




中小企業でのIT利活用によるテレワーク 実現に向けたガイドライン(在宅勤務編) (働き方改革研究会活動報告書)

2018年3月

一般社団法人コンピュータソフトウェア協会
働き方改革研究会

1	はじめに	6
2	活動目的	7
3	活動概要	8
4	在宅勤務セキュリティポリシーの概要	10
4.1	背景と要求事項	10
4.2	本ポリシー策定における基本的な考え方	11
4.3	本ポリシーのスコープ	11
4.4	ポリシーのスコープに含まれないもの	11
4.5	テーラリング	12
4.6	システム構成に対する基本的な考え方	12
4.7	遵守事項、推奨事項、許容事項について	12
4.8	関連ドキュメント	12
4.9	ポリシーの分類	13
5	在宅勤務におけるセキュリティポリシー(貸与端末、宅内LAN)	14
5.1	端末への要求事項	14
5.1.1	貸与PCのセットアップ	14
5.1.2	貸与PC のデータ管理	14
5.1.3	貸与PCの脆弱性管理	15
5.1.4	貸与PCの暗号化	15
5.1.5	貸与PCのアンチウイルスソフトによる完全スキャン	15
5.1.6	貸与PCのアンチウイルスソフトによる電子メールの検知	16
5.1.7	貸与PCと宅内の他の端末との通信遮断	16
5.1.8	貸与PCのRDP接続の禁止、デフォルトポートの変更	16

5.1.9	貸与PCのローカルAdministratorのパスワード	17
5.2	宅内LAN、宅内端末への要求事項	17
5.2.1	宅内LANでの探索、共有	17
5.2.2	無線LANの Protokol	17
5.2.3	エッジルーターのパケットフィルタ	18
5.2.4	宅内端末のアンチウイルスソフトと脆弱性管理	18
6	在宅勤務におけるセキュリティポリシー（Active Directory）	20
6.1	ドメイン	20
6.1.1	ドメインで使用可能な Protokol	20
6.1.2	ドメインアカウントポリシー	20
6.1.3	ビルトインアカウント	21
6.1.4	セキュリティグループの監査	21
6.2	ドメイン端末	21
6.2.1	端末のネットワーク探索、ファイルとプリンターの共有	21
6.3	サーバー	22
6.3.1	サーバーのアンチウイルスはクライアントとは異なる製品を採用する	22
6.3.2	サーバーのRDP接続のデフォルトポート	22
6.3.3	AdministrtorアカウントでサーバーへのRDP接続を行わない	23
7	在宅勤務におけるセキュリティポリシー（VPN・その他通信）	24
7.1	VPN	24
7.1.1	VPNの方式検討	24
7.1.2	VPN装置の脆弱性	24
7.1.3	VPN接続時のクレデンシャル(ID、パスワード等の認証情報)	24
7.1.4	大規模な通信障害	25
7.1.5	VPN接続の否認	25
7.1.6	RADIUS Server	25
7.2	その他通信	25
7.2.1	Firewall、Proxy	25
7.2.2	Video会議	26
8	在宅勤務におけるセキュリティポリシー（ログ）	27
8.1	通信装置	27
8.1.1	VPN装置、ルーターのログ	27
8.2	Windows	27
8.2.1	Windows Serverのログ	27
8.2.2	Windowsクライアント(貸与端末を含む端末)のログ	28
8.3	ログの統合分析	28
8.3.1	ログの統合的分析・管理	28
9	在宅勤務におけるセキュリティポリシー（規程）	29
9.1	データの暗号化	29
9.2	クレデンシャルの保全	29
9.3	在宅勤務で使用される貸与端末の管理	30

9.3.1	貸与端末の管理規程をユーザーに理解させ、遵守することを合意する	30
9.3.2	貸与端末の個人利用の禁止	30
9.3.3	貸与端末の無許可ソフトウェア、クラウドサービスの使用禁止	30
9.3.4	USBメモリの運用	31
10	在宅勤務におけるセキュリティポリシー（教育）	32
10.1	ブラウザがTLSの状態であることを理解させる。	32
10.1.1	Internet Explorer 11 でTLS (HTTPS) 接続した状態  が表示される	32
10.1.2	Internet Explorer 11 で  アイコンをクリックした際の認証情報の表示	32
10.1.3	Internet Explorer 11 で非TLS(HTTP)接続した状態  が表示されない	32
10.1.4	TLS(HTTPS)通信とは	33
10.2	最新のマルウェアの動向や、ソーシャルエンジニアリングの手法を理解させる	34
10.2.1	2018年のセキュリティ脅威の動向	34
10.2.2	フィッシングメールの例と対策	35
10.2.3	マルウェア添付メールの例と対策	36
10.3	アンチウイルスソフトのパターンファイルの操作方法を理解させる	38
10.3.1	アンチウイルスソフトのパターンファイルの重要性	38
10.3.2	パターンファイルのアップデートの確認方法(トレンドマイクロ)	38
	Corp. サーバをアップデートする	38
10.3.3	パターンファイルのアップデートの確認方法(シマンテック)	39
	SEP Cloudをアップデートする	39
	ノートンをアップデートする	40
10.4	電子メールは暗号化されず、平文で通信が行われていることを理解させる	41
10.4.1	インターネットでの電子メール	41
10.4.2	添付ファイルのパスワードの設定方法	41
11	在宅勤務セキュリティチェックリスト	42
11.1	セキュリティポリシーの内容	42
11.2	当社の評価(グレーの網掛け部分)	42
11.2.1	在宅勤務で取り扱う情報資産の種類	42
11.2.2	起こりえるリスクと事業継続への影響度合い	42
12	事例紹介	44
事例紹介1	株式会社内田洋行	44
	「生産性20%アップさせた営業部門の働き方変革自社実践事例」	44
事例紹介2	freee株式会社	46
	「全ての業務をクラウド化して業務効率化余剰時間の創出」	46
事例紹介3	株式会社ウェブインパクト	49
	「オフィスを捨てて完全ノマドワーキング化で10年の報告。～海外を見ずに国内の地方を見よ～」	49
事例紹介4	サイボウズ株式会社	52
	「100人いれば100通り 理想でつながるチームとは」	52
13	中小企業のテレワークを考える	58

中小企業におけるテレワークの課題	58
我々の考えるテレワーク	58
テレワーク自体の課題	59
(参考) モデル実証実験を経て	60
14 コラム	61
テレワークを加速するために必要なこと ～会社に来なくても良い環境づくり～	61
支出精算処理はスマホのワークフローで効率化！	61
いつでも、どこでも、誰もが簡単にテレビ会議ができる環境！	61
紙の重要資料(社外秘・秘密情報)は電子化！	62
社内連絡は電話ではなくチャット！	62
15 テレワークに関わる製品・サービス紹介	63
15.1.1 製品・サービス分類／仮想デスクトップ方式	63
15.1.2 製品・サービス分類／クラウド型アプリ方式	63
15.1.3 製品・サービス分類／会社PCの持ち帰り方式	65
15.1.4 製品・サービス分類／勤怠管理ツール	65
15.1.5 製品・サービス分類／業務管理(プロジェクト管理)ツール	67
15.1.6 製品・サービス分類／ペーパーレス化ツール	67
15.1.7 製品・サービス分類／安全なモバイルテレワークツール	67
15.1.8 製品・サービス分類／RPAツール	68
15.1.9 製品・サービス分類／コンサルティングサービス	68
15.1.10 製品・サービス分類／その他	69
16 研究会参加メンバー一覧	73

1

はじめに

日本の労働生産性が低いとよく言われます。

2015年の日本の労働生産性は、74,315ドル(783万円)でした。これは、OECD加盟35カ国の中でみると22位にあたるそうです。アメリカ合衆国は121,187ドルで、日本の1.63倍です。同じ仕事をして1.63倍の価値を生み出しています。

本当でしょうか。

産業別にみると、製造業、建設業、卸小売飲食宿泊、情報通信、金融保険、不動産、教育・社会福祉サービス、娯楽・対個人サービス、農林水産業でみても1.63倍もアメリカが上回っている産業はありません。中には、日本の方が生産性が上回っている産業も存在します。

(参考：Ⅲ 労働生産性の国際比較 - 公益財団法人日本生産性本部

http://www.jpc-net.jp/annual_trend/annual_trend2015_3.pdf)

そんなに日本人の能力が低いとは思えません。日本人の労働生産性は言われているほど、低い訳ではないと考えます。しかし、労働人口の減少は、現実の問題であり、いかに少ない人数で従来 of 価値を創造するかに重点を置く必要があります。

このための生産性向上は、ワークライフバランスを含めた働き方改革で実現されなければいけません。大変重要な課題であり、ICT産業に従事する我々がその責務を担うべく検討を重ねて参りました。

働き方改革でいわれる多様な働き方の一つに、ICTを活用して時間や場所を有効に活用できるようにするテレワークがあります。

テレワークは、在宅勤務、サテライトオフィス勤務、モバイルワークに分類され、まずはテレワークの在宅勤務に絞って検討を進めて参りました。

検討が進むにつれ、会社の規模、ICTへの知識や取り組み状況、従業員の職種と多種多様な状況が考えられ、いわゆるガイドラインとして教科書的にこれだけ守っていれば良いというものを作り上げることは非常に難しいので、本書では、テレワーク実現に向けた気づき、心得のような形でまとめました。

不十分な部分、飛躍しすぎた結論もあると思われませんが、皆様の生産性の向上にお役に立つ内容となっていることを期待しております。

2018年3月

一般社団法人コンピュータソフトウェア協会

働き方改革研究会 主 査 中村 憲司

副主査 村瀬 正典

2

活動目的

最近の企業のビジネスの在り方は、インターネットの普及や人工知能（AI）、IoTなどの技術革新の進展により多様になってきており、経済の成長力の引き上げを実現するためには、年功や雇用形態にかかわらず、成果や職務、職責に対し、報酬を支払う雇用システムへの進化が必要です。また、技術革新により時間と空間を超えた働き方が進展し、働く方個々人のライフスタイル、ライフステージで様々なニーズ（100人100通りの働き方）も出ています。

年齢にかかわらず優秀な人材・技術者を集めるとともに、新たな仕事に取り組める人材の育成を行い、第4次産業革命をけん引していくため、一般社団法人コンピュータソフトウェア協会も働き方改革を積極的に進めるべく、次の目標を掲げました。

1. 長時間労働の根絶

主要な会員企業の平均所定外労働時間は月20時間程度と低い水準であります。さらに働き方改革を進めることで、魅力的な業界として年齢にかかわらず優秀な人材を集めていきます。

2. 多様な働き方の推進（象徴としてのテレワークの先行）

テレワーク（在宅勤務）の導入、高齢者等を含めた柔軟な再雇用制度、公正な人事評価に役立つITスキルの『見える化』（iCD【i コンピテンシ ディクショナリ】）の普及促進、副業の自由化などを進めることで、会員各社が、従業員にとって働き易く、労働意欲を高める労働環境や人事制度を導入し、多様な働き方を認めることが重要と考えます。

こうした取組を進めていく象徴としてテレワーク（在宅勤務）の導入を先行すべく、会員各社の導入支援のための、中小企業でのIT利活用によるテレワークガイドラインとなる指標を策定することを目指しました。

それと同時に、会員各社の製品・サービスがテレワーク導入の際の有効なツールとして、広く周知され活用されることを期待します。

28CSAJ 第180号
平成29年2月6日

働き方改革宣言

一般社団法人 コンピュータソフトウェア協会
会長 萩原 博典

最近の企業のビジネスの在り方は、インターネットの普及や人工知能（AI）、IoTなどの技術革新の進展により多様になってきており、経済の成長力の引き上げを実現するためには、年功や雇用形態にかかわらず、成果や職務、職責に対し、報酬を支払う雇用システムへの進化が必要です。また、技術革新により時間と空間を超えた働き方が進展し、働く方個々人のライフスタイル、ライフステージで様々なニーズ（100人100通りの働き方）も出ています。

年齢にかかわらず優秀な人材・技術者を集めるとともに、新たな仕事に取り組める人材の育成を行い、第4次産業革命をけん引していくため、次の目標を掲げ、当協会も働き方改革を積極的に進めてまいります。

1. 長時間労働の根絶

当協会において、主要な会員企業の平均所定外労働時間は月20時間程度と低い水準であります。さらに働き方改革を進めることで、魅力的な業界として年齢にかかわらず優秀な人材を集めていきます。

2. 多様な働き方の推進（象徴としてのテレワークの先行）

当協会において、テレワークの導入、高齢者等を含めた柔軟な再雇用制度、公正な人事評価に役立つITスキルの『見える化』（iCD【i コンピテンシ ディクショナリ】）の普及促進、副業の自由化などを進めることで、会員各社が、従業員にとって働き易く、労働意欲を高める労働環境や人事制度を導入し、多様な働き方を認めることが重要と考えます。

こうした取組を進めていく象徴としてテレワークの導入を先行させていただきます。具体的には、会員各社の導入支援のための『中小企業でのIT利活用によるテレワークガイドライン（仮称）』を早急に策定するとともに、2020年までにテレワーク率30%を目指していきます。

3

活動概要

働き方改革研究会に関わる平成29年度活動を時系列で列記しています。

- 平成29年3月24日(金)開催
(働き方改革研究会 準備会／参加30社39名)
議題：主査挨拶
参加各社の取り組み紹介（自己紹介含む）
政府の動きについて（経済産業省）
ディスカッション
セキュリティ委員会からのご提案
- 平成29年5月25日(木)開催
(働き方改革研究会×経営力向上研究会共催：第26回経営力向上セミナー／参加26社31名)
タイトル「残業時間を減らしても、業績アップ!」～働き方改革を成功に導く3つの秘訣～
- 働き方改革で業績向上する3つの成功ポイント
講師：一之瀬 幸生 氏（セントワークス株式会社 ワークライフバランスコンサルタント）
概要：様々な環境の変化と働き方改革の本質
特別なコストをかけなくても出来る働き方改革3つのポイント
- 平成29年6月1日(木)開催
(働き方改革研究会×法務・知財委員会共催：第25回座談会／参加25社31名)
タイトル「働き方改革に伴う、就業規則見直しの留意点」
- 働き方改革に伴う、就業規則見直しの留意点
説明：末 啓一郎 氏（ブレイクモア法律事務所 弁護士）
- 最近の法務知財の旬な話題について
説明：黒住 哲理 氏、村田 和希 氏（ブレイクモア法律事務所 弁護士）
- 平成29年7月19日(水)開催
(第1回働き方改革研究会／参加18社26名)
議題：主査挨拶および研究会スコープについて（アンケート結果含む）
政府の動きについて（経済産業省）
副主査報告
働き方改革事例紹介と意見交換
事例紹介1：株式会社内田洋行「生産性20%アップさせた営業部門の働き方変革自社実践事例」
事例紹介2：freee株式会社「全ての業務をクラウド化して業務効率化余剰時間の創出」
- 平成29年8月8日(火)開催
(第1回セキュリティWG／参加8社8名)
議題：テレワークにおけるセキュリティを考える
- 平成29年8月29日(水)開催
(第2回働き方改革研究会／参加19社24名)
議題：働き方改革事例紹介と意見交換
事例紹介1：株式会社ウェブインパクト

「オフィスを捨てて完全ノマドワーキング化で10年の報告。

～海外を見ずに国内の地方を見よ～

事例紹介2：サイボウズ株式会社「100人いれば100通り 理想でつながるチームとは」

- 平成29年9月14日(木)開催
(第2回セキュリティWG/参加8社9名)
議題：テレワークにおけるセキュリティガイドの検討

- 平成29年9月27日(水)開催
(第3回働き方改革研究会/参加14社17名)
議題：セキュリティガイドに係る方向性について
IoT健康経営の取り組みについて
事例紹介：サイバートラスト「旭川のリモートワークを始めたきっかけ、
健康管理の仕組み(システム)、エビデンス・効果、今後と課題」

- 平成29年10月27日(金)開催
(CSAJ働き方改革研究会・人材育成研究会主催 袋井市(静岡県)、ふくろい生涯現役促進連携協議会共催
高齢者雇用推進セミナー/参加18社41名)
タイトル「第4次産業革命時代におけるIT技術者育成を担う高齢者の役割とは？」
～CSAJ高齢者雇用推進ガイドラインの活用事例紹介～
 - 講演1 生涯現役促進地域連携事業「ふくろいTaskAruネットワーク」の取り組みについて
村田 雅俊 氏(ふくろい生涯現役促進連携協議会事務局長(袋井市産業環境部産業政策課長))
 - 講演2 機構の支援制度について
(独)高齢・障害・求職者雇用支援機構(JEED) 静岡支部
 - 講演3 「コンピュータソフトウェア業 高齢者雇用推進ガイドライン」について
梅澤 隆 氏(国土舘大学 政経学部経済学科 教授(元:CSAJ高齢者雇用推進委員会 委員長))
 - 事例紹介 CSAJ高齢者雇用推進ガイドライン活用事例紹介
山本 祥之 氏(株式会社インテリジェントウェイブ 特別顧問)
佐藤 隆一 氏(株式会社フォーラムエイト東京本社 システム開発グループ主事)
 - パネルディスカッション
モデレータ
富田 伸一郎 氏(CSAJ人材育成研究会主査)
 - パネラー
中村 憲司 氏(CSAJ働き方改革研究会主査)
梅澤 隆 氏(国土舘大学 教授)
山本 祥之 氏(株式会社インテリジェントウェイブ)
佐藤 隆一 氏(株式会社フォーラムエイト)

- 平成29年12月5日(火)開催
(働き方改革研究会・セキュリティ委員会・セキュリティWG合同検討会/参加18社22名)
議題：政府の動きについて(経済産業省)
セキュリティガイドに係る検討
テレワーク推進センターに関する情報提供

4

在宅勤務セキュリティポリシーの概要

4.1 背景と要求事項

CSAJ働き方改革研究会では、ソフトウェア産業の生産性の向上と人材の確保・育成を目指し、多様な働き方や勤務形態、そしてこれらを支える労働契約のあり方を研究しています。総務省統計局の社会生活基本調査¹によると、都道府県別の一日当たりの通勤時間は以下の通りとなっています。

表 4-1

順位	都道府県名	通勤時間
1	神奈川県	1時間45分
2	千葉県	1時間42分
3	埼玉県	1時間36分
4	東京都	1時間34分
5	奈良県	1時間33分
6	大阪府	1時間25分
7	兵庫県	1時間21分
8	京都府	1時間20分
9	茨城県	1時間19分
9	愛知県	1時間19分

少子高齢化社会を迎え介護の負担は増加傾向にあり、加えて、雇用情勢の圧迫から女性の活躍が期待されることですが、育児を取り巻く環境は依然として厳しいものがあります。こうした中で、多様な働き方の一つに在宅勤務があり、社会一般に、介護や育児をする方々や障害者の方々の有力な勤務形態と考えられています。また、通勤時間と睡眠時間には弱い逆相関があり、通勤時間の削減によって、ストレスの解消や質の高い睡眠を得られれば、メンタルヘルスの維持・向上にも資するとも考えられます。

- 介護や育児で通勤勤務が難しい人材も活用できる
- 「痛勤」から解放されることでストレスが軽減される
- 通勤時間を新たな自由な時間として活用できる

一方で、CSAJ会員企業での在宅勤務の実現には以下の課題があると考えられます。

- 多くの在宅業務では企業ネットワークとVPN接続が必要
- 宅内ネットワークのセキュリティ状況やネットワークへの接続状況が一律でない
- 顧客のシステム情報や営業情報、状況に応じて個人情報を取り扱うケースがあり得る
- リスク回避のための新たな設備投資や運用負担の増加が見込まれる
- 新たな就業規則や運用規程の策定や従業員教育が必要となる

特に、企業ネットワークのセグメントが社員の自宅まで延長されるにも関わらず、その形態は様々なものが想定でき、企業内とは異なり一律にセキュリティポリシーを定めることが困難です。在宅勤務におけるリスク分析や懸念事項の解消は、システム管理側にとって非常に大きな負担と言わざるを得ません。

¹ <http://www.stat.go.jp/data/shakai/2016/rank/index.htm>

そこで、こうした問題を解決すべく、CSAJ働き方改革研究会と同セキュリティ委員会は合同で Working-group を結成し、CSAJ会員とコンピュータソフトウェア企業に向けた在宅勤務でのセキュリティポリシーの策定に着手しました。

4.2 本ポリシー策定における基本的な考え方

策定にあたっては、様々な在宅勤務の様態がありリスクが大きく異なることから、次のような考え方をとりました。

- 会員の企業規模に関わらず汎用的に使用できるものを目指し、かつ、在宅勤務を検討する際の「気づき」となるように構成する
- 成果物の改変を自由に、また容易にする
- ISMS、P マーク、情報安全確保支援士等の資格取得を前提としない
- 標準的と考えられるシステム構成を前提としてシステムのスコープを絞るが、異なるシステムでも読み替えが容易であること
- 在宅側のセキュリティ項目(課題)を具体的に網羅するとともに、自己分析が可能なツールを用意する
- 従業員のセキュリティレベルの底上げを図り、会員企業のセキュリティ向上に資するものとする

