情報セキュリティ基準

本情報セキュリティ基準では、情報（以下に定義）の機密性、完全な整合性及び可用性に関する、社外の第三者／取引業者を対象としたイーライリリー・アンド・カンパニー（「リリー」）の情報セキュリティ要件を定める。リリーとの何らかの合意の下、情報セキュリティに関連して社外の第三者／取引業者に課される追加義務は、本情報セキュリティ基準の要件に追加される。

本基準において、「情報」には業務目的でリリーが使用する秘密情報及び個人情報（以下、個別に、及び／または総称して「情報」と称する）が含まれる。個人情報とは、リリーの取引業者のプライバシーとセキュリティに関する基準で定義されたあらゆる情報を指す。秘密情報とは、社外の第三者／取引業者とリリーの間で交わされる書面による合意で定義（または同様に指定）された秘密または専有情報を指す。

なお、本情報セキュリティ基準は、社外の第三者／サプライヤーによって以下のように取り扱われるすべての情報に適用される：（i）作成、（ii）編集、（iii）管理、（iv）処理、（v）アクセス、（vi）受領、（vii）転送、（viii）破棄、（ix）保存または（x）ホスティング，また、あらゆる形式のものが対象であり、次に挙げるものに限定されない：（a）システム、（b）クラウド環境、（c）本番および非本番環境、（d）電子資産およびデバイス［会社提供および個人所有（bring your own device：BYOD）を含む］および（e）ハードコピー

1. **情報セキュリティ方針及び手順：**

社外の第三者／取引業者は、文書化された情報セキュリティに関する方針、基準及び手順を整備ならびに遵守し、情報の機密性、完全な整合性及び可用性の保護に関連する統制環境を整備すること。方針及び手順については、見直し、更新及び上級管理職による承認を年1回実施する。

社外の第三者／取引業者が、私物デバイスを使った情報またはシステムへのアクセスを許可している場合は、BYOD 方針を策定し、それに沿って運用する。

2. **ガバナンス及び研修：**

社外の第三者／取引業者の従業員は、情報の保護及び安全な取り扱いに関する要件を含む、関連する情報セキュリティ研修を修了すること。要請に応じて、修了した研修の概要を提供できるようにする。

社外の第三者／取引業者は、すべての情報セキュリティ関連項目の連絡窓口担当者を指名する。さらに、社外の第三者／取引業者は、本情報セキュリティ基準の遵守を監督する担当者を配置する。

3. **人材面でのセキュリティ対策：**

雇用に先立ち、犯罪歴調査、履歴書または経歴の審査、資格及び経験の審査、ならびに面接を含む雇用前スクリーニングを実施する。

すべての従業員と、秘密保持契約、守秘義務契約またはこれらに相当する契約を交わすこと。契約には以下が含まれるがこれらに制限されない。

a. 雇用／業務終了後の秘密保持義務
b. 許容される電子リソースの使用法を規定する条項（専門的、合法的及び倫理的な電子リソースの使用を含むがこれらに制限されない）

退職者またはアクセスが不要となった個人から資産（物理的及び電子的）を特定ならびに回収するプロセスが整っていること。

Version 1.2
December 1, 2017

情報セキュリティ基準

4. **情報へのアクセス:**

リリーに帰属する、またはリリーに委託された情報を社外の第三者／取引業者がリリー環境外で保有する場合、及び／または社外の第三者／取引業者がリリー環境へのリモートアクセスを行う場合、社外の第三者／取引業者は最低限以下のアカウントアクティブ化管理策を講じること。

a. 職務を遂行するための業務上のニーズに基づきアクセス権を付与する正式な承認プロセス（最小権限、すなわち必要最低限のアクセスレベル）
b. アクセス権の依頼、承認及び付与の分離
c. システム、サービス及びアプリケーションにアクセスするためのユーザーアカウントは共有せず、ユーザーに個別に付与する。
d. 特権及び管理ユーザーアカウントは、標準ユーザーアカウントとは異なり、固有のユーザーログイン ID を有すること。特権ユーザーアカウント（コンピュータシステム内で権限を付与する、一般ユーザーが利用可能な権限より大幅に高いレベルのアクセス権）は、認定ユーザーにのみ限定的に割り当てる。

