# IT Infrastructure Setup and Maintenance

## IT インフラストラクチャー初期設定及び定期保守

### Table of Contents

目次

# IT Infrastructure Setup and Maintenance

Prepared for: **Mr. Casper Tvede, Mr. Keita Kawasaki, Kysmaq**

Date: January 27, 2026

Dear Kysmaq Leadership Team,

Thank you for taking the time to discuss your IT modernization goals with us. We understand the challenges you're facing—email security vulnerabilities, fragmented systems, and the friction of coordinating DNS changes through NTT.

We're pleased to present our proposal for **M365 Security Essentials plus Cloudflare Protection** closely followed by **Ongoing IT Support**, designed to address your immediate security concerns while laying the foundation for a modern, manageable IT environment.

**What this means for Kysmaq:**

- Your staff can work confidently knowing email phishing and spoofing threats are blocked before reaching their inbox
- Your website gains protection against attacks without requiring constant NTT coordination
- You gain direct control over your DNS, eliminating delays and dependencies
- Your team of 11—including your two roaming sales staff—can collaborate seamlessly with proper M365 licensing

We've structured this as a phased approach, beginning with the security and infrastructure fundamentals that will protect your business and enable future improvements.

We look forward to partnering with you on this journey.

Respectfully,

Rick Cogley
eSolia Inc.

## Scope

Secure Kysmaq's email and web infrastructure, establish DNS independence, and prepare the environment for full Microsoft 365 adoption. Provide ongoing IT professional visits for user support and planning next steps.

## Introduction

eSolia is a Tokyo-based B2B IT professional services firm. Since 1999, we have provided bilingual IT support to international companies operating in Japan, functioning as their local IT department with the same skills and expertise as a dedicated in-house team.

**What sets us apart:**

- **Team-based approach** — We never dispatch single engineers. Our team provides comprehensive coverage across helpdesk, infrastructure, security, and project management.
- **Bilingual professionals** — Native-level English and Japanese communication, bridging headquarters and Japan operations seamlessly.
- **25+ years of experience** — Established operational processes, thorough documentation, and proven track record with multinational clients.
- **Vendor neutral** — We recommend solutions based purely on your needs, not vendor relationships.

We focus on solving your problems, not just providing IT services. Our mission is to deliver practical, durable solutions while maintaining the highest standards of professionalism and confidentiality.

Thank you for the opportunity to present this proposal.

— eSolia Inc.

# M365 Security Essentials

## Foundation-Level Protection for Modern SMBs

**Service Package:** M365 Security Essentials + Cloudflare Protection
**Target Audience:** SMBs (10-100 employees) with Microsoft 365 Business Premium
**Implementation Time:** 2-3 weeks
**Regular DNS and Email Security Monitoring:** via eSolia Periodic

---

# The Challenge

Your business runs on Microsoft 365 and cloud services. But out-of-the-box settings leave critical gaps that attackers actively exploit—misconfigured email authentication, exposed admin accounts, and endpoints connecting from anywhere without verification.

Think of it like moving into a new office building: the doors lock, but you haven't installed the security cameras, programmed the access cards, or set up the alarm system.

This package activates your *digital security system*.

---

# What You Get

## 1. Microsoft 365 Business Premium Hardening

We configure the security features already included in your license—features that protect nothing until properly set up.

| Security Control | What It Does | Business Impact |
|---|---|---|
| **Multi-Factor Authentication (MFA)** | Requires phone verification for all sign-ins | Blocks 99.9% of account compromise attacks |
| **Security Defaults Optimization** | Enforces baseline protections across all users | Eliminates common configuration gaps |
| **Admin Account Protection** | Dedicated, MFA-enforced admin accounts | Prevents privilege escalation attacks |
| **Legacy Protocol Blocking** | Disables outdated authentication methods | Closes backdoors that bypass MFA |
| **Conditional Access (Basic)** | Location and risk-based access policies | Blocks suspicious sign-in attempts automatically |
| **Defender for Office 365** | Anti-phishing, Safe Links, Safe Attachments | Catches threats that basic filtering misses |
| **Data Loss Prevention (Basic)** | Prevents accidental sharing of sensitive data | Reduces compliance exposure |
| **Audit Logging Configuration** | 90-day activity retention (default) | Provides investigation trail |

**Note on Advanced Features:**
M365 Business Premium includes Intune for device management. Full device compliance policies, app protection, and endpoint configuration require Intune enrollment—a separate phase that takes 4-6 weeks for proper rollout. This package establishes your security foundation; Intune deployment is available as a follow-on engagement.

