

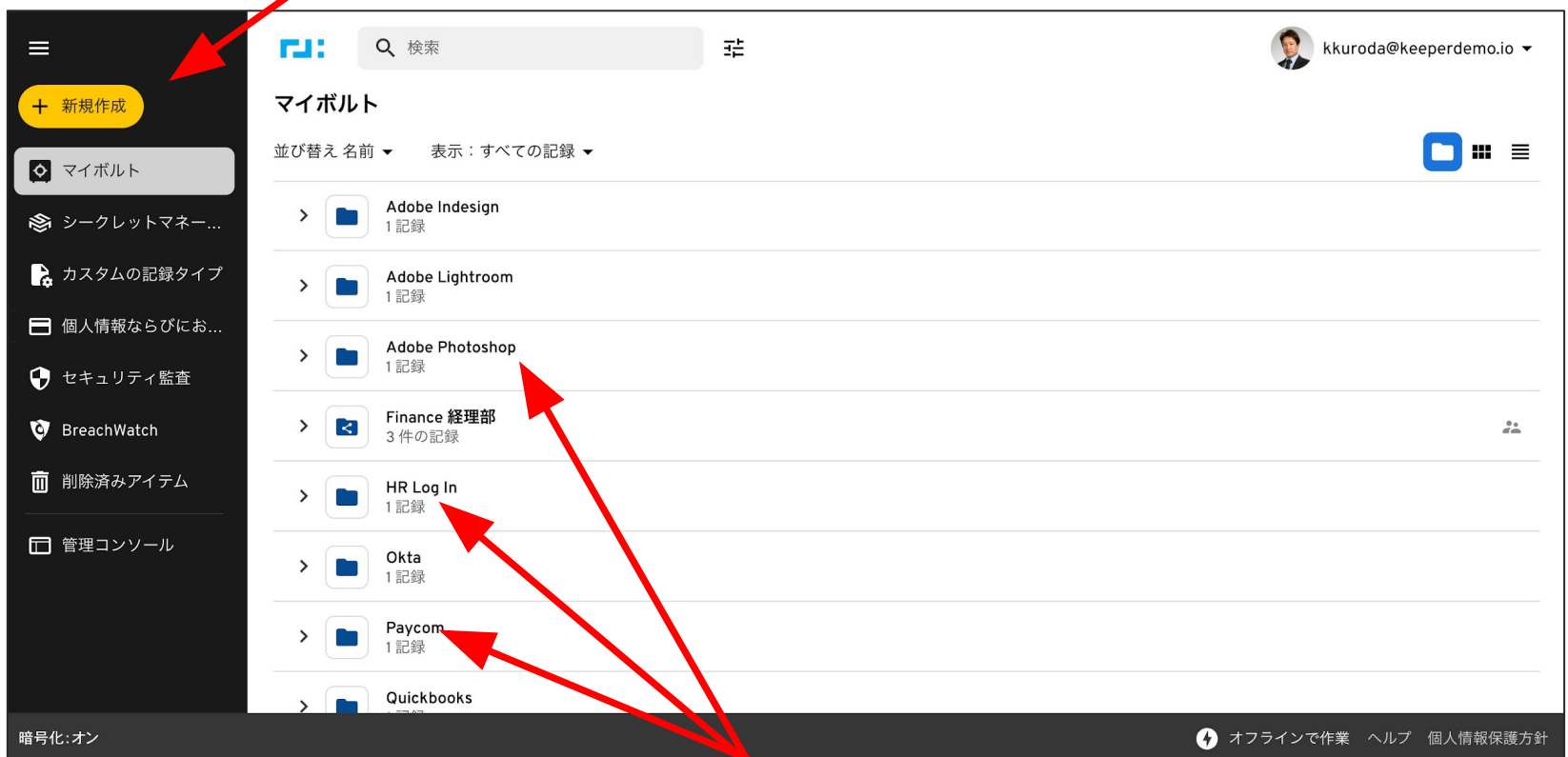
機能紹介・デモ画面



DEMO: ユーザーポルト

データの新規追加

クリックしてアカウントとパスワードを新規登録

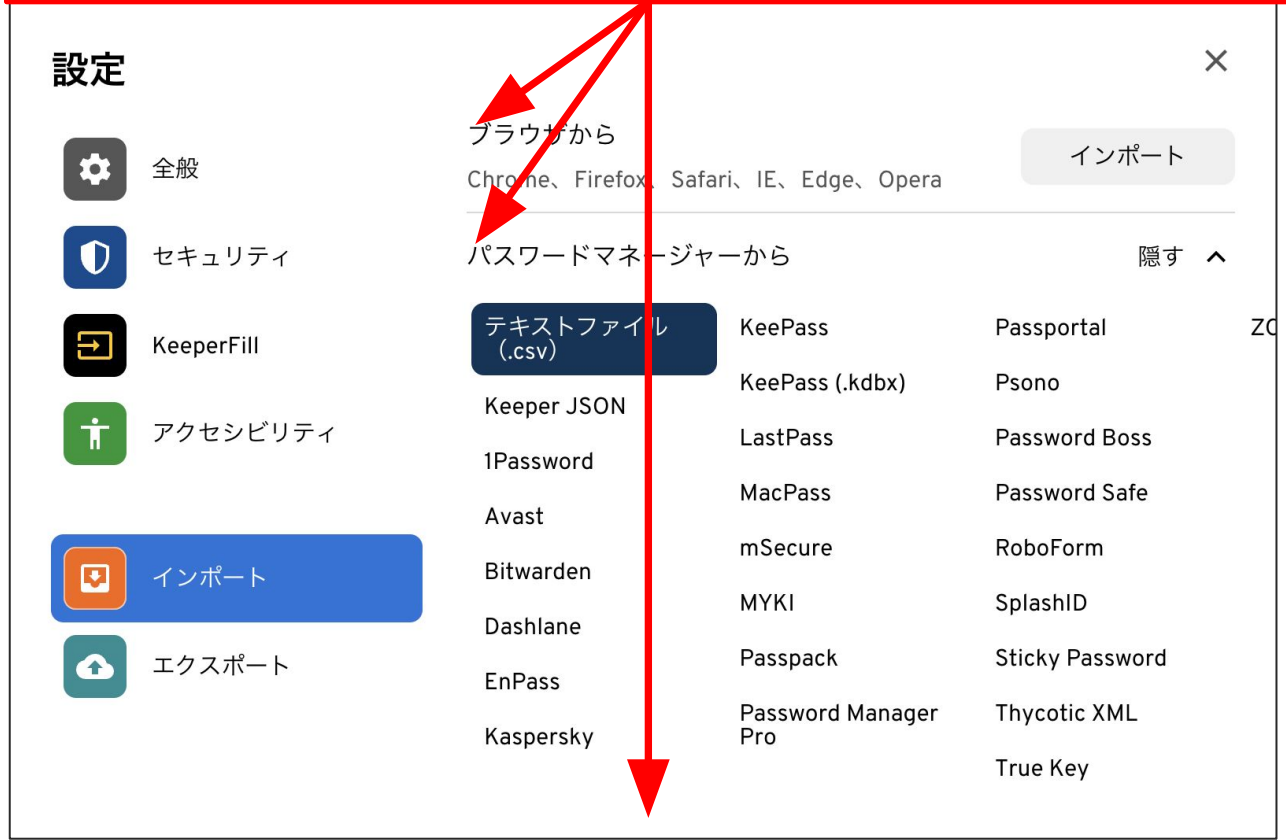


全てのログイン情報を簡単に閲覧

左側のメニューバーで「+ Create New」「Record」の順にクリックするだけでパスワードを保存できます。パスワードの記録にファイルや写真等の添付も可能。
