OCEANBRIDGE

つかえるITを、世界から。

計り知れない被害をもたらすセキュリティインシデント

～ランサムウェア攻撃による被害や内部不正による情報漏えいとその対策について～

株式会社オーシャンブリッジ

株式会社オーシャンブリッジ
OceanBridge Inc.

代表取締役社長：澤　紀和

本　社：東京都港区元赤坂一丁目5番12号
　　住友不動産元赤坂ビル7階
設　立：2001年6月
資本金：1,600万円
事　業：海外製ソフトウェアと戦略的アライアンス
　　をベースとした事業開発及び事業運営

データ圧縮ソフト
NXPowerLite™ by neuxpower

リモートコントロール
islonline by XLAB NOT IDLE

アクセスセキュリティ
UserLock FileAudit by IS Decisions

Web画面共有ツール
Surfly by Surfly

授業・教育支援ツール
Mieroom by XLAB NOT IDLE

高速・多機能ファイルビューア
BRAVA! BLAZON by opentext™

産業用ゼロトラストリモートアクセス
DISPEL by DISPEL

Useful IT from all over the world.

つかえるITを、**世界から。**

海外には、日本でまだ知られていないソフトウェアやITサービスが数多くあります。
オーシャンブリッジはその中からお客様に喜ばれる本当に便利でユニークな製品を見つけ出し、日本のお客様に最適なかたちでお届けします。海外のテクノロジーと日本市場をつなぐ「架け橋」として、日本の産業に貢献していきます。

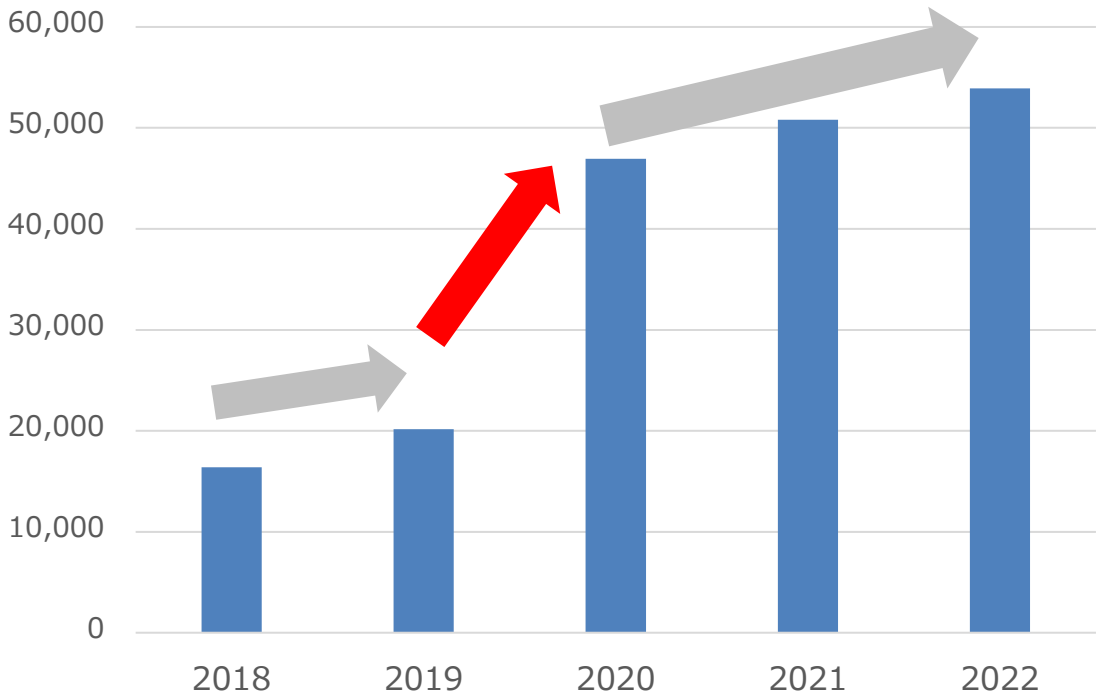
目次

1.ランサムウェア攻撃の被害とリスク

IT・セキュリティ(サイバー攻撃)の動向

新型コロナ禍に伴う**テレワークの拡大後、セキュリティインシデントは急増、**
その後も増加しており、その脅威(種類)も大きく変化・高度化してきている

セキュリティインシデント年間報告件数



出典：JPCERT/CC 「インシデント報告対応レポート」を編集して作成
https://www.jpcert.or.jp/ir/report.html

情報セキュリティ10大脅威 2023

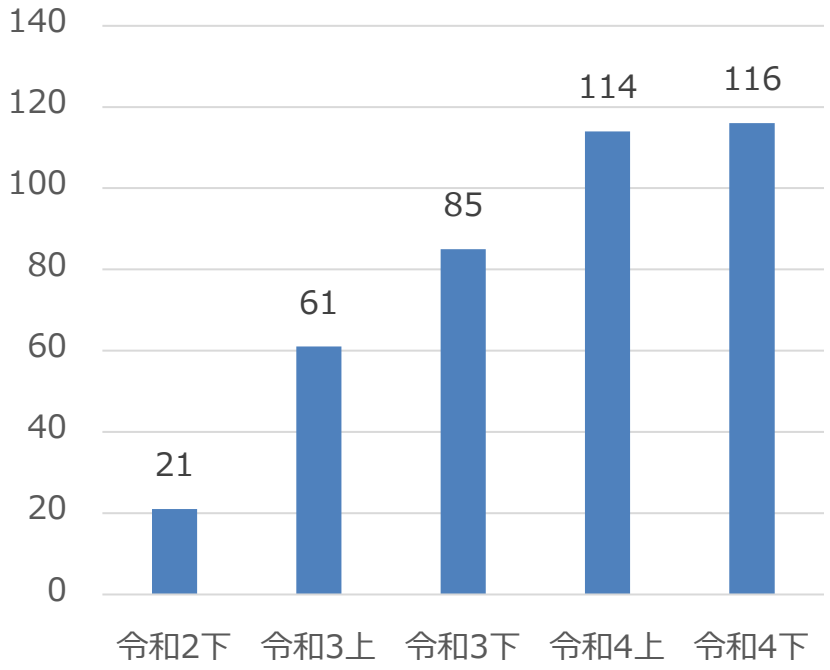
順位	組織	昨年順位
1位	ランサムウェアによる被害	1位
2位	サプライチェーンの弱点を悪用した攻撃	3位
3位	標的型攻撃による機密情報の窃取	2位
4位	内部不正による情報漏えい	5位
5位	テレワーク等のニューノーマルな働き方を狙った攻撃	4位
6位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	7位
7位	ビジネスメール詐欺による金銭被害	8位
8位	脆弱性対策情報の公開に伴う悪用増加	6位
9位	不注意による情報漏えい等の被害	10位
10位	犯罪のビジネス化（アンダーグラウンドサービス）	圏外

出典：IPA 「情報セキュリティ10大脅威 2023」を編集して作成
https://www.ipa.go.jp/security/vuln/10threats2023.html

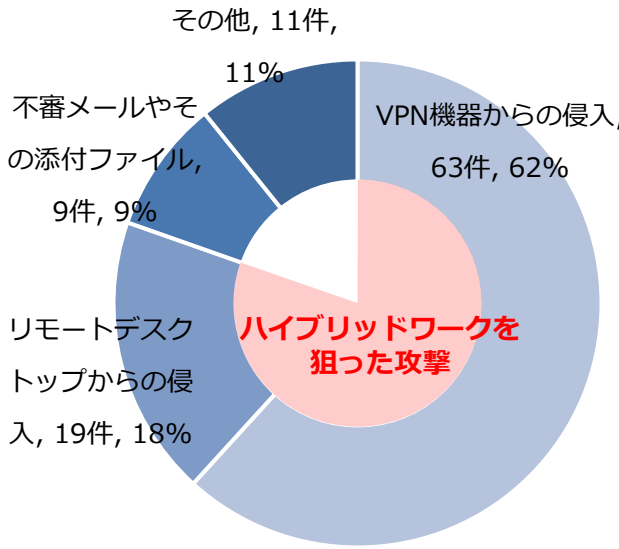
最近のサイバー攻撃(ランサムウェア)の情勢

近年**ランサムウェア被害**が急増。攻撃手法自体の進化(二重の脅迫、ばらまき型から標的型へ)や昨今のハイブリッドワークを狙った攻撃が理由で、
業種・企業規模問わず被害が発生していることが特徴

