

内部統制に必要なアイデンティティ管理 (特権ID) について

CSLGuard

&

ActCenter

2009年5月13日

NTTソフトウェア株式会社

Security

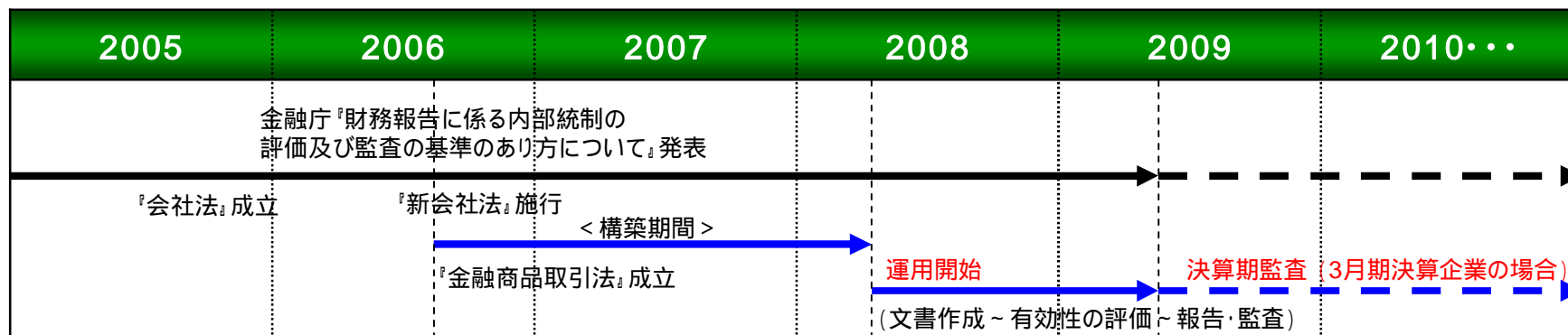
Human

Mobile

内部統制対応の現状

内部統制対応の現状

内部統制に関するこれまでの動き
 ~ 2008年4月からはじまる会計基準より適用 ~



見えてきた内部統制対応の現状(例)

- ・『統制環境や整備上の不備』
 組織構造、権限と責任、ドキュメント化の整理、人的資源などの管理が不十分
- ・『運用上の不備』
 整備段階で意図した内部統制が運用されていない、運用上の誤りが多い
 社内への浸透度が不十分、実施担当者が統制内容や目的を正しく理解していない
- ・『IT統制(日本版SOX法で義務付け)の理解不足』
 一時的な予防処置としてITが導入されている



