Document Ver.1.12

セキュサポ

クラウドCSIRTサービス

AMIYA

(C) AMIYA Corporation

サイバー攻撃は事業継続を揺るがすリスクに

サプライチェーンへ影響するランサムウェア

製造業

被害
自社と子会社のサーバ/PCが暗号化。
ネットワークを遮断させたため、取引に多大な影響

二次被害
主要取引先の国内全工場が操業停止。
関連取引先工場も一時操業停止に

サプライチェーンからランサムウェアが侵入

病院

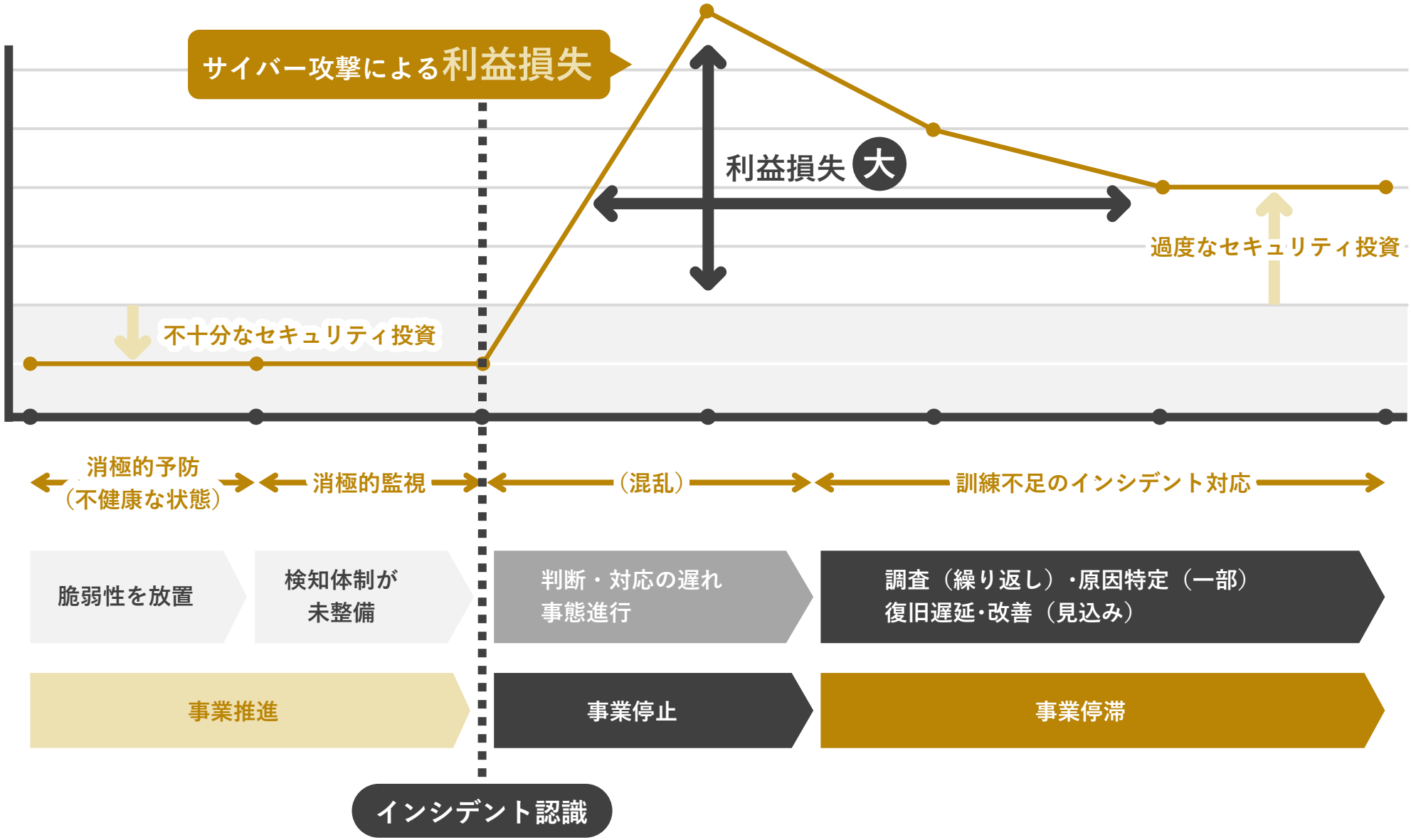
被害
電子カルテシステムがランサムウェアに感染。
患者の診断履歴や病歴が把握不能に

