Windowsの新しいアクセス制御ポリシー
～随意アクセス制御と強制アクセス制御～

横山 哲也
グローバルナレッジ
ネットワーク株式会社

横山 哲也(ヨコヤマ　テツヤ)

- グローバルナレッジネットワーク株式会社
  - http://www.globalknowledge.co.jp
- Windows Server関連研修を担当
- 1999年からActive Directoryを担当
  - 2003年4月～2012年3月 MVP(Directory Services)
- 2005年からVirtual Server、2008年からHyper-Vを担当
  - 2012年4月～ MVP(Virtual Machine)
- 趣味は猫写真 (http://facebook.com/magnyam)
- ブログ「ヨコヤマ企画(http://yp.g20k.jp)」
  - http://www.g20k.jp もご覧ください

本セッションの目標

■ 目標とすること

- 随意アクセス制御と強制アクセス制御の違いを提示
- 適切なアクセス制御システムの提案ができる

■ 目標としないこと

- 強制アクセス制御の具体的な設定手順
  (デモには期待しないでください)

アジェンダ

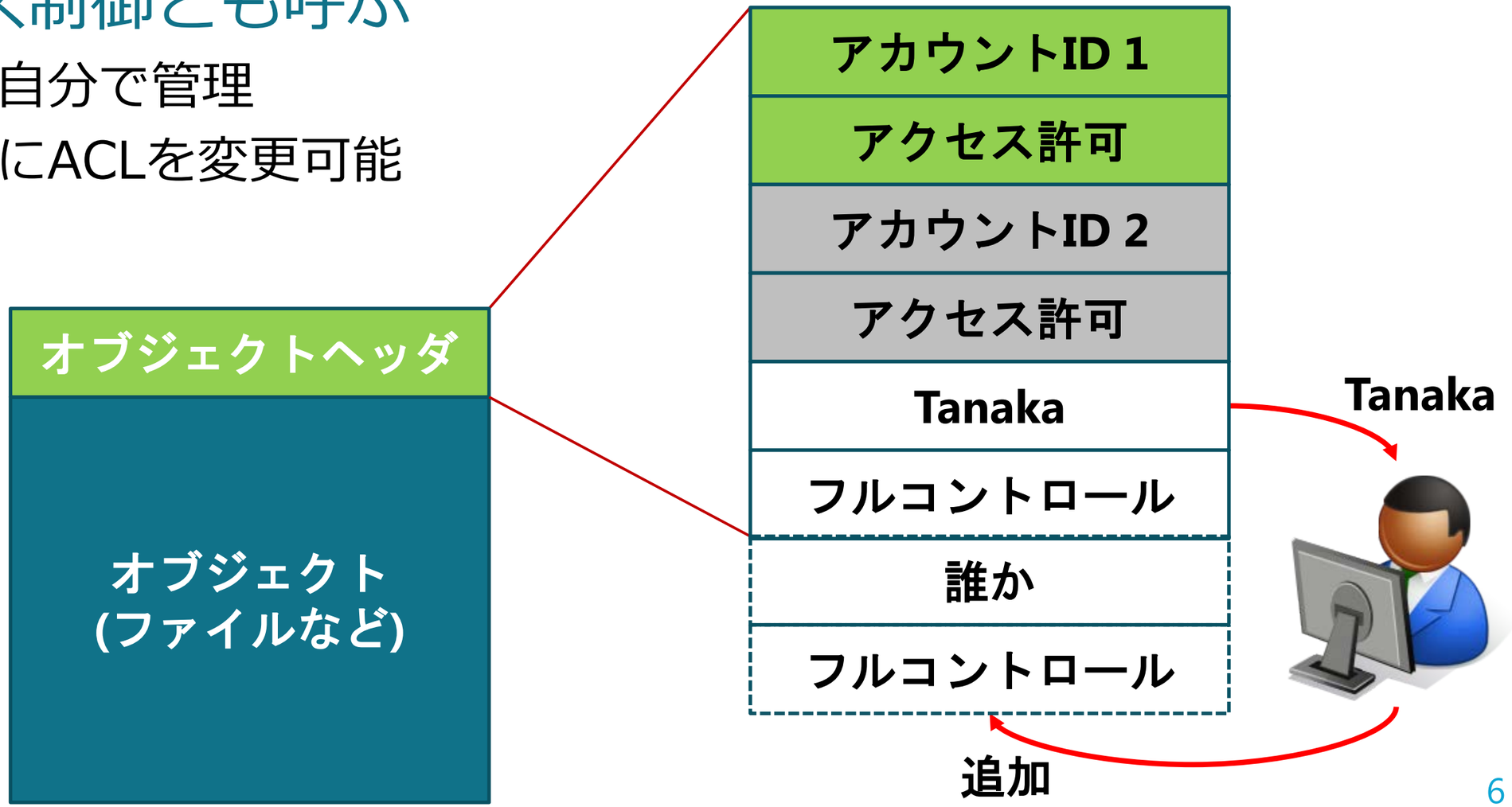
- Windowsのセキュリティモデル: 随意アクセス制御
- 新しいセキュリティモデル: 強制アクセス制御
- Windows Server 2012の新機能: ダイナミックアクセス制御
- 強制アクセス制御(集約型アクセスポリシー)の利用

