ワークスタイル変革と情報セキュリティ

Work-style Innovation and Information Security

中　村　彰　子

要　約　情報セキュリティマネジメントシステムが定着しつつある2011年現在，クラウド，仮想化，スマートフォン，ソーシャルネットワークなど新たな技術分野が注目されている．これらが連携し企業が業務を行うためのワークスタイル変革に向かい始めているが，新技術に対するリスクへの不安も持ち上がっている．それに伴い情報セキュリティに関わる多くの団体がクラウドに関するガイドラインを公表し，次の時代を安全に迎えるための準備を進めている．

本稿では，これまでに公表されているガイドラインを考察し，ワークスタイル変革を成功に導くためにあるべき情報セキュリティマネジメントの方向性を確認する．

Abstract　New technical fields such as cloud computing, virtualization, smart phones, and social networking are attracting attention as of 2011 when the information security management system has been well-established. It begins to face the work-style innovation for the enterprise to perform their business activities in these new technical fields; however, a risk toward these new technologies comes up also. Based on this, a lot of groups related to the information security release the guideline concerning cloud computing, and take a preparation to come safely for the next age.

In this paper the author considers the guideline that has been published in the past, and discusses the desirable future direction of the information security management to assure the success of the work-style innovation.

1. は　じ　め　に

インターネットの普及とともに，マルウエアの侵入や適切に管理がされない情報機器の脆弱性に起因する情報漏洩，複数のコンピュータから標的となるコンピュータに大量の処理負荷を与えるDDoS攻撃と呼ばれる分散型サービス妨害などの多くのリスクが出現し，企業の情報資産が脅かされるようになった．企業が所有する情報資産の取り扱いが見直されるとともに，情報セキュリティリスクはコンピュータ技術によるものだけではなく，紛失や盗難による人的な事故，管理されていない入退室による第三者の侵入によって起こりうる事故など，物理面でのセキュリティからの影響も認識されてきた．そうしたリスクに対し適切な対策を講じないと，顧客からの信頼を失うようになる．そして企業の価値を高めるために，保有する情報資産に対し，人，技術，物を情報セキュリティの側面で統制する情報セキュリティマネジメントシステム（ISMS）が普及するようになった．2005年にはISO/IEC27001としてISMSの要求事項が国際規格となり，認証の取得は企業がセキュリティガバナンスを実践していることを示し，顧客からの信頼を勝ち得るための重要な要素となってきている．

一方クラウド技術の出現によってインターネットビジネス環境は新たな時代を迎えようとし

ている．クラウド技術の発展によりインターネット上のリソースを効果的に利用することで，業務を行う空間が広がるだろう．また，シンクライアント，仮想デスクトップ，スマートフォンの出現により，業務で利用する機器形態も変わりつつある．こうした技術により，在宅勤務，サテライトオフィスや最終的には業務で利用する場所をまったく選ぶことがないノマドワーカーと呼ばれるものまで，あらゆる形態でのビジネス環境が考えられるようになってきた．

2011 年 3 月の東日本大震災の影響により首都圏でも出勤困難な状況が発生し，在宅勤務の導入や利用する端末機器の選択が課題となってきた．不測の事態に速やかに対応できるように，企業は新たな就業形態の見直し時期に来ていることも感じられる．しかしながら，多くの人が利用する技術は攻撃者のターゲットになりやすく，新たな脅威となる悪しき技術も発明される．新たな脅威に対抗する技術は後追いになりがちであるため，今だ不透明なセキュリティ面での懸念がクラウドの導入を遅らせているとも言われている．

