Identity Base Security 実装プロジェクト事例

グローバルセキュリティエキスパート株式会社
ソリューション事業部　エグゼクティブコンサルタント
宮川　晃一

GSX
GLOBAL SECURITY EXPERTS

GSX
GLOBAL SECURITY EXPERTS

Agenda

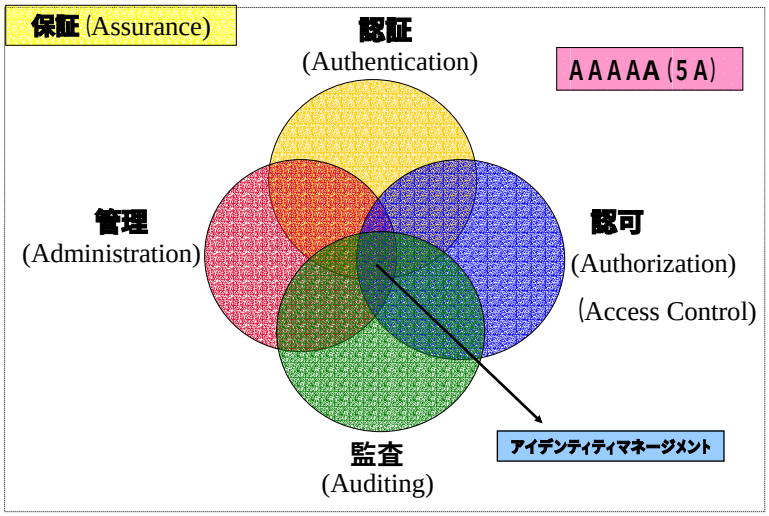
- Identity Management の解説
- プロジェクト事例

Identity Management の解説

GSX
GLOBAL SECURITY EXPERTS

GSX
GLOBAL SECURITY EXPERTS

Identity Management の技術的位置付け



Identity Management とは

Identity Management とは、システムを利用するユーザ情報を一元集中管理し様々な観点からユーザおよび管理者の利便性の向上を図るソリューションである

セキュリティ管理の共通基盤

誰が、どの情報資産に、どのような認証手法で、どういう権限で
アクセスできるかを定義し、それを「一元管理」する仕組み。
かつ、その運行状況を確認できる手段（ログ）が存在する仕組み。

Identity に関するビジネス上の課題

➢ユビキタスネットワークの必要性

- ビジネス要求として、利用場所を限定しないネットワークサービスの要求
- 企業のグローバル化による、24H／365日のサービス要求
- ネットワーク利用者の多様化（派遣社員の増大、ビジネスパートナーの利用）

➢Identity 管理コストの増大

- オープン化に伴う、管理サーバーの増加とそれに伴う管理コストの増加
- ダイナミックな組織改変や改変回数の増加
- 上司、部下の関係の変化

➢セキュリティ対応

- Need to Know の原則（知る必要の原則）の実施の必要性
- 退職ユーザのメンテナンス対応
- 組織改編・人事異動に伴うアクセス権の見直し

➢コンプライアンス／グローバルスタンダード対応

- 個人情報保護法
- ISMS適合性評価制度／BS7799対応

Need to Know の原則とは

情報システムの利用者にアクセス権を与える際は、**「知る必要(Need to know)の原則」**に則る必要がある。

「Need to knowの原則」とは、ある業務を役割として与えられた担当者に対して、その業務を遂行するために**必要な情報にのみアクセスすることを許可**するというもの。

Need to knowの原則を適用することで、情報資産ごとのアクセス権所有者数は最少に絞り込まれる。(最小特権の原則)

アクセス権限者を最少にすることが、**事件・事故が発生するリスクを最小にする効果**を持つ

Identity Management の期待効果

➢コストの削減と生産性向上

- 組織改編・人事異動のメンテナンス負荷の削減
- 自動化による操作ミスの排除
- アクセス権付与時のメンテナンス負荷の削減
- 上司、部下の複雑な関係を自動的に紐付け
- シングル・サインオンによる利用者の生産性向上