Windowsのセキュリティモデル: 随意アクセス制御

Windowsのアクセス許可の基本思想
OSのセキュリティ評価基準ガイドライン
Windows vs UNIX
随意アクセス制御の利点と課題

Windowsのアクセス許可の基本思想

- 随意アクセス制御 = DAC：Discretionary Access Control
  任意アクセス制御とも呼ぶ
  - 自分のものは自分で管理
  - 所有者は自由にACLを変更可能



OSのセキュリティ評価基準ガイドライン

- セキュリティ評価基準ガイドライン
  - TCSEC(Trusted Computer System Evaluation Criteria)
  - 米国安全保障局(NSA)下のNCSC(National Computer Security Center)

クラス	正確な表現ではないが、要するに	主な要件
A	国家安全保障上の最高機密	形式定義
B	外交用	強制アクセス制御
C	一般商用	随意アクセス制御
D	セキュリティなし	

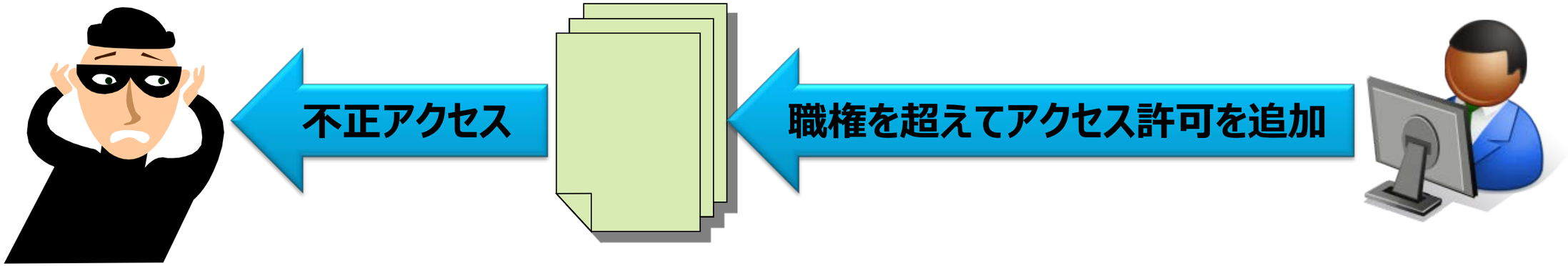
- 現在は国際標準ISO/IEC 15408: コモンクライテリア(CC)
  - Common Criteria for Information Technology Security Evaluation

Windows vs UNIX

- 随意アクセス制御
  - クラスCを満たすための条件の1つ
  - 任意の個人やグループに対して個別にアクセス許可を設定
- 古いUNIXには「所有者」と「所有グループ」の概念のみ
  - クラスCを満たさない
- Windows NT(1993年)は、最初からACLを実装
  - 「UNIXよりもセキュア(安全)である」と宣伝
- 実は、Solarisなどの商用UNIXで早くからACLが実装
  - Linuxでの実装は2003年のカーネル2.6から

随意アクセス制御の利点と課題

- 利点
  - 単純で分かりやすい
- 課題
  - アクセス制御設定の過失・不正に対応できない
    - うっかりEveryoneにフルコントロールを与えてしまう
    - うっかり読み取り許可を必要以上に多くの人に与えてしまう
    - 犯罪者に協力して読み取り権利を与えてしまう
  - コンピュータ犯罪の多くは社内の犯行



