サイバー攻撃などによるインシデント発生時、企業にはどのような対応が求められるのか？

蔦 大輔 弁護士
（森・濱田松本法律事務所）

弁護士監修

法的観点で見るインシデント対応

Supervisor

監修

弁護士
蔦 大輔
（森・濱田松本法律事務所）

弁護士。2017 年から 3 年間、内閣官房内閣サイバーセキュリティセンター（NISC）にて法改正等を担当。2020 年より現職。総務省、警察庁、経済産業省などでサイバーセキュリティに関する検討会の有識者委員を歴任。主たる業務分野は、サイバーセキュリティ、個人情報保護・データ利活用、IT・ICT。サイバー攻撃予防のための取組、攻撃を受けた後の事後対応について豊富な知見を有する。近時の著書として、『類型別 不正・不祥事への初動対応』（中央経済社、2023 年）、『情報刑法 I サイバーセキュリティ関連犯罪』（弘文堂、2022 年）、『60 分でわかる！改正個人情報保護法超入門』（共著、技術評論社、2022 年）、『事例に学ぶサイバーセキュリティ 多様化する脅威への対策と法務対応』（経団連出版、2020 年）など。

目次 Index

はじめに ……2

当局への報告など

(1) 法令に基づく義務 ……3

(2) ガイドラインなどで推奨される事項 ……4

取引先等への対応

(1) 契約に基づく義務 ……5

(2) 損害賠償等の対応 ……5

公表等の対応 ……6

関係者との情報共有の意義 ……7

適切にログを保管し、管理する ……8

あらゆるログの一元管理を実現 …… 9-14

おわりに …… 15

はじめに

サイバー攻撃や不正アクセスなどのサイバーインシデントは、

企業の事業規模、事業内容にかかわらず発生する可能性がありますので、

どのような企業であっても決して他人事ではありません。

こうしたインシデントによって、保有する情報の漏えい、

ランサムウェアによるデータ暗号化、事業停止など、

様々な事態が生じるおそれがあり、企業は様々な対応を迫られます。

以下では、主に法的にどのような対応が必要になるかについて解説いたします。

当局への報告など

① 法令に基づく義務

サイバーインシデントについて、当局への報告が法律上の義務となる場合があります。実務上は、個人情報の保護に関する法律 26 条に基づく個人データ漏えい等発生時の個人情報保護委員会への報告義務（2022 年 4 月に施行）が問題となることが多いです（これは別途個別に詳細を紹介したいと思います）。

出典 (右図)：個人情報保護委員会ウェブサイト
https://www.ppc.go.jp/news/kaiseihou_feature/roueitouhoukoku_gimuka/

その他、様々な分野の事業者に適用される業法（電気通信事業法など）に基づき、サイバーインシデント等の事故発生時に、関係する当局への報告義務が課される場合があります。例えば、電気通信事業法（携帯電話事業や ISP に適用されます）では、通信の秘密の漏えいがあった場合や、一定の要件を満たす重大な事故が発生した場合に、総務大臣に報告する義務があり、また、電気通信事業報告規則に基づき、四半期毎に発生した事故を報告する義務があります。

また、サイバーインシデントが報道等で明るみになった場合などに、当局から問合せがあったり情報提供を求められるケースがあります。多くの場合は任意の情報提供等の要請と思われます。ただし、当局は、特定の業法に基づいて、事業者に対して、資料の提出や情報提供を求める法的権限を持っている場合があります。任意の要請に従わない場合、当局は、この法的権限に基づく情報提供・資料提出の要求を行う可能性があります。これに対応しないと、何らかの法執行（勧告や命令など）が行われる可能性がありますので注意が必要です。

