

セキュリティ講座

著作権表示

クリップアート

- リコージャパン株式会社 プrintアウトファクトリー
 - <http://www.printout.jp/>
- 商用フリーのイラスト素材提供サイト「ビジソザ」
 - <https://bsoza.com/>
- openclipart
 - <https://openclipart.org/>
- いらすとや
 - <http://www.irasutoya.com/>

目次

第1章 最新動向 情報セキュリティ10大脅威	
1-1. 脅威の動向、手口、対策.....	6
1-2. 身近な脅威について～グループ学習～.....	29
第2章 関連制度や規格の動向 JIS, ISO/IEC, IEEEなど	
2-1. 規格の種類.....	31
2-2. 規格詳細.....	37
第3章 インシデントレスポンス	
3-1. インシデントレスポンス(IR)とは.....	45
3-2. インシデントレスポンスのプロセスやタスクの概要.....	48
3-3. インシデントレスポンス事例～グループ演習～ 障害・ヒューマンエラー・不正アクセス.....	64

目次

第4章 セキュア設計

セキュアシステム、セキュアネットワークの設計と構築

- 4-1. サイバー攻撃に備えた設計と構築..... 66
- 4-2. セキュアシステム、ネットワークの設計～グループ演習～..... 93

第5章 セキュア開発概説

- 5-1. ソフトウェア開発、ウェブサイト設計..... 95
- 5-2. セキュアプログラミング～グループ演習～..... 109

第6章 倫理・コンプライアンスの概念

- 6-1. 倫理・コンプライアンスの概念..... 111
- 6-2. 基本的な考え方..... 119

第7章 倫理要綱概説

RFC1087インターネットと倫理および情報処理学会倫理要綱

- 7-1. 行動規範に基づく判断と行動..... 132
- 7-2. 倫理的な判断と行動～グループ演習～..... 140

第1章 最新動向

情報セキュリティ10大脅威

情報資産、脅威、脆弱性、リスクの関係を（再）確認し、管理策との対応を説明できるようになる。

セキュリティのトレンドをいくつか確認し、立場によって対策が変わることを認識する。

セキュリティ管理策を策定する道筋を説明できる。

1-1. 脅威の動向、手口、対策

- (1) 情報資産とは？
 - ① 守るべき情報資産を考える
 - ② 脅威、脆弱性、リスクの関係
 - ③ リスクと管理策の関係
- (2) 情報セキュリティへの脅威の最新動向
 - ① 情報セキュリティ10大脅威 2017
- (3) 標的型攻撃による情報流出
 - ① 標的型攻撃の対策～経営者層～
 - ② 標的型攻撃の対策～システム管理者～
 - ③ 標的型攻撃の対策～セキュリティ担当部署～
 - ④ 標的型攻撃の対策～従業員・職員～
- (4) ランサムウェアによる被害
 - ① ランサムウェアの対策～経営者層～
 - ② ランサムウェアの対策～管理者と利用者～
- (5) IoT機器の脆弱性の顕在化
 - ① IoT機器の脆弱性の対策～利用者～
 - ② IoT機器の脆弱性の対策～開発者～

情報資産とは？

- 業務遂行の過程で生み出される価値あるもののうち、財務情報、人事情報、顧客情報、技術情報などの目に見えないもの

- 経済産業省JNSAの解説より
- TR X 0036-3:2000 (ISO/IEC TR 13335-3:1998)も参照

資産目録なしに
脅威は評価できない！

JNSA: NPO 日本ネットワークセキュリティ協会
(Japan Network Security Association)

「情報セキュリティ」とを考えるにあたり、そもそも何を守りたいのか。その意識付けを行ってください。一つや二つではないはずですし、粒度の違いもあります。それらを漫然と並べただけでは適切な対策が無理そうだと感じてもらえればよいです。だからこそ、資産目録の作成が必要だと実感してもらえれば一番です。

次のスライドの後で、グループ内で話し合ってもらったり、発表してもらうのもよいかもしれません。

守るべき情報資産を考える

- 組織として守りたい情報資産は何ですか？
 - 資産目録を作成(JIS Q 27001 : 2006規格要求事項を改変)
 - すべての情報資産を明確に識別
 - 情報資産、管理責任者を特定
 - 情報資産全てについて、管理責任者を指定
 - 重要な情報資産の全ての目録を作成し維持
 - 情報資産の利用の許容範囲に関する規則を明確にし、文書化
 - 資産に対する脅威を特定
 - 脅威がつけ込むかもしれないぜい弱性を特定
 - 機密性、完全性、可用性の喪失がそれらの情報資産に及ぼす影響を特定
 - 情報は、組織に対しての価値、法的要求事項、取扱いの慎重度合い及び重要性の観点から分類
 - 情報のラベル付け及び取扱いは、分類体系に従って実施

グループワークの前段階として、グループ内で自己紹介とともに情報資産の例を挙げてもらうとよいかもしれません。次のスライドに、情報資産の参考例を挙げてあります。

このスライドの時点で、「脅威」と「脆弱性」の違いを説明できるかどうかを受講者に尋ねてみるとよいです。

参考：情報資産の種類

- 情報/データ（例えば、支払いの詳細を含んだファイル、製品情報など）
- ハードウェア（例えば、コンピュータ、プリンタなど）
- アプリケーションを含むソフトウェア（例えば、テキスト処理プログラム、特別の目的のための開発されたプログラムなど）
- 通信設備（例えば、電話、銅線、ファイバーなど）
- ファームウェア（例えば、フロッピーディスク、CD-ROM、PROMなど）
- 文書（例えば、契約書など）
- 資金（例えば、ATMなど）
- 製造物
- サービス（例えば、情報サービス、計算資源など）
- サービスの信頼と信用（例えば、支払いサービスなど）
- 環境設備
- 要員
- 組織のイメージ

TR X 0036-3:2000 (ISO/IEC TR 13335-3:1998) より

- 9 -

CSAJ

参考スライドは、基本的に説明しなくてかまいません。

PROM (Programmable ROM)は、電氣的(EEPROM)あるいは紫外線(EPROM)によって書き換え可能な不揮発性メモリをまとめた用語として使っています。質問があった場合、単に「プログラム更新可能なROM」と説明すればよいでしょう。

脅威、脆弱性、リスクの定義

JIS Q 27000:2014の用語定義より

- 脅威
 - システム又は組織に損害を与える可能性がある、望ましくないインシデントの潜在的な原因。
- 脆弱性
 - 一つ以上の脅威によって付け込まれる可能性のある、資産又は管理策の弱点。
- リスク
 - 目的に対する不確かさの影響。
 - JIS Q 0073:2010 の 1.1 参照
- 管理策
 - リスクを修正する対策。

2枚先のスライドで図示しますが、脅威と脆弱性とリスクの関係を意識してもらうとよいです。

リスクの定義がわかりにくいので、次のスライドを説明に使うとよいかもしれません。

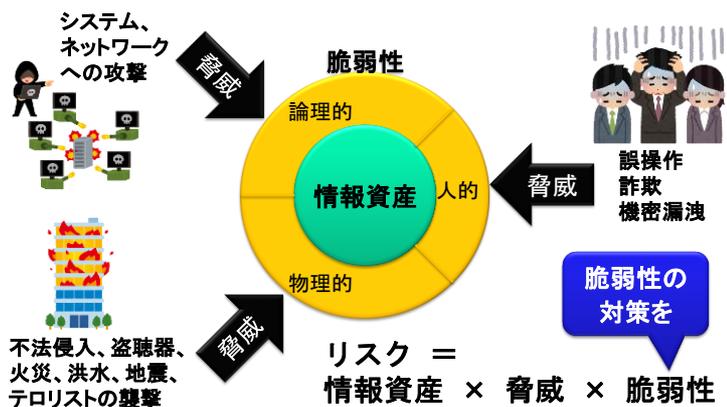
参考：リスクの定義補足

JIS Q 0073:2010 の 1.1 より

- 目的に対する不確かさの影響。
 - 注記 1 影響とは、期待されていることから、好ましい方向及び／又は好ましくない方向にかい（乖）離することをいう。
 - 注記 2 目的は、例えば、財務、安全衛生、環境に関する到達目標など、異なった側面があり、戦略、組織全体、プロジェクト、製品、プロセスなど、異なったレベルで設定されることがある。
 - 注記 3 リスクは、起こり得る事象、結果又はこれらの組合せについて述べることによって、その特徴を記述することが多い。
 - 注記 4 リスクは、ある事象（周辺状況の変化を含む。）の結果とその発生の起こりやすさとの組合せとして表現されることが多い。
 - 注記 5 不確かさとは、事象、その結果又はその起こりやすさに関する、情報、理解若しくは知識が、たとえ部分的にでも欠落している状態をいう。

どんな事業でもプロジェクトでも目的があるはずで、その目的を達成するにあたり、不確かさ、すなわち不確定な要素がいろいろ存在するはずで、その不確定な要素を洗い出し、目的達成にどれくらい負の影響を与えるかがリスクで、不確定要素はリスクとなる、ということです。

脅威、脆弱性、リスクの関係



リスクを下げるにはどうすればよいか、できれば考えさせてください。情報資産の価値を下げたり、脅威の発生を抑えたりすることは困難だったり非現実的だったりします。情報資産に対するリスクを減らすためには、想定される脅威に対する『脆弱性の対策が必要』ということをはっきりさせておきます。

リスク数値化の例

- 資産の重要度と脅威、脆弱性レベルを使った数値化の例

- この表では数値を加算し、0～8で数値化している
- 数値が高いほど危険であることを示している

	脅威レベル	Low(0)			Medium(1)			High(2)		
	脆弱性レベル	L(0)	M(1)	H(2)	L(0)	M(1)	H(2)	L(0)	M(1)	H(2)
情報資産の重要度	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

数値化はあくまでも目安なので、計算式は足し算でも掛け算でも構いません。スライドの表では、レベルを0から始めているため足し算で計算しています。レベルを1から始めれば、掛け算でも同じような場合分けができます。

管理策の定義

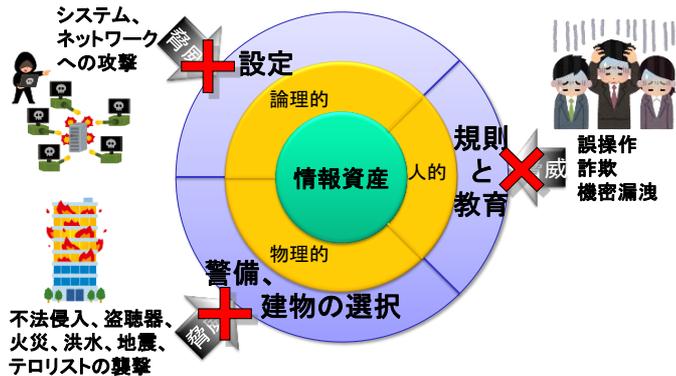
JIS Q 27000:2014の用語定義より

- 管理策 (control)
 - リスクを修正 (modifying) する対策。
 - 注記 1 管理策には、リスクを修正するためのあらゆるプロセス、方針、仕掛け、実務及びその他の処置を含む。
 - 注記 2 管理策が、常に意図又は想定した修正効果を発揮するとは限らない。

リスクを明確にしたら、リスクを軽減する管理策をとる必要があります。管理策はそのまま「リスクを修正する対策」です。どのような対策が考えられるかは次のスライドに描いてあります。

「注記 2」は必ず言及してください。ここにもあるとおり、管理策が常に効果を発揮するとは限りません。管理策を実施した後、必ずチェックが必要です。

リスクと管理策の関係



このスライドは情報資産、脅威、脆弱性、リスク、管理策の関係を示す際に何度でも使ってください。

論理的な脆弱性に対しては、主に設定で対応します。システムの設定だけでなく、ネットワークの設定やソフトウェアの管理も含まれます。

物理的な脆弱性に対しては、警備や建物の選択で対応します。本当に重要な施設であれば、そもそも場所を公開することも不適切です。部屋の配置図で、どの部屋で何を行っているのかが第三者にわかるようでも困ります。たとえば大手の認証局(CA)の場合、認証局の署名に必要な秘密鍵の保管場所は社内でも数人しか知らないそうです。

人的な脆弱性に対しては、規則と教育しかありません。詰込みではなく、日々の意識付けが必要です。人的な脅威が発生した場合、論理的な対策である程度は防げますが、多くの場合は利用者個々人の日ごろからの注意(Due Care)で防げます。

情報セキュリティへの脅威の最新動向

- 情報セキュリティ10大脅威

- IPAが脅威候補を選出し、情報セキュリティ分野の研究者、企業の実務担当者などからなる「10大脅威選考会」が脅威候補に対して審議・投票を行い、決定。



本資料はIPAが2011年から毎年春ごろに公開している資料です。10大脅威選考会はおおよそ100名前後で構成されています。

情報セキュリティ10大脅威 2018

「個人」向け脅威	順位	「組織」向け脅威
インターネット/バンキングやクレジットカード情報等の不正利用	1	標的型攻撃による情報流出
ランサムウェアによる被害	2	ランサムウェアによる被害
ネット上の誹謗・中傷	3	ビジネスメール詐欺による被害
スマートフォンやスマートフォンアプリを狙った攻撃	4	脆弱性対策情報の公開に伴う悪用増加
ウェブサービスへの不正ログイン	5	脅威に対応するためのセキュリティ人材の不足
ウェブサービスからの個人情報の窃取	6	ウェブサービスからの個人情報の窃取
情報モラル欠如に伴う犯罪の低年齢化	7	IoT機器の脆弱性の顕在化
ワンクリック請求等の不当請求	8	内部不正による情報漏えい
IoT機器の不適切な管理	9	サービス妨害攻撃によるサービスの停止
偽警告によるインターネット詐欺	10	犯罪のビジネス化 (アンダーグラウンドサービス)

10大脅威は、個人向けと組織向けと立場ごとに分けられています。本資料では特に目立ってきた3つの脅威について説明をします。基本的にはIPA資料を取りまとめたものなので、他の脅威についてももう少し詳しく知りたい場合は件の資料を参照してください。

ランサムウェアの被害は2016年ごろから目立ってきましたが、2017年末には徐々に下火になっています。その理由として、仮想通貨のマイニングに対する攻撃が増えてきていることがあります。2018年には仮想通貨（暗号資産）マイニングのブームが去り、標的型攻撃やビジネスメール詐欺がまた目立つようになっています。また、セキュリティ人材の不足が徐々に認識されるようになりました。

攻撃トレンドの移り変わりは早いので、IPAやJPCERT/CCの情報を継続して追える体制を作りたいところです。

標的型攻撃による情報流出

標的型攻撃

- メールによるウイルス感染等により組織内部に侵入
- 組織の機密情報が流出
- 取引先や関連会社を踏み台にして本丸を狙うことも

手口

- メールからウイルス感染「ばらまき型」「やり取り型」
- ウェブからウイルス感染「水飲み場型」
- 標的組織の関連会社が踏み台に



事例については、IPAの資料以外のものがあれば紹介してください。

2016年の事例：

旅行会社JTBから678万件の個人情報流出の可能性

- 取引先になりすましたメールの添付ファイルを開き、ウイルスに感染
- 遠隔操作により個人情報を保管しているサーバーへと侵害が拡大

富山大学、標的型攻撃により研究成果等が外部流出の可能性

- 感染PC内には個人情報や原発の汚染水処理に関する研究成果等を保有していた可能性
- 非常勤の研究者のPCがウイルスに感染したことが原因

また、クレームのメールを装い、商品写真と偽ってスパイウェアを添付するケースもあります。

標的型攻撃の対策～経営者層～

- 組織としての対応体制の確立
 - 問題に迅速に対応できる体制(CSIRT)の構築
 - 対策予算の確保と継続的な対策実施

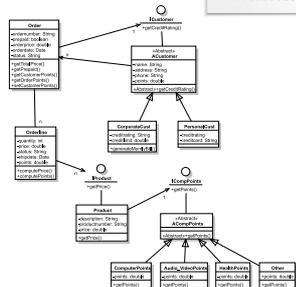


どのような脅威であっても、組織としての対応ではCSIRT構築が必要となります。CSIRTについては第3章「インシデントレスポンス」で改めて説明します。

また、ここに書いてある「継続的な対策」では、ISMSを意識しています。

標的型攻撃の対策～システム管理者～

- 被害の予防
 - 被害を抑止するためのシステム設計
 - アクセス制御・データの暗号化
- 被害の早期検知・事後対策
 - ネットワーク監視・分離



```

01011101010010
10001010110101
01010010101111
01010010010100
1101010010101
  
```

たとえ利用者がメール添付ファイルを開いたとしても、アクセス制御が適切に設定されていれば、権限のないデータにたどりつくことは困難になります。一方、データの暗号化は重要ですが、ネットワークの暗号化は被害の発見を遅らせたり、解析を困難にしたりします。やみくもにすべて暗号化ではなく、暗号化すべき場面をしっかりと意識します。プロキシーやWAFで一度暗号化解除をして監視することも必要です。

