セキュリティ診断サービス
ご 案 内

CONTENTS

サイバーセキュリティの現状 P1 P2
弊社の特徴 P2
セキュリティ診断の必要性 P3
Webアプリケーション診断 P4
ネットワーク診断 P5
Q&A／被害事例 P6
会社概要 P7

CS Security チュウケイセキュリティ株式会社

サイバーセキュリティの現状

情報セキュリティ事故が発生した場合、**「業務の停止」「情報の紛失・改ざん・漏洩」**
「対策費用の増大」などの大きな直接的被害だけでなく、
「損害賠償」「公的な処罰」「社会的信用の低下」「売上の減少」などの
間接的被害も膨らみ、**企業の存亡**に関わる被害になる恐れがあります。

2016年個人情報漏洩インシデント概要データ

漏洩人数	1,396万5,227人
インシデント件数	468件
想定損害賠償総額	2,788億7,979万円
1件あたりの漏洩人数	3万1,453人
1件あたり平均想定損害賠償総額	6億2,811万円
1人あたり平均想定損害賠償総額	3万1,646円

ハッカーからの攻撃は、ハッカーレベルでなければ守れない!!

昨今の市場・現状は、以前より安全性の高い各サーバーやネットワーク機器（システム）において、
セキュリティー対策も重視される様になって参りました。

しかし

インターネットの世界は、無限の暗号が飛びかう型で構成された世界で、常に変化し、”絶対”と言う言葉が
通用しない領域まで来てしまいました。現在、国内に存在するエンジニアたちのレベルも、
まだまだ、世界中の悪いハッカー（クラッカー）には、対応できていないのも現実なのです

**今、我々が使用しているセキュリティシステムは、全てがパッケージ化されたもので
対応していますが、悪いハッカー（クラッカー）から攻撃対象と狙われれば、
いとも簡単に被害を受けてしまうレベルであることも実状なのです。**

弊社の特徴

ワンストップでサービス提供可能

診断・調査・対策をワンストップで提供できます。日々研究し**最新の攻撃手法を発見・所有**しているからこそ、最新の脆弱性の発見も可能です。

最後の砦として弊社を採用

他社に比べ、抜け漏れが少ないとクライアント様から評価いただいております。複数社で診断を行う際、最後尾**「最後の砦」**としてご相談いただくことが多くございます。

費用対効果の高さ

診断内容に費用対効果が高いと、クライアント様から評価をいただいております。同じ価格でも**把握している攻撃手法数が多い**為、診断の網羅性、深度が深く、精度が高くて早い対応が可能です。

実情・予算にあったご提案

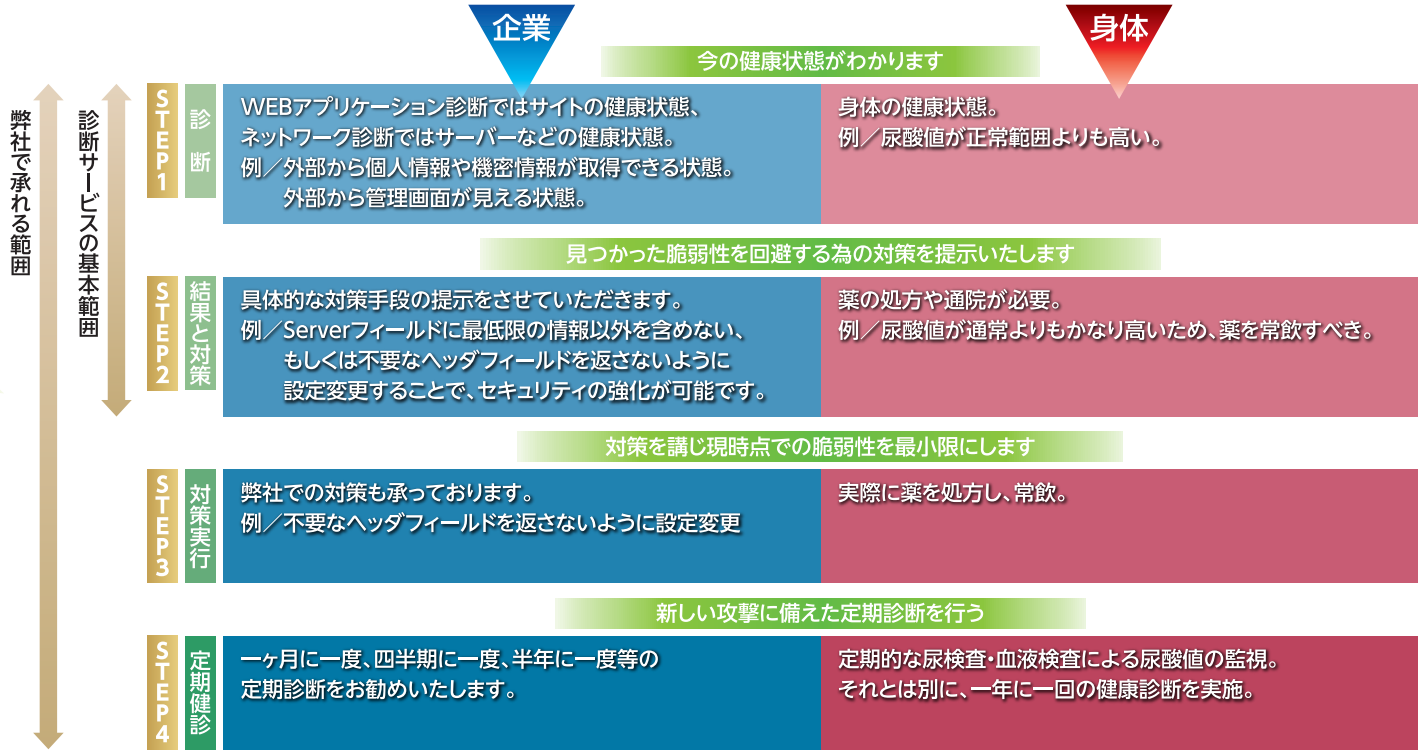
官公庁、大手企業、地方自治体から中小企業まで、様々な業態の対応を長年行っております。そのため、**実情にあった対応や対策、予算にあったご提案**が可能です。

