法律・監査・セキュリティのプロが説く

マイナンバーで変わる、セキュリティリスクと個人情報保護の重要性

2015年6月　トレンドマイクロ株式会社

目次

本ホワイトペーパーは、弁護士法人エルティ総合法律事務所長 藤谷 護人氏と、トレンドマイクロ株式会社 上級セキュリティエバンジェリスト 染谷 征良の対談インタビューを元に編集をしています。

藤谷 護人 氏

弁護士法人エルティ総合法律事務所長

国内弁護士で唯一の公認システム監査人。11年間の千代田区職員時代に住民情報システムの設計・製造・開発のプロジェクトリーダーを経験。多くのシステム訴訟、システム監査等の経験を踏まえて、システム監査とリーガルチェックを組み合わせたサービス「LT式システム開発監理サービス」やIT紛争に特化した民間紛争処理機関「IT・ADRセンター」を創設。個人情報保護やセキュリティに関する講義・講演多数。

染谷 征良

トレンドマイクロ株式会社 上級セキュリティエバンジェリスト

英国・北米で大手セキュリティベンダの競合戦略、製品戦略、テクニカルマーケティングに11年間従事。2008年入社以降、トレンドマイクロではセキュリティエバンジェリストとして法人に対するセキュリティの啓発活動やテクノロジーマーケティングを展開。セキュリティの専門家として、セミナー・講演などを精力的にこなす。

はじめに.

マイナンバー制度と安全管理措置について

マイナンバー制度は、『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』(通称：マイナンバー法)に基づく制度です。2016年1月の運用開始以降、国民の社会保障・税にかかわるあらゆる行政事務がすべてマイナンバーに紐づくかたちで遂行されるようになり、官公庁自治体は、「個人番号利用事務実施者」として、所定の事務手続にマイナンバーを用いていかなければなりません。対する民間事業者も、「個人番号関係事務実施者」として、「給与」や「預金利子」、「株式配当」、「借地料」、「講演／執筆料」など、個人への金銭的な支払いが発生する全取引でマイナンバーを扱っていくことになります。

本文内でも触れられているとおり、マイナンバーは、個人情報の中でもとりわけ利用制限の厳しい、秘匿性の高い情報です。そのため、民間事業者も、政府の特定個人情報保護委員会が策定し、2014年12月に（その正式版を）公表した『特定個人情報の適正な取扱いに関するガイドライン』と、そこに記されている「安全管理措置」に沿いながら、マイナンバー、あるいはマイナンバーを含む個人情報（これらは、「特定個人情報」と呼ばれる）を厳格に管理し、漏えい、滅失、毀損、不正使用のリスクから保護する義務を負います。

この安全管理措置は、マイナンバー法に則ったガイドラインであり、あらゆる民間事業者に対して、マイナンバーを取り扱う事務範囲や、マイナンバーを含むファイル（特定個人情報ファイル）の範囲、マイナンバーを扱う担当者（民間事業者の場合は、「個人番号関係事務実施者」）の範囲などを明確化し、それぞれのガバナンスを徹底していくことを求めています。また、人・組織の安全管理措置のほか、情報システムに適用すべき安全管理措置（「物理的安全管理措置」や「技術的安全管理措置」）として、データ暗号化やアクセス制御、アクセス者の識別・認証、不正アクセス防止、情報漏えい防止などの施策が掲げられています。法人組織は、こうしたガイドラインに基づいて、特定個人情報保護の基本方針や取り扱い規定を定めていくことが必要になります。

果たして、マイナンバーは、企業の情報セキュリティリスクをどれだけ高めるのでしょうか。そして、マイナンバーを漏えい・盗難から守るには何が必要とされるのでしょうか。法律とシステム監査、セキュリティのプロが解説します。

