マイナンバー/特定個人情報保護に対する
デルのセキュリティ対策ソリューション＆サービス

ご提案資料

The power to do more

2015年6月

デル株式会社

デルのセキュリティ戦略

1

ネットワーク

ネットワーク パフォーマンスを下げずに確実に保護と制御します

- 次世代ファイアウォール
- セキュア モバイルアクセス
- メールセキュリティ

Dell SonicWALL

ユーザー

実際の環境でアイデンティティとアクセスを管理します

- アイデンティティ ガバナンス
- 特権管理
- アクセス管理

Dell One Identity Solutions

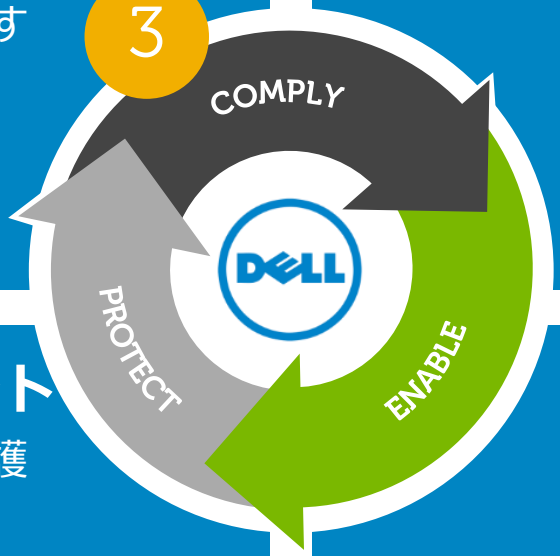
2

データとエンドポイント

場所に関係なくデータを保護します

- 暗号化
- 構成とパッチ管理
- Secure Cloud Client
- 作業領域の保護

Dell Data Protection, Dell KACE, EMM



サービス

脅威に対する保護、予測、対応

- インシデントへの対応
- マネージド セキュリティサービス
- セキュリティ&リスク コンサルティング
- スレット インテリジェンス

Dell SecureWorks

4 デルのアプローチは、お客様のセキュリティ戦略とビジネスニーズを合致させます.

デルのセキュリティソリューション全体像

クライアントソリューション（DDP & Wyse）

- 認証
- 暗号化
- 標的型攻撃
- Thinクライアント

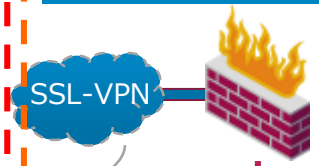
デスクトップPC

ノートPC

Dell Wyse 端末

ネットワークソリューション（SonicWALL）

- 次世代ファイアウォール
- サイバー攻撃防御
- SSL / VPN



無線LAN

DCソリューション（サーバ/ストレージ/バックアップ/管理）

ディレクトリサービス

- ID管理
- アクセス制御
- 監査証跡

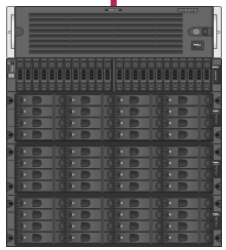
コンバージドサーバ

- 仮想統合化
- 統合管理
- デスクトップ仮想化

データバックアップ

- 重複排除
- レプリケーション
- 暗号化

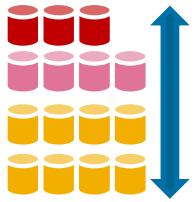
Hypervisor



端末管理（KACE）

- パッチ管理
- 資産管理
- ソフトウェア配布

データ集中化



統合ストレージ

- データ集中化・仮想化
- 階層化/レプリケーション

セキュリティサービス（SecureWorks）

- MSS（マネージド・セキュリティ・サービス）
- CSIRP（Computer Security Incident Response Plan）
- トレーニングサービス
- セキュリティアセスメント
- ログ分析サービス

デルの「マイナンバー」施行に対するお客さまへの取り組み

- マイナンバー法施行における重要課題である、特定個人情報の保護に対して、ITが関連する課題に対してデルのソリューション＆サービスを活用し、包括的にお客さまをご支援いたします。

- 特定個人情報の保護に対する現時点のガイドラインに基づき、民間事業者が最低限実施すべきIT関連対策について、弊社ソリューション＆サービスで対応いたします。

- 具体的には、要求されている以下の項目、
  - A. 基本方針の策定
  - B.運用規定
  - C.組織的安全管理措置
  - D.人的安全措置
  - F.技術的安全管理措置

  に対して、ご支援を提供いたします。（ E.物理的安全管理措置に関しては、弊社のみでの対応は現状行っておりません）

マイナンバー法の概要

- **正式名称:『行政手続における特定の個人を識別するための番号の利用等に関する法律』**
  - 略称: 番号法、マイナンバー法
- **公布日:** 2013年5月31日
- **主旨:** 国民と法人に一意の番号を割り当て、行政手続きを効率的に進めていくため。
- **マイナンバー法の意義:** 国内の行政手続きの基盤とする。法定受託事務（国が自治体に代行を依頼する）であるため、住基ネット（自治事務）のように自治体に選択権はなく、管理が必須となる。
- **マイナンバーの定義:** 正式には個人番号。個人ごとに一意の番号であり、最新の基本4情報（氏名/生年月日/性別/住所）とセットで管理される。
- **マイナンバーの通知:** 国民にはマイナンバーが記載された個人番号カードが2016年1月より交付される。
  - 個人番号カード: マイナンバー、顔写真、氏名、住所、生年月日などが記載される。
- **マイナンバー制度の3機能**
  1. 付番: 個人ごとに一意の番号と基本4情報をセットで管理する
  2. 本人確認: 身元確認とマイナンバーの真正性を証明する
  3. 情報連携: 個別に管理されている様々な国民の情報と連携する
- **マイポータル:** 正式には情報提供等記録開示システム。下記4つの機能を提供予定。
  1. 自己情報へのアクセスログの確認
  2. 各情報保有機関が保有する自己情報を確認
  3. 電子申請を経由する機能（ワンストップサービス）
  4. 行政機関等からのお知らせを表示（プッシュ型サービス）
- **制度の監視:** 第三者委員会である特定個人情報保護委員会が本法制度全般の監視をする。

マイナンバー法の全体像

- **第1章　総則（第1～6条）**
- **第2章　個人番号（第7～16条）**
- **第3章　個人番号カード（第17～18条）**
- **第4章　特定個人情報の提供**
  - 第1節　　特定個人情報の提供の制限等（第19～20条）
  - 第2節　　情報提供ネットワークシステムによる特定個人情報の提供（第21～25条）
- **第5章　特定個人情報の保護**
  - 第1節　　特定個人情報保護評価（第26～28条）
  - 第2節　　行政機関個人情報保護法等の特例等（第29～35条）
- **第6章　特定個人情報保護委員会**
  - 第1節　　組織（第36～49条）
  - 第2節　　業務（第50～56条）
  - 第3節　　雑則（第57条）
- **第7章　法人番号（第58～61条）**
- **第8章　雑則（第62～66条）**
- **第9章　罰則（第67～77条）**
- **附則**

企業実務への影響

- **個人番号関係事務実施者(※1)としての対応**
  - 2015年12月まで: マイナンバー法に関する社員への研修・教育
  - 2016年1月まで: 人事給与・法定調書関連システムの改修
  - 2016年1月から: 社員からのマイナンバー収集および利用開始（税務、社会保障、保険など）

- **個人番号利用事務実施者(※2)としての対応**
  - 2015年12月まで: 特定個人情報保護評価※3およびシステム改修、情報提供ネットワークシステム接続作業
  - 2016年12月まで: 情報提供ネットワークシステムテスト作業
  - 2017年1月から: 情報提供ネットワークシステムとマイポータル運用開始

※1 – マイナンバーを行政手続き目的で内部でのみ利用する組織（行政機関、民間企業などほぼすべて）

※2 – マイナンバーを行政手続き業務のために外部と連携する組織（行政機関、健康保険組合、確定拠出年金法と確定給付企業年金法によって規定された事業主など）

※3 特定個人情報保護評価

- 特定個人情報ファイルを保有するものは個人情報の漏えいその他の事態の発生の危険性および影響に関する評価を自ら実施し、適切に管理するために講ずべき措置を定めた指針を作成し、公表する義務がある。
- 評価作業は、システム開発前（要件定義段階が好ましい）までに実施する必要がある。
- 主な対象リスク: **情報の入手、使用、委託、提供、移転、保管、消去、およびシステム接続におけるリスク**

特定個人情報を取り扱うために民間事業者に求められる安全管理措置

民間事業者はマイナンバーを含む個人情報（以下、特定個人情報）を取り扱うために、特定個人情報保護委員会が発行する「特定個人情報の適正な取扱いに関するガイドライン（事業者編）」に基づき、以下の安全措置を講じる必要があります。
民間企業に求められる「安全管理措置」

A.B.基本方針の策定,運用規定

C.組織的安全管理措置
組織的な体制構築、取扱い規定に基づく運用、情報漏えい等事案に対応する体制整備

D.人的安全措置
事務取扱担当者および全社的な教育・管理強化

E.物理的安全管理措置
管理体制の物理セキュリティ強化、取扱区域の管理、機器および電子媒体の盗難防止

F.技術的安全管理措置
アクセス制御、認証、情報漏えい等の防止、外部からの不正アクセス等防止

対応項目A.B.
基本方針の策定,運用規定

講ずべき安全管理措置の内容			ガイドラインにおける手法の例示	Dellの対応ソリューション	内容
A	–	基本方針の策定	特定個人情報等の適正な取扱いの確保について組織として取り組むための、基本方針を策定	Dell SecureWorks セキュリティ&リスクコンサルティングサービス	マイナンバーに関する特定個人情報保護の 方針・規程の整備サポート サービス
B	–	取扱規程等の策定	特定個人情報等の具体的な取扱いを定める取扱規程等の策定	Dell SecureWorks セキュリティ&リスクコンサルティングサービス	マイナンバーに関する特定個人情報保護の 方針・規程の整備サポート　サービス

