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]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ところですが、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碍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）できるものとします。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る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 Directroy（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）

使用途中の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、Flush、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出てくる。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、Flush、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過ご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ー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ー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ー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の的となる。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ー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
http://www.atmarkit.co.jp/fwin2k/win2ktips/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adminiCount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テラバイトを超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ー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の的となる。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 Administrtor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を使用を禁止する。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、UserPricipalName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を超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。

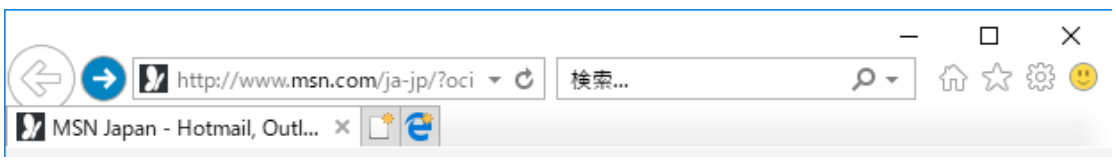
10.1 ブラウザがTLSの状態であることを理解させる。

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で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コーマスでの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分かります。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 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[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カウントとは異なるメールアカウントに（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カウントが入っています。

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、virustotal 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認識した上で、以下の対策を必ず行いましょう。

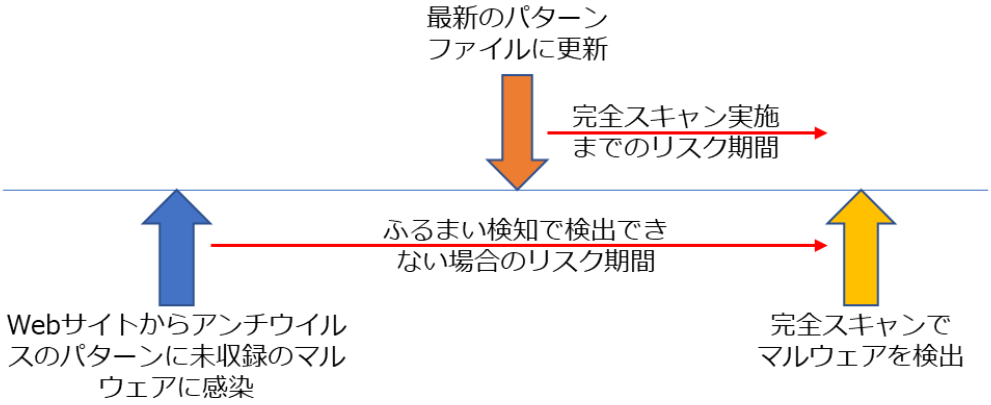
- ✓ 銀行やクレジットカード会社、その他 ID、Password を登録したサイトの正規の URL を確認し、実際に正規のサイトにログインしてサイトの証明書を確認する
- ✓ フィッシング対策協議会[5] 、日本サイバー犯罪対策センター[6]で最新のフィッシングに関する具体的な情報を知る
- ✓ 不安を煽る文面のメールが届いた場合は、絶対にリンクをクリックせず、リンクにマウスオバーして URL が正規であるかを確認する
- ✓ 通常とは異なる体裁や不自然と感じたときは、リンクや添付ファイルを開かず、電話などの異なる手段で確認をとる
- ✓ 送信元が確認できないメールは添付ファイルを決して開か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

[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法を理解させる

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入手することが重要です。
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。こうしたミスを減らすためにも、パターンファイルが最新であるか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。

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。

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。

以下の例では「11.209.80」となっています。

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。

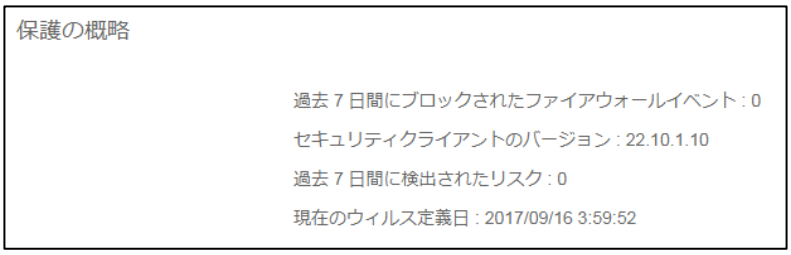
SEP Cloudをアップデートする

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 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

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）を追加するなどとすれば、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ー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。