AMIYA

自動車産業必見！

サイバー攻撃対策に欠かせない“ログ管理のポイント”を徹底解説！

自動車産業
サイバーセキュリティ
ガイドライン
にも対応！

目次 Index

目次 ····· 1

狙われる自動車産業 ····· 2-3

巧妙化するサイバー攻撃と被害状況 ····· 4-7

自動車産業サイバーセキュリティガイドライン ···· 8-9

CSFに沿った対策ポイント ····· 10-12

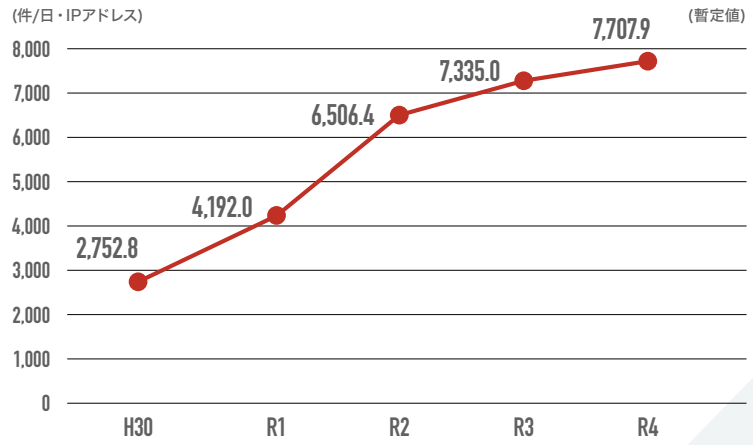
ガイドラインでも必須！ログの要求事項 ····· 13-16

ログ管理のベストプラクティス ALog····· 17-29

サプライチェーンを支える中堅・中小企業をターゲットに

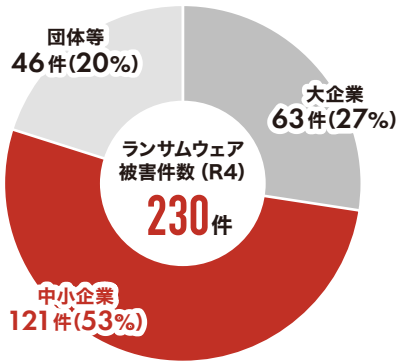
サイバー攻撃の多様化・複雑化に伴い、企業規模を問わずその被害は増加の一途を辿っています。中でも中堅・中小企業の製造業を狙ったサイバー攻撃が増加し、サプライチェーンに波及する事件が多発しました。中でも自動車産業を取り巻くサイバーセキュリティリスクが深刻化しており、本資料では自動車産業がいま取り組むべきサイバーセキュリティ対策について紹介していきます。

サイバー空間における脆弱性探索行為等の観測状況



前年推移　**372.9件増加 (105%)**

ランサムウェア被害の企業・団体等の規模別報告件数



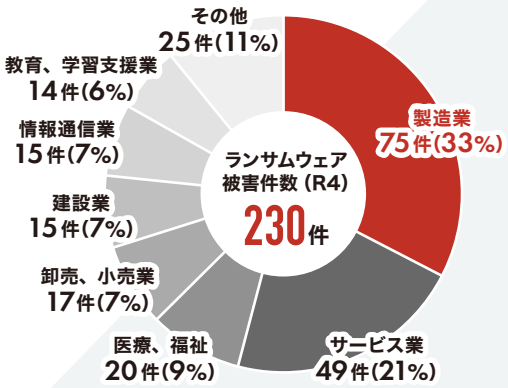
前年推移

大企業　：**14件増加 (129%)**

中小企業：**42件増加 (153%)**

団体　　：**28件増加 (256%)**

ランサムウェア被害の被害企業・団体等の業種別報告件数



前年推移

製造業：**20件増加 (136%)**

注：図中の割合は小数第一位以下を四捨五入しているため、総計が必ずしも 100 にならない。

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」https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_cyber_jousei.pdf
右上「【図表 19：センサーにおいて検知したアクセス件数の推移】」、左下「【図表１：企業・団体等におけるランサムウェア被害の報告件数の推移】」、右下「ランサムウェア被害の被害企業・団体等の業種別報告件数」より作成

自動車関連産業の就業人口は552万人

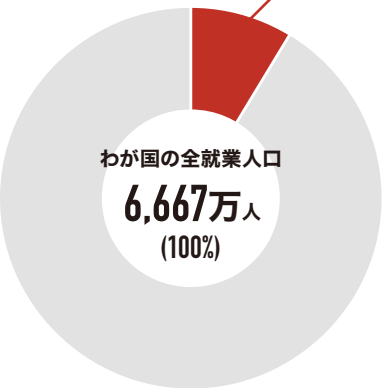
自動車産業は資材調達・製造をはじめ販売・整備・運送など各分野にわたる広範な関連産業を持つ総合産業です。
これら自動車関連産業に直接・間接に従事する就業人口は、当会の推計によると約552万人にのぼっています。

自動車関連産業と就業人口

自動車関連就業人口

552万人

(8.3%)



製造部門	890,000人
自動車製造業（二輪自動車を含む）	199,000人
自動車部分品・付属品製造業	670,000人
自動車車体・付随車製造業	21,000人

利用部門	2,718,000人
道路貨物運送業	1,651,000人
道路旅客運送業	514,000人
運輸に付帯するサービス業等	394,000人
自動車賃貸業	48,000人
郵便業	111,000人

関連部門	395,000人
ガソリンステーション	313,000人
損害保険	8,000人
自動車リサイクル	1,000人
駐車場業	73,000人

資材部門	501,000人
電気機械器具製造業	80,000人
非鉄金属製造業	19,000人
鉄鋼業	117,000人
金属製品製造業	37,000人
化学工業（塗料含む）、繊維工業、石油精製業	31,000人
プラスチック・ゴム・ガラス	150,000人
電子部品・デバイス製造業	32,000人
生産用機械器具製造業	5,000人
情報サービス業	30,000人

販売・整備部門	1,018,000人
自動車小売業（二輪車含む。新車・中古車・自動車部分品・附属品、等）	571,000人
自動車卸売業（二輪車含む。中古車・中古部品・自動車部分品・附属品、等）	203,000人
自動車整備業	244,000人

日本の就業人口の8%…

サイバー攻撃が多発する程

日本経済を支える産業に影響

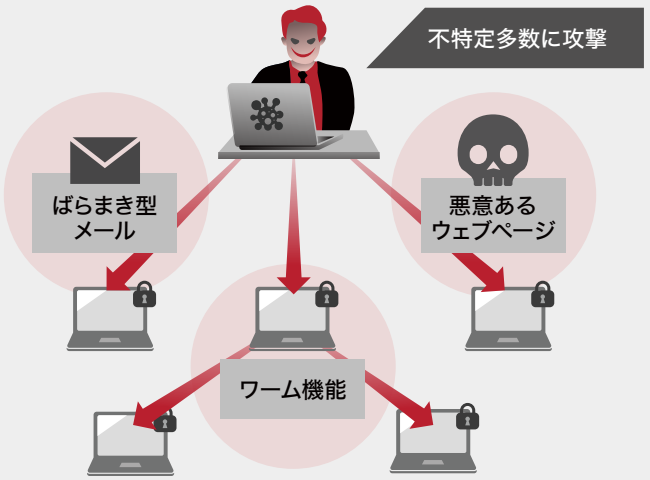
出典 ）一般社団法人 日本自動車工業会「日本の自動車工業」p3 より作成
https://www.jama.or.jp/library/publish/miojj/ebook/2022/MIoJ2022_j.pdf

事業継続を揺るがす攻撃

サイバー攻撃の中でもランサムウェアの手法が巧妙化しています。
新たなランサムウェアに一度でも感染すると、ITシステム全体が感染し業務停止を強いられ、事業継続を脅かす脅威になっています。

従来のランサムウェア攻撃

被害は感染デバイスのみ。事業継続リスクとしては限定的。



ばらまき型メール、悪意あるウェブページなどにアクセス、ランサムのマルウェア本体のダウンロード、感染を誘導します。
この時、感染拡大させるワーム機能が作動する前にネットワークより遮断することで、被害は感染端末のみとなり、**リスクとしては限定的**です。

新たなランサムウェア攻撃

ITシステム全体が停止。事業継続を揺るがすリスク。

VPNをはじめとするシステムの脆弱性を突いて社内ネットワークへの侵入後、ActiveDirectoryの管理者権限とグループポリシーを悪用し効率よく感染拡大させます。気付いたときにはITシステムが全停止していたなど、**事業継続を揺るがすリスク**になっています。

