漏えいのおそれも
報告義務対象!?

監修
蔦 大輔 弁護士
（森・濱田松本法律事務所）

サイバーセキュリティ専門弁護士が解説！

個人情報保護法に基づいた
個人データ漏えい時の対応について

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

個人情報の保護に関する法律 (個人情報保護法) に基づき、
一定の要件を満たす個人データの漏えい、
滅失または毀損（以下「漏えい等」といいます）が発生した場合、
個人情報保護法（以下単に「法」といいます）26 条に基づき、
個人情報保護委員会に報告する義務と、本人に通知する義務が課されます。
（2022 年 4 月 1 日から施行）

サイバーインシデントは、予期せぬタイミングで突発的に発生します。
外部からのサイバー攻撃やランサムウェアへの感染はもちろん、
メールの誤送信、USB メモリの紛失、（元）従業員による顧客名簿等の
機密データの持ち出しなど、個人データの漏えい等を引き起こす
インシデントには様々なものがあります。
実務上、サイバーインシデント発生時には、
個人情報保護法に基づく対応を求められるケースが多いため、
以下では、これらの義務について解説します。

どのような場合に報告等が必要か

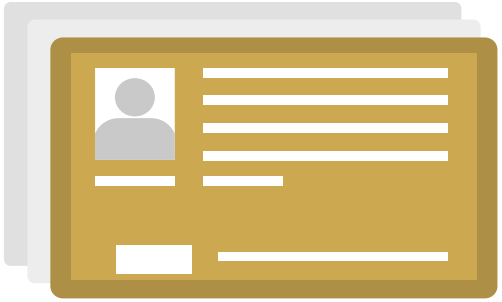
個人情報保護委員会への報告等が必要かどうかは、「個人データ」か、「漏えい等」に該当するか、施行規則に定める「報告対象事態」に該当するかといった要素を検討する必要があります。

1 個人データ

義務の対象となるのは、「個人データ」の漏えい等です。個人データとは、「個人情報データベース等を構成する個人情報」（法 16 条 3 項）です。例えば、顧客の名刺情報が漏えい等したとしても、それが名刺管理ソフト等で名簿データとして管理されたものでない場合、漏えい等した情報は、「個人情報」ではありますが、「個人データ」ではありません。このように、個人情報なのか個人データなのかは、事業者による情報の管理状況によって変わります。