*Features requiring Intune (not included in this package):*

- Device compliance enforcement in Conditional Access
- Mobile Application Management (MAM) policies
- Windows Autopilot device provisioning
- BitLocker enforcement and recovery key management
- Endpoint configuration profiles

---

## 2. Cloudflare Pro + DNS Migration

Your domain is your digital identity. We migrate DNS management to Cloudflare, adding enterprise-grade protection to your existing website and email infrastructure.

| Capability | What It Does | Business Impact |
|---|---|---|
| **DNS Zone Protection** | DDoS mitigation, DNSSEC signing | Prevents domain hijacking and DNS attacks |
| **Website Security** | WAF rules, bot management, SSL/TLS | Protects public-facing web properties |
| **Performance Optimization** | Global CDN, caching, image optimization | Faster site for visitors worldwide |
| **Always Online™** | Cached version during origin failures | Maintains availability during outages |
| **Analytics & Insights** | Traffic patterns, threat intelligence | Visibility into who's accessing your domain |

**Migration Process:**

1. Audit current DNS records and TTLs
2. Replicate zone in Cloudflare
3. Coordinate nameserver cutover (minimal downtime)
4. Verify all services resolve correctly
5. Enable security features progressively

---

## 3. Email Security Configuration (SPF, DKIM, DMARC)

Email spoofing is trivially easy without proper authentication. We implement the full email security stack—configured for maximum protection, not just "passing" compliance checks.

| Protocol | What It Does | Our Configuration |
|---|---|---|
| **SPF (Sender Policy Framework)** | Lists authorized sending servers | Strict `-all` policy (fail unauthorized) |
| **DKIM (DomainKeys Identified Mail)** | Cryptographically signs outbound email | 2048-bit keys, proper selector rotation |
| **DMARC (Domain-based Message Authentication)** | Policy for handling failures | `p=reject` (ultimate goal), phased rollout |

**DMARC Rollout Phases:**

1. **Week 1-2:** `p=none` with monitoring (collect data, identify legitimate senders)
2. **Week 3-4:** `p=quarantine` (suspicious mail to spam)
3. **Week 5+:** `p=reject` (block all unauthorized mail)

*Why "p=reject" matters:* Anything less lets spoofed emails through. Many implementations stop at `p=none` — which does nothing except generate reports.

---

## 4. Ongoing Monitoring via eSolia Periodic

Security isn't a one-time setup. We continuously monitor your configuration through our **Periodic** monitoring platform at periodic.esolia.co.jp.

| Monitoring Area | Check Frequency | Alert Threshold |
|---|---|---|
| **DNS Zone Integrity** | Every 15 minutes | Any record change (A, MX, TXT, CNAME) |
| **SSL/TLS Certificates** | Every 15 minutes | Expiry <30 days, chain issues |
| **Website Availability** | Every 15 minutes | Downtime detected |
| **Domain Reputation** | Daily | Blacklist appearance |
| **DMARC Report Analysis** | Regular (typically daily) | Unauthorized senders detected |

**Monthly Reports Include:**

- DMARC report summary (volume, pass/fail rates, unauthorized senders)
- DNS change log
- Uptime statistics
- Recommendations for improvement

---

## 5. Cloudflare Zero Trust (Endpoint Protection)

Traditional VPNs trust everything inside the network. Zero Trust verifies every connection, every time—without requiring full device enrollment.

| Capability | What It Does | Business Impact |
|---|---|---|
| **WARP Client** | Encrypted tunnel for all device traffic | Protects data in transit everywhere |
| **Gateway DNS Filtering** | Block malicious domains at DNS layer | Prevents malware callbacks, phishing sites |
| **Secure Web Gateway** | HTTP/S inspection and policy enforcement | Blocks downloads from risky categories |
| **Access Policies** | Identity-aware application access | SaaS apps protected without VPN complexity |
| **Device Posture (Basic)** | OS version, disk encryption checks | Baseline security verification |

**Deployment Without Intune:**
This package deploys WARP clients manually or via simple installer distribution. For automatic deployment, compliance enforcement, and advanced posture checks, Intune integration is recommended as a follow-on phase.