最大の特徴は「ホワイトハッカーが守る!!」と言う事です。

セキュリティ診断の必要性

実際に侵入された脆弱なwebサイトの8割以上は、8時間以内の対応で改善可能なものが非常に多いです。
インターネット上に公開されたwebサイトは、無条件にアクセスできるため**「個人情報の流出」**や、**「機密情報の漏洩」**
「サイトにマルウェアを仕込まれることによる加害者への転換」などの様々なリスクを抱えています。
多様なセキュリティ事故を誘発させる恐れがあるだけではなく、**「企業の信頼性の失墜」**
「サービス品質の低下」「業務停止」等、企業の社会的信用や企業イメージに影響を与えます。

人の健康状態に
例えると
企業の健康状態が
見えてきます。



Webアプリケーション診断

攻撃者の視点から様々な擬似攻撃を施行し、Webアプリケーションの安全性を調査します。

調査結果には現時点での脆弱性とその対策を具体的に記載しております。

その対策を行う事により、様々な攻撃による被害の発生を未然に防ぐことができます。一般的な診断の方法として

❶ツールを利用した診断 ❷エンジニアによる手動診断 ❸1と2を併用して行う

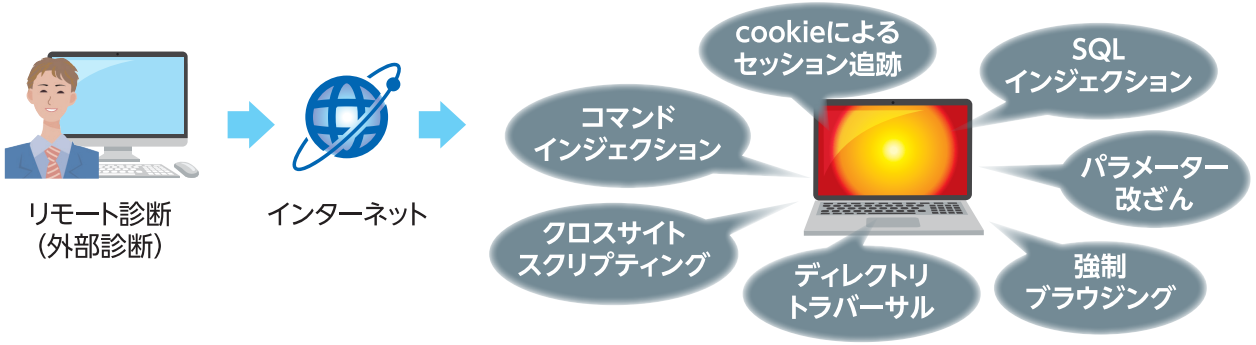
の3つがあります。お客様のご予算や考え方に合わせてご提案させていただきます。

対象となるサイトの例

- お問い合わせフォームがあり、〈顧客情報を入力するサイト〉
- お申し込みやアンケート機能などを有するサイト
- ショピングサイト
- ログインを行う会員制サイト
- 検索機能を有する情報提供サイト

診断の概要

検出された脆弱性に対して、脆弱性の原因、問題箇所、修正方法など、開発者向けの情報をまとめるだけでなく、診断結果からのリスク分析も分かりやすく報告いたします。
※オンサイト(内部診断)の診断をご希望する場合もご相談可能です。



