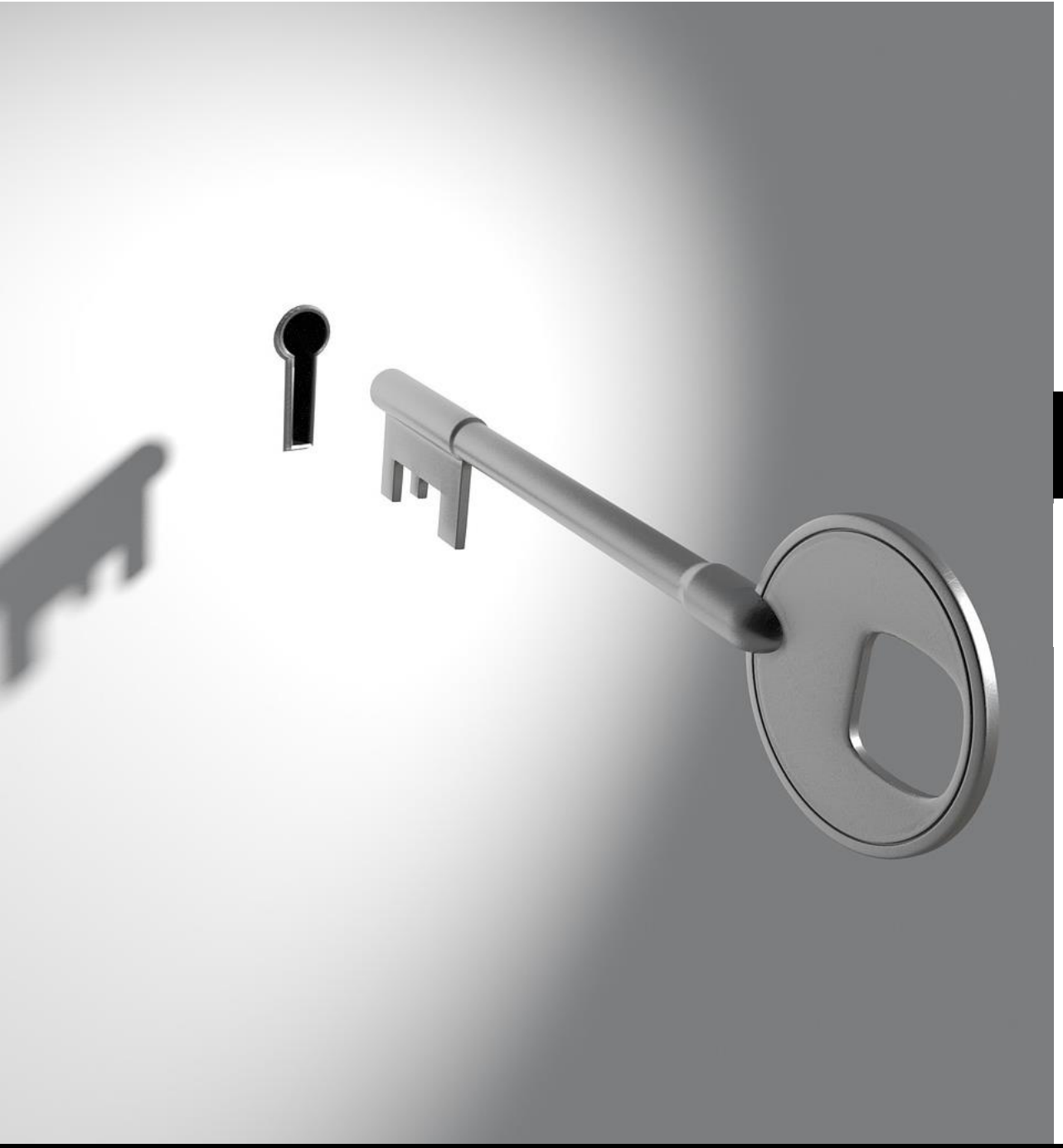
【Ver2308】



その「不安」を「安心」に
～ Security Blanket with You ～

脆弱性診断サービスのご紹介

Security Blanket

株式会社M&K

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」。

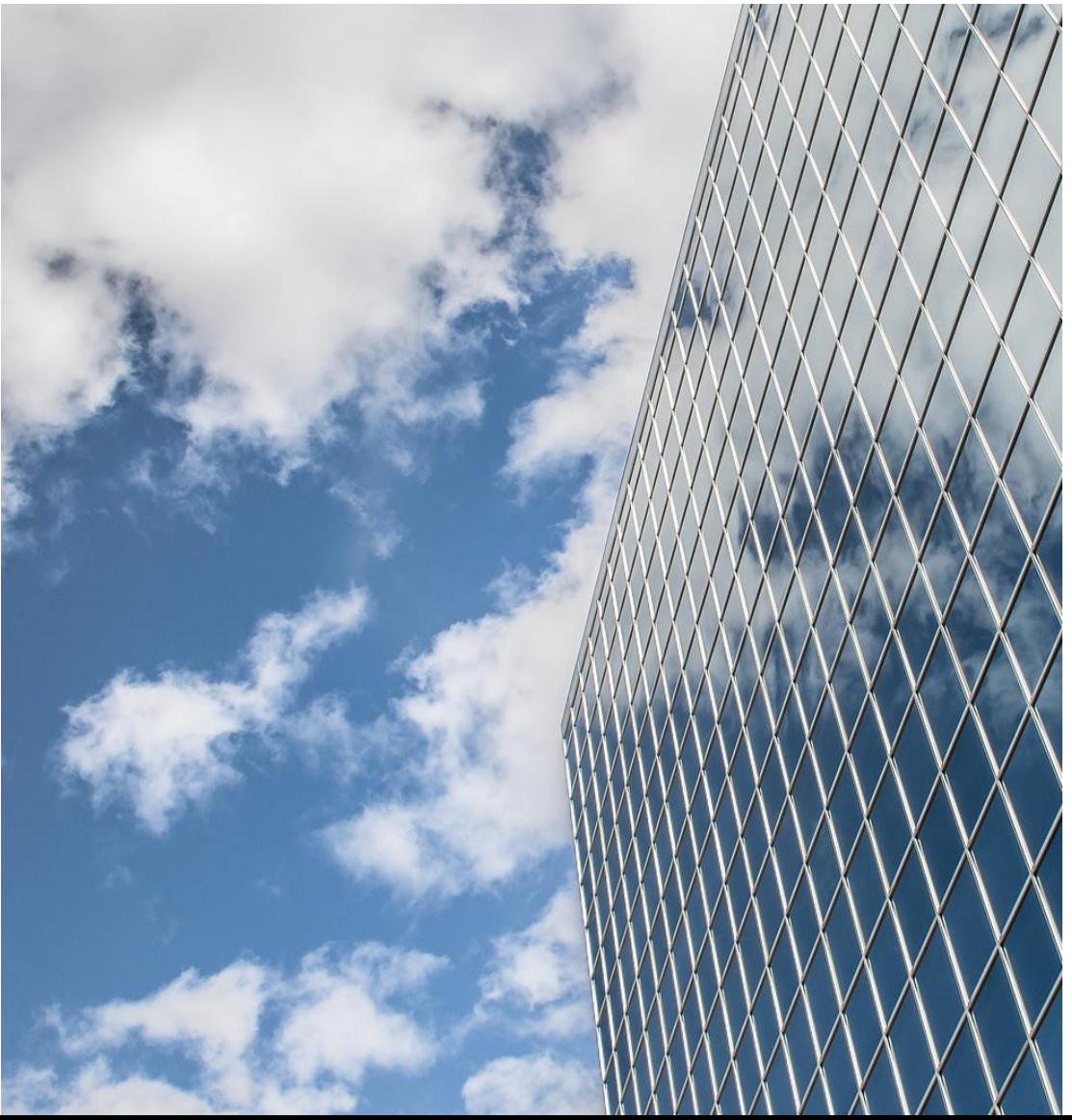
お客様のビジネスにポジティブな影響を与える
システムアドバイザーでありたい。

～　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

所在地	東京本社	：東京都渋谷区神南1-11-3 PORTAL POINT SHIBUYA 505
	名古屋支店	：愛知県名古屋市中区錦1-5-10 名古屋伊藤忠ビル4F
URL	https://www.m-kcompany.co.jp/	
設立	2007年 4月 5日	
事業内容	セキュリティコンサルティングサービス セキュリティ診断サービス インテグレーションサービス 教育支援サービス	
