サイバー攻撃対策としての、保険の重要性

悪意ある者によるサイバー攻撃は、日に日にその手口が巧妙化しています。そのため、人的、ソフトウェア的、設備的にあらゆる対策を講じても、その被害を完璧に抑えられるとは言い切れません。そうした“万一の事態”に備えるのが、サイバー保険です。
NTT ComのSSDには東京海上日動火災保険株式会社が提供するサイバー保険を基本機能として提供しており、サイバー攻撃を受けて万一情報漏えい事故が起こってしまった場合には、最大3,000万円（損害賠償責任に関する補償：最大2,000万円/各種費用に関する補償最大1,000万円）をサイバー保険で補償します。

保険会社担当者コメント

サイバー攻撃は、近年ますます高度化、巧妙化しており、今後、攻撃件数もさらに増加することが懸念されています。企業ではセキュリティシステム対策の強化やオペレーション面での体制の強化だけでなく、ファイナンス面での対策も重要となると考えています。このような背景から、幅広いお客様にご満足いただけるよう、サポートデスクサービスと組み合わせた新たな保険を共同設計させていただきました。

東京海上日動火災保険株式会社
情報通信ソリューション部
NTT室 課長代理
田口 一徹

経済産業省が定めるガイドラインにもリスクの移転についての対策例が明記

「サイバーセキュリティ経営の重要10項目」より

指示4 サイバーセキュリティリスクの把握とリスク対応に関する計画の策定（抜粋）

経営戦略の観点から守るべき情報を特定させた上で、サイバー攻撃の脅威や影響度からサイバーセキュリティリスクを把握し、リスクに対応するための計画を策定させる。
その際、サイバー保険の活用や守るべき情報について専門ベンダへの委託を含めたリスク移転策も検討した上で、残留リスクを識別させる。

対策例

把握したリスクに対して、実施するサイバーセキュリティ対策を以下の観点で検討する。

- リスク低減策の実施（リスクの発生確率を下げる対策）
  例：重要な情報へのアクセス制御、ソフトウェア更新の徹底
- リスク回避策の実施（リスクが発生する可能性を除去する対策）
  例：端末の持ち出し禁止（外部での盗難のリスクを回避）
- リスク移転策の実施（リスクを他社等に移す対策）
  例：クラウドサービスの利用、サイバー保険の加入

出典：経済産業省「サイバーセキュリティ経営ガイドライン Ver.2.0」

経済産業省が企業向けにまとめたセキュリティ対策「サイバーセキュリティ経営ガイドライン Ver.2.0」では、セキュリティ対策の実施を「コストと捉えるのではなく、投資と捉えることが重要」とした上で、「セキュリティ対策の予算や人材等の確保」や「サイバー保険を使ったリスク移転」を挙げています。この「人材」「保険」という観点からも、SSDをお選びいただくお客さまが増えています。

セキュリティサポートデスクに関するお問い合わせ
NTTコミュニケーションズ株式会社
法人のお客さまお問い合わせ窓口［法人コンタクトセンター］
0120-106107 受付時間 9:30～17:00
※携帯電話、PHSからもご利用になれます。土・日・祝日・年末年始は休業とさせていただきます。
ホームページ https://www.ntt.com/ssd/

2022.03

株式会社 エコー・システム

docomo business

株式会社エコー・システム

セキュリティサポートサービスの利用とクラウド管理のセキュリティアプリ導入で現場の負担を軽減し、生産性を大きく向上

導入サービス：セキュリティサポートデスク、マイセキュア ビジネス

1989年、有限会社エコー・システムとして設立、1993年の「販売管理システム」発売以降、多くの業務用パッケージソフトをリリース。1996年には東京に、2004年には大阪に営業所を開設。経営理念を合い言葉にITを活用したお客さまの事業の効率化に向き合う。