二次被害
メディアに公表され、VPNの脆弱性を放置した
体制を批判され、病院経営に影響

サイバー攻撃の影響は、自社だけでなくサプライチェーンへも波及。

(C) AMIYA Corporation

一般的な組織が陥る「サイバー攻撃による利益損失」



(C) AMIYA Corporation

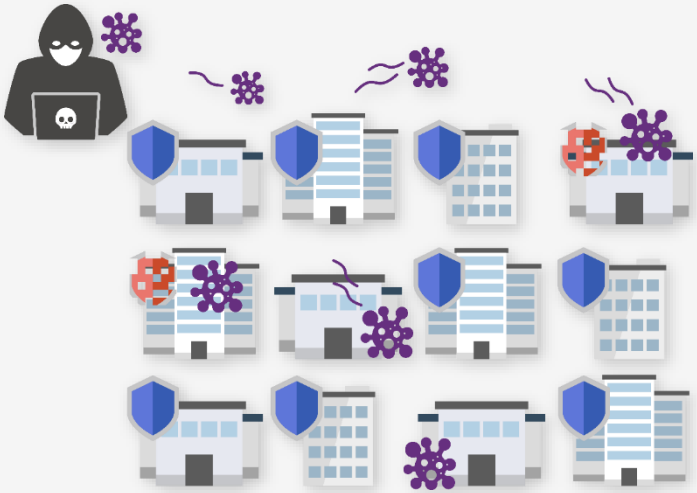
アプローチ①「サイバー攻撃を受けやすいシステムを重点的にケア」

事実 「ランサムウェアの侵入経路の80%が脆弱性や設定不備から」※

サイバー攻撃トレンドの変化

特定組織をターゲット
&計画的に攻撃

脆弱性のある組織を
自動探索&ターゲット



「”予防”（脆弱性や設定不備を無くすこと）を最優先」

※出典 警察庁「令和４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」

(C) AMIYA Corporation

アプローチ②「侵入されることを前提とする」

事実 「ウイルスの感染経路としてメールがよく使われる」
「アンチウイルスソフトでは検知できない可能性が高い」

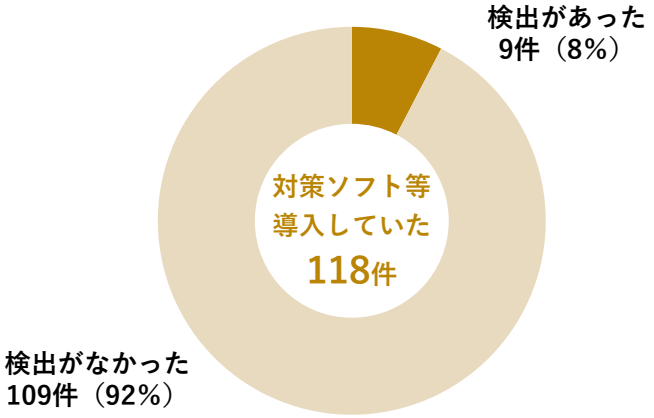
メールからウイルス感染 誰かは開いてしまう

標的型攻撃メール訓練開封率

2021年度		2022年度
約15%	▶	約12%

※出典 東京商工会議所
「「標的型攻撃」メール訓練 実施結果」

ランサムウェア被害時のウイルス検出率※



※出典 警察庁「令和４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」

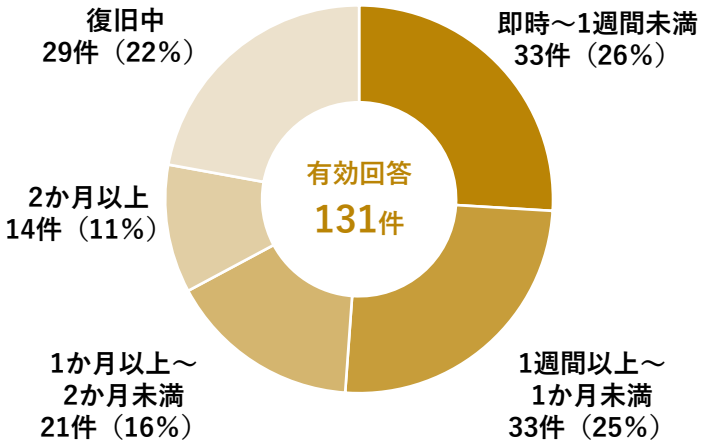
→ 「”検知”できる体制を整備（サイバー攻撃の初期段階で気づく）」

(C) AMIYA Corporation

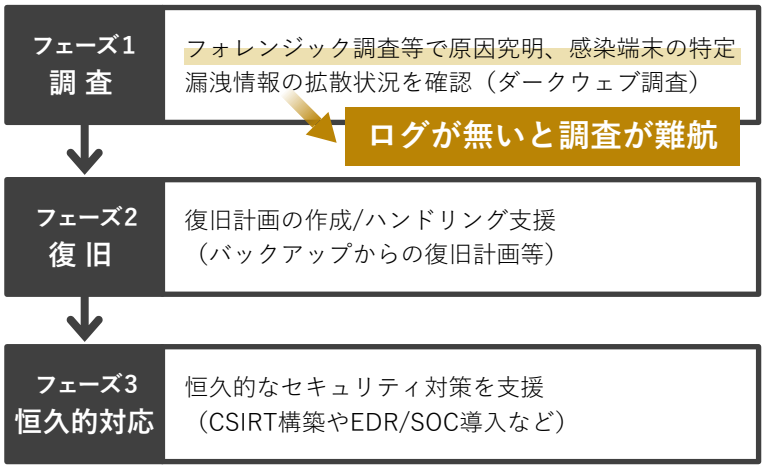
アプローチ③「スピーディなインシデント対応が被害を最小化」

事実 「ログの消失/未取得でインシデント対応が長期化&被害額の増加」

ランサムウェア被害の約50%以上が復旧に1ヶ月以上要する※



インシデント対応フロー

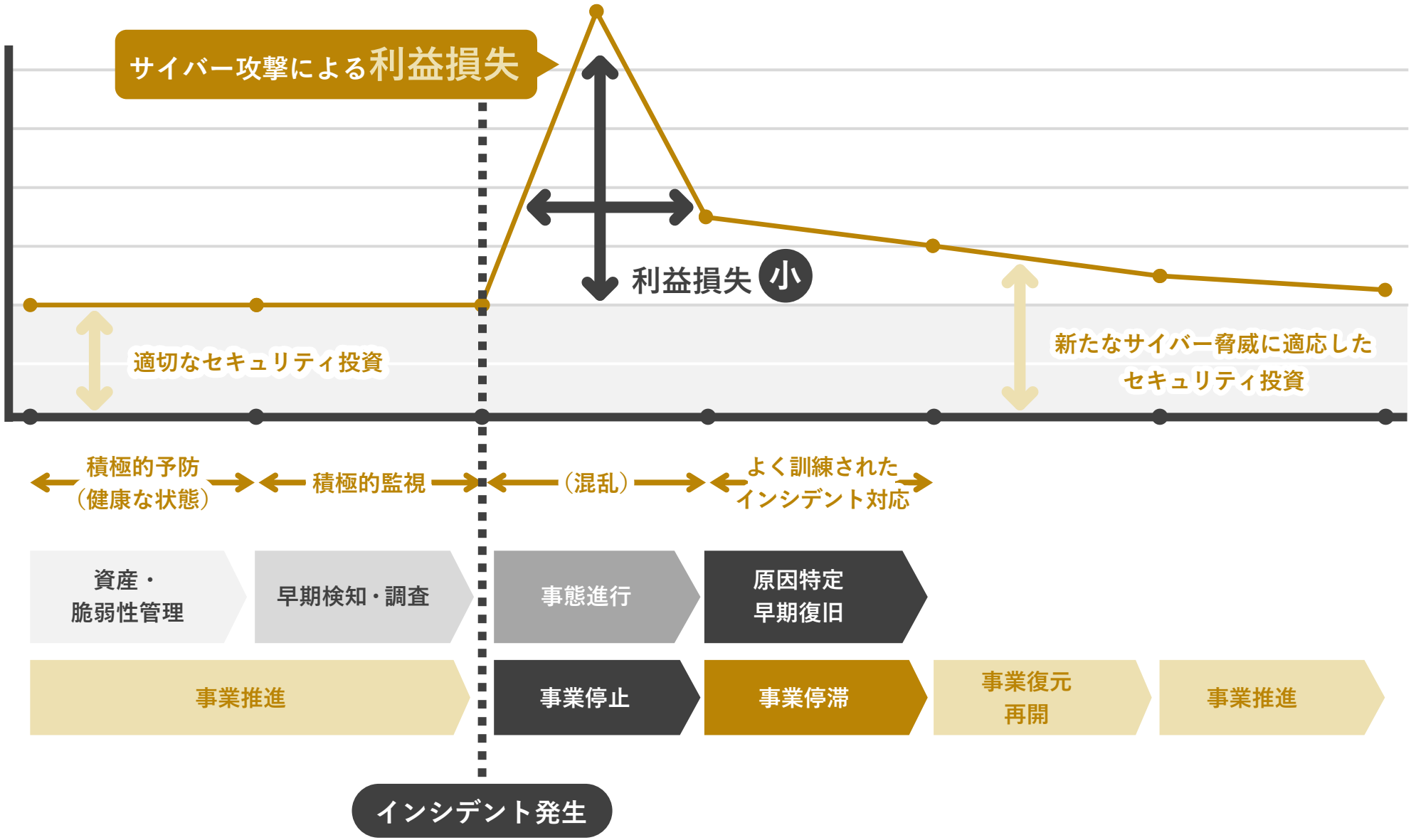


「迅速に”対応”できる体制を整備（ログを統合管理/分析）」

