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

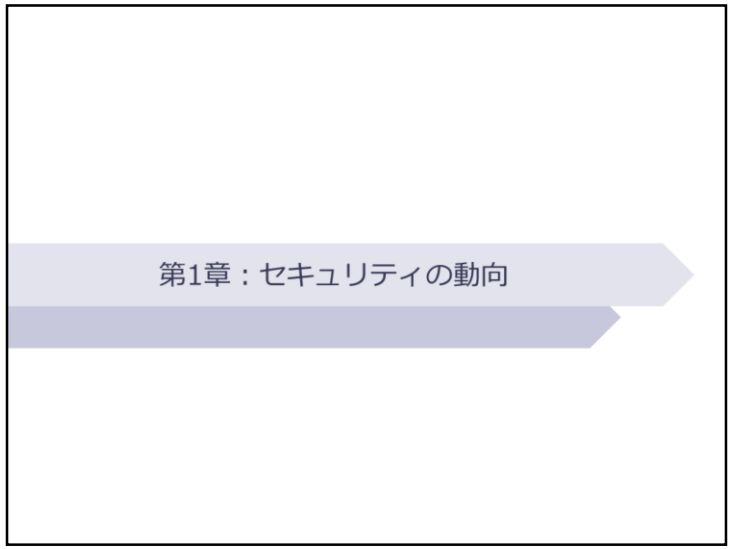
株式会社サンプル

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

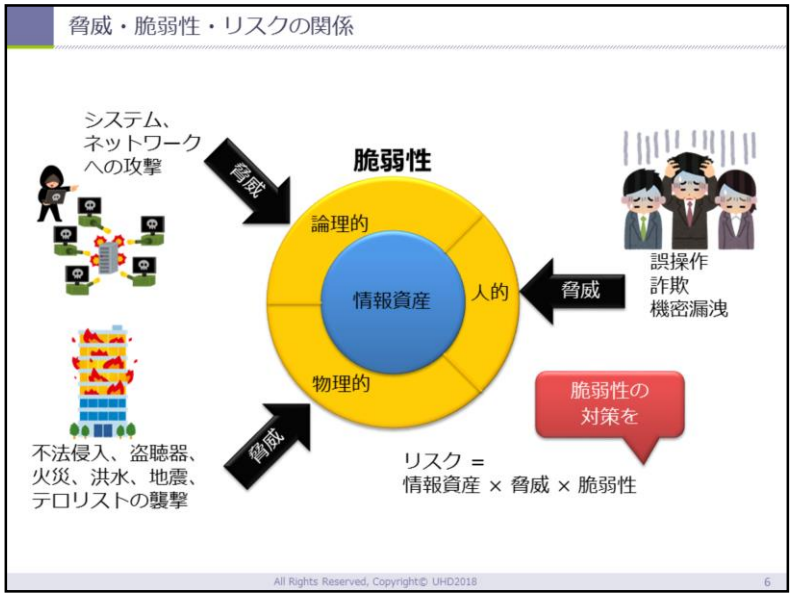
目次


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。



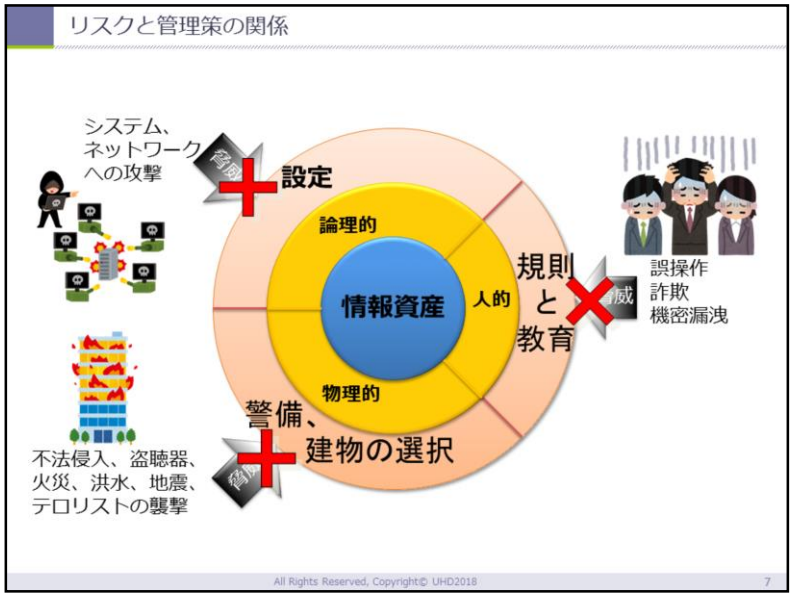
脅威、脆弱性、リスクといった用語は、セキュリティを学ぶうえで多用されますが、それぞれの定義の違いを整理しておく必要があります。

[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。

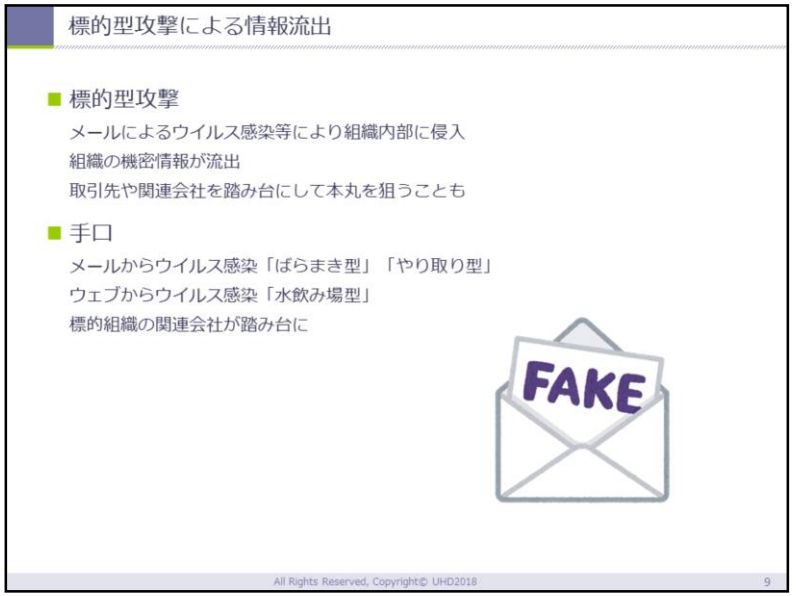
人的な脆弱性に対しては、規則と教育で対応します。これには日々の意識づけが大切です。人的な脅威が発生した場合、論理的な対策である程度は防げますが、多くの場合は利用者個々人の日頃からの注意(Due Care)で防ぐことができます。

