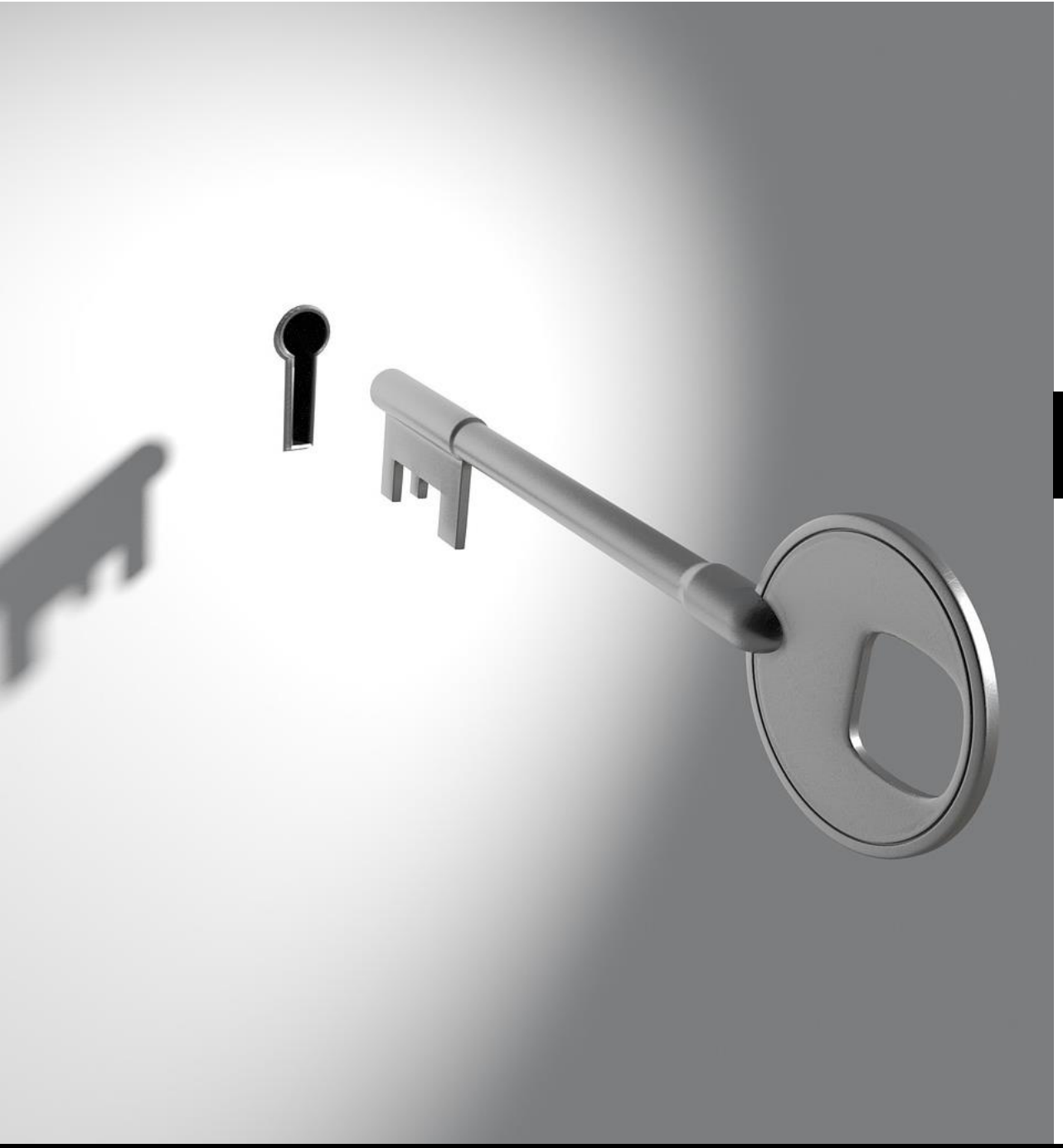
【Ver2306-2】



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

セキュリティコンサルティング サービス紹介資料

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」。

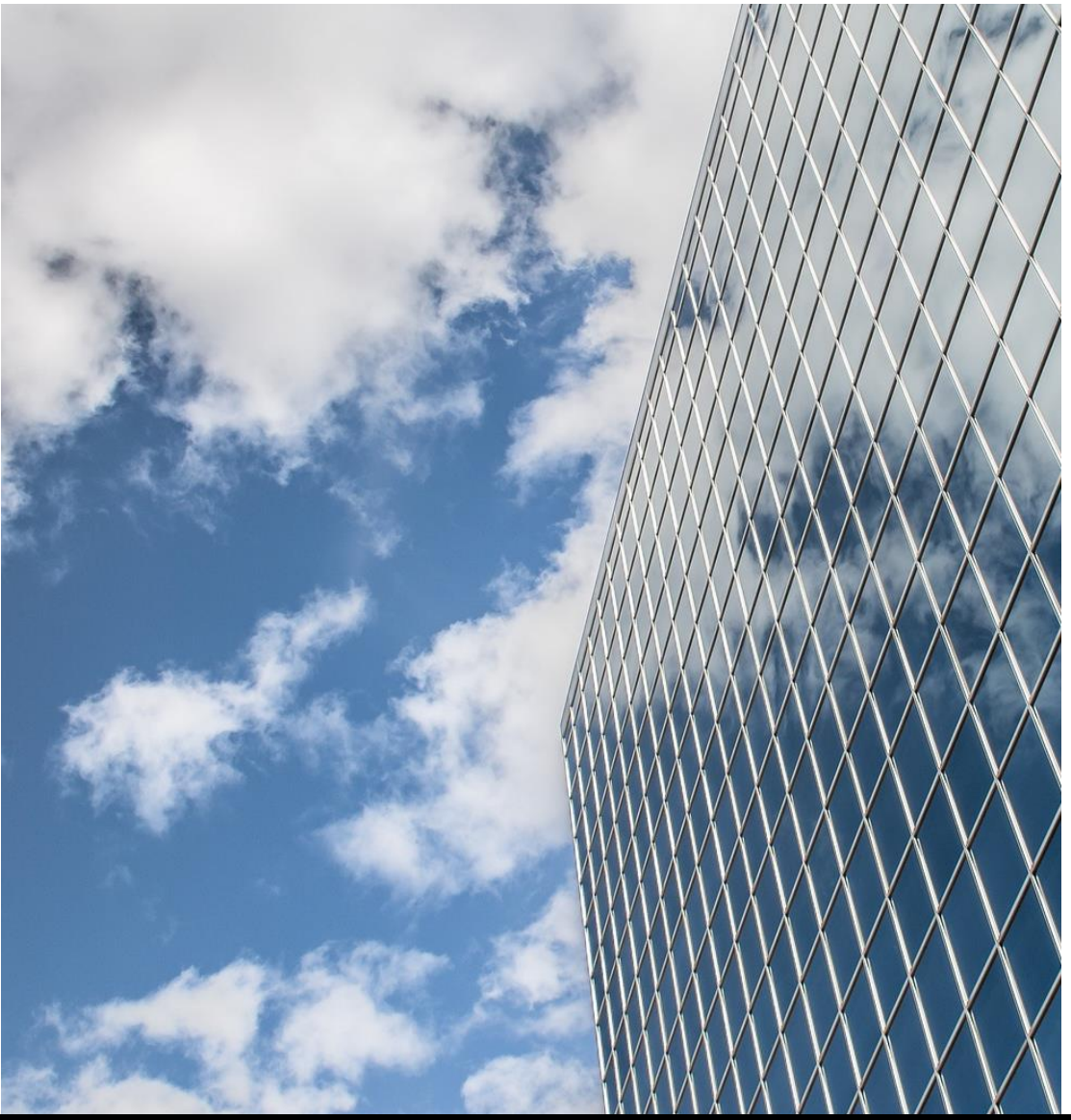
お客様のビジネスにポジティブな影響を与える
システムアドバイザーでありたい。

～　Security blanket with you　～

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。

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ティングし、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。

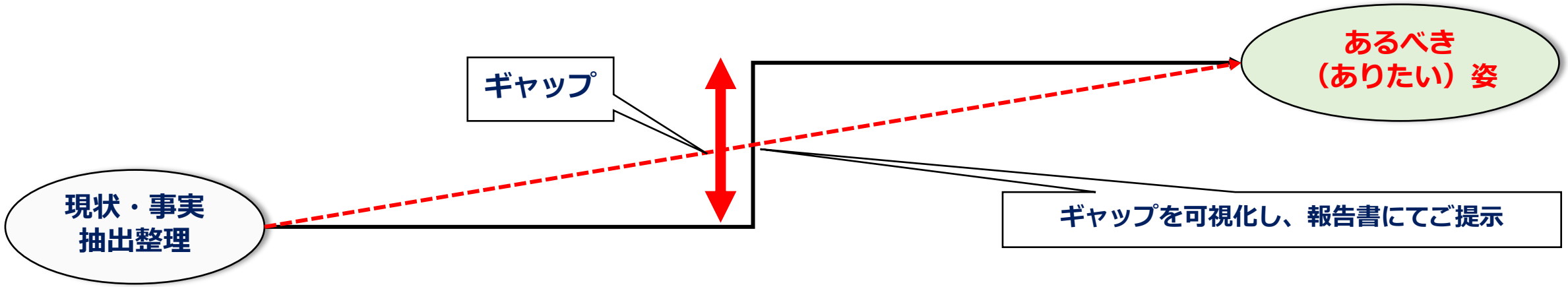
システムアドバイザリーサービス

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。

IT環境アセスメントサービス

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ティングし、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。