経営理念

人との出会い・縁を大切にし、相互理解・相互信頼のもとに、共存共栄し、夢のある会社作りをめざす。

株式会社エコー・システムは、広島市に本社を置くシステム開発会社です。オーダーメイドでの受託開発のほか、「EchoPack販売管理」「トレ！トレ！Meat」など、自社開発の業務用パッケージソフト販売とカスタマイズ、既存システムからの移行（マイグレーション）、また時代に合わせ、「お弁当EDIシステム」をはじめとしたクラウドサービス展開などを幅広く手がけ、お客さま事業のIT化をサポートしています。
同社は、1989年の創業以来、生産性、メンテナンス性にすぐれた「Magic」というツールを使った開発に強みを持ち、同ツールの技術者数や実績においては国内トップクラスです。そしてその技術力への高い評価により、同社は国内に8拠点、約120名の社員を抱えるまでに成長しましたが、お客さまが増えるにつれ、アプリケーションソフトとともに提供するセキュリティソフトのアップデートやインシデント対応が現場の負荷となっていました。
この課題解決とお客様のセキュリティサポート強化のため、2021年秋、同社はNTT Comの「セキュリティサポートデスク（以下SSD）」「マイセキュア ビジネス（以下MSB）」の取扱開始を決定しました。

課題 業務用アプリケーションとともに提供するセキュリティソフトのサポート業務が、事業拡大とともに負荷として顕在化。生産性向上のため、対応が求められる。

導入 NTT Comの提案で、既存のセキュリティソフトから「MSB」にスイッチ。インシデント発生時も、自社対応から「SSD」での対応に切り替える。

効果 セキュリティソフトのサポートがなくなったことで、現場の本業注力が可能に。またお客さま側管理者が行う各端末のアップデート確認の負担も大きく軽減。

期待 「サイバー保険など、お客さまに大きなメリットがあるセキュリティ対策」を訴求、訪問、対面営業が難しいコロナ禍での“ドアノックツール”としても活用を。

課題

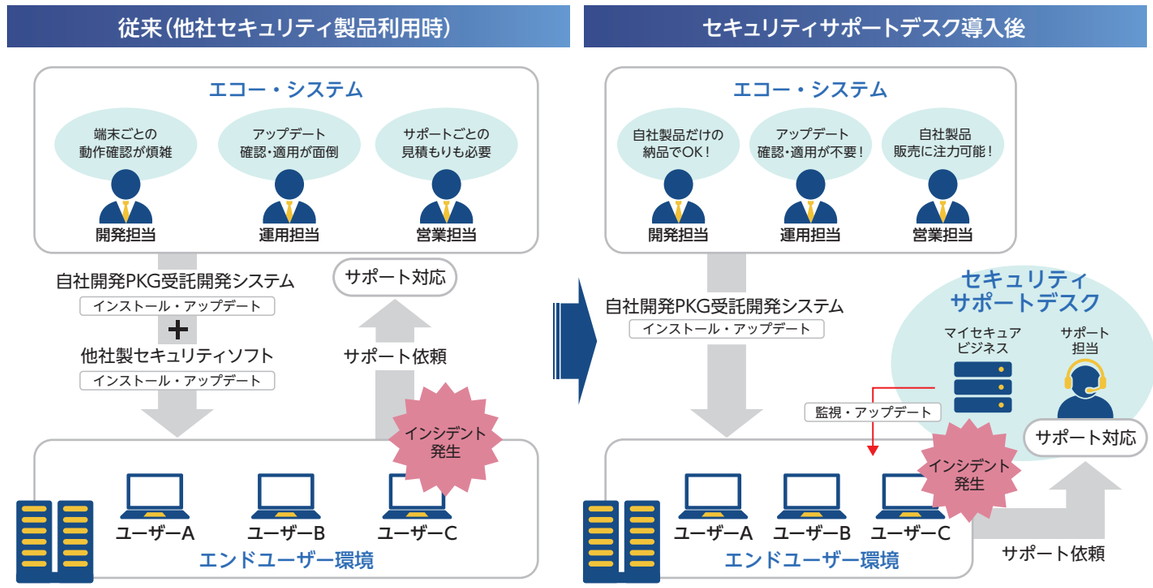
エンドポイントセキュリティの問い合わせ対応と インシデント対応での負荷が本業を圧迫

