JNSA

NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

内部統制におけるアイデンティティ管理とは

2008年度　内部統制におけるアイデンティティ管理WG成果報告

グローバルセキュリティエキスパート株式会社
宮川　晃一
標準化部会

2009 年 6 月3日

本WGの目的

内部統制におけるアイデンティティ管理WGの目的

J-SOX法における「内部統制」の必要性が叫ばれている中で、ITの全般統制として、ITセキュリティに関する対応の必然性が求められています。

その中でも、ID管理（アイデンティティマネージメント）分野については、セキュリティポリシーを実装する上での共通基盤として注目されている分野です。

内部統制とアイデンティティ管理の関連をWG討議の中で紐解き、必要性の啓蒙および導入指針の提示による普及促進、市場活性化を狙うことを目的にしています。

2008年度の活動内容

1．WGの開催（全9回実施）

1）監査法人トーマツの丸山様より、内部統制監査の状況について解説をしていただいた。

2）各IDM製品ベンダー様より、各社の導入事例を紹介していただいた。

3）業種別の仮想企業における導入事例作りをグループに分かれて討議を実施した。

ケース1：　金融業　　カード会社　　PCIDSS対応

ケース2：　製造業　　自動車部品製造会社　　内部統制

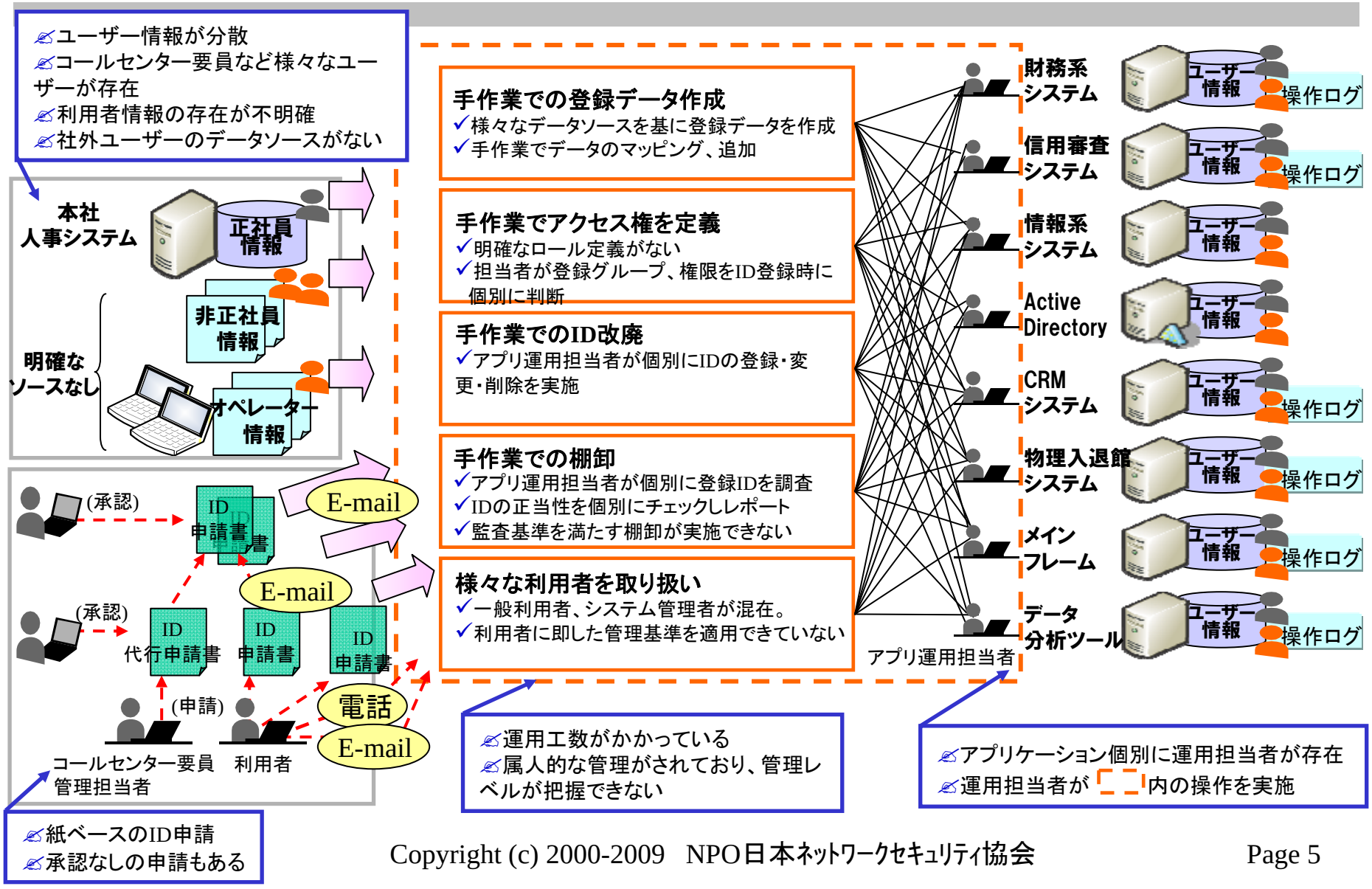
2．「内部統制におけるアイデンティティ管理解説書」（第2版）

6月中旬　発行予定

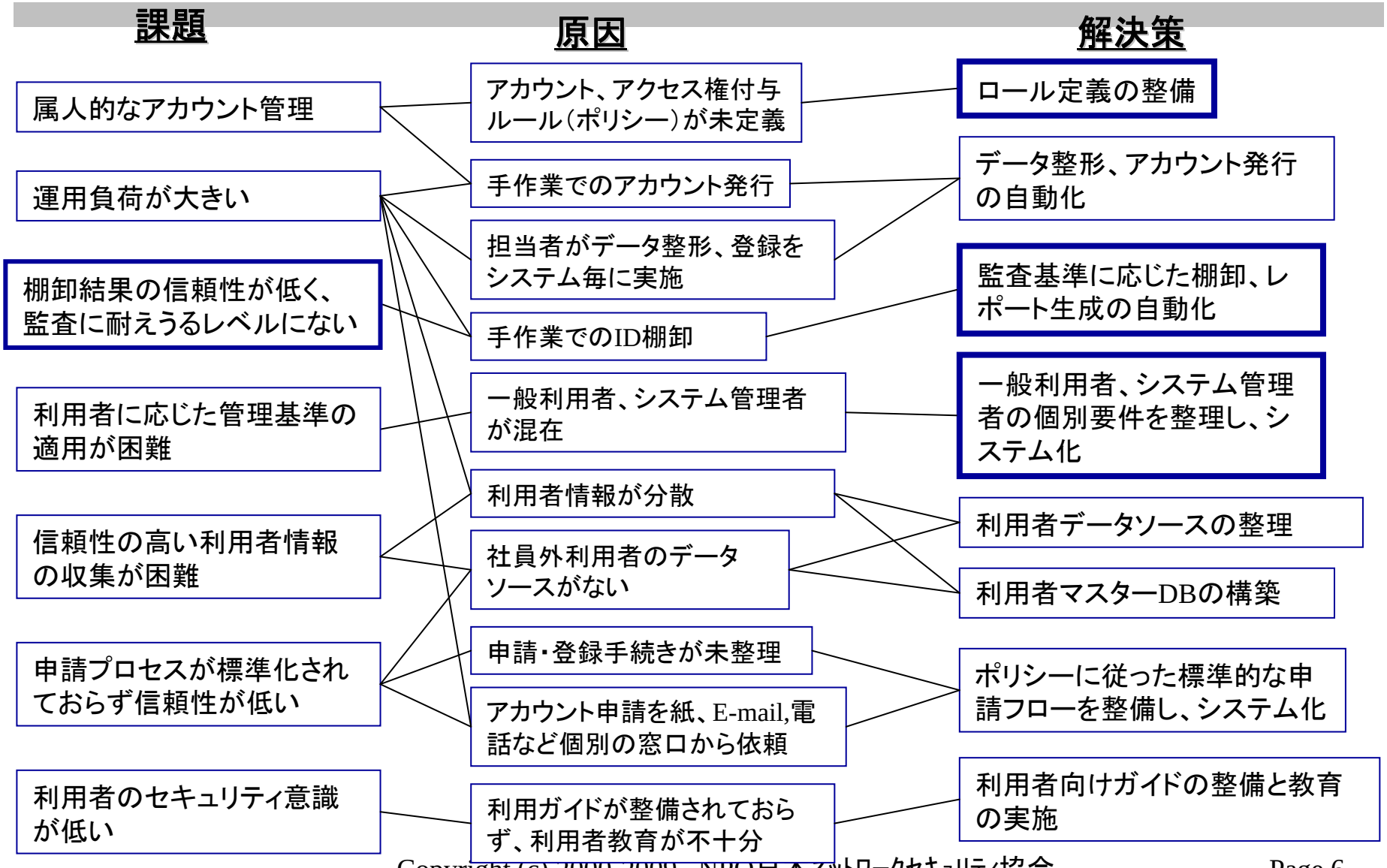
ケース1：金融業の仮想事例

業種		金融（カード会社）
従業員数		3,000 （正社員:2,000名　非正社員:1,000名）
IDユーザー数		3,000
課題	コンプライアンス	監査対応
	情報漏えい対策	必要
	法制度/業界ガイドラインからの要求	SOX、J-SOX、PCI DSS、GLBA、BASEL II
	その他	CoBIT, ITIL
	シェアードサービス	あり
予算	初年度	1億円
	次年度以降	ランニングコスト：1,500万円 システム拡張；2,500万円（対象システム追加など）
社内体制	ISMS	あり
	CoBIT	あり
	ガバナンス体制	内部統制対策室設置
情報システム		■初年度対象システム ・財務系システム（RDBMS） ・情報系システム（LDAP） ・Active Directory ■次年度以降対象システム ・CRMシステム（パッケージ・ソフト） ・物理入退館システム ・メインフレーム ・データ分析ツール
ハードウェア		Windows、Linux、商用UNIX、メインフレーム
IDM対象範囲		B to E（社内システムユーザー対象）
IT運用者数		50名程度
情報の分類	オーナー 決定権者	存在する CIO
その他		自社内にコール・センターあり

