Security Service Guide

セキュリティサービスガイド

BBSec 緊急コンタクトセンター

☎0120-085490

（24時間365日受付）

株式会社ブロードバンドセキュリティ

便利で安全なネットワーク社会を創造する

お客様の情報資産を守り、成長を支援するために

BBSecは、悪意ある攻撃から組織の情報資産を守り、組織がその情報資産をもとに適正に成長していくことを支援するセキュリティ専門事業者です。対策に欠かせないIT/組織両視点からの各種サービスは、お客様の規模や対策の推進状況にかかわらず、今必要とする最適な「答え」を提供します。

BBSec のサービス MAP

セキュリティ監査・コンサルティング

お客様システムの可視化/課題抽出/課題解決を目的とした、組織全体に対するセキュリティ支援サービス。IT・組織両面からセキュリティの盲点を発見し、実現可能な解決策を提示いたします。
また、オンラインビジネス成功に向けた調査サービスを中心に、具体的なデザイン改善・システム開発、効率的なサイト運営をサポートします。

脆弱性診断

お客様システムに潜む脆弱性を検証し、改善案を提示するサービス。時々刻々と変化する外部環境に対応していくために、新規開発時だけでなく、運用中のシステムにも定期的に実施することを推奨しています。

情報漏えいIT対策

慎重かつ堅実な継続的作業を求められるセキュリティ運用を、セキュリティのプロフェッショナルが24時間・365日体制で支援いたします。

セキュリティ監査・コンサルティング：サービス一覧

コンサルティング

情報セキュリティ・アドバイザリ P.9
企業のセキュリティニーズを可視化し、情報セキュリティ強化に向けた組織的な体制づくりを社内ルール/ 情報システム両面から支援します。

AIサービス提供者・利用者向け サイバーセキュリティ対策支援 P.10
経験豊富な情報セキュリティ対策のスペシャリストが『AI事業者ガイドライン』に基づくAIガバナンスの実践を支援します。

ランサムウェアに対応したIT-BCP策定支援 P.11
事業継続を揺るがす脅威、サイバー攻撃を、これまでとは性質の異なる脅威と捉え直し、状況やニーズに合ったサイバーセキュリティIT-BCP策定を支援します。

「防衛産業サイバーセキュリティ基準」準拠支援 P.12
経験豊富な情報セキュリティ対策のスペシャリストが「防衛産業サイバーセキュリティ基準」準拠をご支援いたします。

自動車部品業界向け 情報セキュリティ対策支援 P.13
自工会/部工会・サイバーセキュリティガイドラインV2.2に基づき情報セキュリティ課題に対する対策を支援します。

SWIFT CSCFに基づく 外部評価、内部評価支援 P.14
日本(内資)企業初の CSP assessment provider認定監査機関として、国内および海外の事業体様に向けて、SWIFT CSCF 準拠を支援します。

ISO/IEC 27017 クラウドセキュリティ認証取得支援 P.15
クラウド提供事業者/利用事業者双方の指標となるISO/IEC27017に基づく ISO/IEC 27017クラウドセキュリティ認証取得を支援します。

CSIRT 構築・運用支援 P.16
セキュリティインシデントに立ち向かう社内組織CSIRTのプランニング / 構築 / 運用を専門家の立場から支援します。

インシデント初動対応準備支援 P.17
拡大するサイバーセキュリティの脅威に対応するために今すぐにでも準備すべきことを明確にし、お客様の実情に合わせた初動対応準備態勢構築のための実践的なアドバイスを行います。

Shift Left コンサルティング P.18
安全なサービス提供をめざし普及が急速に進んでいる、開発上級工程でのセキュリティ対策「Shift Left」を可能にするシステム開発を支援します。

情報セキュリティ文書整備支援 P.19
状況にあった実践的な情報セキュリティ文書体系を提案し、既存文書との統廃合や改定案を提示、文書作成/ 改訂作業に対して的確な助言やレビューを行い完成まで支援します。

ゼロトラストプレリミナリーサーベイ P.20
ゼロトラスト・アーキテクチャをベースにした予備的調査を行い、現状を可視化し、ゼロトラスト実現のための計画策定を支援します。

金融機関等向け サイバーセキュリティ プレリミナリーサーベイ P.21
金融分野におけるサイバーセキュリティに関するガイドライン(金融庁)に基づく自己評価結果と対策の妥当性をセキュリティ専門家が第三者の視点で確認します。

電気事業者向け サイバーセキュリティ プレリミナリーサーベイ P.22
電力システムにおけるサイバーセキュリティリスク点検ガイド(経済産業省)に基づく自己点検結果と対策の妥当性をセキュリティ専門家が第三者の視点で確認します。

インシデント対応訓練 P.23
現状の対応態勢における課題を指摘し、改善のための適切なアドバイスを行うことで、お客様のサイバーセキュリティ強化/ 向上に貢献します。

アセスメント

情報セキュリティリスクアセスメント P.24
最適なフレームワークを選択して網羅的に実施するコンサルティング型アセスメントから、短時間・低予算でリスク概要のアセスメントレポートが得られるオンライン自己問診型アセスメントまで、幅広いサービスを提供します。

金融機関向け 情報セキュリティリスクアセスメント P.25
金融機関に要求される高いレベルの情報セキュリティを確保するために、可視化を行い迅速に対応します。

地方公共団体向け 情報セキュリティセルフアセスメント P.26
「総務省 地方公共団体における情報セキュリティポリシーに関するガイドライン」に基づき、現状を短時間で把握するためのサービスです。

アセスメント

産業制御システム向け セキュリティリスクアセスメント
P.27

堅牢なセキュリティ対策を求められる社会生活基盤のインフラや工場 / プラントなどの設備システムに特化したリスクアセスメントです。

EC加盟店様向け セキュリティ・チェックリスト対応アセスメントサービス
P.28

EC加盟店様に求められる「セキュリティ・チェックリスト」への対応をご支援します。

自己問診型 テレワーク環境 情報セキュリティリスクアセスメント
P.29

新しいビジネス様式に必要不可欠なテレワーク環境のセキュリティリスク把握に効果を発揮するアセスメントです。

自己問診型 個人情報に関わる 情報セキュリティアセスメントサービス
P.30

お客様ご自身で自己問診型リスクアセスメントをオンラインで実施いただき、コンサルタントが、第三者の視点から、課題と対策を提示します。

情報セキュリティ自己点検アンケート
P.31

自己点検として、従業員の情報セキュリティポリシーの理解度や遵守状況を測る意識調査をWeb アンケートで行い、結果を分析し、現状の課題を報告します。

サプライチェーン 情報セキュリティリスクアセスメント
P.32

サプライチェーン上の企業に対する情報セキュリティリスク対策の現状を把握、分析し、今後とるべき対策について提案します。

自己問診型 FISCガイドライン準拠性評価
P.33

金融機関向けに簡易的な手法によりFISCガイドライン準拠性を評価し、迅速に課題と次の一手となる対策を提示します。

ネットワーク機器設定評価
P.34

ネットワーク機器の設定を評価し、セキュリティ上の問題点を可視化します。設定ファイルを直接評価することで、ネットワーク経由の通信に擬似攻撃を用いた脆弱性スキャンでは発見できない問題を可視化します。

データベース設定評価
P.35

組織の重要情報が格納されているデータベースの脆弱性を評価するサービスです。内在する脆弱性を事故が起きる前に把握し、対策を施す足掛かりになります。

無線LAN調査
P.36

オフィス内に飛び交う無線LAN の電波を調査し、悪意ある電波、暗号化強度の弱い電波を抽出し、安全なオフィス環境維持を支援します。

教育

情報セキュリティ教育
P.37

情報セキュリティの専門企業として培ってきた経験とノウハウに基いた実践的な各種教育プログラムを提供することで、お客様のサイバーセキュリティ強化/ 向上に貢献します。

標的型攻撃メール訓練
P.38

攻撃の疑似メールを対象者に送付し、受信者とシステムがそのメールを標的型攻撃メールと判断できるかを診断。社員のセキュリティに対する意識づけにも効果を発揮します。

セキュリティ認証取得／準拠支援

PCI準拠支援/オンサイト評価 P.39
クレジットカード業界の国際的セキュリティ基準である"PCI DSS" "PCI P2PE" "PCI 3DS"への準拠をめざす企業を支援します。

PCI準拠支援ソリューション/PCI準拠維持支援 P.40
"PCI DSS" への準拠及び維持に役立つ各種ソリューションや、"PCI DSS" "PCI P2PE" "PCI 3DS" の準拠維持をサポートするコンサルティングサービスを提供しています。

PCI DSSセキュリティ セカンドオピニオン P.41
PCI DSS準拠済企業様のセキュリティを再確認します。

PCI-CPSA/PCI PIN Assessment P.42
"PCI-CPSA" "PCI PIN Assessment"の認証取得・準拠維持支援、コンサルティングサービスとソリューションサービスを提供しています。

PCI DSS Ver4.0.1 SAQ(D-SP) 記入例サンプル提供サービス P.43
金融・旅行・不動産・IR・ECサイトの分析・構築など数多くの業界を把握したWebサイトの充実・改善についての提案や、コンサルティングサービスを提供します。

ゴメス・コンサルティング

サイト評価・設計コンサルティング P.44
金融・旅行・不動産・IR・ECサイトの分析・構築など数多くの業界を把握したWebサイトの充実・改善についての提案や、コンサルティングサービスを提供します。

Webシステム開発 P.45
WebシステムおよびWebサイトの戦略立案・設計・デザイン・システム開発・保守・運用まで、豊富な実績とノウハウを活用し効果的なWebサイトを実現します。

マーケティング・データベース P.46
すぐに使える豊富な統計・リサーチデータを提供。消費者の行動と意識を集約しスコアリングすることで、公正な数字に基づく企画と判断をサポートします。

パフォーマンス監視・改善 P.47
自社のITシステムやクラウド環境の監視だけでなく、アプリケーション監視とリアルユーザー体験の解析を統合。ビジネスへのインパクトを把握し経営課題の解決をサポートします。

脆弱性診断：サービス一覧

脆弱性診断

サイバー保険 P.51
費用の問題から十分な初動対応ができないといった問題が発生しかねない状況を憂え、BBSecから提供する脆弱性診断サービス「SQAT® 脆弱性診断」のすべてに、サイバー保険を付帯しました。

Webアプリケーション・API脆弱性診断 P.52
Webアプリケーション・APIを攻撃するハッカーの手法を用いて、外部から動的に脆弱性を診断し、攻撃の入口となる可能性のある箇所を検出します。

ネットワーク脆弱性診断 P.52
システム全体に影響を及ぼすネットワークからの不正アクセスを防止するため、ネットワーク経由またはオンサイトにて診断いたします。

スマホアプリ脆弱性診断 P.52
スマホアプリ及びスマホアプリ/ サーバ間の通信を診断し、スマホアプリ特有の脆弱性を洗い出します。

IoTセキュリティ診断 P.52
IoTデバイス実機を使った静的・動的解析を実施します。デバイス単体の検査はもちろん、機器の特性・利用シーンに合わせた項目を選定し、効果的・効率的な診断を実施します。

アタックサーフェス調査 P.52
インターネット上の公開情報（OSINT*）を利用して「攻撃者にとって対象組織はどう見えているか」を調査・報告するサービスです。

*Open Source Intelligence

ペネトレーションテスト P.53
綿密な事前調査により「システム内でより脆弱な個所」を特定し、シナリオベースの疑似攻撃を実施。効果的な防御方法を構築して、攻撃被害の最小化を図れます。

クラウドセキュリティ設定診断 P.53
主要クラウドが推奨する環境への適合性診断に加え、マルチクラウド環境に求められる異なる推奨環境を画一的な視点でチェックする設定診断を同時に行います。

ソースコード診断 P.53
独自開発ソフトウェアのソースコードを静的に分析し、セキュアなコーディングルールとデータフローをチェックし、隠された脆弱性とコーディング品質を検証します。

脆弱性診断保守

デイリー自動脆弱性診断 P.54
インターネット越しにシステムの脆弱性をチェックする、高頻度で気軽に実施可能な自動診断ツールです。

Webサイトコンテンツ改ざん検知 P.54
インターネットを介してWeb サイトのコンテンツ改ざん・埋め込みを検知して、レピュテーションリスクを低減する自動ツールです。

ソースコード自動診断 P.54
アプリケーションのソースコードを専用ポータルにアップロードするだけで、ソースコードの脆弱性と品質の診断を行える自動分析ツールです。

情報漏えいIT対策：サービス一覧

マネージドセキュリティ

マネージドセキュリティ P.57
お客様のシステムに対する不正アクセスや悪意ある攻撃を24時間365日体制で監視し、必要によりインシデント発生時の初動対応を実施します。

Managed Security Service for AWS P.59
クラウドサービスの特性を考慮し、攻撃の検知・対応に加え、インシデントが発生する前の予防も支援します。

Managed Security Service for SASE P.60
ゼロトラストの基盤となるSASE-MSSでインシデント対応までカバーします。

WAF運用 P.61
高い技術力が求められるWAF 導入時のチューニングから、24時間365日体制の監視/解析まで、一貫したWAF運用サービスを提供します。

IDS/IPS、UTM、ファイアウォール運用 P.61
様々なセキュリティ関連機器を24時間365日体制でリモート監視/初動対応いたします。

クラウドWAF運用 P.62
クラウドサービスに対する不正アクセスや悪意ある攻撃からセキュリティを守り、利用者のユーザビリティを向上させます。

サーバセキュリティ運用 P.63
主にクラウドを利用されるお客様向けサービスです。既存ネットワーク構成を変更せずに対象サーバへの導入が可能です。

インターネット分離クラウド P.64
マルウェア対策の決定版として評価/期待されるインターネット分離環境を、当社クラウドを利用してリーズナブルな価格で提供します。

SIEM運用/分析 P.65
セキュリティのビッグデータ管理ツールであるSplunkに一元管理されたセキュリティログを監視/解析し、インシデント発生時にお客様にお知らせするサービスです。

エンドポイントセキュリティ P.66
お客様端末を24時間365日体制で監視し、インシデント発生時には端末の隔離など初動対応を実施します。

脆弱性情報提供 P.67
年間1 万件規模に上る様々な脆弱性情報から、自社に必要とされる情報のみをフィルタリングしてお届けする情報提供サービスです。

セキュアメール P.68
一般企業だけでなくインターネット事業者にも利用される、高い実績と信頼性を誇るセキュアメールホスティングサービスです。

AAMS® マルウェア・プロテクト P.69
ユーザの手元に届く前に、標的型攻撃のリスクあるメールを自動隔離し検証します。

セキュリティログ分析/活用支援 P.70
サイバー攻撃から組織を守る上で欠かせない統合ログ管理の活用に向け、企画から構築まで、包括的な支援を行います。

サイバープロテクション（CP） P.71
中小企業・団体向けに、サイバーセキュリティ対策の基本サービスをパッケージ化し、安価かつ手軽な運用で貴社及び貴社取引先を守ります。また業務受託の際にもアピールできます。

インシデント対応

デジタルフォレンジック P.72
重大インシデント発生時の初期対応から復旧、原因追及だけでなく、代替サービスの提供やシステム改善施策まで、インシデントをトータルにサポートする支援プログラムです。

緊急コンタクトセンター P.73
自社での解決が難しいことが想定されるインシデントをサポートするための電話窓口です。24時間365日、当社との取引の有無にかかわらずご相談が可能です。

サイバー脅威情報調査 P.74
不正アクセス被害が発生したり、情報漏えいの恐れが懸念される場合に、ダークWeb上で機密情報が公開されているかを調査して報告するサービスです。

セキュリティ監査・コンサルティング

情報セキュリティ・アドバイザリ

企業のセキュリティニーズを可視化し、実装へと導く

情報セキュリティ強化に向けた組織的な体制づくりを、社内ルール/情報システム両面から支援します。現状分析を行うことにより、対策すべき事項のリストアップや実施の順序、社内体制や情報システムの改善施策などの目標を明確化し、一歩ずつ前に進む為のお手伝いをします。
何から着手すべきかわからない、緊急で対策すべき事項があるなど、お客様のご要望を遠慮なくお聞かせください。個々の企業特性にあわせた、実現可能なプランをご提案いたします。

サービス概要

変化の激しいIT環境において、持続可能な情報セキュリティ対策を展開するためのアドバイスを行います。

■サービス提供準備

ネットワーク環境の把握
貴社ネットワークの構成やセキュリティ対策状況について情報共有いただき、現状を理解します。

セキュリティ対応策の把握
貴社が定めているセキュリティ関連の規程、ルールを共有いただき、現状の統制状況、対策状況を理解します。

インシデント発生時のプロセス把握
貴社が定めているインシデント発生時の手順書、マニュアルを共有いただき、有事の際の準備状況を理解します。

■定常サービス

セキュリティ施策計画支援（年次）
実施計画のレビュー、実施事項の助言をします。

セキュリティ施策推進支援（適宜）
ルール策定等への助言、導入予定の製品 / サービス選定等に対し助言をします。セキュリティ委員会等にオブザーバとして同席します。

インシデント発生時の初動対応助言
マルウェア / セキュリティイベント検知の際の初動対応に関する下記助言をします。
・緊急性判断　・フォレンジック調査要否判断
・応急措置として実施すべき事項の提案　・再発防止策のレビュー

セキュリティトピックス情報提供
最新のセキュリティ情報をお知らせします。（月次ベース）

ニーズにあわせたコンサルティング

お客様のご要望にあわせ、様々なセキュリティに関するコンサルティングサービスを提供します。

- セキュリティ規程、ガイドライン策定コンサルティング
- インシデント対応計画策定コンサルティング
- セキュア開発標準策定コンサルティング
- 個人データ管理に関するコンサルティング
- データマッピングコンサルティング
- ハードニング（堅牢化）コンサルティング
- オフィス移転に伴う情報管理コンサルティング
- 情報資産棚卸調査、リスク評価

など

AIサービス提供者・利用者向け サイバーセキュリティ対策支援

総務省経済産業省『AI事業者ガイドライン』に基づくAIガバナンスの実践

AIのイノベーションおよび利活用を促進するためにAIのリスクを正しく認識し、その低減を図る

AI技術の進化は私たちの生活やビジネスに恩恵をもたらす一方で、新たな脅威も生じています。AIを利用したサイバー攻撃は高度化し、マルウェアやフィッシングが巧妙になっています。ディープフェイクを使った詐欺や偽情報の拡散も増加し、AIのデータ解析能力向上により、個人情報・知的財産・機密データの不正利用リスクやプライバシー侵害の懸念も増大しています。さらに、倫理的・社会的影響から、今後様々な法規制への対応も必要となることが予想されます。
2024年4月に経済産業省と総務省は、生成AIの普及を始めとする近年の技術の急激な変化などに対応し、AIの安全安心な活用を促進することを目的に「AI事業者ガイドライン（第1.0版）」を発表しました。
BBSecは、このガイドラインに基づいたAI提供者およびAI利用者向けのサイバーセキュリティ対策支援サービスを提供、経験豊富な情報セキュリティ対策のスペシャリストが『AI事業者ガイドライン』に基づくAIガバナンスの実践を支援します。

サービス一覧

■AIサービス提供者向けサービス

AIサービス提供者向け セキュリティガイドライン整備支援サービス	
AIサービス提供者向け セキュリティガイドライン雛形提供	経産省・総務省発行「AI事業者ガイドライン」に準拠したAIサービス提供者向けセキュリティガイドライン（雛形）を提供
AIサービス提供者向け セキュリティガイドライン整備支援	AIサービス提供者向けセキュリティガイドライン（雛形）の提供およびお客様の事業に合わせたカスタマイズ

■AIサービス利用者向けサービス

AIサービス利用者向け セキュリティガイドライン整備支援サービス	
AIサービス利用者向け セキュリティガイドライン雛形提供	経産省・総務省発行「AI事業者ガイドライン」に準拠したAIサービス利用者向けセキュリティガイドライン（雛形）を提供
AIサービス利用者向け セキュリティガイドライン整備支援	AIサービス利用者向けセキュリティガイドライン（雛形）の提供およびお客様の事業に合わせたカスタマイズ

AIサービス利用者向け 情報セキュリティ教育サービス	
AIサービス利用者向け 情報セキュリティ教育コンテンツ提供	AIサービス利用に際し知っておくべき最新のセキュリティ脅威、潜在的なリスク、適切な利用方法、セキュリティ対策について説明
AIサービス利用者向け 情報セキュリティ教育	AIサービス利用者向け情報セキュリティ教育コンテンツの提供および講師によるオンライン研修

参照基準 ■「AI事業者ガイドライン（第1.0版）」（2024年4月19日発行）

経済産業省および総務省が、AIを活用する事業者向けに、透明性、公平性、安全性、プライバシー保護、セキュリティ確保などの責任あるAI活用を促すための基本的なガイドラインとして策定。リスク管理や倫理的な判断基準の整備を求め、社会的な信頼構築を目指す、日本におけるAIガバナンスの統一的な指針として位置付けられる。

ランサムウェアに対応したIT-BCP策定支援

事業継続を揺るがす脅威、サイバー攻撃に備えた対応態勢を構築

近年、デジタル化（DX）の進展や新型コロナウイルス感染を契機としたテレワークなどの働き方改革が押しする形で業務でのITシステム活用が飛躍的に進みました。多くの企業は、もはやIT抜きには業務やサービスが成り立たず、その重要性は高まるばかりです。一方、ITシステムをターゲットとした犯罪も悪質化・巧妙化し、被害も深刻化の一途を辿っています。
多くの日本企業におけるIT-BCP（ITに対する事業継続計画）は、主に地震などの大規模自然災害を想定したシステム停止・障害からの復旧を目的として策定されている場合がほとんどです。ところが、サイバーインシデントの場合は、考慮すべき観点が異なり、インシデントの拡大を防止しながら復旧作業を行うため、同じプロセスでは進めることができません。すなわち、サイバー攻撃をこれまでとは性質の異なる脅威と捉え直し、サイバーセキュリティに対応したIT-BCPへの強化が必要なのです。
BBSecは、セキュリティ専業の企業として数多くのお客様のインシデント対応態勢構築に携わった経験を活かした適切なアドバイスやノウハウ提供を行うことで、お客様の状況やニーズに合ったサイバーセキュリティIT-BCP策定を支援します。

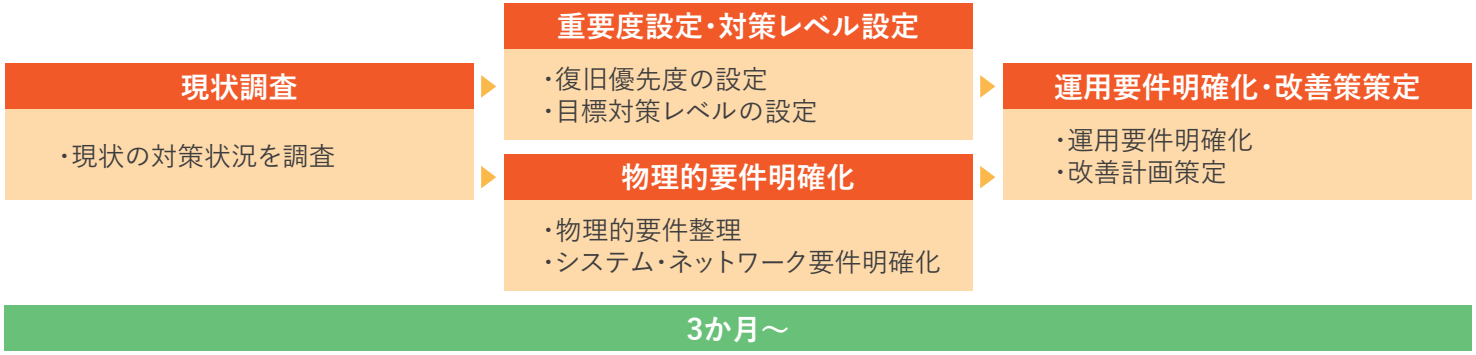
サービスの概要

災害対応とは異なり、サイバーセキュリティ対応では、以下の点に考慮する必要があります。

- 地震などの自然災害と異なり、BCP発動タイミングが明確でないことがある
- サイバー攻撃による被害範囲を把握するのが容易ではない
- ランサムウェア感染など復旧の前に原因を特定し、封じ込めを行った上で、再発防止などの対策が必要となる

サイバー攻撃が特定の企業をターゲットにしている場合、同業他社は影響を受けていません。また、対応や復旧が遅れるほどビジネスインパクトは大きく、また、適切に対処しないと長期間事業が停止し、社会的信頼の失墜を招く恐れがあります。

ランサムウェアに対応したIT-BCP策定支援プロセス例



「防衛産業サイバーセキュリティ基準」準拠支援

情報セキュリティ基本方針/規則/実施手順の策定および改善対策

セキュリティ専門家が防衛産業サイバーセキュリティ基準への準拠を支援

近年、ランサムウェア攻撃やサプライチェーン企業へのサイバー攻撃など、企業や組織が直面するリスクは増加し、これらの脅威は、企業の事業運営はもちろん、国家安全保障にも直結する問題となっています。特に防衛産業は、国家の安全保障を担う重要な役割を果たしているため、サイバーセキュリティの脅威から自身を守るだけでなく、供給する製品やサービスが安全であることを保証する必要があります。このような背景から、防衛省・防衛装備庁は、防衛関連企業に対するサイバーセキュリティ基準として「防衛産業サイバーセキュリティ基準」を2022年4月に整備し、2023年度より運用を開始しています。これは、防衛産業に特化したサイバーセキュリティ基準であり、防衛関連企業の情報セキュリティの確保を通じて、国の防衛装備品および役務の調達を安全に行うためのものです。このため、防衛省・自衛隊の装備品および役務の調達や入札、契約に際しては、「防衛産業サイバーセキュリティ基準」とその関連文書に準拠した情報セキュリティ基本方針・規則・実施手順の策定および改善対策が求められます。
BBSecは、経験豊富な情報セキュリティ対策のスペシャリストが「防衛産業サイバーセキュリティ基準」準拠をご支援いたします。

このようなことでお困りではありませんか？

- 防衛装備品への活用が可能な技術や製品を有しているので防衛産業に新規参入したい
- 防衛省・自衛隊の調達案件に入札したいが、防衛産業サイバーセキュリティ基準が分からない
- 情報セキュリティ要件に求められる高度なセキュリティ体制・対策を構築するノウハウ/リソースが足りない
- 既存の情報セキュリティ基本方針や規程が、防衛省・防衛装備庁が定める防衛産業サイバーセキュリティ基準に準拠しているかを評価したい

準拠支援プロセスとサービスラインアップ

■情報セキュリティ基本方針等および対策ロードマップ策定支援サービス

フェーズ①
1. スコープ選定
2. 既存の基本方針関連文書の準拠性評価
3. 基準に準拠した基本方針策定

フェーズ②
1. 既存の実施要領関連文書の準拠性評価
2. 基準に準拠した規則・実施手順策定
3. 対策ロードマップ案策定

■対策実行支援型サービスBBSec Prime for Defense Industry

フェーズ③
1. 対策ロードマップに基づく改善対策支援
2. 準拠状況の年次確認（PDCA）
3. Q&A 対応、関連情報の提供
4. インシデント発生時の初動対応の助言
5. 月次定例会開催

BBSecは、上記サービス以外にも、準拠支援サービスを各種取り揃えています。
（入札準備支援、システムセキュリティ実装計画書（SSP）添付資料の準備支援、セキュリティ監査（自己監査）支援、情報セキュリティ教育および訓練支援）など

防衛産業サイバーセキュリティ基準

「防衛産業サイバーセキュリティ基準」は、防衛省・防衛装備庁がサイバーセキュリティ強化のためにNIST SP800-171などを参考に厳格な管理策を盛り込み整備した情報セキュリティ基準です。防衛関連企業との契約には「装備品等及び役務の調達における情報セキュリティの確保に関する特約条項」を付すことが定められており、その特約条項に係る要件として、基準に準拠した「情報セキュリティ基本方針」およびシステムセキュリティ管理策についての「情報セキュリティ基準・情報セキュリティ実施手順」の策定が求められています。

