株式会社レスキューナウ　セキュリティチェックシート

◆本チェックシートは、株式会社レスキューナウが提供するサービスについて、そのセキュリティ対策を記載したものです。
◆株式会社レスキューナウは、下記認証登録範囲の情報セキュリティマネジメントシステムについて
ISO/IEC27001:2013／JIS Q 27001:2014 の要求事項に適合し、認証登録番号：IS610416 を保有しています。
<認証登録範囲>
本社、不動前オフィスにおける「危機管理サービスのシステム運用」「コンテンツ配信サービスのシステム運用」
<取得時期>
2006年6月9日 (初回取得時)
<認証期間>
認証機関：BSIグループジャパン株式会社
◆本チェックシートの項目は、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2013年度版
（https://www.meti.go.jp/policy/netsecurity/downloadfiles/cloudsec2013fy.pdf）
を基に、任意で項目の追加削除、及び主客体の解釈を加えて作成したものです。

大項番	中項番	項番	確認事項	備考
1 情報セキュリティ基本方針				
		1	情報セキュリティ基本方針を定めた文書が経営陣によって承認され、全従業員及び関連する外部関係者に公表し、通知すること。	経営者によって承認された情報セキュリティ基本方針を定め、全従業員には社内規程として周知し、関連する外部関係者様向けには当社ホームページ（https://www.rescuenow.co.jp/about/isms）で公開しています。
		2	情報セキュリティに関する基本方針を定めた文書は、定期的または重大な変化が生じた場合にレビューすること。	情報セキュリティマネジメントシステム（以下「ISMS」）を構築し、情報セキュリティの基本方針に定めた通りに運用し、定期的また重大な変化が生じた場合は臨時に監査及び見直しを行っています。
2 情報セキュリティのための組織				
	1 内部組織			
		1	経営陣は、情報セキュリティの責任及び関与を明示し、責任の明確な割り当て及び承認を通して組織内におけるセキュリティを積極的に支持すること。	ISMSの整備・運用方法を明記した文書（以下「ISMSマニュアル」）に経営陣の責任及びコミットメントを明記し、実施しています。 また経営陣を含めて情報セキュリティに関連した課題を取り扱う情報セキュリティ委員会を設置し、組織内で課題を共有しています。
		2	情報セキュリティ責任者とその役割を明確に定めること。	ISMSマニュアルおよび情報セキュリティに関する社内規程（以下「ISMS規程」）にて情報セキュリティに関する責任と役割について明確に定めています。
		3	情報セキュリティ対策、設備の認可に対する手順等を明確にし、文書化すること。	ISMS規程にて、情報セキュリティ対策を明記しています。
		4	クラウドサービス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。また、提供するクラウドサービスについて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。	本チェックシート等にて、クラウドサービス利用者に対し、提供するクラウドサービスに関するセキュリティ対策を記載し、提供しています。
		5	サービスのサポート窓口を明確にし、外部に公開すること。	以下のとおりメールもしくはお電話でお問い合わせいただく窓口を公開しています。 メール：soluion-cs@rescuenow.co.jp 電話：050-3627-8567 提供時間：月～金　9:30～12:00、13:00～17:00（※土日祝・年末年始を除く）
3 人的資源のセキュリティ				
	1 雇用前			
		1	従業員のセキュリティの役割及び責任は、情報セキュリティ基本方針に従って定め、文書化すること。また、雇用前にセキュリティの役割及び責任についての契約書を交わし雇用契約を結ぶこと。	情報セキュリティ基本方針（https://www.rescuenow.co.jp/about/isms）に従い、従業員が順守すべきISMS規程を定めています。 また、雇用する従業員と交わす雇用契約書には就業規則及び社内規程の順守について記載し、署名と押印により明確に同意を得て契約を締結しています。
	2 雇用期間中			
		1	すべての従業員に対して、情報セキュリティに関する意識向上のための教育・訓練を実施すること。	雇用する従業員には、入社時に研修を実施しており、社内規程の教育を行っています。 また、全従業員を対象とした情報セキュリティに関する教育を年に１回以上実施しており、情報セキュリティ基本方針の見直し時期に見直し結果を周知したり、時事トピックスを取り上げたりして情報セキュリティに対する意識向上を促進しています。
		2	セキュリティ違反を犯した従業員に対する対応手続きを備えること。	従業員がセキュリティ違反を犯した場合、当該従業員は当社就業規則に規定された懲戒の対象となることをISMS規程に記載しています。