取得認証	ISO/IEC 27001:2013(ISMS) 一般労働者派遣事業 認定番号：般 13-306487 経済産業省 情報セキュリティ監査企業台帳登録	

✓ 取引社数 **5,000社** 以上

✓ 年間 **500サイト** 以上のセキュリティ診断実績

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

■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。

脆弱性診断サービス

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。

Security Blanket

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

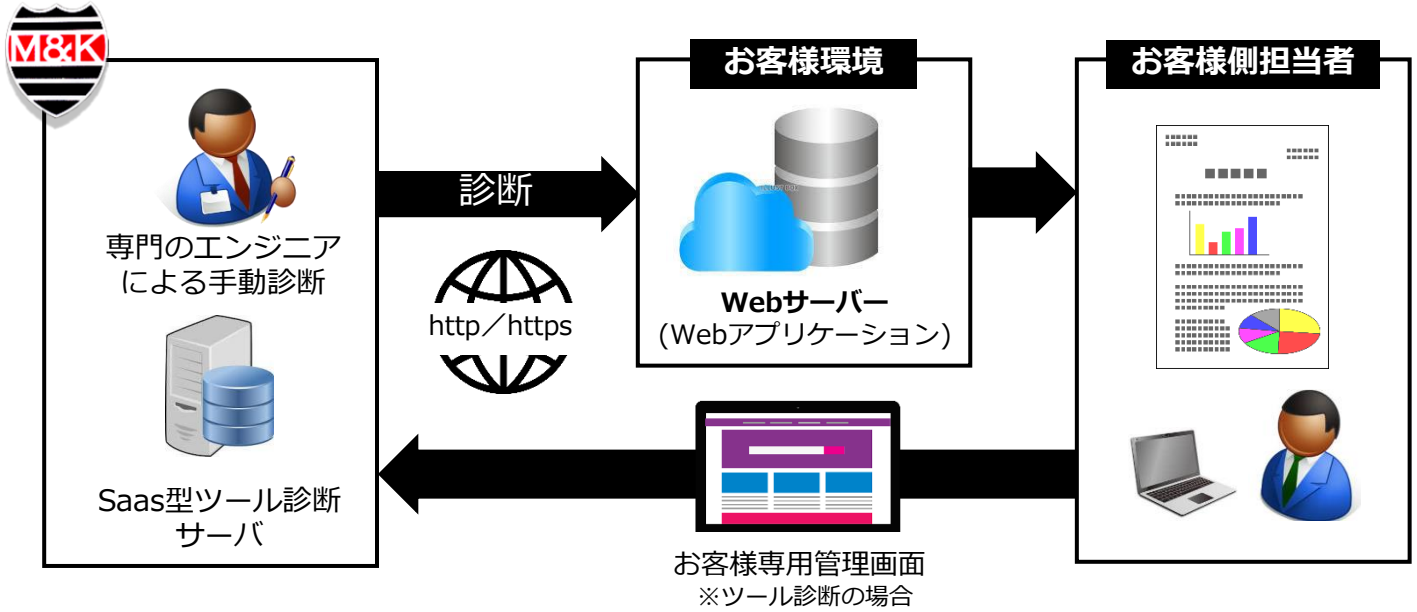
SaaS型のツール診断と、セキュリティエンジニアがサイトの仕様を把握しながら、各種セキュリティカテゴリに対して診断を実施する手動診断をご提供します。
診断対象や予算に応じて柔軟に対応可能です。

