高度ITを活用したビジネス創造プログラム
講師マニュアル

ーセキュリティ講座　Vol.2－

プログラム概要

高度IT 技術を活用したビジネス創造プログラムの概要

1.プログラム開発の目的と背景

■プログラムの目的
第4 次産業革命において必須であるIoT、AI やビッグデータに代表されるIT 系の技術を駆使し、新たな発想（サービス企画・デザイン思考）でビジネスを創造できる高度IT エンジニアを育成する。
■修得すべき能力とその理由
修得すべき能力を図で表すと下記のようなイメージになる。今回は一定のスキル（レベル2～3程
度）を修得しているエンジニアを受講者に想定しているので、学習対象範囲の各能力についての教育訓練プログラムを作成する。

（図1）

1. 分野横断的な発想力、分析力、企画力を備えたビジネス創造力
2. デザイン思考力
3. アジャイル開発力
4. AI
5. IoT
6. ビッグデータ
（統計解析・分散処理）
7. 仮想化
8. セキュリティ

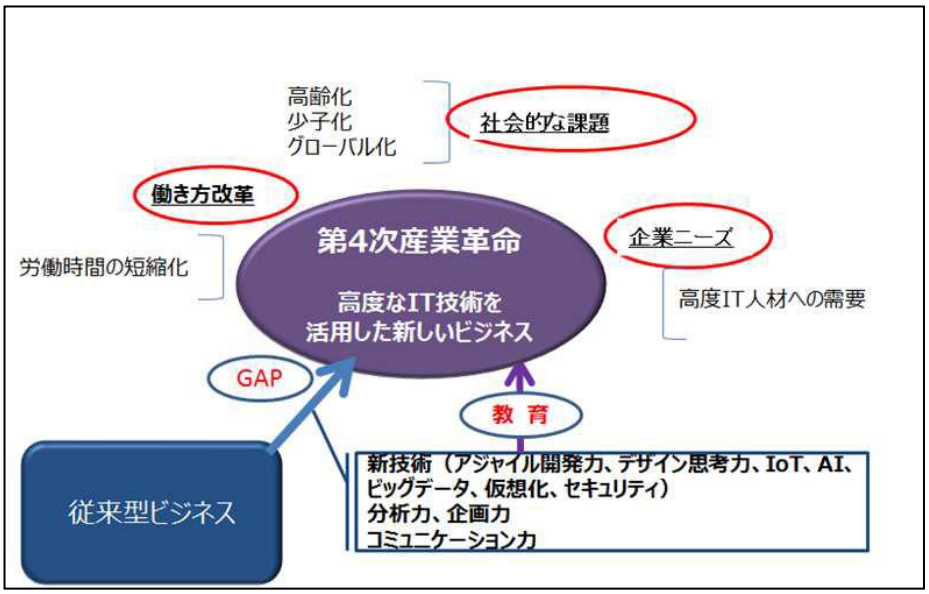
2.プログラム開発の背景

1)「第4 次産業革命」における必要性

現代社会において高齢化・少子化・グローバル化等の社会的な課題が山積する中で、それらの社会的な課題を解決することが求められている。それらの課題の解決には、新しい発想のビジネスが求められていて、それを実現するためには、高度なIT 技術の活用が不可欠である。企業も社会的な課題を解決するための新たなビジネスチャンスを求めてはいるが、現状はほとんどの技術者が従来型ビジネスに対応した人材であり、高度なIT 技術をもった人材へのニーズがある。

また、「働き方改革」という労働時間の短縮化という中で、労働時間が削減されても経済成長を促すには、単位時間あたりの労働生産性の向上が欠かせない。労働生産性の向上には、より高度なIT 技術の修得が不可欠である。

このように、「社会的必要性」「企業ニーズ」「働き方改革」という3 つの要因で上記に挙げた8つの能力が必要である。上述の内容を表したのが図2 である。

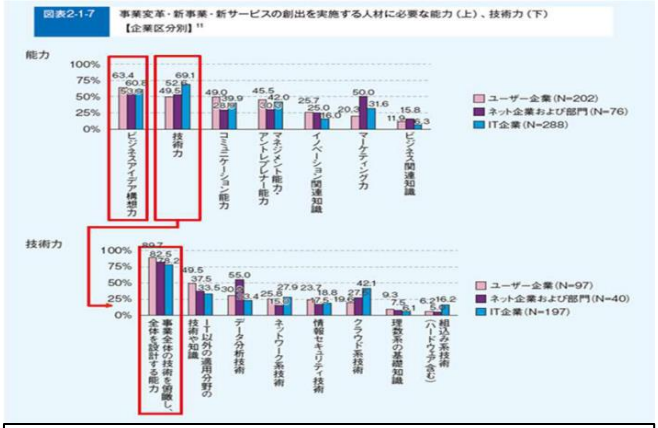


(図2)

2.プログラム開発の背景

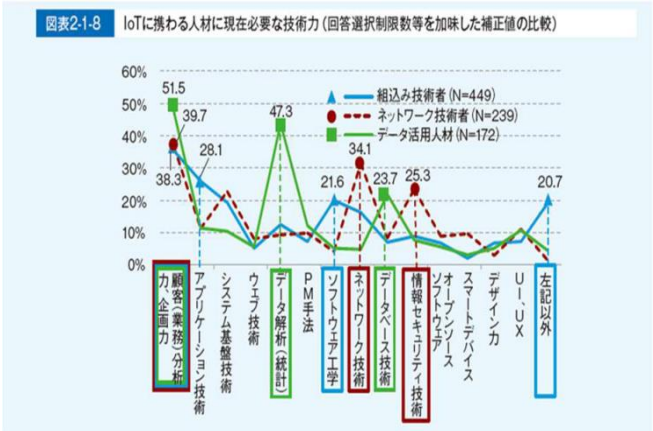
2)8 つの能力の根拠

図2 のように、企業が新しいビジネスを創造するためには、従来型ビジネスとのGAP を埋めるための能力が必要であり、IPA の「IT 人材白書2016」(資料1)によると「ビジネスアイデア構想力」「技術力」が求められる



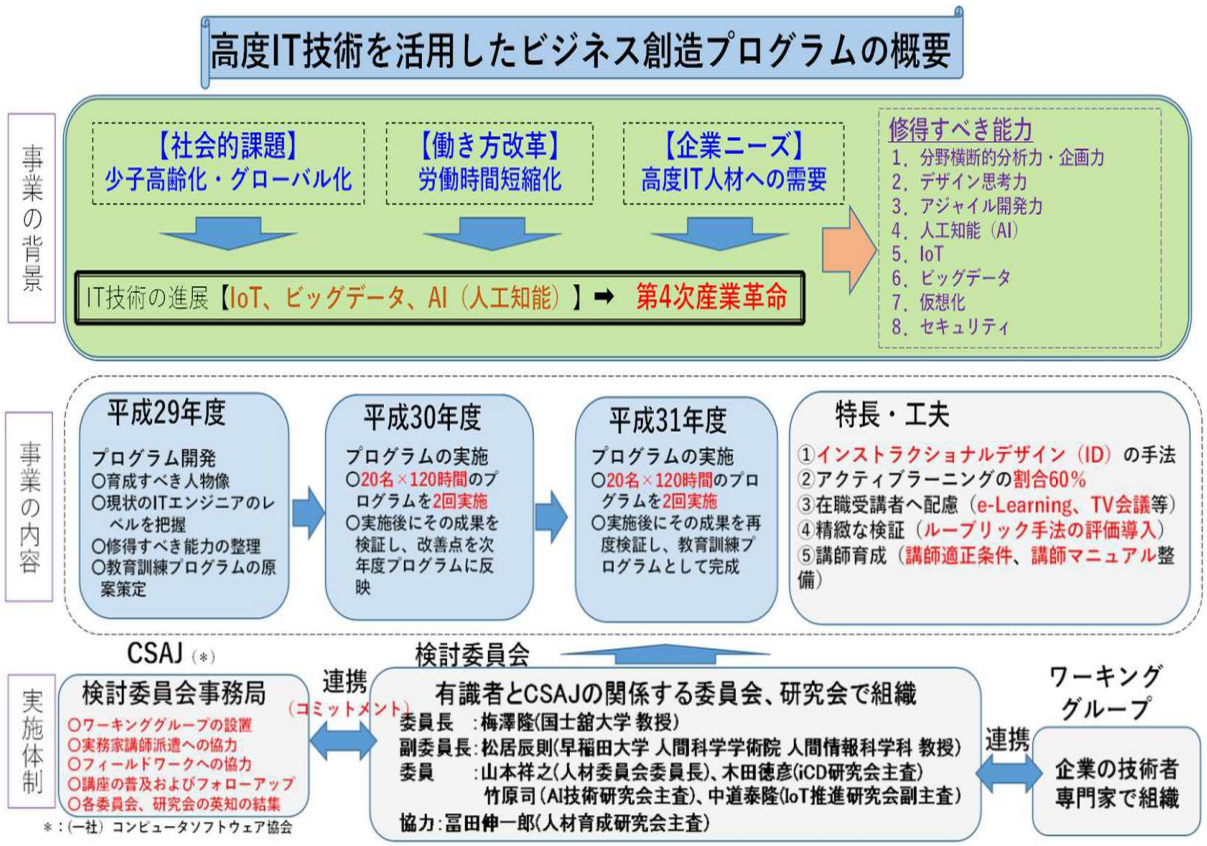
(資料1)
『新事業・新サービス創出に必要な能力・技術力とは？』
(IPA「IT 人材白書2016」)

「ビジネスアイデア構想力」「技術力」とは何かを詳細に見てみると、例えば「IoT に関わる人材に必要な能力は」というIPA のアンケート調査「IT 人材白書2016」（資料2）では「顧客分析・企画力」「データ解析」「ソフトウェア工学」「ネットワーク技術」「データベース技術」「情報セキュリティ」があげられる。



(資料2)
『IoT 人材に必要な技術力とは？』
（IPA「IT 人材白書2016」）

3.実施組織


高度IT技術を活用したビジネス創造プログラムの概要
事業の背景
【社会的課題】
少子高齢化・グローバル化
【働き方改革】
労働時間短縮化
【企業ニーズ】
高度IT人材への需要
IT技術の進展【IoT、ビッグデータ、AI（人工知能）】➡ 第4次産業革命
修得すべき能力
1．分野横断的分析力・企画力
2．デザイン思考力
3．アジャイル開発力
4．人工知能（AI）
5．IoT
6．ビッグデータ
7．仮想化
8．セキュリティ
事業の内容
平成29年度
プログラム開発
○育成すべき人物像
○現状のITエンジニアのレベルを把握
○修得すべき能力の整理
○教育訓練プログラムの原案策定
平成30年度
プログラムの実施
○20名×120時間のプログラムを2回実施
○実施後にその成果を検証し、改善点を次年度プログラムに反映
平成31年度
プログラムの実施
○20名×120時間のプログラムを2回実施
○実施後にその成果を再度検証し、教育訓練プログラムとして完成
特長・工夫
①インストラクショナルデザイン（ID）の手法
②アクティブラーニングの割合60％
③在職受講者へ配慮（e-Learning、TV会議等）
④精緻な検証（ルーブリック手法の評価導入）
⑤講師育成（講師適正条件、講師マニュアル整備）
実施体制
CSAJ（＊）
検討委員会事務局
○ワーキンググループの設置
○実務家講師派遣への協力
○フィールドワークへの協力
○講座の普及およびフォローアップ
○各委員会、研究会の英知の結集
＊：（一社）コンピュータソフトウェア協会
連携
（コミットメント）
有識者とCSAJの関係する委員会、研究会で組織
委員長　：梅澤隆(国士舘大学 教授)
副委員長：松居辰則(早稲田大学 人間科学学術院 人間情報科学科 教授)
委員　　：山本祥之(人材委員会委員長)、木田徳彦(iCD研究会主査)
竹原司(AI技術研究会主査)、中道泰隆(IoT推進研究会副主査)
協力：冨田伸一郎(人材育成研究会主査)
連携
ワーキング
グループ
企業の技術者
専門家で組織

4.高度IT 技術を活用したビジネス創造プログラムの構成

■各講座の時間割

コース名	講義	演習	小計
1．オリエンテーション	2:00	-	2:00
2．デザイン思考講座	4:00	6:00	10:00
3．仮想化講座	4:00	4:00	8:00
4．ビッグデータ講座	7:10	7:50	15:00
5．AI基礎講座	8:35	7:25	16:00
6．IoT活用講座	8:50	7:10	16:00
7．セキュリティ講座	6:30	4:30	11:00
8．アジャイル講座	5:40	6:20	12:00
9．顧客分析・企画力養成講座	4:50	13:10	18:00
10．フィールドワーク（セキュリティ・アジャイル開発・AI）	-	12:00	12:00

■フィールド・ワーク

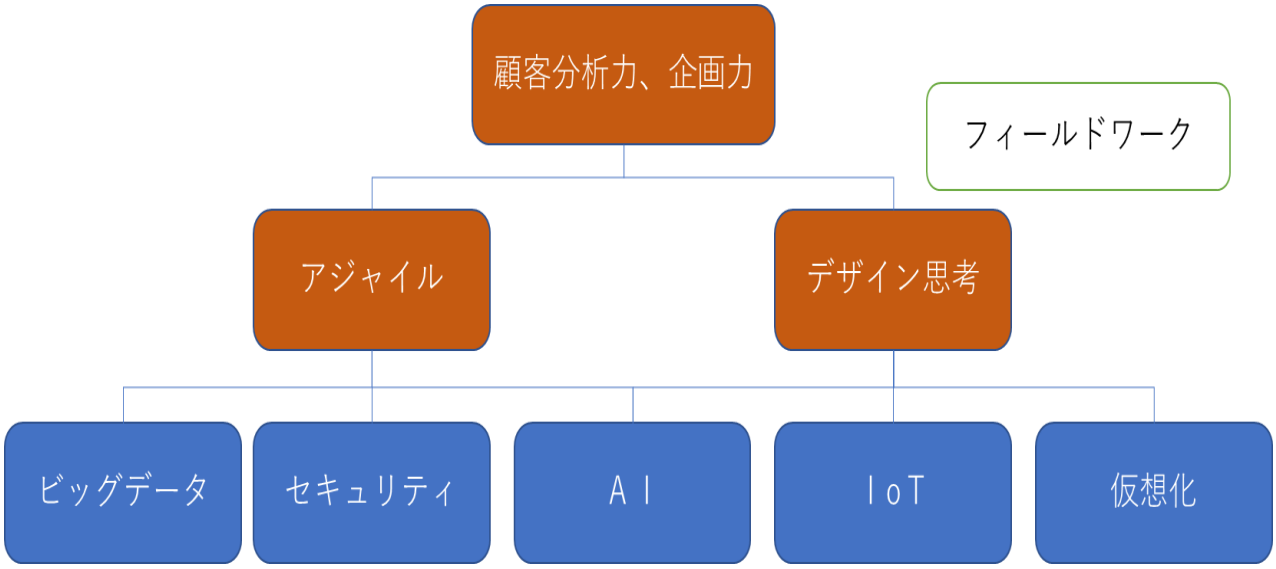
	関連講座	訪問先企業（予定）	学習概要
1	セキュリティ	株式会社ラック様	場所：本社ビル　永田町 内容：1.ラック様のセキュリティ業務の実際 2.JSOCS見学 3.体験ゲーム
2	アジャイル開発	KDDI株式会社様	場所：新宿 内容：1.開発現場の見学 2.KDDI様のアジャイルへの取り組み 3.体感ゲーム
3	Ai基礎	日本電気株式会社様	場所：三田 内容：1. NEC Future Creation Hub 見学 2:AI企画の概要と演習説明 3:【演習】データ・バリューチェーンの作成 4:まとめ

5.高度IT 技術を活用したビジネス創造プログラムの構成

講座の関係図

・赤枠：思考法・発想法

・青枠：IT技術知識・スキル



6. 教育訓練プログラム受講修了及び評価

■受講修了条件
●終了時間：120 時間
●終了時の能力像：「第4 次産業革命において、IT 系の必須技術を駆使し、新たな発想を持ってビジネスを創造できる知識・スキル」

【各講座の時間数】

No	講座名（モジュール名）	時間	No	講座名（モジュール名）	時間
1	オリエンテーション	2	6	IoT活用講座	16
2	デザイン思考講座	10	7	セキュリティ講座	11
3	仮想化講座	8	8	アジャイル講座	12
4	ビッグデータ講座	15	9	顧客分析・企画力養成講座	18
5	AI基礎講座	16	10	フィールドワーク	12
				総合計	120

■評価指標と基準点
下記の指標に対する基準点をすべてクリアする。

	実施タイミング	指標	合格基準
1	ー	出席率	80%以上
2	各講座	e-learning テスト	100%
3	各講座	理解度確認テスト	80%
4	各講座	ルーブリック仕様のアンケート	～ができる（下記に例示）
5	各講座	成果物評価	講師による評価：講師が正常稼働及び理解度を前提に総合的な判定を行う

ルーブリック仕様のアンケート（例）

自己評価		1	2（合格基準）	3
理解度	内容を理解している	メソッドのメリット・デメリットを理解している。	メリット・デメリットをメンバーに説明できる。	メリット・デメリットをについて自分の考えを説明できる
応用力	現場で活用できる	状況に応じてメリット・デメリットを説明できる。	情況にあったメソッドを選択できる。	情況にあったメソッドで課題解決に取り組める。

7. セキュリティ講座概要

ねらい	セキュリティの「知識」と「技能」の基礎を棚卸しし、高度 IT 技術者として期待される役割にふさわしい情報セキュリティ実践のための具体的な技術や手法を学習する。				
開催時間	11 時間（e-learning　3 時間含む）				
受講条件	IT 技術者としての経験が 3 年以上、ICT の基礎知識を持っていること				
学習目標	情報セキュリティの主要な業務である「インシデントレスポンス」、「セキュア設計・開発の主要なタスク及びそのプロセス」、「情報セキュリティ業務を実施する上で必要となる倫理的な行動」の詳細について習得する。				
	時間	講義	演習	学習概要	学習詳細
カリキュラム概要	1:30	0:40	0:50	最新動向　情報セキュリティ 10 大脅威	・脅威の動向、手口、対策 ・情報資産の洗い出しと脅威の検討～グループ学習～
	0:30	0:30	0:00	関連制度や規格の動向　JIS, ISO/IEC, IEEE など	・規格の種類 ・規格詳細
	3:10	0:30	2:40	インシデントレスポンス	・インシデントレスポンス(IR)とは ・IR のプロセスやタスクの概要 ・IR 事例～グループ演習～ 障害・ヒューマンエラー・不正アクセス
	0:40	0:40	0:00	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	・サイバー攻撃に備えた設計と構築 ・セキュアシステム、ネットワークの設計
	1:40	0:40	1:00	セキュア開発概説	・ソフトウェア開発、ウェブサイト設計 ・セキュアプログラミング～グループ演習～
	0:15	0:15	0:00	倫理・コンプライアンスの概念	・倫理・コンプライアンスの概念 ・基本的な考え方
	0:15	0:15	0:00	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	・行動規範に基づく判断と行動 ・倫理的な判断と行動
合計時間	8:00	3:30	4:30		

8．セキュリティ講座　詳細カリキュラム

時間	学習項目	学習項目の狙い	詳細内容
0:10	オリエンテーション	**[ゴール]** ・本講座終了時点で期待される姿を説明できる。 **[目的]** ・この研修における目標を明確にし、研修への意欲を高める	**[講義]** **①オリエンテーション** 1.講師自己紹介 2.コースの目的 ・新規開拓事業ほど（脅威が不明瞭なため）狙われやすいが、セキュリティ対策の基本は常に変わりません（守るべきものを明確にし、守る方策を考える）。講座では実例や実習、法律も交えながら体験し、実践する土台を作ることを目的とします。 3.注意点 ・駆け足で進む ・他の講義と重複している項目もある ・均等に章を見ていくわけではない（強弱あり） ・覚えることではなく、「なぜ」という考え方を強調 ・実習は途中で時間が無くなることもありますが、 極力解説を最小限に抑え、実習に時間を割くこと。 4.配布資料の確認 **①小道具の確認** 1．多めの付箋紙、マジック、模造紙、テープなどを用意。タイマーもあるとよい。 **②実機演習用 PC の確認** 1.各グループ実機演習用 PC セット内容を確認する。 2.実機は第 4 章の演習で使いますが、講義中も随時使用可能としておきます。その場で検索や参照もありとします。
			[演習] なし
1:20	第 1 章　最新動向	**[ゴール]**	**[講義]** **①脅威、脆弱性、リスク、管理策の関係**

		・セキュリティ管理策を策定する道筋を説明できる。 ・セキュリティのトレンドを追うことができる。 **[目的]** ・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。	1．セキュリティを考えるにあたり、守るべき対象を明確にすることがすべての第一歩と改めて認識してもらう。 [小ワーク]守るべき資産に何があるか、グループ内で幾つか挙げ、各グループ一つずつ発表してもらう。この小ワークは演習の最初の手順と同じになります。 ※先行する講座でグループ内の緊張がほぐれているようであれば、自己紹介やアイスブレイクは不要。2.脅威と脆弱性の違いについて説明できるか尋ねてみるのもよい。3．機密性、完全性、可用性の説明は入っていません。受講者の状況に応じて説明を加えてください。 **②最新動向** 1．最新動向については、最新の「情報セキュリティ 10 大脅威」をベースに進められるとよい。受講生 PC で IPA のホームページから直接取得してもらうのもよい。 2．すべて説明するのではなく、新たに加わった脅威を中心に説明する。 3．立場や役割で対策が変わることをはっきりさせる。 4．時事ネタがあれば紹介および対策を簡単に。 [口頭質問]時事ネタを受講生に尋ねてみたり、対策を考えさせてみたりするのもよい。
			[演習] **①情報資産の洗い出しと脅威の検討** 1．この演習では、情報資産、脅威、脆弱性、リスクの関係を具体的に実感してもらうことが目的です。 2．講義中に小ワークとかアイスブレイクを行っていない場合、必要ならばアイスブレイクを行ってください。
0:30	第 2 章　関連制度や規格の動向	**[ゴール]** ・規格に法ったセキュリティ対策をとる場合、どこを	※この章はなるべくさっとやり過ごすようにしてください。どんな時にどの規格を見るか、だいたい理解できれば十分です。 **[講義]** **①規格の種類**

		調べれば何がわかるのかを最低限説明できる。 ・各制度や規格の権威づけを説明できる。権威づけのない決まりごとは、守られないため。 **[目的]** ・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。	1. まずは大枠として、経済協力開発機構 OECD による「セキュリティ文化」という考え方を示します。 2. 規格を読むにあたり、用語がわからないと先へ進めません。基本用語も規格で定義されることを示します。 3. ISMS 認証に関わる規格一覧を示しますが、これは説明する必要はありません。赤く示された、主要な 3 つと比較的新たに加わった規格 1 つをのちに示します。 4. 規格を作ったのはだれか。これは権威づけを行うために重要です。※知らない子供が作った規格を国として推し進めるということはありますか。 **②規格詳細** 1. ISMS 認証の土台となる 27000～27002 の役割は簡単に示してください。 2. 15408 はセキュリティ関連機材調達時に目にすることがあるので、基礎知識として示します。 3. IEEE の作成する規格の例として、802.11 を挙げています。ここで詳しく説明する必要は「まったく」ありません。あくまで、IEEE がどんな規格を作成しているかの例です。 ※規格の名前を覚えることは目的ではありません。また、できれば規格への抵抗感を薄めたい。 ※似たような名前が多くわからないという声がよく出るので、「何のためにどの規格」という点を強調してください。
			[演習] なし
3:10	第 3 章 インシデントレスポンス	**[ゴール]** ・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	**[講義]** ※講義は 30 分程度で、あとは演習に回してください。 **①インシデント管理** [口頭質問]（時間の余裕を見て）そもそもインシデントとは何を意味しているのか数人に尋ねてみる。または、挙手で説明してもらう。 1. そもそも「インシデントとは何か」について明確にしておきます。

		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。 **[目的]** ・インシデント対応の各ステージで何を行うか簡単に説明できる。 ・インシデント管理の流れを説明できる。 ・主要なドキュメントの役割を説明できる。	2．「インシデントレスポンス」は、JIS では「インシデント対応」となっています。意味はどちらも同じなので、本講座では途中から「インシデント対応」で進めています。 3．「インシデント対応」は「インシデント管理」の一部であることと、インシデント発生後の対応であることを確認。 4．平常時の備えにより、異常に気付く土壌を作ることが大事であることを改めて伝える。インシデントが発生してから対応するのでは遅い。 **②インシデント対応** 1．インシデント対応計画と標準運用手順書なしでの対応は、かえって解決を遅らせ、今後の糧にもならないことを伝える。 2．具体的な活動は演習書に記述されています。講義であまり時間をとらないようにしてください。
			[演習] **①インシデント対応事例 - 正当なアカウントによる侵害** 1．正規のアカウントでセキュリティ侵害が発生したことを想定した演習です。本演習は実例に基づいて作成されています。 2．本演習は、課題のインシデントの対策実施が目的ではありません。どのような流れでインシデント対応を行うかを体験してもらう演習です。作業が途中であっても時間を見て先に進んでください。また、その旨を先に受講者に伝えてください。 3．最後の振り返りは、時間が足りない場合は作業時間を短くしたり、模造紙に描く手順を省略したりしてください。 4．本演習のインシデント対応では、「これが正解！」というものはありません。むしろ、皆が何に気づき、何を見逃したかに気づいてもらうことが重要です。 5．演習時間が長いので、グループごとに適宜休憩をとるように伝え

			てください。 6．途中で「インシデント対応の主な活動」の具体例を挙げてあります。これは、「初めてのことなのでどこから手を付けてよいかわからない」という意見があるためです。じっくり読むと時間がかかるので、必要な時に拾い読みする程度にするよう伝えてください。ただ、じっくり読みたいという方を制止する必要はありません。 7．最後の発表では講師がコメントする必要は特にありません。基本的には発表のみで構いません。
0:40	第４章　セキュア設計	**[ゴール]** ・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。 **[目的]** ・セキュア設計は上流工程こそ大事であることを説明できる。 ・脅威モデリングの考え方を説明できる。ただし、実践できることまでは本講座では目的としない。 ・セキュリティ品質をどのようにして確保するか説明できる。 ・TCP/IP 階層モデルや OSI 参照モデルをベー	**[講義]** **①セキュアシステム設計** 1．設計原則は、なんとなく理解しているものも多いと思います。ここでは皆に過去の経験を想起してもらえると効果があります。 [口頭質問]過去に携わったシステムがあれば、この原則を実践できていたか、思い出してください。（時間があれば）実践できてなかった部分を、理由とともに皆に発表してください。 2．システム設計にセキュリティチームがどのようにかかわっていけばよいかを意識させてください。ただ、セキュアシステム設計の図を説明していくと時間が無くなるので、一つ二つの状況を挙げる程度で構いません。 3．脅威モデリングで実際にモデリングを行おうとすると、かなりの知識と経験が必要となります。システム開発時に各コンポーネント、各通信、各オブジェクト（ヒト、物、データなど）に対する脅威モデリングを負担なく実践できるよう、常日頃から意識するよう伝えてください。 **②セキュアネットワーク構築** 1．ネットワーク階層モデルは、現実問題として TCP/IP 階層モデルで十分なのですが、OSI 参照モデルのほうが受講者が分かりやすいようでしたら、適宜説明を切り替えてください。

		スにネットワークセキュリティを説明することができる。 ・各種検疫ネットワークの利点欠点を説明できる。 ・無線 LAN を安全に運用するポイントを説明できる。	2. ネットワーク階層モデルでは、「どの階層にどのようなデータが含まれているか」を強く意識付けしていきます。それらのデータに対し、どのような脆弱性、脅威があるか考えてもらうとよいでしょう。 3. ルーターに関しては、「TCP/IP 第 1 層の機器ではない」とか「第 3 層トランスポート層も見ている」とか受講者が疑問に持つ可能性があります。「ルーティング機能」と「パケットフィルタリング機能」を分けて説明すると理解しやすいかもしれません。 [口頭質問]組織内で検疫ネットワークを構築してる場合、どのような技術を使ったネットワークで、脆弱あるいは不安なポイントはありませんか。差し支えなければぜひ皆に教えてください。
			[口頭質問]組織内で無線 LAN を使っていない方はいませんか。いるとしたら、なぜ使っていないのか理由を教えてください。差し支えない範囲で。 4. セキュアな無線 LAN 構築では、認証、（認可、）暗号化、接続性がポイントとなります。なお、接続性は「可用性」につながります。 **③IoT** 1. IoT であっても、セキュア設計、セキュアネットワーク構築の考え方は変わりません。ただ、IoT 機器それぞれが持つ固有の課題が対応を難しくします。「固有の課題」を洗い出し、各課題のリスクを評価することが対策のポイントとなります。
1:40	第 5 章　セキュア開発概説	**[ゴール]** ・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。	**[講義]** ※ この段階で VirtualBox Manager を起動し、Mutillidae と Kali Linux を起動してもらうとよいかもしれません。その場合は導通確認まで行います。そして問題があれば、演習までに対応します。 ※ VirtualBox の扱いに慣れていない方もいます。必要に応じて、ここで簡単な操作説明をしてください。 **①ソフトウェア開発、Web サイト設計**

		・Web アプリの脆弱性を検出する方法を説明できる。 **[目的]** ・Web アプリの階層構造とセキュリティ境界を指摘できる。 ・安全なコーディング実装の一覧から、内容を説明できる。 ・OWASP Top 10 を例に、継続しているリスクと新たに加わったリスクを識別し、対応を検討できる。 ・脆弱な Web アプリを手動ないし自動で調査する方法を説明できる。	1.「安全なコーディング実装」の並び順は、原文に則っています。しかしながら IPA では順番を入れ替え、出力チェックにあたる 7 番を 3 番にもってきて、出力チェックの重要性を目立たせています。出力チェックの重要性は、ことあるごとに指摘するようにしてください。 2. Web アプリの脆弱性は、データやコマンドそのものの取り扱いと、データの受け渡しで発生しています。しかしながら、押さえるべきポイントは無限ではなく、いくつかに類型化されることを図より示してください。 [小ワーク]（時間があれば）グループ内で、今までかかわった Web アプリがある場合、安全なコーディング実装と脆弱性の図に照らして考慮が浅かった部分がないか話し合ってください。2、3 グループを当てて発表させるとよいです。 **②OWASP Top 10** 1. よく知られているが対策が取られていないリスク、新たに発生したリスクでは、対応が異なります。受講生の状況に応じ、どちらかにウェイトを置いて説明してください。あまりなじみがない方にはインジェクション対策を。基本は押さえられている場合には XXE や最新のリスクに対する対策を示すとよいです。 2. OWASP Top 10 は検索ですぐに探せるので、直接 Top 10 の PDF を見てもらうのも効果的です。 3. リスクへの対策は Top10 すべてについて記述してありますが、ここからいくつかピックアップして説明するようにしてください。ランクの 1,4,9 を基本としますが、[口頭質問]として、受講生に対策を聞きたいリスクを尋ねるのもよい方法です。
			[演習] ※この演習は、許可をもらっていないサイトに対しては決して行わないことを改めて周知します。※この演習は個人でも実施可能ですが、**互いに相談しあうことで問題解決できる**ということもぜひ伝え、自由な雰囲気で会話ができるようにしてください。結果として多少騒がしいくらいがちょうどよいです。 **①手動による Web アプリ脆弱性の調査**

			1. ヒントは英語です。必要ならば、たとえば Google 翻訳を活用して英文を翻訳してもらってください。 2. SQL や英語に不慣れな方もいます。進捗や受講生の様子を見て、別紙の解答を見ながらの作業を基本に演習を行ってもらってください。 3. 目的は、手動による調査はきめ細かくできるが手間と時間がかかることを認識してもらうことです。脆弱性があることは明白なので、未知の脆弱性を探すことを目的とはしないでください。 **②ツールを使った Web アプリ脆弱性の調査** 1. ツールを使うと操作は簡単なものの、すべての脆弱性を見つけ出すわけではないことを強く意識させてください。
0:15	第 6 章 倫理・コンプライアンスの概念	**[ゴール]** ・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。 **[目的]** ・内部不正を防ぐ観点の一つがコンプライアンスであることを示すことができる。 ・コンプライアンスは倫理規定に裏打ちされている必要があることを説明できる。 ・法令遵守だけではないことを説明できる。	**[講義]** ※ 本講座では、違反が「なぜ悪いのか」は特に説明していません。多くの場合、悪いということはわかっているからです。それよりも、コンプライアンス違反でどのような不利益を被るかを実感してもらうほうが効果的と考えます ※ 本章と次章はすべてを説明するのではなく、重要と思われる項目だけ念押ししてください。 **①概念** 1. コンプライアンスが組織内部でどのような位置づけにあるのか、内部不正防止の観点で示してください。 2. よく「コンプライアンス」は「法令遵守」と訳されていますが、法律だけを守ればよいわけではないことを強く意識付けさせてください。 3. 社会通念、倫理、道徳などは、人や国、所属する組織などによって様々です。ここではまず「情報セキュリティ支援業務」という枠にはめ、その中での「倫理規定」であることを示してください。 4. 明文化し、誓約書という形をとることで、コンプライアンス違反か否かを客観的に判断できるようにしないと意味がないことを伝えてください。

