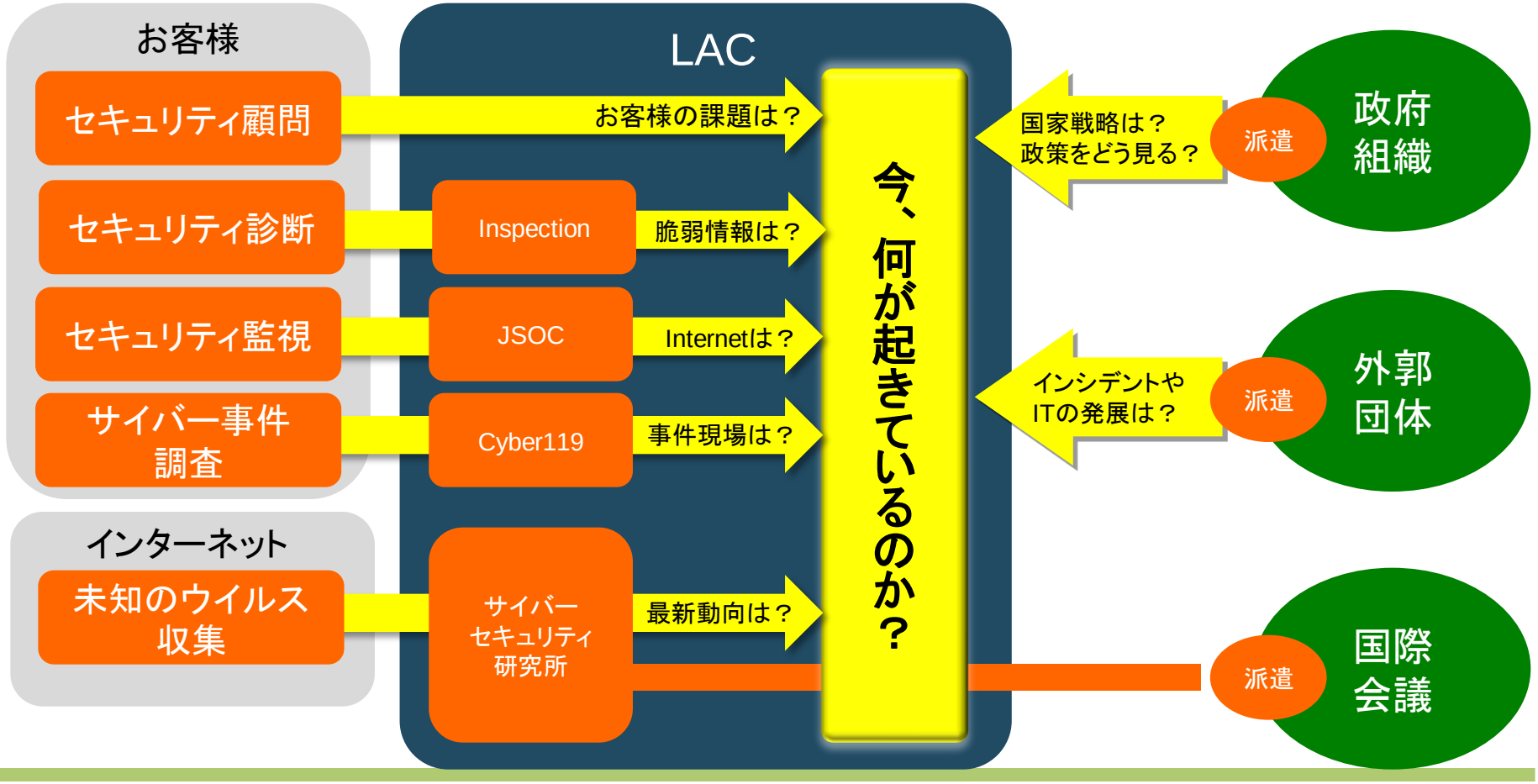
システム更改のタイミングを逃すな！ 今ドキSecurityの対策ポイント

株式会社ラック
ビジネスディベロップメント本部
山田　昌透

株式会社ラックのご紹介

Why?