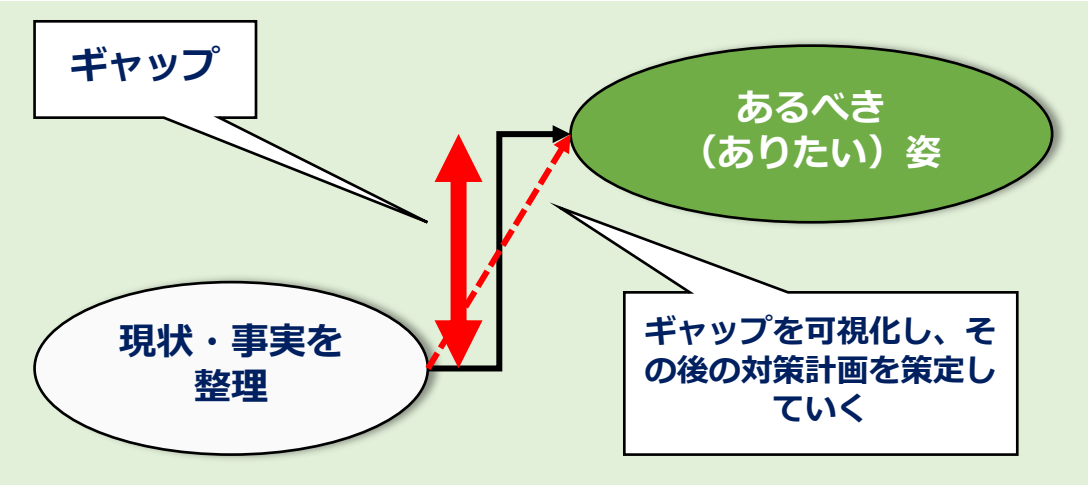
①各種法令・ガイドライン等に定められた取り扱い体制が組織内に整備されているか？
- 組織体制
- 規程/手順書/社内ガイドライン等
- 個人情報の取得/利用/特定/提供の原則が徹底されているか

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

ー　リスクアセスメント　ー

セキュリティ対策を検討していく上で**「リスクアセスメント」**は特に重要になります。
リスクを正しく評価できていなければ、その後の対策も有効なものとならない可能性が発生します。



【リスクアセスメントに関する重要事項】

- リスクアセスメントに対する**組織の取組み方を明確に定義**する
- 資産及びそれらの資産の**リスク所有者を特定**する
- それらの資産に対する**価値、脅威及び脆弱性を特定**する
- 現実的なインシデントの発生可能性、および**インシデント発生時に想定される事業的影響**のアセスメントを行う
- 分析した**リスクの優先順位つけ**を行い、適切な管理策を策定する（リスクの許容も含む）

お客様のITシステム環境や社内運用体制に関する状況確認、保有資産、各種法令・ガイドライン等への適合状況を抽出して整理し、その後の計画策定等をご支援します。

別途、技術的安全対策としての**セキュリティ診断（脆弱性診断、ペネトレーションテスト）もご提供可能**です。

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

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

ISMS認証取得支援

セキュリティコンサルティング、リスクアセスメント等を実施し、ISMSの公的認証取得の為の社内体制構築プロジェクトを支援します

ISO/IEC27001 - ISMSとは ？

・情報セキュリティマネジメントシステム
・リスクベースのマネジメント規格
・発行：2022年2月（日本語版JIS規格は2023年中に発行予定）
・ISO規格：ISO/IEC 27001:2022
・JIS規格：JIS Q 27001:2014

規格のねらいは、

「情報の機密性、完全性及び可用性を維持し、かつ、リスクを適切に管理しているという信頼を利害関係者に与えること」

ー　ISO/IEC27001の規格の構成（要求事項）　ー

PLAN

4.組織の状況

4.1　組織とその状況の理解
4.2　利害関係者のニーズ及び期待の理解
4.3　マネジメントシステムの適用範囲の決定
4.4　情報セキュリティマネジメントシステム

5.リーダーシップ

5.1　リーダーシップとコミットメント
5.2　方針
5.3　組織の役割、責任及び権限

6.計画

6.1　リスク及び機会への取り組み
　6.1.2 情報セキュリティリスクアセスメント
　6.1.3 情報セキュリティリスク対応
6.2　情報セキュリティ目的及びそれを達成するための計画策定

7.支援

7.1　資源
7.2　力量
7.3　認識
7.4　コミュニケーション
7.5　文書化された情報

ACT

10. 改善

10.1　不適合及び是正処置

DO

8.運用

8.1　運用の計画及び管理
8.2　情報セキュリティリスクアセスメント
8.3　情報セキュリティリスク対応

CHECK

9.パフォーマンス評価

9.1　監視、測定、分析、及び評価
9.2　内部監査
9.3　マネジメントレビュー

ー　ISMS構築のポイント　ー

No	概要
1	組織及び利害関係者のニーズと期待を理解し、適用範囲の決定
2	リーダシップを確立、情報セキュリティ方針及び目的を策定
3	リスクアセスメントプロセスの確立及び実施
4	ISMSの文書化、適用宣言書、セキュリティ対応計画の策定・実施
5	資源の決定及び提供、力量の確保、認識、コミュニケーションプロセスの確立
6	導入教育
7	内部監査制度確立及び実施、マネジメントレビューの実施
8	是正対応、継続的改善の実施

ー　サービス提供例　ー

各種法令・ガイドライン等への適合状況、リスクアセスメント、構想立案、実装支援まで、大別して以下の３つのフェーズにてご提供しております。

フェーズ１
各種法令対策向け対応支援
情報セキュリティクイックアセスメント

フェーズ２
情報セキュリティ構想立案支援
プロジェクト

フェーズ3
情報セキュリティ中期構想実装支援
プロジェクト

■各種法令対策向け対応支援
対顧客向け等緊急性を要する体制の整備と運用構築支援

■情報セキュリティクイックアセスメント
情報システム向け簡易リスクアセスメント

【参考期間】約2か月間

■情報セキュリティ構想立案支援PJ
・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
・経営陣向け説明資料作成支援
予算獲得資料作成支援