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

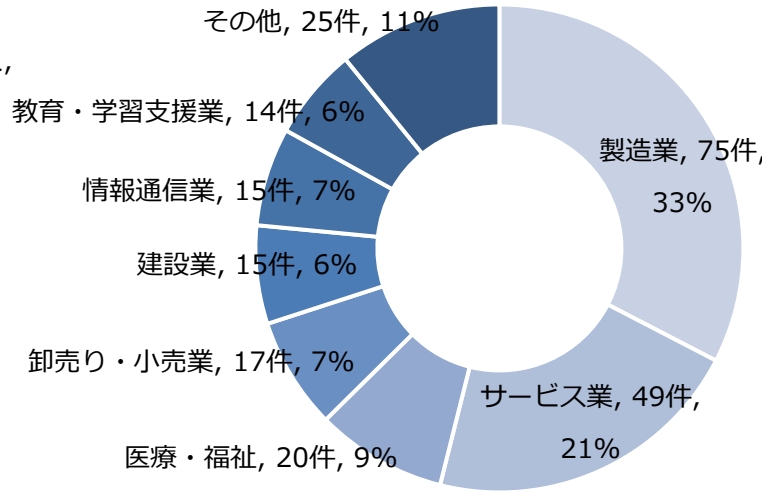


図表6：感染経路



有効回答：102件

図表５：ランサムウェア被害の企業・団体等の業種別報告件数



ランサムウェア被害件数(R4)：230件

出典：警視庁 「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」を編集して作成
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_cyber_jousei.pdf

ランサムウェア攻撃の主な手法例

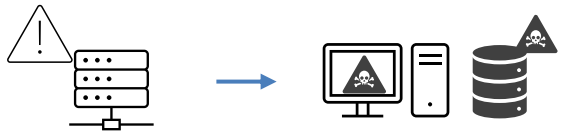
ばらまき型

■ ウイルスを添付した電子メール送付

機械的にウイルスを添付したメールを送付し、
添付ファイルからランサムウェアなどに感染させる。
感染するとファイルやデータが暗号化されてしまう。

■ VPN機器の脆弱性をついての侵入

アップデートがされていないVPN機器の脆弱性から
侵入しランサムウェアに感染させる。
ファイルやデータの暗号化や身代金の要求などの
危険性。



■ 標的型ランサムウェア攻撃

様々な手法で企業・組織のネットワークへ侵入(不正アクセス)。
ラテラルムーブメント(横方向への移動)から、管理サーバーを
乗っ取り、データを暗号化。復旧するための身代金を請求する。
標的となる企業に対して戦略的に行われ、高額な身代金請求や
データの売買を目的としている。

最近のランサムウェアの感染被害例

N社

【発生】
7月4日　N社内すべてのコンテナターミナル内で運用している**システム**に障害が発生。

【原因】
ランサムウェアの被害。
5か所のコンテナターミナル事務所と協会加盟事業者の一部から接続が可能で、**事業者側からの侵入（不正アクセス）**を受けた可能性がある。

【被害】
2日半にわたりコンテナ搬出入ができず、その解消には約一週間を要する見込みであると報じられた。

参照：https://meikoukyo.com/wp-content/uploads/2023/07/0bb9d9907568e832da8f400e529efc99.pdf

どのように侵入（不正アクセス）されたのか？

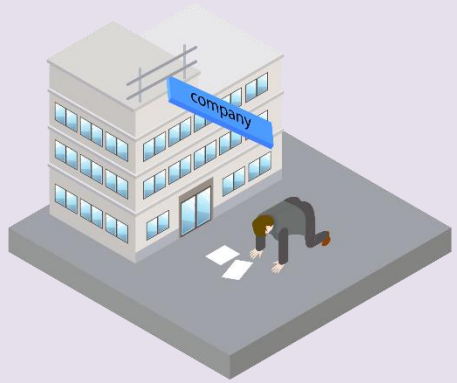
■ **VPN機器の脆弱性をついての侵入**
アップデートがされていないVPN機器の脆弱性から侵入しランサムウェアに感染させる

可能性があるとのこと

ランサムウェア攻撃のリスク

発生した場合に考えられるリスク

- 機密情報流出による損害賠償
- サプライチェーン全体の業務停止
- 多額の身代金支払いによる企業倒産
- 企業イメージの低下による収益損失
- 信頼関係の低下による取引先との取引停止　など



【事例】

大手製造（電機）

情報流出の可能性(2020年)

中国にある子会社への不正アクセスから、国内子会社のアカウント情報を窃取し、契約しているクラウドサービスや関連サーバーを攻撃したとされる。

大手自動車

工場の生産ライン停止(2022年)

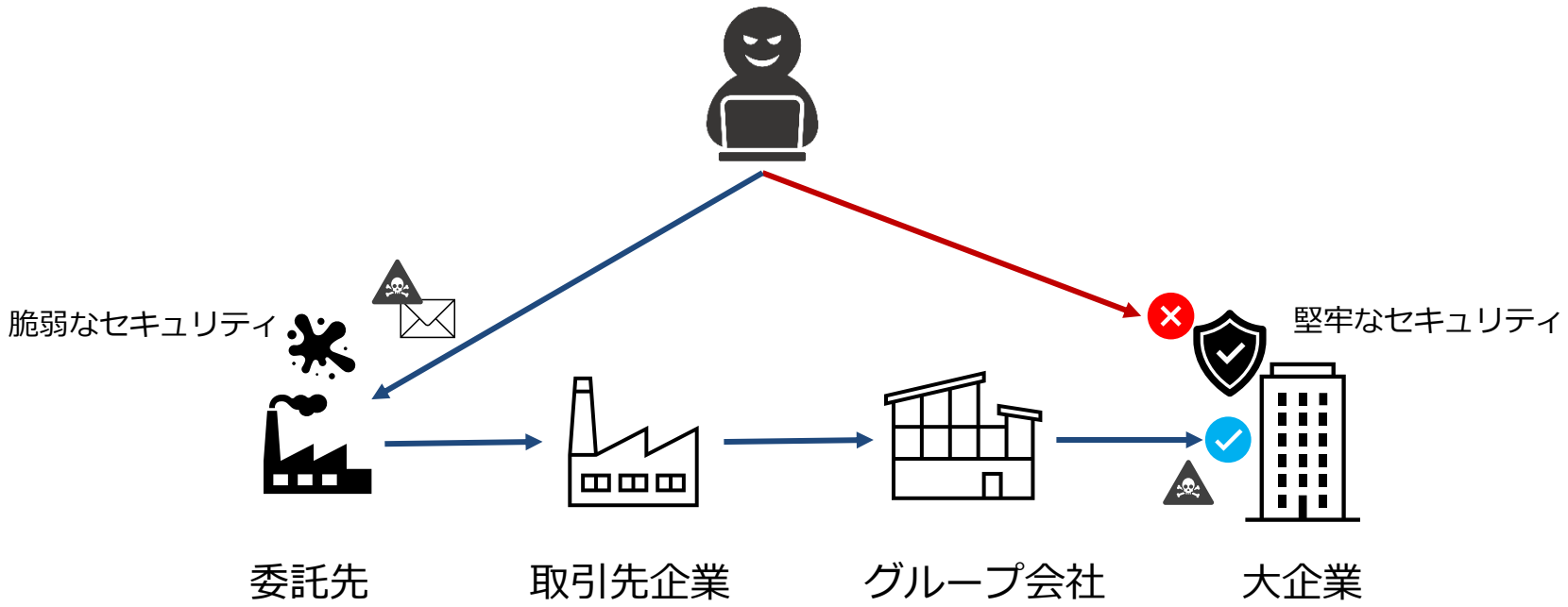
取引先となる部品メーカーにおけるマルウェアの感染により、グループ会社を含めた14工場28ラインが稼働停止。

参照：https://www.mitsubishielectric.co.jp/news/2021/0326.pdf

参照：https://global.toyota/jp/newsroom/corporate/39707924.html

【補足】サプライチェーン攻撃とは

サプライチェーンにおける、企業の繋がりや関連性を狙った攻撃。
セキュリティレベルが高く侵入が難しい大企業を直接狙わず、セキュリティ対策が手薄な関連企業や取引先企業を経由して、標的とする企業へ不正アクセスするサイバー攻撃。
大企業ほどのセキュリティ対策にコストをかけることが難しい中小企業が、
主なターゲットになっている。



ランサムウェア攻撃 対策例

【本人認証の強化】

- ✓ ID・パスワードだけでなく多要素認証の利用や不必要なアカウントの削除を行い、インシデント発生のスキを無くす

【定期的なログの確認による インシデントの早期発見】

- ✓ サーバーやネットワーク機器などのログを確認し、異変があった際に素早く気づく仕組みを構築することで、被害拡大を抑止する

【情報資産の見直し】

- ✓ セキュリティパッチや最新プログラムへの更新
  - VPNやゲートウェイなど、インターネット接続を行う機器は脆弱性を狙った攻撃を受けやすい

【データバックアップ等の取得】

- ✓ データの暗号化など不足の事態に備え、バックアップデータによるシステムの復旧手順などを確認する

2.内部不正による情報漏えいの被害とリスク

内部不正による情報漏えいの被害：最近の動向

【情報セキュリティ10大脅威 2023】

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

依然として増加傾向に

出典：IPA 「情報セキュリティ10大脅威 2023」を編集して作成
https://www.ipa.go.jp/security/vuln/10threats2023.html