自動車部品業界向け 情報セキュリティ対策支援

自工会/部工会・サイバーセキュリティガイドラインV2.2に基づき情報セキュリティ課題に対する対策を支援

自動車産業を取り巻くサイバーセキュリティリスクが深刻化している中、日本自動車工業会と日本自動車部品工業会は、「サイバーセキュリティガイドラインV2.2」を発行し、自動車産業のサプライチェーン全体にガイドラインの活用を推進しています。
サプライチェーンを構成する各社は、セキュリティリスクを正確に理解しながら適切な対策を行うことが求められています。
BBSecは、「サイバーセキュリティガイドラインV2.2」準拠に向けた情報セキュリティサービスを各種取り揃えています。特に、ガイドラインに準拠したセキュリティポリシーや規程類を整備することが、対策の重要な第一歩と捉え、お客様のニーズに合わせたサービスを用意しましたので、是非、ご活用ください。
経験豊富な情報セキュリティ対策のスペシャリストが、効率的かつ効果的にガイドラインへの準拠と情報セキュリティ強化に向けた対策を推進します。

サービス一覧

■自動車部品業界向け サイバーセキュリティプレリミナリーサーベイ

サイバーセキュリティガイドラインに基づく自己点検結果および対策の妥当性をセキュリティ専門家が第三者視点で確認（対策ロードマップ作成のオプションも追加可能）

調査	自己点検結果や文書の確認、インタビューや現地視察による現状把握
評価・分析	セキュリティ専門家による自己点検結果/セキュリティ対策の妥当性評価
報告	評価報告書の作成および報告会の開催

■自動車部品業界向け 情報セキュリティ対策実行支援型サービス BBSec Prime for Auto Parts Industry

サイバーセキュリティガイドラインV2.2に基づくアセスメント終了後、対策ロードマップを作成し、年間を通じた対策実行に関するアドバイザリを提供

アセスメント	・文書確認、インタビュー ・調査・分析、報告書作成 ・報告会
実施計画立案	・対策ロードマップ作成 ・改善事項一覧作成
対策実行支援 アドバイザリ	・情報セキュリティ対策支援　・緊急時初動対応の助言 ・Q&A対応　・月次定例会（訪問/オンライン） ・関連情報提供

自工会/部工会・サイバーセキュリティガイドラインV2.2（2023年9月1日発行）

自動車メーカーやサプライチェーンを構成する各社に求められる自動車産業固有のサイバーセキュリティリスクを考慮した、向こう3年の対策フレームワークや業界共通の自己評価基準を明示することで、自動車産業全体のサイバーセキュリティ対策のレベルアップや対策レベルの効率的な点検を推進することを目的として作成されています。

■自動車部品業界向け 情報セキュリティ文書雛形提供サービス

サイバーセキュリティガイドラインV2.2（Lv1/Lv2/Lv3）に準拠したセキュリティ文書雛形（ポリシー・規程16文書）を提供

・情報セキュリティ基本方針
・情報セキュリティ管理規程
・ネットワーク管理規程
・脆弱性対策規程
・アクセス制御規程
・情報取扱い規程
・暗号鍵管理規程
・マルウェア対策規程
・物理セキュリティ管理規程
・ソフトウェア開発管理規程
・監査ログ管理規程
・セキュリティインシデント対応規程
・情報機器管理および利用規程
・外部委託管理規程
・文書管理規程
・関連法令規程

■自動車部品業界向け 情報セキュリティ文書整備支援サービス

サイバーセキュリティガイドラインV2.2（Lv1/Lv2/Lv3）に準拠したセキュリティ文書雛形（ポリシー・規程16文書）をお客様向けにカスタマイズ

助言タイプ	お客様主体で文書作成を行い、BBSecは助言とレビューにより文書の完成まで支援 *情報セキュリティ文書雛形提供含む	・文書雛形提供（16文書） ・ドキュメント調査 ・インタビュー ・助言とレビュー支援
委託タイプ	BBSec主体で文書作成を行い、お客様のレビューを経て文書を完成 *情報セキュリティ文書雛形提供含む	

※評価結果に基づきご活用いただける自工会/部工会・サイバーセキュリティガイドラインV2.2準拠支援サービスを各種取り揃えています。（標的型攻撃メール訓練、情報セキュリティ教育、脆弱性診断、HW/SWセキュリティ設定評価、インシデント対応訓練、CSIRT構築支援など）
※サイバーセキュリティガイドラインV2.2では、企業の規模に関わらずサプライチェーン全体で活用されることを目的として、取扱う情報により標準的に目指す項目や最終到達点として目指すべき項目を3つのセキュリティレベル（Lv1～Lv3）で定義しています。

SWIFT CSCFに基づく外部評価、内部評価支援

SWIFT CSCFの外部評価・内部評価と更新を継続的にサポート

金融機関が国際決済を実現するための世界的会員制協会「SWIFT」。SWIFTでは、金融メッセージングフォーマットの標準とメッセージングのためのプラットフォームを提供しており、現在、200以上の国や地域で11,000以上の事業体がこのサービスを利用しています。
このSWIFTを利用する事業体は、毎年、外部評価または内部評価による独立検証を実施し、SWIFT CSCF（カスタマーセキュリティコントロールフレームワーク）の要件を満たしていることを確認することが求められます。BBSecは、日本（内資）企業初の CSP assessment provider に認定された監査機関として、これまで培ったノウハウを活かし、国内および海外の事業体様に向けて、SWIFT CSCF 準拠を支援いたします。

日本内資企業初のCSP assessment provider

SWIFTの公開文書や通達など、最新の更新情報をいちはやくお知らせすることが可能です。

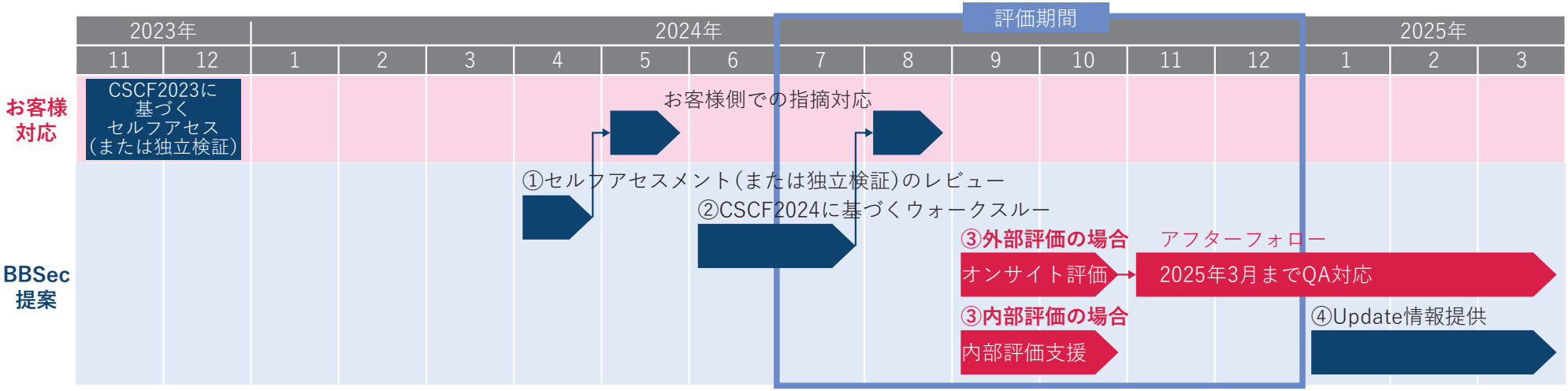
経験に培われた豊富なノウハウ

これまでのセキュリティ監査、コンサルティング、各種サービスで培った知見を活かした高品質なサービスを提供します。

FISC、NIST CSFとのワンストップなコンサルティングが可能

金融事業者が求められる様々なセキュリティ規格を総合的にサポート

スケジュール例とサービス内容



①セルフアセスメントレビュー*1	前年度にお客様が実施したセルフアセスメントレポート（または独立検証結果）を当社にて確認し、不備事項の指摘を実施。2時間×2回の打ち合わせ。
②CSCF2024に基づくウォークスルー	CSCF2024に基づく模擬審査。インタビュー／文書確認／システム全体の確認／セキュリティ設定確認を通じて確認。
③<外部評価>オンサイト評価*2 <内部評価>内部評価支援	**<外部評価>CSCF2024に基づく本審査。終了後、2025年3月まではQA対応を受付。 <内部評価>CSCF2024に基づく内部評価支援。貴行自身での評価対応に5日間同席。 また、教育対応を1日間実施の他、該当期間は評価対応についてのQA受付。**
④Update情報提供	CSCF2025の要件を初めとするSWIFTからのUpdate内容を日本語で案内。

SWIFT評価企業数
32社（33案件）
（2024年1月現在）

*1 上記スケジュールは一例です。年度ごとの実施内容については、個別にご相談ください。　*2 アーキテクチャーやシステム規模によりコストは変動します。

ISO/IEC 27017 クラウドセキュリティ認証取得支援

拡大するクラウドセキュリティの脅威に対応する態勢を構築することで企業価値向上を図る

政府によるクラウド・バイ・デフォルト原則の推進、ガバメントクラウド構想の発表など、情報システムのクラウド化が加速しています。一方、クラウドサービスの利用が急拡大したことに伴い、セキュリティインシデント事例が多く報告されるようになりました。今、クラウド上のデータやソフトウェア資産を守る「セキュリティ」への対応は、最重要事項となっています。
ISO/IEC 27017は、クラウドサービスのための情報セキュリティの管理策および実施の手引きに関する国際規格であり、様々なクラウド上のリスクへの備えを示したガイドラインです。さらにこの国際規格に基づいた第三者認証としてISO/IEC 27017クラウドセキュリティ認証（ISMSクラウドセキュリティ認証）があります。
BBSecは、お客様がクラウドサービスのセキュリティを担保し、DX時代を勝ち抜くために、クラウド提供事業者/利用事業者双方の指標となるISO/IEC 27017に基づくISO/IEC 27017クラウドセキュリティ認証取得を支援するコンサルティングサービスを提供します。

サービスの特長

経験に培われた豊富なノウハウ

情報セキュリティの専門企業として長年培ってきたノウハウと蓄積された知見に基づいた高品質なサービスを提供します。

認証取得の効果

クラウドサービス提供事業者様	国際規格に基づくクラウドセキュリティ認証を取得することで、クラウドサービスのセキュリティに対する堅実な取り組みをアピールすることができ、また競合他社との大きな差別化のポイントともなります。
クラウドサービス利用事業者様	クラウドサービスの利用を前提にした情報セキュリティ管理体制を確立することで、クラウドサービスの利用におけるリスクの低減のみならず、認証取得によるステークホルダーの信頼向上に寄与します。

サービス内容

BBSecは、ISO/IEC 27017認証取得に向けて4つのサービスを用意しています。ISO/IEC 27017認証を最短期間で取得いただくため、お客様の対策状況に応じたメニュー組み合わせをご提案し、効果的かつ効率的な支援を提供します。

サービスメニュー	サービス内容
ISO/IEC 27017認証取得に向けたアセスメントおよび基本要件決定支援	ISO/IEC 27017とのギャップを効率的かつ効果的に把握できる評価シートを用いてお客様の現状をアセスメントします。また、アセスメント結果に基づきギャップ分析を行い、基本要件の決定についてサポートいたします。
ISO/IEC 27017認証取得に必須となる主要規程文書雛形の提供	ISO/IEC 27017は、27001、27002に依拠した規格であり、27002にクラウドサービス利用者とクラウドサービス事業者を追記したガイドライン規格で構成されています。ISO/IEC 27017認証取得で欠かせない基本設計部分の必須文書として27002、27017に準拠した規程文書の雛形を提供します。
ISO/IEC 27017規程文書の整備支援	上記で決定した基本要件の具体化、詳細化を進め、ミーティングに参加、事例の紹介や助言を行い、規格の要求事項を実現する作業をサポートします。また、ご要望に応じてISO/IEC 27017の主要規程文書雛形をお客様向けにカスタマイズします。
ISO/IEC 27017に関する社員教育	弊社が独自で開発したわかりやすいテキストを提供し、ISO/IEC 27017のポイントについて、社員に向けた教育を行います。

CSIRT構築・運用支援

高度化・巧妙化するサイバー攻撃に対する組織の対応力強化

サイバー攻撃が悪質化・巧妙化し、被害も深刻化している現在、侵入を前提とした対応態勢の構築が、企業に求められています。その中で、サイバーセキュリティの監視・対策を行う社内組織 CSIRT（Computer Security Incident Response Team：シーサート）は、事業継続に大きく寄与する全社横断組織として注目されています。
BBSecは、CSIRT構築を必要とする企業・団体に向けて、CSIRTのプランニング / 構築 / 運用を専門家の立場からご支援いたします。経験値を活かした適切なアドバイスやノウハウ提供は、実行力のある組織へと育成する上で大きな手助けとなります。

CSIRT構築により、組織の事業継続性につながるインシデント対応力を強化

CSIRT構築・運用の3つのフェーズ

CSIRT構築から運用に至る3つのフェーズを通して経験豊富なコンサルタントがお客様をサポートいたします。設計/構築フェーズでは、組織にあった実効性の高いCSIRTの早期立上げと、実践的で継続運用可能なレベルのマネジメントシステムの確立を目指します。運用フェーズでは、日々発生する様々な課題への対策に関する助言、インシデント対応訓練の実施など、CSIRTの実行力強化に向けた支援を行います。

フェーズ1（設計）	フェーズ2（構築）	フェーズ3（運用）
CSIRTの定義と平常時を含む体制の整備	インシデント関連を中心とした CSIRT関連ルールの整備	習熟度向上・インシデント対応訓練の実施

CSIRT構築支援サービス

- GAP分析、CSIRT水準策定
- 実施計画策定
- CSIRT憲章作成
  - 社内における位置づけ、対応範囲
  - インシデントの定義
- CSIRT職務定義書作成
  - 組織と体制の定義
  - 担当者の定義、責任、役割
  - 体制図
- インシデント対応関連規程整備
  - インシデント対応ガイドライン作成
  - トリアージの定義
  - エスカレーションフロー策定
  - インシデント対応計画
- インシデント対応ガイドライン等読み合わせ
- 脆弱性対応ガイドライン作成
- CSIRT関連規程整備
  （ISMS・PMS文書整備支援含む）
- CSIRT説明会

CSIRT運用支援サービス

- CSIRT運用開始後の助言、Q&A対応
- CSIRT要員教育
- 他CSIRTとの連携
  （日本シーサート協議会への加盟検討）
- セキュリティトピックス情報提供
- インシデント発生時の初動対応の助言

インシデント対応訓練サービス

- インシデント対応訓練
  - 対応計画に基づいたシナリオ作成
  - ロールプレイング形式による訓練実施
  - 評価・振り返り・改善

CSIRTの役割 CSIRTは、全社に波及する可能性のあるセキュリティインシデントに、組織全体で最速 / 最善の対策を行う為のタスクチームです。平常時は、インシデント発生時に効果を発揮するための体制構築 / 組織を越えた情報交換 / リスクの早期発見 / 社員への注意喚起や啓発活動等を実施しリスクに備えます。

インシデント初動対応準備支援

拡大するサイバーセキュリティの脅威に対応するために今すぐにでも準備すべきことを明確にする

サイバー攻撃が悪質化・巧妙化し、被害も深刻化している現在、日頃よりインシデントの発生を想定した準備を行っておくことが企業に求められています。サイバーセキュリティの監視・対策を行う社内組織として注目を集めているのは CSIRT（Computer Security Incident Response Team）ですが、その構築には時間とコストがかかります。将来的にはCSIRT構築を目指すとしても、今すぐ行うべきこと、行えることはたくさんあります。
BBSecは、昨今のサイバー攻撃の動向を踏まえ、情報セキュリティの専門企業として培ってきた経験とノウハウによって開発された方法論に基づき、インシデント発生時に備えて今、最低限準備すべきことを明確にしました。本サービスでは、経験豊富なセキュリティコンサルタントが、お客様の現状を確認し、お客様の実情に合わせた初動対応準備態勢構築のための実践的なアドバイスを行います。

サービスの特長

インシデント発生時に備えて最低限準備すべきことを明確化

最新のセキュリティ動向を踏まえインシデント発生時にお客様が参照しながらアクションがとれる実践的なアウトプット（インシデント初動対応フロー、インシデント対応ガイドライン）をお客様とともに完成させます。

経験に培われた豊富なノウハウ

情報セキュリティの専門企業として長年培ってきたインシデント対応態勢構築ノウハウとインシデント発生時のお客様のサポートにより蓄積された知見に基づく高品質なサービスを提供します。

コンサルティングプロセス

キックオフ	プロセス策定支援	初動対応ワークショップ	Q&A
・進め方説明 ・既存体制に関するヒアリング ・既存文書の確認 ・作成物イメージの共有	・インシデント初動対応* ガイドラインの作成 ・インシデント対応の 基礎知識に関する教育 ・質疑応答	・ガイドラインの内容に基づいた ディスカッション ・インシデント対応フロー策定	
8週間			2週間

*インシデント初動対応のスコープ：インシデント検知・受付、深刻度判定、封じ込め対応

このようなことでお困りではありませんか？

- 同業他社でインシデントが発生した。
  社長から**自社の対応態勢は大丈夫か**問われている。
- インシデント対応態勢構築の重要性は認識しているが
  CSIRTなど**専門組織を立ち上げる体力が今はない。**
- とにかく、最低限、**今すぐにやらなければいけないことを教えて**欲しい。
- サイバー攻撃に対する漠然とした不安を抱えている。

Shift Left コンサルティング

システム開発の上流工程におけるセキュリティ対策を支援

インシデントの原因をたどると、開発上流工程における脅威への認識不足により、製造段階で脆弱性を作りこんでしまったというケースが多く見られます。本サービスは、安全なサービス実現に向けて普及が進む、開発上流工程でのセキュリティ対策「Shift Left」をサポートするシステム開発支援コンサルティングです。セキュリティ対策がとられた設計により、製造時の手戻りによる時間とコストを軽減して安全なサービス提供を実現できるよう、セキュリティの専門家が支援いたします。

サービスの特長

セキュリティを視野にいれた設計が可能
見逃しがちなセキュリティ上の設計ミスを早期に発見することが可能です。

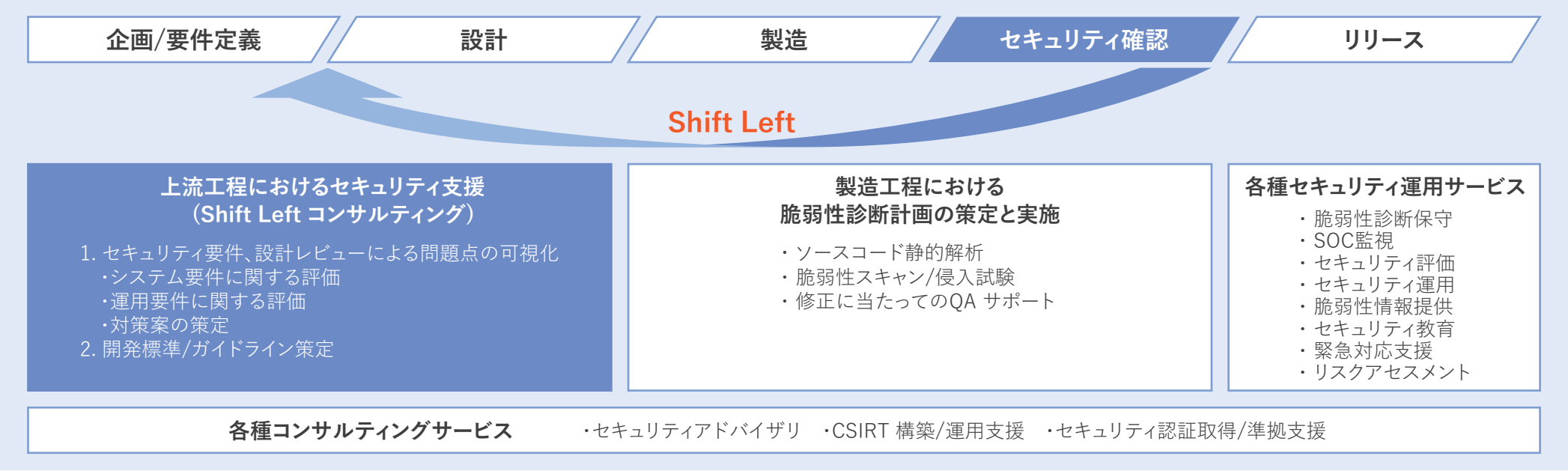
手戻りコストの軽減
システム開発時には脆弱性の作りこみに考慮せず作業がすすめられ、開発のスピードアップにつながります。

開発のスピードアップ/オンスケジュールの開発
リリース直前に発見される脆弱性が大幅に減ることで、手戻りコストが縮小します。

安全なサービスの提供
セキュリティリスクを最小化した信頼できるサービスを提供することができ、企業の信頼性が高まります。

サービス概要

開発上流工程における要件定義や設計のレビューを実施し、同時に開発標準やガイドライン作成を支援します。さらに、製造時やリリース後に対応した当社各種サービスをご利用いただくことで、より安全なシステムの運用が可能になります。



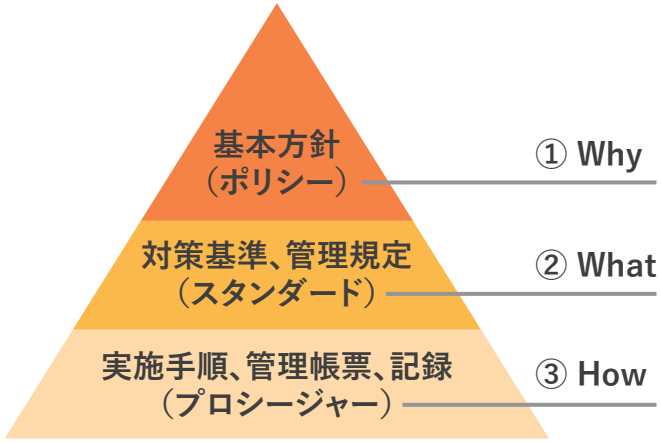
情報セキュリティ文書整備支援

情報セキュリティ対策の第一歩を、その拠り所となる文書整備から始める

サイバー攻撃が悪質化・巧妙化し、被害も深刻化している現在、セキュリティ対策は場当たり的に行うのではなく、体系的、組織的に取り組む必要があります。その推進の拠り所となるのが、情報セキュリティ文書です。企業は、情報資産を脅威から守るために情報セキュリティポリシーを制定し、関連文書を整備し、関係者全員で共有することにより、一丸となって情報セキュリティ対策に取り組むことが求められます。
BBSecは、情報セキュリティ文書整備を専門家の立場からご支援いたします。セキュリティ専業の企業として培ったノウハウに基づく文書雛形の提供や、数多くのお客様の文書整備を支援した経験を活かした適切なアドバイスやノウハウ提供を行うことで、お客様の状況やニーズに合ったセキュリティ文書整備を支援します。

情報セキュリティ文書整備で期待される効果

■組織としての情報セキュリティ管理に関する対外的な説明責任への対応
■情報セキュリティに関する外部監査、認証審査などへの円滑な対応
■経営陣の情報セキュリティに関する意思表明・関与のエビデンス
■従業員の情報セキュリティに関する考え方の統一化、当事者意識の向上
■文書体系の正規化、外部文書（関連法令、ガイドライン等）との整合性確保



サービスの特長

お客様の既存のセキュリティ関連文書、方針、規程、基準、ガイドライン、手続、マニュアル等の確認やヒアリングを通じて現状のセキュリティ文書の整備と運用状況を把握します。
お客様の状況にあった実践的な情報セキュリティ文書体系を提案します。不足文書については雛形*1を提供し、既存文書との統廃合や改定案を提示、文書作成/改訂作業に対して的確な助言やレビューを行い完成まで支援します。

*1：文書雛形は、最新の情報セキュリティ国際標準／ガイドライン（ISMS ISO/IEC 27001/27002/27017、JAMA/JAPIAサイバーセキュリティガイドライン等）をベースに策定しています。

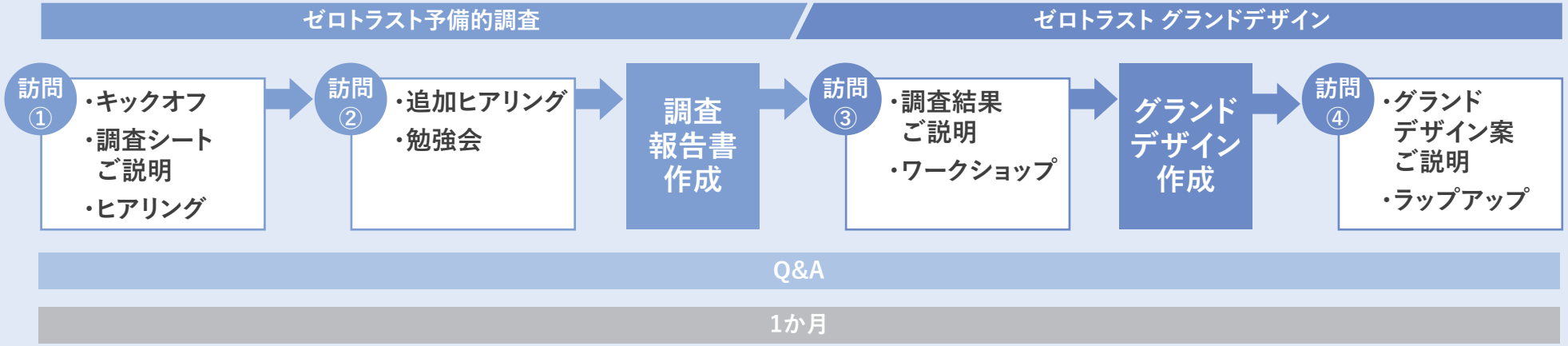
・情報セキュリティ基本方針 ・情報セキュリティ管理規程 ・ネットワーク管理規程 ・脆弱性対策規程	・アクセス制御規程 ・情報取扱い規程 ・暗号鍵管理規程 ・マルウェア対策規程	・物理セキュリティ管理規程 ・ソフトウェア開発管理規程 ・監査ログ管理規程 ・セキュリティインシデント対応規程	・情報機器管理および利用規程 ・外部委託管理規程 ・文書管理規程 ・関連法令規程
・クラウドサービス利用ガイドライン ・CSIRT運用文書類	・テレワーク環境利用におけるガイドライン ・アプリケーション開発標準	・AWS利用セキュリティガイドライン ・ISO/IEC 27017クラウドセキュリティ認証取得必須雛形文書	・Azure利用セキュリティガイドライン

ゼロトラストプレリミナリーサーベイ

ゼロトラストに向けた貴社の現状の課題を把握し、現実的かつ効果的な対策の推進をアドバイス

本サービスは、数多くの支援実績と高度なスキルを有した情報セキュリティコンサルタントが、ゼロトラスト・アーキテクチャ（以下、ゼロトラスト）をベースにした予備的調査（ゼロトラストで求められる各種観点に対する現状調査）を行い、現状を可視化し、ゼロトラスト実現のための計画策定を支援するサービスです。
ゼロトラストとは、信頼できるアクセス要求というものは存在しないという前提で、すべてのアクセス要求をチェックすべきという考え方です。
デジタル・トランスフォーメーション（DX）といわれる昨今のテレワークやクラウドサービスの普及に伴い、業務システムが様々な領域へと進出し、多様化してきていることから、従来のセキュリティ対策では対応しきれないケースが増加しています。
DXによって生じる新たなセキュリティリスクへの対応のためにはゼロトラストにシフトしていく必要があります。

サービス概要・プロセス



ポイント

①予備的調査は、NIST SP800-207による7つの原則を踏まえ、弊社が独自編纂した調査シートを使用し、ゼロトラストで求められる各種観点に対する現状を調査し、可視化します。

②BBSecは、お客様に寄り添ったサービスを信条としています。お客様との対話を通じて、状況に合わせた的確なアドバイスを行いながら、お客様の目指すべきゼロトラストのグランドデザインの策定を支援します。

