資料3-2

「ASP・SaaS向け情報セキュリティ対策に関する研究会」第3回会合資料

ASP・SaaSにおける 情報セキュリティ対策の現状と課題について

2007年10月17日

三菱電機株式会社
インフォメーションシステム事業推進本部
システム統括部　システム第一部
小倉 博行

１．Ａ市／ＣＡＴＶ通信会社様「地域情報システム」（９９年４月稼動）の事例紹介（１）

●Ａ市マルチメディアモデル整備事業（１９９８年度）

１．工事概要
　本工事では、Ａ市内のマルチメディア化・情報化を目的として、放送（CATV）、通信（LAN）、および情報（コンピュータ）を、最新の技術（ＨＦＣ：光同軸網、ＩＰ：インターネットプロトコル、WWW：ワールドワイドウェブ、等）を駆使して融合したネットワークシステム設備（放送・通信・情報融合ネットワークシステム）を構築した。

２．工事主任技術者：**電気工事主任技術者または通信工事主任技術者**（三菱電機）

３．関連法規、検査基準、および検査官

３．１　放送設備（伝送路設備含む）
（１）関連法規　：**有線テレビジョン放送法**
（２）検査基準　：**ＣＡＴＶ技術基準（電波監理局検査基準）**
（３）社内検査官：**第一級有線テレビジョン放送技術者**（ａ社／三菱電機 ）
（４）立会検査官：監督者（Ａ市）、監理者（ｂ社）

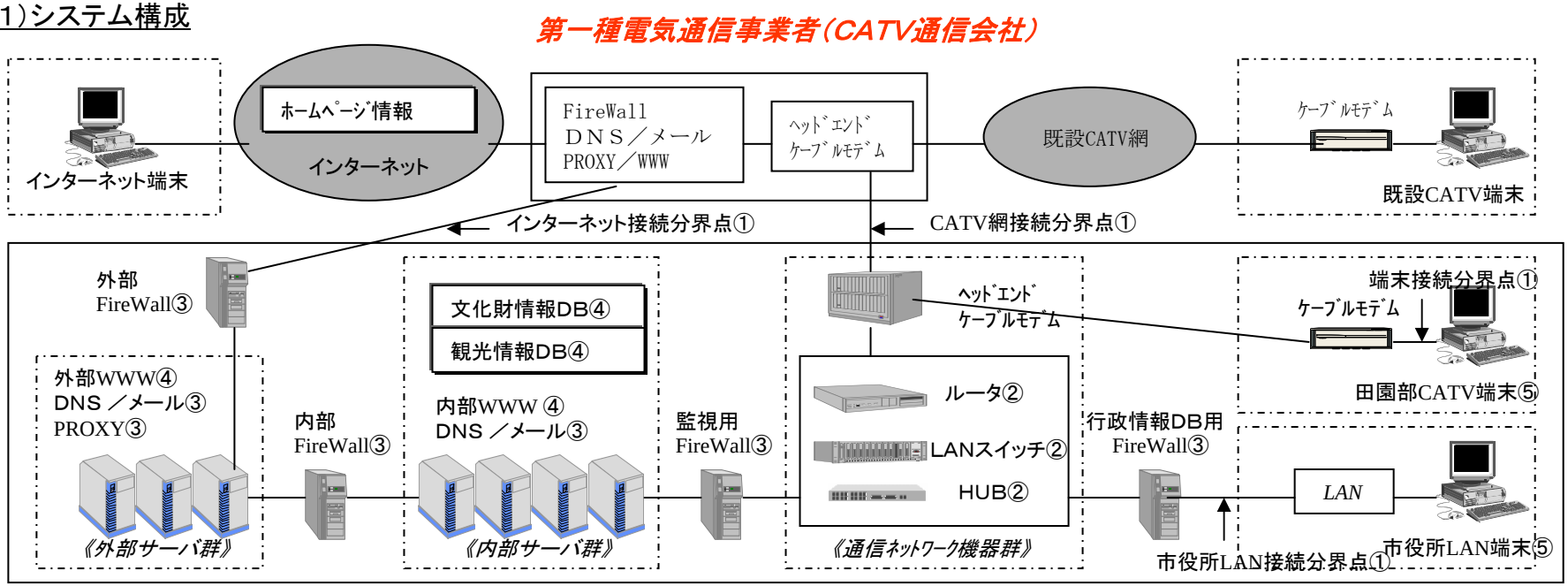
３．２　通信設備
（１）関連法規　：**電気通信事業法**
　　（第４１条 電気通信設備の維持、第４９条 端末設備の接続の技術基準）
（２）検査基準　：**郵政省令で定める技術基準（デジタルデータ伝送役務）**
（３）社内検査官：**工事担任者デジタル一種技術者**（三菱電機 ）
（４）立会検査官：監督者（Ａ市）、監理者（ｂ社）

３．３　情報設備
（１）関連法規　：情報処理の促進に関する法律、
　　セキュリティ関連法規（刑法、建築基準法、消防法、プライバシー条例、著作権法、等）、
　　監査関連法規（商法、監査特例法、証券取引法、公認会計士、等）
（２）検査基準　：通産省監修 システム監査基準（システム開発業務実施基準）
（３）社内検査官：システム監査技術者（三菱電機）
（４）立会検査官：監督者（Ａ市）、監理者（ｂ社）

1．A市／ＣＡＴＶ通信会社様「地域情報システム」（９９年４月稼動）の事例紹介（２）

●A市マルチメディアモデル整備事業（１９９８年度）

(1)システム構成



(2)機能

No	検査項目	検査内容
①	通信ネットワーク接続分界点検査	第一種電気通信事業者(100Base-T)および加入者(10Base-T)との接続分界点仕様の検査を行う。
②	通信ネットワーク機器検査	ルータ・ＬＡＮスイッチ・ＨＵＢのネットワーク機器の検査を行う。
③	ネットワークサーバ機器検査	FireWall、ＤＮＳ（ﾄﾞﾒｲﾝﾈｰﾑｻｰﾊﾞ）／メール、ＰＲＯＸＹ（代理応答）のネットワークサーバ機器の検査を行う。
④	アプリケーションサーバ機器検査	WWW（Ｗｅｂ－ＧＩＳ）、ＤＢ（データベース）のアプリケーションサーバ機器の検査を行う。
⑤	アプリケーションシステム動作確認	文化財情報ＤＢと観光情報ＤＢのWWW閲覧を行い、検索画面表示、地図画面表示、個別画面表示、外字表示、画像表示、および動画表示の動作確認を行う。
⑥	通信ネットワークシステム動作確認	ＣＡＴＶ端末とＬＡＮ端末からそれぞれ、参照経路（ルーティング）、ＤＮＳ参照、メールサービス、およびWWWサービス（内部、外部）の動作確認を行う。

１．Ａ市／ＣＡＴＶ通信会社様「地域情報システム」（９９年４月稼動）の事例研究

【構成員意見】

●現行の法令、仕様（認証基準）、実践のための規範（ベストプラクティス）、ガイドブック、関連・参照可能な基準、ガイドライン、、、色々な項目多すぎ、重複や抜けがあり、現場から見ると何をどこまで遵守したらよいか混乱している状況です。
●根拠法令ですら、電気通信事業法、不正競争防止法、プロバイダ責任制限法、不正アクセス禁止法、個人情報保護法、電気通信事業における個人情報保護に関するガイドライン（総務省）、Ｊ－ＳＯＸ（金融商品取引法）、Ｊ－ＳＯＸ（財務報告に係る内部統制の評価及び監査の基準）、など色々な項目があります。
●情報セキュリティＳＬＡ契約の問題は、その企業のＩＴ化の目標は何で、その効果を上げるためにISMSにどこまで費用を投入することができるかといったＩＴガバナンス（経営戦略）の問題です。Ｊ－ＳＯＸ法を中心としたＩＴガバナンスは、ITやそのプロセスにおけるリスクと費用対効果をバランスさせながら価値を付加することによって、組織目標を達成するために、組織を方向付けし、コントロールする一連の関係構造とプロセスを示しています。
●ＣＡＴＶ通信会社様の内部統制（Ｊ－ＳＯＸ）を監査法人のコンサルを受けて進行されているアプローチは正解だと考えます。
●ISO27001/2と連動した現場で理解できる『実践ガイドライン』の一本化を目指すべきであると考えます。

●ISO27001/2（情報セキュリティ管理）は、 ISO9001(品質管理)、 ISO14001（環境管理）に次いで、社会システムの実践規範の第三の柱に！
●ポリシー（規範）だけでは不十分で、プロセス（実践）が大切。プロセス（実践）での試行錯誤と学習が、ポリシー （規範）に跳ね返り、その再構築に役立つ。
⇒社会科学の方法論「理論と実践の好循環」（マートン[1968]）

