Webサイト管理者が知っておくべき20のセキュリティチェックポイント

株式会社サイバーセキュリティクラウド

目次

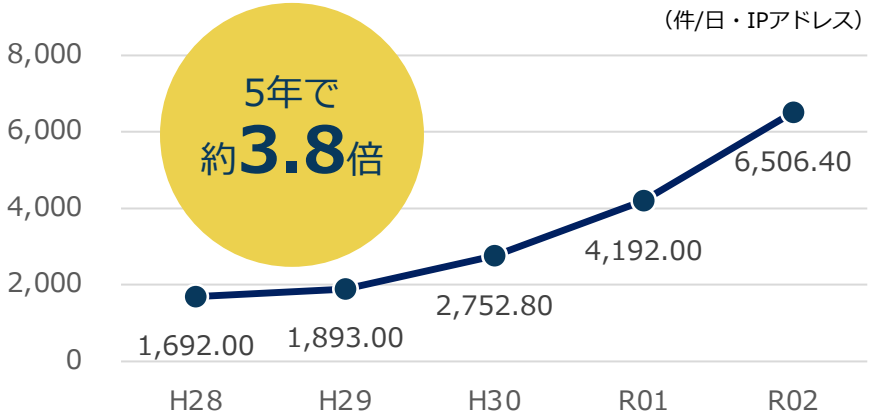
本資料は、IPA(独立行政法人情報処理推進機構）の「安全なウェブサイトの運用管理に向けての20ヶ条 ～セキュリティ対策のチェックポイント～」をもとに構成しています。（URL：https://www.ipa.go.jp/security/vuln/websitecheck.html）

増加するサイバー攻撃

最近ますます、サイバー攻撃という言葉を、さまざまなところで耳にするようになりました。ニュースでも、国内外問わずサイバー攻撃の影響で業務が停止してしまったり、多額の金額が要求されたりと言った事例を多く耳にしていると思います。
警察庁が集約・分析をしているデータをみると、サイバー攻撃やネットワークに接続された機器の脆弱性を探索する準備行為の数は、年々増えていることが分かります。実際にサイバー犯罪の検挙件数も増加しています。

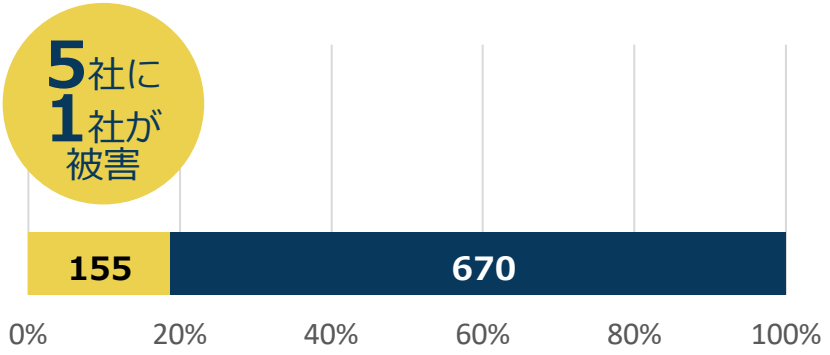
サイバー攻撃は、大手企業だけの問題ではありません。特に近年は大手企業のセキュリティ対策が強固なため、比較的セキュリティ対策が甘い中小企業を狙った攻撃も増えています。
一般社団法人 日本損害保険協会の「「中小企業の経営者のサイバーリスク意識調査2019」によると、中小企業の経営者の約2割が何らかのサイバー攻撃の被害にあったと回答しています。

インターネットとの接続点に設置したセンサーで検知したアクセス件数の推移



※出典：警視庁「令和２年におけるサイバー空間をめぐる脅威の情勢等について」

中小企業経営者がサイバー攻撃の被害にあった割合
(n=825)

