資料2

技術的、マネジメントからみた テレワーキングのための セキュリティ対策

情報通信研究機構

中尾　康二

背景：今日のビジネス環境における期待・危険要因

期待

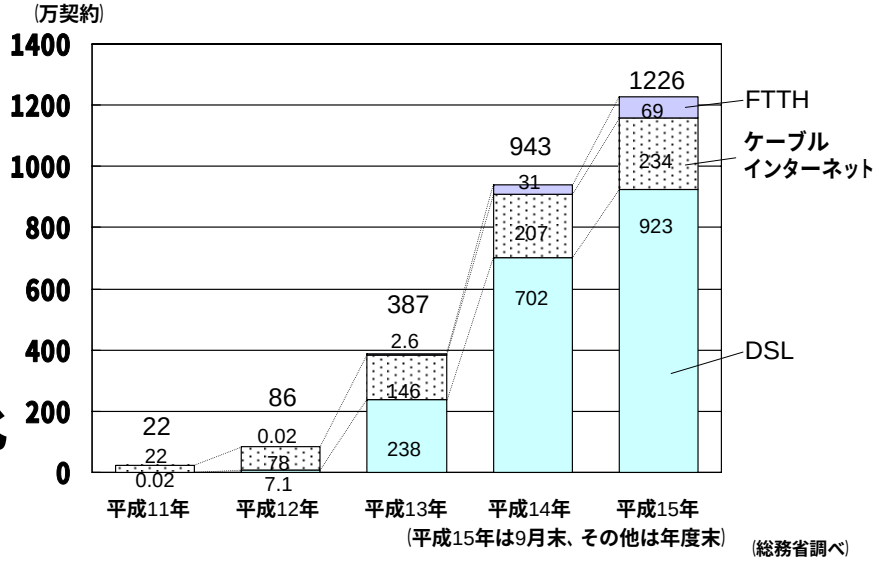
＊顧客やマーケットの要求増大
＊ビジネスパートナー化
＊アクセスの容易性の向上
＊オンラインサービス／Eコマース
＊移動体サービス／広域コミュニケーション

危険要因

＊ITに強度依存体質
＊広域ネットワークによる接続性、利便性の向上
＊ビジネス環境の広がり、分散化

ネットワークへの依存の高まりとセキュリティ被害の深刻化

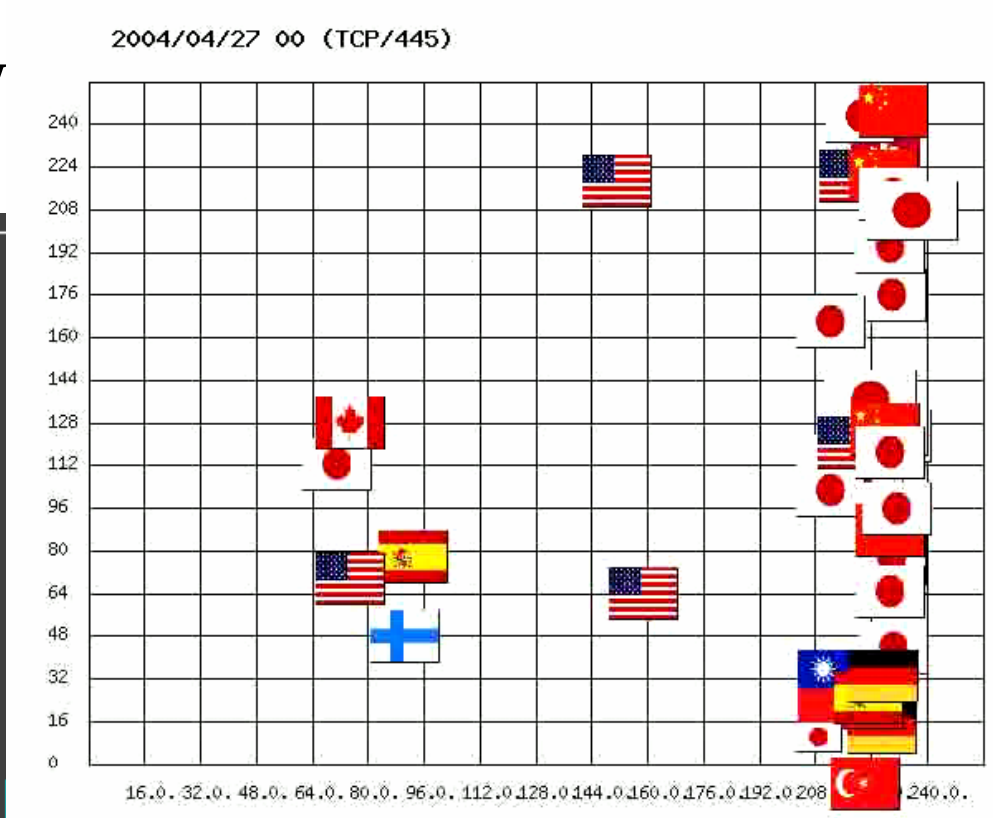
- ブロードバンド、常時接続の普及
  - ブロードバンド回線契約数は1,226万(2003年9月末)
- 社会活動のネットワークへの依存の高まり
  - インターネット利用の高度化と多様化