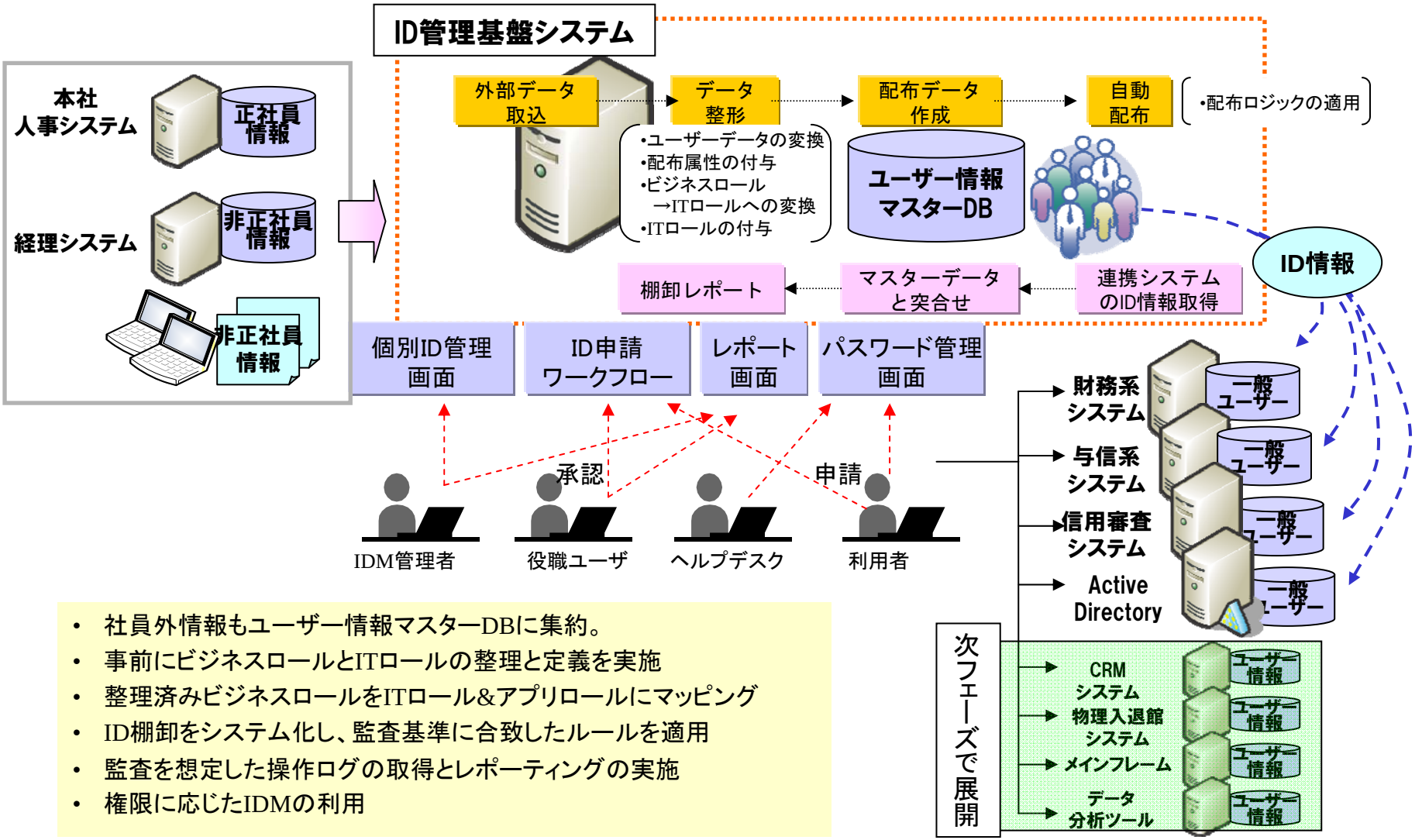
ケース1：現状の課題



ケース1：現状の課題と解決策



ケース1：導入後イメージ

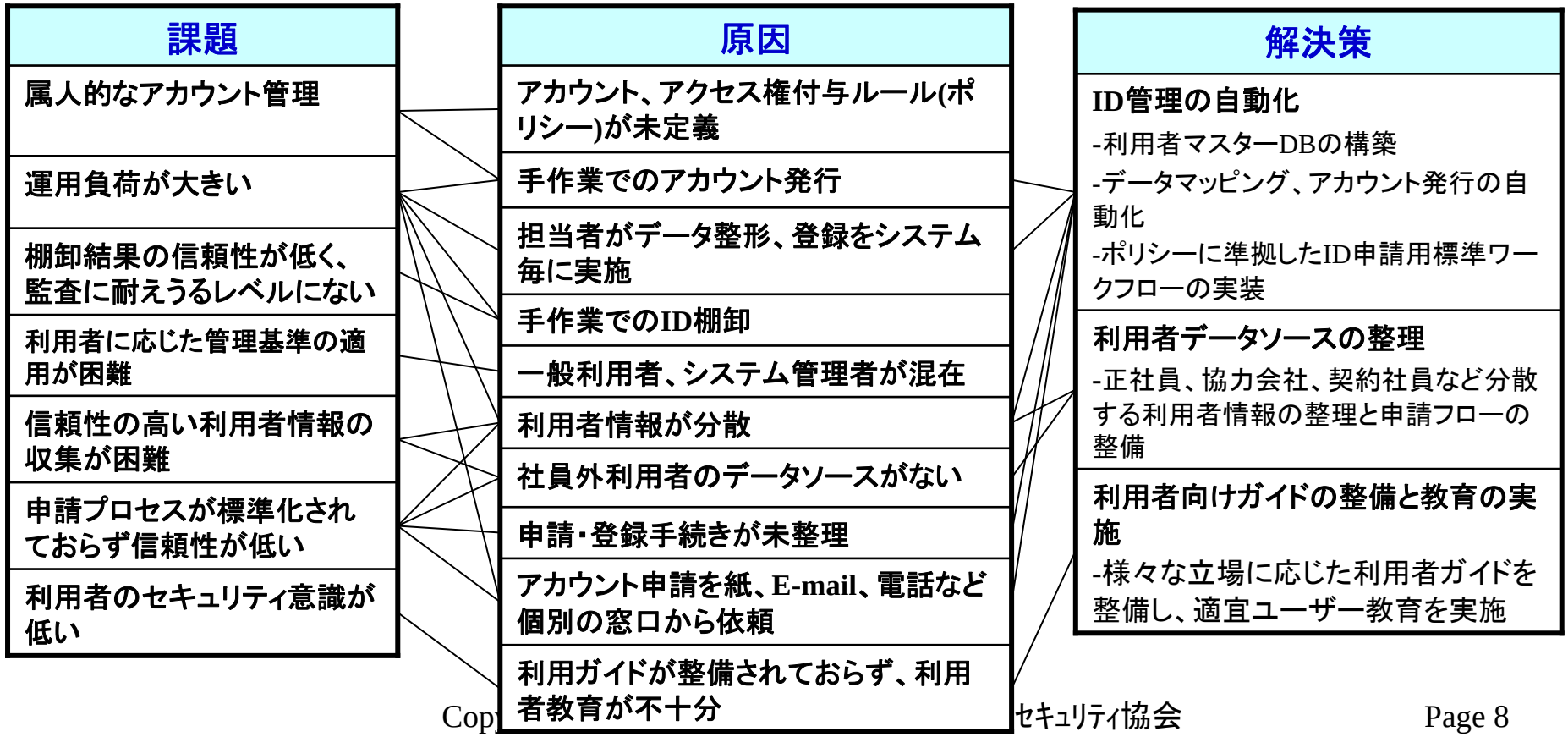


- 社員外情報もユーザー情報マスターDBに集約。
- 事前にビジネスロールとITロールの整理と定義を実施
- 整理済みビジネスロールをITロール&アプリロールにマッピング
- ID棚卸をシステム化し、監査基準に合致したルールを適用
- 監査を想定した操作ログの取得とレポーティングの実施
- 権限に応じたIDMの利用

ケース1：導入後の効果

ID管理システム導入により、下記効果を期待できます

1. ID管理の自動化による業務効率の向上と運用管理コストの削減
2. 棚卸の自動化により不正ユーザーを排除し、セキュリティを強化
3. IDの正当性担保によるアクセス履歴の信頼性と対監査性の向上



ケース2：製造業の仮想事例

項番	検討項目	分類	適用事項
1	業種	製造業	自動車部品メーカー　**社名：JNSA自動車部品製造株式会社**
2	関係会社数		**5社**
3	親会社		なし
4	従業員	正社員／非正社員	**社員：4000人　非正社員：1000人**
5	ID数		**5000ID**
6	事業部数		**3事業部**
7	部署数		**5部、10課**
8	課題	コンプライアンス	一部上場企業であるため、**内部統制の対応が必須**
