セキュリティ対策

提供者：	**ADP - グローバルセキュリティ組織**
バージョン：	**2.0**
リリース日：	**2019 年 9 月**

目次

用語と定義

以下の用語が本文書全体にわたって使用される可能性があります。

使用されている用語または略語	定義
GETS	グローバルエンタープライズテクノロジー＆ソリューション
GSO	グローバルセキュリティ組織
CAB	変更諮問委員会
DRP	災害復旧計画
CIRC	GSO の重大インシデント対応センター
SIEM	セキュリティ情報イベント管理
IDS	侵入検知システム
DNS	ドメインネームシステム
NTP	ネットワークタイムプロトコル
SOC	サービス組織コントロール
TPSI	トラステッドプラットフォームセキュリティインフラストラクチャ

概要

ADP は、クライアント情報のセキュリティ、機密性、完全性を保護するために、管理的、技術的、物理的な安全対策で構成されている、正式な情報セキュリティプログラムを維持しています。このプログラムは、（i）クライアント情報のセキュリティと機密性を保護し、（ii）情報のセキュリティまたは完全性に対する予測される脅威や危険から保護し、（iii）情報への不正アクセスまたは情報の不正使用から保護するために、合理的に設計されています。

この文書に記載されている内容は、リリース日の時点のADPにおける情報セキュリティ対策と実践の概要であり、ADPによって変更される可能性があります。これらの要件と実践は、ISO/IEC 27001:2013情報セキュリティ規格と一貫性を持つように設計されています。ADPは定期的に自社のセキュリティポリシーと標準の評価を行っています。当社の目標は、セキュリティプログラムが効果的かつ効率的に機能し、当社のクライアントとその従業員によって当社に託されたすべての情報を保護できるようにすることです。

第1節 - 情報セキュリティポリシー

情報セキュリティ職務の独立性

ADPの最高セキュリティ責任者は、ADPのグローバルセキュリティ組織（GSO）を監督し、その報告を最高情報責任者に対してではなく、相談役（GC）に対して行います。このようにすることで、ITからの必要な独立性をGSOに提供できます。GSOは、サイバーおよび情報セキュリティとコンプライアンス、業務リスク管理、クライアントセキュリティ管理、従業員の保護、ビジネスレジリエンシーにおいて多面的なアプローチを持つ、部門横断型の総合セキュリティチームです。GSOの上級管理職者は、当社の最高セキュリティ責任者の配下で、セキュリティポリシー、手順、およびガイドラインの管理に責任を負います。

情報セキュリティポリシーの正式な定義

ADPは、情報セキュリティの管理に対するADPのアプローチについて定めた、正式な情報セキュリティポリシーを策定して文書化しました。このポリシーで対象としている具体的な分野には以下が含まれますが、これらに限定されません。

- **セキュリティ管理ポリシー –** セキュリティの観点からの雇用プロセスに関する情報セキュリティの責任と管理など、グローバルセキュリティ組織（GSO）および最高セキュリティ責任者（CSO）の責任について概説しています。
- **グローバルプライバシーポリシー –** 個人情報の収集、情報へのアクセス、正確性、開示、およびクライアントに対するプライバシーステートメントについて説明しています。
- **従業員の電子通信の許容される用途とデータ保護に関するポリシー** – 許容される用途、さまざまな電子通信、暗号化、および鍵管理について説明しています。
- **情報の取り扱いに関するポリシー –** ADP の情報の分類に関する要件を提供し、保護管理を確立しています。
- **物理的セキュリティポリシー –** ADP の各施設のセキュリティ要件と、それらの施設で業務を行う当社の従業員や訪問者のセキュリティ要件を定義しています。
- **セキュリティ業務管理ポリシー –** システムパッチの保守に必要な最小限の管理を提供し、マルウェアからの脅威に効果的に対処し、バックアップおよびデータベースのセキュリティ管理を維持しています。
- **セキュリティ監視ポリシー –** 侵入検知システム（IDS）、ログ、およびデータ損失防止（DLP）のための管理を提供しています。
- **調査およびインシデント管理ポリシー –** インシデント対応、電子情報開示、従業員の保護、従業員の電子的に保存された情報へのアクセスに関する基準を定義しています。
- **アクセスと認証に関するポリシー –** 認証（ユーザーID とパスワードなど）、リモートアクセス、ワイヤレスアクセスの要件について概説しています。
- **ネットワークセキュリティポリシー –** ルーター、ファイアウォール、AD、DNS、メールサーバー、DMZ、クラウドサービス、ネットワークデバイス、ウェブプロキシ、スイッチドネットワークテクノロジーのセキュリティアーキテクチャ。
- **グローバルサードパーティリスクおよび M&A ポリシー –** ADP の事業目標の達成を支援するために第三者を参加させることに対する最低限のセキュリティ対策を定義しています。
- **アプリケーション管理ポリシー –** システム開発ライフサイクルの各ステージに適切なセキュリティ管理機能を確立します。
- **ビジネスレジリエンシーポリシー –** ビジネスレジリエンシープログラムの文書化、実践、維持、継続的な向上のための最小限の要件を定めることによって、ADP の保護、完全性、保全を管理しています。

