LANSCOPE cloud

最新のセキュリティ対策のポイントが分かる

# 情報セキュリティ10大脅威から見る 2022年に注力すべき エンドポイントセキュリティ

# 社会的影響が大きい事案を元にIPAが選出した選考員150名による審議・投票によって決定

情報セキュリティ分野の研究者や企業の実務担当者などが選出されており、エムオーテックスからも3名の選考員が参加


情報セキュリティ

10 大脅威 2021

～よもや自組織が被害に！呼吸を合わせて全力防御！～

株式会社

ERROR

IPA 独立行政法人情報処理推進機構 セキュリティセンター

2021 年 2 月


1位 ランサムウェアによる被害

～組織を狙ったランサムウェアの攻撃が増加～

ランサムウェアとはウイルスの一種で、PC やサーバー、スマートフォンがこのウイルスに感染すると、保存されているデータが暗号化されて利用できなくなったり、画面がロックされて端末が利用できなくなったりする。そしてそれを復旧することと引き換えに金銭を要求される等の被害が発生する。また、データの暴露を行うと脅迫され、金銭の支払い有無にかかわらず、データが暴露されてしまったケースが近年発生している。

＜攻撃者＞
- 組織的犯行グループ
- 犯罪者

＜被害者＞
- 個人
- 組織

＜脅威と影響＞

PC やスマートフォンのデータを暗号化し、データを復旧することと引き換えに、金銭を要求したりコンタクトを促したりする脅迫文を画面に表示するランサムウェアと呼ばれるウイルスの感染が確認されている。ランサムウェアは、メールの添付ファイルを開いたり、ソフトウェアの脆弱性等を悪用されたりすることで感染する。

また、ランサムウェアにより暗号化したデータを復旧するための金銭要求に加え、暗号化する前にデータを窃取しておき、支払わなければデータを公開する等と脅迫する「二重の脅迫（double extortion）」と呼ばれる攻撃も確認されている。

近年、個人よりも多額の金銭の支払いを見込めるためか、組織が狙われやすい傾向にある。

脅迫に従うことによる金銭的被害に加え、暗号化および窃取されたデータが組織にとって重要な情報であった場合、業務の遂行に大きな支障が出たり、個人情報漏えいによる信用の失墜や経済的損失につながったりするおそれがある。なお、金銭を支払ってもデータが復旧されるとは限らない。

＜攻撃手口＞

◆ メールから感染させる

メールの添付ファイルやメール本文中のリンクを開かせることでランサムウェアに感染させる。

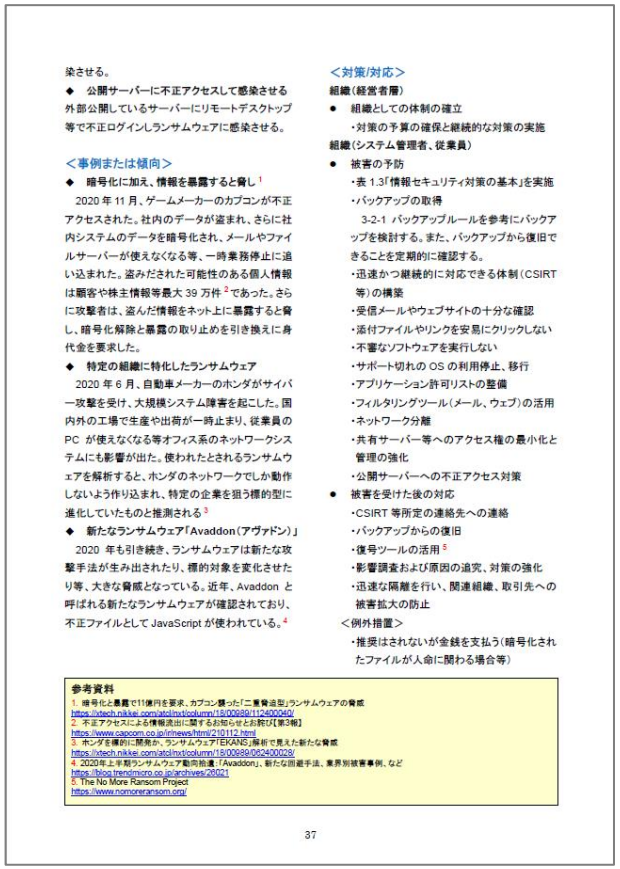
◆ ウェブサイトから感染させる

脆弱性等を悪用しランサムウェアをダウンロードさせるよう改ざんしたウェブサイトや攻撃者が用意したウェブサイトを閲覧させることで、ランサムウェアに感染させる。

◆ 脆弱性によりネットワーク経由で感染させる

ソフトウェアの脆弱性が未対策のままインターネットに接続されている PC に対して、その脆弱性を悪用してインターネット経由でランサムウェアに感染させる。

36


染させる。

◆ 公開サーバーに不正アクセスして感染させる

外部公開しているサーバーにリモートデスクトップ等で不正ログインしランサムウェアに感染させる。

＜事例または傾向＞

◆ 暗号化に加え、情報を暴露すると脅し[1]

2020 年 11 月、ゲームメーカーのカプコンが不正アクセスされた。社内のデータが盗まれ、さらに社内システムのデータを暗号化され、メールやファイルサーバーが使えなくなる等、一時業務停止に追い込まれた。盗みだされた可能性のある個人情報は顧客や株主情報等最大 39 万件[2]であった。さらに攻撃者は、盗んだ情報をネット上に暴露すると脅し、暗号化解除と暴露の取り止めを引き換えに身代金を要求した。

◆ 特定の組織に特化したランサムウェア

2020 年 6 月、自動車メーカーのホンダがサイバー攻撃を受け、大規模システム障害を起こした。国内外の工場で生産や出荷が一時止まり、従業員の PC が使えなくなる等オフィス系のネットワークシステムにも影響が出た。使われたとされるランサムウェアを解析すると、ホンダのネットワークでしか動作しないよう作り込まれ、特定の企業を狙う標的型に進化していたものと推測される[3]

◆ 新たなランサムウェア「Avaddon（アヴァドン）」

2020 年も引き続き、ランサムウェアは新たな攻撃手法が生み出されたり、標的対象を変化させたり等、大きな脅威となっている。近年、Avaddon と呼ばれる新たなランサムウェアが確認されており、不正ファイルとして JavaScript が使われている。[4]

＜対策/対応＞

組織（経営者層）
- 組織としての体制の確立
  - ・対策の予算の確保と継続的な対策の実施

組織（システム管理者、従業員）
- 被害の予防
  - ・表 1.3「情報セキュリティ対策の基本」を実施
  - ・バックアップの取得

    3-2-1 バックアップルールを参考にバックアップを検討する。また、バックアップから復旧できることを定期的に確認する。
  - ・迅速かつ継続的に対応できる体制（CSIRT 等）の構築
  - ・受信メールやウェブサイトの十分な確認
  - ・添付ファイルやリンクを安易にクリックしない
  - ・不審なソフトウェアを実行しない
  - ・サポート切れの OS の利用停止、移行
  - ・アプリケーション許可リストの整備
  - ・フィルタリングツール（メール、ウェブ）の活用
  - ・ネットワーク分離
  - ・共有サーバー等へのアクセス権の最小化と管理の強化
  - ・公開サーバーへの不正アクセス対策
- 被害を受けた後の対応
  - ・CSIRT 等所定の連絡先への連絡
  - ・バックアップからの復旧
  - ・復号ツールの活用[5]
  - ・影響調査および原因の追究、対策の強化
  - ・迅速な隔離を行い、関連組織、取引先への被害拡大の防止

＜例外措置＞
- ・推奨はされないが金銭を支払う（暗号化されたファイルが人命に関わる場合等）

参考資料
1. 暗号化と暴露で11億円を要求、カプコン襲った「二重脅迫型」ランサムウェアの脅威
https://xtech.nikkei.com/atcl/nxt/column/18/00989/112400040/
2. 不正アクセスによる情報流出に関するお知らせとお詫び【第3報】
https://www.capcom.co.jp/ir/news/html/210112.html
3. ホンダを襲撃に関与か、ランサムウェア「EKANS」解析で見えた新たな脅威
https://xtech.nikkei.com/atcl/nxt/column/18/00989/062400028/
4. 2020年上半期ランサムウェア動向抽選「Avaddon」、新たな回避手法、業界別被害事例、など
https://blog.trendmicro.co.jp/archives/28021
5. The No More Ransom Project
https://www.nomoreransom.org/

37

出典：2021年2月26日 IPA 「情報セキュリティ10大脅威 2021」解説書

© 2022 MOTEX Inc.

# 脆弱性を狙った攻撃が新たに登場！ 2022年はサイバー攻撃などの外部脅威が占める結果に

2021年に登場したテレワーク等のニューノーマルな働き方を狙った攻撃も継続でランクイン

| | 順位 | 組織 | 昨年順位 |
|---|---|---|---|
| 外部 | 1位 | ランサムウェアによる被害 | 1位 ▬ |
| 外部 | 2位 | 標的型攻撃による機密情報の窃取 | 2位 ▬ |
| 外部 | 3位 | サプライチェーンの弱点を悪用した攻撃 | 4位 ↑ |
| 外部 | 4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 | 3位 ↓ |
| 内部 | 5位 | 内部不正による情報漏えい | 6位 ↑ |
| 外部 | 6位 | 脆弱性対策情報の公開に伴う悪用増加 | 10位 ↑ |
| 外部 | 7位 | 修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃） | NEW |
| 外部 | 8位 | ビジネスメール詐欺による金銭被害 | 5位 ↓ |
| | 9位 | 予期せぬIT基盤の障害に伴う業務停止 | 7位 ↓ |
| 内部 | 10位 | 不注意による情報漏えい等の被害 | 9位 ↓ |

## 👉 今期のポイント

脅威は、**外部からの攻撃**と**内部からの情報漏えい**の２パターンで**外部からの脅威が半分以上を占める**

注目は、新たに登場した「修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）」で、**脆弱性対策が施される前**に攻撃を受ける脅威が急増

多彩な働き方が拡がる中、**社外におけるセキュリティ対策が**間に合わず狙われる傾向にある

**内部不正による情報漏えい**がランクアップ！退職者などの情報持ち出し事件が多発している

※引用：IPA「情報セキュリティ10大脅威2022」
https://www.ipa.go.jp/security/vuln/10threats2022.html

© 2022 MOTEX Inc.

外部脅威

## ここ数年はマルウェア・ランサムウェア攻撃が増加中！凶悪化することで被害も拡大中です

### 食品加工業

ランサムウェア攻撃を受け**一部工場の操業を停止**せざるを得なくなった。大半のシステムは復旧していたが、**さらなる攻撃で顧客や従業員のデータが危険にさらされるリスク**を考慮して社内のIT専門家および第三者のサイバーセキュリティ専門家と協議の上、身代金を支払った

**身代金支払額**
**約12億円**

### インフラ業

システムにマルウェアが侵入して短時間で **100GB 以上のデータが搾取**。**その一部をインターネットに公開すると脅迫**があり身代金要求を受けていた。同時に第三者がパイプラインへの攻撃を可能とする情報を入手したため、**燃料パイプラインの操業を停止。一部地域で燃料が不足**して住民はパニックに陥った。

**身代金支払額**
**約4億8000万円**

### 医療機関

**電子カルテがランサムウェア**に感染。**バックアップデータも暗号化**されたため復旧に時間を要した。
結果、過去処方した薬剤や診療履歴が分からず、**一時診療が出来なくなった**。約2ヶ月診療人数を制限しつつ対応。身代金要求を受けていたが応じなかった。

**身代金支払額**
**0円（支払いに応じず）**

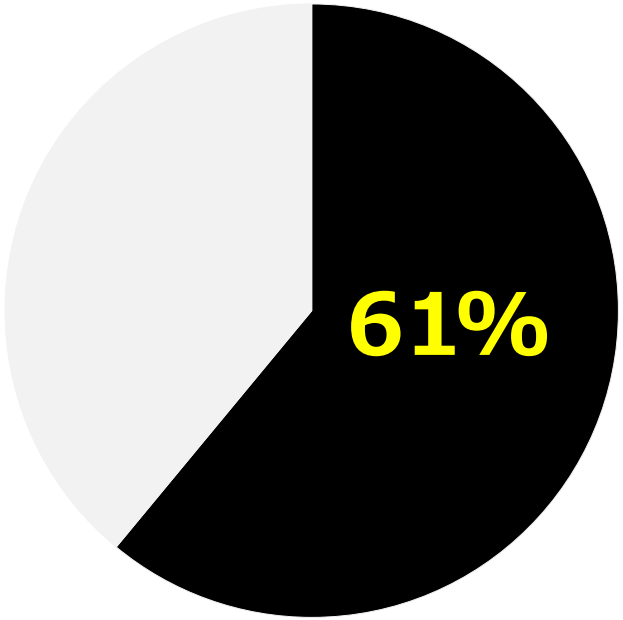
© 2022 MOTEX Inc.

