CRS Center for Rule-making Strategies

NISTの衝撃
セキュリティの国際標準が日本のビジネスを変える

2019年 1月 29日

多摩大学
ルール形成戦略研究所 客員研究員
西尾素己

TAMA UNIVERSITY 多摩大学

1. Who am I

西尾　素己

多摩大学　ルール形成戦略研究所 客員研究員

コンサルティングファーム

米軍事系シンクタンク

幼少期より世界各国の著名ホワイトハットと共に互いに各々のサーバーに対して侵入を試みる「模擬戦」を通じてサイバーセキュリティ技術を独学。

2社のITベンチャー企業で新規事業立ち上げを行った後、セキュリティベンダーにてAndroidアプリから軍事衛星（公表不可）まで幅広い脅威分析と、未知の攻撃手法とそれらに対応する防衛手法の双方についての基礎技術研究に従事。CODE BLUE 2015ではiOSに存在する未知の脆弱性と世界初となる外部ガジェットによるiOSマルウェアの検知手法について学生枠を除く最年少として登壇、特許を取得。

大手検索エンジン企業ではCISO補佐の立場で、サイバー攻撃対策や社内ホワイトハット育成、キャピタルファンドへの技術協力などに従事。

2016年11月よりコンサルティングファームに参画。同時に多摩大学ルール形成戦略研究所にサイバーセキュリティ領域における国際標準化研究担当の客員研究員として着任。2017年にサイバーセキュリティの視点から国際動向を分析するYoung Leadersとして米軍事系シンクタンクに着任。

2. CRSの活動

ルール形成戦略研究所　CRS：Center for Rule making Strategy

役職	氏名	所属等（一部省略）
所長/教授	國分　俊史	コンサルティングファーム 執行役員 パシフィック・フォーラム シニアフェロー
シニア フェロー	甘利　明	衆議院議員　前TPP担当大臣、経済再生担当大臣
副所長	徳岡　晃一郎	多摩大学大学院 教授／経営情報学研究科長 フライシュマンヒラード　パートナー
副所長	ブラッド・グロッサーマン	パシフィック・フォーラム 元エグゼクティブディレクター
副所長	羽生田　慶介	コンサルティングファーム 執行役員
客員教授	福田　峰之	前衆議院議員　前内閣府副大臣、前内閣府大臣補佐官
客員教授	藤井　敏彦	防衛装備庁　長官官房審議官（経産省からの出向）
客員教授	角南　篤	政策研究大学院大学 副学長　内閣府参与 笹川平和財団　海洋政策研究所　所長
客員教授	渡辺　秀明	前防衛装備長長官
客員教授	市川　芳明	日立製作所　社会イノベーション協創統括本部　チーフアーキテクト室長
客員教授	井形　彬	笹川平和財団フェロー、日本再建イニチアチブ研究員
客員教授	米谷　三以	経済産業省　通商政策局　通商法務官
客員教授	岡田　宏記	フジテレビにて報道番組のプロデューサーを長年担当

自民党政務調査会にて、NIST主導で進んでいるサイバーセキュリティの国際ルール形成に対する日本としての対応案を協議

2017年3月23日（木）
IT戦略特命委員会
サイバーセキュリティ小委員会
「NIST主導でのサイバーセキュリティ技術の標準化によって包囲される日本のIoTビジネス」

↓

↑

2017年3月22日（水）
経済構造改革特命委員会
「日本版NIST創設の論点」

3. 安全保障としてサイバーセキュリティを見る

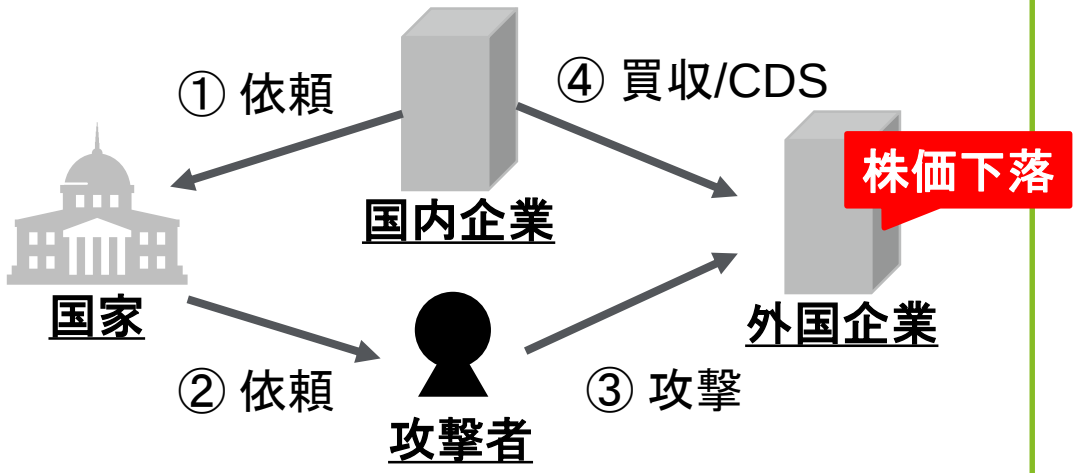
サイバー攻撃の主な動機にはネーションバック、ハクティビズム、金銭目的が存在し、中でもネーションバックでは戦略的なサイバー攻撃が繰り広げられる

サイバー攻撃の動機

ネーションバック	国が国をターゲットとして、相手の国力を削ぐことを目的にサイバー攻撃を実施する
ハクティビズム	政治的、宗教的な主張をハッキング行為によって世界に示す
金銭目的	ランサムウェアやDDoS攻撃などからの復旧を引き換えに身代金を要求する

ネーションバックにおけるポイント

1. 国家規模の資金や組織力が不要
2. 攻撃元特定が困難
3. 安全保障を盾とした国策展開が容易



4. 安全保障を梃にした経済政策

米国は安全保障政策として中国製のIT機器の利用禁止を米政府および米政府と取引する企業（政府のデータを保有する企業も含む）に対して順次実施

米国における中国製品への対応の動向

2018年4月

中国製品に対するリスク提言レポート

Supply Chain Vulnerabilities from China in U.S. Federal Information and Communications Technology

APRIL 2018

Table 2
Examples of Federal ICT Suppliers Connected to Entities of Concern

Entity Name	Risk	Details	Source

- 米中経済安全保障調査委員会が高リスクの中国のICTサプライヤのリストを提示

投影のみ

2018年8月

直近の中国製品締め出しの動き

115TH CONGRESS
2D SESSION

H. R. 5515

SEC. 889. PROHIBITION ON CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE
(a) PROHIBITION ON USE OR PROCUREMENT.—(1) The head of an executive agency may not—

(B) enter into a contract (or extend or renew a contract) with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system.

by Huawei Technologies Company or ZTE Corporation

- 8月13日「2019年度国防権限法」成立
- 政府機関に対し、ZTE社、Huawei社を含む中国企業5社の電子通信製品の取引を禁止
- さらに、**これら5社の製品を(部分的にでも)システム内に利用する組織との取引も禁止**

オーストラリアの5Gプロジェクトにおいても、重要情報漏えいへの懸念からHuawei社およびZTE社製品の締め出しが決定された

オーストラリアにおける5GプロジェクトにおけるHuawei・ZTE製品の利用禁止の動向

2018年7月

REUTERS World Business Markets Politics TV

Detained In Myanmar | Energy & Environment | Brexit | North Korea | Charged: The Future of Autos | Future of Money

BUSINESS NEWS JULY 11, 2018 / 5:57 PM / 2 MONTHS AGO

Australia prepares to ban Huawei from 5G project over security fears

Colin Packham 6 MIN READ

SYDNEY (Reuters) - Australia is preparing to ban Huawei Technologies Co Ltd from supplying equipment for its planned 5G broadband network after its intelligence agencies raised concerns that Beijing could force the Chinese telco to hand over sensitive data, two sources said.