- **総合セキュリティリスク管理ポリシー –** 特定、監視、対応、分析、ガバナンス、新しいビジネスイニシアティブ。

各ポリシーはADPのイントラネットで公開されており、すべての従業員と契約業者がADPのネットワーク内からアクセスできます。

情報セキュリティポリシーの見直し

ADPは、少なくとも1年に1回、またはADPの情報システムの機能に影響を及ぼす大きな変更があった場合に、情報セキュリティポリシーを見直しています。

第2節 - 情報セキュリティの組織構成

情報セキュリティに関する役割と責任

GSOは、サイバーおよび情報セキュリティ標準、業務リスク管理、クライアントセキュリティ管理、従業員の保護、ビジネスレジリエンシーに対するコンプライアンスのために多面的なアプローチを活用している部門横断型のセキュリティチームで構成されています。GSOのすべてのメンバーに対して、役割と責任が正式に定義されています。GSOは、会社の方針に基づいた情報セキュリティプログラムの設計、実践、監督を担当しています。GSOの活動は、ADPの最高セキュリティ責任者、最高経営責任者、最高財務責任者、最高戦略責任者、最高人事責任者、相談役をメンバーとする、執行セキュリティ委員会によって監督されています。

モバイルコンピューティングとテレワークに関するポリシー

ADPでは、コンピューターやデバイスの盗難または紛失から生じる可能性があるデータの流出を防止するため、すべての機密情報をモバイルデバイス上で暗号化することを求めています。会社のネットワークにリモートでアクセスするには、高度なエンドポイント保護とVPNを介した二要素認証も必要です。すべてのリモートデバイスは、パスワードで保護されている必要があります。ADPの従業員は、リモートコンピューティングデバイスの紛失または盗難について、セキュリティインシデント報告プロセスを通じて速やかに報告する必要があります。

ADPとの雇用条件として、すべての従業員と契約業者は、電子通信の許容される用途とデータ保護に関するポリシーおよびその他の関連ポリシーに従わなければなりません。

第3節 - 人事に関するセキュリティ

身元審査

当人の管轄区域の適用される法律要件に従って、ADPはその従業員、契約業者およびサードパーティーの職務と責任に基づいた適切な身元審査を実施します。これらの審査では、候補者を雇用するまたは参加させる前に、クライアントの情報を扱うことに対するその候補者の適合性を確認します。

身元審査には、以下のような要素が含まれる場合があります。

- 身元/雇用資格の確認
- 雇用履歴
- 学歴と専門資格
- 犯罪歴（法的に許可されている場合および現地の国の規制に応じて）

従業員および契約業者との機密保持契約

ADPの雇用契約および契約業者との契約には、従業員や契約業者がアクセスするクライアント情報に関連する義務と責任について述べている条項が含まれています。ADPのすべての従業員および契約業者は機密保持の義務に拘束されています。

情報セキュリティトレーニングプログラム

すべての従業員は、新人研修計画の一環として情報セキュリティトレーニングを修了する必要があります。さらに、ADPは、従業員が通常業務の遂行時に各自の責任を再認識できるように、年次のセキュリティトレーニングを提供しています。