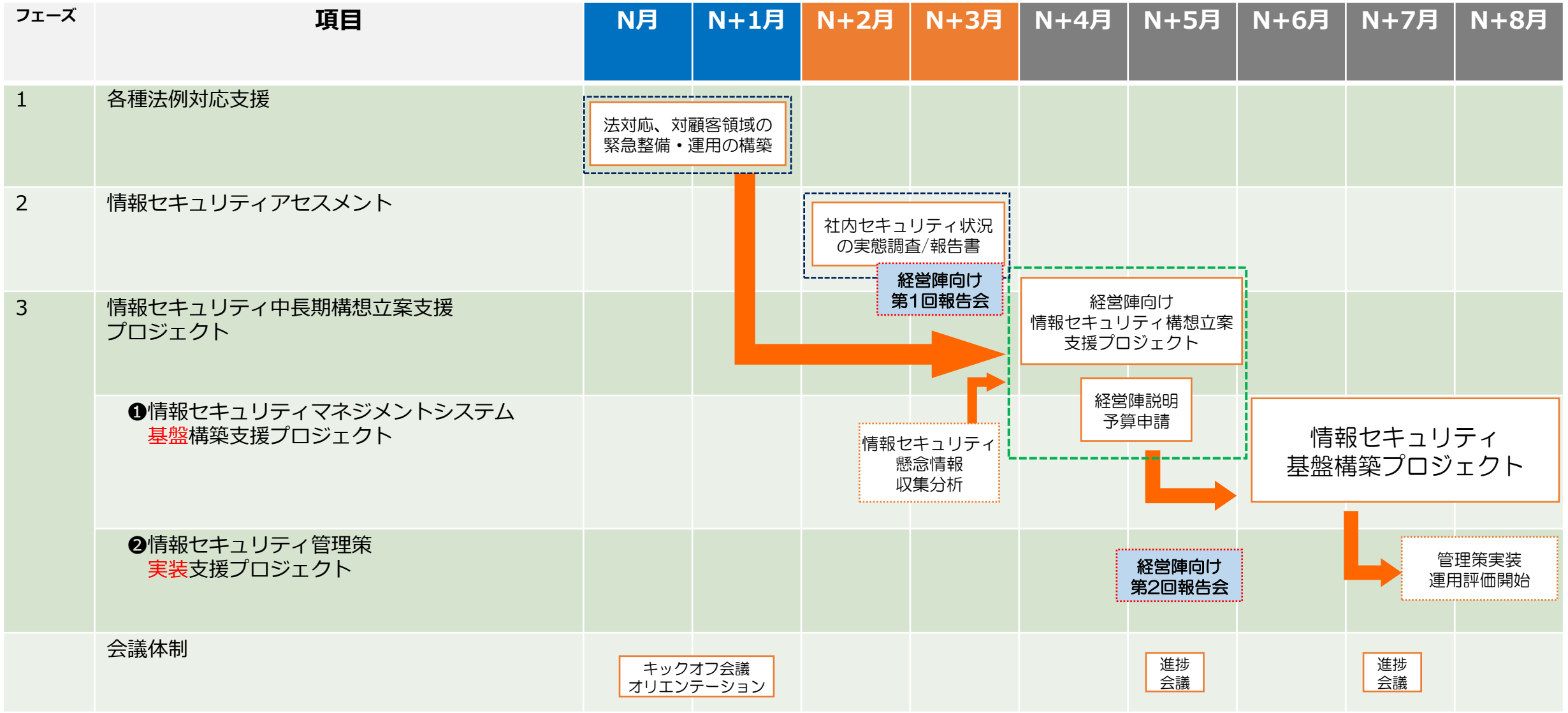
【参考期間】約2か月間

■情報セキュリティ中期構成実装支援PJ
・情報セキュリティマネジメントシステム構築基盤構築
・情報セキュリティ管理策実装支援

【参考期間】約5か月間

※参考期間は企業規模や対象とする範囲にて変動します。あくまでも参考とお考えください。

ー　プロジェクトスケジュール提供例　ー



ー　ISO/IEC27001：2013 →2022への移行支援　ー

ISO/IEC27001：2022への移行対応、更新審査対応についてもご支援が可能です。

【主な変更点：概要】

・管理策数
2013年版：114　→　93に減少（統廃合）
管理策数は、組織的管理策(Organizational controls)及び、技術的管理策(Technological controls)に集中
新規管理策は11個、そのうち 7 個は技術的管理策
それぞれの記述ボリュームは増加傾向

	管理策数	2013年版から継承した管理策	新規管理策
5. Organizational controls	37	34	3
6. People controls	8	8	0
7. Physical controls	14	13	1
8. Technological controls	34	27	7
全体	**93**	**82(88%)**	**11**

ー　ISO/IEC27001：2022　新規管理策　ー

新規管理策11個のうち 、7 個は技術的管理策です。

番号	タイトル	管理策の内容
5.7	Threat intelligence （脅威インテリジェンス）	情報セキュリティ脅威の関連情報の収集・分析による脅威インテリジェンス生成
5.23	Information security foruse of cloud services （クラウドサービス利用における情報セキュリティ）	クラウドサービスの取得、使用、管理及び終了プロセスの組織の情報セキュティ要件に沿った確立
5.30	ICT readiness forbusiness continuity （事業継続のためのICTの備え）	ビジネス継続性の目標及びICT継続性の要件に基づく、ICTに関する準備の計画、実装、維持及び試験
7.4	Physical securitymonitoring （物理セキュリティ監視）	施設への不正な物理的アクセスの継続的監視
8.9	Configurationmanagement （構成管理）	ハードウェア、ソフトウェア、サービス及びネットワークの構成の確立、文書化、実装、監視及び見直し
8.10	Information deletion （情報の消去）	情報システム、デバイス又はその他ストレージメディアからの情報の消去
8.11	Data masking （データマスキング）	アクセス制御やビジネス要件に沿い、法的要件を考慮したデータマスキングの使用
8.12	Data leakage prevention （データ漏洩の防止）	機微なセンシティブ情報を扱うシステム、ネットワーク及びエンドポイント機器における漏洩対策
8.16	Monitoring Activities （監視活動）	ネットワーク、システム、及びアプリケーションの継続的な監視
8.23	Web filtering （ウェブフィルタリング）	外部ウェブサイトへのアクセス管理
8.28	Secure coding （セキュアコーディング）	ソフトウェア開発へのセキュアコーディング原則の適用

Pマーク取得支援

セキュリティコンサルティング、リスクアセスメント等を実施し、Pマークの公的認証取得の為の社内体制構築プロジェクトを支援します

Pマーク（プライバシーマーク）とは ？

・日本産業規格「JIS Q 15001個人情報保護マネジメントシステム－要求事項」に適合し、個人情報について適切な保護措置を講ずる体制を整備している事業者等を評価し、その旨を示すプライバシーマークを付与し、事業活動に関してプライバシーマークの使用を認める制度

Pマーク制定の目的

・消費者の目に見えるプライバシーマークで示すことによって、個人情報の保護に関する消費者の意識の向上を図ること
・適切な個人情報の取扱いを推進することによって、消費者の個人情報の保護意識の高まりにこたえ、社会的な信用を得るためのインセンティブを事業者に与えること

Pマークは、

事業者にとって個人情報保護マネジメントシステム（PMS）を確立し、運用していることをアピールする有効なツールとして活用することが可能

ー　個人情報保護マネジメントシステム（PMS）とは？　ー

個人情報保護マネジメントシステム（PMS）とは、
「漏えい」「紛失」「滅失・毀損」「改ざん、正確性の未確保」「不正、不適正取得」「目的外利用・提供」「不正利用」「開示等の求めなどの拒否」を防ぐために整備し、**管理・監督するためのシステム**です。

PMSの審査基準は、JIS Q 15001をベースとして、以下のような各種法令による基準も加味されます。

・個人情報保護法
・個人情報保護法に関するガイドライン
・地方自治体による個人情報関連の条例
・業界団体の個人情報関連のガイドライン等

PMSとISMSの違い

PMSとISMSでは、以下のような違いがあります

項目	PMS	ISMS
規格	JIS Q 15001	ISO/IEC 27001 JIS Q 27001
保護対象	個人情報の取り扱いのみを対象	情報資産全般の取り扱いを対象 （技術情報や財務情報など）
有効範囲	原則、日本国内のみ	国際的に有効

ー　Pマーク取得のポイント　ー

No	概要
1	マニュアル、個人情報管理規程、個人情報保護方針の作成
2	個人情報の特定
3	関連する法規制、その他要求事項の特定
4	個人情報に対するリスクアセスメント
5	個人情報を含む業務を委託している取引先の評価
6	全従業員に対する教育
7	内部監査
8	マネジメントレビュー