新しいセキュリティモデル:
強制アクセス制御

強制アクセス制御の意味
強制アクセス制御の利点と課題
強制アクセス制御の適用範囲
Linuxの状況

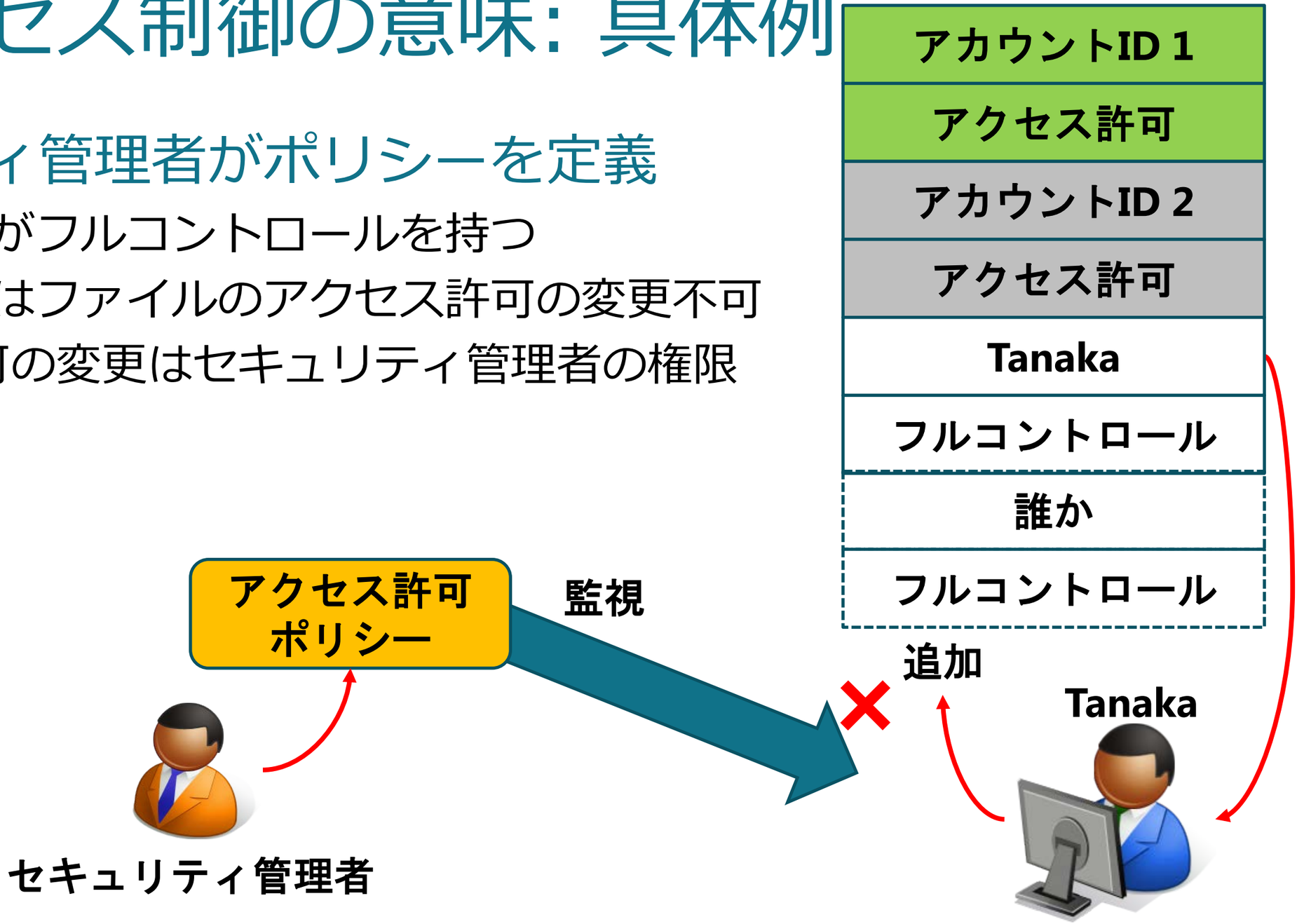
強制アクセス制御の意味

- 強制アクセス制御 = MAC：Mandatory Access Control
- セキュリティ管理者が定義したポリシーに基づいて
  - 自動的にアクセス許可を設定(強制)
  - ファイルの所有者であっても変更ができない

- 例:「個人情報保護規定」というポリシーを顧客に提示
  - 顧客がポリシーに同意した場合に個人情報取得
  - 運用規則は担当者の判断で変更できない

強制アクセス制御の意味: 具体例

- セキュリティ管理者がポリシーを定義
  - Tanakaさんがフルコントロールを持つ
  - Tanakaさんはファイルのアクセス許可の変更不可
  - アクセス許可の変更はセキュリティ管理者の権限



強制アクセス制御の利点と課題

- 利点
  - セキュリティレベルの向上
- 課題
  - ファイル保護ポリシーの定義が恐ろしく面倒
  - 本来、ドキュメントセキュリティは以下の手順で構成

1. 組織のセキュリティポリシーを定義
2. 文書のラベル(機密度)を定義し、文書をラベリング
3. 文書利用者の役割を定義し、利用者(グループ)に枠割を割り当て
4. ラベルと役割に基づいたセキュリティ構成

  - これができている組織は導入しても良い

強制アクセス制御の適用範囲

- 以前の適用範囲
  - 情報漏洩が重大な問題となる軍事用途などに限定
  - 1980年代はクラスBを標準機能としたOSは皆無
- 現在の適用範囲
  - 一般企業でも高いセキュリティが求められる
  - 情報の重要度が増加…特に個人情報の保護機運
  - 情報の公開範囲の拡大…ネットと記憶装置の発達
    - 以前は大量の情報をコピーする方法が少なかった

Linuxの状況

- SELinux…ラベルポリシーによる制御
  - Windows Server 2012に近い
  - シナリオに沿ったポリシーに従って「ラベル」を定義
- TOMOYO Linux…パスポリシーの自動学習による制御
  - SAKURA…「改ざん防止機能付きLinux」として開発
    「カードキャプターさくら」の主人公(木之本桜)
    (http://www3.nhk.or.jp/anime/sakura/)
  - TOMOYO…アクセスを監視、ポリシーを自動生成
    さくらの友人である大道寺知世が、
    さくらを常に見守りビデオに記録することに由来
    (http://i-love.sakura.ne.jp/tomoyo/)

Windows Server 2012の状況

- Linuxの実態
  - 現在のLinuxではSELinuxが標準でインストール
  - (多くの企業では運用ポリシーがないため)
    SELinuxを無効にするのがLinux管理者の最初の仕事(という冗談)
- Windows Server 2012
  - 「集約型アクセスポリシー」⇒「ダイナミックアクセス制御」の一部
  - 強制アクセス制御機能は標準では無効
  - 管理者が明示的に構成