対応項目A.B. の基本方針の策定、運用規定については、弊社 Dell SecureWorks が提供するサービス「マイナンバーに関する特定個人情報保護の方針・規程の整備サポート サービス」にて対応いたします。

対応項目C.
組織的安全管理措置

講ずべき安全管理措置の内容			ガイドラインにおける手法の例示	Dellの対応ソリューション	内容
C	–	組織的安全管理措置	事業者は、特定個人情報等の適正な取扱いのために、次に掲げる組織的安全管理措置を講じなければならない。		
C	a	組織体制の整備	安全管理措置を講ずるための組織体制を整備する。 ≪手法の例示≫ ＊ 組織体制として整備する項目は、次に掲げるものが挙げられる。 1・ 事務における責任者の設置及び責任の明確化 2・ 事務取扱担当者の明確化及びその役割の明確化 3・ 事務取扱担当者が取り扱う特定個人情報等の範囲の明確化 4・ 事務取扱担当者が取扱規程等に違反している事実又は兆候を把握した場合の責任者への報告連絡体制 5・ 情報漏えい等事案の発生又は兆候を把握した場合の従業者から責任者等への報告連絡体制 6・ 特定個人情報等を複数の部署で取り扱う場合の各部署の任務分担及び責任の明確化	1,2,3,4,5,6 Dell SecureWorks セキュリティ&リスクコンサルティングサービス	1,2,3,6 は、マイナンバーに関する特定個人情報保護の 方針・規程の整備サポートサービスに包含可能(オプション) 4,5 は、CSIRP(Computer Security Incident Response Plan)策定支援サービスに包含可能
C	b	取扱規程等に基づく運用	取扱規程等に基づく運用状況を確認するため、システムログ又は利用実績を記録する。 ≪手法の例示≫ ＊ 記録する項目としては、次に掲げるものが挙げられる。 1・ 特定個人情報ファイルの利用・出力状況の記録 2・ 書類・媒体等の持出しの記録 3・ 特定個人情報ファイルの削除・廃棄記録 4・ 削除・廃棄を委託した場合、これを証明する記録等 5・ 特定個人情報ファイルを情報システムで取り扱う場合、事務取扱担当者の情報システムの利用状況(ログイン実績、アクセスログ等)の記録	1,5 Dell SecureWorks マネージド セキュリティサービス	1,5 ログ保管サービスにて、Syslogを保管 2,3,4 に関してファイルを特定して記録(デジタル、アナログ両方)するソリューションは未提供
C	c	取扱状況を確認する手段の整備	特定個人情報ファイルの取扱状況を確認するための手段を整備する。 なお、取扱状況を確認するための記録等には、特定個人情報等は記載しない。 ≪手法の例示≫ ＊ 取扱状況を確認するための記録等としては、次に掲げるものが挙げられる。 1・ 特定個人情報ファイルの種類、名称 2・ 責任者、取扱部署 3・ 利用目的 4・ 削除・廃棄状況 5・ アクセス権を有する者	1,2,3,4,5 Dell SecureWorks セキュリティ&リスクコンサルティングサービス	1,2,3,4,5 マイナンバーに関する特定個人情報保護の 方針・規程の整備サポートサービスに包含可能(オプション)
C	d	情報漏えい等事案に対応する体制の整備	情報漏えい等の事案の発生又は兆候を把握した場合に、適切かつ迅速に対応するための体制を整備する。 情報漏えい等の事案が発生した場合、二次被害の防止、類似事案の発生防止等の観点から、事案に応じて、事実関係及び再発防止策等を早急に公表することが重要である。 ≪手法の例示≫ ＊ 情報漏えい等の事案の発生時に、次のような対応を行うことを念頭に、体制を整備することが考えられる。 1・ 事実関係の調査及び原因の究明 2・ 影響を受ける可能性のある本人への連絡 3・ 委員会及び主務大臣等への報告 4・ 再発防止策の検討及び決定 5・ 事実関係及び再発防止策等の公表	1,2,3,4,5 Dell SecureWorks セキュリティ&リスクコンサルティングサービス	1,2,3,4,5 CSIRP(Computer Security Incident Response Plan)策定支援サービスに体制整備のドキュメントを包含可能
C	e	取扱状況の把握及び安全管理措置の見直し	特定個人情報等の取扱状況を把握し、安全管理措置の評価、見直し及び改善に取り組む。 ≪手法の例示≫ 1＊ 特定個人情報等の取扱状況について、定期的に自ら行う点検又は他部署等による監査を実施する。 2＊ 外部の主体による他の監査活動と合わせて、監査を実施することも考えられる。	1,2 Dell SecureWorks セキュリティ&リスクコンサルティングサービス	1,2 セキュリティ安全管理措置アセスメントサービス

対応項目D.
人的安全管理措置

講ずべき安全管理措置の内容			ガイドラインにおける手法の例示	Dellの対応ソリューション	内容
D	–	人的安全管理措置	事業者は、特定個人情報等の適正な取扱いのために、次に掲げる人的安全管理措置を講じなければならない。		
D	a	事務取扱担当者の監督	事業者は、特定個人情報等が取扱規程等に基づき適正に取り扱われるよう、事務取扱担当者に対して必要かつ適切な監督を行う。	未対応	非IT項目
D	b	事務取扱担当者の教育	事業者は、事務取扱担当者に、特定個人情報等の適正な取扱いを周知徹底するとともに適切な教育を行う。 ≪手法の例示≫ 1＊ 特定個人情報等の取扱いに関する留意事項等について、従業者に定期的な研修等を行う。 2＊ 特定個人情報等についての秘密保持に関する事項を就業規則等に盛り込むことが考えられる。	1,2 Dell SecureWorks セキュリティ&リスクコンサルティングサービス	1,は、セキュリティ啓発トレーニングに包含可能（オプション） 2,は、マイナンバーに関する特定個人情報保護の 方針・規程の整備サポートサービスに包含可能（オプション）

対応項目E.
物理的安全管理措置

		講ずべき安全管理措置の内容	ガイドラインにおける手法の例示	Dellの対応ソリューション	内容
E	–	物理的安全管理措置	事業者は、特定個人情報等の適正な取扱いのために、次に掲げる物理的安全管理措置を講じなければならない。		
E	a	特定個人情報等を取り扱う区域の管理	特定個人情報等の情報漏えい等を防止するために、特定個人情報ファイルを取り扱う情報システムを管理する区域（以下「管理区域」という。）及び特定個人情報等を取り扱う事務を実施する区域（以下「取扱区域」という。）を明確にし、物理的な安全管理措置を講ずる。 ≪手法の例示≫ 1＊ 管理区域に関する物理的安全管理措置としては、入退室管理及び管理区域へ持ち込む機器等の制限等が考えられる。 2＊ 入退室管理方法としては、ICカード、ナンバーキー等による入退室管理システムの設置等が考えられる。 3＊ 取扱区域に関する物理的安全管理措置としては、壁又は間仕切り等の設置及び座席配置の工夫等が考えられる。	未対応	非IT項目
E	b	機器及び電子媒体等の盗難等の防止	管理区域及び取扱区域における特定個人情報等を取り扱う機器、電子媒体及び書類等の盗難又は紛失等を防止するために、物理的な安全管理措置を講ずる。 ≪手法の例示≫ 1＊ 特定個人情報等を取り扱う機器、電子媒体又は書類等を、施錠できるキャビネット・書庫等に保管する。 2＊ 特定個人情報ファイルを取り扱う情報システムが機器のみで運用されている場合は、セキュリティワイヤー等により固定すること等が考えられる。	未対応	非IT項目
E	c	電子媒体等を持ち出す場合の漏えい等の防止	特定個人情報等が記録された電子媒体又は書類等を持ち出す場合、容易に個人番号が判明しない措置の実施、追跡可能な移送手段の利用等、安全な方策を講ずる。 「持出し」とは、特定個人情報等を、管理区域又は取扱区域の外へ移動させることをいい、事業所内での移動等であっても、紛失・盗難等に留意する必要がある。 ≪手法の例示≫ 1＊ 特定個人情報等が記録された電子媒体を安全に持ち出す方法としては、持出しデータの暗号化、パスワードによる保護、施錠できる搬送容器の使用等が考えられる。ただし、行政機関等に法定調書等をデータで提出するに当たっては、行政機関等が指定する提出方法に従う。 2＊ 特定個人情報等が記載された書類等を安全に持ち出す方法としては、封緘、目隠しシールの貼付を行うこと等が考えられる。	1, Dell DDP|Encription	1,の電子媒体持ち出しに対して、様々な形式の媒体に暗号化を実施することが可能 2,は非IT項目
E	d	個人番号の削除、機器及び電子媒体等の廃棄	個人番号関係事務又は個人番号利用事務を行う必要がなくなった場合で、所管法令等において定められている保存期間等を経過した場合には、個人番号をできるだけ速やかに復元できない手段で削除又は廃棄する。 個人番号若しくは特定個人情報ファイルを削除した場合、又は電子媒体等を廃棄した場合には、削除又は廃棄した記録を保存する。また、これらの作業を委託する場合には、委託先が確実に削除又は廃棄したことについて、証明書等により確認する。 ≪手法の例示≫ 1＊ 特定個人情報等が記載された書類等を廃棄する場合、焼却又は溶解等の復元不可能な手段を採用する。 2＊ 特定個人情報等が記録された機器及び電子媒体等を廃棄する場合、専用のデータ削除ソフトウェアの利用又は物理的な破壊等により、復元不可能な手段を採用する。 3＊ 特定個人情報ファイル中の個人番号又は一部の特定個人情報等を削除する場合、容易に復元できない手段を採用する。 4＊ 特定個人情報等を取り扱う情報システムにおいては、保存期間経過後における個人番号の削除を前提とした情報システムを構築する。 5＊ 個人番号が記載された書類等については、保存期間経過後における廃棄を前提とした手続を定める。	未対応	1,5 は非IT項目 2,3,4 はソリューション未対応