- インターネットへの脅威の増加
  - Slammer、Blaster等ウイルス、ワームの蔓延が引き起こすセキュリティ被害の深刻化

- ワームの悪質化(インターネットに接続しただけで感染)
- 最新のセキュリティパッチを適用していない多数のユーザの存在
- ネットワークも攻撃対象に

Example：Sasser W

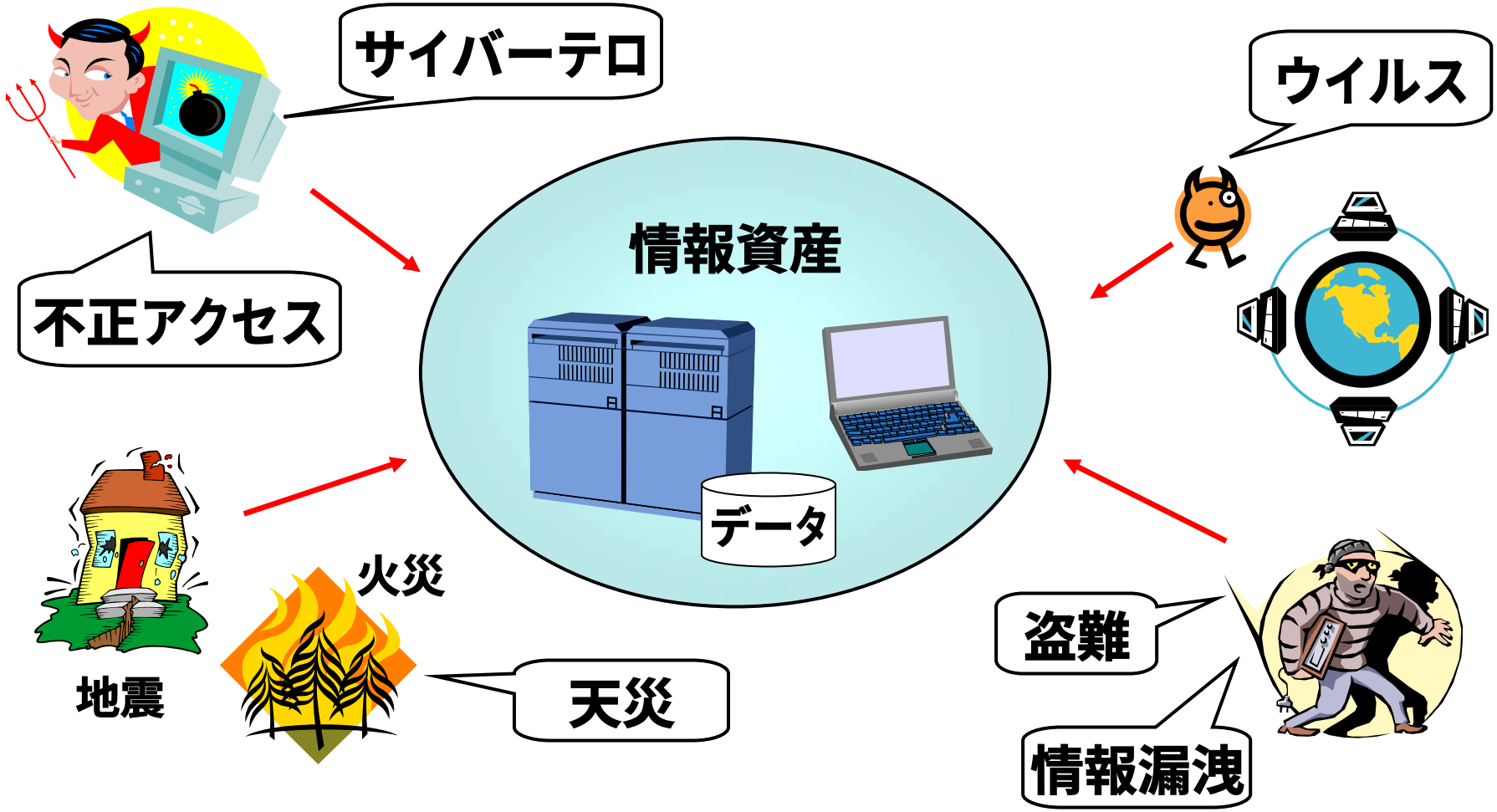


Simple statistics

TCP Scans

WORM Packets

情報セキュリティにおける脅威とは



＜意図的な攻撃、事故、災害＞

