セキュリティチェックシート（経済産業省 ガイドライン版）

本チェックシートは株式会社 World Wide System が提供する「Smart Receico レシートキャンペーンシステム」について、そのセキュリティ対策を記載したものです。また、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 年版を基に、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。本チェックシートは、改善のために予告なく変更することがあります。

プロダクトブランド	SmartPR シリーズ
プロダクト名	Smart Receico レシートキャンペーンシステム
バージョン	Ver6.4.0
データセンター	AWS 東京リージョンを利用

1.セキュリティ基本方針

	確認事項	実施有無	事業者回答
1	経営陣によって承認された情報セキュリティに関する基本方針を定めた文書があること。また、該当文書を全従業員及びクラウドサービス利用者に明示すること。	有	当社、最高情報セキュリティ責任者によって承認されたクラウドサービスに関するセキュリティの基本方針を定めております。 当方針は、全従業員には、社内規程として周知し、クラウドサービス利用者には、当社ウェブサイト（https://ww-system.com/data/security/inp_dtl/）に公開しております。
2	情報セキュリティに関する基本方針を定めた文書は、定期的またはクラウドサービス提供に関係する重大な変更が生じた場合に、レビューすること。	有	情報セキュリティ委員会を構築し、情報セキュリティ保全活動を効果的に推進するために、クラウドサービスに関するセキュリティの基本方針を定め、定めた通りに実施運用し、監査及び見直しを行う仕組みを確立しております。 また、当社、最高情報セキュリティ責任者によって承認されたクラウドサービスに関するセキュリティの基本方針は、情報セキュリティ内部監査において、経営者によって毎年及び重大な変化が発生した場合に見直しております。

2.情報セキュリティのための組織

	確認事項	実施有無	事業者回答
1．内部組織			
1	経営陣は、情報セキュリティに関する取り組みについての責任及び関与を明示し、組織内におけるセキュリティを積極的に支持・支援を行うこと。	有	情報セキュリティの整備・運用方法を明記した文書（以下、「情報セキュリティ規程」）にて、最高情報セキュリティ責任者の責任及びコミットメントを明記し、実施しております。さらに、最高情報セキュリティ責任者を含む情報セキュリティ問題を積極的に扱う組織横断の会議体を設置し、組織内のセキュリティ向上のために活動しています。
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。また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、外部に公開すること。	有	情報セキュリティ規程にて、最高情報セキュリティ責任者は、代表取締役と開発部部長がその責任・権限を担っていると定めております。また同規程にて、情報セキュリティ方針、目標の設定、承認、マネジメントレビューの実施等、全社のセキュリティ活動の推進を行うことが役割であることを明記しています。 クラウドサービスの情報セキュリティに関する窓口は、「情報セキュリティのための組織（CSIRT)」を設け、当社ウェブサイト（https://ww-system.com/data/security/inp_dtl/）に公開しております。
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。	有	情報セキュリティ規程にて、情報セキュリティ対策（日々の活動や緊急対応、役割別 PDCA）を明記しております。
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 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。	有	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、提供しております。
5	クラウドサービスのサポート窓口、苦情窓口を明確にし、外部に公開すること。	有	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おります。

			サポート提供時間は、月～金　１０：００～１２：００ 、１３：００～１７：００（祝日・年末年始は除く）となります。 詳細は当社ウェブサイトをご覧ください。 https://ww-system.com/