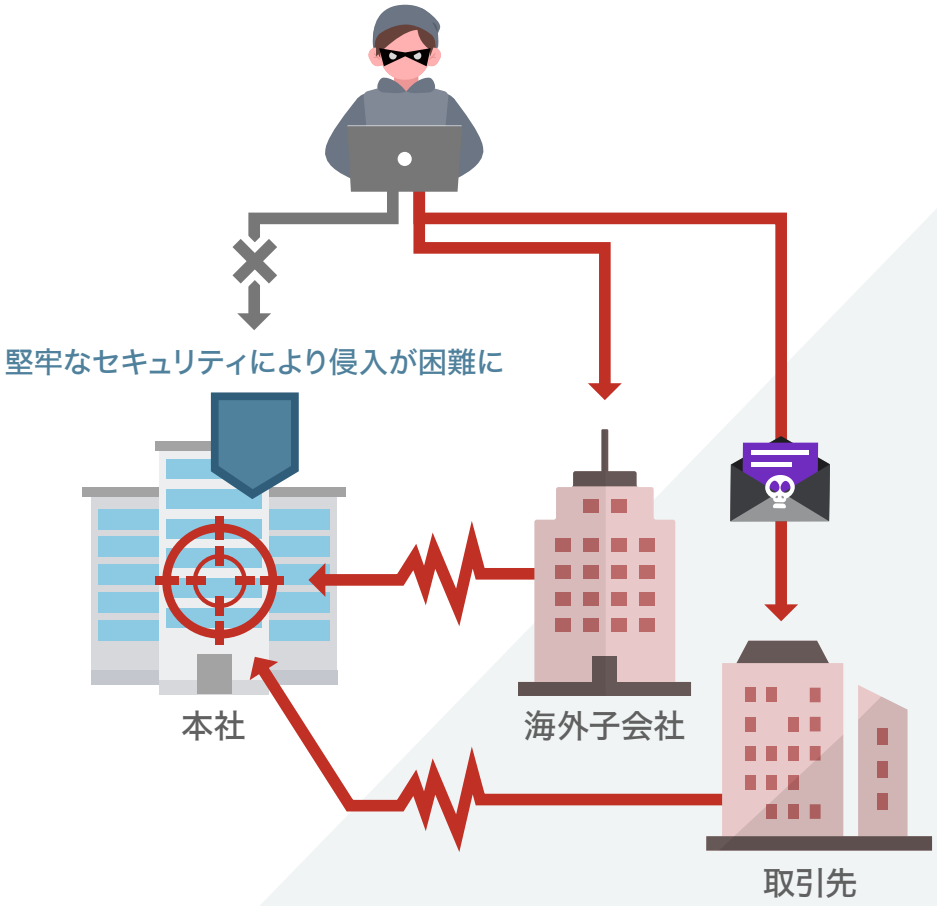
サイバー攻撃はどこを標的に？

ズバリ、守りの弱い中堅・中小企業から

堅牢なシステム構築、対策、体制を築いている企業は攻撃者にとってスムーズな攻撃を阻むため厄介です。

そのため、積極的なセキュリティ対策を取り入れている大企業や政府機関を直接狙うよりかは、セキュリティ予算や人員が限られている中小企業が標的にされ易くなります。また中小企業ではセキュリティを専門とする担当者が不足しがちです。そのため、本来実施すべきセキュリティ対策が疎かになってしまうことも狙われてしまう要因の一つと言えます。

また、親会社の堅牢なシステムとは異なる製品・ポリシーを導入していることから、脆弱性も生じやすく、弱点を突かれてしまうということも。その結果、サプライチェーンにも波及するサイバー攻撃が増加しているのです。



セキュリティ対策が不十分な子会社や
取引先をターゲットにメール等で侵入し、本社へ攻撃。

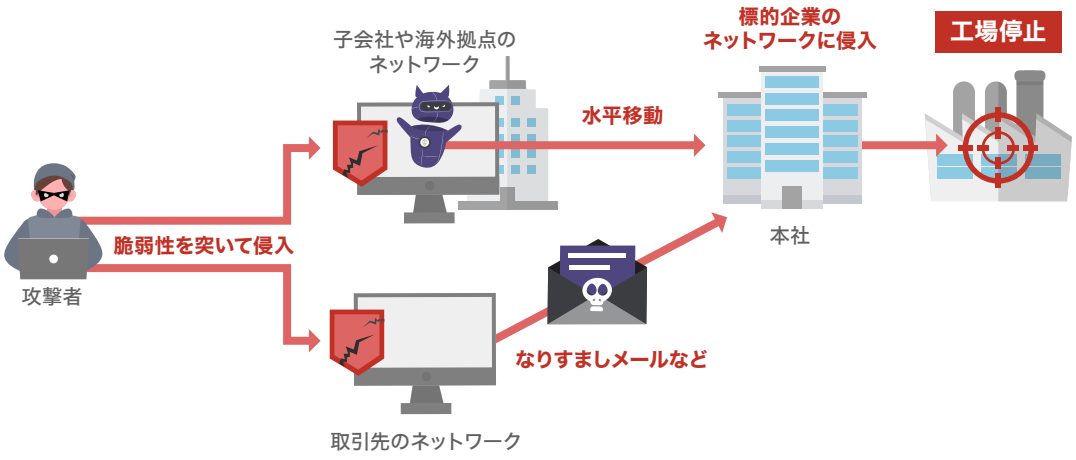
事例から学ぶサプライチェーン攻撃

部品製造メーカー

手法 VPN機器の脆弱性より不正侵入。

対応 外部からの不正アクセスをサーバーが検知するとともに、
一部のサーバーで障害が発生。
被害拡大防止のために、すべてのシステムを停止。

影響 国内の全工場（14工場28ライン）の稼働停止。

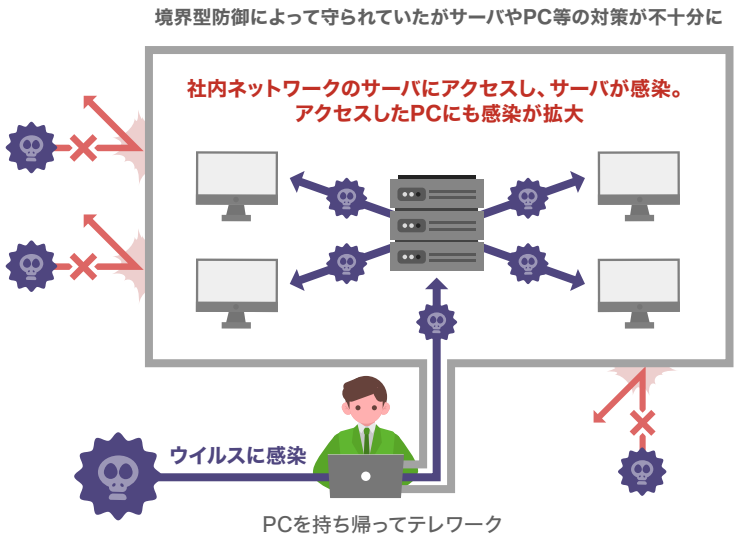


自動車製造メーカー

手法 外部からの不正アクセスをサーバー側で受け、社内のネットワークにウイルスが拡散。
サーバーにアクセスした社員のパソコンより感染拡大。

対応 全社員のパソコン使用を制限。

影響 サーバーへのアクセスのほか、社内システムや電子メール、検査システムへの障害。
国内の工場（3工業）の稼働停止。海外の工場（9工場）が一時生産停止。



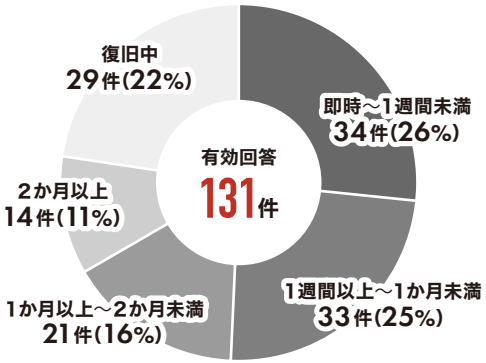
サイバー攻撃に遭うと生じる甚大な被害

サイバー攻撃に遭うと、生じる被害は以下のようなことが考えられます。

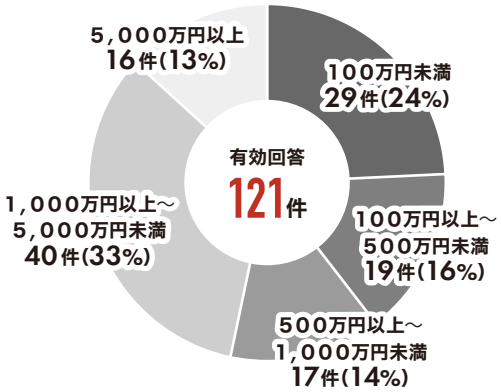
1 データの暗号化
2 システムの障害・破壊
3 不正なアクセスによるデータ搾取・漏えい
4 ブランドイメージの損失・仕様失墜

データ復元（ランサムウェアの解読キー）を引き換えに金銭要求されますが、これに応じないことを大前提にしても、調査、対応、復旧にかかる各種金銭被害がつきものです。

復旧に要した期間



調査・復旧費用の総額



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」
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_cyber_jousei.pdf
左から、「【図表７：復旧に要した期間】」、「【図表８：調査・復旧費用の総額】」より作成

