～施設様の「声」で進化し続ける～

インターネット宿泊予約システム 予約番

セキュリティを強化して宿泊施設運営の安全性を高める
～機能と活用方法のご紹介～

株式会社キャディッシュ

フリーダイヤル
0120-489-468

メール
support@489ban.net

作成：2024年08月30日

© 2024 Cadish Inc.

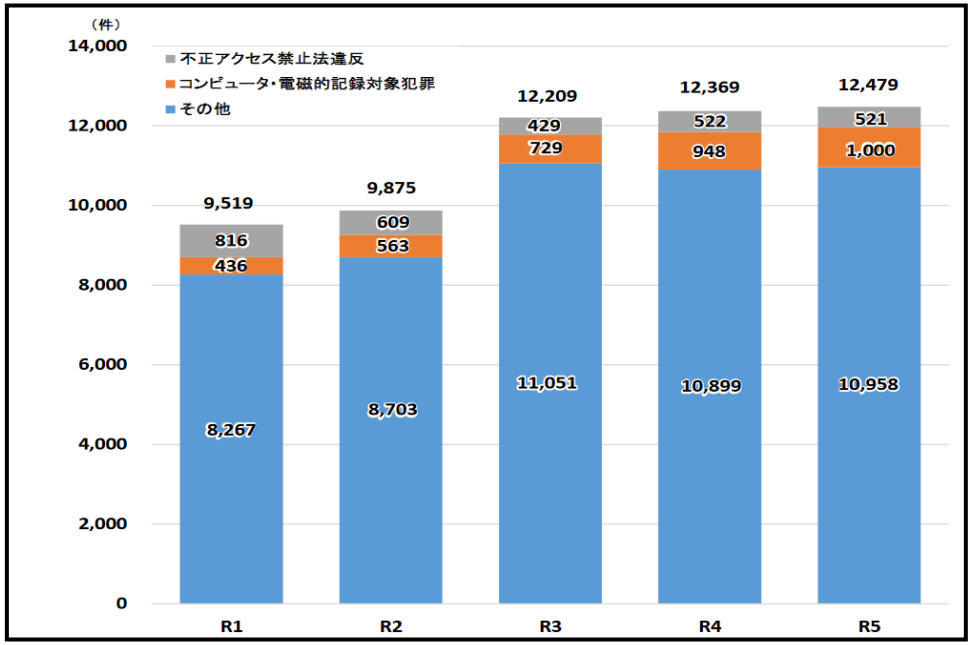
1. 情報セキュリティの脅威

現状

近年、サイバー犯罪が増加しており被害を受ける可能性が高まっています

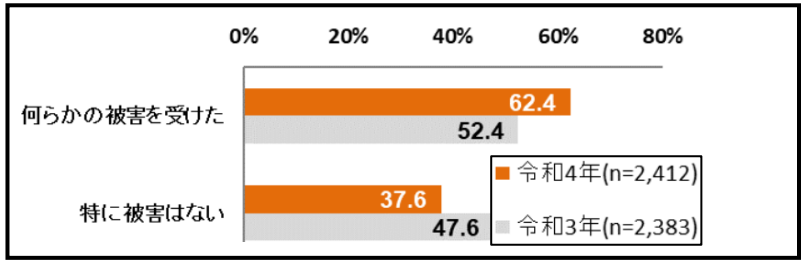
「サイバー犯罪」はコンピューターやネットワークに接続されたデバイスを標的とした、不正アクセスや破壊行為などの犯罪行為の総称です。

・国内でのサイバー犯罪の検挙件数は令和5年（2023年）が過去最多12,479件で直近5年間で約24%増加しています。



出典：警察庁「令和５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」
３ サイバー犯罪の検挙状況 (1) サイバー犯罪の検挙件数の推移
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R5/R05_cyber_jousei.pdf

・企業においても「何らかの被害を受けた」という回答は6割以上あり、1年間で10%増加しています。



※過去１年間の情報通信ネットワークの利用の際に発生したセキュリティ被害をみると、「何らかの被害を受けた」企業が 62.4%となり、10.0 ポイント上昇している。
被害内容は、「標的型メールの送付」が 44.4%と最も高く、次いで「ウイルスを発見又は感染」（32.6%）となっている。

出典：総務省「令和4年通信利用動向調査の結果」
（3）情報通信ネットワークに対するセキュリティ被害と対応の状況（企業）
https://www.soumu.go.jp/johotsusintokei/statistics/data/230529_1.pdf

© 2024 Cadish Inc.