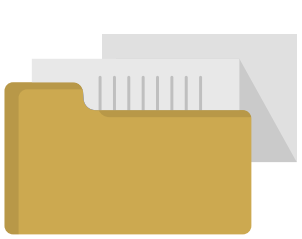
バラバラな状態なら

個人情報



容易に取り出せる状態になると

個人データ



名刺を50音順にファイリング

名刺をデータベース化

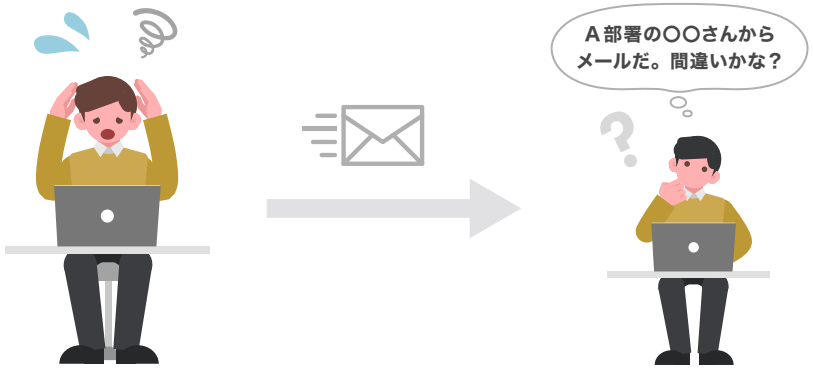
名刺をリスト化

どのような場合に報告等が必要か

2 漏えい

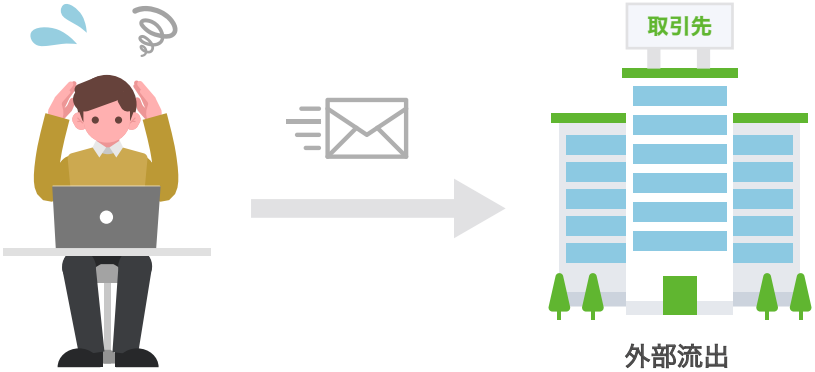
個人情報保護委員会のガイドラインによれば、個人データの「漏えい」とは、個人データの外部流出をいうとされています。例えば、メールを誤送信したケースで、部署Aに送るはずのメールを部署Bに送ってしまった場合、「外部」への流出はないので漏えいには該当しないと考えられます。

部署Aに送る内容を部署Bに送信



漏えいには該当しない

部署Aに送る内容を外部に送信



漏えいに該当する

3 報告対象事態と漏えい等の「おそれ」

施行規則では、以下の４つが報告対象事態とされています。

① 要配慮個人情報（例：医療情報や犯罪被害にあった事実など）を含む個人データの漏えい等
② 財産的被害が生じるおそれがある個人データ（例：クレジットカード番号など）の漏えい等
③ 不正な目的をもって行われたおそれのある（サイバー攻撃、機密情報の持ち出しなど）個人データの漏えい等
④ 1,000 人を超える個人データの漏えい等

サイバー攻撃は③に該当することとなります。
また、これらは、確定的な漏えい等のみならず、漏えい等の「おそれ」も含まれています。
「おそれ」とは、漏えい等が疑われるものの確証がない場合であり、個別の事案ごとに蓋然性を考慮して判断するとされています。

例えば、サイバー攻撃の場合においては、
個人データが格納されているサーバ等において、
情報を窃取する振る舞いが判明しているマルウェアの感染が確認された場合などが、
漏えい等の「おそれ」がある事例として挙げられています。

報告に関する手続

個人情報保護委員会への報告は、速報と確報の２段階に分けて行う必要があります。速報は、報告対象事態を知ったときから３～５日以内が目安とされ、確報については、原則は30日以内(サイバー攻撃等の場合は60日以内)に行う必要があります。

ただし、60日では調査が終わらないこともあります。確報の時点で、合理的努力を尽くしたけれども全ての事項を報告できない場合は、その時点で把握している内容を報告し、判明次第、後で追完することも可能とされています。

個人情報保護委員会への報告

まずは**速報**(新規)

発覚日から、**3~5**日以内

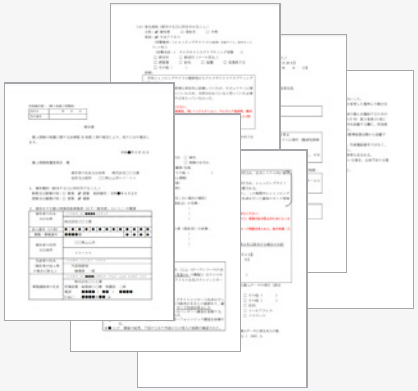
発覚したら、まずは速やかに報告

↓

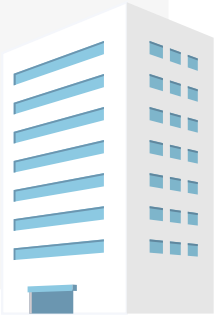
次に**確報**(続報)

発覚日から**30**日以内

サイバー攻撃等の場合は**60**日以内



出典：個人情報保護委員会ウェブサイト
https://www.ppc.go.jp/files/pdf/kisairei_unauthorized_access_minkan.pdf



公表は義務なのか

個人データの漏えい等発生時に、義務として公表が必要かというご質問を多く受けますが、個人情報保護法上、公表は望ましい措置とはされていますが義務ではありません。

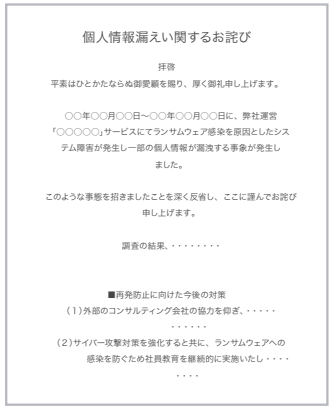
ただし、個人データの漏えい等発生時に、個人情報保護委員会への報告のほか、本人への通知も義務として必要です。その際、保有するデータが古くて本人に連絡ができない場合は、代替措置をとる必要があり、その際に公表が一つの選択肢となります。