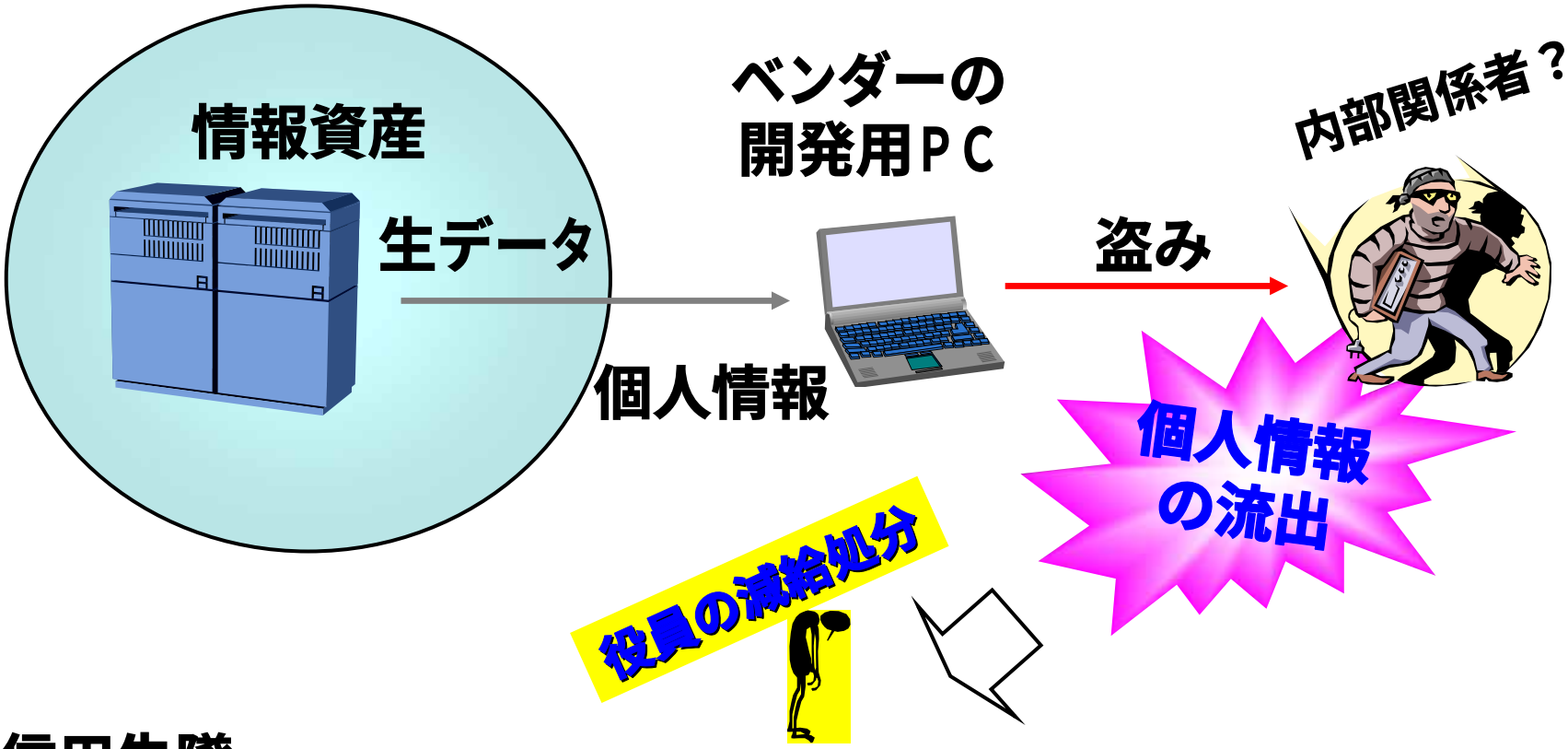
・情報資産の機密性・完全性・可用性を失わせ、組織に影響を与えるもの。

セキュリティに関する脅威の分類

大分類	中分類	小分類
ワーム、ハッキング等の攻撃による脅威	侵入攻撃による脅威	情報漏洩
		改竄
		なりすまし
		踏み台
		バックドア
	DoSによる脅威	ネットワーク輻輳
		サービスダウン
		サービス一時停止
待ち伏せ攻撃による脅威	クロスサイトスクリプティングによる脅威	情報漏洩
		信頼関係悪用
	盗聴（スパイウェア等）による脅威	情報漏洩
物理的攻撃による脅威	ソーシャルエンジニアリング等による脅威	情報漏洩

