NTT東日本

W UTM&セキュリティスイッチ で守る!

ダブルの設置で情報セキュリティ対策を!

サイバー被害を防ぐには多層防御をおすすめします!

UTM（統合脅威管理）

★通信を監視しながらログの取得が可能!
★有害サイトへのアクセスや社内情報流出をブロック!
★ネット回線からの不正アクセス・ウイルス侵入をブロック!

セキュリティスイッチ

内部で感染したウイルス

★持ち込み機器から感染したウイルスの拡散をブロック!
★外部端末からのネットワーク接続をブロック!

※ メーカー・機種等により仕様が異なります。詳しくはお問合せください。
●本製品はネットワーク上の脅威に対してそのリスクを低減させるための装置となります。導入することにより、その脅威を完全に取り除くことを保証するものではありません。

NTT東日本にご相談ください!

企業でも被害が発生中!
サイバー攻撃の実態

日々巧妙化していくウイルスやランサムウェアによるサイバー攻撃。
ビジネスにおいて**多層防御による情報セキュリティ対策**が理想です！ウイルスの侵入を防ぐ「出入口対策」と内部拡散の被害を食い止める「内部経路の対策」。**万が一に備えて今こそ情報セキュリティ対策を見直しましょう！**

「情報セキュリティ10大脅威 2020（組織）」

順位	組織	昨年順位
1位	標的型攻撃による機密情報の窃取	1位
2位	内部不正による情報漏えい	5位
3位	ビジネスメール詐欺による金銭被害	2位
4位	サプライチェーンの弱点を悪用した攻撃	4位
5位	ランサムウェアによる被害	3位
6位	予期せぬIT基盤の障害に伴う業務停止	16位
7位	不注意による情報漏えい（規則は遵守）	10位
8位	インターネット上のサービスからの個人情報の窃取	7位
9位	IoT機器の不正利用	8位
10位	サービス妨害攻撃によるサービスの停止	6位

巧妙化する「標的型攻撃」の手口

独立行政法人情報処理推進機構（IPA、理事長：富田達夫氏）は、情報セキュリティにおける驚異のうち2019年に社会的影響が大きかったトピックなどの中から「10大脅威選考会」の投票によりトップ10を選出、「情報セキュリティ10大脅威2020」（個人と組織）として公表しました。

組織向けの脅威では「内部不正による情報漏えい」が昨年の5位から2位にランクアップ。また、「予期せぬIT基盤の障害に伴う業務停止」が6位に復活ランクインしました。

1位は昨年に続き「標的型攻撃による機密情報の窃取」でした。メールやウェブサイトを通じたり、不正アクセスによるなどしてウイルスに感染させる手口が目立ち、巧妙な仕掛けが施されたウイルスも確認されています。被害を早期検知し、被害後即座に対応できるシステムが求められています。

出典：独立行政法人情報処理推進機構「情報セキュリティ10大脅威 2020」（2020年4月）

DIGITAL TREND

中小のサイバー対策徹底4%

サプライチェーンに死角

中小企業による情報セキュリティー対策の遅れがサプライチェーン（供給網）に与える影響に懸念が強まっている。民間の調査によると、公的機関がまとめた指針に沿った対応をできている中小企業は4%にとどまる。ほぼすべての企業が不正アクセスを受けている実態も分かってきた。サプライチェーンが進化すればするほど、大企業の営業秘密が中小企業を経由して海外に漏れるリスクが増す。

「貴社のパソコンから不審なメールが届いた」。都内で自動車部品をつくる中小企業は受注先の完成車メーカーから注意を受け、パソコンがウイルスに感染していたことが分かった。この企業は完成車メーカーから受発注に伴う重要なデータを受け取る立場にあった。IT（情報技術）担当者がいなかったこの企業は完成車メーカーが指定するシステム会社に駆け込み、再発を防ぐ対策を急いだ。

攻撃、30社全てに

中小企業のサイバー被害は調査が少なく、実態はよく分からない。その中で、全国の中小企業団体のなかでもいち早く1971年からIT関連の部署を持つ大阪商工会議所は2018年9月、神戸大学などと共同で中小企業の実情の調査を始めた。

調査対象の30社と外部の通信を約3カ月にわたって監視したところ、全社で不審な通信が記録され、なんらかのサイバー攻撃を受けていた。あらゆる企業が被害を受けている可能性が示唆されたが、中小企業にとっては被害を受けているかどうかの把握すら難しいことも分かった。大商などは近く、調査内容を精査して詳細を公表する。

侵入者はなぜ中小企業を狙うのか。ソフト検査会社のデジタルハーツ（東京・新宿）セキュリティ事業部の大芝大氏は「大手自動車メーカーの設計図を、セキュリティー対策が手薄な下請けの中小企業から抜き取るといった狙いがある」とみる。いくら大手企業が対策を進めても、製造などの委託先が脆弱であれば共有している重要な情報が危険にさらされる。