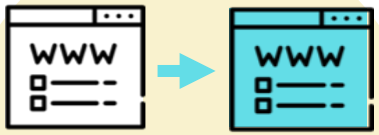


※出典：一般社団法人 日本損害保険協会
「中小企業経営者の意識調査2019｜サイバー保険｜日本損害保険協会」

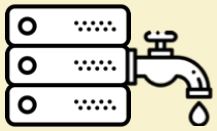
2 サイバー攻撃による被害

実際にサイバー攻撃を受けたときに、どのような被害が考えられるでしょうか？
すぐに思いつくのは、「Webサイト改ざん」や「情報漏えい」などの直接的な被害ではないでしょうか？しかし、実際に被害が起きると**「ブランドイメージの毀損」や「株価の下落」など**の間接的な被害も多く、対応範囲は想像以上のものになります。JNSA（NPO法人日本ネットワークセキュリティ協会）の「インシデント損害額調査レポート　2021年版」では、サイバー攻撃にあった場合の損害額のモデルケースが3例紹介されています。その被害額例は、600万円～3億7,600万円となっていて、サイバー攻撃がどのくらい大きな被害を与えるかが分かります。
このような被害に遭わないためにも、ぜひ次ページからのWebサイトセキュリティチェックを行い、対応できてないところがあれば早急に改善をし、安全なWebサイトを運用に活用ください。

直接的な被害例



Webサイト改ざん



情報漏えい

間接的な被害例

被害状況
調査費用

問い合わせ
窓口設置費用

損害賠償費用

売上機会の
損失

ブランド
イメージの毀損

株価の下落

株主代表訴訟

大規模なマルウェア感染の損害額例

被害額
3億7,600万円

内訳

費用損害（事故対応損害）	
事故原因・被害範囲調査費用	1億円
従業員端末等の入替え費用	1.42億円
再発防止費用	0.5億円
利益損害	0.84億円

※出典： JNSA（NPO法人日本ネットワークセキュリティ協会）「インシデント損害額調査レポート　2021年版」

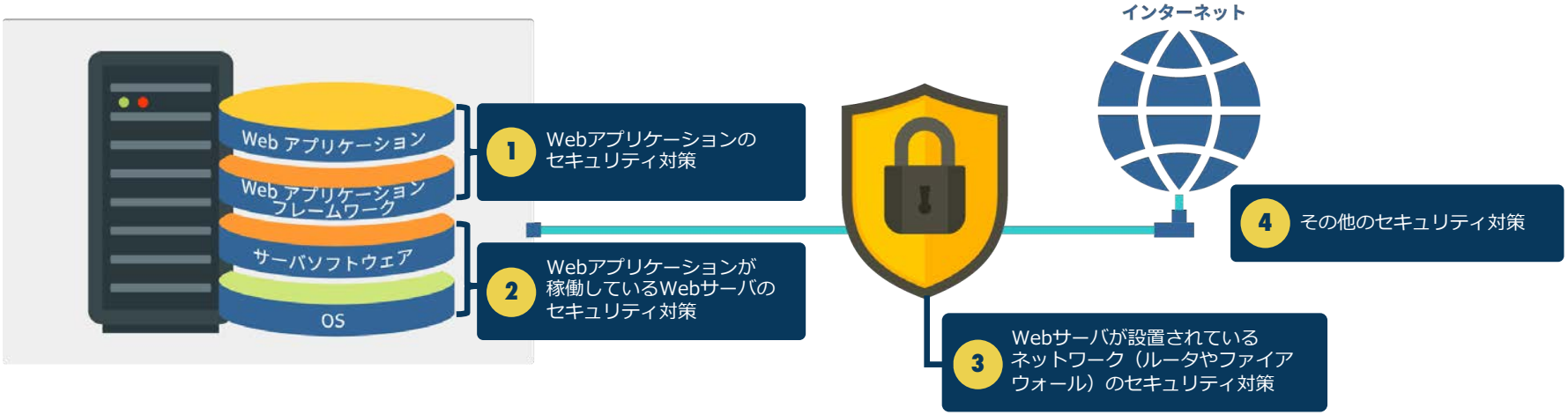
Webサイトのセキュリティ対策チェックポイント

Webサイトを安全に管理するためには、4つの分野の20のポイントをチェックすることがはじめの一歩です。
4つの分野は、以下の通りです。

1) Webアプリケーションのセキュリティ対策
2) Webアプリケーションが稼働しているWebサーバのセキュリティ対策
3) Webサーバが設置されているネットワーク（ルータやファイアウォール）のセキュリティ対策
4) その他のセキュリティ対策