プレリミナリーサーベイ後は、グランドデザインに従い様々なソリューションをご提案、ゴールまでお客様に伴走しながら支援します。

金融機関等向け サイバーセキュリティプレリミナリーサーベイ

「金融分野におけるサイバーセキュリティに関するガイドライン」準拠支援

「金融分野におけるサイバーセキュリティに関するガイドライン」（金融庁）に基づく自己評価結果と対策の妥当性をセキュリティ専門家が第三者の視点で確認

サイバー攻撃の被害は、世界規模で増加傾向にあり、その手口は日々、高度化し、かつ多様化しています。日本国内においても、企業や団体におけるランサムウェアの被害が、業種を問わず拡大しています。中でも金融機関等は、国民生活や経済活動を支えるサイバーセキュリティ法に基づく重要インフラ事業者として、また経済安全保障推進法に基づく基幹インフラ事業者として、サイバー攻撃の最新の傾向を踏まえた強固なサイバーセキュリティ対策を講じる必要があります。こうした状況を背景に、金融庁は、「金融分野におけるサイバーセキュリティに関するガイドライン」を発行しました。金融機関等は、本ガイドラインに基づく自己評価を行って現在のセキュリティレベルを確認し、さらなるセキュリティ向上を目指して対策に取り組むよう求められています。しかしながら、ITやセキュリティの専任者がいない場合、自己評価の進め方がわからない、自己評価結果や対策が妥当かどうか不安である、という声も多く聞かれます。BBSecは、各種金融機関等へのサービス提供経験が豊富なスペシャリストが、ガイドラインに基づく自己評価結果とセキュリティ対策の妥当性を客観的に評価します。ご要望があれば、自己評価のサポートも行います。ガイドラインへの準拠と情報セキュリティ対策強化に、本サービスを是非ご活用ください。

サービスのプロセス

■「金融分野におけるサイバーセキュリティに関するガイドライン」に基づく自己評価結果と対策の妥当性を第三者の視点で確認

準備 ▶ 調査 ▶ 評価・分析 ▶ 報告書作成 ▶ 改善プラン検討 ▶ 全体計画の立案（対策ロードマップ案） ▶ 報告会

調査
- 自己点検結果確認*
- 文書確認
- インタビュー

調査	自己評価結果や文書の確認、関連するメンバーへのインタビューを行い、現状を把握します。（*ご要望があれば、自己評価の支援も行います。）
評価・分析	調査結果を基に、第三者の視点で自己評価結果およびセキュリティ対策の妥当性を評価します。
改善プラン検討	評価結果を基に、お客様の環境で直ちに対応すべき項目を明確にした最適なセキュリティプランを策定し、提案します。
全体計画の立案（対策ロードマップ案）	必要な対策とその優先順位、実施スケジュールについてお客様と打ち合わせを行い、対策ロードマップ案にまとめます。
報告	報告評価報告書を作成し、報告会を開催します。

BBSecは、評価結果に基づきご活用いただける、金融機関等の企業様向けセキュリティ対策支援サービスを各種取り揃えています。（文書整備の支援、標的型攻撃メールの訓練、情報セキュリティ教育、脆弱性診断、HW/SWセキュリティ設定評価、インシデント対応訓練、CSIRT構築支援など）また、お客様の状況やニーズに沿ったセキュリティ対策の推進を、1年を通じて支援するアドバイザリサービスも提供しています。

金融分野におけるサイバーセキュリティに関するガイドライン（2024年10月4日発行）

金融機関等がサイバー攻撃に対して適切に備え、迅速に対応するための基準となる文書です。リスク評価やモニタリングの強化、インシデント発生時の対応手順、経営層を含む組織体制の整備などを求め、金融機関等の全体的なセキュリティ態勢を向上させることを目的としています。これにより、金融システム全体の安全性と顧客の信頼を守ることを目指しています。

電気事業者向け サイバーセキュリティ プレリミナリーサーベイ

電力システムにおけるサイバーセキュリティリスク点検ガイド準拠支援

電力システムにおけるサイバーセキュリティリスク点検ガイド（経済産業省）に基づく自己点検結果と対策の妥当性をセキュリティ専門家が第三者の視点で確認

電力システムなど社会インフラ、重要インフラを取り巻くサイバーセキュリティリスクが深刻化している中、経済産業省は、「電力システムにおけるサイバーセキュリティリスク点検ガイド」および「電力システムにおけるサイバーセキュリティ対策状況可視化ツール」を発行し、電気事業者を主な対象としてその活用を推進しています。
既に多くの企業が点検ガイドで示された評価基準を用いたセルフチェックを行い、セキュリティレベルの達成状況を確認し、さらなるセキュリティ向上を目指して対策に取り組んでいます。しかしながら、ITやセキュリティ専任者がいない中、自己点検結果や対策が妥当か不安であるという声も多く聞こえてくるようになりました。
BBSecでは、経験豊富な情報セキュリティ対策のスペシャリストが、点検ガイドに基づく自己点検結果を客観的な視点で確認し、セキュリティ対策の妥当性を評価します。

サイバーセキュリティリスク点検ガイド

4つの事業区分（発電事業者、小売電気事業者、アグリゲーター、自家用電気工作物設備設置者）の電気事業者および当該事業者が保有する電力制御システム・ITシステムを対象としており、各事業者は、セキュリティリスクを正確に理解しながら適切な対策を行うことを求められています。

サービスのプロセス

■サイバーセキュリティリスク点検ガイドに基づく自己点検結果と対策の妥当性を第三者の視点で確認

準備	調査	評価・分析	報告書作成	報告会
	・自己点検結果確認 ・文書確認 ・インタビュー			

サービスの特長

調査
自己点検結果や文書の確認、関連するメンバーへのインタビュー、現地視察などを行い現状を把握します。

評価・分析
調査結果をもとに第三者の視点で自己点検結果およびセキュリティ対策の妥当性を評価します。

報告
評価報告書を作成し、報告会を開催します。

※BBSecは、評価結果に基づきご活用いただける、電気事業者様向けセキュリティ対策支援サービスを各種取り揃えています。
（文書整備支援、標的型攻撃メール訓練、情報セキュリティ教育、脆弱性診断、HW/SWセキュリティ設定評価、インシデント対応訓練、CSIRT構築支援など）

評価基準 ■電力システムにおけるサイバーセキュリティリスク点検ガイド（2024年3月22日発行）

経済産業省は、サイバーセキュリティ対策の継続的改善・高度化に向け、電気事業者を対象として「電力システムにおけるサイバーセキュリティリスク点検ガイド」および「電力システムにおけるサイバーセキュリティ対策状況可視化ツール」を発行し、対策状況の確認、リスク評価、対策の改善への活用を推進している。

インシデント対応訓練

高度化・巧妙化するサイバー攻撃に対する組織の対応力強化

サイバー攻撃が悪質化・巧妙化し、被害も深刻化している現在、侵入を前提とした対応態勢の構築が、企業に求められています。そのためには、日頃から具体的なインシデントの発生を想定し、インシデント対応を担う組織が、事前に策定したインシデント対応手順に従い、できるだけ短時間で、かつ最小限の被害に抑えるための訓練を重ね、どのようなインシデントが発生しても対応できるように要員の対応力の向上を図ることが重要です。
BBSecのインシデント対応訓練サービスは、昨今のサイバー攻撃の動向を踏まえ、情報セキュリティの専門企業として培ってきた経験とノウハウに基づき開発された実践的な訓練プログラムを提供します。訓練を通して、経験豊富なセキュリティコンサルタントが、お客様の現状の対応態勢における課題を指摘し、改善のための適切なアドバイスを行うことで、お客様のサイバーセキュリティ強化/向上に貢献します。

インシデント対応訓練サービスの特長

BBSecは、お客様のインシデント対応態勢の成熟度や目的に応じて選択いただける2つの訓練形式をご用意しています。
いずれの訓練においても実践的なトレーニングの場を提供します。

サービス名	訓練の特長
インシデント対応訓練（ワークショップ型）	インシデント対応プロセスを体験しながら、要所で参加者によるディスカッションやコンサルタントによる解説を行います。参加メンバーの知識向上や経験の場となるだけでなく、インシデント対応態勢の今後の強化や改善点などの気づきを得ることができます。
インシデント対応訓練（ロールプレイング型）	緊迫感のある状況下で実際の役割に沿ってインシデント対応を疑似体験します。インシデント対応要員の習熟度を高め、組織間連携の問題点やボトルネック工程の把握など、具体的な強化や改善点を発見することでインシデント対応態勢の有効性を高めることができます。

インシデント対応訓練のシナリオ

インシデント対応訓練のシナリオは、国内外で実際に発生したインシデント事例をベースに幾つかの標準シナリオを用意しています。
標準シナリオの他、お客様で実際に発生したインシデントやヒヤリハットの経験を踏まえたオリジナルシナリオ（カスタマイズシナリオ）の開発も可能です。

No.	標準シナリオ	シナリオ説明
1	**標的型メール攻撃によるマルウェア感染**	標的型メール攻撃によりマルウェアに感染、その後、マルウェア感染が拡大し、別のマルウェアへの感染も発生
2	**フィッシングによるランサムウェア感染**	フィッシングサイトでマルウェアに感染。その後、ランサムウェアのダウンロード、権限昇格、横展開、情報窃取、サーバ暗号化を経て、攻撃者は身代金を要求
3	**Webサイトの改ざん**	Webサイトが改ざんされ、マルウェア配布サイトへ誘導された。フィッシングサイトへの誘導も同時発生

情報セキュリティリスクアセスメント

情報セキュリティ対策の現状を可視化し、効果的な対策をアドバイス

現在のサイバー攻撃は、あらゆる技術が駆使され複雑化・巧妙化してきています。また内部関係者から情報漏えいする可能性も懸念され、内外で起こりうる事故を完全に防ぐことは、非常に困難です。「リスクがどこにあるのか」「何を優先すべきなのか」など、現状を把握するための情報セキュリティリスクアセスメントは、情報セキュリティ対策の第一歩です。BBSecは専任コンサルタントが目的や企業環境に最適なフレームワークを選択して網羅的に実施するコンサルティング型アセスメントから、短時間・低予算でリスク概要のアセスメントレポートが得られるオンライン自己問診型アセスメントまで、幅広い情報セキュリティリスクアセスメントサービスを用意しています。
評価基準は、米国国立標準技術研究所(NIST)発行のCyber Security Framework(CSF)をベースガイドラインとしたものを利用します。

サービス一覧

■情報セキュリティリスクアセスメントサービス

コンサルタントがアセスメントを行い、報告書、課題/対策一覧を作成して報告会でご説明し、対策ロードマップを策定

内　容	・現状把握:文書確認、インタビュー、実機確認(設定評価)など ・分析/評価:課題の確認 ・第三者評価報告書、課題/対策一覧の作成 ・報告会の開催、メールによるQ&A対応 ・実施計画立案:対策ロードマップ策定
期　間	3か月～
ポイント	コンサルタントがお客様の状況をしっかり把握した上で行う王道のアセスメント

■簡易コンサル付 情報セキュリティセルフアセスメントサービス

お客様によるWEBでの自己問診アセスメント実施後、コンサルタントが追加ヒアリングを行って報告書を作成し、報告会でご説明

内　容	・WEB上の設問にお客様がマウスクリックで回答 ・コンサルタントによる結果確認と追加ヒアリング ・コンサルタントによる課題/対策一覧と対策ロードマップ案作成 ・報告会の開催、メールによるQ&A対応
期　間	最短8週間+Q&A対応2週間
ポイント	手軽で迅速なセルフアセスメントにコンサルタントの安心サポート(ヒアリングに基づく対策ロードマップ案作成と報告会)を付加

■情報セキュリティ対策実行支援型サービス BBSec Prime

コンサルタントによるアセスメント終了後、対策ロードマップを作成し、年間を通じた対策実行に関するアドバイスを提供

内　容	**リスクアセスメント** →	**アドバイザリ**
	・現状把握 ・分析/評価 ・第三者評価報告書、課題/対策一覧の作成 ・報告会の開催、メールQ&A対応 ・実施計画立案:対策ロードマップ策定	・対策実施支援 ・Q&A対応 ・関連情報提供 ・緊急時初動対応の助言 ・定例会(訪問/オンライン)
期　間	1年間(アセスメント 3か月～)	
ポイント	コンサルタントによるアセスメントと年間アドバイザリがセットになった費用対効果が高いサービス	

■情報セキュリティセルフアセスメントサービス

WEB設問にマウスクリックで回答するだけで2種類のレポートが生成され、セキュリティリスクの概要を短時間に把握

内　容	・WEB回答によるセルフアセスメント: 統制、識別、防御、検知、対応、復旧の実態を可視化 ・評価レポートの作成と送付
期　間	3週間の回答期間後1週間以内に評価レポートを提供
ポイント	予算も時間も抑えて手軽にレポートが得られ、リスク分析や計画策定など次のステップへの移行に活用可能

※業界や目的に特化したリスクアセスメントサービスも用意しています。詳細は個々のサービス紹介ページをご覧ください。

■金融機関向け 情報セキュリティリスクアセスメント･･･P.25　■産業制御システム向けセキュリティリスクアセスメント･･･P.27　■サプライチェーン情報セキュリティリスクアセスメント･･･P.32

金融機関向け 情報セキュリティリスクアセスメント

金融機関に要求される高いレベルの情報セキュリティを確保するために、可視化を行い迅速に対応

金融機関は顧客情報や重要情報を保有しています。また、業界再編に伴うシステム統合や新商品・サービスの拡大などに伴い、金融機関の情報システムは一段と高度化・複雑化しています。現在のサイバー攻撃は、あらゆる技術が駆使され複雑化・巧妙化してきています。また内部関係者から情報漏えいする可能性も懸念され、内外で起こりうる事故を完全に防ぐことは、非常に困難です。BBSecは、金融機関向けにFISCガイドライン準拠性を評価し、迅速に課題と次の一手となる対策を提示する情報セキュリティリスクアセスメントサービスを、お客様のニーズにあわせて各種取り揃えています。リスク分析や計画策定など次の一手に進むために、是非、ご活用ください。

サービス一覧

■金融機関向け 情報セキュリティリスクアセスメントサービス

コンサルタントがアセスメントを行い、報告書、課題/対策一覧を作成し、報告会で説明

内　容	・現状把握：文書確認、インタビューなど ・分析/評価：課題の確認 ・第三者評価報告書、課題/対策一覧の作成 ・報告会の開催、メールによるQ&A対応 ・実施計画立案：対策ロードマップ策定（オプション）
期　間	3か月～
ポイント	コンサルタントがお客様の状況をしっかり把握した上で行う王道のアセスメント

■金融機関向け 情報セキュリティクイックオンラインアセスメントサービス

お客様によるWEBでの自己問診アセスメント実施後、コンサルタントが追加ヒアリングを行い報告書を作成し、報告会で説明

内　容	・WEB上の設問にお客様がマウスクリックで回答 ・コンサルタントによる追加ヒアリング、分析/評価 ・コンサルタントによる報告書作成 ・報告会の開催、メールによるQ&A対応
期　間	1.5か月
ポイント	手軽な自己問診型アセスメントにコンサルタントによる安心サポート（ヒアリング、報告会）をセット

■情報セキュリティ対策実行支援型サービス BBSec Prime

コンサルタントによるアセスメント終了後、対策ロードマップを作成し、年間を通じた対策実行に関するアドバイスを提供

内　容	**リスクアセスメント** →	**アドバイザリ**
	・現状把握 ・分析/評価 ・第三者評価報告書、課題/対策一覧の作成 ・報告会の開催、メールQ&A対応 ・実施計画立案：対策ロードマップ策定	・対策実施支援 ・Q&A対応 ・関連情報提供 ・緊急時初動対応の助言 ・定例会（訪問/オンライン）
期　間	1年間（アセスメント 3か月～）	
ポイント	コンサルタントによるアセスメントと年間アドバイザリがセットになった費用対効果が高いサービス	

■自己問診型 FISCガイドライン準拠性評価サービス

お客様によるWEBでの自己問診アセスメント結果に基づいてコンサルタントが報告書を作成し、電子ファイルで提供

内　容	・WEB上の設問にお客様がマウスクリックで回答 ・コンサルタントによる分析/評価、報告書作成、 メールによる報告書提出、QA対応
期　間	1.2か月
ポイント	手軽な自己問診型のアセスメントながらコンサルタントがポイントをしっかり押さえて報告書を作成（ヒアリング、報告会はありません）

金融機関向け情報セキュリティアセスメントの評価基準

評価基準として金融情報システムセンター（FISC:The Center for Financial Industry Information Systems）が制定した金融機関等コンピュータシステムのための安全対策基準（FISCガイドライン*）を利用します。（*サービス提供時点での最新版に対応）

地方公共団体向け 情報セキュリティ セルフアセスメント

簡易的なアセスメントで現状を可視化し、今後の検討に役立てる

サイバーセキュリティの脅威がますます高度化、複雑化する中、住民の個人情報をはじめとする重要データを保有する地方公共団体におけるセキュリティ対策の重要性もさらに増しています。
このような背景から、総務省は、地方公共団体に対し、『地方公共団体における情報セキュリティポリシーに関するガイドライン』に基づき、サイバー攻撃に対処するための基本方針の策定と公表を求めています。
また、政府や地方公共団体の利用に特化したクラウドサービス『ガバメントクラウド』では、高いセキュリティ基準と信頼性が求められます。
本サービスは、地方公共団体が、これらの要求に迅速に対応するための有効な第一歩として、ガイドラインに則した現状把握を短時間で可能とするサービスです。
サイバーセキュリティの脅威から重要データを護るために、自組織のセキュリティ対策の速やかな現状把握と対策強化検討への移行に向け、是非ご活用ください。

サービスの特長

厳選した設問により、効率的かつ網羅的にアセスメントを実施します。
短期間で評価結果、課題、具体的な対策案を得ることで、迅速に次の対策フェーズに進むことができます。

以下のような課題やご要望に対応します。

- 本格的な情報セキュリティリスクアセスメントを実施したいが**予算が足りない**
- 情報セキュリティリスク対応として**何から手をつけてよいのかわからない**
- **定期的に自己点検**するツールが欲しい
- **ガバメントクラウド**を利用する際の簡易アセスメントを行いたい
- **時間をかけずに**情報セキュリティリスク対応の現状を把握したい
- 情報セキュリティインシデントが発生したので**緊急点検**を行いたい

情報セキュリティリスクアセスメントの評価基準

「総務省　地方公共団体における
情報セキュリティポリシーに関するガイドライン」

地方公共団体が情報セキュリティ管理を適切に行うための基本的な方針と手順を定めたものです。このガイドラインは、地方公共団体が直面するサイバー攻撃や情報漏えいのリスクに効果的に対応し、市民の個人情報や重要な行政情報を保護するための対策を具体化しています。

実施プロセス

環境準備(BBSec) ▶ 利用開始案内 ▶ WEBによるセルフアセスメント ▶ 利用終了 ▶ レポート作成（BBSec） ▶ レポート送付 ▶ 【オプション】コンサルタントによるアドバイザリ※

3週間　／　1週間以内　／　1か月

※ コンサルタントによるアドバイザリ（報告/解説/質疑応答）をご希望の場合は、別途ご支援可能です。

産業制御システム向け セキュリティリスクアセスメント

産業制御システム(ICS)のセキュリティリスクを可視化し、今後とるべき対策に役立てる

近年、工場や発電所などのプラントやインフラの制御システムがサイバー攻撃の対象となるケースが増えています。これらに対するリスクアセスメント(リスクの特定・分析・評価)は、事業継続性を維持するために極めて重要です。
BBSecの産業制御システム向けセキュリティリスクアセスメントサービスは、情報セキュリティ対策の第一歩である現状把握を行い、お客様の現状を踏まえた上で、今後とるべき対策について提案します。

サービスの概要

システムの分析 / 可視化に加え、当社独自のフレームワーク*を用いて現状のセキュリティ対策の有効性と網羅性を検証し、今後の対策ロードマップを提示します。

*情報セキュリティの最新かつ事実上の世界標準でもある米国国立標準技術研究所(NIST)発行の「Cyber Security Framework (CSF)」をベースに、「NIST SP800-53」「NIST SP800-82 」「IPA制御システム分析ガイド」「IEC62443 」等を踏まえた上で、工場など実際に現場で評価を行うことを考慮した評価基準をBBSecが独自編纂

システム全体のリスクアセスメント

当社独自のアセスメント手法により、対象システム全体のリスクアセスメントを行います。

対策ロードマップの策定

アセスメント結果を踏まえ、実現可能な対策ロードマップを策定します。

コンサルティングプロセス

準備 ▶ キックオフ ▶ 調査 ▶ 分析評価 ▶ 改善プラン検討 ▶ 報告書作成 ▶ 報告会 ▶ 対策ロードマップ策定

調査
- ・文書確認
- ・インタビュー
- ・実機確認
- ・資産明確化

産業制御システム向けセキュリティサービス体系

本サービスは、産業制御システム向けセキュリティサービス体系の1サービスとして提供しています。
フェーズに合わせて他のサービスも併用することで、サイバーリスクに強いシステムを構築・運用することが可能です。

現状把握	体制構築	発展維持
■現状可視化、現状評価 ■必要な課題の顕在化と優先順位	■運用改善(モニタリング強化) ■規程、手順書類における改訂 ■組織・体制検討(外部委託を含む)	■日々のセキュリティ運用 ■検知策、対応策 ■教育・訓練
産業制御システム向け リスクアセスメントサービス	体制構築支援	セキュリティ教育
SQAT® for IoT	セキュリティ・アドバイザリ (助言コンサルティング)	セキュリティ・アドバイザリ (助言コンサルティング)

EC加盟店様向け セキュリティ・チェックリスト対応アセスメント

2024年3月 クレジットカード・セキュリティガイドラインが5.0版に改訂

EC加盟店に対してチェックリストによるセキュリティ項目の確認が求められる

2024年3月に改訂されたクレジットカード・セキュリティガイドラインのカード情報保護対策の中で、基本的なセキュリティ対策として**「セキュリティ・チェックリスト」による確認の項目が追加**されました。EC加盟店は新規加盟店契約申し込み前にセキュリティ・チェックリストに記載の対策を実施し、その状況をアクワイアラーに申告することが求められています。さらに2025年4月からは新規のEC加盟店だけでなく、すべてのEC加盟店に対して求められます。

クレジットカード・セキュリティガイドラインとは? セキュリティ・チェックリストとは?

クレジットカード・セキュリティガイドライン

クレジット取引セキュリティ対策協議会から、2020年3月に「実行計画」の後継文書として公表されました。
安全・安心なクレジットカード利用環境を整備するため、クレジットカード会社、加盟店、PSP等のクレジットカード決済に関係する事業者が実施すべきクレジットカード情報の漏えい及び不正利用防止のためのセキュリティ対策の取組を取りまとめたものです。

セキュリティ・チェックリスト

クレジットカード・セキュリティガイドラインの付属文書として2021年3月に第1版が策定されました。
セキュリティ対策強化に必要な取組を示し、EC加盟店におけるセキュリティ意識の向上と基本的なセキュリティ対策の強化、これによるカード会員データの漏えい及び不正利用の防止を目的としてとりまとめたものです。

セキュリティ・チェックリストではどんなことを求められる?

- 管理画面のアクセス制御について
- データディレクトリの公開などECサイトのシステム設定について
- 脆弱性診断の定期実施について

セキュリティ・チェックリストではこのほかにも複数のセキュリティ対策の実施が求められます。

サービス内容

ニーズやご予算に合わせたサービスのご提供が可能です。ご支援期間の延長なども承ります。

コース	内容
アセスメント＋是正支援	**・セキュリティチェックリストの各項目に対する実施状況の確認(アセスメント)** ⇒ Web会議ベースで実施します。(1回2時間×2回) ⇒ アセスメント結果分析と未対応項目に対する具体的な是正方法を含む報告書を作成します。報告書についての説明会を実施します。(1回2時間×1回) **・是正推進支援 3ヶ月間** ⇒ Web会議(各月1回2時間×1回)とメールベースのQA支援を行います。 ⇒ 開発ベンダとの打ち合わせに同席し、開発ベンダに実施いただきたい内容について直接説明等を実施します。
アセスメント	**・セキュリティチェックリストの各項目に対する実施状況の確認(アセスメント)** ⇒ Web会議ベースで実施します。(1回2時間×2回) ⇒アセスメント結果分析と未対応項目に対する具体的な是正方法を含む報告書を作成します。報告書についての説明会を実施します。(1回2時間×1回)
オンライン勉強会	**・セキュリティチェックリストの内容、確認すべき事項についてのオンライン勉強会** ⇒ Web会議ベースで実施します。(1回2時間×1回) **・勉強会開催後最大1ヶ月間のメールベースでのQAサポート**

【ご注意点】セキュリティ・チェックリストは、クレジットカード・セキュリティガイドラインの付属文書であり、これを当社サービスを通じてご提供するものではありません。
セキュリティ・チェックリストについては発行元の定めるルールに従い、入手取り扱うものとなります。

自己問診型 テレワーク環境情報セキュリティリスクアセスメント

新しいビジネス様式に求められるテレワーク環境のセキュリティリスク把握に効果を発揮

テレワーク環境の情報セキュリティ対策は、他のセキュリティ対策同様、テレワーク環境が不正侵入の入口にならないように「リスクがどこにあるのか」、「何を優先すべきなのか」を可視化して把握した上で、「時機を逸さずに対策を実施すること」が必要です。本サービスでは、テレワーク環境が陥りがちな対策漏れを、第三者の視点から組織/IT 両側面から評価・査定・分析し、課題と対策を提示します。

サービスの特長

短期間で現状の把握が可能
標準環境の場合、約1カ月でアセスメントを完了することが可能です。

対策の具体案を提示
アセスメントの評価結果だけでなく、課題と優先順位、具体的な対策案を提示します。

効率的かつ網羅的なアセスメント
自己問診型評価シートへのご記入と当社のアセスメントを連動して行うことにより効率的な全体把握が可能です。

総務省のガイドラインに準拠
テレワークセキュリティガイドライン第5版（総務省）の評価基準を採用。社内外に結果を公表する際に、その信頼性を高めます。

サービスの流れ

準備	現状把握	報告書作成	報告書送付	Q&A
事前情報の確認 サイトご連絡	Webによる 自己問診回答			
	2週間	1週間		2週間

自己問診型チェックシート質問内容

■ 概要把握項目
テレワーク実施の概況、テレワーク実施環境の概況等

■ 運用確認項目
1. 統制・管理について（情報セキュリティ対策の整備、情報資産の重要度区分など）
2. 運用管理について（Web サイトへのアクセス、セキュリティパッチファイルの適用、情報機器の盗難・紛失の対策、外部サービス利用における対策など）

自己問診型 個人情報に関わる情報セキュリティアセスメント

情報セキュリティ対応状況の簡易アセスメントをオンラインで行い現状を可視化、迅速に次の一手を考える

改正個人情報保護法の2022年4月からの全面施行に伴い、個人情報の取扱いルールはより厳しくなり、個人の権利保護が強化されました。その背景には企業からの個人情報漏えいが急増していることが挙げられます。
現在のサイバー攻撃は、あらゆる技術が駆使され複雑化・巧妙化してきています。ひとたび流出してしまうと企業の信用問題に大きな影響を及ぼしてしまう個人情報をどう守っていくかは、すべての企業にとって喫緊の課題と言えるでしょう。
本サービスは、情報セキュリティの観点から個人情報保護対策の現状を把握したいお客様に向けた情報セキュリティリスクアセスメントです。お客様ご自身で自己問診型リスクアセスメントをオンラインで実施いただき、入力結果に基づきセキュリティの専門家であるコンサルタントが、第三者の視点から短期間で評価レポートをまとめ、課題と対策を提示します。

このようなことでお困りではありませんか？

- 個人情報保護強化の必要性は認識しているが、情報セキュリティの観点で何に取組めばよいのかわからない。
- 短時間で、あまり手間をかけずに個人情報に関する情報セキュリティ対応の現状を把握したい。
- 急速なテレワークの普及にルールの整備が追い付いていない。個人情報保護対応に漠然とした不安を感じている。

サービス提供プロセス

サービスのポイント

厳選した質問による自己問診をオンラインで行い、効率的かつ網羅的なアセスメントを実施します。短期間で評価結果、課題と優先順位、具体的な対策案を得ることで、迅速に次の対策フェーズに進むことができます。