1. 情報セキュリティの脅威

2023年セキュリティ事故の事例

■組織の規模や業種は関係無し！次の標的はあなたの組織かも？

事例①：ランサムウェア感染による業務停止

- 2023年7月、A港のターミナルシステムが**ランサムウェアに感染した**。
- **リモート接続機器の脆弱性を悪用**した不正アクセスが原因であった。
- **物理サーバー基盤および全仮想サーバーが暗号化されている**ことが判明した。
- **約2日半**、ターミナルでの**作業が停止**となった。

※ランサムウェアとは、感染するとパソコン等に保存されているデータを暗号化して使用できない状態にした上で、そのデータを復号する対価（金銭や暗号資産）を要求する不正プログラムです。

■委託先に付与しているシステムのアクセス権限は適切ですか？管理できていますか？

事例②：委託先のシステムを介して不正アクセスされ、顧客情報が漏えい

- 2023年11月、A社は同社の保有する**顧客情報が漏えい**したことを公表。
- ユーザーに関する情報が約30万件、取引先等に関する情報が約9万件、従業員等に関する情報が約5万件漏えい。
- **第三者による社内システムへの不正アクセス**が原因。
- 委託先企業であるB社のさらに委託先の企業で従業員のパソコンが**ウイルス感染**したことが発端。

■不要になった情報システムの認証情報が放置されていませんか？

事例③：元勤務先に不正アクセスして社内情報を削除

- 2023年1月、C社の元従業員が**不正アクセス禁止法違反および電子計算機損壊等業務妨害**の疑いで警視庁に逮捕された。
- 本従業員は退職後に、元同僚や元上司の**IDやパスワードを悪用**し、社内ネットワークやクラウドに**不正アクセスして**、人事や技術、顧客に関する**情報を削除**していた。
- **人間関係を理由に退職**しており、**嫌がらせが目的**とみられている。
- データ復旧には**約660万円**を要した。

■メール送信前に顧客情報と宛先を十分確認していますか？

事例④：意図しないメールアドレスに個人情報を送信

- 2023年2月、A大学はメーリングリスト内のメールアドレスの**誤記**により、**意図しない宛先**へ学内外829名の**個人情報を送信**してしまったことを公表した。
- 本来、「**@gmail**.com」とすべきドメインを「**@gmai**.com」としたメールアドレスをメーリングリストに**誤登録**してしまったことにより、個人情報が記載されたメールが本来の宛先ではなく、**実在する別のメールアドレス（gmai.com）**に送られてしまった。

出典：「独立行政法人 情報処理推進機構（IPA）　情報セキュリティ10大脅威 2024」を基に作成
https://www.ipa.go.jp/security/10threats/m42obm00000044ba-att/setsumei_2024_soshiki.pdf

© 2024 Cadish Inc.