2018年8月

日本経済新聞

2018年8月30日（木）

トップ 経済・政治 ビジネス マーケット テクノロジー 国際・アジア スポーツ 社会

速報 朝刊・夕刊

豪政府、華為・ＺＴＥの５Ｇ参入禁止 中国包囲網広がる

2018/8/24付 ［有料会員限定］

保存 共有 印刷 その他

【広州＝中村裕】中国通信機器の２大メーカーの華為技術（ファーウェイ）と中興通訊（ＺＴＥ）が、オーストラリア政府から次世代高速通信「５Ｇ」の参入を正式に禁止されたことが23日、明らかになった。同国政府は、５Ｇの技術を介し、中国メーカー側に重要情報が漏洩することを危惧した。米国も中国２社に対し、厳しい参入制限を行っている。中国包囲網が世界で広がってきた。

５Ｇ参入禁止の決定を受け、ファーウェイの現地法人は23日、「非常に残念な結果だ。我々は５Ｇの世界でリーダーだ。オーストラリアでは既に15年近く、無線技術を安全に提供してきた」との声明を発表した。現在主流の第４世代（４Ｇ）の通信用設備ではファーウェイのオーストラリアでのシェアは５割超と高い占有率を誇っている。

テレコミュニケーション及びビデオ監視サービスの調達について、国防権限法（NDAA FY2019 ）により国家の安全保障上の懸念につながる特定の会社をサプライヤーから排除した

国防権限法（NDAA FY2019）によるサプライヤー排除の対象

合衆国議会

政府のシステム調達におけるサプライヤーの制限

政府機関

規制対象会社	規制内容
ZTE HUAWEI	■Huawei Technologies CompanyまたはZTE Corporation（またはそのような事業体の子会社または関連会社）によって製造された通信機器
Hytera H3C alhua TECHNOLOGY	■Hytera、Hangzhou Hikvision、Dahua（またはそのような事業体の子会社または関連会社）によって製造されたビデオ監視および通信機器
特定なし	■指定された会社またはその会社が生産している製品を使用して供給される通信機器及びビデオ監視機器
特定なし	■国防長官が外国の政府によって所有または管理されている会社であると合理的に考えられる会社が、製造または提供している通信機器またはビデオ監視機器

5. CUIプログラムとNISTフレームワーク

民間企業が取り扱う（機密情報以外の）重要情報を保護するためのガイドラインとして策定されたSP800-171は、今後さらに米国政府調達規制化により産業展開が進む見込み

SP800-171の調達規制化までの動向

CUIと保護策の定義

CUI保護方法の決定とルール形成

2010年11月9日	2010年～2011年	2015年6月	2016年5月14日	2016年9月14日
大統領令（Executive Order）13556	各省庁によるCUIレジストリーへの情報登録	CUI保護技術体系 NIST SP800-171	連邦調達規制（FAR）52.204-21	32 連邦規則（CFR）2002.14

① 各省庁は国立公文書記録管理局（NARA）が管理するCUIレジストリーにCUIを登録すること

② NISTが開発、発行するガイドラインに従ってCUIを適切に保護すること

32 連邦規則（CFR）2002.14では、CUIを「処理、格納、通信」する民間企業のシステムはNIST SP 800-171による保護をミニマムにすることがCUIを保有を求めた

SP800-171の強度に関する緩和策の提案は棄却されている

連邦調達規制 FAR 52.204-21は2019年中に全省庁の政府調達で有効化される見込み

各省庁によりレジストリ登録されたCUIは多様な産業に跨って存在するため、北米事業を行う日本企業は当該情報を取り扱っている可能性が高い

CUIレジストリに登録されている業種別CUIの例

業種	CUI（一例）
自動車	● DHSへの申請情報（自動運転試験走行など） ● テストと評価の結果（耐久性情報や自動運転走行における事故情報など） ● 内部マニュアル
電力・ガス	● インフラへの攻撃を計画するあたり有用である可能性がある情報 ● エネルギーの生産、生成、輸送、伝達、または配分に関する詳細情報 ● 原子力施設、材料、兵器に関する特定の設計およびセキュリティ情報
ヘルスケア	● 個人の過去、現在、または将来の身体的または精神的な健康状態 ● 個人への健康管理の提供記録 ● 化学薬品の使用、保管、または取扱い、および関連システム
重化学工業	● 軍事、宇宙関連情報 ● 流出が米政府にとって不利になる特許情報 ● 既存もしくは研究開発中の製品設計及び性能仕様情報
食品	● 農業に関する経営情報、保全実務情報 ● 農薬生産者情報、害虫情報 ● 水の処理方法と水質に関する詳細情報（バイオテロ対策）
IoT家電	（何に繋がり、どのような情報を処理、保有するかにより変動）

2018年1月以降の米国政府調達においてFAR 52.204-21やDFARS 252.204-7012によってNIST対応が必須化、うち1割程度はDHSを筆頭に非防衛調達であった

米国政府調達におけるNIST必須化のフロー

Executive Order 13556
(CUIの定義と保護方法を指示)

FAR 52.204-21

適応される米国政府調達に関わる全サプライヤーと納入される製品は**NIST SP800-171を満たす**必要がある

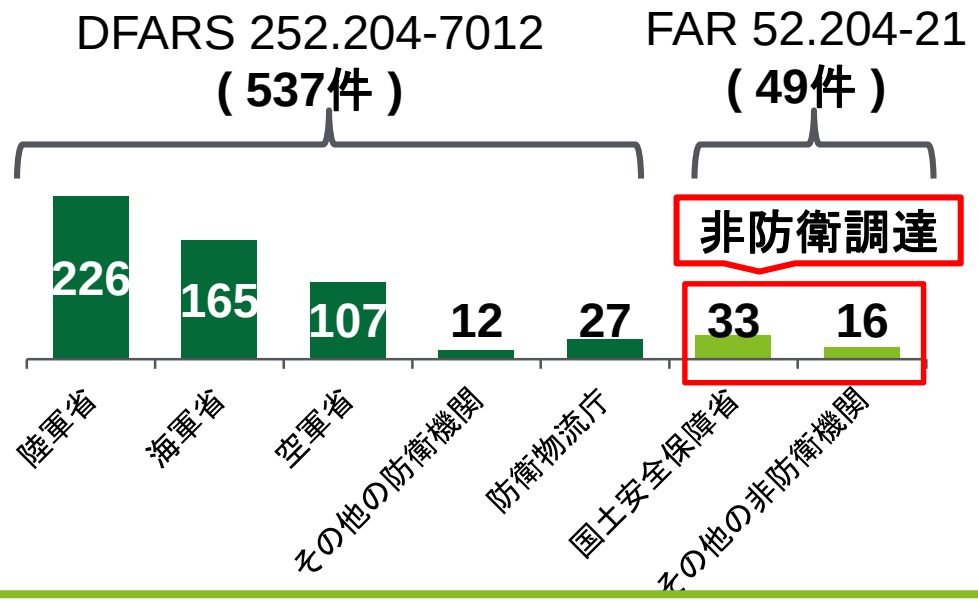
■ Replaces the other safeguarding requirements with comparable security requirements from NIST SP 800-171.

