特権ユーザ管理とは
～ 登場の背景と求められる機能

2012/2/1

日本CA株式会社
楠木秀明（CISSP/CISA）

we can

ca technologies

本日、特権IDのお話をさせて頂く背景

カンターラの活動が貢献し、きっと素晴らしい仕組み(システム)が世の中に出現し、いつか私自身も、一人のユーザとしてその仕組みを利用し恩恵をうける日がくると思っています。

ただシステムを利用する立場からみると「当たり前」と思っている事、例えばシステムは常に使用でき、情報は保護され「安心・安全」が保障されているに違いないと、何の疑いもなく信じています。

しかしシステムを利用させる人達が不正を行った場合、「当たり前」ではなくなります。よってシステムを利用させる人達に不正・ミスがないことを予防・発見するコントロールが整備され、初めて「当たり前」の状態になると考えています。

弊社は、この「当たり前」の状態を実現するためには、特権ユーザ管理は必須と考えておりますので、本日は少しお時間をいただきお話させて頂きます。

目次

①特権ユーザ管理とは

②登場の背景

③求められる機能・コントロール

④今後の特権ユーザ管理

①特権ユーザ管理とは

特権ユーザとは？
特権ユーザと対比されるユーザとの比較

特権ユーザ	利用させる	・ユーザ数、役割の数は少ない ・ユーザー一人当たりの権限が大きく、リスクも大きい ・ユーザの入れ替わり頻度はそれほど高くない ・OSやDBレベルでの利用が多い（例外処理） ・特権IDを使用する 例：運用者/管理者/開発者がroot、DBAで作業
非特権ユーザ（一般ユーザ）	利用する	・ユーザ数、役割の数が多い ・ユーザー一人当たりの権限は小さく、リスクも小さい ・ユーザーの入れ替わり頻度が高い ・Web、C/S等のアプリでの利用（定型処理） ・特権IDは使用しない

特権ユーザとは？
特権IDと、悪用した場合のリスク

特権IDとは

スーパーユーザとも言われるオペレーティングシステムやデータベースにおいて特殊な操作ができるシステムアカウント。

例： UNIX系のroot 、 WindowsのAdministrator
データベースのDBA

リスク

不正プログラム・ログの改ざん
個人情報等のデータの閲覧・持出し
不要IDの作成、権限変更
サービスの起動・停止

特権ユーザ管理とは？

定義

システムを利用させる運用者・管理者・開発者等の担当者が、特権IDを使用し行う一連の作業をコントロールし、不正・ミスから顕在化するリスクを低減すること。

システムを利用する人が思っている以下のような「当たり前」の事を、
- ・不正プログラム・ログの改ざん
- ・個人情報等のデータの閲覧・持出し
- ・不要IDの作成、権限変更
- ・サービスの起動・停止

実施する事、証明できる事　といえるかもしれません。

②登場の背景

特権ユーザ管理が必要とされる背景

背景というものは無いのかもしれません。

コンピュータが世に登場して以来、常に必要とされた管理です。

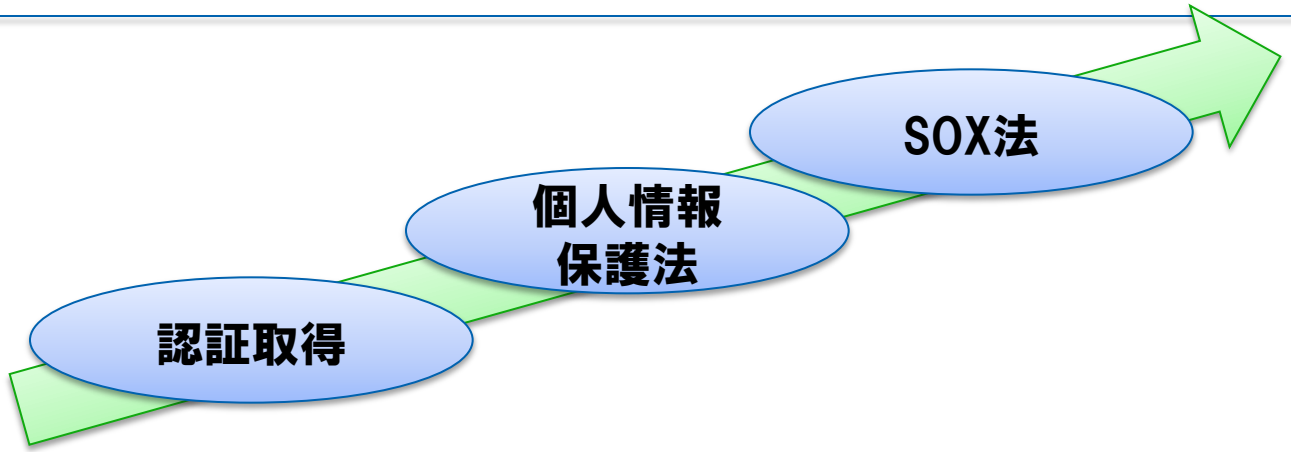
現在よりも、むしろメインフレームのような大型機全盛の時代のほうが特権ユーザ管理は、実施されていたように思われます。