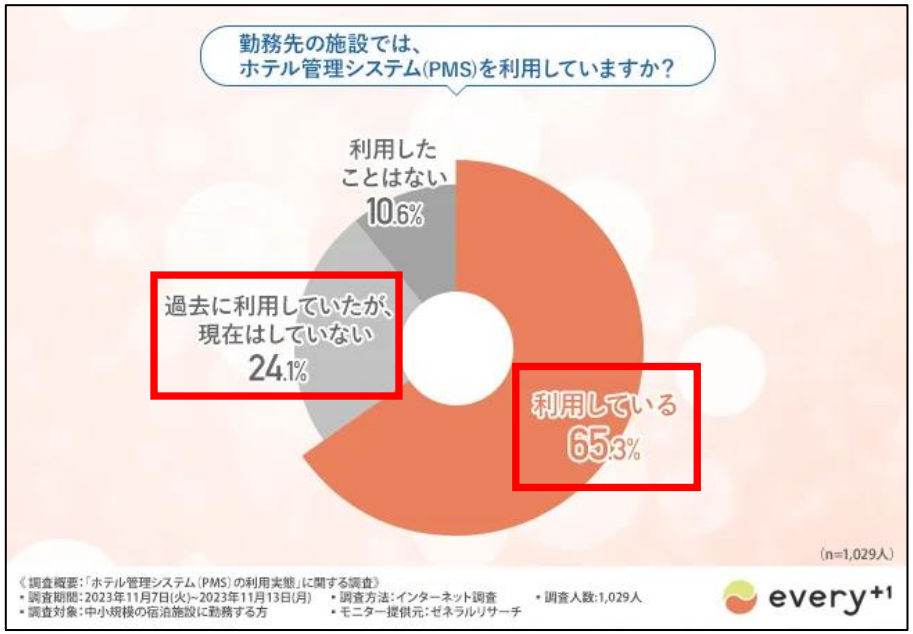
2.宿泊業界における情報漏えいのリスクと要因

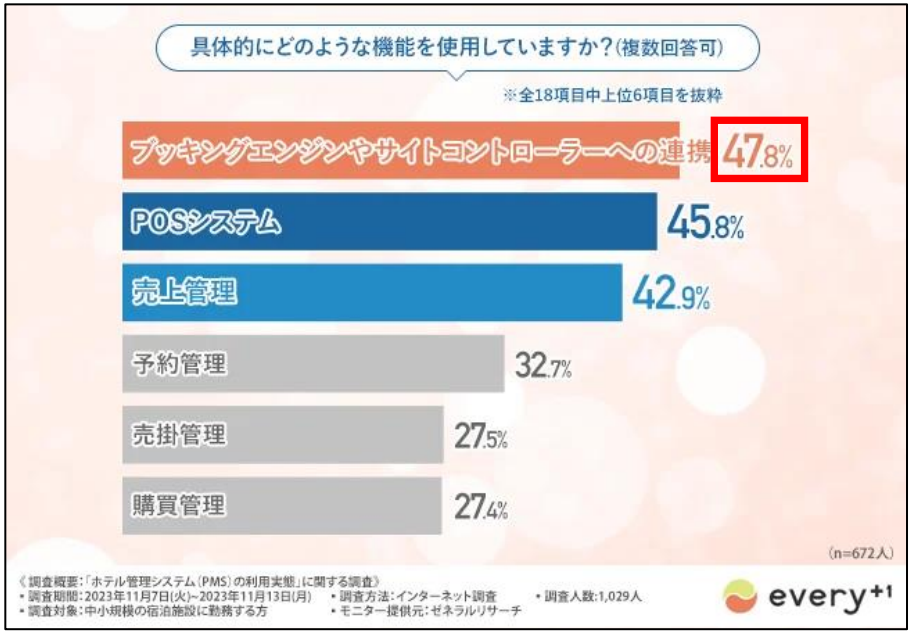
宿泊業界の事例

宿泊施設が利用する「管理システム」に大量に保存されている顧客情報が狙われています。

宿泊施設では「ホテル管理システム（PMS）」「ブッキングエンジン」「サイトコントローラー」などのシステムの導入が進み、大量の予約者情報や会員情報を蓄積して管理できるようになりました。

・ホテル管理システムを利用したことがある宿泊施設は約90%、そのうち約48%がブッキングエンジン等への連携を利用。





出典：「ゼネラルリサーチ調査」「GRIT株式会社（https://www.grit1.jp）」

利便性が向上した一方で、利用しているシステムの管理状況によっては顧客情報の「漏えい」や「悪用」などのリスクがあります。
実際に認証情報を窃取する事案や、不正ログインによりシステムで管理している顧客情報を悪用された事件が発生しています。

事例

警察庁が犯罪者が利用客を装い「アレルギー」について記載したメールをホテルへ送信した事案を告知しました。

出典：警察庁ウェブサイト（https://www.npa.go.jp/bureau/cyber/pdf/Vol.29cpal.pdf）

観光庁が海外の予約サイトにおけるフィッシング被害について注意喚起を行いました。

出典：観光庁ウェブサイト（https://www.mlit.go.jp/kankocho/page06_000354.html）

© 2024 Cadish Inc.

2.宿泊業界における情報漏えいのリスクと要因

管理画面を不正利用されるリスクと影響

「予約番」においても、例えばウイルス感染などによって管理画面の認証情報（アカウントとパスワード）が漏えいした場合、第三者にログインされ個人情報を不正に利用される可能性があります。

（例）ウイルスによる管理画面の不正利用

“施設担当者様
私のアレルギーをまとめた
ファイルを添付します…“

【攻撃者】

①ウイルスを仕込んだ添付ファイルを関係者や顧客に装ってメール送信

【施設】

②添付ファイルを開いたことで管理画面の認証情報を保存しているパソコンがウイルスに感染

③施設の重要情報や認証情報を窃取

情報漏えい

⑥事故対応
・調査、謝罪、補填、再発防止への投資…
・ブランドイメージ低下、信用喪失…

④窃取した認証情報で管理画面にログイン

⑤認証成功
&
不正操作

●予約者や会員情報の窃取
・予約状況リスト、会員一覧
-氏名
-住所
-電話番号
-メールアドレス等…

被害拡大

●管理者になりすまして予約者へメール送信
・メール送信機能の悪用
-宿泊料金などの支払い要求
-クレジットカード情報の要求
-偽サイトへの誘導

●設定変更や削除 etc...

管理画面の認証情報を第三者に不正に取得／利用された場合、被害者への対応や補償はもちろん、社会的な信用の低下など、今後の業務運営に支障が生じてしまう可能性があります。

© 2024 Cadish Inc.

2.宿泊業界における情報漏えいのリスクと要因

管理画面の不正利用を引き起こす要因とは？

「ウイルス感染」以外にも、例えば以下のような事態や状況により管理画面の認証情報（アカウントとパスワード）が第三者に漏えいしてしまう可能性があります。

認証情報 漏えいの原因	概要
ウイルス感染	管理画面を利用しているパソコンがウイルスに感染することにより認証情報が第三者に漏えいし、外部から不正利用されてしまう。 ※実際、感染時にパソコンのブラウザに保存されている各種サービスの認証情報を不正取得して外部に漏えいさせるウイルスは数多く実在します。
担当者の退職	管理担当者の退職時に認証情報を変更していないため、退職後に管理画面を不正利用されてしまう。
委託先との契約解消	コンサルや業務委託などの契約解除時に認証情報を変更していないため、契約解除後に管理画面を不正利用されてしまう。
誤送信	情報共有のミスやメール誤送信などにより、第三者に認証情報が漏えいし、不正利用されてしまう。
認証情報の管理不足	認証情報を管理していないため、現在、管理画面にアクセスできる担当者や人数を正確に把握できていない。
情報資産の管理不足	社内／社外を問わず、適切に管理やセキュリティ更新が行われているかわからない自宅のパソコンや、私物のスマホ／タブレットなどで、認められていない管理画面操作をする担当者がいる可能性がある。

どんなに気を付けていても認証情報の「漏えい」リスクはゼロにはなりません。
ただし「予約番」管理画面が有する「セキュリティ強化対策」でリスクを低減できます。

© 2024 Cadish Inc.

