

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

株式会社M&K 会社紹介資料



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** ～



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

— M&Kが選ばれる理由 —



Thank
You!

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。



セキュリティコンサルティングサービス



ー セキュリティコンサルティングサービス ー

セキュリティ対策の第一歩は、**現状を正確に把握し、リスクを正しく評価する事**が必要です。
現環境のアセスメントを通して、あるべき姿とのギャップを埋める為の施策立案、運用体制見直し等を、経験豊富なコンサルタントとエンジニアが総合的にご支援します。

セキュリティコンサルティングサービス提供内容例

IT環境アセスメントサービス

現在のITシステム環境や社内運用体制に関する状況確認／ヒアリングを実施し、各種法令・ガイドライン等への適合状況、今後の実施すべき内容などをレポートし、ご報告いたします。

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

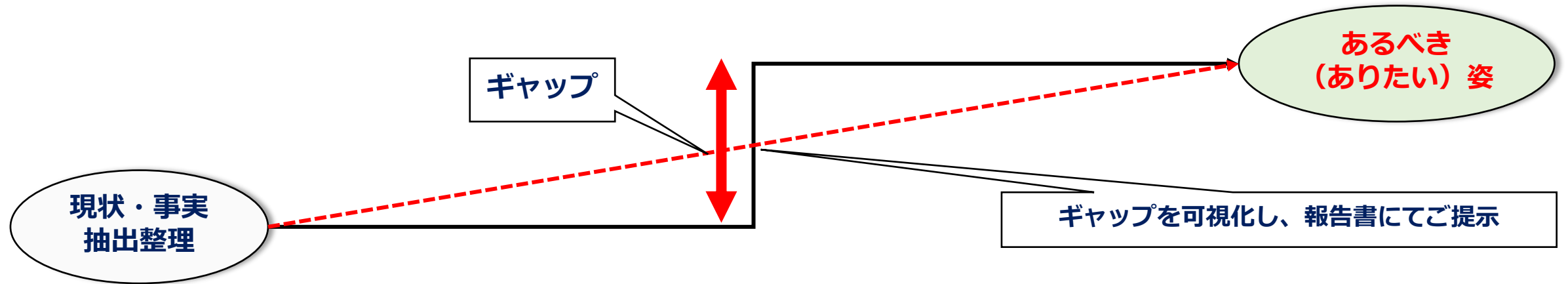
各種認証取得に関するフレームワークに準拠した運用体制構築、技術的な対策強化案をご提示し、公的認証の取得に必要な体制構築・対策強化をご案内いたします。

システムアドバイザリーサービス

システム運用やセキュリティ対策は、継続的に連続性を持って対応する必要があります。
定期的なリスク評価を実施し、その結果に基づいて対策を強化するサイクル確立のお手伝いをします。

IT環境アセスメントサービス

現在のITシステム環境や社内運用体制に関する状況確認／ヒアリングを実施し、各種法令・ガイドライン等への適合状況、今後の実施すべき内容などをレポートニングし、ご報告いたします。



まずは、**正確に現状を把握すること**、

次に **あるべき姿(ありたい姿)へのプロセスを立案すること** が重要なポイントになります。

- ①各種法令・ガイドライン等に定められた取り扱い体制が組織内に整備されているか？
 - ・組織体制
 - ・規程/手順書/社内ガイドライン等
 - ・個人情報の取得/利用/特定/提供の原則が徹底されているか
- ②取り扱い体制および運用の実効性があるか？（運用評価）
 - ・適正な管理がなされているか
 - ・個人情報に関する本人の権利が守られる体制か
- ③各種安全管理措置
 - ・技術/組織/物理/人的安全管理措置が適切に整備され、運用されているか



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

各種認証取得に関するフレームワークに準拠した運用体制構築、技術的な対策強化案をご提示し、公的認証の取得に必要な体制構築・対策強化をご案内いたします。

✓ マネジメントシステムとは？

- ・ 製品やサービス、あるいは事業が、目的（顧客満足、法順守、リスク管理、環境負荷低減など）を達成するために、**プロセスや活動を管理**すること
- ・ 効率的かつ効果的な管理とするために、体系的な方法をとることで、重要なことが漏れたりすることがなくなり、**何を、いつ、どのように、なぜ、どこで行うか、そしてその責任者が誰なのか？**が、クリアになる
- ・ 組織の諸活動を**目的に導くため**の仕組み

具体的な取り組みと工程例

工程①

- ・ 各種法令・ガイドライン等への適合譲許確認
- ・ 情報セキュリティアセスメント

工程②

- ・ 全社を対象範囲とする情報セキュリティ構築の中長期構想立案支援
- ・ 経営層向け説明資料作成支援

工程③

- ・ 情報セキュリティマネジメントシステム基盤構築
- ・ 情報セキュリティ管理策実装支援

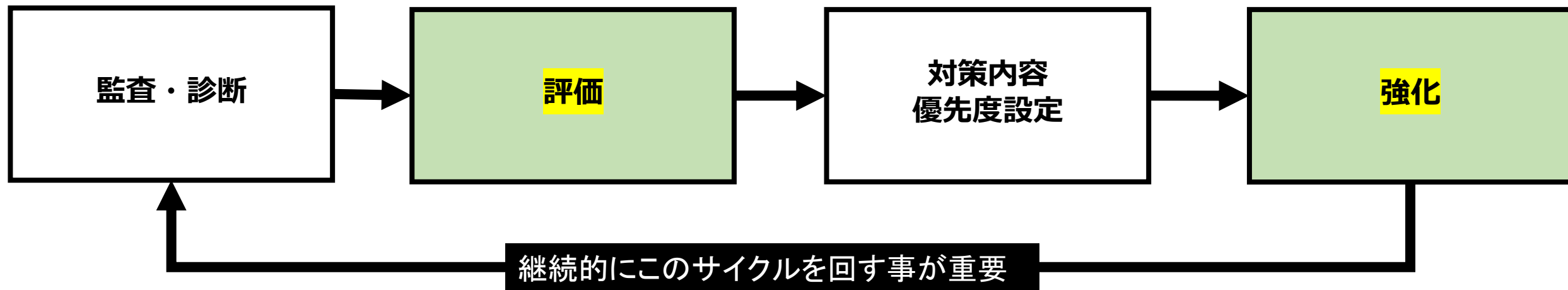
システムアドバイザリーサービス

システム運用やセキュリティ対策は、継続的に連続性を持って対応する必要があります。
定期的にリスクを評価を実施し、その結果に基づいて対策を強化するサイクル確立のお手伝いをします。

