急激に変化する環境に対応した情報セキュリティへのアプローチ

A New Approach to Information Security in Rapidly Changing Environment

2013年6月7日

JSSA情報セキュリティ専門監査人部会&情報セキュリティ研究プロジェクト
合同プロジェクト

内藤　裕之

1.研究プロジェクトの概要

名称

情報セキュリティ合同研究プロジェクト

※情報セキュリティ専門監査人部会と情報セキュリティ研究プロジェクトの合同研究（2008年度より）

活動方法

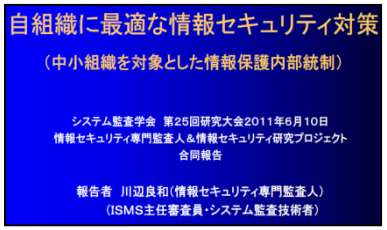
月1回程度のミーティング（大崎、五反田等）と、メーリングリスト、サイボウズLIVEを使用しての情報交換、共有と資料作成

研究会メンバー	
斎藤　敏雄（主査）	日本大学
植野　俊雄	ISU
川辺　良和	㈲インターギデオン
黒川　信弘	情報セキュリティ専門監査人
小谷野　幸夫	㈱さいたまソリューションズ
高野　美久	NECソフト㈱
高橋　孝治	公認会計士
鳥越　真理子	NRIセキュアテクノロジーズ㈱
内藤　裕之	ブリーズ・コンサルティングオフィス
永井　好和	山口大学
長野　加代子	㈱ピーアンドアイ
西澤　利治	㈱電脳商会
西川　征一	㈱西川技術士事務所
水谷　穣	水谷情報技術士事務所
山本　孟	MHOアシストラボ
芳仲　宏	東京地方裁判所

2.今年度の研究テーマ

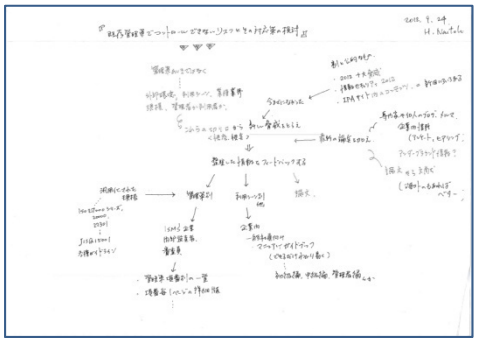
- ここ数年、研究プロジェクトでは既存のセキュリティ管理策に対して、中小組織向けの追加管理策の検討や、システム監査との関係などを研究してきた。
- しかし、昨今の急激な環境変化により、既存の管理策そのものが新たに発生したリスクに対してコントロールしきれないのではないかという疑問が出てきた。
- そこで、今年度は、管理策ありきではなく、環境（情報やシステムの利用シーン等）の変化から新たな脅威をとらえ、リスクへのアプローチ方法を研究することとなった。

