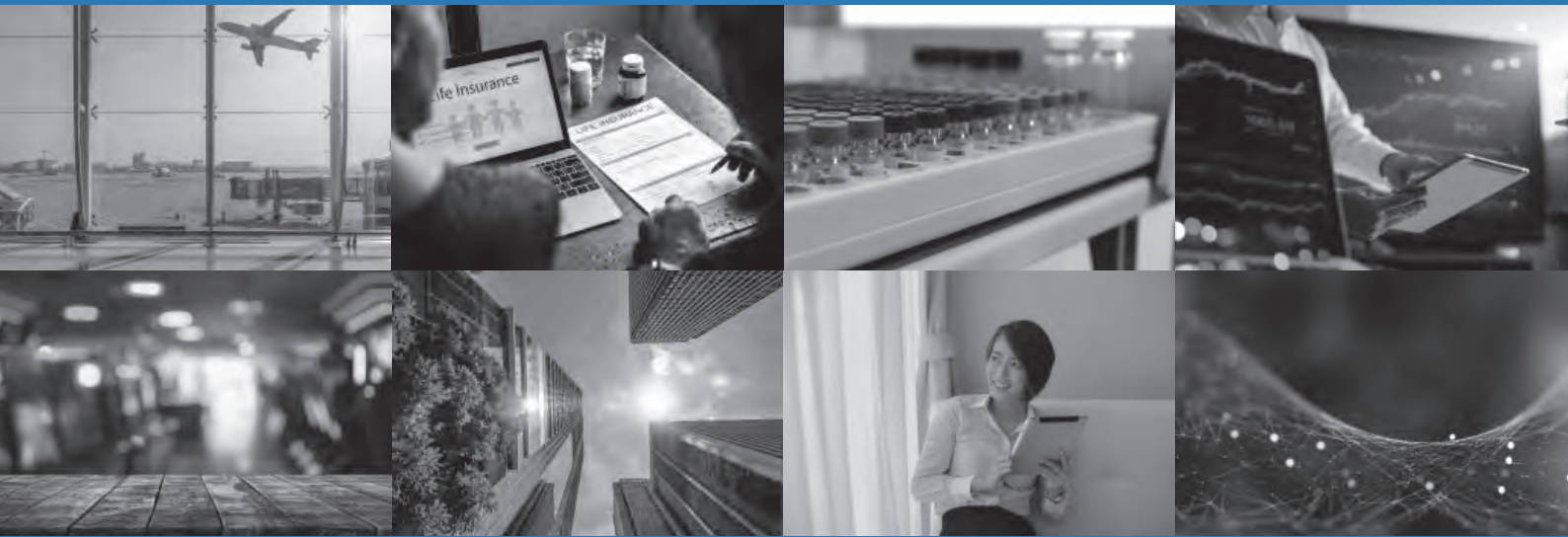


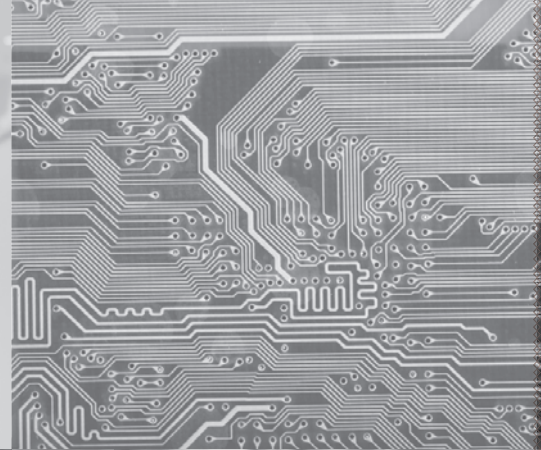
BBSec セキュリティコンサルティング事例集



株式会社ブロードバンドセキュリティ

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
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
韓国支店	15F, Samsung Life Seocho Tower, 4 Seocho-daero 74-gil, Seocho-gu, Seoul 06620, Korea TEL : +82-2-6011-4640