標的型攻撃の対策～従業員・職員～

- 情報リテラシーの向上
 - セキュリティ教育の受講
- 被害の予防
 - OS・ソフトウェアの更新
 - セキュリティソフトの導入・更新



内部へ侵入されることを想定した多層防御を

最近では利用者を罠に誘導する「誘導型攻撃」が増えてきています。これはシステムの脆弱性の解決だけでは不十分で、安易にリンクをクリックしないとか、日ごろからメールのやり取りに注意を払うとかいったセキュリティ教育の実施が必要となります。不定期的な訓練も効果的です。

ランサムウェアによる被害

ランサムウェア

- PC内のファイルの暗号化や、スマートフォンの画面のロックを行い、復元に身代金を要求
- 2016年はランサムウェアの被害が急増している

手口/影響

- メールの添付ファイルやリンクからランサムウェア感染
- ウェブからランサムウェアに感染
(脆弱性等を悪用)
- 感染したPCだけではなく、共有サーバー等別の機器にも影響

事例については、IPAの資料以外のものがあれば紹介してください。

ランサムウェアの日本語化・被害拡大

- 検出されたランサムウェアの件数が2015年の9.8倍
- その中には日本語表記のランサムウェアを確認

ランサムウェアに感染したファイルを復号するツールの登場

- 暗号化されたファイルを復号するツールが登場し、万が一暗号化されてもファイルを復元できる可能性

ランサムウェアの対策～経営者層～

- 組織としての対応体制の確立

- 問題に対応できる体制（CSIRT等）構築
- 予算の確保
- セキュリティ対策の指示



インシデントにはトレンドがあります。また、新しい攻撃は既存の対策では考慮されていないことがあります。目新しい攻撃が見られるようになったら、経営者からセキュリティ対策の指示を改めて行う必要があることを確認してください。

ランサムウェアの対策～管理者と利用者～

システム管理者とPC・スマートフォン利用者の対策

- 情報リテラシーの向上

- 受信メール（添付ファイル・リンク）
ウェブサイトの十分な確認

- 被害の予防

- OS・ソフトウェアの更新
- セキュリティソフトの導入
- フィルタリングツールの活用

- 被害を受けた後の対策

- バックアップからの復旧
- 復元できるかの事前の確認
- 復元ツール・機能の活用



定期的なバックアップと脆弱性対策を

ランサムウェアに感染した場合、やむを得ず身代金を払うケースも少なからずあります。これは、データの損失による被害と身代金を天秤にかけた結果です。Trustwave社のレポートによると、攻撃者から見たランサムウェアのROI（投資に対する利益率）は1425%にもなります。ランサムウェアの脅威を減らすにはROIを減らすことが一番ですが、そのためにはソフトウェアの更新、多層防御、すべての端末へのセキュリティ対策ソフト導入といった、攻撃者が嫌がる対策をとるしかありません。

万が一感染しても、常に最新のバックアップがあれば被害を最小限に食い止め、身代金を払うより低いコストで復旧も可能です。

いずれにしても、利用者の情報リテラシー向上が一番の対策です。

※ Trustwave社はシカゴに本社を持ち、PCI -DSS (クレジットカード業界のセキュリティ基準)の審査機関として世界屈指の実績を持つ、96か国300万ユーザーの顧客を持つ企業です。

IoT機器の脆弱性の顕在化

IoT機器の脆弱性

- IoT機器の脆弱性が悪用され、ウイルス感染や不正利用される
- 不正利用されたIoT機器がボット化し、DDoS攻撃等に悪用されるケースも

手口/影響

- IoT機器の脆弱性を悪用してウイルスに感染させる
- ウイルスに感染後、DDoS攻撃を行い組織のサービスを妨害する
- 不正利用や情報窃取される場合も



事例については、IPAの資料以外のものがあれば紹介してください。

海外ルーターの脆弱性を悪用とした攻撃

- 脆弱性を悪用されたIoT機器はボット化し、DDoS攻撃に悪用される

電気自動車の専用アプリに遠隔操作可能となる脆弱性

- 専用アプリのAPIに認証の仕組みが実装されておらず、遠隔操作される

可能性

医療機器インスリンポンプに遠隔操作可能となる脆弱性

- 患者の治療情報や機器のデータの取得や機器を操作される脆弱性
- 修正版のファームウェアをリリースする予定はない

IoT機器の脆弱性の対策～利用者～

- 情報リテラシーの向上
 - 機器使用前に説明書の内容を確認
- 被害の予防
 - 不要な機能の無効化(telnet等)
 - 外部からの不要なアクセスを制限
 - ソフトウェアの更新(自動化設定含む)



身近なIoT機器の例を一つ挙げ、利用者が最初にすべきことがなにか。受講者に聞いてみてください。導入前であれば、信頼できる製品か否か。導入直後であれば、説明書を読むといったことを最終的に伝えてください。

IoT機器は、利便性のために初期設定が脆弱なものが多く存在します。利用者はまずは説明を読み、不要な機能をまずは無効化する必要があります。なんとなくで使っている機能があれば、改めて説明書を確認するようにします。

IoT機器の脆弱性の対策～開発者～

被害の予防

- セキュアプログラミングの適用
- 脆弱性の解消
- ソフトウェア更新手段の自動化
- 分かり易い取扱説明書の作成
- 迅速なセキュリティパッチの提供
- 不要な機能の無効化(telnet等)
- 安全なデフォルト設定
- 利用者への適切な管理の呼びかけ



利用者は利用しているIoT機器の適切な管理を
開発者は適切な利用者を意識した対策を

IoTの接続先であるサーバーやクラウドでも、今後はIoTを意識した対策を追加する必要があります。IoT機器がBot化して攻撃に利用されるケースが増えていることを伝えてください。

接続の経由地点となるネットワーク接続機器（ルーターやスイッチなど）も同様にIoT接続を意識する必要があります。一度リリースされたIoT機器の中には再起動が難しいものや更新不能なものもあるため、ネットワーク接続機器による間接的な対策とる必要があるかもしれません。

対策の流れは通常システムと同様ですが、対象とするIoT製品やサービスのシステム全体構成を明確にすることが大事になってきます。

1-2. 身近な脅威について～グループ学習～

演習 1 情報資産と脅威の検討



演習は基本的にグループ学習です。演習は答えが一つというものではないため、皆の演習結果を全体で共有することを特に意識してください。

第2章 関連制度や規格の動向

JIS, ISO/IEC, IEEEなど

用語定義の規格を示すことができる。

標準化団体の概要をつかむ。

ISO/IEC 27000～27002については、その規格の目的を示すことができること。

2-1. 規格の種類

- (1) 情報セキュリティ・ガイドライン
- (2) 用語の定義
- (3) ISMSファミリー規格
- (4) 国際標準化団体の例



情報セキュリティ・ガイドライン

- OECD (経済協力開発機構) Guidelines (2015/10/1)
 - 「情報システム及びネットワークのセキュリティのためのガイドライン：セキュリティ文化の普及に向けて」
- 「セキュリティ文化」という新しい概念を提唱
- セキュリティの9原則
 1. 認識の原則
 2. 責任の原則
 3. 対応の原則
 4. 倫理の原則
 5. 民主主義の原則
 6. リスクアセスメントの原則
 7. セキュリティの設計及び実装の原則
 8. セキュリティマネジメントの原則
 9. 再評価の原則



正式名称は以下の通り。

OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security

2015/10/1に改定され、2002年のガイドラインと比べると「セキュリティ文化」という考え方を前面に押し出したものになっています。セキュリティ文化という概念についてぜひ伝えてください。

似たようなガイドラインにプライバシーの8原則があるので、もし質問があった場合は提示してください。

プライバシーの8原則：

1. 収集制限の原則
2. データ内容の原則
3. 目的明確化の原則
4. 利用制限の原則
5. 安全保護の原則
6. 公開の原則
7. 個人参加の原則
8. 責任の原則

用語の定義

- JIS X 0008:2001 (情報処理用語-セキュリティ)
 - 情報処理におけるセキュリティ用語, 定義及び対応する英語について規定
 - ISO/IEC 2382-8:1998 と対応
- JIS Q 0073:2010 (リスクマネジメント-用語)
 - 組織、部門並びに異なる適用分野及び業態において、リスクマネジメントの概念および用語に関する共通の理解を形成するための基本用語集
 - ISO Guide 73:2009 と対応

用語があいまいな
場合に参照する！

工業規格の内容説明より、それぞれの規格がどのような分類をされており、どのような役割でその規格が存在するのか、その位置づけを理解してもらうことを念頭においてください。詳しい内容を説明する時間はおそらくありません。必要であれば、あとで規格書を見るように伝えるだけでも十分です。

JIS X は情報処理に関する規格であることを意味しています。

JIS Q は管理システムに関する規格を意味します。

JIS X 0001～0032までは情報処理用語について定義されており、その中の一つとしてセキュリティ分野の用語をJIS X 0008で定義しています。例えばバックアップ手続きやデータ復元の定義や、脅威とせい弱性の定義などがあります。機密性、完全性、可用性の定義を見てみると、例えば完全性はデータ完全性とシステム完全性を分けて定義していたり、可用性も「セキュリティにおける」と用語の適用範囲を明確にしていたりしています。

JIS Q 0030～0073は、対応するISO Guide またはISO/IEC Guide を基に、技術的内容及び構成を変更することなく作成した日本工業規格です。ただし、すべてのガイドがJIS化されているわけではありません。

これらのガイドは、以下の人々に助言を提供する文章です。

- 規格作成者に対し、規格を起草する際の特定の問題を扱う方法について助言を提供する
- 国家標準機関に対し、標準化の原則に特有な問題を扱う方法について助言を提供する

ISMSファミリ規格

財務情報、知的財産、従業員情報、及び顧客又は第三者から委託された情報を含む、情報資産のセキュリティを管理するための枠組みを策定

ISO/IEC 27000	Information security management systems – Overview and vocabulary
ISO/IEC 27001	Information security management systems – Requirements
ISO/IEC 27002	Code of practice for information security controls
ISO/IEC 27003	Information security management system implementation guidance
ISO/IEC 27004	Information security management – Measurement
ISO/IEC 27005	Information security risk management
ISO/IEC 27006	Requirements for bodies providing audit and certification of information security managementsystems
ISO/IEC 27007	Guidelines for information security management systems auditing
ISO/IEC TR 27008	Guidelines for auditors on information security controls
ISO/IEC 27010	Information security management for inter-sector and inter-organizational communications
ISO/IEC 27011	Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
ISO/IEC 27013	Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000
ISO/IEC 27014	Governance of information security
ISO/IEC TR 27015	Information security management guidelines for financial services
ISO/IEC TR 27016	Information security management – Organizational economics
ISO/IEC TR 27019	Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry
ISO 27799:2008	Health informatics – Information security management in health using ISO/IEC 27002

» 作成中の規格、中止となった規格は除く

表について説明する必要はありません。この中から 27000, 27001, 27002, 27014 のみ代表して取り上げられることを示してください。27000は用語の定義、27001はISMS要求事項、27002は実践規範についての規格です。そして27014は情報セキュリティガバナンス（組織の情報セキュリティ活動を指導し、管理するシステム）についての規格です。すべての規格を説明することはできないので、特に組織の活動についての規格である27014を取り上げています。それぞれに対応するJIS規格があるので、説明はJIS規格を基に行ってください。

国際標準化団体の例

基礎知識として

国際標準化団体とは、地域による制限なく標準化作業に参加可能な標準化団体

- ISO (国際標準化機構)
 - International Organization for Standardization
 - 国家間の技術的障壁を取り除くための、汎用的な国際標準を策定する非政府組織。
- IEC (国際電気標準会議)
 - International Electrotechnical Commission
 - 電気工学、電子工学、および関連した技術を扱う国際的な標準化団体。一部規格はISOと共同開発。
- ITU (国際電気通信連合)
 - International Telecommunication Union)
 - 世界最古の国際機関。無線通信と電気通信分野において各国間の標準化と規制の確立を図る。国連の専門機関の一つ。

ISOとIECは共同で規格策定を行うことがあることに軽く触れてください。

標準化団体を知ることで、各規格の権威づけが明確になります。

ISOは汎用的な国際標準を、IECは電気電子技術の国際標準を策定するという違いにも軽く触れてください。

ITUは国連の専門機関の一つであることと、通信分野の標準化に関わることに触れればよいです。

国際標準化団体の例

基礎知識として

- IEEE (米国電気電子学会 ※公式な日本語名称はアイ・トリプル・イー)
 - Institute of Electrical and Electronic Engineers
 - 通信、情報技術、発電製品とサービスの多くを支えている国際標準規格のリーディングデベロッパー
- JISC (日本工業標準調査会)
 - Japanese Industrial Standards Committee
 - 経済産業省に設置されている審議会。工業標準化全般に関する調査・審議を行う
- IETF (インターネット技術標準化タスクフォース)
 - Internet Engineering Task Force
 - インターネットにおける標準は rough consensus に基づき実装/運用を行い決めていく。その rough consensus を形成する議論を行い、標準を策定していく場がIETFである
 - IETFにおける技術仕様は RFC (Request For Comments) という名前で文書化、保存され、だれでも自由に参照できる。

IEEEは「米国電気電子学会」とスライド通りに訳されることがありますが、これは正式な名称ではありません。日本語に訳された名称は存在せず、日本語名称も「アイ・トリプル・イー」となっています。

JISCで策定した規格がいわゆるJIS規格となっています。

JPNICによると、IETFの特徴として以下を挙げています。この考え方には触れておいてください。

IETFにおける技術仕様の策定は、ラフコンセンサス(Rough Consensus)、ランニングコード(Running Code)という点の特徴として挙げられます。標準は変わらないという前提のもと、最初から詳細な技術仕様を決定し、この仕様通りに実装していくのが、従来型のプロセスでした。これに対してIETFでは、まずラフな仕様を作成し、それから相互接続実験や実運用を通じて、工夫、改善を加えながら詳細な仕様を実装していくという、非常に柔軟な仕様策定プロセスとなっています。

2-2. 規格詳細

(1) ISMSファミリー規格

- ① ISO/IEC 27000:2014
- ② ISO/IEC 27001:2013
- ③ ISO/IEC 27002:2013
- ④ ISO/IEC 27014:2013
- ⑤ ISO/IEC 15408-1:2009

(2) IEEE802.11 無線LAN



ISO/IEC 27000:2014

- JIS Q 27000:2014 (情報技術-セキュリティ技術-情報セキュリティマネジメントシステム-用語) と対応

- ISMS ファミリ規格に関連する用語及び定義について規定
- 一部抜粋
 - 2.28 情報セキュリティガバナンス (governance of information security)
組織 (2.57) の情報セキュリティ活動を指導し、管理するシステム。
 - 2.57 組織 (organization)
自らの目的 (2.56) を達成するため、責任、権限及び相互関係を伴う独自の機能をもつ、個人又は人々の集まり。
 - 2.56 目的 (objective)
達成する結果。

用語があいまいな
場合に参照

可能であれば、JIS Q 27000:14を表示していくつかの例を示し、この規格がどのような内容なのか雰囲気だけでも伝えてください。どういう場面でこの規格が必要となるのかを重点的に示してください。

以後も同じ要領で、詳細の説明よりどのような目的の規格なのか伝われば十分です。

<http://www.jisc.go.jp/app/jis/general/GnrJISSearch.html>

ISO/IEC 27001:2013

- JIS Q 27001:2014 (情報技術-セキュリティ技術-情報セキュリティマネジメントシステム-要求事項) と対応
 - ISMSを確立、実施、維持、継続的な改善を行うための要求事項を提供
 - 組織自身の情報セキュリティ要求事項を満たす組織の能力を組織の内部で評価するため、または外部関係者が評価するために用いることも意図
 - 一部抜粋
 - 9.1 監視、測定、分析及び評価
 - 組織は、情報セキュリティパフォーマンス及び ISMS の有効性を評価しなければならない。
 - 組織は、次の事項を決定しなければならない。
 - a) 必要とされる監視及び測定の対象。これには、情報セキュリティプロセス及び管理策を含む。
 - b) ~省略~

ISMSの仕様、
要求事項を定義

ISO/IEC 27001と27002は、ともに同じ規格BS7799から派生してきたワンセットの規格であることは伝えたいほうが良いかもしれませんが。まずはこれら2規格の全体像を把握してからほかの規格の理解に取り組んでもらうほうが分かりやすいかと思います。27001で仕様を定義し、27002で実施基準、行動規範を定義していることを押さえておきます。

ISO/IEC 27002:2013

- JIS Q 27002:2014 (情報技術-セキュリティ技術-情報セキュリティ管理策の実践のための規範) と対応

- 組織の情報セキュリティリスクの環境を考慮に入れて、管理策の選定、実施する手引き。
- 組織の情報セキュリティマネジメントの指針を作成する場合に用いることも意図。

