ISGA
Information Security Governance Association

情報セキュリティガバナンス協議会
2013年度　ワーキンググループ2
最終報告

クラウドサービスの利用に係わるセキュリティリスク対処の検討

コンテンツ

2014年6月30日

1. 背景・目的

■ 背景・目的

他社に情報資産の管理を委ねるクラウドサービスの利用は、ユーザ企業の情報セキュリティガバナンス確立に大きな影響を与える。クラウドサービスは定型サービスであり、ユーザ側で情報資産を管理できる範囲が制限されるため、ガバナンスが及びにくいことがその理由である。多くの事業者はリスクに対し真摯に対応しているが、情報開示が充分でなく、ユーザ側にはリスクの状況を把握しにくいのが現状である。

こうした背景を踏まえ、経済産業省では「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」を発行（２０１１年４月）し、それに基づき、特定非営利活動法人日本セキュリティ監査協会（JASA）ークラウドセキュリティ推進協議会において、クラウド情報セキュリティ監査制度の策定に取り組んでいる。また、クラウドサービス事業者の情報開示を促進するため、一般財団法人マルチメディア振興センターが「クラウドサービス安全・信頼性に係る情報開示認定制度」を運営している。

そこで、本WGでは、ユーザがクラウドサービスの利用について判断する際に、どのような情報が必要か、そうした情報が入手可能かを調査し、ユーザがクラウドサービス利用検討の際に有益な情報を提示すると共に、安全なクラウドサービス利用に向けたクラウドサービス事業者に対する要望を報告書としてとりまとめた。

この報告書の内容は、ユーザ企業における安全なクラウドサービス利用を促進し、さらには経済産業省の施策や、JASAークラウドセキュリティ推進協議会の活動に寄与するものと期待される。

2. 検討メンバー

■ 検討メンバー　（社名：五十音順　氏名：敬称略）

グローバルセキュリティエキスパート㈱	多山　信彦
㈱京王ＩＴソリューションズ	古宮　敏雄
住友商事㈱	北方　孝好
積水化学工業㈱	平尾　安明
㈱高島屋	上原　佳都雄
デロイトトーマツリスクサービス㈱	丸山　満彦
日本コムシス㈱	杉本　博之

（事務局）

㈱三菱総合研究所	川口　修司
㈱三菱総合研究所	江連　三香

３. 検討経緯

■ 会合

第１回	８／ ２（金）	自己紹介、目的・アウトプット等の事務局説明、スケジュール調整	（三菱総合研究所）
第２回	８／30（金）	検討課題へのアプローチ（懸念事項、調査必要事項の洗い出し）	（積水化学工業）
第３回	９／26（木）	ユースケースの紹介 ㈱ディアイティ／独立行政法人情報処理推進機構　河野省二様ご講演 「ｸﾗｳﾄﾞ ｾｷｭﾘﾃｨｶﾞ ｲﾄﾞ ﾗｲﾝと活用ｶﾞ ｲﾄﾞ ﾌﾞｯｸ」	（三菱総合研究所）
第４回	10／24（金）	ユースケースから考えられる検討課題について意見交換 ＜*宿題*＞契約書／ＳＬＡ／事業者からの報告書　記載事項の調査	（京王ＩＴソリューションズ）
第５回	11／21（木）	クラウドサービス契約書に盛り込まれている条項の事例紹介 ＜*宿題*＞契約締結条項の整理	（住友商事）
第６回	12／12（木）	契約書に何を盛り込むべきかの検討	（グローバルセキュリティエキスパート）
第７回	１／23（木）	ＪＡＳＡ（ＪＣＩＳＰＡ）ご担当との意見交換	（三菱総合研究所）
第８回	２／14（金）～15（土）	【宿泊集中討議】	（WG1、WG2合同：京王電鉄㈱殿の会議施設等）
第９回	３／14（金）	報告書の構成確認	（日本コムシス）

