2024 年5 月 24日

お客様各位

社会保険労務士法人出口事務所
代表社員　篠木裕美

情報セキュリティ調査および対応策に関する報告書（2024 年5 月 24日現在）

このたびは、関係者の皆様に多大なご迷惑をお掛けしておりますことを、深くお詫び申し上げます。

昨年６月に発生しました株式会社エムケイシステムのシステム障害に関して、調査および対応策の現状を以下の通りご報告申し上げます。

また、社会保険労務士法人出口事務所の情報セキュリティ調査および対応策を以下の通りご報告申し上げます。

なお、本事案は情報セキュリティに関するものであり、本報告書においても重要な情報が部分的に含まれていることから弊事務所内においても厳秘扱いとしています。貴社におかれましても、本書面の取り扱いには充分注意頂き、関係者以外には一切漏洩することがないよう、厳密な管理をお願い申し上げます。

1. 株式会社エムケイシステムのセキュリティ対応策

株式会社エムケイシステムのセキュリティ対応策については、資料１「個人情報保護委員会からの指導、報告の求めに対応したセキュリティ対応策について」をご参考ください。

また、新たなセキュリティ対策に関する報告が発表されましたら随時、弊事務所ホームページに掲載させていただきます。

最終的なセキュリティ対策に関する報告が発表されましたら、改めてご報告させていただきます。

2. 社会保険労務士法人出口事務所の情報セキュリティ調査および対応策

社会保険労務士法人出口事務所の情報セキュリティ調査および対応策については、資料２「情報セキュリティ、個人情報保護の体制」をご参考ください。

ただし、情報セキュリティ、個人情報保護の体制に終わりはありません。引き続き、専門家による調査の実施、アドバイスにより対応をしましたら、随時、弊事務所ホームページに掲載させていただきます。

以上

資料１

個人情報保護委員会からの指導、報告の求めに対応したセキュリティ対応策について

2024年5月17日

MKSYSTEM
Professional Internet Solution System

01.

個人情報保護委員会からの
行政指導について

3月25日　個人情報保護委員会から　指導・報告等の求め

貴社の個人情報等の取扱いに関し、下記1のとおり個人情報の保護に関する法律（平成15年法律第57号。以下「法」という。）第147条の規定により指導し、下記2のとおり法第146条第1項の規定により報告等を求める。

１．法第147条の規定による指導

（指導の趣旨）
当委員会に提出された漏えい等報告書（受付番号377997060121)に係る漏えい等事案に関し、貴社における個人データの取扱いについて、法第23条に規定する個人データの安全管理のために必要かつ適切な措置のうち、個人情報の保護に関する法律についてのガイドライン（通則編）「10（別添）講ずべき安全管理措置の内容」に示す技術的安全管理措置(10-6 (2)アクセス者の識別と認証及び(3)外部からの不正アクセス等の防止）に不備が認められた。

（指導の内容）
（１）上記の指導の趣旨を踏まえ、法第23条及びガイドラインに基づき、必要かつ適切な措置を講ずること
（２）再発防止のための措置を確実に実施するとともに、爾後、適切に運用し（必要に応じて見直すことを含む。）、継続的にその取り扱う個人データの漏えい等の防止その他の個人データの安全管理のために必要かつ適切な措置を講ずること。

3月25日　個人情報保護委員会から　指導・報告等の求め

１．法第147条の規定による指導

（指導の趣旨）
当委員会に提出された漏えい等報告書（受付番号377997060121)に係る漏えい等事案に関し、貴社における個人データの取扱いについて、**法第23条に規定する個人データの安全管理**のために必要かつ適切な措置のうち、**個人情報の保護に関する法律についてのガイドライン（通則編）「10 講ずべき安全管理措置の内容」**に示す技術的安全管理措置(10-6 (2)アクセス者の識別と認証及び(3)外部からの不正アクセス等の防止）に不備が認められた。

個人情報の保護に関する法律についてのガイドライン（通則編）（抄）
3-4-2安全管理措置（法第23条関係）

個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又は毀損（以下「漏えい等」という。）の防止その他の個人データの安全管理のため、必要かつ適切な措置を講じなければならないが、当該措置は、個人データが漏えい等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の規模及び性質、個人データの取扱状況（取り扱う個人データの性質及び量を含む。）、個人データを記録した媒体の性質等に起因するリスクに応じて、必要かつ適切な内容としなければならない。

3月25日　個人情報保護委員会から　指導・報告等の求め

（指導の趣旨）
当委員会に提出された漏えい等報告書（受付番号377997060121)に係る漏えい等事案に関し、貴社における個人データの取扱いについて、法第23条に規定する個人データの安全管理のために必要かつ適切な措置のうち、個人情報の保護に関する法律についてのガイドライン（通則編）「10　講ずべき安全管理措置の内容」に示す**技術的安全管理措置(10-6 (2)アクセス者の識別と認証及び(3)外部からの不正アクセス等の防止）**に不備が認められた。

10-6　技術的安全管理措置

個人情報取扱事業者は、情報システム（パソコン等の機器を含む。）を使用して個人データを取り扱う場合（インターネット等を通じて外部と送受信等する場合を含む。）、技術的安全管理措置として、次に掲げる措置を講じなければならない。（中略）

(2)アクセス者の識別と認証

個人データを取り扱う情報システムを使用する従業者が正当なアクセス権を有する者であることを、識別した結果に基づき認証しなければならない。

(3)外部からの不正アクセス等の防止

個人データを取り扱う情報システムを外部からの不正アクセス又は不正ソフトウェアから保護する仕組みを導入し、適切に運用しなければならない。

3月25日　個人情報保護委員会から　指導・報告等の求め

（指導の内容）

(1)上記の指導の趣旨を踏まえ、法第23条及びガイドラインに基づき、必要かつ適切な措置を講ずること。
(2)再発防止のための措置を確実に実施するとともに、爾後、適切に運用し（必要に応じて見直すことを含む。）、継続的にその取り扱う個人データの漏えい等の防止その他の個人データの安全管理のために必要かつ適切な措置を講ずること。

法第146条第1項の規定による報告等の求め

（要求の理由）
上記の「（指導の内容）(1)及び（2)」の事項について、貴社が講じた措置を当委員会において確認する必要があるため。

（要求の内容）
上記の**「（指導の内容）(1)及び（2)」の事項について講じた措置（予定も含む。）**を、関係資料を添付の上、**令和6年4月26日（金）までに報告**するよう求める。

4月23日　弊社から個人情報保護委員会への報告内容（概要）

１．「アクセス者の識別と認証」に関する措置
(ア)パスワード再設定
(イ)パスワードポリシー強化
(ウ)不要アカウントの削除
(エ)デバイス認証の開始

２．「外部からの不正アクセス等の防止」に関する措置
(ア)ソフトウェアの更新管理の徹底（自動化・省力化による迅速な適用）
(イ)安全な環境でのログの長期保管
(ウ)WAF(ウェブアプリケーションファイアーウォール)ルールの見直し

３．「再発防止のための措置を確実に実施するとともに、爾後、適切に運用し（必要に応じて見直すことを含む。）、継続的にその取り扱う個人データの漏えい等の防止その他の個人データの安全管理のために必要かつ適切な措置を講ずること。）」に関する措置。
(ア)ふるまい検知EDRの導入とSOCによる監視
(イ)ペネトレーションテストの定期的実施（年2回）
(ウ)情報セキュリティの外部専門家とアドバイザリー契約の締結

02.

再発防止に向けたセキュリティ強化対策
（個人情報保護委員会への報告）

セキュリティ対策強化の観点：CIS Control Version 8

調査で確認された原因を踏まえ、**米国CIS（Center for Internet Security）が定義する、CIS Controls（V8）**をベースに抜本的対策を開始しました。

Control 01. 組織の資産のインベントリと管理

Control 02. ソフトウェア資産のインベントリと管理

Control 03. データ保護

Control 04. 組織の資産とソフトウェアの安全な構成

Control 05. アカウント管理

Control 06. アクセス制御管理

Control 07. 継続的な脆弱性管理

Control 08. 監査ログ管理

Control 09. 電子メールとWebブラウザの保護

Control 10. マルウェアの防御

Control 11. データ復旧

Control 12. ネットワークインフラストラクチャ管理

Control 13. ネットワークの監視と防御

Control 14. セキュリティ意識向上とスキルのトレーニング

Control 15. サービスプロバイダーの管理

Control 16. アプリケーションソフトウェアセキュリティ

Control 17. インシデントレスポンスと管理

Control 18. ペネトレーションテスト

CIS Control の運用に向けた環境準備の進捗状況①

項目	タイトル	項目数	IG1	IG2	IG3
Control 1	組織の資産のインベントリと管理	5	2	2	1
Control 2	ソフトウェア資産のインベントリと管理	7	4	2	1
Control 3	データ保護	14	6	6	1
Control 4	組織の資産とソフトウェアの安全な構成	12	7	4	1
Control 5	アカウント管理	6	4	2	0
Control 6	アクセス制御管理	8	5	2	1
Control 7	継続的な脆弱性管理	7	4	3	0
Control 8	監査ログ管理	12	3	8	1
Control 9	電子メールとWebブラウザの保護	7	2	4	1
Control 10	マルウェアの防御	7	3	4	0
Control 11	データ復旧	5	3	0	0
Control 12	ネットワークインフラストラクチャ管理	8	1	6	1
Control 13	ネットワークの監視と防御	11	0	6	5

CIS Control の運用に向けた環境準備の進捗状況②

項目	タイトル	項目数	IG1	IG2	IG3
Control 14	セキュリティ意識向上とスキルのトレーニング	9	8	1	0
Control 15	サービスプロバイダーの管理	7	1	3	2
Control 16	アプリケーションソフトウェアセキュリティ	14	0	11	2
Control 17	組織の資産とソフトウェアの安全な構成	9	3	5	0
Control 18	ペネトレーションテスト	5	0	3	1

	IG1	IG2	IG3
総数	**57**	**130**	**153**
対応済	**56**	**128**	**146**
進捗	**98.2%**	**98.5%**	**95.4%**

2024年3月末時点です

AWSサービスをフル活用　ネットワークセキュリティの全般的強化

AWS WAF

Web Application Firewall

従来のファイアウォールやIDS/IPSで防ぐことが
出来ない攻撃からwebアプリケーションを防御する。

Amazon
Detective

Detective

セキュリティに関する検出結果や疑わしいアクティビティの根本原因を分析、調査、および迅速に特定。Detective は、AWS リソースからログデータを自動的に収集し、機械学習、統計分析、グラフ理論を使用して、セキュリティ調査を迅速かつ効率的に行う。

Amazon
GuardDuty

GuardDuty

処理状況をモニタリングして悪意のあるアクティビティがないか確認、セキュリティ検出結果を提供する脅威検出サービス。
潜在的なセキュリティ脅威(バックドア、ポートスキャン、マルウェア) を検知。

AWS Config

Config

AWSアカウントにあるAWSリソースの設定を評価。監査、審査出来るサービス。AWSリソースの設定ミスを検知。

AWS Certificate
Manager

Certificate Manager (ACM)

AWSで使用するパブリックおよびプライベート SSL/TLS 証明書のプロビジョニング、管理、展開。ACMにより、SSL/TLS 証明書のアップロード、更新等の面倒なプロセスを手動で行う必要がなくなる。

Amazon
CloudWatch

CloudWatch

アプリケーションを監視し、パフォーマンスの変化に対応し、リソースの使用を最適化し、運用状況を管理。仮想サーバーのCPU使用率、Diskの読み書き回数、インターフェースの通信量など、仮想サーバーの代表的な監視項目は予め用意されている。

AWS
IAM

Identity and Access Management

「認証」と「認可」の設定を行うサービス。「認証」「認可」を正しく設定することで、AWSの利用者や、AWSのサービスがアクセスできる範囲を制御。

AWS System
Manager

System Manager

環境内のリソースをセキュアかつ効率よく運用するための管理ソリューション
ソフトウェア更新管理の自動化

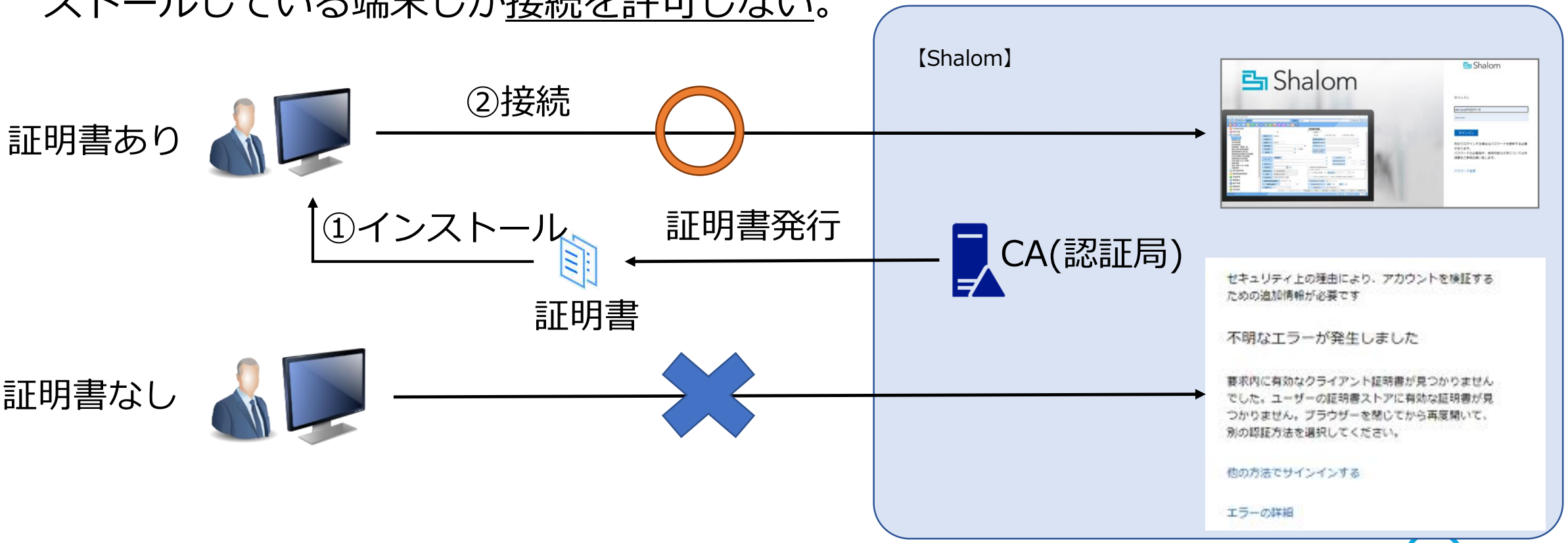
稼働後に実施した主なセキュリティ対策

No	対策内容	詳細
1	ネットワークセキュリティ対策の強化	**AWSのセキュリティ機能をフル活用 ＋多要素認証の追加**
2	エンドポイントセキュリティ対策強化	**ウィルス対策ソフト ＋ふるまい検知EDR（SOC）**
3	OS及びソフトウェアの更新管理の徹底	**自動化、省力化による Update適用期間の縮小**
4	ペネトレーションテスト（脆弱性検査等）の定期的な実施	**新規リリース時＆年2回の定期実施**
5	リスクアセスメント、情報セキュリティ監査の定期的な実施	**テーマごとに毎月実施**
6	情報セキュリティの運用体制見直し（情報セキュリティ専門家活用）	**外部専門家とのアドバイザリー契約**
7	情報セキュリティインシデントに対する体制整備（CSIRT構築運用）	**分散型CSIRT （インシデント発生時のみ活性化）**
8	従業員に対するセキュリティ教育（定期的な啓発活動）	**役割別、階層別教育内容への転換**
9	事業継続計画（IT-BCP）の見直し	**AWS基盤に応じた計画の立案・実行へ**