➢サービスレベルの向上

- ポータルによる情報のパーソナライズ化
- BtoE から BtoE, BtoC への適応範囲を容易に拡張
- ユビキタスネットワークの実現基盤

➢セキュリティの向上とコンプライアンス対応

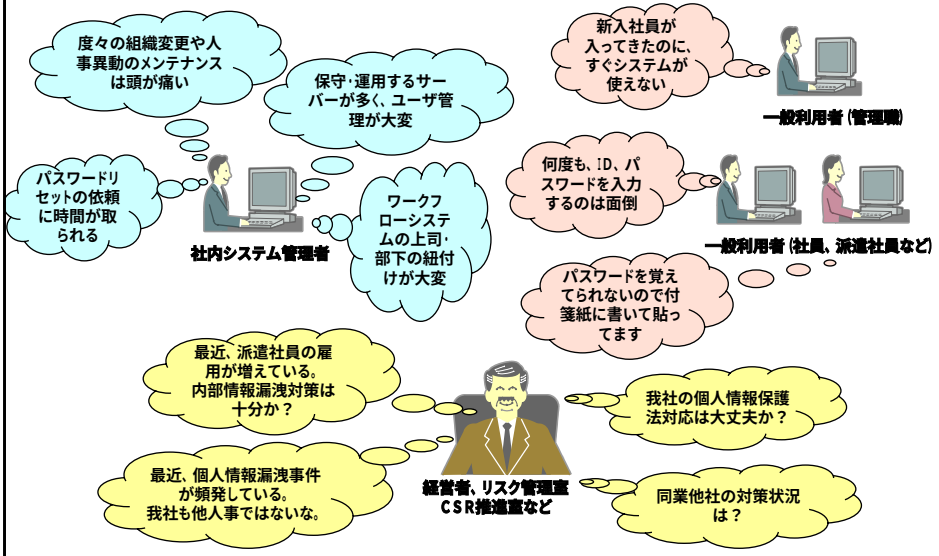
- Need to Know の原則に従ったアクセス権付与
- 組織改編・人事異動に伴う、Identity管理の自動化
- 認証・アクセスログの取得が容易になる
- 個人情報保護法対応、ISMS，BS7799対応

国内企業の取り組み状況

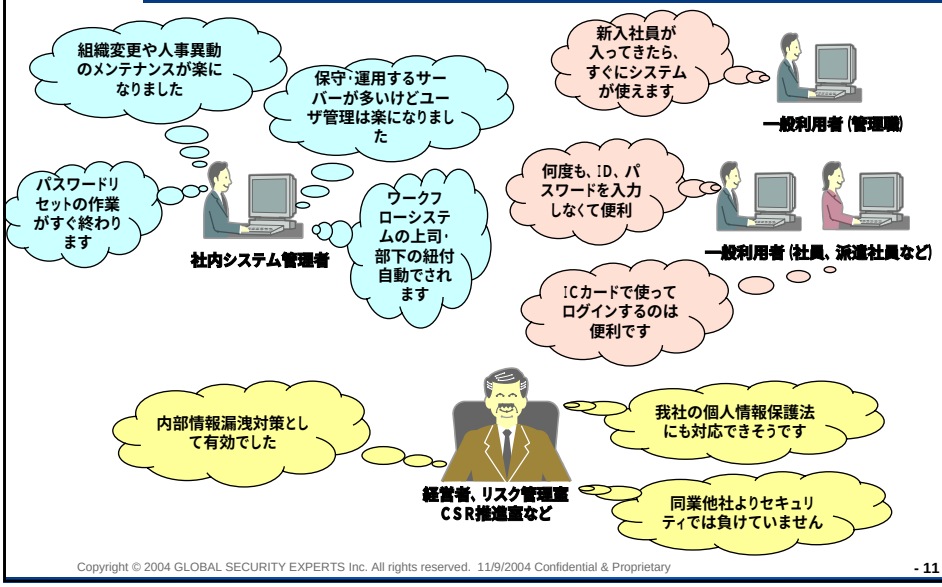
➢大手企業は何かしらの手段で対策を実施
- 共通マスターの構築
- 一部システムのみ適用
- アクセス権付与の自動化までは未整備
- 単純なWebシングル・サインオンを導入済み
- 全社社内ポータルは実施しているが効果はあまり出ていない
- ICカードについては、物理セキュリティの適用がほとんど

➢外的要因からの必要性による検討開始
- 個人情報保護法対応
- 情報漏えい対策の1つ
- 各業界団体の指導

企業内の声：Identity Management 実施前



企業内の声：Identity Management 実施後



個人情報保護法と Identity Management

経済産業省 （10月13日）

「個人情報の保護に関する法律についての経済産業分野を対象するガイドライン」

個人情報保護法　第20条

個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。
個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のため、組織的、人的、物理的、及び**技術的安全管理措置**を講じなければならない。
その際、本人の個人データが漏えい、滅失又はき損等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の性質及び個人データの取扱い状況等に起因するリスクに応じ、必要かつ適切な措置を講じるものとする。
なお、その際には、個人データを記録した媒体の性質に応じた安全管理措置を講じることが望ましい。

