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

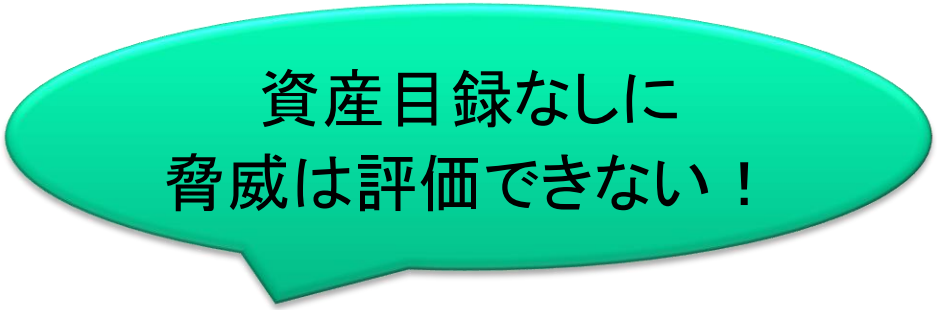
情報セキュリティ10大脅威

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

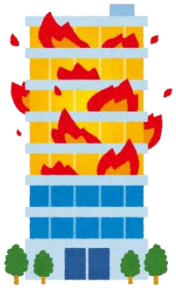
情報資産

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

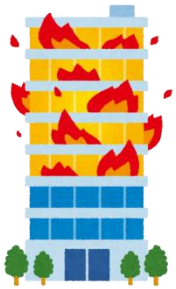
人的

物理的

規則
と
教育

脅威

誤操作
詐欺
機密漏洩

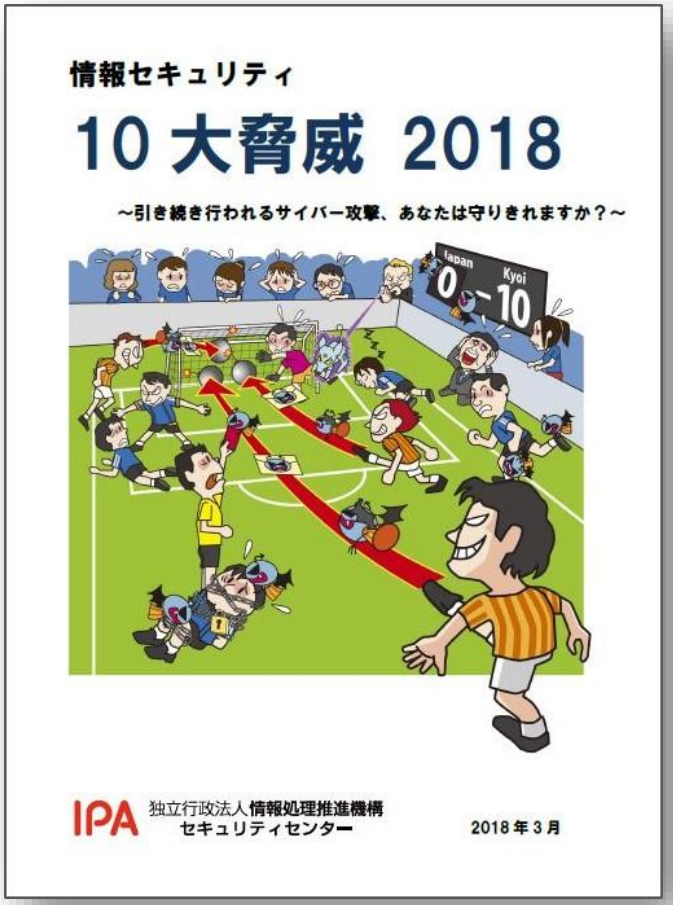


不法侵入、盗聴器、
火災、洪水、地震、
テロリストの襲撃

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

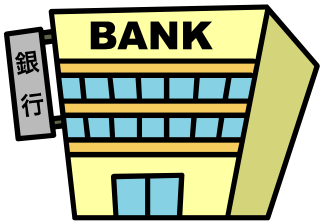
- メールによるウイルス感染等により組織内部に侵入
- 組織の機密情報が流出
- 取引先や関連会社を踏み台にして本丸を狙うことも

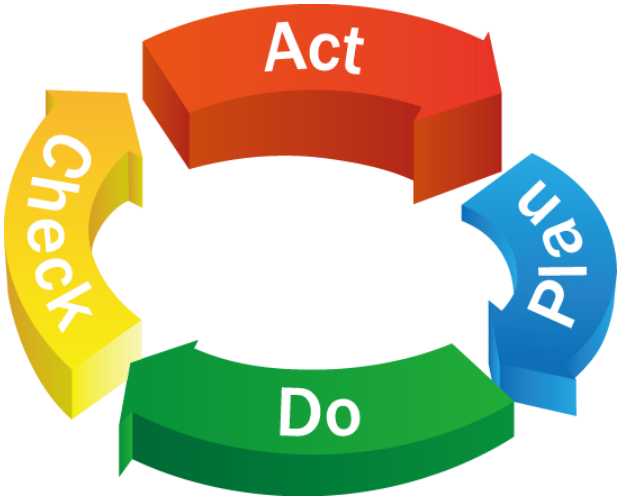
手口

- 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～

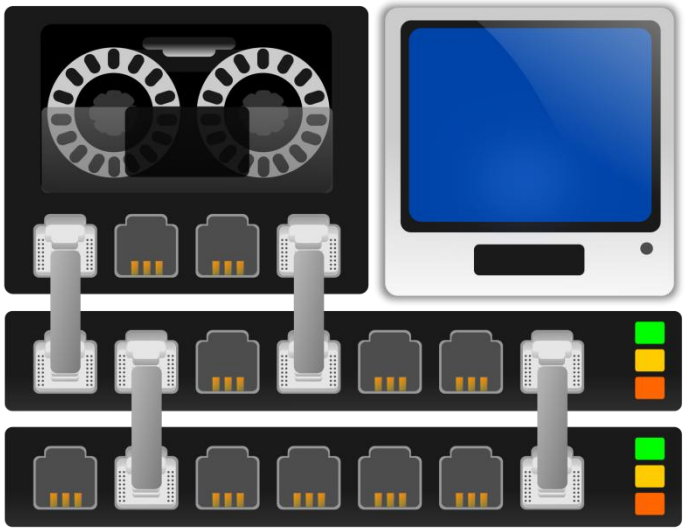
– 組織としての対応体制の確立
  - 問題に迅速に対応できる体制(CSIRT)の構築
  - 対策予算の確保と継続的な対策実施