多要素認証の導入　CA（証明書）認証

CA認証による現状社労夢の多要素認証（2024年2月14日から稼働予定）

Shalom環境であらかじめ社労夢に接続する端末に**証明書を配布**し、その証明書をインストールしている端末しか接続を許可しない。

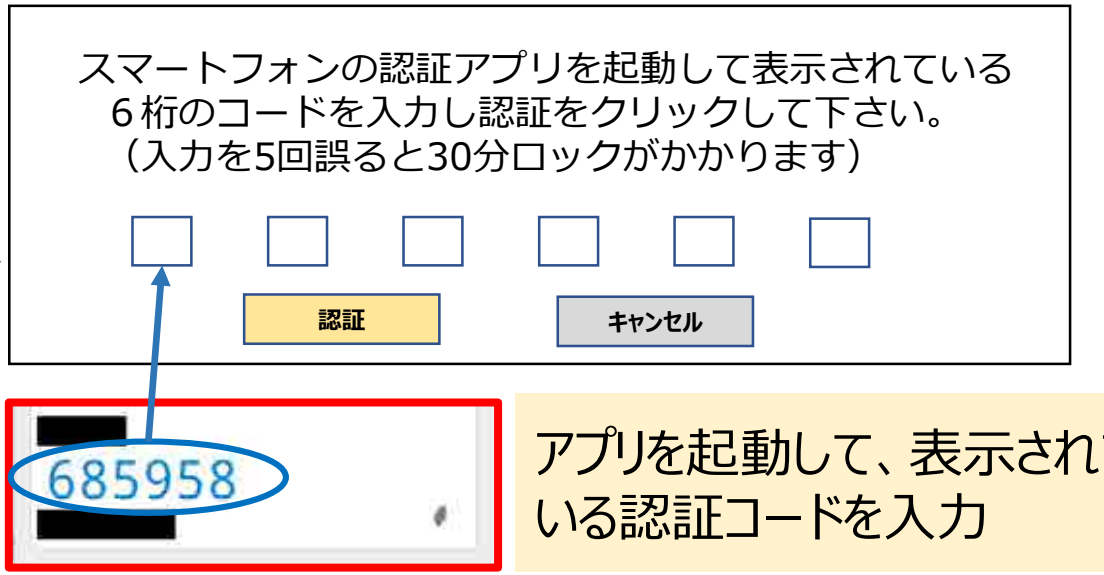


仮想デバイス認証によるWEB化システムの２要素認証

（2024年4月以降提供開始予定）

【仮想デバイス認証とは】

スマートフォン上で６桁の乱数を発生し、WEBシステムログイン時に確認されるダイアログに発行される6桁の数字を入力することで、接続元の正当性を検証する。



「ログイン」ボタンのクリック時に、ID・PWが**正しかった場合**は、仮想デバイス認証の入力画面が表示される。
(ID・PWに誤りがある場合は従来通りのメッセージ)

アプリを起動して、表示されている認証コードを入力

EDRの導入①　（2023年6月導入済）

EDR（Endpoint Detection and Response）とは、ユーザーが利用するパソコンやサーバ（エンドポイント）における不審な挙動を検知し、迅速な対応を支援するセキュリティソリューションです。

	EDR（2023年6月導入済）	アンチウィルス（継続して利用）
目的	**●事後対策** マルウェアに感染した後の被害を最小化する	**●事前対策** マルウェアに感染しないようにする
仕組み	**● エンドポイントの監視** エンドポイントにある各デバイスにエージェントを組み込み、エージェントから吸い上げた情報を常時監視。	**● パターンマッチング方式による検出** マルウェアに見られるデータのパターンをウイルス定義ファイルに登録し、コンピュータ上のファイルに同様のデータパターンがないか、コンピュータをスキャンして調べる。
強み（特長）	ウイルス定義ファイルが不要。検知するのは異常や不審な挙動であるため、**未知の脅威であっても対応**できる。	ウイルス定義ファイルに登録済みの既知の脅威は、ほぼ確実に検出できる。

パターンマッチング方式で対応出来ない
全く未知の脅威に対応します

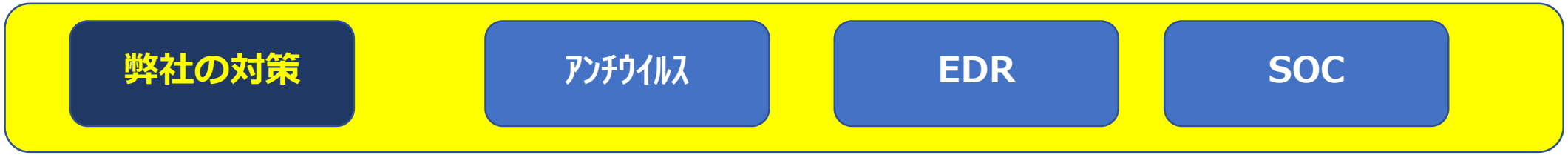
EDRの導入②　（2023年6月導入済）

振る舞い検知（EDRの特長）

パターンマッチング方式では、マルウェアの検体を入手し、ユーザのコンピュータをスキャンします。
ところが、亜種を含めるとマルウェアの新種が、1日に100万個から200万個も発見されている現状では、
パターンマッチング方式では、検体の入手と解析が追いつきません。
そこで、マルウェアのコードではなく、プログラムの振る舞い・挙動に着目し、不審な動作をするプログラムを
マルウェアと判定する「**振る舞い検知**」の仕組みが誕生しました。
振る舞い検知では、検体を必要としないため、これまで発見されたことがない**未知の脅威も検知**できます。

SOC

SOCとは「Security Operation Center 」の略称であり、**24時間365日体制**でネットワークやデバイス
を常時監視し、異常や不審な挙動が発生した場合には、管理者に通知したり、遮断します。



３つの機能の組み合わせで万全のセキュリティ対策

組織の強化　セキュリティ運用体制の見直し　2023年8月から順次実施

継続的な取り組み

専任化

デジタルアーキテクチャデザイン部 新設

・製品企画部インフラ担当を独立部門に昇格、増員
・外部より、セキュリティ専門家を部門長として採用
・セキュリティ専門企業とコンサル契約

関係者のリソース増員

CSIRT体制の強化

・社内規程制定　社長直下の組織化
・平常時と緊急時のCSIRT体制、役割の明文化

専門性強化

セキュリティプロジェクトMTGの定例化

・社内主要部門責任者＋デジタルアーキテクチャデザイン部のMTGを定例化
・外部セキュリティ専門家の参加
・CIS COTROL V8対応の進捗と各種セキュリティ施策の進捗を確認
・AWS社、iret社との定期、非定期MTG


MKSYSTEM
Professional Internet Solution System

資料２

社会保険労務士法人出口事務所

情報セキュリティ、個人情報保護の体制

2023年8月2日、
2024年5月15日、5月24日改定
社会保険労務士法人　出口事務所
代表社員　特定社会保険労務士　出口裕美

今日のテーマ

社会保険労務士法人出口事務所
情報セキュリティ、個人情報保護の体制

- はじめに
- １．システム障害等とは
- ２．出口事務所の情報セキュリティ、個人情報保護の体制
- さいごに

はじめに　社会保険労務士法人出口事務所

◆ ホームページ　https://www.deguchi-office.com/

◆ 東京オフィス
〒 169-0075
東京都新宿区高田馬場1-24-16　内田ビル３階
（JR線山手線/東京メトロ東西線　高田馬場駅　徒歩3分）

◆JR山手線「高田馬場」駅 早稲田口 徒歩3分
◆東京メトロ東西線「高田馬場」駅 5番出口 徒歩2分

◆ 栃木オフィス
〒 322-0002栃木県鹿沼市千渡1766-5

◆JR日光線「鹿沼」駅 バス7分
◆東武日光線「新鹿沼」駅 バス15分
◆東北自動車道「鹿沼」IC 車12分

◆ 設立日
（2004年6月1日　社会保険労務士事務所開業）
2014年11月11日　法人設立

◆ ビジョン
共に学び、共に育み、共に成長する！

◆ 代表社員（代表取締役）　代表　出口裕美（特定社会保険労務士）
法人社員（取締役）　副代表　鵜養昌利（特定社会保険労務士）
栃木オフィス代表　出口和宏（特定社会保険労務士）

◆ 社員・職員　社会保険労務士　6名（うち特定社会保険労務士　４名）
管理・総務他　12名
東京オフィス12名　栃木オフィス6名　合計18名

◆ 事務所の特徴　デジタル化（DX化）に強い社労士事務所【システム開発支援】

はじめに　プロフィール

経歴
栃木県出身　中央大学商学部卒
税理士・社会保険労務士事務所　勤務
社会保険労務士・行政書士事務所　勤務
社会保険労務士法人出口事務所（社会保険労務士事務所）設立
篠木マネジメント株式会社（コンサルティング会社）設立
中小企業マネジメントセンター（労働保険事務組合）　設立

現在
社会保険労務士法人出口事務所　代表社員
篠木マネジメント株式会社　代表取締役
中小企業マネジメントセンター　理事長
全国社会保険労務士会連合会　代議員
　社労士業務デジタル推進部会　委員
東京都社会保険労務士会　常任理事
　デジタル・IT化推進特別委員会　委員長
東京都社会保険労務士会新宿支部　副支部長
新宿労働保険事務組合協議会　会長
一般社団法人社労夢全国会　理事
一般社団法人自立した人と組織を育成する協会 理事
社会保険労務士白門会　副会長

特定社会保険労務士
出口（篠木）裕美
DEGUCHI　HIROMI

出版・メディア等
2013年「人事労務管理課題解決ハンドブック」共著（出版社：日本経済新聞出版社）
2014年「事例でわかる 選ばれる医療機関の経営と労務管理」共著（出版社：日本法令）
2015年「ダイバーシティマネジメントの実践」共著（出版社：労働新聞社）
2017年「改正個人情報保護法対応版　個人情報キチッと管理」共著（出版社：労働新聞社）
2018年「開業社会保険労務士専門誌SR50号　働き方改革関連法案」（出版社：日本法令）
2020年　NHK「ニュースウォッチ９」出口事務所のコロナに関する取り組みなどを紹介
2021年　日経チャンネル「デジタル強靭化時代の人事労務戦略フォーラム」
2022年　東日本電信電話株式会社・株式会社日本法令「企業のBCPとクラウドストレージ活用」
2022年「新しい働き方対応　会社経営の法務・労務・税務」共著（出版社：新日本法規出版）
2022年「社労士事務所の属人化を防ぐExcelを活用した業務管理方法」DVD（発売元：日本法令）
2023年「デジタル給与払い導入のための企業の実務対応」DVD（発売元：日本法令）
2023年「社労士事務所の属人化を防ぐWord/Excel連絡票を活用した業務受託方法」DVD（発売元：日本法令）
2024年「社会保険労務士の世界がよくわかる本」共著（出版社：日本実業出版社）

１．システム障害等とは

グローバルリスクマネジメントの調査結果（2021年）

グローバル	日本
1.サイバー攻撃／情報漏えい	1.サプライチェーンや流通の途絶
2.事業中断	2.市場動向の急激な変化
3.景気後退／回復遅延	3.サイバー攻撃／情報漏えい
4.優秀な人材の流出や確保不能	4.事業中断
5.法規制の変更	5.優秀な人材の流出や確保不能
6.サプライチェーンや流通の途絶	6.気象／自然災害
7.物価変動／原材料・資源の不足	7.景気後退／回復遅延
8.風評被害／ブランドの毀損	8.地政学的な不安定さ
9.イノベーション／顧客ニーズへの対応の失敗	9.環境・社会・ガバナンス（ESG）／企業の社会的責任（CSR）
10.競争の激化	10.製造物責任／製品の回収

資料　Aon plc（NYSE：AON、エーオン）、第９回グローバル リスクマネジメント調査
https://www.aon.com/2023-global-risk-management-survey/japan

１．システム障害等の原因

情報セキュリティ10大脅威 2024［組織］

順位	「組織」向け脅威	初選出年	10大脅威での取り扱い（2016年以降）
1位	ランサムウェアによる被害	2016年	9年連続9回目
2位	サプライチェーンの弱点を悪用した攻撃	2019年	6年連続6回目
3位	内部不正による情報漏えい	2016年	9年連続9回目
4位	標的型攻撃による機密情報の窃取	2016年	9年連続9回目
5位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	2022年	3年連続3回目
6位	不注意による情報漏えい等の被害	2016年	6年連続7回目
7位	脆弱性対策情報の公開に伴う悪用増加	2016年	4年連続7回目
8位	ビジネスメール詐欺による金銭被害	2018年	7年連続7回目
9位	テレワーク等のニューノーマルな働き方を狙った攻撃	2021年	4年連続4回目
10位	犯罪のビジネス化（アンダーグラウンドサービス）	2017年	2年連続4回目

参照：IPA独立行政法人情報処理推進機構
「情報セキュリティ10大脅威 2024」https://www.ipa.go.jp/security/10threats/10threats2024.html

