ハザード分類

1. 攻撃対象

- ネットワーク接続のPC
- サーバ
- クライアント
- ファームウェア／ハードウェア
- データ管理ソフトウェア
- インフラストラクチャユーティリティやツール

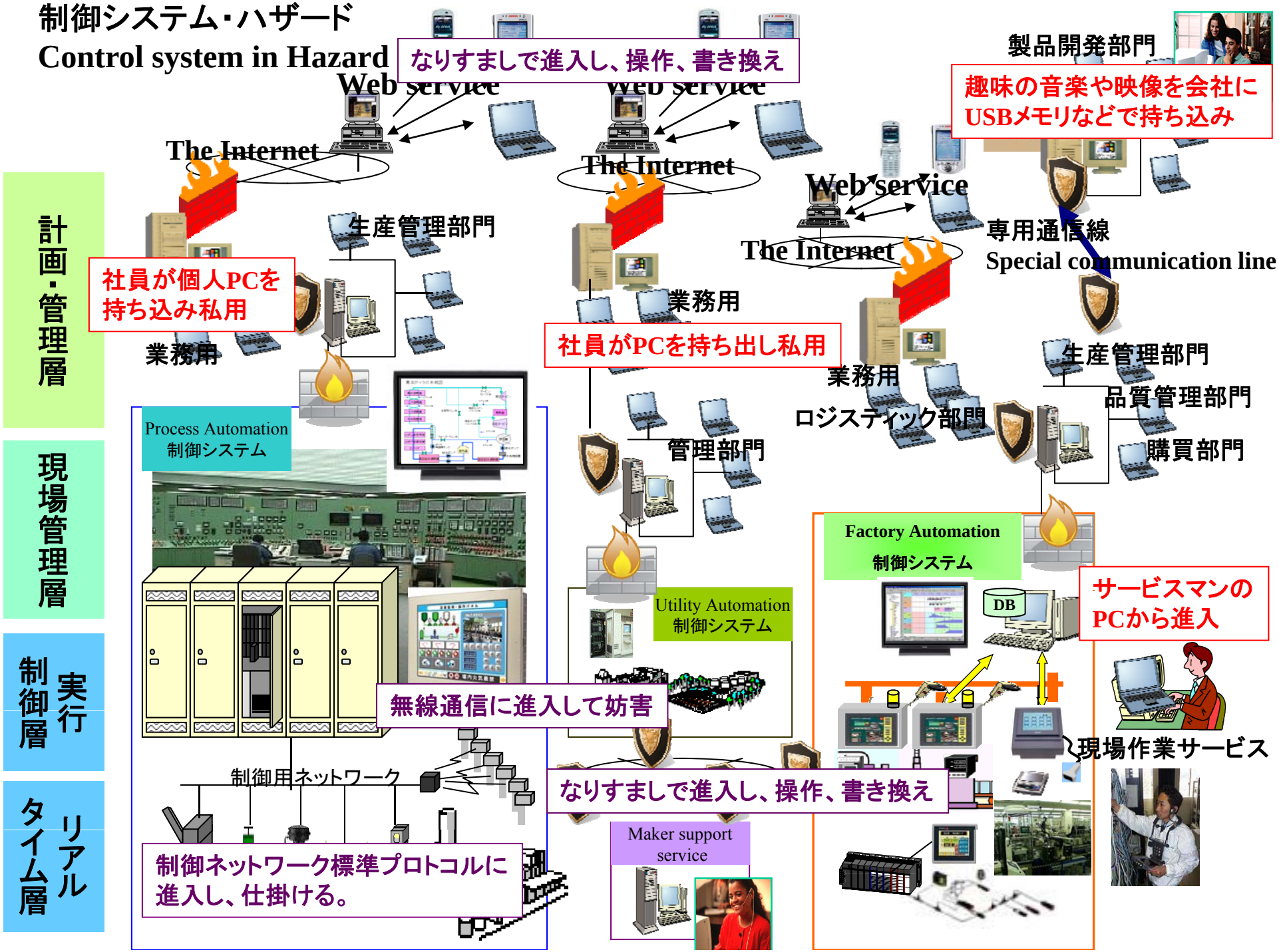
2. 現象の特徴

- ナパーム爆弾タイプ
  - 時限爆弾型
  - 条件成立型
- クラスター爆弾タイプ
  - 転移増殖型
- 工作員タイプ

3. 攻撃の分類

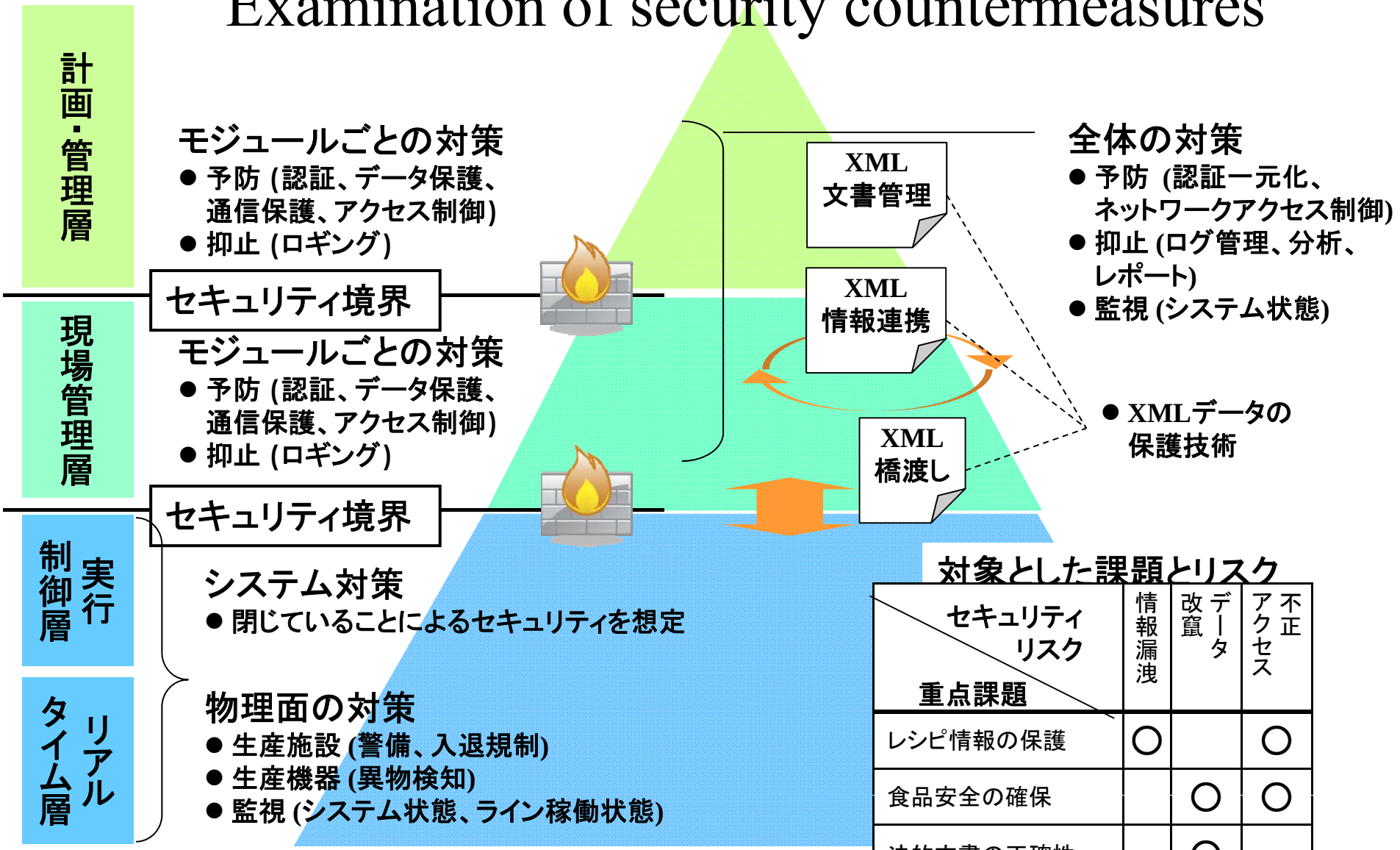
- 外部からの攻撃
  - ✓ ﾌｨｯｼﾝｸﾞ
  - ✓ SQLｲﾝｼﾞｪｸｼｮﾝ
  - ✓ Man Machine Interface in The Middle
  - ✓ ｸﾛｽｻｲﾄｽｸﾘﾌﾟﾃｨﾝｸﾞ
- 故意過失による脅威
  - 不適切な行為
    - ✓ 個人ｱｸｾｽ
  - 人為的ミス
    - ✓ PCの紛失
    - ✓ USBﾒﾓﾘの紛失
    - ✓ P2Pｿﾌﾄによるﾃﾞｰﾀ流出
  - 悪意のある不正行為
    - ✓ ID／ﾊﾟｽﾜｰﾄﾞの盗用
    - ✓ ID不正利用
    - ✓ データ書き換え
    - ✓ ﾊｰﾄﾞや媒体の持ち出し
  - 感染
    - ✓ ｳｨﾙｽ／ﾜｰﾑ
    - ✓ ｽﾊﾟｲｳｪｱ／ｷｰﾛｶﾞｰ
    - ✓ ﾎﾞｯﾄﾈｯﾄ