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

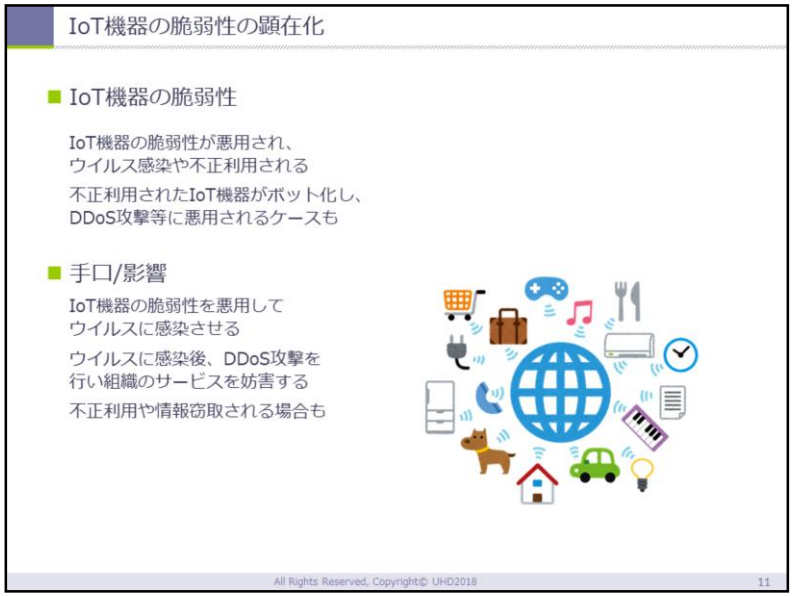
■富山大学への標的型攻撃により研究成果等が外部流出の可能性

·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。

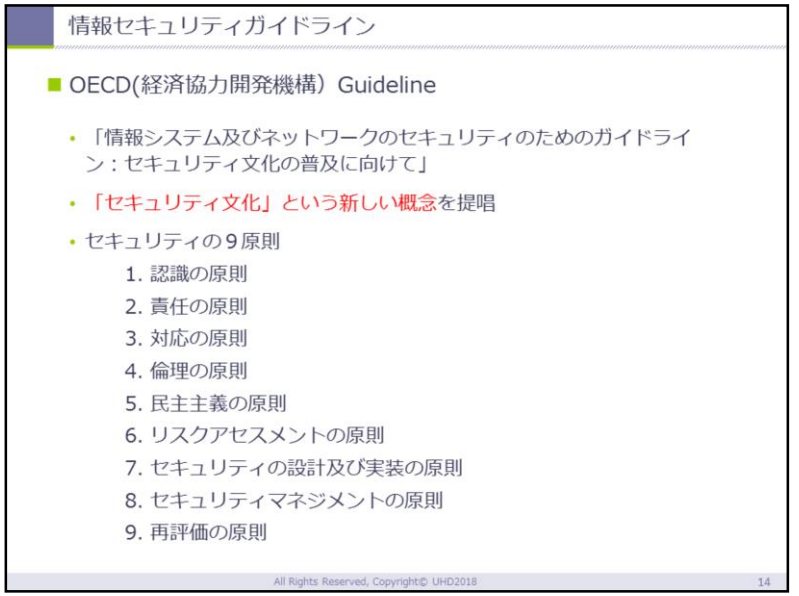
[ITU] 世界最古の国際機関。無線通信と電気通信分野において各国間の標準化と

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。

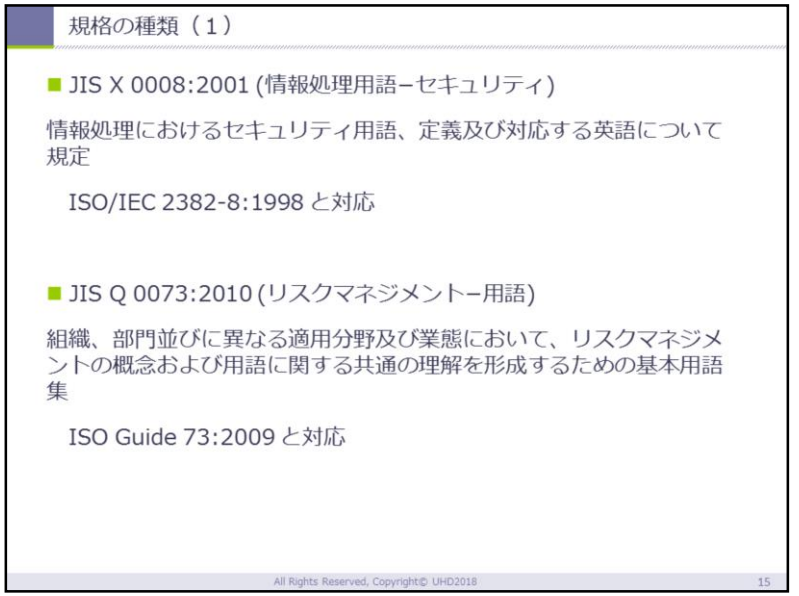
8. セキュリティマネジメントの原則（Security management）：参加者は、セキュリティマネジメントへの包括的アプローチを採用するべきである。