 ログインしたい他のアプリ毎に2要素認証(2FA)を設定してワンタイムパスワードを生成することもできるため、安全にご利用頂くことができます。

データのインポート

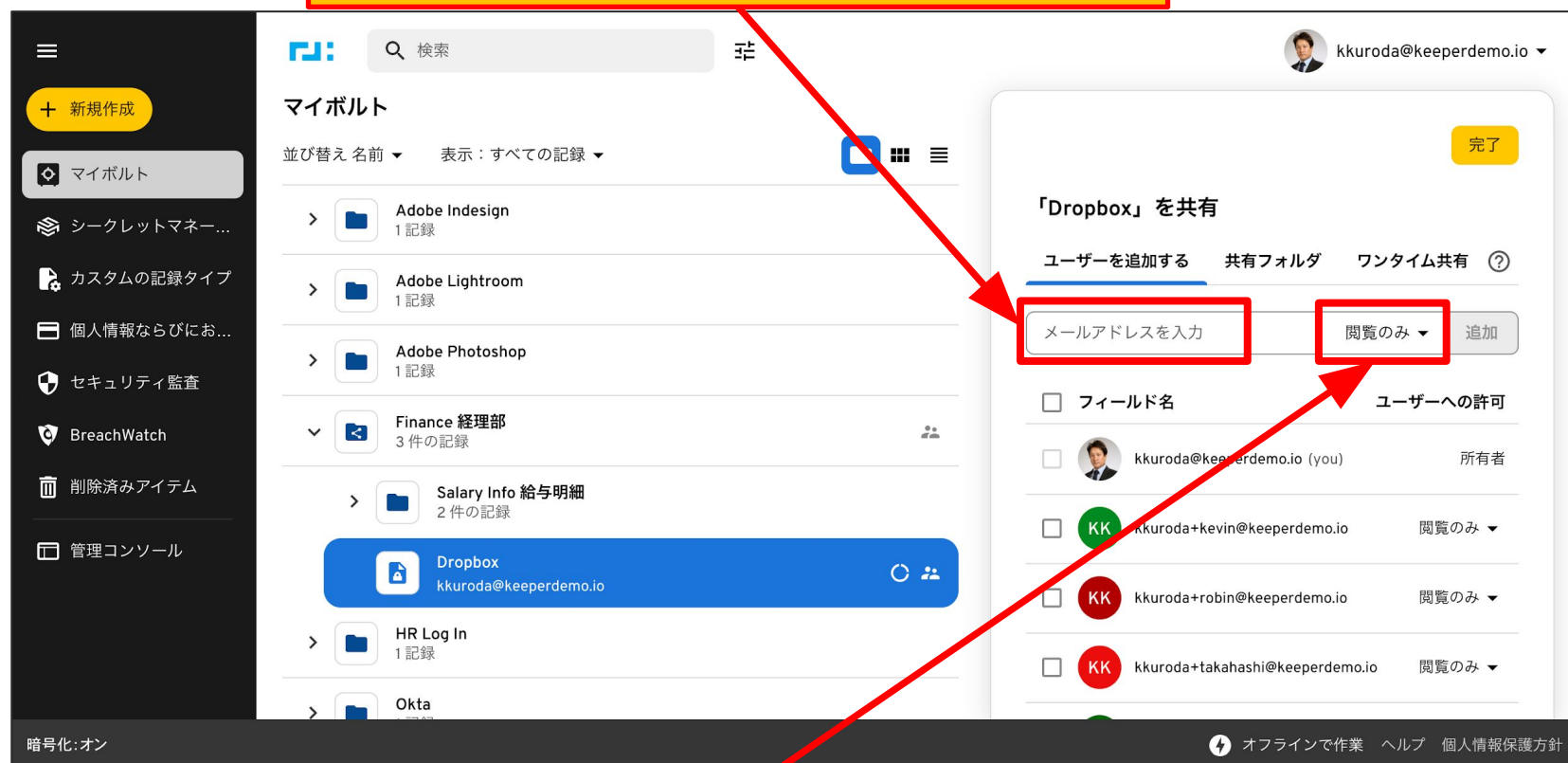
ブラウザ、他社パスワード管理、Excel (CSV形式) からインポート



右上プロフィール -> 設定 -> インポート
 一般的なブラウザ、他のパスワードマネージャー、CSVファイルからパスワードを直接インポートできます。
 ブラウザに保存されているパスワードを自動的に収集して保存してくれるため、非常に使いやすく、迅速に利用を開始することが可能です。

