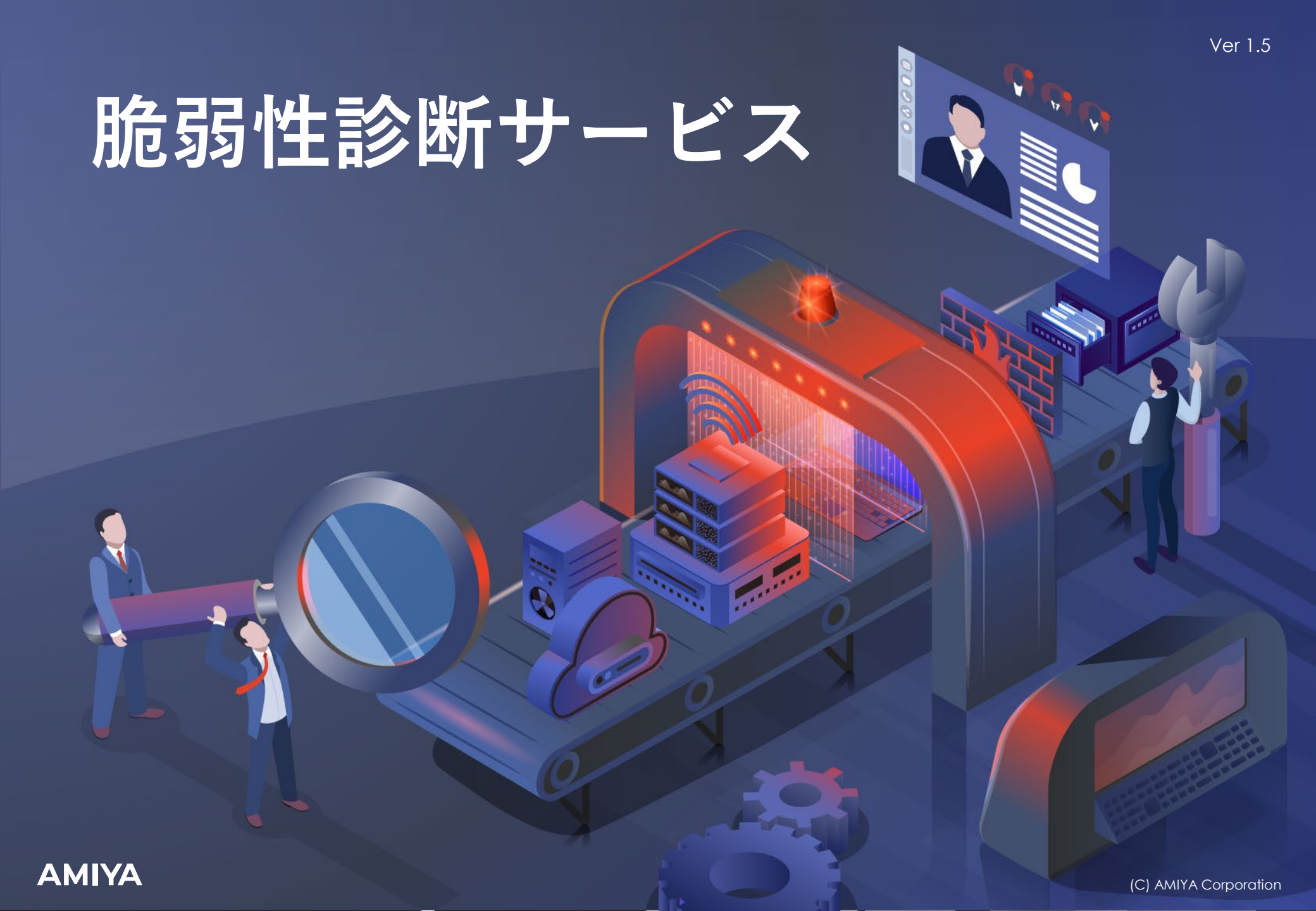
Ver 1.5

脆弱性診断サービス



AMIYA

(C) AMIYA Corporation

増える企業への課題

自社のセキュリティレベルを把握したい

セキュリティツールの導入、IT統制に対応しているが、ITシステムの脆弱性は把握できていない。

セキュリティ人材の育成・リソース不足

セキュリティ担当の人材育成をするコストとソース確保が困難に

必要なセキュリティ対策がわからない

課題が見えないため、
何から取り組めばいいかわからない。

(C) AMIYA Corporation

サイバー攻撃の大半は脆弱性から

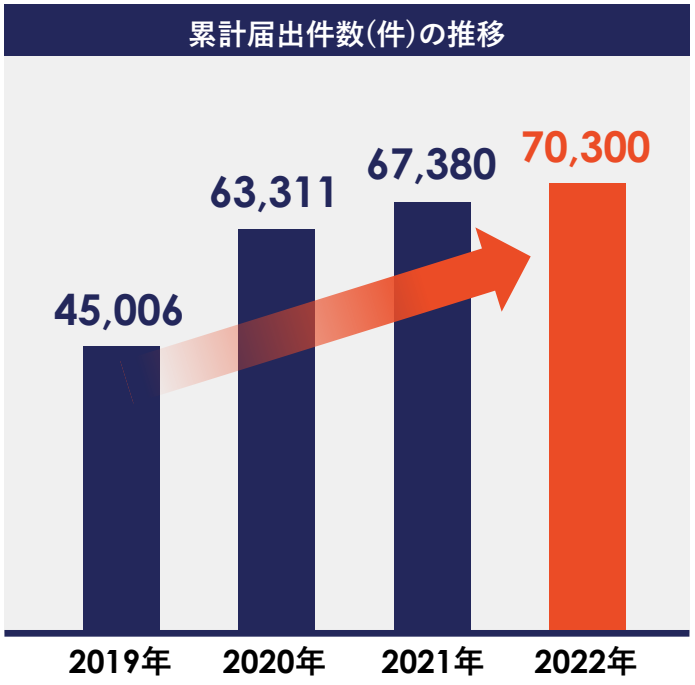
サイバー攻撃の大半が脆弱性を狙った攻撃

順位	「組織」向け脅威
1	ランサムウェアによる被害
2	サプライチェーンの弱点を悪用した攻撃
3	標的型攻撃による機密情報の窃取
4	内部不正による情報漏えい
5	テレワーク等の ニューノーマルな働き方を狙った攻撃
6	修正プログラムの公開前を狙う攻撃 （ゼロデイ攻撃）
7	ビジネスメール詐欺による金銭被害
8	脆弱性対策情報の公開に伴う悪用増加
9	不注意による情報漏えい等の被害
10	犯罪のビジネス化 （アンダーグラウンドサービス）

脆弱性による被害で発生した脅威

出典：独立行政法人情報処理推進機構 (IPA) 情報セキュリティ10大脅威 2023
