付録　インシデント及び脆弱性情報一覧

No.	分類	発生箇所	報告書との対応	概要	公表年	発覚の経緯	原因	被害内容	対応内容	再発防止策
1	インシデント	SaaS事業者		システム更新時のプログラム破損によるサービス障害停止	2021	システム更新作業後、翌営業日の業務が不可となったことで発覚。	システム更新作業時のミスにより更新ファイルが破損、破損したファイルがクラウド環境に配布・自動適用され、障害が発生した。	システムを利用する百数十の団体で書類の印刷や発行ができなかった。	—	システム更新作業に関する管理手順等の見直しや社員教育を徹底した。
2	インシデント	ネットワーク		クラウドファンディングサイトでの個人情報誤表示	2021	手続き実施時に他者の情報が表示される事象があることが支援者から連絡された。	サービスの設定ミスにより、意図しない情報が表示された。	支援募集サイト上にアクセスした利用者とは異なる個人情報(*)が誤表示され、情報が漏えいした。 （*)氏名、メールアドレス、生年月日、性別、職業、会社名、住所、電話番号、過去の購入履歴	原因究明後にシステムの再構築を実施し、同様の問題が発生しないことを確認した。 電子メールでお詫びと経緯を説明した。	システムの不具合発生を未然に防止する体制を構築し、再発防止に向け情報管理体制を強化した。
3	インシデント	ネットワーク		デフォルトドメイン取得による詐欺サイトへの誘導	2020	大手組織を含むドメイン名において、検索サイトから接続した際に、詐欺サイトへ遷移される事象が発生。サイトに接続した利用者からの問い合わせがあった。	CDNサーバーに登録したCNAMEレコードの消し忘れを用いたサブドメインテイクオーバー。	サイトに接続した利用者が詐欺サイトに誘導される事象が発生。 大手組織を含む複数の国内外のドメイン名が影響を受けており、検索にかかるものだけでも100件以上であった。	—	—
4	インシデント	ネットワーク	10	IT資産管理・監視ソフト改ざんによるダウンロード利用者環境からの情報漏えい	2020	—	IT資産管理・監視ソフトウェアの開発工程でマルウェアに感染し、バックドアの役割を持つ改ざんされたコードが混入した。 バックドアを含んだバージョンにアップデートした利用者から情報が漏えいした。	バックドアが含まれたIT資産管理・監視ソフトウェアをインストールした利用者は一万数千社社程度であった。	バックドアを含んだソフトウェアビルドをダウンロードサイトから削除。 該当バージョンする利用する全ユーザーに対しアップデートを推奨。	—
5	インシデント	オンプレミス	11	リモート監視・管理ツール（オンプレミス版）へのランサムウェア攻撃	2021	—	ゼロデイ脆弱性。 未修正の脆弱性の悪用により、ランサムウェアに感染するスクリプトが配られ、実行された。	影響を受けた組織は数千数百程度。	オンプレミスの利用者に対して、即時にオフラインにすることの通知、SaaSとして提供されるサービスのシャットダウンなど。	—
6	インシデント	ネットワーク		ドメイン登録サービスの脆弱性を悪用したメールアドレスやドメインの改ざん	2020	サービス応答時間の遅延発生。	悪意のある第三が脆弱性を利用して、会員情報(メールアドレス、パスワード）を書き換えて不正アクセスを行った。	悪意のある第三者が、お客様のIDと、ドメイン登録サービスにおける通信を改ざんできる不具合を利用して、サービスの会員情報(メールアドレス)を書き換えた。	本事象の対象のお客様との連絡と、正しい情報に修正。	—
7	インシデント	SaaS		プロジェクト管理ツールへの不正アクセスによる情報漏えい	2021	社内外の関係者とインターネット上で情報共有するツールへの不正アクセスの形跡が確認された。	不正アクセス。 多要素認証が採用されておらず、不正アクセスを早期に検知する仕組みも十分ではなかった。	影響を受けた顧客数は百数十件。 閲覧、ダウンロードが行われた情報には顧客システムの関連情報など含まれていた。 警視庁へは被害相談済であるが窃取された情報の悪用は確認されていない。	多要素認証を用いた認証強化による不正ログインの防止。 複数のログの収集・管理、監視の強化。	専任のCISOの任命および情報セキュリティ体制の強化を実施した。