２．Ｂ県様「電子県庁システムアウトソーシング」（０４年４月稼動）事例紹介（１）

■特徴

（１）電子申請・電子調達システムといった県民向け情報システムは元より、財務会計・人事給与・税務システムといった基幹系業務システムについても、大型電算機からサーバへのダウンサイジングに併せてiDCにアウトソーシングしている。

（２）サーバー系システムに移行できない業務システムはiDCの大型電子計算機ホスティングサービスを利用することで、福岡県は大型電算機の所有を廃止した。

（３）帳票出力業務(カット紙：500万枚/年、連続帳票：150万枚/年)、県庁への出力帳票託送についてもiDCにアウトソーシングした。

（４）上記の結果、インターネットを含め、全ての電子県庁システムの監視・運用業務を24時間365日、一元的にIDCで実施した。

■契約形態

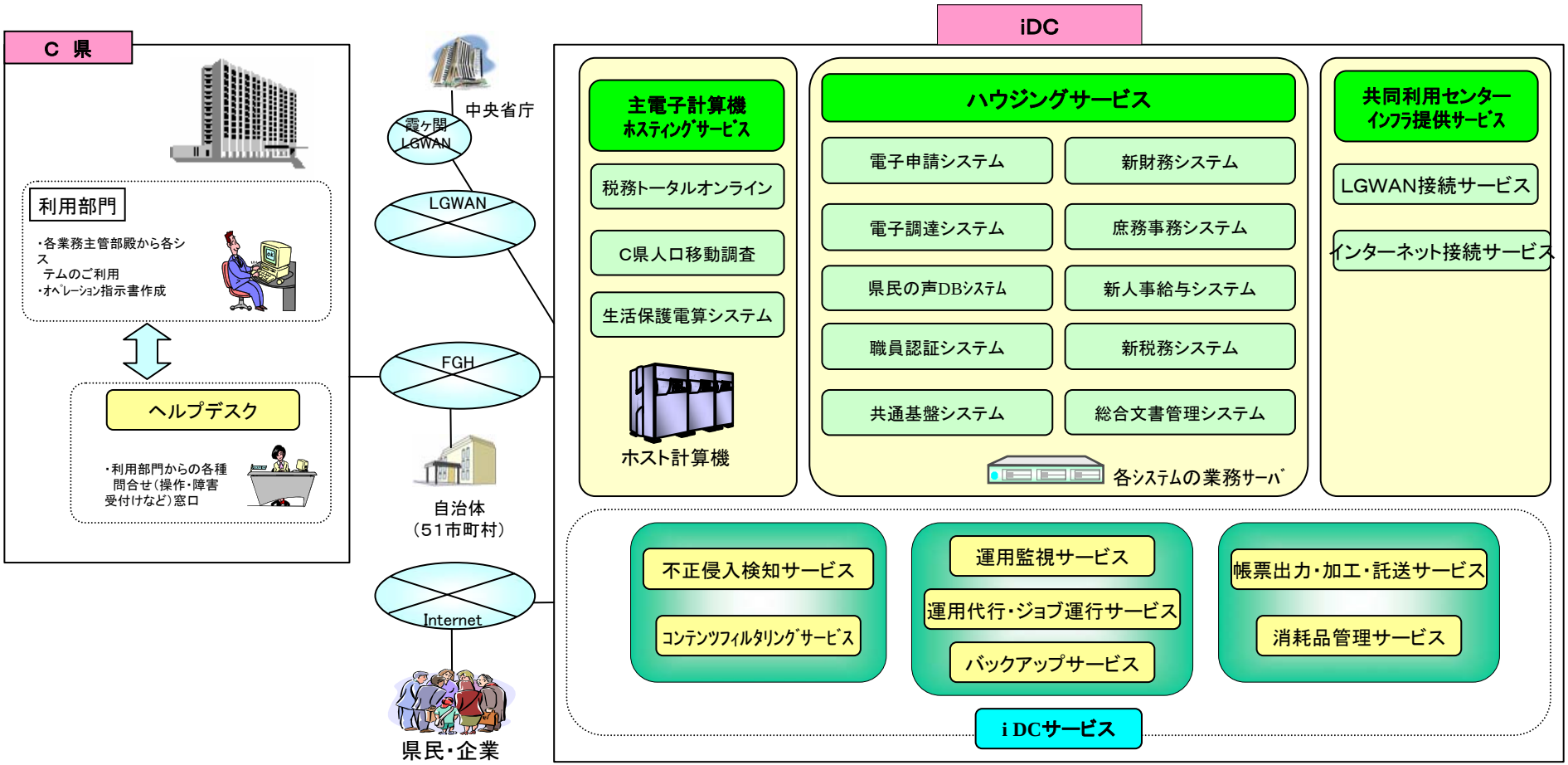
　契約は単年度契約で、毎年、セキュリティ対策・トラブル対応・提供サービス等を細かく規定。更に、システム運用の品質条件として「公共ITにおけるアウトソーシングに関するガイドライン」に基づきＳＬＡ(例えばｽﾄﾚｰｼﾞ ｻｰﾋﾞｽの稼動率99.99%以上等)を受託者と協議のうえ締結。

■課題

　最近のDoSアタックや不正侵入などインターネットを介したセキュリティの脅威に対して、引き続き、的確で確実な監視体制を維持する方策。ＩＳＭＳに基づき、SLAを遵守した運用管理体制を維持する方策。