90年代後半の分散系のシステムが主流になってから、特権ユーザ管理の実施が非常に困難になり、2000年以降課題とされる企業が増加したと感じています。

特権ユーザ管理がニーズが増した要因

幾つかの外的要因があったのかもしれません。

振り返えってみると
　ISMS・Pマーク等の認証取得
　個人情報保護法
　SOX法
といったタイミングで、多くの企業で特権ユーザ管理を再考されたように感じています。



SOX法での指摘事項 Top10

10項目のうち7項目がシステムを利用させる特権ユーザの不正・ミスにより顕在化するリスクが指摘されている。

1	識別されていない、もしくは、解決されない権限の分離の問題
2	財務システムが稼動するOS(UNIX等)のアクセス制御
3	財務システムに利用されるデータベースが保護されていない
4	開発スタッフが本番環境の業務トランザクションを実行可能
5	多数のユーザが本番環境の管理者ID(スーパーユーザ)を利用可能な状態
6	退職者、過去の外注社員がシステムにアクセス可能
7	財務アプリケーションにおけるデータ入力期間の制限
8	カスタム開発プログラム、テーブル、インターフェース等が保護されていない
9	手作業のプロセスの手続きが定義されていない、もしくは、定義に従っていない
10	システム文書が実際のシステムと食い違っている

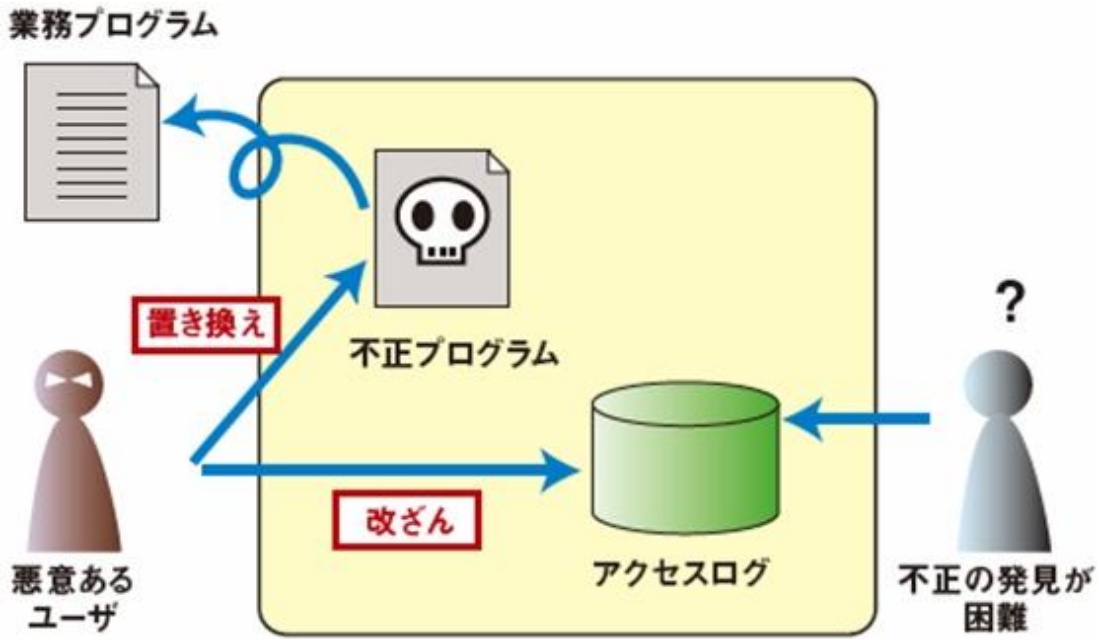
＊ Ken Vander Wal, National Quality Leader, E&Y ISACA Sarbanes Conference, 4/6/04