- 一部抜粋

- 7.2.2 情報セキュリティの意識向上、教育及び訓練管理策

- 組織の全ての従業員、及び関係する場合には契約相手は、職務に関連する組織の方針及び手順についての、適切な、意識向上のための教育及び訓練を受け、また、定めに従ってその更新を受けることが望ましい。

ISMSの実施基準、
行動規範を定義

あらためて、ISO/IEC 27002は実施基準であることの念押しをしておきます。ISMSを維持するためにどうすればよいのか、実際の行動規範が書かれています。

BS7799-1からの経緯を説明すると、初めて学ぶ受講者の場合は混乱のもとになります。ただし、質問として以前のISO/IEC 17799との関連や、BS7799-1からの経緯を聞かれた場合には軽く触れてあげてください。

もともとはイギリスの規格であるBS7799を国際規格化すべく、BS7799-1とBS7799-2として2部構成にしました。そして合意を得やすい内容であるBS7799-1が先に規格化することに成功しました。こうしてできたのがISO/IEC17799です。ISO/IEC17799は日本でもJIS X 5080:(今は廃版)として定義されました、その後、情報セキュリティ管理システムの仕様を規格化しているBS7799-2がISO/IEC27001として規格化され、その仕様に基づいた行動規範という形でISO/IEC27002が規格化されています。

ISO/IEC 27014:2013

- JIS Q 27014:2015 (情報技術-セキュリティ技術-情報セキュリティガバナンス) と対応

- 情報セキュリティガバナンスについての概念及び原則に基づくガイダンス
- 組織が情報セキュリティに関連した活動を評価、指示、モニタ及びコミュニケーションできるようになる
- 一部抜粋

- 5.3 プロセス 5.3.1 概要

経営陣は、情報セキュリティを統治するために、“評価”、“指示”、“モニタ”及び“コミュニケーション”の各プロセスを実行する。

さらに、“保証”プロセスによって、情報セキュリティガバナンス及び達成したレベルについての独立した客観的な意見が得られる。

組織の情報セキュリティ活動を指導し、
管理するシステムについての規格

ISO/IEC27014を取り上げている理由として、ガバナンスの重要性が問われるようになったことがあります。内容の詳細よりも、情報セキュリティガバナンスの規格が存在するという事実を知ってもらえれば十分です。

組織の情報セキュリティ活動を指導し、管理するシステムについての規格であるISO/IEC 27014は2013年に第1版が発行されました。JIS化されたのは2015年であるため、最近の動向として紹介します。

経済産業省としても以下のような事件が多発したことから、2009年度よりの第二次情報セキュリティ基本計画にて「情報セキュリティガバナンス」を位置づけています。

(経済産業省「情報セキュリティガバナンス概要紹介」より抜粋)

【発生している事件・事故の具体例 (2006年～)】

- ・元A証券社員が全個人口座148万6651件の情報を無断で持ち出し一部を売却
- ・金融機関多数において伝票、名簿等の顧客情報を誤廃棄・紛失 (都市銀行、地方銀行等)
- ・ファイル共有ソフト (Winny等) による情報漏えい事件の多発 (ITベンダ、通信事業者、学校法人等)

【コンプライアンス問題の例】

- ・インサイダー (情報漏えい) (印刷業者、放送事業者等)

【膨大な被害額】

- ・国内個人情報漏えい事件の想定損害賠償総額：2兆円超 (2007年) [日本ネットワークセキュリティ協会調べ]
- ・不正アクセスによる被害規模 (事例)：数億円～数十億円/一件あたり (2006年) [(独) 情報処理推進機構調べ]

ISO/IEC 15408-1:2009

- CC (Common Criteria)と同義
- JIS X 5070-1:2011 (セキュリティ技術-情報技術セキュリティの評価基準-第1部:総則及び一般モデル)と対応
 - 評価機関の行った、異なるセキュリティ評価の結果を比較可能にする。
 - セキュリティ評価のときに IT 製品のセキュリティ機能及びその IT 製品に適合される保証手段に対する共通の要件群を提供することによって、この比較を可能にする。
 - 実装の確かさを、評価保証レベル(EAL)によりレベル分け。
 - EAL1~3:一般民生用
 - EAL4:政府機関向け
 - EAL5~7:軍用レベルほか、政府最高機密機関レベル向け

情報技術に関連した製品及びシステムが適切に設計され、その設計が正しく実装されていることを評価するための国際標準規格

情報セキュリティから少し外れますが、情報機器のセキュリティもここで触れておきます。

ISO/IEC 15408は、情報技術セキュリティの観点から、情報技術に関連した製品及びシステムが適切に設計され、その設計が正しく実装されていることを評価するための国際標準規格です。

評価保証レベル (EAL : Evaluation Assurance Level)

EAL1~3:一般民生用

EAL4:政府機関向け

EAL5~7:軍用レベルほか、政府最高機密機関レベル向け

IEEE802.11 無線LAN

IEEE802.11n	2009/9	2.4 - 2.5GHz 5.15 - 5.35GHz 5.47 - 5.725GHz	65Mbps - 600Mbps	障害物に強い (2.4GHz帯)
IEEE802.11ac	2014/1	5.15 - 5.35GHz 5.47 - 5.725GHz	292.5Mbps - 6.93Gbps	802.11a/nもサポート
IEEE802.11ad	2013/1	57 - 66GHz	4.6Gbps - 6.8Gbps	ビデオ信号の無線化 バス信号の無線化
IEEE802.11ax	策定中	2.4 - 2.5GHz 5.15 - 5.35GHz 5.47 - 5.725GHz	- 9607.8 Mbps	利用者が集中する高密度環境を想定 スループット向上(体感でacの4倍) a/b/g/n/acとの下位互換

- IEEE802.11i

- 無線LANセキュリティ規格 (2004/6策定)
 - Medium Access Control (MAC) Security Enhancements
- 標準暗号AES規格を採用
- CCMP (counter mode with cipher block chaining/message authentication code protocol)
 - AESを使う暗号通信プロトコルの1つ
 - 暗号化機能だけでなく、データの改ざん検出機能も備える
- IEEE 802.11i準拠のセキュリティ規格として、Wi-Fi AllianceではWPA2を定める

このページは飛ばしてもらって構いません。IEEE委員会の仕事の一例として提示しています。

IEEE802.11axは駅、空港、競技場などの高密度環境を想定し、最大ビットレートの向上よりスループットの向上を目指しています。具体的には、高密度環境におけるユーザ当たりの平均スループットを少なくとも4倍に高めることを目標としています。2019年の規格化を予定していますが、ドラフト規格に対応したIEEE 802.11ax対応Wi-Fiルーター(ASUS RX-AX88U)が2017年8月30日に発表されています。

第3章 インシデントレスポンス

インシデント対応が必要になった際に大きく戸惑わないように、インシデント管理の流れと対応の位置づけを説明できるようにする

最低限必要なドキュメントと、ドキュメントがなぜ必要かを説明できる。

3-1. インシデントレスポンス(IR)とは

- (1) 情報セキュリティインシデント
- (2) インシデントレスポンス (対応) とは



情報セキュリティインシデント

JIS Q 27000:2014の用語定義より

- 情報セキュリティインシデント
 - 望まない単独若しくは一連の情報セキュリティ事象、又は予期しない単独若しくは一連の情報セキュリティ事象であって、**事業運営を危うくする確率**及び**情報セキュリティを脅かす確率**が高いもの。
- 情報セキュリティ事象
 - 情報セキュリティ方針への違反若しくは管理策の不具合の可能性、又はセキュリティに関係し得る未知の状況を示す、システム、サービス又はネットワークの状態に関連する事象。
- インシデントの例
 - 情報流出、フィッシングサイト、不正侵入、マルウェア感染、Web改ざん、DoS (DDoS)など

JPCERT/CC (<https://www.jpCERT.or.jp/ir/>) より

インシデントレスポンスの説明の前に、そもそも「情報セキュリティインシデント」が何を指すのかここで定義を示してください。ただ、あまり字面の定義にとらわれず、内容や概念を伝えるようにしてください。たとえばかいつまむと、そのまま放っておくと事業運営に支障をきたす事象ということでしょうか。

インシデントレスポンス（対応）とは

インシデント発生後の被害を最小限にするための「事後」対応のこと。

JIS 22300:2013（社会セキュリティ用語）より

－ インシデント対応（IR: incident response）

- 差し迫ったハザードの原因を食い止めるため、及び不安定又は中断・阻害を引き起こす可能性のある事象の結果を軽減し、正常な状況に復旧するために講じる処置。

情報セキュリティインシデントに対し、インシデント対応がよくクローズアップされますが、インシデント対応とはインシデント発生後の被害を最小限にするための「事後」対応にすぎません。この「事後」対応であることは伝えてください。インシデント対応を行うためには、相応の準備が必要です。その準備はインシデント管理と呼ばれ、その一部がインシデント対応となります。

3-2. インシデント対応のプロセスや タスクの概要

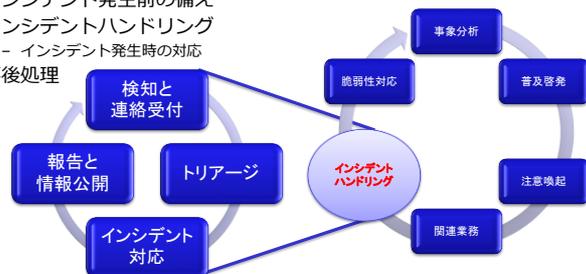
- (1) インシデント管理とインシデント対応チーム
- (2) インシデント管理 - インシデント発生前の備え
 - ① インシデント対応ポリシー
- (3) インシデント管理 - インシデントハンドリング
 - ① 検知と連絡受付
 - ② トリアージ
 - ③ トリアージ判定後の流れ
 - ④ インシデント対応
 - ⑤ インシデント対応計画
 - ⑥ 標準運用手順書
- (3) インシデント対応 - 主な活動
 - ① 初動、調査、修復
- (4) インシデント管理 - 事後処理



インシデント管理とインシデント対応チーム

- インシデント管理 (IRM: Incident Response Management)

- インシデント発生前の備え
- インシデントハンドリング
 - インシデント発生時の対応
- 事後処理



- インシデント対応チーム (IRT: Incident Response Team)

- 別名シーサート (CSIRT: Computer Security IRT)
- 情報セキュリティインシデントに対応する専門チーム
- インシデント管理は、IRT/CSIRTを中心に実施

インシデント管理 3つの流れは、次のページから追っていきます。
このスライドの絵の起点は「事象分析」です。

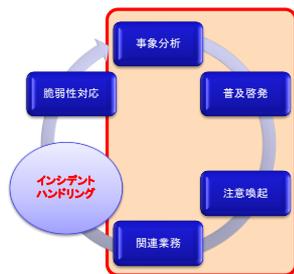
インシデント対応を行うにはインシデント管理が不可欠です。これはインシデント発生前の備えを行い、インシデント発生時の対応を明確にし、事後処理を行う一覧の活動となります。

インシデント対応を行うチームがインシデント対応チームであり、インシデント管理策はインシデント対応チームが中心となり実施することとなります。

インシデント管理 – インシデント発生前の備え

IRTがインシデント発生に備えて、インシデントの防止、予防を中心に行う平常時の活動

- 組織の準備
 - リスクの特定
 - **インシデント対応ポリシー**
 - IRP: Incident Response Policy
- IRT/CSIRTの準備
 - 任務の明確化
 - 連絡手段の明確化
 - 成果物の明確化
 - 必要とされるリソース
 - トレーニング、ハードウェア、ソフトウェアなど
 - ドキュメント類
 - チーム内ポリシー、ナレッジ管理
- インフラの準備
 - コンピュータ機器構成（資産管理）
 - ネットワーク構成



インシデント管理の1段階目、インシデント発生前の備えでは、インシデント対応ポリシーがすべての基準となることを明確にしてください。

CSIRT準備の成果物の一つであるドキュメントですが、チーム内ポリシーでは、証拠の取り扱いとしての証拠の収集、文書化、保管、発送の手引きなどが記述されています。ナレッジ管理では、調査に必要となる知識や関連情報を効率的に見つけられるように一か所にまとめる必要があります。

インシデント管理 – インシデント発生前の備え

- 平常時の事象分析：情報の収集と分析
 - インシデントの兆候、新たな脅威情報、OSやアプリケーションの脆弱性情報を収集し分析する
- 平常時の注意喚起：アドバイザリの発行/配布
 - 平常時の事象分析により得た情報に基づき、新たな脅威、脆弱性に対処するための情報を提供する
- 普及啓蒙
 - インシデント対応教育・セミナーの実施
- インシデント関連業務
 - 脆弱性の検査とパッチの適用
 - ファイアウォールソフトウェアの導入
 - 侵入検知システムの導入と監視
 - インシデント発生時の訓練
 - IRTの連絡窓口とのコミュニケーションチェックの中でも実施される

インシデント発生前の備えとして、平常時の事象分析や注意喚起といった行動が重要となってきます。いざ問題が起きてから行動しては遅い、ということは認識が必要です。

インシデント対応ポリシー

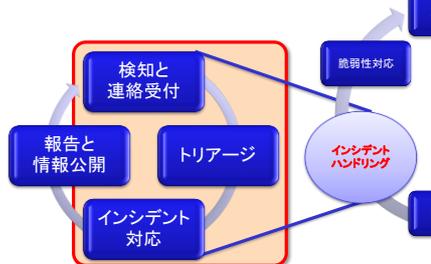
インシデント対応ポリシー (IRP) には以下の要素を含む

- マネジメント層の責任表明
- ポリシーの目的と目標
- ポリシーの範囲
 - だれに、何に、どのような状況で適用されるか
- コンピュータセキュリティインシデントの定義
- インシデントが組織にもたらす結果
- 組織構造、役割、責任、権限レベル
 - IRTによる装置の押収、接続の切断権限
 - IRTによる疑わしい活動の監視権限
 - インシデントについての報告義務
- インシデントの優先順位(または重大度レベル)
- 実施評価
- 報告フォームとコンタクトフォーム

このスライドで、インシデント対応の基準となるポリシーの要素を紹介しています。特にIRTの権限を明確にしておかないと、インシデント対応時に支障が出てきます。このポリシーには経営者層や組織による権威付けが必要です。

インシデント管理 – インシデントハンドリング

- 検知と連絡受付
 - 組織内の保守作業
 - 外部からの通報
- トリアージ
 - 重症度を判定し優先順位を決定
- インシデント対応
 - 情報共有、連携
 - **インシデント対応計画**
 - IRP: Incident Response Plan
 - **標準運用手順書**
 - SOP: Standard Operating Procedures
 - 技術的対応
- 報告と情報公開
 - 事後処理で行ってもよい



インシデントハンドリングの各段階についての詳細を次のスライドから進めていきます。このスライドでは全体の流れだけ伝えてください。

検知と連絡受付

- インシデントの検知方法
 - 組織内の保守作業
 - 外部からの通報での認識
- 組織内の保守作業などで検知する場合のポイント
 - 保守作業にインシデントの証拠がないかのチェック項目を含める
 - チェック方法と「異常」となる判定基準を決めておく
- 通報による検知のポイント
 - 外部からのインシデント関係の問い合わせ窓口を作り周知する
 - 連絡方法は複数用意する
 - 電話、ファックス、ホームページ、メールなど
 - 組織内部者からの通報にもIRTが対応する
- 検出したインシデントは関係者の間で事象共有し、最終的にIRTに集約する

いかに連絡しやすい環境を作るかがポイントになります。技術的にインシデントを検知したとしても、業務への影響を考察するのは人間です。検知した、あるいは連絡を受けたインシデントは事象共有し集約することが大事なことを伝えてください。

トリアージ

- 重症度を判定し優先順位を決定する作業
 - IRTメンバは、速やかに現状把握と重症度の判定を行う
 - インシデント対応の作業対象、作業項目の優先順位を決定する
- トリアージの判定基準は一定ではない
 - IRTが「守るべきものは何か」という基本的な活動ポリシーに依存する
 - 判定は3W1H、いつ(when)、どこで(where)、何が(what)、どう(how)発生したかを用いる
- トリアージの結果、インシデント対応を行わない場合もある
 - 侵入検知システムの誤検知(フォルスポジティブ)
 - 検知装置の判定基準値の誤設定
 - 通報者の勘違い

インシデントに対応するか否かを決定する重要な段階です。判定に迷った場合、「守るべき情報資産は何か?」「どのようなリスクが存在するか」というセキュリティ対策の基本に戻って考えてください。個々の事象にとらわれると収拾がつかなくなることがあります。