*What's included:*

- WARP client deployment to company devices
- Gateway DNS and HTTP policies
- Basic device posture rules
- Access policies for critical applications

*What requires Intune (future phase):*

- Automatic client deployment via MDM
- Strict device compliance enforcement
- Certificate-based device trust
- Conditional access integration

---

## What Comes Next

This package establishes your security foundation. Common follow-on engagements include:

| Phase | Focus |
| --- | --- |
| **Intune Deployment** | Full device management, compliance policies |
| **E5 Security Upgrade** | Advanced threat protection, insider risk |
| **ISO 27001 Preparation** | ISMS documentation, certification readiness |
| **Incident Response Planning** | Playbooks, tabletop exercises |

# eSolia IT Support Services

Reliable, professional IT support tailored to your organization's needs:

**TotalSupport** — Comprehensive Managed IT

Your virtual IT department. We handle all aspects of your IT operations:

- Help desk for end-user support
- System administration and maintenance
- Vendor management and coordination
- Project planning and execution
- Strategic IT consulting
- Regular reporting and reviews

Ideal for organizations that want to outsource IT operations entirely.

**Co-Support** — Collaborative Partnership

Work alongside your existing IT team:

- Augment your team's capabilities
- Provide specialized expertise
- Handle overflow and after-hours support
- Knowledge transfer and training
- Backup for vacations and absences

Ideal for organizations with internal IT that need additional capacity or expertise.

**Support Delivery**

- Bilingual support (English and Japanese)
- Business hours and after-hours options available
- Remote and on-site support
- Work tracking

eSolia's support team brings decades of combined experience supporting businesses in Japan, with deep knowledge of both local and international IT environments.

## Next Steps

- **Review** — Review this proposal and let us know any questions
- **Discussion** — Schedule a call to discuss details
- **Agreement** — We prepare the MSA and SoW documents
- **Signatures** — Both parties sign
- **Kickoff** — Begin onboarding

We are flexible and can adjust scope and terms based on your feedback.

## In Closing

Thank you for considering eSolia. We look forward to supporting your IT needs in Japan.

Please contact us anytime with questions.

**eSolia Inc.**

Tel: 03-4577-3380
Email: hello@esolia.co.jp
Web: https://esolia.co.jp/en

---

# IT インフラストラクチャー初期設定及び定期保守

宛先: **キャスパー ツヴェデ 様、川崎 慶太 様, キースマック**

日付: 2026年1月27日

キースマック 御中

拝啓　時下ますますご清栄のこととお慶び申し上げます。

先日は、貴社のIT環境モダナイゼーションについてお話を伺う機会をいただき、誠にありがとうございました。メールセキュリティの脆弱性、システムの分散化、そしてNTT様経由でのDNS変更に伴うご不便など、現状の課題について理解いたしました。

つきましては、貴社の喫緊のセキュリティ課題に対応し、将来的に管理しやすいIT環境の基盤を構築するため、「M365セキュリティエッセンシャルズ ＋ Cloudflare保護」及び「継続ＩＴサポート訪問」サービスをご提案申し上げます。

**本サービスによるメリット：**

- フィッシングやなりすましメールを受信前にブロックし、安心して業務に集中できる環境を実現
- NTT様との都度調整なしに、ウェブサイトを攻撃から保護
- DNS管理を自社でコントロールし、変更時の遅延や依存を解消
- 神保町オフィスの皆様および外回りの営業2名様を含む11名全員が、適切なM365ライセンスのもとスムーズに連携可能

