CBK#1 Access Control Systems & Methodology

CBK#2 Telecommunications and network Security

CBK#3 Security Management Practices

CBK#4 Applications & Systems Development Security

CBK#5 Cryptography

CBK#6 Security Architecture & Models

CBK#7 Operations Security

CBK#8 Business Continuity Planning & Disaster Recovery

CBK#9 Law, Investigation & Ethics

CBK#10 Physical Security

The International CISSP Summary
Japanese edition

国際 CISSP サマリー
日本語版

Written by
John Wallhoff (CISA, CISSP)

Translated by
Yoko Ishizuki(CISSP)

1 イントロダクション

国際 CISSP サマリーの前バージョンは, CISSP 検定の準備をしている際にプロジェクトとして書き, 2002 年に CISSP オープンスタディーグループであるwww.ccure.orgで「CISSP サマリー2002」として発表した. 世界中の人々からリクエストをもらい, この文書に多くの人が感謝し, 他の問題に関してのコメントをもらったり印刷できるバージョンが欲しいと言われたりした.

ある日, 私はこのサマリーを日本語に翻訳したいというリクエストをもらった. CISSP 試験は英語以外の言語では受けることができないので, CISSP 検定の普及と認知へのサポートとなる素晴らしいアイディアであると思った. そして, その他の言語に翻訳することも興味深いと考えた.

このプロジェクトの目的は, 「国際 CISSP サマリー」を同じデザインと構造のままできるだけ多くの言語に翻訳することである. これは CISSP セミナーや本の代替とするために書かれたものではなく, 10 の CBK に含まれている全てのトピックのチェックリストである.

このサマリは, CISSP 試験で要求される 10 の知識ドメイン共通部(CBK, Common Body of Knowledge Domains)を全てカバーする. 更に便利だと思われる関連リンクとリファレンスのページを追加した. このページは全く完全ではなく, もっとたくさん見つけなければならない.

これから試験を受けようとしている人たちへの私のお薦めは, 自分自身の学習計画を立てることである. 全てのドメインに従事してきた人もいるかもしれないが, ほとんどの人はいくつかのドメインは簡単に感じるがその他は難しいと感じるだろう. 私は, 空いた時間(夜子ども達が寝た後)を使って 2 カ月半勉強したが, 常にたくさん読み過ぎなのか少なすぎなのかわからなかった.

試験準備に関して最後になるが重要なこと. 昔, 大学のある教師が私のクラスで言った. 「4 入 5 出」これは試験のために何時間使うかに関しての言葉ではない. 試験に合格するために何時間寝られるかに関しての言葉である. もしほとんどの日に 4 時間寝たら合格し, 5 時間寝たら落ちるということである. しかし, 安心されたい. 私は毎日 5 時間以上寝て合格した. 試験の準備をしている皆にとって, 質の方が量よりも重要なのである.

それでも試験を受けようと思っている皆に幸運を祈っている.

2002 年 11 月

John Wallhoff

2 目次

3 CBK#1 アクセスコントロールのシステムと方法論(Access Control Systems & Methodology)

3.1 セキュリティ原則

機密性(Confidentiality):
許可されていない人, プログラム, プロセスに情報が開示されないこと.
完全性(Integrity):
情報は正確で完全であり, 許可されていない変更から守られなければならない.
可用性(Availability):
情報, システム, リソースはタイムリーに利用可能である必要がある. そしてそれにより生産性が影響を受けない.

3.2 識別(Identification)

サブジェクト(ユーザまたはプログラムまたはプロセス)が, 自ら名乗るエンティティーであることを裏付ける方法. 識別は保証書を使用して確認される.

3.2.1 バイオメトリックス(Biometrics)

その個人にユニークな属性によって識別すること. 識別を確認する, 最も効率的で正確な方法.

3 つの主要な尺度 -
- FRR / 誤拒否率(False Rejection Rate)もしくは第一種の過誤 – 正当なサブジェクトが誤って拒否される確率.
- FAR / 誤受け入れ率(False Acceptance Rate)もしくは第二種の過誤 – 不当なサブジェクトが誤って受け入れられる確率.
- CER / 等誤り率(Crossover Error Rate) – FRR と FAR が等しいパーセンテージ.

他に考慮すべき事項 -
- 登録時間(Enrollment Time) – 評価される生態的特徴のサンプルを提示することによって, システムに最初に「登録」するのに要する時間.
- スループットレート(Throughput Rate) – システムが個人を処理, 識別, 認証するレート.
- 受容性 (Acceptability) – システムを使用する際のプライバシー, 侵襲性, 心理的・物理的な安心の考慮.

バイオメトリックシステムのタイプ -
指紋(Fingerprints): friction ridge によって表される端や分岐とマニューシャと呼ばれる他の詳細な特徴から成る.
手掌スキャン(Palm Scan): 手掌には, その人物にユニークな皺, 隆線, 溝がある.
掌形(Hand Geometry): 人の手の形(手と指の長さと幅)が手の構造を測る.
網膜スキャン(Retina Scan): 眼球後ろ側の網膜の血管パターンをスキャンする.
虹彩スキャン(Iris Scan): 瞳孔の周りの, 色のついた部分のスキャン.
署名ダイナミックス(Signature Dynamics): 署名する際に取得されるスピードと時間の電子信号.
キーボードダイナミックス(Keyboard Dynamics): 特定のフレーズをタイプする時の電子信号を取得する.
声紋(Voice Print): 人々の話す声とパターンの違いを識別.
顔スキャン(Facial Scan): 骨の構造, 鼻の隆線, 目の幅, 額の大きさ, 顎の形等の属性や特徴を考慮する.
ハンドトポロジー(Hand Topology): 個人の手や指のサイズや幅を見る.

3.3 認証(Authentication)

サブジェクトは証明のためにセカンドピースを提示しなければならない.

パスワード(Passwords):
個人を認証するために使用される, 保護された文字列.
クリッピングレベル(Clipping level) – ユーザがロックアウトされるまでに許された, ログイン失敗の回数.
パスワードチェッカー(Password checkers) – ユーザが選んだパスワードのテスト.
パスワードジェネレータ(Password Generators) – ユーザのパスワードを生成するもの.
パスワードエイジング(Password Aging) – パスワードの有効期限.
ログイン試行の制限(Limit Login Attempts) – ログイン試行の失敗回数をある回数に設定する.
認知パスワード(Cognitive password):
事実もしくは意見に基づいた情報を使用して個人の識別を行う.
ワンタイムパスワード(One-time passwords) /ダイナミックパスワード(dynamic password):
パスワードが使用された後は無効になる.
トークンデバイス(Token Device):
チャレンジ・レスポンスの枠組みを使用したパスワードジェネレータ.
同期トークンデバイス(Synchronous token device) – 認証プロセスのコアピースとして時間やイベントを使用して認証サービスと同期を取る.
時間ベース同期トークンデバイス(Time based synchronous token device) – デバイスと認証サービスの内部時計は全く同じ時刻を持っていなければならない.
イベント同期(Event-synchronization) – ユーザはコンピュータ上でログオンシーケンスの初期化を行い, トークンデバイスのボタンを押す必要がある.
非同期トークンデバイス(Asynchronous token device) – チャレンジ・レスポンスの枠組みを使用して認証サービスと通信を行う.
暗号鍵(Cryptographic Keys):
秘密鍵や電子署名を提供する.
パスフレーズ:
パスワードよりも長い文字列. ユーザがこのフレーズをアプリケーションに入力し, アプリケーションがその値を仮想パスワードに変換する.
メモリカード:
情報を保持するカード. しかし情報の処理はしない.
スマートカード:
マイクロプロセッサを持ち, IC がカード自体に組み込まれているため, 情報を処理する能力を持ったカード. スマートカードはまた, 2 要素認証メソッドも提供する. なぜならユーザはユーザ ID と PIN を入力してスマートトークンを開錠するからである.

3.4 承認(Authorization)

サブジェクトが正しく識別され認証された後, オブジェクトに対するアクセス権を供与すること.
知る必要性(Need-to-know):
ユーザは, 社内において自らの仕事の責任を果たすのに最低限必要な権限と許可を持つ.

3.5 シングルサインオン(Single Sign-on)

ユーザが認証情報を 1 度だけ入力しプライマリ・セカンダリのネットワークドメイン内の全てのリソースにアクセスすることが出来る.
スクリプティング(Scripting):
バッチファイルやスクリプトにそれぞれのプラットフォームに必要な, それぞれのユーザの ID, パスワード, ログオンコマンドが含まれている
スクリプトが認証情報を含んでいるので, 保護された領域に保存され, スクリプトの伝送は慎重に行われなければならない.
Kerberos:
対称鍵暗号を使用してエンドツーエンドセキュリティを提供する.
主要な構成要素 -

- KDC / 鍵発行局(Key Distribution Center):
全てのユーザと全てのサービスの暗号鍵を持つ. 認証サービスを提供し, 鍵発行機能を持つ. KDC は例えばユーザ, アプリケーション, サービスのような, プリンシパル(principal)と呼ばれるエンティティーにセキュリティサービスを提供する.
KDC によってチケットが生成され, プリンシパルが他のプリンシパルに認証される必要がある際に与えられる.
KDC はコンポーネントとプリンシパルの組に対してセキュリティサービスを提供する. これを Kerberos ではレルム(realm)と呼ぶ.
- AS / 認証サービス(Authentication Service):
KDC はプリンシパルを認証する.
- TGS / チケット認可(Ticket Granting):
KDC はチケットを生成しプリンシパルに渡す.
弱点 -
KDC は単一点障害(single point of failure)になる.
AS はたくさんのリクエストを扱わなければならない.
秘密鍵がユーザのワークステーションに一時的に保存される.
セッション鍵は復号されユーザのワークステーションに存在する.
パスワード推測に対して脆弱である.
ネットワークトラフィックは守られない.
ユーザがパスワードを変えたときには秘密鍵が変更され, KDS が更新されなければならない.
SESAME:
公開鍵暗号を使用して秘密鍵を配布する.
Privilege Attribute Certificate と呼ばれる認証チケットを使用する..
パスワード推測に対して脆弱である.
シン・クライアント(Thin Clients):
サーバに認証される端ダム端末.

3.6 アクセス制御モデル(Access Control Models)

サブジェクトがオブジェクトにアクセスする方法を決めるフレームワーク.
DAC / 任意アクセス制御(Discretionary Access Control):
リソースの所有者が, そのリソースにアクセスできるサブジェクトを特定できる.
アクセスは, ユーザに付与された認証に基づいて制限される.
最も一般的な DAC の実装は ACL によるものである
MAC / 必須アクセス制御(Mandatory Access Control):
ユーザはセキュリティクリアランスを付与され, データは分類される.
分類はリソースの機密ラベルに保存される.
システムにおいてオブジェクトへのアクセスリクエストを実行するかどうかの判断をする際には, サブジェクトのクリアランスとオブジェクトの分類に基づいて行われる.
このモデルは情報分類と機密性が極度に重要な環境で使用される.

機密ラベル(Sensitivity labels):
MAC が使用される場合には全てのサブジェクトとオブジェクトには機密ラベルがある. 機密ラベルには分類と, 異なるカテゴリが含まれている. 分類は機密レベルを示し, カテゴリはその分類においてどのオブジェクトが持っているかを示す.
RBAC / ロールに基づいたアクセス制御(Role-based access control):
非任意アクセス制御(nondiscretionary access control)とも呼ばれる.
サブジェクトとオブジェクトが交流する方法を決めるために中央で管理されたコントロールセットを使用する.
社内でユーザが持っているロールに基づいてリソースへのアクセスを許可する.
RBAC モデルでは以下の物を使用できる-
- ロールに基づいたアクセス(Role-based access): 社内におけるロールに基づいて決められる.

- タスクに基づいたアクセス(Task-based access): ユーザに割り当てられたタスクによって決められる.
- (Lattice-based access): そのロールに割り当てられた機密レベルによって決められる.

3.7 アクセス制御の手法と技術(Access Control Techniques and Technologies)

様々なアクセス制御モデルをサポートするために利用できる手法と技術.
ロールに基づいたアクセス制御(Role-Based Access Control):
社内での職位の義務を全うするために必要なタスクと責任に基づく.
RBAC は以下と共に用いられる -
- DAC, 管理者はロールを作り, オーナーはこれらのロールがリソースにアクセスできるかどうかを決める.
- MAC, ロールは作成され, 機密ラベルがこうしたロールに割り当てられてセキュリティレベルを表す.

ルールに基づいたアクセス制御(Rule-Based Access Control):
オブジェクトに対して許可されることされないことを示す特定のルールに基づく.
これは, 管理者がルールを設定し, またユーザはこうした制御を変更することが出来ないため MAC の一種である..
制限されたインターフェイス(Restricted Interfaces):
ユーザのアクセスケイパビリティーを特定の機能, 情報へのリクエストや特定のシステムリソースへのアクセスを許可しないことによって制限する.
3 種類の制限されたインターフェイス -
- メニューとシェル(Menus and shells): ユーザには実行可能なコマンドだけが与えられる.
- データベースビュー(Database views): データベースに格納されたデータへのユーザアクセスを制限するメカニズム.
- 物理的に制限されたインターフェイス(Physically constrained interfaces): キーパッド上の特定のキーや画面上の特定のタッチボタンだけを提供することによって実現可能.

アクセス制御行列(Access Control Matrix):
サブジェクトとオブジェクトのテーブルで, 個々のサブジェクトが個々のオブジェクトに対して実行できる動作を示す.
通常, DAC モデルの属性であり, アクセス権限はサブジェクト(ケイパビリティー, capabilities)やオブジェクト(アクセスコントロールリスト, ACLs,)に直接割り当てられる.
ケイパビリティーテーブル(Capability Tables):
特定のサブジェクトが特定のオブジェクトに対して所有するアクセス権限を定める.
サブジェクトはケイパビリティーテーブルの制限を受ける.
Kerberos で使用される.

アクセスコントロールリスト(Access Control Lists):
特定のオブジェクトへのアクセスが認証されたサブジェクトのリスト. どのレベルの認証が付与されているかが定義されている.
認証は個人, ロール, グループに対して決められる.
内容依存アクセス制御(Content-Dependent Access Control):
オブジェクトへのアクセスはオブジェクトの内容によって決められる.

3.8 アクセスコントロール管理(Access Control Administration)

中央集権型(Centralized):
あるエンティティー(部署や個人)が全てのユーザへのリソースアクセス付与に責任を持つ.
ユーザのアクセス権限をコントロールする, 首尾一貫し統一された手法を提供する.
中央集権型アクセス制御技術の例:
- Radius / Remote Authentication Dial-in User Service:

認証プロトコルで, ユーザ(ダイヤルアップユーザ)を認証・承認する.
- TACACS / Terminal Access Controller Access Control System:

クライアント・サーバプロトコルで Radius と同様の機能を提供する.
3 つの世代 -
 * TACACS – 認証と承認を組み合わせる.
 * XTACACS – 認証, 承認, アカウンティングプロセスを分ける.
 * TACACS+ - 認証, 承認, アカウンティングプロセスを分け, 拡張された 2 要素ユーザ認証を使用する.
非中央集権・分散型アクセス管理(Decentralized and Distributed Access Administration):
リソースに近い人々にアクセスコントロールを与える.
組織を通じての統一性や公平性を提供しない.
非中央集権型アクセス制御管理技術の例.
セキュリティドメイン(Security Domain) -
信頼のレルムとして表現される.
全てのサブジェクトとオブジェクトはセキュリティポリシー, 手続き, ルールを共有し, 同じ管理システムによって管理される.
それぞれのセキュリティドメインは, 異なるポリシーや異なる管理を持つことにより異なる.
ヒエラルキー構造やリレーションによって構築される.
オペレーティングシステムやアプリケーション内で使用され, 重要なシステムファイルやプロセスを偶発的な損害から守る.
セキュリティレベルの保護はメモリースペースとアドレスを分けることにより行われる.
セキュリティドメインは, ユーザが利用可能なリソースとして表される.
ハイブリッド(Hybrid):
中央集権型と非中央集権型のアクセス制御管理手法の組み合わせである.

3.9 アクセス制御手法(Access Control Methods)

3.9.1 管理上の制御(Administrative Controls)

ポリシーと手続き(Policy and Procedures) -
ハイレベルなプランで, 組織においてセキュリティがどのように実践されるか, どのようなアクションが許されるか, どのレベルのリスクを会社が受け入れられるかに関してのマネジメントの意志を言明する. シニアマネジメントは DAC, MAC, RBAC アクセス手法のどれを使用するか決め, またこの管理の方法が中央集権的か非中央集権的かを決める.

人事管理(Personnel Controls) -
従業員がセキュリティメカニズムをどのように遵守するか, そしてこうした期待に関して従わないことに関する問題を示す.
- 職務分離(Separation of duties): 個人が, 企業にとって不利になるような重要なタスクを 1 人で実行することができない.
- 共謀(Collusion): 不正を行う為に複数の必要であり, それを行う為には協力しなければならない.
- 職務ローテーション(Rotation of duties): 複数の職位の任務を遂行する方法を知る必要がある.
管理構造(Supervisory Structure) -
個々の従業員には報告を行う上司が存在し, 上司はその従業員の行動に責任を持つ.
セキュリティ啓蒙トレーニング(Security Awareness Training) -
人間は通常最も弱いリンクでありほとんどのセキュリティ侵害や危険の原因となる.
テスト(Testing) -
セキュリティコントロールやメカニズムは全て定期的にテストされ, 設定されたセキュリティポリシー, 目標, 目的を適切にサポートすることを確認する必要がある..

3.9.2 物理的制御(Physical Controls)

ネットワーク分離(Network Segregation) -
物理的・論理的方法で実行される.
境界セキュリティ(Perimeter Security) -

個人, 施設, 施設内の備品を守ることによって物理アクセス制御を提供するメカニズム.
コンピュータコントロール(Computer Control) -
インストールされ, 設定された物理的コントロール.
ワークエリア分離(Work Area Separation) -
アクセス制御と企業全体のセキュリティポリシーをサポートするために使用されるコントロール.
データバックアップ(Data Backups) -
緊急時やネットワーク/システムの崩壊時の情報へのアクセスを確実にする.
ケーブリング(Cabling) -
施設内の全てのケーブルは通路を遮ったり, 切断, 焼失, 捲縮, 盗聴の危険がないように敷設される必要がある.

3.9.3 論理的制御(Logical Controls)

システムアクセス -
アクセス制御の目的を強化する技術的制御.
ネットワークアーキテクチャ(Network Architecture) -
環境の分離・保護を提供するために様々な論理的制御によって構築・強化される. 隔離は物理的・論理的に行うことが出来る.
ネットワークアクセス(Network Access) -
他のネットワークセグメントへのアクセスは粒状でなければならない. ルータやスイッチが使われ, 特定の種類のトラフィックだけがそれぞれのセグメントを通過できるようにできる.
暗号化とプロトコル(Encryption and protocols) -
情報がネットワークを通ったりコンピュータ内にあるときに, 情報を守るための技術的コントロールとして働く.
コントロールゾーン(Control Zone) -
電子信号を発するネットワークデバイスを守る特定のエリア.
監査(Auditing) -
技術的コントロールで, ネットワーク内, ネットワークデバイス上, 特定のコンピュータ上のアクティビティーを追跡する.

3.10 アクセス制御タイプ(Access Control Types)

(P – 物理的(Physical) / A – 管理上の(Administrative) / T – 技術的(Technical))

予防(Preventative): 望ましくない事が起こるのを抑止・回避するために使用される制御.
P - 柵, 錠, バッジシステム, 警備員, バイオメトリックシステム, マントラップドア , 照明, CCTV, アラーム
A – セキュリティポリシー, 監視・監督, 職務分離, ジョブローテーション, 情報分類, 人事手続き, 試験, セキュリティ啓蒙トレーニング.
T - ACL, ルータ, 暗号化, IDS, アンチウイルスソフトウェア, ファイアウォール, スマートカード, ダイアルアップコールバックシステム.

探知(Detective): 起きてしまった事を特定するために使用される制御.
P - 警備員, バイオメトリックシステム, 講堂探知機, CCTV, アラーム, バックアップ.
A – 監視・監督, ジョブローテーション, 人事手続き, 調査, セキュリティ啓蒙トレーニング.
T – 監査ログ, IDS, アンチウイルスソフトウェア, ファイアウォール.