DFARS 252.204-7012

適応されるDoD配下のプロジェクトにおいて、全サプライヤーは**NIST SP800-171を満たす**必要がある

(1) By submission of this offer, the Offeror represents that it will implement the security requirements specified by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 "Protecting Controlled Unclassified

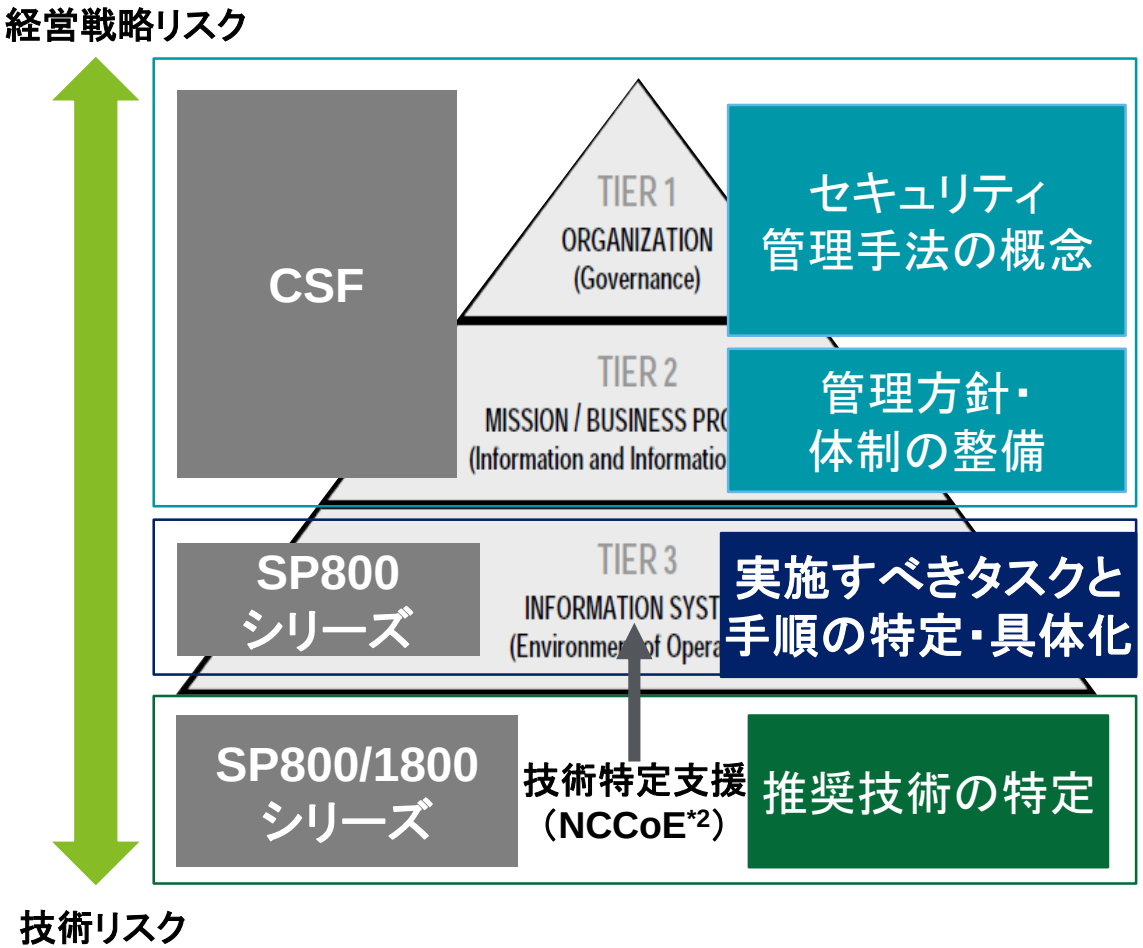
NIST対応必須の米国政府調達の分析結果



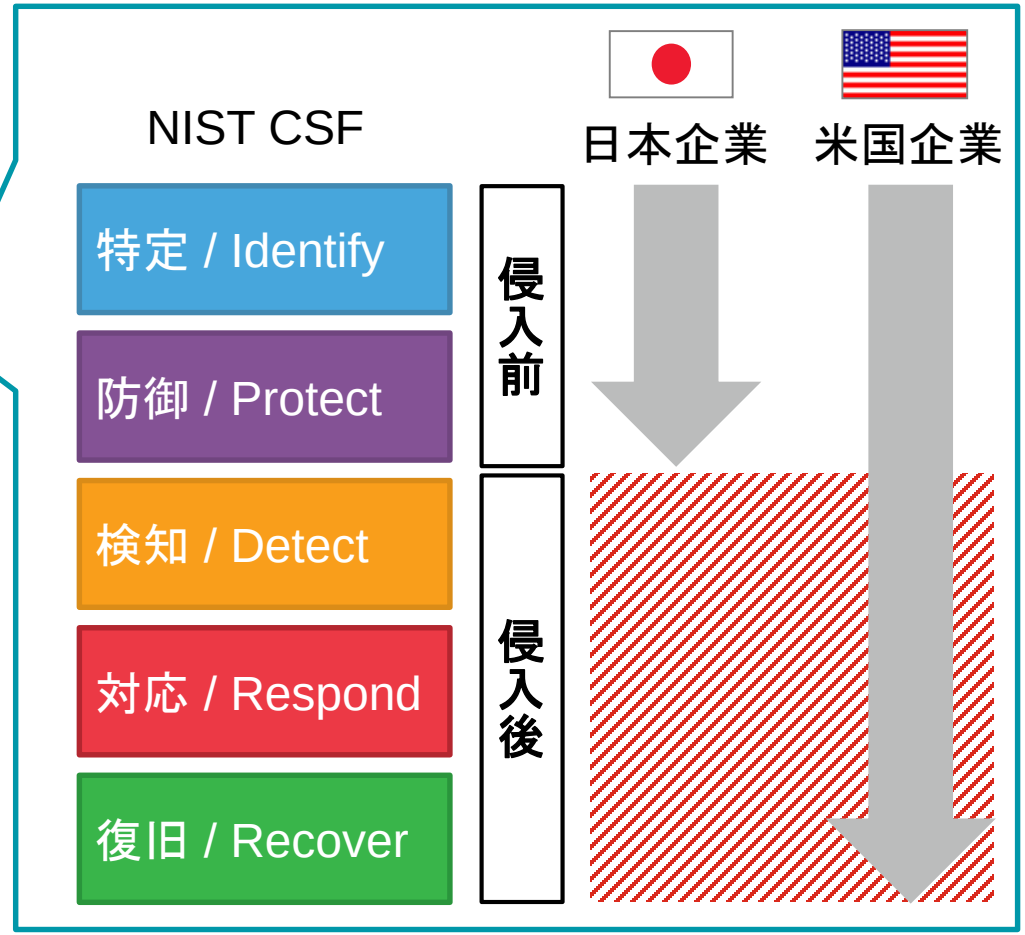
- 2018年1月1日～2018年9月13日までの一年間でNIST対応を必須とした米国政府調達は**586件**
- そのうち**1割程度は非防衛調達**であった。
- 中でもDHS（国土安全保障省）は**物流関連の調達**にNIST対応を課している
- 米国政府は2019年に向けてFAR 52.204-21をほぼすべての省庁の調達要件とするとしている

