

弊社サービスへの不正アクセスに伴う一連の対応について

10月23日 17時55分更新 【第22報】

ライデン・スクール セキュリティ強化対策「ログイン時２段階認証」設定のお願い。

再発防止、セキュリティ強化の一環として、「ログイン時２段階認証」を必ずご利用ください。「ログイン時２段階認証」機能は、ログイン時に「ユーザー名」と「パスワード」による認証に加え、メールアドレスに送信される確認コード（送信から15分間のみ有効）を用いて認証を行います。従来の「ユーザー名」と「パスワード」のみによる認証より、本人確認のプロセスがより強固になります。

対象サービス：**s.ktaiwork.jp**
s2.ktaiwork.jp

[PDF：ログイン時２段階認証機能の設定手順書をご覧ください、設定をお願いいたします。](#)

10月23日 17時35分更新 【第21報】

このたびの不正アクセスにより多大なるご迷惑とご心配をおかけしておりますことを、深くお詫び申し上げます。

本日時点で判明している事実、影響範囲、対応状況、および今後の対応方針についてご報告いたします。

ご説明資料

<https://raiden.site.ktaiwork.jp/wp-content/uploads/sites/2/2026/10/【説明資料】不正アクセスによる個人情報漏えいの可能性に関して20261023.pdf>

報告書

<https://raiden.site.ktaiwork.jp/wp-content/uploads/sites/2/2026/10/【報告書】不正アクセスによる個人情報漏えいの可能性に関して20261023.pdf>

10月22日 16時05分更新 【第20報】

SpeeCAN RAIDENセキュリティ強化対策「ログイン時２段階認証」設定のお願い。

再発防止、セキュリティ強化の一環として、「ログイン時２段階認証」を必ずご利用ください。「ログイン時２段階認証」機能は、ログイン時に「ユーザー名」と「パスワード」による認証に加え、メールアドレスに送信される確認コード（送信から15分間のみ有効）を用いて認証を行います。従来の「ユーザー名」と「パスワード」のみによる認証より、本人確認のプロセスがより強固になります。

対象サービス：**raiden.ktaiwork.jp**
raiden2.ktaiwork.jp
raiden3.ktaiwork.jp

以下のPDF：ログイン時２段階認証機能の設定手順書をご覧ください、設定をお願いいたします。

<https://raiden.site.ktaiwork.jp/wp-content/uploads/sites/2/2026/10/ログイン時２段階認証機能の設定手順書20261023l.pdf>

10月22日 10時40分更新 【第19報】

システムの調査と検証のため、現在一部の機能の利用を制限しております。
ご不便ご迷惑をおかけして申し訳ありません。

対象サービス：**raiden.ktaiwork.jp**
raiden2.ktaiwork.jp
raiden3.ktaiwork.jp
raiden2.speecan.jp
s.ktaiwork.jp
s2.ktaiwork.jp

対象機能：外部システムからのAPI連携機能の停止

※なお、弊社オプションの気象情報連携機能については影響ありません。

影響：外部システムからの連携ができないため、SpeeCAN RAIDENから手動発信をして頂く必要があります。
外部システムがエラーを検知する可能性がありますので、外部システムの業者にも影響についてご確認ください。

10月21日 19時30分更新 【第18報】

【第16報】でご案内しました機能制限について、調査と検証が完了したため、制限を解除しました。
ご不便ご迷惑をおかけして申し訳ありませんでした。

10月21日 17時20分更新 【第17報】

不正アクセスにより、多大なるご迷惑とご心配をおかけいたしますことを深くお詫び申し上げます。

2026年10月13日 01:17から2026年10月13日 7:16までのあいだ、不正なプログラムによって、弊社システムから外部に不正なメールが配信されました。その調査経過についてご報告致します。

配信内容：フィッシング詐欺

(実在する企業等を装い、偽サイトなどへ誘導して情報を盗み取る手口)

配信総数：1,423,428通

うち、少なくとも869,575通については、

当社内に保有するメールアドレスへの配信ではないことが明らかになりました。

今後、外部機関でダークウェブ調査を行い、結果について後日ご報告いたします。

※2026年10月13日 07:16時点で不正なメール配信を停止しています。

10月21日 17時00分更新 【第16報】

システムの調査と検証のため、現在一部の機能の利用を制限しております。
ご不便ご迷惑をおかけして申し訳ありません。

対象サービス：**raiden.ktaiwork.jp**
raiden2.ktaiwork.jp
raiden3.ktaiwork.jp
raiden2.speecan.jp
s.ktaiwork.jp
s2.ktaiwork.jp