ー　Pマーク取得工程例　ー

01 プロジェクトスタート

現状把握・計画策定
現状把握の為のヒアリング・活動計画書の作成
社内構築体制組成（プロジェクトチーム：マネジメントシステム・プログラム策定チーム）

02 文書作成

ＰＭＳ文書策定
ＰＭＳ基本方針作成／ＰＭＳ文書作成／基本規程の作成
内部規程類の作成、記録様式類の作成／現状把握・計画策定

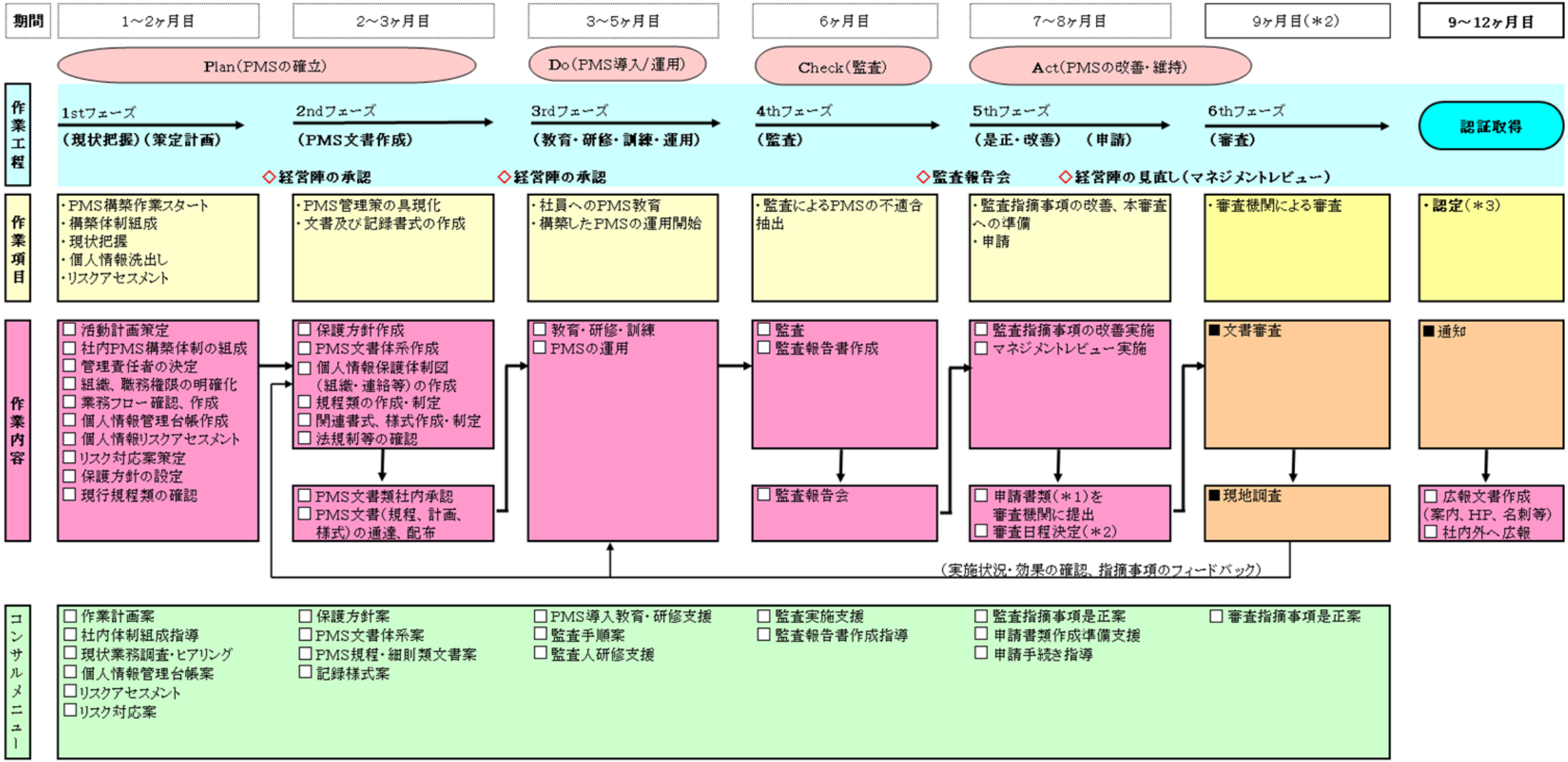
03 運用開始

教育・運用
ＰＭＳ文書の通達・教育訓練日常業務への定着化
導入教育研修・ＰＭＳの運用開始／ルールの遵守、励行・手順書の整備、確認記録類の整備、保管

04 申請

内部監査／申請・審査・審査指摘事項
監査の実施内部監査支援監査報告報告会
Pマーク申請書類作成支援

― Pマーク取得スケジュール例 ―



PMS：個人情報保護マネジメントシステム

＊1: 申請種類-申請書、登記簿謄本、PMS、組織定款、JIS Q 15001との対応表、教育実施記録、監査実施記録等。
＊2: 標準的日程として、＊1の申請書類提出から約3～4ヶ月後に、現地調査が行われる。
＊3: 月例の審査委員会にて、評議され認証書が発行される。

システムアドバイザリーサービス

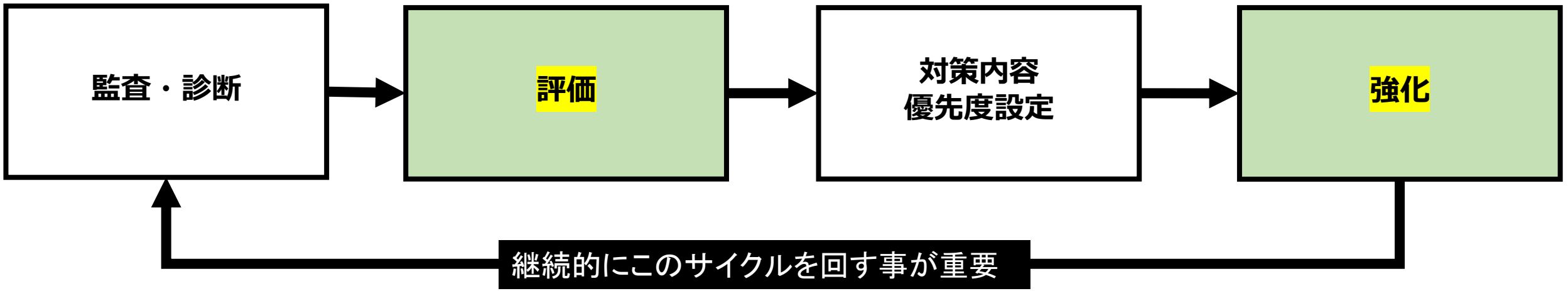
システムアドバイザリーサービス

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



ー　情報セキュリティ全般の考え方　ー

「予防」と「対応」

セキュリティインシデントが発生しないようにするには、適切な「情報セキュリティ対策」が必要です。
情報セキュリティ対策は、2つに大別され、1つは「事前対策」であり、もう一つは「事後対策」です。
事前対策は「予防」、**事後対策は「対応」**に分類されます。

リスク管理手法

体系的かつ網羅的にサイバーセキュリティ対策を行う上で参考となるのが、米国国立標準技術研究所（NIST）が作成・公開している「重要インフラのサイバーセキュリティを改善するためのフレームワーク（以下「サイバーセキュリティフレームワーク」）」です。
サイバーセキュリティフレームワークは、業界標準、ガイドライン、ベストプラクティスをとりまとめたものです。
重要インフラ保護政策を一貫として作成されたもので、主たるターゲットはインフラ事業者ですが、他の業界に置いてもモデルとして活用することが可能です。
サイバーセキュリティフレームワークは、サイバーセキュリティ対策をリスクマネジメントとして捉えており、サイバーセキュリティに関するリスク管理のコア機能を**「識別（特定）」「防御（保護）」「検知」「対応」「復旧」の5つのフェーズに分けて整理**しています。

代表コンサルタント紹介

ー　代表コンサルタント　ー

戸木　貞晴　MBA，CISSP

TOKI　Masaharu

中小企業診断士
高度情報処理技術者
システムアナリスト
システム監査技術者
ITコーディネータ
経営学修士　学術修士

元大手Sier 情報セキュリティ責任者　専門分野：情報セキュリティ

ISMS認証取得、プライバシーマーク取得、セキュリティ事件事故レスキューチーム、セキュリティ監査、システム監査業務に従事 大手製造業、ベンチャー企業、中小製造業、中小サービス業、地方銀行及びメガバンクの システム監査、セキュリティシステム導入、セキュリティ監査、セキュリティ診断、セキュリティアドバイザリーサービス等のコンサルティングサービスを大企業及び中小企業に多数サービス提供経験

顕著な功績：

①「大手通販会社」個人情報漏洩事故レスキュー責任者 事故発生直後の対応からISMS認証取得まで担当。情報セキュリティマネジメントシステムの安定運用までサービス提供 当該企業は、セキュリティ分野の著しい改善により経済産業大臣から表彰を受ける
②大手Sierにてセキュリティ関連製品及びサービスの企画、販促戦略立案の責任者を歴任
③セキュリティ講演会、セキュリティ教育授業開催多数（ビジネススクール情報戦略担当講師）

保有資格一覧

■セキュリティ関連
1. CISSP Certified Information Systems Security Professional
2. 公認情報セキュリティ主任監査人CAIS
3. 公認内部監査人CIA
4. 情報システム内部監査士
5. 高度情報処理技術者
   システム監査技術者
   情報セキュリティアドミニストレーター
6. 元ISMS審査員
7. 元プライバシーマーク審査員

■情報システム関連
1. 高度情報処理技術者 システムアナリスト
2. 高度情報処理技術者 上級システムアドミニストレータ
3. プロジェクトマネジメントスペシャリスト（PMS）資格取得
4. ITコーディネータ試験合格・IT研修修了
5. 元CCNA（Cisco Certified Network Associate）

■その他
1. 国内ビジネススクール　経営情報特任講師
2. 中小企業基盤整備機構（独法）CIO育成専門家

セキュリティ診断サービス

技術的安全対策措置

― セキュリティ診断サービス ―

各種法令対策や公的認証取得における技術的安全対策の可視化に必要な各セキュリティ診断もご提供しております。

Security Blanket

セキュリティ診断サービス提供内容例

クラウドコンプライアンス診断

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

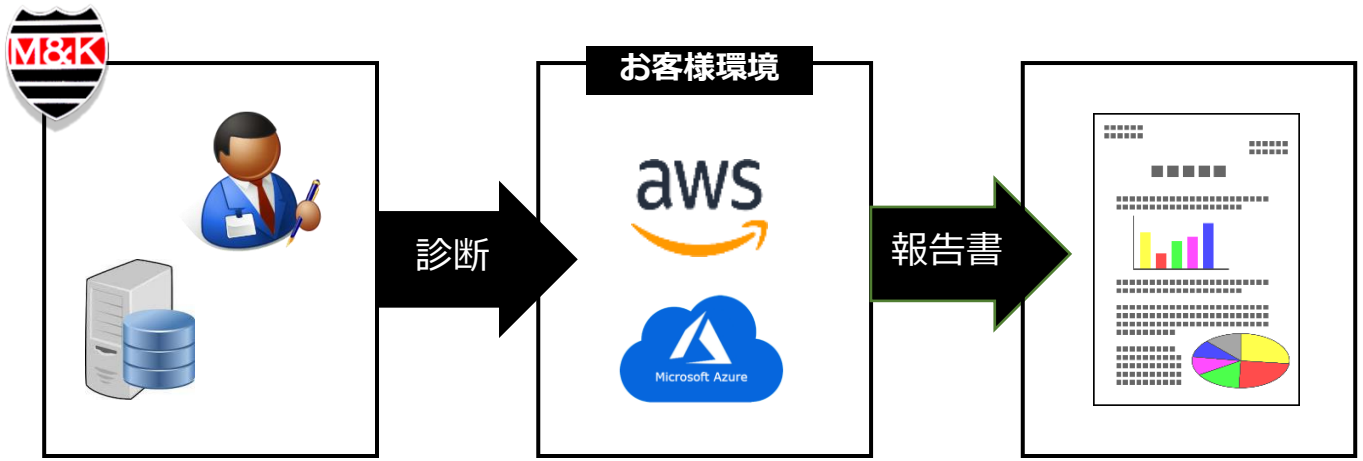
アプリケーションのソースコードに関するセキュリティ上の問題点を、診断コンサルタントが査閲し、可視化された問題点と対策を提示します。