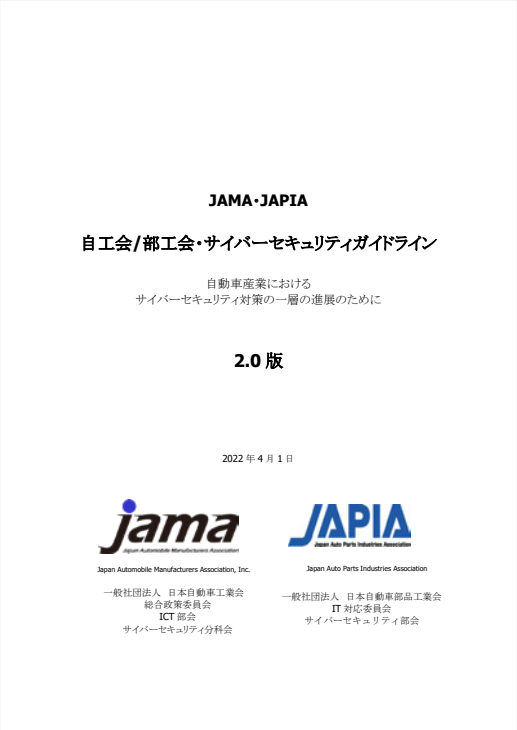
初動対応でいかに被害を最小化できたかが後の対応・対処に影響

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過徴金
風評被害	イメージ低下、社会的地位の低下

自動車産業サイバーセキュリティガイドライン

自動車産業全体が“対応すべき”セキュリティ対策の指針

自動車産業を取り巻くサイバーセキュリティリスクが深刻化している中、日本自動車工業会（JAMA）と日本自動車部品工業会（JAPIA）は、
「サイバーセキュリティガイドラインV2.0」を発行し、自動車産業のサプライチェーン全体にガイドラインの活用を推進しています。
自動車業界だけでなく、製造業全体及び、サプライチェーンを構成するすべての企業にも非常に有効なガイドラインです。
是非、現在の対策と照らし合わせ見直しいただくことをおすすめします。



JAMA・JAPIA

自工会/部工会・サイバーセキュリティガイドライン

自動車産業における
サイバーセキュリティ対策の一層の進展のために

2.0 版

2022 年 4 月 1 日

Japan Automobile Manufacturers Association, Inc.

一般社団法人　日本自動車工業会
総合政策委員会
ICT 部会
サイバーセキュリティ分科会

Japan Auto Parts Industries Association

一般社団法人　日本自動車部品工業会
IT 対応委員会
サイバーセキュリティ部会

自工会/部工会・サイバーセキュリティガイドライン V2.0 (日本語版)

https://www.jama.or.jp/operation/it/cyb_sec/docs/cyb_sec_guideline_V02_00.pdf

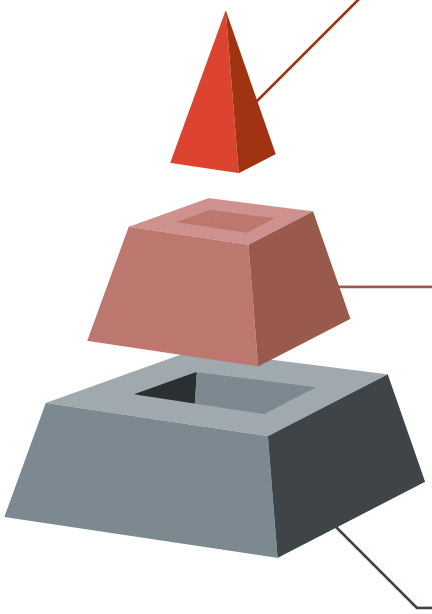
セキュリティ対策状況のセルフ評価・チェックシート

https://www.jama.or.jp/operation/it/cyb_sec/docs/cyb_sec_guideline_CS_v02_00.xlsx

出典）自工会 / 部工会・サイバーセキュリティガイドライン V2.0（日本語版）
https://www.jama.or.jp/operation/it/cyb_sec/docs/cyb_sec_guideline_V02_00.pdf

ガイドラインの構成

自動車産業サプライチェーン全体のセキュリティの向上を目的に、企業の規模によらず自動車産業全体が優先して実施すべき重要項目に加え、
取り扱う情報によって標準的に目指す項目や最終到達点として目指すべき項目をレベルごとに表記されています。

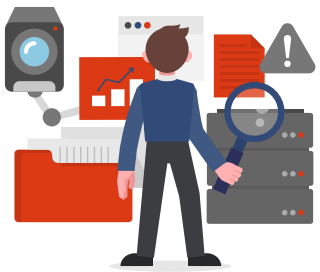
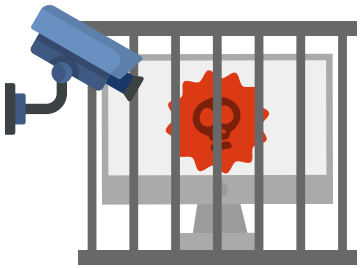
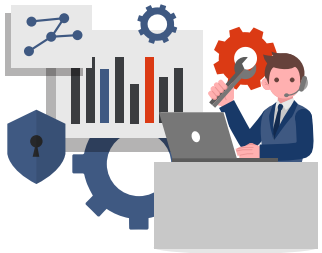


レベル	定義	各レベルの達成を目指すべき会社
level 3	現時点*で自動車業界が到達点として目指すべき項目 ※2022年4月	会社規模・技術レベルの観点で自動車業界を代表し牽引すべき立場の会社、またはそれを目指す会社 Lv1～3の全項目を達成
level 2	自動車業界として標準的に目指すべき項目	以下のいずれかに該当する会社 • サプライチェーンにおいて社外の機密情報（技術・顧客情報等）を取り扱う会社 • 自動車業界として重要な自社技術/情報を有する会社 • 相応の規模／シェアを有し、不慮の供給停止等により業界のサプライチェーンに多大な影響を及ぼし得る会社 Lv1,2の全項目を達成
level 1	自動車業界として最低限、実装すべき項目	自動車業界に関係する全ての会社 Lv1の全項目を達成

出典）自工会 / 部工会・サイバーセキュリティガイドライン V2.0（日本語版）https://www.jama.or.jp/operation/it/cyb_sec/docs/cyb_sec_guideline_V02_00.pdf ＜図：自動車産業 CS ガイドラインのセキュリティレベル定義＞