※ 本カタログは2020年03月現在のものです。これらは予告なしに変更する場合がございますので予めご了承ください。
※ 記載の会社名、商品およびサービスの名称は、当社ならびに各社の商標または登録商標です。



目次

金融	
金融庁のセキュリティ指針準拠を BBSec と共に	02
製造	
高品質なリスクアセスメントを的確な計画・対策につなげる	03
保険	
金融庁の指導に円滑に応えるための態勢を整える	04
小売	
同業他社の情報漏洩を受けて体制を強化	05
インフラ	
重要インフラにふさわしいセキュリティ体制を実現	06
情報通信	
セキュリティリスクの高いビジネスモデルを防御する	07
エンターテインメント	
インシデント発生時の情報共有を迅速に	08
卸売	
安全なクラウド活用を実現する	09
製造	
自社の特許技術をセキュリティ対策で守る	10
卸売	
自社ブランド維持の為に、第三者の専門的視点を取り入れる	11
情報通信	
常にお客様から求められる、セキュリティの信頼性を高める	12
情報通信	
多拠点のセキュリティリスクを正確に把握する	13
製造	
海外拠点の現状を第三者の視点で確認する	14
情報通信	
世界中に広がる拠点で、セキュリティ基準に準拠する	15

金融庁のセキュリティ指針準拠を BBSec と共に

金融機関である同社は、金融庁の指針に準拠すべく対策に乗り出した。最初に、自らの課題をリスクアセスメントで可視化し、検証 / 計画 / 対策 を繰り返し実施。その段階で蓄積したノウハウは、同社のスキルアップだけでなく、グループ企業の金融機関の指導にも役立てている。同社は、時間の経過と共に強固なセキュリティ基盤をもつ組織へと成長し続けている。

目的：金融庁指針に基づいたセキュリティ対応態勢整備

< BBSec のソリューション >

- ・ 現状の可視化：リスクアセスメント
- ・ 社内防衛体制の整備：
CSIRT 構築コンサルティング
- ・ 効果的な対策の模索：
セキュリティアドバイザリ
- ・ 情報管理の基礎データ構築：
データマップコンサルティング
- ・ 開発技術の強化：
セキュア開発標準策定コンサルティング
- ・ ログ解析の体制・方針検討：
セキュリティログコンサルティング
- ・ 運用リスク回避のための情報源：
脆弱性情報提供

< 効果・評価 >

- ・ 自社 / グループ企業も含め、情報システム部門のセキュリティに対する意識が改善され、日々の運用におけるセキュリティ対策が細やかに行われるようになった。
- ・ 今後、現状対応できていない部分を順次改善すると共に、定期的なアセスメントを行い、問題点を可視化していく。

高品質なリスクアセスメントを 的確な計画・対策につなげる

世界を市場として活躍する同社は、サステナビリティ活動の一環として「グローバルな情報セキュリティ体制の確立」を掲げ、現状の可視化、対策の計画 / 具現化をすすめている。多くの企業同様、セキュリティ専従者が不在の同社は、BBSecの高度かつ客観的な知見を効果的に活用し国内外の工場 / 拠点を含めたセキュリティ態勢を整えつつある。

目的：中期計画への効果的なセキュリティ対策の落とし込み

< BBSec のソリューション >

- ・ 現状の可視化：リスクアセスメント
- ・ 規程・ガイドラインの精度向上：文書支援コンサルティング
- ・ Web システム強化：脆弱性診断
- ・ 効果的な対策の模索：セキュリティアドバイザリ
- ・ ログ解析の体制・方針検討：セキュリティログコンサルティング
- ・ ログ解析の体制構築：SIEM 構築支援
- ・ 運用リスク回避のための情報源：脆弱性情報提供

< 効果・評価 >

- ・ リスクアセスメントにより課題が明確となり、次の一手が打てるようになった。
- ・ セキュリティ関連規定が整備され、加えたセキュリティログを活用した監視体制が構築されたことで、社内のセキュリティ基盤が更に強化された。