4.3 本ポリシーのスコープ

前述のように、在宅勤務には、様々な形態が考えられることから、本ポリシーは、以下をスコープおよび前提条件として策定されています。

- **対象企業:** CSAJ の会員の大半をなす、50 名以下のソフトウェア企業での利用を可能とします。
- **対象ユーザー:** 対象企業の従業員、役員とします。また、アプリケーション開発に携わる IT リテラシーを有しているが、セキュリティの専門家ではありません。
- **業務内容:** 顧客もしくは自社のアプリケーション開発(企画、要件定義、外部設計、内部設計、保守)と、関連するドキュメントの作成やデータの作成を含む)であり、完全性、機密性、可用性の確保と、責任追及性と否認防止が求められる業務を前提にしています。
- **端末:** Windows PC であり会社貸与品としています。BYOD は対象外です。
- **宅内 LAN 環境:** 有線もしくは無線 LAN を利用し、エッジルーターには一般的な家庭用ルーターを利用し、ISP を通じてインターネット回線に接続していることを想定しています。スマートフォンでのテザリングはこの範疇に入ります。また、家族、第三者が会社貸与以外の端末を LAN に接続していることを前提にしています。
- **企業 LAN 環境:** 企業側のネットワークには Firewall および VPN 装置が設置されており、Active Directory によるドメインの構築とユーザー管理が行われていることを前提としています。
- **運用:** セキュアな運用を支えるシステム以外の「規程」や「教育」を包含しています。

4.4 ポリシーのスコープに含まれないもの

本ポリシーのスコープには、以下が含まれないことに注意してください。

- アプリケーション開発におけるセキュアコーディング、ソース管理、セキュリティ品質向上はスコープ外としています。
- 個人情報、センシティブな情報の保護のためには、個別のリスクに応じて必要とされる機能や役割の追加が必要です。これらの保護を保証するものではありません。



4.5 テーラリング

本ポリシーは事業状況、利用状況に応じて、テーラリング (tailoring) できるものとし、不足している機能を追加したり、過剰と思われる項目を削除したり、現状の業務にあわせて改変することは自由です。リスク分析に基づいたテーラリングを推奨します。また、テーラリングのためのチェックリストを用意しています。



4.6 システム構成に対する基本的な考え方

セキュリティ確保のためには、一定のコストがかかりますが、WindowsおよびActive Directoryの標準機能をベースに、ポリシー確保のための必要最低限のシステム及び機器の導入を前提としています。

- Active Directory (Windows Server 2008R2 以上)
- RADIUS Server (Windows Server NPS を含みます)
- Firewall (機能を有するルーターを含みます)
- VPN 装置 (Firewall との兼用、機能を有するルーターを含みます。プロトコル: L2PT/IPSec、PPTP、TLS-VPN 等はリスクに応じて検討すべきであり、定義はしていません。)
- アンチウイルスソフトウェア



4.7 遵守事項、推奨事項、許容事項について

ポリシーは想定状況や事例に応じて、遵守事項 (SHALL: するものとする、SHALL NOT: しないものとする) と、推奨事項 (SHOULD: すべきである、SHOULD NOT: すべきではない)、許容事項 (MAY: してもよい、NEED NOT: しなくてもよい) を記述していますが、あくまでも目安であり、会員企業のリスクに応じた整合性が確保されとは限らないことに留意してください。



4.8 関連ドキュメント

- 情報セキュリティ
<https://ja.wikipedia.org/wiki/%E6%83%85%E5%A0%B1%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%AA%E3%83%86%E3%82%A3>
- NIST Special Publication 800-63-3 Digital Identity Guidelines
<https://pages.nist.gov/800-63-3/sp800-63-3.html>
- 府省庁対策基準策定のためのガイドライン(平成 28 年度版)
平成 28 年 8 月 31 日 内閣官房 内閣サイバーセキュリティセンター
<https://www.nisc.go.jp/active/general/pdf/guide28.pdf>



4.9 ポリシーの分類

ポリシーは以下の分類を策定しています。

- 貸与端末、宅内 LAN
- Active Directory (企業側)
- VPN・その他通信
- ログ
- 規程
- 教育

このうち、規程と教育については、ポリシーの例示だけでは具体性に欠けるため、実際に使用可能な規定内容や教育コンテンツを示しています。

なお、規程については、会員企業の就業規則や既存の規程との整合性は保証されないため、適用にあたっては十分な留意が必要です。また、教育は常に最新の状況をフォローすべきものであり、従業員のセキュリティ知識にみあったコンテンツを適宜、提供することが重要です。

5

在宅勤務におけるセキュリティポリシー (貸与端末、宅内LAN)



5.1 端末への要求事項

従業員に貸与される端末は以下の要求を満たさなければならない。

5.1.1 貸与PCのセットアップ

社内利用したPCを在宅端末に転用する場合：

意図しない、存在を意識していないデータ、ソフトウェアの排除のため、サポート中のWindowsが新規にセットアップされ、最新のセキュリティパッチが適用され、アンチウイルスソフトの稼働、パターンの更新が確認されたものであることを管理者が確認する。(遵守事項)

ユーザーが利用中の端末を在宅端末に転用する場合：

意図しない、存在を意識していないデータ、ソフトウェアの排除のため、最新のセキュリティパッチが適用され、アンチウイルスソフトの稼働、パターンの更新が確認されたものであり、重要な企業情報、個人情報が含まれていないことを管理者が確認する。(遵守事項)

使用中のPCには、意図しないもしくは存在を認識していないアプリケーションやオープンソース、企業の情報資産や個人情報が存在する場合がある。利用者及び管理者が認識していないソフトウェアは脆弱性管理がなされない可能性があるため、情報漏洩の原因となることを排除するためである。

企業情報、個人情報は在宅端末のローカルストレージには保存されないことを前提にポリシーを設計しているためである。

5.1.2 貸与PC のデータ管理

必要なデータの管理手順：

業務に必要なデータだけが貸与端末に存在し、業務に必要なデータの管理手順を管理者とユーザーが合意するため、PCの貸与時点でのOS、デスクトップアプリケーションソフト、クラウドシステム、使用するブラウザ、java、Flash、IME (Input Method)、開発ツール、コミュニケーションツール、オープンソース、フリーソフトウェア等、搭載されているすべてのソフトウェアのバージョン、サービスパックの適用状況を管理者とユーザーが把握する。(遵守事項)

成果物やデータ受け渡しの際の暗号化方式やパスワード等のカギの管理、バージョン管理、その他必要な手順を管理者とユーザーが合意する。(遵守事項)

必要に応じて資産管理システムを用いて集中管理を行い、PCの貸与時点での搭載されているすべてのソフトウェアのバージョン、サービスパックの適用状況を管理者が把握する。(許容事項)

ユーザーが使用するソフトウェアやデータの特性、性質、品質を、管理者とユーザーが把握することは、企業のセキュリティを維持するために極めて重要であり、脆弱性対策には欠かせない事項である。また、生成もしくは加工された成果物やデータには、企業情報や個人情報が含まれること、一般的に社外秘の情報であることから、これらのバージョン管理や、受け渡しの手順、暗号化方式、パスワードのやり取りの

方法などを定め、合意する必要がある。危殆化した暗号化方式や電子メールの非暗号化添付などは情報漏洩の恐れを否定できず、インシデントが発生した場合、情報漏洩の原因の一つとして調査する必要がある。このような無用な調査を防ぐ意味でも、この合意は重要となる。

ソフトウェア管理、データ管理の上で、その労力を削減するため資産管理ソフトを利活用することは推奨される。

5.1.3 貸与PCの脆弱性管理

OS、ミドルウェア、アプリケーションの脆弱性管理手順：

OS、デスクトップアプリケーションソフト、クラウドシステム、使用するブラウザ、java、Flash、IME (Input Method)、開発ツール、コミュニケーションツール、オープンソース、フリーソフトウェア等、搭載されているすべてのソフトウェアの脆弱性パッチの適用状況を管理者が把握するため、業務に必要なシステムの管理手順（パッチ適用、状況の報告等）についてユーザーと管理者が合意する。（遵守事項）

必要に応じて資産管理システムを用いて集中管理を行い、PCの貸与時点での搭載されているすべてのソフトウェアのバージョン、サービスパックの適用状況を管理者が把握する。（許容事項）

ユーザーが使用するすべてのソフトウェアの脆弱性を管理者とユーザーが把握することは、セキュリティ維持の根本であり、データの把握と同様に欠かせない事項である。オープンソースやフリーソフトウェアについては、管理者だけでなくユーザー自身にも定期的にダウンロードサイトの確認を求めるなどし、また、バージョンアップやディスコン、EOL情報については、他の開発者と共有することが求められる。前項同様、資産管理ソフトの利活用は推奨される。

5.1.4 貸与PCの暗号化

貸与PCのハードディスク暗号化手順：

貸与PCの紛失、盗難に備えて、貸与端末のハードディスクをBitLockerで暗号化し、ハードディスクから直接データが読み出されないように設定する。BitLockerの復号鍵は印刷し、管理者が安全に保管する。管理者は復号鍵の受け渡しや復号手順を定める。（遵守事項）

PCのハードディスクを抜き出し、他のPCに接続することでハードディスクの情報を抜き出すことが可能である。紛失や盗難にあった際、悪意ある者による情報漏洩を防ぐため、Windowsの標準機能であるBitLockerでのハードディスク暗号化が必要となる。

5.1.5 貸与PCのアンチウイルスソフトによる完全スキャン

貸与PCのアンチウイルスソフト完全スキャン手順：

マルウェアに感染した時点でアンチウイルスソフトが未対応であり、マルウェア感染が見逃されることを防ぐために、月に2回以上、アンチウイルスソフトのパターンファイルを最新に更新したうえで、貸与端末に接続されているすべてのドライブを完全スキャンする。管理者は完全スキャンの手順を定め、ユーザーとともに実施状況を把握する。（遵守事項）

アンチウイルスソフトの管理システムを利用し、完全スキャンの自動スケジューリング、実施状況やマルウェアの検出状況を把握する。（推奨事項）

新たなマルウェアが発生した時点で、アンチウイルスソフトウェアがそのハッシュ値やふるまい、特徴を把握しておらず、マルウェアとして認識せずに見逃してしまうことがある。一方で、独自の情報収集や利用者からの報告によって、マルウェアを認識するように日々パターンファイルや認識メカニズムは更新さ

れている（この間はマルウェアが潜伏しているdeltaとなる）。そこで、見逃した潜伏しているマルウェアを検出するには、すべてのファイルをスキャンする完全スキャンが必要となる。他方、完全スキャンには時間がかかることが多く、その間、PCの動作が重くなることから敬遠されるが、昨今の状況を鑑みるとできるだけdeltaを短くすることが必要である。

アンチウイルスソフトウェアの管理システムによって労力を軽減することは推奨される。

5.1.6 貸与PCのアンチウイルスソフトによる電子メールの検知

貸与PCのアンチウイルスソフトの電子メール検知手順：

マルウェアの感染源として、電子メールの添付ファイルや埋め込まれたリンクがあげられることから、電子メールのアンチウイルスソフトによるマルウェア検出を実施する。管理者は電子メールの検知設定の手順を定め、ユーザーとともに検出設定、検出状況を把握する。（遵守事項）

アンチウイルスソフトの管理システムを利用し、電子メールのマルウェア検出設定や検出状況を把握する。（推奨事項）

マルウェアの大半は電子メールを利用して感染を拡大する。多くのアンチウイルスソフトウェアは電子メールの添付ファイルに潜むマルウェアを検出できるようになっているが、必ずしもデフォルト値で電子メールのマルウェア検出を行うとは限らない。また、ユーザーが故意にもしくは誤って設定を変更してしまう可能性もあることから、管理者とユーザーは検出設定や状況を把握することが重要である。アンチウイルスソフトウェアの管理システムの利用は前項同様である。

5.1.7 貸与PCと宅内の他の端末との通信遮断

貸与PCの（Windowsもしくはアンチウイルスソフトの）パーソナルファイアウォールの設定手順：
宅内の他の端末からのマルウェア感染やリモート操作などによる、情報漏洩、改ざん、サービス停止を防ぐために、貸与端末のパーソナルファイアウォールの接続拒否のリモートアドレスを設定する。管理者は接続が許可されるプリンター、エッジルーター以外の端末との通信遮断手順を定め、ユーザーとともに設定状況を把握する。（遵守事項）

宅内LANに接続された貸与PC以外の、PC、タブレット、スマートフォンとのIP接続を拒否することで、宅内LANからの脅威を低減することが可能となる。宅内の貸与PC以外の端末のIPアドレスを調査する方法としては、巻末に照会したフリーソフトやスクリプトを利用するとよい。

5.1.8 貸与PCのRDP接続の禁止、デフォルトポートの変更

貸与PCのリモートデスクトップ接続の禁止設定、デフォルトポートの変更手順：

リモートデスクトップ接続によるブルートフォース攻撃や不正接続を防止するため、貸与PCのリモートデスクトップ接続を行わない設定を施す。また、接続を許可する場合は、接続可能ユーザーを貸与PCに設定するとともに、デフォルトポートである3869（TCP/UDP）を変更し、可能であれば接続が許可されるIPアドレスとともにパーソナルファイアウォールに登録する手順を管理者は定め、ユーザーと合意する。（遵守事項）

リモートデスクトップのデフォルトポートは広く知られており、ブルートフォース攻撃的となる。このデフォルトポートを通じた攻撃を防御するため、リモートデスクトップのポートをプライベートポート（49152-65535）に設定変更する。これによって、攻撃側が即座にブルートフォース攻撃を行えないようにする。可能であれば接続する端末のIPアドレスを登録するとよい。

5.1.9 貸与PCのローカルAdministratorのパスワード

貸与PCのローカルAdministratorのパスワード設定および管理

窃取されたローカルAdministratorのパスワードによる不正ログオンを防止するため、貸与PCのローカルAdministratorのパスワードは、端末ごとにすべて固有の設定とし、管理者が管理する。ローカルAdministratorのパスワードが必要な設定がある場合に備えて、管理者とユーザーの間でローカルパスワードの授受方法、保管、管理方法を定め、ユーザーと合意する。(遵守事項)

Microsoft LAPSを利用し、管理PCのローカルAdministratorパスワードをすべてユニークにする。(推奨事項)

企業PCの管理を軽減するため、ローカルAdministratorのパスワードを全社共通にする場合がある。この場合、一台でもローカルAdministratorのパスワードが漏洩すれば、全社的な情報漏洩につながる恐れがあり、大変危険である。この事象を防ぐため、マイクロソフトから個別にローカルのAdministratorをユニークにするツール (Microsoft LAPS) が無償で公開されている。必要に応じて使用するとよい。

5.2 宅内LAN、宅内端末への要求事項

宅内LANの取り扱いは以下の要求を満たさなければならない。

5.2.1 宅内LANでの探索、共有

宅内LANで宅内の他の端末やNASと探索、共有を許可しない：

貸与端末からの情報漏洩、宅内端末からのマルウェア感染などのリスクを低減するため、宅内LANに接続された他のPCやスマートフォン、NAS等と貸与端末の間でフォルダ共有を一切行わない。(遵守事項)

貸与端末以外の宅内端末は業務とは無関係であり、本来的に接続は許可されない。そのため、宅内端末やNAS等の脆弱性管理やアンチウイルスソフトによる管理の有無に関わらず、貸与端末とのファイル共有、探索を禁止し、宅内端末からのマルウェア感染、Exploitによる乗っ取り、宅内端末からの情報漏洩リスクを低減する。

設定は、コントロール パネル¥ネットワークとインターネット¥ネットワークと共有センター¥共有の詳細設定 で、[プライベート]、[ゲストまたはパブリック]、[ドメイン] のいずれも [ネットワーク探索]-[ネットワーク探索を無効にする]、[ファイルとプリンターの共有]-[ファイルとプリンターの共有を無効にする]を指定する。

ファイル共有等を監視するため、資産管理ソフトを利活用することは推奨される。

5.2.2 無線LANのプロトコル

宅内LANで無線LANを使用する際は、WPA2を使用する：

脆弱な無線LANプロトコルの使用による情報漏洩を防ぐため、無線LANの接続にはWPA2を使用し、暗号化はAESで行う。事前共有鍵はパスフレーズを使用する場合は20桁以上 (IEEE 802.11 推奨値) とするが、極力、無線LANルーターに付属する事前共有鍵の自動設定機能 (Wi-Fi Protected Setup) を使用する。管理者は無線LANルーターの事前共有鍵の自動設定の方法と、ファームウェアアップデートについて、ユーザーと情報を共有の上、合意する。パスフレーズを保管する場合は、その方法について合意する。(遵守事項)

無線LANは近隣から攻撃が可能であることから、脆弱性を有しないプロトコルを使用し、かつ、事前共有鍵長を長くすることが必要である。パスフレーズを入力する場合、ランダムで長い桁数の入力には困難なことから、自動設定機能を使用することが簡便でセキュリティ上も望ましい。

5.2.3 エッジルーターのパケットフィルタ

宅内LANのエッジルーターは、初期設定パスワードを変更し、パケットフィルタを設定する：

WAN側からの攻撃や不正侵入を防ぐため、エッジルーターの初期設定の管理者パスワードを12桁以上に変更し、次の送信元ポートのパケット廃棄設定とファームウェアアップデートについて、ユーザーとユーザーと情報を共有の上、合意する。変更したパスワードの保管方法についても合意する。（遵守事項）

WAN→LAN

TCP/UDP 23,135,137,138,139,445,2049 廃棄（拒否）

TCP 12345 廃棄（拒否）（遵守事項）

WAN側外部からの攻撃を防ぐため、エッジルーターを適切に設定することが必須である。

ポート	説明
20/TCP・UDP	ftp data
21/TCP・UDP	ftp
23/TCP・UDP	telnet
135/TCP・UDP	DCE/RPC
137/TCP・UDP	NetBIOS Name Service
138/TCP・UDP	NetBIOS Datagram Service
139/TCP・UDP	NetBIOS Session Service
445/TCP・UDP	Microsoft-DS SMB file sharing
2049/TCP・UDP	NFS

5.2.4 宅内端末のアンチウイルスソフトと脆弱性管理

貸与端末以外の宅内LANに接続する端末にはアンチウイルスソフトを設定する：

宅内端末から貸与端末へのマルウェア感染、攻撃を防ぐため、宅内LANに接続する端末にはアンチウイルスソフトを設定し、最新のパターンファイルの適用、1～2週間に一度の完全スキャンの実施、OS、アプリケーションソフトの脆弱性パッチの適用を行う。宅内端末に接続するスマートフォンについても、Androidについてはアンチウイルスソフトの適用を行い、Android、iPhoneについてはOSの更新、アプリケーションの更新を行う。

前項の実施が困難な場合は、スマートフォン、ポケットWi-Fiルーターによるテザリング接続を実施し、宅内LANには接続しない。テザリングに使用するスマートフォン、ポケットWi-Fiルーターは、必要に応じてアンチウイルスソフトの適用、OSの更新、アプリケーションの更新を行う。（遵守事項）

ユーザーは、宅内LANに接続する端末のアンチウイルスソフトの完全スキャンの実施ログ、Windowsアップデートの実施ログ（スクリーンショット）を保管し、管理者の監査に備える。（推奨事項）

取り扱う情報の重要性に応じて、ゼロディ攻撃によるマルウェア感染防止は困難との認識のもと、アンチウイルスソフトとともに、EDR（Endpoint Detection and Response）製品を導入し、不正な挙動の検出と感染時のネットワークの遮断、悪意あるプロセスの停止、管理者への通知を一元管理し、インシデントの拡大防止とインシデント対応時間の短縮を図る。（推奨事項）

マルウェアの最大の感染源は電子メールであり、宅内端末との(IP)接続をパーソナルファイアウォールでブロックしても、マルウェアの感染の危険性は残る。宅内端末についても、貸与端末と同等程度のセキュリティ維持が望まれる。なお、テザリングを使用する場合は、テザリングに使用するデバイスのセキュリティ維持も必要である。

マルウェアは亜種が多く、ある時点において、一つのアンチウイルスソフトウェアがすべての亜種に対応することは困難である。従って、完全スキャンを1-2週単位で実施し、検出に努める必要がある。

個人情報、生体情報、営業情報などの重要な機密情報を扱う場合は、マルウェア感染を前提として、EDR製品の導入も検討すべきである。

6

在宅勤務におけるセキュリティポリシー (Active Directory)

企業側で使用される（貸与端末から接続される）Active Directoryは以下の要求を満たさなければならない。



6.1ドメイン

6.1.1 ドメインで使用可能なプロトコル

ドメインコントローラー、サーバー、ワークステーションでは脆弱なプロトコルをグループポリシーで禁止設定する：

Windowsの古いプロトコルの脆弱性を利用するマルウェア等の被害を防ぐため、後方互換性に配慮しつつ、Lan Manager、NTLMv1、SMBv1を禁止する。（遵守事項）

古いプロトコルしか利用できないNAS等の調査を実施し、撤廃、リプレースを行う。（遵守事項）

NTLMの監査を実施する。（推奨事項）

マイクロソフトが使用を推奨していないプロトコルの脆弱性を利用するマルウェア、特にランサムウェアの被害が増加したことを踏まえ、Lan Manager、NTLMv1、SMBv1を禁止する。なお、古いNAS等でこれらのプロトコルが必要なものは、早急にリプレースをする。

6.1.2 ドメインアカウントポリシー

ドメインのアカウントポリシーを設定し、全社的にパスワードの最低長、アカウントロックを強制設定する：

ブルートフォース攻撃や辞書攻撃等での不正侵入、乗っ取りを防ぐため、Active Directoryのドメイングループポリシーでパスワードのポリシー、アカウントロックアウトのポリシーを設定する。パスワードの長さは12文字以上、複雑さの要件を満たす必要を有効にし、アカウントロックアウトの閾値を10回ログオンに失敗ロックアウト期間を30分に設定する。（遵守事項）

