【公表予定】

資　料　6

IPA Better Life with IT

第８回営業秘密官民フォーラム

サイバーセキュリティ対策・内部不正防止対策

2022年6月20日

独立行政法人情報処理推進機構
統括参事／セキュリティセンター長
瓜生 和久

ご説明内容

- 情報セキュリティの10大脅威2022
- 「組織における内部不正防止ガイドライン」の改訂

情報セキュリティの10大脅威2022

個人・組織とも、上位は情報の窃取・悪用・脅迫に関わる脅威です。
これらの脅威を念頭に、引き続きサイバーセキュリティ対策が必要です。

昨年	個人	順位	組織	昨年
2	フィッシングによる個人情報等の詐取	1	ランサムウェアによる被害	1
3	ネット上の誹謗・中傷・デマ	2	標的型攻撃による機密情報の窃取	2
4	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	3	サプライチェーンの弱点を悪用した攻撃	4
5	クレジットカード情報の不正利用	4	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
1	スマホ決済の不正利用	5	内部不正による情報漏えい	6
8	偽警告によるインターネット詐欺	6	脆弱性対策情報の公開に伴う悪用増加	10
9	不正アプリによるスマートフォン利用者への被害	7	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	新
7	インターネット上のサービスからの個人情報の窃取	8	ビジネスメール詐欺による金銭被害	5
6	インターネットバンキングの不正利用	9	予期せぬIT基盤の障害に伴う業務停止	7
10	インターネット上のサービスへの不正ログイン	10	不注意による情報漏えい等の被害	9

情報セキュリティ10大脅威 2022 「個人」・「組織」向け脅威の順位

ランサムウェア被害事例

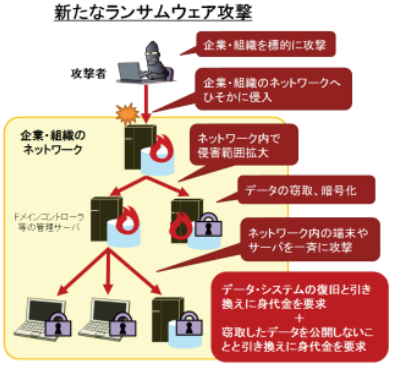
■2021年の事例 ①：病院へのランサムウェア攻撃
- 2021年10月、病院のシステムがランサムウェアに感染し電子カルテや会計システムにアクセスできなくなる等の被害
- 暗号化解除と引き換えに身代金を要求されたが応じず
- システム復旧まで新規患者の受け入れを中止する等の影響
- 2022年1月、通常診療を再開

■2021年の事例 ②：バックアップの暗号化による被害の長期化
- 製粉会社へのサイバー攻撃により、ランサムウェアに感染
- システムのオンラインバックアップを管理していたサーバーも暗号化
- 早期復旧が困難となり四半期決算報告書の提出にも影響