当局への報告など

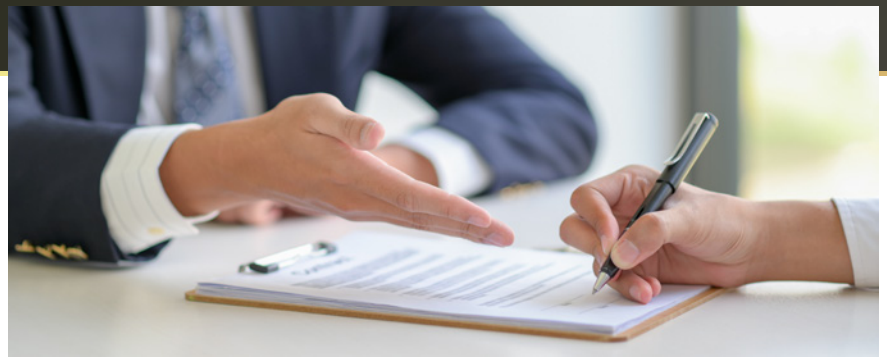
② ガイドラインなどで推奨される事項

サイバーセキュリティに関する様々なガイドラインなどに基づき、サイバーインシデント発生時に、関係する当局への報告が求められている場合があります。ガイドラインは、基本的に法的拘束力を持たないため、従わなかったことからといって直ちに何らかの不利益を被るわけではありませんが、ガイドラインに沿った行動を取ることが望ましい場合も多いため検討が必要です。

その他、サイバー攻撃を受けた事業者は、大抵の場合、サイバー犯罪被害者の立場にあります（不正アクセス禁止法違反など）。サイバー犯罪被害に遭った場合には、警察に通報・相談するといった対応も望ましいところです。被害届の提出や告訴はハードルが高いかもしれませんが、単に相談するなら相対的にハードルは低いとも言えます。

出典：警察庁ウェブサイト
https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/index.html

取引先等への対応



1 契約に基づく義務

企業は、事業活動を行う中で、様々な相手方と様々な契約を締結しています。業務委託契約、ライセンス契約など、データの取引を伴う契約も数多くあると思われます。その際には、契約条項に注意が必要です。

例えば、秘密保持に関する条項が契約書の中に含まれており、秘密情報と位置づけた情報が漏えい等した場合には、相手方への報告が契約上の義務となっているケースがあります。また、サイバー攻撃などの事故が発生した場合、または発生したおそれがあるときに、同じく相手方への報告が契約上の義務となっているケースもあります。契約上の義務である以上、それを守らなかった場合には契約違反として何らかの契約上の不利益を被るおそれがありますので注意が必要です。

2 損害賠償等の対応

サイバー攻撃を受けた企業は基本的に被害者という立場ですが、情報管理に過失があったことがサイバー攻撃の原因であり、それによって第三者が損害を被った場合には、その第三者から損害賠償請求を受ける可能性があります。取引先から預かっているデータがサイバー攻撃による影響を受けてしまった（漏えいなど）場合にはこうした法的リスクについても注意が必要です。

公表等の対応

サイバー攻撃を受けた場合、法的な義務として公表が求められるケースは多くはないですが、上場会社の場合、サイバーインシデントが投資判断に著しい影響を及ぼす場合には、適時開示として公表が必要となる場合がありますし、その他ガイドラインで公表が推奨されている場合には、対応を検討する必要があります。

また、法令やガイドラインに基づき公表が必要とされているわけではないとしても、レピュテーションリスクなどを勘案して、注意喚起のため、報道などで既に被害が知られてしまったことについて説明するため、または広報のためなど、様々な目的・事情の下で任意に公表を行うことが望ましいケースもありますので検討が必要です。

サイバーインシデント発生時に求められる対応

Must

法的に義務のある対応

- 個人情報保護委員会への報告義務
- 特定業法に基づいた、当局への報告義務
  ※事業者に適用される該当業法がある場合
- 取引先等への対応義務
  ※契約に基づく義務、損害賠償等への対応など

Best

法的拘束力は持たないが従うのが望ましい対応

- ガイドラインに基づいた対応

Better

後の事を考えると実施するのが望ましい対応

- 警察への被害届提出 (ないしは相談)
- 公表

関係者との情報共有の意義

以上のとおり、サイバーインシデントの発生時に法的にどのような対応が必要になるかについていくつか例を挙げてきました。ここで紹介した様々な制度等については、2023 年 3 月 8 日に公開された「サイバー攻撃被害に係る情報の共有・公表ガイダンス」(※) にも詳細が記載されていますので、そちらも参考にしていただければと思います。当局への相談や報告を行う中でログの提供などを求められるケースがありますので、義務を果たす、または要請にこたえるためには、適切なログの保存が重要です。