矯正(Corrective): 起きてしまった事を修正するために使用される制御.
P - 柵, 錠, バッジシステム, 警備員, バイオメトリックシステム, マントラップドア, 照明, CCTV, アラーム
A – セキュリティポリシー.
T - IDS, アンチウイルスソフトウェア.

抑止(Deterrent): セキュリティ違反を抑止するために使用される制御.
P - バックアップ
A – 監視・監督, 職務分離, 人事手続き(Personnel Procedures).
T – 暗号化, IDS, ファイアウォール.

復旧(Recovery): リソースや能力を回復するために使用されるコントロール.
P - 柵, 錠, 警備員, マントラップドア, 照明, アラーム, バックアップ
A -
T - アンチウイルスソフトウェア.

補償(Compensation): 他のコントロールの代替となるものを提供するために使用されるコントロール.
P -
A – 監視・監督, 人事手続き.
T -

監視情報の再考(Review of audit information):
監視削減(Audit reduction) – 監視ログ内の情報量を削減する.
変動検出ツール(Variance-detection tool) – コンピュータとリソースの使用傾向を監視し, 変動を検出する.
攻撃シグネチャ検知ツール(Attack signature-detection tool) – アプリケーションが特定の攻撃を示す情報のデータベースを持つ.

キーストローク監視(Keystroke Monitoring):
アクティブなセッション中にユーザが入力したキーストロークを監視して記録する.

3.11 アクセス制御監視(Access Control Monitoring)

IDS / 不正侵入検知(Intrusion detection):
ネットワーク型(Network-based) – ネットワークもしくはネットワークのセグメントを監視する.
ホスト型(Host-based) – 特定のシステムを監視する.
知識ベース(Knowledge-based) / シグネチャ型(signature-based) – 攻撃がどのように行われたかについてのモデルが構築される.
挙動ベース(Behaviour-based) / 統計的(Statistical) – ユーザやシステムの行動の予測からの乖離を監視・検知する.
TIM / Time-based induction machine – リアルタイムで異常行動を検知する.
ハニーポット(Honeypot) – ネットワーク内の「偽の」システムで, 鍵をかけず, ポートを開けておく.
ネットワークスニファー(Network sniffers) – ネットワークトラフィックの傍受を目的としてネットワークに接続されるある種の盗聴機.

3.12 アクセス制御に対する脅威(Threats to Access Control)

辞書攻撃(Dictionary Attack):
攻撃者がユーザの信任を識別することを可能にするプログラム. こうしたプログラムにはよく使用される言葉や文字の組み合わせのリストがあり, プログラムはこれらの値をログオンプロンプトに入力する.
総当たり攻撃(Brute Force Attack):
あらかじめ設定されたゴールを達成するために, 異なる入力を継続的に試行する攻撃. ウォーダイアリングにも用いられる.
ログオンのなりすまし(Spoofing at Login):
偽のログイン画面を示し, ユーザの信任情報を得ようとするプログラム.

4 CBK#2 Telecommunications & Network Security

4.1 Open System Interconnect Model

Protocol - Standard set of rules that determine how systems will communicate across networks.

OSI Model	TCP/IP
Application	Application
Presentation	
Session	
Transport	Host-to-host
Network	Internet
Data Link	Network Access
Physical	

Each layer adds its own information to the data packet.

4.1.1 7. Application layer

Processes and properly formats the data and passes it down to the next layer.
Protocols used - SMTP, HTTP, LPD, FTP, WWW, Telnet, TFTP.

4.1.2 6. Presentation layer

Provides a common means of representing data in a structure that can be properly processed by the end system.
Formats Graphic into TIFF, GIF or JPEG.
Handles data compression and encryption.

4.1.3 5. Session layer

Establishing a connection between the two computers, maintaining it during the transferring of data and controlling the release of this connection.
Protocols used - SSL, NFS, SQL, RPC

4.1.4 4. Transport layer

Provides end-to-end data transport services and establishes the logical connection between two communicating computers.
Protocols used - TCP, UDP, SPX
Information is passed down from different entities at higher layers to the transport layer, which must assemble the information into a stream.

4.1.5 3. Network layer

Insert information into the packet's header so that it can be properly routed.
Protocols used - IP, ICMP, RIP, OSPF, BGP, IGMP.
Protocols that work at this layer do not ensure the delivery of the packets.

4.1.6 2. Data Link layer

The operating system format the data frame to properly transmit over networks (Token Ring, Ethernet, ATM or FDDI).
Protocols used - SLIP, PPP, RARP, L2F, L2TP, FDDI, ISDN
Each network technology has defined electronic signalling and bit patterns.

4.1.7 1. Physical layer

Converts bits into voltage for transmission.
Standard interfaces - HSSI, X.21, EIA/TIA-232, EIA/TIA-449

The session layer enables communication between two computers to happen in three different modes:
- Simplex: Communication takes place in one direction.
- Half-duplex: Communication takes place in both directions, but only one system can send information at a time.
- Full-duplex: Communication takes place in both direction and both systems can send information at the time.

4.2 TCP/IP - Transmission control protocol/Internet protocol

IP:
The main task is to support internetwork addressing and packet forwarding and routing.
Is a connectionless protocol that envelops data passed to it from the transport layer.
TCP:
Is a reliable and connection-oriented protocol, that ensures that packets are delivered to the destination computer.
If a packet is lost during transmission, TCP has the capability to resend it.
Provides reliability and ensures that the packets are delivered.
There is more overhead in TCP packet.
Data - Stream-> Segment -> Datagram -> Frame
UDP:
Is a best-effort and connectionless oriented protocol.
Does not have packet sequencing, flow and congestion control and the destination does not acknowledge every packet it receives.
There is less overhead in UDP packet.
Data - Message -> Packet -> Datagram -> Frame
TCP Handshake:
1. Host sends a SYN packet
2. Receiver answers with a SYN/ACK packet
3. Host sends an ACK packet
IPv4 - Uses 32 bits for its address
IPv6 - Uses 128 bits for its address

4.3 LAN media access technologies

Ethernet:
Characteristics: Share media / Uses broadcast and collision domains / Uses carrier sense multiple access with collision detection (CSMA/CD) access method / Supports full-duplex on twisted-pair implementations / Can use coaxial or twisted-pair media / Defined by standard 802.3
10base2 implementation: ThinNet, uses coaxial cable, maxlength 185 meters, provides 10 Mbps.
10base5 implementation: Thicknet, uses coaxial cable, maxlength 500 meters, provides 10 Mbps.
10base-T implementation: Uses twisted-pair wiring, provides 10 Mbps, usually implemented in star topology.
Fast Ethernet implementation: Uses twisted-pair wiring, provides 100 Mbps.
Token ring:
Uses a token-passing technology with a star configured topology.
Each computer is connected to a central hub, MAU - Multistation Access Unit.
Transmits data at 16 Mbps.
Active monitor - Removes frames that are continuously circulating on the network.
Beaconing - If a computer detects a problem with the network, it sends a beacon frame. It generates a failure domain where computers and devices will attempt to reconfigure certain settings to try and work around the detected fault.
FDDI—Fiber Distributed Data Interface:
Is a high speed token-passing media access topology.
Transmits data at 100 Mbps
Provides fault tolerance by providing a second counterrotating fiber ring.
Enables several tokens to be present on the ring at the same time.

4.4 Cabling

4.4.1 Coaxial Cable

Is more resistant to EMI electromagnetic interference, provides a higher bandwidth and longer cable lengths compared to twisted pair.
Can transmit using a baseband method, where the cable carries only one channel
Can transmit using a broadband method, where the cable carries several channels.

4.4.2 Twisted pair

Is cheaper and easier to work with than coaxial cable.
STP Shielded twisted pair - Has an outer foil shielding which is added protection from radio frequency interference.
UTP Unshielded twisted pair - Different categories of cabling that have different characteristics.

4.4.3 Fiber-optic cabling

Because of the use of glass, it has higher transmission speeds that can travel over longer distances and is not affected by attenuation and EMI when compared to cabling that uses copper. It does not radiate signals like UTP cabling and is very hard to tap into.
Is expensive.

4.4.4 Cabling problems

Noise - The receiving end will not receive the data in the form that was originally transmitted. Can be caused by motors, computers, copy machines, florescent lightning and microwave ovens.
Attenuation - The loss of signal strength as it travels or caused by cable breaks and cable malfunctions.
Crosstalk - When electrical signals of one wire spill over to another wire. UTP is much more vulnerable to this than STP or coaxial.
Plenum space - Network cabling that is placed in an area to meet specific fire rating to ensure that it will not produce and release harmful chemicals in case of a fire.
Pressurized conduits - Encapsulation of wires so if there is an attempt to access a wire, the pressure of the conduit will change and sound an alarm or send a message to the administrator.

4.5 Types of transmission

Analog transmission signals - Modulation of signals, electromagnetic waves.
Digital transmission signals - Represents binary digits as electrical pulses.

Asynchronous communication - Two devices are not synchronized in any way. The sender can send data at anytime and the receiving end must always be ready. Can be a terminal and a terminal server or modem.
Synchronous communication - Takes place between two devices that are synchronized, usually via a clocking mechanism. Transfers data as a stream of bits.

Baseband - Uses the full cable for its transmission
Broadband - Usually divides the cable into channels so that different types of data can be transmitted at a time.

Unicast method - A packet needs to go to one particular system
Multicast method - A packet need to go to a specific group of systems
Broadcast method - A packet goes to all computers on its subnet

4.6 Network Topology

4.6.1 Ring Topology

Has a series of devices connected by unindirectional transmission links, that forms a ring. Each node is dependent upon the preceding nodes and if one system failed, all other systems could fail.

4.6.2 Bus Topology

A single cable runs the entire length of the network. Each node decides to accept, process or ignore the packet. The cable where all nodes are attached is a potential single point of failure.
Linear bus - Has a single cable with nodes attached to it.
Tree topology - Has branches from the single cable and each branch can contain many nodes.

4.6.3 Star Topology

All nodes connect to a central hub or switch. Each node has a dedicated link to the central hub.

4.6.4 Mesh Topology

All systems and resources are connected to each other in a way that does not follow the uniformity of the previous topologies.

4.7 LAN Media Access Technologies

MTU - Is a parameter that indicates how much data a frame can carry on a specific network.
Token passing:
Is a 24-bit control frame used to control which computers communicate at what intervals. The token grants a computer the right to communicate. Do not cause collisions because only one computer can communicate at a time.
CSMA Carrier sense multiple access:
CSMA/CD (collision detection) - Monitor the transmission activity or carrier activity on the wire so that they can determine when would be the best time to transmit data. Computers listen for the absence of a carrier ton on the cable, which indicates that no one else is transmitting date at the same time.
Contention - The nodes have to compete for the same shared medium
Collision - Happens when two or more frames collide.
Back-off algorithm - All stations will execute a random collision timer to force a delay before they attempt to transmit data.
CSMA/CA (collision avoidance) - Is an access method where each computer signals its intent to transmit data before it actually does so.
Collision Domains:
Is a group of computers that are contending or competing for the same shared communication medium.
Polling:
Some systems are configured to be primary stations and others are secondary stations. At predefined intervals, the primary station will ask the secondary station if it has anything to transmit.

4.8 Protocols

ARP - Knows the IP address and broadcasts to find the matching hardware address, the MAC address.
RARP - Knows the hardware address and broadcasts to find the IP address.
Masquerading attack - An attacker alter a system's ARP table so that it contains incorrect information (ARP table poisoning).
DHCP - A computer depends upon a server to assign it the right IP address.
BOOTP -Can receive a diskless computers IP address from a server

ICMP - Delivers messages, reports errors, replies to certain requests, reports routing information and is used to test connectivity and troubleshoot problems on IP networks.

4.9 Networking devices

Device	OSI Layer	Functionality
Repeater	Physical	Amplifies signals and extends networks.
Bridge	Data link	Forwards packets and filters based on MAC adresses; forwards broadcast traffic, but not collision traffic.

Router	Network	Seperates and connnects LANs creating internetworks; routers filter based on IP addresses.
Brouter	Data link andNetwork	A hybrid device that combines the functionality of a bride and a router. A brouter can bridge multiple protocols and can route packets on some of those protocols.
Switch	Data link(More intelligent switches work at the network layer)	Provides a private virtual link between communicating devices, allows for VLANs, reduces traffic and impedes network sniffing.
Gateway	Application(although different types of gateways can work at otherLayers)	Connects different types of networks, performs protocol and format translations.

Comments on bridges:
Three types of bridges:
- Local bridge: Connects two or more LAN segments within a local area.
- Remote bridge: Can connect two or more LAN segment over a wide area network by using telecommunications.
- Translation bridge: If two LANs being connected are different types and use different standards and protocols.
Broadcast storm - Because bridges forward all traffic, the forward all broadcast packets.
STA Spanning Tree Algorithm - Ensures that frames do not circle networks forever, provides redundant paths in case a bridge goes down, assigns unique identifiers to each bridge, assigns priority values to these different bridges and calculates path costs.
Source routing - The packets hold the forwarding information so that they can find their way to the destination themselves without bridges and routers dictating their paths.

VLAN Virtual LANs:
Enable administrators to logically separate and group users based on resource requirements, security or business needs instead of the standard physical location of the users.
PBX Private Branch Exchange:
Is a telephone switch that is located on a company's property.

4.10 Firewalls

Restrict access from one network to another, internally or externally.
DMZ - Demilitarized Zone:
A Network segment that is located between the protected and the unprotected networks.

4.10.1 Packet filtering

A method controlling what data can flow into and from a network.
Take place by using ACL's, which are developed and applied to
a device.
Is based on network layer information, which means that the device cannot look too far into the packet itself.
Is not application dependent.
Do not keep track of the state of a connection.
Provides high performance.
Used in first-generation firewalls.

4.10.2 Stateful Packet Filtering

It remembers and keeps track of what packets went where until that particular connection is closed. This requires the firewall to maintain a state table, which is like a score sheet of who said what to whom.
Make decisions on what packets to allow or disallow.
Works at the network layer.

4.10.3 Proxy firewalls

Stands between a trusted and untrusted network and actually makes the connection, each way, on behalf of the source.
Makes a copy of each accepted packet before transmitting it and repackages the packet to hide the packet's true origin.
Works at the application layer

4.10.4 Dual-homed firewall

Has two interfaces; one facing the external network and the other facing the internal network.
Has two NICs and has packet forwarding turned off.
Are often used when a company uses proxy firewalls.

4.10.5 Application-level proxies

Inspect the entire packet and make access decisions based on the actual content of the packet.
Understand different services and protocols and the commands that are used within them
There must be one application-level proxy per service.
Works at the application level.

4.10.6 Circuit-level proxy

Creates a circuit between the client computer and the server
It knows the source and destination addresses and makes access decisions based on this information.
Can handle a wide variety of protocols and services.
Works at the network layer.

4.10.7 SOCKS

Is an example of a circuit-level proxy gateway that provides a
secure channel between two TCP/IP computers.
Does not provide detailed protocol-specific control.

4.11 Firewall architecture

4.11.1 Bastion Host

It is the machine that will be accessed by any and all entities trying to access or leave the network.
Can support packet filtering, proxy and hybrid firewall applications.

4.11.2 Screened Host

Is a bastion host firewall that communicates directly with a border router and the internal network.

4.11.3 Screened Subnet

The bastion host, housing the firewall, is sandwiched between
two routers. The external applies packet filtering and the internal also filters the traffic.

4.11.4 Shoulds of Firewalls

The default action of any firewall should be to implicitly deny any packets not explicitly allowed.

4.11.5 Masquerading / spoofing

The attacker modifies a packet header to have the source address of a host inside the network that she wants to attack.

4.11.6 Honeypot

Is a computer that sits in the DMZ in hopes to lure attackers to it instead of actual production computers.

4.12 Networking Services

NOS - Networking operations system:

Is designed to control network resource access and provide the necessary services to enable a computer to interact with the surrounding network.
DNS - Domain Name service:
Is a method of resolving hostnames.
Networks are split up into zones
The DNS server that holds the files for one of these zones is said to be the authoritative name server for that particular zone.
It is recommended that there be a primary and secondary DNS server for each zone.
Directory Services:
Has a hierarchical database of users, computers, printers, resources and attributes of each.

4.13 Intranets and Extranets

4.13.1 Intranets

When a company uses Internet– or Web-based technologies inside their networks.

4.13.2 Extranets

Enable two or more companies to share common information and resources.

4.13.3 NAT Network Address Translation

Is a gateway between a network and the Internet, or another network, that performs transparent routing and address translation.

4.14 MAN - Metropolitan Area Network

Usually a backbone that connects businesses to WANs, the Internet and other businesses.
A majority are SONET / Synchronous Optical Network or FDDI rings.

4.15 WAN - Wide Area Network

Are used when communication needs to travel over a larger geographical area.
Dedicated links:
Also called leased line or point-to-point link.
T-carriers:
Dedicated lines that can carry voice and data information over trunk lines.
S/WAN - Secure WAN:
Based on VPNs that are created with IPSec.

4.16 WAN Technologies

4.16.1 CSU/DSU - Channel Service Unit / Data Service Unit

Is required when digital equipment will be used to connect a LAN network to a WAN network.
DSU converts digital signals to be transmitted over the telephone company's digital lines.
CSU is the unit that connects the network directly to the telephone company's line.
Provides a digital interface for DTE - Data Terminal Equipment.
Provides an interface to the DCE - Data Circuit-Terminating Equipment device.

4.16.2 Switching

Circuit switching - Sets up a virtual connection that acts like a dedicated link between two systems.
Packet switching - Packets can travel along many different routes to arrive to the same destination.

4.16.3 Frame relay

Is a WAN protocol that operates at the data link layer.
Uses packet-switching technology.

CIR /committed information rate - Companies that pay more to ensure that a higher level of bandwidth will always be available to them.
Two main types of equipment used:
- DET / Data Terminal Equipment - Customer owned.
- DCE / Data Cricuit-Terminating Equipment - Service provider's or phone company's

4.16.4 Virtual Circuits

PVC / Permanent virtual circuit - Works like a private line for a customer with an agreed-upon bandwidth availability.
SVC / switched virtual circuits - Require steps similar to a dial-up and connection procedure.
X.25:
Is an older WAN protocol that defines how devices and networks establish and maintain connections.
Is a switching technology.
Data is divided into 128 bytes and encapsulated in High-level Data Link Control (HDLC) frames. The frames are then addressed, and forwarded across the carrier switches.

4.16.5 ATM - Asynchronous Transfer Mode

Is a switching technology.
Uses a cell-switching technology. This means that data is segmented into fixed size cells, 53 bytes, instead of variable-size packets.
Is a high-speed networking technology used for LAN, WAN and service provider connections
Sets up virtual circuits, which act like dedicated paths between the source and destination. These virtual circuits can guarantee bandwidth and QoS.

4.16.6 SMDS - Switched Mulitmegabit Data Service

Is a high-speed packet-switched technology used to enable customers to extend their LANs across MANs and WANs
Is connectionless and can provide bandwidth on demand.

4.16.7 SDLC - Synchronous Data Link Control

Is based on networks that use dedicated, leased lines with permanent physical connections.
Provides the polling media access technology, which is a mechanism that enables secondary stations to communicate on the network.

4.16.8 HDLC - High-level Data Link Control

Is a bit-oriented link layer protocol used for transmission over synchronous lines.
Works with primary stations that contact secondary stations to establish data transmission.

4.16.9 HSSI - High-Speed Serial Interface

Is used to connect multiplexers and routers to high-speed communication services like ATM and frame relay.

4.16.10 Multiservice Access

Combine different types of communication categories over one transmission line.
Jittering - When someone using VoIP for phone call experiences lags in the conversation.

4.16.11 H.323

Is a part of ITU-T recommendations that cover a wide variety of multimedia communication services.

4.17 Remote Access

4.17.1 Dial-up and RAS

RAS / Remote Access Service server - Performs authentication by comparing the provided credentials with the database of credentials it maintains.

Wardialing - Is a process used by many attackers to identify remote access modems.