従業員の責任と懲戒手順

ADPは、ADPのすべての従業員が遵守しなければならないセキュリティポリシーを公開しています。セキュリティポリシーに対する違反は、アクセス権の取り消しおよび/またはコンサルティング契約や雇用の解除を含む懲戒処分につながる場合があります。

雇用契約の解除の責任

雇用契約の解除の責任は正式に文書化されており、少なくとも以下の処分が含まれます。

- 各従業員が所有するすべての ADP の情報と資産を、保存されている媒体を問わず返却
- ADP の施設、情報、システムへのアクセス権の解除
- 残りの有効な共有アカウントのパスワードを変更（該当する場合）
- 知識の移転（該当する場合）

第 4 節 - 資産管理

資産の許容される用途

資産の許容される用途は、ADPおよびクライアントの情報が当該資産の使用によって流出しないようにするため、複数のポリシーで説明されており、ADPの従業員と契約業者に適用されます。これらのポリシーで説明されている分野の例は次のとおりです：電子通信の使用、電子機器の使用、情報資産の使用。

情報の分類

ADPによって、またはADPに代わって取得、作成、維持される情報は、該当する場合、次のセキュリティ分類が割り当てられます。

- 公開 - 例：マーケティング用パンフレット、発行済みの年間レポート
- ADP 社外秘 - 例：社内コミュニケーション、業務手順
- ADP 機密 - 例：個人情報および要配慮個人情報
- ADP 制限付き - 例：財務予測、戦略的計画情報

情報の取り扱いの要件は､情報セキュリティ分類と直接関連しています｡個人情報および要配慮個人情報は、常にADP機密と見なされます。すべてのクライアント情報は、機密として分類されます。

ADPの従業員は、情報資産をそのセキュリティ分類レベルに従って保護および取り扱う責任があります。これにより、分類レベルごとの情報の保護と適用される取り扱いの要件が提供されます。ADPにおける機密性の分類は、第三者によって保存、転送、または取り扱われるすべての情報に適用されます。

機器とメディアの廃棄

ADPの機器、文書、ファイル、メディアを廃棄または再利用する際には、それらに元々保存されていたクライアントの情報がその後に取得されることを防ぐために、適切な措置が講じられています。コンピューターまたは電子ストレージメディア上のすべての情報は、分類に関係なく、メディアが物理的に破壊されない限り、ADPの施設外に公開または再利用される前に、安全に廃棄されます。機器、文書、ファイル、メディアに保持されているADPの情報の安全な破壊/消去の手順が正式に文書化されています。

輸送中の物理メディア

クライアントの情報が含まれている印刷資料を盗難、紛失、および/または不正なアクセス/変更から保護するために、（i）輸送中（封印した封筒、コンテナ、および認可されたユーザーへの手渡しなど）、および（ii）レビュー、改訂、またはその他の処理中（安全な保管場所から持ち出された場合）に、組織的な安全対策が実践されています。

第5節 - アクセス制御

アクセス制御のビジネス要件

ADPのアクセス制御ポリシーは、業務で定義された要件に基づいています。ポリシーと制御の基準は、提供されるサービスのすべてのコンポーネントで適用されるアクセス制御に明確化されており、「最小権限」と「need to know」の原則に基づいています。

インフラストラクチャへのアクセス - アクセス制御の管理

移動、追加、作成、削除のアクセス要求は、ログに記録され、承認され、定期的にレビューされます。

関連する業務上の役割に個々のユーザーが正しく対応しており、職務変更後にアクセスを継続していないことを確認するため、正式なレビューが少なくとも1年に1回行われます。このプロセスは監査の対象であり、SOC1[1]タイプ2レポートで文書化されます。ID管理システム内から、ADPの専任チームがADPの施設や情報システムへのアクセス権を付与、拒否、キャンセル、解除、廃止/無効化します。ADPは、専任のGETSチームによって一元管理される集中型のIDおよびアクセス管理（IAM）ツールを使用しています。集中型のIAMツールを通じて要求されたアクセス権に従って、ユーザーのスーパーバイザーが関与可能な検証ワークフローがトリガーされます。アクセス権は一時的に提供されるものであり、そのアクセスが永続的のままになることを防止するためのワークフローが存在します。施設への従業員のアクセス権は、アクセスカード（従業員バッジ）を無効にすることによって雇用最終日の直後に廃止されます。従業員のユーザーIDは直ちに無効化されます。すべての従業員の資産は返却され、適切なラインマネージャーによっておよび確認され、構成管理データベースの資産リストと照合されます。職務の変更や組織の変更に伴い、ユーザープロファイルやユーザーのアクセス権は、該当する事業部門の管理者とIAMチームによって修正される必要があります。さらに、個々のユーザーの権限が関連する業務上の役割に対応していることと、異動後に無関係なアクセス権が残っていないことを検証するために、アクセス権の正式なレビューが毎年実施されます。