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

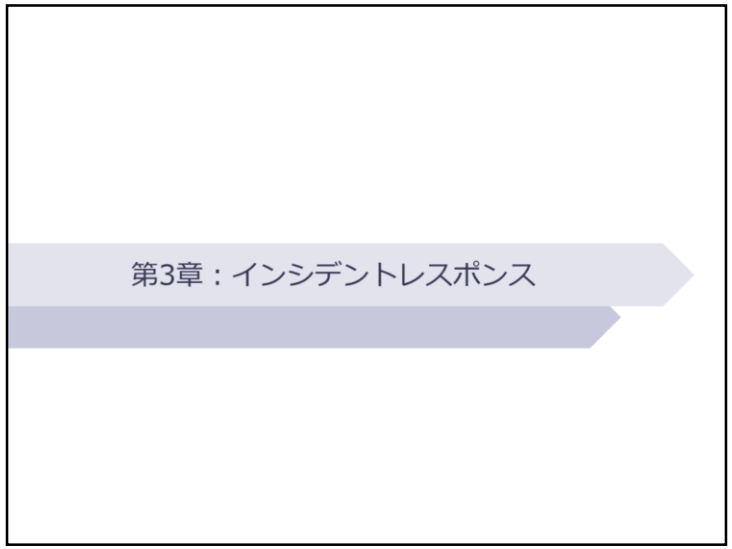
＊情報技術に関連した製品及びシステムが適切に設計され、その設計が正しく実装されていることを評価するための国際