8	インシデント	SaaS		リモートアクセスサービスの不具合による誤表示	2020	ログイン画面に第三者のユーザーIDとみられる情報が含まれるエラーメッセージが表示されたという報告を利用者から受けた。	アプリケーションの不具合	当該サービスは数百社が利用。 認証系サーバのサービス停止により、リモートからのシステムの利用ができなくなり、当該サービスを利用している組織において、リモート環境での代替手段がない業務については担当者が出社して対応した。	—	—
9	インシデント	SaaS		メールアプリの脆弱性を悪用した標的型攻撃	2020	米国のサイバーセキュリティ関連企業がデジタルフォレンジック、及びインシデントレスポンスの調査を通じて脆弱性を発見した。	・nmapの脆弱性 ・MIMEのライブラリであるMFMutableの脆弱性	脆弱性の標的となった企業は数社。 メーカーは顧客へ損害を与えるため悪用された形跡は見つかっていないとしている。	修正アップデートを配布。	—
10	脆弱性	SaaS事業者	3	某国が利用するCOVID-19接触追跡アプリので個人情報が閲覧可能	2020	—	不適切な仕様での設計	COVID-19の接触追跡アプリをインストールしていた100万人以上の利用者の名前・国民ID・健康状態・位置情報などが誰でも取得可能な状態となっていた。	健康状態データに含まれていた名前、場所の除外、アプリをアップデート（認証を追加）した。	—
11	インシデント	再委託先	5	設定ミスにより顧客情報が閲覧可能	2020	アカウントが不正利用された可能性についての調査を行う過程でお客様情報を三者が閲覧できる状態になっていたことが判明した(アカウントは不正利用されていなかった）。	データバックアップに利用していたクラウドのストレージが公開設定となっており、第三者に閲覧可能な状況となっていた。	クラウドのストレージに保管している以下の情報が第三者から閲覧可能な状態であった。 ・イベント開催場所名 ・物品送付、返送先住所 ・物品受渡のご担当者様名 ただし、不正利用の形跡は確認されなかった。	クラウドサービスが不正利用されないように、以下３点を確認した。 ・Webサービスが必要最小限の設定になっていること。 ・同じID・パスワードを他システムで利用しないことを見直した。 ・不要なアカウントはが削除されていること。	ハードディスクが暗号化されていることを確認した。 全PCにウイルス対策ソフトが導入されていることを確認した。 クラウドサービスへの不正アクセス防御の為に、使用履歴をWeb 画面で確認し、海外で利用されていない事を継続的に確認した。
12	インシデント	SaaS事業者		不正アクセスにより顧客の年齢確認書類画像データ流出	2021	サーバーへに対する通常では想定されない挙動の検出。	クラウドサーバへの不正アクセスにより、情報が取得された。	百数十万件以上のアカウントの年齢確認書類の画像データ(運転免許証、健康保険証、パスポート、・マイナンバーカード等)が流出した。	不正アクセス元IPアドレスの遮断、ネットワーク制限の強化。 外部組織によるシステムチェックと原因調査。 監視、アクセス制限の強化。 緊急対策委員会の設置。 会員情報不正使用による二次被害防止への対処方法、会員個別連絡、注意喚起施策検討開始。 総務省、警視庁へ不正アクセスの被害相談。	外部ネットワークからのアクセスやリクエスト制限の厳格化、アプリケーションの認証設定の見直し。 情報の保管場所の移動と暗号化。 システムや情報へのアクセス制御と権限の厳格化及びパスワードポリシーの強化。 サーバーへのログイン認証の厳格化と監査証跡の強化。 社内エンドポイントへの定常的な動態調査基盤の導入。 脆弱性診断実施、診断結果にもとづく実装の見直しとセキュリティ強化。 eKYCサービス導入。
13	脆弱性	SaaS		Github Actionsにおける処理の不備により秘密情報が取得可能	2021	—	Github Actionsの不備により、プルリクエスト時にマージ競合エラーを発生させ、秘密情報を取得することが可能であった。	—	—	—
14	脆弱性	SaaS		Github Actionsにおける処理の不備により新規ファイル作成等書き込み処理が可能	2021	—	Github Actionsの不備により、プルリクエスト時に新規ファイルを作成する等書き込み処理が可能であった。	—	—	—

付録　インシデント及び脆弱性情報一覧

No.	分類	発生箇所	報告書との対応	概要	公表年	発覚の経緯	原因	被害内容	対応内容	再発防止策