【出典】ASPIC Japan「ASP・IDC活用による電子自治体アウトソーシング実践の手引き」（2006年）

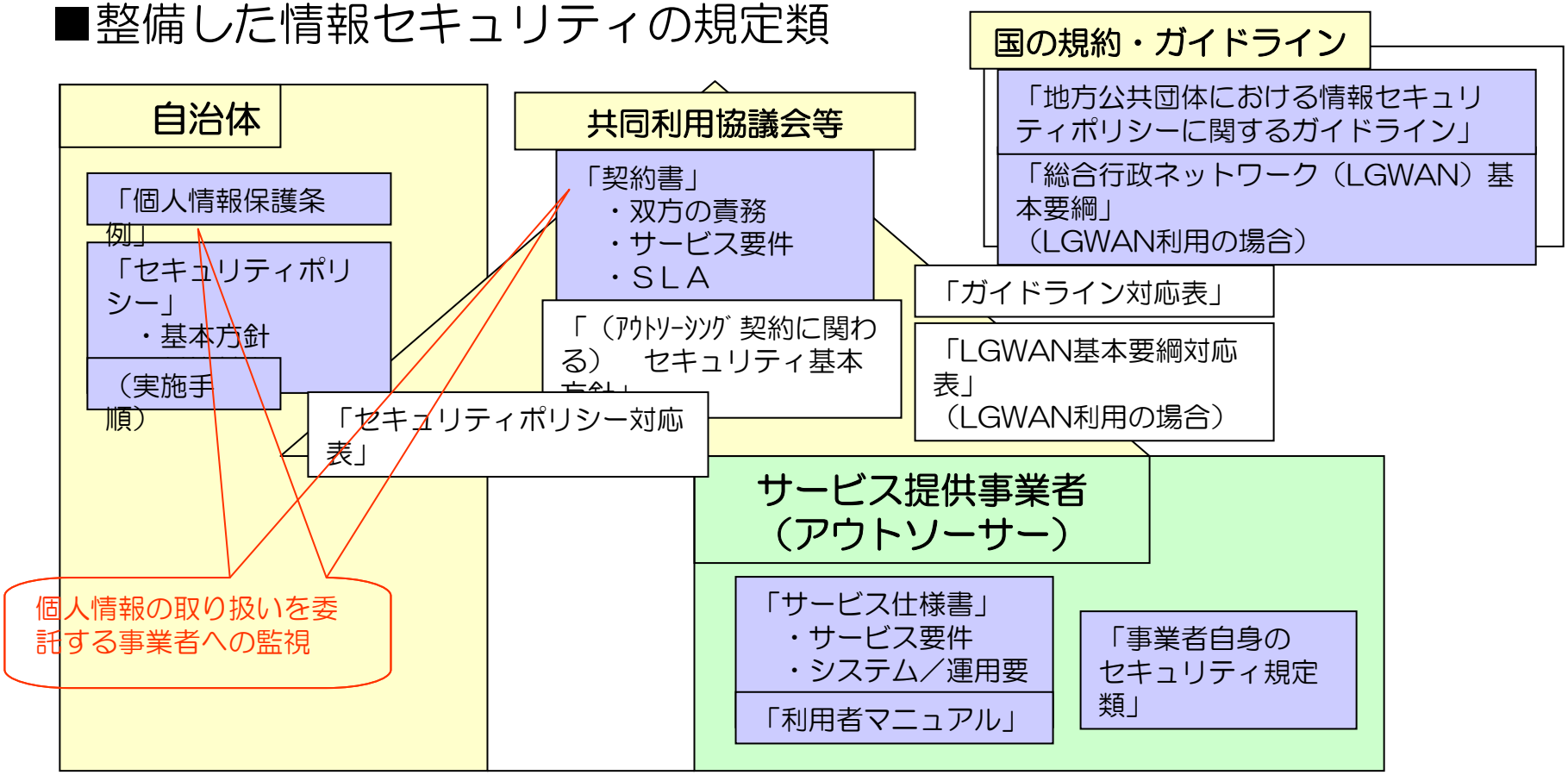
2．B県様「電子県庁システムアウトソーシング」（０４年４月稼動）事例紹介（２）



出所：（株）キューデンインフォコム資料

2．C県様「市町村共同利用電子申請システム」（０４年１０月稼動）の事例紹介（１）

■整備した情報セキュリティの規定類



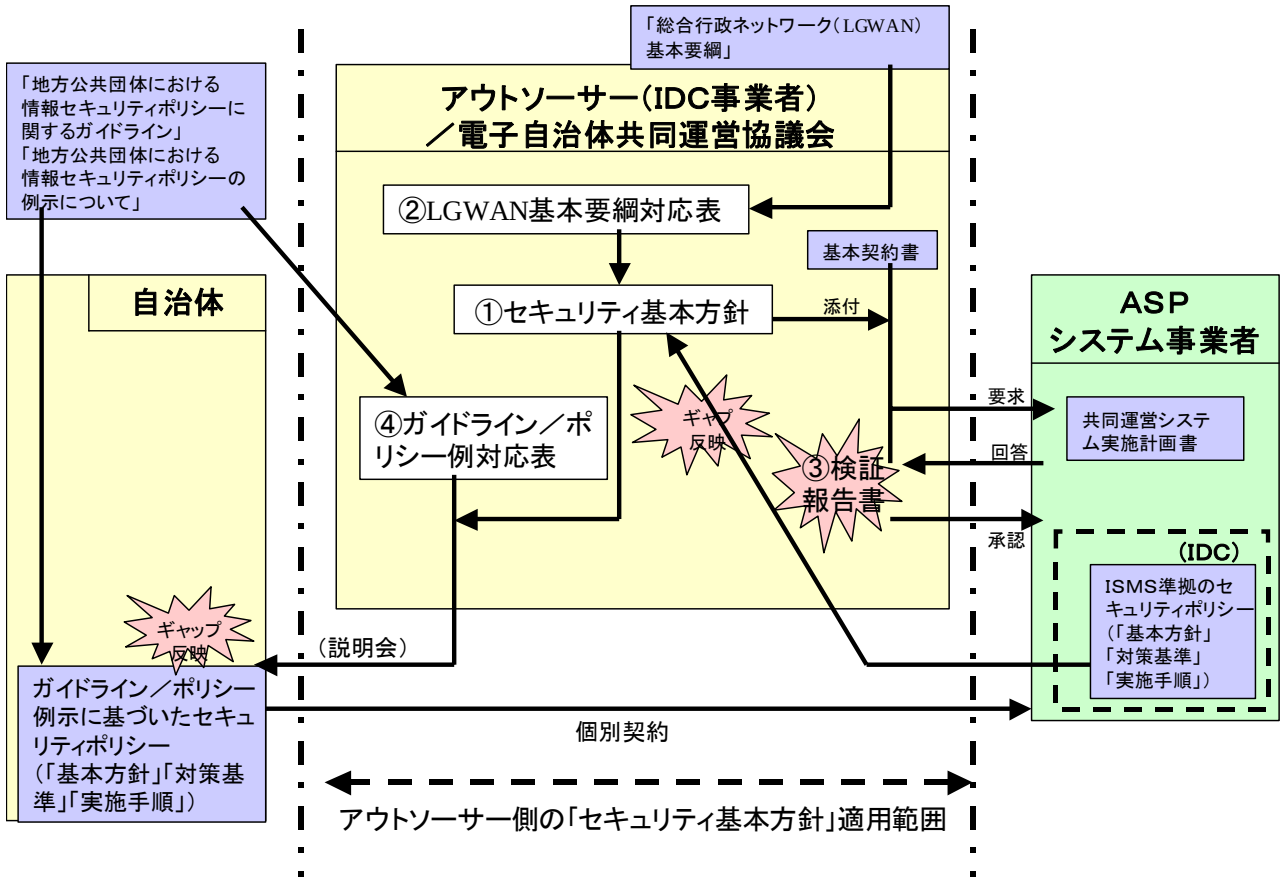
注）白地：関連する文書・規定類
　　着色：当該契約に関し整備すべきセキュリティ関連の規定類

【出典】ASPIC Japan「ASP・IDC活用による電子自治体アウトソーシング実践の手引き」（2006年）

２．Ｃ県様「市町村共同利用電子申請システム」（０４年１０月稼動）の事例紹介（２）

■アウトソーサー側の「セキュリティ基本方針」適用範囲

（注）青地文書（白地文書以外）は、既存文書を想定。



３．D県様「共同利用型電子申請受付システム」（０５年３月稼動）事例紹介

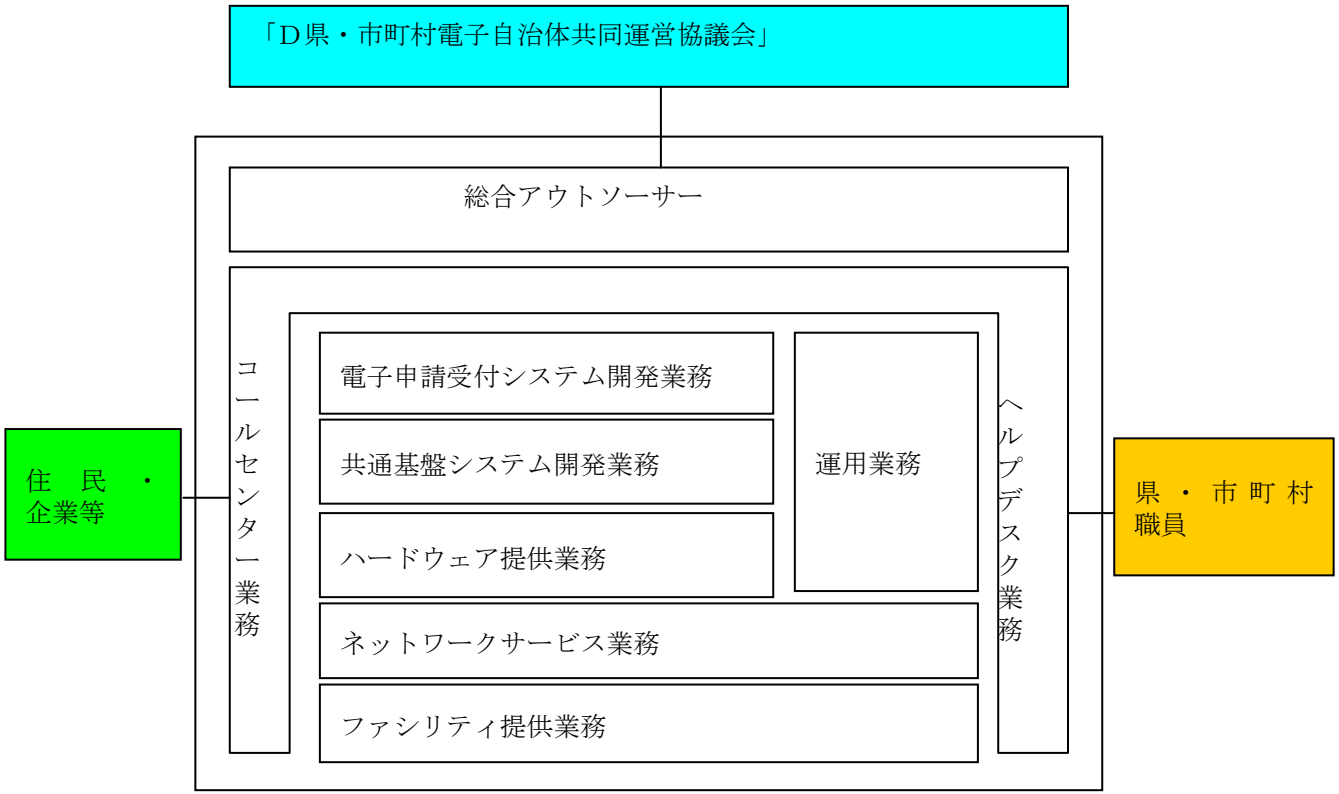
■特徴
・電子申請の実現に当たっては、業務の抜本的な見直しを図るため、BPR手順書を作成。当該手順書に基づき業務の見直しを実施している。
・申請手数料の収納にインターネットバンキングを利用(平成17年12月)。
・携帯電話申請機能を実装。運用開始は平成18年3月。
■経緯
・サービス提供に必要となる高度なファシリティ、セキュリティを有するサーバ設置スペースの確保（ハウジングサービス）および、サーバやネットワークのシステムの運用管理等については、専門事業者へアウトソーシングした。
■契約形態
・「県・市町村電子自治体共同運営協議会」を代表するD県と企業体（３社）間による業務委託契約（複数年契約）。
・当該契約とは別にSLA契約を締結。※総事業費（システム構築経費（ハード・ソフト）、運用経費等）の1/2を県が負担、残りの1/2を各市町村が人口割で負担。
■課題・各自治体の庁内業務の効率化を促進する文書管理システム、統合型GISの県・市町村共同開発・運用を目指している。