インシデント事例　～情報漏洩～

B社の顧客情報５６万人分の会員カード情報流出が発覚。
（2003年6月）



・信用失墜
・顧客への詫び状、商品券送付（500円×全会員115万人⇒5億7500万円！）

情報セキュリティ対策とは（具体例）

情報セキュリティ対策の実施

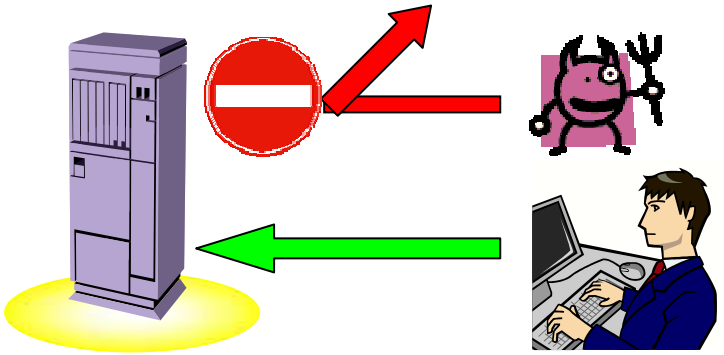
①物理的対策

不正侵入等から保護

②人的対策

情報セキュリティの
重要性の周知徹底

③技術的対策



情報資産へのアクセス制御

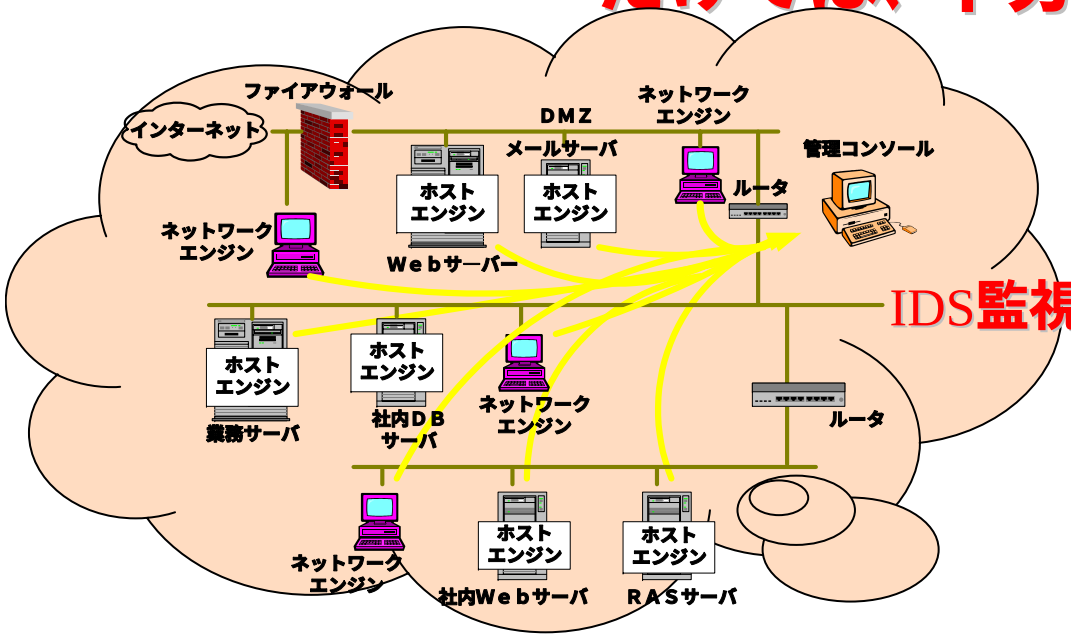
④運用等における対策

情報セキュリティ対策の
遵守状況の確認

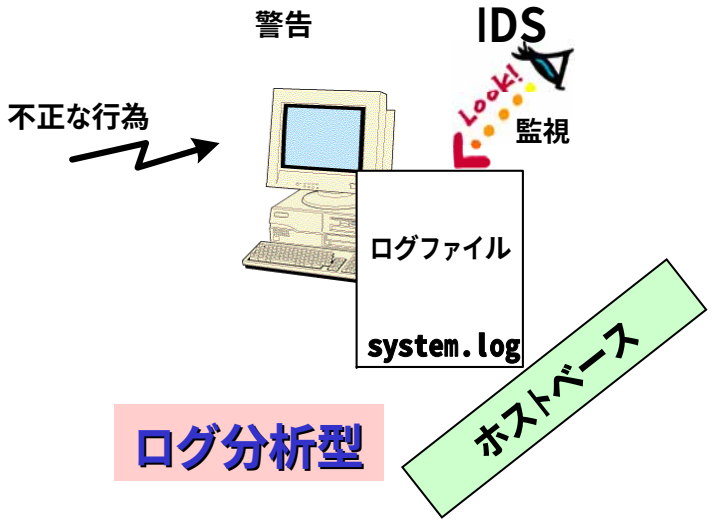
⑤緊急時における対策

危機管理面の整備

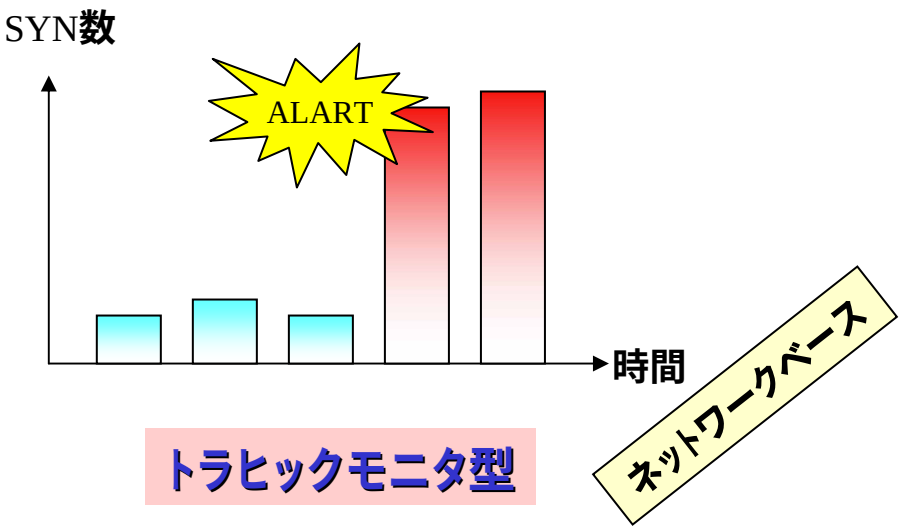
技術的な対策（管理策）、例えば、不正検知技術だけでは、十分でない。



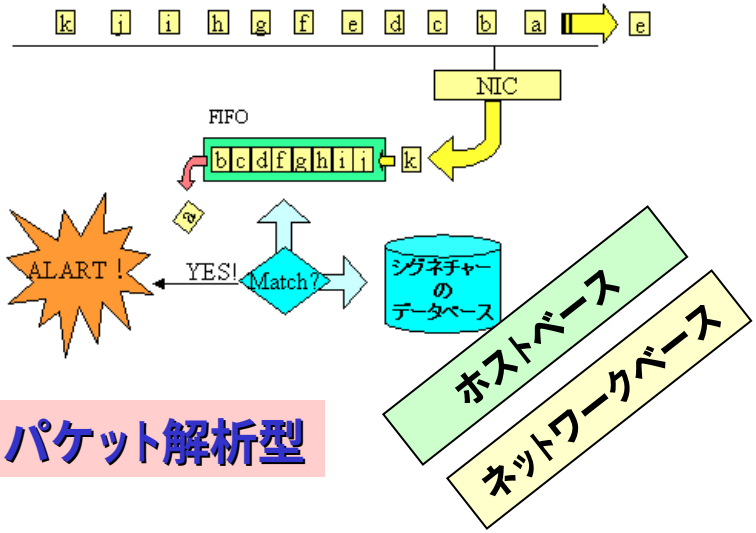
IDS監視構成



ログ分析型



トラヒックモニタ型



パケット解析型

Contents of ISO/IEC17799(改版前)

10 Security Management Domains (マネジメント領域)

1. Security policy (セキュリティポリシー(基本方針))
2. Security organisation (組織のセキュリティ)
3. Asset classification & control (資産の分類及び管理)
4. Personnel security (人的セキュリティ)
5. Physical & environmental security (物理的及び環境的セキュリティ)
6. Communications & operations management (通信及び運用管理)
7. Access control (アクセス制御)
8. Systems development & maintenance (システムの開発及び保守)
9. Business Continuity (事業継続管理)
10. Compliance (コンプライアンス(適合性))

36 Objectives (目的)

Specifies requirements

127 Security Controls (セキュリティ対策)

Satisfies objectives?

ISO/IEC **17799**における Teleworking (**改版：最新**)

11.7.2 Teleworking

Control

A policy, operational plans and procedures should be developed for teleworking activities.

Implementation guidance

Organizations should only authorize teleworking activities if they are satisfied that appropriate security arrangements and controls are in place and that these comply with the organization's security policy.

Suitable protection of the teleworking site should be in place against, e.g., **the theft of equipment and information**, the unauthorized disclosure of information, unauthorized remote access to the organization's internal systems or misuse of facilities. Teleworking activities should both be authorized and controlled by ***management***, and it should be ensured that suitable arrangements are in place for this way of working.