https://www.ipa.go.jp/files/000108838.pdf

脆弱性を突いた攻撃は増加の一途



出典：独立行政法人情報処理推進機構 セキュリティセンター
一般社団法人 JPCERT コーディネーションセンター
ソフトウェア等の脆弱性関連情報に関する届出状況
https://www.ipa.go.jp/files/000107505.pdf

✖ セキュリティツールを導入しても、脆弱性を放置したままでは一発アウト

(C) AMIYA Corporation

ツール導入だけでなく、脆弱性診断も

脆弱性診断していなかったら

対策としてツール導入をしっかりしていても、
セキュリティの穴を突いて攻撃を受ける

脆弱性診断・対策していたら

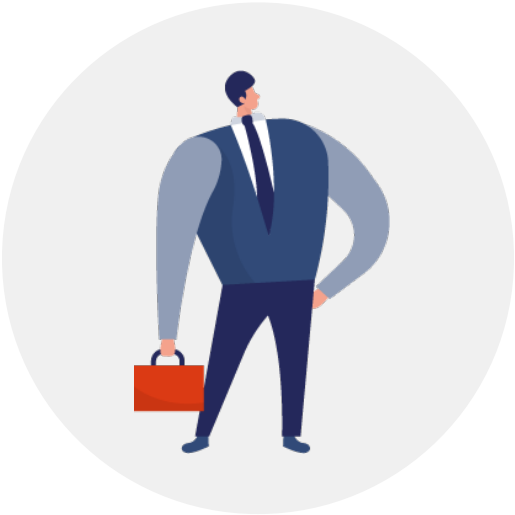
既知の脆弱性を用いた侵入を防ぐことが可能に

(C) AMIYA Corporation

脆弱性診断サービス

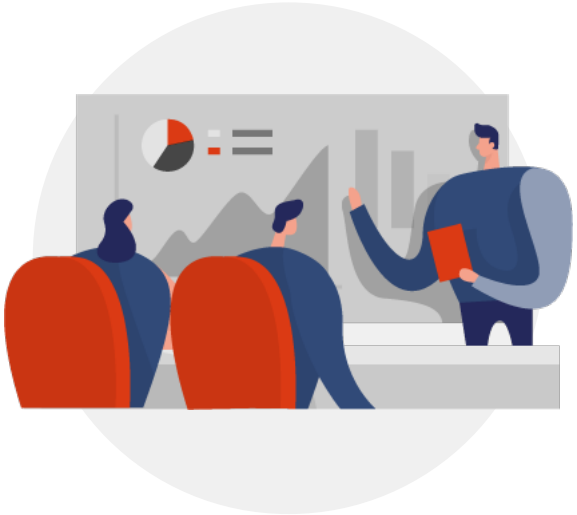
ITシステムの脆弱性調査とその対策案を提供するプラットフォーム脆弱性診断サービスです。
専任のエンジニアが診断ツールと豊富な知識で脆弱性を洗い出し、レポート提出と結果報告会によるアフターフォローまでを提供。
サイバー攻撃者と同じ目線で、脆弱性を調査。対策すべき脆弱性を発見し、サイバー攻撃のリスクを大幅に削減します。

