大手建設会社Ａ工務店が**下請け企業に**発信した通達文（抜粋）

■**最低限実施**していただきたい対策

サイバー攻撃のほとんどが、メールまたはセキュリティ対策が不十分なソフト及び機器を介して行われることから、**次の対策を直ちに実施して下さい**。なお、自社での実施が難しい場合は、日常的にお取引している IT 業者等に相談して下さい。

① 標的型メールの事例紹介及び**標的型攻撃メール訓練の実施を通じた社員への注意喚起**。
② 会社で利用しているメールサービス又はメールシステムに、**スパムメール・ウイルスメール検知・隔離・駆除オプション等を追加**する。
③ パソコンおよびサーバーに**アンチウイルスソフト**を入れ、ソフトのパターンファイル更新を自動にし、**常に最新の状態を保つ**。
④ パソコンおよびサーバーの **OS・業務ソフトウエア（オフィス・アドビ等）セキュリティの更新**を自動にし、常に最新の状態を保つ。
⑤ ファイアウオール・ルーター等の**ネットワーク装置の自動アップデート**を有効にし、機器を常に最新の状態に保つ。自動アップデートの設定ができない場合は、IT 業者等を通じて、機器のセキュリティ更新に関する情報を定期的に入手して更新する。
⑥ 万一サイバー攻撃を受けて、ファイルを暗号化されたり、システムを破壊されたりしても、すぐに復旧できるよう、業**務データをバックアップ**しておく。オフライン（光学ディスク・テープ）及びオンライン（クラウドストレージ）へのバックアップを併用することが望ましい。

■より**安全性を高める**ために推奨する対策

① ウイルスの侵入を防ぐ従来型のアンチウイルスソフトでも防げない、最新のウイルスが侵入してきたとしても、**ウイルスの活動開始を検知し、感染をブロックする仕組み（EDR）を導入**する。（アンチウイルス対策ソフトでは防げないウイルスが急増している）
② 在宅勤務等で、社員が社外から社内ネットワークにリモートでアクセスするためのパスワードを万一盗まれても、社内に侵入されないよう、リモートアクセス用のネットワーク機器（SSL-VPN 装置）またはクラウドサービスのパスワード認証に、**スマートフォンへのコード送信等の認証を加えた多要素認証**を導入する。
③ 万一攻撃の被害に遭ってしまった場合に、適切な再発防止策を取るために必要となる攻撃経路・原因を確認するためのパソコン、サーバーおよびネットワーク機器の**監査ログの取得**。
④ 万一攻撃の被害に遭ってしまった場合の、復旧等にかかる多額の費用をカバーするための、**サイバー保険への加入**。

大手メーカーＢ重工が**取引先**に発信した依頼文（抜粋）

弊社お取引先様におかれましても・・・具体的なセキュリティ対策については下記をご参照下さい。

① 正規の従業員になりすました**不審なメール**が届いた場合、記載されたＵＲＬのクリック、および添付ファイルを開かないこと。

② **ＯＳやソフトウエアを古いまま放置せず**、アップデートやセキュリティパッチを適用することで常に**最新の状態**に保つこと。

③ **ウイルス対策ソフト**を全てのＰＣに導入し、ウイルス定義ファイルを**最新の状態**に保つこと。

④ **各種パスワード**を「長期間」、「シンプルなもの」を「使い回さない」ように**管理を強化**すること。

⑤ データ保管などの **Web サービス**やファイル**共有設定**を見直し、無関係な人が**情報を覗き見できないよう**にすること。

⑥ データの消失に備え、**バックアップ**を定期的に実施するとともに、**復旧手順**の確認を行うこと。

⑦ ＩＰＡ(情報処理推進機構)などのセキュリティ専門機関のサイトで脅威や攻撃の手口を知り、**社内で共有**すること。

⑧ 情報セキュリティ**インシデント発生時の連絡体制**および**対応マニュアル**を整備し、関係者にて共有しておくこと。

なお、弊社では今後の不審メール対策として、以下の対策を実施します。

Excel マクロファイル(.xlsm)、Word マクロファイル(.docm)、パスワードで暗号化された Zip ファイルが添付された社外からの受信メールを遮断し、メール受信者に遮断した旨を通知する。
通常の Excel ファイル、Word ファイル、パスワード無しの Zip ファイルは受信可能です。