社内でのプロセス理解、過剰な投資や運用負荷を抑えた適切なIT統制環境の構築

適切なIT統制環境構築に向けて

ITの利用/IT統制

個々の業務プロセス、個別の対象システムの個別のリスクに応じた対策が重要

ITに対する統制活動

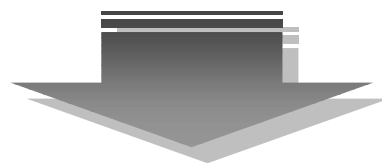
業務処理統制

- ・業務処理システムデータの正確性、網羅性
- ・マスターデータの維持管理
- ・システムの利用に関する認証
- ・操作範囲の限定などアクセス管理

全般統制

- ・システムの開発、保守に係る管理
- ・システムの運用・管理
- ・内外のアクセス管理、システムの安全性確保
- ・外部委託の契約管理

金融庁：『財務報告に係る内部統制の評価及び監査に関する実施基準』より



情報システムや企業秘密情報への厳密なアクセス管理の基になるID情報、
全ての権限を持つID(特権ID)の管理を統合し、厳密化することが重要となります！

内部統制/IT統制の有効な手段として…



ID管理/特権ID管理、ユーザ認証/アクセス制御、監査ログ取得

Security

Human

Mobile

内部統制/IT統制におけるアイデンティティ管理 「特権ID管理のニーズ」とその対応策

特権IDとIT統制

特権IDとは

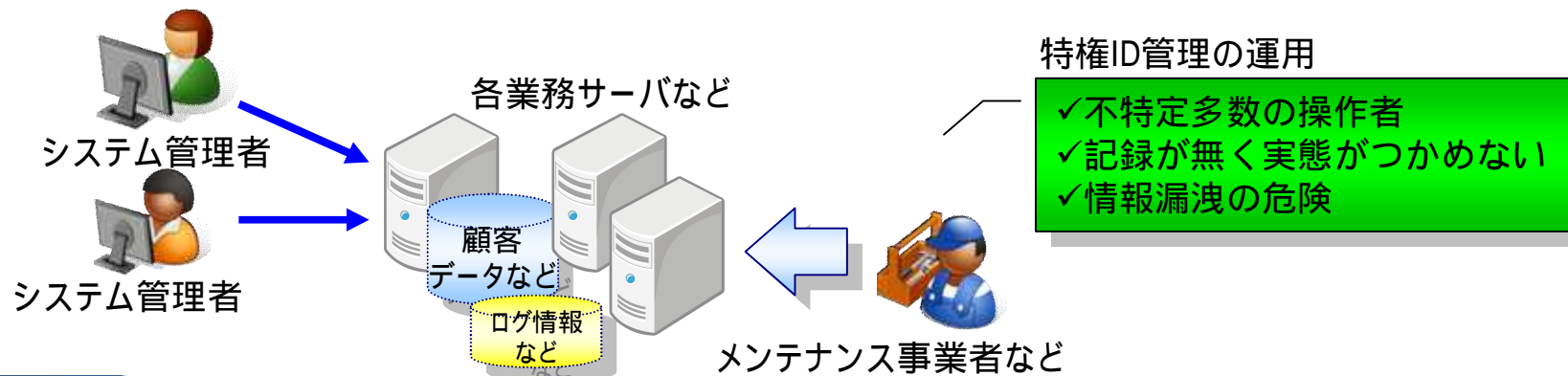
情報システムのメンテナンス(業務アプリケーションの入れ替え、OSのパッチ作業など)に用いるルート権限や、アドミニストレータ権限など特別なユーザ権限のID/パスワードのこと。

特権IDを取り巻く様々なリスク

- ・サーバ数が増え、管理が行き届いていない
- ・システム個別に管理者が存在し、全体の管理が見渡せない状況になっている
 - ・手作業による運用で、管理漏れが生じている
 - ・棚卸しをしても、どれがあるべき姿なのかわからない