情報セキュリティ対策は「**リスクがどこにあるのか**」「**何を優先すべきなのか**」を把握した上で、「**時期を逸することなく行うこと**」が重要です。

個人情報に関わる情報セキュリティアセスメントの評価基準

■**BBSec-DSS for Privacy Protection**　個人情報保護に関する情報セキュリティ要件を取入れた弊社独自のDSS(Data Security Standard)を評価の基準として使用します。

情報セキュリティ自己点検アンケート

意識調査で貴社の現状課題をしっかりと把握

情報セキュリティは、PDCAサイクルを回し、常に見直すことが重要です。本サービスは、自己点検として、従業員の情報セキュリティポリシーの理解度や遵守状況を測る意識調査をWebアンケートで行い、結果を分析し、現状の課題を報告します。
アンケートは、お客様のご要望、ニーズに合わせて開発する「カスタムメイド」と、BBSecが長年培ってきた経験と蓄積された知見に基づき最適化されたセキュリティ項目を網羅した「標準アンケート」を用意しています。

アンケートの設問

■カスタムメイド

お客様のご要望、ニーズに合わせたオリジナルのアンケート

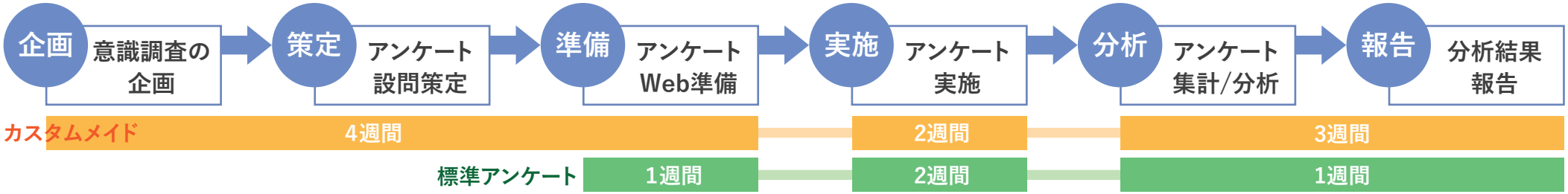
- ●意識調査の企画
- ●アンケート設問策定支援
- ●アンケートWeb準備
- ●アンケート提供
- ●アンケート結果集計・分析
- ●報告書作成
- ●報告会

■標準アンケート

最適化されたセキュリティ項目を網羅した標準アンケート

- ●アンケートWeb準備
- ●アンケート提供
- ●アンケート結果集計・分析
- ●報告書作成

アンケートのプロセス



★標準テンプレート利用の場合、最短1か月で実施可能です。
★意識調査の分析結果をレポートで報告します。今後の情報セキュリティ強化ポイントが明確になります。
★アンケート結果を踏まえた効果的な情報セキュリティ教育を提供することも可能です。詳細は別途お問い合わせください。

自己問診型セキュリティリスクアセスメント

「我が社は大丈夫なのか?」
その問いに答える、リスクアセスメントのスタートアップサービスです。
Web上の設問にマウスクリックで回答するだけで、2種類のレポートを入手することができます。現状を把握しリスク分析や計画策定など次の一手に進むための第一歩として、是非ご活用ください。

■レポート

自己問診型リスクアセスメント	識別、防御、検知、対応、復旧の実態を可視化
CSIRT成熟度モデル評価	CSIRT 構築・運用の目標水準と現状とのギャップを可視化

サプライチェーン情報セキュリティリスクアセスメント

情報セキュリティリスクの可視化と対策検討

大手企業が情報セキュリティ対策を強化する中、新たな攻撃スタイルとしてサプライチェーン攻撃が注目を集めています。
「A chain is only as strong as its weakest link」(鎖全体の強度は、その中の最も弱い環で決まる)
攻撃者は、サプライチェーン上の情報セキュリティ対策が手薄な取引先、子会社、グループ関連会社を経由して最終的なターゲットとなる企業や組織を狙います。このため、グローバル企業は、喫緊の課題としてサプライチェーンの情報セキュリティリスク管理に取り組み始めています。
BBSec は、第三者の視点でサプライチェーン上の企業に対する情報セキュリティリスク対策の現状を把握、分析し、今後とるべき対策について提案します。

コンサルティングプロセス

準備 ▶ キックオフ ▶ 調査 ▶ 分析 ▶ 改善プラン検討 ▶ 報告書作成 ▶ 報告会 ▶ 対策ロードマップ策定

調査
・文書レビュー
・ヒアリング

ポイント 可視化した課題に対しリスク評価し、ビジネス固有のリスクを加味した重み付けを行うことにより課題の優先度を定義します。
また、課題に対し具体的な対応策について、対策ロードマップとしてご提示します。

サプライチェーンの情報セキュリティ対策の有効性と網羅性をチェック

情報セキュリティリスクアセスメントの評価基準

サイバーセキュリティ対策基準「NIST SP800-171」をベースにサプライチェーンのリスクアセスメントを実施します。

サイバーセキュリティ対策基準「NIST SP800-171」

NIST(National Institute of Standards and Technology:米国標準技術研究所)が定めたセキュリティ基準で、アメリカ国防総省は、取引のある全世界の企業・サプライヤーに対して本基準を遵守するよう求めています。本基準は、政府機関や防衛産業のみならず民間企業にとっても有用であることから、様々な産業においてサプライヤーが準拠すべきセキュリティ基準として事実上の国際標準として各国で活用され始めています。

自己問診型 FISCガイドライン準拠性評価

FISCガイドライン準拠性評価をオンラインで行うことで現状を可視化し、今後の検討に役立てる

金融機関は顧客情報や重要情報を保有しています。また、業界再編に伴うシステム統合や新商品・サービスの拡大等に伴い、金融機関の情報システムは一段と高度化・複雑化しています。
現在のサイバー攻撃は、あらゆる技術が駆使され複雑化・巧妙化してきています。また内部関係者から情報漏えいする可能性も懸念され、内外で起こりうる事故を完全に防ぐことは、非常に困難です。
本サービスは、金融機関向けに簡易的な手法によりFISCガイドライン準拠性を評価し、迅速に課題と次の一手となる対策を提示するサービスです。お客様ご自身で自己問診型リスクアセスメントをオンラインで実施いただき、入力結果に基づきセキュリティの専門家であるコンサルタントが評価レポートをまとめ提示します。

サービスの特長

■ポイント

お客様による回答

WEB上のFISCガイドラインに基づく設問に対してマウスクリックで回答します。

評価・報告

お客様による回答完了後、1週間以内に評価報告書をメールいたします。

現状を把握

評価報告書により今後の情報セキュリティ強化ポイントが明確になります。

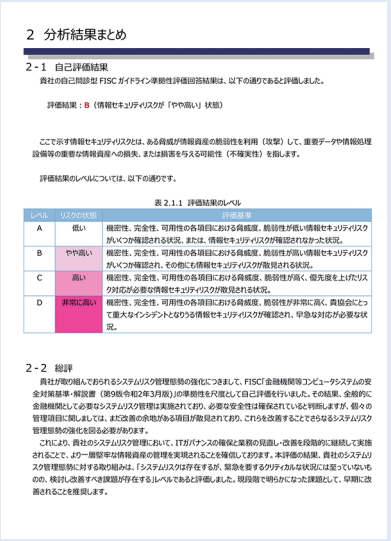
評価基準

評価基準として金融情報システムセンター(FISC:The Center for Financial Industry Information Systems)が制定した金融機関等コンピュータシステムのための安全対策基準(FISCガイドライン*)を利用します。

(*サービス提供時点での最新版に対応)

入力画面

報告書サンプル



FISC安全対策基準(FISCガイドライン)

- 「銀行法」、「金融庁所管の監督指針」に紐づいており、金融情報システムに関する事実上わが国唯一の権威ある安全対策の拠りどころとして広く活用されています。
- 金融機関等の情報システムに関する安全対策の具体的指針を、「統制基準、実務基準、設備基準、監査基準」の4つの視点で示します。

ネットワーク機器設定評価

ネットワーク機器の設定ファイルを分析 / 評価。セキュリティ上の問題を可視化し改善案を提供

ネットワークインフラを適正にハードニング（堅牢化）するためには、アクセス制御をはじめとした適切な設定は必要不可欠です。しかし現状では”追加設定漏れ”によるリスクの拡大は、避けて通れない道です。本サービスでは、ネットワーク機器の設定を評価し、セキュリティ上の問題点を可視化します。設定ファイルを直接評価することで、ネットワーク経由の通信に擬似攻撃を用いた脆弱性スキャンでは発見できない問題を可視化します。

評価の流れ

対象となるネットワーク機器の設定ファイルをご提示いただき、当社で分析/評価し、発見された問題/そのリスク/対策方法を報告します。
設定ファイル受領後3週間が報告会開催の目安です。

設定ファイル受領

分析

自動ツールと専門技術者の目視による解析を組み合わせ、問題点を抽出します。

評価・報告書作成

問題点を【緊急・重大・危険度 高 / 中 / 低・問題なし】の六段階で評価し、対処すべき改善案を検討します。

報告会

分析結果の報告と共に改善案を提示し、質疑応答/ディスカッションを行います。

アクションリスト提示

再チェック

問題箇所に対するお客様による改善状況を確認します。
※再チェックは、報告書提出から3か月以内とさせていただきます。
※再チェックの結果は、報告書の指摘事項に基づいた合否のみの報告です。

具体的な脆弱性箇所と修正方法を提示、再チェックにより改善を把握

ネットワーク機器の設定に脆弱性があると・・・

設定ミスやパッチファイルの追加設定非対応などのネットワーク機器の設定不備は、悪意ある攻撃者によるバックドア構築や攻撃の踏み台として悪用されるリスクを生み出します。
非公開のネットワーク機器のソフトウェアは攻撃を受けにくいという通説も、実際に感染のインシデントが報告されており、リスク回避にはつながりません。

<指摘例>CISCO IOS（Catalyst3650）の場合

当社による指摘レベル：
レベル3（高）

指摘時の設定

```
400 line vty 5 15
401 access-class 23 in
….
406 transport input telnet ssh
```

Telnet サービスの利用

修正提案

```
406 transport input none
または、
406 transport input ssh
```

データベース設定評価

多角的な評価によりシステムの要であるデータベースのリスクを発見

組織の重要情報が格納されているデータベースを評価するサービスです。内在するセキュリティリスクを可視化し、重大なインシデントが発生する前に有効な対策を施します。本評価では、リスクの可視化に加え、国内外のセキュリティ基準適合状況やデータベース環境・管理面に関する助言も同時に実施いたしますので、企業のリスクマネジメントに対する指標としても効果を発揮します。

サービスの特長

各種設定を調査
設定情報とコンポーネントへ適用している各種環境設定を評価します。

問題箇所特定と緊急度を可視化
必要不可欠な問題点の特定に加え、その緊急度・解決策をスピーディにお知らせします。

管理面や運用面の問題点も抽出
外部からの攻撃や内部からの情報漏えい対策として、権限設定などの管理面で配慮すべき対策や解決方法を提案します。

主要データベースに対応
Oracle、MySQL、Microsoft SQL Server、PostgreSQL など、主要なデータベースに対応しています。
※対応DBの詳細は、当社までお問い合わせください。

主な評価項目

評価項目	評価内容
アカウント管理に関する設定	データベース接続ユーザに対する特権をはじめとする各種権限の付与状況や、ロールが適切に設定されているか等を診断します。
認証に関する設定	セキュアな認証方式が設定されているか、デフォルトのパスワードを設定していないか等を診断します。
監査・ロギングに関する設定	保存ポリシーなど、監査やログ取得に関する各種設定が適切になされているか、監査データへのアクセス権限等を診断します。
パラメータに関する設定	データベースの構成に関する各種パラメータの値がセキュリティ基準に適合しているか診断します。
パッチ適応状況	導入しているデータベースのソフトウェアに存在する脆弱性を修正するセキュリティパッチが適用されているか診断します。

評価例

指摘事項	データベースにおけるアクセス制御の不備
この脆弱性におけるリスク	攻撃者がネットワークへ侵入した場合、容易にデータベースへアクセスすることが可能である。そのため、現状では、データベースに存在する個人情報をはじめとした重要情報が流出する危険性をはらんでいるといえる。
対策例	ネットワーク単位でのアクセス許可に加え、パスワード認証を設定する。

無線LAN調査

オフィスに忍び寄る不正アクセスを見つけ出し、潜在的なリスク低減へとつなげる

オフィス内でアクセス可能な無線LANが、すべて安全とは限りません。セキュリティ対策がなされていない公衆WiFiや悪意ある電波に接続すると、「盗聴」「なりすまし」「不正アクセスによる情報漏えい」などにつながる危険性があります。自社のオフィスにおいて、インターネットを有効活用しながら安心して業務を遂行できる環境を社員に提供するために、BBSecの「無線LAN調査サービス」では、社内でアクセス可能な無線LANの実態調査とそのリスク検証を行います。

サービスの特長

一般社員のセキュリティリスクを軽減
誰もがアクセスできるリスクある無線LANを把握することができます。

リスクある無線LANを把握
不正な無線LANを抽出するだけでなく、暗号化強度が弱い信頼すべき事業者の無線LANも把握することができます。

自社改善の成果を検証
調査結果に基づく、社内環境再整備の結果を再調査で確認することができます。

更なる改善のためのコンサルティングと連携
自社での改善が難しい場合は、プロフェッショナルな立場から様々な回避方法をご提案いたします。

サービスの流れ

準備

調査

ツールによる調査 / スペシャリストによる調査

調査対象エリアに存在する無線LANのアクセスポイントを洗い出します。通常のアクセスポイントスキャンでは発見が難しいステルス化された無線 LAN（故意 / 偶発的を共に含む）や不要な無線 LAN、暗号化されていない危険な無線LANなどの発見が可能です。

分析・報告書作成

オフィス内の無線LANの電波状況を可視化してレポートします。

報告会

総務部門などITに詳しくない部門の皆様にも現状把握ができるよう、わかりやすく解説していきます。

お客様による対処

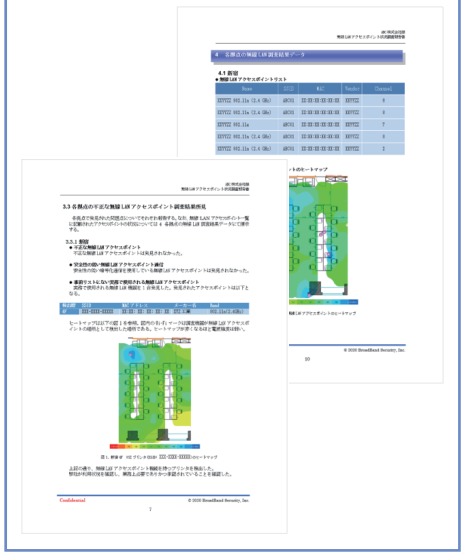
再調査（オプション）

お客様ご自身により、リスクあるアクセスポイントを撤去いただいた後、当社にて再調査を実施します。

改善コンサルティング（オプション）

お客様ご自身では解決できなかったアクセスポイントへの対応、日々変化する状況への対応策など、無線LANから御社を守るための様々な施策を共に考えていきます。

レポートサンプル



情報セキュリティ教育

セキュリティ・リテラシーを高め組織全体のセキュリティ対応力を強化

サイバー攻撃対策の要は「人」です。サイバー攻撃が悪質化・巧妙化し、被害も深刻化している現在、情報セキュリティ対策は、技術的なソリューションの導入だけでは不十分です。BBSecは、情報セキュリティの専門企業として培ってきた経験とノウハウに基いた実践的な各種教育プログラムを提供することで、お客様のサイバーセキュリティ強化/向上に貢献します。

高度化・巧妙化するサイバー攻撃対策の要となる人材の育成をサポート

お客様のご要望、ニーズに合わせてカリキュラムを検討し、実践的な各種教育プログラムを提供します。以下は参考プランです。

対象	教育プログラム	サービス内容
■一般従業員 ■情報システム部門 ■経営幹部	情報セキュリティ研修	組織での役割やレベルに応じたセキュリティ教育を行います。業務遂行上、遵守すべきセキュリティ事項の説明に加え、ニュースで取り上げられた最近のセキュリティトピックをわかり易く解説します。
	標的型攻撃メール訓練	擬似標的メールを社員に送付し開封したかどうかを確認し組織対応力を可視化します。メール訓練の前後に教育を実施し、標的型攻撃の手口、最近の被害事例などを中心に解説し、従業員に注意喚起を促します。
	情報セキュリティに対する意識調査と教育	WEBアンケート形式で情報セキュリティに関する質問に回答することにで、社員の意識調査を実施します。集計結果の分析に基づき、情報セキュリティ対策が必要な項目を中心に社員教育を実施します。
■情報システム部門 ■アプリケーション開発者	セキュアWebアプリケーション開発講座	OWASP Top10など最新情報を踏まえWebアプリケーションのセキュア開発について講義します。
■情報システム部門 ■CSIRT	インシデント対応訓練	情報セキュリティインシデントへの組織対応力を高めるため、具体的なシナリオに従ってロールプレイング形式で訓練を実施します。
■情報システム部門	ハードニング講座	●Linux OS環境における堅牢化講座 ●Windows Server環境における堅牢化講座 ●IIS環境における堅牢化講座 ●MS SQL環境における堅牢化講座 ●クラウド環境における堅牢化講座
	ペネトレーション技術者養成講座	【理論編】講義によるペネトレーションテストに必要な技術的知識の習得を目指します。 【実践編】講義とハンズオンによるペネトレーションテストを実践します。
■情報システム部門 ■設計開発部門	SecuriSTシリーズ ・脆弱性診断士養成 ・ゼロトラストコーディネーター養成 他	開発工程で抑えるべきセキュリティ要件を網羅した非セキュリティ人材向けセキュリティ教育講座です。IT担当者だけではなく、営業・事業企画担当者もセキュリティの知識を学び、共通言語化することで、お客様のセキュリティ事業の立ち上げを支援する内容を学べます。

※上記教育サービスは、お客様企業の役職員を対象とし、お客様ごとの個別開催となります。集合形式だけでなく、オンライン形式でも提供可能です。詳細はお問い合わせください。

標的型攻撃メール訓練

企業を標的型攻撃から守る最後の砦は社員一人一人の経験値に基づく判断

セキュリティシステムを通り抜け、社員の手元に届いてしまう正常通信を装った標的型攻撃を完全に排除する方法は、現段階では存在しません。その為、これら攻撃に対する唯一の対策はメールを受け取った一般社員がそのメールにリスクを感じ、添付ファイルの開封やリンクへのクリックを行わないということです。標的型攻撃メール訓練サービスは、日々送られてくるメールに対し、個々の社員が標的型攻撃のメールであるか否かを判断する力を養い、会社のリスクを軽減させるプログラムです。

サービスの特長

社内の実情を可視化
標的型攻撃メールに対する組織対応力を把握、可視化することができ、現状を踏まえた次の一手を考える上での素材となります。

スキルアップツールとして活用可能
定期的な実施により、社員のスキルアップ状況を把握することが可能です。

ニーズにあわせ、カスタマイズも可能
標準パッケージに加え、結果報告会や社員アンケートなどのオプションをご用意しています。また、お客様の企業規模や風土など、個別のニーズにあわせたカスタマイズも可能です。

社員のセキュリティへの意識づけができます
訓練は、標的型攻撃メールへの対応力向上だけでなく、個々の社員のセキュリティに対する意識づけを強化することにつながります。

報告体制も同時に確認
インシデント発生時の迅速な報告体制づくりにも役立ちます。

サービス概要

BBSecから擬似攻撃メールを訓練対象者に配信します。擬似攻撃メールには添付ファイルや誘導用URL リンクがついており、メールを受け取った対象者がそれを開封したかを確認していきます。

メール訓練

準備	訓練メール	種明かしメール	集計・報告書
・関係者への説明 ・セキュリティ機器へのホワイトリスト登録 ・メール送信テスト	・擬似攻撃メール配信	・訓練対象者に種明かしメールを配信	・結果集計 ・報告書作成、結果報告

セキュリティ教育（オプション）

事前教育	自己判断	アンケート習熟テスト	事後教育
・訓練対象者に対する事前教育実施	・対象者による自己診断	・アンケート及び習熟度確認テスト実施	・事後教育実施

訓練終了、社内報告および再教育実施等

PCI準拠支援/オンサイト評価

実績あるPCI DSS準拠訪問評価機関として、信頼のコンサルティング/訪問評価を実施

カード決済の利便性は誰もが認める一方、情報漏えい事故はとどまるところを知りません。PCI DSS 、このような事故を未然に防ぐ為に設計されたクレジットカード業界の国際的なセキュリティ基準です。BBSecでは、PCI DSSに準拠をめざす組織に対し、蓄積されたノウハウを生かし、現状整理やGAP分析などの初期段階からオンサイト評価に至るまで、一貫した支援を展開しています。

サービスの特長

オンサイト評価の認定評価機関(QSA)
2008 年にPCI DSS評価機関として認定されて以来積み重ねてきたノウハウで、効率的な準拠への道筋を示すことが可能です。

PCI P2PE、PCI 3DS認定評価機関
QSA に加え、P2PE(カードデータのPoint to Point暗号化)、PCI 3DS (3D セキュア) の準拠支援、オンサイト評価も可能です。

専門コンサルタントが準拠をサポート
QSA、CISSPなどの国際的な資格をもつコンサルタントと高い技術力をもつスペシャリストが、お客様をサポートいたします。

グローバル対応
アジア及び欧米でのオンサイト評価の資格を保有。グローバル企業の海外拠点にも、日本本社と同一視点のGAP分析や評価判断が可能です。

QSA有資格者(AQSAを含む)	29
準拠認定付与案件数	811
準拠認定付与企業数	154

(2024年3月現在)

準拠までの標準的プロセス

現状分析後、何をすべきかを明確に提示します。その後、準拠取得への早道となるスコープの最小化を行い、PCI DSS の要求事項を満たす文書 / プロセス / システムを共に整備していきます。

Phase 1 GAP分析(現状調査と現状認識)
・文書レビュー、業務ヒアリング
・プライマリアカウント番号(PAN)のデータフロー確認
・現状の可視化(レポーティング)

Phase 2 構築(準拠対策)
・スコープの最小化検討　・システム改修検討
・運用体制改善検討　・規程／手順書改訂

Phase 3 オンサイト評価
・PCI DSS認定評価人QSAによるオンサイトの準拠評価
・準拠レポートROC及び準拠証明書AOCの作成
・ROC、AOCをカード会社に提出(貴社)

準拠認定
・企業の信頼性とブランドが向上
・情報漏えいなどのインシデントが発生時、
・カード会社の救済措置プログラムを受けられる。

サービス一覧

	プロセス	
準拠支援	PCI準拠支援コンサルティング	お客様へのヒアリングを通じ、PCI DSS準拠までの道のりをトータルで支援します。PCI P2PEやPCI 3DSへの準拠支援も対応します。
準拠支援	PCI ウォークスルー	短期間で全要件の簡易的なインタビュを行い、現状確認と対策説明を実施します。準拠前の全体チェックを行いたいという企業様にお勧めです。
準拠支援	SAQ作成支援コンサルティング	自己問診票(SAQ)にてPCI DSS準拠をご検討されている企業様のSAQ作成をご支援します。SAQタイプの選定からSAQ作成後のレビューまでサポートします。
準拠支援	委託先セキュリティ点検	PCI DSS要件で求められる委託先のセキュリティチェックを実施します。委託内容に合わせ、物理セキュリティの確認や端末の実機確認等を行います。
オンサイト評価	PCI DSS オンサイト評価	PCI SSCより認定を受けたQSAによる訪問審査です。リモート対応を中心として価格を抑えた「Value オンサイト評価」や、対象要件を絞って短期間で実施する「データセンター向けオンサイト評価」も提供します。
オンサイト評価	PCI P2PE オンサイト評価	PCI P2PEは、カード情報の伝送経路におけるPoint to Point暗号化を定めた基準です。P2PEソリューションを提供する企業様向けに、PCI P2PEオンサイト評価を実施します。
オンサイト評価	PCI 3DS オンサイト評価	非対面取引におけるクレジットカードの不正利用対策として、3Dセキュアへの注目が高まっています。3Dセキュアを提供する企業様向けに、PCI 3DSオンサイト評価を実施します。

PCI準拠支援ソリューション/PCI準拠維持支援

PCI準拠支援ソリューション　PCI DSS準拠の負担を軽減できるサービスを提供

BBSecでは、PCI DSS準拠と、その後の準拠維持にかかる工数を削減したい、という企業様の声を受け、運用負担を軽減させる独自のソリューションを開発・提供しています。運用担当者様の業務負担を大幅に削減するとともに、手動で実施すると発生する可能性がある記録の見落としやチェック漏れを防止して、正確な確認作業を自動化することを可能とします。

サービス一覧

日々ログ	PCI DSS準拠組織へのセキュリティ運用支援サービス。 ログ解析で、継続的なPCI DSS準拠を強力にサポートします。
クレジットカード情報 非保持化コンサルティング	業務ヒアリングならびにネットワーク図 / PANの伝送状況 / 非保持化ソリューションの確認を行い、非保持化におけるセキュリティ向上を支援いたします。

PCI準拠維持支援　QSA有資格者がお客様のPCI DSS / PCI P2PE / PCI 3DS準拠維持をサポート

PCI DSS、PCI P2PE、PCI 3DSに準拠していることが一度確認できても、日々の業務やシステムの改修、運用変更、業務変更などが変化していく中で準拠を維持することは簡単ではありません。また、毎年1 回の監査も必要です。準拠維持支援では、準拠状況を適切に維持できているかどうかを確認し、問題点があれば早期発見、解決に役立てるためにご質問対応、最新情報を提供します。

準拠維持のための活動

準拠状況を維持するためには、回数や期間が定められた様々な要件に対応することが必要です。維持支援のフェーズでは以下のような年間スケジュールを利用し、日々の業務の中に準拠維持対応を組み込むことを目指します。

要件	実施内容	具体的数値基準	●●●●年 1 2 3 4 5 6 7 8 9 10 11 12
1.2.7	ネットワークセキュリティコントロールの設定レビュ	6 カ月に1回以上	予定 実績
3.2.1	保存されたアカウントデータに関するレビュ	3か月に1回以上	予定 実績
12.4.2	セキュリティポリシーと運用手順のレビュー	少なくとも四半期に1回	予定 実績
12.10.4	セキュリティインシデント対応の責任者教育	1年に1回以上	予定 実績
12.10.6	事故(インシデント)対応計画の見直し	1年に1回以上	予定 実績

サービスの特長

定期的なフォローアップ監査

面談や記録書類の確認を通して、PCI DSS準拠を維持するために必要な定期的な実施項目の確認を行ないます。
・業務変更に伴うデータフロー図の変更　・変更管理記録　・アカウント管理記録
・教育実施記録　・各種システムのログ　など

質疑応答

準拠維持をしていく中で発生した疑問や質問事項に対し、当社QSAが助言いたします。

情報提供

規格や関連する法律の改定や業界動向の最新動向を情報提供します。

サービス一覧

PCI準拠維持支援 コンサルティング	定期的な証跡確認やご質問対応を通じて、PCI DSS、PCI P2PE、PCI 3DS準拠の維持を支援いたします。組織体制やネットワークの変化に伴うご相談もお受けします。
SAQ準拠維持支援 コンサルティング	自己問診票(SAQ)で準拠した場合でも、オンサイト評価と同様に年1 回の更新が必要です。コンサルタントの目で最新の証跡を確認しながら、SAQ作成をサポートいたします。
PCIウォークスルー	短期間で全要件の簡易的なインタビューを行い、現状確認と対策説明を実施します。日々の運用は自力で行っているが、更新前のチェックをしたいという企業様にお勧めです。

PCI DSSセキュリティセカンドオピニオン

PCI DSS準拠済企業様のセキュリティを再確認すると共に、v4.0 要件12.5.2で要求される PCI DSS適用範囲レビューの要求を満たす第三者レポートを提供

PCI DSS環境　本当に安全ですか？

社会的に最も影響が大きいセキュリティ上の脅威であるクレジットカードの不正利用は世界中で後を絶ちません。憂慮すべきは、クレジットカード情報を守るためにPCI DSSに準拠していても情報漏えい事故が発生してしまうケースがあることです。PCI DSS準拠活動を正しく、適切に行っていれば起きるはずのない事故（セキュリティインシデント）が、昨今発生しております。なぜ、PCI DSSに準拠したはずなのにこうしたインシデントが発生するのでしょうか。