✓ 企業全体のセキュリティレベルを上げ、「安心・安全」なIT環境を維持する為には？

- ・ ITサービスを利用・活用する際、社内において統一の基準を設けて運用する事
- ・ 定期的な監査・診断等により可視化された結果に基づき、リスクを正しく評価する事
- ・ 対策の優先順位を決めて定期的に強化する事
- ・ 設定した基準が遵守されているか定期的に診断する事

「評価」と「強化」を分けて考え、高いセキュリティレベルを継続するお手伝いをします





セキュリティ診断サービス





ー セキュリティ診断サービス ー

ITの利活用が進む昨今、サイバーセキュリティのリスクは日々増加の一途を辿っています。正しくリスクを正しく評価する為には、IT環境に潜む脆弱性を可視化し、適切な対策を実施する事が重要です。経験豊富な診断コンサルタントと独自開発のツールにて、費用対効果の高い高品質なサービスをご提供いたします。

セキュリティ診断サービス提供内容例

クラウド環境設定診断

AWS/Microsoft Azure等のパブリッククラウド利用における管理設定項目の不備を可視化し、セキュリティレベル向上の為の対策内容を提示します。



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。

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。

ソースコード診断

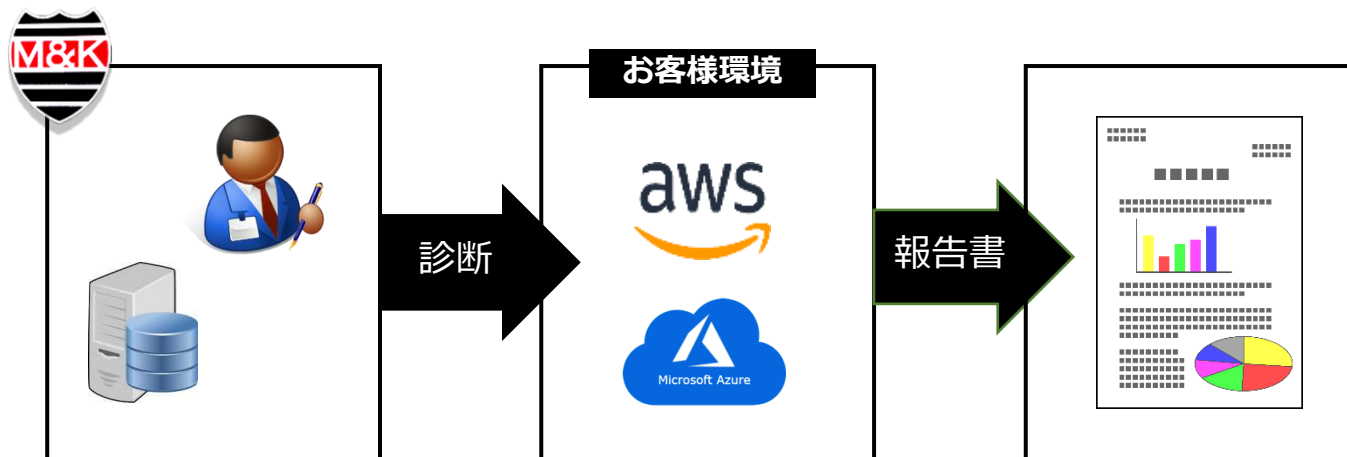
アプリケーションのソースコードに関するセキュリティ上の問題点を、診断コンサルタントが査閲し、可視化された問題点と対策を提示します。

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。

クラウド環境設定診断

AWS/Microsoft Azure等のパブリッククラウド利用における設定項目の不備を可視化し、セキュリティレベル向上の為の対策内容を提示します。



- ・インターネット経由にて診断を実施します
- ・CISベンチマークに基づくベストプラクティスへの適合状況を可視化し、パブリッククラウド利用における管理設定上の不備を検出します
- ・読みやすい日本語のレポートにて、セキュリティレベルの向上に必要な対策を提示します

AWS 

CIS Amazon Web Services Foundations L1 (v1.4.0)

- ・IDとアクセス管理 : IDおよびアクセス管理に関連するオプションを構成するための推奨事項
- ・ストレージ : ストレージポリシーを設定するために従うべきセキュリティの推奨事項
- ・ロギング : AWSのアカウントロギング機能を設定するための推奨事項
- ・監視メトリクス : フィルターとアラームの推奨事項
- ・ネットワーク : 仮想プライベートクラウド (VPC) のセキュリティ関連の推奨事項