このポイントの中には、Webサイト運営を外部に発注していてWebサイト管理者の方だけでは分からない箇所もあると思いますが、その場合は、委託先に確認するようにしましょう。

万が一、サイバー攻撃の被害にあった場合、発注者側の要求事項にセキュリティについての記載がなかったため、Webサイトの開発会社ではなく発注者側に責任が認められたケースもあります。Webサイト管理者の方も開発会社に任せきりではなく、このチェックリストを使って安全なWebサイトを運営しましょう。



4 Webサイトのセキュリティ対策 20のチェックリスト

Webアプリケーションのセキュリティ対策

01	公開すべきでないファイルを公開してないか？	☐
02	不要になったページやWebサイトを公開のままにしていないか？	☐
03	Webサイトの脆弱性へ対策を実施しているか？	☐
04	Webアプリケーションを構成しているソフトウェアの脆弱性対策を定期的にしているか？	☐
05	不必要なエラーメッセージを返していないか？	☐
06	Webアプリケーションのログを保管し、定期的に確認しているか？	☐
07	インターネットを介して送受信する通信内容の暗号化はできているか？	☐
08	不正ログインの対策ができているか？	☐

Webアプリケーションが稼働しているWebサーバのセキュリティ対策

09	OSやサーバソフトウェア、ミドルウェアをバージョンアップしているか？	☐
10	不要なサービスやアプリケーションがないか？	☐
11	不要なアカウントが登録されていないか？	☐
12	推測されやすい単純なパスワードを使用していないか？	☐
13	ファイル、ディレクトリへの適切なアクセス制御をしているか？	☐
14	Webサーバのログを保管し、定期的に確認しているか？	☐

Webサーバが設置されているネットワーク（ルータやファイアウォール）のセキュリティ対策

15	ルータなどを使用してネットワークの境界で不要な通信を遮断しているか？	☐
16	ファイアウォールを使用して、適切に通信をフィルタリングしているか？	☐
17	Webサーバ（または、Webアプリケーション）への不正な通信を検知または、遮断しているか？	☐
18	ネットワーク機器のログを保管し、定期的に確認しているか？	☐

その他のセキュリティ対策

19	クラウドなどのサービス利用で、自組織の責任範囲を把握し、必要な対策ができているか?	☐
20	定期的にセキュリティ検査（診断）、監査をしているか？	☐

Webサイトのセキュリティ対策 20のチェックリスト

前ページのチェックリストの20の項目すべてにチェックが付いたでしょうか？
もし、チェックを付けることができなかったり、不明な点があったりした場合は、次のページからの各項目の解説を読んで対応を行いましょう。

また、Webサイトは常に更新や新規コンテンツの追加をしていると思いますので、このチェックは1回だけ行って終わりにするのではなく、定期的にチェックを行いましょう。

5 Webアプリケーションのセキュリティ対策

Check 01 公開すべきでないファイルを公開してないか？

設定ファイルや個人情報などの重要な情報を格納したファイルは公開すべきものではありません。このようなファイルは、インターネット上からアクセスできない場所に保管しましょう。不要なファイルは削除する必要があります。

ファイルを誤って公開していた場合は、非公開にするだけではなく、検索エンジンのキャッシュに残っていないかの確認も必要です。

Check 02 不要になったページやWebサイトを公開のままにしていないか？

期間限定のキャンペーンページや不要になったWebサイトやページを公開したまま放置していると、管理者が変わったときに忘れられて管理されなくなる恐れがあります。脆弱性が発覚したときに、忘れられたページまで対応ができず、そのページからサイバー攻撃の被害にあうことが考えられます。