当社では、本来業務であるシステム受託開発の他に、業務用アプリケーションと他社製のセキュリティソフトを組み合わせて、パッケージ販売を展開しています。一般的にセキュリティソフトには“相性”があり、当社が開発した業務用アプリケーションの動作に対しても不具合を及ぼすことがあります。したがって、パッケージに含まれるエンドポイントセキュリティの選択はお客さまにおまかせするのではなく、当社からは他社製品を推奨しご提供して参りました。
しかし、お客さまがその製品をご利用になる上で、サービスに関するお問い合わせはすべて提供元である弊社にエスカレーションされるため、お問い合わせ対応により弊社の技術部隊の稼働が逼迫することもありました。
また昨今では、マルウェアなど不正な添付書類を含むメールやフィッシングメールが激増したことで、インシデント対応といったお客さまサポートも大きな負荷となっていました。
このように本来業務以外の対応が、システム開発などの生産性向上の大きな妨げになっており、提供するアプリケーションとお客さまサポート面で早急な対策をとる必要がありました。

導入

インシデント対応を機に「MSB」「SSD」を お勧めいただき、本格採用へ

こうした課題が解決に向け動き出したのは、1つのできごとがきっかけでした。当社のお客さまから「メールに添付されたマルウェアを開封してしまった」という報告があり、当時このお客さまに向け共同でネットワーク更改のご提案を行っていたNTT Comと共に当該PCの隔離などの対応を行いました。そしてインシデントが一段落した時、NTT Comの担当者から、MSBとSSDを勧められたのです。
SSDでは他社製品と同じエンドポイントセキュリティであるMSBをサポート対象としているため、エンドユーザーからのMSBに関する問い合わせは全てSSD側で回答してもらえるということ、またインシデント時のサポートも基本機能に含まれるということで、これまで当社が抱えていた課題を一挙に解決するものでした。早速過去にインシデントが発生したお客さまにMSB/SSDのセット提案をしたところ、受注第1号となりました。
受注の背景には、NTT Comの提案支援体制の充実が大きく起因しています。NTT Com担当者による全国支店への提案手法勉強会や、提案時にサービス主管だけでなくサイバー保険の提供元である東京海上日動火災もオンラインで提案支援してくれるなど手厚いサポートがあったため、サービスに関する詳細知識がなくともお客さまにアピールができ、採用を決めた初期の段階から、提案に対する不安はありませんでした。



効果

開発、運用担当の直接的負担軽減のほか 営業/技術の内部稼働も大きく削減可能に

MSB/SSDセット提案のお客さまの反応は絶大でした。MSBは利用料金が他サービスと比較して安いにもかかわらず、クラウド上の脅威情報を参照することで常に最新の脅威に対応できるということから、導入を決めるお客さまが多いです。またSSDでは、セキュリティアラートに関する質問に対して迅速な回答を得られることや、インシデント時のセキュリティ専門家による電話サポート、インシデント対応費用を補償してくれるサイバー保険に大変魅力を感じていただいています。このように、MSB/SSDはお客さまの関心が高いため商談での会話が進みやすく、案件開拓としてのドアノックツールとしては最適だと思っています。
当社としても、MSB/SSDをお客さまに導入いただくことで大きなメリットを得ております。MSBはサービス側でセキュリティソフトをアップデートするため、当社がお客さまを訪問して1台1台PCを設定する作業がなくなり、稼働はかなり削減されました。また、セキュリティに関する問い合わせは全てSSD側で受けてもらえるので、当社の担当者が別件に対応している場合でもお客さまをお待たせすることはありません。このように、当社の営業部隊や技術部隊もMSB/SSDの導入により稼働が効率化され、本来業務に集中することで生産性の向上に大きく繋がっています。

