ZJMR190701101

報道関係者各位

プレスリリース

2019 年 7 月 1 日

ゾーホージャパン株式会社

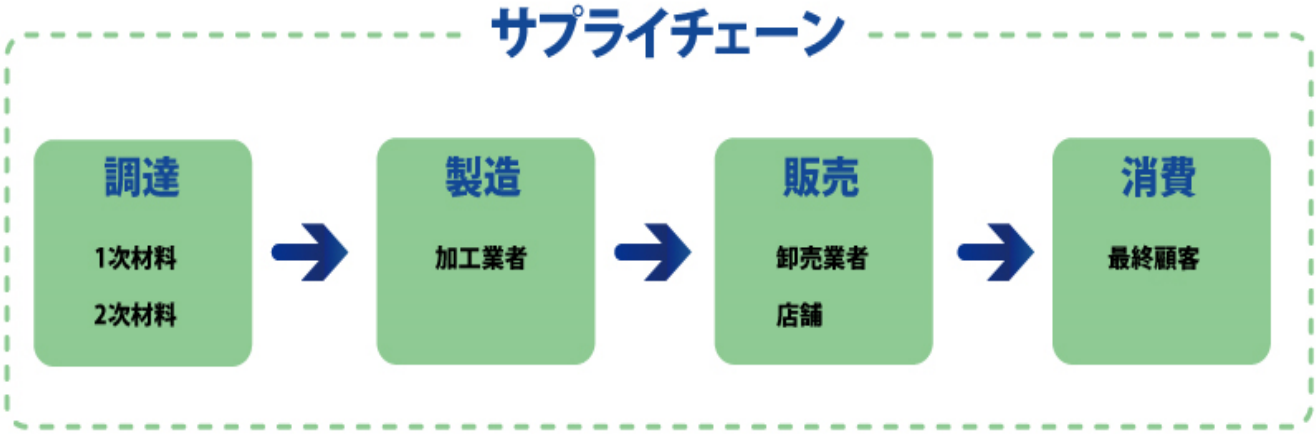
NIST SP800-171 要約版資料、

サプライチェーンセキュリティ対策ツールを無償提供開始

サプライチェーンのセキュリティ対策で遅れを取っている日本。各企業はただちに対応を

セキュリティ上の問題があるとして米国企業とファーウェイとの取引の事実上の禁止に至った「ファーフェイ問題」も記憶に新しいところ。

わずか十数年前にはセキュリティ対策と言えば“個人コンピューターからのウイルスファイル削除”が常識でしたが、もはやグループ会社や関連企業はもちろん、加えてサプライチェーン全体でのセキュリティ対策が必要となっています。



昨今のこのような状況を受け、ゾーホージャパン株式会社（代表取締役：迫 洋一郎、本社：横浜市）は、2019 年 7 月 1 日、自社とサプライチェーンのセキュリティ対策にすぐ活用できる文書「NIST SP800-171 の実践におけるヒント」および「業務委託契約書テンプレートと契約書別添セキュリティチェックシート」の無償提供を開始しました。

NIST 発行の情報セキュリティ関連文書：

https://www.manageengine.jp/solutions/nist_publications/lp/index.html

サプライチェーンセキュリティ：
https://www.manageengine.jp/solutions/supply_chain_security/lp/index.html

■サプライチェーンのセキュリティ対策　海外の動き

2017 年にはオーストラリア軍から F35 戦闘機に関する情報を含むデータが流出、しかもサイバー犯罪者の侵入には 4 ヶ月も気が付かなかったといいます。不正アクセスを受けたのは従業員 50 人規模の航空宇宙関連契約企業でした。

ウクライナでは 2015 年と 2016 年に産業用制御系システムがサイバー攻撃を受け、大規模停電が発生。エネルギー等の重要インフラ事業者に、セキュリティ対策が義務化されました（NIS Directive)。

米国は 2016 年に DFARS Clause252.204-7012 を発行、「米国防衛省と取引をするすべての企業に対して、NIST SP800-171 に準拠した IT システムの整備を要求」しています。

■ガイドライン NIST SP800-171 とは

NIST SP800-171 とは米国政府機関が定めたセキュリティ基準を示すガイドラインです。政府機関だけではなく、取引企業からの情報漏えいを防ぐため、業務委託先におけるセキュリティ強化を要求する内容になっています。