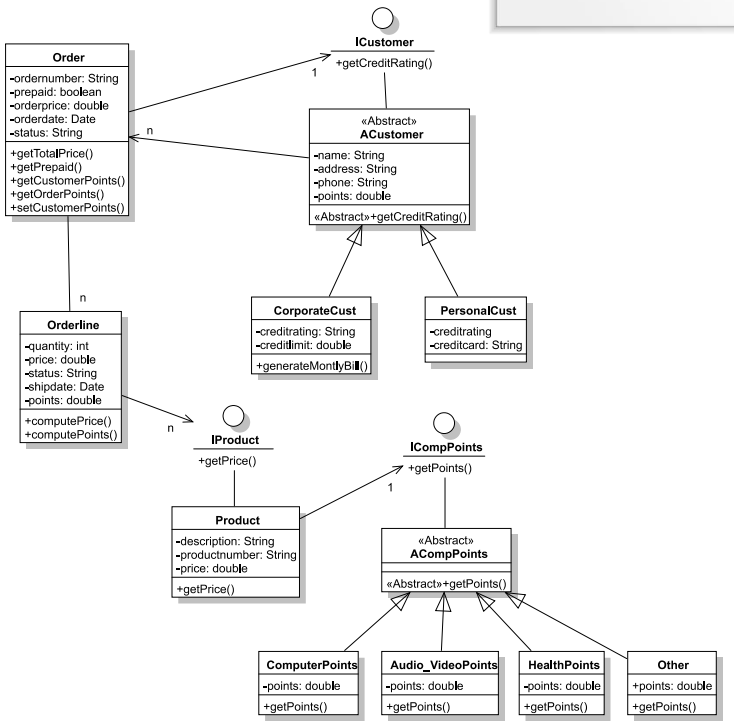




標的型攻撃の対策～システム管理者～

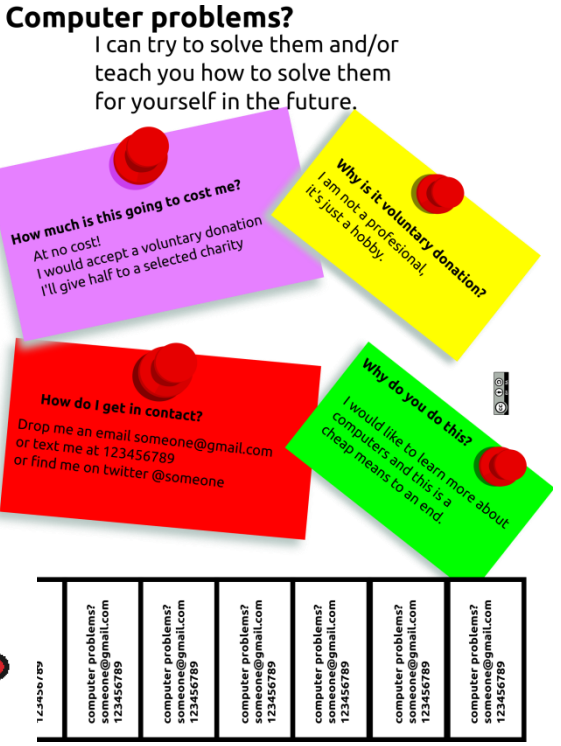
- 被害の予防
  - 被害を抑止するためのシステム設計
  - アクセス制御・データの暗号化
- 被害の早期検知・事後対策
  - ネットワーク監視・分離

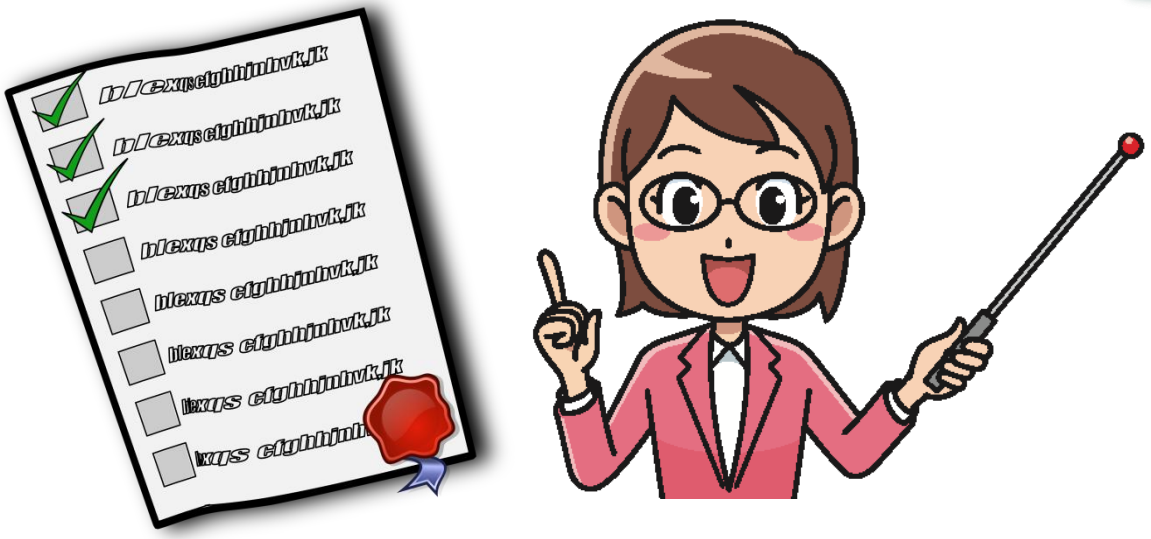




標的型攻撃の対策～セキュリティ担当部署～

- 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

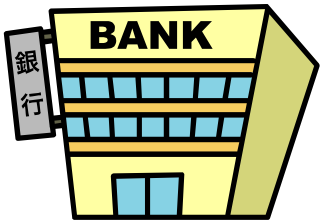
- PC内のファイルの暗号化や、スマートフォンの画面のロックを行い、復元に身代金を要求
- 2016年はランサムウェアの被害が急増している

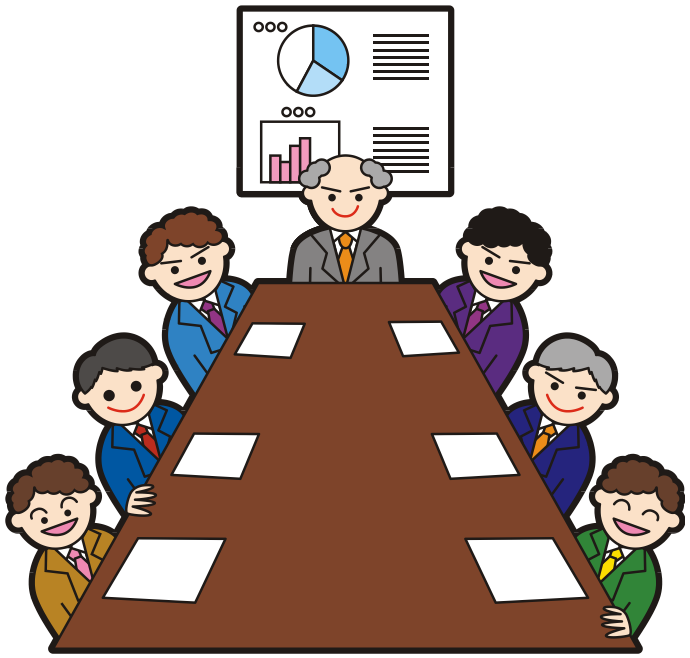
手口/影響

- 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

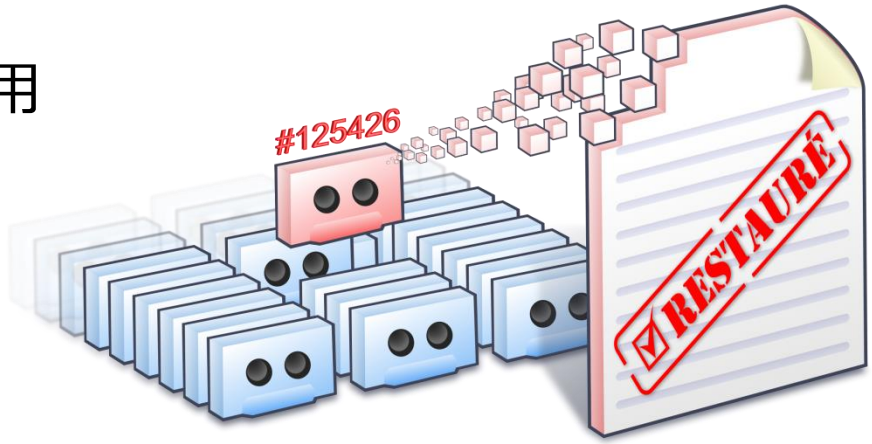




ランサムウェアの対策～管理者と利用者～

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

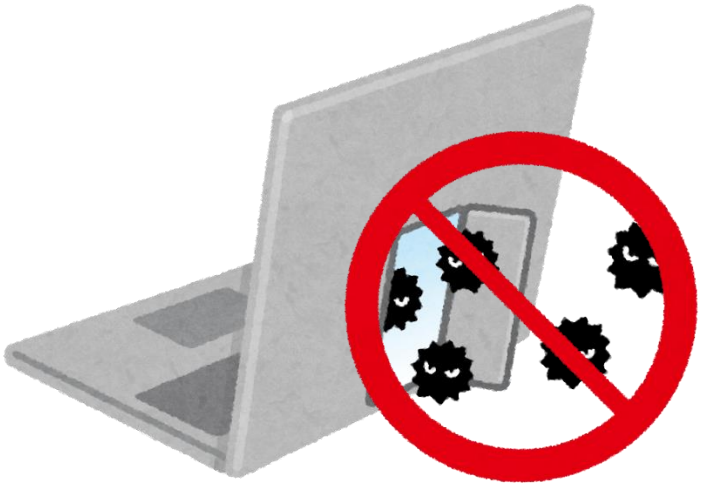
- IoT機器の脆弱性が悪用され、ウイルス感染や不正利用される
- 不正利用されたIoT機器がボット化し、DDoS攻撃等に悪用されるケースも