内部不正とは？

社員やその関係者など会社内部の人による不正行為。
大きく2つの要因に起因する。

1. 人為的要因
   - 従業員による故意の情報の持ち出し
   - 横領
   - メールの誤送信　など

2. 技術的要因
   - PCやスマートフォンなどの情報漏洩の媒体となるものに対する
     セキュリティ対策を実施していない　など

実際にあった内部不正による情報漏えい：事例

【転職先企業への情報漏えい】
某企業のパートナー企業の技術者が、企業秘密のデータを転職先企業に提供した。その後調査では、技術者にはデータと引き換えに役員としての地位を与えることを約束していたことがわかった。

【市役所職員による情報流出】
某市議会に立候補していた元同市役所職員が自身の選挙に関して、有権者にハガキを送るために市民3万人分の個人情報を持ち出した。
一部のPCにはアクセス接続制限がされておらず、そこから情報を取得していたとされる。

【個人の借金返済のために個人情報の売却】
某教育系のグループ企業に勤めていた派遣のエンジニアが会員3,500万人の個人情報を流出。社内のシステムへのアクセス権限が大きかったこともあり誰にも気づかれることなく犯行を実施できた。

参照：https://www.benesse.co.jp/customer/bcinfo/01.htm
参照：http://www.jipa.or.jp/jyohou_hasin/sympo/pdf/jyohobouei/01_2.pdf
参照：https://www.city.hiratsuka.kanagawa.jp/joho/page06_00025.html

内部不正で起こり得るリスクや被害

情報資産に関するリスク

- 情報漏えい
- データ改ざん
- データの悪用
- データの隠蔽や削除

懸念：
金銭の略取
など

【想定される被害】

懸念：
個人情報流出
など

- 企業の信用喪失
- 将来的な売上の損失
- 既存顧客の損失

内部不正対策として

対策を一つすれば良い、というわけではなく様々な観点で行う必要があります。

内部不正を防ぐための管理の観点	
資産管理	情報の格付け、アクセス権指定・管理など
物理的管理	物理的な保護（情報機器など）と入退管理
技術・運用管理	内部不正モニタリングシステムの適用や ネットワーク利用のための安全管理など
原因究明と証拠確保	情報システムにおけるログ・証跡の記録と保存
人的管理	教育による内部不正対策の周知徹底
コンプライアンス	法的手続きの整備、誓約書の要請
職場環境	公平な人事評価の整備 適正な労働環境及びコミュニケーションの推進など
事後対策	事後対策に求められる体制の整備や 処罰等の検討及び再発防止
組織の管理	内部不正に関する通報制度の整備など

出典元：IPA 【組織における 内部不正防止ガイドライン】
https://www.ipa.go.jp/security/guide/hjuojm00000055l0-att/ps6vr7000000jvcb.pdf

最優先で行うべき対応は？

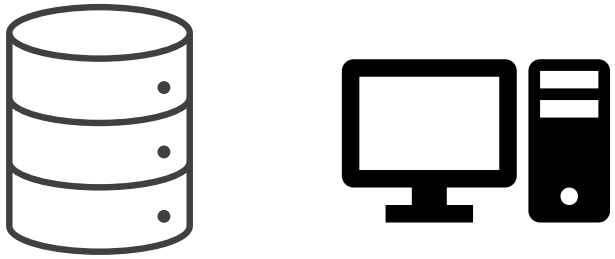
内部不正を防ぐための管理の観点	
原因究明と証拠確保	情報システムにおけるログ・ 証跡の記録と保存

出典元：IPA 【組織における 内部不正防止ガイドライン】
https://www.ipa.go.jp/files/000057060.pdf

情報漏えいが発生した際には、流出元・原因の特定に証跡（ログ）が欠かせません。
ログの監査を行うことで、その経緯を把握し不正アクセスの被害の拡大を抑止することができます。
対策をしている間にも情報漏えいはいつ発生するか分かりませんので、まずは証跡を残せる環境を整えることを推奨します。

ログの監査はどうすればよい？

PCやサーバーなどのコンピューターは操作した内容を記録しています。
ログの監査は、記録（ログ）内容をもとにルールに則って正しく使われているかなどを確認します。
様々な種類のログがありますが、情報漏えいの元となるのはファイル（データ）なので、
まずはファイルへのアクセスログを監査していくことを推奨します。