各国も米国に追従し NIST SP800-171 が実質上の国際標準化

米国防省と取引をしている全世界の企業に対して NIST SP800-171 への準拠が要求されており、米国防省と取引をする企業は NIST SP800-171 への対策は避けられません。

また、米国政府だけの取り組みにとどまらず主要国でも米国に追随する動きがはじまっています。

すなわち、NIST SP800-171 に準拠しない企業とその製品やサービスは、グローバルサプライチェーンからはじき出されてしまうおそれがあるということです。

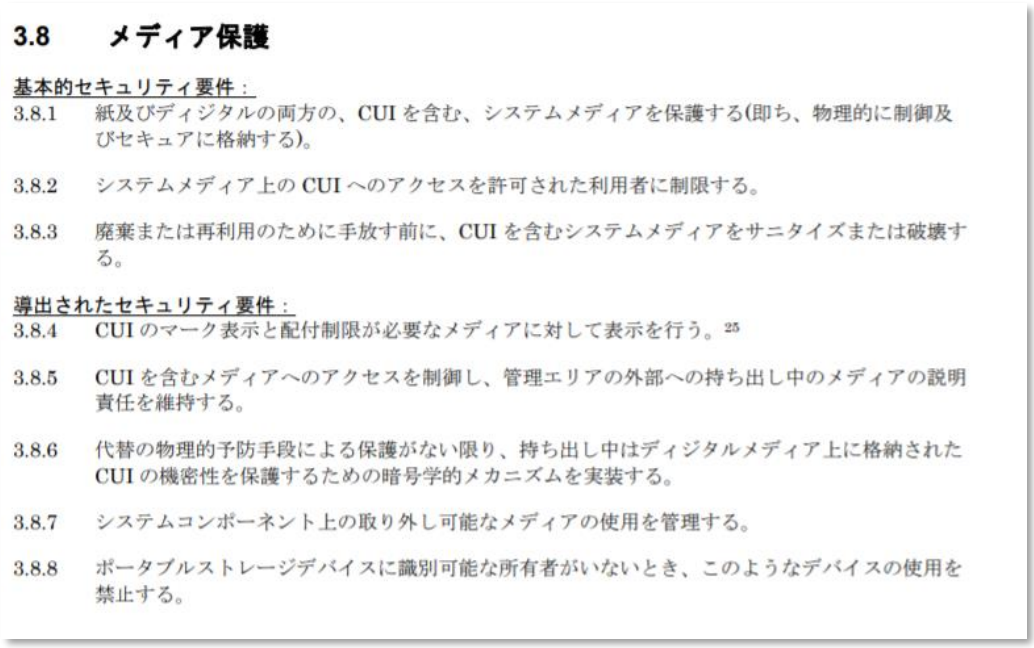
NIST SP800-171 への対応　国内での進捗

日本政府は、防衛産業をハイレベルな産業サイバーセキュリティのモデルとすべく、防衛調達の新基準を NIST SP800-171 と同等にすることを決定しました。新基準への準拠は下請けとなる中小企業も対象となっています。日本国内の各企業も NIST SP800-171 への対応を免れる余地がないのは明らかです。

■あらゆる企業で活用できる「NIST SP800-171 の実践におけるヒント」

ゾーホージャパン株式会社は「NIST SP800-171 の実践におけるヒント」を作成し、提供することにしました。無料でどなたでもダウンロードいただけます。

各企業ともに NIST SP800-171 への対応が急務ですが、NIST SP800-171 は全部で 80 ページにも及ぶ法的なドキュメントで、一般の方がすぐ利用できるガイドラインの形にはなっていません。



