国内外の事例から見る
最適な内部セキュリティ対策

2003年8月1日

コンピュータ・アソシエイツ株式会社
eTrustブランドユニット
宮下　毅

今日のテーマ

- なぜ情報漏洩は起きるのか
  - 最近の内部情報漏洩に関するニュース
  - 漏洩された情報は、どこへ？
  - 内部情報漏洩による損害と企業の責任
- どうすれば内部情報漏洩を防げるのか
  - 外部セキュリティと内部セキュリティ
  - 内部情報漏洩はどのようにしておきるのか
  - 内部セキュリティ対策が進まなかった理由
  - どのようにして対策が進められるか？
- eTrust の紹介
- eTrust Access Controlの紹介
- 海外の事例
- 国内の事例

最近の内部情報漏洩事件に関するニュース

りそな銀行の久米田支店から375人分の顧客データが流出

- 7月4日（共同通信）
- 「りそな銀行」の久米田支店（大阪府岸和田市）から375人分の顧客データが流出していたことがわかり、大阪府警東署は4日までに窃盗容疑で捜査を始めた。同行を傘下に持つ「りそなホールディングス」（大阪市中央区）によると、流出したのは同支店と取引がある375人の氏名や住所、生年月日、取引内容などのデータ。6月下旬に外部流出が判明し、同行は今月2日、同署に窃盗容疑で被害届を出した。顧客データはコンピューター管理されており、行員がそれぞれのパスワードを入力しなければ引き出すことはできないという。同署は内部犯行の可能性があるとみて、データの管理システムなどを調べている。調べでは、流出したのは大阪府岸和田市にある久米田支店の顧客の氏名、住所、生年月日や取引内容など。同行は6月下旬に流出を把握、2日に東署に被害届を出した。広報部は「流出発覚の経緯については捜査に差し障るため、明らかにできない」と話している。

- 7月9日
- 元りそな銀行員を詐欺容疑で逮捕、顧客情報流出にも関与か
  - 大阪府警捜査二課などは9日、顧客の預金通帳などを使って現金を勝手に引き出したとして、りそな銀行久米田支店（大阪府岸和田市）の元主任、田之上康司容疑者（40）＝同府松原市高見の里1＝を詐欺などの疑いで逮捕した。久米田支店では今月、375人分の顧客情報が外部に流出していたことが判明。田之上容疑者は流出についても関与をほのめかす供述をしているという。調べによると、同容疑者は同支店の渉外課員だった6月中旬から下旬の間、顧客から預かった預金通帳と印鑑の押された払戻請求書を使って数回にわたり、預金約200万円を引き出し詐取した疑い。同容疑者は消費者金融などに約1000万円の借金があったといい、「返済に充てた」と容疑を認めているという。銀行の内部調査で不正が発覚、同容疑者は今月4日付で懲戒解雇された。

ローソン、約56万件の会員情報が流出

- 6月27日（毎日新聞）
- 大手コンビニエンスストアのローソンは26日、ポイントカード、ローソンパス会員カードの会員約56万人分の個人情報が社外流出した、と発表した。流出情報は住所、氏名、生年月日、自宅と携帯電話の番号で、口座番号や年収などの信用情報は含まれていない。ローソンは社内調査委員会を設けて流出経路の解明を急いでおり、特定でき次第、警視庁に窃盗か不正アクセス防止法違反容疑で告訴する方針。顧客の個人情報流出はコンビニ業界では初めて。
  流出した個人情報は、02年8月17日時点でカード会員だった顧客に関する情報。今月9日、会員から「変なダイレクトメール（DM）が来ている」と問い合わせがあり、調査した結果、流出が判明した。名簿業者などを通じてDM会社に渡ったとみられるが、外部からの不正なアクセスか内部から持ち出されたかは不明。ローソンによると、個人情報にアクセスできるのは、社内と委託会社に約10台ある特定のコンピュータだけで、パスワードを知っているのは社内と委託会社で計20人という。
  ローソンは、DM会社から情報を回収し使用中止の確約書も取り付けたが、他のDM会社に渡っているかどうか確認できていない。カード会員は02年6月から募集しており、情報流出の確認後も募集を継続している。
  ローソンパス会員カードは会費無料で、現在の会員数は約115万人。うち80万人分にはクレジットカード機能もついている。ローソンで買い物をするたびにポイントが加算され、一定のポイントがたまると商品と交換できる仕組みだ。
  ローソンは、カード会員115万人全員に謝罪のため、社長名の手紙と500円分の商品券を送る。
- ＜個人情報流出＞ローソンを調査へ　細田担当相（毎日新聞）
  - 細田博之・個人情報保護担当相は27日午前の記者会見で、大手コンビニエンスストアのローソンで、約56万人分の個人情報が流出した問題で「どのようにして起きたのか、故意がなかったかどうかなどを、関係省庁と連携して調べていきたい」と述べ、原因調査を実施する考えを示した。