１．情報セキュリティ対策の基本

- 多数の脅威があるが「攻撃の糸口」は似通っている
- 基本的な対策の重要性は長年変わらない
- 下記の**「情報セキュリティ対策の基本」を常に意識することが重要**

攻撃の糸口	情報セキュリティ対策の基本	目的
ソフトウェアの脆弱性	ソフトウェアの更新	脆弱性を解消し攻撃によるリスクを低減する
ウイルス感染	セキュリティソフトの利用	攻撃をブロックする
パスワード窃取	パスワードの管理・認証の強化	パスワード窃取によるリスクを低減する
設定不備	設定の見直し	誤った設定を攻撃に利用されないようにする
誘導(罠にはめる)	脅威・手口を知る	手口から重要視するべき対策を理解する

参照：IPA独立行政法人情報処理推進機構
「情報セキュリティ10大脅威 2024」https://www.ipa.go.jp/security/10threats/10threats2024.html

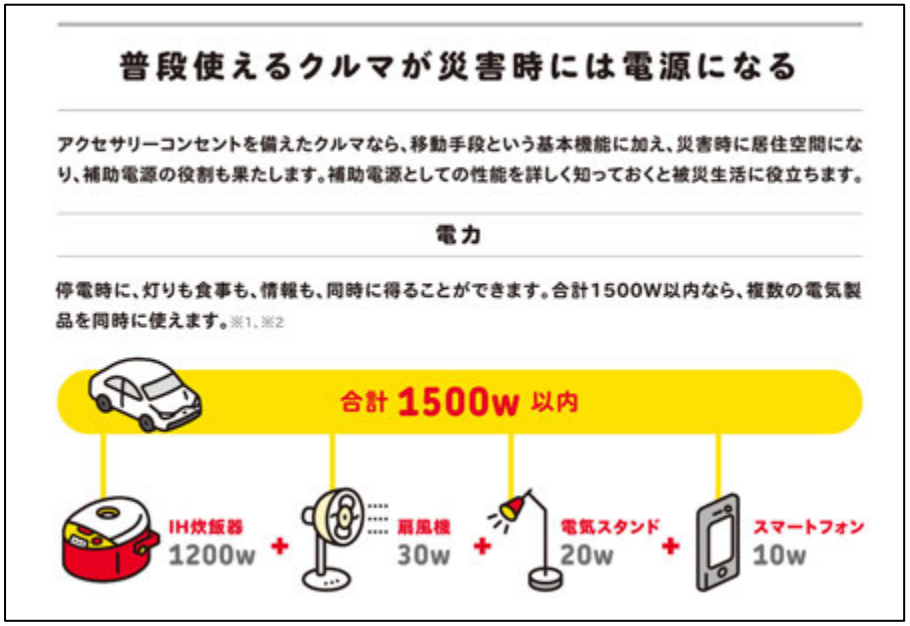
１．情報セキュリティ対策の基本＋α

- 昨今はクラウドサービスの利用も一般的になってきている
- クラウドサービスを利用を想定した＋αの対策を行い、備える必要がある

備える対象	情報セキュリティ対策の基本＋α	目的
インシデント全般	責任範囲の明確化(理解)	インシデント発生時に誰(どの組織)が対応する責任があるのかを明確化(理解)する
クラウドの停止	代替案の準備	業務が停止しないように代替策を準備する
クラウドの仕様変更	設定の見直し	仕様変更により意図せず変更された設定を適切な設定に直す(設定不備による情報漏えいや攻撃への悪用を防止する)

参照：IPA独立行政法人情報処理推進機構
「情報セキュリティ10大脅威 2024」https://www.ipa.go.jp/security/10threats/10threats2024.html

参考　自然災害等の対策



Point
・車も電源になる
・必要な備品を購入

参照：トヨタの防災「家とクルマの防災ブック」
Jackery「ポータブル電源」

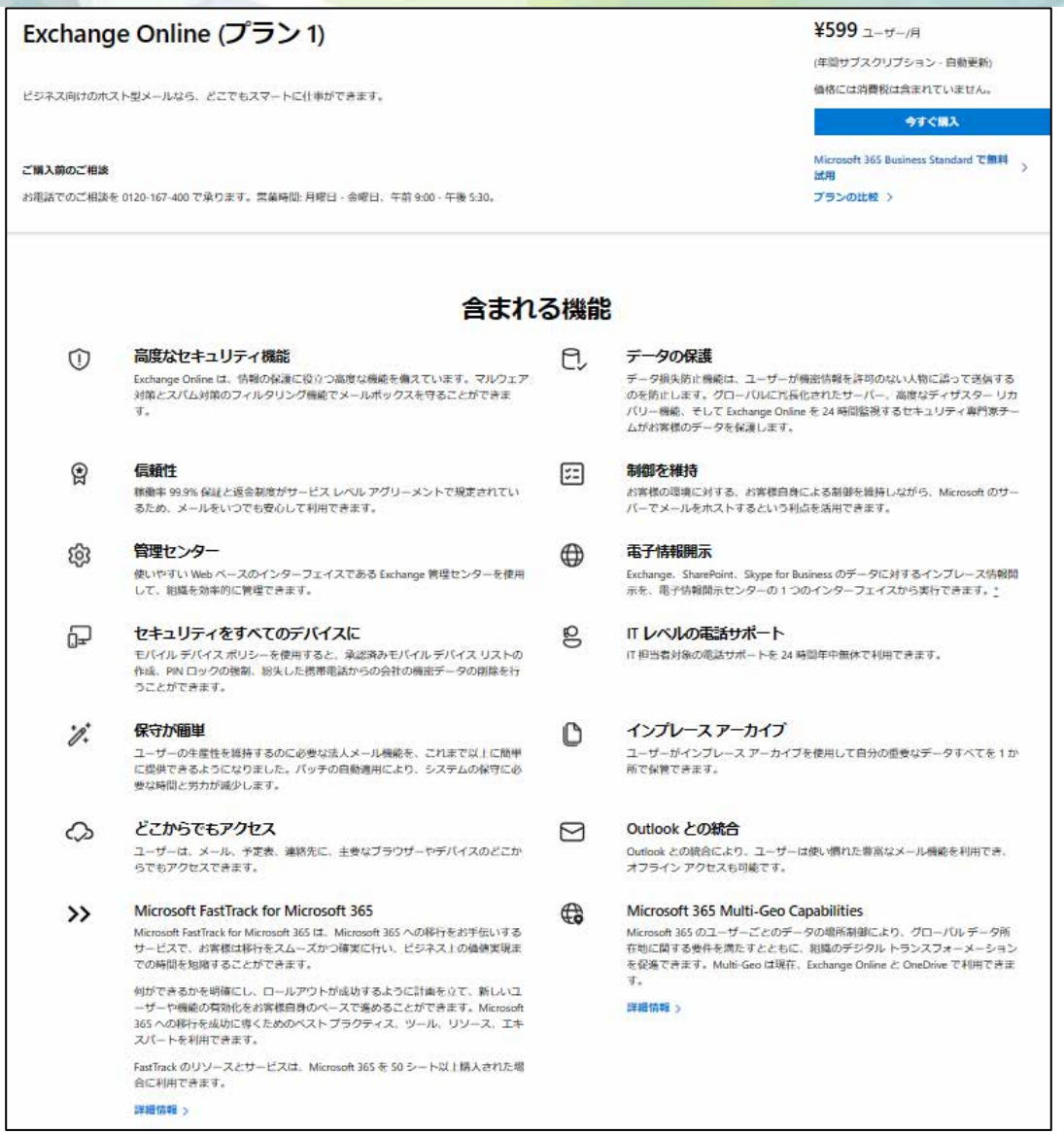
２．出口事務所の情報セキュリティ、個人情報保護の体制

	実施済の措置	進捗
1	リスクアセスメント・情報セキュリティ　外部専門家による調査の実施　→2023/6/7相談、6/13打合、6/14注文、6/27診断、7/20報告	済
2	各機器のOS 及びソフトウェアの最新化（定期的）	済
3	アカウントのパスワードポリシーの強化、パスワード再設定	済
4	業務委託元とのパスワードのパスワードポリシーの強化、パスワード再設定≪新規契約の企業・パスワード変更を希望した企業のみ≫	済
5	業務委託元向けのセキュリティセミナー開催　2023/8/2開催	済
6	アカウントの棚卸し（不要アカウントの無効または削除）	済
7	OS及びソフトウェアの更新管理の徹底	済
8	情報セキュリティの運用体制見直し	済
9	従業員に対するセキュリティ教育（定期的な啓発活動）	済
10	事業継続計画（BCP）の見直し	済
11	Microsoft365のメールサーバー（Exchange Online）に移行	済

２．出口事務所の情報セキュリティ、個人情報保護の体制

	実施済の措置	進捗
12	ネットワークセキュリティ対策（UTM等）強化 UTM運用事業者との責任分担の明確化（UTMは2019年に導入済み） ログポリシー見直し（ログ保存期間確認やアラートメール設定等） セキュリティインシデント発生時（コンピューターウイルス感染等）の対応手順や相談窓口の明確化	済
13	ウイルス対策ソフトを最新化した上でのフルスキャンの実施 Windows セキュリティ導入 （導入前は市販のウイルス対策ソフト利用）	済
14	エンドポイント端末へのAppGuard SBEの導入及び保護 全職員、全パソコンAppGuard SBE導入 （導入前は特定のノートPCのみAppGuard Solo利用）	済
15	クラウドストレージバックアップシステムの導入 （導入前は事務所内での自前バックアップ）	済
16	二要素認証の対象システム拡大≪事務所≫	済
17	二要素認証の対象システム拡大≪システムレンタル企業≫	試験中 6/5実施予定

参考　Microsoft365　Exchange Online



Exchange Online (プラン 1)

ビジネス向けのホスト型メールなら、どこでもスマートに仕事ができます。

ご購入前のご相談

お電話でのご相談を 0120-167-400 で承ります。営業時間: 月曜日 - 金曜日、午前 9:00 - 午後 5:30。

¥599 ユーザー/月

(年間サブスクリプション - 自動更新)

価格には消費税は含まれていません。

今すぐ購入

Microsoft 365 Business Standard で無料試用 >

プランの比較 >

含まれる機能

高度なセキュリティ機能
Exchange Online は、情報の保護に役立つ高度な機能を備えています。マルウェア対策とスパム対策のフィルタリング機能でメールボックスを守ることができます。

データの保護
データ損失防止機能は、ユーザーが機密情報を許可のない人物に誤って送信するのを防止します。グローバルに冗長化されたサーバー、高度なディザスター リカバリー機能、そして Exchange Online を 24 時間監視するセキュリティ専門家チームがお客様のデータを保護します。

信頼性
稼働率 99.9% 保証と返金制度がサービス レベル アグリーメントで規定されているため、メールをいつでも安心して利用できます。

制御を維持
お客様の環境に対する、お客様自身による制御を維持しながら、Microsoft のサーバーでメールをホストするという利点を活用できます。

管理センター
使いやすい Web ベースのインターフェイスである Exchange 管理センターを使用して、組織を効率的に管理できます。

電子情報開示
Exchange、SharePoint、Skype for Business のデータに対するインプレース情報開示を、電子情報開示センターの 1 つのインターフェイスから実行できます。

セキュリティをすべてのデバイスに
モバイル デバイス ポリシーを使用すると、承認済みモバイル デバイス リストの作成、PIN ロックの強制、紛失した携帯電話からの会社の機密データの削除を行うことができます。

IT レベルの電話サポート
IT 担当者対象の電話サポートを 24 時間年中無休で利用できます。

保守が簡単
ユーザーの生産性を維持するのに必要な法人メール機能を、これまで以上に簡単に提供できるようになりました。パッチの自動適用により、システムの保守に必要な時間と労力が減少します。

インプレース アーカイブ
ユーザーがインプレース アーカイブを使用して自分の重要なデータすべてを 1 か所で保管できます。

どこからでもアクセス
ユーザーは、メール、予定表、連絡先に、主要なブラウザーやデバイスのどこからでもアクセスできます。

Outlook との統合
Outlook との統合により、ユーザーは使い慣れた高度なメール機能を利用でき、オフライン アクセスも可能です。

Microsoft FastTrack for Microsoft 365
Microsoft FastTrack for Microsoft 365 は、Microsoft 365 への移行をお手伝いするサービスで、お客様は移行をスムーズかつ確実に行い、ビジネス上の価値実現までの時間を短縮することができます。

何ができるかを明確にし、ロールアウトが成功するように計画を立て、新しいユーザーや機能の有効化をお客様自身のペースで進めることができます。Microsoft 365 への移行を成功に導くためのベスト プラクティス、ツール、リソース、エキスパートを利用できます。

FastTrack のリソースとサービスは、Microsoft 365 を 50 シート以上購入された場合に利用できます。

詳細情報 >

Microsoft 365 Multi-Geo Capabilities
Microsoft 365 のユーザーごとのデータの場所制御により、グローバル データ所在地に関する要件を満たすとともに、組織のデジタル トランスフォーメーションを促進できます。Multi-Geo は現在、Exchange Online と OneDrive で利用できます。