3.8　メディア保護

基本的セキュリティ要件：

3.8.1　紙及びディジタルの両方の、CUI を含む、システムメディアを保護する(即ち、物理的に制御及びセキュアに格納する)。

3.8.2　システムメディア上の CUI へのアクセスを許可された利用者に制限する。

3.8.3　廃棄または再利用のために手放す前に、CUI を含むシステムメディアをサニタイズまたは破壊する。

導出されたセキュリティ要件：

3.8.4　CUI のマーク表示と配付制限が必要なメディアに対して表示を行う。[25]

3.8.5　CUI を含むメディアへのアクセスを制御し、管理エリアの外部への持ち出し中のメディアの説明責任を維持する。

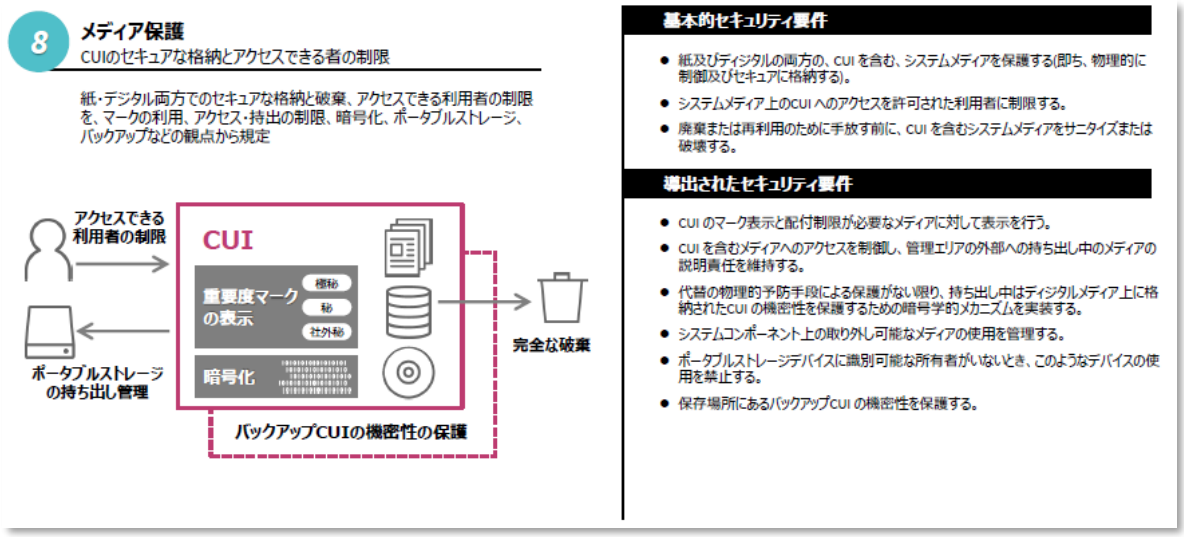
3.8.6　代替の物理的予防手段による保護がない限り、持ち出し中はディジタルメディア上に格納された CUI の機密性を保護するための暗号学的メカニズムを実装する。

3.8.7　システムコンポーネント上の取り外し可能なメディアの使用を管理する。

3.8.8　ポータブルストレージデバイスに識別可能な所有者がいないとき、このようなデバイスの使用を禁止する。

参考：NIST SP800-171 /情報処理推進機構　（IPA）

「NIST SP800-171 の実践におけるヒント」は、企業や組織における“実践”に役立つ情報だけを抽出し、オリジナルの図解の解説も添えた NIST SP800-171 の要約版です。



NIST SP800-171 についての社内教育を実施する際のテキストとしてもご利用いただけます。

■業務委託先企業のセキュリティ対策はどのように管理するか

自社のセキュリティ対策よりも困難なのは、業務委託先企業にセキュリティ対策を“講じさせ”て、“守らせる”ことです。

独立行政法人 情報処理推進機構　（IPA）発行の「情報セキュリティ 10 大脅威 2019」では「サプライチェーンの弱点を悪用した攻撃」が組織における脅威の第 4 位にランクインしています。

順位	組織	昨年順位
1位	標的型攻撃による被害	1位
2位	ビジネスメール詐欺による被害	3位
3位	ランサムウェアによる被害	2位
4位	サプライチェーンの弱点を悪用した攻撃の高まり	NEW
5位	内部不正による情報漏えい	8位

参考：情報セキュリティ 10 大脅威 2019/情報処理推進機構 （IPA）

サプライチェーンの大部分を担う業務委託先企業におけるセキュリティ対策が急務であることは言うまでもありません。

IPA が 2019 年 4 月に公開した「IT サプライチェーンにおける情報セキュリティの責任範囲に関する調査」報告書によると、96.5%の委託元企業が責任範囲を明記する用途で「契約書」を活用しています。