長いパスフレーズの使用を推奨する。（推奨事項）

紛失、盗難などのオフライン攻撃が考えられるため、加えて、Active Directoryでのパスワード登録の際に、辞書検定ができない（ランダム性を確保できない）ため、複雑だが短いパスワードよりも、長いパスフレーズが有効である。また、ランダムなフレーズは記憶が困難であり、利便性が悪い。そこで、両親の名を並べたり、子供のころの先生や友人などのフルネーム、学校最寄りの駅やバス停など、本人しか知らないパスフレーズを使用することを推奨する。

例：takahiro#Yamada9（16文字・複雑性）

fumie&shinichirou（16文字・複雑性なし）

Koujimachiyonchoume（19文字・複雑性なし）

<https://pages.nist.gov/800-63-3/> Authentication and Lifecycle Management

6.1.3 ビルトインアカウント

Active DirectoryのBuilt in AccountをDefault値から変更する：

マルウェアや乗っ取られた端末からの不正ログイン、ブルートフォース攻撃を防ぐため、ビルトインのAdministratorを異なるアカウント名に変更する。(遵守事項)

ルーター等のネットワーク機器、管理ツール、アプライアンス等のAdmin、Administrator等も同様に変更を行う。(推奨事項)

Active Directoryには既定のAdministratorアカウントが用意されており、このアカウントはロックアウトされないため、ブルートフォース攻撃の格好の対象となる。既定のアカウント名を変更することで直接的な攻撃を防ぐとともに、存在しないアカウントに対するログオン失敗等のログをフィルタリングなしに監査でき、攻撃の発生を検知することが容易となる。

変更にあたっては、タスクスケジューラ、バックアップ等でのAdministratorアカウントの利用状況を事前に調査し、システムに影響を及ぼさないように留意する。

[https://technet.microsoft.com/ja-jp/library/mt634171\(v=vs.85\).aspx](https://technet.microsoft.com/ja-jp/library/mt634171(v=vs.85).aspx)

<http://www.atmarkit.co.jp/fwin2k/win2kktips/1273renadm/renadm.html>

6.1.4 セキュリティグループの監査

Administrators、Enterprise Admins、Account Operator等のセキュリティグループ、Guestアカウントの監査を実施する：

高位の権限を有するセキュリティグループに対するマルウェアやエクスプロイトによるメンバー改ざん、内部の不正行為を検知するため、セキュリティグループのメンバーを定期的に監査する。加えてGuestアカウントが無効であることも監査する。(推奨事項)

AD属性のadminCountを監査し、特権を与えたことのないユーザーが特権を所有していないかを監査する。(推奨事項)

特権を有するセキュリティグループのメンバーを監査することで、想定外の特権資格者が存在しないことを確認する。また、Guestアカウントが無効となっていることを確認する。

ADDSの属性エディターでadminCountが1となっていると、過去を含め特権を有したことが記録されることから、以下のPowerShellコマンドで特権を有したユーザーの一覧を監査する。

```
Get-AdUser -filter {adminCount -eq 1} -Properties * |select SamaccountName, ObjectCategory
```

Office365などを利用している場合、Guestアカウントを利用して、外部のユーザーとのコミュニケーションを図る場合がある。不用意な情報漏洩を防ぐために、クラウドでのGuestアカウントの取り扱いとリスク、監査についても検討するとよい。

How to get all guests users in an Office 365 tenant using PowerShell Azure AD

<https://gallery.technet.microsoft.com/office/How-to-get-all-guests-4293b47c>

6.2 ドメイン端末

6.2.1 端末のネットワーク探索、ファイルとプリンターの共有

貸与端末を含むすべての端末でネットワーク探索、フォルダ共有、ファイル共有を無効にする：

共有フォルダを利用し拡散するマルウェアの脅威を防ぐため、端末のネットワーク探索、ファイルと

プリンターの共有を無効にする。ファイル共有は、アクセス権設定が施されアクセスログの残るFile Server、NASを利用する。(遵守事項)
管理者はFile Server、NASのアクセス権を監査する。(遵守事項)

端末間の安易な共有を許可すると、管理者が各端末の共有状況や権限設定を把握することが難しくなる。共有フォルダのアクセス権にEveryoneが許可された場合、マルウェアによる情報漏洩を招く恐れがある。この場合、情報漏洩の範囲を特定できない恐れもあるファイルの共有は、管理者がアクセス権の設定ができ、アクセスログが取得できるFile Server、NASを使用し、万一のインシデントの際に、情報漏洩の範囲を特定できるようにする。管理者は定期的にファイル共有、ファイルストレージの実態を調査し、アクセス権を監査する。

ファイル共有・権限をレポートする (PowerShell)

<http://www.waynezim.com/2014/03/powershell-file-sharing-permissions-report/>

PowerShell Get List Of Folders Shared

<https://superuser.com/questions/769679/powershell-get-list-of-folders-shared>

```
$Servers = ( Get-ADComputer -Filter { DNSHostName -Like '*' } | Select -Expand Name )
foreach ($Server in $Servers)
{
    (net view $Server) | % { if($_.IndexOf(' Disk ') -gt 0){ $_.Split(' ')[0] } } | o
ut-file C:\file_shares¥$Server.txt
}
```

※DNS Host Nameを取得するため、実際に接続されていないPCがあると、RemoteExceptionが発生する。



6.3 サーバー

6.3.1 サーバーのアンチウイルスはクライアントとは異なる製品を採用する

サーバーのアンチウイルスはクライアントPCとは異なるベンダーの製品を採用する：
多数のマルウェアと亜種に対応するため、ファイルサーバー、アプリケーションサーバー、DBサーバーで稼働させるアンチウイルス製品と、クライアントPCのアンチウイルス製品は、異なるベンダーとする。(推奨事項)

クライアントPCとサーバーで異なるベンダー製品を採用すれば、それだけ多くのマルウェアに対するフィルタが増え、クライアントPCで検出できなくてもファイルサーバーで検出できる可能性が高くなる。特に、外部から受け取ったPDFやOffice文書などに潜むマルウェアは亜種が多く、対応するパターンファイルの更新までの期間(デルタ)のリスクを減らす必要がある。

大容量のファイルサーバーは、アンチウイルスの完全スキャンに数日から数週間かかるケースがある。ファイルサーバーを単一のインスタンスで構築すれば、利用側からは便利だが、完全スキャンの周期が長くなることでデルタのリスクが増大する。このことから、10テラバイトを越すようなファイルサーバーは、インスタンスを分割することも検討する。

6.3.2 サーバーのRDP接続のデフォルトポート

サーバーのリモートデスクトップ接続のデフォルトポートの変更手順：
リモートデスクトップ接続によるブルートフォース攻撃や不正接続を防止するため、接続可能ユーザ

ーはネットワークレベル認証でRDPを実行しているコンピューターからの接続のみ許可し、デフォルトポートである3869 (TCP/UDP) を変更し、可能であれば接続が許可されるIPアドレスとともにパーソナルファイアウォールに登録する手順を管理者は定め、ユーザーと合意する。(遵守事項)

貸与PCと同様である。リモートデスクトップのデフォルトポートは広く知られており、ブルートフォース攻撃的となる。このデフォルトポートを通じた攻撃を防御するため、リモートデスクトップのポートをプライベートポート (49152-65535) に設定変更する。また、ネットワークレベル認証を設定し、ユーザーを登録することで、攻撃側がブルートフォース攻撃を行えないようにする。

6.3.3 AdministratorアカウントでサーバーへのRDP接続を行わない

サーバーのリモートデスクトップ接続のユーザーアカウントにAdministratorを使わない：
ソースコードの変更やコンテンツの変更、システム設定変更に対する否認を防止するため、リモートデスクトップ接続は必ず個別のユーザーアカウントを使用する。(遵守事項)

ビルトインアカウントを使用してソースコードやシステムの設定変更を行った場合、実際に誰が変更を加えたかの実証が困難になる。共有可能なアカウントは使用せず、必要に応じて、グループポリシーでAdministratorを異なるIDにしておき、最小限の管理者だけが使用するように利用規則を検討する。

7

在宅勤務におけるセキュリティポリシー (VPN・その他通信)

VPNおよびその他の通信の取り扱いは以下の要求を満たさなければならない。



7.1 VPN

7.1.1 VPNの方式検討

VPNの方式を検討し、接続手順と認証方式を定め保守する：

ユーザーと企業の通信経路をVPNによる認証・暗号化を実施し、第三者の侵入、盗聴から保護するため、VPN接続手順を定め、ユーザーに教育する。ユーザー認証方式、ユーザーの在宅勤務の有無、休職、退職時の保守方式を定め実施する。(遵守事項)

VPNには、IPSec、TLS、PPTP、SOFTEtherなどの方法があるが、接続方式および認証方式についてのリスクと通信負荷を検討した上で、接続方式とアカウントの保守を手順化することが重要である。特に退職者が発生した場合に、アカウントを削除する、PWを変更するなどの措置が必要であるため、VPN接続における共通パスワードなどは絶対に禁止する。

7.1.2 VPN装置の脆弱性

VPN装置の脆弱性を管理する：

VPN装置の脆弱性によるサービス停止攻撃や不正ログオンを防止するため、VPN装置のファームウェア、プロトコル、暗号化方式の脆弱性を管理し、必要に応じてパッチを適用したり、運用を停止する。アクセスログを適切に保存し、外部からの不法侵入の有無、ブルートフォース攻撃などの攻撃の有無を監視する。(遵守事項)

VPN装置の暗号化ライブラリはオープンソースが使用されるケースが多く、オープンソースの脆弱性に起因するVPN装置の脆弱性管理はサービス維持において極めて重要である。また、外部からのブルートフォース攻撃などの攻撃の有無を監視することは言うまでもない。

7.1.3 VPN接続時のクレデンシャル(ID、パスワード等の認証情報)

VPN接続時のクレデンシャルの保護、運用管理を行う：

VPN接続のクレデンシャルの特性に応じて適切に保護するため、有効期限における更新、変更方法、失効時やロックアウト時の手順、クレデンシャルの盗難、紛失時の手順(暗号化方式、通信手順)と、クレデンシャルの保存方法を定め、ユーザーを教育する。(遵守事項)

認証方式によってクレデンシャルの管理は異なる。①ID、パスワード、②電子証明書USBトークン、③ワンタイムパスワードハードウェアトークン、④ワンタイムパスワードソフトウェアトークン、⑤生体認証、

⑥マトリクス認証等の認証方式、それぞれに更新、変更、失効、盗難、紛失といった事象に適切に対応するための手順と、クレデンシャルの保存方法を定め、ユーザー教育を行う必要がある。

7.1.4 大規模な通信障害

インターネットやVPNの通信障害が発生した場合の手順を定める：

自然災害等による大規模なインターネットへの接続障害やVPN装置の故障などによって、長時間、VPN接続ができない場合に適切に対応するため、代替措置を定めておく。代替措置によって、暗号強度の低下やなりすましの発生が起きないように留意する。状況に応じて、在宅勤務を解除するなどを定めておく。(遵守事項)

VPN装置の故障で、一定期間VPN接続ができない際に、安易に電子メールで成果物を送受信したりすると、思わぬ情報漏洩（誤送信、PCの盗難・紛失によるメールボックスの漏洩）を招く恐れがある。業務の優先度合いと保秘の度合いを鑑み、在宅勤務を解除する条件などを定めておく必要がある。

7.1.5 VPN接続の否認

VPN接続での否認、なりすましの排除：

VPN接続での接続否認やなりすましを排除するため、共通ID/パスワードや、電子証明書のOrganizationやIssuerだけをクレデンシャルとするような認証方式の使用を禁止する。ID/パスワードの場合は、ユーザーごとに個別に発行し、電子証明書の場合は、UserPrincipalNameやEmailなどのユニークな項目で認証を実施する。(遵守事項)

電子証明書でのVPN接続では共通ID/PWや電子証明書でのOrganizationやIssuerで認証を許可する例が多いが、これでは、VPN接続を行っていないという否認に対抗できず、情報漏洩、改ざんなどが発生した場合の追及が困難になる。

クレデンシャルは接続ユーザーごとに必ずユニークにする必要がある。

7.1.6 RADIUS Server

VPN装置アカウント管理とADのアカウント管理を連動する：

管理ミスによって発生する、認証してはならないユーザーの認証を防ぐため、VPN装置のRADIUS ServerはActive Directory Network Policy Serverとするか、VPN装置からActive Directory ServerとLDAP連携させる。(遵守事項)

これらの設定によって、VPN接続できるユーザーとActive Directoryのユーザーが一元化され、退職や権限失効の際に、ADのユーザーを無効すれば、VPN接続も不可能となるような運用が可能となる。管理漏れという人為的なミスを最小化することは極めて重要である。



7.2 その他通信

7.2.1 Firewall、Proxy

ブラックリストを適用する：

インターネット上の有害なサイト、IPとの通信を遮断するため、IP、URLのブラックリストをFirewall、

Proxy Serverに登録する。(推奨事項)

ランサムウェア等のマルウェアが利用するIPやフィッシングサイトは、ブラックリスト化されており、FirewallやProxy Serverに登録することで、電子メールのリンクや添付ファイルに隠されたマルウェアの通信を遮断し、被害を防ぐことが可能となる。ただし、ブラックリストの保守には多大な労力がかかることから、自動化を前提に検討する。

Cisco TALOS

<https://www.talosintelligence.com/>

7.2.2 Video会議

プライベート空間の映り込みを防ぐ：

自宅からビデオ会議に参加する際は、プライベート空間の映り込みによるプライバシーの暴露を防ぐため、カメラの位置に配慮する等、管理者は手順書でユーザーに注意喚起する。(遵守事項)

在宅勤務におけるビデオ会議は非常に有力なツールとなりえる反面、自宅内の様子が会議参加者に暴露される場合がある。意図せぬプライバシー暴露を防止するため、ユーザーには、プレビューでカメラの位置を調整するなどの設定喚起を行う。

8

在宅勤務におけるセキュリティポリシー (ログ)

サーバー、端末、通信装置のログ取り扱いは以下の要求を満たさなければならない。



8.1 通信装置

8.1.1 VPN装置、ルーターのログ

VPN装置のログを保全する：

外部攻撃やインシデントの原因究明に備えて、アクセスログ、設定ログは上書き禁止とし、Syslogサーバー等に適切に保存する。適切な容量を超えた場合は、自動的にバックアップし、最低1年以上のログを保存できる体制を整備する。設定ログは定期的に監査し、外部からの改ざんがないことを確認する。
(遵守事項)

ATP攻撃では、攻撃開始から発見に至るまで、数か月かかるケースが散見されるため、VPN装置のログは最低1年保管するべきである。ルーター等の通信装置のAdministratorアカウントは、広く知られているケースがある。IDが既知のためブルートフォース攻撃には脆弱な体制であることを前提に、予期せぬConfig設定変更がないことを監査するべきである。



8.2 Windows

8.2.1 Windows Serverのログ

Windows Serverのログを保全する：

外部攻撃やインシデントの原因究明に備えて、システムログ、セキュリティログ、アプリケーションログ、アンチウイルスソフトのログは上書き禁止とし、自動的にアーカイブするように設定する。各ログは分析の取り扱いを考慮し、50MByte~100MByte程度の容量に達した時点でアーカイブするように設定する。このほか、役割・機能に応じてIIS、NTLM、DHCP、DNS Server等のログを含め1年以上保存する。
(遵守事項)

インシデント発生時のドメインコントローラーでは、数時間でセキュリティログが100MByteを越すケースも散見されることから、既定値（Windows 2008, 2012, 2016の主要ログで20MByte、上書き）では全く不十分である。また、NTLMなどはグループポリシーで監査を設定しないと記録されないため、機能、役割に応じて設定することが重要である。また、DHCPは1週間単位で上書きされるため、タスクスケジューラでバックアップするバッチ処理を実行する必要がある。

なお、いずれも規定値ではCドライブに保存されるため、起動ドライブの容量を圧迫しないように十分に配慮する必要がある。

8.2.2 Windowsクライアント(貸与端末を含む端末)のログ

Windowsクライアント(端末)のログを保全する：

外部攻撃やインシデントの原因究明に備えて、システムログ、セキュリティログ、アプリケーションログ、アンチウイルスソフトのログは上書き禁止とし、自動的にアーカイブするように設定する。各ログは分析の取り扱いを考慮し、50MByte~100MByte程度の容量に達した時点でアーカイブするように設定する。起動ドライブを圧迫しないよう、定期的に圧縮するなどの措置を講じる。(遵守事項)

クライアントの場合、ディスクに余裕がない場合があることから、定期的にアーカイブされたログを圧縮しディスクスペースの確保に努める措置が必要である。



8.3 ログの統合分析

8.3.1 ログの統合的分析・管理

各種ログを統合的に分析・管理・長期保存できるシステムの整備：

広範な外部攻撃やインシデントの原因究明に備えて、端末からサーバー、通信装置を含むログの統合分析や長期保存、バックアップなどの管理システムを整備する。(推奨事項)

発生事象を時系列で分析できなとインシデント発生時に原因の究明や適切な防御措置が遅れ、被害を拡大する場合あり、インシデント対応コストの増大を招く。分析能力を有していなくても、ログが特定のサーバーで集中管理されるだけでも、初期対応には十分に有効となることに留意されたい。

9

在宅勤務におけるセキュリティポリシー

(規程)

在宅勤務に関わる規程は、以下の要件を満たさなければならない。すべての規程は実効性を担保するため従業員への詳しい説明及び違反の際の懲罰規程を設けることが望ましい。

9.1 データの暗号化

個人情報や企業情報が含まれるデータファイルには、必ずパスワードを設定し、暗号化する規程を設ける。電子メールの添付ファイルとして暗号化データを送信する場合、復号用のパスワードを電子メール(平文)で送信しないように規程するのが望ましい。

規程例：

第〇条（データの暗号化）

1. 個人情報や営業情報が含まれるデータファイルは、会社規程の暗号化方式で暗号化し、復号のためのパスワードを設定しなければならない。パスワードは12桁以上のパスフレーズとし、パスワードの受け渡しに電子メールを利用してはならない。
2. データファイルとパスワードを収めた電子ファイルは必ず格納する媒体単位で分離して保管し、同一の記録媒体、サーバー、端末に保管してはならない。

第〇条（暗号化方式）

1. 当社の暗号化方式は以下のとおりとする。

データ暗号：	AESブロック長128ビット、鍵長256bit
メッセージダイジェスト：	SHA-256
セキュリティ通信：	TLS1.2
2. 但し、顧客都合、システム都合で当社規程を充足できない場合は、想定されるリスクと対策を文書でシステム管理部門に申請し、個別に許可を受けることで使用できる。

9.2 クレデンシャルの保全

ID、パスワードなどのユーザー認証に使用されるクレデンシャル（認証情報）は電子メール以外の相手が特定できる経路で通知、連絡しなければならない。

規程例：

第〇条（クレデンシャルの連絡方法）

1. ユーザー認証に使用されるクレデンシャルは、社内、社外を問わず電子メール、USBメモリを使って相手方に受け渡しをしてはならない。
2. 紙媒体を使用する場合は、必ず、鍵のかかるロッカー等に保管しなければならない。
3. 相手方への受け渡し方法として以下の方法を推奨する。
 - A) 紙媒体の場合は、簡易書留で送付する事とし、電話、電子メール等で事前に相手方に通知を行っておく。この場合、クレデンシャル一式（IDとPWなどの認証情報）を送付してもよい。
 - B) 電話の場合は、当方から相手方に電話をかけたうえで本人であることを確認する。この場合、クレデンシャル一式を口頭で伝達してもよい。

- C) FAXの場合は、受け取り相手が受信用紙を直接受け取れる状態を確認した上で送信する。誤送信に備え、クレデンシャル一式を送付してはならない。必ず、パスワードは単独で送信する。
 - D) 携帯電話のショートメッセージの場合は、事前に相手方に送付通知を行っておく。誤送信に備え、クレデンシャル一式を送付してはならない。必ず、パスワードは単独で送信する。
 - E) クラウドストレージの場合は、クラウドストレージへのログオンのためのクレデンシャルを前項AからDの方法で受け渡した場合に限り、当該クレデンシャル一式を送付してもよい。但し、相手方がクレデンシャル一式を受領した後、速やかに削除しなければならない。
4. 前項CおよびDで誤送信が判明した場合は、該当するシステムから誤送信したクレデンシャルをすべて破棄し、当社管理者に届けなければならない。

9.3 在宅勤務で使用される貸与端末の管理

9.3.1 貸与端末の管理規程をユーザーに理解させ、遵守することを合意する

規程例：

第〇条（貸与端末の管理規程の合意と遵守）

1. 当社は貸与端末の管理規程を、規程施行並びに改定の都度、貸与端末を使用する従業員に詳しく説明しなければならない。
2. 前項を満たした場合、当社は必要に応じて、従業員から管理規程を遵守する旨の誓約書の提出を求めることができる。
3. 従業員は規程に関する疑義があれば、当社担当者に質問するなどして疑義の解消に努め、管理規程の意図と内容を十分に理解した上で、管理規程を遵守しなければならない。