対応項目F.
技術的安全管理措置

		講ずべき安全管理措置の内容	ガイドラインにおける手法の例示	Dellの対応ソリューション	内容
F	–	技術的安全管理措置	事業者は、特定個人情報等の適正な取扱いのために、次に掲げる技術的安全管理措置を講じなければならない。		
F	a	アクセス制御	情報システムを使用して個人番号関係事務又は個人番号利用事務を行う場合、事務取扱担当者及び当該事務で取り扱う特定個人情報ファイルの範囲を限定するために、適切なアクセス制御を行う。 ≪手法の例示≫ ＊ アクセス制御を行う方法としては、次に掲げるものが挙げられる。 1・ 個人番号と紐付けてアクセスできる情報の範囲をアクセス制御により限定する。 2・ 特定個人情報ファイルを取り扱う情報システムを、アクセス制御により限定する。 3・ ユーザーIDに付与するアクセス権により、特定個人情報ファイルを取り扱う情報システムを使用できる者を事務取扱担当者に限定する	Active Directory等	弊社グローバルサービスによる導入支援サービスにて、Active Directory 等の機能を活用したアクセス制御環境の構築支援を提供
F	b	アクセス者の識別と認証	特定個人情報等を取り扱う情報システムは、事務取扱担当者が正当なアクセス権を有する者であることを、識別した結果に基づき認証する。 ≪手法の例示≫ ＊ 事務取扱担当者の識別方法としては、ユーザーID、パスワード、磁気・ICカード等が考えられる。	DDP|ST	指紋およびFelicaの多要素認証で対応
F	c	外部からの不正アクセス等の防止	情報システムを外部からの不正アクセス又は不正ソフトウェアから保護する仕組みを導入し、適切に運用する。 ≪手法の例示≫ 1＊ 情報システムと外部ネットワークとの接続箇所に、ファイアウォール等を設置し、不正アクセスを遮断する。 2＊ 情報システム及び機器にセキュリティ対策ソフトウェア等（ウイルス対策ソフトウェア等）を導入する。 3＊ 導入したセキュリティ対策ソフトウェア等により、入出力データにおける不正ソフトウェアの有無を確認する。 4＊ 機器やソフトウェア等に標準装備されている自動更新機能等の活用により、ソフトウェア等を最新状態とする。 5＊ ログ等の分析を定期的に行い、不正アクセス等を検知する。	1, Dell SonicWALL 4, Dell KACE 3,5 Dell SecureWorks マネージド セキュリティサービス	1,は、Dell SonicWALL 次世代ファイアウォールによる保護を提供 2, ソリューション未対応 3, Dell SecureWorks マネージド セキュリティサービスによる監視で不正ソフトウェアの有無を確認 4, Dell KACE による、様々なソフトウェア更新の自動適用 5, Dell SecureWorks マネージド セキュリティサービスによるログの常時監視もしくは、コンサルティングサービスによる定期分析
F	D	情報漏えい等の防止	特定個人情報等をインターネット等により外部に送信する場合、通信経路における情報漏えい等を防止するための措置を講ずる。 ≪手法の例示≫ 1＊ 通信経路における情報漏えい等の防止策としては、通信経路の暗号化等が考えられる。 2＊ 情報システム内に保存されている特定個人情報等の情報漏えい等の防止策としては、データの暗号化又はパスワードによる保護等が考えられる。	1, Dell SonicWALL 2, Dell DDP|Encription	1, Dell SonicWALL のSSL/VPN 機能により、通信経路の暗号化 2, Dell DDP| Encription によるデータの暗号化

Dell SecureWorks マイナンバーに関する特定個人情報保護の方針・規程の整備サポート サービス

当該対応項目	
A	基本方針の策定
B	取扱規程等の策定
C-a 1,2,3,6	組織的安全管理措置 / 組織体制の整備
C-c 1,2,3,4,5	組織的安全管理措置 / 取扱状況を確認する手段の整備
D-b 2	人的安全管理措置 / 事務取扱担当者の教育

プロジェクトメソドロジー

- デルのメソドロジーをご紹介致します。

情報収集と要件確認

- プロジェクトキックオフ
- スケジュール調整
- 既存の個人情報保護方針・規程文書など、関連資料の収集
- マイナンバー収集・利用環境の確認
- IT環境の把握

ドラフト作成とレビュー

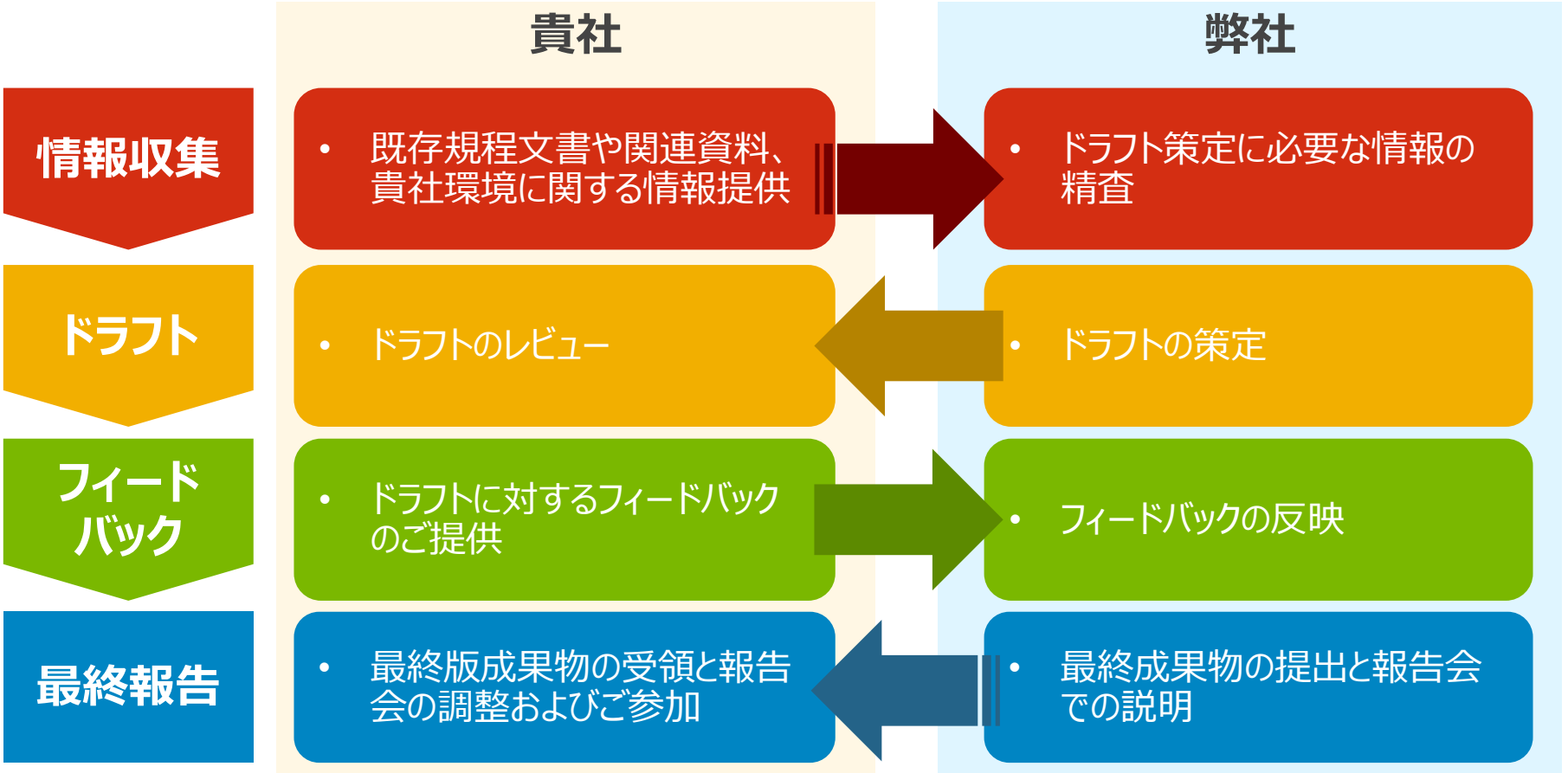
- 情報収集結果に基づく、マイナンバー情報保護方針・規程のドラフト文書作成
- 既存方針・規程との整合性チェックなどに関するレビューと貴社からのフィードバック

