クラウドサービスを
利用するための考察

2013年3月29日

企業内ITC・ITガバナンス研究会

はじめに

既にわが国においてもクラウドコンピューティングのビジネスが活発化してきている。

東日本大震災の被災地では、基幹業務のサーバーが何らかの被害を受けて使用不能になったり、情報の利用が困難になったりして、情報資産のダメージを生じるケースが多数発生し、改めてビジネスリカバリー対策として注目されている。

クラウドであれば、ネットワークさえつながればすぐにでも再利用が可能で、ビジネスの立ち上がりが早いことが期待できるからである。当然サービスを提供するメーカーやベンダーもビジネスチャンスと捉え、売り込みに躍起になっている。

企業内 ITC・IT ガバナンス研究会として、今年度はクラウドコンピューティングを利用するにあたって予想されるビジネス上のリスクを、情報リスクに伴うリスクを防止するという視点に立って研究を進めることとした。

2013年3月

執筆者　一同

執筆メンバー　ITガバナンス研究会

千枝　和行　　(0029302004C)
坂本　徳明　　(0064952006C)
牧田　一雄　　(0052712005C)
古川　正紀　　(0005462001C)
山﨑　直和　　(0035252003C)
久住　昭之　　(0035712003C)
瀬戸　昭彦　　(0065252006C)

(注)本記載内容は、ITコーディネータ個人としての見解を述べたものであって、個人が所属する企業・団体としての見解を述べたもので無いことをお断りします。
また、本書において使用しているシステム名や製品名などで各メーカー等の登録商標を使用している部分があるが、文中においては TM、コピーライト表記はしておりません。

目次

2012年度研究レポート

情報リスクからみたクラウドサービスを利用する為の対策の研究
～ ビジネスリスクを軽減するために ～

千枝 和行

平成24年3月15日

情報リスクからみたクラウドサービスを利用する為の対策の研究
～　ビジネスリスクを軽減するために　～

ＩＴガバナンス研究会
千枝　和行

１．はじめに

クラウドコンピューティングが広く知れ渡り、特別な仕組みという認識ではなく、お金の保管に銀行を利用するように、当たり前に情報システムやＩＴ資源を利用できることが理解されつつあり、情報利用形態の大きなパラダイムシフトが進みつつある。大いに歓迎すべきトレンドであると評価する。特に企業体力の弱い中小企業にとっては、経営資源の効率的運用を考える上で大きな効果が期待される。

一方、銀行に例えるなら、現金の強奪、あるいはお金を奪い取ることを目的とした詐欺的な行為などは後を絶たない。対策を練っても、手を変え品を変え管理の弱い部分を狙って、新たなリスクが発生し続けている。情報システムにも同様なことが言え、各企業・官公庁もインシデント発生に伴う対策に追われるのが現状である。経営の効率化・体質強化が期待されるＩＴ技術である反面、情報リスクに伴う経営リスクに繋がる危険性をはらんでいる。

本ＩＴガバナンス研究会もクラウドコンピューティングの利用研究に関しては３年目を迎え、以下の点を考慮し本年度の研究テーマを探索した。

① 初年度はクラウドコンピューティングの実態とそれを利用する側の考慮点を踏まえながら、導入を考えている利用者に対し、考慮すべき点を中心に研究結果を述べた。
② ２年目は、前年度の利用点を踏まえ、その前提となる経営者への答申の仕方や、考慮すべき経営上及びＩＴ利用上の周辺の知識について研究結果を言及した。

本年度は、上記の内容を踏まえた上で、クラウドコンピューティングを利用するにあたって想定されるビジネス上のリスクを、情報リスクに伴うリスクを防止するという視点に立って研究を進める事とした。検討資料として経済産業省が取りまとめた「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」を考慮しながら、各研究員の得意とする視点に基づいて、クラウドサービスの活用を有効ならしめるための情報セキュリティ対策について研究結果を述べる事とする。

クラウドコンピューティング特徴をＱＣＤ（早い、美味い、安いの吉野家）的に表現すると、

①早い　　・システム立ち上げの短縮化
②美味い　・業務の可視化（モニタリング）
　　・ソフトの柔軟化（選択肢）
　　・ビジネスの安全化
　　・品質チェックの義務化（不味い）
③安い　　・費用のスケーラブル化

そして

④新しい　・コンピュータ資源（業務規模）のスケーラブル化

であり、情報技術を中心としたビジネス再構築を行う上で、効果測定すべき項目と考えている。

一方、利用する企業側は新技術とはいえど経営統制（ガバナンス）の一環として機能

していなければビジネスリスクを負うことになり、それが実際に発生した場合には経営上のインパクトが大きいことが想定される。

読者諸兄も既にお気づきと思うが、クラウドコンピューティングだからと言って、情報セキュリティに関する特別な技術が存在するわけではなく、既存の規制基準や対策を拡張適用すれば、殆どのインシデントケースをカバーできると考えている。

問題は、そのような対策、つまりセキュリティポリシーの制定、情報セキュリティ基準の制定、経営者による承認と全社普及、情報セキュリティを管理する組織の制定と運用など、必要な措置が体系的に取られていないケースが存在した場合である。その様なケースでも、クラウドサービスを利用することを契機に、情報セキュリティ体制を整えれば宜しいわけで、その意味でも従前の情報セキュリティ解説と重なる部分があることを承知の上で、あえて各研究員が得意とする知識・経験を加味し、必要事項を満載した。勉強方々、参考にしてもらえたらうれしい限りである。

以上の通り、本稿は前年度の研究に引き続き、情報インシデントに注目しながら情報セキュリティリスクとビジネスリスクの観点から論ずることとする。

尚、リスクの捉え方は各研究員の自由研究とし、統一した視点やテーマ或いは方法論は設定しないこととした。

2．クラウドコンピューティング情報リスク

クラウドコンピューティング導入の際に、検討しなければならない情報リスクを以下に例示する。

・経営環境面

事象	具体的現象	想定される原因	ビジネス課題	セキュリティガイド
ソフトウェア動作不良による情報連携の失敗	業務システム間で必要な情報の受け渡しができず、業務停止に陥り、ステークホルダーに迷惑をかけた	業者の経験不足 未経験の現象発生	契約上の縛り（ＳＬＡ） 事前の動作確認 ステークホルダー対応	6.2.3（契約） 10.1.2（変更管理）
クラウドシステム停止のリスク	原因不明のトラブルでクラウドシステムが停止することにより業務が停止し、ステークホルダーに迷惑をかけた	業者の経験不足 未経験の現象発生 技術的限界	契約上の縛り（ＳＬＡ） ステークホルダー対応 情報の分散化	6.2.3（契約）
ビジネス復旧の遅延のリスク	災害発生時にシステムの普及が遅れ、ビジネス復旧に影響が出て、ステークホルダーに迷惑をかけた	業者の経験不足 未経験の現象発生 技術的限界	リカバリーシステムの徹底 ステークホルダー対応 情報の分散化 重要情報のバックアップ対策	6.2.3（契約） 10.5.1（バックアップ）

・システム環境面

事象	具体的現象	想定される原因	ビジネス課題	セキュリティガイド
設置先へのサイト攻撃	悪意のあるサイト攻撃により、システムが停止することによって業務が停止し、ステークホルダーに迷惑をかけた	設置場所でのサイト攻撃対策の不徹底	契約上の縛り（ＳＬＡ） ステークホルダー対応 広報活動 情報の分散化	6.2.3（契約） 10.1.1（操作手順書） 13.1.1（事象の報告）

新型ウィルスの攻撃	悪意のあるウィルス攻撃によりシステムが停止、若しくは情報漏えいが発生することによって情報が流出し、ステークホルダーに迷惑をかけた	設置場所でのウィルス対策の不徹底	契約上の縛り（ＳＬＡ） ステークホルダー対応 広報活動 コード埋め込みの禁止措置 ウィルスバスターの更新 ネットワークの保全	10.1.1（操作手順書） 10.2.2（第三者が提供） 10.4.1（悪意あるコー） 10.5.1（バックアップ） 10.6.2（ネットワーク） 13.1.1（事象の報告）
設置場所での機密情報漏えいのリスク	自社の情報が闇市場で売買され、ステークホルダーに迷惑をかけた	設置場所の管理者による悪用	契約上の縛り（ＳＬＡ） ステークホルダー対応 広報活動 従業員教育の徹底 当該従業員の処罰 犯罪者への刑事訴訟	6.2.3（契約） 8.1.3（雇用条件） 8.2.2（教育訓練） 8.2.3（懲戒手続） 8.3.2（資産の返却） 13.1.1（事象の報告）

・利用環境面

事象	具体的現象	想定される原因	ビジネス課題	セキュリティガイド
業務推進遅延のリスク	一旦停止したシステムが想定時刻内にシステムが復旧せず業務が再開できない	業者の経験不足 未経験の現象発生 技術的限界	契約上の縛り（ＳＬＡ） 情報の分散化 業務形態の分散化	6.2.3（契約） 13.1.1（事象の報告）
利用レスポンスの遅延	必要時間内にレスポンスが返ってこず、業務に遅延が発生する	業者の経験不足 性能の限界	契約上の縛り（ＳＬＡ） 情報の分散化 複数業者への分散化	6.2.3（契約） 13.1.1（事象の報告）

・情報環境面

事象	具体的現象	想定される原因	ビジネス課題	セキュリティガイド
情報喪失リスク	自社の情報が闇市場で売買され、ステークホルダーに迷惑をかけた	業者の経験不足 技術的限界	情報資産の回収 ステークホルダー対応 広報活動	7.1.1（資産目録） 7.1.2（管理責任者） 7.1.3（利用の許容範囲）

			情報の定期的廃棄	7.2.2　情報のラベル付け

3．クラウドコンピューティング利用時の情報リスク対策

クラウドコンピューティング導入・運用など利用の際に、検討しなければならない情報リスクと対策を「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」の条文からピックアップし、解説を交えた文章を、以下に例示する。

クラウドコンピューティング利用時の情報セキュリティ対策	
領　域	クラウドコンピューティングの経営環境面
事　象	ソフトウェア動作不良による情報連携の失敗
具体的現象	特にミドルウェアの動作不良による情報連携の失敗： 業務システム間で必要な情報の受け渡しができず、業務停止に陥り、ステークホルダーに迷惑をかけた。
想定される原因	業者の知識不足、経験不足。
ガイドライン	6.2.3　第三者との契約におけるセキュリティ クラウド利用者は，組織の情報若しくは情報処理施設が関係するアクセス・処理・通信・管理にかかわる第三者との契約，又は情報処理施設に製品・サービスを追加する第三者との契約に，クラウドサービスの利用契約が含まれるものとして考えることが望ましい。 クラウド利用者は，クラウドサービスへのセキュリティ要求事項を明確化し，自組織のセキュリティ要求事項をすべて満たしているか，契約に含有されているかを確認する事が望ましい。また，クラウド事業者との契約を比較した結果が経営陣（又は情報セキュリティ委員会）に承認されていることが望ましい。 【ポイント：情報管理システムを第三者に委託する場合に、契約により遵守すべき情報セキュリティ事項を明確にすることを確認する】 10.1.2　変更管理 クラウド事業者は，クラウドサービスの情報処理設備及びシステムの変更において，クラウド利用者に影響を及ぼすものは，クラウド利用者に事前に通知することが望ましい。クラウド事業者は，クラウドサービスの情報処理設備及びシステムの変更においてクラウド利用者に通知する項目並びに変更履歴を，クラウドサービスの利用を検討する者及びクラウド利用者に明示することが望ましい。 【ポイント：クラウド事業者がソフトウェア・ミドルウェアの正常な動作はもちろんのこと、ソフトウェア、ハードウェアの変更管理に関する十分な経験と知識を有する事を確認する】
備　考	

平成 24 年 3 月 15 日

クラウドコンピューティング利用時の情報セキュリティ対策	
領　域	クラウドコンピューティングの経営環境面
事　象	クラウドシステム停止のリスク
具体的現象	クラウドシステムのサービス停止による業務停止： 原因不明のトラブルでクラウドシステムが停止することにより業務が停止し、ステークホルダーに迷惑をかけた。
想定される原因	業者の経験不足。 技術的限界。
ガイドライン	6.2.3　第三者との契約におけるセキュリティ クラウド利用者は，組織の情報若しくは情報処理施設が関係するアクセス・処理・通信・管理にかかわる第三者との契約，又は情報処理施設に製品・サービスを追加する第三者との契約に，クラウドサービスの利用契約が含まれるものとして考えることが望ましい。 クラウド利用者は，クラウドサービスへのセキュリティ要求事項を明確化し，自組織のセキュリティ要求事項をすべて満たしているか，契約に含有されているかを確認する事が望ましい。また，クラウド事業者との契約を比較した結果が経営陣（又は情報セキュリティ委員会）に承認されていることが望ましい。 【ポイント：情報管理システムを第三者に委託する場合に、契約により遵守すべき情報セキュリティ事項を明確にすることを確認する】
備　考	

平成 24 年 3 月 15 日

クラウドコンピューティング利用時の情報セキュリティ対策	
領　域	クラウドコンピューティングの経営環境面
事　象	ビジネス復旧の遅延のリスク
具体的現象	決められた時間内のシステム復旧の失敗： 災害発生時にシステムの普及が遅れ、ビジネス復旧に影響が出て、ステークホルダーに迷惑をかけた。
想定される原因	業者の経験不足。 技術的限界。
ガイドライン	6.2.3　第三者との契約におけるセキュリティ クラウド利用者は，組織の情報若しくは情報処理施設が関係するアクセス・処理・通信・管理にかかわる第三者との契約，又は情報処理施設に製品・サービスを追加する第三者との契約に，クラウドサービスの利用契約が含まれるものとして考えることが望ましい。 クラウド利用者は，クラウドサービスへのセキュリティ要求事項を明確化し，自組織のセキュリティ要求事項をすべて満たしているか，契約に含有されているかを確認する事が望ましい。また，クラウド事業者との契約を比較した結果が経営陣（又は情報セキュリティ委員会）に承認されていることが望ましい。 【ポイント：情報管理システムを第三者に委託する場合に、契約により遵守すべき情報セキュリティ事項を明確にすることを確認する】 10.5.1　情報のバックアップ クラウド事業者は，クラウド利用者が求める情報，ソフトウェア及びソフトウェアの設定において，クラウド利用者がバックアップ手順を策定できるように情報を提供することが望ましい。 【ポイント：クラウド事業者が必要なバックアップ手段を有し、実施できる事を確認する】
備　考	

平成 24 年 3 月 15 日

クラウドコンピューティング利用時の情報セキュリティ対策	
領　域	クラウドコンピューティングのシステム環境面
事　象	クラウド事業者へのサイト攻撃
具体的現象	悪意あるサイト攻撃による業務妨害： 悪意のあるサイト攻撃により、システムが停止することによって業務が停止し、ステークホルダーに迷惑をかけた。
想定される原因	設置場所でのサイト攻撃対策の不徹底。
ガイドライン	6.2.3　第三者との契約におけるセキュリティ クラウド利用者は，組織の情報若しくは情報処理施設が関係するアクセス・処理・通信・管理にかかわる第三者との契約，又は情報処理施設に製品・サービスを追加する第三者との契約に，クラウドサービスの利用契約が含まれるものとして考えることが望ましい。 クラウド利用者は，クラウドサービスへのセキュリティ要求事項を明確化し，自組織のセキュリティ要求事項をすべて満たしているか，契約に含有されているかを確認する事が望ましい。また，クラウド事業者との契約を比較した結果が経営陣（又は情報セキュリティ委員会）に承認されていることが望ましい。 【ポイント：情報管理システムを第三者に委託する場合に、契約により遵守すべき情報セキュリティ事項を明確にすることを確認する】 10.1.1　操作手順書 クラウド事業者は，クラウド利用者のクラウドサービスとして提供する仮想システム基盤についての操作手順の作成に協力することが望ましい。 【ポイント：サイト攻撃を受けたときの手順が明確に記載されていることを確認する】 13.1.1　情報セキュリティ事象の報告 クラウド事業者は，情報セキュリティインシデントを受け付ける窓口を設置することが望ましい。クラウド事業者は，クラウドサービス自体のトラブル発生時でも情報セキュリティインシデントに対応できる窓口を運用することが望ましい。 【ポイント：クラウド事業者にサイト攻撃があった場合の利用者への報告体制が取られている事を確認する】
備　考	

平成 24 年 3 月 15 日

クラウドコンピューティング利用時の情報セキュリティ対策	
領　域	クラウドコンピューティングのシステム環境面
事　象	クラウド事業者への新型ウィルスの攻撃
具体的現象	新型ウィルスの攻撃： 悪意のあるウィルス攻撃によりシステムが停止、若しくは情報漏えいが発生することによって情報が流出し、ステークホルダーに迷惑をかけた。
想定される原因	設置場所でのウィルス対策の不徹底。
ガイドライン	6.2.3　第三者との契約におけるセキュリティ クラウド利用者は，組織の情報若しくは情報処理施設が関係するアクセス・処理・通信・管理にかかわる第三者との契約，又は情報処理施設に製品・サービスを追加する第三者との契約に，クラウドサービスの利用契約が含まれるものとして考えることが望ましい。 クラウド利用者は，クラウドサービスへのセキュリティ要求事項を明確化し，自組織のセキュリティ要求事項をすべて満たしているか，契約に含有されているかを確認する事が望ましい。また，クラウド事業者との契約を比較した結果が経営陣（又は情報セキュリティ委員会）に承認されていることが望ましい。 【ポイント：情報管理システムを第三者に委託する場合に、契約により遵守すべき情報セキュリティ事項を明確にすることを確認する】 10.1.1　操作手順書 クラウド事業者は，クラウド利用者のクラウドサービスとして提供する仮想システム基盤についての操作手順の作成に協力することが望ましい。 【ポイント：ウィルス攻撃を受けたときの手順が明確に記載されていることを確認する】 10.2.2　第三者が提供するサービスの監視及びレビュー クラウド事業者は，クラウドサービスにおいて，第三者が提供するサービス，報告及び記録を，常に監視し，レビューすることが望ましい。 クラウド事業者は，クラウドサービスにおいて，第三者が提供するサービスを，監査することが望ましい。 クラウド事業者は，提供しているクラウドサービスにおいて，第三者が提供するサービス，報告及び記録を，常に監視し，レビューしていることを開示することが望ましい。 クラウド事業者は，提供しているクラウドサービスにおいて，第三者が提供するサービス，報告及び記録を，常に監視し，レビューした記録を，クラウド利用者に明示することが望ましい。