●ＳＬＡの管理・運用の留意事項
ア　ＳＬＡ設定値
　ＳＬＡ設定値は、住民用（２４時間・３６５日）と職員用（勤務時間帯）とで、コスト・パフォーマンスを考慮した上げ下げを行なう。
イ　ＳＬＡの見直し、再設定
　自治体ではＳＬＡ数値化は困難なので、ASPIC「実践の手引き」等を参照して設定する。特に、業務システムのＳＬＡは実例が少ないので、実績値に基づく見直しや他自治体との比較が必要であり、毎月の報告会や毎年の検討会等でＳＬＡの見直し再設定を行なう。
ウ　ＢＰＲ（業務プロセス革新）
　自治体の行財政改革（ＩＴによる構造改革）を目的として、システムの単なるＳＬＡ数値の見直し再設定をするのではなく、業務自体の抜本的見直しを行なうＢＰＲ（業務プロセス革新）や経営評価指標KPI（Key Performance　Indicator）の見直しを行い、ＥＡ（業務・システム全体最適化）に基づく、住民サービス向上・経費削減を行なう。

【出典】ASPIC Japan「ASP・IDC活用による電子自治体アウトソーシング実践の手引き」（2006年）

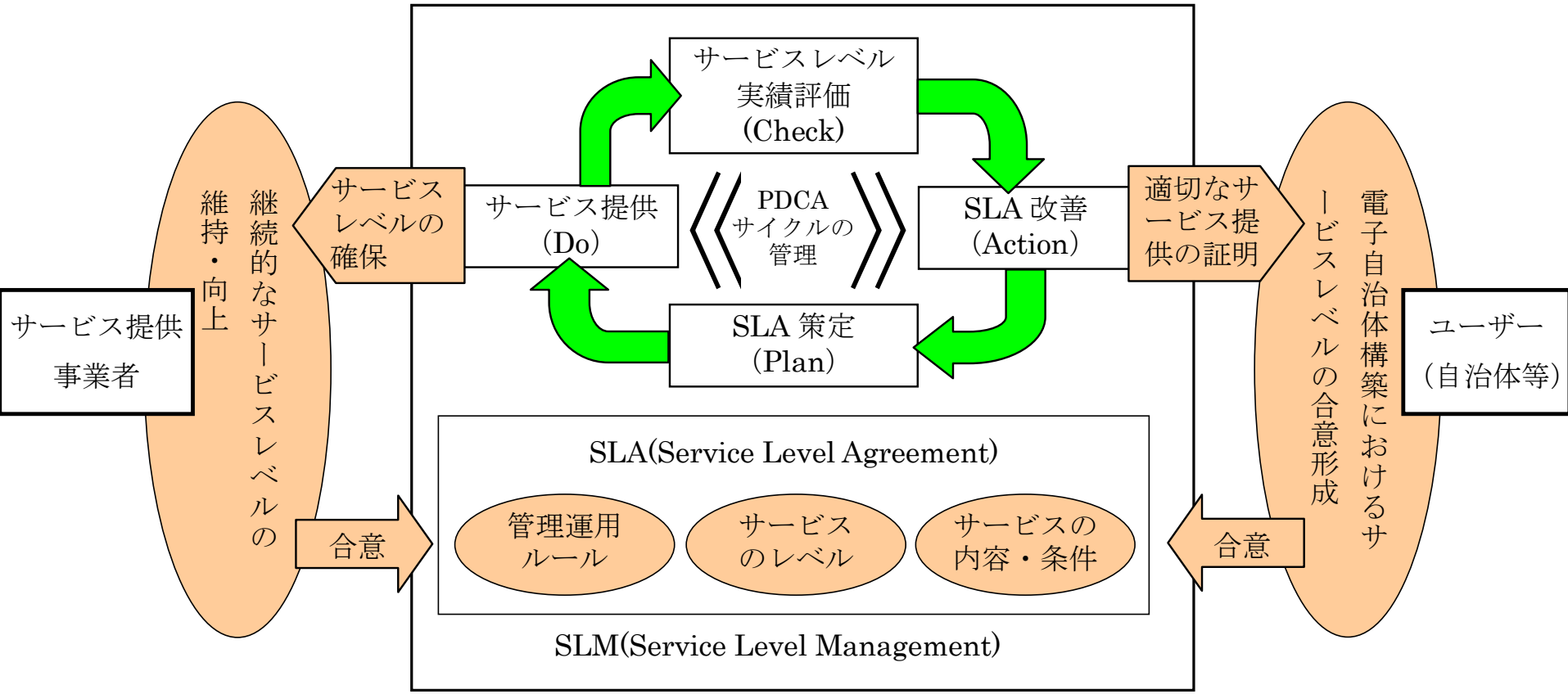
３．Ｄ県様「共同利用型電子申請受付システム」（０５年３月稼動）事例紹介

D県共同利用型電子申請受付システム概要図



【出典】ASPIC Japan「ASP・IDC活用による電子自治体アウトソーシング実践の手引き」（2006年）

３．Ｄ県様「共同利用型電子申請受付システム」（０５年３月稼動）事例紹介



【出典】ASPIC Japan「ASP・IDC活用による電子自治体アウトソーシング実践の手引き」（2006年）P.65

4．電子自治体構築に関連する基準や認証制度

●情報セキュリティマネジメントの実践のための規範
⇒「政府機関の情報セキュリティ対策のための統一基準(第2版)」：政府機関全体としての情報セキュリティ水準の向上を図るために策定された「政府機関統一基準」の改訂（平成19年6月14日「情報セキュリティ政策会議」（議長：内閣官房長官）決定）

■情報セキュリティ監査ガイドライン　⇒ISO/IEC27002（JIS X 5080）
- 自治体のセルフチェックを重要視している「実践ガイドライン」

地方公共団体における情報セキュリティ監査の在り方に関する調査研究報告書（平成15 年12 月25 日総務省）
⇒JIS X 5080と整合をとり、「報告書」の別添1 管理基準（975項目）、別添2 セルフチェックリスト（258項目）、またはLASDEC「やってみよう　情報セキュリティ　内部監査」（80項目）⇒仮説ビデオ

■ISMS （情報セキュリティマネジメントシステム）　⇒ISO/IEC27001

■プライバシーマーク制度　⇒ JIS Q15001
- 個人情報の適切な保護・管理を実施している事業者を認定
- 特に住民の個人情報に関わるシステムを委託するASP・IDC事業者は、取得が望ましい

■ ISO/IEC 15408　⇒ＳＴ確認
- 製品やシステムがあるレベルのセキュリティ要件を満たしていることを認証するための評価基準

■ ITIL （IT Infrastructure Library）　⇒ISO/IEC20000
- ベストプラクティス（参考にすべき先行事例集）

【出典】ASPIC Japan「ASP・IDC活用による電子自治体アウトソーシング実践の手引きP.140～144」（2006年）

●セキュリティ対策を含むASP・SaaSのアーキテクチャ設計の必要性

情報セキュリティマネジメントシステム（ISMS）が規定する安全性【機密性、完全性、可用性】の個別最適化だけでなく、信頼性【完全性、正確性、正当性、継続性】を加えた全体最適化に結びつくITガバナンス技術体系への展開を見据えた情報セキュリティ・アーキテクチャ（政府CIO連絡会議決定に準拠）を設計する。

なお、上記アーキテクチャは、運用プロセスITIL（ISO/IEC20000）、情報セキュリティ管理ISMS（ISO/IEC27000、JISX5080）、内部統制（IT全般統制）COBITといった国際標準に基づくITガバナンス機能要件に準拠することが前提。