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。

WEB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。



- インターネット経由にて診断を実施します
- お客様側での新たな投資や設備のご用意は不要です
- 読みやすい日本語のレポートにて、WEBアプリケーションに潜在する脆弱性を可視化し、セキュリティレベルの向上に必要な対策を提示します
- エンジニアよる手動診断とツール診断を柔軟に組み合わせ、診断対象の規模や特性に合わせた費用対効果の高い診断が可能です

Pro

専門の診断エンジニアによる手動診断を提供します。
新規システムの公開前など、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。

Advance

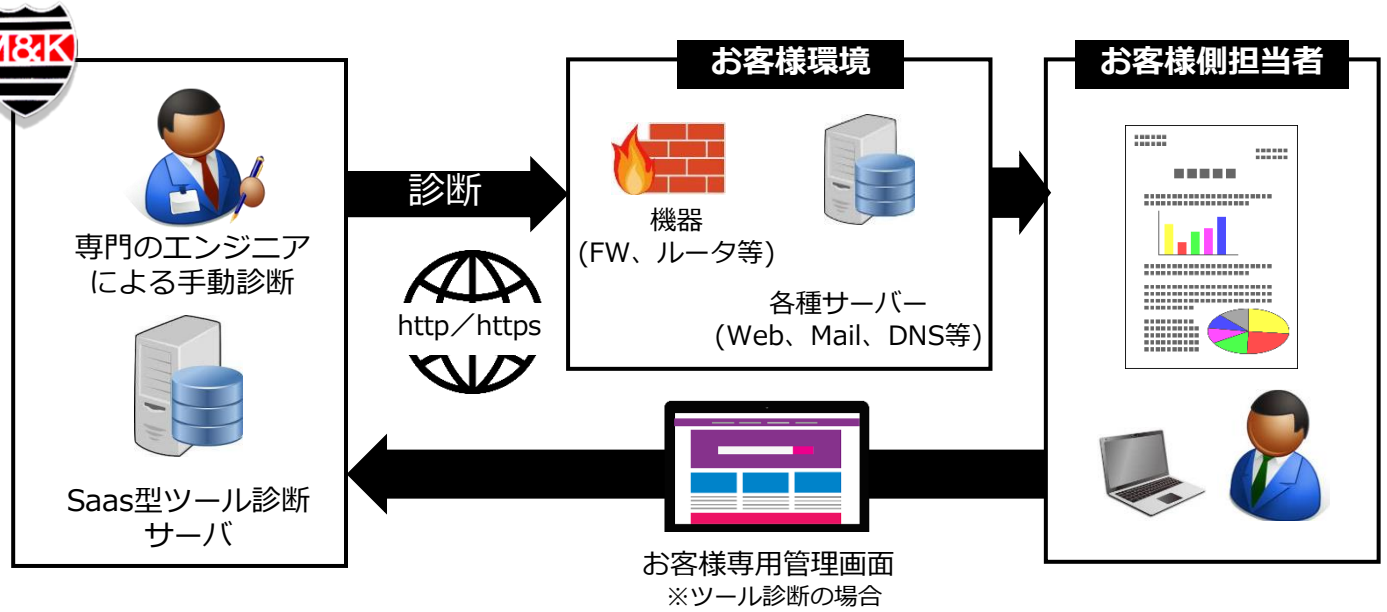
サイト全体はツールで安価に診断し、重要な機能だけはエンジニアによる高度な診断を実施したい時など、手動診断とツール診断を組み合わせた最適な診断方法と提供します。

Standard／365

SaaS型の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システムがある場合におすすめです。

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。



- インターネット経由にて診断を実施します
- お客様側での新たな投資や設備のご用意は不要です
- 日々新たな脅威が報告されるOS、ミドルウェアに関する脆弱性を読みやすい日本語のレポートで確認できます
- エンジニアよる手動診断とツール診断を柔軟に組み合わせ、診断対象の規模や特性に合わせた費用対効果の高い診断が可能です

Pro

専門の診断エンジニアによる手動診断を提供します。
新規システムの公開前など、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。