詳細情報 >

参考　システム障害等の対応　顧問先への情報発信

・ホームページ（ブログ）
https://www.deguchi-office.com/blog

Point
ブログは顧問先、職員達、
同業者、将来の顧問先に
向けて情報発信

・ホームページ（会員専用ページ）の活用

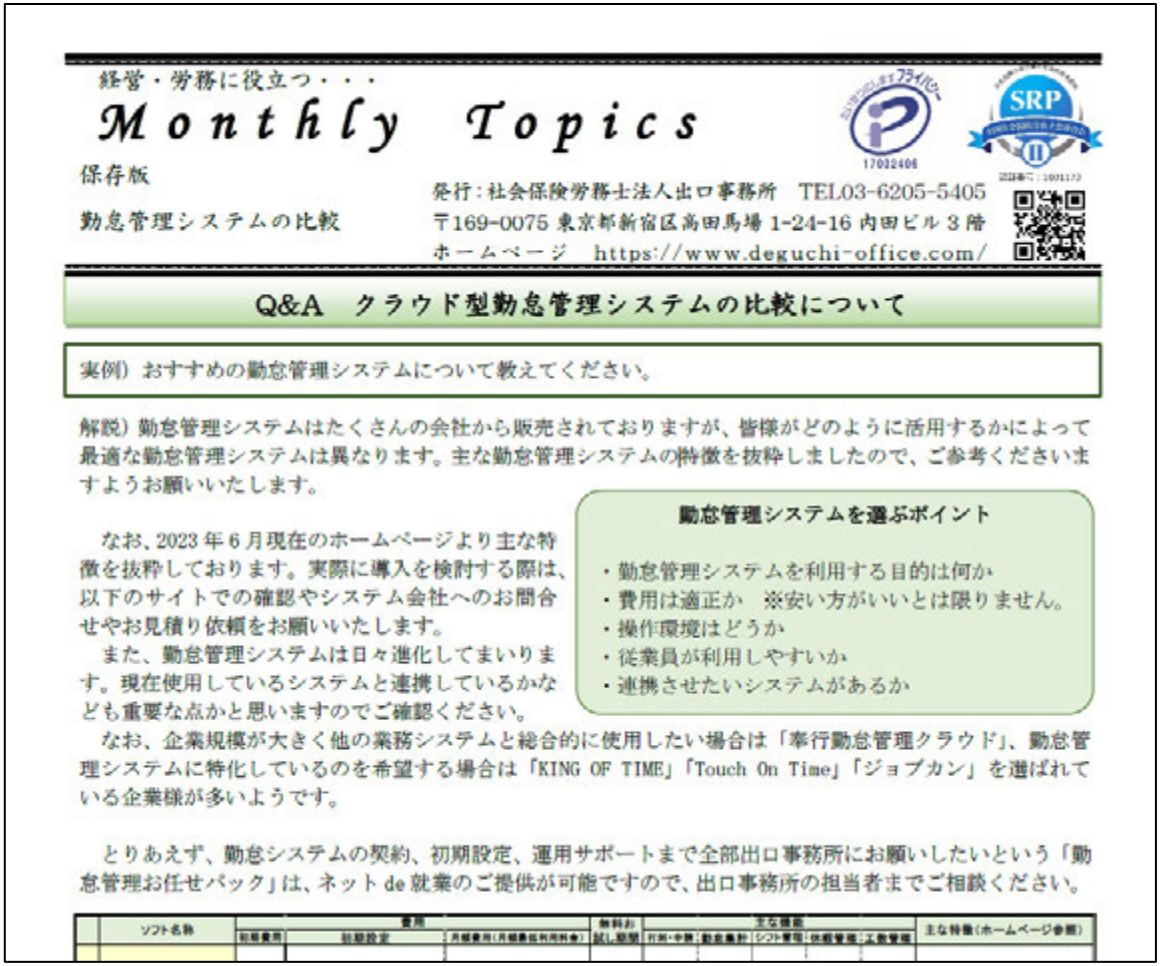
Point
会員専用ページは顧問先、
職員達に向けて情報発信

参考　システム障害等の対応　代替書式活用

代替書式（WordやExcel）
を提供

６月８日より、必要な書式を随時提供
→手続依頼は「入社連絡票等」
→勤怠管理は「勤怠管理表」
→給与計算は「給与支給控除一覧表」

参考　システム障害等の対応　代替システムの提案



経営・労務に役立つ・・・

Monthly Topics

保存版

勤怠管理システムの比較

発行：社会保険労務士法人出口事務所　TEL03-6205-5405
〒169-0075 東京都新宿区高田馬場 1-24-16 内田ビル 3 階
ホームページ　https://www.deguchi-office.com/

Q&A　クラウド型勤怠管理システムの比較について

実例）おすすめの勤怠管理システムについて教えてください。

解説）勤怠管理システムはたくさんの会社から販売されておりますが、皆様がどのように活用するかによって最適な勤怠管理システムは異なります。主な勤怠管理システムの特徴を抜粋しましたので、ご参考くださいますようお願いいたします。

なお、2023 年 6 月現在のホームページより主な特徴を抜粋しております。実際に導入を検討する際は、以下のサイトでの確認やシステム会社へのお問合せやお見積り依頼をお願いいたします。

また、勤怠管理システムは日々進化してまいります。現在使用しているシステムと連携しているかなども重要な点かと思いますのでご確認ください。

勤怠管理システムを選ぶポイント

- 勤怠管理システムを利用する目的は何か
- 費用は適正か　※安い方がいいとは限りません。
- 操作環境はどうか
- 従業員が利用しやすいか
- 連携させたいシステムがあるか

なお、企業規模が大きく他の業務システムと総合的に使用したい場合は「奉行勤怠管理クラウド」、勤怠管理システムに特化しているのを希望する場合は「KING OF TIME」「Touch On Time」「ジョブカン」を選ばれている企業様が多いようです。

とりあえず、勤怠システムの契約、初期設定、運用サポートまで全部出口事務所にお願いしたいという「勤怠管理お任せパック」は、ネット de 就業のご提供が可能ですので、出口事務所の担当者までご相談ください。

	ソフト名称	費用			無料お試し期間	主な機能					主な特徴（ホームページ参照）
		初期費用	初期設定	月額費用（月額最低利用料金）		打刻・申請	勤怠集計	シフト管理	休暇管理	工数管理	

Touch On Time（タッチオンタイム）

ジョブカン 勤怠管理

クラウド勤怠管理システム
KING OF TIME

Edge 奉行
勤怠管理クラウド

２．出口事務所の情報セキュリティ、個人情報保護の体制

リスクアセスメント報告書（2023/6/7相談、6/13打合、6/14注文、6/27診断、7/20報告）

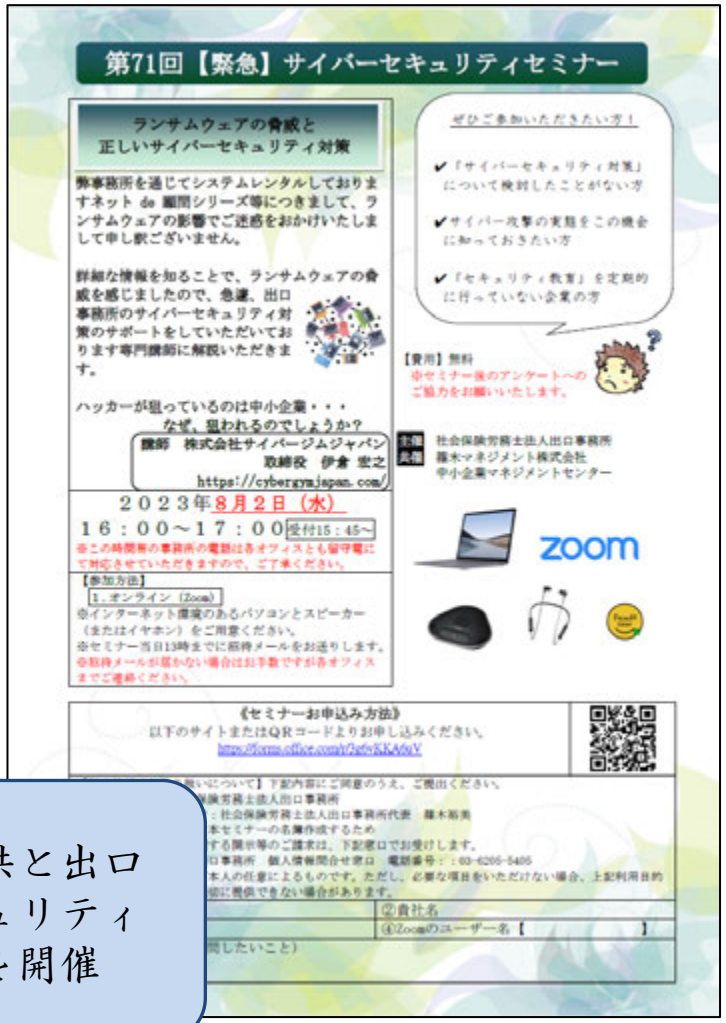
アセスメント基準

リスクアセスメントの基準を以下に示します。

■総合評価の基準

LEVEL 4	業界でも最高水準であり、他社にとってのベストプラクティスとなりえる
LEVEL 3	業界の平均的な企業群よりも優れた水準にある
LEVEL 2	業界の平均的な企業群と同等な水準にある
LEVEL 1	業界の平均的な企業群との比較において劣っている

※他社との比較は、当社の認証取得事業、情報セキュリティ事業における2000件超の支援実績をもとに評価したものですが、あくまでアセッサーの定性的な判断によるものですのでご了承ください。



顧問先等に情報提供と出口事務所の情報セキュリティについてセミナーを開催

参照：株式会社サイバージムジャパン
「リスクアセスメント報告書　2023/7/20」

参考　セキュリティ診断前の情報セキュリティの体制

セキュリティ診断前のセキュリティ・ネットワーク環境

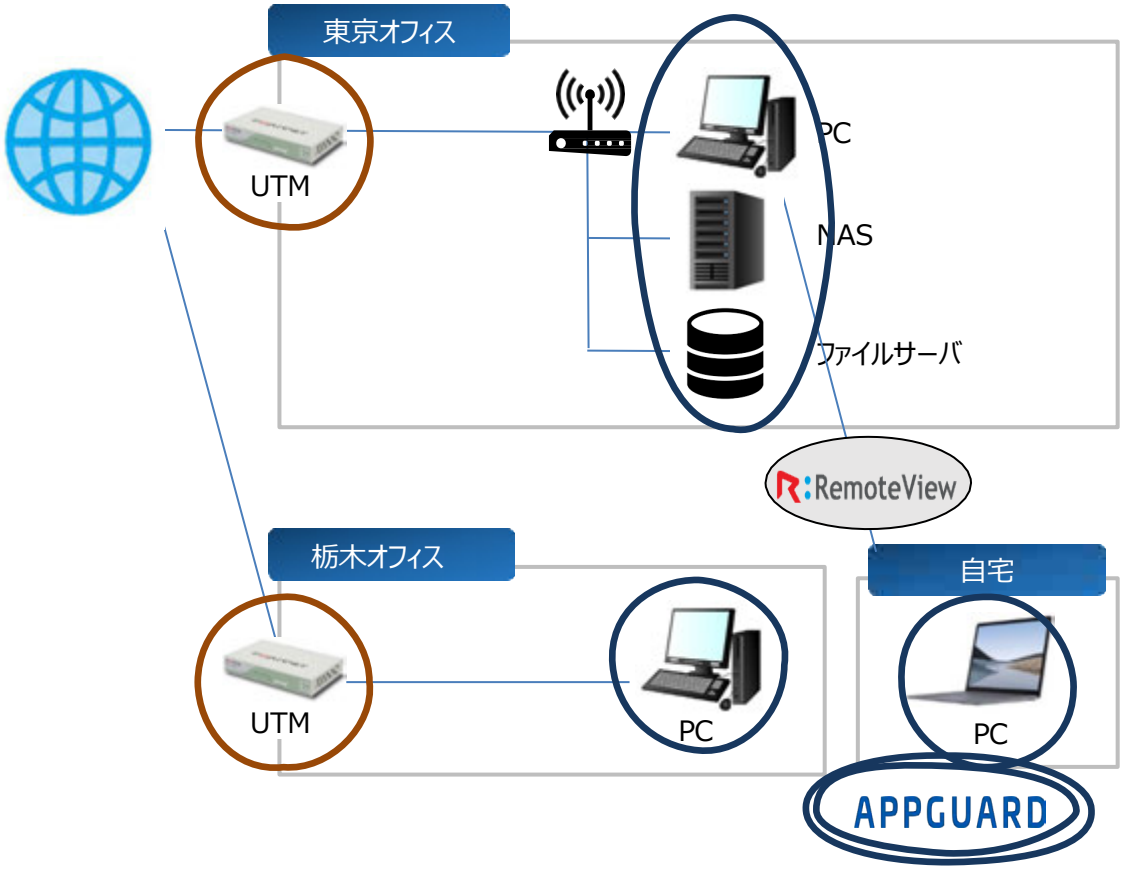
アセスメント基準

リスクアセスメントの基準を以下に示します。

■総合評価の基準

LEVEL 4	業界でも最高水準であり、他社にとってのベストプラクティスとなりえる
LEVEL 3	業界の平均的な企業群よりも優れた水準にある
LEVEL 2	業界の平均的な企業群と同等な水準にある
LEVEL 1	業界の平均的な企業群との比較において劣っている

※他社との比較は、当社の認証取得事業、情報セキュリティ事業における2000件超の支援実績をもとに評価したものですが、あくまでアセッサーの定性的な判断によるものですのでご了承ください。



参考　セキュリティ診断前の情報セキュリティの体制

セキュリティ診断後のセキュリティ・ネットワーク環境

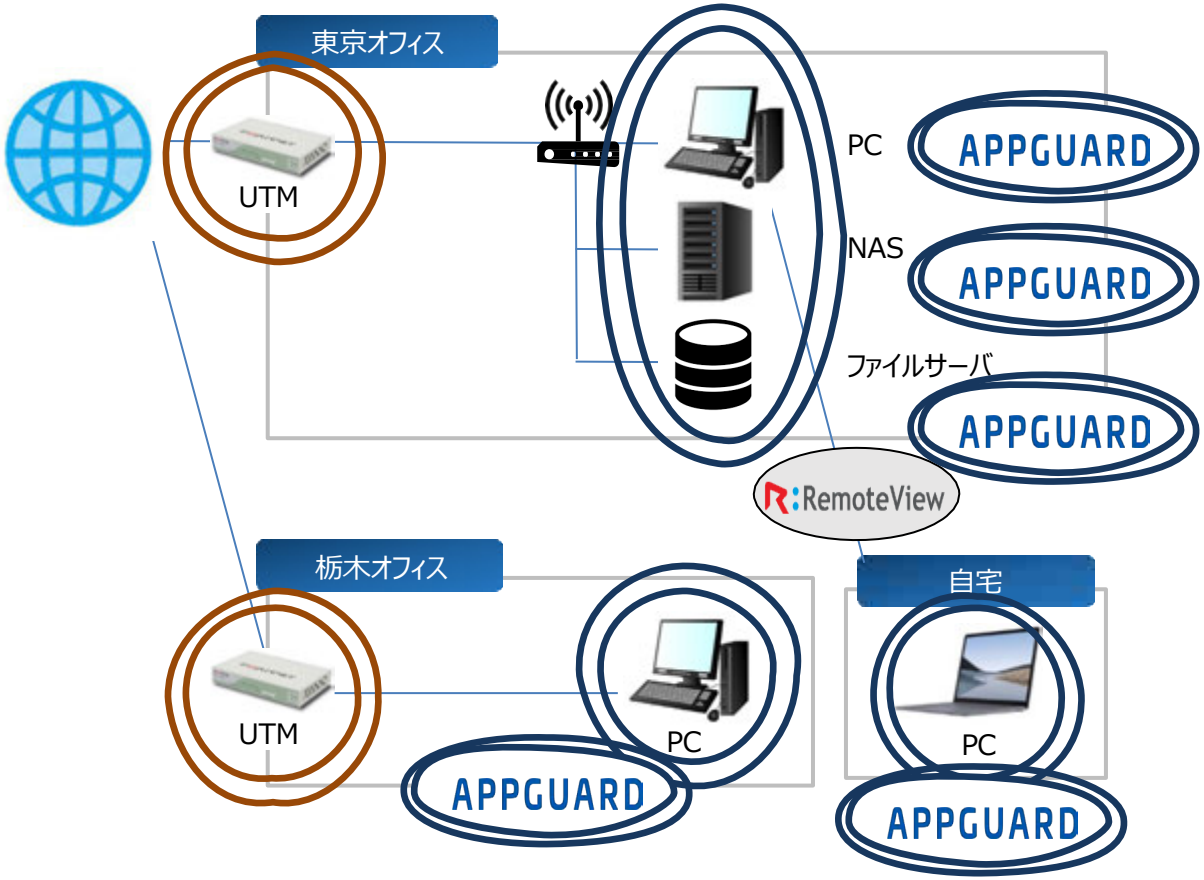
アセスメント基準

リスクアセスメントの基準を以下に示します。

■総合評価の基準

LEVEL 4	業界でも最高水準であり、他社にとってのベストプラクティスとなりえる
LEVEL 3	業界の平均的な企業群よりも優れた水準にある
LEVEL 2	業界の平均的な企業群と同等な水準にある
LEVEL 1	業界の平均的な企業群との比較において劣っている

