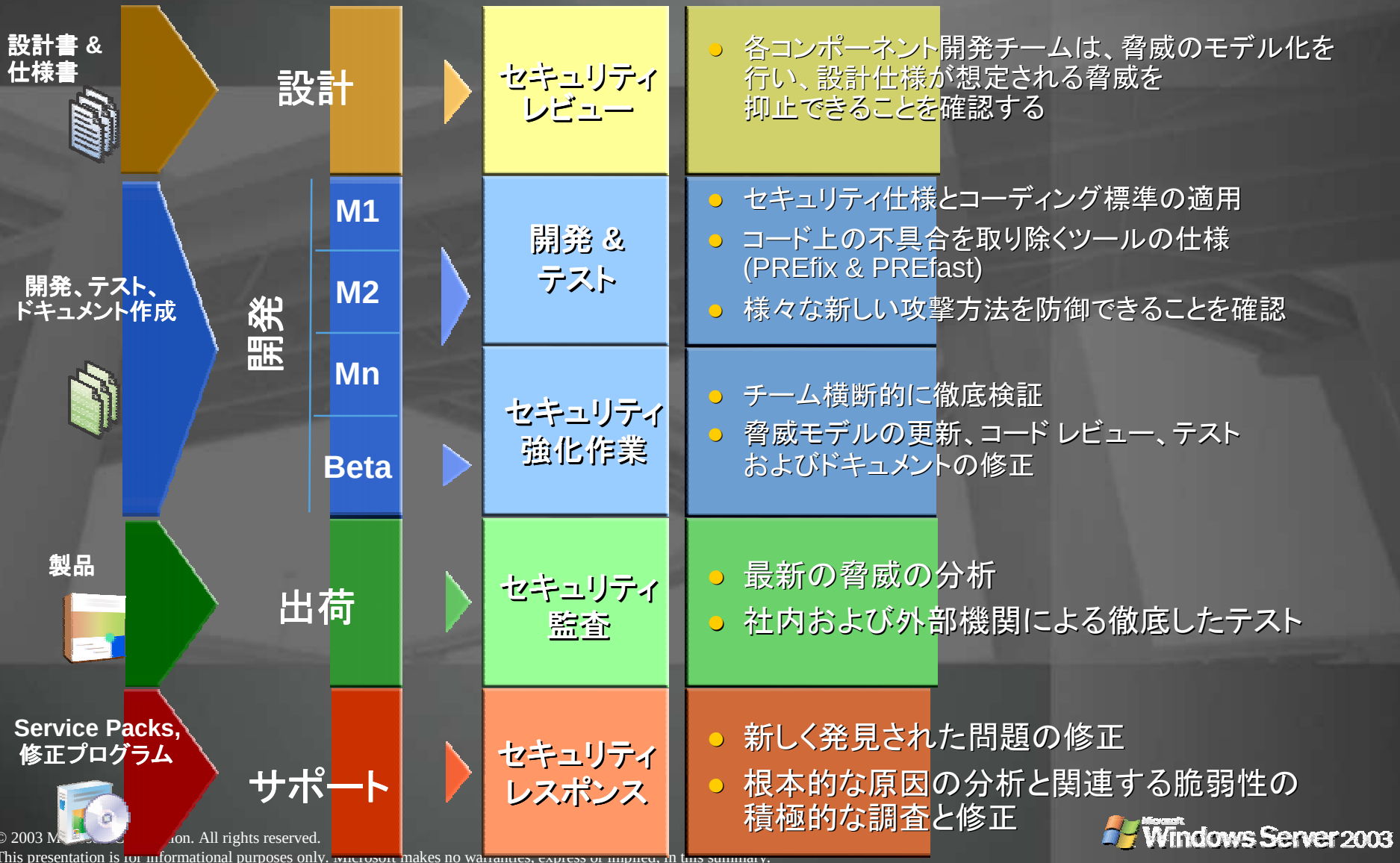
継続的な製品品質の向上
Trustworthy Computingに基づく製品リリース プロセス