■事例と対策レポート（IPA）：
事業継続を脅かす 新たなランサムウェア攻撃 について
～「人手によるランサムウェア攻撃」と「二重の脅迫」～

データ･システムの復旧と引き換えに身代金を要求
＋
窃取したデータを公表しないことと引き換えに身代金を要求

https://www.ipa.go.jp/files/000084974.pdf



内部不正対策：「組織における内部不正防止ガイドライン」

「組織における内部不正防止ガイドライン」を第5版に改訂しました（2022年4月）

https://www.ipa.go.jp/security/fy24/reports/insider/

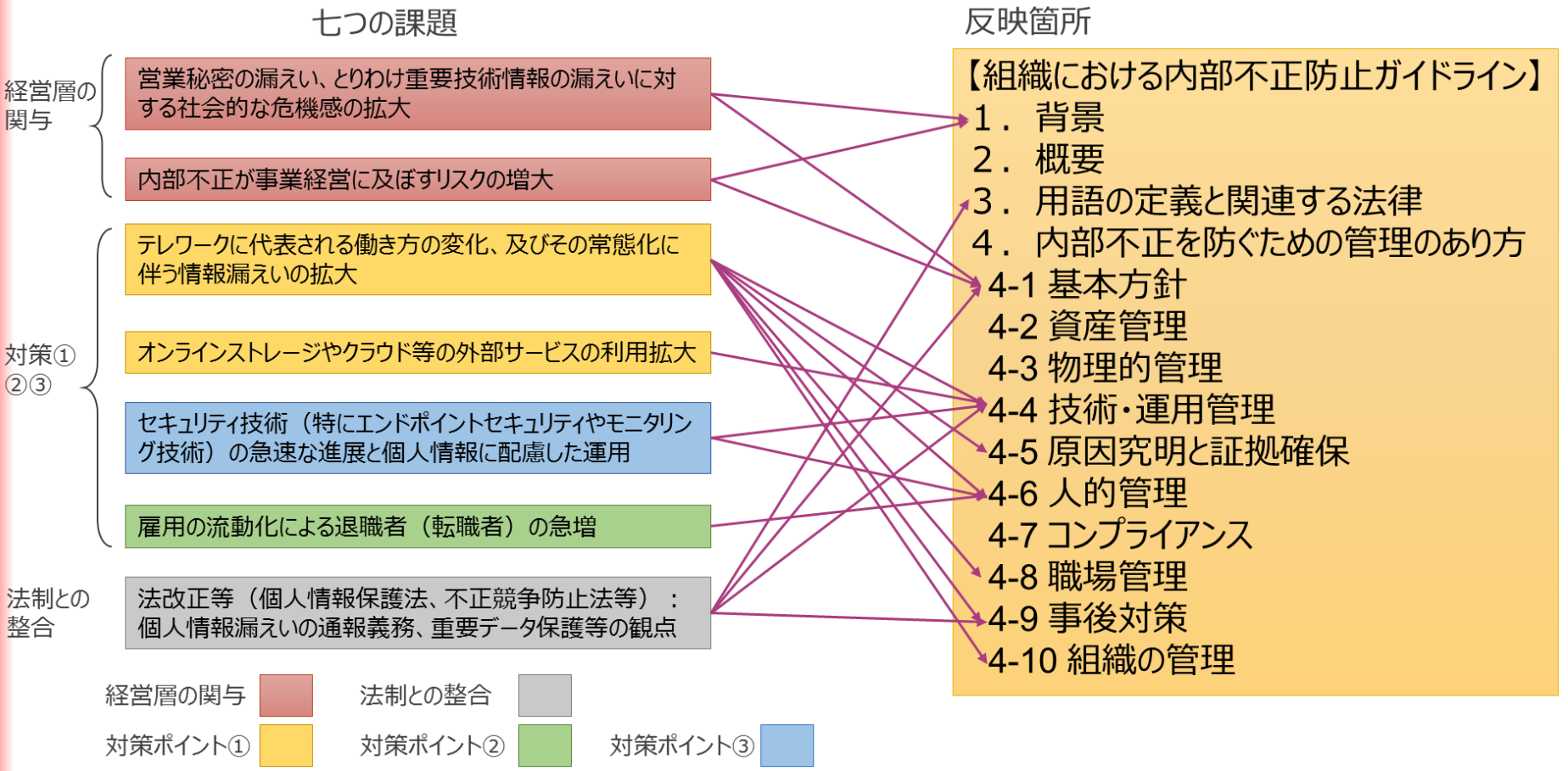
組織における内部不正防止ガイドライン なぜ改訂したのか？

■前回改訂からの社会の変化
（１）経営層の関与強化（社会的な危機感の拡大）
（２）関連法制度の改正（不正競争防止法、個人情報保護法改正・・）
（３）ニューノーマル（テレワーク、クラウド、データ分散・・）の普及
（４）雇用の流動化（退職者による内部不正リスク拡大）
（５）AI等の新技術普及