4.17.2 ISDN - Integrated Services Digital Network

Breakes the telephone line into different channels and transmits data in a digital form versus the old analog method.
Three methods -
- BRI / Basic Rate Interface - 2 B channels and 1 D channel.
- PRI / Primary Rate Interface - 23 B channels and 1 D channel.
- BISDN / Broadband - Handle different types of services at the same time.

The D channel provides for a quicker call setup and process of making a connection.

4.17.3 DSL - Digital Subscriber Line

Is a broadband technology.
The services can be symmetric -> Speed upstream <> downstream.
Connected all the time.

4.17.4 Cable modems

Provide high speed access.
Connected all the time.

4.18 VPN - Virtual Private Network

Is a secure private connection through a public network.

4.18.1 PPTP - Point-to-point tunnelling protocol

Is an encapsulation protocol based on PPP.
Works at the data link layer and it enables a single point-to-point connection.
Encrypts and encapsulates PPP packets
When negotiating takes place, PPTP cannot encrypt this information because encryption is in the process of being invoked.
Can only work on top of IP networks

4.18.2 L2TP - Layer 2 Tunnelling Protocol

Can run on top and tunnel through networks that use other protocol
Is not an encryption protocol.
Supports TACACS+ and RADIUS

4.18.3 L2F - Layer 2 Forwarding

Provides mutual authentication
No encryption

4.18.4 IPSec

Handles multiple connections at the same time
Provides secure authentication and encryption
Supports only IP networks
Focuses on LAN-to-LAN communication rather than a dial-up protocol
Works at the network layer and provides security on top of IP
Can work in tunnel mode, meaning the payload and header is encrypted or transport mode, meaning that only the payload is encrypted.

4.18.5 PPP - Point-to-Point

Is used to encapsulate messages and transmit them through an IP network.

4.18.6 PAP - Password Authentication Protocol

Provides identification and authentication of the user attempting to access a network from the remote system.

4.18.7 CHAP - Challenge Handshake Authentication Protocol

Is an authentication protocol that uses challenge/response mechanism to authenticate instead of sending a username and password.

4.18.8 EAP - Extensible Authentication Protocol

Provides a framework to enable many types of authentication techniques to be used during PPP connections.

4.19 Network and resource availability

4.19.1 Single point of failure

If one device goes down, a segment or the entire network is negatively affected.

4.19.2 RAID - Redundant Array of Inexpensive Disks

A technology used for redundancy and performance improvement that combines several physical disks and aggregates them into logical arrays.

4.19.3 Clustering

A group of servers that are viewed logically as one server to users and are managed as a single system.

5 CBK#3 セキュリティ管理の実践(Security Management Practices)

5.1 セキュリティの基本原則(Fundamental Principles of Security)

5.1.1 *セキュリティ目標(Security objectives)*

機密性(Confidentiality):
必要なレベルの機密性を実現する能力を提供する.
完全性(Integrity):
情報とシステムの正確性と信頼性が提供され, 許可されていないデータの変更が防止されているときに保全性が守られていると言える.
可用性(Availability):
サービスや生産の中断を防ぐ.

5.1.2 定義(Definitions)

脆弱性(Vulnerability):
ソフトウェア, ハードウェア, 手続き上の弱さで, コンピュータやネットワークに入り環境内部のリソースへの許可されないアクセスを行おうとしている攻撃者に, 開いたドアを提供することになるかもしれないものである.
脅威(Threat):
情報やシステムにとっての潜在的な危険
リスク(Risk):
脆弱性を突いた脅威の可能性.
露出(Exposure):
脅威による損害への露出.
対策(Countermeasure) /予防策(safeguard):
潜在的なリスクを軽減する.
トップダウンアプローチ(Top-down approach):
開始, サポート, 指揮がトップマネジメントから中間マネジメントを通じ, スタッフメンバーに進む.
ボトムアップアプローチ(Bottom-up approach):
セキュリティプログラムが, 適切なマネジメントのサポートや指揮なしに IT スタッフによって開発される.
運用上のゴール(Operational goals):
日々のゴール.
戦術上のゴール(Tactical goals):
中期のゴール.
戦略上のゴール(Strategic goals):
長期のゴール.
リスク管理(Risk Management):
リスクを特定して評価し, 受け入れられるレベルまで軽減した上でそのリスクレベルを維持するために適切なメカニズムを実行するプロセス.

5.2 リスク分析(Risk Analysis)

セキュリティ予防策を正当化するためにリスクを特定し可能性のある損害を見積もる手法.
3 つの主要なゴールがある:
- リスクを特定する
- 潜在的な脅威の影響を計る
- リスクの影響と対策のコストの経済的バランスを提供する.

リスクには潜在的な損害が存在する: 企業は実際に脆弱性を突かれた場合に何らかの損害を受けるだろう.
遅効型の損害(Delayed loss): リスクが最初に起こった後に企業に悪い影響がある.

5.2.1 量的アプローチ(Quantitative Approach)

生じる損害と対策のコストに実際の数字を当てはめる.
脅威とリスクの可能性を決めるときに明確なパーセンテージを定める.
質的なアイテムを定量化しようとする手法であるため, 純粋に量的なリスク分析は不可能である.

リスク分析のステップ-
- 情報と資産の価額を定める.
- リスク毎に潜在的な損失を見積もる
- 脅威分析を行う
- リスク毎の全体の潜在的な損失を導き出す
- それぞれのリスクに対する対策を選択する
- リスクの軽減, 譲渡, 受け入れをする

リスクの計算(Calculating risks) -
EF (露出要素, Exposure Factor) = 特定の脅威によって起こる資産損失のパーセンテージ
SLE (単一損失予測, Single Loss Expectancy) = 資産価値 * 露出要素
ARO (年次発生率, Annualized Rate of Occurrence) = 1 年間に脅威が起こる頻度の推定値.
ALE (年次損失予測, Annualized Loss Expectancy) = 単一損失予測 * 年次発生率

5.2.2 質的アプローチ(Qualitative Approach)

リスクの可能性の様々なシナリオを一通り見て, 脅威の深刻度と資産の重要性にランクを付ける.
シナリオを作成する際の手順:
- シナリオは主要なそれぞれの脅威を扱う
- シナリオはビジネスユニットマネジャーによって現実性のチェックをされる
- RA チームはそれぞれの脅威に対して様々な防御策を推薦する
- RA チームは脅威, 資産, 防御策を使用してそれぞれの最終的なシナリオを作成する.
- チームは成果をマネジメントに提出する.

5.2.3 デルファイ法(Delphi Technique)

グループ意思決定の手法で, グループのメンバーのそれぞれが, 特定のリスクの結果について率直な意見を言うことを保証する.

5.2.4 対策とリスクの計算(Calculating countermeasures and risk)

企業にとっての防御策の価値 = (防御策導入前の ALE) - (防御策導入後の ALE) - (防御策の年間費用)
総リスク = 脅威 * 脆弱性 * 資産価値
残余リスク = (脅威 * 脆弱性 * 資産価値) * コントロールギャップ

5.2.5 リスクの対処(Handling Risk)

リスク移転(Transfer risk) -> 保険の購入
リスク軽減(Reduce risk) -> 対策の導入(Implements countermeasures)
リスク拒否(Rejecting risk) -> リスクを拒否もしくは無視する.
リスク受け入れ(Accept the risk) -> 企業がどのレベルのリスクの元にあるか, また可能性のある損害のコストについて理解し, それと共存して行くことに決める.

5.3 セキュリティプログラム(Security Program)

ポリシーのカテゴリー(Categories of policy):
- 規制(Regulatory)
- 勧告(Advisory)
- 情報提供(Informative)

5.3.1 セキュリティポリシー(Security Policy)

シニアマネジメントが作成する全体的な声明で, 組織内においてセキュリティがどのような役割をするかを定める.
一般的な形式で多くの事項についてカバーするために広く外観的な言葉で書かれている.
- 組織のセキュリティポリシー(Organisational security policy): 組織内の全てのセキュリティ活動の範囲と方向を示す.
- 特定の問題のポリシー(Issue-specific policies): 包括的な枠組みを構築し, 全ての従業員がセキュリティ問題にどのように従うかについて理解するために, マネジメントがより詳細な説明と注意が必要だと感じる特定のセキュリティ問題を扱う.
- 特定のシステムのポリシー(System-specific policy): 実際のコンピュータ, ネットワーク, アプリケーション, データに近いマネジメントの意思を示す.

5.3.2 標準(Standards)

ハードウェアとソフトウェア製品がどのように使用されるかを定める. 特定の技術, アプリケーション, パラメータ, 手順が組織全体で決まった方式で実行されるようにする方法を提供する.
こうしたルールは通常企業内で強制される.

5.3.3 ベースライン(Baselines)

組織全体に必要なセキュリティの最低限のレベルを提供する.

5.3.4 ガイドライン(Guidelines)

特定のスタンダードが当てはまらない場合に, ユーザ, IT スタッフ, オペレーションスタッフ, その他に対する推奨されたアクションおよび運用上のガイドとなる.

5.3.5 手順(Procedures)

あるタスクを遂行するためのステップバイステップのアクションである.
ポリシーチェインの最も低いレベルとみなされる.

5.4 データの分類(Data Classification)

データ分類の主要な目的は, それぞれのタイプの情報に必要なレベルの機密性, 完全性, 可用性を示すことである.
これによりデータが最も効率的に保護される.

一般的な分類レベル (高レベルから順に):
商業ビジネス(Commercial business) ->
- 秘密(Confidential)
- プライベート(Private)
- 取り扱い注意(Sensitive)
- 公開(Public)

軍(Military) ->
- 最高機密(Top secret)
- 機密(Secret)
- 秘密(Confidential)
- 非機密だが取り扱い注意(Sensitive but unclassified)

- 非機密(Unclassified)

5.5 責任のレイヤー(Layers of Responsibility)

5.5.1 シニアマネジャー(Senior Manager)

組織のセキュリティと資産の保護に最終的な責任を持つ.

5.5.2 セキュリティプロフェッショナル(Security professional)

セキュリティに関して職務上責任を持ち, マネジャーの指示を実行する.

5.5.3 データオーナー(Data Owner)

通常シニアマネジメントの一員で, データの保護と使用の最終的な責任を持つ.
自分が責任を持っているデータの分類を決め, ビジネスニーズが生じたときにはその分類の変更を行う.
日々のデータ保持の責任をデータ管理者に委譲することがある.

5.5.4 データ管理者(Data Custodian)

データの保持と保護の責任を付与される.

5.5.5 ユーザ(User)

仕事に関連したタスクのために日常的にデータを使用する個人全て.
職位内で必要なレベルのデータアクセスを持っていなければならない. また, 他に対するデータの C/I/A を保護するために運用上のセキュリティ手順に従う責任がある.

5.5.6 Structure and practices

職務分離(Separation of duties):
危険なタスクを 1 人で実行することができないようにすること.
共謀(Collusion):
ある種の破壊や不正を行うのに複数の人間を必要とする. これによりこうした不正の可能性が著しく低下する.
機密保持契約(Nondisclosure agreements):
従業員が何らかの理由で辞職する場合に企業を守る.
ジョブローテーション(Job rotation):
特定の個人にビジネスセグメントのコントロールをあまりに与えすぎないように, 長期間 1 人の人間を同じポジションに置いておかない.

5.6 セキュリティ啓蒙(Security Awareness)

トレーニングのタイプ(Types of training):
- オペレーターへのセキュリティ関連ジョブトレーニング
- セキュリティが重要な職位の特定の部署やグループに対する啓蒙トレーニング
- IT サポート人員やシステムアドミニストレーターに対する技術的セキュリティトレーニング
- セキュリティ実行者や情報システム監査者に対する高度な InfoSec トレーニング
- シニアマネジャー, ファンクショナルマネジャー, ビジネスユニットマネジャーに対するセキュリティトレーニング

6 CBK#4 アプリケーションおよびシステムの開発(Applications & Systems Development Security)

6.1 データベースシステムとデータベース管理(Database systems and database management)

データベースのタイプ(Types of databases):
- 階層型(Hierarchical)
- メッシュ(Mesh)
- オブジェクト指向(Object-oriented)
- リレーショナル(Relational)

DBMS / データベース管理システム(Database Management System) -
様々なタイプのユーザがアドホッククエリを使って大きな構造的なデータセットを管理するためのプログラム群.
データベース(Database):
意味のある方法で保存されたデータの集合で, 必要に応じて複数のユーザやアプリケーションがアクセスし, 閲覧し, データの更新を行うことが出来る.
データベース用語(Database terms)/jargon -
- レコード(Record): 関連するデータアイテムの集合
- ファイル(File): 同じタイプのレコードの集合
- データベース(Database): 相互に参照されるファイルの集合
- DBMS: データベースを管理しコントロールする
- ベースリレーション(Base relation): データベースに保存されたテーブル
- タプル(Tuple): データベース内の行
- 属性(Attribute): データベース内の列
- 主キー(Primary key): 行を一意に決める列
- ビュー(View): データベース内に定義された仮想的な関係で, サブジェクトが閲覧できるデータをコントロールする
- 外部キー(Foreign key): あるテーブルのある属性が他のテーブルの主キーになっている
- セル(Cell): 行と列の交差
- スキーマ(Schema): データベースを表すデータ
- データディクショナリ(Data dictionary): データエレメントとその関係の中央のリポジトリ.
- 濃度(Cardinality): リレーション内の行数
- 度(Degree): リレーション内の列数.
- ドメイン(Domain): ある属性が取りうる値の集合.

6.1.1 データベースモデル(Database models)

リレーショナルデータモデル(Relational data model) -
属性(列)とタプル(行)を使用し情報を格納・整理する.
主キーがレコード内の全てのデータを対応する値に対応づけるフィールドである.

階層型データモデル(Hierarchical data model) -
レコードとフィールドを論理木構造で関係づける.
子は 1 つでも複数でもなくてもよい.
一対多の関係をマッピングする際に有用.

分散データモデル(Distributed data model) -
複数のデータベースにデータが保存されているが, 論理的にはつながっている.
それぞれのデータベースは別々の管理者が管理できるが, 全体の論理的データベースは 1 人もしくは 1 つのグループが管理しなければならない.

リレーショナルデータベースのコンポーネント:
DDL / データ定義言語(Data Definition Language) -
データベースの構造とスキーマを定義する.
- 構造(Structure): テーブルサイズ, キープレースメント, ビュー, データエレメントリレーションシップ.
- スキーマ(Schema): 保存され操作されるデータのタイプとプロパティ.
DML / データ操作言語(Data Manipulation Language) -
ユーザがデータベースを閲覧, 操作, 使用することができるコマンド全て.
QL / クエリ言語(Query Language) -
ユーザがデータベースにリクエストをすることができる.
レポートジェネレータ(Report Generator) -
ユーザが定義した形式でデータの印刷を行える.

6.1.2 データディクショナリ(Data dictionary)

データエレメントとそのリレーションシップの中央のリポジトリ.
データエレメント, スキーマオブジェクト, 参照キーの集合.
スキーマオブジェクト(Schema objects) – テーブル, ビュー, インデックス, プロシージャー, 関数, トリガを含む.

6.1.3 キー(Keys)

主キー(Primary key) -
テーブル内でユニークに識別し, テーブル内の個々のタプルもしくは行を明らかに指し示す.
テーブル内の候補キーのサブセットである.
外部キー(Foreign key) -
他のリレーション内の主キーに相当する, あるリレーション内の属性(行).

6.1.4 整合性(Integrity)

同時性問題(Concurrency problems) -
異なるサブジェクトが最新の情報を得られるようにする.
意味整合性(Semantic integrity) -
構造的・意味的なルールが守られるようにする. これらのルールはデータ型, 論理値, 一意性制約, オペレーションに関係し, データベース構造に悪影響を及ぼす.
参照整合性(Referential integrity) -
存在しないレコードや NULL 値の主キーへの参照をしているレコードを持たないようにするメカニズム.
エンティティー整合性(Entity integrity) -
属性が NULL の場合.
ロールバック(Rollback) -
現在のトランザクションを終了させ, データベースに対する更新を全てキャンセルする文.
コミット(Commit) -
トランザクションを終了させ, そのユーザが行った全ての更新を実行する.
チェックポイント(Checkpoint) -
システムの不具合が生じたときやエラーが検知されたときに, ユーザがいつでもシステム障害前の時点に戻ることができる.

6.1.5 データベースセキュリティ問題(Database security issues)

集約(Aggregation) -
特定の情報にアクセスするクリアランスや許可がユーザにないが, この情報の構成要素へのアクセスが許可されている場合, このユーザは残りの見当をつけることができ, 制限された情報を得ることができる.

推論(Inference) -
サブジェクトがアクセスを制限されている情報を, アクセスできるデータから推定するときに起きる. 低いセキュリティレベルのデータが,高いセキュリティレベルのデータを間接的に表すときに見られる.
内容依存アクセス制御(Content-dependents access control) -
アクセス制御を決めるときにファイルの内容を見る. このタイプのアクセス制御は処理のオーバーヘッドが高いがより細かいコントロールができる.
セル隠蔽 Cell suppression) -
推論攻撃に使用されうる情報を含んだ特定のセルを隠したり見せなかったりすること.
パーティショニング(Partitioning) -
データベースをいくつかの部分に分け, 許可されていない者がデータを集めて推論したり発見したりすることを難しくする.
ノイズと混乱(Noise and perturbation) -
攻撃者を誤った方向へ誘導したり混乱させたりして実際の攻撃を意味のないものにするために, 偽の情報を挿入する技術.
データベースビュー(Database views) -
1 つのグループや特定のユーザに特定の情報を閲覧することを許可し, 他のグループには全く許可しない.
Polyinstantiation -
リレーションにおいて同じ主キーのタプルを含むことができ, それぞれのインスタンスはセキュリティレベルで識別される.

OLTP / オンライントランザクション処理(On Line Transaction Processing) -
問題を監視し, 起きたときに適切に対応するメカニズムを提供する.
- 2 相コミットサービス(Two-phase commit service): 全てのデータベースが受け入れて更新をするまでトランザクションが完了しない
データウェアハウジング(Data warehousing) -
複数のデータベースから得たデータを組み合わせて大きなデータベースにし, 完全な情報取得とデータ分析を行う
データマイニング(Data mining) -
データウェアハウス内のデータをより有用な情報にする処理.
- メタデータ(Metadata): データマイニングツールによって作成されたデータで, 関連性, 相関を見つけるためのもの..
OODB / オブジェクト指向データベース(Object-Oriented Data Bases) -
コードと分析の再使用が簡単で, 保守の手間が省けると言う特徴がある. また, 問題の分析からデザインや実現への移行が容易である.
主要な短所としては, ラーニングカーブが急であること, 開発と運用のためのハードウェア・ソフトウェアのオーバーヘッドが高いことが挙げられる.
オブジェクトリレーショナルデータベース(Object-Relational Databases) -
オブジェクト指向とリレーショナル技術の特徴を組み合わせる.