	クラウド事業者は，提供しているクラウドサービスにおいて，第三者が提供するサービスを，監査していることを開示することが望ましい。 クラウド事業者は，提供しているクラウドサービスにおいて，第三者が提供するサービスを監査した結果をまとめた報告書等を，クラウド利用者に提示することが望ましい。 【ポイント：第三者が提供するサービスが、ウィルス攻撃の温床になっていないことを確認する】 10.4.1　悪意のあるコードに対する管理策 クラウド事業者は，クラウドサービスの提供において，悪意のあるコードへのクラウド事業者の責任範囲と，クラウド利用者の責任範囲を明らかにすることが望ましい。 クラウド事業者は，クラウドサービス内で，悪意のあるコードからクラウドサービスの利用者を保護するために，検出，予防及び回復のための管理策，並びにクラウド利用者に適切に意識させるための手順を実施することが望ましい。 【ポイント：ウィルス攻撃に対する対策が施されていることを確認する】 10.5.1　情報のバックアップ 情報及びソフトウェアのバックアップは，合意されたバックアップ方針に従って定期的に取得し，検査することが望ましい。 【ポイント：情報の破壊が確認された場合に、その情報をリアルタイムに修復する機能があることを確認する】 10.6.2　ネットワークサービスのセキュリティ すべてのネットワークサービスについて，セキュリティ特性，サービスレベル及び管理上の要求事項を特定し，また，いかなるネットワークサービス合意書にもこれらを盛り込むことが望ましい。 【ポイント：システムへの不正侵入に対する対策が取られている事を確認する】 13.1.1　情報セキュリティ事象の報告 クラウド事業者は，情報セキュリティインシデントを受け付ける窓口を設置することが望ましい。クラウド事業者は，クラウドサービス自体のトラブル発生時でも情報セキュリティインシデントに対応できる窓口を運用することが望ましい。 【ポイント：クラウド事業者に新型ウィルス攻撃があった場合の利用者への報告体制が取られている事を確認する】
備　考	

クラウドコンピューティング利用時の情報セキュリティ対策	
領　域	クラウドコンピューティングのシステム環境面
事　象	設置場所での機密情報漏えいのリスク
具体的現象	設置先作業員による不正行為： 設置場所の作業員からの情報漏えいで、自社の情報が闇市場で売買され、ステークホルダーに迷惑をかけた。
想定される原因	設置場所の管理者による悪用。 設置場所の技術力不足。
ガイドライン	6.2.3　第三者との契約におけるセキュリティ 組織の情報若しくは情報処理施設が関係するアクセス・処理・通信・管理にかかわる第三者との契約，又は情報処理施設に製品・サービスを追加する第三者との契約は，関連するすべてのセキュリティ要求事項を取り上げることが望ましい。 【ポイント：情報管理システムを第三者に委託する場合に、契約により遵守すべき情報セキュリティ事項を明確にすることを確認する】 8.1.3　雇用条件 従業員，契約相手及び第三者の利用者は，契約上の義務の一部として，情報セキュリティに関する，これらの者の責任及び組織の責任を記載した雇用契約書に同意し，署名することが望ましい。 【ポイント：システム管理する従業員を雇用する際及び就業期間中に、当人に対し法令順守、企業規則遵守、顧客利益遵守等を認識していることを確認する】 8.2.2　情報セキュリティの意識向上，教育及び訓練 組織のすべての従業員，並びに，関係するならば，契約相手及び第三者の利用者は，職務に関連する組織の方針及び手順についての適切な意識向上のための教育・訓練を受け，また，定めに従ってそれを更新することが望ましい。 【ポイント：システム管理に従事する従業員に対し、定期的に情報セキュリティに関する教育訓練を実施する仕組みがあることを確認する】 8.2.3　懲戒手続 セキュリティ違反を犯した従業員に対する正式な懲戒手続を備えることが望ましい。 【ポイント：システム管理に従事する従業員がセキュリティ管理に反する行為を行った場合に、懲戒手続きが存在することを確認する】 8.3.2　資産の返却 クラウド事業者は，クラウドサービスにおいて，クラウドサービスの利用者が，

	雇用，契約又は合意の終了時に返却する資産を，クラウド利用者が管理できる機能を提供することが望ましい。クラウド事業者は，クラウドサービスにおいて，クラウドサービスの利用者が，雇用，契約又は合意の終了時に返却する。 資産を，クラウド利用者が管理できる機能について，クラウドサービスの利用を検討する者に明示することが望ましい。 【ポイント：システム管理に従事する従業員が、その雇用関係を終了した場合でも、セキュリティが守れることを確認する】 13.1.1　情報セキュリティ事象の報告 クラウド事業者は，情報セキュリティインシデントを受け付ける窓口を設置することが望ましい。クラウド事業者は，クラウドサービス自体のトラブル発生時でも情報セキュリティインシデントに対応できる窓口を運用することが望ましい。 【ポイント：クラウド事業者から情報漏えいがあった場合の利用者への報告体制が取られている事を確認する】
備　考	

平成 24 年 3 月 15 日

クラウドコンピューティング利用時の情報セキュリティ対策	
領　域	クラウドコンピューティングの利用環境面
事　象	業務推進遅延のリスク
具体的現象	システム停止による業務遅延： 一旦停止したシステムが想定時刻内にシステムが復旧せず業務が再開できず、ステークホルダーに迷惑をかけた。
想定される原因	業者の経験不足。 技術的限界。
ガイドライン	6.2.3　第三者との契約におけるセキュリティ クラウド利用者は，組織の情報若しくは情報処理施設が関係するアクセス・処理・通信・管理にかかわる第三者との契約，又は情報処理施設に製品・サービスを追加する第三者との契約に，クラウドサービスの利用契約が含まれるものとして考えることが望ましい。 クラウド利用者は，クラウドサービスへのセキュリティ要求事項を明確化し，自組織のセキュリティ要求事項をすべて満たしているか，契約に含有されているかを確認する事が望ましい。また，クラウド事業者との契約を比較した結果が経営陣（又は情報セキュリティ委員会）に承認されていることが望ましい。 【ポイント：情報管理システムを第三者に委託する場合に、契約により遵守すべき情報セキュリティ事項を明確にすることを確認する】 13.1.1　情報セキュリティ事象の報告 クラウド事業者は，情報セキュリティインシデントを受け付ける窓口を設置することが望ましい。クラウド事業者は，クラウドサービス自体のトラブル発生時でも情報セキュリティインシデントに対応できる窓口を運用することが望ましい。 【ポイント：クラウドシステムによるシステム復旧への遅延があった場合の利用者への報告体制が取られている事を確認する】
備　考	

平成 24 年 3 月 15 日

クラウドコンピューティング利用時の情報セキュリティ対策	
領　域	クラウドコンピューティングの利用環境面
事　象	利用レスポンスの遅延
具体的現象	システムレスポンス低下による業務遅延： 必要時間内にレスポンスが返ってこず、業務に遅延が発生する、ステークホルダーに迷惑をかけた。
想定される原因	業者の経験不足。 性能の限界。
ガイドライン	6.2.3　第三者との契約におけるセキュリティ クラウド利用者は，組織の情報若しくは情報処理施設が関係するアクセス・処理・通信・管理にかかわる第三者との契約，又は情報処理施設に製品・サービスを追加する第三者との契約に，クラウドサービスの利用契約が含まれるものとして考えることが望ましい。 クラウド利用者は，クラウドサービスへのセキュリティ要求事項を明確化し，自組織のセキュリティ要求事項をすべて満たしているか，契約に含有されているかを確認する事が望ましい。また，クラウド事業者との契約を比較した結果が経営陣（又は情報セキュリティ委員会）に承認されていることが望ましい。 【ポイント：情報管理システムを第三者に委託する場合に、契約により遵守すべき情報セキュリティ事項を明確にすることを確認する】 13.1.1　情報セキュリティ事象の報告 クラウド事業者は，情報セキュリティインシデントを受け付ける窓口を設置することが望ましい。クラウド事業者は，クラウドサービス自体のトラブル発生時でも情報セキュリティインシデントに対応できる窓口を運用することが望ましい。 【ポイント：クラウドシステムでレスポンス遅延があった場合の利用者への報告体制が取られている事を確認する】
備　考	

平成 24 年 3 月 15 日

クラウドコンピューティング利用時の情報セキュリティ対策	
領　域	クラウドコンピューティングの情報環境面
事　象	情報喪失リスク
具体的現象	情報漏えい・喪失時の損失： 自社の情報が盗み取られ、闇市場で売買され、ステークホルダーに迷惑をかけた。
想定される原因	業者の経験不足。 利用者の不注意。
ガイドライン	7.1.1　資産目録 すべての資産を明確に識別し，また，重要な資産すべての目録を作成し，維持することが望ましい。 【ポイント：盗難に備え自社の資産の目録が作成してある事を確認する】 7.1.2　資産の管理責任者 情報及び情報処理施設と関連する資産のすべてについて，組織の中に，その管理責任者を指定することが望ましい。 【ポイント：盗難に備え自社の資産の管理者が任命され、トラブル発生時にエスカレーションする仕組みがある事を確認する】 7.1.3　資産利用の許容範囲 情報及び情報処理施設と関連する資産の利用の許容範囲に関する規則は，明確にし，文書化し，実施することが望ましい。 【ポイント：盗難リスクを軽減するために、利用範囲が設定されている事を確認する】 7.2.2　情報のラベル付け及び取扱い 情報に対するラベル付け及び取扱いに関する適切な一連の手順は，組織が採用した分類体系に従って策定し，実施することが望ましい。 【ポイント：盗難に備え自社の資産の目録が作成してある事を確認する】
備　考	

ITコーディネータのための
クラウド業者目利きの指標

「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」より

2012年3月29日

ITガバナンス研究会
坂本　徳明

○ はじめに

経済産業省が平成23年4月1日に公表した「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」の序文には，次のことが書かれている。

～クラウドコンピューティングは，「IT の所有」から「IT の利用」への転換を促すと予想され，その利用によって，組織が情報システムの構築・運用作業から解放されることが期待される。クラウドコンピューティングを利用することは，運用管理コストの低減，需要に応じた柔軟かつ迅速な調達に応えると同時に，大規模データ解析，最先端のアプリケーション利用が安価に実現できるため，様々な業界からその普及，発展が期待されている。そのような期待があるにもかかわらず，現時点でクラウドコンピューティング利用は限定的である。その原因の一つとして，情報セキュリティに対する懸念がある。クラウドコンピューティングは，クラウド事業者の管理の下で他の利用者とコンピュータ資源を共有するため，情報の機密性・完全性・可用性にかかわる情報セキュリティについて懸念されているからである。
国内の組織の情報セキュリティには，情報セキュリティマネジメントの実践のための規範JISQ 27002に基づく管理策の実施が推奨されている。JISQ 27002には，第三者の提供するサービスの利用に関する管理策があるが，組織がIT を所有せずに全面的にクラウドコンピューティングを利用する場合には，この管理策が求める事項だけでは組織の情報セキュリティを確保するためには不足があるのが実情である。そのため，クラウド利用者の視点からJIS Q 27002の各管理策を再考し，クラウドコンピューティングを利用する組織においてこの規格に基づいた情報セキュリティ対策が円滑に行われることを目的として，このガイドラインを作成した。
このガイドラインには，組織がクラウドコンピューティングを全面的に利用する極限状態を想定し，①自ら行うべきこと，②クラウド事業者に対して求める必要のあること，さらに，③クラウドコンピューティング環境における情報セキュリティマネジメントの仕組みについて記載している。組織において，このガイドラインを参考にクラウドコンピューティングに対応した情報セキュリティの仕組みを整備するとともに，クラウド利用者のみで行うことができない管理策を認識し，クラウド利用者がクラウド事業者に対して様々な情報を求める必要がある。クラウド事業者においても，このガイドラインを参考に適切な情報を提供し，利用者との協力関係を向上することが望まれる。このガイドラインの利活用によって，クラウド利用者がクラウドコンピューティングの利用にあった情報セキュリティ対策を実施し，クラウドコンピューティングの活用が促進されることが望まれる。～

ITガバナンス研究会では，ITコーディネータ（以下，ITC）が中小企業へのクライドコンピューティング導入を支援する上で，セキュリティの観点から，ITC自身が適切なクラウド事業者を選別できなければならないと考えている。そのため、ITCがクラウド事業者を選別するために有用と思われる事項を，「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」から抽出し，クラウド事業者を目利きするための指標としてまとめた。

○ 本書の考え方

外部組織が提供するクラウドサービスを利用するということは，情報を取り扱うプロセス，システム並びにネットワークという情報資産を自組織の外部に置くことを意味する。クラウド利用者は，外部組織であるクラウド事業者からこれらの情報資産を利用できるサービスの提供を受け，これを利用して組織事業の基礎を成す情報の大部分を保存し又は処理するものとすれば，外部組織に依拠せずに情報セキュリティのマネジメントをすることはできない。これがクラウドサービス利用のための情報セキュリティが求められる理由である。

クラウド事業者はクラウド利用者とは独立した組織である。クラウドサービスの提供にかかわる資産に対する脅威，ぜい弱性及び事故の可能性の評価に資するような，何らかの情報を開示するかどうかは，専らクラウド事業者自らの事業判断にゆだねられている。したがって，クラウド利用者がセキュリティ要求事項を確立するには，クラウド利用者自らが行うリスクアセスメントに必要な情報を指定して，その情報を開示するよう，クラウド事業者に対して協力を要請することが望まれる。

ITガバナンス研究会ではこの点に着目し，中小企業がクラウドコンピューティングを導入することで生じるリスクと，そのリスクを回避・低減させるために必要とされるクラウド事業者への要請と、期待される対応をクラウド業者の目利きの指標とした。

○ 本書の見かた

「クラウド利用者が対応すべきリスク」	：	クラウドコンピューティングの導入により生じる可能性のあるリスク
「リスクに対するクラウド業者への要求」	：	リスクを回避・低減するために必要なクラウド事業者への協力要請
「クラウド業者から提供されるべき機能」	：	クラウド事業者への協力要請への回答として、クラウド事業者から提供されるべき機能
「クラウド業者から提供されるべき情報」	：	クラウド事業者への協力要請への回答として、クラウド事業者から提供されるべき情報
「クラウド業者が実施すべき事柄」	：	クラウド事業者への協力要請への回答として、クラウド事業者が実施すべき事柄
「マネジメントガイドライン項番」	：	リスクと対応の詳細が記載されている「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」の項番

想定されるリスクは，導入するクラウドコンピューティングの形態やクラウドコンピューティングを適用する業務によって異なる。
そのため，本書の利用に際しては，まず，適用しようとするクラウドコンピューティングについてリスクアセスメントを行う必要がある。
その上で，自社で管理できないリスクを洗い出し，クラウド事業者が適切に対応が出来るかどうかを見極める。