典型的な監査ポイント

特定のユーザに権限が集中している場合、不正が起こりやすくなる！

特定の個人へ権限の集中し、不正につながる例

架空口座に1円未満の端数を入金するように財務関連のプログラムを修正し、
本番プログラムを置換し、その痕跡が残らぬように履歴を改ざん



特権ユーザ管理を実施していなければ不正がなかった事を証明するのは困難

③求められる機能・コントロール

求められるコントロール

①不正・ミスの影響を低減する為に、管理不備IDを最適化
②不正・ミスを発見する為に、4W1H(Why以外)を特定
③不正・ミスか否かを判断する為に、作業計画(Why)と妥当性確認
④不正・ミスを予防する為に、不要な作業を制御

誰が	担当者と使用されているID
いつ	日付、時間は？
どこで	アクセス経路は？直接ログイン？リモートアクセス？
何を	プログラムやログ以外に、他に不正をしていないか？
どのように	改ざん？閲覧(漏えいの可能性有)？など
なぜ	組織が認めている必要な作業か？それ以外は不正の可能性有。

→ 管理不備ID群(共有ID、残存ID、承認不備ID、高権限ID、パスワード不備)排除

発見 → 4W1Hをアクセスログから発見

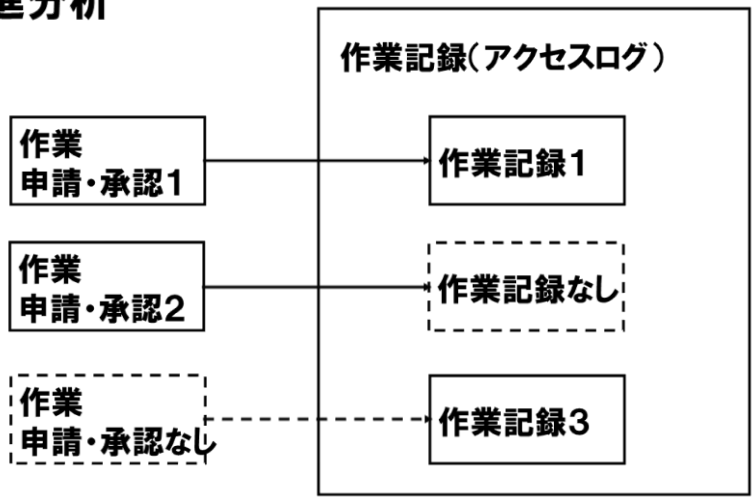
予防 → 4W1Hを限定するアクセス制御で予防

→ ログの中には存在しない。よって担当者自身が計画し、第三者により妥当性(承認)を確認する。

求められるコントロール
2方向での監査・モニタリングが実施できれば良い

順進分析:「作業申請・承認」から「作業記録(アクセスログ)」を確認する(作業準拠性)
逆進分析:「作業記録(アクセスログ)」から「作業申請・承認」を確認する(不正の検知)

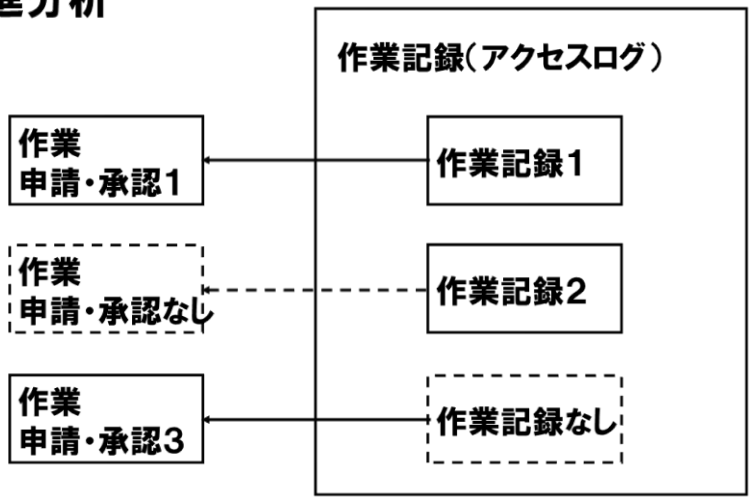
順進分析



「作業申請・承認」から「作業記録(アクセスログ)」を照合
- 記録漏れの「作業申請・承認2」は発見され、記録漏れが発見可能
- 申請・承認を迂回した「作業記録3」は発見されず、「作業記録3」に申請・承認がないことが発見できない