外部脅威

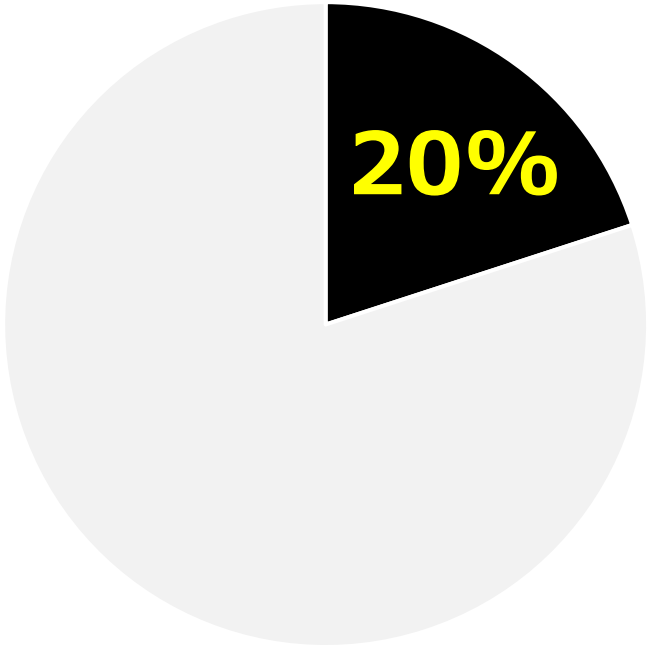
# 多くの組織では支払いを拒否しているものの、一部では2億円の身代金を支払っている

一度支払うと再度脅迫され、追加の身代金を支払うケースも確認されている

**日本の調査対象者のうち過去1年以内に**
**ランサムウェア被害に遭った割合**




**被害組織のうち**
**実際に身代金を払った割合**




**支払った身代金の平均額**

**225万ドル**
**（約2億2500万円）**

**身代金の支払い後、さらなる脅迫を受けた割合**

**100%**
**(平均95万ドルを追加で支払い)**

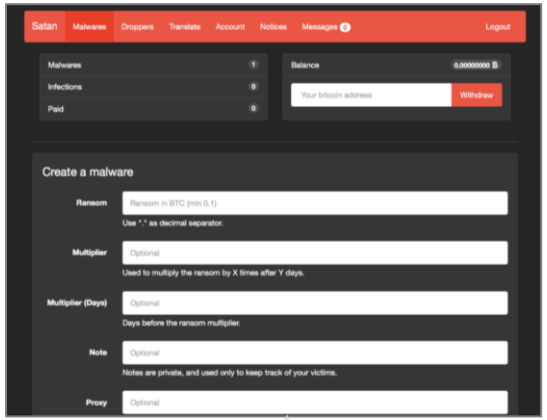
出典：一般社団法人日本プライバシー認証機構「拡大するランサムウェアビジネス」より引用
2021年9月～11月、日本や諸外国の主要業界に従事するITセキュリティ担当者2,200人を対象に調査

© 2022 MOTEX Inc.

外部脅威

## 企業をランサムウェアに感染させることでカンタンに報酬を得られる仕組み
## 「Ransomware as a Service（通称：RaaS）というビジネスモデルが闇ビジネス化しています

### ランサムウェア作成




闇サイトの RaaS サイトを活用。
必要事項を入力するだけで
簡単にランサムウェアを作成！

### 攻撃

作ったランサムウェアで PC を
攻撃。データを暗号化し、身代
金を請求

### 報酬を山分け

【RaaS 提供者】　【攻撃者】

振り込まれた身代金を RaaS
サイト提供者と攻撃者で山分け

© 2022 MOTEX Inc.

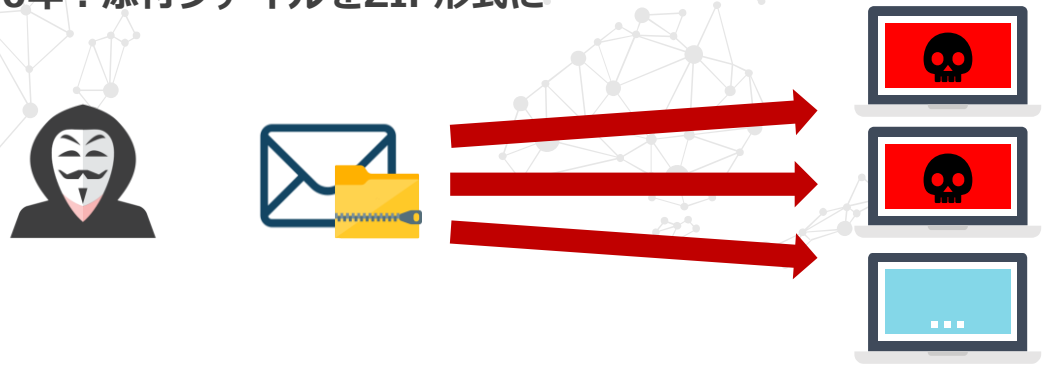
外部脅威

# Emotetによる被害が再燃！！対策するも攻撃手法を進化させ凶悪化し続けています

## Emotetの攻撃手法

### 2019年：Wordの添付ファイル

### 2020年：添付ファイルをZIP形式に

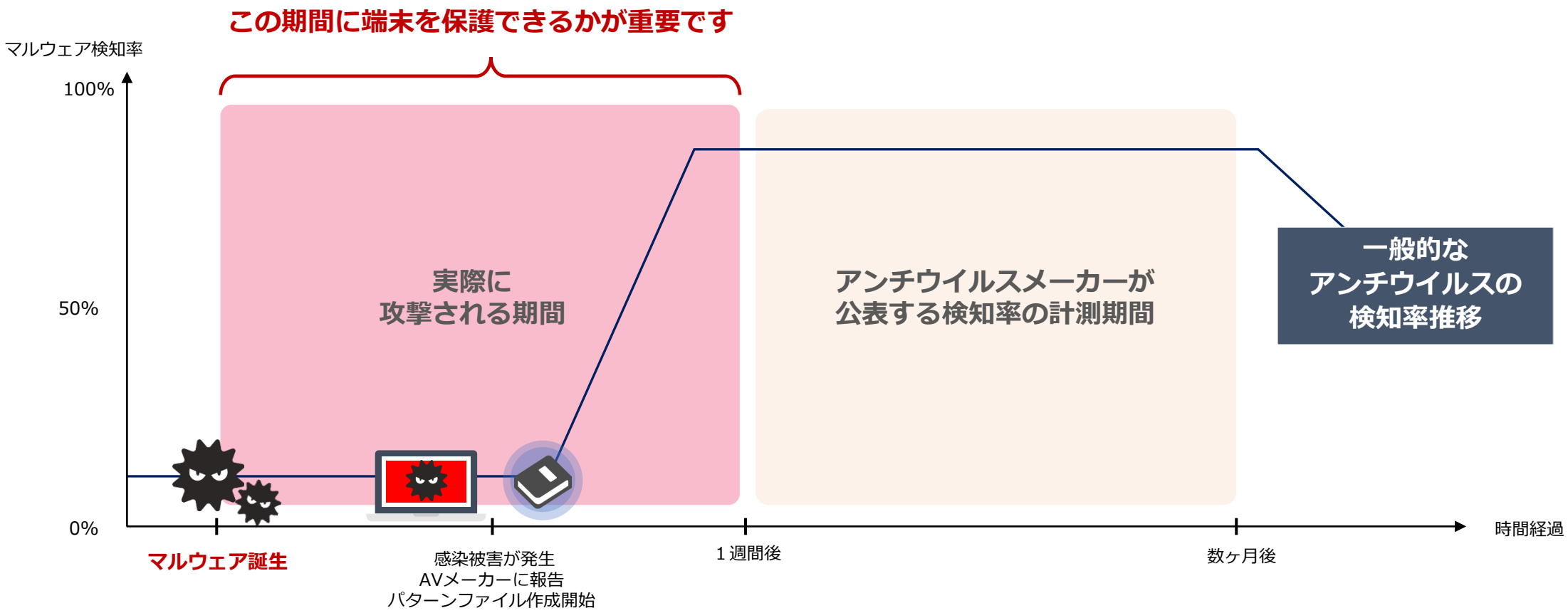


© 2022 MOTEX Inc.

外部脅威

## 従来型アンチウイルスではゼロディ（＝未知のマルウェア）を止めることが難しい

シグニチャ型は被害が発生してからパターンファイルを作成するため、その間に感染してしまう危険性があります

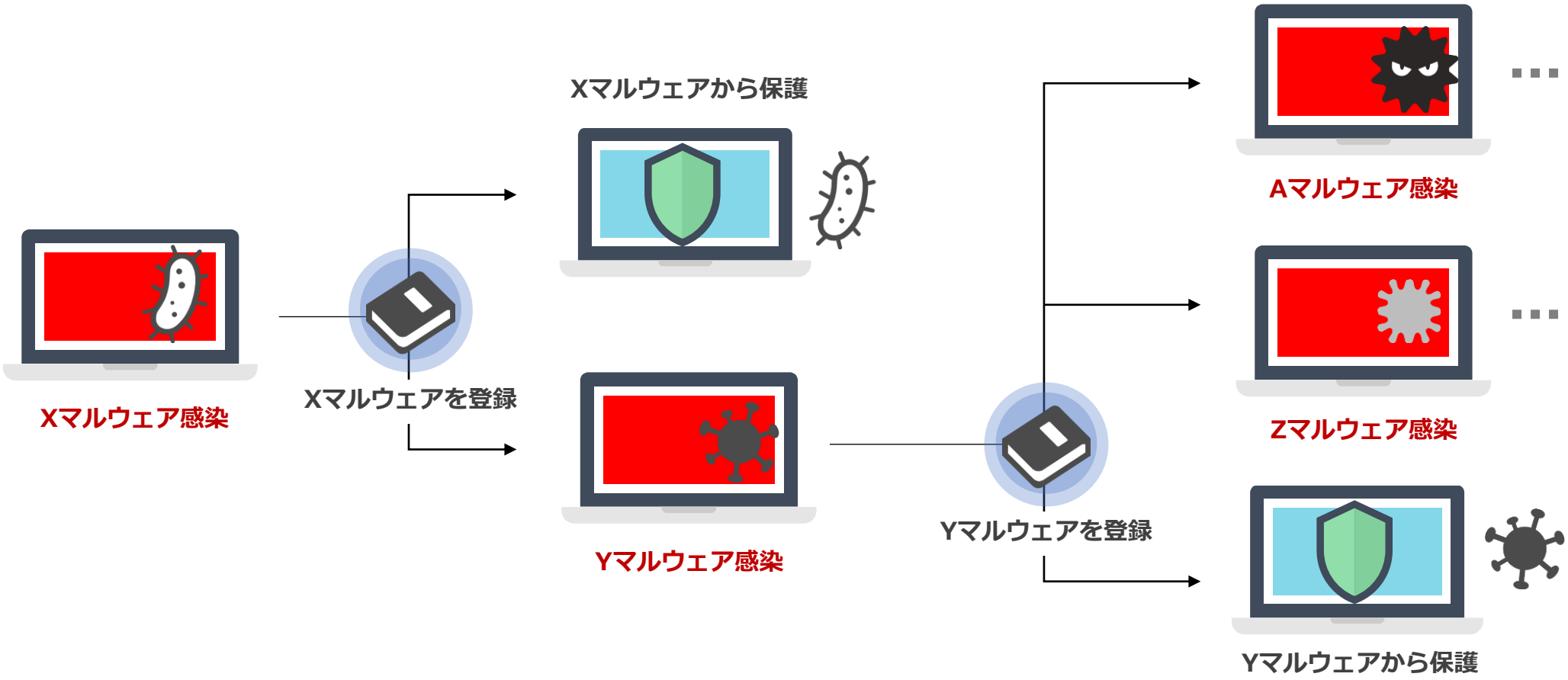



© 2022 MOTEX Inc.