	3 雇用の終了又は変更			
		1	従業員の雇用の終了または変更となった場合に、情報資産の返却やアクセス権の解除・変更の手続きについて明確にすること。	従業員の組織変更によるアクセス権の変更および退職時の手続は、ISMS規程に明記しています。詳細は以下の通りです。 ・アクセス権、リモートアクセス権の変更申請により削除または変更 ・退職時は全てのシステムで登録されている当該アカウントを削除し、貸与PC、鍵、カードキー等を回収
4 資産の管理				
		1	情報資産について明確にし、重要な情報資産の目録及び各情報資産の利用の許容範囲に関する文書を作成し、維持すること。また情報資産について管理責任者を指定すること。	ISMS規程に基づき情報資産台帳を作成しており、情報資産台帳はISMSの運用ルールに従い定期的に見直し、更新しています。
		2	組織に対しての価値、法的要求事項、取り扱いに慎重を要する度合い及び重要性の観点から情報資産を分類すること。	情報資産台帳では、資産名、資産形態、保有部門、保管場所、公開レベル、利用可能者、個人情報有無、オーナー、情報管理者、資産価値、法的要求事項、廃棄方法、保管期限、更新日ごとに情報資産を分類しています。
5 物理的及び環境的セキュリティ				
		1	重要な情報資産がある領域を保護するために、物理的セキュリティ境界（壁、有人受付、カード制御による入口等）を用いること。	重要な情報資産がある領域にはエリアとして分割しており、ISMSで管理する社内レイアウト図に明記しています。
		2	重要な情報資産がある領域へ許可された者のみがアクセスできるように入退室等を管理するための手順、管理方法を文書化すること。	重要な情報資産がある領域にはセキュリティカード制御による入退室制限を実施しています。 入退室管理手順や管理方法はISMS規程の記載内容に従い運用しています。
		3	サーバーが設置されているデータセンターは耐震構造となっていること。	取り扱いサービス毎に異なるデータセンターを選択しており、それぞれで耐震対策を行っています。 詳しくは各サービスのセキュリティチェックシートをご確認ください。
		4	データセンターの落雷対策を確認すること。	取り扱いサービス毎に異なるデータセンターを選択しており、それぞれで落雷対策を行っています。 詳しくは各サービスのセキュリティチェックシートをご確認ください。

		5	データセンターの水害対策を確認すること。	取り扱いサービス毎に異なるデータセンターを選択しており、それぞれで水害対策を行っています。 詳しくは各サービスのセキュリティチェックシートをご確認ください。
		6	データセンターの静電気対策を確認すること。	取り扱いサービス毎に異なるデータセンターを選択しており、それぞれで静電気対策を行っています。 詳しくは各サービスのセキュリティチェックシートをご確認ください。
6 運用のセキュリティ・アクセス制御				
		1	クラウドサービスの提供に用いるアプリケーション、オペレーティングシステム、サーバー、ネットワーク機器の運用管理の手順について文書化し、維持していくこと。	アプリケーション、OS、サーバー、ネットワーク機器の運用管理の手順については文書を作成しています。この文書は操作方法の変更や機材追加・変更が発生する都度、更新しています。
		2	クラウドサービスの提供に用いるアプリケーション、オペレーティングシステム、サーバー、ネットワーク機器の変更について管理すること。またクラウドサービス利用者に影響を及ぼすものは事前に通知すること。	アプリケーションのアップデートやオペレーティングシステムのメンテナンス等利用者に影響を及ぼすものについては、 ３週間前にクラウドサービス上で通知しています。
		3	クラウドサービスを利用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。利用できるOSとブラウザに変更が生じる場合は事前に通知すること。	利用できるウェブブラウザの種類・バージョンについては、各サービスごとのホームページに公開しています。
		4	クラウドサービスの提供に用いるアプリケーション、オペレーティングシステム、サーバー、ネットワーク機器の技術的脆弱性に関する情報は、定期的に収集し、適切にパッチの適用を行うこと。	脆弱性情報について日次で収集するとともにベンダーやセキュリティ機関（JPCERT等）からの情報を随時受け、影響について確認しています。またパッチの適用についても手順に則り適用作業を実施しています。
		5	クラウドサービスの資源の利用状況について監視・調整をし、利用状況の予測に基づいて設計した容量・性能等の要求事項について文書化し、維持していくこと。	クラウドサービスの利用状況については監視を実施しています。利用状況の推移から増強・増設の計画を立て、その内容については文書を作成しています。