- システムログ
- パソコンログ
- サーバーログ
- **ファイルアクセスログ**

3.多層防御での対策と強化すべきポイント

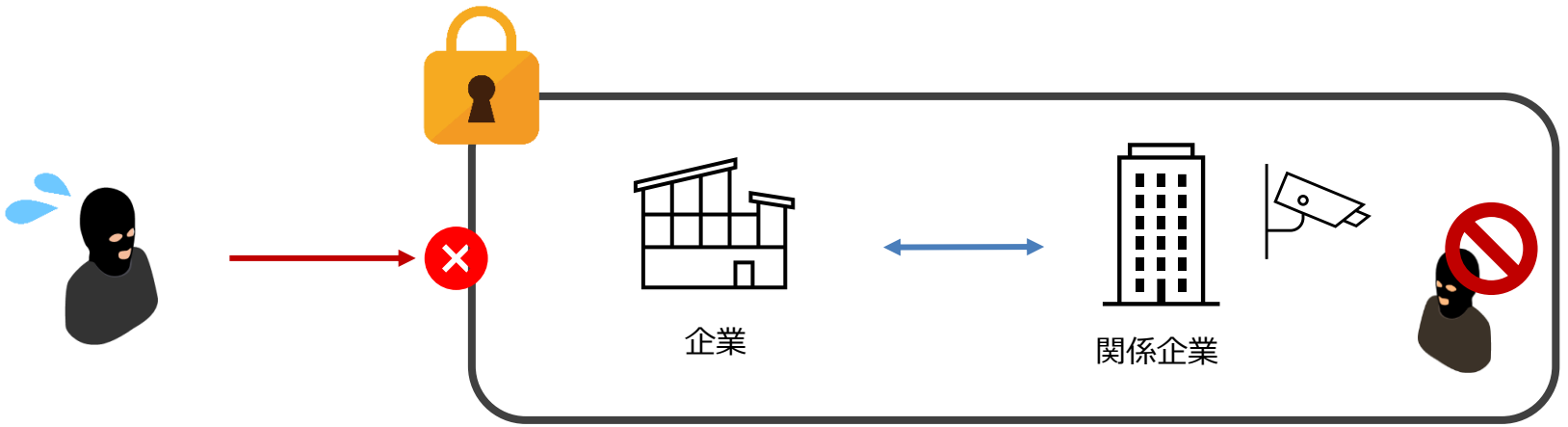
不正アクセスや内部不正に対するセキュリティ対策が必要

様々な手段を使いネットワークへ不正アクセス後、ランサムウェアに感染させるケースが多い。

関係企業含めてシステムやネットワークに侵入させないことが重要！
（サプライチェーン）

しかし、どんなに対策しても不正アクセスや内部不正を100%防げるとは限りません。

【多層防御】を提案します！



重要性が増す多層防御

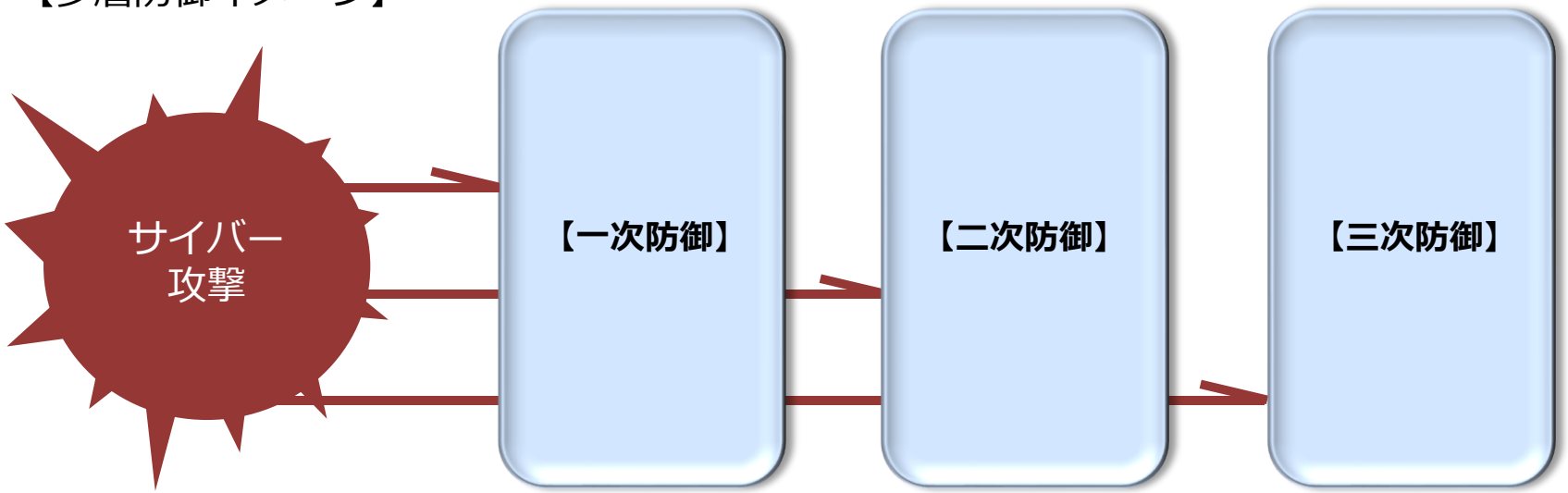
■ 多層防御とは

- 複数の防御層を重ねてセキュリティ対策することでサイバー攻撃の脅威から情報資産を守ること

■ 多層防御はなぜ必要か

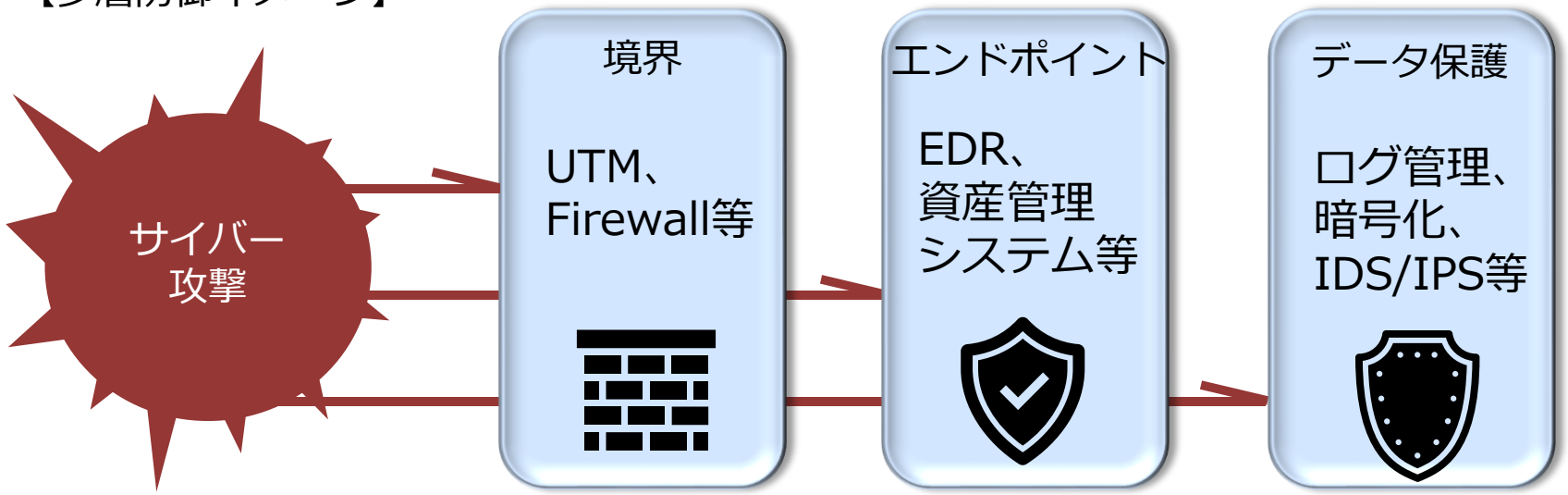
- サイバー攻撃の高度化に伴い、従来の**境界型セキュリティでは限界がある**
- 不正アクセスや**内部不正に対するゼロトラスト**な姿勢が求められる
- 多層防御(= 検出ポイントを増やす)により**不正監視**を強化できる

【多層防御イメージ】



一般的な多層防御イメージと対応するセキュリティツール

【多層防御イメージ】



■ 入り口対策

- 不正アクセスやマルウェアの内部ネットワークへの侵入を防ぐための対策

■ 内部対策

- 不正アクセスや侵入したマルウェアの感染を拡大を防ぐための対策

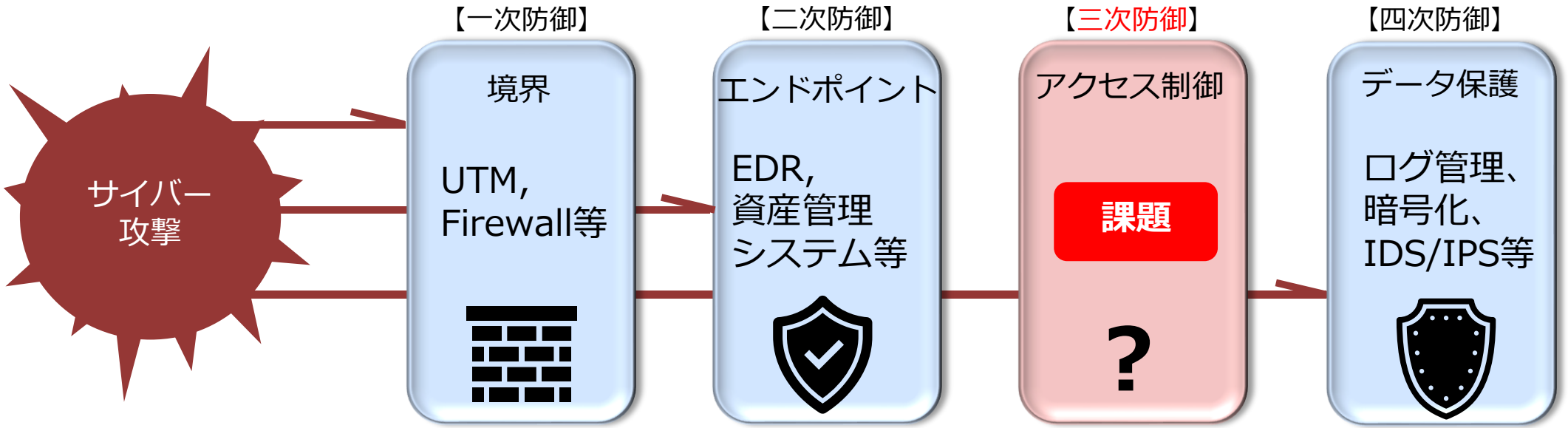
■ 出口対策

- 不正アクセスや侵入したマルウェアの外部への感染を防ぐための対策

ランサムウェア攻撃対策として不足しているアクセス制御

- 多くの組織は境界、エンドポイント、データ保護層については対応が進んでいる
- 一方で、**アクセス制御**は対応が後手に回りがち

多くの組織ではアクセス制御が不足し、
多層防御として対策が不十分になっている



Active Directoryだけではアクセス制御は不十分

Windowsサーバーに搭載されている機能。
管理するネットワーク上にある資源や利用者の情報や権限などを一元管理できる。

【機能：例】

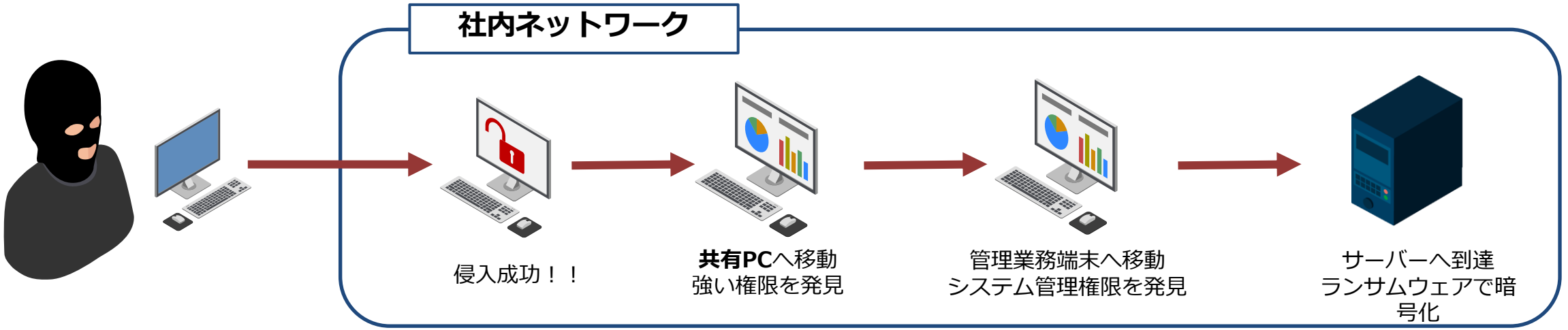
- **ユーザー認証とアクセス制御**
  - ユーザーIDとパスワードを使ってユーザー認証を行う。ドメインごとの権限（ルール）に則ったユーザーの制御を行うことができる。