外部脅威

## 攻撃に使われるマルウエアは「1回限り」の使い捨てで、常に新たなマルウエアばかりに…

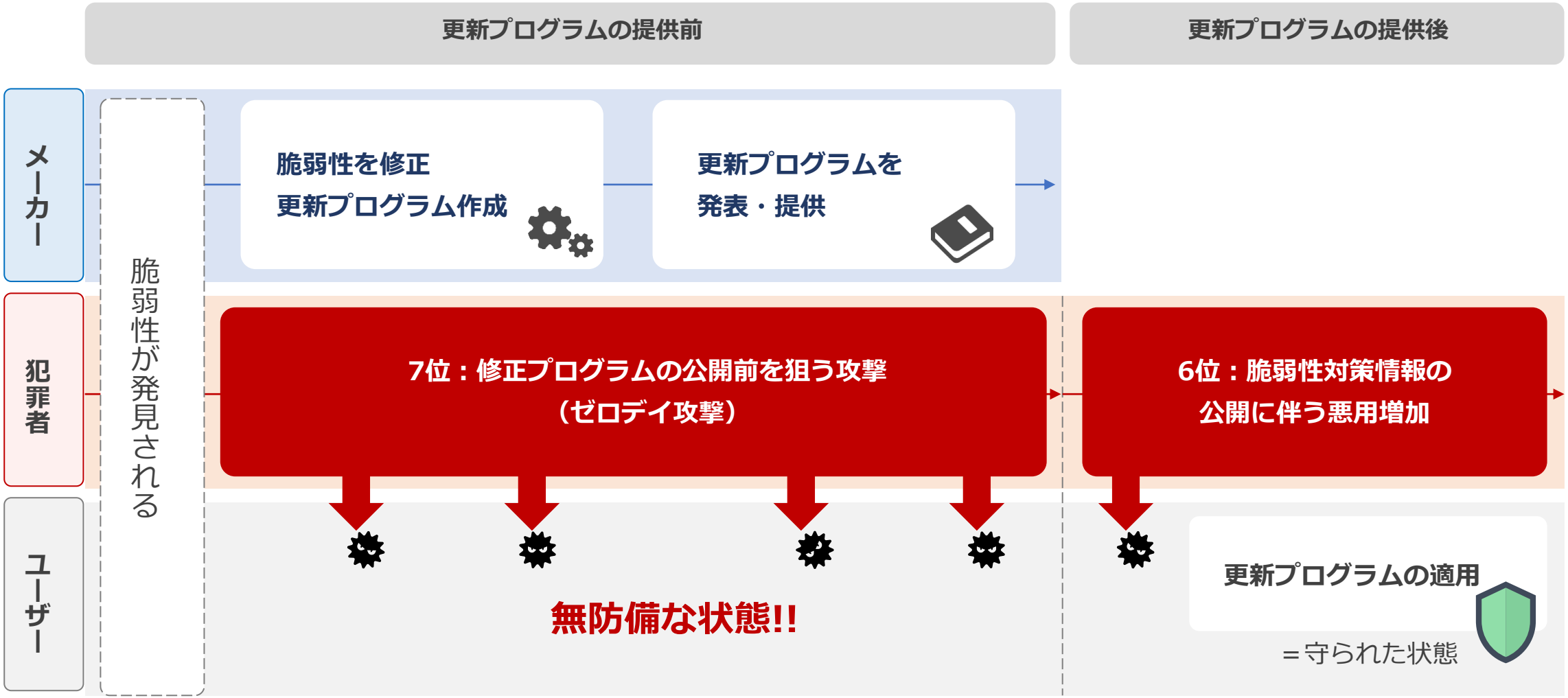
新しいマルウェアが次々と出現するため、シグニチャによる検知には限界が発生してしまいます




© 2022 MOTEX Inc.

## NEW!! 修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）

**脆弱性情報・更新プログラムが公開・提供される前に犯罪者が攻撃を仕掛けることで感染！**
**脆弱性対策を行っていても攻撃を受けてしまう可能性があります**

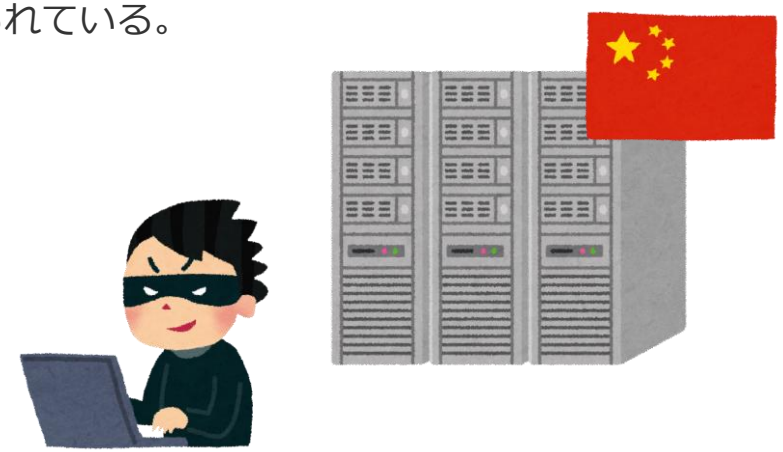



© 2022 MOTEX Inc.

## ゼロデイ攻撃は修正策が存在しない欠陥を突いてくる攻撃！
## 検知が困難で対策済の大手企業のセキュリティ対策でも検知できずに攻撃を受けています

### 大手メーカー

国内の大手メーカーの中国拠点にあるウイルス対策管理サーバーがゼロデイ攻撃を受け、**防衛・ライフライン等国家情報を含む機密情報が漏えいした可能性**。原因は**VPNのハッキング**が濃厚で高い技術を持つハッカー集団に脆弱性を突かれたことが原因と考えられている。



### 官公庁（海外）

Webサーバーソフト**「Apache Log4j2」の脆弱性を利用したサイバー攻撃**を受けた。ランサムウェアによるものかは不明なものの、感染した要素を封じ込めるための隔離措置を講じ、継続監視環境に置いたとのこと。


© 2022 MOTEX Inc.

内部情報漏えい

# 価値がある情報が故に社内や関係者からの悪意のある情報漏えいが急増しています

外部指摘で初めて発覚するケースも・・・自社のみならず委託先やグループ内など範囲が広いケースが増加

## 退職者による情報漏えい

転職先である競合企業へ、**顧客情報や技術情報などの秘密情報を持ち出す**などで損害を受けたと、損害賠償請求に発展


## 情報収集の悪用

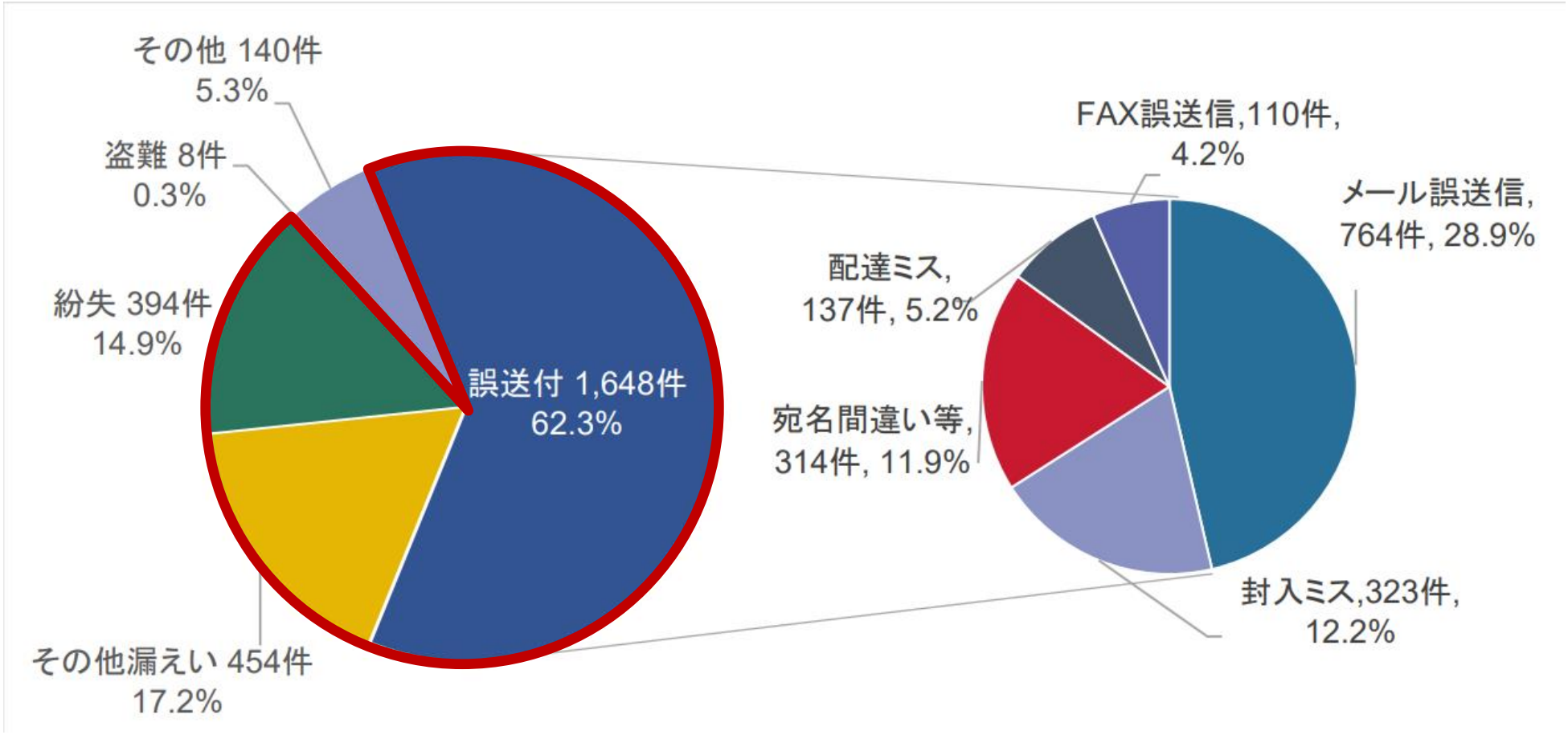
証券会社の委託先SEが、顧客のIDとパスワードを盗み、**顧客に成りすまして資産売却・現金化**、損害額は2億円に上る

## 個人情報の入った機器を転売

業務用のノートPCを無許可で持ち出し業務を行ったのち、約14万件の個人情報が保存されたノートPCを**オークションにて転売し収入**を得ていた

© 2022 MOTEX Inc.

