その「不安」を「安心」に

～ Security Blanket with You ～

モバイルアプリケーション診断サービス

株式会社M&K

【Ver2604】

その「不安」を「安心」に

M&Kは単なるセキュリティ診断会社ではありません。

お客様の不安を解消し、セキュリティ対策の「見える化」を
お手伝いする「おせっかいな集団」。

お客様のビジネスにポジティブな影響を与える
システムアドバイザーでありたい。

～　Security Blanket with you　～

SECURITY BLANKET

それが、私たちM&Kの想いです。

会社概要

株式会社M&K

本社所在地	東京都渋谷区広尾1-11-2 BLOCKS EBISU 3F
名古屋支店	愛知県名古屋市中区錦1丁目4-27 ジェムストーン錦ビル 4-B
設立年月日	2007 年 4 月
役員	代表取締役　　小西　正記
U R L	https://www.m-kcompany.co.jp/
認証資格	ISO/IEC 27001:2022(ISMS)

経済産業省
情報セキュリティ監査企業台帳登録
情報セキュリティサービス基準審査登録
「Security Blanket」
サービス登録番号：019-0016-20

一般競争参加資格（全省庁統一資格）

取引社数
5,000社
以上

年間
500サイト
の診断実績

豊富な経験と確かな技術力で お客様の「安心・安全」をご支援します。

安心・安全なIT環境作りをお手伝いするM&Kのサービス群

■セキュリティコンサルティングサービス

- IT環境アセスメントサービス
- 情報セキュリティマネジメントシステム構築支援
- ISMS認証取得支援／Pマーク認証取得支援
- システムアドバイザリーサービス

■セキュリティ診断サービス

- クラウド環境設定診断
- WEBアプリケーション診断
- システムプラットフォーム診断
- モバイルアプリケーション診断
- ソースコード診断
- ペネトレーションテスト

■インテグレーションサービス

- クラウドインテグレーション
- セキュアコーディング支援
- WAF導入支援
- WEBサイト改ざん検知導入支援
- NGAV製品導入支援

■教育支援サービス

- 標的型メール攻撃訓練サービス
- セキュリティ講習サービス
- Eラーニング環境構築
- コンテンツ作成代行

ー　M&Kが選ばれる理由　ー

POINT 1

診断事業者として15年以上の実績

セキュリティ診断に関する高い技術力とノウハウを保有しており、大手セキュリティ事業者との技術協業も行っています。

POINT 2

自動診断ツールを自社開発

診断事業者としての経験とノウハウを詰め込んだ自動診断ツールを開発
自社製品の為、即時性の高いカスタマイズ・アップデートが可能です。
国内自社開発なので、診断結果レポートの読みやすさもご評価いただいております。

POINT 3

自動診断ツールをSaaS型で提供

自社開発の自動診断ツールをSaaS型で提供しています。
お客様側での新たな設備投資や自前での機器保有を必要とせず、安価で手軽な費用対効果の高いセキュリティ診断が定期的に実施可能です。

POINT 4

ビジネスパートナーへの提供実績

経験豊富なエンジニアのきめ細やかで信頼性の高いサービス提供により、複数のビジネスパートナー様にご評価頂いております。

モバイルアプリケーション診断サービス

Security Blanket シリーズ

SECURITY BLANKET

ー　脆弱性診断サービス　Security Blanket シリーズ　ー

「脆弱性」とは、WEBアプリケーションやOS／ミドルウェア、ネットワーク等のシステムプラットフォームに潜在するセキュリティ上の弱点や欠陥のことです。

これらの脆弱性を悪用すると、外部の第三者がシステムに侵入できたり、本来は閲覧できないはずの重要な情報を見る事ができてしまったりという事が起こり得ます。

「脆弱性診断」とは、このような被害を未然に防ぐ為に**システムに潜在する脆弱性の有無を診断し、リスクの可視化、必要な対策の洗い出し**を目的に実施します。

M&Kでは、専門エンジニアによる手動診断および、SaaS型ツール診断による脆弱性診断サービスをご提供します。
お客様のWebサイトに対し、攻撃者の視点から様々な疑似攻撃を考察・試行することで、**安心・安全なIT環境の運用**をご支援します。

