09)
 - http://www.lifehacker.jp/2009/03/post_612.html
- せめて、HDDの最期はこの手で... (2007/11/28)
 - <http://www.atmarkit.co.jp/fsecurity/column/ueno/50.html>

データ完全削除

米国でのデータ消去に関する規格

	書き込みパターン	
NSA推奨方式	乱数2回→ゼロ	3回
米国防総省準拠方式 (DoD5220.22-M)	固定値1→固定値1の補数→乱数→検証	7回
グートマン推奨方式	乱数4回→固定値1→……→固定値27→乱数4回	35回

試しに手元にあったデータ消去ソフトで、「米国防総省規定 (DoD5220.22-M) に従ってデータ領域をすべて7回上書き」というのを実行してみました。

使用したのは、SATA150の300GBのハードディスク。

そして待つこと、**約25時間……**。

参考Web: <http://www.atmarkit.co.jp/ait/articles/0711/28/news141.html>

HDD完全消去option



再利用不可能な形に破壊



73

HDDのデータを瞬時に無効化

HDD内データ無効化技術



そのまま捨ててはいけない

中古で購入したルーターの電源を入れて設定をしようとしたら

```
*****
*1. USERNAME      BANK OF JAPAN
*2. TYPE          Cisco892J
*3. HOSTNAME      [REDACTED]
*4. IOS Ver       15.1.4M1    UNIVERSAL
*5. CONFIGURATON  BRI0:1     Used 64K
*                  To ULTINA BOJ-VPN-N2
*                  FE0 - 7    Used 100Base-TX
*                  To Ethernet LAN
*6. HISTORY       2011, [REDACTED] Initial Configuration
*****

User Access Verification

Password:
Password: _
```

ただし真偽は不明

引用: <http://togetter.com/li/731289>

中古のタブレットから見つかった通信教育利用者の大切な情報 (1/2)

筆者の友人が中古品市場でベネッセが提供していたタブレットを発見した。それを調べてみると、さまざまなデータが残っていたのだ。同社の対応も含めて報告したい。

[萩原栄幸, ITmedia]



PR [国内外のオブジェクトストレージ導入・活用事例が満載](#)

PR [サイボウズがセキュリティ品質向上に報奨金を導入した理由](#)

筆者の友人がリユース・リサイクル市場を調査したところ、「興味深い事実が判明した」と相談をしてきた。友人は国産のスマホやタブレットのデータ消去ソフトの開発を行っている技術者であり、仕事の一環として調べていた時に発見したという。今回はその件について、友人の承諾を得たのでここに報告したい。

見つかった情報

- 使用者の氏名（状況によっては住所）
- 登録したメールアドレスのアカウント、メールの内容
- Facebookの内容
- Google Playの利用内容
- LINEのアカウントを利用していること

おすすめの本

- 欺術 - 史上最強のハッカーが明かす禁断の技法
- 「あざむく術」と書いて「ぎじゅつ」
- ISBN: 479732158X



Social Eng. 一事例

- 標的となる会社にて、外部からアクセス可能なアカウントを作成させる
⇒ あとで不正侵入に利用
- 方法：電話を3回するだけ！

Social Eng.事例 (1/3)

- **取引相手**になりすまし、標的の会社の**受付**に電話
 - 「ジョーンズなんとかさんだっと思います。そちらの会社にいらっしゃるジョーンズさんという名前の方を教えてください。⇒(回答をもらう)
 - あ、S.ジョーンズさんだっと思います。部署はどちらでしたか...あ、そうそう"システム開発部"でした。ありがとうございます」
- 成果：社内的人物のfull-nameと所属情報を取得

Social Eng.事例 (2/3)

- **社内の給与係になりすまし、S.ジョーンズさんに電話**
 - 電話：「私は給与係のものだが、あなたの給与支払いの手続きでミスがあった。社員番号を教えて欲しい」
- 当該社員の社員番号を取得
 - 社内において社員番号は秘密でも何でもないので、あっさり教えてくれる

Social Eng.事例 (3/3)

- **S.ジョーンズ**さんになりすまし、**システム管理者**に電話
 - 「出張中で外から会社アクセスしたいのだが、
臨時にアカウントを作成してくれないか？私の名前は
S.ジョーンズで所属部署は～、社員番号は～だ」
- システム管理者は、当該情報の情報をスラスラと話しているので本人だと勘違いし、アカウントを作成してしまう
- 完成！ 外部から標的の会社アクセス可能に！
⇒ しかも「非技術的な侵入手法」は一切なしで！

悪意による行為とは...