脆弱性診断サービス



専任のエンジニア

サイバー攻撃者と同じ目線で
お客様環境を診断

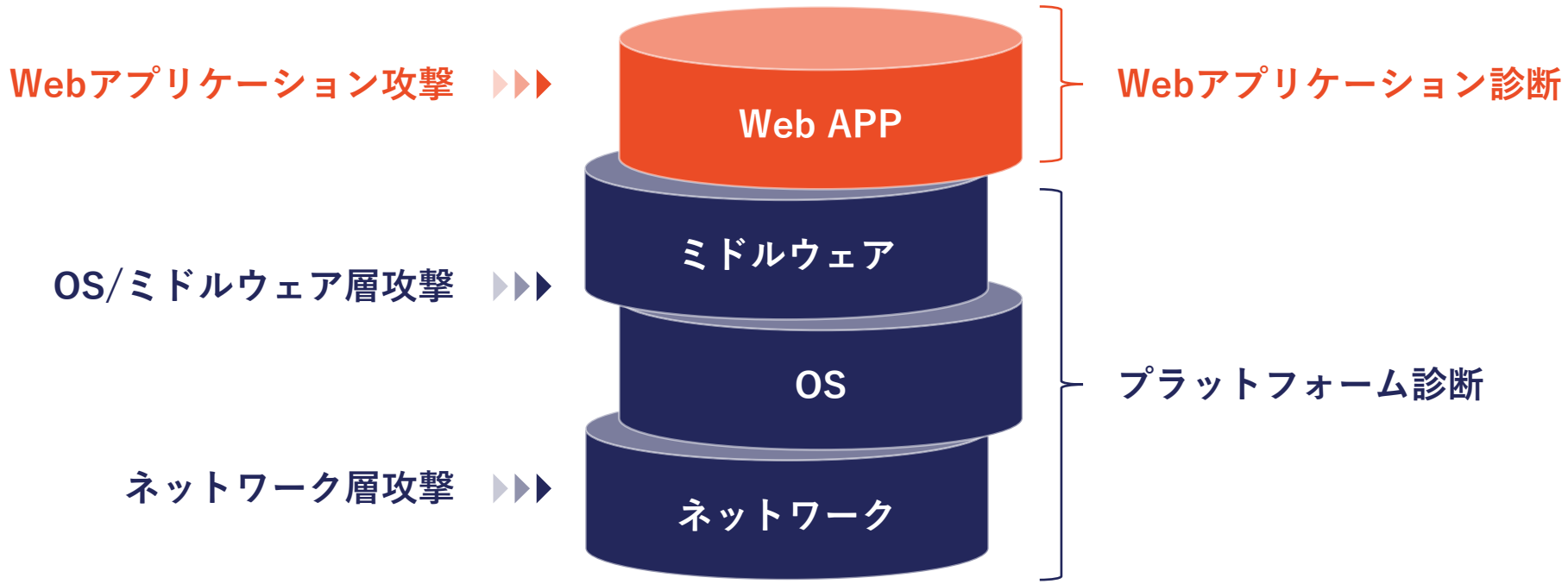


レポート/報告会

(C) AMIYA Corporation

2つの脆弱性診断サービス

Webアプリケーションに内在する脆弱性を調査するWebアプリケーション診断と
システムに内在する脆弱性を調査するプラットフォーム診断を提供します。

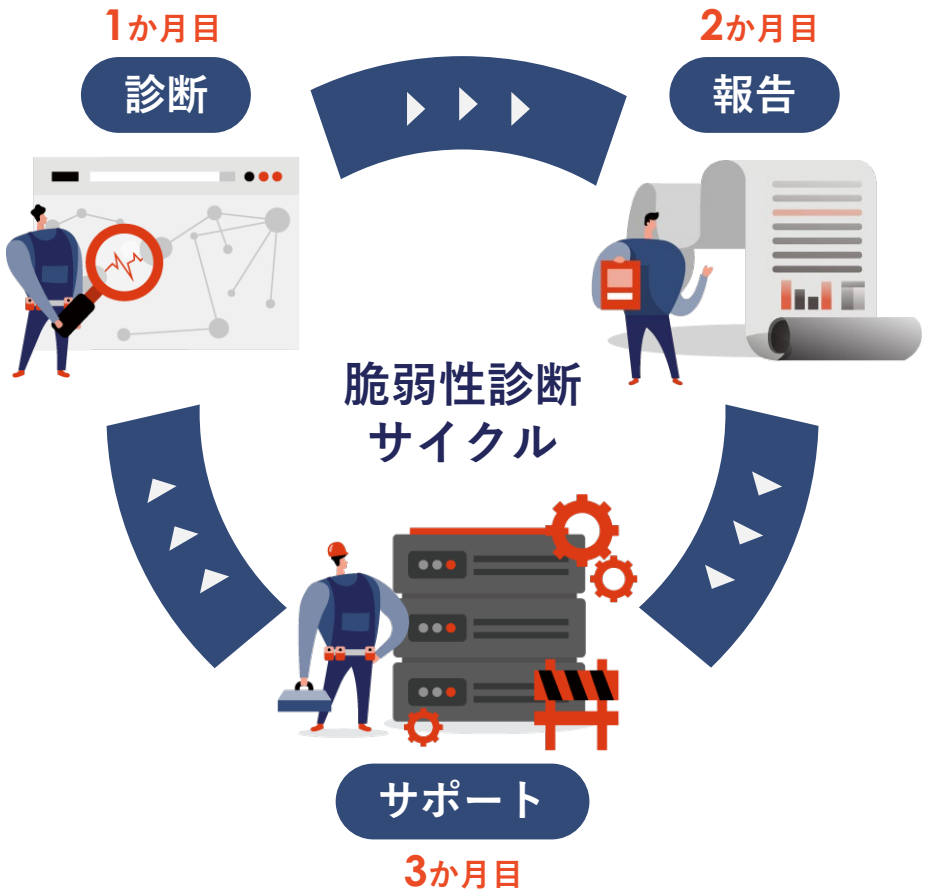


(C) AMIYA Corporation

POINT1

持続型診断

ITシステムの脆弱性は日々新しいものが増え続けるのが実情。
そのため、脆弱性診断は、「一度したら終わり」ではなく、定期的に実施することが効果的。
定期的に脆弱性診断することで、新たな脆弱性も見落としません。