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。

クラウドコンプライアンス診断

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

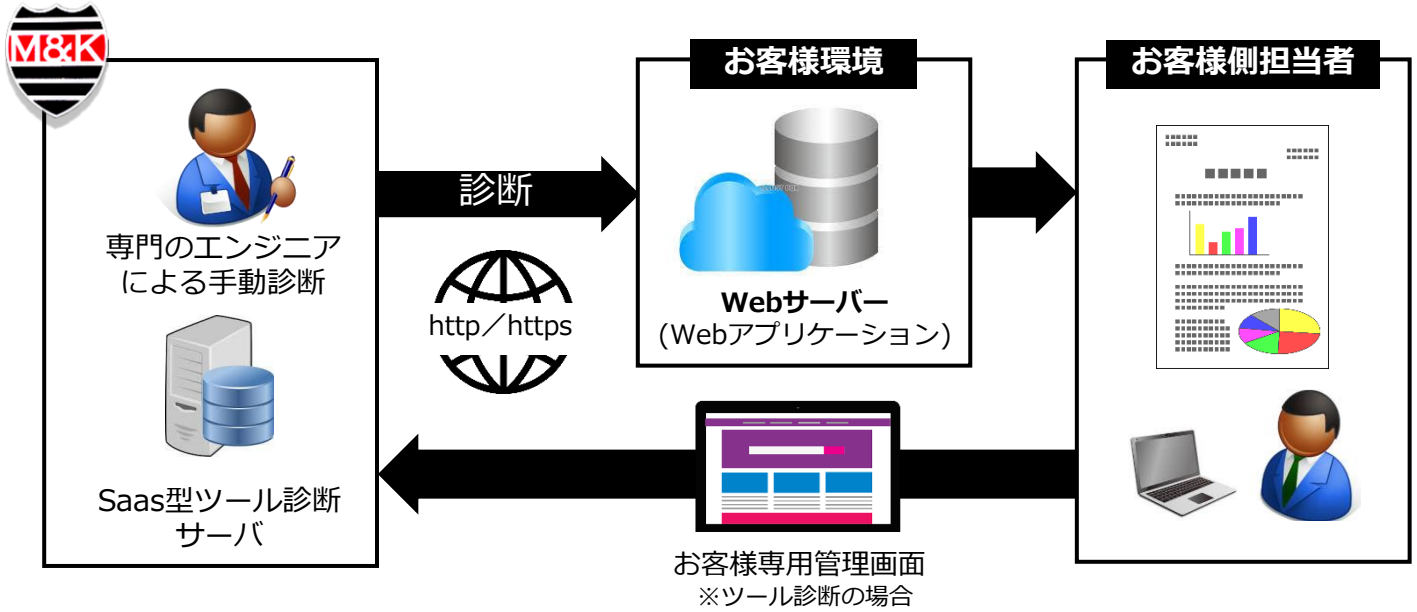
Microsoft Azure

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

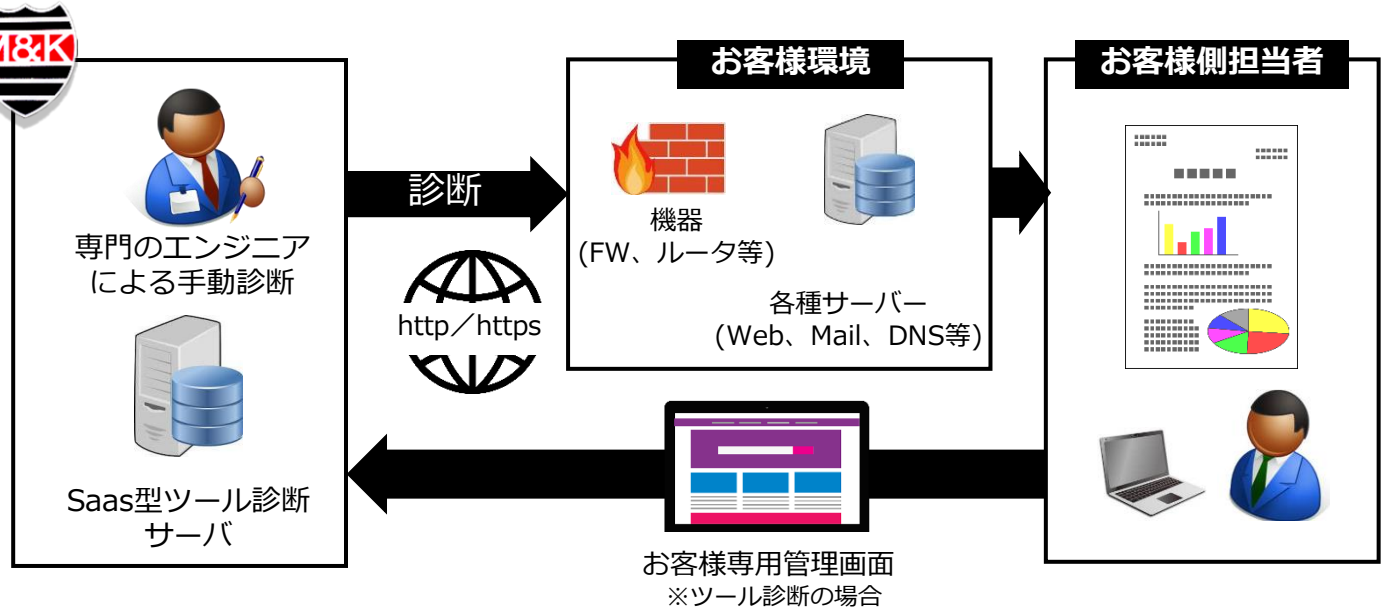
サイト全体はツールで安価に診断し、重要な機能だけはエンジニアによる高度な診断を実施したい時など、手動診断とツール診断を組み合わせた最適な診断方法と提供します。

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

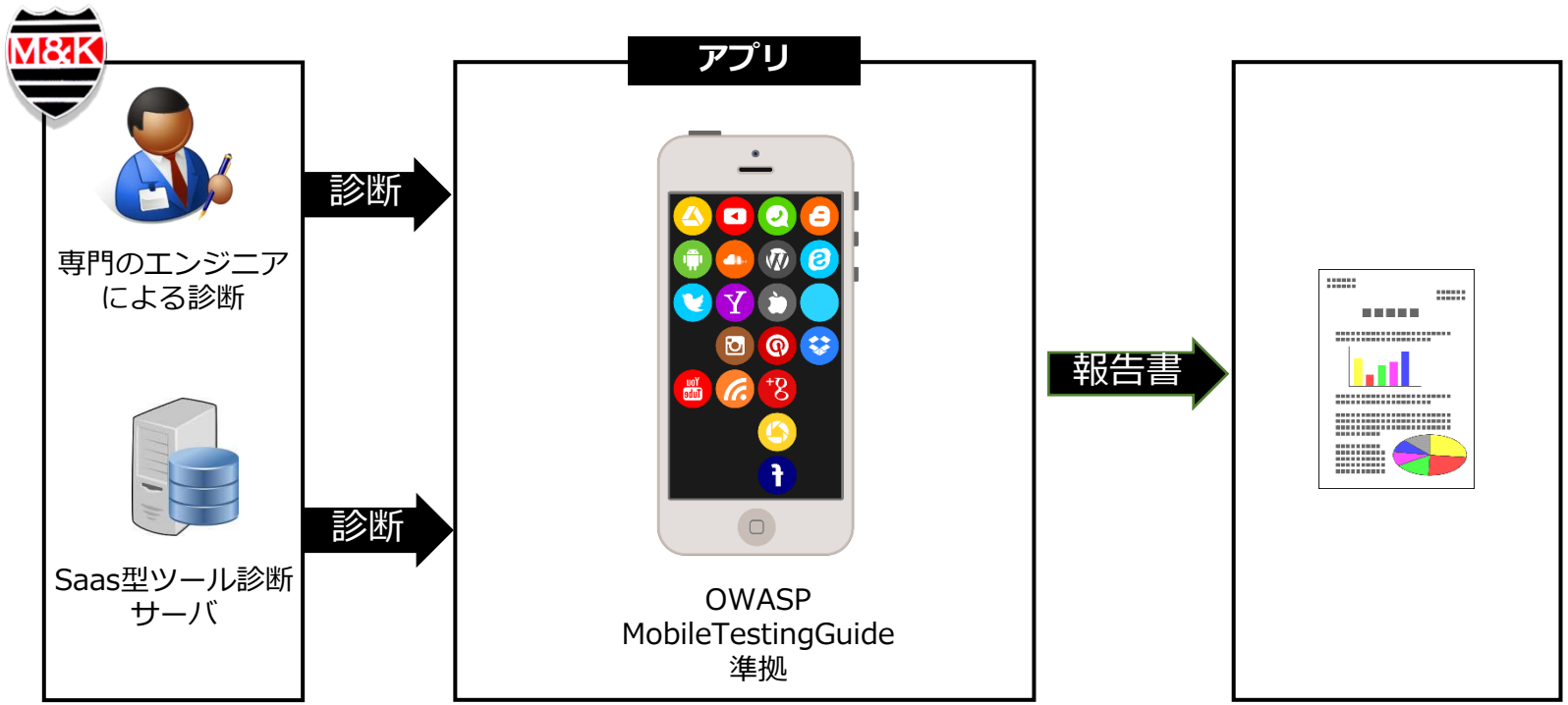
サイト全体はツールで安価に診断し、重要な機能だけはエンジニアによる高度な診断を実施したい時など、手動診断とツール診断を組み合わせた最適な診断方法と提供します。