NISTはサイバーセキュリティ基準のミニマムスタンダードとして、組織レベルから業務プロセス、情報システムといった技術レベルまでカバーするガイドライン群を作成

NISTの定義するサイバーセキュリティ対策のアプローチ



NIST CSF (Cybersecurity Framework)



米国では重要インフラのセキュリティフレームワークが18カテゴリー400以上の項目でカバーされるNIST CSFをベースとして作成されサプライヤーは準拠を求められ始めている

NIST対応が必要な米の重要インフラの分類

重要インフラの分類	
化学	医療・公衆衛生
商業施設	食糧・農業
重要製造業	政府施設
ダム	金融
防衛産業	情報技術
救急	通信
原子力	エネルギー
交通	上下水道

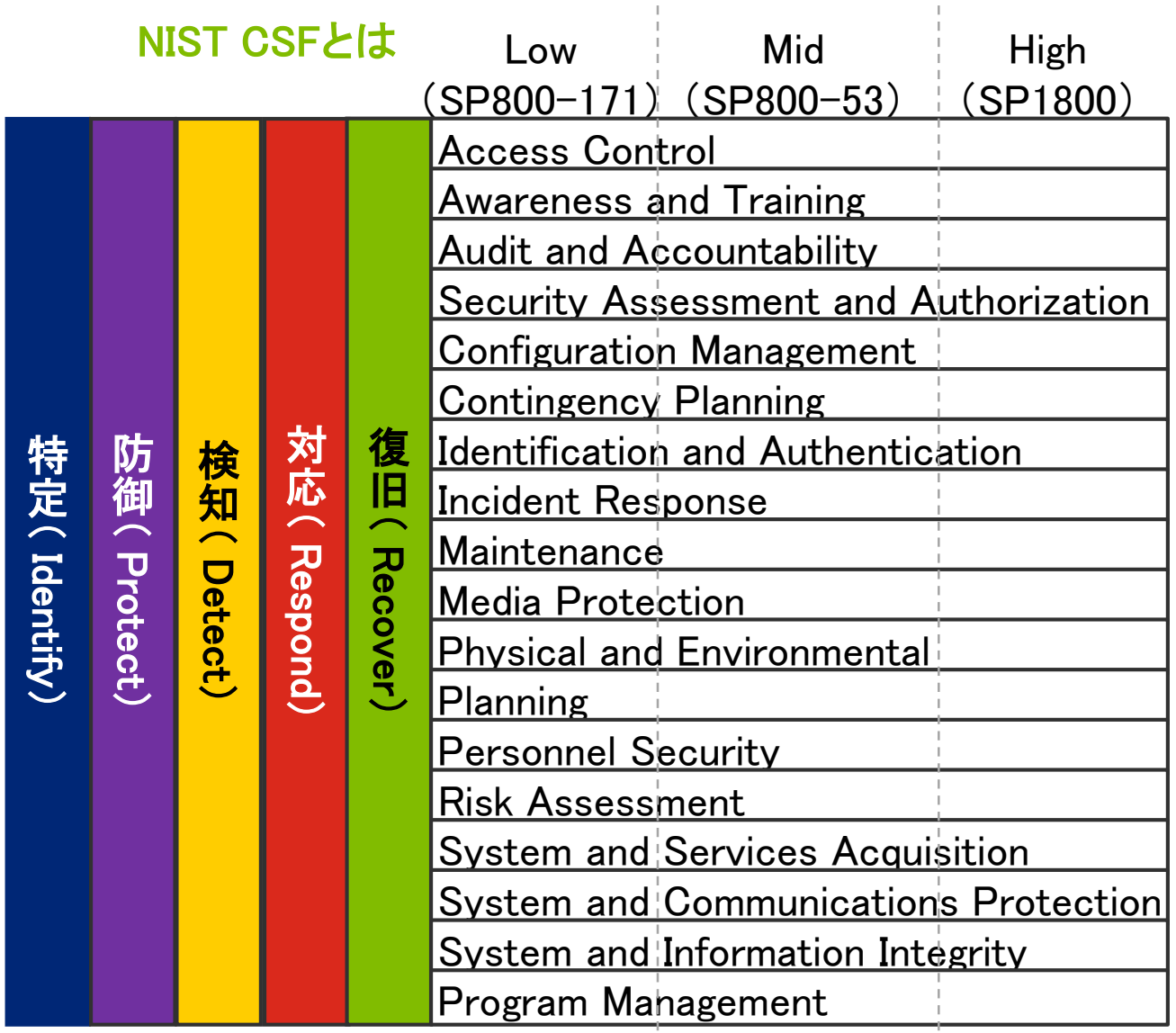
DHS主導

NIST主導

業界主導

NIST CSFをベースに業界特有の項目を検討し追加する際にはCSFの既存項目を緩和し独自のセキュリティフレームワークを開発・運用している

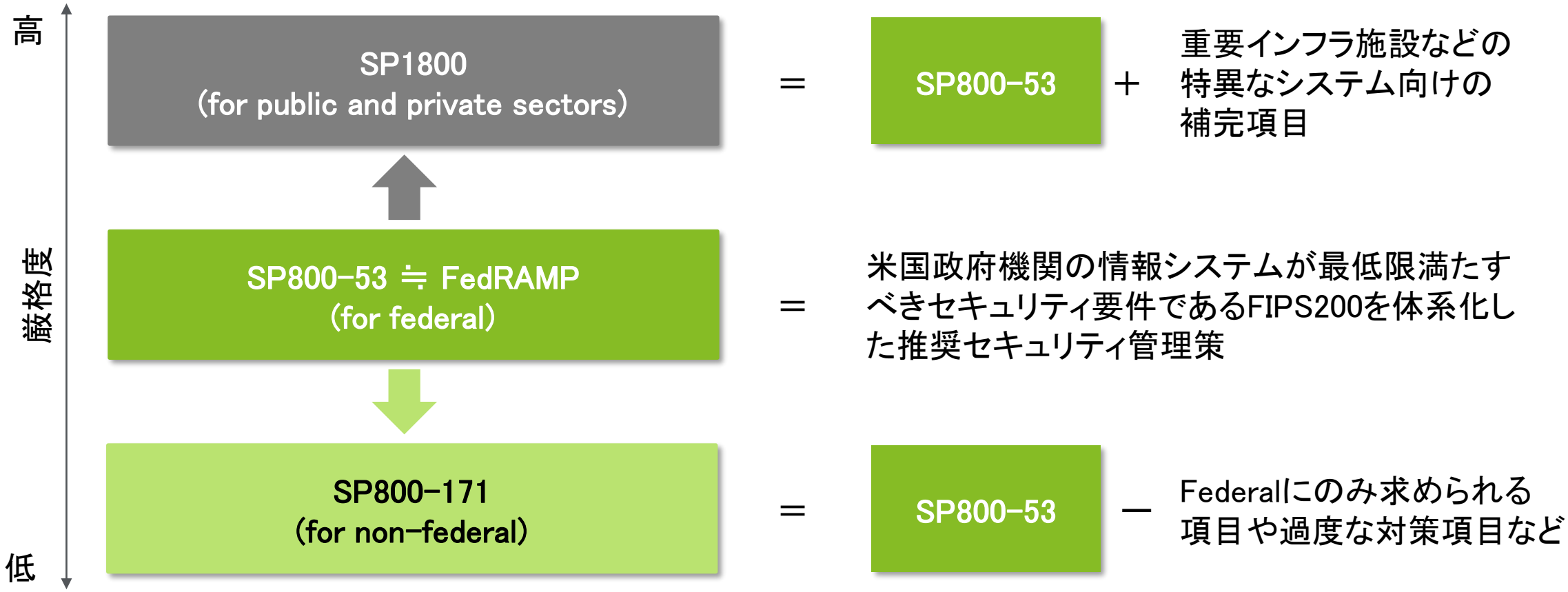
NIST CSFとは



	Low（SP800-171）	Mid（SP800-53）	High（SP1800）
Access Control			
Awareness and Training			
Audit and Accountability			
Security Assessment and Authorization			
Configuration Management			
Contingency Planning			
Identification and Authentication			
Incident Response			
Maintenance			
Media Protection			
Physical and Environmental			
Planning			
Personnel Security			
Risk Assessment			
System and Services Acquisition			
System and Communications Protection			
System and Information Integrity			
Program Management			

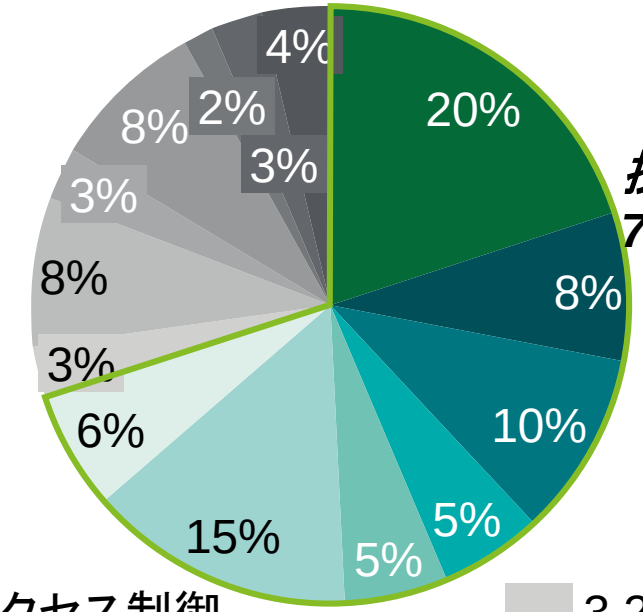
NIST SP800-171を厳格化したものとして、SP800-53を認証制度化したFedRAMP、SP1800が存在する

FedRAMPとNIST SP800、SP1800シリーズの関係



実施すべき具体的なタスクと手順を、CSFから特定・具体化した、SP 800-171には技術要件が77項目、非技術要件が33項目存在し、その多くを技術要件が占める

分類ごとの項目数割合と要件分類



技術要件が70%を占める

- 3.1 アクセス制御
- 3.4 構成設定管理
- 3.5 識別と認証
- 3.7 メンテナンス
- 3.10 物理的保護
- 3.13 システムと通信の保護
- 3.14 システムと情報の完全性
- 3.2 意識と訓練
- 3.3 監査と責任追跡性
- 3.6 インシデントレスポンス
- 3.8 メディア保護
- 3.9 人的セキュリティ
- 3.11 リスクアセスメント
- 3.12 セキュリティアセスメント

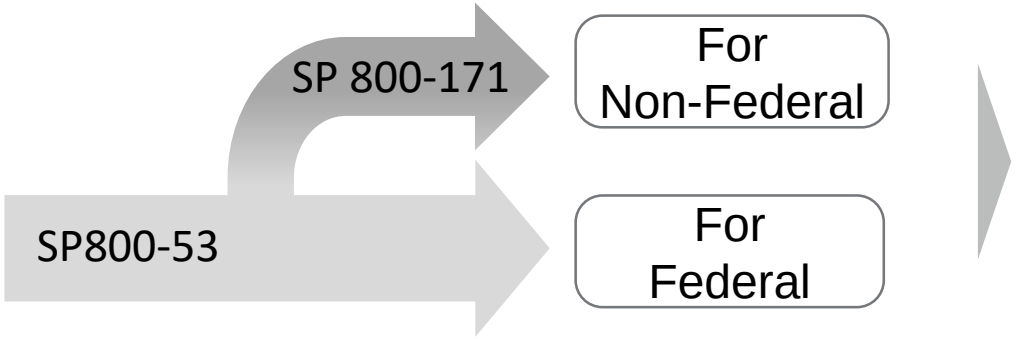
技術要件 (77項目)		
3.1	アクセス制御	22項目
3.4	構成設定管理	9項目
3.5	識別と認証	11項目
3.7	メンテナンス	6項目
3.10	物理的保護	6項目
3.13	システムと通信の保護	16項目
3.14	システムと情報の完全性	7項目

非技術要件 (33項目)		
3.2	意識と訓練	3項目
3.3	監査と責任追跡性	9項目
