GMO CLOUD

# GMO サイバー攻撃
# ネット de 診断 ASM ガイド

GMO グローバルサイン・ホールディングス株式会社

© 2025 GMO GlobalSign Holdings K.K. All Rights Reserved.

GMO CLOUD

# 内容



© 2025 GMO GlobalSign Holdings K.K. All Rights Reserved.

## 1. はじめに

本ガイドでは、ＧＭＯサイバー攻撃ネットde診断ASMをご利用すいただく際に必要となる、お手続きや操作方法についてご案内いたします。

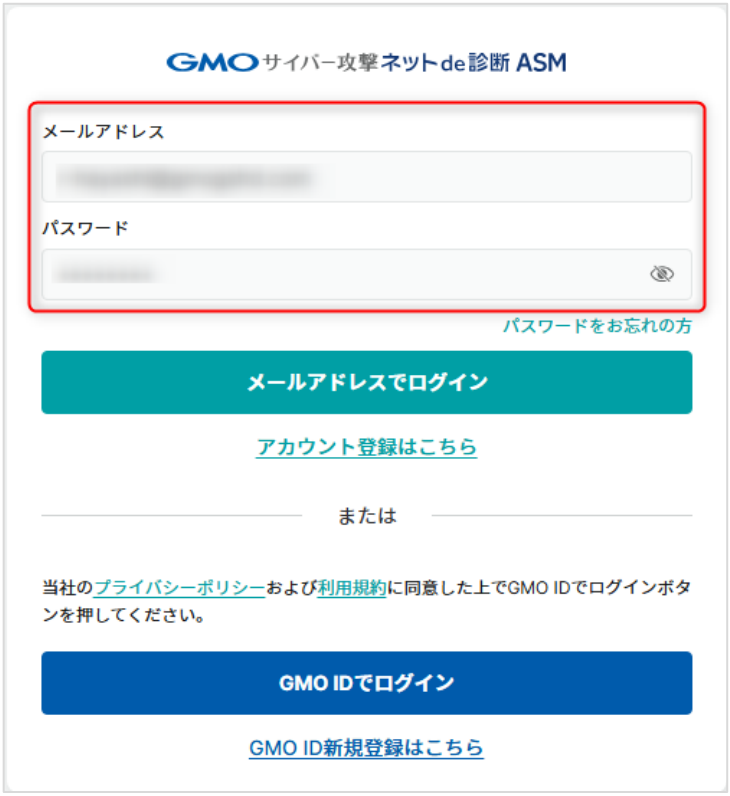
## 2. アカウント有効化

ネットde診断ASMのご契約が完了すると、 下記のようなメールが届きますので、

メール本文の最下部の**「ネットde診断をはじめる」**をクリックしてください。※ログイン画面へ移動します。

## 3. ログイン方法

ログイン画面(https://shindan.gmo-cybersecurity.com/)に、**メールアドレス**と前項の「アカウント有効化」で
ご確認いただいた**パスワード**を入力し、**「メールアドレスでログイン」**ボタンをクリックしてください。




## 4. 診断

診断方法は、下記の２つからお選びいただけます。

| 簡易診断（10 分程度） | 詳細診断（15 分程度） |
|---|---|
| **サーバーあるいは Web サイトに対する通常アクセス時に発生する通信のみ診断します。（不正アクセス禁止法に抵触しない範囲）**<br><br>**一部を対象としたポートスキャンやサービスに対する通常利用の範囲で基本的な設定やバージョン情報の取得を実施します。** | **簡易診断に加え、より高度なサイバー攻撃を想定する脆弱性を利用した通信を発生させる。**<br>**※WAF などを導入している場合、アラートが発報する可能性有り**<br><br>**現時点では過去診断(実績: 15 万件以上)によるサービスやホストのダウンは報告無し。** |

## 5. 詳細診断の注意事項

以下のようなケースにおいて、意図しないメールやコメント、その他通知等が発生する可能性がございますので、診断前に Web サイトの管理者様にその旨をご案内ください。

但し、脆弱性診断を実施する際に時折発生する事象であり、情報漏洩や Web サイトの改ざんなどのインシデント（重大な事故）につながるわけではありません。

ご心配な場合、簡易診断モードにて診断いただくか、一度弊社担当者までご相談ください。

| # | Web サイトの特徴 | 想定される影響 |
|---|---|---|
| 1 | 問合せフォームが存在 | フォームの送信や送信エラーに対する通知の発生 |
| 2 | ブログ記事へのコメントが投稿可能 | コメント投稿時の通知、スパム検出機能による警告の発生 |
| 3 | ユーザー登録やログイン機能が存在 | 新規登録や不正ログイン試行による通知の発生 |
| 4 | 管理者用ページが存在 | 認証失敗や不正アクセス試行による通知の発生 |
| 5 | サーバーのリソース監視や異常検知が行われている | 一定の負荷やアクセスの検出に対する通知の発生 |