セキュリティ診断サービス提供内容例

WEBアプリケーション／モバイルアプリケーション診断

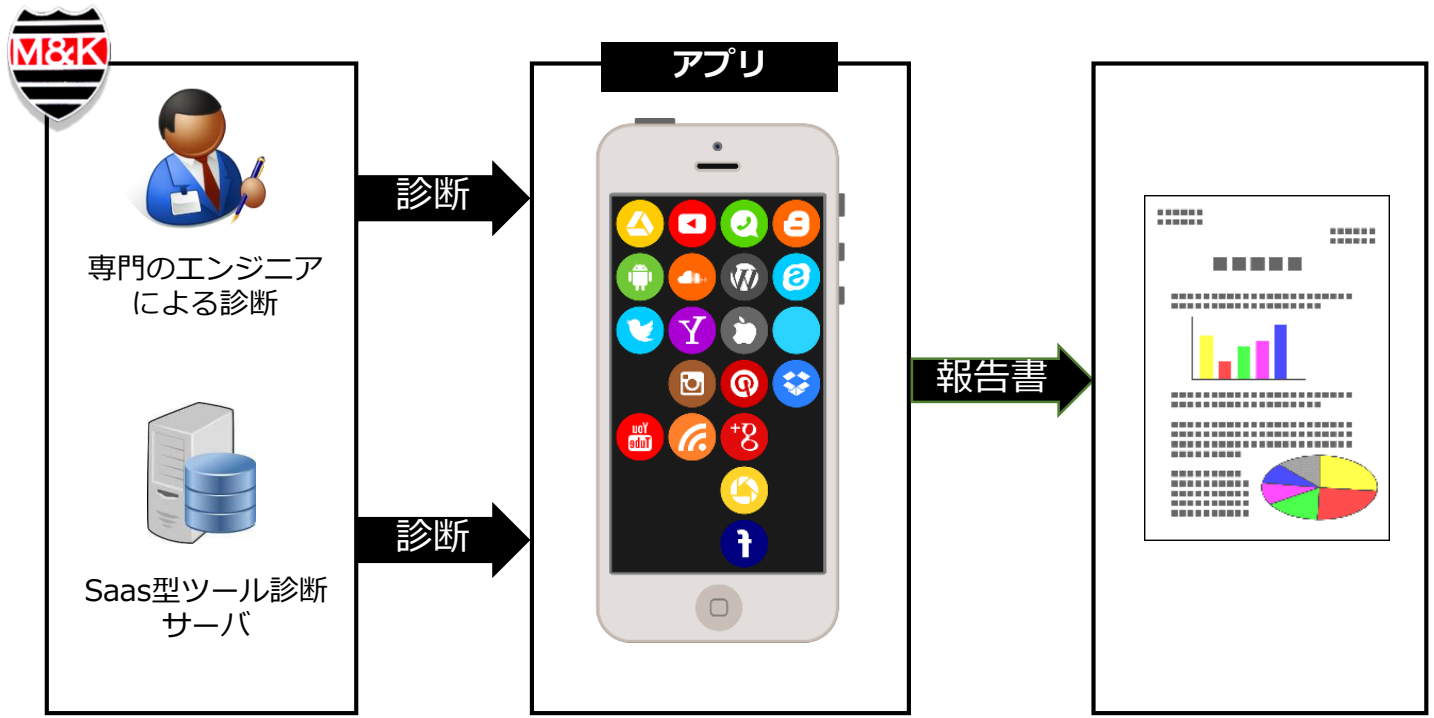
SaaS型のツール診断と、セキュリティエンジニアがサイトの仕様を把握しながら、各種セキュリティカテゴリに対して診断を実施する手動診断をご提供します。
診断対象や予算に応じて柔軟に対応可能です。