- ノートン(Norton) 【犯罪者N】 No.1,2,3
- <http://www.youtube.com/watch?v=6bQNmd881Vs>
- 【犯罪者N逮捕】 編もある

情報リテラシーと情報倫理

- 情報リテラシー
 - ICT技術を活用する基本的な能力 (作成、整理、検索等)
 - 基本的な情報セキュリティ対策も含まれる
 - 特にWebブラウザ、電子メールソフトのSecurity設定は熟知のこと
- 情報倫理
 - ICT技術の利用において必要とされるモラル/道徳
問題：誹謗中傷、学校裏サイト、他人のプライバシー暴露

知っていますか？

- Twitter ⇒ つぶやき
 - この「名称」が、「事実錯誤」を生んでいる！
 - 実態：世界中の人に対して大声で叫ぶことと同意
- 特徴：急速に拡散 ⇒ “Retweet” という鎖で第三者が情報拡散
- 驚異的な伝搬力。内容次第では “つぶやき” が大勢の声に
 - 第三者のprivate暴露事件 ⇒ 結果 / 考察

- ホテルのアルバイトしていた女性が、Twitterで芸能人や企業社長、政府高官の密会を次々につぶやく
- 友人とうわさ話をする「感覚」だった(事実錯誤)
⇒ あっという間に拡散。世間の注目を浴びる
⇒ Privacy上問題と指摘 ⇒ 炎上、非難の的に
- 2ちゃんねるでバイト先ホテル、女性本人が特定、その後、当該女性の個人情報ネット上でさらされる事態に
- 今も氏名で検索すると、該当Webサイトが閲覧可能な状態
- ホテル支配人は公式に謝罪。女性には厳しい処分を課すと言及。

SNSでやってはならない

- 他者の誹謗中傷・脅迫
⇒ 名誉毀損、殺人予告、ネットストーカー
- 両親や友人に言えないこと
 - バイトテロ：非社会的行動の写真をアップロード
⇒ 慰謝料、刑法に基づく処罰

判断基準

書き込む内容を調布駅前で大きな声で叫べるか？

その後

「バイトテロ、一生許せない」 あのそば店社長からの手紙

バイトの悪ふざけで倒産した多摩市「泰尚」の慟哭

宇賀神 宰司

2013年12月16日（月）

[>>バックナンバー](#)

1/2ページ

 おすすめ  シェア 4,074  共有 50  ブックマーク 497  ツイート 1,996

「バイトテロ」で企業が倒産に追い込まれる事態がついに発生してしまった。

東京都多摩市。東京都下の丘陵地帯に造成された多摩ニュータウンにあるそば屋の「泰尚（たいしょう）」。幹線道路沿いの好立地で営業していたにも関わらず今年8月に閉店。東京地裁に破産を申請して、10月9日に破産手続き決定を受けた。

1000万円超えの損害賠償請求

引用: <http://business.nikkeibp.co.jp/article/opinion/20131213/257028/>

Background check

- SNSは監視対象
⇒ 社員・学生・応募者の素性確認のため
- 差別？
⇒ 区別である

守るべき3つの基本モラル

1. 他人を誹謗中傷しない (他人のことを書かない)
2. 他人のプライバシーを侵害しない
3. 著作権について知り、著作権侵害をしない

著作権

- 以下の表現形式で自らの思想・感情を**創作的**に表現した著作物を**排他的に利用**する権利
 - 言語、音楽、絵画、建築、図形、映画、写真、プログラム
- 権利について
 - 権利発生：作品生成と同時に自然発生
 - 権利消滅：作者の死後 50年後
 - 譲渡 または 利用許諾という形で、他者に作品を利用させることが可能