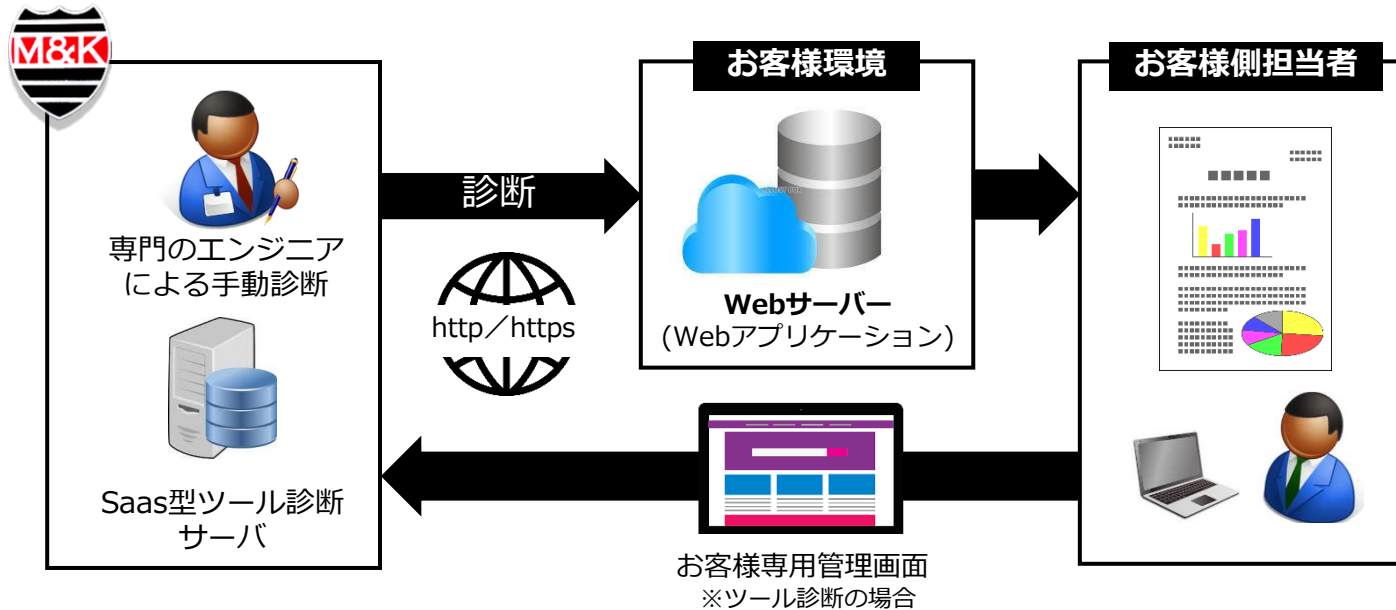
Microsoft Azure 

CIS Microsoft Azure Foundations v1.3.0 L1 (v1.3.0)

- ・IDとアクセス管理 : IDおよびアクセス管理に関連するオプションを構成するための推奨事項
- ・セキュリティセンター : セキュリティポリシーを設定する際に従うべきセキュリティの推奨事項
- ・ストレージアカウント : ストレージアカウントポリシーを設定するために従うべきセキュリティの推奨事項
- ・データベースサービス : 一般的なデータベースサービスポリシーを設定するために従うべきセキュリティの推奨事項
- ・ロギングと監視 : ログと監視のポリシーを設定するために従うべきセキュリティの推奨事項
- ・ネットワーク : ネットワークポリシーを設定するために従うべきセキュリティの推奨事項
- ・仮想マシン : 仮想マシンポリシーを設定するために従うべきセキュリティの推奨事項
- ・その他セキュリティ注意事項 : 一般的なセキュリティと運用管理を設定するために従うべきセキュリティの推奨事項
- ・AppService : Azure App Serviceのセキュリティに関する推奨事項

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
- ・エンジニアに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

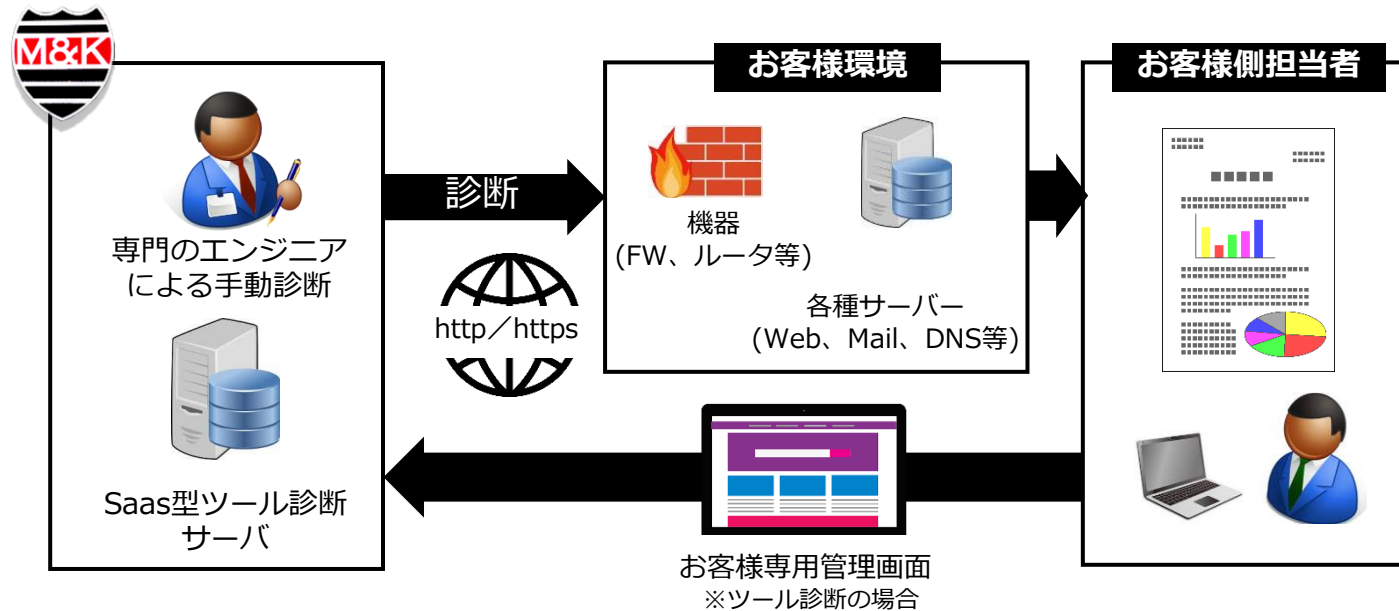
サイト全体はツールで安価に診断し、重要な機能だけはエンジニアによる高度な診断を実施したい時など、手動診断とツール診断を組み合わせた最適な診断方法と提供します。

