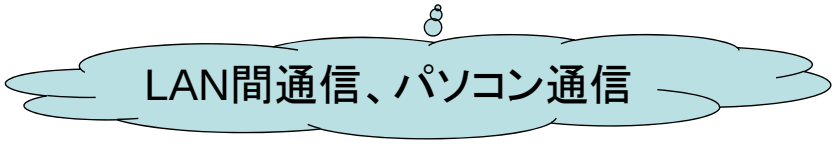
情報セキュリティ（宮崎明雄）

情報セキュリティ技術の概要

- ネットワーク社会とセキュリティへの脅威
  - ーセキュリティに対する脅威の分類
- ネットワーク社会のセキュリティを守る技術の概要
  - ーアクセス管理技術
  - ー暗号技術
  - ー電子透かし技術
  - ーその他の対策
    （コンピュータウィルス用ワクチン、・・・）

ネットワークの発展とインターネット

中央集中型ネットワーク ⇒ LAN ⇒ インターネット



ローカル ⟷ グローバル

インターネットによるサービス

- ●電子メール、WWW（World Wide Web）
- ●電子掲示板（ニュースグループ）
- ●ファイル転送（FTP）
- ●遠隔ログイン（TELNET）

- 情報セキュリティとは何か？ ⇒ IT社会・ネットワーク社会において、私たちが安全に仕事や生活するためのいろいろな取り組みや仕組み。
- セキュリティはコンピュータを使う人しか関係ない？ ⇒ No！ 日常生活を安全にするためのテクニックもセキュリティ。
- セキュリティを高めるには？ ⇒ リスク（危険）を減らす。
- リスクは資産、脅威、脆弱性からできている。
- リスクを構成する三要素のうち、資産と脅威があるだけではリスクは顕在化しない（危険が現実のものとはならない）。脆弱性があってはじめてリスクが顕在化する。
- リスクを減らすには？ ⇒ 資産、脅威、脆弱性のうちどれかをなくす。まずはどれか一つをなくすようにする。脅威など自分ではどうすることもできないものもある。脆弱性を体系的に減らしていくのが常套手段。

【例】

「（資産） 家の中に現金（それも大金）がある。」

「（脅威） 世の中に泥棒がいる。」

これだけではリスクは顕在化しないが、

「（脆弱性） 家に鍵をかけ忘れて外出してしまった。」

という事態が重なってリスクが顕在化してしまう。

この例でリスクを減らすためには、まずは

「家の戸締りをきちんとする、鍵をかける・・・。」

という対策をとる（現実的対応策・実現可能）。

「泥棒のいない世の中をつくる。」

という対策もあるが、これは困難（理想的・非現実的対応策）。

セキュリティを高める ⇒ リスク(脆弱性)を減らす

ペリメータモデルを使って抽象化し、脆弱性を減らす

①「内にある資産は基本的に安全である」と仮定する。

②「脅威は外からやってくる」と仮定する。

③内と外の間に境界線(ペリメータライン)設定し、境界線上の出入りを厳しくチェックすることで脅威の進入を防ぐ。

ペリメータモデル(内は安全、外は危険)

- IT社会・ネットワーク社会特有の考え方?⇒ No! 昔からあった。(例)お城、塀、壁、など。
- このモデルさえ適用すれば安心? ⇒ No! 内側が信用できるか? 内側に悪い人がいたら大変!
- それでは内側も疑うようにしたら? 内側も監視・検閲したら? ⇒ 社会全体がぎすぎすする。精神衛生上よくない。

【参考図書】

岡嶋裕史, “セキュリティはなぜ破られるのか 10年使える「セキュリティの考え方」, ” 講談社ブルーバックス, 2006年7月.

セキュリティに対する脅威の分類

脅威を与える原因による分類

- ●偶発的:
  - ー天災(地震、火災、水害、・・・)
  - ー故障(HW故障、SW故障、回線障害、・・・)
  - ー誤動作(データ入力ミス、誤接続、SWバグ、・・・)
- ●意図的:
  - ー第三者の悪意の行為(不正アクセスなど)
  - ー取引相手の悪意の行為(取引内容の事後否認、コンテンツの不正コピーなど)

第三者による脅威(1)