不要なページやWebサイトは閉鎖しましょう。

Check 03 Webサイトの脆弱性へ対策を実施しているか？

Webサイト開発時には、サイバー攻撃対策への考慮が非常に重要です。特に顧客情報を入力するフォームがある場合は要注意です。

具体的には、IPA（独立行政法人情報処理推進機構）が公表している「安全なウェブサイトの作り方」を参考に対策が実施されているか確認してください。

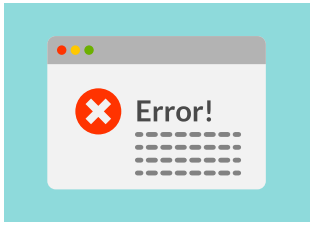
Check 04 Webアプリケーションを構成しているソフトウェアの脆弱性対策を定期的にしているか？

Webアプリケーションは様々なソフトウェアやフレームワーク、CMS等で構成されています。これらのソフトウェアに脆弱性が発見された場合、適宜バージョンアップ等の対策が必要です。そのため、Webサイトがどのようなソフトウェアで作られているか把握して脆弱性対策をとる必要があります。

Webアプリケーションのセキュリティ対策

Check 05 不必要なエラーメッセージを返していないか？

Webアプリケーションのエラーメッセージから、ウェブサイトの設定情報などが漏えいし、攻撃に悪用されることがあります。攻撃者に余計な情報を与えないためにも、エラーメッセージの内容は必要最低限にする必要があります。



Check 06 Webアプリケーションのログを保管し、定期的に確認しているか？

ログは、事故や故障、不正アクセス等の不審な動きがあった際に、原因を追究するための重要な情報源です。必要に応じてログを保管し、定期的に確認をしましょう。

Check 07 インターネットを介して送受信する通信内容の暗号化はできているか？

Webアプリケーションと利用者の間で交わされる通信は、盗聴や改ざん、なりすましなどの被害を受ける恐れがあります。しかし、通信内容を暗号化（HTTPS化）すれば、仮に盗聴などの被害を受けても重要情報が不正に取得されることを防止できます。

Check 08 不正ログインの対策ができているか？

漏えいしたIDやパスワードを悪用した不正ログインにより、情報漏えいや金銭被害などが生じる恐れがあります。
利用者に対して、「複雑で推測されにくいパスワードを設定する」「パスワードを使いまわさない」等の対策をアナウンスするとともに、不正ログインを防止したり検知したりするためのシステム面の対策も有効です。

Webサーバのセキュリティ対策

Check 09 OSやサーバソフトウェア、ミドルウェアをバージョンアップしているか？

OSやサーバソフトウェア、ミドルウェアのバージョンアップは、セキュリティ対策の基本です。修正プログラムが公表された際は適用し、脆弱性を解消してください。

Check 10 不要なサービスやアプリケーションがないか？

Webサーバ上で不要なサービスが起動している悪用される可能性があります。最低限必要なもの以外は、停止してリスクを回避しましょう。古いバージョンのアプリケーションの脆弱性を攻撃される恐れがあるため、不要になったアプリケーションも削除してください。

Check 11 不要なアカウントが登録されていないか？

Webサーバのアカウントに不要なアカウントはありませんか？アカウント一覧を作成し、最低限必要なもの以外は削除しましょう。
特にテスト用に作成したアカウントが残っているケースがあります。

Check 12 推測されやすい単純なパスワードを使用していないか？

推測されやすいパスワードを設定している場合、悪用される可能性が高まります。推測されにくい複雑なパスワードを設定・使用してください。

Check 13 ファイル、ディレクトリへの適切なアクセス制御をしているか？

Webサーバ上のファイル、ディレクトリに適切なアクセス制御がされていない場合、第三者に非公開のファイルを見られたり、プログラムが実行されたりする可能性があります。

Check 14 Webサーバのログを保管し、定期的に確認しているか？

Webサーバ上では各種ログファイル（「システムログ」「アプリケーションログ」「アクセスログ」「データベース操作ログ」など）があります。これらのログファイルを確認することにより、事故や故障、不審な動きがあったことに気づくきっかけになります。