システムを守る上で一番重要な**特権ユーザID(特権ID)**の管理が重要 IT統制の始まり



特権IDの管理

特権ID管理とは

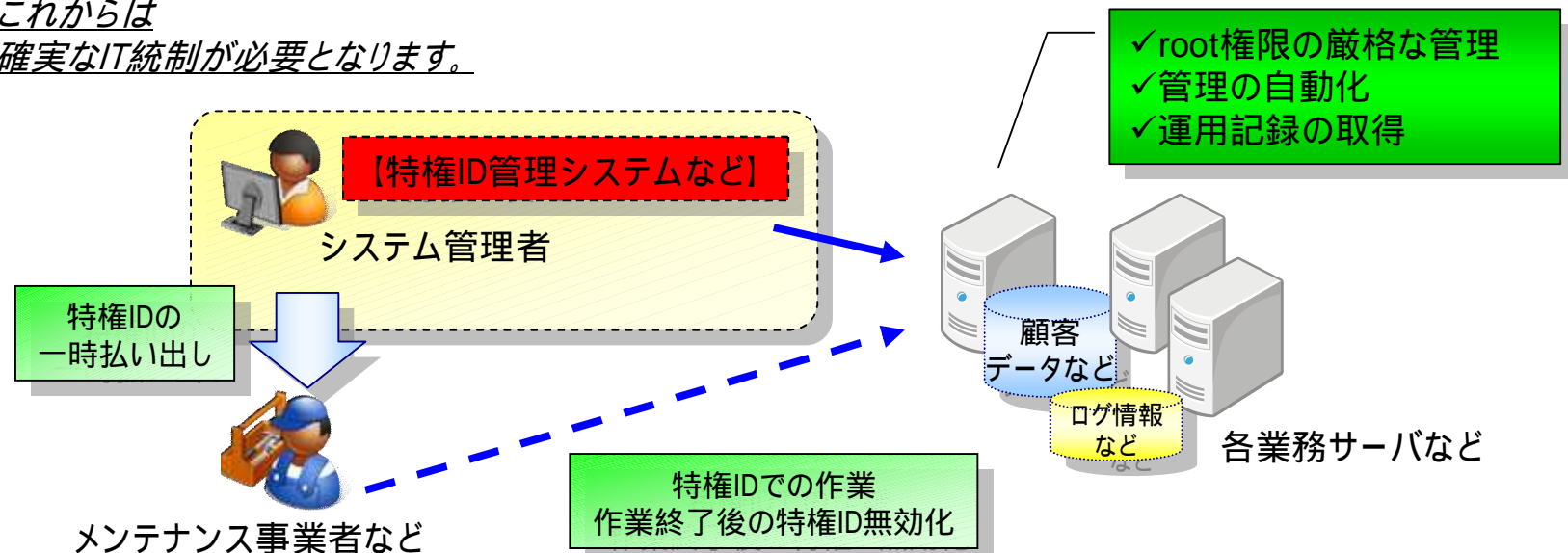
特権IDの払い出し、消滅の管理

特権IDのアクセス記録

具体的には…

- ・ **必要な日/時間のみ**払い出しを行う
- ・ 一時的に払い出しの特権IDは、作業終了時(ログオフ時など)、**自動的に無効化**させる
 - ・ 強制的な**パスワードの自動変更**、**自動的なIDの削除**
- ・ 払い出しの記録や、**アクセスログの記録**を取得
- ・ 業務サーバ上のアカウントと管理IDの**差分チェック**、**棚卸し(監査)**を実施

これからは
確実なIT統制が必要となります。



特権IDを管理するための課題

個人情報や機密情報管理など、内部統制やセキュリティ対策への取り組みは重要。
その中でも様々な情報にアクセス可能な**特権IDのアクセス管理**は特に重要事項です！

できることの非常に多い特権IDは、ID払い出しの期間設定、払い出し状況の把握、パスワード変更の徹底、**ログ収集等**が求められます。

開発者・メンテナンス者の特権ID管理に関する課題

サーバ数が多い(数十台～数百台のサーバ群)ための課題

課題-1) 全社ポリシーの徹底が難しい

払い出すIDの徹底した管理を行いたい

(大元のIDは貸与しない、パスワードの長さや、ロック条件も統一したい)

課題-2) 貸出期間の徹底とパスワード変更が困難

期限切れIDの利用停止を徹底したい

定期的にパスワード変更したい、貸し出し後のパスワードを即座に変更したい。

課題-3) 作業の軽減を図りたい

管理しているIDの棚卸しチェックを簡易化したい

収集したアクセスログの検証事務を軽減したい

特権IDを管理するための対策

開発者・メンテナンス者の特権ID管理に関する課題

課題-1) 全社ポリシーの徹底が難しい

課題-2) 貸出期間の徹底とパスワード変更が困難

課題-3) 作業の軽減を図りたい



解決策

解決-1) 全サーバの特権ID集中管理と運用

スケジュールに従った自動払い出し
払い出すIDのセキュリティルールを統一
実IDを直接参照させずに仮IDとひも付け
管理端末より全特権IDの照会

解決-2) 払い出し後の特権ID自動運用

貸出期間を過ぎた特権IDの自動停止
ログオフ時のパスワード自動変更、動的なパスワードの自動変更

解決-3) 作業の軽減

サーバの実IDと管理IDの差分チェック
差分がある場合の、不要IDの自動削除
全システムのアクセスログを取得とログ分析ツールに転送(ログ集約管理)

アイデンティティ管理における、特権ID管理～まとめ～

特権ID管理とは

特権IDの払い出し、消滅の管理

特権IDのアクセス記録

必要な日/時間のみ、作業終了時の無効化、強制的なパスワード自動変更、自動的なID削除
払い出し、アクセスの記録、業務サーバ上のアカウントと管理IDの差分チェック、棚卸し(監査) など