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。

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。



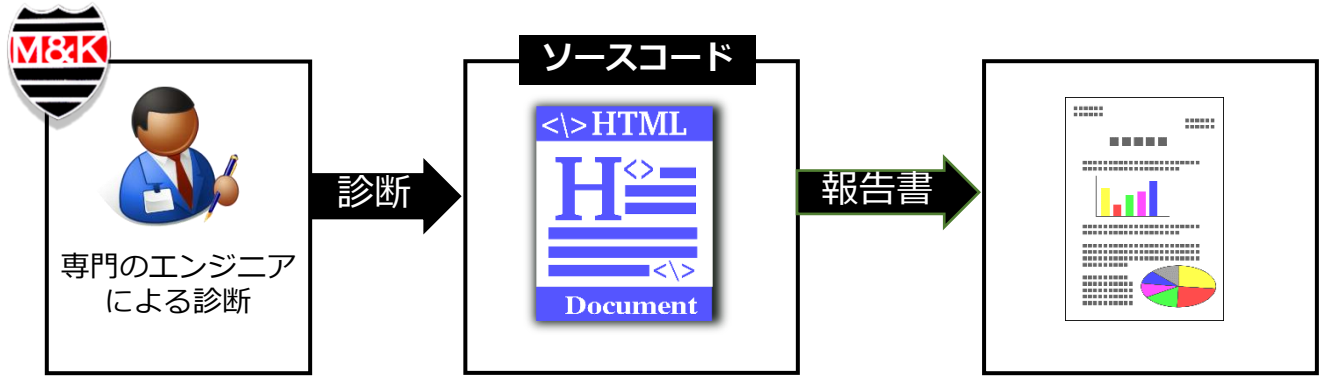
・モバイルアプリのソースコード一式をお預かりします

・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。



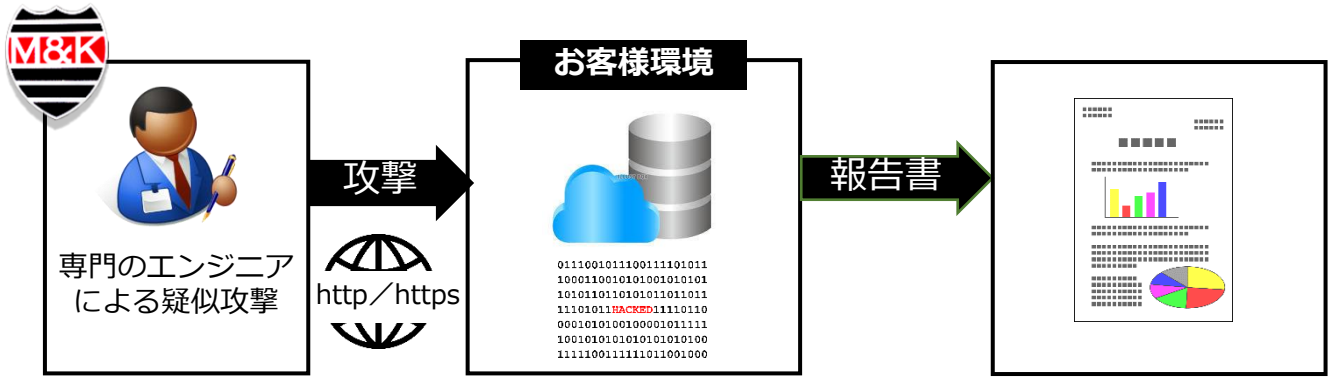
・Webアプリケーションのソースコード一式をお預かりします

・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

Appendix

セキュリティとは何か？

セキュリティには、大きく分けて２種類の考え方があります。

①情報セキュリティ

情報セキュリティとは、企業が保有する**情報**を保全する事です。
必要なデータ・システムが必要な時に利用でき、不必要なアクセスを制御し、漏洩等の事故が発生しないように管理・維持する事が求められます。
これらは、「**情報セキュリティの3要素**」と呼ばれる以下の3つの項目を維持する事で安全な状態が保たれていると言えます。

- **機密性(Confidentiality)**
  機密性とは、**許可されたものだけが利用できるように設計されていること**を指します。
  許可されたものとは、ユーザ（人）だけではなく、クライアント端末（コンピュータ）などの物に対しても、「アクセス許可（権限）」を適切に与える必要があります。
  特定の端末からのアクセス限定にすることや2要素認証を取り入れることで機密性の高いシステムを維持することができます。

- **完全性(Integrity)**
  完全性とは、**改ざんや破壊が行われておらず、内容が正しい状態にあること**を指します。
  ファイルの中身が不正に書き換えられていないこと、ネットワークなど経由する間に情報が失われていないことなどを証明する必要があります。

- **可用性(Availability)**
  可用性とは、**システム障害が発生しにくく、障害が発生しても影響を最小限に抑え、復旧までの時間が短く設計されていること**を指します。
  機密性や完全性が維持されていても、システム自体が使えなくては意味がありません。サイバー攻撃の際なども、可用性の高い状態を維持するには常にシステムの状態を監視し、健全な状態である事を確認するする必要があります。

②サイバーセキュリティ

情報セキュリティに関する**「情報」の保全に加えて、「情報システム」、「情報通信ネットワーク」も保護対象にしたもの**になります。
2014年に施行されたサイバーセキュリティ基本法において定義されています。

セキュリティ対策を実施する上では、対策の範囲の明確化、それらに対する現状を正確に把握、その評価結果に基づいた適切な対策の実施、定期的に再評価、これら一連のサイクルを定期的に継続し、理想とする姿に近づけていく事が重要になります。

サイバーセキュリティ基本法

サイバーセキュリティ基本法とは？

サイバーセキュリティ基本法（平成26年（2014年）法律第104号、以下「基本法」という）2条に定義されている「サイバーセキュリティ」を前提としています。
この法律は、サイバーセキュリティを「…電磁的方式…により記録され、又は発信され、伝送され、若しくは受信される情報漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム（情報通信ネットワーク又は電磁的記録媒体を通じた電子計算機に対する不正な活動による被害の防止のために必要な措置を含む。）が講じられ、その状態が適切に維持管理されていること」と定義しています。

即ちサイバーセキュリティ基本法とは、**データ、情報システム、情報通信ネットワークを安全に保つための対策として、それを維持すること**を意味しており、かなり広い定義であると言えます。

保護対象となる「情報」とは？

「情報」には形がありません。何らかの記録媒体に保存されたデータはもちろん、誰かが発した言葉や、人の脳の中に記録されているものも「情報」にあたります。
サイバーセキュリティの文脈において保護対象となる「情報」は、電磁的方式によりやり取りされるもの、つまりサーバや端末、記録装置などの記録媒体に保存されたデータに限定されます。

外部からの攻撃に関する対策とは限らない

サイバーセキュリティ対策は、外部からのサイバー攻撃（サイバーテロ、サイバー諜報活動（サイバーインテリジェンス、サイバーエスピオナージ）を含む）への対策はもちろんのこと、他にも例えば、企業の従業員による**機密性の高い情報（データ）の不正な持ち出し等の内部不正への対策、不正送金への対策**などもサイバーセキュリティに含まれます。
さらに、基本法の定義には、**情報システムの安全性および信頼性の確保**の対策も該当しますので、**災害などによる大規模停電や、人為ミスなどによって企業の情報システムに障害が発生した場合に、迅速に復旧するための措置**に関しても、サイバーセキュリティに含まれることになります。

サイバー攻撃はインターネットを通じた攻撃だけではない

基本法の定義における「情報通信ネットワーク又は電磁的記録媒体を通じた電子計算機に対する不正な活動」という文言は、サイバー攻撃を念頭に置いたものであり、これによる被害を防ぐために必要な措置を講じ、維持することもサイバーセキュリティの定義に含まれます。即ちインターネットを通じたオンラインの状態だけではなく、**USBメモリなどの記憶媒体の持ち込みや、フロア入退出による施錠管理などのオフライン状態の物理的なセキュリティ対策**も講じなければいけないという事になります。

情報セキュリティポリシーの作成

情報セキュリティの対策基準

情報セキュリティの脅威は**「人的脅威」**、**「技術的脅威」**、**「物理的脅威」**に分かれます。

人的脅威

従業員の不正や偶発的な誤りで発生してしまう脅威を「人的脅威」と呼び、**「意図的な脅威」**と**「偶発的な脅威」**に分かれます。
「意図的な脅威」は、機密情報を持ち出す「不正持出し」や、情報の盗み見、ソーシャルエンジニアリングなど、「偶発的な脅威」は、メールの誤送信や標的型攻撃メール受信によるウイルス感染、USBメモリの紛失などが挙げられます。
原因は、**従業員の情報セキュリティに対する意識の低い事**や、**社内で規定が定められていない**などの理由が考えられます。