3.6	インシデントレスポンス	3項目
3.8	メディア保護	9項目
3.9	人的セキュリティ	2項目
3.11	リスクアセスメント	3項目
3.12	セキュリティアセスメント	4項目

SP 800-171は、Federal(政府機関)向けの要件であるSP 800-53を基に、個々の要求強度を下げずにNon-Federal(民間組織)向けの要件を抽出したものである

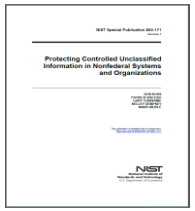
SP 800-171とSP 800-53の関係(1/2)

■SP 800-53 を基に、Non-Federal向けに要件を抽出



■個々の要求強度（レベル）はSP 800-53と同等

■ NIST Special Publication 800-171



Organizations can use Special Publication 800-53 to obtain additional, non-prescriptive information related to the security requirements (e.g., supplemental guidance related to each of the referenced security controls, mapping tables to ISO/IEC security controls, and a catalog of optional controls that can be used to help specify additional security requirements if needed). **This information can help clarify or interpret the requirements in the context of mission and business requirements, operational environments, or assessments of risk. Nonfederal organizations can implement a variety of potential security solutions either directly or using managed services, to satisfy the security requirements and may implement alternative, but equally effective, security measures to compensate for the inability to satisfy a requirement.**

「SP 800-53の要件を理解することでSP 800-171の要件の実装レベルの理解が支えられ、これによりSP 800-171要件に準拠したセキュリティ対策を実装することが可能になる」

The confidentiality impact value for CUI is **no less than *moderate*** in accordance with Federal Information Processing Standards (FIPS) Publication 199.

~Page 5

The moderate impact *value* defined in FIPS Publication 199 may become part of a moderate impact *system* in FIPS Publication 200, which in turn, requires the use of the moderate security control baseline in **NIST Special Publication 800-53** as the starting point for tailoring actions.