４. 全体構成

ISGA
Information Security Governance Association

■ **全体構成**

Step1	クラウド サービス 利用状況	■ メンバーからの事例紹介及びJASAヒアリングにてユースケースや導入実態を確認。 ■ 基幹システムや周辺システムの提供されるサービス機能の確認。 ■ 「クラウド・コンピューティング　ユースケース　ホワイトペーパー」の参照　等
Step2	パブリッククラウド 利用者としてのリスク認識	■ メンバーの事例から懸念されるリスクを洗い出し。 ■ ・「クラウドセキュリティマネジメントガイドライン（附属書Ａ）」や「活用ガイドブック（第３章）」を参照して検討。 ■ クラウドサービスがマルチテナント方式であるためのリスクの洗い出し。
Step3	パブリッククラウド 利用者の情報活用と意識改革	■ 導入判断／事業者選択の判断／運用上の判断に利用できる情報の検討。 ■ 意識改革が必要である点の認識。
Step4	クラウドサービス 契約	■ 契約書／ＳＬＡによる、事業者とのサービス基準確認。 ■ チェックリストによる、事業者とのサービス基準確認。 ■ 監査により、契約書ではカバーできない部分のレベルを確保。
Step5	クラウドサービス 事業者への提言	■ 統一的な基準・項目による情報開示（事業者選択のアピールにもなる）の必要性。 ■ わかりやすい説明の必要性。

5. クラウドサービス利用状況

■ **クラウドサービス利用状況**

◆WG２メンバーの利用状況

- クラウドサービス利用はまだ多くない。
- 基幹システムでの利用事例はなく、グループウェアや一部の業務利用などの周辺システムに限られている。
- SaaSタイプがほとんどである。

◆一般的な利用状況

- 国内では、クラウドの認知度は向上しており、2013年で21.1%が利用。クラウドの利用／導入率は堅調に増加。（IDC Japan, 2013年）
- メールや掲示板といった周辺システムでの利用は進んでいるが、受発注、物流等の基幹システムでの利用はあまり進んでいない。（日経IT Pro, 2013年）

WG2メンバーのクラウド利用状況

メンバー	利用事例	クラウド分類		
		デリバリーモデル	共有形態	利用用途
A社	外部DCで運用される 電子メールサービス	SaaS	パブリック	周辺システム
	外部DCで運用される ファイルサーバーサービス	SaaS	パブリック	周辺システム
B社	外部DC内に電子ファイルを保存	SaaS	パブリック	周辺システム
	大容量業務用データの外部保存による授受	SaaS	パブリック	周辺システム
	Office365のグループウエア利用 （電子メール、掲示板、予定表）	SaaS	パブリック	周辺システム
	メール送信時の自動的暗号化機能利用（外部サービス）	SaaS	パブリック	周辺システム
	メール送受信データの一定期間保管、管理者閲覧（外部サービス）	SaaS	パブリック	周辺システム
C社	業務用モバイル端末からの印刷サービス	SaaS	パブリック	周辺システム
	大容量業務用データの外部保存による授受	SaaS	パブリック	周辺システム
	SNSのサービスを利用した、客先とのデータ共有	SaaS	パブリック	周辺システム
D社	電子メール／グループウェア	IaaS	プライベート	周辺システム
	家庭向け省エネ・節電コンサルティングサービス	SaaS	パブリック	周辺システム
E社	関連会社のOAシステム	SaaS	パブリック	周辺システム
	社内メール便追跡サービス	SaaS	パブリック	周辺システム
	環境情報管理システム	SaaS	パブリック	周辺システム
F社	大容量ファイル受け渡しサービス	SaaS	プライベート	周辺システム
	e-learningによる教育	SaaS	プライベート	周辺システム
	与信管理支援サービス（ASP）	SaaS	パブリック	周辺システム
	安否確認システム	SaaS	プライベート	周辺システム
	電子契約サービス（ASP）	SaaS	パブリック	周辺システム
	WEB会議システム	SaaS	プライベート	周辺システム

6. 利用者としてのリスク認識

Information Security Governance Association

■ 利用者としてのリスク認識

◆WG2メンバーのリスク認識

- 情報漏えいや情報消滅といった企業情報の取扱いに関する内容が大半を占める。
- 利用者側で根本的な対策を取ることは難しく、事業者から提供されるサービスを許容して利用することを前提に、利用の可否及びサービス事業者の選択を検討する必要がある。