6.2 システムライフサイクルのフェーズ(System life cycle phases)/ソフトウェアライフサイクル開発プロセス(software life cycle development process)

6.2.1 システムライフサイクルのフェーズ(System Life Cycle Phases)

- プロジェクト開始(Project initiation):
  - プロジェクト定義の構想
  - 提案と書記長さ
- 機能デザイン分析と計画(Functional design analysis and planning)
  - 要件を明らかにし, 定義する
  - システム環境の仕様を決める

- システムデザイン仕様(System design specifications)
  - 機能デザインレビュー
  - 機能分析
  - 詳細計画の導入
  - コードデザイン
- ソフトウェア開発(Software development)
  - ソフトウェアの開発とプログラミング
- インストール(Installation) / 実装(implementation)
  - 製品のインストール
  - テストと監査
- 運用(Operational)/保守(maintenance)
  - 製品の変更, 修正, マイナーな変更
- 廃棄(Disposal) / 更新と入れ替え(Revision and replacement)
  - 更新や全ての入れ替えによって製品を変更

6.2.2 ウォーターフォールモデル(The Waterfall Model)

- システム要件(System requirements)
- ソフトウェア要件(Software requirements)
- 分析(Analysis)
- プログラムデザイン(Program design)
- コーディング(Coding)
- テスト(Testing)
- 運用と保守(Operations & Maintenance)

6.2.3 V&V を組み入れた修正版ウォーターフォールモデル(Modified Waterfall Model incorporating V&V)

- システム実現可能性(System feasibility) -> 妥当性確認(validation)
- ソフトウェアプランと要件(Software plans & requirements) -> 妥当性確認(validation)
- 製品デザイン(Product design) -> 検証(verification)
- 詳細デザイン(Detailed design) -> 検証(verification)
- コーディング(Coding) -> 単体テスト(unit test)
- 製品のインテグレーション(Integration Product) -> 検証(verification)
- 実装(Implementation) -> システムテスト(system test)
- 運用と保守(Operations & Maintenance) -> 妥当性再確認(revalidation)

6.2.4 セキュリティ問題

- システム開発のそれぞれのフェーズでセキュリティが考慮されなければならない. セキュリティは開発の最後で取り扱ってはならない. なぜならコスト, 時間, 手間がかかり機能が欠けるからである.
- 職務分離が, ロール, 環境, 製品開発に関する機能において実践されなければならない.
- プログラマーは作成されているコードに直接アクセスできないようにする.
- システム内のセキュリティメカニズムのテストと評価に関する証明
- システムとそのセキュリティレベルに関するマネジメントの正式な認定.
- 変更に関しては承認を得, テストし, 記録しなければならない. そしてその変更はシステムのセキュリティレベルやセキュリティポリシーの実施能力に影響を与えてはならない.

6.2.5 変更管理のサブフェーズ(Change control sub-phases)

- リクエスト管理(Request control)
- 変更管理(Change control)
- リリース管理(Release control)

6.2.6 変更管理のプロセス(Change control process)

- 変更の正式なリクエストをする
- リクエストを分析する
  - 実行計画を立てる
  - 実行のコストを計算する
  - セキュリティに対する影響をレビューする
- 変更リクエストを記録する
- 承認を得るために変更リクエストを提出する
- 変更の開発
  - 製品のコーディングを行い, 機能の追加や削除を行う.
  - これらのコードの変更を正式な変更リクエストにリンクさせる
  - テストと品質承認のためにソフトウェアを提出する
  - 品質が適切な物になるまで繰り返す
  - バージョンの変更を行う

6.2.7 コンフィギュレーション管理(Configuration management)

- コンフィギュレーションの特定(Configuration identification)
- コンフィギュレーションコントロール(Configuration control)
- コンフィギュレーションステータスアカウンティング(Configuration status accounting)
- コンフィギュレーション監査(Configuration audit)

6.2.8 CMM / ソフトウェアプロセス成熟度モデル(Software Capability Maturity Model)

- Level 1: 初期レベル(Initiating) – 有能な人々と英雄; プロセスは正式でなく場当たり的
- Level 2: 反復できるレベル(Repeatable) – プロジェクト管理プロセス; プロジェクト管理の実践が制度化されている
- Level 3: 定義されたレベル(Defined) – エンジニアリングプロセスと組織のサポート; 技術的な実践がマネジメントの実践と統合され制度化されている
- Level 4: 管理されたレベル(Managed) – 製品とプロセスの改善; 製品とプロセスが量的にコントロールされている
- Level 5: 最適化されたレベル(Optimized) – プロセスの改善の継続; プロセス改善が制度化されている

6.3 アプリケーション開発方法論(Application Development Methodology)

6.3.1 言語のタイプ(Types of languages)

マシン語(Machine language): コンピュータやプロセッサが直接理解して処理できる.
アセンブリ言語(Assembly language): システムは直接理解できないので処理されてマシン語に変換される.
高級言語(High-level language): システムは直接理解できないので処理されてマシン語に変換される.

6.3.2 プログラム(Programs)

インタープリタ型プログラム(Interpreted programs): プログラムによって命令が 1 つずつ読まれ解釈される.
コンパイルされたプログラム(Compiled programs): 高級言語で書かれコンパイラと呼ばれるプログラムによってマシンが読める形式に変換される.

6.3.3 OOP / オブジェクト指向プログラミング(Object-Oriented Programming)

クラスおよびクラス内のオブジェクトを使用する.

クラスが定義されると, 作成されたクラスのメンバーやインスタンスのために属性が再利用される.
オブジェクトは属性値をカプセル化する. すなわち, この情報は 1 つの名前の元にパッケージ化されて他のオブジェクトによって 1 つのエンティティーとして再利用される.
オブジェクトには共通部分が存在する- 他のコンポーネントと相互作用するインターフェイス
オブジェクトにはプライベートな部分が存在する- 実際にどのように動くか, リクエストされたオペレーションをどのように実行するか
インターフェイスから入力されたメッセージが, リクエストされて実行されるオペレーションやメソッドを特定する.
情報隠蔽(Information hiding) – 他のコンポーネントは, それぞれのオブジェクトが内部でどのように動くかについて知っている必要はない.
抽象化(Abstraction) – 不必要な詳細を隠し, 重要な継承プロパティが吟味・レビューされるようにする機能

6.3.4 オブジェクト指向のフェーズ(Phases of object-orientation)

OORA / オブジェクト指向要件分析(Object-Oriented Requirements Analysis) -
オブジェクトのクラスとその相互作用を定義する.
OOA / オブジェクト指向分析(Object-Oriented Analysis)
オブジェクト指向の概念においては, 問題ドメイン内の特定の問題を理解しモデリングする.
DA / ドメイン分析(Domain Analysis)
与えられたドメイン内の全てのアプリケーションに共通するクラスとオブジェクトを特定する.
OOD / オブジェクト指向デザイン(Object-Oriented Design)
オブジェクトはモジュールの基本単位; オブジェクトはクラスのインスタンス.
OOP / オブジェクト指向プログラミング(Object-Oriented Programming)
他のプログラミングアプローチのようなタイプや変換ではなくオブジェクトやメソッドの採用を強調する.

6.3.5 OOP の特長

カプセル化(Encapsulation) – 内部データとオペレーションを隠す.
多相性(Polymorphism) – オブジェクトのコピーを作成し, これらのコピーに変更を加える.
Polyinstantiation – オブジェクト内のデータ間の違いにより, 低いセキュリティレベルのサブジェクトが高いセキュリティレベルの情報を知ることのないようにする.
継承(Inheritance) – プロパティと属性を共有する.
多重継承(Multiple inheritance) – あるクラスが複数の親クラスから動作特性を継承する状態.
委譲(Delegation) – オブジェクトからのリクエストを他のオブジェクトに転送もしくは委譲すること. この転送は, リクエストを受け取ったオブジェクトがリクエストにサービスするためのメソッドを持ってない場合に必然となる.

6.3.6 データモデリング(Data Modelling)

構造化分析アプローチ(Structured analysis approach):
アプリケーション内の全てのオブジェクトとサブジェクトを見て, 関係, コミュニケーションパス, 継承プロパティーをマッピングする.
データモデリング(Data modelling):
データが処理される方法やコンポーネントとは独立してデータを考える.

6.3.7 データ構造(Data Structures)

データ構造(Data Structure):
データエレメント間の論理的関係の表現.
凝集性(Cohesive):

凝集性のあるモジュールは, 他のモジュールの助けをほとんどもしくは全くなくてもあるタスクを実行できる
- 低凝集性(Low Cohesion): 分散していて複数のタスクを実行する.
- 高凝集性(High Cohesion): 1 つのタスクに集中する.
最適なプログラミングではできる限り凝集性の高いモジュールを使用するが, 異なるモジュールはデータをやり取りしコミュニケートしなければならないため, 通常は完全に凝集的にはならない.
結合(Coupling):
アプリケーション内のモジュール間の相互結合の尺度.
- Low Coupling: 独立したモジュール.
- High Coupling: 他のモジュールに依存する
結合土が低いほどよりよいソフトウェアデザインである. なぜならモジュールが独立だからである. コンポーネントが独立であるほどアプリケーションが簡潔で, 変更やトラブルシューティングが容易である.

6.3.8 OMA / オブジェクト管理アーキテクチャー(Object Management Architecture)

ORB / オブジェクトリクエストブローカ(Object Request Brokers):
コンポーネント間の全てのコミュニケーションを管理し, 異質で分散した環境において相互に作用しあうことを可能にする.
CORBA / Common Object Request Broker Architecture:
異なるソフトウェア, プラットフォーム, ハードウェア環境における相互運用性を提供する.
場所や開発者に関わらず, アプリケーションが相互にコミュニケートできるようにする. この互換性を実現するために, ユーザは小さな初期コードとインターフェイス定義言語(Interface Definition Language, IDL)を開発する.
COM / 共通オブジェクトモデル(Common Object Model):
プログラム間でのオブジェクトの交換をサポートする.
DCOM / 分散型共通オブジェクトモデル(Distributed Common Object Model):
ネットワーク環境でオブジェクトを共有するための標準を定義する.
環境内のユーザ, リソース, コンポーネントを一意に識別するために, グローバルでユニークな識別子である GUID を使用する.
ODBC / オープンデータベース接続(Open Database Connectivity):
様々なタイプのリレーショナルデータベースへの接続に使われる標準 SQL を提供する.
DDE / 動的データ交換(Dynamic Data Exchange):
IPC を提供することにより異なるアプリケーションでデータを共有する.
2 つのアプリケーション間での直接対話を可能にするコミュニケーションメカニズム.
DCE / 分散コンピューティング環境(Distributed Computing Environment):
RPC を元にした, コミュニケーションレイヤを持つ管理サービスの集合.
ネットワーク層の上にあるソフトウェアのレイヤで, その上のアプリケーションにサービスを提供する.
ユニバーサル一意識別子(UUID)を使用し, 環境内のユーザ, リソース, コンポーネントをユニークに識別する.
RPC 関数はプログラムを送りネットワーク越しに送信するために準備することによって, 引数とコマンドを収集する.
DFS(Distributed File Services, 分散ファイルサービス) が, 全ての DCE ユーザが共有するために使用する単一の統合されたファイルシステムを提供する.

6.3.9 エキスパートシステム(Expert systems) / 知識ベースシステム(knowledge based systems)

人工知能を使用し人間の知識をエミュレートして問題解決する.
知識ベースとアルゴリズムセットとルールを持ち, 知識と入ってきたデータから新しい事実を推論するために使用されるコンピュータプログラム.

- ルールベースプログラミング(Rule-based programming): エキスパートシステムの一般的な開発手法である.
- パターンマッチング(Pattern matching): if-then ロジックユニットに基づく.
- 推論エンジン(Inference engine): 自動的に事実をパターンにマッチングさせ, どのルールが当てはまるかを決定するメカニズム.

6.3.10 人工ニューラルネット(Artificial Neural Networks)

脳のニューラル構造に基づいた電子モデル.
ニューロンとその回路の基本的な機能を模倣して新しい方法で問題を解決しようとしている.

6.3.11 Java

プロセッサに依存しない中間コードであるバイトコードを生成するのでプラットフォームに依存しない. Java 仮想マシンはバイトコードをマシン語に変換する.
Java アプレットは, アプレットのアクセスをユーザシステムの特定の領域にのみ制限したサンドボックスを採用したセキュリティスキームを使用しているので, 不正やアプレットの不具合から守られる.

6.3.12 ActiveX

マイクロソフトの技術で, インターネットユーザがダウンロードして機能やインターネット体験を強化するためのコントロールを書くために使用される.
プログラムがどこから来たかをユーザに知らせることによりセキュリティを守っている. 電子証明と信頼された認証局に依存したコード署名技術を使用している.

6.3.13 不正なコード(Malicious Code)

ウイルス, ワーム, トロイの木馬, 論理爆弾等
以下によって検知される:
- ファイルサイズの増加
- 予期しない多くのディスクアクセス
- 更新・変更日時の変更

6.3.14 ウイルス(Virus)

他のプログラムを探して自らのコピーを埋め込んで感染するプログラム. 感染したプログラムが実行されると埋め込まれたウイルスが実行され感染が広がる.
- ブートセクターウイルス(Boot sector virus): データをブートセクターに移動するか, 新しい情報で上書きする
- ステルスウイルス(Stealth virus): ファイルやブートレコードに施した変更を隠す.
- ポリモーフィック型ウイルス(Polymorphic virus): 自らと異なるが動作はするコピーを作成する.
- マルチパートウイルス(Mulitpart virus): ハードディスクのブートセクターおよび実行ファイルに感染する.
- セルフガーブリングウイルス Self-garbling virus: 自らのコードを変造してアンチウイルスソフトウェアから隠そうとする. ウイルスが広まるにつれてコードのエンコード方法が変化する.

6.3.15 ワーム(Worm)

ホストアプリケーションがなくとも自分自身で再生成される自己完結型プログラム.

6.3.16 論理爆弾(Logic bomb)

あるイベントが発生したときにプログラムやコードストリングを実行する.

6.3.17 トロイの木馬(Trojan horse)

他のプログラムとして偽装されたプログラム.

6.4 攻撃(Attacks)

6.4.1 DoS / サービス拒否(Denial of Service)

攻撃者は被害者の帯域やリソースを消費しシステムのクラッシュを引き起こしたり他のパケットの処理を妨害したりする.

6.4.2 Smurf

3 者必要である: 攻撃者, 被害者, 増幅用ネットワーク
攻撃者はパケットヘッダの送信元 IP アドレスをスプーフもしくは変更し, ICMP ECHO パケットが被害者のシステムから送信されたように偽装する. この ICMP ECHO メッセージは増幅用ネットワークにブロードキャストされ, 返答が返される. これにより被害者のシステム・ネットワークは使用できなくなる.

6.4.3 Fraggle

UDP を武器として選択する.攻撃者はスプーフされた UDP パケットを増幅用ネットワークにブロードキャストし, その返答は被害者のシステムに返される.

6.4.4 SYN Flood

スプーフされたパケットで SYN メッセージを継続的に送信する. 被害者はこのコミュニケーションソケットに必要なリソースを割り当て, SYN/ACK メッセージを返し, ACK メッセージを待つ.

6.4.5 Teardrop

攻撃者は, システムがフリーズもしくはリブートするような非常に小さいパケットを送信する. いくつかのシステムではパケットが大きすぎないかについてはチェックしないが, 小さすぎないかについてはチェックしないために起きる.

6.4.6 DDoS / 分散サービス拒否(Distributed Denial of Service)

DoS の論理的な拡張.
攻撃者はスレーブ/ゾンビマシンをコントロールするマスターコントローラーを構築する

6.4.7 DNS DoS 攻撃(DNS DoS Attacks)

偽の IP アドレスを指す新しいレコードで DNS サーバのレコードを入れ替える.
キャッシュ汚染(Cache poisoning) – 実際のレコードを入れ替えるのではなくサーバのキャッシュにデータを挿入する.

7 CBK#5 暗号(Cryptography)

7.1 定義(Definitions)

アルゴリズム(Algorithm): 暗号化および復号に使用される数学的法則の集合.
暗号法(Cryptography): データを意図した個人にのみ利用可能な形でデータを保存・送信することができるようにする科学.
暗号システム(Cryptosystem): メッセージを暗号化したり復号したりする, ハードウェア・ソフトウェアによる暗号の実装.
暗号解読(Cryptoanalysis): 暗号文から鍵なしで平文を得たり, 暗号を破ったりすること.
暗号理論(Cryptology): 暗号法と暗号解読の学問.
暗号文(Ciphertext): 暗号化され読むことができないフォーマットのデータ.
暗号化(Encipher): データを読むことができないフォーマットへ変換すること.
復号(Decipher): 読むことができるフォーマットにデータを変換すること.
鍵(Key): 秘密のビット列や命令で, 暗号化・復号にとって重要な物.
キークラスタリング(Key clustering): 2 つの異なる鍵が 1 つの平文から同じ暗号文を生成すること.
キースペース(Keyspace): 鍵の構築に使用できる値.
平文(Plaintext): 読むことができるフォーマットのデータ. “Cleartext”とも呼ばれる.
ワークファクター(Work factor): ある暗号システムを破るための時間, 手間, リソースの推定値.

7.2 暗号のタイプ(Types of ciphers)

換字式暗号(Substitution cipher): ビット, 文字, 文字ブロックを他のビット, 文字, 文字ブロックで置き換える.
転置式暗号(Transposition cipher): 置換が使用される. すなわち文字の順序がスクランブルされる. 鍵は, 文字の移動先を決める.
頻度分析(Frequency analysis): メッセージや会話で使用された文字の頻度パターンを分析する.
Running key cipher: 本(ページ, 行数, 語数)のような我々の周りの物理世界のステップを使用する. それぞれの単語はシーケンス番号によって示される.
Concealment cipher: テキスト内の単語の全ての X 番号は真のメッセージの一部である.
ステガノグラフィー(Steganography): データを他のメッセージの中に隠し, データの存在を隠すこと. メッセージは wave ファイル, 画像, ハードディスクの未使用領域, 使用不能とマークされたセクターに隠される.
クリッパーチップ(Clipper chip): NSA が設計した, データ暗号化用チップで, 不正使用できないようになっている. スキップジャック(Skipjack)アルゴリズムを使用している. クリッパーチップ毎に一意のシリアルナンバーがあり, ユニットキーのコピーはこのシリアルナンバーでデータベースに格納される. 送信側のクリッパーチップは LEAF(Law Enforcement Access Field)値を生成して送信メッセージに含めて送る. 80 ビット鍵と 16 ビットチェックサムに基づいている.
鍵寄託(Key Escrow): ユニットキーが 2 つのセクションに分けられ 2 つの異なる寄託エージェンシーが維持する.
Fair cryptosystems: 復号に必要な鍵を分ける. この方法は公開鍵を使うソフトウェア暗号における手法であり, ハードウェア暗号チップが使用されている場合には鍵寄託を使用する.

7.3 暗号の手法(Methods of Encryption)

7.3.1 対称暗号(Symmetric Cryptography)

暗号化と復号で同じ鍵を使用する. 提供できるのは機密性のみである. 速く, また解読が困難である.
長所- 非対称システムに比べて非常に速い. 鍵サイズが大きいと解読が難しい

短所 – 鍵配布(鍵を適切に渡すのにセキュアなメカニズムが必要) / スケーラビリティー(ユーザの組毎にユニークな鍵が必要) / セキュリティの制限 (機密性しか提供できない)
帯域外(Out-of-band method): 鍵はメッセージとは異なるチャネルを通じて送信される.

7.3.2 非対称アルゴリズム(Asymmetric Algorithms)

2 つの異なる非対称な鍵が数学的な関係を持つ. これを公開鍵と秘密鍵と呼ぶ.
長所- 対称システムに比べて鍵配布の点で優れている/ 対称システムに比べてスケーラビリティーがある/ 機密性, 認証, 否認防止機能も提供する
セキュアメッセージフォーマット(Secure message format) – 受信者の公開鍵で暗号化する
オープンメッセージフォーマット(Open message format) – 送信者の秘密鍵で暗号化する
セキュアアンドサインドフォーマット(Secure and signed format) – 送信者の秘密鍵で暗号化し, それを受信者の公開鍵で暗号化する

7.4 2 種類の対称鍵アルゴリズム(Two types of symmetric algorithms)

7.4.1 ストリーム暗号(Stream ciphers)

メッセージをビットやバイトのストリームとして扱い, それぞれに対して数学的処理を行う. 鍵はストリーム暗号へのランダム値入力で, これにより鍵ストリームデータのランダム性が保証される. 一度に 1 ビットずつ暗号化・復号を行うので, ハードウェア実装により適している. ビットそれぞれが処理されるので集中的であり, シリコンレベルでの処理が適している.

強度が高く効率的な暗号アルゴリズムの特徴- 鍵ストリーム値が長期間反復されない/ 統計的に予測不可能/ 鍵ストリームは鍵と線形の関係がない/ 統計的に鍵ストリームにバイアスがない(0 と 1 の数が同程度)
鍵ストリーム生成器(Key stream generator) – 暗号文を生成するために平文に XOR 処理されてビットストリームを生成する.

7.4.2 ブロック暗号(Block ciphers)

メッセージがビットのブロックに分けられる. 拡散(diffusion)と混乱(confusion)を使用する. それぞれのステップで S ボックス(S-box, substitution box)を使用する. これは, 平文に対してどの関数がどの順序で適用されるかを決定する鍵である. 通常データバスの幅(64 ビット)と等しいデータブロックを処理するために, ソフトウェアでの実装に適している. ブロック暗号はストリーム暗号をエミュレートするモードでも実行されることがある.