		・コンプライアンス遵守対策を列挙できる。 ・コンプライアンス違反に適用可能な法律やガイドラインをいくつか示すことができる。	**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の 3 項目は、受講生に実際の状況を想像する時間をあたるように進めてください。ただ読むだけとなるならば、むしろ飛ばすほうが良いかもしれません。知った気になるだけで、実態が伴わなくなってしまいます。 2．関連する法律・ガイドラインの細かい説明は全く不要です。よく言われる禁止事項には法律の裏打ちがあるということを知ってほしいところです。そして、実際の法律を見てもらうことで禁止事項に権威付けをしています。 ※法律はオンライン六法全書や総務省のサイトでも紹介されています。ブラウザで検索したり、実際にスクリーンで見せたりすることでより実感できるはずです。
			[演習] なし
0:15	第 7 章　倫理要綱概説	**[ゴール]** ・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、守るべき倫理規定と行動規範を守ることができる。 **[目的]** ・インターネットにおける非倫理的な活動を説明できる。 ・情報処理学会における行動規範を、一覧を見ながら説明できる。 ・情報処理技術者に倫理要綱が必要な背景を説明できる。	**[講義]** **①行動規範に基づく判断と行動** 1．インターネット上で容認できない非倫理的な活動が、RFC1087 で表明されています。このポリシーはコンピュータ上の情報資源にも適用できることは伝えてください。 2．情報処理学会倫理要綱では、情報処理技術者が異なる立場で守るべき行動規範が示されています。この行動規範は情報に携わるすべての人に適用できます。 3．情報処理技術者は、専門家として今や社会に大きな影響を与えるのにもかかわらず、社会的立場は非常に弱いものとなっています。高度情報処理技術者が率先して高い倫理性を持ち、と自律的な行動規範を遵守することで、今後の情報処理技術者の社会的地位向上を目指すということをぜひ伝えてください。現在は高い専門性が社会的に認知されていないからこそ、情報セキュリティもないがしろにされ、社会的な混乱も生じているといえます。
			[演習(実施は省略)]

			※ 進捗を見て、演習を割愛してかまいません。倫理要綱に従った場合、シナリオのどの時点で問題回避に向かうことができたか考える材料として紹介してください。 （演習実施時のポイント） **①倫理的な判断と行動** 1．みずほ銀行合併時のシステム障害を実例として挙げています。大規模な障害と損害は、どうすれば避けることができたかをグループで検討させます。 2．政治力学上やむを得ないところもありますが、スケジュールに縛られコンプライアンスがないがしろにされたことが被害を大きくしています。「あの時こうしていれば」という場面がいくつもあります。 3．回答例は「システム障害を撲滅する 10 カ条」であり、演習の「解答例」とはなっていません。演習で検討した各グループの回答を類型化すると、この 10 カ条のどこかに収まるはずです。時間があれば、各グループの検討結果が回答例のどこに分類されるのか、ぜひ並べてみてください。

セキュリティ講座

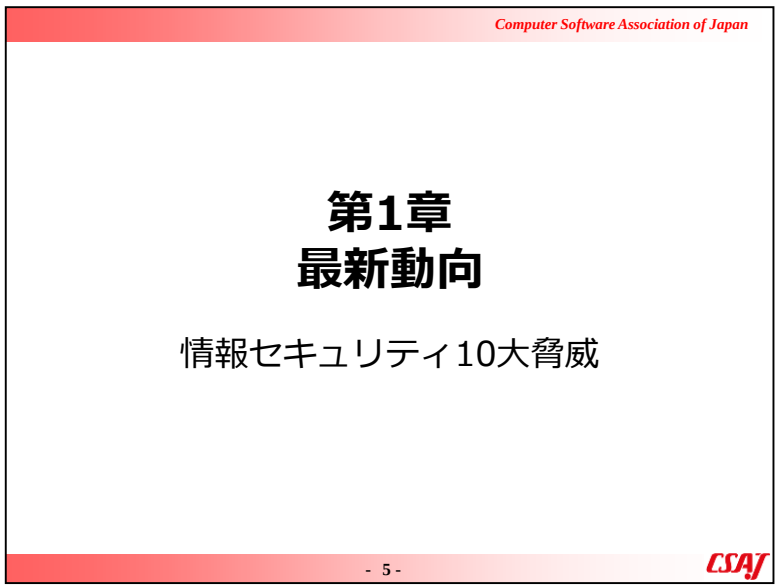
著作権表示

クリップアート

- リコージャパン株式会社　プリント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

目次



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

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、電気的(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。

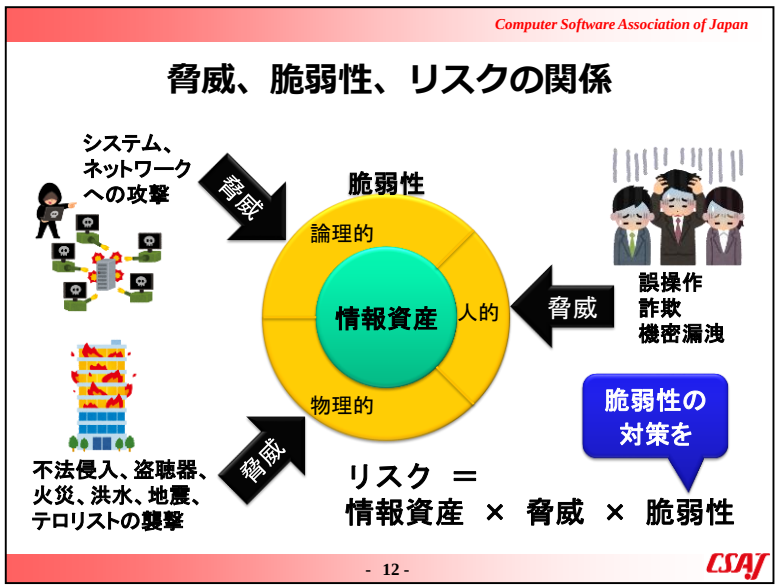
リスクの定義がわかりにくいので、次のスライドを説明に使うとよいかもしれません。

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す。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す。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す。不確定要素はリスクとなる、ということです。



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。

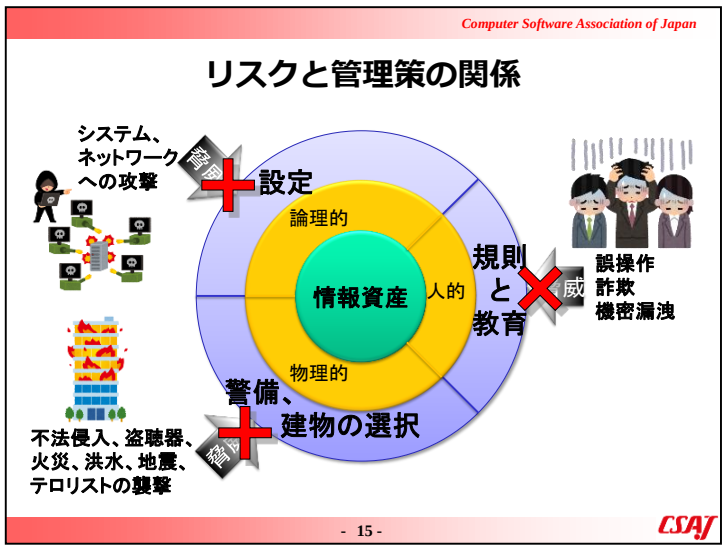
管理策の定義

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。



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みます。

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。

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年こ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。

Computer Software Association of Japan

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

CSAJ

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：

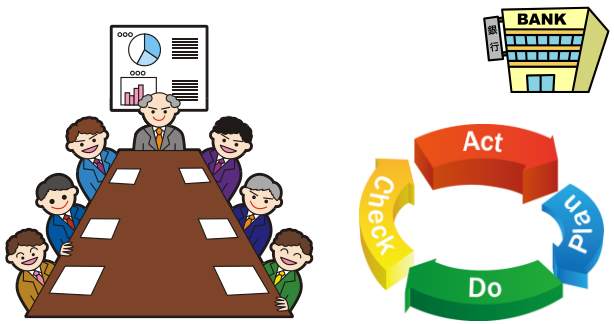
旅行会社JTBから678万件の個人情報流出の可能性
- ●取引先になりすましたメールの添付ファイルを開き、ウイルスに感染
- ●遠隔操作により個人情報を保管しているサーバーへと侵害が拡大

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

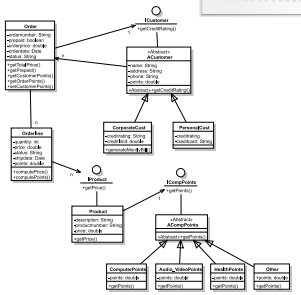


どのような脅威であっても、組織としての対応ではCSIRT構築が必要となります。CSIRTについては第３章「インシデントレスポンス」で改めて説明します。

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～

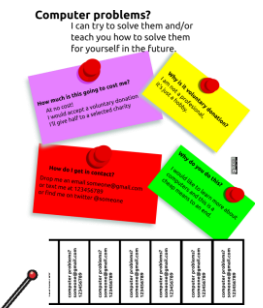
- 被害の予防
  - 被害を抑止するためのシステム設計
  - アクセス制御・データの暗号化
- 被害の早期検知・事後対策
  - ネットワーク監視・分離

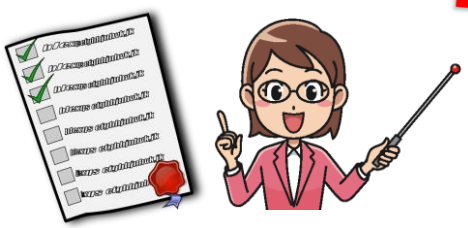


たとえ利用者がメール添付ファイルを開いたとしても、アクセス制御が適切に設定されていれば、権限のないデータにたどりつくことは困難になります。一方、データの暗号化は重要ですが、ネットワークの暗号化は被害の発見を遅らせたり、解析を困難にしたりします。やみくもにすべて暗号化ではなく、暗号化すべき場面をしっかり意識します。プロキシーやWAFで一度暗号化解除をして監視することも必要です。

標的型攻撃の対策～セキュリティ担当部署～

- 被害の予防
  - セキュリティ教育の実施
  - 情報の管理とルール策定
  - 組織内CSIRTの運用
  - サイバー攻撃に関する情報共有





標的型攻撃は、一度発生すれば同業他社でも発生する可能性が高い攻撃です。速やかな情報共有が被害を食い止めます。JPCERT/CCに報告することで社内だけでなく広く注意喚起することも可能です。また、被害を未然に防ぐためには日ごろからのセキュリティ教育が必須です。一度にまとめてたくさんではなく、定期的に短い時間で少しづつ意識付けをするほうが効果的です。

Computer Software Association of Japan

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

CSAJ

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

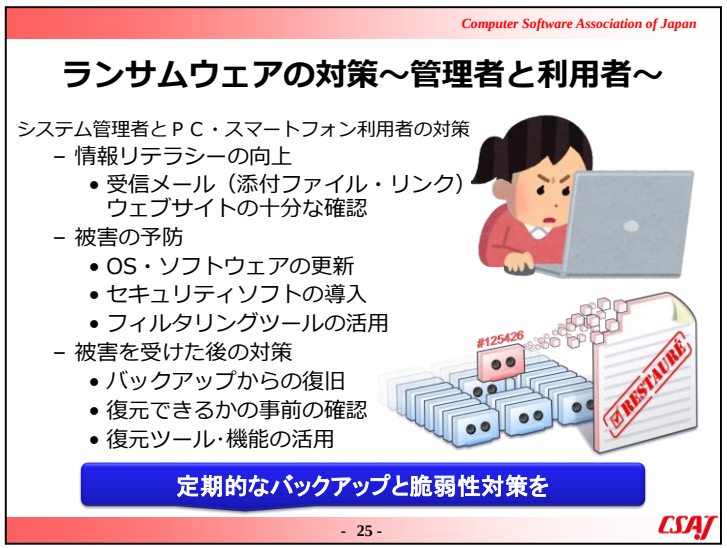
暗号化されてもファイルを復元できる可能性

Computer Software Association of Japan

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社のレポートにいると、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ヵ国３００万ユーザーの顧客を持つ企業です。

Computer Software Association of Japan

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

CSAJ

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

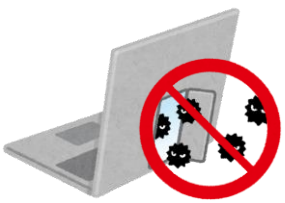
医療機器インスリンポンプに遠隔操作可能となる脆弱性

- 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

Computer Software Association of Japan

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。

Computer Software Association of Japan

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出てきます。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。

対策の流れは通常の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となってきます。

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ういう分類をされており、どういう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、脅威とぜ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

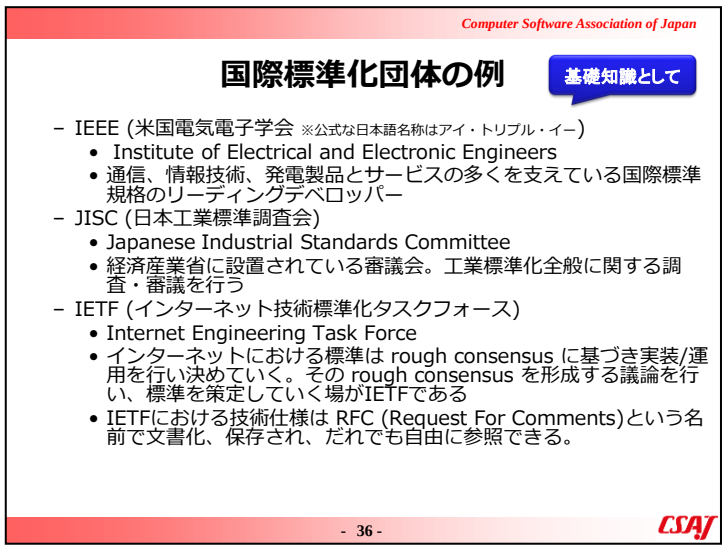
- ISO (国際標準化機構)
  - International Organization for Standardization
  - 国家間の技術的障壁を取り除くための、汎用的な国際標準を策定する非政府組織。
- IEC (国際電気標準会議)
  - International Electrotechnical Commission
  - 電気工学、電子工学、および関連した技術を扱う国際的な標準化団体。一部規格はISOと共同開発。
- ITU (国際電気通信連合)
  - International Telecommunication Union)
  - 世界最古の国際機関。無線通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。



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)という点が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元、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

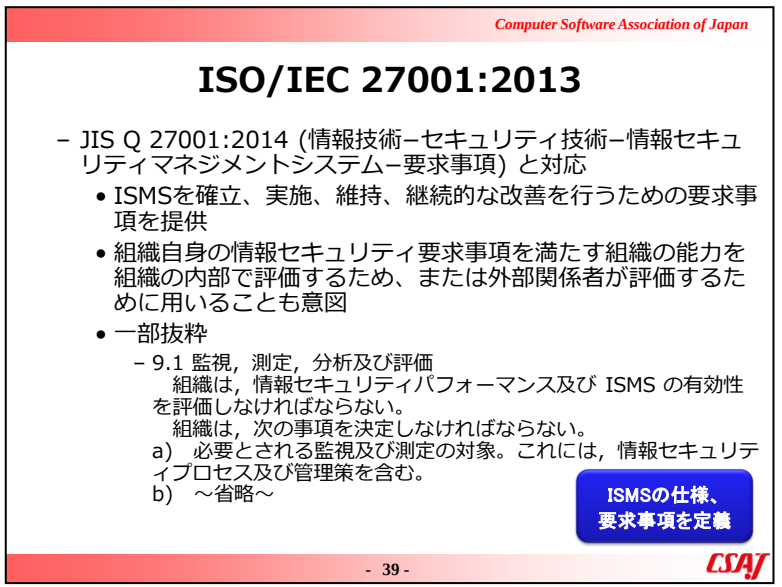
- JIS Q 27000:2014 (情報技術−セキュリティ技術−情報セキュリティマネジメントシステム−用語) と対応
  - ISMS ファミリ規格に関連する用語及び定義について規定
  - 一部抜粋
    - 2.28 情報セキュリティガバナンス（governance of information security）
      組織（2.57）の情報セキュリティ活動を指導し，管理するシステム。
    - 2.57 組織（organization）
      自らの目的（2.56）を達成するため，責任，権限及び相互関係を伴う独自の機能をもつ，個人又は人々の集まり。
    - 2.56 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が伝われば十分です。

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



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ほうが良いかもしれません。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。

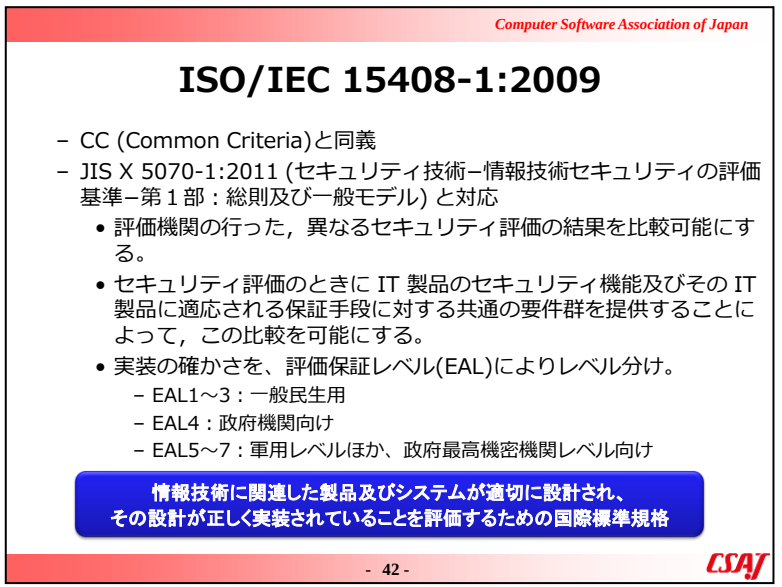
組織の情報セキュリティ活動を指導し、管理するシステムについての規格であるISO/IEC 27014は2013年に第1版が発行されました。JIS化されたのは2015年であるため、最近の動向として紹介します。

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]



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を使う暗号通信プトロコルの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倍に高めるという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、マルウエア感染、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。

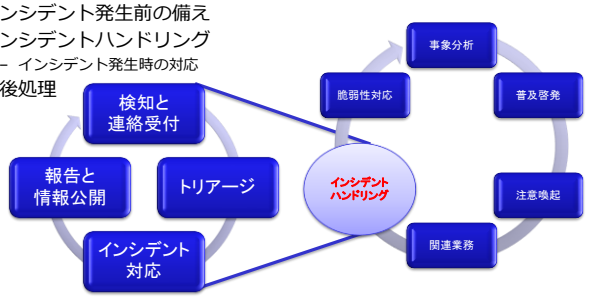
情報セキュリティインシデントに対し、インシデント対応がよくクローズアップされますが、インシデント対応とはインシデント発生後の被害を最小限にするための「事後」対応にすぎません。この「事後」対応であることは伝えてください。インシデント対応を行うためには、相応の準備が必要です。その準備はインシデント管理と呼ばれ、その一部がインシデント対応となります。

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。

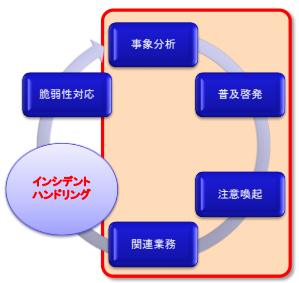
インシデント対応を行うにはインシデント管理が不可欠です。これはインシデント発生前の備えを行い、インシデント発生時の対応を明確にし、事後処理を行う一覧の活動となります。

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ことが必要です。

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。

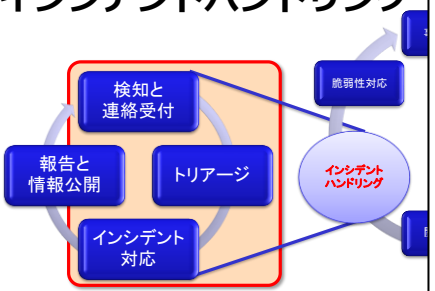
インシデント対応ポリシー

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

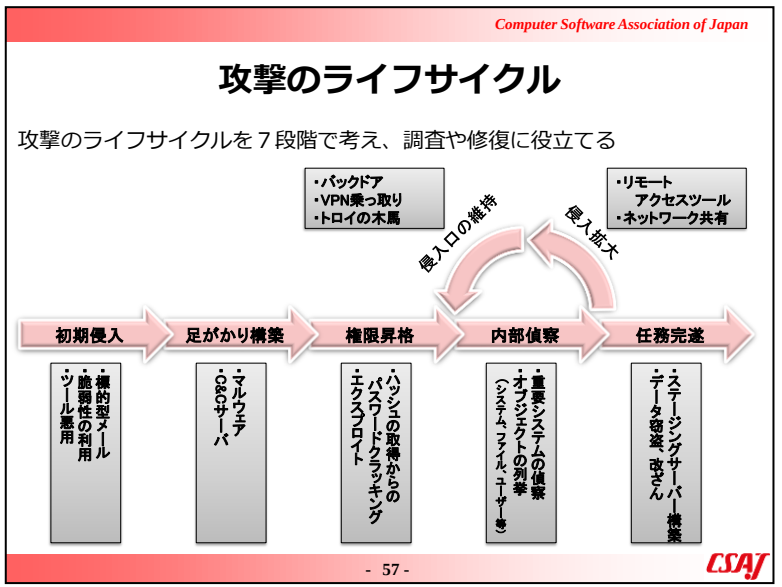
インシデントに対応するか否かを決定する重要な段階です。判定に迷った場合、「守るべき情報資産は何か？」「どのようなリスクが存在するか」というセキュリティ対策の基本に戻って考えてください。個々の事象にとらわれると収拾がつかなくなることがあります。

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。



・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的な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。

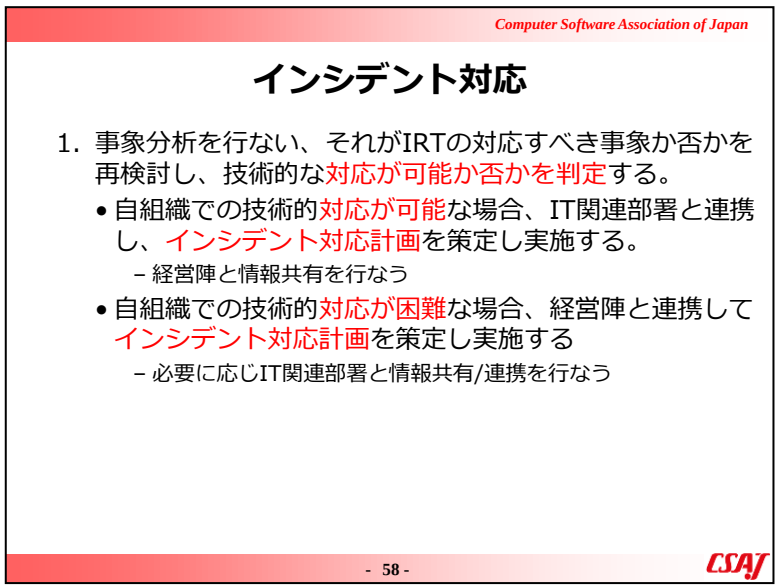
・補足説明

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



・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

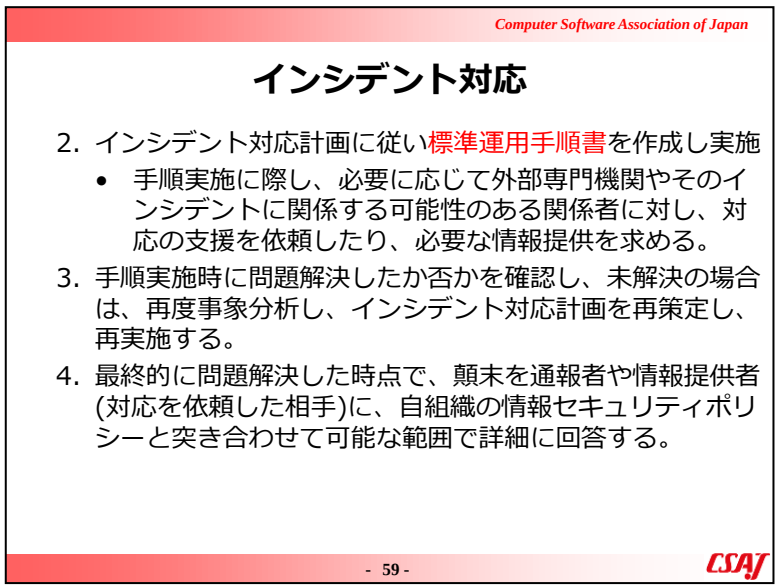
　インシデント発生後のインシデント対応は慌てて行ってはいけません。自己判断で勝手に対応を行うことで、より状況が悪くなることもあります。まずはインシデント対応計画を策定し、その計画に従った標準運用手順書を作成し、その手順書に従った作業を行う必要があります。

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



・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

CSAJ

・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

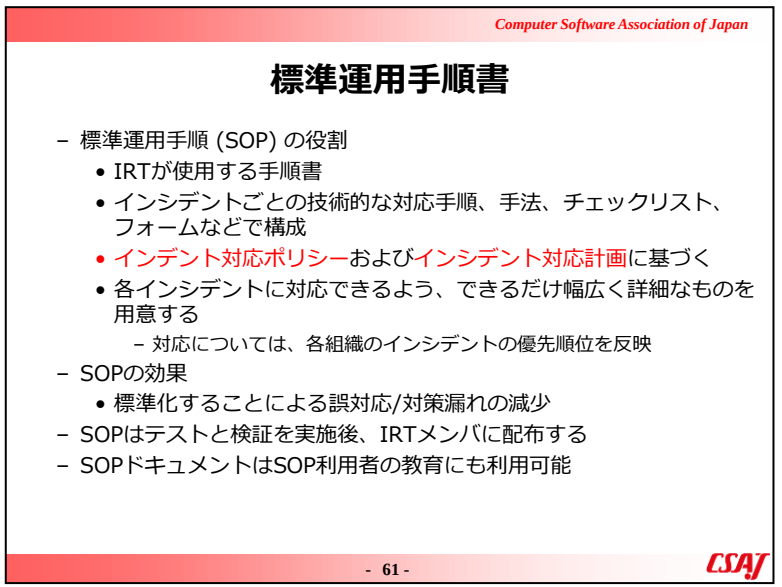
・質問（問いかけ）

・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



・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

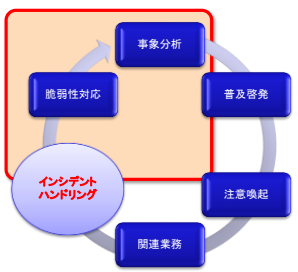
・（ある場合は）演習の使い方・注意点・フィードバックのポイント・使用ツール

Computer Software Association of Japan

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



CSAJ

・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）

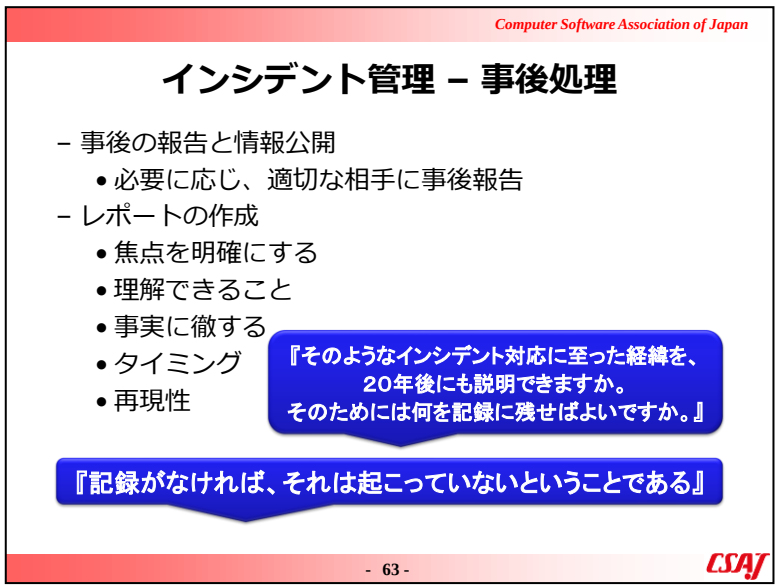
なぜ事後処理が必要か。

・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



・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とありますが、「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。

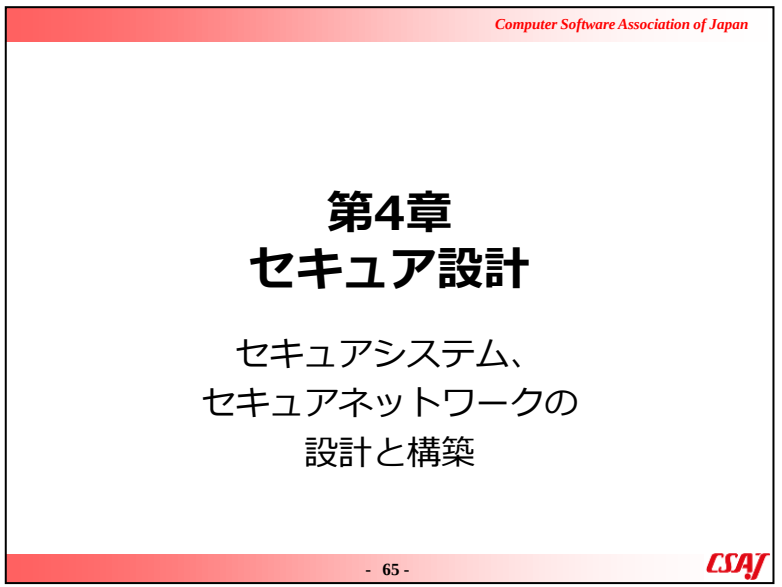
・質問（問いかけ）

・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。



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。

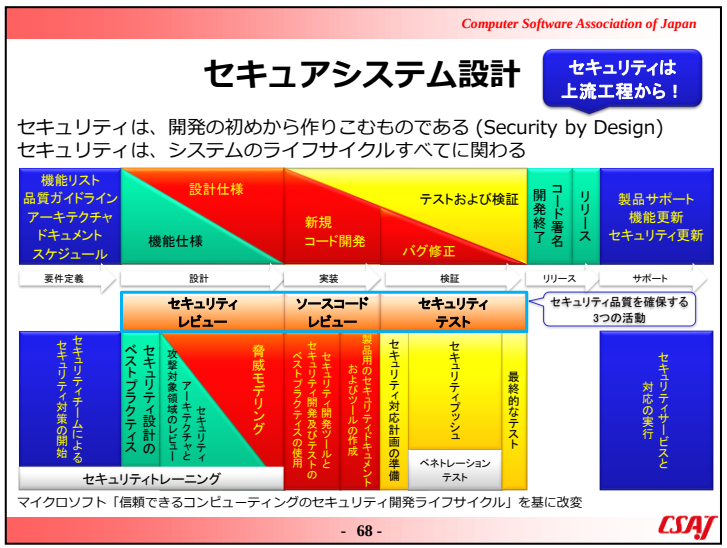
・質問（問いかけ）

・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



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るか
・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

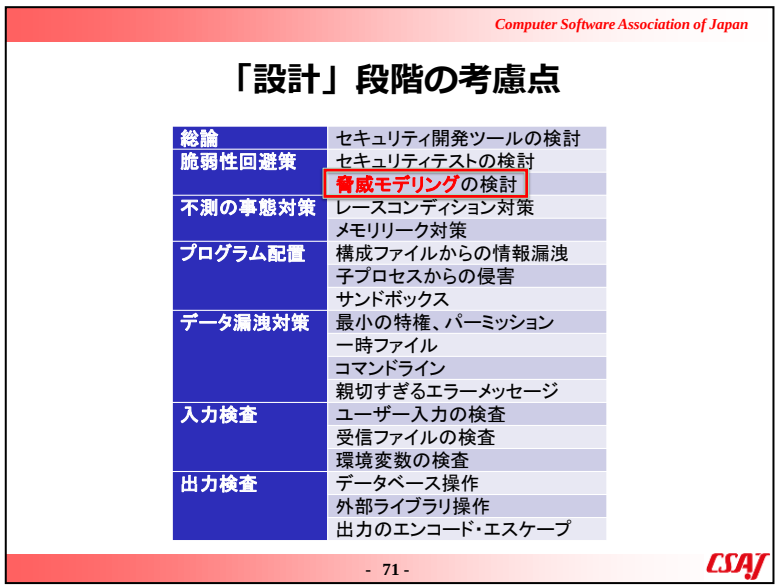
「要件定義」段階の考慮点

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。



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)

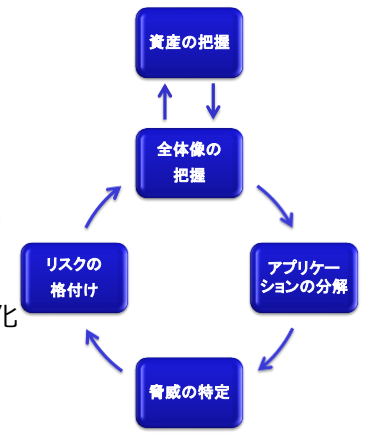
STRIDE & DREAD 脅威モデリングは、1999年にマイクロソフトが提唱した手法で、OWASPおよびIPAでも採用されています。マイクロソフトの製品群はこの脅威モデリングの下で設計されており、その効果は実地で実証されています。