1. マイナンバーのセキュリティリスク

1-1. 膨らむセキュリティリスク

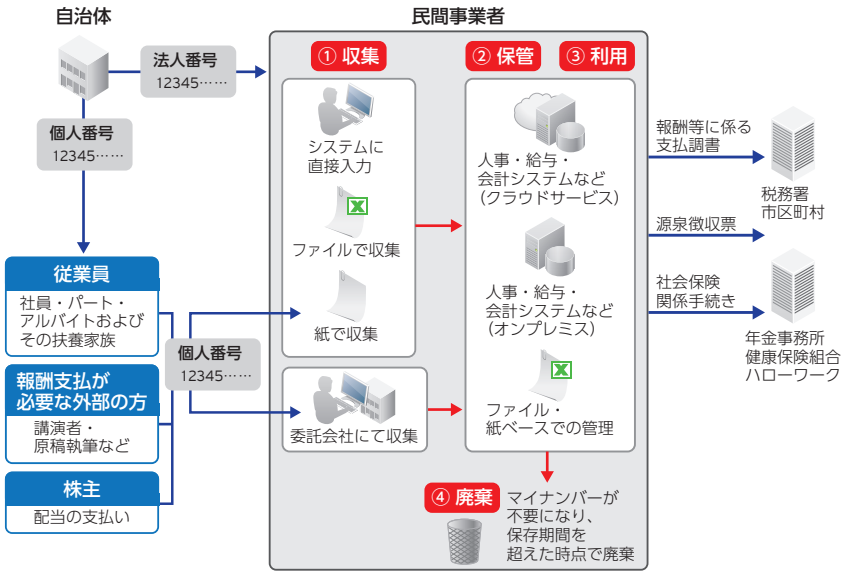
「社会保障・税番号（マイナンバー）」は、すべての国民を識別するための12桁の「個人番号」であり、社会保障・税にかかわるあらゆる行政手続きに用いられる情報です。2015年10月から日本の全国民に対する通知が始まり、2016年1月に「マイナンバー制度」の運用がいよいよ始まります。それに伴い、大きく懸念されているのが、法人組織のセキュリティリスクの増大です。

周知のとおり、マイナンバーを取り扱うのは、官公庁自治体だけではありません。あらゆる民間事業者が「個人番号関係事務実施者」として、従業員（とその扶養家族）、株主、個人の取引先、あるいは顧客などのマイナンバーを扱っていく必要があり、マイナンバーと、マイナンバーを含む「特定個人情報」を厳格に管理し、漏えい、滅失、毀損、不正使用などのリスクから守る義務を背負うことになります（図1参照）。

マイナンバーを取り扱う民間事業者の責務は重大です。弁護士であり公認システム監査人でもある藤谷 護人氏は次のように指摘しています。

「例えば『株主のマイナンバーが流出したら』と考えただけでも、マイナンバーがいかに重要な情報かが容易に推し量れます。自社でマイナンバーを取り扱う場合には、当然自己責任となりますが、人事業務や株式事務を外部に委託している場合にも監督責任が発生します。その中で、万が一マイナンバーを漏えいさせた場合、致命的なダメージを被りかねません」

図1 民間事業者におけるマイナンバーの流れ



1-2. マイナンバーで高まる個人情報の絶対価値

マイナンバーには、「情報の守り手」にとって非常に厄介な特性があります。それは、マイナンバー自体の価値もさることながら（コラム参照）、マイナンバーに紐付く一連の個人情報の（犯罪者にとっての）経済価値を高めてしまうことです。

マイナンバーのようなユニークな番号が国民一人ひとりに割り振られるということは、様々な個人情報がそれに紐付くため、結果個人情報の絶対的価値も高めます。これにより、サイバー攻撃や内部犯行の標的にされやすくなります。さらに、マイナンバーはメールアドレスやID／パスワードとは異なり、相当の理由がない限り変更の難しい絶対的な番号です。犯罪者にすれば、マイナンバーを軸に窃取した様々な情報をデータベース化すればその価値がより一層上がっていく、『費用対効果の高い情報』と言えます。

