大手企業でも情報漏えい!?
PC管理手法を見直そう
- ISM CloudOne -

2024年 6月 5日

QualitySoft

©QualitySoft Corporation All right reserved

QualitySoft

Agenda

1. はじめに
2. クオリティソフトについて
3. ITセキュリティの動向・傾向について
4. ISM CloudOneでの対策方法ご紹介
5. まとめ

©QualitySoft Corporation All right reserved

はじめに

©QualitySoft Corporation All right reserved

はじめに

本セミナーには様々な企業の担当者様がご参加いただいておりますが、主に情報システム管理に携わっている方が多いかと存じます。企業の業種業態や規模の大小によって情報システムの在り方は様々で、どういう状態であれば「正解」と言えるかは一様に決められるものではありません。
しかし、それぞれの企業における**ビジネス状況や時代の移り変わりに合わせて情報システムを柔軟に変化し続ける**ことは業種業態や企業規模を問わず、あらゆる企業に求められることです。

本セミナーは2024年のITセキュリティ周りの動向・傾向を発信し、IT資産管理手法の見直しや課題解決を促進することを主旨としております。
既にご存知の内容も含まれるとは存じますが、復習も兼ねた情報収集の機会と捉えていただき、最後までご聴講いただけますと幸いです。

©QualitySoft Corporation All right reserved

クオリティソフト株式会社について

©QualitySoft Corporation All right reserved

QualitySoft

クオリティソフト株式会社について

社名	クオリティソフト株式会社
Web	https://www.qualitysoft.com/corporate/infodata/profile/
設立	1984年2月24日
主な事業	IT資産管理ソフト開発・販売
主な製品	ISM CloudOne、QNDシリーズ
本社	和歌山県白浜町
営業拠点	東京・大阪・名古屋
開発拠点	和歌山・長野・宮城
海外拠点	上海