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

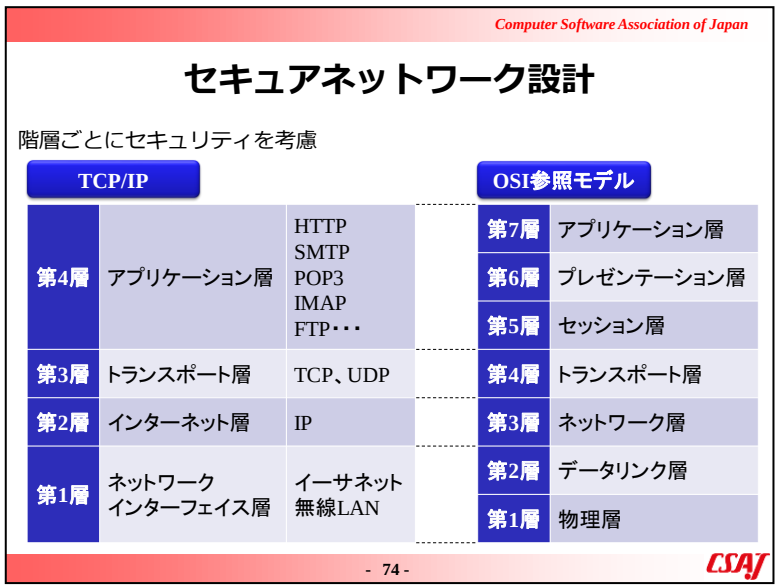
- 資産の把握
  - 守るべき対象を確認
- 全体像の把握
  - 主要な機能や特徴を確認
- アプリケーションの分解
  - 信頼境界、データフロー、入出力の特定
- 脅威の特定
  - 本当に困ることをリスト化
- リスクの格付け
  - 資産価値×脅威×脆弱性



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はなく、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。

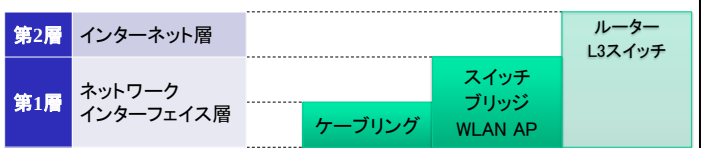


ここでは復習として、TCP/IP階層モデルとOSI参照モデルの対応を提示しています。ネットワークをセキュアに保つには、各階層でどのような情報がやり取りされているかと、その情報を守る方法は何かを把握することがポイントとなります。

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



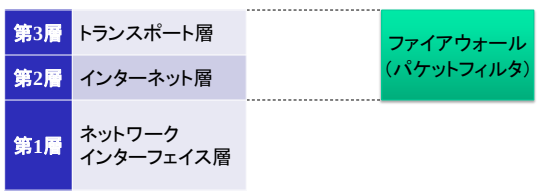
ルーターは第3層の装置として認識されていますが、ルーティング時にMACアドレスを変換することに軽く触れ、意識付けは行ってください。ルーターにキャッシュされるMACアドレスがARPスプーフィングで汚染されている場合、ルーティング先が意図しないホストになる場合があります。

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ーを用いケースがあります。

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



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。

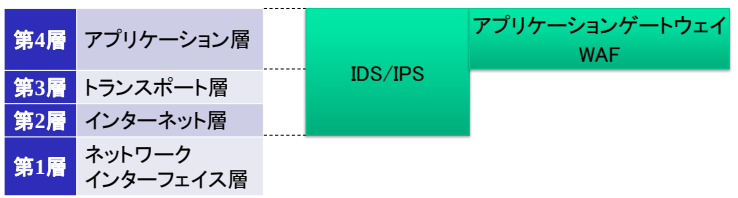
ステートフル・インスペクションは、動的パケットフィルタリングのバリエーションの一つと考えるとわかりやすいかもしれません。情報セキュリティスペシャリスト試験（平成27年秋期午前II問３）では、ステートフル・インスペクションについては以下の説明が正解とされています。

「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。

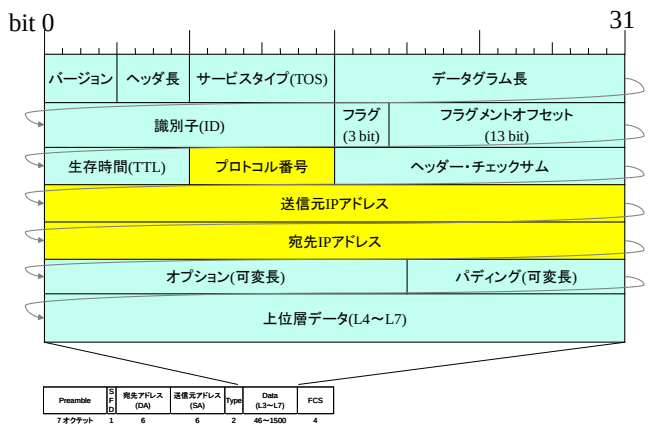
参考：Ethernet v2 フレーム形式

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

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。

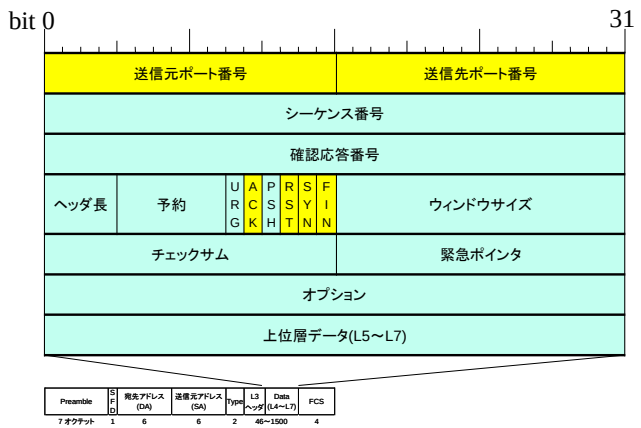
どんなデータをチェックできるのか説明する参考資料として使ってください。詳しい説明は不要です。

参考：IPパケット形式



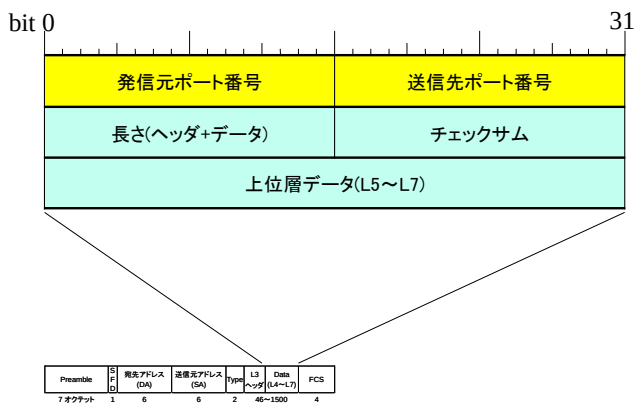
どんなデータをチェックできるのか説明する参考資料として使ってください。詳しい説明は不要です。

参考：TCPヘッダー形式



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。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。

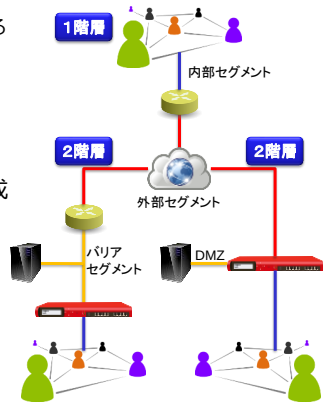
参考：UDPヘッダー形式



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。

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

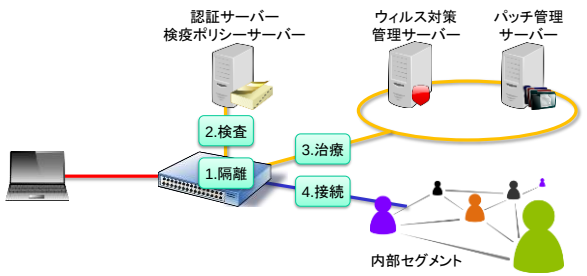


ネットワークのセキュリティ境界を意識付けしてもらえれば十分です。外部公開するサーバーがなければセキュリティ境界は内部と外部しかないので、1階層で十分です。逆に、3階層以上の多層構造となっている場合、無駄なコストをかけていないか、各ネットワークセグメントの性格について調査する必要があるかもしれません。

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で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：ウィ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に対応したウィ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ことがあります。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こっている
    - {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. つながる世界を拡げていくためには、「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ってくる

IPA「ＩｏＴ開発における セキュリティ設計の手引き」より

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。

Computer Software Association of Japan

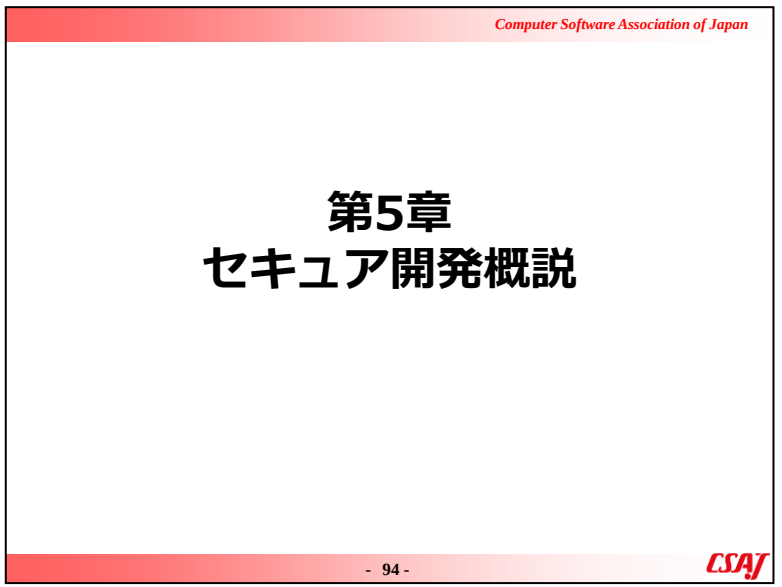
4-2. セキュアシステム、ネットワークの設計 ～グループ演習～

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

CSAJ

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



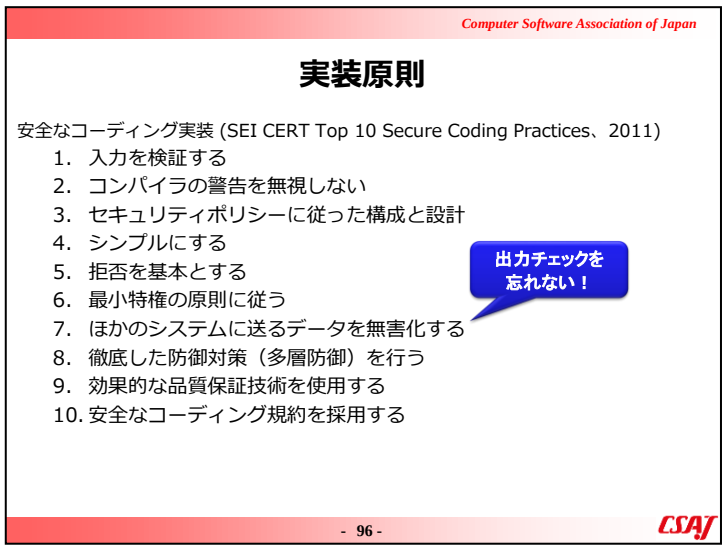
Webアプリを例とし、アプリケーション内のセキュリティ境界を説明できる。

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

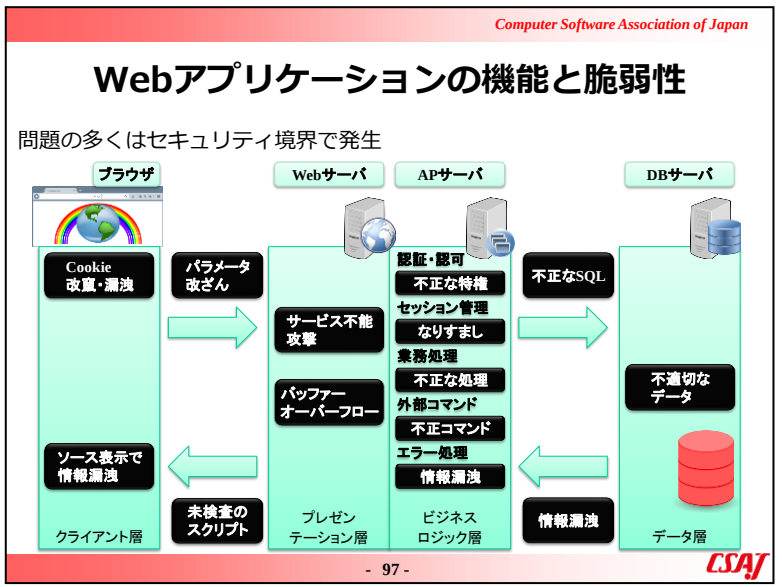


IPAが提供するセキュアプログラミング講座でも同じ実装原則を提示しています。ただし順番が異なっているため、このスライドではオリジナルに合わせた順番にしてあります。

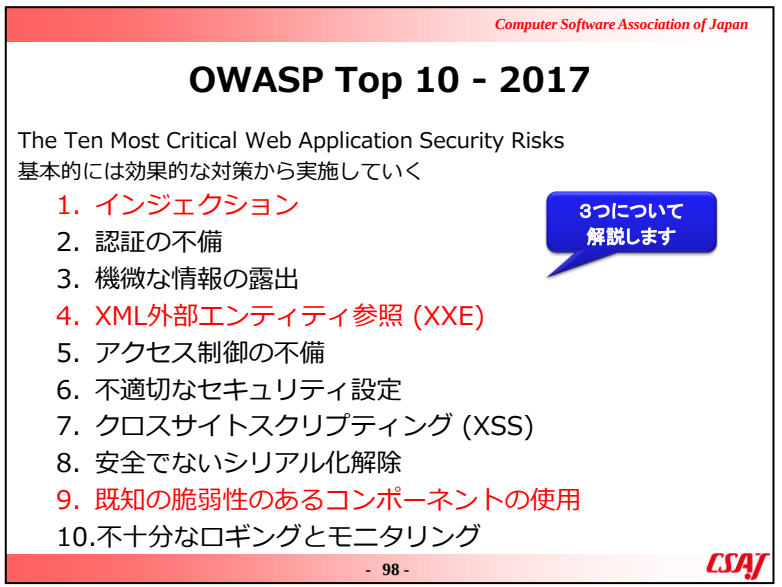
https://wiki.sei.cmu.edu/confluence/display/seccode/Top+10+Secure+Coding+Practices

「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。



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。



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ーワード」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、アカウンティング（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
- パ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。

Computer Software Association of Japan

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

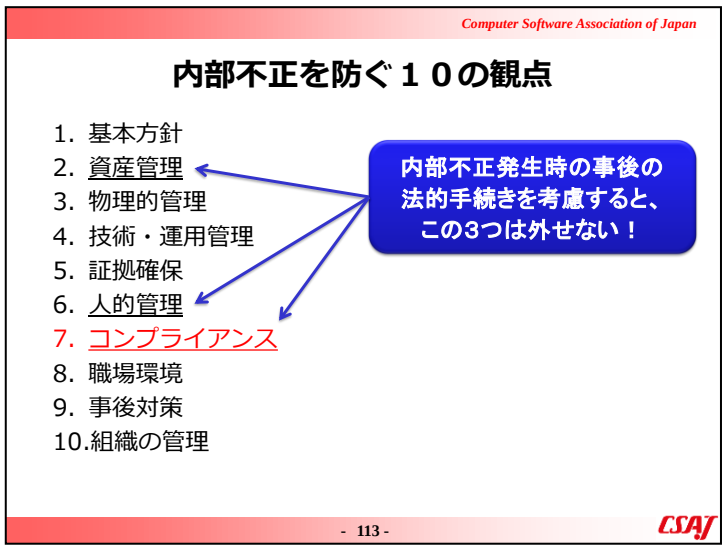
（1）組織における内部不正防止
（2）内部不正を防ぐ１０の観点
（3）コンプライアンスとは
　① コンプライアンス遵守対策
　② コンプライアンス～法的手続きの整備～
　③ コンプライアンス～誓約書の要請～

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の割の良い行動です。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出てきます。



・説明の流れ

全ての観点で対策が必要なわけではないですが、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。

Computer Software Association of Japan

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となる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

Computer Software Association of Japan

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ィア、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

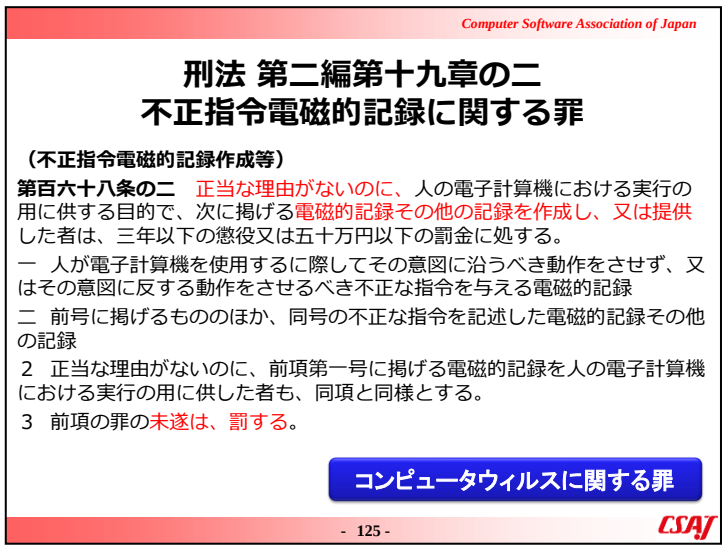
- 刑法
- サイバーセキュリティ基本法
- 著作権法
- 電気通信事業法
- 電子署名及び認証業務に関する法律
- 電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律
- 電波法
- 特定電子メールの送信の適正化等に関する法律
- 不正アクセス行為の禁止等に関する法律
- 有線電気通信法

・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っと紹介します。

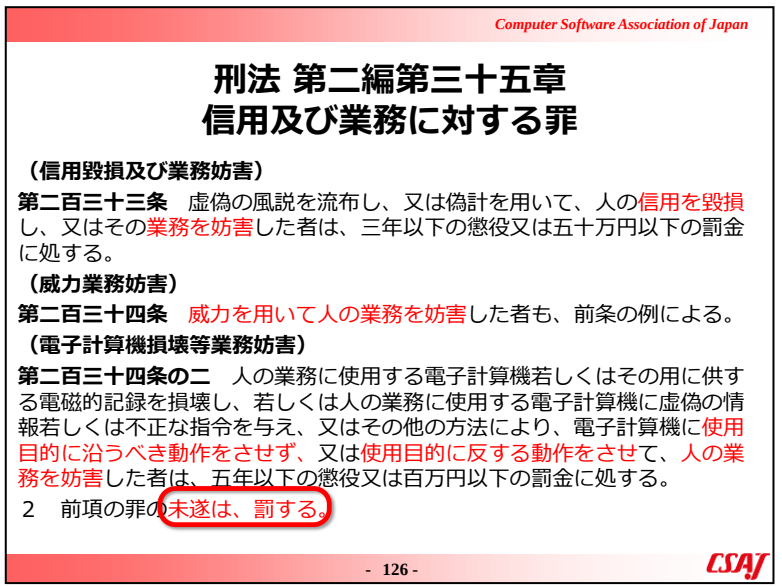


・説明の流れ

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「コンピュータウィルスに関する罪」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。

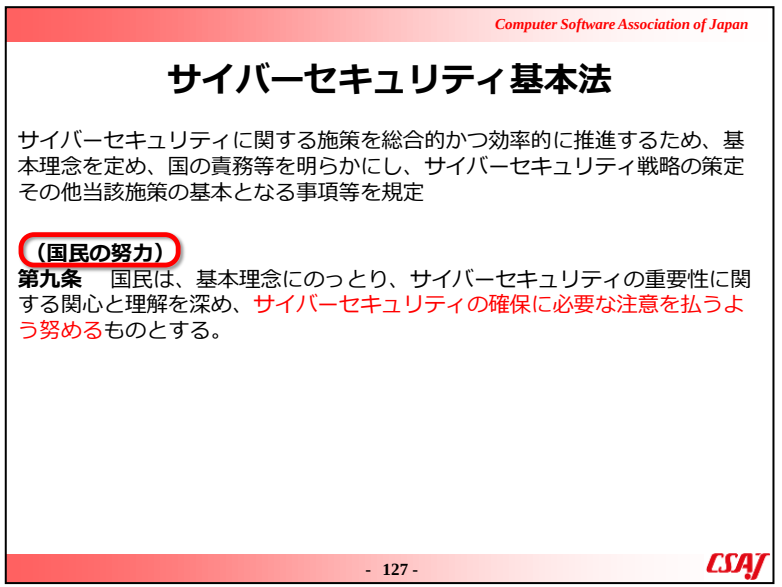


・説明の流れ

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。



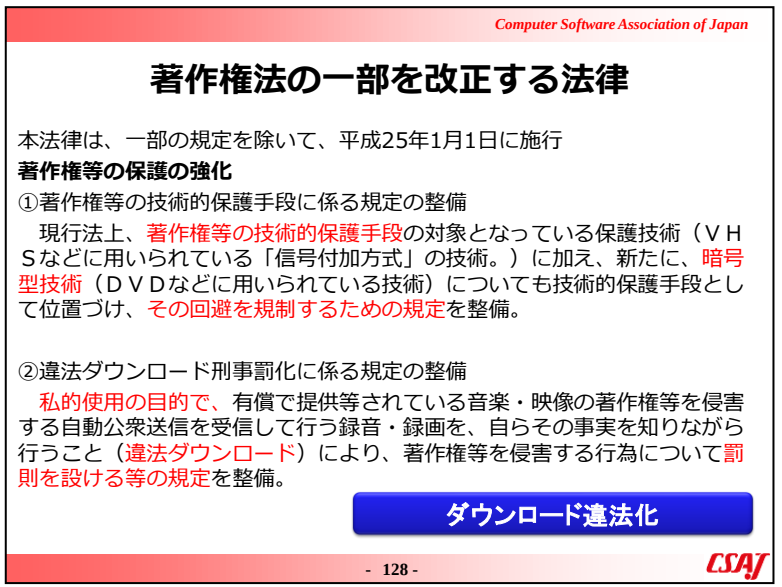
・説明の流れ

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

ュリティ対策以前に、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。

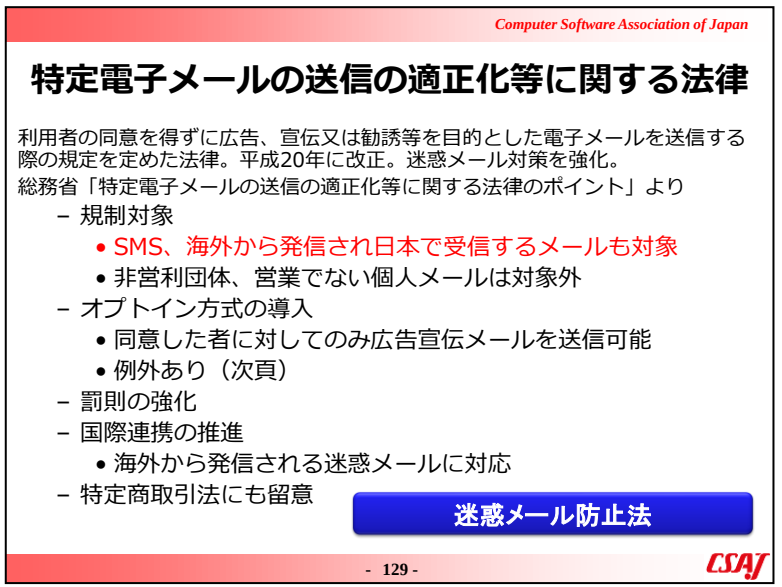


・説明の流れ

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。



・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）

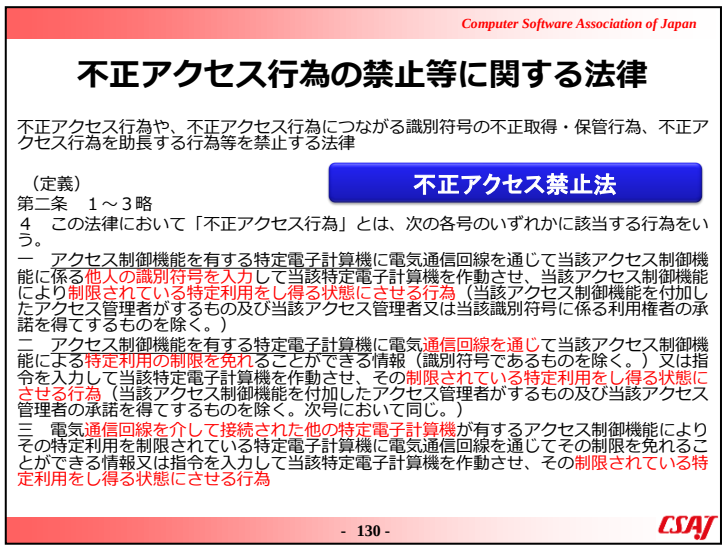
海外から発信されるメールも対象となっている。国際連携も視野。

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。



・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実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～
　① 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こと
  - 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。

Computer Software Association of Japan

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。

CSAJ

・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。

Computer Software Association of Japan

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

CSAJ

・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。

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　プリント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

目次

第1章
最新動向

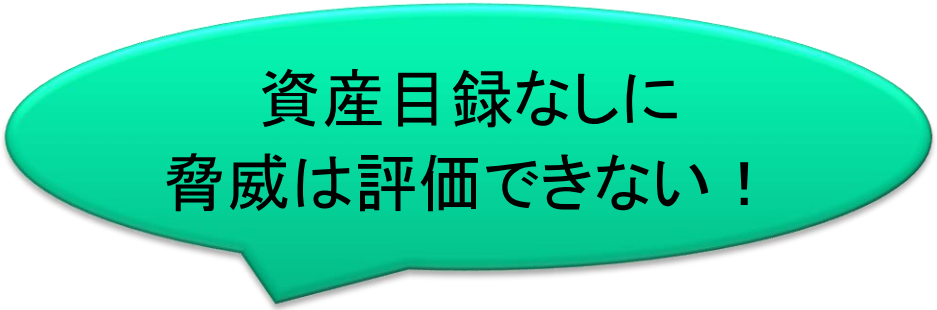
情報セキュリティ10大脅威

1-1. 脅威の動向、手口、対策

（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



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

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

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

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。

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。

脅威、脆弱性、リスクの関係

システム、
ネットワーク
への攻撃

脅威

脆弱性

論理的

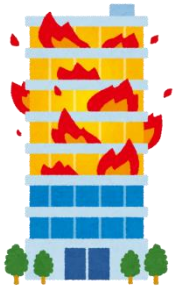
情報資産

人的

物理的

脅威

誤操作
詐欺
機密漏洩



脅威

不法侵入、盗聴器、
火災、洪水、地震、
テロリストの襲撃

脆弱性の
対策を

リスク ＝
情報資産 × 脅威 × 脆弱性

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

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。

リスクと管理策の関係

システム、
ネットワーク
への攻撃

脅威 ＋ 設定

論理的

情報資産

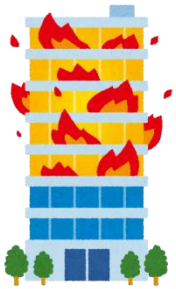
人的

物理的

規則
と
教育

脅威

誤操作
詐欺
機密漏洩

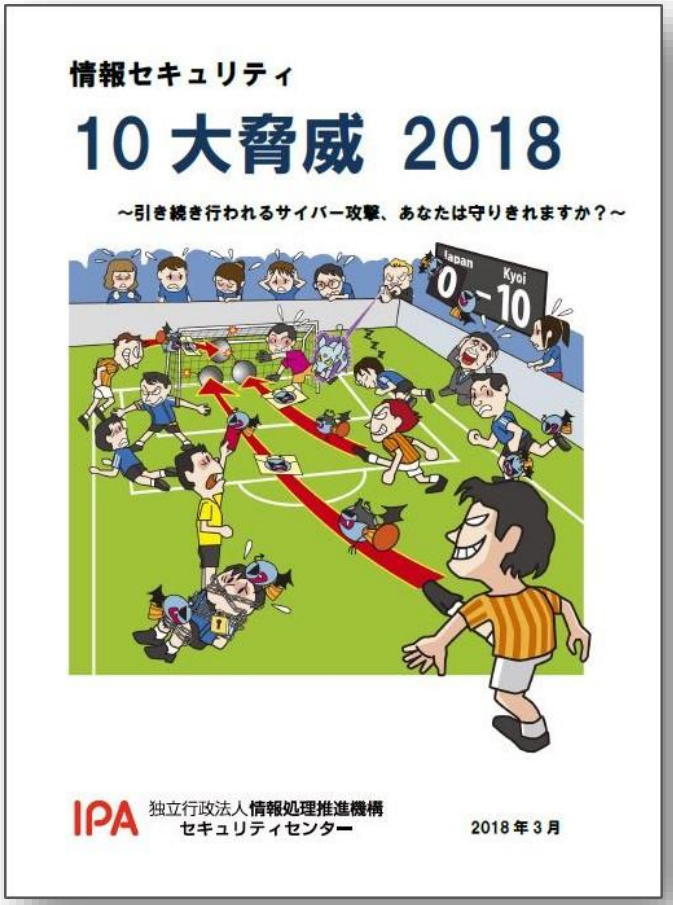


不法侵入、盗聴器、
火災、洪水、地震、
テロリストの襲撃

脅威 ＋ 警備、
建物の選択

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。



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）

標的型攻撃による情報流出

標的型攻撃

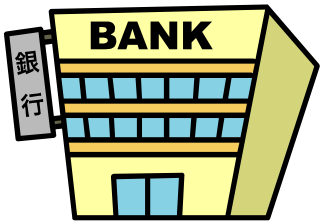
- メールによるウイルス感染等により組織内部に侵入
- 組織の機密情報が流出
- 取引先や関連会社を踏み台にして本丸を狙うことも

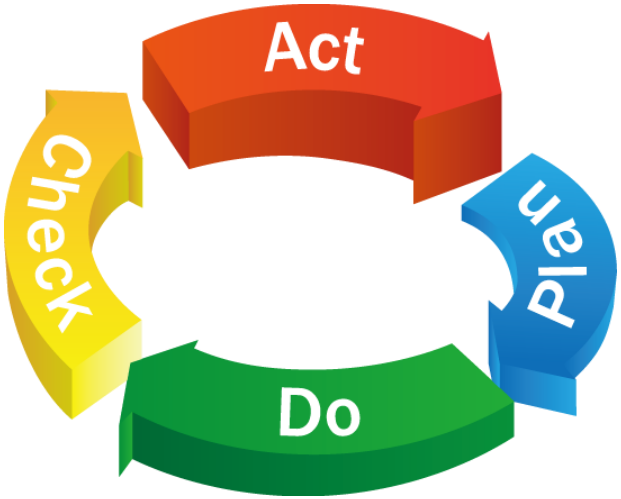
手口

- 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

標的型攻撃の対策～経営者層～

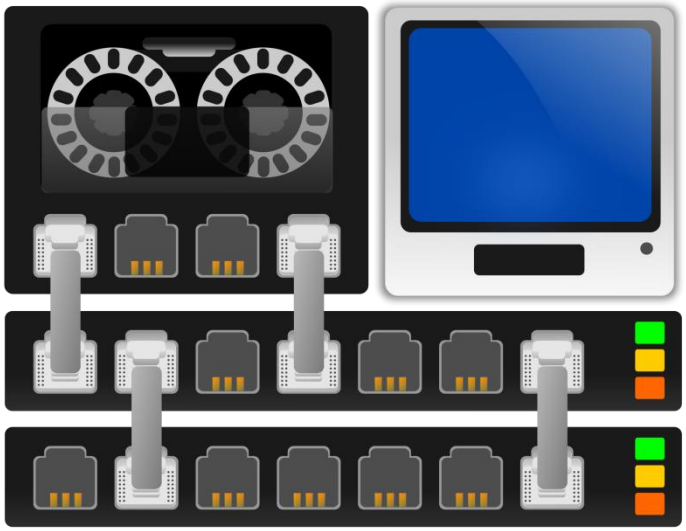
– 組織としての対応体制の確立
  - 問題に迅速に対応できる体制(CSIRT)の構築
  - 対策予算の確保と継続的な対策実施