さらに、上記ガイダンスでは、サイバー攻撃に関する技術的な情報について、関係者と「共有」することも主たるテーマの一つです。情報共有は、関係者に情報を共有してそのフィードバックを受けることによって、インシデント対応に必要な情報を得ることや、他組織が同じ攻撃を受けることを予防するという意義があります (ガイダンス Q1) ので、その観点でも、各種ログ等を適切に保存し、情報共有に備えておくことが重要と考えられます。

(※) サイバー攻撃被害に係る情報の共有・公表ガイダンス
https://www.nisc.go.jp/pdf/council/cs/kyogikai/guidance2022_honbun.pdf

報告義務を果たすためにも

情報提出要請に応えるためにも

フィードバックにより、対応に必要な情報を得るためにも

他組織が同じ攻撃を受けることを予防するためにも

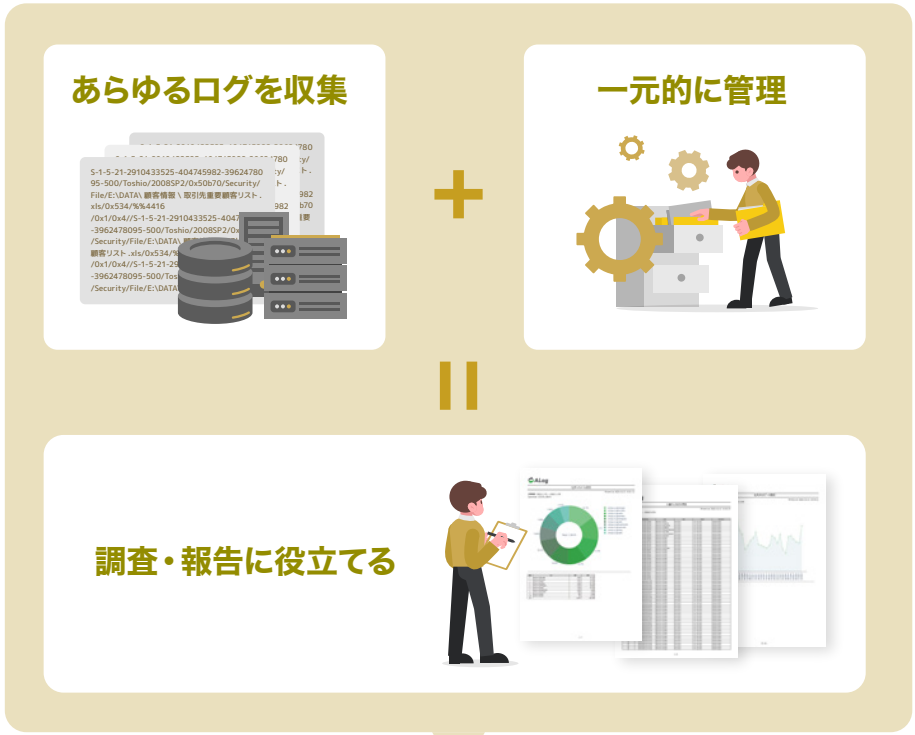
適切なログ保管と管理が必要不可欠

適切にログを保管し、管理する

では、適切なログ保管と管理とはどのようなものなのでしょう？ここからは具体的なログ管理方法について解説していきたいと思います。

まず第一に必要となる要素、それはなんといってもログの保管。PC、サーバ、ネットワーク機器、クラウドサービスなど情報提出の為に必要十分な種類のログをきちんと収集し、適切な期間保管しましょう。そして第二に、収集したログデータを必要な時に必要な分だけすぐに取り出せる状態にしておくこと。これもまた非常に大事なポイントです。システムが吐き出す生のままのログデータは非常に膨大。