2010



2011

2012


今年度の研究開始当初のメモ。これが出発点。

3.環境変化と新たな脅威の顕在化①

組織を取り巻く環境変化
ICTの急激な発展
グローバル化
少子高齢化
省資源、省エネルギー、地球環境の保全意識の高まり

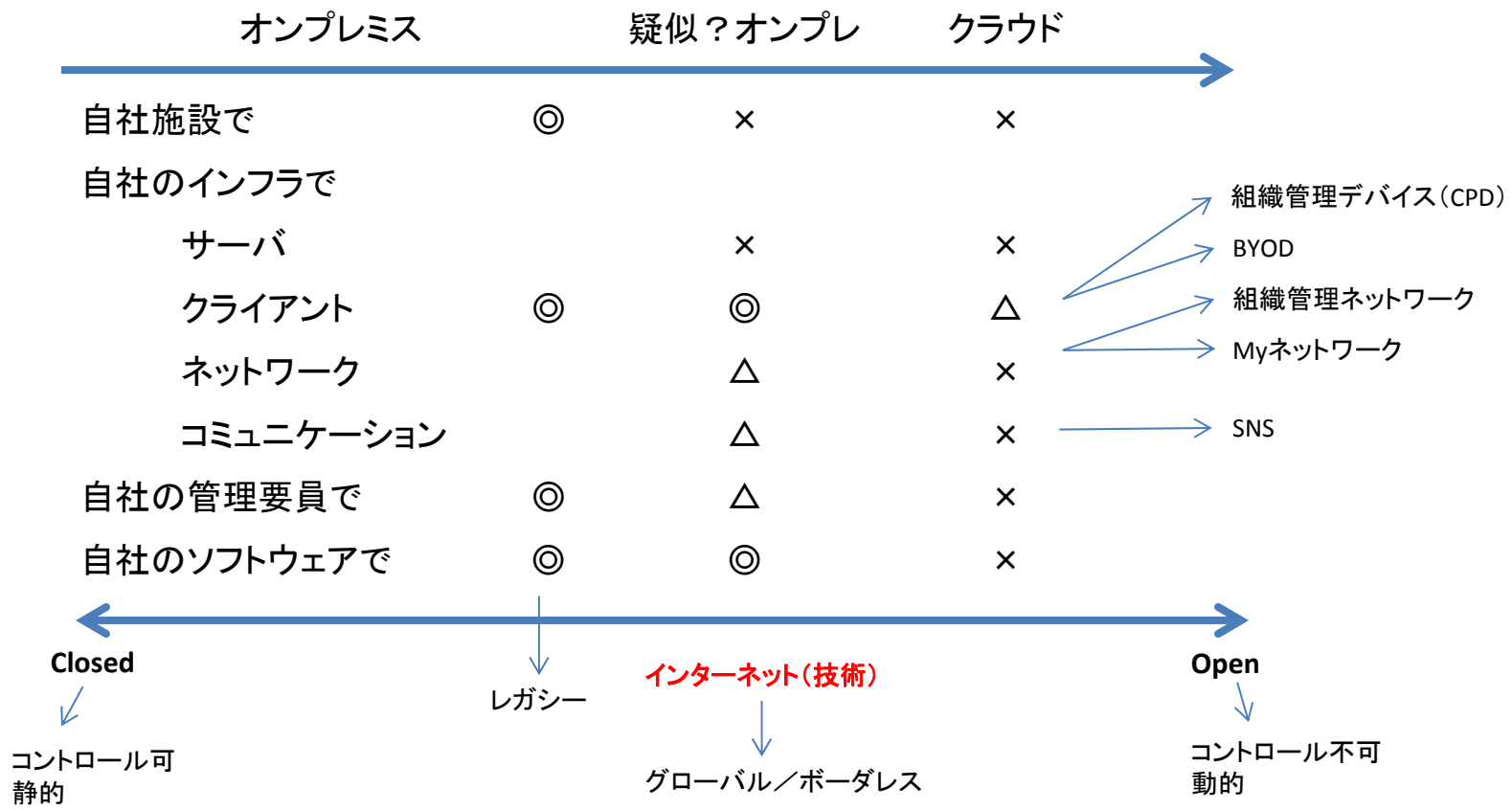
ICTの発展により生じていること
ITのコモディティ化
ITの新たな利用法の出現
コミュニケーション手段の多様化
ワークスタイルの多様化
ITを介した新たな業務の出現
ITによる大量データの収集と拡散
実世界とITが緊密に結合されたシステムの出現