期待

コロナ禍での対面営業が難しいなか 有力なドアノックツールとして活用を

お客さまにMSB/SSDをご提案すると、やはりNTT Comの“キャリアとしての信頼”に、大きな評価をいただきます。特に、ネットワークに関する“プロ”として認識していただいており、協業する上で非常に心強いパートナーだと感じています。
先日、NTT Comが提供するセキュリティ商材の1つに、インターネット接続時のセキュリティを強化するvUTMもSSDのサポート対象に含まれていることをお聞きしました。今後はSSD/MSBのセット提案の中に、vUTMといった他のセキュリティサービスを適宜追加検討し、お客さまに提案していきたいと考えています。
当社にとっても、こうした魅力あるサービスの提案は、新規顧客開拓に有効だと考えています。とくにコロナ禍においては、非対面のコミュニケーションが求められることから、お客さまにアポをとることも難しい状況です。しかしこうしたセキュリティ商材でお客さまの関心を引き、その後の営業につながるドアノックツールとして活用していきたいと思います。ネットワークの付加価値としてのセキュリティ商材提案を皮切りに、当社の営業活動を本格化し、本業のシステム開発の受注確度を最大限に上げることで、お互いにとってWINWINな関係を継続して築けていければと思っています。

セキュリティサポートデスク導入の効果

エコー・システム

- 開発担当：自社製品納入時に他社セキュリティをインストールする手間、個別の端末ごとに動作確認する手間がなくなり、業務がスムーズになりました。
- 運用担当：各端末のセキュリティソフトのアップデートは、コロナ禍でリモートワークが進んだことで大きな負担でした。SSD導入で、その負担がなくなりました。
- 営業担当：インシデント対応の作業見積もりを作成し、お客さまにご承認いただくフローは時間のかかる作業でした。SSD導入で営業に注力できるようになりました。

エンドユーザー

- 管理者：リモートワークが進み、それぞれのスタッフがセキュリティソフトのアップデートをきちんと行っているかの把握が難しくなっていました。SSDでは、クラウドで稼働するMSBが自動的にアップデートを行うため、そうした心配がなくなりました。
- スタッフ：インシデントが発生したとき、エコー・システムの担当者はていねいに対応してくれましたが、やはり他の案件と重なり時間がかかることもありました。SSDでは専任のセキュリティ担当者が対応してくれるので、解決がスピーディになりました。

株式会社エコー・システム

取締役 兼 東京事業所長
津賀田 晃

SI企業に10年以上開発技術者として従事。主に中堅中小企業の流通業務システムの開発を行う。その後営業へ転身し、お客さまのソリューション提案に従事。請負開発を中心にISMS取得コンサルやインフラ関係の構築提案など、IT全般に関与。現在は、実績を認められ東京事業所の所長と合わせて取締役に就任。採用や営業・開発の管理業務など全体の運営や、新規顧客、重要顧客について営業同行などを行っている。

ネットワーク化するビジネスにあわせ、巧妙化するサイバー攻撃 いま求められるセキュリティ対策とは？

企業同士がネットワークでつながり、仕事の現場でもクラウドの活用が広がる現在、
企業のセキュリティ対策には「エンドポイント」と「クラウド」をカバーする“多層防御”が求められています。

業務のデジタル化が進み、あらゆる企業がネットワークでつながっている現在、悪意ある者からの不正アクセスやマルウェアによるサイバー攻撃は、大企業だけでなく、大企業の子会社、関連会社や、大企業と取引のある中小企業（サプライチェーン）へと広がっています。
大企業の多くは、サイバー攻撃に備えて防御を固めており、攻撃や侵入は容易ではありません。そこで悪意ある者は、防御が比較的手薄な中小企業を狙い、そこで入手した情報をもとに、大企業にビジネスメール詐欺を仕掛けたり、ランサムウェアに代表されるマルウェア感染を狙った不正なメールを送るなどして、金銭的利益を得ようとしているのです。
独立行政法人情報処理推進機構（IPA）が発表した「情報セキュリティ10大脅威2022」においても、「サプライチェーンの弱点を悪用した攻撃」は、前年より順位を1つ上げ、第3位にランクインしています。
またその手口について、「令和3年警察白書」は、「ソフトウェアやシステムの脆弱性を悪用した攻撃」「標的型メール攻撃を通じた不正プログラム感染」が多数発生しているとしています。