パスワードやファイルの共有

ログイン情報やファイルを
他のユーザーと共有



共有した相手の権限レベルを選
択

誰かとログイン情報を共有するにはボルトに保存されているエントリーを選び、オプション欄の共有ボタンから簡単に情報をシェアできます。共有先が実際のパスワードを見られない状態でパスワードを共有することもでき、安全に情報をシェアすることが可能です。

ブラウザ拡張機能

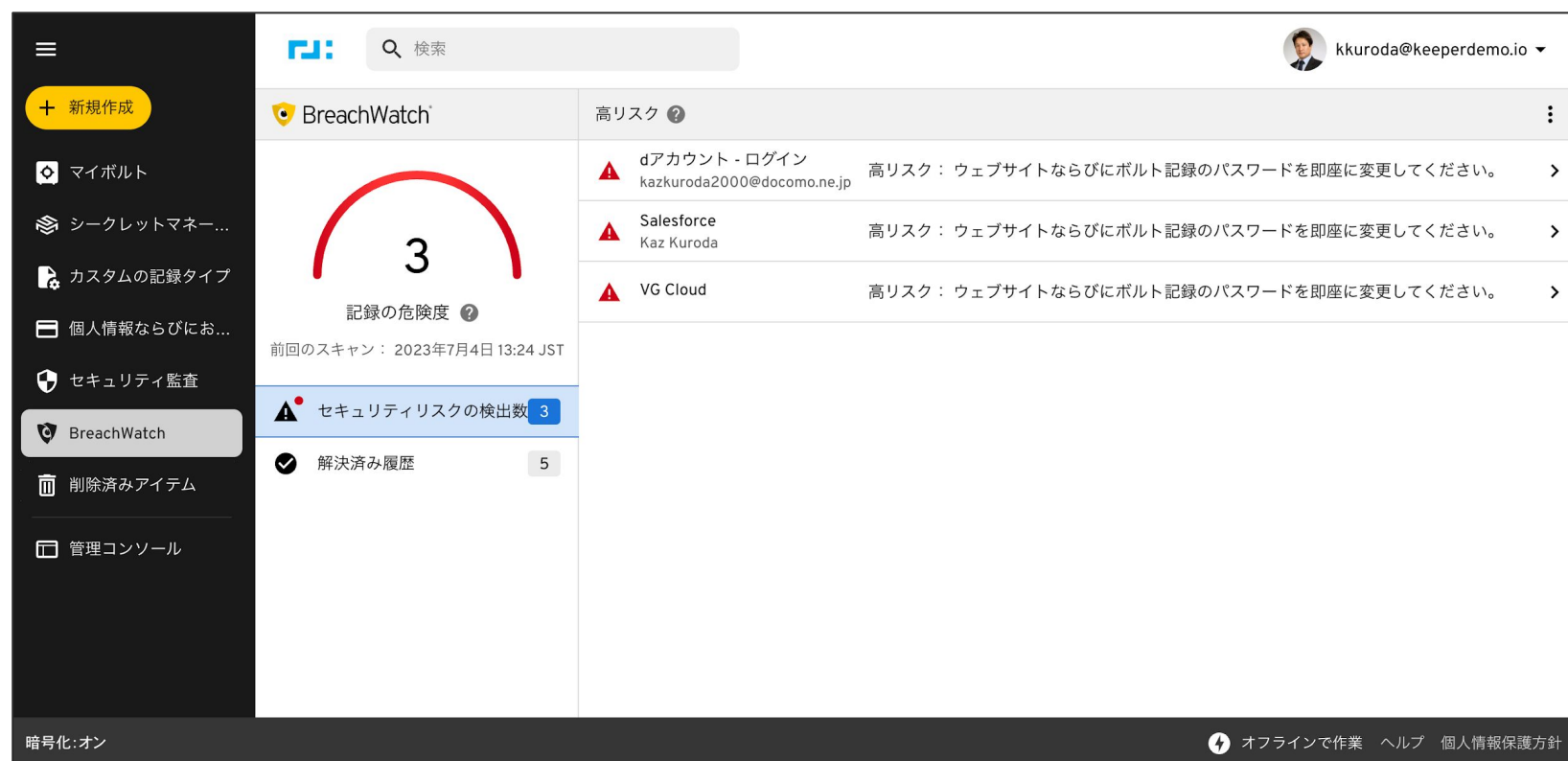
KeeperFill ブラウザー拡張は操作が
とても簡単



Keeperのブラウザ拡張機能を使うと、パスワードや支払情報を保存して様々なウェブフォームに自動入力できます。また、Keeperのボルトに保存されているパスワードも簡単に検索可能です。初めてサイトにログインする時に登録を促すポップアップ画面が表示され、簡単にアカウントのパスワードを保存が可能です。