個人情報保護法と Identity Management

技術的安全管理措置

技術的安全管理措置とは、個人データ及びそれを取り扱う情報システムへのアクセス制御、不正ソフトウェア対策、情報システムの監視等、個人データに対する技術的な安全管理措置をいう。技術的安全管理措置には、以下の事項が含まれる。

①個人データへのアクセスにおける識別と認証
②個人データへのアクセス制御
③個人データへのアクセス権限の管理
④個人データのアクセスの記録

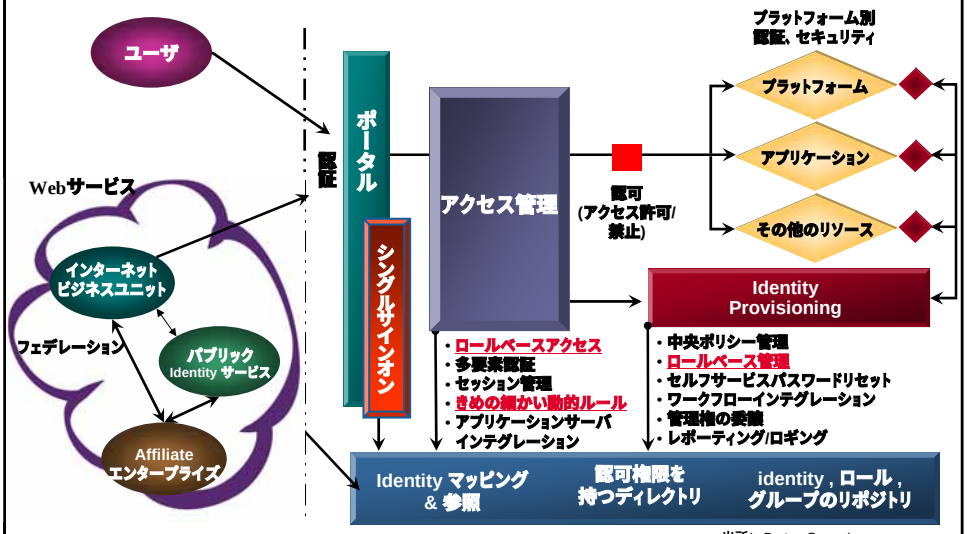
→ アイデンティティ・マネージメント適用範囲

⑤個人データを取り扱う情報システムに対する不正ソフトウェア対策
⑥個人データの移送・通信時の対策
⑦個人データを取り扱う情報システムの動作確認時の対策
⑧個人データを取り扱う情報システムの監視

個人情報漏洩事件後の対応状況（約1年間）

	信販A社	信販B社	流通C社	流通D社	鉄道E社	鉄道F社	通信G社	通信H社
情報セキュリティ教育	○	○	○	○	○	○	○	○
情報セキュリティ監査	○	○		○	○	○	○	
ﾃﾞｰﾀｱｸｾｽ権限の制限	○	○	○	○			○	○
生体認証			○	○	○			
ﾛｸﾞ管理	○	○			○	○	○	○
PC 機能制限	○	○					○	
暗号化	○				○			○
高ｾｷｭﾘﾃｨｴﾘｱの設置	○	○		○	○		○	○
監視ｶﾒﾗ	○	○		○	○			