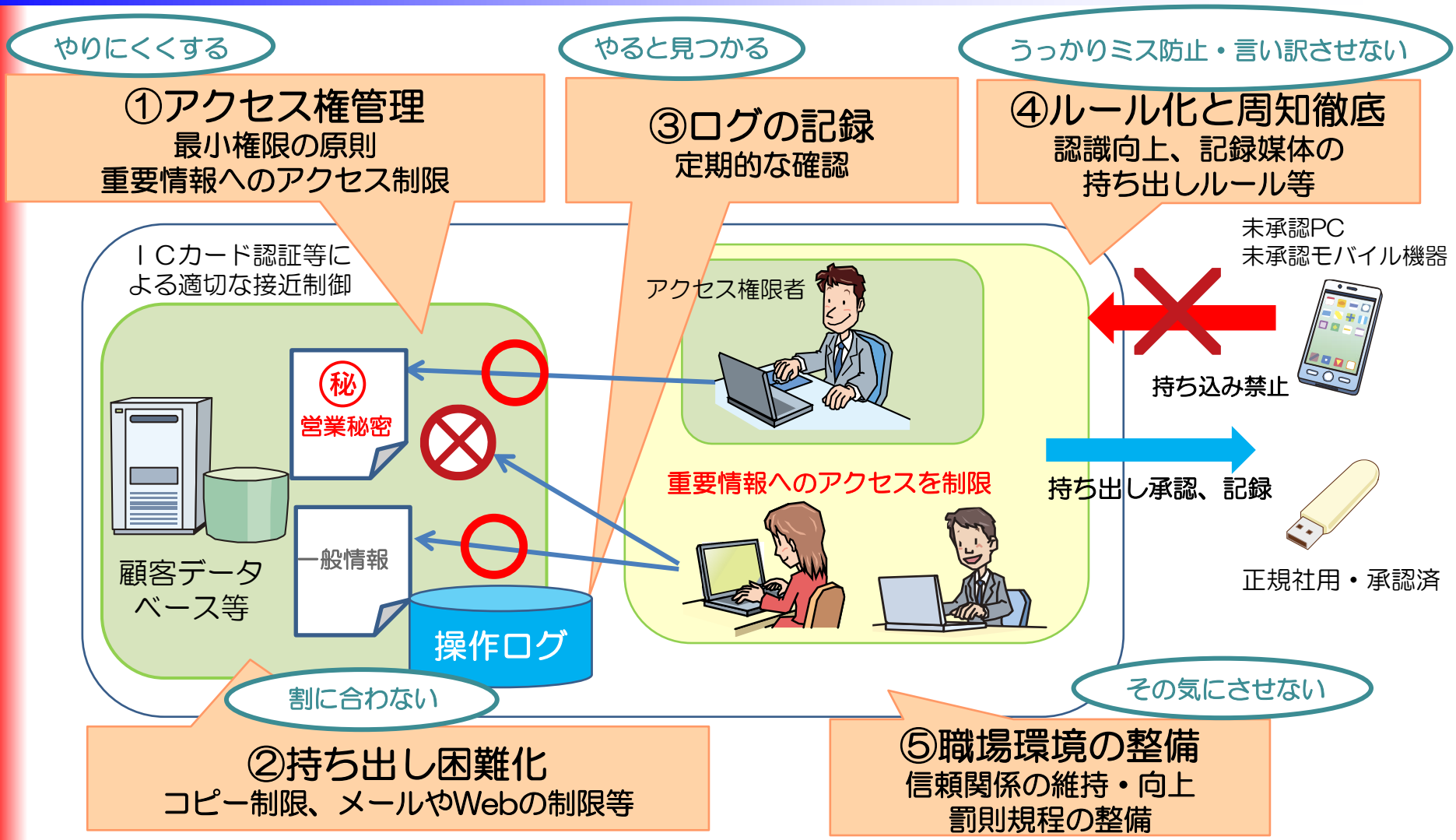
■ガイドライン見直しの必要性
変化（１）（２）に関する記載強化
変化（３）～（５）に対応するための対策強化
①テレワーク・クラウド等の普及に伴う対策
②退職者関連対策の強化
③ふるまい検知等の新技術導入時の対策
（行動モニタリングと適正な運用）