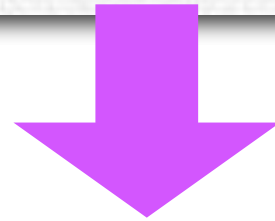
やりがちなこと

- 新聞の切り抜きをWebで公開
- 他者の作品を許可なくWebで公開
- SNSやファイル共有、ファイル交換(P2P)で他者の作品(創作物)を送受信可能な状態にする
- ネット上のイラスト/写真を無断で利用

「利用規約」の確認、必要なら「使用許諾」を

いらすとやに掲載されているイラストは、**無料でご利用いただけますが著作権は放棄しておりません。**
ご利用いただく場合にはご利用規約をご覧の上、不明な点についてはメールにてご連絡下さい。

ご利用規約 | プライバシーポリシー | 免責事項



ご使用規定

当サイトで配布している素材は、個人、法人、商用、非商用問わず無料でご利用頂けます。クレジットの表記、メールでの連絡など必要ありません。詳しくは「[よくあるご質問](#)」をご覧ください。

当サイトのイラストは以下の場合に限って、ご利用をお断りします。

- 公序良俗に反する目的での利用
- 素材のイメージを著しく損なうような利用
- 素材をそのまま再配布・販売
- その他著作者が不適切と判断した場合

以下の場合、有償にて対応させていただきます。メニューの「[お問い合わせ](#)」からご連絡下さい。

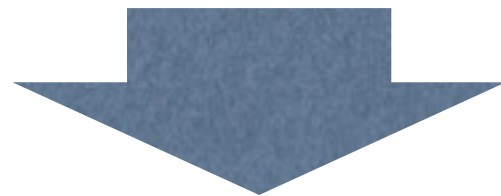
- 素材を20点以上使った商用デザイン
- 素材の高解像度データの作成（[高解像度イラストのサンプル](#)）
- ご希望のイラストを作成
- 素材を商標登録、著作権の買い取り、独占的使用権の買取

参考資料

- コピーライトワールド, (社) 著作権情報センター
 - <http://www.kidscric.com/>
- ZAQセキュリティ情報, インターネットモラル
 - <http://support.zaq.ne.jp/security/moral.html>
- 総務省, インターネットトラブル事例集
 - http://www.soumu.go.jp/main_sosiki/joho_tsusin/kyouiku_joho-ka/jireishu.html
- (社) コンピュータソフトウェア著作権協会(ACCS)
 - <http://www2.accsjp.or.jp/>