現状: シナリオを描くのが面倒
結論: 状況によっては極めて有益だが、不用意に有効にすべきでは無い

Windows Server 2012の新機能:
ダイナミックアクセス制御

ダイナミックアクセス制御とは

集約型アクセスポリシー(強制アクセス制御)

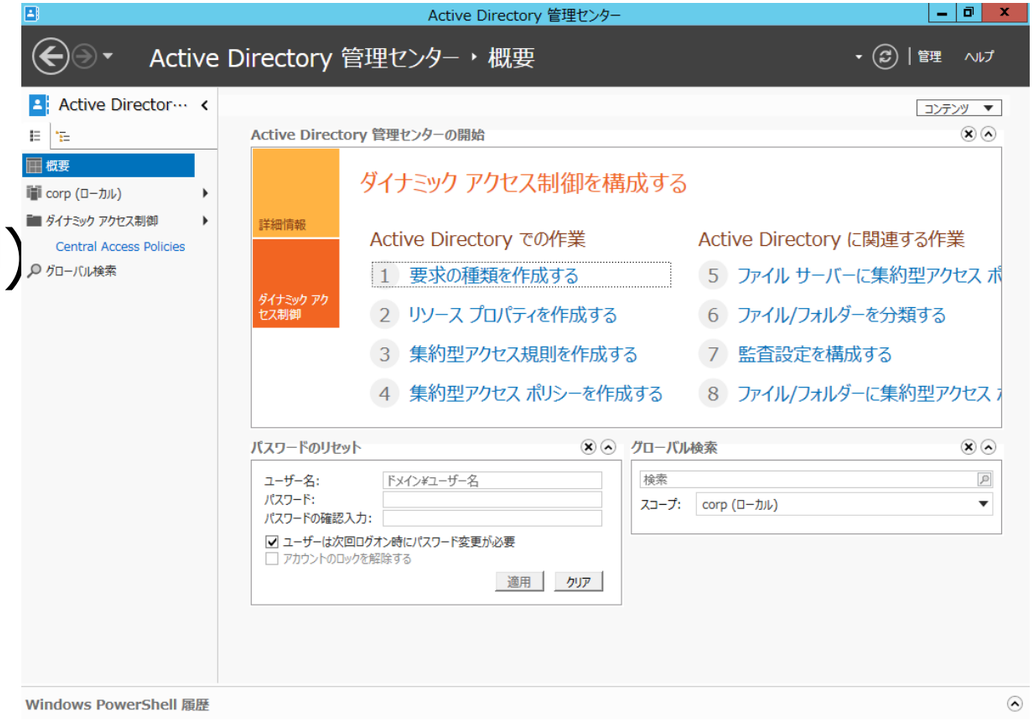
機密情報の保護機能の強化

機密情報の監査機能の強化

アクセス拒否の修復

ダイナミックアクセス制御とは

- 以下の4つの機能の総称
  - データの識別…ファイルの自動分類および手動分類(FCIの応用)
  - ファイル アクセスの制御…集約型アクセス ポリシー
  - ファイル アクセスの監査… 集約型監査ポリシーの応用
  - RMS保護の適用…RMS暗号化を自動適用
- 以下の4つのシナリオを実現
  - 集約型アクセスポリシー(強制アクセス制御)
  - 機密情報の保護機能の強化
  - 機密情報の監査機能の強化
  - アクセス拒否の修復
- Active Directory管理センター



集約型アクセスポリシー

- 強制アクセス制御のWindowsでの実装
- マイクロソフトは「強制アクセス制御」とは主張していない

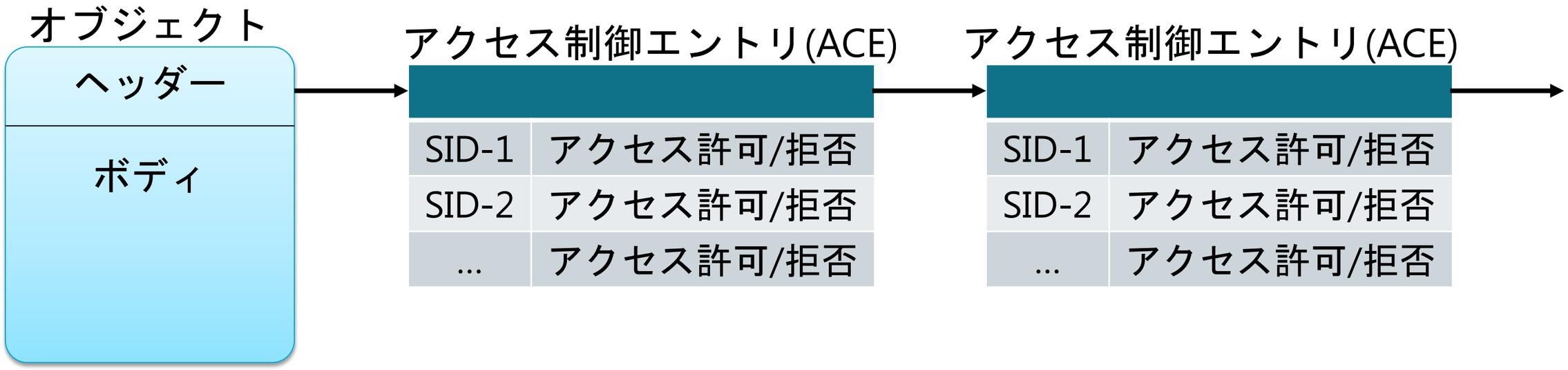
- アクセスには、以下のすべての許可が必要
  - 共有アクセス許可
  - NTFSアクセス許可
  - 集約型アクセス許可