■会社紹介動画

https://www.youtube.com/watch?v=MUGb2Inz42Y

©QualitySoft Corporation All right reserved

QualitySoft

ITセキュリティの動向・傾向について

©QualitySoft Corporation All right reserved

QualitySoft

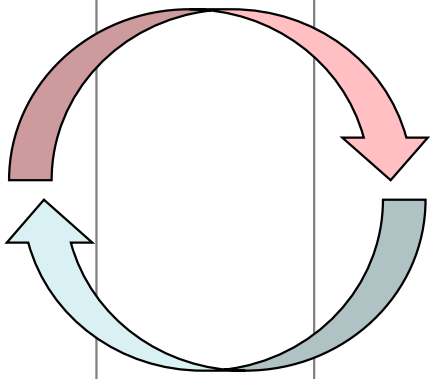
ITセキュリティの動向・傾向について

外的要因

- **法改正**

（働き方改革、個人情報保護法改正、など）

- **サイバー攻撃の増加/高度化**
- **IT技術の進化/陳腐化**
- **業界毎の取り組み**
- **取引先からの要求**



内的要因

- 社員数の増減
- 取引先の増減
- 会社知名度の変化
- 人材確保
- 社員のITリテラシー
- 内部統制

セキュリティは外的要因と内的要因の両面を理解して講じていくものですが、
本日は影響を受けやすい外的要因にフォーカスしてご案内いたします。

©QualitySoft Corporation All right reserved

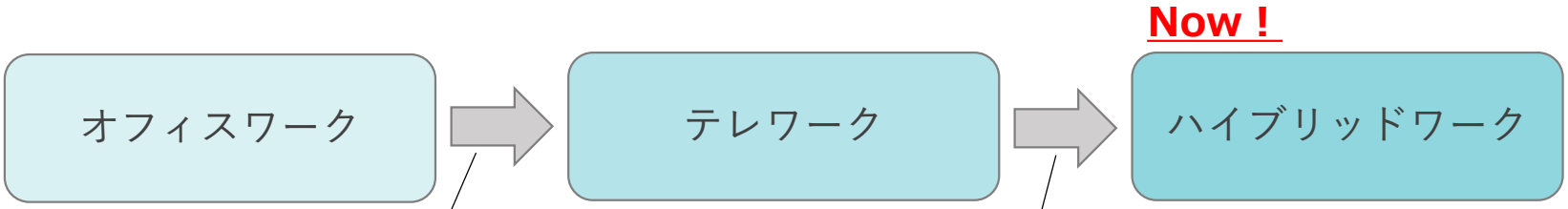
QualitySoft

ITセキュリティの動向・傾向について
～ 働き方の変化 ～

©QualitySoft Corporation All right reserved

ITセキュリティの動向・傾向について

働き方の変化



▼テレワークへの変化を促した要素
- 東京オリンピック対策
- 働き方改革
- コロナ禍
- VDI技術やチャットツールの進化
- Web会議ツールの進化

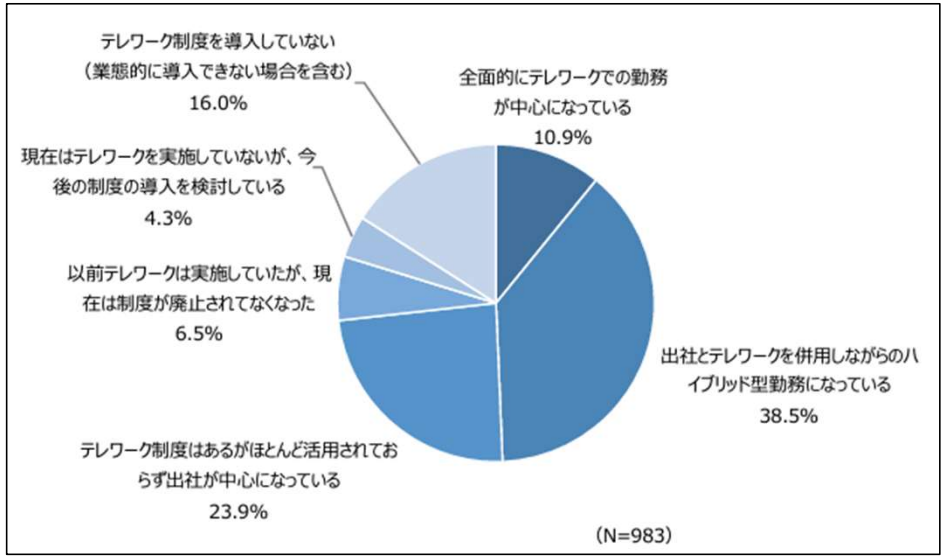
▼ハイブリッドワーク変化を促した要素
- テレワークによる業務効率低下
- テレワークによるコミュニケーション品質低下
- 売り手市場の人材採用事情
- 多様な働き方への対応

ハイブリッドワークを継続する企業は多い

©QualitySoft Corporation All right reserved

ITセキュリティの動向・傾向について

ハイブリッドワーク



Q：あなたの勤務先におけるテレワークの実施状況をお答えください。

・出社とテレワークを併用しながらのハイブリッド型が38.5%で現在の主流となっている。「全面的にテレワークでの勤務が中心」は10.9%にとどまっている。

・「テレワーク精度はあるが活用されておらず出社が中心」が23.9%、「以前は実施していたが、現在は廃止された」が6.5%となり、出社回帰の兆候が出ている。

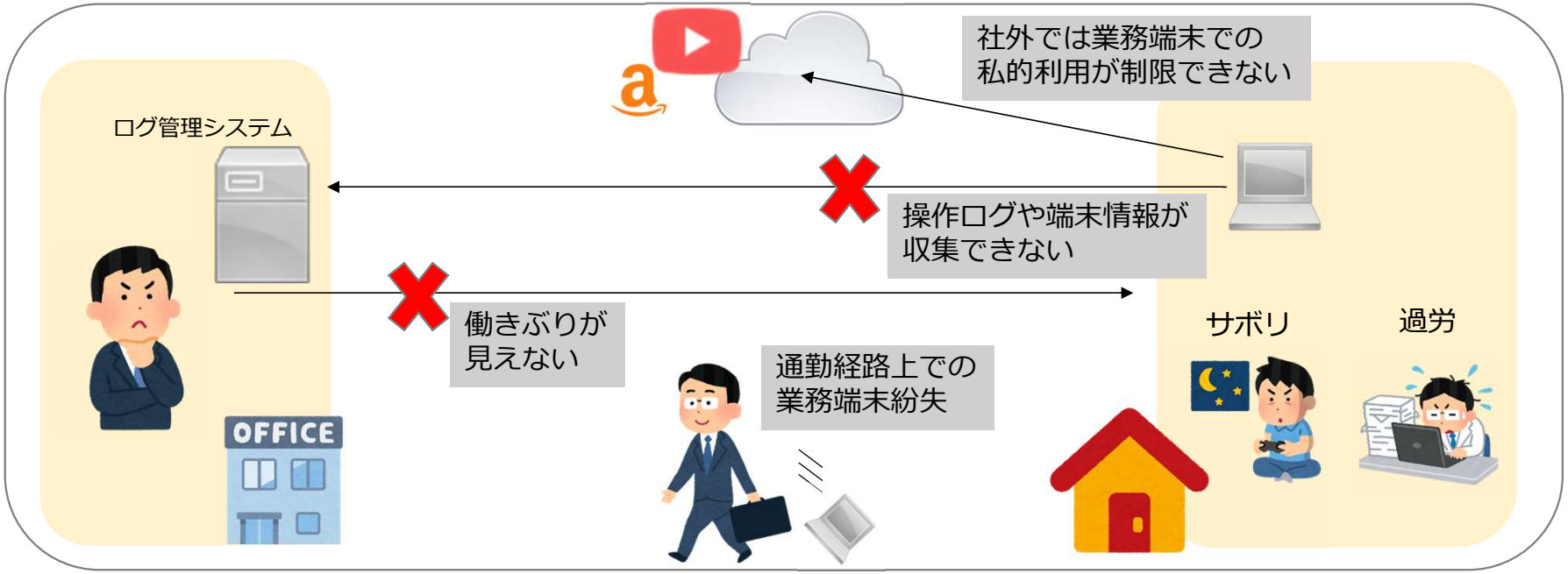
・業種別では情報通信が最も活用されている。建設・不動産、金融・保険、サービス等で出社回帰が目立っている。

