BIPROGY

iSECURE サイバーセキュリティ®

BIPROGY セキュリティソリューション

Foresight in sight

システムインテグレーターとして培ってきた知識や経験を生かし、企業や業種にあわせたバランスの良いセキュリティ対策を提案します。

サイバー攻撃による被害は大きくなり、 セキュリティ対策は経営上の重要な課題のひとつとなりました。またIoTやクラウドの普及などにより、新しい脅威が台頭しています。いまやセキュリティ対策は、システムの防御策だけではなく、サイバー攻撃を受けた後の対策も必要です。そのためには、インシデント発生時の対応・復旧まで視野に入れた体制作りが必須です。金融機関をはじめ、幅広い業界でセキュリティ対策に従事してきたBIPROGYが、ビジネスや業態に合わせて、適切なセキュリティ対策をワンストップで提案します。

サイバーリスクとセキュリティ対策のポイント

サイバーセキュリティのリスクは、企業経営にさまざまな悪影響を及ぼします。

- 標的型攻撃
- 内部不正
- ランサムウエア
- Webサイト改ざん
- 未知の脆弱性攻撃
- DDoS攻撃

常に変化し、多様化するサイバー攻撃に備え、セキュリティを経営課題として捉え取り組む必要があります。

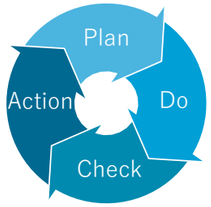
BIPROGYの考えるセキュリティの重要ポイント

- 多層防御によるサイバー攻撃対策
- インシデントへの迅速な検知と対応
- 脆弱性情報の収集と対応
- マネジメントシステムによる継続的な運用

セキュリティ対策のポイントは、複雑に絡み合い、連携して機能します。
バランスよくマネジメントし、維持・改善していくことが重要となります。

2つの対策アプローチとサービスの全体像

セキュリティ管理の強化



現状のセキュリティ状況を把握し、体制や規程類の整備をすることにより、PDCAサイクルを回します。

セキュリティサービス

BIPROGYグループのセキュリティサービスでは、現状のセキュリティ実装・運用の評価、見直しなど、さまざまな角度からセキュリティに関する課題解決を支援します。

企業におけるセキュリティ課題

セキュリティ対策や運用において、過不足や見直すべき部分が、あるかどうか分からない。	アセスメント
セキュリティ事故が発生した際に対応する体制や経験がなく、迅速な対応ができるか不安である。	CSIRT構築支援
既存のポリシーは、会社の実情や最新セキュリティ動向に即していないため、形骸化している。	ポリシー見直し支援
多様化・複雑化する攻撃手法に対して脆弱性の有無が気になる。	脆弱性診断
クレジットカード情報を取り扱うシステムにおいて、どの範囲にどこまで対策を行えば良いか分からない。	PCI DSS準拠支援