		6	クラウドサービスの提供に用いるアプリケーション、オペレーティングシステム、サーバー、ネットワーク機器について脆弱性診断を行うこと。また、その結果を基に対策を行うこと。	自社にて第三者機関が提供する診断ツールを用いて年間少なくとも１回脆弱性診断を行っています。 またその結果に基づき改善等対応作業を実施しています。
		7	モバイルコードの利用が認可された場合は、認可されたモバイルコードが、明確に定められたセキュリティ方針に従って動作することを確実にする環境設定を行うことが望ましい。 また、認可されていないモバイルコードを実行できないようにすることが望ましい。	モバイルコードの利用を許可しておりません。
		8	クラウドサービス利用者の情報、ソフトウェア及びソフトウェアの設定について定期的にバックアップを取得し、検査すること。	お客様のデータは毎日無停止でバックアップを取得しています。
		9	クラウドサービスの提供に用いるアプリケーション、オペレーティングシステム、サーバー、ネットワーク機器の稼働監視をすること。サービスの停止を検知した場合は、利用者に対して通知すること。	稼働状況については監視しています。 サービスの停止を検知した場合は、ご契約時にご登録いただいた緊急連絡先へ一斉メール通知を行います。
		10	クラウドサービスの提供に用いるアプリケーション、オペレーティングシステム、サーバー、ネットワーク機器の障害監視をすること。障害を検知した場合は、利用者に対して通知すること。	機器障害については監視をしています。 サービスの提供に影響がある場合は、ご契約時にご登録いただいた緊急連絡先へ一斉メール通知を行います。
		11	システムの運用担当者の作業については記録すること。	システムの運用担当者の作業についてはすべて記録を残しています。作業を実施する際には変更管理ルールに則り、作業内容について承認者の承認を得て、相互確認を行いながら実施しています。
		12	例外処理及びセキュリティ事象を記録した監査ログを取得すること。また該当のログのアラートについては定期確認し、改竄、許可されていないアクセスがないように保護する。	監査ログについては、日次で該当ログのアラートを取得しています。また該当ログは運用管理者及びアクセスが許可された者がアクセスできる場所に保管しています。
		13	クラウドサービス上で取得する利用者の活動、例外処理及びセキュリティ事象を記録した監査ログについて明示すること。また監査ログの保持する期間、提供方法、提供のタイミングについて明示すること。	アプリケーションの監査ログの保存期間や保存形式、閲覧はアプリケーションの運用管理者が管理できるようになっています。提供するクラウドサービスへのアクセスログは、半年間保存しています。 ※監査ログ機能による提供が不可能なログの提供サービスは行っていません。
		14	クラウドサービスの提供に用いるアプリケーション、オペレーティングシステム、サーバー、ネットワーク機器については正確な時刻源と同期させること。	NTP を利用して、オペレーティングシステム、ネットワーク機器等、正確な時刻源と時刻同期を実施しています。
		15	クラウド基盤システムへのアクセスについては、各個人に一意な識別子にし、セキュリティに配慮したログオン手順、認証技術によって制御すること。またアクセス制御方針について文書化すること。	システムのアカウントについてはISMS規程に則り、各個人に一意の識別子を付与しています。 またシステムにアクセスする際にはVPN網を利用し、さらにアクセスが許可されていない者がアクセス、ログオンできないよう制御しています。アカウントや暗号化の方針についてはISMS規程に定めています。
		16	クラウド基盤システムへのアクセス権限の追加・削除・変更について手順を備えること。また特権の割り当て及び利用は制限し、管理すること。	システムへのアクセス権限の追加・削除・変更の方法については手順の文書化を行っています。 特権については利用者をインフラ運用管理担当者のみとしています。
		17	システムの運用担当者が利用するパスワードについては管理し、また良質なパスワードにすること。	パスワードについてはISMS規程に則り、管理しています。
		18	クラウド事業者は、クラウド利用者がネットワークサービスの利用に関する方針を策定できるよう、クラウドサービス利用の管理に係る情報の種類及びその内容を提示することが望ましい。	ログイン方法、権限付与等に内容についてはサービスマニュアルに記載しております。
		19	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。	提供するクラウドサービスは災害等の緊急時に利用するという観点からアクセス制御は行っていません。
		20	クラウド事業者は、各クラウド利用者に割り当てたコンピューティング資源に、他のクラウド利用者や許可されていないユーザがアクセスできないように管理し、物理的な設定や移行にかかわらず、仮想環境の分離を確実にすることが望ましい。 ネットワーク若しくはインタフェースの分離がなされていない場合、クラウド事業者は、アプリケーションレイヤの通信のエンドツーエンドでの暗号化を考慮することが望ましい。 クラウド事業者は、クラウド利用者の情報及びソフトウェアへのバックドアアクセスの可能性を識別するために、クラウド環境における情報セキュリティについて評価を実施することが望ましい。	提供するクラウドサービスはマルチテナント構成となっています。 登録されたデータについてはサービスを利用されているお客様以外アクセスできないようにデータへのアクセス制限を行っています。