こうした理由もあり、社会保障番号や国民IDといった番号の利活用が進んでいる米国や韓国では、社会保障番号を含む個人情報を標的にした大規模な情報窃取・盗用事件が起きています(表1参照)。

現時点では、米国や韓国の社会保障番号や国民IDと日本のマイナンバーは仕組みや用途が異なりますが、国内でも民間のさまざまな分野でマイナンバーの活用が中長期的に検討されています。そうなれば、マイナンバーを悪用して出来ることの幅も広がり、犯罪者から狙われるリスクがますます膨らんでいく可能性があります。

表1 海外における社会保障番号に関連した事件

(1)社会保障番号漏えい事件

時期	国	業務	攻撃手法	被害内容	被害規模
2015年2月	米国	医療保険サービス	外部からの不正アクセスによる窃取	氏名、生年月日、加入者ID、社会保障番号、住所、電話番号、電子メールアドレス、勤務先情報が漏えい	約8,000万件
2014年4月	カナダ	歳入庁	脆弱性を利用した不正アクセスによる情報改ざん	納税者の社会保障番号の削除	900件
2014年1月	韓国	クレジットカード複数社	内部犯行による情報の不正持ち出し	住民登録番号(国民ID)や金融機関の口座番号を含む顧客の個人情報の漏えい	約2,000万件

(2) 社会保障番号が悪用された事件

時期	国	事件内容
2015年2月	米国	盗んだIDで税申告ソフトを通じて、大量の不正な税申告をオンラインで行い、還付金を得ようとする事件が発生
2014年10月	米国	詐欺目的で、不正にSSNと銀行口座情報を購入しようとし、2年3か月の実刑判決が言い渡された
2011年	米国	ある女性がSSNを悪用され続け、高校卒業の時点でクレジットカードとローン口座を42件作成され、150万ドルの借金をされていた

コラム　マイナンバーの経済リスクを読む

――米国社会保証番号の個人評価額は「5,570円」

トレンドマイクロは2014年12月、日本、米国、欧州の個人ユーザ1,903人を対象にプライバシーとセキュリティリスクに関する意識調査※を実施しました。

その中で、信頼できる企業なら個人情報を売るか、また売るとすれば、どの個人情報をいくらで売るかについて質問しました。すると、回答者の半数以上が「売る」と答え、売値は、「ID・パスワード」が最も高く7,580円、次いで「健康情報」が5,980円、その次に「社会保障番号(米国のみ)」が5,570円という結果でした。

この調査における個人情報の「平均評価額」は1,965円。つまり、(米国の結果ではあるが)社会保障番号のような、“国民番号”は、消費者自身も「価値の高い情報」と見なしており、それは情報窃取をねらうサイバー攻撃者・犯罪組織、さらには内部犯にとっても同じということになります。また、個人情報は組み合わさるほどその価値は増します。言い換えれば、マイナンバーはそれ自体標的にされ、かつ窃取された際に企業が被る経済的な損失もかなり大きくなるということです。

※「IoT時代のプライバシーとセキュリティ意識」　URL：http://www.go-tm.jp/iot_2015

2．マイナンバー対策のポイント

2-1．マイナンバー対策の出発点

現状では、法人組織におけるマイナンバー制度への理解はまだ十分とは言えず、マイナンバー対策の方向性をつかみあぐねている向きも少なくありません。実際、トレンドマイクロが今年3月に実施した調査でも、マイナンバー制度に伴うITシステムの対応について「完了している」と答えた回答者（官公庁自治体・民間事業者）は全体の4.3%（民間4.5%／官公庁自治体3.4%）にとどまり、逆に、「まだ何も行っていない」、「情報収集段階」とした向きは50.5%（民間52.8%／官公庁自治体40.5%）にも上っています。