各要件の安全な設定　やっているつもりで見落としていませんか？

●もし、準拠範囲設定（スコープ設定）が適正でないと…

PCI DSSに準拠していない環境からPCI DSS準拠環境に意図しないアクセス経路が存在すると、非準拠環境への侵入がきっかけで漏えい事故が発生する可能性があります。

●もし、許可すべき通信が適切でないと…

「業務に必要な通信」の範囲を大きくとらえて、不要な通信（ポートやノード）が許可されている場合、不正なアクセスを検知できない可能性があります。

●もし、ファイル改ざん検知に設定漏れがあると…

ファイル改ざんや不正ファイルの設置について、正しく検知条件設定が施されていないと、
不正操作の発見ができない場合があります。

●もし、ログレビュー方法が不適切だと…

異常と判断する条件設定が適切でない場合、不正操作の発見ができない場合があります。

サービスの特長

PCI SSC 認定審査機関（Qualified Security Assessors）によるセキュリティ確認

国内外の様々な企業の審査やコンサルを実施してきた10年以上の実績に基づくセキュリティチェックを行います。

セキュリティ再確認による情報漏えい事故と経営リスクの低下

準拠済であっても改めて確認するべきポイントを「セカンドオピニオン」的に再確認できるため、不安を解消できます。

安価/スピーディーにセキュリティのウィークポイントのチェックが可能

情報漏えい事故が起きる要因となる箇所に対してピンポイントでのチェックを行います。

v4.0 要件12.5.2で要求されるPCI DSS適用範囲レビューの要求を満たす第三者レポート

評価会社以外の目線で適用範囲を確認したレポートであるため、要件12.5.2を満たす証跡として有用です。

サービス内容

①スコープの再確認

ネットワーク運用において、評価範囲（スコープ）が適正に設定されているか？ 本来接続すべきではない接続先とのインターフェースが存在しないか？ を第三者目線で再確認します。

②業務ヒアリング

カード情報が使用される実務部門の実体をヒアリングします。
文書化されていないPANデータフロー等が存在しないか、CHDデータマトリクスを使用し確認します。

③セキュリティ設定の再確認

PCI DSS準拠当初に実施された各要件を満たすセキュリティ設定やシステム堅牢化設定は今も正しく構成されているのか？長期間の運用におけるヌケ・モレ・見落としが生じていないか？ これらを資格ある評価人が改めてセキュリティにおける「セカンドオピニオン」として再確認します。

・ネットワーク機器（ファイアウォール、ルータ、IDS/IPSなど）
・セキュリティ上重要な役割を持つサーバ類（改ざん検知機構、ログ保全機構など）
・Excelベースのチェックシートによる確認結果ご報告を行います。

PCI-CPSA/PCI PIN Assessment

PCI-CPSA

PCI-CPSA (Payment Card Industry Card Production Security Assessors)はPCI SSCおよび国際カードブランドが制定したPCIカード生産及びプロビジョニングに対する物理、論理セキュリティが定義された国際標準です。

認証評価の区別

■物理セキュリティ

職員管理、資材管理、製造手続き及び監査追跡、パーソナライズされる前のカード情報の保護および処理を規定

■論理セキュリティ

職員の役割及び責任/セキュリティポリシー及び手順、データ/ネットワーク/システムセキュリティ/ユーザー管理およびシステムアクセス制御/暗号キー管理を規定

ペイメントカードの製作及びプロビジョニングに関連するサービス提供者は、PCI-SSCから認定を受けたCPSA認証企業による評価が毎年求められます。

サービスの特長

BBSecはPCI SSCから認証を受けたCPSA企業として、お客様のCPSA認証維持のための認証評価、コンサルティングとソリューションサービスを提供します。

総合的なセキュリティコンサルティングの提供

高度なセキュリティ技術とノウハウを備えたCPSAがCard Production評価を行うにあたり、コンサルティングからソリューションまでノンストップで包括的サービスを提供します。

グローバル対応力

日本/韓国/タイに拠点・スタッフを有しマルチ言語に対応可能です。海外拠点の認証評価が必要な時、BBsecの優れた現地対応支援を提供します。

PCI PIN Assessment

PCI PIN評価は、ペイメントカードを扱う組織がオンライン及びオフライン支払カード取引中にPINデータを安全に管理、処理、転送しているかの評価を実施します。PINの取引を処理する組織はPCI PINプログラムの準拠が必要です。

サービスの特長

BBsecはPCISSCから認証を受けたQPA企業として、お客様のQPA認証評価、コンサルティングとソリューションサービスを提供します。

総合的なセキュリティコンサルティングの提供

幅広い業力を持った専門QSAの経験をもとに、高度セキュリティ監査技術とノウハウを備えた専門QPAがPin Security認証評価を行います。

グローバル対応力

日本/韓国/タイ/英語のマルチ言語に対応し海外拠点の認証評価が必要な時、BBsecの優れた現地対応支援を提供します。

PIN評価のプロセス

Phase 1 GAP分析
- コンサルティング
- 事前監査

Phase 2 PIN評価
- 現場評価
- データフロー、暗号鍵管理プロセス、ソリューションの確認
- 修正事項の案内

Phase 3 PIN評価プロセス完了
- QPAによる最終報告書提出

対象企業は2年ごとに認証評価を行う必要があります。

PCI DSS Ver4.0.1 SAQ(D-SP) 記入例サンプル提供サービス

SAQ記入例を元に新書式への対応を最短支援

イシュア、サービスプロバイダの皆様 Ver4.0.1 SAQ D-SPの書式変更は既に対処済みでしょうか?

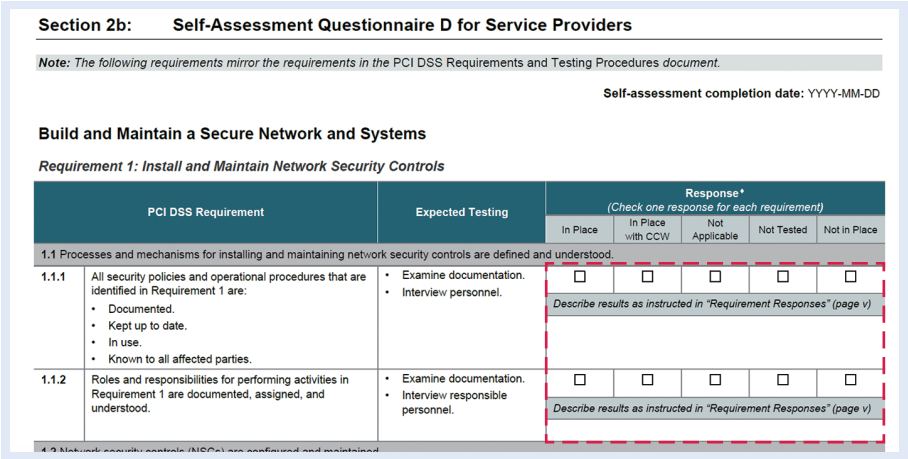
2024年4月以降は新書式でのSAQ提出が必須です

全要件へ記述(作文)が必要

従来はチェック式の記述のみでしたが、Ver4.0からは約250もある要件すべてに対して結果を選択した説明を記述することが必要となりました。
In Placeを選択する場合、根拠の説明と裏付けとなる証跡について記述が必要です。

ネットワーク図やカード会員データー覧が必須

従来は問診に答える形式でしたが、図の挿入や表の作成が要求されるように変更されています。ネットワーク図、カード会員データ/機密認証データー覧、システムコンポーネント一覧の作成が必須となりました。



Section 2b: Self-Assessment Questionnaire D for Service Providers

Note: The following requirements mirror the requirements in the PCI DSS Requirements and Testing Procedures *document.*

Self-assessment completion date: YYYY-MM-DD

Build and Maintain a Secure Network and Systems

Requirement 1: Install and Maintain Network Security Controls

PCI DSS Requirement		Expected Testing	Response* (Check one response for each requirement)				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
1.1 Processes and mechanisms for installing and maintaining network security controls are defined and understood.							
1.1.1	All security policies and operational procedures that are identified in Requirement 1 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	• Examine documentation. • Interview personnel.	☐	☐	☐	☐	☐
			Describe results as instructed in "Requirement Responses" (page v)				
1.1.2	Roles and responsibilities for performing activities in Requirement 1 are documented, assigned, and understood.	• Examine documentation. • Interview responsible personnel.	☐	☐	☐	☐	☐
			Describe results as instructed in "Requirement Responses" (page v)				

サービスの特長

■SAQ記入例を元に新書式への対応を最短支援いたします

・SAQ完成に必要な支援のみにフォーカスするため、短時間かつ低コストで提供可能です。
・サンプルファイルがあるため、短時間でも効果的にレクチャが可能です。

準拠済端末(カード会社の端末)の利用中心のイシュア様を想定した環境での記載例サンプルや自社内にサーバ類を多くお持ちの環境向けサンプルなど、実践的な記載文面を多く含むサンプルをご提供予定です。

サービス内容

サービス	内容
SAQ(D-SP)サンプルファイルご提供	認定評価人(QSA)監修のもと、SAQ(D-SP)全要件に対し汎用的に活用できる記入例を用意しております。 モデルケースを設定し、要件をどのように満たすか? を簡潔に記述しているため、自社向けの記述を最短で書き進めることが可能です。 また、どのような証跡を記載すれば良いか?も例示されているため、スムーズに準備できます。
コンサルタントによる記述方法のレクチャ	ご希望に応じ、訪問またはリモートにてSAQ作成に向けたレクチャを実施します。 サンプルを元に記述に必要な考え方を解説します。 自社環境向けに記述が必要なポイ ントがクリアになります。

サイト評価・設計コンサルティング

UI/UX面での課題点の抽出、改善方向性の策定、リニューアルアドバイス

様々な業種に多数実績あり。業界を把握したWebサイトの充実・改善について提案します。
「ユーザーの動向分析」「業界の動向分析」「今後の方向性の適切な提案」をバランスよく実施できることがBBSecの強みです。
金融・旅行・不動産・IR・ECサイトの分析・構築など数多くの業界へコンサルティングサービスを提供します。

サービス一覧

項目	
サイト/アプリ評価レポート	ユーザーにいかに目標を達成してもらうかについて、Webサイトの全体構造に対する7つのUX要素で検証していきます。これにより網羅的な分析と改善施策の抽出が可能となります。(UXハニカム構造。Peter Morville提唱)。当社はインターネット創成期からコンサルティングサービスを行なってきました。その20年以上のノウハウは、2000項目以上のサイト評価基準に結集されています。
オンラインUXテスト (リモート型ユーザビリティテスト)	従来型のユーザビリティテストは、期間・コストの面から多くのモニターによる調査が困難でした。弊社では、ユーザビリティテストと同じくユーザー操作に焦点をあてた調査でありな がら、Webアンケート調査と同じく、まとまった規模のサンプル数(300～1,000名規模)を確保できます。
アクセス解析・ KPI(主要業績評価指標)策定	KPI策定サービスでは、御社のビジネスゴールのすりあわせをした後で、想定されるユーザーセグメントごとのサイト内遷移状況を整理します。その上で、今後継続的に把握していくべきKPI(主要業績評価指標)を策定します。
サイト運営時/リニューアル時における常時アドバイス	自社のWebサイトを運営や、リニューアルプロジェクトを進めるにあたっては、知識・経験、社内体制、業界動向などを含め、多くの要因により悩みが尽きません。常に最新の業界動向を調査している実態をもとに、御社のWebサイト運営への継続的なアドバイスを申し上げます。

Webサイトランキング情報

30業界・4,600サイトをゴメスの客観的基準で評価し、ランキング発表を行っています。利用者の視点を中心に各業界に特化した評価基準を策定しています。

Webサイトランキング情報

●ウェブサイトの使いやすさ　●企業・経営情報の充実度　●財務・決算情報の充実度　●情報開示の積極性・先進性

上場企業が株主・投資家向け広報活動を行うためのウェブサイトの使いやすさや情報の充実度を評価することを目的として2005年から毎年公表しています。

金融・マネー	不動産	旅行・交通	その他
オンラインバンク(19行) オンライン証券(15社) 地方銀行(105行) 投信運用会社(69社) M&Aプラットフォーム(6サイト) ソーシャルレンディング(5社) iDeCoサイト(15社) 少額短期保険(15社) 自動車保険(6社)	賃貸不動産アプリ(8社) 売買不動産アプリ(5社) 賃貸不動産スマホサイト(11社) 売買不動産スマホサイト(7社) 投資用不動産(8社) 賃貸不動産(12社) 売買不動産(7社)	国内宿泊予約(12社) 海外ツアー旅行(15社) 国内ツアー旅行(16社) 海外航空券(19社) 国内航空券(9社) ホテルチェーンサイト(19社)	転職情報(10社) アルバイト情報(10社) 人材派遣(12社) ネットスーパー(7社) 中古車情報(19社) 大学サイト(457校) 自治体サイト(50自治体)

Webシステム開発

UI/UXと管理効率化を両立させたWebシステムの開発

ユーザー視点で考えた、お客様に寄り添った提案をします。WebシステムおよびWebサイトの戦略立案・設計・デザイン・システム開発・保守・運用まで、豊富な実績とノウハウを活用し効果的なWebサイトを実現します。

サービスの特長

設計
ユーザー要件の整理・定義を行い、お客様が現在抱えている課題点・懸念点を明らかにします。その後、整理した要件より導き出されるシステム機能、パフォーマンス要件等を設計します。

Webシステム開発・構築
お客様が抱えている課題をヒアリングし、課題解決のみではなく、業務の改善も含めたシステムの開発・構築を行います。

CMS導入
CMSの導入により全ページの更新が可能になります。初期構築、操作サポートも行います。

Webマーケティング
売買成約まであらゆる数値を可視化し、お客様のニーズに沿ったターゲット選定、企画等を提案します。

ECサイト構築
規模・ご要望に合わせたご提案を行います。サイト分析・構築のノウハウを活かし、お客様の視点で使いやすいUIでの構築を行います。

運用
公開後のサイト更新、ログ解析により効果計測をいたします。それに伴う改善策の立案・実施などを行います。

サービスの強み

弊社では過去20年以上に渡るサイト分析・構築ノウハウをもとに、お客様の成功のための課題の洗い出しから具体的なデザイン・HTML制作まで総合的に進めてまいります。

現状分析	・問題意識のヒアリング、アクセス解析状況の確認　・競合他社の状況分析　・御社内体制および業務フローの確認
コンセプト策定・サイト設計	・サイトリニューアルの目的の整理　・ユーザーセグメントおよび訴求コンテンツの整理　・サイトマップ作成、ユーザーフロー作成、KPI策定
基本デザイン設計	・トップページデザイン作成　・テンプレートデザイン作成
プロトタイプユーザビリティテスト	・サンプルデザインに対するユーザーテスト
HTML制作	・主要ページレイアウト、デザイン設計　・その他ページレイアウト　・デザイン設計　・主要ページ、その他ページHTML制作
CMS導入・システム対応	・CMS適用、システム対応等
業務フローアドバイス	・各種ガイドライン整備、運営体制アドバイス

マーケティング・データベース

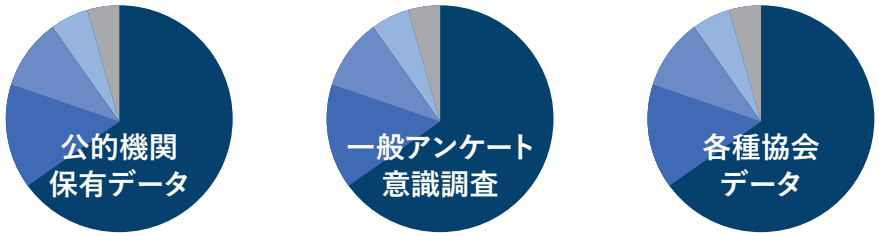
ユーザーの行動・意識に特化したデータを提供

企業情報や財務情報ではなく、ユーザーや消費者の購買行動、サービス利用時の重視点など、人の行動や意識に特化したデータを提供いたします。行動や意識に特化したデータを収集・分析することで、経営戦略、事業計画、営業計画、マーケティング計画を策定する際の顧客分析・市場分析を、調査や加工といった工数をかけずに行うことができます。また、データは統計学・経済学に基づきスコアリングすることで信頼性が客観的に評価されたデータを取捨選択することができます。

サービスの特長

ユーザーの行動や意識に特化したデータを格納

公的機関の発表する統計情報等の公開データの他、一般のアンケート調査や意識調査といったユーザーの行動や意識に特化したデータを格納しています。



加工せずに使用できる統計・リサーチデータ

PDF・テキストデータ・CSVデータなどの形式が不揃いの統計データ・リサーチデータをメタデータ化、EXCEL形式・PPT形式に変換しご提供いたします。

データスコアによるデータの”格付け”

統計学に基づいた評価ロジックを、慶應義塾大学 沖本竜義教授監修のもと構築。データを客観的に評価・格付けいたします。

データリクエストで探索・更新を代行

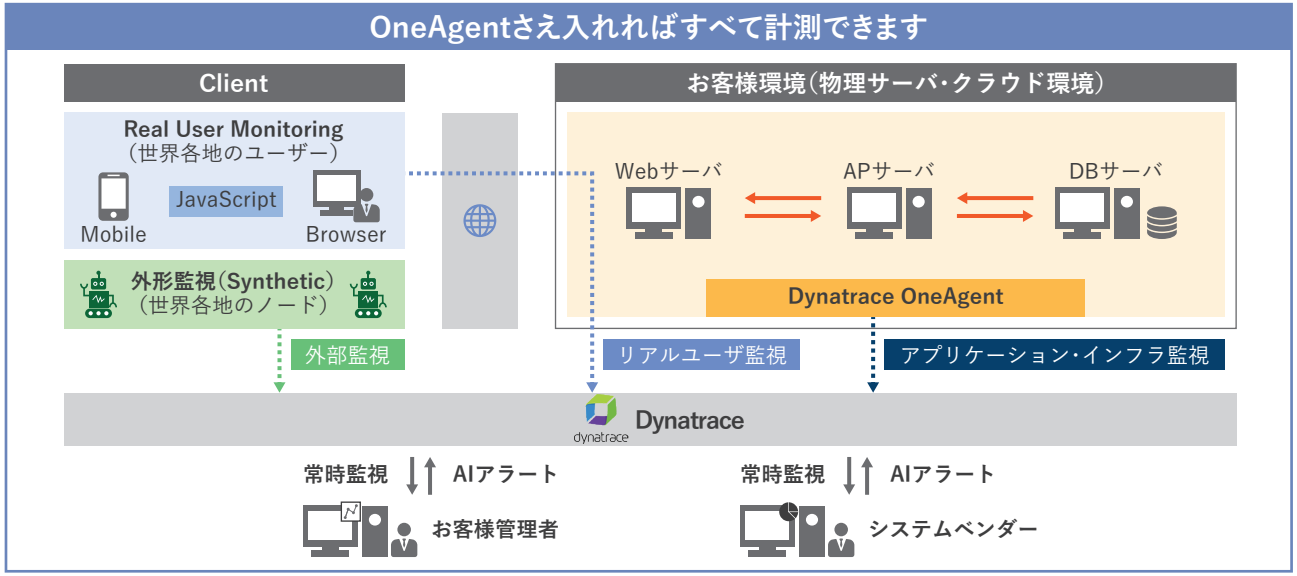
ご指定のフォーマットに沿ってWEB上のデータを探索・収集・加工いたします。また、定期的にデータの更新も代行いたします。

パフォーマンス監視・改善

フルスタックデジタルパフォーマンス監視・分析・改善

Dynatraceによるパフォーマンスマネジメントを通してビジネス課題を解決します。自社のITシステムやクラウド環境の監視だけでなく、アプリケーション監視とリアルユーザー体験の解析を統合。ビジネスへのインパクトを把握し経営課題の解決をサポートします。独自技術による自動化とAI学習により、IT運用の効率化が可能となります。

サービス構成図



サービスの特長

自動監視による障害対応時間の短縮

予兆検知から原因特定まで完全自動監視します。調査分析や会議の時間を大幅に削減できます。

サービスのコードレベル分析

全トランザクションを自動キャプチャします。問題の根本原因をコードレベルで特定します。

ユーザ体験のリアルタイム分析

特定の問題やパフォーマンスによるユーザ影響を一元的に可視化でき、DevOpsの推進に貢献します。

AIによるアラート洪水の防止

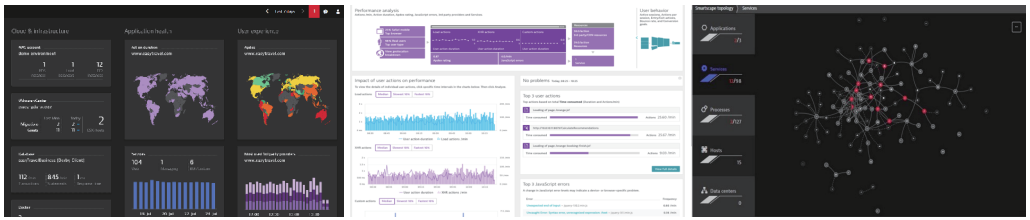
根本原因を特定するアラートのみの通知により、運用の効率化が図れます。

問題の影響範囲やシステム構成を可視化

OneAgentをインストールするだけで、アプリケーションスタックを自動マップ化します。

パフォーマンス改善コンサルティング

実績あるコンサルタントがUI/UX観点・SEO観点も踏まえ、パフォーマンス改善をサポートします。



脆弱性診断

脆弱性診断：概要

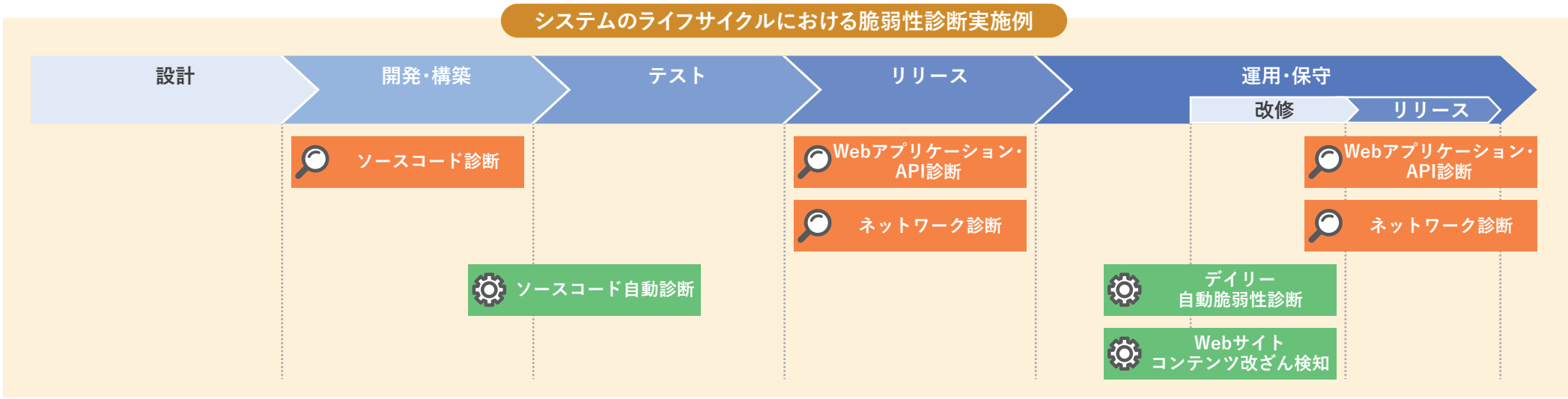
| SQAT®：Software Quality Analysis Team
| Cracker Probing-Eyes® | クラウドセキュリティ

悪意ある攻撃を受ける前に、自らリスクを発見して防御することで、事業継続性を高める

今や企業の情報公開にとどまらず、オンライントレードやネットショッピングなど、Webシステムの活用は事業活動に必要不可欠な存在となっております。その一方で、企業のネットサイトは、悪意ある攻撃者による情報システムへの侵入経路として危険にさらされています。
システムに存在する脆弱性は、時として深刻な被害にもつながる看過できない脅威であり、脆弱性対策は事業継続性における必須の課題です。その第一歩は、脆弱性の存在を検知し、内包するリスクを適切に把握するところから始まります。脆弱性診断により、悪意ある攻撃を受ける前に、自らリスクを発見し、防御するための問題特定ができます。

システムのライフサイクルにおけるあらゆるフェーズとあらゆる対象範囲に脆弱性診断を

脆弱性診断は、一度実施すればよいというものでも、特定の対象のみに対して実施すれば十分というものでもありません。システムのライフサイクルに応じて、できるだけ適切なタイミング、適切な対象範囲への実施を検討してください。BBSecの脆弱性診断は、時々刻々と変化する環境に対応するため、システムの各フェーズにおいて多様な対象範囲にご利用いただくことで、お客様システムの健全化に貢献します。



サービスの特長

高精度な脆弱性診断

専門技術者がチームを組み脆弱性診断を実施。セキュリティ情報の常時リサーチに基づく診断パターンの更新により、診断品質の維持と向上を図っています。

様々な業界からの診断依頼に対応

偏ることなく、幅広い業種から脆弱性診断のご依頼を受けています。

継続利用によるメリット

定期的な脆弱性診断は、新たな脆弱性の発見、最新の攻撃手法に対するシステムの耐久力把握、診断結果を活用したリスク管理などに有効です。

コーポレートガバナンスに貢献

第三者による脆弱性診断は、事業継続性に対するコーポレートガバナンスとしても活用されています。

脆弱性診断

SQAT®:Software Quality Analysis Team

自動診断と手動診断を組合せ、高精度の脆弱性診断を提供

BBSecの脆弱性診断は、独自開発を含む複数のツールを使用した自動診断と、経験豊富なセキュリティエンジニアによる精度の高い手動診断を組み合わせることで、高レベルの診断結果を導き出します。

サイバー保険付帯

費用の問題から十分な初動対応ができないといった問題が発生しかねない状況を憂え、BBSecから提供する脆弱性診断サービス「SQAT® 脆弱性診断」のすべてに、サイバー保険を付帯しました。

詳細は上記または次頁

診断の流れ

診断範囲確定後、ツール診断と手動診断を行います。ツール診断で発生する誤検知や過検知、検知の見落としを人的な診断によりフォローし、正確な実態の把握を可能にします。さらに、検出された脆弱性にどのように対処すべきかを報告書・報告会でご説明いたします。診断後、脆弱性への対応状況を確認する再診断も提供しています。

チームによる診断・分析・保守　～ 診断者による偏りを排除し、継続的かつ一貫性のあるサービス品質を提供します ～

調査 ▶ 診断範囲確定 ▶ ツール診断 ▶ エンジニア診断 ▶ 分析 ▶ 報告書作成 ▶ 報告会 ▶ 再診断 ▶ 診断保守 ▶ 定期診断

診断保守 … 通常、半年または一年間隔 …

診断を業務ごとに組織化し、徹底的に個人能力依存を排除することで、品質のバラツキ防止とキャパシティ拡大を同時に実現し、納期／費用などの顧客満足度向上を実現。

高品質を提供するポイント

■診断項目の網羅性

・複数のツール診断と手動診断を組み合わせて高レベルの診断結果を導き出します。
・ツール診断より実態に即した診断結果のご提供が可能です。

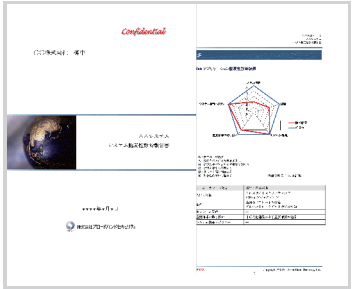
ツール診断結果	緊急	重大	高	中	低	情報		
手動診断結果	緊急	重大	高	中	低	情報		

検出された全てのポイントを検証 → 誤検知・過検知を取り除き、実態を把握

最終診断結果 重大

■お客様のニーズに合わせて作成される報告書

診断結果の報告書は、検出された脆弱性や問題箇所一覧、当社セキュリティエンジニアによる分析、再現手順、推奨対策を備えたレポートとなります。重大な問題発見時には、報告書に先立ち、速報もお送りしています。またお客様のニーズに合わせて、経営層向けのエグゼクティブサマリの作成も承っております。