一般財団法人日本情報経済社会推進協会（JIPDEC） セミナー参考資料「企業IT利活用動向調査2024」集計結果より抜粋

©QualitySoft Corporation All right reserved

ITセキュリティの動向・傾向について

ハイブリッドワークならではの課題



働き方の変化に対応したセキュリティが必要

アマゾン アイコン by Icons8
YouTube アイコン by Icons8

©QualitySoft Corporation All right reserved

QualitySoft

ITセキュリティの動向・傾向について
～ 技術の進化 ～

©QualitySoft Corporation All right reserved

ITセキュリティの動向・傾向について

AI技術の進化/コモディティ化

ChatGPT

Copilot

■メリット

業務効率アップ　/　分析難易度の低下　/　分析精度向上

マイクロソフト コパイロット アイコン by Icons8

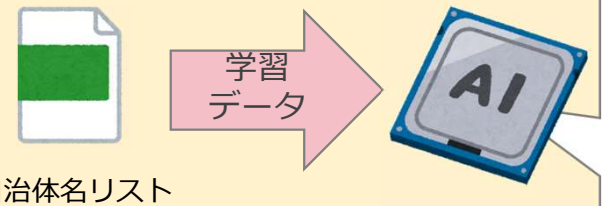
チャットチャット アイコン by Icons8

©QualitySoft Corporation All right reserved

ITセキュリティの動向・傾向について

AI技術の進化/コモディティ化

■AIの学習の仕組み（参考）



自治体名リスト
47都道府県名

■自治体名
・北海道
・青森
New！ ・東京

もしも一般に公開されているAIに、
企業秘密や保有する個人情報が学習されてしまったら…？

©QualitySoft Corporation All right reserved

ITセキュリティの動向・傾向について

AI技術の進化/コモディティ化

■対策すべきこと

- 社員を教育する
- 社内規定を定める

→ 運用で対策が必要

- 利用を制限する
- 利用を監視する

→ システムで対策が必要

どちらか一方に頼らず両面でカバーが必要

©QualitySoft Corporation All right reserved

QualitySoft

ITセキュリティの動向・傾向について

～ セキュリティに対する考え方の変化 ～

©QualitySoft Corporation All right reserved

QualitySoft

ITセキュリティの動向・傾向について

組織向けの脅威の順位

表 1.2 情報セキュリティ 10 大脅威 2024「組織」向けの脅威の順位

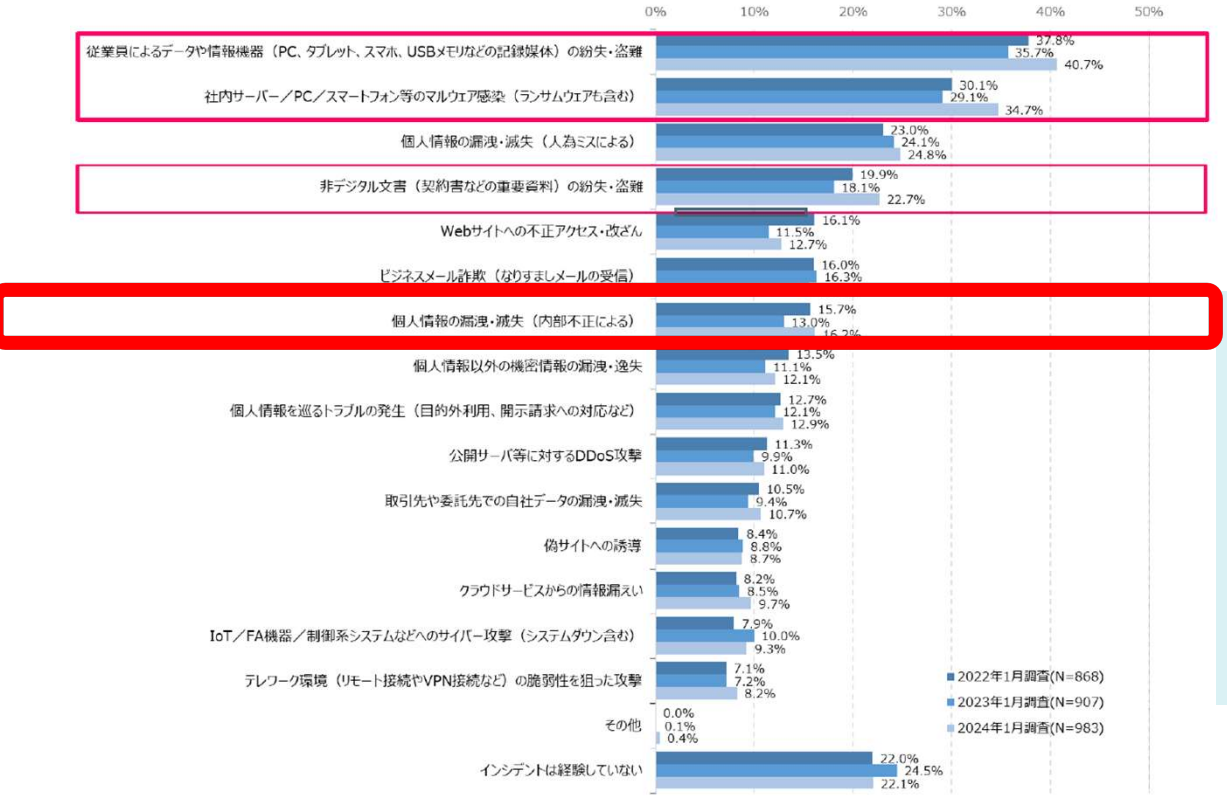
順位	「組織」向け脅威	初選出年	10 大脅威での取り扱い（2016 年以降）
1	ランサムウェアによる被害	2016 年	9 年連続 9 回目
2	サプライチェーンの弱点を悪用した攻撃	2019 年	6 年連続 6 回目
3	内部不正による情報漏えい等の被害	2016 年	9 年連続 9 回目
4	標的型攻撃による機密情報の窃取	2016 年	9 年連続 9 回目
5	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	2022 年	3 年連続 3 回目
6	不注意による情報漏えい等の被害	2016 年	6 年連続 7 回目
7	脆弱性対策情報の公開に伴う悪用増加	2016 年	4 年連続 7 回目
8	ビジネスメール詐欺による金銭被害	2018 年	7 年連続 7 回目
9	テレワーク等のニューノーマルな働き方を狙った攻撃	2021 年	4 年連続 4 回目
10	犯罪のビジネス化（アンダーグラウンドサービス）	2017 年	2 年連続 4 回目