※他社との比較は、当社の認証取得事業、情報セキュリティ事業における2000件超の支援実績をもとに評価したものですが、あくまでアセッサーの定性的な判断によるものですのでご了承ください。



参考　UTM（統合脅威管理）

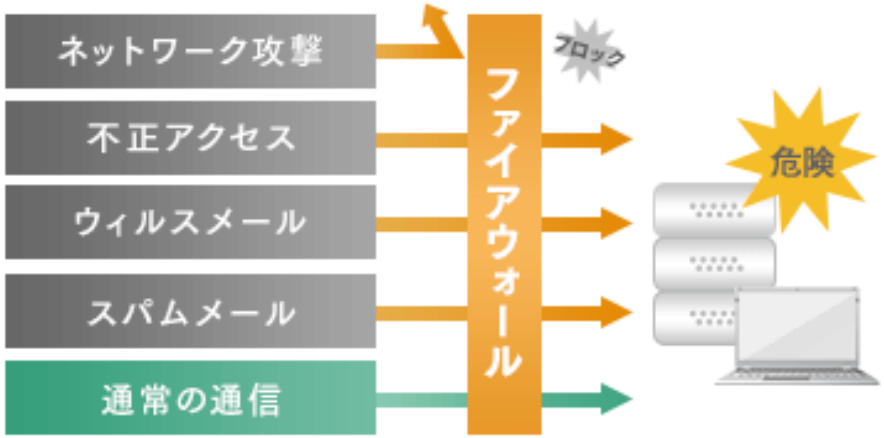
UTM（Unified Threat Management・統合脅威管理）とはファイアウォールやアンチウイルス、不正侵入防御、IDS/IPS（不正侵入検知・防御システム）などの**セキュリティ機能が一つにまとまっている製品のこと**です。導入することで不正侵入やスパムなどのサイバー攻撃を防止することができます。

UTMのメリット・・・職員達が安心して仕事ができる
UTMのデメリット・・・コストが高い
複数の機能が搭載されているため、ファイアウォールと比べるとその分コストは高くなります。

参照：ITメディア
UTMとファイアウォールの違いとは

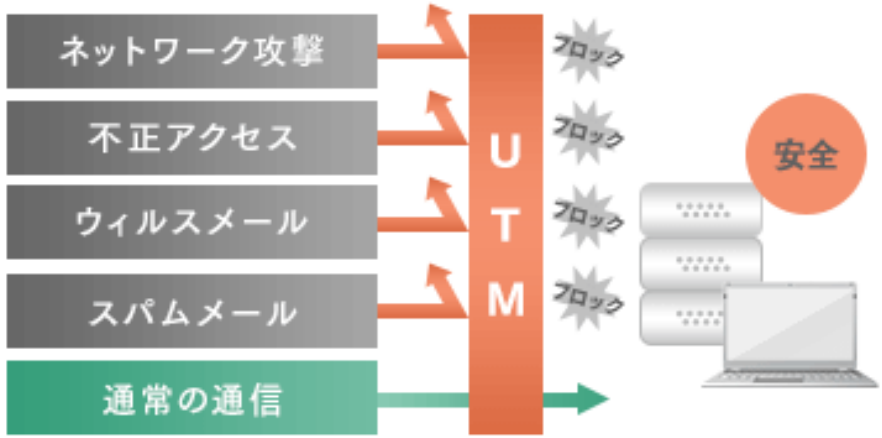
参考　UTM（統合脅威管理）

ファイアウォールの防御範囲



- 外部からのアクセスを監視、内部ネットワークに対する不正アクセスを防ぐ
- 決められたルールに則って、外部ネットワークからのアクセスが正常かどうかを判断

UTMの防御範囲



- 多方面のセキュリティ機能、対策が広範囲で行える
- UTMはファイアウォールの機能も搭載

［UTMとファイアウォールの違い］

参照：ITメディア
UTMとファイアウォールの違いとは

参考　AppGuard

参照：Blue Planet-works, Inc
https://www.blueplanet-works.com/solution/appguard.html

参考　AppGuard

起こってほしくないことは防止する。AppGuardがもたらす新概念

これまでの「防御」の守り方

悪い物を検知して駆除

攻撃者との積極バトルを展開する守り方である

「防御」とは戦闘などにおいて敵の攻撃から身を守る、防ぐことを意味しています。

攻撃者の一方的な攻撃に対して一発も殴られないように様々な検知技術を使い防衛バトルを展開する。

試合後、どちらがリングに立っているかは試合が終わってみないと分からない状態。

AppGuardが提唱する「防止」の守り方

何も起こらない環境を作る

攻撃者の相手をせず、「自分自身を磨く」守り方である

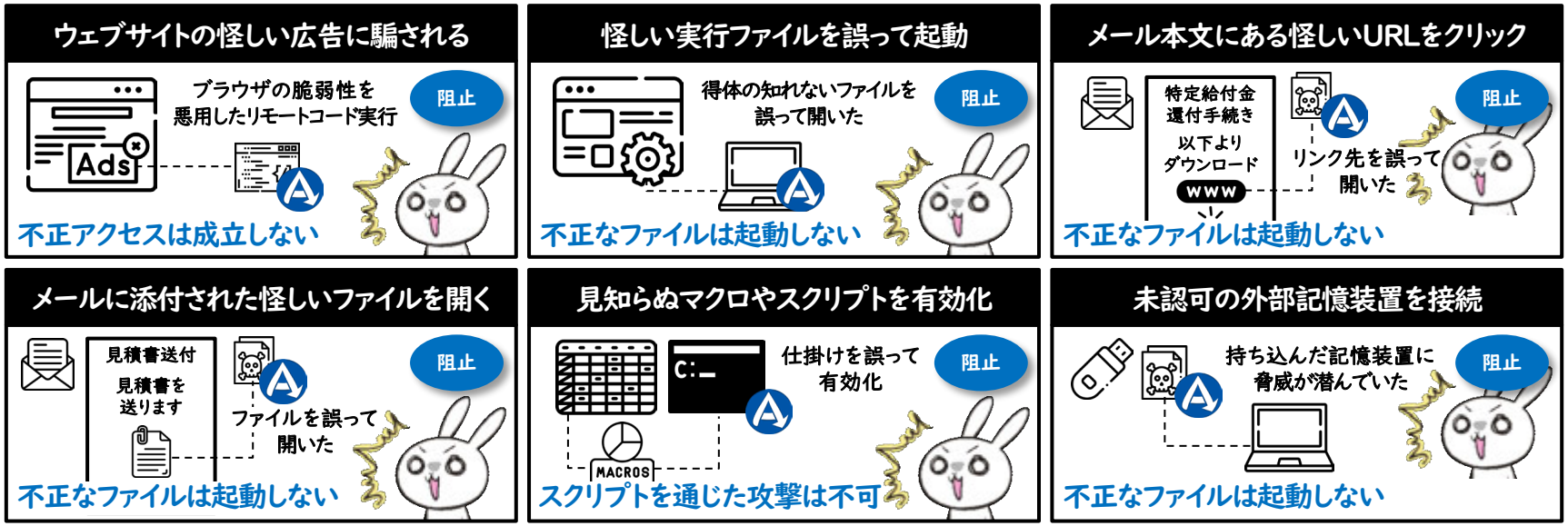
「防止」とは起こってほしくないことが起こらないように対策をすることを意味しています。

攻撃者がどんな攻撃を仕掛けてこようとも動じない。それよりも常に自分を律し規則正しく健康的な行動を心がけることで最初から攻撃出来ない環境を自分に作り上げる。勝敗は試合前から既に決まっている状態。

参照：Blue Planet-works, Inc
「AppGuardのご紹介」

参考　AppGuard

防止が実施されたPCでは攻撃プロセスの成立を軒並み阻止する



AppGuardは独自の特許技術と米国政府機関を20年以上守り続ける実績で、皆様のPCを「攻撃から防止された状態」に作り上げるサイバーセキュリティ製品です。

お問い合わせは以下から

https://www.blueplanet-works.com/contact/

参照：Blue Planet-works, Inc
「AppGuardのご紹介」

参考　AppGuard

AppGuard製品ラインナップ

Blue Planet-works
Safety for the Connected World

▶ AppGuardのラインナップ

	AppGuard Solo	AppGuard SBE	AppGuard Enterprise	AppGuard Server
定価（税別）	@6,000円/年	@6,000円/年 （クラウド型管理コンソール利用料を含む）	@6,000円/年 （クラウド型管理コンソール利用料は含まない）	@60,000円/年 （クラウド型管理コンソール利用料は含まない）
対象OS		Windows Client OS		Windows Server OS
対象企業規模	10名以下	1～300名まで	1名～	-
特徴	・メーカーサポートセンター対応 ・中小規模組織向けポリシーテンプレート ・利用者自身がポリシー設定	・クラウド型管理コンソールで統合管理 ・中小規模組織向けポリシーテンプレート ・運用サービス付帯必須	・完全カスタマイズ導入 ・管理方式はクラウド/オンプレミス選択可 ・組み込み販売可	・完全カスタマイズ導入 ・管理方式はクラウド/オンプレミス選択可
併売サービス	-	・AGE/SBEおまかせ導入パッケージ ・AGE/SBE運用サービス	・AGE/SBEおまかせ導入パッケージ ・AGEカスタム導入パッケージ ・AGE/SBE運用サービス ・AGMSホスティング	・AGSおまかせ導入パッケージ ・AGSカスタム導入パッケージ ・AGS運用サービス ・AGMSホスティング/Server
制限事項	インターネット接続必須	クラウド型管理のみ提供		

※ AppGuard Industrialをご希望の場合は別途ご相談ください

参照：Blue Planet-works, Inc
「AppGuardのご紹介」

参考　二要素認証の対象システム拡大

二要素認証では、これら３つの要素のなかから２つを組み合わせて認証を行いますが、同じ要素を組み合わせた場合は二要素認証にはなりません。同じ要素を組み合わせは、二段階認証と呼ばれます。

参照：ITトレンド
https://it-trend.jp/onetime_password/article/93-0003

参考　複数の複合機（プリンター）導入

例　東京オフィス複合機（プリンター等）

種類	機種名	利用目的
① 複合機	RICOH	カラー印刷・製本印刷・コピー・スキャン
② 複合機	Brother （1）	カラー印刷・コピー・スキャン
③ 複合機	Brother （2）	カラー印刷・コピー・スキャン
④ プリンター	Brother （1）	モノクロ印刷
⑤ プリンター	Brother （2）	モノクロ印刷
⑥ プリンター	Brother （3）	モノクロ印刷
⑦ プリンター	Brother （4）	モノクロ印刷
⑧ ラベルプリンター	Brother	ラベル作成
⑨ インクジェットプリンター	Canon	封筒作成・名刺作成
⑩ ドットプリンター	EPSON （1）	給与明細・複写式の手続用紙
⑪ ドットプリンター	EPSON （2）	給与明細・複写式の手続用紙
⑫ ドットプリンター	EPSON （3）	給与明細・複写式の手続用紙

参考　クラウドサービスや業務システムの権限管理

権限	説明	目安
Lv1	各台帳の閲覧のみ可能	インターンシップ
Lv2	各台帳のデータの編集や新たなデータの登録を行なうことが可能	アルバイト
Lv3	Lv2 までの権限に加えて、データ取込・出力の操作が可能	正社員（試用期間）
Lv4	Lv3 までの権限に加えて、各種マスタ情報の設定を行なうことが可能	正社員
Lv5	Lv4 までの権限に加えて、ユーザー権限設定の変更が可能	管理職 役員

Shalom 参考　クラウドサービスや業務システムの権限管理

ID	契約	マイナンバー管理	権限	所属	使用者
130321 - 01	○	○	Lv5	東京	●●
02	○	○	Lv5	東京	●●
03	○	○	Lv5	東京	●●
06	○		Lv4	東京	●●
07	○	○	Lv5	東京	●●
09	○	○	Lv4	東京	●●
10	○	○	Lv5	東京	●●
11	○	○	Lv4	東京	●●
12	○	○	Lv5	栃木	●●
13	○	○	Lv2		●●
14	○	○	Lv5	栃木	●●
15	○	○	Lv4	東京	●●
17	○		Lv4	東京	●●
18	○	○	Lv4	栃木	●●
19	○		Lv4	栃木	●●
21	○	○	Lv4	東京	●●
22	○		Lv2	東京	●●
23	○		Lv4	栃木	●●
24	○		Lv2	東京	●●
合計	19	13			