義務

個人情報保護委員会への報告

義務

本人への通知



個人情報漏えい関するお詫び

拝啓
平素はひとかたならぬ御愛顧を賜り、厚く御礼申し上げます。

○○年○○月○○日～○○年○○月○○日に、弊社運営「○○○○○」サービスにてランサムウェア感染を原因としたシステム障害が発生し一部の個人情報が漏洩する事象が発生しました。

このような事態を招きましたことを深く反省し、ここに謹んでお詫び申し上げます。

調査の結果、・・・・・・・・

■再発防止に向けた今後の対策
（1）外部のコンサルティング会社の協力を仰ぎ、・・・・・・・・・・・・
（2）サイバー攻撃対策を強化すると共に、ランサムウェアへの感染を防ぐため社員教育を継続的に実施いたし・・・・・・・・

義務なし

世間への公表

ただし

連絡が取れない人がいる場合
公表も考えるべき

エビデンスとしてのログの重要性

近年、個人情報保護委員会は、個人データの漏えい等の報告に関して、エビデンスを重視する傾向があるように思われます。

例1

例えば、サイバー攻撃事案の場合には、セキュリティベンダへのフォレンジック調査など、第三者に調査を委託しているかどうかが報告フォームのチェック項目に入っています。また、同委員会は、エビデンスをもって漏えい等がないことを確認できれば、漏えい等はないと判断できるという考え方を示しています。

例2

例えば、設定ミス等でインターネット上で誰でも個人データが閲覧できる状態になってしまった場合でも、閲覧不能とするまでの間に実際に第三者が閲覧していないことをアクセスログ等で確認できれば、「漏えい」には該当しないとされます。逆に、ログ等でそれが確認できなければ、漏えいのおそれに該当しうるとされてしまいます。

ログは情報流出の有無を明らかにする手掛かりとなりうる

エビデンスとしてのログの重要性

また、サイバー攻撃事案においては、情報窃取の振る舞いを行うマルウェアに感染すると漏えい等の「おそれ」があるとされていますが、単にマルウェアを検知したことをもって直ちに漏えいのおそれがあるというわけではなく、防御システムによるマルウェアの実行抑制の状況や外部通信の遮断状況等について考慮したうえで漏えいの「おそれ」があるかどうかを判断することとされています。

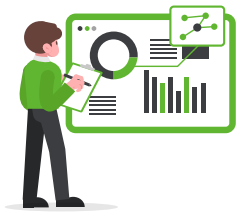
以上のことから、サイバー攻撃を受けたとき、何らのログも取得していないまたは残っていないために情報が漏えいしたかどうかは不明という場合、基本的には漏えいのおそれがあるという前提で対処する必要があると考えられます。適切に各種ログを取得し、いざというときに適切な判断を下せるような体制を整えておくことが重要です。

適切なログ管理で重要なこと

ログ取得

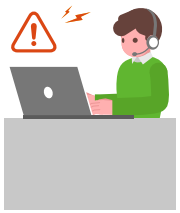
まずはログを取得してまとめることが重要です。様々な種類のログを収集し、保管することは有事の際に役立ちます。

レポート分析



目的に応じて加工・分析することで、セキュリティインシデントやシステム障害の調査、業務改善等に役立てることができます。

アラート監視



ログを常時監視し、異常を検知した際にはアラート通知することで外部からの攻撃や内部不正などのトラブルを早期に発見できます。

安全な保管

暗号化等を用いてログの改ざんから守りましょう。保管期間はセキュリティポリシーに沿って任意で設定できることが大切です。

NEXT どのようなログを取得すべき？ >>

何のログを取得すべきか

では、具体的にはどのようなログを取得すれば良いのでしょうか?