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

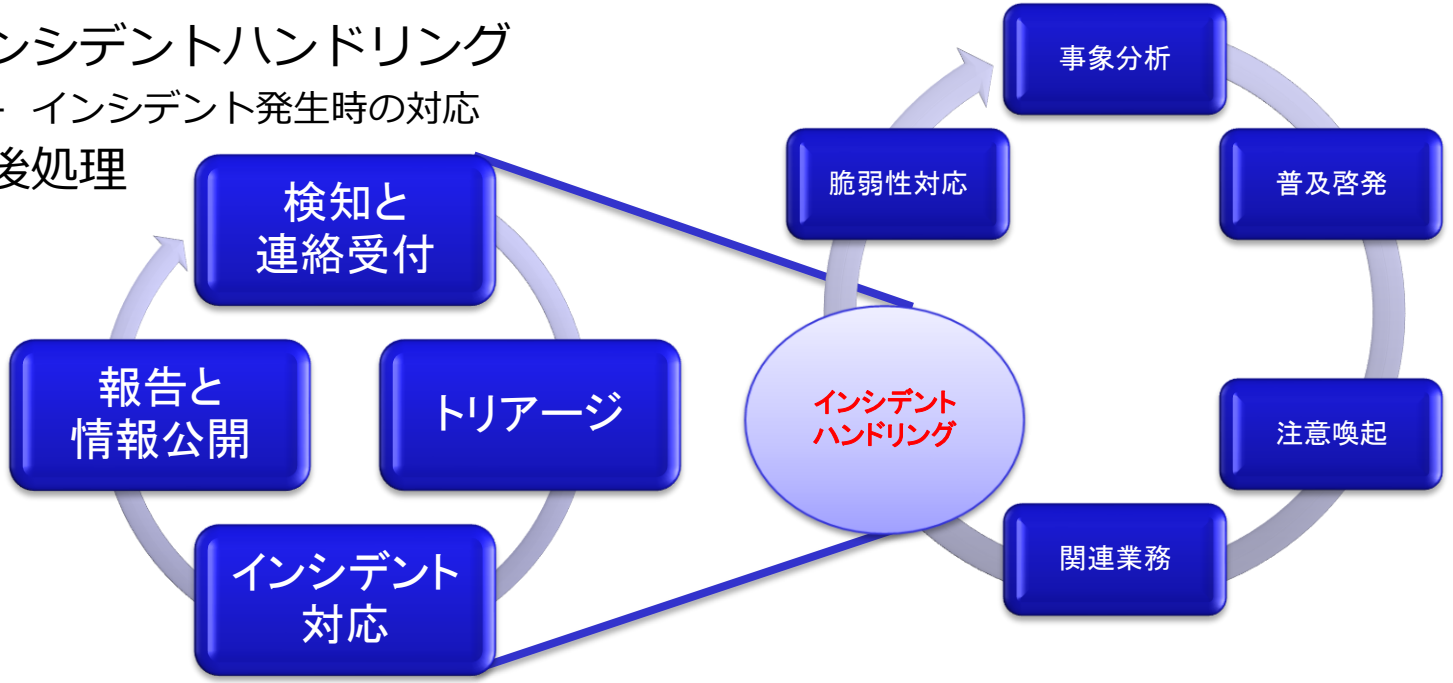
- インシデント対応（IR: incident response）
  - 差し迫ったハザードの原因を食い止めるため，及び不安定又は中断・阻害を引き起こす可能性のある事象の結果を軽減し，正常な状況に復旧するために講じる処置。

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

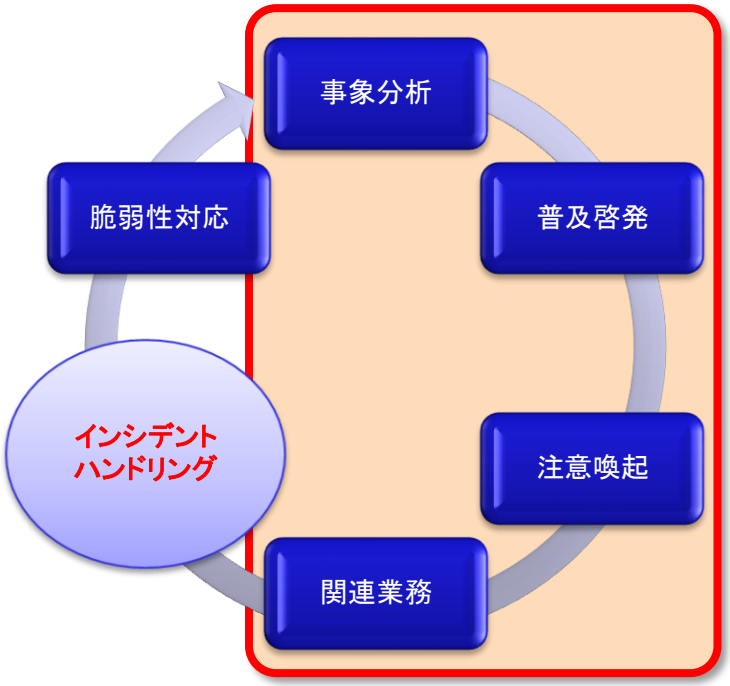


- インシデント対応チーム（IRT: Incident Response Team）
  - 別名シーサート (CSIRT: Computer Security IRT)
  - 情報セキュリティインシデントに対応する専門チーム
  - インシデント管理は、IRT/CSIRTを中心に実施

