内部セキュリティの最新動向

株式会社アットマーク・アイティ
編集局長　新野淳一

新しい言葉「内部セキュリティ」

- 従来のセキュリティは主に：
  ファイアウォール外側からの脅威対策
  - 脅威：不正侵入、改ざん、盗聴、ウイルス／ワーム
  - 対策：アンチウイルス、ファイアウォール、IDS、VPN／暗号化
- 内部セキュリティ
  - まだ確立された言葉ではなく、ベンダによって多様な使われ方があるが、大枠は、
    「ファイアウォール内側にある脅威への対策」

ファイアウォールの内側にある脅威

- サーバへの不正アクセス
  - サーバ上のファイルやDBへ権限外の不正アクセス
  - ルート権限などの不正利用、私的領域利用
- ネットワークなどの私的使用
  - 仕事に関係ないWebサイトへのアクセス
  - 私用メール、大量データ転送などの不正帯域利用
- 情報流出
  - 見積書、顧客一覧など、社員が持つ社外秘流出
  - 人事情報など、管理されているはずの情報の流出

なぜ内部セキュリティが注目？

- 社内からも守るべきデータが登場
  - 顧客のプライバシー意識の向上
  - 個人情報保護法など
  - 社内の情報に対する保護の重要性が拡大
- 事故による情報流出のリスク
  - 故意でなくとも、事故やウイルスによって情報が流出するリスクが高まっている
- データの遍在性が高まる
  - ノートPC、携帯電話、Webアプリケーション、モバイル環境の普及で、情報が社外に持ち出される

内部にある脅威への対策は？

- サーバ不正アクセスへの対策
  - すべてのサーバ、DBへの統合的なアクセス管理
  - サーバ管理者と、人事・経理など情報責任者の分離
- ネットワークなどの私的使用への対策
  - URLフィルタリング、プロキシ、帯域管理など
  - 単語フィルタリングなど内容へ踏み込む場合も
- 情報流出への対策
  - デジタルライツ・マネジメントで、権限のない者はファイルを受けとっても読めないように

内部セキュリティの特徴

- セキュリティポリシーの設定が重要
  - 情報ごとに、重要度が異なる
  - 情報ごとに、利用者が異なる
- アイデンティティ管理が不可欠
  - 個人ごとに、アクセス権が異なる
  - URLフィルタの内容、帯域などの調整
  - ファイルへの電子署名、暗号化などの鍵管理

内部セキュリティに関係する技術

- つまり内部セキュリティの大枠には、下記の技術などが関係している
  - セキュリティポリシー
  - アイデンティティ管理
  - アクセス管理
  - URLフィルタリング、帯域管理
  - デジタルライツ・マネジメント

セキュリティポリシーの動向（1）

- セキュリティポリシーとは？
  セキュリティ対策と維持のための指針・仕組みを記した文書
  - エグゼクティブ・ポリシー
    トップダウンによる、企業の経営視点から見たセキュリティ方針
  - ポリシー・スタンダード
    実際に守るべき規定を具体的に記述した文書
  - プロシージャ
    ポリシースタンダードを実施するための詳細な手順
- 標準的なセキュリティポリシーのガイドラインや認定取得制度として、「BS7799」「ISMS」などがある
- セキュリティポリシーを整備することで、組織が強化されるという認識が起こりつつある

セキュリティポリシーの動向（2）

- セキュリティポリシーの例（電子メール）
  - ポリシー・スタンダード
    - 不用意に会社のメールアカウントを外部へ公開してはならない
    - 社外のメーリングリストへの投稿は、業務上必要な場合のみに限定し、その内容に十分注意すること
  - プロシージャ
    - 当社の標準電子メールソフトウェアは○○○○である
    - 電子メールソフトウェア△△△△は使用禁止とする
    - 受信メールの添付ファイルを開く前には必ずウイルススキャンを行わなければならない
    - 添付ファイル付きのメールを送信する場合には、送信前に必ず添付ファイルの内容を再確認しなければならない

セキュリティポリシーの動向（3）

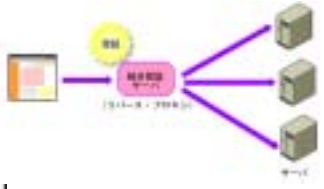
- 内部セキュリティ対策は、おおまかなポリシーでもできる
  - 社内情報資源の精査と分類と重要度設定など
  - アクセス権限と会社の役職・肩書きなどとのすり合わせなど
- ポリシー管理策定・運用支援ソフトウェアが登場
  - eTrust Policy Compliance（CA）
  - MagicPolicy（アズジェント）
  - LivingPolicy（ラック）
  - etc....

