2020 年 10 月 14 日

HENNGE 株式会社

Incident No: HEA2020101401

Post-Incident Report
HENNGE Email Archive メール検索結果の反映遅延

■ 発生事象

2020 年 9 月 1 日（火）に確認された Google 転送設定の仕様変更により、G Suite と HENNGE Email Archive サービスをご利用いただいているすべてのお客様に対して、アーカイブ検索結果の反映に時間がかかる状況が発生いたしました。なお、本事象による、HENNGE Email Archive サービスのログデータの欠損等のダウンタイムは検知していません。

■ 発生日時（本報告の時刻表記は JST/日本時間で記載します）

2020 年 9 月 1 日（火）9 時 00 分頃 から 2020 年 9 月 8 日（火）8 時 00 分頃まで

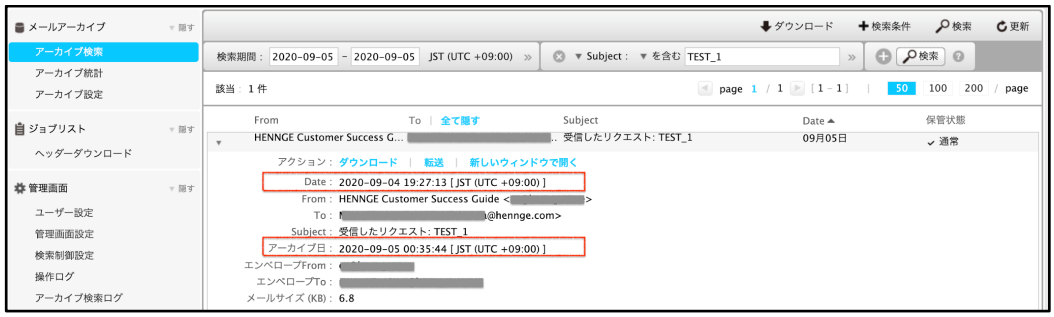
■ 影響範囲

1. 上述の発生時間帯、HENNEG Email Archive サービスへのアクセス及び画面操作は可能でしたが、アーカイブ検索において、一部のメールが結果に表示しない、または通常(*1)よりも遅延して反映する状況が発生いたしました。

   *(*1)* メール送受信からアーカイブ検索の反映まで、*9* 時間以内を指標としています。

2. 上述の発生時間帯に送受信されたメールにおいて、実際の送受信日ではない期間で、アーカイブ検索結果が表示する可能性があります。

   例）
   9 月 *4* 日に受信したメールを *HENNEG Email Archive* サービスで検索すると、*9* 月 *4* 日の検索期間では表示せず、*9* 月 *5* 日の検索期間に表示する。



赤枠の「*Date*」は送受信メールの *Date* ヘッダーから取得した日時、「アーカイブ日」は *HENNGE Email Archive* で受付した日時です。

HENNGE Email Archive は、Google 転送設定機能からメールを受付した時間を「アーカイブ日」とし、検索期間の対象はこのアーカイブ日としています。これは、送受信メールの Date ヘッダーは、必ずしも実際の送信日時が記録される仕様ではないためです。なお、アーカイブデータの完全性を担保するサービス設計上、アーカイブ日の修正を行うことはできません。

3. G Suite 管理コンソールで設定する、HENNGE Email Archive サービス用転送設定のバウンスメールの通知(*2)を有効にしているお客様環境で、実際のメール送信者に配送遅延の通知(*3)が届く状況が発生いたしました。

*(*2) G Suite* 管理コンソールの設定箇所
アプリ ＞ *G Suite* ＞ *Gmail* の設定 ＞ 詳細設定 ＞ （転送設定の）編集

[3. 上記の種類のメッセージに対しては、次の処理を行います *]* >> *[* 受信者を追加 *]* >> *[* 登録ユーザー *]* >> *[* 迷惑メールと配信のオプション *]* >> *[* この受信者からのバウンスメールを送信元に送信しない *]* が有効となっている。

*(*3)* 送信者に届く通知
From: Mail Delivery Subsystem <mailer-daemon@googlemail.com>
件名：*Delivery Status Notification（Delay)*

■　発生原因

HENNGE Email Archive は、G Suite 管理コンソールで設定する転送設定を利用し、お客様が送受信するメールのコピーを、HENNGE の受信メールサーバーに転送しています。この転送されたメールを保存し、アーカイブ検索に反映する処理を行っています。この HENNGE の受信メールサーバーは、不正なメール流入を防止するため、Google 社が SPF レコードに公開する IP アドレスからのみ接続許可しています。

事象発生時、一部のメール転送(*4)において、Google 社非公開の IP アドレスから HENNGE の受信メールサーバーに対して接続が行われ、HENNGE 側で接続拒否する状況が発生いたしました。結果、HENNGE 側が接続許可している IP アドレスからメールの再送が行われるまで、受信が遅延し、アーカイブ検索の反映等、今回の発生事象の原因となりました。

*(*4) Google* 社の仕様変更は、*8* 月 *24* 日*(*月*)*頃より全てのテナントに順次実施されました。以下に、仕様変更の概略を記載します。

受信メールに対するセキュリティ向上のため、受信ゲートウェイ設定を経由したメール、及び、*SPF* 認証に失敗したメール群は、従来の受信ルーティング設定により経由する *MTA* ホストではなく、別のホスト（**.unverified-forwarding.1e100.net*）を経由します。