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
- ・エンジニアに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

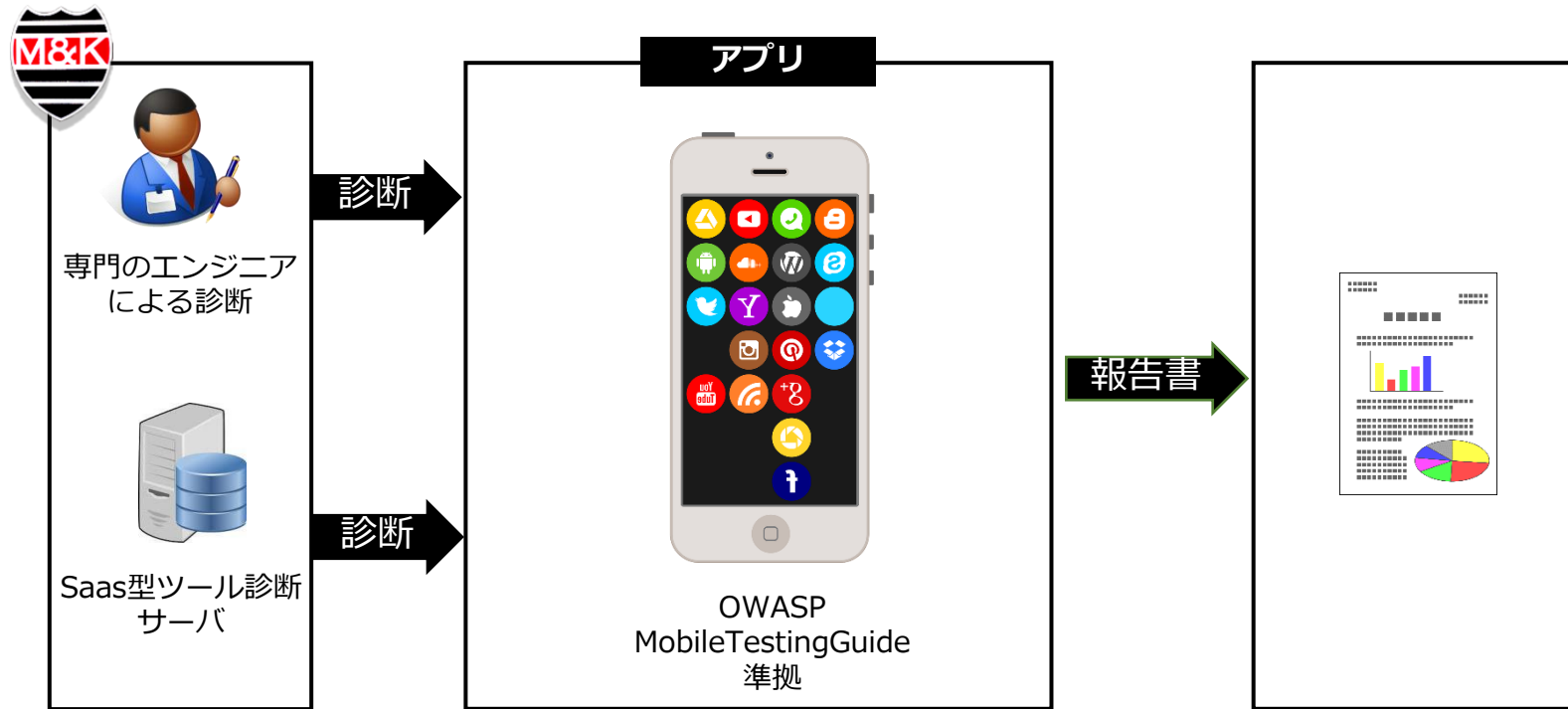
サイト全体はツールで安価に診断し、重要な機能だけはエンジニアによる高度な診断を実施したい時など、手動診断とツール診断を組み合わせた最適な診断方法と提供します。

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。

モバイルアプリケーション診断

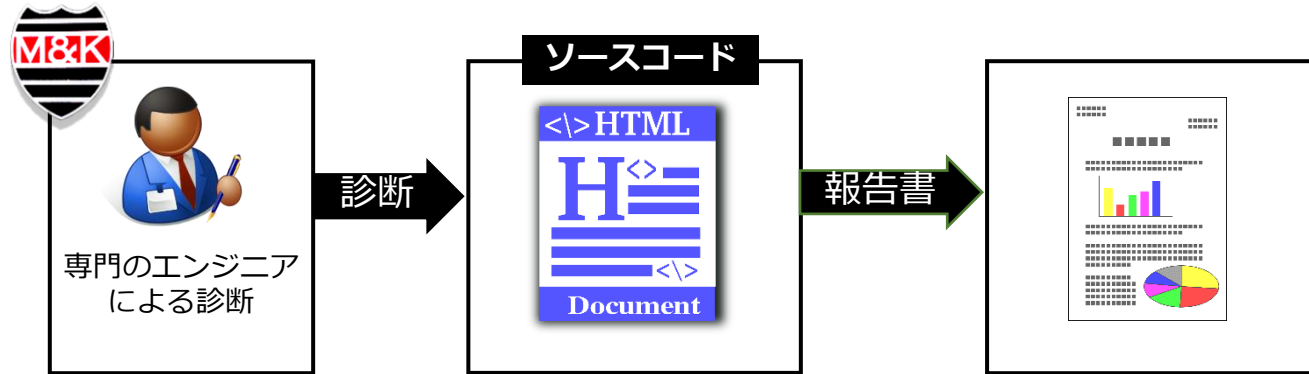
iOS/Androidで作成されたモバイルアプリケーションに潜むセキュリティ上の問題点を可視化します。ネイティブアプリも対応可能です。



- ・ 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、ツール診断およびエミュレータ等を利用した動的検査を実施します
- ・ 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