トリアージ判定後の流れ

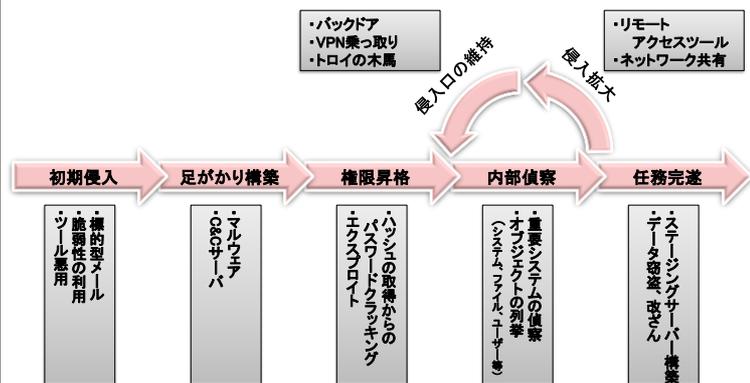
得られた情報から事実関係を確認し、IRT が対応すべきか否かを判定
判定時は、必要に応じて通報者やそのインシデントに関係する可能性のある
関係者と情報交換し詳細を確認

- IRT が対応すべきと判断した場合
 - インシデントレスポンスのフェーズに移行する。
- IRT が対応するインシデントではないと判定した場合
 - 判定の根拠を組織のポリシーと突き合わせ、可能な範囲で詳細に、通報者や関係者に回答/報告する。
- IRTの対応とは無関係に、関係者に速やかな対応の依頼や、情報提供をすべきと判定した場合
 - 注意喚起などの情報発信を行なう

インシデントが発生した場合、対応の有無にかかわらず結果を回答または報告する必要があることを抑えてください。

攻撃のライフサイクル

攻撃のライフサイクルを7段階で考え、調査や修復に役立てる



・説明の流れ

トリアージで、攻撃のライフサイクルを考慮することで判断の助けになることを示します。

・ポイント（絶対に覚えてほしいこと、など）

流れにそって考える、やみくもにつまみ食いの判断をしないことを伝えてください。

・質問（問いかけ）

業務時間外に社員のアカウントで、管理外の外部ホストに対する暗号化通信が見つかった場合、攻撃のどの段階に至っていると考えられますか？そして、何から対応したらよいですか。

・補足説明

以前の考え方だと、ライフサイクルに「侵入拡大」「侵入口の維

持」のループはありませんでした。攻撃は、このループによって拡大していくことがあります。

- ・ファシリテーションテクニック

- ・たとえ話、小ネタ

- ・（ある場合は）演習の使い方・注意点・フィードバックのポイント・使用ツール

インシデント対応

1. 事象分析を行ない、それがIRTの対応すべき事象か否かを再検討し、技術的な**対応が可能か否か**を判定する。
 - 自組織での技術的**対応が可能**な場合、IT関連部署と連携し、**インシデント対応計画**を策定し実施する。
 - 経営陣と情報共有を行なう
 - 自組織での技術的**対応が困難**な場合、経営陣と連携して**インシデント対応計画**を策定し実施する。
 - 必要に応じIT関連部署と情報共有/連携を行なう

・説明の流れ

トリアージの結果からインシデント対応計画を策定するまでの判断です。次のスライドにも続いています。

・ポイント（絶対に覚えてほしいこと、など）

インシデント対応が自組織内で可能か否かで計画が変わることを伝えてください。

・質問（問いかけ）

いずれの場合も経営陣と情報共有や連携を行うのはなぜ？

- ・補足説明

インシデント発生後のインシデント対応は慌てて行ってはいけません。自己判断で勝手に対応を行うことで、より状況が悪くなることもあります。まずはインシデント対応計画を策定し、その計画に従った標準運用手順書を作成し、その手順書に従った作業を行う必要があります。

インシデント対応計画には、スライドで示す要素が含まれています。計画を作成する主体はインシデント対応チームです。自組織で対応可能なインシデントの場合、IT部門と協力して作成します。自組織で対応困難なインシデントの場合、経営陣との連携が必要となります。

- ・ファシリテーションテクニック

- ・たとえ話、小ネタ

- ・（ある場合は）演習の使い方・注意点・フィードバックのポイント・使用ツール

インシデント対応

2. インシデント対応計画に従い**標準運用手順書**を作成し実施
 - 手順実施に際し、必要に応じて外部専門機関やそのインシデントに関係する可能性のある関係者に対し、対応の支援を依頼したり、必要な情報提供を求める。
3. 手順実施時に問題解決したか否かを確認し、未解決の場合は、再度事象分析し、インシデント対応計画を再策定し、再実施する。
4. 最終的に問題解決した時点で、顛末を通報者や情報提供者(対応を依頼した相手)に、自組織の情報セキュリティポリシーと突き合わせて可能な範囲で詳細に回答する。

・説明の流れ

インシデント対応は速やかに行うべきですが、手順や流れを追うことが大事です。

・ポイント（絶対に覚えてほしいこと、など）

まずはインシデント対応計画を策定し、その後標準運用手順書を作成することで、初めてインシデント対応が行えることを伝えてください。計画なし、手順書なしでは対応者によって結果が変わったり、今回のインシデントを次回に生かすこともできなくなります。

・質問（問いかけ）

問題解決したか否かはどうやって判定したらよいでしょうか（IoC: Indicator of Compromise 痕跡情報、脅威インジ

ケーターの絡みで)。

- ・補足説明
- ・ファシリテーションテクニック
- ・たとえ話、小ネタ
- ・(ある場合は) 演習の使い方・注意点・フィードバックのポイント・使用ツール

インシデント対応計画

インシデント対応計画 (IRP)には以下の要素が含まれる

- インシデント対応の使命(ミッション)
- ストラテジ(戦略)および目標
- 上級管理職による承認
- インシデント対応への組織的な取り組み
- IRTによる他の職員への連絡方法
- インシデント対応機能の測定用の表
- インシデント対応機能を熟成させるための手引き
- 組織全体へのインシデント対応計画の適合方法

・説明の流れ

このページはさらっと流して構いません。

・ポイント（絶対に覚えてほしいこと、など）

計画作成時の指針としてこのページを参考にできる

・質問（問いかけ）

・補足説明

・ファシリテーションテクニック

- ・たとえ話、小ネタ
- ・（ある場合は）演習の使い方・注意点・フィードバックのポイント・使用ツール

標準運用手順書

- 標準運用手順 (SOP) の役割
 - IRTが使用する手順書
 - インシデントごとの技術的な対応手順、手法、チェックリスト、フォームなどで構成
 - インシデント対応ポリシーおよびインシデント対応計画に基づく
 - 各インシデントに対応できるよう、できるだけ幅広く詳細なものを用意する
 - 対応については、各組織のインシデントの優先順位を反映
- SOPの効果
 - 標準化することによる誤対応/対策漏れの減少
- SOPはテストと検証を実施後、IRTメンバに配布する
- SOPドキュメントはSOP利用者の教育にも利用可能

・説明の流れ

このページもさらっと流して構いませんが、手順書作成の効果はぜひ伝えてください。また、手順書はポリシーと計画（どちらも略語はIRP）に従う必要があることを伝えてください。

・ポイント（絶対に覚えてほしいこと、など）

手順書を作成する意味

・質問（問いかけ）

手順書を作らないとどんな問題が起きうるか。

- ・補足説明

標準運用手順書は、インシデント発生前の備えで作成したインシデント対応ポリシーと、インシデント発生後に作成したインシデント対応計画に基づいて作成します。手順書を作成することで誤対応や対策漏れが減少します。この手順書はテストと検証を実施したのち、インシデント対応チームに配布します。この手順書は後日教育に利用することもできます。

- ・ファシリテーションテクニック

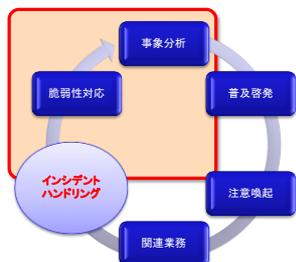
- ・たとえ話、小ネタ

- ・（ある場合は）演習の使い方・注意点・フィードバックのポイント・使用ツール

インシデント管理 - 事後処理

インシデント対応の収束後、インシデントから復旧し、再発を防止することを目的とする活動

- インシデントの直接の原因の究明
 - 原因の例：パッチの適用忘れ、設定間違い、未知の脆弱性の悪用など。
- 原因究明に必要な情報収集
 - 外部の信頼できる組織との情報共有が有効な場合がある
- 脆弱性対応
 - インシデントの直接原因となったISMSの弱点を埋める
 - よりよい予防、防止、管理策を検討、開発などを実施



・説明の流れ

インシデント対応が終わっても、インシデント管理はまだ続くことを示します。

・ポイント（絶対に覚えてほしいこと、など）

インシデント対応後に行うべきこと

・質問（問いかけ）

なぜ事後処理が必要か。

・補足説明

- ・ファシリテーションテクニック
- ・たとえ話、小ネタ
- ・（ある場合は）演習の使い方・注意点・フィードバックのポイント・使用ツール

インシデント管理 – 事後処理

- 事後の報告と情報公開
 - 必要に応じ、適切な相手に事後報告
- レポートの作成
 - 焦点を明確にする
 - 理解できること
 - 事実に徹する
 - タイミング
 - 再現性

『そのようなインシデント対応に至った経緯を、
20年後にも説明できますか。
そのためには何を記録に残せばよいですか。』

『記録がなければ、それは起こっていないということである』

・説明の流れ

最終的にレポートを作成しないと、その事象はなかったも同然になってしまうこと

・ポイント（絶対に覚えてほしいこと、など）

「そのレポートで、20年後にも何が起きてどう対応できたか説明できますか？」

・質問（問いかけ）

・補足説明

インシデント管理は、インシデント対応をして終わりではありません。事後の報告と情報公開は必須の活動です。事後報告のレポートのポイントはいろいろありますが、「そのようなインシデント対応に至った経緯を20年後に説明」することを念頭に作成するとよいです。大事なことは、記録がなければ、それは起こってないということだという意識です。

- ・ファシリテーションテクニック

- ・たとえ話、小ネタ

- ・（ある場合は）演習の使い方・注意点・フィードバックのポイント・使用ツール

3-3. インシデント対応事例～グループ演習～

演習 2 インシデント対応事例 - 正当なアカウントによる侵害



・説明の流れ

この演習は、実際に起きたインシデントの対応を例にとっています。正しい対応というのは設けてありませんが、どのように考えていくのか、その流れを体験してもらうのが目的です。時間をかなり取られますので、時間管理に注意してください。

・ポイント（絶対に覚えてほしいこと、など）

受講者の考えは決して否定しないでください。もし的外れに思えても、その場合はどうしてその考えに至ったのか話してもらい、皆で検討するようにしてください。

・質問（問いかけ）

- ・補足説明
- ・ファシリテーションテクニック
- ・たとえ話、小ネタ
- ・（ある場合は）演習の使い方・注意点・フィードバックのポイント・使用ツール
可能ならば、チームごとにホワイトボードや付箋紙を使える環境を用意してください。

第4章 セキュア設計

セキュアシステム、
セキュアネットワークの
設計と構築

安全なシステムを設計するポイントを説明できる。

安全なネットワークを構築するポイントを説明できる。

脅威を洗い出す流れを説明できる。

4-1. サイバー攻撃に備えた設計と構築

- (1) 設計原則
 - ① セキュアシステム設計
 - ② セキュリティ品質の確保
 - ③ 「要件定義」段階の考慮点
 - ④ 「設計」段階の考慮点
- (2) 脅威モデリング～STRIDE & DREAD～
 - ① 脅威モデリングの手順
- (3) セキュアネットワーク設計
 - ① ネットワークインターフェイス層
 - ② インターネット層とトランスポート層
 - ③ アプリケーション層
 - ④ ファイアウォールの構成
- (4) 検疫ネットワーク
 - ① 認証VLAN型検疫ネットワーク
 - ② エージェント型検疫ネットワーク
 - ③ DHCP検疫ネットワーク
 - ④ ゲートウェイ型検疫ネットワーク
- (5) 無線LANに対する脅威
 - ① 無線LANセキュリティ機能
 - ② 無線LANの接続性
- (6) IoTセキュリティ設計



設計原則

ソフトウェアエンジニアリングの原則 (Saltzer and Schroeder [1975])

1. 特権をできるだけ持たせない
2. 仕組みを単純にする
3. 設計はオープンにする
4. (セキュリティメカニズムで) 完全に仲介させる
5. フェイルセーフをデフォルトとする
6. 権限を集中させない
7. (複数ユーザーが依存する) 共通メカニズムの最小化
8. 気持ちで受け入れられるか。簡単に使えるか。

・説明の流れ

詳しく説明する必要はないですが、一つ一つ、受講生が状況を考える時間をとってください。

・ポイント (絶対に覚えてほしいこと、など)

設計についてのスライドで紹介している8原則は、1975年に提唱されすでに40年以上たっていますが、今現在も通用する原則です。特に、「設計はオープンにする」という部分は意識させてください。公開することで、多方面からの検証を受けられるため、よりセキュアにできるようになります。クローズな設計では、その設計がセキュアか否かの判定もできなくなります。

・質問 (問いかけ)

・補足説明

内容についてはここがわかりやすいです。

<https://linuxjf.osdn.jp/JFdocs/Secure-Programs-HOWTO/follow-good-principles.html>
IPA「セキュア・プログラミング講座」

・ファシリテーションテクニック

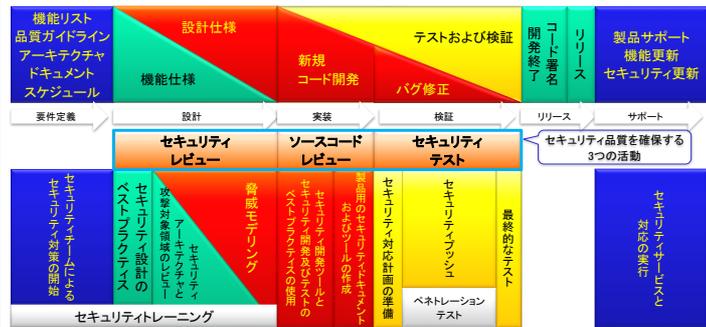
・たとえ話、小ネタ

・(ある場合は) 演習の使い方・注意点・フィードバックのポイント・使用ツール

セキュアシステム設計

セキュリティは
上流工程から！

セキュリティは、開発の初めから作りこむものである (Security by Design)
セキュリティは、システムのライフサイクルすべてに関わる



マイクロソフト「信頼できるコンピューティングのセキュリティ開発ライフサイクル」を基に改変

・説明の流れ

細かく各段階を説明する必要はありません。セキュリティ・バイ・デザイン、セキュリティは設計に左右されることを伝えられれば良いです。

・ポイント（絶対に覚えてほしいこと、など）

セキュリティ対策は要件定義段階から始まっていること、セキュリティ品質を確保する3つの活動について留意してもらってください。

・質問（問いかけ）

システムや情報機器がセキュアであることを、どうやって保証しますか？

・補足説明

・ファシリテーションテクニック

・たとえ話、小ネタ

・（ある場合は）演習の使い方・注意点・フィードバックのポイント・使用ツール

次のスライドでは、セキュリティ品質を確保する3つの活動であるセキュリティレビュー、ソースコードレビュー、セキュリティテストについて紹介しています。

セキュリティ品質の確保

- セキュリティレビュー
 - セキュリティ要件の定義書、ソフトウェア構造、業務仕様、モジュール分割の設計書、テスト計画書などをレビュー
- ソースコードレビュー
 - セキュアコーディング規約、既知の脆弱性対策、ライブラリ関数、設計にない機能の組み込み、セキュリティ機能の迂回などをレビュー
- セキュリティテスト
 - 単体テスト、結合テスト、システムテスト時に実施
 - テスト項目は設計段階に決定
 - テストの後送りは禁止
 - テストパターンは要点を絞る

セキュリティレビューは、セキュリティ対策漏れを早くに見つけ出し、設計者へフィードバックすることを目的に行います。次のような観点でドキュメント類の確認を行います。

- セキュリティ要件に対する対策漏れがないか
- 既知の脆弱性パターンに陥っていないか

ソースコードレビューは、実装工程で開発者がコーディングしたソースコードをレビューし、十分なセキュリティ対策が行われているか、あるいはセキュリティ脆弱性につながってしまう部分がないかを読み取る作業です。ソースコードレビューは次の段階を踏んで実施します。

- 下読み どこに何があるかの把握
- 成熟度点検 ある程度の品質水準に達しているか否かの評価
- 機能点検 バグ、すなわち機能面の不具合の検出
- 脆弱性点検 セキュリティ脆弱性の検出

セキュリティテストの目的は、作り上げたプログラムに十分なセキュリティ対策が実装されているかどうかを確認することにあります。次のような観点で確認します。

- 既知の脆弱性パターンに陥っていないか
- セキュリティ設計通りの実装ができていないか
- 設計工程までに検討しきれなかった脆弱性対策がないか

「要件定義」段階の考慮点

総論	開発言語の特性がもたらす問題 既存ソフトウェアの脆弱性分析 開発工程と脆弱性対策の検討
脆弱性回避策	脅威モデリングの開始
セキュリティ機能	認証、認可 暗号技術と疑似乱数の検討
不測の事態対策	ログと監査 サービス不能攻撃対策