(a) 第三者の悪意の行為により生じる現象

情報セキュリティの確保

①機密性(Confidentiality):ネットワーク上やコンピュータ内の情報を不適切な人間には決して見せないようにすること。

②完全性(Integrity):ネットワーク上やコンピュータ内の情報が常に完全な形で保たれ、不正によって改ざんされたり破壊されたりしないこと。

③可用性(Availability):ネットワーク上やコンピュータ内の情報や資源(通信路やコンピュータ)がいつでも利用できること。

第三者による脅威(2)

(b) 第三者による脅威の現象別による分類

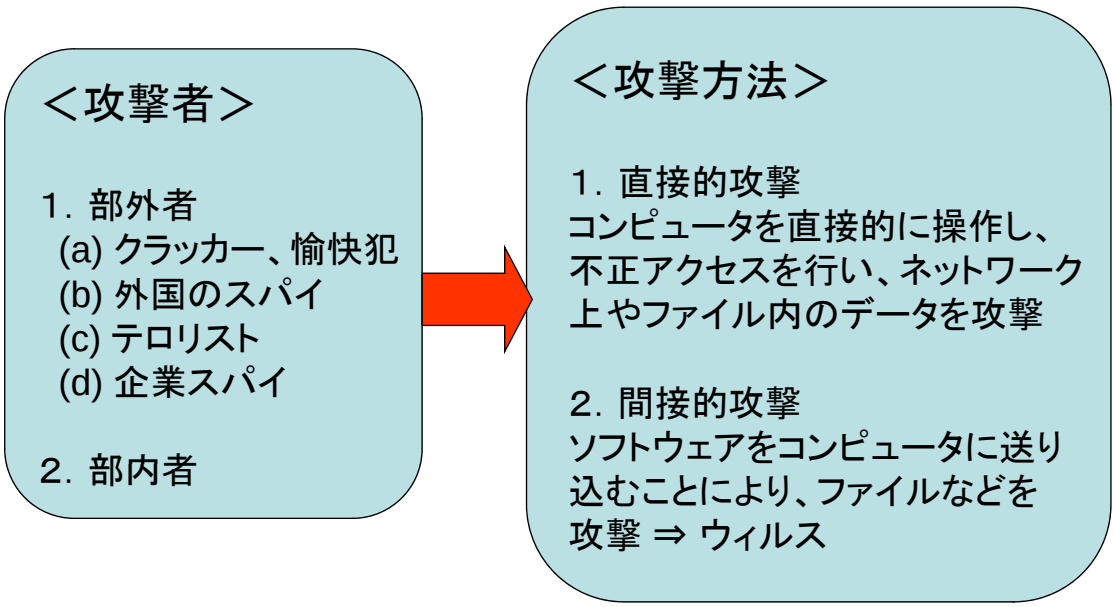
①機密性の喪失:不適切な主体にネットワーク上やコンピュータ内の情報を見られる。(例:メールサーバ内のメールの内容を見られる。)通信路上(特に無線)での傍受、ディスクの不当な読み出し、ディスプレイ画面の盗み見など。

②完全性の喪失:ネットワーク上やコンピュータ内の情報を不当に改ざんされたり、破壊されたりする。(例:電子商取引において、金額情報が改ざんされる。)通信路上のデータ、ディスク内のデータの改ざんや破壊など。

③可用性の喪失:ネットワークやコンピュータの機能や、保存されている情報が不当な利用によって使えなくなる。(例:第三者が通信路上に不当に大量のデータを流すために、本来の利用者がその通信路を使えなくなる。)通信路、コンピュータのパワー、ディスクの不当な利用など。

第三者による脅威(3)

(c) 第三者による脅威の攻撃者と攻撃方法による分類



第三者による脅威(4)

(d) 第三者による脅威の影響の大きさによる分類

①情報システムへの影響: 情報セキュリティが失われると、情報システムが正常に運用できなくなる。

②業務への影響: 情報システムが正常に運用できなくなることにより、企業などの業務へ大きな影響を及ぼす。

③国民生活への影響: 銀行のオンラインシステムなどがダウンするとその影響は業務への影響にとどまらず、国民生活へも大きな影響を及ぼす。

影響の大きさの指標: P×M

- P: 対象となる事象が生じる確率 (例:不正アクセスの成功確率)
- M: その事象が生じた場合の影響の大きさ(定量的指標) (例: 盗まれたパスワードの数、データの破壊による復旧に必要とする経費)

