

『UTM（統合脅威管理システム）』 ご提案資料

株式会社野村総合研究所
社会情報システム事業部

2026年5月 改版



2022年4月に施行された改正個人情報保護法によって、個人情報の漏えい等が発生した場合に、個人情報保護委員会や被害者本人への通知が義務化されました

- これまで、個人情報の漏えいなどが発生した際における**個人情報保護委員会への報告や被害者本人への通知**は、義務ではありませんでした。しかし、2022年4月に施行される改正個人情報保護法においてこれが**義務化され、法定刑も引き上げられ**ました。そのため、セキュリティ対策の重要性がより一層増しています。

1. 改正法における漏えい等報告・本人通知の概要

新設された条文

- 漏えい等が発生し、**個人の権利利益を害するおそれ大きい場合に、委員会への報告・本人への通知を義務化**（改正法第22条の2）。
- 対象となる事態、委員会への報告・本人への通知の方法等については、委員会規則で定めることとしている。

改正後の個人情報の保護に関する法律（平成15年法律第57号）

（漏えい等の報告等）

第22条の2 個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失、毀損その他の個人データの安全の確保に係る事態であって個人の権利利益を害するおそれ大きいものとして個人情報保護委員会規則で定めるものが生じたときは、個人情報保護委員会規則で定めるところにより、当該事態が生じた旨を個人情報保護委員会に報告しなければならない。ただし、当該個人情報取扱事業者が、他の個人情報取扱事業者から当該個人データの取扱いの全部又は一部の委託を受けた場合であって、個人情報保護委員会規則で定めるところにより、当該事態が生じた旨を当該他の個人情報取扱事業者に通知したときは、この限りでない。

2 前項に規定する場合には、個人情報取扱事業者（同項ただし書の規定による通知をした者を除く。）は、本人に対し、個人情報保護委員会規則で定めるところにより、当該事態が生じた旨を通知しなければならない。ただし、本人への通知が困難な場合であって、本人の権利利益を保護するため必要に代わるべき措置をとるときは、この限りでない。

・漏えい等報告の趣旨は、「委員会が事態を早急に把握し必要な措置を講じることができるようにすること」

・本人通知の趣旨は、「通知を受けた本人が漏えい等の事態を認識することで、その権利利益を保護するための措置を講じられるようにすること」

個人情報保護委員会「規制の事前評価書」より抜粋

2017年5月に施行された個人情報保護改正によって、全てのシルバー人材センターが個人情報保護法の適用対象となっております

【2017年5月30日施行：個人情報保護法改正の要旨】

- ① パーソナルデータの利活用を目的とした、個人情報の定義の明確化と手続き面の整備
- ② 不正な目的での第三者への提供、盗用に対する罰則規定の追加
- ③ **個人情報保護法の適用対象をすべての事業者に拡大**

すべての事業者が「個人情報取扱事業者」となり、個人情報保護法の適用を受けます。

● 改正のポイント ●

1. 個人情報保護委員会の新設

個人情報取扱事業者に対する監督権限を各分野の主務大臣から委員会に一元化。

2. 個人情報の定義の明確化

- ① 利活用に資するグレーゾーン解消のため、個人情報の定義に身体的特徴等が対象となることを明確化。
- ② 要配慮個人情報（本人の人種、信条、病歴など本人に対する不当な差別又は偏見が生じる可能性のある個人情報）の取得については、原則として本人同意を得ることを義務化。

