2026 年 2 月 16 日
興和江守株式会社

サイバーセキュリティ事案の収束と再発防止に向けた取り組み

1. 概要

2026 年 1 月 7 日、当社システムにおいて暗号化を伴う不正アクセスの影響を確認しました。直ちに端末のネットワーク遮断等の初動を行い、外部専門機関の支援のもと、調査および封じ込めを進めました（2026 年 1 月 7 日 公表）。

外部専門機関によるフォレンジック調査[①]では、解析対象において外部への明確な情報漏洩の痕跡は確認されておりませんが、情報窃取の可能性を完全に否定することはできないため、調査を継続しております。

2. 現在までの対応

・安全性確認と新環境の整備

既存環境と切り離した新ネットワークおよび新端末の安全性確認を実施し、段階的に業務利用を開始しました（2026 年 1 月 20 日 公表）。

・メール送受信の再開（多層防御と運用変更）

受信・送信時の検知や誤送信防止を行うとともに、添付ファイルは安全な専用環境に格納し、ダウンロード用 URL を通知、パスワードは別送する方式としております（2026 年 1 月 26 日 公表）。

3. お取引、ご利用に関するお願い

当社からの添付ファイルは、専用環境の URL をご案内し、パスワードを別送する方式としております。送信者情報や内容にお心当たりがない場合は URL を開かず、当社担当者までご確認ください。

4. 再発防止に向けたロードマップ

以下の三段階のロードマップに基づき、段階的かつ継続的に再発防止対策およびセキュリティ強化を進めてまいります。

【短期（即時～2026 年 3 月末）｜被害の封じ込めと再発リスクの低減】

・安全性を確認した新環境での段階的な業務再開と、運用ルールの定着

・メール送受信における多層的な防御と、安全な添付ファイル提供方式の継続運用

---

① 不正アクセス、ランサムウェア感染などのインシデントが発生した際に証拠を保全しながら事実関係を解明する調査

・インシデント対応で得られた知見を踏まえた初動対応および連絡体制の整理
これらの対応により、同様の事象が発生した場合でも、早期に把握し被害拡大を防止できる状態を整えます。

【中期（～2026 年 9 月）｜検知力・可視性の強化と標準運用への移行】
・NIST サイバーセキュリティフレームワーク[②]を参照し、技術面・運用面・体制面を含むセキュリティ対策の現状把握と改善優先度の整理を実施
・Windows の標準的なセキュリティ設定を計画的に適用し、端末およびサーバーの挙動可視性と耐性を向上
・重要システムを対象に、外部サービスによる常時監視を導入し、異常の早期検知と対応判断を支援する体制を整備
・多要素認証（MFA）を含む認証強化を段階的に進め、不正利用リスクの低減を図る

【長期（2026 年下期～）｜継続的改善とセキュリティ成熟度の向上】
・最小特権と継続的な認証を前提とした運用および設計を段階的に導入
・脆弱性および設定管理の定常化、訓練を含む事業継続体制の定期的な見直し
・第三者の視点による定期的な評価を活用し、改善状況の確認とセキュリティ向上のサイクルを定着
これらの取り組みは、業務への影響を考慮しながら段階的に進め、定期的に実効性を確認します。

5. 今後の開示方針
重要な進展（節目の完了、外部専門機関の所見更新等）が認められた場合には、速やかに当社ホームページにて公表いたします。必要に応じて、対象となるお取引先様および関係者様へ個別にご連絡します。

6. これまでの公表
・2026 年 1 月 7 日　事案発生（事実認知・影響・問い合わせ先の案内）
・2026 年 1 月 20 日 対応第 1 報（新環境・新端末の安全性確認と段階的再開の方針）
・2026 年 1 月 26 日 対応第 2 報（メール送受信の再開と添付ファイル送付方式変更）
・2026 年 2 月 16 日 対応第 3 報（事案の収束と再発防止に向けた取り組み）

---

② 米国国立標準技術研究所（NIST）が策定した、組織のサイバーセキュリティ対策を体系的に整理・評価するための指針