混乱(Confusion) – 異なる未知の鍵値が使用される.
拡散(Diffusion) – 多くの異なる関数を通じて平文にビットを挿入する. これによりアルゴリズムを通じて分散される.
S ボックス – ビットをどのように順序を変えるか, 移動するかについての指示をする参照テーブルを持つ. 復号処理で使用される鍵はどの S ボックスをどの順序で使用するかを決定する.

7.5 対象鍵システムのタイプ(Types of symmetric systems)

7.5.1 データ暗号標準(Data Encryption Standard, DES)

NIST が承認したアルゴリズムで, IBM の 128 ビットアルゴリズム Lucifer を基にしている. ブロック暗号アルゴリズムで, 入力・出力共に 64 ビットである. 56 ビットが実際の鍵で 8 ビットがパリティに使われる. 64 ビットのブロックが半分に分けられそれぞれの文字が一度に暗号化される. 文字は 16 ラウンドの転置と置換関数で処理される. 動作には 4 つの異なるモードがある:
ECB モード/ 電子コードブック(Electronic Code Book) – もともとの暗号モード. 平文に対して換字と置換が行われる. ファイル内のデータは一定の順序で暗号化される必要はない. チャレンジ・レ

スポンスや鍵管理タスク等の小さいデータに使用される. また ATM 機の PIN の暗号化にも使用される.
CBC mode / 暗号ブロック連鎖(Cipher Block Chaining) –前のブロックの値が次のブロックのテキストに重ねあわせられる.
CFB Mode / 暗号フィードバックモード(Cipher Feedback Mode) – 最後の暗号化されたブロックが乱数を生成するためのアルゴリズムで処理される. この乱数が現在処理している平文のブロックに対して使用されて暗号文を作成する. このモードは個々の文字が必要なときに使用される.
OFB Mode / 出力フィードバック(Output Feedback) - 暗号文を生成するために平文と組み合わせられるランダムなバイナリビットのストリームが生成され, ストリーム暗号のように働く. 暗号文はアルゴリズムに戻され, 次のビットストリームを暗号化するための一部を形成する.
DEA – データ暗号化アルゴリズム(Data Encryption Algorithm)
FIPS – 連邦政府情報処理規格(Federal Information Processing Standard)

7.5.2 Triple-DES (3DES)

計算に 48 ラウンドかかる. パフォーマンスが重く, 暗号化や復号に最大で DES の 3 倍の時間がかかる.

7.5.3 Advanced Encryption Standard (AES)

NIST の DES に代わる標準. ラインダールが優勝した. これは可変ブロック長と可変鍵長のブロック暗号である.
3 つの不可逆変換の層から成る循環変換を採用している.: 非線形層(The non-linear layer) / 線形混合層(the linear mixing layer) / 鍵加算層(the key addition layer). 地域制限のない高速チップやスマートカード上の小さなプロセッサに適している.
International Data Encryption Algorithm (IDEA):
64 ビットブロックで処理するブロック暗号. 鍵長は 128 ビット. 64 ビットのデータブロックは 16 の小さなブロックに分けられ, それぞれが 8 ラウンドの数学関数で処理される PGP 暗号ソフトウェアで使用されている.
Blowfish:
64 ビットブロックで処理するブロック暗号. 鍵長は 448 ビットまでで, データブロックは 16 ラウンドの暗号関数で処理される.
RC5:
ブロック暗号で, 様々なブロック長, 鍵長, ラウンド数が使用できる. ブロックサイズは 32/64/128 ビット, 鍵長は 2048 ビットまで.

7.6 非対称鍵システムのタイプ(Types of asymmetric systems)

7.6.1 RSA

認証(電子署名)と暗号化を提供する. このセキュリティは大きな数の因数分解が困難であることに由来する. 2 つのの大きな素数から作成される.
SSL と共に多くのウェブブラウザで使用されている. また, PGP や公開鍵暗号システムを採用している政府システムでも使用されている.

7.6.2 エルガマル(El Gamal)

電子署名と鍵交換に使用される. 有限体上の離散対数計算に基づく.

7.6.3 楕円曲線暗号システム(Elliptic Curve Cryptosystem , ECC)

電子署名, セキュアな鍵配布, 暗号化を提供する. 他のシステムに比べてリソースが少なくてすむ. 公開鍵システムの楕円曲線の性質に基づいている.

7.7 ハイブリッド暗号方式(Hybrid Encryption Methods)

7.7.1 公開鍵暗号(Public Key Cryptography)

非対称暗号アルゴリズムによって生成された 2 つの鍵を使用して, 暗号化鍵と鍵配布を保護する. 秘密鍵は対称暗号アルゴリズムによって生成され, 大量の暗号化に使用される.
- 非対称暗号アルゴリズムは公開鍵と秘密鍵を使用して暗号化・復号を行う.
- 対称暗号アルゴリズムは秘密鍵を使用して暗号化・復号を行う.
- 秘密鍵は実際のメッセージを暗号化するのに使用される
- 秘密鍵は対称鍵の別称
- 非対称鍵は公開鍵もしくは秘密鍵のことを指す.

Diffie-Hellman 鍵交換(Diffie-Hellman Key Exchange)
公開鍵暗号の考えを最初に紹介した. 鍵配布に使用され, メッセージの暗号化や復号はできない.
セッション鍵(Session keys)
2 人のユーザ間のメッセージを暗号化するのに使用される秘密鍵. 1 つのセッションでのみ有効.

7.8 対称鍵システム対非対称鍵システム

属性	対称鍵	非対称鍵
鍵	2 つ以上のエンティティーが 1 つの鍵を共有する	一方のエンティティーが公開鍵を持ち, 他方が秘密鍵を持つ
鍵交換	帯域外	秘密鍵は暗号化されメッセージと一緒に送られる. つまり鍵は帯域内で配布される.
速度	アルゴリズムが複雑でなく速い.	アルゴリズムが複雑で襲い
鍵長	固定長	可変長
用途	大量の暗号, すなわちファイルの暗号化やコミュニケーションパス.	鍵暗号化および鍵配布.
提供できるセキュリティ	機密性と保全性	機密性, 保全性, 認証, 否認防止

7.9 公開鍵基盤(Public Key Infrastructure, PKI)

電子証明書(Digital certificate) – 他の識別情報と共に個人の公開鍵を含む証明書.
認証局(Certificate authority, CA) – 公開鍵証明書を維持・発行する組織.
証明書失効リスト(Certificate revocation list, CRL) – 何らかの理由により無効になった証明書全てのリスト. このリストは定期的に整備される.
証明書(Certificate) – 公開鍵を, 所有者と主張する人とユニークに認証するのに十分な要素と結び付けるために使用されるメカニズム.
登録局(Registration authority, RA) – 証明書登録業務を行う.
PKI のエンティティーと機能 - CA / RA / 証明書リポジトリ(certificate repository) / 証明書失効システム(certificate revocation system) / 鍵のバックアップ・回復システム(key backup and recovery system) / 自動鍵更新(automatic key update) / 鍵履歴管理(management of key histories) / 他の CA との相互認証(cross-certification with other CAs) / タイムスタンプ(timestamping) / クライアントソフトウェア(client-side software)
PKI が提供するもの- 機密性 / アクセスコントロール / 完全性 / 認証

7.10 一方向関数(One-way function)

一方向の計算が逆方向に比べ用意であるような数学関数.

トラップドア一方向関数(Trapdoor one-way function) – 公開鍵暗号の基になっているもの. 公開鍵は暗号化を行い, 秘密鍵(トラップドア)は復号を行う

7.11 メッセージ完全性(Message integrity)

一方向ハッシュ(One-way hash)
可変長メッセージを圧縮してハッシュ値と呼ばれる固定長の値に変換する関数..
メッセージダイジェスト(Message digest) – 一方向ハッシュのハッシュ値
公開鍵暗号では一方向関数が使用されている
機能- 逆方向には実行できない/ メッセージの完全性を提供するが, 機密性, 認証は提供しない. / 一方向ハッシュの結果はハッシュ値である / メッセージの指紋(fingerprint)を作成するためのハッシュ計算に使用される.
電子署名(Digital signatures)
暗号化された, メッセージのハッシュ値
デジタル証明標準(Digital signature standard, DSS)
電子署名およびその機能や容認できる使用についての標準. 電子署名アルゴリズム(Digital Signature Algorithm, DSA)とセキュアハッシュアルゴリズム(Secure Hash Algorithm, SHA)を必要とする.

7.12 他のハッシュアルゴリズム

MD4 – 128 ビットのハッシュ値を生成する. ソフトウェア実装で高速計算に用いられ, マイクロプロセッサに最適化されている.
MD5 - 128 ビットのハッシュ値を生成する. MD4 より複雑. テキストを 512 ビットのブロックで処理する.
MD2 - 128 ビットのハッシュ値を生成する. MD4 や MD5 より遅い.
SHA – 160 ビットのハッシュ値を生成する. メッセージの署名を計算する DSA に入力される. メッセージ全体ではなくメッセージダイジェストが署名される.
SHA1—SHA の更新版.
HAVAL – 可変長の一方向ハッシュ関数で MD5 の改良版. テキストを 1024 ビットのブロックで処理する.

7.12.1 一方向関数に対する攻撃

衝突(Collision) – あるアルゴリズムによって 2 つの異なるメッセージに対して同じ値を生成すること.
誕生日攻撃(Birthday attack) – 総当たりによるハッシュ関数への攻撃. 攻撃者は同じハッシュ値を持つ 2 つのメッセージを見つけようとする

7.12.2 使い捨て方式(One-time pad)

破ることが不可能で, pad は一度しか使用されない
繰り返しのないランダムビットセットを使用し, 暗号文を生成するためにメッセージにビット毎の XOR 処理を行う.
ランダム鍵はメッセージと同じ長さで 1 回しか使用されない.
乱数のパッドを必要とする人全てに配布するのが難しい.

7.13 鍵管理(Key Management)

Kerberos – 暗号化に使用するセッション鍵を鍵発行局(key distribution center, KDC)が保存, 配布, 維持する.
Diffie-Hellman – 鍵交換アルゴリズム (key exchange algorithm, KEA)を使用する.

7.13.1 鍵管理の原則(Key Management principles)

暗号デバイスの外では平文であってはならない.

バックアップコピーを作成し, 必要なときに簡単に使えるようにしておく.
緊急時の鍵復元のために, 複数人のコントロールを選択することも出来る. すなわち鍵を復元する必要があるときに, 復元プロセスを行うのに複数の者が必要である.

7.13.2 鍵および鍵管理のルール

- 必要なレベルの保護を行う為に鍵長は十分長くなければならない.
- 鍵の保管や送信はセキュアな方法で行わなければならない.
- 鍵は非常にランダムでキースペースの全範囲を使用していなければならない.
- 鍵の寿命は保護すべきデータの機密性に対応していなければならない.
- 鍵が使用される頻度が高いほど, 寿命は短くなければならない.
- 鍵は非常事態のためにバックアップするか鍵寄託を利用するべきである.
- 鍵の寿命が来た場合は適切に破壊しなければならない.

7.14 リンク暗号化と終点間暗号化(Link versus end-to-end encryption)

7.14.1 リンク暗号化(Link encryption)

衛星リンク, T3, 電話回線などのような特定のコミュニケーションパスにおいて全てのデータを暗号化する.
パケットの一部であるユーザ情報, ヘッダ, トレーラ, アドレス, ルーティングデータ等も暗号化される.
パケットスニファや盗聴に対する防御となる.
ホップ毎にパケットが復号され, また暗号化される.
物理レベルで行われる.

7.14.2 終点間暗号化(End-to-end encryption)

情報のみが暗号化される.
通常, 送信元のコンピュータのアプリケーション層において初期化される.
送信元から送信先まで暗号化されたままである.
それぞれのアプリケーションやユーザは異なる鍵を用いることにより高いグラニュラリティの暗号化が行える.

7.15 電子メイル標準

7.15.1 プライバシー強化メイル(Privacy-enhanced mail, PEM)

認証, メッセージの完全性, 暗号化, 鍵管理の機能を持つ.
使用されるコンポーネント:
- CBC モードの DES でメッセージが暗号化される
- 認証は MD2 もしくは MD5 で行われる
- 公開鍵管理は RSA によって行われる
- X.509 標準が証明書構造とフォーマットに使用される

7.15.2 メッセージセキュリティプロトコル(Message Security Protocol, MSP)

メッセージに署名して暗号化し, ハッシュ関数を実行する.

7.15.3 Pretty Good Privacy (PGP)

最初に普及した公開鍵暗号システム
鍵管理に RSA 公開鍵暗号を使用し, データの大量暗号化には IDEA 対称暗号を使用している.
PGP ではパスフレーズが使用され, これはユーザのハードディスクに保存される, ユーザの秘密鍵を暗号化するのに使用される.
鍵管理アプローチは「信用の輪(web of trust)」に依存している.

鍵リング(Key ring) – 他のユーザから受け取った, 署名された公開鍵を集めたものをそれぞれのユーザが持っている.

7.16 インターネットセキュリティ

7.16.1 HTTP

TCP/IP の最上位に位置する
ステートレスなプロトコルで, クライアントとウェブサーバは操作毎に接続を確立し, 切断する.

7.16.2 S-HTTP – セキュアハイパーテキスト転送プロトコル(Secure Hypertext Transport Protocol)

セキュアなコミュニケーションを提供するために開発された.
計算によって得られたセッション鍵でメッセージを暗号化する.
完全性と送信者の認証機能を持つ.
ステートレスなプロトコルではない
複数の暗号化モードおよびタイプをサポートする.
公開鍵技術と対称暗号を使用できる.
個々のメッセージの暗号化が必要なときに使用される.

7.16.3 HTTPS

2 つのコンピュータ間のコミュニケーションを保護する.
クライアントとサーバ間の保護された回線を提供するために SSL と HTTP を使用する.
2 つのコンピュータ間の全ての情報の暗号化が必要なときに使用される.

7.16.4 SSL – セキュアソケットレイヤー(Secure Sockets Layer)

コミュニケーションチャネルを保護する.
公開鍵暗号を使用する.
データ暗号化, サーバ認証, メッセージの完全性, 最適なクライアント認証を提供する.
どちらかがセッションを終了させるリクエストをするまでコミュニケーションパスは開いている.
アプリケーション層の下でトランスポート層の上に位置する.

7.16.5 MIME – 多目的インターネットメイル拡張(Multipurpose Internet Mail Extension)

マルチメディアデータおよび電子メイル添付を送信する方法を示す.

7.16.6 S/MIME – セキュア MIME(Secure MIME)

電子メイルの暗号化と電子署名の標準で, ファイル添付とセキュアなデータ伝送機能を持つ.
暗号化アルゴリズムによって機密性を,ハッシュアルゴリズムによって完全性を, X.509 公開鍵証明書によって認証を, 署名されたメッセージによって否認防止を提供する.

7.16.7 SET – セキュアエレクトロニックトランザクション(Secure Electronic Transaction)

クレジットカード番号を暗号化して送信するために開発された.
3 つの主な部分から成る: 電子財布, 店側のウェブサイトのサーバ上で実行されているソフトウェア, および店の取引銀行にある支払サーバである.

7.16.8 クッキー(Cookies)

ユーザのハードディスクにブラウザが持つテキストファイル.
人口統計学的に, 宣伝用情報に使用される
ユーザとサーバ間のセッションの制限時間を適用するのにも使用される.
重要な情報を含んだクッキーは, 送信するサーバ側で暗号化されるべきである.

7.16.9 SSH – セキュアシェル

リモートコンピュータへのターミナルアクセスを手興する, トンネリングメカニズムとして機能する.
telnet, ftp, rlogin rexec, rsh の代わりに使用すべきである.
2 つのコンピュータがハンドシェイクをして, セキュアなチャネルが確立される.

7.16.10 IPSec – インターネットプロトコルセキュリティ(Internet Protocol Security)

2 つのデバイス間のデータ交換を保護するためのセキュアチャネルを確立する手法.
セキュアなネットワーク層通信のための, 広く受け入れられた標準である.
公開鍵暗号を採用し, 強力な暗号と認証方法を持つ.
VPN を確立するために使用される.
オープンでモジュール構成のフレームワークなので, 柔軟性がある.
2 つの基本的なセキュリティプロトコルがある:
- AH – 認証ヘッダ(Authentication Header): 認証プロトコル.
- ESP – 暗号ペイロード(Encapsulating Security Payload): 認証と暗号化のプロトコルで, 送信元認証, 機密性, メッセージの完全性を提供するために暗号メカニズムを使用している.

2 つのモードで動作する:
- トランスポートモード(Transport mode): メッセージのペイロードが暗号化される
- トンネルモード(Tunnel mode): メッセージのペイロード, ルーティング, ヘッダ情報が暗号化される

SA – セキュリティアソシエーション(Security association) – 認証および暗号化鍵, 使用するアルゴリズム, 鍵の有効期限, 送信元 IP アドレスを持つ. それぞれの接続に 1 つの SA が対応する.
SPI – セキュリティパラメータインデックス(Security parameter index) – 異なる SA を追跡し, デバイスにどの SA を呼び出すかを伝えるインデックス.
ISAKMP – インターネットセキュリティアソシエーションおよび鍵管理プロトコル(Internet Security Association and Key Management Protocol) – 認証と鍵交換アーキテクチャーで, 使用される鍵メカニズムには依存しない.

7.17 攻撃

7.17.1 暗号文攻撃(Ciphertext-only attack)

攻撃者は複数のメッセージの暗号文を持っている. それぞれのメッセージは同じ暗号化アルゴリズムを用いて暗号化されている.

7.17.2 既知平文攻撃(Known-plaintext attack)

攻撃者は 1 つもしくは複数のメッセージの平文および暗号文を持っている.

7.17.3 選択平文攻撃(Chosen-plaintext attack)

攻撃者者平文と暗号文を持っており, 暗号化する平文を選択することが出来る.

7.17.4 選択暗号文攻撃(Chosen-ciphertext attack)

攻撃者は復号する暗号文を選択し, 復号されて得られた平文にアクセスできる.

7.17.5 仲介者攻撃(Man-in-the-middle attack)

他の会話を盗聴する. 電子署名をセッション鍵交換に使用することにより, 攻撃を回避することが出来る.

7.17.6 辞書攻撃(Dictionary attacks)

パスワードファイルを一方向関数にかけ, 一方で一般によく使用されるパスワードのリストを同じ一方向関数にかける. そしてこれらのファイルを比較する.

7.17.7 リプレイ攻撃(Replay attack)

攻撃者はチケットをコピーしてその暗号化を破る. そして後からそのクライアントのふりをしてチケットを再送し, 許可されていないリソースへのアクセスを得る.

8 CBK#6 セキュリティ構造とモデル(Security Architecture & Models)

8.1 セキュリティモデル(Security Model)

特定のセキュリティポリシーを適切にサポートするための要件を概説するもの.

8.2 コンピュータアーキテクチャー(Computer Architecture)

8.2.1 CPU – 中央演算装置(Central Processing Unit)

マイクロプロセッサである.
制御ユニット, 整数論理演算ユニット(ALU, Arithmetic Logic Unit), 主記憶装置(primary storage)を持つ.
CPU が必要とする命令とデータは主記憶装置に保持される.
主記憶装置は命令を保持する一時記憶領域で, 命令は CPU が解釈しデータ処理をする.
バッファーオーバーフロー(Buffer overflow) – 処理されるデータはブロック単位で CPU に入力される. ソフトウェア命令において入力されるデータのブロックの大きさを適切に設定されていないと, 余分なデータが入り込み実行されてしまう.
実記憶装置(Real storage) – 命令とデータが処理されると, システムの記憶領域, 実記憶装置に移動される.