3. 個人情報の有用性を確保（利活用）するための整備

匿名加工情報（特定の個人を識別することができないよう個人情報を加工した情報）の利活用の規定を新設。

4. いわゆる名簿屋対策

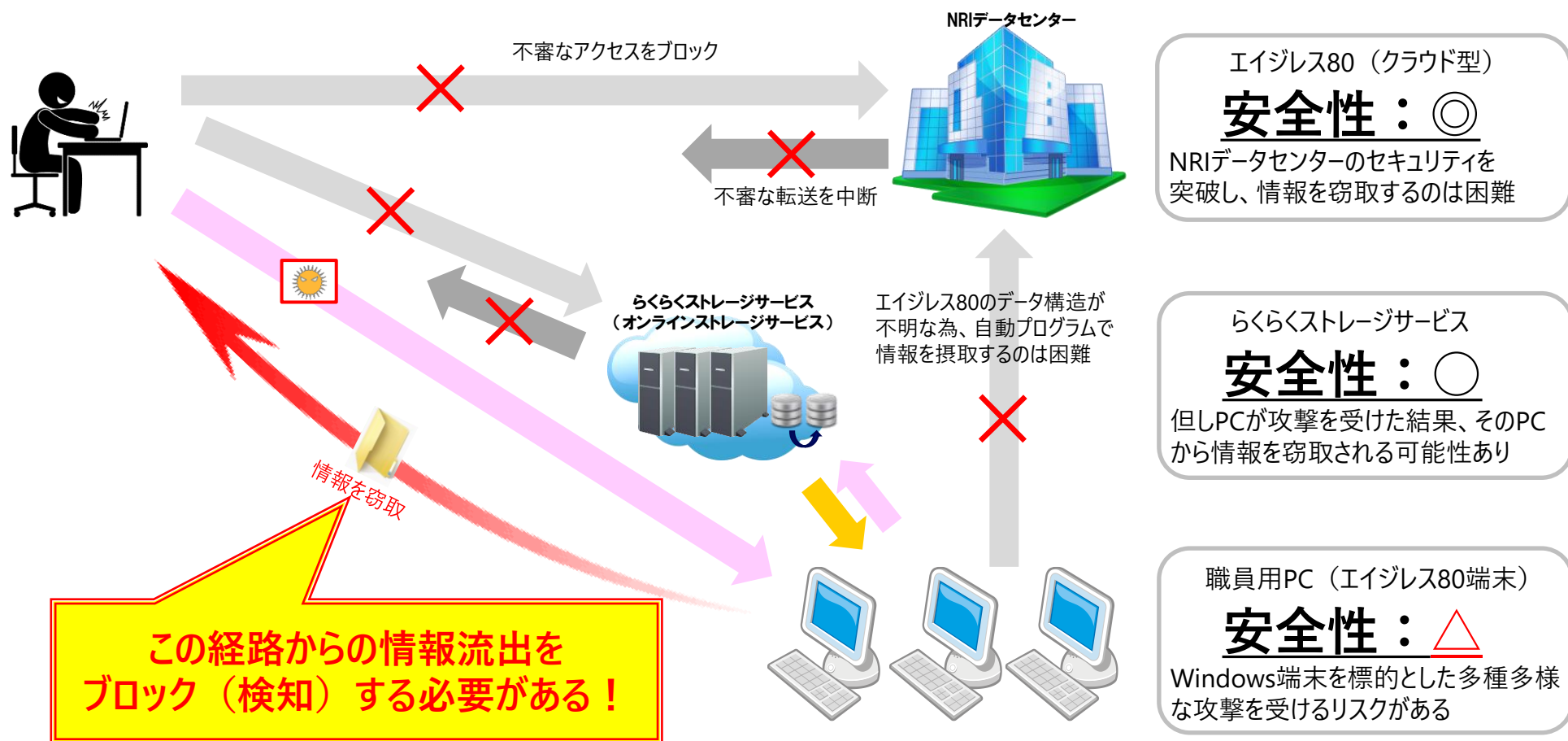
- ① 個人データの第三者提供に係る確認記録作成等を義務化。（第三者から個人データの提供を受ける際、提供者の氏名、個人データの取得経緯を確認した上、その内容の記録を作成し、一定期間保存することを義務付け、第三者に個人データを提供した際も、提供年月日や提供先の氏名等の記録を作成・保存することを義務付ける。）
- ② 個人情報データベース等を不正な利益を図る目的で第三者に提供し、又は盗用する行為を「個人情報データベース提供罪」として処罰の対象とする。

5. その他

- ① 取り扱う個人情報の数が5000以下である事業者を規制の対象外とする制度を廃止。
- ② オプトアウト（※）規定を利用する個人情報取扱事業者は所要事項を委員会に届け出ることを義務化し、委員会はその内容を公表。（※本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止する場合、本人の同意を得ることなく第三者に個人データを提供することができる。）
- ③ 外国にある第三者への個人データの提供の制限、個人情報保護法の国外適用、個人情報保護委員会による外国執行当局への情報提供に係る規定を新設。