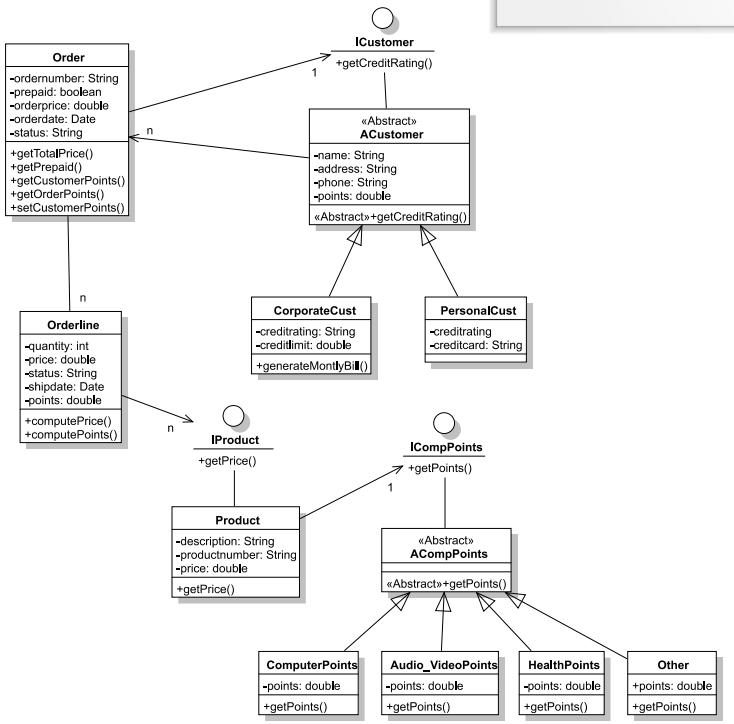




標的型攻撃の対策～システム管理者～

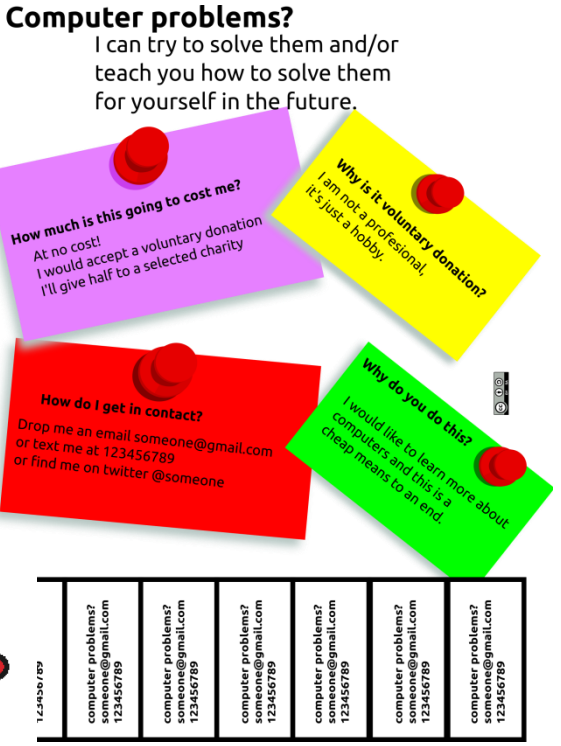
- 被害の予防
  - 被害を抑止するためのシステム設計
  - アクセス制御・データの暗号化
- 被害の早期検知・事後対策
  - ネットワーク監視・分離

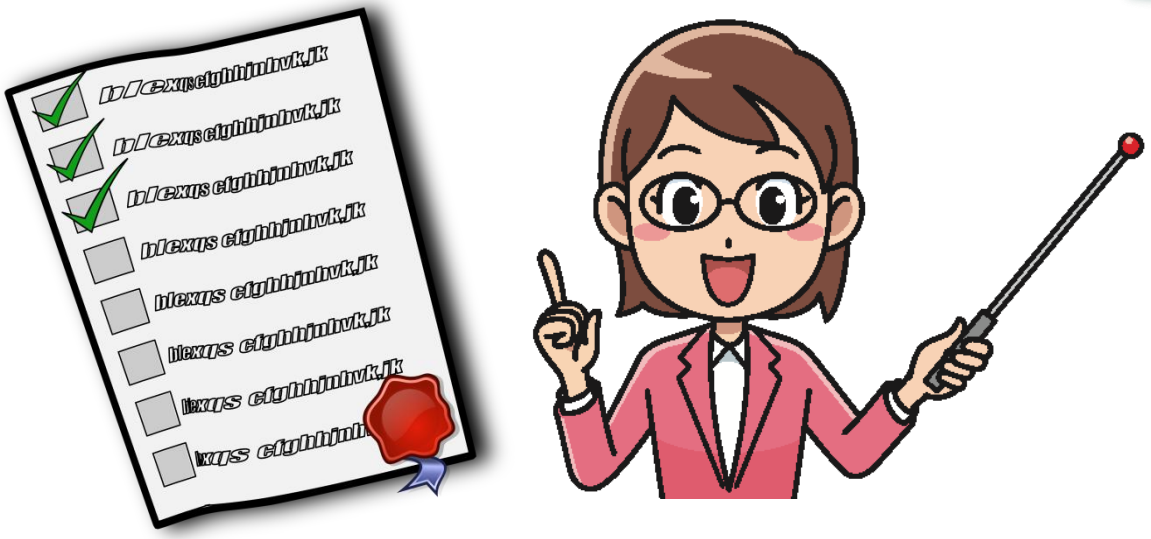




標的型攻撃の対策～セキュリティ担当部署～

- 被害の予防
  - セキュリティ教育の実施
  - 情報の管理とルール策定
  - 組織内CSIRTの運用
  - サイバー攻撃に関する情報共有





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

ランサムウェアによる被害

ランサムウェア

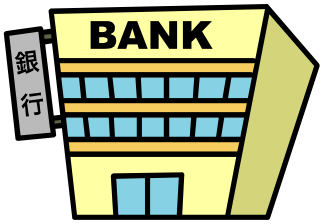
- PC内のファイルの暗号化や、スマートフォンの画面のロックを行い、復元に身代金を要求
- 2016年はランサムウェアの被害が急増している

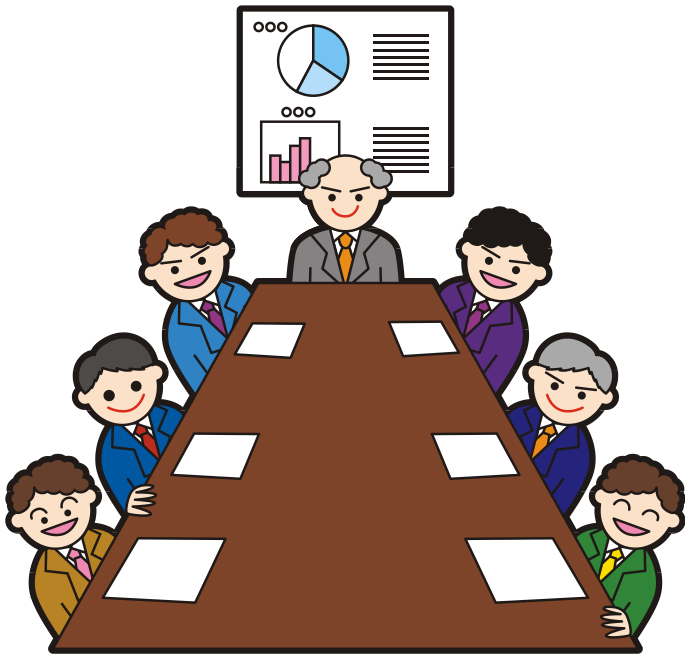
手口/影響

- 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

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

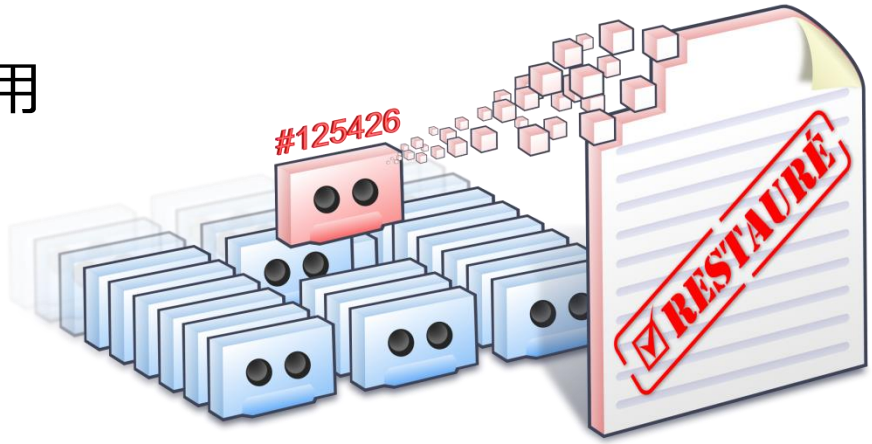




ランサムウェアの対策～管理者と利用者～

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

IoT機器の脆弱性の顕在化

IoT機器の脆弱性

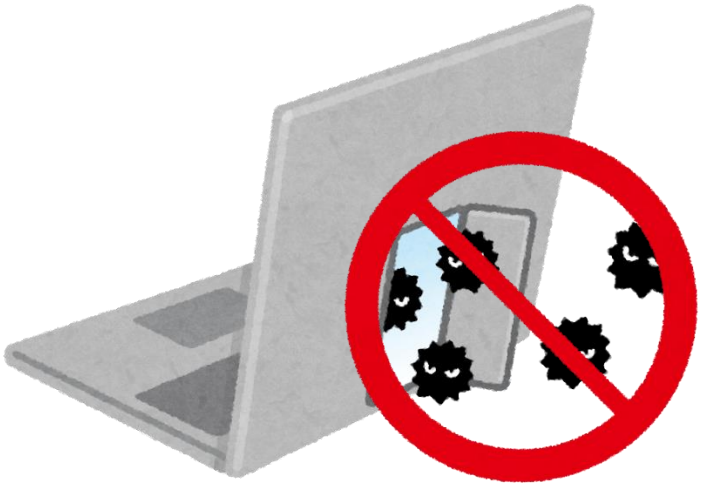
- IoT機器の脆弱性が悪用され、ウイルス感染や不正利用される
- 不正利用されたIoT機器がボット化し、DDoS攻撃等に悪用されるケースも

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

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)



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

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

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

（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

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！

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

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。

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。

2-2. 規格詳細

（1）ISMSファミリ規格

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

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 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

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/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 製品に適応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**

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を使う暗号通信プトロコルの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

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

（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、マルウエア感染、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（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

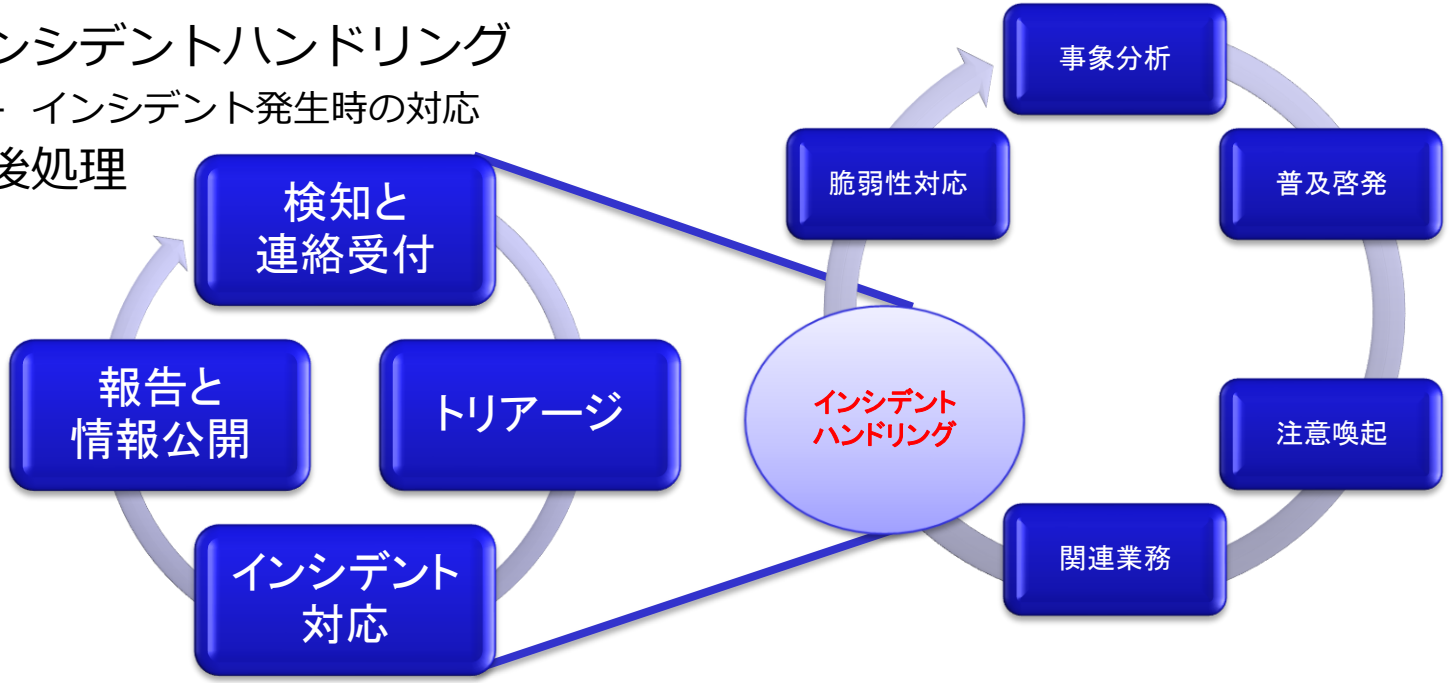
- インシデント対応（IR: incident response）
  - 差し迫ったハザードの原因を食い止めるため，及び不安定又は中断・阻害を引き起こす可能性のある事象の結果を軽減し，正常な状況に復旧するために講じる処置。

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

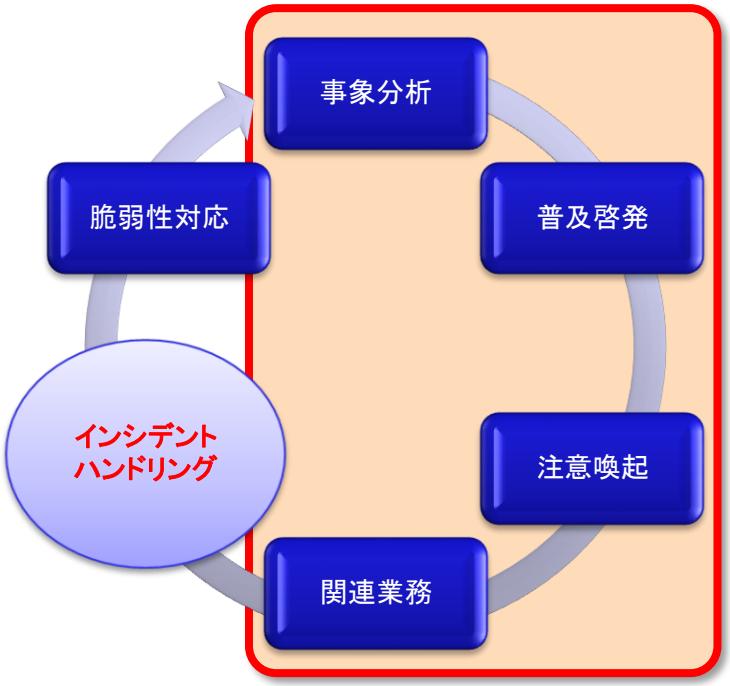


- インシデント対応チーム（IRT: Incident Response Team）
  - 別名シーサート (CSIRT: Computer Security IRT)
  - 情報セキュリティインシデントに対応する専門チーム
  - インシデント管理は、IRT/CSIRTを中心に実施

インシデント管理 – 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 – 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

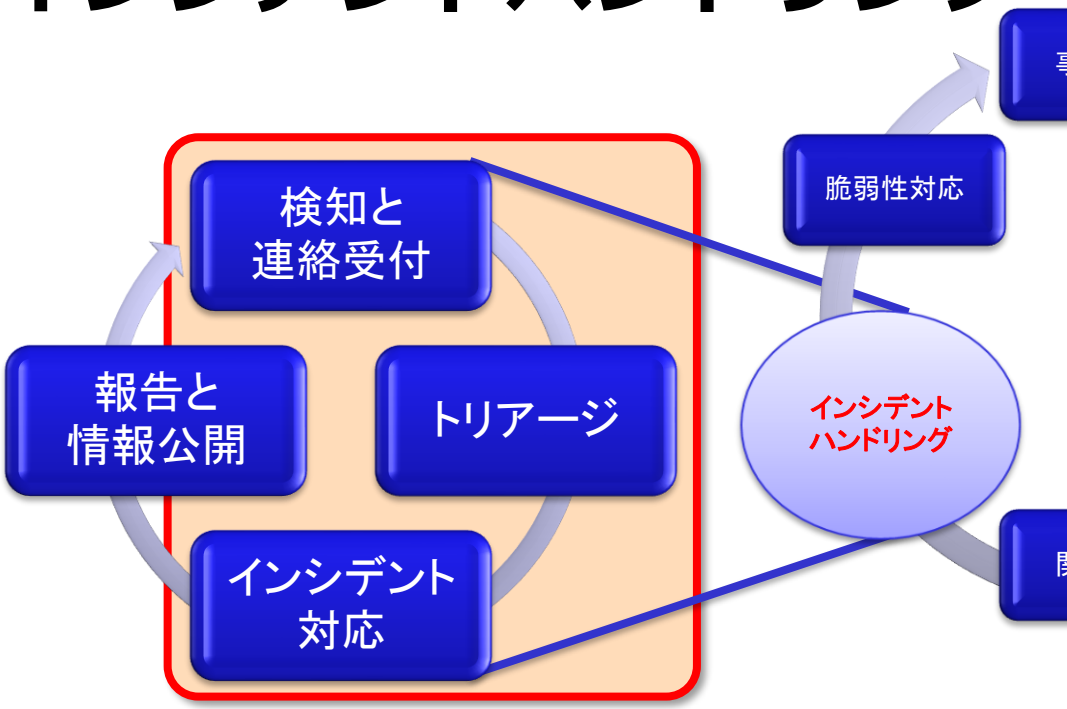
インシデント対応ポリシー

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

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



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

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

トリアージ判定後の流れ

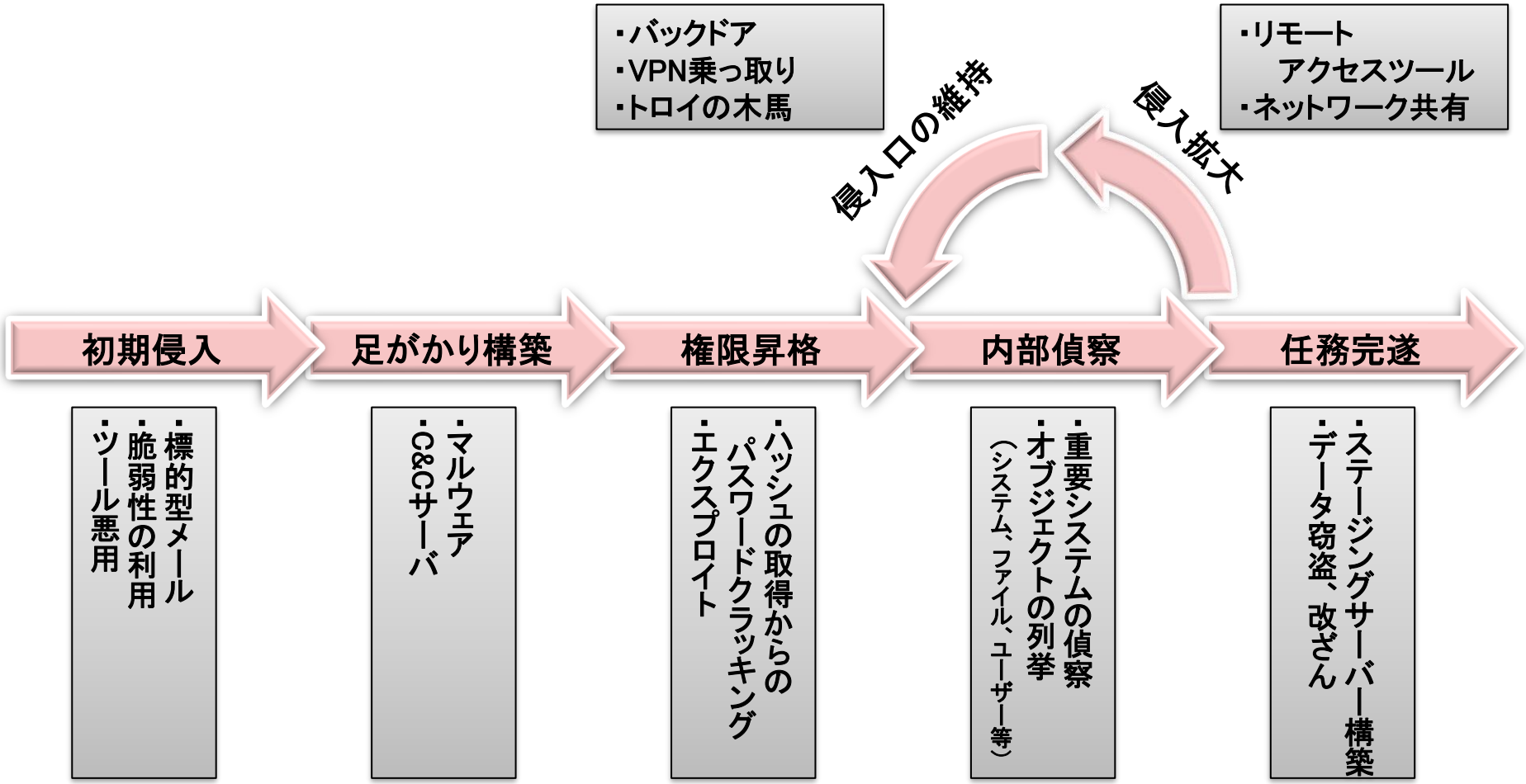
得られた情報から事実関係を確認し、IRT が対応すべきか否かを判定

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

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



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

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。

インシデント対応計画

インデント対応計画 (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

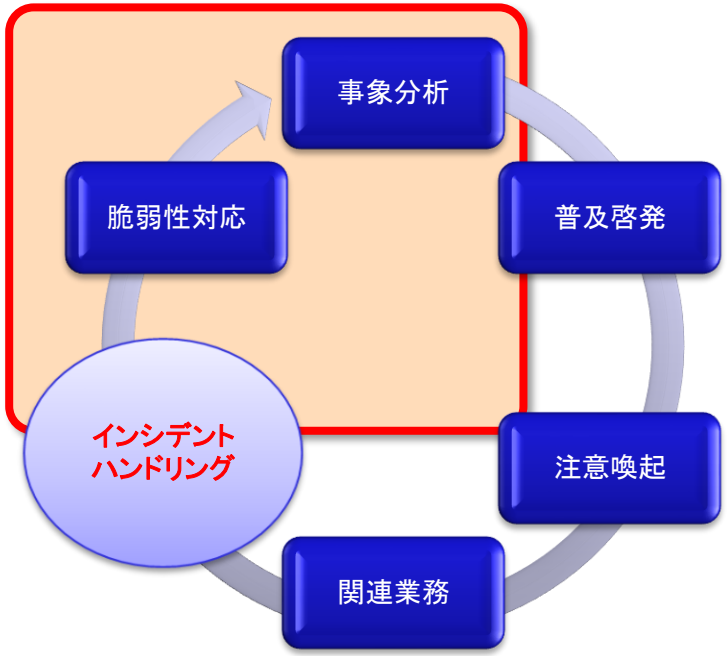
標準運用手順書

- 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

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



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』

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

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

（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

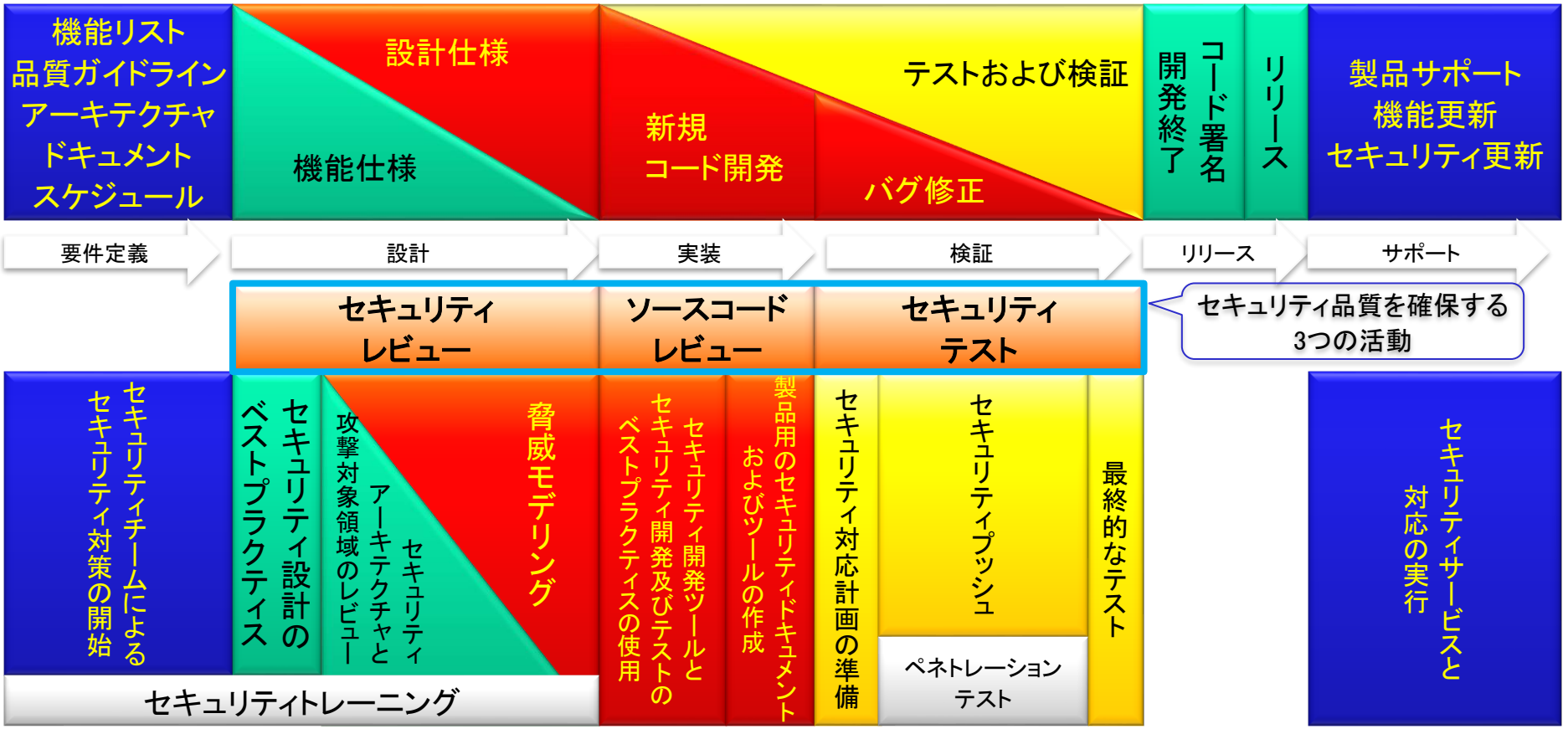
ソフトウェアエンジニアリングの原則 (Saltzer and Schroeder [1975])

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。

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

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

「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

「設計」段階の考慮点

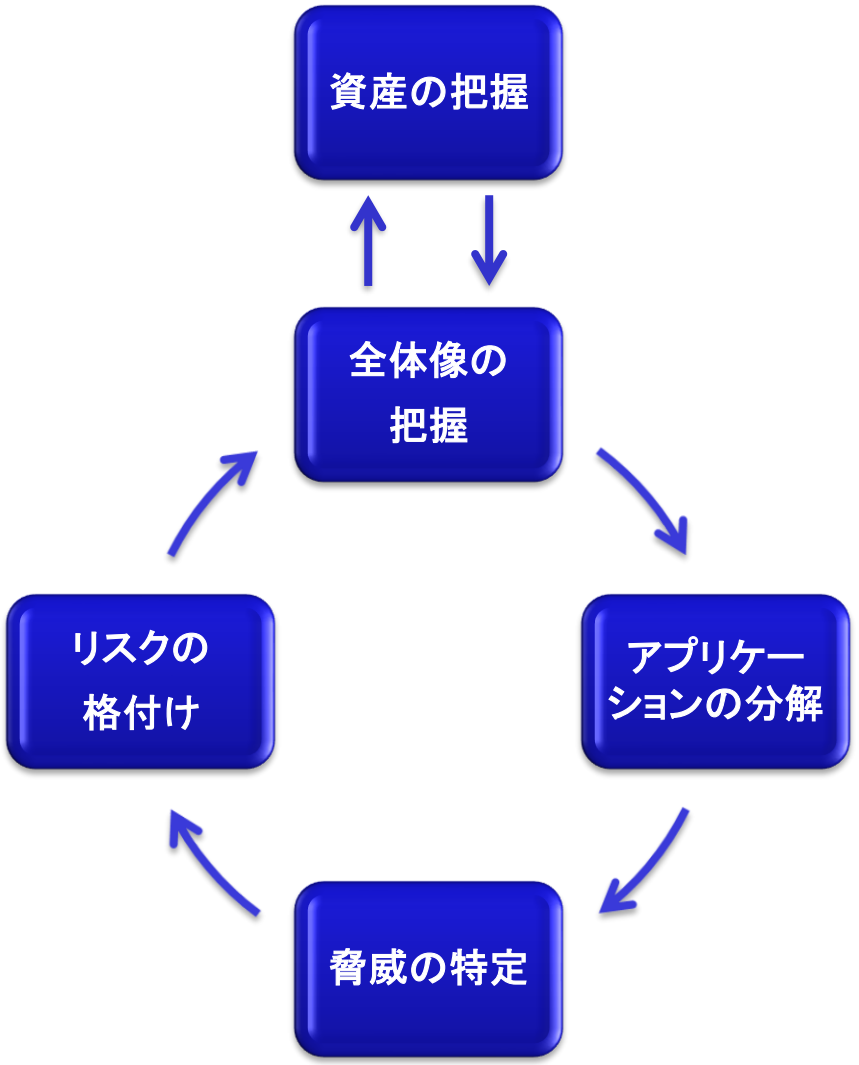
総論	セキュリティ開発ツールの検討
脆弱性回避策	セキュリティテストの検討
	脅威モデリングの検討
不測の事態対策	レースコンディション対策
	メモリリーク対策
プログラム配置	構成ファイルからの情報漏洩
	子プロセスからの侵害
	サンドボックス
データ漏洩対策	最小の特権、パーミッション
	一時ファイル
	コマンドライン
	親切すぎるエラーメッセージ
入力検査	ユーザー入力の検査
	受信ファイルの検査
	環境変数の検査
出力検査	データベース操作
	外部ライブラリ操作
	出力のエンコード・エスケープ

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)

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



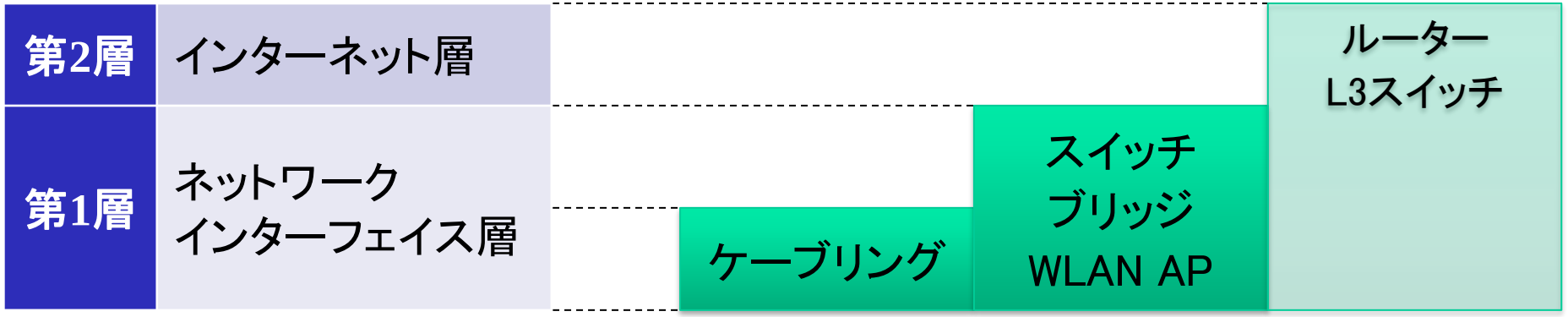
セキュアネットワーク設計

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6層	プレゼンテーション層
			第5層	セッション層
第3層	トランスポート層	TCP、UDP	第4層	トランスポート層
第2層	インターネット層	IP	第3層	ネットワーク層
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2層	データリンク層
			第1層	物理層