そのような中で、マイナンバーという重要情報が加わる中、法人組織は何から着手すればよいのでしょうか。

それは「リスクアセスメント」にほかならないと、藤谷氏は指摘しています。

「組織内のどのプロセスとシステムで、どういったリスクが高まるかをしっかりと認識し、把握することが、マイナンバー対策の出発点であり、マイナンバー制度の運用前に是が非でも取り組むべき施策です」

藤谷氏によれば、今日のサイバー攻撃や内部犯行を防ぎ切るのは難しく、「予防策」と「抑制策」の両輪をバランスよく回すことがセキュリティ対策の要諦であるといえます。

ここで言う「予防策」とは、システム的な施策を意味し、それによって情報漏えいの可能性は狭められるものの、『穴』は必ず残ります。その穴から情報が漏れるリスクを抑えるのが「抑制策」で、こちらは、人の心理に働きかけて不正を抑止する取り組みです。

この2つの施策をバランスよく展開するには、「社内のどこに、どのような情報があり、それぞれの機密性・重要度がどういったレベルにあるのか、また、それぞれの情報にどのようなプロセスが紐づき、誰がアクセスできるのか」を可視化しておくことが不可欠です。そのうえで、予防・抑制の両施策が、「どの人に、どう効いているか」をチェックしていく必要があります。

「国も、マイナンバーの漏えい・悪用を抑止するために、（法人組織の大小にかかわらず）特定個人情報の取り扱いの違反者に対して、（これまでの個人情報保護法に基づく罰則以上に）厳しい罰則を定めています。ですが、マイナンバーの重要性や経済価値を勘案すると、それだけで内部不正やサイバー攻撃の十分な抑止につながるとは正直思えません。だからこそ、法人組織のしっかりとした対策が必須とされるのです（藤谷氏）」