■BBSec ポータルによるシームレスな情報共有

BBSecポータルをご利用いただくことで、スケジュール・進捗状況の確認や依頼・お問い合わせのステータス管理など、コミュニケーションを円滑に図ることが可能です。
回答遅延が発生しないよう、専用のサポートデスクが対応いたします。

■国際的基準を反映した脆弱性評価

CVSS（Common Vulnerability Scoring System）、PCI DSS、OWASP Top10、CAPEC、NIST、CWE 等、国際的な脆弱性評価基準をもとに作成された当社独自基準をもとに、発見された脆弱性のランク付けを行っております。
診断によって検出された問題箇所は一つ一つ誤検知・過検知を取り除くとともに、対象システムの特性や出現条件の難易度等によりリスク評価を行います。

■充実の再診断サービス

診断結果の報告書納品後、お客様にて修正いただいた箇所の再診断を無償で実施いたします。
再診断をご利用いただける期間は、報告書納品日より3か月と、一般的な業界標準より余裕のある期間を設けております。

脆弱性診断　SQAT®:Software Quality Analysis Team

脆弱性診断サービスにサイバー保険を付帯

サイバー攻撃の手法は日々更新されており、さらに取引先や子会社などを含むサプライチェーンを踏み台にした攻撃など、どんなにセキュリティ対策を実施していても自組織のみではインシデント発生を防ぎきれないのが現状です。
また、インシデント対応には多額の費用が掛かります。費用の問題から十分な初動対応ができないといった問題が発生しかねない状況を憂え、BBSecから提供する脆弱性診断サービス「SQAT® 脆弱性診断」のすべてに、サイバー保険を付帯しました。

サービス概要

BBSecによる脆弱性診断の契約日から1年間、情報漏えいやサイバー攻撃に起因する賠償損害や、事故発生時に対策を講じた場合の費用損害について、実際の初動対応には平均して1,000万円程度必要であるという当社データをもとに、**最大1,000万円まで補償**されるプランを付帯いたしました。

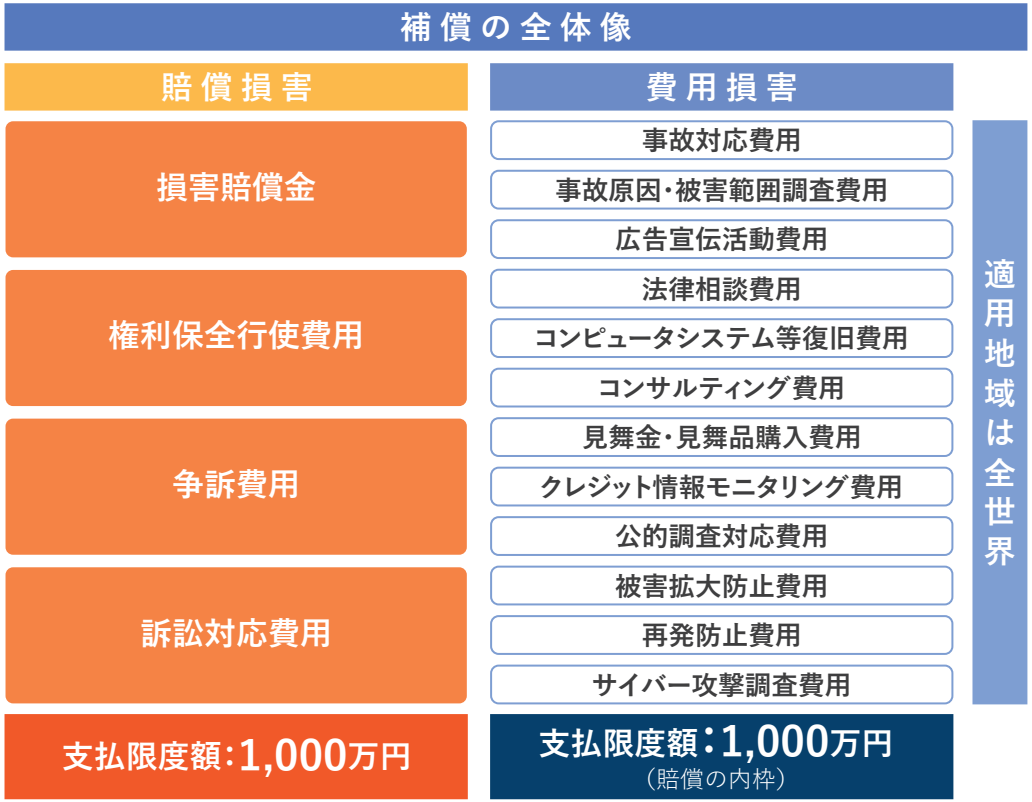
サイバー保険付帯の対象となる脆弱性診断

BBSecのSQAT® セキュリティ診断サービスすべてが対象となります。
また、複数回脆弱性診断を実施した場合、最新のご発注日から1年間有効となります。

- **■WEBアプリケーション・API脆弱性診断**
- **■ネットワーク脆弱性診断**
- **■スマホアプリ脆弱性診断**
- **■IoTセキュリティ診断**
- **■アタックサーフェス調査**
- **■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**
- **■ソースコード診断**

さらにBBSecはクレジットカード情報漏えい事故調査機関（PFI）であることから、万が一、クレジットカードの情報漏えいが発生した場合でもご相談可能です。

サイバー保険付帯の対象となる脆弱性診断



脆弱性診断

SQAT®:Software Quality Analysis Team

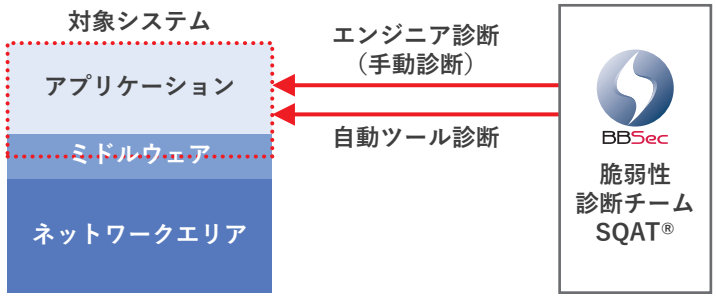
サービス一覧

■Webアプリケーション・API脆弱性診断

サイバー保険付帯

SQAT® for Web

Webアプリケーション・APIを攻撃するハッカーの手法を用いて、外部から動的に脆弱性を診断することで、攻撃の入口となる可能性のある箇所を検出します。診断は最新のセキュリティ情報 に基づき実施されますので、開発時の脆弱性初期診断だけでなく、定期的な実施など 既存システムの脆弱性対策の確認にも活用することをおすすめしています。

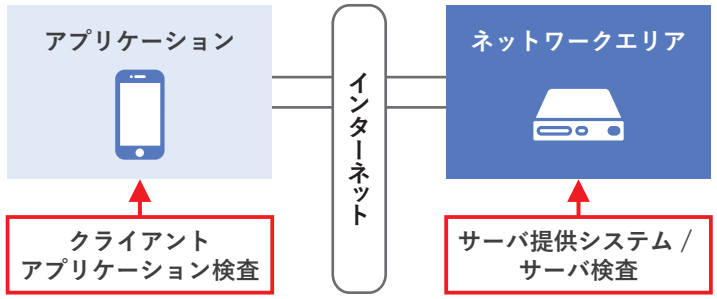


■スマホアプリ脆弱性診断

サイバー保険付帯

SQAT® for Smartphone

スマートフォンアプリケーションの脆弱性が問われる中、サーバ検査・クライアントアプリケーション検査を通じ、利用者情報が適切に取り扱われているかを診断するサービスです。本診断は、総務省が提言する「関係事業者向け スマートフォン利用者情報取扱指針」で示された基本原則を考慮した診断です。

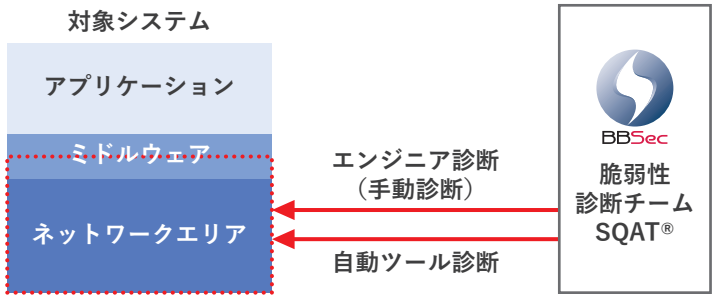


■ネットワーク脆弱性診断

サイバー保険付帯

SQAT® for Network

システム全体に影響を及ぼすネットワークを外部より、またはオンサイトにて動的診断いたします。ネットワークへの侵入はシステム構成により企業全体へと影響を及ぼす可能性があり、脆弱性に対する対策は極めて重要です。ファイアウォール等のセキュリティ機器の診断を行うことにより、機器自体の問題やセキュリティパッチ適用漏れを見つけることができます。



■IoTセキュリティ診断

サイバー保険付帯

SQAT® IoT

対象のデバイス固有の機能（各種プロトコル・インタフェース接続）を利用し、攻撃者にとって有益となる「不正操作」「情報の窃取」「踏み台化」が可能であるかを診断します。また、利用されているOS/ミドルウェアの既知の脆弱性の有無も確認します。

診断メニュー	
静的ソースコード解析	ファームウェア解析・バイナリ解析
ネットワークスキャン	ファジング
ハードウェア解析	ネットワークキャプチャ（通信内容解析）

■アタックサーフェス調査

サイバー保険付帯

SQAT® ASM

Webシステムやネットワーク機器などの外部との接点にある「サイバー攻撃の対象となりうるIT資産」が、攻撃者の視点からどのように見えているかをOSINT技術を活用して脅威となり得る情報を収集します。幅広く貴組織で未把握の脅威を確認するのに有効です。

脆弱性診断　SQAT®:Software Quality Analysis Team

■ペネトレーションテスト

サイバー保険付帯

SQAT® ペネトレーションテスト

事前の綿密な調査により特定した「システム内でより弱い（脆弱な）個所」を起点にシナリオベースの疑似攻撃を仕掛け、システムの堅牢性を確認する検査です。実際の攻撃を体験することで、効果的な防御方法（システム・運用方法）の構築が可能となり、万一攻撃者にシステムへ侵入された場合の被害を最小化できます。

	脆弱性診断	ペネトレーションテスト
対象	ネットワークやインフラ、Webアプリケーション	ネットワークやインフラ、Webアプリケーションに加え、物理侵入テストを含む場合あり
目的	脆弱性を検知・検出・侵害により発生するリスクの特定・分析	不正アクセス、侵害行為が成立するかどうかの確認
範囲	広く網羅的に診断	侵入する、侵害行為が成立するためのポイントを探すことが目的となるため、必ずしも範囲は広くない
期間	対象範囲及び仕様により決まるが、ペネトレーションテストよりは短期間	脆弱性診断よりも長い期間を要する場合もある

■クラウドセキュリティ設定診断

サイバー保険付帯

クラウドサービスの利用が浸透する中、それぞれのサービス事業者が独自基準を設けているがために、各種設定状況を同一基準で評価できないという課題が発生しています。本サービスは、主要クラウドが推奨する環境への適合性診断に加え、マルチクラウド環境に求められる異なる推奨環境を画一的な視点でチェックする設定診断を同時に行います。

	ベンチマーク対応領域			本診断対応領域		
	AWS	Azure	GCP	AWS	Azure	GCP
アカウント管理	●	●	●	●	●	●
ロギング	●	●	▲	●	●	●
ネットワーク	●	▲	●	●	●	●
ストレージ	▲	●	▲	●	●	●
データベース	▲	▲	▲	●	●	●

※対応領域は一例になります。詳しくはお問い合わせください。

■ソースコード診断

サイバー保険付帯

SQAT ®Core

独自開発ソフトウェアのソースコードを静的に分析し、セキュアなコーディングルールとデータフローをチェックし、隠された脆弱性とコーディング品質を検証し、結果をお伝えすると共に回避の為の改善案も提示します。

対象開発言語			
C/C++	Java	C#	VB.NET
JavaScript	ASP	VBScript	VB6
PHP	Android	Objective-C	Ruby
Python	Perl	PL/SQL	TypeScript
Go(Golang)	Groovy	Kotlin 他	

脆弱性診断保守　Cracker Probing-Eyes®

日々増殖する脅威にタイムリーに対応し、リスクを最短で回避するお手伝い

定期的な脆弱性診断により、その時点でのリスクを最小化することは極めて重要ですが、次の脆弱性診断までの間に発生する外的変化にできるだけ早く気づき、いち早く対応することも忘れてはなりません。
BBSecでは、インターネット越しに高頻度で気軽に実施可能な自動診断ツールを脆弱性診断保守向けに提供しております。Webアプリケーション、ネットワーク、ソースコードに対する簡易診断ツール、Webサイトの改ざんをチェックするツールにより、お客様のリスク軽減を支援しています。

サービスの特長

最新のセキュリティ情報に基づく脆弱性診断

世界的なセキュリティ基準をベースにBBSecの独自基準を設けることで、信頼性の高い最新のセキュリティ情報をもとにした脆弱性診断を行っています。

わかりやすいレポート機能

自動脆弱性診断では、発見された脆弱性を緊急度毎に色分けし、グラフで毎日報告。新しい攻撃パターンが発見された時の影響や対策実施後の効果などが一目でわかります。コンテンツ改ざん検知では、検査周期毎に検査結果メールを配信します。

優れたユーザインターフェース

簡単な設定や操作は、常時使うツールに求められる隠れた重要要素です。長年の経験をもとに利用者の利便性を最大限考慮し、ツールを整備しました。

簡単ですぐに使用可能

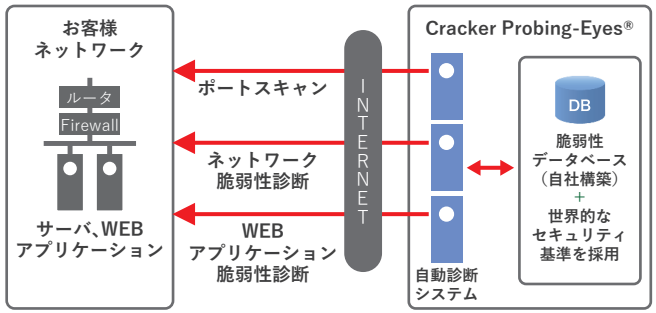
インターネット越しに指定の頻度で診断や検査を実施するだけ。お客様のシステムの設定変更や新たな設備投資は不要です。

サービス一覧

■デイリー自動脆弱性診断

Cracker Probing-Eyes®

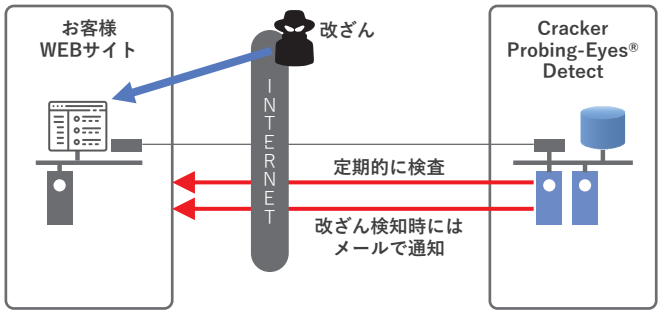
1日1回、インターネット越しにお客様サイトの脆弱性をチェックする自動診断サービスです。米国国家安全保障局(NSA)、米コンピュータセキュリティ研究所(CSI)、米連邦捜査局(FBI)、およびSANS など、世界トップクラスのセキュリティ組織により策定された規格や基準に準じた信頼性の高い診断プログラムは、お客様のシステムを健全に保つ上で、大きな効果を発揮します。



■Webサイトコンテンツ改ざん検知

Cracker Probing-Eyes® Detect

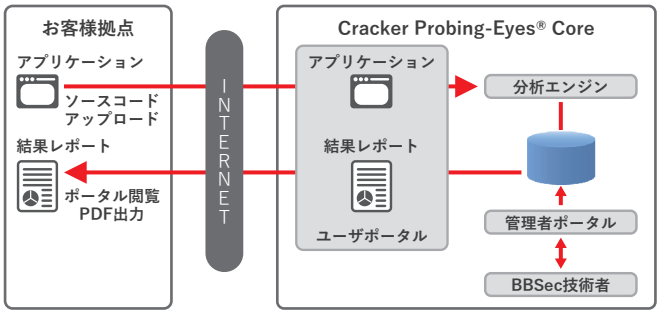
インターネットを介して、お客様のWeb サイトコンテンツの改ざん・埋め込みを診断する自動ツールです。難読化されたスクリプトを解読するプログラムを搭載しており、悪意ある通信先を高感度で判定します。インシデント発生の可能性がある場合は、すぐにメールでお知らせいたしますので、被害を最小限に留めることができます。



■ソースコード自動診断

Cracker Probing-Eyes® Core

アプリケーションのソースコードを専用のポータルにそのまま圧縮/アップロードするだけで、ソースコードの脆弱性と品質の診断を行える自動分析ツールです。お客様はあらたな設備投資不要でご利用いただけます。開発のあらゆるタイミングで品質分析が行えるため、開発の上流工程で問題への対応が可能となり、コストや労力の削減を実現できます。



BroadBand Security, Inc.

BBSecが発行するホワイトペーパー、事例紹介などをご覧いただけます。

当社のサービス／コンサルティングを活用していただいたお客様の事例や、最新のセキュリティ事情など、
お客様のお役に立つ資料をご覧いただけます。

掲載資料

- セキュリティコンサルティング事例
- ユーザ事例
- SQAT® セキュリティレポート
- SQAT® 情報セキュリティ瓦版
- コーポレートプロフィール
- その他

https://www.bbsec.co.jp/report/index.htm

情報漏えいIT対策

マネージドセキュリティ　MSS:Managed Security Service

悪意ある攻撃をフルタイムで監視、防御

IT 資産やシステムを不正アクセスや悪意ある攻撃から守る為には、日々のセキュリティ監視・運用は欠かすことはできません。当社のSOC(セキュリティオペレーションセンター)は、お客様ご担当者に代わり24時間365日体制で不正アクセス・攻撃を監視し、インシデント発生時には適切な対応を実施します。また、トラフィックモニタリングにより収集されたデータをもとに各種分析サービスもオプションとして提供しており、セキュリティの「入口・出口対策」として是非お役立てください。

サービスの特長

高い専門性(エンジニア、情報収集)
各種機関との連携/ 情報交流により、最新の情報を常に把握し、サービスに適用しています。

マルチベンダー対応
監視対象のデバイスは、メーカーに依存することなく一括管理します。

納得の信頼性
サービス仕様及び対応レベルをお客様と共に定義した上でオペレーションすることで、お客様システムを確実に脅威から守ります。

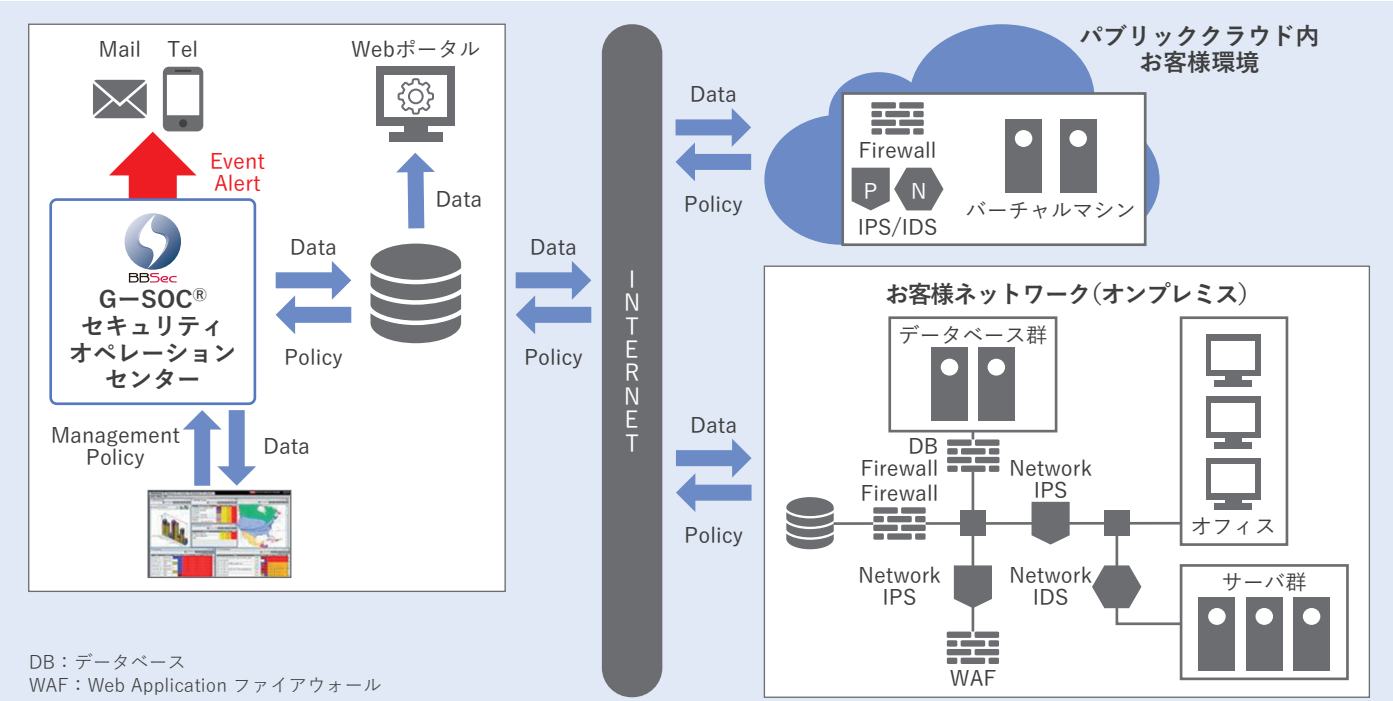
パブリッククラウド対応
パブリッククラウドサービス利用のお客様にもサービスを提供*。オンプレミスのシステムと同一の管理画面からステータスを確認ができます。
(*サービスプロバイダー様のポリシーにより利用できない場合があります。)

サービス項目

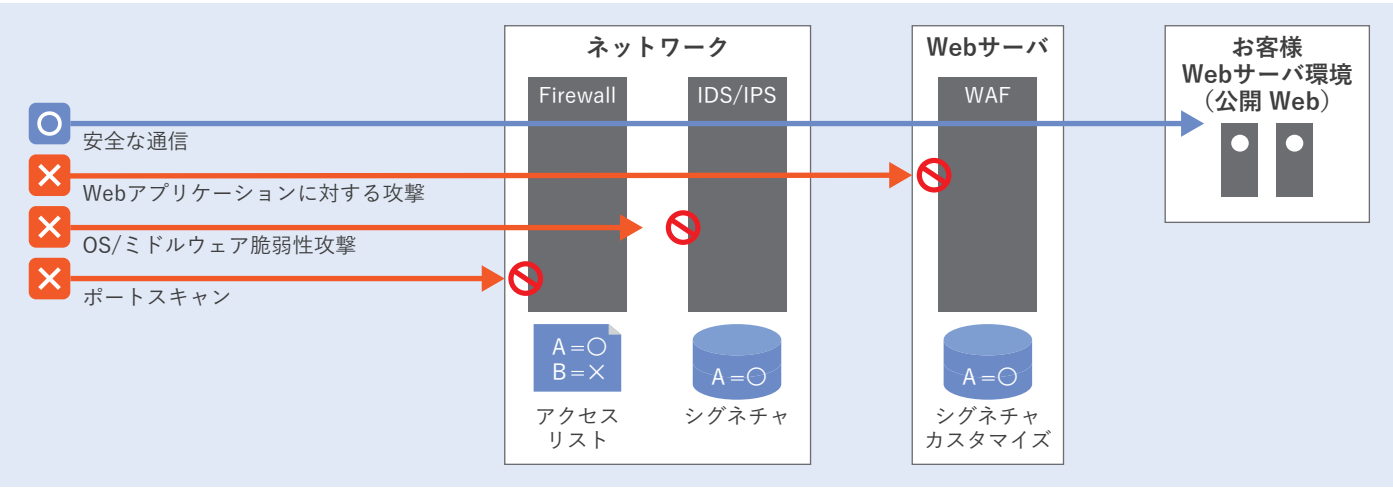
項目		
ヘルスモニタリング	・稼動及び、リソース状態の監視 ・サービス稼動状態のモニタリング（※個別対応）	・ICMP ・PORT alive check
イベントモニタリング	・セキュリティイベント収集及び分析による攻撃検知 ・複数デバイスのイベント相関関係による攻撃分析	・Attack 検知及び分析
レスポンス &テクニカルサポート	・セキュリティ攻撃に関する分析報告（リアルタイム） ・情報連携のためのポータルサイトの提供	・セキュリティ報告 ・Web ポータルサイト
ヘルプデスク(24 時間365 時間体制)	・障害／攻撃の検知時の報告 ・セキュリティ攻撃に関する問い合わせの受付及び支援	・e-mail , 電話 ・ポータルサイト
ログ管理	・セキュリティイベントログの保管（基本：3 ヶ月） ※個別対応可能（期間・提示方法）	・SIEM
レポーティング	・定期レポート ・作業、侵入事故、監視レポート	・月次レポート（統計情報）
オペレーションマネージメント	・セキュリティデバイスのポリシー設定・変更・運用代行 ・セキュリティデバイス障害時の復旧支援（切分け・ベンダー手配）	・作業／管理代行 ・障害対応

マネージドセキュリティ　MSS:Managed Security Service

サービス構成



対象



ファイアウォール、不正侵入防御システム（IDS ／ IPS）、UTM、Web アプリケーションファイアウォール（WAF）に対するMSSサービスを提供しています。

マネージドセキュリティ　Managed Security Service for AWS

クラウドサービスの特性を考慮し、攻撃の検知・対応に加え、インシデントが発生する前の予防も支援

サービスの特長

予防
主要なセキュリティベストプラクティスを用いた、設定の堅牢化を絶えず図ることにより、インシデントを予防します。

検知
貴社AWS環境における脅威を24時間365日監視し、侵害の予兆・形跡があれば即時報告します。

対応
攻撃と判断された場合、所定のポリシー・フローに沿って、対応します。

サービス提供のロードマップ

監視導入設計（セットアップ）

セットアップ
貴社AWS環境・業務及び体制にとって最適な監視体制を構築するため、初期導入準備を進めます。
・G-SOCとの接続準備　・構成などのAWS環境の確認　・連絡ポリシー・フローの策定

監視/イベント対応（運用）

チューニング
アラートをモニタリングし、お客様に最適な監視閾値の分析・検討を行います。
※クリティカルアラートの連絡は、この期間ベストエフォート対応となります。
・過検知アラートの抑止　・監視対象最小脅威レベルの策定

モニタリング
チューニングにより最適化された監視・運用体制を始動します。クリティカルな脅威があった場合、その脅威度などに応じ、しかるべき対応を実施します。
・アラートモニタリング　・過検知などの判定　・攻撃内容・影響の解析　・定期レポーティング

Why BBSec?