企業を支えるシステムは、DX、クラウド化、テレワーク導入 など多種多様な目的に応じて年々増加しています。

そのため、ログ管理をはじめるにあたって、様々なシステム の中の何のログを取得すべきか?という悩みがつきもの。

適切なログ管理を実現するために、以下の表なども参考にしながらまずは取得すべきログを明確にしましょう。

システム別のログ活用法

システム	活用シーン	記録内容例
Firewall	サイバー攻撃対策	• HTTP、NTTPS等のプロトコロによる外部への通信 • ぜい弱なPCや内部サーバーの探索 • 通過した通信、または拒否された通信
	障害原因調査	• ネットワーク障害検知 • 通信ボトルネックの特定
IDS/IPS	サイバー攻撃対策	• IDS/IPSが検知した、または検知から漏れた通信
プロキシサーバ	サイバー攻撃対策	• Webプロキシサーバを介さない外部への通信 • HTTP、HTTPS等のプロトコルによる外部への通信 • Webサーバが利用者から受け取った入力内容
	内部不正対策	• 転職サイト閲覧
	勤務実態の把握	• SNSサイトの閲覧

何のログを取得すべきか

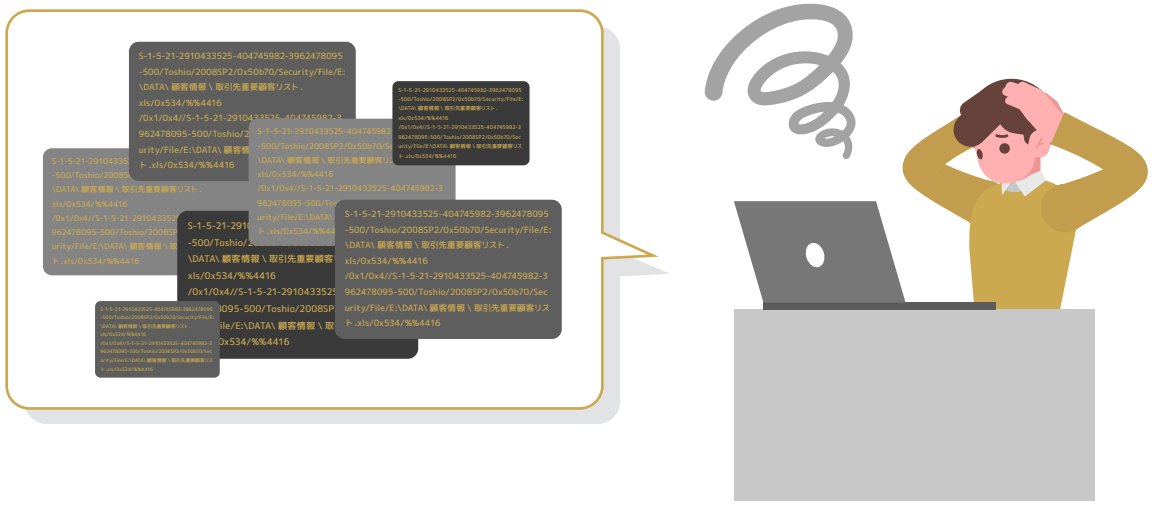
システム	活用シーン	記録内容例
DHCPサーバ	サイバー攻撃対策	• 被害範囲の特定
DNSサーバ	サイバー攻撃対策 内部不正対策	• HTTP、HTTPS等のプロトコルによる外部への通信 • データの異常アップロードサイズ/回数
メールサーバ	サイバー攻撃対策	• なりすましメール • 実行ファイル添付メール
Active Directory	サイバー攻撃対策	• ファイルサーバなどへのアクセスや権限の奪取 • 情報システムへのログインログアウトなど認証の成功や失敗の記録 • 特権管理権限の利用 • 大量ログインの失敗 • ユーザアカウントの作成/削除
	勤務実態の把握	• ログオン/ログオフ
	監査報告	• 特権管理権限の利用

何のログを取得すべきか

システム	活用シーン	記録内容例
ファイルサーバ	サイバー攻撃対策	• ランサムウェアによる被害範囲の特定 • ファイル参照や、編集などの成功や失敗の記録
	内部不正対策	• ファイル参照や、編集などの成功や失敗の記録 • 退職予定者のファイルアクセス
データベースサーバ	サイバー攻撃対策 内部不正対策	• 規定外ツールによるDB操作 • アクセス失敗したユーザー • 発行されたSQLクエリ • アクセス頻度 • DBスキーマの変更・削除 • アカウントの変更・削除
アプリケーション	サイバー攻撃対策	• 発生したエラーの記録 • ユーザーによる予期しない操作の成功や失敗の記録
	内部不正対策	• 禁止サイトへのアクセス試行・履歴 • 外部デバイスへのコピー履歴
PC	勤務実態の把握	• PCの作動状況