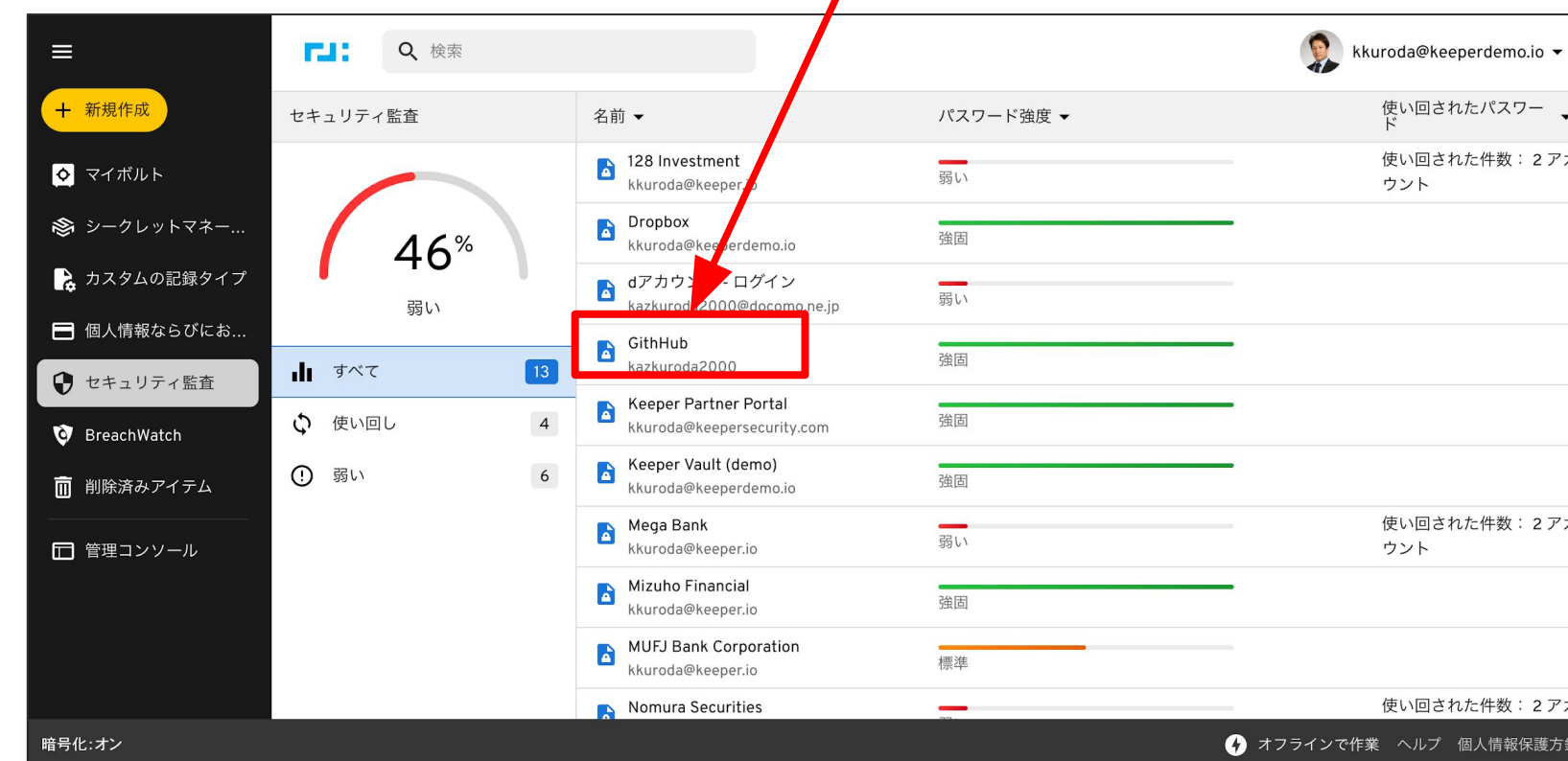
ダークウェブモニタリング (BreachWatch)

BreachWatchはダークウェブ上に流出したパスワードを監視する便利なツールです。



セキュリティ監査

ログイン情報やファイルを他のユーザーと共有



BreachWatchはKeeperアカウントに保存されているログイン情報やパスワードを常にモニタリングし、情報漏洩がないかチェックしてくれます。ダークウェブ上にデータが漏洩していないか確認でき、サイバーセキュリティ対策を全体的にアップします。管理者の方は従業員全体の監視チェックが可能です。

セキュリティ監査画面では、パスワードの強度をモニタリングが可能です。パスワードを使いまわしている・安全ではないパスワードを利用している内容が一目でわかるため、どのパスワードを変更すべきかわかります。