組織における内部不正防止ガイドライン 課題と改訂箇所

内部不正対策の課題を抽出・対応する改訂箇所を特定し、反映しています



変化に対応した対策強化に関連して：
～そもそも内部不正防止の基本対策とは～

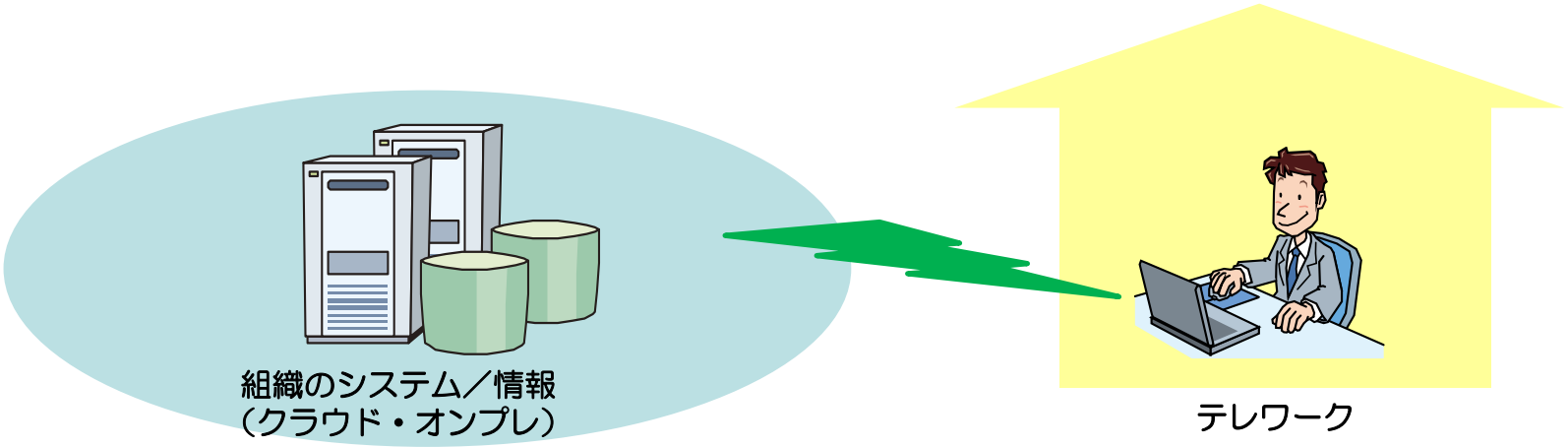


対策の継続した見直し、改善

変化に対応した対策強化：
①テレワーク・クラウドの普及に伴う対策

対策ポイント：技術的な対策・証拠保全等の事後内部不正対策

- 重要情報の保存場所・管理者の明確化　うっかりミス防止・言い訳させない
- クラウド利用ルール・テレワーク端末からのクラウド利用統制（クラウドプロキシ・CASB等）　やりにくくする
- テレワーク端末の記録媒体を暗号化　割に合わない
- エンドポイントを含めたログ取得・分析　やると見つかる

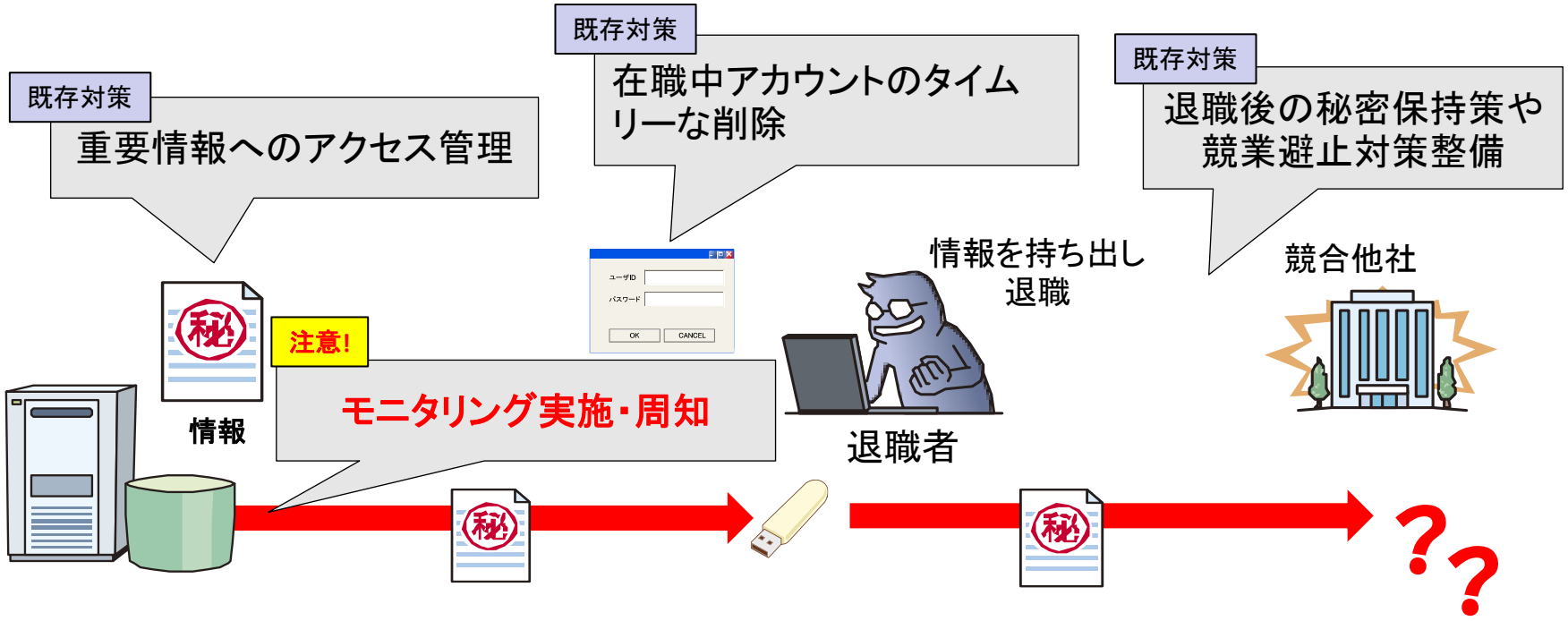


変化に対応した対策強化：
②退職者関連対策

やると見つかる

対策ポイント：　①退職前のモニタリング　②モニタリング周知

- 退職者の内部不正を防止する目的でシステムのモニタリングを行うことは抑止策として有用。
- プライバシーやコンプライアンス上の注意点：
  モニタリングの目的と実施について周知・合意があることが前提。
- **正しく業務を行っている役職員を保護するため**であることを広く周知する。