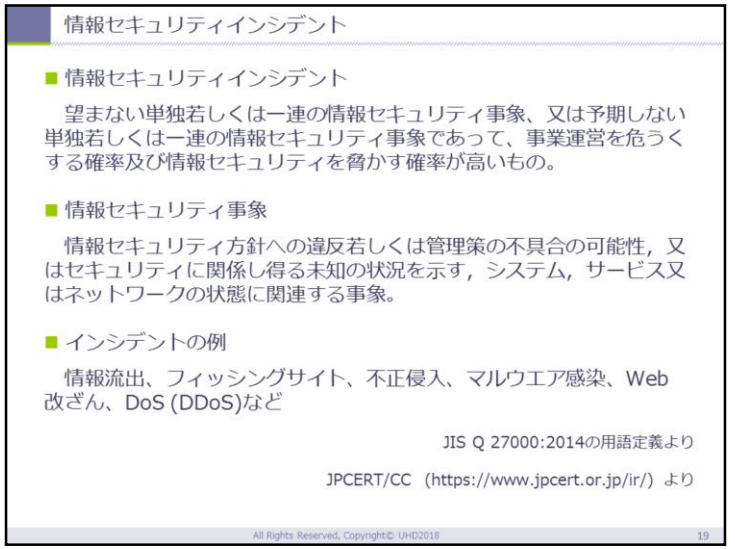
標準規格です。

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

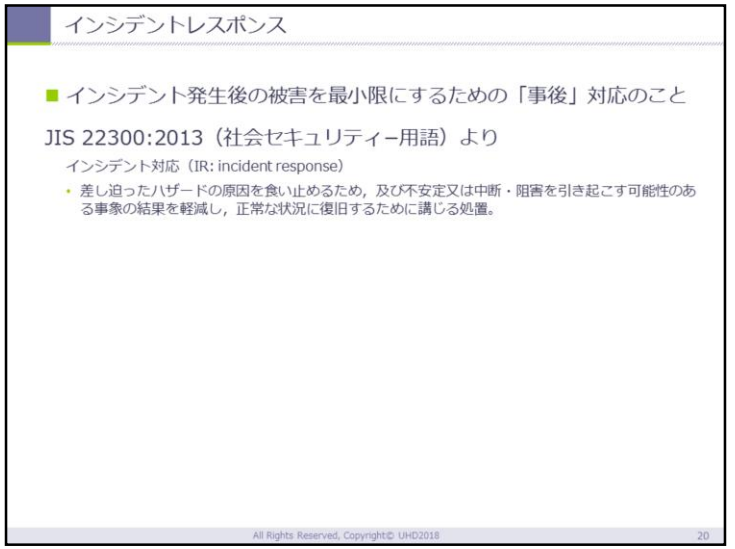
・PCやルータなどの物理機器の盗難や破壊工作

情報セキュリティ事象の例

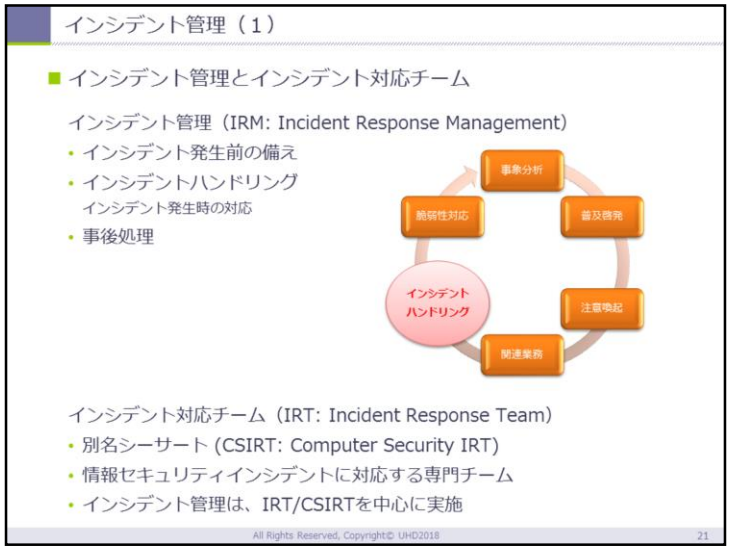
・情報セキュリティシステムの脆弱性の発見

・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）

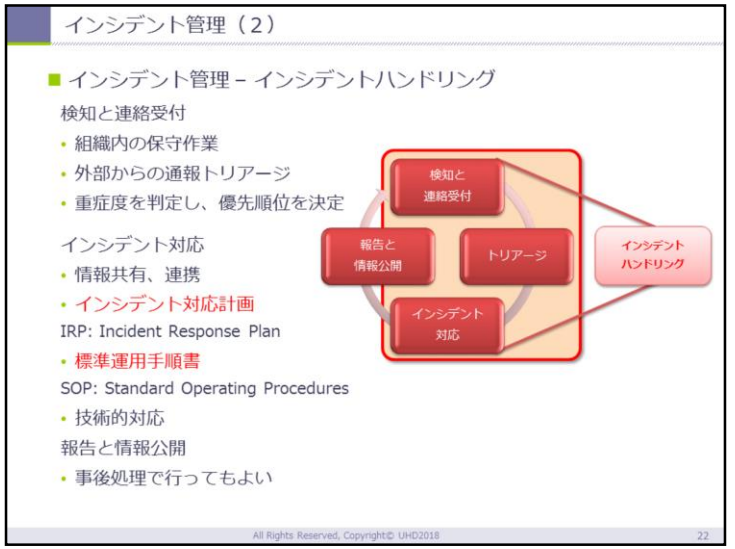
[インフラ準備]

・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。

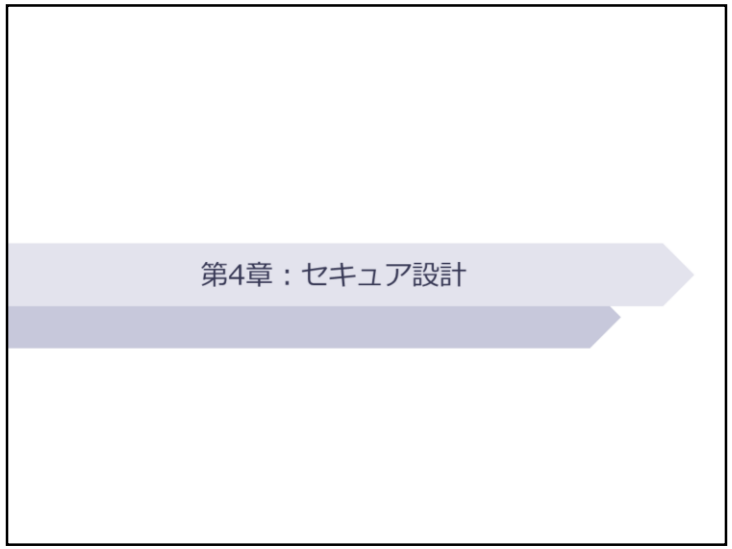
トリアージ後に、IRTが対応すべきと判断された場合は、インシデントレスポンスのフェーズに移行します。発生した情報セキュリティインシデントの事象分析を行い、技術的に対応が可能か否かを判定し、IRT内で技術的に対応可能な場合には、組織のIT関連部署と連携し、インシデント対応計画を策定し、実施します。また、発生した情報セキュリティインシデントが、IRTでは技術的に対応が困難な場合は、組織の幹部や経営陣と連携して対応計画を練る必要があります。そこで策定されたインシデント対応計画に従い、インシデント対応ポリシーに基づいた技術的な対応手順、手法、チェックリスト、フォームなどで構成された標準運用手順書を作成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

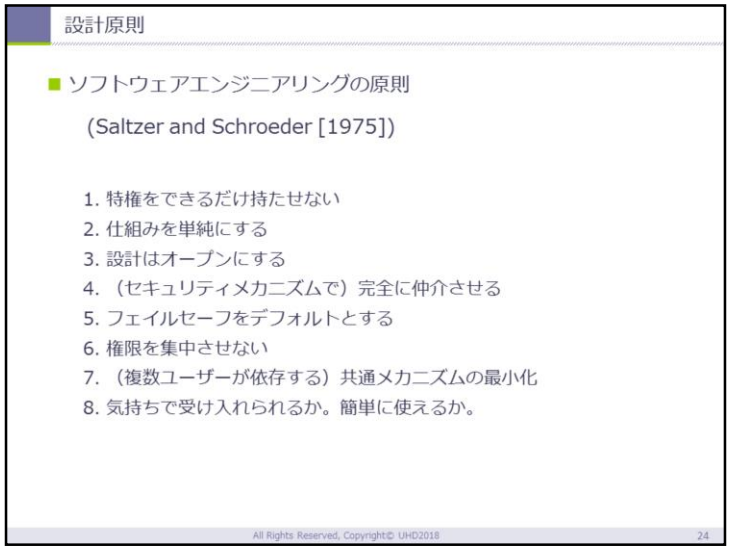
インシデント収束後には、再発防止を目的とした事後処理を行います。インシデントの原因究明を行い、情報収集し、脆弱性の対応をとります。また、事後レポートを作成し、情報公開を行います。レポート作成には、

・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

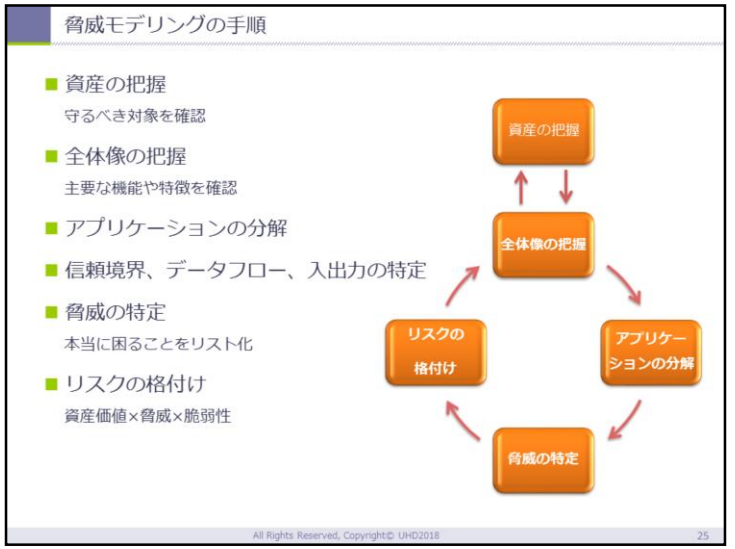
セキュリティレビューは、セキュリティ対策漏れを早くに見つけ出し、設計者へフィードバックすることを目的に行います。