2-2．求められる「脅威の侵入・内部犯行ありき」の総合対策

内部犯は情報に対するアクセス権や特権を用いて、システムに直接アクセスし、サイバー犯罪者は一般社員や公開システムを侵入口に攻撃を行います（図2、図3参照）。

図2 外部からの攻撃(サイバー攻撃)による情報窃取の流れ

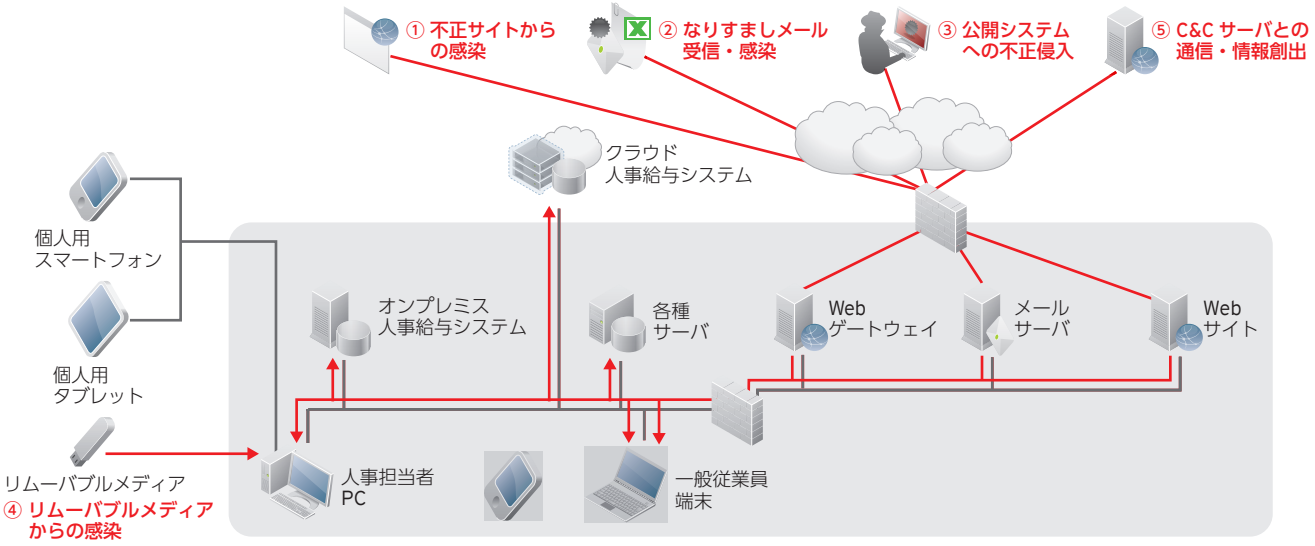
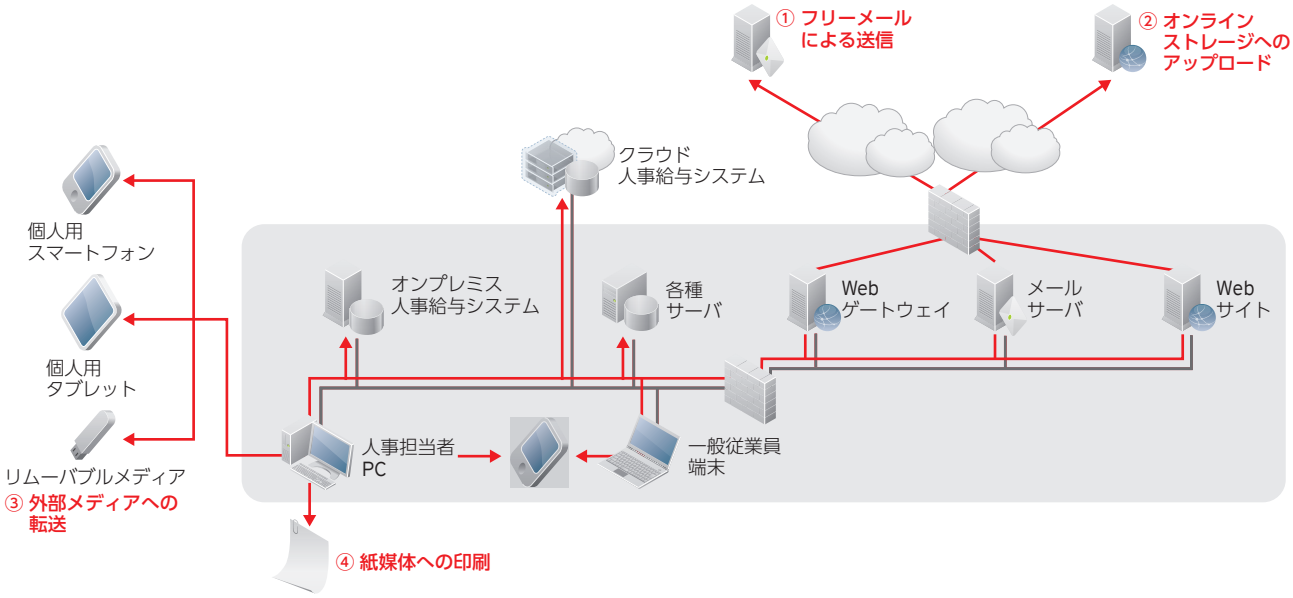


図3 内部犯行による情報窃取の流れ



藤谷氏が指摘するとおり、内部犯行やサイバー攻撃を防ぎ切るのは難しく、実際これまでも、数多くの法人組織が内部犯行とサイバー攻撃によって個人情報窃取の実害を被ってきました。しかも、内部犯行やサイバー攻撃は、あらゆる規模の、あらゆる業種・業態の法人組織が内包する脅威です。これも、マイナンバー管理を一層難しくします。

「マイナンバーの場合、マイナンバー関係業務の直接的な委託先ばかりではなく、その背後に連なる再委託先、再々委託先の監督責任も、大元の発注元に課されます。それらの委託先の中には、中・小規模の事業者が含まれるでしょう。そうした中小企業は、今やサイバー攻撃の格好の標的でもあり、内部犯行のリスクも潜在させています。ですから、業務の発注元は、そうした法人組織のセキュリティ・ガバナンスにも十分な配慮が必要とされます(藤谷氏)」