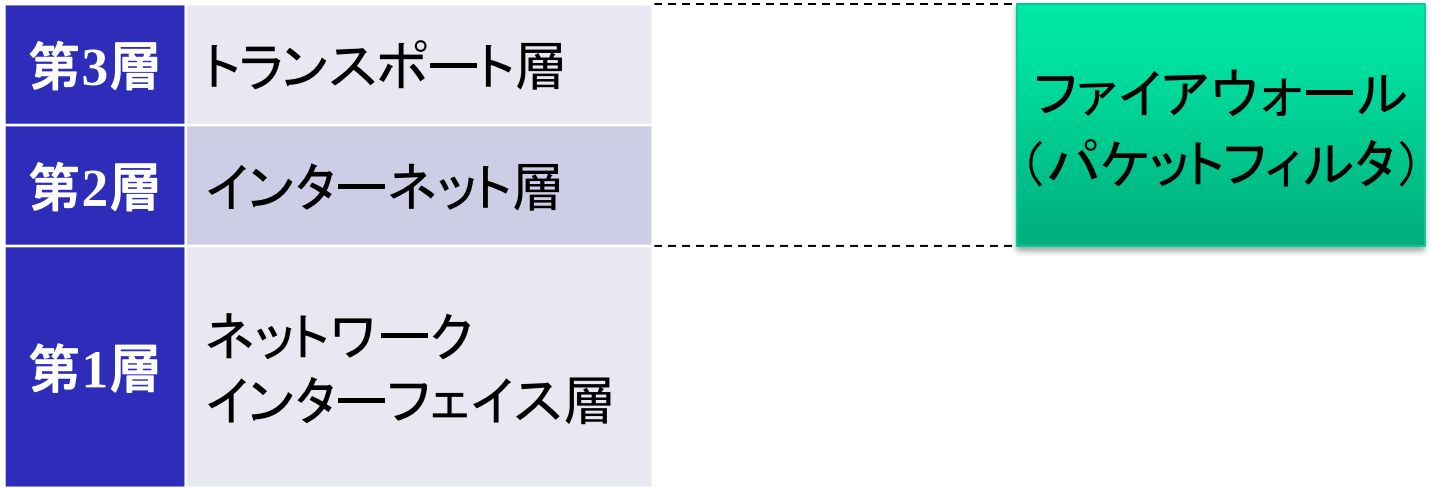
ネットワークインターフェイス層

- 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



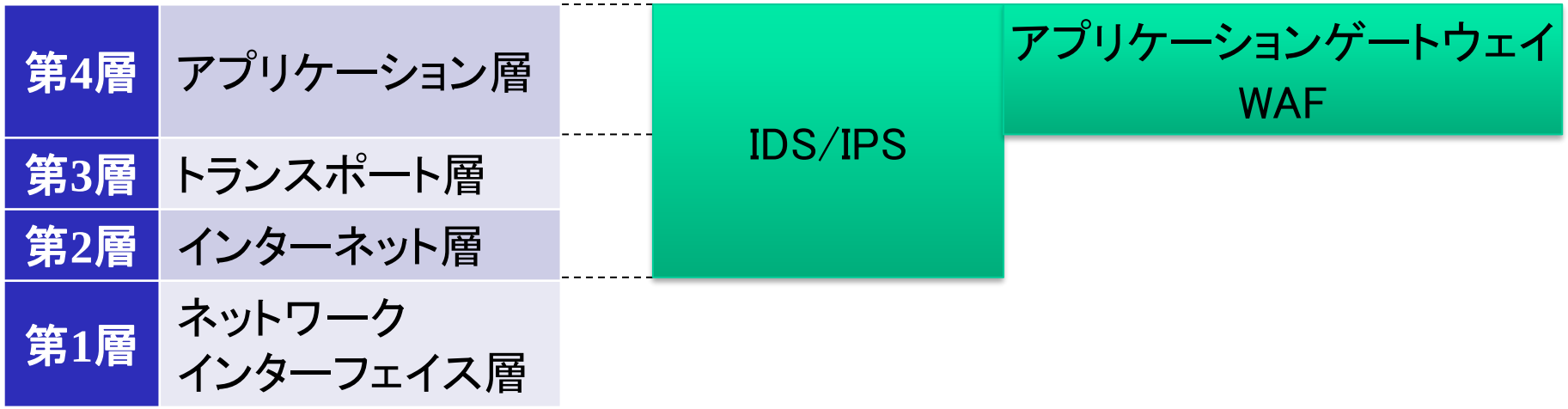
インターネット層とトランスポート層

- 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



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。

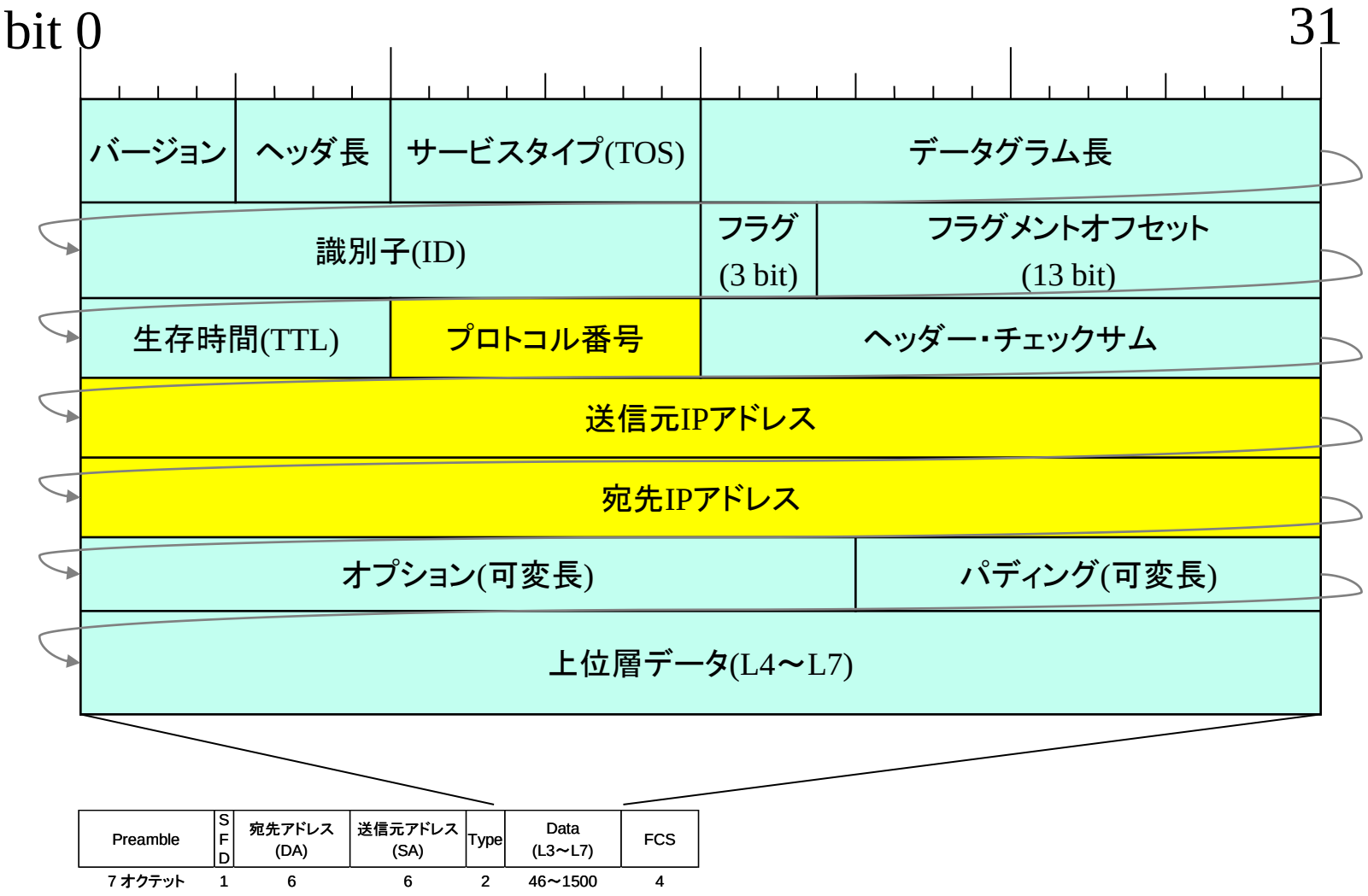


参考：Ethernet v2 フレーム形式

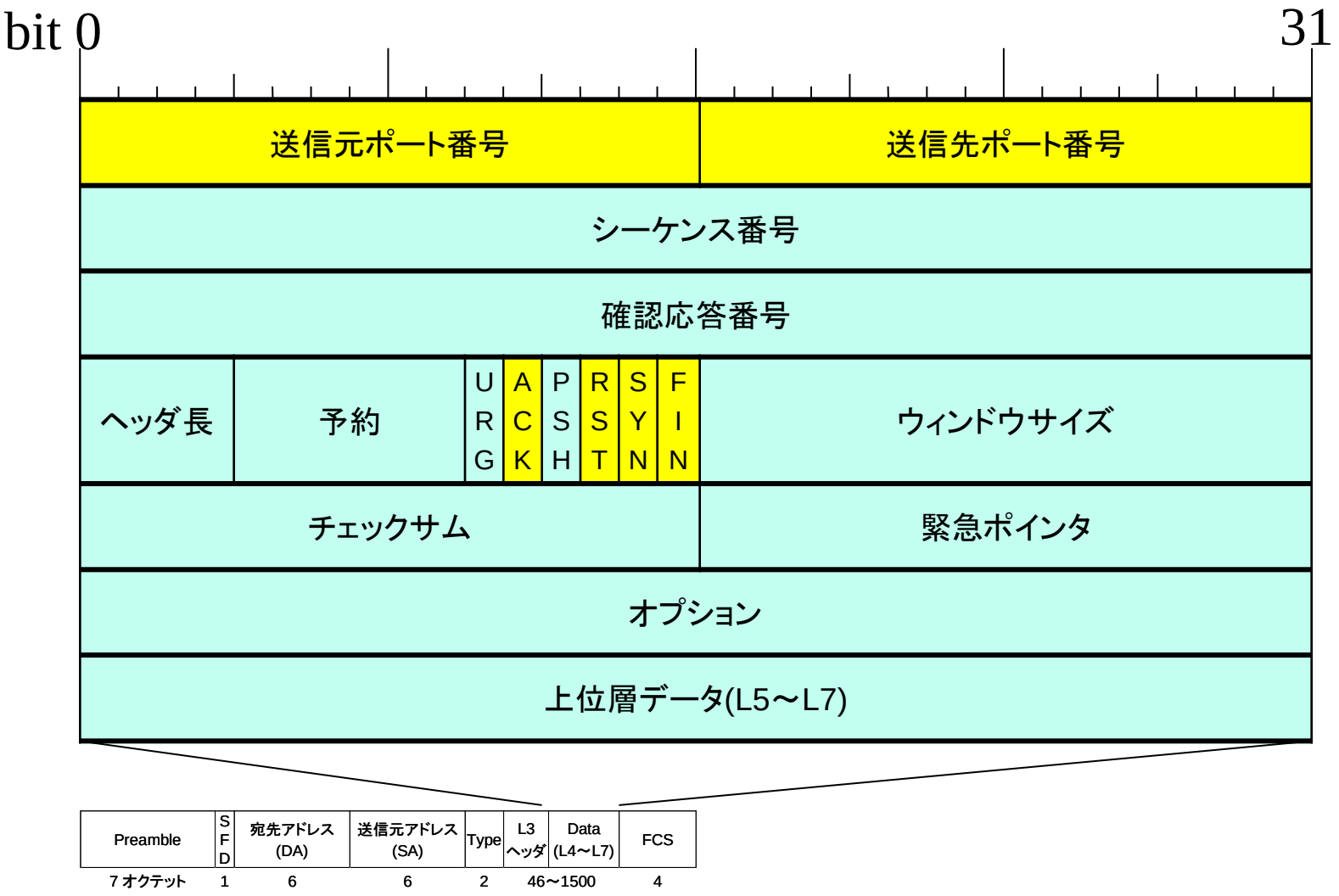
Preamble	SFD	宛先アドレス (DA)	送信元アドレス (SA)	Type	Data (L3～L7)	FCS
7 オクテット	1	6	6	2	46～1500	4

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。

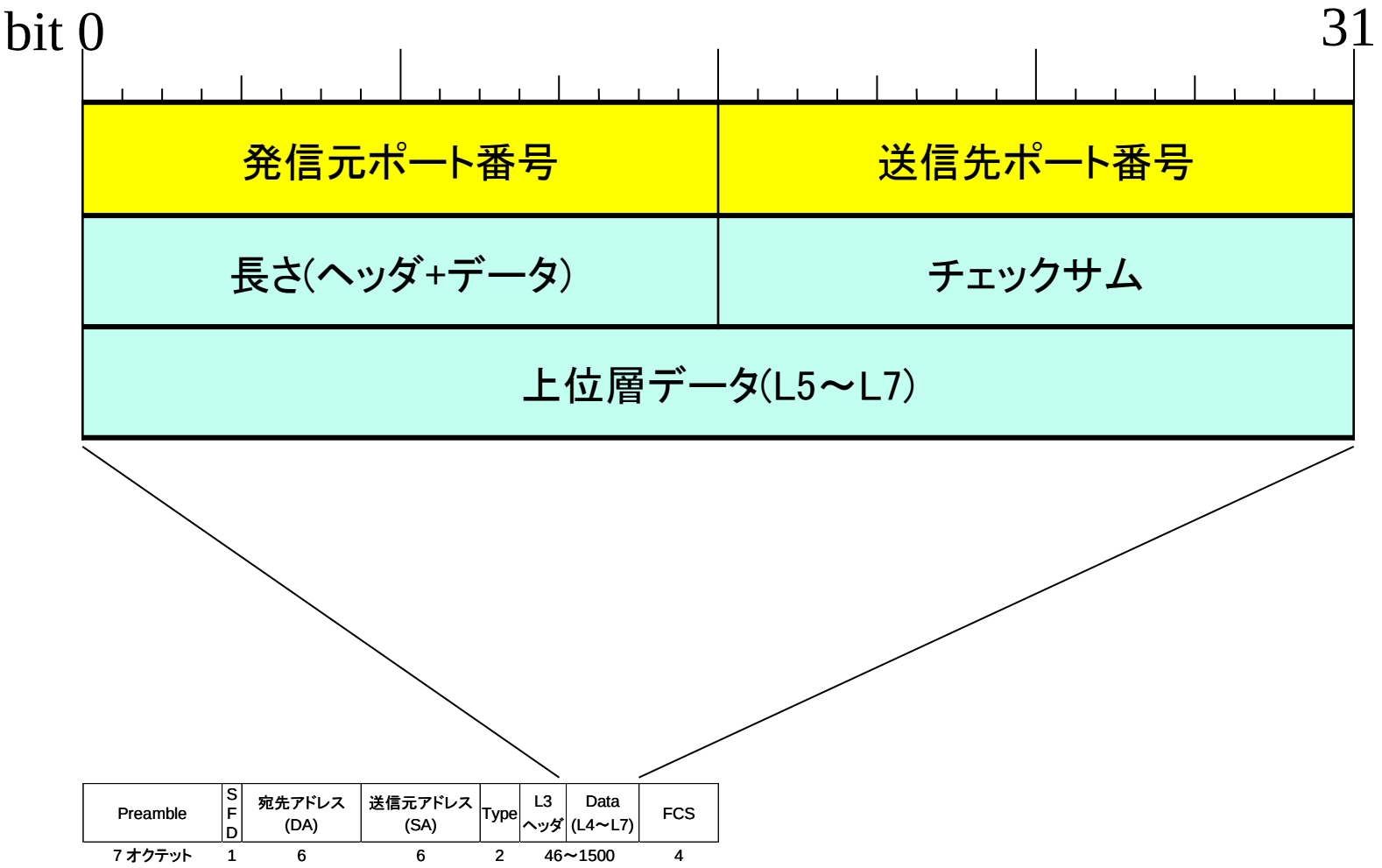
参考：IPパケット形式


bit 0
31
バージョン
ヘッダ長
サービスタイプ(TOS)
データグラム長
識別子(ID)
フラグ
(3 bit)
フラグメントオフセット
(13 bit)
生存時間(TTL)
プロトコル番号
ヘッダー・チェックサム
送信元IPアドレス
宛先IPアドレス
オプション(可変長)
パディング(可変長)
上位層データ(L4～L7)
Preamble
SFD
宛先アドレス (DA)
送信元アドレス (SA)
Type
Data (L3～L7)
FCS
7 オクテット
1
6
6
2
46～1500
4

参考：TCPヘッダー形式



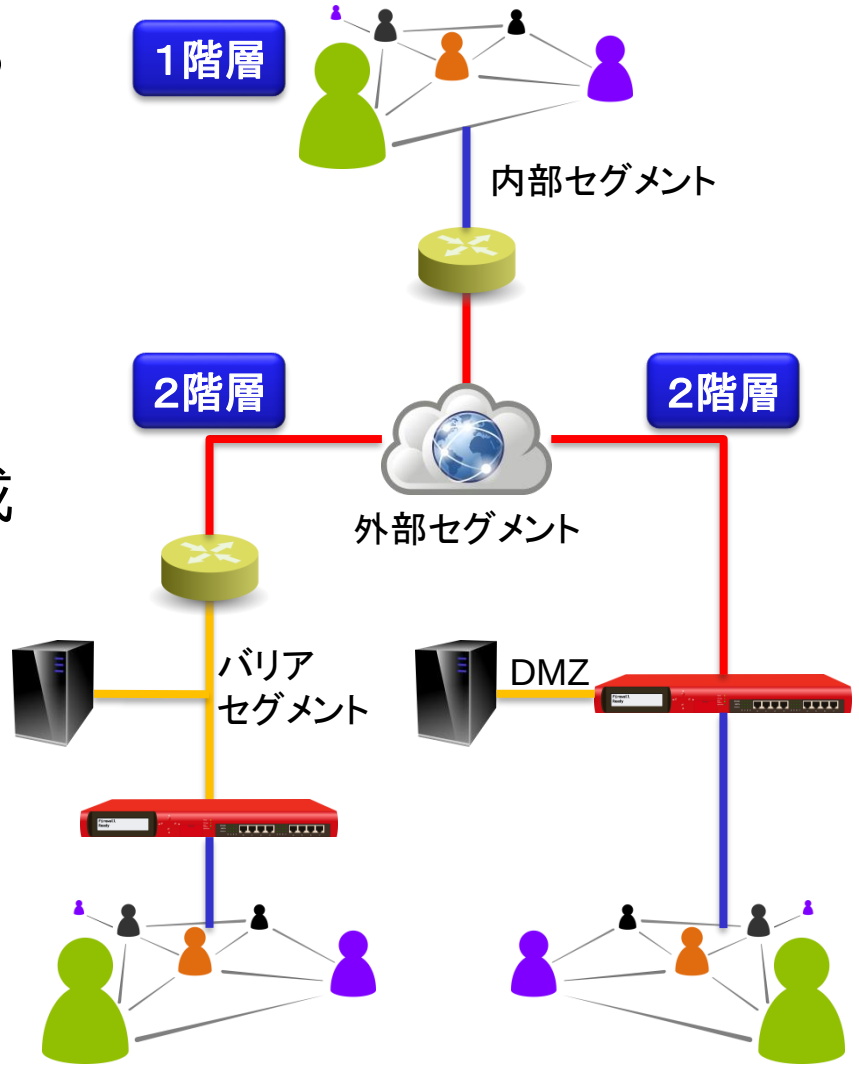
参考：UDPヘッダー形式



ファイアウォールの構成

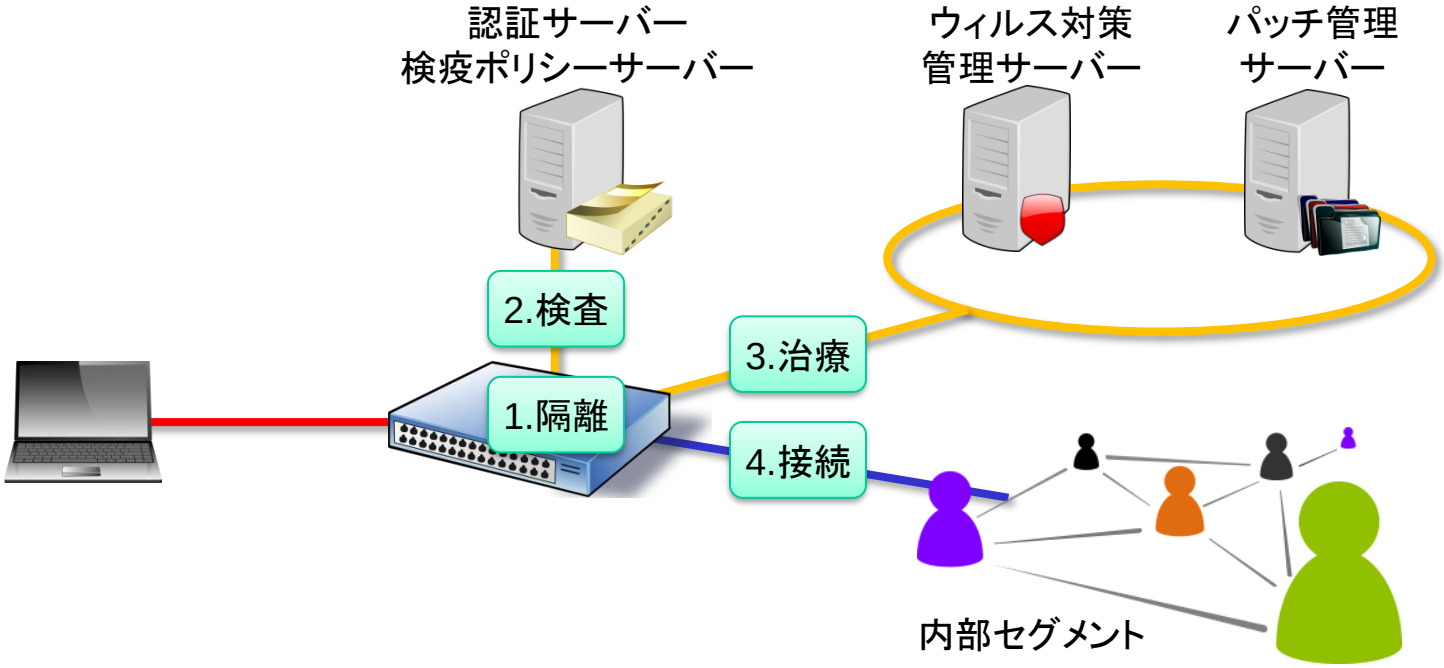
求められる信頼レベルにより構成を変える

- 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



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：ウィ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



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

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

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

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

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

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こっている
    - {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。

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. つながる世界を拡げていくためには、「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ってくる

IPA「ＩｏＴ開発における セキュリティ設計の手引き」より

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

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

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

（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

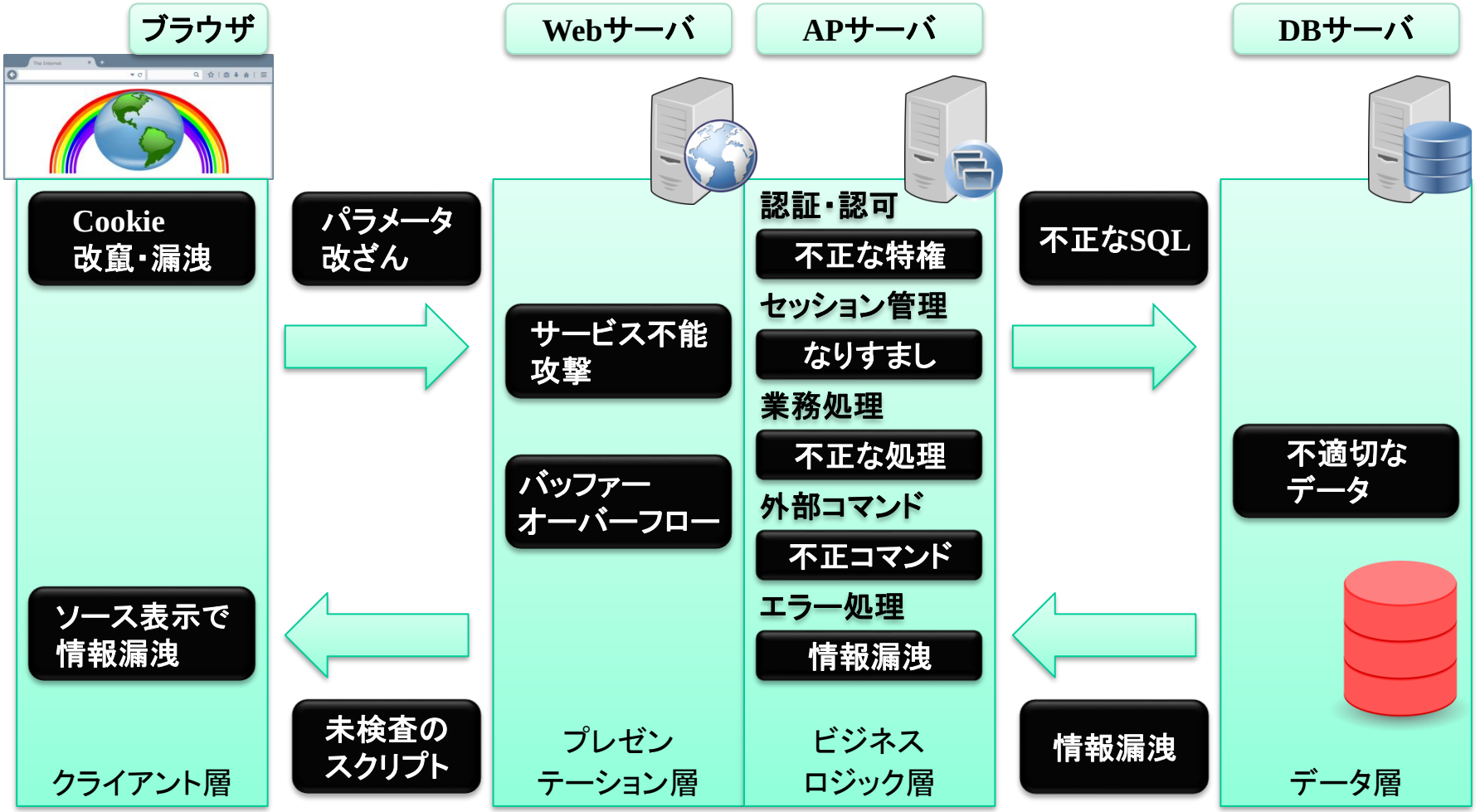
安全なコーディング実装 (SEI CERT Top 10 Secure Coding Practices、2011)

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！

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



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

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

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

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

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

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

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
- パ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

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

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

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

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

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

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

（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

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！

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。

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。

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。

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

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

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

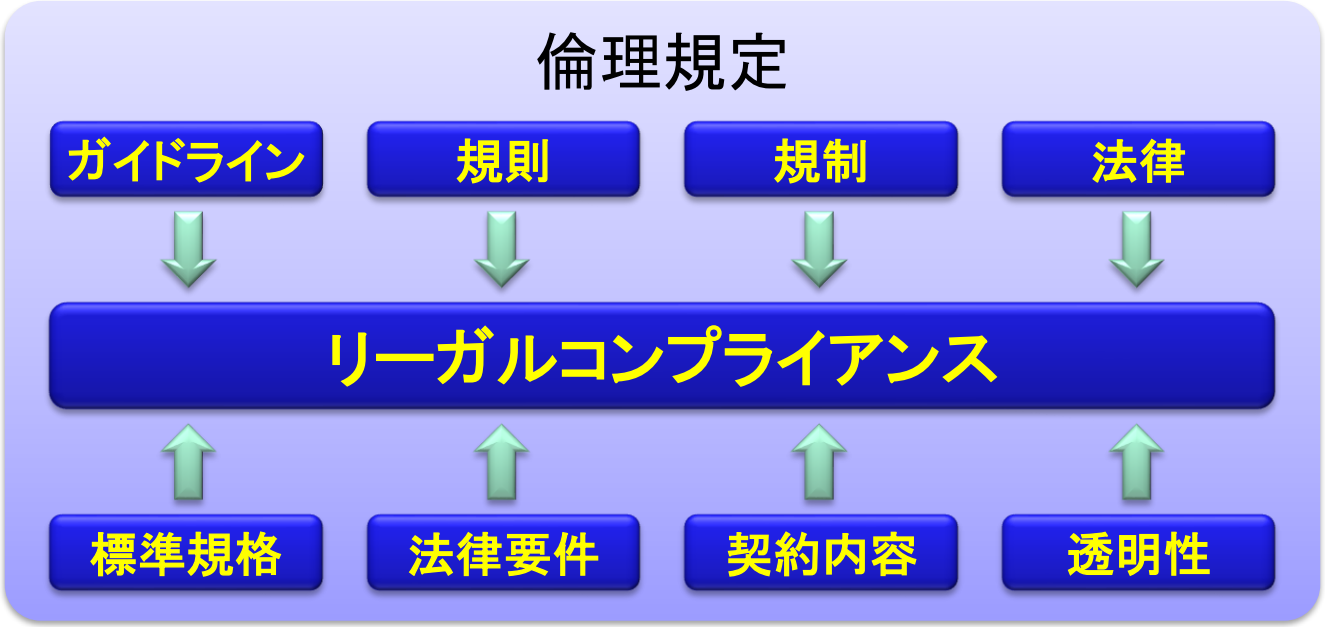
⑤ 特定電子メールの送信の適正化等に関する法律

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



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

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

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

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

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。

コンピュータウィルスに関する罪

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。

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。

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

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

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

不正アクセス禁止法

（定義）
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作動させ、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作動させ、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ができる情報又は指令を入力して当該特定電子計算機を作動させ、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

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

（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～

① 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こと
  - 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

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

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。

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。

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。

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。

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。

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

株式会社ウチダ人材開発センタ
UCHIDA HUMAN DEVELOPMENT CO.,Ltd.

セキュリティ講座

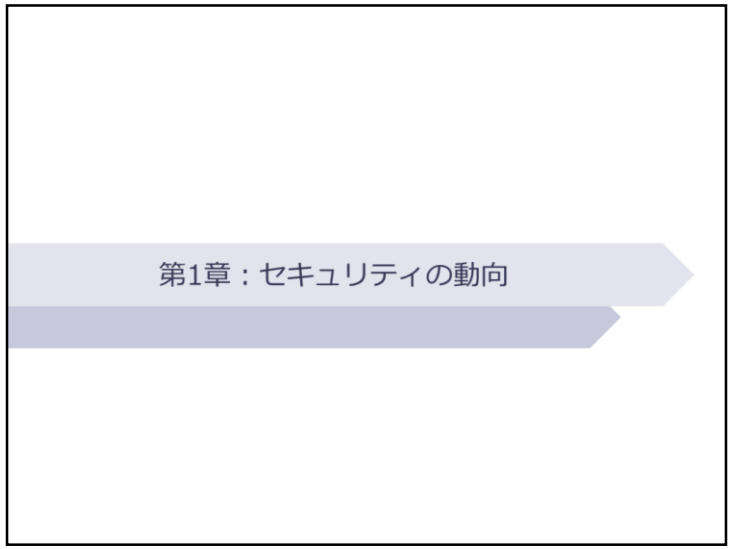
株式会社サンプル

e-learningの目的

- e-learningの目的
  - 講義・演習を始める前に、セキュリティ分野の概念や用語を学ぶことで、この後の学びを円滑かつ効果的に進めることを目的としています。このe-learningを通じ、セキュリティ分野の全体像を把握していきましょう。

- 講義・演習を始める前の基礎知識
  - 情報セキュリティの概要
  - 規格について
  - インシデントレスポンスとは
  - セキュア設計・開発について
  - 倫理・コンプライアンスについて

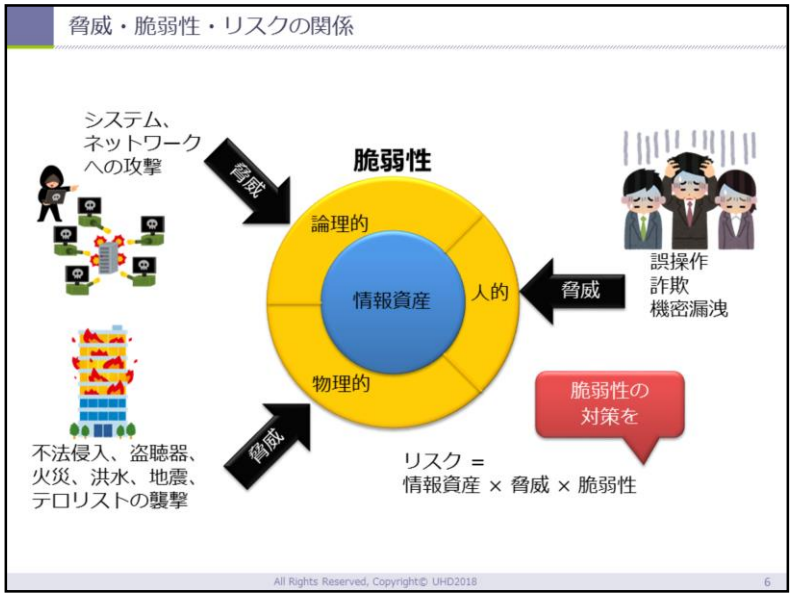
目次


第1章：セキュリティの動向

セキュリティを考えていくうえで、情報資産とはなにかを考えましょう。何が狙われ、何を守るべきかを理解していなければ、セキュリティを考えていくことはできません。本講座で扱う情報資産とは、データや情報など目に見えないものです。業務の過程でつくられたり、入手した様々なデータや情報は会社にとって価値のあるものです。自分の携わる業務において、情報資産とはなにかを想像してみましょう。それは１つや２つではないはずです。それらを並べただけでは適切な対策をとれません。守るべきモノをリスト化し、目録を作成することが重要となってきます。

情報資産の種類は、データや情報に限定されません。データや情報を扱うハード

ウェアや、データや情報を扱うためのソフトウェア、さらには組織のイメージやサービス、それを築いている信頼と信用なども含まれています。こういった守るべきモノを把握し、何から、どのように、誰が守るのかをまとめたものを「資産目録」といいます。



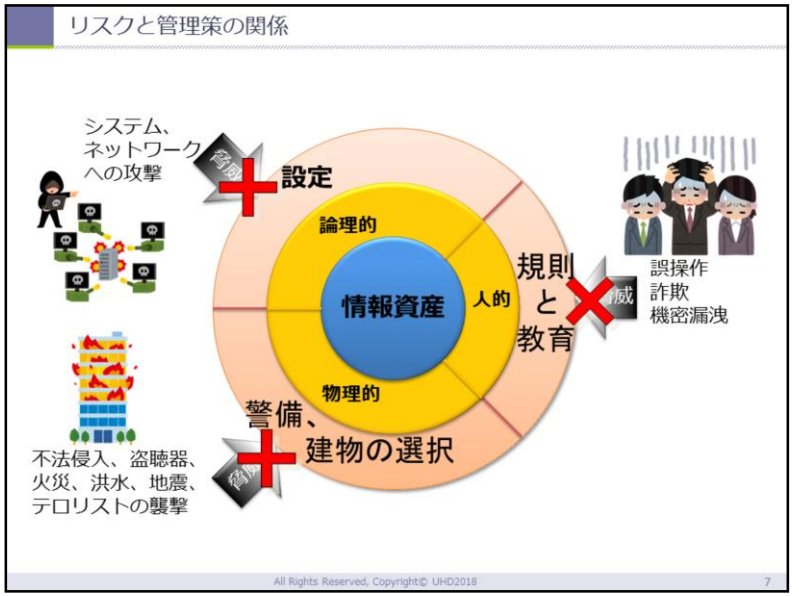
脅威、脆弱性、リスクといった用語は、セキュリティを学ぶうえで多用されますが、それぞれの定義の違いを整理しておく必要があります。