情報セキュリティの観点からクラウド業者を目利きするための指標

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項番			クラウド利用者が対応すべきリスク	リスクに対するクラウド業者への要求（クラウド業者目利きの指標）	クラウド業者から提供されるべき機能	クラウド業者から提供されるべき情報	クラウド業者が実施すべき事柄
5.1 情報セキュリティ基本方針	5.1.1	情報セキュリティ基本方針文書	クラウドサービスを利用している場合には，自らの基本方針とクラウド事業者の基本方針に差異があったり、クラウド事業者が適切な管理を怠っていると、自らの基本方針に影響を及ぼす可能性がある。	クラウド事業者は，情報セキュリティ基本方針をクラウド利用者に明示することが望ましい。		情報セキュリティ基本方針の明示	
6.1 内部組織	6.1.3	情報セキュリティ責任の割当て	クラウドサービス利用における責任において，自らが対応できない内容について，クラウド事業者が負う責任が不明確になり、適切なセキュリティ管理ができない可能性がある。	クラウド事業者は，クラウドサービスに関する情報セキュリティ責任者を専任することが望ましい。クラウド事業者は，クラウドサービスの情報セキュリティに関する窓口を明確にし，開示することが望ましい。		情報セキュリティに関する窓口の開示	情報セキュリティ責任者の専任
	6.1.4	情報処理設備の認可プロセス	情報セキュリティレベルの低いクラウドサービスを利用することにより、自らが定める情報セキュリティレベルを満足できないリスクがある。	クラウド事業者は，クラウド利用者がクラウドサービスの受け入れを行うために必要な資料を作成し，提供することが望ましい。クラウド事業者は，SLAなど，サービス開始前の合意事項を明確にすることが望ましい。クラウド事業者は，SLAなど，サービス開始前の合意事項をクラウドサービスの利用を検討する者に明示することが望ましい。		・クラウドサービスの受け入れを行うために必要な資料の提供 ・SLAなど，サービス開始前の合意事項の明示	
	6.1.5	秘密保持契約	クラウドサービスを利用するために自社の情報資産をクラウド事業者に預けることにより、自社の営業秘密を不当に第三者に開示され、又は流用される可能性がある。	クラウド事業者は，秘密保持契約を作成することが望ましい。クラウド事業者は，クラウド利用者との契約時には秘密保持契約を締結することが望ましい。			利用者との秘密保持契約の締結
	6.1.6	関係当局との連絡	クラウドサービスの利用において問題や苦情が発生した場合、迅速に対応されない可能性がある。	クラウド事業者は，提供するクラウドサービスの情報セキュリティに関して関連する監督官庁などを明確にし，開示することが望ましい。クラウド事業者は，個人情報の保護に関して監督官庁などを明確にし，開示することが望ましい。クラウド事業者は，サポート窓口，苦情窓口を明確にし，開示することが望ましい。		・情報セキュリティや個人情報保護に関連する監督官庁などの開示 ・サポート窓口，苦情窓口を明確にし，開示	
6.2 外部組織	6.2.1	外部組織に関係したリスクの識別	クラウドサービスが業務プロセスに与える影響を特定することができず、適切なリスクアセスメントができないリスクがある。	クラウド事業者は，クラウドサービス利用における注意事項を明確にすることが望ましい。クラウド事業者は，クラウドサービスに関連したリスクについて，最新情報を収集し，必要に応じて開示することが望ましい。		サービスに関連したリスクについて最新情報の開示	・サービス利用における注意事項の明確化 ・サービスに関連したリスクについて最新情報を収集
7.1 資産に対する責任	7.1.1	資産目録	クラウドコンピューティング環境にあるクラウド利用者の資産の管理場所が分からなくなるリスクがある。	クラウド事業者は，クラウドコンピューティング環境にあるクラウド利用者の資産に関する資産目録の一覧が取得できるインタフェースをクラウド利用者に提供することが望ましい	利用者の資産に関する資産目録の一覧が取得できるインタフェース		
	7.1.2	資産の管理責任者	クラウドコンピューティング環境にあるクラウド利用者の資産の管理責任者が分からなくなるリスクがある。	クラウド事業者は，クラウドコンピューティング環境にあるクラウド利用者の資産の責任者を明確にし，顧客対応のエスカレーションプロセスに追加することが望ましい。			利用者の資産の責任者の明確化

情報セキュリティの観点からクラウド業者を目利きするための指標

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項番			クラウド利用者が対応すべきリスク	リスクに対するクラウド業者への要求（クラウド業者目利きの指標）	クラウド業者から提供されるべき機能	クラウド業者から提供されるべき情報	クラウド業者が実施すべき事柄
7.2 情報の分類	7.2.1	分類の指針	クラウドコンピューティング環境にあるクラウド利用者の資産が、組織に対しての価値，法的要求事項，取扱いに慎重を要する度合いに応じた分類がされないため、適切な管理が出来なくなるリスクがある。	クラウド事業者は，クラウドコンピューティング環境にあるクラウド利用者の情報に付加されるメタデータの項目などを明確にし，開示することが望ましい。クラウド事業者は，クラウドコンピューティング環境にあるクラウド利用者の情報がどのように分離されて管理されているかを明確にし，開示することが望ましい。		・利用者の情報に付加されるメタデータの項目などの開示 ・利用者の情報がどのように分離されて管理されているかの開示	
	7.2.2	情報のラベル付け及び取扱い	情報に対するラベル付け及び取扱いに関する適切な一連の手順は，組織が採用した分類体系に従って策定し，実施することが望ましい。	クラウド事業者は，クラウドコンピューティング環境にあるクラウド利用者の情報を分類するためにフォルダ分類やラベル機能を提供することが望ましい。クラウド事業者は，クラウドコンピューティング環境にあるクラウド利用者の情報を一時的に分類するためにマーキングなどの機能を提供することが望ましい。	利用者の情報を分類するためにフォルダ分類やラベル機能		
8.3 雇用の終了又は変更	8.3.2	資産の返却	クラウドサービスの利用者が，雇用，契約又は合意の終了時に、クラウドコンピューティング環境にある資産が返却されないリスクがある。	クラウド事業者は，クラウドサービスにおいて，クラウドサービスの利用者が，雇用，契約又は合意の終了時に返却する資産を，クラウド利用者が管理できる機能を提供することが望ましい。クラウド事業者は，クラウドサービスにおいて，クラウドサービスの利用者が，雇用，契約又は合意の終了時に返却する資産を，クラウド利用者が管理できる機能について，クラウドサービスの利用を検討する者に明示することが望ましい。	契約又は合意の終了時に返却する資産を，クラウド利用者が管理できる機能		
	8.3.3	アクセス権の削除	クラウドサービスの利用者に対するアクセス権を，雇用，契約又は合意の終了時に、クラウド利用者によるアクセス権の削除ができないなど、適時削除されないリスクがある。	クラウド事業者は，クラウドサービスの利用者に対するアクセス権を，クラウド利用者が，雇用，契約又は合意の終了時に削除し，また，変更に合わせて修正する機能を提供することが望ましい。クラウド事業者は，クラウドサービスの利用者に対するアクセス権を，クラウド利用者が，雇用，契約又は合意の終了時に削除し，また，変更に合わせて修正する機能の提供に関して次の事項を実施することが望ましい。 a) これらの機能を提供すること b) これらの機能の有無を開示すること c) これらの機能の詳細をクラウドサービスの利用を検討するものに明示すること	サービスの利用者に対するアクセス権を，クラウド利用者が，雇用，契約又は合意の終了時に削除し，また，変更に合わせて修正する機能		
9.1 セキュリティを保つべき領域	9.1.5	セキュリティを保つべき領域での作業	クラウドサービスによって，クラウド利用者が予期せぬ利用ができるようになることで、セキュリティを保てなくなるリスクがある。（例モバイルコンピューティングからの利用が可能になる，など）。	クラウド事業者は，クラウドサービスによって，クラウド利用者の利用環境を拡大させるような機能が存在する場合は，その機能を開示することが望ましい（例モバイルコンピューティングからの利用が可能になる，など）。		クラウド利用者の利用環境を拡大させるような機能の開示	
	9.2.6	装置の安全な処分又は再利用	クラウドサービスの利用を終了した場合，使用されていた機器などが再利用されるため、，取扱いに慎重を要するデータやライセンス供与されたソフトウェアが他で使われるリスクがある。	クラウド事業者は，バックアップを含め，取扱いに慎重を要するデータ及びライセンス供与されたソフトウェアを含む情報の取り扱いに留意することが望ましい。クラウド事業者は，記憶媒体を内蔵した装置を処分する場合には，記録された情報を復元できないように安全に処分することが望ましい。また，再利用の場合には，機密情報の漏えい等につながらないように対処することが望ましい。			・取扱いに慎重を要するデータ及びライセンス供与されたソフトウェアを含む情報の取り扱いへの留意 ・記録された情報の安全処分 ・再利用時の機密情報の漏えい等への対処

情報セキュリティの観点からクラウド業者を目利きするための指標

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項番			クラウド利用者が対応すべきリスク	リスクに対するクラウド業者への要求（クラウド業者目利きの指標）	クラウド業者から提供されるべき機能	クラウド業者から提供されるべき情報	クラウド業者が実施すべき事柄
10.1 運用の手順及び責任	10.1.1	操作手順書	クラウドサービスとして提供される仮想システム基盤の操作が分からず、適切な運用ができないリスクがある。	クラウド事業者は，クラウド利用者のクラウドサービスとして提供する仮想システム基盤についての操作手順の作成に協力することが望ましい。協力の具体例としては次がある。 a) 操作マニュアルの提示 b) 問い合わせ窓口の設置 c) 利用者の操作手順作成を支援するサービスの提供	問い合わせ窓口	操作マニュアルの提示	提供する仮想システム基盤についての操作手順作成への協力
	10.1.2	変更管理	クラウドサービスの情報処理設備及びシステムの変更がクラウド利用者に事前に通知されず，影響を及ぼすリスクがある。	クラウド事業者は，クラウドサービスの情報処理設備及びシステムの変更において，クラウド利用者に影響を及ぼすものは，クラウド利用者に事前に通知することが望ましい。		クラウド利用者に影響を及ぼす可能性のある情報処理設備及びシステムの変更に関する情報	クラウド利用者に影響を及ぼす可能性のある情報処理設備及びシステム変更の事前通知
	10.1.3	職務の分割	クラウドサービスにおいて、組織の資産に対する責任範囲が明確でない場合，認可されていない又は意図しない変更又は不正使用のリスクがある。	クラウド事業者は，提供するクラウドサービスにおいて，組織の資産に対する，認可されていない又は意図しない変更又は不正使用の危険性を低減するために，クラウド利用者によって，分割することが望ましい職務及び責任範囲を，クラウドサービスの利用を検討する者に明示することが望ましい。		クラウド利用者によって分割することが望ましい職務及び責任範囲に関する情報	
10.2 第三者が提供するサービスの管理	10.2.1	第三者が提供するサービス	クラウド利用者は，クラウド事業者が，第三者（クラウドサービスを構成するためのネットワークを提供するプロバイダや関係する他のクラウド事業者など）が提供するサービスに関する合意に含まれる，セキュリティ管理策，サービスの定義及び提供サービスレベルによって，クラウド利用者が影響をうける可能性がある。	クラウド事業者は，クラウドサービスにおいて，重大なサービス不具合又は災害の後においても，合意されたサービス継続レベルを維持することを確実にするように設計された実行可能な計画とともに，第三者（クラウドサービスを構成するためのネットワークを提供するプロバイダや関係する他のクラウド事業者など）が十分なサービス提供機能を維持することを確実にすることが望ましい。			第三者が十分なサービス提供機能を維持することを確実にする
	10.2.2	第三者が提供するサービスの監視及びレビュー	クラウド利用者は，クラウド事業者が，第三者（クラウドサービスを構成するためのネットワークを提供するプロバイダや関係する他のクラウド事業者など）が提供するサービスに関する合意に含まれる，セキュリティ管理策，サービスの定義及び提供サービスレベルによって，クラウド利用者が影響をうける可能性がある。	クラウド事業者は，クラウドサービスにおいて，第三者（クラウドサービスを構成するためのネットワークを提供するプロバイダや関係する他のクラウド事業者など）が提供するサービス，報告及び記録を，常に監視し，レビューすることが望ましい。			第三者が提供するサービス，報告及び記録の監視とレビュー
	10.2.3	第三者が提供するサービスの変更に対する管理	クラウドサービスにおいて，クラウド事業者の利用する第三者（クラウドサービスを構成するためのネットワークを提供するプロバイダや関係する他のクラウド事業者など）のサービス提供の変更が影響を及ぼす可能性がある	クラウド事業者は，クラウドサービスにおいて，第三者（クラウドサービスを構成するためのネットワークを提供するプロバイダや関係する他のクラウド事業者など）のサービス提供の変更による影響を管理することが望ましい。			第三者のサービス提供の変更による影響の管理
10.3 システムの計画作成及び受入れ	10.3.1	容量・能力の管理	クラウドサービスにおける，容量・能力の限界値を把握することができず，要求されたシステム性能を満たすことができないリスクがある。	クラウド事業者は，クラウドサービスにおいて，システム全体の容量・能力の限界値及びクラウド利用者に割り当てられる容量・能力の限界値を把握することが望ましい。			システム全体の容量・能力の限界値及び利用者に割り当てられる容量・能力の限界値の把握
	10.3.2	システムの受入れ	クラウドサービスに関する新しい情報システム及びその改訂版・更新版が提供される場合の対応手続きが明確でない場合、適切なテストが実施されず、改訂版や更新版の提供で影響をうけるリスクがある。	クラウド事業者は，クラウドサービスの改訂版・更新版の提供プロセスを，クラウド利用者に明示することが望ましい。		サービスの改訂版・更新版の提供プロセス	

情報セキュリティの観点からクラウド業者を目利きするための指標

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項番			クラウド利用者が対応すべきリスク	リスクに対するクラウド業者への要求（クラウド業者目利きの指標）	クラウド業者から提供されるべき機能	クラウド業者から提供されるべき情報	クラウド業者が実施すべき事柄
10.4 悪意のあるコード及びモバイルコードからの保護	10.4.1	悪意のあるコードに対する管理策	悪意のあるコードを，検出，予防及び回復のための管理策だけでなく，クラウドサービスの利用者に対してクラウドサービス利用時の考慮事項を適切に意識させるための手順などが策定されていない場合、悪意のあるコードからクラウド利用者を保護できないリスクがある。	クラウド事業者は，クラウドサービスの提供において，悪意のあるコードへのクラウド事業者の責任範囲と，クラウド利用者の責任範囲を明らかにすることが望ましい。		悪意のあるコードへのクラウド事業者の責任範囲と，クラウド利用者の責任範囲	
10.5 バックアップ	10.5.1	情報のバックアップ	クラウド利用者は，クラウドサービス上で扱う情報，ソフトウェア及びソフトウェアの設定において，バックアップの必要性を確認せず、のバックアップ手順を策定していない場合、情報やソフトウェアを喪失するリスクがある。	クラウド事業者は，クラウド利用者が求める情報，ソフトウェア及びソフトウェアの設定において，クラウド利用者がバックアップ手順を策定できるように情報を提供することが望ましい。		バックアップ手順策定に必要な情報	
10.6 ネットワークセキュリティ管理	10.6.2	ネットワークサービスのセキュリティ	クラウドサービスに含まれるすべてのネットワークサービス（組織が自ら提供するか外部委託しているかを問わない）について，セキュリティ特性，サービスレベル及び管理上の要求事項に，適合することを確認しない場合、ネットワークのセキュリティを確保できないリスクがある。	クラウド事業者は，クラウドサービスに含まれるすべてのネットワークサービスについて，セキュリティ特性，サービスレベル及び管理上の要求事項を，クラウド利用者と合意することが望ましい。			ネットワークサービスに関するセキュリティ特性，サービスレベル及び管理上の要求事項のクラウド利用者との合意
10.8 情報の交換	10.8.4	電子的メッセージ通信	クラウド利用者は，クラウドサービスにおいて，電子的メッセージ通信を利用する場合は，電子的メッセージ通信に含まれた情報を適切に保護する機能があることを確認しない場合、情報が保護されないリスクがある。	クラウド事業者は，クラウドサービスにおいて，電子的メッセージ通信を提供する場合は，電子的メッセージ通信に含まれた情報を適切に保護する機能を提供することが望ましい。	電子的メッセージ通信に含まれた情報を適切に保護する機能		
10.10 監視	10.10.1	監査ログ取得	クラウド利用者は，クラウドサービス上で取得されるクラウドサービスの利用者の活動，例外処理及びセキュリティ事象を記録した監査ログの存在を確認しない場合、サービスの安全性、信頼性を担保できないリスクがある。	クラウド事業者は，クラウドサービス上で取得するクラウドサービスの利用者の活動，例外処理及びセキュリティ事象を記録した監査ログを特定し，取得する機能をクラウド利用者に提供することが望ましい。	監査ログの特定・提供		
	10.10.2	システム使用状況の監視	クラウド利用者は，クラウドサービスの使用状況を監視する手順を確立できない場合，適切な運用が出来ないリスクがある。	クラウド事業者は，クラウドサービス上で使用状況をクラウド利用者が監視できる機能を提供することが望ましい。	使用状況の監視		
	10.10.3	ログ情報の保護	クラウド利用者は，クラウドサービス上の，ログ機能及びログ情報が，改ざん及び認可されていないアクセスから保護されていることを確認しない場合、不正や誤謬を検知できないリスクがある。	クラウド事業者は，クラウドサービス上で，ログ機能及びログ情報は，改ざん及び認可されていないアクセスから保護する機能を提供することが望ましい。	ロギング機能 ログ情報改ざん防止 ログアクセス制御		
	10.10.4	実務管理者及び運用担当者の作業ログ	クラウド利用者は，クラウドサービス上に構築した利用者システムの実務管理者及び運用担当者の作業が，記録されていることを確認しない場合、不正な運用管理を検知できないリスクがある。	クラウド事業者は，クラウドサービス上で，クラウド利用者のシステムの実務管理者及び運用担当者の作業を，記録する機能を提供することが望ましい。	利用者作業の記録		
	10.10.5	障害のログ取得	クラウド利用者は，クラウドサービス上の障害のログを取得できない場合，障害原因の分析や障害に対する適切な処置をとることができないリスクがある。	クラウド事業者は，クラウド利用者に提供する，障害のログの範囲を定めることが望ましい。クラウド事業者は，クラウド利用者に障害のログを提供する機能を提供することが望ましい。	障害ログの提供		
	10.10.6	クロックの同期	クラウド利用者は，クラウドサービスと組織内のシステムとの時刻差が発生するか確認しない場合、クラウド利用者は，クラウドサービスと組織内のシステムとの時刻差によって発生する問題に対処できないリスクがある。	クラウド事業者は，クラウドサービスのすべての情報処理システム内のクロックを，合意された正確な時刻源と同期させることが望ましい。	正確な時刻減との同期		