パスワードポリシー

ADPのアソシエイトのパスワードポリシーは、サーバー、データベース、ネットワークデバイスおよびアプリケーションにおいて、デバイスやアプリケーションが許可している範囲で適用されます。パスワードの複雑さは、保護されるデータやコンテンツのリスクベースの分析から導出されます。各ポリシーは、必要に応じた増強、二要素、または生体認証の使用を含むがそれらに限定されない、強度と複雑さに関する一般的な業界標準に適合しています。

クライアントアプリケーションの認証要件は製品ごとに異なり、フェデレーションサービス（SAML 2.0）は、GETSによって管理される統合されたネットワークとセキュリティレイヤを使用する特定のADPのアプリケーションで利用できます。

セッションタイムアウト

ADPでは、業界標準と一致しているリスクベースのアプローチに基づき、すべてのサーバー、ワークステーション、アプリケーション、VPN接続に対して自動タイムアウトを適用しています。セッションの再確立は、ユーザーが有効なパスワードを入力した後にのみ可能です。

---

[1] ADPによって提供されている特定の米国でのサービスの場合は、SOC2タイプ2レポートで監査されます。

第6節 - 暗号化

暗号化の制御

ADPでは、ADPとADPのサードパーティーとの間で交換される機密情報は、業界で受け入れられている暗号化技術と強度で暗号化されていなければならないこと（または転送チャネルが暗号化されていなければならないこと）を求めています。もしくは、専用回線を使用することができます。

鍵管理

ADPには、対称鍵と非対称鍵の管理を含む、明確に定義された鍵管理とキーエスクロー手順について記載した社内の暗号化セキュリティ標準があります。

ADPの情報に対して使用される暗号鍵は、常に機密情報として分類されます。それらの鍵へのアクセスは、例外的に承認された場合の、知っている必要があるユーザーのみに厳しく制限されています。暗号化キーおよびキーのライフサイクル管理は、業界標準の慣行に従っています。

第7節 - 物理的および環境的なセキュリティ

物理的セキュリティに対するADPのアプローチには2つの目的があります。ADPのアソシエイトのための安全な職場環境を創出することと、ADPのデータセンターやその他の戦略的なADPの拠点に保管されている個人情報を保護することです。

ADPのセキュリティポリシーでは、ADPの管理職者に、特定のレベルの物理的セキュリティを必要とする領域を明確にすることを求めています。その領域へのアクセス権は、認可された目的のための認可されたアソシエイトのみに提供されます。ADPのセキュリティ確保領域は、ビデオ監視システム、セキュリティバッジ（IDによって管理されたアクセス）の使用、出入口への警備員の配置など、さまざまな物理的セキュリティ対策が講じられています。来訪者は、認可された場合のみアクセス権が提供され、常に監視されます。

第8節 - 運用のセキュリティ

IT運用手順の定式化

GETSは、ITインフラストラクチャの運用と保守を担当するADPの部門です。GETSはIT運用のポリシーと手順を正式に管理および文書化しています。これらの手順には以下のものが含まれますが、それらに限定されません。

- 変更管理
- バックアップ管理
- システムエラーの処理
- システムの再開と復旧
- システムの監視
- ジョブのスケジューリングと監視

インフラストラクチャ変更管理

幅広いさまざまなADPのチームの代表者を含む、定期的な変更諮問委員会（CAB）がGETSによって開催されています。CABの会議では、展開の方法や本番環境への昇格の影響についてや、本番インフラストラクチャにおけるその他の変更を調整するために話し合います。