本プロジェクトは段階的に進め、まずはセキュリティとインフラの基盤整備から着手いたします。

貴社のIT環境改善のお手伝いができれば幸いです。ご検討のほど、よろしくお願い申し上げます。

敬具

株式会社イソリア
コグレー

## スコープ

キースマックのメールとウェブインフラストラクチャを保護し、DNS独立性を確立し、完全なMicrosoft 365導入に向けた環境を準備します。ユーザーサポートと次のステップの計画のために、継続的なIT専門家の訪問を提供します。

## はじめに

イソリアは、東京を拠点とする法人向け（B2B）ITプロフェッショナルサービス企業です。1999年以来、日本で事業を展開する国際企業に対し、バイリンガルITサポートを提供し、専任のIT部門と同等のスキルと専門性を備えたローカルIT部門として機能してまいりました。

**私たちの強み:**

- **チームベースのアプローチ** — 単独のエンジニア派遣は行いません。ヘルプデスク、インフラ、セキュリティ、プロジェクト管理まで、チームで包括的にカバーします。
- **バイリンガルプロフェッショナル** — 英語・日本語ネイティブレベルのコミュニケーションで、本社と日本拠点をシームレスに橋渡しします。
- **25年以上の実績** — 確立された運用プロセス、徹底したドキュメンテーション、多国籍クライアントとの実績があります。
- **ベンダーニュートラル** — ベンダーとの関係ではなく、お客様のニーズに基づいた最適なソリューションをご提案します。

私たちはITサービスを提供するだけでなく、お客様の課題解決に注力します。プロフェッショナリズムと守秘義務の最高基準を維持しながら、実践的で耐久性のあるソリューションをお届けすることが私たちの使命です。

本提案の機会をいただき、誠にありがとうございます。

— 株式会社イソリア

# M365 セキュリティ・エッセンシャルズ

### 現代の中小企業のための基盤レベルの保護

**サービスパッケージ:** M365 セキュリティ・エッセンシャルズ + Cloudflare 保護
**対象:** Microsoft 365 Business Premiumを利用するSMB（従業員10～100名）
**導入期間:** 2～3週間
**DNS及びメール定期的監視:** イソリアPeriodicによる

---

## 課題

御社のビジネスはMicrosoft 365とクラウドサービスで運営されています。しかし、初期設定のままでは重大なセキュリティギャップが残ります。攻撃者はこれらを積極的に悪用します。メール認証の設定ミス、露出した管理者アカウント、どこからでも検証なしで接続するエンドポイント...

新しいオフィスビルに入居するようなものです。ドアには鍵がかかりますが、防犯カメラの設置、入館カードのプログラミング、警報システムの設定はまだ完了していません。

このパッケージは、御社のデジタルセキュリティシステムをアクティベーションします。

---

## サービス内容

### 1. Microsoft 365 Business Premium セキュリティ強化

御社のライセンスに既に含まれているセキュリティ機能を設定します。これらの機能は適切に設定されるまで何も保護しません。

| セキュリティ統制 | 機能 | ビジネスへの影響 |
|---|---|---|
| **多要素認証（MFA）** | すべてのサインインに電話認証を要求 | アカウント侵害攻撃の99.9%をブロック |
| **セキュリティ既定値の最適化** | 全ユーザーに基本保護を適用 | 一般的な設定ギャップを解消 |
| **管理者アカウント保護** | 専用のMFA強制管理者アカウント | 権限昇格攻撃を防止 |
| **レガシープロトコルのブロック** | 古い認証方式を無効化 | MFAをバイパスするバックドアを閉鎖 |
| **条件付きアクセス（基本）** | 場所とリスクに基づくアクセスポリシー | 疑わしいサインイン試行を自動ブロック |
| **Defender for Office 365** | フィッシング対策、安全なリンク、安全な添付ファイル | 基本フィルタリングが見逃す脅威を検出 |
| **データ損失防止（基本）** | 機密データの誤った共有を防止 | コンプライアンスリスクを低減 |
| **監査ログ設定** | 90日間のアクティビティ保持（デフォルト） | 調査用の証跡を提供 |