３.人的資源のセキュリティ

	確認事項	実施有無	事業者回答
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。また該当文書を雇用予定の従業員に対して説明し、この文書に対する明確な同意をもって雇用契約を結ぶこと。	有	最高情報セキュリティ責任者によって承認されたクラウドサービスに関するセキュリティの基本方針（https://ww-system.com/data/security/inp_dtl/）及び社内セキュリティに関する従業員が遵守すべき社内規程（情報セキュリティ規程）を定めております。 また、雇用する従業員とは、雇用契約書を締結し、その中で就業規則及び社内規程の遵守について署名、押印をもって明確に同意を確認しております。
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。	有	雇用する従業員（採用の日から３ヶ月間は試用期間）には、入社オリエンテーションの一環で、社内規程の教育を行っております。 また、社内規程の変更の都度、全従業員に通知し、周知を行っております。さらに、教育・研修を実施し、セキュリティ、コンプライアンス等に関する教育についても必要に応じて実施しております。
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。	有	セキュリティ違反を犯した従業員は、当社就業規則に規定された懲戒の対象となることが、情報セキュリティ規則に明記されております。
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、アクセス権等の返却・削除・変更の手続きについて明確にすること。	有	従業員の退職・休職時の手続は、情報セキュリティ規則に明記されております。
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。	有	情報資産管理台帳にて、情報資産名称、管理部署または責任者、機密性、完全性、可用性レベル、利用許可範囲、媒体・保存先、保存期間ごとに分類し、記載しており、当台帳は、情報セキュリティ委員会において、定期的に見直し、更新しております。
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。	有	情報資産管理台帳にて、情報資産名称、管理部署または責任者、機密性、完全性、可用性レベル、利用許可範囲、媒体・保存先、保存期間ごとに分類し、記載しており、当台帳は、情報セキュリティ委員会において、定期的に見直し、更新しております。
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(例えば、有人受付、カード制御による入口)を用いること。	有	情報資産がある領域（執務エリア）は、有人受付を用いて、一般エリアとの物理的な境界を設けております。 重要な情報資産がある領域(入室制限エリア)は、施錠を用いて物理的な境界を設けております。
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。	有	重要な情報資産がある領域は、情報セキュリティ規則に明記されており、許可された者のみがアクセスできるように施錠をしております。
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。	有	AWS の提供するホワイトペーパーをご確認ください。
4	データセンターの落雷対策を確認すること。	有	AWS の提供するホワイトペーパーをご確認ください。
5	データセンターの水害対策を確認すること。	有	AWS の提供するホワイトペーパーをご確認ください。
6	データセンターの静電気対策を確認すること。	有	AWS の提供するホワイトペーパーをご確認ください。

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。	有	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。こちらの文書については操作方法の変更や機材追加・変更が発生する毎に更新しております。
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。	有	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、7 日前までにクラウドサービス上にて連絡をしております。
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。	有	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、当社ウェブサイト（https://ww-system.com/data/terms/pdf/requirements.pdf）に公開しております。
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。	有	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、影響について確認をしております。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おります。
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。	有	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おります。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おります。
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。	有	外部診断会社による脆弱性診断を年 1 回程度を目安に実施しておりますが、システムの変更状況や運用実績、過去の診断結果を踏まえて、毎年必ず実施するものではありません。 なお、外部診断を行わない期間についても、社内によるコードレビューや脆弱性スキャンツールの活用、パッチ適用などのセキュリティ対策を継続的に行い、安全性の維持に努めております。
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、	有	モバイルコードの利用を否認しております。

	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。		
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。	有	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おります。取得したバックアップデータは不定期ですがリストア試験を行い、正常に復元できることを確認しております なお、取得しているバックアップは、予期せぬサーバー障害や災害に備えた対策を目的としており、お客様の誤操作等によるデータ紛失時の復旧機能としては提供しておりません。
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。	有	稼働状況については監視をしております。 サービスの停止を検知した場合は、当社のニュースサイトにて連絡を行います。
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。	有	機器の状況については監視をしております。 障害が発生し、サービスの停止が発生した場合は、当社のニュースサイトにて連絡を行います。
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。	有	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おります。また作業を実施する際には変更管理に則り、作業内容について責任者の承認を得て、相互確認を行いながら実施しております。
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。	有	監査ログについては、日次で該当ログのアラートについて取得をしております。また該当のログについては運用管理者及びアクセスが許可されたものがアクセスできる場所に保管しております。
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。	有	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おります。当社サービスへのアクセスログに関しては、３６５日間に保存しております。 ※監査ログ機能で提供している以外のログの提供