ファイルに1回アクセスしただけでも
約20行程のイベント情報が出力されて解読困難・・・



ただただログを取り貯めているというだけでは「いざという時、必要な状況が探せない…」、「他システムのログと突き合わせてログを相関分析できない…」というような事態に陥りかねません。ログ管理ツールなどを活用しながら、収集したログは一元的に管理することが望ましいと言えます。

あらゆるログの一元管理を実現

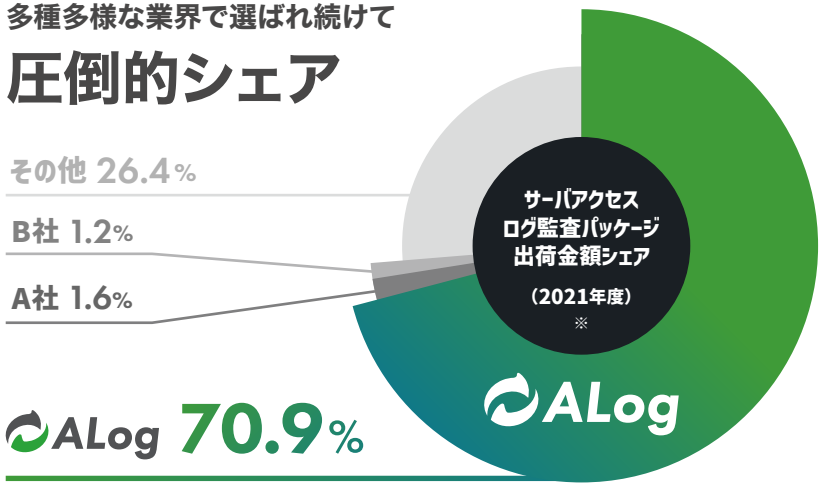
網屋のALogを利用すれば、あらゆるITシステムのログを自動で収集、一元的に管理することができます。