脅威モデリングは要件定義電界から開始し、設計段階で検討します。内容や手順は2つ先のスライドで紹介します。

解説はスライドの項目のいくつかを、自らの経験と照らしていくつか紹介すれば十分です。すべてを詳しく説明する必要はありません。

既存ソフトウェアの脆弱性分析では使用する言語と、そのフレームワークやライブラリの持つ脆弱性の検討を行います。特にIoT機器の場合、提供されたライブラリが脆弱性を持つことがあるので注意が必要です。

「設計」段階の考慮点

総論	セキュリティ開発ツールの検討
脆弱性回避策	セキュリティテストの検討 脅威モデリングの検討
不測の事態対策	レースコンディション対策 メモリリーク対策
プログラム配置	構成ファイルからの情報漏洩 子プロセスからの侵害 サンドボックス
データ漏洩対策	最小の特権、パーミッション 一時ファイル コマンドライン 親切すぎるエラーメッセージ
入力検査	ユーザー入力の検査 受信ファイルの検査 環境変数の検査
出力検査	データベース操作 外部ライブラリ操作 出力のエンコード・エスケープ

Webアプリの場合だと、出力された結果が不特定多数に閲覧される可能性があります。入力検査だけでなく、ビジネスロジック処理の結果である出力の検査が重要になってきます。

設計段階より後の、実装からリリースまでの段階については次章で具体例を挙げつつ説明することを伝えてください。

脅威モデリング～STRIDE & DREAD～

- 脅威の特定
 - なりすまし (Spoofing Identity)
 - 改ざん (Tampering with data)
 - 否認 (Repudiation)
 - 情報漏洩 (Information Disclosure)
 - サービス妨害 (Denial of Service)
 - 権限昇格 (Elevation of Privilege)
- 脅威の評価
 - 潜在的損害の大きさ (Damage potential)
 - 再現性 (Reproducibility)
 - 悪用性 (Exploitability)
 - 影響を受けるユーザー (Affected users)
 - 検出可能性 (Discoverability)

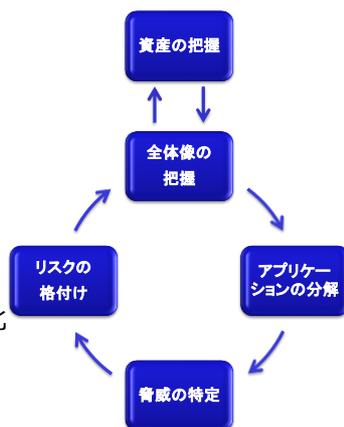
STRIDE & DREAD 脅威モデリングは、1999年にマイクロソフトが提唱した手法で、OWASPおよびIPAでも採用されています。マイクロソフトの製品群はこの脅威モデリングの下で設計されており、その効果は実地で実証されています。

<https://msdn.microsoft.com/ja-jp/library/ff648641.aspx>

https://www.owasp.org/index.php/Threat_Risk_Modeling

脅威モデリングの手順

- 資産の把握
 - 守るべき対象を確認
- 全体像の把握
 - 主要な機能や特徴を確認
- アプリケーションの分解
 - 信頼境界、データフロー、入出力の特定
- 脅威の特定
 - 本当に困ることをリスト化
- リスクの格付け
 - 資産価値×脅威×脆弱性



脅威モデリングは、情報資産、脅威、脆弱性を特定し、リスクを洗い出す作業をアプリケーションに対して行う作業となります。設計段階で脅威モデリングを行うことで、実装段階に入ってからの手戻りを最小限にとどめることができます。これはセキュリティの向上だけでなく、コスト削減や開発期間の短縮にもつながる作業となります。

セキュアシステムの設計のスライドはここまでです。実装以降は章を分けて説明します。

次のスライドからはセキュアネットワーク設計となります。

セキュアネットワーク設計

階層ごとにセキュリティを考慮

TCP/IP			OSI参照モデル	
第4層	アプリケーション層	HTTP SMTP POP3 IMAP FTP...	第7層	アプリケーション層
第3層	トランスポート層	TCP、UDP	第6層	プレゼンテーション層
第2層	インターネット層	IP	第5層	セッション層
第1層	ネットワーク インターフェイス層	イーサネット 無線LAN	第4層	トランスポート層
			第3層	ネットワーク層
			第2層	データリンク層
			第1層	物理層

ここでは復習として、TCP/IP階層モデルとOSI参照モデルの対応を提示しています。ネットワークをセキュアに保つには、各階層でどのような情報がやり取りされているかと、その情報を守る方法は何かを把握することがポイントとなります。

なお、実際の対策ではOSI参照モデルで第4層まで考慮し、TCP/IP階層モデルで第4層を考えるのが分かりやすいです。ただし、SOCKSサーバーを考えるならば、すべてOSI参照モデルで説明したほうが分かりやすいかもしれません。

ネットワークインターフェイス層

- 通信経路のセキュリティ

- 物理的接続（ケーブリング、電波）
- 暗号化



- MACアドレスセキュリティ

- MACアドレスフィルタリング
- VLAN
- ルーター/L3スイッチによるMACアドレス操作



ルーターは第3層の装置として認識されていますが、ルーティング時にMACアドレスを変換することに軽く触れ、意識付けは行ってください。ルーターにキャッシュされるMACアドレスがARPスプーフィングで汚染されている場合、ルーティング先が意図しないホストになる場合があります。

ケーブリングでは、セキュリティ対策の目的で光ファイバを用いることがあります。通信の傍受が困難で、かつ、傍受の検知が容易であるということから、短距離でも組織内の基幹通信で光ファイバを用いるケースがあります。

無線LANのアクセスポイントのセキュリティは、後半のスライドで「無線LANのセキュリティ」として別途に紹介します。

インターネット層とトランスポート層

– パケットフィルタリング

- 静的パケット・フィルタリング
- 動的パケット・フィルタリング
- ステートフル・インスペクション
 - 振り分けはインターネット層とトランスポート層の情報を使用
 - 最初の判断ではアプリケーション層の情報を使用

第3層	トランスポート層	ファイアウォール (パケットフィルタ)
第2層	インターネット層	
第1層	ネットワーク インターフェイス層	

静的パケットフィルタリングについては、ルーター上のファイアウォールとして一般的に搭載されていることを伝えればよいでしょう。

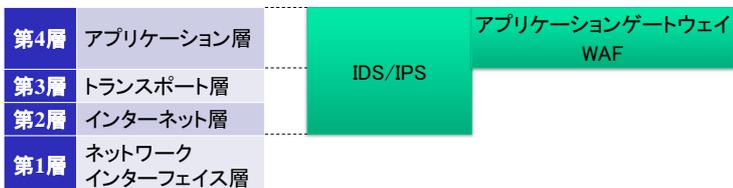
ステートフル・インスペクションは、動的パケットフィルタリングのバリエーションの一つと考えるとわかりやすいかもしれません。情報セキュリティスペシャリスト試験（平成27年秋期午前II問3）では、ステートフル・インスペクションについては以下の説明が正解とされています。

「パケットフィルタリングを拡張した方式であり、過去に通過したパケットから通信セッションを認識し、受け付けたパケットを通信セッションの状態に照らし合わせて通過させるか遮断させるかを判断する。」

通信セッションは、OSI参照モデルのセッション層、TCP/IP階層モデルのアプリケーション層の機能です。

アプリケーション層

- IDS（侵入検知システム）/IPS（侵入防御システム）
 - シグニチャーベース。難読化処理された攻撃に弱い
- アプリケーションゲートウェイ
 - アプリケーション層の情報でフィルタリング
- WAF（Webアプリケーションファイアウォール）
 - 通信を一度終端してから解析。難読化処理にも対応。



上記のシステムは全パケットに対してアプリケーション層のデータをチェックし、その結果で応答を変化させている点が、ステートフルインスペクションとの違いとなります。ステートフルインスペクションでは、まずはアプリケーション層のデータをチェックしたうえでセッションの特徴を特定し、以後はそのセッションであればアプリケーション層をすべてチェックすることなく通過/拒否を決定します。

参考 : Ethernet v2 フレーム形式



Preamble: フレームの送信を伝える。中身は101010...の繰り返し

SFD (Start Frame Delimiter): 宛先アドレスの開始を伝える。中身は10101011

DA (Destination Address): フレームの宛先MACアドレス

SA (Source Address): フレームの送信元MACアドレス

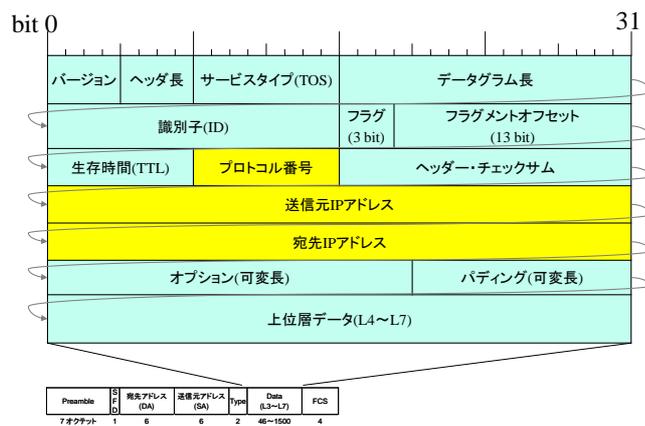
Type: 上位層の種類を伝える。IPなら0x0800、ARPなら0x0806

Data: OSI参照モデルで言う3層(例:IP)から7層(例:HTTP)のデータが収まる。

FCS (Frame Check Sequence): DAからDataまでの内容整合性をチェックするデータ。

どんなデータをチェックできるのか説明する参考資料として使ってください。詳しい説明は不要です。

参考：IPパケット形式



どんなデータをチェックできるのか説明する参考資料として使ってください。詳しい説明は不要です。

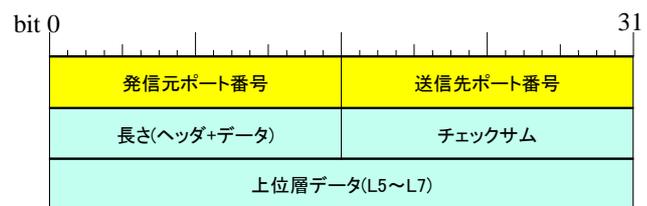
参考：TCPヘッダ形式



Preamble	S F D	宛先アドレス (DA)	送信元アドレス (SA)	Type	L3 ヘッダ [L4~L7]	Data [L4~L7]	FCS
7オクテット	1	6	6	2	46~1500	4	

どんなデータをチェックできるのか説明する参考資料として使ってください。説明の中で3-way handshakeとかクリスマスツリースキャンとか出てきた場合はフラグの説明に使えるかもしれません。ただ、詳しい説明は不要です。

参考 : UDPヘッダ形式



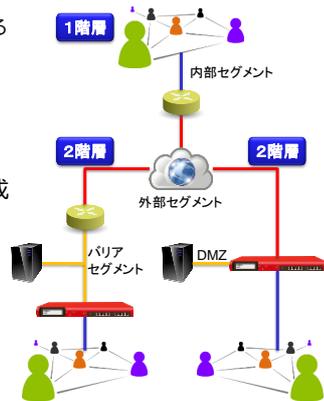
Preamble	SF	宛先アドレス (DA)	送信元アドレス (SA)	Type	L3 Data ヘッダ (L4~L7)	FCS
7オクテット	1	6	6	2	46~1500	4

どんなデータをチェックできるのか説明する参考資料として使ってください。詳しい説明は不要です。

ファイアウォールの構成

求められる信頼レベルにより構成を変える

- 1階層の防御
 - ルーター 1 台による構成
- 2階層の防御
 - バリアセグメントまたは DMZ（非武装地帯）を構成
- アドレス変換
 - セキュリティ境界で変換
 - NAT, NAPT

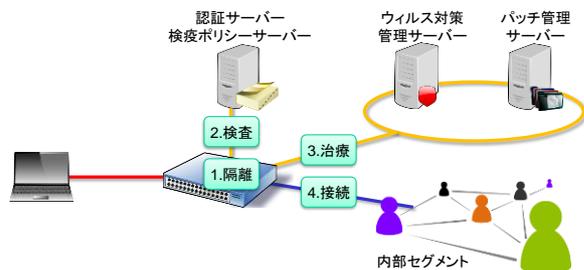


ネットワークのセキュリティ境界を意識付けしてもらえれば十分です。外部公開するサーバーがなければセキュリティ境界は内部と外部しかないので、1階層で十分です。逆に、3階層以上の多層構造となっている場合、無駄なコストをかけていないか、各ネットワークセグメントの性格について調査する必要があるかもしれません。

例えばDMZに内部のみに公開するサーバーを置き、外部アクセスをさせたくないのに3階層にするというケースがあります。この場合は内部のみに公開するサーバーは別ネットワークとし、DMZに置かなければすみます。具体的には、2階層のモデルと、別途に1階層のモデルで内部公開サーバーを接続するか、そもそもアクセス制限が不要であれば内部セグメントに接続すれば、内部公開サーバーに対する外部からの脅威の考慮を削減できます。

検疫ネットワーク

- ネットワーク接続端末を隔離し、検疫後に内部セグメント接続を許可
 1. 隔離：DHCPサーバー、認証VLANスイッチ、802.1xスイッチ
 2. 検査：認証サーバー、検疫ポリシーサーバー、資産管理システム
 3. 治療：ウイルス対策管理サーバー、パッチ管理サーバー
 4. 接続：内部セグメントへ接続



検疫ネットワークの仕組みは標準化が進み、マイクロソフトが提唱しているNAP (Network Access Protection)では、Active Directory上で検疫ポリシーを設定し、NAPに対応したウイルス対策ソフトウェアと連携することができます。また、CISCOでは独自の仕組みとしてNAC (Network Admission Control)があり、これもNAPと連携することができます。信頼できるコンピューティング環境の国際業界標準規格を制定するための非営利団体であるTCG (Trusted Computing Group)では、エージェント型の検疫ネットワークであるTNC (Trusted Network Connect) を策定し、これもまたNAPと連携できるようになっています。

認証VLAN型検疫ネットワーク

- 802.1xやWeb認証をサポートしたVLANスイッチでLANを切り替え
 - 認証時に検疫も実行
- 利点
 - 物理ポート単位で接続管理が可能
 - LANの完全な隔離
- 欠点
 - ブラウザーを使えない場合、専用クライアントソフトが必要
 - トータルの導入コストが高い

スイッチや無線LANアクセスポイントなどの、全てのネットワーク接続機器がIEEE802.1Xに対応している必要があります。そのため、既存環境によっては導入コストが非常に高くなる場合があります。新規にネットワークを構築する際に考慮するとよいかもかもしれません。最も確実にネットワークを切り離し、物理的接続ポート単位で検疫を行える検疫ネットワークは認証VLAN型です。

DHCP検疫ネットワーク

- IPアドレス割当変更でネットワークを切り替え
- 利点
 - 既存のネットワーク構成変更がほとんど不要
 - 専用エージェントが不要
 - 導入が比較的容易
- 欠点
 - 固定IPに対応できない
 - ワームやブロードキャストが防げない

たとえばWindows ServerのNAPを用いた場合、DHCPサーバーをWindows Serverで提供するだけで済みます。設定のみで検疫ネットワークを構築できる手軽さがあります。しかし、OSI参照モデルのデータリンク層は切り離されず、ブロードキャストドメインが同じであることに注意する必要があります。

エージェント型検疫ネットワーク

- クライアントPCのエージェントがネットワークアクセス制御を行う
 - 接続時にエージェントがポリシー・サーバーと通信
 - 専用プログラムやパーソナルファイアウォールなどがエージェント
- 利点
 - 既存ネットワークの変更が不要
- 欠点
 - クライアントPCへのエージェント導入が必須

TCG TNCでは、エージェントを介した検疫ネットワークの標準を策定しています。欠点としてエージェント導入が必須とはなっていますが、検疫ネットワーク接続時に強制的にエージェントを導入することもできますので、導入そのもの;には手間はかかりません。このTNC仕様に準拠していれば、例えば異なるベンダーのウィルス対策ソフトやファイアウォール設定を一括管理することも可能です。

ゲートウェイ型検疫ネットワーク

- ファイアウォールやルーターを使用
 - 通過する通信をチェックし、フィルタリングルールを動的に変更
- 利点
 - セキュリティ境界の通信すべてをチェックできる
 - 導入が比較的容易
- 欠点
 - ゲートウェイを通過しない通信に対して無力
 - 例：内部セグメントに直接接続されてしまった場合