1か月目 脆弱性診断

対象となるシステムに対し、最新シグネチャによる
脆弱性診断で脆弱性を発見。

2か月目 レポート/報告会

診断結果と発見された脆弱性について分かりやすくまとめた
レポートを作成。
報告会により、今後の対応についてわかりやすく説明。

3か月目 サポート対応

優先度の高い脆弱性から
脆弱性対応のアドバイス、進捗を管理

(C) AMIYA Corporation

POINT2

わかりやすさを追求

脆弱性に関するレポートは、セキュリティ用語が多く、実際にどのような影響があるのか理解できない場合も。
セキュリティエンジニアが脆弱性情報とその対策方法について”わかりやすく”レポートにまとめます。

CVSS v3.0をベースにした独自評価基準

基本評価基準 × 現状評価基準

・攻撃の難易度
・攻撃による影響
・攻撃による影響の想定範囲 等

＝

影響度をわかりやすく理解

独自評価値

・影響/深刻度合いを報告
・解決/緩和策の有無

(C) AMIYA Corporation

POINT3

診断で終わらない、対策までをワンストップで

発見した脆弱性に対策するまでが脆弱性診断。
購入ルートに関わらず、パッチ適用などの脆弱性対策をワンストップで提供します。

脆弱性診断サービス

ランサポ

診断

報告・サポート

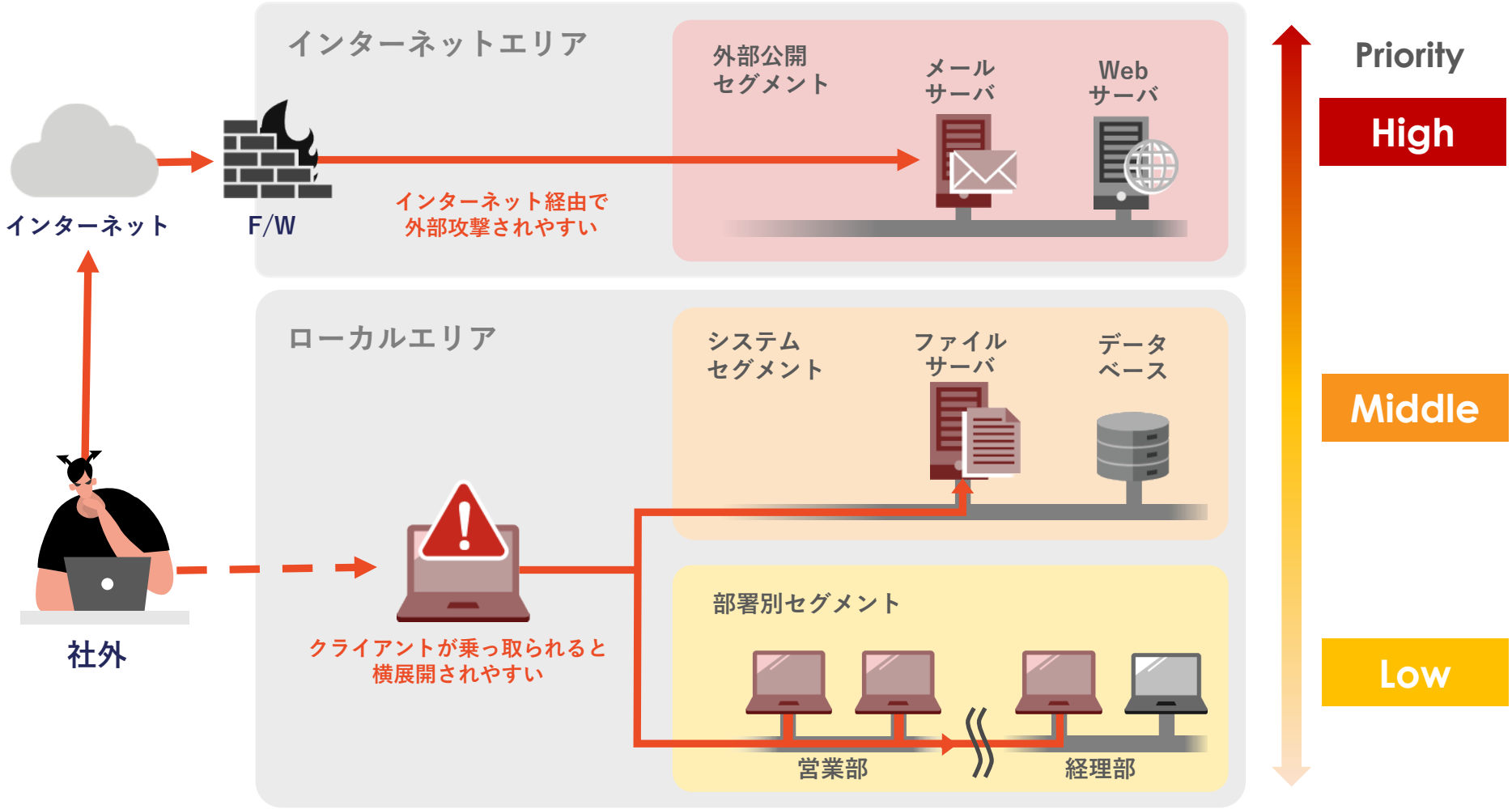
対策

『ランサポ』は、お客様の情報システム業務全般をクラウドから代行／支援するサービスです。
エンジニアを派遣しない、低コストかつハイパフォーマンスなクラウド情シスサービスです。