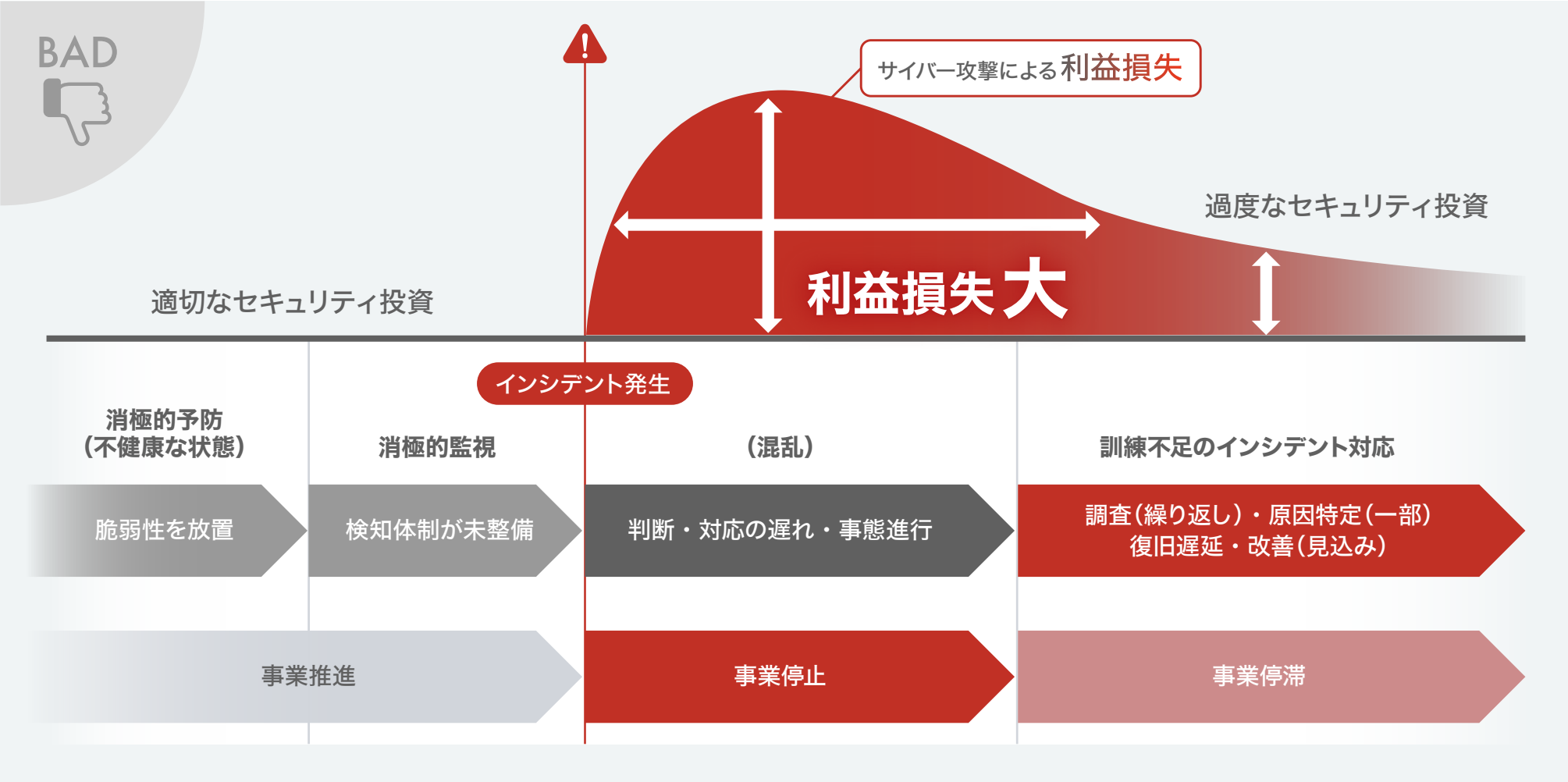
サイバーセキュリティフレームワークと ガイドラインの対策ポイント

サイバーセキュリティフレームワークとは、米国国立標準技術研究所という米国政府機関によって、
複雑で多様なセキュリティ対策を一定の基準を設け、組織や業界を超えて包括的に利用できる枠組みのことです。
自工会/部工会サイバーセキュリティガイドラインは、このフレームワークを活用したチェック項目があります。

	特定	防御	検知	対応・復旧
				
目的	守る対象を明確にし リスクを特定する	攻撃されたことを迅速に把握	攻撃を防ぐ対策実施	検知被害の対応と修復
対策	・情報資産の管理(情報・機器) ・リスク対応 ・取引内容・手段の把握 ・外部への接続状況の把握 ・社内接続ルール ・他社との情報セキュリティ要件 ・アクセス権	・マルウェア対策 ・不正アクセスの検知	・物理セキュリティ ・通信制御 ・認証・認可 ・パッチやアップデート適用 ・データ保護 ・オフィスツール関連	・被害範囲の特定 ・業務改善 ・バックアップ ・復元・リストア

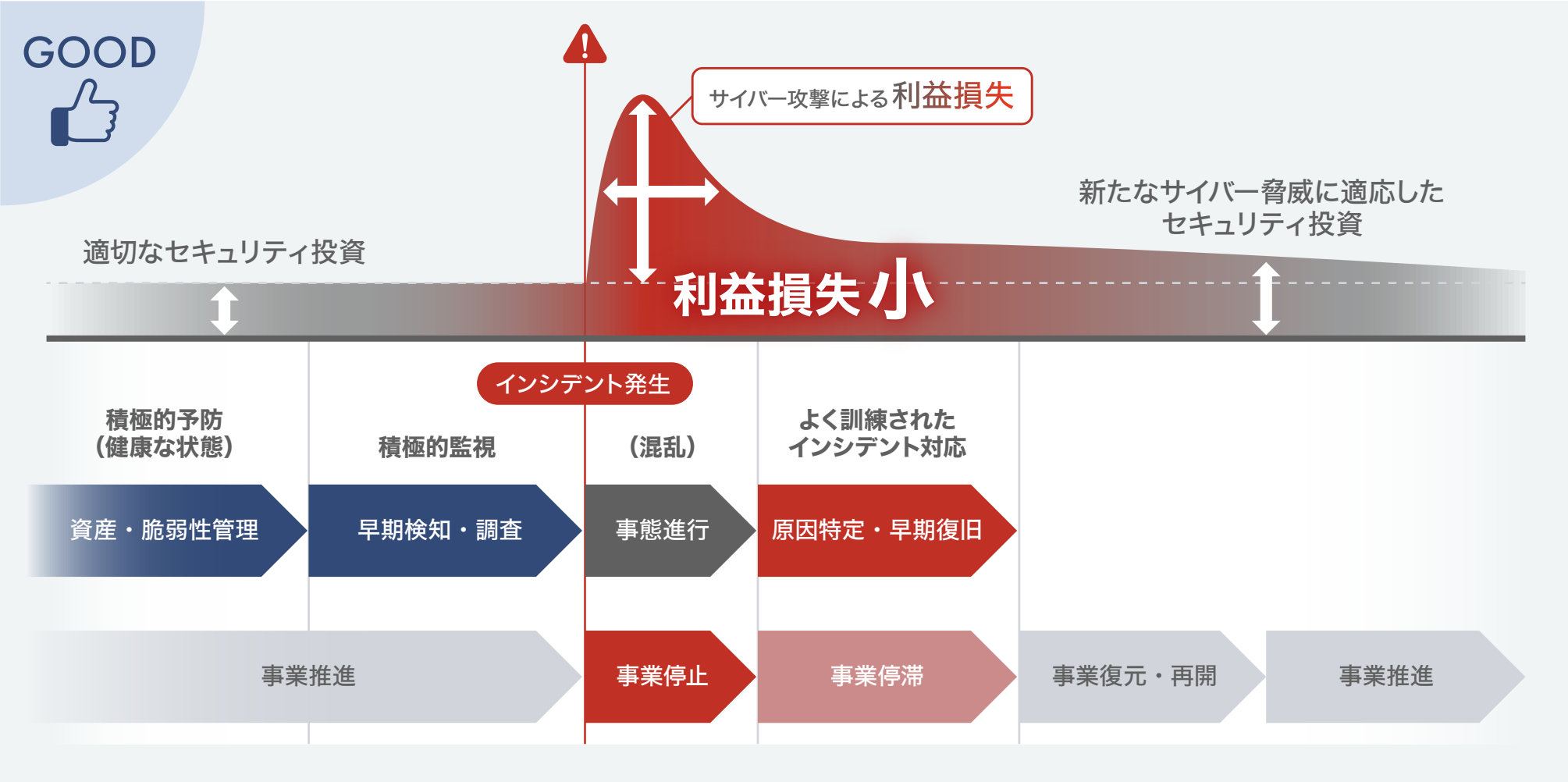
後回しになりがちな『検知』『対応・復旧』

サイバーセキュリティフレームワークで取り組む対策において、『特定』『防御』といった侵入されない前提の対策を講じている企業は多いでしょう。
“これで侵入されないだろう”という安心感により、侵入を前提とした対策、つまり『検知』『対応・復旧』が後回しにされがちです。
しかし、侵入を防ぐことはほぼ不可能です。そして一度侵入を許してしまうと、甚大な利益損失が生じてしまうのです。



侵入されることも前提に対策することが被害を最小化する

そのため、侵入されることを前提に『検知』『対応・復旧』の対策を講じているかで、被害範囲、そして利益損失の度合いが変わってきます。
そのため、ガイドラインにはこれらの対策で重要となる、”ログ管理”について要件がまとめられています。



ガイドラインでも必須！ ログの要求事項

目的

- 保護すべきデータの漏洩・サイバーセキュリティ対策の徹底、強化
- 不正アクセスを防止
- 情報システムの不正利用や、情報システムの不正操作・変更を防ぐことで、情報漏えい、改ざんを防ぐ
- 情報システムを安定稼働させる
- 情報漏えい、改ざんや情報システム停止の際の原因調査を可能にする
- 不正アクセス・不正侵入による情報漏えい、改ざん、システム停止を防ぐ
- システム停止、データ消失による業務影響を最小化する
- 早期の業務復旧

自工会/部工会・サイバーセキュリティガイドライン

ログ管理が必要となる項目番号

17　53　81　122　142　143　144　145　146

JAMA・JAPIA

自工会/部工会・サイバーセキュリティガイドライン

自動車産業における
サイバーセキュリティ対策の一層の進展のために

2.0 版

2022 年 4 月 1 日

出典 ）自工会 / 部工会・サイバーセキュリティガイドライン V2.0 (日本語版) https://www.jama.or.jp/operation/it/cyb_sec/docs/cyb_sec_guideline_V02_00.pdf

ログの要求事項（保管編）

項番	達成条件	達成基準（規則）
17	サイバー攻撃や情報漏えいの新たな手口を知り、対策を社内部署へ共有している。 **サイバー攻撃や予兆を監視・分析をする体制を整備**している。	サイバー攻撃や予兆の検知 分析結果から適切な対応・体制構築
53	**アクセスログは、安全に保管しアクセス制御された状態で管理**されている。	適切な期間のログを保持 ログを保管先・システムへのアクセス制御等の適用
142	通信内容を常時監視し、**不正アクセスや不正侵入を** **リアルタイムで検知/遮断および通知する仕組み**を導入している。	リアルタイム検知・遮断する仕組み
143	インシデント発生時の調査のために**必要なログを取得**している。	必要なログを取得している
145	**ログを分析し、サイバー攻撃を検知する仕組みを導入**している。	異常発見時に通知する仕組み
146	社内に**侵入したマルウェアと不正なサーバーとの通信を遮断する対策**を実施している。	不正なサーバーへの通信を遮断する仕組み