この方式は、内部セグメントとのセキュリティ境界に新たにゲートウェイ機器を導入することで、外部セグメントからの接続を検疫する仕組みです。ブラウザ型クライアントを使用する場合、ブラウザ上で認証を受けたのち、ブラウザで動作するクライアントが検疫チェックを行い、内部セグメントへの接続を許可します。インストール型の検疫クライアントを使えばこれらの処理も自動化できます。

無線LANに対する脅威

- 主な脅威

- 無線LAN区間における盗聴
 - 暗号化機能で対処
- 他の端末からの不正接続
 - 接続端末の制限機能で対処
- 利用者端末へのなりすまし
 - 認証機能で対処
- 不正なアクセスポイントにおける盗聴
 - 認証機能と暗号化機能で対処

無線LANの脆弱性はよく話題に上りますが、そもそも何が脅威で、その脅威に対する脆弱性が何で、対策が何かをしっかりと検討していない場合を多く見かけます。ほんのわずかなポイントを抑えるだけでも、無線LANは暗号化されていない有線LANよりも安全な通信方式です。

受講生に対し、「そもそも無線LANだと何が危険だとおもいますか？」と問いかけてもよいかもしれません。大概の脅威は対策が施されています。

また、「どんなに対策しても傍受されるよね？」と問われた場合、傍受と盗聴は違うということを伝えてください。

例えば警察無線を傍受しただけで捕まることはありません。傍受した内容に対し何らかのアクション（例：通信内容の記録、通信内容の）をとった場合に電波法違反が問われることがあります。そもそも適切に通信が暗号化されており、認証が設定されていれば、盗聴には失敗します。あくまでも「盗聴を防ぐ」という観点で無線LANを考えるように伝えてください。傍受そのものには違法性はありません。

参考：電波法

第五十九条 何人も法律に別段の定めがある場合を除くほか、特定の相手方に対して行われる無線通信（電気通信事業法第四条第一項又は第百六十四条第三項の通信であるものを除く。第百九条並びに第百九条の二第二項及び第三項において同じ。）を傍受して**その存在若しくは内容を漏らし、又はこれを窃用してはならない。**

第百九条の二 暗号通信を傍受した者又は暗号通信を媒介する者であつて当該暗号通信を受信したものが、当該暗号通信の**秘密を漏らし、又は窃用する目的で、その内容を復元した**ときは、一年以下の懲役又は五十万円以下の罰金に処する。

無線LANセキュリティ機能

- 接続制限機能
 - SSID
 - MACアドレスフィルタリング
- 認証機能
 - IEEE802.1x
 - RADIUS + EAP
 - PSK (Pre-Shared Key)
- 暗号化機能
 - WPA2
 - AES暗号の実装であるCCMP暗号化を使用
 - IEEE802.11iの実装
 - WPA3
 - IoT機器の増加を想定
 - 容易な設定と、鍵交換プロトコルの強化

重要な点として、認証機能を有効にし、WPA2を有効にすることを示してください。WPA2で採用された、AES暗号の実装であるCCMP暗号化（Counter-mode CBC-MAC Protocol）は、上記の暗号化機能の中では最も強固なセキュリティ実装となります。

WPA/WPA2のPSK（俗にパスワードとか呼ばれることもある）を使った認証はホームモードと呼ばれることもありますが、すべてのユーザーで同じPSKを使用するため、だれが接続したのかが追跡できません。組織や企業では極力認証サーバーを用いるべきです。

WEP暗号解読の現実的な手法を、神戸大学と広島大学のグループが2008/10/9のCSS2008（コンピュータセキュリティシンポジウム2008）において発表および実演を行いました。その結果だと、10秒程度でWEPは解読されています。WPA-TKIPについても同じツールで7分ほどでパスワードを解析できています。このツールの名前は仮称KOBECRACKと呼ばれますが、2017年末の時点では非公開となっています。要望があれば、いつでもでもおよび実演は行うとのこと。なお、Kali-Linuxに含まれているaircrack-ngを用いた場合でも数十分から数時間で解析可能です。

無線LANの接続性

電波の到達範囲を意識する

- 電波干渉
 - IEEE802.11b/g/n で 4 つ以上のアクセスポイントが検出される場合は干渉が起きている
 - {1/6/11}, {2/7/12}, {3/8/13}, {4/9/14}, {5/10}の3ないし2チャンネルの組合せまであれば干渉しない
 - IEEE802.11aは干渉しない。
- 受信レベル制御
 - 送信レベルを上げず受信レベルを上げれば電波干渉を回避
- アンテナ設置
 - 電波が必要範囲に到達していない場合、室内アンテナ設置で対処可能
 - 管理外の電波により電波干渉が生じている場合、室内アンテナ設置と送信レベルを上げることで対処可能（非推奨）
 - 管理外アクセスポイントが隣接する場合や、ISM帯を使用する機器が隣接する場合など。

送信レベルを上げるということは、他の無線LANへの干渉を増長するうえ、管理区域外まで電波が届くことになり盗聴の危険性が高まります。直進性の高く遮蔽しやすい5GHz帯の電波を使えば、管理区域外からの電波を軽減できるだけでなく、他の無線LANへの干渉も抑えられます。ただし遮蔽物に弱いため、可能であれば見通しの良い位置にアクセスポイントを置く必要があります。

ISM (Industry Science Medical)帯は本来無線通信用ではなく、産業科学医療用に用いられる電波帯です。周波数割当計画脚注J37によると、「この周波数帯で運用する無線通信業務は、これら（産業科学医療）の使用によって生じ得る有害な混信を容認しなければならない」とあります。2.4GHz帯を用いる無線LANは、このISM帯の電波を用いているため、混信は許容しなければなりません。

IoTセキュリティ設計の課題

- IoTもインターネットシステムとしてはパソコンと変わらない。
 - 対策はパソコンと同様のことを想定。
- IoT固有の課題が対応を困難にする。
 1. ネットに繋がる脅威をこれまで考慮してなかった分野の機器の接続が想定される
 2. 生命に関わる機器やシステムが繋がることが想定される
 3. 「モノ」同士が、無線等で自律的に繋がることが想定される
 4. 「モノ」のコストの観点から、セキュリティ対策が省かれることが想定される
 5. ネットを介して収集される情報の用途は、「モノ」側では制御が困難であり、バックエンドにあるシステムやクラウドサービス側での管理範囲となる
 6. つながる世界を拓いていくためには、「モノ」同士の技術的（通信プロトコル、暗号、認証等）、およびビジネス的な約束事が不可欠となる

IoT製品やサービスのセキュリティ設計の基本も、パソコン上で動作する情報システムと変わりません。

IoT のセキュリティ設計

IoT 製品やサービスのセキュリティ設計を行う場合は、以下の手順で実施

- 情報資産の明確化
 1. 対象とする IoT 製品やサービスのシステム全体構成を明確化
 2. システムにおいて、保護すべき情報・機能・資産を明確化
- 脅威分析
 3. 保護すべき情報・機能・資産に対して、想定される脅威を明確化する。
- 対策検討
 4. 脅威に対抗する対策の候補（ベストプラクティス）を明確化
 5. どの対策を実装するか、脅威レベルや被害レベル、コスト等を考慮して選定

システムの全体構成を明確化します。そして、そのシステムにおいて保護すべき情報資産を明確化します。

明確になった情報資産に対し、想定される脅威を明確化します。ここで脅威モデリングを用いることもできます。

脅威を明確にしたのち、どのような対策があるかのベストプラクティスを明確化します。

最後にリスクを評価して、どの対策を実装するのかを選定します。

4-2. セキュアシステム、ネットワークの設計 ～グループ演習～

演習3 セキュアシステム、ネットワークの設計 - 脅威モデリング



仮想マシンの基本情報は以下の通りです。

仮想マシン名 mutillidae
Kali-Linux

IPアドレス 192.168.33.10/24
192.168.33.11/24

ログイン対象 Linux MySQL
Linux

アカウント vagrant root
root

パスワード vagrant
my_password toor

第5章 セキュア開発概説

Webアプリを例とし、アプリケーション内のセキュリティ境界を説明できる。

Webアプリのリスクのトレンドを追えるようになる。

Webアプリの脆弱性を検出する方法を説明できる。

5-1. ソフトウェア開発、ウェブサイト設計

- (1) 実装原則
- (2) Webアプリケーションの機能と脆弱性
- (3) OWASP Top 10 - 2017
 - ① 1.インジェクション
 - ② 2.認証の不備
 - ③ 3.機密データの露出
 - ④ 4.XML外部エンティティ (XXE)
 - ⑤ 5.アクセス制御の不備
 - ⑥ 6.セキュリティ設定のミス
 - ⑦ 7.クロスサイトスクリプティング (XSS)
 - ⑧ 8.安全でないシリアル化解除
 - ⑨ 9.既知の脆弱性を持つコンポーネントの使用
 - ⑩ 10.不十分なログと監視



実装原則

安全なコーディング実装 (SEI CERT Top 10 Secure Coding Practices, 2011)

1. 入力を検証する
2. コンパイラの警告を無視しない
3. セキュリティポリシーに従った構成と設計
4. シンプルにする
5. 拒否を基本とする
6. 最小特権の原則に従う
7. ほかのシステムに送るデータを無害化する
8. 徹底した防御対策（多層防御）を行う
9. 効果的な品質保証技術を使用する
10. 安全なコーディング規約を採用する

出力チェックを
忘れない！

IPAが提供するセキュアプログラミング講座でも同じ実装原則を提示しています。ただし順番が異なっているため、このスライドではオリジナルに合わせた順番にしています。

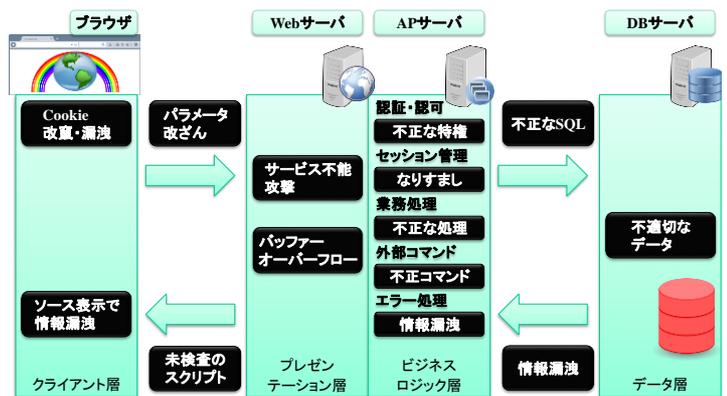
<https://wiki.sei.cmu.edu/confluence/display/seccode/Top+10+Secure+Coding+Practices>

「多層防御」について補足です。セキュリティが考慮されない頃のプログラミング原則として、同じ処理は一度のみ実行するというものがあります。この考え方は多層防御と真逆の考え方ですが、セキュリティを考慮した場合は入力時、ビジネスロジック処理の前後、他のシステムに送るデータの無害化などで同じ処理を複数回実行することで安全を保ちます。例えば、スクリプトをエスケープする処理は、ビジネスロジックの文字列連結前後で実行する必要があります。

実装原則の基となる考え方は、「すべての外部入力は信用できず、すべての出力は確実にする」という考え方です。この考え方は、すべてのプログラミング言語に当てはまります。一つずつ細かく説明できる時間があればよいのですが、この「入力と出力を確実にする」という考え方の根本に触れればとりあえずは十分です。

Webアプリケーションの機能と脆弱性

問題の多くはセキュリティ境界で発生



- 97 -

CSAJ

実装原則があっても、どこで適用するかが問題となります。漫然と「すべてのプログラム」では、対策も検証も困難です。本スライドで提示する分類の中で、実装原則が保たれているか検証することで、対策の抜けや漏れを少なくできます。14か所のセキュリティ境界を提示していますが、ほとんどのWebアプリではこの14か所で必要十分です。

OWASP Top 10 - 2017

The Ten Most Critical Web Application Security Risks

基本的には効果的な対策から実施していく

1. インジェクション
2. 認証の不備
3. 機微な情報の露出
4. XML外部エンティティ参照 (XXE)
5. アクセス制御の不備
6. 不適切なセキュリティ設定
7. クロスサイトスクリプティング (XSS)
8. 安全でないシリアル化解除
9. 既知の脆弱性のあるコンポーネントの使用
10. 不十分なロギングとモニタリング

3つについて
解説します

脆弱性の上位10傑はスライドの通りですが、脆弱性の対策は上位の10傑だけで終わらせないように注意してください。たとえば1つ前のバージョンである2013年版に上位に入っていた脆弱性である「クロスサイトリクエストフォージェリ(CSRF)」は、フレームワークレベルで対応するようになりましたが、設定のミスによって表出します。また、「未検証のリダイレクトとフォワード」は、XML外部エンティティの脆弱性の一部としていまだにWebアプリの8%で発見されています。

OWASP Top 10 2017 日本語版が2017/12/26にリリースされました。その中で、A8として「安全でないデシリアライゼーション」となっていますが、本稿では「安全でないシリアル化解除」としました。

1.インジェクション

未検証のユーザー入力が各種命令に紛れることで悪意のある攻撃を行う

- 入力を変換するか、パラメータ化するインターフェースを持つ安全なAPIを選択する
- ホワイトリスト方式のサーバー側入力検証
 - ただし、特殊な文字入力を許すアプリケーションでは必ずしも効果的ではない
- 動的に命令を作成する場合、特殊文字をエスケープ処理
 - パラメータ化できないSQLのテーブル名や列名など
- SQLインジェクションの場合、大量のデータ開示を避けるための制御を行い、制限を設ける
- WAF (Web Application Firewall)を使用する

インジェクションにはSQL, NoSQL, OS, LDAPなどを含みます。

SQLインジェクション攻撃については1998年12月25日にJeff Forristal氏(rain.forest.puppy氏)によって、Windows NTのWeb技術の脆弱性として初めて指摘されました（<http://phrack.org/issues/54/8.html>）。以後、近年に至るまでWebアプリの脆弱性として常に上位を占めています。

WAFの導入は、アプリ自体を更新できない時の対策です。WAFによる仮想パッチに頼ることはしないようにします。

2. 認証の不備

ユーザーの識別、認証、セッション管理は、認証関連の攻撃に対する防御で重要

- 可能なら多要素認証を実装する
- デフォルトの資格情報は使用しない（管理者は特に）
- 脆弱なパスワードのチェック
- 根拠あるパスワードポリシーを作成して従わせる
- アカウントリスト攻撃に備え、登録時や資格情報復元時、そしてAPIによる操作を厳密に確認する。
- ログイン失敗回数の制限、リトライ時間の延長。
- ログイン失敗を記録し、資格情報の詰め込みやブルートフォースなど攻撃の場合は管理者に通知する
- ログイン後に無作為なセッションIDを生成する、安全かつ埋め込み済みのセッション管理機能をサーバー側で使用する
- セッションIDはURLに埋め込まず、安全に保管し、ログアウト後やタイムアウト後に破棄する

アカウントセキュリティの3要素として、認証、認可、アカウントイング（ログと監査）がありますが、本10傑ではそれぞれの脆弱性を分けて考えています。これに対し、日本語では認可（Authorization）の訳語がもともとなかったことでもわかるように、認証はしても、認可は全員一緒というシステムが多く見受けられました。認証すら、全員同じアカウントというケースも多く存在します。セキュリティ対策時も認証、認可に加え、識別（Identify）も混同しないように注意すべきです。

※ Authorization の訳語は認定、認可、許可、などベンダーによって様々ですが、JIS X 0008:2001 では、「認可」として定義されています。

3. 機微な情報の露出

必要だが今使っていない機密データが安全であるか

- 処理、保管、転送するデータを分類し、分類ごとに制御
- 不必要な機密データを保管しない
- 今使用していない機密データが暗号化されているか
- 標準アルゴリズムやプロトコルが最新かつ強力か、鍵が適切な場所にあるか
- 転送時に安全なプロトコルで暗号化されているか
- 機密データを含む応答のキャッシュを無効化
- 状況に応じて適切なソルト付きハッシュ関数を使う
- 構成や設定の効果を別途に検証

機密データの露出については、まずは情報資産台帳を作ること
で対策を取りやすくなります。

「ソルト」という言葉で疑問を持つ受講者もいると思いますが、もとは「味付け」くらいの意味です。機密データ（例えばパスワード）の前後に付加するデータがソルト、そしてソルト値です。パスワードの保存でハッシュ関数を使いますが、単なるハッシュだとレインボークラックで解読される可能性があります。ユーザごとに異なるある程度の長さのデータをパスワードの前後に付加してハッシュ関数にかけることで、レインボークラックによる解読を困難にすることができます。なお、ソルト値は乱数である必要は必ずしもありません。また、ソルト値は機密情報である必要はなく、パスワードハッシュとともに保存しても構いません。

4.XML外部エンティティ参照 (XXE)