システムキャパシティプランニングと受け入れ

キャパシティの要件は継続的に監視され、定期的に見直されています。これらの見直しに伴い、システムとネットワークは適宜スケールアップまたはスケールダウンされます。キャパシティの変更やテクノロジーの進化によって大幅な変更が必要になった場合は、GETSのベンチマーキングチームが関連するアプリケーションおよび/またはシステムに対してストレステストを実施することがあります。ストレステストの結論として、チームは、（i）コンポーネント、（ii）システム構成またはバージョン、または（iii）ミドルウェア構成またはバージョンの変更を測定することによって、パフォーマンスの進化に関する詳細なレポートを提供します。

悪意のあるコードからの保護

業界標準のベストプラクティスに従ってADPの資産を保護するために、業界標準のエンドポイント保護テクノロジーが活用されています。

バックアップ管理ポリシー

ADPには、すべての本番ホスティングオペレーションで本番環境の情報をバックアップすることを求めるポリシーがあります。バックアップの範囲と頻度は、関連するADPのサービスのビジネス要件、関連する情報のセキュリティ要件、災害復旧に関する情報の重要性に従って決まります。バックアップの問題や例外を特定するため、GETSによって定期バックアップの監視が行われます。

セキュリティログの記録と監視

ADPは、一元管理型で読み取り専用のログ記録インフラストラクチャ（SIEM）と、ログ相関分析およびアラートシステム（TPSI）を導入しています。ログのアラートはCIRCによって監視され、適時に処理されます。

これらのシステムはすべて、固有のネットワークタイムプロトコル（NTP）ベースの時刻参照を使用して同期されています。

各ログには、少なくとも以下の要素が含まれています。

- タイムスタンプ
- 利用者（オペレーターまたは管理者の ID）
- 目的（イベントに関する情報）

ADPのアプリケーションの監査証跡とシステムログは、以下の情報を追跡するために設計および設定されています。

- 認可されたアクセス
- 特権操作
- 不正アクセスの試み
- システムアラートまたは障害
- システムセキュリティ設定の変更（システムでそのようなログを許可している場合）

これらのログは、ADPの認可された担当者のみが利用でき、データが安全なログ記録機器に保存される前に改ざんされることを防止するために、ライブモードで送信されます。

インフラストラクチャシステムと監視

ADPは、毎日24時間体制のインフラストラクチャ監視を提供するために、適切な手段を採用しています。障害のアラートは、その深刻度と解決するために必要なスキルに応じて、さまざまなチームによって管理されます。

ADPのホスティングセンターの施設では、関連する処理システムやネットワークコンポーネント上で常時稼働する監視アプリケーションを採用し、発生する可能性がある問題に備えてADPのスタッフに問題や警告の予防的な通知を提供しています。

技術的脆弱性管理

ホスティングインフラストラクチャに設置されるすべてのコンピューターは、専門のセキュリティ強化オペレーティングシステム（またはセキュアビルドプロセス）のインストールに準拠しなければなりません。ホスティングされるオペレーションシステムには、当社のインフラストラクチャ内で使用されるすべてのタイプのサーバーに対して、強化、承認、標準化されたビルドを採用しています。オペレーティングシステムの標準インストールは禁止されています。これらのインストールは、一般的なシステムアカウントパスワードなどの脆弱性を生み、インフラストラクチャへのリスクを引き起こす可能性があるためです。これらの構成は、脆弱性につながる可能性がある不要なサービスを実行しているホストコンピューターの露出を少なくします。

ADPには、インターネットに接続されたウェブベースのアプリケーションとそれらのアプリケーションに対応するインフラストラクチャコンポーネントのリリースおよび定期的な脆弱性評価とコンプライアンスレビューを実施するための方法論が文書化されており、少なくとも15種類の主要なテストカテゴリがあります。評価の方法論は、Open Web Application Security Project（OWASP）、SANS Institute、Web Application Security Consortium（WASC）など、社内および業界のベストプラクティスに基づいています。