また、マイナンバー関連業務の処理にクラウドのサービスを用いているならば、クラウドのセキュリティ・ガバナンスも強化しなければならならず、結果的に、契約条項の見直しが必要になる可能性もあります。このような必要施策を洗い出し、適切に対処していくうえでも、リスクアセスメントと情報資産の棚卸を実施し、全体のリスクを可視化していくことが肝心です。

「マイナンバー対策は、社内の人事給与システムを改修したり、人事担当者の端末だけにセキュリティ対策を施したりといった局所的な施策で済む話ではありません。内部犯行やサイバー攻撃による脅威の侵入があることを前提に、情報の流れ（コンテキスト）や場所に基づく総合的な対策を優先度をつけて講じていくことが重要です（染谷）」

実際、例えば、従業員からマイナンバーを収集するに当たっても、全従業員の業務端末から、メールあるいは人事システム（オンプレミスやクラウド）にマイナンバー情報が流れます（前出図1参照）。この流れを考えても、組織全体、すべての端末で対策を強化することが絶対条件だということが分かります。

2-3. マイナンバー対策を情報資産のたな卸しのきっかけに

トレンドマイクロの2015年調査によると、社内にある重要度の高い情報が何かを定義し、情報資産の棚卸を定期的に実施している企業は、全体の24.4％でしかありません。

「この実施率の低さは、マイナンバー対策はもとより、日本の法人組織の情報セキュリティ全体にとって憂慮すべきものです。実施できている組織とそうでない組織では、そもそもセキュリティ対策の包括度で100点満点中最大47点も差が出ることが分かっています。また対策スコアがベースラインを上回る組織の42.6%がマイナンバーに伴いセキュリティを強化する一方、ベースラインを下回る組織ではその割合は13.9%にすぎず、50.1%がまだ何も決まっていないという状況です。ただしそうだからこそ、マイナンバー対策をいいきっかけにリスクアセスメントや情報資産の棚卸から実施すべきです（染谷）」。

マイナンバー制度の運用は、既に決められたことで、すべての民間事業者・自治体が否応なしでの対応が求められています。それならば、それを逆に自社・自組織のセキュリティ基盤や体制の見直し、強化につなげていくという、マインドの変革が今、求められているのではないでしょうか。