情報セキュリティの観点からクラウド業者を目利きするための指標

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項番			クラウド利用者が対応すべきリスク	リスクに対するクラウド業者への要求（クラウド業者目利きの指標）	クラウド業者から提供されるべき機能	クラウド業者から提供されるべき情報	クラウド業者が実施すべき事柄
11.1 アクセス制御に対する業務上の要求事項	11.1.1	アクセス制御方針	クラウド利用者は，既存のアクセス制御方針が，クラウドサービスが提供するアクセス制御機能で実現できるか確認しない場合、アクセス制御の有効性を担保できないリスクがある。	クラウド事業者は，提供するクラウドサービスにおいて，アクセス制御機能を提供することが望ましい。クラウド事業者は，提供するクラウドサービスにおいて設定可能なアクセス制御機能について，クラウドサービスの利用を検討する者に明示することが望ましい。	アクセス制御		
11.2 利用者アクセスの管理	11.2.1	利用者登録	クラウド利用者は，利用者登録の正式な手順（クラウドサービスの利用者IDの登録・削除など）が，クラウド事業者が提供するクラウドサービス利用者IDの登録・削除機能で実現できることを確認しない場合、適切なアクセス制御が担保できないリスクがある。	クラウド事業者は，クラウドサービスの利用者IDの登録・削除機能を提供することが望ましい。	利用者ID登録・削除		
	11.2.2	特権管理	クラウド利用者は，既存の特権の割当て及び利用を，制限し，管理する仕組みが，クラウドサービス上で実現できるか確認しない場合、クラウド利用者は，クラウドサービスの特権の割当て及び利用を，制限し，管理できないリスクがある。	クラウド事業者は，クラウドサービスの特権の割当て及び利用を，制限し，管理する機能を提供することが望ましい。	特権の割当・制御		
	11.2.3	利用者パスワードの管理	クラウド利用者は，既存のパスワードの割当ての正式な管理プロセスが，クラウドサービスが提供する機能で実現できるか確認しない場合、パスワード管理が適切に行われないリスクがある。	クラウド事業者は，クラウドサービスにおいて利用するパスワードの割当ての管理機能を提供することが望ましい。	パスワード割当		
	11.2.4	利用者アクセス権のレビュー	クラウド利用者は，クラウドサービスの利用者のアクセス権をレビューする正式なプロセスが，クラウドサービスの機能で実現できることを確認しない場合、利用者のアクセス権のレビューができないリスクがある。	クラウド事業者は，クラウドサービスにおいて，クラウド利用者がアクセス権をレビューする機能を提供することが望ましい。	アクセス権のレビュー		
11.4 ネットワークのアクセス制御	11.4.2	外部から接続する利用者の認証	クラウド利用者は，自らが管理していないネットワーク（公衆無線LANや携帯電話網による接続など）からクラウドサービスを利用する際の適切な認証を行わない場合、不正アクセスを防御できないリスクがある。	クラウド事業者は，クラウドサービスへの接続方法に応じた認証方法を提供することが望ましい。クラウド事業者は，クラウドサービスへの接続方法に応じた認証方法を，クラウドサービスの利用を検討する者に明示することが望ましい。	クラウドサービスへの接続方法に応じた認証方法		
	11.4.6	ネットワークの接続制御	クラウド利用者は，クラウドサービスのネットワークについて，アクセス制御方針及び業務用ソフトウェアの要求事項に沿って，利用者のネットワーク接続能力を制限することが望ましい。利用者のネットワークへのアクセス権は，アクセス制御方針の要求に従って，維持し更新することが望ましい。	クラウド事業者は，クラウドサービスで利用可能なネットワークサービスを特定することが望ましい（例メッセージ通信（例えば，電子メール），ファイル転送，など）。		利用可能なネットワークサービスに関する情報	

情報セキュリティの観点からクラウド業者を目利きするための指標

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項番			クラウド利用者が対応すべきリスク	リスクに対するクラウド業者への要求（クラウド業者目利きの指標）	クラウド業者から提供されるべき機能	クラウド業者から提供されるべき情報	クラウド業者が実施すべき事柄
11.5 オペレーティングシステムのアクセス制御	11.5.1	セキュリティに配慮したログオン手順	クラウド利用者は，クラウドサービスのオペレーティングシステムにログオンする場合，セキュリティに配慮したログオン手順によって制御されることを確認することが望ましい。	クラウド事業者は，クラウドサービスのオペレーティングシステムにクラウド利用者がログオンする場合，セキュリティに配慮したログオン手順で制御する機能を提供することが望ましい。	セキュリティに配慮したログオン手順で制御する機能		
	11.5.2	利用者の識別及び認証	クラウド利用者は，クラウドサービスにおいて，すべてのクラウドサービスの利用者が各個人の利用ごとに一意な識別子（利用者ID）を保有することができるか確認しない場合、クラウドサービス利用者の同一性を検証できないリスクがある。	クラウド事業者は，クラウドサービスにおいて，すべてのクラウドサービス利用者に，各個人の利用ごとに一意な識別子（利用者ID）を保有することができるようにすることが望ましい。	各個人の利用ごとに一意な識別子（利用者ID）を保有する機能		
	11.5.3	パスワード管理システム	クラウド利用者は，クラウドサービスのパスワードを管理するシステムの機能を確認しない場合，良質なパスワードを確保できないリスクがある。	クラウド事業者は，クラウドサービスのパスワードを管理するシステムを，対話式とすることが望ましい。	対話式でパスワードを管理する機能		
	11.5.4	システムユーティリティの使用	クラウド利用者は，クラウドサービスのシステム及び業務用ソフトウェアによる制御を無効にすることのできるユーティリティプログラムについて確認しない場合，そのプログラムの使用を制限し，厳しく管理することができないリスクがある。	クラウド事業者は，システム及び業務用ソフトウェアによる制御を無効にすることのできるユーティリティプログラムを特定することが望ましい。			システム及び業務用ソフトウェアによる制御を無効にすることのできるユーティリティプログラムの特定
	11.5.5	セッションのタイムアウト	クラウド利用者は，クラウドサービスの利用中に，一定の使用中断時間が経過したときは，使用が中断しているセッションが遮断されることを確認しない場合、不正アクセスを防御できないリスクがある。	クラウド事業者は，クラウドサービスの利用中に，一定の使用中断時間が経過したときは，使用が中断しているセッションを遮断する機能を提供することが望ましい。	使用が中断しているセッションを遮断する機能		
	11.5.6	接続時間の制限	クラウド利用者は，利用におけるリスクが高いと判断したクラウドサービスに対しては，接続時間の制限を利用できるか確認しない場合、切断されないリスクがある。	クラウド事業者は，利用におけるリスクが高いと判断されたクラウドサービスは，接続時間の制限を利用できる機能を提供することが望ましい。	接続時間の制限を利用できる機能		
11.6 業務用ソフトウェア及び情報のアクセス制御	11.6.1	情報へのアクセス制限	クラウド利用者は，クラウド利用者及びクラウド利用者のサポート要員によるクラウドサービスへのアクセスを，既定のアクセス制御方針に従って制限できることを確認しない場合、アクセス制御が機能しないリスクがある。	クラウド事業者は，クラウド利用者におけるクラウドサービスへのアクセス制限の要求モデルを定めることが望ましい。		アクセス制限の要求モデルに関する情報	
	11.6.2	取扱いに慎重を要するシステムの隔離	クラウド利用者は，取扱いに慎重を要するシステムを，クラウドコンピューティングを利用して，構築する場合には，専用の（隔離された）コンピュータ環境上に構築できることを確認することが望ましい。	クラウド事業者は，取扱いに慎重を要するシステムを，クラウドコンピューティング内に構築する場合に備えて，専用の（隔離された）コンピュータ環境上に構築できる機能を提供することが望ましい。	隔離されたコンピュータ環境上に構築できる機能		
11.7 モバイルコンピューティング及びテレワーキング	11.7.1	モバイルのコンピューティング及び通信	クラウド利用者は，モバイルコンピューティング設備・通信設備を用いた場合のリスクから保護するための正式な方針に，クラウドサービスを加え，適切な情報セキュリティ対策を採用することが望ましい。	クラウド事業者は，クラウドサービスにおいて，モバイルコンピューティングを利用できる機能を提供する場合は，適切な情報セキュリティ対策を採用することが望ましい。			モバイルコンピューティングに関する適切な情報セキュリティ対策の採用
	11.7.2	テレワーキング	クラウド利用者は，クラウドサービスをテレワーキングで利用する場合，テレワーキングのための方針，運用計画及び手順を策定し，実施することが望ましい。	クラウドサービスにおいてテレワーキングを利用する機能を提供する場合は，テレワーキングの適切な保護を実施することが望ましい。			テレワーキングの適切な保護の実施

情報セキュリティの観点からクラウド業者を目利きするための指標

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項番			クラウド利用者が対応すべきリスク	リスクに対するクラウド業者への要求（クラウド業者目利きの指標）	クラウド業者から提供されるべき機能	クラウド業者から提供されるべき情報	クラウド業者が実施すべき事柄
12.1 情報システムのセキュリティ要求事項	12.1.1	セキュリティ要求事項の分析及び仕様化	クラウド利用者は，システム構築の標準を記載した規程にクラウドサービス利用時の項目を追加することが望ましい。クラウド利用者は，システム利用標準に外部のクラウドサービスを利用する場合に必要な項目を追加することが望ましい。クラウド利用者は，システム利用標準には組織のセキュリティ基本方針とクラウド事業者のセキュリティ基本方針が組織のセキュリティ基本方針に反しないことを確認することが望ましい。	クラウド事業者は，クラウドサービスで実装（提供）している情報セキュリティ対策及び機能を列記し，開示することが望ましい。		クラウドサービスで実装（提供）している情報セキュリティ対策及び機能の開示	
12.3 暗号による管理策	12.3.1	暗号による管理策の利用方針	クラウドサービス上で利用する情報の暗号化機能が提供されていることを確認しない場合、情報を保護するための暗号による管理策の利用に関する方針が活かされないリスクがある。	クラウド事業者は，暗号化に対応しているサービスを明確にし，クラウド利用者に明示することが望ましい。クラウド事業者は，暗号化されないサービスについて代替機能があれば明確にし，開示することが望ましい。		暗号化に関する情報	
12.5 開発及びサポートプロセスにおけるセキュリティ	12.5.1	変更管理手順	クラウド利用者は，変更管理規定にクラウドに関する項目を追加しない場合、変更管理が適切に行われないリスクがある。	クラウド事業者は，システムの変更が行われた際にはクラウド利用者に通知することが望ましい。クラウド事業者は，システムの機能が変更，追加された際にはクラウド利用者に通知することが望ましい。		システムの変更に関する情報・通知	
	12.5.2	オペレーティングシステム変更後の業務用ソフトウェアの技術的レビュー	オペレーティングシステムを変更するときに，重要な業務用ソフトウェアをレビュー・試験しない場合，組織の運用又はセキュリティに悪影響を及ぼすリスクがある。	クラウド事業者は，クラウドサービスを利用することができるオペレーティングシステムやウェブブラウザの種類とバージョンを明示することが望ましい。クラウド事業者は，クラウドサービスを利用することができるオペレーティングシステムやウェブブラウザの種類とバージョンに変更が生じる場合は，予めクラウド利用者に通知することが望ましい。		クラウドサービスを利用することができるオペレーティングシステムやウェブブラウザの種類とバージョン	
	12.5.4	情報の漏えい	情報漏えいの可能性を考慮して，クラウドサービスの利用手順を策定・周知徹底しない場合、情報漏えいのリスクがある。	クラウド事業者は，クラウドサービスにおける情報漏えいに関する対策を行い，円滑なシステムの運用に支障のない範囲でクラウド利用者にその対策内容を開示することが望ましい。		情報漏えいに関する対策の内容	情報漏えいに関する対策の実施
12.6 技術的ぜい弱性管理	12.6.1	技術的ぜい弱性の管理	クラウド利用者は，クラウド事業者から技術的ぜい弱性について情報を収集しない場合、ぜい弱性に組織がさらされている状況を評価し，それと関連するリスクに対処するために，適切な手段をとることができないリスクがある。	クラウド事業者は，提供するクラウドサービスに関連するリスクについて情報収集を行うことが望ましい。			提供するクラウドサービスに関連するリスクについて情報収集
13.1 情報セキュリティの事象及び弱点の報告	13.1.1	情報セキュリティ事象の報告	クラウド利用者は，クラウドサービスの利用者が利用中に気づいた事象について報告し，集約できる体制を構築しない場合、セキュリティインシデントを看過するリスクがある。	クラウド事業者は，情報セキュリティインシデントを受け付ける窓口を設置することが望ましい。			情報セキュリティインシデント受付窓口の設置
13.2 情報セキュリティインシデントの管理及びその改善	13.2.2	情報セキュリティインシデントからの学習	クラウド利用者は，クラウドサービスの情報セキュリティインシデントについて記録し定量化することが望ましい。	クラウド事業者は，複数のクラウド利用者からの情報セキュリティインシデントの報告をまとめ，定期的にクラウド利用者に報告することが望ましい。			情報セキュリティインシデントの定期的な報告
	13.2.3	証拠の収集	クラウド利用者は，情報セキュリティ事故が法的処置に及ぶ場合を想定して，クラウド事業者が証拠などの情報を保管しているか確認しない場合、情報セキュリティインシデント後の個人又は組織への事後処置が法的処置（民事又は刑事）に及ぶ場合には，関係する法域で定めている証拠を収集，保全及び提出することができないリスクがある。	クラウド事業者は，法的な証拠となる可能性がある情報については記録し，適切に保管しておくことが望ましい。クラウド事業者は，どのような記録がどの程度の期間保管されているかをクラウド利用者に明示することが望ましい。		法的な証拠となる可能性がある情報について、どのような記録がどの程度の期間保管されているかを明示	法的な証拠となる可能性がある情報の記録・保管
14.1 事業継続管理における情報セキュリティの側面	14.1.2	事業継続及びリスクアセスメント	クラウド利用者は，クラウドサービス利用を前提とした業務プロセスの中断について，リスクアセスメントを実施し，業務を中断させる事象の発生確率とその中断のもたらす損害等の影響，業務の中断が情報セキュリティに及ぼす影響を検討して，リスクを識別しない場合、事業を継続できなくなるリスクがある。	クラウド事業者は，クラウドサービスのサービスレベルについて中断の発生確率及び影響，並びに中断が情報セキュリティに及ぼす結果とともに，特定することが望ましい。			サービス中断の発生確率及び影響，並びに中断が情報セキュリティに及ぼす結果の特定

情報セキュリティの観点からクラウド業者を目利きするための指標

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項番			クラウド利用者が対応すべきリスク	リスクに対するクラウド業者への要求（クラウド業者目利きの指標）	クラウド業者から提供されるべき機能	クラウド業者から提供されるべき情報	クラウド業者が実施すべき事柄
15.1 法的要求事項の順守	15.1.1	適用法令の識別	クラウド利用者は，クラウドサービスの利用目的に応じて，関連する法令，規制及び契約上の要求事項などを洗い出すことが望ましい。	クラウド事業者は，関連する法令，規制及び契約上の要求事項が策定されている地域（国，州など）を明示する事が望ましい。		関連する法令，規制及び契約上の要求事項が策定されている地域（国，州など）の明示	
	15.1.3	組織の記録の保護	クラウド利用者は，クラウドサービス上で利用する重要な記録は法令や規制に従って保護することが望ましい。	クラウド事業者は，法令や規制に従って，クラウドサービス上の記録を保護することが望ましい。			法令や規制に従ったクラウドサービス上の記録の保護
	15.1.6	暗号化機能に対する規制	クラウド利用者は，暗号技術をクラウドサービス上で利用する際には，輸出規制などに抵触しないか確認することが望ましい。	クラウド事業者は，クラウド利用者が輸出規制などに抵触しないよう，暗号化機能に係る法令等の情報をクラウド利用者に提供することが望ましい。		暗号化機能に係る法令等の情報	
15.2 セキュリティ方針及び標準の順守，並びに技術的順守	15.2.2	技術的順守点検	クラウド利用者は，クラウドサービスが組織のセキュリティ実施標準に順守しているかを定期的に点検することが望ましい。	クラウド事業者は，クラウドサービスが組織のセキュリティ実施標準に順守しているかを定期的に点検し，その結果をクラウド利用者に開示することが望ましい。		セキュリティ実施標準に順守しているかの定期結果の開示	セキュリティ実施標準に順守しているかの定期点検
15.3 情報システムの監査に対する考慮事項	15.3.1	情報システムの監査に対する管理策	クラウド利用者は，情報システムの監査の対象にクラウドサービスを追加することが望ましい。	クラウド事業者は，利用者の情報システム監査実施に有用な情報を提供することが望ましい。		利用者の情報システム監査実施に有用な情報	

2012年度研究レポート

連邦政府情報システムにおける推奨セキュリティ管理策

牧田　一雄

連邦政府情報システムにおける推奨セキュリティ管理策

識別子	ファミリ	クラス
AC	アクセス制御(Access Control)	技術
AT	意識向上およびトレーニング(Awareness and Training)	運用
AU	監査および責任追跡性(Audit and Accountability)	技術
CA	承認、運用認可、セキュリティ評価 (Certification*, Accreditation, and Security Assessments)	管理
CM	構成管理(Configuration Management)	運用
CP	緊急時対応計画 (Contingency Planning)	運用
IA	識別および認証(Identification and Authentication)	技術
IR	インシデント対応(Incident Response)	運用
MA	保守(Maintenance)	運用
MP	記録媒体の保護(Media Protection)	運用
PE	物理的および環境的な保護(Physical and Environmental Protection)	運用
PL	計画(Planning)	管理
PS	人的セキュリティ(Personnel Security)	運用
RA	リスクアセスメント(Risk Assessment)	管理
SA	システムおよびサービスの調達(System and Services Acquisition)	管理
SC	システムおよび通信の保護(System and Communications Protection)	技術
SI	システムおよび情報の完全性(System and Information Integrity)	運用