情報漏えいはPC端末内に保存された情報の流出から発生するケースが多く、どう対策を行うかが重要となります

【サイバー攻撃に対するセキュリティ強度について】



組織内の意識改革に加え、セキュリティ機器の導入による対策が有効です。

① 事務局内の意識改革によるリスク低減

● ITリテラシーの周知・徹底

- 怪しげなWebサイト・URLにアクセスしない
- 不審なメールは開封しない ←サービス業としての側面を持つ為、現実問題として徹底は難しい

● 情報リテラシーの周知・徹底

- 不用意に重要な情報を残さない（どうしても保管が必要な場合はらくストに保存）
- パスワードの厳格な運用を徹底する
- 複数の担当者によるIDの使い回しを行わない

② セキュリティ製品導入によるリスク低減

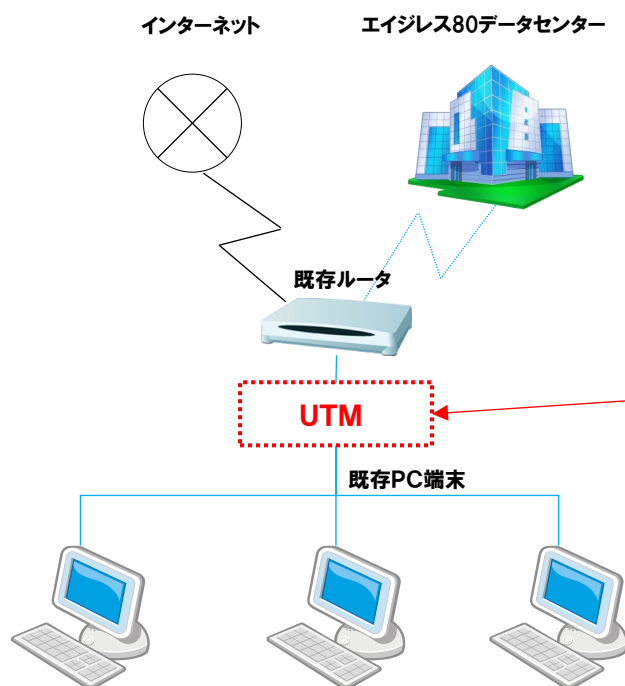
- 端末にセキュリティ対策を施していない → **ウイルス対策ソフト**（導入率：約80％）
- 端末内に共有フォルダを作成している → **らくらくストレージサービス**（導入率：約30％）
- マイナンバー対応や個人情報保護法改正を受け、個人情報管理に一層の注意を払う必要がある。通信の監視・制御を行い、未然に被害を防ぐための対策を行いたい。

→ **UTM(統合脅威管理システム)**

個人情報取扱事業者の「安全管理措置」の一つとしても、U T Mの導入が推奨されています。

- U T Mの導入は、個人情報取扱事業者に求められている「技術的安全管理措置」の一つの手法として推奨されています。

P C 端末からのデータ流出を防ぐ対策の一つとして、ぜひ導入をご検討下さい。



【第20条 安全管理措置の実施】

個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又は毀損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。

【技術的安全管理措置】

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》

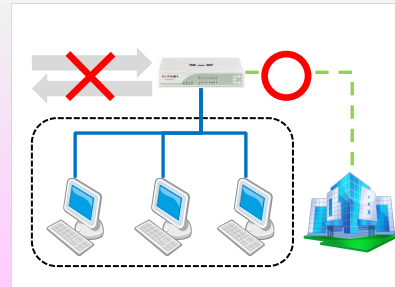
- * 情報システムと外部ネットワークとの接続箇所に、ファイアウォール等を設置し、不正アクセスを遮断する。
- * 情報システム及び機器にセキュリティ対策ソフトウェア等（ウイルス対策ソフトウェア等）を導入する。
- * 導入したセキュリティ対策ソフトウェア等により、入出力データにおける不正ソフトウェアの有無を確認する。
- * 機器やソフトウェア等に標準装備されている自動更新機能等の活用により、ソフトウェア等を最新状態とする。
- * ログ等の分析を定期的に行い、不正アクセス等を検知する。