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

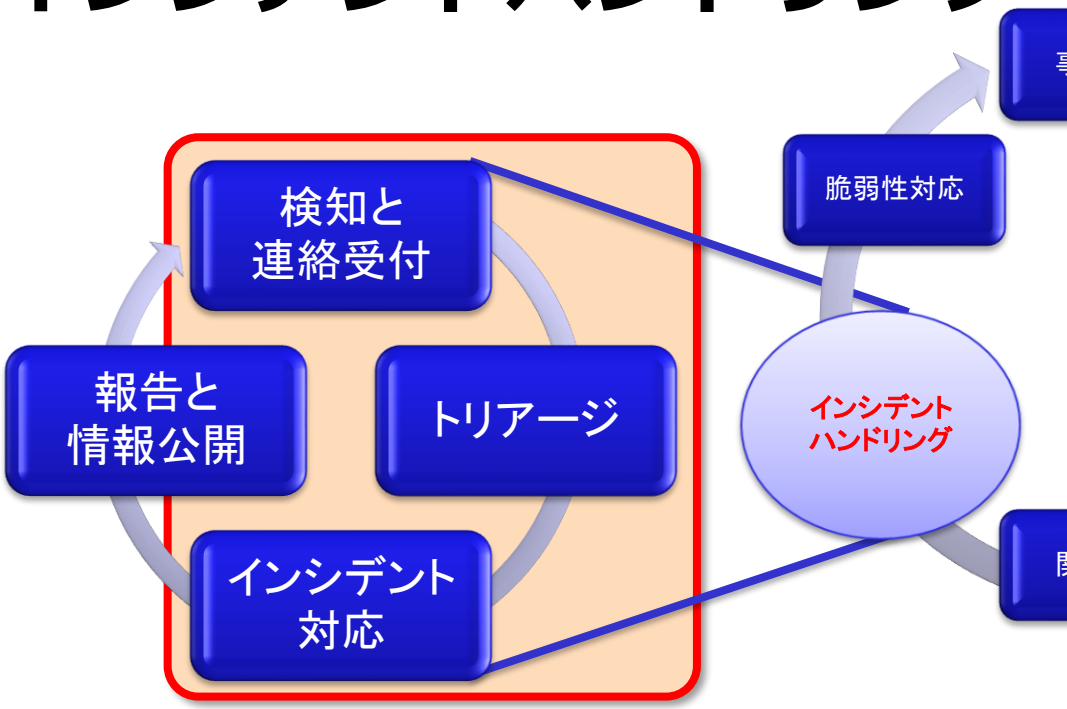
インシデント対応ポリシー

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

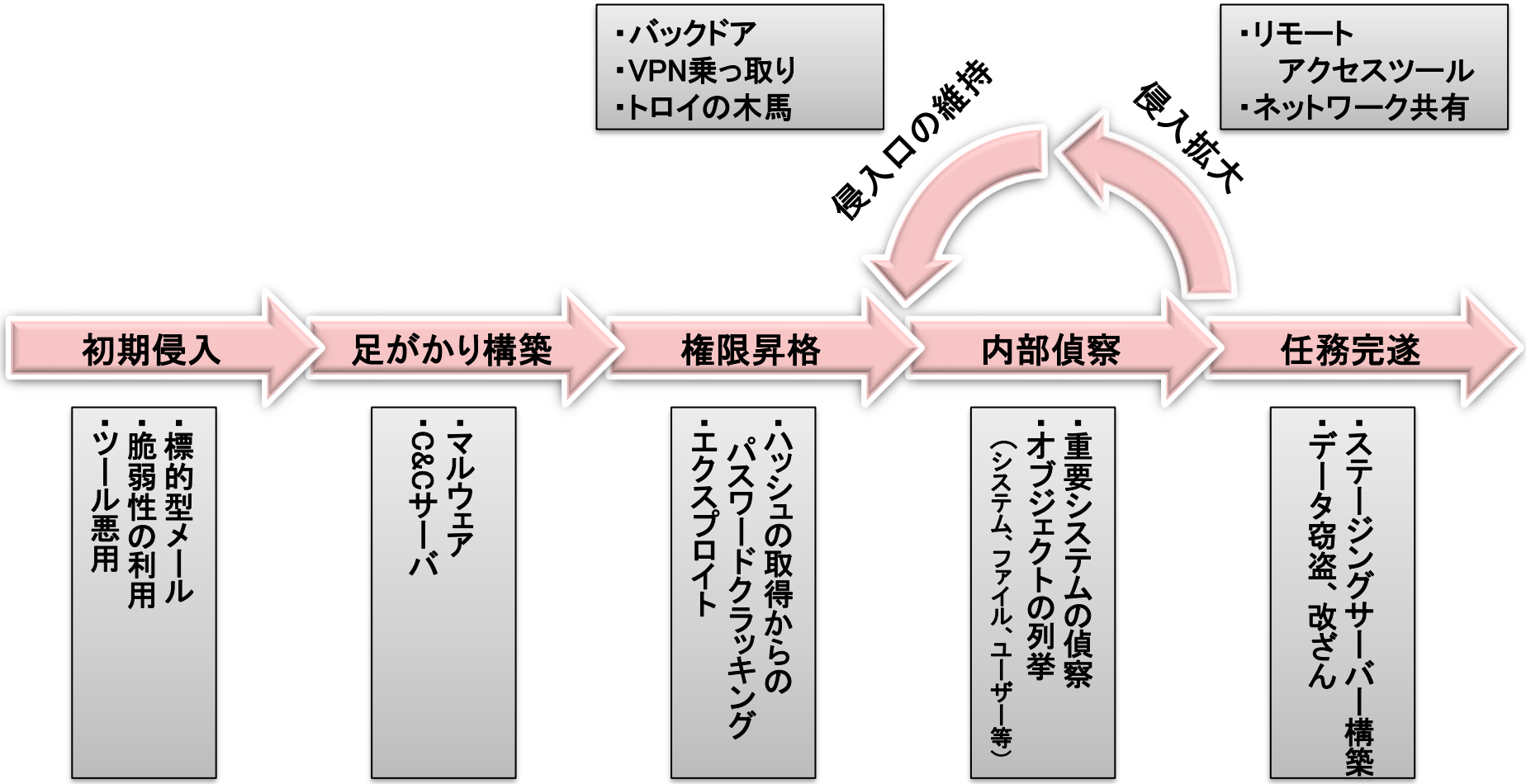
得られた情報から事実関係を確認し、IRT が対応すべきか否かを判定

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

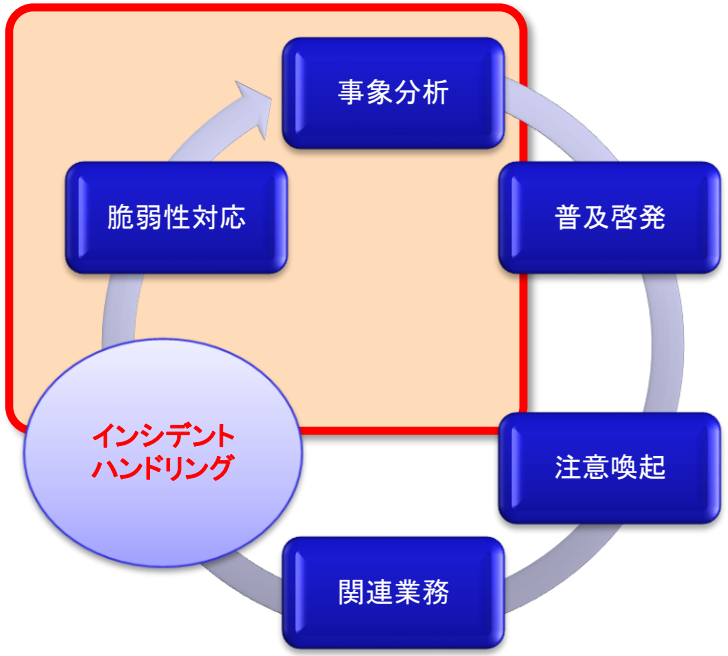
標準運用手順書

- 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

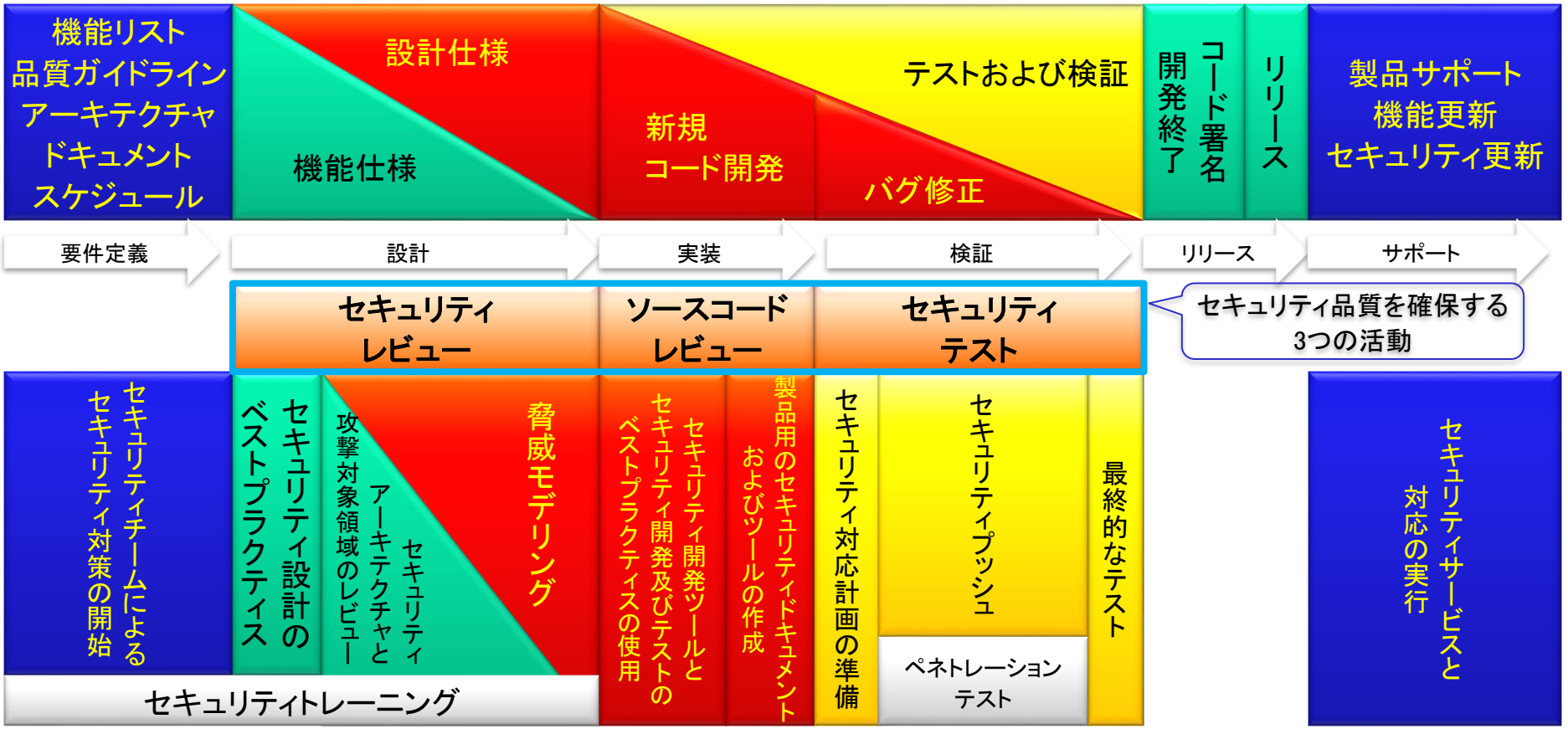
ソフトウェアエンジニアリングの原則 (Saltzer and Schroeder [1975])