ログの要求事項（分析編）

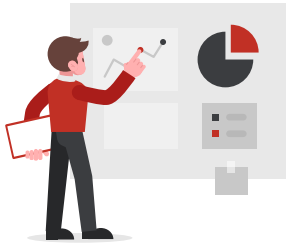
項番	達成条件	達成基準（規則）
81	内部情報漏洩対策として、**複数ログを組み合わせて、異常行動を自動検知できる仕組み**を導入している。	不正な持ち出しが検知できること 不正な持ち出しをアラートが通知できること
122	**認証ログのモニタリング**を実施している。	認証ログのモニタリングより 不審な認証を検知できること
144	重要なシステムについて、**アプリケーション操作ログを取得**している。	ユーザー、管理者の操作ログを取得すること

ガイドラインで求められるログ管理の機能

ログ取得

様々な種類のログを収集し、
見やすい形に整形して出力、
保管する機能は、ログ管理のメイン機能です。

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る必要があります。
また、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。

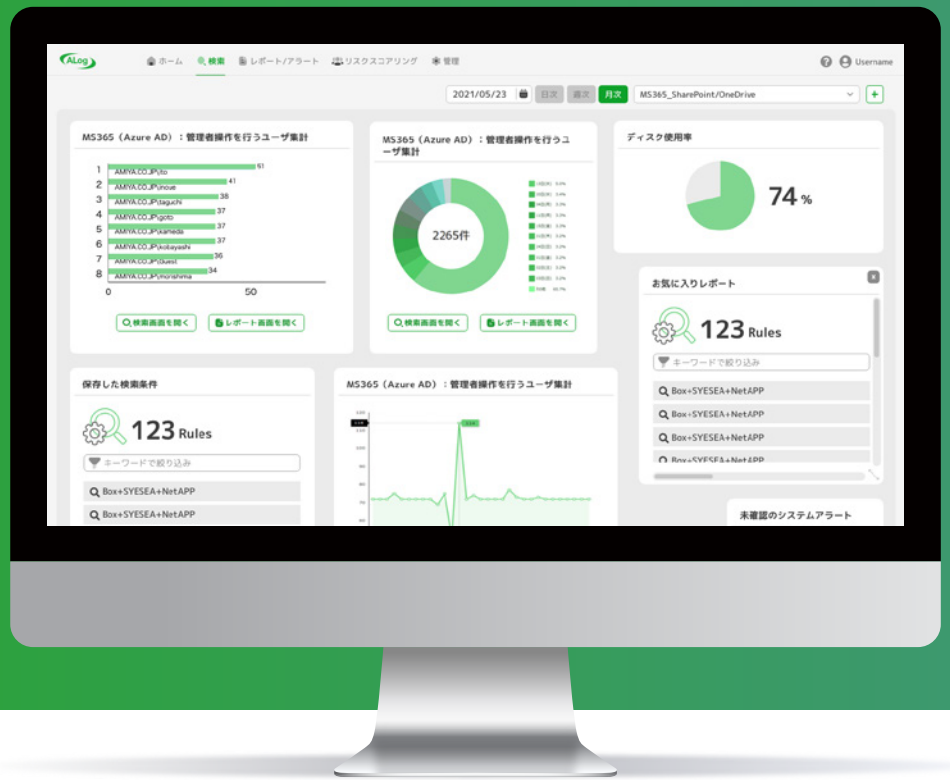
遮断

不正アクセスの疑いを検知、
他システムとの連携により攻撃者の侵入経路を閉ざし、
被害を抑えることができます。

▶▶▶ 次ページからはログ管理のベストプラクティス、ALog をご紹介します。

“わかりやすさ” を追及した国産SIEM ALog

ALogは、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SIEM製品です。
「ログ管理の難しいをカンタンに」を、コンセプトに専門知識やノウハウがなくとも、誰でもカンタンなのに高度なログ管理を実現できるのが特徴です。



＼累計 5,500 契約以上！／

大手自動車メーカー、
大手サプライヤー実績多数

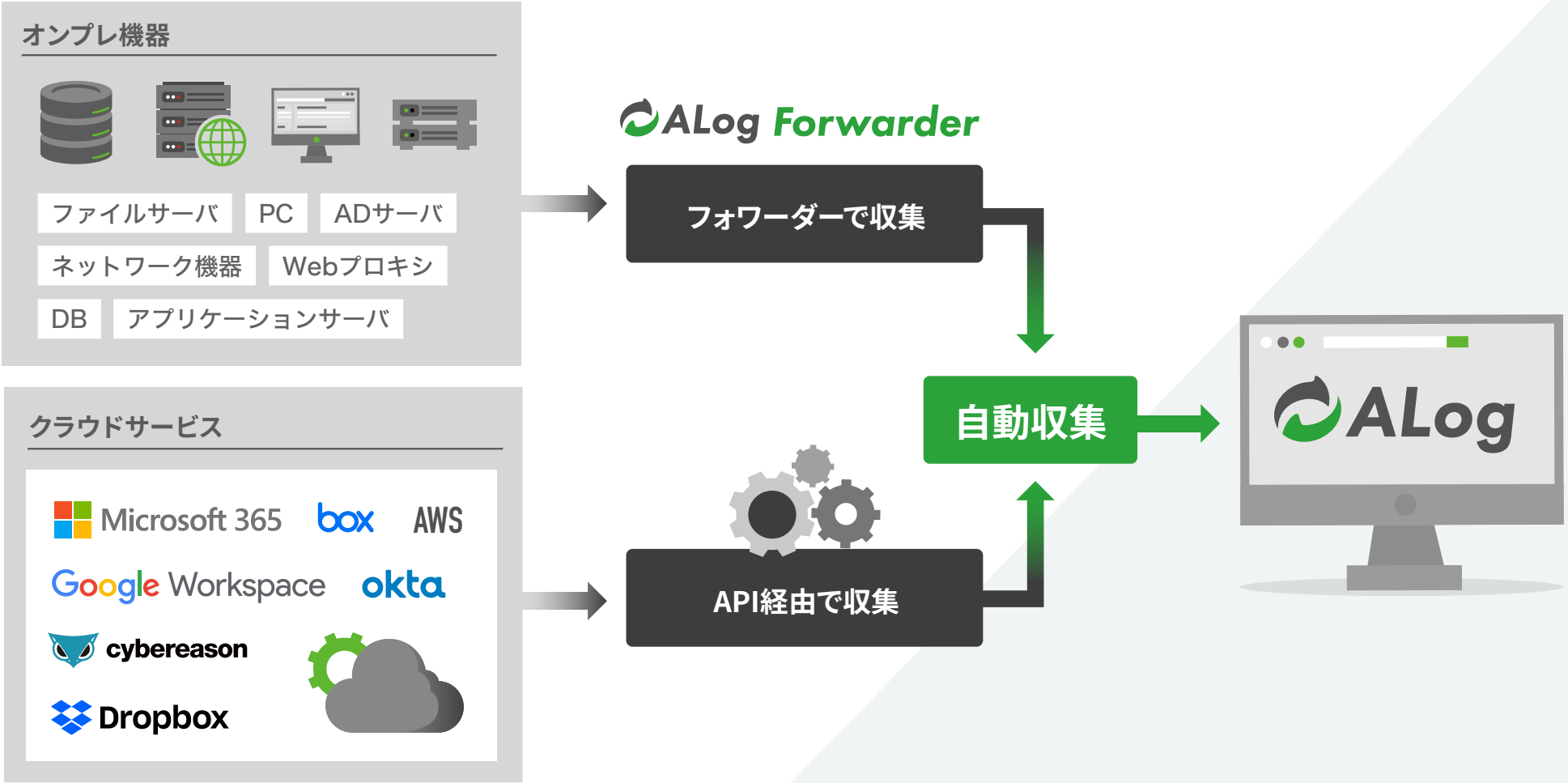
主な導入企業

品川区 Panasonic NISSHINBO NTT Communications YAHOO! JAPAN SUBARU LINE株式会社

mixi GROUP トレイダーズ証券 KDDI SBI証券 MUSÉE PLATINUM OBAYASHI SEKISUI HOUSE LANDNET

あらゆるログを自動収集

調査に必要となる、あらゆるＩＴシステムのログをカンタン自動収集します。
システムや取り込むフォーマットが異なっていても、ログは時刻フォーマットのみで取り込めるので、設計不要で運用スタートできます。
まとめておくことで調査・分析をスムーズに。



取得だけじゃない、唯一無二の翻訳機能

イベントログの大半は膨大で複雑です。その複雑なイベントログをわかりやすく、『いつ、誰が、何をした』と、どなたでも理解できる、一目でわかる形式に翻訳するので、インシデントハンドリングに差が付きます。