→ 順進では、申請・承認を迂回した不正を検知できない場合がある

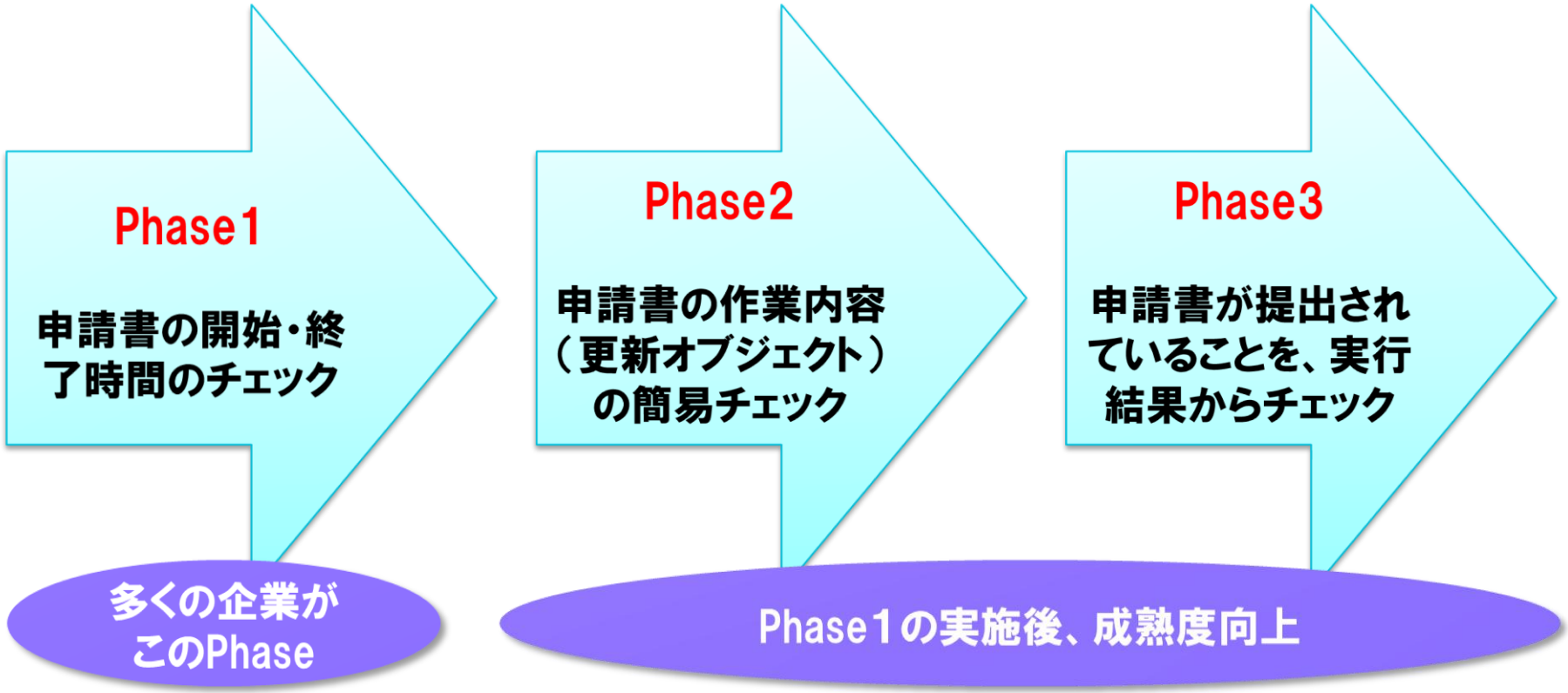
逆進分析



「作業記録(アクセスログ)から「作業申請・承認」を照合
- 申請・承認を迂回した「作業記録2」はサンプルされ、迂回の不正が発見可能
- 記録漏れの「作業申請・承認3」はサンプルされず、記録漏れであることに気づかない