Security機能、規則の欠如

- 「守れるルール」の策定と周知/教育
- 組織内部の人間による理解と協力
- 組織トップの積極的な関与とリーダーシップ



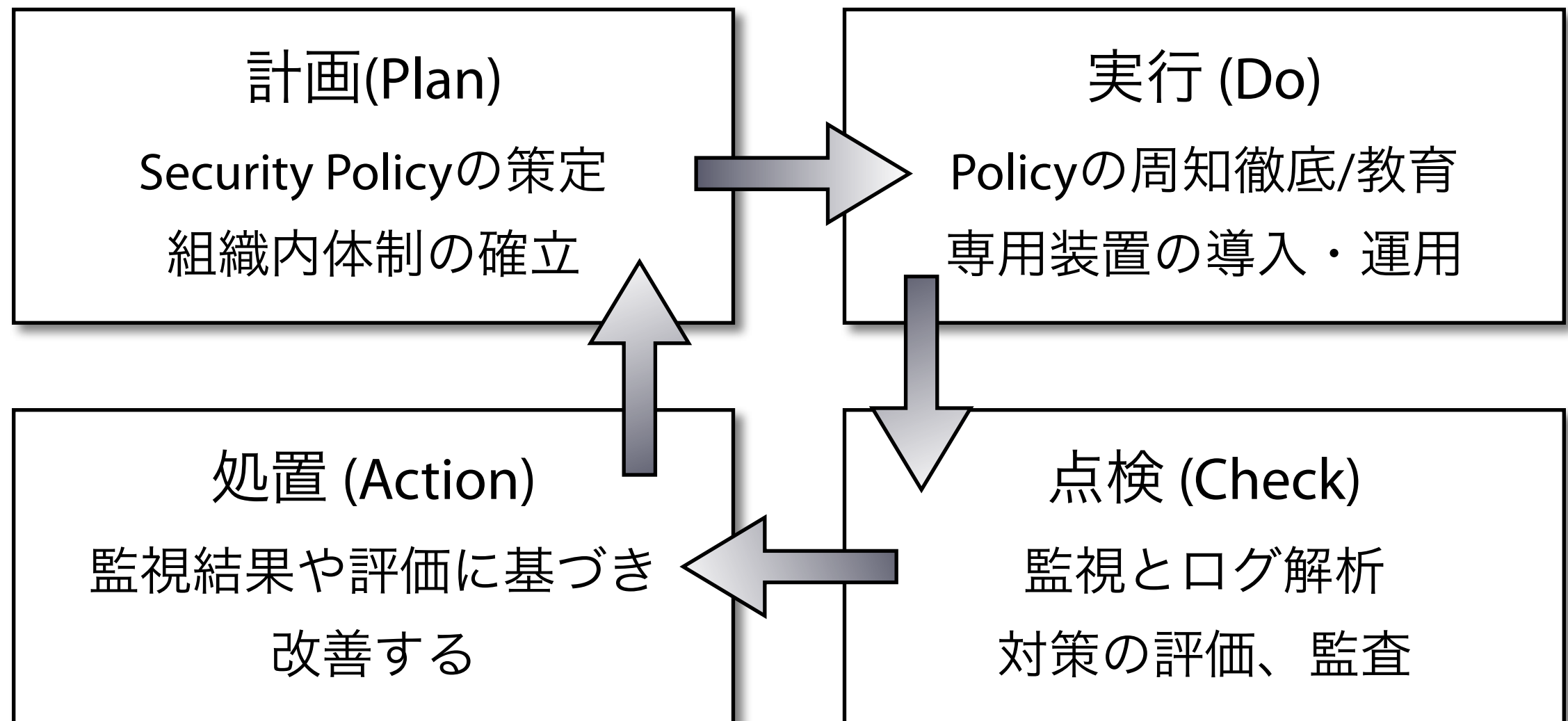
ISMS: Information Security Management System

ISMSによる対策 (1)

- ISMSとは情報セキュリティマネジメントシステム (Information Security Management Systems)
- 情報セキュリティの確保・維持のための体系
 - 技術的、物理的だけでなく、人的、組織的視点
 - PDCAサイクル (Plan, Do, Check, Action)の実施
- 経営層を中心とした組織的体制の確立を目指す
 - 重要な出発点: 「組織のトップが情報セキュリティに取り組む」ということを明確にする

ISMSによる対策 (2)