●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。



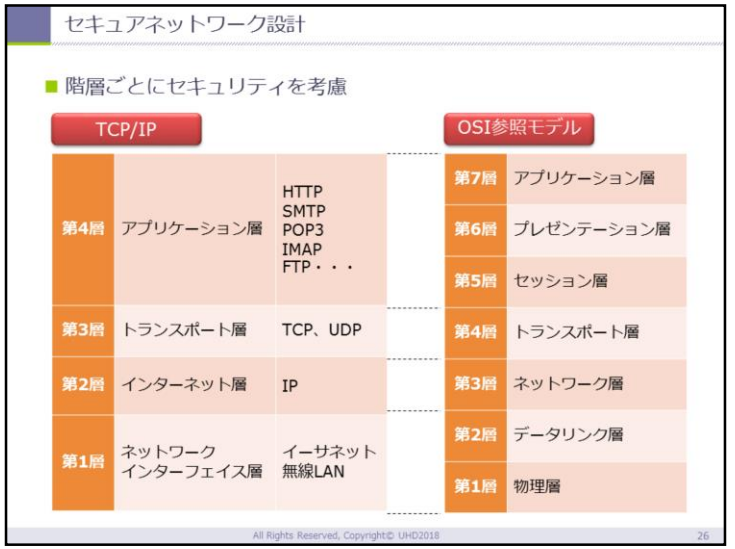
脅威モデリングは、情報資産、脅威、脆弱性を特定し、リスクを洗い出す作業をアプリケーションに対して行う作業です。設計段階で脅威モデリングを行うことで、実装段階に入ってからの手戻りを最小限にとどめることができます。これはセキュリティの向上だけではなく、コスト削減や開発期間の短縮にもつながる作業となります。1999年にマイクロソフトが提唱した STRIDE & DREAD 脅威モデリングは、OWASPおよびIPAでも採用されている脅威モデリングです。その効果は実地で検証されています。

～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

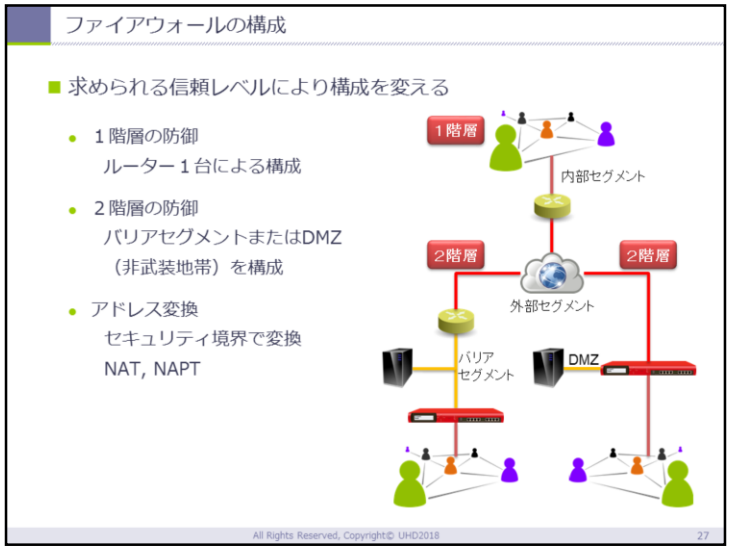
グと無線での電波の双方での接続セキュリティを考慮する必要があります。ケーブリングでは、セキュリティ対策の目的で光ファイバを用いることがあります。通信の傍受が困難で、かつ、傍受の検知が容易であるということから、短距離でも組織内の基幹通信で光ファイバーを用いるケースがあります。また、一般にルーターは、第3層の装置として認識されていますが、ルーティング時にMACアドレスを変換する働きがあります。ですから、ルーターにキャッシュされているMACアドレスがARPスプーフィングで汚染されている場合、ルーティング先が意図しないホストになる場合があります。その他、暗号化などの技術も通信経路のセキュリティとして考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

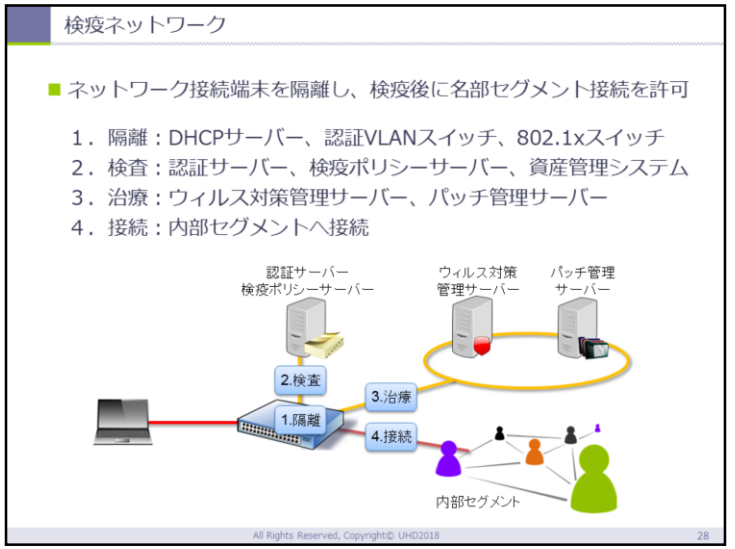
インターネット層・トランスポート層での主なセキュリティ対策としてパケット・フィルタリングが知られています。パケットフィルタリングには、静的パケット・フィルタリング、動的パケット・フィルタリング、ステートフル・インスペクションなどがあります。静的パケット・フィルタリングは、ルーター上のファイアウォールとして一般的に搭載されています。過去に通過したパケットから通信セッションを認識して、受け付けたパケットを通信セッションの状態に照らし合わせて通過させるか、遮断させるかを判断するという、ステートフル・インスペクションは、動的パケット・フィルタリングのひとつとして考えると分かりやすいかもしれません。