※出典 警察庁「令和４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」

(C) AMIYA Corporation

組織が獲得すべき「組織的サイバーレジリエンス能力」



(C) AMIYA Corporation

サイバーセキュリティ対策のよくある課題

01

セキュリティ対策を考える・実行する

『セキュリティ人材がいない』

02

数あるセキュリティ製品/サービスから

『優先すべきセキュリティ対策がわからない』

03

海外製品をベースとした

『セキュリティ対策サービスは高額』

(C) AMIYA Corporation

クラウドCSIRTサービス「セキュサポ」

サイバー攻撃動向から組織が対応しておくべきセキュリティ運用を
予防・検知・対応の各フェーズでの推奨を提供します。

セキュサポ　中小・中堅企業に必要十分なセキュリティ運用を月額固定で

予防
- アタック サーフェス調査
- 脆弱性診断
- セキュリティ 情報連携

検知
- SOC 構築
- SOC 運用（攻撃検知）
- SOC 運用（内部不正）

対応
- 初動対応 アドバイス
- 分析（原因/影響範囲）
- サイバー保険

その他
- 相談窓口
- レポート
- 報告会

(C) AMIYA Corporation

予防 アタックサーフェス調査

サイバー攻撃の対象となりうるIT資産や攻撃経路（アタックサーフェス）を調査・管理し、リスクを低減。

発見	• 企業が保有するIPアドレス/ホスト名の発見 • 未把握のシステムの発見
↓	
情報収集	• システムの情報収集（OS、ソフトウェア、バージョン情報、オープンポートなど） • 設定不備の発見（不必要なRDPポートの解放など）
↓	
リスク評価	• 収集情報を元に、リスクを評価
↓	
リスク対応	• リスクへの対応（パッチ適用など）

(C) AMIYA Corporation

予防 脆弱性診断

インターネットに公開しているシステムに対する定期的（4半期ごと）な脆弱性診断でリスクを低減。

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

予防 セキュリティ情報連携

緊急度の高い脆弱性情報を共有

New message

To:

Subject:

セキュサポ契約ユーザ様

Fortigate SSL-VPNにおけるリモートコード実行の脆弱性を悪用した攻撃の情報があがっております。
もし、該当される場合は、リンク先の内容をご確認ください。