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

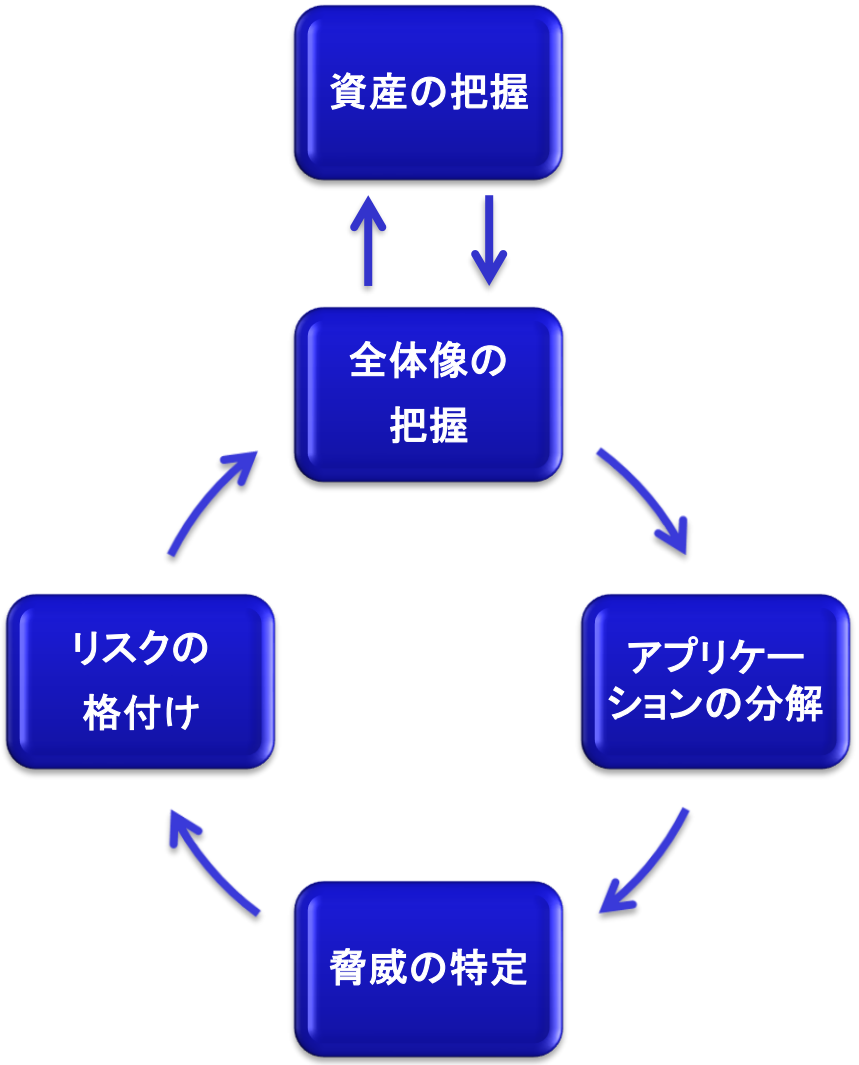
総論	セキュリティ開発ツールの検討
脆弱性回避策	セキュリティテストの検討
	脅威モデリングの検討
不測の事態対策	レースコンディション対策
	メモリリーク対策
プログラム配置	構成ファイルからの情報漏洩
	子プロセスからの侵害
	サンドボックス
データ漏洩対策	最小の特権、パーミッション
	一時ファイル
	コマンドライン
	親切すぎるエラーメッセージ
入力検査	ユーザー入力の検査
	受信ファイルの検査
	環境変数の検査
出力検査	データベース操作
	外部ライブラリ操作
	出力のエンコード・エスケープ