漏洩された情報は、どこへ？

ＫＤＤＩの「ａｕ」の携帯電話からＮＴＴドコモの電話に対し、「出会い系サイト」をＰＲする迷惑メールが送りつけられる被害が急増

- ＫＤＤＩの「ａｕ」の携帯電話からＮＴＴドコモの電話に対し、「出会い系サイト」をＰＲする迷惑メールが送りつけられる被害が急増し、ＫＤＤＩは2日までに発信元の２００台の通話と通信機能を停止した。さらに別の２００台からも迷惑メールが発信されており、近く同様の措置をとる。発信元の携帯は数十の企業、個人名義で登録されていた。通信記録には相手側に届かなかった「エラーメール」がほとんどなく、アドレス名簿が業者側に流出していた可能性もあるという。（読売新聞）

不渡り情報3500件流出信組職員、金融業者に渡す

- 6月9日（共同通信）
- 富士信用組合（神戸市中央区、奥畑文雄理事長）の職員（43）が、管理していた約3500件の不渡り情報が入ったフロッピーディスクを、大阪市内の金融業者に渡していたことが9日、同信組の調査で分かった。職員は「大阪市の金融業者に『情報を買い取る』と言われ渡した」と話したという。同信組は職員を6日に懲戒解雇し9日、窃盗容疑で生田署に告訴した。同信組によると、流出したのは、兵庫県内5カ所の手形交換所が1999年4月から2003年5月までの間に作成した県内の企業などに関する不渡り情報。職員は5月10日、金を借りるため大阪市の金融業者を訪ねた際「前払い金」として1万円を渡され、その後、フロッピーを渡したという。

恐喝未遂の元自衛官に実刑

- 4月17日（共同通信）
- 自衛隊の通信システムデータ流出をめぐり、開発元の富士通への恐喝未遂罪などに問われた元陸上自衛官のシステムコンサルタント岸川隆久被告（33）に横浜地裁は17日、懲役2年8月（求刑懲役4年）の判決を言い渡した。共犯とされた会社役員小松正明被告（58）と同道岡苦楽被告（51）はいずれも懲役2年（求刑懲役3年）。小林康男裁判官は「データが国外に流出した場合、日本の安全保障に影響があるなどの弱みに付け込んだ。社会に与えた影響は大きく、刑事責任は重大」と述べた。判決によると、岸川被告は、勤務先の富士通川崎工場で通信システムデータを入手。3人は共謀し昨年6月から7月にかけ、富士通側に「持ち出した富士通社員が北朝鮮に売ろうとしているのを抑えている」と持ち掛け、現金を脅し取ろうとした。

内部情報漏洩による損害と企業の責任

情報漏えい事件と企業責任

- コンピュータ犯罪に関する法規制の特徴
  - 犯罪を犯したものに対する罰則
  - 企業に対する管理対策を義務化

- 情報セキュリティ対策は，企業の自己責任

情報漏えい事件と企業責任

- 宇治市の住民基本台帳データ不正流出事件
  - 宇治市の住民基本台帳データ流出
  - 外部委託業者のアルバイトがMOに入れて持ち出し
  - 慰謝料として原告1人あたり1万5000円の請求が認められる
  - （仮に宇治市全市民が訴えたとすると、×約20万人＝30億円）
- 某エステ会社　個人データ流出事件
  - Webで収集した顧客データをアクセス制限なしに公開サーバ上に保存。
  - ブラウザからだれでも閲覧が可能な状態になっていた。
  - 流出した携帯電話番号を変更するための費用や一部の賠償に応じている。