なお、今回の脆弱性では二段階認証も突破できるとされています。
詳細は後日発表されるため追加情報があれば順次展開予定です。

＝＝＝＝＝＝＝＝＝＝

【参考URL】
https://www.bleepingcomputer.com/news/security/fortinet-fixes-critical-rce-flaw-in-fortigate-ssl-vpn-devices-patch-now/
https://www.ipa.go.jp/security/security-alert/2023/alert20230613.html

【影響度】
緊急

【攻撃された場合に起こる事象】
リモートコード実行の可能性

【脆弱性の対象】
FortiOS 6.0.17, 6.2.15, 6.4.13, 7.0.12, and 7.2.5より前の全バージョン。
詳細は後日発表される予定。

【恒久対策】
バージョンアップ

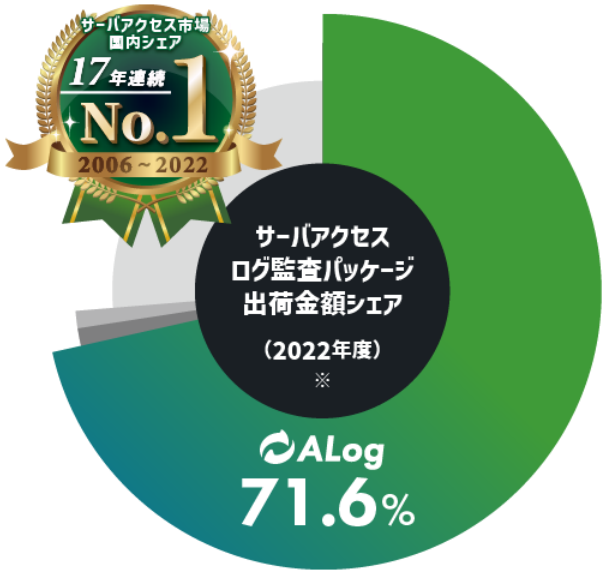
＝＝＝＝＝＝＝＝＝＝

以上、情報共有となります。
ご確認よろしくお願いいたします。

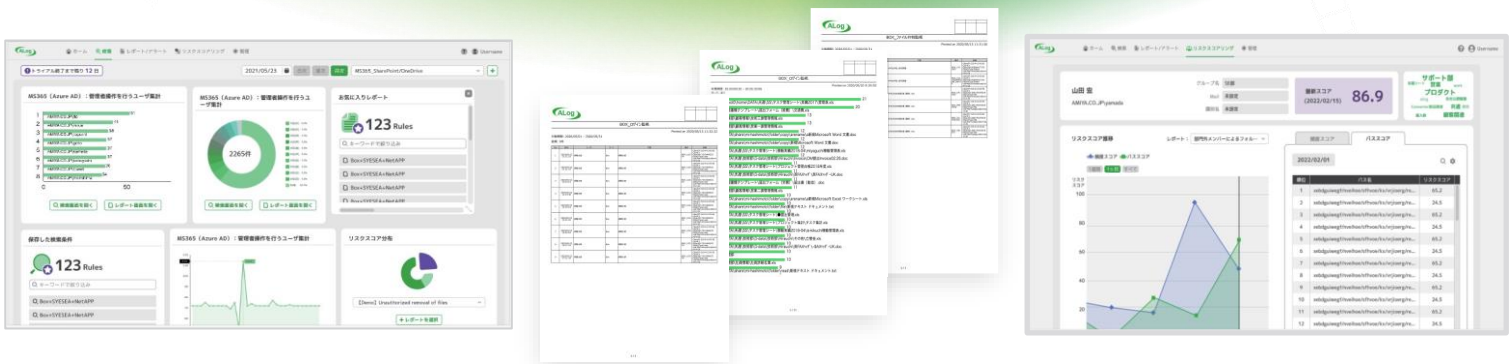
(C) AMIYA Corporation

検知 SOC構築 –ログ管理システムの導入

SIEM「ALog」を導入、ログ統合管理/攻撃検知システムを構築



出典： デロイト トーマツ ミック経済研究所
「内部脅威対策ソリューション市場の現状と将来展望 2023年度」2024年2月 発刊
https://mic-r.co.jp/mr/03010/