[アプリケーション層]

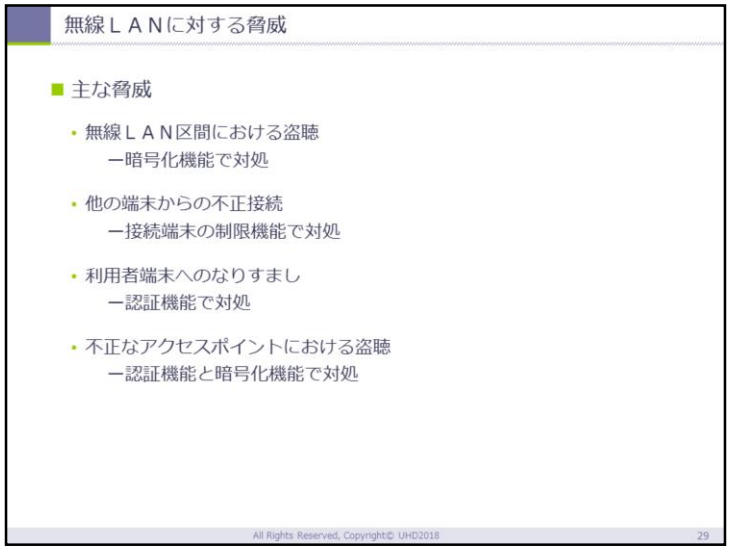
アプリケーション層では、IDS（侵入検知システム）/IPS（侵入防御システム）、アプリケーションゲートウェイ、WAF（Webアプリケーションファイアウォール）といったセキュリティ対策がとられます。IDS/IPSは、シグニチャーベースで、難読化処理された攻撃に弱い、アプリケーションゲートウェイは、アプリケーション層の情報でフィルタリング、WAFは、通信を一度解除してから解析で難読化処理にも対応といったように、それぞれの対策にメリット・デメリットがみられます。



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。



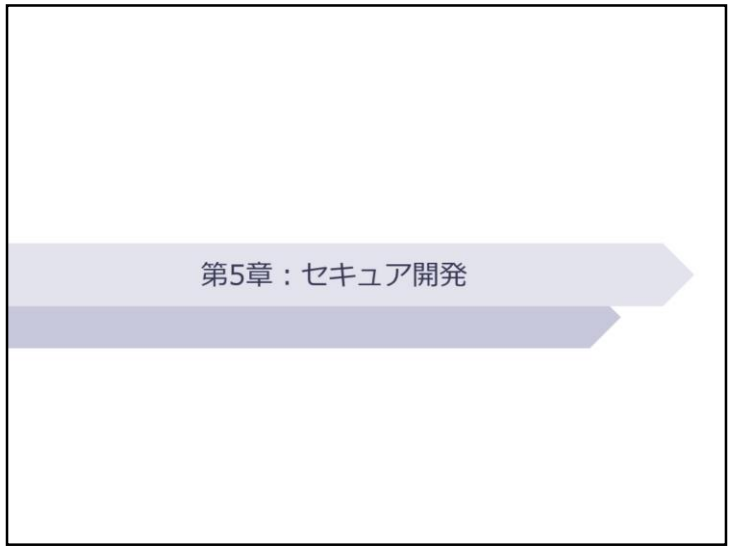
無線LANの脆弱性はよく話題に上りますが、何が脅威で、何がその脅威に対する脆弱性で、何を対策すべきかをしっかり検討していないケースが多く存在します。ほんのわずかなポイントを抑えるだけでも、無線LANは暗号化されていない有線LANよりも安全な通信方式です。まずは、傍受と盗聴は違うということを認識しましょう。例えば、警察無線を傍受しただけで捕まることはありません。傍受した内容に対し、何らかのアクション（例：通信内容の記録、通信内容の）をとった場合に電波法違反が問われることがあります。そもそも適切に通信が暗号化されており、認証が設定されていれば、盗聴には失敗します。あくまでも「盗聴を防ぐ」という観点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