9.3.2 貸与端末の個人利用の禁止

規程例：

第〇条（貸与端末の個人利用、第三者利用の禁止）

1. 従業員は貸与端末を業務目的外の個人利用をしてはならない。
2. 貸与端末には、業務目的外のソフトウェアのインストールやデータの複写をしてはならず、業務目的以外のWebサイト・サービスへの接続や電子メール、チャット等の通信、電子媒体や電子機器の有線・無線での接続によるデータの複写、動画・音楽の再生、印刷などをしてはならない。
3. 従業員は貸与端末を業務目的以外で、第三者に貸与端末もしくは端末の資源の一部および全部使用させてはならない。これには、第三者との画面共有や電子媒体の共有、プログラムの実行やデータ共有等が含まれる。

9.3.3 貸与端末の無許可ソフトウェア、クラウドサービスの使用禁止

規程例：

第〇条（貸与端末の無許可ソフトウェア、クラウドサービスの使用禁止）

1. 従業員は貸与端末に、当社が許可していないソフトウェア（これにはアプリケーションソフト、オープンソース、フリーソフト、公開されているソースコードやライブラリ、ドライバーソフトウェア等が含まれる）をインストールし、もしくは複写し、ソフトウェアの実行やコンパイル、リンク、ビルドなどを行ってはならない。
2. 従業員は貸与端末で、当社が許可していないクラウドサービス（これには、ストレージサービス、ファイル転送サービス、電子メール、P2Pサービス、SNS、Webアプリケーション、データ変換、Webサービス等が含まれる）を使用してはならない。

9.3.4 USBメモリの運用

規程例：

第〇条（USBメモリの使用禁止、使用条件）

1. 従業員は貸与端末に、当社の許可なくUSBメモリを接続してはならない。
2. 当社が業務目的でUSBメモリの使用を許可した場合でも、USBメモリに業務データを保存することは必要最小限にとどめ、永続的に業務データを保管してはならない。業務使用が終了時点で、業務データをすべて削除しなければならない。
3. USBメモリに業務データを保存する場合は、必ず当社規程の暗号化を施さなければならない。暗号化されたデータの復号のためのパスワードは、同じUSBメモリに保存してはならない。
4. 当社がUSBメモリの使用を許可した場合でも、当社外の第三者（これには当社顧客や従業員の家族も含まれる）の端末にUSBメモリを接続したり、第三者に貸与してはならない。
5. 接続が許可されたUSBメモリは貸与端末での使用の前後に、最新の状態のアンチウイルスソフトで完全スキャンを実施しなければならない。
6. 前項のUSBメモリの使用の際に、異常があった場合は、即座に使用を停止するとともに、アンチウイルスソフトのログとともに異常の詳しい状況を可及的かつ速やかに管理者に通知し、対応の指示を仰がなければならない。
7. USBメモリを紛失もしくは盗難にあった際は、USBメモリのデータ内容や紛失、盗難の詳しい状況を可及的かつ速やかに管理者に通知し、対応の指示を仰がなければならない。
8. USBメモリを保管する際は、鍵のかかるロッカー等に保管し、安易に第三者（これには当社顧客や従業員の家族も含まれる）が操作可能な状態で放置してはならない。

10

在宅勤務におけるセキュリティポリシー

(教育)

在宅勤務に関わる従業員への教育は、以下の要件を満たさなければならない。最新のセキュリティ動向に合わせ順次内容はレベルアップすることが望ましい。なお、教育コンテンツは、セキュリティ関連のニュースサイトやセキュリティベンダーのブログ、IPAのWebページなどを活用することを推奨する。

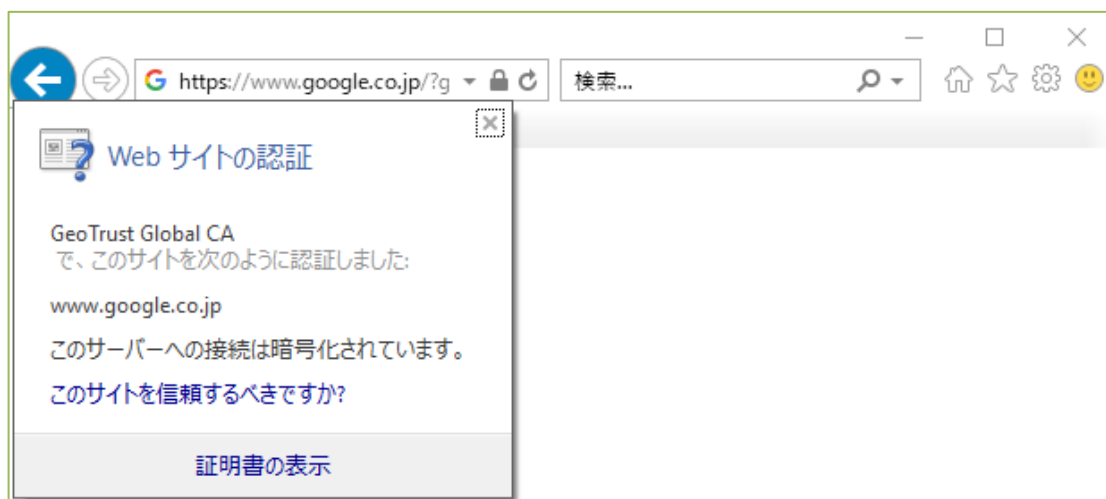
10.1 ブラウザがTLSの状態であることを理解させる。

使用するブラウザごとに、TLS接続状態のアイコンや、証明書情報の取得方法を理解させる。

10.1.1 Internet Explorer 11 でTLS (HTTPS) 接続した状態 が表示される



10.1.2 Internet Explorer 11 で アイコンをクリックした際の認証情報の表示



10.1.3 Internet Explorer 11 で非TLS(HTTP)接続した状態 が表示されない



10.1.4 TLS(HTTPS)通信とは

TLSとはTransport Layer Security (トランスポート・レイヤー・セキュリティ) の略称で、インターネットやLAN上でセキュリティ通信を行うためのプロトコル (通信手順) です。古くはSSL (セキュア・ソケット・レイヤー) と呼ばれており、SSL1.0→SSL2.0→SSL3.0→TLS1.0→TLS1.1→TLS1.2とバージョンアップを重ね改良されてきました。SSL2.0やSSL3.0は仕様に脆弱性があるため、現在は使用が禁止されており、誤解を避けるために、SSLとは言わずTLSという呼び方が定着しています。また、TLS1.0も脆弱性を利用した攻撃が発生しており、セキュリティ面で改良されているTLS1.2の使用が推奨されています。

TLSの主な機能としては、①接続先のサーバーが成りすましてないことを証明する、②通信内容を暗号化する、③経路上での通信内容の改ざんを防ぐ、などがあげられ、オンラインバンキングやEコマースでのIDやパスワードの保護、決済情報や個人情報の保護などで幅広く使用されています。Windowsでもログオン情報をActive Directoryサーバーに送信する場合は、TLSが利用されており、あらゆるITシステムの情報保護の基盤技術として活用されています。

このTLSはサーバー側に第三者の認証局が発行した電子証明書を組み込むことで、安全性を担保しています。認証局は会社の登記簿や担当者の実在等を確認して「実際に存在する会社や組織」に証明書を発行するため、ブラウザで証明書情報が確認できれば、そのサーバーは実在の企業や団体のものであることがわかります。一方、自分で発行した証明書や偽物の証明書、有効期限が切れてしまった証明書は、企業や組織のなりすましが考えられます。このような第三者の認証局が発行した有効な証明書が確認できない場合、ブラウザから下図のような警告が表示がされるため、接続を避けなければなりません。



また、非TLS (HTTP) 通信では、情報はすべて暗号化されていない平文ですので、その状態で、IDやパスワードなどの認証情報や、個人情報、顧客情報、クレジットカード情報などを送信するのは、極めて危険です。また、マルウェアを送り込むフィッシングサイトの可能性も考えられます。

10.2.1 2018年のセキュリティ脅威の動向

トレンドマイクロによれば、2018年の脅威の動向として以下があげられています。

- ① 2017年に猛威を振るったランサムウェアが高度化、工場などの生産ラインや産業用IoT機器を攻撃し、より高額な利益を得ようとする「ネット恐喝」が出現する可能性。
- ② WebカメラやIoTデバイスの乗っ取りが進化し、スマートスピーカーやスマートホーム関連機器の狙った家宅侵入、ウェアラブル端末や医療機器へのバイオハッキングといった新たなサイバー攻撃が増加する。
- ③ 約50億ドルもの被害を及ぼしたビジネスメール詐欺が増加しさらに加速、90億ドルに達する。

ランサムウェアは攻撃対象を個人から企業にし、高額な身代金を要求する方向にあります。実際に、2017年のWannaCryではホンダの生産ラインが感染しました。一般に、生産ラインや産業機器は閉域網での運用がなされていますが、この閉域網にもインターネットゲートウェイが存在したり、USBメモリ等の外部ストレージが接続を許可するケースは多数存在します。マルウェアが巧妙化する現在においては、生産ライン等の閉域網の運用を見直すことが防御の重要なポイントになります。

WebカメラやIoTデバイスの乗っ取りは、初期ID、初期パスワードを変更せずにDefault設定のまま利用するケースが問題として指摘されています。攻撃側としては、総当たり攻撃などで一つ一つ攻略するよりも、手っ取り早く乗っ取れるデバイスを探す方が時間もコストも節約でき、また逆探知などのリスクから解放されます。スマートデバイスやIoT機器、産業機器もPC同様にパスワードをしっかりと設定し、ファームウェアやソフトウェアのバージョンアップを心掛ける必要があります。

ビジネスメール詐欺では、実際に、2017年9月に発生した日本航空のビジネスメール詐欺では、実に325万ドルもの被害が発生しましたが、その際の詐欺メールは極めて巧妙な手口（ソーシャルエンジニアリング）を使っています。2017年の「サイバーセキュリティに関する総務大臣奨励賞」の初の受賞者であるpiyokango氏の分析では、以下の特徴を有していました。²

- ① 画面上は取引先の名前とメールアドレスが表示され、取引先のメールアドレスとは1文字違い
- ② 直前に送付された正規の請求書の「訂正版」(PDF)を装っていた
- ③ 振込先は別の口座に変更
- ④ 送信者が取引先の担当者名であり、実物と酷使しておりサインもされていた

欧州でも数十億円単位の詐欺が発生しており、いずれも似通ったドメイン名を使ったり、メールアカウントを乗っ取るなどして送金を要求しています。これらに共通するのは、「高位の役職者」や「取引先」を騙り、「緊急の案件」や「期日が迫っており業務に支障が出る」といった心理的圧迫を行うソーシャルエンジニアリングによるものです。従って、通常とは異なる手段や方式で送金や営業情報を求められたときは、必ず、電話、FAX、ショートメールなどの異なる経路を用いて、即座に確認を取ることが重要です。

² <http://d.hatena.ne.jp/Kango/20171220/1513795615>

10.2.2 フィッシングメールの例と対策

Apple を騙ったフィッシングメール



上記の Apple 社を騙ったフィッシングメールでは、赤い線で囲った「AppleID」のリンクが Apple 社のサイトではなく、[http://warning-appleid-apple\[.\]com](http://warning-appleid-apple[.]com) となっています。この URL を疑わしいファイルや URL を分析するサービスを提供している [virustotal](https://www.virustotal.com/)³ で検索すると 67 のアンチウイルスベンダーのうち、2 社が悪意のあるサイト (Malicious site)、1 社がフィッシングサイトであるとの情報が提供されました。この URL は最後の部分が `-apple.com` となっており、下部の黒線で囲った部分は Apple 社の正規の URL のリンクとなっていて、巧妙に Apple 社のサイトであるように見せかけています。また、タイトルが「あなたの Apple ID のセキュリティ質問を再設定してください。」となっており、筆者にとっては遠隔地である静岡から iCloud にアクセスした、という内容であり、いかにも不正アクセスが行われたような内容となっています。攻撃側はこうした不安をあおったり、緊急性の高い問題のように見せかけて、不正サイトにつながるリンクをクリックさせるような工夫をしています。

³ <https://www.virustotal.com/ja/>

一方で、パスワードを変更するようなサイトは暗号化のために TLS 通信を行うので、http://ではなく https:// で始まるべきです。また、Apple 社に登録したメールアドレスとは異なるメールアドレスに（偽の）警告メールが届いたのも不自然です。

多くのフィッシングメールは、こうし不自然な特徴を持っています。

- ✓ 「緊急」「至急確認してください」といった不安を煽る文面
- ✓ 不自然な言い回し、「てにをは」の使い方がおかしい
- ✓ ID、Password、口座番号、暗証番号の入力を要求するのに、URL が https:// で始まらない
- ✓ 電子証明書に実際の企業名が入っていない

10.2.3 マルウェア添付メールの例と対策

発注書に見せかけてマルウェアが含まれているExcelを添付したフィッシングメール



上記は発注書に見せかけ、マルウェアを潜ませた Excel を添付してきた例です。あて先と CC には、実在する社員のメールアドレスが入っており、添付の Excel のファイル名は、日付と実際にメールが届いた本人のメールアドレスが入っています。

このメールはいくつか不自然な点があります。まず、メール本文にメールの送り先の名前がなく、また、発信者の名前も入っていません。日本のビジネスメールとしては体裁がおかしいといえます。また、送信者のメールアドレスは個人アカウントのもので、企業ドメインから発信されたものではありません。

一方で、発信者に覚えがある、似たような名前の人を知っている、という状況であれば、発注書という言葉につられて Excel を開いてしまうかもしれません。

筆者の使用しているアンチウイルスベンダーで添付ファイルをスキャンしたところ「安全なファイルです」との判定を受けましたが、virstotal でスキャンした結果、57 社中 6 社のアンチウイルスベンダーが「トロイの木馬」と判定していました。

フィッシングメールは、アンチウイルスソフトからの検知を逃れるために、短時間に次から次へとドメイン名を変更するため、最新のパターンファイルに更新したアンチウイルスソフトが動作していても被害にあう可能性があります。前ページの Apple 社の例でも分かるように、67 社中 64 社は安全なサイトと判断をしていました⁴。また、マルウェアも、多数の亜種が存在しており、すべての亜種をアンチウイルスが把握している訳ではありません。つまり、アンチウイルスソフトだけでは防げないケースがあるということを確認した上で、以下の対策を必ず行いましょう。

- ✓ 銀行やクレジットカード会社、その他 ID、Password を登録したサイトの正規の URL を確認し、実際に正規のサイトにログインしてサイトの証明書を確認する
- ✓ フィッシング対策協議会⁵、日本サイバー犯罪対策センター⁶で最新のフィッシングに関する具体的な情報を知る
- ✓ 不安を煽る文面のメールが届いた場合は、絶対にリンクをクリックせず、リンクにマウスオーバーして URL が正規であるかを確認する
- ✓ 通常とは異なる体裁や不自然と感じたときは、リンクや添付ファイルを開かず、電話などの異なる手段で確認をとる
- ✓ 送信元が確認できないメールは添付ファイルを決して開かない

⁴ 2月19日時点では virustotal での検索では 67 社中 7 社が有害との判定でした。

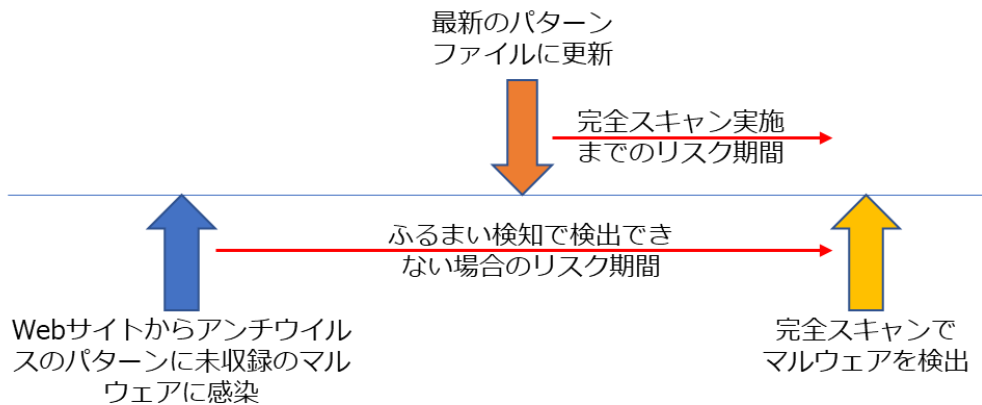
⁵ <https://www.antiphishing.jp/>

⁶ <https://www.jc3.or.jp/topics/virusmail.html>

10.3 アンチウイルスソフトのパターンファイルの操作方を理解させる

10.3.1 アンチウイルスソフトのパターンファイルの重要性

アンチウイルスソフトがインストールされていても、ウイルスパターンファイルが更新されていないと、最新のマルウェアに対応できない可能性が高まります。万一、パターンファイルに登録されていない新たなマルウェアに感染しても、感染を検出できず、パターンファイルが更新した後に完全スキャンを実行しなければ感染を知ることができない可能性が高まります。完全スキャンが実施されるまでの期間に、キーロガーやリモート操作によって情報が漏洩する可能性も否定できません。



こうしたリスクを減らすためには、完全スキャンをこまめに実施することとともに、最新のパターンファイルを手に入れることが重要です。

また、多くのアンチウイルスソフトはパターンファイルだけでなくマルウェアの特有の動作やふるまいを監視し、マルウェア検知する機能を有していますが、パターンファイルによるマルウェア検知ができれば、より多重的にマルウェア対策を行うことができます。

加えて、在宅勤務での宅内ネットワークは、企業ネットワークに設置されている Proxy Server を経由しない等、インターネット接続の方式が異なる場合もあり、ネットワーク設定の違いによって、アンチウイルスのパターンファイルの更新が意図せずに遅れることもあります。こうしたミスが減らすためにも、パターンファイルが最新であることを常に意識することは、IT 業界に従事する私たちにとって重要なことといえます。

10.3.2 パターンファイルのアップデートの確認方法(トレンドマイクロ)

本項では、トレンドマイクロのウイルスバスターコーポレートエディションを例にパターンファイルの更新方法を説明します。

Corp. サーバをアップデートする

Web コンソールにログインします。

上側メニューより [アップデート] > [サーバ] > [手動アップデート] をクリックします。

全ての項目にチェックが含まれている事を確認し、[アップデート]を選択します。

★ ダッシュボード 診断 ▾ クライアント ▾ ログ ▾ **アップデート ▾** 管理 ▾ プラグイン

手動サーバアップデート

アップデートするコンポーネント

<input checked="" type="checkbox"/>	エンドポイントコンポーネント
<input checked="" type="checkbox"/>	ウイルス対策
<input checked="" type="checkbox"/>	ファイウェア対策

概要
サーバ ▶ 予約アップデート
クライアント ▶ **手動アップデート**
ロールバック ▶ アップデート元

アップデート進捗を確認するため、完了するまで、別のページに移動せずそのままお待ちください。

ステータス

コンポーネント	進行状況	ステータス
ウイルス対策		
スマートスキャンエージェント/パターン	■■■■■■■■■■	100% 使用可能なアップデートなし
ウイルスパターンファイル	■■■■■■■■■■	100% 成功
IntelliTrap/パターンファイル	■■■■■■■■■■	100% 使用可能なアップデートなし
IntelliTrap除外/パターンファイル	■■■■■■■■■■	100% 使用可能なアップデートなし
ウイルス検索エンジン(32ビット)	■■■■■■■■■■	100% 使用可能なアップデートなし
ウイルス検索エンジン(64ビット)	■■■■■■■■■■	100% 使用可能なアップデートなし
メモリ検査/パターンファイル	■■■■■■■■■■	100% 使用可能なアップデートなし
ファイウェア対策		

完了のメッセージが表示されたらウイルスバスター Corp. サーバのアップデートは終了です。ステータスに「使用可能なアップデートなし」と表示された場合は、すでに最新の状態です。ウイルスバスター Corp. サーバのウイルスパターンファイル番号を確認します。[アップデート] > [概要] を選択します。

★ ダッシュボード 診断 ▾ クライアント ▾ ログ ▾ **アップデート ▾** 管理 ▾

アップデートの概要

予約サーバアップデート: **有効** 次回のサーバアップデート開始日時: 2014/12/8

通知ステータス

概要
サーバ ▶
クライアント ▶
ロールバック

以下の例では「11.209.80」となっています。

ウイルスパターンファイル

現在のバージョン: 11.209.80
前回のアップデート: 2014/12/8

10.3.3 パターンファイルのアップデートの確認方法(シマンテック)

本項では、シマンテックのSEP Cloudを例にパターンファイルの更新方法を説明します。

SEP Cloudをアップデートする

SEP Cloudは自動的にパターンファイルのアップデートが実施されますので、インターネットに接続できる環境であれば常に最新のパターンファイルが適用されています。

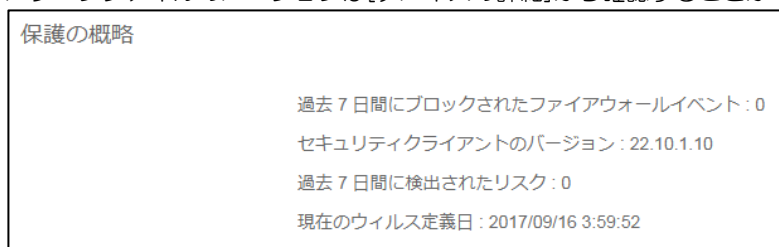
また、インターネット上に配備されている管理サーバーより、パターンファイルのアップデートを明示的に指示することも、パターンファイルのバージョンを確認することもできます。