8.2.2 メモリ(Memory)

RAM / ランダムアクセスメモリ(Random Access Memory) – 電源が切れると内容が消える揮発性メモリである.
RAM のタイプ:
- スタティック RAM(Static RAM) – データを保存すると, 継続的にフラッシュしなくても保持されている.
- ダイナミック RAM(Dynamic RAM) – 電荷が漏洩し減少していくため, 保存されているデータを定期的にリフレッシュする必要がある.
ROM / リードオンリーメモリー(Read-only memory) – 不揮発性メモリ. ROM 内に保存されたソフトウェアはファームウェアと呼ばれる.
EPROM / Erasable and programmable read-only memory – 保持しているデータを電気的に消したり書いたりできる.

8.2.3 キャッシュメモリ(Cache memory)

RAM の一部で, 高速な読み書きに使用される.

8.2.4 PLD – プログラマブル・ロジックデバイス(Programmable Logic Device)

プログラミング処理によって変更できるコネクションや内部ゲートを持つ集積回路.

8.2.5 メモリマッピング(Memory Mapping)

実メモリもしくはプライマリメモリ(Real or primary memory) – CPU が直接アクセスできる. 実行されているプログラムに関連する命令やデータの格納に利用される.
セカンダリメモリ(Secondary memory) – より遅いメモリ(磁気ディスク等)で, 不揮発性のストレージを提供する.
順次メモリ(Sequential memory) – その場所に直接アクセスするのではなく, 先頭から順に探すことによって情報が得られる. 磁気テープなど.
仮想メモリ(Virtual memory) – プライマリメモリと協働してセカンダリメモリを使用し, CPU に対して, 実メモリロケーションのように見える大きなアドレススペースを提供する.

8.2.6 メモリアドレッシング(Memory addressing)

レジスタアドレッシング(Register addressing) – CPU 内のレジスタや, 主記憶装置内で指定された特殊目的レジスタをアドレッシングする.
直接アドレッシング(Direct addressing) – メモリ位置の実際のアドレスを特定することにより主記憶装置のある部分をアドレッシングする. メモリアドレスは通常実行されるメモリページか, ページ 0 に制限されている.
絶対アドレッシング(Absolute addressing) – プライマリメモリスペース全てのアドレッシング.
インデックス付きアドレッシング(Indexed addressing) – プログラムの命令で定義されたアドレスの内容を, インデックスレジスタの内容に加えることによりメモリアドレスとする. この, 計算によって出された有効なアドレスが, 要求されたメモリ位置へのアクセスに使用される. したがって, インデックスレジスタがインクリメントあるいはデクリメントされると, メモリ位置の範囲にアクセスできる.
含意アドレッシング(Implied addressing) – プロセッサ内のオペレーションが実行されなければならないとき, 例えば算術操作の結果としてセットされた桁上がりビットをクリアする場合などに使用される. この操作は内部レジスタに対して行わなければならず, また内部レジスタは命令自体の中に指定されるので, アドレスを与える必要はない.
間接アドレッシング(Indirect addressing) – アドレス位置がプログラムの命令内で指定され, 最終的に要求する位置のアドレスを含んでいるときのアドレッシング.

8.2.7 CPU モードとプロテクションリング(CPU Modes and Protection Rings)

プロテクションリング(Protection rings) – それぞれのリング内のどのプロセスがアクセスでき, どのコマンドが実行できるかについての厳格な境界を定める. 内部リング内で動いているプロセス(スーパーバイザーモード/特権モード)は外部リングで動いているプロセス(ユーザモード)よりも多くの権限を持つ.

8.2.8 オペレーションの状態(Operating states)

実行可能状態(Ready state) – アプリケーションは処理を再開する準備ができている.
管理状態(Supervisory state) – システムは, システムもしくは優先順位の高いルーチンを実行している.
問題状態(Problem state) – システムはアプリケーションを実行している.
待ち状態(Wait state) – アプリケーションは特定のイベント, 例えばユーザの文字入力やプリントジョブの完了を待っている..

8.2.9 マルチスレッディング, マルチタスキング, マルチプロセシング(Multi-threading, -tasking, -processing)

マルチスレッディング(Multithreading) – 1 つのアプリケーションが, 異なるスレッドを使用するコールを一度に複数実行できる..
マルチタスキング(Multitasking) – CPU が一度に複数のプロセスやタスクを実行できる.
マルチプロセシング(Multiprocessing) – コンピュータが複数の CPU を持ち, 命令の実行にそれらをパラレルで使用することができる.

8.2.10 入出力装置管理(Input/Output Device Management)

デッドロック状態(Deadlock situation) – 使用後に構造が壊されてリリースされない場合, リソースは他のプログラムやプロセスに使用されなければならない.

8.3 システム構造(System architecture)

8.3.1 TCB – 高信頼コンピューティング基盤(Trusted Computing Base)

コンピュータシステム内のプロテクションメカニズムのトータルな組み合わせとして定義されている. ハードウェア, ソフトウェア, ファームウェアを含む.

オレンジブックに由来する.
オレンジブックでは, 高信頼システムとは, アクセス権やセキュリティポリシーに反することなくユーザのために機密性の高いあるいはそれ以外のデータの完全性を守るための対策を活用するハードウェア, ソフトウェアとして定義されている. システム内の全ての防御メカニズムを網羅して, セキュリティポリシーを施行し, 期待されるように振る舞う環境を提供する.

8.3.2 セキュリティ境界(Security perimeter)

TCB の外部のリソースとして定義される.
機密情報が意図しない方法で流れないようにするために, 信頼されたコンポーネントと信頼されていないコンポーネントとの間のコミュニケーションをコントロールしなければならない.

8.3.3 参照モニタ(Reference monitor)

抽象的な機械で, サブジェクトのオブジェクトに対する全てのアクセスを仲介し, サブジェクトが必要なアクセス権を持った上で許可されないアクセスからオブジェクトを保護して有害な変更から守る.
これはアクセス制御コンセプトであり, 実際の物理的コンポーネントではない.

8.3.4 セキュリティカーネル(Security kernel)

TCB の中のメカニズムから成り, 参照モニタコンセプトを強化する.
TCB の中心部分で, 高信頼コンピューティングシステムを構築するアプローチとして最も一般的に使われる.
3 つの要件:
- 参照モニタコンセプトを実行するプロセスを分離し, 不正防止機能がなければならない.
- 参照モニタは全てのアクセス試行に対して呼び出され, これを回避することができてはならない. したがって, 参照モニタは完全でかつフールプルーフ機能が備わっていなければならない.
- 完全かつ包括的にテスト・検証することができるように十分に小さくなければならない.

8.3.5 ドメイン(Domains)

サブジェクトがアクセスできるオブジェクトの集合として定義される.
実行ドメイン(Execution Domain) – 特権ドメイン内のプログラムは異なるドメイン内のプログラムが環境に悪影響を及ぼさないことを保証しながら命令の実行やデータの処理を行うことができる必要がある.
セキュリティドメイン(Security Domain) – サブジェクトあるいはオブジェクトが割り当てられたプロテクションリングに対して直接の相関を持つ. プロテクションリングの番号が小さいほど特権が高く, セキュリティドメインが大きい.

8.3.6 リソース隔離(Resource isolation)

ハードウェアセグメンテーション(Hardware segmentation) – メモリは論理的にだけでなく物理的にも分離される.

8.3.7 セキュリティポリシー(Security policy)

ルール, 実行, 手順をまとめたもので, 機密情報をどのように管理, 保護, 配布するかについて定めている.
複数レベルセキュリティポリシー(Multilevel security policy) – 高セキュリティレベルから低セキュリティレベルへの情報フローを阻止するセキュリティポリシー.

8.3.8 最小特権(Least privilege)

リソースやプロセスは, 機能を遂行するために必要なレベル以上の特権を持たないということを意味する.

8.3.9 レイヤー化(Layering)

構造化されたヒエラルキー構造で, 基本機能は低いレイヤーで, より複雑な機能は高いレイヤーで処理する.

8.3.10 データ隠蔽(Data hiding)

異なるレイヤーのプロセスがお互いにコミュニケートする必要がない場合にはそのためのインターフェイスを持たない.

8.3.11 抽出(Abstraction)

オブジェクトのクラスが特定のパーミッションを割り当てられ, 受け入れられるアクティビティーが定義される. これによりそれぞれのオブジェクト毎にクラスが扱われないため, 異なるオブジェクトの管理が容易になる.

8.4 セキュリティモデル(Security Models)

セキュリティポリシーを実行するのに必要なデータ構造と技法の仕様を定めることにより, ポリシーの抽象ゴールを情報システムの言葉にマッピングする.

8.4.1 状態機械モデル(State machine model)

システムのセキュリティを検証するために状態が使用される. つまり, 現在のパーミッションおよびオブジェクトにアクセスしているサブジェクトのインスタンスは全て捕らえられなければならない.
状態遷移(State transitions) – 状態を変えることができるアクティビティ.
状態機械モデルを採用したシステムは, その存在の全てのインスタンスにおいてセキュアな状態である. セキュアな状態で起動し, コマンドを実行し, セキュアにトランザクションを行う. また, サブジェクトはセキュアな状態においてのみリソースへのアクセスを許可される.

8.4.2 Bell-LaPadula モデル(Bell-LaPadula model)

システムセキュリティと機密情報の漏洩に関する問題を扱う.
複数レベルセキュリティシステム(Multilevel security system) – Bell-LaPadula モデルを採用したシステムでは, 異なるクリアランスを持つユーザがシステムを使用し, システムは異なる分類のデータを処理する.
情報が分類されるレベルは使用される操作手続きを決め, 格子を形成する.
格子(Lattice) – 認証されたアクセスの下限と上限.
アクセスコントロールの機密性の面を実現する状態機械モデルである.
アクセス制御行列とセキュリティレベルが,異なるオブジェクトへのサブジェクトのアクセス可否を決めるために使用される.
このモデルではサブジェクト, オブジェクト, アクセス操作(読み, 書き, 読み書き), セキュリティレベルが使用される.
情報フローセキュリティモデルで, 情報は下位のあるいは比較できない分類のオブジェクトには流れない.
2 つの主要なルール:
- シンプルセキュリティルール(The simple security rule) – あるセキュリティレベルのサブジェクトはより上位のセキュリティレベルのデータを読むことができない. “no read up”ルールと呼ばれる.
- スタープロパティ(*-property) – あるセキュリティレベルのサブジェクトはより下位のレベルに書き込むことができない. “no write down”ルールと呼ばれる.
セキュアな状態は, セキュアコンピューティング環境と, セキュリティ維持オペレーションによって許可されたアクションとして定義される.
基本セキュリティ定理(Basic Security Theorem) – システムがセキュリティ状態で初期化され, 全ての繊維がセキュアであれば, その後の状態は入力に関わらずセキュアである.
このモデルは機密性を提供するが, システムが保持するデータの完全性は扱わない.

8.4.3 Biba モデル(Biba model)

情報フローモデルで, あるセキュリティレベルから別のセキュリティレベルへの情報フローについて扱う.
状態機械モデルを採用している.
サブジェクトが下位レベルのデータを読むことができるときに脅威となる, データの完全性の問題を扱っている.
あらゆる完全性レベルからのより上位レベルへの情報フローを阻止する.
2 つの主要なルール:
- ”No write up” – サブジェクトはより高いレベルの完全性レベルに書き込むことができない.
- ”No read down” – サブジェクトはより低い完全性レベルのデータを読むことができない.

8.4.4 Clark-Wilson モデル(Clark-Wilson model)

商業アプリケーションにおいて, 許可されたユーザが許可されていないデータの更新, 不正, エラーを行うことを防止することに焦点をあてることにより情報の完全性を守る.
ユーザはオブジェクトに直接アクセスしたり操作したりすることができず, プログラムを通じてオブジェクトにアクセスしなければならない.
また, 操作を様々な部分に分けてそれぞれの部分を別のユーザが行わなければならない職務分離も採用している. このことにより許可されたユーザが許可されていないデータの更新を行うことを防ぎ, 完全性が守られる.
システム外部からの情報を追跡するために監査も必要である.

8.4.5 情報フローモデル(Information flow model)

フローの方向だけでなく, あらゆる種類の情報フローを扱うことができる.
異なるレベル間のフローと共に, 同じレベルやオブジェクト間で起こるセキュアでない情報フローを見る.
不正な情報フローが許可されていない場合にシステムはセキュアである.

8.4.6 非干渉モデル(Non interference Model)

上位セキュリティレベルで行われたアクションが, 下位で行われたアクションに対して影響を与えたり干渉したりすることのないよう保証する.

8.5 運用のセキュリティモード(Security Modes of Operation)

8.5.1 専用セキュリティモード(Dedicated Security Mode)

全てのユーザにクリアランスもしくは承認が与えられており, またシステム内で処理されるデータに関して「知る必要」がある.
全てのユーザには, システム上の情報へのアクセス承認が与えられ, この情報に関して機密保持契約に署名している.
システムでは情報の分類レベルを 1 つ使用することが出来る.

8.5.2 システム高度セキュリティモード(System-High Security Mode)

全てのユーザには, 情報アクセスのためのセキュリティクリアランスもしくは承認が与えられているが, システム内で処理される情報に関して「知る必要」は必ずしもない(データの一部のみ).
全てのユーザには最高レベルのクリアランスが必要だが, ユーザはアクセス制御行列を通じて制限される.

8.5.3 分割セキュリティモード(Compartmented Security Mode)

全てのユーザにはシステムで処理される情報へのアクセスのクリアランスが与えられるが, 「知る必要」や正式なアクセス承認はないかもしれない.

職務を遂行するために必要がないため, ユーザはある程度の情報へのアクセスのみに制限されている. また, ユーザはデータに対する正式なアクセス許可は与えられていない.
コンパートメントはそれぞれのレベルでのサブジェクトのアクセスの回数が制限されているセキュリティレベルである.
CMW / コンパートメント(Compartments) – もし必要なクリアランスを持っているなら, ユーザはデータの複数のコンパートメントを処理することが出来る.

8.5.4 複数レベルセキュリティモード(Multilevel Security Mode)

システムで処理される情報に対する正式なアクセス許可を全てのユーザが持っていないとき, 同時に 2 つ以上の情報分類レベルを処理することを許可する.

8.5.5 信頼と保証(Trust and Assurance)

信頼(Trust) – 顧客に対して, 当該システムにどれくらいのセキュリティを期待できるか, どのレベルのセキュリティが提供されるかについて述べる.
保証(Assurance) – 全てのコンピューティング状況において, システムは正しく, また期待されたように動く.

8.6 システム評価方法(System Evaluation Methods)

システムのうちセキュリティに関連した部分, つまり TCB, アクセス制御メカニズム, 参照モニタ, カーネル, 保護メカニズムを評価する.

8.6.1 オレンジブック(The Orange Book) / TCSEC

TCSEC - Trusted Computer System Evaluation Criteria.
製品について, うたわれているセキュリティプロパティがあるか, 特定のアプリケーションや機能に適切であるかを評価する.
評価においては, システムの機能, 効率性, 保証について調べセキュリティ要件の典型的なパターンを扱うクラスを使用する.
オペレーティングシステムに的を絞っている.

セキュリティレベルのヒエラルキー区分 -
A – 検証された保護(Verified protection)
B – 必須の保護(Mandatory protection)
C – 任意保護(Discretionary protection)
D – 最低限の保護(Minimal security)
トピック – セキュリティポリシー, 責任追跡性, 保証, 文書化
領域 -
セキュリティポリシー(Security policy) – 明確でしかもきちんと定義され, システム内のメカニズムによって実行される.
識別(Identification) – 個々のサブジェクトはユニークに識別されなければならない.
ラベル(Labels) – アクセス制御ラベルはオブジェクトに適切に関連付けられていなければならない.
文書化(Documentation) – テスト, デザイン, 仕様ドキュメント, ユーザガイド, マニュアルを含む.
責任追跡性(Accountability) – 監査データは, 責任追跡性のために残し, 保護しておかなければならない.
ライフサイクル保証(Life cycle assurance) – ソフトウェア, ハードウェア, ファームウェアは個々にテストすることができ, それぞれがライフタイム中効率的にセキュリティポリシーを実行しなければならない.
継続的保護(Continuous protection) – セキュリティメカニズムとシステム全体は, 異なる状況にも継続的に期待通りにまた受け入れられるように働かなければならない.
評価レベル -
D – 最低限の保護(Minimal Protection)

C1 – 任意セキュリティ保護(Discretionary Security Protection)
C2 – アクセス制御による保護(Controlled Access Protection)
B1 – ラベル式保護(Labeled Security)
B2 – 構造化保護(Structured Protection)
B3 – セキュリティドメイン(Security Domains)
A1 – 検証された設計(Verified Design)

8.6.2 レッドブック(The Red Book) / TNI

TNI – Trusted Network Interpretation.
ネットワークとネットワークコンポーネントのセキュリティ評価トピックを扱う.
隔離されたローカルエリアネットワークと広域インターネットワークシステムの両方を扱っている.
扱っているセキュリティアイテム:
* コミュニケーションの完全性(Communication integrity)
— 認証(Authentication)
— メッセージ完全性(Message integrity)
— 否認防止(Nonrepudiation)
* サービス拒否の予防(Denial of service prevention)
— 運用の継続(Continuity of operations)
— ネットワーク管理(Network management)
* コンプロマイズ予防(Compromise protection)
— データの機密性
— トラフィックフローの機密性
— 選択的ルーティング(Selective routing)
レーティング -
- なし(None)
- C1 – 可(Minimum)
- C2 – 良(Fair)
- B2 – 優(Good)

8.6.3 ITSEC

ITSEC – 情報技術セキュリティ評価規格(Information Technology Security Evaluation Criteria).
ヨーロッパでのみ使われている
2 つの主要な属性- 機能と保証(Functionality and Assurance.)
セキュリティ製品とセキュリティシステムの両方のクライテリアで, その両方を評価対象(TOE, Target of Evaluation として扱っている.

8.6.4 コモン・クライテリア(Common Criteria)

国際的な評価基準.
EAL – 評価保証レベル(Evaluation assurance level).
プロテクション・プロファイル(Protection profile) – セキュリティ要件, その意味, 理由の集合で, EAL 評価に相当する.
2 つの主な属性 – 機能と保証 (Functionality and Assurance.)
プロテクション・プロファイルの 5 つのセクション-
- 記述要素(Descriptive elements)
- 根拠(Rationale)
- 機能要件(Functional requirements)
- 開発保証要件(Development assurance requirements)
- 評価保証要件(Evaluation assurance requirements)

8.7 認証(Certification) <-> 認定(Accreditation)

8.7.1 認証(Certification)

セキュリティコンポーネントとその整合性の技術的な評価で, 認定のために行われる.
セキュリティメカニズムと制御およびそれらの効率性の査定プロセスである.

8.7.2 認定(Accreditation)

システムの全体的なセキュリティが適切であることをマネジメントが正式に受け入れること.
認証プロセスの結果の情報をマネジメントが公式に受け入れること.

8.8 オープンシステム(Open Systems) <-> クローズドシステム(Closed Systems)

8.8.1 オープンシステム(Open Systems)

公開された仕様に基づくシステムで, サードパーティーベンダがアドオンコンポーネントや装置を開発できる.
異なるベンダの異なる OS, アプリケーション, ハードウェア装置との間の相互運用性を提供する.

8.8.2 クローズドシステム(Closed Systems)

業界の標準に従わないアーキテクチャーを採用している.
異なるタイプのシステムやアドオン機能との間のコミュニケーションを簡単にするための相互運用性と標準インターフェイスは採用されていない.
独自仕様であり, 似たシステムとだけコミュニケーションができる.

8.9 セキュリティモデルとセキュリティ構造に対する脅威

8.9.1 コバートチャネル(Covert Channels)

許可されていない方法で, エンティティーが情報を受け取る方法. セキュリティメカニズムでコントロールされない情報フローである.
コバートタイミングチャネル(Covert timing channel) – システムリソースの使用を調節することによって情報を他のプロセスにリレーする.
コバートストレージチャネル(Covert storage channel) – プロセスがあるストレージロケーションにデータを書き込むときに, 他のプロセスが直接あるいは間接にそれを読むこと. この問題はプロセスが別々のセキュリティレベルにある場合に生じる. したがって機密データの共有のためのものではない.
- 対策:
こうしたチャネルに対してユーザができることはあまりない.
HTTP を使ったトロイの木馬に対しては, 不正侵入検知システムや監査によって隠れたチャネルを見つけることが出来る場合もある.