15	インシデント	SaaS	6	改ざんされたスクリプトにより認証情報が窃取され、顧客情報やソースコードが漏えい	2021	ツール提供事業者がスクリプトが改ざんされたこと、改ざんれたスクリプトを含むツールを利用した場合、利用者に影響を及ぼす可能性があることを公開した。	脆弱性をつかれ、ツールの開発環境においてスクリプトが改ざんされた。	スクリプトが改ざんされたツールを使った利用者から数万件の情報（個人、取引先、口座関連）が流出した。	改ざんされたスクリプトの修正。 経緯の説明およびフォレンジック。	今回のインシデントに関連する内部の秘密情報をすべて変更。 ツールの監視、監査体制を構築。 改ざんされた環境が廃棄されたことを確実にするため、サードパーティサーバーのホスティングプバイダーとの協業、影響を受けるユーザーへの推奨対処。
16	脆弱性	OSS	14	Kubernetesに脆弱性によりクラスタ内の通信を傍受される可能性	2020	—	Kubernetesの設計上の欠陥。	—	パッチを適用すると、ユーザーが依存する機能への変更が避けられないため、代わりに脆弱な機能へのアクセスを制限する緩和策を実施することを推奨した。	—
17	脆弱性	OSS	15	Homebrewのライブラリの脆弱性によりリポジトリ内への書き込み、実行が可能	2021	—	GitHubActionsを利用しているHomebrewライブラリの脆弱性。	—	すべてのリポジトリから脆弱性を排除した。 新しいメンテナを迎え入れ、既存のメンテナが を支援できるように、ドキュメントを改善した。	—
18	脆弱性	OSS		Cloudflareのライブラリの脆弱性によりライブラリが改ざん、サーバ上で任意のコードが実行可能	2021	—	CloudflareのライブラリcdnjsにZipslipの脆弱性。	cdnjsのライブラリ更新用サーバーに任意のコードを実行することが可能な脆弱性が存在し、cdnjsを完全に侵害可能。その結果インターネット上のウェブサイトの内12.7%を改ざんすることが可能な状態だった。（被害発生のレポートは確認できていない。）	各種認証情報の無効化。	—
19	脆弱性	SaaS		GitHub上の継続的インテグレーション（CI)サービスの脆弱性により、秘密情報を含むファイルがビルド中に閲覧可能	2021	—	—	—	セキュリティパッチの提供。	—
20	脆弱性	ネットワーク	9	CDNのキャッシュに攻撃コードを注入させることで、意図しないスクリプトを実行可能	2020	—	—	細工された HTTP ヘッダを含む HTTP リクエストを処理することで、CDN のキャッシュが汚染され、Web サイト閲覧者に悪意あるコンテンツが配信される可能性があった。	・CDN における対策 HTTP ヘッダに対して適切な検証処理および無害化処理を実施した。 ・Web サーバにおける対策 ・HTTP リクエストに含まれる内容を信頼しない。また、レスポンスには適切かつ安全なエンコーディングを用いる。 ・CDN における回避策 ・悪意あるコンテンツの配信を防ぐため、HTTP リクエストのヘッダに不審な内容が含まれていたらキャッシュしない。 ・Web サーバにおける回避策 ・悪意あるコンテンツの配信を防ぐため、動的に生成したコンテンツが CDN にキャッシュされることを防ぐ。	—
21	インシデント	再委託先	4	再委託先(海外法人)社員が、無許可で取引先/従業員情報等をダウンロードし、外部クラウドストレージサービスに保管	2021	再委託先法人の監視システムがセキュリティアラートを送信したため、調査したところ、再委託先の社員が取引先/従業員情報などをダウンロードし、外部クラウドストレージにアップロードしていたことが発覚した。	再委託先に取引先情報や従業員情報などのデータへのアクセス権限があった。	流出は確認されていないが、数万件の情報に流出の可能性があった。	アップロードされたデータは、再委託先の監視のもと削除。 外部クラウドサービス事業者の調査で、アップロードされたデータを第三者がコピーしたり、ダウンロードした形跡がないことを確認した。	外部委託先を含めたセキュリティ強化と情報管理を徹底した。
22	脆弱性	OSS	13	Gitの脆弱性によりリモートコードが実行可能	2021	—	シンボリックリンクをサポートし、かつ、大文字と小文字を区別しないタイプのファイルシステムにおて、特別に細工されたリポジトリを使われた場合、特定のタイプのクリーン/スマッジフィルタを悪用することでgit cloneを実行している間にコードが実行される危険性がある。	不明	「Git v2.30.2」へアップデート。	—