独立行政法人情報処理推進機構セキュリティセンター（IPA） 発行 「情報セキュリティ10大脅威2024」より抜粋

©QualitySoft Corporation All right reserved

ITセキュリティの動向・傾向について

セキュリティ・インシデントの経験（直近1年）



■アンケート結果からみる傾向

・「非デジタル文書のj紛失・盗難」と**「個人情報の漏洩・滅失（内部不正による）」も前回よりも上昇している。**

・「従業員による紛失・盗難」が過去2回と同じく最も多くなっており、前回よりも上昇している。

・「マルウェア感染」が過去2回よりも上昇し、ランサムウェアなどサイバー攻撃による被害が増えていると見られる

一般財団法人日本情報経済社会推進協会（JIPDEC） セミナー参考資料「企業IT利活用動向調査2024」集計結果より抜粋

©QualitySoft Corporation All right reserved

QualitySoft

ITセキュリティの動向・傾向について

▼直近３年の間に起きた有名なセキュリティインシデント

①世界的有名な自動車メーカーがサプライチェーン攻撃を受け、14の工場が稼働停止

②元国営企業の子会社で、派遣社員が1,000万件超の顧客情報を流出

③著名なスマホアプリメーカーで44万件の個人情報流出

■Check

・大手企業においても被害を受けている
・海外拠点や子会社を経由して被害を受けるケースも多い
・内部不正がきっかけとなるケースも多い

©QualitySoft Corporation All right reserved

QualitySoft

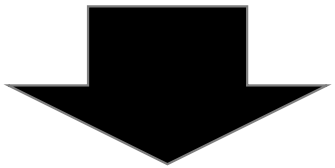
ITセキュリティの動向・傾向について

▼サイバー攻撃の高度化

- 標的型攻撃の増加
- サプライチェーン攻撃の増加

▼情報漏えいの増加

- 情報機器紛失に伴うもの
- 内部不正に伴うもの



自社だけではなく取引先も含めた対策状況の可視化が必要

©QualitySoft Corporation All right reserved

QualitySoft

ITセキュリティの動向・傾向について

セキュリティガイドラインの策定

■業界毎に策定されているガイドライン（参考）

・自動車産業サイバーセキュリティガイドライン

・工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン

・法律事務所　弁護士情報セキュリティ規程

・建設現場における情報セキュリティガイドライン

・医療情報システムの安全管理に関するガイドライン

※業種業態に合わせたガイドラインの有無問わず、
取引先のセキュリティ状況を問うケース増加
大手企業が取引先に求めることが多い
新規取引だけでなく、継続の場合も同様

**ビジネスを維持・拡大していく上でも
セキュリティ向上が必要**

©QualitySoft Corporation All right reserved

QualitySoft

ITセキュリティの動向・傾向について

求められるセキュリティ対策項目の例

項目	詳細
機密情報を取扱う**パートナー企業のセキュリティ対策状況を把握**する	・チェックシートを作成しパートナー企業から回答を受領する ・パートナー企業に訪問し点検を実施する
PCで利用を許可または**禁止するソフトウェアを定め**、ソフトウェアの無断インストールを禁止し、**違反がないか定期的に確認**している	・社内で利用許可または禁止するソフトウェアの一覧を作成し周知すること ・ソフトウェアの無断インストールを制限すること ・定期的にソフトウェアのインストール状況を確認すること ※システムでインストール制限している場合は確認不要
PCからの**データ書き出しを仕組みで制限**している	・データ書き出しを制限する仕組みを導入すること
不正なWebサイトへのアクセスを制限している	・不正なWebサイトへのアクセスを制限すること
情報システム・情報機器、ソフトウェアへ**セキュリティパッチやアップデート適用を適切に行って**いる	・セキュリティパッチやアップデート適用を、規則と期限を定め実施すること
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	・PCが操作されたログを取得、保管すること

運用で対応すべきものもあるが、
システム的に制限をかけることでしか対応できないものも多い

©QualitySoft Corporation All right reserved

ITセキュリティの動向・傾向について
～ まとめ ～

©QualitySoft Corporation All right reserved

QualitySoft

ITセキュリティの動向・傾向について

ここまでのまとめ

企業として求められる情報システム・情報セキュリティは
最適化し続ける必要があります。

働き方の変化に対応	テクノロジーの変化に対応	ビジネス拡大させる上での セキュリティ対応

クラウド型IT資産管理ツール　ISM CloudOneの活用を推奨いたします。

©QualitySoft Corporation All right reserved

QualitySoft

ISM CloudOneでの対策方法ご紹介

©QualitySoft Corporation All right reserved

QualitySoft

ISM CloudOneでの対策方法ご紹介

ISM CloudOneとは…

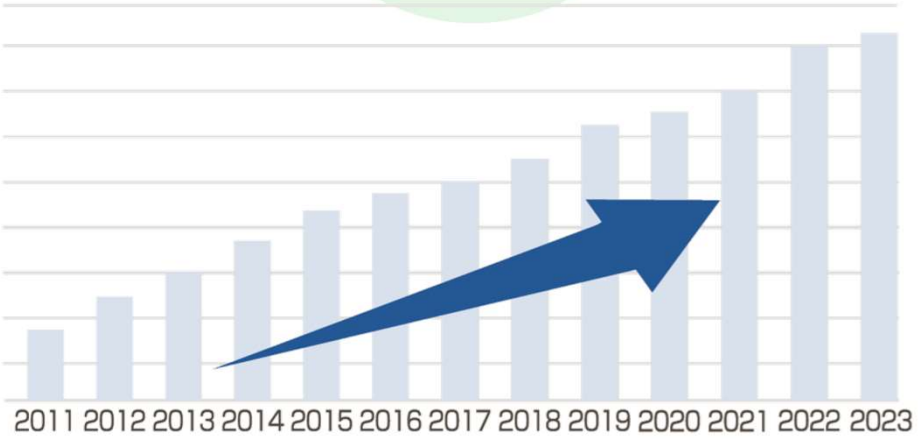
IT資産管理・クライアント管理ツール
（SaaS・クラウド）

7年連続シェアNo.1

※デロイト トーマツ ミック経済研究所株式会社
「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」
https://mic-r.co.jp/mr/02620/