適切にログを保管し、管理する

必要なログの種類があきらかになったら、次はそれらを適切な期間保管するとともに必要な時にすぐに取り出せる状態にしておくことが重要です。
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かつ複雑。
ただただ機器ごとに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。ログ管理ツールの活用も視野に入れることをお勧めいたします。



NEXT おすすめのログ管理ツール >>

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。

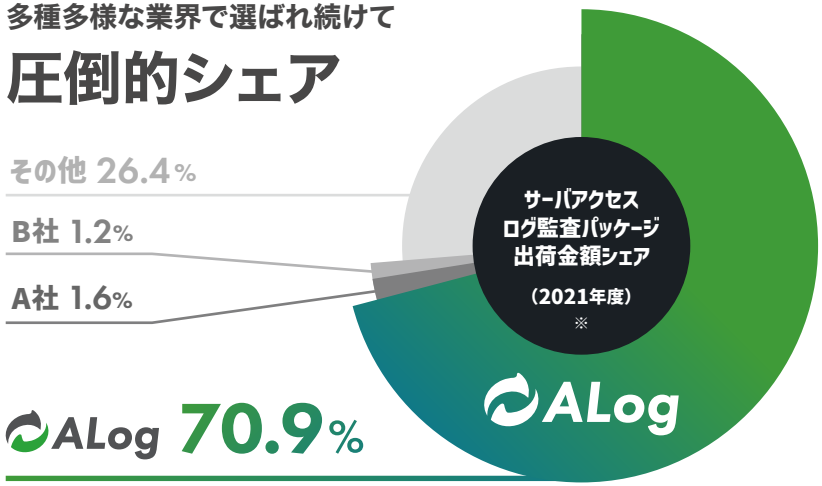
「ログ管理の難しいをカンタンに」を、コンセプトに開発されており、たとえ専門知識やノウハウがなくとも、誰でもカンタンに高度なログ管理を実現できるのが特徴です。

Panasonic　NISSHINBO　NTT Communications　MUSEE PLATINUM
トレイダーズ証券　KDDI　SBI証券　OBAYASHI
mixi GROUP　品川区　LANDNET　SEKISUI HOUSE
YAHOO! JAPAN　SUBARU　LINE株式会社