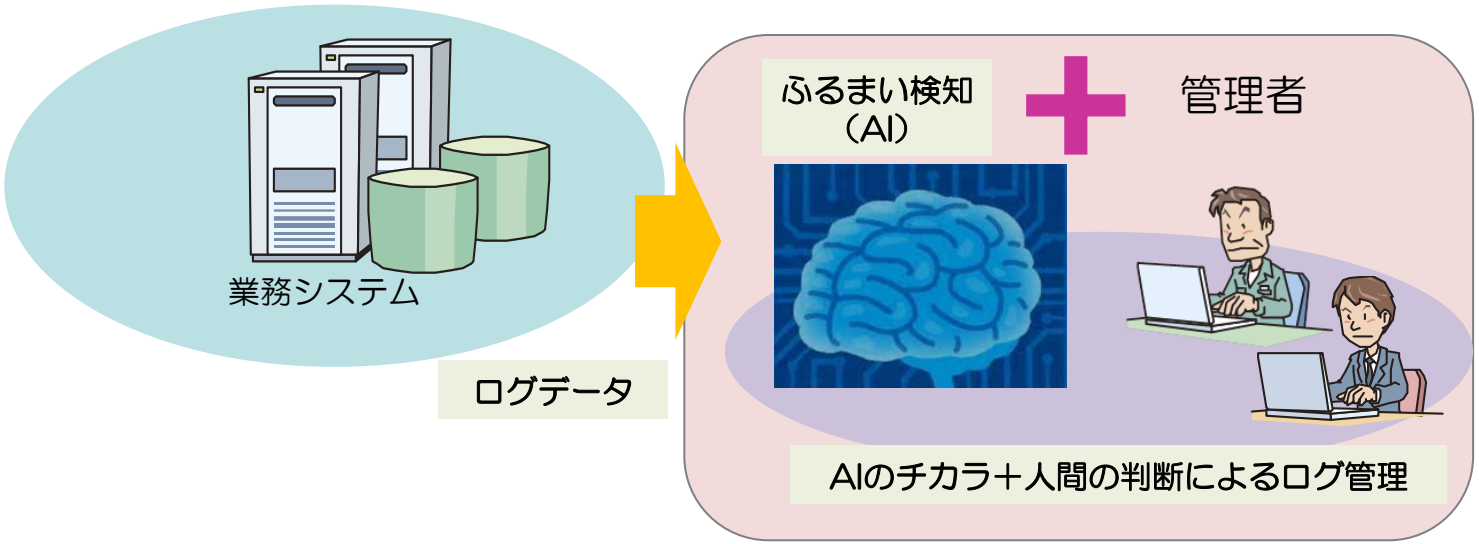


変化に対応した対策強化：
③ふるまい検知等の新技術対策

やると見つかる

対策ポイント：　AI等の技術活用＋「人間」による判断

- パソコン・システム上におけるふるまい検知を含む各種モニタリング
- 役職員の人権・プライバシーに配慮した運用
- モニタリングを労働規約等で周知
- 分析をAIまかせにせず人間による「判断」とAIによる「自動化・効率化」を組み合わせた運用を行う（組織としてモニタリングの説明責任を負う）



内部不正防止ガイドライン第5版公開後の反響

多くのメディアに掲載、ご紹介いただきました！

1．ImpressクラウドWatch
　IPA、「組織における内部不正防止ガイドライン」第5版を公開
　https://cloud.watch.impress.co.jp/docs/news/1400929.html
2．マイナビニュース　Tech
　IPA、「組織における内部不正防止ガイドライン」第5版を公開
　https://news.mynavi.jp/techplus/article/20220406-2314716/
3．Security NEXT
　【セキュリティ ニュース】IPA、内部不正防止ガイドラインを改訂 - テレワーク増加も反映
　https://www.security-next.com/135547
4．IT Media
　IPAの「内部不正防止ガイドライン」、5年振りに更新　テレワーク普及など踏まえ改訂
　https://www.itmedia.co.jp/news/articles/2204/07/news082.html
5．ZDNET　Japan
　IPA、「内部不正防止ガイド」を改訂--テレワークや検知技術を追加
　https://japan.zdnet.com/article/35185943/
など

IPA

Better Life with IT