導入実績

80,000社以上



※2022年10月時点

世界導入国

55カ国以上

©QualitySoft Corporation All right reserved

QualitySoft

ISM CloudOneでの対策方法ご紹介

サイバー攻撃対策

- 自動脆弱性診断
- ふるまい検知
- 操作ログ取得

など

ISM CloudOne

- IT資産管理
- スマートデバイス管理

情報漏えい対策

- BitLocker管理
- 操作ログ取得
- 外部デバイス制御

など

©QualitySoft Corporation All right reserved

QualitySoft

ISM CloudOneでの対策方法ご紹介

対策すべき項目

©QualitySoft Corporation All right reserved

QualitySoft

ISM CloudOneでの対策方法ご紹介

対策すべき項目

5 項目

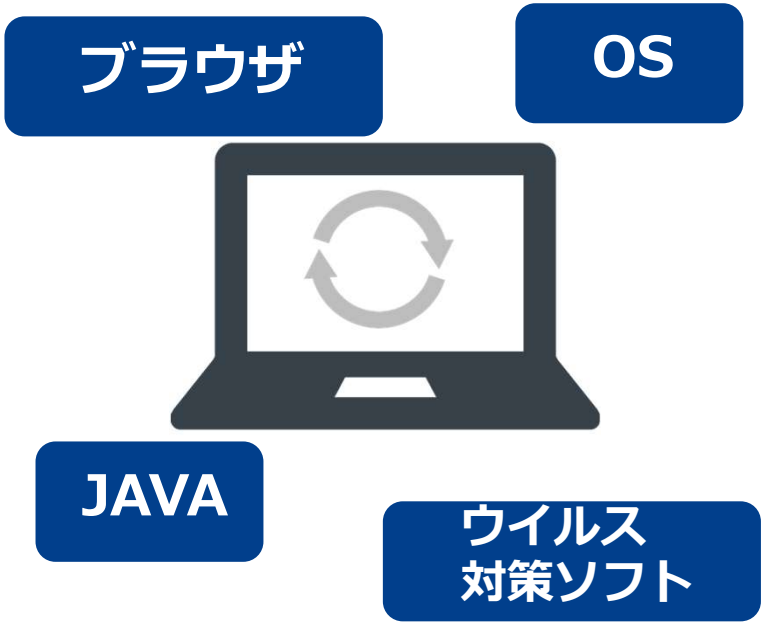
1. 脆弱性を放置したままにしていないか
2. 情報の持ち出しをできないようにする
3. 操作ログ取得、証跡を確保
4. 不審なWebサイトへのアクセス制御
5. 利用するソフトウェア・SaaSの確認

©QualitySoft Corporation All right reserved

QualitySoft

ISM CloudOneでの対策方法ご紹介

脆弱性を放置したままにしていないか



■放置リスク

マルウェア感染

不正アクセス

標的型攻撃

Webサイトの改ざん

DoS攻撃/DDoS攻撃

©QualitySoft Corporation All right reserved

ISM CloudOneでの対策方法ご紹介

脆弱性への対策

ダッシュボードでのセキュリティ状況チェック

■確認できること（例）

- OSセキュリティパッチ適用診断サマリ
- アンチウイルスソフト診断サマリ
- 管理端末の暗号化状況サマリ
- アラート発生状況

©QualitySoft Corporation All right reserved

QualitySoft

ISM CloudOneでの対策方法ご紹介

脆弱性への対策

問題が生じている端末への対処

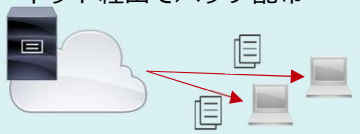
3 件 [1-3] CSV出力（一覧） CSV出力（詳細）

ハードウェア名	NG内容（OSセキュリティ更新プログラム診断）	グループ名	利用者名	OS	Windows 10 / 11 バー...
BDLSRV	KB5037771	test	試験 太郎	Microsoft Windows 11 Enterprise	23H2
SANAI-WIN11-01	KB5036893	未所属		Microsoft Windows 11 Pro	22H2
AUTO-LOG2	KB5037771	_自動ログ	上田 太郎	Microsoft Windows 11 Pro	22H2