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に対応

オンプレからクラウドまで、あらゆるシステムのログデータに対応。

攻撃や内部不正の検知をはじめ、有事の際の調査、監査対応まで、マルチなシーンに活用できます。

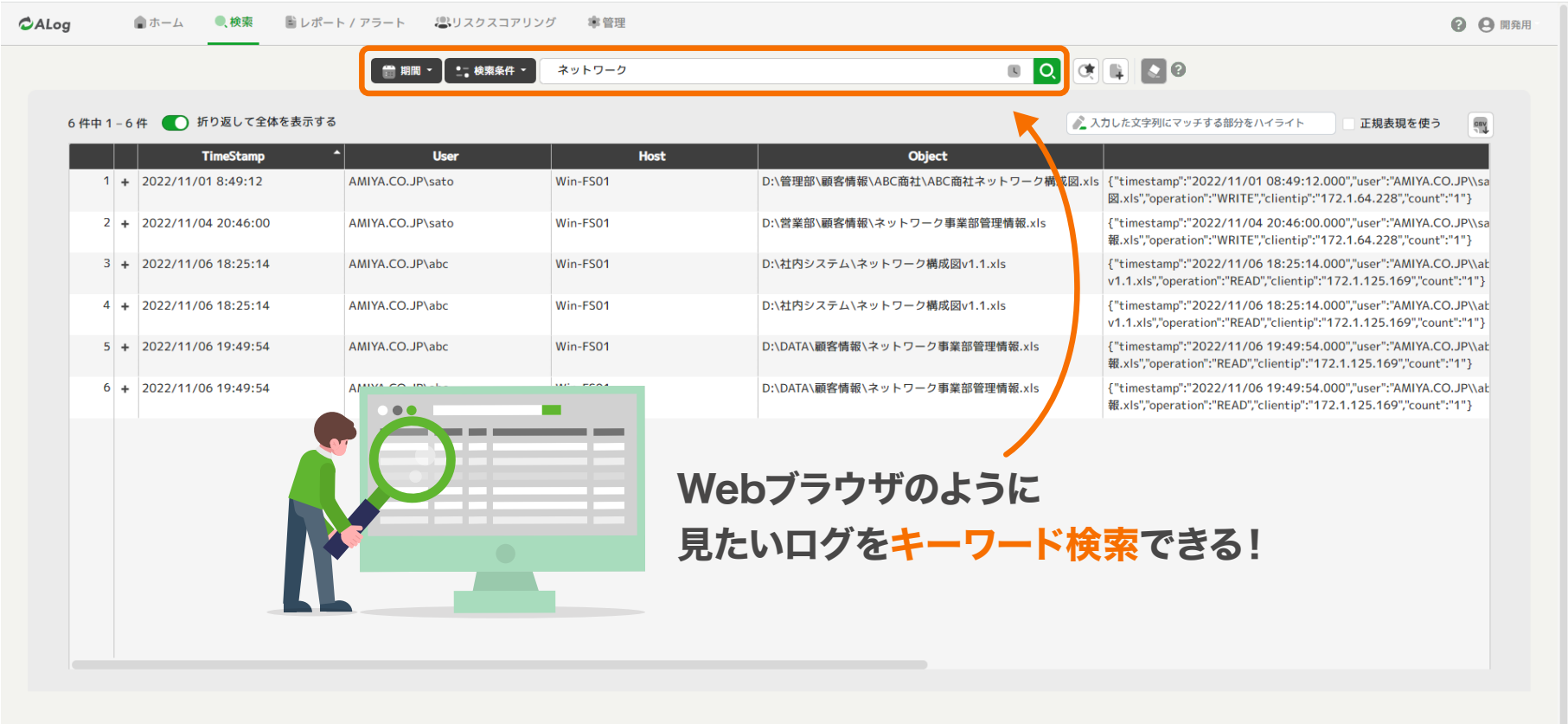
POINT 2

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

誰でも“カンタンに”ログ管理 特許取得のログ翻訳変換技術

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

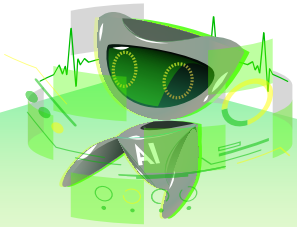
日時	ユーザー	サーバ	ファイル	操作
2022/09/29 15:44:19.825	amya Sasaki	amyfs001	D:\fsvol1\営業部\重要顧客リスト.xls	READ
2022/09/28 23:43:21.422	amya Yamada	amyfs001	D:\fsvol1\企画部\FY13事業計画.doc	WRITE
2022/09/28 12:45:02.259	amya\Sato	amyfs003	D:\fsvol1\経理部\給与明細_田中.xls	DELETE
2022/09/27 02:38:12.245	amya Akagi	amyfs002	D:\fsvol1\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

POINT 4

誰でも“カンタンに”ログ管理 AIリスクスコアリング機能

AIによるリスクスコアリング機能

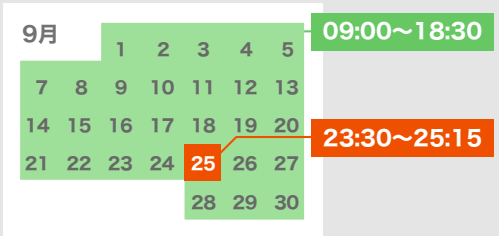
AIが膨大なログデータからユーザー毎の普段の行動パターンを機械的に学習、
いつもと違う行動をインシデントの予兆と捉え自動で通知します。



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

個人データは、確実な漏えいのみならずその「おそれ」が発覚した際にも、個人情報保護委員会への報告義務が発生します。
具体的には、３～５日以内の速やかな速報の提出と、30日以内の確報の提出です。（サイバー攻撃等の場合は60日以内）

個人情報保護委員会は、報告書を確認する際、エビデンスの有無を重要視する傾向が高く、
貴重なエビデンスとなりうるシステムログの取得および適切な管理は
企業運営において非常に重要な役割を担うという事がわかります。

しかしながら一口にシステムログの取得および適切な管理といっても、
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、個人データ漏洩事故に備えて