制御システム・ハザード
Control system in Hazard



セキュリティ対策の検討

Examination of security countermeasures



対象とした課題とリスク

重点課題 ＼ セキュリティリスク	情報漏洩	データ改竄	不正アクセス
レシピ情報の保護	○		○
食品安全の確保		○	○
法的文書の正確性		○	

MOF2008にて、XMLコンソーシアム　セキュリティ部会が取りまとめた報告書より引用

出典：MOF2008合同デモシステム向けセキュリティ報告書より

SCMや管理業務連携でのセキュリティ

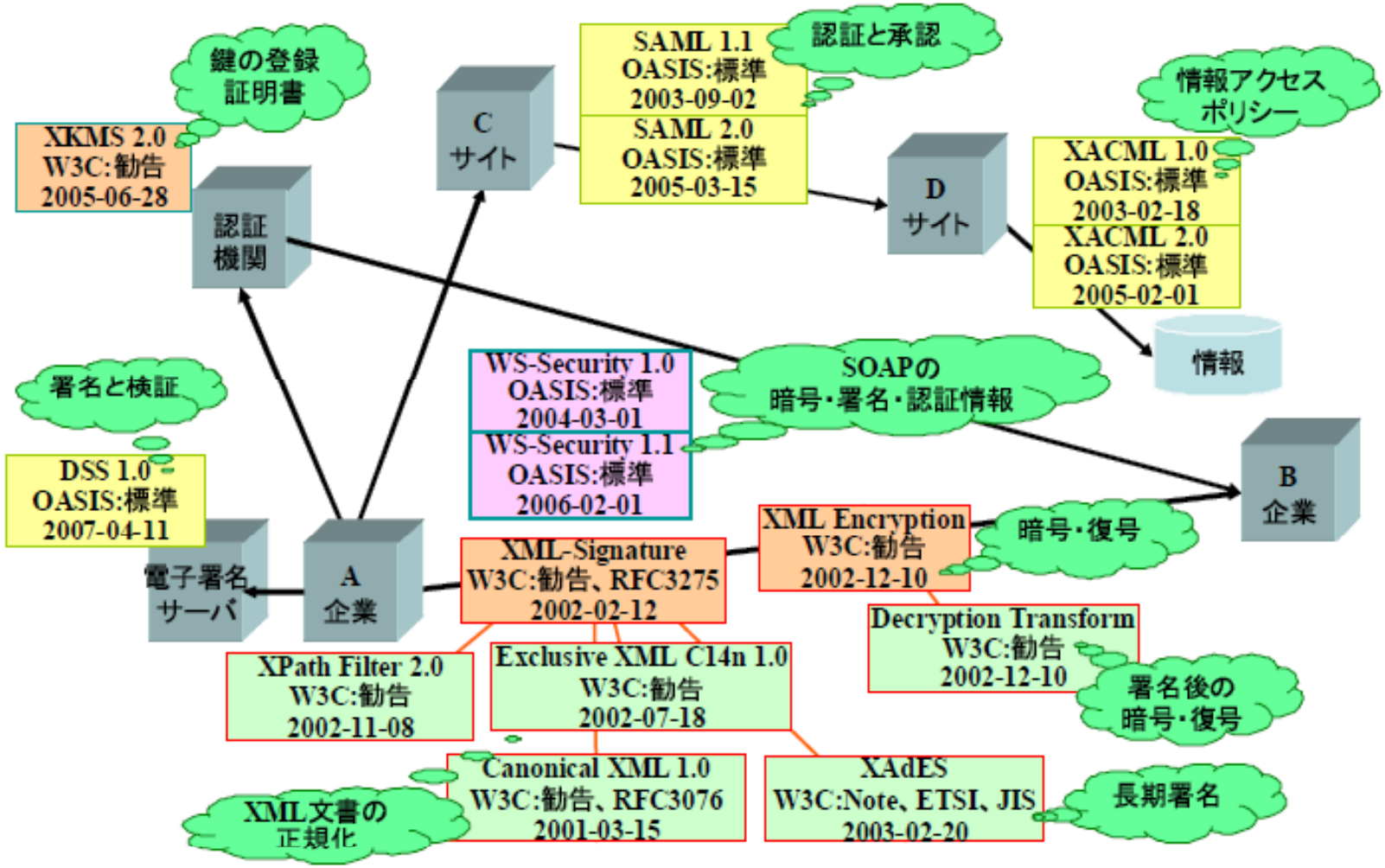


図 3 XML セキュリティ関連規格一覧

出典：MOF2008合同デモシステム向けセキュリティ報告書より

電子署名

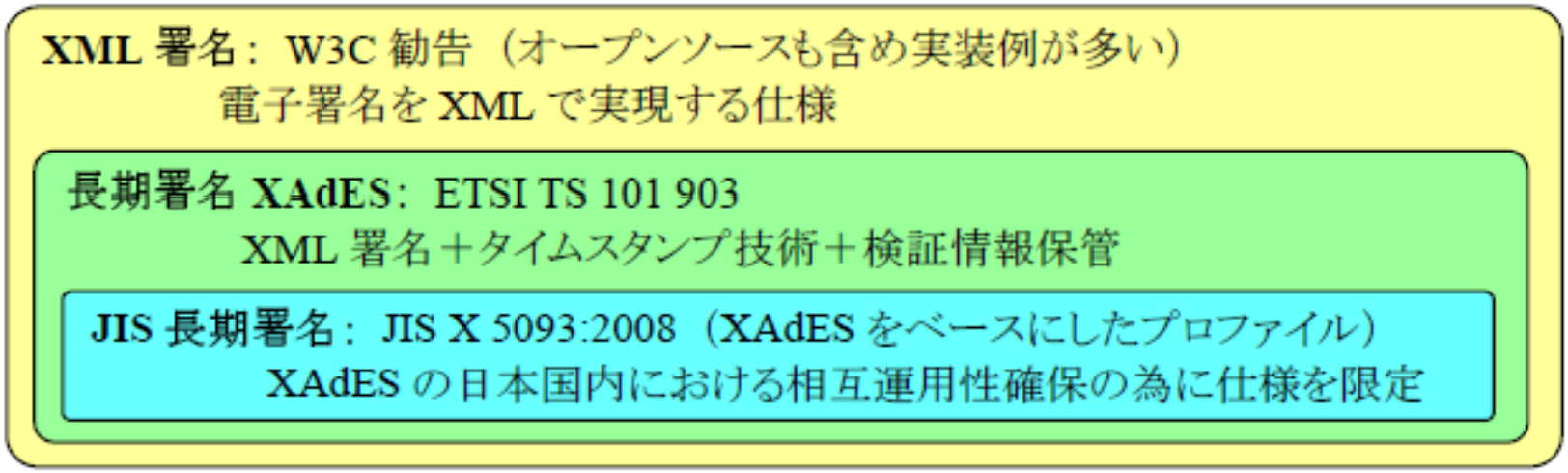


図 4 各種電子署名標準規格の関係

→ 短期的に改竄や否認を防止する目的であれば **XML** 署名で良い。

→ 正確な存在時刻を保証するなら長期署名 **XAdES**（**XAdES-T**）が必要。