ワークスタイル変革に臨むにあたって，クラウドや仮想化技術に対し予測されるリスクを視野に入れて，セキュリティ計画を進めることが企業の重要な課題となる．

2. 情報セキュリティのこれまでとライフスタイル変革への影響

情報セキュリティマネジメントが普及するなかで，如何なる対策を講じても払拭できないリスクとして情報資産の漏洩や紛失がある．外出先で利用するモバイル PC の紛失や盗難による情報漏洩対策として，機器の持ち出し管理，機密度の高い情報データの持ち出し禁止やディスクの暗号化などが行われているが，事故が起きたときの対処は簡単ではない．たとえ暗号化していても紛失したデータの識別，第三者に渡った可能性の追及，顧客への対応など調査を行わなければならない．そのためにたとえ紛失してもデータを失うことがないシンクライアント端末が推奨され始めた．更に仮想デスクトップにいたってはゲスト OS に対しての管理も必要なしで利用可能とし，仮想化技術はワークスタイルを変革する一方でセキュリティ面での効果にも期待される技術として提言され始めた．また，クラウド技術の利用により，仮想サーバのセキュリティは専門部門で確実に維持され，エンドユーザの負担が軽減されるようになった．

その反面，WEB メールなど重要な情報資産のセキュリティ管理を第三者に委任してよいのかという不安も聞かれる．あるいは，クラウド事業者側でのグローバル連携により思いもよらない国のサーバに重要なデータを保管することも考えられる．今までの情報セキュリティマネジメントとは異なり，多くのステークホルダーが情報セキュリティを管理する立場になる．ISMS は組織が保有する情報資産を対象に，利用する適用範囲を持って情報セキュリティマネジメントを実施するものである．また，クラウドサービスを利用する場合にステークホルダーの情報セキュリティ管理に対する責任範囲が複雑になってきている．そうした危機感からいくつかの団体でクラウドセキュリティを提唱するようになってきた．次章では代表的な三団体におけるクラウドセキュリティの取り組みを取り上げる．

3. クラウドセキュリティの標準化動向

クラウドを進める団体の中でもセキュリティに特化して取り組むものが現れ始めた．主に不特定多数のユーザが共有で利用するパブリッククラウドをターゲットにしていると考えられるが，企業が独自に構築するプライベートクラウドや両者を混合したハイブリッドクラウドでも，運用管理者は個々の役割の範囲で同様のセキュリティ対策を策定するべきである．

3.1　ENISA のクラウドコンピューティングに関する情報セキュリティ文書

EU の機関である欧州ネットワーク情報セキュリティ庁（European Network and Information Security Agency：以下 ENISA）はクラウドの将来的なリスク対応のための計画として，2009 年 11 月にクラウドコンピューティングのセキュリティに関するガイドライン「クラウドコンピューティング：情報セキュリティ確保のためのフレームワーク」と「クラウドコンピューティング：情報セキュリティに関わる利点，リスクおよび推奨事項」などを公表した．日本では 2010 年 10 月，独立行政法人情報処理推進機構（以下 IPA）が日本語化し公表している[1]．

「クラウドコンピューティング：情報セキュリティ確保のためのフレームワーク」ではクラウド利用者とクラウドプロバイダを対象にベースラインとして責務の範囲を示している．その境界として，ソフトウエアサービスを提供する SaaS (Software as a Service)，プラットフォーム基盤をサービスする PaaS (Platform as a Service)，サーバやストレージなどインフラをサービスする IaaS（Infrastructure as a Service）それぞれのケースを考慮しているが，特にサービス利用時にクラウド利用者は自己の責務に含まれるものが何かを検証すべきとしている．

「クラウドコンピューティング：情報セキュリティに関わる利点，リスクおよび推奨事項」ではクラウドの情報セキュリティに関する利点として，利用者が信頼のおける IaaS のプロバイダを選べば，専門の管理者が集中して効率的なパッチ管理をするので，利用者がパッチ管理する必要がなくなることなどがあげられている．