保険

金融庁の指導に

円滑に伝えるための態勢を整える

総合保険代理店である同社は、金融庁からの指導である FISC ガイドラインへの継続的な準拠を実現すべく、「FISC ガイドライン」を基準とした現状の可視化および準拠に必要な規定類のレベルアップを BBSec と共に進めている。また、第三者である BBSec のアセスメント結果は、金融庁への報告書として利用できるため、定期的なアセスメントを行っている。

目的：第三者の評価結果に基づく FISC ガイドライン準拠状況の報告

< BBSec のソリューション >

- ・ FISC ガイドラインへの準拠状況の可視化：
FISC アセスメント
- ・ 準拠に必要な規定・ガイドラインの精度向上：
FISC 文書支援

※ FISC (金融情報システムセンター The Center for Financial Industry Information Systems)

< 効果・評価 >

- ・ 年次の金融庁への報告が円滑に行えるようになったのと同時に、組織に所属するメンバーすべてが FISC 準拠を意識するようになった。
- ・ 今後、FISC 準拠だけにこだわらず、情報資産を守るための様々なマニュアルの整備 / 体制強化を行っていく。

同業他社の情報漏洩を受けて 体制を強化

全国に店舗をもつ同社は、同じ業界で発生したインシデントにより危機感を覚え、セキュリティ対策の強化に乗り出した。自社が保有する処方箋などの個人情報守る態勢、インシデントが発生してもすぐに気づける仕組み (SIEM)、社内規定の整備など、IT / 組織両面からのセキュリティ強化を推進している。

目的：IT / 組織両面からのセキュリティ対策レベルの底上げ

< BBSec のソリューション >

- ・ 現状の可視化：リスクアセスメント
- ・ 規程・ガイドラインの精度向上：
文書支援およびインシデント対応計画作成支援
コンサルティング
- ・ ログ管理体制構築・運用：
SIEM 構築支援、運用支援
- ・ Web システム強化：脆弱性診断
- ・ 強固なセキュリティ基盤構築・運用：
マネージドセキュリティ

< 効果・評価 >

- ・ リスクアセスメントの実施によりセキュリティ対策面での課題が明確となり、効果的な対策計画を立案することができた。
- ・ 優先度設定のアドバイスにより、早期に対策を推進することができた。
- ・ 現場での精力的な活動が功を奏し、経営層のセキュリティに対する意識にも変化が現れた。

インフラ

重要インフラにふさわしい セキュリティ体制を実現

国の重要インフラ関連事業者である同社は、それに見合うセキュリティ強化を常に求められている。同社はリスクアセスメントにより現状を可視化後、人的リソースが不足するなか、専門家である BBSec と協力体制をとることで、強固なセキュリティ基盤を構築。更に CSIRT を構築することで、それを運営していく人的態勢も整えていった。

目的：組織全体に及ぶセキュリティ体制の強化

< BBSec のソリューション >

- ・ 現状の可視化：
リスクアセスメント、制御系システムリスクアセスメント
- ・ 規程・ガイドラインの精度向上：
文書支援コンサルティング
- ・ 効果的な対策の模索：
セキュリティアドバイザー
- ・ 運用リスク回避のための情報源：
脆弱性情報提供
- ・ 社内防衛体制の整備：
CSIRT 構築コンサルティング
- ・ ログ管理体制構築・運用：
SIEM 構築支援、運用支援
- ・ 強固なセキュリティ基盤構築・運用：
インターネット分離、マネージド
セキュリティ

< 効果・評価 >

- ・ リスクアセスメントにより、強固なセキュリティ基盤構築を実現するためには何が必要か、どのように進めればよいかが明確化した。
- ・ セキュリティ専門家が社内におらず、適切な改善がタイムリーにできるかという不安も、BBSec をパートナーとして活用していくことで、解決できることがわかった。

セキュリティリスクの高い ビジネスモデルを防御する

情報通信業界の大手である同社は、主力となるインターネット調査などの調査手法そのものが情報漏えいリスクが高いことを自ら意識し、セキュリティ強化への指針をたてた。通常業務が忙しく、専任担当者を配置することができない社内事情の中、BBSec のサポートでそれを補完し、アンケートに答える消費者、その情報を必要とする企業双方に安心を提供している。