DEMO: 管理コンソール

ダッシュボード・タブ

トピックイベントの確認

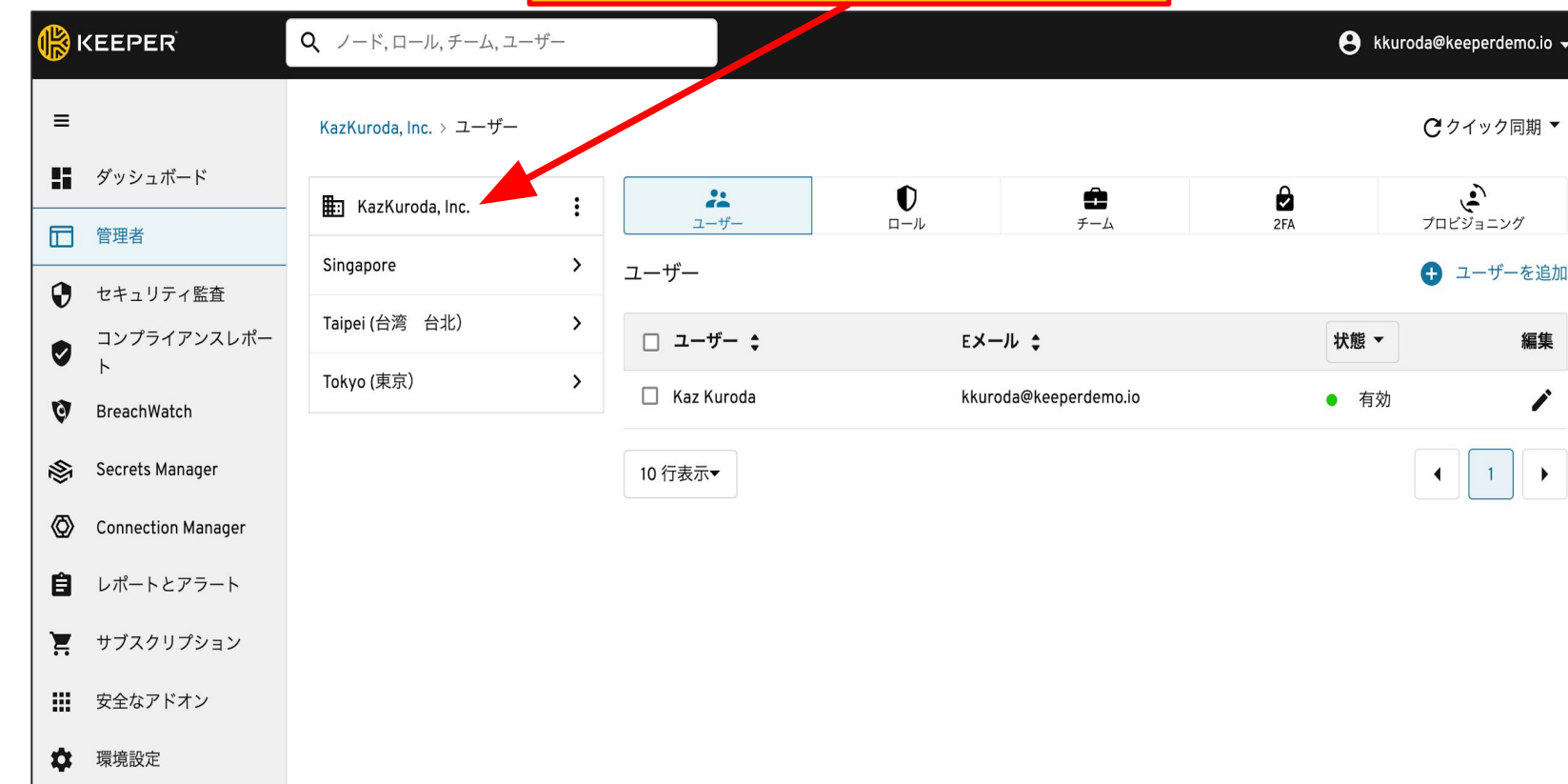


総合セキュリティスコアとダークウェブ上に流出したパスワードの確認

ダッシュボードではトピックイベントの確認ができ、セキュリティ監査ではパスワードの記録から社全体の総合セキュリティスコアの確認ができます。BreachWatch ダークウェブモニタリングをご購入のお客様は全従業員の漏洩パスワードの数値が確認できます。

管理者・タブ

管理者のタブからノードの作成



ノードを作成。このタブでは、ユーザを追加、ロールで強制ポリシーを作成、チームで共有フォルダを作成、二要素認証の設定、プロビジョニングを行えます。

プロビジョニング

プロビジョニング方法を選択



← プロビジョニングメソッドを選択

ノード
KazKuroda, Inc.

- SSO Connect® Cloud を使用したシングルサインオン
SAML 2.0 互換アイデンティティプロバイダを使用して、Keeper ユーザーをプロビジョニングならびに認証できます。Keeper SSO Connect® Cloud は 100% クラウドベースです。新規デバイスの承認は、ユーザーが使用している既存のデバイスから実行するか、Keeper 管理者に実行を依頼してください。
- SSO Connect® On-Prem を使用したシングルサインオン
SAML 2.0 互換アイデンティティプロバイダを使用して、Keeper ユーザーをプロビジョニングならびに認証できます。Keeper SSO Connect® On-Prem を Windows または Linux 環境へインストールする場合、ホストされたサービスが必要になります。新しいデバイスの承認は自動的に処理されます。
- Active Directory か LDAP 同期
Active Directory や LDAP ベースのディレクトリサービスを使用して、ユーザーアカウントをプロビジョニング可能です。Keeper Bridge™ ソフトウェア

キャンセル 次へ

社員数の多い企業様の管理者の方がKeeperのパスワードマネージャを採用した後に一番初めに行って頂くことはプロビジョニングかと思えます。SSO, Active DirectoryやLDAP, SCIM, メールアドレスで自動プロビジョニング、コマンドライン プロビジョニングからご選択いただけます。