(C) AMIYA Corporation

プラットフォーム診断

外部からの攻撃に合いやすいインターネットエリア（公開セグメント）から、
侵入横展開されることを想定したローカルエリア（社内ネットワーク）まで、エリアに分かれた診断プランを準備しております。
影響度合いの高いエリアより優先的に診断することで効果的なサイバー攻撃対策へと繋がります。



(C) AMIYA Corporation

14万件を超える調査項目

14万件を超える調査項目により、脆弱性を見逃しません。新たな脆弱性は日々更新。

Windows

- Windows 2008 Server
- Windows 2012 Server
- Windows 2016 Server
- Windows 2019 Server
- Windows 7
- Windows 10

Unix互換プラットフォーム

- Solaris
- Linux
- FreeBSD/OpenBSD/NetBSD

他プラットフォーム

- Cisco
- Palo Alto
- NetApp
- Amazon AWS
- Microsoft Azure
- MS SQL サーバー
- Oracle
- その他多数

ネットワーク機器

- Fortinet Fortigate
- Fortinet FortiManager
- Fortinet FortiOS
- Sophos XG
- SonicWall
- Trend Micro IWSVA
- psSense
- Squid
- Check Point
- Symantec Proxy
- Juniper
- OTRS
- FireEye
- Blue Coat Proxy
- McAfee Firewall Enterprise
- Haon Security Router
- ModSecurity
- Palo Alto
- Cisco ASA
- WinProxy
- DeleGate
- SOCKS
- Zebra
- CCProxy

Fortinetサンプル

ID	名称	深刻度
163711	Fortinet Fortigate – Inter-VDOM 情報漏洩 (FG-IR-22-036)	MEDIUM
163262	Fortinet FortiOS のバッファオーバーフロー (FG-IR-21-206)	MEDIUM
163254	Fortinet FortiManager Buffer Overflow (FG-IR-21-206)	HIGH
163253	Fortinet FortiOS Buffer Overflow (FG-IR-21-206)	HIGH

Fortinet FortiOS Buffer Overflow (FG-IR-21-206)

HIGH　Nessus プラグイン ID 163253

情報　依存関係　扶養家族

概要

リモートホストは、バッファオーバーフロー脆弱性の影響を受けます。

説明

リモートホストは、6.0.x ～ 6.0.14、6.2.x ～ 6.2.10、6.4.x ～ 6.4.8、7.0.x ～ 7.0.5 の FortiOS のバージョンを実行しています。したがって、バッファオーバーフローの脆弱性の影響を受けます。認証されたリモート攻撃者がこの問題を悪用し、細工された CLI の「execute restore image」および「execute certificate remote」操作による TFTP プロトコルを介して、システムで任意のコードやコマンドを実行する可能性があります。

Nessus はこの問題をテストしておらず、代わりにアプリケーションの自己報告されたバージョン番号にのみ依存しています。

ソリューション

FortiOS をバージョン 6.2.11、6.4.9、7.0.6、7.2.0 以降に更新してください。

関連情報

https://www.fortiguard.com/psirt/FG-IR-21-206

(C) AMIYA Corporation

「脆弱性診断結果報告書」で効果的な対策をレビュー

診断結果と発見された脆弱性についてわかりやすくまとめたレポートを作成。
全ての脆弱性に対応するのではなく、重要かつ最適な対策を導き出し、今後の対応についても分かりやすく説明。
効果的なセキュリティ対策を実現します。

目次サンプル

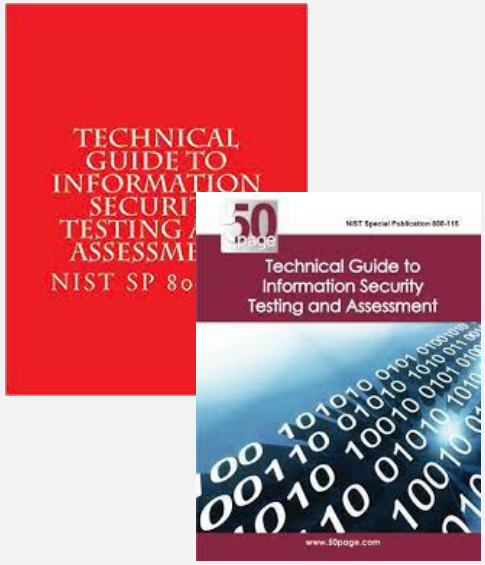
1　診断目的
2　診断概要
3　診断対象
4　総合評価
5　脆弱性評価
5.1　CVSS V3.0 評価
6　診断結果
6.1　ホスト別検出数
6.2　脆弱性レベル：緊急（CRITICAL）
6.3　脆弱性レベル：重要（HIGHT）
6.4　脆弱性レベル：警告（MEDIUM）
6.5　脆弱性レベル：注意（LOW）
7　実施すべき対策
7.1　SSL バージョンおよびプロトコルの検出
・
・
・
・