		21	提供するクラウドサービスにおいて利用者のID登録・削除機能を提供すること。	提供するクラウドサービスにおいて、利用者IDの登録・削除の機能を提供しています。
		22	提供するクラウドサービスにおいて特権の割り当て及び利用制限し、管理する機能を提供すること。	提供するクラウドサービスにおいて、サービス利用に関わる権限の割り当て等を管理する機能を提供しています。

		23	提供するクラウドサービスにてパスワード管理ができるような機能を提供すること。また良質なパスワードを確実にする機能があること。	提供するクラウドサービスにおいて、パスワードの文字数、複雑度等を設定する機能を提供しています。
		24	提供するクラウドサービスで提供している情報セキュリティ対策及び機能を列記し、明示すること。	提供するクラウドサービスにおいて、提供しているセキュリティ対策及び機能については各サービスのサポートサイトにて公開しています。
		25	一定の使用中断時間が経過したときには、使用が中断しているセッションを遮断すること。またリスクの高い業務用ソフトウェアについては、接続時間の制限を利用すること。	提供するクラウドサービスでは、人事データ運用などリスクの高い処理画面においては一定時間操作がなかった場合にログイン画面に戻るようになっています。
		26	ネットワークを脅威から保護、またネットワークのセキュリティを維持するためにネットワークを適切に管理し、アクセス制御をすること。	セキュリティを維持するためにネットワーク構成の管理、ネットワーク機器監視を実施しています。またアクセス制御についても文書化し、管理・実施しています。
		27	ネットワーク管理者の権限割り当て及び利用は制限し、管理すること。またネットワーク管理者もアクセスを管理するためにセキュリティに配慮したログオン手順、認証技術によって制御すること。	ネットワーク管理者の権限については、システムの運用管理担当者のみとしています。アクセスする際にはVPN網を利用します。またアクセスが許可されていない者がアクセス、ログオンできないように制御しています。アカウントや暗号化方針についてはISMS規程にて定めています。
		28	外部及び内部からの不正なアクセスを防止する装置（ファイアウォール等）を導入すること。また利用することを許可したサービスへのアクセスだけを提供すること。	ファイアウォールを導入しています。サービスで利用するポートのみを開放しており、その他のポートについてはアクセスできないように制限しています。
		29	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。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ものに明示すること。	提供するクラウドサービスの認証方法は以下のとおりです。 IDパスワードによるフォーム認証
		30	クラウドサービスの契約が終了した場合にデータが消去されること。消去されるなら、その時期や削除される範囲について確認すること。	契約終了日から2週間以内にサービスの利用環境および、そこに登録されたデータの削除を行います。 また、その際には削除完了通知を発行します。 ※データの返却は行っておりません。
		31	クラウドサービスを利用するネットワーク経路が暗号化されていることを確認すること。クラウドサービスで利用する情報がシステム上で暗号化されていること。	伝送データは、すべて暗号化しています。
7 供給者関係				
		1	外部組織がかかわる業務プロセスから、情報資産に対するリスクを識別し、適切な対策を実施すること。	お客様が登録した情報については、特定の状況によりお客様からのご依頼があった場合を除き変更や削除を実施しません。また本サービス以外の目的のために利用・複製したり、第三者への利用の許可や開示、漏洩したりすることもありません。
8 情報セキュリティ事象・情報セキュリティインシデント				
		1	すべての従業員はシステムまたはサービスに関連する情報セキュリティの事象を覚知した場合、できるだけすみやかに報告するようにすること。また、セキュリティ弱点を覚知した場合はどのようなものでも記録し、報告すること。	情報セキュリティ事象が発生または発見した場合の報告手順や報告する上での観点、連絡経路等をISMS規程に定めています。
		2	情報セキュリティインシデントに対する迅速、効果的で毅然とした対応をするために責任体制及び手順書を確立すること。	ISMS規程に情報セキュリティインシデントに対応するための報告連絡手段や対応手続を定めています。