サービス	想定されるリスク	リスクの分類	リスクの回避策
電子メールサービス	アクセス制御ができないことによる第三者からの不正アクセス 非暗号化による通信とデータ保存による情報漏えい	情報漏えい（パスワード情報を含む）	容易に推測されないパスワードの利用 運用による暗号化対策の実施
電子メール暗号化サービス	外部サービスとの連携による情報漏えいポイントの増加 サービス変更によるシステム障害や対応工数の増加	情報漏えい 事業継続	なし（サービスを容認）
電子メール一定期間保管・管理者閲覧サービス	外部サービスの連携による情報漏えいポイントの増加 メールデータの外部保存による情報漏えい	情報漏えい	なし（サービスを容認）
グループウェアサービス	社内機密情報の外部保存による情報漏えい サービスの終了	情報漏えい 情報消滅 事業継続	一部機能のオンプレミス化 他社サービスへの移行を事前検証
ファイルサーバサービス	社内機密情報の外部保存による情報漏えい 非暗号化による通信とデータ保存による情報漏えい	情報漏えい 情報消滅	アカウント認証によるアクセス制限 事前に暗号化してデータ保存
大容量ファイル送受信サービス	社内機密情報の外部保存による情報漏えい	情報漏えい 情報消滅 海外当局による検閲	セキュリティ要件を満たしたサービス事業者の選択 利用者の限定
モバイル端末からの印刷サービス	社内機密情報の外部保存による情報漏えい	情報漏えい 情報消滅 海外当局による検閲	なし（サービスの非採用）
SNS	メンバー公開による不特定の第三者への情報漏えい	情報漏えい	なし（サービスの非採用）
社内メール便追跡サービス	外部サーバへ社員の個人情報を保管することによる個人情報の漏えい	情報漏えい	契約書、覚書による情報の扱いに関する契約締結
eラーニング	ラーニングデータの消失	情報消滅	なし（サービスを容認）
与信管理支援サービス	決算非公開企業の場合に与信不可	ー	なし（サービスを容認）
安否確認システム	緊急時のシステム障害によるサービス利用不可	ー	なし（サービスを容認）
電子契約サービス	障害発生によるシステム利用不可	契約遅延／情報消滅	なし（サービスを容認）

7. 利用者の情報活用と意識改革①

■ **利用者の情報活用と意識改革**

◆クラウド導入の判断で活用する情報

●必要な情報
・システムの自社構築または外部システムの導入の方針決定は、経営層の判断を仰ぐことになる。クラウドサービス利用の可否判断においては、自社環境での構築との比較を行い、コスト、セキュリティの両面での説明が必要。

●情報活用のポイント
・**低価格でクラウドが利用できること**
　必要とする処理機能が、自社構築のように痒いところに手が届くものではないこと、サービス範囲外の項目があることが前提
・**セキュリティ面で安心であること**
　現段階では、クラウドサービス事業者に関する監査制度は始まったばかりで、セキュリティレベルを同じ基準で判断することは難しいが、主要なクラウドサービス事業者であれば事業者自らの事業継続のための必要最低限の要件は準備されていると考えられる。

自社構築とクラウドサービス導入との比較

判断項目	自社構築（オンプレミス）	クラウドサービス導入
初期コスト	必要	不要
利用コスト	システム全体にかかるコスト	利用分のみのコスト
災害対策コスト	高い	低い
調達期間	長い	短い
セキュリティ管理	自社の設計による	事業者のサービスによる
バックアップ	自社の設計による	オプションサービス

資料：Amazon Web Service

7. 利用者の情報活用と意識改革②

ISGA
Information Security Governance Association

■ **利用者の情報活用と意識改革**

◆クラウドサービス事業者の選択で活用する情報

●必要な情報
クラウドサービス事業者の選択では、自社が必要とする処理機能への対応面、及び保守・運用への対応面について、クラウドサービス事業者のサービスレベルや技術レベルの比較が必要。

●情報活用のポイント
・経済産業省　情報セキュリティ政策室（平成２６年）の「クラウドセキュリティガイドライン活用ガイドブック」「4.3クラウドサービス事業者の選択」では以下が記載。
- 経済産業省の「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」に従って情報を提供している事業者を、まず候補業者の対象にし
- 事業者が第三者認証を取得しているか。
- 事業者がホワイトペーパーなどを開示しているか。

などを調査し、選択要件の補完情報とすることが推奨。また、
- 事業者に預けるデータの種類・範囲が明確になれば、リスクが絞られ、それにより情報の重要性に見合ったセキュリティレベルや対応策が明らかになる