導入までの流れ

※診断後の対策も行っております。診断レポート提出時に、内容についてもお打ち合わせさせていただきます。

STEP1 サイト確認
診断対象サイトの確認、及びヒアリングをさせていただきます。
対象サイトのご提示及び、**テスト用アカウント**の発行をお願いします。

STEP2 遷移図作成
診断対象サイトの**遷移図を作成**させていただきます。
※テストデータ等のご依頼をさせていただく場合がございます。

STEP3 ご提案
診断範囲及び診断内容の提案、及びお見積書を提出させていただきます。
診断スケジュールの調整をさせていただきます。

STEP4 お申し込み
必要事項を記載し、註文書のそうふをお願いします。
※診断開始前にテストデータを作成、FW等の設定変更を依頼する場合がございます。

STEP5 診　断
診断実行中に重大な脆弱性が発覚した場合は、**速報にて通知**します。
※診断中にテストアカウント等の準備をご依頼する場合がございます。

STEP6 レポート
診断完了後、約5営業日以内に診断報告書を提出させていただきます。
※オプションにて報告会も実施させていただきます。

ネットワーク診断

サーバやネットワーク機器に対して、不正アクセスによって侵入ができる調査結果には、
現時点での脆弱性とその対策を具体的に記載しております。その対策を行う事により、
侵入、改ざん、情報漏洩などの被害の発生を未然に防ぐことができます。
導入時に安全に構築されたサーバやネットワーク機器であっても、時間の経過とともにOS、またはミドルウェア等に
脆弱性が見つかったり、構成変更、設定変更により脆弱性が生まれてしまう恐れがあります。

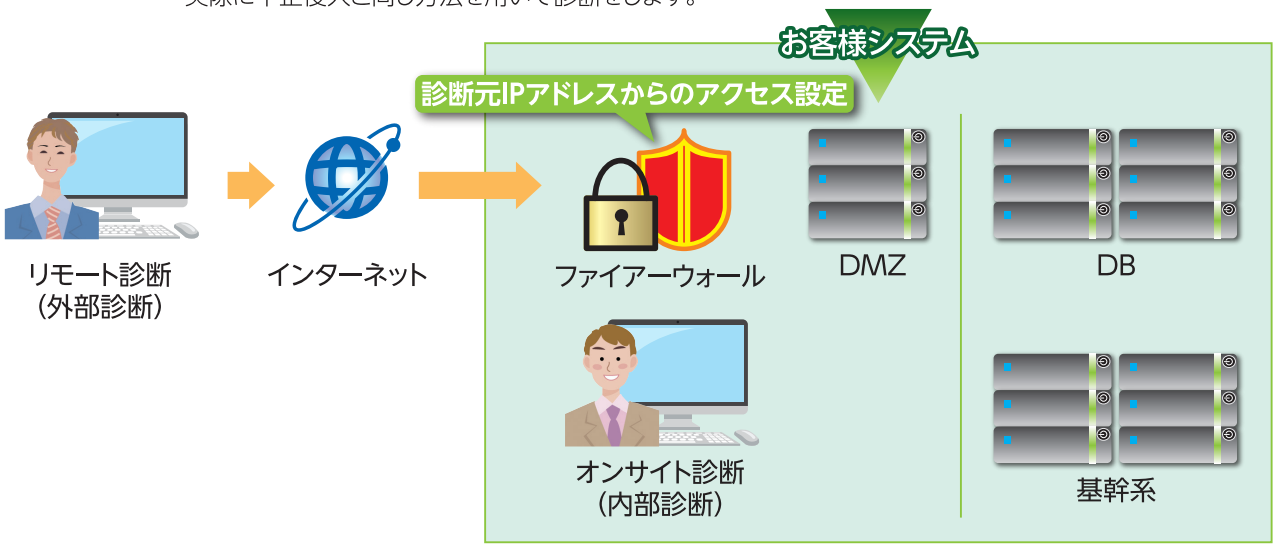
対象となるサイトの例

- Webサーバー、メールサーバー、
  ファイアーウォールなどの
  公開型システム、
  以上のいずれが該当するかを
  試行し、安全性を調査します。

診断の概要

専門のエンジニアがサーバー、ネットワーク機器の脆弱性及び、
セキュリティ対策（パッチ適用、パスワード設定、アクセス制御等）が
適切になされ、堅牢性が十分であるかどうか評価します。