一回でも認証が通ってしまえば、権限内で何でもできてしまう。
なりすましなどの外部から不正アクセスをされた場合には、
制御を行うことができない。

アクセス制御が不十分だとラテラルムーブメントの危険性が

■ ラテラルムーブメントとは

- 攻撃者が組織のネットワークに侵入したあとに、情報資産にアクセスするために使用する一連の手法
- 攻撃者は、正規ユーザになりすましラテラルムーブメント(横方向への移動)により権限の強いWindowsアカウント情報を数週間から数か月かけて窃取しネットワーク全体を掌握する
- **社内のアクセスは安全という通説が通用しづらい（ゼロトラスト）**



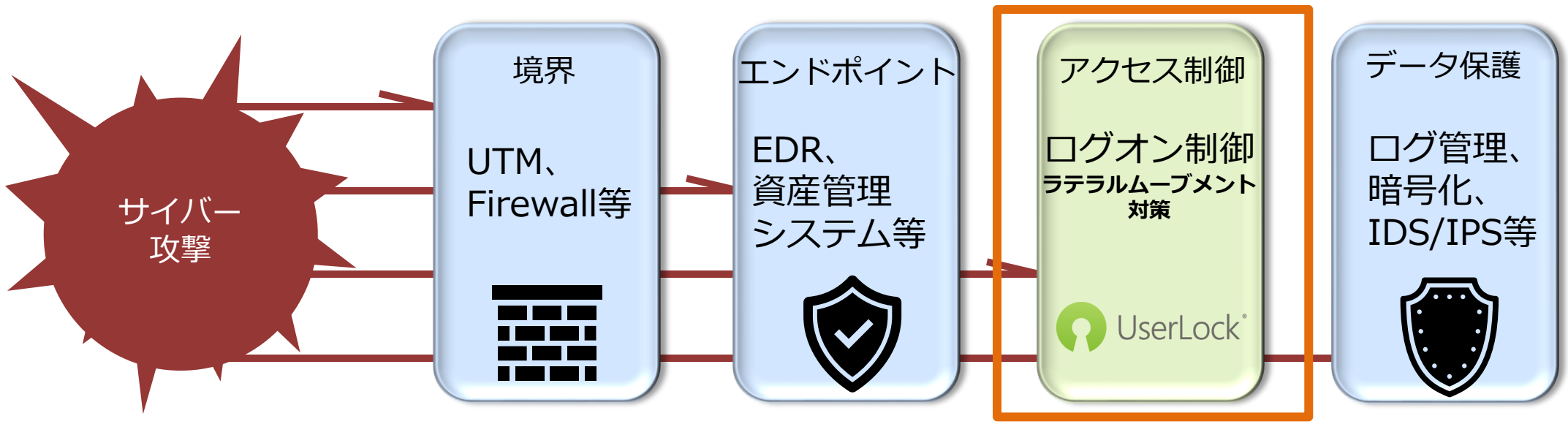
アクセス制御が不十分だとラテラルムーブメント（ランサムウェア攻撃）は防げない!!
社内ネットワーク内のアクセスにもセキュリティ対策は必須!!

アクセス制御の実装による内部セキュリティの強化

■ 既存セキュリティ製品と被らないユニークな守備範囲で多層防御を実現

- UserLockはアクセス制御にピンポイントでセキュリティを実装
- ログオン制御やラテラルムーブメント対策に特化した機能を提供

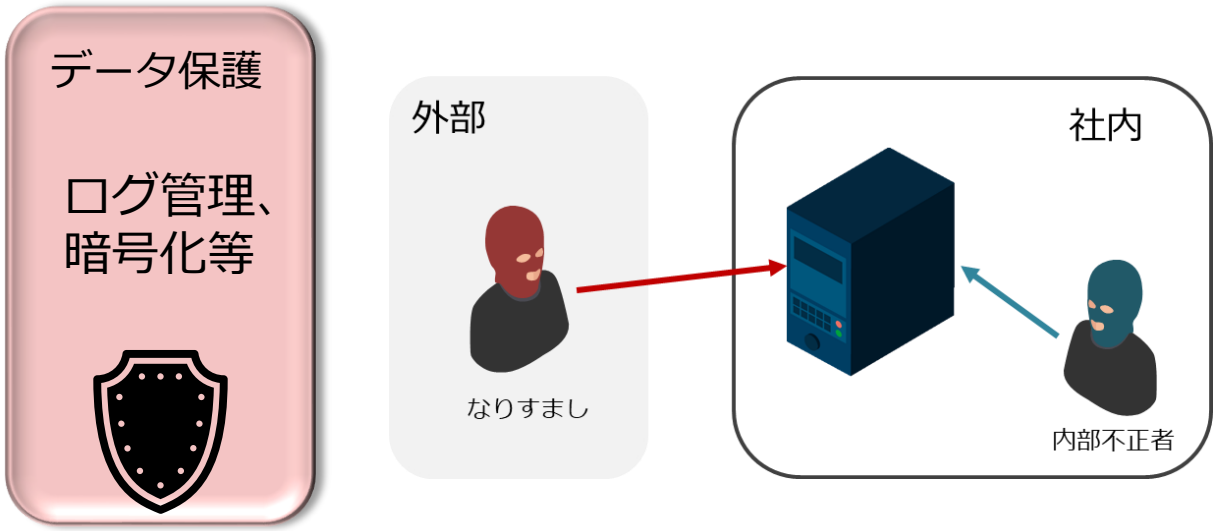
UserLock® でアクセス制御を実装し、
ランサムウェア攻撃の被害を防ぐ。



内部不正対策として必要なデータ保護層の強化

内部による不正やなりますましによる侵入など、最終的には保管されているデータ（情報資産）へのアクセス目的です。ログ管理はファイルサーバーやクラウドストレージなど不審な動きに気づき、被害の拡大を防ぐのに有効です。

対策としてファイルの暗号化という方法もありますが、運用ルールの変更やシステム導入などハードルが少々高いため、まずは手軽に始められるログ管理を推奨します。

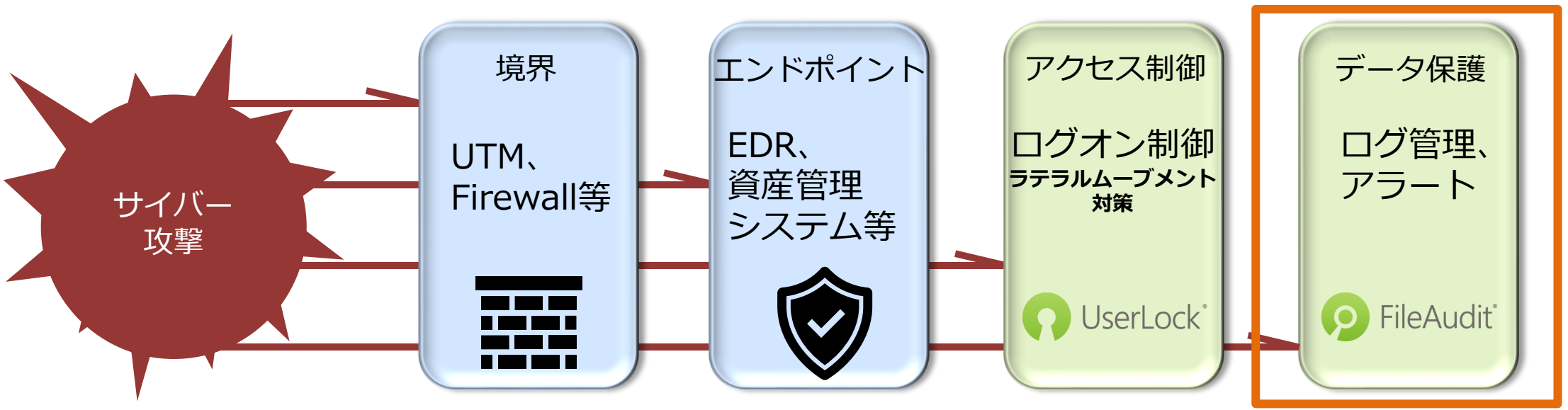


ログ管理から適切なデータ保護とファイルセキュリティの強化

■ 非IT管理者でも運用できるシンプルなログ管理ツール

- FileAuditはファイルサーバー・クラウドストレージのファイルアクセスログ管理が可能
- ワンクリックでアクセス状況を確認し、柔軟なアラート設定で素早く異常を検知