第9節 - 通信のセキュリティ

ネットワークセキュリティ管理

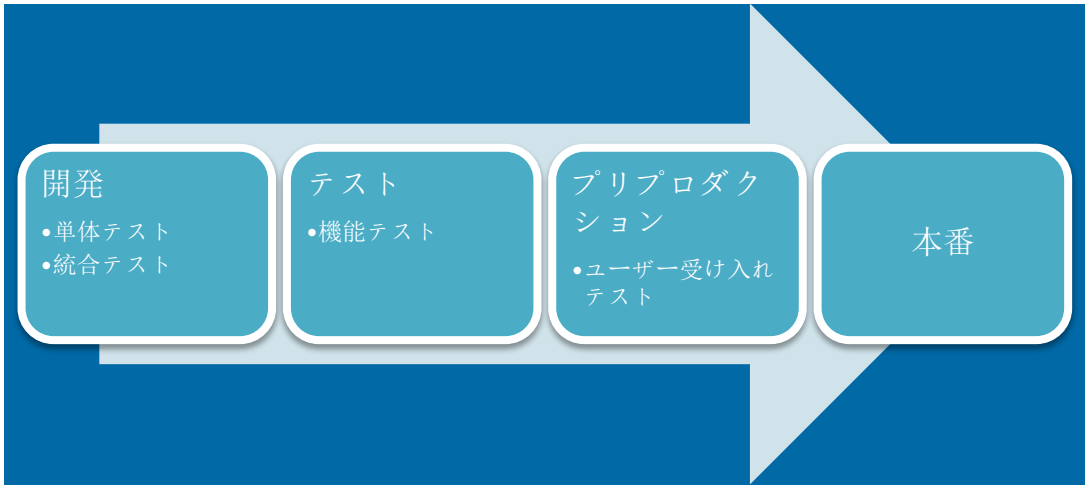
ADPは、ネットワークインフラストラクチャレベルで（毎日24時間）トラフィックを監視して疑わしい活動や潜在的な攻撃を特定するネットワークベースの侵入検知システムを使用しています。

情報の交換

ADPは、サードパーティーに送信されたADPのクライアントの情報が、認可された情報システムとリソースの間でのみ転送され、ADPの安全で認可された転送メカニズムを通じてのみ交換されるように、適切な管理を実践しています。

開発およびサポートプロセスにおけるセキュリティ

開発サイクル中には、適切な文書が生成され、テストフェーズのためのテスト計画が作成されます。異なるステージが、以下の各フェーズでの関連する承認によって環境ごとに定義されます。



- テスト環境からプリプロダクション環境に移行するには、ADP の品質チームによる承認が必要です。
- プリプロダクションから本番に移行するには、IT 運用チームによる承認が必要です。

開発チームは、安全なコーディング手法を利用することが求められています。アプリケーションの変更は、本番システムに到達する前に、開発環境とリグレッション環境でテストされます。テストが行われ、文書化されます。承認されると、変更が本番環境に展開されます。ペネトレーションテストは、重要な変更の後に実施されます。

幅広いさまざまなADPのチームの代表者を含む、定期的な変更諮問委員会（CAB）がGETSによって開催されています。CABの会議は定期的に開催され、影響についての話し合い、展開の方法に対する合意、ソフトウェアパッケージの本番環境への昇格の承認のほか、本番インフラストラクチャにおけるその他の変更についての情報交換が行われます。

ADPのIT運用チームは、ソフトウェアパッケージの本番環境への昇格前に最終承認を提供します。

開発環境におけるセキュリティ

本番環境と開発環境は分離されており、相互に独立しています。職務の正しい分離を適用するために、適切なアクセス制御が採用されています。ソフトウェアパッケージは開発プロセスの各ステージでアクセス可能であり、そのステージの関連チームのみが利用できます。

テストデータ

ADPのアプリケーション管理ポリシーに従い、クライアントからの明示的な要求と承認がない場合、開発およびテストにおいて実データやサニタイズされていないデータを使用することは許可されていません。

第11節 - サプライヤーとの関係

社外の関係者に関連するリスクの特定

サードパーティーに対するADPのセキュリティ要件への準拠を判定するため、および適用されている管理方法のギャップを特定するため、ADPおよび/またはクライアントの情報へのアクセスを必要とするサードパーティーのリスク評価が定期的に実施されます。セキュリティギャップが特定された場合、社外の関係者と新しい管理方法が合意されます。