特権ID管理における課題と解決策

課題

課題 - 1) 全社ポリシーの徹底が難しい
課題 - 2) 貸出期間の徹底とパスワード変更が困難
課題 - 3) 作業の軽減を図りたい

解決策

解決 - 1) 全サーバの特権ID集中管理と運用
解決 - 2) 払い出し後の特権ID自動運用
解決 - 3) 作業の軽減

セキュリティリスクを抑止し、統制の取れたシステム環境の構築が必要です！

NTTソフトウェアの「アイデンティティ管理ソリューション」
が解決いたします！

Security

Human

Mobile

NTTソフトウェアにおける 「アイデンティティ管理ソリューション」

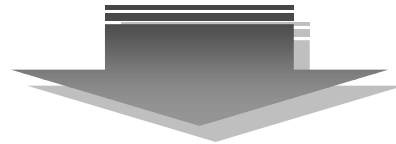
NTTソフトウェアの「アイデンティティ管理ソリューション」

開発者・メンテナンス者の特権ID管理に関する課題

課題-1) 全社ポリシーの徹底が難しい

課題-2) 貸出期間の徹底とパスワード変更が困難

課題-3) 作業の軽減を図りたい



< NTTソフトウェアのアイデンティティ管理ソリューション >

CSL Guard

コンソールガード

クライアント/サーバ系、Web系
システムへのシングルサインオン

アクセス制御

不正アクセス防止・検出、
ログ監査

 **NTTソフトウェア**

ActCenter

アクトセンター

特権ID管理

監査ログ取得
運用者ログ監査

不正アカウントチェック

効率的な
スケジュール管理

アイデンティティ管理ソリューションの特長

▶ 特権ID管理ビジネスへの取り組み

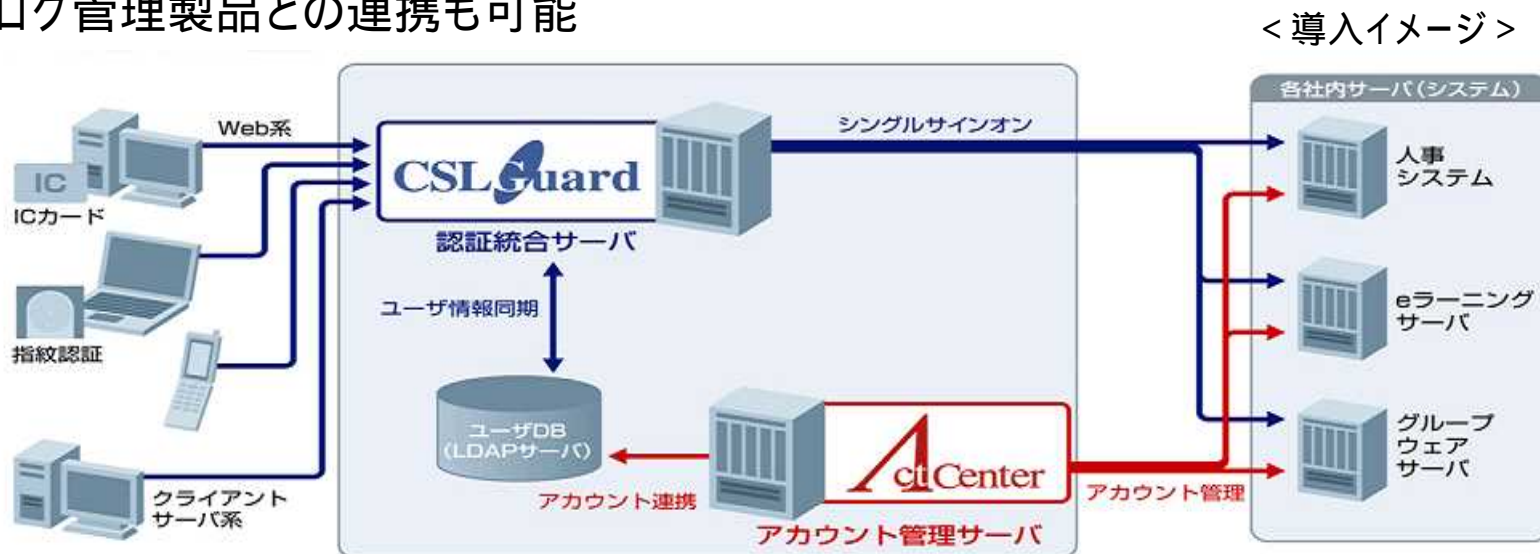
- ◆ 1998年からの長年にわたる数多くの実績
- ◆ 自社開発製品による製品改善要求の対応(カスタマイズ実績多数)