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



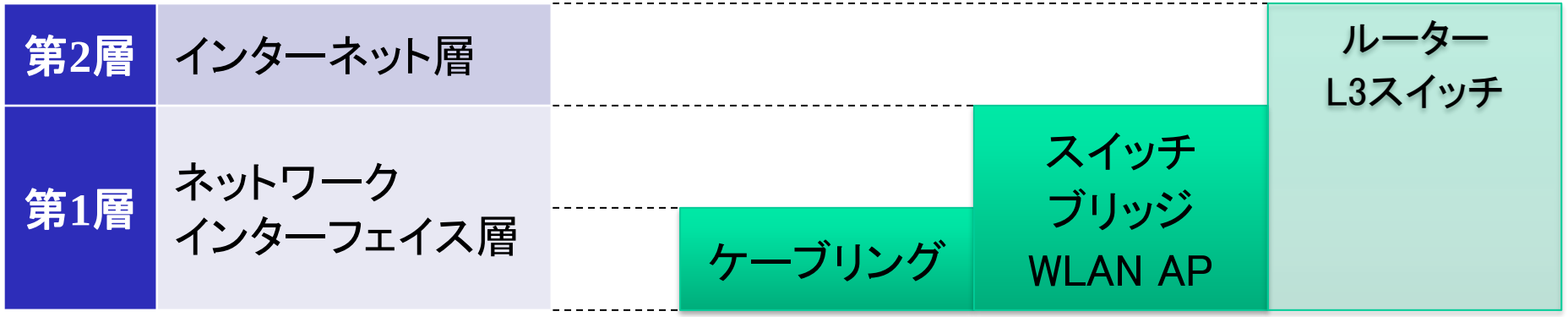
セキュアネットワーク設計

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

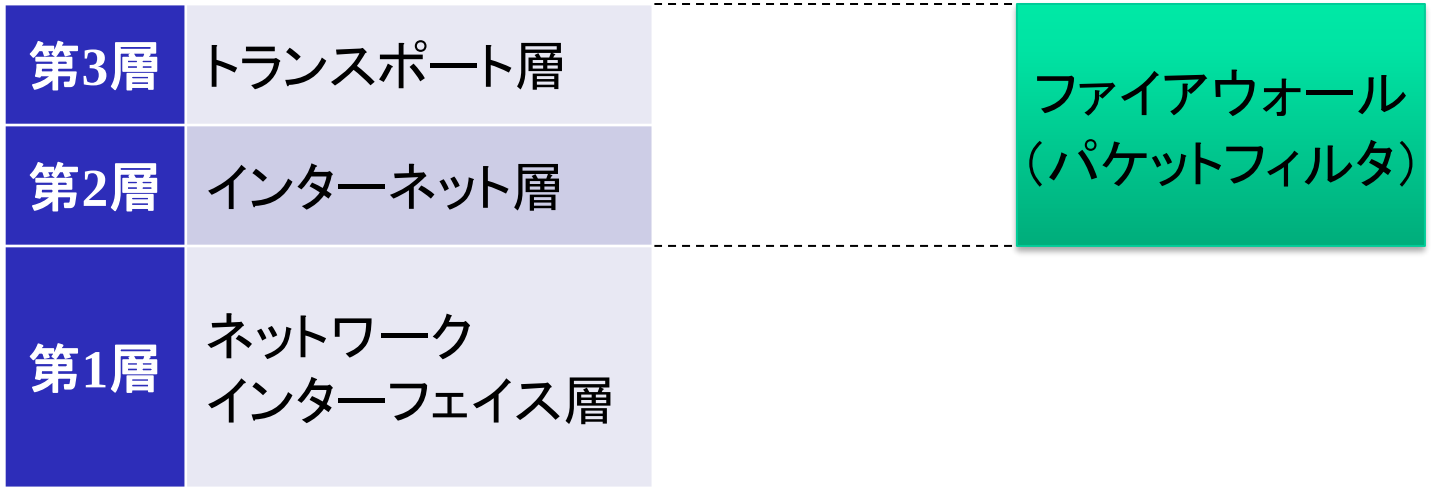
ネットワークインターフェイス層

- 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