取引相手による脅威

1. 証拠性の喪失: 取引相手が契約書などの取引文書を偽造や改ざんし、取引内容や取引事実を不当に事後否認する。⇒ 認証機能(デジタル署名(捺印・署名のデジタル版))
2. 提供情報の不正コピー(原本性の喪失): 取引相手に対し販売した情報(コンピュータプログラム、マルチメディアデータなど)を不正にコピーして他の人たちに配る。⇒ 不正コピー防止技術(電子透かし技術)

情報資産・情報資源に対して情報セキュリティを確保するためには

①機密性（Confidentiality）：ネットワーク上やコンピュータ内の情報を不適切な人間には決して見せないようにすること。

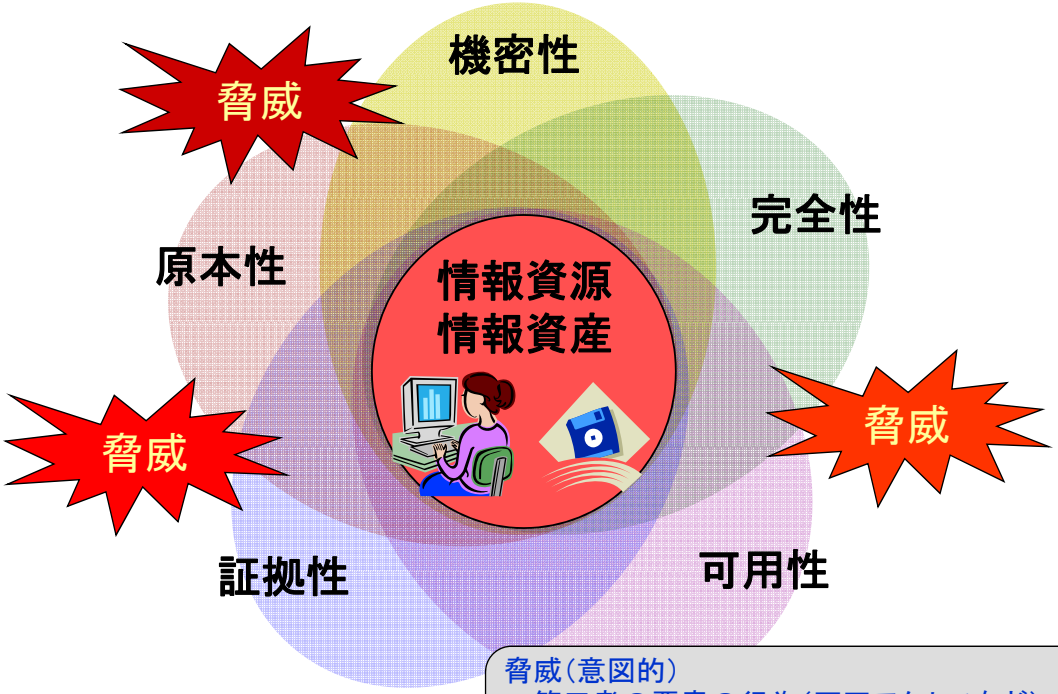
②完全性（Integrity）：ネットワーク上やコンピュータ内の情報が常に完全な形で保たれ、不正によって改ざんされたり破壊されたりしないこと。