23	インシデント	OSS		ダイジェスト認証をやぶられソースコードリポジトリに不正アクセス	2021	—	認証を突破されて、悪意のあるコミットを実施された。	ユーザーデータベースが流出した可能性がある。	パスワードのリセットの実施および新しいパスワードの再設定を依頼した。	—
24	脆弱性	OSS		某アプリケーション向けのプライベート該当可否チェック処理にOSコマンドインジェクションの脆弱性が存在し、悪用することで任意のコードが実行可能	2021	—	プライベート該当可否チェック処理に用いていたOSSの脆弱性。	攻撃者がデータベースにアクセスできた可能性がある。	パッチの適用。	—
25	インシデント	OSS		ワークフローエンジンに不正な操作が行われ、暗号通貨の採掘に利用	2021	ワークフローエンジンのインスタンスの影響調査時に、保護されていないインスタンスが発見された。	多くのインスタンスで、訪問したユーザーなら誰でもワークフローを展開できるようなパーミッションが設定されていた。	攻撃者がオープンダッシュボードにアクセスし、独自のワークフローを送信することが可能であった。	アプリケーションの設定ミスや脆弱性を攻撃者が突いた場合、ポッド、ノード、クラスタ上で動作するすべてのコードをすぐに可視化し、環境内の攻撃を検知して対応できるよう支援した。	—
26	脆弱性	IaaS及びPaaS	7	Webベースの開発環境の脆弱性によりデータベースの認証情報が取得され、データの閲覧、修正、削除が可能	2021	—	—	侵入者が全てのデータベースを読み書きでき、全て削除してしまうことが可能。 ターゲットとなる環境に対する事前のアクセスは必要なく、何千もの組織に影響を与える可能性がある。	影響を受けるDBアカウントごとにプライマリーキーを再生成して、キーのローテーションを行う。	—

付録　インシデント及び脆弱性情報一覧

No.	分類	発生箇所	報告書との対応	概要	公表年	発覚の経緯	原因	被害内容	対応内容	再発防止策
27	脆弱性	IaaS及びPaaS		MS社のOpen Management Infrastructure(OMI)の脆弱性により、リモートコードが実行可能	2021	—	—	—	修正プログラム適用。	—
28	脆弱性	IaaS及びPaaS	8	Azure Container Instances（ACI)の脆弱性により悪意のあるコンテナから他顧客のコンテナを攻撃可能	2021	—	Azure Container Instances（ACI)の脆弱性。	悪意のあるAzureユーザーは、これらの問題を悪用して、他のユーザーのコンテナ上でコードを実行したり、顧客の秘密やプラットフォームにデプロイされたイメージを盗んだり、ACIのインフラを仮想通貨（暗号通貨）のマイニングに悪用したりする可能性がある。	MicrosoftはACIの修正プログラムをリリース。予防措置として、ACI上でコンテナを実行している場合は、2021年8月31日以前にプラットフォームにデプロイされた特権的な認証情報を失効させ、アクセスログに異常がないか確認することを推奨した。	—
29	脆弱性	OSS		Webサービスフレームワークにおける脆弱性によるサービス運用妨害の恐れ	2021	—	Apache CXF におけるサーバサイドのリクエストフォージェリの脆弱性。	サービス運用妨害 (DoS) 状態にされる可能性がある。	プログラムの修正。	—
30	脆弱性	OSS		GitHub上のプロジェクトに含まれたマルウェアがダウンロードされることによるトロイウイルスに感染する恐れ	2020	—	—	数十件のオープンソースプロジェクトが、バックドアがしこまれたコートを提供していた。	—	—
31	インシデント	利用者		教育機関が利用している外部クラウドサーバのアカウントを悪用し大量のフィッシングメール送信	2021	大量のフィッシングメールを確認した。	関係者が登録したメールアカウントの1つに安易なパスワードが設定されており、外部からの不正ログインされた。	外部からの不正ログインがあり、数回い分けて合計一万数千件のフィッシングメールを送信。	外部クラウドサーバのメール機能を禁止し、CISOから情報セキュリティ管理責任者に対し、パスワード管理の徹底等について再指示した。	再発防止の指導や情報システムの総点検、技術面・運用面の対策強化など、サイバーセキュリティ対策の強化をより推進した。