2-4. マイナンバー・特定個人情報を守るトレンドマイクロのソリューション

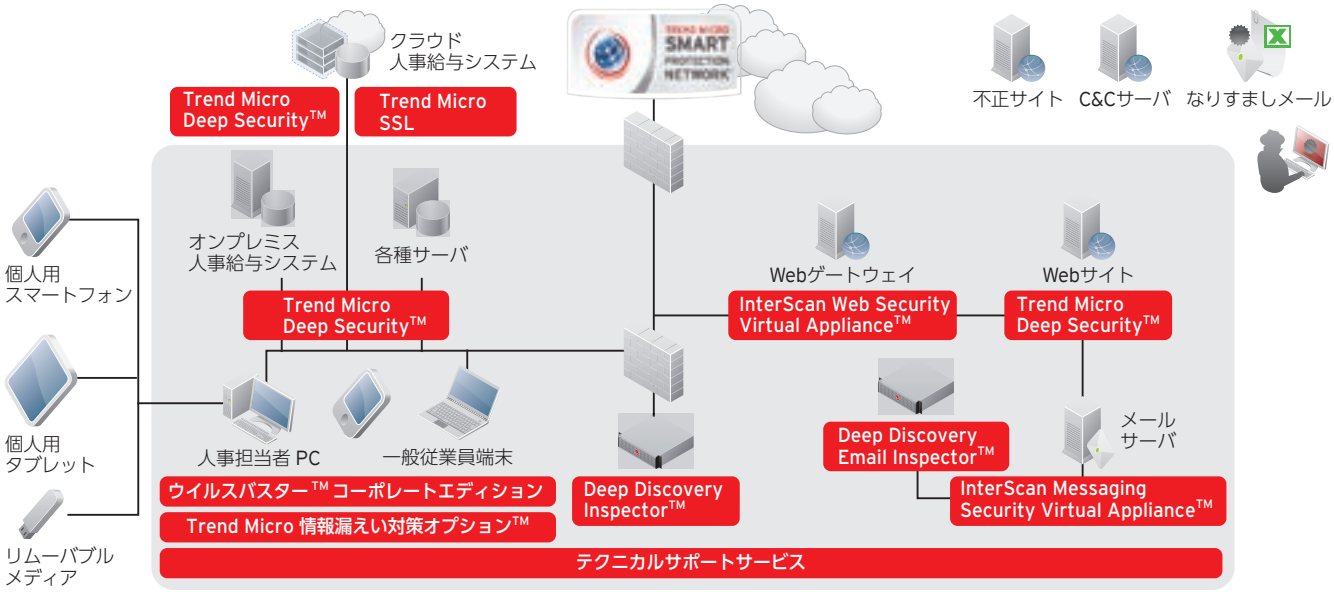
トレンドマイクロは、マイナンバー・特定個人情報を狙う組織内外からの脅威に対抗していくための製品・ソリューションを包括的に提供しています（表2、図4参照）。

エンドポイントからネットワーク、物理環境からクラウド環境にいたるまで、企業のネットワーク／ITを構成するあらゆるレイヤーの防御を固めるのと同時に、企業ネットワーク内部での不正プログラムや内部犯の挙動をすみやかに見つけ出すことで、適切かつスピーディな対処が可能になります。こうした対策を行うことにより、サイバー攻撃・内部犯行の「予防」と「抑制」の施策を効果的に回すことができます。

表2 対策のポイント

	脅威	対策	トレンドマイクロ製品
内部犯行への対策	USB メモリやスマホなどの記録媒体による不正な持ち出し	●PC 端末に接続できる記録媒体の利用制限	●Trend Micro 情報漏えい対策オプション™
	特定個人情報の外部流出（メール添付、プリンター .etc）	●特定個人情報を含むファイルの流出監視 / ブロック	●Trend Micro 情報漏えい対策オプション ™
	クラウドストレージや Web メールへの不正アップロード	●外部クラウドストレージ、Web メールへのアクセス制限	●InterScan Web Security Virtual Appliance™
外部からのサイバー攻撃への対策	標的型メールによるマルウェア感染	●標的型メールの検知	●Deep Discovery Email Inspector™
	不正サイトを通じたマルウェア感染	●不正サイトへのアクセス遮断 ●マルウェア感染からの保護	●ウイルスバスター ™ コーポレート エディション ●InterScan Web Security Virtual Appliance™
	脆弱性を悪用する攻撃	●サーバの脆弱性対策 エンドポイント端末の脆弱性対策	●Trend Micro Deep Security™ ●Trend Micro 脆弱性対策オプション ™
	遠隔操作による内部情報の抜き取りや不正な内部探索活動	●外部への不正なネットワーク通信・接続の検出 ●ファイルやレジストリの変更監視 ●早朝の内部活動の検知・可視化	●InterScan Web Security Virtual Appliance™ ●Deep Discovery Inspector™
	重要な情報が保管されているサーバへの侵入	●セキュリティログ監視 / 変更監視	●Trend Micro Deep Security™

図4 トレンドマイクロの製品・ソリューション・マップ



〒151-0053
東京都渋谷区代々木 2-1-1　新宿マインズタワー
大代表 TEL：03-5334-3600 FAX：03-5334-4008
URL：http://www.trendmicro.co.jp

TREND MICRO™

Securing Your Journey to the Cloud

BR-REPO-024