2023 年 6 月 28 日

お客様各位

株式会社エムケイシステム
代表取締役　三宅　登

セキュリティ調査に関する報告書

このたびは、お客様、顧問先様、お取引先様、関係者の皆様に多大なご迷惑をお掛けしておりますことを、深くお詫び申し上げます。

このたび発生しました情報セキュリティインシデント（以下「本事案」という）に関して、調査結果を以下の通りご報告申し上げます。

なお、本事案は情報セキュリティに関するものであり、本報告書においても重要な情報が部分的に含まれていることから弊社内においても厳秘扱いとしています。貴社におかれましても、本書面の取り扱いには充分注意頂き、関係者以外には一切漏洩することがないよう、厳密な管理をお願い申し上げます。

１．発生事象

2023 年 6 月 5 日（月）未明、弊社情報ネットワーク内の複数のサーバがサイバー攻撃により被害を受け、サーバ上のデータが暗号化されました。この攻撃により、暗号化されたデータへのアクセスができなくなり、結果としてシステムが停止し、再構築を余儀なくされる事態となりました。

２．本事案の対応経緯（初期検知と初動対応）

2023 年 6 月 5 日（月）未明、弊社担当者が弊社のデータセンターで稼働するサーバへアクセスできないことからシステム異常を認知しました。事象を認知した後、弊社担当者がデータセンターへ入館し状況を確認した結果、弊社サービスを使用しているサーバがランサムウェアに感染していることが判明しました。事象確認後、同日 9 時頃からデータセンターで稼働していた全てのサーバをネットワークから遮断し、マルウェアの感染拡大や被害拡大防止のための対処を行いました。

本事案に関する主な初動対応は以下の通りです。

日付	対応状況
2023/6/5（月）6:00 頃	システムやサービスにアクセスできない状況を確認、システム異常を検知
2023/6/5（月）7:00 頃	弊社内での調査開始。ランサムウェアによる感染を認知
2023/6/5（月）9:00 頃	全てのサーバをネットワークから遮断（LAN ケーブル抜線） VPN サービスを停止、アカウント無効化
2023/6/5（月）	事案認知直後から全てのサーバ及びパソコンの侵害の有無について状況把握を実施
2023/6/5（月）午後	外部の情報セキュリティ専門会社へ対応要請 ～その後、状況ヒアリングや初動対応及び原因調査のためのデータ保全等を実施
2023/6/6（火）	大阪府警（捜査当局）へ本事案について連絡、事情聴取に対応

日付	対応状況
2023/6/6（火）～7（水）	状況把握を進めるとともに、復旧対応や原因調査等について協議 情報セキュリティ専門会社にて調査対象機器や保全対象のヒアリング・準備を開始
2023/6/8（木）	個人情報保護委員会へ報告
2023/6/8（木）	調査対象機器へのデータ保全を実施、
2023/6/16（金）	原因調査のためのデータ保全を追加実施
事案発生直後～現在	システム復旧に向けた再構築
2023/6 月中旬～現在	再発防止策及び対策強化策の内容精査
2023/6 月最終週	調査報告書について、希望するユーザへ配布
2023/7 月中旬	個人情報保護委員会へ確報情報として報告（予定）

3．保全対象機器

本事案の原因調査のため、本事案が発生した弊社ネットワークにおいて、侵害可能性として考えられる経路上の機器や攻撃者によって侵害された重要サーバ（AD サーバ、SQL サーバ、仮想基盤サーバ等）を中心に保全対象を選定し、対象機器のディスクイメージまたはログを保全致しました。

（1）保全した対象機器（サーバ機器）

ホスト名	用途	ディスク容量	保全日時
xxx01	AD サーバ（ドメイン a）	279GB	6/8　14:04～14:39
xxx02	AD サーバ（ドメイン a）	932GB	6/17　16:49～19:12
xxx03	AD サーバ（ドメイン b）	279GB	6/8　14:33～14:59
xxx04	SQL サーバ（ドメイン a）	279GB	6/16　11:49～12:18
xxx05	仮想基盤サーバ	279GB	6/16　11:53～12:20

（2）保全した対象機器（ネットワーク機器）

機器名	ファイル種別	出力期間	ファイル数
Firewall/VPN	ログファイル	2023/3/16　0:59～2023/6/6　23:59	66
	設定ファイル	2023/1/19～2023/6/14	70
Firewall	ログファイル	2023/6/4　0:00～2023/6/6　0:00	4
	設定ファイル	2023/6/15	1

４．状況把握と被害状況

本事案による侵害状況について、弊社内の全てのサーバ及びパソコンに対して調査を実施した結果、侵害された機器は全て AD ドメイン（ドメイン a 及びドメイン b）に参加している Windows サーバであることが確認されています。

なお、これら侵害を受けた Windows サーバからファイル共有されていたストレージサーバのデータ領域も暗号化の被害が発生していることを確認しています。また、侵害を受けたサーバの中には仮想サーバが稼働する仮想基盤サーバがあり、これらサーバのデータも暗号化されたことで仮想サーバへのアクセスができなくなり、全ての仮想サーバが利用できない事態となりました。

一方で、社内システムに相当するドメインについては、サーバ（物理サーバ/仮想サーバ）・パソコンともに侵害被害が発生していないことを確認しています。

５．侵害状況の概要

（１）不正アクセスの痕跡と侵入経路（ネットワーク機器）

VPN Firewall（社内）より採取した本事案の発生時をまたぐログデータの解析から、データ漏洩などを想定される不審な挙動は確認できておりません。社内システムでの侵害被害も発生していないことも加え、侵入経路としての可能性は低いと考えます。社労夢サービス側の Firewall はブロック通信のログのみを出力する設定になっていた為、通信の詳細は調査出来ていません。