目的：情報セキュリティ体制全体の整備とシステム堅牢化

< BBSec のソリューション >

- ・ システムの堅牢化：ハードニングコンサルティング
- ・ 開発技術の強化：セキュア開発コンサルティング
- ・ 規程・ガイドラインの精度向上：
文書支援コンサルティング
- ・ 情報管理手法の検討：
個人データに関するコンサルティング
- ・ 運用リスク回避のための情報源：
脆弱性情報提供
- ・ 強固なセキュリティ基盤構築・運用：
マネージドセキュリティ

< 効果・評価 >

- ・ セキュア開発やインフラ運用など情報部門のセキュリティ体制が整備され、さらに Web サイトの保護も実現できた。
- ・ 迅速な対応に、高い評価をいただいた。
- ・ 今後、さらなる体制の強化を順次、実現していく予定。

インシデント発生時の 情報共有を迅速に

総合エンターテインメント企業である同社は、多数あるグループ会社のセキュリティ強化に乗り出した。自社のセキュリティ基盤を盤石なものにすると同時に、組織横断的なセキュリティ対策の文化を定着させるために CSIRT を構築。現在、多数のグループ企業を束ねる CSIRT は、地道な努力で効果を発揮している。

目的：多数のグループ企業と経営層をつなげる CSIRT の構築

< BBSec のソリューション >

- ・ インシデント対応：緊急対応
- ・ 効果的な対策の模索：セキュリティアドバイザリ
- ・ Web システム強化：脆弱性診断
- ・ 強固なセキュリティ基盤構築・運用：マネージドセキュリティ
- ・ ログ管理体制構築・運用：SIEM 構築支援
- ・ 社内防衛体制の整備：CSIRT 構築コンサルティング
- ・ 事務所のセキュリティ設計：オフィス環境コンサルティング

< 効果・評価 >

- ・ 組織を越えた Face to Face のコミュニケーションを強化することで、インシデント発生時の情報共有が迅速化した。また、所属社員が、日々の行動の中で不安を感じた時にすぐに相談してくれるようになり、大規模インシデントの予防にもつながっている。
- ・ チケット制による無駄のないコンサルティング提案は、当社にとって好都合だった。

安全なクラウド活用を 実現する

専門商社である同社は、システムの最適化をめざしクラウドを利用していたが、昨今話題となっているクラウド経由のウィルス侵入を発見し、さらなるセキュリティ強化へと舵を切った。まず社内に残るウィルスを排除し、続いてシステムのセキュリティ対策の可視化とインシデント発生時の対応策を、BBSecと共に再構築した。

目的：インシデントの原因特定、再発防止策の構築

< BBSec のソリューション >

- ・ 現状の可視化：リスクアセスメント
- ・ IT 環境評価：Active Directory 環境評価
- ・ ログ管理体制構築：
セキュリティログコンサルティング

< 効果・評価 >

- ・ リスクアセスメントにより、今まで行ってきた対策だけでは、気づけていないリスクがあることを認識することができた。
- ・ セキュリティ対策をどこまで実装すれば適切なのか迷っていたが、BBSec のアドバイスにより、実施すべきアクションを明確化できた。
- ・ BBSec のセキュリティ専門ベンダーとしての高度な助言は、大変役に立った。

自社の特許技術を セキュリティ対策で守る

電子部品の製造 / 販売を世界規模で展開する同社は、自社の最大の資産である特許技術をサイバー攻撃から守る必要に迫られていた。形骸化したセキュリティポリシーの刷新と全社的なセキュリティ基盤の強化に取り組み必要があったが、その具体的な進め方が分からず、BBSecの専門的なアドバイスを必要とした。

目的：全社的なセキュリティ基盤の強化

< BBSec のソリューション >

- ・ 社員のセキュリティ能力判定・啓蒙：
標的型攻撃メール訓練
- ・ 規程・ガイドラインの精度向上：
セキュリティポリシー / ルール文書支援
コンサルティング
- ・ 効果的な対策の模索：
セキュリティアドバイザリ