**高度な機能について:**
M365 Business PremiumにはIntuneによるデバイス管理が含まれています。完全なデバイスコンプライアンスポリシー、アプリ保護、エンドポイント構成にはIntune登録が必要です。これは適切な展開に4～6週間かかる別フェーズとなります。本パッケージはセキュリティの基盤を確立します。Intune展開は後続の契約として対応可能です。

*Intuneを必要とする機能（本パッケージに含まれません）：*

- 条件付きアクセスにおけるデバイスコンプライアンス適用
- モバイルアプリケーション管理（MAM）ポリシー
- Windows Autopilotデバイスプロビジョニング
- BitLocker強制と回復キー管理
- エンドポイント構成プロファイル

---

## 2. Cloudflare Pro + DNS移行

御社のドメインはデジタルアイデンティティです。DNS管理をCloudflareに移行し、既存のウェブサイトとメールインフラにエンタープライズグレードの保護を追加します。

| 機能 | 内容 | ビジネスへの影響 |
| --- | --- | --- |
| **DNSゾーン保護** | DDoS軽減、DNSSEC署名 | ドメインハイジャックとDNS攻撃を防止 |
| **ウェブサイトセキュリティ** | WAFルール、ボット管理、SSL/TLS | 公開ウェブサイトを保護 |
| **パフォーマンス最適化** | グローバルCDN、キャッシュ、画像最適化 | 世界中の訪問者に対してサイトを高速化 |
| **Always Online™** | オリジン障害時のキャッシュバージョン提供 | 障害時の可用性を維持 |
| **分析とインサイト** | トラフィックパターン、脅威インテリジェンス | ドメインへのアクセス状況を可視化 |

**移行プロセス:**

1. 現在のDNSレコードとTTLを監査
2. Cloudflareでゾーンを複製
3. ネームサーバー切り替えを調整（最小限のダウンタイム）
4. すべてのサービスが正しく解決されることを確認
5. セキュリティ機能を段階的に有効化

---

## 3. メールセキュリティ設定（SPF、DKIM、DMARC）

適切な認証がなければ、メールのなりすましは非常に簡単です。単なるコンプライアンス「合格」ではなく、最大限の保護を目的とした完全なメールセキュリティスタックを実装します。

| プロトコル | 機能 | 当社の設定 |
| --- | --- | --- |
| **SPF (Sender Policy Framework)** | 許可された送信サーバーをリスト化 | 厳格な `-all` ポリシー（未承認は失敗） |
| **DKIM (DomainKeys Identified Mail)** | 送信メールに暗号署名 | 2048ビット鍵、適切なセレクターローテーション |
| **DMARC (Domain-based Message Authentication)** | 認証失敗時のポリシー | `p=reject`（最終目標）、段階的導入 |

**DMARC導入フェーズ:**

1. **第1〜2週:** `p=none` + 監視（データ収集、正当な送信元を特定）
2. **第3〜4週:** `p=quarantine`（疑わしいメールを迷惑メールへ）
3. **第5週以降:** `p=reject`（すべての未承認メールをブロック）

*「p=reject」が重要な理由:* それ以外の設定では、なりすましメールが通過します。多くの実装は `p=none` で止まります。これはレポートを生成するだけで、何も保護しません。

---

## 4. イソリアPeriodicによる継続監視

セキュリティは一度きりの設定ではありません。当社の**Periodic**監視プラットフォーム（periodic.esolia.co.jp）を通じて、御社の設定を継続的に監視します。

| 監視対象 | 確認頻度 | アラート閾値 |
|---|---|---|
| **DNSゾーン整合性** | 15分ごと | レコード変更（A、MX、TXT、CNAME） |
| **SSL/TLS証明書** | 15分ごと | 有効期限30日未満、チェーンの問題 |
| **ウェブサイト可用性** | 15分ごと | ダウンタイム検出 |
| **ドメインレピュテーション** | 毎日 | ブラックリスト掲載 |
| **DMARCレポート分析** | 定期（通常毎日） | 未承認の送信元を検出 |