		情報漏えい	過去に特権ユーザによる、**知財情報の漏えい**の事故が発生している
		運用	情報システム**子会社に委託**をしており、本社では企画のみを実施
9	予算	初年度予算	**1億円**
		次年度以降	**2．500万円（3年間）**
10	社内体制	ISMS	なし　セキュリティポリシーはお飾り程度のものはある
		Cobit	なし
		ガバナンス体制	専任者はいない
11	情報システム	対象システム	**ERP/RDB** － 本社にて連結会計を実施
			Exchange/ActiveDirectory － 事業部単位に個別運用されている
			M/F － 部品管理システムで一部使用している
			Webアプリ － 大部分の業務アプリケーション
			C/Sシステム － OA系のシステムで一部存在
			Notes － 全社グループウエア
		対象システム数	**25システム**
		H／W	**50サーバー　Windows/Unix/MF**
12	IDM対象範囲		**本社および各事業部**
			海外拠点
			派遣社員含む非正規社員を含む
13	情報システム部門	スタッフ数（本社）	**10**
		スタッフ数（3事業部）	**30**
14	意思決定者	オーナー	**社長**
		責任者	**CIO**

ケース2：製造業の特色

- **組織**
  - 本部より事業部の力が強い。
  - 情報システム部門はカンパニー毎に存在する。
  - 企画は本部が実施し、運用構築は情報システム部門が実施する。
  - 海外拠点が存在する。