技術的脅威

悪意のある第三者からの攻撃などによる脅威は「技術的脅威」と呼びます。例えば不正アクセスやネットワークの盗聴、通信の改ざんだけではなく、OSやミドルウェア、アプリケーションの脆弱性をついた**セキュリティ上の不具合を狙った脅威**もあります。コンピュータウイルスやマルウェアに感染させるのもこれに該当します。
攻撃者は常に対策が不十分なシステムを探しています。被害を未然に防ぐ為にも**システムやコンピュータの健全性を定期的に確認する事が重要**です。

物理的脅威

情報資産の破壊などによって発生する脅威を「物理的脅威」と呼び、地震や火災、水害、病気によるパンデミックなどの災害は**「環境的脅威」**と呼ばれます。
その他、**コンピュータの破壊や窃盗**なども考えられます。
システムを構成している**サーバの障害やハードウェア故障などによるシステム停止**で、復旧ができなくなってしまうことなども挙げられます。

これらの3つの脅威に対して、自組織の基本的な考え方を示したものが**「情報セキュリティポリシー」**であり、適切な対策がなされている状態であれば、情報セキュリティ対策の基準が保たれていると言えます。

企業などの団体では情報セキュリティ対策を統一するために、**文書で定める**ことが必要になります。

脆弱性診断とは何か？そもそも脆弱性って？

「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。
専用のエンジニアによる高度な診断を提供する手動診断や、ユーザ側にて手軽に実施可能なツール診断など様々なタイプの脆弱性診断が存在します。

①エンジニアによる手動診断

専門性を持ったエンジニアが、WEBサイトやWEBアプリケーションの構造や特性を理解した上で、脆弱性の有無を確認します。診断項目によってはツールでの診断も組み合わせながら、幅広く深い診断を実施します。新規公開予定のシステムや、大幅な改修・機能追加があった際には公開前には実施しておく事が推奨されます。

②ツール診断

エンジニアによる手動診断と比較すると、診断できる幅や深さは簡易的にはなりますが、手軽に費用対効果の高い診断が実施できるのが「ツール診断」です。
リリース後のシステムに対して定期的に脆弱性の確認を実施したいという場合におすすめです。

新規開発されたシステムやソフトウェアには、必ずと言ってよいほど脆弱性が潜在しています。
特にWEBアプリケーションに関しては、古くから存在する基本的な脆弱性への対策が出来ていない場合、重大なセキュリティ事故に繋がる可能性が非常に高くなります。

企業価値を守る為にも、目的や用途に合わせた適切な診断を定期的に実施し、安心・安全はシステム環境を整えておく事は大変重要です。

	手動診断	ツール診断
推奨用途	新規公開前のシステムや、個人情報などの重要な情報を保有しているシステムの診断に有効 大規模な改修や機能追加後にも実施する事を推奨	手軽に脆弱性診断を実施したい場合 リリース後のシステムの軽微な改修や機能追加後の診断や、 OSやミドルウェア等に関する定期的な脆弱性の確認に有効
費用	規模によるが、高額になるケースが多い	安価なものが多く、定額で無制限で利用できるタイプもあり

セキュリティインシデント発生時の損害は？

企業にとって、セキュリティインシデントの発生は金銭的な損害だけでは無く、ブランドイメージの失墜や信頼損失など、その影響は計り知れないものがあります。
今や、**セキュリティ対策は企業価値を守る為に必要不可欠**なものと言っても過言ではありません。

セキュリティ対策に上限はありません。
「ここまでやれば絶対に安全に」というような線引きはできませんが、**守るべき資産に見合った適切な投資**をして対策を講じる事が重要です。

重要な情報が漏洩してしまった場合の賠償や、事業が停止に追い込まれた際の遺失利益、ブランドイメージ低下による業績悪化などの最悪の事態を想定し、
経営課題と認識して適切な予算を配分する事を推奨します。

種類	具体的損失
費用損害(事故対応損害)	被害発生から収束に向けた各種事故対応に関して自社で負担する費用
賠償損害	情報漏洩などにより、第三者から損害賠償請求がなされた場合の被害
利益損害	ネットワークの停止などにより、事業が中断された場合の利益損失
金銭損害	ランサムウェアなどによる直接的な金銭の支払い
行政損害	個人情報保護法において命令違反等により化される罰金
無形損害	風評被害、ブランドイメージの低下

国内における損害事例

	事故概要と主な対応	主な支出費目	左記費用の支出額（※）
	**公式オンラインショップ**におけるシステム上の脆弱性を突かれ**不正アクセス**を受けた結果、会員登録者の顧客情報、クレジットカード情報が漏えい。 被害者へのお詫び・注意喚起を、メール・郵送にて実施。	**個人情報漏えい見舞費用**	**約4億円**
	**自社開発アプリのサーバ**が**不正アクセス**を受け、保存されていた個人情報が漏えい。被保険者のコールセンターへ数万件を超える問合せがあり、コールセンター対応者の増員・外部委託を実施。	**コールセンター委託費用**	**約5,000万円**
	飲食店を展開する企業本社の**コンピュータシステム**が**マルウェア**に感染し、店舗における電子決済が利用不可に。店舗における決済をアナログで対応するため、約1週間にわたり社員の残業、休日出勤が発生。	**超過人件費**	**約7,000万円**
	実在する取引先A社を装った**なりすましメールの添付ファイルを開封**したことにより、**マルウェア**に感染。他の取引先への拡散していることが発覚し、原因調査・被害範囲の特定、再発防止策の策定について迅速な対応・報告が余儀なくされた。	**原因・被害範囲調査委用**	**約3,000万円**

※支出額とは、事故により実際に生じた金額であり、弊社の保険金支払額ではありません。

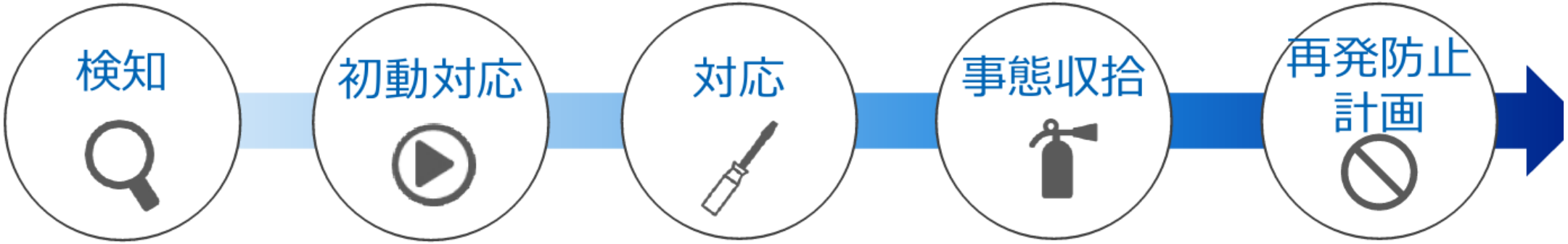
- ✓ サイバー事故が発生すると、被害者からの問い合わせや見舞対応に関する費用、臨時対応に係る超過人件費など、多額の費用支出が発生します。
- ✓ 事故発生時には、事故の裏付けとなる証拠の抽出や、サイバー攻撃による被害状況の特定を行う「フォレンジック調査」が必要となります。「フォレンジック調査」には、専門知識とノウハウを要するため、端末1台あたり約20～100万円×端末台数分の費用が発生することがあります。

対応プロセス例と想定費用

ケーススタディ（架空）

業種・規模：　製造業、社員数約1,000名、売上高約300億円
事故・被害：　標的型メール攻撃により、社内PC10台がマルウェアに感染。取引先の機密情報および顧客の個人情報約60,000件が流出
経緯：　セキュリティ運用管理会社に情報流出の可能性を指摘され発覚。その後本格調査に乗り出し、事故・被害の全容を把握

求められる対応



検知	初動対応	対応	事態収拾	再発防止計画
• 検知内容の精査	• 影響の調査 • 影響箇所・範囲の特定　等	• ログ収集 • 証拠保全 • 原因・被害調査 • バックアップ復元　等	• 見舞金 • 広報対応 • 弁護士費用　等	• 再発防止のための各種施策(技術対策、教育、ルール作り等)の計画策定

想定費用

検知	初動対応	対応	事態収拾	再発防止計画
(社内で対処)	約 500 万円	約 3,000 万円	約 4,000 万円	約 500 万円

※ 上記金額はあくまで想定です。個社の状況、事故の内容、対応業者等により金額は変わります。

サイバーセキュリティ経営ガイドライン

サイバーセキュリティ経営ガイドラインとは？

サイバーセキュリティ経営ガイドラインとは、**サイバーセキュリティが経営課題**であることを前提としつつ、**経営者が認識すべき3つの原則**と、**サイバーセキュリティ経営における重要な10項目**を上げているガイドラインのことです。独立行政法人情報処理推進機構（IPA）は「サイバーセキュリティ経営ガイドライン ver2.0実践のためのプラクティス集（第2版）」を公開しており、経営ガイドラインで示された事項を実践するための参考となります。

企業のサイバーセキュリティは、**全社的に組織的に経営課題として**リスクマネジメントを行う必要があります。近年の企業はITやICTに対する依存度が高まっており、インシデント発生を含めサイバーセキュリティに関するリスクをゼロにすることは難しく、セキュリティインシデントが発生した場合に業務に与える影響も大きくなっている背景があります。