「今、何が起きているのか？」
常に最新のITセキュリティ動向を広く深く把握
お客様のセキュリティパートナー



アジェンダ

- 最新セキュリティ事情
- 本題
  - OSの特権ID管理権強化事例
    - 検討～導入　事例1
    - 検討　事例2

最新セキュリティ事情　その1

- 金融機関のWebサービスへの攻撃
  - Webサービスを停止させる
  - Distributed Denial of Service（DDoS攻撃）
  - 北米の銀行がターゲット
- リスト型不正ログイン攻撃
  - ポータルサイト、ショッピングサイトなどに不正なログインの試行が発生

最新セキュリティ事情　その2

- Webサイトの改ざん
  - 見た目の改ざんではなく、マルウェアを仕込まれる
  - アクセスしたユーザがマルウェアに感染
  - 被害者であり、加担者になるということ

- インターネットバンキングを狙った不正送金マルウェア
  - Man in the Browser（MITB）
  - 利用者の端末が専用のマルウェアに感染して発生

セキュリティ上の課題／整理方法

	外部脅威	内部悪意	内部過失	対策
リスト型不正ログイン	○			早期検知（WAF）
Webサイトの改ざん	○			Web診断、脆弱性対策
インターネットバンク不正取引（MITB）	○			マルウェア検出（ワンタイムパスワード）
Webサービス停止（DDoS攻撃）	○			Contents Delivery Network（CDN）導入
情報持ち出し・漏洩	○	○	○	特権ID管理、アクセスログ
不正操作	○	○	○	特権ID管理、アクセス制御

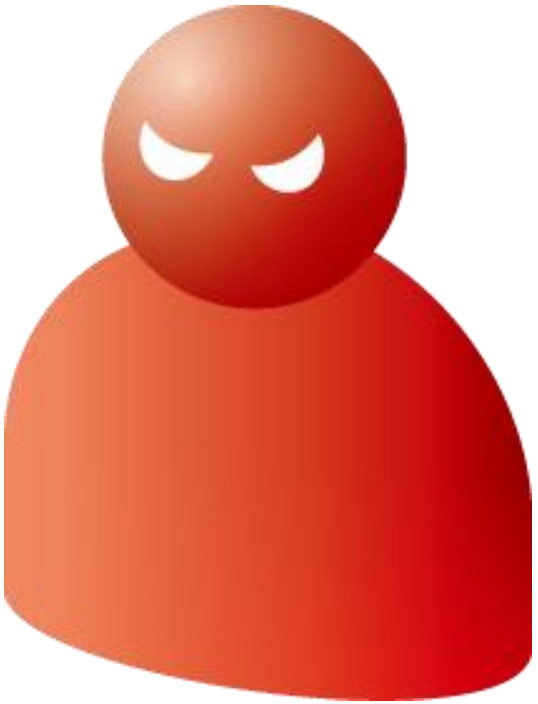
OSの特権ID管理強化事例

OSの特権IDとは？

- Windowsであれば「Administrator」
- Linux／Unixであれば「root」
- 初期状態では、
  - サーバを停止・初期化できる
  - ユーザを作成できる
  - データを削除できる
- よくある光景
  - 運用者が全員Administratorのパスワードを知っている

最悪のシナリオ

- 1:Administratorでログイン
  - 2:架空のユーザIDを作成
  - 3:架空のユーザIDに特権同等権限を割り当て
- 4:架空のユーザIDでログイン
  - 5:顧客データをコピー
- 6:Administratorでログイン
  - 7:架空のユーザIDを削除
  - 8:一連の操作履歴・ログを削除



原則の確認

- 内部統制の基本
  - 職務分掌
    - ◆発注担当者と、支払い担当者は、別の人が担当する
- セキュリティの基本
  - 権限の分離
    - ◆システムの管理者とビジネスの責任者は別の人

事例1:プロジェクト概要

- 大手金融機関
  - UNIXサーバから、Linuxサーバへ更改
  - 社内情報系システム
  - 仮想化環境
- 目的
  - コスト削減、アプリケーションの見直し
  - 監査・内部統制およびセキュリティ強化
- 検討項目
  - OSの特権ID管理ソリューション選定

事例1:ソリューション選定(OS vs 製品)

項目	OSの標準機能	特権ID管理製品
ポリシー設定	各サーバで個別に設定	一括管理 OSと別体系の管理者
保存する単位	複数ファイル (ログイン:wtmp、スイッチ:sulog 等)	管理対象イベント全てが1ファイル
ログフォーマット	イベントごとに異なる	イベントに依存しない
ログへのアクセス制御	OSパーミッション設定に依存	OS管理者も削除不可
ユーザスイッチログ	スイッチ後のIDでログが残る	スイッチ前のIDでログ取得が可能
コスト	ライセンスは費用なし	ライセンス費用が必要