FileAudit® で内部不正に
いち早く気づく環境を整える。



4.UserLockによるアクセス制御

UserLockとは

UserLock®

ActiveDirectoryと連携し既存環境に簡単にアドオンできる
アクセス制御ツール

多要素認証 の付加	柔軟な **ログイン制御**	**クローズド環境** 対応	**シングルサインオン** の付加
ログイン管理			

UserLock製品コンセプト

■ Active Directoryの認証を強化

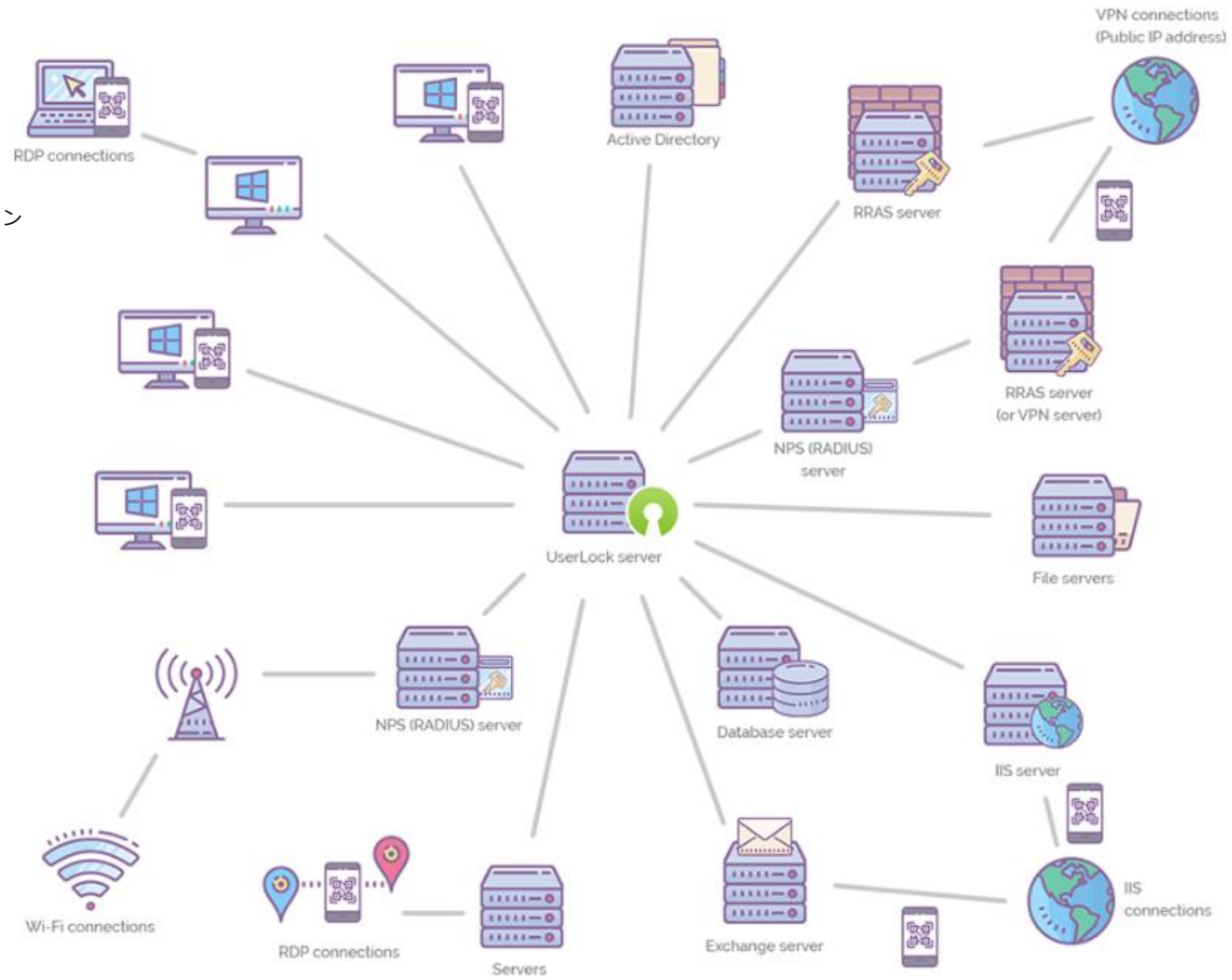
オンプレミスAD認証と連携し、以下のログインを保護します

1. 対話型セッション※（ワークステーションおよびターミナル）
   ※Windowsマシンへの直接ログオン、もしくはRDPログオンによって確立されるセッション
2. Wi-Fi セッション
3. VPN セッション
4. IIS セッション
5. ローカルアカウントのセッション(監査のみ)

ADでログイン認証するポイント

＝

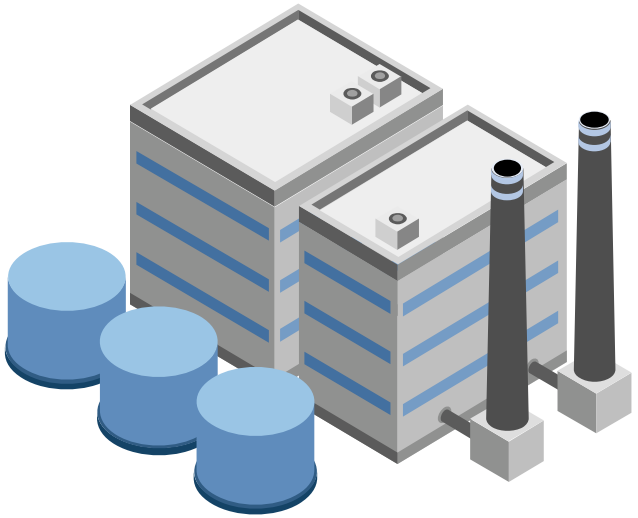
UserLockで保護するポイント



UserLockの動向について

日本国内でも多くの組織がセキュリティ強化でUserLockを検討中

- **業界**
  - 自治体、製造、IT、インフラ、防衛、金融等
- **お客様の特徴**
  - ① ガイドライン等で高いセキュリティ対策が求められている
  - ② ハイブリッドワークを行っている
  - ③ 既存のセキュリティ対策にプラスアルファが欲しい
  - ④ サプライチェーンの一角としてセキュリティ対策が必要　**等々**



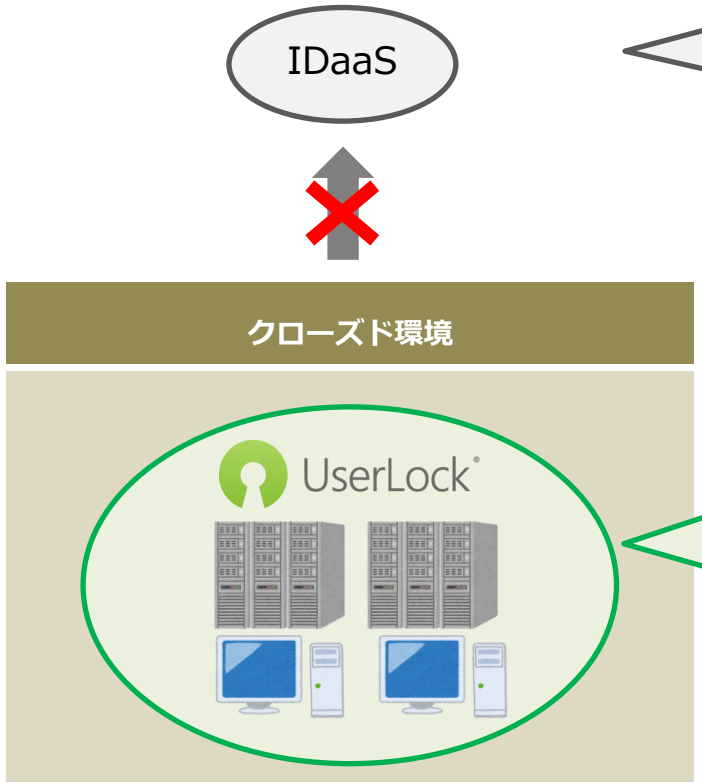
上記は一例にすぎません。
UserLockは業種・業界問わずセキュリティ強化を希望する全ての業界でご利用いただけます。