・日本セキュリティ監査協会（平成２４年５月）「クラウド情報セキュリティ管理基準利用ガイド」に、検討すべき基本的なリスク（21項目）が掲載。
・「フリーミアム」（Free：無料　Premium：有償からの造語）を活用し、正式採用の前に「実際に使ってみる」ことも選択要件としては効果的。

7. 利用者の情報活用と意識改革③

■ **利用者の情報活用と意識改革**

◆運用上の課題解決で活用する情報

●必要な情報
運用上の課題は、主にシステム障害への対応や稼働状況の分析、及び稼働予測、システムの改善など、サービス利用者では管理できない事項に関してコミュニケーションを取ることが必要。

●情報活用のポイント
・サービス利用者は、運用契約、SLA（Service Level Agreement）などの締結条項として記載した内容が、齟齬なく実行されているかを管理することが必要。
・クラウドコンピューティングユースケースディスカッショングループがまとめた「ホワイト・ペーパー（第4.0版）」（2010年）の「8.4　SLAに関する考慮事項」「8.5 SLAの要件」に締結の要件が記載。
・前出の「活用ガイドブック」でも以下のアドバイスが記載。
  - システム／データのバックアップを定期的に取得するサービスが実行されているか。
  - システム運用でのアクセス制御として、多要素認証（二段階認証、二要素認証）に対応されているか。
  - 管理者用ネットワークの制限ができるか。

7. 利用者の情報活用と意識改革④

■ **利用者の情報活用と意識改革**

◆意識改革の必要性

- 企業においては、自社構築（オンプレミス）からクラウドへとシステムの利用形態が移りつつあり、利用する側の意識も変えていく時期が到来。
- 利用者は、様々なクラウドサービスを適切に選択し、既存システムと連携を取りながら、ユーザ満足を図りつつ、グループ企業の全体最適化を進めていくことが必要。

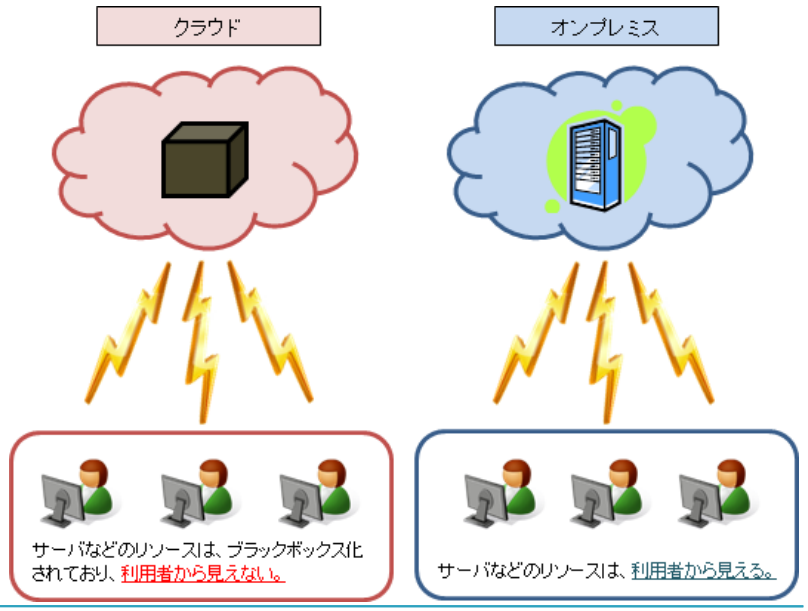
(1)ブラックボックス化への課題認識

基本的に内部構成はブラックボックス化されているため、障害発生時の原因と復旧の目途が立ちにくい。サービスレベル（SLA）を明確にし、「エンドユーザとして、快適にサービスが利用できているかどうか」という観点で把握。

(2)情報（データ）に対する利用者責任の認識

最終的に情報（データ）に対して責任を負うのは、今までと同様利用者側にあること、また、日本以外の国にデータセンタが設置されることで、情報の取扱いの違いや現地の規制当局による情報の差し押さえなどのリスクがあることを認識。