システムプラットフォーム診断

外部に公開しているシステムのネットワークや内部のネットワークに対し、OS、ミドルウェア等のプラットフォームに関するセキュリティ上の問題点を可視化します。

モバイルアプリケーション診断

iOS／Androidで作成されたモバイルアプリケーションに潜むセキュリティ上の問題点を可視化します。ネイティブアプリも対応可能です。



・モバイルアプリのソースコード一式をお預かりし、専門のエンジニアがソースコードにおけるセキュリティ上の問題点や潜在的に潜むリスクを、ツール診断およびエミュレータ等を利用した動的検査で可視化します

・検出された問題点の概要と箇所、推奨する対策方法をまとめた報告書を提示します

・「OWASP Mobile Security Testing Guide」、「OWASP Mobile Application Security Verification Standard」に準拠した診断を提供します

Pro

※近日リリース予定

専門の診断エンジニアによる手動診断を提供します。
新規アプリの公開前など、全体をしっかりと診断したい時や、重要な情報を保有するシステム等におすすめです。
API診断やサーバサイド側の診断との組み合わせも可能です。

Standard

ツールによる診断を提供します。
手軽に安価に診断を実施したい時や、年間を通して定期的に診断を実施したい場合などにおすすめです。

ー　Security Blanket シリーズ　サービスラインナップ　ー

診断対象	サービス名称		概要
モバイルアプリケーション	Security Blanket for Mobile	Pro	エンジニアによる手動診断
		Advance	エンジニアによる手動診断　＋　ツール診断
		Standard	ツール診断のみ

診断対象	サービス名称		概要
API	Security Blanket	Pro	エンジニアによる手動診断

診断対象	サービス名称		概要
共通	オプション	報告会	診断後の報告会実施（診断結果報告＆対策アドバイス）

ー　診断レベル　ー

診断メニュー	診断基準
ツール診断	「OWASP Mobile Security Testing Guide」に基づきツールでの診断が可能な項目のみ
L1診断	「OWASP Mobile Application Security Verification Standard L1」に準拠した診断
L2診断	「OWASP Mobile Application Security Verification Standard L2」に準拠した診断
リバースエンジニアリング診断	「OWASP Mobile Application Security Verification Standard R」に準拠した診断

ー　診断レベルについて　ー

■OWASP Mobile Application Security Verification Standard（MASVS）

・MASVS-L1：標準的セキュリティ

基本的な要件を満たし、一般的な脆弱性の被害を受けない事を評価する基準であり、すべてのモバイルアプリケーション向けのベストプラクティス

・MASVS-L2：多重防御

標準要件を超える高度なセキュリティ制御にて、より巧妙な攻撃への耐性があるということ評価する基準であり、モバイルバンキングなどの機密データを扱うアプリケーション等に最適

・MASVS-R：リバースエンジニアリングと改ざんに対する耐性

最先端のセキュリティ策が実装されており、機密コードやデータを抜き出すための改ざん、改造、リバースエンジニアリングなどのクライアント側の攻撃への耐性があることを評価する基準
機密性が非常に高いデータや知的財産の保護、アプリの改ざん防止の手段として有効

■OWASP Mobile Security Testing Guide（MSTG）

モバイルアプリのセキュリティ診断を実施するためのマニュアルであり、MASVSに記載されている要件を検証するための技術プロセスに関する説明書

ー　診断レポート評価基準　ー

国際的な脆弱性評価基準CVSS、CVE、PCIDSS、OWASP Top 10等のガイドラインを基にした弊社独自の基準にて評価します。

※CVSS(Common Vulnerability Scoring System)：コンピュータ・セキュリティ非営利団体が推進する脆弱性評価システム
※CVE(Common Vulnerabilities and Exposures)：セキュリティに関わる事象、用語等を標準化し辞書を作成するプロジェクト
※PCIDSS（Payment Card Industry Data Security Standard）：会員データを安全に取り扱うことを目的として策定されたクレジットカード業界の国際セキュリティ基準
※OWASP TOP10（Open Web Application Security Project）：OWASPが定期的に発行するWebセキュリティとして警戒をしなければいけない項目のTOP10