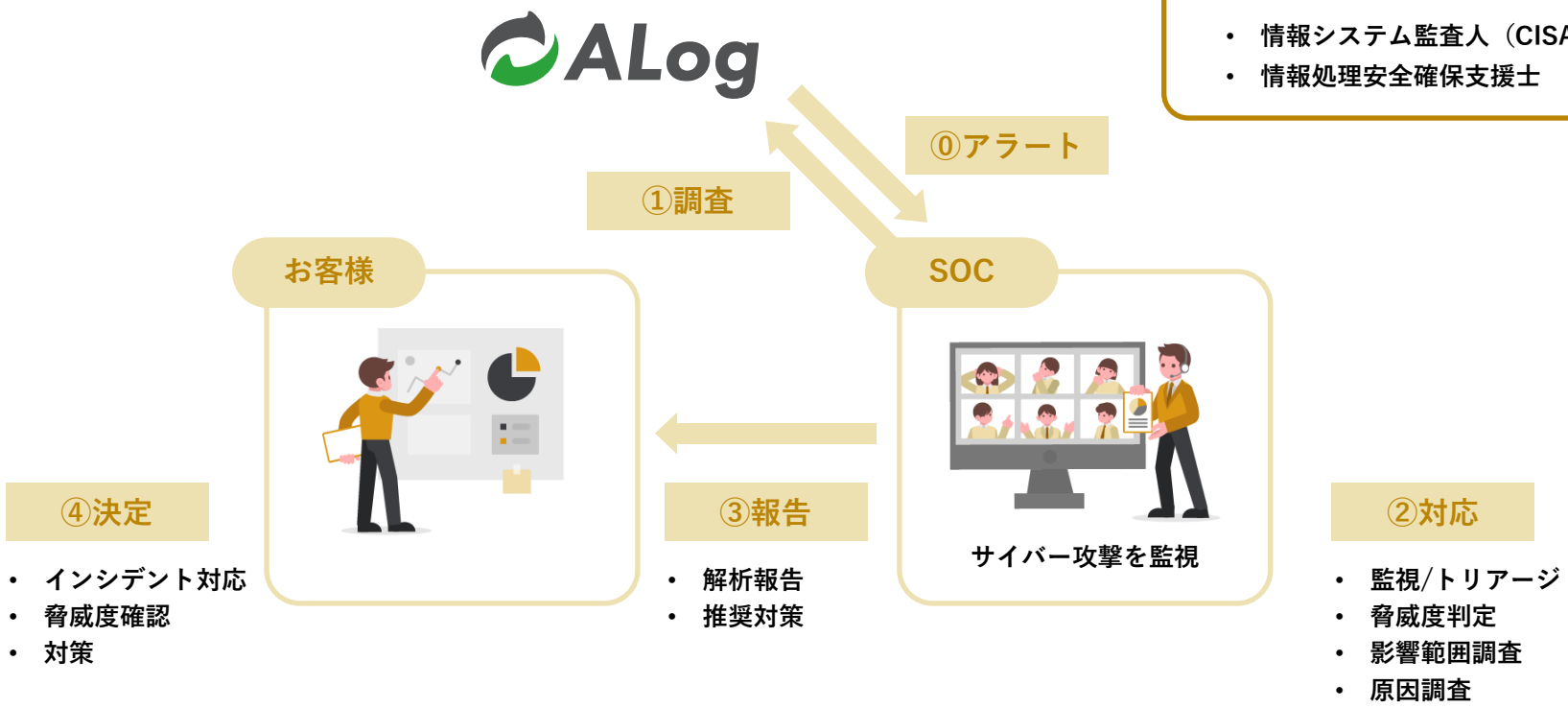
(C) AMIYA Corporation

検知 SOC運用

サイバー攻撃アラートを監視、分析、報告。有事の際は、原因の分析、影響範囲を特定。

セキュリティスペシャリスト対応保有資格

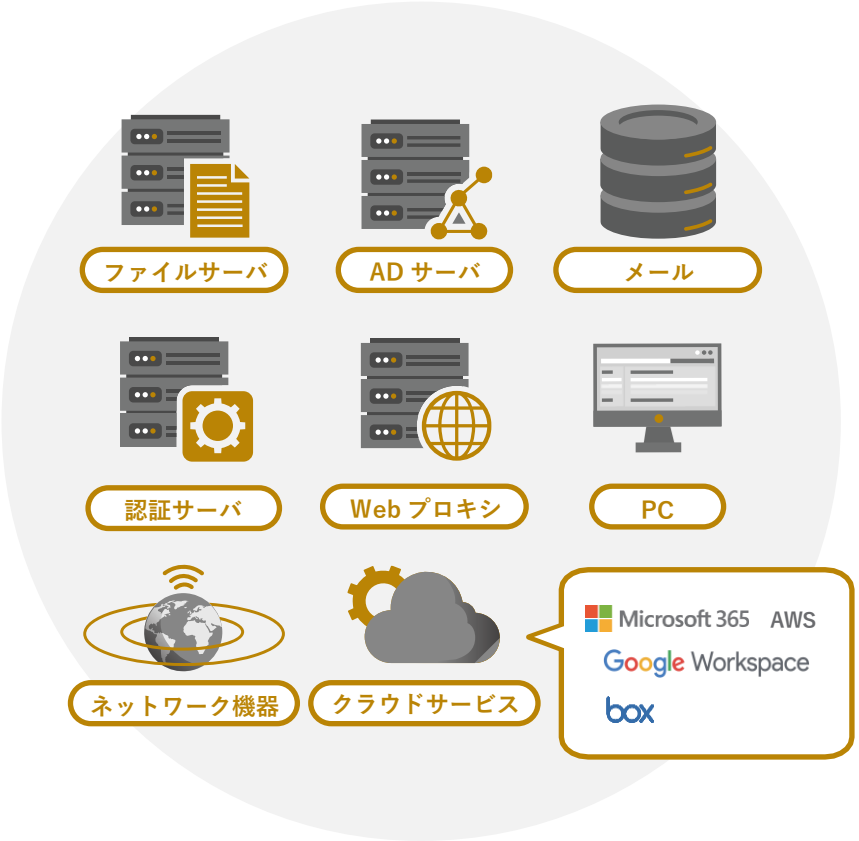
- 情報システム監査人（CISA）
- 情報処理安全確保支援士



(C) AMIYA Corporation

検知 網羅的だから死角を最小化

組織のITシステムを網羅的に監視、単一のログからは気付けないサイバー攻撃も検知/分析



サービス範囲（対応システム一覧）

ファイルアクセスログ
（Windowsファイルサーバ / SharePoint / OneDrive / Box / Google ドライブ）

認証ログ（Active Directory / Microsoft Entra ID）

ネットワークログ（FortiGate/PaloAlto/SonicWall）

PCログ（SKYSEA / LANSCOPE）

メールログ（Exchange Online / Gmail）

Proxyログ（i-Filter）

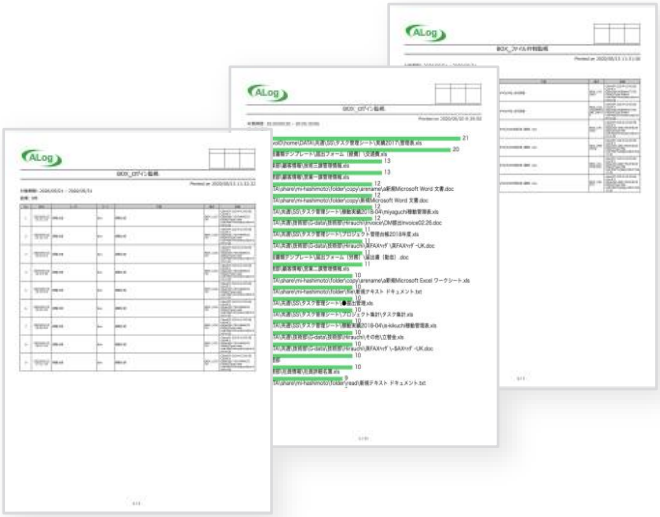
VPNログ（Verona / FortiGate）

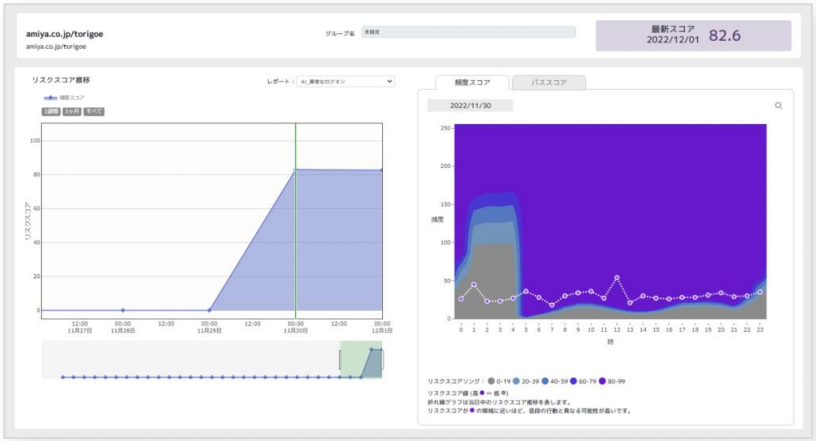
※※状況に応じて、解析に必要なログ
（DHCP、DNS、システムログなど）を取得します。
※順次監視対象を拡大中。
記載がないシステムについてもご相談ください。