3.「予約番」のセキュリティ強化対策

①-1.「2段階認証」で不正アクセス防止などに効果を発揮できます

従来の認証情報に加え、正規の管理者のみに通知される「ワンタイムパスワード」で認証する方式です。
管理画面ログイン時の本人確認を2回に分けて行うことで、セキュリティを高め、不正アクセス防止などに効果を発揮します。

	従来の認証方式	2段階認証方式
認証要素	「アカウント」と「パスワード」 	「アカウント」と「パスワード」  ＋ **ワンタイムパスワード** 
補足	第三者に認証情報が漏えいした場合に管理画面の全機能を悪用される可能性があります。	管理画面にログインするためには従来の認証方式に加え「ワンタイムパスワード」での認証が必要です。 「ワンタイムパスワード」は一定時間ごとに自動的に変化するため、認証情報の漏えいなどによる不正アクセス防止に有効です。 **※「ワンタイムパスワード」を正規の管理者に通知する方法を「メール」または「アプリ」からお選びいただけますので運用に応じてご選択ください。**

© 2024 Cadish Inc.

3.「予約番」のセキュリティ強化対策

①-2.「2段階認証」で不正アクセス防止などに効果を発揮できます

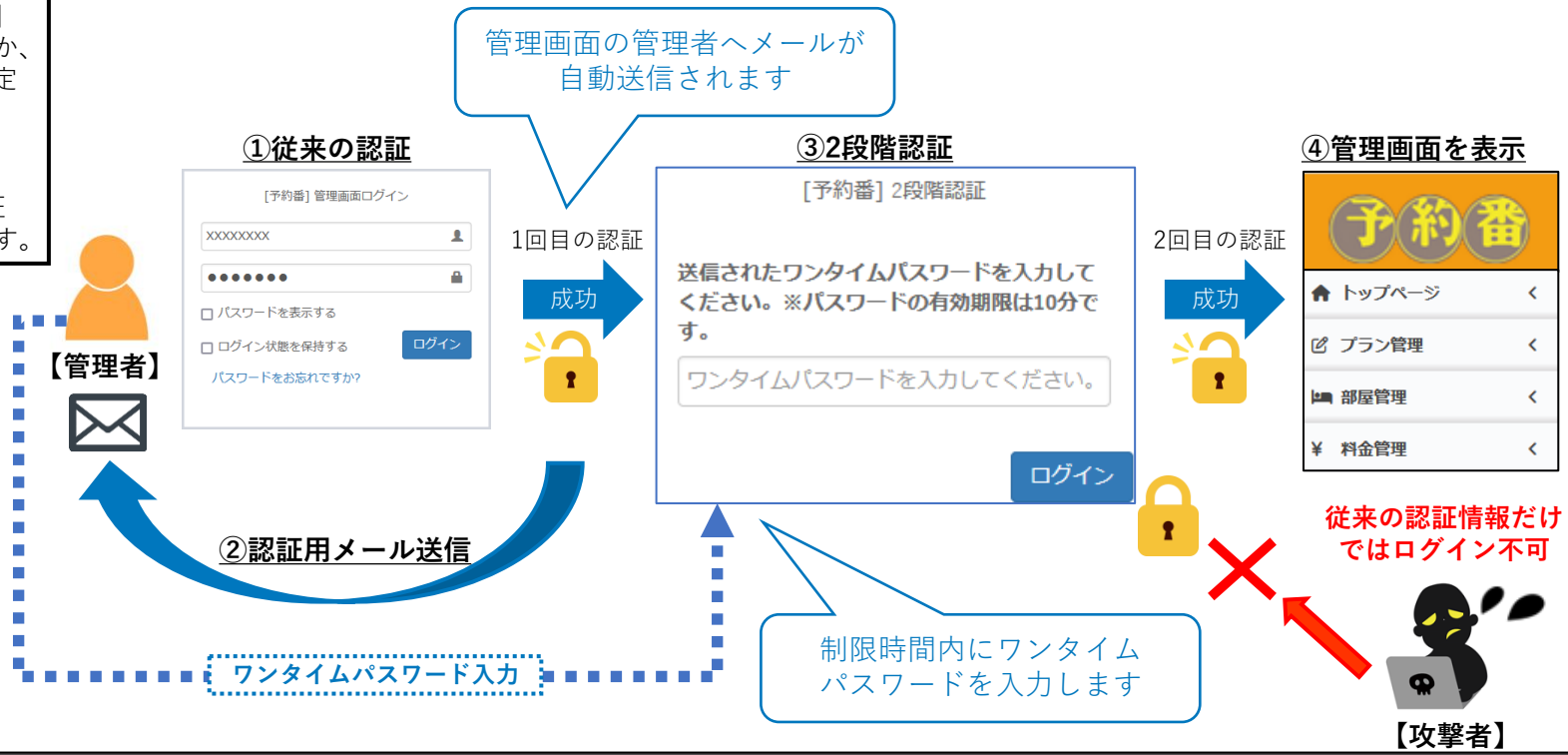
■「メール」を用いておこなう2段階認証

概要

予め指定したメールアドレスに通知される「ワンタイムパスワード」で認証をおこないます。
「ワンタイムパスワード」は認証の度に変化するほか、有効期限があるため、一定時間経過後の利用を「無効」にできます。