2017～18年に米デル日本法人（川崎市）とEMCジャパン（東京・渋谷）が実施した調査によると、情報処理推進機構（IPA）の指針に準拠したセキュリティー対策ができている中小・中堅企業は4%どまり。デル日本法人が18年12月から19年1月にかけて実施した別の調査では、IT担当者が1人以下の中小・中堅企業は38%に達し、19%の企業では専任の担当者がいなかった。

IPAは17年に、サプライチェーンにおけるセキュリティーリスクについて249社に聞いた。取引先が仕事を頼む「再委託先」など、直接の取引はないが自社と関係する企業のサイバー対策を把握できている企業は47%にとどまった。大企業から見ると事業の委託が連鎖するほど、状況の把握は難しくなる。

海外から侵入も

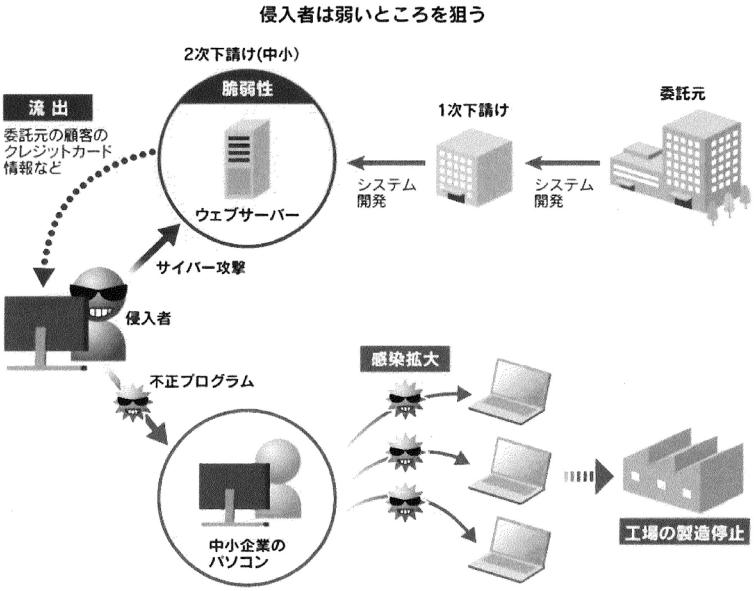
侵入者は対策が弱い中小企業にフィッシングメールを送ったり、ウイルスに感染させたりしてサプライチェーンへの侵入を試みる。MS&ADインターリスク総研サイバーリスク室の土井剛室長は「特定はできないが海外からの攻撃が多く、政府が関与していることもあるようだ」と指摘する。

実態を把握しようとする試みはある。デジタルハーツは経済産業省やIPAなどと組み、20年2月までに宮城・福島・岩手の各県にある100～200社程度の被害を調査する計画だ。中小企業に専用の機器を設置し、外部との通信をAIで分析する。

現場に駆けつける必要があると判断すれば、同社の仙台の拠点から技術者が派遣される。同社の富崎暉樹セキュリティ・コンサルタントは「実際の事業ではどのくらいの価格設定にすれば中小企業の利用が広がるかも確かめたい」と話す。

IPAの情報セキュリティー・ビジネスにおける10大脅威19年版によると「サプライチェーンの弱点を悪用した攻撃の高まり」が初めて4位に入った。

欧米ではすでにサプライチェーンを意識したサイバーセキュリティーの強化が進んでいる。米国では17年、防衛調達に参加する全ての企業に対してセキュリティー対策を義務化した。IPAの横山尚人氏は「セキュリティー対策が不十分な事業者はサプライチェーンからはじき出されることになりかねない」と警鐘を鳴らす。（石橋茉莉）



責任の所在、被害時の課題

サプライチェーンが狙われると、被害は複数の企業にまたがる。事故が起きれば、責任の所在が問題になる。情報処理推進機構（IPA）の横山尚人氏によると、責任の範囲は企業がかわす契約書のなかで定める。だが「サイバー対策を想定していない契約もまだ多い」という。

IPAがIT（情報技術）業務の委託に限って調査したところ、システムの脆弱性といった「新たな脅威」が顕在化した際の対応について、委託元と委託先が責任範囲を文書に記載していない例は全体の8割にのぼった。

経済産業省などは契約のなかでどのように責任の範囲を定めるかの議論を進めてきた。例えば契約書に役割分担表などを付け、セキュリティーの確保は委託先・委託元の間でどちらの責任とするかを事前に明確にするといった手法があるという。契約書でもサイバー対策への意識が求められている。

出典：日本経済新聞、2019年7月2日付