平成26年12月11日 個人情報保護委員会「特定個人情報に関する安全管理措置（事業者編）」より抜粋

UTMの主要な機能

① 不正侵入の検知/防御

- ・不正な動きを検知しトラフィックを制御。不正な侵入の検知および防御を行う。
- ・正常な通信に擬態している脅威も検知することが可能。



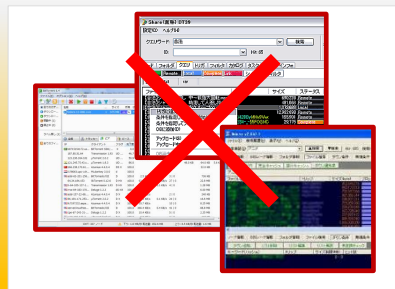
② Webコンテンツフィルタリング（不正サイトへのアクセス制限）

- ・海外サイトや違法サイトなど、業務上不必要な情報かつ脅威を受けやすい場所へのアクセス制限を実施。（NRIによる推奨設定でご提供を行います）



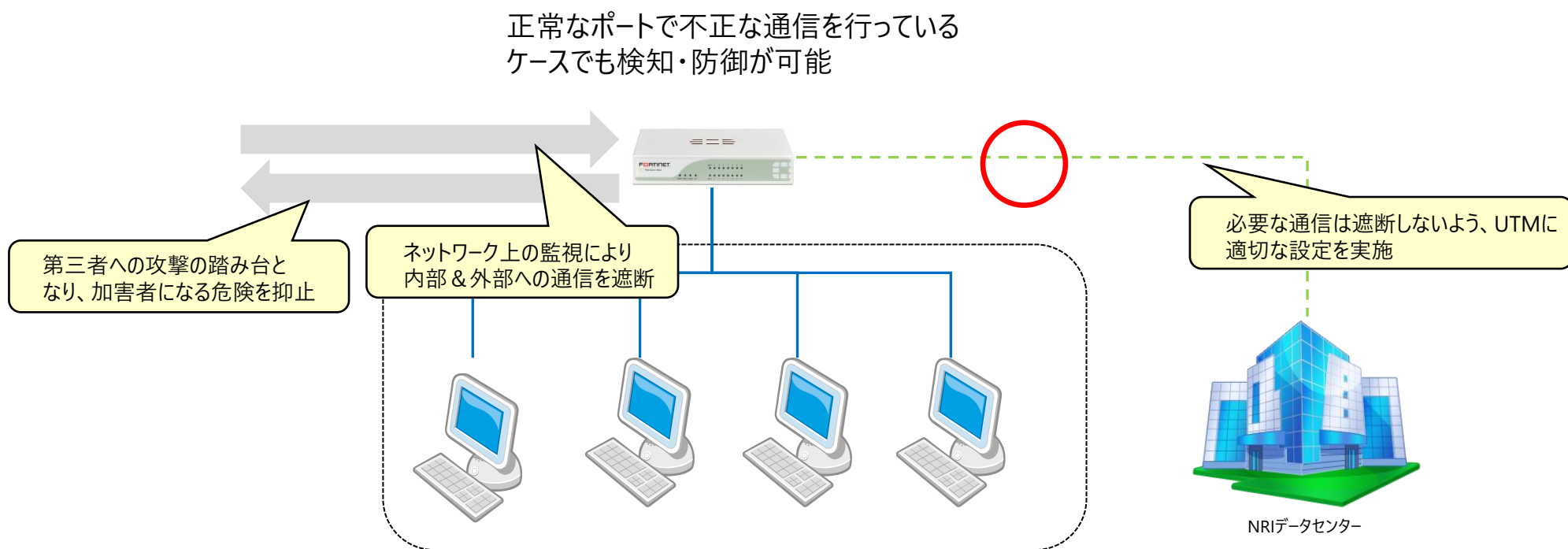
③ 情報漏えい対策

- ・P2Pソフト（Winny、Share等）への接続を禁止。
- ・業務情報の漏えいリスクを軽減。重要な情報が世界中に流出する事態を未然に防ぐ。



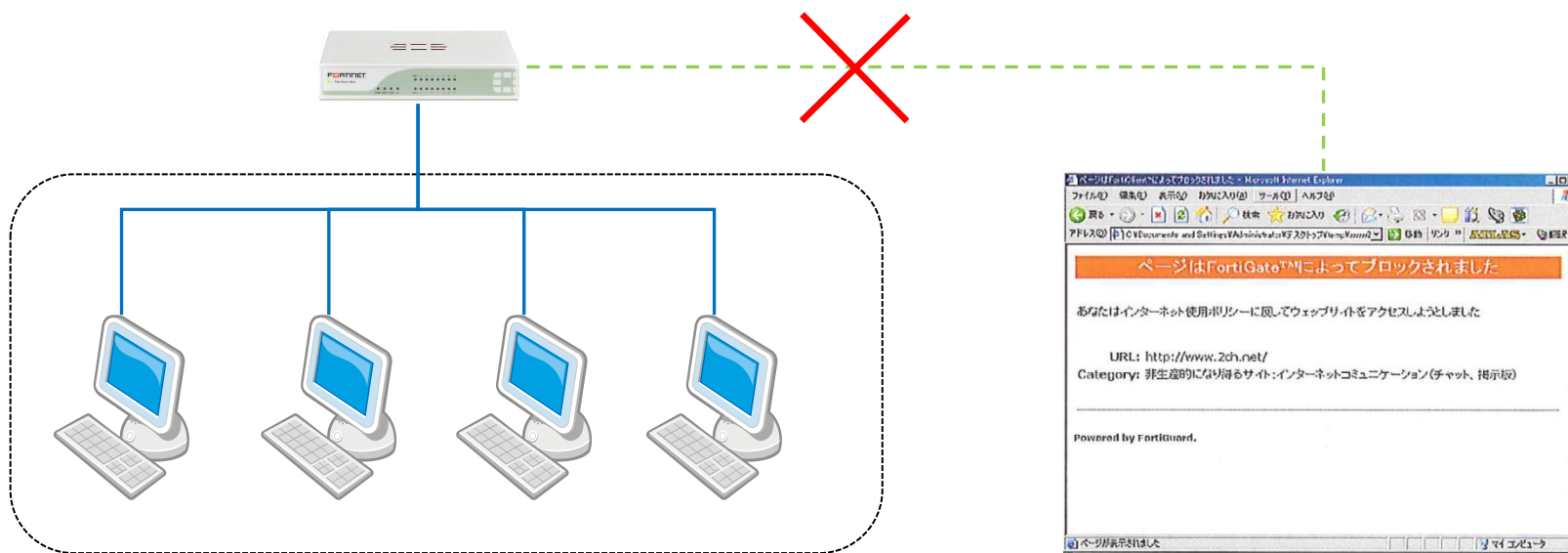
① 不正侵入の検知/防御

- 従来のポート番号レベル、送信元アドレスでのフィルタリングでは防ぎきれない通信に対応
- 不正トラフィックを制御し、組織への被害や第三者への攻撃の踏み台となることを事前に抑止