情報セキュリティリスクとしては「ポリシーと組織関連のリスク」「技術調達のリスク」「法的なリスク」「クラウドに特化していないリスク」の四つに大別されている．「ポリシーと組織関連のリスク」では“SaaS, PaaS, IaaS のロックイン”つまり“特定の事業者のサービスに処理を依存する結果，その事業者への依存から離れられなくなること”や“サプライチェーンにおける障害”などがあげられている．また，「技術調達のリスク」では“クラウドプロバイダ従事者の不正―特権の悪用”や“利用者側の強化手順と，クラウド環境との間に生じる矛盾”など，クラウド利用者側からの視点でクラウドプロバイダに関するリスクがあげられている．「法的なリスク」では情報漏洩事故発生時に開示すべき“電子的証拠”の取り扱い，国をわたっての“司法管轄の違いからくるリスク”などがあげられている．そして「クラウドに特化していないリスク」では従来から存在する重要なリスクとして除外できない問題である“ネットワークの途絶”，“特権の拡大”，“ソーシャルエンジニアリング”などがあげられているが，クラウドサービスを利用する場合には大いに注意すべきリスクである．

一方脆弱性については「クラウドに特化した脆弱性」と「クラウドに特化しない脆弱性」の二つに大別されている．「クラウドに特化した脆弱性」はクラウドプロバイダの視点で考えられており，特徴的なことには，利用者要求による“過剰な SLA 要求からのビジネスリスク”や“複数利害関係者間で矛盾する SLA 条項”，“利用者に監査または認証の証明書が提供されない問題”などがあげられている．「クラウドに特化しない脆弱性」では“プロバイダの選定不備”や“プロバイダによる NDA 違反”などがあげられている．つまり，クラウド利用者とクラウドプロバイダは相互にリスクにも脆弱性にもなり得ることが想定される．こうした分類においてクラウド利用者は，何が自己の責務に含まれるかを検証すべきとしている．

3. 2　CSA のクラウドセキュリティ・ガイダンス

クラウドセキュリティアライアンス（Cloud Security Alliance 本拠地：米国ワシントン州ファーンデール，以下 CSA と呼ぶ）はセキュリティの啓発のため，クラウドコンピューティングの適切な利用を促進することをミッションとして 2008 年に米国で設立された．2010 年 6 月には日本支部が開設された．

2009 年 4 月，クラウドセキュリティ・ガイダンス（Security Guidance for Critical Areas of Cloud Computing）が CSA より発表された[2]．クラウドセキュリティ・ガイダンスは「Ⅰ 導入・実装ハンドブック編」と「Ⅱ 法律問題編」の 2 部構成になっている．前者では従来の情報セキュリティマネジメントシステムのリスクアセスメントレベルで“クラウドにおける脅威”，“クラウド・リスク分析”を“資産からのリスクの識別”から留意すべきこととしている．CSA ではクラウドコンピューティングの問題点として「クラウドコンピューティングの不正および犯罪目的の利用」「安全ではないインターフェースおよび API」「悪意ある内部者」「共有技術問題」「データ消失または漏洩」「アカウントもしくはサービスのハイジャック」「未知のリスクのプロフィール」の七つを上げており，より詳細なものとして ENISA の報告書を指している．これらの問題点を考察する時に，最終的には，利用者の有している IT セキュリティポリシーと統合されなければならないとしており，クラウド利用者を主体としている．「クラウド事業者の選択」では，クラウド事業者がどのようなレベルのサービスを実際に提供するのか，客観的な評価がなされるべきとしている．また，「技術的対応策」として SaaS，PaaS，IaaS を区別してリスクを解説している．

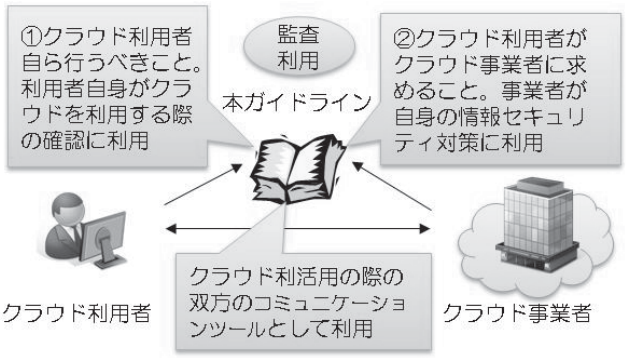
後者の「Ⅱ 法律問題編」では e-Discovery，民事，不正競争防止法などから言及するのはもちろんであるが，ネットワークセキュリティの問題，仮想化技術から発生する問題点，フォレンジック的な問題点があげられている．

