2025 年 5 月 23 日

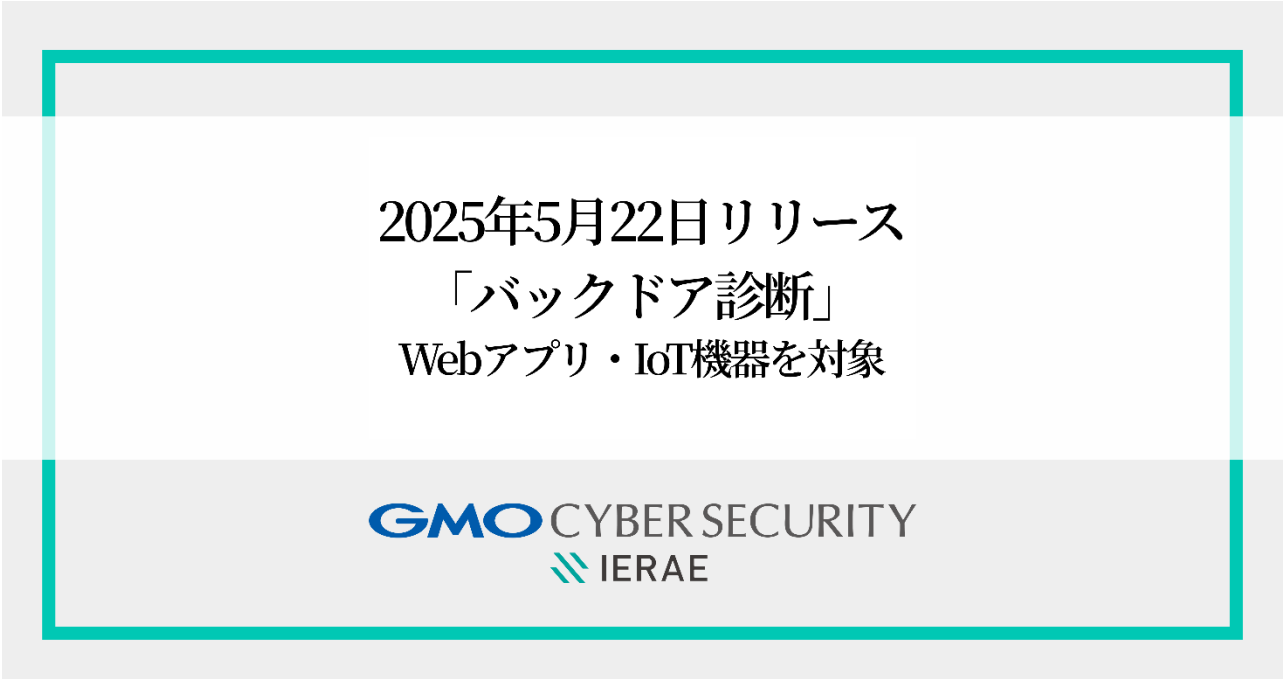
報道関係各位

GMO サイバーセキュリティ by イエラエ株式会社

GMO サイバーセキュリティ by イエラエ、ペネトレーションテストの新オプション「バックドア診断」をリリース

～ホワイトハッカーが Web アプリケーションや IoT 機器を対象に“悪意のあるコード”が混入をしていないかチェック～

GMO インターネットグループでサイバー攻撃対策事業を展開する GMO サイバーセキュリティ by イエラエ株式会社（代表取締役 CEO：牧田 誠　以下、GMO サイバーセキュリティ by イエラエ）は、2025 年 5 月 22 日（木）、ペネトレーションテスト（※1）のオプションサービスとして、Web アプリケーションや IoT 機器を対象に“悪意のあるコード”が混入していないかホワイトハッカーがチェックする「バックドア（※2）診断」の提供を開始しました。