特許取得のログ翻訳変換技術 ※特許第 6501159 号

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

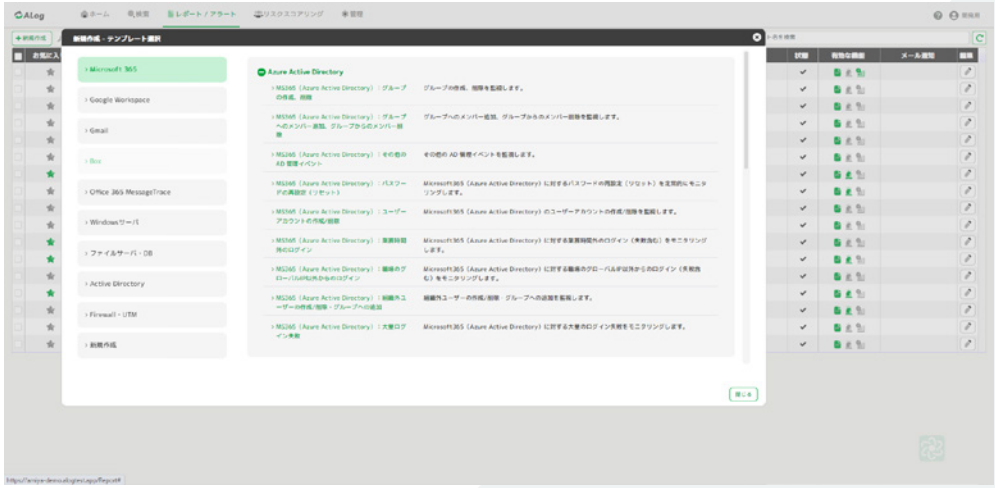
日時	ユーザー	サーバ	ファイル	操作
2022/09/29 15:44:19.825	amya Sasaki	amyfs001	D:\fsvol1\営業部\重要顧客リスト.xls	READ
2022/09/28 23:43:21.422	amya Yamada	amyfs001	D:\fsvol1\企画部\FY13事業計画.doc	WRITE
2022/09/28 12:45:02.259	amya\Sato	amyfs003	D:\fsvol1\経理部\給与明細_田中.xls	DELETE
2022/09/27 02:38:12.245	amya Akagi	amyfs002	D:\fsvol1\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

効果的な監視項目をセット

何をどう監視して分析したらいいのかを解決するには、ログ、そしてセキュリティといった幅広い知見が必要ですが、
ALogなら事前に効果的な監視項目をテンプレートとしてインプットしています。
このテンプレートはサイバー攻撃の手法やガイドラインの変化に応じて更新していくので、監視の最適化もお任せできるのがポイントです。

対象システム

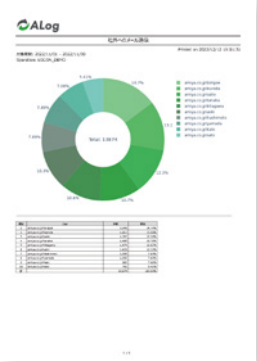
- Windowsサーバ
- ファイルサーバ/DB
- Active Directory
- Firewall - UTM
- Microsoft365
- Google Workspace
- Gmail
- Box
- Cybereason



レポート・アラートサンプル

IPAやJPCERTガイドラインに対応

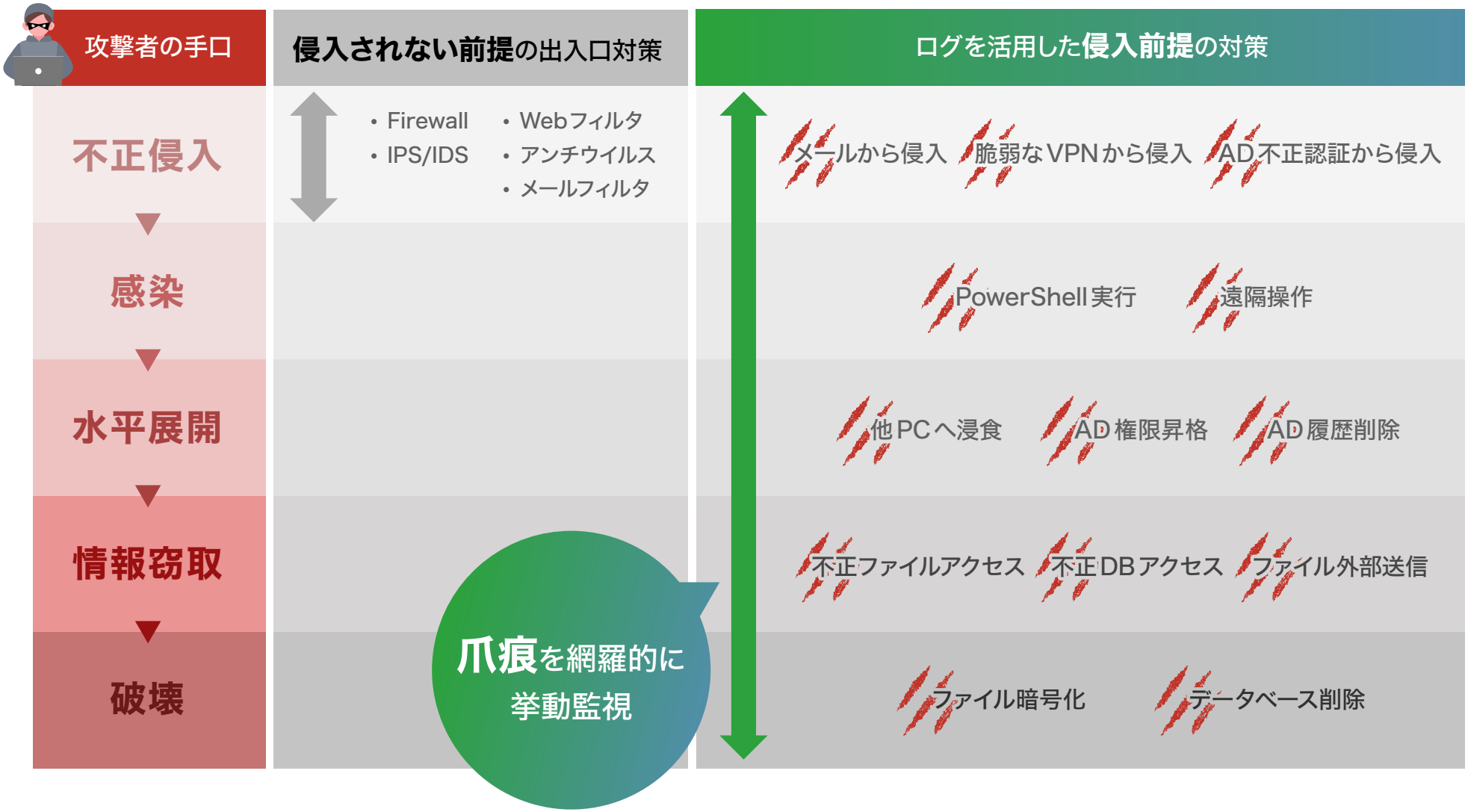
- 不審なユーザアカウントの作成/削除
- 無効なアカウントによるログオンチャレンジ
- 特権ユーザのログオン
- ランサムウェアによる被害範囲の特定
- 不正アクセスの把握
- 業務時間外のアクセス監視
- パスワードの再設定(リセット)
- 職場のグローバルIP以外からのログイン