Windows Server 2003

継続的な製品品質の向上

既に出荷済で広く利用されている製品での実績:

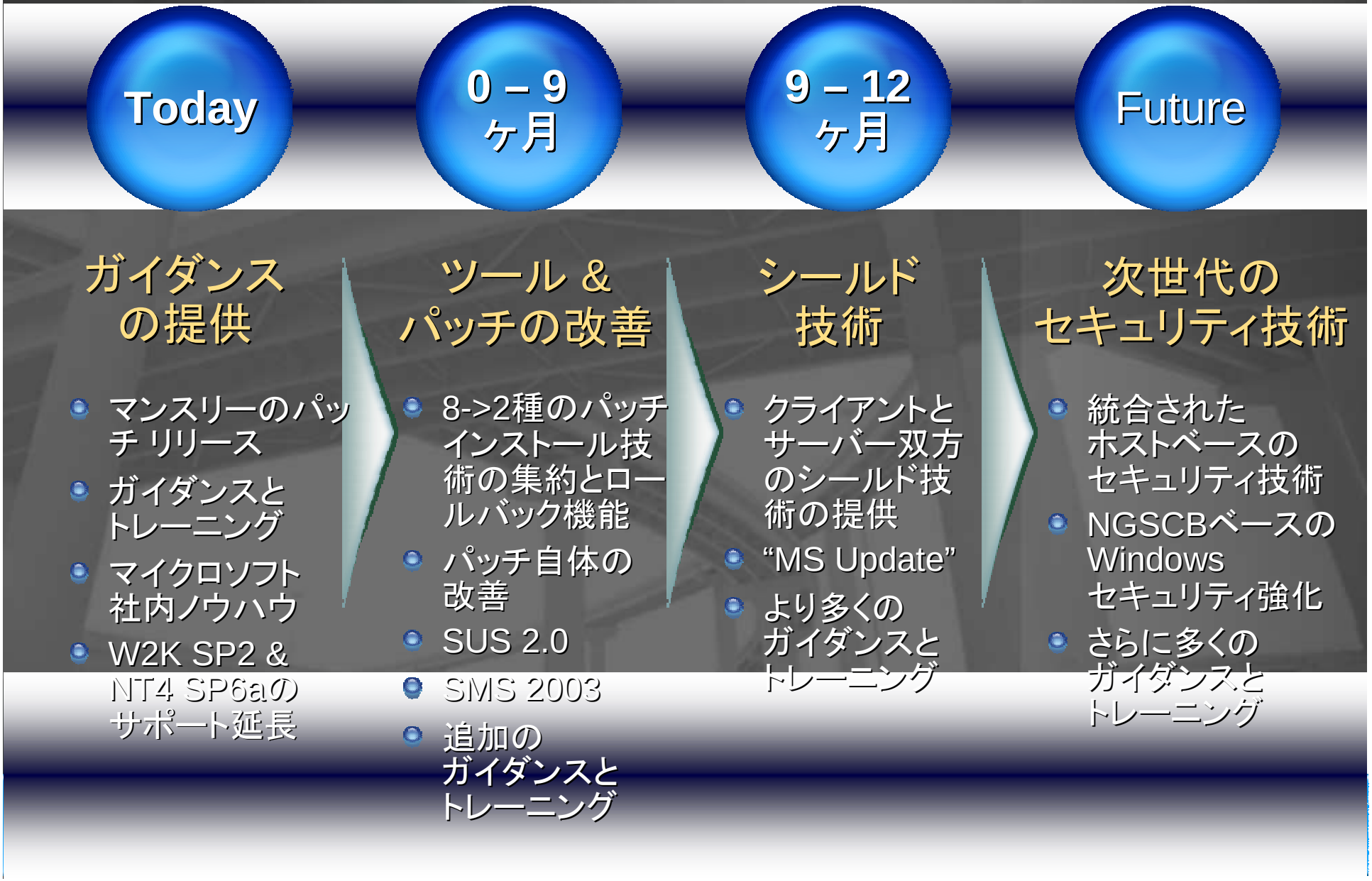
全ての製品に対して例外なくTwCに基づく製品開発を実践:

緊急または重要な脆弱性の数 (出荷開始から特定期間中まで)

	…90日	…150日	TwC に基づく製品開発?
Windows 2000 Servers	13	23	No
Windows Server 2003	6	9	Yes

Windows Server 2003

セキュリティ ロードマップ



Windows Server 2003 のセキュリティ

Windows Server 2003

Active Directory のセキュリティ

- Cross-Forest Trusts
  - 管理者が外部のフォレスト間の信頼を設定することが可能
- Cross-Forest Authentication
  - ユーザー アカウントとコンピュータ アカウントが異なるフォレストにある場合のリソースへのアクセスをセキュリティで保護
- Cross-Forest Authorization
  - 管理者がローカルグループまたは ACL に含むユーザーおよびグループを信頼するフォレストから選択することが可能
- IAS およびCross-Forest Authentication
  - Active Directoryのフォレストが 2way の信頼の cross-forest モードにある場合、IAS/RADIUS は、ほかのフォレストにあるユーザーアカウントを認証することができる

PKI の強化

- Cross–Certification サポート
- 役割の分離
- カスタム認証テンプレート (バージョン 2)
- Delta CRL
- キーアーカイブ/回復
- 自動登録
- 管理者操作の監査

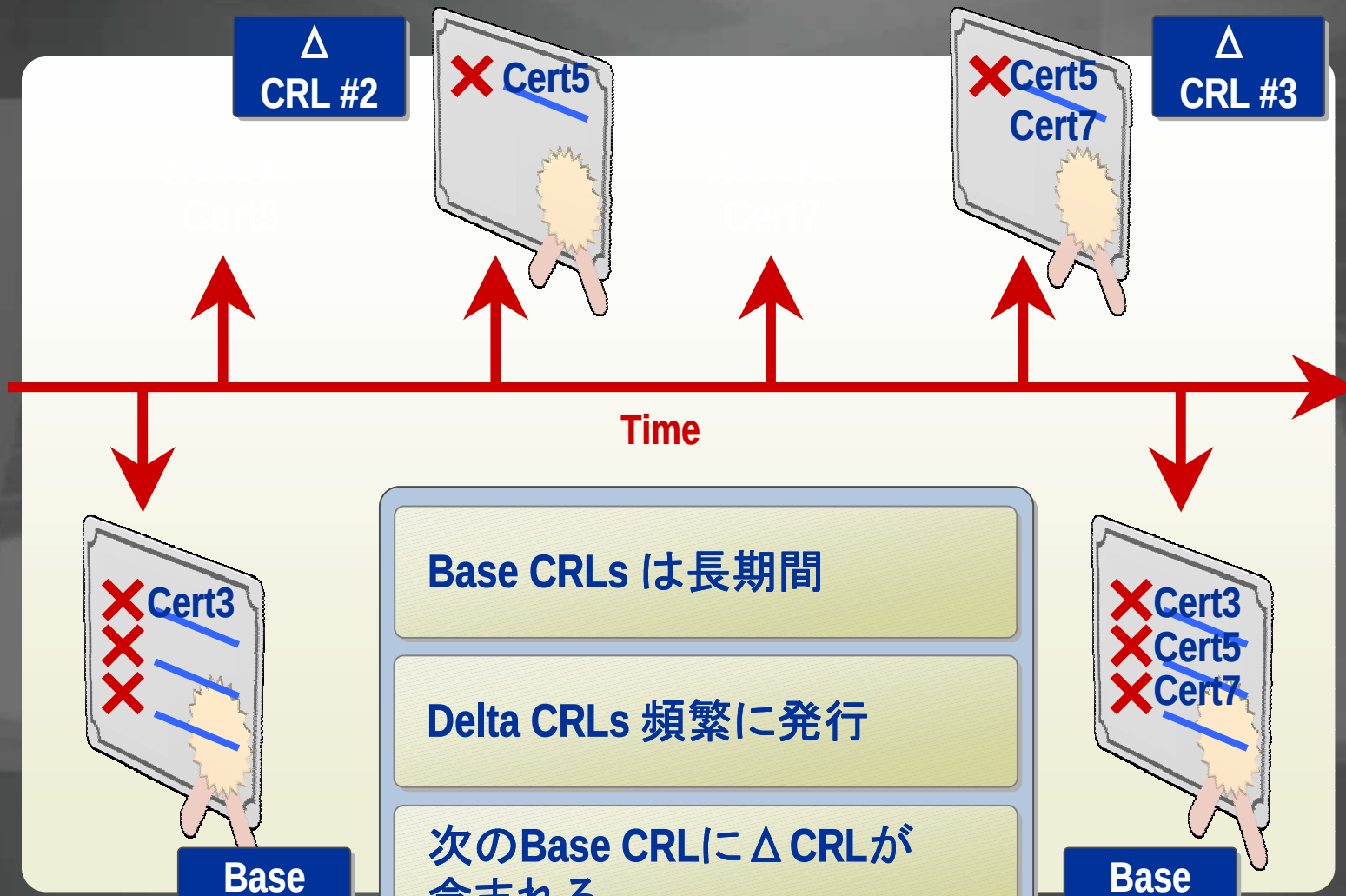
参照:Windows Server 2003 PKI 運用ガイド

http://www.microsoft.com/japan/technet/prodtechnol/windowsserver2003/maintain/operate/ws03pkog.asp

Δ CRL

- 前回の変更からの差分だけを含むCRL
  - 単純な“1:1モデル”を採用
- デルタCRLでの変更は次回の完全なCRLの公開に含まれる
- フルCRLに比べてサイズが小さい
- ネットワークへの影響を最小限に保ちながら、公開の頻度をあげることが可能