< 効果・評価 >

- ・ ポリシー作成に係る具体的な進め方を確認でき、実態のあるポリシーを作り上げることができた。
- ・ 当社の事情をご理解いただきながら最適なアドバイスを提供してくれた。
- ・ 今後、作成されたポリシーを効果的に社内展開していきたい。

卸売

自社ブランド維持の為に、 第三者の専門的視点を取り入れる

食品関連の卸売企業である同社は、自社ネットワークのリニューアルにあたり、現行のリスクを洗い出すことによって、よりセキュアなネットワークを構築しようと考えた。リスクの洗い出しは社内でも行えるが、思い込みによる見逃しが発生する可能性も高く、第三者の専門的視点によるチェックをBBSecに依頼した。

目的：全社的なセキュリティ基盤の強化

< BBSec のソリューション >

- ・ 社員のセキュリティ能力判定・啓蒙：
標的型攻撃メール訓練
- ・ 現状の可視化：リスクアセスメント

< 効果・評価 >

- ・ リスクの可視化により、再設計時に考慮すべき点が明確となった。
- ・ BBSec の第三者の視点によるリスクアセスメントは高品質との評価をいただいた。
- ・ 今後、可視化できた課題に対応しながらネットワークのリニューアルを進めていく。

常にお客様から求められる セキュリティの信頼性を高める

インターネットビジネスのソリューションカンパニーである同社は、インターネット経由で収集されたデータを分析するビジネスモデルの信頼性をより高めるために、セキュリティ対策の強化にのりだした。当初はその重要性を把握できずにいた経営陣への BBSec による丁寧な説明は、全社をあげての対策の大きな後押しとなった。

目的：企業信頼性向上につながるセキュリティ体制強化

< BBSec のソリューション >

- ・ 現状の可視化：リスクアセスメント
- ・ 規程・ガイドラインの精度向上：
文書支援コンサルティング
- ・ 効果的な対策の模索：
セキュリティアドバイザリ

< 効果・評価 >

- ・ 自社が抱えるセキュリティリスクの洗い出しができ、今後、何を解決していけばよいか明確になった。
- ・ BBSec のコンサルタントには大きな信頼を寄せている。

多拠点のセキュリティリスクを 正確に把握する

全国規模でシステムを運用する同社は、各所に点在する事業所にも本社同様のセキュリティ対策を絶えず指導してきた。しかし、他社同様、各所でどの程度セキュリティ対策が取られているかは、正確に把握できずに困っていた。そこで、同社はセキュリティの専門会社である BBSec にその調査を依頼することで、全社規模のサイバーリスクを把握しようと考えた。

目的：全国に分散する地方拠点のサイバーリスク把握

< BBSec のソリューション >

- ・ 情報管理の基礎データ構築：情報資産棚卸調査
- ・ 現状の可視化：情報資産リスク評価

< 効果・評価 >

- ・ スピード感を持った対応とレポートの品質に高い評価をいただいた。
- ・ 今後、可視化されたリスクへの対策を順次進め、セキュリティリスクを軽減していく。
- ・ 加えて、情報資産とそのリスクは常に変動するため、継続的な棚卸とリスク評価を実施していき、サプライチェーン全体への拡大も検討していきたい。

製造

海外拠点の現状を 第三者の視点で確認する

世界を舞台に活躍する医療機器の製造・販売の国内大手企業である同社は、多数ある同社の海外拠点でのポリシー準拠状況を把握したいと考え、手始めに代表的な複数拠点を第三者の視点から調査するため、BBSec にアセスメントを依頼した。同社は単に調査だけでなく、拠点訪問時に拠点での啓蒙活動もあわせて希望した。

目的：海外拠点のセキュリティ対策可視化と啓蒙

< BBSec のソリューション >

- ・ 海外拠点のセキュリティ対策可視化：海外拠点調査

< 効果・評価 >

- ・ 本社から把握することが難しい現地法人の実態と課題を把握することができた。
- ・ PCIDSS に関する高い知見に評価を得た。
- ・ 海外調査には欠かせない、英語を中心とした高い語学力に評価を頂いた。
- ・ 今後、調査結果をもとに、自社でレベルアップをめざすと共に、定期的に専門家によるチェックを受けていきたい。