最終成果物の提示

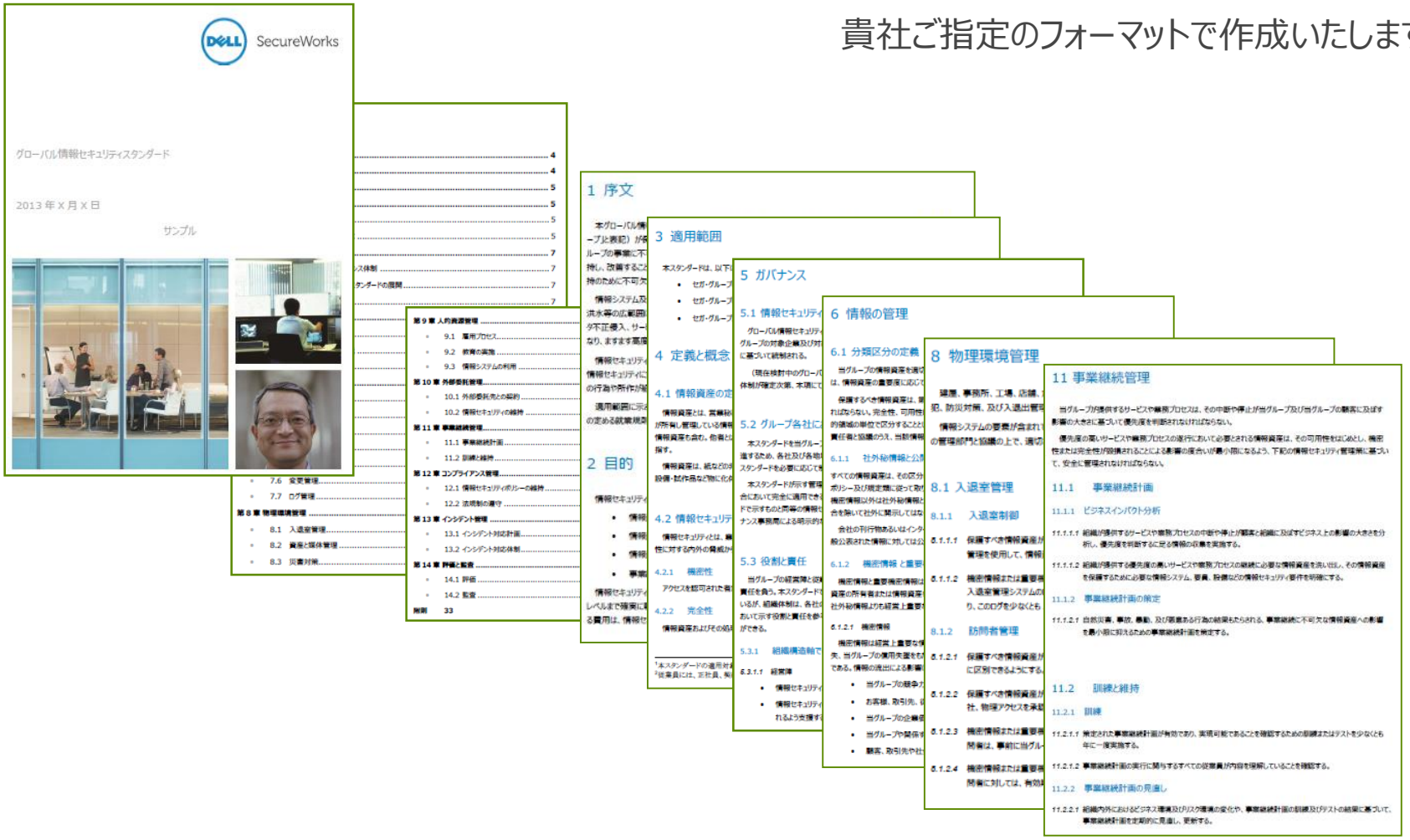
- 貴社からのフィードバック内容を反映した最終成果物の提示
- 成果物内容に関する解説（必要な場合）

方針・規程策定作業の段取り

方針・規程案のドラフト策定にあたっては、貴社からの情報・意見提供やドラフトに対するレビューとフィードバックを必要に応じて反復しながら、以下の工程に沿って推進いたします



成果物のサンプルイメージ



貴社ご指定のフォーマットで作成いたします。

想定タスクと参考スケジュール

想定されるタスクとご参考スケジュールは以下の通りです。

フェーズ	タスク	M1	M2
情報収集/要件確認	プロジェクトキックオフ		
	事前情報収集		
ドラフト作成/レビュー	ドラフト作成		
	レビューとフィードバック		
最終成果物提示	最終成果物作成		
	成果物内容の解説		

サービス要件について

- **サービス内容**
  - マイナンバーに関する特定個人情報保護の方針・規程の整備サポート
- **対象範囲**
  - 貴社国内におけるマイナンバー収集・利用環境
- **オンサイトワークショップ（ヒアリングおよびレビューディスカッション）**
  - 回数：合計4回まで1回あたり2時間まで（弊社営業日9:00-18:00内で実施）
  - 場所：貴社本社オフィス
- **想定成果物**
  - マイナンバーに関する特定個人情報保護の方針・規程
    - 性質: マイナンバー法に基づく特定個人情報保護のための管理施策を纏めたもの
    - 容量: 方針 – 3～5ページ程度、規程 – 10～20ページ程度
  - フォーマット: 貴社フォーマット（指定がない場合は弊社所定フォーマット）
  - 言語: 日本語
- **報告会**
  - 貴社本社オフィスにて1回実施 (日本語/弊社営業日9:00-18:00のうち、2時間程度)
- **備考**
  - 文書化に必要な情報や随時発生する確認事項について、貴社より速やかに情報提供またはご回答いただくことを前提としています。
  - 上記に記載されていない文書の作成、作業などは一切含みません。

プロジェクトチームの責任範囲について

貴社
プロジェクトチーム

- 社内関係者へのプロジェクト主旨説明や協力依頼、およびスケジュール調整をお願い致します。
- 既存文書や関連資料などドキュメントのご提供をお願い致します。
- 打ち合わせに必要な場所や設備のご提供をお願い致します。
- 弊社作成成果物に対するレビューとフィードバックの実施をお願い致します。

Dell SecureWorks
プロジェクトチーム

- 経験とノウハウに基づくアドバイスの提供致します。
- サービス要件に基づく文書作成作業を行います。
- 成果物の作成および貴社フィードバックに基づく最終版の作成を致します。
- 成果物の品質チェックを致します。
- プロジェクトマネジメントを行います。



Dell SecureWorks
マネージド セキュリティ サービス

当該対応項目		
C-b 1,5	組織的安全管理措置	取扱規程等に基づく運用
F-c 3,5	技術的安全管理措置	外部からの不正アクセス等の防止

セキュリティ脅威をグローバル規模で可視化

75+ か国	4,500+ 社のお客様	1,000+ 人の専門家	33万+ デバイスの監視	5 SOC	1,100億+ イベント監視/日	4,100+ イベント報告/日

SecureWorks

Positioned as a Leader in the Gartner "Magic Quadrant for Managed Security Services, Worldwide" by Kelly Kavanagh, December 30, 2014

Figure 1. Magic Quadrant for Managed Security Services, Worldwide

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Dell SecureWorks.

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

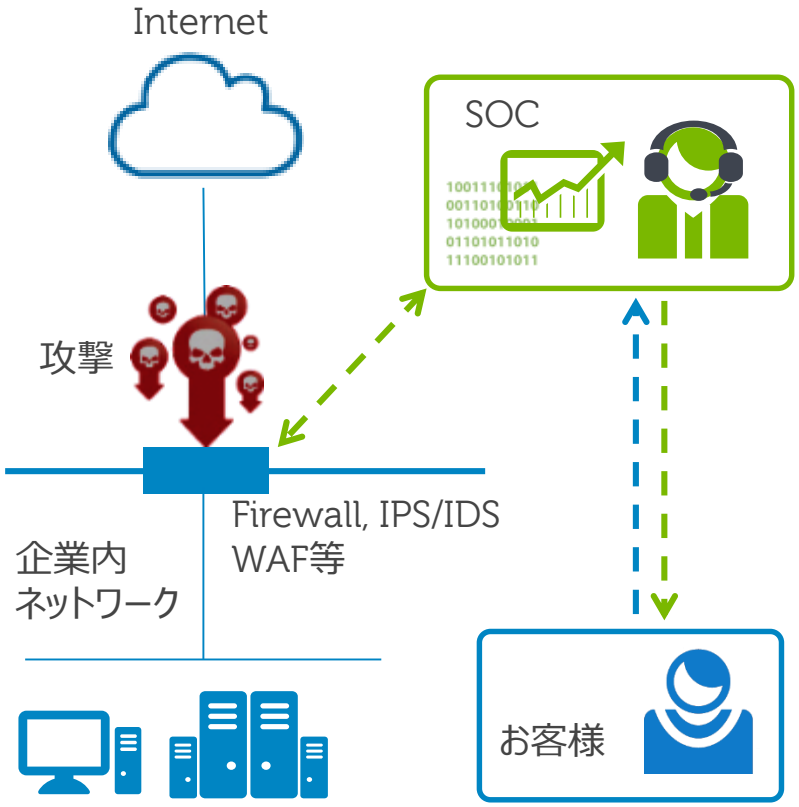
Source: Gartner (December 2014)

SecureWorks

膨大な監視ポイントと攻撃者の監視を通じて、グローバルの可視化でお客様を守り管理コストを削減する

マネージド セキュリティ サービス(MSS)

昨今、企業・組織に対して「サイバー攻撃」が多発しています。この対策として、セキュリティ対策システムの監視・運用を業務委託するサービスです。
Security Operation Center (SOC)がお客様のネットワークセキュリティ機器に対する不正アクセスの監視・運用・インシデント対応などを行います。



お客様にとっての利点

① 既知の脅威の通過を防ぐ

- 24時間365日、通信ログを専門家の目で確認し異常を検知する
- 関連するログを相関的に分析し、インシデントとして結論を導く

② 「未知の脅威」や亜種にいち早く対応する

- アンチウイルスをはじめとするセキュリティ製品のアップデート頻度不足をカバー
- ゼロデイ攻撃など、パッチ対策が後手に回るような攻撃に対応

③ セキュリティ事故の早期発見

- 他社も含めた世界中の脅威動向などから、鮮度の高いセキュリティ関連情報を継続的に入手する
- 事故が発生しても、早期発見による拡散、および被害の拡大を防止する

膨大な監視ポイントと攻撃者の監視を通じて、グローバルの可視化でお客様を守り管理コストを削減する

マネージド セキュリティ サービス(MSS)

セキュリティデバイスの監視および管理

– Firewall、IDS/IPS、アンチウイルス、次世代型Firewall、WebアプリケーションFirewallなどの常時監視と運用管理を実施致します。。

–プロアクティブなセキュリティ対策を提供致します。

セキュリティ分析・相関分析

– 脆弱性管理、セキュリティイベント管理、ログ管理、SOCアナリストによる分析などを行います。

※注
- MSSでサポートしている「主要な」ベンダー・モデルを記載しております。
- 機能によっては現状サポートできていないものもございます。
- 詳細および最新のサポート状況については個別にお問い合わせいただくようお願い致します。