(C) AMIYA Corporation

国際標準ガイドラインに準拠

NIST SP800-115「Technical Guide to Information Security Testing and Assessment」に準拠した脆弱性診断を実施。
運用体制はISMS認証を取得し、適切にお客様の情報を取り扱います。

NIST SP800-115に準拠

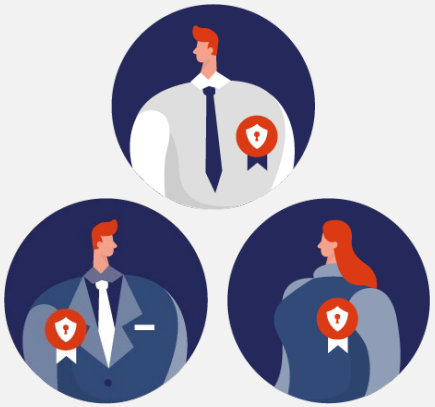


運用体制はISMSを取得

ANAB ACCREDITED ISO/IEC 17021 MANAGEMENT SYSTEMS CERTIFICATION BODY
bsi.
ISMS ISR004

IS 502082 / ISO 27001:2013

セキュリティ資格者多数在籍



情報処理安全確保支援士

(C) AMIYA Corporation

インターネットエリア脆弱性診断

Priority > **High**

インターネットに公開しているITシステムは攻撃のしやすさから狙われる傾向にあります。
そのため、インターネットエリアのシステムを優先して脆弱性に対応することをお勧めします。

条件

公開セグメントにインターネット経由でアクセス

対象

Webプロキシ / リバースプロキシ / メールサーバ /
スイッチ / VPN / NW機器 等

価格

毎月の診断に	月額サービス費用	100,000 円
お試し診断に	スポット診断	300,000 円

※「月額サービス」は年間での契約となります。
※10 IPアドレスまでを対象に診断します。

(C) AMIYA Corporation

ローカルエリア脆弱性診断

Priority > Middle Low

脆弱性が放置されがちなローカルエリアを対象にすることは、サイバー攻撃の被害を最小化に抑える効果が見込めます。
不正侵入されることを前提に、ローカルエリアについても脆弱性に対象することをお勧めします。

条件

診断用端末を社内ネットワークに持ち込みアクセス

対象

クライアント端末 / ファイルサーバ / データベース/
Active Directory / 社内ポータル / 各種サーバ等

価格

毎月の診断に	月額サービス費用	400,000 円
お試し診断に	スポット診断	1,500,000 円

※「月額サービス」は年間での契約となります。
※1セグメント（/24）までを対象に診断します。

(C) AMIYA Corporation

Webアプリケーション診断

Webアプリケーションに対して、手動及び自動ツールを用いて脆弱性診断を実施。
コーディングミスにより内在した脆弱性を見つけ、安全なWebサイト構築を支援します。

認証

- 不適切な認証
- パスワードリマインダの検証
- パスワードポリシー

承認

- セッションの推測
- セッションの固定
- 不適切な承認
- セッションの盗難

クライアント側での攻撃

- クロスサイトスクリプティング
- クロスサイトリクエストフォージェリ
- コンテンツの詐称
- クリックジャッキング

情報漏洩

- ディレクトリインデクシング
- 推測可能なリソース位置
- ウェブサーバ・アプリケーションの特定

コマンドの実行

- バッファオーバーフロー
- 書式文字列攻撃
- LDAPインジェクション
- OSコマンドインジェクション
- SQLインジェクション
- SSLインジェクション
- XMLインジェクション
- パラメータ改ざん

ロジックを狙った攻撃

- 機能の悪用
- パストラバーサル
- リダイレクタ
- 不適切なプロセスの検証

(C) AMIYA Corporation

「報告書」で対策に繋げる

診断結果と発見された脆弱性についてわかりやすくまとめたレポートを作成。
全ての脆弱性に対応するのではなく、重要かつ最適な対策を導き出し、今後の対応についても分かりやすく説明。

4-3.総合評価について

総合評価については、発見された脆弱性の個数や危険性に基づいて下記の基準を定めています。

判定	概要
S	脆弱性が検出されませんでした。
A	軽微な脆弱性が検出され、 早急な対応が不要である場合です。
B	セッションの固定などの他の脆弱性と組み合わせることにより被害を受ける可能性がある脆弱性が検出され、修正することが推奨されます。
C	クロスサイトスクリプティング（XSS）などの危険性の高い脆弱性が検出され、早期に修正する必要があります。
D	個人情報の漏えいやデータの破壊、 サービスの停止に繋がる緊急度の高い脆弱性が検出され、 非常に危険な状態です。

6.診断結果詳細

No01. SQLインジェクション

発生箇所	対象URL
危険度	CRIT

SQL インジェクションは、ユーザからの入力が安全でない方法でデータベースの SQL クエリに組み込まれることによって発生します。
本発生箇所では、下記の 20 秒間スリープを実行させる SQL 命令を含む文字列を発生箇所のパラメータに挿入することにより、SQL 命令を実行し、20 秒処理を停止させます。

```
'+(select*from(select(sleep(20)))a)+'
```