**月次レポートの内容:**

- DMARCレポートサマリー（送信量、認証成功/失敗率、未承認の送信元）
- DNS変更ログ
- 稼働統計
- 改善のための推奨事項

---

## 5. Cloudflare Zero Trust（エンドポイント保護）

従来のVPNはネットワーク内のすべてを信頼します。Zero Trustは、完全なデバイス登録なしで、毎回すべての接続を検証します。

| 機能 | 内容 | ビジネスへの影響 |
| --- | --- | --- |
| **WARPクライアント** | すべてのデバイストラフィックの暗号化トンネル | どこでも転送中のデータを保護 |
| **Gateway DNSフィルタリング** | DNSレイヤーで悪意のあるドメインをブロック | マルウェアのコールバック、フィッシングサイトを防止 |
| **セキュアウェブゲートウェイ** | HTTP/S検査とポリシー適用 | リスクのあるカテゴリからのダウンロードをブロック |
| **アクセスポリシー** | IDを認識したアプリケーションアクセス | VPNの複雑さなしでSaaSアプリを保護 |
| **デバイスポスチャ（基本）** | OSバージョン、ディスク暗号化チェック | 基本的なセキュリティ検証 |

**Intuneなしでの展開:**
本パッケージでは、WARPクライアントを手動または簡単なインストーラー配布で展開します。自動展開、コンプライアンス適用、高度なポスチャチェックには、Intune統合を後続フェーズとして推奨します。

*含まれる内容:*

- 会社デバイスへのWARPクライアント展開
- Gateway DNSおよびHTTPポリシー
- 基本的なデバイスポスチャルール
- 重要アプリケーションのアクセスポリシー

*Intuneが必要な内容（将来のフェーズ）:*

- MDMによる自動クライアント展開
- 厳格なデバイスコンプライアンス適用
- 証明書ベースのデバイス信頼
- 条件付きアクセス統合

---

## 次のステップ

本パッケージはセキュリティの基盤を確立します。一般的な後続の契約には以下が含まれます:

| フェーズ | 重点領域 |
| --- | --- |
| **Intune展開** | 完全なデバイス管理、コンプライアンスポリシー |
| **E5セキュリティアップグレード** | 高度な脅威保護、インサイダーリスク |
| **ISO 27001準備** | ISMS文書化、認証準備 |
| **インシデント対応計画** | プレイブック、卓上演習 |

# eSolia ITサポートサービス

お客様の組織のニーズに合わせた信頼性の高いプロフェッショナルなITサポート：

**TotalSupport** — 包括的マネージドIT

お客様のバーチャルIT部門として、IT運用のすべての側面を担当します：

- エンドユーザーサポートのヘルプデスク
- システム管理とメンテナンス
- ベンダー管理と調整
- プロジェクト計画と実行
- 戦略的ITコンサルティング
- 定期的なレポートとレビュー

IT運用を完全にアウトソーシングしたい組織に最適です。

**Co-Support** — コラボレーティブパートナーシップ

既存のITチームと協力して：

- チームの能力を強化
- 専門的な知識を提供
- オーバーフローと時間外サポートを処理
- ナレッジ移転とトレーニング
- 休暇や不在時のバックアップ

追加のキャパシティや専門知識が必要な社内ITを持つ組織に最適です。

**サポート提供方法**

- バイリンガルサポート（英語と日本語）
- 営業時間および時間外オプションあり
- リモートおよびオンサイトサポート
- 作業追跡

eSoliaのサポートチームは、日本でのビジネスサポートにおける数十年の経験を持ち、国内外のIT環境に関する深い知識を持っています。

## 次のステップ

- **レビュー** — 本提案をご確認、ご質問をお知らせください
- **ディスカッション** — 詳細を話し合う電話を設定
- **契約書** — MSAとSoW文書を準備
- **署名** — 両者で署名
- **キックオフ** — オンボーディング開始

スコープと条件はフィードバックに基づいて柔軟に調整可能です。

## 最後に

イソリアをご検討いただきありがとうございます。日本でのITニーズをサポートできることを楽しみにしております。

ご質問があればいつでもお気軽にお問い合わせください。

**株式会社イソリア**

Tel: 03-4577-3380
Email: hello@esolia.co.jp
Web: https://esolia.co.jp

---