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

こちらもおすすめ！

セキュリティ資料 無料配布中

【弁護士監修】
法的観点で見るインシデント対応

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の発生時、企業には法的にどのような対応が必要になるか。弁護士蔦大輔氏監修のもとわかりやすく解説しています。

資料をダウンロード

これさえ見ればわかる！
ログ管理スターターガイド

ログは、企業のあらゆる課題解決に活用できる重要なデータです。本書では、ログ管理初心者向けに、ログがどのように活用できるのかを紹介していきます。

資料をダウンロード

サイバー攻撃の被害は
Active Directoryで最小化する！

あらゆるサイバー攻撃が AD を経由することに着目し、内部対策の中でも AD をテーマに、AD における対策や AD のログ管理などを解説していきます。

資料をダウンロード

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。

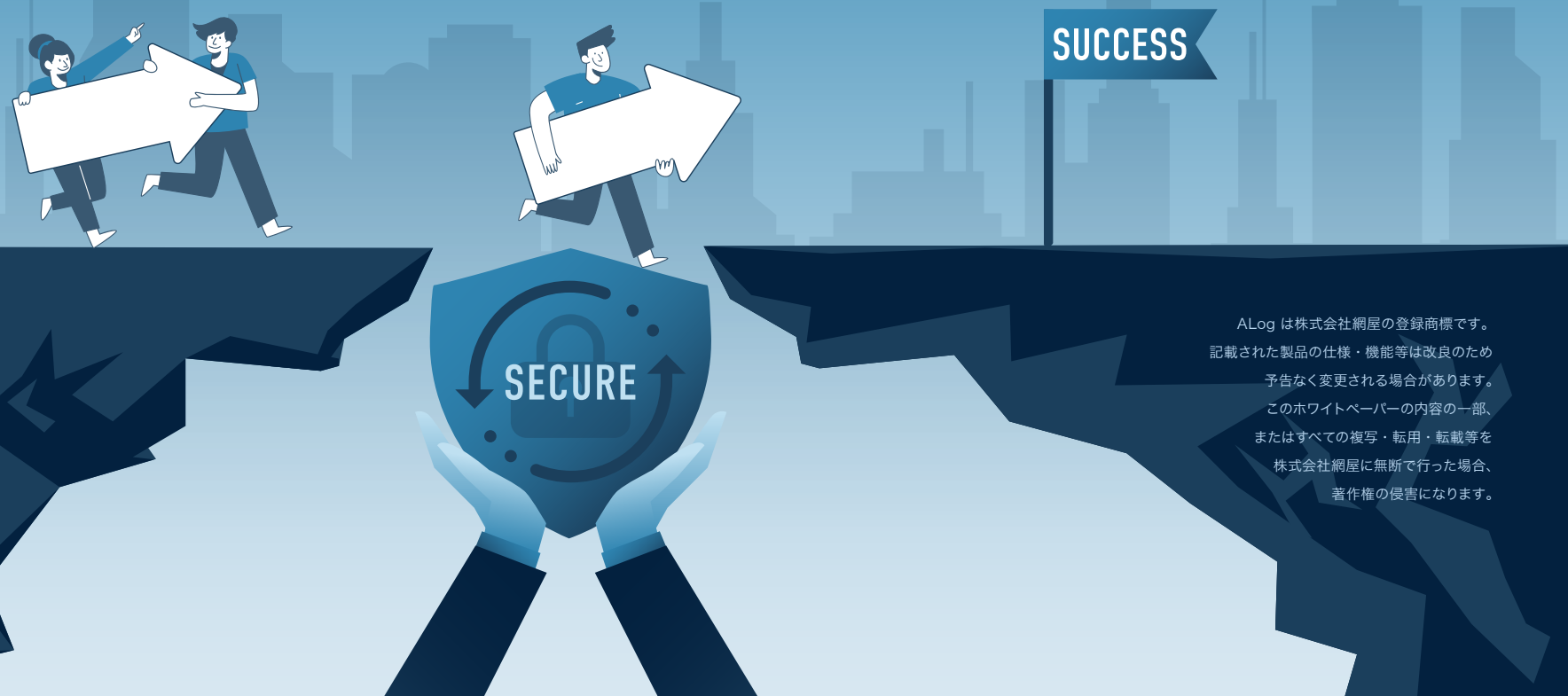
サイバー攻撃は、経済的余裕度に関係なく、全ての事業法人がターゲットになります。

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