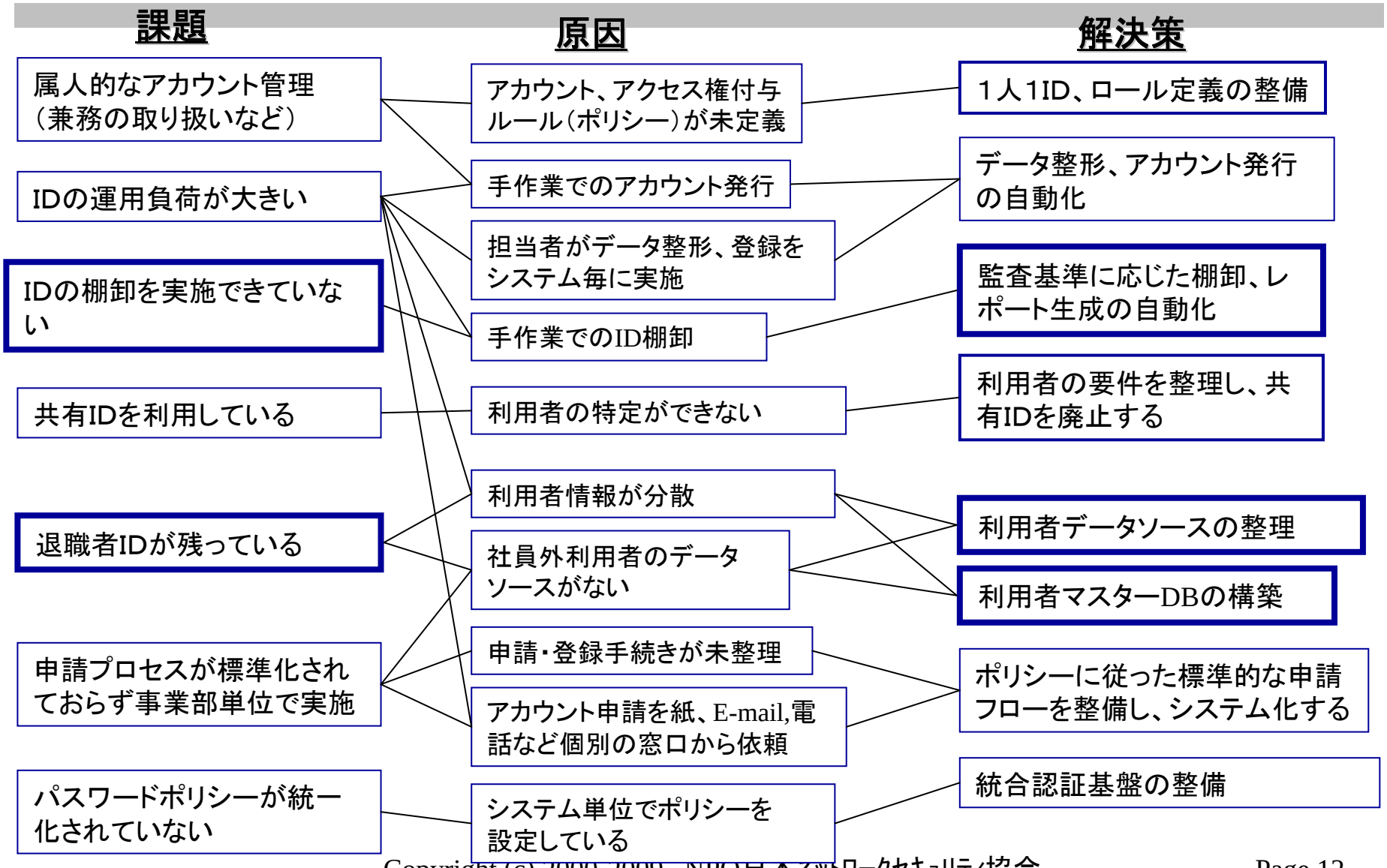
- **予算**
  - 予算は事業部予算。（企画は本部）
  - ITのシェアードサービス化により、課金するケースがある。

- **ID運用における特徴**
  - システムを使用しないのに、IDを持っている。
  - 共有IDの使用が多い。
    - 機械にIDが組み込まれている。
    - 非正社員は共有IDが多い。
    - 役割にIDが紐づいている。
  - 関連会社からの出向などで、IDおよびメールアドレスを2つ持っている。