32	インシデント	SaaS事業者		ランサムウェア攻撃によるレポートサービス利用停止	2021	利用者からレポートサービスが利用ができない旨の連絡を受けた。	閉じられていなかったポートに対する不正アクセスである可能性が高い。	サービスの利用停止（お客様の情報・当社の業務データに関する情報ともに情報流出は発生していない）。	サーバーへの不正アクセスを防止するセキュリティ強化の対策措置を実施とサーバー運用に関わる体制や手順などの見直しを実施した。	—
33	インシデント	SaaS事業者		オンライン学習サービスの海外からの不正アクセスによりID/パスワードが閲覧可能	2020	障害アラートの受信。	サービスの開発者がフィッシング被害に遭い、認証情報やアクセスキーが窃取された。攻撃者がアクセスキーを用いてDBサーバーに侵入し、DBサーバーのパスワードを変更したことでサービスが停止した。	約百数十万人分のID/パスワードが不正に取得された可能性がある。	フィッシング攻撃への対策。 ソースコード内の機微情報の確認・削除。 サーバーの管理者パスワードの変更と検知機能導入を実施。 利用者にパスワード変更を呼びかけた。	ソースコード管理の認証機能強化。 ソースコード内機微情報排除強化。 クラウド開発プラットフォームの認証機能強化。 パスワード操作権限の限定の追加対策。 情報セキュリティマネジメント強化。 社内体制の構築と従業員への教育実施。
34	インシデント	利用者		なりすましによる社内ネットワークへの不正ログイン	2020	なりすましログインの検知。	ユーザによるパスワードの使いまわし。	不正ログインを受けた可能性があるネットワークIDが約数十万件。 名前、生年月日、性別、国/地域、メールアドレスの情報が閲覧された可能性がある。	被害にあったログイン機能を廃止。 二段階認証を設定を依頼。	—
35	インシデント	利用者		不正に取得された口座番号やキャッシュカードの暗証番号等を悪用した不正利用	2020	複数の金融機関で不正利用に関する案内が相次ぎ公開された。	不正に取得された口座番号やキャッシュカードの暗証番号等の悪用。	口座登録の受付停止を行った銀行、数十行。 正利用(疑い含む)発表/報道された銀行、十数行 不正利用件数：百数十件 不正利用被害総額：数千万円	口座の不正利用発生を受けた金融機関の新規登録を当面停止。 オンライン本人確認システム（eKYC）を確実に講じ、再開時期を検討。更にSMS認証も導入。 eKYCではd払いアプリでユーザーのセルフィーと運転免許証などの本人確認書類を撮影した画像をアップロードし、本人の同一性を確認する。	—
36	インシデント	SaaS事業者		金融機関への不正アクセスによる顧客の資産流出	2020	顧客から身に覚えのない取引があるという申告を受けた。	不正ログイン。	口座を所持している顧客の有価証券売却及び当該口座からの出金など。 被害総額は約１億円。	被害にあった可能性のある顧客に対して出金停止、パスワードリセットを実施した。	多要素認証の導入。 通知機能(ログイン、出金指示、など）、ログ員監視機能の強化。 ガバナンスの強化。
37	インシデント	SaaS事業者		プリペイドカードの送金機能を使った不正送金	2020	Webサービスへのへ大量のログイン試行を検知した。	不正ログインによって外部に情報漏えいした可能性がある。	千数百人が不正ログインされた。 数百万円分が不正送金された。 会員サイトにログインすると、名前、生年月日、カードの番号下4ケタと有効期限などの個人情報や、買い物などの履歴が閲覧できるようになる。	Webサービスの当面停止。 不正ログインの可能性が確認された会員のカード利用の一時停止。 被害の発生が判明した場合の可及的速やかな全額補償対応。 調査対象期間を拡大し更なる不正ログイン被害の有無の調査。 最終的サービスを取りやめた。	第三者機関によるセキュリティ総点検を実施し、結果をふまえてセキュリティ対策の強化を実施。
38	インシデント	SaaS事業者		不正アクセスによる海外の子会社からの情報漏えい	2021	利用しているクラウドサービスで異常なアクセスを検知した。	窃取したアカウント情報を利用して従業員になりすまして不正アクセスされた。	同社の国内取引先の金融機関口座に関わる数千件の情報と、同社の一部国内取引先に関する同社保有情報数百件が流出した。	グループ全従業員のアカウント情報の修正や廃止、アクセス制御の強化などを実施。	—
