News Release

報道関係各位

2022 年 2 月 25 日
一般社団法人ソフトウェア協会（SAJ）
Software ISAC

経済産業省における「昨今の情勢を踏まえたサイバーセキュリティ対策の強化について」の注意喚起を受けて

一般社団法人ソフトウェア協会（住所：東京都港区、会長：荻原 紀男、略称：SAJ）の Software ISAC では、経済産業省の昨今の情勢を踏まえた、サイバーセキュリティにおける「リスク低減のための措置」、「インシデントの早期検知」、「インシデント発生時の適切な対処・回復」の大きく3つの項目の注意喚起を受け、より多くの皆様にわかりやすく、Web サイトやメール等で周知を行います。

具体的に想定されるサイバー攻撃としては、複数のコンピュータからサーバに大量のリクエストやデータを送り、サーバの機能を停止させる「DDoS（Distributed Denial of Service attack／分散型サービス拒否攻撃）」や、Web サイトを運営者の意図しない内容に改ざん（画像や文章が変更されたり、コンピュータウイルスのダウンロード可能なサイトに変更されたりするなど）、企業の新型コロナウイルス感染症禍において依存度の高い Web サイトなどのサーバなどが狙われる可能性があります。

また送信されてくる電子メールにコンピュータウイルスを添付したり、メールの本文に含まれる URL（http://www.～や、https://www.～の Web アドレス）に接続してコンピュータウイルスをダウンロードさせたりする攻撃（大量のメールを送る「マスメール攻撃」や、業界や組織を絞って行う「標的型メール攻撃」、その他にも ID やパスワードの窃取を主目的とした「フィッシング攻撃」）などが予想されます。

そこで、以下の３点について、ぜひ実行することを早急にご検討ください。

①経済産業省の注意喚起にあるアクセスコントロールとは、機器やネットワーク、データなどにアクセス（触れることが）できる制御を行うことであり、これを実施することや、複数の認証の仕組みを用いる多要素認証などの認証の強化、組織内に存在するセキュリティパッチなどの更新を含め、ソフトウェアを最新版にし、既知の脆弱性によるサイバー攻撃が起きにくい環境を構築することに加え、導入済みの OS（Operating System の略であり、Windows 10 や MacOS のこと）やセキュリティ製品の設定を見直すようにしましょう。特にセキュリティ製品には多くの種類があり、セキュリティ対策ソフト、様々なセキュリティの統合管理製品の UTM（Unified Threat Management の略）、サーバであれば WAF（Web Application Firewall）などがあります。
例えば、コンピュータにコマンド（命令）を送ることができる PowerShell は、インターネットやメール、オフィス製品が使えれば良い職場環境であれば、通常利用することはありません。不要な機能は無効化する設定の強化を行いましょう。（PowerShell の制御）
また、導入しているソフトウェアを最大限有効活用することによって、組織のセキュリティ対策の強化も可能です。

②電子メールに添付されるファイルがどのような形式のファイルであるのかを認識できるようにするために、拡張子を表示させ、危険な拡張子ともいえる「.scr」「.exe」「.pif」「.cpl」などは、できる限り利用者に届く前に排除するようにしましょう。（悪意のあるファイルを添付したフィッシングメール）

③組織としてサイバー攻撃のリスクを低減するために、「最低限検討すべき緩和策」を端末と Web アプリケーションなどにおいても見直しを行いましょう。特に、経済産業省の注意喚起にも記載されたパスワードについては、デフォルト（初期設定）のパスワードは見直すことは勿論のこと、15 文字以上のパスワードで連続した文字や繰り返し、ID 情報なども含まないような形で設定しなおしましょう。またより長く設定が可能なパスフレーズの活用も効果的です。さらに、漏洩してしまったパスワードを利用している場合にもサイバー攻撃のリスクは高まります。漏洩パスワード、そして漏洩パスワードの特徴と類似するパスワードは利用しないようにしましょう。

以上のように、既に導入している製品や機能を使ってセキュリティ対策を強化することが可能です。Software ISAC では既に「情報システム開発契約のセキュリティ仕様作成のためのガイドライン」を、独立行政法人情報処理推進機構（IPA）内に設置された「モデル取引・契約書見直し検討部会」配下の「セキュリティ検討プロジェクトチーム（PT）」にてとりまとめています。

既存のセキュリティ製品の設定を見直す（高くする）だけでも、組織内のセキュリティレベルを向上できる効果があります。これを機に既に導入している製品そのものの有効活用をご検討ください。詳細は以下のページをご参照ください。

●経済産業省「昨今の情勢を踏まえたサイバーセキュリティ対策の強化について」
（令和 4 年 2 月 23 日）
https://www.meti.go.jp/press/2021/02/20220221003/20220221003-1.pdf

●独立行政法人情報処理推進機構「情報システム開発契約のセキュリティ仕様作成のためのガイドライン」
① Guideline – SoftwareISAC
② 情報システム開発契約のセキュリティ仕様作成のためのガイドライン
③ 詳細設定対策に必要な措置
④ MITRE ATT&CK に基づく詳細設定対策
⑤ 最低限検討すべきデフォルト緩和策 端末編
⑥ 最低限検討すべきデフォルト緩和策 Web アプリケーション編
⑦ 漏洩パスワード TOP200 の特徴

■一般社団法人ソフトウェア協会（略称「SAJ」）について

Software Everywhere　～すべてはソフトウェアで動く、これからのデジタル社会へ～
われわれ SAJ は、すべてのソフトウェアを対象とし、デジタル社会を推進するために、「ソフトウェア(国)の未来を創る」をビジョンに見据え、ソフトウェアに関わるすべての組織（チーム)・人をサポートすることをミッションとし、活動しています。
https://www.saj.or.jp/

■Software ISAC について

IoT デバイスの普及に伴い、サイバー空間の脅威は非常に高まっています。また、OSS の活用が進む上で、脆弱性ハンドリングはますます難しくなっています。開発者は安全で安心なソフトウェアの提供をするために、脅威の手法や脆弱性情報を素早く入手する必要があります。そこで、セキュア開発や脆弱性管理の工数最適化や、ソフトウェアサプライチェーンの強靭化の研究を行い、安心・安全な日本への貢献を行う開発者のための情報交換基盤を提供することを目的に発足しました。
以下、Software ISAC 公式 Web サイトでは、組織概要の詳細や規則についてもご覧いただけます。
https://softwareisac.jp/

【お問い合わせ先】

一般社団法人ソフトウェア協会　事務局　総務課　渋谷
E-mail：gyoumu1@saj.or.jp
Tel：03-3560-8440