ユースケース：クローズド環境におけるアクセス制御

■ クリティカルなネットワークでは原則インターネット接続が許可されていない

→ **AD情報を外に出さないオンプレミス型のアクセス制御システムが必要**

→ **インターネット接続を必要とするIDaasでは対応不可**



IDaaS
- クラウド利用が前提
- OS、ネットワークレベルのアクセス管理は非対応

UserLock
- オンプレミスActive Directoryと連携
- **完全オンプレミス**での二要素認証やアクセス制御を実現

ユースケース：多要素認証＋同時ログイン制御によるなりすまし対策

■ 不正アクセスからのラテラルムーブメントの脅威

社員のアカウントになりすましながら、機密情報が保持された端末を狙う

→ IDとパスワードだけでは、なりすましログインのリスクが残ってしまう

■ なりすましログイン対策には多要素認証＋同時ログイン制御が有効

- 社員間のアカウント不正利用を防ぐ
- 不正利用検知時にシステム管理者だけでなく、社員自身にもアラートを通知

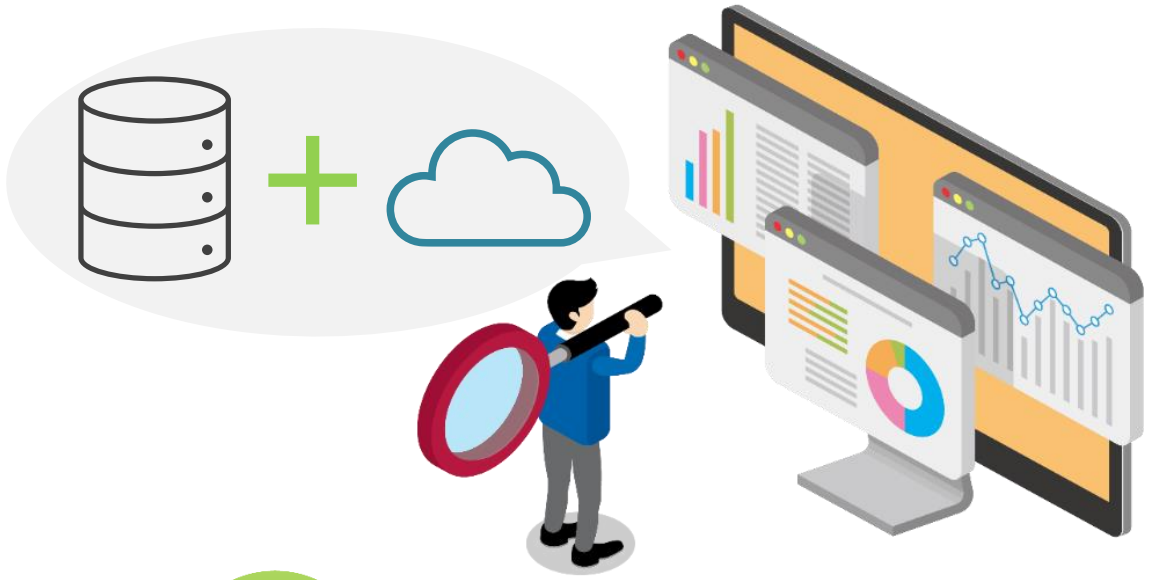
ユースケース：踏み台サーバーを運用したシステムのセキュリティ強化

- サプライチェーンの共有ネットワークやサーバーへのログイン
  - → ID・パスワードだけでは踏み台サーバーへ不正ログインされてしまう可能性がある
  - → 深夜・休日などの業務時間外のアクセス拒否ができない
  - → アクセス状況の可視化ができない

- 二要素認証＋柔軟なセキュリティポリシーの追加によりセキュリティの強化
  - 踏み台サーバーだけでなく、接続先のサーバーも保護
  - アクセス状況のリアルタイム監視とアラート通知で不正ログインを素早く把握

5.FileAuditによるログ監査・ファイルセキュリティ強化

FileAuditとは



FileAudit®
ファイルオーディット

ファイルアクセス監査・セキュリティ強化

オンプレミス・クラウドストレージに対応した、非IT管理者でも使いこなせるように設計されたシンプルなファイルアクセスログ管理ツール。ログ管理だけでなく、ファイルセキュリティの強化を実現。