対象機能：**FAX、放送連携、ファイル添付**

各機能の状況

- FAX** : 発信画面でチェックを付けることができず、発信できません。
- 放送連携** : 開始音、終了音のチャイムなどの音源ファイルが取得できず、エラーになります。エラーの表示が出ず発信操作を完了できた場合でも、放送実行時にエラーになり放送ができない場合があります。
- ファイル添付** : 正常に添付できない場合があります。

10月21日 15時00分更新 【第15報】

不正アクセスにより、多大なるご迷惑とご心配をおかけいたしますことを深くお詫び申し上げます。

LINE（お友達全員）、LINE（セグメント配信・LINE Developersコンソール）、X、Facebookとの連携をご利用いただいています契約者様につきましては、再度設定をしていただく必要があります。

以下の手順に沿って、お手続きをお願いいたします。

お手数をおかけしますが、どうぞよろしくお願いいたします。

●LINE（お友達全員）

1. LINE Developersコンソール(*1)を開き、「Messaging API」をクリックし、「チャンネルシークレット」の「発行」をクリックして、チャンネルシークレットを再発行する
2. RAIDENの「管理画面」-「拡張設定」-「LINE」の「Channel secret」に保存いただく
※連携情報を他事業者と共有している場合、他事業者との連携が停止するため、新しい連携情報を共有いただく必要があります。

●LINE（セグメント配信）

1. LINE Developersコンソール(*1)で「LINEログイン」の「チャンネルシークレット」と「Messaging API」の「チャンネルシークレット」を再発行する
2. RAIDENの「管理画面」-「拡張設定」-「LINEセグメント配信」で「Messaging API Channel secret」と「LINEログインChannel secret」に保存いただく
※連携情報を他事業者と共有している場合、他事業者との連携が停止するため、新しい連携情報を共有いただく必要があります。

●X(旧Twitter)

SpeeCAN RAIDENの「管理画面」-「拡張設定」-「Twitter」タブにある「Xに連携」をクリックして、再度、連携設定を実施してください。

※「Xに連携」をクリックすると、アプリの承認画面が表示されますので、画面の案内に従って承認操作を行ってください。Xのログイン画面が表示される場合は、画面の案内に従ってログイン操作を行ってください。

●Facebook

SpeeCAN RAIDENの「管理画面」-「拡張設定」-「Facebook」タブにある「Facebookに連携」をクリックして、再度、連携設定を実施してください。

※「Facebookに連携」をクリックすると、アカウント確認画面が表示されますので、「次へ」を選択してください。Facebookログイン画面が表示される場合は、画面の案内に従ってログイン操作を行ってください。

*1 LINE Developersコンソールへのアクセス手順

- <https://www.linebiz.com/jp/login> へアクセスする
- 「LINE公式アカウント」の「管理画面にログイン」をクリックする
- 「LINEアカウント」または「メールアドレス」をクリックしてログインする
- アカウントリストから連携対象のアカウントをクリックする
- 画面右上の「設定」をクリックし、画面左側の「Messaging API」をクリックする
- 「その他の設定はLINE Developersから行えます。」のリンクをクリックする
- プロバイダーから連携対象のプロバイダーをクリックする

LINEのお友達全員とセグメント配信の確認方法については、以下のPDFをご確認ください。

<https://raiden.site.ktaiwork.jp/wp-content/uploads/sites/2/2026/10/20261021line-seg.pdf>

10月21日 9時05分更新 【第14報】

不正アクセスにより、多大なるご迷惑とご心配をおかけいたしますことを深くお詫び申し上げます。

総務省への代行報告の件で、代理店様に以下の要領でメールさせていただきましたので、内容ご確認の上、ご入力願います。

件名：【重要】弊社サービスへの不正アクセス発生に伴う、総務省様への報告代行のご案内（代理店様）

（10月20日16時47分送信）

対象：以下のサービス販売の代理店様

SpeeCAN RAIDEN

(raiden.ktaiwork.jp,raiden2.ktaiwork.jp,raiden3.ktaiwork.jp,
raiden2.speecan.jp,s.ktaiwork.jp,s2.ktaiwork.jp)

NET119

(net119.speecan.jpとnet119fd.speecan.jpのURLが対象)

119RAIDEN

(fs119.ktaiwork.jpのURLのみが対象)