7 ネットワークのセキュリティ対策

Check 15 ルータなどを使用してネットワークの境界で不要な通信を遮断しているか？

境界ルータなどのネットワーク機器を使用して、外部から内部ネットワークへの不要な通信は遮断してください。
運用上、外部から内部ネットワークへに通信が必要な場合は、情報を秘匿するためVPN 等を利用することを検討してください。内部に侵入された場合、悪用される恐れがあるため、内部から内部ネットワークおよび内部から外部ネットワークについても、不要と判断される通信は遮断する必要があります。

Check 16 ファイアウォールを使用して、適切に通信をフィルタリングしているか？

ファイアウォールを設置していても、フィルタリングが適切でなければ意味がありません。「どのサーバ」の「どのサービス」に「どこから」のアクセスを許可するのかを把握し、設定を見直してください。

Check 17 Webサーバ（または、Webアプリケーション）への不正な通信を検知または、遮断しているか？

IDSやIPS、WAF（ワフ）は、Webサイトと利用者の間の通信を検査し、不正な通信を自動的に検知または遮断するソフトウェア、もしくはハードウェアです。
ウェブサイトに脆弱性が発見された場合、Webアプリケーションを速やかに修正できないことがあります。修正されるまでの間、攻撃による影響を低減する対策としてIDSやIPSおよびWAFを導入してウェブアプリケーションを保護することは有効な手段の一つです。

Check 18 ネットワーク機器のログを保管し、定期的に確認しているか？

ログは、事故や故障、不審な動きがあった際に原因を追究するための重要な情報源です。必要に応じてログを保管し、定期的に確認をする必要があります。

8 その他のセキュリティ対策

Check 19 クラウドなどのサービス利用で、自組織の責任範囲を把握し、必要な対策ができているか？

クラウドやホスティングのサービスを利用してウェブサイトを運営している場合、1～18, 20のチェックポイントで記述したセキュリティ対策をサービス事業者側が提供していることがあります。クラウドなどのサービスを利用する場合は、サービス事業者側の作業範囲とセキュリティ対策を把握し、不足する対策は自組織で対応することを検討してください。

AWSでは、この責任範囲を「責任共有モデル」と定義し、サービス提供者の責任を「クラウド**の**セキュリティ」、サービス利用者の責任を「クラウド**における**セキュリティ」としています。AWSのIaaSを利用する場合、サービス提供者のAWSはセキュリティグループとしてファイアウォールの機能を提供しますが、ファイアウォールの構成自体はサービス利用者が責任を負う範囲です。