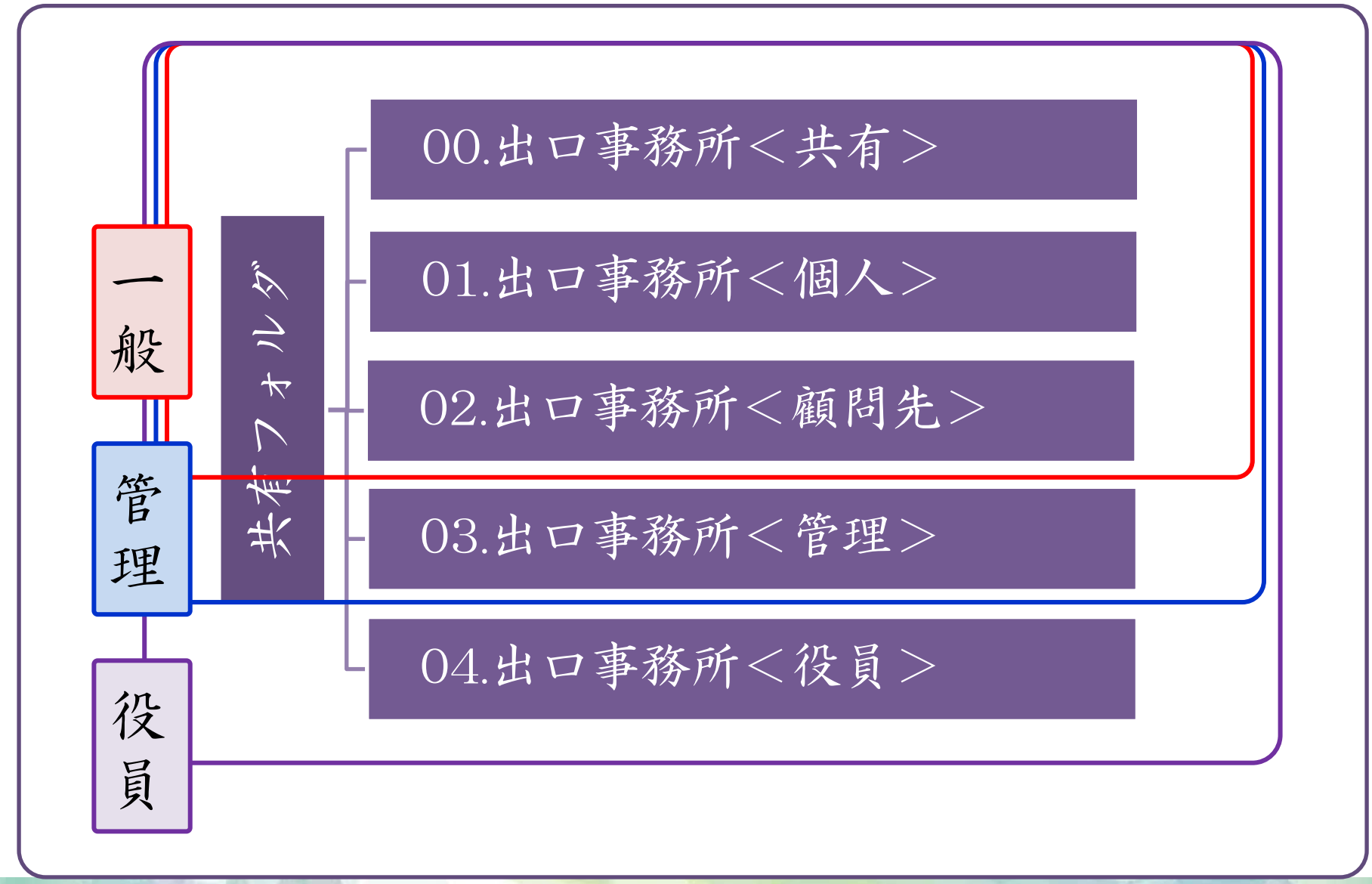
使用時のルール

・席を外す場合、外出する場合など一定時間使用しないときはログオフしましょう。
・利用者以外のIDの利用は禁止です。
※IDですべてのログ管理を行っています。責任を持って、利用してください。
・気付いた点等あれば、速やかに総務に伝えてください。
・新規のID追加(＋5,000 /月)またはマイナンバー契約の追加(＋5,000 /月)を希望する場合は、各オフィス代表に伝えてください。

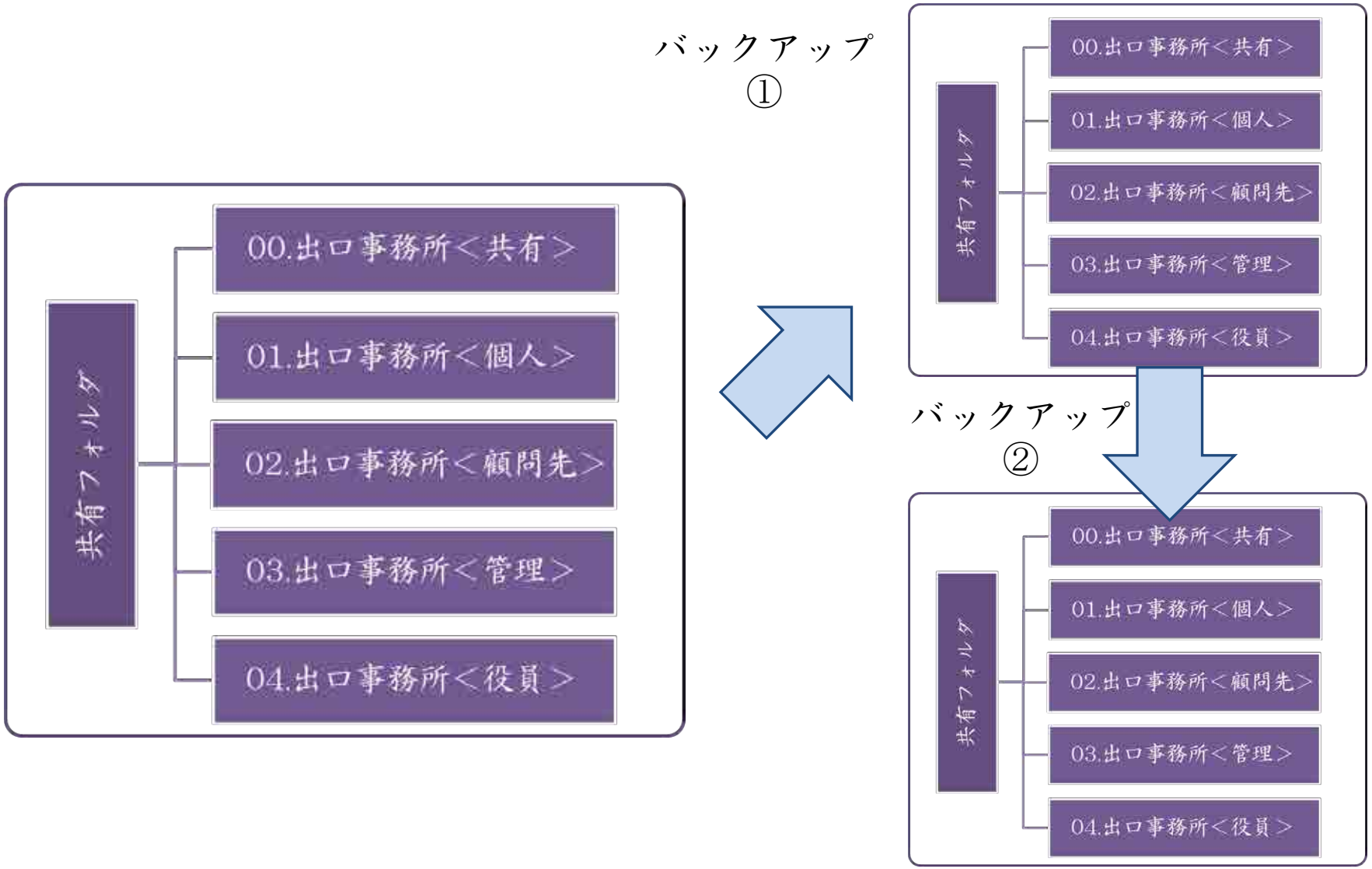
参考　クラウドサービスや業務システムの権限管理

	アップロード	ダウンロード	プレビュー	リンクの取得	ファイル編集	削除	所有	目安
共同所有者	○	○	○	○	○	○	○	役員
編集者	○	○	○	○	○	○	×	職員
ビューア/アップローダ	○	○	○	○	○	×	×	顧問先
プレビュー/アップローダ	○	×	○	×	×	×	×	
ビューア	×	○	○	○	×	×	×	会員サイト
プレビューア	×	×	○	×	×	×	×	
アップローダ	○	×	×	×	×	×	×	

参考　クラウドサービスや業務システムの権限管理



box 参考　クラウドストレージバックアップシステムの導入



参考　クラウドサービスや業務システムの権限管理

box

データの履歴管理・バックアップ

- 重要な資料を上書き保存してしまった…

→いつでも以前のバージョンに戻せます

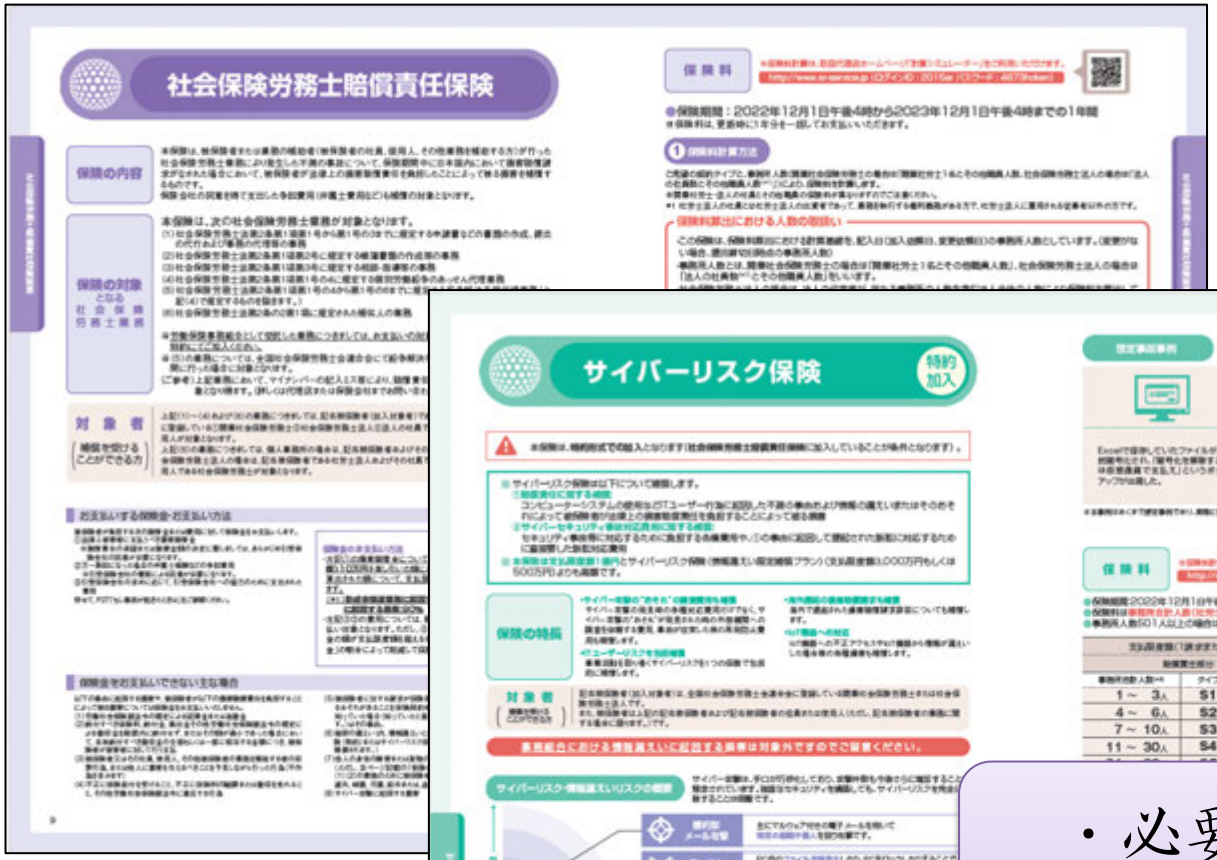
- ファイルの「最新版」が分からない…

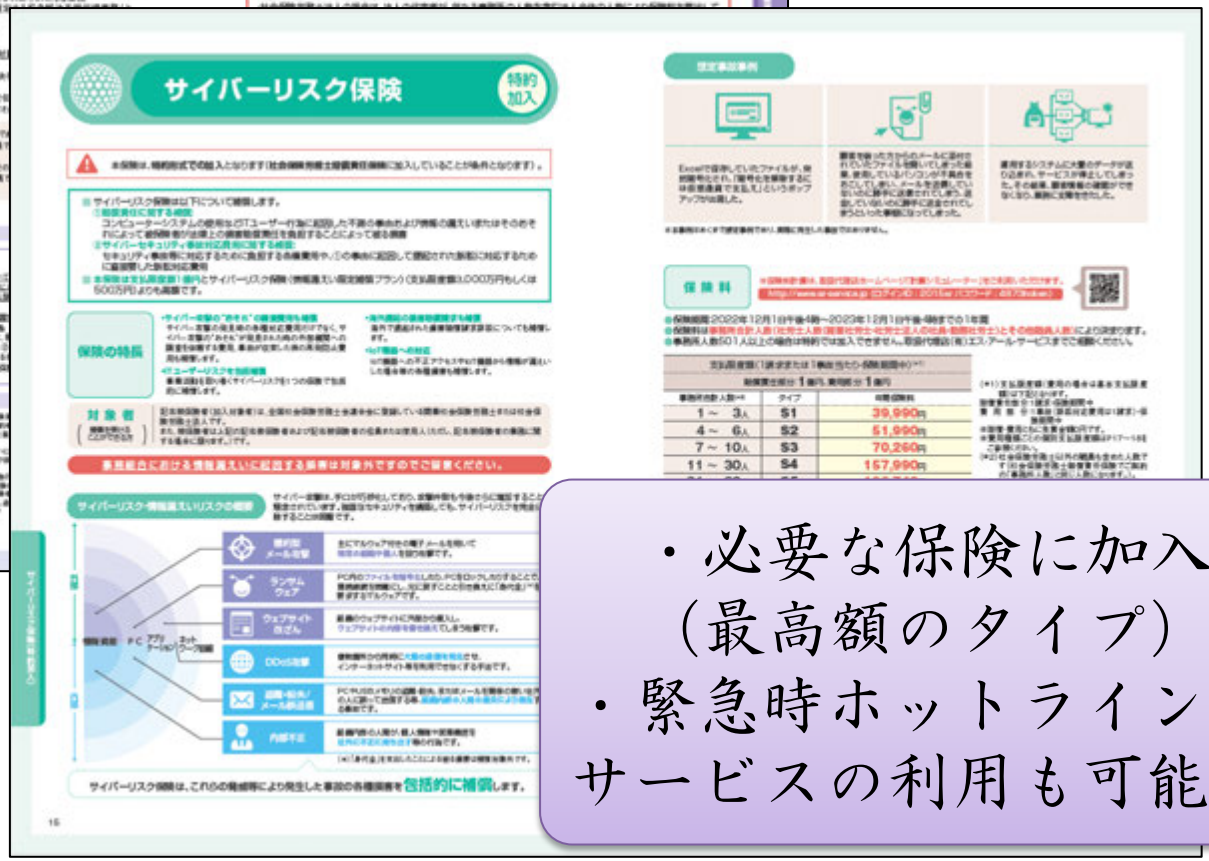
→過去のファイルの更新履歴が確認できます

- 誤ってファイルを削除してしまった…

→バックアップデータから復元できます

参考　社会保険労務士賠償責任保険・サイバーリスク保険





・必要な保険に加入
（最高額のタイプ）
・緊急時ホットライン
サービスの利用も可能

参照：東京海上日動火災保険株式会社
「社会保険労務士賠償責任保険」「サイバーリスク保険」

参考　ハードディスク、USB

原則　ハードディスク、ＵＳＢの利用禁止

例外　許可されたUSBのみ利用可
※使用できるパソコンの設定を変更します

許可されたUSB
①マイナンバーの受け渡し用（セキュリティが高いもの）
使用前に使用管理簿「管理表　キー付USB使用履歴」に
記載したうえで、上司の承認を得ること