ルール

ルールで強制ポリシーを作成。マスターパスワードの複雑さのポリシー設定。



強制ポリシー

ログイン設定

二要素認証

プラットフォーム制限

ポルト機能

記録タイプ

共有&アップロード

KeeperFill

アカウント設定

IP のホワイトリスト化

Keeper Secrets Manager

アカウント移管

マスターパスワードの複雑さ

マスターパスワードの最低必要条件を設定します。

① マスターパスワードの最小の長さは、デフォルトで12です。

最小の長さ 12 0-9 0 !@# 0 A-Z 0 a~z 0

マスターパスワードの有効期限

マスターパスワードの有効期限が切れるまでの日数: 00 日間

SSO ユーザー

SSO でログインするユーザーに、マスターパスワードの作成またはログインを許可します。

生体認証

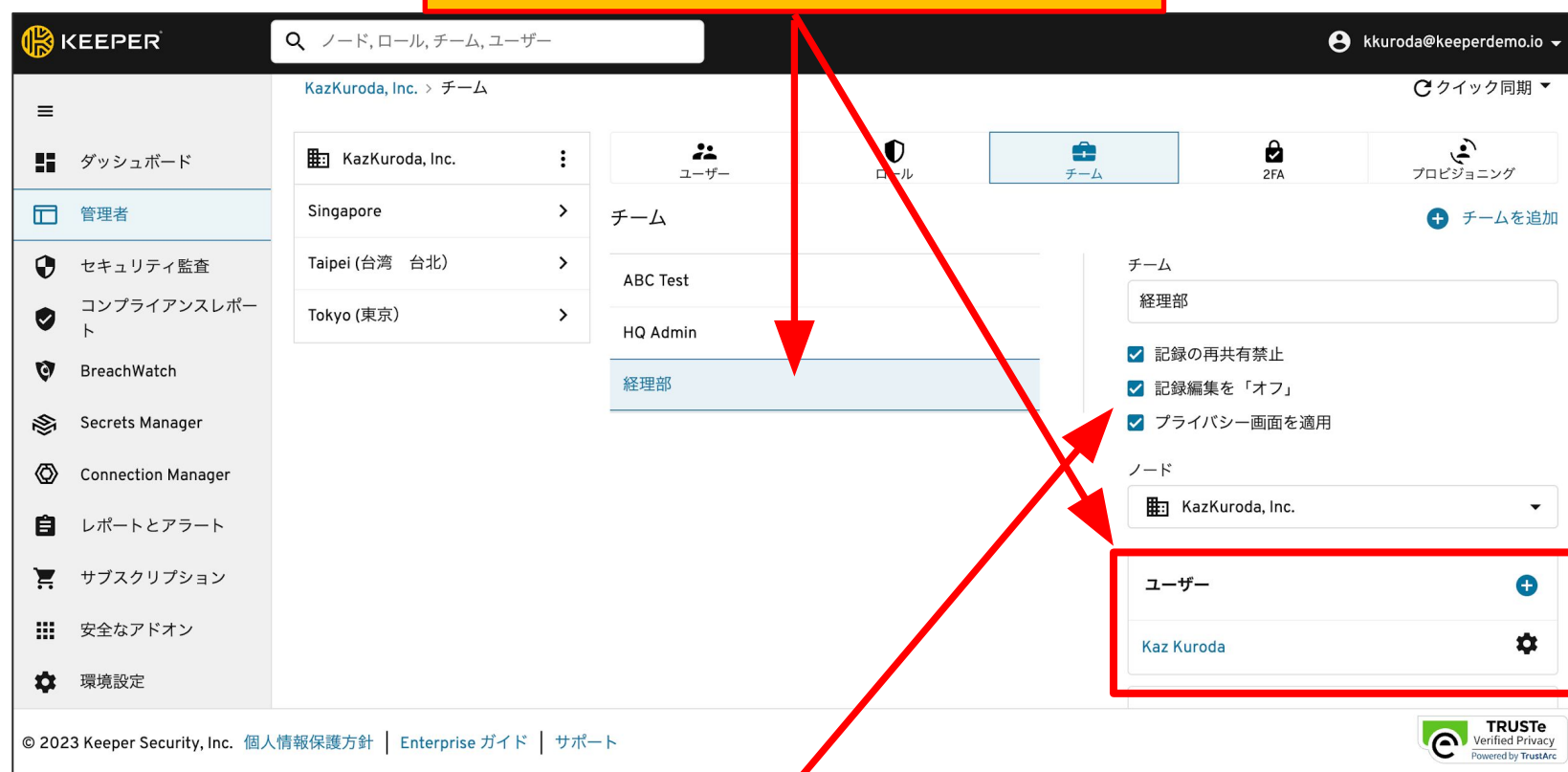
プラットフォーム 許可

完了

ルールで強制ポリシーでは従業員全体に対して、ログイン設定、二要素認証の設定、アクセスできるプラットフォームの制限、共有 & アップロードの許可設定や退社された方々のアカウント移管の同意の設定等ができます。マスターパスワードを全従業員にユーザポルトへの登録をさせることで漏洩の有無が確認できる。その場合、マスターパスワードの有効期限を持たせない運用方法も可能です。