	SP800-26		管理策	補足ガイダンス	管理強化策	具体的なコントロール目標と手法	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
CP		緊急時対応計画 (Contingency Planning)	適用				
							5 セキュリティ基本方針 5.1 情報セキュリティ基本方針 5.1.1 情報セキュリティ基本方針文書 5.1.2 情報セキュリティ基本方針のレビュー 14 事業継続管理 14.1 事業継続管理における情報セキュリティの側面 14.1.1 事業継続管理手続への情報セキュリティの組込み 14.1.2 事業継続及びリスクアセスメント 14.1.3 情報セキュリティを組み込んだ事業継続計画の策定及び実施 14.1.4 事業継続計画策定の枠組み 14.1.5 事業継続計画の試験，維持及び再評価
CP-1		緊急時対応計画の方針と手順	組織は、以下のものを策定および周知徹底し、定期的にレビュー／更新する。(i) 正式に文書化された、緊急時対応計画の方針。これらの方針では、目的、適用範囲、役割、責任、経営陣のコミットメント、組織間の調整、およびコンプライアンスを取り扱う。(ii)正式に文書化された、緊急時対応計画の方針の導入に関する手順。この手順は、緊急時対応計画に関する方針の導入、ならびに関連する管理策の導入を容易にするために使用される。	緊急時対応計画の方針と手順は、適用法、大統領令、指令、方針、規制、基準、およびガイダンスに準拠する。緊急時対応計画の方針は、組織の一般的な情報セキュリティ方針の一部とすることができる。緊急時対応計画の手順は、一般的なセキュリティプログラムの一部として作成することもできれば、必要に応じて特定の情報システムに特化した形で作成することもできる。緊急時対応計画の作成に関するガイダンスは、NIST Special Publication 800-34に記載されている。セキュリティ方針および手順のガイダンスは、NIST Special Publication 800-12 に記載されている。	なし。		
	9					9. 非常事態計画 OMB Circular A-130、III 9.1. 重要項目: 最も重要で機密性の高い業務とそれをサポートするコンピュータリソースが明確化されているか? 9.1.1 重要なデータファイルや業務が特定され、ファイルのバックアップ頻度が文書化されているか? FISCAM SC- SC-1.1および3.1,NIST SP 800-18 9.1.2 重要な業務をサポートするリソースは明確になっているか? FISCAM SC-1.2 9.1.3 処理の優先順位を確定し、マネジメント層の承認を受けているか? FISCAM SC-1.3 9.2. 重要項目: 包括的な非常事態計画を策定し、文書化しているか? 9.2.1 計画は、影響のある主要な部門の承認を受けたか? FISCAM SC-3.1 9.2.2 リカバリの責任は割り当てられているか? FISCAM SC-3.1 9.2.3 業務を復旧させる詳細な手順が定められているか? FISCAM SC-3.1 9.2.4 代替処理サイトはあるか? ある場合、契約や機関間の合意は行われているか? FISCAM SC-3.1,NIST SP 800-18 9.2.5 バックアップの保管場所は明確になっているか? NIST SP 800-18 9.2.6 バックアップは所定の方法で作成され、最新のファイルが損傷を受けた場合にバックアップが破壊されるのを防ぐために、オフサイトにおけるローテーションの頻度は十分か? FISCAM SC-2.1 9.2.7 システムやアプリケーションのドキュメントは、離れた場所に保管しているか? FISCAM SC-2.1 9.2.8 バックアップからリストアした後、システムのデフォルトはすべてリセットされるか? FISCAM SC-3.1 9.2.9 バックアップ保管サイトと代替サイトは、主サイトとは地理的に離れた場所にあり、物理的に保護されているか? FISCAM SC-2.1 9.2.10 非常事態計画は、該当する全ての職員に配布されているか? 9.3. 重要項目: テスト済みの非常事態計画や災害復旧計画を使用しているか? 9.3.1 計画の最新版の写しが、離れた場所に安全に保管されているか? FISCAM SC-3.1 9.3.2 職員は自分の役割や責任について訓練を受けているか? FISCAM SC-2.3.NIST SP 800-18	
CP-2		緊急時対応計画	組織は、情報システムの緊急時対応計画を作成し導入する。緊急時対応計画には、緊急時の役割、責任、担当者名とその連絡先情報、およびシステムの混乱や障害が発生した場合の復旧関連の活動などを取り扱う。組織内で指定された責任者は、緊急時対応計画をレビュー、承認し、計画のコピーを主な緊急時対応要員に配付する。	なし。	(1) 組織は、関連する計画に責任を負う組織内の部署と連携して、緊急時対応計画を作成する。 管理強化策の補足ガイダンス：関連する計画の例としては、事業継続計画、災害復旧計画、運用継続計画、事業復興計画、インシデント対応計画、および緊急時行動計画などがあげられる。 (2)組織は、重大な事態に直面した時に、必要な情報処理能力および通信を確保し、環境的なサポートを利用できるようにするための、容量計画を作成する。		
	4.1.4					4.1.4 非常事態計画の策定とテストを行ったか? NIST SP 800-18	
	9.1.1					9.1.1 重要なデータファイルや業務が特定され、ファイルのバックアップ頻度が文書化されているか? FISCAM SC- SC-1.1および3.1 NIST SP 800-18	

	9.2 9.2.1 9.2.2 9.2.3 9.2.10					9.2. 重要項目: 包括的な非常事態計画を策定し、文書化しているか? 9.2.1 計画は、影響のある主要な部門の承認を受けたか? FISCAM SC-3.1 9.2.2 リカバリの責任は割り当てられているか? FISCAM SC-3.1 9.2.3 業務を復旧させる詳細な手順が定められているか? FISCAM SC-3.1 9.2.10 非常事態計画は、該当する全ての職員に配布されているか? FISCAM SC-3.1
	12.1.8					12.1.8 緊急時の手順は定められているか? NIST SP 800-18
	12.2.2					12.2.2 非常事態計画はあるか? NIST SP 800-18
CP-3		緊急時対応トレーニング	組織は、情報システムに関する緊急時の役割と責任について要員をトレーニングし、[指定:組織が定める頻度(少なくとも年1 回)]間隔で再トレーニングを行う。	なし。	(1) 組織は、組織の要員が、重大な状況下において効果的に対応できるように、緊急時対応トレーニングに模擬的なイベントを取り込む。 (2) 組織は、より徹底的で現実的なトレーニング環境を提供するための自動化メカニズムを使用する。	
	9.3.2					9.3.2 職員は自分の役割や責任について訓練を受けているか?
CP-4		緊急時対応計画のテストと実習	組織は、(i)[指定:組織が定めるテストおよび/または実習]を通じて、情報システムの緊急時対応計画を、[指定:組織が定める頻度(少なくとも年1 回)]間隔でテストおよび/または実習し、計画の有効性と組織の計画実施準備状況を判断する、また、(ii)緊急時対応計画のテスト/実習の結果をレビューし、訂正活動に着手する。	緊急時対応計画の潜在的な弱点を特定するには、さまざまなテスト/実習方法がある(たとえば、緊急時対応計画の全面的なテスト、機能ごとの実習/机上での実習など)。緊急時対応計画のテストおよび/または実習の難易度や厳密さは、FIPS199 が定める情報システムの影響レベルによって変わる。緊急時対応計画のテストおよび/または実習には、緊急時対応計画に従って緊急活動が行われた場合の、組織の業務や資産への影響(ミッション能力の削減など)および個人へ影響の特定が含まれる。情報技術の計画および機能をテスト、トレーニングおよび実習するプログラムに関するガイダンスは、NIST Special Publication 800-84 に記載されている。	(1) 組織は、関連する計画に責任を負う組織内の部署と連携して、緊急時対応計画のテストおよび/または実習を行う。 管理強化策の補足ガイダンス:関連する計画の例としては、事業継続計画、災害復旧計画、運用継続計画、事業復興計画、インシデント対応計画、および緊急時行動計画などがあげられる。 (2) 組織は、緊急時対応計画のテスト/実習を代替処理拠点で行い、緊急時対応要員が施設および使用可能なリソースに習熟できるようにするとともに、代替拠点が有する緊急時の運用サポート能力を評価する。 (3) 組織は、緊急時対応に関わる問題をより広く扱い、より現実的なテスト/実習のシナリオや環境を選択し、情報システムおよびシステムがサポートするミッションの重要性を効果的に強調するすることによって、緊急時対応計画の徹	
	4.1.4					4.1.4 非常事態計画の策定とテストを行ったか? NIST SP 800-18
	9.3.3					9.3.3 計画は定期的にテストされ、適宜再調整されているか?
CP-5		緊急時対応計画の更新	組織は、情報システムの緊急時対応計画を[指定:組織が定める頻度(少なくとも年1回)]間隔でレビューし、必要な場合には、修正する(たとえば、システム/組織の変更に伴う修正、または計画の導入、実施、テスト時に起きた問題に対処するための修正など)。	組織的な変更には、情報システムがサポートするミッション、機能、またはビジネスプロセスの変更が含まれる。組織は、緊急時対応計画(事業継続計画、災害復旧計画、運用継続計画、事業復興計画、インシデント対応計画、または緊急時行動計画など)に責任を持つ組織内の部署に対して、組織的な変更を行う旨を通知する。	なし。	
	9.3.1 9.3.3					9.3.1 計画の最新版の写しが、離れた場所に安全に保管されているか? FISCAM SC-3.1 9.3.3 計画は定期的にテストされ、適宜再調整されているか?
	10.2.12					10.2.12 非常事態計画等の関連ドキュメントは、システムの変更を反映するように更新されているか? FISCAM SC-2.1.NIST SP 800-18
CP-6		(情報システムの)代替保管拠点	組織は、代替保管拠点を特定し、情報システムのバックアップ情報を保存するのに必要な取り決めに着手する。	情報システムのバックアップを取る頻度およびバックアップ情報を代替保管拠点へ転送する頻度(指定されている場合)は、組織の情報システムの目標復旧時間および目標復旧ポイントによって決まる。	(1) 組織は、主要保存拠点から地理的に離れた場所を代替保管拠点とし、同一災害の影響を受けないようにする。 (2) 組織は、タイムリーかつ効果的な回復作業が容易になるように、代替保管拠点の設定を行う。 (3) 組織は、非常時(区域全体におよぶ混乱や災害が発生した場合など)に発生すると思われる、代替保管拠点へのアクセスに関わる問題を特定し、それらの問題を緩和するための活動を明確にする。	
	9.2.4 9.2.5 9.2.7 9.2.9					9.2.4 代替処理サイトはあるか? ある場合、契約や機関間の合意は行われているか? FISCAM SC-3.1.NIST SP 800-18 9.2.5 バックアップの保管場所は明確になっているか? NIST SP 800-18 9.2.7 システムやアプリケーションのドキュメントは、離れた場所に保管しているか? FISCAM SC-2.1 9.2.9 バックアップ保管サイトと代替サイトは、主サイトとは地理的に離れた場所にあり、物理的に保護されているか? FISCAM SC-2.1
CP-7		(情報システムの)代替処理拠点	組織は、代替処理拠点を指定し、主要処理拠点が機能しない場合に、組織の重要なミッション/ビジネス機能を支える情報システムの運用を、代替処理拠点にて[指定:組織が定める期間]内に再開させるための、取り決めに着手する。	業務を再開させるために必要な機器は、代替拠点で入手できる、または、契約により代替拠点へ配送されるようにする。情報システムの再開に要する時間枠は、組織が定める目標復旧時間に準拠する。	(1) 組織は、主要保存拠点から地理的に離れた場所を代替保管拠点とし、同一災害の影響を受けないようにする。 (2) 組織は、タイムリーかつ効果的な回復作業が容易になるように、代替保管拠点の設定を行う。 (3) 組織は、組織の可用性要件に従い、代替処理拠点に関する取り決め(サービス優先度に関する規定を含む)を作成する。 (4) 組織は、代替処理拠点の設定を十分に行い、組織にとって最低限必要な運用能力をサポートする運用拠点とし	

	9.1.3					9.1.3 処理の優先順位を確定し、マネジメント層の承認を受けているか? FISCAM SC-1.3 9.2.4 代替処理サイトはあるか? ある場合、契約や機関間の合意は行われているか? FISCAM SC-3.1,NIST SP 800-18 9.2.5 バックアップの保管場所は明確になっているか? NIST SP 800-18 9.2.7 システムやアプリケーションのドキュメントは、離れた場所に保管しているか? FISCAM SC-2.1 9.2.9 バックアップ保管サイトと代替サイトは、主サイトとは地理的に離れた場所にあり、物理的に保護されているか? FISCAM SC-2.1	
	9.2.4 9.2.5 9.2.7 9.2.9						
CP-8		電気通信サービス	組織は、主要な通信サービスの他に、代替の通信サービスを指定し、主要な通信サービスが利用できなくなった場合に、組織の重要なミッション/ビジネス機能を支える情報システムの運用を、代替通信サービスにて[指定:組織 が定める期間]内に再開させるための、取り決めに着手する。	主要な通信サービス、および/または代替の通信サービスが一般の通信事業者によって提供される場合、組織は、TSP(Telecommunications Service Priority:国家安全保障上の緊急時対応で使用するすべての通信サービスに対する電気通信サービス優先権)を要求する。TSP プログラムついての詳述http://tsp.ncs.gov を参照のこと。	(1) 組織は、組織の可用性要件に従い、主要な通信サービスおよび/代替通信サービスに関する取り決め(サービス優先度に関する規定を含む)を作成する。 (2) 組織は、代替通信サービスと主要通信サービスが、単一障害点を持たないようにする。 (3) 組織は、主要サービスプロバイダから十分に隔離された代替サービスプロバイダから通信サービスを受けることで、同一災害の影響を受けないようにする。 (4) 組織は、主要な通信サービスプロバイダおよび代替通信サービスプロバイダが、適切な緊急時対応計画を備えることを要求する。		
CP-9		情報システムのバックアップ	組織は、情報システムに含まれる、ユーザレベル、およびシステムレベルの情報(システム状態についての情報を含む)を[指定:組織が定める頻度]間隔でバックアップし、バックアップ情報を保管場所(または記憶場所)に格納 し、保護する。	情報システムのバックアップを取る頻度およびバックアップ情報を代替保管拠点へ転送する頻度(指定されている場合)は、組織の情報システムの目標復旧時間および目標復旧ポイントによって決まる。バックアップする情 報に関しては、情報の完全性および可用性の確保が重要である一方で、情報の種類やFIPS199 の影響レベルによっ ては、情報の不正開示に特別な注意を払わなければならないこともある。また、リスクアセスメントの結果によっては、 バックアップ情報の暗号化が必要となる場合もある。転送中のバックアップ情報の保護に関しては、本管理策の範囲外 である。関連セキュリティ管理策:MP-4、MP-5。	(1) 組織は、記録媒体の信頼性と情報の完全性を確認するために、バックアップ情報のテストを[指定:組織が定める頻度]間隔で行う。 (2) 組織は、緊急時対応計画のテストの一環として、情報システム機能の復旧時にバックアップ情報を選択的に使用する。 (3) 組織は、オペレーティングシステムやそのほかの重要な情報システムソフトウェアのバックアップコピーを、別の場所にある施設、または運用ソフトウェアと同じ場所にない耐火性容器に保存する。 (4) 組織は、システムのバックアップ情報を、不正な変更から保護する。 管理強化策の補足ガイダンス:組織は、情報システムのバックアップの完全性を保護するために、適切なメカニズム(電子署名、暗号学的ハッシュ関数など)を採用する。システムバックアップ情報の機密性の保護は、本管理策の		10.5 バックアップ 10.5.1 情報のバックアップ
	9.1.1					9.1.1 重要なデータファイルや業務が特定され、ファイルのバックアップ頻度が文書化されているか? FISCAM SC- SC-1.1および3.1,NIST SP 800-18 9.2.6 バックアップは所定の方法で作成され、最新のファイルが損傷を受けた場合にバックアップが破壊されるのを防ぐために、オフサイトにおけるローテーションの頻度は十分か? FISCAM SC-2.1 9.2.9 バックアップ保管サイトと代替サイトは、主サイトとは地理的に離れた場所にあり、物理的に保護されているか? 9.3.1 計画の最新版の写しが、離れた場所に安全に保管されているか? FISCAM SC-3.1 12.1.9 バックアップ手順は定められているか? NIST SP 800-18		
	9.2.6 9.2.9						
	9.3.1						
	12.1.9						
CP-10		情報システムの復旧と再構成	組織は、情報システムの混乱または障害の発生後、システムを元の状態に復旧し再構成するための、メカニズムを使用する。	情報システムを元のセキュアな状態に復旧し、再構成するには、すべてのシステムパラメータ(デフォルトまたは組織が設定したもの)に安全な値を再設定する、セキュリティにとって重要なパッチを再適用する、セキュリティ関連の構成設定を復旧する、システム文書および運用手順を利用可能にする、アプリケーションおよびシステムソフトウェアを安全に再インストールし、安全な設定を行う、安全性の確認が取れている最新のバックアップ情報をロードする、システムの全面的なテストを行う、などが必要となる。	(1) 組織は、情報システムの全面的な復旧や再構成を、緊急時対応計画のテストの一部として含ませる。		
	9.2.8					9.2.8 バックアップからリストアした後、システムのデフォルトはすべてリセットされるか? FISCAM SC-3.1	