ソースコード診断

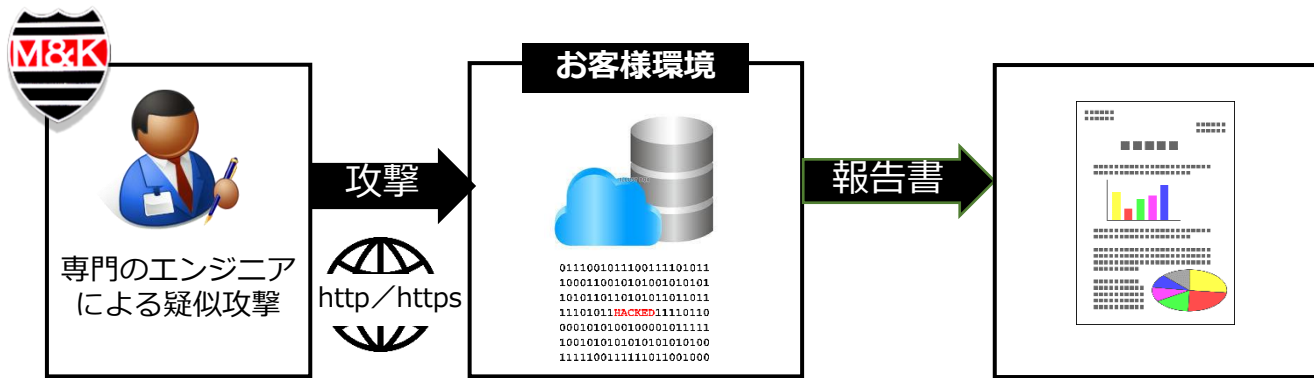
アプリケーションのソースコードに関するセキュリティ上の問題点を、診断コンサルタントが査閲し、可視化された問題点と対策を提示します。



- 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



インテグレーションサービス



— インテグレーションサービス —

可視化したセキュリティリスクへの対策強化を目的としたシステム改修や製品導入、あらかじめセキュリティを意識し可用性の高いシステムプラットフォームの新規構築など、各種インテグレーションをご提供します。

インテグレーションサービス提供内容例

クラウドインテグレーション

AWS、Microsoft Azure等のパブリッククラウドの設計・構築を代行します。
セキュリティ対策も考慮した安心・安全なシステム環境をご提供いたします。



セキュアコーディング支援

専門のセキュリティエンジニアがWEBアプリケーション開発に関するコーディングについてアドバイスを実施します。
リスクを最小化し安全面を考慮したコーディング手法をご案内します。



WAF導入支援

お客様側での設備投資が不要で、低コストで利用可能なクラウド型のWEBアプリケーションファイアウォール（WAF）の導入を支援します。
クラウド型なので、運用面の心配もありません。



Scutum

WEBサイト改ざん検知導入支援

悪意のあるWEBサイトの改ざんを検出する仕組みの導入を支援します。
クラウド型なので低コストで利用可能でありながら、精度の高いスク립ト検知型のサービスをご提供します。



クラウドインテグレーション

AWS、Microsoft Azure等のパブリッククラウドの設計・構築を代行します。



- ・ コンテナ、サーバレス等のクラウドネイティブアーキテクチャを活用したアプリケーション稼働基盤設計を代行します
- ・ オンプレミス環境からの移行、リフト&シフト対応も可能です
- ・ 経験豊富なエンジニアがクラウド利用における管理設定項目等に関するセキュリティ面も意識した安心・安全な基盤を設計します
- ・ システム運用に関するご相談や体制構築に関するご支援も承ります