ICTの発展が人々の生活と社会に与える影響を抽象的に表現すると

閉鎖から開放へ
不連続から連続へ
地理的距離の消滅
境界の消滅
24時間体制
予測できない因果連鎖の出現
ブラックボックスの増加
コントロールできない領域の増加

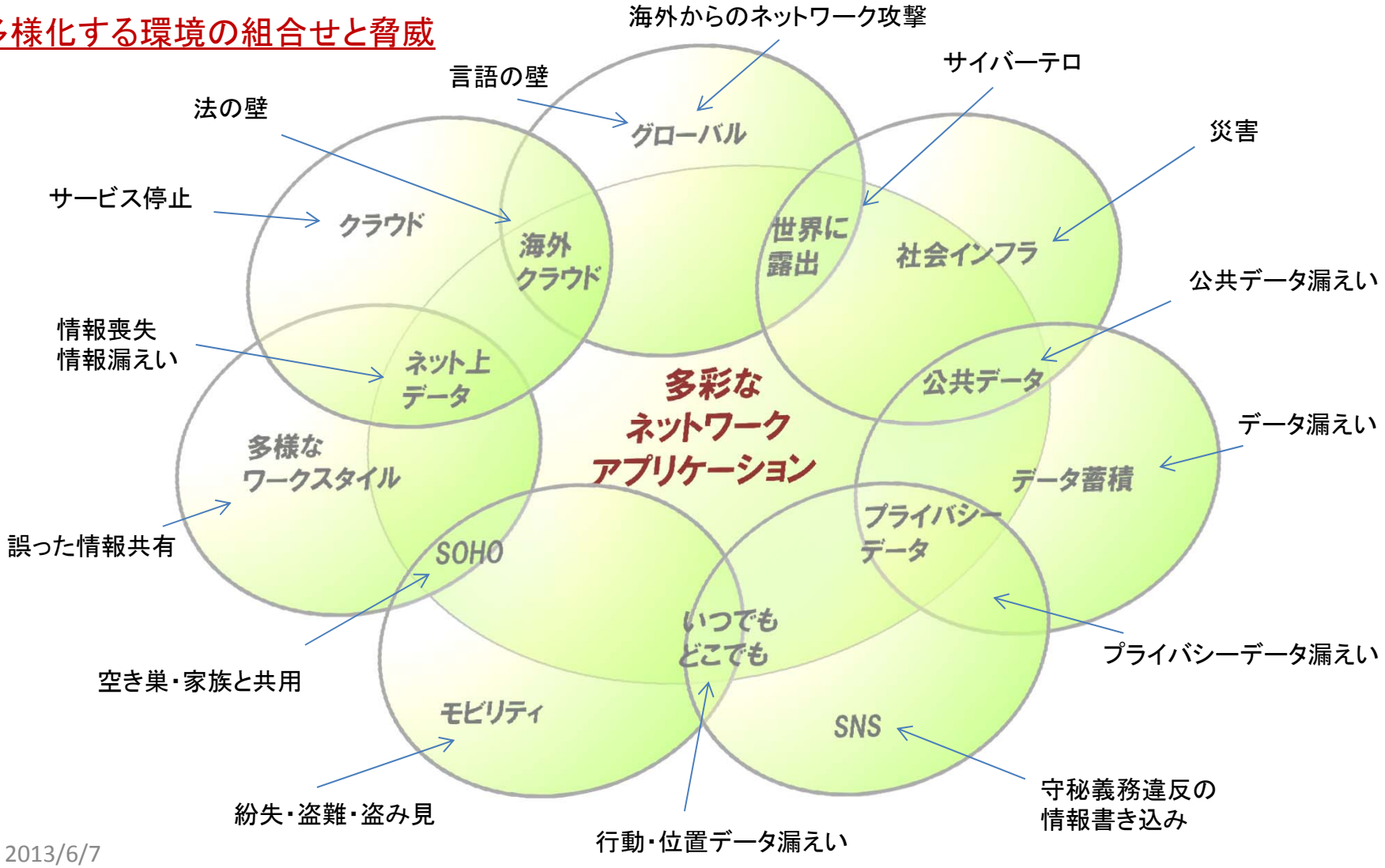
3.環境変化と新たな脅威の顕在化②

- 情報利用もオンプレミスからクラウドへ移行中



3.環境変化と新たな脅威の顕在化③

多様化する環境の組合せと脅威



2013/6/7

3.環境変化と新たな脅威の顕在化④

- 新しい利用環境の組合せで発生する脅威
  - 複数の利用環境が互いに交差して構成される総合的利用環境には、互いに交差する環境を経由した新しい脅威が生まれる。
- 利用環境の変化に伴うリスクの高まり
  - BYOD拡大　→　業務の情報漏えいリスクが高まる。
  - グローバル化　→　海外からの攻撃、プロ集団の標的になりうる。
  - 禁止から活用へ　→　組織の管理方法が追いつかない
  - SNS　→　組織の秘密の暴露リスク、プライバシー絡みで統制困難