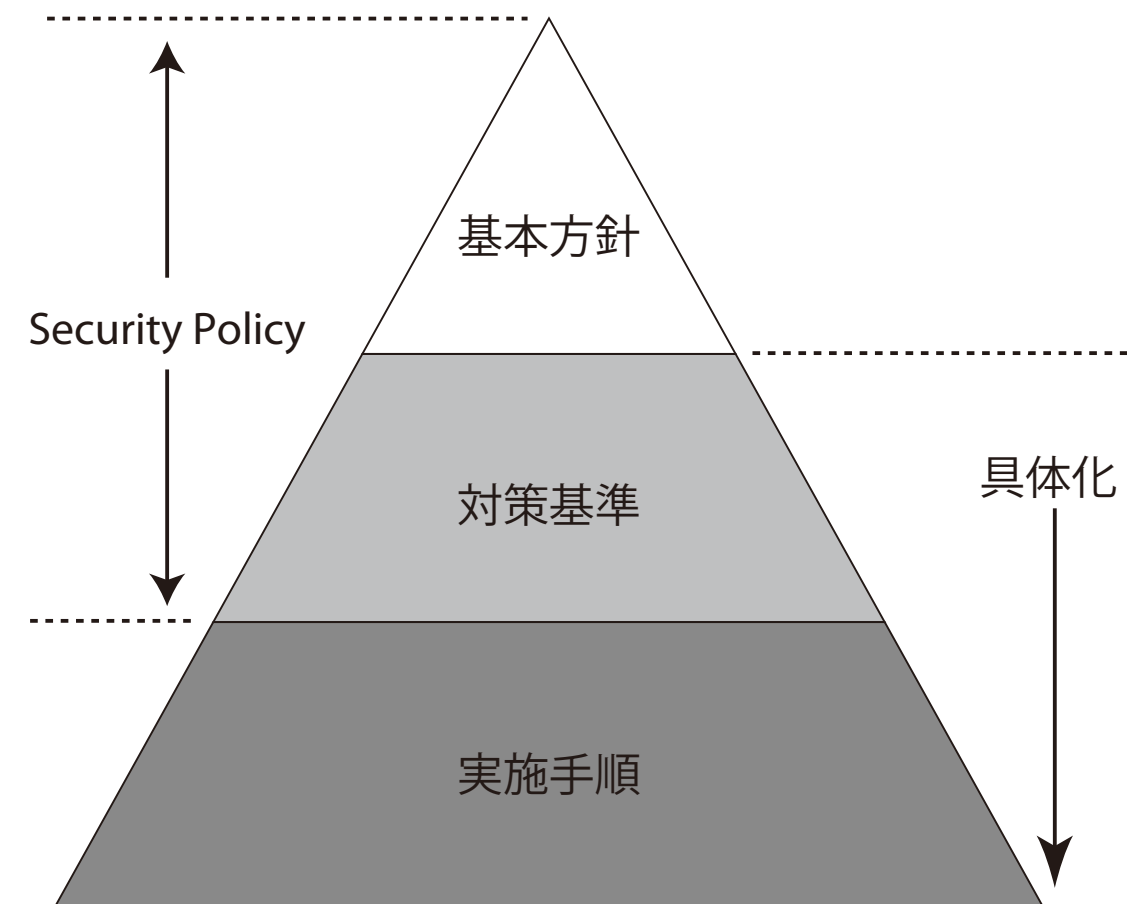
PDCAサイクル



ISMSによる対策 (3) - Plan編

Security Policyの策定

- Security Policyとは: 一貫したSecurity対策のための方針と基準
- 技術、運用/管理、組織体制を含む
- 三層構造 (基本方針、対策基準、実施手順)
- うち上位二層を“Security Policy”という
- 頻繁に更新されるものではない



ISMSによる対策(4) - Plan編

Security Policyの説明

- **基本方針**
 - 何を守り、どのようなリスクがあるかを明確化、責任者と担当者の決定.
- **対策基準**
 - どの情報資産を、こういった脅威から、どのように保護するか？
を具体的に定めたもの。セキュリティ対策の基準。
 - 利便性への考慮
- **実施手順**
 - 対策基準を行動に移せるようにするための具体的な手順書、マニュアル
 - 環境の変化に応じて**適宜更新**する。

電通大のSecurity Policy

- 電気通信大学 情報セキュリティポリシー
 - http://www.uec.ac.jp/about/disclosure/sec_policy/
- DOs and DON'Ts
 - <https://www.cc.uec.ac.jp/rule/DosAndDonts.pdf>
- 当然だが
 - 基本的人権の保護、各種法の遵守
 - セキュリティ侵害の禁止とセキュリティ維持の義務
 - 公共性の遵守、商用利用の禁止

すべての方へ

利用上の注意

学内ネットワークの学術目的以外の利用は禁止されています。

不正利用が発覚した場合は、学内規にしたがって調査や再発防止に必要な情報として利用者の氏名を含む情報を収集します。悪質な場合は処罰されます。

BitTorrent, eDonkey, Share, Winny, その他全てのP2Pファイル共有ソフトウェアは利用が禁止されております。通信が検出されるとネットワークへの接続が24時間遮断されます。また、学内規にしたがい、再発防止徹底のため、使用者の氏名、(学籍番号)、連絡先等の情報を収集します。悪質な場合は処分を検討します。

- 一部ウェブブラウザやネットワーク機器でP2P機能が有効になっているものがあります。これにより意図せずP2P通信が行われる可能性がありますので十分に注意してください。
- SkypeはP2P技術を利用していますが、基本的にコミュニケーション用ソフトウェアですので問題なく利用できます。

たとえ正規なものであっても、外部FTPサーバへの短時間での連続したログインの失敗は攻撃とみなされ、ネットワークへの接続が24時間遮断される恐れがあります。ご注意ください。

引用: <https://www.cc.uec.ac.jp/guidance.html>