「ログ管理の難しいをカンタンに」を、コンセプトに開発されており、たとえ専門知識やノウハウがなくとも、誰でもカンタンに高度なログ管理を実現できるのが特徴です。

こんな企業にご利用いただいています

多種多様な業界で選ばれ続けて

圧倒的シェア



ALog 70.9%

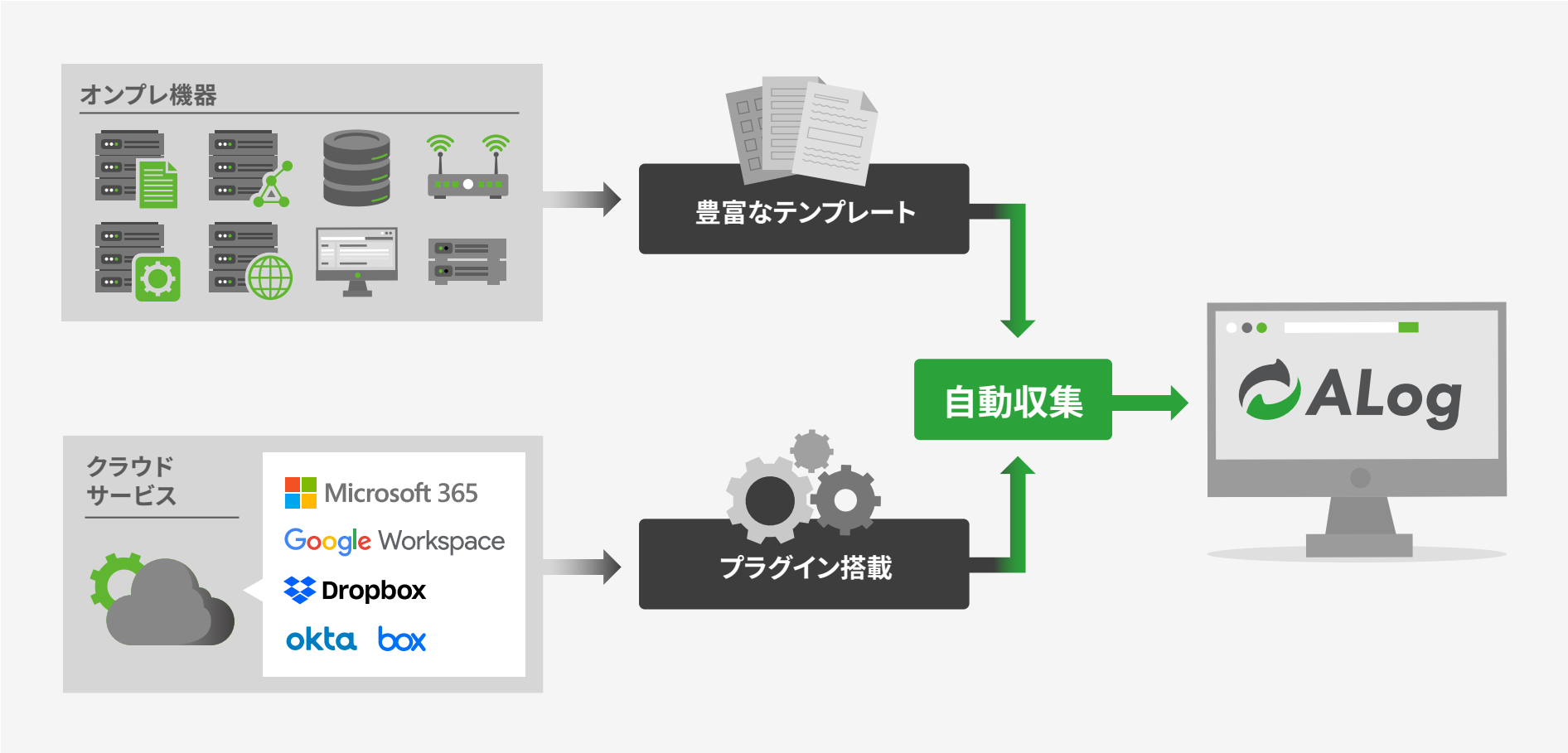
※出典：https://mic-r.co.jp/mr/02620/　デロイト トーマツ ミック経済研究所
「内部脅威対策ソリューション市場の現状と将来展望 2022 年度」2023 年 01 月 発刊