主要サポート機器一覧

分類	ベンダー	モデル
Firewall	Check Point Cisco Juniper McAfee Sidewinder Nokia	Firewall-1 Firefly, Power-1, IPxx, 2xxx, 4xxx, 12xxx PIX Netscreen, SSG Secure Firewall IP XXX
IDS/IPS	Cisco IBM ISS McAfee Sourcefire(NG) Tipping Point Dell	IDS/IPS Proventia-G, GX I, M 3Dxxxx iSensor
Malware Protection	FireEye	WebMPS, EmailMPS

分類	ベンダー	モデル
NGFW/UTM	Cisco Check Point IBM ISS Juniper Dell Fortinet PaloAlto Networks	ASA UTM Proventia Mxx, MXxxxx SRX SonicWALL SuperMassive, NSA, TZ Fortigate PA
WAF	Citrix f5 Imperva	NetScaler Application Security Manager SecureSphere
Endpoint (PC)	Bit9	Carbon Black

Dell SecureWorks MSS は、
お客様環境で**複雑化する多層防御**に対し、**確実な監視、管理を提供**いたします。
日々の**管理業務を軽減**し、問題発生時の**解決時間を短縮**することが可能です。
また、Dell SecureWorks の**CTUリサーチ**からの攻撃者情報を利用することで、
事前の防御対策等、**ゼロデイ攻撃の対策**をご支援します。

Dell SecureWorks
CSIRP(Computer Security Incident Response Plan)策定支援サービス

当該対応項目		
C-a 4,5	組織的安全管理措置	組織体制の整備
C-d 1,2,3,4,5	組織的安全管理措置	情報漏えい等事案に対応する体制の整備

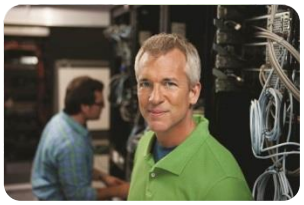
Dell SecureWorks
セキュリティ安全管理措置アセスメントサービス

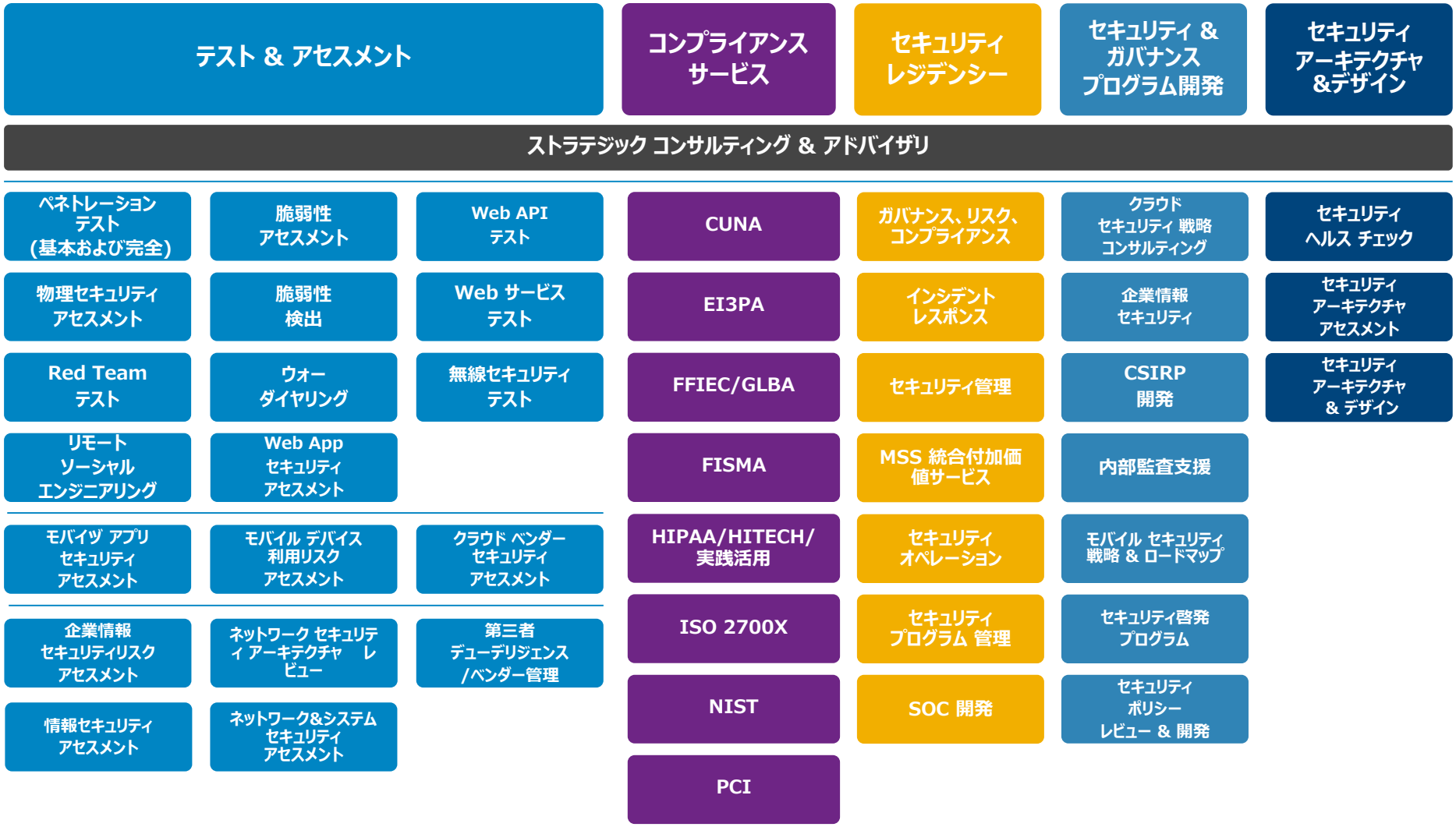
当該対応項目		
C-e	組織的安全管理措置	取扱状況の把握及び安全管理措置の見直し

Dell SecureWorks
ログ分析サービス

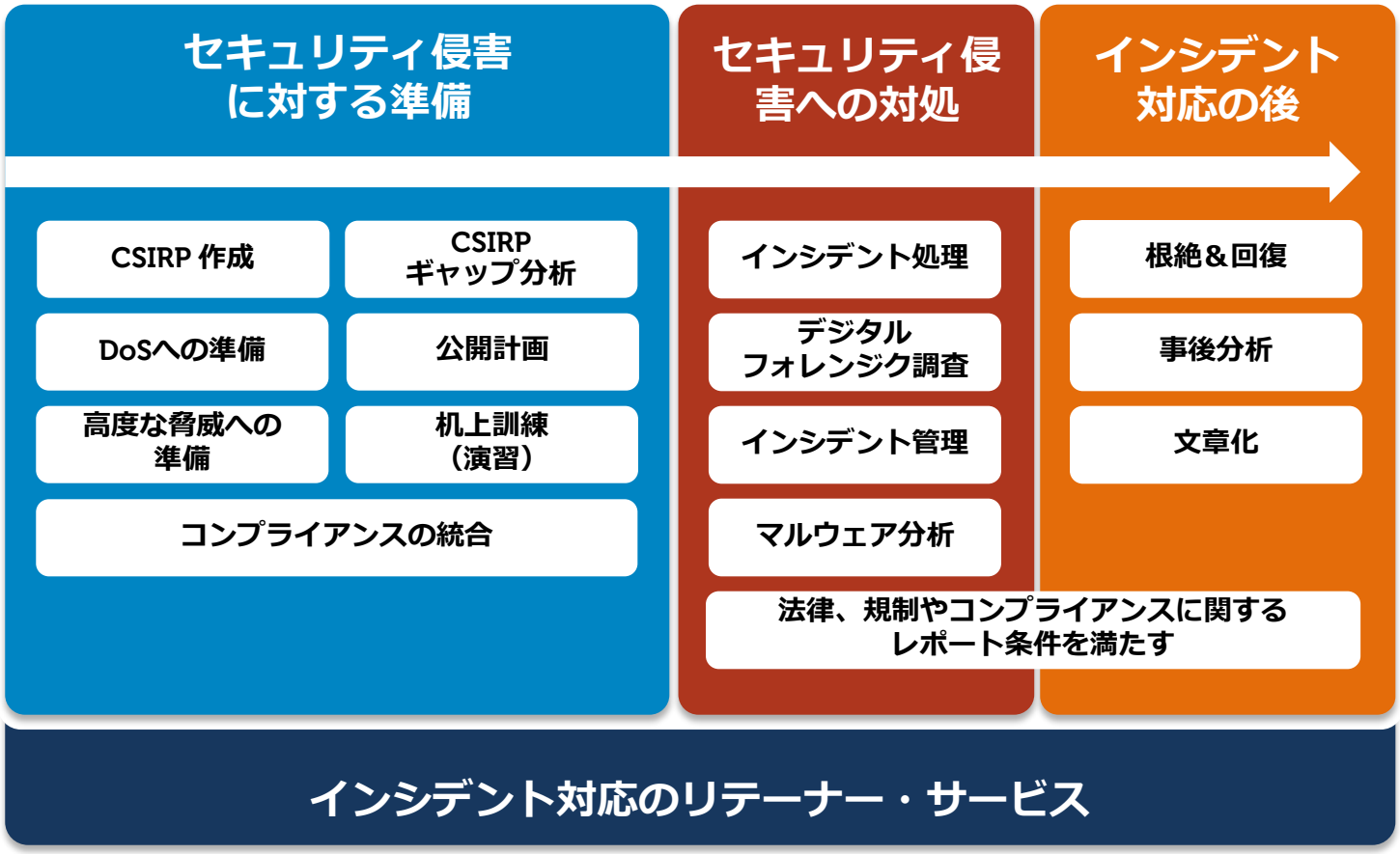
当該対応項目		
F-c 5	技術的安全管理措置	外部からの不正アクセス等の防止

