作業着手前・作業完了後のトラブル発生時に関して

各ドメインにて、脆弱性対応に着手する前および、下記の「作業内容に関して」に記載した作業完了後に、脆弱性による問題が発見された場合は、責任範囲外とさせていただきます。

作業内容に関して

ディレクトリ・ファイルの削除等、サーバー側で行ったほうが適切な処理は行えません。
削除が必要な場合、本番環境での作業のため、ディレクトリ・ファイルの削除等は、貴社側で対応していただくのが安全かと思っております（※1）。
下記以外の対応は業務範囲外とさせていただきます。下記以外で業務が発生した場合、別途協議させていただきます。

- **a-blog cmsのアップデート**
  - バージョンアップ前後の差分を確認し、問題ないかを確認
  - 脆弱性に対応したバージョンを満たすバージョンへのパッチバージョンのみのオンラインアップデート
  - オンラインアップデートで、もしも問題が発生した場合、バージョンアップ前のコアファイルをアップロードして対応し、キャッシュクリア後に確認
- **a-blog cmsの脆弱性対応**
  - アップデートを実施するまでの応急処置とアップデート後の脆弱性対応として、https://developer.a-blogcms.jp/blog/news/entry-4197.htmlに記載されている以下の応急処置の実施をします。
    - 2025/03/20以降に設置された不審ファイルが無いかをscan.phpにて確認し、不審ファイルを発見した場合、削除はせず（※2）、貴社にて判断後、不審ファイルのパーミッションを000へと変更いたします。scan.phpは確認後削除いたします。
    - （是非を判断中　「しない」とのお返事ありのため、実施しない　.htaccess で PHP の実行を制限します。CMSのindex.phpのみ実行できるようにする場合、メンテナンスプログラムや、CMS外のプログラムも動作しなくなります。）

注意事項について（※必ずご一読ください）

※1　**アップデート前に攻撃に利用されたファイルの削除をする場合は、貴社にてお願いいたします。**
※2　不審ファイルと疑わしいファイルを発見次第、スプレッドシートにまとめてお渡しします。現在、Discordへ報告されている不審ファイルを、作業前までにスプレッドシートにまとめてお渡ししますので、判断のご参考にしてください（この**不審ファイルのファイル名に関しては、アップルップル様よりネットやSNS等に載せないようにと注意喚起されております**ので、よろしくお願いいたします）。
私では不審ファイルかの判断ができないため、貴社にて不審ファイルを判断後、不審ファイルのパーミッションを000へと変更いたします。不審ファイルのパーミッションを000へと変更することで、アップデートまでの暫定的な対策になります。

アップデート後は、不審ファイルの削除を推奨いたします。不審ファイルを削除される場合は、貴社にてお願いいたします。
※3　Ver3.1系までへのアップデートはしないため、.htaccessで、攻撃元のIPアドレスを制限することはできません。
※4　a-blog cmsのコアファイルのカスタマイズは基本的にされていないことを前提で作業します。
コアファイルは以下を指します。**バックアップが必要なファイルがありましたら、作業前にお知らせ下さい。本番環境での作業のため、バックアップが無いと作業前に戻せません。**

ファイル/ディレクトリ	内容
`acms.js`	CMS全体に関わるJavaScript（管理画面等）
`index.php`	ルーティングの起点、CMSの入口
`js/`	共通JS（管理画面など）
`lang/`	多言語ファイル
`php/`	CMS本体の処理
`private/config.system.default.yaml`	デフォルト設定ファイル
`themes/system/`	システムテーマ（管理画面など）

作業手順に関して

作業は全て、パッチバージョンのみ脆弱性に対応したバージョンまでオンラインアップデート（以下URLでのアップデート方法）をいたします。
▼オンラインアップデートについて
https://developer.a-blogcms.jp/document/update/online-update.html

以下の手順で進行します。

1. アップデート前のドメインを応急処置する
    - FTP情報、a-blog cmsログイン情報を頂き次第、応急処置として作業内容に関してに示しました「**a-blog cmsの脆弱性対応**」を行います。
2. アップデートが可能なドメインから、順次作業内容に関してに示しました「**a-blog cmsのアップデート**」を実施します。
    - オンラインアップデート後、作業内容に関してに示しました「**a-blog cmsの脆弱性対応**」を行います。
3. アップデート作業完了後、川﨑の方で不審ファイル削除。**貴社にて不審ファイルを削除をお願いいたします（削除の承諾得た）。**
4. アップデート完了画面スクショを[redacted]さまへ送信。

作業時にトラブルや疑問点が発生し、開発元に質問をする際は、貴社のa-blog cmsビジネスパートナー権限の、Discordまたは、脆弱性に関しての問い合わせ先のメールにて、間接的に質問対応いただきます。