以下の要件を含むパスワード制御を適切に実施すること。

a. 履歴及び期限
b. 仮パスワードを安全に通知し、初回使用後の変更を指示する。
c. アカウントで障害が発生したと考えるに足る理由がある場合は即時パスワードを変更する。
d. 共有システム、サービス及びアプリケーションアカウントについては、パスワードを知っている人物の社外の第三者／取引業者退職時、あるいはアクセスを要しない職位への異動時にパスワードを変更する。
e. パスワードをリセットする前にユーザーの身元を確認する。
f. すべてのデフォルトパスワードはデフォルト値から変更する。
g. パスワードの強度は一般的なセキュリティ基準（ISO、NIST など）の長さ及び複雑さに準ずる。

以下の非アクティブ化管理策を講じること。

a. 退職者及び／または業務においてアクセス権が不要となった人物のアカウントを適時に非アクティブ化する正式なプロセス（例：24 時間以内）
b. 社外の第三者／取引業者の人事異動の対象者がアカウントを有する、またはリリーの情報システムへのアクセス権を有する場合、24 時間以内に人事異動をリリーに通知するプロセス

以下のアクセス管理策を実施すること。

a. すべてのユーザー、システムアカウント、テストアカウント、一般アカウントを対象に、年 1 回以上の定期的なアクセスレビューを実施及び記録する。
b. 所定回数以上ログインに失敗した場合、ユーザーアカウントをロックする。
c. しばらく使用されていないアカウント（例：過去 90 日間、四半期に 1 回、年 2 回及び年 1 回の処理に使用されるアカウントを除く）を無効化する。
d. アカウントロックアウトやセッションタイムアウトなどのセッション管理策講じる。
e. インターネットに接続されたアプリケーションについては 2 段階認証を実施する。
f. リモートアクセス［例：バーチャル・プライベート・ネットワーク（VPN）、リモート・デスクトップ・プロトコル（RDP）については 2 段階認証を実施する。

5. **ネットワーク及びシステムセキュリティ:**

リリーに帰属する、またはリリーに委託された情報を社外の第三者／取引業者がリリー環境外で保有する場合、及び／または社外の第三者／取引業者がリリー環境へのリモートアクセスを行う場合、社外の第三者／取引業者は最低でも以下のネットワーク及びシステムセキュリティ管理策を講じること。

a. オペレーティングシステム、アプリケーション及びネットワークデバイスの基準を強化する。

b. セキュリティ関連の修正モジュールのリリース及び一般的なセキュリティ基準（ISO、NIST など）に準じた評価後、すべてのシステムについてオペレーティングシステムへの修正モジュール適用及び主要コンポーネントの更新を実施する。
    - インターネットに接続されたアプリケーションの高リスク脆弱性については、7 日以内に修正モジュールを適用する。
c. システムのメンテナンスを行い、最新のセキュリティ修正モジュール／サービスパックが適用されるようにする。

ネットワークセキュリティ管理策：

a. リリーに帰属する、またはリリーに委託された情報を非武装地帯（DMZ）に保存しない。
b. ニーズに基づきインバウンド及びアウトバウンドトラフィックを制限するすべてのネットワークインタフェースでファイアウォールポリシーを実施する。
c. 侵入検出または侵入防止システムを実装し、不正または悪意のあるネットワークトラフィックを検出及び対処する。
d. 社外の第三者／取引業者は本基準の第 5 項に準じて、ネットワークデバイスのセキュリティ設定を更新する。
e. リリーと社外の第三者／取引業者の間でシステムまたはアプリケーションの可用性についてサービス品質保証契約（service level agreement：SLA）が交わされている場合、DDoS（Distributed Denial of Access）攻撃に対する保護を配備する。

システムセキュリティ管理策：

a. エンドポイントデバイスは暗号化され、パスワードで保護されていること。
b. モバイルエンドポイント（スマートフォン、タブレット）はモバイルデバイス管理システムを使って安全を確保する。
c. サーバー及びエンドポイントは、最新状態に保たれたウイルス／マルウェア保護対策を使って安全を確保する。