			サービスは行っておりません。
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。	有	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おります。
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。	有	システムのアカウントについては当社規定に則り、各個人に一意の識別子を付与しております。またシステムにアクセスする際には IP アドレス制限、Basic 認証を利用し、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に制御しております。アカウントや暗号化方針については当社規定にて定めております。
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。	有	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なっております。特権については利用者を本システムの運用管理担当者のみとしております。
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。	有	パスワードについては情報セキュリティ規程に則り、管理しております。
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。	有	本サービスを利用する際の認証方法、アクセス制限の設定について当社ウェブサイト（https://ww-system.com/data/terms/pdf/illegalaccess.pdf）にて明記しております。
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。	有	IP アドレス制限(有償)、BASIC 認証(有償)を提供しております。機能については当社ホームページ（https://ww-system.com/data/terms/pdf/illegalaccess.pdf）にて公開しております。
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	有	本サービスはマルチテナント構成となっております。登録されたデータについては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ベースおよびネットワークの分離やアクセス制限を行っております。

	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。		
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。	有	提供する本サービスにおいて、利用者 ID の登録・削除の機能を提供しております。
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。	有	提供する本サービスにおいて、特権の割り当て等の管理する機能を提供しております。
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。	有	提供する本サービスにおいて、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おります。
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。	有	提供する本サービスにおいて、提供しているセキュリティ対策及び機能については、当社ウェブサイト（https://ww-system.com/data/terms/pdf/illegalaccess.pdf）にて公開しております。
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。	有	提供する本サービスでは、使用中断時間が一定期間を経過すると再度ログイン画面が表示されるようにしております。但し、こちらはお客様の環境により時間に差異がある場合がございます。※ユーザ画面は接続時間の制限はございません。
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。	有	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おります。またアクセス制御についても文書化し、管理・実施しております。
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。	有	ネットワーク管理者の権限については、本システムの運用管理担当者のみとしております。アクセスする際には VPN 網、秘密鍵を用いた認証を利用し、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おります。アカウントや暗号化方針については当社規定にて

			定めております。
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。	有	ファイアウォールを導入しております。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おります。
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。	有	提供する本サービスにおいて、提供しているセキュリティ対策及び機能については、当社ウェブサイト（https://ww-system.com/data/terms/pdf/illegalaccess.pdf）にて公開しております。
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。	有	本サービスの契約を終了された場合、１０営業日以内に入力データ、ユーザ情報、記録・監査ログ、バックアップデータを完全に消去します。
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。	有	伝送データは、すべて暗号化しています。ディスクに保存されるデータは全て暗号化しております。データベースは、一部の情報を暗号化しております。
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。	有	本サービスにお客様が登録した情報については、その情報の内容を問わず、最善の注意を持って管理し、別段の定めがある場合を除き利用規約（３０条 守秘義務　https://ww-system.com/data/terms/pdf/terms.pdf)、相手方の書面による承諾を得ることなく、本サービス以外の目的のために利用あるいは複製し、または第三者に利用させ、もしくは開示、漏洩いたしません。 なお、当社にて外部組織を利用する場合は、当社規定に則り利用規約（１８条 再委託 https://ww-system.com/data/terms/pdf/terms.pdf）選定、契約を行います。契約時には、セキュリティ要求事項を含んだ正式な契約書を締結することになっております。

			本サービスではAWS 東京リージョンを利用しております。こちらも上記の規約に則り、正式な契約書を締結しております。
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の中で発見したまたは疑いをもったセキュリティ弱点はどのようなものでも記録し、報告するようにすること。	有	情報セキュリティ規程にて、セキュリティ事故の定義、発生時の報告について定めており、またウィルス感染の疑いや利用しているサービスから情報漏えい等の事故があった場合の報告連絡手段、対応手続を定めております。
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。	有	情報セキュリティ規程にて、情報セキュリティインシデントに対応するため、報告連絡手段、対応手続を定めております。 クラウドサービスに関する情報セキュリティインシデントに対応するため、CSIRTを設立しております。責任体制は、情報セキュリティ規程にて、最高情報セキュリティ責任者を責任者とした情報セキュリティ委員会を整備しております。インシデントの対応手順は、情報セキュリティ規程にて、運用体制と活動プロセスを明記し、さらに、システム障害、機密漏洩、被害等、人的誤りを含む情報セキュリティ上のインシデントは、適切な連絡経路を通してできるだけ速やかに報告し、組織全体にわたって管理を行うことを明記しております。
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。	有	CSIRTを設け、窓口・対応・関係者への連絡を実施しております。但し、定期的な明示はしておりません。脆弱性が発見された場合は、その都度公的機関(JPCERT)、自社Webページなどを利用してクラウド利用者に情報を明示しています。また、本サービスのメンテナンスやアップデート、インシデント情報を、「お知らせ一覧」に公開しています。
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は、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	有	事業継続計画書の中で事業継続リスク分析及びビジネスインパクト分析をおこなっております。その中で各業務プロセスの中断発生確率、復旧許容