つまり、サイバー攻撃への対策としてのセキュリティ強化は、業種や企業規模を問わず、中小企業においても喫緊の課題なのです。

IPA「情報セキュリティ10大脅威2022」

	脅威の内容	昨年順位
1位	ランサムウェアによる被害	1位
2位	標的型攻撃による機密情報の窃取	2位
3位	サプライチェーンの弱点を悪用した攻撃	4位 ↑
4位	テレワーク等のニューノーマルな働き方を狙った攻撃	3位 ↓
5位	内部不正による情報漏えい	6位 ↑
6位	脆弱性対策情報の公開に伴う悪用増加	10位 ↑
7位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	NEW
8位	ビジネスメール詐欺による金銭被害	5位 ↓
9位	予期せぬIT基盤の障害に伴う業務停止	7位 ↓
10位	不注意による情報漏えい等の被害	9位 ↓

自社の情報が漏洩することで、サプライチェーンでつながる取引先企業にも損害を与える可能性が生まれ、また損害額が大きく膨らむ可能性がある。対策は急務だ。

出典：独立行政法人情報処理推進機構（IPA）「情報セキュリティ10大脅威2022」

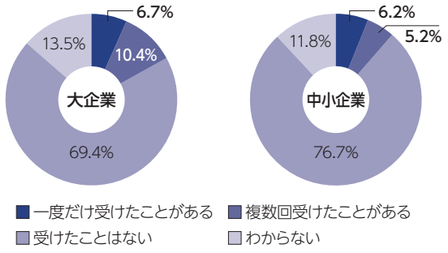
サイバー攻撃による金銭的損害が企業の存続を左右する可能性も

こうした攻撃によりマルウェアなどに感染すると、感染範囲の調査費用、復旧費用、事業の中断にともなう損失など、多くのコストがかかります。さらに感染により、取引先など第三者に被害がおよんだ場合、その損害の賠償を求められる可能性もあります。
NPO日本ネットワークセキュリティ協会（JNSA）が発行する「インシデント損害額調査レポート2021」が挙げる「従業員がメールに添付されていたファイルを開いたところ、マルウェアに感染した」という事例では、事故原因・被害範囲を調査するための費用に500万円、再発防止策としてメールフィルタリングサービスの導入に100万円、合計600万円の被害額が報告されています。
そして同レポートでは、インシデントレスポンス事業者へヒアリングした事故原因・被害範囲調査費用として、PCとサーバー数台程度でもおおむね300～400万円が必要で、マルウェア感染が拡大するなど大規模な被害になれば、その費用は数千万円に拡大する場合もあるとしています。
また一般社団法人日本損害保険協会の「国内企業のサイバーリスク意識・対策実態調査2020」では、これまでにサイバー攻撃の被害を受けた会社は大企業で17.1%、中小企業でも11.4%で、その被害額が100万円以上となったのは大企業で15.9%、中小企業で12.7%と、被害の可能性、被害額は企業規模を問わないことが明らかになっています。