→ その中で、特にワークスタイルやコミュニケーションデバイスの変化によって発生した新たな脅威について考えてみた。

4.従来型管理策、MSの限界①

従来の想定

PCは社内LANのみ

社外との通信手段はメールかVPN

持ち出しは専用PC（Windowsノート）

データは社内サーバーか専用データセンターに

携帯は会社支給のガラケー（or PHS）

新しいインフラの登場

クラウド、スマホ、タブレット
Facebook、Twitter、LINE他
ソーシャルアプリ

社員がTwitterでつぶやいた会社の機密情報がRTされ数万人に公開

ソーシャルアプリに登録したら既存のFacebook友達にスパムメールが送信される

企業のFacebookページがやらせで炎上

クラウド事業者の障害でユーザーのデータが消失（バックアップも）

大規模な地震、津波で、バックアップがすべて消失

顧客情報をevernoteにアップして外出時にiphoneでチェックしていたが、そのiphoneを紛失

新しいインフラ（クラウド、スマホ、ソーシャル）が既存の管理システムを骨抜きにする

4.従来型管理策、MSの限界②

会社のルール

コンサル会社提供の
見てくれは立派な
マニュアル

中身は・・・

データ持ち出し禁止

私用端末持ち込み禁止

自宅作業禁止

クラウドコンピューティング
スマートフォン
ソーシャルネットワーク
想定外の災害・・・

全面禁止・・・違反は見て見ぬふり

例外規定　ただし業務上必要な場合は
上長の・・・

実効なし

規定をしてもチェックできない。
気付かないうちに情報漏洩、法令違反・・・

変化し続ける環境にルールを合わせるのは至難の業

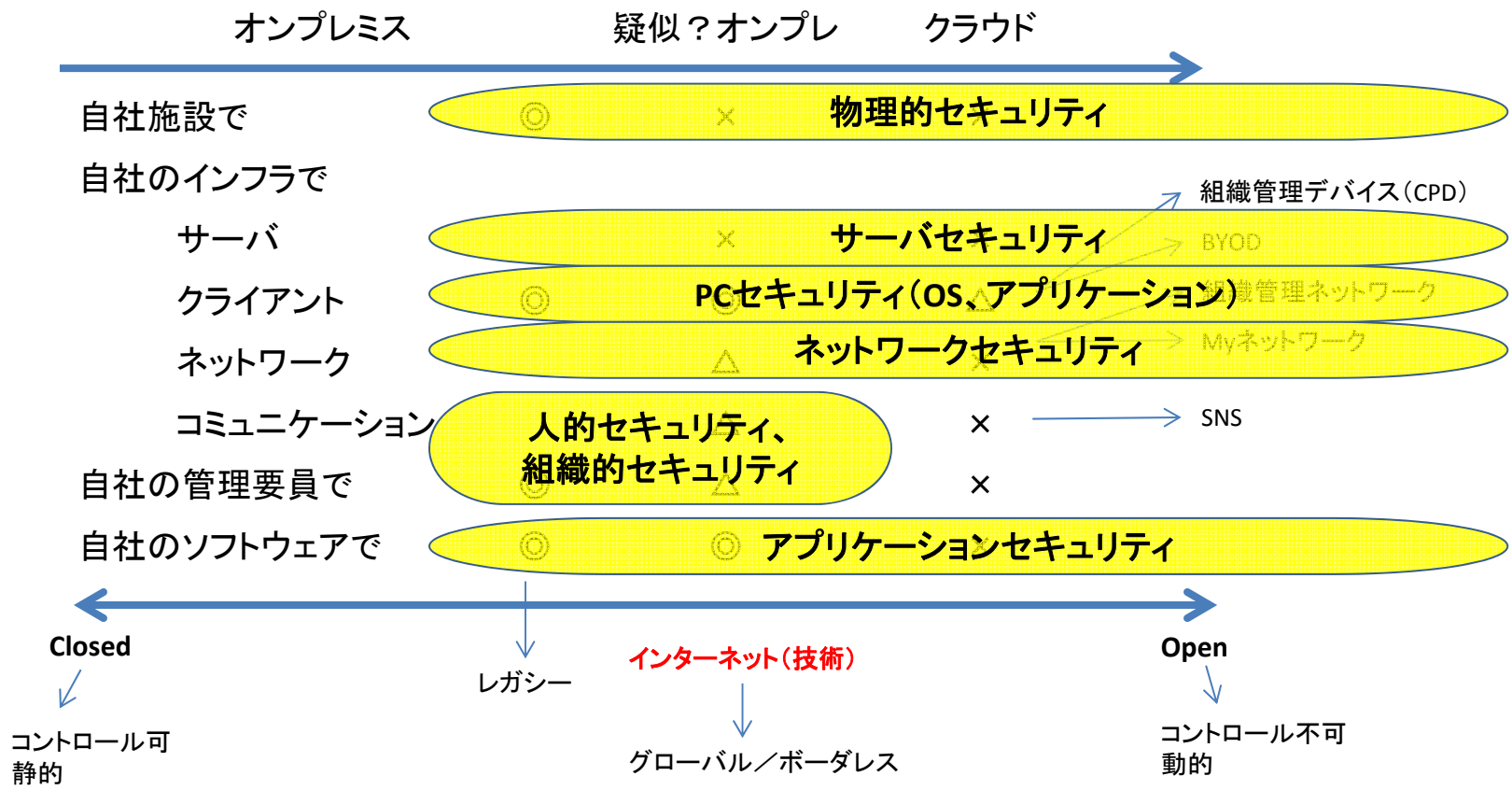
4.従来型管理策、MSの限界③

- 情報を取り扱う環境に対してルールを規定
  - 環境は常に変化する。
  - 内部環境×外部環境×媒体＝無限のパターン？
    → 人がついていけない、メンテナンスしきれない、変更ミス・・・