	と。		時間から優先度を定め、要求されたレベル、時間で復旧できるように事業継続計画書・事業継続計画手順書を作成しております。
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。	有	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おります。
3	事業継続計画については定期的に試験・更新すること。	有	事業継続計画書を作成し、定期的に試験及び見直しを行なっております。また、クラウドサービスの可用性を確実にするための対策および目標復旧時間については情報を提供することが可能です。
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。	有	クラウドサービス提供に用いる機材は全てデータセンターに設置しており、停電・電力障害が発生した場合も電力が供給されるようになっております。
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。	有	クラウドサービス提供に用いる機材は全てデータセンターに設置しており、火災検知・通報システム及び消火設備を用意しております。
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、維持すること。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。	有	情報セキュリティに影響を及ぼす可能性のある変更(関連する法令、国の定める指針その他の規範と改正状況を反映した資源、組織、規定、規格の変更)は、情報セキュリティ委員会の中で、確認されることになっております。情報セキュリティ規程に作成・利用される文書・記録は、文書ごとに、管理者、承認者、保管期間を定め、適切に管理しております。
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。	有	当社ウェブサイト上に公開している利用規約（第７条 準拠法、合意管轄裁判所 https://ww-system.com/data/terms/pdf/terms.pdf ）において、準拠法および裁判管轄について定めております。
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	有	当社ウェブサイト上に公開している利用規約（２５条 知的財産権等 https://ww-system.com/data/terms/pdf/terms.pdf）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おります。
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。	有	情報セキュリティ規程にて、物理的境界及びその他の各境界へのアクセスが許可される者について定めており、アクセス許可がされていない者はアクセスできないように制限をかけております。またアクセス許可判断方針についても定めております。
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。	有	当社ウェブサイト上に公開している利用規約（https://ww-system.com/data/terms/pdf/terms.pdf）に従って取り扱っております。
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が望ましい。 また、クラウド事業者は、クラウド利用者の個別の監査要求に応える代わりに、クラウド利用者との合意に基づき、独立したレビュー及び評価の結果を提供することが望ましい。	有	外部診断会社による脆弱性診断を年１回程度を目安に実施しておりますが、システムの変更状況や運用実績、過去の診断結果を踏まえて、毎年必ず実施するものではありません。 なお、外部診断を行わない期間についても、社内によるコードレビューや脆弱性スキャンツールの活用、パッチ適用などのセキュリティ対策を継続的に行い、安全性の維持に努めております。 https://ww-system.com/data/quality/inp_dtl/
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。	有	情報セキュリティ規程にて、記録媒体の情報取扱方法（保管、廃棄）を定め、適切に取り扱っております。
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)。	有	情報セキュリティ規程にて、クリアデスク（重要な情報資産は、作業終了時には、施錠されたキャビネット、引出しに保管）と離席する場合は、第三者が容易に操作及び閲覧ができないようスクリーンロック等の対策を講じるよう定め、実施しております。
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	有	情報セキュリティ規程にて、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

	集し、適切にパッチの適用を行うこと。		め、遵守しております。 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おります。
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。	有	サービス提供の終了およびサービス廃止の場合、９０日前までに通知致します。詳細は利用規約（１７条 サービスの廃止 https://ww-system.com/data/terms/pdf/terms.pdf）にて定めております。
5	サービス提供にあたって役割分担および責任範囲を明示していること。	有	サービスの責任分界点については、(https://ww-system.com/data/terms/pdf/boundary.pdf)にて公開しております。

公開日時：
２０２３年5月1日 １２:００

更新日時：
２０２５年5月１５日 １２:００