事例1:選定における決定打

- 権限分離の原則
  - システム運用の管理者＝OSの特権ID
  - 業務の責任者＝特権ID管理ソリューションの採用

事例1:システムイメージ／権限分離イメージ

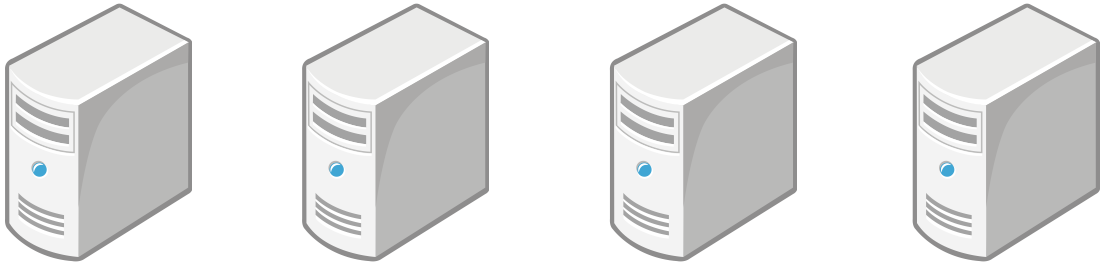
開発チーム・運用チーム

業務の責任者

監査

Windows、Linux

VMware



CA ControlMinder
操作履歴を管理
・パスワード管理
・ログイン制御
・ファイルアクセス制御
・ユーザなりかわり制御

事例1:分かったこと

- 課題としては分かっているが・・・
  - 監査から指摘されたものの・・・
  - 稼働中のシステムへの影響・・・
  - 現在の運用を変えたくない

- システム更改のタイミングはチャンス
  - 業務システムへの影響見極め可能
  - 運用の見直しも可能

事例2:プロジェクト概要

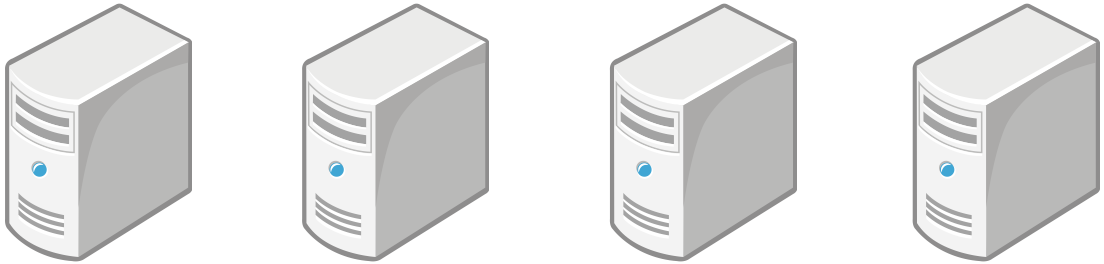
- 大手金融機関
  - 監査指摘事項への対応
  - 特権IDの管理・監査を検討
  - システム全体の共通基盤・統合ツールとしての導入
  - 運用チーム（外部委託）主体の検討