（※1）システムやネットワークの脆弱性を確認するために、ホワイトハッカーが実際に攻撃を試みるテスト

（※2）ソフトウェアやハードウェアに意図的または不正に組み込まれた、外部からの不正アクセスを可能にする手段

【バックドア脅威と調査ニーズの高まり】

近年のサイバー攻撃動向としてサプライチェーンを悪用した侵入手口が増加しています。IPA が発表した「情報セキュリティ 10 大脅威 2024」では、「サプライチェーンの弱点を悪用した攻撃」が組織分野の第 2 位にランクインしています。実際に、取引先から導入したソフトウェアの脆弱性を悪用され、バックドア型マルウェアを埋め込まれたケースが確認されています。このような事例を踏まえ、システム内部に仕掛けられた「バックドア」への関心・調査ニーズが高まっています。

2022 年 5 月に成立した「経済安全保障推進法」に関連して、2023 年 4 月には「基幹インフラ役務の安定的な提供の確保」に関する基本指針が閣議決定され、2024 年 5 月に制度の運用が開始されました。

「基幹インフラ役務の安定的な提供の確保」の制度においては、基幹インフラ役務を提供する特定社会基盤事業者が特定重要設備の導入や重要な維持管理等を委託しようとする際に、事前に届出を行い・審査を受けるよう定められました。特定社会基盤事業者は届出項目の中で、特定重要設備に悪意のあるコード等が混入していないかを確認する受入検査やその他の検証体制を構築すること、及び脆弱性テストを設備導入前までに実施することなどが求められています。

【ホワイトハッカーの知見を活用したバックドア診断】

GMO サイバーセキュリティ by イエラエではこれまでに培った Web アプリケーションや IoT 機器に対する攻撃者目線のソースコード解析やリバースエンジニアリング、動的解析等のノウハウを活用し、バックドアが設置されていたり悪意のあるコードが混入されたりしていないかをホワイトハッカーが自ら調査します。

GMO サイバーセキュリティ by イエラエがバックドア診断サービスを提供するきっかけは、複数の金融系のお客様から取引先からの納品物の受入テストの一項目として「バックドアの設置有無の調査」をご相談いただいたことでした。なお、お見積もりはソースコードの量や診断工数などの要件により変動するため個別対応となります。

■バックドア診断　診断項目例

バックドア診断でソースコードに基づいた調査を行う場合、以下の観点に沿ってソースコードを確認します。またテスト対象の機器・システムの種類や関連する各種業界規制等に基づいたカスタマイズも承ります。

①　設計・仕様書との乖離確認

診断観点	実施内容
仕様書に存在しない API	仕様書に存在しない API が実装されているかを確認します。
仕様書に存在しないリクエストパラメータ	仕様書に存在しないリクエストパラメータが定義されているかを確認します。
仕様書に存在しない公開サービス	仕様書に存在しないサービスが外部に公開されていないかを確認します。 ソースコード上からポートリッスンしている箇所を確認します。

②　バックドアになり得る処理の有無

診断観点	実施内容
OS コマンド実行や動的コード実行	OS コマンド実行や動的なコード実行（例: eval）を行っている箇所や前後に、不自然な処理内容が存在しないかを確認します。
アウトバウンド通信（通信処理）	通信を行っている箇所や前後に、不自然な処理内容が存在しないかを確認します。
設定値の動的な変更	セキュリティとして重要な値やアプリケーションの設定値等が動的に変更されている箇所の確認およびその設定値の内容を確認します。

③　適切なデータ保護や管理方法の確認

診断観点	実施内容
脆弱な暗号化やハッシュ	脆弱な暗号化アルゴリズムやハッシュアルゴリズムが使用されていないか、また、不適切な利用方法が存在しないかを確認します。
平文通信	平文通信の有無を確認して、中間者攻撃に対して脆弱でないかを確認します。
認証情報や個人情報等のログ出力	認証情報や個人情報等のログ出力が行われていないかを確認します。