ASP・SaaSは、ITIL（ISO/IEC20000）に基づく高品質・可視化された運用プロセスを実現し、「情報」の安全性（機密性、完全性、可用性）と信頼性（完全性、正確性、正当性、継続性）の各リスクをバランスさせながらコントロールする「ASP・SaaSのシステム構造」上でアプリケーションソフトウェア「機能」が動作する。

（注）システム生産標準規格COBIT（Control Objectives for Information and related Technology）は「情報関連技術のコントロール目標」の略であり、「情報通信技術に関連したリスクや便益を認識し、マネジメントすることを支援するよう、ITガバナンスを躍進させるツール」として、情報セキュリティ管理システムISMSの３つの情報基準を含む７つの情報基準（有効性、効率性、機密性、完全性、可用性、準拠性、信頼性）の全体最適化するようデザインされている。

コンプライアンス（ＩＴガバナンス）

安全性
（機密性、完全性、可用性）

信頼性
（完全性、正確性、正当性、継続性）

システムアーキテクチャ
（アプリケーション、ネットワーク、ソフトウェア、ハードウェア、運用、セキュリティ）

●国際標準に基づくＩＴガバナンス（注１）の機能要件

（注１）ＩＴガバナンス：ITやそのプロセスにおけるリスクと費用対効果をバランスさせながら価値を付加することによって、組織目標を達成するために、組織を方向付けし、コントロールする一連の関係構造とプロセス。2006年10月、アテネにて開催された、第1回国連IGF(ｲﾝﾀｰﾈｯﾄ･ｶﾞﾊﾞﾅﾝｽ･ﾌｫｰﾗﾑ) では、インターネットのアクセス、開放性、セキュリティ、多様性について議論。日本経団連が、第1回IGFにミッションを派遣し、産業界の立場から、先進的な経験事例や、携帯電話のスパムメール撲滅等のベストプラクティスを発信。

基盤的プラットフォーム
（決済機能、認証機能、運用管理機能、データバックアップ機能、時刻同期機能　等）

情報セキュリティ基盤
（ファイアウォール、不正侵入検知システム（IDS）、ウイルス対策、情報漏洩防止、統合ＩＤ管理、ログ証跡管理　等）

ＩＤ管理 → ユーザー認証
ＩＤアクセス制御（機密性・可用性）

証跡管理 → ログ管理（ＳＯＸ法監査）

運用管理（集中管理）
・構成管理
・開発・変更管理
・脆弱性管理
・インシデント管理

統制管理

バックアップ、原本保存、インシデント対応（注２）
（注２）ウイルス感染や不正アクセス、情報漏洩、迷惑メール送信、サービス拒否攻撃(DoSアタック)など

セキュリティ対策の網羅性確保 → ISO/IEC2700 (JISX5080)［ＩＳＭＳ］

運用業務の網羅性確保 → ITIL(ISO/IEC20000)［運用］

一貫性・網羅性のある実践規範⇒情報セキュリティマネージメントシステムは、３つの情報基準（機密性、完全性、可用性）の最適化

統一的に出来るようにする
内部統制（IT全般統制（注３））

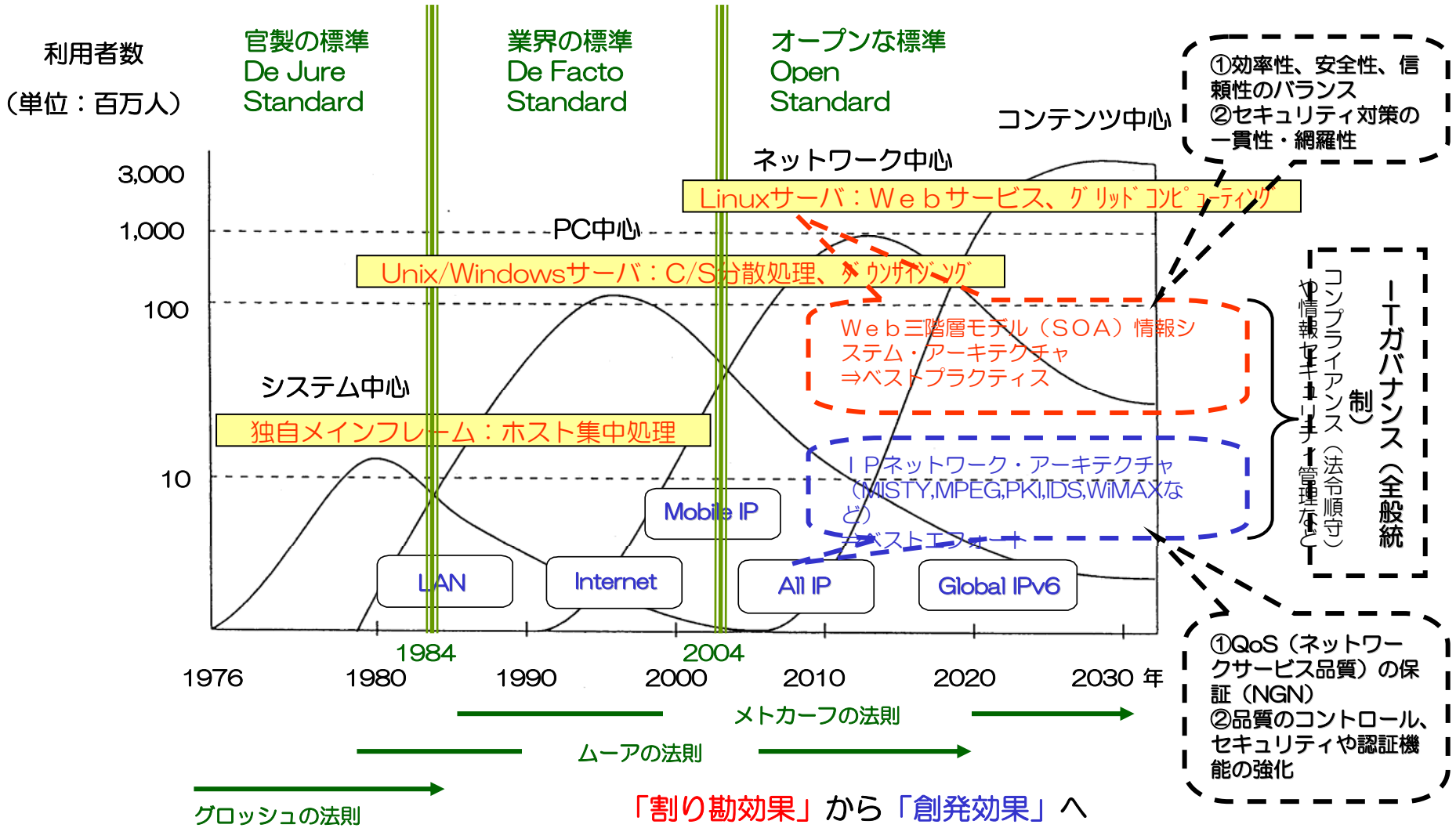
運用は集中管理にして、高品質、かつ可視化された運用プロセスによる運用・保守サービスの提供を実現