※アプリによる2段階認証よりも手軽に利用できます。

◆「メール」を用いた2段階認証の流れ
①従来の認証情報（アカウントとパスワード）でログインします。
②ログインと同時に管理者へ「ワンタイムパスワード」が記載されたメールが届きます。
③メールに記載された「ワンタイムパスワード」を入力しログインします。
④管理画面を表示します。



「メールを用いた2段階認証」設定方法

・管理画面「アカウント管理」＞「アカウント設定」＞ ワンタイムパスワードの送信先となる「メールアドレス」の確認または変更。
・「2段階認証」＞「メール認証」を選択＞「ワンタイムパスワードメールを送信する」 ＞ メールで受信したワンタイムパスワードを入力して「変更する」。

© 2024 Cadish Inc.

3.「予約番」のセキュリティ強化対策

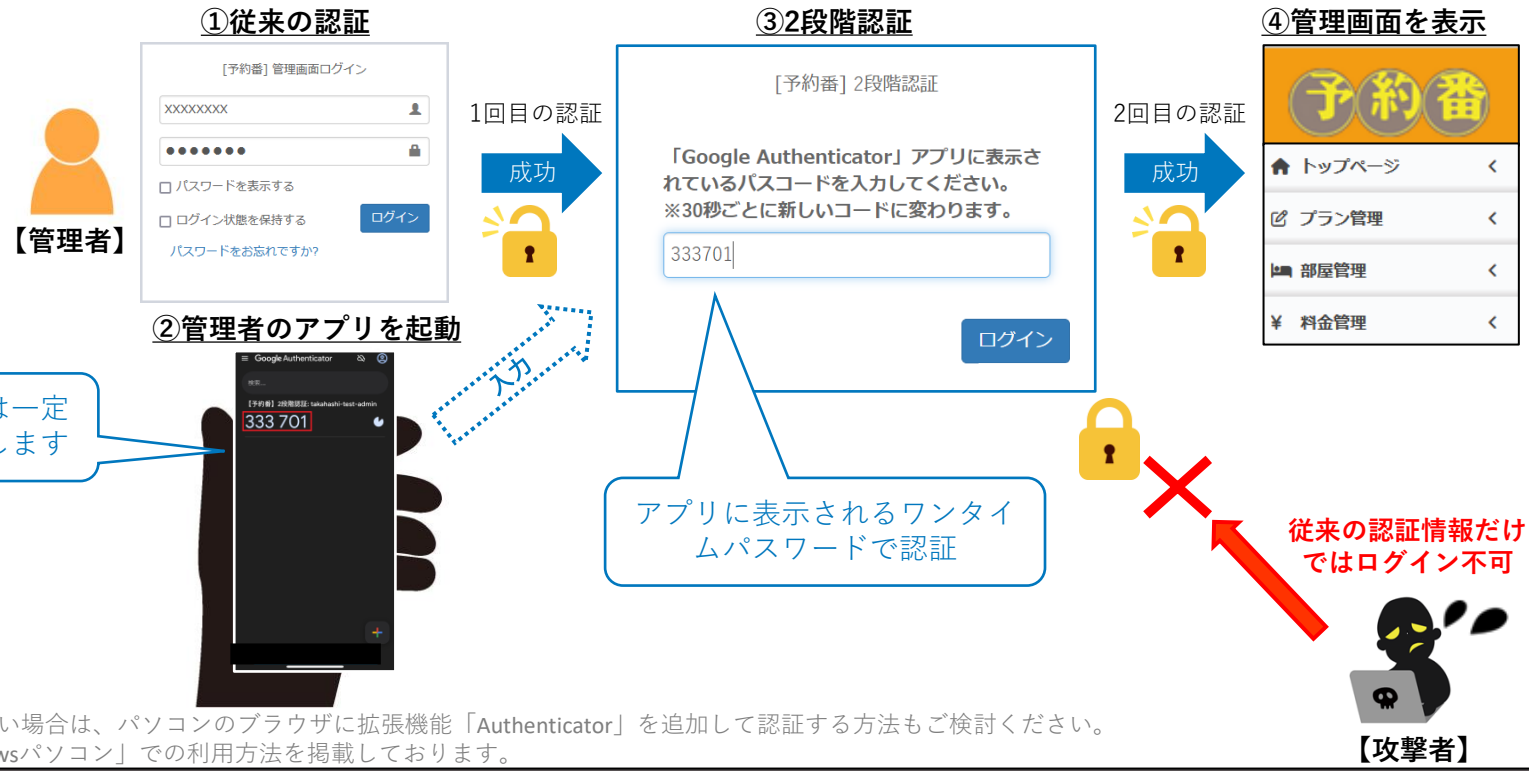
①-3.「2段階認証」で不正アクセス防止などに効果を発揮できます

■「アプリ」を用いておこなう2段階認証

概要

Googleが提供する2段階認証用のアプリ（Google Authenticator）を利用して2回目の認証をおこないます。
※管理者が利用する端末（スマートフォンなど）にアプリをダウンロードする必要があります。
ダウンロード用のQRコードは管理画面に掲載しております。

