補助金申請における情報セキュリティ白書の活用提案

はじめに

コインバンク株式会社では、人手不足や働き方改革の流れを受けて、省人化や業務効率化を実現する業務アプリケーションの開発プロジェクトを支援しています。これらのシステム構築費について、ものづくり補助金や新事業進出補助金等の制度を活用し、デジタル化投資を加速したいと考えています。補助金は革新的な事業や新規市場への進出を支援すると同時に、社会的意義やリスク管理も評価します。本ホワイトペーパーは、独立行政法人情報処理推進機構（IPA）が発行した『情報セキュリティ白書2025』の知見を活かし、省人化アプリ開発におけるセキュリティ対策の必要性と具体的な計画を示します。

1. 現状と脅威の把握

1.1 サイバー攻撃の高度化と業務アプリケーションへの影響

『情報セキュリティ白書2025』によれば、ランサムウェアや標的型攻撃、DDoS攻撃に加え、生成AIを悪用した攻撃が増加しており、サイバー攻撃の手口は年々巧妙化しています。省人化や業務効率化を目的としたアプリケーションは、組織の業務プロセスや顧客情報に深く関わるため、攻撃者の標的になりやすい領域です。 2024年にはSnowflake Inc.が提供するマルチクラウドデータウェアハウスプラットフォームを利用する複数組織で認証情報が漏えいし、165の企業が潜在的に危険に晒されたと報じられました。攻撃者は漏えいした認証情報と多要素認証が無効なアカウントを悪用してデータベースにアクセスし、通信大手や銀行、チケット販売サービスなどで数億単位の顧客データが流出した事例が確認されています。こうした事例は、業務アプリケーションの開発においてもシステム全体の認証強化とアクセス権限管理が欠かせないことを示しています。

1.2 フィッシングと内部不正の急増

生成AIの登場により、フィッシングメールが急増しています。白書では、ChatGPTのリリース以降、悪意のあるメールが4,151%増加し、82.6%のフィッシングメールがAIを活用しているとの調査結果を引用しています。さらに、テレワークとクラウド利用の拡大により、重要情報が社外のデバイスやクラウドに分散し、内部不正や情報漏えいのリスクが高まっています。IPAは、経営層による基本方針の策定や権限管理の徹底、EDR・DLP・CNAPPといった技術導入の重要性を強調しています。

1.3 AI・クラウド基盤の集中リスク

クラウドサービスはAmazon、Microsoft、Googleの3社が市場の3分の2以上を占めており、AI基盤もこの3社に集中しています。単一企業への依存は大規模な障害時に事業継続を脅かす単一障害点となり、環境負荷やプライバシー・著作権リスクも生じます。補助金申請では、こうしたリスクを正しく認識し、冗長化や法令遵守の仕組みを設計することが評価対象となります。

2. 補助金申請におけるセキュリティの重要性

ものづくり補助金や新事業進出補助金は、技術革新や新規市場への挑戦を支援すると同時に、事業の持続性や社会的意義も評価します。サイバー攻撃のリスクを軽視したシステム構築は補助金の趣旨に合致しませ

ん。『情報セキュリティ白書2025』のデータを根拠に、以下の点を強調することで評価を高め、正当なセキュリティ投資を申請します。

1. **安全・安心な社会インフラの構築** – 省人化・業務効率化アプリは、行政手続きや製造現場の管理、金融機関の業務処理など社会インフラの一部を担う存在です。不十分なセキュリティは情報漏えいと業務停止を招き、社会的信用を失う危険があります。白書が指摘するランサムウェア被害やフィッシング急増の現状を示し、システムの安全性向上が社会インフラ保全に寄与することを訴求します。
2. **被害コストと投資効果の比較** – データ侵害の平均コストが約7.3億円、金融業では約9.1億円に達する事実を提示し、適切なセキュリティ投資が莫大な損失回避につながることを示します。補助金を活用したセキュリティ対策が投資対効果の高い施策であることを強調します。
3. **セキュア・バイ・デザインへの対応** – 国はシステム設計段階からセキュリティを組み込む「セキュア・バイ・デザイン」を推進しており、補助金でもこの理念に沿った事業が評価されます。本申請では、省人化アプリケーションの設計段階から暗号化・認証・監査ログ等を実装する方針を明記し、政策と整合させます。
4. **サプライチェーンの安全性** – 開発委託先やクラウド基盤のセキュリティが脆弱な場合、自社の業務アプリに被害が波及するリスクがあります。例えばSnowflakeを利用する複数企業で認証情報が漏えいし、連鎖的にデータ流出が発生した事例は、委託先・サービスプロバイダのセキュリティ評価の重要性を示しています。関連事業者やベンダーのセキュリティを事前に評価する計画を提案します。
5. **人材育成と啓発活動** – 経営層が基本方針を策定し、従業員訓練やソーシャルエンジニアリング対策を実施することで組織全体のセキュリティリテラシーを高める計画を記載します。