③可用性（Availability）：ネットワーク上やコンピュータ内の情報や資源（通信路やコンピュータ）がいつでも利用できること。

④証拠性（Evidential）：相手に契約書などの文書を偽造・改ざんさせない（偽造・改ざんの有無が確認できる）、不当に事後否認させないこと。

⑤原本性（Original）：情報（コンピュータプログラム、マルチメディアデータなど）をコピーできない、あるいは不正にコピーされないこと。

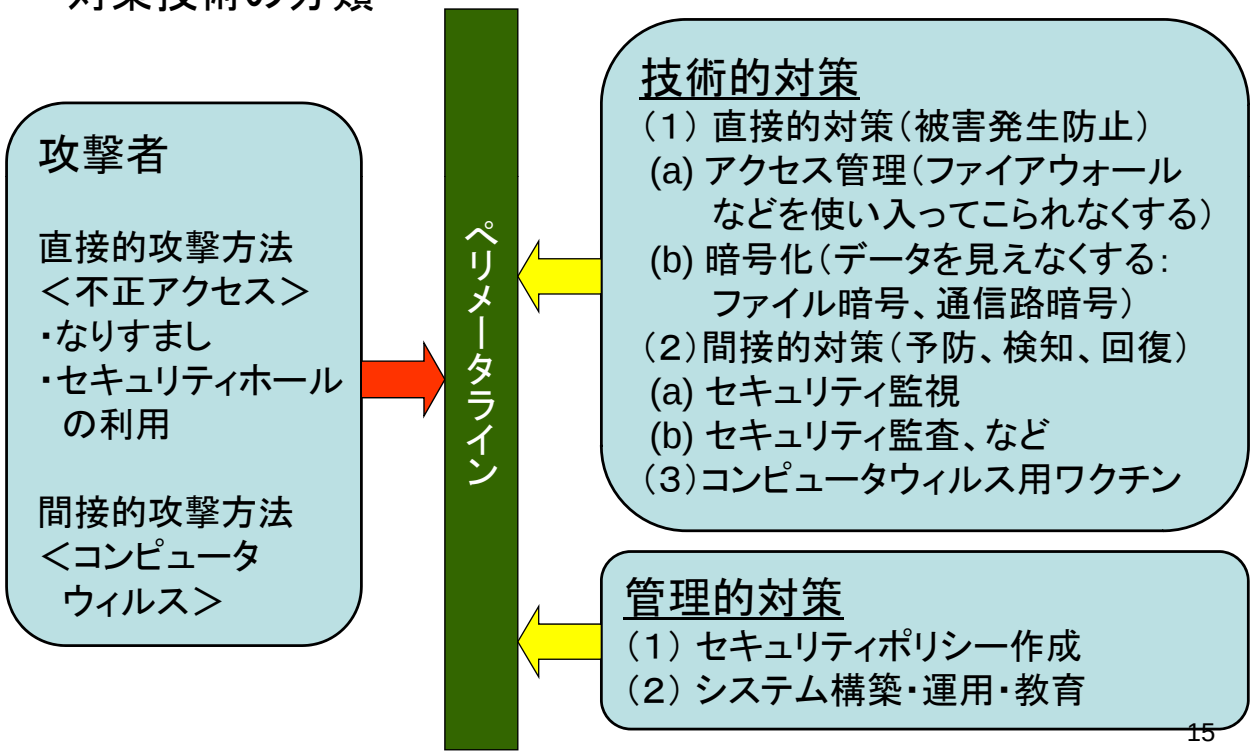
脅威（偶発的）
－天災（地震、火災、水害、・・・）
－故障（HW故障、SW故障、回線障害、・・・）
－誤動作（データ入力ミス、誤接続、SWバグ、・・・）



脅威（意図的）
－第三者の悪意の行為（不正アクセスなど）
－取引相手の悪意の行為（取引内容の事後否認、コンテンツの不正コピーなど）

セキュリティを守る技術の概要

対策技術の分類



管理的対策：セキュリティポリシーについて

- セキュリティポリシー：　セキュリティに関する組織（自治体、企業などの組織）としての方針
- セキュリティポリシーの策定
- セキュリティポリシーに基づくセキュリティ対策システムの構築と運用、セキュリティ教育の実施

情報セキュリティ（宮崎明雄）

アクセス管理技術

- アクセス管理技術の分類
- ユーザ認証技術
- クライアント認証技術
- リモートユーザ認証技術
- アクセス制御
- ファイアウォール
- セキュリティ評価基準