■状況に応じたツールで対処

- ファイル配布機能
- リモートコントロール機能
- メール/メッセージ通知

例）テレワーク端末にインターネット経由でパッチ配布



例）適用失敗原因を遠隔で確認

©QualitySoft Corporation All right reserved

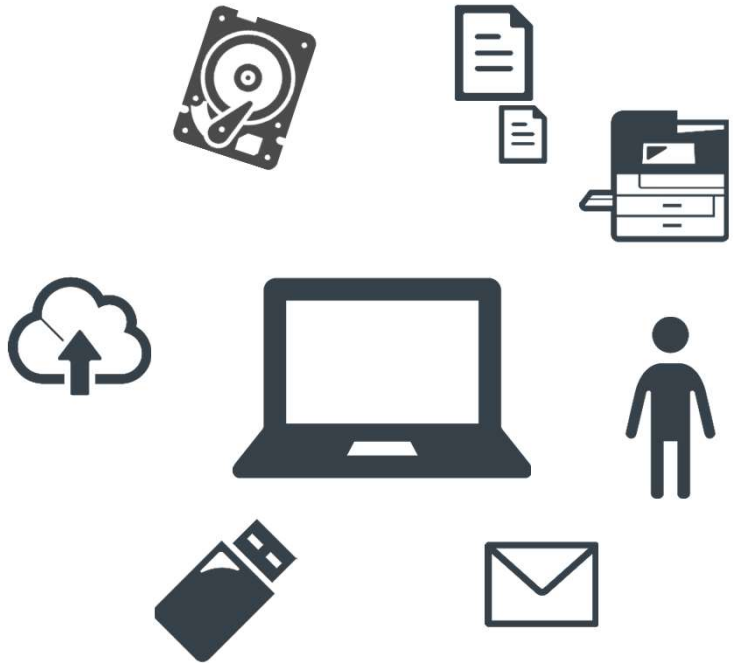
QualitySoft

ISM CloudOneでの対策方法ご紹介

情報の持ち出しをできないようにする

紛失・盗難対策

内部不正対策



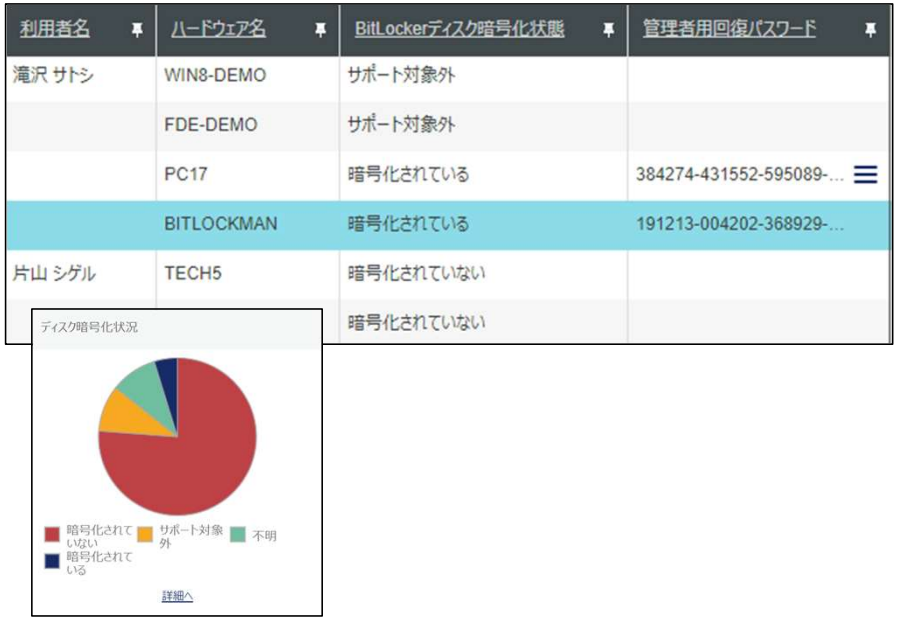
©QualitySoft Corporation All right reserved

QualitySoft

ISM CloudOneでの対策方法ご紹介

情報の持ち出しへの対策（BitLocker制御）

暗号化状況の可視化



暗号化の遠隔実行

紛失時の情報漏えいリスクを低減

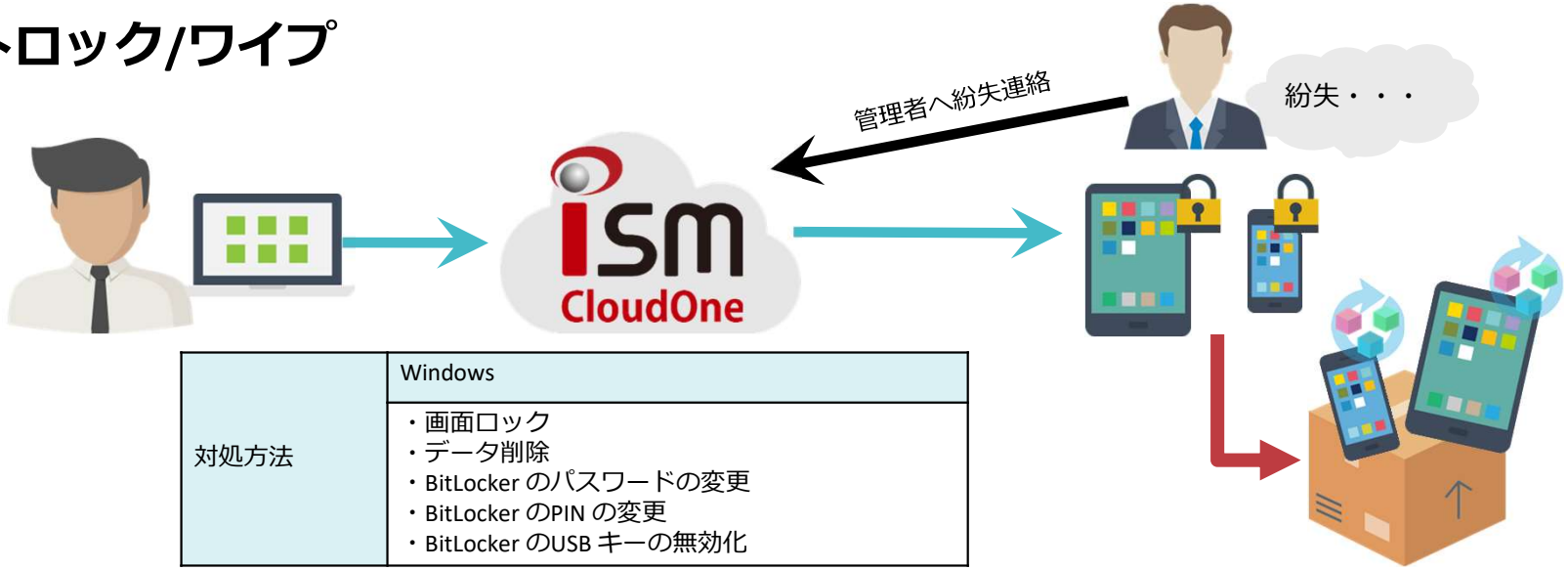
©QualitySoft Corporation All right reserved