▶ シングルサインオン、アクセス制御、アカウント管理を一社でトータルに提供

- ◆ CSLGuardとACTCenterの連携が容易(シングルサインオンとアカウント管理の連携)
- ◆ 運用者向け管理機能が充実
- ◆ クライアントサーバ系アプリケーション、Web系アプリケーションへの対応

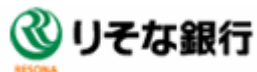
▶ 監査ログ一元取得

- ◆ ユーザ認証, SSO履歴, セキュリティ情報更新などの作業履歴を一括管理
- ◆ 他社ログ管理製品との連携も可能



導入事例

■ お客様: リそな銀行様



■ 導入時期: 2002年～

■ システム規模: サーバ (2,000台程度)

■ ユーザ: 100名

■ 導入期間: 8ヶ月程度

■ 利用パッケージソフト: CSLGuard

< 導入イメージ >



ベンダ作業員の作業終了後に作業用パスワードはランダムに変更される

【課題】

- ・UNIX、Windowsなどオープン系システムのセキュリティ強化、運用管理者のID管理工数削減 など
- ・運用管理者、社内外のメンテナンス者、AP開発担当者など、アクセスするタイミングや使用時間もバラバラ
- ・管理者・開発者の運用管理者のアイデンティティ管理、特に、特権IDのきめきめ細かい管理が課題となっていた

【解決へのアプローチ】

- ・膨大な管理工数を削減するためのID管理システム導入 (お客様要望に応じて開発)
- ・特権IDのきめ細かい管理 (作業終了後の自動無効化、PWの定期自動変更、アクセス時間の管理など)

【ソリューションとその成果】

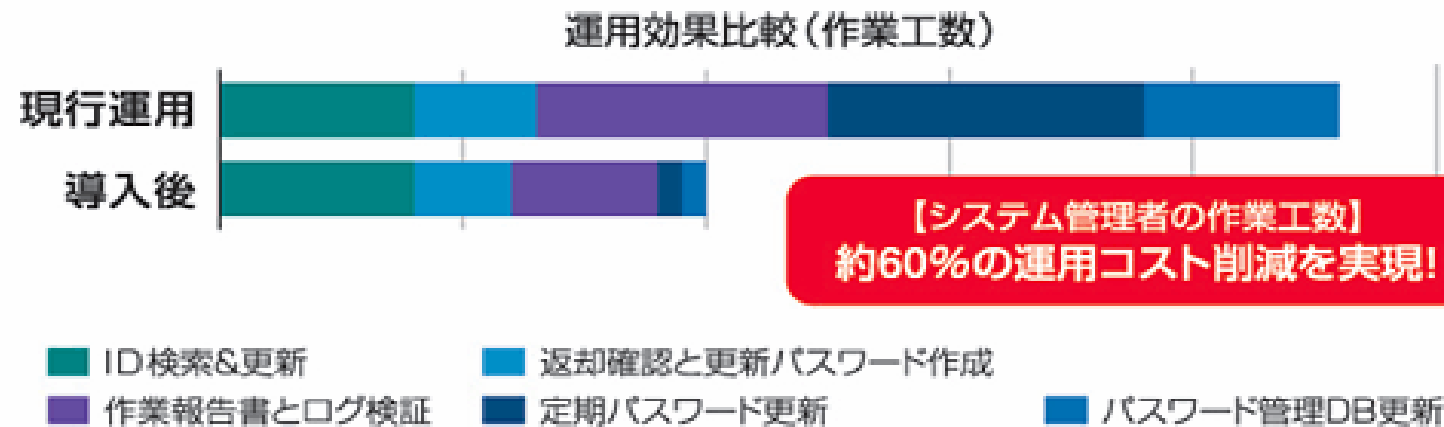
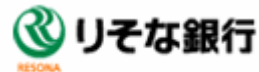
- ・金融業界のシステム運用管理者の運用ノウハウを機能として実現 (地方銀行など金融業界向けの内部統制強化)
- ・運用管理者のID管理工数大幅削減