② Webコンテンツフィルタリング機能

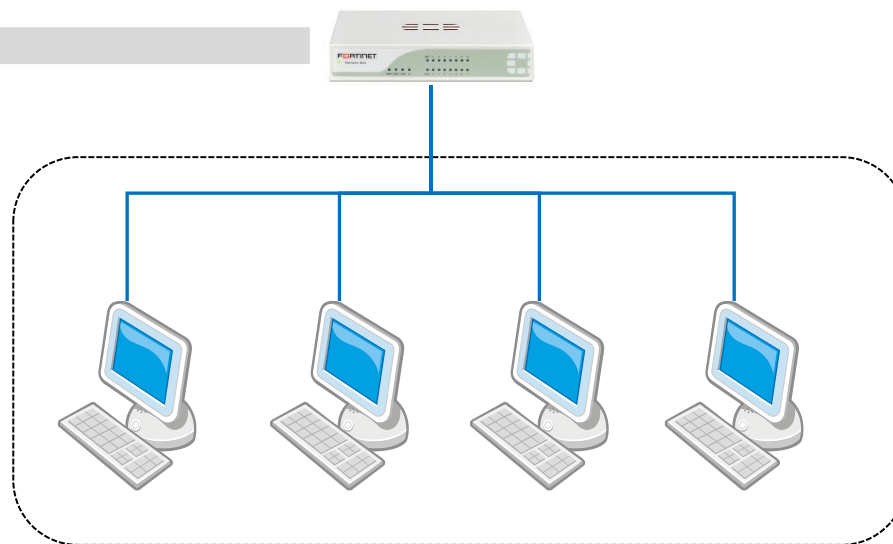
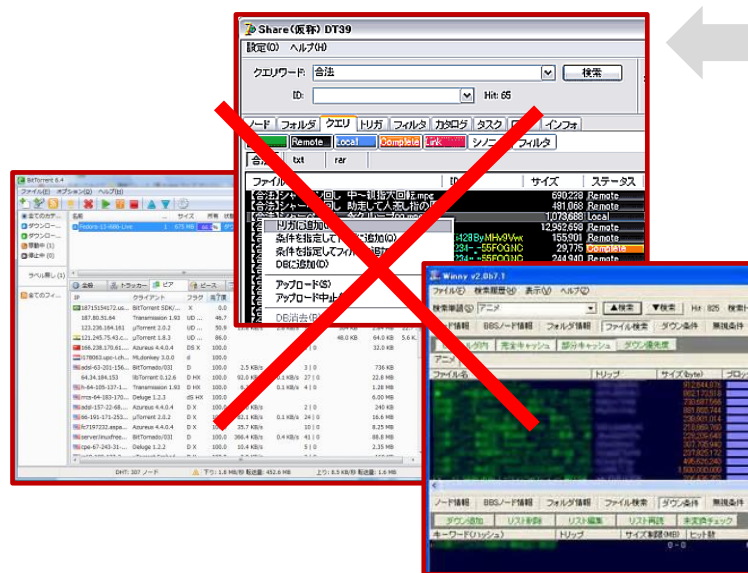
- 業務上不要な（有害な）Webサイトの閲覧を禁止し、業務効率の低下や犯罪に巻き込まれるリスクを低減
- 単純なホワイトリスト・ブラックリストだけではなく、定義されたカテゴリ毎に許可・禁止などのフィルタリング設定が可能なので、新しく解説されたWebサイトにも対応



※Webコンテンツフィルタリング設定は、NRIによる推奨設定でのご提供となります。
個別のWebサイトに関する閲覧可否を希望される場合は、マニュアルをご参照の上センター様にて設定をお願い致します。

③ 情報漏えい対策

- 企業内部情報の流出事故の原因となることの多いP2Pソフト（Winny、Shareなど）への接続を禁止
- 組織の社会的評価を損ね、閉鎖へと追い込みかねない事態を未然に防止



『UTM（統合脅威管理システム）』の特徴

【UTM(統合管理システム)の特徴】

- 世界中のセキュリティ研究センターによる、24時間365日の監視・運用体制を実現
- 刻々変化する最新の脅威を検知しながら迅速に対応し、脅威が蔓延する前に最新のシグネチャを配信

統合脅威管理システム/次世代ファイアウォール
『FortiGate』



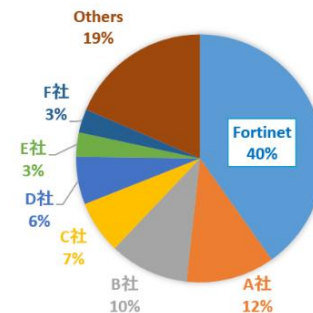
【NRIによる、安心のサポート体制】

- エイジレス80や、ウイルス対策ソフト（SEP）の定義ファイル更新など、シルバー人材センターの利用環境に適したチューニングを施しています。エイジレス80の通信・プログラム利用に影響を与えません。
- エイジレス80コールセンターによるワンストップサポートを実現。他社で導入した場合と異なり、現地エンジニアと連携して障害対応を行う体制が構築されています。

【信頼性】

- 製造元のFortinet社はUTMアプライアンス（統合脅威管理製品）のパイオニアであり、次世代ファイアウォール・UTM分野ではシェアNo.1の世界的なリーディング企業です。

国内セキュリティ機器市場
(2015年 出荷台数)



導入費用について

【導入タイプ】 ※事業所ごとのご導入が必要となります。（本部・支部の2拠点をお持ちのセンター様は2台ご導入が必要です）

① 標準タイプ（P C 台数：30台まで）

リース料：10,200円/月額

保守料：6,000円/月額



38.5 x 216 x 165 mm (1.00kg)