危険度レベル	
緊急	パスワード漏えい、管理者権限昇格など、システム全体に影響する問題です。これらの問題が発生する可能性が極めて高く、即日対応する必要があります。
重大	情報漏洩や、なりすましなど、ユーザ被害が発生する可能性が高い問題です。 このレベルには、クロスサイトスクリプティングやSQLインジェクションなどの問題があり、インシデント報告やOWASP TOP10などで上位を占めるセキュリティ上の問題です。このことから、早急に対応する必要があります。
高	総当たり攻撃や認証回避など、セキュリティ上の問題が発生する可能性があります。 システムの仕様などにより、セキュリティ上必要な対策が実施されていない場合このレベルに分類されます。問題が発生する可能性があるため、対応を必ず行うことを推奨します。
中	システムの設定情報や管理情報の漏洩等、システムに対する攻撃手段を提供する可能性がある問題です。 直接被害が発生する可能性は高くないですが、他のセキュリティ上の問題と組み合わさるとレベルが上がる可能性があります。 問題になる可能性があるため対策を検討してください。
低	バージョン情報表示や、バナー情報表示など、攻撃者の興味を引く可能性のある問題です。 直接悪用されるよりは、このレベルの情報から攻撃手法を絞っていくことがあります。 予防するうえで対策を検討してください。
情報	品質やセキュリティのさらなる向上のために弊社が推奨する項目です。

ー　主な診断項目例　ー

※詳細は別紙の診断項目一覧にてご確認ください。

	診断項目
データ・ストレージの保護	ローカルストレージ
	デバイスアクセスポリシー
	メモリ
	サードパーティ
	ログ
	キーボード
	バックアップ
	機密データ利用目的への説明
暗号化	暗号化標準アルゴリズムの構成の検証
	乱数生成
	対称暗号化
	キーの目的/管理
認証・認可	認証のテストに関する一般的なガイドライン（モバイルアプリ側）
	ステートフル認証とステートレス認証（モバイルアプリ側）
	OAuth 2.0（モバイルアプリ側）
	ユーザーのログアウト（モバイルアプリ側）
	補助認証（モバイルアプリ側）
	二要素認証（モバイルアプリ側）
	ログインアクティビティとデバイスのブロック（モバイルアプリ側）
	資格情報の確認
	生体認証
	ローカル認証
ネットワーク通信	ネットワークトラフィックの保護
	エンドポイント識別検証
	SSL/TLSを適用
	ネットワーク上のデータ暗号化
	証明書ストアと証明書の固定
	セキュリティプロバイダーの更新
	IPアドレスの開示

概要	診断項目
プラットフォーム（OS）	IPCメカニズム（機能）
	ディープリンク
	ユニバーサルリンク
	カスタムURLスキーム
	アプリの権限
	IPC メカニズム（ストレージ）
	クリップボード
	ペンディングインテント
	アプリ拡張機能
	UIアクティビティ共有
	WebViewクリーンアップ
	WebViewを通じて公開されるJavaオブジェクト
	WebViewでのJavaScript実行
	WebViewプロトコルハンドラー
	iOS WebView
	WebViewのネイティブメソッド
	ユーザーインターフェイスを介した機密データの漏洩
	オーバーレイ攻撃対策
	自動生成されたスクリーンショット内の機密情報の検索
クライアントコードの品質	アプリ内更新
	脆弱なサードパーティライブラリ
	ローカルストレージの入力検証
	オブジェクトの永続性
	インジェクションの欠陥の検査
	暗黙的なインテント
	バイナリセキュリティ機能
	WebViewでのURL読み込み
	メモリリーク