→ 逆進では、記録漏れが確認できない場合がある

突合条件における3つのPhase



監査証跡
開始（logon）
：
操作内容
：
終了（logoff）

各Phaseのご説明
～Phase1：申請書の開始・終了チェック

Phase1

「申請書の開始・終了時間のチェック」

申請書に記載されているサーバで担当者が、予定の開始・終了時間外に作業をしていない事の確認する。

申請書イメージ

突合対象項目	***その他申請項目例***
開始日/開始時間	利用目的
終了日/終了時間	作業内容
サーバ名	承認者　　etc
ユーザID	

各Phaseのご説明
～Phase2：申請書の作業内容チェック

Phase2

申請書の作業内容（更新オブジェクト）の簡易チェック

Phase1に加え、申請書に記載されている更新オブジェクト（データ、プログラム、DBの表等）への作業（アクセス）を確認する
→ 注）更新オブジェクトは代表的なもののみ記載。全ての更新オブジェクトを申請書に記載させるのは困難である。例えば、パッチ適用時は更新オブジェクト多数かつベンダー等への情報収集作業の工数がかかる。よって予定された更新オブジェクト以外にアクセスしていないか否かをチェックすることは、多くの企業で未実施である

申請書イメージ

突合対象項目	***その他申請項目例***
開始日/開始時間	利用目的
終了日/終了時間	作業内容
サーバ名	承認者　　etc
ユーザID	
リソース名（データ名、DBの表名等）	

各Phaseのご説明
～Phase3：申請書の提出を実行結果からチェック

Phase3

申請書が提出されていることを実行結果からチェック

Phase1・2に加え、申請書が未提出の作業がないか否かを、実行結果をもとにチェック。企業毎にリスクが存在する可能性があるアクセス経路を特定し、その経路の実行結果が存在すれば申請内容の存在有無をチェックする
→ 注）実行結果には、正常な業務処理のログとメンテナンス等の人間系のログが混在。通常、モニタリングは人間系のログに絞りこみモニタリングを実施するので、人間系のログが何であるかを定義する事が本Phaseでは必須