チーム

チームで共有フォルダを作成

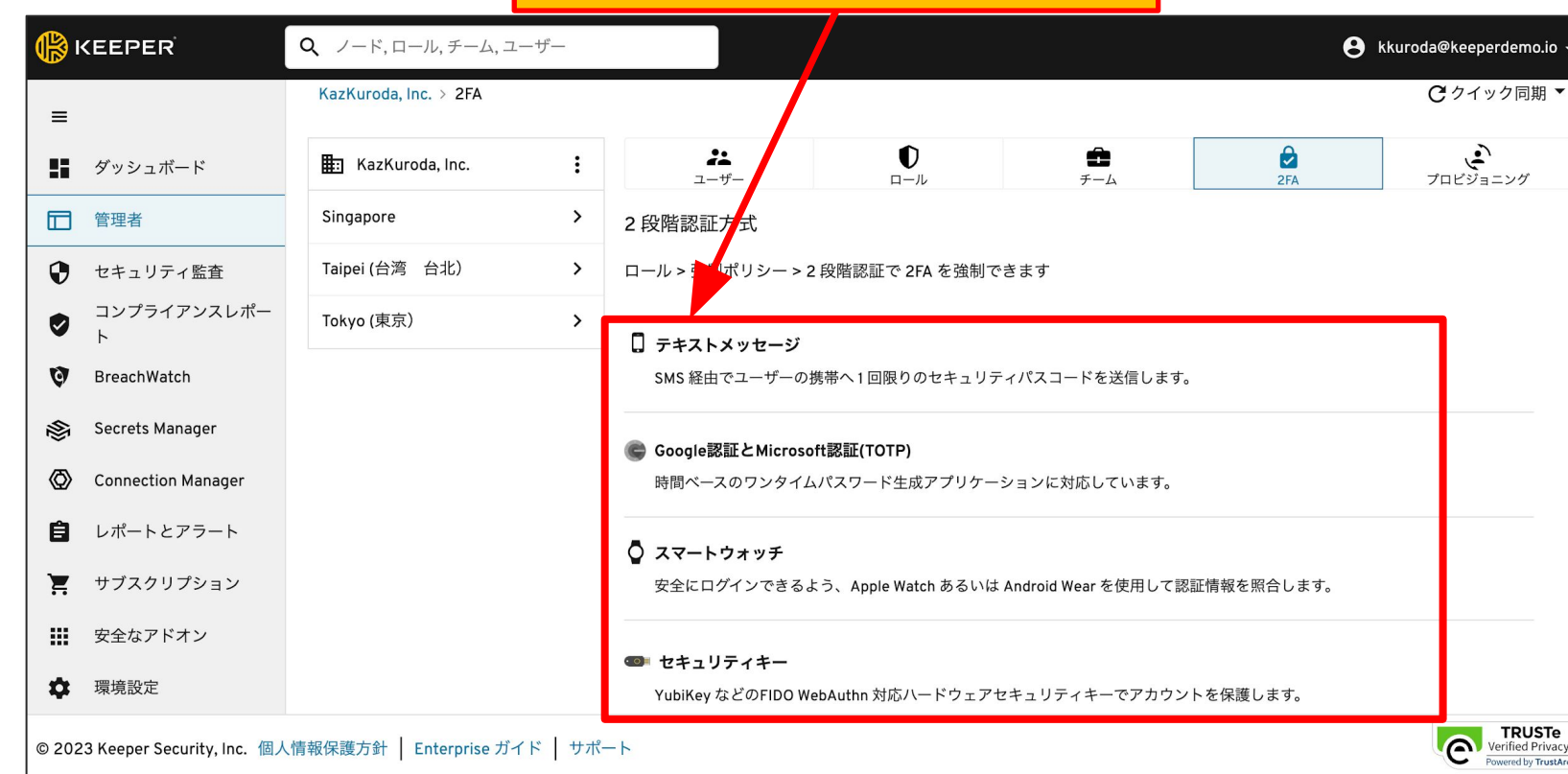


記録の再共有を禁止、記録編集を「オフ」、プライバシー画面を適用可能

チームで作成された共有フォルダを作成することで、共有されたユーザはそのフォルダにアクセスが出来るようになります。もし契約社員や協力会社の方にパスワードを非表示でアクセスさせたい場合は、「プライバシー画面を適用」をクリックをしておくことで、それらのユーザはパスワードを閲覧せずにアクセスをすることが可能となります。

2FA

2段階認証方式



2段階認証方式 (2FA) の説明。2FAの設定方法は、ルール -> 強制ポリシー -> 2段階認証で2FAを設定できます。

セキュリティ監査・タブ

セキュリティ監査スコアを確認、全従業員の「記録パスワード」の強度や、二要素認証が使われているかの確認

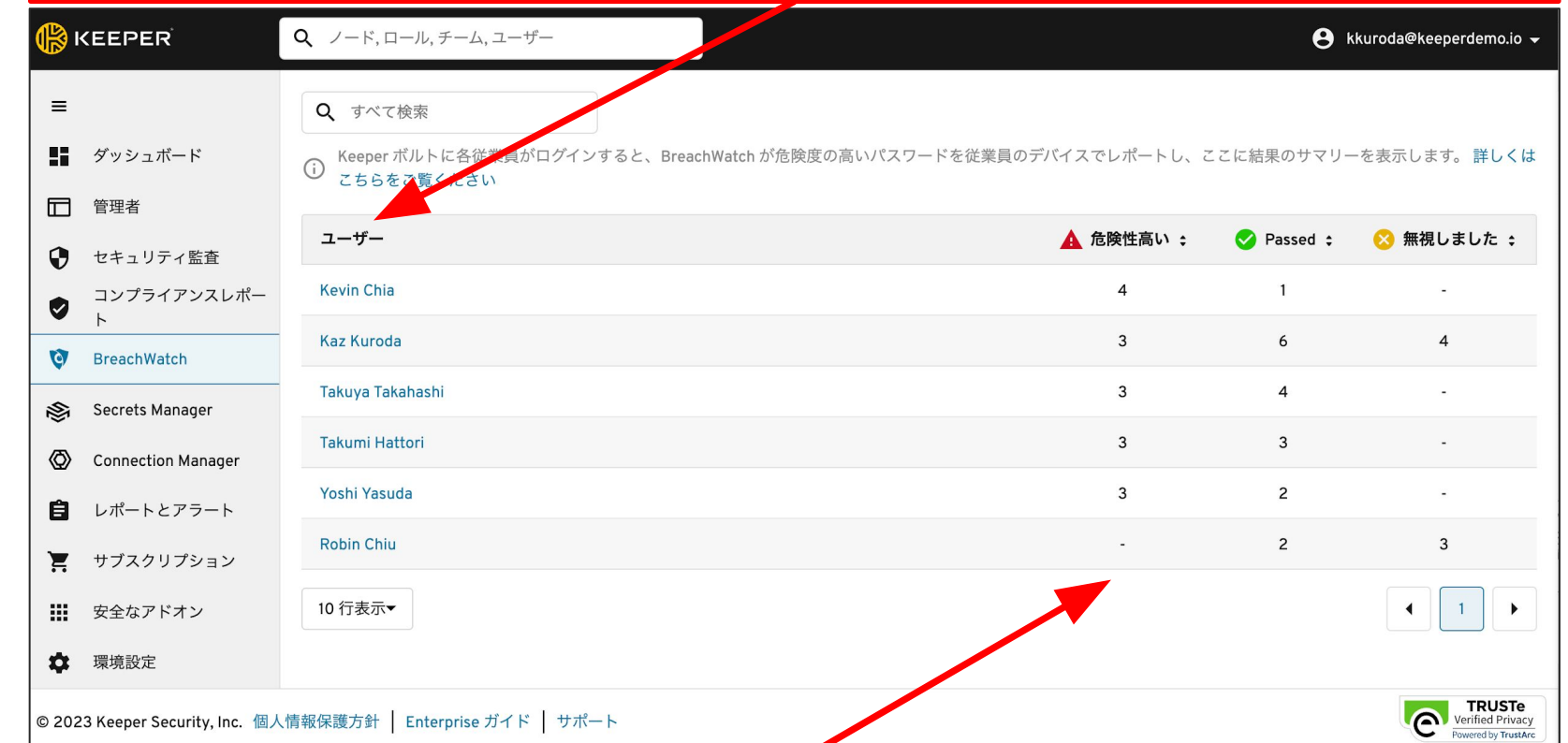


従業員個々のパスワードを「弱い」、「まあまあ」、「強固」の数を表示

セキュリティ監査タブでは、社全体のパスワードのセキュリティ監査スコアを表示。また従業員個々の全てのパスワードの強度を表示。Keeperはゼロ知識を採用しているため、管理者は、従業員がどのアカウントでどのようなパスワードを使っているかまでは確認ができない仕様になっています。