カリフォルニア州、企業への機密漏洩報告義務法案を執行

- 7月1日
- 企業がネットワークシステムに蓄積する顧客の機密情報が、暗号化されずに外部に漏洩した場合、その企業が当事者に対して漏洩の事実を電子メールなどで報告する義務を課する法案が、7月からカリフォルニア州で執行される。米国初の試みとなるこの法案は、個人名とそれにともなうソシアルセキュリティ番号、運転免許証番号、州登録番号、クレジットカード番号、およびデビットカード番号などのどれか一つでも漏洩した場合に執行対象となるもので、個人情報保護政策として今後全米へ展開される気運が高まっている。「自動車部品に欠陥が発覚した場合にその車種を保有するすべてのユーザーに対してリコールが発生する自動車業界の仕組みを、顧客の守秘情報に対して適用した」と語る政府関係者は、この法案の制定に当たって市場調査した結果、調査対象企業の半数近くが過去1年の間に顧客の機密情報漏洩を経験していた事実も明らかにしている。

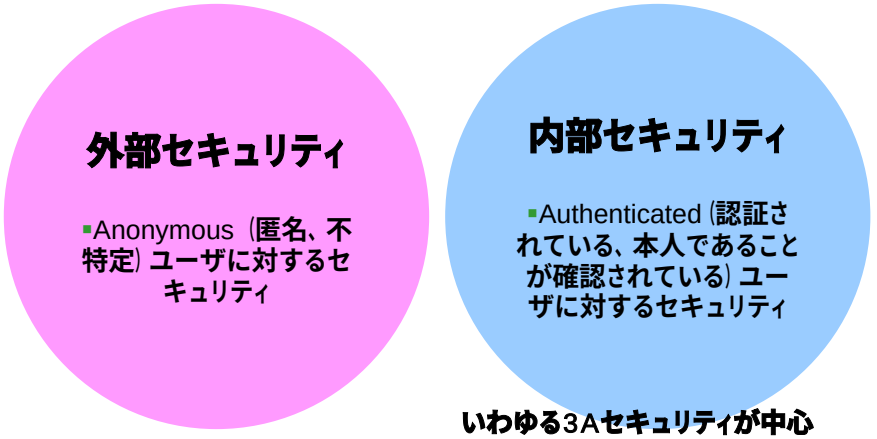
内部情報漏えいによる自社への影響

- 集団訴訟による経営への影響
  - 賠償金
  - 業務への影響
- 社会的信用の失墜
  - 企業イメージの低下
  - 株価への影響
- 恐喝
  - 情報の買取要求

■NPO日本ネットワークセキュリティ協会（http://www.jnsa.org）の「2002年度情報セキュリティインシデントに関する調査報告書」に詳細な調査資料があります。
- ◆<第1部> 情報セキュリティのインシデントに関する調査および被害算出モデル
- ◆<第2部> 情報漏洩による被害想定と考察(賠償額および株価影響額)