セキュアコーディング支援

専門のセキュリティエンジニアがWEBアプリケーション開発に関するコーディングについてアドバイスを実施します。



専門のエンジニア
によるアドバイス



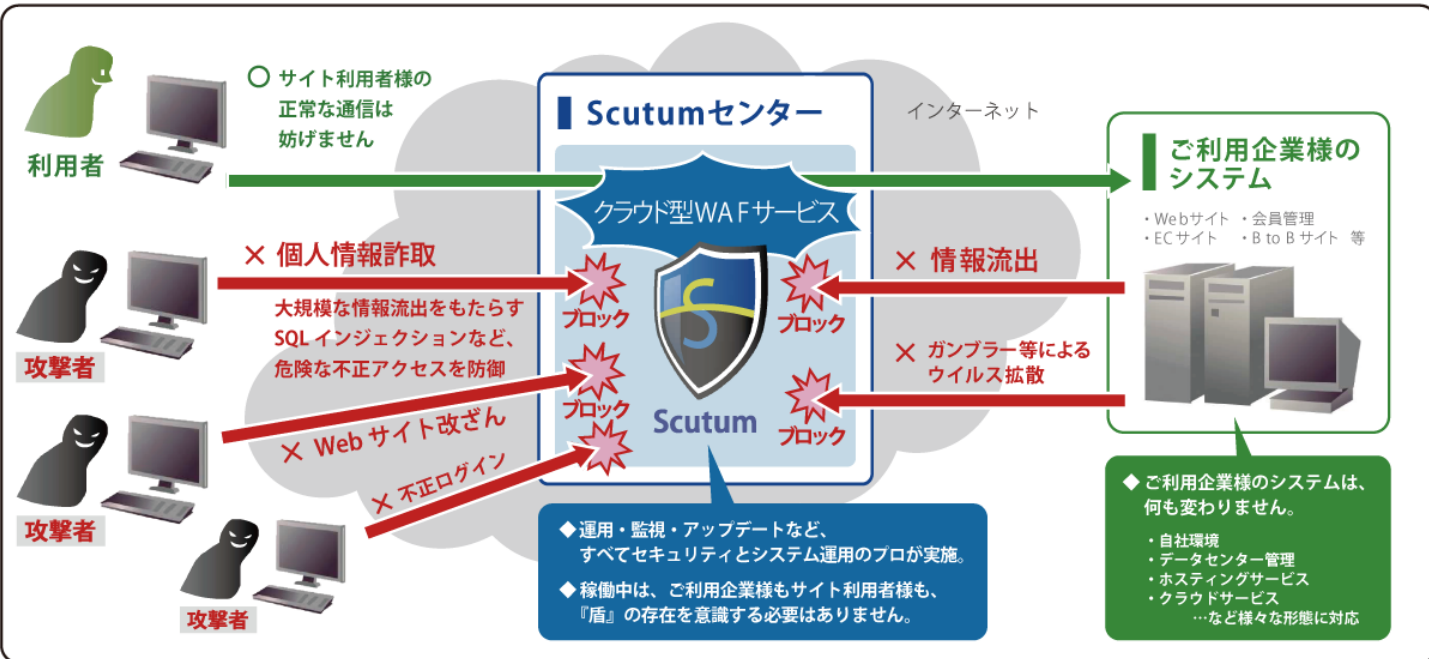
ソースコード



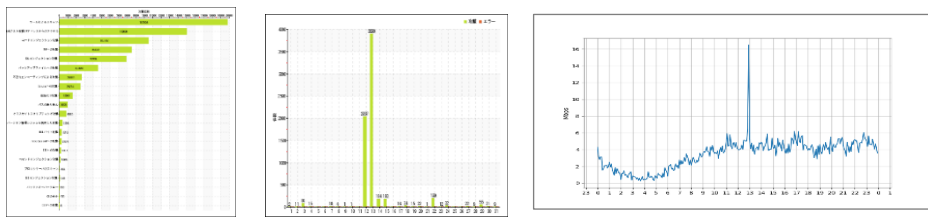
- ・ WEBアプリケーションの開発工程からセキュリティ対策に関するアドバイスを実施します
- ・ 実際のハッカーが用いる手法を理解したセキュリティエンジニアがソースコードを確認しますので、有効性の高い対策が可能です
- ・ 脆弱性診断やペネトレーションテストと組み合わせる事により、堅牢なシステム開発が可能です

WAF導入支援

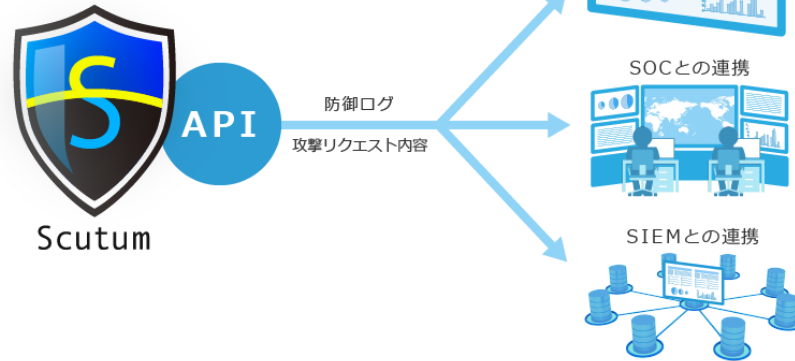
クラウド側のWEBアプリケーションファイアウォール (WAF) である「Scutum」の導入を支援します。



- ・お客様側で新たな設備投資や自前機器のご用意は不要です
- ・お客様システムへの通信を「Scutum」経由にする事により、悪意のある攻撃や通信を検知・遮断します
- ・クラウド型なので、シグネチャーの更新や最新の脆弱性への対応時のアップデートなども、お客様側での運用は不要です
- ・API連携機能もあり、お客様システムとの連携も可能です