機密情報の保護機能の強化

- 条件付きアクセス制御リスト(ACL)
  - 例1: SalesおよびDevに所属していれば…
  - 例2: HRまたはManagerに所属していれば…
    - 複数ACLと違って、アクセス許可を1箇所にまとめられる
- FCI…ルールに従ってファイルを自動分類
- RMS…ルールに従ってファイルを自動的に暗号化

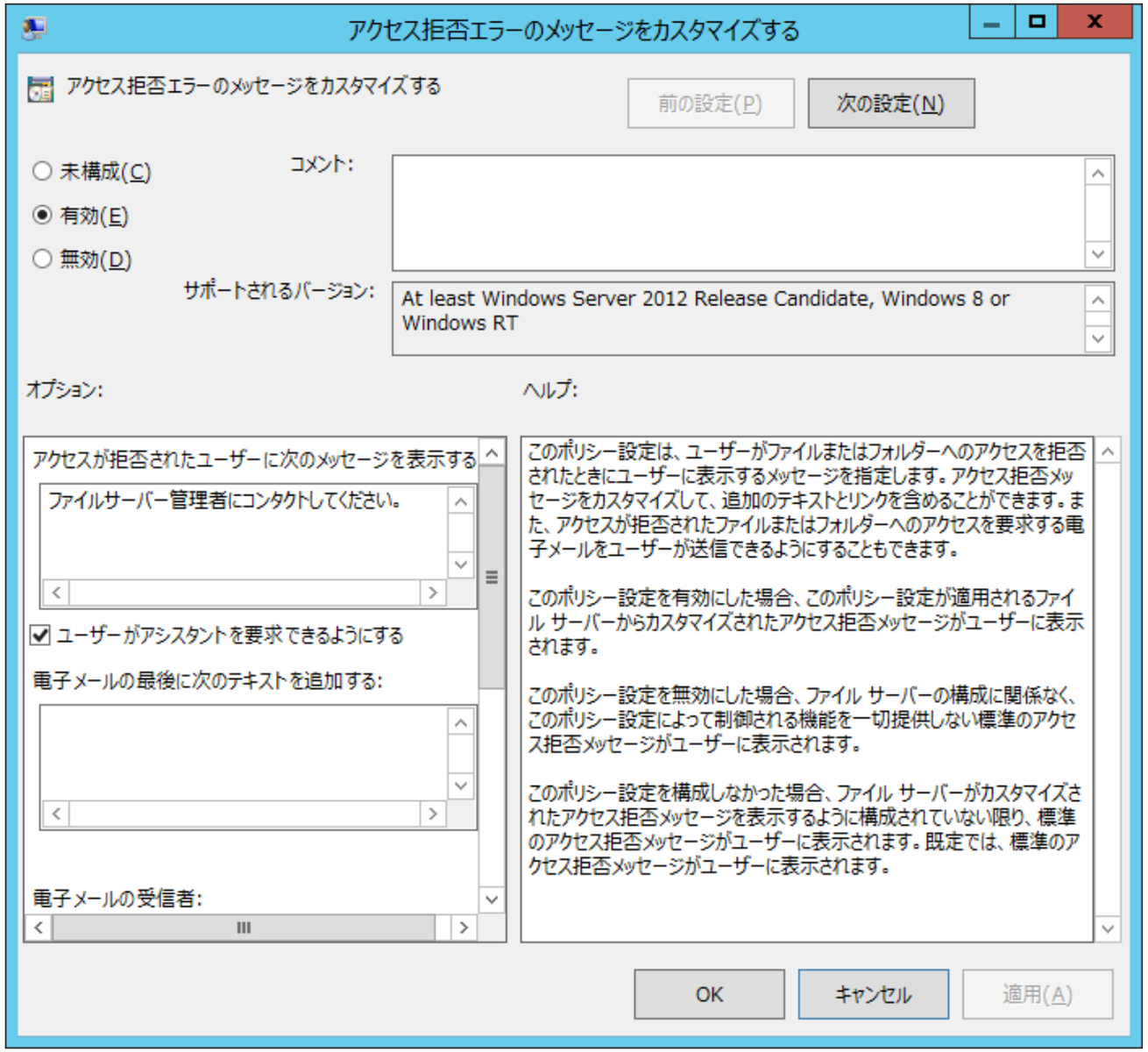
機密情報の監査機能の強化

- 条件付きアクセス制御リスト
  - ACL自体の拡張
- そもそもACLとは



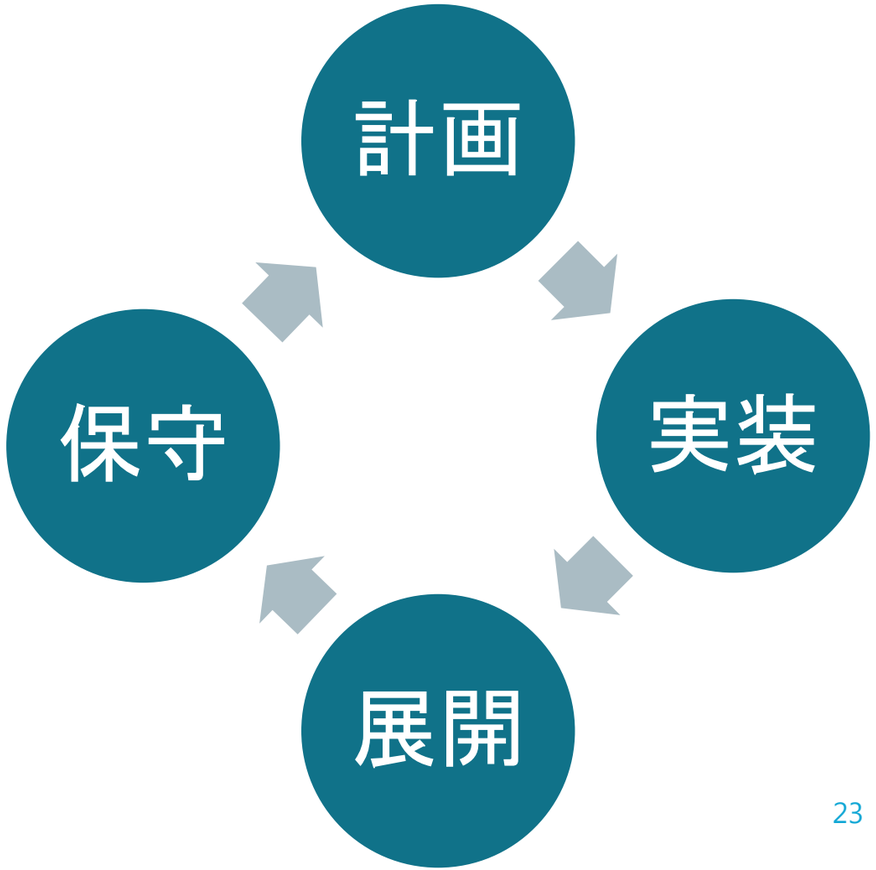