どうすれば内部情報漏洩を防げるのか

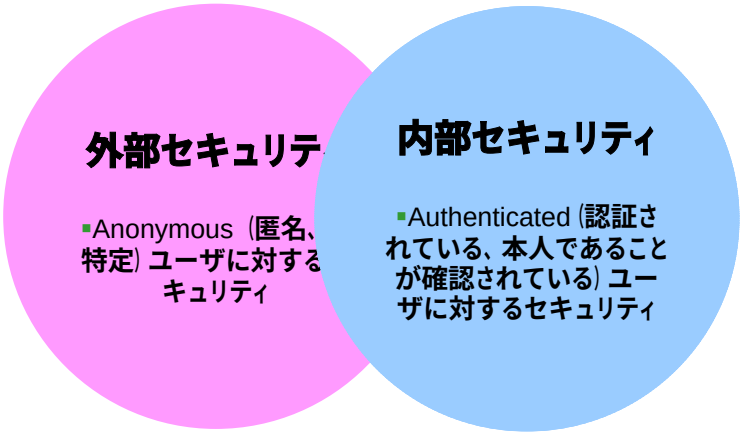
外部セキュリティと内部セキュリティ



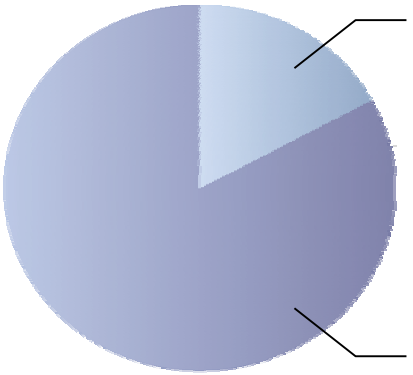
いわゆる3Aセキュリティが中心

- ユーザは誰なのかを特定（Authentication）
- ユーザへ適切なアクセス権を設定（Authorization）
- ルール設定の管理や運用（Administration）

外部セキュリティと内部セキュリティ



情報漏洩は内部から



17% **外部からの侵入**

83% **内部からの流出**

出典：CSI/FBI 2002**年コンピュータ犯罪およびセキュリティ調査**

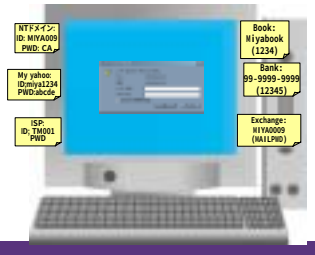
内部情報漏洩はどのようにしておきるのか

代表的な内部セキュリティの問題

- 特権ユーザ（スーパーユーザ）の存在
  - 特権ユーザ：UNIXではroot、Windowsでは Administrator。
  - 特権ユーザはシステムのなかでは万能の神
    - どんなファイルでも読みとり、変更、削除が可能
    - どんなプロセスでもストップ可能
    - 自分のログファイルも変更削除可能
  - 複数の特権ユーザの存在
    - サーバの運用担当者、バックアップ・オペレータ、パスワード管理担当者・・・。
    - 経営者も情報システム部長も、この事実を知らない
    - 自分のメールが盗み見られているかもしれない
  - 特権ユーザ自身の意識の問題
    - 一般的に、特権ユーザ（システム管理者）は、自分が特権ユーザ権限を日常的に使っていることのリスクを理解していない。また、アクセス権限を小さくしたいなどとは思わない。

代表的な内部セキュリティの問題

- パスワードの設定のジレンマ
  - 一人のユーザは平均5つのシステム（各業務アプリ、Windowsドメイン、メインフレーム、Eメール、イントラネットなど）のIDとパスワードを持っている。
  - ユーザの70%以上が容易に推測できるパスワードを使っている。

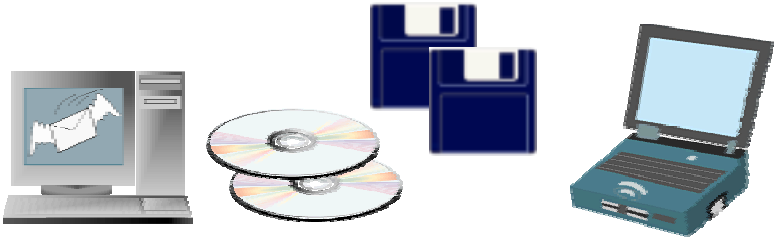


代表的な内部セキュリティの問題

- セキュリティ・ポリシーの実効性の問題
  - セキュリティポリシーを作っても、全てのサーバのセキュリティ設定を監視、メンテナンスすることができない。
  - 複数のサーバがネットワーク化されている環境では、1台のサーバ、1つのアプリケーションのセキュリティが甘いと、すべてのサーバ、すべての情報資産を危険にさらしてしまう可能性がある。