・USBを認識させない設定
・現在は利用実績無し

参考　個人情報保護基本方針

個人情報保護方針
制定　2015年4月1日
改定　2017年1月1日
改定　2022年4月1日
社会保険労務士法人出口事務所
代表　篠木　裕美

当法人は、当法人が取り扱う全ての個人情報の保護について、社会的使命を十分に認識し、本人の権利の保護、個人情報に関する法規制等を遵守します。また、以下に示す方針を具現化するための個人情報保護マネジメントシステムを構築し、最新のＩＴ技術の動向、社会的要請の変化、経営環境の変動等を常に認識しながら、その継続的改善に、全社を挙げて取り組むことをここに宣言します。

１．個人情報は、社会保険労務士業務、給与計算代行業務、労務コンサルティング業務における当法人の正当な事業遂行上並びに職員の雇用、人事管理上必要な範囲に限定して、取得・利用及び提供をし、特定された利用目的の達成に必要な範囲を超えた個人情報の取扱い（目的外利用）を行いません。また、目的外利用を行わないための措置を講じます。
２．個人情報保護に関する法令、国が定める指針及びその他の規範を遵守致します。
３．個人情報の漏えい、滅失、き損などのリスクに対しては、合理的な安全対策を講じて防止すべく事業の実情に合致した経営資源を注入し個人情報セキュリティ体制を継続的に向上させます。また、万一の際には速やかに是正措置を講じます。
４．個人情報取扱いに関する苦情及び相談に対しては、迅速かつ誠実に、適切な対応をさせていただきます。
５．個人情報保護マネジメントシステムは、当法人を取り巻く環境の変化を踏まえ、適時・適切に見直してその改善を継続的に推進します。

以上

参考　個人情報に関する公表文

個人情報に関する公表文

■個人情報の取扱いについて
1、当法人が取り扱う個人情報の利用目的
（1）ご本人から直接書面によって取得する個人情報（ホームページや電子メール等によるものを含む）の利用目的取得に先立ち、ご本人に対し書面により明示します。
（2）前項以外の方法によって取得する個人情報の利用目的

分類	利用目的
お客様情報（お電話などからのお問合せ等によるもの）	ご利用履歴管理のため お問合せ対応のため
業務の受託に伴い、お客様からお預かりする個人情報	受託した社会保険手続業務、給与計算業務等を適切に遂行するため

■保有個人データに関する事項の周知
当法人で保有している保有個人データ又は第三者提供記録に関して、ご本人様又はその代理人様からの利用目的の通知、開示、内容の訂正、追加又は削除、利用の停止、消去及び第三者への提供の停止の請求（以下、「開示等の請求」といいます）につきましては、以下の要領にて対応させていただきます。

ａ）事業者の名称
社会保険労務士法人出口事務所
〒169-0075
東京都新宿区高田馬場1-24-16　内田ビル3階
代表社員　篠木 裕美
ｂ）個人情報の管理責任者
管理者の役職名：マネージャー
所属部署：社会保険労務士法人出口事務所　管理部
連絡先：電話03 - 6205 - 5405
ｃ）全ての保有個人データの利用目的

分類	利用目的
お客様情報（お電話などからのお問合せ等によるもの）	お問合せ対応のため ご利用履歴管理のため ご発注いただいた業務に関するご連絡のため 当法人サービスのご案内のため
当法人職員情報	職員の人事労務管理、業務管理、健康管理、セキュリティ管理のため
当法人への採用応募者情報	採用応募者への連絡と当法人の採用業務管理のため
当法人へのインターンシップ応募者情報	インターンシップ応募者への連絡と当法人のインターンシップ業務管理のため
特定個人情報	番号利用法に定められた利用目的のため

（省略）

参考　情報セキュリティ基本方針

情報セキュリティ基本方針

社会保険労務士法人出口事務所（以下、当法人）は、お客様からお預かりした情報資産を事故・災害・犯罪などの脅威から守り、お客様ならびに社会の信頼に応えるべく、以下の方針に基づき全社で情報セキュリティに取り組みます。

1.経営者の責任
当法人は、経営者主導で組織的かつ継続的に情報セキュリティの改善・向上に努めます。

2.社内体制の整備
当法人は、情報セキュリティの維持及び改善のために組織を設置し、情報セキュリティ対策を社内の正式な規則として定めます。

3.従業員の取組み
当法人の従業員は、情報セキュリティのために必要とされる知識、技術を習得し、情報セキュリティへの取り組みを確かなものにします。

4.法令及び契約上の要求事項の遵守
当法人は、情報セキュリティに関わる法令、規制、規範、契約上の義務を遵守するとともに、お客様の期待に応えます。

5.違反及び事故への対応
当法人は、情報セキュリティに関わる法令違反、契約違反及び事故が発生した場合には適切に対処し、再発防止に努めます。

制定日　2015年4月1日
改定　2022年6月30日

社会保険労務士法人出口事務所
代表　篠木　裕美

参照：IPA独立行政法人情報処理推進機構
https://www.ipa.go.jp/security/security-action/about-sa/index.html

参考　業務委託契約書

業務委託契約書（雛形）

委託者　　（以下「甲」と称する）と
受託者　　社会保険労務士法人出口事務所　　（以下「乙」と称する）とは
下記のとおり契約する。

契約事項	委託業務の範囲	(1)労働・社会保険諸法令に基づく書類の作成、提出等。 (2)労働・社会保険諸法令に基づく帳簿類の作成、管理、保管等。 詳細は別紙「委託業務の範囲及び報酬の内訳書」による。
	期　　間	令和　　年　　月　　日　～　令和　　年　　月　　日
	報酬額及び支払方法	本契約に基づく報酬額、報酬細目、支払時期及び方法は内訳書による。
	特約事項	再委託先がある場合には、再委託先も本契約の当事者として契約し、受託者乙と再受託者丙は、ともに同等な受託者としての義務を果たすものとする。

（省略）

参照：全国社会保険労務士会連合会「SRPⅡ認証制度　書類」
https://www.shakaihokenroumushi.jp/members/related_information/tabid/327/Default.aspx

参考　情報セキュリティ　ウイルス対策ソフト

【ウイルス対策ソフト】

- Microsoft Defender

Windows Defenderは、マイクロソフト社が提供する、Windows用のセキュリティソフトです。Windows 10以降のOSには標準でインストールされており、無料で利用できます。Windows Defenderは、ウイルスやスパイウェア、マルウェアなどの脅威からPCを保護するために設計されています。Windows Defenderは、リアルタイム保護、スキャン保護、ファイアウォールなどの機能を備えており、信頼性が高く、使いやすいと評価されています。Windows Defenderは、市販のセキュリティソフトと比較しても性能が高く、多くのユーザーから高い評価を受けています。

参考　情報セキュリティ　書類・パソコン破棄

年	書類　一般（保存期間　4年）	経営（保存期間　7年）	経営（保存期間　7年）	破棄日
2025				
2024				2024/●●/●

参考：現在（年）	2024	
2023	2023/12/31	1
2022	2022/12/31	2
2021	2021/12/31	3
2020	2020/12/31	4
2019	2019/12/31	5
2018	2018/12/31	6
2017	2017/12/31	7

年	パソコンの破棄（デスク・ノート）		ハード等	破棄日
2025				
2024	●●			2024/●●/●

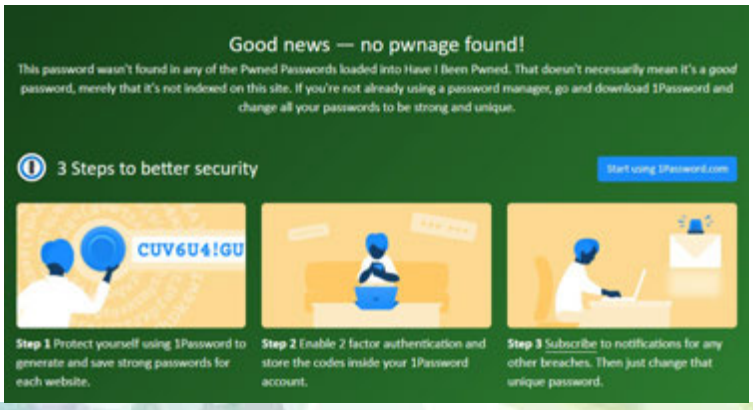
	サイト	主な利用	ユーザー名	メールアドレス	PW	URL
1	株式会社●●●	パソコン破棄（注文→破棄→証明書発行）				
2	株式会社●●	書類破棄（注文→破棄→証明書発行）				

参考　情報セキュリティ　パスワード管理

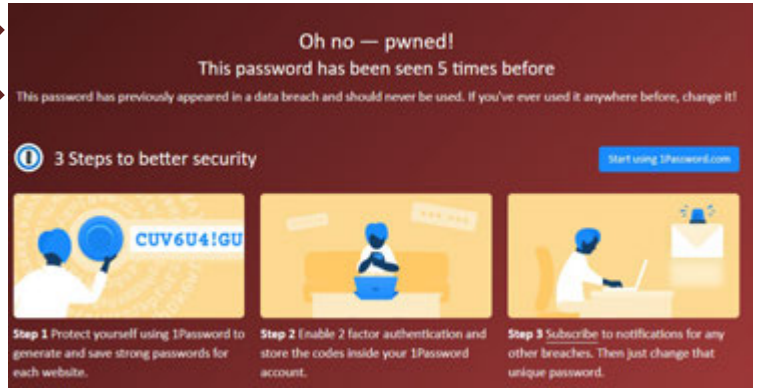
【パスワード】

- パスワードを作るときは以下のサイトで、過去に使われたことがあるパスワードか確認してください。また、理想的には定期的に確認する必要があります。
- https://haveibeenpwned.com/Passwords/
- 過去に使われたパスワードの場合、Oh no – pwned! と表示されるので、そのパスワードは使わないでください。
- 過去に使われたパスワードを使っていると、パスワードは見破られやすくなります。

○



×



参考　情報セキュリティ　パスワード管理

【前提】

ID/パスワードだけでは機密情報を守るには不十分ですが、せめてなるべく安全なパスワードを設定しましょう（＋多要素認証が使えれば設定しましょう）

【安全ではないパスワード】

□　IDとパスワードが同じである、またはパスワードにIDの一部が含まれている。
□　パスワードに、自分の名前、電話番号、誕生日を使っている。
□　パスワードに、「1234」や「1111」、「abcd」などの単純な羅列を使っている。
□　パスワードに、辞書にある単語をそのまま使っている。
□　連続したキーボード配列、単純な繰り返しで推測しやすいパスワードを使っている。
□　さまざまなサービスで、同じパスワードを使用している【SNS、ネットショップなど】。
□　他人に一度でもパスワードを教えたことがある。