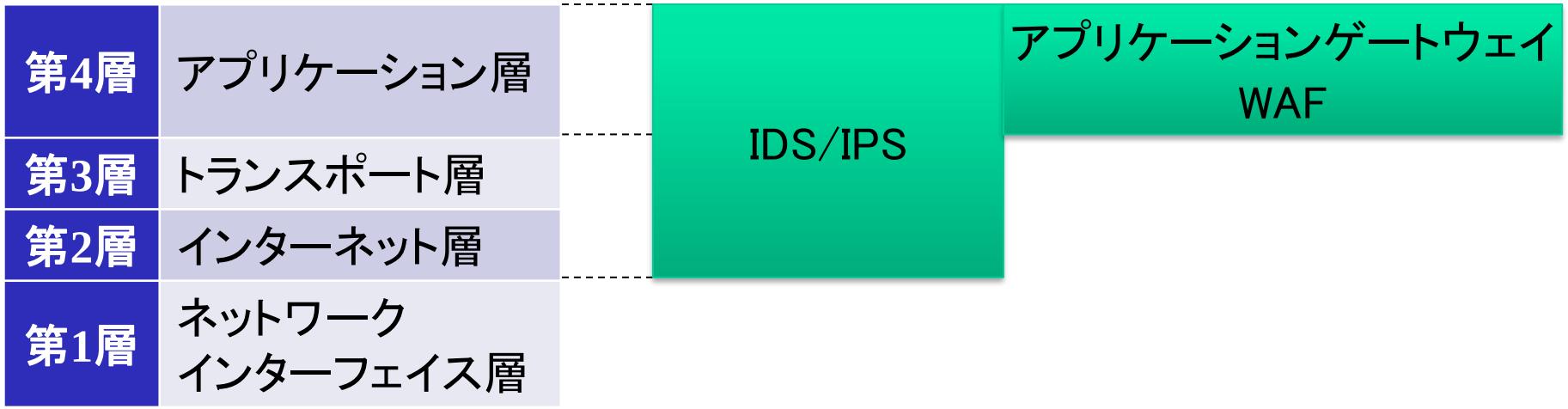
インターネット層とトランスポート層

- 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。

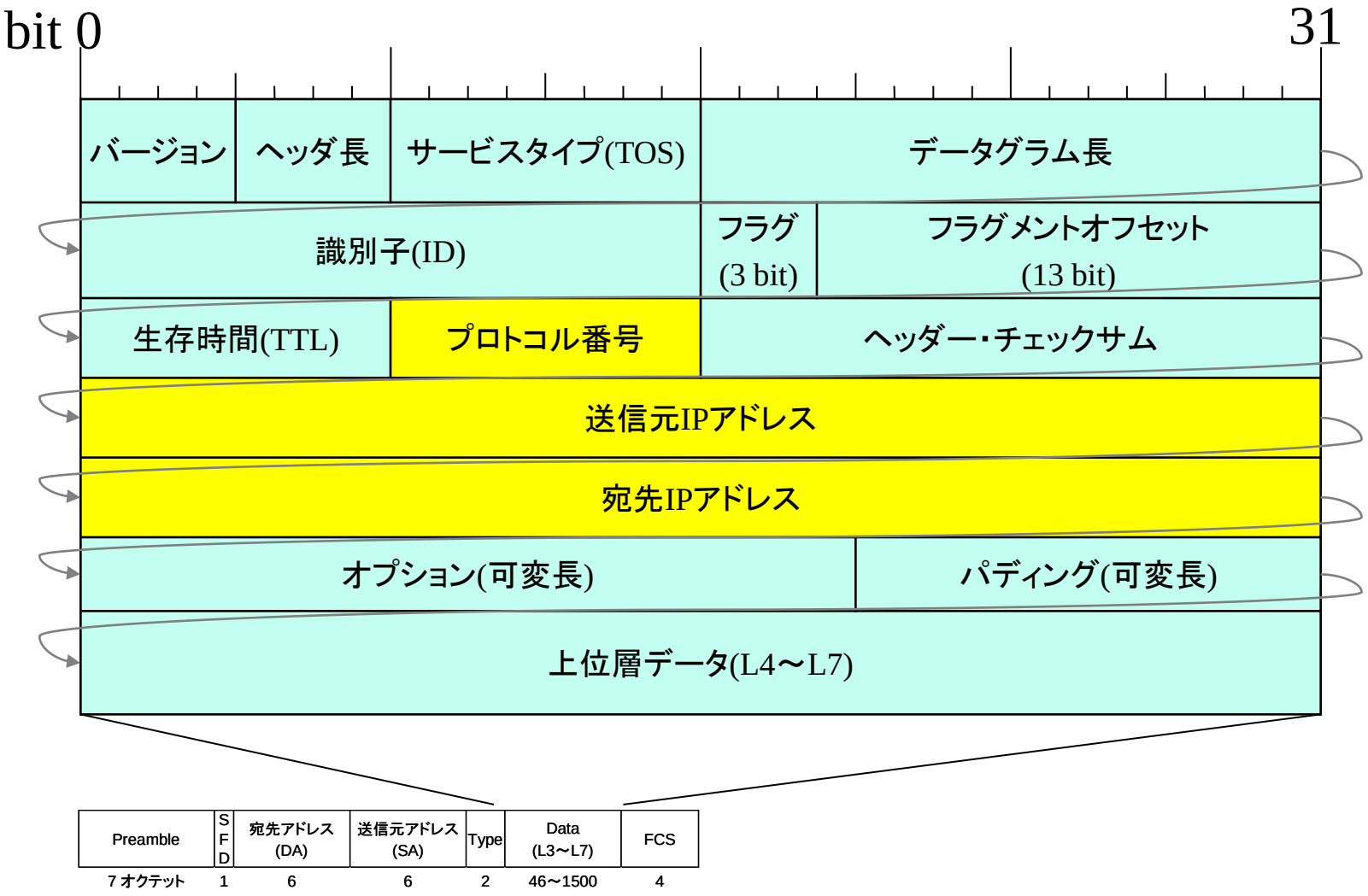


参考：Ethernet v2 フレーム形式

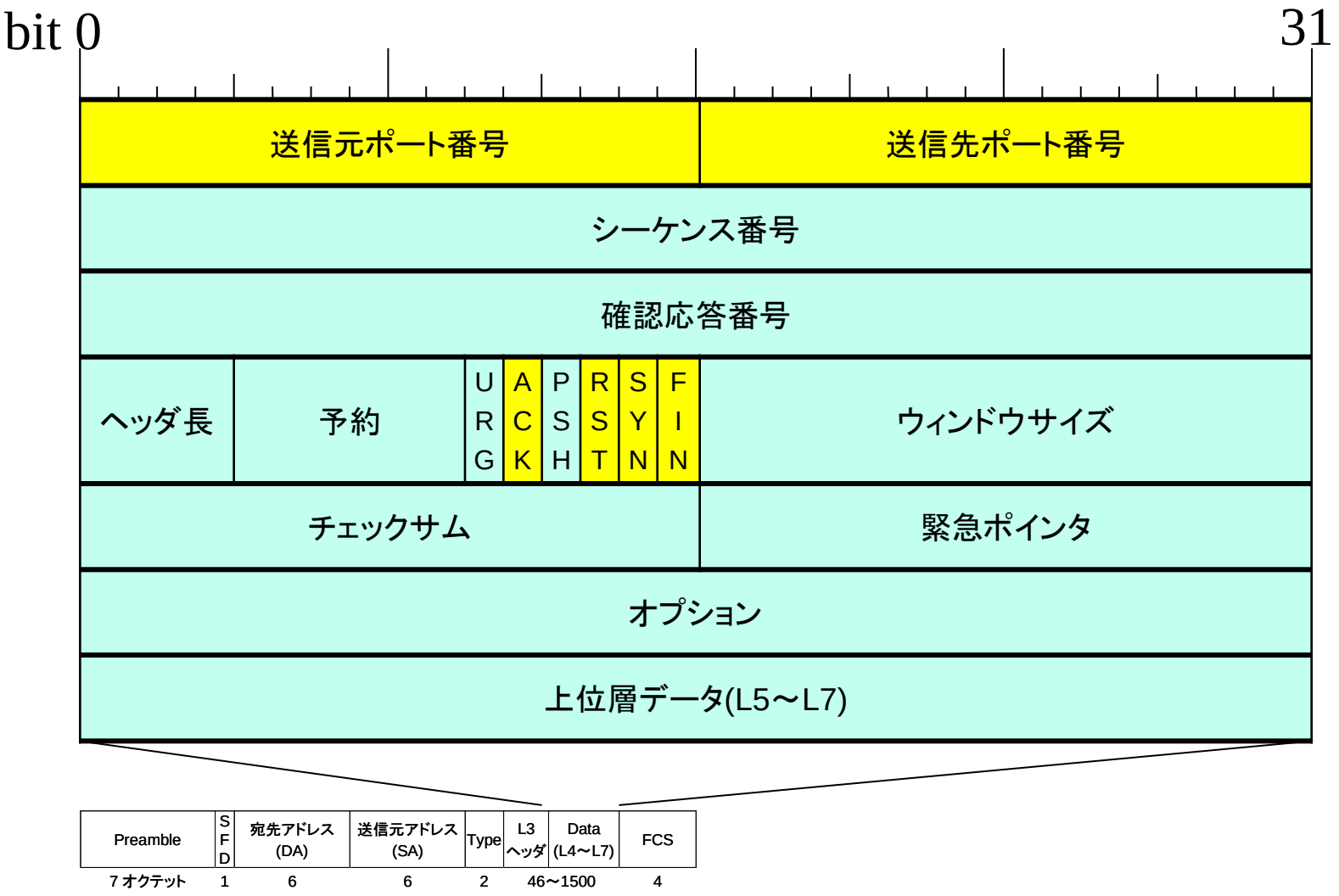
Preamble	SFD	宛先アドレス (DA)	送信元アドレス (SA)	Type	Data (L3～L7)	FCS
7 オクテット	1	6	6	2	46～1500	4