POINT 1

オンプレからクラウドまであらゆる種類のログデータを自動で収集

各種サーバやネットワーク機器など、オンプレ環境の様々なログを自動取得するためのテンプレートをご用意。

クラウドサービスにおいても、API を利用した収集プラグインが実装されており、オンプレ環境と同様にカンタンにログが取り込めます。



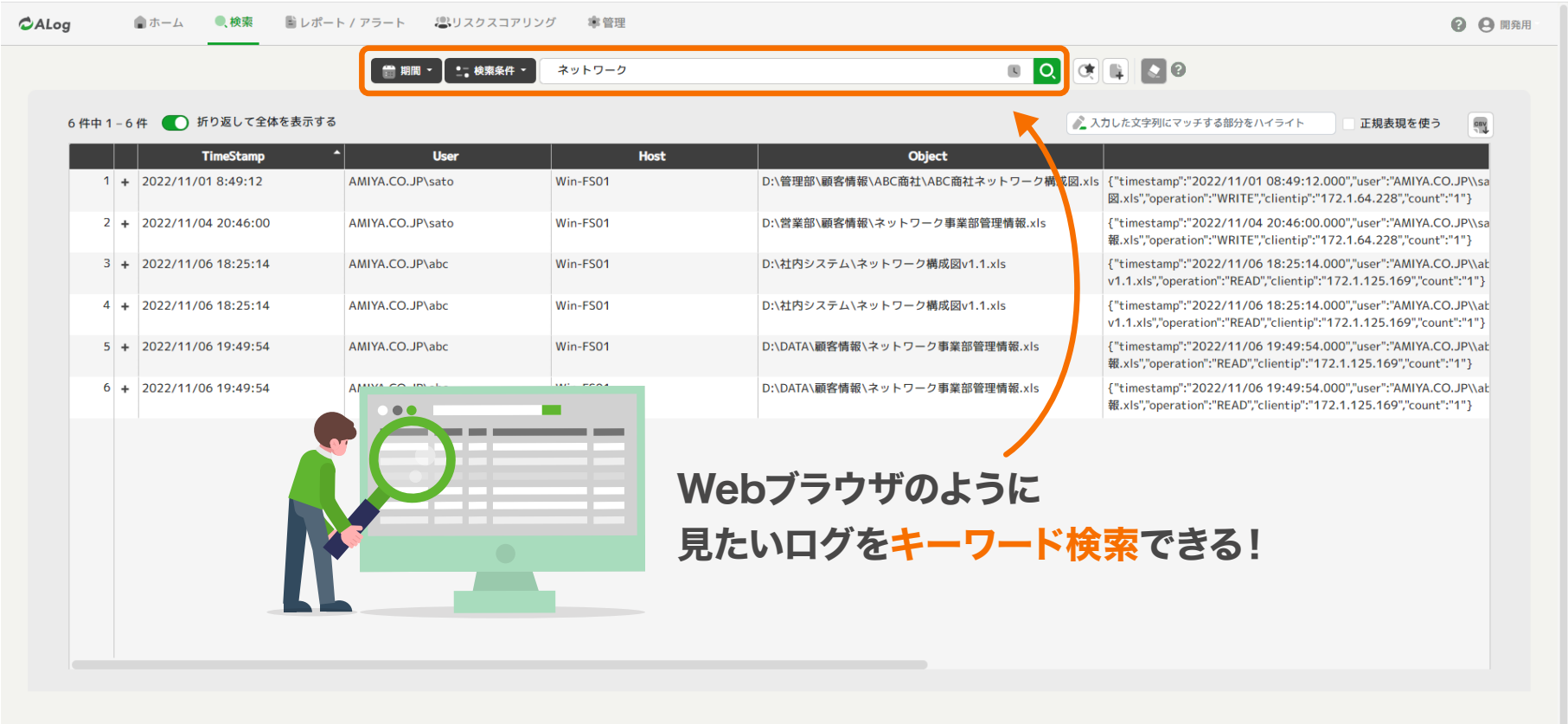
POINT 2

直感的な検索画面と高速処理で欲しいログにすぐ辿り着ける

直感的な検索インターフェースで、思いのままに欲しいログが探せます。

また長期保管や広範囲のログ取得により、保管したログボリュームが大量になっても並列処理により、

安定した検索速度を維持できるので、欲しいログにすぐに辿り着くことが出来ます。



POINT 3

使い勝手の良さにこだわった様々な機能で誰でも“カンタンに”ログ管理

ALog には、使い勝手の良さにこだわった様々な機能が標準で備わっています。
例えば、特許取得のログ翻訳変換技術や AI によるリスクスコアリング機能もそのひとつ。
専門知識やノウハウがなくとも、誰でも“カンタンに”高度なログ管理を実現できます。

特許取得のログ翻訳変換技術

＊特許第 6501159 号

複雑で膨大な Windows イベントログからアクセス記録を抽出。
「いつ・誰が・何をしたか」誰でも一目でわかる”アクセスログ”に出力します。

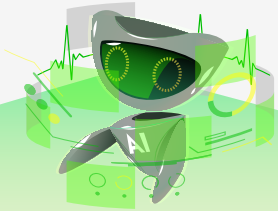
ログを 抽出 + 解析 + 要約

いつ　だれが　どのファイルに　何をした

日時	ユーザー	サーバ	ファイル	操作
2022/09/29 15:44:19.825	amya Sasaki	amyfs001	D:\fsvol1\営業部\重要顧客リスト.xls	READ
2022/09/28 23:43:21.422	amya Yamada	amyfs001	D:\fsvol1\企画部\FY13事業計画.doc	WRITE
2022/09/28 12:45:02.259	amya\Sato	amyfs003	D:\fsvol1\経理部\給与明細_田中.xls	DELETE
2022/09/27 02:38:12.245	amya Akagi	amyfs002	D:\fsvol1\営業部\製品別購入者一覧.xls	WRITE