ダークウェブモニタリング (BreachWatch)

BreachWatchではユーザ毎にダークウェブ上に流出したパスワードを使用しているユーザごとに表示できる



ダークウェブ上に流出しているパスワードの数を表示

BreachWatchをご購入頂いた企業様は、管理者が従業員がダークウェブ上に流出したパスワードを使用しているかが確認出来ます。これによって、従業員に対してパスワードの変更を託すことが出来、会社のサイバーセキュリティを向上させることができます。

レポートとアラート・タブ

レポートとアラートタブでは、カスタムレポートとカスタムアラートを作成することができる



KEEPER

ノード, ロール, チーム, ユーザー

kkuroda@keeperdemo.io

レポート アラート 外部ログ

カスタムレポート追加

タイムライングラフ表示

トップイベント: 過去 30 日 (2023/6/4 - 2023/7/4)

記録が開かれました	76
ログインしました	64
コンソールへのログイン	3
記録が入力されました	6
コンソールログインが失敗しました	4

日付

レポート

- Recent Activity 過去 30 日
- All Security Events 過去 30 日


© 2023 Keeper Security, Inc. 個人情報保護方針 | Enterprise ガイド | サポート

TRUSTe Verified Privacy Powered by TrustArc

レポートとアラートタブから、10項目約200種類のレポートとアラートが作成できます。Webhookを利用することで、アラートをTeamsやslackに送信することも可能です。外部ログを設定することで、SIEM連携が出来、SIEM側で確認することもできます。

環境設定・タブ

環境設定では会社のロゴの追加や、招待メールの作成が可能



KEEPER

ノード, ロール, チーム, ユーザー

kkuroda@keeperdemo.io

メール招待状

カスタムメール招待を送信

件名

Keeper パスワードマネージャ 採用のお知らせ Keeper Invitation

メッセージの見出し

Keeper パスワードマネージャの設定のお願い (全社員向け)

メッセージ

弊社はサイバーセキュリティ対策のため、Keeper Securityのパスワードマネージャを採用いたしました。設定方法はこちらをご覧ください。https://docs.keeper.io/user-guides-jp/quick-start-guides/quick-start-guide ご質問等ありましたら、IT部門の黒田 kkuroda@keeperdemo までご連絡ください。 Our organization purchased Keeper, the world's leading password manager and digital vault. Your Keeper admin has invited you to join your organization's account.

アカウント設定ボタン

Button Text

閉じる 保存

© 2023 Keeper Security, Inc. 個人情報保護方針 | Enterprise ガイド | サポート

TRUSTe Verified Privacy Powered by TrustArc

より多くの従業員に心配なく、またなるべく早くKeeperのパスワードマネージャを使用して頂くために、貴社のロゴを追加頂き、また下記の例文等で社員の利用開始を早めることを推奨します。「弊社は社員の方々の効率性を上げることとサイバーセキュリティ対策のため、Keeper Securityのパスワードマネージャを採用いたしました。設定方法はこちらをご覧ください。

https://docs.keeper.io/user-guides-jp/quick-start-guides/quick-start-guide ご質問等ありましたら、IT部門の田中 tanaka@xyz123.com までご連絡ください。」 11



KEEPER®

導入検討スケジュール: 最短約3か月で運用開始

1ヶ月

1ヶ月

1ヶ月

検討開始

トライアル

ご契約

オンボーディング

運用開始

初回MTG

トライアル

ご契約手続き

環境構築

社内展開

✓ 検討可否の決定

- ✓ 懸念点の洗い出し
- ✓ プランの確定
- ✓ ご予算の確認
- ✓ パートナーの選定

- ✓ 稟議のご実施
- ✓ 利用規約のご確認
- ✓ 運用開始までのスケジュールリング

- ✓ プロビジョニング
- ✓ ポリシー設定
- ✓ 社内マニュアル作成
- ✓ 社内運用体制の構築

- ✓ 社内トレーニングの実施
- ✓ 社内マニュアルの配布

- ✓ 会社紹介
- ✓ 製品概要説明
- ✓ デモ実施
- ✓ プラン紹介

- ✓ 懸念点をサポート
- ✓ 概算の提示

- ✓ オーダーの送信 (パートナー経由)
- ✓ オーダー処理
- ✓ 請求書発行手続き (パートナー経由)

- ✓ オンボーディングの実施
- ✓ トレーニングの実施

- ✓ サポートの開始

貴社

弊社

識別

防御

検知

対応

復旧

システム、人、資産、データ、機能に対するサイバーセキュリティリスクの管理に必要な理解を含める

- ・資産管理
- ・脆弱性対策
- ・ガバナンス
- ・セキュリティリスクアセスメント
- ・中長期計画策定
- ・サプライチェーンリスク管理

重要サービスの提供を確実にするための適切な保護対策を検討し、実施する

- ・ID/パスワード管理
- ・アクセス制御
- ・教育およびトレーニング
- ・情報漏えい対策
- ・情報を保護するためのプロセスおよび手順
- ・機器の保守メンテナンス
- ・保護技術の調査と導入

サイバーセキュリティイベントの発生を識別するのに適した対策を検討し、実行する

- ・ログイベントの収集
- ・ログイベントの解析
- ・セキュリティモニタリングの範囲と優先順位策定
- ・継続的なセキュリティモニタリング
- ・検知プロセスの整備

検知されたサイバーセキュリティインシデントに対処するための適切な対策を検討し、実施する

- ・インシデント対応計画の作成
- ・社内コミュニケーション策定
- ・侵害時の拡大防止
- ・侵害時の業務影響把握
- ・インシデント対応手順書整備

レジリエンスを実現するための計画を策定・維持し、サイバーセキュリティインシデントによって阻害されたあらゆる機能やサービスを元に戻すための適切な対策を検討し、実施する

- ・復旧計画の作成
- ・侵害発生後の原因特定
- ・侵害発生後の改善案策定
- ・社外コミュニケーション策定

Thank You