3. 3　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

日本においてもクラウドサービスの利用促進のために 2011 年 4 月に経済産業省より「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」が公表された[3]．JISQ27002 をベースにクラウド利用者がクラウドサービスを利用する際に考慮する情報セキュリティガイドラインとし，図 1 に示すようにクラウド利用者が実践すべき対策とクラウド事業者に求めるべき対策の二つの視点をとりあげている．

クラウド利用者は主に入力と出力を，クラウド事業者は演算と保存を分担するものとして，情報セキュリティガバナンスのフレームワークを構成する．JISQ27002 では業務を行う適用範囲の全ての従業員の参加を求めているが，クラウドサービスでは重要な要素を預かる外部要員によって複雑に構成され JISQ27002 の管理策に関わることも想定される．

クラウドコンピューティングでは SaaS，PaaS，IaaS で構成されるサプライチェーンが形成される．すなわち SaaS 事業者は PaaS の利用者となり，PaaS の事業者が IaaS の利用者になることもある．よって，CSA と同じくクラウド利用者，クラウド事業者が関わりサプライチェーンを形成するクラウドのセキュリティマネジメントが考慮されている．付属書として，表 1 を例としたリスクアセスメントのマトリクス例があげられており，クラウド利用者，クラウド事業者それぞれに対する管理の可否が割り付けられている．



（出典：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の公表～クラウドサービスの安全・安心な利用に向けて～[3]）

図 1　情報セキュリティマネジメントガイドラインの利用方法の例

表 1　PaaS におけるシステム管理面における管理の可否（例）

対象（クラウド上）		PaaS利用者			クラウド事業者		
		一般ユーザ	アプリケーション開発者	ユーザ管理者	運用担当者	開発技術者	責任者
ユーザアプリケーション	操作	●	–	–	–	–	–
	設定	●	–	–	–	–	–
	ログ閲覧	–	–	●	–	–	–
ID管理	操作	–	–	●	–	–	–
	設定	–	–	●	–	–	–
	ログ閲覧	–	–	●	–	–	–
API	操作	–	●	–	–	–	–
	設定	–	●	–	–	–	–
	ログ閲覧	–	●	–	–	–	–
実行環境	操作	–	–	–	●	–	–
	設定	–	–	–	–	●	–
	ログ閲覧	–	–	–	●	●	–
OS	操作	–	–	–	●	–	–
	設定	–	–	–	–	●	–
	ログ閲覧	–	–	–	●	●	–
ファイアウォール	操作	–	–	–	–	●	–
	設定	–	–	–	–	●	–
	ログ閲覧	–	–	–	●	●	–
仮想マシン	操作	–	–	–	–	●	–
	設定	–	–	–	–	●	–
	ログ閲覧	–	–	–	●	●	–
ホストマシン	操作	–	–	–	–	●	–
	設定	–	–	–	–	●	–
	ログ閲覧	–	–	–	●	●	–

（出典：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の公表～クラウドサービスの安全・安心な利用に向けて～[3]）

クラウドセキュリティの実施は複雑化し，クラウドサービスの普及を一層困難にすると思いがちであるが，こうしたガイダンスをベースに，利用者のポリシーを持って管理方針を明確にし，SLA で責任を示せば，クラウドセキュリティマネジメントの役割を明確にできる．