(C) AMIYA Corporation

検知 内部不正対策や監査にも活用

組織のポリシー違反やITシステム監査の対応にも活用





ポリシー違反

- 業務時間外のログイン・ファイル操作
- 許可されていないWebサイトへのアクセス
- 許可されていない外部へのファイル共有
- 退職予定者のファイルアクセス/メール送信
- 重要フォルダへのアクセス

ITシステム監査

- 管理者権限ユーザのログオン
- 管理者権限ユーザの操作履歴
- 管理者権限ユーザのDB操作履歴
- ファイル/フォルダのアクセス権変更
- ユーザアカウントの追加/削除（消し忘れ）

(C) AMIYA Corporation

対応 初動対応/分析

適切な初動対応を支援、さらに原因や影響範囲を分析し、迅速な対応

＼分析／
ALogで原因調査

初動対応アドバイス

01
感染端末の隔離

同一ネットワーク内への感染拡大を防ぐため感染した端末をネットワークから隔離

02
感染端末の証拠保全

メモリやHDD/SSDのドライブの証拠保全のため感染端末は隔離した状態のまま維持

03
パスワード変更

ブラウザに保存されているパスワードや利用しているサービスのパスワードを変更

04
関係各所への報告

警察やCSIRTで定められている個人情報漏洩の外部団体等必要機関に連絡

(C) AMIYA Corporation

対応 サイバー保険

損害を保険で補償 （限度額500万円）

当サービスには、サイバー保険が標準付帯。
原因や影響範囲の調査といった事故調査費用を
保険でカバーできるので、まさかの過大コストに
脅威を感じる必要がありません。