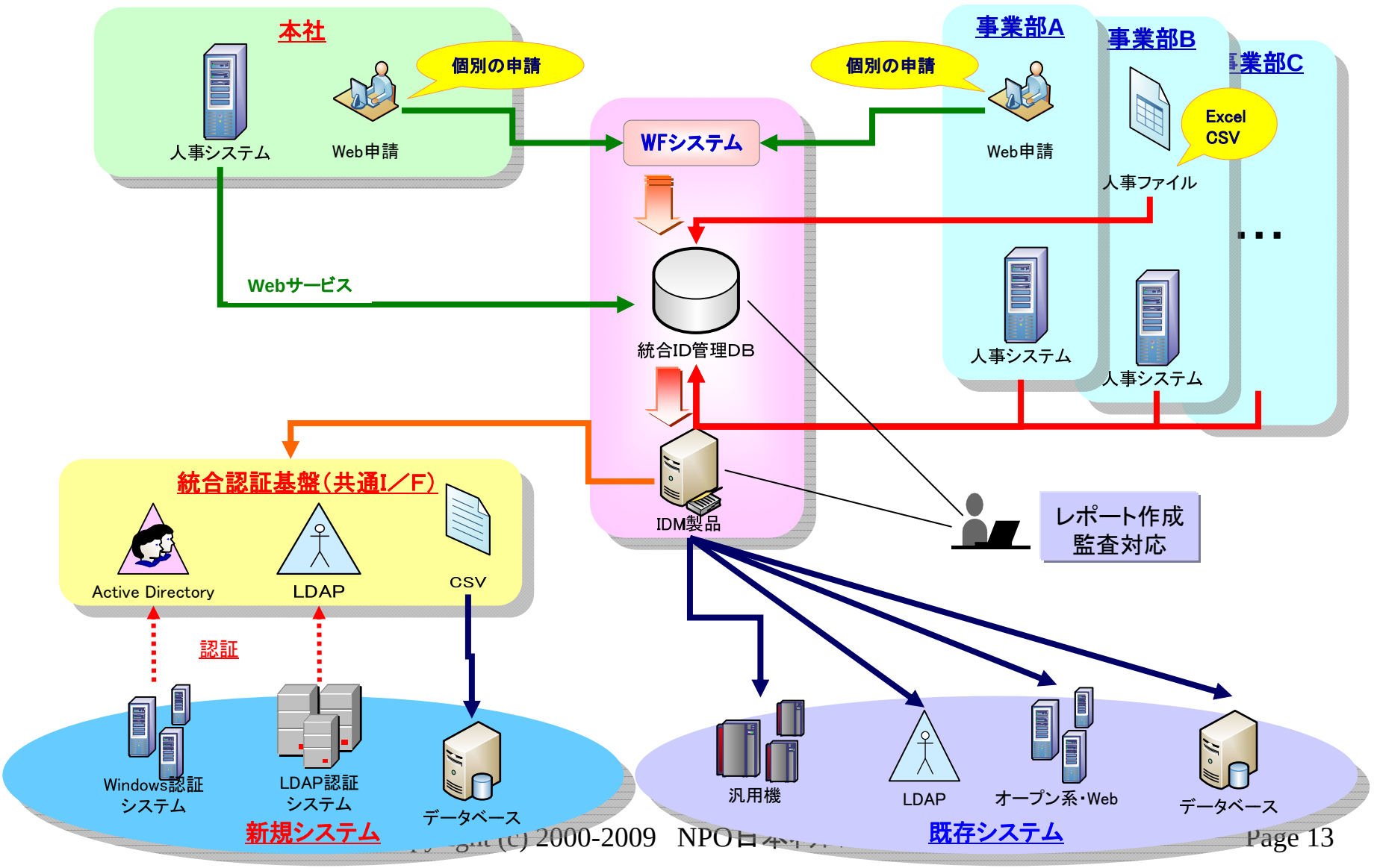
ケース2：対応状況と対応優先度

No	事業部	主なシステム		アーキテクチャ	監査の指摘	課題	解決策	優先度
1	フレーム	営業 設計 製造 管理	①ERP	①SAP AS／アカウントはSAP内。	利用者の役割や職務を変更した利用者又は、組織から離れた利用者のアクセス権の即座の解除や停止が確実に行われていない。（情報セキュリティ管理基準7.2.1.10より抜粋）	登録IDの定期的な棚卸し・レビュー	・退職者の自動削除 ・SOD自動分析	A
2	内装	営業 設計 製造 管理	①メインフレーム	①ホストOS390／アカウントはホストOS内	利用者の登録・削除の際、利用者と利用者自身の行動とを対応付けが出来ていない。（情報セキュリティ管理基準7.2.1.1より抜粋）	IDの一元管理	・IDリポジトリ構築とプロビジョニングによるID連携	C
3	電装	営業 設計 製造 管理	①個別パッケージ	①Webアプリ(Web+DB)／アカウントはDB内。	利用者の登録の際、割当てらたアクセスレベルが、組織の基本方針と異なっており、職務分掌に矛盾している。（情報セきりティ管理基準7.2.1.5より抜粋）	利用者IDの登録承認プロセスの確立	・WF導入と責任者の明確化	B
4	本社	営業 設計 製造 管理	①OA系（メール、GW、F/S） ②人事システム ③会計システム ④製造・物流システム	①メールはExchangeServerを使用。アカウントはADに連携。	割当てた全ての特権に対して、認可プロセスを記録できていない。（情報セキュリティ管理基準7.2.2.4より抜粋）	特権IDの登録承認プロセスの記録	・WF導入と承認プロセス監査ログ	B

ケース2：現状の課題と解決策



ケース2：導入後イメージ



ケース2：導入後の効果

ID管理システム導入により、下記効果があった。

1.ID管理の自動化による業務効率の向上と運用管理コストの削減

2.棚卸の自動化により不正ユーザーを排除し、内部統制を強化

3.共有IDの排除、人以外の機械が利用しているIDの把握が可能

4.IDの正当性担保によるアクセスログの信頼性と監査性の向上

5.統合認証基盤の整備による、セキュリティポリシーを平準化

2009年度の活動予定

1. WG名称の変更

「セキュリティにおけるアイデンティティ管理WG」