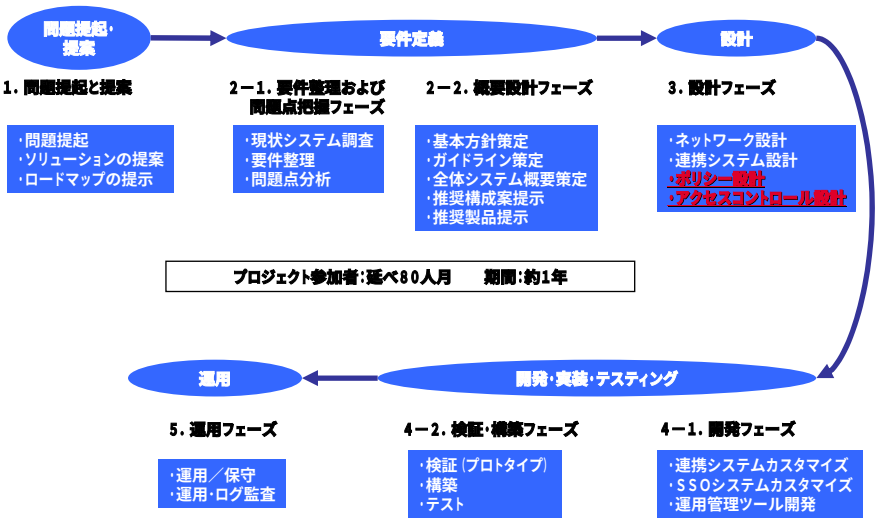
Identity Management の全体像



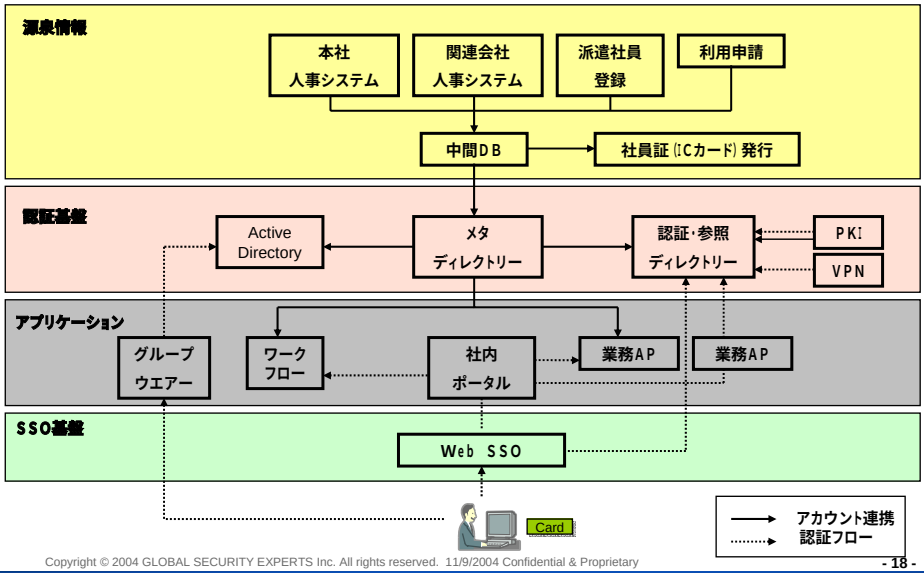
出所: Burton Group Inc

プロジェクト事例

Identity Management 導入 project の流れ



導入構成事例

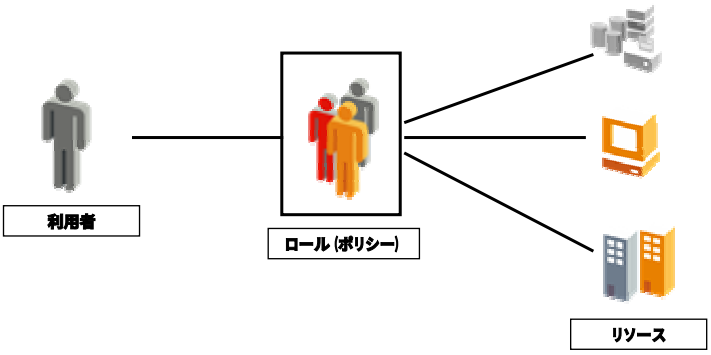


GSX GLOBAL SECURITY EXPERTS

ロールベースセキュリティ

➢ロールベースセキュリティ

- 利用者ユーザと組織や職務との関係に基づき、リソースへのアクセスを管理する手法のこと。(ポリシーベースセキュリティとも言う)