Advance

サイト全体はツールで安価に診断し、重要な機能だけはエンジニアによる高度な診断を実施したい時など、手動診断とツール診断を組み合わせた最適な診断方法と提供します。

Standard／365

SaaS型の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システムがある場合におすすめです。

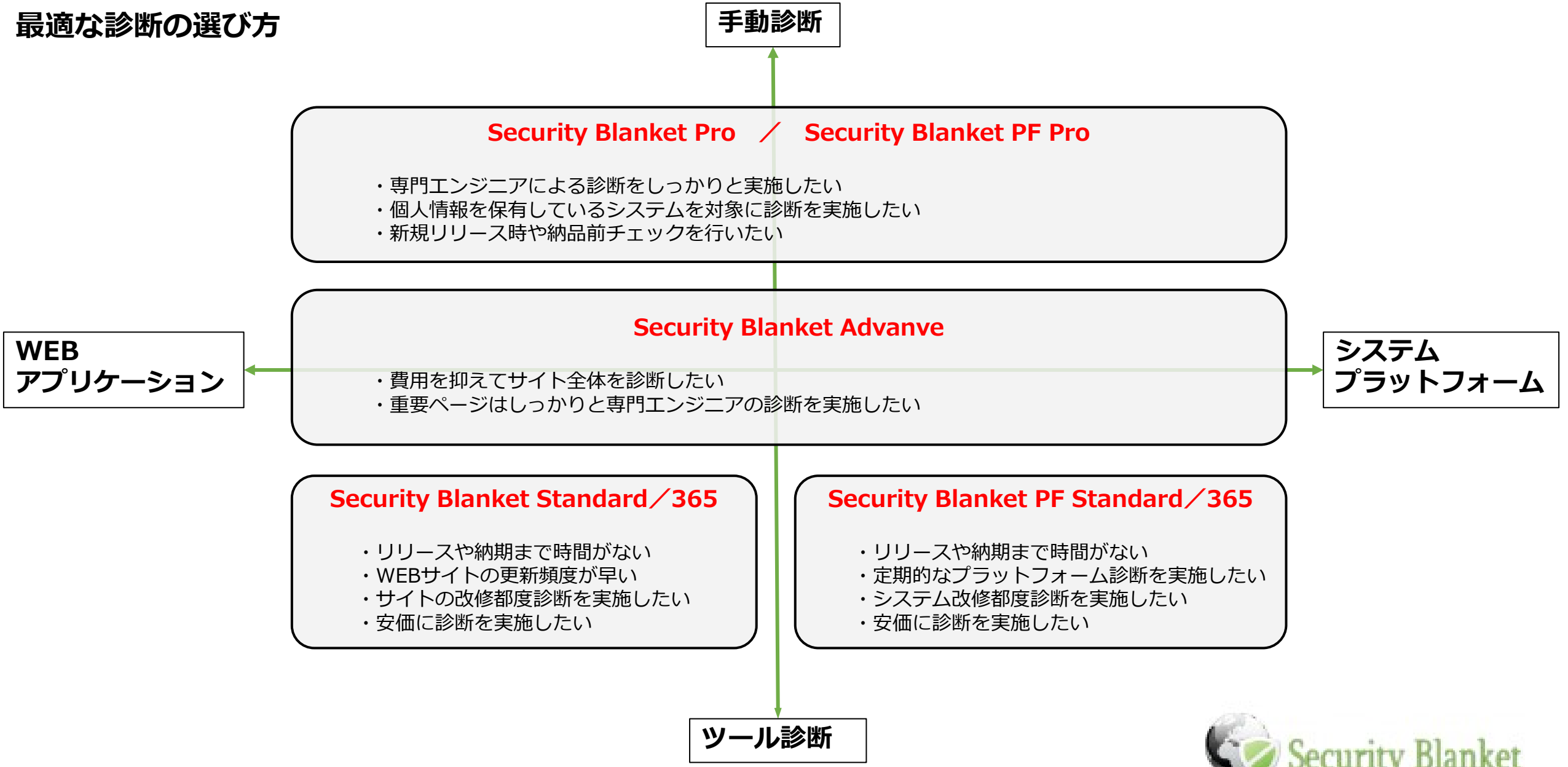
ー　Security Blanket シリーズ　サービスラインナップ　ー

診断対象	サービス名称		概要
WEBアプリケーション	Security Blanket	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（スポット診断ライセンス提供／1回単位）
		365	ツール診断（診断回数無制限ライセンス提供／1年間）

診断対象	サービス名称		概要
システムプラットフォーム	Security Blanket PF	Pro	エンジニアによる手動診断
		Standard	ツール診断（スポット診断ライセンス提供／1回単位）
		365	ツール診断（診断回数無制限ライセンス提供／1年間）

診断対象	サービス名称		概要
共通	オプション	設定代行	ツール診断時の初回設定代行＆初回診断実施
		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）
		オンサイト	お客様指定場所での診断実施