② 拡張タイプ（P C 台数：31台以上）

リース料：12,700円/月額

保守料：9,000円/月額



38.5 x 216 x 160 mm (1.01kg)

【サポート内容】

- ・定義ファイル更新、製品ライセンスに対する情報提供
- ・障害切り分け、故障時の代替機提供、設置回収

（お問い合わせ窓口：エイジレス80コールセンター TEL: 03-6683-3669 FAX: 03-6660-9768）

【注意事項】

- ・上記は税抜費用となります。

特記事項

【ご導入にあたって】

- 「P C 台数」は、同一ネットワーク配下に接続されている P C の台数となります。
センター様の利用環境によってはエイジレス80の端末台数と異なる場合がございますので、お申し込みの際はご注意ください。
- 通信の監視を行うため、U T M の導入により通信に関する体感速度が低下する場合がございます。
- 設置時はエイジレス80ほか各種ネットワーク接続が行えませんのでご了承ください。
- U T M 本体の導入に関しては、一括支払いのご要望にも対応しています（保守期間は 5 年間）。
リース契約に関しては、5 年リース契約のみを承っております。
詳細は営業担当までご相談ください。

【中途解約および契約期間について】

- 契約期間内で中途解約される場合、保守契約期間の未経過月分のご精算が必要です。
- 本製品は、期間の延長および再リースを承っておりません。
- 契約期間満了後は、後継機種へのお切り替えをご検討ください。

【参考】 近年の個人情報流出事案

カプコン 不正アクセスによる個人情報流出(2020年)

<概要>

第三者からのオーダーメイド型ランサムウェアによる不正アクセス攻撃を受け、同社の顧客・取引先等、計約35万人の個人情報<氏名・住所・電話番号・メールアドレス・人事情報等>が流出。個人情報が流出した人へ、個別に連絡、経緯・状況の説明を行った。

<経緯>

2020年11月、社内システムへの接続障害を確認。オーダーメイド型ランサムウェア(※)によるサイバー攻撃が発生。障害の原因が、ランサムウェアの攻撃によるネットワーク上の機器に対するファイルの暗号化であることが判明。

<対策>

外部との接続を常時監視するシステムの導入や、機器の不正な挙動等を早期に検知するシステムの導入など、再発防止に向けた種々のセキュリティ強化策を実施。

(※)・・・感染した端末やそこに保存されているファイルを使用不能にし、その解除と引き換えに身代金（Ransome）を要求するマルウェア

株式会社インターメスティック 不正アクセスによる個人情報流出(2021年)

<概要>

株式会社インターメスティックにおいて、同社が運営するメガネブランド「Zoff（ゾフ）」及び「GLASSAGE（グラスサーージュ）」が保有する計9万6,911件の顧客個人情報<氏名・性別・生年月日・電話番号・メールアドレス>、従業員の個人情報が流出。個人情報が流出した人へ、個別に連絡、経緯・状況の説明を行った。

<経緯>

2021年5月、社内サーバへの不正アクセスを確認。調査の結果、2020年11月に社内ネットワークに接続するための装置が複数回にわたり第三者の侵害を受けており、その後2021年5月まで複数回にわたり侵入がなされていたことが判明。

<対策>

社外との通信、サーバやシステムへのアクセスに対する監視と管理の強化、マルウェアや不審な通信の監視などの端末側のセキュリティ強化など、ITセキュリティ対策を実施。

【参考】 2022年4月施行 改正個人情報保護法の概要

個人情報の保護に関する法律等の一部を改正する法律（概要）

- 平成27年改正個人情報保護法に設けられた「いわゆる3年ごと見直し」に関する規定（附則第12条）に基づき、個人情報保護委員会において、関係団体・有識者からのヒアリング等を行い、実態把握や論点整理等を実施。
- 自身の個人情報に対する意識の高まり、技術革新を踏まえた保護と利活用のバランス、越境データの流通増大に伴う新たなリスクへの対応等の観点から、今般、個人情報保護法の改正を行い、以下の措置を講ずることとしたもの。