2. テーマ候補

1）ロールマネジメント

－日本におけるロールマネジメントを考える

－各メーカーのロール管理製品の勉強会

2）ID管理技術最新動向

－ open ID , Liberty , IEEE の動向など

3）日本版SOX1年目の監査動向

－監査法人様より

3. 活動頻度

原則月１回のWG実施

謝　辞

本WGにご協力していただいた皆様へ

ご協力いただき、大変ありがとうございました。

氏名	所属
柿崎　司	株式会社アクシオ
富士榮　尚寛	伊藤忠テクノソリューションズ株式会社
大日向　文章	伊藤忠テクノソリューションズ株式会社
工藤 浩	伊藤忠テクノソリューションズ株式会社
中島　浩光	株式会社インフォセック
高橋　諄	NRIセキュアテクノロジーズ株式会社
小澤　浩一	京セラコミュニケーションシステム株式会社
宮川　晃一	グローバルセキュリティエキスパート株式会社
篠原　信之	グローバルセキュリティエキスパート株式会社
鈴木　靖	グローバルセキュリティエキスパート株式会社
佐藤　秀之	グローバルセキュリティエキスパート株式会社
高柳　裕之	グローバルセキュリティエキスパート株式会社
守屋　聡	サン・マイクロシステムズ株式会社
佐藤　公理	サン・マイクロシステムズ株式会社
中山　雄一	サン・マイクロシステムズ株式会社

順不同
敬称略

謝　辞

氏名	所属
大西 昇	ソリトンシステムズ
目黒　学	ソリトンシステムズ
小林　智恵子	東芝ソリューション株式会社
丹羽　奈津子	日本IBM株式会社
竹日　正弘	日本IBM株式会社
南郷理恵子	日本IBM株式会社
山本　扇治	日本アイ・ビー・エム　システムズ・エンジニアリング株式会社
酒井　美香	日本アイ・ビー・エム　システムズ・エンジニアリング株式会社
北野　晴人	日本オラクル株式会社
澤井　真二	日本オラクル株式会社
大鐘　博子	株式会社日本システムディベロップメント
小坂　嘉誉	日本CA
兼岡　禎朗	日本CA
星野　敏彦	日本ヒューレット・パッカード株式会社
大竹　章裕	株式会社ネットマークス
高木　経夫	株式会社ネットマークス
笈川 光浩	株式会社日立製作所 システム開発研究所
富山　朋哉	株式会社日立製作所 システム開発研究所
恵美　玲央奈	株式会社富士通ソーシアルサイエンスラボラトリ
今堀　秀史	富士通関西中部ネットテック株式会社
原田　篤史	三菱電機(株)情報技術総合研究所

順不同
敬称略