システムのブラックボックス化



8. クラウドサービス契約①

ISGA
Information Security Governance Association

■ クラウドサービス契約

◆契約書

・クラウドサービス利用時は、外部委託でオンプレミスにシステムを構築し運用する場合の契約条項の他、クラウドサービスの特性に応じた契約条項を追加する必要がある。

(1)クラウドサービスの機能要件

業務機能の追加・変更時は、契約書・SLAで明確化

(2)クラウドサービスの非機能要件

性能、キャパシティ要件、セキュリティ要件、サイバー攻撃対策要件、運用要件、障害対策要件、災害対策要件

(3)コンピュータセンタ

バックアップセンターの有無、耐震強度、津波等による水害対策、自家発電装置等電源喪失時の設備、液状化対策、システム運用要員確保等

契約条項（例）

項番	契約条項	備考:サービス利用者側の確認事項等
1	契約の成立	契約の自動継続の条件等の確認
2	本サービスの利用料	利用料の他、各種コスト等の確認
3	本サービスの利用方法	アカウント情報（ユーザ ID、パスワード）の適切な管理・使用。特に共用 ID の管理状況確認。
4	サービス利用者データの取り扱い	機密性の高い情報の情報漏えい対策は、詳しく確認
5	バックアップ	役割・作業分担、追加費用の有無確認
6	禁止事項	事業者のデータアクセスについて禁止等、事業者側の禁止事項についての網羅性確認
7	譲渡禁止	クラウドサービス事業者側の業務継続（譲渡禁止）も必要に応じて取り決めが必要
8	本サービスの一時的な提供停止	SLA で具体的に定義必要
9	本サービスの廃止	クラウドサービス事業者側の業務継続も必要に応じて取り決めが必要（項番 7 と同様）
10	本契約終了後の処理	情報漏えい対策が必要
11	損害賠償の制限	損害賠償金額等の妥当性について確認
12	免責	免責となる損害の内容について確認
13	本利用規約の変更	クラウドサービス事業者が一方的に有利な内容になっていないか確認（利用料金の変更等）
14	輸出法の遵守	データセンタ等の所在地確認が必要（国内、国外）
15	合意管轄	クラウド事業者の所在地確認が必要
16	準拠法	個人情報保護法等国内法の適用対象か確認が必要（データセンタの所在等確認）
17	再委託	再委託は原則禁止、再委託時は事前承認する契約を推奨
18	監査	必要に応じてサービス利用者が監査できる内容の条項追加を推奨

資料:「クラウドセキュリティガイドライン活用ガイドブック」の16項目に必要と判断された「再委託」「監査」を追加。

8. クラウドサービス契約②

Information Security Governance Association

■ クラウドサービス契約

◆SLA

- SLAはクラウド利用契約書の補足事項として作成され、契約書の付属書類として添付される。
- 利用者としてはクラウドのサービスレベルはSLAに基づき確認。
- SLAは「努力目標」としての規定に留めた項目があるため、内容は十分確認する必要がある。

SLA（例）

項番	SLA 項目		備考：サービス利用者側の確認事項等
1	アプリケーション運用	サービス提供時間	業務要件を満たすか確認
2		オンライン応答時間	マルチテナント要因等による応答時間の劣化を許容できるか確認
3		バッチ処理時間	同上
4		カスタマイズ性	定期的、定型的な変更は、サービス利用者自身で可能か確認
5		外部接続性	他のアプリケーションとの連携が可能か確認（API の提供有無を確認）
6		同時接続利用者数	業務要件を満たすか確認
7		利用者への通知	障害発生時のサービス利用者への通知対象内容、通知方法が妥当か確認
8		ディザスターリカバリ	バックアップセンタ、データの隔地保管の有無。サービス再開までに要する時間、どの時点まで回復可能か等を確認
9		重大障害時の代替手段	CP、業務 CP（BCP）の内容を確認
10	サポート	サポート窓口	連絡先が具体的に定義されているか確認
11		サポート緊急窓口	同上。特に、夜間、休祭日の窓口が定義されているか確認
12		サービス提供状況の報告方法	月次報告等、定期的な報告の有無を確認
13	データの管理	バックアップの方法	データ保全方法を具体的に確認
14		ログの取得	個人情報等機密性の高いデータを取り扱う場合は、取得するログの種類、保管期間、保全手段等の確認
15	セキュリティ	情報取扱者の制限（サービス利用者）	自社のセキュリティ管理基準で定めているアクセスコントロール要件を満たすか確認
16		情報取扱環境（クラウドサービス事業者）	クラウドサービス事業者は、システム的に情報にアクセスできないこと、物理的にもアクセスできない環境であることを確認
17		通信の暗号化レベル	公衆回線を利用する場合は、暗号化しているか確認
18		ウイルス対策管理	既知のウイルス対策はもちろん、未知のウイルス対策状況も確認
19		公的認証取得	ISMS、プライバシーマークの取得状況を確認。なお、ISMS の場合は利用するクラウドサービスが取得対象であることを確認
20		サービスに関する第三者評価	Web アプリケーション診断、ペネトレーションテスト、ネットワーク・サーバの脆弱性診断等の脆弱性診断を定期的に実施していることを確認