管理コンソールでPCを選択します。

[製品のLiveUpdate] をクリックするとパターンファイルのアップデートができます。



パターンファイルのバージョンは[デバイスの詳細]から確認することができます。



さらに、一般向けセキュリティソフトの『ノートン セキュリティ』を利用した場合のパターンファイルの更新方法をご説明します。

ノートンをアップデートする

ノートンは自動的にパターンファイルのアップデートが実施されますので、インターネットに接続できる環境であれば常に最新のパターンファイルが適用されています。

なお、クライアント端末にて、①のセキュリティをクリック、②のライブアップデートをクリックすることで、パターンファイルの更新を手動で行うこともできます。



10.4.1 インターネットでの電子メール

一般に、電子メールはすべての情報（本文やメールサーバーへの認証情報など）を平文で送受信しています。したがって、インターネットの接続点で流れているパケットを盗聴すれば、電子メールの内容はすべて判明してしまいます。

電子メールの認証情報が漏洩すると、メールのなりすましが成立するため、多くのプロバイダーやメールサービスでは、クライアントの端末から発信元の電子メールサーバーまでの間を、SMTP over SSLやSMTP over TLSで暗号化し送信しますが、発信元の電子メールサーバーから、相手までは、やはり平文で送信されてしまいます。

電子メールでパスワード付きの添付ファイルを送信する際に、「パスワードは別途、メールでご案内します。」とし、実際に別便でパスワードを送信するケースを見かけますが、送信元サーバーからさきはすべて平文ですので、パスワード付きの添付ファイルも、別便で送ったパスワードは第三者が入手可能です。したがって、悪意を持った攻撃側にすればこれらの暗号化はまったく無意味で、解読が可能な状態といえます。

10.4.2 添付ファイルのパスワードの設定方法

もし、電子メールに暗号化ファイルを添付する場合は、事前に電話やSMSなどを使って相手方とパスワードを取り決めておき、パスワードを電子メールではやり取りしないことが必要です。パスワードは、毎回固定とせず、例えば相手方の携帯電話番号に本日の日付（20180201）を追加するなどすれば、毎回、携帯番号11桁+8桁という強力なパスワードを付与することができます。

これに加えて、定期的にルールを変更し、相手方の会社の住所や代表電話番号にプラスアルファすれば、互いに便利で、かつ安全です。但し、こうしたパスワードのルールは電子メールで交換せず、口頭や電話などの異なる経路を使用することが必要です。

11

在宅勤務セキュリティチェックリスト

別表の在宅勤務チェックリストは、在宅勤務におけるセキュリティポリシーを表形式にまとめたもので、「セキュリティポリシーの内容」と「当社の評価」という構成になっています。ポリシーごとに自社で実施すべきかを評価し、実施すべきかを判定できます。

11.1 セキュリティポリシーの内容

ポリシーごとに、対策の概要、詳細、脅威シナリオ、脅威分類が簡潔に示されています。対策詳細や脅威シナリオ、脅威分類については、各社の状況に応じて追加・変更を検討してください。

11.2 当社の評価(グレーの網掛け部分)

ポリシーに対して、在宅勤務で取り扱う情報資産（データや認証情報等）と起こりうる脅威に対する評価を書き込むようになっています。

11.2.1 在宅勤務で取り扱う情報資産の種類

守るべき情報資産が明確にすることで、対策が必要なのか、不要なのか、どのような運用が必要になるかの判断が可能になります。そのため、本項目では在宅勤務で取り扱う情報資産（データやシステム）の保秘レベルを記述します。

例えば、個人情報を取り扱うシステムのコーディングを在宅で行う場合、個人情報の暗号化方式や取り出す手順、DBの認証情報などは極秘情報に該当します。一方で、外部にも公開している自社のホームページのメンテナンスを行う場合は、コンテンツマネジメントシステムへのログオン情報は極秘ですが、データ自身は公開情報になります。そこで、在宅でアクセスするシステムを①ハードウェア、②OS、③ネットワーク、④システム本体（プログラム、ミドルウェア）、⑤開発環境、⑥データ（コンテンツ、マスター）に分解し、認証情報や個人情報などの守るべき情報資産を棚卸します。そのうえで、極秘、関係社外秘（パートナーや顧客を含む）、社外秘、公開可能といった保秘レベルと、情報資産の暗号化の要否を具体的に記述します。

11.2.2 起こりえるリスクと事業継続への影響度合い

ポリシーに対する現状と、起こりえるリスクを機密性、完全性、可用性、否認防止・責任追跡性の観点から評価します。サンプルを通して、評価方法を説明します。

セキュリティポリシーの内容は、Active Directoryの古いプロトコルを禁止するというものです。2017年に大きな被害をもたらしたWannacryは、SMBv1の脆弱性を狙いシステムに侵入してユーザーデータを暗号化するというものでした。脅威シナリオには、このような実際の脅威を前提に、情報漏洩や改ざん、運用障害が指摘されています。

■ セキュリティポリシーの内容

No	分類	対策項目	対策詳細	脅威シナリオ	脅威分類 <事象/結果>
1	Active Directory	Windows で動作する古いプロトコルを禁止する。	後方互換性に配慮しつつ、Windows で動作する古いプロトコル、Lan Manager、NTLMv1、SMBv1 を禁止する。	古く脆弱性を有するプロトコルを禁止しないと、WannaCry などのプロトコルの脆弱性を狙うマルウェアによって、リモート操作、情報漏洩、改ざん、運用障害を招く。	情報漏洩、情報改ざん、運用障害

このポリシーに対して、自社の分析を記入するのが「当社の評価」の部分です。分析例では、SMB1.0 に対応している NAS を開発部門が使用しており、それぞれ機密性、完全性、可用性、否認防止・責任追跡性の観点から、情報漏洩や改ざんの可能性と、それによって「損害賠償が発生する」と具体的に記述されています。損害賠償以外にも信用低下や失注の発生、パッケージの売り上げ減少といった内容をより詳細に記述し、算定できれば金額も評価に記述するとよいでしょう。そして、対策項目の実施判定で自社でのポリシー適用を決定します。

セキュリティポリシーには、企業の規模や営業形態によっては過剰な部分もあり、損害が軽微と見込まれる場合には、優先順位を下げる、もしくは適用しないという判断も、当然、あり得ます。そのため、3 段階で評価を行い、事業へ影響を及ぼすポリシーから実施計画を立てるべきです。

■ 当社の評価

当社で起こりえるリスクと事業継続への影響度合いを具体的に検討し、 3 段階（極めて重大・重大・軽微）で評価する					対策項目の実施判定 実施済み・する・不要 (するとした場合は、実施 期限)
現状	機密性 情報の漏洩	完全性 情報の改ざん・消去	可用性 業務・事業の停止	否認防止・責任追跡性 情報の改ざん・消去を 誰が行ったか証明で きない	
SMB1.0 の NAS を開発部門が使用中。	重大。第三者に顧客向けシステムのソースコードが漏洩する可能性がある。この場合、損害賠償が発生する。	重大。顧客向けシステムのソースコードが改ざんされた場合、保守が困難になる。この場合、検証や復旧の費用と損害賠償が発生する。	極めて重大。万一、ランサムウェアに暗号化された場合、開発が停止になり、復旧には数か月程度かかる。納期遅れによる損害賠償が発生する。	同左	NAS のリプレースを 3 月までに実施し、その後、ポリシーを適用する。

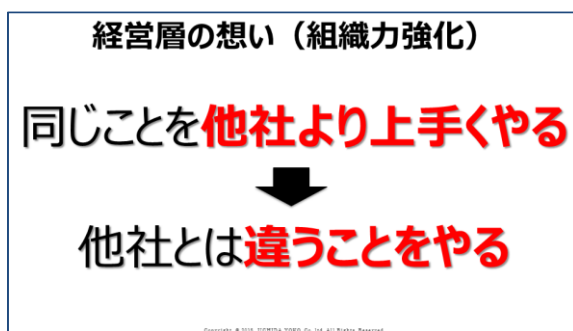
加えて、ツールやアプライアンスの導入、運用方式の変更などが発生する場合は、従業員への告知と教育も加味し、対策をしなかった場合の損害額と、対策におけるコスト総額が対比できれば、よりバランスのとれたセキュリティ投資が実現できます。

12 事例紹介

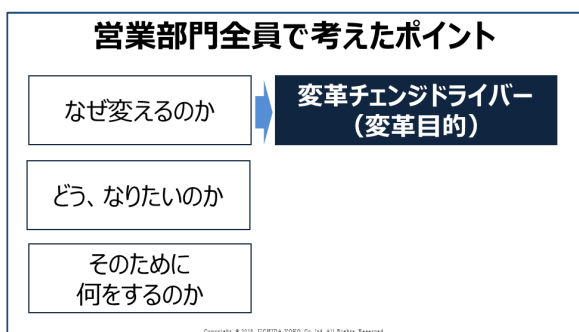
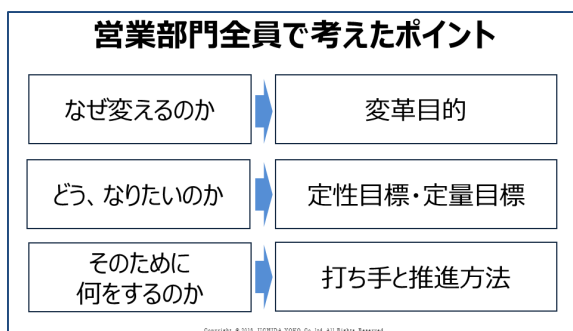
研究会内で発表いただいた企業事例の紹介です。

事例紹介1 株式会社内田洋行

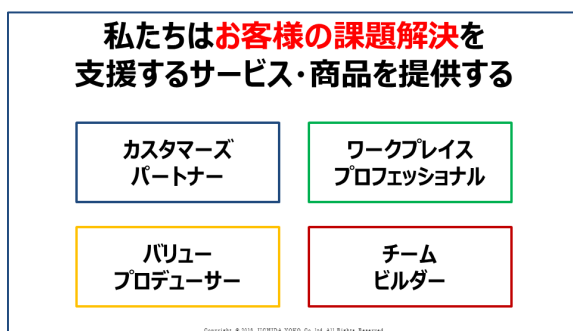
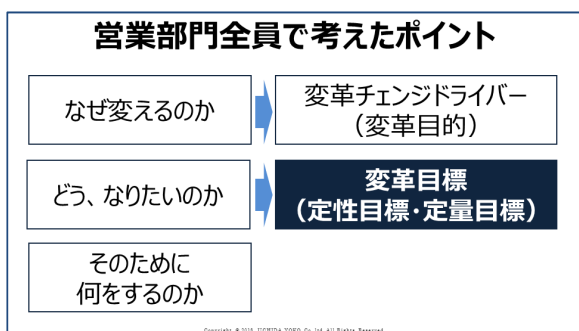
「生産性20%アップさせた営業部門の働き方変革自社実践事例」

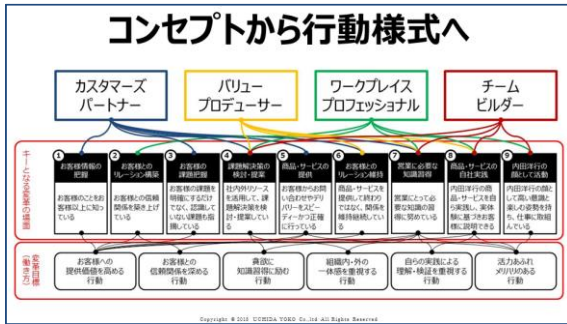


バリューアウト型営業になる



- なぜ今、変わらなければいけないのか**
- 1 外部環境要因 (社会・市場)**
 - 市場環境 (顧客) のニーズや要求が高度になった
 - プロダクトだけでなくソリューションの提案も求めている
 - ソリューション自体もコモディティ化が進んでいる
 - 2 内部環境要因 (社内)**
 - 意思決定のスピードを上げなくてはいけない
 - ニーズやシーズに応えられる営業を増やしたい
 - 組織の壁を壊して社内外協業で価値を創出したい
 - 3 タイミング**
 - オフィスが移転する
 - コミュニケーションシステムが刷新された



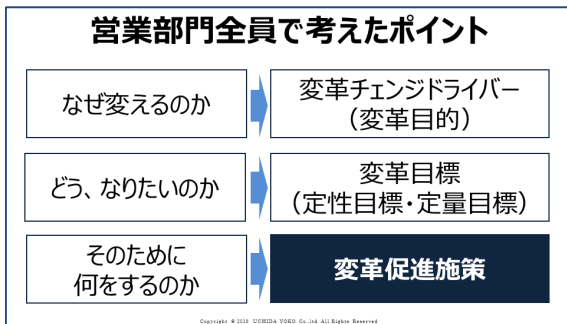


シーンメイキング®

どこでもコレボレーション
 クイックゼミナール
 「ちょっと5分」
 Don't Disturb
 豚づめミーティング
 やつぱり仲間と話したい
 距離なんて関係ない
 ワチで打ち合わせまよ
 おもてなしは任してくれ
 思いっきり電話
 ロングウッドに集う
 立ち会議なんてあたりまえ
 立ちメールもあたりまえ

「ほくがやります」
 デザイナーはベストバディ
 今日は私が先生です
 集中タイム!
 すぐやるうぜ
 集合!
 オフィスの生き字引
 これどう思う?
 落ち着く時間
 クラウド達人
 1時間で仕上げる
 隣の仕事が見える
 それ、いいね

Copyright © 2018 CCSIDA TOKYO Co., Ltd. All Rights Reserved.



変革促進施策の具体化

行動変革	環境整備
ルールプロセス <ul style="list-style-type: none"> ペーパーストックレス 情報の漏洩、隠蔽防止 行動計画と振り返り 自主的学習機会創出 経営プログラム 見えるプログラム 企業に貢献、嬉しい仕組み(協力) ペーパーレス会議 など 	ICT <ul style="list-style-type: none"> スマートフォン、IP電話、FMC 業務用タブレット モバイルPC、タブレット端末 表計算ソフト (VDT) 知の蓄積化 (サイネージ) クラウド、VPN接続 提案共有システム 各種管理システム 社内外、社内チャット ワークプロセスシステム テレワークシステム 電子ホワイトボード オンデマンドプリント 行動学習支援の集約 (スタジアム) など
組織人材スキル <ul style="list-style-type: none"> 組織システム、ビジョン定義 人事管理の強化 リーダー教育 各種スキル研修 (ドキュメンテーション、プレゼンテーション、ファシリテーション、ロジカルシンキング、ICT活用、内閣計画など) 業務の効率化・標準化 自律的行動 など 	ワークスペース <ul style="list-style-type: none"> 自費が決まるとはレイアウト 「仕事」によって組み分けセッション 音響にこだわる音響機材 (スタートアップ専用) 知の蓄積化 (相互学習の場) 収納庫の適正配置 どこでもコミュニケーションシステム など

Copyright © 2018 CCSIDA TOKYO Co., Ltd. All Rights Reserved.



生産性向上に関する指標の例

- 平均リードタイム 22.5日短縮
- 平均受注率 51.6%向上
- 平均受注額 66.1%向上
- 売上高 約20%向上

Copyright © 2018 CCSIDA TOKYO Co., Ltd. All Rights Reserved.



事例紹介2 free株式会社



「全ての業務をクラウド化して業務効率化余剰時間の創出」



**クラウドが実現する
新しい働き方**

2017/7/19
free 株式会社

free株式会社のご紹介
スモールビジネスに関わるみんなが
創造的な活動にフォーカスできるよ



- ✓ クラウド会計ソフト free を中心に、バックオフィス業務のテクノロジーによる自動化・クラウド化を推進
- ✓ 2012年7月創業、現在では従業員280人超
- ✓ シリコンバレー・VC等から累計96億円以上の資金調達
 - 主要株主: DCM, リクルートホールディングス, SBI Fintech Fund, Pavilion Capital (Temasek), Infinity Venture Partners, 未来創生ファンド

ビジネスの開始から、運営、そして成長までをサポートする free



☆ はじめる



会社設立 free
(2015年6月リリース)
設立数4,000突破!
開業 free
(2016年10月リリース)

ひ 運営する



クラウド会計ソフト free
(2013年3月リリース)

ア 育てる



クラウド給与計算ソフト free
(2014年5月リリース)

バックオフィスのプロセス全体を効率化し、創造的な活動にフォーカスできるようにする

free では、自ら会計 free を活用して
圧倒的な業務効率化を実現



経理担当1名(兼任)で、社員280人のバックオフィス業務を運営
兼任の残りの工数は、事業計画の作成など経営企画業務に従事



各部署から上がってきたデータのチェックのみ。あとは支払、報告書の作成がメインで、仕訳入力作業はほとんどありません。

更に、バックオフィスだけでなく
全業務をクラウド化



会計・給与計算



free
給与フリー

営業管理



salesforce

書類作成・メール・スケジュール



Google Apps

全員がダッシュボードを共有

紙を一切印刷しないmeeting

タスク管理

ユーザサポート



zendesk

マーケティング



Marketo

開発コード管理



asana

電子契約



DocuSign

入社手続きもペーパーレス


チャット




LiveChat

GitHub

人事労務でもSaaSを使い倒す




従業員管理




Namely

給与計算フリー




free

Google スプレッドシート




Google

契約書締結・管理




DocuSign

入社手続




free

給与・勤怠管理




free

レビュー




Namely

採用管理




Jobvite

SO管理



Google


給与計算フリー



free

会計フリー (会計連携)

結果的に人事労務業務は0.5人月



100-500名規模法人
人事労務担当者数

平均 3.1人

free 社内
人事労務担当者数

free 社内 0.5人


※給与計算、勤怠管理、社会保険等行政手続、年末調整など人事労務に関する業務担当者数を調査
(2017年2月、free 実施のインターネット調査より)

残りの0.5人月は付加価値業務やメンバーの成長へ投資


- ✓ 入社意欲向上を図る入社前コミュニケーションの検討
- ✓ メンバーサクセスアワー、あえ共ホットラインへの対応
- ✓ 育児支援制度の体系化
- ✓ 人事労務free開発へのフィードバック
- ✓ 外部の勉強会への積極的な出席

7


バックオフィスが仕掛け、みんなで盛り上げる「カルチャードリブン経営」




創業以来の伝統である1:1



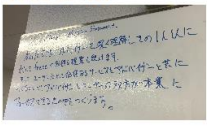
経営会議議事録も事業計画も全員に共有



マネージャー→ジャーナリスト



チームをつくつたらず
ミッション・ステートメント



8

透明化と全員参加による腹落ち感醸成



社長も混じっての全社員参加議論で、価値基準(バリュー・クレド)を作成




毎週・毎月の全社員集会
経営数値も全て開示



9


言葉に組織に浸透するfreeの価値基準



- ユーザーにとって本質的な価値があると自信を持って言えることをする。
⇒ 本質的(マジ)で価値ある
- 理想から考える。現在のリソースやスキルにとらわれず挑戦しつづける。
⇒ 理想ドリブン
- まず、アウトプットする。そして考え、改善する。
⇒ アウトプット→思考
- 取り組んでいることや持っているリソースの性質を深く理解する。
その上で枠を超えて発想する。
⇒ Hack Everything
- 人とチームを知る。知られるように共有する。
オープンにフィードバックしあうことで一緒に成長する。
⇒ あえて、共有する

10

価値基準浸透のポイント(学び)



戦力の逐次投入 NG

- ✓ エース級社員を価値基準委員会に投入
- ✓ 中途半端が一番よくない

間違っても、独自解釈でもOK

- ✓ 自分なりの解釈を持ってもらうことに注力
- ✓ 押し付けない

タッチポイント
ひたすら増加

- ✓ キャッチーな言葉にする(会話で使いやすい)
- ✓ 結局は露出が大事
- ✓ 当たり前のことやってみる。できそうなことはどんどんやってみる

11

戦力の逐次投入NG



価値基準委員会をエース級メンバーで組成しています。
(メンバーサクセスチームは事務局として2名アサイン)



12

間違っても、独自解釈でもOK

← free

どんどん「あなた／あなたのチームの価値基準」という感覚で聞きだしたり、発表してもらうことで、深く考えてもらえる機会を作ると浸透が進む

価値基準1on1
(メンバーがレター形式で価値基準に対する考えをインタビュー。賛否の価値基準あるとしたら?など)

第23回 天下一価値基準 トーナメント 開催決定!
予選: 7/20(土) 13時~18時
決勝: 7/28(土) 22時
主催: 自由経営委員会
価値基準トーナメント@忘年会
(チームの価値基準に基づいた行動やアウトプット自慢大会)

Slackのスタンプ

13

タッチポイントひたすら増加

← free

結局、どれぐらい目に入るかがとても重要

来客用飲料

年賀状

ポスター

サイコロ

14

道の素晴らしいアウトプットに...そしてこれからの改善に...
乾杯。

センギマン

アウトプット思考
まず、アウトプットする。そして考え、改善する。

15

まるで自宅のような職場環境が生産性を上げ、結果として短時間で成果を生み出す

← free

まるで自宅のような職場環境が生産性を上げ、成果を生み出す

自由経営委員会が主催する「アウトプット思考」のセミナー。参加者から「まるで自宅のような職場環境が生産性を上げ、結果として短時間で成果を生み出す」という声が多く聞かれました。

佐々木 大輔
自由経営委員会 代表取締役

<http://superceo.jp/sp/book/vol25/contents/kukan.html>

16

3年連続、働きがいのある会社ランキングに入賞

← free

2017年度版「働きがいのある会社ランキング」で3位入賞
2015年度ランキングより3年連続でランクアップ

- 2015年度 → 5位 (従業員 25-99名)
- 2016年度 → 4位 (従業員 100-999名)
- 2017年度 → 3位 (従業員 100-999名)

GREAT PLACE TO WORK Japan

freeのメンバーサクセスチーム

世界のバックオフィスを変革するムーブメントを作る核となるような組織作りを意識。メンバーがワクワクして活動できるようメンバーサクセスポリシーという考え方を作り、特に組織カルチャー作りや組織活動のサポートに注力する

17

← free

スモールビジネスに携わるすべての人が
創造的な活動にフォーカスできるよう

<https://www.freee.co.jp/>

18



事例紹介3 株式会社ウェブインパクト



「オフィスを手を離れて完全ノマドワーキング化で10年の報告。～海外を見ずに国内の地方を見よ～」

「オフィスを手を離れて完全ノマドワーキング化で10年の報告」
～海外を見ずに、地方を見よ～

株式会社ウェブインパクト
代表取締役 高柳 寛樹

株式会社ウェブインパクト

「まったく新しい働き方の実践」とその後

WEBIMPACT, INC. 2

オフィスを手を離れるとどんな事が起こったか

- ・ 辞める人
- ・ 残る人
- ・ 入る人

WEBIMPACT, INC. 3

モビリティの意味

- ・ 「テレワーク」は自宅への出勤というまやかし
- ・ 管理しない管理

WEBIMPACT, INC. 4

法律との闘い

- ・ 労務
- ・ 税務
- ・ 入管関連法
- ・ 「中国」という特殊性

WEBIMPACT, INC. 5

人材の採用とオフショア

- ・ 「日本人」の意味
- ・ 「ナショナルリティ」の意味
- ・ 「地方」という概念
- ・ 競争が無いところで戦う方法

WEBIMPACT, INC. 6

デジタルネイティブと世代間ギャップ

- LINE採用面接
- 高校生を正規雇用するとどうなるか
- 中学生を正規雇用するとどうなるか
- マス広告とデジマ
- フリック入力とキーボード

WEBIMPACT, INC.