## 内部情報漏えいの約9割は悪意のない「うっかりミス」で誰にでも起こり得ます
## 万が一の対策に加え、インシデント発生時に漏えいリスクの影響範囲を把握できる体制が必要です



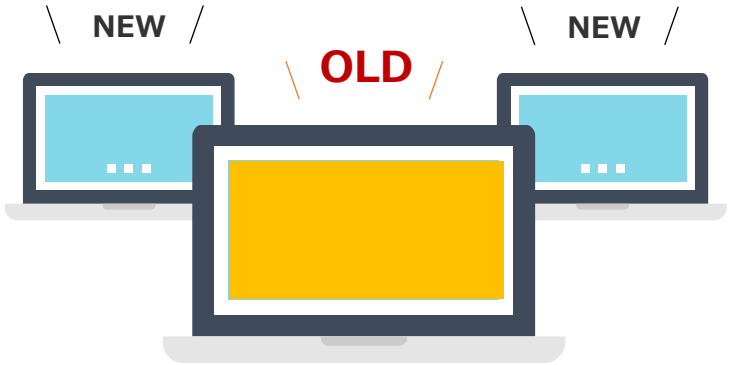

※引用：JIPDE 2020年度「個人情報の取扱いにおける事故報告集計結果」https://privacymark.jp/system/reference/pdf/2020JikoHoukoku_211005.pdf

© 2022 MOTEX Inc.

# 攻撃を受けない環境づくり、攻撃を受けた際の防御・再発防止策を打てる体制づくりをしましょう

リスクは多岐に渡るため、まずは基本の設定をしっかり行うことがセキュリティリスクを減らす事に繋がります

## 脆弱性対策




最新の脆弱性情報をキャッチアップし、OSやアプリを**常に最新の状態**にすることで脆弱性対策しましょう

## 内部情報漏えい対策

**操作履歴を取得**し、**リスクにつながる操作を制御**すると共に社員に対し**セキュリティ啓蒙**を行いましょう

## サイバー攻撃対策

**攻撃を検知・隔離**をすることで感染させない対策・体制を整えましょう

© 2022 MOTEX Inc.

# LANSCOPE クラウド版で実現する情報セキュリティ10大脅威2022対策

脆弱性対策　／　内部情報漏えい　／　サイバー攻撃対策

© 2021 MOTEX Inc.

# PC・スマホを一元管理！IT資産管理・MDM「LANSCOPE クラウド版」

PC・スマホを一元管理！IT資産管理・MDM

LANSCOPE cloud

- iOS・Android・Windows・macOSを一元管理
- Apple・Googleの認定プログラム対応で充実のモバイル管理
- 操作ログ・ファイル配信・記録メディア制御でPC管理

資産管理 | 位置情報取得 | レポート

セキュリティ | 操作ログ | AE/ABM対応

https://www.lanscope.jp/an/


© 2022 MOTEX Inc.

# 脆弱性対策

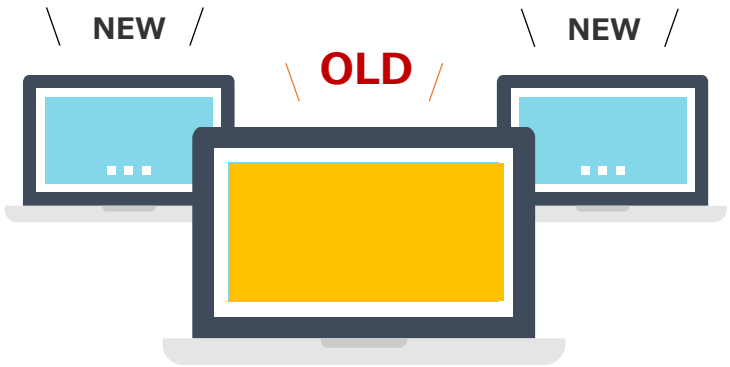
LANSCOPE クラウド版で実現する情報セキュリティ10大脅威

© 2021 MOTEX Inc.

# 情報セキュリティ10大脅威の第6位・初登場第7位の「脆弱性情報公開前後を狙った攻撃」に備えましょう

セキュリティ対策に重要な「脆弱性対策」を悪用した脅威がランクイン！可能な限り対策を施しましょう

## 脆弱性対策




最新の脆弱性情報をキャッチアップし、OSやアプリを**常に最新の状態**にすることで脆弱性対策しましょう

## 内部情報漏えい対策

**操作履歴を取得**し、**リスクにつながる操作を制御**すると共に社員に対し**セキュリティ啓蒙**を行いましょう

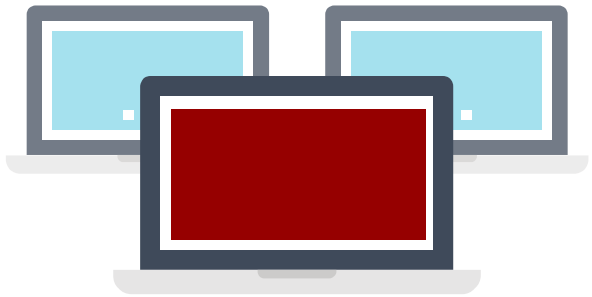
## サイバー攻撃対策

**攻撃を検知・隔離**をすることで感染させない対策・体制を整えましょう

© 2022 MOTEX Inc.

## 資産情報を自動で収集し、社内の管理すべきデバイスがどれだけあるかを自動で把握
## 脆弱性の有無を自動でレポーティングし、必要に応じてアップデートまで実施することが可能です

### IT資産管理



社内にあるデバイスを把握し、各デバイスの**資産情報を自動で収集**することができます。

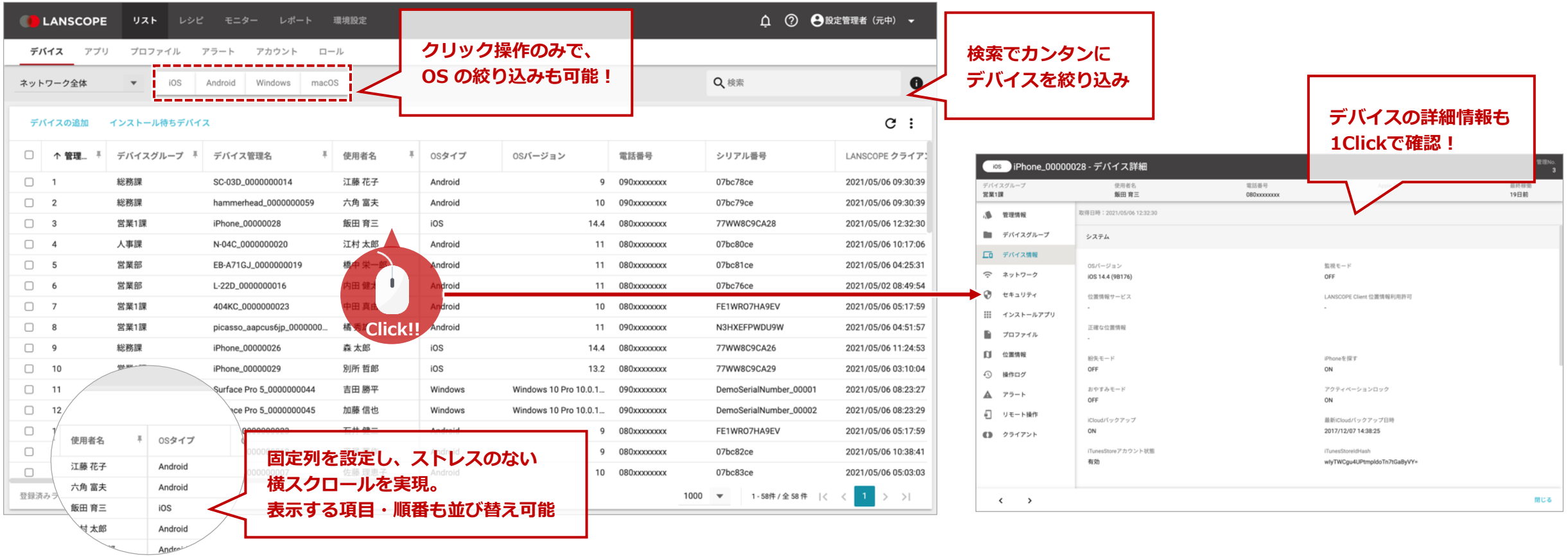
### 脆弱性レポート

OSやアプリのバージョンを**自動収集**。対策が必要なデバイスを、**アップデートすることも可能**です。

© 2022 MOTEX Inc.

脆弱性対策

# PC・スマホ・タブレットの混在環境でも最新のデバイス情報を一覧で台帳表示できます



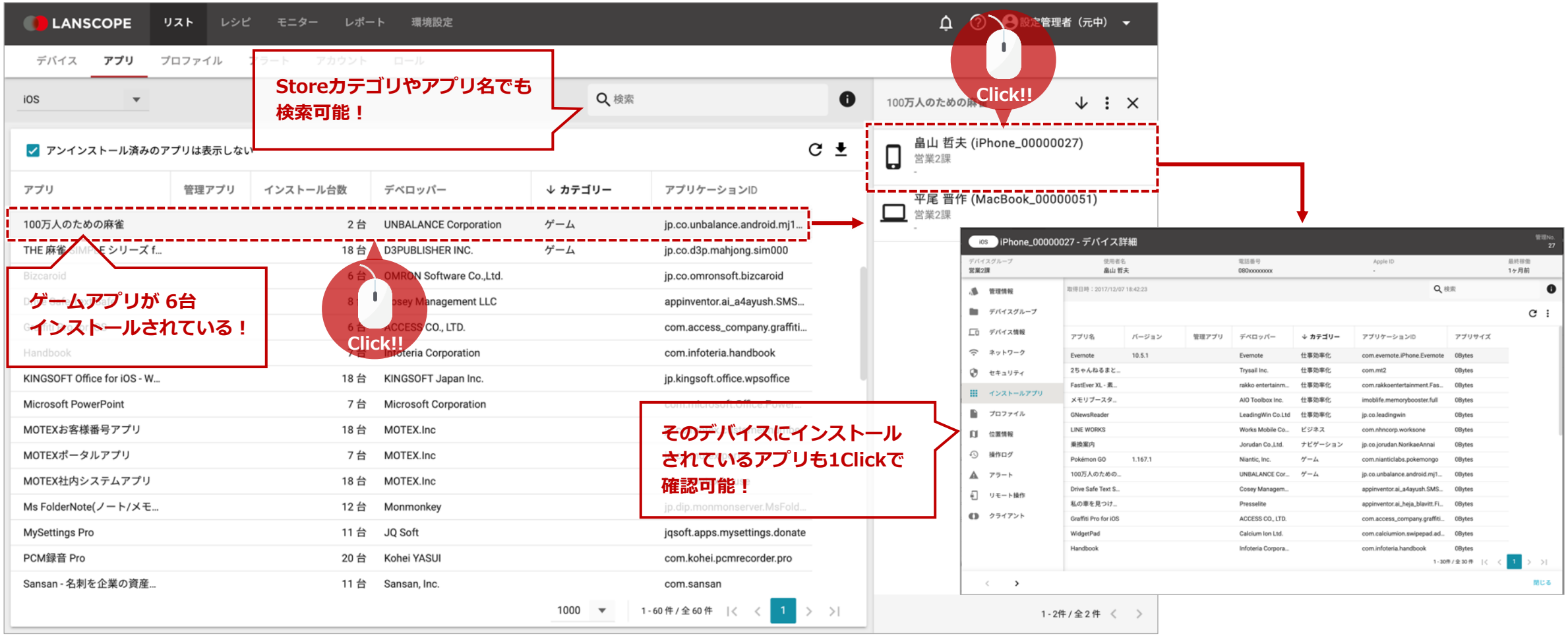

## 台数が多くなればなるほど、必要性が高まる資産管理

デバイスのハードウェア情報を1台ごとに確認していくのは資産の棚卸や人事異動の際のメンテナンス時に不便です。LANSCOPE なら、通信キャリアが混在している環境や、OSが混在している場合でも、確認したいデバイス情報の項目を一覧で表示、台帳の自動作成が可能です。

© 2022 MOTEX Inc.