企業の取り組みとしては、セキュリティ対策の実施を「コスト」と捉えるのではなく、**将来の事業活動・成長に必須なものと位置づけて「投資」と捉える**ことが重要とされています。

サイバーセキュリティを経営の問題として考える上では**「経営ガイドライン」**、もしくは一般財団法人日本経済団体連合会が公開した**「サイバーリスクハンドブック」**が参考になります。

【参考文献】

・経済産業省　独立行政法人情報処理推進機構（IPA）発行：サイバーセキュリティ経営ガイドラインver2.0実践のためのプラクティス集（第2版）
https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v2.0.pdf

・一般財団法人日本経済団体連合会（経団連）発行：サイバーリスクハンドブック　取締役向けハンドブック日本語版
http://www.keidanren.or.jp/policy/cybersecurity/CyberRiskHandbook.pdf

セキュリティ診断の種類と違い

WEBアプリケーションやシステムプラットフォームに関するセキュリティ診断は、専門のエンジニアが実施する手動のタイプや、ユーザ側にて手軽に実施できるツールタイプのものなど様々なものがありますが、大別して３種類に分類できます。

①システムに潜在するリスクを可視化する「脆弱性診断」

WEBアプリケーションのソースコードや、システムプラットフォームに使われているOS／ミドルウェア、ネットワークに潜在する「脆弱性を可視化」するものです。
可視化された脆弱性は適切な対策を施す事により、セキュリティインシデントのリスクを大幅に減らす事が可能です。

②セキュリティ対策の有効性を検証する「ペネトレーションテスト（侵入テスト）」

脆弱性診断があくまでもリスクの可視化であるのに対し、ペネトレーションテストは、専門のエンジニアが実際の攻撃に用いられる手法を使い、対象システムへの侵入を試みる疑似攻撃を実施します。
現時点でのセキュリティ対策の有効性や、脆弱性診断で可視化されたリスクへの対処状況などを把握する事が可能となり、システムの堅牢性が明確になります。

③クラウドサービス利用における管理項目の「セキュリティ設定診断」

クラウドサービスの急速な普及に伴い、設定ミスによるセキュリティインシデントの発生も増加の一途を辿っています。ID／PWの設定不備や、クラウドストレージの閲覧権限設定不備等に起因する重要情報の漏洩等が代表的な被害です。
このような事故を未然に防ぐ為に、各クラウドサービスにはそれぞれベストプラクティスとされているガイドラインが存在します。セキュリティ設定診断は、現在のクラウド利用における設定をガイドラインと照合し、その適合状況を可視化するのものです。

	脆弱性診断	ペネトレーションテスト	クラウドセキュリティ設定診断
目的	潜在する脆弱性やリスクの可視化	システムへの侵入可否の確認	クラウド利用時のセキュリティ設定状況の可視化
診断方法	ツール診断と手動診断の組み合わせが主流	主にエンジニアによる手動診断が主流	主にツール診断が主流
効果	診断結果に基づいた適切な対処が可能	セキュリティ対策の有効性確認、明確化	クラウド利用におけるガイドラインとの適合状況把握

高いセキュリティレベルを保ったシステム運用を実現する為には、これら3種類の診断を組み合わせて**適切な診断を定期的に実施**する事が重要です。

適切な診断とは？

診断サービスを検討する際は、守るべき情報資産や企業価値などを考慮し、万が一セキュリティ事故が発生した際の損害等を見据えた内容で実施する事を推奨しています。
現状のアセスメントをしっかりと実施し、想定される被害や想定損害額などを把握し、それらを未然に防ぐために必要な診断を、適正な費用で実施する事が重要です。

①エンジニアによる手動診断、ペネトレーションテスト

高度な専門性を持ったエンジニアが、対象システムの診断を手動で実施し、実際の脆弱性を悪用した攻撃が可能かどうか確認します。
対象システムの規模にもよりますが、熟練のエンジニアが担当する為、費用も高額になる事が多いですが、**ECサイトのようなクレジットカード情報を扱うシステムや、大量の個人情報を保有しているようなシステム**の場合は、必ず実施する事を推奨しています。
新規に開発したシステム等に関しても、初回公開前には手動での診断を実施する事が望ましいと考えます。

②ツールによる自動診断

対象システムによって向き不向きはありますが、安価に費用対効果の高い診断を実施したいような際はツールによる自動診断もおすすめです。
システムの規模やサイトの画面数等に依存せず、定額での診断が可能です。
且つ、**手動診断と比較すると短納期で診断結果を得る事が出来ます。**
急に診断が必要になった際にまずは実施してみるという場面や、過去に手動診断を実施したシステムへの定期診断等でのご利用にも最適です。
ただし、**手動診断と比較した場合、ツールではカバーしきれない項目もあり、複雑な構成のシステム等においては、細部までの診断が出来ない事もあります。**
ログイン機能を有するシステムにおける認証機能の有効性確認や、ECサイト等におけるセッション管理機能などの診断はツールでは出来ません。

	エンジニア手動診断	ツール自動診断
推奨される診断対象	・ECサイト ・大量の個人情報を扱うシステム ・医療／金融関連システム ・新規公開前のシステム ・ログイン機能の有効性確認 ・セッション管理機能の有効性確認	・企業のコーポレートサイトなど、攻撃による影響が小規模と想定されるサイト ・静的なコンテンツのみのサイト ・定期的な継続診断利用
メリット	・細部まで精度の高い診断が可能 ・実施の攻撃手法に沿った診断により、セキュリティ対策の有効性が確認可能	・安価で網羅的な診断が可能 ・オンデマンドでいつでも実施可能 ・診断期間が短い（数時間から1日程度） ・診断結果が即時出力可能
デメリット	・エンジニアが稼働する為、費用が高額になるケースが多い ・診断期間が長い（数日から数週間）	・診断項目に制限があり、細部まで診断できない事がある

脆弱性が見つかったら？

悪意のある攻撃者は、代表的な脆弱性が潜在しており、容易に攻撃ができるWEBアプリケーションを日々探しています。
脆弱性の存在を正しく把握し、プログラムの特性やアプリケーションの機能に応じた適切な対策を取ることより、被害の多くは未然に回避できると言われています。

①適切な改修や追加対策を実施する

可視化した脆弱性に応じた**プログラムの改修や、動作環境のアップデートなど、検出された脆弱性に対する改修を実施**します。
ソースコードの改修等による根本的な脆弱性対策が望ましいですが、なんらかの制約により、改修が難しいケースもあります。
そのような場合は、WEBアプリケーションへの攻撃を防御する事に特化した**WAF（WEBアプリケーションファイアウォール）の導入**を推奨します。

・WAF（WEBアプリケーションファイアウォール）
一般的なファイアウォールがネットワークレイヤーを防御するのに対し、WEBアプリケーションレイヤーへの攻撃を防御する事に特化した製品がWAFです。
様々な製品やサービスがありますが、いずれもWEBアプリケーションに対して高い防御力を発揮します。
最近では、運用面やコスト面で導入がし易く、新たな脆弱性への対応も迅速な**クラウドサービス型（SaaS型）のWAF**が評価されています。

②定期的な再評価を実施する

脆弱性対策を実施し、公開したWEBアプリケーションに関しても、**定期的な再評価を実施**する事をお勧めします。
特に、WEBアプリケーションの動作環境、プラットフォームに利用される事が多い、ミドルウェアやオープンソースソフトウェアには、**日々新たな脆弱性が発表**されています。
四半期に一度や、半年に一度など、運用面におけるポリシーを明確に定め、それに沿った運用を継続することが重要です。
なお、定期的な確認に加えて、WEBアプリケーションの機能追加や、WEBサイトのページ改修などを実施した際には、その都度脆弱性の有無を確認する事が推奨されます。
また、WEBサイトの異常を検出する**改ざん検知の仕組みなどを導入**する事により、外部からの攻撃を迅速に把握する事が可能になります。

IPA 独立行政法人情報処理推進機構からも安心なWEBサイトの作り方についての指針が公開されています。

・安全なウェブサイトの作り方
https://www.ipa.go.jp/security/vuln/websecurity.html

セキュリティ10大脅威（2023年版）

順位	脅威	取組み例
1位	ランサムウェアによる被害	組織的教育／ネットワーク、エンドポイントの防御
2位	サプライチェーンの弱点を悪用した攻撃	規則の徹底／委託先組織の管理／ポリシーの統一化
3位	標的型攻撃による機密情報の窃取	組織的教育／ネットワーク、エンドポイントの防御
4位	内部不正による情報漏えい	組織的教育／重要情報の管理手法
5位	テレワーク等のニューノーマルな働き方を狙った攻撃	組織的教育／ネットワーク、エンドポイントの防御
6位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	脆弱性情報の収集と対応／資産の把握
7位	ビジネスメール詐欺による金銭被害	組織的教育／規則の徹底／コンプライアンス管理
8位	脆弱性対策情報の公開に伴う悪用増加	脆弱性情報の収集／資産の把握
9位	不注意による情報漏えい等の被害	組織的教育／メール誤送信対策
10位	犯罪のビジネス化（アンダーグラウンドサービス）	組織的教育／サイバーセキュリティ事情の理解

【出展】 IPA　情報セキュリティ10大脅威 2023
https://www.ipa.go.jp/about/press/20230125.html

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/