代表的な内部セキュリティの問題

- ノートPC、Eメール、FD、CD-R、USBメモリなどを通じた情報の持ち出し
  - 全てのユーザにとって目に見える、身近な問題。
  - ユーザがアクセスすることができる情報は、それが持ち出されるリスクを管理することは困難。

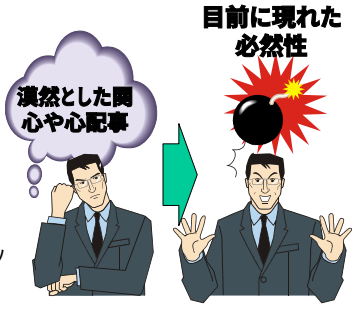


内部セキュリティ対策が進まなかった理由

- セキュリティ対策への経営的観点の欠如
  - 経営者の理解不足
  - 対策の全体像が見えないので、どこから手をつけるべきなのかがわからない。
  - 全社的視野での優先順位がつけられない（ビジネスゴール、資産、脅威、リスク、戦略）
  - 投資に対してどのような見返りがあるのかが具体化できないので、判断できない。
  - 自社で情報漏洩などの事件が起きるまでは、自社の問題として認知がされない。
- 情報システム部の問題
  - 内部セキュリティの強化は、管理業務の負荷が増えるというイメージがあり、情報システム部が、導入に対して消極的なことが多い。
  - 社内のリソース不足（時間、人材、費用）
  - システム運用部門は、厳しいコスト削減のプレッシャーがあり、今稼働しているシステムへの追加の投資を起案しにくい状況が続いている。

どのようにして対策が進められるか？

- 受動的な対策
  - 法制度への準拠のように、払わなければいけないコスト（必要コスト）としての納得
  - 個人情報保護法の施行、不当競争防止法の改正
  - 自社で問題が発生し、すぐに対策をとらなければいけない緊急対応（多くの場合、パッチワーク的になってしまう）
- 能動的な対策
  - IT投資としてメリットを具体化
  - セキュリティ監査（ISMS、BS7799など）による企業としての信頼性の確保



内部情報漏洩対策のキー

- 情報アクセスの4W1Hを適切にコントロールする
  - What　システムリソースに対して
  - Who　誰が
  - When　いつ
  - Where　どのマシンから
  - How　どのプログラムによって
- 機能として考えると
  - ログイン制御
  - パスワード制御
  - ネットワーク制御
  - ファイルアクセス制御
  - プロセス制御
  - 管理権限の分割
  - 集中管理

内部情報漏洩対策のキー

- 導入を成功させるための製品選びの条件
  - 将来も使い続けることができること
    - 幅広いプラットフォームサポート
    - 段階的な構築・導入ができること
    - 将来のセキュリティポリシーの変更にも迅速かつ柔軟に対応できること
  - システム運用の現場にも支持されること
    - 最小の運用負荷
    - 安定稼動すること
    - 現在稼働しているアプリケーションに変更せずに導入できること
  - 経営層からの支持されること
    - 監査レポートが出力できること
    - 必要に応じてアクセスのトレースができること

eTrustのご紹介

eTrust ブランド・ユニット

http://www.caj.co.jp/etrust/

CAのセキュリティプロダクトカテゴリ

Security Command Center

一元的な集中管理

Portal による
パーソナライゼーション

容易な配置

Access Management: アクセス管理

ダイナミックなセキュリティ

エンドtoエンドなアクセス制御

クロスプラットフォーム
セキュリティ

強力な認証

ユーザプロビジョニング

シングル・サイン・オン

Identity Management: アイデンティティ管理

ウィルスのブロッキング

プロアクティブな脅威管理

ICE – 隔離, 封じ込め, 消滅

Threat Management:
スレット(外的脅威) 管理

スレット(外的脅威)管理製品

アイデンティティ管理とアクセス管理製品

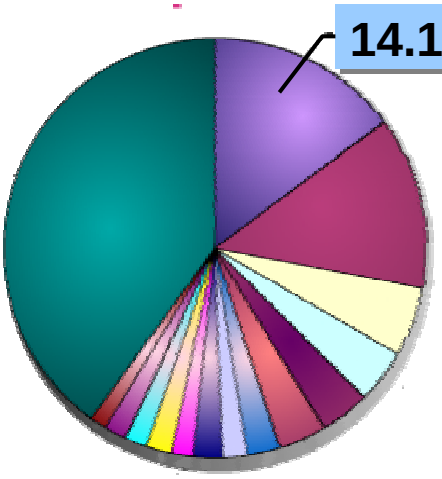
IAM : Identity and **A**ccess **M**anagement