脆弱性対策

# “このアプリ” は “どのデバイス” にインストールされているか？1Click で把握できます

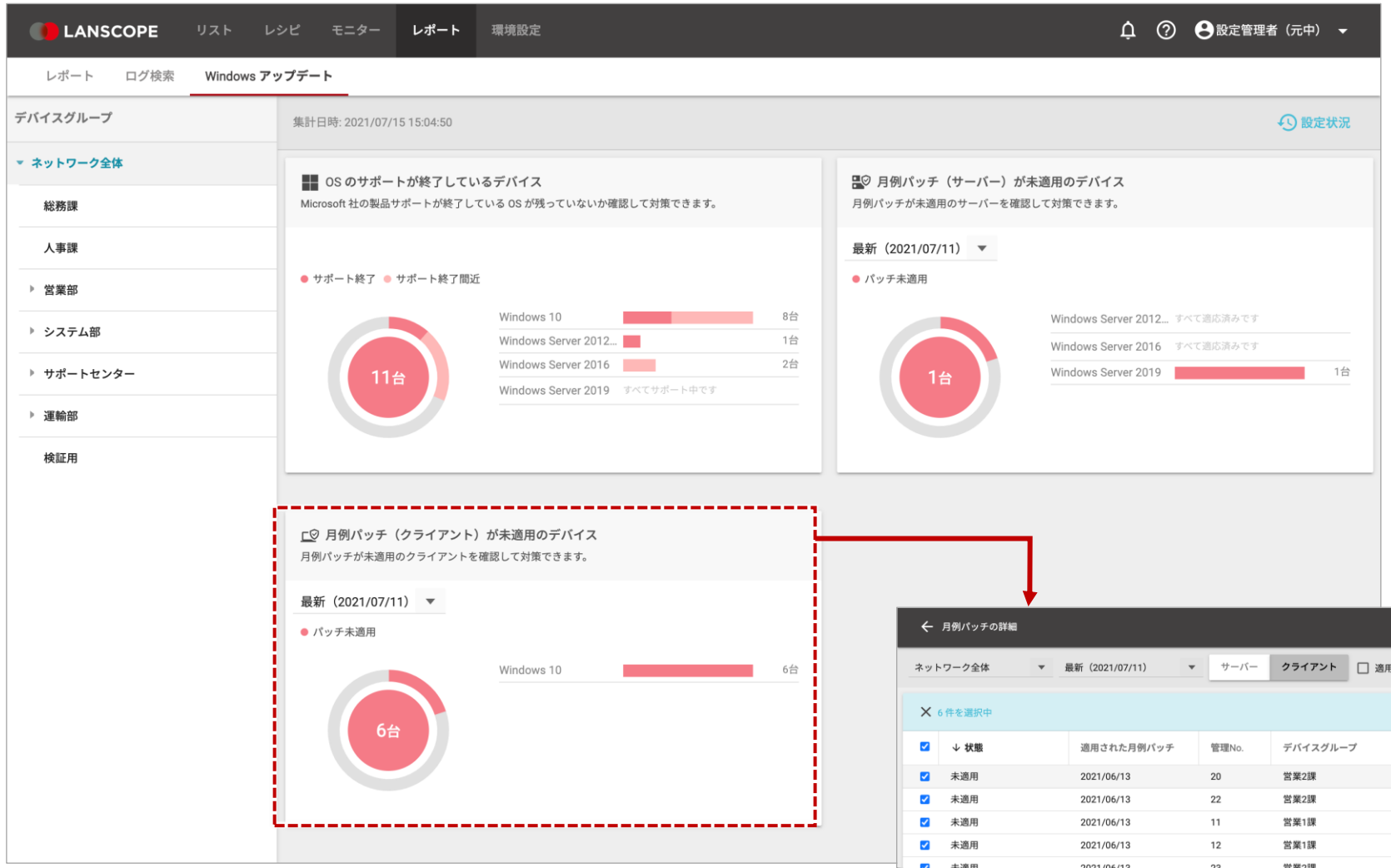



脆弱性の対象が明確な場合、クリックするだけで、社内のどの端末にインストールされているかが把握できます

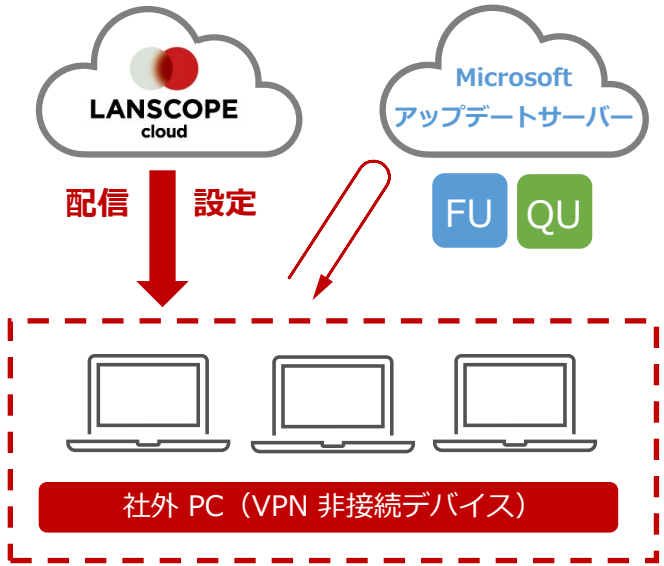
© 2022 MOTEX Inc.

脆弱性対策

# 機能更新・品質更新プログラムの適用状況を、“視認性の良い” レポート形式で把握
# 1Click で未適用デバイスを確認し、最新のプログラムを適用




**社内ネットワークに接続されない**
**デバイスもLANSCOPE で配信可能**




**OSバージョンなどをフィルタで絞り込みを行う事も可能**

© 2022 MOTEX Inc.

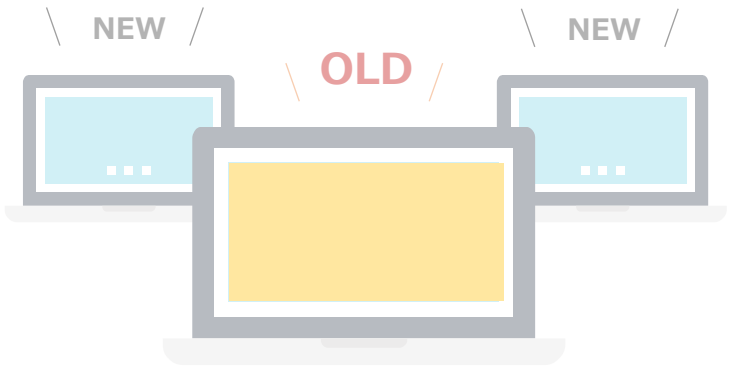
## 内部情報漏えい

LANSCOPE クラウド版で実現する情報セキュリティ10大脅威

© 2021 MOTEX Inc.

## 悪意のある情報漏えいを防ぐために、リスクのある操作を制御することができます
## さらに万が一の対策として暗号化や証跡を残すことができうっかりミスにおける影響範囲も把握できます

### 脆弱性対策




最新の脆弱性情報をキャッチアップし、OSやアプリを**常に最新の状態**にすることで脆弱性対策しましょう

### 内部情報漏えい対策

**操作履歴を取得**し、**リスクにつながる操作を制御**すると共に社員に対し**セキュリティ啓蒙**を行いましょう

### サイバー攻撃対策

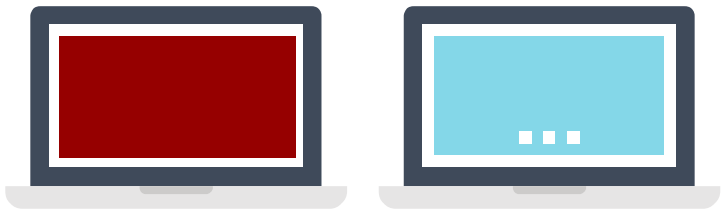
**攻撃を検知・隔離**をすることで感染させない対策・体制を整えましょう

© 2022 MOTEX Inc.

# 操作履歴の取得で証跡＆抑止効果！リスクのある操作を制御することでセキュアな環境づくりを実施

ログは取得するだけでは効果を発揮できません。リスクにつながる操作を察知しインシデントを未然に防ぐことが重要です

## 操作ログ取得・操作制御

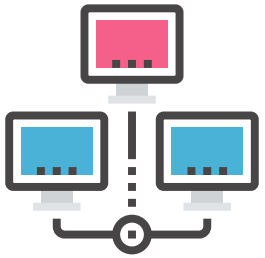


操作履歴を取得し、リスクとなる操作を監視・制御が可能です

## 暗号化の適用状況を把握

盗難紛失による情報漏えいに備えて、Windowsの暗号化機能「BitLocker」の適用状況を把握すると共に、複合キーを一括管理できます

## リモートロックワイプ

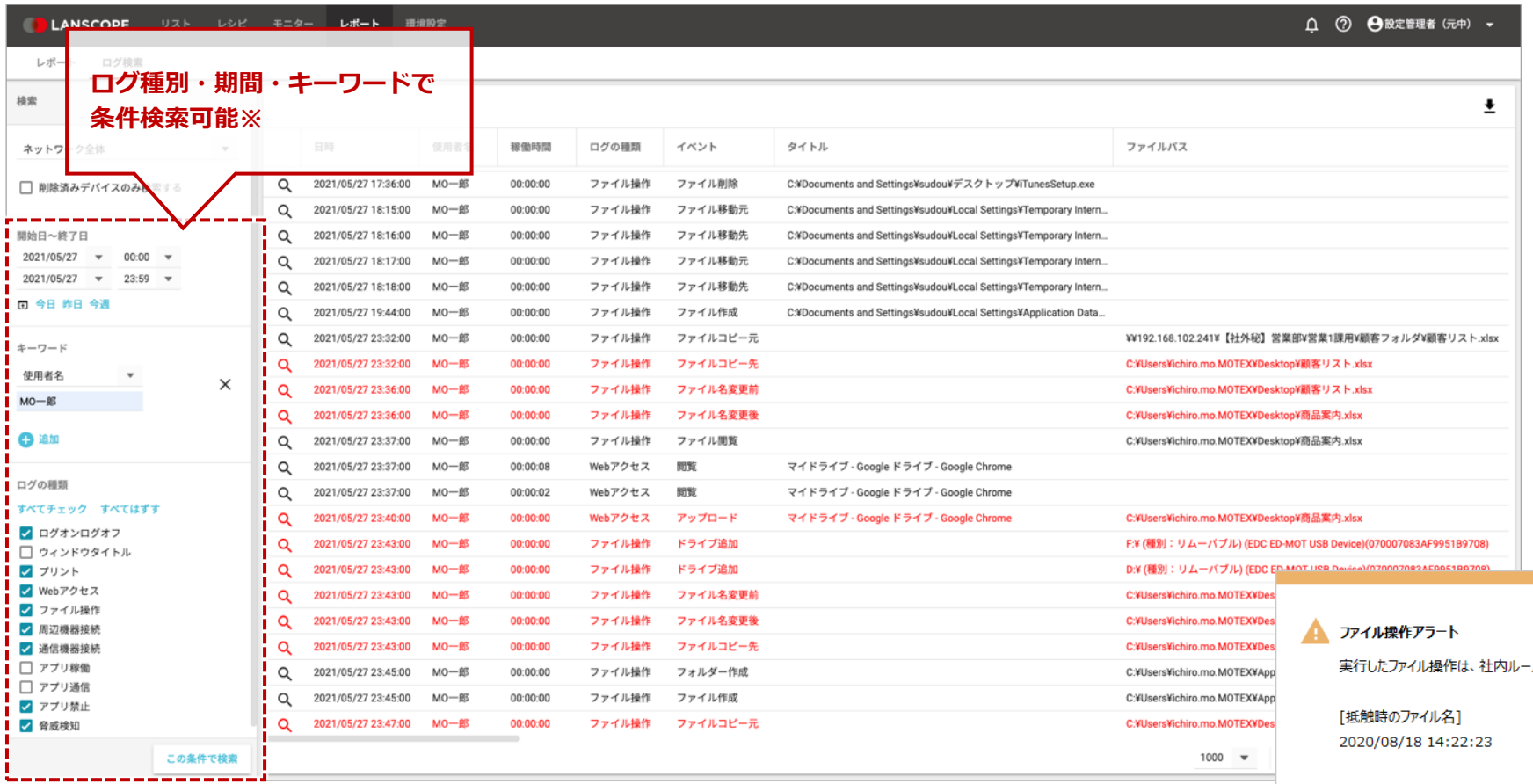


盗難紛失による情報漏えいに備えて、位置情報の取得が可能です。さらにリモートロックワイプで情報を守ります

© 2022 MOTEX Inc.