iSECURE コンサルティング サービス

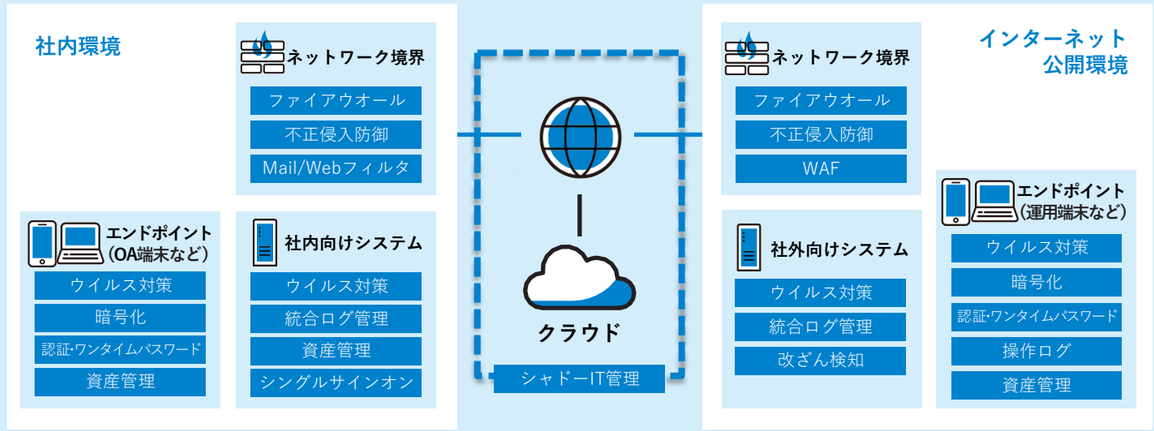
セキュリティ実装・運用の強化

サイバー攻撃に対してシステムを防御するだけでなく、事前の準備、平常時の活動、インシデント発生を想定した対策が重要です。

特定	防御	検知	対応	復旧
事前にシステム・情報資産を評価し、リスクを特定する。	サイバー攻撃などに対して適切なセキュリティ対策で防御する。	情報の漏えいやサイバー攻撃、侵入などを素早く検知する。	発生したインシデントにいち早く対応し、被害を最小に抑える。	システムを復旧させ、インシデントの原因を探り、改善につなげる。

セキュリティプロダクト

BIPROGYグループでは、さまざまなセキュリティ要件に対応可能なセキュリティプロダクトを提供します。



商品ラインナップ

セキュリティサービス

分類	サービス名称	サービス内容
コンサルティング	アセスメント	サイバー攻撃に対するセキュリティ対策状況を分析・評価
	アドバイザリー	最新のサイバーセキュリティ動向に関する情報提供や、お客さまからお問い合わせいただいたサイバーセキュリティに関する質疑に回答
	ポリシー見直し支援	既存セキュリティポリシーの各文書を見直す際に助言・提言を行い、セキュリティポリシーの改善を支援
	PCI DSS準拠支援	クレジットカード情報を保存・処理・通過するシステムを、PCI DSSへ準拠させるための支援
	CSIRT構築支援	実効性のあるCSIRTを立ち上げるための計画立案から体制整備や関連ドキュメント策定などを支援
脆弱性診断	プラットフォーム診断	プラットフォームにおける既知の脆弱性の有無や不適切なシステム設定などを確認し、対策方法をあわせて報告
	Webアプリケーション診断	Webアプリケーションの脆弱性を検出し、対策方法をあわせて報告
運用	マネージド・セキュリティ・サービス	組織のセキュリティ担当者が継続的に実施すべきセキュリティ運用を支援

セキュリティプロダクト

分類	機能概要
認証強化	PCのログオン認証をICカードや指紋などにより強化
	リモートアクセス時の認証をワンタイムパスワードにより強化
アクセス制御	許可されていないトラフィック、不正侵入を試みるトラフィックを遮断
	インターネット接続先（URL)の制限と記録
	Webアプリケーションの脆弱性を狙ったトラフィックを遮断
	不正なデータベースへのリクエストを遮断
	広告・勧誘などの迷惑メールを遮断
データ保護	USBメモリーなどの外部記録媒体に対する使用制限
	モバイルPCの紛失・盗難時における情報漏えいリスクを低減するために、 HDD暗号化
	データの改ざんを検知

分類	機能概要
不正プログラム対策	PCやサーバーに侵入した不正プログラムを駆除
	ネットワーク経路上で不正プログラムを含むトラフィックを遮断
	OSやミドルウエアなどのソフトウエアの脆弱性を狙ったトラフィックを遮断
	内部ネットワークに侵入した不正プログラムによる不審なトラフィックを検出
	不正プログラムに感染したPCなどから出力される攻撃パケットの遮断
認証連携	複数の社内システムなどをシングルサインオンによって認証連携
	複数のクラウドサービスをシングルサインオンによって認証連携
証跡管理	OA端末の操作ログ取得（実行したプログラム、メールへのファイル添付など）
	運用管理端末の操作ログ取得（操作画面の録画）
リモート接続	インターネットVPNを利用した社内システムへのセキュアなリモート接続

BIPROGY株式会社

本社　〒135-8560
東京都江東区豊洲1-1-1
電話　03-5546-4111（大代表）

最新情報・導入のご相談は
Webサイトもご覧ください

●お問い合わせ先

お問い合わせは、下記お問い合わせフォームよりお願い致します。
https://pr.biprogy.com/inqsys/inquiry_form.html?product_id=1184

https://pr.biprogy.com/solution/tec/security/

090001113-1 2210