被害を最小化するアラート監視網

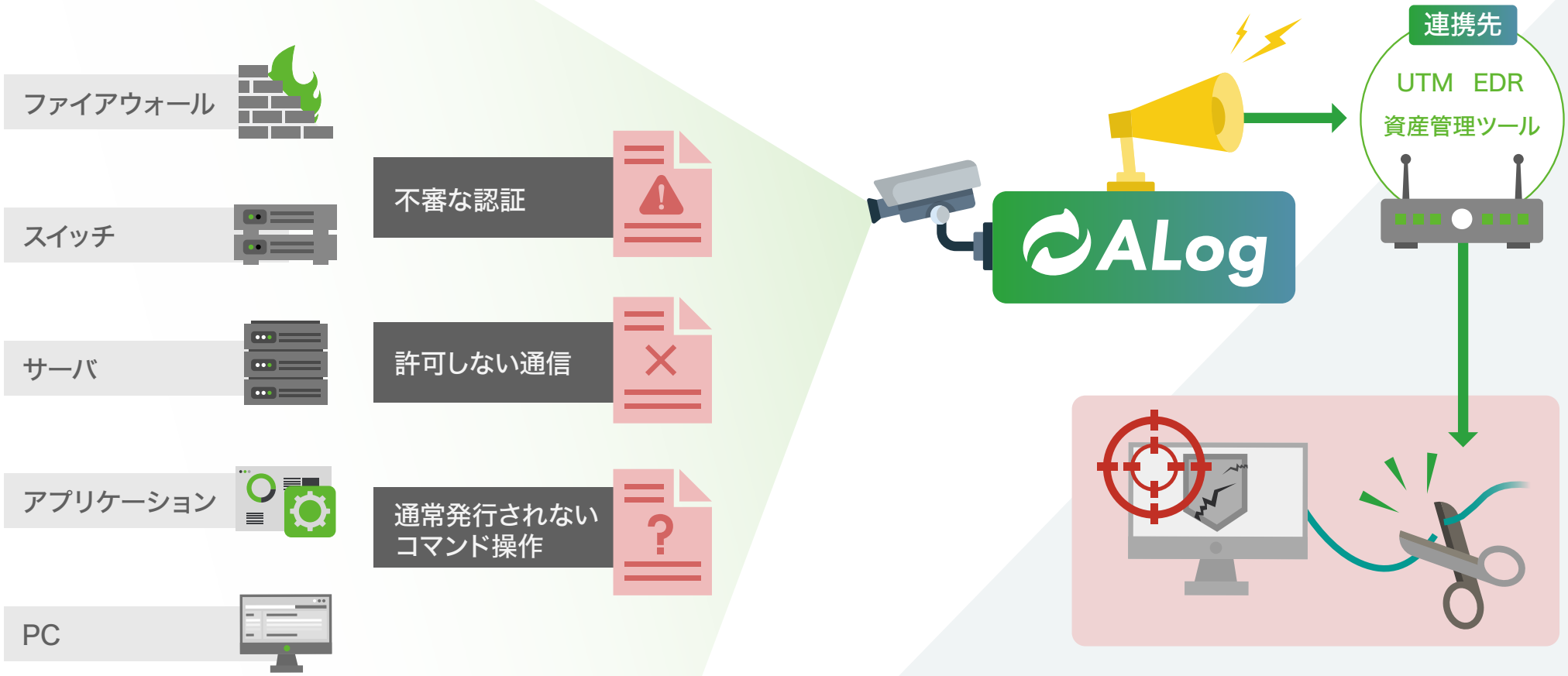
侵入されることを前提に、侵略行為が進む前にアラート監視をします。

フェーズごとに残る攻撃の痕跡を素早く検知することで、被害を最小化、さらには未然に防ぐ効果があります。



不審な挙動を自動遮断

ALogでログを収集し、監視、不正アクセスの疑いがあるログを検知した場合、
その情報をネットワークより遮断できるUTMやEDRなどに連携することで、自動遮断できるようになります。



ALogのエラー情報を受信端末を特定し、自動でネットワークより遮断！

あらゆるログを自動収集

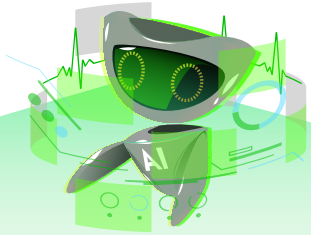
普段の傾向をAIが分析＆異常を自動判定して、リスクをスコアリングします。
”いつもと違う”ことに敏感になることで不正アクセスの早期検知に繋がります。

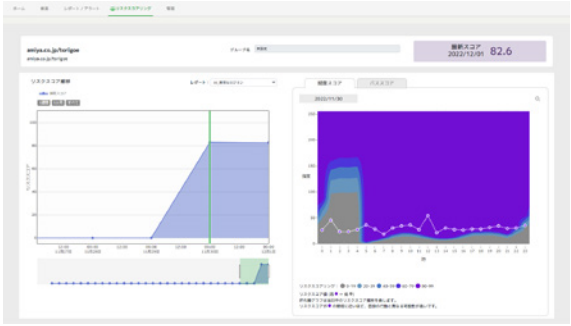
いつもとは違う **時間帯によるアクセス**

いつもとは違う **大量に発生したアクセス**

いつもとは違う **IP・端末からのアクセス**

いつもとは違う **データ操作**

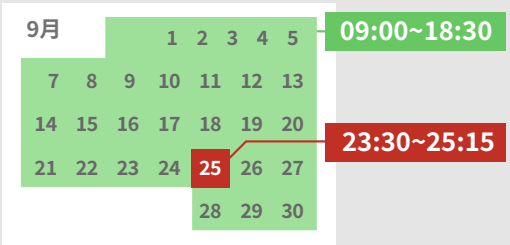




普段との違いで見つかる 内部不正

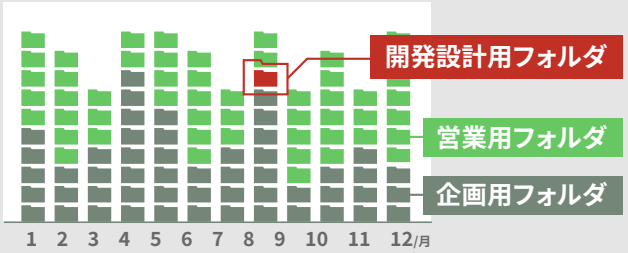
いつもと違う時間のアクセス

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

アクセスとデータを保護するセキュリティ機能

ログは安全に保管し、アクセス制御された状態で管理します。

ガイドライン上、半年分のログ保管が必要ですが、1年分のログを自動保管しているので安心です。

アクセス

- IPアドレス制御
- 二要素認証
- 暗号化通信

データ

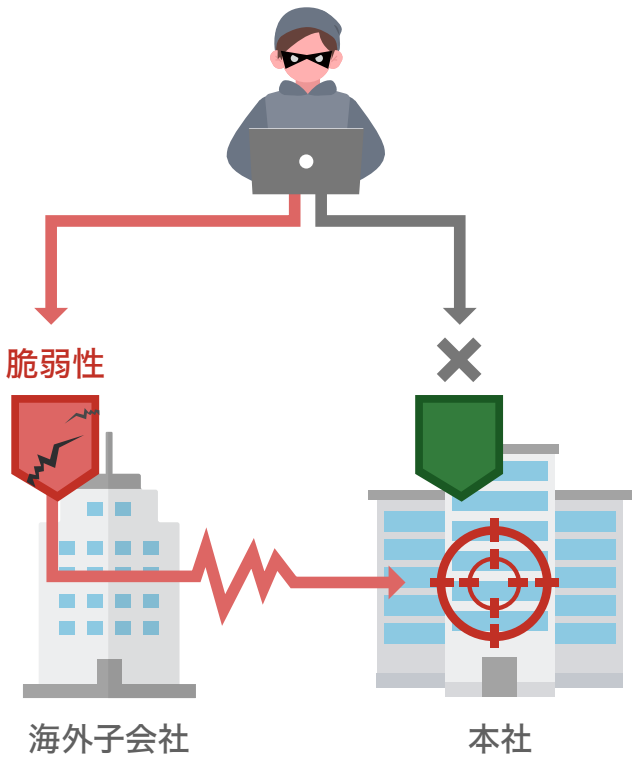
最低1年分のデータを自動保管！

- バックアップ
- データ暗号
- 操作ログ取得

海外子会社を経由したサイバー攻撃

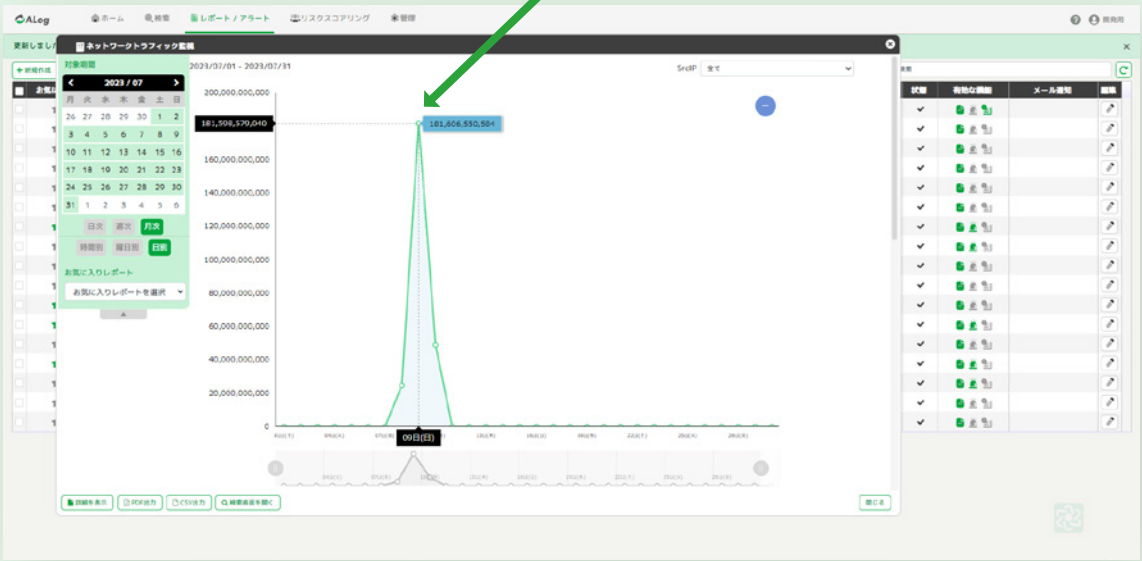
ネットワーク機器のログから、本社向けのトラフィックの変化をチェックすることで、脆弱性スキャンの疑いを検知します。
急激な通信量増加から、ポートスキャンを疑い、脆弱性対策などが十分であるか、予防へと繋げます。