8.9.2 バックドア(Back Doors)

メンテナンスフック(maintenance hooks)とも呼ばれる.
開発者だけが知っていて呼び出すことが出来る, ソフトウェア内の命令.
- 対策:
コードのリビューとユニットテスト, 統合テストを行うことによってバックドアを見つけることができる.
バックドアに対する防御策-
ホスト型不正侵入検知システム
設定ファイルや機密情報の書き換えから防ぐためにファイルシステムのパーミッションを使用する.
厳格なアクセス制御

ファイルシステムの暗号化
監査

8.9.3 タイミング問題(Timing Issues)

非同期攻撃とも呼ばれる.
システムがタスクを完了するために必要な一連のステップのタイミングの差を利用する.
A time-of-check versus time-of-use attack, also called race conditions, could replace autoexec.bat.
- 対策:
ホスト型不正侵入検知システム
ファイルシステムのパーミッションと暗号化
厳格なアクセス制御
監査

8.9.4 バッファーオーバーフロー(Buffer Overflows)

”smashing the stack”とも呼ばれる.
プログラムに入力されるデータの長さをチェックせずに CPU で処理する場合に起こる.
- 対策:
適切なプログラミングと望ましいコーディングの実践.
ホスト型不正侵入検知システム
ファイルシステムのパーミッションと暗号化
厳格なアクセス制御
監査

9 CBK#7 運用セキュリティ(Operations Security)

9.1 制御と防御(Controls and Protections)

ハードウェア, ソフトウェア, メディアリソースを以下の事項から守るために行う:
- 運用環境内の脅威
- 内部, 外部の侵入者
- リソースに対して不適切なアクセスを行うオペレータ

9.1.1 制御のカテゴリ(Categories of Controls)

- 予防的制御(Preventative Controls):
システムに入った意図しないエラーの大きさと影響を軽減するため, また内部もしくは外部からのシステムへの認められていない侵入者を防ぐために設計される.
- 検知的制御(Detective Controls):
起きてしまったエラーを検知するために使用される.
- 訂正的制御(Corrective Controls) / 復旧制御(Recovery Controls):
データ回復手順を通じて損失事件の影響を軽減するために行われる.
- 抑止的制御(Deterrent Controls) / 指示的制御(Directive Controls):
外部の制御と協働するために使用される.
- アプリケーション制御(Application Controls):
ソフトウェアの運用上の不正を最小にし, また検知するためにソフトウェアアプリケーション内に設計された制御.
- トランザクション制御(Transaction Controls):
トランザクションの様々な段階に対して行う制御. 制御のタイプは, 入力, 処理, 出力, 変更, テストである.

9.1.2 オレンジブックコントロール(Orange Book Controls)

運用上の保証(Operational assurance):
- システム構造(System architecture)
- システム完全性(System integrity)
- コバートチャネル分析(Covert channel analysis)
- 高信頼設備管理(Trusted facility management)
- 高信頼リカバリ(Trusted recovery)

9.1.3 ライフサイクル保証(Life cycle assurance)

- セキュリティテスト(Security testing)
- 設計の仕様と検証(Design specification and testing)
- コンフィギュレーション管理(Configuration management)
- 高信頼配布(Trusted distribution)

9.1.4 コバートチャネル分析(Covert channel analysis)

- B2:
システムにはコバートストレージチャネルに対する防御策がなければならない. 全てのコバートストレージチャネルについてコバートチャネル分析を行わなければならない.
- B3 および A1:
システムにはコバートストレージチャネルおよびコバートタイミングチャネルに対する防御策がなければならない. 両タイプについてコバートチャネル分析を行わなければならない.

9.1.5 高信頼設備管理(Trusted Facility Management)

B2:
システムにおいてオペレータとシステム管理者のロールを分けなければならない.
B3 および A1:
システムにおいてセキュリティ関連機能を行うセキュリティ管理者機能を明確に特定しなければならない.

9.1.6 職務分離とジョブローテーション(Separation of duties and job rotation)

- 最小特権(Least privilege):
システムのユーザは, 自分の仕事を行うのに必要な最小限の権利と特権を持っており, それらはまた最小限の期間だけ認められていることを意味する.
- Two-man control:
2 人のオペレータがそれぞれの仕事をリビューし, 承認し合う. これにより責任が生じ, 非常に慎重を期すべきトランザクションやリスクの高いトランザクションにおける不正行為を極力減らすことができる.
- デュアルコントロール(Dual control):
慎重を期すべきタスクを完了するために 2 人のオペレータが必要である.
- ジョブローテーション(Job rotation):
異なるセキュリティ分類の異なるタスクに移る前にセキュリティ関連タスクを遂行するためにオペレータに割り当てられた期間を制限するプロセス.

9.1.7 高信頼リカバリ(Trusted Recovery)

システム故障やシステム不具合が生じたときに, セキュリティが侵害されないことを保証すること.
B3 レベルと A1 レベルのシステムにのみ必要.
- Failure preparation:
定期的に重要なファイル全てのバックアップを取る.
- システムリカバリ(System recovery)
コモン・クライテリアにおいて以下の 3 つの階層型リカバリタイプが定義されている-
  - 手動リカバリ(Manual recovery)
  - 自動リカバリ(Automated recovery)
  - 不適切な損害のない自動リカバリ(Automated recovery without undue Loss)

9.1.8 コンフィギュレーション/変更管理制御(Configuration / Change Management Control)

変更制御プロセスを実行・サポートする手順:
- 変更の申し出(Applying to introduce a change)
- 意図した変更のカタロギング(Cataloging the intended change)
- 変更のスケジューリング(Scheduling the change)
- 変更の実施(Implementing the change)
- 適切な関係者への変更のレポート(Reporting the change to the appropriate parties)

9.1.9 クリッピングレベル(Clipping Levels)

あるタイプのエラーやミスが許される閾値で, 不審であるとみなす前に許されるミスの回数. クリッピングレベルを超えると, 更なる違反はリビューのために記録される.

9.1.10 管理上の制御(Administrative Controls)

コンピュータセキュリティに対する脅威や影響を軽減するために経営管理によって行われる制御.
- パーソナルセキュリティ(Personal Security)
  - 雇用前調査と経歴調査(Employment Screening or Background Checks)
  - 1 週間単位での休暇取得義務(Mandatory Taking of Vacation in One Week Increment)

- ジョブアクション警告もしくは解雇(Job Action Warnings or Termination)
- 職務と責任の分離(Separation of Duties and Responsibilities)
- 最小特権(Least Privilege)
- 知る必要性(Need to Know)
- 変更/コンフィギュレーション管理制御(Change/Configuration Management Controls)
- 記録保存と文書化(Record Retention and Documentation)

9.1.11 記録保存(Record Retention)

データ残存(Data Remanence) -
消去後のメディアに残っているデータのこと

9.1.12 運用制御(Operations Controls)

コンピュータオペレーションを守るために行われる日々の手順.
リソース保護(Resource Protection):
組織のコンピューティング資源と資産を損失や侵害から保護するコンセプト. ハードウェア, ソフトウェア, データ資源をカバーする.

9.1.13 ハードウェア制御(Hardware Controls)

- ハードウェア保守(Hardware Maintenance)
- 保守アカウント(Maintenance Accounts)
- 診断ポート制御(Diagnostics Port Control)
- ハードウェア物理制御(Hardware Physical Control)

9.1.14 ソフトウェア制御(Software Controls)

- アンチウイルス管理(Anti-virus Management)
- ソフトウェアテスト(Software Testing)
- ソフトウェアユーティリティ(Software Utilities)
- 安全なソフトウェア保存(Safe Software Storage)
- バックアップ制御(Backup Controls)

9.1.15 特権エンティティー制御/特権オペレーション機能(Privileged Entity Controls / Privileged operations functions)

- システムコマンドへの特別アクセス(Special access to system commands)
- 特殊パラメータへのアクセス(Access to special parameters)
- システム制御プログラムへのアクセス(Access to the system control program)

9.1.16 メディア資源保護(Media Resource Protection)

意図の有無に関わらず機密データの漏洩による全てのセキュリティリスクから保護するために行われる-
- メディアセキュリティ制御(Media Security Controls):
機密情報の損失を防ぐために設計されるべきであり, また以下のことが行える:
  - ロギング
  - アクセス制御
  - 適切な廃棄
- Media Viability Controls
データストレージメディアの実行可能性(viability)を守るために使用されるべきである.
システムリカバリプロセスにおいて必要とされる-
  - マーキング(Marking)
  - ハンドリング(Handling)
  - 保管(Storage)

9.1.17 物理アクセス制御(Physical Access Controls)

対象
- ハードウェア
- ソフトウェア

外部サポートプロバイダがデータセンターに入る場合には特別な監視の手配が行わなければならない.

ピギーバッキング(Piggybacking): 許可されていない人物が, 許可された人物の後ろからドアを通ること. これを防ぐためにマントラップの概念が設計された..

9.2 監視と監査(Monitoring and Auditing)

9.2.1 監視(Monitoring)

コンピュータ設備のオペレーションに影響を及ぼしかねないセキュリティ事件の発見のためのメカニズム, ツール, 手法を含んでいる.
監視手法(Monitoring techniques) -
- 侵入検知(Intrusion detection)
- 侵入テスト(Penetration testing)
  - スキャンとプローブ(Scanning and probing)
  - デーモンダイヤリング(Demon Dialling)
  - スニフィング(Sniffing)
  - ゴミ箱あさり(Dumpster Diving)
  - ソーシャルエンジニアリング(Social Engineering)
- クリッピングレベルを使用した違反処理

9.2.2 監査(Auditing)

運用上のセキュリティ制御監視の基礎となる.
監査証跡(Audit Trails):
これにより, セキュリティ実行者がトランザクション履歴を追うことができる.
問題管理コンセプト(Problem Management Concepts):
- 管理可能なレベルに不具合を減らす
- 問題の発生, 再発生を防ぐ
- 問題がコンピュータサービスやリソースに及ぼす悪影響を軽減する.

9.3 脅威と脆弱性(Threats and Vulnerabilities)

9.3.1 脅威(Threats)

不慮の損害(Accidental loss):
意図せずに生じる損害で, オペレータ教育や習熟の不足やアプリケーション処理手順の不具合による.
- オペレータの入力ミスや削除
- トランザクション処理エラー

不適切なアクティビティ(Inappropriate Activities):
犯罪行為までは行かないがジョブアクションや解雇につながるコンピュータ行動.
- 不適切な内容
- 会社のリソースの無駄遣い
- セクシャルハラスメントや人種ハラスメント
- 特権や権利の濫用

不法なコンピュータオペレーションと意図的な攻撃:
個人の経済的利益や破壊を目的とし, 意図的で不法と見なされるコンピュータアクティビティ.

- 盗聴(Eavesdropping)
- 不正行為(Fraud)
- 窃盗(Theft)
- サボタージュ(Sabotage)
- 外部攻撃(External Attack)

9.3.2 脆弱性(Vulnerabilities)

- トラフィック分析/トレンド分析(Traffic / Trend Analysis)
- 保守アカウント(Maintenance Accounts)
- データスキャベンジング攻撃(Data Scavenging Attacks)
- IPL 脆弱性(IPL Vulnerabilities)
- ネットワークアドレスハイジャック(Network Address Hijacking)

9.4 電子メイルとインターネットセキュリティ問題(E-mail and Internet Security Issues)

9.4.1 電子メイル(E-mail)

- SMTP – メッセージを転送するエージェントとして働く.
- POP – インターネットメイルサーバプロトコルで, メッセージの出入りをサポートする. メッセージが POP サーバからダウンロードされると, 通常はサーバから削除される.
- IMAP – インターネットプロトコルで, ゆーざがメイルサーバ上のメイルにアクセスすることを可能にする. メッセージはメイルサーバからダウンロードされるか, サーバ上のメイルボックスと呼ばれるユーザ自身のリモートメッセージフォルダに残される.

9.4.2 ハッキングと攻撃の手法(Hack and Attack Methods)

- ポートスキャンとネットワークマッピング(Port Scanning and Networking mapping):
ネットワークマッピングツールは, ネットワーク上のたくさんのシステムに対して, 一見悪意のないパケットを送る.
ポートスキャンは, コンピュータ上の開いているポートを特定する.
- スーパーザッピング(Superzapping):
IBM メインフレームセンターで使用されるユーティリティで, オペレーティングシステム内のアクセス制御を回避することができる.
- ブラウジング(Browsing):
侵入者がアクセスを許可されていない情報を得るために使用される.
サーバやワークステーション上に保存されている他人のファイルを見たり, 不注意に捨てられた情報をゴミの中から探したり, フロッピーディスクに保存された情報を見ることによって行われる.
- スニファ(Sniffers)
トラフィックをモニタするツール.
このツールはハードウェア, もしくはプロミスキャスモードのネットワークインターフェイスカード(NIC)を持ったコンピュータ上で動くソフトウェアである.
- セッションハイジャック(Session Hijacking)
攻撃者は検知されることなく会話の間に入り込む.
- パスワードクラッキング(Password Cracking)
パスワードを捕らえ暴く-
  - 辞書攻撃(Dictionary attack): ハッキングツールに大量の単語のリストを入れる. このツールは捕らえたパスワードと, リスト内の単語に一方向ハッシュ関数をかけ, ハッシュ値が合致するかどうか比較する. もし合致したらパスワードが得られ, そうでなければリスト内の次の単語に進む.
  - 総当たり攻撃(Brute force attack): 数多くの様々な文字のバリエーションを試す. それぞれのバリエーションに対してハッシュ値を求め, それを捕らえたパスワードのハッシュ値と比較する.
- バックドア(Backdoors)

攻撃者によりインストールされたプログラムで, 後日, ログイン情報を入力したり認証プロセスを経たりすることなしにコンピュータに再度入り込むことができるもの.

10 CBK#8 事業継続計画と災害復旧計画(Business Continuity Planning & Disaster Recovery Planning)

10.1 BCP / 事業継続計画(Business Continuity Planning)

主要な要素:
- 範囲と計画の開始(Scope and Plan Initiation)
- ビジネス影響分析(Business Impact Assessment)
- 事業継続計画作成(Business Continuity Plan Development)
- 計画の承認と実施(Plan Approval and Implementation)

10.1.1 範囲と計画の開始(Scope and Plan Initiation)

BCP プロセスを開始する.
計画の範囲策定を伴う.

役割と責任(Roles and Responsibilities) -
BCP 委員会(The BCP Committee):
委員会は, 計画の策定, 実行, テストを行う責任を負うために作られる
上級管理職や全てのファンクショナルビジネスユニット, 情報システムおよびセキュリティ管理者の代表から成る.
上級管理職の役割:
計画の 4 段階の全てに関して最終的な責任を負う.

10.1.2 BIA / ビジネス影響分析(Business Impact Assessment)

事業部門において中断イベントによる影響を把握するためのプロセスである.
影響は財務に関わるもの(数量的)か, 運営に関わるもの(質的, 例えば顧客に対応することができない等)である.
脆弱性評価は BIA プロセスの一部であることが多い.
企業の存続にとって致命的となるシステムを特定し, 災害や中断イベントによって引き起こされる許容休止時間を見積もる.

BIA の主要な 3 つのゴール-
- 臨界優先順位(Criticality Prioritization):
致命的となる事業部門のプロセス全てを確認して優先順位をつけ, 中断イベントの影響を見積もらなければならない.
- ダウンタイムの見積もり(Downtime Estimation):
, 存続している企業であり続け, 事業が許容できる MTB(Maximum Tolerable Downtime, 最大許容ダウンタイム)を見積もらなければならない..
- リソース要件(Resource Requirements):
重要なプロセスに必要なリソースをこの段階で明確にする. 最も時間に依存するプロセスに最大のリソース割り当てを行う.

BIA の 4 つのステップ -
- 必要な評価材料を収集する:
許容レベルの運営を続けるためにどの事業部門が重要であるか見定める.
- 脆弱性評価を実施する:
完全なリスク評価より小規模で, BCP もしくは DRP のための情報を提供することに焦点を絞っている.
機能は損失影響分析を実施することである.
重要なサポート分野を定義しなければならない.

- 収集した情報を分析する:

10.1.3 事業継続計画の整備(Business Continuity Plan Development)

BIA で収集した情報を用いて実際の事業継続計画を整備すること.
これには計画の実施, テスト, 進行中の計画の保守が含まれる.

主な 2 つのステップ -
- 継続戦略を定義する:
ビジネスは災害による中断イベントをどのように管理すると想定されるか.
- 継続戦略を文書化する:
結果を文書化する.

10.1.4 計画の承認と実施(Plan Approval and Implementation)

最終的なシニアマネジメントの署名をもらい, 全社レベルで計画を認知し, 必要に応じてメンテナンス手順を実施することが含まれる.

10.2 DRP / 災害復旧計画(Disaster Recovery Planning)

情報システムリソースに多大な損失を与える中断イベントについて, 事前, 事中, 事後に取るべきである首尾一貫した行動の包括的なステートメント.
主要な目的は, 代替サイトで重要なプロセスを実行し, 迅速な復旧手順によって, 組織にとっての損失が最小になるようなタイムフレームで本来のサイトと通常のプロセスに戻ることができるようにすることである.

災害復旧プロセスのフェイズ:
- データ処理継続計画(Data Processing Continuity Planning)
- データ復旧計画のメンテナンス(Data Recovery Plan Maintenance)

10.2.1 データ処理継続計画(Data Processing Continuity Planning)

代表的な代替処理タイプ-
- 相互扶助契約(Mutual aid agreements / Reciprocal agreements):
似たようなコンピューティングニーズを持った他の企業との契約.
利点は低コスト
欠点は, イベントの最中にそれぞれの組織が完全な運営プロセスを行えるほどの余分なキャパシティを持っていることが非常にありそうにないことであるという点である.

10.2.2 サブスクリプションサービス(Subscription services)

- ホットサイト(Hot site):
完全に設定したコンピュータ設備で, 電力, 暖房, 換気, 空調(HVAC), 機能しているファイルサーバやプリンタサーバ, ワークステーションを持つ.
利点は 24 時間/7 日利用可能なことである.
欠点は費用がかかること, サービスプロバイダがキャパシティ以上のものを売るかもしれないこと, 情報が 2 カ所に保存される際のセキュリティの危険, コントロールが 2 回行われなければならないため管理リソースを多く必要とすることである.
- ウォームサイト(Warm site)
電力, 暖房, 換気, 空調とコンピュータを持つ設備であるが, アプリケーションがインストールされていない場合がある.
利点はコストがホットサイトよりかからないこと, サイト(場所)の選択が柔軟に行えること, ホットサイトと比較して管理リソースが少なくて済むことである.
欠点は, 新しいサイトで生産処理を始めるための時間と労力の差である.

- コールドサイト(Cold site)
緊急時に設備を持ち込むことができるが, サイトにハードウェアは全くない.
利点は低コスト.
欠点は災害が起こった際に機能しない可能性があることである.

10.2.3 複数センター(Multiple centers)

処理が複数のセンターに分散しており, 冗長性に関して分散アプローチを取り, 利用可能なリソースを共有する.
利点は低コスト.
欠点は大きな災害では複数サイトの処理能力を簡単に凌駕してしまうことである.

10.2.4 サービスビューロー(Service bureaus)

代替バックアッププロセスサービスの全てを提供してもらうことをサービスビューローと契約する.
利点は迅速な反応と可用性である.
欠点は, 大規模な災害時に費用とリソースの取り合いになることである.

- データセンターバックアップの他の選択肢:
  - ローリング/モバイルバックアップサイト(Rolling/mobile backup sites)
  - 組織内もしくは外部からの代替ハードウェア供給
  - プレハブビルディング

移行処理における耐障害性と冗長性レベルに使用される 3 つのコンセプト:
- Electronic vaulting:
バックアップデータをオフサイトの場所に転送すること. これは主に代替サイトのサーバに, コミュニケーションラインを通じてデータのダンプを行うバッチ処理である.
- リモートジャーナリング(Remote journaling):
代替サイトにトランザクション処理を平行して行うこと. データが生じるたびに, リアルタイムのデータがコミュニケーションラインを使って送信される.
- Database shadowing:
リモートジャーナリングのライブ処理を使用するが, 複数のサーバにデータベースセットを複製することによってさらなる冗長性を持たせる.