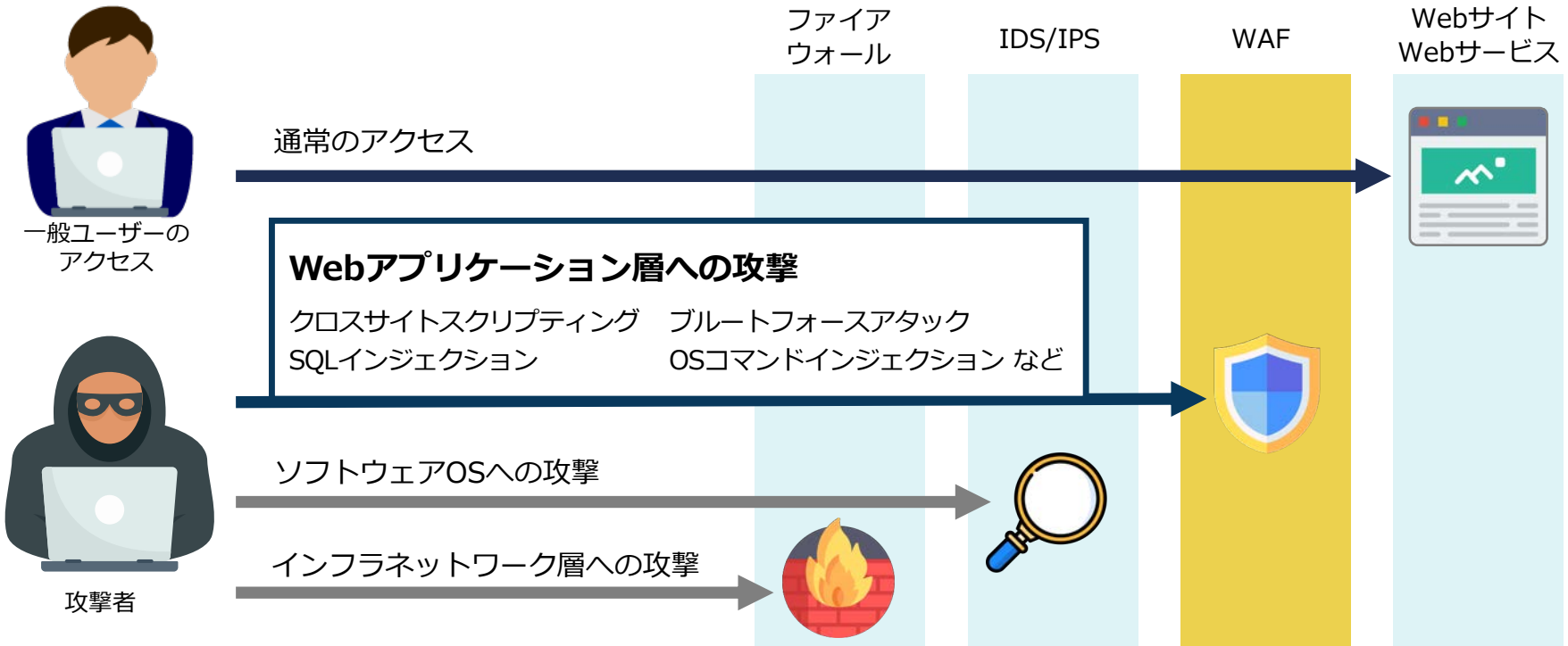
Check 20 定期的にセキュリティ検査（診断）、監査をしているか？

組織内部で1～19までのセキュリティ対策を実施しているか確認した上で、外部の組織によるサーバやネットワーク機器、Webアプリケーションに対する脆弱性検査（診断）やセキュリティ監査を受けることは、対策漏れなどを洗い出すために効果的な手段です。

公開時だけではなく、運用後に定期的な検査（診断）、監査を継続することが重要です。

Webアプリケーションのセキュリティ対策にはWAFが効果的

チェックポイント17で、Webアプリケーションのセキュリティ対策の１つとしてWAF（ワフ）を取り上げました。
このWAFは、従来のファイアウォールやIDS/IPSでは防ぐことができない**不正な攻撃からWebアプリケーションを防御**するファイアウォールです。ファイアウォール、IDS/IPSとともにWAFを組み合わせることで、さまざまなサイバー攻撃に有効な高セキュリティな環境を実現することができます。
Webサイトのセキュリティ対策強化としてWAFを導入することは非常に効果的です。



クラウド型WAF「攻撃遮断くん」のご案内

攻撃遮断くん

累計導入社数・
累計導入サイト数
国内No.1※

導入サイト数
15,000
サイト以上

低価格・定額制で柔軟な料金プラン

お客様の環境にあった柔軟プランを用意。
月額1万円（税別）から利用可能。

さまざまなWebシステムに導入可能

サーバにインストールするタイプとDNSを切り替えるタイプの2タイプがあるので、お客様の環境に合わせて導入可能。

運用はおまかせ！サポートも充実

運用はおまかせなので、専任の担当者は不要です。
日本発のサービスで、サポートもすべて日本語で迅速。

※ 日本マーケティングリサーチ機構調べ　調査概要：2021年10月期_指定テーマ領域における競合調査

お問い合わせ

03-6416-1579
（平日10:00～18:00）

mkt@cscloud.co.jp

https://www.shadan-kun.com/

会社概要

会社名	**株式会社サイバーセキュリティクラウド**
本社所在地	**〒150-0011 東京都渋谷区東3-9-19　VORT恵比寿maxim3階**
代表電話	**03-6416-9996**
FAX番号	**03-6416-9997**
Webサイト	**http://www.cscloud.co.jp**
事業内容	**Webセキュリティ事業**　■Webセキュリティサービスの開発・運用・保守・販売 ■サイバー攻撃対策コンサルティング