39	インシデント	利用者	1	クラウドの設定不備により、部外者から機密情報が閲覧可能	2020	複数の組織で、クラウドシステムに保管された情報が第三者からアクセスされた。	クラウドの設定ミス。	クラウドを利用していた多くの組織で、情報が外部から閲覧可能となっていた。閲覧可能となっていた情報は数百万件以上。	ゲストユーザの一部の機能の無効化。 恒常的な対策として、ゲストユーザの権限設定の見直しを行うことが望ましいことを公開。	ユーザーに対しゲストユーザーに対する共有設定の確認を呼び掛けとベストプラクティスの更新。
40	インシデント	利用者		クラウドの公開設定ミスにより、非公開ファイルが閲覧可能	2021	クラウドセキュリティアナリストによる報告。	設定ミス。	以下のような情報が閲覧できる状態であった。 ・アンケート結果 ・クラウド利用手順書 ・クラウド二要素認証操作マニュアル ・クラウド認証用証明書インストール手順 ・クラウド認証用証明書	アクセス権限を修正。	—
41	インシデント	再委託先		委託先エンジニアがGithubにソースコードを公開したことによるソースコードの流出	2021	—	不適切な情報の取り扱い。	Github上にソースコードが公開された。	公開されたソースコードの削除。	—
42	インシデント	オンプレミス		マネージド・サービス・プロバイダへの不正アクセスおよびマルウェア感染	2020	社内のパソコンの不審な挙動を検知した。	利用していたソフトウェアの脆弱性によるウイルス感染。	不正アクセスにより流出した主な情報は、サーバ設定情報、アカウント情報、認証プロセスのメモリダンプなどのIT関連情報。 機微な情報や機密性の高い情報、取引先に係る情報、個人情報などの流出は確認されなかった。	当該ソフトウェアの使用を停止。	ファイアーウォールの設定。 早期の攻撃検知のため、サーバ監視機能を強化。

付録　インシデント及び脆弱性情報一覧

No.	分類	発生箇所	報告書との対応	概要	公表年	発覚の経緯	原因	被害内容	対応内容	再発防止策
43	インシデント	利用者		社外から正規アカウントを悪用しVDI経由で社内データに不正アクセス	2020	不正アクセスの検知。	社員が社外からのリモートアクセスに利用していたBYOD端末から正規のアカウントが窃取されVDI経由で社内ネットワークに侵入された。	数百件以上の情報が流出した可能性がある。	BYOD、シンクライアント専用端末のリモートアクセス環境停止。 全社員のパスワード変更。	ゼロトラストネットワーク構築。 EDR導入。
44	インシデント	利用者	2	第三者へのURL誤送信により疾病者情報が閲覧可能	2021	誤送信先からの宛先間違いの連絡。	クラウドへのアクセス権を付与したメールを１名の方に誤送信した。	インターネット上で1か月にわたり、第三者（メール誤送信を受けた人）が、数千人の疾病情報（氏名、年齢、性別、居住自治体名、症状など）を閲覧できる状態だった。 メール誤送信を受けた人以外の流出や悪用の事実は確認されていない。	クラウドにアップロードしていたファイルを全て削除。 対象者への事実関係の連絡と謝罪。 ファイルの参照権限を受けた人以外の参照があったかを確認を調査。	再発防止として、クラウドを使用せず、電話、FAXで個人情報の送信を行うことが報じられた。
45	インシデント	SaaS事業者		SNSサービス上の個人情報の移転に関する本人への説明不足	2021	SNSサービスの個人情報保護に不備があったと報道されたことにより発覚。	利用規約において、「利用者の居住国と同等のデータ保護法制を持たない第三国に個人情報を移転することがある」と説明するも国名までは明記していなかった。	アプリケーションの利用者に対して、国外で一部利用者情報を取り扱っていたことについて十分な説明されていなかった。	個人情報へのアクセス遮断。 データの国内移転。	国名や目的の明示を踏まえたプライバシーポリシーの改定。 データセキュリティに対するガバナンス体制、情報保護強化。
46	インシデント	再委託先		委託先の社員の不正アクセスによる顧客口座からの不正送金	2021	身に覚えのない取引が行われたとして顧客からコールセンターへ通報があったことで発覚。	元従業員がバックアップファイルから顧客の情報を抜き取り、自身のPC宛に顧客情報を送信、それらを利用して、なりすましにより顧客の口座から不正に送金を行った。	数百名分の顧客情報（ID、暗証番号等）からなりすましにより合計約数億円を不正送金された。	不正送金された顧客へ全額返金。	—