10月20日 14時00分更新 【第13報】

不正アクセスにより、多大なるご迷惑とご心配をおかけいたしますことを深くお詫び申し上げます。

10月16日15時30分更新【第10報】個人情報保護委員会への代行報告の件

でお知らせさせていただいていました内容につきまして以下の要領にてメールさせていただきましたので、内容ご確認の上、ご入力願います。

件名：【重要】 弊社サービスへの不正アクセス発生に伴う、個人情報保護委員会様への報告代行のご案内
(10月19日15時58分送信)

対象：

SpeeCAN RAIDEN

(raiden.ktaiwork.jp, raiden2.ktaiwork.jp, raiden3.ktaiwork.jp,
raiden2.speecan.jp, s.ktaiwork.jp, s2.ktaiwork.jp)

NET119

(net119.speecan.jpとnet119fd.speecan.jpのURLが対象)

119RAIDEN

(fs119.ktaiwork.jpのURLのみが対象)

10月19日 10時00分更新 【第12報】

このたびの不正アクセスにより多大なるご迷惑とご心配をおかけしておりますことを、深くお詫び申し上げます。これまで公式ブログや管理者様向けメールなどを通じて随時情報更新に努めてまいりました。さらに、今回の不正アクセスの経過と今後の対応についてより詳細なご説明を行う必要があると判断いたしました。現時点で判明している事実、影響範囲、対応状況、および今後の対応方針について、お伝えできる範囲で、PDFにまとめました。

https://raiden.site.ktaiwork.jp/wp-content/uploads/sites/2/2026/10/2026_10_19AccessIncident.pdf

10月16日 18時10分更新 【第11報】

当社が運営するNET119と119RAIDENにおきまして、第三者による不正アクセスが行われ、個人情報が漏洩した可能性があることを確認いたしました。

現時点で不正アクセスの侵入経路を遮断しており、システム内に不正なプログラムがないことも確認しております。

なお、現時点でサービス停止の予定はございません。通常通りご利用いただける状態です。

現時点で判明している事実関係と当社の対応状況につきまして、下記のとおりお知らせいたします。

1. 経緯

2026年10月11日16時30分、発生したSpeeCAN RAIDENの不正アクセスの調査過程において、2026年10月14日8時30分、当社が運営するNET119と119RAIDENへの、不正アクセスが疑われる痕跡を確認いたしました。侵入経路の遮断及び不正なプログラムの設置がないことの確認は実施済みだったため、影響範囲を特定するための調査をしております。

2. 漏洩した可能性のある情報

以下対象サービスで個人情報が漏洩した可能性があります。

なお、映像通報は現時点で漏洩の可能性はございません。

● NET119 (net119.speecan.jpとnet119fd.speecan.jpのURLが対象)

利用者の名前、生年月日、性別、住所、電話番号、メールアドレス、FAX番号、
他サービス登録時に入力した情報

9,020件のメールアドレスに紐づく上記個人情報

漏洩した可能性のあるメールアドレスを各消防本部様に個別にお知らせさせていただく
予定です。なお、要配慮個人情報には漏洩していないことは確認できております。

● 119RAIDEN（fs119.ktaiwork.jpのURLのみが対象）

連絡先の名前・メールアドレス・電話番号・FAX番号、担当者、契約情報

メールアドレス：約97000件

電話番号：約17000件

FAX 番号：約400件

3. 原因

第三者による不正アクセスが行われたことにより発生したものです。

4. 今後の対応

本件の発覚後、影響範囲の調査を続けております。

10月16日 15時30分更新 【第10報】

不正アクセスにより、多大なるご迷惑とご心配をおかけいたしますことを深くお詫び申し上げます。

個人情報保護委員会への報告の件でお知らせさせていただきます。

本来、各ご契約者様から個人情報保護委員会への報告を行う必要がありますが、個人情報保護委員会様と相談させていただき、弊社の方で代行報告を行う予定で準備を進めております。