海外子会社の脆弱性から不正アクセス



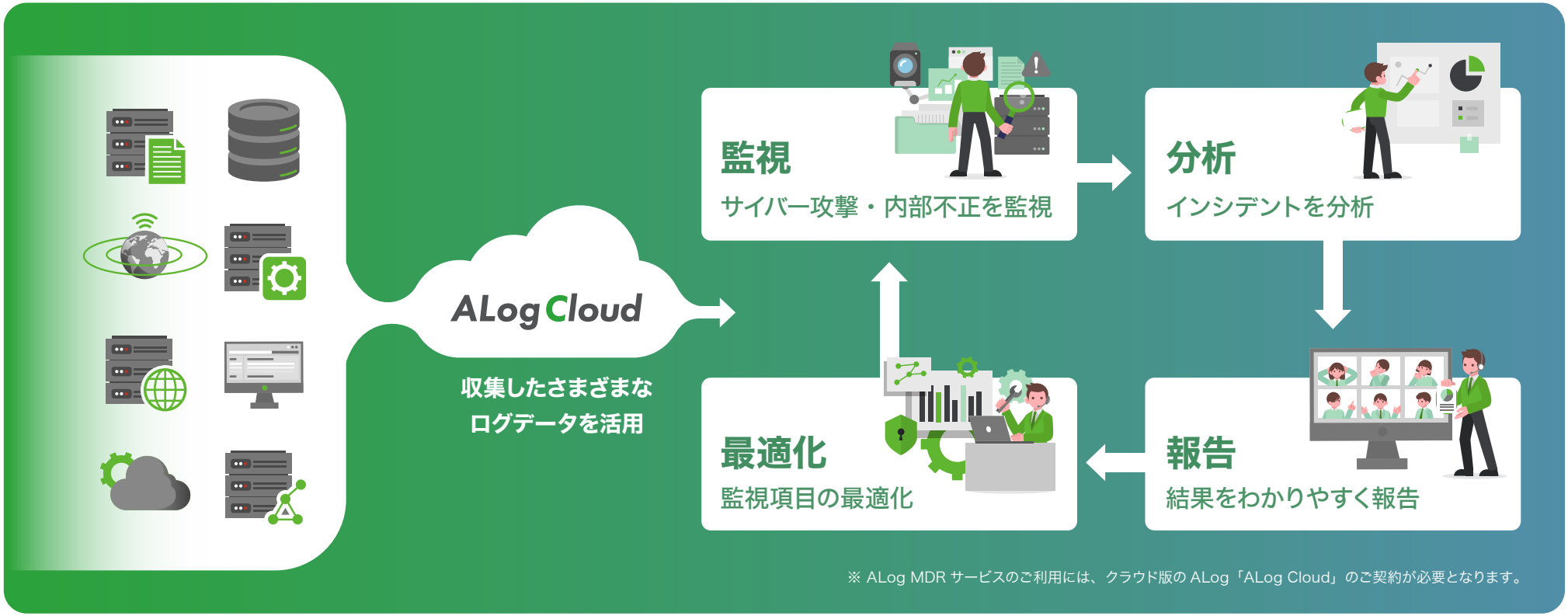
UTMの通信ログから
海外子会社→本社向けのトラフィック変化をチェック

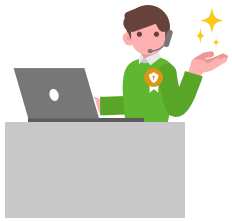
海外子会社ネットワークから本社ネットワークへの通信量が増加
スキャン活動の可能性大



監視の体制整備にMDRサービス

ALogを活用したサイバー攻撃対策の監視運用をまるっとお任せ。
監視から最適化まで一任し、ガイドラインに必要な監視体制を網羅します。





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

中小・中堅企業のセキュリティを幅広くカバー

ログ管理だけではなく、幅広いセキュリティ支援を実施しています。

特定 → 特定 → 特定 → 特定 → 特定

セキュサポ　中堅企業が必要とするセキュリティ対策を包括的に提供

- アタックサーフェイス調査
- 脆弱性診断
- サイバー攻撃検知
- 内部不正検知
- インシデントレスポンスサイバー保険相談窓口

AMIYA Security　サイバーセキュリティサービスを包括的に提供

アタックサーフェイス調査	EDR導入	ALog MDRサービス	フォレンジックサービス
脆弱性調査	ゼロトラスト コンサル/導入/運用	EDR運用サービス	インシデントレスポンス コンサルサービス
セキュリティ監査	セキュリティトレーニング		
セキュリティ設定診断	標的型攻撃メール訓練		
CSIRT構築 コンサルサービス			

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

appendix：機器別のログで分かる事

ActiveDirectory

- 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
- 大量のログイン失敗
- ユーザアカウントの作成/削除

FireWall

- HTTP、HTTPS等のプロトコルによる外部への通信
- ぜい弱なPCや内部サーバの探索
- 通過した通信、または拒否された通信

ファイルサーバ

- ランサムウェアによる被害範囲の特定
- ファイルの参照や、編集などの成功や失敗の記録

メールサーバ

- なりすましメール
- 実行ファイル添付メール

データベース

- 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
- アカウント変更・削除

Webプロキシ

- 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

DNSサーバ

- 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

アプリケーション

- 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

IDS / IPS

- IDS/IPSが検知した、また検知から漏れた通信

DHCPサーバ

- IP割振りによる感染端末の特定

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。

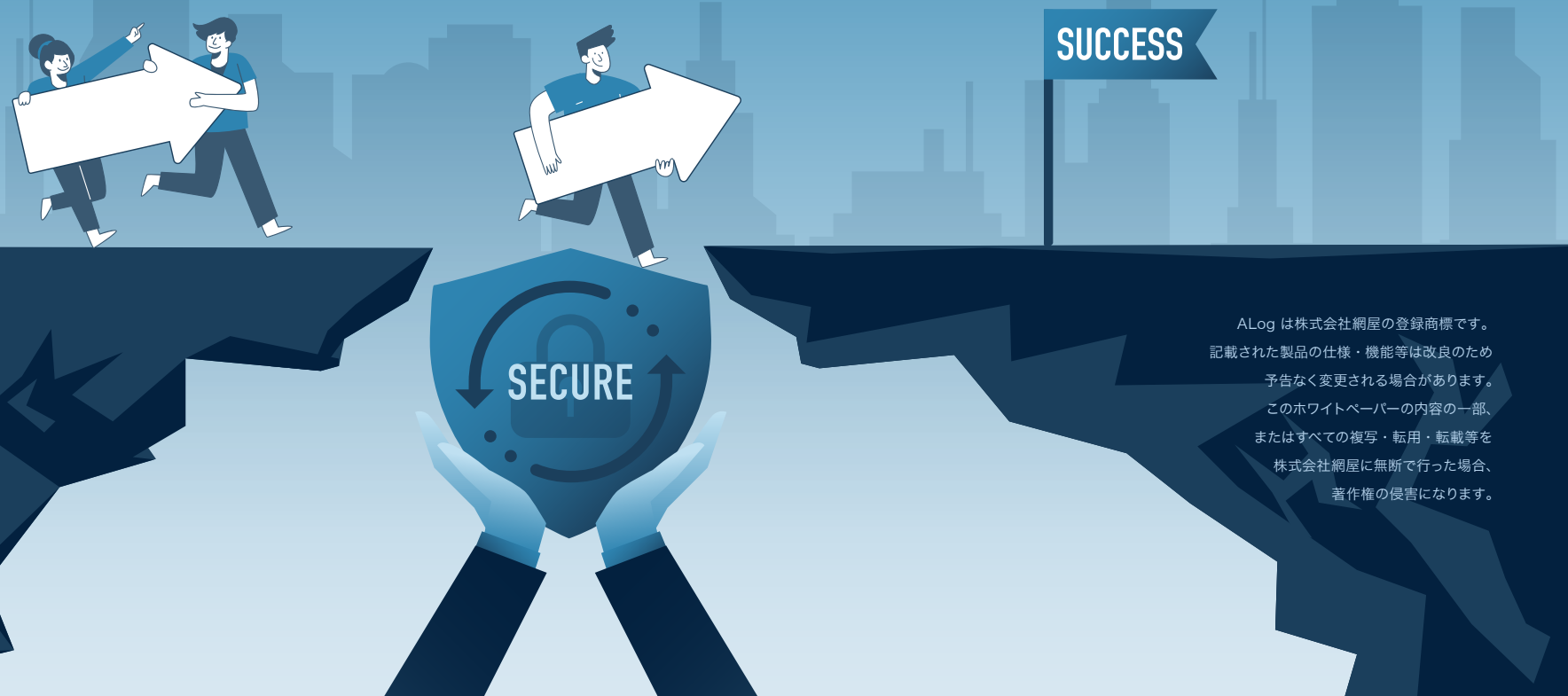
サイバー攻撃は、経済的余裕度に関係なく、全ての事業法人がターゲットになります。

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。