3Aセキュリティ
Authentication(**ユーザ認証**)
Authorization(**権限付与**)
Audit (**監査**)

eTrust Access Controlでなにができる

- これらの内部情報セキュリティ問題を解決できます。
  - 特権ユーザーの権限を分割することができます。
  - パスワードのルールを設定することができます。
  - セキュリティポリシーを統合管理することができます。
  - 全てのデータへのアクセスログを残し、それを安全に保管することができます。

CAは3Aセキュリティソフトの No.1



IDC Worldwide 3A Security Software Revenue by Vendor 2001

コンピュータアソシエイツは
3Aセキュリティソフトの
No.1ベンダー

eTrust Access Control

eTrust Access Controlとは？

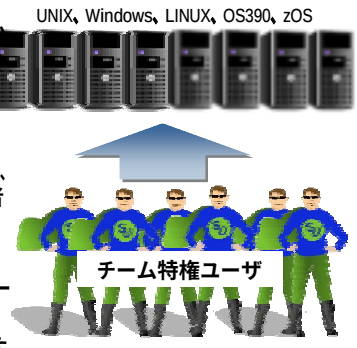
- UNIX(NT)のシステムとデータを保護するためのセキュリティ管理インフラ
  - カーネルに変更を加えないので、現在稼働しているシステム環境にそのまま適用可能。
  - セキュリティポリシーの統合管理を実現
- 主要機能
  - ログイン制御
  - パスワードポリシー設定
  - ネットワーク制御
  - システムリソースの保護
  - ファイル／プロセスの保護
  - 管理権限の分割
  - システム監査
  - 集中管理

eTrust Access Controlの優位性

- トラステッドOSや他のセキュアOSに対してに対して
  - OSを一切改造しないため、OSのパッチレベルに左右されないセキュリティレベルを実現、既存のOS環境にインストールするだけで、強固なセキュリティ環境を実現
  - アプリケーションへの影響もなし（Sun Microsystem社、Oracle社、SAP社、PeopleSoft社の認定取得）
  - サポートするOS（UNIX, Windows,LINUX）
  - 導入実績（国内、国外とも）
  - 異種OS、複数プラットフォーム間におけるセキュリティ・ポリシーを一元管理が可能

eTrust Access Controlを導入しないとどうなるか？

- **サーバの数が多い場合**
  - **多数のサーバに対して、セキュリティ・ポリシーを設定すること、継続的にメンテナンスすることができない。**
  - **どのように設定されているかを一覧することができない。**
  - **一人のサーバセキュリティ管理者が管理できるサーバの台数には限界があるので、複数のサーバ管理者が存在し、多くのユーザに対して特権ユーザの権限をあたえることになる。**
  - **結果として複数のサーバ管理者が存在することになり、セキュリティ管理のレベルがそれぞれのサーバ担当者の技術レベルやモラルに依存する。**
- **複数のサーバOSを使っている場合**
  - **UNIX, Windows, LINUXそれぞれの技術エキスパートを社内に持たなければいけない**
  - **それぞれのOSごとに設定方法が異なるので、統一したポリシーを設定するのが困難。**



eTrust Access Controlを導入しないとどうなるか？

- システム監査を行う場合
  - システムから取得されるアクセス監査ログの信憑性がない。
- 情報漏洩
  - 社内からの情報漏洩が起きていても、公になるまで、そのことに気づく方法がない。気づいても、原因を突き止めることができない可能性が高い。
- ユーザ管理
  - パスワードの設定はユーザのモラルに依存する。
  - ユーザごと、OSごとにユーザアカウントを作り、それぞれにアクセス権限を設定しなければいけない。