AIによるリスクスコアリング機能

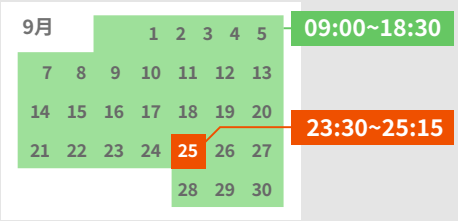
AI が膨大なログデータからユーザー毎の普段の行動パターンを機械的に学習、
いつもと違う行動をインシデントの予兆と捉え自動で通知します。



普段との違いで見つかる 内部不正

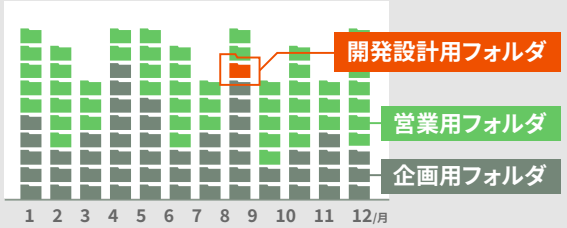
いつもと違う時間のアクセス

佐藤さんのデータアクセス



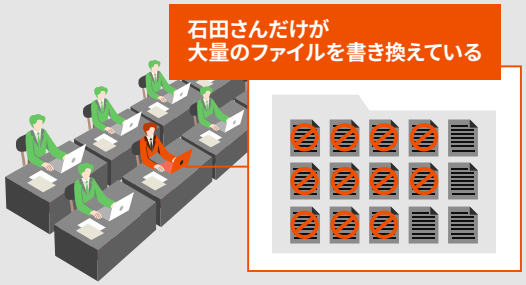
いつもと違うフォルダへのアクセス

鈴木さんのフォルダアクセス



普段との違いで見つかる 外部攻撃

ランサムウェアが引き起こすファイルの暗号化



そうは言ってもやっぱり人手が足りない…

→ ALog はログ管理業務もお任せできます！

運用お任せ「ALog MDRサービス」

長年ログと向き合ってきたメーカーだからこそできる、ログ管理の MDR サービス。
そのノウハウを駆使して企業のセキュリティ対策をサポートします。

※ ALog MDR サービスのご利用には、クラウド版の ALog「ALog Cloud」のご契約が必要となります。

おわりに

サイバー攻撃などによるインシデント発生時、
企業には顧客や取引先などとの契約内容に沿った対応が迫られる他、
個人情報保護委員会や特定業法に基づいた当局への報告義務を果たすことが求められます。

なお当局への相談や報告を行う中で、影響・被害範囲の特定や
状況把握に欠かせないログデータの提出を求められるケースが多く発生します。
その為、義務を果たす、または要請に応える為には、
いかなる企業も日頃から適切な範囲のログを適切な期間、保管しておかなければなりません。

ただし一口にログ管理といっても、様々なシステムやサービスのログを
それぞれ別々に取り貯めているだけでは、求められるログデータを必要時すぐに提出することは困難です。
後半に紹介した ALog のようなログ管理ツールの導入も検討しながら、
一元的なログ管理で有事の際に備えておくことが重要です。

明日起こるかもしれない、サイバーインシデントに備えて

はじめよう！ログ管理

ALog

詳しい製品概要資料をご覧になりたい方はこちら

製品概要資料ダウンロード（無料）

詳しい製品のご紹介や、無料トライアル体験を
ご希望の方は以下にお問い合わせください

電話でのお問い合わせ

03-6822-9996

メールでのお問い合わせ

bv-sales@amiya.co.jp

株式会社網屋　データセキュリティ事業部

Secure the Success.