侵入を防止するアクセス管理技術

① **エンティティ認証（Entity Authentication）技術**：人や物の正体が本当に主張している人や物であるかを検証する技術

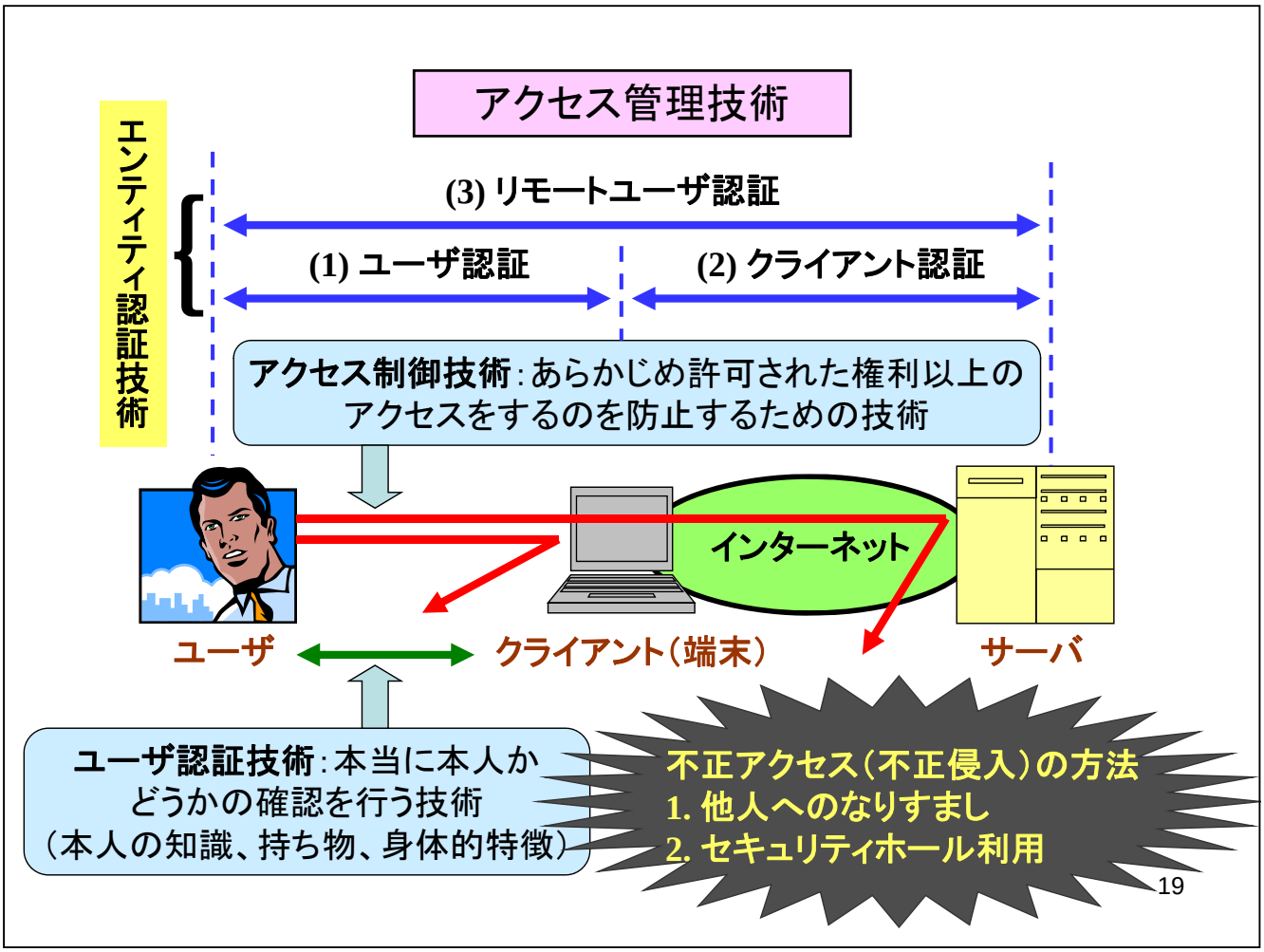
② **アクセス制御（Access Control）技術**：それぞれの人や物が、あらかじめ許可された権利以上のアクセスをするのを防止するための技術

不正侵入の方法

① **他人へなりすましての侵入**（パスワード認証の場合、何らかの方法で、(a) 他人のパスワードを入手する、(b) 他人のパスワードを類推しつつ、合致するまで繰り返す方法が考えられる。）

② **セキュリティホール（セキュリティ上の問題点）を利用しての侵入**（メールサーバプログラムsendmailのセキュリティホールなど）

③ **DOS (Denial Of Service) 攻撃**（外部からの攻撃。正当な利用者にコンピュータなどを使わせなくする攻撃。大量のデータを攻撃対象とするサーバに送り、正当な利用者に使わせなくする。）