また、業務委託先企業のセキュリティ対策を管理するには、契約関連文書のテンプレートの見直しが有効であることも示されています。

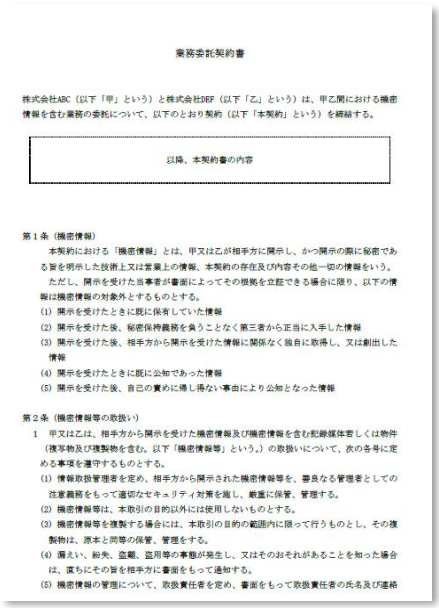
■業務委託契約書テンプレートと契約書別添セキュリティチェックシート

ゾーホージャパン株式会社では、ニュートン・コンサルティング株式会社の監修を受け、業務委託契約書テンプレートと契約書別添セキュリティチェックシートを作成し、無償ダウンロード提供を開始しました。

業務委託契約書テンプレートと契約書別添セキュリティチェックシートは、ニュートン・コンサルティング社のセキュリティコンサルティング経験に基づく知識および、経済産業省や各機関が公開した以下のような規約やガイドラインから、業務委託先企業のセキュリティ対策に必要な要素を抜き出して共通項としてまとめたものです。

- サイバーセキュリティ経営ガイドライン ver2.0
- JISQ15001：2017 版 附属書 A
- 重要インフラのサイバーセキュリティを改善するためのフレームワーク 1.1 版
- NIST SP800-171
- CIS Controls ver7
- ISO27001　付属書 A
- ISO27017　付属書 A
- 中小企業の情報セキュリティ対策ガイドライン第 3 版
- PCI_DSS_v3.2

業務委託先企業の管理にすぐに活用できるツールです。



業務委託契約書

株式会社ABC（以下「甲」という）と株式会社DEF（以下「乙」という）は、甲乙間における機密情報を含む業務の委託について、以下のとおり契約（以下「本契約」という）を締結する。

以降、本契約書の内容

第１条（機密情報）

本契約における「機密情報」とは、甲又は乙が相手方に開示し、かつ開示の際に秘密である旨を明示した技術上又は営業上の情報、本契約の存在及び内容その他一切の情報をいう。

ただし、開示を受けた当事者が書面によってその根拠を立証できる場合に限り、以下の情報は機密情報の対象外とするものとする。

(1) 開示を受けたときに既に保有していた情報

(2) 開示を受けた後、秘密保持義務を負うことなく第三者から正当に入手した情報

(3) 開示を受けた後、相手方から開示を受けた情報に関係なく独自に取得し、又は創出した情報

(4) 開示を受けたときに既に公知であった情報

(5) 開示を受けた後、自己の責めに帰し得ない事由により公知となった情報

第２条（機密情報等の取扱い）

1 甲又は乙は、相手方から開示を受けた機密情報及び機密情報を含む記録媒体若しくは物件（複写物及び複製物を含む。以下「機密情報等」という。）の取扱いについて、次の各号に定める事項を遵守するものとする。