最適な診断の選び方



Security Blanket

ー　診断レポート評価基準　ー

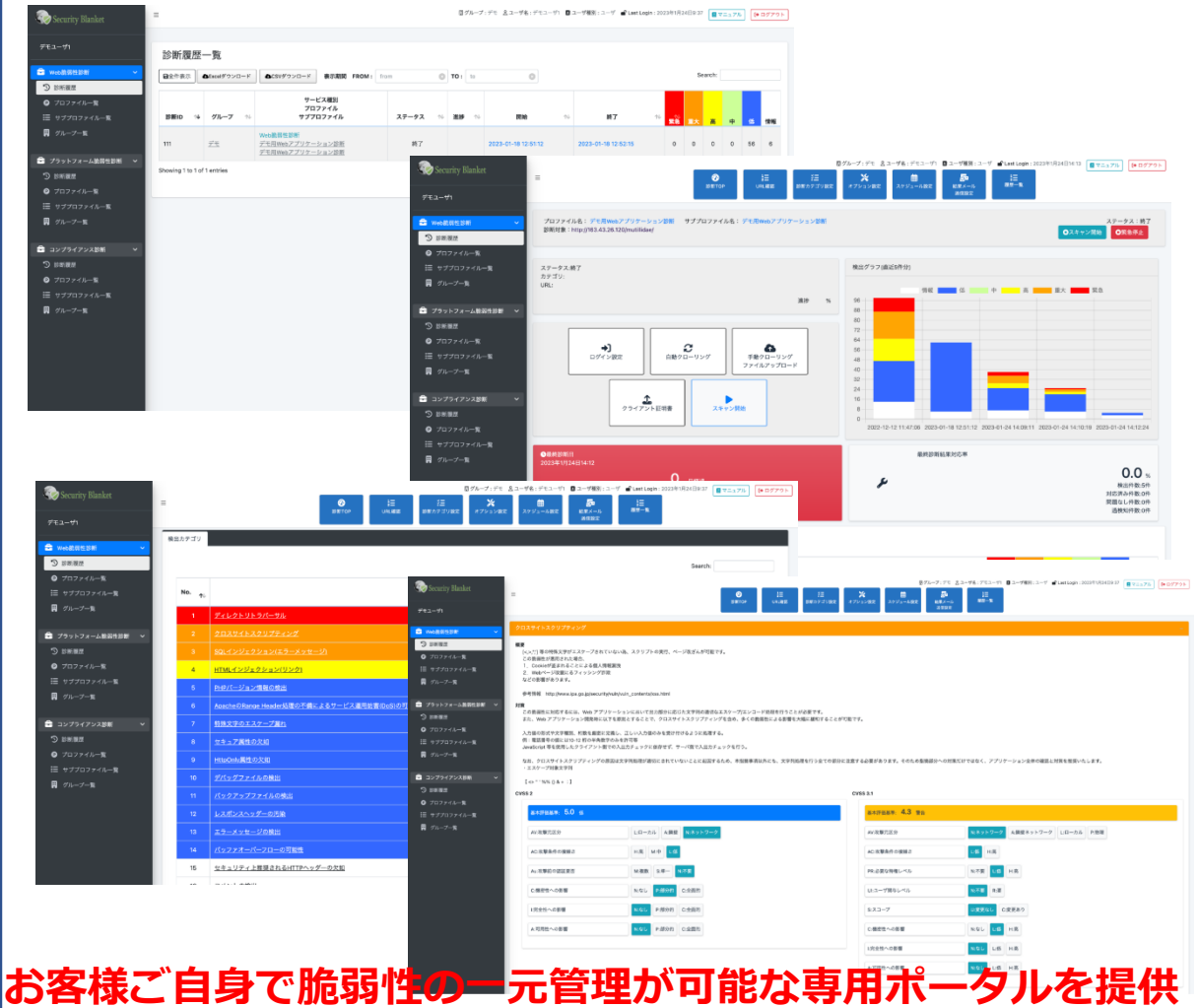
国際的な脆弱性評価基準CVSS、CVE、PCIDSS、OWASP Top 10等のガイドラインを基にした弊社独自の基準にて評価します。

※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　管理ポータル・診断レポートイメージ　ー

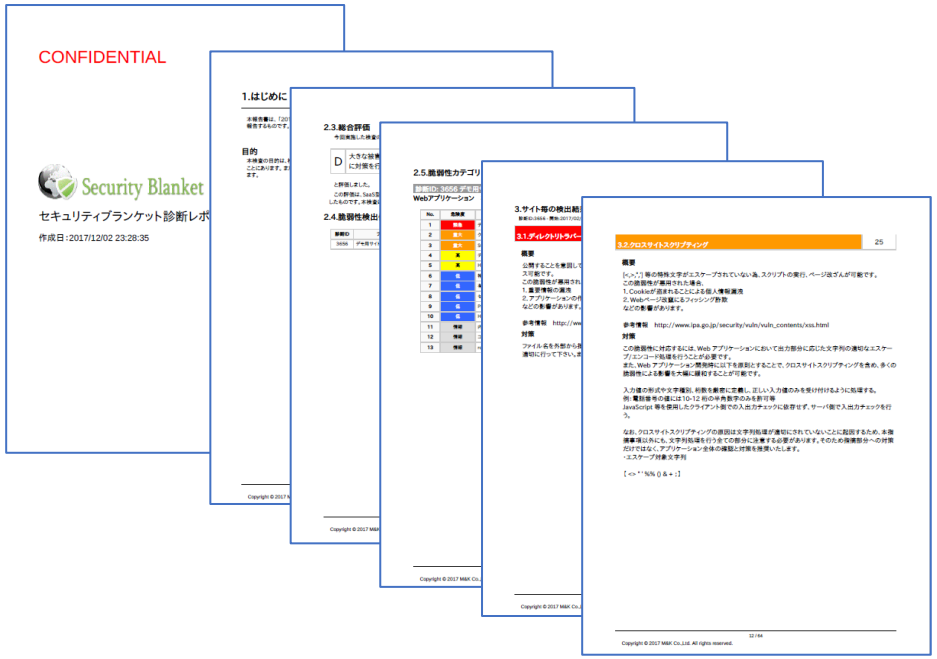
管理ポータル



お客様ご自身で脆弱性の一元管理が可能な専用ポータルを提供

診断レポートイメージ

・標準評価基準のCVSS、PCIDSS、OWASP Top 10をもとに弊社独自の基準を作成しランク付け
・わかりやすい日本語によるレポート
・緊急・高・中・低・情報による5段階評価
・お客様のタイミングでレポート出力可能(ツール診断)



※詳細はサンプルレポートにてご確認ください。

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。

Security Blanket

WEBアプリケーション診断

調査項目		手動	ツール
認証	ログイン	○	×
	その他	○	×
セッション管理	Cookieの取り扱い	○	○
	セッションID	○	○
	クロスサイトリクエストフォージェリ	○	△
入出力処理	SQLインジェクション	○	○
	クロスサイトスクリプティング	○	○
	ディレクトリトラバーサル	○	○
	コマンドインジェクション	○	○
	ヘッダーインジェクション	○	○
	リンクインジェクション	○	○
	パラメータ推測	○	×
	バッファオーバーフロー	○	○
	HTTPレスポンス分割	○	○
	リクエスト改竄	○	×
	その他	○	○