- ISMS（ISO27001）でも管理策の大多数は情報使用環境に対する管理策

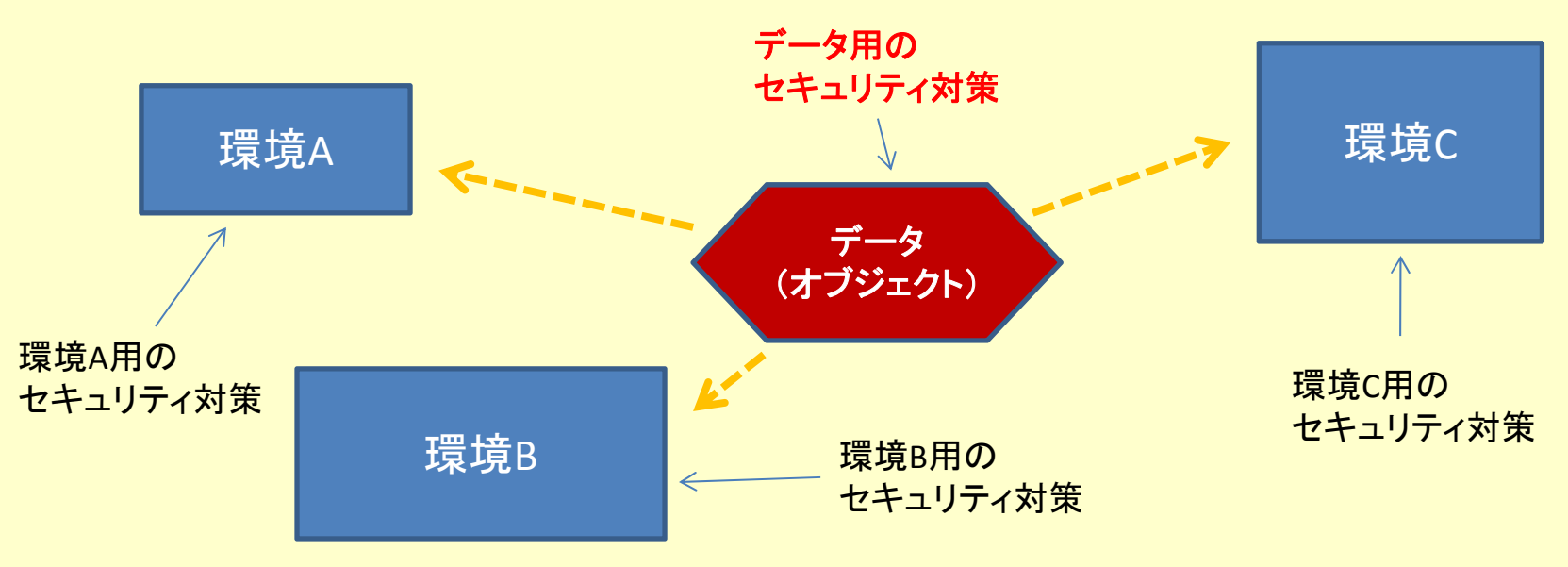
4.従来型管理策、MSの限界④

- 階層ごとに細分化されたセキュリティ対策が必要



5.環境からオブジェクトへ①

- これらの、情報を扱う環境（場所、インフラ、機器、組織etc）に対するセキュリティアプローチだけでは限界がある。
- それに対して、インフラやアプリケーション等の階層に依存しないで、オブジェクトである「データ」に対する情報セキュリティ対策に着目し、それをオブジェクトアプローチと呼ぶことにした。



5.環境からオブジェクトへ②

- オブジェクトアプローチによる管理策の例

管理目的	説明	管理策の例
データの 堅牢性維持	データはアクセスが許可されたもの以外には参照・改ざんが出来ないような形態で保管・伝送する。	データの暗号化 鍵管理 パスワードポリシー
データの 復元性維持	一つ又は二つの環境で喪失又は使用できなくても、利用できる。	データの分散保管
データの 自立性維持	データにはプロパティが付加され、プロフィールに基づいて、アクセスやデータ項目の値が制限され、完全性と責任追跡性が確保される。	IRM RMS 電子透かし
データの互換性維持	複数の異なる環境で読出し可能な保管形態をとる。	互換性の高いファイル形式での保存

6.今後に向けて（環境＋オブジェクト）

- オブジェクトアプローチの課題
  - 互換性の問題
  - ベンダー依存
- インフラ・ネットワーク環境でのセキュリティも進化している
  - 仮想化セキュリティ
  - リスクベース認証
  - シンクライアント
  - I&AM

→ **多方向からのアプローチでリスクに対処することが大切**

ex　コンテンツ、プラットフォーム、ネットワーク、デバイス

7.おわりに

- 当合同研究プロジェクトでは、毎年、情報セキュリティに関する最新のテーマと、システム監査のあり方をさまざまな切り口から議論し、継続して研究していきます。

- ご興味のある方の参加をお待ちしています。