サイバーリスクによる被害状況

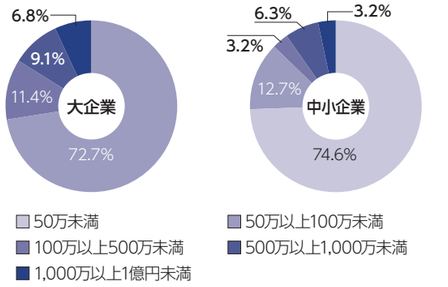
これまでにサイバー攻撃の被害を受けた企業

中小企業の1割超がサイバー被害を経験している



サイバー被害を受けた際の被害総額

企業規模に関係なく高額被害が発生している



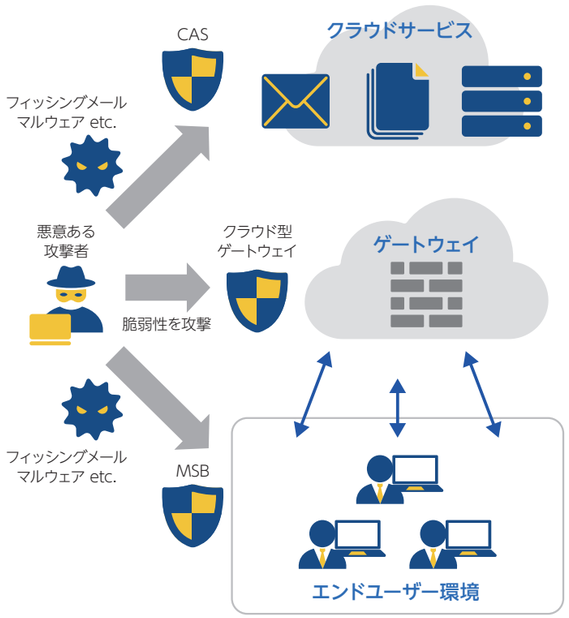
出典：一般社団法人日本損害保険協会「国内企業のサイバーリスク意識・対策実態調査2020」

これらの調査結果は被害を認識している企業のものであり、被害が発生しなかった企業、攻撃や被害に気づいていない企業も含めると、ほぼすべての中小企業になんらかのサイバー攻撃が行われています。
そしてその被害と企業規模によっては経営の行方を左右する問題にも発展するのです。
こうしたサイバー攻撃による被害を防ぐためには、「メールの添付書類の取り扱いに気をつける」「メールにあるリンクを無造作にクリックしない」といった、従業員のセキュリティ意識を高める教育が第一であることは言うまでもありません。しかし人に頼ったセキュリティ対策は、個人の資質によりその効果が左右されるほか、ヒューマンエラーの発生は防げません。さらに悪意ある攻撃者の手口は年々巧妙になっていることから、人に頼らない、ソフトウェア的な対策が、より重要となっています。

管理者に負担をかけず、かつ高水準で脅威を防ぐソフトウェア的対策とは

では具体的なソフトウェア的対策は、どのように進めるべきでしょうか。以前は社員が使う端末（エンドポイント）にセキュリティソフトを導入し、定義ソフトをアップデートしながら使うことが一般的でした。
しかし昨今はコロナ禍により加速したテレワーク、タブレットやスマートフォンを含んだエンドポイントの多様化で、そうしたアップデートを社内で一括管理することが難しくなってきています。
さらに業務でのクラウド活用が拡大したことで、エンドポイントを経由しないファイルのやりとりや共有が一般化し、エンドポイントの防御だけではマルウェアなど不正なファイルの検出は困難となっています。つまり、少なくともエンドポイントとクラウドの多層防御を想定したセキュリティ対策の実施が求められているのです。

最低限実施しておくべき多層防御



端末インストール型のセキュリティソフトが検出できるのは、端末にダウンロードした不正なファイルのみ。クラウド経由での不正なファイル流通にも対策が必要だ。

そこで最低限実施すべき多層防御のソリューションとして、NTT Comの「マイセキュア ビジネス（以下MSB）」「Cloud App Security（以下CAS）」「セキュリティサポートデスク（以下SSD）」をご紹介します。