世界中に広がる拠点で、 セキュリティ基準に準拠する

大手通信キャリアである同社は、自社サービスのセキュリティレベルの維持及び取引先への表明のため、定期的なセキュリティ監査を必要とした。しかし組織としての規模があまりに大きく、さらに各国の異なる統制への適合と組織が決めた統一基準との埋められない乖離があり、どこをめざしていくべきか悩んでいた。

目的：海外拠点のセキュリティ・スタンダードへの準拠

< BBSec のソリューション >

- ・ セキュリティ認証取得：
海外のデータセンターにおける PCI DSS 準拠支援コンサルティングおよびオンサイト評価
- ・ セキュリティ認証取得：
グローバルに展開するクラウドサービスの PCI DSS 準拠支援コンサルティングおよびオンサイト評価
- ・ セキュリティ内部監査支援：
海外拠点に対する ISO 27001 準拠状況確認など、内部監査を支援

< 効果・評価 >

- ・ 海外拠点への訪問監査の日程調整に柔軟に対応頂き、オンスケジュールで監査を完了した。
- ・ 自社の内部監査では気づかないリスクが発見され、業務改善を図ることができた。
- ・ コンサルティングにおいて PCI DSS 準拠スコープの明確化、縮小化を指導してくれた。
- ・ PCI DSS が求める要件の理解度が向上し、自社のセキュリティ向上に繋げることが出来た。

主なコンサルティング例

組織を守るためのセキュリティ対策の実現 / 維持を、お客様の組織の状況にあわせて可能となるよう、専門的なアドバイスを行っています。下記の例に限らず様々なご要望に対応していますので、是非ご相談ください。

効果的な対策の模索

- セキュリティアドバイザー

セキュリティ対策の推進方法や優先順位など、お客様社内の体制にあわせた提案ならびに推進支援を行います。

現状の可視化 / 調査

- リスクアセスメント
- 制御系システムリスクアセスメント
- 情報資産棚卸調査 / リスク評価
- 標的型攻撃メール訓練
- 国内支社 / 海外拠点のセキュリティ対策調査
- データマッピングコンサルティング

セキュリティ対策の第一歩は、現状を正しく把握することです。BBSec の可視化 / 調査コンサルティングサービスは、専門家の視点から現状を可視化し、今後の対策についてのアドバイスを行います。

セキュリティルール策定

- セキュリティポリシー / 規程 / ガイドライン 文書支援
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

組織としての姿勢や行動規範をつかさどる各種セキュリティルールの策定を専門家の立場からアドバイスいたします。

社内体制構築

- CSIRT 構築コンサルティング
- インシデント対応計画策定支援
- 個人データ管理に関するコンサルティング

情報システム部門の枠を超えるセキュリティ対策 / インシデントへの対策立案や運営ノウハウをわかりやすくサポートします。

情報システムのセキュリティ対策強化

- システムハードニングコンサルティング
- セキュリティログコンサルティング
- SIEM 構築支援、運用支援
- セキュア運用支援（インターネット分離、マネージドセキュリティ 他）

堅牢な情報システムを構築 / 運用するためのシステム構築手法や運用支援を行います。

セキュリティ認証取得 / 準拠

- PCI 準拠 / 維持支援
- クレジットカード加盟店の情報非保持化コンサルティング
- FISC 準拠アセスメント / FISC 文書支援
- 国内 / 海外拠点のセキュリティ認証取得 / オンサイト評価 / 内部監査

自社のセキュリティ対策を組織の評価へとつなげる各種セキュリティ認証取得 / 準拠をお手伝いいたします。さらに、状況把握が難しい海外を含む支店や関連事業者の調査も行っています。

オフィスのセキュリティ対策

- オフィスのセキュリティ設計コンサルティング
- 無線 LAN 調査サービス

安全が確保されるべきオフィスのセキュリティ対策を支援しています。