内部情報漏えい対策

# 「どの部署の」「誰が」「いつ」「何をしたのか」をリアルタイムに取得することができます




| 取得できる操作ログ（Windows） |
|---|
| ログオン・ログオフログ |
| ウィンドウタイトルログ・アプリ利用ログ |
| ファイル操作ログ（コピー／移動／作成／上書き／削除／名前の変更） |
| 記録メディアの追加／削除、書込みログ |
| Web サイト閲覧ログ |
| Web サイト アップロード／ダウンロード／書込みログ |
| プリントログ |
| 通信機器接続ログ（Wi-Fi／Bluetooth） |

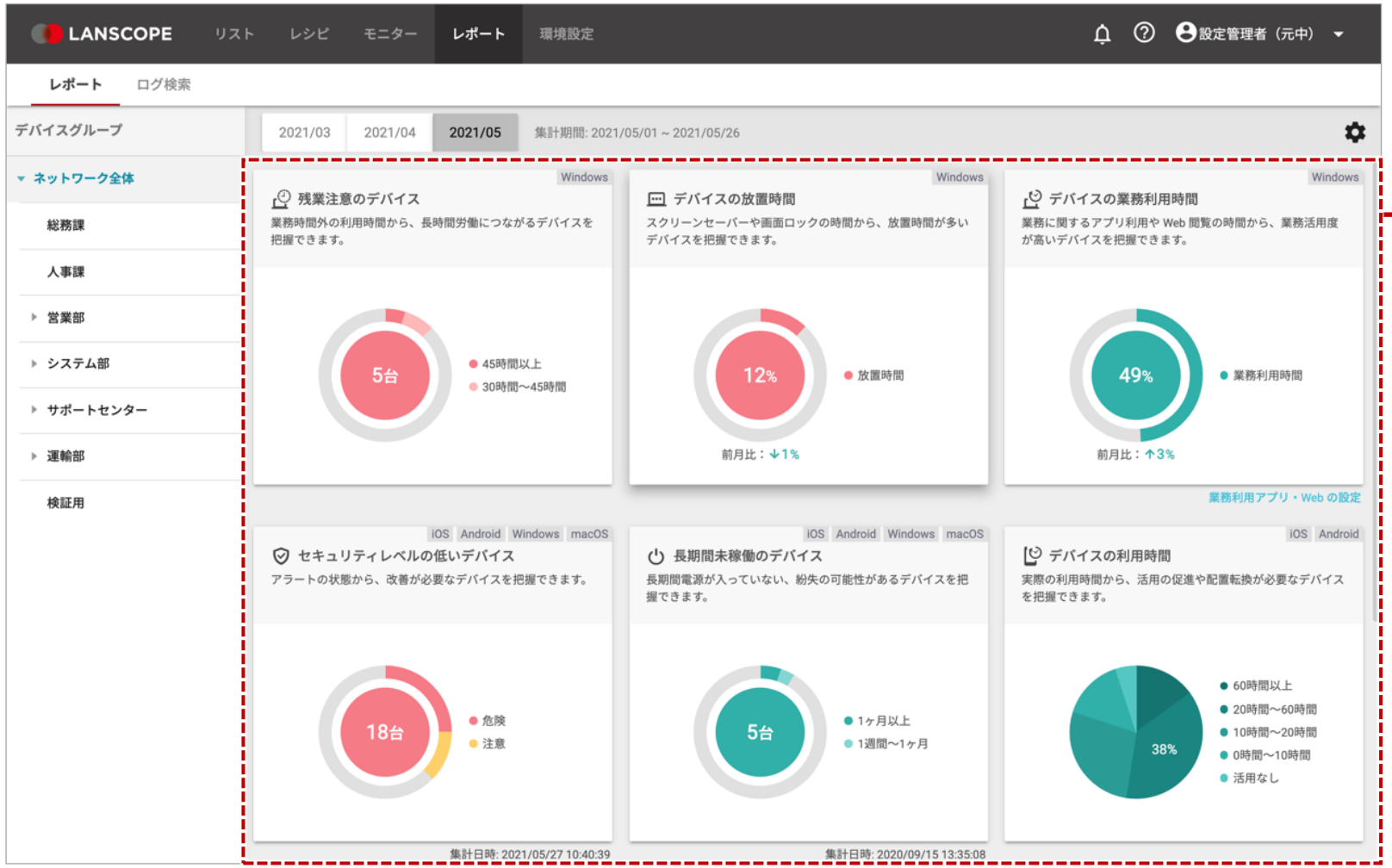

**違反操作があった場合は、リアルタイムに警告通知が可能**

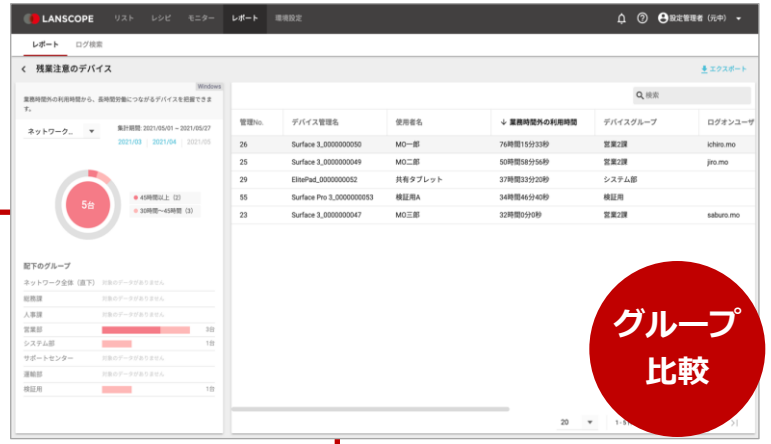
※ 管理コンソール上で検索できるログは当日を含む過去100日分です。
※ 期間・対象デバイスを指定し CSV 形式で一括出力が可能です。指定できる期間は過去2年分です。
別途オプション（ログ運用オプション）を購入することで、過去5年分を指定して出力可能です。

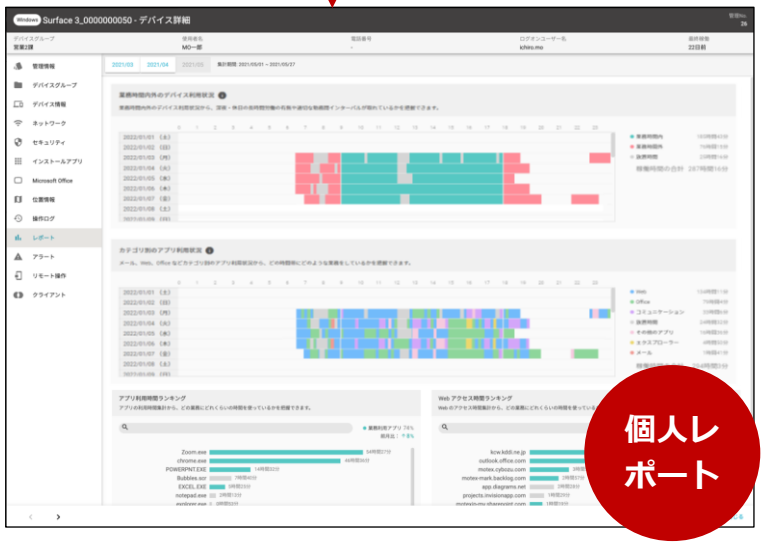
© 2022 MOTEX Inc.

内部情報漏えい対策

## 取得した操作ログを元に様々な視点でレポート化！
## ドリルダウンで、配下の「グループ比較」や「課題のあるデバイス」を特定、活用状況を把握することができます



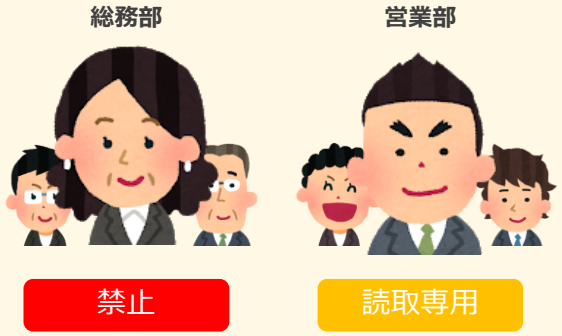

© 2022 MOTEX Inc.