7

コンプライアンスの呪縛

- 合法と脱法とグレーゾーン
- 「コモンセンス」の意味

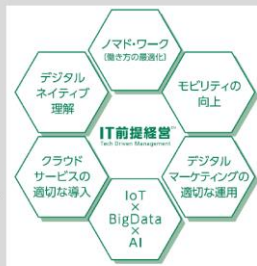
WEBIMPACT, INC.

8

「IT前提経営™(Tech Driven Management)」という考え方

「IT前提経営™」の主定義

デジタルネイティブが中心となる時代において適切なITを経営に導入することでビジネスを最大化するとともにそこに携わる顧客、従業員を含むすべてのステークホルダーを幸せにする経営の概念を指します。



「IT前提経営™」の定義の補足

コミュニケーションの円滑化、働き方の柔軟化、モビリティの向上、業務生産性の向上、BCP/LCP等を目的としたモバイル化、自動化、IoT活用、AI活用、ビッグデータ活用、ロボティクス活用、移動手段の再検討等もこれに含まれます。

WEBIMPACT, INC.

9

書籍の紹介 (配布資料)

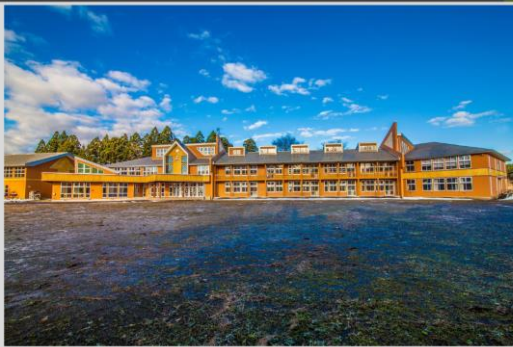
- 日経ビジネスオンライン: 社員を全員「ノマドワーカー」にした会社 (2012年7月27日掲載) business.nikkeibp.co.jp/article/opinion/20120724/234799/
- 「まったく新しい働き方の実践〜「IT前提経営」による「地方創生」〜」ハーベスト社 高柳寛樹 著



WEBIMPACT, INC.

10

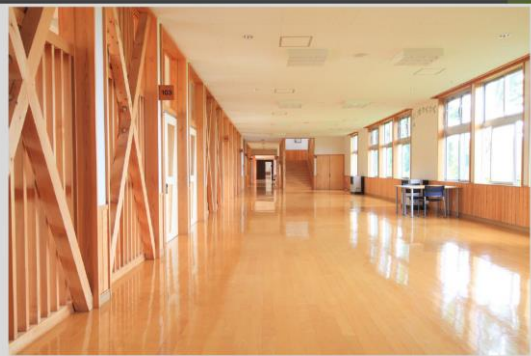
五城目コア (秋田県五城目町: BABAME BASE)



WEBIMPACT, INC.

11

五城目コア (秋田県五城目町)



WEBIMPACT, INC.

12

五城目コア (秋田県五城目町)



WEBIMPACT, INC.

13

五城目コア (秋田県五城目町)



WEBIMPACT, INC.

14

蘇州コア（中国）



WEBIMPACT, INC.

15

蘇州コア（中国）



WEBIMPACT, INC.

16

蘇州コア（中国）



WEBIMPACT, INC.

17

カンボジア キリロム工科大学との業務提携

2017年6月、次世代ソフトウェアエンジニア育成に関する教育プログラムを設立、提携を発表。



WEBIMPACT, INC.

18

カンボジア キリロム工科大学



WEBIMPACT, INC.

19

ウェブインパクトに関するお問い合わせは

https://www.webimpact.co.jp/pr_contact/

WEBIMPACT, INC.

20



事例紹介4 サイボウズ株式会社



「100人いれば100通り 理想でつながるチームとは」

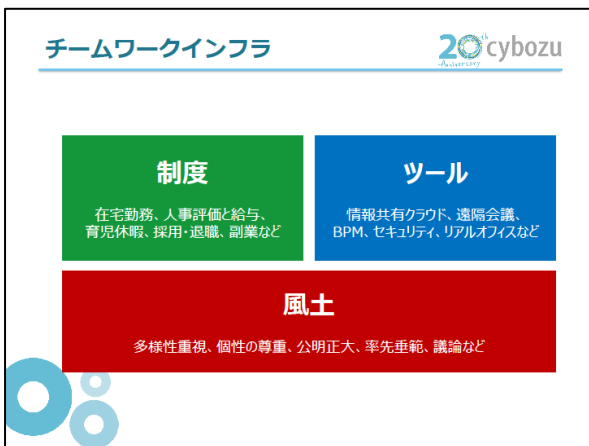
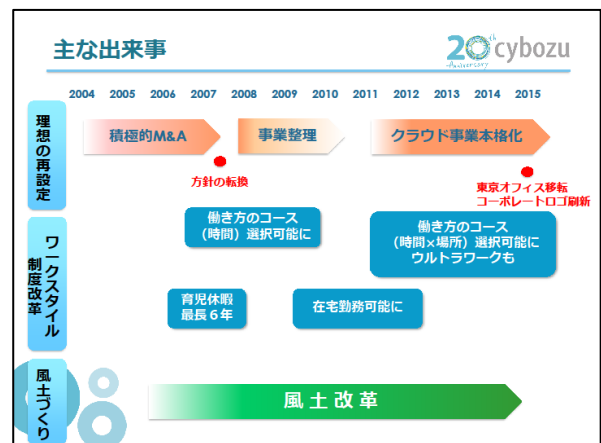
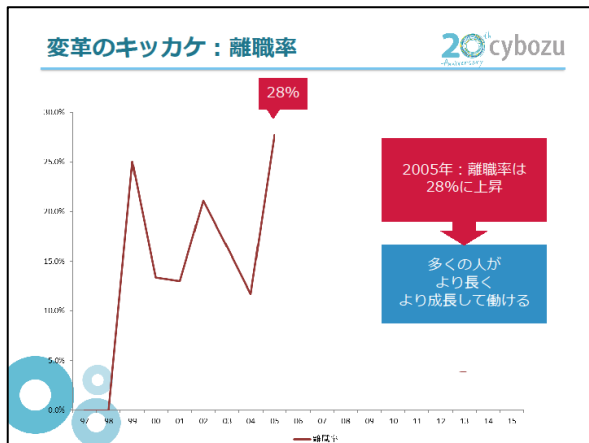
20th anniversary cybozu

**100人いれば100通り
理想でつながるチームとは**
～多様性のある働き方への移行～

サイボウズ株式会社
事業支援本部 石渡清太

20th anniversary cybozu

多様性のある働き方への移行



サイボウズ働き方改革の歴史 20th anniversary cybozu

働き方改革	(補記)	金社セキュリティ体制強化
2007 PS/DS開始	短期離職対策第一歩 ・選択のしやすさ ・チームへのわかりやすさ ・優秀なというメッセージ	
2009 副業許可制	副業の柔軟化第一歩	
2010 在宅勤務試験運用		
2011 PS2導入、在宅勤務本運用開始	時間管理が必要とされる業務 (如山学業) DS, PS, PS2 要日本人商売で全員在宅勤務より柔軟化するために単発的変更を可能に。	
2012 ウルトラワーク試験運用開始 副業解禁	場所の自由度、通常時と準常時の区別などを踏まえた変更	
2013 ウルトラワーク本運用開始 9分制採用開始		CSM (cybozu Security Meeting) 設立
2014 9分制本運用開始		
2015 1か月超変化の場合は選択変更を明確化	日本橋移転、Cisco導入により在宅勤務のハードルが劇的に下がる さらに多様化進む。 ママインターン 中途採用者増加 (短時間・在宅)	
2016	副業→複業 中途採用者増加 (短時間・在宅)	
2017 複業採用開始 9分制廃止	副業→複業 (定額や成果も明確化)	セキュリティ室の設置

チームワークインフラ 20thcybozu

制度

在宅勤務、人事評価と給与、育児休暇、採用・退職、副業など

ツール

情報共有クラウド、遠隔会議、BPM、セキュリティ、リアルオフィスなど

風土

多様性重視、個性の尊重、公明正大、率先垂範、議論など

働き方の多様化へのチャレンジ 20thcybozu

1. 働き方の選択（残業なし、短時間勤務、週3日勤務等）
2. 都合に合わせて働く場所と時間帯を選べるウルトラワーク
3. 最大6年の育児休暇
4. 副業(複業)の自由化（誰でも会社に断りなく副業可）
5. 退社しても再入社できる育自分休暇
6. ストックオプションの廃止と社内持ち株会（100%の補助金）の設置
7. 給与を「社内相対評価」から「社外相対評価(市場性) + 社内絶対評価(信頼度)」へ

働き方の多様化へのチャレンジ 20thcybozu

8. 人事部感動課（社内に感動を作る専門職種）
9. 自由に作れる部活動（年1万円/人）
10. お誕生日会（3,000円/人）
11. 部内イベント支援（年1万円/人）
12. 喜びの叫び（四半期の全社懇親会）
13. 仕事Bar（仕事について語る場。1,500円/人）
14. イベント10（単発のイベント補助。一回半額/人）
15. ドラマ誘致（今までに10回以上登場）
16. スタ場（勉強会を開催したときの飲食代補助）

多様化：その1 **時間**の選択 20thcybozu

ワークを重視するかライフを重視するか。働く時間を選択できる。

1. **ワーク重視型 (PS2)**
裁量労働（専門、企画型）
2. **ワークライフバランス型 (PS)**
残業はできるがある程度に抑えたい
3. **ライフ重視型 (DS)**
残業ナシ または 短時間勤務
育児、介護、副業、通学、..理由は不問

多様化：その2 **場所**の選択 20thcybozu

働く場所を選択できる。

1. **雇用機会の創出**
個別の事情により、オフィスで勤務できない人に就業機会を提供する。障がい者雇用などにも。
2. **業務効率の向上**
オフィス以外の就業場所を提供することにより、個人の業務効率を向上させる。
3. **ライフ重視の支援**
出社ができるが、家で働きたい人の支援をする。
*主にDS(ライフ重視の働き方)を選択している人を想定

多様化：**時間×場所** 20thcybozu

～ライフスタイルに合わせたワークスタイル～

		時間		
		長		
		80%以下	90%	チームとしての報酬
場所	ウルトラワーク	(A3)	(A2)	PS2 (A1)
	自由	(B3)	(B2)	PS (B1)
		(C3)	(C2)	DS (C1)
		短		個人としての報酬
				オフィス (会社の指定場所) (定時未満)

多様化：チームにコミットしない時間 **20thcybozu**

複業OK！

- やってはいけない複業
⇒ **会社の資産***を毀損する複業
*モノ、カネ、情報、時間（業務時間中の副業）、ブランド等
- 事前確認が必要なこと
⇒ 会社の情報、ブランド、役職名、製品名等を使うときは、業務か、資産を毀損しないかを確認のため**申請は必要**
- 注意事項
 - ・ 自己責任で。
 - ・ 本来業務に影響があれば**評価に影響**。
 - ・ 他の会社に雇用される場合は必ず連絡。

副業と複業 **20thcybozu**

	副業	複業
位置付け	サブ主に対して副	パラレル/マルチすべて並列
主目的	副収入を得るため。	自分らしい個性的なキャリアを積むため。
対象	収入を得られる業務が対象。	家事・育児、介護、ボランティア活動など、すべての価値創造活動が対象。

多様化：キャリア **20thcybozu**

育自分休暇 OK！

- サイボウズ退職後6年間は復職可能。（35歳以下）
- 社外での経験を活かして活躍できるメンバーに再びジョインしてもらい、組織の強さを高める。

多様化：コミュニケーションの促進 **20thcybozu**

- ・ 自由に作れる部活動（年1万円/人）
- ・ 部門役職不問のお誕生日会（3,000円/人）
- ・ 部内イベント支援（年1万円/人）
- ・ 全社イベント（喜びの）叫び（全社懇親会）
創業記念パーティー、リリースパーティー等
- ・ 仕事Bar（仕事について語る場。1,500円/人）
- ・ イベント10（単発のイベント補助。一回半額/人）
- ・ 人事部感動課（感動を表現する専門職種）
- ・ サイボウズ・オブ・ザ・イヤー表彰
- ・ 産休中社員、パパママコミュニケーション

部内×部外、仕事×仕事以外、リアル×バーチャルを含めたコミュニケーションの活性、見える化。

チームワークインフラ **20thcybozu**

制度 在宅勤務、人事評価と給与、育児休暇、採用・退職、副業など	ツール 情報共有クラウド、遠隔会議、BPM、セキュリティ、リアルオフィスなど
風土 多様性重視、個性の尊重、公明正大、率先垂範、議論など	

多様化：ツール **20thcybozu**


- 時間、場所を選ばない情報共有、業務
 - ✓ マルチデバイス対応グループウェアと運用（自由にファストで作れるコミュニケーションスペース）（必要な情報を必要な人に伝えるメンション機能）
- 場所を選ばないリアルタイムコミュニケーション
 - ✓ TV会議システム
 - ✓ 全社員Web会議システム
- セキュリティ対策
 - ✓ 物理的、システムの、管理的、人的対策（セキュリティ管理関連部門横断組織（CSM）の設置）（クラウド事業者として、社内セキュリティとして）
- **オフィスづくり**

新日本橋オフィスコンセプト 

Big Hub for Teamwork

多様化、分散化を見据えたうえで、情報やヒトを集結させ、リアルコミュニケーションが活発に行われることにより、サイボウズチームの一体感を高め、エコシステムを含めてハイパフォーマンスを生み出し続けるチームワークの中心拠点。

アクセシビリティ、町の文化、信頼性 ⇒ 東京日本橋タワーへ移転



Communicational

Changeable

Sense5 + 1

Eco Expand

Trust & Secure

Various Concentration

High Performance

Fast & Easy + Entertain

Show case

オフィス：チームにアクセスする方法 



リアルオフィスに
出社する



バーチャルオフィスに
アクセスする

* どこからでもバーチャルオフィスにアクセスできる
* リアルに出社することで得られる効果もある

コミュニケーションの方法 



同期型
・ その場ですぐ
・ リアルな声/表情



非同期型
・ 都合に合わせて
・ 可視化/蓄積

チームワークインフラ 

制度


在宅勤務、人事評価と給与、育児休暇、採用・退職、副業など

ツール

情報共有クラウド、遠隔会議、BPM、セキュリティ、リアルオフィスなど

風土

多様性重視、個性の尊重、公正正大、率先垂範、議論など


2つの風土 

公正正大

- ・ 嘘のない風土を作る。
- ・ 「公の場で明るみに出ても、正しいと大きな声で言えること」
- ・ 多様な人材が同じチームで働くために、サイボウズにおいて基本となる行動規範と定義。
- ・ プライバシー情報とインサイダー情報を除いて隠し事をしない。
- ・ 嘘をつく人、情報を隠す人がいると、多様性のある組織は無駄にやこしくなる。

自立と議論

- ・ 多様性を重視すれば、答えは一つとは限らない。
- ・ 社員同士が建設的に議論して問題を解決するための手段が必要。
- ・ 「問題解決の手法」を繰り返し社内研修
- ・ 「説明責任（気になることは質問しなければならない）」
- ・ 「質問責任（担当者は説明しなければならない）」の考え方を周知徹底

人事制度策定プロセス 

「説明責任・質問責任」の考え方の浸透

社員からの意見・提案

ワークショップを繰り返し、草案を策定

本部長会において社長が意思決定

人事制度は与えられるものではない

「ルールより目的」を徹底する



- どのような制度であっても、目的を理解せずに使うと、期待する効果を得るのは難しい。
- また、厳密に制度を作り、運用していくには大きなコストがかかる。
- 「何のための有休か、何のための育児休暇か、何のための部活動か。」
- **目的を共有・共感することが大事。**



人事制度の方針



「100人いれば 100通りの働き方があってよい」

従業員一人ひとりの個性が違うことを前提に、それぞれが望む働き方や報酬が実現できればよいという考え方。
公平性よりも個性を重んじることで、一人ひとりの幸福を追求する。

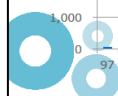
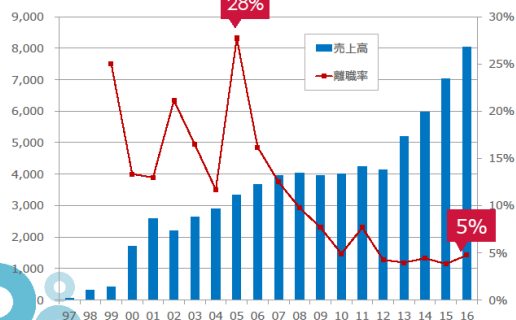
「我が社には多様性がない」と考えるダイバーシティ経営とは逆に、「すでに十分多様なメンバーが集まっている」と考える。



多様性のある働き方への移行と その成果



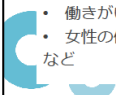
離職率の変化



成果



- 採用力の向上
- 堅調な女性採用、ママインターンの実施と採用
- 産育休後の復帰率100%
- 女性社員比率が約4割に
- 役員女性比率20% (2/10)
- 新入社員男女比率逆転
- 退職社員7名がサイボウズに復帰
- 震災時全員在宅勤務で決算発表
- 社長もフリーアドレス化
- 社内結婚増加
- ダイバーシティ企業経営100選 (経済産業省: H25)
- 働きがいのある会社ランキング2017 5位 (~999人)
- 女性の働きがいのある会社ランキング2017 1位 (~999人) など



創りたいチーム、制度の軸



より多くの方が
より長く
より成長して働ける

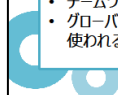
チームワークあふれる 「社会」を創る

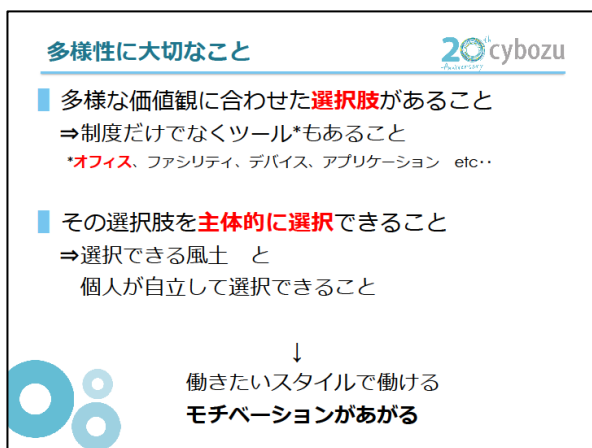
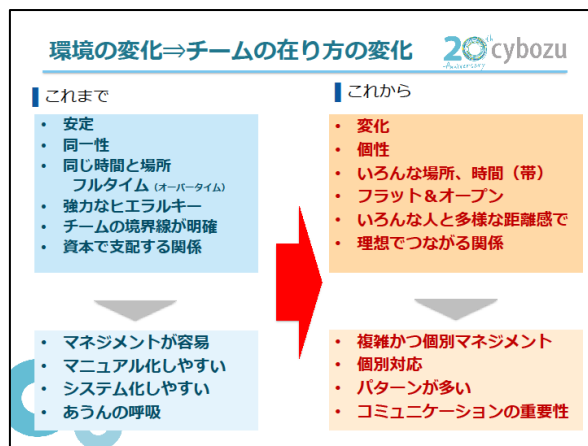
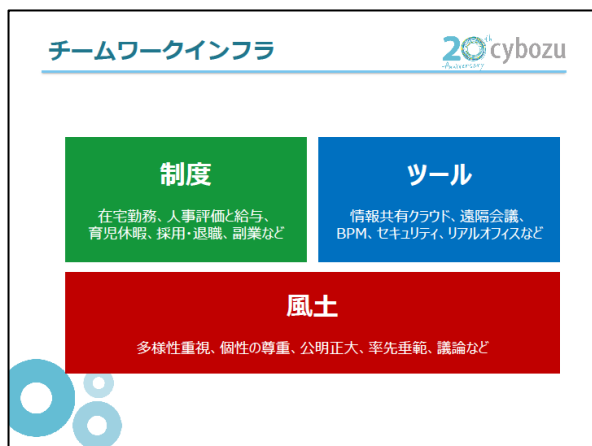
- 優れたグループウェアの開発
- チームワーク強化メソッドの提案
- グローバルに展開し、世界で一番使われるメーカーになる

