

# 被害



前提:

個別システムとなっていた経理システムを、クラウド上に統合基盤として再構築した。

被害:

公開前の決算情報が漏洩していることが判明した

#経理部門 #決算情報 #情報漏洩

# 原因：アカウント管理不足により、不正アクセスされた

## 対策：

- ・不要なアカウントの棚卸しを実施
- ・クラウドの公開設定を社内のIPに限定
- ・アカウントの適切な権限設定

## 今回の経緯：

企業に恨みをもった経理部社員が退職

退職した経理社員のアカウントが削除されずそのまま放置されていた

退職した経理社員が、退職後クラウド上の経理システムにアクセスしたところ、インターネット上からアクセス可能であった

経理システムにアクセスし、公開前の決算情報のデータをダウンロード

退職者が競合企業に公開前の決算情報のデータを売買した

# 被害



前提:

個別システムとなっていた経理システムを、クラウド上に統合基盤として再構築した。

被害:

公開前の決算情報が漏洩していることが判明した

#経理部門 #決算情報 #情報漏洩

# 原因：クラウドの公開設定に誤りがあった

対策：

- ・不要なアカウントの棚卸しを実施
- ・クラウドの公開設定を社内のIPに限定
- ・アカウントの適切な権限設定

今回の経緯：

攻撃者が会社についてインターネット上を調査

クラウドの公開設定がインターネットからも閲覧できるよう設定されてた

経理システムにアクセスし、公開前の決算データをダウンロード

攻撃者がインターネット上にデータを漏洩させた

# 被害



前提:

個別システムとなっていた経理システムを、クラウド上に統合基盤として再構築した。

被害:

公開前の決算情報が漏洩していることが判明した

#経理部門 #決算情報 #情報漏洩

# 原因：多要素認証を設定していなかった

対策：

- ・多要素認証を設定する
- ・アカウントの適切な管理
- ・脆弱なパスワードを設定しない

今回の経緯：

他国にある子会社が不正アクセスされ、アカウント情報が盗まれた

盗まれたアカウントを用いて、日本のクラウド上にある経理システムにアクセス

経理システムから公開前の決算情報をダウンロード

決算情報をSNS上に漏洩させた

# 被害



前提:

個別システムとなっていた経理システムを、クラウド上に統合基盤として再構築した。

被害:

公開前の決算情報が漏洩していることが判明した

#経理部門 #決算情報 #情報漏洩

# 原因：脆弱なパスワードが設定されていた

## 対策：

- ・多要素認証を設定する
- ・アカウントの適切な管理
- ・脆弱なパスワードを設定しない

## 今回の経緯：

攻撃者に買収された派遣社員が経理システムに管理者としてログインしたところ、脆弱なパスワードだったためログインが可能であった

経理システムから公開前の決算情報をダウンロード

攻撃者に情報を提供した



# 被害



前提:

個別システムとなっていた経理システムを、クラウド上に統合基盤として再構築した。

被害:

公開前の決算情報が漏洩していることが判明した

#経理部門 #決算情報 #情報漏洩

# 原因：要件定義の不足により、システムに設計ミスがあった

対策：

- ・非機能要件含め要件定義を行う
- ・アカウントの適切な管理
- ・システムテストの結果を確認する

今回の経緯：

攻撃者がメンテナンス業者を装って社内に侵入

経理システムにアクセスし、データベースに対してSQLインジェクションを実施したところ、情報の窃取が可能だった

経理システムから公開前の決算情報を窃取した

# 被害



前提:

クラウド上で社員の個人情報  
を管理、人事情報を活用し  
人材育成を推進する。

被害:

社員の名前、住所、等級、所  
属部署などの情報が漏洩し  
ていることが判明した

#人事部門 #人事情報 #情報漏洩

# 原因：多要素認証を設定していない

## 対策：

- ・ID・パスワードを誰でも見える場所に置かない
- ・クラウドにログインできる端末を制限する
- ・多要素認証を使用する

## 今回の経緯：

会社に恨みをもった社員が復讐に使えるような情報を探し社内ホームページを探索

人事部のページでクラウド上の人事管理支援システムのID・パスワードが記載されたファイルを発見

システムにアクセスしデータを持ち出した

# 被害



前提:

クラウド上で社員の個人情報  
を管理、人事情報を活用し  
人材育成を推進する。

被害:

社員の名前、住所、等級、所  
属部署などの情報が漏洩し  
ていることが判明した

#人事部門 #人事情報 #情報漏洩

# 原因：ローカルに社員情報を保存していた

対策：

機微な情報は自身の端末に保存しない

業務に関係のないサイトは見ない

ウイルス感染が疑われる場合はネットワークから隔離する

今回の経緯：

社員の一人が会社の端末でネットショッピングをしていると悪意のあるサイトにアクセスしてしまった。

その後、ウイルス感染した旨のポップアップが表示

ポップアップに書かれていた偽のサポートセンターに連絡

修理と偽り遠隔操作される

作業のためにエクスポートしていたものを盗み見られて漏洩

# 被害



前提:

クラウド上で社員の個人情報  
を管理、人事情報を活用し  
人材育成を推進する。

被害:

社員の名前、住所、等級、所  
属部署などの情報が漏洩し  
ていることが判明した

#人事部門 #人事情報 #情報漏洩

# 原因：インターネットからアクセスできる設定だった

対策：

無関係の人物から見られる場所で業務をしない

インターネットからアクセスできないようにする

多要素認証を使用する

今回の経緯：

悪意を持った人物がカフェでテレワークしていた社員を発見

クラウドにログインするところを盗撮

後日盗撮された情報をもとにログインされ、情報が流出した



# 被害



前提:

クラウド上で社員の個人情報  
を管理、人事情報を活用し  
人材育成を推進する。

被害:

社員の名前、住所、等級、所  
属部署などの情報が漏洩し  
ていることが判明した

#人事部門 #人事情報 #情報漏洩

# 原因：ID、パスワードがデフォルトのままだった

対策：

初回起動時のパスワード変更を義務化する  
脆弱なパスワードを設定できないようにする

ログイン試行回数を設ける

情報をエクスポートできない設定にする

今回の経緯：

ID、パスワードが初期設定から変更されておらず、容易に想像できるものであったため、人事管理支援システムへのログインに成功  
システムに保存されていた情報をエクスポートし盗みだした。

# 被害



前提:

クラウド上で社員の個人情報  
を管理、人事情報を活用し  
人材育成を推進する。

被害:

社員の名前、住所、等級、所  
属部署などの情報が漏洩し  
ていることが判明した

#人事部門 #人事情報 #情報漏洩

# 原因：要件定義の不足による Webシステム上の設計ミス

対策：

非機能要件含め要件定義を行う  
アカウントの適切な管理  
システムテストの結果を確認する

今回の経緯：

攻撃者がメンテナンス業者を装って社内に  
侵入

人事管理支援システムにアクセスし、データ  
ベースに対してSQLインジェクションを実施  
したところ、情報の窃取が可能だった  
システムから社員情報を窃取された

被害



## 前提：

取引先管理、ナレッジ蓄積のため、クラウド上に営業支援システムを構築した。

**被害:**

取引先の情報(会社名、取引データ、担当窓口等)が漏洩していることが判明した

#營業部門 #取引先 #情報漏洩

# 原因：クラウドへのアクセス 権限の設定不備

## 対策：

クラウドへのアクセス権限は業務上必要な  
範囲で権限を付与するように再設定する  
外部リンクへアクセスしないよう教育する

## 今回の経緯：

アクセス制限がかけられておらず、IPアドレ  
スやドメイン名を入力すればどこからでもア  
クセスできるようになっていた。

管理者アカウントのID PWが一般的なもの  
になっており、容易に予測できるものであっ  
た。

# 被害



前提:

取引先管理、ナレッジ蓄積のため、クラウド上に営業支援システムを構築した。

被害:

取引先の情報(会社名、取引データ、担当窓口等)が漏洩していることが判明した

#営業部門 #取引先 #情報漏洩

**原因：漏えいした認証情報で  
不正侵入され、情報を窃取**

**対策：**

**多要素認証を設定する**

**不審なメールを開かない訓練を実施する**

**今回の経緯：**

**営業社員がフィッシングメールに引っ掛かってしまった。**

**営業社員のPCがマルウェアに感染し、営業社員のIDパスワードを窃取された**



# 被害



前提:

取引先管理、ナレッジ蓄積のため、クラウド上に営業支援システムを構築した。

被害:

取引先の情報(会社名、取引データ、担当窓口等)が漏洩していることが判明した

#営業部門 #取引先 #情報漏洩

# 原因：営業社員がお金をもらって取引先情報を売った

対策：

クラウド上のファイルをローカルにダウンロードできないように設定する

業務に関係のないサイトは見ない

ウイルス感染が疑われる場合はネットワークから隔離する

機微な情報は自身の端末に保存しない

今回の経緯：

営業社員の一人が待遇に不満を持っていたところ、競合他社から情報買取の相談があり、問題の営業社員は取引先情報を売った。

# 被害



前提:

取引先管理、ナレッジ蓄積のため、クラウド上に営業支援システムを構築した。

被害:

取引先の情報(会社名、取引データ、担当窓口等)が漏洩していることが判明した

#営業部門 #取引先 #情報漏洩

**原因：クラウドシステムで利用しているミドルウェアの脆弱性を悪用された**

**対策：**  
**責任分界点を明確にする**

**今回の経緯：**

システム担当者側は、クラウドシステムで利用しているミドルウェアのパッチ適用はベンダー側で実施する認識、ベンダー側は利用者側の指示で実施する認識だった。両社ともミドルウェアの脆弱性を確認していなかった。

結果、サイバー攻撃の標的となってしまうクラウド上に存在する情報が漏洩してしまった

# 被害



前提:

取引先管理、ナレッジ蓄積のため、クラウド上に営業支援システムを構築した。

被害:

取引先の情報(会社名、取引データ、担当窓口等)が漏洩していることが判明した

#営業部門 #取引先 #情報漏洩

# 原因：パスワードルールを設定しなかった

対策：

脆弱なパスワードを設定できないようにする

ログイン試行回数を設ける

今回の経緯：

ユーザがパスワードを設定する際に、文字数や文字の種類を指定しておらず、脆弱なパスワードとなっていた。

また、ログインの試行回数も設けられておらず、総当たり攻撃でパスワードクラックされた。

脆弱なパスワードが突破されてしまった

# 被害



前提:

不審者侵入検知を目的に工場内各所に導線解析を行うクラウド型IoTカメラを導入

被害:

工場内の社員配置や不在時間などがわかる情報がリアルタイムに公開されていた。

#工場 #IoTカメラ #情報漏洩

# 原因：クラウドの公開範囲が不適切

対策：

- ・クラウドの接続元IPのフィルタ
- ・ID PWを予測しづらいものに変更しておく

今回の経緯：

アクセス制限がかけられておらず、IPアドレスやドメイン名を入力すればどこからでもアクセスできるようになっていた。

管理者アカウントのID PWが一般的なものになっており、容易に予測できるものであった。



# 被害



前提:

不審者侵入検知を目的に工場内各所に導線解析を行うクラウド型IoTカメラを導入

被害:

工場内の社員配置や不在時間などがわかる情報がリアルタイムに公開されていた。

#工場 #IoTカメラ #情報漏洩

# 原因：PWの入力が不要な状態であった

対策：

- ・ログイン画面を設ける
- ・定期的に侵害をチェック

今回の経緯：

カメラにアクセスする際にPWなどの入力が不要であったため

インターネット上でカメラの映像が公開され、常に閲覧できる状態であった

# 被害



前提:

不審者侵入検知を目的に工場内各所に導線解析を行うクラウド型IoTカメラを導入

被害:

工場内の社員配置や不在時間などがわかる情報がリアルタイムに公開されていた。

#工場 #IoTカメラ #情報漏洩

# 原因：データの暗号化が不十分であった

対策：

データ送信において暗号化機能のあるカメラを利用

今回の経緯：

録画データを社内の専用ネットワークからクラウド上にアップロードする

導線解析はクラウド上のアプリで行われ、各従業員の端末から不審な動きをしている人物や異常に写り込みが多い人物を照会することができる

# 被害



前提:

不審者侵入検知を目的に工場内各所に導線解析を行うクラウド型IoTカメラを導入

被害:

工場内の社員配置や不在時間などがわかる情報がリアルタイムに公開されていた。

#工場 #IoTカメラ #情報漏洩

**原因：カメラが設置されており組織外のものであった**

**対策：**

**資産管理の徹底**

**通報の仕組みを構築する**

**今回の経緯：**

**カメラの設置や保守は外部ベンダに一任しており、常連のベンダであったことから設置時の立ち会いなどは実施していなかった**

**そのため具体的なカメラの台数や設置箇所は把握しておらず、クラウド上で分析された不審者の情報を閲覧するのみの利用方法となっている**

# 被害



前提:

不審者侵入検知を目的に工場内各所に導線解析を行うクラウド型IoTカメラを導入

被害:

工場内の社員配置や不在時間などがわかる情報がリアルタイムに公開されていた。

#工場 #IoTカメラ #情報漏洩

**原因：多要素認証を設定していない**

**対策：**  
**他要素認証を設定する**  
**PWの運用ルールを徹底**

**今回の経緯：**  
**IDとパスワードのみの認証方式を採用しており、付箋に書いてある情報からログインが成功した**



# 被害



前提:

工場設備の予兆保全を目的に、クラウドでデータ分析をする振動センサを導入した。

被害:

振動センサーのデータが漏洩していることが判明した。

#工場向け #予兆保全 #情報漏洩

# 原因：クラウドの公開範囲の設定に誤りがあった

対策：

- ・アクセス制御
- ・外部リンクへアクセスしないよう教育する

今回の経緯：

保全課では新たにクラウド環境を契約し、  
予兆保全の分析環境を構築した

クラウドシステムを導入した実績をベンダー  
のHPに掲載

標的型攻撃メールでIDとPWを入力してし  
まった結果、データ分析に関わるデータ、運  
転データ等が漏洩した

# 被害



前提:

工場設備の予兆保全を目的に、クラウドでデータ分析をする振動センサを導入した。

被害:

振動センサーのデータが漏洩していることが判明した。

#工場向け #予兆保全 #情報漏洩

# 原因：通信経路におけるデータの暗号化の未実施

対策：

- ・暗号化機能のあるセンサーを導入
- ・物理的侵入の管理
- ・不審端末パトロール

今回の経緯：

株価操作のため攻撃者が金で雇われた  
攻撃者がメンテナンス業者を装って工場に  
侵入

工場の中に攻撃端末を設置。

攻撃端末からセンサーとクラウド間の通信  
を窃取

データが流出

# 被害



前提:

工場設備の予兆保全を目的に、クラウドでデータ分析をする振動センサを導入した。

被害:

振動センサーのデータが漏洩していることが判明した。

#工場向け #予兆保全 #情報漏洩

# 原因：不正なりモートアクセスによりサーバに接続された

対策：

- ・ポートを制限する
- ・業者を一人にせず監視する
- ・脆弱なPWを設定しない
- ・権限管理

今回の経緯：

悪意のあるメンテナンス業者がPCをネットワークに接続し、リモートアクセスを試行。

ポートが開放されており、一般的PW等を入力したところログインに成功

サーバ内の全てのファイルにアクセスすることができた。

# 被害



前提:

工場設備の予兆保全を目的に、クラウドでデータ分析をする振動センサを導入した。

被害:

振動センサーのデータが漏洩していることが判明した。

#工場向け #予兆保全 #情報漏洩

# 原因：パスワードルールを設定してなかった

## 対策：

- ・脆弱なパスワードを設定できないようにする
- ・ログイン試行回数を設ける

## 今回の経緯：

ユーザがパスワードを設定する際に、文字数や文字の種類を指定しておらず、脆弱なパスワードとなっていた。

また、ログインの試行回数も設けられておらず、総当たり攻撃でパスワードクラックされた。

脆弱なパスワードが突破されてしまった



# 被害



前提:

工場設備の予兆保全を目的に、クラウドでデータ分析をする振動センサを導入した。

被害:

振動センサーのデータが漏洩していることが判明した。

#工場向け #予兆保全 #情報漏洩

# 回答：物理侵入しセンサーを紛失

対策：

- ・運用ルールを決める
- ・物理侵入対策
- ・資産管理の徹底

今回の経緯：

運用ルールや設置箇所が明確にされておらず、データ漏洩の事実が発覚後にセンサーの紛失が発覚した

センサーの所在は不明であり、最終的に第三者の手に渡ったと考えられる

# 被害



前提:

工場設備の予兆保全を目的に、クラウドでデータ分析をする振動センサを導入した。

被害:

振動センサーのデータが漏洩していることが判明した。

#工場向け #予兆保全 #情報漏洩

# 回答：多要素認証を設定していない

対策：

- ・他要素認証を用いる
- ・付箋を貼らない

今回の経緯：

IDとパスワードのみの認証方式を採用しており、付箋に書いてある情報からログインが成功した

# 被害



前提:

最適化運転のためにIoTセンサーを工場に大量設置

クラウド上で制御監視を実現

被害:

センサー値を不正改ざんされ、  
異常の発見が遅れ、工場の  
安全計装が作動し緊急停止。

#データ改ざん #工場 #停止

# 原因：クラウドの公開範囲の設定に誤りがあった

対策：

公開範囲を限定的なものとする  
脆弱性情報を収集し常に対策する

今回の経緯：

設定ミスのため、公開範囲が変更されていた

公開されている情報を元にデータの改ざんを試みた

クラウドシステム上に脆弱性がありデータの改ざんに成功した

# 被害



前提:

最適化運転のためにIoTセンサーを工場に大量設置  
クラウド上で制御監視を実現

被害:

センサ値を不正改ざんされ、  
異常の発見が遅れ、工場の  
安全計装が作動し緊急停止。

#データ改ざん #工場 #停止

# 原因：通信経路におけるデータの暗号化の未実施

対策：

通信の暗号化

不審端末対応のため資産管理

セキュリティポリシーの見直し

今回の経緯：

不正無線LANが設置されていた。

メンテナンス業者を装い、工場内に攻撃端末が設置された

通信経路の暗号化がされていないことに伴う中間者攻撃でデータが書き換えられてしまった

セキュリティ方針やポリシーにデータ暗号化の規定が含まれていなかったため

データの暗号化に関する知識や理解が不足していたため



# 被害



前提:

最適化運転のためにIoTセンサーを工場に大量設置  
クラウド上で制御監視を実現

被害:

センサ値を不正改ざんされ、  
異常の発見が遅れ、工場の  
安全計装が作動し緊急停止。

#データ改ざん #工場 #停止

# 原因：不正なリモートアクセスによりサーバに接続された

対策：

パスワードポリシーの適用

ソフトウェアやファームウェアの更新を定期的に行う

多要素認証を導入

従業員教育を実施する

今回の経緯：

設定されているパスワードが弱く、容易に推測可能だった。

リモートアクセスの設定が不適切で、外部からのアクセスが許可されていた。

社内端末からIoT管理画面にアクセスされ、不正操作を施行される。

サーバやIoTセンサのファームウェアやソフトウェアに既知の脆弱性が存在

工場の従業員や管理者が偽のログインページに認証情報を入力した

一度侵入されると他のシステムにも容易にアクセスできた。

# 被害



前提:

最適化運転のためにIoTセンサーを工場に大量設置  
クラウド上で制御監視を実現

被害:

センサ値を不正改ざんされ、  
異常の発見が遅れ、工場の  
安全計装が作動し緊急停止。

#データ改ざん #工場 #停止

# 原因：パスワードルールを設定しなかった

対策：

パスワードポリシーの強制  
セキュリティ教育

今回の経緯：

IoT機器管理画面に不正アクセスされ、  
IoT機器が不正な動作をするようになった。  
セキュリティ意識が低く、パスワードルールの必要性が認識されていなかった。

サーバやIoTセンサに攻撃者が総当り攻撃  
や辞書攻撃を実行し、認証情報を取得。

脆弱なパスワード利用に伴う個人情報の流出

脆弱なパスワード流出に伴う管理者権限の流出

# 被害



前提:

最適化運転のためにIoTセンサーを工場に大量設置  
クラウド上で制御監視を実現

被害:

センサー値を不正改ざんされ、  
異常の発見が遅れ、工場の  
安全計装が作動し緊急停止。

#データ改ざん #工場 #停止

# 原因：物理侵入しセンサーを紛失

対策：

入館管理システムの導入

監視カメラと警報システムの設置

教育 意識向上

物理セキュリティの強化

資産管理の徹底

今回の経緯：

常に空いている窓が存在し、そこから工場に侵入され、センサー類を盗難された

工場の物理セキュリティが不十分であり、入退室管理システムが導入されていなかったため、従業員を装い侵入され、センサー類が盗難された。

物理セキュリティに対する投資が優先されていなかったため。

経営陣が物理セキュリティの重要性を十分に認識していなかったため。

# 被害



前提:

最適化運転のためにIoTセンサーを工場に大量設置

クラウド上で制御監視を実現

被害:

センサー値を不正改ざんされ、  
異常の発見が遅れ、工場の  
安全計装が作動し緊急停止。

#データ改ざん #工場 #停止

# 原因：多要素認証を設定していない

対策：

全社的なセキュリティ教育の実施

多要素認証実装計画の立案、承認

多要素認証の実装

多要素認証の実装を行うためのポリシーの策定

今回の経緯：

経営陣がセキュリティリスクを十分に認識されておらず、IDとパスワードのみの認証方式が採用されていた。

IoT機器管理画面には、ブラウザに記憶されていたID、パスでログインができた。

セキュリティに関する教育や情報共有が不足していた

認証システムの脆弱さにより、パスワード流出の際にすぐに不正なアクセスが見られた