※申請書内容はPhase2と同様だが、チェック方法が逆進となる
（Phase1・2は順進）

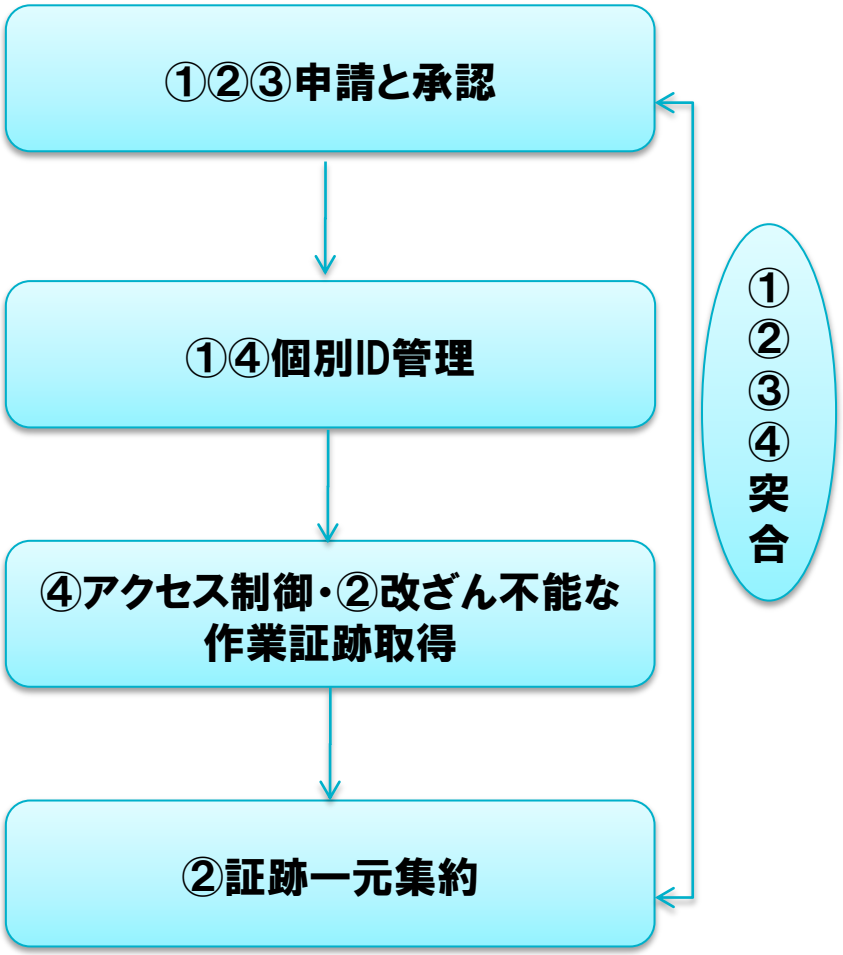
求められるコントロールと機能

①不正・ミスの影響を低減する為に、管理不備IDをコントロール

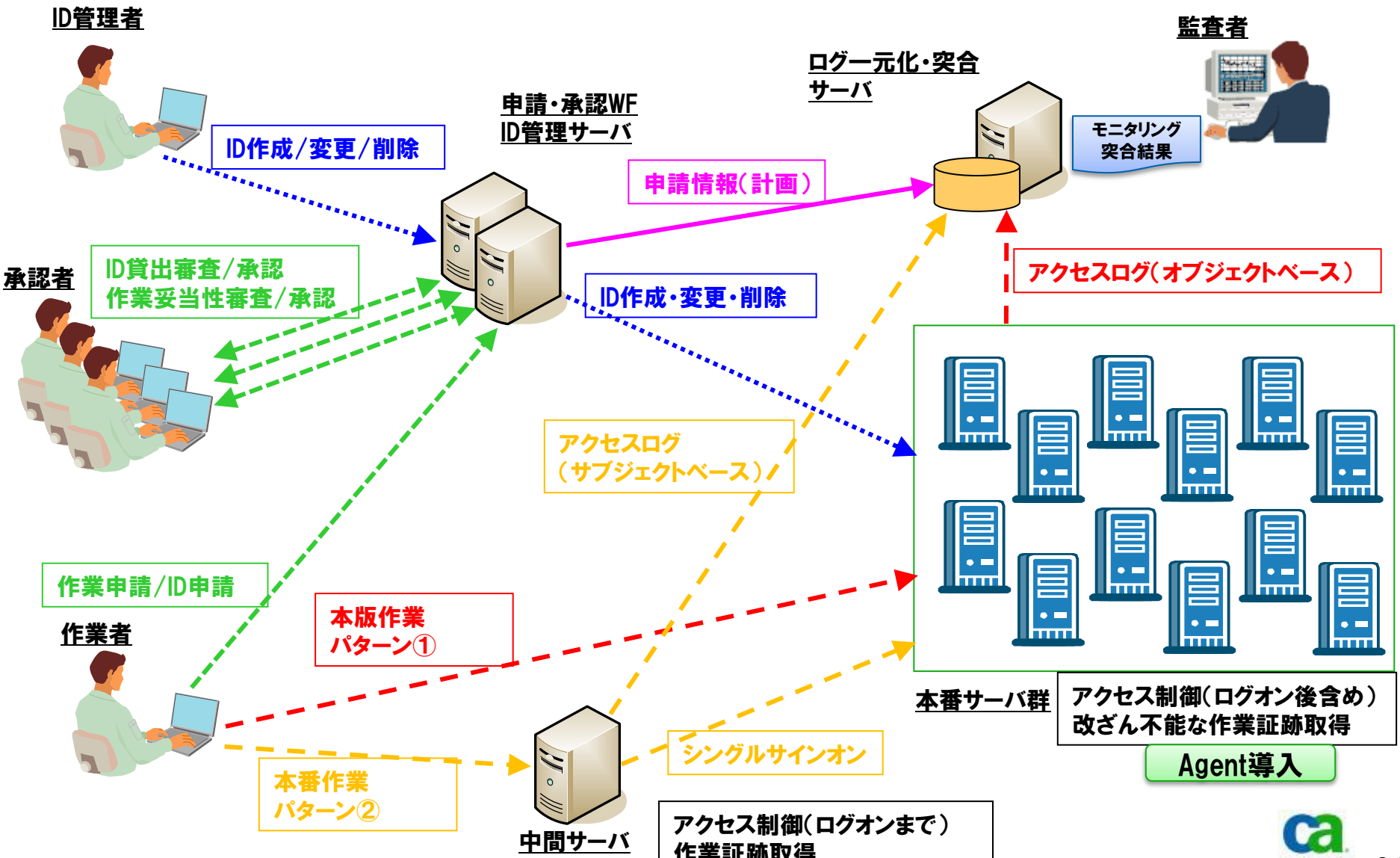
②不正・ミスを発見する為に、4W1H（Why以外）を特定するコントロール

③不正・ミスか否かを判断する為に、作業計画（Why）と妥当性確認

④不正・ミスを予防する為に、不要な作業を制御するコントロール



求められるコントロールと機能のシステムイメージ



アクセス制御・ログ収集は2タイプ必要
中間サーバ(ゲートウェイ)経由と、直接ログインの2経路

経路	説明	システムランク	メリット	デメリット
中間サーバ経由	ゲートウェイサーバを設置し、そのサーバを経由した後、各業務サーバにアクセス 。 ゲートウェイサーバ上で操作を記録するサブジェクト(ユーザ)主体のログになる。	全て 例重要度A,B,C	①構築期間が台数に依存しない ②業務サーバに対する変更がない	①ネットワーク構成の変更が発生する可能性が有る ②各業務サーバに直接ログインした場合のログが取得できない ③オブジェクト(ログ、プログラム等)改ざん検知/予防ができない ④バッチ等の内部処理に関するログ収集ができない
直接ログイン	各業務サーバ毎にログインしアクセス。 各業務サーバ毎で操作を記録するオブジェクト(リソース)主体のログになる。	一部のみ 例:重要度高のAランクのみ	①ネットワーク構成の変更が発生する可能性は無い ②各業務サーバに直接ログインした場合のログも取得できる ③オブジェクト(ログ、プログラム等)改ざん検知/予防ができる ④バッチ等の内部処理に関するログも収集可能	①構築期間が台数に依存する ②業務サーバに対してモジュールを導入する必要がある