内部情報漏えい対策

# USB メモリなどの記録メディアの利用を制御し、情報漏えいを防止することができます

## 1．全体設定

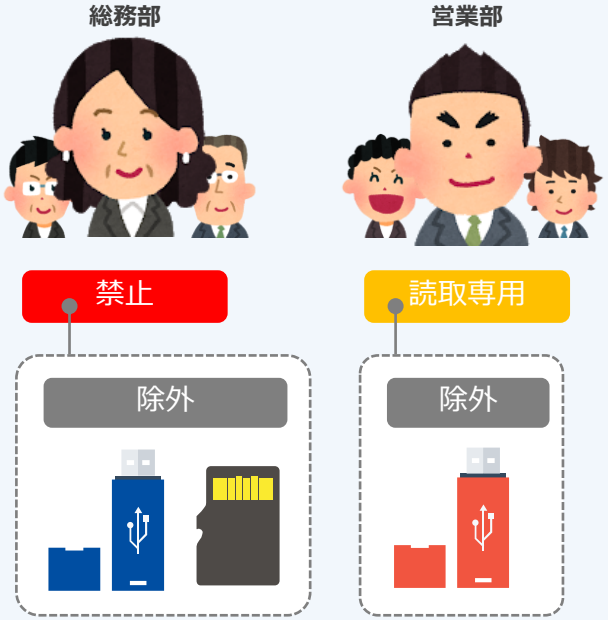
**グループ毎**に「許可」「禁止」「読取専用」から制御レベルを選択します




＋

## 2-A．特定の記録メディアごとに許可

**禁止・読取専用設定のグループ**に対し特定の記録メディアの除外設定が可能です

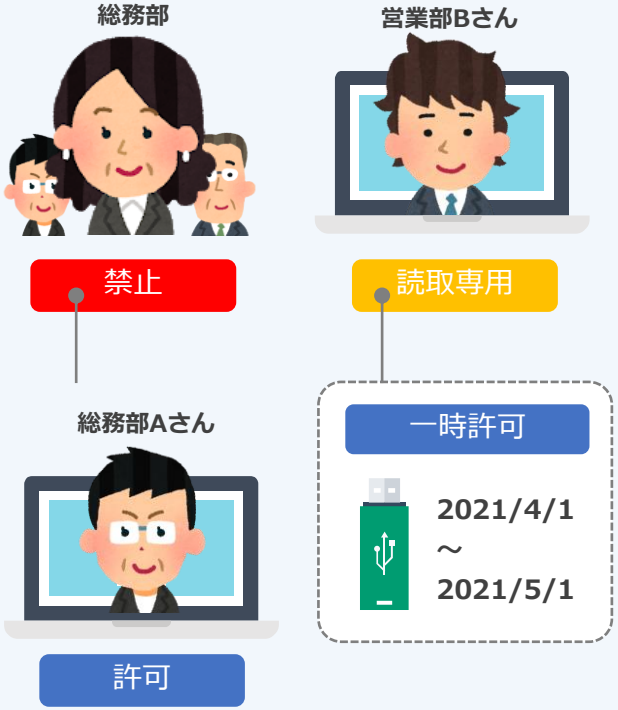



**除外設定パターン**
[シリアルNo][ベンダーID/プロダクトID][キーワード]

OR

## 2-B．特定のデバイスごとに制御

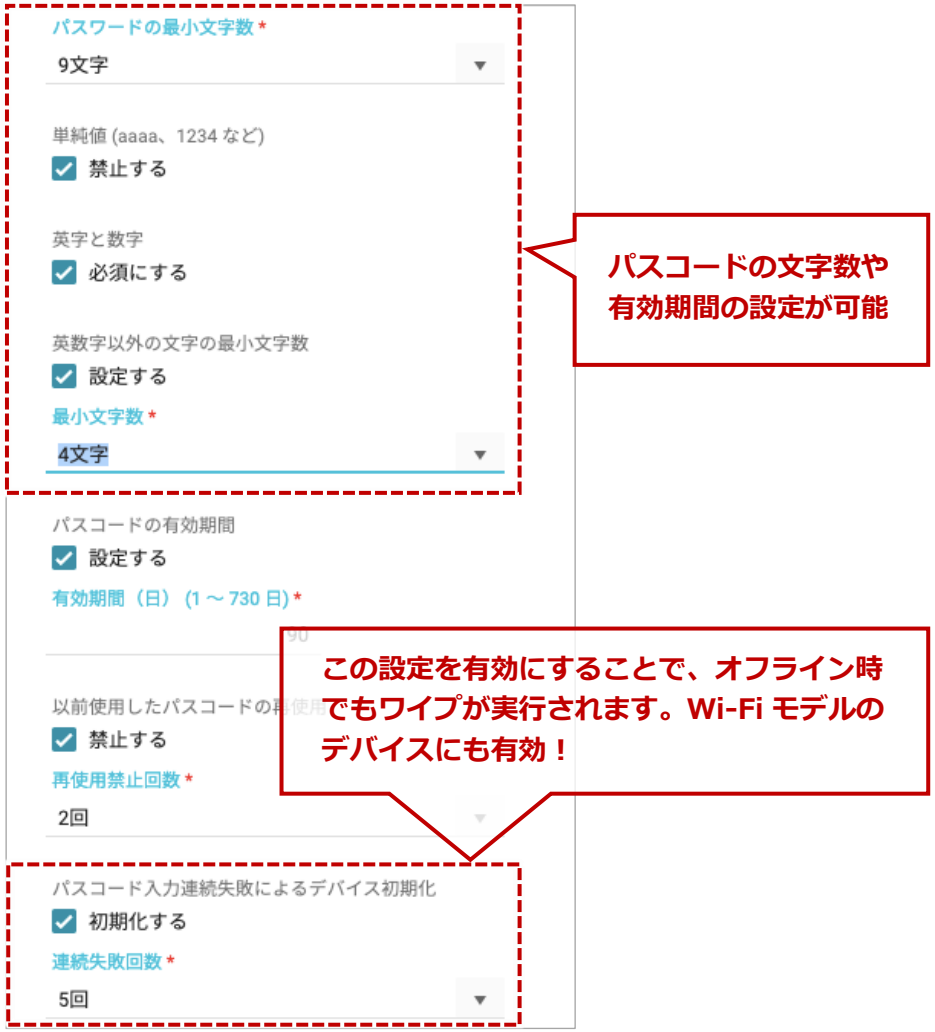
**グループとは異なる設定をデバイス（PC）単位**に設定可能です。また一時的に許可・読取専用の設定も可能です。




© 2022 MOTEX Inc.

内部情報漏えい対策

# 利用者に依存しがちなパスコードの設定ルールを会社で統一することができます




| iOSの設定項目 |
|---|
| パスコードの最少文字数 |
| 単純値（aaaa、1234など）を禁止 |
| 英字と数字が必要 |
| 英数字以外の文字の最少文字数 |
| パスコードの有効期間 |
| 以前使用したパスコードの再使用を禁止 |
| パスコード入力連続失敗によるデバイス初期化 |
| パスコードの設定ルールを一括で設定・配布 |
| デバイスロック開始までの最大許容時間 |
| 画面ロック解除時のパスコード要求までの最大許容時間 |

| Androidの設定項目※ |
|---|
| パスワードの最少文字数 |
| 使用しなければならない文字の種類 |
| パスワードの有効期間 |
| パスワードの有効期限を事前の通知 |
| 以前使用したパスワードの再使用を禁止 |
| 以前使用したパスワードの再使用を禁止 |
| パスワード入力連続失敗によるデバイス初期化 |
| スリープ開始までの最大許容時間 |

👉 **パスワードポリシー設定の重要性**

パスワードを設定していない場合、画面ロックの解除は容易です。情報漏えいを防ぐためにも、利用者にパスワードの設定条件を委ねるのではなく、会社のポリシーをデバイスに設定することは、紛失対策の基本と言えます。

⚠ Android10以降のデバイスの場合、Android Enterprise の利用が必要です。

© 2022 MOTEX Inc.

内部情報漏えい対策

# Windows デバイスの紛失対策を支援！BitLockerの設定の有無・回復キーの一括管理が可能です

BitLockerはOS バージョンアップへの対応など親和性の高さ、追加コストが発生しない等で多くの企業が利用しています

## BitLocker 設定有無の確認


BitLocker を利用したリモートワイプが実行できるよう設定が有効になっているか確認できます。

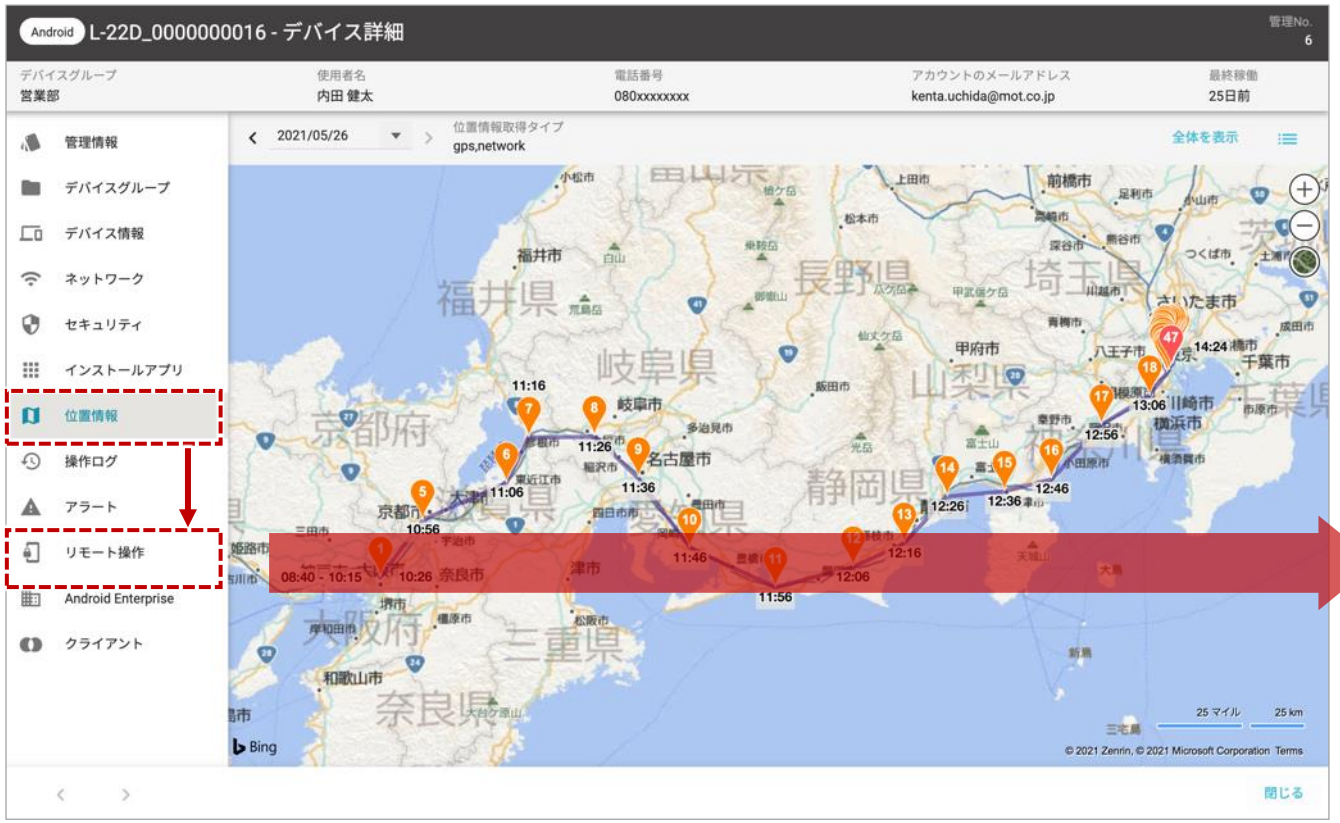
## BitLocker 回復キーの管理


回復キーを自動収集できるので、デバイス毎にファイルや印刷で保存する必要がなくなります。

© 2022 MOTEX Inc.

内部情報漏えい対策

# 位置情報から所在確認！遠隔でリモートロックやワイプを実行し情報漏えいを防止できます





※ OSによってリモートロック・ワイプの仕様は異なります。Windows Server OS はリモートロック・ワイプ機能に対応していません。
※ Windows はスリープ状態の場合、位置情報が取得できません。
※ Windows7・Windows Server OS・macOS デバイスは位置情報取得機能には対応していません。

© 2022 MOTEX Inc.

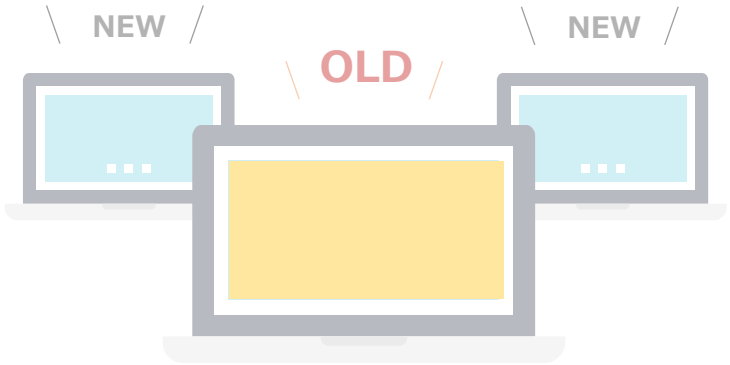
# サイバー攻撃対策

LANSCOPE クラウド版で実現する情報セキュリティ10大脅威

© 2021 MOTEX Inc.

## 情報セキュリティ10大脅威の7割を占めるサイバー攻撃リスクに対応
## 巧妙化するランサムウェアやゼロデイ攻撃に対応できる対策が求められます

### 脆弱性対策




最新の脆弱性情報をキャッチアップし、OSやアプリを**常に最新の状態**にすることで脆弱性対策しましょう

### 内部情報漏えい対策

**操作履歴を取得**し、**リスクにつながる操作を制御**すると共に社員に対し**セキュリティ啓蒙**を行いましょう

### サイバー攻撃対策

**攻撃を検知・隔離**をすることで感染させない対策・体制を整えましょう

© 2022 MOTEX Inc.

# 亜種・未知のマルウェアも99%予測検知！攻撃原因をカンタンに解析できます

AIを活用した最新技術により従来型では検知が難しかった未知・亜種のマルウェアも高確率で検知できます

## 未知・亜種のマルウェア検知

AIを活用した新技術により、未知・亜種のマルウェア・ランサムウェアを９９%という高確率で検知が可能です

## 攻撃原因を解析・対策

攻撃を受けてしまった原因をクリックだけでカンタンに解析・再発防止策を打てます

© 2022 MOTEX Inc.