導入事例

特権ID管理システムの導入効果

管理者のID管理工数を約60%削減！

導入効果



- 1,000台以上のサーバを運用している都市銀行で、運用管理者のアイデンティティ管理だけで23人/月の工数がかかっていたものが、このソリューションを導入した結果、半分以下の10人/月に削減された。
- 工数削減のポイントは、定期パスワード更新の工数がほぼゼロになったことなどであり、デリバリチャネルの多様化で生じてくる問題をちょうど解決できる点にも注目したい。

導入事例

■ お客様: 沖縄銀行様



■ 導入時期: 2004年～

■ システム規模: 100システム以上

■ ユーザ: 約1,500人(パート従業員分も含む)

■ 導入期間: 約6ヶ月間

■ 利用パッケージソフト: CSLGuard

【課題】

- ・個人情報保護対策
- ・共有端末 / 共有ID利用におけるセキュリティ確保
- ・各業務APごとにパスワードポリシーが異なっている
- ・各業務APのアカウント管理運用コストが膨大

【解決へのアプローチ】

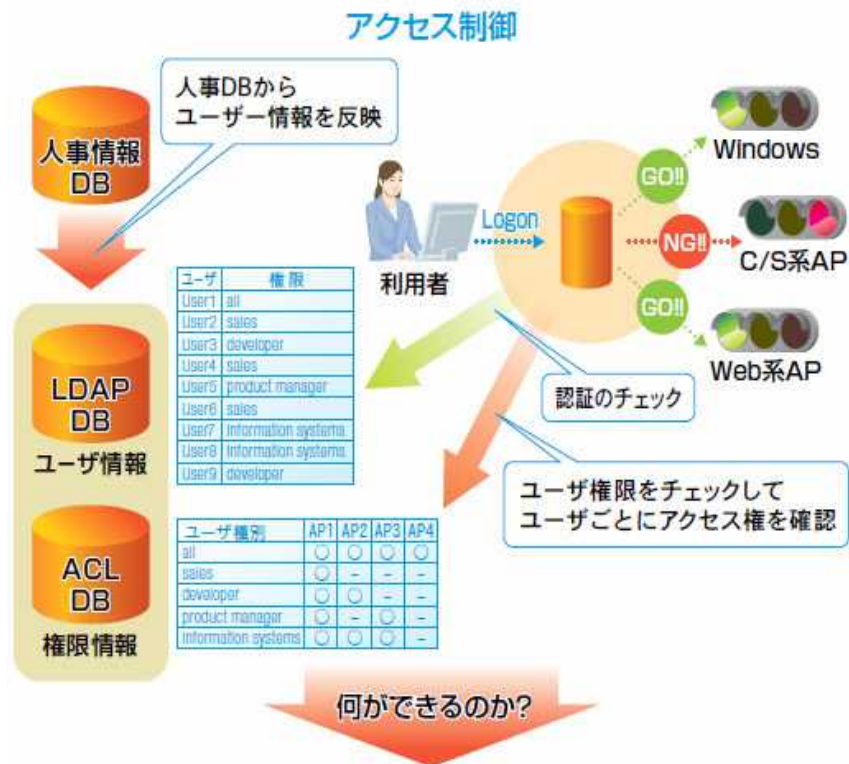
- ・C/S系、Web系の両システムへの対応
- ・お客様独自開発APとの連携(API利用)
- ・CSLGuardを核とした個人認証システムを構築