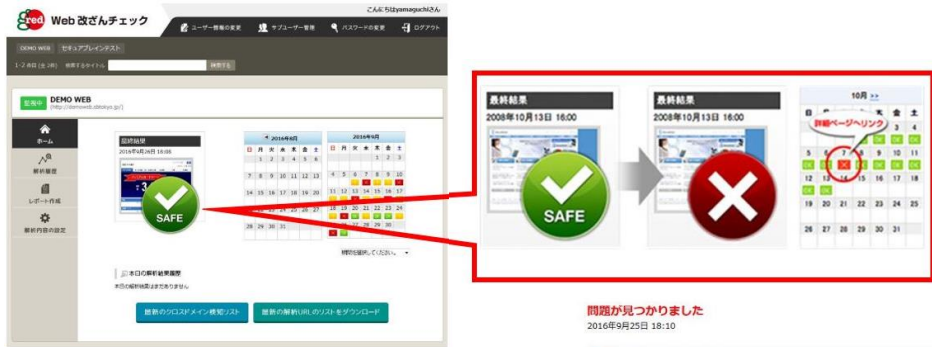


- ・お客専用の管理画面にてリアルタイムに状況の確認が可能です
- ・月次レポートの作成、報告会等も対応可能です

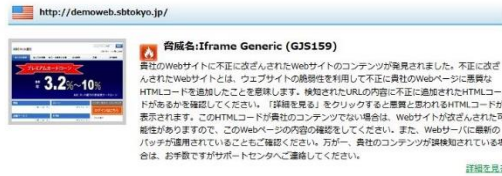


WEBサイト改ざん検知導入支援

クラウド側の改ざん検知サービスである「Gred Web改ざんチェック Cloud」の導入を支援します。



問題が見つかりました
2016年9月25日 18:10



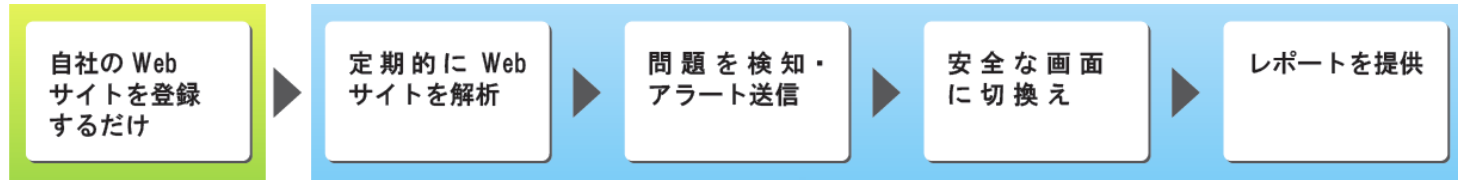
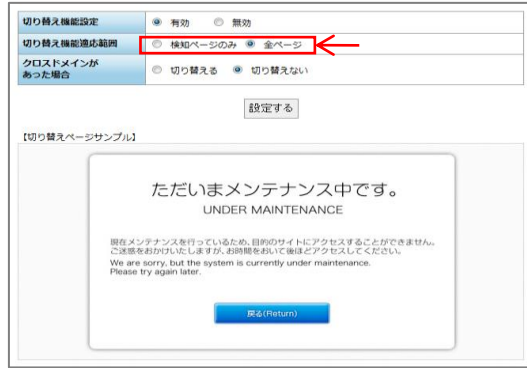
改ざんを検知したページのソースコードを表示し、問題のある箇所をハイライト表示

```

問題が見つかりました
http://denoweb.sbtokeyo.jp/

以下のソースコード内のイライト部に問題があります。
1  <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1"
2  <html xmlns="http://www.w3.org/1999/xhtml" xml:lang="ja" lang="ja">
3  <head>
4  <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
5  <meta http-equiv="Content-Style-Type" content="text/css" />
6  <meta http-equiv="Content-Script-Type" content="text/javascript" />
7  <meta http-equiv="ImageToolbar" content="no" />
8  <meta name="description" content="" />
9  <meta name="viewport" content="" />
10 <link rel="stylesheet" href="css/common.css" type="text/css" />
11 <script type="text/javascript" src="js/common.js"></script>
12 <title>ABCネット銀行</title>
13 </head>
14 <body>
15 <div id="top">
16 <div id="header">
17 <div id="logo">
18 </div></div>
19 <div id="form">
20 <form action="http://www.google.com/cgi" id="cse-search-box">
21 <input type="text" name="q" value="" />
22 <input type="hidden" name="ie" value="UTF-8" />
23 <input type="text" name="g" size="21" /></div>
24 <input type="image" src="images/serch.gif" alt="検索" name="sa" value="検索" />
25 </div>
26 </body>
27 </html>
    
```

- ・お客様側で新たな設備投資や自前機器のご用意は不要です
- ・お客様サイトを定期的に巡回（1日4回）し、改ざんの可能性を検知します
- ・スクリプト検知側を採用しており、新旧比較による差分検知型に比べて誤検知を最小化していますので、WEBサイト更新時のアラート等もありません
- ・改ざんを検知した際には、自動的にメンテナンス画面に切り替わる機能もあり、危険な状態のまま長期間公開されているという事が無くなります。





教育支援サービス



— 教育支援サービス —

セキュリティインシデントの発生原因には、人的要因が多く見られます。
組織に従事する従業員の皆さまのITリテラシーやセキュリティポリシーの理解度向上を支援します。

教育支援サービス提供内容例

標的型攻撃メール訓練サービス

被害が急増している「標的型攻撃メール」に対する訓練を実施します。
バラマキ型にて添付ファイル型、リンククリック型に対応しており、
企業のセキュリティポリシーに沿った訓練が手軽に実施可能です。

セキュリティ講習会

専門のエンジニア、コンサルタントがセキュリティ対策に関する基礎
や考え方などを実例を交えてご紹介します。
企業の従業員のみなさまのセキュリティに関する理解度の向上に活用
いただけます。

e-ラーニング

お客様側での設備投資が不要で、低コストで利用可能なクラウド型の
ラーニングサービスをご提供します。
学習コンテンツはお客様側にて自由に編集頂けます。

コンテンツ作成代行

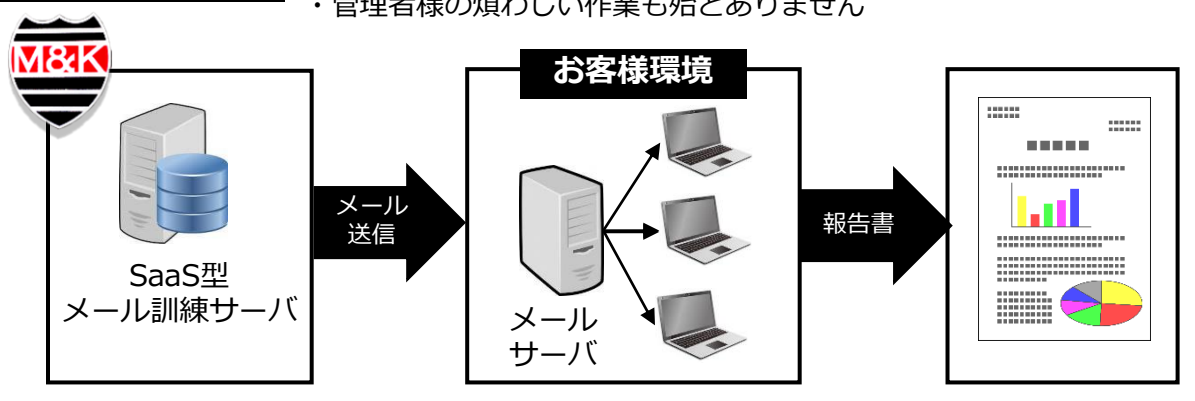
e-ラーニングの学習コンテンツ作成を代行します。
お客様のご要望や、企業のセキュリティポリシーをお伺いし、最適な
学習内容を専門のコンサルタントが作成いたします。

標的型攻撃メール訓練サービス (Security Blanket MT)