チームワークあふれる 「会社」を創る

- 多様性(個性)重視
- 公明正大
- 自立と議論の文化

この2つを両立させたい





ご清聴ありがとうございました。
kiyota_ishiwata@cybozu.co.jp

20th cybozu



中小企業におけるテレワークの課題

一般的に考えられるテレワーク導入における課題は次のものが挙げられます。

- コミュニケーション
- セキュリティ
- 労務管理・業務管理

しかしながら、中小企業における課題はさらに、

- システム導入コスト
- 経営者の頭の切り替え

があると考えます。テレワークを実施する際のICTシステム・ツールの導入に非常に高額な投資を必要とするため、資金力に乏しい中小企業にはハードルの高いものとなっています。さらに、ICT投資への理解並びに、導入の意義、社員へのセキュリティ教育など、経営者自身が従来の働かせ方から頭を切り替えて、実現への真剣な取り組みが重要となります。

また、特に昨今問題となっている情報漏洩、セキュリティといった観点からテレワークを見つめ直す必要があると考え、前述しますセキュリティチェックポイントを作成しました。



我々の考えるテレワーク

「クラウドファーストな」テレワーク

我々は、クラウドサービス、アウトソーシングサービスを徹底的に活用したテレワークが中小企業に適した環境であると考えます。

いきなり全てをクラウド化というわけにはいかない現状を認識した上で、目指すべき理想形としての会社業務のクラウド化・アウトソーシング化が、中小企業の課題を解決する一つの考え方であるという結論に達しました。

中小企業は、テレワークを開始するための人材（人）も、設備（物）も、資金（金）も、ノウハウ（情報）もありません。

一般にいわれる自宅での貸与PCからのVPN接続によるテレワークでは膨大な費用かかる一方、PC、紙・USB等リムーバブルメディアでのデータ持出による自宅でのテレワークでは、漏えい・紛失リスクがあまりにも大きすぎます。

クラウドサービスの利用により、仕事の仕方が紙ベースから脱却でき、少ない人材で多様な業務の推進が可能になると確信しています。

▶▶▶ テレワーク自体の課題

テレワークを検討する中で、テレワーク自体の課題として、次のものがあがりました。

■ 職種や業務によっては向き不向きがある

CSAJ 会員各社で職種を i コンピテンシディクショナリ (iCD) のスキル構成図や iCD 別冊から考えると、次のようなものが考えられます。

- ・戦略、企画、研究開発
- ・システム実装（受託・パッケージ）
- ・システム利活用（情報サービス）
- ・システム支援（マネジメント・人材育成）
- ・営業業務
- ・総務、人事、経理

このような職種の中に細分化した業務があります。

「一人で作業しやすい仕事」がテレワークに向いていると言われていています。戦略・企画・研究開発・システム実装（プログラマー）がよく言われている職種です。

リモートアクセスやクラウドサービス、BPOの利用により、上記職種のほぼ全てでテレワークが可能ではないかと考えられます。テレワークに向かないのは、生産・製造現場の仕事だけとの指摘をされる方もいます。

しかし、社外の方と電話やテレビ会議ではなく、直接面談する職種またはそれに係る職種の業務については難しいものと考えます。

具体的には、お客様先に常駐して作業を行うシステム実装の職種はテレワークが難しいものとなります。

大企業で細分化された業務を行う総務、人事、経理については、テレワークを行う素地があるものと見受けられますが、中小企業で、一人または、数名で総務、人事、経理の仕事を纏めてされている方は、お客様の対応等を考えますと、テレワークという訳にはいかないといわざる負えません。

■ 事前作業としてデジタル化、情報分類が必要

経費精算や稟議書のハンコをついてもらう、書類が紙なせいで会社に出なければ行けないといった点をシステム化により、テレワークを可能とすることができます。

しかし、過去に紙で頂いた資料、紙でしかのこっていない資料を探して、確認する状況がテレワークを難しくするでしょう。

会社に連絡して、デジタル化して送ってもらうといった対応が考えられます。

いかに過去の紙の資産をデジタル化するか、検索しやすいように分類するか、テレワークを行う事前作業として必要な作業となると考えます。オフィスから溜まった紙をなくすことを考えてみてはいかがでしょうか。

■ 人自身にテレワークの向き不向きがある

職種や業務によってテレワークに向き不向きがあると前述しました。多くの職種や業務でテレワークは可能と考えましたが、いづくところは「人」です。

当研究会のワーキンググループの打合せにおいても、「ある人物だけにはテレワークをさせられない」といった意見が複数ありました。日頃の行動から見て的的な確な意見かもしれません。

オフィスと異なり人が見ていない状況では、自己管理が求められます。普段の行動からそういった状況を上司も不安に思うのも当たり前です。

結局のところ必要となるのは、部下と上司の信頼関係となるでしょう。

上司は部下を信頼すると共に、今まで以上に部下に目配りする姿勢が必要になりますし、部下としては上司が状況をわかりにくいことを意識して、自分で仕事を進めて行く自主性が必要となります。オフィスと異なり人が見ていない状況でキチンと仕事ができる、そのような人材育成が必要です。



(参考) モデル実証実験を経て

厚生労働省と総務省が連携して実施した「テレワークモデル実証事業」(3年間)の結果としてとりまとめた「テレワークではじめる働き方改革」があり、テレワークの定義や本書の活用方法、現状や効果について紹介され、さらに各モデル類型共通の知識・ノウハウ、モデル類型ごとに異なる知識・ノウハウをご紹介されています。過去の実証実験等を通して各種の参考となるガイドラインがあり、テレワークを導入する場合の十分な手引書が存在しています。我々は、既に存在するテレワークの導入・運用ガイドブック等を踏襲し、その上で中小企業における指標を策定するものです。

- テレワークではじめる働き方改革(厚生労働省)
テレワークの導入・運用ガイドブック
http://work-holiday.mhlw.go.jp/material/pdf/category6/01_01.pdf
- テレワーク導入のための労務管理等Q&A集(一般社団法人日本テレワーク協会)
<http://work-holiday.mhlw.go.jp/material/pdf/category6/02.pdf>
- テレワーク関連ツール一覧(第2.0版) 2017年(一般社団法人日本テレワーク協会)

14 コラム



テレワークを加速するために必要なこと ～会社に来なくても良い環境づくり～



支出精算処理はスマホのワークフローで効率化！

交通費精算処理はこんな流れになっていませんか？

- ① Excelのフォーマットに必要事項を入力して印刷
- ② 領収書等あれば現物を添付して上長に手渡し
- ③ 上長は伝票の内容を確認して問題がなければ承認印を押下して経理部門へ渡す
- ④ 経理部門も伝票の内容をチェックして問題がなければ承認して個人口座へ振り込む

- 支出申請がスマホを使ったワークフローで処理できれば会社へ行かずとも精算できる
- 領収書はスマホで撮影した画像をワークフロー添付できれば更に便利になる
- 交通費はカレンダーの行先ルートと連動できれば、申請処理自体がいらなくなる

こうなると会社に行かなくとも支出精算処理が可能となるだけでなく、事務処理自体が発生時点で処理できてしまうので、これぞIT活用と業務改革による「働き方改革」となるのではないのでしょうか！



いつでも、どこでも、誰もが簡単にテレビ会議ができる環境！

「会議があるから出社しなければいけない」とか「打ち合せのために出張しなければいけない」というのは昔の話。skypeやハングアウト等のビデオ通話をテレビ会議（Web会議含む）のツールとして使えば、いつでもどこでもスマホから参加できます。

社内LANに限定したテレビ会議は接続テスト等の事前準備が必要だったり、いざという時に繋がらなかったり、かなり面倒なイメージがあります。

ビデオ通話を社内でも上手く活用すれば、面倒な準備をすることなく、簡単に誰でもテレビ会議に参加できます。慣れてくれば、テレワークでも社内の人と気軽に、違和感なくコミュニケーションツールとして有効に利用できるのではないのでしょうか！



紙の重要資料(社外秘・秘密情報)は電子化！

業務に必要な資料がバインダーに綴じられた「紙」であるとテレワーク時には困ります。

社内では、まだまだ「紙」の資料を参照しながら作業していることがあるでしょうが、テレワークだと「紙」の資料自体が社外秘や秘密情報であったりすると、情報セキュリティリスクが高くなるため、テレワーク先で資料の管理が求められ、テレワーク従事者の負担が大きくなります。

まずは、紙の重要資料は電子化して必要に応じて共有できること。そして資料を参照しながら作業がしやすい「大きなディスプレイ」を用意するなどの環境整備も必要です。

また、災害対策を考慮すると、セキュリティ条件さえクリアできれば、共有の電子データは社内設置の共有サーバーではなく、パブリッククラウドにあるのがベストではないでしょうか！



社内連絡は電話ではなくチャット！

多くの会社で、部署共通の固定電話での通話から個人配付の携帯電話（スマホ）での通話に変わってきました。

もう一步「働き方改革」を進めて、社内の連絡は通話ではなくチャットを利用すれば、会話自体がデジタル化されているので、関係者との共有も簡単で、作業履歴として残り、検索も可能となり便利です。また、耳で聞いて記憶するより、正しい情報として伝わります。

チャットでの連絡が習慣化すると、社外の共有スペース等(例えばビルの共有喫煙室)で大声で通話することによる情報漏えいや、マナー違反も解消されます。

社内連絡が、チャットになると相手の状況を気にせずに連絡できるので、テレワークだけでなく、フリーアドレスで仕事がしやすい環境になり、働き方も変わるのではないのでしょうか！

15

テレワークに関わる製品・サービス紹介

CSAJ正会員及び賛助会員へ平成30年2月28日～3月12日の期間、働き方改革に関わる製品・サービスの募集を行い、掲載申し込みがあった該当製品・サービスは以下の通り。詳細は、各問い合わせ先へ直接ご連絡ください。

▶▶▶ 15.1.1 製品・サービス分類／仮想デスクトップ方式

表 15-1

会社名	株式会社アール・アイ
製品・サービス名	Shadow Desktop
製品・サービスの特徴	PC上のファイルをクラウドストレージへ仮想化。持ち運び時はデータレス、一度アクセスしたファイルはキャッシュとして編集できるのでオン・オフライン問わず利用可。導入前後の操作が変わらないため教育不要。
製品・サービスの紹介URL	https://www.ri-ir.co.jp/ri_product/shadowdesktop/
製品・サービス価格	月額980円／年額11,400円(税別)
お問合せ先	電話番号:03-6853-7800 メールアドレス:sales@ri-ir.co.jp
セキュリティポリシー関連項目	5.1.2 貸与PCのデータ管理 5.1.4 貸与PCの暗号化
セキュリティチェックリスト関連項目	30【貸与端末】社内利用したPCを在宅端末に転用する場合は、Windowsを新規にセットアップし、不要なデータ、ソフトウェアを排除する。

▶▶▶ 15.1.2 製品・サービス分類／クラウド型アプリ方式

表 15-2

会社名	ファイルフォース株式会社
製品・サービス名	Fileforce®
製品・サービスの特徴	企業向けに特化したクラウドストレージ。ファイルサーバーで実現している権限管理の運用を変えずに情報資産を中央一元管理できます。社内外とのファイル共有も安全・簡単に行えるため、リモートワーク環境にも最適です。
製品・サービスの紹介URL	https://www.fileforce.jp/
製品・サービス価格	標準価格:1ID: ¥1500/月 100GB: ¥2000/月 * 最低契約 5ID/100GB ¥9,500 * ボリュームディカウント有り
お問合せ先	セールス sales@fileforce.jp
セキュリティポリシー関連項目	6. Active directory 9.1 データの暗号化 10.4.1 インターネットの電子メールについて
セキュリティチェックリスト関連項目	4【Active Directory】端末同士のフォルダ共有、ファイル共有を禁止する。 19【規程】個人情報や企業情報が含まれるデータファイルには、必ずパスワードを設定し、暗号化する。

表 15-3

会社名	ピー・シー・エー株式会社
製品・サービス名	PCAクラウド
製品・サービスの特徴	1万社超の法人が利用するクラウド型業務システム。16種類の業務アプリサービ

	スを選択可能。SOC1(内部統制)、SOC2(セキュリティ)取得で安全・安心。最新機能「リマインダー」でテレワークの利便性向上。
製品・サービスの紹介URL	http://pca.jp/pcacloud10000/index.html
製品・サービス価格	月額13,500円/月(税別)
お問合せ先	電話番号:03-5211-2700
セキュリティポリシー関連項目	5.1.1貸与PCのセットアップ 5.1.2.貸与PCのデータ管理 5.1.3貸与PCの脆弱性管理
セキュリティチェックリスト関連項目	14【VPN・通信】インターネットやVPNの通信障害が発生した場合の手順を定める。 21【規程】在宅勤務で使用される貸与端末の管理規定を定める。 22【規程】貸与端末の管理規定内容をユーザーに理解させ、遵守することを合意する。

表 15-4

会社名	日本事務器株式会社
製品・サービス名	Ezharness DaaS Plus
製品・サービスの特徴	クラウドに配置したWindows環境を利用することで、安全なデスクトップ環境を場所や端末を選ばずご利用できるサービスです。
製品・サービスの紹介URL	http://ezharness.jp/service/daas-plus/
製品・サービス価格	1ユーザー月額6,400円～
お問合せ先	日本事務器 事業推進本部 ITプラットフォームソリューション企画部 電話番号:050-3000-1523
セキュリティポリシー関連項目	2.1.1 貸与PCのセットアップ
セキュリティチェックリスト関連項目	—

表 15-5

会社名	日本事務器株式会社
製品・サービス名	recipe.learning
製品・サービスの特徴	クラウド型eラーニングサービスです。以下の特徴があります。 ・どこでも、様々な端末で利用可能 ・使いたい時だけ使える ・教材を簡単に作成出来ます
製品・サービスの紹介URL	https://www.recipe.co.jp/cloud/e_learning
製品・サービス価格	初期費用:10万円 月額費用:基本料金 1万円、1ID 150～200円
お問合せ先	NJCネットコミュニケーションズ 営業部 電話番号:050-3000-1515
セキュリティポリシー関連項目	—
セキュリティチェックリスト関連項目	—

表 15-6

会社名	日本事務器株式会社
製品・サービス名	らくーざ
製品・サービスの特徴	らくーざはフリーアドレスを導入している企業に最適なサービスです。 ・フリーアドレスを導入したのに固定化してしまった ・誰がどこにいるかわからない などの問題を解決します。
製品・サービスの紹介URL	http://www.racooza.com/
製品・サービス価格	初期費用:無料 月額費用:1ID 50円、1エリア 2,000円

お問合せ先	NJCネットコミュニケーションズ 営業部 電話番号:050-3000-1515
セキュリティポリシー関連項目	—
セキュリティチェックリスト関連項目	—

▶▶▶ 15.1.3 製品・サービス分類／会社PCの持ち帰り方式

表 15-7

会社名	株式会社ZenmuTech
製品・サービス名	ZENMU for PC
製品・サービスの特徴	データを無意味化し、PC内とUSBメモリやスマートフォンなどの外部メディアに分散保管。オフラインでも、安心・安全にローカルに保存したデータを利用可能。万一、PCの盗難や紛失に遭っても、情報漏洩になりません。
製品・サービスの紹介URL	https://zenmutech.com/products/zenmu-for-pc-ws
製品・サービス価格	定価(1台の場合) サブスクリプション:年額 9,600円 パーペチャル:27,400円(永久ライセンス)、保守料4,100円(年額)
お問合せ先	メールアドレス:info@zenmutech.com 電話番号:03-5436-6541
セキュリティポリシー関連項目	5.1.4 PCの暗号化
セキュリティチェックリスト関連項目	34【貸与端末】貸与端末のハードディスクをBitLockerで暗号化する。

▶▶▶ 15.1.4 製品・サービス分類／勤怠管理ツール

表 15-8

会社名	株式会社ラネクシー
製品・サービス名	PC操作ログの収集・管理ソフトウェア「MylogStar 3」(マイログスター)
製品・サービスの特徴	MylogStarは物理環境・シンクライアント環境にかかわらず、業界トップクラスの精度の高い収集力で操作ログなどを取得できるソリューションです。また、取得した操作ログは直観的に使える管理画面で効率的に管理・活用ができます。
製品・サービスの紹介URL	http://www.mylogstar.net/
製品・サービス価格	MylogStar3 Network版 (例:100台構成)1,416,000円～
お問合せ先	電話番号:03-6261-4711 メールアドレス:mis_sales@runexy.co.jp
セキュリティポリシー関連項目	8.2.1 Windows Serverのログ 8.2.2 Windowsクライアント(貸与端末を含む端末)のログ 9.3.4 USBメモリの運用
セキュリティチェックリスト関連項目	25【規程】USBメモリの運用規定を定める。 46【ログ】貸与端末、サーバーのセキュリティログ、アプリケーションログ、システムログ、アンチウイルスソフトのログの保存を行う。 48【ログ】ログを統合的に分析・管理する。

表 15-9

会社名	株式会社ソリューション・アンド・テクノロジー
製品・サービス名	WiMS/SaaS 勤務管理システム
製品・サービスの特徴	クラウド型勤務管理システムです。出退勤の管理に加え、どの業務にどれだけ時間をかけたのか、1日の業務内容と要した時間を可視化できます。パフォーマンス分析と将来予測でのアラートでチーム力向上に役立ちます。
製品・サービスの紹介URL	https://wims-saas.solty.co.jp/

製品・サービス価格	初期設定サービス費用: 応相談、月額利用料: 1人当たり290円
お問合せ先	クラウドソリューション統括部 電話番号: 03-3222-0201(代) E-Mail: wims@biz.solty.co.jp
セキュリティポリシー関連項目	—
セキュリティチェックリスト関連項目	—

表 15-10

会社名	株式会社ヒューマンテクノロジーズ
製品・サービス名	勤怠管理システムKING OF TIME
製品・サービスの特徴	60万ユーザーを支えるクラウド勤怠管理システム。外出先からのスマホGPS打刻、生体認証での本人確認打刻、テレワークの管理も楽にするWindowsログオン/ログオフの時間管理など新しい技術をいち早く取り入れています。
製品・サービスの紹介URL	https://www.kingtime.jp
製品・サービス価格	月額300円×利用人数
お問合せ先	KING OF TIME営業担当 メールアドレス: kot_sales@h-t.co.jp 電話番号: 03-4577-9567
セキュリティポリシー関連項目	—
セキュリティチェックリスト関連項目	—

表 15-11

会社名	応研株式会社
製品・サービス名	就業・勤怠管理システム「就業大臣NX」
製品・サービスの特徴	負担の大きいスケジュール・シフト管理やタイムカード集計を一気に効率化。充実した機能で労働時間を見る化します。また、長時間労働の抑制や適正な労働時間管理に役立つアラート機能も搭載。
製品・サービスの紹介URL	http://www.ohken.co.jp/product/shugyo/
製品・サービス価格	就業大臣NX スタンドアロン 250,000円(税抜)～
お問合せ先	応研株式会社 東京本社 電話番号: 03-3299-0789
セキュリティポリシー関連項目	—
セキュリティチェックリスト関連項目	—

表 15-12

会社名	応研株式会社
製品・サービス名	大臣スマート打刻サービス
製品・サービスの特徴	スマートフォンで出退勤の打刻や打刻履歴確認が行える「大臣スマート打刻サービス」。直行直帰の多い外勤社員、建設現場や訪問介護の職員、派遣勤務やテレワークでも正確な勤怠管理を可能にします。
製品・サービスの紹介URL	http://www.ohken.co.jp/product/dsd/
製品・サービス価格	年額 2,400円(1IDあたり/税抜)
お問合せ先	応研株式会社 東京本社 電話番号: 03-3299-0789
セキュリティポリシー関連項目	—
セキュリティチェックリスト関連項目	—

▶▶▶ 15.1.5 製品・サービス分類／業務管理(プロジェクト管理)ツール

表 15-13

会社名	ナレッジスイート株式会社
製品・サービス名	KnowledgeSuite(ナレッジスイート)
製品・サービスの特徴	クラウド型グループウェア/SFA/CRM/マーケティングオートメーションが全て統合連携され、ユーザー数無制限で利用できる、中小中堅企業向けビジネスアプリケーション
製品・サービスの紹介URL	http://knowledgesuite.jp
製品・サービス価格	ユーザー数無制限月額ストレージ課金:グループウェア6,000円/月～ SFA 50,000円/月～
お問合せ先	電話番号:03-5440-2081
セキュリティポリシー関連項目	—
セキュリティチェックリスト関連項目	—