FileAudit 特徴

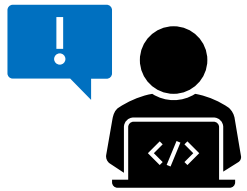
セキュリティ・ITガバナンス強化・現場運用の広範囲をカバー

オンプレミス & クラウド対応

- Windowsファイルサーバー
- Dropbox/O365/Google/ Box
- 一元的なファイルログ管理

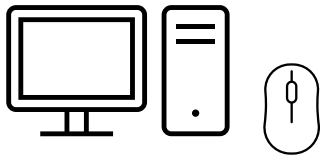
情報漏えい対策

- 内部不正対策
- 不正アクセス検出
- ランサムウェア攻撃被害の拡大の抑止



導入・利用が容易

- エージェントレス
- 非IT管理者による運用を想定したUI



ログ管理における3つのポイント

1. いつでもログを視認できる環境

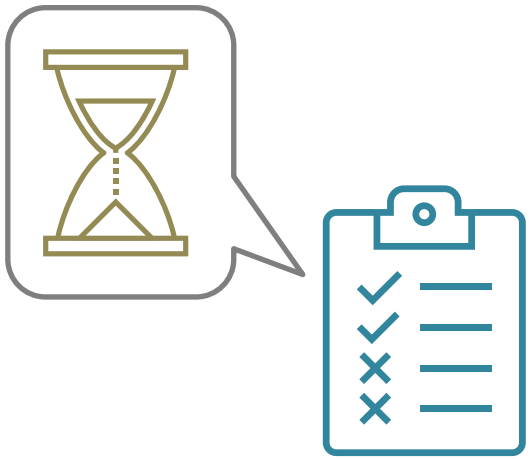
2. ログの一貫性の確保

3. いかに早く異常に気付けるか

1.いつでもログを視認できる環境

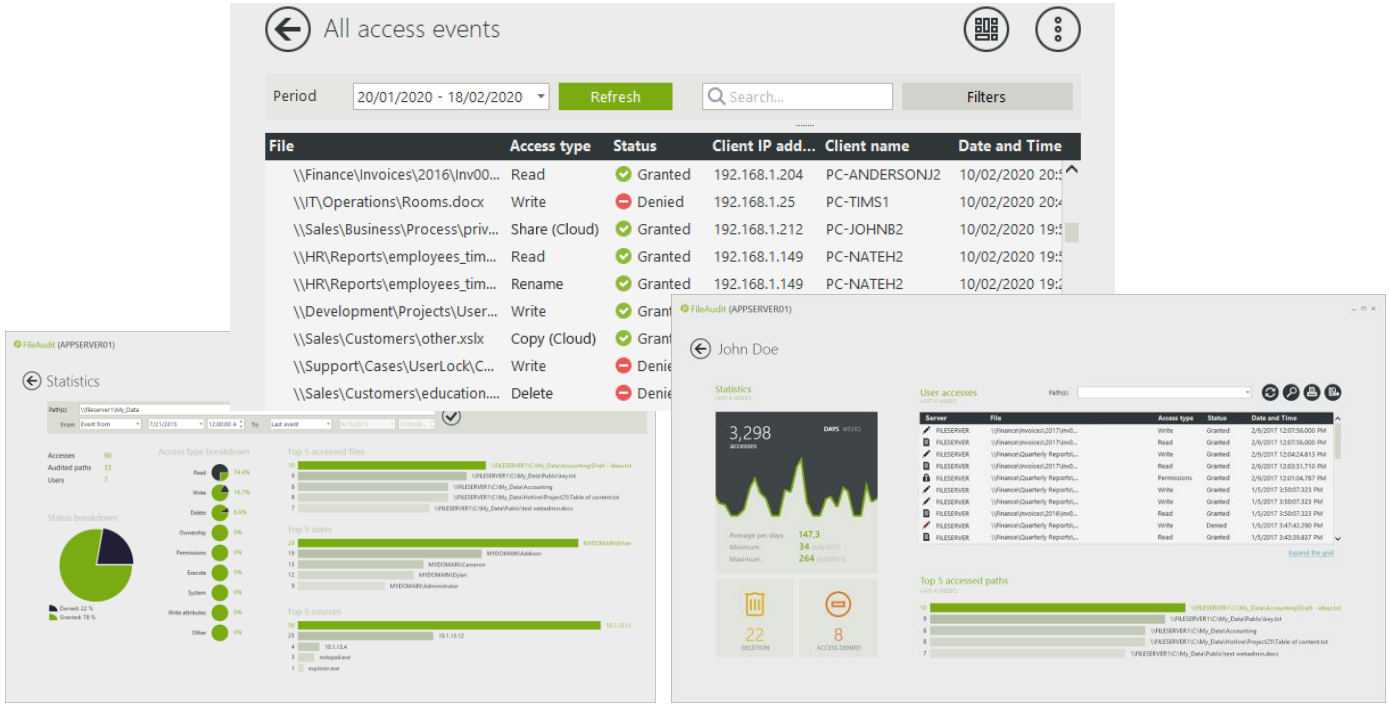
【課題】

定期的なログの確認として、様々な場面で
レポートの作成が求められる。
その都度、CSVで出力してデータを抽出・
整形するという作業に時間がかかっている。



【FileAuditなら】

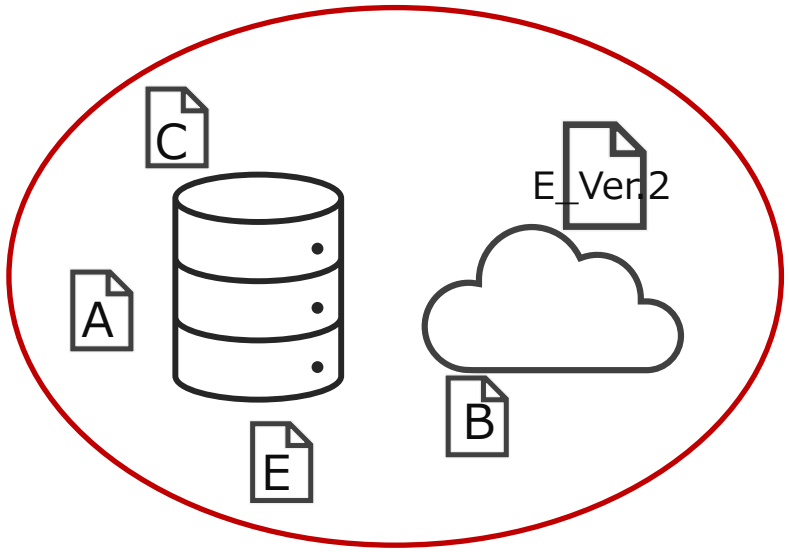
ワンクリックでレポート表示。アクセスイベント（読み込みや削除など）ごとに簡単に確認することができます。またユーザーがいつ・どのようなファイルを開いたか確認することもできます。



2.ログの一貫性の確保

【課題】

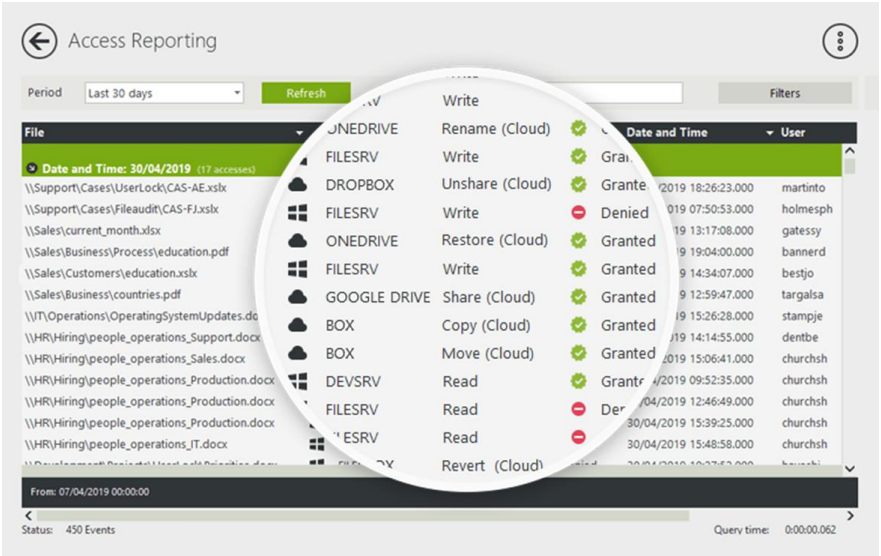
ユーザーが様々な場所にファイルを保存するため、ファイルが散在し管理の手間がかかっている。ログの一貫性を欠いている状態になりがち。



【FileAuditなら】

ファイルサーバー・クラウドストレージに対応しているため、ひとまとめに確認することが可能。横串検索も対応。

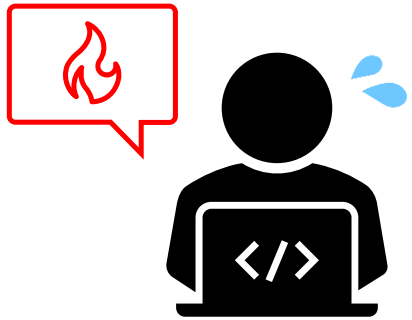
OneDrive　SharePoint Online　box
Dropbox Business　Google Drive



3.いかに早く異常に気付けるか

【課題】

一般的なログツールはログをチェックするまで、何か問題が起きていないか気付き、対応することができない。
とは言えど、ログの監査をこまめにやる余裕もなく、そもそも問題に気づく仕組みがない



【FileAuditなら】

様々な条件でアラートを柔軟に設定することが可能。例えば、退職間際の社員による機密情報の持ち出しの際は大量にファイルをダウンロードすることが想定されますが、アクセス時間やファイル数など細かく設定し、アラートを通知することで素早く気づくことができます。

FileAuditで手間なくセキュアなログ監査を実現

FileAudit®

1. **手間がかからないログ管理**
   （レポート作成不要、エージェントレス、シンプルなUI）

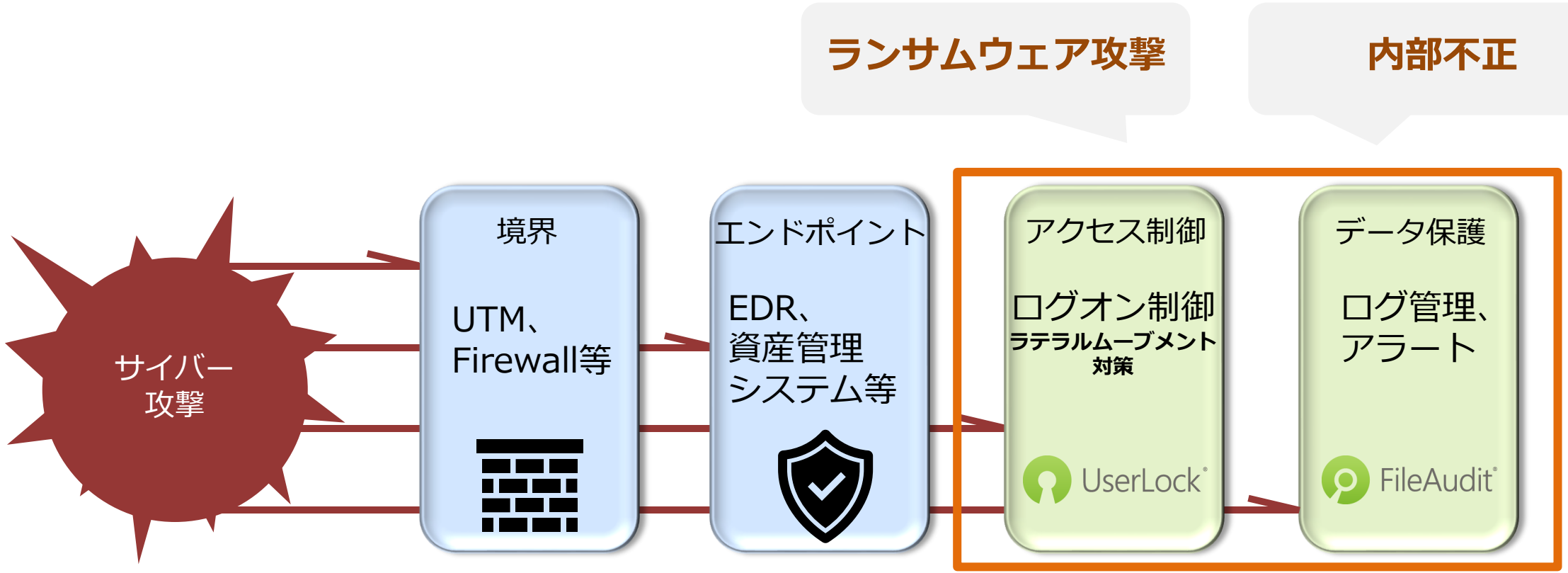
2. **ログの一貫性の確保**
   （クラウドストレージ対応）

3. **異常に気づくことができる環境：柔軟なアラート通知**
   （内部不正や不注意、なりすましによる情報漏えいの被害拡大の抑止）

6.まとめ

多層防御：より強固なセキュリティ環境の実装へ

多層防御に【アクセス制御の実装】、【データ保護層の強化（ログ管理）】を行うことで、
ランサムウェア攻撃や内部不正対策に対応したより強固なセキュリティ環境を構築することができます。
今後のサイバーセキュリティ対策の検討の一助になりましたら幸いです。



OCEANBRIDGE

つかえるITを、世界から。

製品、サービス、その他ご質問やご不明な点などございましたら
下記までお問い合わせください

ISD製品担当：
userlock@oceanbridge.jp

株式会社オーシャンブリッジ

〒107-0051　東京都港区元赤坂一丁目5番12号 住友不動産元赤坂ビル7階
TEL：03-6809-0967　FAX：03-6809-0976
www.oceanbridge.jp