47	インシデント	利用者		データ入力ミスによる本人の医療情報サービス利用不可	2021	医療機関で以下のトラブルが発生したことで発覚。 ・保険資格情報が登録されていないといったエラー表示された。 ・健康保険証に記載された情報が一致せず、患者情報が確認ができなかった。	データ入力の不備により本人とは異なる医療関係情報が紐づけられてしまった。	数万件のマイナンバーの取り違えにより、医療機関にて本人確認が行えないトラブルが発生した。 アプリケーションサイトでで他人の健康状態の情報が表示されるリスクがあった。	当該機能の運用開開始を延期した。	—
48	インシデント	利用者		ワクチン接種受付システムに登録された情報が閲覧可能	2021	特殊な解析ツールを用いて、システムに特定の操作を行うと医療関連の個人情報が閲覧可能であるため、早急な対応をすべきとの情報提供があった。	特殊な解析ツールを利用すると医療関連の個人情報(氏名、生年月日、職種、接種券番号)が閲覧可能となっていた。	医療関連の個人情報（氏名・生年月日・職種・管理番号）数百件が閲覧可能となっていた。	システムの改修。 システム改修が完了するまでシステムを中止し、コールセンターでの予約対応を実施。 個人情報を閲覧された可能性のある方への書面を送付による謝罪。	—
49	インシデント	オンプレミス	12	データ移行作業時のトラブルによる金融機関でのサービス利用停止	2021	データ移行作業中にシステム障害が発生し、一部のシステムがが利用できなくなる障害が発生した。	データ移行作業中に発生した過負荷によるメモリ不足。	数千台のシステムのうち、約半分がサービス停止した。	機器の再起動。	メモリ容量の増量。
50	インシデント	再委託先		元従業員による機密情報の持ち出し	2021	元従業員が返却した社有PCから技術情報を不正送付した痕跡を確認したことで発覚。	社内サーバーに接続し、営業秘密を含む情報を添付してフリーアドレス宛に送信することで情報が持ち出された。	百数十件の秘密情報が数十回にわたりが持ち出されていた。	転職前の組織は逮捕発表とともに、転職先の組織に対し営業秘密の利用停止と破棄を求める民事訴訟を提起する方針であり、元従業員への損害賠償請求も検討していると公表した。	・情報資産管理の再強化（管理ポリシーの厳格化、棚卸しとアクセス権限の再度見直し） ・退職予定者の業務用情報端末によるアクセス権限の停止や利用の制限の強化 ・全役員と全社員向けのセキュリティー研修（未受講者は重要情報資産へのアクセス不可） ・業務用OA端末の利用ログ全般を監視するシステムの導入
51	インシデント	利用者		電子決済サービスの不正利用	2020	不正利用を受けたユーザーの申告や内部調査で発覚。	口座開設時の本人認証の仕組みの不備を悪用。	不正出金被害は百数十件、総額で数千万円。	サービス停止。 被害金額の保証。	口座開設時の二要素認証の導入、 モニタリング態勢の整備などのセキュリティの強化。
52	インシデント	IaaS及びPaaS		ドメイン管理会社での環境変更作業のミスによりドメイン名ハイジャック可能	2021	—	ドメイン管理会社が既存システムをクラウドへ移行する際の設定ミス。	第三者が任意のコンテンツを表示可能なドメインテイクオーバーが可能な状態になっていた。	—	—
53	脆弱性	オンプレミス		Vmware vCenter仮想マシンの管理ソフトの脆弱性によりリモートコードが実行可能	2021	—	Vmware vCenter仮想マシンの管理ソフトの脆弱性。	ポート 443 にネットワークアクセスできる悪意のある行為者は、この問題を悪用して、vCenter Server をホストする基本オペレーティングシステム上で無制限の特権でコマンドを実行する可能性がある。	解決方法 CVE-2021-21972 を修正するために、以下の「対応表」の「修正バージョン」欄に記載されているアップデートを、影響を受けるデプロイメントに適用してください。 回避策 CVE-2021-21972 に対する回避策は、以下の「対応表」の「回避策」欄に記載されています。	—
54	脆弱性	オンプレミス		ロードバランサ機器の脆弱性によりAPI（HTTP)経由でリモートコードが実行可能	2021	—	—	脆弱性が悪用されると、認証されていない遠隔の第三者が任意のコードを実行するなどの可能性がある。	F5 Networksから脆弱性（CVE-2021-22986）を修正したバージョンが公開。十分なテストを実施の上、修正済みのバージョンを適用する。	—