自社のSOCを保有し24h365dの監視が可能

MSSサービスの実績が豊富

セキュリティ専門ベンダー

AWS認定資格者が多数在籍

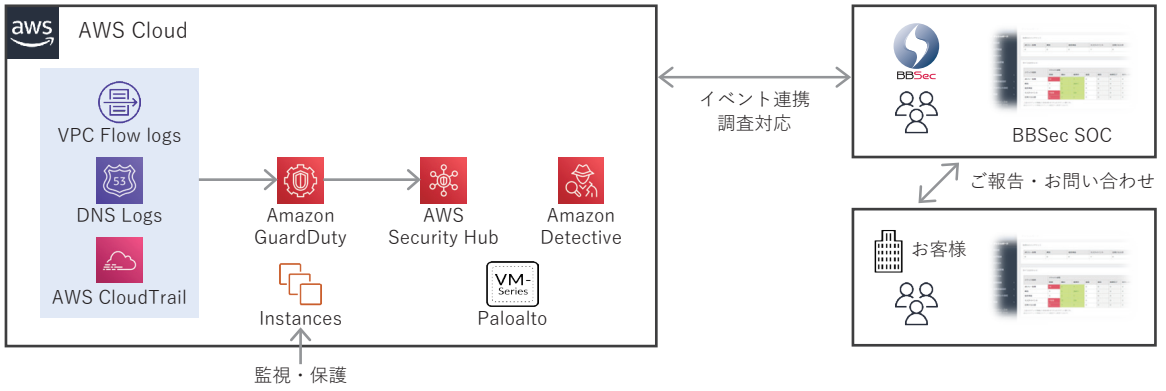
AWSマネージドセキュリティサービス一覧

お客様が利用したいサービスを柔軟にご選択頂けます。

サービス	項目	
セットアップ	導入前ヒアリング	サービス提供準備
	サービス開始前テスト	
監視／イベント対応	アラート精査(チューニング)	モニタリング
	詳細調査分析	AWS WAF運用監視
	お客様向けウェブポータル	月次レポート
	月次報告会	

サービスご提供例

AWSネイティブサービスに対するマネージドセキュリティサービスに加えて、マルチベンダーでサービス提供が可能です。弊社監視システムとお客様のS3バケットを連携し監視を行います。
インシデント発生時には有人SOCがお客様へ連絡しサービス内容に応じた対応を実施いたします。



マネージドセキュリティ

| SASE-MSS powered by Cato Cloud from Cato Networks
| SASE-MSS powered by Prisma® Access from Palo Alto Networks®

ゼロトラストの基盤となるSASE-MSSでインシデント対応までカバー

BBSecの高度で専門的な知識・ノウハウを有するエンジニアが、クラウド提供型セキュリティプラットフォームを用いて、24時間365日体制のMSSを提供します。本サービスを使用することで、お客様の運用負担を軽減しながらも、社内/社外を問わず、高い水準でセキュリティレベルを保つことができます。

サービスの特長

クラウド導入時のセキュリティセットアップ

MSSの導入フェーズでは、お客様環境のヒアリングやMSSを利用するための疎通・検知確認を行うなどセキュリティ機能のセットアップを行います。

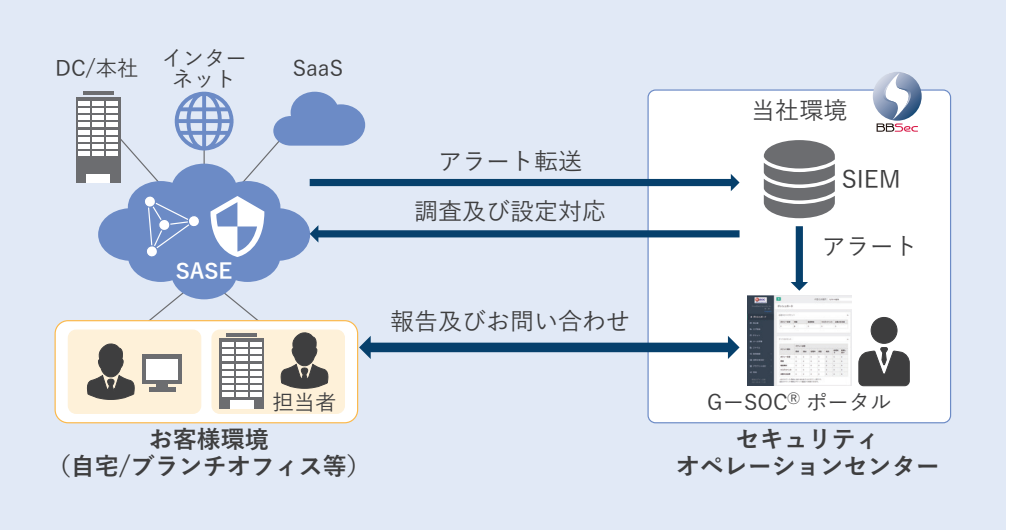
24時間365日、セキュリティを監視

アラートチューニングを実施した上でBBSecの監視G-SOC®チームが24時間365日、絶え間なく監視します。これにより大量のアラートに埋もれる事なくセキュリティ事故等の被害の拡大を防ぎます。

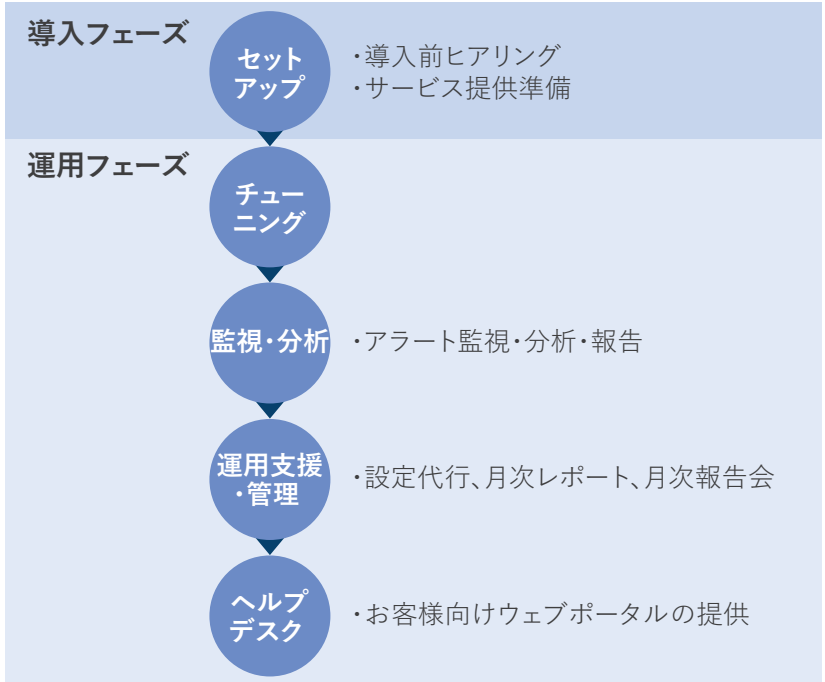
専門家の知見を共有

月次報告会にてナレッジの共有及び定常的な運用管理を行うことで、お客様の負担を増やすことなくSASEを十分に活用することが可能となります。

サービス構成



SASE-MSS導入の流れ



SASE MSS 対象製品

- **Cato Cloud**
  Cato Networks社が提供する「Cato Cloud」は、1つの監視コンソールで世界中の拠点、端末を統合管理可能なクラウドサービスです。
- **Prisma Access**
  パロアルトネットワークス社が提供する「Prisma® Access」は、オンプレミスの次世代ファイアウォール製品に相当する機能をクラウドサービスとして利用できるサービスです。

各種セキュリティデバイス監視・運用支援

WAF運用

Webアプリケーションの脆弱性をつく攻撃を防御するWAF(Web Application Firewall)。BBSecでは、業界トップクラスのImperva社のSecureSphere Web Application Firewallをはじめ、各種WAFのセキュリティ運用を支援しています。高い技術力を要する導入時のチューニングから、ツールから発せられるアラートを24 時間365 日体制で監視・解析する運用までの一貫したサービスは、お客様から高い評価をいただいています。

SecureSphere Web Application Firewall 運用サービスの具体例

項目	BBSec のサービス
Web セキュリティ	24時間365日体制で監視し、ツールが発呼したアラートを解析し、誤検知を排除すると共に、その危険度を判断します。 緊急を要するインシデントが発生した場合には、お客様にお知らせすると共にご要望に応じた対策を実施します。
アプリケーション攻撃の阻止	
ThreatRadar Threat Intelligence	
プラットフォーム・セキュリティ	
高度な保護機	お客様のサイトの状況にあわせ、ホワイトリスト、ブラックリストの登録を行う等のチューニングを実施します。
ポリシー/ シグネチャの更新	セキュリティ更新がなされているか常時監視いたします。
ログ/ 監視	各種セキュリティログの監視を24時間365日体制で行います。

主たる監視対象デバイス:ベンダーニュートラルで対応

項目	
WAF	Imperva: SecureSphere　他

IDS/IPS、UTM、ファイアウォール運用

OS やミドルウェアへの攻撃を検知 / 防御するIDS(Intrusion Detection System)/IPS(Intrusion Prevention System)は、DoS攻撃などに大きな効果を発揮します。また、利用頻度の高いファイアウォール、ファイアウォールの弱点をカバーするUTM(Unified Threat Management)もセキュリティ機器として重要です。

主たる監視対象デバイス:ベンダーニュートラルで対応

項目	機種
IDS/IPS	・McAfee：Network Security Platform　・Trend Micro：Tipping Point IPS シリーズ
UTM	・Fortinet：Fortigate　・Palo Alto：PA シリーズ
Cloud Security	・Imperva：Incapsula　・Trend Micro：DeepSecurity
ファイアウォール	・Fortinet：Fortigate　・Palo Alto：PA シリーズ

クラウドセキュリティ監視・運用支援

クラウドWAF運用　Imperva: CloudWAF（旧Incapsula）に対するMSS

Imperva社のCloudWAFサービスを活用することでウェブサイトのセキュリティを守り、DDoS攻撃によるパフォーマンスの低下を防止します。既存Webサイトへのトラフィックを CloudWAFネットワークを経由させることで、不正なトラフィックを排除し正規利用者のユーザビリティを向上させます。

サービスの具体例

サービス	サービス内容	CloudWAFに対するMSS提供内容・条件
イベントモニタリング	・障害/攻撃を検知した際の通知 ・セキュリティ攻撃に関する分析	・WAF障害/攻撃検知通知 e-mail（日本語） ・ DDoS攻撃通知 e-mail（日本語）
24×365ヘルプデスク	・セキュリティ攻撃に関する問い合わせの受付及び支援 ・テクニカル・サポート（技術的な問い合わせ対応）	・情報連携のためのWebポータルサイトでの提供 （名称：G－SOC®ポータル）
オペレーション代行	・ポリシー設定・変更の運用代行	・WAFホワイトリスト・シグネチャの設定（月5回まで）
レポーティング（オプション/有償）	・一ヶ月の運用内容を統計情報として文書形式で報告	・月次レポートをWebポータルサイトに掲載

サーバセキュリティ運用　Trend Micro: Cloud one Workload Security（旧DeepSecurity）に対するMSS

主にクラウドを利用されるお客様向けサービスです。新たな機器の設置は無いため、既存ネットワーク構成を変更せずに対象サーバへの導入が可能です。

サービス項目

サービス	概要	サービスレベル	
		Lv.1	Lv.2
マネージャーサーバ提供	マネージャーサーバ(共有)を提供	●	●
不正プログラム対策機能	サーバにウイルスが感染することを防止	●	●
Webレピュテーション機能	Webの脅威に対する保護を提供(不正なURLへのアクセスを防御)	●	●
ファイアウォール機能	サーバへのアクセスを制限することが可能	●	●
侵入防御機能	仮想パッチ（脆弱性ルール）によって、既知の脆弱性を突いた攻撃からサーバを保護	●	●
変更監視機能	ファイルやシステムのレジストリに対する不正な変更を検出	●	●
セキュリティログ監視機能	ログファイルに含まれるセキュリティイベントに対する可視性を提供	●	●
システム(サービス状態)監視	監視対象機器に対して24時間365日の遠隔による監視	△*1	●
セキュリティイベント監視	セキュリティイベントのアラート内容を通知	△*1	●
セキュリティイベント分析	セキュリティイベントの分析、分析結果の報告	×	●
ログ管理	直近3か月分のセキュリティイベントログを保存、ご依頼に応じて提供。	×	●
ヘルプデスク	24時間365日、メールまたは電話での問合せ対応、G－SOC®ポータルサイトの提供	△*2	●
レポーティング（オプション/有償）	月次レポートの提供	×	OP

*1 マネージャーサーバーからの自動通知メール送付のみ　*2 メールのみ受付

インターネット分離クラウド　BISC : BBSec Internet Security Cloud

エンドユーザを確実に守る“インターネット分離環境”をインフラ提供と運用サービスでフルサポート

マルウェア対策の決定版として高い評価を得ているインターネット分離。金融庁をはじめ、様々な指導的機関が利用を推奨しており、今後、利用が加速度的に増加していくことが想定されています。BBSecのクラウド型インターネット分離サービス"BISC"は、お客様の外部接続環境を当社クラウドにお預かりし、セキュリティ監視やマルウェア検知、悪性サイトへの通信の自動遮断を、リーズナブルな価格で提供するインターネット分離ソリューションのトータルパッケージです。

サービスの特長

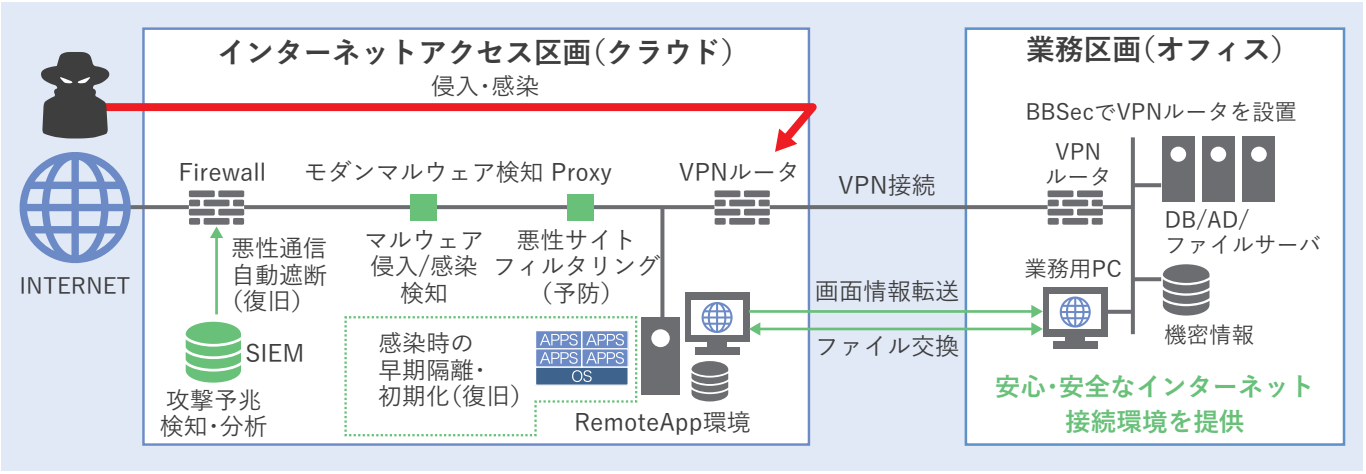
短期間で導入可能
契約から利用開始まで約1.5ヶ月。圧倒的な導入スピードを提供します。

圧倒的な価格優位性
今まで予算面で導入をあきらめていた企業にインターネット分離を実現します。

他に類を見ない広範なサービス範囲
SOC（セキュリティオペレーションセンター）によるセキュリティ運用機能付与やSIEM を用いた調査・対応機能強化が可能です。

標準機能で安全・安心な運用が可能
当社クラウド資産の活用により、従来ご担当者の大きな負担であったインシデント発生時の調査や復旧などの作業を劇的に軽減できます。

サービス構成



BBSec インターネット分離クラウドと他ソリューションの違い

WebフィルタリングとAnti-Virusによる「抑止」、インターネット分離と推奨セキュリティ設定による「予防」、未知のマルウェア検知ソリューションやSIEM/SOCによる「検知」、インシデント発生時の初期化対応による「復旧・回復」、フォレンジックサービスによる「事後対応」の5大セキュリティ対応を全て網羅。お客様は日常業務を大幅に軽減することができ、当社からの報告に基づき、最も大切な“対策”にフォーカスすることが可能です。

	抑止	予防	検知	復旧・回復	事後対応
BISC	BBSecサービス提供範囲				
オンプレミス分離環境	分離環境で実現		お客様対応範囲		
無害化ソリューション	無害化で実現	お客様対応範囲			

SIEM運用/分析

Splunkで一元管理されたログを24時間365日体制で監視/解析

ビッグデータ収集・解析システム「Splunk」に一元管理されたセキュリティログを当社セキュリティ技術者が監視/ 解析し、インシデント発生時にお客様にいち早くお知らせするサービスです。お客様契約のクラウド環境、ないしは、オンプレミス環境に集約されたログを監視/ 解析するサービスと、当社にログを送付していただき監視/ 解析するサービスの2種類を準備しています。対象ログは、セキュリティ機器のものだけでなく入退館システムのログ等も含まれ、包括的なセキュリティ管理が可能です。

サービスの特長

高い分析力

セキュリティ専門ベンダであることを生かしたノウハウを活用して監視ログを解析しています。

相関分析カスタマイズによる精度向上

単発のセキュリティイベントでは攻撃かどうか判別できない事象に対して複数のイベントを相関的に分析するルールをカスタマイズ・チューニングすることによりアラート品質を高めます。

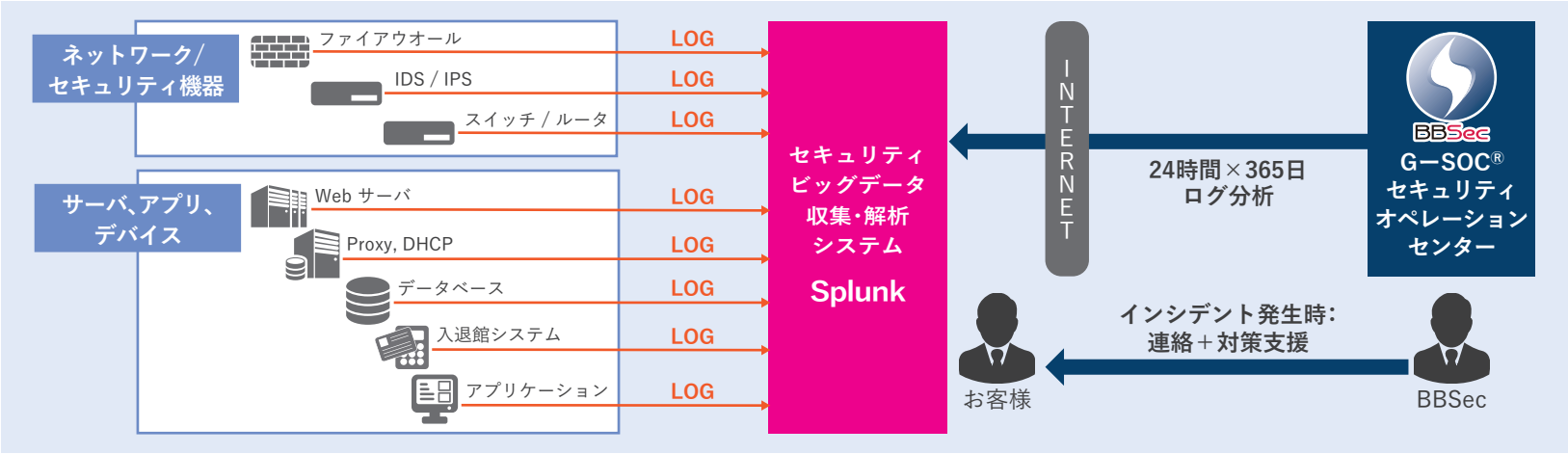
様々な情報を相関分析に活用可能

SOC(セキュリティオペレーションセンター)によ入退館システム・勤怠システムなどの情報システム以外のログや、PC一覧表・IPアドレス管理表などのアセット情報と連携することで、より精度の高い相関分析を実現することができます。

遠隔監視型とSaaS型の双方を提供

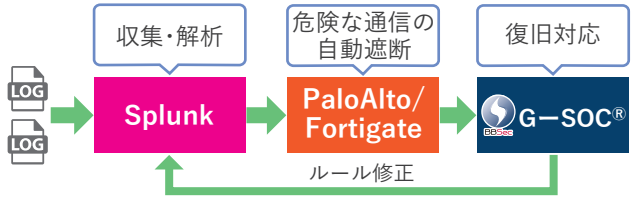
お客様環境のSplunkを活用する方法だけでなく、各種ログをBBSecに送付して分析機能を提供するSaaS型のサービスも提供しています。

サービス構成



Splunk 自動遮断連携　セキュリティデバイスによる検知と遮断をワンストップで実現

市場シェアの高い PaloAlto PAシリーズ、ないしは、Fortinet Fortigateシリーズをご利用の方向けの検知/遮断のワンストップサービスです。SIEM運用/分析サービスのオプションとして提供いたします。詳しくは当社までお問い合わせください。



エンドポイントセキュリティ

組織の端末を24/365体制で監視し、インシデント発生時には端末隔離等の初動対応を実施

従来型のアンチウイルス製品では検知が困難なファイルレス攻撃や、システム内の正規ツールを悪用する寄生戦術（LotL）など、これらの攻撃に対応するためには、次世代エンドポイントセキュリティ製品の導入が不可欠です。BBSecのEDR-MSSは、豊富な実績にもとづいて、お客様端末を24時間365日体制で監視し、インシデント発生時には端末の隔離など初動対応を実施します。

サービスの特長

お客様の運用負担軽減

EDRの運用をBBSecが24時間/365日体制で行うため、お客様の夜間休日対応が不要になるなど、勤務時間の正常化にも効果を発揮します。

重大インシデントへの柔軟かつ連携した対応

高い専門性を必要とする重大インシデント発生後の追加調査や、デジタルフォレンジックにも柔軟かつ連携した対応が可能。また当社他サービス（セキュリティデバイス運用、マルウエア検知等）を組み合わせてご利用いただくことにより、お客様環境に最適化したサービスをご提供可能です。

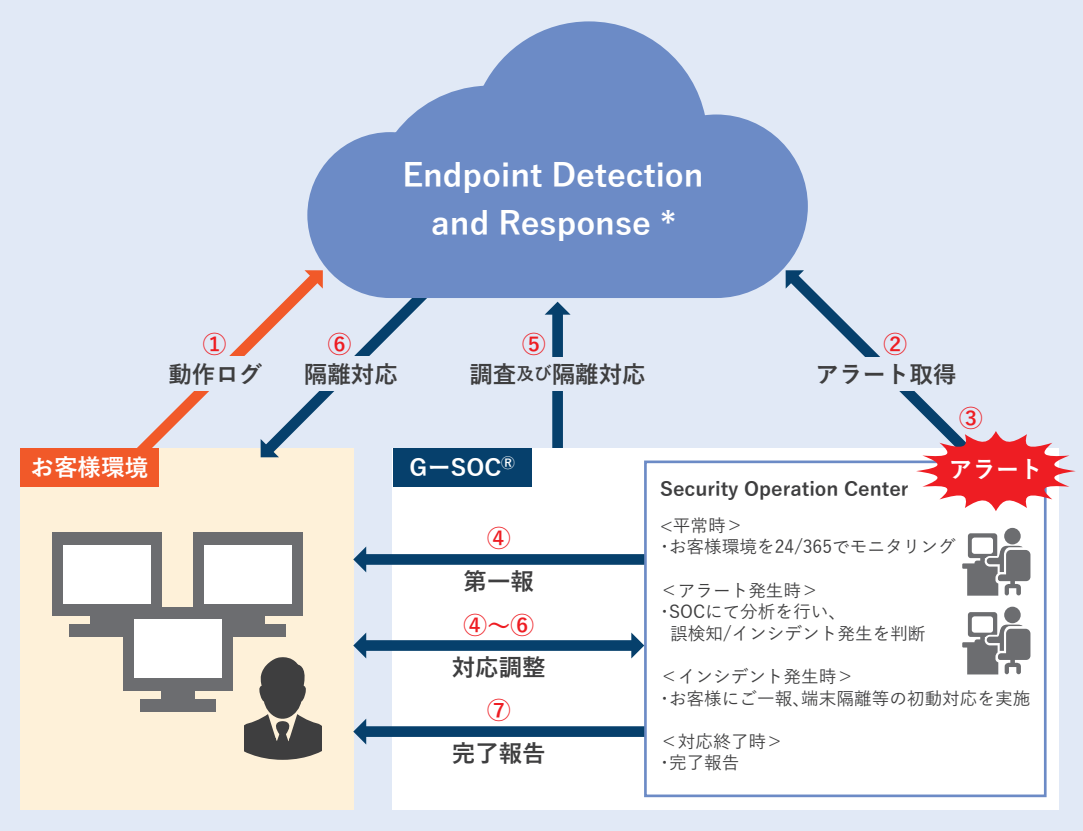
迅速な運用支援によるリスク最小化

端末隔離など、インシデント発生時の初動を24時間365日体制で実施。短時間での初期対応は組織のリスク軽減に効果を発揮します。

一貫したポリシー設定、対策が可能

当社サービスにより、インフラからエンドポイントまで、一貫したセキュリティポリシー、サービス品質の提供が可能です。

サービス構成



＊対象製品
- SentinelOne Singularity Endpoint
- VMware Carbon Black
- Microsoft Defender for Endpoint

※ EDR-MSSをご利用いただける各製品のエディションについては、お問い合わせください。

脆弱性情報提供　SAS:Secure Net Alert Mail Service

不要な情報を省き、お客様のシステムに必要な脆弱性情報のみを早期通知

ソフトウェア製品やウェブサイトの脆弱性情報は年間1万件規模で報告されており、もはや企業の情報システム担当者だけでは、個々の脆弱性情報が自社システムに影響を及ぼすか否かの判断をする処理能力を超えています。しかしその一方で、個々の対策を怠ると、甚大な被害を生み出す危険性をはらんでいます。BBSecの脆弱性情報提供サービスは、このジレンマを解決する為に莫大な脆弱性情報の中から自社に必要となる脆弱性情報のみをフィルタリングしてお届けする情報提供サービスです。

サービスの特長

1時間単位の脆弱性情報配信
1時間毎の情報発信により最新情報を入手することができ、迅速な対応を可能にします。

ニーズにあわせた3つのプランをご用意
把握に便利な日本語版、即時性を優先する日本語 / 英語混在版、マルチテナント版の3種類をご用意しています。

セキュリティ・アドバイザリと連携可能
入手した脆弱性情報に対する対応方法をアドバイスするサービスもご用意しています。

脆弱性管理機能を内包
個々の脆弱性に対してお客様環境での脅威判定に用いるためのCVSS計算機能、脆弱性対応状況を管理するための対応ステータス管理機能など、お客様の日々の脆弱性管理業務を支援する機能を提供いたします。

サービスの特徴

項目	ベーシック	エクスプレス	マルチテナント
特徴	日本語による脆弱性情報	スピード重視の脆弱性情報（英語または日本語）	複数の顧客(システム) の脆弱性管理が可能
配信情報	JVN*1に掲載された日本語レポート 主に脆弱性の概要、想定される影響、対策方法、CVSS 基本値を案内	NVD*2掲載の英語レポート / JVN掲載の日本語レポートのいずれか早期に公開されたレポートを優先配信。情報は、脆弱性の概要、CVSS基本値が中心。	顧客(管理対象システム) 毎にベーシック、又はエクスプレスのいずれかの配信方式を選択
情報提供方法	メール配信（PDF レポート添付）、管理Web-GUI による情報参照		
配信間隔	1時間毎		
オプション	セキュリティ・アドバイザリサービス：脆弱性情報に対する対応方法をアドバイスします		

*1 Japan Vulnerability Notesの略。IPAとJPCERT/CCが共同運営する脆弱性情報データベース　*2 National Vulnerability Databaseの略。米国国立標準技術研究所が運営する脆弱性情報データベース

サービス概念図

セキュアメール　AAMS® : Anti-Abuse Mail Service

サービス事業者も利用するセキュリティノウハウが集約されたメールサービス

マルウェア添付のメールやスパムメールなどのビジネスの妨げとなる有害メールを、最新の情報に基づきフィルタリングするメールホスティングです。セキュアメールは、企業のみならずインターネット事業者にも利用されており、数十万IDの運用実績を誇ります。誤送信抑止対策や添付ファイルパスワード付ZIP変換、メールアーカイブなど、豊富なオプションサービスをご用意しています。