4. ワークスタイル変革実践のためのセキュリティマネジメントとは

ワークスタイル変革の種類には在宅勤務，フリーアドレス，サテライトオフィスなど業務を行う場所での区別と，モバイル PC，シンクライアント，あるいは仮想デスクトップや USB 型認証キーデバイスなどの利用機器での区別が考えられる．その多くは業務を従来通りのオフィスの固定場所ではなく外部で実施し，業務アプリケーションはクラウドの構成をとるものが多い．そのためクラウドが構成するサプライチェーンやリスクを考慮しなければならない．クラウドセキュリティマネジメントにワークスタイルそれぞれのセキュリティポリシーを考慮し検討しなければならないとなると，更に複雑な運用管理になることが想像される．しかしながら，クラウド利用者がクラウドセキュリティを認識し，クラウド事業者に対しクラウドセキュリティを適切に管理させれば，クラウドガイダンスにあるようなクラウド事業者までのリスクマネジメントが可能である．

すなわち，ワークスタイルはクラウド利用者側の環境に大きく依存する．よって本章では各ワークスタイル環境を意識して経済産業省の情報セキュリティマネジメントガイドラインの章立てに沿い，クラウド利用者としての視点から，エンドポイント[*1] でのリスクや対策の必要性を考える．

4.1 情報セキュリティ基本方針

従来の ISMS でのセキュリティを念頭に以降の管理策においてはワークスタイル毎に利用の方針を決める必要がある．

4.2 情報セキュリティのための組織

ワークスタイル毎に自己が負う責任と，クラウド事業者など関連する者が負う責任を SLA などで明確にし，サポート窓口を明確にする必要がある．また，事業継続を考慮しサプライチェーンを認識する必要がある．

4.3 資産の管理

情報資産は目録を作成し，機密度に応じて持ち出し可能なデータ，業務エリア外で閲覧可能なデータなどと明示することが望まれる．サテライトオフィスや在宅時など，ある程度閉塞された場所であればまだ良いが，屋外など関わる第三者が特定できない場合には，持ち出すデータを制限する必要がある．場合によっては利用者が削除したデータであってもサプライチェーンのどこかで保管されていることもある．情報データのライフサイクルとして所有権や分類，ガバナンス構造を意識するため，クラウド事業者が管理する場合にはその取り扱いについても SLA などで明示した方が良い．現在，クラウド事業者が情報データを取り扱う場合にデータを分散し，一台のクラウドサーバからではデータとして意味をなさないように，データを解釈できなくする秘密分散などの技術も考えられている．二台に限らず複数台でパリティストライプセットを形成すれば，事業継続にも役立つ．仮想化の進展で効果を期待できる技術である．

4.4 人的資源のセキュリティ

機器に対する管理が厳重であっても，人的リスクの完全な回避はできない．パスワード管理，情報へのアクセスなど，より徹底して周知する必要がある．

4.5　物理的及び環境的セキュリティ

ISMS では業務を行う適用範囲を重視するため，ワークスタイルによる業務範囲は特に重要な要素であると考えられる．サテライトオフィスや業務エリアを明確にしたフロアなどのフリーアドレスでの業務であれば，施錠管理，入退出管理など物理面での管理が比較的明確であるが，在宅勤務の場所や外出先での利用は第三者の目にふれることがないことなど人的な面での考慮が必要になる．在宅勤務であれば窓の外から覗かれることがないこと，例え家族であっても業務内容が見られないようにすること，機器を施錠管理することなどをポリシーに入れることが望ましい．外出先であれば，データを保管しないシンクライアント機器や USB 型認証キーデバイスであっても，電車内や人の多い場所での利用は覗き見などに注意が必要である．

4.6　通信及び運用管理

利用する通信システムは誤用のないよう設定を確実にし，クラウドサービスでネットワーク構成を提供する事業者に対しサービスレベルの維持を確認することが必要である．利用する機器に OS がある場合はパッチ管理，利用するソフトウエアの管理が必要であるが，集中管理ができない場合には適切な運用管理に懸念が残る．一方，仮想デスクトップのサーバ OS の場合，クラウド事業者がパッチを管理することになるが，適切な時間にすみやかに行わないと利用時にリスクが及ぶこともある．また複数の仮想サーバを保有する場合に脆弱性が発覚すればリスクが拡散し対応が遅れる懸念がある．さらに，仮想デスクトップはサーバの設定によってはロールバック時に古いパターンファイルなどが戻ってしまう危険も考えられる．いずれにせよ脆弱性対策は方針を明確にし，利用者は最新の情報を認識する必要がある．情報の交換，媒体の利用に関するセキュリティ対策は従来と同様に重要であり必須である．