セキュリティ & リスク コンサルティング

	柔軟な アプローチ	明確な 方法論	選択肢に対す るビジョン	技術に関する 深い専門知識	業務に関する 知識
コア資産					
サービス	テストと評価	コンプライアンス & 認定サービス	セキュリティ レジデンシィ サービス	セキュリティ & ガバナンス プログラム開発	
ビジネス 価値	効率性と 有効性の向上	現状の判断、 選択肢の明確化	コンプライアンス への セキュリティ対策	社会インフラの 保護	プログラムの 練度を向上


テスト & アセスメント
コンプライアンス サービス
セキュリティ レジデンシー
セキュリティ & ガバナンス プログラム開発
セキュリティ アーキテクチャ &デザイン
ストラテジック コンサルティング & アドバイザリ
ペネトレーション テスト (基本および完全)
脆弱性 アセスメント
Web API テスト
物理セキュリティ アセスメント
脆弱性 検出
Web サービス テスト
Red Team テスト
ウォー ダイヤリング
無線セキュリティ テスト
リモート ソーシャル エンジニアリング
Web App セキュリティ アセスメント
モバイツ アプリ セキュリティ アセスメント
モバイル デバイス 利用リスク アセスメント
クラウド ベンダー セキュリティ アセスメント
企業情報 セキュリティリスク アセスメント
ネットワーク セキュリティ アーキテクチャ レビュー
第三者 デューデリジェンス /ベンダー管理
情報セキュリティ アセスメント
ネットワーク&システム セキュリティ アセスメント
CUNA
ガバナンス、リスク、コンプライアンス
クラウド セキュリティ 戦略 コンサルティング
セキュリティ ヘルス チェック
EI3PA
インシデント レスポンス
企業情報 セキュリティ
セキュリティ アーキテクチャ アセスメント
FFIEC/GLBA
セキュリティ管理
CSIRP 開発
セキュリティ アーキテクチャ & デザイン
FISMA
MSS 統合付加価値サービス
内部監査支援
HIPAA/HITECH/ 実践活用
セキュリティ オペレーション
モバイル セキュリティ 戦略 & ロードマップ
ISO 2700X
セキュリティ プログラム 管理
セキュリティ啓発 プログラム
NIST
SOC 開発
セキュリティ ポリシー レビュー & 開発
PCI
セキュリティ 啓発 トレーニング ソリューション (CISO Office)
オンデマンド セキュリティ トレーニング
セキュリティ 啓発 ニーズ アセスメント
セキュリティ 啓発プログラム開発
カスタム セキュリティ トレーニング サービス
フィッシング 模擬訓練
セキュリティ管理 啓発プログラム

インシデント レスポンスに関する
全てを網羅するサービスをご提供いたします



Dell SecureWorks
セキュリティ啓発トレーニング サービス

当該対応項目		
D-b 1	人的安全管理措置	事務取扱担当者の教育

オンデマンドのセキュリティトレーニング
クラウドベースのラーニングポータル

Dell DDP|ST Security Tools

当該対応項目		
F-b	技術的安全管理措置	アクセス者の識別と認証

Dell Data Protection | Security Tools

高度な認証機能によりデータを守ります。

Dell Data Protection | Security Toolsはドライブ暗号化とローカルで管理する高度な認証を実施する設計をされています。 **フィッシング詐欺、スピアフィッシング、ソーシャルエンジニアリング、ウイルス、APT攻撃などのウイルスやパスワードリセット**に備え保護します。LatitudeノートPC, Precisionワークステーション、OptiPlexデスクトップのシステムにおいてコストをかけずにお客様に提供可能で、Dellのオプションの指紋認証や、スマートカードリーダー、非接触型指紋認証リーダーなどのハードウェア認証オプションと共に利用が可能です。

ノートPC /
デスクトップPC

パスワード入力
指紋認証リーダー
スマートカードリーダー

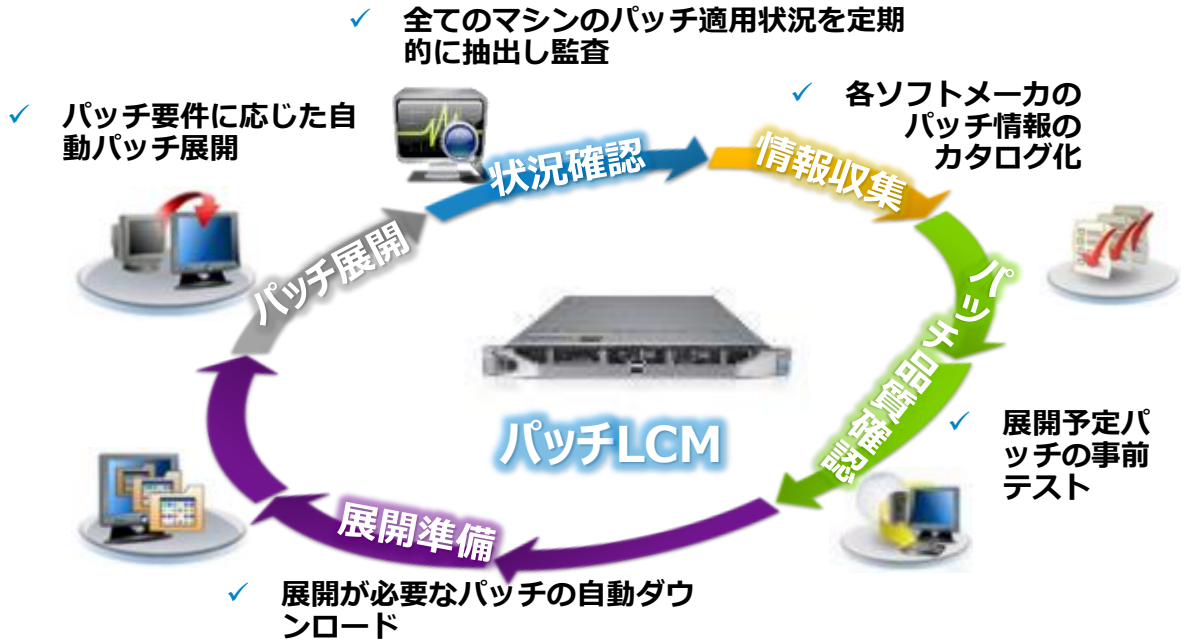
ControlVault
™

Dell KACE K1000

当該対応項目		
F-c 4	技術的安全管理措置	外部からの不正アクセス等の防止

エンドポイント脆弱性対策について

- **ソフトウェアを最新に保つことで、外部からの不正アクセス等を防止します。**
- **パッチマネジメントに必要な膨大な工数を自動化により大幅削減します。**
  - サイバー攻撃対象の頻度が高いアプリケーションを幅広くサポートします。
  - ポリシに応じ、アップデート要件を柔軟に設定可能です。
  - パッチダウンロードから展開まですべてを自動で実現します。



対応リポジトリ

Supported OS

メーカー	Platform
Apple	Mac OS
Microsoft	Windows OS

Supported Applications

メーカー	製品
Microsoft	全般
Apple	全般
Adobe	全般
Google	Chrome
Mozilla	Firefox
Oracle	JRE
VMware	全般
Citrix Systems	Reciver
WinZip	WinZip
McAfee	Antivirus
Sophos	Antivirus
Symantec	Antivirus
Trend Micro	Antivirus
Novell	Novell Client
Real Networks	RealPlayer
Lumension	All products

リポジトリは、デイリーで更新されます。対応製品は、その時々の状況により更新します。

Dell SonicWALL Next Gen Firewall

当該対応項目		
F-c 1	技術的安全管理措置	外部からの不正アクセス等の防止

サイバー攻撃・脅威　防御ソリューション

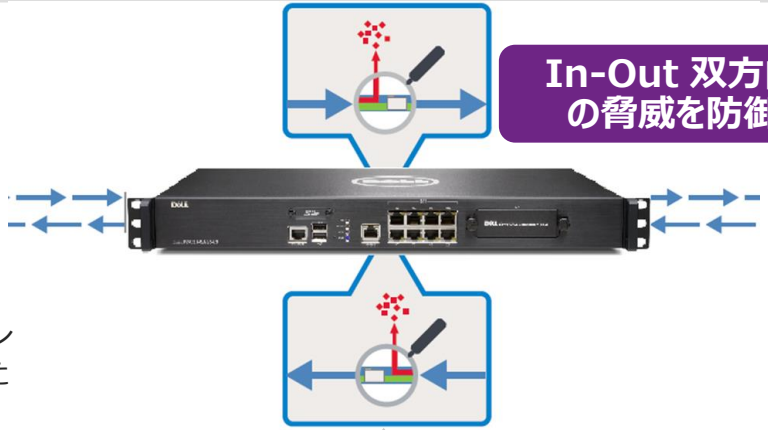
多層防御を1台の次世代ファイアウォールで対策致します。

ファイアウォール | VPN | ゲートウェイ アンチウイルス | アンチ スパイウェア | IPS/IDS | コンテンツ フィルタリング | アプリケーションの可視化/コントロール

● 多層型アプローチにより、内部ネットワークやリモートサイト等のあらゆる場所にアンチウィルス保護が適用され、すべてのファイルを監視。また、キーロガーやバックドア等の侵入や送出をブロックします。

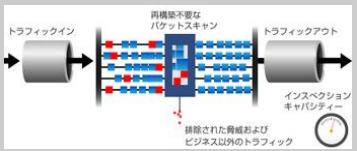
● ディープパケットインスペクションにより、アプリケーション層を狙ったExploit攻撃を検知・防御します。