サービスの特長

国内有数のメールASP
数十万アカウントの大規模メールシステムを動かし続けています。

SOCによる24時間365日運用
メール専任エンジニアが24 時間体制でシステムの安定稼動を見守り、大量のDoS攻撃が発生しても迅速に対応しています。

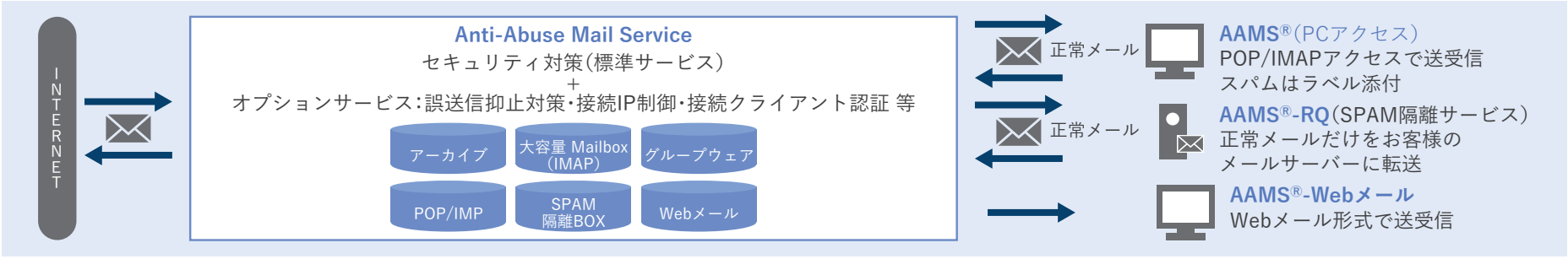
ニーズに合わせたサービス提供
メールホスティングサービス、メールゲートウェイサービスの2 種類をご用意しています。

メールコンプライアンス実現に最適
メール全件保存やメール監査などのオプションを選択することで、J-SOX 法で要求されるメールコンプライアンスを簡単に実現できます。

主たる機能

添付ファイルWebアップロード	メール送信時に添付ファイルが存在する場合、自動的に添付ファイルをZIP暗号化しWeb上のファイルストレージにアップロード、そのファイルにアクセスするための情報(URLとパスワード)を、別メールにてお知らせいたします。 問題があった場合は送信済みの添付ファイルを相手がダウンロードする前に取り消すことができます。
添付ファイルパスワード付ZIP 変換	社内から外部への送信メールに添付されたファイルを、自動でZIP暗号化/パスワード付与を行う情報漏えい対策です。 パスワードは、送信者にメールで通知されますので、それを受信者に送ることで、受信者はファイルを解凍することができます。
誤送信抑止対策	ユーザが送信したメールを誤送信抑止サーバに一定時間保留することでメールの誤送信を防ぐ機能です。
メール保存（アーカイブ）	社内でのメール、社外とのメールを問わず、全ての送受信メールをユーザPOP/IMAP領域とは別領域の大容量ストレージに保存します。
アカウント不正利用検知	複数の条件、パラメータの組み合わせにより、外部から不正に利用されていると思われるアカウントを検出し、メールの送信を抑止。 意図せず「SPAM配信企業」と判定されてしまうような事故の発生リスクを低減します。
Webメール	社外（外出先・自宅等）からのメール利用環境の利便性を高めるWeb メール機能を提供しています。 iOS / Android / Windows Mobile などのスマートフォンにも標準対応しています。

サービス構成



AAMS® マルウェア・プロテクト　AAMS® MP : AAMS® Malware Protect

ユーザに届く前に標的型攻撃リスクのあるメールを自動隔離、検証

AAMS® マルウェア・プロテクトは、ユーザの手を煩わせることなく、メールマルウェア感染チェックとその結果に対する技術者解析（SOCサービス）を提供する、標的型攻撃対策メールホスティングサービスです。高度なメールフィルタリング機能により、リスクのあるメールは、エンドユーザへの配信を一時停止し検証を行い、それメール以外はリアルタイムにエンドユーザへ配信。ビジネスに影響を与えることなく、安全なメール環境を確保できます。

サービスの特長

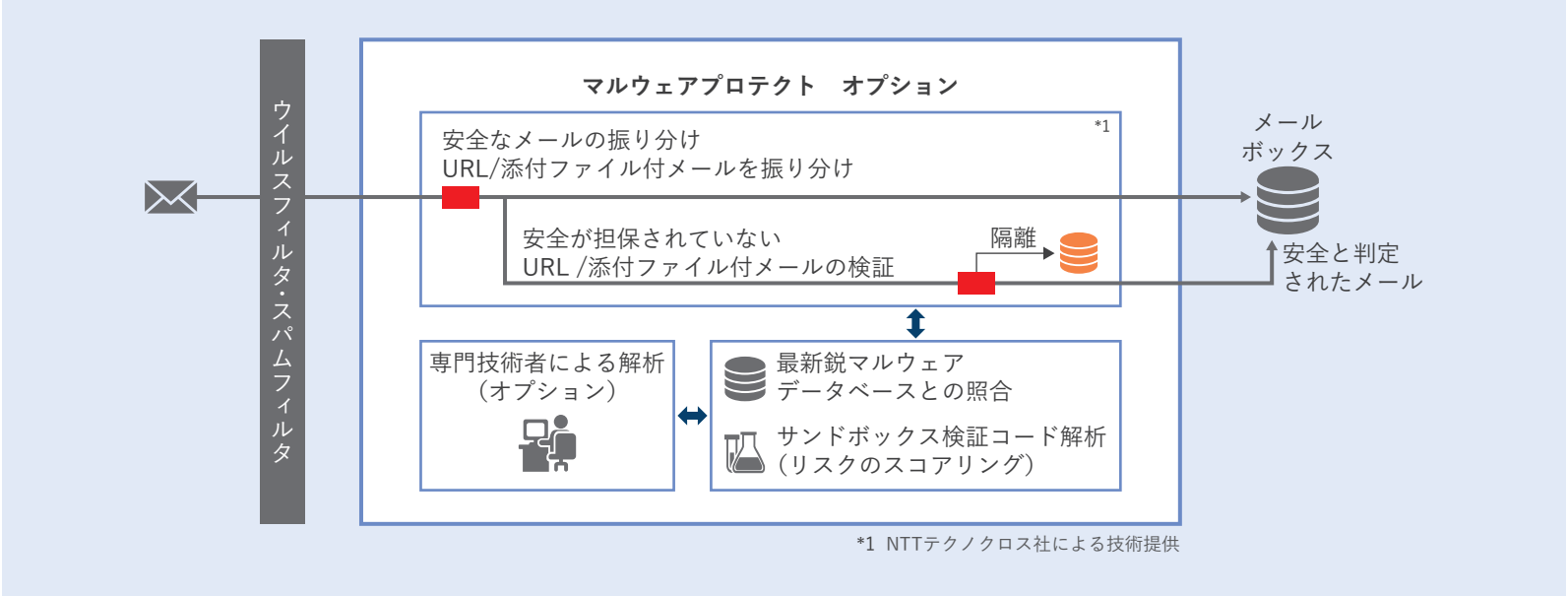
ビジネスに影響を与えないメール配信速度
メール配信に求められるビジネススピードを維持しながら、リスク軽減が可能です。

管理者の負担軽減
マルウェア感染リスクのあるメールをサーバに自動で格納して検査を行う為、検証結果に対する対策を行う以外の作業は不要です。

国外へのデータ流出リスクを回避
国内環境で全ての保管/検証を行う為、海外へのデータ流出リスクへの懸念は不要です。

ユーザのマルウェア接触度を大幅削減
マルウェア感染の根本治癒となる、エンドユーザへのマルウェア感染メールの 到達を劇的に削減することができます。

サービス構成



*1 NTTテクノクロス社による技術提供

セキュリティログ分析/活用支援

ログの分析から統合管理・分析環境(Splunk)の構築・運用までトータルにサポート

サイバー攻撃から組織を守る上で、ログは極めて重要な財産です。本サービスは、社内に蓄積された各種ログの分析支援や有効活用に向けたコンサルティング、更には、統合ログ管理/分析システム(SIEM)の導入とその運用までを包括的に支援する統合サービスです。すでにシステムを保有している企業だけでなく導入を検討中の企業にも、企業ポリシーや体制にあった最適なログ分析を実現できるよう、支援します。

サービス構成

検証・可視化

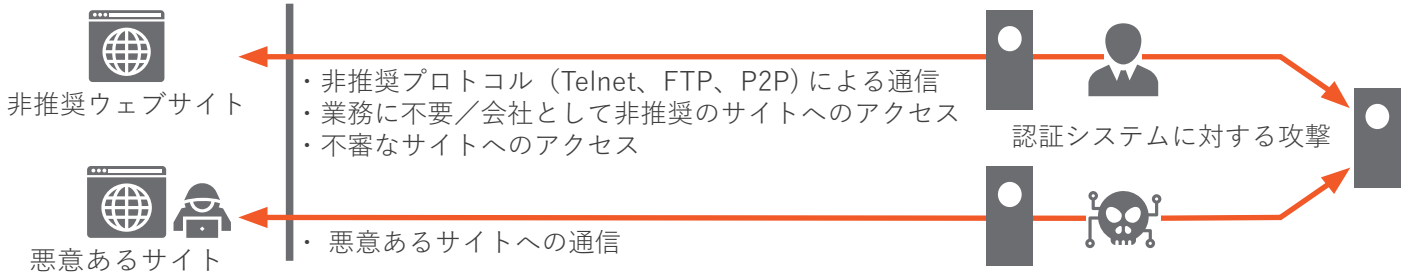
企画・教育

構　築

運　用

ログ解析

一定期間(1～3ヶ月)のログをお預かりし、ログから不正挙動の痕跡を可視化してリスクを顕在化します。



ログ取得環境整備コンサルティング

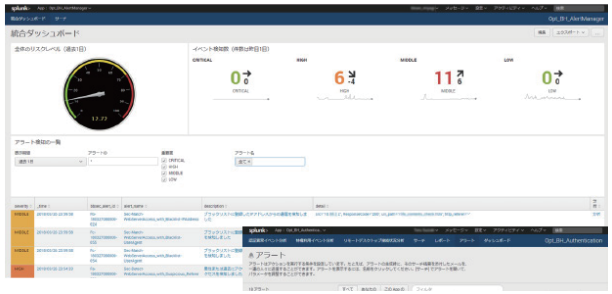
現状調査をもとに、最適なログ取得環境を提言します。

キックオフ ▶ ログ取得の目的・対象の定義 ▶ 現状調査 ▶ 分析 ▶ ベストプラクティスの提示 ▶ 改善プラン検討 ▶ 報告書作成 ▶ 報告会

現状調査
- 管理ポリシー
- 取得状況
- 支援体制
- 運用プロセス

Splunk(総合ログ管理・分析システム)構築支援/分析App 提供

統合ログ管理・分析システムの構築および分析App(分析ルールセット)をご提供し、稼働当初より有益な分析ができるよう支援いたします。



Splunk セキュリティ監視

侵害の疑い ▶ デジタルフォレンジック

サイバープロテクション（CP）

中小企業・団体向けセキュリティパッケージサービス

サイバー攻撃対策は何をしたらいいか分からない。そんなにお金や人を費やせない。
でも何かしないといけない・・
そのようなお悩みの解決に、サイバー攻撃に対する基本対策をパッケージしました。

サイバーセキュリティお助け隊

IPAサイバーセキュリティお助け隊登録（サービス登録番号：2023-001）

サービスの特長

貴社・貴団体のサイバーセキュリティ担当者として

①24時間の端末監視・運用（EPP+EDR）
②専用の相談窓口（電話・メール対応）
③インシデント発生時の対応（駆付け／リモート）
④簡易サイバー保険（インシデント対応費用を補償）
※限度額・条件あり

業務受託時のアピールに効果的

全国に駆け付け（離島・島しょ部も含む） ※交通費も補償対象

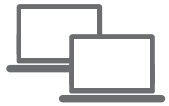
インシデントが発生し、端末が隔離された後の復旧支援に対してお客様のご負担を抑えつつ実施します（現場に駆付け、またはリモートで対応可能）

対象端末1台から導入可能

端末全台に導入しない場合は、機密・個人情報を扱う、インターネットに接続するクリティカルでリスクの大きな端末への導入を推奨します。

豊富なセキュリティオプションサービス

ニーズ・ご予算に応じ、従業員向けセキュリティ教育など当社サービスと組み合わせることにより、安心・安全に情報資産の守りを強化可能です。



端末監視ソフト（EPPとEDR）をインストールするだけ。
ソフトやセキュリティプロテクションチームが日々監視を行い、
インシデント発生時には迅速にサポートします。

・監視
・アラート通知

・相談

・インシデント
・対応支援

監視・運用

EPP+EDR+SOCが
お客様の端末を
24時間365日体制で監視

相談窓口

導入したEPPやEDRに関する
お困りごとは電話やメールで
サポート（平日9時～18時）

駆け付け/リモート対応

インシデント発生時には
現場に駆け付け、または
リモートでサポート

＋

簡易サイバー保険付帯

インシデント対応費用も、保険で補填できるので安心 ※限度額等諸条件あり

① 監視ソフト（EPPとEDR）とセキュリティ・オペレーション・センター（SOC）による24時間365日の端末監視
② 相談窓口（お客様サポートセンター）
③ インシデント発生時の緊急対応支援
④ 簡易サイバー保険（緊急対応支援を行った際の費用等の補償）

サイバーセキュリティお助け隊とは？

サプライチェーンを構成する中小企業・団体もサイバー攻撃の脅威に曝されている実情に対し、経済産業省がその普及を後押ししている制度・サービスです。

デジタルフォレンジック

プロフェッショナルの技術とノウハウで、お客様の迅速な緊急対応を支援

情報漏えいやサイバーアタックなどの重大インシデント発生時に、当社のトップクラスのセキュリティコンサルタントを中心にお客様のためのチームを組み、インシデントの収束を支援いたします。さらに、証拠保全や今後の対策検討など、事態を打開し影響を最小限にとどめる為の広範囲のサポートを行い、お客様ビジネスが可能な限り早く平常に戻る様、当社サービスの一時利用も含め協力をしてまいります。

サービスの特長

24×365体制の緊急窓口を設置

いつ何時訪れるか想定できないIT セキュリティインシデントに対応するため、24時間365日体制の受付窓口を準備しています。

ハイスキルのセキュリティ技術者が対応

状況を正確に把握して的確な判断と対策を行う為に、高い経験値と技術力をもつ技術者が初期対応の陣頭指揮にあたります。

様々な緊急の状況に対応

「激しいサイバーアタックをうけ、どう対策してよいかわからない」など、判断のつかない緊急事態にも丁寧に対応いたします。

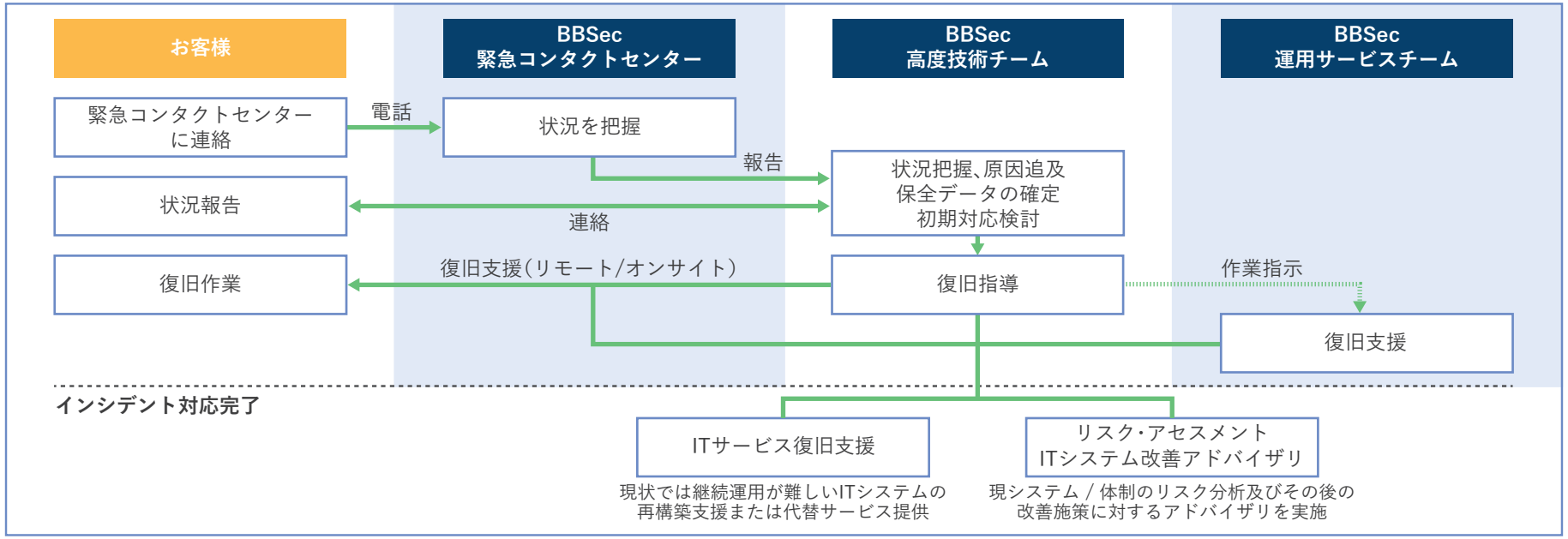
お客様業務を最大限確保

インシデント対応やデータ保全と並行し、お客様業務の停止期間を最小化させる為の施策を共に考えてまいります。

サービス構成

セキュリティの専門事業者ならではの迅速かつ高度な初期対応

インシデント検知 ▶ 被害状況確認 ▶ 原因調査・把握 ▶ 防御 ▶ 被害規模確認 ▶ 根治 ▶ 証拠保全 ▶ サービス再開 ▶ 対策検討・実施



緊急コンタクトセンター

プロフェッショナルの技術とノウハウで、お客様の緊急対応を支援

自社での対応が難しい重大インシデントが発生もしくは懸念された場合には、当社「緊急コンタクトセンター」に急ぎご連絡ください。当社のセキュリティ・スペシャリストが、お客様のインシデントの状況を把握し、解決へと向かう道を共にお手伝いさせていただきます。

サービスの特長

インシデント受付に条件をつけない
当社のお客様である / なしにかかわらず、対応いたします。

24時間365日体制で受付
24 時間365 日体制の緊急コンタクト窓口を開設しています。

BBSec 緊急コンタクトセンター

☎0120-085490（24時間365日受付）

サイバー脅威情報調査

プロフェッショナルの技術とノウハウで、お客様の緊急対応を支援

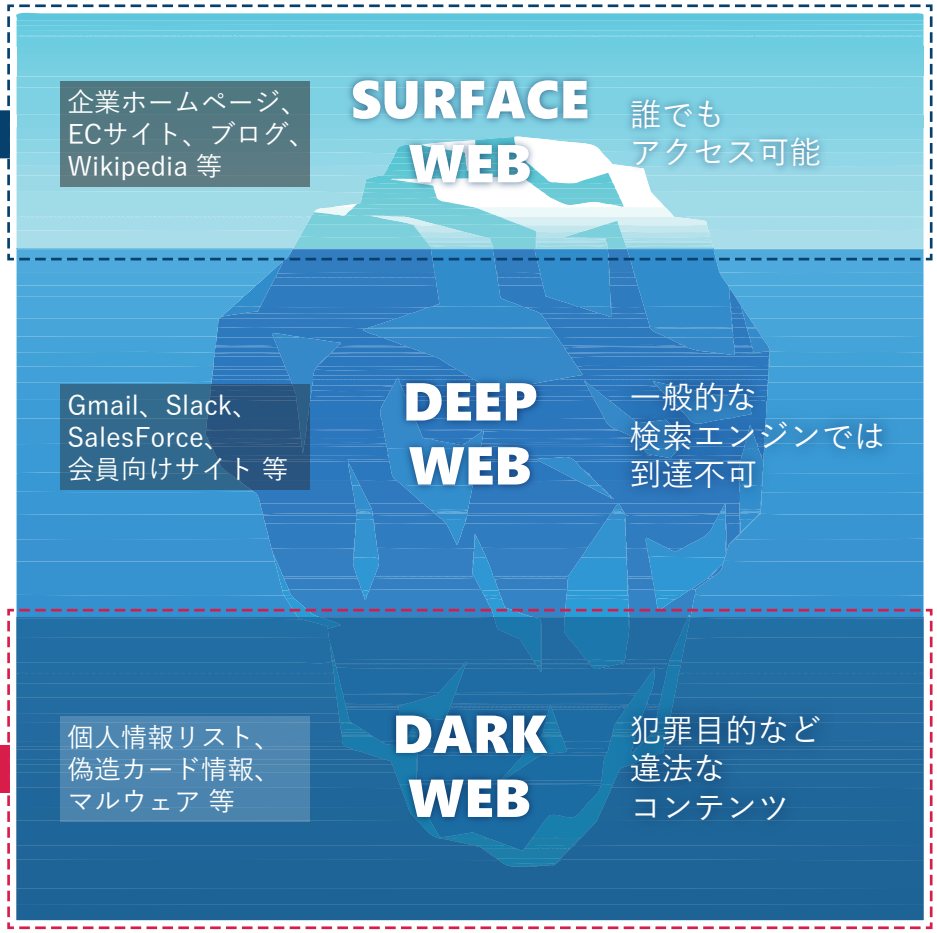
サイバー脅威に備えるために必要なのは、自組織が晒されている脅威の状況を知ることです。想定外の脅威や脅威の緊急度を把握することは、適切な対策を講じる重要なカギとなります。「サイバー脅威情報調査」は、不正アクセス被害が発生したり、情報漏洩の恐れが懸念されたりした場合に、ダークWeb上で機密情報が公開されているかを調査・報告するサービスです。

アタックサーフェス調査　SQAT® ASM

インターネット上で合法的に入手可能な公開情報からサイバー攻撃の脅威となり得る情報を収集します。幅広く貴組織で未把握の脅威を確認するのに有効です。

サイバー脅威情報調査

匿名性が高く、特殊な方法でないとアクセスできないダークWeb上の情報を調査します。犯罪に直結しうるコンテンツの中に貴組織の重要情報がないか、確認します。



Corporate Site

便利で安全なネットワーク社会を創造する

BBSec

https://www.bbsec.co.jp/

セキュリティサービス　ウェビナー　IR/企業情報

セキュリティ対策に欠かせないIT／組織両視点からのサービスで、
お客様が今必要とする最適な「答え」をご提供します。

Owned Media

Webサイト提案から構築までトータルにサポート

Gomez®

https://www.gomez.co.jp/

Webサイトランキング
コンサルティングサービス
サイト構築・運用サービス

私たちは、「利用者の視点」からインターネットの
あるべき姿を追求し、サービスを提供します。

Owned Media

日本のセキュリティを強くしたい

SQAT® Software Quality Analysis Team

https://www.sqat.jp/

セキュリティ診断サービス
セキュリティ情報
イベント情報

BBSecの脆弱性診断は、精度の高い手動診断と自動診断を
組み合わせ、お客様システムの健全化に貢献します。

SQAT®.jpは、BBSecセキュリティサービス本部の管理・運営によるサイトです。
「SQAT®」は、BBSecが提供する脆弱性診断サービスです。

法人・技術者・コンサルタントの保有資格

BBSecでは、信頼できる事業者であることを公的に認識いただくため、法人としての各種資格を取得しています。
また、解決策に偏りがないよう、資格を保有する技術者を中心に、チームでお客様を支援します。

組織としてのセキュリティ

■情報セキュリティマネジメントシステム：ISO/IEC 27001:2013=JIS Q 27001:2014 ICMS-SR0328 / JIS Q 27001 *1

■品質マネジメントシステム：ISO9001：2015 GIJP-1399-QC ISO 9001:2015 *2

■プライバシーマーク：JISQ 15001：2006 10470048

■PCI DSS認証監査機関：QSA(Qualified Security Assessor Company) QUALIFIED SECURITY ASSESSOR *3

■P2PE認証監査機関：Point-to-Point Encryption Assessor Company POINT-TO-POINT ENCRYPTION ASSESSOR

■3Dセキュア認定評価機関：PCI 3DS Assessor Company

■カード情報漏えい事故を取り扱う調査機関：PFI(PCI Forensic Investigator)

■クレジットカード製造におけるセキュリティ評価機関：CPSA(Card Production Security Assessor)

■情報セキュリティサービス基準適合サービス登録 *4

*1 情報セキュリティマネジメントシステム：ISO/IEC 27001:2013=JIS Q 27001:2014
登録範囲に含まれる組織：本社、有明オフィス、大阪支店、データセンター、天王洲オフィス、名古屋支店
セキュリティ診断/ コンサルティングサービス、セキュアメールサービス、マネジメントサービス　左記業務にかかわる情報セキュリティマネジメント

*2 ISO9001:2015(Quality Management System)
適用業務：Information security assessment and audit(情報セキュリティに関わる監査業務)

*3 The QSA logo is a trademark or service mark of PCI Security Standards Council, LLC in the United States and in other countries and is being used herein under license.

*4 情報セキュリティサービス基準適合サービス登録
対象サービス(登録番号)：情報セキュリティ監査サービス(018-0038-10)、脆弱性診断サービス(018-0038-20)、デジタルフォレンジック(018-0038-30)、マネージドセキュリティサービス(018-0038-40)

技術者・コンサルタント

国家資格

・ITストラテジスト(ST)　・システムアーキテクト(SA)　・ネットワークスペシャリスト(NW)
・データベーススペシャリスト(DB)　・システム監査技術者(AU)　・情報処理安全確保支援士(SC)

ベンダー資格

CISCO	・シスコ技術者認定資格 プロフェッショナル
LPI	・Linux技術者認定試験(LPIC-3)
ITIL Foundation	・Information Technology Infrastructure Library(ITIL)
AWS	・AWS Certified Security - Specialty(AWS SCS) ・AWS Certified Advanced Networking - Specialty(AWS ANS) ・AWS Certified Database - Specialty(AWS DBS) ・AWS Certified Data Analytics - Specialty(AWS DAS) ・AWS Certified Machine Learning - Specialty(AWS MLS) ・AWS Certified Solutions Architect - Professional(AWS SAP) ・AWS Certified DevOps Engineer - Professional(AWS DOP) ・AWS Certified Solutions Architect Associate(AWS SAA) ・AWS Certified SysOps Administrator - Associate(AWS SOA) ・AWS Certified Developer - Associate(AWS DVA) ・AWS Certified Cloud Practitioner(AWS CLF)
Palo Alto	・Palo Alto PSE Platform-Professionals ・Palo Alto Networks Certified Network Security Engineer(PCNSE) ・Palo Alto AMPLIFY Security Fundamentals
Vmware	・VMware Sales Professional ・VMware Technical Solutions Professional(VTSP) ・VMware Endpoint Protection Post-Sales Accreditation
Splunk	・Splunk Core Certified Power User ・Splunk Accredited Sales Rep I ・Splunk Accredited Sales Engineer I ・Splunk Enterprise Certified Admin
Microsoft	・Azure Fundamentals
ESET	・ESET認定技術者
GSX	・グローバルセキュリティエキスパート セキュリスト（SecuriST）認定脆弱性診断士 WEB ・グローバルセキュリティエキスパート セキュリスト（SecuriST）認定脆弱性診断士 NW
PCI SSC	・QSA ・P2PEQSA ・CPSA物理 ・CPSA論理 ・3DS Assessor ・PCI Forensic investigator(PFI)
ISC2	・CISSP
ISACA	・CISA ・CISM
PMI	・PMP
SANS	・GCFA ・GNFA ・GREM ・GCFE ・GCIH ・GPEN

BBSec
BroadBand Security, Inc.

https://www.bbsec.co.jp/

SEC110 Security for Enterprise business Continuity

BBSec 緊急コンタクトセンター　☎0120-085490（24時間365日受付）

＜事業拠点＞

東京本社	〒160-0023 東京都新宿区西新宿8-5-1 野村不動産西新宿共同ビル4F	TEL:03-5338-7430
大阪支店	〒530-0001 大阪府大阪市北区梅田1-1-3 大阪駅前第3 ビル30F	TEL:06-6345-3880
名古屋支店	〒460-0003 愛知県名古屋市中区錦1-6-18 J･伊藤ビル6F	TEL:052-265-7591
韓国支店	15F, Samsung Life Seocho Tower, 4 Seocho-daero 74-gil, Seocho-gu, Seoul 06620, Korea	TEL:+82-2-6011-4640
天王洲オフィス	〒140-0002 東京都品川区東品川2-5-8 天王洲パークサイドビル3F	TEL:03-6433-3116
東北セキュリティ診断センター	〒010-0001 秋田県秋田市中通1-4-32 秋田センタービル8階	TEL:018-838-6330
セキュリティオペレーションセンター	東京都内	

SG_リ_09-1_2025.01