4.7　アクセス制御

アクセス制御はクラウドや仮想化などでは特に重要な課題となる．クラウドではサプライチェーンが複雑になると，全ての運用管理時点でアクセス制御のポリシーが守られていることを確実にするのが困難である．例えエンドポイントで複雑なパスワード管理を行っていても，ある時点で脆弱なパスワード利用があれば全体のリスクとなることも考えられる．アクセス制御のポリシーはサプライチェーンにおいてどうあるべきか明確にしなければならない．

またシンクライアント機器や仮想デスクトップ，USB 型認証キーデバイスにいたってはログインする ID やパスワードが全てのキーとなる．もし第三者の目にふれることがあれば致命的なリスクとなる．複雑なパスワード利用や変更管理，また二要素パスワードやワンタイムパスワードの利用なども検討すべきである．

ISMS の詳細事項には「モバイルコンピューティング＆テレワーキング」の項目があるが，ここで求められているものはまさにその正式な利用方針である．

4.8　情報システムの取得，開発及び保守

ここではデータの取り扱いや，クラウドをまたがるサプライチェーンの場合の暗号化などの問題が考えられるが，パブリッククラウドで必ず取り上げられるのは保管される国の法律である．安価なクラウドサービス利用時は特に現地のプライバシーに関する保護規定が懸念となる．情報の保管場所は機密度に応じ適切な事業者に保管されるよう契約する必要がある．また，

データを保管する場合の暗号技術についても国によっては法律で利用が禁じられることも考慮しなければならない．

4. 9　情報セキュリティインシデントの管理

情報セキュリティインシデントが発生した場合には管理するサプライチェーンが複雑になるほど発生原因を特定し，責任を追及すること，またインシデント対応を行うことが困難になる．仮想サーバにおいては侵入検知などの対応が取れていることがクラウド事業者に対する条件としてSLAに明示することも必要である．アクセス制御に関わるアイデンティティについては万が一に第三者に知られたならばクラウド事業者には識別することはできないため，利用者は管理の認識と事故発生時の早急な対応が重要であることを認識しておく必要がある．

4. 10　事業継続管理

事業継続はクラウドセキュリティの中でも重要な要素になると考えられる．機密性も重要であるが，可用性の確保が更に重要である．機密性はデータの取り扱い，事件発生時のインシデント管理として追求や対応手順を明確にしなければならないが，サプライチェーンの輪が途切れた時に業務ができなくなることを念頭に，中断すると問題となる業務の可用性を高めるには，遮断時に変更可能な経路まで考慮する必要があるかもしれない．クラウド事業者にとっては災害発生時に確保できる上限を明示し，有事のときの切り替えなどの顧慮をする必要もある．利用者もクラウドが利用できない場合の代替策を考える必要があるだろう．

4. 11　順守

国による法令はデータにおいて重要なポイントとなること，暗号化やプライバシーなどの取り扱いについて4. 8節で述べたが，米国e-discovery法などではインシデント対応のため情報データの開示を求められることもある．パブリッククラウドにおいて情報データの取り扱いは利用する地域の法令にも注意せねばならない．