数多くのセキュリティ・アワードを受賞

Secure Computing Magazine Award
（セキュア・コンピューティング・マガジン・アワード）

SC MAGAZINE
SC Annual Awards

2003年
Best Internet Security
（ベスト・インターネット・セキュリティ賞）

2002年
Best of Authentication and Access Control
（ベスト認証アクセスコントロール賞）
Best Buy
（ベスト・バイ賞）

LINUX WORLD 2002

LINUXWORLD CONFERENCE & EXPO
Finalist at LinuxWorld (2/02; 8/02)

CNET Linux Magazine
Editors' Choice Award

c|net
Editors' Choice
CNET.com

"Editor's Choice Award" (7/01)

アライアンス＆パートナーシップ

PeopleSoft certified PeopleSoft 8.0 Software Integration

PeopleSoft policies have been created to meet specific security requirements of its applications, virtually eliminating the risk of attacks and errors carried outside the application - at the operating system level - that would otherwise result in crashes and data corruption.

ORACLE

Oracle9i Application Server has been certified ca smart with eTrust Access Control

SUNTONE CERTIFIED

SAP

海外・国内導入事例における導入事例

eTrust Access Control国内外の導入実績

- 海外事例
  - 金融機関
    - ABNアムロ銀行、CITIグループ、Chase Manhattan銀行、Lehman Brothers証券
  - 製造業
    - Ford社、Bridgestone Firestone社
  - データセンタ、サービスプロバイダ
    - Verizon社、Sabre社、EDS社
  - 政府機関
- 日本国内導入実績
- 50社、300サーバ以上
  - 金融機関
    - 都市銀行、信託銀行、消費者金融、生命保険、クレジットカード
  - 製造業
    - 機械、化学、薬品
  - 官公庁
  - データセンタなど

Citi Bank

- IT環境
  - サーバー2,000台、クライアント 5,000台
    - Sun Solaris 2.6, 2.7, 2.8; AIX 4.3.3, HP-UX 10, 11.0, Compaq Tru64 UNIX 5.0, NT 4.0, and Windows 2000 Advanced Edition.
  - 全米10拠点、ワールドワイドで展開中
- Access Controlsを社内セキュリティ標準に
  - eTrust Access ControlはCorporate Information Security Office (CISO)にサーティファイを受け、UNIX、NTの標準装備に。
  - Citi はeTrust Access Control によって社内のセキュリティポリシーを構築
- お客様の声
  - eTrust Access Controlは、Citiのセキュリティポリシーにとって有用な“基盤”となっています。

Ford Motor Company

- フォード社のニーズ
  - 社内のセキュリティポリシーがどのように実行されているかを把握し、素早く修正ができること
  - ビジネス上重要性の高いデータへのアクセスを厳密に管理し、アクセスのイベントを管理できること、その履歴を残せること
  - ユーザアカウント管理をシンプルにすること
- ディレクトリーを中心としたユーザ管理、アクセス管理とeTrust Access Controlを統合。

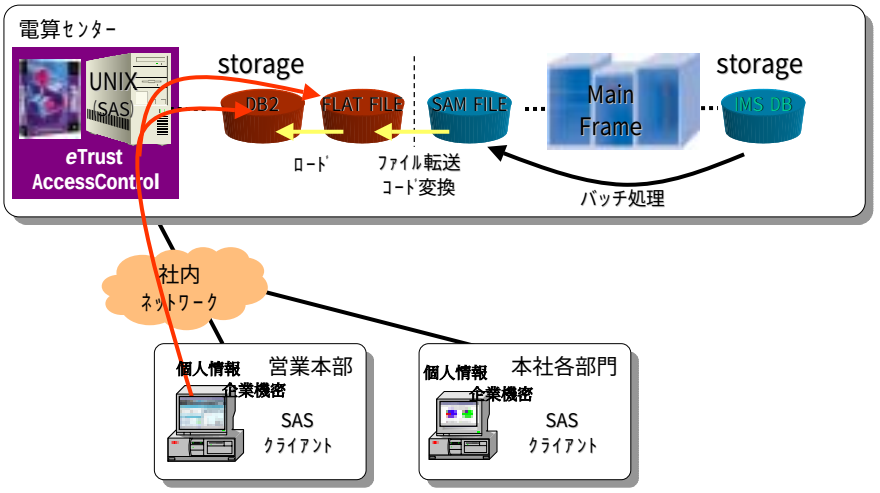
J.P. Morgan Chase & Co.