COBIT 米国情報システムコントロール協会(ISACA)［ITガバナンス］

IT全般統制の実践規範（ベストプラクティス）⇒７つの情報基準（有効性、効率性、機密性、完全性、可用性、準拠性、信頼性）の全体最適化

（注３）IT全般統制：セキュリティやＩＤアクセス管理、外部委託管理など、情報システムの開発、変更、保守・運用に関する統制

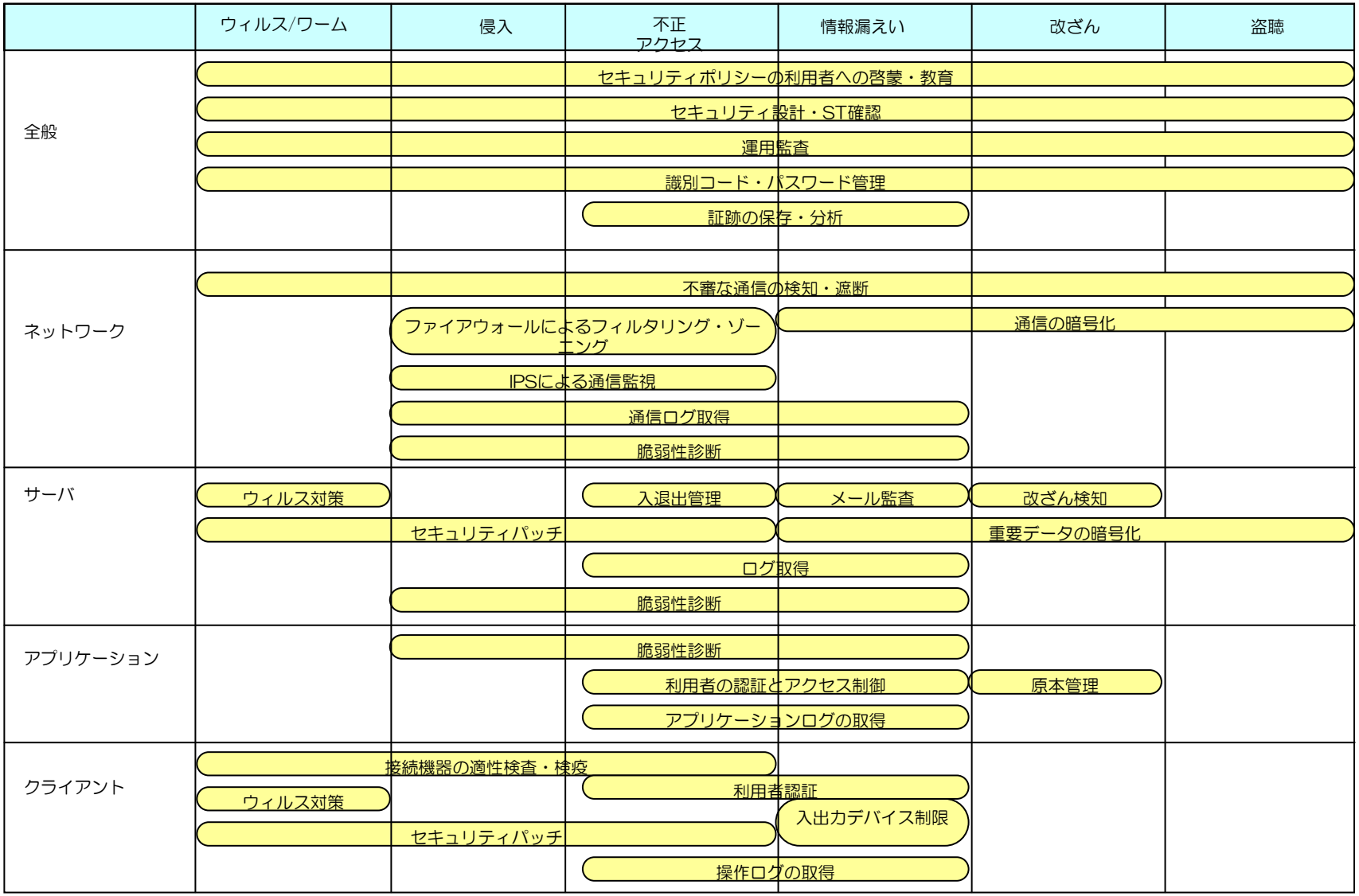
●ネットワーク中心時代の情報セキュリティガバナンス



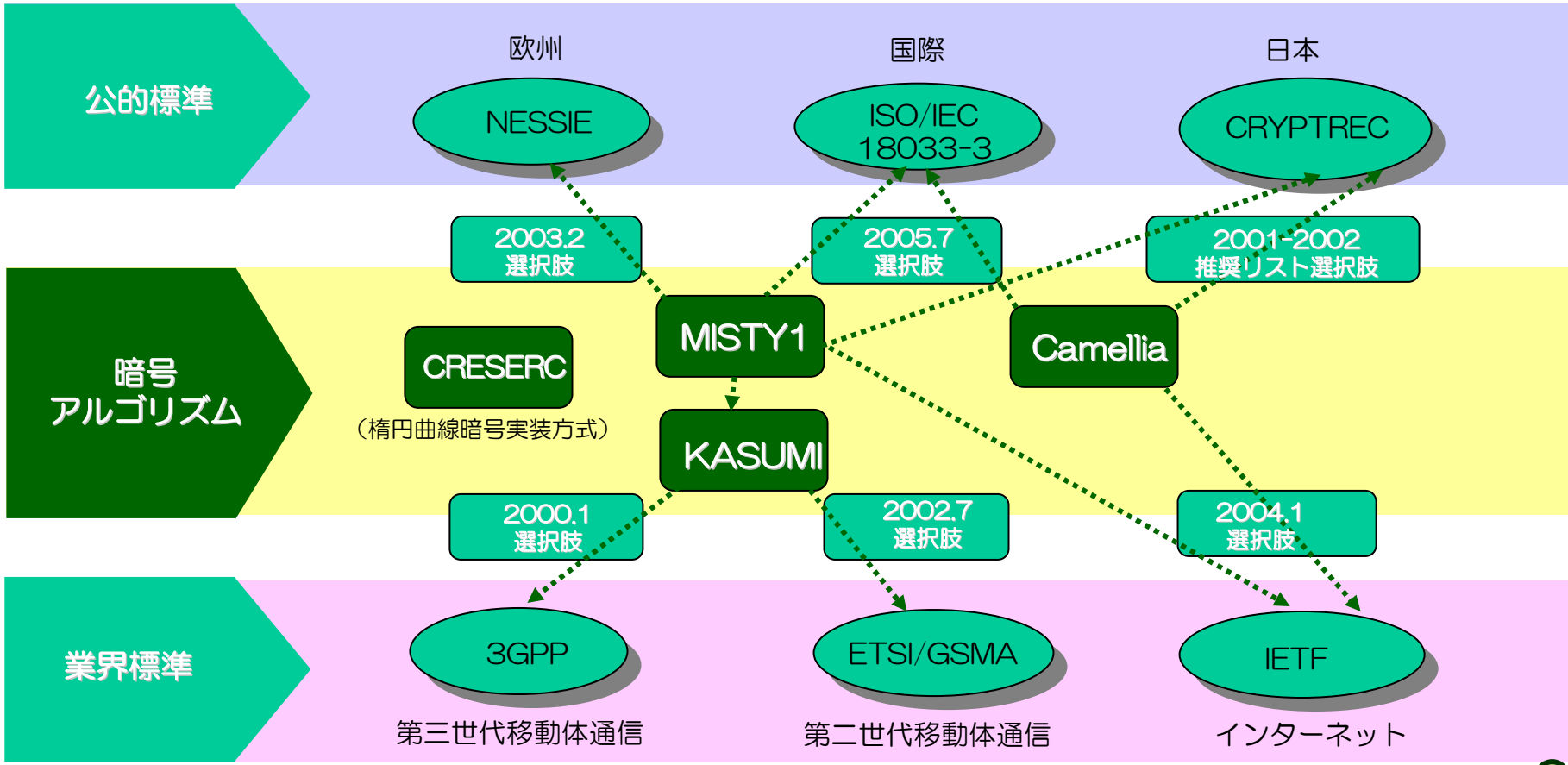
「割り勘効果」から「創発効果」へ

出典：David Moschella, “Waves of Power” ，1997 / 02 に加筆（2004年総務省「ユビキタスネット社会の実現に向けた政策懇談会」村上篤道 三菱電機役員技監）資料をもとに作成

●実証済みのＷｅｂサービスシステム構築モデル（オープン化・Ｗｅｂ化・インターネット化を前提としたシステムの情報システム構造）に基づく、セキュリティ・アーキテクチャの実装設計を行って、一貫性・網羅性のある多層的な情報セキュリティ対策を行うことが必要



（1）暗号アルゴリズムの標準化状況（MISTY、KASUMI、Camelliaなど）



弊社は、MISTY、KASUMI、Camelliaなど世界最高水準の暗号技術を開発しました。
この暗号技術をベースに、耐タンパ実装技術（不正アクセスから鍵を保護する技術）、携帯端末や自動車用電子機器等への組込みセキュリティ技術、ネットワーク経由の攻撃を検知・遮断するネットワークセキュリティ技術などの研究開発を行っています。