【情報処理推進機構(IPA)の公式発表：安全なパスワード（定期変更は不要）】

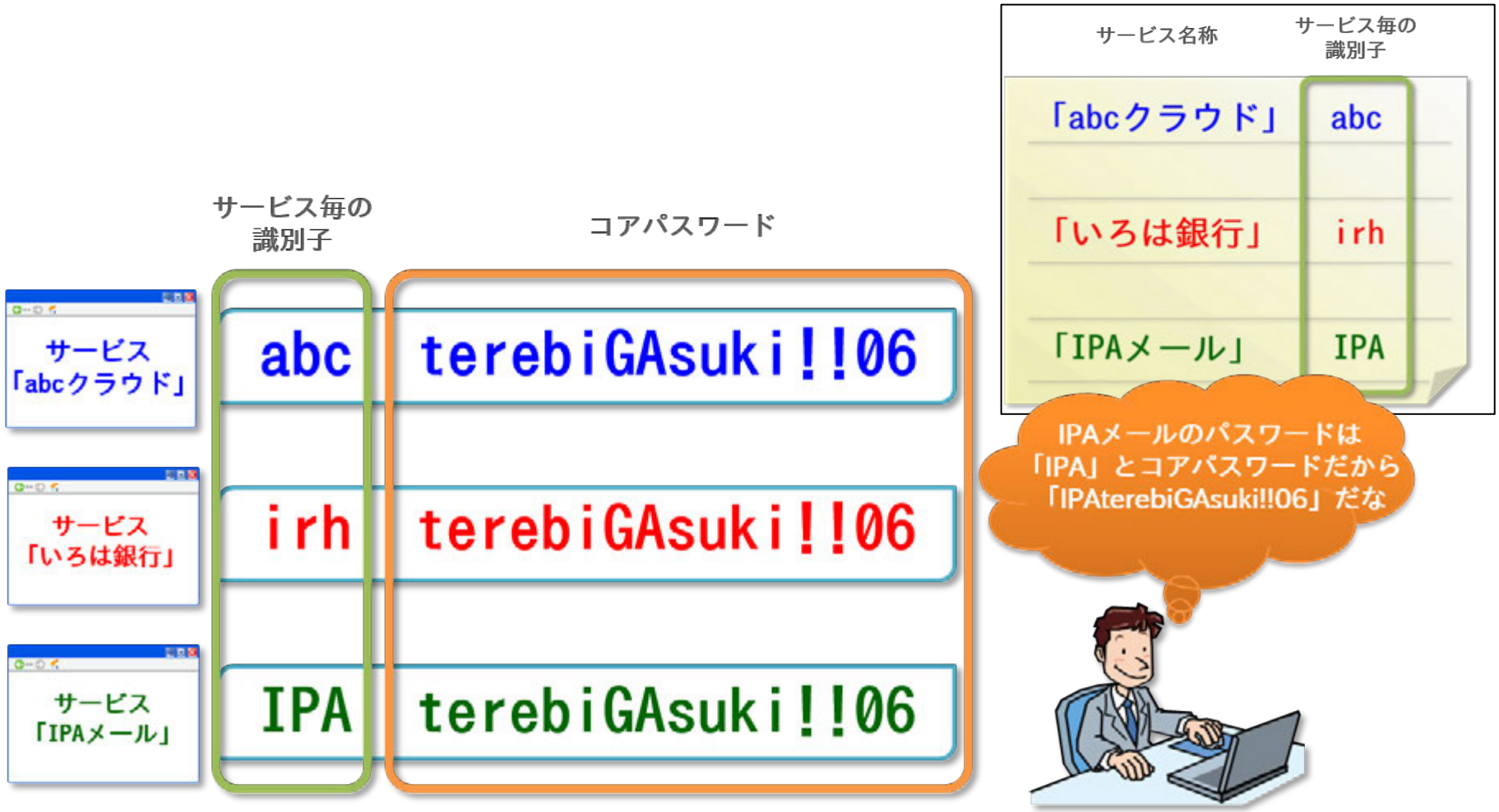
□　最低でも10文字以上の文字数で構成
□　パスワードの中にアルファベットの大文字と小文字の両方、数字や、「@」、「%」、「〃」などの記号も混ぜている
□　サービスごとに違うパスワードを設定している
　（例）コアパスワード＋各サービスパスワード

参考：https://www.ipa.go.jp/security/chocotto/
https://www.ipa.go.jp/security/anshin/attention/2016/mgdayori20160803.html

参考　情報セキュリティ　パスワード管理

参考：
https://www.ipa.go.jp/security/anshin/attention/2016/mgdayori20160803.html

参考　情報セキュリティ　パスワード管理



参考：
https://www.ipa.go.jp/security/anshin/attention/2016/mgdayori20160803.html

参考　情報セキュリティ　全社共通のルール

コンピューターウイルスに感染したときの対応（例）

コンピューターウイルスやランサムウェアに感染したかも？と思ったときの対処

コンピューターウイルスやランサムウェア（総称して「マルウェア」といいます）に感染したときには以下の症状が出ます。
ケース1：ファイルやアプリが暗号化されて開かない
ケース2：脅迫的な画面が表示される
ケース3：処理速度の低下・身に覚えのない通信
ケース4：不審なメールの添付ファイルやURLをクリックした
ケース5：心当たりのない通知・広告・ポップアップ画面が頻繁に表示される

1.とりあえずは**有線でも無線でもネットにつながる回線から切断（LANケーブルを抜く。Wifiを切断する）**した上で、**本体の電源はそのまま**にして、証拠保全を図りましょう。
2.出口**事務所内の相談窓口**に連絡して対処方法を相談しましょう。
3.社会保険労務士賠償責任保険の窓口
　安心110番(●●●●- ●●● - ●●●)もしくは
　コマ損賠責航空グループ(●●●●@ ●●●● . ●●)
詳細は以下のサイトを参照
https：●●●●●●

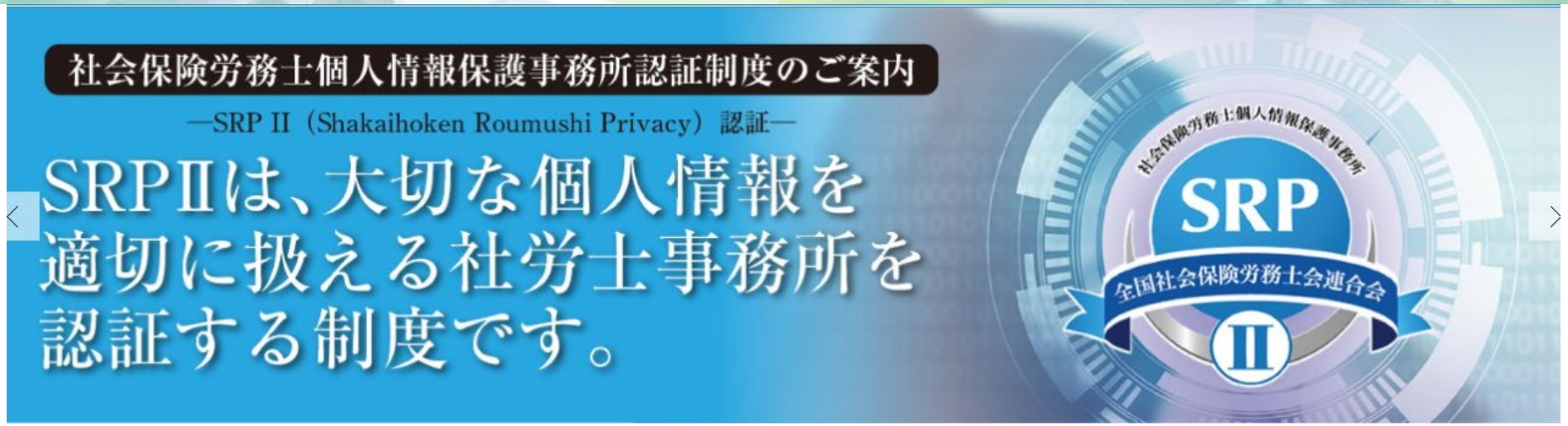
参考　情報セキュリティ　SECURITY ACTION

資料　SECURITY ACTION自己宣言
https://security-shien.ipa.go.jp/security/index.html

資料　５分でできる！自社診断 《設問に回答》
https://security-shien.ipa.go.jp/diagnosis/selfcheck/index.html

参照：IPA独立行政法人情報処理推進機構

参考　社会保険労務士個人情報保護事務所認証制度（SRPⅡ）



資料　SRPⅡ（社労士事務所における個人情報保護）
https://www.shakaihokenroumushi.jp/organization/tabid/507/Default.aspx

参照：全国社会保険労務士会連合会「ＳＲＰⅡ」

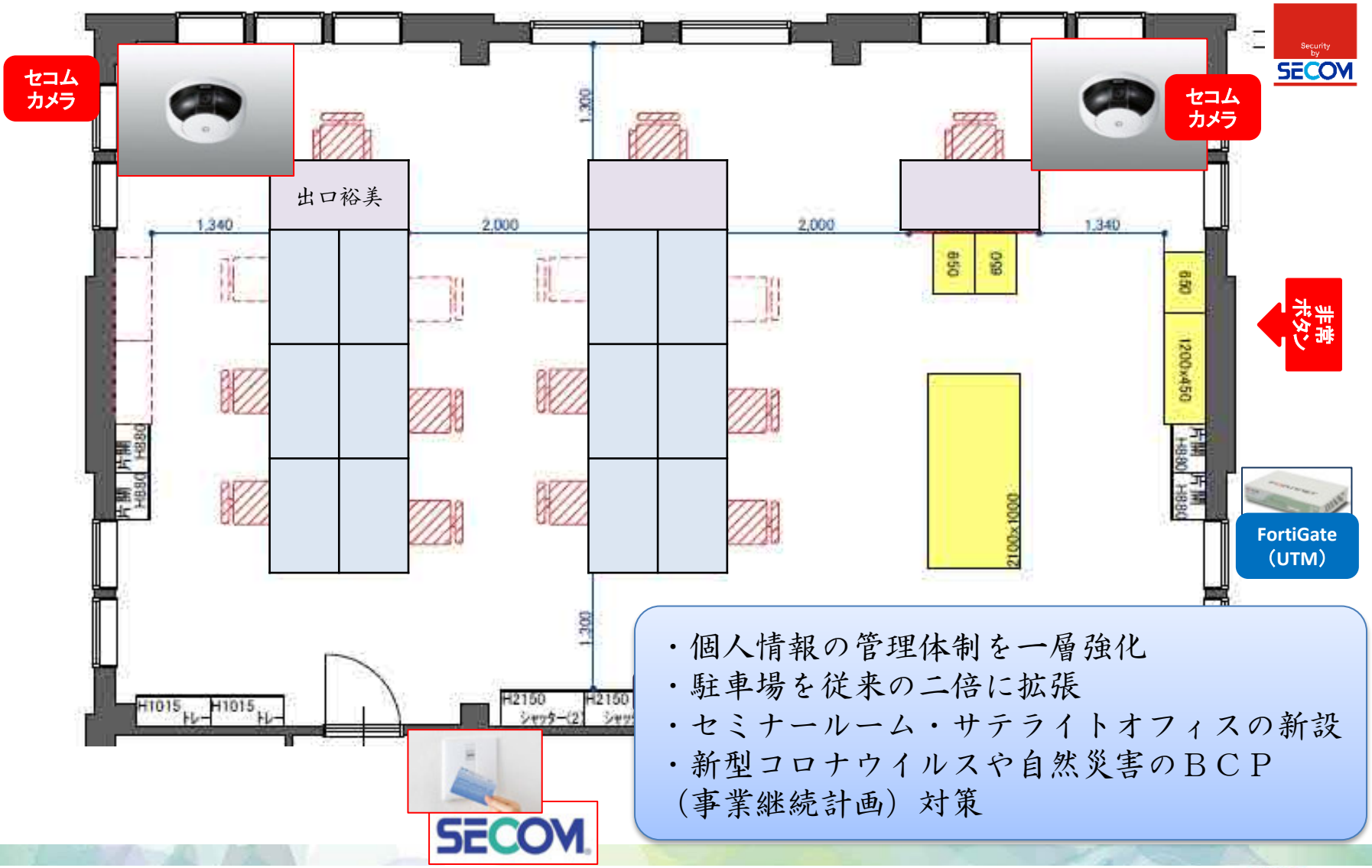
参考　出口事務所の取組事例

目標	出口事務所の事例
	・老齢・障害・遺族年金等の相談および請求 ・健康保険・介護保険等の相談および請求 ・労災保険等の相談および請求
	・大学生のインターンシップ導入 ・学生への労働保険・社会保険の教育 ・学生への働き方の教育 ・職員の子供達の職場見学
	・女性代表社員の対外的活動、執筆、講演 ・高い割合の女性管理職 ・多様な働き方導入コンサルティング

SDGs17の目標	SDGsの169ターゲット	出口事務所の事例
	11.b 2020年までに、包含、資源効率、気候変動の緩和と適応、災害に対する強靱さ（レジリエンス）を目指す総合的政策及び計画を導入・実施した都市及び人間居住地の件数を大幅に増加させ、仙台防災枠組2015-2030に沿って、あらゆるレベルでの総合的な災害リスク管理の策定と実施を行う。	・東京オフィスのレイアウト変更 ・栃木オフィスの設立・サテライトオフィス設置 ・地方創生テレワーク

参考　東京オフィス　セキュリティ・ネットワーク情報

栃木オフィス２階　セキュリティ・ネットワーク情報



・個人情報の管理体制を一層強化
・駐車場を従来の二倍に拡張
・セミナールーム・サテライトオフィスの新設
・新型コロナウイルスや自然災害のＢＣＰ（事業継続計画）対策

栃木オフィス１階　セキュリティ・ネットワーク情報

（サテライトオフィス兼セミナールーム）

セコム
カメラ

・職員達が
安心して働ける環境に
（施錠チェックの自動化）
・東京オフィスの職員も
サテライトオフィス勤務可

参考　東京オフィスと栃木オフィスの距離・移動時間

Point
適度な距離
BCP（事業継続計画）策定

東京オフィス（東京都新宿区）

電車等2時間20分

約
120
km

自動車1時間50分

栃木オフィス（栃木県鹿沼市）

さいごに

外務省
Ministry of Foreign Affairs of Japan

外務省について | 会見・発表・広報 | 外交政策 | 国・地域 | 海外渡航・滞在 | 申請・手続き

その他のお知らせ

社会保険業務で使用する外部システムへの不正アクセスについて

1 事案の概要

2 対象となり得る職員等

3 対象となるデータの項目

4 原因

5 二次被害又はそのおそれの有無及びその内容

6 本件に関するお問い合わせ先

外務省のホームページにも以下のような報告がありました

「5　二次被害又はそのおそれの有無及びその内容
　システムの診断調査を専業とするセキュリティ専門会社が、精密な調査を実施した結果、システム内の登録されていたデータが外部に転送された痕跡は確認されませんでした。また、登録されていたデータがダークウェブ等に掲載されていないか調査を実施しましたが、当該データの掲載や公開は確認されませんでした。このことを裏付けるように、本連絡時点までに不正利用など二次被害の報告も寄せられていません。」

外務省ホームページ
https://www.mofa.go.jp/mofaj/ms/h_w/page24_002288.html

さいごに

アマゾン ウェブ サービス（AWS）のホームページにも以下のような報告がありました

「社会保険労務士向けクラウドサービス『社労夢』などを提供する株式会社エムケイシステム。2,700 以上の社労士事務所が導入し、約 832 万人の個人情報を管理するサービスのセキュリティ強化に向けて、オンプレミス環境に構築していたサービス基盤を、アマゾン ウェブ サービス（AWS）に移行することを決定。着手から約 10 日で環境を構築し、AWS 上でのサービス提供を開始しました。」

アマゾン ウェブ サービス（AWS）ホームページ
https://aws.amazon.com/jp/solutions/case-studies/mk-system/

さいごに

社会保険労務士法人出口事務所
情報セキュリティ体制

システム障害だけではなく、自然災害等の対応も含めて
「こんなときどうするか」を常に考えて経営しております

専門家による調査の実施、アドバイスにより迅速な対応ができ
さらに情報セキュリティ体制が整いました

情報セキュリティ、個人情報保護の体制に終わりはありません
引き続きみなさまから信頼される社労士法人をめざします