10.2.5 データ復旧計画のメンテナンス(Data Recovery Plan Maintenance)

計画を最新で適切な物に保つ.

10.2.6 DRP のテスト(Testing the DRP / Disaster Recovery Plan)

テストのタイプ-
- チェックリスト(Checklist):
計画のコピーがマネジメントにレビューのために配布される.
- 構造化ウォークスルー(Structured Walk-Through):
ビジネスユニットのマネジメントが計画のレビューのために集まる.
- シミュレーションテスト(Simulation Test):
全てのサポート要員が訓練の遂行セッションで集まる.
- パラレルテスト(Parallel Test):
重要なシステムが代替サイトで実行される.
- 完全中断テスト(Full-Interruption Test):
通常の生産が中断され, 実際の災害復旧プロセスが行われる.

災害復旧プロセスの主要な要素-
- 復旧チーム(The recovery team):
災害の宣言時に復旧手順を実行する任務が明確に定義される.
主要な職務はあらかじめ決められた重要なビジネス機能を代替のバックアップ処理サイトで行うことである.

10.2.7 救助チーム(The salvage team)

本来のサイトを通常業務環境の状態に戻すために派遣される.
このチームは多くの場合, 本来のサイトを再開できるかどうかの宣言をする権限を与えられる.

10.2.8 通常業務再開(Normal operations resume)

最小の混乱やリスクで生産業務を代替の場所から本来の場所に戻す全ての手順.
全ての業務が本来のサイトで完全に生産モードに戻るまで緊急事態が終わったとは言えない.

10.2.9 その他の復旧問題(Other recovery issues)

- 外部のグループとのインターフェイス
- 従業員関係
- 不正行為と犯罪
- 金銭出費
- メディア関係

11 CBK#9 法律, 調査, 倫理(Law, Investigations & Ethics)

11.1 倫理(Ethics)

11.1.1 ISC2

倫理綱領(Code of Ethics Canons) -
- 社会, 団体, インフラストラクチャーを守る
- 立派に, 正直に, 正しく, 責任を持ち, 合法的に行動する
- 雇用主に, 勤勉で有能なサービスを提供する.
- 仕事を進歩させ, 守る.

11.1.2 IAB - Internet Activities Board

非倫理的で受け入れられない行動は–
- 意図的に, インターネットのリソースに対して許可されないアクセスを行おうとすること
- インターネットの使用を意図的に妨害すること
- 意図的な行動によってリソースを浪費すること
- コンピュータベースの情報の完全性を破壊すること
- 他社のプライバシーを危うくすること
- インターネット上の実験の実行を無視すること

11.1.3 GASSP – 一般的に受け入れられるシステムセキュリティ原則(Generally Accepted System Security Principles)

セキュリティ専門家, IT 製品開発者, 情報オーナー, あるいは情報セキュリティの原則の定義や制定に豊富な経験を持つ他の組織からの指導により, GASSP を策定し維持することを求める.

11.1.4 MOM – 動機, 機会, 手段(Motivations, Opportunities and Means)

動機(Motivations) – ある犯罪の「誰が」と「なぜ」
機会(Opportunities) – ある犯罪の「どこで」と「いつ」
手段(Means) – ある犯罪が成功するために必要な能力.

11.2 運用セキュリティ(Operations security)

11.2.1 サラミ(Salami)

量がわずかで気づかれないことを狙い, アカウントから小額の資金を差し引くこと

11.2.2 データ搾取 (Data Diddling)

現存するデータの改竄を指し, しばしばこうした変更はアプリケーションに入力される前や, 処理を終えるとすぐに行われ, アプリケーションから出力される.

11.2.3 過剰な権限(Excessive Privilege)s

タスクを実行するために必要である以上のコンピュータ権限, 許可, 特権を持っている場合に起きる.

11.2.4 パスワード・スニフィング(Password Sniffing)

コンピュータ間で送信されるパスワードを得ようとしてネットワークトラフィックを盗聴すること.
IP スプーフィング(IP Spoofing):
パケット内の IP アドレスを他のアドレスに手動で変更する.

11.2.5 サービス不能(Denial of Service) - DoS
システムが通常提供するサービスの提供を拒否させる.

11.2.6 ごみ箱漁り(Dumpster Diving)
人や企業の攻撃に使うために他の人のごみを漁り, 捨てられたドキュメント, 情報, その他の価値ある物を探すこと.

11.2.7 Emanations Capturing
電子機器から放射される電波の盗聴.

11.2.8 Wiretapping
通信シグナルの盗聴.

11.2.9 ソーシャル・エンジニアリング(Social Engineering)
騙されて知らず知らずのうちに与えてしまう情報を使う技術.

11.2.10 偽装(Masquerading)
攻撃者がアイデンティティを欺く方法

11.3 責任とその派生(Liability and Its Ramifications)

11.3.1 Due Care
社内のアクティビティーに企業が責任を持ち, 会社, リソース, 従業員を守るために必要な行動を取っていることを示すために行われるステップ.

11.3.2 Due Diligence
保護メカニズムを継続的に維持/運営する継続的なアクティビティー.

11.3.3 Prudent man rule
似た状況で懸命な人々が取ると思われる任務を遂行すること.

11.3.4 Downstream liabilities
複数の企業が, 統合されたやり方で協働するときには, 特別なケアによりそれぞれの企業が必要なレベルの保護, 義務, 責任を提供することを約束しなければならない. そしてこれらはそれぞれの企業が署名する契約書に明確に定義されている必要がある.

11.3.5 Legally recognized obligation
他者を不当なリスクから保護するために企業に求められる行動根拠がある. 企業がこの規準を遵守しない場合は他者の障害や損害につながる.

11.3.6 直接的因果関係(Proximate causation)
損害がその企業の責任で引き起こされたものであると証明することができる.

11.4 法律の種類(Types of Laws)

11.4.1 民法(Civil law)
Tort とも呼ばれる.
個人や企業にとっての損害につながる悪事を扱う
民事訴訟の結果は懲役刑ではなく財務的制限となる.

11.4.2 刑法(Criminal law)

個人の行動が, 一般市民を守るために制定された政府の法律を犯すときに使われる..
刑罰は普通, 懲役刑である.

11.4.3 行政法(Administrative law)

業績や振る舞いを規制する基準を扱う.
政府機関がこうした基準を作成し, 企業や企業内の個人に適用される.

11.5 知的所有権法(Intellectual Property Laws)

11.5.1 企業秘密(Trade secret)

企業秘密とされるリソースは極秘にされ, 確実な予防措置や行動で守られなければならない.

11.5.2 著作権(Copyright)

リソースのアイディアの表現を保護する.

11.5.3 商標権(Trademark)

言葉, 名前, シンボル, 音, 形, 色, 装置, もしくはこれらの組み合わせを保護する.

11.5.4 特許権(Patent)

個人や企業が法的所有権を与えられ, 特許権によってカバーされる革新の複製について他者を排除することができる.
著作権により 17 年間の所有権の制限を与えられる.

11.6 コンピュータ犯罪調査(Computer Crime Investigations)

11.6.1 Incident response team

基本アイテム -
- 連絡を取ったり報告をしたりする外部機関やリソースのリスト.
- 連絡を取るコンピュータフォレンジック専門家のリスト.
- 証拠を安全に保存する手順.
- 証拠を探す手順
- 報告に含めるべきアイテムのリスト.
- 同様の状況で他のシステムをどのように扱うかについて示すリスト.

11.6.2 コンピュータ・フォレンジックス(Computer Forensics)

フォレンジック調査(Forensics investigation) -
第一ステップ: 攻撃されたシステムの信頼できるイメージを作成し, このコピーでフォレンジック分析を行う. 調査の段階でデータの破壊をしてしまってもオリジナルのシステムには影響を与えないことを保証できる. また, システム上で何かをしたり電源を切ったりする前に, システムのメモリはファイルにダンプしなければならない.
第二ステップ / 分析過程の管理(Chain of custody): 証拠を収集し整理する際には, 非常に厳格できちんとした手順に従わなければならない.
全ての証拠にはラベルを貼り, 誰がその証拠を安全にし, 有効にしたかを示すことを定める..
分析過程の管理は, 証拠が法廷に証拠として示されるためにどのように収集, 分析, 輸送, 保存されてきたかを示す履歴である. 電子的な証拠は簡単に変更できるため, 明確に定義された分析過程の管理によって証拠が信頼しうるものであることを実証する.

11.6.3 証拠のライフサイクル(The life cycle of evidence)

以下が含まれる

- 収集と特定
- 保管, 保存及び輸送(Storage, preservation and transportation.)
- 法廷での提出
- 被害者もしくは所有者に返される.

11.6.4 証拠(Evidence)

最良の証拠(Best evidence) – 最も信頼性が高いため, 裁判で使用される一次的証拠. 契約書のような 文書証拠にも使われる.
二次的証拠(Secondary evidence) – 最良の証拠に比べ, 有罪/無罪を証明する際に信頼性や強さで劣ると見られる.
直接証拠(Direct evidence) – バックアップ情報を参照せずにそれだけで事実を証明できる.
決定的証拠(Conclusive evidence) – 反駁や否定できない証拠.
状況証拠(Circumstantial evidence) – 中間事実を証明でき, それにより他の事実の推定や推測に使われる.
補強証拠(Corroborative evidence) – 考えやポイントを証明する助けとなる証拠. それ自体では役に立たず, 一時的証拠の保管ツールとして使われる.
意見証拠(Opinion evidence) – 目撃者が証言するとき, 意見ルールによって事実に関するその人の意見ではなく事実のみを証言することが定められている.
伝聞証拠(Hearsay evidence) – 法廷で提出される口頭もしくは書面の証拠に関しては, また聞きであったりあるいは正確さや信頼性の直接の証明がなかったりする.

11.6.5 証拠の特徴(Characteristics of evidence)

証拠たりうるには以下の要件を満たさなくてはならない:
十分(Sufficient) – 論理的な人に対して発見の有効性を説得するに足りること. また, 簡単に疑問視されないこと.
信頼できる(Reliable) / 適切(Competent) – 事実と矛盾せず, 事実に基づき, 状況的でないこと.
関連(Relevant) – 発見に対して合理的でふさわしいこと.
合法的(Legally permissible) – 合法的に得たものであること.

誘惑(Enticement) <-> *おとり(Entrapment*):
誘惑(Enticement) -
合法かつ倫理的.
おとり(Entrapment) -
違法で非倫理的.

11.7 フォン・フリーカー(Phone Phreakers)

Blue boxing – 電話会社のシステムに対して, 長距離電話をかけることができるように欺くトーンをシミュレートする装置.
Red boxes – 公衆電話で硬貨を入れる音をシミュレートする.
Black boxes – フリーダイヤルを受けるために回線の電圧を操作する.

12 CBK#10 物理的セキュリティ(Physical Security)

12.1 物理的セキュリティコントロール(Physical Security Controls)

コントロールのタイプ:

- 管理上の制御(Administrative controls)
  - 施設選択もしくは建設(Facility selection or construction)
  - 施設管理(Facility management)
  - 人事コントロール(Personnel controls)
  - トレーニング(Training)
  - 緊急対応と手順(Emergency response and procedures)
- 技術的制御(Technical controls)
  - アクセス制御(Access controls)
  - 侵入検知(Intrusion detection)
  - アラーム(Alarms)
  - 監視(Monitoring (CCTV))
  - 暖房, 換気, エアーコンディショニング(Heating, ventilation and air conditioning (HVAC))
  - 電力供給(Power supply)
  - 火災検知と消火(Fire detection and suppression)
  - バックアップ(Backups)
- 物理的制御(Physical controls)
  - フェンス(Fencing)
  - 錠(Locks)
  - 照明(Lighting)
  - 施設建材(Facility construction materials)

12.2 施設管理(Facility Management)

12.2.1 場所選択の問題(Issues with selecting a location)

- Visibility
- Surrounding area and external entities
- Accessibility
- Natural disaster

12.2.2 Construction issues when designing and building a facility

- Walls
- Doors
- Ceilings
- Windows
- Flooring
- Heating and Air Conditioning
- Power Supplies
- Water and Gas Lines
- Fire Detection and Suppression

12.2.3 Concerns

The load - How much weight that can be held of a building's walls, floors and ceilings needs to be estimated and projected to ensure that the building will not collapse in different situations.
Positive flow (water and gas lines) - Material should flow out of building, not in.
Internal partitions - Many buildings have hung ceilings, meaning the interior partitions may not extend above the ceiling; therefore an intruder can lift a ceiling panel and climb over the partition.

12.3 Physical Security Component Selection Process

12.3.1 Security Musts

Obliged by law to obey certain safety requirements

12.3.2 Security Shoulds

Protection procedures that should be put into place to help protect the company from devastating activities and their results.

12.3.3 Hardware

SLAs / Servicelevel agreements - Ensure that vendors provide the necessary level of protection.
MTBF / Mean Time Between Failure - Is used to determine the expected lifetime of a device or when an element within that device is expected to give out.
MTTR / Mean Time To Repair - Is used to estimate the amount of time between repairs.

12.3.4 Power Supply

Power protection -
- Online systems: Use a bank of batteries
- Standby UPS: Stay inactive until a power line fails
- Backup power supplies: Used to supply main power or charge batteries in a UPS system.
- Voltage regulators and line conditioners: Can be used to ensure a clean and smooth distribution of power.

Electrical Power Definitions:

Ground	The pahtway to the earth to enabled excessive voltage to dissipate
Noise	Electromagnetic or frequency intererence that disrupts the power flow and can dagusse fluctations
Transient noise	Short duration of power line disruption
Clean power	Power that does not fluctate
Fault	Momentary power loss/out
Blackout	Complete / Prolonged loss of power
Sag	Momentary low voltage
Brownout	Prolonged low voltage
Spike	Momentary high voltage
Surge	Prolonged high voltage
Inrush	Initial surge of power at the beginning

12.4 Environmental issues

Positive drains - Their contents flow out instead of in.
Relative humidity - 40 to 60 % is acceptable
High humidity - Can cause corrosion
Low humidity - Can cause excessive static electricity
Positive pressurization - When an employee opens a door, the air goes out and outside air does not come in.

12.4.1 Fire detectors

Smoke activated - Photoelectric device.
Heat activated - Rate-of-rise temperature sensors and fixed-temperature sensors.
Flame activated - Senses the infrared energy
Automatic Dial-up Alarm - Call the local fire station to report detected fire.

12.4.2 Fire suppression

Portable extinguishers should be located within 50 feet of any electrical equipment and located near exists.

12.4.3 Fire classes and suppression medium

A	Common combustibles	Water or Soda Acid
B	Liquid	CO2, Soda Acid or Halon
C	Electrical	CO2 or Halon

Water - Suppresses the temperature required to sustain the fire.
Soda Acid - Suppresses the fuel supply of the fire
CO2 - Suppresses the oxygen supply required to sustain the fire
Halon - Suppresses the combustion through a chemical reaction

12.4.4 Replacement list for Halon

FM-200, NAF-S-III, CEA-410, FE-13, Water, Inergen, Argon, Argonite.

12.4.5 Water Sprinkler

Wet Pipe - Always contain water in the pipes and are usually discharged by temperature control level sensors.
Dry Pipe - The water is held by a valve until a specific temperature is reached. There is a time delay between the predefined temperature being met and the release of water.
Preaction - Combine the use of wet and dry pipe system. Water is not held in the pipes and is only released into the pipes once a predefined temperature is met. Once this temperature is met, the pipes are filled with water, but it does not release right away. A link has to melt before the water is released from the sprinkler head itself.
Deluge - The same as a dry pipe system except the sprinkler head is open.

12.5 Perimeter Security

12.5.1 Facility Access Control

Enforced through physical and technical components
Locks:
Are the most inexpensive access control mechanisms.
Are considered deterrent to semiserious intruders and delaying to serious intruders.
Preset Locks - Are locks usually used on doors.
Cipher Locks / programmable locks - Use keypads to control access into an area or facility.
Options available on many cipher locks:
- Door delay: If the door is held open for a long period of time, an alarm will trigger to alert personnel of suspicious activity.
- Key-override: A specific combination can be programmed to be used in emergency situations to override usual procedures or for supervisory overrides.
- Master-keying: Enables supervisory personnel to change access codes and other features of the cipher lock.
- Hostage alarm: If an individual is in duress and/or held hostage, there can be a combination he or she enter to communicate this situation to the guard station and/or police station.

Device Locks - To protect devices by using Switch controls, slot locks, port controls, peripheral switch control and cable traps.

12.5.2 Personnel Access Controls

Proper identification to verify if the person attempting to access a facility or area should actually be allowed in.
Piggybacking - When an individual gains unauthorized access by using someone else's legitimate credentials or access rights.

12.5.3 Magnetic cards

Memory card - The reader will pull information form it and make an access decision.
Smart card - The individual may be required to enter a PIN or password, which the reader compares against the information held within the card.

12.5.4 Wireless Proximity Readers

User activated - Transmits a sequence of values to the reader
System sensing - Will recognize the presence of the coded device within a specific area.
- Transponders: The card and reader have a receiver, transmitter and battery
- Passive devices: The card does not have any power source of its own
- Field-powered devices: The card and reader contain a transmitter and active electronics.

12.5.5 External Boundary Protection Mechanism

Fencing:
3-4 feet - Deter casual trespassers
6-7 feet – Considered too high to climb easy
8 feet with 3 strands of barbed wire - Deter intruders
Mantrap - The entrance is routed through a set of double doors that may be monitored by a guard.

12.5.6 Lighting

Should be used to discourage intruders and provide safety for personnel, entrances, parking areas and critical sections.
Critical areas should be illuminated 8 feet high and 2 feet out.

12.5.7 Surveillance Devices

Three main categories -
- Patrol Force and Guards - Can make determinations
- Dogs - Are loyal, reliable and have a sense of smell and hearing
- Visual Recording Devices: Camera, CCTV, …

12.5.8 Detecting

Proximity Detection System / Capacitance detector -
Emits a measurable magnetic field while in use. The detector monitor this electrical field and an alarm sounds if the field is disrupted.
Photoelectric or Photometric System -
Detects the change in the level of light within an area.
Wave Patterns -
Generates a wave pattern that is sent over an area and reflected back to the receiver.
Passive Infrared System -
Identifies the changes of heat waves with an area it is configured to protect.
Acoustical-Seismic Detection System -
Is sensitive to sounds and vibrations and detects the changes in the noise level of an area it is placed.

12.6 Media Storage Requirements

Data that is no longer needed or used must be destroyed.
Object reuse - The concept of reusing data storage media after its initial use
Data remanence - Is the problem of residual information remaining on the media after erasure.
Stages of data erasure -
- Clearing: Overwriting of datamedia intended to be reused in the same organization or monitored environment.
- Purging: Degaussing or overwriting media intended to be removed from a monitored environment.
- Destruction: Completely destroying the media and therefore residual data.

13 Related links

On the Internet you can find many sites covering information security. All of them are not a relevant study guide for IS professionals, but may include very interesting information. The links listed below are just some of all those links.

(ISC)2
www.isc2.org
The starting point for your CISSP examination

CCCURE
www.cccure.org
The best studyguide for the CISSP examination, with documents and links.

ISACA
www.isaca.org
Foundation for information security auditors, administers the CISA certification.

CERT Coordination Center
www.cert.org
A center of Internet security expertise.

Incidents.org
www.incidents.org
A virtual organization of advanced intrusion detection analysts, forensics experts and incident handlers.

NIST CSRC
www.csrc.nist.gov
Computer Security Resource Center at NIST .

14 References

CISSP 試験の準備のために，多くの本や参考書を使用
することができる．私の場合は以下の参考書を使用した．

CISSP all-in-one Certification Exam Guide
Shon Harris
Has been the primary study guide for me. Practice questions are included in the book an on a CD.

The CISSP Prep Guide
Ronald L. Krutz and Russel Dean Vines
Was a supplementary study guide for me. Practice questions are included in the book.

ISO/IEC 17799
ISO standard (prior the british standard BS 7799)
Code of practice for information secrity. The basis for ISO certification in Information Security.

CCCURE
www.cccure.org
Allready mentioned. Still you will find reference materia for your preparation here..