	SP800-26		管理策	補足ガイダンス	管理強化策	具体的なコントロール目標と手法	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
IR		インシデント対応(Incident Response)	運用				
IR-1		インシデント対応の方針と手順	組織は、以下のものを策定および周知徹底し、定期的にレビュー／更新する。(i) 正式に文書化された、インシデント対応の方針。これらの方針では、目的、適用範囲、役割、責任、経営陣のコミットメント、組織間の調整、およびコンプライアンスを取り扱う。(ii) 正式に文書化された、インシデント対応方針の導入に関する手順。この手順は、インシデント対応方針の導入、ならびに関連する管理策の導入を容易にするために使用される。	インシデント対応の方針と手順は、適用法、大統領令、指令、方針、規制、基準、およびガイダンスに準拠する。インシデント対応の方針は、組織の一般的な情報セキュリティ方針の一部とすることができる。インシデント対応の手順は、一般的なセキュリティプログラムの一部として作成することもできれば、必要に応じて特定の情報システムに特化した形で作成することもできる。セキュリティ方針および手順のガイダンスは、NIST Special Publication 800-12に記載されている。インシデントの対応および報告に関するガイダンスは、NIST Special Publication 800-61 に記載されている。マルウェアによるインシデントの対処の仕方と防止法についてのガイダンスは、NIST Special Publication 800-83	なし。		13 情報セキュリティインシデントの管理 13.1 情報セキュリティの事象及び弱点の報告 13.1.1 情報セキュリティ事象の報告 13.1.2 セキュリティ弱点の報告 13.2 情報セキュリティインシデントの管理及びその改善 13.2.1 責任及び手順 13.2.2 情報セキュリティインシデントからの学習 13.2.3 証拠の収集
	14					14. 事故対応能力 OMB Circular A-130、III.FISCAM SP-3.4.NIST SP 800-18 14.1. 重要項目: システムにセキュリティ事故が発生した時にユーザーを手助けすることができるか? 14.1.1 正式な事故対応能力が利用可能か? FISCAM SP-3.4.NIST SP 800-18 14.1.2 事故を報告するプロセスが定められているか? FISCAM SP-3.4.NIST SP 800-18 14.1.3 事故が監視され、解決されるまで追跡しているか? NIST SP 800-18 14.1.4 職員は、事故を察知して処理するようトレーニングを受けているか? FISCAM SP-3.4.NIST SP 800-18 14.1.5 セキュリティアラートやアドバイザリを入手し、それに対応しているか? NIST SP 800-18 14.1.6 事故が発生した後に、事故対応手順やコントロール手法を変更するためのプロセスが定められているか? NIST SP 800-18 14.2. 重要項目: 事故に関連した情報を適切な機関と共有しているか? 14.2.1 事故情報や共通の脆弱性、脅威を、相互接続されたシステムのオーナーと共有しているか? OMB A-130、III.NIST SP 800-18 14.2.2 事故、共通の脆弱性や脅威に関わる事故情報をFedCIRC3 と共有しているか? OMB A-130、III.GISRA 14.2.3 必要に応じ、事故情報をFedCIRC、NIPC4、各地の法執行機関に報告しているか? OMB A-130、III.GISRA	
IR-2		インシデント対応のトレーニング	組織は、情報システムに関するインシデント対応の役割と責任について、要員をトレーニングし、[指定:組織が定める頻度(少なくとも年1 回)]間隔で再トレーニングを行う。	なし。	(1) 組織は、組織の要員が、重大な状況下において効果的に対応できるように、インシデント対応トレーニングに模擬的なイベントを取り込む。 (2) 組織は、より徹底的かつ現実的なトレーニング環境を提供するための、自動化メカニズムを使用する。		
	14.1.4					14.1.4 職員は、事故を察知して処理するようトレーニングを受けているか? FISCAM SP-3.4.NIST SP 800-18	
IR-3		インシデント対応のテストと実習	組織は、[指定:組織が定めるテストおよび／または実習]を通じて、情報システムのインシデント対応能力を、[指定:組織が定める頻度(少なくとも年1 回)]間隔でテストおよび／または実習し、インシデント対応の有効性を判断し、結果を文書化する。	情報技術の計画および機能をテスト、トレーニングし、実習するためのプログラムに関するガイダンスは、NIST Special Publication 800-84 に記載されている。	(1) 組織は、インシデント対応能力のテスト／実習を、より徹底的かつ効果的に行うための、自動化メカニズムを使用する。 管理強化策の補足ガイダンス:組織は、インシデント対応のテスト／実習を、より徹底的かつ効果的に行うための、自動化メカニズムを採用する。このために組織は、インシデント対応に関わる問題をより広く扱い、より現実的なテスト／実習のシナリオや環境を選択し、情報システムおよびシステムがサポートするミッションの重要性を効果的に強調するすることによって、インシデント対応計画の徹底的かつ効果		
IR-4		インシデントの対応	組織は、セキュリティインシデントを処理するためのインシデント処理機能を導入する。この機能には、準備、検知と分析、封じ込め、根絶、復旧などが含まれる。	インシデントに関する情報は、監査の監視、ネットワークの監視、物理的なアクセスの監視、およびユーザ／管理者の報告書など、さまざまな情報源から入手することができるが、これらに限定されるわけではない。組織は、継続的なインシデント対応活動から学んだ教訓を、インシデント対応手順に取り入れ、その手順を導入する。関連セキュリティ管理	(1) 組織は、インシデント対応プロセスをサポートする自動化メカニズムを使用する。		13.1 情報セキュリティの事象及び弱点の報告 13.1.1 情報セキュリティ事象の報告 13.1.2 セキュリティ弱点の報告
	2.1.5					2.1.5 セキュリティアラートやセキュリティ事故を分析し、是正措置を講じているか? FISCAM SP 3-4.NIST SP 800-18 14.1.1 正式な事故対応能力が利用可能か? FISCAM SP-3.4.NIST SP 800-18 14.1.2 事故を報告するプロセスが定められているか? FISCAM SP-3.4.NIST SP 800-18 14.1.6 事故が発生した後に、事故対応手順やコントロール手法を変更するためのプロセスが定められているか? NIST SP 800-18	
	14.1.1 14.1.2 14.1.6						

IR-5		インシデントの監視	組織は、情報システムのセキュリティインシデントを継続的に追跡し、文書化する。	なし。	(1) 組織は、セキュリティインシデントの追跡、およびインシデントに関する情報の収集と分析を支援する自動化メカニズムを使用する。		13.2.3 証拠の収集
	14.1.3					14.1.3 事故が監視され、解決されるまで追跡しているか? NIST SP 800-18	
IR-6		インシデントの報告	組織は、インシデント情報を関係当局に迅速に報告する。	報告するインシデント情報の種別、内容、適時性、および報告先の当局または組織は、適用法、大統領令、指令、方針、規制、基準、およびガイダンスに準拠する。組織の担当者は、サイバーセキュリティーインシデントに関する報告を、US-CERT Concept of Operations for Federal Cyber Security Incident Handling が規定する時間内に、US-CERT(US コンピュータ事故緊急対応チーム (http://www.us-cert.gov)に対して行う。また、さらなるセキュリティインシデントを防止するために、発生したインシデント情報以外にも、情報システムの欠点や脆弱性に関する情報を、組織内の適切な担当者に時期を失せず報告する。インシデント報告のガイダンスは、NIST Special Publication	(1) 組織は、セキュリティインシデントの報告を支援する自動化メカニズムを使用する。		13.2.1 責任及び手順 13.2.2 情報セキュリティインシデントからの学習
	14.1.2					14.1.2 事故を報告するプロセスが定められているか? FISCAM SP-3.4,NIST SP 800-18	
	14.1.3					14.1.3 事故が監視され、解決されるまで追跡しているか? NIST SP 800-18	
	14.2.1					14.2.1 事故情報や共通の脆弱性、脅威を、相互接続されたシステムのオーナーと共有しているか? OMB A-130、III,NIST SP 800-18	
	14.2.2					14.2.2 事故、共通の脆弱性や脅威に関わる事故情報をFedCIRC3 と共有しているか? OMB A-130、III,GISRA	
	14.2.3					14.2.3 必要に応じ、事故情報をFedCIRC、NIPC4、各地の法執行機関に報告しているか? OMB A-130、III,GISRA	
IR-7		インシデント対応の支援	組織は、情報システムのユーザに対して、セキュリティインシデントの対応と報告に関する助言と支援を与える人的資源を提供する。この人的資源は、組織のインシデント対応能力に不可欠である。	インシデント対応を支援するために導入される人的資源には、ヘルプデスクや支援グループなどがある。また、必要に応じて、フォレンジックサービスへのアクセスなどが考えられる。	(1) 組織は、インシデント処理関連の情報およびサポートを、ユーザが入手しやすくするための、自動化メカニズムを使用する。		
	8.1.1					8.1.1 アドバイスしてくれるヘルプデスクやグループがあるか?	
	14.1.1					14.1.1 正式な事故対応能力が利用可能か? FISCAM SP-3.4,NIST SP 800-18	

		管理策:	補足ガイダンス:	管理強化策:
CP	緊急時対応計画 (Contingency Planning)	運用		
CP-1	緊急時対応計画の方針と手順	管理策:組織は、以下のものを策定および周知徹底し、定期的にレビュー／更新する。(i) 正式に文書化された、緊急時対応計画の方針。これらの方針では、目的、適用範囲、役割、責任、経営陣のコミットメント、組織間の調整、およびコンプライアンスを取り扱う。(ii)正式に文書化された、緊急時対応計画の方針の導入に関する手順。この手順は、緊急時対応計画に関する方針の導入、ならびに関連する管理策の導入を容易にするために使用される。	緊急時対応計画の方針と手順は、適用法、大統領令、指令、方針、規制、基準、およびガイダンスに準拠する。緊急時対応計画の方針は、組織の一般的な情報セキュリティ方針の一部とすることができる。緊急時対応計画の手順は、一般的なセキュリティプログラムの一部として作成することもできれば、必要に応じて特定の情報システムに特化した形で作成することもできる。緊急時対応計画の作成に関するガイダンスは、NIST Special Publication 800-34に記載されている。セキュリティ方針および手順のガイダンスは、NIST Special Publication 800-12 に記載されている。	なし。
CP-2	緊急時対応計画	管理策:組織は、情報システムの緊急時対応計画を作成し導入する。緊急時対応計画には、緊急時の役割、責任、担当者名とその連絡先情報、およびシステムの混乱や障害が発生した場合の復旧関連の活動などを取り扱う。組織内で指定された責任者は、緊急時対応計画をレビュー、承認し、計画のコピーを主な緊急時対応要員に配付する。	補足ガイダンス:なし。	管理強化策: (1) 組織は、関連する計画に責任を負う組織内の部署と連携して、緊急時対応計画を作成する。 管理強化策の補足ガイダンス:関連する計画の例としては、事業継続計画、災害復旧計画、運用継続計画、事業復興計画、インシデント対応計画、および緊急時行動計画などがあげられる。 (2)組織は、重大な事態に直面した時に、必要な情報処理能力および通信を確保し、環境的なサポートを利用できるようにするための、容量計画を作成する。
CP-3	緊急時対応トレーニング	管理策:組織は、情報システムに関する緊急時の役割と責任について要員をトレーニングし、[指定:組織が定める頻度 (少なくとも年1 回)]間隔で再トレーニングを行う。	補足ガイダンス:なし。	管理強化策: (1) 組織は、組織の要員が、重大な状況下において効果的に対応できるように、緊急時対応トレーニングに模擬的なイベントを取り込む。 (2) 組織は、より徹底的で現実的なトレーニング環境を提供するための自動化メカニズムを使用する。
CP-4	緊急時対応計画のテストと実習	管理策:組織は、(i)[指定:組織が定めるテストおよび／または実習]を通じて、情報システムの緊急時対応計画を、[指定:組織が定める頻度(少なくとも年1 回)]間隔でテストおよび／または実習し、計画の有効性と組織の計画実施準備状況を判断する、また、(ii)緊急時対応計画のテスト／実習の結果をレビューし、訂正活動に着手する。	補足ガイダンス:緊急時対応計画の潜在的な弱点を特定するには、さまざまなテスト／実習方法がある(たとえば、緊急時対応計画の全面的なテスト、機能ごとの実習／机上での実習など)。緊急時対応計画のテストおよび／または実習の難易度や厳密さは、FIPS199 が定める情報システムの影響レベルによって変わる。緊急時対応計画のテストおよび／または実習には、緊急時対応計画に従って緊急活動が行われた場合の、組織の業務や資産への影響(ミッション能力の削減など)および個人へ影響の特定が含まれる。情報技術の計画および機能をテスト、トレーニングおよび実習するプログラムに関するガイダンスは、NIST Special Publication 800-84 に記載されている。	管理強化策: (1) 組織は、関連する計画に責任を負う組織内の部署と連携して、緊急時対応計画のテストおよび／または実習を行う。 管理強化策の補足ガイダンス:関連する計画の例としては、事業継続計画、災害復旧計画、運用継続計画、事業復興計画、インシデント対応計画、および緊急時行動計画などがあげられる。 (2) 組織は、緊急時対応計画のテスト／実習を代替処理拠点で行い、緊急時対応要員が施設および使用可能なリソースに習熟できるようにするとともに、代替拠点が有する緊急時の運用サポート能力を評価する。 (3) 組織は、緊急時対応に関わる問題をより広く扱い、より現実的なテスト／実習のシナリオや環境を選択し、情報システムおよびシステムがサポートするミッションの重要性を効果的に強調することによって、緊急時対応計画の徹底的かつ効果的なテスト／実習を行うための、自動化メカニ
CP-5	緊急時対応計画の更新	管理策:組織は、情報システムの緊急時対応計画を[指定:組織が定める頻度(少なくとも年1回)]間隔でレビューし、必要な場合には、修正する(たとえば、システム／組織の変更に伴う修正、または計画の導入、実施、テスト時に起きた問題に対処するための修正など)。	補足ガイダンス:組織的な変更には、情報システムがサポートするミッション、機能、またはビジネスプロセスの変更が含まれる。組織は、緊急時対応計画(事業継続計画、災害復旧計画、運用継続計画、事業復興計画、インシデント対応計画、または緊急時行動計画など)に責任を持つ組織内の部署に対して、組織的な変更を行う旨を通知する。	管理強化策:なし。

CP-6	(情報システムの)代替保管拠点	管理策:組織は、代替保管拠点を特定し、情報システムのバックアップ情報を保存するのに必要な取り決めに着手する。	補足ガイダンス:情報システムのバックアップを取る頻度およびバックアップ情報を代替保管拠点へ転送する頻度(指定されている場合)は、組織の情報システムの目標復旧時間および目標復旧ポイントによって決まる。	管理強化策: (1) 組織は、主要保存拠点から地理的に離れた場所を代替保管拠点とし、同一災害の影響を受けないようにする。 (2) 組織は、タイムリーかつ効果的な回復作業が容易になるように、代替保管拠点の設定を行う。 (3) 組織は、非常時(区域全体におよぶ混乱や災害が発生した場合など)に発生すると思われる、代替保管拠点へのアクセスに関わる問題を特定し、それらの問題を緩和するための活動を明確にする。
CP-7	(情報システムの)代替処理拠点	管理策:組織は、代替処理拠点を指定し、主要処理拠点が機能しない場合に、組織の重要なミッション/ビジネス機能を支える情報システムの運用を、代替処理拠点にて[指定:組織が定める期間]内に再開させるための、取り決めに着手する。	補足ガイダンス:業務を再開させるために必要な機器は、代替拠点で入手できる、または、契約により代替拠点へ配送されるようにする。情報システムの再開に要する時間枠は、組織が定める目標復旧時間に準拠する。	管理強化策: (1) 組織は、主要保存拠点から地理的に離れた場所を代替保管拠点とし、同一災害の影響を受けないようにする。 (2) 組織は、タイムリーかつ効果的な回復作業が容易になるように、代替保管拠点の設定を行う。 (3) 組織は、組織の可用性要件に従い、代替処理拠点に関する取り決め(サービス優先度に関する規定を含む)を作成する。 (4) 組織は、代替処理拠点の設定を十分に行い、組織にとって最低限必要な運用能力をサポートする運用拠点として、すぐに利用できるようにする。
CP-8	電気通信サービス	管理策:組織は、主要な通信サービスの他に、代替の通信サービスを指定し、主要な通信サービスが利用できなくなった場合に、組織の重要なミッション/ビジネス機能を支える情報システムの運用を、代替通信サービスにて[指定:組織 が定める期間]内に再開させるための、取り決めに着手する。	補足ガイダンス:主要な通信サービス、および/または代替の通信サービスが一般の通信事業者によって提供される場合、組織は、TSP(Telecommunications Service Priority:国家安全保障上の緊急時対応で使用するすべての通信サービスに対する電気通信サービス優先権)を要求する。TSP プログラムついての詳述http://tsp.ncs.gov を参照のこと。	管理強化策: (1) 組織は、組織の可用性要件に従い、主要な通信サービスおよび/代替通信サービスに関する取り決め(サービス優先度に関する規定を含む)を作成する。 (2) 組織は、代替通信サービスと主要通信サービスが、単一障害点を持たないようにする。 (3) 組織は、主要サービスプロバイダから十分に隔離された代替サービスプロバイダから通信サービスを受けることで、同一災害の影響を受けないようにする。 (4) 組織は、主要な通信サービスプロバイダおよび代替通信サービスプロバイダが、適切な緊急時対応計画を備えることを要求する。
CP-9	情報システムのバックアップ	管理策:組織は、情報システムに含まれる、ユーザレベル、およびシステムレベルの情報(システム状態についての情報を含む)を[指定:組織が定める頻度]間隔でバックアップし、バックアップ情報を保管場所(または記憶場所)に格納し、保護する。	補足ガイダンス:情報システムのバックアップを取る頻度およびバックアップ情報を代替保管拠点へ転送する頻度(指定 されている場合)は、組織の情報システムの目標復旧時間および目標復旧ポイントによって決まる。バックアップする情 報に関しては、情報の完全性および可用性の確保が重要である一方で、情報の種類やFIPS199 の影響レベルによっては、情報の不正開示に特別な注意を払わなければならないこともある。また、リスクアセスメントの結果によっては、バックアップ情報の暗号化が必要となる場合もある。転送中のバックアップ情報の保護に関しては、本管理策の範囲外 である。関連セキュリティ管理策:MP-4、MP-5。	管理強化策: (1) 組織は、記録媒体の信頼性と情報の完全性を確認するために、バックアップ情報のテストを[指定:組織が定める頻度]間隔で行う。 (2) 組織は、緊急時対応計画のテストの一環として、情報システム機能の復旧時にバックアップ情報を選択的に使用する。 (3) 組織は、オペレーティングシステムやそのほかの重要な情報システムソフトウェアのバックアップコピーを、別の場所にある施設、または運用ソフトウェアと同じ場所にない耐火性容器に保存する。 (4) 組織は、システムのバックアップ情報を、不正な変更から保護する。 管理強化策の補足ガイダンス:組織は、情報システムのバックアップの完全性を保護するために、適切なメカニズム(電子署名、暗号学的ハッシュ関数など)を採用する。システムバックアップ情報の機密性の保護は、本管理策の範囲外である。関連セキュリティ管理策:MP-4、MP-5。