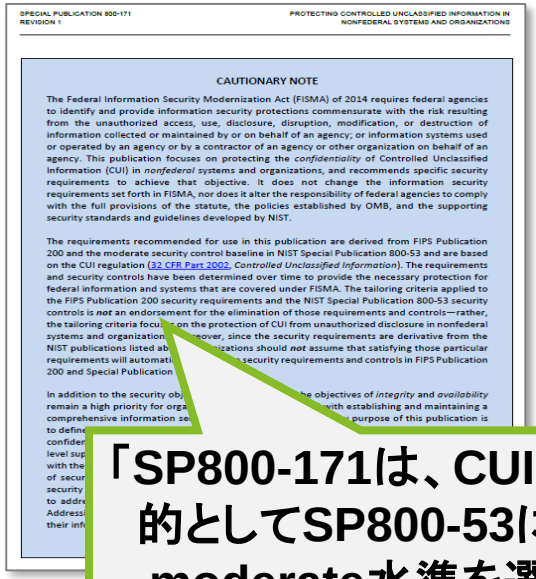
Page5, footnote 14

「CUIの機密影響値はNIST SP 800-53のModerateに劣らない」

SP 800-171はCUI保護に必要な要件をSP800-53から抽出するための“カタログ”に過ぎないため、準拠のためにSP800-53を参照すべき

SP 800-171とSP 800-53の関係(2/2)

SP800-171 rev1


SPECIAL PUBLICATION 800-171 REVISION 1

PROTECTING CONTROLLED UNCLASSIFIED INFORMATION IN NONFEDERAL SYSTEMS AND ORGANIZATIONS

CAUTIONARY NOTE

The Federal Information Security Modernization Act (FISMA) of 2014 requires federal agencies to identify and provide information security protections commensurate with the risk resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of an agency; or information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. This publication focuses on protecting the *confidentiality* of Controlled Unclassified Information (CUI) in *nonfederal* systems and organizations, and recommends specific security requirements to achieve that objective. It does not change the information security requirements set forth in FISMA, nor does it alter the responsibility of federal agencies to comply with the full provisions of the statute, the policies established by OMB, and the supporting security standards and guidelines developed by NIST.

The requirements recommended for use in this publication are derived from FIPS Publication 200 and the moderate security control baseline in NIST Special Publication 800-53 and are based on the CUI regulation (32 CFR Part 2002, *Controlled Unclassified Information*). The requirements and security controls have been determined over time to provide the necessary protection for federal information and systems that are covered under FISMA. The tailoring criteria applied to the FIPS Publication 200 security requirements and the NIST Special Publication 800-53 security controls is *not* an endorsement for the elimination of those requirements and controls—rather, the tailoring criteria focu... on the protection of CUI from unauthorized disclosure in nonfederal systems and organizations. Moreover, since the security requirements are derivative from the NIST publications listed ab... izations should *not* assume that satisfying those particular requirements will automati... security requirements and controls in FIPS Publication 200 and Special Publication ...

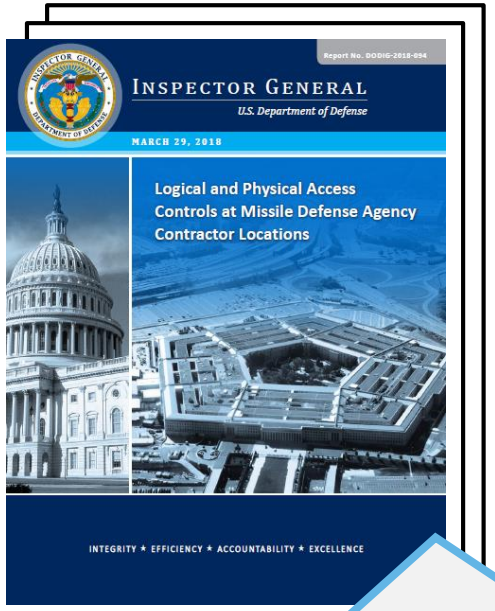
In addition to the security obj... the objectives of *integrity* and *availability* remain a high priority for orga... with establishing and maintaining a comprehensive information se... purpose of this publication is to define... confider... level sup... with the... of secur... security ... to addre... Address... their inf...

「SP800-171は、CUI保護を目的としてSP800-53におけるmoderate水準を選択して構築された」

SP800-171	SP800-53
3.1.1 アクセスを認可したユーザとプロセスに制限せよ	AC-2 アカウント管理
3.1.2 トランザクションと機能を、認可ユーザが許可した種別に制限せよ	AC-3 アクセス強制
3.1.3 CUIの情報フローを制御せよ	AC-17 リモートアクセス
3.1.4 責務の分離を実施せよ	AC-4 情報フロー強制
3.1.5 最小特権原則を採用せよ	AC-5 責務の分離
⋮	AC-6 最小特権
	⋮

米国防衛業界では、DoD IGがMDA管轄のBMDSに関する契約者に対して抜き打ちでSP800-171準拠状況の監査を実施した

【参考】防衛業界におけるDFARS/SP800-171準拠状況監査の概要 (1/2)

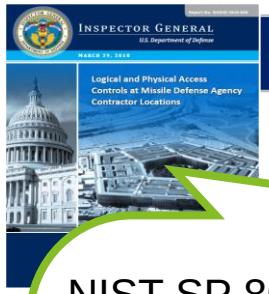


2017年3月~12月にかけて、国防総省(DoD)下の 独立監視機関であるDoD IGは、弾道ミサイル防衛システム(BMDS)を構成する、制御すべき非機密技術情報(UCTI)をミサイル防衛局(MDA)の契約者が、DFARSが要求するP800-171に沿って保護しているか、監査を実施した。

調査項目	未準拠割合
多要素認証の実施	5/7
パスワードの複雑さ	4/7
定期的なシステムリスク評価の実施	7/7
サードパーティのネットワーク保護監視	1/7
制御すべき非機密技術情報の個人端末での利用禁止	1/7
リムーバブルメディアの適切な保護	5/7
不活動期後または制限回数超過後のログオン試行の自動ロック	5/7
システムへのアクセス制御と特権管理	5/7
システム活動報告の適切な維持とレビュー	4/7

監査における準拠性判定の根拠にはSP800-53の要件が引用されており、実質的にSP800-53の粒度での対応が強制されると見ることができる

【参考】防衛業界におけるDFARS/SP800-171準拠状況監査の概要 (2/2)



指摘事項の例（監査レポート抜粋）

NIST SP 800-171 requires contractors to periodically scan systems and applications to identify vulnerabilities, mitigate those vulnerabilities, and develop plans of action and milestones when contractors are unable to **mitigate vulnerabilities in a timely manner**. We compared unclassified network scan results from [省略] for Contractors A, B, C, E, and G and found that **server and workstation vulnerabilities were not mitigated in a timely manner.**

