2026
Digital x Future
宮崎県デジタル人財育成コンソーシアム

【会員向け情報提供レポート】 発信：宮崎県デジタル人財育成コンソーシアム 事務局

最近のサイバー事件から考える「自社は何を守るべきか」

2026 年 10 月 28 日時点 ｜ 経営者・情報担当者向け ｜ 配布資料（全 3 頁）

先に結論 すべてを最新に作り直す必要はありません。まず「自社が使うサービス」「守るべき情報」「障害時の連絡先」を確認し、優先順位を決めることが重要です。

1．今、何が起きているのか

事件 A：GMO「お名前.com デスクトップクラウド」不正アクセス

クラウド上の Windows 環境を提供するサービスで不正アクセスが発生し、10 月 21 日にサービス停止。攻撃者は顧客情報の公開と利用者端末への攻撃を予告しました。10 月 27 日には攻撃者による情報公開が確認され、10 月 28 日には問題のサイトのドメイン停止が公表されています。

重要なのは「クラウド事業者に預けている情報や認証情報が盗まれれば、顧客側の口座や業務にも影響し得る」という点です。一方、手元の PC へ侵入した経路がリモートデスクトップの共有機能だった、などの説明は現時点では確定した事実ではありません。

事件 B：PHP2shell ― Web サイトの土台に見つかった弱点

PHP は企業 Web サイトや各種 Web システムで広く使われるプログラム言語です。2026 年 10 月、外部から不正なプログラムを実行されるおそれのある脆弱性が公表され、IPA が更新を呼びかけました。10 月 26 日には米 CISA が実際に悪用された脆弱性として登録。国内の被害事例は、IPA の 10 月 27 日更新時点では把握されていません。

2 つは別の問題です。発生時期が近いからといって「PHP の弱点が GMO 事件の侵入口だった」とは言えません。

経営者・担当者が理解しておきたいこと

- **自社のPCが無事でも、利用するクラウド・外部委託先が攻撃されることがある。**
- **攻撃を受けなくても、緊急停止や更新対応で受注・決済・Web受付が止まり得る。**
- **「感染した／しない」だけでなく、認証情報の被害（ID・パスワード・アカウントの流出・不正利用）・業務停止の被害（受注・決済・受付・システムのストップ）・顧客情報の被害（保有データの流出・公開・信用失墜）を分けて考える。**

2．よくある疑問に答える ―「それで安全なのか？」

よくある疑問	押さえておきたい答え
ウイルス対策ソフトがあれば十分？	必要ですが万能ではありません。既知の不正ソフトの検知には役立つ一方、盗まれた ID・パスワードの不正使用や委託先の障害は防げません。
二段階認証なら絶対安全？	大幅にリスクを下げますが、偽サイトへの誘導、認証済みセッションの窃取等の手口があり、絶対ではありません。可能ならパスキー等の耐フィッシング性が高い認証も検討します。
パスワードは覚えきれない	使い回しは避け、信頼できるパスワード管理機能・管理アプリを使うのが現実的です。管理用アカウント自体にも強い認証を設定します。
古い PHP は本当に危険？	「古い＝直ちに侵入済み」ではありません。ただしサポート終了版は修正が受けにくくなります。使用有無・外部公開・保有情報・代替策から優先順位を決めます。
クラウドに預ければ安心？	事業者が担う防御と、利用者が担う ID 管理・アクセス権・バックアップは別です。契約上の役割分担と障害時の対応を確認します。
バックアップはクラウド同期でよい？	同期だけでは不十分です。誤削除や暗号化が同期されることもあるため、分離された世代バックアップと復元試験が必要です。

3．「PC が乗っ取られる」はどういう意味か

クラウド上の業務環境を手元の PC から遠隔操作する際、接続設定によってファイル・クリップボード等を共有できる場合があります。こうした共有は業務を便利にする反面、攻撃者が悪用できる範囲を広げる可能性があります。ただし「共有を有効にしただけで必ず PC が乗っ取られる」わけではありません。

被害を疑ったとき 感染が疑われる端末は社内ネットワークから隔離し、担当者・保守会社へ連絡します。安全な別端末で重要アカウントの認証情報を変更し、取引・アクセス履歴を確認。証拠を保全するため、独断で初期化やファイル削除をしないでください。

※ 特定サービスの利用者への緊急指示と、一般企業の日常的な対応は分けて考えてください。すべての会社が一斉に PC の電源を抜く必要はありません。

4．中小企業が「まず 1 週間で」施する 5 項目

優先	経営者・担当者が確認すること
① 取引先と資産を把握	自社サイト、メール、会計、顧客管理、クラウド、リモート接続を一覧化。サービス名・管理者・契約先・連絡先を記す。
② 重要アカウントを守る	管理者、メール、金融、クラウドに多要素認証を設定。使い回しパスワードを廃止し、退職者の権限も点検。
③ Web サイトの更新状態を確認	制作会社・サーバー会社へ「PHP 等の使用版、サポート期限、今回の脆弱性への対応状況」を問い合わせる。更新は事前バックアップ・動作検証とセット。
④ バックアップの復元を試す	重要データについて、日常環境から分離したバックアップと、実際に戻せるかを確認。
⑤ 有事の初動を決める	「誰が判断するか／どこへ電話するか／いつ業務を止めるか」を A4 一枚で決め、社内へ知らせる。

5．IT ベンダには、この 4 つだけ尋ねる

- 当社のどのシステム・サービスが今回の問題の影響を受けますか。根拠は何ですか。
- 今すぐ必要な対策と、計画的に実施できる対策を分けるとどうなりますか。
- 変更作業で業務停止は必要ですか。事前テストと元に戻す手順はありますか。
- 最小限の対策案と、本格更新案について、費用・残るリスクを比較できますか。

経営判断のポイント 「危ないから全部買い替え」も「今まで問題なかったから放置」も避けましょう。業務への影響、被害の大きさ、対策費用の 3 点で判断します。

公式情報・相談先（2026 年 10 月 28 日確認 ）

・IPA「PHP の脆弱性対策について」
https://www.ipa.go.jp/security/security-alert/2026/alert20261022.html

・GMO インターネット「デスクトップクラウド」第 13 報 https://internet.gmo/news/article/259/

・IPA「中小企業の情報セキュリティ対策ガイドライン」
https://www.ipa.go.jp/security/guide/sme/about.html

編集注：本資料は添付の AI 対話記録を出発点に、上記の一次情報で確認可能な部分を整理したものです。事件の詳細は今後更新される可能性があります。