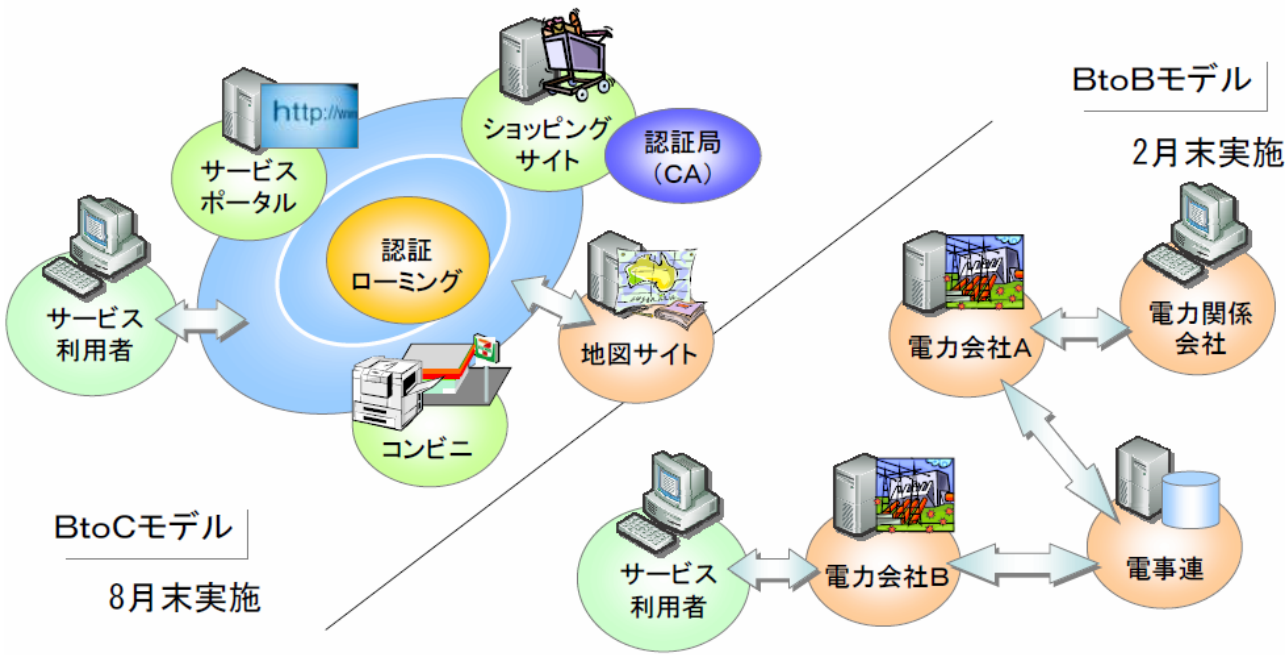
（独）情報通信研究機構（ＮＩＣＴ）委託研究

（２）「異なるCA間の認証ローミング技術に関する研究開発」

・ NICT委託研究として平成１７年度・平成１８年度の２年計画で実施
・ 三菱電機株式会社と株式会社テプコシステムズ（幹事企業）の共同研究
・ 実施計画上の課題は、以下の２点

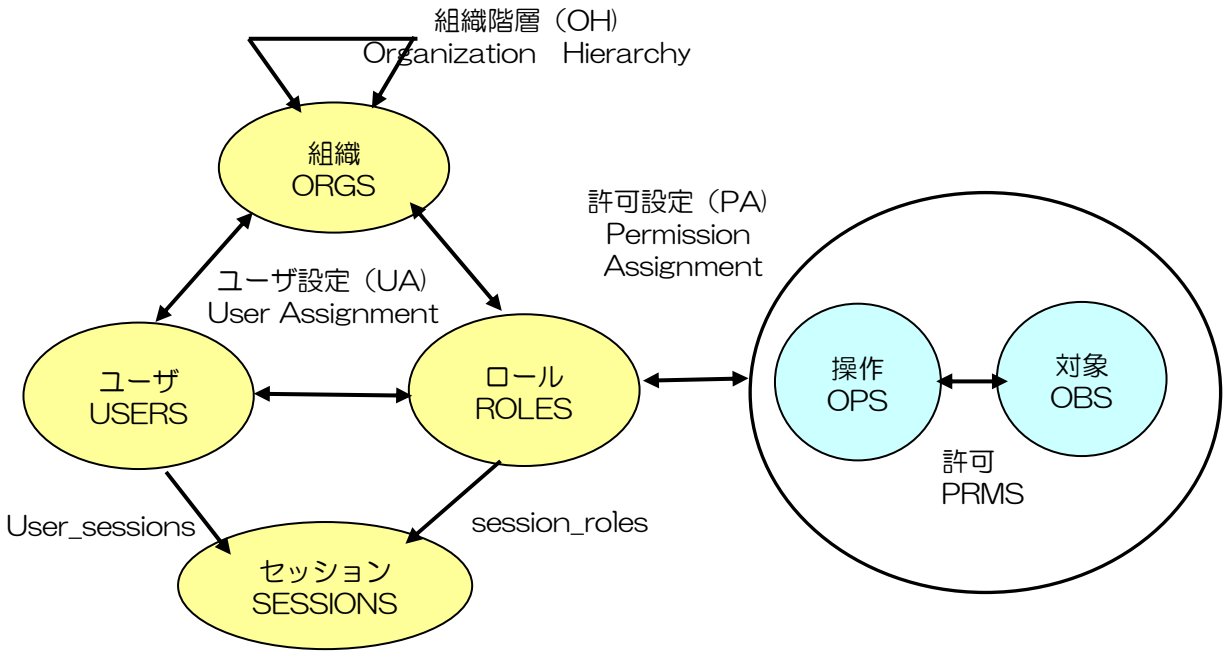
①異なるＣＡ間でアイデンティティ情報の受け渡しが発生しない高速かつ安全な認証方式の開発（三菱電機担当）

②上記認証方式を実環境で有効に機能させるための実証実験（テプコシステムズ担当）



【出典：総務省「地域情報プラットフォームフォーラム」，http://www.applic.or.jp/seminar/pfforum2006/】

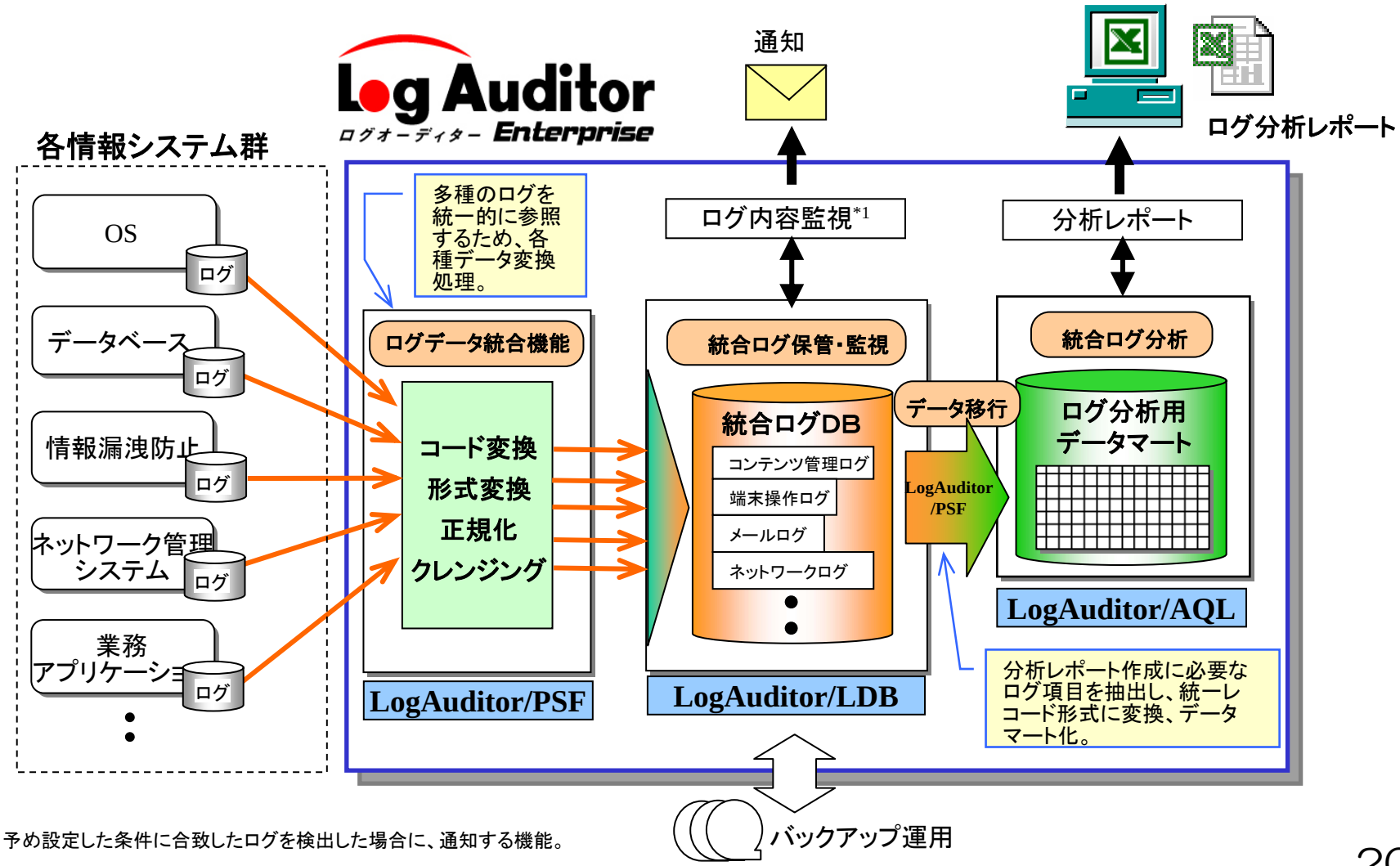
（3）国際標準(NIST)ロールベースアクセス制御（RBAC）システム MistyGuard〈MissionCore〉