（２）不正アクセスの痕跡と侵入経路（サーバ機器）

保全したサーバ機器を調査した結果、対象機器の全てにおいてランサムウェアによるデータ暗号化の痕跡を確認しました。また、サービス提供セグメントで稼働していた公開システム（RemoteAPP サーバ）からリモートデスクトップ（RDP）を介してドメイン a の AD サーバへ不正アクセスされた痕跡を確認しました。

アクセス日時	アカウント種別	
2023/6/5　1:12:28	User	何らかの手段でアカウント取得しログイン
2023/6/5　1:42:39	Admin	管理者権限を奪取

これらのアクセス痕跡から、攻撃者はドメイン a のアカウント情報を何らかの方法で取得し、公開システム（RDP サーバ）へログインしたものと考えられます。その後、攻撃者はドメイン a の管理者権限を奪取し、その権限を利用して同ドメインに所属するサーバに対して侵害を行ったものと考えられます。

（３）侵入後の不正プログラム及びランサムウェア実行

攻撃者は、AD サーバへログイン後の 1:43 よりリモートアシスタントツールやハッキングツールなどの実行を開始し、3:14 からランサムウェアによる暗号化へと移行していることを確認しています。

実行日時	プログラムの概要
2023/6/5　1:43～1:49	リモートアシスタントツール
	ハッキングツール
	侵入テストに利用されるフレームワーク
	リモートアシスタントツール

2023/6/5　2:18	プロセス一覧表示ツール
2023/6/5　3:14～	ランサムウェア（データ暗号化）･･･各サーバにおいて

（4）不正プログラム（マルウェア）

調査対象機器のうち、仮想基盤サーバ及び SQL サーバから不審なプログラムを確認、検体解析をした結果、本事案で悪用されたマルウェア（ランサムウェア）であることを確認しています。

当該マルウェアの名称をはじめとする概要については、関係当局及びセキュリティ専門会社より今後の情報セキュリティ面のことを考慮し、一切の対外的公表を慎むよう指導を頂戴していることより控えさせて頂きます。

6．情報漏洩の有無について

AD サーバ及び個人情報を保持する SQL サーバの調査において、暗号化の実行に利用されたランサムウェアプログラムの存在やデータ暗号化の痕跡は確認されておりますが、SQL サーバに関するプログラムの実行やサービスに対する接続痕跡、データベース情報の抽出・圧縮や外部転送などの情報搾取を示唆するプログラムの実行の事実や痕跡は確認されておりません。

以下の通り、SQL サーバ内のフォルダへのアクセスや不審なプログラムの実行などが確認されています。

実行日時	操作内容・実行内容
2023/6/5　3:15	データ暗号化
2023/6/5　4:05	フォルダアクセス
2023/6/5　4:06	隠しファイル、ルートキットなどの検出ツール実行
2023/6/5　4:08	ランサムウェアプログラム作成

また、本事案に関連する情報のダークウェブ等での掲載についても調査を実施していますが、現時点においても該当情報の掲載や公開は確認されておりません。

以上のことより、本事案への調査の現時点において、情報漏洩の事実は確認されていないこと、ご報告いたします。

7．再発防止策

現在までの調査で確認された本事案の原因を踏まえ、米国 CIS（Center for Internet Security）が定義する CIS Controls（V8）をベースとした抜本的な改革を推進していく所存です。

初段の対応として、以下の再発防止策を実施します。

（1）ネットワークセキュリティ対策の強化

システムに対するアクセス要件を整理し、アクセス権限を必要最小限に制限します。

＊6/30 迄に実施：利用者 ID、管理者 ID のアクセス制限の見直し及び再定義

（２）エンドポイントセキュリティ対策の強化（既知脅威情報だけでなく未知の脅威対応　他）

＊実施済み：AWS 上の仮想サーバ、自社 PC を含め、全台に EDR 導入、
24 時間/365 日体制での監視体制開始

（３）脆弱性管理の徹底とペネトレーションテストの実施

脆弱性情報の適切な入手と把握、迅速かつ適切な脆弱性対応を実施します。

＊6/30 迄に実施：ペネトレーションテストの実施

＊6/30 以降：脆弱性対応の適用利用について定期的な確認を実施（年 2 回）

（４）ネットワークセキュリティ対策の強化

＊実施済み：クラウド基盤を IDC から AWS に変更し、AWS セキュリティポリシーの適用
ネットワーク接続に AppStream2.0 を採用しセキュリティ強化
脆弱性対応最新セキュリティプログラムの適用

（５）強固な認証方式の利用

＊6/30 迄に実施：強固なパスワードポリシーの利用（利用者、管理者）

＊早期に実施：二要素認証などを活用した強固な認証方式の利用

（６）定期的なアカウントの棚卸

＊6/30 迄に実施：不要なアカウントの無効化または削除

（７）定期的なログレビューの実施

＊6/30 以降：ログの安全な保管及び長期保存

＊定期的に実施：ログの定期的なレビューや分析による不審なアクティビティの検出

（８）リスクアセスメント、情報セキュリティ監査の定期的な実施

＊7 月より月 1 回　定期的に実施

（９）情報セキュリティの運用体制の見直し

＊実施済み：情報キュリティ専門家の活用

＊7 月から：情報セキュリティ部門の増員

以上