以下の内容を考慮する必要がある。

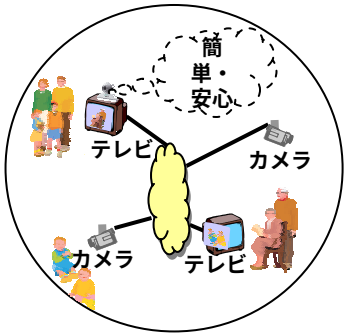
1) 遠隔作業の場所の既存の物理的なセキュリティの確保。
   建物及び周辺環境の物理的セキュリティを考慮すること。
2) 提案された物理的な遠隔作業の環境を利用。
3) 遠隔作業の通信に関するセキュリティ要求事項の明確化
   ＊組織の内部システムへの遠隔アクセスの必要性，
   ＊アクセスや情報交換などの通信情報の取扱いに慎重度合，
   ＊アクセスする内部システムの取扱いに慎重を要する度合。
4) 住環境を共有する者（例えば，家族，友達）からの情報又は資源への認可されていないアクセスの脅威を考慮。
5) テレワークで利用する資源の知的財産管理の考慮。
6) テレワーク環境への個人端末を用いたアクセスに関するセキュリティチェックの徹底。
7) 利用するソフトウェアに関するライセンス管理の徹底。
8) 利用環境でのウイルス駆除環境構築、FW利用の徹底。

さらに以下の追記内容がある。

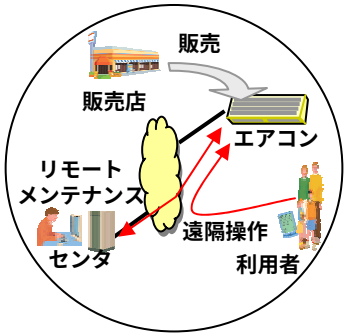
a) テレワーク活動のための適切な装置及び保管棚・庫の準備。
b) 許可される作業，作業時間，保持してもよい情報の分類，及び，テレワーク作業者のアクセスが認可される内部システム・サービスの明確化。
c) 安全な遠隔アクセスを図る方法も含め，適切な通信装置の配備、準備。→ 必要な技術のガイドライン：例) ISO 18028
d) 遠隔作業を行う場所の物理的なセキュリティ。
e) 家族及び来訪者による装置及び情報へのアクセスに関する規則及び手引。→ ガイドライン化が必要
f) ハードウェア及びソフトウェアの支援及び保守の規定。
g) バックアップ及び事業継続のための手順。
h) 監査及びセキュリティの監視。
i) 遠隔作業をやめるときの，監督機関並びにアクセス権限の失効及び装置の返還

アプリケーション、コンテンツのセキュリティ確保

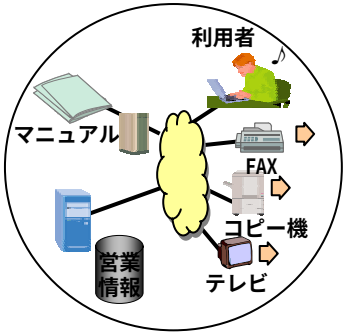
家族との遠隔
コミュニケーション



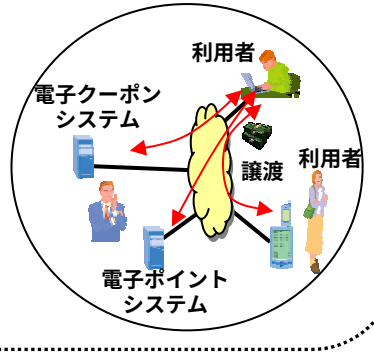
家電の遠隔操作や
リモートメンテナンス



テレワーク
(在宅勤務)



電子商取引



情報セキュリティ基盤技術の確立

情報セキュリティマネジメントの確保・普及

インターネットの安全性・信頼性を向上させる技術
（電子商取引などの基盤技術）→　セキュアなＰ２Ｐ通信の確立

本人確認機能を保有するセキュアなネットワーク基盤の構築

インターネット

サーバーセキュリティ対策に関わる技術

不正侵入、DoS、ウイルスなどに耐性のあるネットワーク基盤の構築

重点研究開発項目

提言

1) 議論内容をまとめ、テレワークのための
セキュリティ要件を明確化する。

2) セキュリティ要件を満足するためのセキュ
リティガイドラインの策定を実施する。

3) 上記ガイドラインに必要となる技術資料を
参考情報としてまとめる。