# AI を活用した次世代型アンチウイルス製品と連携、操作ログから、未知・亜種のマルウェア感染原因を特定

CPMS Cyber Protection Managed Service × LANSCOPE cloud

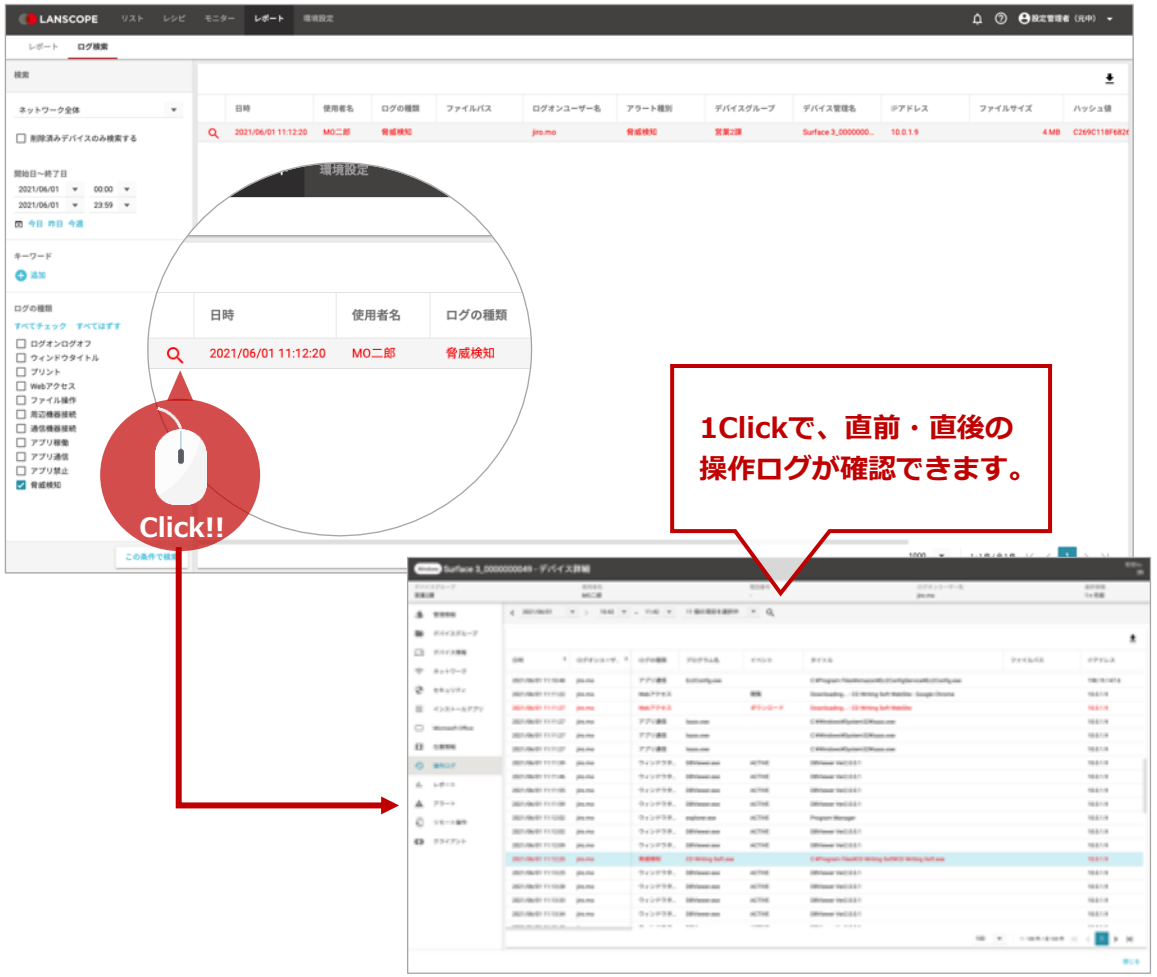
マシーンラーニングの特許技術を活用した「予測脅威防御」で、マルウェアの特徴点を見つけて実行前に検知・隔離します。LANSCOPE クラウド版と連携することで、マルウェアに感染してしまった直前の操作を特定。原因の追求や再発防止に活用できます。

検知率は99% *
未知のマルウェアも
検知・隔離

PC への負荷が小さく
快適なパフォーマンス
を発揮

月額450円/台から！
ニーズに合わせて
必要なプランを選択

https://www.lanscope.jp/cpms/




* 2018 NSS Labs Advanced Endpoint Protection Test 結果より

© 2022 MOTEX Inc.

サイバー攻撃対策

# 未知・亜種のマルウェアもマシンラーニングで99%検知！次世代のアンチウイルス


## 次世代型AIアンチウイルス

CPMS Powered by BlackBerry

AIを活用したマシンラーニングによる予測検知が可能で、未知・亜種のマルウェアも99%の高検知が実現。LANSCOPE連携で簡易EDR、オプションのOpticsによるDERが可能

- AIによる高精度な予測検知
- シグニチャレスで日々のアップデート不要
- 過検知が少なく低負荷

https://www.lanscope.jp/cpms/blackberryprotect/

© 2022 MOTEX Inc.

# 数理モデルに基づくアプローチ！人工知能が未知のマルウェアを動作前に防御

検知の高さはもちろん、シグニチャレスなのでアップデートの手間・クライアント負荷がありません

**AI（人工知能）**
**による自動判断**

**DNAレベルの**
**マルウェア解析**

**毎日のアップデートや**
**インターネット接続不要**

© 2022 MOTEX Inc.

# 未来に発生するマルウェアを予測して検知！あらゆる未知・亜種のマルウェアから保護

BlackBerry Protectの検知方式は、2年以上前の過去の検知エンジンでも、未知のマルウェアを予測検知しています

**MyWebSearch**
26か月前に予測

**Emotet**
27か月前に予測

**PolyRansom**
28か月前に予測

**GandCrab**
26か月前に予測

**installCore**
27か月前に予測

**Petya-Like**
20か月前に予測

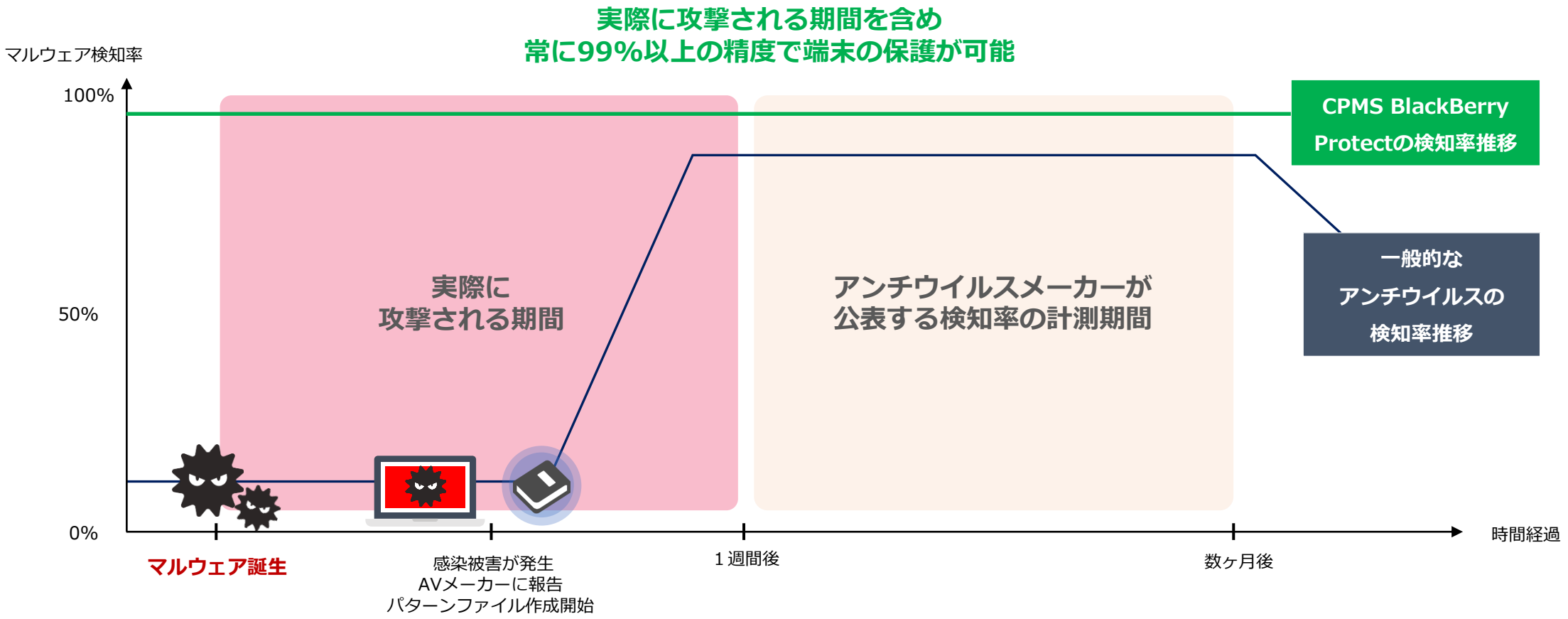
**GoldenEye**
13か月前に予測

**WannaCry**
19か月前に予測

© 2022 MOTEX Inc.

# AIを活用した「予測脅威防御」で未知マルウェアも99%以上の超高精度で防御

AI技術を活用したシグニチャレスの独自のマルウェア検知手法のため、パターンファイルの有無に左右されない検知精度




© 2022 MOTEX Inc.

サイバー攻撃対策

## 検知したマルウェア以外の「端末に潜む脅威」を発見、攻撃の流れを操作を紐づけて可視化

CPMS BlackBerry Protectの検知力に加え、調査・封じ込め・復旧まで一連の対応が可能で、負荷の少ないEDR機能です


BlackBerry Protect

BlackBerry Optics

マルウェア以外の「危険なプロセス」や「コマンドの実行」も検知・隔離可能

※BlackBerry Opticsの導入が必要です。詳細はお問合せください

© 2022 MOTEX Inc.

https://go.motex.co.jp/l/320351/2017-06-21/c55z

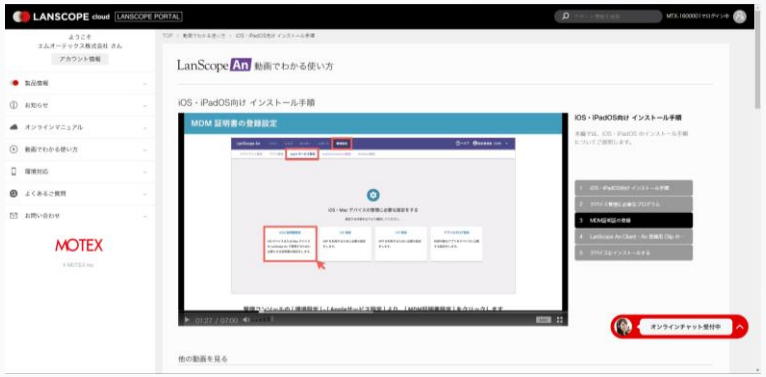
LANSCOPE cloud

# 60日間無料体験キャンペーン中

LANSCOPE クラウド版の体験版は 60日間たっぷり利用できます。十分に機能を検証していただき、ご検討ください。設定したポリシーや取得した情報を含め、そのまま製品版へのデータ引き継ぎが可能です。また体験版利用中も、弊社サポートセンターにお電話やメールで問い合わせが可能。体験期間中は、マニュアルやオンラインで学べるトレーニング動画も公開しています

●各種マニュアル・問い合わせが可能


●動画で設定方法を説明



https://www.lanscope.jp/an/