▶▶▶ 15.1.6 製品・サービス分類／ペーパーレス化ツール

表 15-14

会社名	株式会社ブルーポート
製品・サービス名	iTutor(アイチューター)
製品・サービスの特徴	導入企業1200社以上のマニュアル作成ソフト「iTutor」。業務の効率化に必要な操作マニュアルや手順書を簡単に作成できます。その上、伝わり易い動画やトレーニングコンテンツも同時に生成でき、働き方改革の推進に役立ちます。
製品・サービスの紹介URL	http://www.itutor.jp/
製品・サービス価格	550,000円～
お問合せ先	株式会社ブルーポート 営業推進部 電話番号:03-3261-0317
セキュリティポリシー関連項目	—
セキュリティチェックリスト関連項目	—

▶▶▶ 15.1.7 製品・サービス分類／安全なモバイルテレワークツール

表 15-15

会社名	株式会社応用電子
製品・サービス名	FKEY SConnect
製品・サービスの特徴	あんしん Windowsウイルスをブロック、毎回クリーンなPC かんたん PCにインストールするだけ、1台から導入可能 べんり PC1台で2役、1クリック接続
製品・サービスの紹介URL	https://fkey.jp/fsv100h
製品・サービス価格	オープン価格 (想定市場売価 1ライセンス9,600円/年より)
お問合せ先	https://fkey.jp/contact#form
セキュリティポリシー関連項目	5.1.7 貸与PCと宅内の他の端末との通信遮断 5.1.8 貸与PCのRDP接続の禁止 5.2.1 宅内LANでの検索、共有
セキュリティチェックリスト関連項目	19【規程】個人情報や企業情報が含まれるデータファイルには、必ずパスワードを設定し、暗号化する。 23【規程】貸与端末に個人利用のソフトウェアのインストールや、データをインポー

トさせない。
30【規程】社内利用したPCを在宅端末に転用する場合は、Windowsを新規にセットアップし、不要なデータ、ソフトウェアを排除する。

▶▶▶ 15.1.8 製品・サービス分類／RPAツール

表 15-16

会社名	ネクストウェア株式会社
製品・サービス名	WinActor(ウインアクター)
製品・サービスの特徴	WinActorは、日々のパソコン定型業務を自動化するソフトウェア型ロボットです。小規模組織から、大企業まで様々な用途で定型作業に要する時間をロボットが削減し、貴重な人材&時間の確保で働き方改革を支援します。
製品・サービスの紹介URL	http://www.nextware.co.jp/product/winactor/
製品・サービス価格	WinActor フル機能版 標準定価 ¥908,000.-/年 実行版 標準定価 ¥248,000.-/年 管理ロボ 標準価格 ¥2,280,000.-/年
お問合せ先	東京オフィス 電話番号:03-5447-2511 名古屋オフィス 電話番号:052-201-9880 大阪オフィス 電話番号:06-6281-2711
セキュリティポリシー関連項目	8.2.1 Windows Serverのログ 8.2.2 Windowsクライアント(貸与端末を含む端末)のログ
セキュリティチェックリスト関連項目	46【ログ】貸与端末、サーバーのセキュリティログ、アプリケーションログ、システムログ、アンチウイルスソフトのログの保存を行う。

▶▶▶ 15.1.9 製品・サービス分類／コンサルティングサービス

表 15-17

会社名	ネクストウェア株式会社
製品・サービス名	WinActor導入支援パック
製品・サービスの特徴	WinActorは、少しパソコンに詳しい人がちょっとしたコツを理解して、システムエンジニアが要らずに使えます。しかし、本当の力を発揮するには、豊富な経験を活かした導入支援サービスや教育サービスの利用が効果的です。
製品・サービスの紹介URL	http://www.nextware.co.jp/product/winactor/
製品・サービス価格	WinActor導入支援パック 訪問型有償トライアル2ヶ月お試しパック 参考価格 ¥190,000.- 集合型有償トライアル2ヶ月お試しパック 参考価格 ¥120,000.- 初期導入支援スタートパック 参考価格 ¥500,000.- シナリオ作成技術相談パック 参考価格 ¥350,000.- シナリオ作成支援 別途、都度見積
お問合せ先	東京オフィス 電話番号:03-5447-2511 名古屋オフィス 電話番号:052-201-9880 大阪オフィス 電話番号:06-6281-2711
セキュリティポリシー関連項目	8.2.1 Windows Serverのログ 8.2.2 Windowsクライアント(貸与端末を含む端末)のログ
セキュリティチェックリスト関連項目	43【ログ】貸与端末、サーバーのセキュリティログ、アプリケーションログ、システムログ、アンチウイルスソフトのログの保存を行う。

表 15-18

会社名	日本事務器株式会社
製品・サービス名	Customer Success Service
製品・サービスの特徴	「ワークスタイル変革」を志向する企業にソリューションの提供だけではなく、企業の生産性向上、社員同士のコラボレーションの深耕を目指し、行動改革や環境整

	備推進といった施策をお客様と共創するサービスです。
製品・サービスの紹介URL	なし
製品・サービス価格	20万円～
お問合せ先	事業推進本部 ITプラットフォームソリューション企画部 電話番号:050-3000-1523
セキュリティポリシー関連項目	—
セキュリティチェックリスト関連項目	—

▶▶▶ 15.1.10 製品・サービス分類／その他

表 15-19

会社名	株式会社コネクティル
製品・サービス名	テレワーク適性検査サービス
製品・サービスの特徴	テレワーク勤務に必要な基本的な資質や志向性などを5つの指標軸で検査し、テレワーク適性度を診断します。検査結果は、社員のテレワーク勤務可否の判断材料としての活用や、注意点の確認を行うことができます。
製品・サービスの紹介URL	http://www.workdive.co.jp/service/aptitude_test/
製品・サービス価格	3,000～15,000円
お問合せ先	メールアドレス: info@workdive.co.jp
セキュリティポリシー関連項目	—
セキュリティチェックリスト関連項目	—

表 15-20

会社名	クオリティソフト株式会社
製品・サービス名	ISM CloudOne
製品・サービスの特徴	PCやスマートフォンのIT資産管理、セキュリティ対策が行えるクラウド型の製品です。自動脆弱性診断や操作ログ取得、ソフトウェア起動制御、外部デバイス制御等の機能を搭載しており環境を問わず端末管理が行えます。
製品・サービスの紹介URL	https://ismcloudone.com/
製品・サービス価格	各販売店様のホームページよりご確認ください。 https://ismcloudone.com/partner/
お問合せ先	メールアドレス: sales@qualitysoft.com 電話番号:0120-014-691
セキュリティポリシー関連項目	<p>5.1.2 貸与PCのデータ管理/ハードウェア・ソフトウェアの管理</p> <p>5.1.3 貸与PCの脆弱性管理/OS・ソフトウェアのバージョン管理を支援</p> <p>5.1.4 貸与PCの暗号化/ISMのHDD暗号化機能なら暗号化のステータス管理と複合鍵の統合管理がコンソール上から可能</p> <p>5.1.6 貸与PCのアンチウイルスソフトによる電子メールの検知/ふるまい検知で未知のマルウェアや脆弱性攻撃を防御</p> <p>5.1.8 貸与PCのRDP接続の禁止、デフォルトポートの変更/遠隔操作アプリケーションの利用を制限</p> <p>5.2.2 無線LANのプロトコル/ネットワーク接続制御で無線LANの接続先を制限する</p> <p>5.2.4 宅内端末のアンチウイルスソフトと脆弱性管理/OS・ウイルス対策ソフトのバージョン管理を支援</p> <p>8.2.2 Windowsクライアント(貸与端末を含む端末)のログ/PCの操作ログ取得を支援</p> <p>9.3.2 貸与端末の個人利用の禁止/不適切なWEBアクセスを制御</p> <p>9.3.3 貸与端末の無許可ソフトウェア、クラウドサービスの使用禁止/不適切なソフトウェアの利用を制限</p> <p>9.3.4 USBメモリの運用/外部デバイスの申請～管理を支援</p>

セキュリティチェックリスト関連項目	<p>30【貸与端末】社内利用したPCを在宅端末に転用する場合は、Windowsを新規にセットアップし、不要なデータ、ソフトウェアを排除する。</p> <p>31【貸与端末】ユーザーが利用中の端末を在宅端末に転用する場合は、OS、アプリケーションのセキュリティパッチの適用を確認する。</p> <p>33【貸与端末】OS・ミドルウェア、アプリケーションの脆弱性を管理する</p> <p>35【貸与端末】アンチウイルスによる完全スキャンを実施する</p> <p>36【貸与端末】電子メールのアンチウイルスソフトによるマルウェア検知を実施する</p> <p>45【宅内端末】アンチウイルスソフトを適用する</p> <p>46【ログ】貸与端末、サーバーのセキュリティログ、アプリケーションログ、システムログ、アンチウイルスソフトのログの保存を行う。</p>
--------------------------	---

表 15-21

会社名	株式会社バース情報科学研究所
製品・サービス名	BIRDS FAX+(バース ファックス プラス)
製品・サービスの特徴	WEBブラウザとインターネット環境があれば会社宛のFAXを社外から確認、FAX送信もできるクラウド型サービスです。受信FAXの自動振分やステータス管理、参照・編集制限など業務用機能を搭載しています。
製品・サービスの紹介URL	https://www.birds.co.jp/service/fax/
製品・サービス価格	[初期]32,000円 ※ライトプラン [月額]基本料:22,000円、受信料(1,001枚目より):20円×枚、送付料:15円×枚
お問合せ先	営業本部ES営業部 部長 佐々木邦之 メールアドレス: sasaki@birds.co.jp 電話番号: 03-5744-7151
セキュリティポリシー関連項目	10.1 ブラウザがTLSの状態であることを理解させる。
セキュリティチェックリスト関連項目	26【教育】ブラウザがTLS/SSLの状態であることを理解させる。

表 15-22

会社名	グローバルフレンドシップ株式会社
製品・サービス名	GFI電子割符®(システム等開発用ライブラリ)
製品・サービスの特徴	電子情報をビットレベルで分割し分散管理する為の複数ファイルを生成します。それら分割後のファイルは個人情報等の法令の定義項から除外されることの確認ができております。更に復元条件設定が可能です。
製品・サービスの紹介URL	http://www.gfi.co.jp/
製品・サービス価格	個別応談(商用開発以外にも、試作、実証実験、自社内使用等対処)
お問合せ先	メールアドレス: gfi-info@gfi.co.jp
セキュリティポリシー関連項目	<p>5.1.2 貸与PCのデータ管理</p> <p>5.1.4 貸与PCの暗号化</p> <p>7.1.1 VPNの方式検討</p> <p>7.1.3 VPN接続時のクレデンシャル(ID、パスワード等の認証情報)</p> <p>7.1.4 大規模な通信障害</p> <p>7.1.5 VPN接続の否認</p> <p>8.1 通信装置</p> <p>8.2 Windows</p> <p>8.3 ログの統合分析</p> <p>9.1 データの暗号化</p> <p>9.2 クレデンシャルの安全</p> <p>9.3.4 USBメモリの運用</p> <p>10.4 電子メールは暗号化されず、平文で通信が行われていることを理解させる</p>
セキュリティチェックリスト関連項目	<p>10【VPN・通信】VPNの方式を検討し、接続手順と認証方式を定め保守する。</p> <p>12【VPN・通信】VPN接続時のクレデンシャル (ID、パスワード等の認証情報) の保護、運用管理を行う。</p> <p>15【VPN・通信】VPN接続での否認、なりすましを排除する。</p> <p>19【規程】個人情報や企業情報が含まれるデータファイルには、必ずパスワードを設定し、暗号化する。</p>

表 15-23

会社名	株式会社ヒューマンテクノロジーズ
製品・サービス名	人事管理システムhuubHR
製品・サービスの特徴	紙やExcelで活用できずに眠ったままの人事データを簡単・スムーズ・安全に一元管理できるクラウド人事管理システム。マイナンバー管理にも対応。
製品・サービスの紹介URL	https://www.huubhr.jp/
製品・サービス価格	月額100円×利用人数
お問合せ先	huubHR営業担当 メールアドレス:kot_sales@h-t.co.jp 電話番号:03-4577-9567
セキュリティポリシー関連項目	—
セキュリティチェックリスト関連項目	—

表 15-24

会社名	株式会社ヒューマンテクノロジーズ
製品・サービス名	Windowsログオン認証 KING OF TIME セキュアログイン
製品・サービスの特徴	クラウド認証でWindowsログオンを簡単・安全にしてくれるセキュリティサービス。勤怠管理システムKING OF TIMEと連携すればWindowsログオン・ログオフ時間を出退勤時間として使うことができます。
製品・サービスの紹介URL	https://www.kot-sl.jp/
製品・サービス価格	月額200円×利用人数
お問合せ先	KING OF TIME セキュアログイン 営業担当 メールアドレス:fps@h-t.co.jp 電話番号:03-4570-8554
セキュリティポリシー関連項目	—
セキュリティチェックリスト関連項目	—

表 15-25

会社名	日本事務器株式会社
製品・サービス名	LanScope Cat for Cloud
製品・サービスの特徴	PC操作ログ管理、PC資産管理、アプリ稼働管理、外部デバイス管理で、利用デバイス、環境、利用者の安全・安心を確保します。
製品・サービスの紹介URL	https://ezharness.jp/service/hosting-plus/lanscope/
製品・サービス価格	LanScope Cat for Cloud Basic ローレンジモデル 34,800円～
お問合せ先	日本事務器 事業推進本部 ITプラットフォームソリューション企画部 電話番号:050-3000-1523
セキュリティポリシー関連項目	5.1.1 貸与PCのセットアップ 5.1.2 貸与PCのデータ管理 5.1.3 貸与PCの脆弱性管理 8.2.2 Windowsクライアント(貸与端末を含む端末)のログ
セキュリティチェックリスト関連項目	21【規程】在宅勤務で使用される貸与端末の管理規定を定める。 24【規程】貸与端末に会社が許可していないソフトウェア、ツール、オープンソース、クラウドシステム等を利用させない。 31【貸与端末】ユーザーが利用中の端末を在宅端末に転用する場合は、OS、アプリケーションのセキュリティパッチを適用を確認する。 33【貸与端末】OS、ミドルウェア、アプリケーションの脆弱性を管理する。

表 15-26

会社名	BBソフトサービス株式会社
製品・サービス名	Zenlok Archive (ゼンロックアーカイブ)

製品・サービスの特徴	Zenlokは、電子メールと連携し退職者を含めたメールデータをクラウド上に最大7年間 容量無制限で暗号化し保管します。Office365とG Suiteといったクラウドメールだけでなく、SMTPリレー接続できるメールにも対応しています。簡易的な管理画面で、検索、エクスポートなど情報監査に必要な機能を1ライセンス 年額 2,400円にて提供します。
製品・サービスの紹介URL	https://zenlok.jp/
製品・サービス価格	製品名: Zenlok Archive 価格: 年額 1ライセンス 2,400円(税抜)
お問合せ先	Zenlok事業統括部 Zenlok営業担当 メールアドレス: biz-service@bbss.co.jp
セキュリティポリシー関連項目	—
セキュリティチェックリスト関連項目	—

16

研究会参加メンバー一覧

主査	中村 憲司	株式会社大和コンピューター 代表取締役社長
副主査	村瀬 正典	株式会社バース情報科学研究所 代表取締役社長 *
	恵志 章夫	ITエージェント株式会社 代表取締役社長
	小川 敦	株式会社アール・アイ 代表取締役
	石坂 俊成	株式会社アール・アイ
	山根 太郎	アクセルユニバース株式会社 代表取締役
	有澤 真紀	アクセルユニバース株式会社
	板東 直樹	アップデートテクノロジー株式会社 代表取締役社長 *
	土屋 和洋	石渡電気株式会社
	山本 祥之	株式会社インテリジェント ウェイブ 特別顧問
	山中 亮	株式会社インテリジェント ウェイブ
	伊達 友里	株式会社インテリジェント ウェイブ 経営管理本部 総務部
	呉 哲	株式会社インテリジェント ウェイブ 経営管理本部 経営企画部 リーダー
	長谷川 浩	株式会社インテリジェント ウェイブ
	加藤 浩輔	株式会社インテリジェントウェイブ 総務部
	高柳 寛樹	株式会社ウェブインパクト 代表取締役社長
	山崎 繁	株式会社ウェブインパクト ソリューション営業部 部長
	宮脇 学	株式会社ウェブインパクト ソリューション営業部 課長
	畠田 伸一郎	株式会社ウチダ人材開発センタ 事業推進・常務取締役
	野間 操	株式会社内田洋行 知的生産性研究所 CWコンサルティングサービス課 担当課長
	羽田 知洋	オー・エイ・エス株式会社
	富永 芳男	株式会社OSK
	安田 徹	株式会社オービックビジネスコンサルタント 開発本部 ICTセンター 課長
	村田 哲也	株式会社オープンストリーム 業務推進本部 本部長
	松尾 志穂美	株式会社オープンストリーム 業務推進本部 副本部長
	萱沼 徹	キャップクラウド株式会社 代表取締役CEO
	佐藤 智明	株式会社クライル 代表取締役
	保倉 豊	グローバルフレンドシップ株式会社 代表取締役社長
	船引 隆司	クロノス株式会社
	松本 悦宜	株式会社神戸デジタル・ラボ
	小林 淳也	株式会社国和システム 事業戦略室 室長
	佐藤 健太郎	株式会社国和システム 事業戦略部事業計画課
	小山 忍	株式会社コスモ・コンピューティングシステム CP管理本部・主任
	白水 公康	サイバートラスト株式会社 セキュアIoTプラットフォーム推進事業本部・部長
	石渡 清太	サイボウズ株式会社 事業支援本部 内部統制部 シニアエキスパート・政策渉外担当
	川村 貴宏	さくらインターネット株式会社 人事部
	金成 葉子	株式会社シーシーダブル 代表取締役社長
	清水 通則	株式会社シーシーダブル 企画本部長
	田代 貴志	株式会社大和コンピューター i 農業開発部 部長
	奥元 健一	株式会社大和コンピューター RFIDソリューション部 部長
	稲葉 雄一	ナレッジスイート株式会社 代表取締役社長
	澁谷 和幸	株式会社ネオジャパン SMB営業部 課長
	宮川 美晴	株式会社ネオジャパン 経営企画室 室長

山田 志貴	株式会社ネオジャパン
馬場 琴美	ネクストウェア株式会社 総務部 部長
太田垣 博嗣	ネクストウェア株式会社 社長室
松倉 泉	株式会社Harness LLP 代表取締役
小澤 薫	社会保険労務士法人ヒューマン・プライム 代表
矢崎 哲也	社会保険労務士法人ヒューマン・プライム コンサルタント・社会保険労務士
砂田 剛	株式会社ファーストリンク 代表取締役
木村 康宏	freee株式会社 社会インフラ企画部長
若山 寛幸	マルワソフト株式会社 代表取締役
佐久間 祈	マルワソフト株式会社
村田 一	ラクラス株式会社 取締役
坂尻 洋一	リコーITソリューションズ株式会社
林 英司	レバレジーズ株式会社 レバテック事業部 部長
杉山 弘行	静岡県袋井市 企画財政部 ICT街づくり課 情報政策課長
矢内 英直	静岡県袋井市 企画財政部 ICT街づくり課 情報政策係長
大石 隆之	静岡県袋井市 企画財政部 ICT街づくり課 情報政策係
寺田 和英	静岡県袋井市 企画財政部 ICT街づくり課 情報政策係

セキュリティワーキンググループメンバー

主査	板東 直樹	アップデートテクノロジー株式会社 代表取締役社長 *
	山本 祥之	株式会社インテリジェント ウェイブ 特別顧問
	中村 憲司	株式会社大和コンピューター 代表取締役社長
	村瀬 正典	株式会社バース情報科学研究所 代表取締役社長 *
	藤田 美雄	株式会社大塚商会 経営計画室経営計画・IR課課長
	石渡 清太	サイボウズ株式会社 事業支援本部 内部統制部 シニアエキスパート・政策渉外担当
	国枝 直之	日本事務器株式会社 *
	浅野 利也	日本事務器株式会社
	加藤 智巳	株式会社ラック 理事 ITプロフェッショナル統括本部 サイバーセキュリティ事業部 シニアコンサルタント

事務局	原 洋一	一般社団法人コンピュータソフトウェア協会 理事・事務局長
	戸島 拓生	一般社団法人コンピュータソフトウェア協会 業務課 係長
	澤口 瑠璃	一般社団法人コンピュータソフトウェア協会 業務課

※敬称略、メンバーは社名五十音順

※部署・役職は平成29年12月時点

※「*」は、執筆メンバー

**中小企業でのIT利活用による
テレワーク実現に向けた
ガイドライン(在宅勤務編)**

(働き方改革研究会活動報告書)

2018年3月30日 第1版

CSAJ Computer Software Association of Japan
一般社団法人コンピュータソフトウェア協会

〒107-0052
東京都港区赤坂1-3-6
赤坂グレースビル
TEL : 03-3560-8440
FAX : 03-3560-8441
<http://www.csaj.jp/>