XML処理における外部実体（エンティティ）参照を利用し、ファイルや情報を不正に取得する

- 開発者のトレーニングが不可欠
- 可能ならJSONのようなより単純なデータ書式を使用し、さらに、機密データはシリアル化しないようにする
- アプリケーションで使うXML処理やライブラリを修正更新する
- アプリケーションで使うすべてのXMLパーサーでXML外部実体参照とDTD処理を無効化する
- XMLホワイトリストによるサーバー側の入力検証、フィルタリング、そして無害化
- 根本的な対策が難しい場合、WAFによる検出、監視、防御を検討

信頼できないソースからのXMLドキュメントを受け入れることで発生する脆弱性です。XML解析処理を経て攻撃が成立します。

例として、シングルサインオン(SSO)でSAMLを使う場合はXMLを使用しているため、IDの処理に脆弱性が発生する可能性があります。

5. アクセス制御の不備

信頼できるサーバー側のコードやAPIでのみアクセス制御可能

- 既定のアクセス許可を「拒否」にする
- ドメインをまたがったリソース共有(CORS)も含め、一度実装したアクセス制御機能を一貫して使用する（必ずその機能を通す）
- レコードの所有者が持つべきアクセス制御を強制する
- ディレクトリ参照やメタデータの確認を無効化し、ファイルのバックアップをWebルートに置かない。
- アクセスログをとり、適時に管理者に報告
- 自動攻撃の被害を最小限にするための、アクセス速度を制限するAPIと制御
- ログアウト後にJWT (JSON Web Token)も無効化する

アクセス制御機能の悪用は、攻撃者が攻撃の初期段階で必ず試みます。

静的アプリケーションセキュリティテスト(SAST)や動的アプリケーションセキュリティテスト(DAST)を用いても、アクセス制御機能が有効に機能しているかの検証はできないため、(フレームワークに自動チェック機能がなければ) 手作業で不備を発見する必要があります。

CORS: Cross-Origin Resource Sharing

6.不適切なセキュリティ設定

一貫した、繰り返し可能なセキュリティ設定プロセスを設ける

- 適切に機能制限されたアプリケーションを、素早く簡単に異なる環境に展開できるようにする。この手順は自動化できることが望ましい。
- 不要な機能を排した最小限の動作環境
- バッチ管理の一環として設定のレビューと更新を行う
- コンポーネント間やテナント間を効果的かつ安全に分離するセグメント化アプリケーション設計を用いる
 - たとえばセグメント化、コンテナ化、クラウドのセキュリティティグループを用いる
- クライアントに対してセキュリティ指示を出す
 - たとえばセキュリティヘッダーを用いる
- 全ての環境で、構成や設定が機能しているか検証するプロセスを自動化

セキュリティ設定そのものが攻撃されるわけではなく、セキュリティ設定の不備によって攻撃可能な脆弱性が残ってしまうことが問題です。一般論として、使わない機能のメンテナンスはおろそかになるため、脆弱性が残りやすくなります。

脆弱性の例として、サンプルアプリ経由の攻撃、ディレクトリ一覧が有効なままで情報漏洩、詳細なエラーメッセージが有効なままだったりトレース機能が有効だったり。

デフォルトの設定は脆弱であると認識して対応すべきです。

7.クロスサイトスクリプティング (XSS)

攻撃対象はユーザーのブラウザ

- XSSを自動的に排除するフレームワークを使用する
 - 最新の Ruby on Rails や React JS など
 - 各フレームワークの限界も考慮する
- 信頼できないHTTP要求のエスケープ処理
- コンテンツセキュリティポリシーを有効にすることが、XSSに対する制御を緩和する多重防御となる。
 - 信頼できるコンテンツ参照元のホワイトリスト
 - ディレクティブの制限
 - インラインのスクリプトは禁止し排除
 - eval関数

一般的には、攻撃対象はユーザーのブラウザであることを押さえておきます。ただし、ブラウザのスクリプトエンジンに脆弱性が存在する場合、ユーザーのコンピュータそのものが攻撃対象になることもあります。

ユーザー入力やリンクに悪意あるスクリプトがある場合、最低でもHTML出力時にエスケープ処理をすれば被害は防げます。しかし、悪意あるスクリプトがそのままデータベースやメモリに保存されると、攻撃の成功確率が高くなります。ユーザー入力は信用できないものとして、必ず入力時にもエスケープ処理を行います。

8.安全でないシリアル化解除

シリアル化解除で、悪意ある、または改ざんされたオブジェクトが渡される

- 信頼された送信元からのシリアル化データのみ受け取る
- シリアル化は基本データ型に限定する
- 電子署名でシリアル化データの整合性をチェックする
- シリアル化解除の前に、定義済みのクラスからオブジェクトを生成し、データ型に制約をかける
- 可能なら、シリアル化解除のコードは低い権限で実行する
- シリアル化解除の例外や失敗はログに残す
- シリアル化解除を行うサーバーやコンテナのネットワーク接続の入出力を制限し、監視する
- あるユーザーが定期的にシリアル化解除を行っているようであれば、シリアル化解除を監視し、アラートを上げる

この脆弱性の悪用は困難なため、スクリプトキディレベルで使用されることはないでしょう。しかし一度悪用されれば、アプリケーション内部のデータを改ざん可能なため、深刻な被害が予想されます。

オブジェクトのシリアル化は、通信時やデータの保存時に行われ、盗聴や改ざんが可能な状況に置かれます。そこで、暗号化や電子署名を用いたり、そもそも機微な情報をシリアル化せず基本データ型のみシリアル化して型チェックを厳密に行うことで深刻な被害を防ぐことができます。

9.既知の脆弱性のあるコンポーネントの使用

「そのアプリは脆弱じゃないですか？」と聞かれて答えられるか

- 未使用の機能、コンポーネント、ファイル、文書を削除
- クライアント側とサーバー側で、使用コンポーネントと関連コンポーネントのバージョンを継続的に管理する
 - CVEやNVDやJVNとの突き合わせを行う
- 安全な接続を介し、公式リソースからコンポーネントを入手する
- メンテナンスされていない、またはバージョンが古くセキュリティパッチが提供されていないライブラリやコンポーネントの監視
 - パッチが適用できない場合、仮想パッチを適用する

既知の脆弱性に対する攻撃手法は公開されていることが多く、悪用も比較的簡単です。脆弱性の種類によりリスクの大きさも変わりますが、そのリスクが自組織の情報資産の場合は大きくなるということもあります。システム内部でどのようなコンポーネントを使っているか洗い出すことから始めます。

10.不十分なロギングとモニタリング

対応すべきインシデントはいつ発生するかわからない

- 全てのログイン、アクセス制御失敗、サーバー側の入力検証失敗が、疑わしいあるいは悪意あるアカウントか識別する十分なユーザー情報とともに記録されているか確認
- 集中的なログ管理ソリューションによって扱えるログ形式か
- 改ざんや削除を防止する整合性制御を備えた高価値なトランザクションを必要とするのが監査証跡
- 時勢にあった、効果的な監視とアラートを採用する
- インシデント対応計画と復旧プランを策定または採用する

ログが十分かどうかは、一通りの脆弱性対策を終えてから実際に侵入テストを行い、侵入がモニタリングできているか、ログからどのような侵入が行われたかを調査できるか試すのが一番確実です。

5-2. セキュアプログラミング～グループ演習～

演習 4 手動によるWebアプリケーションの脆弱性チェック

演習 5 ツールを使ったWebアプリケーションの脆弱性チェック



時間が許せば、手動による脆弱性チェックは自力で考えてほしいところです。難しいようであれば先に解答例を渡し、解答例通りに手動チェックができる体験をしてもらえれば十分です。

ツールを使った脆弱性チェックは待ち時間が長いため、待ち時間の間に講義を進めてください。

第6章 倫理・コンプライアンスの概念

コンプライアンスが重要視される背景を説明できる。

コンプライアンス違反がもたらす結果を指摘できる。

コンプライアンスを守らせる方法を指摘できる。

6-1. 倫理・コンプライアンスの概念

- (1) 組織における内部不正防止
- (2) 内部不正を防ぐ10の観点
- (3) コンプライアンスとは
 - ① コンプライアンス遵守対策
 - ② コンプライアンス～法的手続きの整備～
 - ③ コンプライアンス～誓約書の要請～



組織における内部不正防止

5つの基本原則（IPA「組織における内部不正防止ガイドライン」より）

- 犯行を難しくする（やりにくくする）
 - 対策を強化することで犯罪行為を難しくする
- 捕まるリスクを高める（やると見つかる）
 - 管理や監視を強化することで捕まるリスクを高める
- 犯行の見返りを減らす（割に合わない）
 - 標的を隠したり、排除したり、利益を得にくくすることで犯行を防ぐ
- 犯行の誘因を減らす（その気にさせない）
 - 犯罪を行う気持ちにさせないことで犯行を抑止する
- 犯罪の弁明をさせない（言い訳させない）
 - 犯行者による自らの行為の正当化理由を排除する

正当な手段で利益が得られるのに、わざわざ犯行を犯すことはありません。まずは「犯行が割に合わない」ことを徹底します。しかし実際には、犯行はハイリスクハイリターン割の良い行動です。米セキュリティ企業Trustwave社より、マルウェア攻撃による犯罪の投資対効果(ROI)は1425%にも及ぶというレポートが2015年6月9日に公開されました（New Trustwave Report Reveals Criminals Receive 1,425 Percent Return on Investment from Malware Attacks）。そこで、上記の5つの原則すべてを考慮する必要があります。

内部不正を防ぐ10の観点

1. 基本方針
2. 資産管理
3. 物理的管理
4. 技術・運用管理
5. 証拠確保
6. 人的管理
7. コンプライアンス
8. 職場環境
9. 事後対策
10. 組織の管理

内部不正発生時の事後の
法的手続きを考慮すると、
この3つは外せない！

・説明の流れ

全ての観点で対策が必要なのではないですが、内部不正発生時の事後の法的手続きを考慮すると、資産管理、人的管理、コンプライアンスについての対策は必須と考えてください。

・ポイント（絶対に覚えてほしいこと、など）

コンプライアンスは、内部不正を防ぐ観点の一つに過ぎないこと。
。内部不正を防ぐ観点からは、考慮すべき観点がほかにもあることを忘れない。

コンプライアンスとは

- 企業が経営活動を行う上で、各種規則などや法令など、さらには社会的規範などを守ること。
 - 「法令遵守」だけではない。
 - 社内規定、社会通念、倫理、道徳の遵守も含まれる。
- コンプライアンスは倫理規定に裏打ちされる必要がある。



・説明の流れ

どんな規定であっても、非倫理的なものは認められません。
倫理規定については次のスライドで、倫理原則として示します。

・ポイント（絶対に覚えてほしいこと、など）

「法令順守」だけではないこと。社内規定、社会通念、倫理、道徳の遵守もコンプライアンスに含まれる。

ルールを守っているから良い、ルールの抜け道に過ぎない、では済まされないのがコンプライアンスであること。

倫理規定

- 情報セキュリティ支援業務を行う者が守るべき5つの倫理原則
- 1. 全てのプロフェッショナルおよび業務との関係において、嘘をつかず、誠実でなければならず、専門的な基準および事実とデータに基づいたサービス提供を誠実に行わなければならない。
- 2. 業務上の判断は、偏見、利益相反、他者の過度の影響を受けず、常に客観的に行われなければならない。
- 3. 顧客または雇用者に現在の技術発展レベルと法律に基づいたプロフェッショナルサービスを提供するために必要なレベルの、専門知識とスキルを維持しなければならない。
- 4. 専門的、業務上知り得た情報の機密性を、法的または専門的な権利または開示義務が無い限り、厳守しなければならない。
- 5. 注意深く行動し、信用を損なってはならない。

・説明の流れ

このスライドの説明は流してもらっても構いません（このスライドは最後に再登場します）が、専門家として「事実に基づく」「客観的」な判断、個人の感情や想像、ポリシーを加えないことが大事であることは伝えてください。

・ポイント（絶対に覚えてほしいこと、など）

事実に基づく。客観的な判断。スキルの維持。機密の厳守。信用を損なわない。

コンプライアンス遵守対策

- 2つの観点で対策
 - 法的手続きの整備
 - 内部不正を犯した内部者に対する解雇等の懲戒処分を考慮し、就業規則等の内部規程を整備し、正式な懲戒手続に備える。
 - 誓約書の要請
 - 役職員に対して重要情報を保護する義務があることを理解させるため、「秘密保持誓約書」等の提出を要請する。

・説明の流れ

ルールを守らせるためには、ルールがなければならない。そして、ルールがあることを伝えないといけない。ごくごく普通の話として理解させてもらいたいところです。

・ポイント（絶対に覚えてほしいこと、など）

規定のあと出しにならないよう、最初に規定を整備し、提示する必要があること

コンプライアンス～法的手続きの整備～

- 内部規程において懲戒処分及び秘密保持義務に関する項目を定めておく
 - 懲戒処分の対象となる内部不正に関する記載
 - 秘密保持義務の対象となる重要情報を客観的に特定できる記載
 - 懲戒処分の根拠となる内部規程および労働法制
 - 適切な懲戒処分を決定するための、査問委員会等による事実関係の明確化
 - 刑事告発及び民事訴訟の法的な手続きに関する内部規程の整備

・説明の流れ

内部規定に含める項目をさっと見てもらえれば構いません。

・ポイント（絶対に覚えてほしいこと、など）

最終的には法的手続きの際に必要な規定を定めておきます。

コンプライアンス～誓約書の要請～

- 秘密保持誓約書の提出がないと、重要情報を保護する義務があることの意識付けができない恐れがある
 - 秘密保持の対象となる重要情報を客観的に特定できる記載
 - 入社時以外にも特定の機会に誓約書を要請することが望ましい

・説明の流れ

ルールを作ったら、ルールを守る、という誓約書がなければ意味がなくなります。法的な手続きの根拠にするためにも必須な要請です。

・ポイント（絶対に覚えてほしいこと、など）

誓約書の要請は、機会があるごとに行う必要があること。

6-2. 基本的な考え方

(1) リーガルコンプライアンスポリシー

- ① ルールを守った行動をとる
- ② 情報を適切に保護・管理する
- ③ 関係者との健全な関係を保つ

(2) 関連する法律・ガイドライン

- ① 刑法 第二編第十九章の二 不正指令電磁的記録に関する罪
- ② 刑法 第二編第三十五章 信用及び業務に対する罪
- ③ サイバーセキュリティ基本法
- ④ 著作権法の一部を改正する法律
- ⑤ 特定電子メールの送信の適正化等に関する法律
- ⑥ 不正アクセス行為の禁止等に関する法律



リーガルコンプライアンスポリシー

情報セキュリティを実践する高度情報処理技術者として守るべきポリシー

1. 社会の一員としてルールを守った行動をとること
2. 情報を適切に保護・管理すること
3. 業務に際し関係者との健全な関係を保つこと



・説明の流れ

倫理規定を前提とし、その中で法令遵守が必要であるというイメージです。

1. ルールを守った行動をとる

- 法律及び社会規範を遵守すること
- 自らあるいは他者に示唆され脱法/違法行為を行わず、他者にそれを示唆せず、命じないこと
- 業務をルールに基づき誠実に実行すること



・説明の流れ

組織の規定の上位に、法律と社会規範があります。組織の規定が法律と社会規範に違反している場合、法的手続きの際に当該組織の規定が違法であると判断されます。

・ポイント（絶対に覚えてほしいこと、など）

法律と社会規範に違反しない範囲で、組織の規定に基づき業務を遂行すること。

2. 情報を適切に保護・管理する

- 業務を通じて取得した情報を、関連法や規則を遵守し厳重に管理すること
- 高度な情報セキュリティ環境を構築し、安全な通信環境を提供すること
- 個人情報の保護規定を厳正に遵守すること



・説明の流れ

いわゆる情報セキュリティの話です。個人情報に囚われがちですが、組織として重要な情報はほかにもあります。特許申請前のアイデア、設計、組織の体制や機密の所在など。ここでも情報資産の棚卸、明確化が必要となります。

・ポイント（絶対に覚えてほしいこと、など）

個人情報に限らず、業務で取得した情報の厳重な管理。組織の規定や関連法案の遵守。

3. 関係者との健全な関係を保つ

- 反社会的勢力とは取引を行わないこと
- 取引先との間に公正かつ自由な関係を維持し、不当な要求を行わないこと
- 第三者の知的財産権を尊重し、適切な利用を行うこと



・説明の流れ

間接的かつ不当に他者を貶める行為は、結果として業界の健全な競争や発展を阻害し、社会の発展を妨げることになります。「自組織さえよければよい」という考え方は、結果的に自組織の属する社会の首を絞めることになります。