55	脆弱性	オンプレミス		HTTP.sysの脆弱性により認証不要でリモートコードが実行可能	2021	—	Windows OS に存在する RCE 脆弱性。	悪用された場合、攻撃者がリモートから任意のコードを実行できる可能性がある。また本脆弱性は、Blue Screen of Death(BSoD)を引き起こす概念実証(PoC)コードも確認されており、DoS 攻撃を受ける可能性がある。	Microsoft より修正パッチが提供されている。	—

付録　インシデント及び脆弱性情報一覧

No.	分類	発生箇所	報告書との対応	概要	公表年	発覚の経緯	原因	被害内容	対応内容	再発防止策
56	脆弱性	IaaS及びPaaS		WindowsServerコンテナの脆弱性に対するゼロデイ攻撃によるアクセス権侵害の可能性	2021	—	・Windows Server コンテナの脆弱性 ・Kubernetesクラスタの設定ミス	このマルウェアはKubernetesクラスタのコンピューティングリソースを利用してクリプトジャックを行い、侵害クラスタ上で実行されている何百ものアプリケーションから機密データを漏出させる可能性がある。 このマルウェアは大規模ネットワークの一部で、攻撃キャンペーンは1年以上前から行われていることが判明した。特定攻撃キャンペーン部分にアクティブな被害者がいることも確認された。	ユーザーは「Windowsコンテナをセキュリティ機能と考えて利用しないこと」を推奨するMicrosoftのガイダンスに従うべき。 Microsoftではコンテナ化をセキュリティ境界として利用するのであれば、厳密にHyper-Vコンテナだけを使うことを推奨。 Windows Serverコンテナで実行されるプロセスはすべて、ホストのadminと同じ権限を持っているものと仮定しておく必要がある。 Windows Serverコンテナでセキュリティを確保する必要のあるアプリケーションを実行しているなら、これらのアプリケーションはHyper-Vコンテナに移行することを推奨。	—
57	脆弱性	オンプレミス		Vmware vCenter Serverに脆弱性により認証していない状態で任意コードが実行可能	2021	—	—	ファイルアップロード機能に関連した脆弱性で、悪用されるとリモートの攻撃者によって対象システムで任意のコードを実行される危険性がある。	9月21日にCVE-2021-22005を含む複数の脆弱性を修正したセキュリティアップデートをリリースした。	—

表の見方

分類	「インシデント」または「脆弱性」のどちらであるかを記載。 「脆弱性」の場合、クラウドがその脆弱性を含んでいる場合に影響を及ぼす可能性があるという観点から一覧に記載している。よってクラウドへの影響がなかった可能性もある。
発生箇所	インシデントまたは脆弱性が発生した箇所。
報告書との対応	クラウドサービスのサプライチェーンリスクマネジメント調査報告書「図表3-1-2：SaaSに係るITサプライチェーン上のリスク所在のイメージ」上のインシデントまたは脆弱性情報に付与されている番号。
概要	インシデントまたは脆弱性の概要。 公開されている情報からわかったことのみを記載。不明確な情報は記載していない。
公表年	インシデントまたは脆弱性の公表年。
発覚の経緯	インシデントまたは脆弱性が発覚した経緯。 脆弱性の場合は「－」。 公開されている情報からわかったことのみを記載。不明確な情報は記載していない。 公開情報から確認できなかった場合は「－」。
原因	インシデントまたは脆弱性が発覚した経緯を記載。 公開されている情報からわかったことのみを記載。不明確な情報は記載していない。 公開情報から確認できなかった場合は「－」。
被害内容	インシデントまたは脆弱性による被害の内容。 公開されている情報からわかったことのみを記載。不明確な情報は記載していない。 公開情報から確認できなかった場合は「－」。
対応内容	インシデントまたは脆弱性に対する対応内容を記載。 公開されている情報からわかったことのみを記載。不明確な情報は記載していない。 公開情報から確認できなかった場合は「－」。
再発防止策	インシデントまたは脆弱性に対する再発防止策を記載。 公開されている情報からわかったことのみを記載。不明確な情報は記載していない。 公開情報から確認できなかった場合は「－」。

本資料及び調査報告書は以下のURLで入手可能です。

https://www.ipa.go.jp/security/fy2021/reports/scrm/index-cloud.html　（2022年5月31日確認）