CP-10	情報システムの復旧と再構成	管理策：組織は、情報システムの混乱または障害の発生後、システムを元の状態に復旧し再構成するための、メカニズムを使用する。	補足ガイダンス：情報システムを元のセキュアな状態に復旧し、再構成するには、すべてのシステムパラメータ（デフォルトまたは組織が設定したもの）に安全な値を再設定する、セキュリティにとって重要なパッチを再適用する、セキュリティ関連の構成設定を復旧する、システム文書および運用手順を利用可能にする、アプリケーションおよびシステムソフトウェアを安全に再インストールし、安全な設定を行う、安全性の確認が取れている最新のバックアップ情報をロードする、システムの全面的なテストを行う、などが必要となる。	管理強化策： (1) 組織は、情報システムの全面的な復旧や再構成を、緊急時対応計画のテストの一部として含ませる。

		管理策:	補足ガイダンス:	管理強化策:
IR	インシデント対応(Incident Response)	運用		
IR-1	インシデント対応の方針と手順	管理策:組織は、以下のものを策定および周知徹底し、定期的にレビュー／更新する。(i) 正式に文書化された、インシデント対応の方針。これらの方針では、目的、適用範囲、役割、責任、経営陣のコミットメント、組織間の調整、およびコンプライアンスを取り扱う。(ii) 正式に文書化された、インシデント対応方針の導入に関する手順。この手順は、インシデント対応方針の導入、ならびに関連する管理策の導入を容易にするために使用される。	補足ガイダンス:インシデント対応の方針と手順は、適用法、大統領令、指令、方針、規制、基準、およびガイダンスに準拠する。インシデント対応の方針は、組織の一般的な情報セキュリティ方針の一部とすることができる。インシデント対応の手順は、一般的なセキュリティプログラムの一部として作成することもできれば、必要に応じて特定の情報システムに特化した形で作成することもできる。セキュリティ方針および手順のガイダンスは、NIST Special Publication 800-12に記載されている。インシデントの対応および報告に関するガイダンスは、NIST Special Publication 800-61 に記載されている。マルウェアによるインシデントの対処の仕方と防止法についてのガイダンスは、NIST Special Publication 800-83 に記載されている。	管理強化策:なし。
IR-2	インシデント対応のトレーニング	管理策:組織は、情報システムに関するインシデント対応の役割と責任について、要員をトレーニングし、[指定:組織が定める頻度(少なくとも年1 回)]間隔で再トレーニングを行う。	補足ガイダンス:なし。	管理強化策: (1) 組織は、組織の要員が、重大な状況下において効果的に対応できるように、インシデント対応トレーニングに模擬的なイベントを取り込む。 (2) 組織は、より徹底的かつ現実的なトレーニング環境を提供するための、自動化メカニズムを使用する。
IR-3	インシデント対応のテストと実習	管理策:組織は、[指定:組織が定めるテストおよび／または実習]を通じて、情報システムのインシデント対応能力を、[指定:組織が定める頻度(少なくとも年1 回)]間隔でテストおよび／または実習し、インシデント対応の有効性を判断し、結果を文書化する。	補足ガイダンス:情報技術の計画および機能をテスト、トレーニングし、実習するためのプログラムに関するガイダンスは、NIST Special Publication 800-84 に記載されている。	管理強化策: (1) 組織は、インシデント対応能力のテスト／実習を、より徹底的かつ効果的に行うための、自動化メカニズムを使用する。 管理強化策の補足ガイダンス:組織は、インシデント対応のテスト／実習を、より徹底的かつ効果的に行うための、自動化メカニズムを採用する。このために組織は、インシデント対応に関わる問題をより広く扱い、より現実的なテスト／実習のシナリオや環境を選択し、情報システムおよびシステムがサポートするミッションの重要性を効果的に強調することによって、インシデント対応計画の徹底的かつ効果的なテスト／実習を行うための、自動化メカニズムを採用す
IR-4	インシデントの対応	管理策:組織は、セキュリティインシデントを処理するためのインシデント処理機能を導入する。この機能には、準備、検知と分析、封じ込め、根絶、復旧などが含まれる。	補足ガイダンス:インシデントに関する情報は、監査の監視、ネットワークの監視、物理的なアクセスの監視、およびユーザ／管理者の報告書など、さまざまな情報源から入手することができるが、これらに限定されるわけではない。組織は、継続的なインシデント対応活動から学んだ教訓を、インシデント対応手順に取り入れ、その手順を導入する。関連セキュリティ管理策:AU-6、PE-6。	管理強化策: (1) 組織は、インシデント対応プロセスをサポートする自動化メカニズムを使用する。
IR-5	インシデントの監視	管理策:組織は、情報システムのセキュリティインシデントを継続的に追跡し、文書化する。	補足ガイダンス:なし。	管理強化策: (1) 組織は、セキュリティインシデントの追跡、およびインシデントに関する情報の収集と分析を支援する自動化メカニズムを使用する。

IR-6	インシデントの報告	管理策：組織は、インシデント情報を関係当局に迅速に報告する。	補足ガイダンス：報告するインシデント情報の種別、内容、適時性、および報告先の当局または組織は、適用法、大統領令、指令、方針、規制、基準、およびガイダンスに準拠する。組織の担当者は、サイバーセキュリティーインシデントに関する報告を、US-CERT Concept of Operations for Federal Cyber Security Incident Handling が規定する時間内に、US-CERT(US コンピュータ事故緊急対応チーム（http://www.us-cert.gov）に対して行う。また、さらなるセキュリティインシデントを防止するために、発生したインシデント情報以外にも、情報システムの欠点や脆弱性に関する情報を、組織内の適切な担当者に時期を失せず報告する。インシデント報告のガイダンスは、NIST Special Publication 800-61 に記載されている。	管理強化策： (1) 組織は、セキュリティインシデントの報告を支援する自動化メカニズムを使用する。
IR-7	インシデント対応の支援	管理策：組織は、情報システムのユーザに対して、セキュリティインシデントの対応と報告に関する助言と支援を与える人的資源を提供する。この人的資源は、組織のインシデント対応能力に不可欠である。	補足ガイダンス：インシデント対応を支援するために導入される人的資源には、ヘルプデスクや支援グループなどがある。また、必要に応じて、フォレンジックサービスへのアクセスなどが考えられる。	管理強化策： (1) 組織は、インシデント処理関連の情報およびサポートを、ユーザが入手しやすくするための、自動化メカニズムを使用する。

2012年度研究レポート

クラウドコンピューティング情報リスク

古川　正紀

1. クラウドコンピューティング情報リスク
クラウドコンピューティング導入の際に、検討しなければならない情報リスクを以下に例示する。

【ポリシーおよび組織的リスク】

テーマ	事　象	原　因	ビジネス課題	セキュリティーガイド
	ロックイン	・ 技術とソリューションにおける標準の欠如 ・ プロバイダの選定不備 ・ サプライヤの冗長化（SUPPLIER REDUNDANCY）の欠如 ・ 利用規約の完全性と透明性の欠如	・ 企業の評判 ・ 個人の秘密データ ・ 個人データ ・ 個人データ（重要） ・ サービス提供 ― リアルタイムによるサービス ・ サービス提供	10.2.1（第三者が提供するサービス） 10.2.2（第三者が提供するサービスの監視及びレビュー） 10.2.3（第三者が提供するサービスの変更に対する管理） 12.6.1（技術的ぜい弱性の管理）
	ガバナンスの喪失	・ 役割と責任の不明確性 ・ 役割定義の適用の不備 ・ クラウド外の契約上の義務または責任のクラウドへの適用 ・ 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 ・ クラウドをまたがるアプリケーションに潜在する相互依存性 ・ 技術とソリューションにおける標準の欠如 ・ 複数の司法管轄権を跨るデータ格納とそれに対する認識の欠如 ・ ソースコードエスクロー（預託）契約の欠如 ・ 脆弱性診断プロセスに関する管理の欠如 ・ クラウドのインフラに適用できる認証スキームの欠如 ・ 司法管轄権に関する情報の欠如	・ 企業の評判 ・ 顧客の信頼 ・ 従業員の忠誠心と経験 ・ 個人の秘密データ ・ 個人データ ・ 個人データ（重要） ・ サービス提供 ― リアルタイムによるサービス ・ サービス提供	4.2.1（クラウドサービス利用におけるリスクアセスメントの留意点） 5.1.1（情報セキュリティ基本方針文書） 5.1.2（情報セキュリティ基本方針のレビュー） 8.1.3（雇用条件） 12.6.1（技術的ぜい弱性の管理）
	コンプライアンスの課題	・ 利用者に監査または認証の証明書が提供されない問題 ・ 技術とソリューションにおける標準の欠如 ・ 複数の司法管轄権を跨るデータ格納とそれに対する認識の欠如 ・ クラウドのインフラに適用できる認証スキームの欠如 ・ 司法管轄権に関する情報の欠如 ・ 利用規約の完全性と透明性の欠如	・ 認証	14.1.2（事業継続及びリスクアセスメント） 15.1.1（適用法令の識別） 15.1.3（組織の記録の保護） 15.2.1（セキュリティ方針及び標準の順守） 15.2.2（技術的順守点検） 15.3.1（情報システムの監査に対する管理策）

	他の共同利用者の行為による信頼の喪失	・ リソース分離の欠如 ・ 不信の伝播に対する隔離の欠如 ・ ハイパーバイザの脆弱性	・ 企業の評判 ・ 個人の秘密データ ・ 個人データ ・ 個人データ(重要) ・ サービス提供 ― リアルタイムによるサービス ・ サービス提供	6.2.1 (外部組織に関係したリスクの識別) 7.1.3 (資産利用の許容範囲)
	クラウドサービスの終了または障害	・ プロバイダの選定不備 ・ サプライヤの冗長化(SUPPLIER REDUNDANCY)の欠如 ・ 利用規約の完全性と透明性の欠如	・ 企業の評判 ・ 顧客の信頼 ・ 従業員の忠誠心と経験 ・ サービス提供 ― リアルタイムによるサービス ・ サービス提供	6.2.3 (第三者との契約におけるセキュリティ) 10.1.2 (変更管理)
	クラウドプロバイダの買収	・ 利用規約の完全性と透明性の欠如	・ 企業の評判 ・ 顧客の信頼 ・ 従業員の忠誠心と経験 ・ 知的財産 ・ 個人の秘密データ ・ 個人データ ・ 個人データ(重要) ・ 人材データ ・ サービス提供 ― リアルタイムによるサービス ・ サービス提供	6.2.3 (第三者との契約におけるセキュリティ) 10.1.2 (変更管理)
	サプライチェーンにおける障害	・ 利用規約の完全性と透明性の欠如 ・ クラウドをまたがるアプリケーションに潜在する相互依存性 ・ プロバイダの選定不備 ・ サプライヤの冗長化(SUPPLIER REDUNDANCY)の欠如	・ 企業の評判 ・ 顧客の信頼 ・ 個人の秘密データ ・ 個人データ ・ 個人データ(重要) ・ サービス提供 ― リアルタイムによるサービス ・ サービス提供	10.2.1 (第三者が提供するサービス) 10.2.2 (第三者が提供するサービスの監視及びレビュー) 10.2.3 (第三者が提供するサービスの変更に対する管理)

1. クラウドコンピューティング情報リスク
クラウドコンピューティング導入の際に、検討しなければならない情報リスクを以下に例示する。

【技術的リスク】

テーマ	事　象	原　因	ビジネス課題	セキュリティーガイド
	リソースの枯渇(リソース割当の過不足) ・ 顧客に対し、追加的な機能を提供できない ・ 現在、契約中の機能を提供できない	・ リソースの使用に関する不正確なモデリング ・ クラウドのインフラに対する投資またはリソース割当の不足 ・ リソースの利用上限制限ポリシーの欠如 ・ サプライヤの冗長化(SUPPLIER REDUNDANCY)の欠如	・ 企業の評判 ・ 顧客の信頼 ・ サービス提供 ・ アクセス制御／認証／権限付与(root／管理者対その他)	
	隔離の失敗	・ ハイパーバイザの脆弱性 ・ リソース分離の欠如 ・ 不信の伝播に対する隔離の欠如 ・ 内部(クラウド)ネットワークへの偵察行為が発生する可能性 ・ 共同利用者からの覗き見の可能性	・ 企業の評判 ・ 顧客の信頼 ・ 個人の秘密データ ・ 個人データ ・ 個人データ(重要) ・ サービス提供 ー リアルタイムによるサービス ・ サービス提供	
	クラウドプロバイダ従事者の不正ー特権の悪用	・ 役割と責任の不明確性 ・ 役割定義の適用の不備 ・「知る必要性」原則の不適用 ・ AAAの脆弱性 ・ システムまたはOSの脆弱性 ・ 物理的なセキュリティ手順の不備 ・ 暗号化状態でのデータ処理が不可能であること ・ アプリケーションの脆弱性またはパッチ管理の不備	・ 企業の評判 ・ 顧客の信頼 ・ 従業員の忠誠心と経験 ・ 知的財産 ・ 個人の秘密データ ・ 個人データ ・ 個人データ(重要) ・ 人材データ ・ サービス提供 ー リアルタイムによるサービス ・ サービス提供	

管理用インターフェースの悪用（操作、インフラストラクチャアクセス）	・ AAAの脆弱性 ・ 管理用インターフェースへのリモートアクセス ・ 設定ミス ・ システムまたはOSの脆弱性 ・ アプリケーションの脆弱性またはパッチ管理の不備	・ 企業の評判 ・ 顧客の信頼 ・ 個人の秘密データ ・ 個人データ ・ 個人データ（重要） ・ サービス提供 ー リアルタイムによるサービス ・ サービス提供 ・ クラウドサービスの管理用インターフェース	
データ転送途上における攻撃	・ AAAの脆弱性 ・ 通信路暗号の脆弱性 ・ アーカイブおよび転送中のデータの暗号化の強度不足または未実施 ・ 内部（クラウド）ネットワークへの偵察行為が発生する可能性 ・ 共同利用者からの覗き見の可能性 ・ 利用規約の完全性と透明性の欠如	・ 企業の評判 ・ 顧客の信頼 ・ 知的財産 ・ 個人の秘密データ ・ 個人データ ・ 個人データ（重要） ・ 人材データ ・ バックアップまたはアーカイブデータ	
データ漏えい（アップロード時、ダウンロード時、クラウド間転送）	・ AAAの脆弱性 ・ 通信路暗号の脆弱性 ・ 内部（クラウド）ネットワークへの偵察行為が発生する可能性 ・ 共同利用者からの覗き見の可能性 ・ 暗号化状態でのデータ処理が不可能であること ・ アプリケーションの脆弱性またはパッチ管理の不備	・ 企業の評判 ・ 顧客の信頼 ・ 従業員の忠誠心と経験 ・ 知的財産 ・ 個人の秘密データ ・ 個人データ ・ 個人データ（重要） ・ 人材データ ・ クレデンシャル ・ ユーザディレクトリ（データ） ・ クラウドサービスの管理用インターフェース	
セキュリティが確保されていない、または不完全なデータ削除	・ 機密性の高いメディアのサニタイゼーション（記録の抹消）	・ 個人の秘密データ ・ 個人データ ・ 個人データ（重要） ・ クレデンシャル	

DDoS攻撃（分散サービス運用妨害攻撃）	・ 設定ミス ・ システムまたはOSの脆弱性 ・ フィルタリングリソースの不備または設定ミス	・ 企業の評判 ・ 顧客の信頼 ・ サービス提供 ― リアルタイムによるサービス ・ サービス提供 ・ クラウドサービスの管理用インターフェース ・ ネットワーク（接続等）	
EDoS攻撃（経済的な損失を狙ったサービス運用妨害攻撃）	・ AAAの脆弱性 ・ ユーザプロビジョニングの脆弱性 ・ ユーザプロビジョニング削除の脆弱性 ・ 管理用インターフェースへのリモートアクセス ・ リソースの利用上限制限ポリシーの欠如	・ 企業の評判 ・ 顧客の信頼 ・ サービス提供 ― リアルタイムによるサービス ・ サービス提供	
暗号鍵の喪失	・ 不適切な鍵管理手順 ・ 乱数生成器への低エントロピーの入力	・ 知的財産 ・ 個人の秘密データ ・ 個人データ ・ 個人データ（重要） ・ 人材データ ・ クレデンシャル	
不正な探査またはスキャンの実施	・ 内部（クラウド）ネットワークへの偵察行為が発生する可能性 ・ 共同利用者からの覗き見の可能性	・ 企業の評判 ・ 顧客の信頼 ・ サービス提供 ― リアルタイムによるサービス ・ サービス提供	
サービスエンジンの侵害	・ ハイパーバイザの脆弱性 ・ リソース分離の欠如	・ 個人の秘密データ ・ 個人データ ・ 個人データ（重要） ・ 人材データ ・ サービス提供 ― リアルタイムによるサービス ・ サービス提供	
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	・ 利用規約の完全性と透明性の欠如 ・ 複数利害関係者間で矛盾するSLA条項 ・ 役割と責任の不明確性	・ 知的財産 ・ 個人の秘密データ ・ 個人データ ・ 個人データ（重要）	