想定されるリスク

攻撃者は、攻撃コードを含む入力を送信し、重要なアプリケーションデータの読み取り、変更、削除、認証の回避、データベース内の権限の昇格、データベースサーバの制御など、SQL のクエリで操作できる広範囲な対象が影響を受けます。

対策

Web アプリケーションにおいて SQL 文を生成する際には、可変な項目を後から変更可能なパラメータとして処理する方法であるプレースホルダを用いて処理を行ってください。
上記の対応ができない場合は、SQL 文を組み立てる際に書式を正しく構成するなどして SQL 文が変更されないようにしてください。
また、保険的な対策として、エラーメッセージに SQL 文を表示しない設定を行うことやデータベースの権限を適切に設定する対策を検討してください。

(C) AMIYA Corporation

Webアプリケーション診断

価格

ベース	スポット診断 ※10リクエストまで	600,000 円
追加	10リクエスト追加	150,000 円

再診断

条件：危険度Middle以上の再診断は無償（３ヶ月以内）

リクエストとは

例）お問い合わせフォーム→3リクエスト

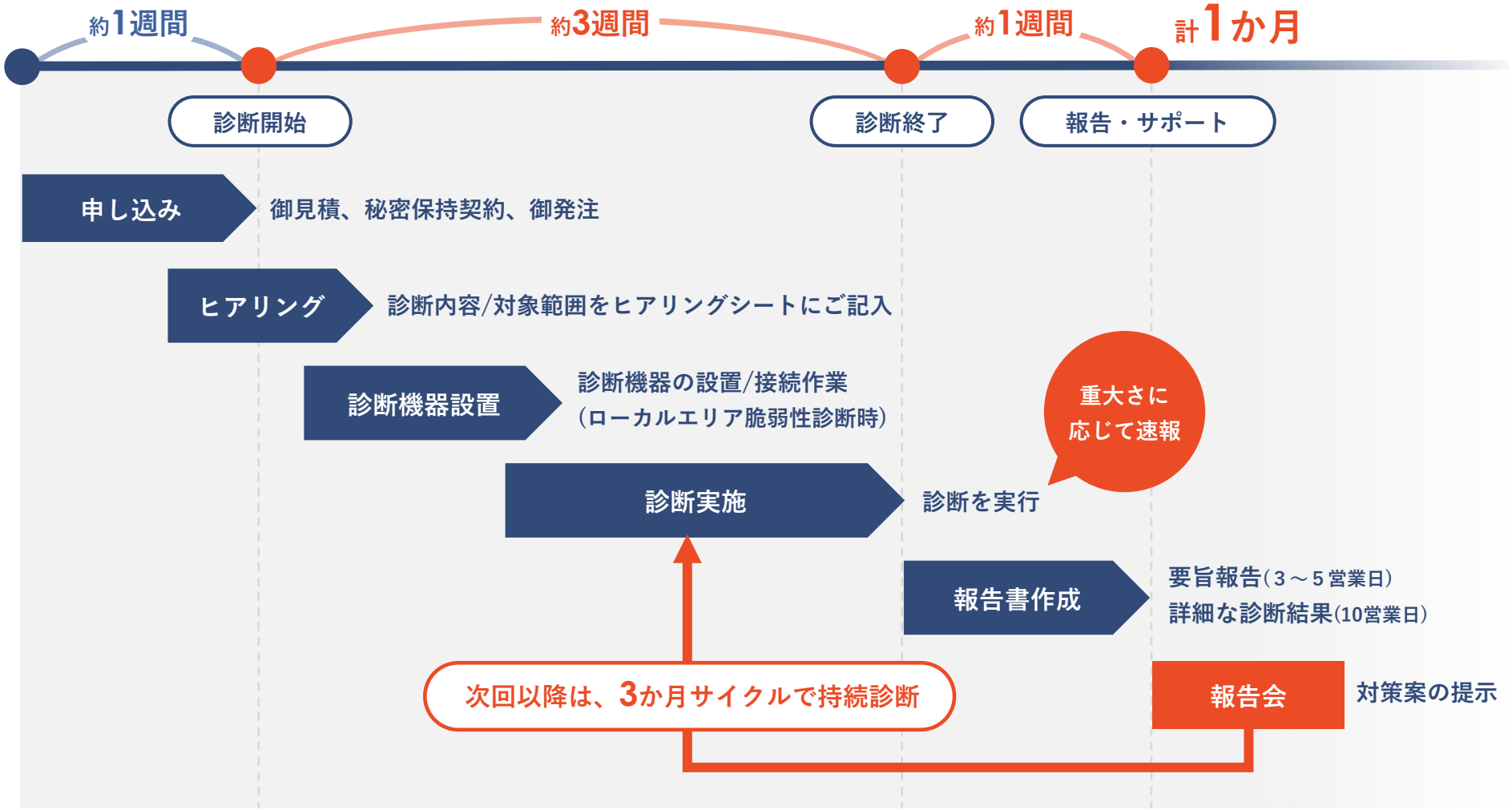
①お問い合わせページ表示（Get）
②お問い合わせ 送信クリック（POST）
③お問い合わせ 送信完了（Get）