調査/対応費用
原因・影響範囲調査、復旧・再発防止

賠償金発生
被害者、取引先からの
損害賠償金や弁護士費用

利益喪失
事業中断による事業損失

金銭被害
ランサムウェア等による金銭支払い

法的対応
法律/規則違反に対する罰金や課徴金

風評被害
イメージ低下/社会的地位の低下

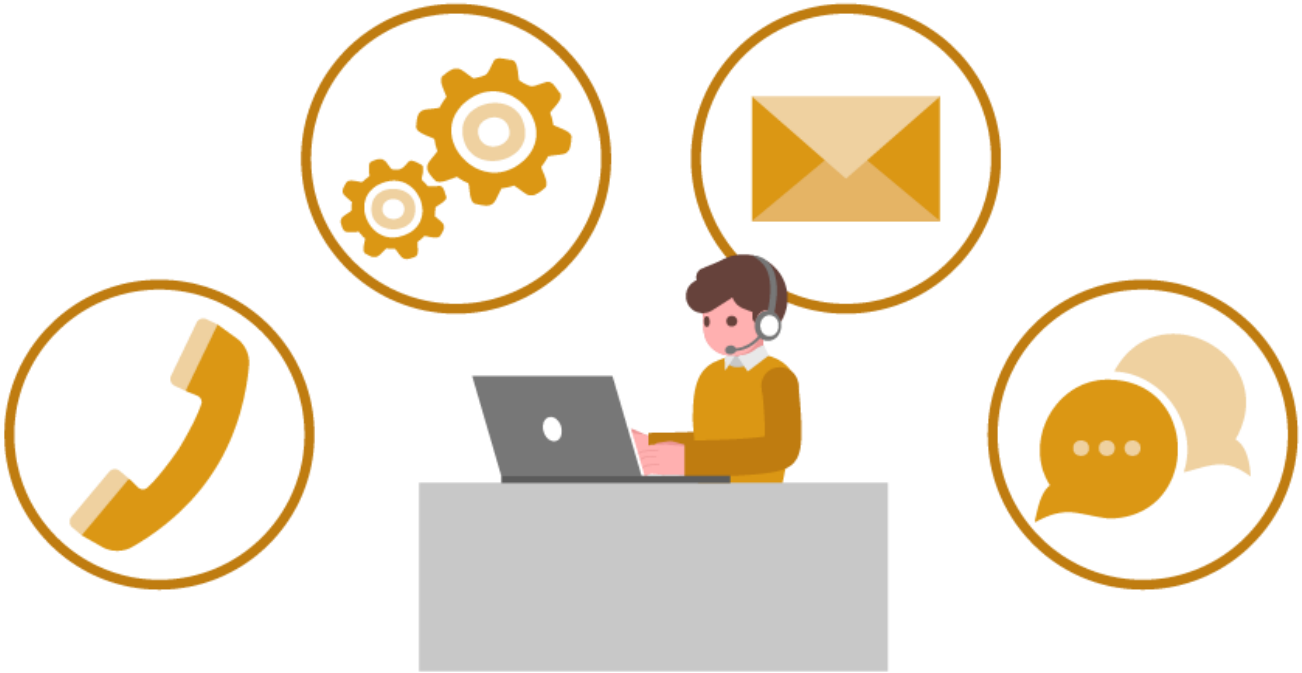
(C) AMIYA Corporation

その他 相談窓口

不審なメールを受信した際やウイルス感染が疑われる
症状が発生した際には、CSIRT窓口に相談ください。
担当スタッフがお客様に代わり調査いたします。

セキュリティ上の
「ムズカシイ」は
窓口に

相談



(C) AMIYA Corporation

その他 月次レポート/報告会

ユーザー企業のセキュリティ状況について
月次でレポーティング。
セキュリティ強化の取り組みを文書として残す
ことで、対外的にアピールする証跡にできます。

レポートの背景も
分かりやすく

解説

(C) AMIYA Corporation

工数課金ではなく、定額サービス

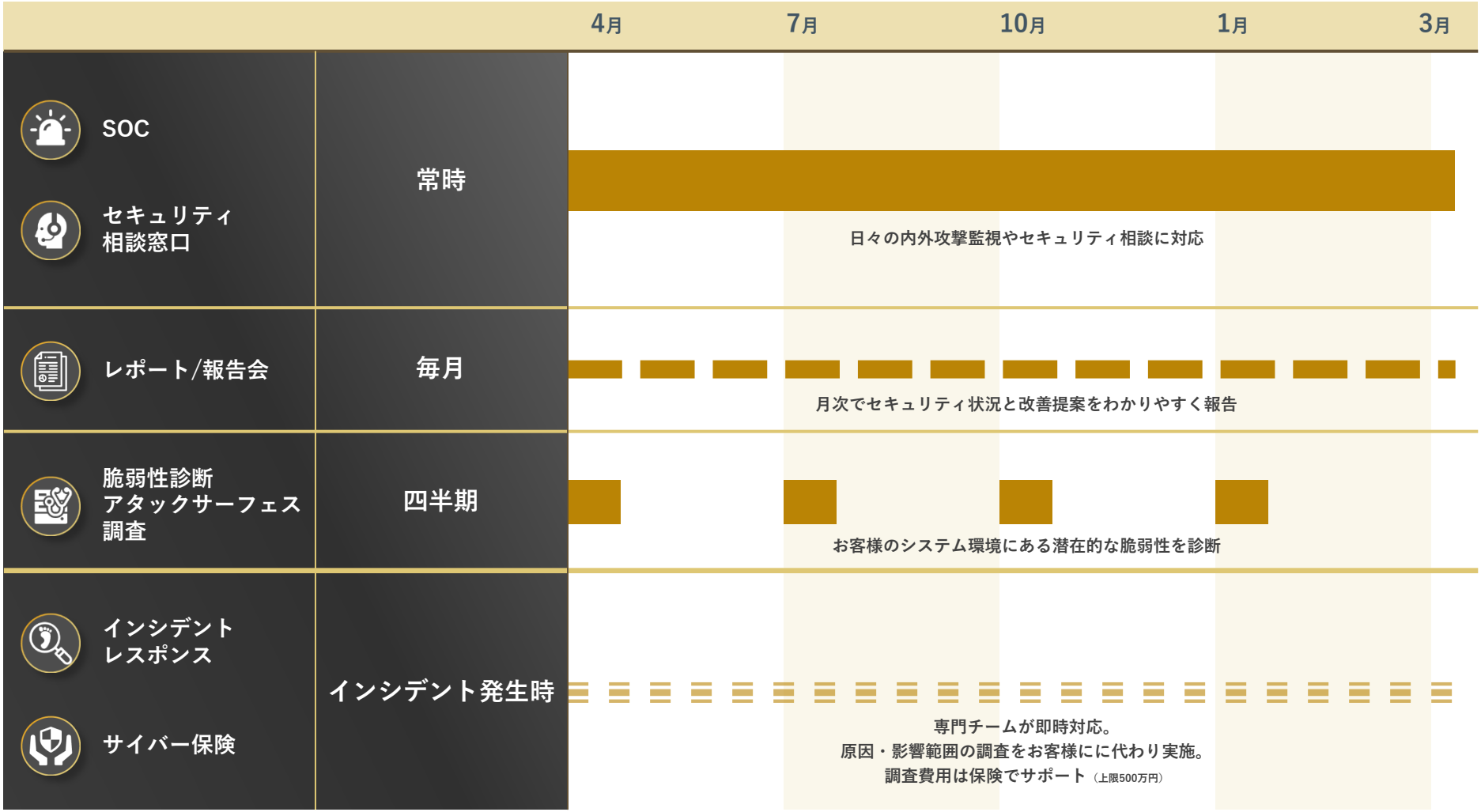
セキュリティは、対応が広範多岐に渡るため、人員の派遣や工数見積だと費用が膨大になりがち。
しかし当サービスは、