[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。家で例える場合、浸水や火事、泥棒などが脅威にあたります。

[脆弱性] 1つ以上の脅威によってつけ込まれる可能性がある資産又は管理策の弱点。家で例える場合、鍵の付いていない窓や、使用期限の切れている消火器、倒れやすいタンスなどが脆弱性にあたります。

[リスク] 目的に対する不確かさの影響。家で例える場合、上記の脅威や脆弱性によって受けるかもしれない損害の可能性です。分かりにくいと思いますが、例えば今自分が携わっているプロジェクトがあると想定します。どんなプロジェクトでも達成目的があるはずです。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存在するはずです。その不確定な要素を洗い出し、それらが目的達成にどれくらい負の影響を与えるかがリスクです。リスクは脅威レベルや脆弱性レベルと情報資産の重要度から数値化することができます。

[管理策] リスクを修正する対策。家で例える場合、鍵や防犯装置の設置などがリスクに対する管理策になります。



情報セキュリティに対するリスクとその管理策は、脆弱性の性質によって論理的、物理的、人的要素に分けて考えられます。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みます。

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。重要な施設であれば、そもそも場所を公開することが不適切な場合もあります。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分かってしまっては困ります。例えば、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。

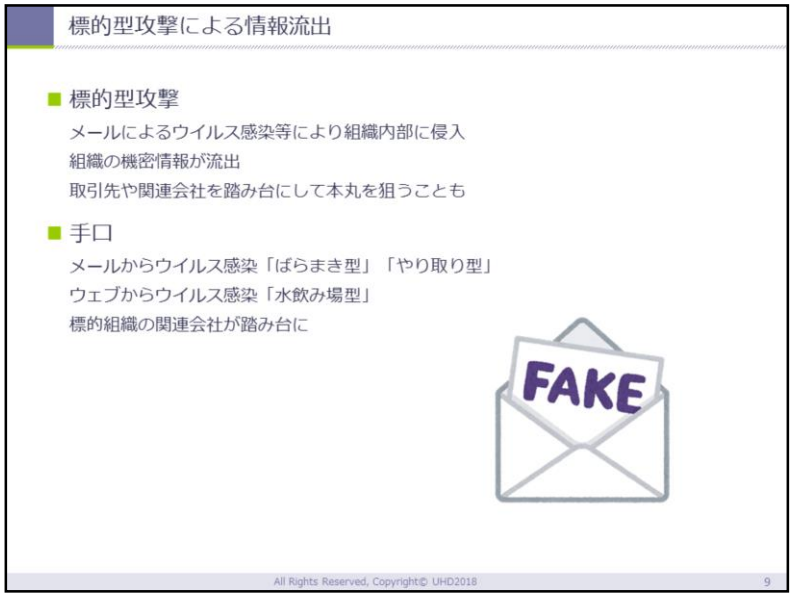
人的な脆弱性に対しては、規則と教育で対応します。これには日々の意識づけが大切です。人的な脅威が発生した場合、論理的な対策である程度は防げますが、多くの場合は利用者個々人の日頃からの注意(Due Care)で防ぐことができます。

情報セキュリティ脅威

情報セキュリティ10大脅威　2017

「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**
スマートフォンやスマートフォンアプリを 狙った攻撃	3	ウェブサービスからの個人情報の窃取
ウェブサービスへの不正ログイン	4	サービス妨害攻撃によるサービスの停止
ワンクリック請求等の不当請求	5	内部不正による情報漏えいとそれに伴う業務停止
ウェブサービスからの個人情報の窃取	6	ウェブサイトの改ざん
ネット上の誹謗・中傷	7	ウェブサービスへの不正ログイン
情報モラル欠如に伴う犯罪の低年齢化	8	**IoT機器の脆弱性の顕在化**
インターネット上のサービスを悪用した攻撃	9	攻撃のビジネス化（アンダーグラウンドサービス）
IoT機器の不適切な管理	10	インターネットバンキングや クレジットカード情報の不正利用

10大脅威は、個人向けと組織向けに分けられていますが、他にも様々な脅威があります。ランサムウェアの被害は2016年頃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。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が必要です。次ページから、近年特に目立ってきた３つの脅威について説明していきます。



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侵害が拡大

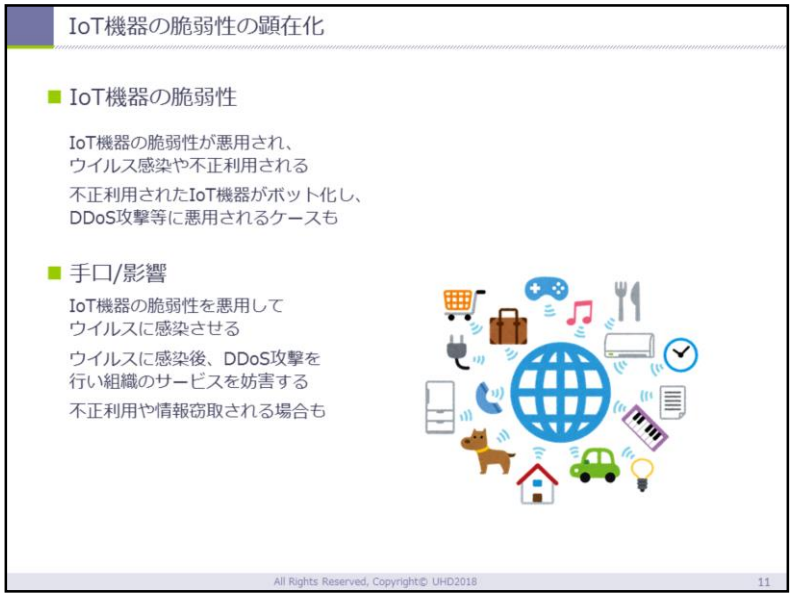
■富山大学への標的型攻撃により研究成果等が外部流出の可能性

·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がありました。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など、日頃からメールのやり取りに注意を払うなどといったセキュリティ教育が必要となります。

ランサムウェアに感染し、やむを得ず金品を支払ってしまったケースも多々あります。これは、データの損失による被害と要求された金品を天秤にかけた結果です。Trustwave社のレポートによると、攻撃者からみたランサムウェアのROI（投資に対する利益率）は1,425%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。



IoT機器は、利便性のために初期設定が脆弱な傾向があります。利用者はまずは説明を読み、不要な機能を無効化する必要があります。「何となく」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しょう。

第2章：関連制度と規格の動向

工業製品などの国際的な共通サイズや共通規格の標準が標準団体によって定められているように、ITの世界でも様々な国際標準化団体があり、規格や仕様の標準化が行われています。セキュリティを学ぶうえでも、関連する標準化団体とその規格を知っておく必要があります。以下がその代表的な団体です。

[ISO] 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] 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。

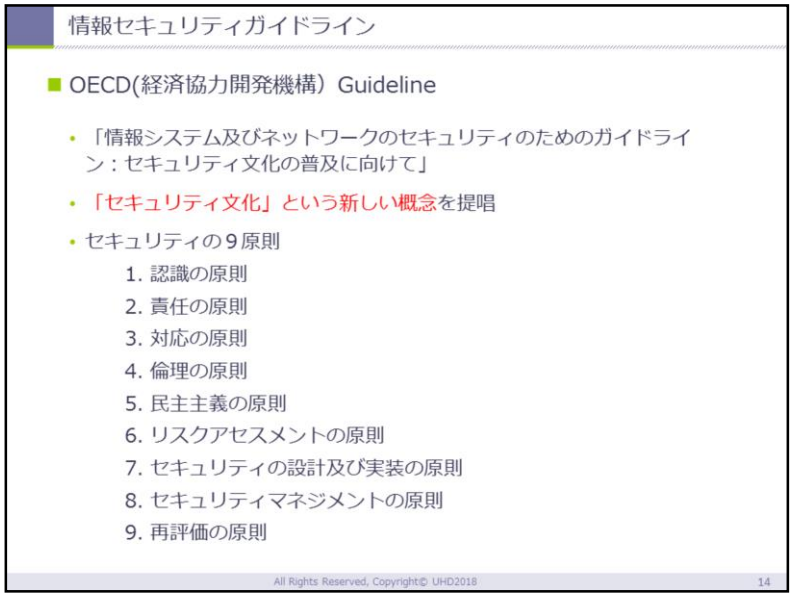
[ITU] 世界最古の国際機関。無線通信と電気通信分野において各国間の標準化と

規制の確立を図る。国連の専門機関の一つ。

[IEEE] 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] 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。



情報セキュリティに対する国際的なニーズを受けて、1992年にOECDは「 Guidelines for the Security of Information Systems（情報システムのセキュリティに関するガイドライン）」を策定しました。セキュリティ文化という新しい概念を提唱し、セキュリティの9原則を制定しています。

1. 認識の原則（Awareness）:参加者は、情報システム及びネットワークのセキュリティの必要性並びにセキュリティを強化するために自分達にできることについて認識すべきである。

2. 責任の原則（Responsibility）:すべての参加者は、情報システム及びネットワークのセキュ リティに責任を負う。

3. 対応の原則（Response）:参加者は、セキュリティの事件に対する予防、検出及び対応のために、時宜を得たかつ協力的な方法で行動すべきである。

4. 倫理の原則（Ethics）:参加者は、他者の正当な利益を尊重するべきである。

5. 民主主義の原則（Democracy）:情報システム及びネットワークのセキュリティは、民主主義社会の本質的な価値に適合すべきである。

6. リスクアセスメントの原則（Risk assessment）:参加者は、リスクアセスメントを行うべきである。

7. セキュリティの設計及び実装の原則（Security design and implementation）：参加者は、情報システム及びネットワークの本質的な要素としてセキュリティを組み込むべきである。

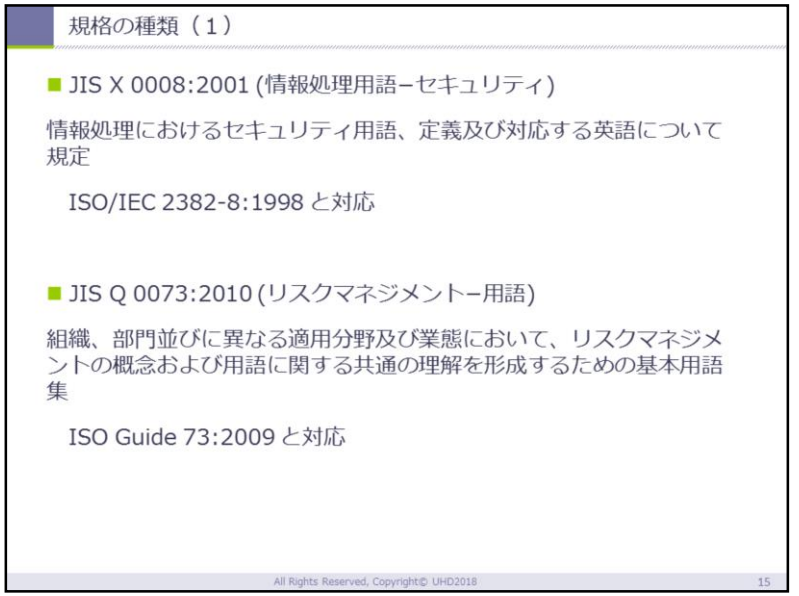
8. セキュリティマネジメントの原則（Security management）：参加者は、セキュリティマネジメントへの包括的アプローチを採用するべきである。

9. 再評価の原則（Reassessment）：参加者は、情報システム及びネットワークのセキュリティのレビュー及び再評価を行い、セキュリティの方針、実践、手段及び手続に適切な修正をすべきである。

（経済産業省 商務情報政策局 情報セキュリティ政策室 情報処理振興事業協会 セキュリティセンター）

また、似たようなガイドラインにプライバシーの８原則があります。

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



JIS X は情報処理に関する規格です。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１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、脅威と脆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ます。

JIS Q は管理システムに関する規格です。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。

ISMSファミリの規格について、すべてを覚える必要はありませんが、必要な時に参照できるようにしておきましょう。また、ISMSファミリ規格は、それぞれに対応するJIS規格があります。いくつか重要な規格をみていきましょう。

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

＊用語が曖昧な場合にその定義を知るために参照します。

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

＊ISMSの仕様や、要求事項が定義されています。

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。

＊ISMSの実施基準、行動規範が定義されています。

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

＊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。

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 製品に適応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

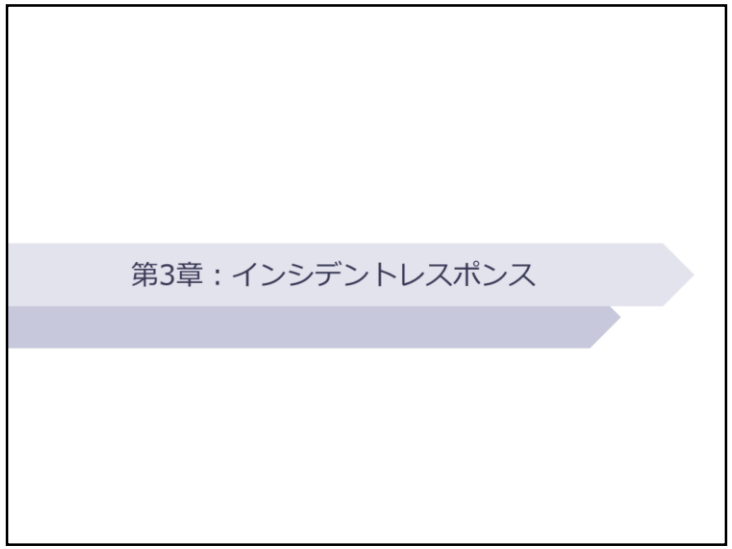
＊情報技術に関連した製品及びシステムが適切に設計され、その設計が正しく実装されていることを評価するための国際

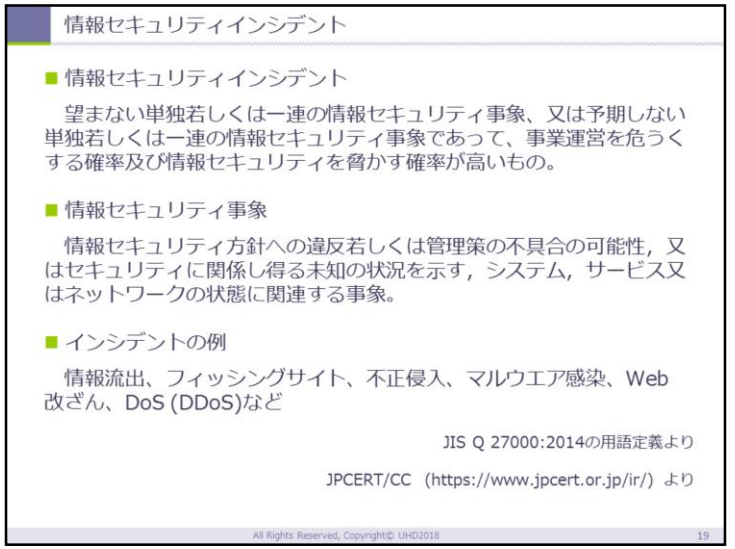
標準規格です。

IEEE802.11は、IEEEによって策定された無線LANの規格です。1997年にMACと周波数ホッピング及び直接シーケンスの変調方法が定義されたことから始まっています。ほとんどの規格において無線免許が必要がない、無線LANの標準規格です。通信方法やハードウェアの進化やセキュリティ対策の進歩によって、IEEE802.11の規格も追加されています。

2004年6月に策定されたIEEE802.11iは、無線LANにおけるセキュリティの標準規格です。この規格の基本は、「暗号化通信」と「ユーザ認証」にあります。それまでのWEPによる暗号化よりも強力な暗号化技術と、WEPではできなかったユーザ認証を802.1Xを組み合わせることで、従来の規格では企業などでの使用で不十分と言われていたセキュリティレベルを格段に引き上げ

ました。


第3章：インシデントレスポンス



事業運営に影響を与えたり、情報資産を侵害するような事故や事件を統合して情報セキュリティインシデントと呼びます。ISO27001の規格では、情報セキュリティインシデントのほかに、情報セキュリティに関連するかもしれない未然の状況も、情報セキュリティの事象として扱い、適切な処理を義務づけています。

情報セキュリティインシデントの例

・ウィルス感染

・不正アクセスや攻撃

・情報媒体（CDやフラッシュメモリなどの）の紛失や盗難

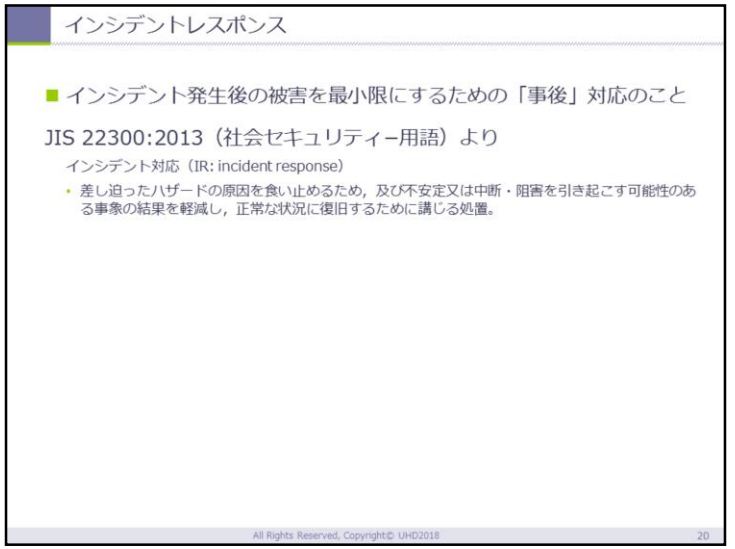
・PCやルータなどの物理機器の盗難や破壊工作

情報セキュリティ事象の例

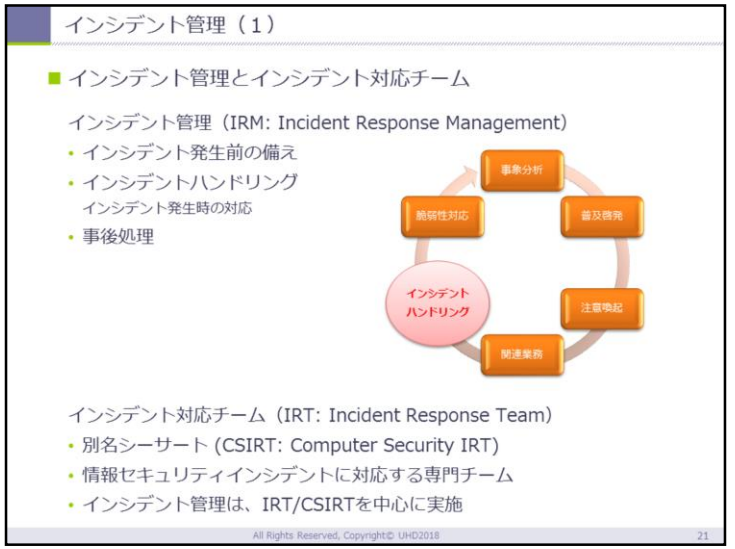
・情報セキュリティシステムの脆弱性の発見

・端末の誤操作（メールの誤送信なども含む）

・ユーザーのセキュリティポリシー違反



情報セキュリティインシデントによって引き起こされる被害や不具合を未然に防ぎ、万が一、情報セキュリティインシデントが発生した場合も、その被害を最小限にするめの対応をインシデントレスポンスと呼びます。狭義には、情報セキュリティインシデントの発生後の対応を指しますが、事前の準備、発生時の対応、事後処理の３ステージをまとめてインシデントレスポンスとして扱います。



インシデント管理（IRM)を適切に実施するためには、インシデント発生に備えて、その防止、予防、対策、処理、報告、記録などを行うインシデント対応チームが必要です。インシデント対応チームは、以下のようにまとめられます。

[基礎準備]

・リスクの特定

・インシデント対応ポリシー（IRP: Incident Response Policy）の作成

[論理的・人的準備]

・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）

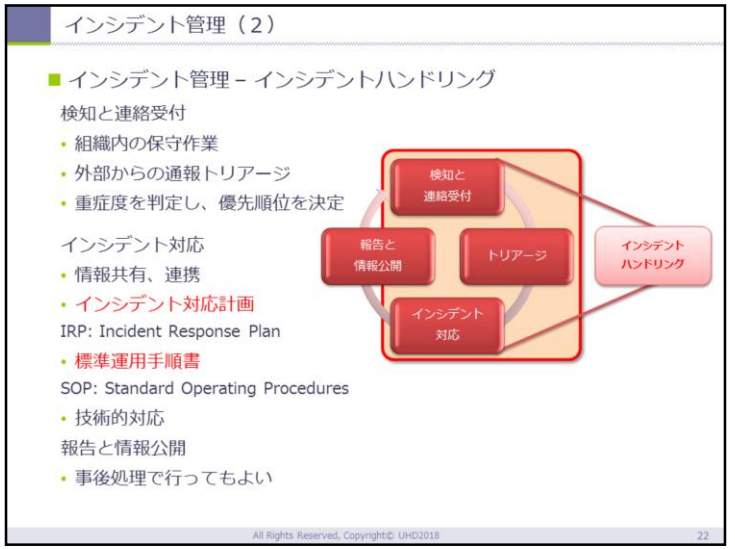
[インフラ準備]

・コンピュータ機器構成（資産管理）

・ネットワーク構成

平常時には、情報収集と分析を行い、組織全体への注意喚起や啓蒙活動などのインシデントの防止、予防活動と、ハードウェアの脆弱性の検査やパッチの適用、ファイアウォールの導入、侵入検知システムの監視と

インシデント発生時の対応訓練などを行います。



インシデントハンドリングとは、情報セキュリティインシデントが発生が検知され、発生報告がされた時の対応を指します。

組織内外から「異常」が報告されたら、事前に設定された判断基準に基づきチェックを行い、情報セキュリティインシデントの検出を行い、関係者の間で事象共有を行い、IRTに情報を集約します。まず、最初にトリアージを行います。トリアージとは、発生した重症度を判定し、優先順位を決定する作業です。トリアージの判定基準は一定ではありません。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基づき判断します。判定は3W1H、いつ(when)、どこで(where)、何が(what)、どう(how)発生したかを用いて行います。また、トリアージの結果、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、通報者の勘違いなどといったように、インシデント対応を行わない場合もあります。

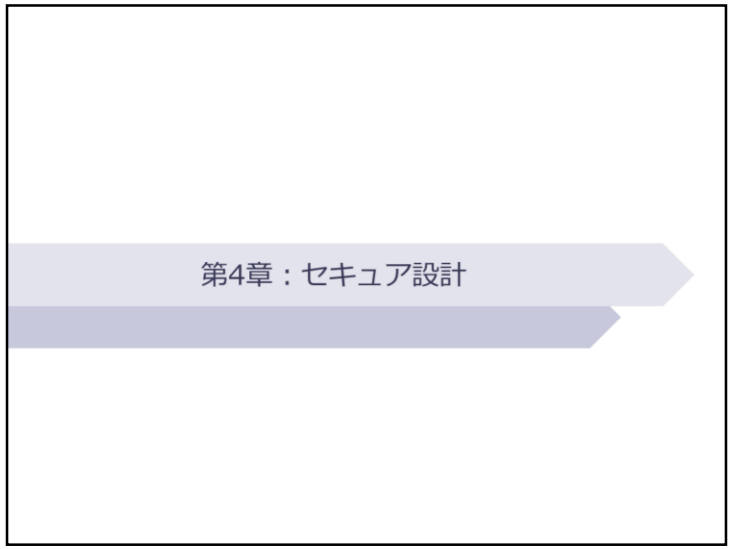
トリアージ後に、IRTが対応すべきと判断された場合は、インシデントレスポンスのフェーズに移行します。発生した情報セキュリティインシデントの事象分析を行い、技術的に対応が可能か否かを判定し、IRT内で技術的に対応可能な場合には、組織のIT関連部署と連携し、インシデント対応計画を策定し、実施します。また、発生した情報セキュリティインシデントが、IRTでは技術的に対応が困難な場合は、組織の幹部や経営陣と連携して対応計画を練る必要があります。そこで策定されたインシデント対応計画に従い、インシデント対応ポリシーに基づいた技術的な対応手順、手法、チェックリスト、フォームなどで構成された標準運用手順書を作成し、インシデントに対応します。

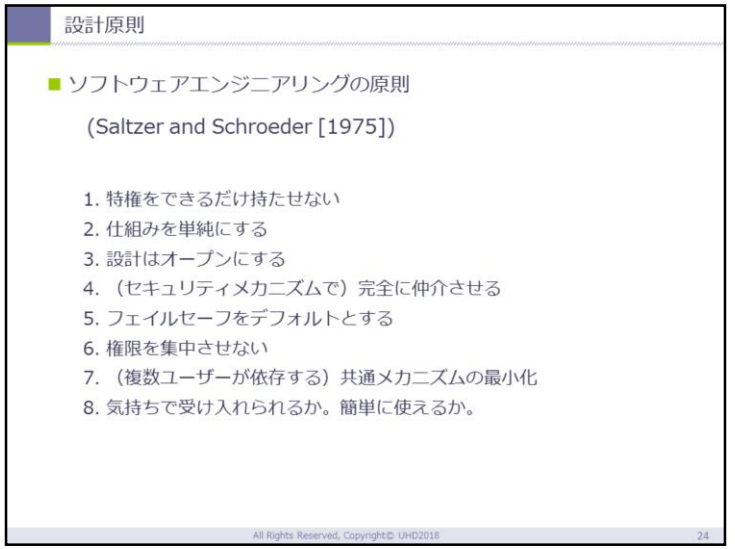
インシデント収束後には、再発防止を目的とした事後処理を行います。インシデントの原因究明を行い、情報収集し、脆弱性の対応をとります。また、事後レポートを作成し、情報公開を行います。レポート作成には、

・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

といった内容が必要です。


第4章：セキュア設計



安全なシステム構築のためには、サイバー攻撃に備えた設計が必要です。すでに1975年には、ソフトウェアエンジニアリングの原則として8項目が挙げられています。8項目の原則は、現在でも通用する原則です。

1. 特権をできるだけ持たせない。

ユーザやプログラムに、できるだけ権限を持たせないようにすることで、アクシデントやエラー、攻撃者によるダメージが最小限に抑える。

2. 仕組みを単純に。

防御システムは小さく単純明快に設計する。

3. オープンな設計。

防御する仕組みは、公開された仕組みで、パスワードや秘密鍵のように比較的少ない項目 (そして簡単に変えられる)で秘密を守れるようにする。

4. 完全に仲介を行う。

チェックする仕組みは、壊されない場所に置き、すべてのアクセスをチェックする。

5. フェイル・セーフをデフォルトとする

デフォルトではサービスを拒否する。防御機構はどのアクセスを許可 しているのか、状況を認識する。

6. 権限を集中させない。

対象へのアクセスに当たって、もしある防御システムが破られても、無制限なアクセスを許すようにさせないために、複数の条件をつける。

7. 共通した仕組みはできるだけ用いない。

共通する仕組みの数とその利用度合を最小限にする。

8. 気持ちで受け入れられるか、簡単に使えるか。

ヒューマン・インタフェースは、ユーザが日常何気なく正しい防御の仕組みを使え るように、使いやすく設計する。

セキュアシステム設計は、システムのライフサイクルすべてに関わるもので、開発のはじめから組み込んで設計を行います。また、セキュリティ品質を確保するために、次の３つの活

動に留意して開発を行います。

●セキュリティレビュー

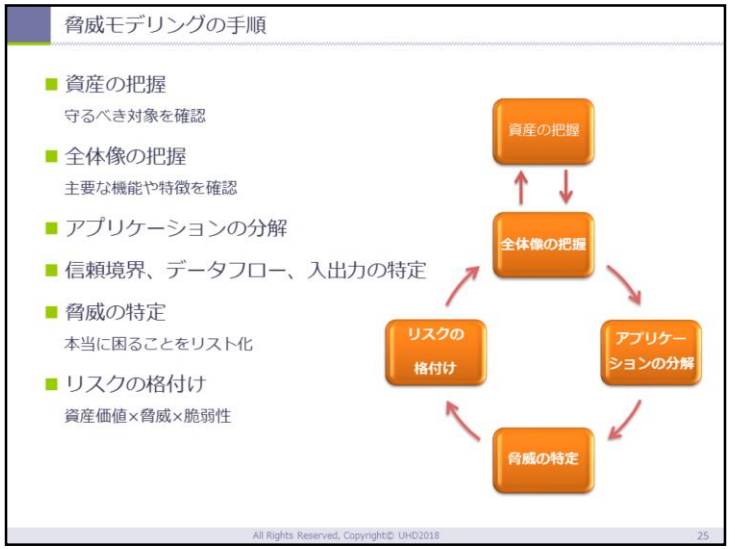
セキュリティレビューは、セキュリティ対策漏れを早くに見つけ出し、設計者へフィードバックすることを目的に行います。

●ソースコードレビュー

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。

●セキュリティテスト

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。



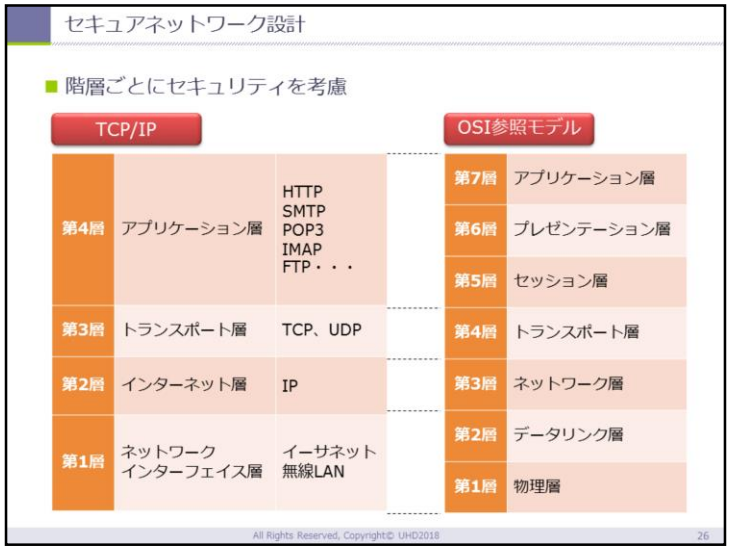
脅威モデリングは、情報資産、脅威、脆弱性を特定し、リスクを洗い出す作業をアプリケーションに対して行う作業です。設計段階で脅威モデリングを行うことで、実装段階に入ってからの手戻りを最小限にとどめることができます。これはセキュリティの向上だけではなく、コスト削減や開発期間の短縮にもつながる作業となります。1999年にマイクロソフトが提唱した STRIDE & DREAD 脅威モデリングは、OWASPおよびIPAでも採用されている脅威モデリングです。その効果は実地で検証されています。

～STRIDE & DREAD 脅威モデリング～

●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)



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。ここでは、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。

TCP/IPの階層ごとにみていきます。

[ネットワークインターフェイス層]

ネットワークインターフェイス層においては、通信経路のセキュリティとMACアドレスセキュリティを考慮します。通信経路は、有線でのケーブリン

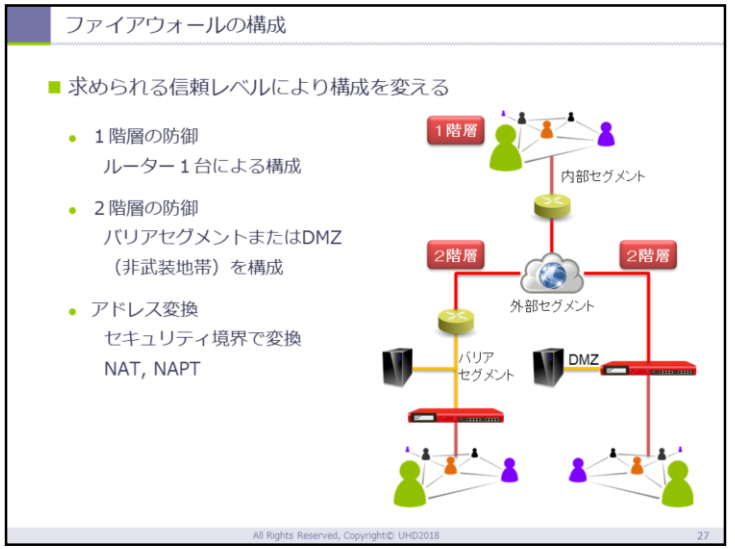
グと無線での電波の双方での接続セキュリティを考慮する必要があります。ケーブリングでは、セキュリティ対策の目的で光ファイバを用いることがあります。通信の傍受が困難で、かつ、傍受の検知が容易であるということから、短距離でも組織内の基幹通信で光ファイバーを用いるケースがあります。また、一般にルーターは、第3層の装置として認識されていますが、ルーティング時にMACアドレスを変換する働きがあります。ですから、ルーターにキャッシュされているMACアドレスがARPスプーフィングで汚染されている場合、ルーティング先が意図しないホストになる場合があります。その他、暗号化などの技術も通信経路のセキュリティとして考慮していかなければなりません。MACアドレスセキュリティにおいては、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アドレス操作といったようなセキュリティ対策がとられています。