【ソリューションとその成果】

- ・既存Webシステムと共用できる仕組みに統合化
- ・業務アプリケーションの起動制御は認証基盤と連携 など

< 導入イメージ >

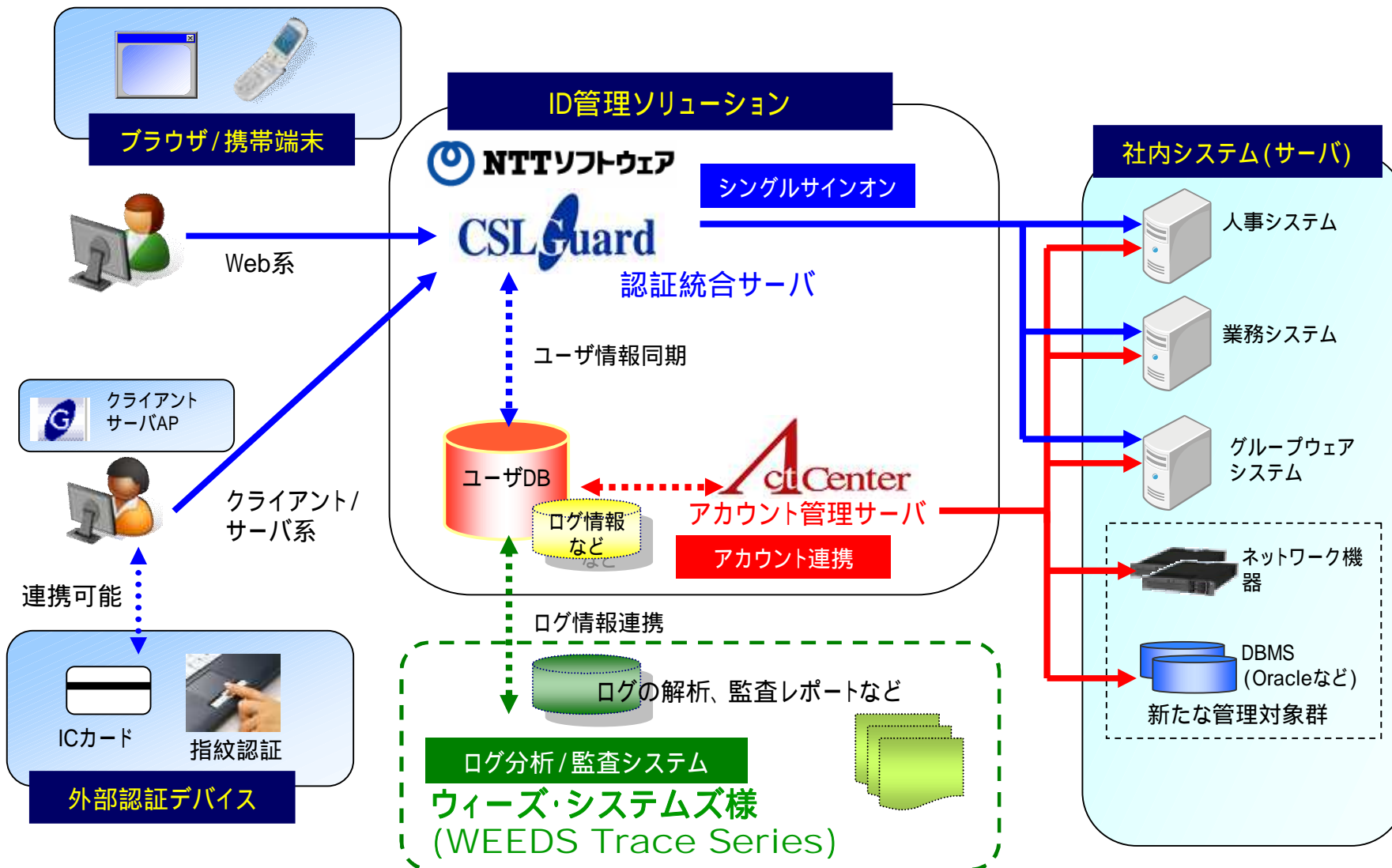
沖縄銀行が導入したソリューション



- ◆ アクセス制御 (URLディレクトリ単位/アプリケーション単位/属性にて権限振り分け)
- ◆ アプリケーションへの情報引継ぎ
- ◆ 監査ログの一元化

ウィーズ・システムズ様製品との連携

ウィーズ・システムズ様製品との連携(イメージ)