→ 有効期限をこえて長期間保管するなら長期署名 **XAdES**（**XAdES-A**）が必要。

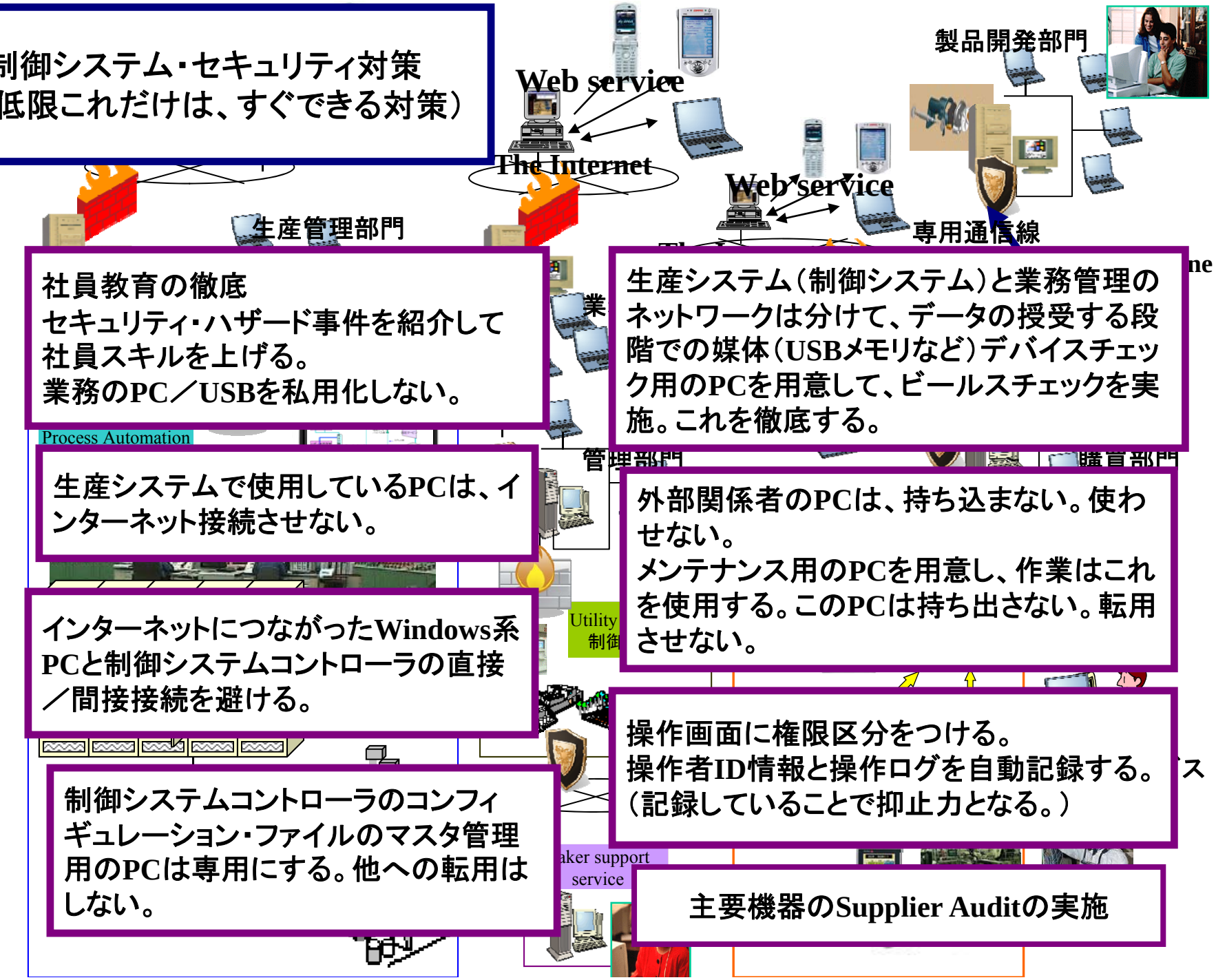
出典：MOF2008合同デモシステム向けセキュリティ報告書より

セキュリティ対策の評価

- 客観性と網羅性をもって評価するには…
- 情報セキュリティマネジメント (ISMS)
  - JIS Q 27001:2006「情報技術―セキュリティ技術―情報セキュリティマネジメントシステム―要求事項」（http://www.webstore.jsa.or.jp）
  - 国際標準ISO/IEC 27001の日本語訳
  - リスク管理や、PDCAサイクルに沿ったセキュリティ管理など
- より具体的なセキュリティ対策の評価
  - JIS Q 27002:2006「情報技術―セキュリティ技術―情報セキュリティマネジメントの実践のための規範」
  - 国際標準ISO/IEC 17799の日本語訳
  - アクセス制御、暗号化やネットワークセキュリティを含む通信及び運用管理などについても規定

出典：XMLコンソーシアムセキュリティ部会　VEC協賛セミナーでの発表資料より

制御システム・セキュリティ対策
（最低限これだけは、すぐできる対策）



社員教育の徹底
セキュリティ・ハザード事件を紹介して社員スキルを上げる。
業務のPC／USBを私用化しない。

生産システム（制御システム）と業務管理のネットワークは分けて、データの授受する段階での媒体（USBメモリなど）デバイスチェック用のPCを用意して、ビールスチェックを実施。これを徹底する。

生産システムで使用しているPCは、インターネット接続させない。

外部関係者のPCは、持ち込まない。使わせない。
メンテナンス用のPCを用意し、作業はこれを使用する。このPCは持ち出さない。転用させない。

インターネットにつながったWindows系PCと制御システムコントローラの直接／間接接続を避ける。

操作画面に権限区分をつける。
操作者ID情報と操作ログを自動記録する。
（記録していることで抑止力となる。）

制御システムコントローラのコンフィギュレーション・ファイルのマスタ管理用のPCは専用にする。他への転用はしない。

主要機器のSupplier Auditの実施