- 失効状態の遅延を減少できる

CRL公開スケジュール



- Base CRLs は長期間
- Delta CRLs 頻繁に発行
- 次のBase CRLにΔCRLが含まれる

Windows Server 2003

アクセス権

- 既定のNFTS のアクセス権を強化
  - 変更前: Everyone フル コントロール
  - 変更後:
    - Everyone 読み取りおよび実行(ルートのみ)
    - 読み取り、実行、フォルダの作成、ファイルの作成
    - SYSTEM作成者、管理者フル コントロール
- 既定の共有アクセス権
  - 変更前: Everyone フル コントロール
  - 変更後: Everyone 読み取り
- 新たな機能
  - 有効なアクセス権の確認ツール
  - GUI から所有者を変更

サービスのロックダウン

- Alerter
- Clipbook
- Distributed Link Tracking (Server)
- Imapi CDROM Burning Service
- Human Interface Devices
- ICS/ICF
- Intersite Messaging
- KDC
- License Logging Manager
- Terminal Server Discovery Service
- Windows Image Acquisition
- Messenger
- NetMeeting
- NetDDE
- NetDDE DSDM
- RRAS
- Telnet
- Themes
- WebClient
- Windows Audio

システムサービスアカウント

ローカル システム

- 管理するパスワードがない
- セキュリティ チェックを回避

ユーザー アカウント

- ローカル システムより低い権限で実行
- LSA シークレットとしてパスワードを保存
- 構成が複雑になる可能性がある

ローカル サービスおよびネットワーク サービス

- 管理するパスワードがない
- 認証されたユーザーよりも若干低いアクセス権でのみ実行
- ローカルサービスではネットワークをまたがって認証を行うことができず、ネットワーク サービスはコンピュータ アカウントとして認証を行う