調査項目		手動	ツール
画面遷移	重要の更新	○	×
	権限昇格	○	×
ユーザ管理	履歴	○	×
	パスワード	○	×
暗号	通信の暗号化	○	×
ロジック流出	バッグドアとデバッグオプション	○	×
	エラー処理	○	○
	情報公開	○	○
	コメント	○	○
メール	スパムメール	○	×
画面設計	不適切な画面設計	○	×
	ユーザへの説明	○	×

調査項目		手動	ツール
一般的な脆弱性	既知のソフトウェア脆弱性	○	×
	強制ブラウジング	○	○
	ディレクトリリスティング	○	○
	ファイルダウンロード・アップロードの	○	×
Webサーバ設定	システム情報の開示	○	○
	不要なメソッド	○	○
	初期アカウント	○	×
	ディレクトリ存在の確認	○	○
	サーバエラーメッセージ	○	○

システムプラットフォーム診断

診断項目	
ホストのスキャン	ポートスキャン
	実行中のサービスの検出
ネットワークサービスの脆弱性	DNSに関する調査
	メールサーバーに関する調査
	RPCに関する調査
	ファイル共有に関する調査
	SNMPに関する調査
	SSHサーバーに関する調査
	データベースサーバーに関する調査
	パスワードに関する調査
	管理サイトに関する調査
	その他サービスに関する調査

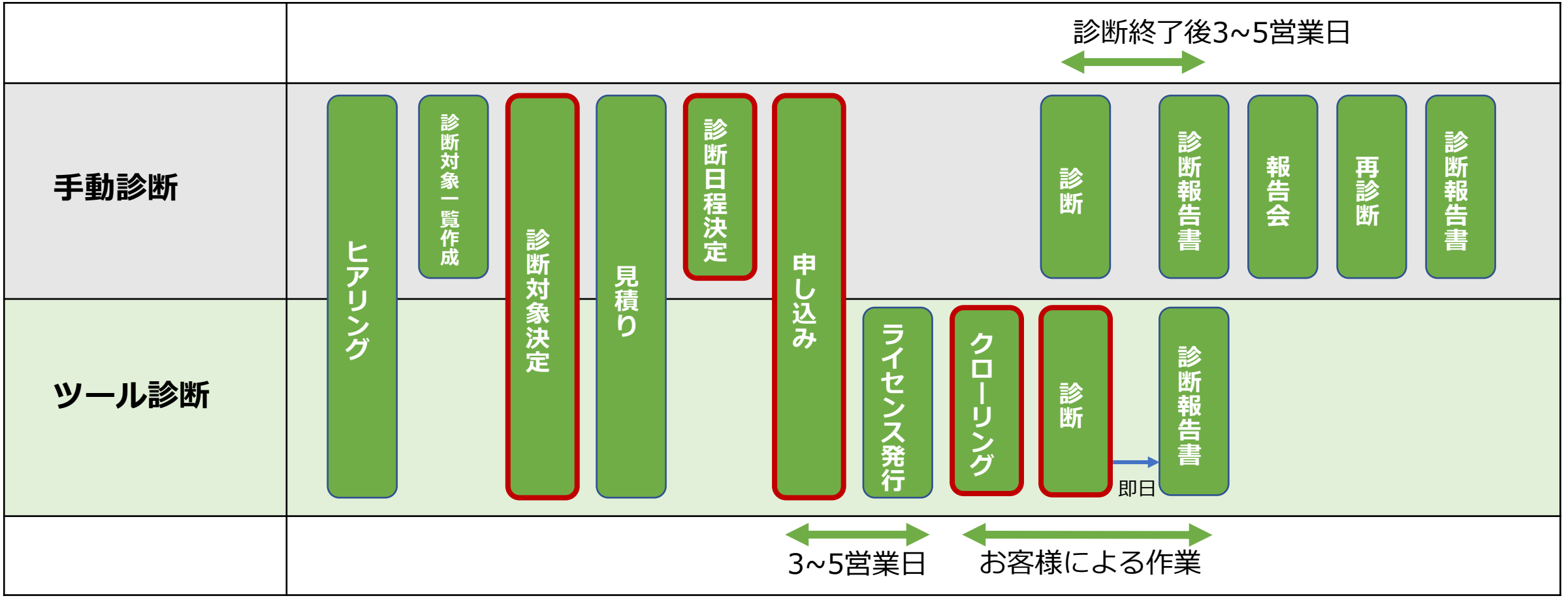
診断項目	
Webサーバーの脆弱性	Webサーバーの脆弱性
	Webアプリケーションサーバーの脆弱性
	許可されているHTTPメソッド
	暗号化方式に関する調査
	証明書に関する調査
各種OSの脆弱性	Windowsの既知の脆弱性
	Solarisの既知の脆弱性
	各種Linuxの既知の脆弱性
	その他各種OSの既知の脆弱性

診断項目	
悪意あるソフトウェア	バックドアの調査
	P2Pソフトウェアの調査
ネットワーク機器の脆弱性	各種ルータ機器の既知の脆弱性
	各種ファイアウォール機器の既知の脆弱性
	その他各種ネットワーク機器の既知の脆弱性
その他	その他ホスト全体の調査
	情報