概要	診断項目
リバースエンジニアリング	ルート化・脱獄の検知
	シミュレータ・エミュレータの検知
	アプリの署名
	ファイル完全性
	ランタイム完全性
	デバッグシンボルの削除
	難読化
	コードのデバッグとエラーログ
	リバースエンジニアリング ツールとフレームワーク検知
	リバースエンジニアリング ツールとフレームワーク検知
	アンチデバッグ検出
	デバッグ制限

ー　サービス提供条件　ー

モバイルアプリケーション診断

・診断時間　　：原則、平日10:00~18:00での対応となります。
（作業の進捗により左記時間外も実施する場合があります。）
・報告書提出日　：診断完了後、3営業日以内に診断結果をまとめた報告書を提出いたします。
・診断速報報告書：手動診断において、5段階の危険度レベルのうち上位2段階(緊急・重大)に該当する問題が検出された場合には、診断の完了を待たず、該当の問題に対する診断速報報告書をご提供致します。
・診断手法　　：ソースコード、IPA／AKPファイル等をご提示頂き、ツールによる静的解析、およびエミュレータ等を利用した動的解析、エンジニアによるリバースエンジニアリング等を実施します。
・留意事項　　：ツール診断の場合、難読化されたファイルのみでの診断は実施出来ません。
必ずソースコードのご提示をお願い致します。

API診断

・診断時間　　：原則、平日10:00~18:00での対応となります。
（作業の進捗により左記時間外も実施する場合があります。）
・報告書提出日　：診断完了後、3営業日以内に診断結果をまとめた報告書を提出いたします。
・診断速報報告書：手動診断において、5段階の危険度レベルのうち上位2段階(緊急・重大)に該当する問題が検出された場合には、診断の完了を待たず、該当の問題に対する診断速報報告書をご提供致します。
・秒間アクセス数：手動診断の場合は10アクセス/秒。ツール診断の場合は30アクセス/秒が基本となります。（調整可能）
・留意点　　：サーバサイド側へのアクセスが発生致しますので、当社診断環境からのアクセス許可を頂く必要があります。

ー　価格表　ー

サービス	診断レベル	診断種別	回数	サービス内容	価格	
Security blanket for Mobile	Stanndard	ツール	1回	1アプリケーション／1ロール		¥330,000
	Pro-L1（MASVS-L1）	手動		1アプリケーション／1ロール ※基本料金に10画面までの診断含む	基本料金	¥1,100,000
					追加料金 ※1画面あたり	¥100,000
	Pro-L2（MASVS-L2）	手動			基本料金	¥1,650,000
					追加料金 ※1画面あたり	¥150,000
	Pro-R（MASVS-R）	手動			基本料金	¥1,100,000
					追加料金 ※1画面あたり	¥100,000

サービス	診断レベル	診断種別	回数	サービス内容	価格
Security blanket	API	ツール＋手動	1回	1API／1ロール	個別見積

サービス	診断レベル	診断種別	回数	サービス内容	価格
報告会	–	–	1回	お客様先での報告会	¥100,000

※1　手動診断を併用するL1以上の診断に関しては、画面数・遷移数等により価格が変動致します。
※2　アカウント、ロール等が複数存在する場合は、数量分の費用が必要です。
※3　API診断のみの場合には、別途基本料金（Webアプリ診断に準ずる）を申し受けます。
※4　表記の価格はすべて税抜きです。

～ Security Blanket with you ～

株式会社M&K

https://www.m-kcompany.co.jp/

本社　　：東京都渋谷区広尾1-11-2
BLOCKS EBISU 3F

名古屋支店：愛知県名古屋市中区錦1丁目4-27
ジェムストーン錦ビル 4-B