◆「アプリ」を用いた2段階認証の流れ
①従来の認証情報（アカウントとパスワード）でログインします。
②管理者のアプリ（Google Authenticator）を起動します。
③アプリ内に表示される「ワンタイムパスワード（パスコード）」を入力しログインします。
④管理画面を表示します。



※スマートフォンなどの端末が無い場合は、パソコンのブラウザに拡張機能「Authenticator」を追加して認証する方法もご検討ください。
管理画面上部「Q&A」に「Windowsパソコン」での利用方法を掲載しております。

「アプリを用いた2段階認証」設定方法

管理画面「アカウント管理」＞「アカウント設定」＞「2段階認証」＞「Google Authenticator」を選択 ＞ 「表示されたQRコードをアプリでスキャン」＞スキャン後、「Google Authenticator」アプリに表示された「ワンタイムパスワード」を入力し「変更する」。

© 2024 Cadish Inc.

3.「予約番」のセキュリティ強化対策

②信頼できるネットワークや管理者によるログインのみ許可してセキュリティを強化できます

■管理画面へのログインを特定のIPアドレスからのみ許可する「IPアドレス制限」

「IPアドレス制限」概要

インターネットに接続している事業所や、業務を委託している会社などには、それぞれ一意の「インターネット上の住所（**IPアドレス**）」が割り振られています。
予め指定した「IPアドレス」からのみ管理画面へのログインを許可することで、第三者からの不正なログインを拒否できます。

※前述の「2段階認証」との併用で更にセキュリティが高まります。

【管理画面へのログインを制限する仕組み】
①認証情報（アカウントとパスワード）でログインします。
②管理画面にログインする人（デバイス）のIPアドレスをチェックします。
③ IPアドレスの許可リストにあるIPアドレスからのみ接続を許可します。
④管理画面を表示します。

予め作成した「許可リスト」を基に接続を制限できます

※( )内はIPアドレスの例です。

「IPアドレス制限」の利用方法

管理画面上部「Q&A」＞「予約番を安全に利用するためには 」＞「管理画面にアクセスできるIPアドレスを制限する方法 」をご確認ください。
※IPアドレス制限を利用するためには弊社宛にメールで「利用希望」のご連絡が必要です。

© 2024 Cadish Inc.

3.「予約番」のセキュリティ強化対策

③特定の役割に基づく最小限の管理権限を付与することでリスクを低減できます

■管理画面の「サブアカウント」を作成して操作の権限を設定できる「アカウント管理」

「アカウント管理」概要

管理画面の「サブアカウント」を複数作成できます。
さらに、権限を設定できるためログイン後の操作を業務の役割に応じて制限できます。
例えば、通常のアカウントを施設（本社）が管理し、事業所の担当者や業務を委託する会社にサブアカウントを作成して提供できます。

・担当者の役割や権限に応じて、管理画面で実施できる操作を制限したい…
・1つの管理画面を複数人で利用しており、誰が設定したのか不明な時がある…

「アカウント管理」の活用方法（例）

・管理画面の設定状況と予約状況のみ確認する担当者 → **管理画面の編集不可**
・プランやデザインの設定業務を委託している業者 → **予約者情報や会員情報の閲覧不可**

施設（本社）

アカウント：sample-admin

アカウントごとにパスワードと2段階認証を設定できます

役割に応じたアカウントを提供し操作も制限できます

権限は7項目あり管理者の役割に応じて設定できます

※「権限なし」の場合は画面に警告を表示し操作を受け付けません。

管理画面ログイン用のサブアカウントを作成	事業所の担当者 **サブアカウント：sample-staff**	業務委託会社 **サブアカウント：sample-vendor**

※「サブアカウント」は通常アカウントの「admin」の部分を任意の文字列に変更して作成します。

権限設定（例）		
プランの設定	参照のみ	全て許可
デザイン設定	参照のみ	編集可能
予約情報・レポート	参照のみ	権限なし
顧客管理	参照のみ	権限なし

「アカウント管理」の利用方法

管理画面「アカウント管理」＞「一覧」＞「新規作成」＞「アカウント／メールアドレス／パスワード」「権限設定」を入力し「アカウントを登録する」。
※サブアカウントにも「2段階認証」の設定をおすすめします。（作成したサブアカウントにログイン後、「アカウント管理」から設定できます。）

© 2024 Cadish Inc.