- Citigroupに次ぐ全米第二位の金融機関
  - 本社は New York、従業員95,000人
- IT環境
  - Sun Solaris, AIX
  - サーバー450台、クライアント1800台
- 対策
  - “Root”問題を解決。
  - 運用管理者だけでなく、業務アプリケーションでも、root権限が頻繁に多くのユーザによって使われていたため、アクセスログも“”root ばかりだった。現在は、アプリケーションの一部としてeTrust Access Controlは組み込まれている。
- お客様の声
  - “eTrust Access ControlはJ.P. Morgan Chaseのお客様に対するアカウンタビリティの基礎となっています。eTrust Access Controlなしで業務を遂行するのは非常に困難ともいえるでしょう。実際、eTrust Access Controlは、日々の業務を運営していくための私たちのITインフラの重要な一部です。

    John Richards, Vice President, J.P. Morgan Chase Manhattan Bank.

国内事例A社　システム構成

メインフレームからオープン系プラットフォーム (UNIX) へのダウンサイジング化にともない、メインフレームと同等の信頼性と安全性を実現



国内事例　金融B社

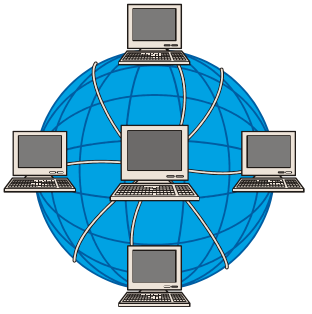
- 現在、システム運用を数社に委託している。
- eTrust Access Controlへの評価
  - 「SUコマンドを使用した後も、もとのIDで履歴がとれるだけでも導入する価値がある」

国内事例　データセンタC社

- 導入の目的　運用担当者のミスを防止
- C社で起きていた問題
  - 年に何度か、ケアレスミスによるアクシデントが発生。例えば、マシンを間違えシャットダウンしたり、サービスを停止。
  - 「人間が操作するのだから、どうしても間違いは在る。それを責めるだけでは何にも解決しない。rootユーザーの操作（コマンド）を、制限する必要がある」との事。
- 「人的教育」＋「eTrust Access Control」の両面での対策で、サービスレベルの向上を実現

国内事例　ASP事業D社

- 本来、お客様毎に、管理権限を定義し、役割に基づいたアクセス制御とアクセスに対する監査が実施できる事が理想。しかし現状は、全お客様システムに対する管理権限を限定された管理者に付与。限定しているとはいえ管理権限を持つ者を定期的に見直し、その正当性を保証したい
- アカウントとパスワードを定期的に更新するための仕組みが必要。
- eTrust Access Controlによりアカウントとパスワードの一括管理、定期的な更新を行う。
- 各種OSに依存されるパスワードのポリシーも統一する事が可能となった。



みなさんの内部情報漏洩対策をお手伝いします。

- 社内のセキュリティ対策啓蒙支援
  - 日本独自調査による内部セキュリティ対策白書“経営課題としてのアクセス・マネージメント”の提供（9月発行予定）
  - ＣＡオリジナル市場意識調査の提供
    - 経営における会社情報のセキュリティ対策に関する意識調査
  - 経営者向け内部セキュリティ対策セミナーのご案内
- 国内事例の紹介
  - 事例セミナー
- 海外事例の紹介
  - リファレンスユーザの情報
- セキュリティ対策のROIの算出
  - ROIスプレッドシートによる試算

ご静聴ありがとうございました。