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。

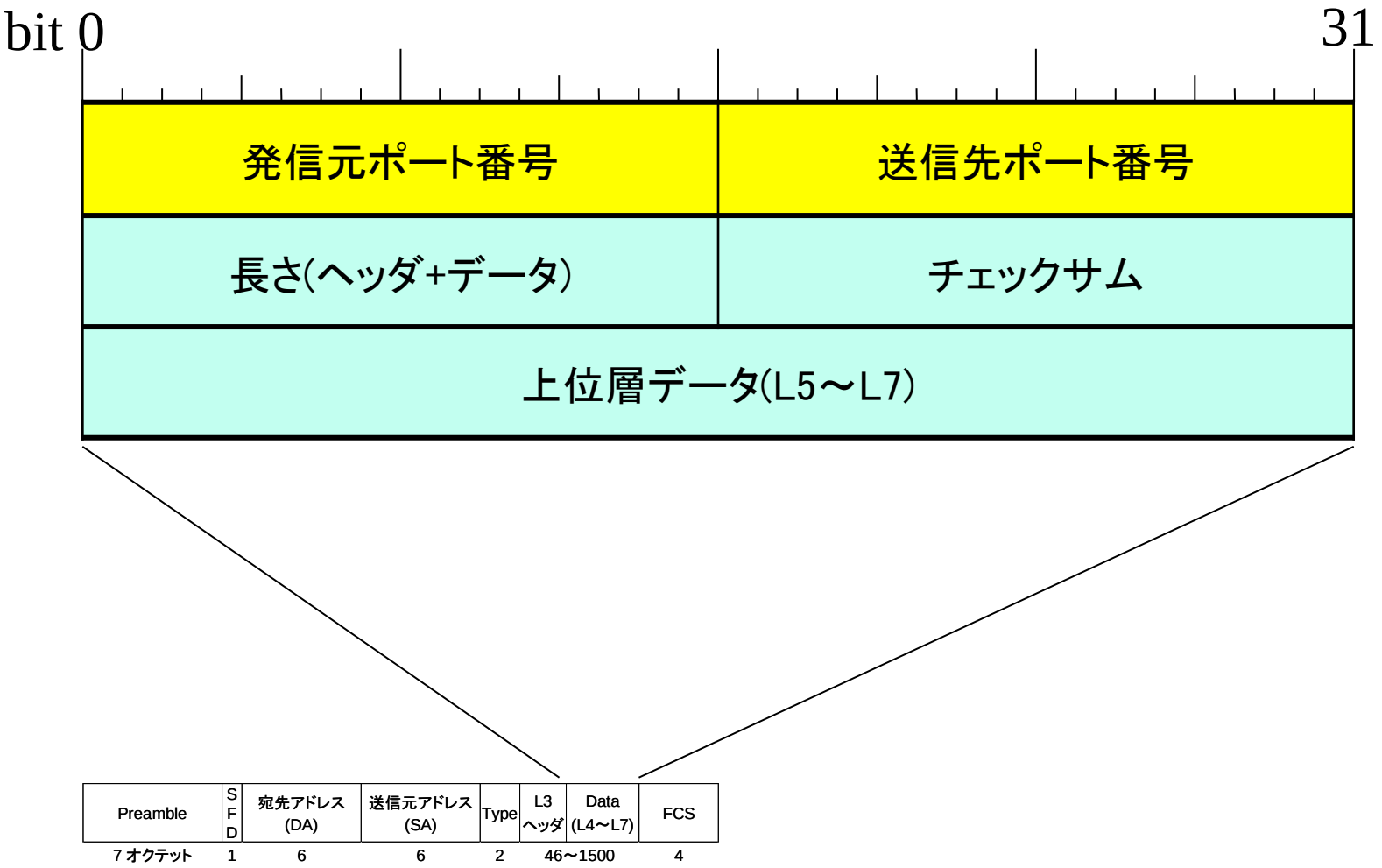
参考：IPパケット形式


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



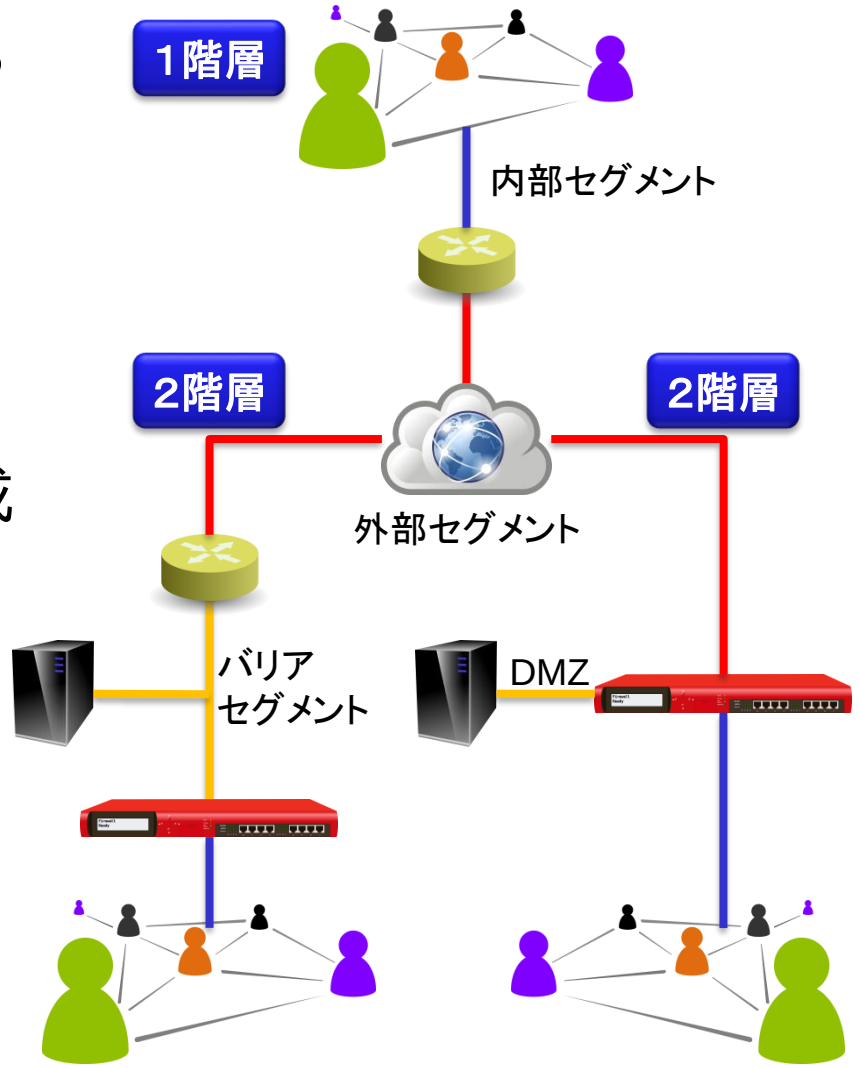
参考：UDPヘッダー形式



ファイアウォールの構成

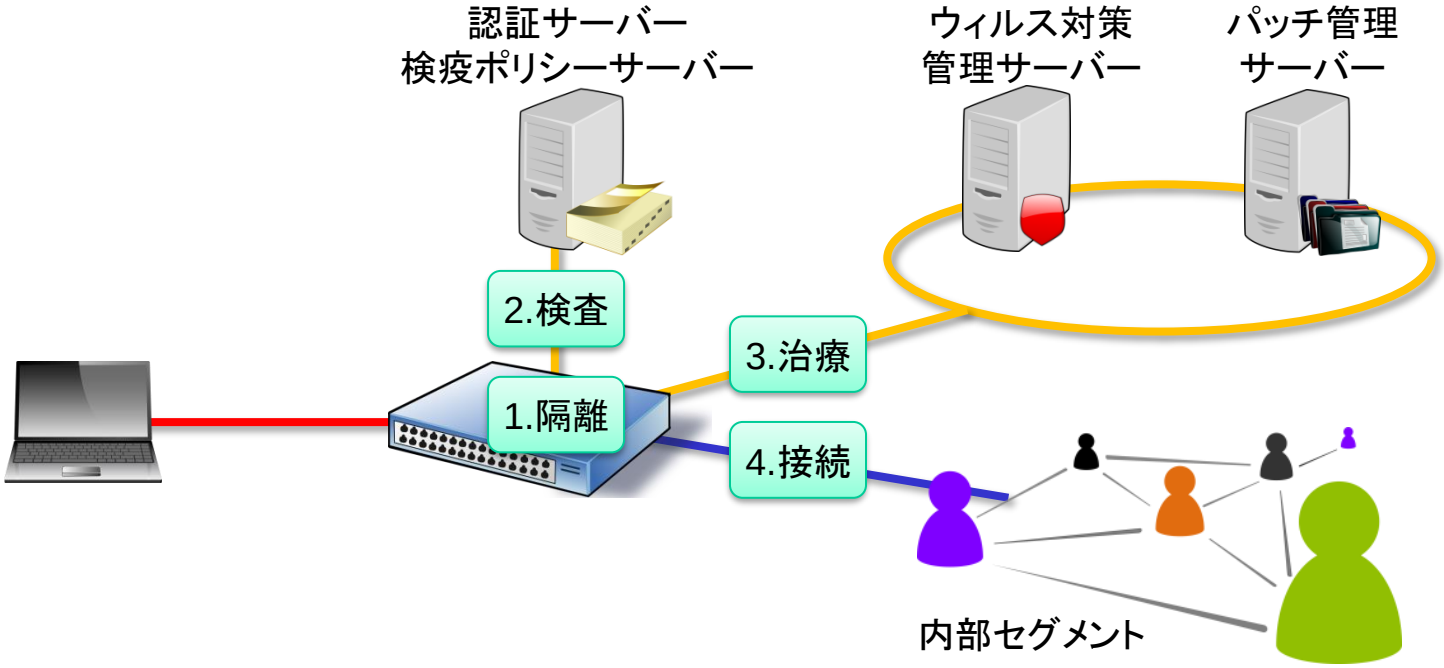
求められる信頼レベルにより構成を変える

- 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

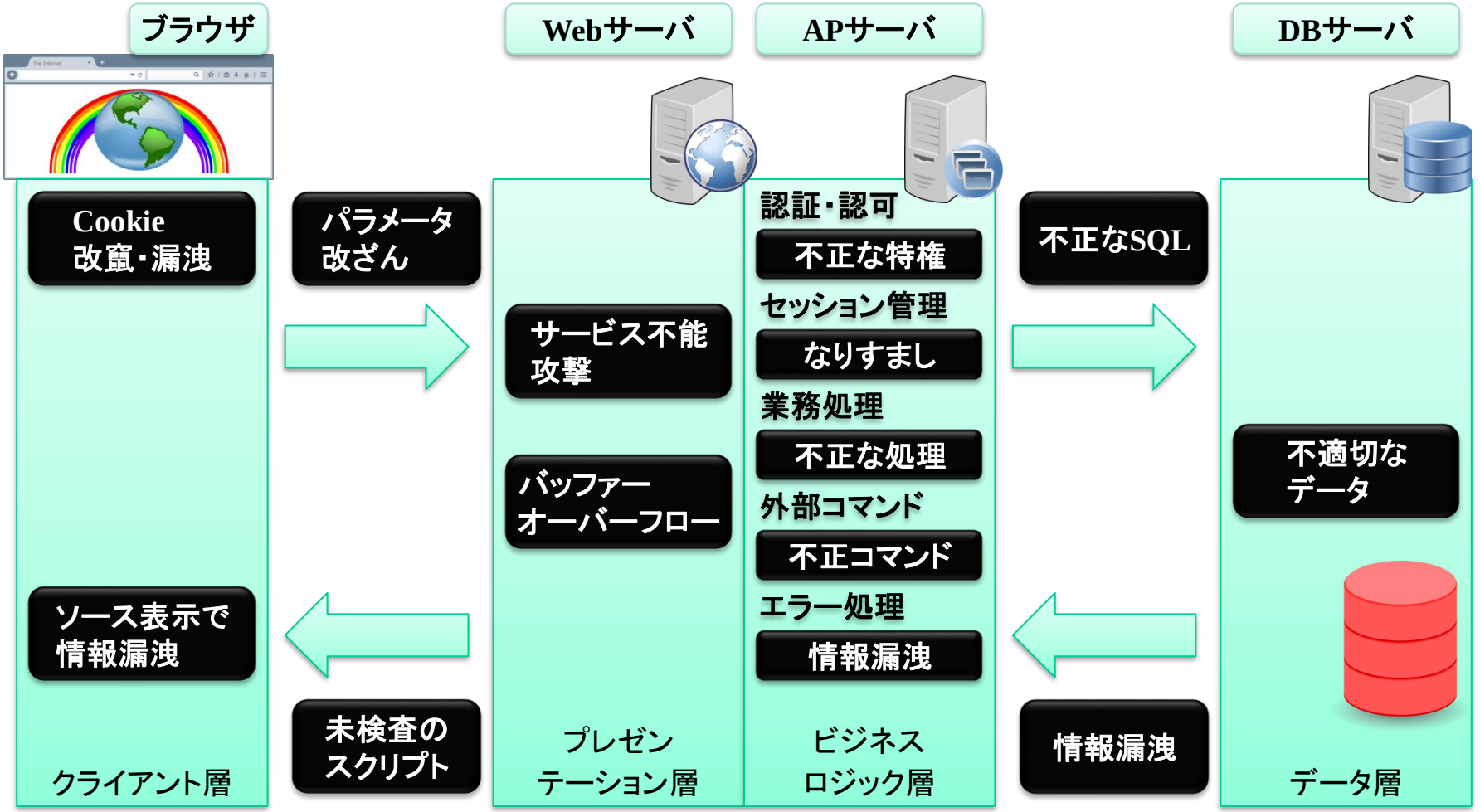
安全なコーディング実装 (SEI CERT Top 10 Secure Coding Practices、2011)

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