エンティティ認証技術の概要

ユーザ認証技術

① **本人の知識を利用するもの（パスワード認証技術）**：IDナンバー、暗証番号、パスワードなど ⇒ 実装が容易、忘れる危険性、類推が可能

② **本人の持ち物を利用するもの**：磁気カード、ICカードなど ⇒ 偽造が困難（？）、失くす可能性、特別な読み取り装置が必要

③ **本人の身体的特徴を利用するもの**：指紋、声紋、網膜パターンなど ⇒ 他人の偽造が困難、確実性が高い、プライバシー問題、変更が不可能、特別な装置が必要

クライアント（端末）認証技術

サーバ側からみて、クライアントが正しいものかどうかを確認する。
⇒ 共通鍵暗号を用いるチャレンジ・アンド・レスポンス法

リモートユーザ認証技術

リモート環境において、サーバ側でユーザを認証する。
⇒ パスワード＋通信路暗号方式（ワンタイムパスワード方式）

アクセス制御技術の概要

①**クライアントコンピュータでのブロック**：パスワードが合致していないような場合には、クライアントへの侵入を拒否する。

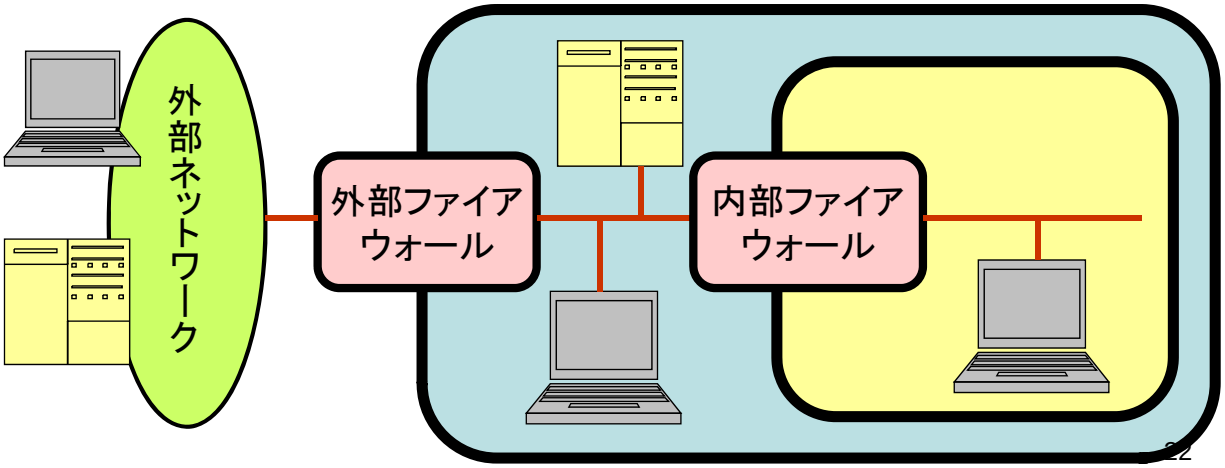
②**ネットワークの入り口でのブロック（ファイアウォール（firewall, 防火壁）技術）**：特定のネットワークへの不当な侵入を防止する。企業用ネットワークとインターネットを接続し、その間で選択的にデータのやり取りを行う場合には重要な技術である。

③**サーバでのブロック**：OS（オペレーティングシステム）の機能を用いて、ユーザによって、見ることも書き込むこともできないファイル、見ることはできるが書き込めないファイル、見ることも書き込むこともできるファイルを設定する。その設定により権利の無い主体の不正アクセスを制御する。

ファイアウォールの概要

① **外部ファイアウォール**：外部ネットワークからの不正な侵入を阻止するとともに、内部ネットワークからの不用意な情報の流出を防止することを目的とし、外部ネットワークと内部ネットワークの接続点に設置する。

② **内部ファイアウォール**：内部ネットワークにおいて、さらにサブネットワークが複数存在する場合に、各サブネットワーク間での情報の流通を制御することを目的として、サブネットワーク間の接続点に設置する。



ファイアウォールの機能要件

a. **アクセス制御**: ネットワークの間で転送されるデータ、または利用ユーザさらにはコンピュータなどのアクセス対象資源の制限を実施する。

b. **認証**: 利用を試みるユーザやコンピュータが、確かに正当なアクセス権をもっているかどうかを検証する。

c. **暗号化**: パスワードや転送データの暗号化を実施する。

d. **監視**: ネットワーク上のトラフィック量、またはコンピュータやルータなどの通信機器の現在の使用状況や現在のアクセスログなどの状況を監視する。

e. **監査**: 実際にアクセス制御が正当に実施されていたかを、アクセス制御を実施したコンピュータの稼動環境や稼動状況を定期的に監査する。