ー　サービス提供の流れ　ー

WEBアプリケーション診断の流れ

赤枠：お客様による作業

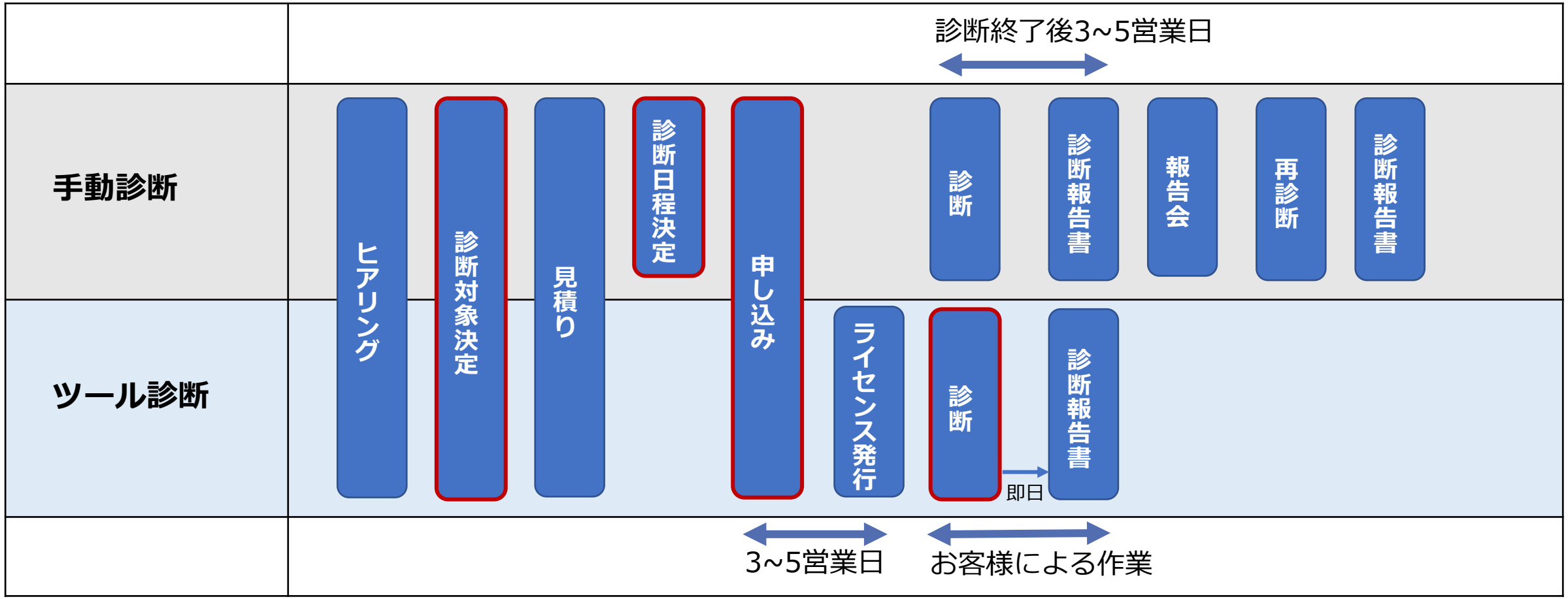


ー　サービス提供の流れ　ー

Security Blanket

システムプラットフォーム診断の流れ

赤枠：お客様による作業



ー　サービス提供条件　ー

WEBアプリケーション、システムプラットフォーム診断共通

・診断時間　　：基本10:00~18:00とさせていただきます。
（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　　：診断は内部の構造や仕組みに関する情報を一切持たず、入出力のみに着目して結果を分析する 「ブラックボックステスト」と呼ばれる手法により行います。

WEBアプリケーション診断

・診断可能画面数：1日あたり5画面程度の診断の実施が可能です。（手動診断の場合）
・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　　：診断対象にメールの送信機能が含まれている場合は、診断中に大量のメールがお客様に届いてしまう可能性があります。メール送信機能を対象外とすることも可能です。
クローリング時等にサイト内に削除、登録等の機能がある場合、実行される可能性がございます。

対象サービス：SecurityBlanket　PRO・Standard・Advance ・365

システムプラットフォーム診断

・診断可能IP数　：　2日間で3IP程度の診断の実施が可能です。（手動診断の場合）

ー　価格表　ー

Security Blanket

サービス	診断対象	診断種別	対象	サービス内容	価格	備考
SecurityBlanket 365	Web アプリケーション	ツール	年間	1サイト診断の1年間ライセンス※1	¥330,000	1FQDNに年間無制限で診断可能
SecurityBlanket Standard			2回	1サイト・２回診断ライセンス	¥220,000	1FQDNに２回診断可能 推奨は100URL程度。 （8時間以内の診断予定として）
SecurityBlanket PF 365	システム プラットフォーム		年間	1IP診断の1年間ライセンス	¥231,000	1IPアドレスに年間無制限で診断可能
SecurityBlanket PF Standard			1回	1IP診断ライセンス	¥77,000	1IPアドレスに1回診断可能

サービス	診断対象	診断種別	対象	サービス内容	価格	備考
SecurityBlanket Pro	Web アプリケーション	手動	基本料金	フル手動診断	¥880,000	10URL 3IP※3　報告会・再診断含む
			追加１URL		¥24,000	
SecurityBlanket Advance		手動+ツール	基本料金	自動＋主要箇所手動診断	¥550,000	報告会・再診断含む
			1 URL	手動診断1URL追加	¥24,000	
SecurityBlanket PF Pro	システム プラットフォーム	手動	基本料金	手動システムプラットフォーム診断	¥550,000	3IP　報告会・再診断含む
			追加1IP		¥50,000	

サービス	診断対象	診断種別	対象	サービス内容	価格	備考
ツール設定代行	Web アプリケーション	オプション	1回	クローリング等の設定代行&初回診断	¥100,000	
オンサイト費用	共通			オンサイト診断（3日以内）※日数により変動する	¥150,000	交通費別途 （東京・神奈川・埼玉・千葉を除く）
報告会				お客様先での報告会	¥100,000	