お客さまのニーズを満たしたセキュリティサービス。導入後もSSDの充実したサポートにより安心して運用可能

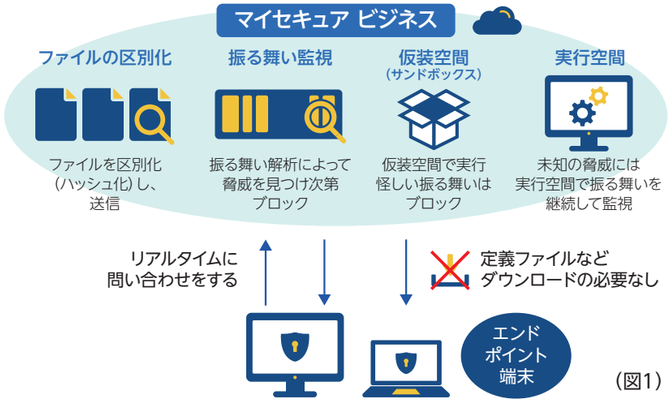
MSB（図1）はクラウド参照型の次世代エンドポイントセキュリティです。定義ファイルを端末側に置いてパターンマッチングをする従来型とは異なり、クラウド上の脅威データベースを参照するため、常に最新の脅威情報を参照するかつ、定義ファイルの管理も不要になります。未知の脅威に対しては、振る舞い検知の実施、また、未知の脅威が実行したものをリカバリーし、安全な状態へ復旧するロールバック機能など最先端の防御機能が搭載されております。
CAS（図2）は「Microsoft365」「Box」「Dropbox」「Google Workspace」など、ビジネスシーンで一般的に使われるクラウドサービスを網羅的に監視するセキュリティサービスで、社外に置かれるメールやクラウド共有ストレージデータのセキュリティを強化します。各クラウドサービスとはAPI連携するため、DNSの切り替えや、メールフローを変更する必要はなく、導入が大変スムーズです。
またサンドボックス機能による標的型メール攻撃対応や、メール本文やファイル内を検索するキーワード検索機能を利用することで、情報漏えい対策が可能となります。

ただ、こうした多層防御のために複数のセキュリティサービスを利用すると、各サービスのアラート対応や必要に応じた設定変更ための専門知識が必要となり、社内の限られたリソースでは対応が困難となります。これらの課題を解決するのがSSDです。
SSD（図3）はセキュリティに関する総合窓口として安心をお客さまにご提供するサービスです。MSB／CASといった各層のセキュリティサービスのアラートについての不明なことがあれば、24時間365日、セキュリティの専門家に相談が可能です。
さらに万が一インシデントが発生した場合も、年中無休の電話サポート機能により初動対応を支援します。さらに、インシデントで発生した損害賠償費用や弁護士費用、調査費用、などは基本機能に含まれるサイバー保険により最大3,000万円まで幅広く補償されます。
ここでご案内したNTT Comのセキュリティ対策サービスは、1IDからのライセンス数でも利用可能で、ご利用いただきやすい料金設定であることも特長です。御社のセキュリティ対策に、ぜひご検討ください。

マイセキュア ビジネス

あらゆる端末をクラウドが監視、アップデートも自動で実施

Point！
- ファイルサイズが小さくスキャンも高速、端末に負担をかけず利用可能
- クラウド上にある定義ファイルを参照、最新の脅威にもリアルタイムに対応
- 端末ごとの定義ファイル更新は不要で管理者の運用負荷を大幅に軽減



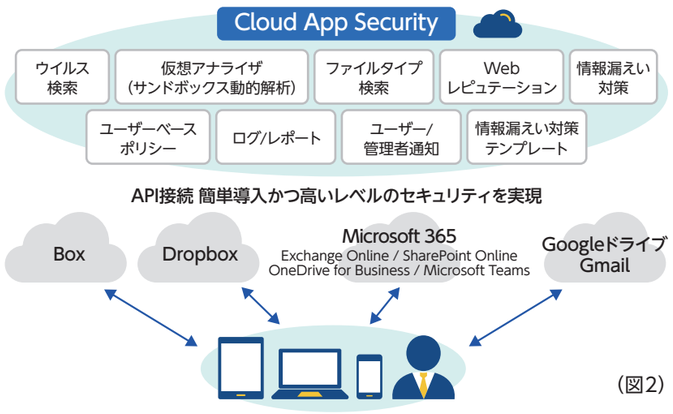
（図1）

「マイセキュア ビジネス」は、クラウド従来型のセキュリティソフトにみられる、ファイルサイズが大きい、動作による負荷で端末の反応が重くなる、定期的な定義ファイルの更新が必要などのデメリットがなく、端末に負担をかけることなく動作し、かつ定義ファイル更新に手間なく最新の脅威に対応できます。脅威の判定は「危険／グレー／安全」の3段階で、グレー判定のファイルは挙動を継続監視、のちにウイルスと判定された場合はそのファイルが行った変更を自動修復し、端末を守ります。