アクセス拒否の修復

- アクセスが拒否されたときにダイアログボックスを表示
  - アクセス拒否の理由
  - コンタクト先の提示
- SharePointやRMSのアクセス拒否と同様
- ディレクトリクォータ等は拒否メッセージをわざわざメールで送信



強制アクセス制御(集約型アクセスポリシー)の利用

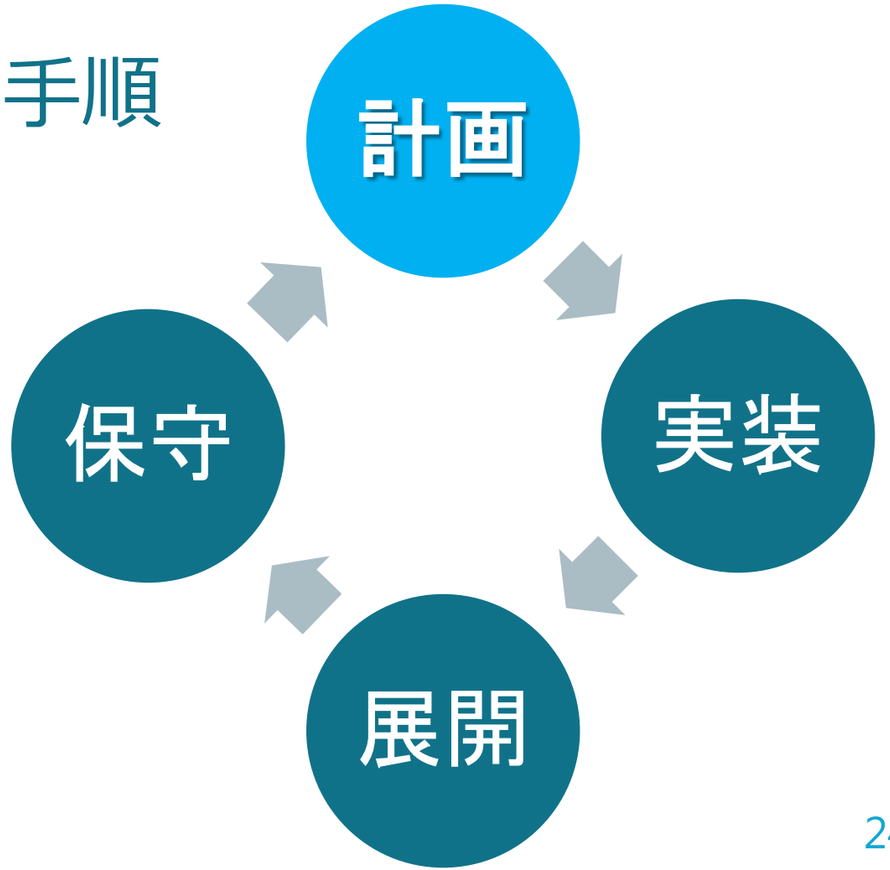
計画…必要なセキュリティポリシーを計画
実装…セキュリティポリシーを定義
展開…セキュリティポリシーをサーバーに適用
保守…セキュリティポリシーの監視や変更