「防衛サプライヤは【（組織が定めた）一定の時間】に脆弱性へのパッチ適用を完了しなければならない」という要件を参照した上で、「不適合」と判定

SP800-171要件の記載

3.11.3 Remediate vulnerabilities in accordance with assessments of risk.

- 目的・アクション(What)を中心に記載
- 推奨技術や要求強度(How)は800-53参照

(3.11.3に紐づく) 53コントロールの記載

RA-5 VULNERABILITY SCANNING

a. Scans for vulnerabilities in the information system and hosted applications [*Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process*] and when new vulnerabilities potentially affecting the system/applications are identified and reported;

b. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and

1. Enu
2. Forn
3. Mea

c. Analyzes

d. Remedia accordan

e. Shares in assessme similar v deficienc

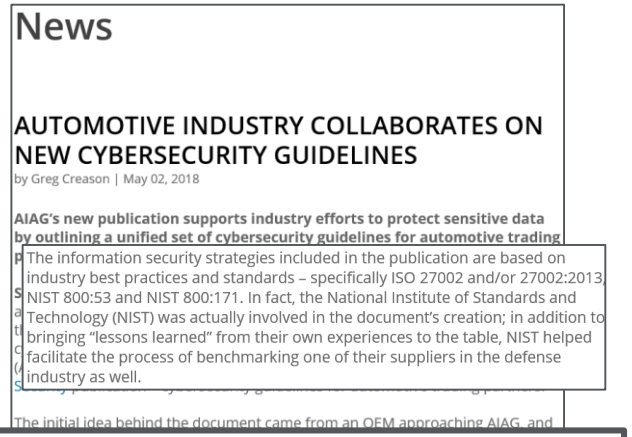
Supplemental comprehensiv scanning for

d. Remediates legitimate vulnerabilities [*Assignment: organization-defined response times*] in accordance with an organizational assessment of risk(略)

脆弱性への対応について「組織は【一定の時間】定義しなければならない」ことの要求はSP800-53にのみ記載されている

米国ではさらに、民間独自の取り組みとして各産業でNISTを参照するセキュリティガイドラインが設けられ、業界ごとにセキュリティの底上げに取り組んでいる

自動車業界における民間独自の取り組み


News

AUTOMOTIVE INDUSTRY COLLABORATES ON NEW CYBERSECURITY GUIDELINES

by Greg Creason | May 02, 2018

AIAG's new publication supports industry efforts to protect sensitive data by outlining a unified set of cybersecurity guidelines for automotive trading

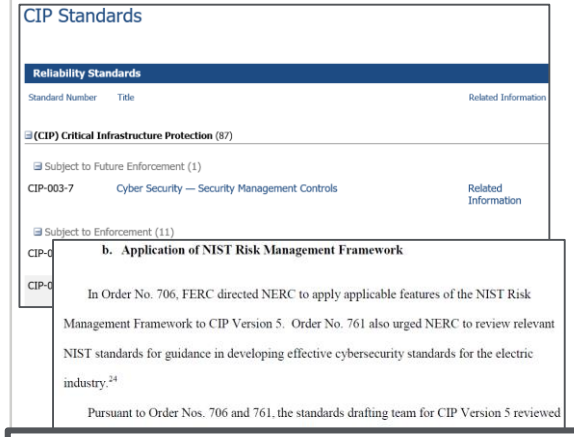
The information security strategies included in the publication are based on industry best practices and standards – specifically ISO 27002 and/or 27002:2013, NIST 800:53 and NIST 800:171. In fact, the National Institute of Standards and Technology (NIST) was actually involved in the document's creation; in addition to bringing "lessons learned" from their own experiences to the table, NIST helped facilitate the process of benchmarking one of their suppliers in the defense industry as well.

The initial idea behind the document came from an OEM approaching AIAG, and

- 2018年5月2日 AIAG(全米自動車産業協会)は参加企業に向けて**NIST SP800-171に基づく**サイバーセキュリティ対策のガイドラインを発行

AIAG Automotive Industry Action Group

エネルギー業界における民間独自の取り組み


CIP Standards

Reliability Standards

Standard Number | Title | Related Information

(CIP) Critical Infrastructure Protection (87)

Subject to Future Enforcement (1)

CIP-003-7 Cyber Security — Security Management Controls — Related Information

Subject to Enforcement (11)

b. Application of NIST Risk Management Framework

In Order No. 706, FERC directed NERC to apply applicable features of the NIST Risk Management Framework to CIP Version 5. Order No. 761 also urged NERC to review relevant NIST standards for guidance in developing effective cybersecurity standards for the electric industry.[24]

Pursuant to Order Nos. 706 and 761, the standards drafting team for CIP Version 5 reviewed

- NIST CSFを元にチェックリスト方式で最低限のセキュリティ対策が示され、大規模発送電設備における順守を義務付け

NERC NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

NISTによる技術実装に関するベストプラクティス(SP1800)展開

文書番号	テーマ	対象業界
SP1800-1	モバイル機器上の電子健康記録のセキュリティ対策	医療
SP1800-2	エネルギー業界におけるアイデンティティ及び資産管理	エネルギー
SP1800-5	IT資産管理	金融
SP1800-7	状況認識(監視)	エネルギー
SP1800-8	ワイヤレス輸液ポンプのセキュリティ対策	医療
SP1800-9	アクセス権管理	金融

⋮

- NIST SP800準拠のセキュリティ対策について、各業界における実務的なベストプラクティスとしてSP1800文書群が作成、公開されている

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE — NIST National Institute of Standards and Technology U.S. Department of Commerce

欧州では2018年から欧州で活動する企業に対し国際標準で定められたサイバーセキュリティ技術の利用を2016年8月に法律で義務付けた

欧米市場の法制度の変化

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

米国立標準研究所

- 国防総省と取引のあるサプライヤーは2017年12月31日までにNIST　SP800-171の技術体系で構築された社内システムに移行することを要請する通達を発行
- 2018年の途中からアメリカ市場で取引する事業者にはSP800-171もしくはSP800-53の技術体系で構築されたシステムに移行しなければ米国での活動が出来なくなる方針

EUROPEAN COMMISSION

欧州理事会

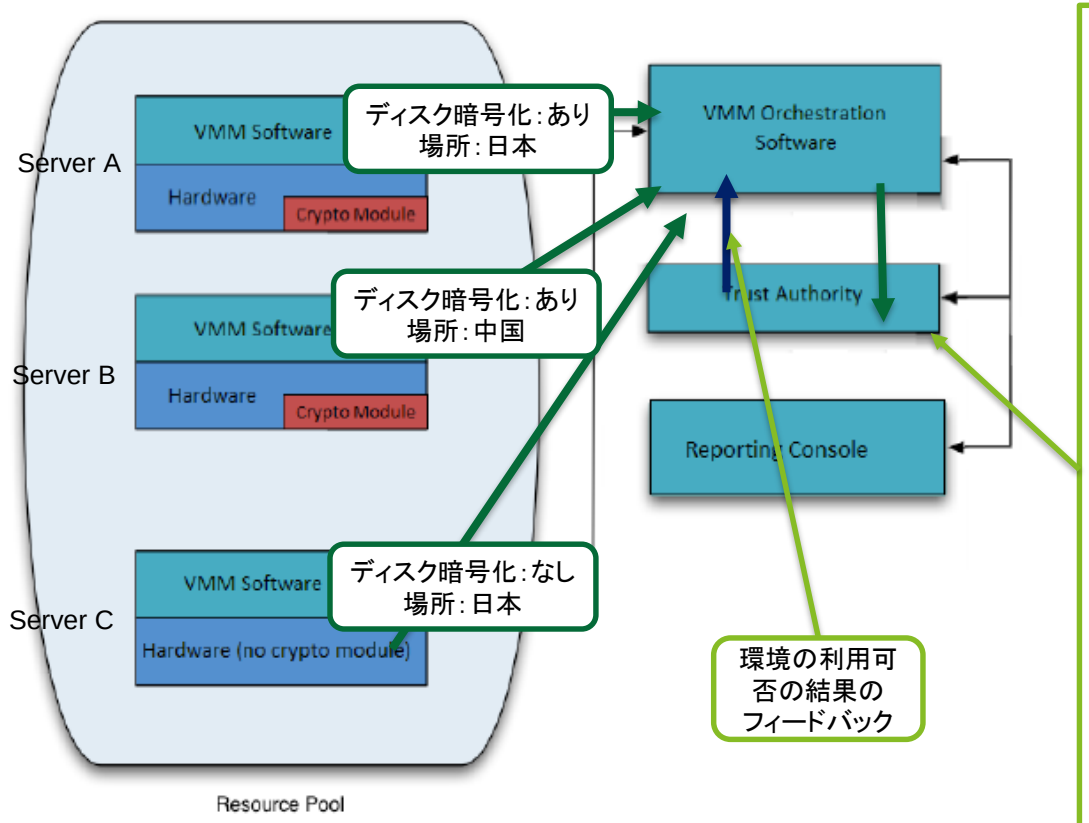
enisa
European Network and Information Security Agency