④　悪意ある文字列の埋め込みの確認

診断観点	実施内容
意図しない認証情報の埋め込み	ソースコード内に認証情報がハードコードされているかを確認します。
アウトバウンド通信 （外部 FQDN や外部 IP アドレス）	外部通信されうる外部 FQDN や外部 IP アドレスがソースコード内に存在しないかを確認します。
難読化された文字列	Base64 などのエンコードによって、難読化された文字列が存在しないかを確認します。

⑤　脆弱性の有無の確認

診断観点	実施内容
脆弱性の有無の確認	ソースコードを確認し、各観点での脆弱性の調査をします。

■対象サービス

・Web ペネトレーションテスト：https://gmo-cybersecurity.com/service/assessment/pentest/
・IoT ペネトレーションテスト：https://gmo-cybersecurity.com/service/assessment/iot/

サービスについてのお問い合せ先：https://gmo-cybersecurity.com/contact/service/

【今後の展望】

GMO サイバーセキュリティ by イエラエは、経済安全保障の重要性が一層高まる中、オフショア開発やアウトソーシングの拡大に伴い増大するソフトウェアのサプライチェーンリスクへの対応として、各種システムや機器に潜在するバックドアの検出・排除を目的とした診断サービスの提供を開始しました。 国内外のセキュリティコンテストで上位入賞実績を持つホワイトハッカーを中心に、ペネトレーションテストで培ったソースコード解析やリバースエンジニアリングといった高度な技術を駆使し、悪意あるコードや不審な挙動を検出・特定することで、システムの信頼性向上に貢献してまいります。 今後も、グローバルで通用する技術力と知見を元に、各種システムの安全かつ安定した運用や、基幹インフラ役務の安定的な提供を支援し、安心・安全なデジタル社会の実現に向けて尽力してまいります。(サイバーセキュリティ事業本部 高度診断部　部長　白木光達)

【GMO サイバーセキュリティ by イエラエについて】
(https://gmo-cybersecurity.com/)

GMO サイバーセキュリティ by イエラエは、国内最大規模のホワイトハッカーで組織されたサイバーセキュリティのプロフェッショナルカンパニーです。GMO サイバーセキュリティ by イエラエは、「世界一のホワイトハッカーの技術力を身近に」を目指して、各種脆弱性診断、ペネトレーションテスト、セキュリティ

コンサルタント、SOC サービス、フォレンジック調査まで包括的にサイバーセキュリティ対策サービスをご提供します。

以上

【報道関係お問い合わせ先】

●GMO サイバーセキュリティ by イエラエ株式会社
マーケティング部　広報担当　伊礼
TEL：03-6276-6045
E-mail：pr@gmo-cybersecurity.com

●GMO インターネットグループ株式会社
グループ広報部　PR チーム　田部井
TEL：03-5456-2695
お問い合わせ：https://www.group.gmo/contact/press-inquiries/

【GMO サイバーセキュリティ by イエラエ株式会社】（URL：https://gmo-cybersecurity.com/）

会　社　名	GMO サイバーセキュリティ by イエラエ株式会社
所　在　地	東京都渋谷区桜丘町 26 番 1 号　セルリアンタワー
代　表　者	代表取締役 CEO　牧田　誠
事 業 内 容	■Web アプリ及びスマホアプリ脆弱性診断　■ペネトレーションテスト ■不正利用(チート)診断　■IoT 脆弱性診断　■自動車脆弱性診断 ■フォレンジック調査　■CSIRT 支援　■クラウドセキュリティ診断 ■クラウドセキュリティ・アドバイザリー
資　本　金	1 億円

【GMO インターネットグループ株式会社】（URL：https://www.group.gmo/ ）

会　社　名	GMO インターネットグループ株式会社　（東証プライム市場　証券コード：9449）
所　在　地	東京都渋谷区桜丘町 26 番 1 号　セルリアンタワー
代　表　者	代表取締役グループ代表　熊谷　正寿
事 業 内 容	持株会社（グループ経営機能） ■グループの事業内容 インターネットインフラ事業 インターネットセキュリティ事業 インターネット広告・メディア事業 インターネット金融事業 暗号資産事業
資　本　金	50 億円