		3	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明示すること。	各サービスにおける情報セキュリティインシデントは、社内での監査を行い公開が必要なインシデントについては弊社ホームページ等にて公開します。
9 事業継続マネジメントにおける情報セキュリティの側面				
		1	業務プロセスの中断を引き起こし得る事象が特定されていること。	事業継続計画書の中で業務プロセスの中断を起こし得るリスクの特定を行っています。
		2	クラウド事業者は、クラウドサービスを提供するシステムの冗長化を図るとともに、クラウドサービスの冗長化の状況を、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。	全てのサーバー、ネットワーク、ストレージ、データについて冗長化を実施しています。
		3	事業継続計画については定期的に試験・更新すること。	事業継続計画書は定期的に試験・更新を実施しています。
		4	クラウドサービス提供に用いる機材は、停電や電力障害が生じた場合に電源を確保するための対策を講じること。	提供するクラウドサービスが稼働するデータセンターごとに対応を講じています。
		5	クラウドサービス提供に用いる機材を設置する部屋には、火災検知・通報システム及び消火設備を用意すること。	提供するクラウドサービスが稼働するデータセンターごとに対応を講じています。
10 順守				
		1	関連する法令、規則及び契約上の要求事項並びにこれらの要求事項を満たすための組織の取り組み方を明確に定め、文書化し、最新に保つこと。また重要な記録については消失、破壊及び改ざんから保護し、適切に管理すること。	関連法規の更新状況についてはISMSで定期的に確認し、該当文書を更新することになっています。 ISMSで管理対象となっている文書や記録は、保管部署や保管期間を定め適切に管理しています。
		2	クラウド事業者は、クラウド事業を営む地域（国、州など）、データセンターの所在する地域（国、州など）及びクラウド事業者自らが適用を受ける法令、規制及び契約上の要求事項を明示することが望ましい。	提供するサービス毎にデータセンター、稼働する地域の選択を行っていますが、全て国内で稼働しております。適用をうける法令、規約及び契約上の要求事項は国内法に準拠します。
		3	クラウド事業者は、自らの知的財産権についてクラウド利用者に利用を許諾する範囲及び制約を、クラウド利用者に通知することが望ましい。	提供する各サービスの利用規約において、知的財産権について利用を許諾する範囲を定めています。
		4	認可されていない目的のための情報処理施設の利用は阻止すること。	ISMS規程にて制限区画やその他の区画へのアクセスが許可される者について定めており、アクセスが許可されていない者はアクセスできないように制限しています。
		5	個人データ及び個人情報は、関連する法令、規制、及び適用がある場合には、契約事項の中の要求にしたがって確実に保護すること。	個人情報保護基本方針、個人情報の取り扱いに関するガイドラインに沿って保護し、取り扱います。個人情報保護基本方針、個人情報の取り扱いに関するガイドラインは当社ホームページ上に公開しています。 https://www.rescuenow.co.jp/about/privacy-policy
		6	クラウド事業者は、独立したレビュー及び評価（例えば、内部／外部監査、認証、脆弱性、ペネトレーションテストなど）を定期的に実施し、情報セキュリティ基本方針及び適用される法的要件を組織が遵守していることを確実にすること。	提供する各サービスについてセキュリティ対策の評価を定期に実施しています。
11 その他				
		1	記録媒体（書類、記録メディア）の保管管理については適切に行うこと。また廃棄する際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。また再利用の際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。	ISMS規程にて、記録媒体の情報取扱方法（保管、廃棄）を定め、適切に取り扱っています。
		2	重要な情報資産については、机の上に放置せず安全な場所に保管すること（クリアデスク）。また離席時には情報を盗み見られないように情報端末の画面をロックすること（クリアスクリーン）。	ISMSマニュアルに則り、クリアデスクおよびスクリーンロック等の対策を講じるよう定め、実施しています。

		3	従業員のパソコンにウィルス対策を行うこと。また技術的脆弱性に関する情報は、定期的に収集し、適切にパッチの適用を行うこと。	ISMS規程にて、クライアントPCに関する利用者の遵守事項（ウィルス対策等）を定め、遵守しています。 技術的脆弱性に関する情報は、ウィルス、スパイウエア、技術的脆弱性等への対策について、情報収集と情報周知を実施しています。
		4	サービス提供を終了する場合は、利用者に対して事前に通知を行うこと。	サービス提供の終了およびサービス廃止の場合、１年以上前に通知します。