6. **ロギング及びモニタリング**：

一般的なセキュリティ基準（ISO、NIST など）に準じてロギング活動を記録及び実施すること。異常な活動をモニターすることを推奨する。

7. **脅威及び脆弱性の管理**：

社外の第三者／取引業者は、アプリケーション、オペレーティングシステム及び他のインフラコンポーネントについて継続的な脆弱性評価及び適時の修正プロセスを整備する。さらに、ウイルス、ボット及び他の悪質なコードを含む新規及び既存のセキュリティ脆弱性ならびに脅威を特定、評価、軽減し、これらから保護できるようサービス及びプロセスをデザインする。

社外の第三者／取引業者は以下の管理策を整備すること。

a. 情報を扱うネットワーク及びアプリケーションを対象に独自のペネトレーションテストを年 1 回実施する。
b. 情報を扱うプラットフォーム及びネットワークの脆弱性スキャンを四半期に 1 度実施し、一般的なセキュリティ基準、とりわけシステムハードニングに関する基準との整合性を確保する。
c. ペネトレーションテスト、脆弱性スキャン及びコンプライアンスアセスメントで特定された問題を解決するためのリスクベースの修正プログラム
d. 社外の第三者／取引業者はリリーのネットワークペネトレーションテスト依頼に随時対応する。

情報セキュリティ基準

8. **変更管理**:

社外の第三者／取引業者は以下を含む文書化された変更管理方針を実施する。

a. 承認、分類、テスト及びバックアウトプランテストの要件
b. 依頼、承認及び実施における職務の分掌
c. 所定の時間内（例：24 時間）での緊急な変更の管理及び審査

9. **資産の管理**:

リリーに帰属する、またはリリーに委託された情報を社外の第三者／取引業者がリリー環境外で保有する場合、及び／または社外の第三者／取引業者がリリー環境へのリモートアクセスを行う場合、社外の第三者／取引業者はシステム／デバイス及びソフトウェア資産を含む資産リストを維持すること。

社外の第三者／取引業者は、情報（ハードコピー及び電子版）が不要になった場合に一般的なセキュリティ基準（ISO、NIST など）に準じた破棄を確保すべく、資産処分管理策を整備し、適切な破棄を証明する文書を維持する。

10. **情報の取り扱い**:

リリーに帰属する、またはリリーに委託された情報を社外の第三者／取引業者がリリー環境外で保有する場合、及び／または社外の第三者／取引業者がリリー環境へのリモートアクセスを行う場合、社外の第三者／取引業者は情報と他の顧客情報との分離を確保すること。さらに、社外の第三者／取引業者は、自社環境における情報の流れに関する説明書を提出できること。

リリーと社外の第三者／取引業者間の通信（e メール、ファイル転送、リモート接続など）は、リリーが提供するサービスを使って行うこと。

情報紛失の防止、検知及び対応にはプロセス及びツールを使用する。

リリーのビジネスオーナーの書面による承認（リリーのリムーバブルストレージ依頼プロセスにより取得）を得ることなく、リムーバブルストレージデバイスを使って情報を保存または転送してはならない。かかるデバイスを使用する際は、デバイスに保存されたすべての情報を暗号化すること。

11. **暗号化**:

リリーに帰属する、またはリリーに委託された情報を社外の第三者／取引業者がリリー環境外で保有する場合、及び／または社外の第三者／取引業者がリリー環境へのリモートアクセスを行う場合、情報の送信時には暗号化を行う。

社外の第三者／取引業者が保有または管理する暗号化キーは、アクセス管理された安全な場所に保管すると共に、実証されたキー復元機能を備えていること。

暗号化の手順と実行は、一般的なセキュリティ基準（ISO、NIST など）に準ずること。

12. **物理的セキュリティ**:

リリーに帰属する、またはリリーに委託された情報を社外の第三者／取引業者がリリー環境外で保有する場合、及び／または社外の第三者／取引業者がリリー環境へのリモートアクセスを行う場合、ハードコピー及び情報システム（例：ハードウェア、ソフトウェア、文書、データ）を保護するためのプロセス及び物理的管理策を策定、実施する。