網屋の事業は、セキュリティ。

セキュリティ製品やサービスを自ら開発・製造・販売する、セキュリティの総合プロバイダです。

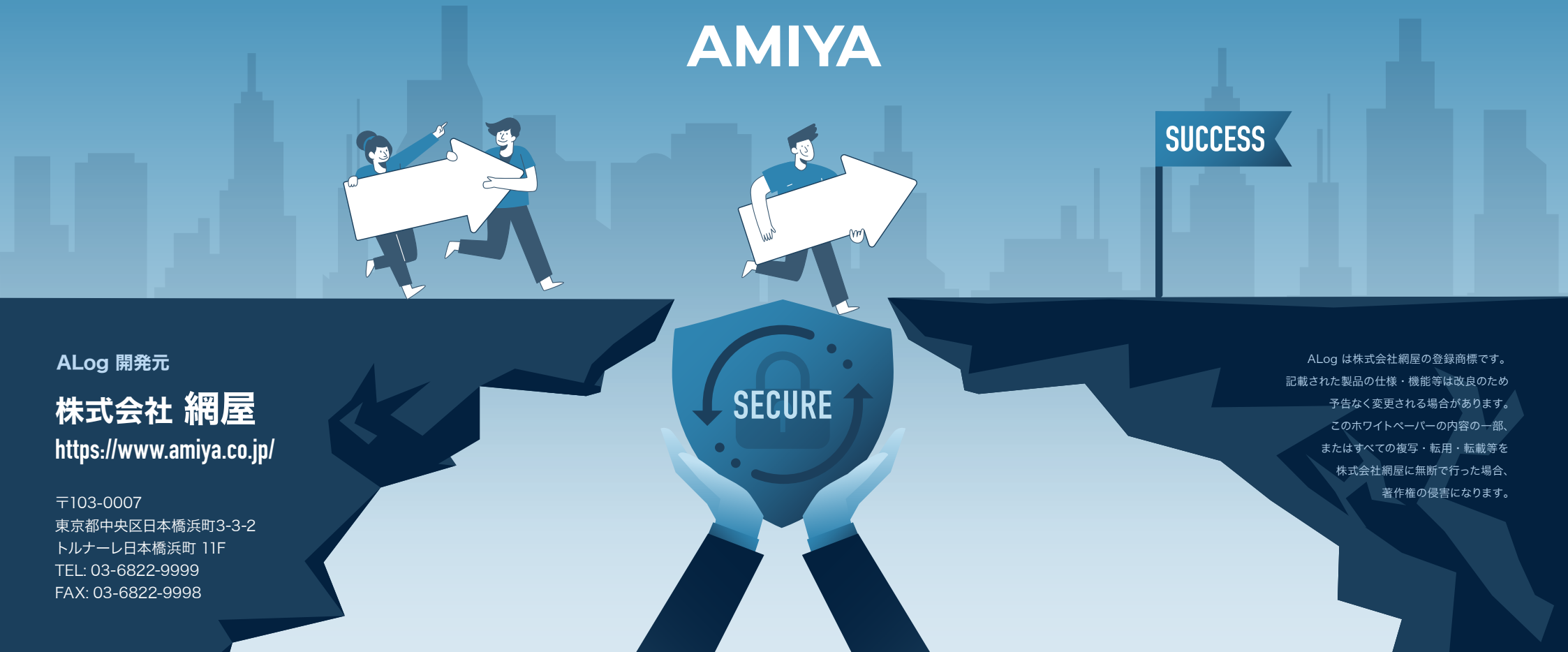
サイバー攻撃は、経済的余裕度に関係なく、全ての事業法人がターゲットになります。

サイバー攻撃の脅威を「セキュリティの自動化」で解決し、

高水準のセキュリティを誰でも享受できる社会を創りたい。

それが私たちのアイデンティティです。

AMIYA



ALog 開発元

株式会社 網屋

https://www.amiya.co.jp/

〒103-0007
東京都中央区日本橋浜町3-3-2
トルナーレ日本橋浜町 11F
TEL: 03-6822-9999
FAX: 03-6822-9998

ALog は株式会社網屋の登録商標です。
記載された製品の仕様・機能等は改良のため
予告なく変更される場合があります。
このホワイトペーパーの内容の一部、
またはすべての複写・転用・転載等を
株式会社網屋に無断で行った場合、
著作権の侵害になります。