## 6. 診断結果

ドメイングループ一覧 >> グループ名 をクリックすると、グループ全体の脆弱性の評価がご確認いただけます。


A~E は、総合評価を表します。

A = 診断対象範囲内に脆弱性が発見されていない状態

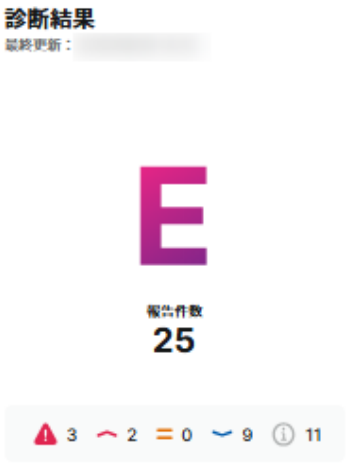
B = リスクレベル低の脆弱性が存在する状態
対応の要否をご確認ください

C = リスクレベル中の脆弱性が存在する状態
対策実施を推奨します

D = リスクレベル高の脆弱性が存在する状態
個人情報等の漏洩、改ざん等の現実的なおそれがあります

E = リスクレベル緊急の脆弱性が存在する状態
速やかな対処を強く推奨します

ドメイン名をクリックすると、ドメインごとの評価と、検出された脆弱性の詳細がご確認可能です




このマークはリスクレベルを表記しています。


中～緊急の対応が必要と判断

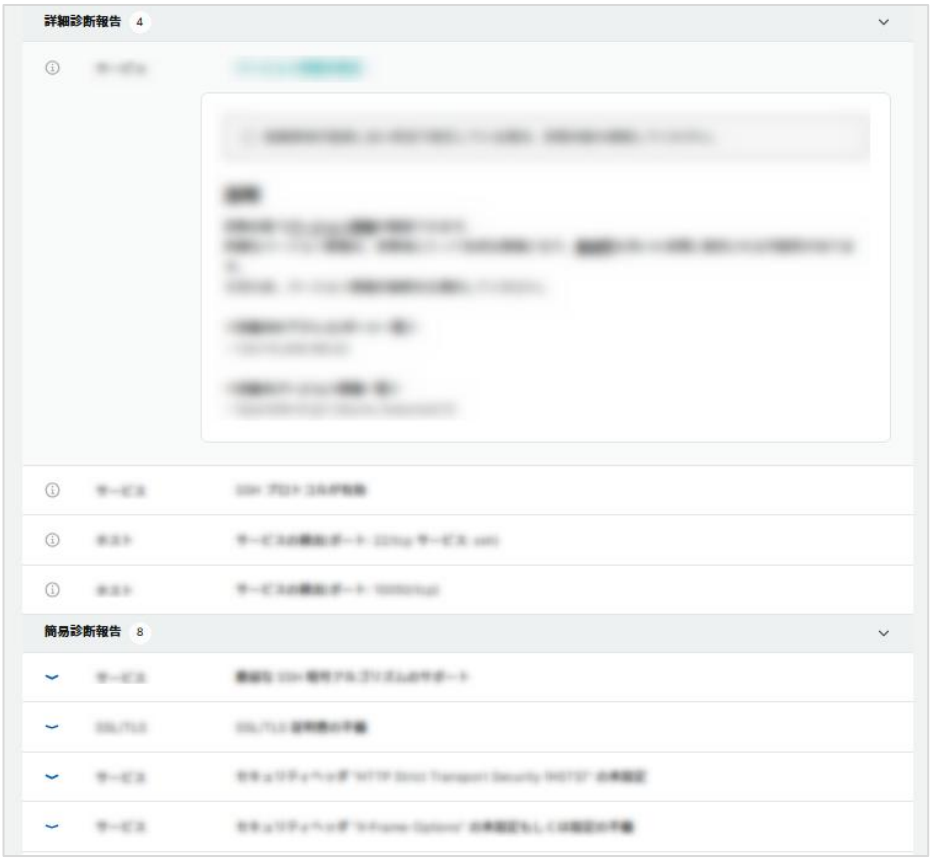
| 【評価基準】 | |
|---|---|
| 「info」のみ検出されている | A評価 |
| 「low」がある | B評価 |
| 「medium」がある | C評価 |
| 「high」がある | D評価 |
| 「critical」がある | E評価 |

結果画面の下部では、脆弱性の詳細がご確認いただけます。

・脆弱性の内容

・想定される影響

・対策方法



## 7. よく検出される脆弱性

| 診断項目種別 | 診断項目 | リスクレベル |
|---|---|---|
| **SSL/TLS** | 古い OpenSSL における情報漏洩の脆弱性 | 緊急 |
| **OS** | サポートの終了した OS の利用 | 高 |
| **OS** | サポートの終了したソフトウェアの利用 | 高 |
| **サービス** | データベースバックアップのディレクトリリスティングが可能 | 高 |
| **サービス** | 公開されるべきでない情報を閲覧可能（Wordpress 設定ファイル,データベース,システム設定情報,ソースコード等） | 高 |
| **サービス** | ログイン情報が平文で送信される<br>Telnet プロトコルが有効になっている | 中 |