国際標準(NIST)ロールベースアクセス制御（RBAC:Role-Based Access Control）モデル

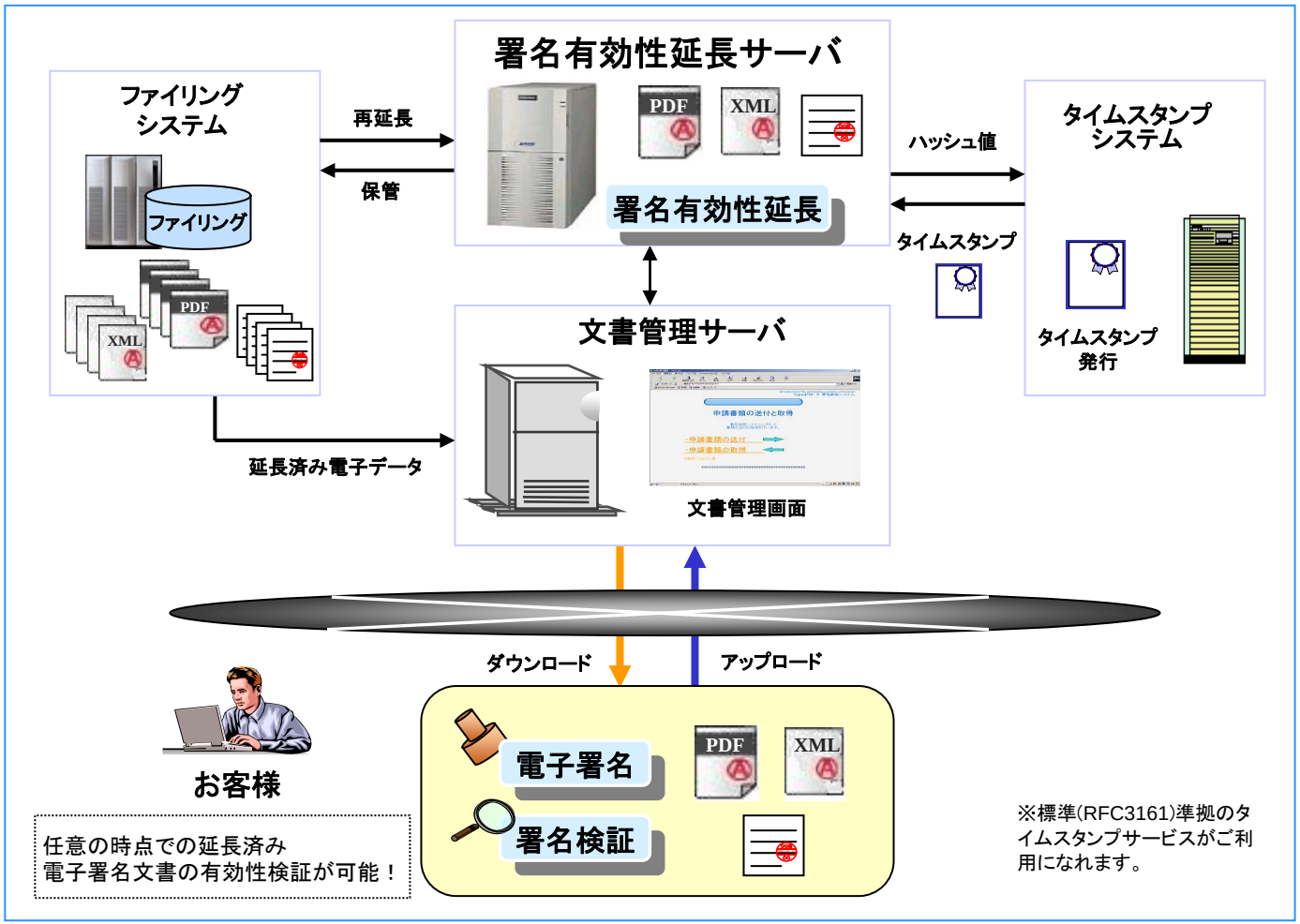
（4）三菱統合ログ管理・分析システム　MistyGuard〈LogAuditor〉

- ✓ 統合ログ管理・分析システムとして、LogAuditor Enterpriseをご提供。
- ✓ 多種大容量のログを統合し、高速に検索・集計した結果をMicrosoft Excel等にレポート出力するシステム。



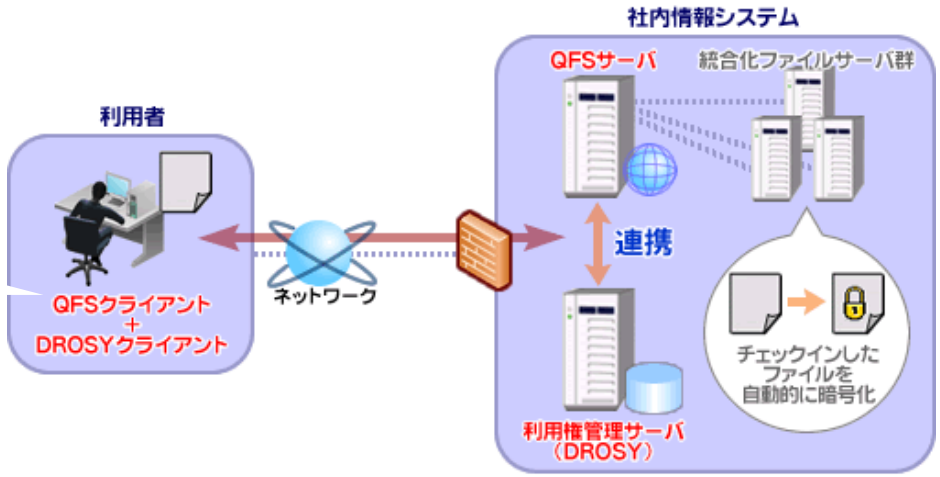
*1：予め設定した条件に合致したログを検出した場合に、通知する機能。

（5）三菱署名有効性延長システム　MistyGuard<EVERSIGN>
⇒文書ファイルの原本の真性を確認する電子署名長期保存技術（RFC3126準拠モデル）



（6）三菱情報情報漏えい防止ソリューション ⇒HP IceWall QFS-DROSY®連携ソリューション

弊社では、HP社の製品である、WebDAVファイルサーバ・ソリューション「HP IceWall Quick File Store」と弊社の企業機密管理ソリューション「MistyGuard®<DROSY Enterprise Edition>」を統合した、「HP IceWall QFS-DROSY®連携ソリューション」を提供しています。「HP IceWall QFS-DROSY®連携ソリューション」は、通信規約「HTTP」を拡張した次世代規格「WebDAV」の採用により拠点間のファイルサーバ共用を容易にした「HP IceWall QFS」（正式名 HP IceWall Quick File Store）と、ファイルごとに利用権を管理できるDRM（利用権管理）技術を採用した「DROSY」（正式名 MistyGuardR<DROSY Enterprise Edition>）が連携することにより、複数のドメインやネットワーク越しでもコンプライアンスを強化しつつファイル管理・共有を可能にします。



操作性
- エクスプローラライクな操作感で、誰でも簡単に利用可能
- 簡易ドキュメント管理機能で、ラクラク文書管理

利便性
- ショートカット機能で大容量ファイル送付も安心
- Windowsドメインの制約を受けないファイル共有

性能
- ワークスペース機能の採用により、軽快なアクセスを実現
- サーバ側でのファイル操作による高速動作

セキュリティ
- Webシングルサインオン製品 HP IceWall SSOと連携することで、セキュアなアクセス管理を実現
- 監査証跡として利用できるアクセスログの収集が可能

ロック
- チェックイン・チェックアウトによるファイルのロックが可能
- 付加情報（フラグ、コメント、編集者）の設定が可能

権限・暗号化
- フォルダ単位に利用権を設定
- 格納したファイルを自動的に暗号化（Word、Excel、PowerPoint、PDF、TIFF/JPG）

アクセス制御
- ファイルのアクセスを制限
- ファイルの利用履歴を把握
- チェックアウトしたファイルの利用権を制御