資料：「クラウドセキュリティガイドライン活用ガイドブック」

8. クラウドサービス契約③

■ **クラウドサービス契約**

◆チェックリスト

・契約書・SLAに記載できない事項は、サービス利用者が自らの責任で情報を整理し、文書化して当事者間で確認する。
・セキュリティ管理基準等について、一定水準以上の実効性が確保できると思われる。

【活用事例】

(1)クラウドサービス利用時の基本的なチェック項目

例）経済産業省「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」
末尾付録「クラウド利用における実施の手引き一覧」

(2)システムの特性に応じた追加チェック項目の検討

・クラウドサービスの「利用者」による分類
利用者を特定しない／取引先が利用／社内で利用
・クラウドサービスで「取り扱うデータ」による分類
機密性の高いデータ／公開情報

(3)システムの特性に応じた追加チェック事項の例示

－　サイバー攻撃対策
例）IPA「セキュリティ対策状況チェックリスト」
－　個人情報保護対策
例）経済産業省「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とするガイドライン」

8. クラウドサービス契約④

■ **クラウドサービス契約**

◆監査

- サービス利用者は、利害関係のない第三者による客観的な評価結果を得ることができれば、安心してクラウドを利用することができる。事業者自らが、第三者による監査を受け、監査結果を広く利用者に開示する制度の整備が望まれる。
- サービス利用者としては制度の整備を待つだけではなく、開示された監査結果を評価するスキルが必要である。

9. クラウドサービス事業者への提言

■ **クラウドサービス事業者への提言**

◆統一的な開示項目と開示基準の策定

- 利用者側として知りたいのは、安全かどうかということ、利用者が受ける制約（あるいは許容すべきリスク）は何かということであり、セキュリティ対策内容の仔細について評価することは稀である。
- 事業者側も積極的には情報開示をしていないため、クラウドサービスの導入検討企業は、情報収集の段階において、多大な時間と労力を要することが多いのが実情である。
- 事業者が、利用者が気にするポイントを想定し、ある程度統一的な開示項目と基準を策定して積極的に公開（または、すぐに開示できる準備）することが、クラウドサービスの導入促進につながる。

◆わかりやすい説明（情報開示）

- クラウドサービス事業者は、細かなセキュリティ対策を説明するよりも、どうして安全なのかをわかりやすく説明できることも必要である。
- 利用者にとって不利となるような情報（リスク）を包み隠すことなく、リスクがあるならば開示し、許容できるかできないかを企業側に問うことも、信頼を得ることにつながる。

１０. まとめ

■ まとめ

・この報告書では、クラウドサービスの現状、想定されるリスクとその対策の考え方をまとめた。

・協議会メンバーの自社事例を参考情報としたが、クラウドサービスを本格的に導入している会社が少なく、サンプル事例も限定的なものとなった。

・そこで、実態を把握するため、JASAのご担当者との意見交換を行い、クラウドサービス事業者の監査制度について説明を頂き、クラウドサービスの信頼性や、事業者の選択、また契約締結について具体的なお話を聞かせていただいた。
・独立行政法人情報処理推進機構（IPA）のご担当者から、「ガイドラインとガイドブック」と題して、サービス利用者としての利活用の解説をいただいた。

・報告書作成に向けては、テーマを絞って集中討議を開催するなど、課題に対して十分な検討が行われ、またお互いの気付きの機会ともなり、成果が得られた。

・今後、クラウドサービスの導入は急速に展開されると推測されるが、事業者と利用者がお互いの役割を認識し、締結された契約に基づき実行されることが重要となる。この報告書が、読者の皆さまの良きヒントになることを期待する。

ＷＧ２の皆さん、外部の講師としてご協力頂いた方々、ありがとうございました。