ご同意をいただく必要がありますので、準備ができ次第、メールにてお知らせさせていただきますので、どうぞよろしくお願いいたします。

10月15日 17時50分更新 【第9報】

不正アクセスにより、多大なるご迷惑とご心配をおかけいたしますことを深くお詫び申し上げます。

被害の拡大を防止するために緊急停止しておりました以下のサーバは
本日15時頃に復旧完了しておりますので、お知らせさせていただきます。

SpeeCAN RAIDEN（raid3n.ktaiwork.jpのお客様が対象）

ライデン・スクール（s2.ktaiwork.jpのお客様が対象）

すべてのサービスは完全に復旧しており、安全にシステムをご利用いただける状況になっております。

不正アクセスの侵入経路は遮断いたしました。システム内に不正なプログラムがないことも確認しております。

脆弱性につきましても随時対応を進めております。上記のサーバも含め、情報漏洩の範囲につきましては、引き続き調査中です。

念のため、すべてのお客様は、ログインパスワードを変更した後にシステムをご利用ください。

【ログインパスワードの変更方法】

RAIDENにログイン→管理画面→設定→ログインアカウントから該当のアカウントを選択
→変更ボタンを押して、パスワードの変更をお願いいたします。

どうぞよろしくお願いいたします。

10月15日 13時30分更新【第8報】

不正アクセスにより、多大なるご迷惑とご心配をおかけいたしますことを深くお詫び申し上げます。被害の拡大を防止するため緊急停止しました以下のサーバを本日15時頃を目途に復旧予定ですので、前もってお知らせさせていただきます。

SpeeCAN RAIDEN（raidен3.ktaiwork.jpのお客様が対象）

ライデン・スクール（s2.ktaiwork.jpのお客様が対象）

安全性は社内で確認の上、ご利用いただける状況になりましたが、念のため、ログインパスワードを変更していただき、ご利用ください。どうぞよろしくお願いいたします。

10月15日 10時12分更新【第7報】

「外部機関への報告状況」につきまして

不正アクセスの件では、ご迷惑をおかけしており、申し訳ございません。

多数のユーザー様からお問い合わせをいただいております、掲題の件の対応状況について以下の通りご報告いたします。

本件の発生発覚後、速やかに事実関係の確認を行うとともに、個人情報保護委員会へ報告いたしました。また、警察、ISMS事務局、プライバシーマーク事務局、近畿総合通信局（総務省）、近畿経済産業局をはじめとする関係機関へも相談・通報のうえ、引き続き、原因の究明および影響範囲の調査に全力を挙げて取り組んでおります。

なお、お問合せのお電話を多数頂戴しており、電話がつながりにくい状態になっております。お手数をおかけしますが、電話がつながらない場合、info@arcadia.co.jp宛てにメールをいただけますようお願いいたします。お時間がかかるかもしれませんが、順次対応させていただきますので、ご理解の程どうぞよろしくお願いいたします。

10月14日 17時12分更新【第6報】

現時点で映像通報は漏洩の可能性はございません。

15時00分更新のNET119の内容を更新しております。

10月14日 16時00分更新【第5報】

さらに詳細調査を進めた結果、119RAIDENで漏洩の可能性がある対象URLが以下は対象外であることが判明しました。

- ・ fs119.speecan.jp
- ・ 119r.speecan.jp

15時00分更新の119RAIDENの内容を更新しております。大変お騒がせいたしました。

10月14日 15時00分更新【第4報】

詳細調査を進めた結果、NET119と119RAIDENにも第三者による不正アクセスが行われた形跡があり、個人情報が漏洩した可能性があることを確認いたしました。

現時点での調査結果として、以下対象サービスで個人情報が漏洩した可能性があることを確認いたしました。

対象サービス	NET119 (映像通報は現時点で漏洩の可能性はございません)	119RAIDEN
対象URL	net119.speecan.jp net119fd.speecan.jp	fs119.ktaiwork.jp
漏洩の可能性がある個人情報の項目	利用者の名前、生年月日、性別、住所、電話番号、メールアドレス、FAX番号、他サービス登録時に入力した情報	連絡先の名前、メールアドレス、電話・FAX番号 担当者、契約情報 履歴として保存されている本文に記載されている内容
漏洩の可能性がある個人情報の最大件数	約13000件	メールアドレス：約97000件 電話番号：約17000件 FAX 番号：約400件

影響範囲を拡大し、弊社の全サービスを対象に不正なプログラムが設定されていないか調査を進めております。

なお、現時点でサービス停止の検討はございません。通常通りご利用いただける状態です。

続報は本記事で公開させていただきます。

10月14日 10時40分更新【第3報】

今回の弊社サービスへの不正アクセスに伴い、不審な連絡等の二次被害が懸念されます。管理者様におかれましては、登録者の皆様へ向けて以下のような内容で注意喚起いただけますと幸いです。

“

【注意喚起】不審なメールやメッセージにご注意ください

登録制メールサービス提供者にて不正アクセスが確認されたことに伴い、不審なメールやメッセージにご注意ください。

不審な連絡に対して、氏名、住所、パスワード、口座情報などの個人情報を決して提示・入力しないでください。

身に覚えのない送信元や不審なメッセージに記載されたURL・添付ファイルは開かないでください。

”