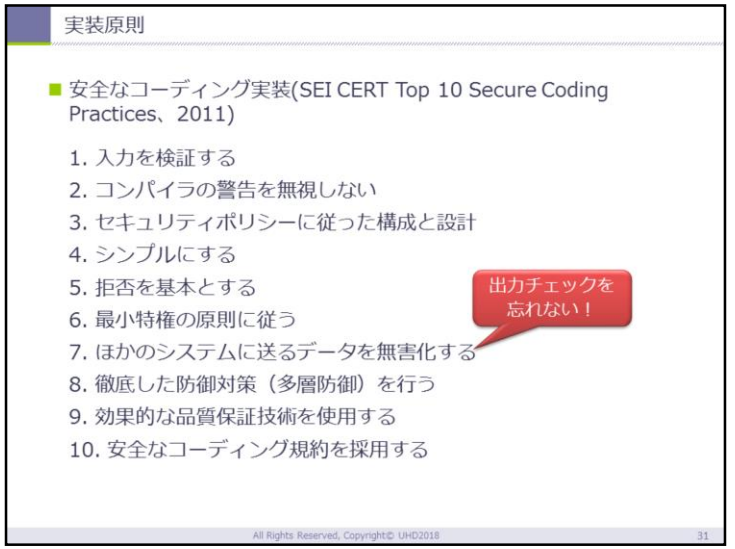
主な無線LANセキュリティ技術には、次のようなものがあります。

●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

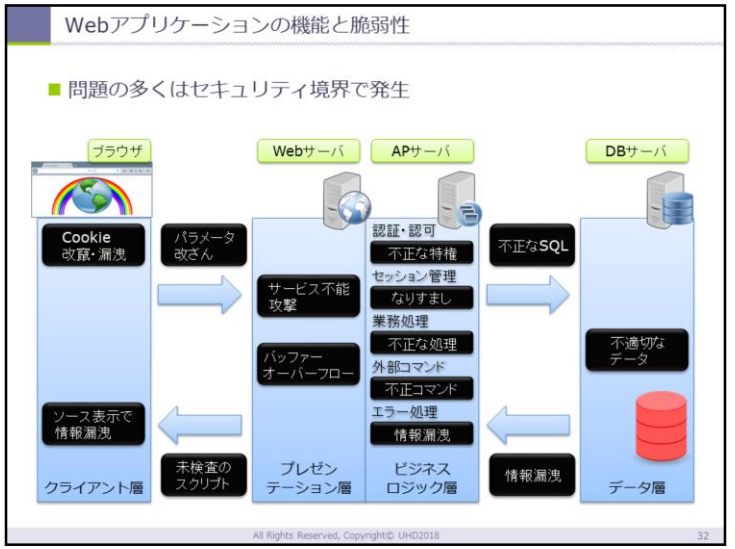
りとしても全てを失ってしまうのではなく、被害がある程度限定できるようにする。

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

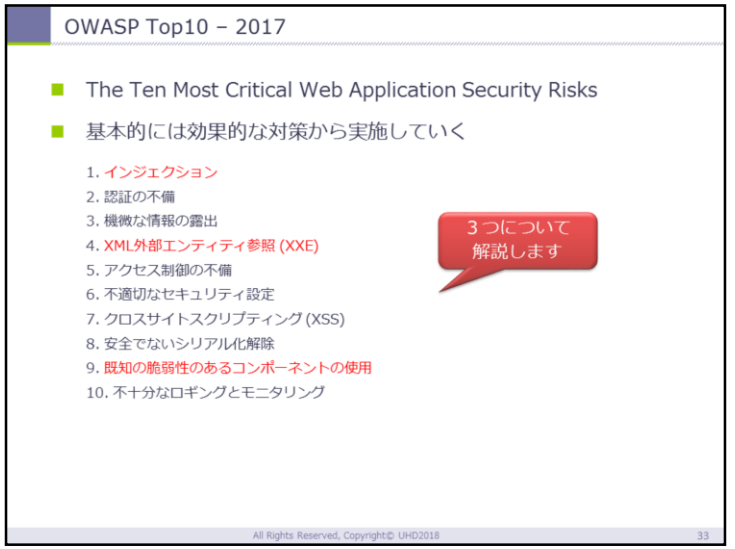
効果的な品質保証テクニックを使う。優れた品質保証技術は、脆弱性を特定し、排除するのにも有効である。

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。

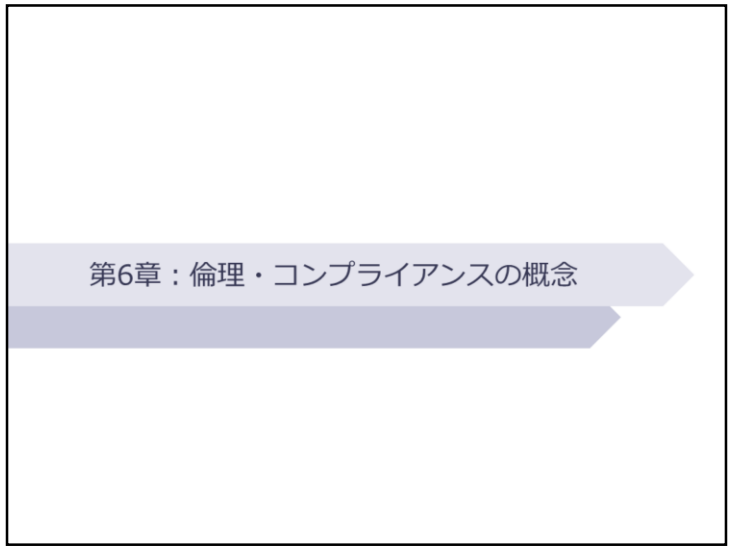
●クライアント側とサーバー側で、使用コンポーネントと関連コンポーネントのバージョンを継続的に管理する。