データセンターの物理的制御を行い、業務上のニーズに基づきアクセス権を正式に管理する。混乱または喪失を防止するため、データセンターの環境管理策（温度、湿度、バックアップ電源）を整備する。

情報セキュリティ基準

情報の送信、保存または処理を行う社外の第三者／取引業者については、年 1 回の独自物理的セキュリティ評価の実施が義務づけられる。

13. **レジリエンス／事業継続性／情報のバックアップと復元**:

災害または中断発生時の、契約上のビジネス要件及び情報の重要度に則した事業継続性及び障害復旧に関する契約の要求事項に加えて、社外の第三者／取引業者は以下の管理策を整備する。

主要なデータ処理施設に冗長電源及び冗長処理能力を配備する。

契約に規定された期間内にリリーの機能を回復させるべく、代替の処理サイトを確保する（該当する場合）。

レジリエンステストを年 1 回実施し、効果的な復元能力を備えていることを実証する。

重要度に基づき、対象となるシステム及びデータの定期的なバックアップを行う。バックアップのテストを定期的に実施し、実用可能性を確認する。

バックアップテープ及び／または送信の適切な安全を証明する。

14. **記録の保存及び破棄**:

社外の第三者／取引業者は、該当する契約で指定された期間のみ情報を保存する。ただし、関係法令によってより長い保存期間が義務づけられている場合はこの限りではない。

契約終了時、社外の第三者／取引業者はリリーの指示に従って情報を返却、削除または破棄する。

リリーの要請に応じて、社外の第三者／取引業者は指示に従って情報が破棄されたことを証明すること。

15. **情報セキュリティインシデントへの対応、管理及び報告**:

リリーに帰属する、またはリリーに委託された情報を社外の第三者／取引業者がリリー環境外で保有する場合、及び／または社外の第三者／取引業者がリリー環境へのリモートアクセスを行う場合、社外の第三者／取引業者は、セキュリティインシデント（例：露出、侵害、盗用）の管理及び対応手順を備え、情報の機密性、完全な整合性及び／または可用性への脅威を伴う事象を合理的に検知、調査、対応、緩和及び通知できること。インシデントへの対応及び管理手順を文書化、検証し、年 1 回以上見直しを行う。リリーは要請に応じてかかる手順書を審査できる。

情報に影響を及ぼす可能性のあるセキュリティインシデントが疑われるまたは認知された場合、社外の第三者／取引業者は 24 時間以内にリリーに同インシデントを通知する。社外の第三者／取引業者は、リリー及び社外の第三者／取引業者の連絡先を規定する、文書化されたプロセスを整備し、リリーと社外の第三者／取引業者の間で交わされた契約に準じて当該通知要件を遵守する。

セキュリティインシデントが実際に発生または疑われる場合、社外の第三者／取引業者はリリーに全面的に協力し、状況、根本的原因の把握、及び必要な対策の決定にあたる。

16. **下請業者の管理**:

本情報セキュリティ基準は、リリーに帰属する、またはリリーに委託された情報をリリー環境外で取り扱う、及び／またはリリー環境へのリモートアクセスを行う社外の第三者／取引業者が使用するすべての下請業者に適用される。社外の第三者／取引業者は、情報セキュリティ基準を各下請業者に伝達し、遵守を図る責任を有する。なお、下請業者

にはリプログラフィックスや遠隔地保管の社外の第三者業者／取引業者、ソフトウェア開発業者、クラウドホスティング業者、データセンター業者が含まれるがこれらに限定されない。

社外の第三者／取引業者は下請業者との間で、情報の機密性、可用性及び完全な整合性を維持するための管理策を含む実施すべき管理策の概要を規定する契約書を締結すること。

社外の第三者／取引業者は、初期及び継続的評価を実施し、下請業者による情報セキュリティ基準の遵守、ならびにセキュリティインシデント及び問題の適切な管理を確保すること。

社外の第三者／取引業者は、情報を取り扱う、あるいは情報が存在する社外の第三者／取引業者またはリリーのシステム、及び情報へのアクセスを行うことになる下請業者を使用する前に、リリーに当該下請業者ならびに情報が扱われる国を通知し、文書による承認を得ること。