外部からの侵入・内部からの攻撃の両方の視点で攻撃方法を想定し、
実際に不正侵入と同じ方法を用いて診断をします。



Q&A あなたの会社は大丈夫ですか？

なぜハッカーはウチの会社をサイバー攻撃の標的にするの？

情報は知的財産、顧客・個人データ、または機密性の高い文書など、企業が保有する最も価値ある資産の一つです。ほとんどの会社はマニュアルや顧客リストなど、競合他社にとって価値ある情報を社内のサーバーなどに保有しています。これが、あらゆる企業がサイバー攻撃の標的となる一番の理由です。

ほとんどの日本企業は、サイバー攻撃に対する準備ができていないのでは？

多くの日本企業では予算のなさを理由に、サイバーセキュリティを昔ながらのアンチウイルスソフトウェア（ウイルス対策ソフト）に依存しています。サイバーセキュリティに投資している会社であっても、その多くはセキュリティホールを塞ぐことや、攻撃を防ぐための壁を設けるといった、予防的な対策に対して予算の大部分を注ぎ込んでいます。しかしこれは本質的にサイバー攻撃への対策に繋がりません。犯罪者たちは常に新しい脆弱性を見つけ、自分たちの活動を隠蔽しつつ、企業のネットワークに侵入する方法を考案し、実行し続けているからです。

企業がサイバー攻撃を受けた結果、どんなことが起こる？

サイバー攻撃によって、機密情報が漏洩した場合、短期的・長期的両方のコストがかかります。短期的なコストは、PCやサーバーのクリーンアップ、回復、調査などが挙げられます。長期的には、情報漏洩による競争力の低下、企業信用力やブランドの失墜、顧客に対するお詫びや保証の費用、規制監査の費用等が挙げられます。このようにサイバー攻撃による損害が、企業に与えるダメージは計り知れません。

ハッカーがわざわざ中小企業をサイバー攻撃の標的にすることはあまりないのでは？

サイバー攻撃の半分以上は中小企業を標的としており、年々この傾向は高まっています。要因として、①規模が小さな企業ほどサイバー攻撃への防御策を講じておらず、従業員のセキュリティに対する意識が低い。②多くの中小企業が詐欺に利用できる財務情報や、なりすまし犯罪に利用できる個人情報を自社サーバー内に保存している。③中小企業にあっても、取引のある大企業とデータネットワークのコネクションを持っていたり、フィッシングメールへのアドレス提供など、サイバー攻撃の犯罪者が利用できるネタがたくさんある、などが挙げられます。

被害事例

事例1

東証一部企業 売り上げ300億円ほど。
さくらマネージドサーバーにて、15サイトのサイト管理。
ある1サイトからサーバーに侵入され、
全てのサイトが被害にあう。

- 被害状況などの調査費用:100万円
- 復旧／新規サーバー構築及び移管費用:890万円
- 再度繰り返さないための運用監視:月50万円

事例2

サービス業（人材紹介など）。
年商約10億円。
運営サイトの一つがサイバー攻撃にあい
リスティング経由で相談。

- 事故調査及び復旧費用:200万円
- 事故にあったサイト以外のセキュリティ診断&対策:90万円
- 事故再発を防ぐため3サイト及び3事業所の監視:月200万円

●施設警備・交通誘導警備・イベント警備・駐車場警備・雑踏警備　他●

チュウケイセキュリティ株式会社

〒060-0061 札幌市中央区南1条西7丁目4 塩業ビル4F
http://www.chukei-s.com
☎011-280-8000 FAX011-200-0344

■会社概要

許　認　可	警備業 北海道公安委員会認定 第100000728号
設　　立	平成19年8月8日
資　本　金	1,000万円
事業内容	施設警備業　交通誘導警備業　雑踏警備業　身辺警備業　ビル管理　設備 アパート業務　サイバーセキュリティ事業
従業員数	120名
加入団体	(社)全国警備業協会　(社)北海道警備業協会
取引銀行	北洋銀行　北海道銀行　北海道信用金庫　札幌中央信用組合
主な契約先	札幌市　ワタキューセイモア㈱北海道支店　山崎製パン㈱札幌工場　石橋病院 札幌太田病院　札幌秀友会病院　㈱川西製餡所　丸栄清水電設㈱ 札幌電設工事㈱　㈱勉建設　北電力設備工事㈱　伊藤組土建㈱ スミセキ・コンテック㈱　北海道タツヲ電気㈱　日網道路設備㈱ ㈱札幌ロードメイク ナラサキライン㈱　㈱りけん　㈱札幌設備　㈱明翔　㈱創建 ㈱サツイチ　㈱SPTM　㈱北海メンテナンス　㈱佐野重機協友建設工業㈱ パナソニック環境エンジニアリング㈱　他 敬称略順不同

●サポート●

株式会社 YELL Dijital Solutions

〒104-0061 東京都中央区銀座8-10-7 東成ビル3F