5.　今後の技術，ワークスタイルによるセキュリティ対策

ワークスタイル変革に関わるものとして，スマートフォンやタブレット型コンピュータの普及が影響していくと考えられる．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」では「モバイルのコンピューティング及び通信」に留意するよう記載されているが，現在利用者が増えており仮想化でのワークスタイルとしても期待されている．スマートフォンではデータの保管，メールのやり取り，WEB閲覧の他，アプリケーションをダウンロードし利用するなど従来のコンピュータと同レベルの機能が可能となってきたが，既にマルウエアなどの攻撃も発見されており，リスクが高まってきている．こうした背景においてスマートフォンはコンピュータ機器と同様のセキュリティ対策ではリスク対応が実現できないとし，NPO日本ネットワークセキュリティ協会では「スマートフォン活用セキュリティガイドラインβ版－スマートフォンの安全な利活用のすすめ」[4]を2011年4月に公表した．クラウドのガイドラインが作られる一方こうした新たなガイドラインも発表されている．

その他にもTV会議システム，WEB会議システムなど業務のスタイルはまだ変革しつつある．次の段階では機能分化するセキュリティマネジメントの体系を追求する必要があるかもし

れない.

6. お わ り に

情報セキュリティが障害となり，新たなビジネスに進むことができないという言葉が時々聞かれる．しかし情報セキュリティ以前にビジネス目標が明らかでなければならない．その次にビジネス目標を達成するためのリスクを洗い出し，初めて情報セキュリティ対策を検討することができる．情報セキュリティガバナンスはビジネスガバナンス，IT ガバナンスとともにあって成り立つものであり，先行して単独で行われるものではない.

また，情報セキュリティルールは単に規則で縛るものではなく，利用者とそのステークホルダーを守るためのものであることを理解していただきたい．クラウドの技術は悲しいことにダーククラウドと呼ばれる悪意のある方向性にも発展している．悪意のある利用者のターゲットは多くの利用者が求めるものに対し，未発覚の脆弱性の要素を突いたものであることが多い.

ソーシャルネットワーク，スマートフォン，あるいは更なる新たな技術に対して，顕在化していくリスクを注視し，最適な情報セキュリティ対策を検討し組み込んでいく，そして利用者に広く周知することによってワークスタイル変革の未来を期待することができると考える.

＊ 1　ネットワークに接続された PC やシンクライアント，スマートフォンなど，末端のデバイスの総称である.

参考文献
［1］「欧州 ENISA のクラウドのセキュリティに関するガイドラインの翻訳」，独立行政法人情報処理推進機構，2010 年 10 月，http://www.ipa.go.jp/security/publications/enisa/index.html
［2］「クラウドセキュリティ・ガイダンス」，日本クラウドセキュリティアライアンス，2010 年 6 月，http://www.cloudsecurityalliance.jp/report/10kaisetsu.pdf
［3］「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の公表」，経済産業省商務情報政策局情報セキュリティ政策室，2011 年 4 月，http://www.meti.go.jp/press/2011/04/20110401001/20110401001.html
［4］「スマートフォン活用セキュリティガイドライン β 版－スマートフォンの安全な利活用のすすめ」，NPO 日本ネットワークセキュリティ協会，2011 年 4 月，http://www.jnsa.org/result/2010/smap_guideline_Beta.pdf
［5］ Tim Mather，Subra Kumaraswamy，Shahed latif，（下道 高志 監訳）「クラウドセキュリティ ＆ プライバシー ―リスクとコンプライアンスに対する企業の視点」，オライリー・ジャパン，2010 年 6 月
［6］ NRI セキュアテクノロジー，「クラウド時代の情報セキュリティ」，日経 BP 社，2010 年 10 月
［7］ 佐々木 俊尚，「仕事をするのにオフィスはいらない」，株式会社光文社，2009 年 7 月

※上記参考文献に挙げた URL は 2011 年 7 月 4 日時点での存在を確認.

執筆者紹介　中　村　彰　子（Shoko Nakamura）
日本ユニシスグループの ISMS 認証取得開始に伴い 2004 年 4 月より情報セキュリティマネジメント業務に従事し，現在は日本ユニシスグループ情報セキュリティ企画部門として各種施策を担当している．公認情報セキュリティ主任監査人（CAIS），公認情報システム監査人（CISA），公認情報セキュリティマネージャ（CISM），Certified in Risk and Information Systems Control（CRISC）