最後に

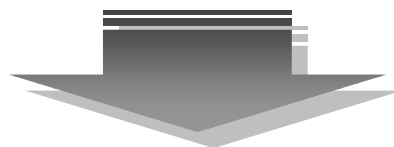
内部統制が義務化され、情報セキュリティは、ビジネスから切り離せなくなってきました。

ID管理 / 特権ID管理

ユーザー認証、アクセス制御


監査ログ取得

これらはITを有効活用した内部統制を実現する有効な手段となります。



NTTソフトウェアでは、部分的な対応ではなく、様々な製品 / ソリューションやサービスを組み合わせることで、お客様における内部統制対策をご支援を致します。

【お問合せ先】

NTTソフトウェア株式会社  **NTTソフトウェア**
営業推進本部
第二営業部 ソリューション営業部門 中山・長野・谷口
〒108-8202
東京都港区港南2-16-2 太陽生命品川ビル27階
TEL : 03-5782-7261 FAX : 03-5782-7221
mail : tssol@cs.ntts.co.jp http://www.ntts.co.jp

参考資料

【参考】NTTソフトウェアが選ばれる理由

豊富な導入実績

メガバンク、他金融、情報・通信、大学、官公庁、製造・流通など、1998年からの長年にわたる幅広い業界と数多くの導入実績

柔軟な製品提供

自社開発の国産製品であり、サポート部門と開発部門が一体となった対応。お客様固有の業務への対応が必要な際にも、迅速にお客様のご要望にあった最小限のカスタマイズが可能。万が一の障害が発生時も、自社のサポート部門により迅速な障害解析・復旧対応が可能。

各種法令に対応

FISC安全対策基準、J-SOX法対応の実績のある製品。

また、米国版SOX法についても、メガバンクや大手金融業のお客様での対応実績あり。

最新の技術動向に対応

柔軟な拡張性・将来性。また、PKIやICカード連携など最新の技術動向に迅速に対応。

世界標準のSAML2.0 (LibertyAlliance) やOpenIDにいち早く対応するなど、先端技術に柔軟に対応できる先進性の高い製品。

【参考】主な導入実績(一例)

官公庁/金融/大学/製造・流通、情報・通信など、大小約130システム以上の導入実績

業界	主な導入先	主な導入ポイント
官公庁・公共団体	・省庁系団体・自治体など	全国システム運用者向け 職員向けPKI認証との連携
金融	・銀行、カード、保険会社など セキュリティ向上 & 運用コスト削減や次世代IT基盤整備による需要増加	金融監督庁セキュリティ対応 (FISC) SOX法対応
大学	・総合大学、専門大学など IT基盤更新および統合化による需要増加	学生サービスの向上 システム管理作業効率化
サービス業	・サービスプロバイダなど	インターネットサービス プロバイダ 利用者向け
他	・通信業、製造・流通系企業など 特に製造業・通信業の導入 需要増加	セキュリティ対策 効率化 など

【参考】NTTソフトウェアのトータルセキュリティソリューション

メールの誤送信

重要メールの漏えい

メール暗号化ソフトウェア
CipherCraft®/Mail

誤送信防止と暗号化で
安心してメールを送信

重要文書の
外部・内部漏えい

ファイル暗号化ソフトウェア
CipherCraft®/File

簡単な操作で電子ファイル
の暗号化を実現

利用者が管理するID、
パスワードの増加

アイデンティティ管理
負担の増加

CSL Guard

actCenter

TrustBind®
Federation Manager

シングルサインオン・ユーザ管理 アクセス制御 アカウント管理一覧

不正アクセス

漏えい時の調査や
監査対応

NetDetector

SAVVY / MailRetriever for NetDetector

環境を変えずに導入できる全文検索エンジン搭載のメールアーカイブシステム
通信ログの記録と監視と追跡を実現する「ネットワークの監視カメラ」