事例2:システムイメージ／権限分離イメージ

開発チーム・運用チーム

手組み
操作履歴を管理
・パスワード管理
・ログイン制御
・ファイルアクセス制御
・ユーザなりかわり制御

Windows、Unix／Linux



レポート

業務の責任者

比較　事例1

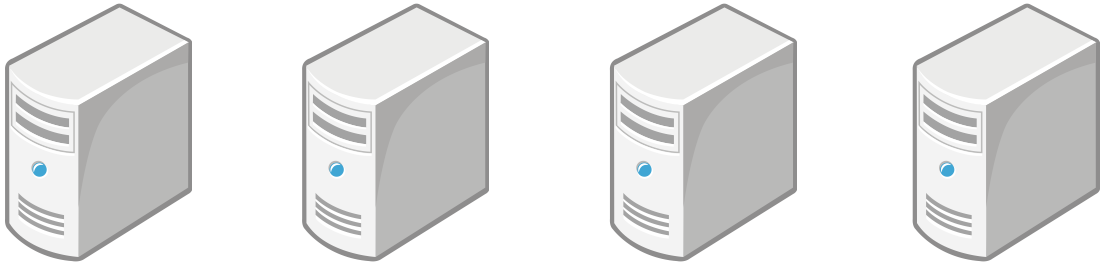
開発チーム・運用チーム

業務の責任者

監査

Windows、Linux

VMware



CA ControlMinder
操作履歴を管理
・パスワード管理
・ログイン制御
・ファイルアクセス制御
・ユーザなりかわり制御

事例2:分かったこと:本質的な問題

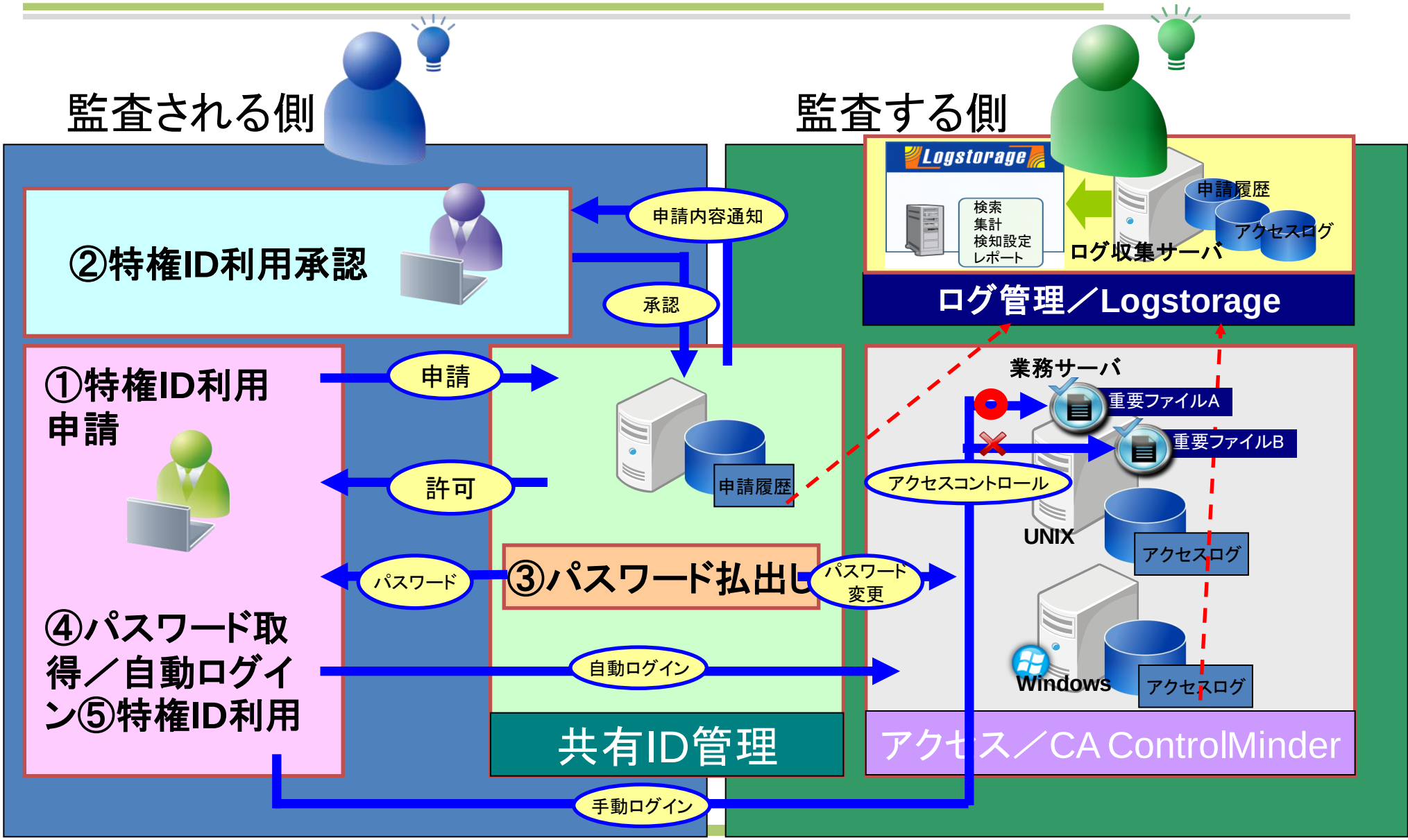
- 監査される側が開発したツールによるレポート
  - ログ収集＝＞加工＝＞レポート
- 監査される側の正当性を証明しようとしている
  - ログ収集＝＞改ざん＝＞虚偽報告

  - お客様(業務の責任者)と運用委託先には、長いおつきあいという歴史と信頼関係
  - 私から指摘しても、ご納得いただけません

刑事ドラマに例えるなら・・・

おかあさんの証言は、息子さんのアリバイの証拠にならないんです

お奨めのソリューション・権限分離モデル



まとめ

- 「権限分離」原則の徹底を！
  - 「特権ID」と「特権IDの監査」の分離
- システム更改のタイミングは、徹底のチャンス！

- 「特権ID」を狙ったサイバー攻撃も！
  - Webの脆弱性対策の再確認
  - Webの特権IDの設定見直し

アシストフォーラム
企業の情報活用をアシストする
ASHISUTO FORUM 2013
東京／名古屋／大阪／福岡

ご清聴ありがとうございました

LAC
安心とともに

付録:OS標準ログの課題

システムログ（syslog）

/var/log/messagesなど
マシン起動、停止、rootユーザのログイン等
一般的なシステムログ

ログインログ

/var/log/wtmp
ユーザのログイン、ログアウト履歴

/var/log/btmp
ユーザのログイン失敗、ログアウト失敗

コマンドログ

/var/log/pacct
ユーザのコマンド実行履歴

OS標準ログの課題

■複数のログファイルに分散されている
⇒一連の操作の流れの把握が困難

■時刻の情報に年やタイムゾーンがない
⇒長期間保存の場合、ログファイル管理が別途必要

■テキスト形式で出力（システムログ）
⇒改ざんが出来る

■シスログ転送はUDPプロトコルを使用
⇒取りこぼしの可能性がある