

サイバーセキュリティ パートナーシップだより



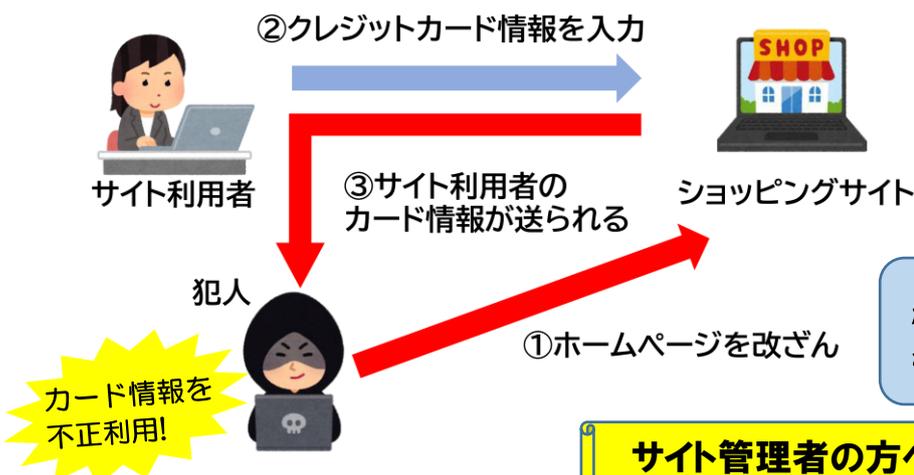
ウェブサイトの改ざん対策

～サイト利用者の個人情報がねらわれています！～

ショッピングサイトを改ざんし、利用者が購入時に入力したクレジットカード情報などを不正に入手する「Web（ウェブ）スキミング」という手口をご存じですか？

サイトを管理されている方については、そのサイトが不正に改ざんされていないか、今一度確認をお願いします。

Webスキミングの仕組み



改ざんサイトによって

盗まれてしまう情報の例

- クレジットカード情報などの決済情報
- ログイン用の ID・パスワード
- 会員登録情報

個人情報の漏えい対策
を見直しましょう！



サイト管理者の方へ

改ざんされる原因	対策
① サイトの管理者用アカウントを不正に利用された（推測されやすいパスワードを設定していた）	・推測されにくいパスワードを設定 ・管理画面へのアクセス制限を実施
② コンテンツ管理システムや OS（基本ソフト）等の脆弱性を攻撃されて侵入された	・古いバージョンを使っていないか確認 ・ソフトウェアを最新のものにアップデート

利用者の方へ

- クレジットカードの利用明細をこまめに確認する
- 心当たりのない利用があった場合は、クレジットカード会社や警察に相談する
- セキュリティ対策ソフトの導入・活用を検討する



山口県警察サイバー犯罪相談窓口
入力フォーム



県警ホームページにて広報資料
や動画を公開中です。
（詳しくは QR コード参照）