・ポイント（絶対に覚えてほしいこと、など）

短期的な利益にとらわれないこと。

関連する法律・ガイドライン

総務省「情報セキュリティ関連の法律・ガイドライン」を参照

- 刑法
- サイバーセキュリティ基本法
- 著作権法
- 電気通信事業法
- 電子署名及び認証業務に関する法律
- 電子署名等に係る地方公共団体情報システム機構の
認証業務に関する法律
- 電波法
- 特定電子メールの送信の適正化等に関する法律
- 不正アクセス行為の禁止等に関する法律
- 有線電気通信法

・説明の流れ

情報セキュリティに関する法律は徐々に整備されており、一方の法律の抜け穴を別の法律が埋めるような形になっています。コンプライアンス規定を作成する際のガイドラインとしても機能します。

・ポイント（絶対に覚えてほしいこと、など）

各法律の概要。この講座では、赤文字で示した内容だけさつと紹介します。

刑法 第二編第十九章の二 不正指令電磁的記録に関する罪

(不正指令電磁的記録作成等)

第百六十八条の二 正当な理由がないのに、人の電子計算機における実行の用に供する目的で、次に掲げる電磁的記録その他の記録を作成し、又は提供した者は、三年以下の懲役又は五十万円以下の罰金に処する。

一 人が電子計算機を使用するに際してその意図に沿うべき動作をさせず、又はその意図に反する動作をさせるべき不正な指令を与える電磁的記録

二 前号に掲げるもののほか、同号の不正な指令を記述した電磁的記録その他の記録

2 正当な理由がないのに、前項第一号に掲げる電磁的記録を人の電子計算機における実行の用に供した者も、同項と同様とする。

3 前項の罪の未遂は、罰する。

コンピュータウイルスに関する罪

・説明の流れ

刑法の中から、情報セキュリティに関連する項目をいくつか紹介しています。このスライドの刑法は、いわゆる「コンピュータウイルスに関する罪」のことです。

・ポイント（絶対に覚えてほしいこと、など）

「未遂」も罰する規定となっています。

刑法 第二編第三十五章 信用及び業務に対する罪

(信用毀損及び業務妨害)

第二百三十三条 虚偽の風説を流布し、又は偽計を用いて、人の信用を毀損し、又はその業務を妨害した者は、三年以下の懲役又は五十万円以下の罰金に処する。

(威力業務妨害)

第二百三十四条 威力を用いて人の業務を妨害した者も、前条の例による。

(電子計算機損壊等業務妨害)

第二百三十四条の二 人の業務に使用する電子計算機若しくはその用に供する電磁的記録を損壊し、若しくは人の業務に使用する電子計算機に虚偽の情報若しくは不正な指令を与え、又はその他の方法により、電子計算機に使用目的に沿うべき動作をさせず、又は使用目的に反する動作をさせて、人の業務を妨害した者は、五年以下の懲役又は百万円以下の罰金に処する。

2 前項の罪の未遂は、罰する。

・説明の流れ

セキュリティインシデントがほかの法律に抵触しなくても、最終的に「信用棄損及び業務妨害」に該当すれば、罰することができます。セキュリティ侵害行為そのものを罰せなくても、侵害行為の結果から攻撃者を罰することができるようになっています。

・ポイント（絶対に覚えてほしいこと、など）

この規定でもやはり「未遂」は罰します。

サイバーセキュリティ基本法

サイバーセキュリティに関する施策を総合的かつ効率的に推進するため、基本理念を定め、国の責務等を明らかにし、サイバーセキュリティ戦略の策定その他当該施策の基本となる事項等を規定

(国民の努力)

第九条 国民は、基本理念にのっとり、サイバーセキュリティの重要性に関する関心と理解を深め、**サイバーセキュリティの確保に必要な注意を払うよう努めるものとする。**

・説明の流れ

この法律は、「国民の努力」となっています。実際には教育によってセキュリティの確保に注意を払わせるべきなのですが、まだまだこれからでしょうか。

・補足説明

経験談として、30代の社会人が組織内資料を自由閲覧（および編集！）できる状態にしていた。指摘したうえで、何が問題になるか考えさせたところ、「（組織内資料を）自由に閲覧編集できて何が悪いのですか」との回答があった。問題となるケースをいくつか示して納得はしたようだが、そもそも想像力が働いていない模様（ここでは情報漏洩や改ざんによる影響）。セキ

ユリティ対策以前に、何が問題となるかの理解がそもそもできていない状況が少なからずあります。

著作権法の一部を改正する法律

本法律は、一部の規定を除いて、平成25年1月1日に施行

著作権等の保護の強化

①著作権等の技術的保護手段に係る規定の整備

現行法上、**著作権等の技術的保護手段**の対象となっている保護技術（VHSなどに用いられている「信号付加方式」の技術。）に加え、新たに、**暗号型技術**（DVDなどに用いられている技術）についても技術的保護手段として位置づけ、**その回避を規制するための規定**を整備。

②違法ダウンロード刑事罰化に係る規定の整備

私的使用の目的で、有償で提供等されている音楽・映像の著作権等を侵害する自動公衆送信を受信して行う録音・録画を、自らその事実を知りながら行うこと（**違法ダウンロード**）により、著作権等を侵害する行為について**罰則を設ける等の規定**を整備。

ダウンロード違法化

・説明の流れ

著作権法も情報（ここでは音楽・映像コンテンツ）そのものに適用できるよう、強化されています。

・ポイント（絶対に覚えてほしいこと、など）

いわゆる「ダウンロード違法化」の規定の存在。暗号型技術の回避を規制するための規定も整備されているという現状。

特定電子メールの送信の適正化等に関する法律

利用者の同意を得ずに広告、宣伝又は勧誘等を目的とした電子メールを送信する際の規定を定めた法律。平成20年に改正。迷惑メール対策を強化。

総務省「特定電子メールの送信の適正化等に関する法律のポイント」より

- 規制対象
 - SMS、海外から発信され日本で受信するメールも対象
 - 非営利団体、営業でない個人メールは対象外
- オプトイン方式の導入
 - 同意した者に対してのみ広告宣伝メールを送信可能
 - 例外あり（次頁）
- 罰則の強化
- 国際連携の推進
 - 海外から発信される迷惑メールに対応
- 特定商取引法にも留意

迷惑メール防止法

・説明の流れ

いわゆる「迷惑メール防止法」の規定。

・ポイント（絶対に覚えてほしいこと、など）

海外から発信されるメールも対象となっている。国際連携も視野。

非営利団体のメールは対象外なので、例えばNPO法人からの迷惑メールは本法律では対処できないこと。

・補足説明

NPO法人に対し迷惑メールをやめるように依頼しても、迷惑メ

ール防止法の観点からは、NPO法人はその依頼を聞いて迷惑メール（そもそも善意であり、迷惑と考えていないこともある）をやめる必要もないし、罰せられることもありません。では、NPO法人からの迷惑メールで業務に支障が出たらどうすればよいでしょうか。この場合、ほかの法律（例えば特定商取引法）で阻止することが可能かもしれません。

不正アクセス行為の禁止等に関する法律

不正アクセス行為や、不正アクセス行為につながる識別符号の不正取得・保管行為、不正アクセス行為を助長する行為等を禁止する法律

(定義)

不正アクセス禁止法

第二条 1～3略

4 この法律において「不正アクセス行為」とは、次の各号のいずれかに該当する行為をいう。

一 アクセス制御機能を有する特定電子計算機に電気通信回線を通じて当該アクセス制御機能に係る**他人の識別符号を入力して当該特定電子計算機を起動させ、当該アクセス制御機能により制限されている特定利用をし得る状態にさせる行為**(当該アクセス制御機能を付加したアクセス管理者がするもの及び当該アクセス管理者又は当該識別符号に係る利用権者の承諾を得てするものを除く。)

二 アクセス制御機能を有する特定電子計算機に電気通信回線を通じて当該アクセス制御機能による**特定利用の制限を免れること**ができる情報(識別符号であるものを除く。)又は指令を入力して当該特定電子計算機を起動させ、その**制限されている特定利用をし得る状態にさせる行為**(当該アクセス制御機能を付加したアクセス管理者がするもの及び当該アクセス管理者の承諾を得てするものを除く。次号において同じ。)

三 電気通信回線を介して**接続された他の特定電子計算機**が有するアクセス制御機能によりその特定利用を制限されている特定電子計算機に電気通信回線を通じてその制限を免れることのできる情報又は指令を入力して当該特定電子計算機を起動させ、その**制限されている特定利用をし得る状態にさせる行為**

・説明の流れ

「不正アクセス禁止法」はよく登場するので、このスライドでは少し時間をとって内容を読んでもらい、質問がなければそのまま次へ進んで構わないです。

・ポイント（絶対に覚えてほしいこと、など）

対象となるコンピュータは「アクセス制御機能を有する」コンピュータであること。つまり、アクセス制御機能を設けていなければ、不正アクセス禁止法は適用できないということ。

その制限を免れて特定の機能を利用することを「不正アクセス」と呼ぶこと。

・補足説明

最近はずいぶん減りましたが、Webアプリでディレクトリ参照が有効（アクセス制御機能なし）で、そのディレクトリにある機微な情報ファイルを閲覧されたとしても、閲覧者が罰せられることはありません（傍受扱い）。ただし、その

情報を用いて何らかのアクションを起こした場合、別の法律で罰することができるかもしれません。

第7章 倫理要綱概説

RFC1087 インターネットと倫理
および
情報処理学会 倫理要綱

情報セキュリティを实践する高度情報処理技術者として、守るべき倫理規定と行動規範を守ることができる。

7-1. 行動規範に基づく判断と行動

- (1) RFC1087 倫理とインターネット
- (2) 情報処理学会倫理要綱
 - ① 倫理要綱～1.社会人として～
 - ② 倫理要綱～2.専門家として～
 - ③ 倫理要綱～3.組織責任者として～
 - ④ なぜ倫理要綱が必要か



RFC1087 倫理とインターネット

- IAB（現在のインターネットアーキテクチャ委員会）による、インターネットの資源の正しい利用に関するポリシーの表明
- 以下の活動を非倫理的で容認できないとする
 - インターネットの資源への認可されていないアクセスを得ようとする
 - インターネットの意図された利用を混乱させること
 - そのような活動を通じて資源（人、能力およびコンピュータ）を無駄にすること
 - コンピュータベースの情報のインテグリティ（完全性）を破壊すること
 - ユーザのプライバシーを侵すこと



<https://www.ipa.go.jp/security/rfc/RFC1087JA.html>

・説明の流れ

インターネットにおける非倫理的で容認できない活動は、RFC (Request For Comments)の中でも示されているということを伝えてください。

・ポイント（絶対に覚えてほしいこと、など）

覚えてほしいというよりは、想像してほしい内容です。

これらの容認できない活動が何をもたらすか、考えてもらいたいです。

・補足説明

IAB (旧Internet Activities Board、現Internet Architecture Board: インターネットアーキテクチャ委員会):は、インターネットソサエティ(ISOC)がインターネットの技術的・工学的開発を監督するために設置した委員会

情報処理学会倫理要綱

情報処理学会は、情報処理分野で指導的役割を果たす最大の学会。

- 前文

- 我々情報処理学会会員は、情報処理技術が国境を越えて社会に対して強くかつ広い影響力を持つことを認識し、情報処理技術が社会に貢献し公益に寄与することを願い、**情報処理技術の研究、開発および利用にあたっては、適用される法令とともに、次の行動規範を遵守する。**

1. 社会人として（5項目）
2. 専門家として（4項目）
3. 組織責任者として（4項目）

- 「情報セキュリティ支援業務を行う者が守るべき5つの倫理原則」は上記の2.と3.に対応する

<https://www.ipsj.or.jp/ipsjcode.html>

・説明の流れ

情報処理学会では、情報処理技術が社会や国家に対して強く広い影響力があるにもかかわらず、携わる技術者の社会的地位が低いことを憂慮しています。矜持のない技術は目先の利益に囚われがちで、かつ情報処理技術の場合、社会に対する影響が大きいことが問題です。

情報処理技術者の地位向上のために、何が必要で、どうすればよいかをこの「倫理要綱」で提案しています。

・ポイント（絶対に覚えてほしいこと、など）

立場によって、行動規範の重要性に違いがあること。

情報処理技術に携わるなら、守るべき倫理規範。

倫理要綱～1.社会人として～

- 1.1 他者の生命、安全、財産を侵害しない。
- 1.2 他者の人格とプライバシーを尊重する。
- 1.3 他者の知的財産権と知的成果を尊重する。
- 1.4 情報システムや通信ネットワークの運用規則を遵守する。
- 1.5 社会における文化の多様性に配慮する。



・説明の流れ

倫理要綱では、おそらく当たり前のことしか訴えていません。内容を確認するとともに、自らの普段の行動に照らし合わせて考えてもらうとよいかもしれません。

・ポイント（絶対に覚えてほしいこと、など）

技術者も社会人であり、ここで示す5つの内容は最低限守るべき内容であること。

倫理要綱～2.専門家として～

- 2.1 たえず専門能力の向上に努め、業務においては最善を尽くす。
- 2.2 事実やデータを尊重する。
- 2.3 情報処理技術がもたらす社会やユーザへの影響とリスクについて配慮する。
- 2.4 依頼者との契約や合意を尊重し、依頼者の秘匿情報を守る。



・説明の流れ

情報セキュリティに携わる技術者であれば、このスライドの内容は常日頃意識してほしい内容です。

・ポイント（絶対に覚えてほしいこと、など）

「事実やデータを尊重する」こと。たとえば勝手な判断で（あるいは恣意的に）ログの情報を部分的に切り出したりしない。

ほかにも、情報処理技術は社会に影響を与える力があることを認識すること。

倫理要綱～3.組織責任者として～

- 3.1 情報システムの開発と運用によって影響を受けるすべての人々の要求に応じ、その**尊厳を損なわない**ように配慮する。
- 3.2 情報システムの相互接続について、管理方針の異なる情報システムの存在することを認め、その接続が**いかなる人々の人格をも侵害しない**ように配慮する。
- 3.3 情報システムの開発と運用について、**資源の正当かつ適切な利用**のための規則を作成し、その実施に**責任を持つ**。
- 3.4 情報処理技術の原則、制約、リスクについて、自己が属する組織の**構成員が学ぶ機会**を設ける。



・説明の流れ

組織対組織で利害がぶつかったときにどうすべきか考えてください。

・ポイント（絶対に覚えてほしいこと、など）

相手の人格や尊厳を尊重する。規則と責任。組織内への周知。

倫理規定（再掲）

- 情報セキュリティ支援業務を行う者が守るべき5つの倫理原則
- 1. 全てのプロフェッショナルおよび業務との関係において、嘘をつかず、誠実でなければならず、専門的な基準および事実とデータに基づいたサービス提供を誠実に行わなければならない。
- 2. 業務上の判断は、偏見、利益相反、他者の過度の影響を受けず、常に客観的に行われなければならない。
- 3. 顧客または雇用者に現在の技術発展レベルと法律に基づいたプロフェッショナルサービスを提供するために必要なレベルの、専門知識とスキルを維持しなければならない。
- 4. 専門的、業務上知り得た情報の機密性を、法的または専門的な権利または開示義務が無いかぎり、厳守しなければならない。
- 5. 注意深く行動し、信用を損なってはならない。

・説明の流れ

このスライドは、情報処理学会倫理要綱と、情報セキュリティ支援業務者の倫理規定を比較するためのスライドです。本章ここまでのスライドと比較する時間が取れれば、改めて見てもらうようにしてください。

・ポイント（絶対に覚えてほしいこと、など）

倫理要綱で情報処理技術者に訴えたい内容。

なぜ倫理要綱が必要か

情報処理技術が社会的に大きい影響力を持つアプリケーションを数多く産み出しつつあるという現実があり、これを受けて情報処理技術者は**自己の行動に対する責任を持たなければならない**という考え方が生じてきたため。

社会的な影響力を持つ医師、建築家、弁護士などは、専門家として高い倫理性が法的に義務付けられている。情報処理技術者は高度の専門性を求められているにもかかわらず、**制度的には専門家として認められていない**。この弱い立場を支えるためにも、情報処理技術者は**自律的な行動規範を持つ必要がある**。



・説明の流れ

「ルールがあるから守る」のではなく、自らで行動規範持つことが大事。自らの行動が、情報処理技術者の専門家としての立場を高めるという意識が必要であること。

・ポイント（絶対に覚えてほしいこと、など）

情報処理技術者は、社会的な影響力を持つ技術の持ち主であるという矜持。

・質問（問いかけ）

自らの持つ情報処理技術がどのような形で社会的に影響を与えますか。

情報セキュリティの意識が薄い場合、社会にどのような悪影響を与えますか。

7-2. 倫理的な判断と行動～グループ演習～

演習6 コンプライアンス事例の検証



・説明の流れ

この演習を行う時間は恐らくありません。しかし自習用のシナリオとして、「自分だったらここでどうするか」を考える材料にしてください。

- ・ポイント（絶対に覚えてほしいこと、など）
過去の事例から学ぶ。