QualitySoft

ISM CloudOneでの対策方法ご紹介

情報の持ち出しへの対策

・リモートロック/ワイプ



	Windows
対処方法	・画面ロック ・データ削除 ・BitLocker のパスワードの変更 ・BitLocker のPIN の変更 ・BitLocker のUSB キーの無効化

紛失時の情報漏えいリスクを低減

©QualitySoft Corporation All right reserved

QualitySoft

ISM CloudOneでの対策方法ご紹介

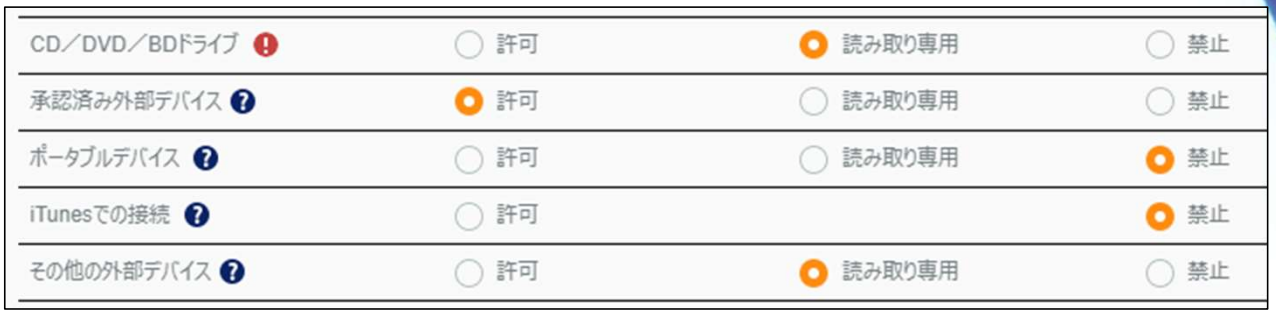
情報の持ち出しへの対策

・外部デバイス制御

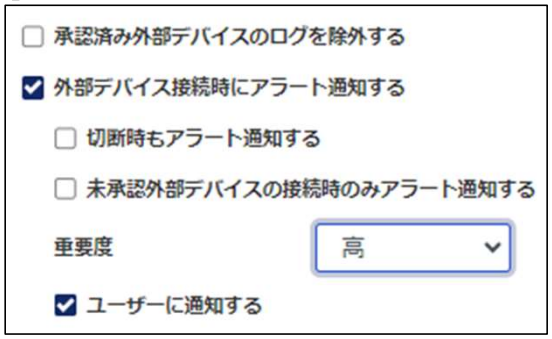
会社全体

部署別拠点別

端末単位



・ログ取得



操作ログ種別	重要度	ログ取得日時	コンピューター名	アラート種別
外部デバイス	中	2023/08/30 10:33:23	AUTO-LOG2	未承認外部デバイス接続
外部デバイス	中	2023/08/18 11:33:59	AUTO-LOG2	未承認外部デバイス接続
外部デバイス	中	2023/08/18 10:46:00	AUTO-LOG2	外部デバイス接続
外部デバイス	中	2023/08/18 09:22:20	AUTO-LOG2	未承認外部デバイス接続
外部デバイス	中	2023/08/10 10:21:34	AUTO-LOG2	外部デバイス接続
外部デバイス	中	2023/08/08 11:44:51	AUTO-LOG2	未承認外部デバイス接続

情報持ち出しの制御と可視化及び監視を実現

©QualitySoft Corporation All right reserved

ISM CloudOneでの対策方法ご紹介

操作ログ取得、証跡を確保

いつ、どこで

誰が（何が）

どのような

操作を行ったのか

©QualitySoft Corporation All right reserved

QualitySoft

ISM CloudOneでの対策方法ご紹介

操作ログ取得・証跡確保の対策

- インシデント発生時の追跡
- 不正行為の抑止
- SaaS利用状況の可視化

©QualitySoft Corporation All right reserved

QualitySoft

ISM CloudOneでの対策方法ご紹介

不審なWebサイトへのアクセス制御

不審なサイト

業務に関係のサイトSNS

私用オンラインストレージ

私用Webメール

©QualitySoft Corporation All right reserved

ISM CloudOneでの対策方法ご紹介

不審なWebサイトへのアクセス制御の対策

148種 72億7741万コンテンツ[※1]の中から制御対象を選択し、制御可能

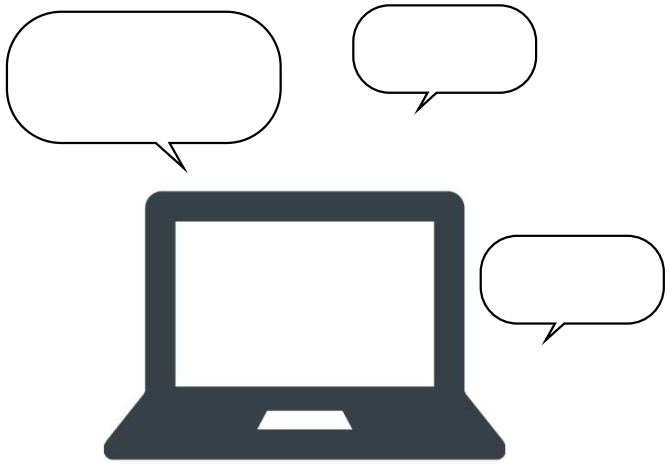
※1　出展）アルプスシステムインテグレーション株式会社
「マルチデバイス対応Webフィルタリング InterSafe Cats データベース」
2023年9月1日時点　　https://www.alsi.co.jp/security/iscats/database/