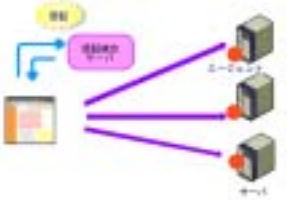
アイデンティティ管理の動向（1）

- アイデンティティ管理とは
  - システム全体に渡って統合的に利用者の情報（ID、パスワード、権限ほか）を管理し、利用者を特定する
  - Windows、LinuxなどOSのほか、Oracle、Notes/Dominoのようなアプリケーションもアイデンティティ管理の対象となる
- アイデンティティ管理で実現されること
  - シングルサインオン
  - パーソナライズ
  - アクセス管理など

アイデンティティ管理の動向（2）

- アイデンティティ管理の仕組みの例
  - リバースプロキシ方式：
    認証サーバが、ユーザーの代わりに各サーバへログオンする（左）
  - エージェント方式：
    認証サーバに認証済みチケットをもらい、それを各サーバのエージェントに見せる（右）





アイデンティティ管理の動向（3）

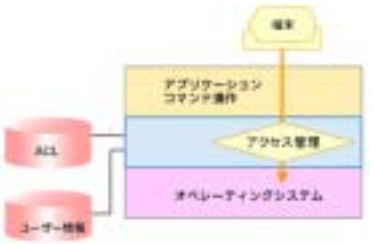
- 相互運用性が大事
  - 複数のOS、プラットフォームのアイデンティティを統合管理するために、相互運用性が大事
  - アイデンティティ情報のやり取りとしてLDAP（Light-weight Access Protocol）が多く使われている
- アイデンティティ管理製品
  - eTrustAdmin（CA）
  - Novell eDirectory（ノベル）
  - Active Directory、MIIS（マイクロソフト）
  - iPlanet Directory Server（サン・マイクロシステムズ）
  - Tivoli Identity Manager（IBM）、etc...

アクセス管理の動向（1）

- アクセス管理が、内部セキュリティ対策の柱
  - ポリシーに基づくアクセス権限の管理
  - 複数のOS、アプリケーションのセキュリティを統合
  - OS以上にきめこまかいアクセス管理を実現
    - 例：UNIXでも細かいACLを実現
    - 例：サーバ間の権限も管理
    - 例：rootなど管理者権限に対しても制御が行える
    - 例：アクセス履歴を残す
    - 例：プロセスに対する権限管理
    - 例：改ざん通知

アクセス管理の動向（2）

- アクセス管理の実現の例
  - OSのレイヤーの上に、アクセス管理レイヤーを入れて、コマンドやアプリケーションなどからのアクセスを管理する



アクセス管理の動向（3）

- 製品選択が重要
  - アクセス管理には、アイデンティティ管理におけるLDAPほど相互運用性はなく、製品選択が重要となっている
  - ポリシー、アイデンティティ管理、アクセス管理は連携することに注意
- アクセス管理製品
  - eTrust Access Control（CA）
  - Tivoli Access Manager for OSs（IBM）
  - SystemWalker（富士通）
  - Trusted Solaris（サン・マイクロシステムズ）、etc...

私的利用などの対策動向（1）

- URLフィルタリング
  - アダルトサイトや通販サイト、掲示板など、業務に関係ないWebサイトへのアクセスを遮断
- 帯域管理
  - 社内外へのトラフィック、帯域幅をコントロール
  - 特定のユーザーによる帯域の消費を防ぐ
- 対応製品
  - Security Gateway（シマンテック）
  - BorderManager（ノベル）
  - PacketShaper（パケッティア）
  - etc...

私的利用などの対策動向（2）

- 単語フィルタリング、情報フィルタリング
  - 「飲み会」のような私的メールをリストアップ
  - 「顧客名簿」のような重要な内容の流出をストップ
  - ウイルスや宛先間違いなどの事故によって、重要なメールが流出することもブロック
- メールフィルタリング製品
  - SEQRIA Mail（ジャストシステム）
  - CS MAILsweeper（丸紅ソリューション）
  - etc...

情報流出対策の動向（1）

- ファイルの暗号化
  - 文書などのファイルに署名・暗号化し、権限のある者しかファイルを参照できなくする
  - 社外などに重要情報が流出しても、暗号化されているためある程度安全
  - デジタルライツ・マネジメントで、コピー禁止などきめ細かい操作に対応したMS Office Systemの登場で、今後注目が高まる可能性がある
- 現状はまだ技術の普及を待っている状態

情報流出対策の動向（2）

- PKIの技術が現在の主流
  - 現在は、S/MIME、PGPのようなメールの署名・暗号化が中心
  - 暗号化のための鍵管理、証明書管理などは、PKIが主流であり続けるだろう
- 対応製品
  - S/MIME、PGP対応メーラ
  - MS Office System（マイクロソフト）
  - etc...

ポイント

- 内部セキュリティの脅威はさまざまある
- しかし、サーバのアクセス管理を固めることが、まず基本
- アクセス管理には、ポリシー策定、アイデンティティ管理との連携が伴う
- ネットワークの私的利用対策は、企業の事情に応じて採用
- 情報流出への対策は、今後の課題

自分戦略をつかめ

@IT atmarkIT
http://www.atmarkit.co.jp/

株式会社 アットマーク・アイティ
〒100-0005 東京都千代田区丸の内3-3-1新東京ビル8F