17. **情報セキュリティ審査権：**

社外の第三者／取引業者は、リリーとその代理人、監査人（社内外）、規制当局及び他の代表者による、情報の完全な整合性確認及び本情報セキュリティ基準の遵守状況の監視を目的とした社外の第三者／取引業者（及び社外の第三者／取引業者が使用する下請業者）の施設、帳簿、システム、記録、アクセス登録簿、データ、慣行及び手順書の調査、監査、検査及び審査の実施を許可する。

18. **システム開発ライフサイクル**

以下の要件は、社外の第三者／取引業者がリリーのために構築するシステム、ソフトウェアまたはアプリケーションにのみ適用される。

ソフトウェア開発の技術手法：

a. 方針、手順及び基準を伝達し、遵守を図り、業界基準に合わせて所定のシステム開発手法を正式に実施する。プログラミング基準を策定し、関係者に伝達する。基準には、アーキテクチャ及び設計仕様、ビジネスロジックのレビュー、安全なアルゴリズム及びライブラリの選択、テストコードの除去、及び一般的な安全面での欠陥（例：OWASP 脆弱性上位 10 種類）の修正が含まれる。
b. コードレビューを実施し、前述のプログラミング基準の遵守を確認する。
c. 非本番環境における本番データの使用は必要時のみとし、使用時は本番環境と同じセキュリティ管理策を講じるか、あるいはテストで使用する本番情報は十分に難読化すること。
d. パブリックドメインソフトウェア（例：オープンソースソフトウェア、シェアウェア、フリーウェア）を使用する場合は、潜在的な法的リスク（例：著作権の侵害）を含む潜在的リスクについて適切に精査すること。
e. パブリックドメインソフトウェア（例：オープンソースソフトウェア、シェアウェア、フリーウェア）を使用する場合は管理策を講じ、この種のソフトウェアの導入により悪影響（例：ウイルス、トロイの木馬、「バックドア」などのセキュリティ侵害）が生じないようにする。
f. ソースコードは、業界で認められたバージョン管理ツールで維持管理し、ソースコードのチェックアウトについて厳格な管理策を講じる。社外の第三者／取引業者は環境コードの変更を監視する監視システムを配備すること。
g. すべての社内開発及び購入したソフトウェアについてセキュリティライフサイクルを管理する。

コードリリース：

a. 社外の第三者／取引業者は、選択した開発モデルの継続的改善に取り組む。
b. 社外の第三者／取引業者は、予定されたソフトウェアアップグレードについて、リリースが適切に計画、管理、テスト、承認及び通知されることを証明する正式な変更／リリース管理方針／手順書を有すること。
c. 変更／リリース管理サイクルは要件の定義から始まる。予定しているリリースの要件にリリーへの影響、フィードバック及びニーズを適切に含める。

d. 各リリースサイクル中に回帰テストを実施する。テストはさまざまなレベル（例：ユニット、統合及びシステム、ユーザー）で実施する。ユーザーテストは、正式なテスト計画に基づき、システムの設計及び開発に携わっていない独立当事者が実施する。
e. 開発ライフサイクルの各段階（要件、設計、テスト、ユーザー受け入れ、稼働開始）で正式な承認を取得する。承認取得時は、承認者、承認日及び承認対象が明確であること。
f. リリース及び修正モジュールは、配備及び／または使用に関する十分な指示と共に提供する。これには、リリーが自社で適用するリリースまたは修正モジュールの提供を受ける場合と、社外の第三者／取引業者がリリー環境で適用した変更についてリリーが通知を受ける場合がある。
g. システム設計を正式に作成し、要件のコードへの翻訳を支援する。

臨時変更／バグ修正

a. 緊急／バグ修正変更の正式な手順が整備されており、これらの変更が適時かつ管理された方法で行われること。
b. 既知のバグまたは欠陥をリリーに通知する正式なプロセスが整備されていること。
c. バグ修正変更の正式なテストを実施すると共に、適切な記録と承認を行う。承認は、変更実施者ではない者が行うこと。