©QualitySoft Corporation All right reserved

QualitySoft

ISM CloudOneでの対策方法ご紹介

利用するソフトウェア・SaaSの確認



ユーザーの利用している
ソフトウェア／SaaSサービス
把握できていますか？

情報漏えいの危険性が高いもの

業務に関係のないもの

脆弱性が潜んだもの

©QualitySoft Corporation All right reserved

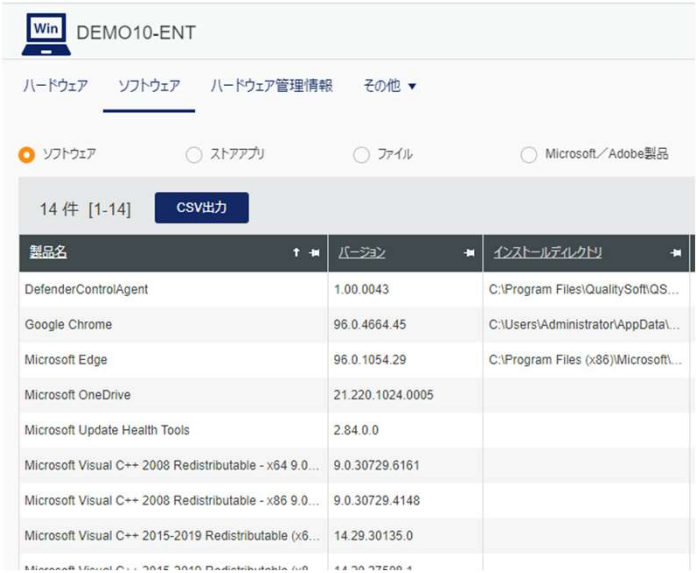
QualitySoft

ISM CloudOneでの対策方法ご紹介

ソフトウェア・SaaSサービス可視化の対策

ソフトウェア

利用ソフトの可視化



起動制御

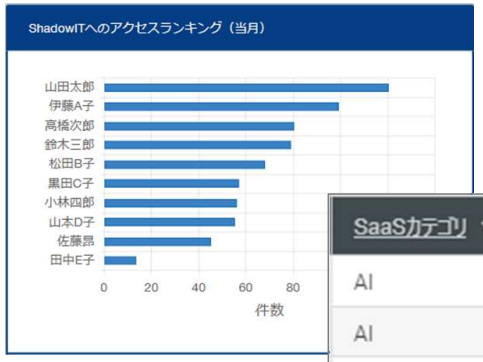
©QualitySoft Corporation All right reserved

QualitySoft

ISM CloudOneでの対策方法ご紹介

ソフトウェア・SaaSサービス可視化の対策

SaaS



シャドーIT状況の可視化

利用・アクセスを制御

SaaSカテゴリ	SaaSサービス名	SaaSドメイン
AI	Aichatting	aichatting.net
AI	alt BRAIN	altbrain.ai
AI	elai.	app.elai.io
AI	AI GIJIROKU	app.gijiroku.ai
AI	Google Bard	bard.google.com
AI	bing AI（汎用）	bing.com
AI	ChatGPT	chat.openai.com
AI	clipdrop（汎用）	clipdrop.co
AI	CREEVO	creevo-music.com

ChatGPTの
隠れ利用も
しっかり捕捉

規制内容	許可	書き込み規制	規制	一時解除
ウェブアプリケーション	○	●	○	○
プログラムダウンロード	○	○	○	●
更新ファイル・ドライバ	○	●	○	○
デジタル素材	○	●	○	○
IT	○	●	○	○
ダイナミックDNS	○	●	○	○
AI	○	○	○	●

©QualitySoft Corporation All right reserved

QualitySoft

まとめ

対策すべき項目	有効な機能
1. 脆弱性を放置したままにしていないか	自動脆弱性診断、ファイル配布
2. 情報の持ち出しをできないようにする	外部デバイス制御、操作ログ、BitLocker制御、 リモートロック/削除、URLフィルタリング
3. 操作ログ取得、証跡を確保	操作ログ取得
4. 不審なWebサイトへのアクセス制御	URLフィルタリング、操作ログ取得
5. 利用するソフトウェア・SaaSの確認	SaaS利用レポート、禁止ソフトウェア制御 URLフィルタリング

©QualitySoft Corporation All right reserved

QualitySoft

まとめ

ism CloudOne

IT資産管理・クライアント管理ツール（SaaS・クラウド）

7年連続 シェアNo.1※

※デロイト トーマツ ミック経済研究所株式会社　「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」
https://mic-r.co.jp/mr/02620/

30日間　10ライセンスご用意

ご希望のオプションも一緒にお試しいただけます！

営業担当：馬場淳木　　j.baba@qualitysoft.com

お問合せ窓口ML　　canon-toiawase@qualitysoft.com

©QualitySoft Corporation All right reserved

©QualitySoft Corporation All right reserved