社外の関係者との情報セキュリティに関する契約

ADPは、ADPのセキュリティ要件を満たすための適切なセキュリティコミットメントを含むすべてのサードパーティーとの契約を締結します。

第12節 - 情報セキュリティインシデント管理

情報セキュリティインシデントと改善策の管理

ADPでは、セキュリティインシデントに対して迅速に、一貫性を持って、効果的に対応するための方法論が文書化されています。

インシデントが発生した場合、ADPの所定のチームが、以下の分野に対処する正式なインシデント対応計画を発動します。

- インシデントの分類またはインシデントの深刻度に基づくエスカレーション
- インシデントの報告/エスカレーションのための連絡先リスト
- 関連するクライアントとの初期対応およびフォローアップのガイドライン
- 適用されるセキュリティ侵害通知に関する法律の遵守
- 調査ログ
- システムの復旧
- 問題の解決、報告、レビュー
- 根本原因と改善措置
- 学んだ教訓

ADPのポリシーでは、セキュリティインシデント、インシデント管理、およびセキュリティインシデントの報告に関するすべての従業員の責任を定義しています。また、ADPは、報告の要件の認識を浸透させるために、ADPの従業員や契約業者を対象とした定期的なトレーニングを実施しています。トレーニングは、必ず修了するように追跡管理されます。

第13節 - ビジネスレジリエンシー管理における情報セキュリティの側面

ADPのビジネスレジリエンシープログラム

ADPは、当社のサービスと業務を円滑に遂行し、クライアントに可能な限り最高のサービスを提供できるように努めています。当社の優先事項は、ビジネスサービスの提供を妨げる可能性があるテクノロジー、環境、プロセス、健康におけるリスクを特定すること、そしてそれらを軽減することです。ADPは、当社における軽減、準備、対応、回復の各プロセスを配置した総合的なフレームワークを作成しており、以下のような項目が含まれています。

- リスク評価
- リスク脅威分析
- ビジネス影響分析
- 計画の策定
- 事業継続計画
- 災害復旧計画
- 健康と安全に関する計画
- 現実的な対応
- 危機管理
- 緊急対応
- テストと検証
- レビュー
- 改訂
- 演習

第14節 - コンプライアンス

セキュリティポリシーと基準の遵守

ADPは、定期的に社内でコンプライアンスレビューを実施するプロセスを採用しています。さらに、ADPはSOC1[2]タイプ2監査を定期的に実施しています。これらの監査は、著名な第三者の監査法人によって実施され、該当する場合、クライアントからの要請に応じて監査報告書は毎年提供可能です。

技術的なコンプライアンス

ADPは、ベストプラクティスに従った技術的なコンプライアンスを強化するために、定期的にネットワーク脆弱性スキャンを行っています。スキャンの結果は、優先順位が付けられ、ホスティングチームとその管理職者と共同で是正措置計画として策定されます。

脆弱性スキャンは、社内および社外の両方の環境に対して定期的に行われます。さらに、ソースコードのスキャンとペネトレーションテストが製品ごとに行われます。専用のアプリケーションスキャンツールを利用して、アプリケーションレベルの脆弱性が特定された場合は、製品開発管理チームと共有され、是正措置のための品質保証プロセスに組み込まれます。結果が分析され、是正措置の計画が策定され、優先順位が付けられます。

データの保存

ADPのクライアント情報に関するデータ保存ポリシーは、適用法に準拠するように策定されています。クライアント契約の最後で、ADPはクライアントの情報に関連する契約上の義務に従っています。ADPは、クライアントの事業活動の継続に必要なすべてのクライアント情報を、クライアントに返却するか、（データのダウンロードによって）クライアントが取得できるようにします（過去に提供済みでない場合）。その後、ADPは、適用法に基づいて求められた範囲、クライアントが承諾した範囲、または紛争解決の目的に必要な範囲を除く、残りのクライアント情報を確実に破棄します。

[2] ADPによって提供されている特定の米国でのサービスの場合は、SOC2タイプ2の実施報告書も存在します。