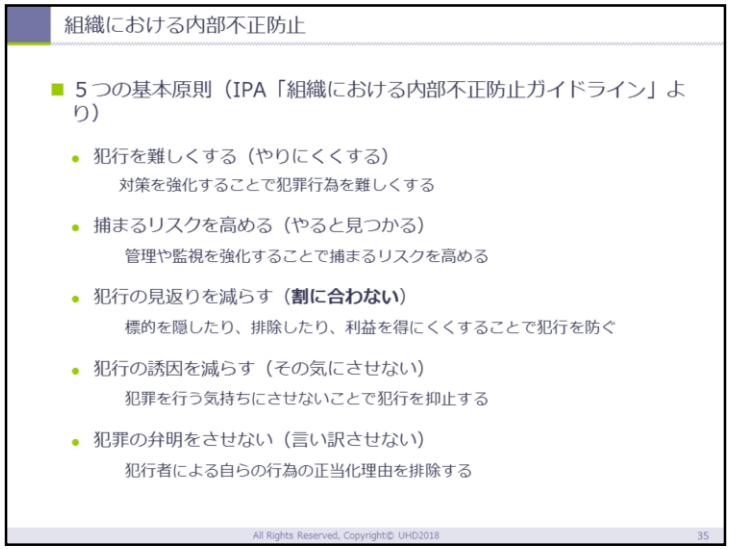
●安全な接続を介し、公式リソースからコンポーネントを入手する。

●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。

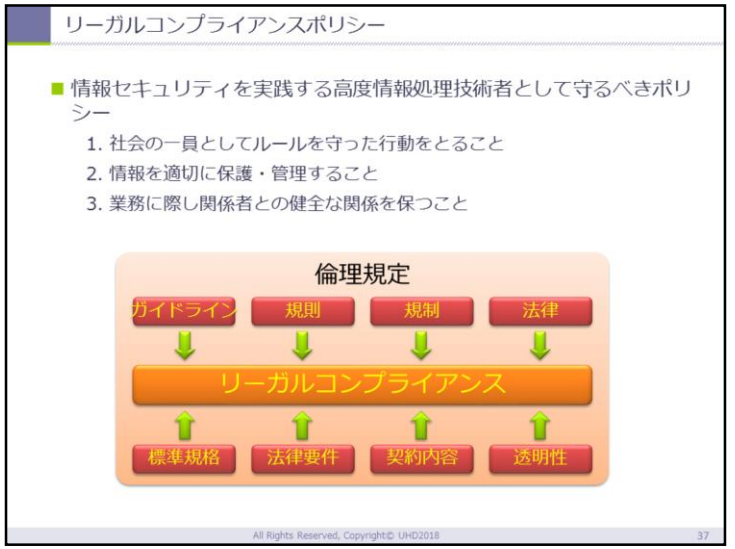
4. 専門的、業務上知り得た情報の機密性を、法的または専門的な権利または開示義務が無いかぎり、厳守しなければならない。

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

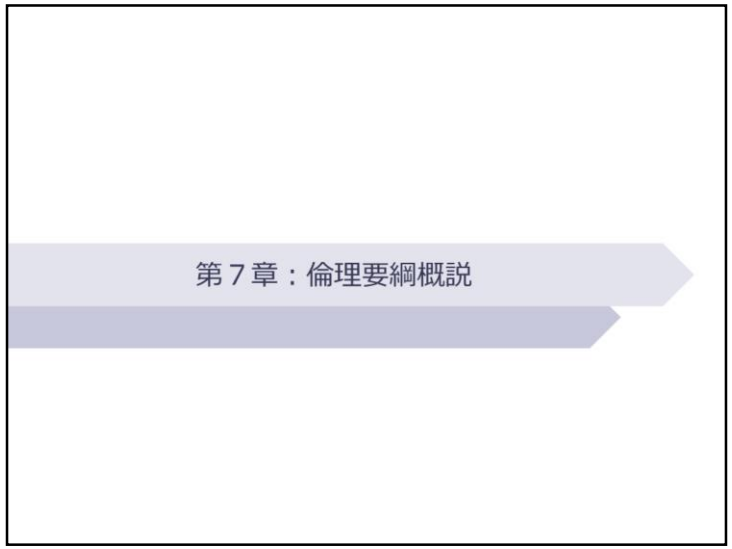
●個人情報の保護規定を厳正に遵守すること

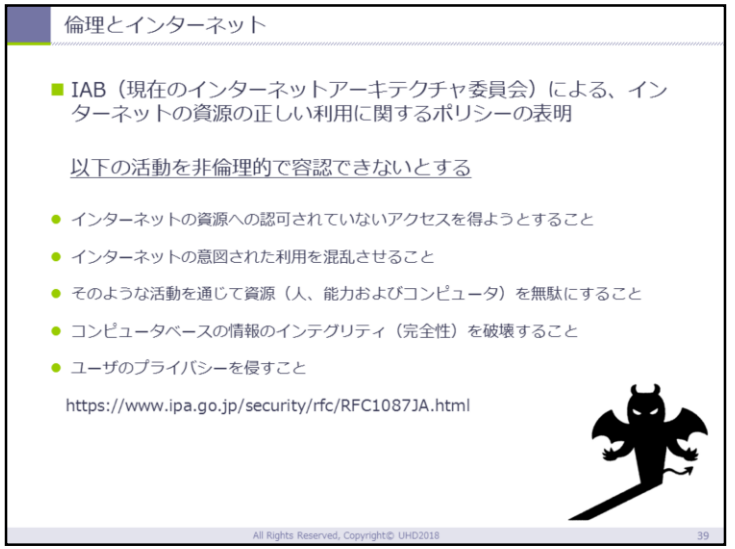
3. 関係者との健全な関係を保つ

●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

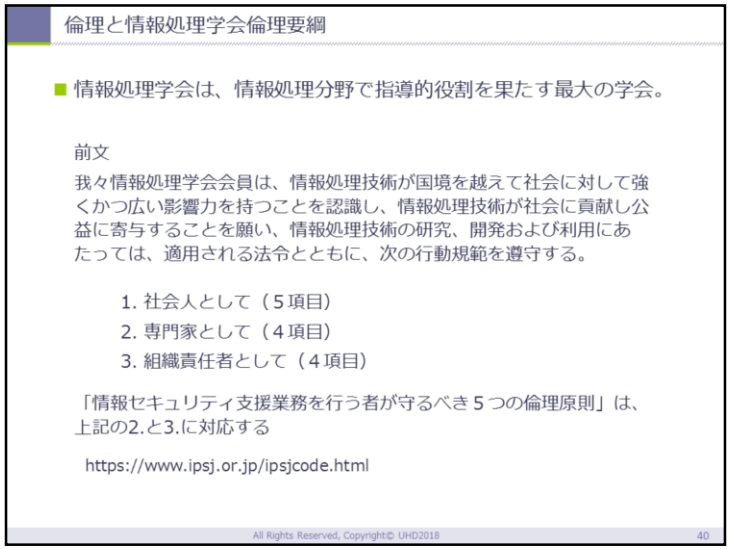

第７章：倫理要綱概説



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。