※診断対象URLのリクエスト数を弊社にてカウント可能

(C) AMIYA Corporation

申し込みから1か月で対応

ご依頼の診断内容とお客様のスケジュールにあわせて診断を実施。
重大な脆弱性を発見した場合は内容/対策を速報し、サポート対応まで最短1か月で提供します。



(C) AMIYA Corporation

包括的な情報システム業務を、月額固定で。

クラウド情シスサービス
ランサポ

『ランサポ』は、お客様の情報システム業務全般をクラウドから代行／支援するサービスです。
エンジニアを派遣しない、低コストかつハイパフォーマンスなクラウド情シスサービスです。

以下のすべてに月額固定で対応します。

サーバ、ネットワークの運用/監視業務
ドキュメント整備・更新、死活監視、保守管理、月次レポート

障害/トラブル対応
サーバ、ネットワーク、クラウド、PCなどに対する問い合わせ対応及び障害対応

定型業務代行
アクセス権申請対応、アカウント管理ポリシー管理、設定変更など

PCマスターイメージ作成
PCマスターイメージの作成・定期更新

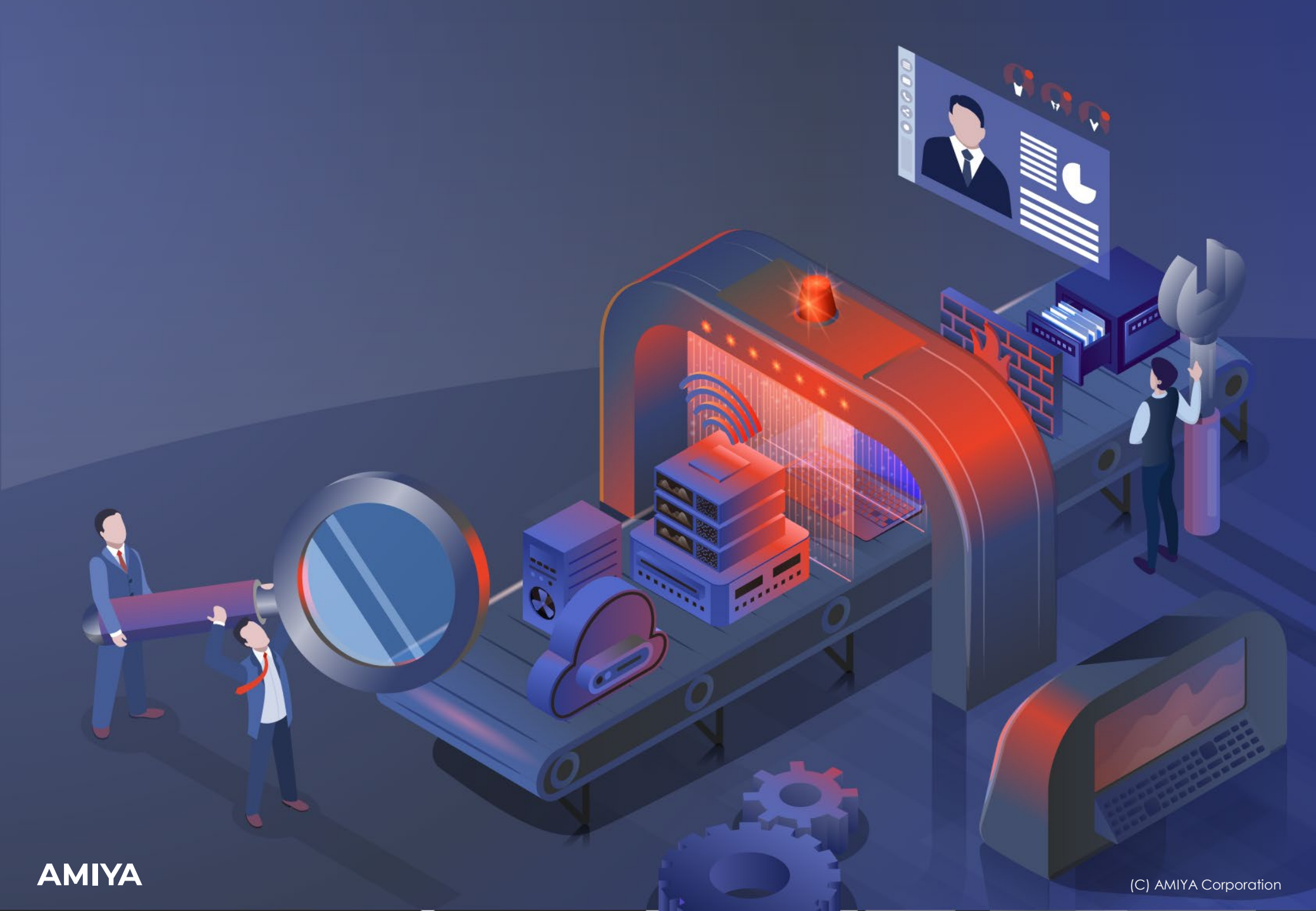
年間計画の作成支援
次年度の予算やロードマップ作成を支援

BCP関連支援
リスクレベルに応じたBCP対策を支援

クラウド移行支援
最適なクラウドの選定や移行方法などを支援

セキュリティ対策支援
今後のセキュリティ対策をアドバイス

(C) AMIYA Corporation



AMIYA

(C) AMIYA Corporation