改正法の内容

1. 個人の権利の在り方

- 利用停止・消去等の個人の請求権について、不正取得等の一部の法違反の場合に加えて、個人の権利又は正当な利益が害されるおそれがある場合にも要件を緩和する。
- 保有個人データの開示方法（※）について、電磁的記録の提供を含め、本人が指示できるようにする。
（※）現行は、原則として、書面の交付による方法とされている。
- 個人データの授受に関する第三者提供記録について、本人が開示請求できるようにする。
- 6ヶ月以内に消去する短期保存データについて、保有個人データに含めることとし、開示、利用停止等の対象とする。
- オプトアウト規定（※）により第三者に提供できる個人データの範囲を限定し、①不正取得された個人データ、②オプトアウト規定により提供された個人データについても対象外とする。
（※）本人の求めがあれば事後的に停止することを前提に、提供する個人データの項目等を公表等した上で、本人の同意なく第三者に個人データを提供できる制度。

2. 事業者の守るべき責務の在り方

- 漏えい等が発生し、個人の権利利益を害するおそれがある場合（※）に、委員会への報告及び本人への通知を義務化する。
（※）一定数以上の個人データの漏えい、一定の類型に該当する場合に限定。
- 違法又は不当な行為を助長する等の不適正な方法により個人情報を利用してはならない旨を明確化する。

3. 事業者による自主的な取組を促す仕組みの在り方

- 認定団体制度について、現行制度（※）に加え、企業の特定分野（部門）を対象とする団体を認定できるようにする。
（※）現行の認定団体は、対象事業者のすべての分野（部門）を対象とする。

4. データ利活用に関する施策の在り方

- イノベーションを促進する観点から、氏名等を削除した「仮名加工情報」を創設し、内部分析に限定する等を条件に、開示・利用停止請求への対応等の義務を緩和する。
- 提供元では個人データに該当しないものの、提供先において個人データとなることが想定される情報の第三者提供について、本人同意が得られていること等の確認を義務付ける。

5. ペナルティの在り方

- 委員会による命令違反・委員会に対する虚偽報告等の法定刑を引き上げる。
（※）命令違反：6月以下の懲役又は30万円以下の罰金
→ 1年以下の懲役又は100万円以下の罰金
虚偽報告等：30万円以下の罰金 → 50万円以下の罰金
- データベース等不正提供罪、委員会による命令違反の罰金について、法人と個人の資力格差等を勘案して、法人に対しては行為者よりも罰金刑の最高額を引き上げる（法人重科）。
（※）個人と同額の罰金（50万円又は30万円以下の罰金） → 1億円以下の罰金

6. 法の域外適用・越境移転の在り方

- 日本国内にある者に係る個人情報等を取り扱う外国事業者を、罰則によって担保された報告徴収・命令の対象とする。
- 外国にある第三者への個人データの提供時に、移転先事業者における個人情報の取扱いに関する本人への情報提供の充実等を求める。

※ その他、本改正に伴い、「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」及び「医療分野の研究開発に資するための匿名加工医療情報に関する法律」においても、一括法として所要の措置（漏えい等報告、法定刑の引上げ等）を講ずる。

※この資料に記載された会社名、製品・サービス名はそれぞれ各社の商標もしくは登録商標です。

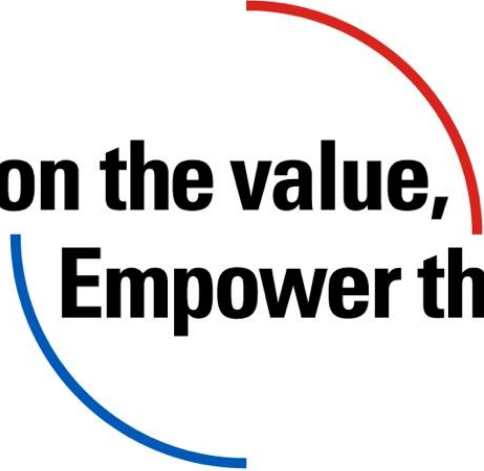
※本資料に記載された内容は、2026年5月現在のものであり、当社は予告することなく製品・サービスの仕様および価格を変更し、または提供・販売を中止することがありますことをご了承ください。

お問合せ先

株式会社野村総合研究所 社会情報システム事業部

電話：03-6660-9766 FAX：03-6660-9767

〒135-0042 東京都江東区木場1-5-25 タワーS棟



**Envision the value,
Empower the change**