[インターネット層・トランスポート層]

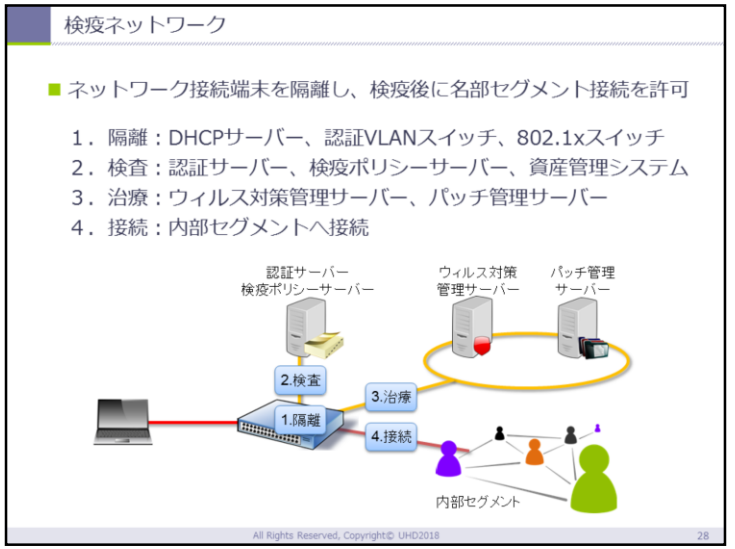
インターネット層・トランスポート層での主なセキュリティ対策としてパケット・フィルタリングが知られています。パケットフィルタリングには、静的パケット・フィルタリング、動的パケット・フィルタリング、ステートフル・インスペクションなどがあります。静的パケット・フィルタリングは、ルーター上のファイアウォールとして一般的に搭載されています。過去に通過したパケットから通信セッションを認識して、受け付けたパケットを通信セッションの状態に照らし合わせて通過させるか、遮断させるかを判断するという、ステートフル・インスペクションは、動的パケット・フィルタリングのひとつとして考えると分かりやすいかもしれません。

[アプリケーション層]

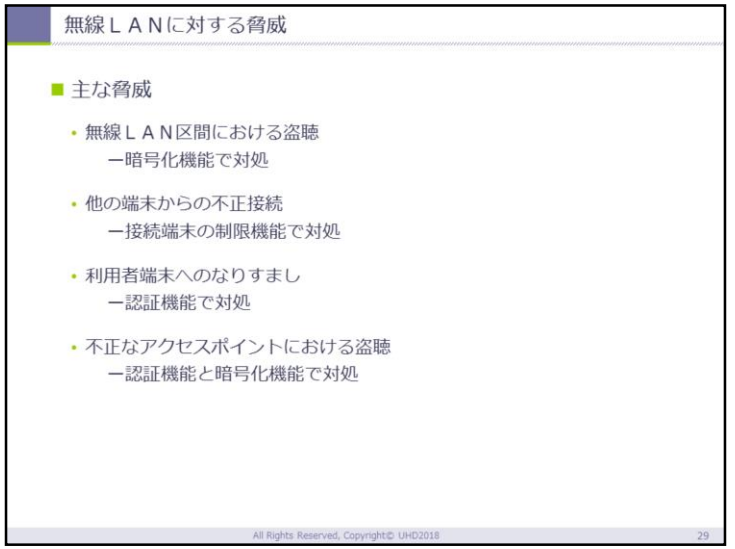
アプリケーション層では、IDS（侵入検知システム）/IPS（侵入防御システム）、アプリケーションゲートウェイ、WAF（Webアプリケーションファイアウォール）といったセキュリティ対策がとられます。IDS/IPSは、シグニチャーベースで、難読化処理された攻撃に弱い、アプリケーションゲートウェイは、アプリケーション層の情報でフィルタリング、WAFは、通信を一度解除してから解析で難読化処理にも対応といったように、それぞれの対策にメリット・デメリットがみられます。



ファイアフォールの構成を考えるうえで重要なことは、ネットワークのセキュリティ境界を意識しながら構成していくということです。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に内部限定で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で３階層にするというケースがあります。この場合、内部限定で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に対応したウィ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。



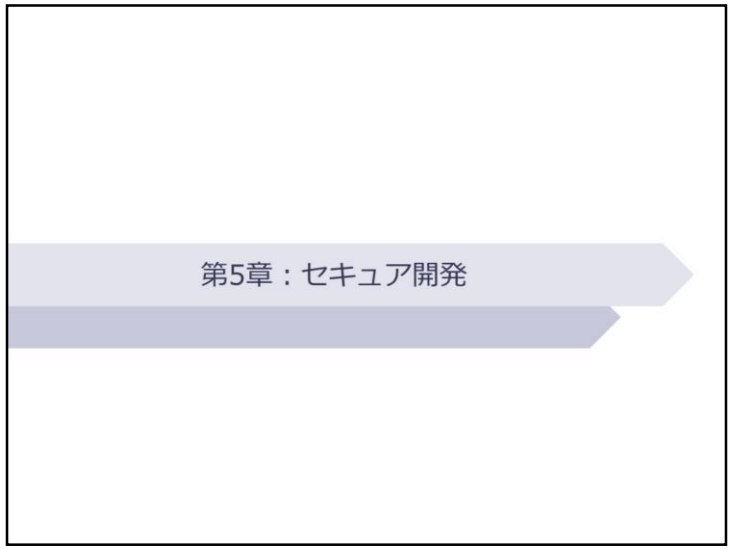
無線LANの脆弱性はよく話題に上りますが、何が脅威で、何がその脅威に対する脆弱性で、何を対策すべきかをしっかり検討していないケースが多く存在します。ほんのわずかなポイントを抑えるだけでも、無線LANは暗号化されていない有線LANよりも安全な通信方式です。まずは、傍受と盗聴は違うということを認識しましょう。例えば、警察無線を傍受しただけで捕まることはありません。傍受した内容に対し、何らかのアクション（例：通信内容の記録、通信内容の）をとった場合に電波法違反が問われることがあります。そもそも適切に通信が暗号化されており、認証が設定されていれば、盗聴には失敗します。あくまでも「盗聴を防ぐ」という観点で無線LANを考えていきましょう。

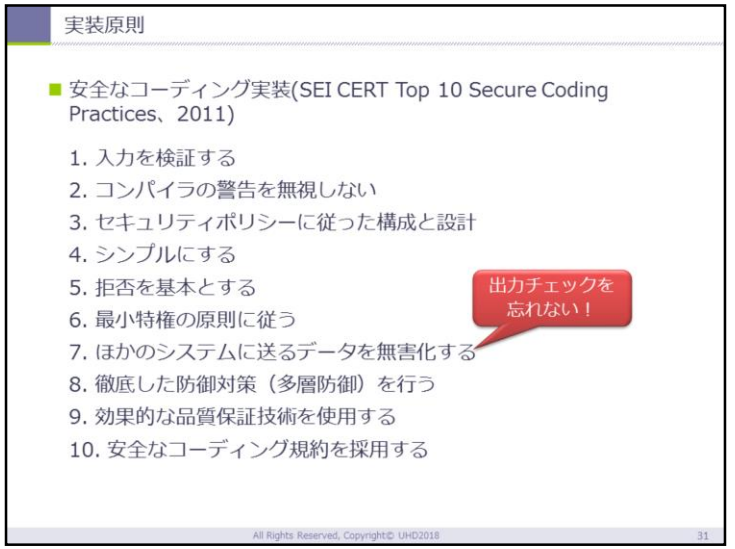
主な無線LANセキュリティ技術には、次のようなものがあります。

●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
・WEP (使用禁止。１０秒程度で解読可能)
・WPA (TKIP暗号化を使用。脆弱性の指摘あり)
・WPA2 (AES暗号の実装であるCCMP暗号化を使用)
・IEEE802.11iの実装


第5章：セキュア開発



安全なコーディングを実装するための10の原則です。

1. 入力を検証する（Validate input.）

すべての信頼されていないデータソースからの入力を検証する。適切な入力検証は、多くのソフトウェアの脆弱性を緩和することができる。コマンドライン引数、ネットワーク・インタフェース、環境変数、およびユーザが管理しているファイルなどほとんどの外部データソースは信頼できない。DBMS から取得したものも行うこと。特に Web の場合はユーザフォームからの入力だけではなく、クッキーや HTML のヘッダーブロックの値なども含めてクライアントから受け取った値を使用する場合には精査する。

2. コンパイラの警告を無視しない（Heed compiler warnings.）

コンパイラの警告に注意を払わなければならない。コンパイラはプログラムコードに対して必ず行われる最初の精査行為である。コンパイラのオプションを設定することでより多くの情報を得ることができる。

3. セキュリティポリシーに従った構成と設計（Architect and design for security policies.）

セキュリティポリシー実現のための実装と設計を行う。守るべきものを特定してそれを守るために行うものであり、すべてを同様に守るようにするものではない。極端な表現ではあるが、すべてを同様に守るということはすべてを同様に守らないということと同じ意味になる。それぞれのアプリケーションやシステムで決めたセキュリティポリシーにしたがって行う。ソフトウェアアーキテクチャを作成し、実装し、セキュリティポリシーを適用するためのソフトウェアを設計する。

4. シンプルにする（Keep it simple.）

シンプルを維持する。同じ結果を得られる実装は、ひとつとは限らず、複数の選択候補があるならば、できるだけシンプルなものを選択すべきである。シンプルにすることで最初の開発からその後のデバッグや保守といった開発作業全般でミスを犯す可能性を低くできる。逆に複雑にしても攻撃を避けられるわけではなく単にミスの発生を高め、それが結果的に脆弱性となる可能性を高めている。

5. 拒否を基本とする（Default deny.）

拒否をデフォルトにする。許可ベースではなく、拒否ベースでアクセス決定する。デフォルトではアクセスが拒否され、保護スキームはアクセスが許可される条件を識別していることを意味する。

6. 最小権限の原則に従う（Adhere to the principle of least privilege.）

どのプロセスも、実行するために必要な最低限の特権セットで実行すべきである。権限が昇格されている時間を最小限にするべきである。このアプローチによって、攻撃者が昇格した権限で任意のコード実行する機会を減らすことができる。

7. ほかのシステムに送るデータを無害化する（Sanitize data sent to other systems.）

外部に渡すデータは渡した先で問題を起こさないように加工する。渡す先によって問題となる条件は異なるのでそれに合わせた加工をする必要がある。

8. 徹底した防御対策（多層防御）を行う（Practice defense in depth.）

多層防御を行う。根本的対策だけでなく、保険的対策も含めた異なるタイプ防御策を行うようにすることである。すなわちひとつの対策がもしも不完全であったり、攻撃者に破られた

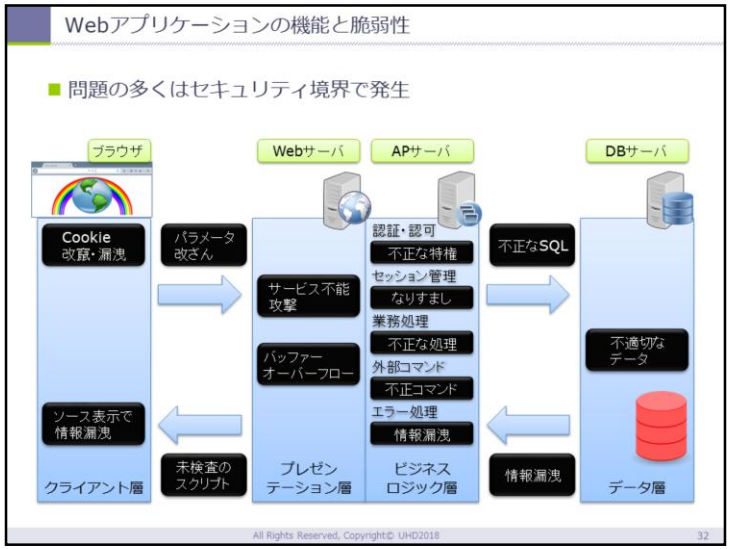
りとしても全てを失ってしまうのではなく、被害がある程度限定できるようにする。

9. 効果的な品質保証技術を使用する（Use effective quality assurance techniques.）

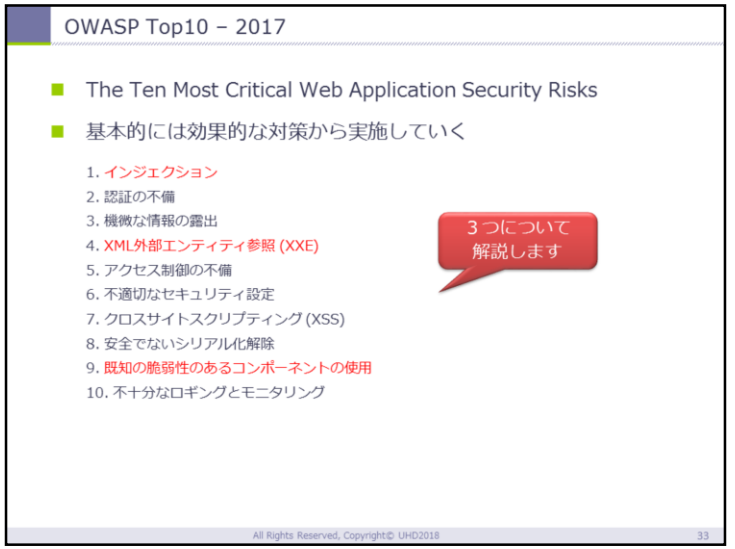
効果的な品質保証テクニックを使う。優れた品質保証技術は、脆弱性を特定し、排除するのにも有効である。

10. 安全なコーディング規約を採用する（Adopt a secure coding standard.）

セキュアコーディング標準を採用する。ターゲット開発言語やプラットフォームのためのセキュアコーディング標準を適用し開発する。



Webアプリケーションの開発においては、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アプリケーションではこの14か所で必要十分です。



OWASP（Open Web Application Security Project）とは、Webアプリケーションなどのソフトウエアのセキュリティに関する情報共有や普及啓発を目的とした世界的なオープンソースソフトウエア・コミュニティです。OWASP Top 10とは、OWASPが数年おきに発表する、Webアプリケーションの脆弱性トップ10を指摘したものです。実際のWebアプリケーションの開発においては、2017年度版に出ているトップ10のみならず、前回の2013版では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)」や「未検証のリダイレクトとフォーワード」なども注意しておくべきです。それぞれの脆弱性については、講義で触れますが、ここでは特に注意が必要な３つの脆弱性の概要について覚えていきましょう。

[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という脆弱性です。対策として、

●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する。（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する。

●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

があります。

[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という脆弱性です。対策として、

●開発者のトレーニングをする。

●SON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、そして無害化する。

●根本的な対策が難しい場合、WAFによる検出、監視、防御を検討する。

があります。

[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が、開発においての鍵になります。対策として、

●未使用の機能、コンポーネント、ファイル、文書を削除する。

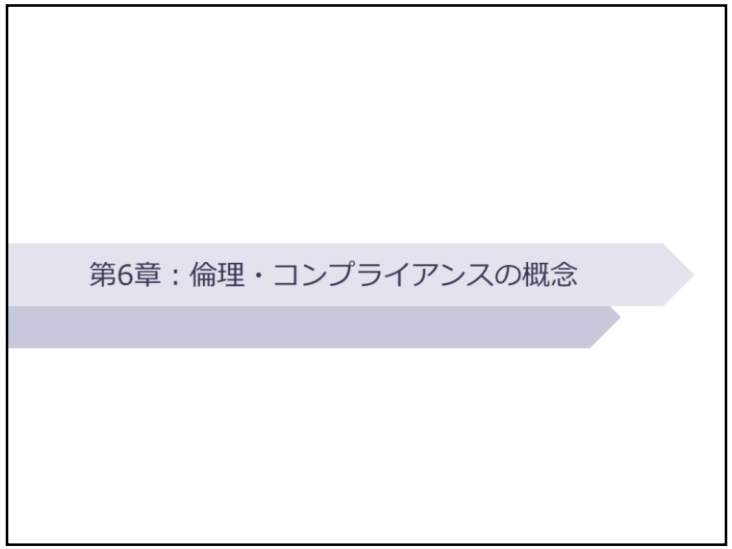
●クライアント側とサーバー側で、使用コンポーネントと関連コンポーネントのバージョンを継続的に管理する。

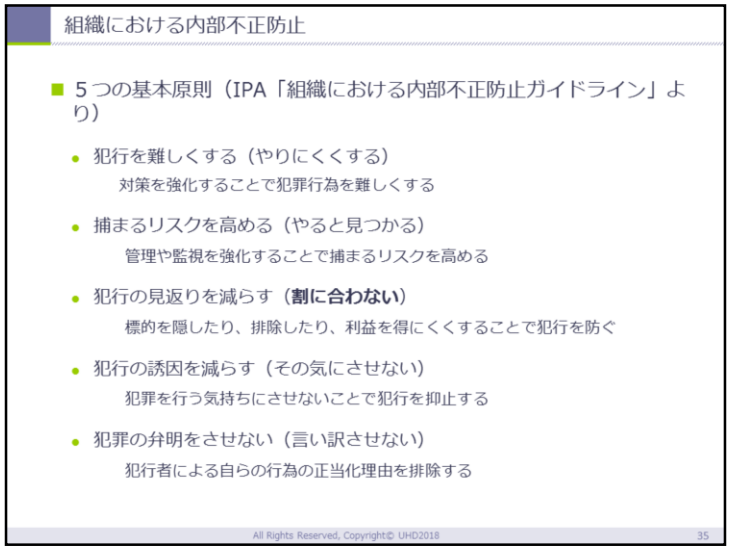
●安全な接続を介し、公式リソースからコンポーネントを入手する。

●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する。

●パッチが適用できない場合、仮想パッチを適用する。

などが、考えられます。


第6章：倫理・コンプライアンスの概念



まずは「犯行が割に合わない」ことを徹底します。犯行はハイリスクハイリターンの割の良い行動です。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1,425%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５つの原則すべてを考慮する必要が出てきます。

また、内部不正を防ぐための10の観点としては、

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

が挙げられます。すべての観点からの対策が必要であるというわけではありませんが、内部不正発生時の事後の対策（法的手続き等）を考慮すると、2. 資産管理、6. 人的管理、7. コンプライアンスは必須であるといえます。

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。

情報セキュリティ支援業務を行う者が守るべき５つの倫理原則を紹介します。

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。

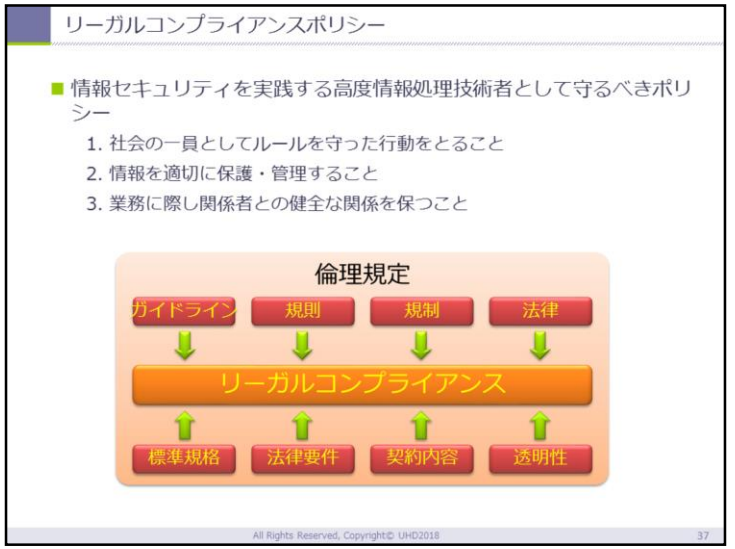
4. 専門的、業務上知り得た情報の機密性を、法的または専門的な権利または開示義務が無いかぎり、厳守しなければならない。

5. 注意深く行動し、信用を損なってはならない。

また、コンプライアンスは、組織として考え続けることが重要で、作成しただけでは意味がありません。関係者に周知させ、遵守させてはじめて意味をなします。そのためには、次の２つの対策が必要です。

●法的手続きの整備

●誓約書の養成



リーガルコンプライアンスポリシーとして３つの守るべきポリシーを理解し、遵守し、遵守させることは、セキュリティ対策の人的リスクの対策の基本となります。

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

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

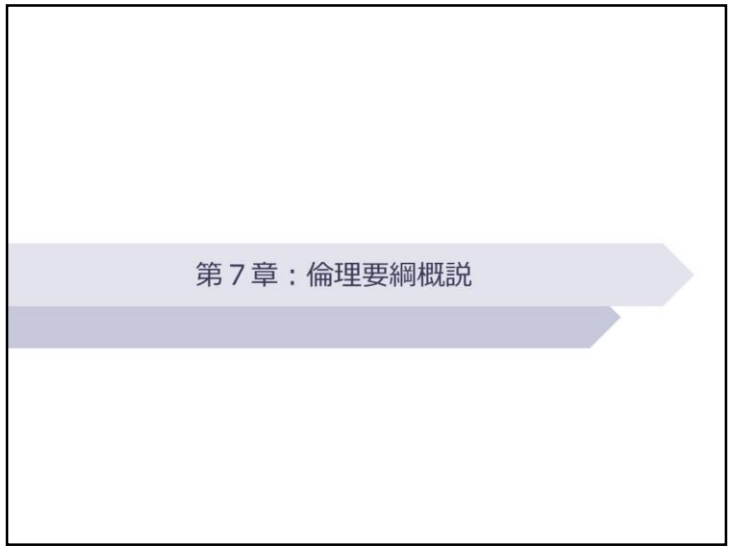
●個人情報の保護規定を厳正に遵守すること

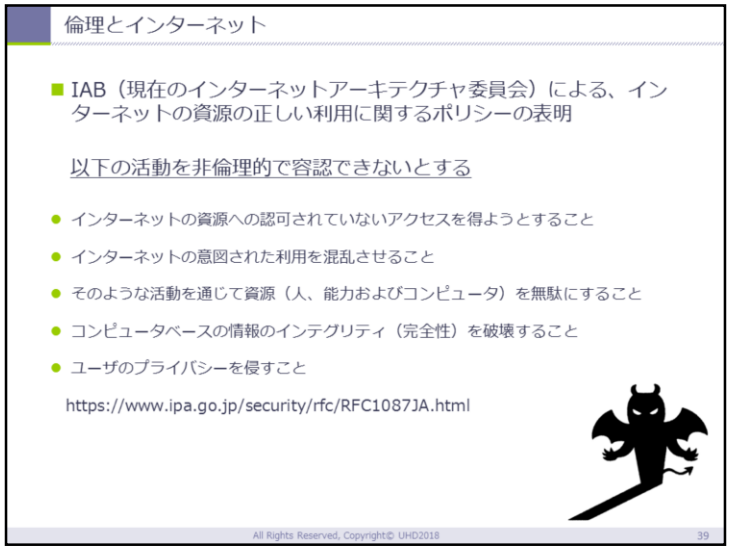
3. 関係者との健全な関係を保つ

●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

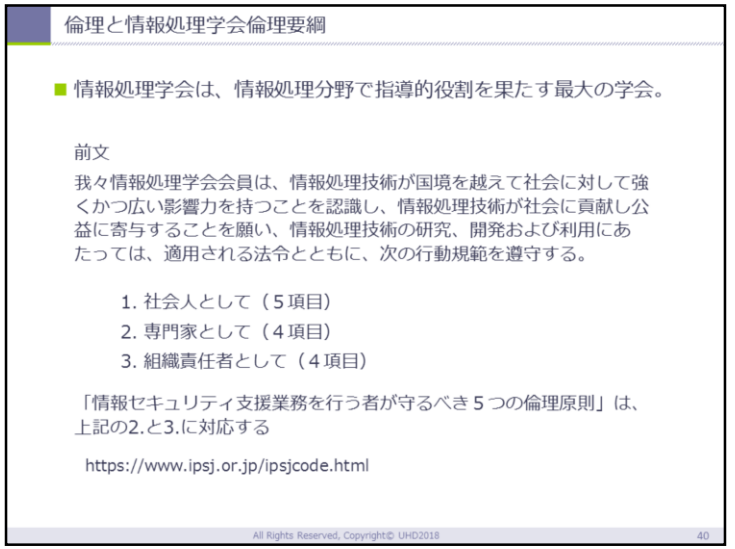

第７章：倫理要綱概説



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まれてきています。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ますが、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ません。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ります。

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が表明した、インターネットの資源の正しい利用に関するポリシーです。



情報処理学会の倫理要綱は、きちんと確認する必要があります。

[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。

[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。

[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。

セキュリティ講座
演習資料

ver 1.0

演習環境の下準備手順

演習 4 と演習 5 でパソコンを使った演習を行うため、実機の環境構築手順を示します。

作業1. VirtualBox のインストール

__1. Oracle VirtualBox を、標準設定のままインストール。

__2. [ファイル(F)]-[ホストネットワークマネージャー(H)...]を開き、 [作成(C)]をクリック。

__3. 新しくできた Host-Only Ethernet Adapter #2 で、以下の設定を行う

アダプター(A)
◉アダプターを手動で設定(M)　←選択
IPv4 アドレス:　192.168.33.1
IPv4 ネットマスク(M):　255.255.255.0
DHCP サーバー(D)
□サーバーを有効化(E)　←チェック無し

__4. [ファイル(F)]-[環境設定(P)...]-[ネットワーク]で、右側の「新しい NAT ネットワークを追加します。」ツールボタンをクリックして追加する。

作業2. 仮想マシンのインポート

__1. [ファイル(F)]-[仮想アプライアンスのインポート(I)...]

__2. pen_training.ova を選択し、そのまま[インポート]

作成された 2 つの仮想マシンのうち、Kali-Linux の USB 設定を変更する。

__3. 仮想マシン Kali-Linux を選択し、[設定(S)]をクリック

__4. [USB]-[☑USB コントローラーを有効化(U)]で、[◉USB 1.1 (OHCI) コントローラー]を選択する。

作業3. 動作確認

__1. 仮想マシン Mutillidae をダブルクリックして起動。
起動しない場合、メッセージに従って修正を行ってください。

__2. ホスト PC から以下の ping が届くことを確認。

```
ping 192.168.33.10
```

__3. 以下のアカウントでログインできることを確認。

```
mutillidae login: vagrant
Password: vagrant
```

__4. 仮想マシン Kali-Linux をダブルクリックして起動。
起動しない場合、メッセージに従って修正を行ってください。

__5. 以下のアカウントでログインできることを確認。

```
Username: root
Password: toor
```

__6. ホスト PC から、以下の ping が届くことを確認。

```
ping 192.168.33.11
```

__7. 先にログインした Mutillidae のコンソールから、以下の ping が届くことを確認。

```
ping 192.168.33.11
```

__8. 仮想マシン Mutillidae と Kali-Linux をシャットダウンし、作業終了。

演習1. 情報資産と脅威の検討

どんなものが情報資産となるか改めて認識したうえで、脅威、脆弱性、リスクをグループで検討していきます。最後にリスクについて検討し、全体で共有を行います。

作業1. 個人作業（1 分）

__1. （差支えない範囲で）自組織で守るべき情報資産を 1 つ書き出してください。

作業2. グループ作業（2 分）

__1. 守るべき情報資産をグループメンバに提示してください。

作業3. 個人作業（7 分）

__1. 各情報資産に対する脅威を 3 つ以上列挙してください。

作業4. グループ作業（15 分）

__1. 脅威についてグループ内で全体共有し、脆弱性とリスクを検討してください。

__2. 見落としがち、または対策が難しそうなリスクを 1 つ選び、全体で対策を検討する。

作業5. 全体共有(5 分)

__1. 選んだ脅威と対策検討結果を発表していきます。対策は完全でなくてかまわないので、どのような検討を行って、どのような点が問題なのか伝えるようにしてください。

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

以下のケーススタディでどのような行動をとるべきか。節目節目で考えます。
時間は目安です。演習時間が限られているため、時間内にできたところまでで演習結果をまとめ、グループ間で発表を行います。各グループの進捗の違いも今後の参考となります(なぜ早く進んだのか、なぜ時間がかかったのか、など)。

作業1. 検知と連絡受付、トリアージ (15 分)

1. あなたの組織のセキュリティスタッフが、セキュリティ情報およびイベント管理ツール (SIEM: Security Information and Event Management)のテスト運用を開始しました。VPN のログも監視対象に含めたところ、アカウント Akira が数日間にわたり複数のシステム、複数の IP アドレスから同時に VPN ログインしていることが検知されました。

__1. セキュリティスタッフのメンバーがこの時点ですぐに行わなければならないことは何でしょうか。グループ内で話し合って 3 つほど挙げ、優先順位をつけてください。

作業2. インシデント対応 – 初動、調査（45 分）

2. アカウント Akira を無効化したところ、すぐにアカウント Ibuki による同様のアクセスが検知されました。セキュリティスタッフは経営陣と CSIRT に状況を報告することにしました。そしてあなたは CSIRT のメンバーとして**初動対応**をとることになりました。

初動対応の流れを簡単に示します。慣れている方は読み飛ばして構いません。

インシデント対応の主な活動は 3 つあります。実際には、組織全体の利害関係者間で活動内容について文書化されている必要があります。

1. 初動
   - 対応チーム編成、データの検討、インシデント見極め
   - 適切な対応を判断できるだけの情報を集める
2. 調査
   - どういう経緯で何が起こったのか
   - 責任の所在
3. 修復
   - 修復計画は、インシデント対応の初期段階で検討
   - 法律、ビジネス、政治、技術面を考慮
   - 修復のタイミング
     - 脅威の存在を示す痕跡がなくなったタイミングで実施

上記 3 つの主な活動内容の例をざっと以下に示します。

1. 初動～一般的な活動～
   - セキュリティスタッフに対する、状況の聞き取り調査
   - 状況を技術的に正しく判断できる IT スタッフに対する聞き取り調査
   - インシデントに関連すると思われる事業部門の職員への聞き取り調査
   - ネットワークログやセキュリティログによる、インシデント発生の裏付け
   - 集めたすべての情報の文書化

2. 調査～次の 5 段階で調査を実施～
    1. 最初の手がかり
        - インシデントと関連性があるか
            - 進行中のインシデントと関係なければ除外する
        - 具体的かつ詳細か
            - 5W1H を意識する
        - 利用できる手がかりか
            - 関連性があっても原因につながらない手がかりもある
    2. 脅威が存在することを示す痕跡（IOC[1]: Indicator of Compromise）
        - 作業ディレクトリ名、出力ファイル名、ログインイベント、永続化メカニズム（データベース）、IP アドレス、ドメイン名、マルウェアのプロトコル上の特徴など
        - インシデント検出の自動化でも使用可能
        - ホストベースインディケーター
            - シグニチャーベース
            - 方法論ベース
        - ネットワークベースインディケーター
    3. 疑わしいシステムの特定
        - 検証
            - そのシステムは本当に疑わしいシステムか。
        - ラベル付け
            - バックドア導入、データ窃盗、認証情報収集、SQL インジェクション、など
        - 優先順位付け
    4. 証拠の保全
        - システム操作時間は最小限で。システム上の変更は極力避ける。適切に文書化する。
        - ライブレスポンス（稼働中のシステムの情報収集）
            - プロセスリスト、稼働中のネットワーク接続、イベントログ、レジストリなど
        - メモリー収集[1]（可能な場合）
        - フォレンジックディスクイメージ[1]

5. データ解析
    - マルウェア解析
        - 疑わしいプログラムのトリアージ
        - マルウェアの基本機能の洗い出し
        - リソースと予算があれば、疑わしいマルウェアの動作解析
    - ライブレスポンス解析
        - システムへの不正アクセスによる影響の把握
        - 些細な見逃しが致命的となることもある
    - フォレンジック解析
        - 疑惑の裏付け、または否定する情報を発見する
        - 攻撃シナリオを想定し、解析範囲を絞り込む
            - 限られた時間の使い方を強く意識する

3. 修復～重要な調査情報をまとめる～

修復の計画は３つに分けて考えます

1. 態勢整備
    - 修復を確実に成功させるため、段階を踏んだ手順
    - 手順策定、連絡先の交換、責任の明示、可視化、リソース確保、スケジュール調整など
2. 短期的戦術
    - 今起こっているインシデントに対する対処
    - システム再構築、パスワード変更、パケットフィルタリング、広報、業務処理の変更
3. 長期的戦略
    - 情報セキュリティ管理体制の見直し

そして、重要な調査情報をまとめておきます。

- 集めた証拠の一覧
- 影響を受けたシステムの一覧
- 疑わしいファイルの一覧
- アクセスされた、または窃取されたデータの一覧
- 攻撃者による重大な活動の一覧
- ネットワークベースの、脅威の存在を示す痕跡
- ホストベースの、脅威の存在を示す痕跡
- 侵害を受けたアカウントの一覧
- 進行中のタスクと、処理すべきタスクの一覧