Cloud App Security（クラウドアップセキュリティ）

クラウド上のファイルをチェックし安心安全な業務環境を実現

Point！
- 複数のクラウドサービスのセキュリティ対策をワンストップで実現
- ウイルス、マルウェア対策のほか、任意のキーワードによる「情報漏洩対策」も可能
- 各クラウドサービスとはAPIで連携、DNSやメールフローの変更は不要で導入が容易



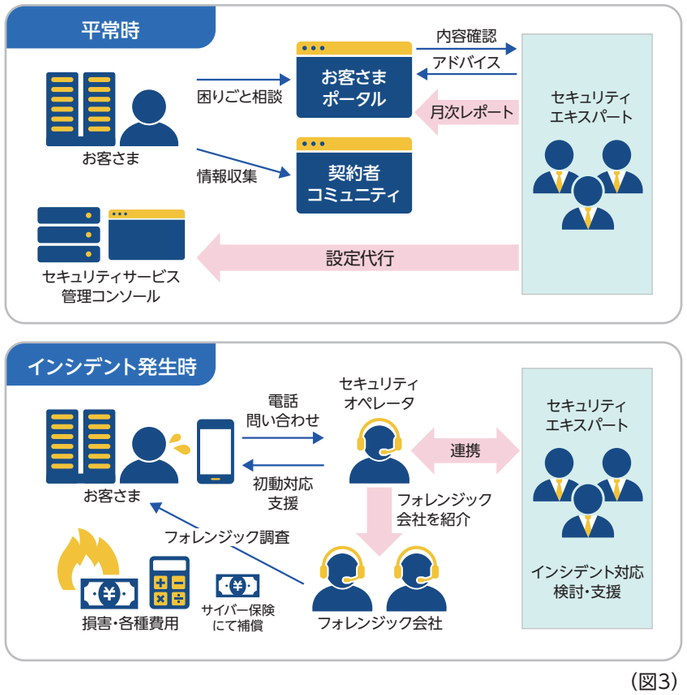
（図2）

メールやクラウドストレージなどのクラウドアプリのセキュリティ強化に特化したサービスが「Cloud App Security」です。導入も保護対象アプリのお客さま管理者アカウント情報を入力するだけで、API接続されすぐに利用開始いただけます。クラウドに届いたメールやクラウドにアップロードされたファイルに不正なものがないか、安全な環境（サンドボックス）で解析し、ウイルスやマルウェアの拡散を防止します。またお客さまのご用意したテンプレートに従ってファイルの内容をスキャン、個人情報、機密情報の漏洩を防ぎます。管理ログにより利用状況の可視化も可能です。

セキュリティサポートデスク

平常時からインシデント発生時、事後対応までトータルで「安心」をお届け

Point！
- ポータル経由で複数セキュリティサービスについてのお問い合わせが一元的に可能
- インシデント発生時はお電話で初動対応などハンドリングをサポート
- インシデントで発生した費用はサイバー保険で3,000万円まで補償



（図3）

セキュリティ対策の重要性は理解していても、社内に詳しい人材がいない、十分な予算がかけられないなどの課題を抱えているお客さまにご利用いただきたサービスが、「セキュリティサポートデスク」です。SSDは「平常時」「インシデント発生時」「事後対応」の各段階において、セキュリティのお悩みを解消し、安心をお届けします。まず平常時はお客さま向けに用意されたポータルサイトで、セキュリティの相談や各種セキュリティサービスのアラート内容に対して専門家がコンサルティング。会員コミュニティでの情報交換、日々の運用についての気軽な相談も可能です。またオプションで各セキュリティサービスを相関的に分析し、潜在的な脅威を可視化する月次分析レポートをご提供致します。万一インシデントが発生した場合は、年中無休（9時～18時）でお電話にてサポート、脅威の封じ込めなど“やるべき初動対応”をアドバイスします。さらにインシデントにより損害が発生した場合は、付帯する「サイバー保険」により最大3,000万円（損害賠償責任に関する補償：最大2,000万円／各種費用に関する補償：最大1,000万円）の補償が受けられます（詳しくは次ページをご覧ください）。