● インスタント メッセンジャーおよびP2Pトラフィックのアプリケーション制御 （その他の潜在的なセキュリティリスクを削減）します。



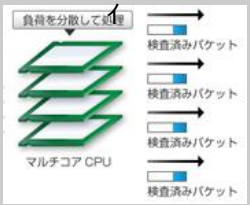
【セキュリティOn】

RFDPI特許技術
(再構築なしのDPI)



【ハイパフォーマンス】

マルチコアを徹底活用
RFDPIで実現するｽｹｰﾗﾋﾞﾘﾃｨ



● GRID NetWork上にあるクラウドベースのシグネチャデータベースへ問い合わせることで、Dell SonicWALL内部のシグネチャを拡張し、一千万以上のマルウェアに対応します。

● 第三社評価機関から『次世代ﾌｧｲｱｳｫｰﾙ』部門ならびに「IPS(侵入検知)」において”Recommended(推奨)”の高い評価を受けています。

NSS Labs

● 国内外数多くの受賞歴がございます。

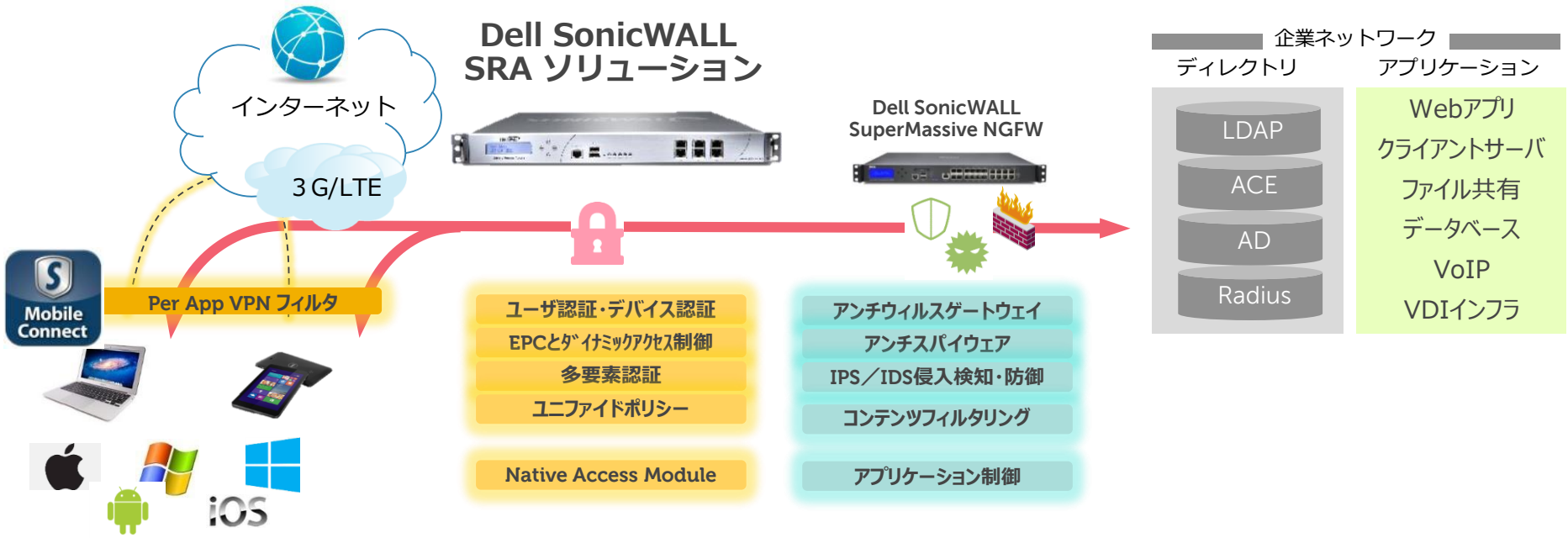
BEST OF SHOW AWARD INTEROP 特別賞

Dell SonicWALL SSL/VPN

当該対応項目		
F-d 1	技術的安全管理措置	情報漏えい等の防止

セキュアリモートアクセス

BYODやワークスタイル改革、災害対策を支えるセキュアリモートアクセスです。



Detect (検知)
エンドポイントコントロール (EPC)とﾀﾞｲﾅﾐｯｸｱｸｾｽｺﾝﾄﾛｰﾙ

接続前にデバイス検査し、認定ﾃﾞﾊﾞｲｽの可否、ｱﾌﾟﾘｹｰｼｮﾝの有無、ﾊﾞｰｼﾞｮﾝﾁｪｯｸなど詳細を認識します。EPCとUnified Policyによりﾀﾞｲﾅﾐｯｸｱｸｾｽｺﾝﾄﾛｰﾙを提供します。

Protect(防御)
Unified Policy

設計時も運用時も、容易な操作性を提供します。
ｵﾌﾞｼﾞｪｸﾄﾍﾞｰｽのﾎﾟﾘｼｰ管理が、ﾕｰｻﾞｰ、ｸﾞﾙｰﾌﾟ、ﾘｿｰｽ、ﾙｰﾙのｱｸｾｽｺﾝﾄﾛｰﾙﾎﾟﾘｼｰ設定を容易にします

Connect（接続）
Smart Access & Smart Tunneling

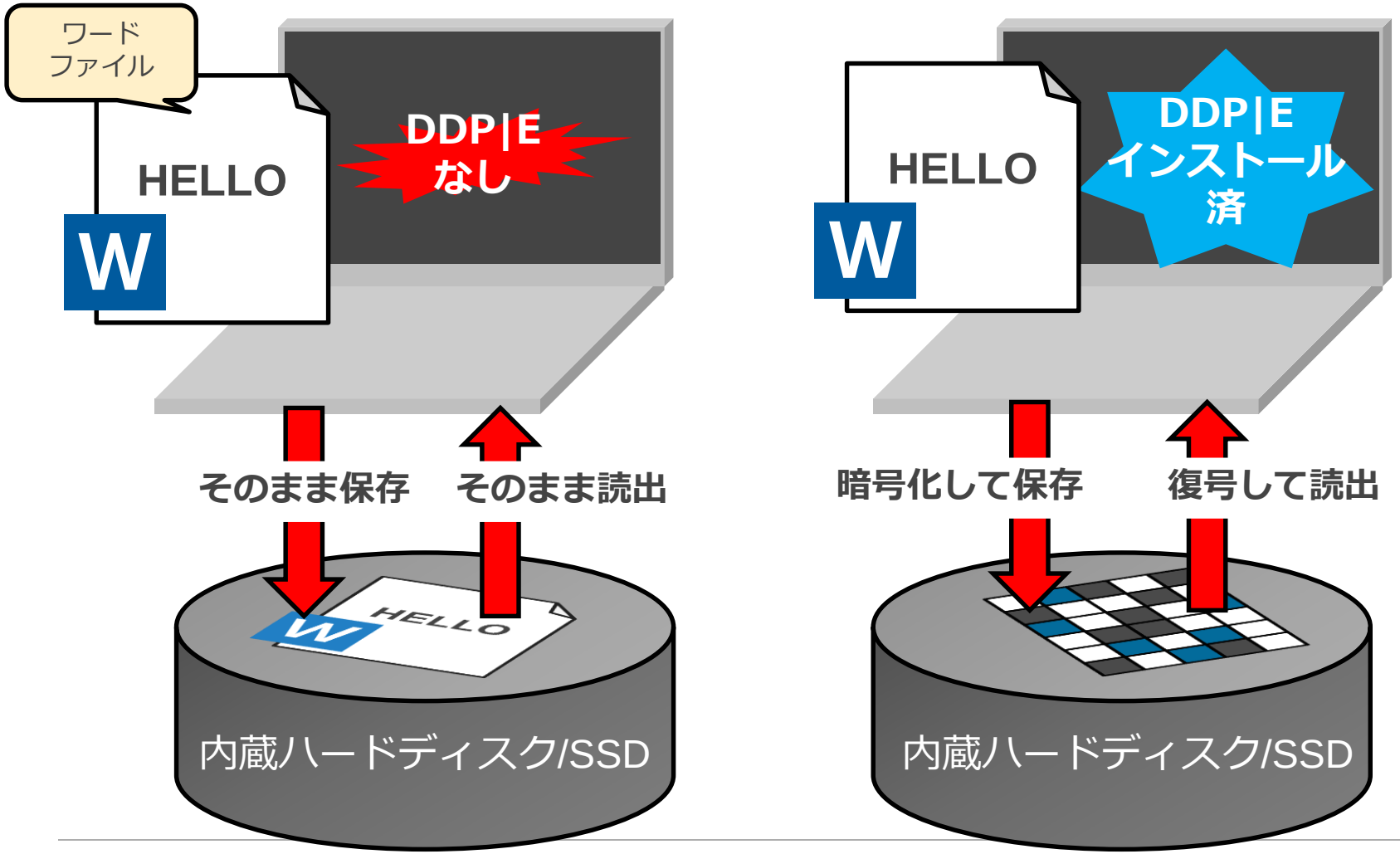
様々なﾃﾞﾊﾞｲｽやﾕｰｻﾞｰに合わせたｱｸｾｽ先を表示します。
ｾｷｭｱなﾕｰｻﾞｰと判別された時はｽﾏｰﾄﾄﾝﾈﾘﾝｸﾞにより完全な社内環境を提供します。