1. クラウドコンピューティング情報リスク
クラウドコンピューティング導入の際に、検討しなければならない情報リスクを以下に例示する。

【法律的リスク】

テーマ	事　象	原　因	ビジネス課題	セキュリティーガイド
	証拠提出命令と電子的証拠開示	・ リソース分離の欠如 ・ 複数の司法管轄権を跨るデータ格納とそれに対する認識の欠如 ・ 司法管轄権に関する情報の欠如	・ 企業の評判 ・ 顧客の信頼 ・ 個人の秘密データ ・ 個人データ ・ 個人データ(重要) ・ サービス提供 ー リアルタイムによるサービス ・ サービス提供	
	司法権の違いから来るリスク	・ 司法管轄権に関する情報の欠如 ・ 複数の司法管轄権を跨るデータ格納とそれに対する認識の欠如	・ 企業の評判 ・ 顧客の信頼 ・ 個人の秘密データ ・ 個人データ ・ 個人データ(重要) ・ サービス提供 ー リアルタイムによるサービス ・ サービス提供	
	データ保護に関するリスク	・ 司法管轄権に関する情報の欠如 ・ 複数の司法管轄権を跨るデータ格納とそれに対する認識の欠如	・ 企業の評判 ・ 顧客の信頼 ・ 個人の秘密データ ・ 個人データ ・ 個人データ(重要) ・ サービス提供 ー リアルタイムによるサービス ・ サービス提供	
	ライセンスに関するリスク	・ 利用規約の完全性と透明性の欠如	・ 企業の評判 ・ サービス提供 ー リアルタイムによるサービス ・ 認証	

1. クラウドコンピューティング情報リスク
クラウドコンピューティング導入の際に、検討しなければならない情報リスクを以下に例示する。

【クラウドに特化していないリスク】

テーマ	事　象	原　因	ビジネス課題	セキュリティーガイド
	ネットワークの途絶	・ 設定ミス ・ システムまたはOSの脆弱性 ・ リソース分離の欠如 ・ 事業継続計画および災害復旧計画の欠如、不備、テストの未実施	・ サービス提供 ― リアルタイムによるサービス ・ サービス提供	
	ネットワークの管理（ネットワークの混雑、接続ミス、最適でない使用）	・ 設定ミス ・ システムまたはOSの脆弱性 ・ リソース分離の欠如 ・ 事業継続計画および災害復旧計画の欠如、不備、テストの未実施	・ 企業の評判 ・ 顧客の信頼 ・ 従業員の忠誠心と経験 ・ サービス提供 ― リアルタイムによるサービス ・ サービス提供 ・ ネットワーク（接続等）	
	ネットワークトラフィックの改変	・ ユーザプロビジョニングの脆弱性 ・ ユーザプロビジョニング削除の脆弱性 ・ 通信路暗号の脆弱性 ・ 脆弱性診断プロセスに関する管理の欠如	・ 企業の評判 ・ 顧客の信頼 ・ 個人の秘密データ ・ 個人データ ・ 個人データ（重要） ・ サービス提供 ― リアルタイムによるサービス ・ サービス提供	
	特権の（勝手な）拡大	・ AAAの脆弱性 ・ ユーザプロビジョニングの脆弱性 ・ ユーザプロビジョニング削除の脆弱性 ・ ハイパーバイザの脆弱性 ・ 役割と責任の不明確性 ・ 役割定義の適用の不備 ・ 「知る必要性」原則の不適用 ・ 設定ミス	・ 個人の秘密データ ・ 個人データ ・ 個人データ（重要） ・ 人材データ ・ アクセス制御／認証／権限付与（root／管理者対その他） ・ ユーザディレクトリ（データ）	

ソーシャルエンジニアリング攻撃（なりすまし）	・ セキュリティ意識の欠如 ・ ユーザプロビジョニングの脆弱性 ・ リソース分離の欠如 ・ 通信路暗号の脆弱性 ・ 物理的なセキュリティ手順の不備	・ 企業の評判 ・ 顧客の信頼 ・ 従業員の忠誠心と経験 ・ 知的財産 ・ 個人の秘密データ ・ 個人データ ・ 個人データ（重要） ・ 人材データ ・ アクセス制御／認証／権限付与（root／管理者対その他） ・ クレデンシャル	
運用ログの喪失または改ざん	・ ログの収集および保存に関するポリシーの欠如または手順の不備 ・ AAAの脆弱性 ・ ユーザプロビジョニングの脆弱性 ・ ユーザプロビジョニング削除の脆弱性 ・ 法的対応体制の不備 ・ システムまたはOSの脆弱性	・ 運用ログ（クラウド利用者およびクラウドプロバイダ）	
セキュリティログの喪失または改ざん（フォレンジック捜査の操作）	・ 物理的なセキュリティ手順の不備！情報源が不明 ・ AAAの脆弱性 ・ ユーザプロビジョニングの脆弱性 ・ ユーザプロビジョニング削除の脆弱性	・ セキュリティログ	
バックアップの喪失、盗難	・ 物理的なセキュリティ手順の不備！情報源が不明 ・ AAAの脆弱性 ・ ユーザプロビジョニングの脆弱性 ・ ユーザプロビジョニング削除の脆弱性	・ 企業の評判 ・ 顧客の信頼 ・ 個人の秘密データ ・ 個人データ ・ 個人データ（重要） ・ 人材データ ・ サービス提供 ― リアルタイムによるサービス ・ サービス提供 ・ バックアップまたはアーカイブデータ	

	構内への無権限アクセス(装置その他の設備への物理的アクセスを含む)	・ 物理的なセキュリティ手順の不備	・ 企業の評判 ・ 顧客の信頼 ・ 個人の秘密データ ・ 個人データ ・ 個人データ(重要) ・ 人材データ ・ サービス提供 ― リアルタイムによるサービス ・ サービス提供 ・ バックアップまたはアーカイブデータ	
	コンピュータ設備の盗難	・ 物理的なセキュリティ手順の不備	・ 個人の秘密データ ・ 個人データ ・ 個人データ(重要) ・ 人材データ ・ 物理的なハードウェア	
	自然災害	・ 事業継続計画および災害復旧計画の欠如、不備、テストの未実施	・ 企業の評判 ・ 顧客の信頼 ・ 個人の秘密データ ・ 個人データ ・ 個人データ(重要) ・ 人材データ ・ サービス提供 ― リアルタイムによるサービス ・ サービス提供 ・ バックアップまたはアーカイブデータ	

2012年度研究レポート

クラウドサービスの利用と情報セキュリティリスクについて（考察メモ）

山﨑　直和

平成24年3月30日
ITガバナンス研究会
山崎　直和

クラウドサービスの利用と情報セキュリティリスクについて（考察メモ）

１．検討の方向性（考え方）

今回、外部のクラウドサービスを利用するにあたり、どのような情報セキュリティリスクが潜在しているか、その対応策としてどのようなものがあるか、等を検討していくにあたり、まずは実際に発生したセキュリティ事故（障害事例）に着目して検討を進めることにした。

２．検討手順

一般的に実際に発生したセキュリティ事故（障害事例）についてはその特性上、公表されることは少ないため、某雑誌に掲載されていた事例より抽出することにした。その事例をセキュリティ事故として通常考えられる分類ごとにマッピングしたのが別表である。

この表に記載の事例のうち、クラウドサービスの利用時にも考慮が必要と考えられるものについて「○」を記載し深堀検討を進めていくこととした。具体的には「○」を記載した項目のうち、青網掛けをした事例に着目して詳細検討を行うことにした。

以上

別表

No.	分類	具体的に考えられるセキュリティ事故(例)	クラウドサービス利用時においても配慮が必要と思われるもの(想定)	クラウドサービスに関係する障害事例(報道ベース) ※行政＆情報システム2011年8月号より抜粋	回避策(一例)
1	機微情報(個人情報等)の漏洩	PC端末等の盗難／紛失による漏洩			情報機器管理の徹底
2		USBメモリ等の保存メディアの盗難／紛失による漏洩			情報機器管理の徹底
3		公開サイトへの誤掲載による漏洩			人的ミスの撲滅(情報リテラシーの徹底)
4		システムバグ等による意図しない相手への情報共有	○	・2009年3月、Coocle Docsのアプリケーションバグにより意図しない相手へのドキュメント共有が発生。	システム品質の向上
5		メール誤送信による漏洩			人的ミスの撲滅(情報リテラシーの徹底)
6		ウィルスやスパイウェア感染による漏洩	○		ウィルス対策等の徹底
7		情報機器処分時のデータ消し忘れ等による漏洩			人的ミスの撲滅(情報リテラシーの徹底)
8		ネットワーク上からのハッキングによる漏洩	○		通信の暗号化
9		「なりすまし」による漏洩	○		本人確認機能の強化
10		PC画面の盗み見等による漏洩			セキュリティ教育の徹底
11		データ持ち出し時の事故等による漏洩			人的ミスの撲滅(情報リテラシーの徹底)
12		悪意を持った内部関係者(運用員等)による漏洩	○		罰則規定強化
13		悪意を持った外部関係者(委託事業者等)による漏洩	○		契約上の縛り(SLA縛り)
14		機微情報が記載された紙等の不適切な廃棄による漏洩			人的ミスの撲滅(情報リテラシーの徹底)
15		バックアップデータの不適切な扱いによる漏洩	○		情報機器管理の徹底
16		その他理由による情報漏洩			
17	情報消失	PC端末等の盗難／紛失による消失			情報機器管理の徹底
18		USBメモリ等の保存メディアの盗難／紛失による消失			情報機器管理の徹底
19		ウィルス感染等による消失	○		ウィルス対策等の徹底
20		突然の電源断による消失	○		システム品質の向上
21		保存メディアの損傷等による消失	○		情報機器管理の徹底
22		誤消去等の人為的なトラブルによる消失	○		人的ミスの撲滅(情報リテラシーの徹底)
23		システムの脆弱性を突く外部からの攻撃による消失	○	・2009年4月、Vaserv.com内のウェブサイトのデータが仮想化技術Hyper-VMの脆弱性を突く攻撃により消失。(約10万人のデータが破壊、約50%の顧客に影響あり)	システム品質の向上
24		ディスク障害等のハードウェアトラブルによる消失	○	・2009年10月、T-Mobileの多機能携帯電話「Sidekick」用サービスからサーバ障害によりユーザデータが消失。	システム品質の向上
25		保存ミス等、データの取り扱い不全による消失	○		人的ミスの撲滅(情報リテラシーの徹底)
26		その他理由による情報消失			
27	業務停止	ウィルス感染による業務停止	○		ウィルス対策等の徹底
28		サーバ、システム等のダウンによる業務停止	○	・2009年7月、Google App Engineがデータストアアクセスによるエラー率向上が原因で約4時間利用不能になる。 ・2010年6月、Google App Engine for Businessにおいて、機能停止、パフォーマンス低下、エラー等の問題が続発。 ・2011年5月、NTTPCのWebARENA CLOUD9のファイルシステムトラブルにより仮想サーバ停止、データ不整合が発生。 ・2011年4月、アマゾンのAmazon Web Serviceのストレージ機能の不具合が発生したことで、同サービスを利用した他サイトが停止。	システム品質の向上
29		ネットワークからのアタック攻撃(Ddos攻撃等)による業務停止、アクセス障害	○	・2009年12月、セールスフォースのDNSサービスプロバイダーがDDoS攻撃によりアクセス障害が発生。	専用ネットワークの適正
30		停電や電源障害等による業務停止	○	・2011年2月、Google App Engineがプライマリーデータセンターの電源障害により停止。	システム品質の向上
31		システム誤操作等の人為的ミスによる業務停止	○		人的ミスの撲滅(情報リテラシーの徹底)
32		その他の理由による業務停止			
33	その他	ソフトウェアの不正コピー、不正インストール	○		セキュリティ教育の徹底
34		掲示板・チャット等への荒らし行為			セキュリティ教育の徹底
35		ファイル交換ソフトなどの違法利用			セキュリティ教育の徹底
36		アカウントの不正利用	○		セキュリティ教育の徹底

2012年度研究レポート

「クラウドサービスを利用して実現したシステムでセキュリティリスクが考えられる事象」について

久住　昭之

「クラウドサービスを利用して実現したシステムで情報セキュリティリスクが考えられる事象」について

ITガバナンス研究会
久住　昭之

○「情報セキュリティリスクが考えられる事象」を考える上での観点
（1）クラウド未利用システムとクラウド利用システムで、実現環境にどのような違いがあるか、その違いが異なる情報セキュリティリスク（クラウド利用時特有）を発生させることにつながるか。
（2）実現環境とは異なる要因による情報セキュリティリスクとしてどのようなものが考えられるか

（1）実現環境の違いにより想定されるリスク

実現環境	実現環境面での違い		違いにより想定されるリスク		リスク回避策
	クラウド未利用システム	クラウド利用システム	オペレーショナルリスク（事業者がやるべきことをやらないリスク）	非オペレーショナルリスク	
設備環境	自社専用	複数利用者共用		同一設備を使っている他利用者に対する外部からのサイバー攻撃の巻き添えになることによるシステム利用不能・データへのアクセス不可、データの改ざん・消失や漏洩等	（改ざん・消失に対する）データバックアップ／システム分散
				クラウドサービス提供者を狙ったサイバー攻撃等によるシステム利用不能・データへのアクセス不可、データの改ざん・消失や漏洩等	同上
				他利用者アプリケーションのバグ影響によるシステム利用不能・データへのアクセス不可、自社データの改ざん・消失や漏洩等	同上
				工事・点検等による設備事故に伴うシステム利用不能、自社データの消失・漏洩等	同上
			設備管理の怠慢によるシステム停止やデータ消失等		（起こさないための）管理体制や実施状況の定期的モニタリング（監査） （起きた場合に備えた）データバックアップ／システム分散
立地環境	自社判断で決定可能	クラウドサービス提供者に依存（不明確）		自然あるいは外的事故等の人為災害によるシステム利用不能、データ消失等	立地条件確認
オペレーション環境	自社情報セキュリティポリシーに基づきオペレーション内容を決定し、具体的な実施手順や実施について統制が可能	契約において自社セキュリティポリシーにあったオペレーション内容とサービスレベルを規定可能だが、その実施および具体的な実施手順等はクラウドサービス提供者に依存	クラウド未利用システムで自社が要求するレベルと同等レベルのサービスレベルを契約で規定していても、（タイムラグの発生や怠慢等により）実行されないことによるインシデント発生		（起こさないための）実施体制・状況の定期的モニタリング（監査） 契約上、違反時のペナルティを規定
			クラウド未利用システムで自社が要求するレベルと同等レベルのサービスレベルを契約で規定していても、具体的実施手順の不備や人為ミスによるインシデント発生		（起こさないための）実施体制・状況、手順書整備状況、要員教育実施状況の定期的モニタリング（監査）

（2）他要因により想定されるリスク

区分	想定されるリスク	リスク回避策
経営	クラウドサービス提供者の倒産によるサービス提供中止、設備等の差し押さえによる自社データへのアクセス不可やデータ漏洩・消失	利用しているクラウドサービス提供者の経営状況のモニタリング、システム分散
	クラウドサービス提供者の経営環境変化によるサービス提供中止による自社データの他サービスへの移行不可	同上
政治	（DC立地場所で適用される法に基づく）当局によるデータの差し押さえによる自社データへのアクセス不可やデータ漏洩・消失	立地場所の把握と政情把握、法制度の確認、システム分散
	第三者によるDCそのものへの物理的な破壊的攻撃（テロによる爆破等）の巻き添えによるデータの消失	システム分散

※上記（1）、（2）のリスク発生要因は、主として情報システムを自社のコントロール下に置けず、事業者に依存することによる。

2012年度研究レポート

クラウドサービスの利用と情報セキュリティリスク対応

瀬戸　昭彦

	事象	リスク対象	考えられる原因など
1	情報漏えい	取引先や顧客などの営業機密情報 社員の人事情報や個人情報 開発中の新商品に関する情報 社内での会議情報	不正アクセス 目的外使用 管理ミス セキュリティホール ファイル共有ソフトから
2	データ喪失	顧客情報 販売情報などの営業情報 人事情報 会計	天災 バックアップ取得ミス 記録媒体の盗難 サーバ、ストレージ等の物理障害
3	運営事業者によるサービス停止	継続的なサービス利用 中途解約でのデータの保障	対象サービスの終了 事業者の倒産 システムの見直し、変更
4	データの改ざん	クラウドシステムに保管してあるデータ	不正アクセス、フィッシング
5	データ保管場所不明	海外拠点での保管 保管場所を指定できない	クラウド事業者の都合
6	解約時のデータ確保	登録してるデータの確保 記憶媒体への残存	