(1) 情報取扱管理者を定め、相手方から開示された機密情報等を、善良なる管理者としての注意義務をもって適切なセキュリティ対策を施し、厳重に保管、管理する。

(2) 機密情報等は、本取引の目的以外には使用しないものとする。

(3) 機密情報等を複製する場合には、本取引の目的の範囲内に限って行うものとし、その複製物は、原本と同等の保管、管理をする。

(4) 漏えい、紛失、盗難、盗用等の事態が発生し、又はそのおそれがあることを知った場合は、直ちにその旨を相手方に書面をもって通知する。

(5) 機密情報の管理について、取扱責任者を定め、書面をもって取扱責任者の氏名及び連絡

委託先セキュリティ管理チェックシート

(契約書別添)セキュリティチェックシート

カテゴリー	#	提供サービスに関するチェック項目	対応済：○ 一部対応済：△ 未対応：× 対象外：－	対応状況		
例		貴社の安全管理に係る基本方針や、情報の取扱に関する規程類を定めていますか。	○	「個人情報保護規程」 「電子情報管理取扱規程」	情報資産の安全管理に係る基本方針、各管理段階に係る取扱規程、情報資産取扱状況の点検および監査に係る規程が整備、運用されている。	
セキュリティポリシー	1	情報の安全管理に係る基本方針や、情報の取扱に関する規程類を定めていますか。	○			
システムセキュリティ	2	サーバOS・アプリケーション等の脆弱性に対する対応ルールを定めていますか。	○			
	3	システムの権限対応門則化構成がとられていますか。	○			
	4	システムのモニタリングは実施されていますか（24時間有人監視等）。	○			
	5	システムの状態チェック(ペネトレーションテストなどの定期的な実施はありますか。	○			
ネットワークセキュリティ	6	ネットワークセキュリティに関する機器(IDS/IPS/WAFなどサンドボックス等)は導入されていますか。	○			
	7	WEB通信内容は暗号化されていますか(SSL証明書のセキュリティレベル等)。	○			

ゾーホージャパン株式会社が無償提供する「NIST SP800-171 の実践におけるヒント」および「業務委託契約書テンプレートと契約書別添セキュリティチェックシート」をすべての企業で活用していただき、サプライチェーン全体でのセキュリティ対策を完了されることを願っております。

ManageEngine について

ManageEngine は、ゾーホージャパン株式会社が提供するネットワークや IT サービス、セキュリティ、デスクトップ・ノート PC、ビジネスアプリケーションなどを管理する製品・サービス群です。必要十分な機能に限定、かつ、直感的な操作が可能な画面設計により、短期間での導入が可能であり、その後の運用フェーズにおいても手間がかからず、よりシンプルな IT 運用管理を実現します。

また、中堅・中小企業でも導入しやすいリーズナブルな価格で、これまで大手 IT ベンダーが提供する複雑で高額なツールを利用していた企業や、ツールを自社開発していた組織にも採用されてきました。現在では、日本国内の一般企業、官公庁や自治体などへ、5,000 ライセンスを超える販売実績があり、安心して使える製品・サービスです。

最大で 29 言語に対応する製品・サービスは、北米、欧州をはじめ、南米、中東、アジアなど世界で 18 万社以上の企業や組織が導入し、企業・組織の IT 運用管理のシンプル化、グローバル化に貢献しています。

ManageEngine

https://www.manageengine.jp/

ゾーホージャパン株式会社について

ゾーホージャパン株式会社は、ワールドワイドで事業を展開する Zoho Corporation Pvt. Ltd.（本社：インド　タミル・ナドゥ州チェンナイ　CEO：Sridhar Vembu）が開発/製造したネットワーク管理開発ツールや企業向け IT 運用管理ソフトウェア、企業向けクラウドサービスを日本市場に提供すると同時に関連するサポート、コンサルティングなども提供しています。

企業向け IT 運用管理ツール群「ManageEngine」は、世界 18 万社を超える顧客実績を誇り、国内でも販売本数を伸ばしています。「ManageEngine」は、ネットワーク管理の OEM 市場でスタンダードとして認知されてきたネットワーク管理開発ツール「WebNMS」のノウハウや経験を生かして開発されたものです。

また、業務改善/生産性向上を支援する企業向けクラウドサービス群「Zoho」は、世界で 4,500 万人を超えるユーザーに利用されています。国内では「Zoho CRM」を中心にユーザー数を増やしており、40 種類以上の業務アプリケーションを 1 セットで利用できる「Zoho One」の提供も始まっています。

http://www.zoho.co.jp/

【お問い合わせ先】

■報道関係からのお問い合わせ先：ゾーホージャパン株式会社　マーケティング部
Mail：jp-memarketing@zohocorp.com　TEL：045-319-4613
■お客様からのお問い合わせ先：ゾーホージャパン株式会社　営業部
Mail：jp-mesales@zohocorp.com　TEL：045-319-4612
■ゾーホージャパン URL：http://www.zoho.co.jp/
■ManageEngine 事業サイト URL：https://www.manageengine.jp/