セキュリティポリシーの計画

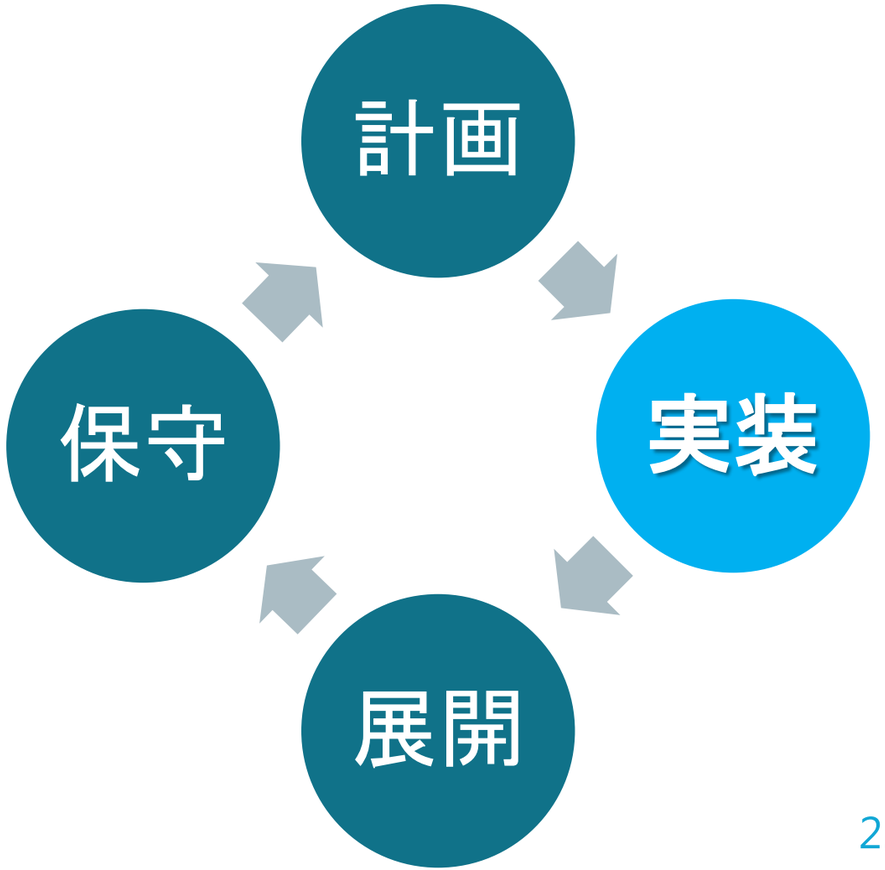
- 計画…どのようなセキュリティポリシーが必要かを計画

- 集約型アクセスポリシー最大の課題
- 復習: ドキュメントセキュリティの構成手順
  1. 組織のセキュリティポリシーを定義
  2. 文書のラベル(機密度)を定義し、
     文書をラベリング
  3. 文書利用者の役割を定義し、
     利用者(グループ)に枠割を割り当て
  4. ラベルと役割に基づいたセキュリティ構成