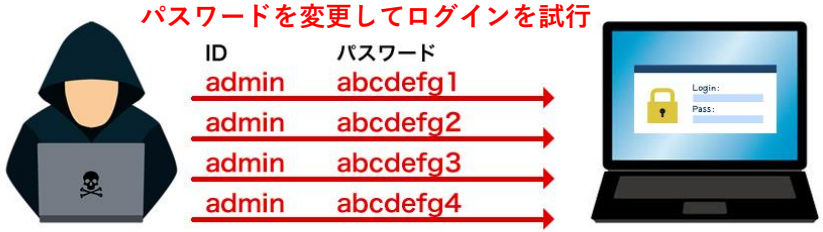
3.「予約番」のセキュリティ強化対策

④総当たりでログインを試行する攻撃から管理画面へのログインを防ぎます

■ログインの試行が一定回数を超えると1分間アカウントをロック

第三者が認証情報のアカウント（ID）を知っている場合、考えられるパスワードを全て試す形で不正にログインを試みるサイバー攻撃があります。
例えば「アルファベット」と「数字」の組み合わせであることがわかっていた場合、その文字の組み合わせを全て試して、
強引にログインしようとするものです。（多くの場合、プログラムされたコンピューターが試行している場合がほとんどです。）

パスワードを変更してログインを試行



パスワードの桁数が短いほど当然、ログインの成功率は高くなります

出典：サイバーセキュリティ.com「ブルートフォースアタック（総当たり攻撃）とは？そのやり方・実際にかかる時間・対策方法は？」
https://cybersecurity-jp.com/column/17426

「アカウントロック」概要

予約番のログイン認証で、一定回数失敗すると1分間アカウントをロックします。
ロック中は正しいパスワードを入力してもログインを受け付けません。
※ロックが解除されると正しい認証情報でログインできるようになります。

連続したログインの試行を抑止できます

一定回数
ログインを試行

失敗

※会員機能をご利用の場合は、会員ログイン画面でも「アカウントロック」が適用されます。

**上記のようにアカウントロック機能は備えていますが、基本行動として推測されにくい複雑なパスワードの設定をお願いします。
もちろん、「2段階認証」を併用していただくことで管理画面への不正ログインのリスクを大幅に低減できます。**

© 2024 Cadish Inc.

4.セキュリティに関するQ&A

Q 「予約番」に限らず、安全に情報システムを利用するために普段から気を付けた方が良いことはありますか？

A 基本的に有効と考えられているセキュリティ対策をピックアップしてご紹介します。

01 定期的なアップデート

OSやブラウザ、セキュリティ対策ソフト、アプリ等を常に最新に維持する。

アップデートには、機能改善のほか、セキュリティ上の問題点（脆弱性）の修正なども含まれております。
アップデートを放置すると、不具合が起きたり、ウイルスや不正アクセスの被害を受けたりする可能性が高まります。

※「予約番」管理画面へのアクセスに、数年前のかなり古いバージョンのブラウザをご利用になられている方も実際にいらっしゃいます。
セキュリティリスクがあることはもちろん、「予約番」管理画面の正常動作も保証いたしかねますので早急にアップデートをお願いします。

02 ウイルス対策ソフトの導入

ウイルス対策ソフトは、目視での判断が難しい危険なサイトや怪しいメールなどからパソコンやユーザーを保護してくれます。
インターネットの接続をリアルタイムで監視し、ウイルス等の脅威の検出や排除をおこなってくれるソフトウェアです。

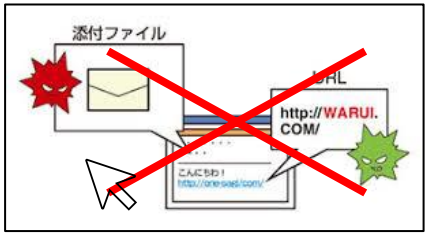
© 2024 Cadish Inc.

4.セキュリティに関するQ&A

03 パスワードの適切な運用

・**複数のサービスで同じパスワードを利用しない。（他のサービスで利用しているパスワードを予約番で利用しない。）**
※1つのサービスでパスワードが漏えいすると、他のサービスでも不正利用されて被害が拡大するリスクがあります。
・**長期間同じパスワードを利用しない。**
※例えば、操作権限がある方の退職や異動が生じた場合はパスワードを変更する。
・**推測されにくいパスワードを設定する。**
※パスワードは「大文字と小文字のアルファベット、数字、記号を含む10桁以上」が推奨されています。
複雑なパスワードは「考えられるパスワードを全て入力しログインを試行するサイバー攻撃（P.11）」への対策に効果的です。

04 不審なメールへの注意



・**不審なメールを開封しない。**
・**不審なメールの画像をクリックやタップしない。**
※一見、画像であってもリンクになっていて、偽りのWebサイトが開くおそれがあるので注意します。
・**不審なメールに添付されているファイルを開かない。**

※受信者が過去にメールをやりとりしたことのある名前、メールアドレス、本文の一部を流用し、あたかもその相手からの返信メールであるかのように見せて、添付ファイル（ウイルス）を送り付けてくる事例もあります。