ここから作業 2 の演習手順です。

__1. 職員からの聞き取り結果の一部を下方に示します。ここからどのような状況が読み取れるか、ほかにどのような情報が必要かをグループ内で検討してください。そして、**調査の手がかり**となる項目を検討し、列挙していってください。

__2. 列挙した調査項目の優先順位を決めてください（高・中・低くらいの粒度で）。

__3. 優先順位の高い調査項目から、継続中の攻撃を排除または修復する方法を考え、まとめます（不完全で構いません）。

職員からの聞き取り結果の一部：

- 組織内の複数の部署で標的型攻撃メールを約 3 か月前に受信。合計１００通。PDF ファイルが添付されていた。受信者の中に Akira は入っていたが、Ibuki は入っていなかった。Akira を含め何人かが添付ファイルを開いたが、感染が確認されたのは Akira だけである。
- 標的となったメールアドレスは、先日開いた技術カンファレンスの講演者とその関係者のアドレスに限られていた。
- 技術カンファレンスでは、研究を進めている画期的な新技術について紹介を行った。その研究の機密データは別途のサーバーSV01 に保管され、機密プロジェクト関係者以外が読み書きできないよう、適切にアクセス制御設定がされている。
- 通信ログから、 1 か月前にサーバーSV01 から外部 FTP サーバーへ cab 形式ファイルが送信されていることは確認できた。暗号化されていたため cab ファイルの内容はわからない。機密データは削除されていない。
- 各職員のアカウントには、各自で使用する PC に対するローカル管理者権限が与えられていた。
- システム管理者の利便性から、ローカル管理者である administrator のパスワードはすべてのサーバーとクライアントで共通化されていた。
- Akira のパソコンから Gh0st RAT (Remote Access Tool)が発見されたが、RAT の通信は件のメール受信後数日しか観測されていない。
- Akira は VPN 経由で自宅から組織内のネットワーク環境に接続していた。

作業3. インシデント対応 – 調査 – 脅威が存在することを示す痕跡（15 分）

3. 攻撃の脅威は今も続いています。脅威があることを裏付けし、修復後に脅威がなくなったことを保証するために、**脅威が存在することを示す痕跡、インディケーター(IOC)**を明確にしなければなりません。

__1. インディケーターは手がかりを根拠に決定していきます。この事例では、どのような情報がインディケーターとして使えるか、グループ内で検討してください。インディケーターの例をいくつか示します。

- **攻撃元 IP アドレスと接続先ポート番号**
- **サーバーSV0 における cab ファイルの作成イベント**
- **など**

作業4. インシデント対応 – 調査 – 疑わしいシステムの特定、証拠の保全 (15 分)

4. IOC のインディケーターを基に脅威の検知を行ったところ、ほかのコンピュータからも依然としてビーコンが送出されていることがわかりました。外部 FTP サーバーへの接続はサーバーSV0 のみであることも確認できました。攻撃者が使用しているアカウントは、今のところ Akira と Ibuki のアカウントだけです。アカウント Akira による VPN 接続には、Akira の家からの接続も含まれています。組織内で使用されているサーバーは 10 台、クライアント数は 1000 台あります。CSIRT では、インシデントに巻き込まれた**疑わしいシステムを特定**し、**証拠の保全**対象にするコンピュータを選ぶ必要があります。

インシデント対応ではほとんどの場合、すべてのコンピュータの証拠保全を行う必要はなく、また保全を行う時間も解析する時間もありません。

__1. 証拠の保全対象となるコンピュータを次の中から選んでください。保全対象となる理由、ならない理由をグループ内で検討し、納得できるようにしてください。

1. **職場にある Akira のコンピュータ**
2. **職場にある Ibuki のコンピュータ**
3. **家にある Akira のコンピュータ**
4. **サーバーSV0**
5. **10 台のサーバすべて**
6. **ビーコンが送出されているコンピュータ**
7. **すべてのクライアントコンピュータ**

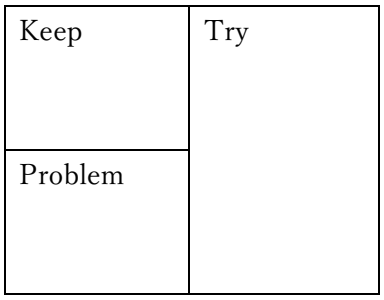
作業5. インシデント対応 – 調査 –証拠の分析（20 分）

5. 保全した**証拠を分析**した結果、以下の事実が分かりました。

- Akira のコンピュータから以下の情報が攻撃者に知られた可能性がある
- ユーザー名、パスワード、クライアント証明書、ローカル管理者パスワード
- Akira のコンピュータの PDF リーダーのバージョンが古いままであった
- ローカル管理者パスワードを使い、SV0 に侵入。
- Ibuki のアカウントは SV0 から入手したと思われる。
- 攻撃者による内部偵察は 3 週間に及んでいたこと。
- SV0 の機密データは暗号化 RAR ファイルとして圧縮し、拡張子を cab に変換し、FTP 送信していた。
- 送信後に RAR ファイルを削除し、Windows のデフラグツールを使用して削除データの復元を困難にしていた。
- VPN 接続に使用された IP アドレスの 1 つが、Gh0st RAT のビーコン送付先と一致していた。その IP アドレスは、プロバイダーとしても、地域としても、Akira とは全く無関係であった。
- 暗号化 RAR ファイルと VPN 接続の影響で、具体的にどのような機密が漏洩したかは突き止められなかった。

__1. CSIRT では修復作業を行うことにしました。修復計画の短期的戦術として、今起きているインシデントに速やかに対処するにはどのような対策をとればよいでしょうか。グループで検討し、対策の例を列挙してください。

作業6. ふりかえり – KPT (Keep-Problem-Try)法 (30 分)



__1. 模造紙で Keep/Problem/Try の枠をつくります。

__2. 本演習で気づいたことのうち、今後も続けていきたいことを各個人で付箋紙に書き、Keep 欄に貼り付けます。

__3. 本演習を通じて問題となったこと、改善が必要と感じたことを各個人で付箋紙に書き、Problem 欄に貼り付けます。

__4. グループで Keep 欄と Problem 欄を整理してください。そして、Keep を改善する案や Problem を解決する案を（すべてでなくてよいので）付箋紙にまとめ、Try 欄に貼り付けます。

__5. 出来上がった模造紙を用い、Try 欄から特に重要と思われるものを 3 つ選び、全体で発表を行います。

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～

脅威モデリングが効果的であることはセキュアシステム開発で実証されつつあります。しかし脅威モデリングでは、どのような脅威があるのかをすべて洗い出すのが難しく、脅威がどのような場合に顕在化するか明確にすることに時間がかかります。そこで、脅威モデリングと対になるセキュリティ要件をシステム上で考えることで、モデリングの負担を減らすことも考えられています。脅威の対策はセキュリティ要件とほぼ同義ですが、幅広いセキュリティの知識と経験から脅威を洗い出す脅威モデリングよりも、具体的なシステムに限定して必要な要件を洗い出すほうが手続きとしては取り組みやすくなります。

ここでは渋滞ナビシステム構築を考えてみます。このシステムではスマートフォンやカーナビのナビアプリで取得した交通状況をサーバー上に蓄積し、走行地区ごとの渋滞情報をナビアプリに配信するサービスを提供するものとします。

まずは脅威モデリングに倣い、セキュリティ要件を整理します。
コンピューター上の事象は次の 3 段階で考えられます。

1. 『誰が』
2. 『どの情報/資産に対して』
3. 『読み/書き/実行するのか』

これらを以下の用語で表現することにします。

1. 『アクター』
2. 『資産』
3. 『操作』

作業1. アクターの洗い出し（10 分）

本ナビシステムのアクターとして考えられる登場人物を挙げ、分類してください。これはグループ内で検討し、共有します。

作業2. 資産の洗い出しと操作（20 分）

個人作業で行います。

本ナビシステムの資産として考えられるものを挙げていきます。その際、「意図しない人に勝手に使われては困る情報や機能」に限定していくつか列挙してください。すべてでなくてかまいません。そして、洗い出した資産に対し、主要なアクター（1～2 アクターでよい）に許可される操作を列挙してください。

セキュリティ要件を洗い出していくと、いくつかのパターンが見えてきます。このパターンを類型化することで対策を単純化できます。簡単なケースとして、『「攻撃者」は「○○資産」を読めない』というルールはかなり頻繁に登場するのでまとめることができるでしょう。

例：

資産	セキュリティ要件
2 地点間の通過所要時間 ├開始地点と終了地点 └通過所要時間（秒）	「利用者」は、「所要時間」を読める、書けない 「ナビアプリ」は、「所要時間」を読める、書ける 「第三者」は、「所要時間」を読めない、書けない
2 地点間通過速度の揺らぎ ├開始地点と終了地点 └速度の偏差	「利用者」は、「揺らぎ」を読めない、書けない 「ナビアプリ」は、「揺らぎ」を読める、書ける 「第三者」は、「揺らぎ」を読めない、書けない
特定地点の道路状況取得	「利用者」は、「道路状況取得」を実行できる 「ナビアプリ」は、「道路状況取得」を実行できる 「第三者」は、「道路状況取得」を実行できる
…	…

※ 一つの資産が複数の資産の集合体であることもあります

※ 本来は物理的資産も考えますが、ここでは情報資産に限定して構いません。

※ 「攻撃者」が○○機能の「妨害」を実行できない、というセキュリティ要件もあります。資産に対するセキュリティ要件は、ここでは自由に考えてください。

資産	セキュリティ要件

※ 本作業で洗い出したセキュリティ要件はそのまま脅威モデリングの脅威と対応します。

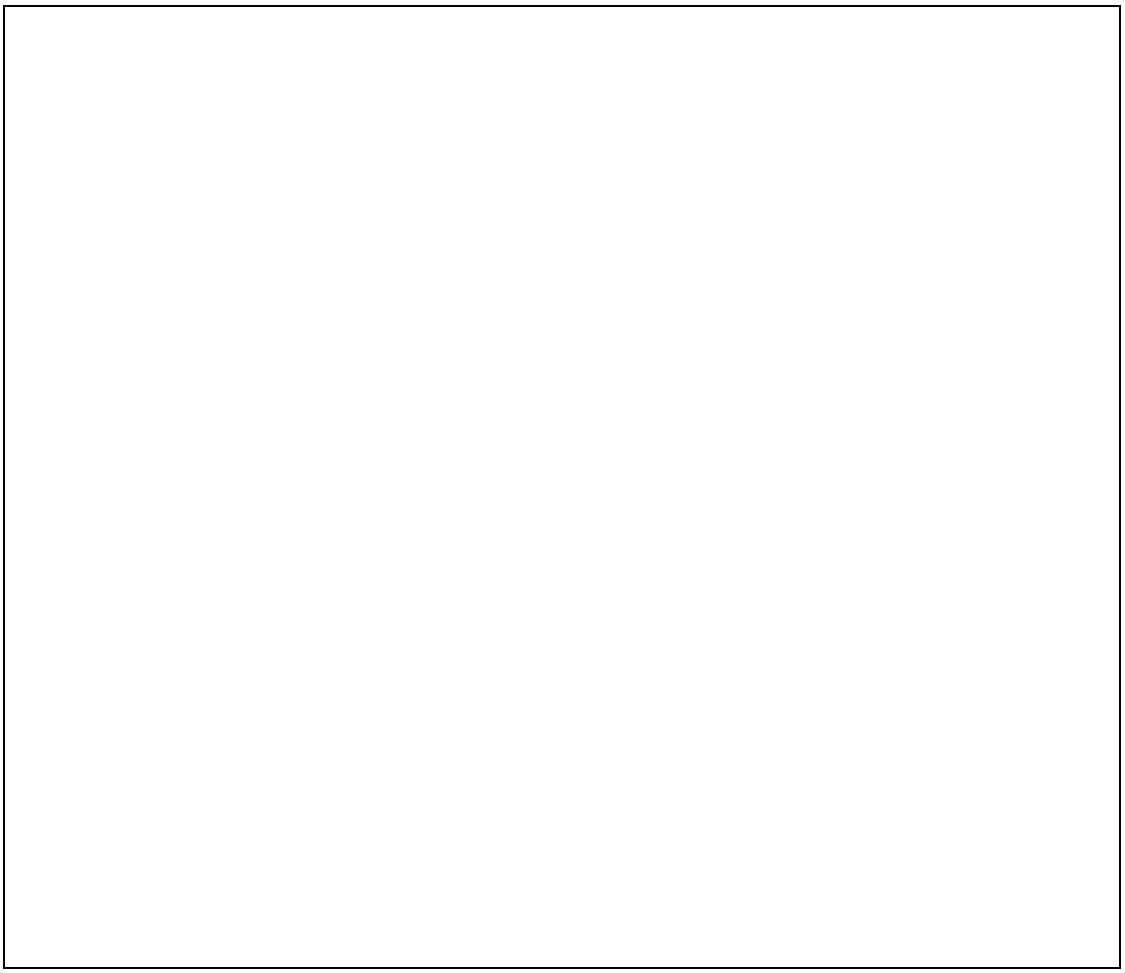
作業3. 資産の所在（20 分）

個人作業で行います。

多くの情報資産は、ネットワークを介してクライアントとサーバー間を行き来します。そのすべての経路において脅威が存在します。本件の渋滞ナビシステムではどのようなソフトウェア、装置、経路に脅威が存在するでしょうか。

想定されるネットワークの概略図を描き、先の（情報）資産に対する脅威の存在する箇所、すなわちセキュリティ要件を確認すべき個所を考え、脅威の例をいくつか書きこんでください。

※ 本来なら、どの情報資産に対する脅威かを明らかにすべきですが、ここでは脅威だけをあげていただければ構いません。



○をつけたすべての個所でセキュリティ要件が満たされたならば、それはセキュアなシステムであることになります。

作業4. グループディスカッション（20 分）

作業２と３の結果をグループ内で共有し、どのようなセキュリティ要件が存在し、どの箇所で検証すべきかを共有及び検討してください。気づかなかったアイディアや構成、セキュリティ要件があった場合は記録しておきます。

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

ここでは OWASP で提供する OWASP Mutillidae（ミューティリデ） 2 という、意図的に脆弱にした Web アプリケーションを用い、Web アプリケーションの脆弱性の体験とテストを行います。
最初は手動で脆弱性を探し、引き続き脆弱性チェックツールを使ってみます。
演習は個人ごとに行えますが、攻撃手法やチェックツールの検査結果の読み取り方でぜひディスカッションを行ってください。
なお、オプション演習は後回しにし、時間に余裕がある場合に実施してください。

作業1. 脆弱な Web アプリ Mutillidae の起動と表示（5 分）

__1. VirtualBox マネージャーを起動します。
__2. 仮想マシン Mutillidae をダブルクリックして起動します。ログインはしません。
__3. VirtualBox マネージャーが起動するホスト PC でブラウザーを開き、以下の URL にアクセスします。

```
http://192.168.33.10/mutillidae/
```

作業2. SQL インジェクション（10 分）

最初に SQL インジェクションのテストを行います。

__1. 以下のメニューを選びます。
[OWASP 2017]-[A1 - Injection (SQL)]-[SQLi - Extract Data]-[User Info (SQL)]
__2. 以下のデータ入力後に[View Account Details]をクリックし、通常動作を確認します。

```
Name        admin
Password    adminpass
```

問題 1.

このページには SQL インジェクションの脆弱性が含まれています。
[Hints and Videos]も参考にしつつ、以下の確認をしてください。
必要であれば、インターネットの翻訳サイトで英語を翻訳してください。

1-1) SQL インジェクションの脆弱性があることの確認
1-2) 様々な入力を試して表示されるエラーメッセージから、どのような内部処理をしているか推察してください。
1-3) 脆弱性を用い、全ユーザー情報を閲覧できることを示す
1-4) （オプション）試行錯誤して、データベース名と SQL サーバーへのログインユーザー名、バージョンなどの取得を試みてください。

作業3. コマンドインジェクション（10 分）

コマンドインジェクションを試します。

__1. 以下のメニューを選びます。

[OWASP 2017]-[A1 - Injection (Other)]-[Command Injection]-[DNS Lookup]

__2. （オプション)ホスト PC がインターネットにつながっている場合、Hostname/IP 欄で幾つか動作を確認してください。

問題 2.

このページにはコマンドインジェクションの脆弱性が含まれています。

[Hints and Videos]も参考にしつつ、以下の確認をしてください。

2-1) /etc/passwd を表示させる

2-2）内部の IP アドレスを調査する

2-3）その他、ディストリビューション確認やカーネルバージョン確認など。

作業4. （オプション）認証の不備（10 分）

SQL インジェクションの脆弱性を用い、認証の不備を試します。

__1. 以下のメニューを選びます。

[OWASP 2017]-[A2 - Broken Authentication and Session Management] -[Authentication Bypass] -[Via SQL Injection]-[Login]

__2. 以下のデータ入力後に[Login]をクリックし、ログイン失敗を確認します。

```
Name        admin
Password    password
```

__3. 以下のデータ入力後に[Login]をクリックし、通常動作を確認します。

```
Name        admin
Password    adminpass
```

__4. [Logout]でログアウトします。

問題 3.

[Hints and Videos]も参考にしつつ、ユーザー名もパスワードも分からない前提で、SQL インジェクションを用いてログインしてください。

作業5. （オプション)機微な情報の露出 （10 分）

機密情報ではないですが、機微な情報として PHP 情報を取り出してみます。

__1. 以下のメニューを選びます。

[OWASP 2017]-[A3 - Sensitive Data Exposure]-[Information Disclosure] -[PHP Info Page]

問題 4.

以下の情報を確認してください。

PHP Version _____

OpenSSL Library Version _____

作業6. XML 外部エンティティ参照 (XXE) (10 分)

XML 外部エンティティ参照 (XXE)では、XML 検証ページに不正な XML を入力し、スクリプトを実行させてみます。

__1. 以下のメニューを選びます。
[OWASP 2017]-[A4 - XML External Entities]-[XML External Entity]-[XML Validator]

__2. [Hints and Videos]-[XML External Entity (XXE) Injection]を開き、[Videos]のすぐ上に例示されている以下の XML(改行は任意)を入力し、[Validate XML]をクリックします。

```
<?xml version="1.0"?>
<change-log>
  <text>
    &lt;script&gt;alert(&quot;Hello World&quot;)&lt;/script&gt;
  </text>
</change-log>
```

__3. <text>要素に記述されているスクリプトは実行されましたか(はい ・ いいえ)。

残りのペネトレーションテストは、時間に余裕があるときに試してみてください。

手動で行うペネトレーションテストは時間がかかることは実感できたはずです。また、脆弱性を確認するだけであれば、具体的な攻撃方法を考える必要もありません。例えば SQL インジェクションの脆弱性チェックでは、シングルクォーテションの入力だけでも確認できます。

次の演習では、Kali Linux に同梱されているペネトレーションテストツールを用いた脆弱性検査を幾つか体験します。

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

作業1. 下準備 (5 分)

__1. VirtualBox で、Kali-Linux をダブルクリックして起動します。

__2. 以下の情報でサインインします。

```
Username: root
Password: toor
```

引き続き環境を日本語化します。

__3. デスクトップ上部のメニュー右端の▽を開き、メニュー左下の設定ツールをクリックして開きます。

__4. Region & Language で、日本語表示設定をします。

__5. Restart をクリックし、サインインしなおしてください。

作業2. OWASP ZAP (10 分)

OWASP が提供する OWASP ZAP は、操作が簡単なペネトレーションテストツールです。まずはこのツールを試してみます。

__1. [アプリケーション]-[03 - Web Application Analysis]-[owasp-zap]を実行します。Apache License は[Accept]してください。

__2. Do you want to persist the ZAP Session? では、一番上のラジオボタンにチェックを入れて、[Start]します。

__3. [Tools]-[Options…]-[Language]で日本語にし、owasp-zap を開き直します。

__4. ZAP セッションの保持方法をどうしますか？ では、一番上のラジオボタンにチェックを入れて、[開始]します。

__5. クイックスタート タブの攻撃対象 URL に以下を入力し、[攻撃]をクリックしてしばらく待ちます。スキャンが終了したか否かは、[停止]ボタンの状態で判断できます。

```
http://192.168.33.10/mutillidae/
```

問題 1. スキャン終了後の以下の項目を確認してください。

1-1) OS コマンドインジェクションが見つかったページの PHP ファイル名

/index.php?page=_____

1-2) SQL インジェクションが見つかったページの PHP ファイル名（一部で構いません）

/index.php?page=_____

1-3) パストラバーサルで、気になる URL を試してください。
1-4) その他、見つかった脆弱性で気になるものがありましたら確認してください。

作業3. Nikto2 (10 分)

引き続き、Web サーバーのスキャナである Nikto を試します。Nikto はオープンソース(GPL)で、できるだけ短い時間にテストを行うように設計されています。

__1. [アプリケーション]-[02 - Vulnerability Analysis]-[nikto]を実行します。

__2. 以下のコマンドで Nikto によるスキャンを実行します。

```
nikto -host http://192.168.33.10/mutillidae/ -o /tmp/output.txt
```

問題 2. 結果ファイル/tmp/output.txt を見て(less /tmp/output.txt)、以下の確認をしてください。

2-1) クリックジャッキング対策はされていますか。　　(はい ・ いいえ)
2-2) ディレクトリ一覧が有効な URL はどこですか。いくつか列挙し、その URL の動作を確認してください。

/multidae/_____
/multidae/_____
/multidae/_____
/multidae/_____

2-3) HTTP の TRACE メソッドは有効ですか。　　(はい ・ いいえ)

※ クリックジャッキング：リンクやボタンを偽装して、利用者の意図しない動作をさせようとする手法。

作業4. Skipfish (オプション)

最後に、Google が提供するセキュリティチェックツールである Skipfish の使い方の一例を紹介します。本演習環境で実施すると、チェックにほぼ半日かかります。もし実行する場合、途中で停止（Ctrl + C）して結果を確認するようにします。

__1. 仮想マシン Mutillidae に、以下のアカウントでサインインします。

```
mutillidae login: vagrant
password: vagrant
```

__2. DB サーバーmysql と Web サービス apache2 を再起動します。

```
sudo service mysql restart
sudo service apache2 restart
```

※ ここまでの作業でサービスが落ちたり止まったりしている場合があるため。

__3. 使用状況確認のため、top コマンドを実行しておきます。

```
top
```

__4. 仮想マシン Kali-Linux で、以下を実行します。
[アプリケーション]-[03 - Web Application Analysis]-[skipfish]

__5. 表示された端末で、以下のコマンドを実行してスキャンします。

```
touch /tmp/test.wl

skipfish -W /tmp/test.wl ¥
-S /usr/share/skipfish/dictionaries/minimal.wl ¥
-o /tmp/result ¥
-auth-user admin ¥
-auth-pass adminpass ¥
http://192.168.33.10/mutillidae/
```

__6. なにがしかのキーを押してスキャンを開始します。

__7. 途中で止める場合、Ctrl+C で止めてください。それまでのスキャン結果は保存されます。

__8. 以下のコマンドで実行結果を表示します。

```
firefox /tmp/result/index.html
```

実行結果の見方に関するドキュメントはありません。赤い丸や赤い旗の項目を展開し、trace を見ることで、どのような脆弱性が発見されたか確認できます。

演習6.　コンプライアンス事例の検証

ここではあるシステム障害事例を基に、コンプライアンスの観点でどのような問題があったか考えていきます。

作業1.　銀行の統合に伴うシステム障害事例（10 分）

まずは以下のシステム障害の経緯と結果を確認してください。

銀行の統合にあたり、３銀行の勘定系システムを統合することになった。

11 年 12 月（残り 2 年 4 か月） 3 銀行のシステムをＩ社のシステムで一本化し、14 年 4 月 1 日に稼働させることを計画。
12 年 12 月（残り 1 年 4 か月） 3 銀行の頭取による政治力学的な事情により、Ｉ社、Ｆ社、Ｈ社の既存システムをリレーコンピューターでつなぐ方式に計画を変更。
13 年 3 月～6 月　（残り約 1 年） 金融庁よりスケジュールの遅れを指摘される。指摘されたスケジュールの遅れは担当部署からたびたび報告され、経営陣も把握しているものの、適切な指示も詳細な調査も行われなかった。
13 年 5 月（残り 11 か月） 追加システムの特殊なバグ（後日判明）がテストで発見できないまま、３銀行のシステム移行計画が持ち株会社の取締役会で決定される。
13 年 12 月　（残り 4 か月） Ｈ 社のシステムが大手取引先の大量データ処理に向いていないことが分かり、Ｆ 社のシステムを引き継ぐことに計画を変更。同時に金融機関コード、店番号コードの取り扱いを変更。
14 年 3 月上旬　（残り 1 か月） 口座振替の強化テストを実施。ただし時間的余裕がないことから、口座振替データ誤入力時のシステム全体の負荷を調べる異常テストは行われなかった。
14 年 3 月 22 日（残り 10 日） 直前の強化テスト実施後、同月 22 日の経営会議で、システム担当部署からの「おおむね問題なく進んでいる」との回答により、それ以上の確認はせずシステム移行を決定した。異常テストが行われなかったことは、ここでは報告されなかった。
14 年 3 月 25 日の週 のちに語られたＩ社担当者の言によると、3 月 25 日の週の時点でシステム完全統合のめどは立っておらず、4 月 1 日の稼働は絶望的であることが分かったと明かす。
14 年 3 月 31 日（前日）

口座振替データの入力を開始したが、新旧の「金融機関コード」「店番号」が混りミスマッチ発生。
14 年 4 月 1 日（当日） システム稼働を強行。大規模障害発生 のちの語られた F 社担当者の言によると、システム統合作業は 3 月 31 日夜に終わったため、ATM の試験がほとんどできなかったと明かす。

主な結果は以下の通り。

- ATM 障害発生、口座振替は、手作業で修正を続けたが、約 10 万件が未処理
- 顧客の口座データの消失等の二次被害も発生、収束までに約 1 ヶ月を要した
- 金融庁は日銀と共同で持ち株会社に対し 1 カ月立ち入り検査を実施し、業務改善命令を出す
- システム障害に伴う損害は 18 億円程度と発表
- 現場担当者の処分は無し。管理職以上は社内規定に従い処分。情報統括役員は降格の上、辞任。全役員 117 名を減給処分。
- 最終的に 18 年 12 月にシステム統合完了を宣言。しかし 23 年 3 月 14 日、想定外の大量振り込み処理を、統合した F 社の旧システム(01 年より稼働)が対応できず障害発生。24 年、勘定系システムの全面刷新・統合プロジェクトを立ち上げる。延期が続くも、31 年末のシステム切り替え完了を目指す。

作業2. 事例の検討 （40 分）

この事例をコンプライアンス遵守の観点から見ると、法令順守の問題ではなく、社内規定の問題です。このようなシステム障害をなくすためにはどのような対策をとればよいか、グループ内で検討し、３個～１０個程度の箇条書きの形でまとめてください。

作業3. 検討結果の共有 （10 分）

問題点と対策の検討結果のいくつかをグループ単位で発表し、全体で共有を行います。基本的には質疑応答なしで構いません。

作業4. 演習　Kali Linux を使った Windows Server 2003 へのペネトレーション

※ Kali Linux に収録されている armitage と Metasploit を使って Windows Server 2003 のぜい弱性を発見し、不正侵入テスト（ペネトレーションテスト）を実施します。

※ 注意：**Kali Linux はぜい弱性検査や攻撃のシミュレーションなどに使用できる強力なツールですが悪用すると不正な操作も可能です。自分の管理していないマシンに対して使用すると、「不正アクセス行為の禁止等に関する法律」（「不正アクセス禁止法」）に抵触するので、外部との接続が遮断されている環境、自分が完全に管理している環境以外での使用は、行わないようにしてください。**

1. KaliLinux 仮想マシンを起動し、root でログインします。（パスワードは toor）
2. Win2003std 仮想マシンを起動し、Administrator でログインしておきます。（パスワードは password）
3. 画面の上（中央よりやや右に）4 つの GUI 画面の選択アイコンがあるので左から 2 つめ
4. Terminal を起動します。（画面下中央のドックから黒い「$」アイコンをクリック）
5. postgresql.conf ファイルを変更します。

```
# vim /etc/postgresql/10/main/postgresql.conf <Enter>  <---(<Enter>キーを押す)
:set  nu  <Enter>  <---(<Enter>キーを押す。行番号を表示させる)
<i>キーを押し-挿入-モードに変更し、63 行目を変更
 63 port  =  5433
      ↓
 63 port  =  5432
<ESC>キーを押して-挿入-モードを抜ける
:wq  <Enter>  <---(<Enter>キーを押す。:wq でファイルに変更を書き込み vim エディタを終了)
```

6. 以下のコマンドで postgresql を起動します。

```
# service  postgresql start <Enter>  <---(<Enter>キーを押す)
[ ok ] Starting postgresql (via systemctl): postgresql.service.
```

7. metasploit 用のユーザ msf とデータベース msf を作成します。

```
# su postgres  <Enter>
postgres@kali:/root$ createuser msf -P -S -R -D
新しいロールのためのパスワード:   msf  <Enter><---(<Enter>キーを押す)
もう一度入力してください：  msf    <Enter><---(<Enter>キーを押す)
postgres@kali:/root$ createdb  -O  msf  msf   <Enter><---(<Enter>キーを押す。-O はオー)
postgres@kali:/root$ exit    <Enter><---(<Enter>キーを押す)
exit
~#
```

8. metasploit の設定ファイルを編集します。（変更前のファイルを保存してから編集）

```
# cd /usr/share/metasploit-framework/config  <Enter><---(<Enter>キーを押す)
# cp  -p  database.yml  database.yml.org  <Enter><---(<Enter>キーを押す)
# vim   database.yml    <Enter><---(<Enter>キーを押す)
<i>キーを押し-挿入-モードに変更
development:
  adapter: postgresql
  database: msf
  username: msf
```

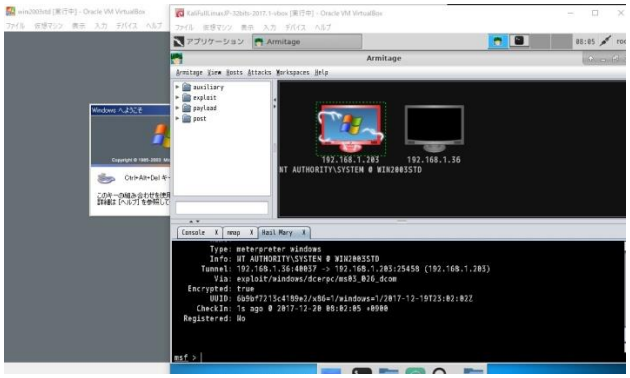
```
  password: hQm2rEM6U3esDNnSCEUPYqKLdfTDgwx+aB/kOfNSVmA=
  以下省略

production:
  adapter: postgresql
  database: msf
  username: msf
  password: msf     <----この行を msf に変更する（これは変更後の状態）
  host: localhost
  port: 5432
  pool: 5
  timeout: 5

test:
  adapter: postgresql
  database: msf_test
  username: msf
  password: hQm2rEM6U3esDNnSCEUPYqKLdfTDgwx+aB/kOfNSVmA=
  以下省略
<ESC>キーを押して-挿入-モードを抜ける
:wq  <Enter>  <---(<Enter>キーを押す。:wq でファイルに変更を書き込み vim エディタを終了)
```

9. GUI を 1 つめの画面に切り替え（4 つの GUI 画面の選択アイコンの左端をクリック）し、。armitage を起動します。(画面左上隅の［アプリケーション］をクリックし「08.Exploitation Tools」＞「armitage」をクリックします。)
10. 「Connect...」ウィンドウが開くので、Pass 欄に「msf」と入力し、[Connect]ボタンをクリックします。
11. 「Start Metasploit?」ウィンドウが開き、Metasploit のサーバを起動するか？と尋ねられるので、［はい］ボタンをクリックします。
12. 「入力」ウィンドウで、「攻撃コンピュータの IP を特定できませんでした。どれですか？」と尋ねられるので 192.168.1.36 と入力し[OK]ボタンをクリックします。
13. メニューバー内の「Hosts」をクリックし、「Nmap Scan」＞「Quick Scan(OS detect)」をクリックします。
14. 「入力」ウィンドウで、スキャンレンジ（範囲）を尋ねられるので「192.168.1.0/24」入力し[OK]ボタンをクリックします。(画面下に nmap タグをもつペインが開きスキャンが開始されます)
15. スキャンが終わると画面上左の Workspace ペインに見つかったマシンが登録されています。(本来表示されないはずの 192.168.1.36 マシンも表示されている)
16. Workspace ペイン内に登録された 192.168.1.203 の Windows マシンをクリックし、メニューバーの「Attacks」をクリックしプルダウンメニュー内の「HailMerry」をクリックします。
17. 「Really？」ウィンドウが開き英語で「一度開始すると HailMerry はワークスペース内のホストにフラッドエクスプロイト攻撃を仕掛けます」と警告されますが、[はい]ボタンをクリックします。
18. スキャンが終わるとワークスペース内に制圧（不正侵入された状態）のホストのアイコ

ンが表示されます。



19. 制圧されたホストのアイコンを右クリックし「Metapreter 番号」>「Explore」>「Browse File」をクリックすると画面下に Windws2003 仮想マシンの C:¥Windows¥System32 内のファイル一覧が表示されます。左上のフォルダをクリックすると現在のディレクトリの 1 つ上のディレクトリに移動します。いろいろ操作して実感してください。
20. 「Metapreter 番号」>「Explore」>「Log keystrokes」を実行し[launch]ボタンをクリックして実行すると、Windows のキーボード入力をキャプチャできます（少し反応が遅い)。Windows でメモ帳を開いて何か入力（アルファベットと数字が分かりやすい）してみてください。
21. 「Metapreter 番号」>「Explore」の他のメニューも実行してみてください。

演習終了