3. システム構築計画と補助対象費用

3.1 セキュリティを考慮したシステム構築の概要

主要施策	内容・目的	関連白書情報
セキュア・バイ・デザイン	システム設計段階から暗号化、アクセス制御、監査ログを組み込み、セキュリティテストを実施する	政府が「セキュア・バイ・デザイン」を推進
MFAと統合ID管理	全アカウントにMFAを義務付け、アカウント棚卸しを定期的に実施する	内部不正防止のため権限管理の重要性を強調
EDR／DLP／CNAPPの導入	エンドポイントの挙動監視、データの持ち出し防止、クラウド環境の統合保護を実施する	IPAが導入を推奨
Attack Surface Management	インターネット公開資産を常時監視し、脆弱性を早期発見・修正する	ASMツール利用を推奨
量子耐性暗号の検討	NIST等が標準化を進めるポスト量子暗号への移行計画を策定し、長期的な安全性を確保する	量子コンピューター対応暗号の必要性
マルチクラウドと冗長化	単一クラウドへの依存を避け、事業継続性を高める。AI活用時にはプライバシー・著作権保護を徹底する	AI基盤の集中リスクとプライバシー問題
教育・訓練	フィッシングやソーシャルエンジニアリング演習、生成AIの悪用対策などの教育プログラムを実施する	AIを利用したフィッシングの急増

3.2 補助金対象として計上する費用例

1. **ソフトウェアライセンス費**：MFAプラットフォーム、EDR、DLP、CNAPP、ASMツールなどの導入費用。
2. **ハードウェア・インフラ費**：マルチクラウド構成の設定費用、オンプレミスサーバーの新規構築や冗長化、量子耐性暗号対応機器等。
3. **システム設計・開発費**：セキュア・バイ・デザインに基づくアーキテクチャ設計、ソフトウェア開発およびセキュリティテストにかかる人件費。
4. **教育・研修費**：従業員へのフィッシング訓練、生成AIの悪用対策研修、情報セキュリティ資格取得支援費用。
5. **外部コンサルティング費**：セキュリティ専門家によるシステム監査やサプライチェーン評価、ペネトレーションテストの費用。
6. **環境・エネルギー対策費**：省電力化や再生可能エネルギー利用を目的としたデータセンター構成の見直し費用。

4. 評価ポイントへの対応

ものづくり補助金や新事業進出補助金では、革新性、事業化の可能性、社会的意義、リスク管理等が評価されます。本計画では以下の点を明確にすることで、申請の加点を狙います。

- **革新性・新規性**：省人化や業務効率化アプリケーションに量子耐性暗号の導入を検討するなど先進的技術を採用し、生成AIの悪用を踏まえた独自のフィッシング対策システムを実装します。
- **事業化の可能性**：セキュリティ対策により利用者からの信頼を獲得し、新規顧客や新たな利用部門の拡大が期待できます。また、冗長化されたインフラは他社へのBtoBサービスとして展開可能であり、業務アプリの機能を横展開する余地があります。
- **社会貢献と安全性**：業務効率化・省人化ソリューションの安全性向上は、行政手続きや産業界の生産性向上に寄与し、国のDXおよびサイバーセキュリティ政策の推進に貢献します。
- **リスク管理**：白書が指摘する脅威に具体的に対応する計画を示すことで、リスク管理の適切性をアピールします。

5. まとめと今後の展望

『情報セキュリティ白書2025』は、サイバー脅威の現状と政策動向を網羅した航海図です。コインバンク株式会社はこの白書の知見を活用し、ものづくり補助金や新事業進出補助金の申請においてセキュリティ対策を明確にすることで、高評価を獲得し、事業の安全性と競争力を同時に高めることを目指します。セキュリティへの投資はコストではなく、顧客信頼と社会的評価を得るための戦略的投資です。今後も最新の情報セキュリティ動向を継続的に追跡し、事業計画に反映させていきます。