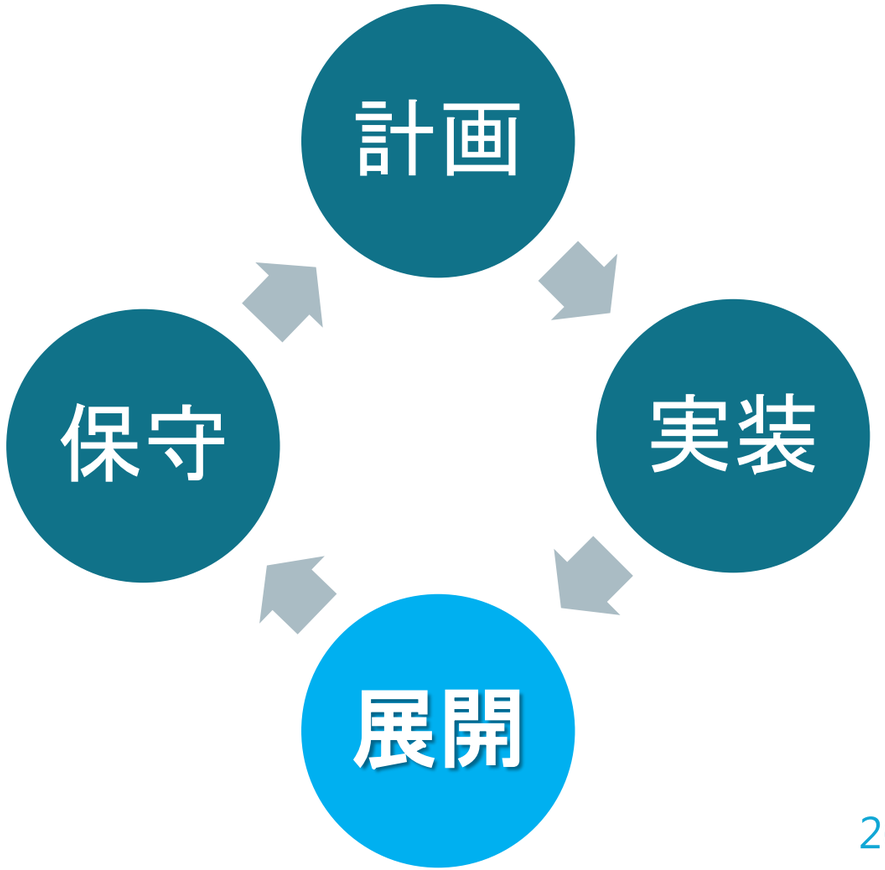
セキュリティポリシーの実装

- 実装…セキュリティポリシーを定義
- ツール
  - Active Directory管理センター
  - グループポリシー
  - PowerShell



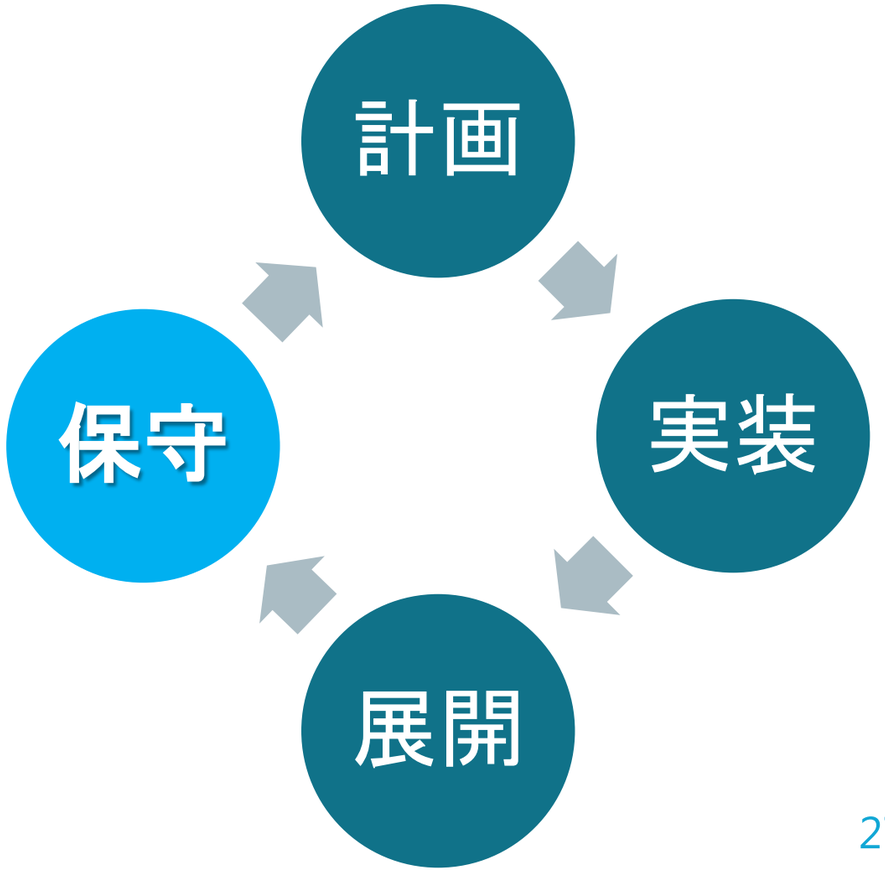
セキュリティポリシーの展開

- 展開…セキュリティポリシーをサーバーに適用
- ツール
  - グループポリシー
  - ファイルサーバーリソースマネージャ(FSRM)
    - FCI



セキュリティポリシーの保守

- 保守…セキュリティポリシーの変更などの保守作業
- 計画フェーズと同じ



まとめ

- Windowsのセキュリティモデル: 随意アクセス制御
  - 自分のものは自分で管理
- 随意アクセス制御の課題
  - 無断で持ち出しが可能
- 新しいセキュリティモデル: 強制アクセス制御
  - セキュリティ管理者の許可した範囲でのみ利用可能
- 強制アクセス制御の利用
  - ダイナミックアクセス制御

現状: シナリオを描くのが面倒
結論: 状況によっては極めて有益だが、不用意に有効にすべきでは無い

参考資料

- 【集中連載】速習！ Windows Server 2012 コアテクノロジ［第4回］速習！ ダイナミックアクセス制御 (安納順一)
  - http://www.computerworld.jp/topics/560/Windows%20Server/203131/［第4回］速習！%20ダイナミックアクセス制御
- Microsoft TechNet
  - http://technet.microsoft.com/ja-jp/windowsserver/hh534429

Q & A

Thank You!

ありがとうございました