- 当社がもつセキュリティツール『ALog』を使用するため
- セキュリティエンジニアを現地派遣せず、遠隔で全て応対できるため

圧倒的なコストパフォーマンスをサブスクリプションで提供できます。

(C) AMIYA Corporation

サービススケジュール



(C) AMIYA Corporation

サービス価格/環境/提供条件　オンプレミス環境

利用料金

月額：￥420,000-（1,000アカウント迄）
：￥520,000-（1,001～2,000アカウント迄）
：￥720,000-（2,001～5,000アカウント迄）
※5,001アカウントを超える場合はご相談ください。

▶ オプション（サービス範囲の拡張）

別途ご相談

条件

＜オンプレミス環境でSIEM製品（ALog）を利用する場合＞

以下がサービス費用に含まれます。
・ALog オンプレミス版 基本利用料
・ALog オンプレミス版（5GB/day）
・ALogインストール作業
・ALog設定作業　※ただし、ログ取得対象の登録は10システム迄

以下はサービス費用に含まれません。お客様にて事前のご確認をお願いします。
・ALogをインストールするサーバのご準備
・ログ取得対象システムのログ出力設定
・遠隔サポート用のVPNツールをご準備

対応可能システム一覧

ファイルアクセスログ
（Windowsファイルサーバ / SharePoint / OneDrive / Box / Google ドライブ）

認証ログ（Active Directory / Microsoft Entra ID）

トラフィックログ（FortiGate/Palo Alto/SonicWall）

PCログ（SKYSEA / LANSCOPE）

メールログ（Exchange Online / Gmail(GoogleWorkspace)）

Proxyログ（i-Filter）

VPNログ（Verona / FortiGate）

＜共通＞

* 年間での契約となります。（自動更新）
* 当サービスは、リモート（遠隔）での対応となります。
* 対応時間は平日9 – 17時となります。
（対応時間外のアラート対応は、翌営業日となります）
* 対応可能システム一覧に記載のないシステムへの対応可否についてはご相談ください。

(C) AMIYA Corporation

サービス価格/環境/提供条件　クラウド環境

利用料金

月額：￥450,000-（1,000アカウント迄）
：￥550,000-（1,001～2,000アカウント迄）
：￥750,000-（2,001～5,000アカウント迄）
※5,001アカウントを超える場合はご相談ください。

▶ オプション（サービス範囲の拡張）

別途ご相談

条件

＜クラウド環境でSIEM製品（ALog）を利用する場合＞

以下がサービス費用に含まれます。
・ALog クラウド版 基本利用料
・ALog クラウド版 （5GB/day）
・ALog Cloudの設定作業　※ログ取得対象の登録は10システム迄

以下はサービス費用に含まれません。お客様にて事前のご確認をお願いします。
・ログ転送フォワーダー用サーバのご準備（別途必要な場合があります。）
・ログ転送フォワーダーのインストール作業および設定（別途費用にて対応可能）
・ログ取得対象システムのログ出力設定

対応可能システム一覧

ファイルアクセスログ
（Windowsファイルサーバ / SharePoint / OneDrive / Box / Google ドライブ）

認証ログ（Active Directory / Microsoft Entra ID）

トラフィックログ（FortiGate/Palo Alto/SonicWall）

PCログ（SKYSEA / LANSCOPE）

メールログ（Exchange Online / Gmail(GoogleWorkspace)）

Proxyログ（i-Filter）

VPNログ（Verona / FortiGate）

＜共通＞

* 年間での契約となります。（自動更新）
* 当サービスは、リモート（遠隔）での対応となります。
* 対応時間は平日9 – 17時となります。
（対応時間外のアラート対応は、翌営業日となります）
* 対応可能システム一覧に記載のないシステムへの対応可否についてはご相談ください。

(C) AMIYA Corporation

比較表

	セキュサポ	B社 ＳＯＣサービス（ミドルレベル）	C社 ＳＯＣサービス（ハイレベル）
脆弱性診断	○	△オプション	△オプション
相談窓口	○	△オプション	△オプション
サイバー保険	○	×	×
ログ管理製品	○ALog 標準提供	×別途購入必要	×初期費用で購入
ログ運用代行	○	×お客様が運用	△オプション
外部攻撃監視代行	○アラート＋ログ分析	○アラート	○アラート＋ログ分析
内部不正監視代行	○レポート+AI分析	×	×
監査対応レポート	○	×	×
24365検知	○自動メール通知	○メール通知・電話	○メール通知・電話
24365対応	×	△電話でお客様をサポート	○SOWに従い実施
インシデント対応支援	○	○	○
イニシャルコスト	ゼロ	製品導入 300万円	製品導入 800万円
ランニングコスト	40万円/月	30～40万円/月	80万円/月～

(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

セキュサポ

クラウドCSIRTサービス

AMIYA

(C) AMIYA Corporation