Dell DDP|E Encryption

当該対応項目		
E-c 1	物理的安全管理措置	電子媒体等を持ち出す場合の漏えい等の防止
F-d 2	技術的安全管理措置	情報漏えい等の防止

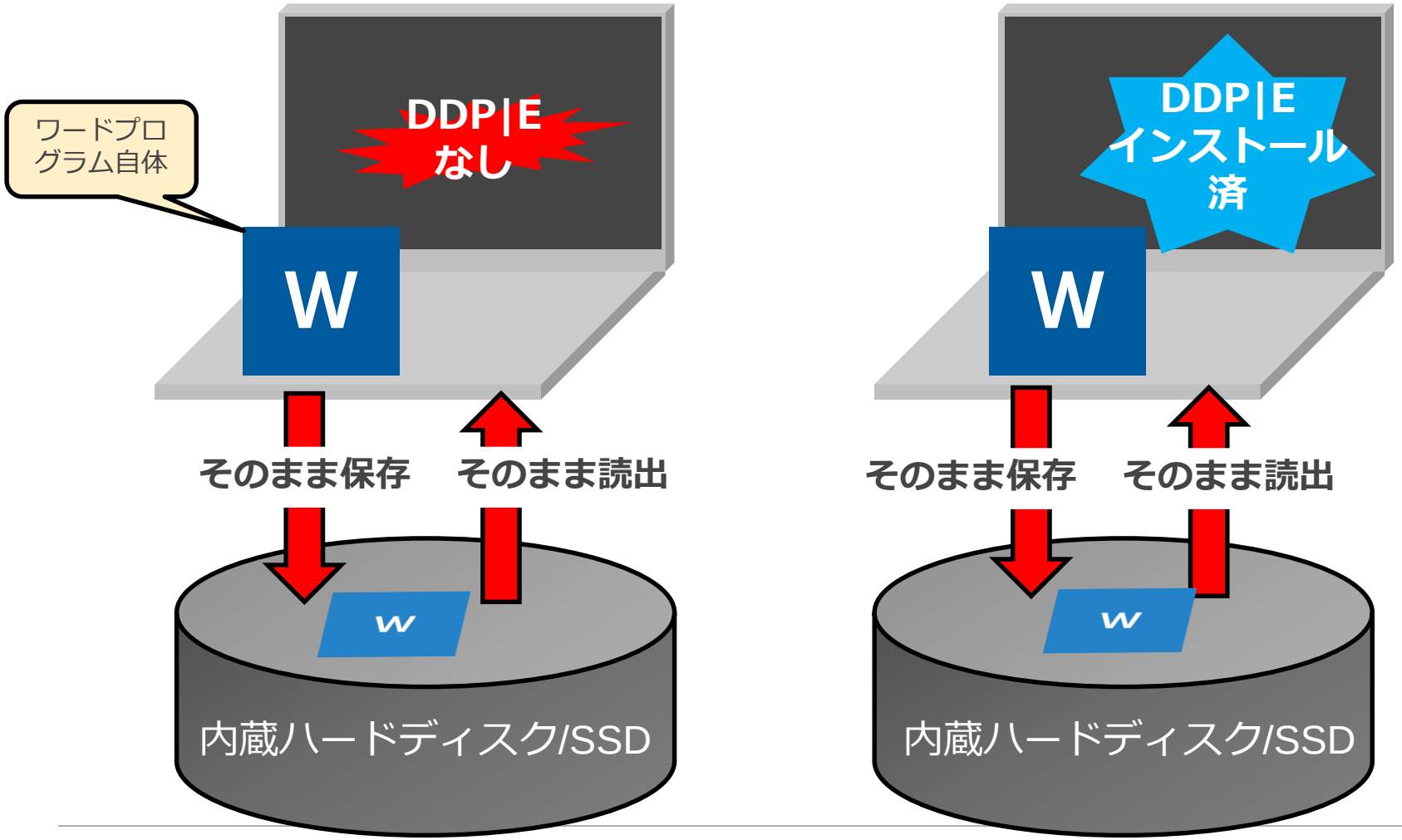
DDP|Eってなに？

ファイルをハードディスクに保存する際に暗号化する技術です。**ユーザが存在を意識することはほぼゼロです。**※1、※2

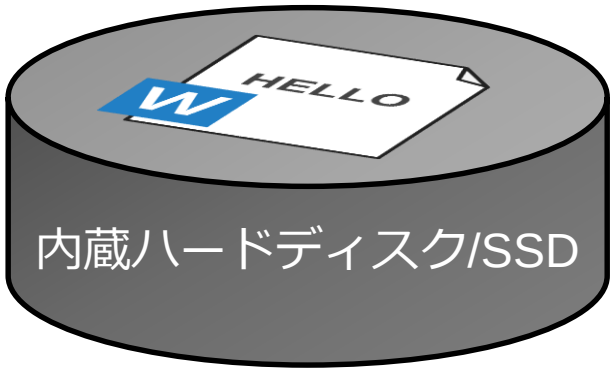


※1 USBメモリ利用時に、USBメモリに暗号化して保存する設定あり（PWDによる復号）
※2 DELL社員のPCは、全てDDP|E（Enterprise）インストール済です。意識したことありますか？
※3 シングルサインオンで機能します。

DDP|Eってなに？
プログラムはそのまま保存（インストール）されます。



DDP|Eのメリット：PCの紛失・盗難や廃棄時、または内部犯行によりハードディスクから直接データを抜かれる危険性を大幅に減少致します。



紛失・盗難時、廃棄時、もしくは内部犯行により、HDDから直接情報を抜かれる可能性アリ

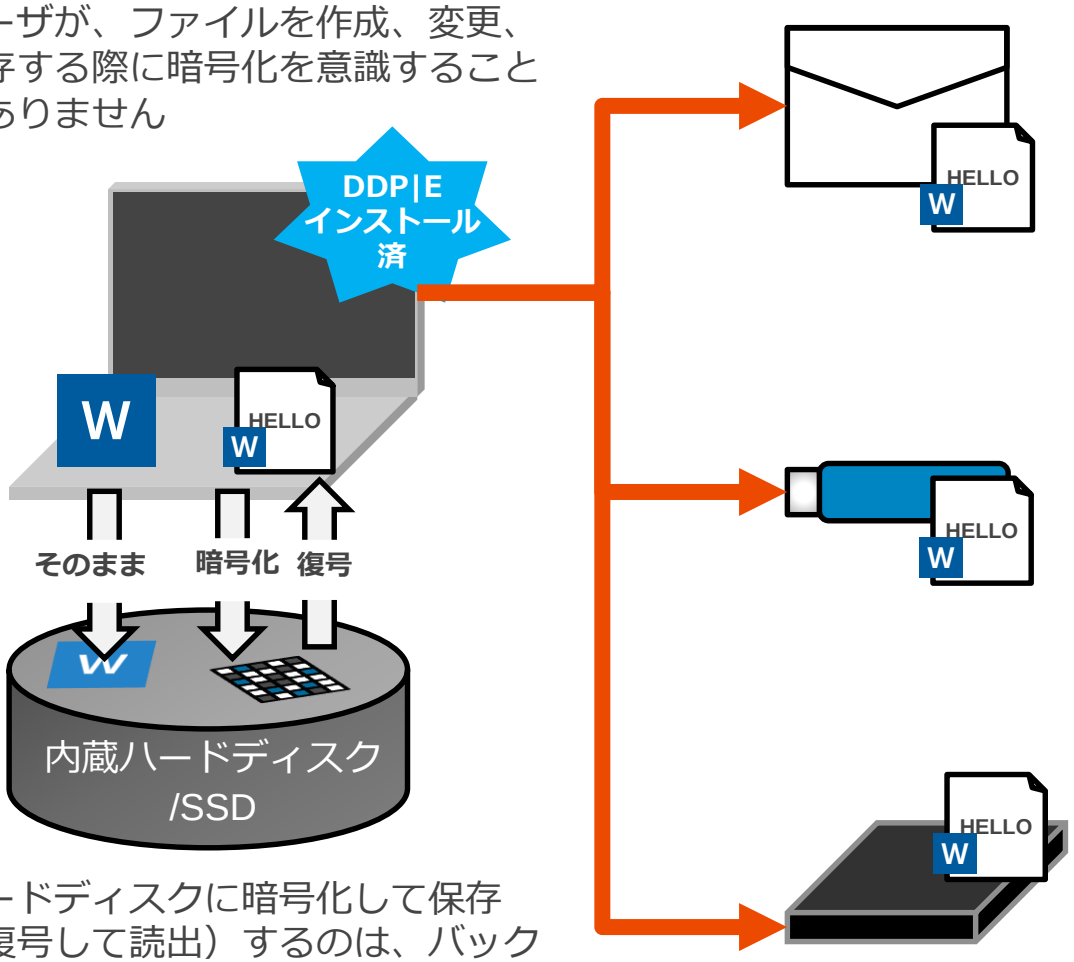
紛失・盗難時、廃棄時、もしくは内部犯行時も、HDD上のファイルが暗号化されているため情報が抜かれる可能性は極めて低い

ご存知でしたか？

「ファイルの消去」では、HDD上のデータを消すことは出来ません！
HDDから消去（＝読み取れなくする）ためには、特殊な工具等で物理的にHDDを破壊するか、特殊なソフトウェアでHDDを別の情報で完全に上書きするような作業が必要です！！

ユーザがDDP|Eの存在を意識することは原則ない。セキュリティポリシーで「保護されていないUSBのアクセスをブロック」を選択した場合、ファイルを自動暗号化致します。

ユーザが、ファイルを作成、変更、保存する際に暗号化を意識することはありません



ハードディスクに暗号化して保存（復号して読出）するのは、バックグラウンドサービスによる自動実行です。

メールへの添付等では、DDP|Eがファイルを復号化し、暗号化されていないファイルを添付する。必要に応じて、パスワードを設定した、自己解凍型の実行形式ファイルを作成し、添付することが可能です。

USBメディアに保存する際の暗号化/非暗号化ポリシーを初期設定で設定可能。その設定をした場合のみ、USBを初めて使用する時にパスワードを設定することで、ファイルは暗号化されます。USBを共有する場合には初期設定でロードされたDDP|Eのプログラムにて復号を行います。

SCSI接続外付HDDは内蔵ハードディスクと同様に固定ドライブとして保護され、暗号化・復号化は内蔵HDDと同様に自動で実行されます。(このHDDを他のPC（たとえDDPEがインストールされていても）に接続しても読み取れません)

ありがとうございました。