10月13日 18時47分更新【第2報】

0.0.1 10月13日 状況のご報告

0.0.1.1 漏洩した可能性がある情報に関して

0.0.1.2 漏洩の可能性がある個人情報の最大件数

0.0.2 経緯

0.0.3 漏洩した可能性のある情報

0.0.4 原因

0.0.5 今後の対応

0.0.6 本件に関するお問い合わせ窓口

1 10月13日 15時50分更新 【第1報】

1.0.1 停止開始日

1.0.2 対象サービス

10月13日 状況のご報告

本日の調査において、外部からの不正な侵入経路が判明いたしました。

これを受け、被害の拡大を防止するため、侵入経路となっていた以下のサービスを緊急停止いたしました。

SpeeCAN RAIDEN（raidен3.ktaiwork.jpのお客様が対象）

ライデン・スクール（s2.ktaiwork.jpのお客様が対象）

不正なアクセス元となったIPアドレスを特定し、アクセスを拒否するように設定しました。

今回停止していないサービスにつきましては、サーバーの点検を行った結果、不正なプログラムが設定されていないことを確認しました。

漏洩した可能性がある情報に関して

漏洩した可能性がある情報は、SpeeCAN RAIDENで扱っている以下となります。

連絡先の名前、メールアドレス、電話・FAX番号

担当者、契約情報

履歴として保存されている本文に記載されている内容

なお、SpeeCAN RAIDENでクレジットカードなどの決済情報の取り扱いはありませんので漏洩対象ではありません。

漏洩の可能性がある個人情報の最大件数

メールアドレス：約3136000件

電話番号：約105000件

FAX 番号：約15000件

本件数は、あくまでも推定値であり、継続して調査を進めております。

当社が運営するSpeeCAN RAIDENにおきまして、第三者による不正アクセスが行われ、個人情報漏洩した可能性があることを確認いたしました。本事象の発生により、多大なるご迷惑とご心配をおかけいたしますことを深くお詫び申し上げます。

なお、現時点で不正アクセスの侵入経路を遮断しております。現時点で判明している事実関係と当社の対応状況につきまして、下記のとおりお知らせいたします。新たな事実が判明した場合は、速やかにお知らせいたします。

経緯

2026年10月11日16時30分、当社が運営するSpeeCAN RAIDENにおきまして、不正アクセスが疑われる不審な挙動を確認いたしました。これを受け、2026年10月12日3時ごろ、侵入経路を塞ぐ応急措置を講じました。同時に影響範囲を特定するための調査を開始いたしました。

漏洩した可能性のある情報

現時点での調査結果として、以下対象サービスで個人情報が漏洩した可能性があることを確認いたしました。

対象サービス	raiden.ktaiwork.jp raiden2.ktaiwork.jp raiden3.ktaiwork.jp raiden2.speecan.jp s.ktaiwork.jp s2.ktaiwork.jp
対象項目	連絡先の名前、メールアドレス、電話・FAX番号 担当者、契約情報 履歴として保存されている本文に記載されている内容

原因

第三者による不正アクセスが行われたことにより発生したものです。

今後の対応

本件の発覚後、不正アクセスの侵入経路を遮断し影響範囲の調査を続けております。新たな事実が判明し次第、本記事内で速やかにお知らせいたします。

本件に関するお問い合わせ窓口

本件に関してご不明な点がございましたら、以下までご連絡ください。

個人情報相談窓口

050-5830-0750

info@arcadia.co.jp

受付時間午前9時～午後5時（土日祝・年末年始は除く）

10月13日 15時50分更新 【第1報】

不正アクセスに伴う一部サービスの緊急停止について

現在、不正アクセスの侵入経路となった対象サービスを緊急停止しております。
（現在は復旧しております）

当社が運営するSpeeCAN RAIDENおきまして、第三者による不正アクセスが行われたことに伴い、本日2026年10月13日（火）11時00分から一部サービスの緊急停止を実施いたします。
現時点で復旧日時は未定です。早急な復旧に向けて全社を挙げて対応を進めております。

停止開始日

2026年10月13日（火）11時00分から
現時点で復旧日時は未定で、本記事内で随時ご案内します。

対象サービス

SpeeCAN RAIDEN（raidен3.ktaiwork.jpのお客様が対象）
ライデン・スクール（s2.ktaiwork.jpのお客様が対象）

関係者の皆様には多大なるご迷惑とご心配をおかけいたしますことを、深くお詫び申し上げます。
ご不便をおかけし大変恐縮ですが、何卒ご理解とご協力を賜りますようお願い申し上げます。



[【重要】【日程変更】サーバー設備増強に伴うサービス一時停止のお知らせ](#)



[PHPの脆弱性に関する当社の対応について](#)