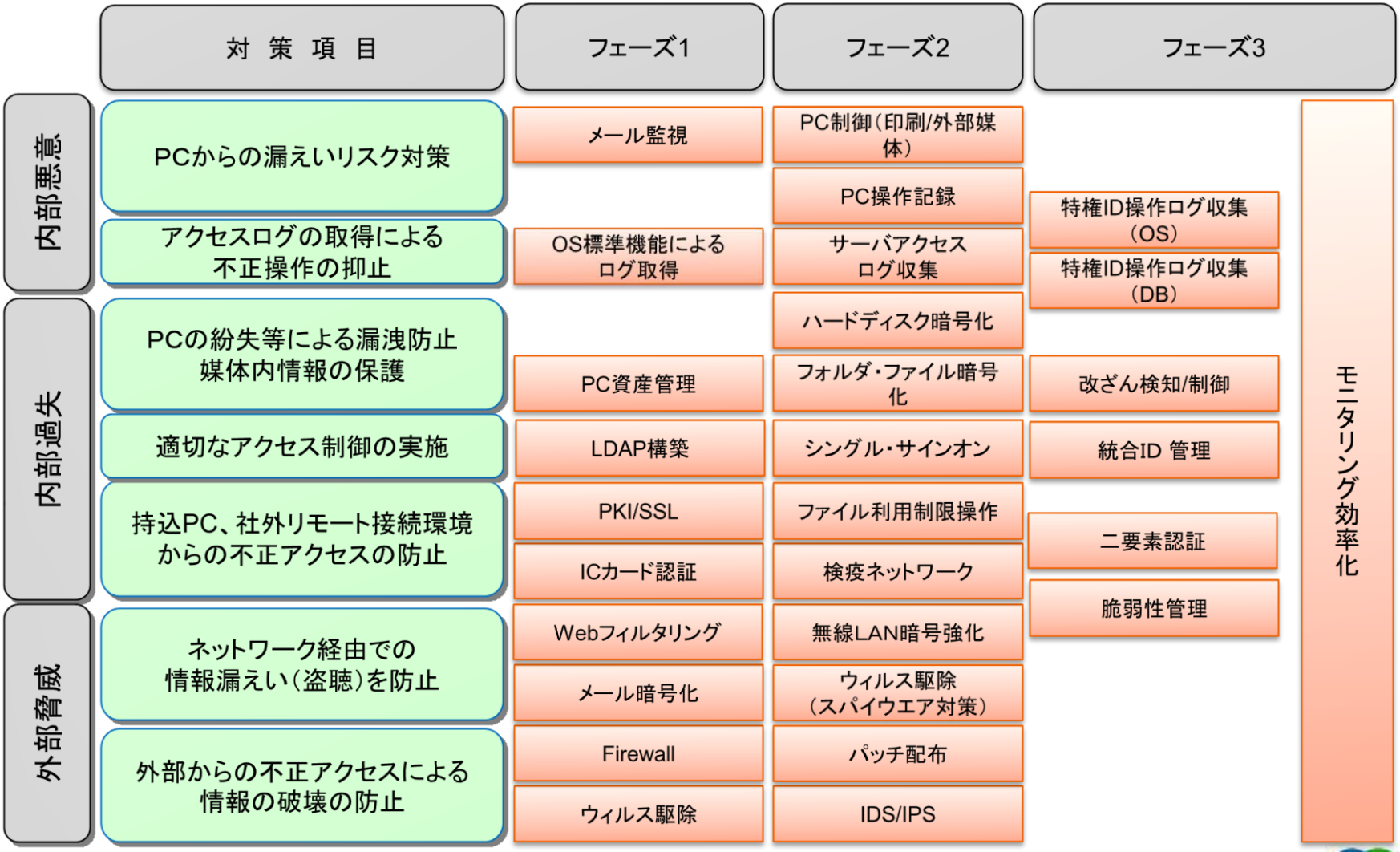
直接ログイン
(重要システムのみ)

中間サーバ経由
(全システムが対象)

システムランクに応じて併用する事が望ましい

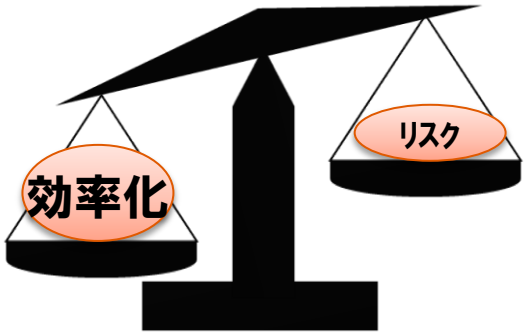
④今後の特権ユーザ管理

リスクコントロールの拡張例



特権ユーザ管理の今後

昨今の時代背景を考えた場合、効率化を考慮した特権ユーザ管理を計画しなければ、経営層の賛同は…



今後の傾向

①手動作業の効率化

1. ID管理・共有ID貸出の業務を手動から自動化し工数を削減
   - 紙ベースの申請業務
   - ユーザID作成/変更/削除、パスワード変更
   - 共有ID払出し業務
   - ID棚卸

2. モニタリングを人海戦術で実施する部門の工数削減
   - 計画(作業申請)と、結果(ログ)の突合の簡素化
   - 専任のモニタリング部門の人員/工数削減

②環境変化への追従

3. リモートアクセス時の本人確認強化
オフショア、クラウド化、システム依存度の増加等が進むにつれ、以前まではリモートアクセスを認めていなかった場面でも、リモートアクセスを実施しなければならない環境が増加。
従来型のID/paswordでの本人認証は、安全とは言い難いため二要素認証(持っている)を検討。
IDと人の結びつけを強固にする傾向。

さいごに
特権ユーザ管理の定義変更する時期と考えています。

定義

システムを利用させる運用者・管理者・開発者等の担当者が、特権IDを使用し行う一連の**作業をコントロールし、不正・ミスから顕在化するリスクを低減すること。**

システムを利用させる運用者・管理者・開発者等の担当者が、特権IDを使用し行う一連の**作業全般を標準化・自動化することで効率化する。その副次的効果としてリスク低減も可能となる。**


technologies