企業のセキュリティポリシーに沿った様々なメール訓練を手軽に実施いただけます。

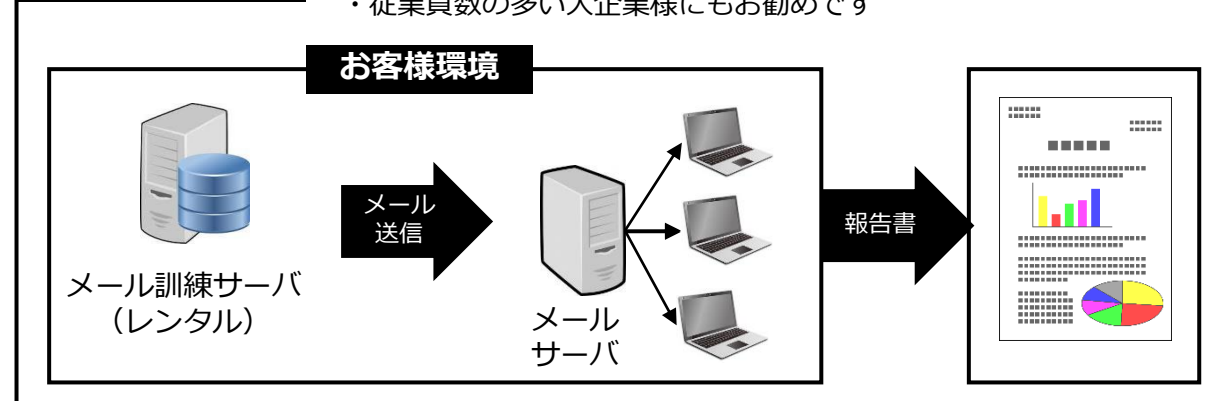
SaaS型

- ・低コストで簡単導入
- ・管理者様の煩わしい作業も殆どありません

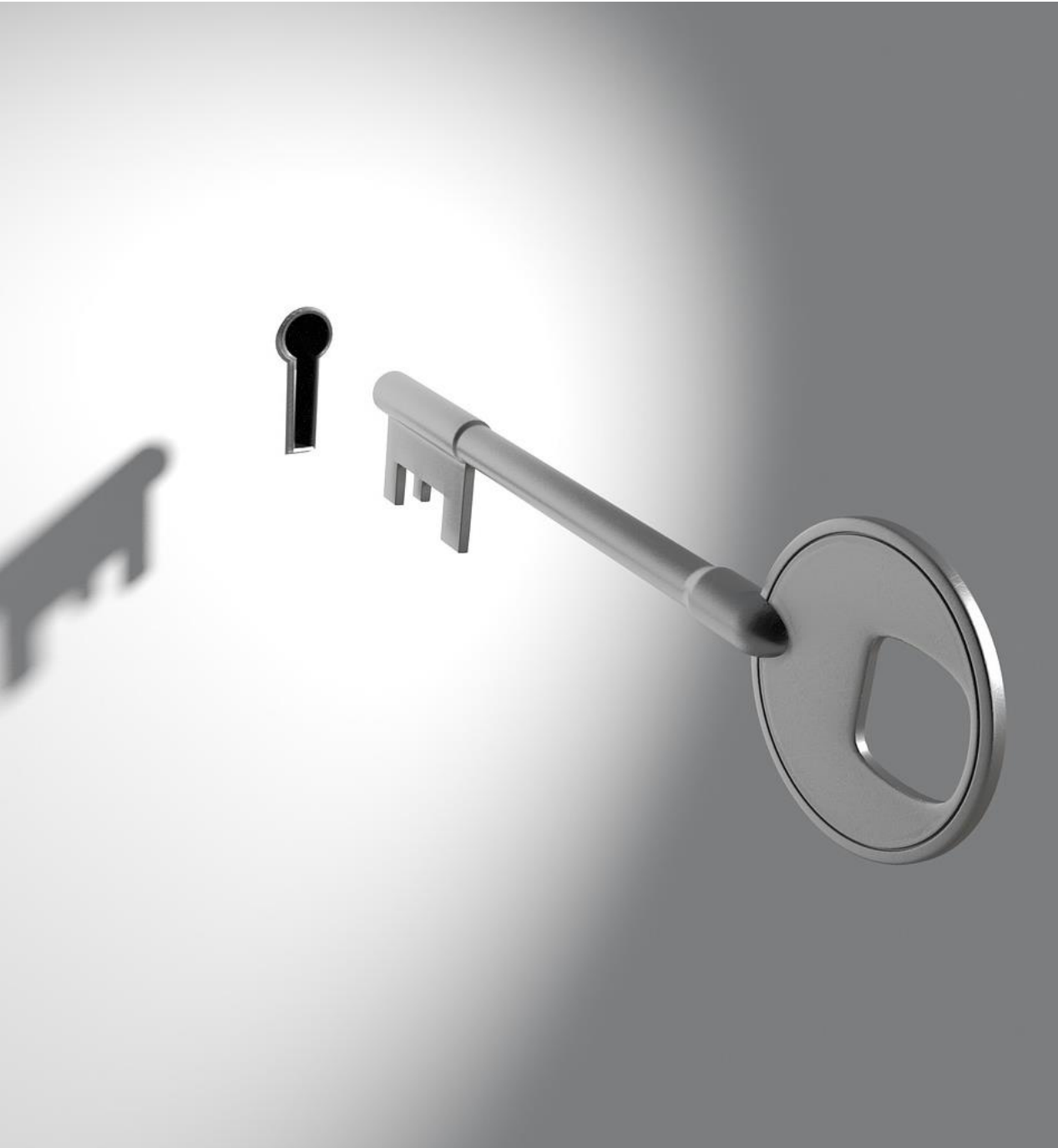


オンプレミス型

- ・企業毎のセキュリティポリシーに沿った導入が可能
- ・従業員数の多い大企業様にもお勧めです



- ・企業規模や目的に合わせて、SaaS型、オンプレミス型の二通りから選択可能です
- ・メール本文や添付ファイルの内容、送信間隔や送信方法 (Zip暗号化等) まで自由にカスタマイズ頂けます
※テンプレートのご用意もあります。
- ・URLリンクや添付ファイル型等、攻撃方法のカスタマイズ可能です
- ・訓練対象 (従業員) のOSやアプリを表示し、開封環境が確認できるレポートを提示します



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/>