■　事象発生からの時系列と弊社対応

以下に、事象発生から現在に至るまでの時系列を記載します。

9 月 01 日(火) 09:00	後の調査で、HENNGE Email Archive の受信（インバウンド）メールの受信通数が、通常の統計よりも減少し始める
9 月 01 日(火) 09:00	後の調査で、HENNGE Email Archive の送信（アウトバウンド）メールの受信通数が、通常の統計よりも減少し始める
9 月 04 日(金) 10:00	一部のお客様より、Google より配送遅延メールが届く事象に関する問い合わせを受け、調査開始。
9 月 04 日(金) 12:20	サービス環境の異常は確認できなかったものの、通常時の統計と比較して、9 月 01 日以降のアーカイブメール数が減少していることを確認。問題発生と認識し、詳細な調査に着手。
9 月 04 日(金) 12:43	HENNGE Email Archive ロードバランサ用途のサーバーインスタンスを追加。
9 月 04 日(金) 12:46	ステータスダッシュボードで初報配信。

9 月 04 日(金) 13:16	事象改善が見られず、HENNGE Email Archive ロードバランサ用途のサーバーインスタンスのリソース増強を実施。
9 月 04 日(金) 15:00	事象改善が見られず、HENNGE Email Archive の新しい、別 IP アドレスのロードバランサ用途のサーバー追加準備。
9 月 04 日(金) 15:02	ステータスダッシュボードで影響範囲の修正報告。
9 月 04 日(金) 16:37	HENNGE Email Archive の新しい、別 IP アドレスのロードバランサ用途のサーバー追加。
9 月 04 日(金) 18:24	事象再現性がとれた G Suite テナントから問題発生状況を Google 社へエスカレーション実施。
9 月 04 日(金) 22:53	事象改善が見られず、基盤側に起因した可能性を疑い、Amazon Web Service サポートに発生事象の問い合わせを実施。
9 月 05 日(土) 09:35	Amazon Web Service サポートより、基盤側の問題はない旨と、また、Google からの接続セッション数に減少が見られる旨の回答を受領。
9 月 05 日(土) 10:12	ステータスダッシュボードで対応状況を更新
9 月 05 日(土) 11:00	事象改善が見られず、サーバーインスタンスの接続にかかる設定調整。
9 月 05 日(土) 14:30	事象改善が見られず、ロードバランサの設定値調整。
9 月 05 日(土) 16:05	ステータスダッシュボードで対応状況を更新
9 月 05 日(土) 20:30	Google 社より事象発生状況の追加エビデンス提示の要請があったため再エスカレーションを実施。
9 月 05 日(土) 23:00	事象改善が見られず、転送先ホストの切り替えを検討。
9 月 06 日(日) 10:07	ステータスダッシュボードで対応状況を更新
9 月 06 日(日) 12:00	HENNGE Email Archive ロードバランサ用途のサーバーへの接続に対して、許可外の IP アドレス群の存在を複数確認。IP アドレス所有者が Google 社であったことから、非公開 IP アドレスが追加された可能性を疑い、許可 IP アドレスの追加を検討、準備。
9 月 06 日(日) 13:22	ステータスダッシュボードで対応状況を更新
9 月 06 日(日) 13:30	HENNGE Email Archive ロードバランサ用途のサーバーインスタンスのリソース増強と、許可 IP アドレス群の追加を実施。改善傾向を確認。
9 月 06 日(日) 14:12	ステータスダッシュボードで対応状況を更新
9 月 06 日(日) 19:06	通常の統計と比較し、アーカイブメール数が増加して受信していることを確認。Google 側に滞留しているメールキューが順調に処理されている状況と判断。 ステータスダッシュボードで対応状況を更新
9 月 07 日(月) 10:45	ステータスダッシュボードで対応状況を更新
9 月 07 日(月) 11:00	Google 社より、発生原因記載の仕様変更についての回答を受領。
9 月 07 日(月) 18:38	ステータスダッシュボードで対応状況を更新
9 月 08 日(火) 08:00	モニタリング状況より、通常の統計と比較し、正常稼働に戻ったことを判断。
9 月 08 日(火) 10:55	ステータスダッシュボードで事象解消を配信。

■　恒久対応策

同事象の発生を迅速に検知できますよう、監視サービスを構築しています。当該サービスは、9 月 08 日以降運用を開始しており、今後の想定外の Google 社の IP アドレス追加が実施された場合においても、迅速なアラート検知と、その後の対応が可能な状態になっています。

なお、Google サポートに問い合わせを行った結果、今回弊社が確認した IP アドレス群については、Google の SPF レコードに公開された IP アドレスの範囲と異なるものの、Google 社が管理する送信メールサーバーの IP アドレスである旨の回答を得ております。

また、事象発生原因となりました Google 社による当該アップデート情報は、~~公開時期未定であるものの、今後 Google 公式ウェブサイトにて開示を検討されている旨の回答も得ております。~~10 月 14 日時点で、以下のサイト上の「IP address ranges for unverified forwarding」章にて開示された事を確認いたしました。

[参考情報]
https://support.google.com/a/answer/60764?hl=en

以上