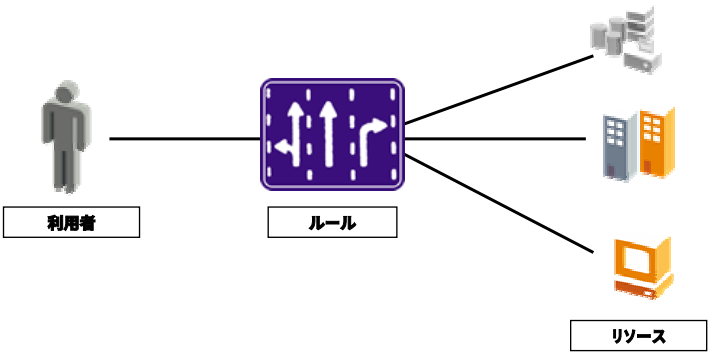


GSX GLOBAL SECURITY EXPERTS

ルールベースセキュリティ

➢ルールベースセキュリティ

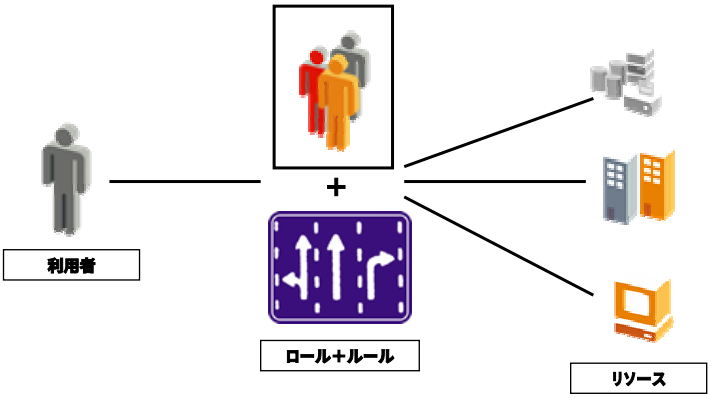
- ビジネス・ルール (そのときの条件やアクション) を用いて、リソースへのアクセスを管理する手法のこと。動的にリソースのアクセス権を変更できる。



Identity Base セキュリティ

➢アイデンティティベースセキュリティ

- ロールベースセキュリティとルールベースセキュリティをうまく組み合わせて、より少ない定義（ポリシー）をシンプルに実装する手法のこと



ロールの設計例

➢会社組織をベースに設計

＜基本ガイドライン＞

- 組織階層毎にロールを持たせる
  ＝＞ただし、階層は上位から3階層とする
  下位階層は利用する社員があまりいない
  ＝＞**ルールで対応**
- 職位別、役職別にロールを持たせる
  担当組織の長は自組織以下のロール内容を変更できる。（権限委譲）
  ＝＞ただし、兼務は除外する
  実務兼務と肩書きのみの兼務
  ＝＞**ルールで対応**
- 組織を横断して業務を行う、プロジェクト別にロールを持たせる
- ロールの入れ子による、アクセス権の冗長性を排除

ルールの設計例

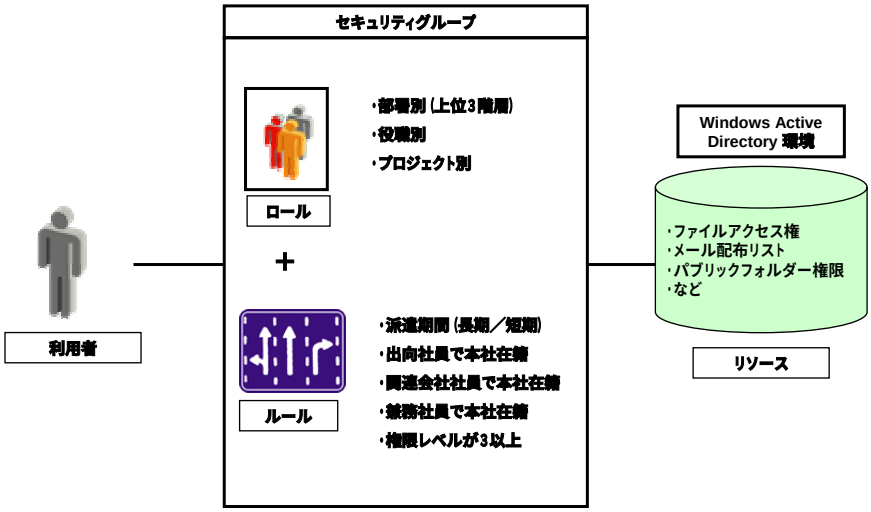
➢ロールでは煩雑すぎるものをルールとして設計

＜基本ガイドライン＞

- 組織階層で例外／特例をルールで定義
  - 下位組織で特別なアクセス権が必要なばあい
  - 出向社員で本社内で作業を行う社員
  - 派遣社員で長期の場合は、担当組織と同じロールを付与

- 職位別、役職別で例外／特例をルールで定義
  - 兼務者で実務上必要な場合は、兼務組織と同じロールを付与
  - 同一組織内でも異なるロールが必要な場合を特権レベルで管理

Identity Base セキュリティの実装例



まとめ

➢Identity Base Security とは

- Identity Management 上でロールやルールをうまく活用し、セキュリティの原則である、Need to Know の原則に従って、確実でかつシンプルなアクセスコントロールを実施すること。

➢Identity Management とは

- セキュリティを向上させながら、かつ管理コストを削減できるソリューションである。
- 今後のビジネス規模拡大における、ITインフラのセキュリティ共通基盤およびユビキタスネットワークサービスの基盤となるものである。

謝辞

- ご清聴ありがとうございました。