※1　1サイト＝１ＦＱＤＮとなります。
※2　ログイン機能など認証システムが存在する場合、1ライセンスで診断できる範囲は1認証システムまでとなります。
　　認証システムが複数存在する際は、数に応じてライセンスが必要となります。
※3　1URL＝1画面となります。同一URL内で画面が遷移する場合は画面数にてカウントします。
※4　表記の価格はすべて税抜きです。

ー　提供実績（2022年3月末時点）　ー

・診断実績：年間約500案件、のべ5,000社以上の診断実績を保有
・診断ツールのOEM提供等、大手パートナー企業への技術提供：4社

診断実績　業種一例	
官公庁	航空
証券	クレジット
銀行	アパレル
人材派遣	旅行
その他 （Sier、Nier、販社向けにエンジンをOEM提供）	

サービス	顧客	診断対象
WEB手動リモート診断	国内大手デパート	ECサイト
WEB手動リモート診断	キャリア系クレジット会社	会員管理サイト（会員数約300万人）
ネットワーク手動オンサイト診断	国内大手SIer	サーバルームのネットワーク
WEB手動リモート診断	国内大手ISP	ユーザ向けコンテンツ（会員数70万人）

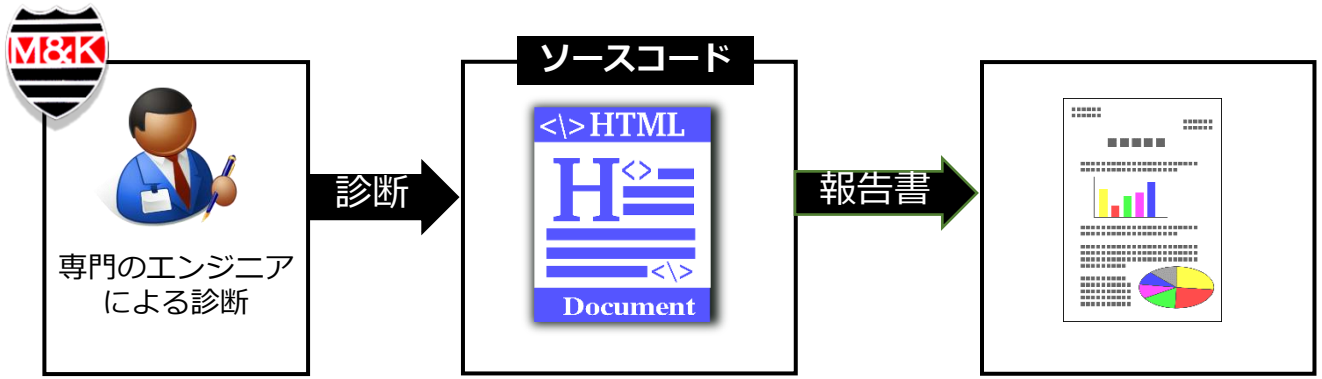
ー　参考　ー

Security Blanket

脆弱性診断に加えて、以下のサービスも提供可能です。

ソースコード診断

アプリケーションのソースコードに関するセキュリティ上の問題点を、診断コンサルタントが査閲し、可視化された問題点と対策を提示します。



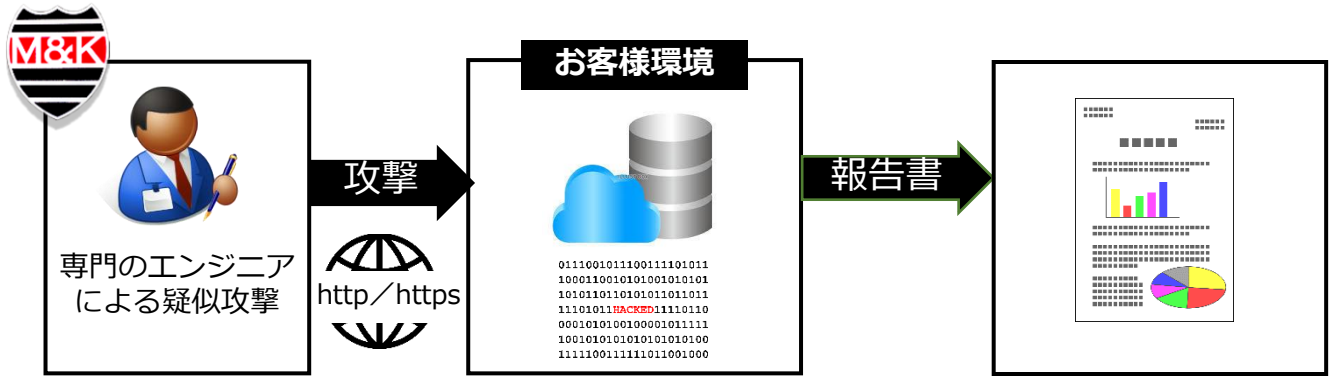
・Webアプリケーションのソースコード一式をお預かりします

・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検査します

・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レポートを提示します

ペネトレーションテスト

システムに潜在する脆弱性を悪用した侵入や情報搾取など、実際の攻撃を想定した疑似侵入テストを実施し、システムの堅牢性を評価します。



・悪意のあるハッカーが実際に利用する手法を用いて、専門のエンジニアが疑似的に対象対象システムに攻撃を実施します

・PCI DSSやOWASP等のガイドラインに準拠した診断結果をご提示します

・脆弱性診断にて可視化されたリスクの検証や、実施済みのセキュリティ対策の有効性の確認が可能です

株式会社M&K

本社　　：東京都渋谷区神南1-11-3
　　PORTAL POINT SHIBUYA 505

名古屋支店：愛知県名古屋市中区錦1-5-10
　　名古屋伊藤忠ビル4F

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