05 その他の対策

・**定期的に社内セキュリティ教育や情報システム運用状況の点検を行う。**
・**操作権限がある方を常に明確にして限定する。**
・**役割に応じて、必要な権限のみを与えた認証情報（アカウント）を利用させる。**
※（P.10）管理画面の「サブアカウント」を作成して操作の権限を設定できる「アカウント管理」をご活用ください。
・**操作の必要がない時は不要なサービスからログアウトしておく。**

【参考】警察庁ウェブサイト「日頃からの備え」 出典：警察庁ウェブサイト（https://www.npa.go.jp/bureau/cyber/pdf/Vol.29cpal.pdf）
・**業務用端末と個人端末を混同しない。（環境を混ぜない。）**
※個人端末（私物）はアップデート状況や、管理状況が個人に任されており危険であるため業務に利用させるべきではありません。
・**アカウントやパスワードをブラウザに保存しない。**
※ブラウザに保存することでログインなどの手間は省けますが、権限のない方に意図せず利用されるほか、ウイルス感染時に盗まれるといったリスクを伴います。

© 2024 Cadish Inc.

【補足事項】予約番「Q&A」ページと参考サイトのご案内

■予約番「Q&A」ページ

管理画面の上部「Q&A」に「予約番のセキュリティ対策」でご紹介した機能の詳しい設定方法などを掲載しております。

「Q&A」ページのQRコード

▼「予約番」を安全に利用するためには

https://489ban.tayori.com/q/reserve/category/99619/

※下記のQ&Aを掲載しております。

- セキュリティを高め管理画面の認証情報を適切に管理する重要性
- 管理画面のログイン時に「2段階認証（ワンタイムパスワードによる追加認証）」を利用したい
- 管理画面ログイン時の「2段階認証（ワンタイムパスワードによる追加認証）」をメールでおこないたい
- 管理画面にアクセスできるIPアドレスを制限する方法
- Windowsパソコンでの2段階認証(Google Authenticator)利用方法
- 管理画面の認証情報を再設定すべきタイミング
- 2段階認証(Google Authenticator)でログインできなくなった場合の対応方法

■参考サイト

政府や独立行政法人情報処理推進機構（IPA）は、企業に対してセキュリティの啓発活動をおこなっております。

下記のサイトをご案内いたしますので施設様の「セキュリティ体制の構築」や「社内のセキュリティ教育」を検討される際にお役立てください。

▼新5分でできる！情報セキュリティ自社診断（ダウンロード版）　※独立行政法人 情報処理推進機構（IPA）

https://www.ipa.go.jp/security/sme/f55m8k0000001waj-att/000055848.pdf

▼情報セキュリティ対策チェックリスト（宿泊施設用）　※国土交通省総合政策局　情報政策課サイバーセキュリティ対策室

https://www.mlit.go.jp/common/001401614.pdf

▼インターネットの安全・安心ハンドブック　※内閣サイバーセキュリティセンター（NISC）

https://security-portal.nisc.go.jp/guidance/handbook.html

© 2024 Cadish Inc.

【お知らせ】過去にご紹介した予約番の機能と活用方法

「予約番」は施設様からのご要望やご意見を取り入れ、日々改善をおこなっております。
改善した機能を知っていただき、ご活用いただくことで「お手間軽減」「売上向上」など少しでも施設様のお役にたてるのではないかと考えております。

今回ご案内しました「予約番の機能と活用方法」は、過去にも違うテーマでお知らせをしております。
管理画面の上部「活用方法」からいつでもご覧いただけますので「ご存知ない機能」や「利用していない機能」がございましたら是非活用をご検討ください。

■「活用方法」ページ
https://489ban.tayori.com/q/dispatch-news

「活用方法」ページのQRコード

※過去の「予約番の機能と活用方法」のテーマ

・**リピート予約を促す「会員プロモーション」**（2023年11月）
獲得した会員（リピーター）の満足度を高め、再訪のきっかけをつくるうえで役立つ機能と具体的な活用事例を紹介しています。

・**自社の予約を後押しする「クーポン機能」**（2023年3月）
プランの「販売促進」や割引計算などの「手間削減」が期待できる「クーポン」の機能と具体的な活用事例を紹介しています。

・**プランの販売強化・手間削減**（2022年9月）
お客様の「満足度向上」や施設様の「販売管理の手間削減」が期待できる機能と具体的な活用事例を紹介しています。

・**キャンセル・ノーショウ対策**（2022年4月）
キャンセル料の「徴収漏れ」や「販売機会損失」への対策など、施設様の取り組みを後押しする機能と具体的な活用事例を紹介しています。

・**コロナ禍の対応**（2021年10月）
「安全・安心」の取り組みをお客様へ伝えるためにご活用いただける機能と具体的な活用事例などを紹介しています。

株式会社キャディッシュ
フリーダイヤル 0120-489-468
メール support@489ban.net
https://www.489ban.net/services/489ban/
https://www.cadish.co.jp

© 2024 Cadish Inc.