2023 年 08 月 31 日

障害経緯報告書

株式会社ラクス

この度は、貴社ご利用の「クルメル」（以下、弊サービス）障害により、多大なるご迷惑をおかけ致しまして誠に申し訳ございません。今回発生致しました事象の経緯について下記のとおりご報告致します。

記

1. 概要

以下に記載している期間、弊サービスのメール配信環境のもつドメイン・IP アドレスが外部セキュリティ団体のブラックリストに登録されたことにより、当該ブラックリストを参照する一部の宛先に対してメール配信が遅延、あるいは失敗する状態となっておりました。

影響期間

2023 年 8 月 19 日 09 時 00 分　～　2023 年 8 月 29 日 12 時 00 分

2. 経緯

2023 年 8 月 19 日　9 時 00 分頃

一部宛先へブラックリスト起因によるブロック発生。

（後日配信ログ調査によりブロックを確認）

2023 年 8 月 20 日　9 時 30 分頃

配信環境の IP アドレスの 1 つが IP ブラックリストに登録されたことを検知。この際ドメインのブラックリストへの登録はなし。

2023 年 8 月 21 日　9 時 30 分頃

定期のブラックリスト監視チェックにてクルメルの利用するドメイン(hcm-nc. jp)がブラックリスト登録されたことを確認。また同時にドメインに関連する IP アドレス（137IP）もブラックリストに登録されたことを確認。

2023 年 8 月 21 日　9 時 45 分頃

ブラックリスト運営団体にブラックリスト登録原因の調査とブラックリストからの解除を要請。

2023 年 8 月 21 日　13 時 00 分頃

ブラックリスト運営団体より一部ユーザーより特定電子メール法に違反したメールの送信及びトラップアド

レスへの配信が多数検知されたためブラックリスト登録が実施された旨の回答を得る。

2023年8月21日　19時00分頃

解消に時間を要する可能性が高いため、ブラックリスト登録されたドメインとは別ドメイン(hcm-gc.jp)の回避用サーバより添付・TLS配信を除くメール配信（添付なし、かつ平文でのメール配信のみ）を開始。

2023年8月22日　16時00分頃

ブラックリスト運営団体より連携されたメール件名の送信元ユーザー抽出と当該ユーザーを高エラー配信環境に隔離。（当該顧客には別途是正勧告を実施。）

2023年8月22日　20時00分頃

前日19時より対応の添付配信メール・TLS通信メールの回避環境の構築完了後、添付配信メール・TLS通信メールも回避ドメイン(hcm-gc.jp)より配信開始。

2023年8月22日　21時00分頃

回避ドメイン(hcm-gc.jp)にてブラックリスト起因による配信エラーを確認。回避用ドメイン(hcm-gc.jp)についても同様にブラックリスト登録されたことを確認。新たに回避用ドメインに対してブラックリスト運営団体に問い合わせを開始。

2023年8月23日　12時00分頃

ブラックリスト運営団体より新たに問題のあるメール件名情報の提供を受け、送信元ユーザーの抽出を行い、高エラー配信環境に隔離。（当該顧客には別途是正勧告を実施。）

措置を講じたことをブラックリスト運営団体に報告、解除申請を実施。

2023年8月23日　16時00分頃

ブラックリスト運営団体より新たに問題のあるメール件名情報の提供を受け、送信元ユーザーの抽出を行い、高エラー配信環境に隔離。（当該顧客には別途是正勧告を実施。）

2023年8月24日　09時00分頃

ブラックリストに登録されていたドメインの解除を確認。

2023年8月24日　10時30分頃

ドメインのブラックリストは解除済みであるが、IP アドレス単位のブラックリスト登録が継続していることを確認。

2023年8月24日　12時30分頃

IP アドレスの解除申請を進めるとともに、配信履歴からブラックリスト登録の原因となるトラップアドレス

の抽出と当該アドレスへの配信停止を実施。以降、顧客環境毎にトラップアドレスの精査・配信停止と解除申請を継続実施。

2023年8月24日　18時00分頃

IPアドレスブラックリスト登録状況：130

2023年8月25日　18時00分頃

IPアドレスブラックリスト登録状況：61

2023年8月26日　18時00分頃

IPアドレスブラックリスト登録状況：51

2023年8月27日　18時00分頃

IPアドレスブラックリスト登録状況：43

2023年8月28日　18時00分頃

IPアドレスブラックリスト登録状況：15

2023年8月29日　12時00分頃

IPアドレスブラックリスト登録状況：0

3. 暫定対応（本障害への対処内容）

・特定電子メール法違反顧客への対応

① ブラックリスト運営団体から指摘のあったユーザーへの是正勧告、是正確認及び配信環境の隔離

・ブラックリストによるメール不達事象への回避対応

① 予め用意していた回避用ドメインを経由したメール送信によるメール不達事象の回避

② 新規ドメインでの迂回用配信環境の構築（上述回避用ドメインのブラックリスト登録後の対応）

・ブラックリスト解除への対応

① ブラックリスト運営団体に対する解除申請

② お客様へのトラップアドレス（タイポアドレス含む）精査のご依頼

③ お客様の配信リストのオプトイン・配信メールへのオプトアウト設置のご依頼

④ ブラックリスト運営団体からの情報に基づくトラップアドレスの調査及び該当アドレスへの送信停止

・当該期間の配信エラーへの対応

① 当該事象期間中の配信エラー一括リセット対応を 8 月 31 日(木)に実施完了

4. 原因

1. 一部のユーザーにて特定電子メール法違反のメールの送信及びトラップアドレスへの配信があり、外部セキュリティ団体のブラックリストに登録されたため。
2. 特定電子メール法違反へのリスクに対しては以下対策を行っていたが、不十分であったため。
   ① 高エラー配信ユーザーの配信環境振り分け管理・当該ユーザーへの是正勧告
   ② コンテンツチェックのフォロー（キーワード・URL のチェック）
   ③ 事象発生時の影響範囲局所化のため、複数ドメイン・IP セグメントを持った配信環境の整備
   ④ プロバイダより指摘のあった特定電子メール法違反ユーザーへの是正勧告
   ⑤ トラップアドレスの精査・配信停止措置
   ⑥ 各種ブラックリスト団体の登録状況の確認及び解除申請

5. 恒久対応・再発防止策（今後の対応方針）

1. 本事象の予防措置として以下を実施する。
   ① 高エラー配信ユーザーの配信環境振り分け管理の強化
   ② 新規契約顧客への配信リスト精査の依頼徹底
   ③ トラップアドレスの精査強化（トラップアドレス精査に利用するツールの精度向上）
   ④ 配信リストにトラップアドレスが含まれていることをお客様に通知するアプリケーション機能の追加
2. 本事象が万一再発した場合に備え以下を実施する。
   ① 影響が甚大なブラックリストの登録状況に関する監視周期の見直し
   ② 現配信環境のドメイン及び IP セグメントを増やし、影響範囲の局所化及び回避環境の増強

この度は、貴社並びに貴社クライアント様に多大なるご迷惑をおかけいたしまして、誠に申し訳ございません。
重ねて深くお詫び申し上げます。

以上