欧州ネットワーク情報セキュリティ庁

- 2018年5月10日までに、国際標準で定められたサイバーセキュリティ技術を用いた社内システムに移行しなければ、欧州での事業活動が許されない法律が発効
- 上記のシステム変更以降を前提に2018年5月25日よりGDPRの運用を開始し、情報漏洩企業にはグループ連結売上の4%の罰金を課していく方針

クラウドが動作する基盤の属性情報（設置場所、パッチ、対策ソフトの有無など）を収集・格納し、属性情報を基準にしたリソースの利用の統制・選択を可能にする

ソリューションの基本構想



*1: NISTIR 7904より抜粋

- セキュリティポリシーの定義

項目	条件
ディスク暗号化	必須
設置許可場所	日本

- 利用可否判定前のカタログ（属性情報収集後）

リソース名	利用可否	ディスク暗号化	設置場所
Server A		Y	日本
Server B		Y	中国
Server C		N	日本

- 利用可否判定後のカタログ

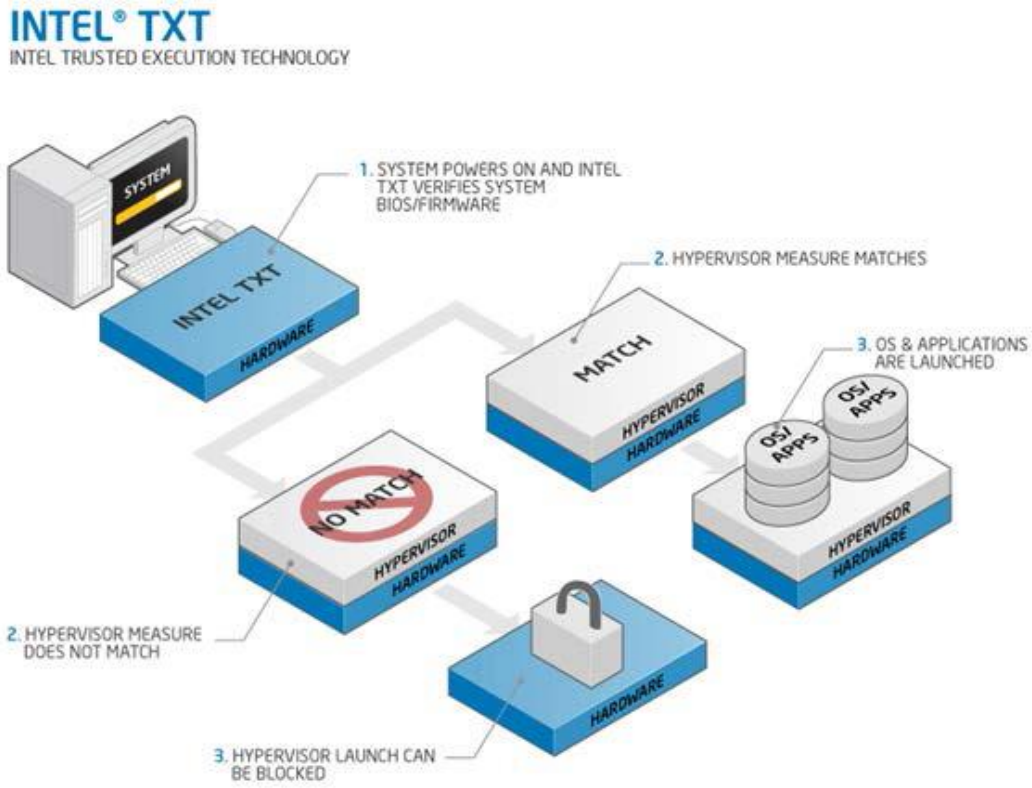
リソース名	利用可否	ディスク暗号化	設置場所
Server A	Y	Y	日本
Server B	N	Y	中国
Server C	N	N	日本

- サービスの元締めソフトウェアに連携

具体的な検証技術例：Intel Trusted Execution Technology (Intel TXT)を利用した、チップレベルでの基盤の属性情報のコントロールが可能となる

Intel Trusted Execution Technology

- Intel Trusted Execution Technology(Intel TXT)はチップレベルで属性情報を保持し、必要応じてその情報を共有する技術となります。
- Intel TXTは設置されているサーバのBIOSのバージョンやパッチレベル、ポートの設定情報収集し、格納します。
- そのサーバにてクラウドサービス用のゲストOSを動かすための仮想化ソフト（Hypervisor）を起動する際に、そのサーバ内のIntel TXTの属性情報を参照し、クラウドサービスが定義したセキュリティポリシーと突合し、起動の制御を行うことができます。



*1: NISTIR 7904より抜粋

6. 日本企業の現状と採るべき対応

防衛業界向けセミナーにて防衛装備庁長官官房審議官である藤井氏から日本におけるSP800-171対応は防衛装備庁がリードしこの流れは防衛にとどまらないと明言

防衛省のサイバーセキュリティ強化の取り組み

防衛装備庁長官官房審議官
藤井 敏彦 氏

一部抜粋

NIST（米国標準技術研究所）が作成したサイバーセキュリティの標準である**SP800-171への対応は、喫緊の課題**です。
防衛装備品は、海外との共同研究・開発が大きい柱です。
したがって、パートナーである米国と共同研究・開発を行う際に、米国が日本政府、日本企業に**同等のセキュリティ基準**を求めてくることは容易に想像できます。

また、**FedRAMP**への対応も懸念事項です。
FedRAMPは米国政府のクラウド調達の基準であり、今後、**国際標準になる**と想定されます。

この動きを受けて、自民党IT戦略特命委員会は、2017年5月23日に**「日本版FedRAMP」の創設**を明言しました。そして、まずは早急な対応が見込まれる防衛産業分野を優先し、**防衛装備庁が主導**して着手することが提言された経緯があります。

もちろん、**この動きは防衛産業分野にとどまりません**。
防衛産業での成果は重要インフラ分野、さらにその他の産業分野にも活用されます。そして、日本版FedRAMPに準拠すれば、国際標準にも準拠しているといえる環境の実現を目指さなければなりません。

2017年11月28日に防衛装備庁にて新調達ガイドライン説明会が開催され、NISTと同等のサイバーセキュリティレベルの導入を企業に求める方針が発表された

3　今後の予定

○　防衛産業との意見交換

　これまで実施してきた官民検討会の枠組みを踏襲して開催し、防衛産業以外の企業についてもオブザーバーとして参加を呼びかける。

○　情報の範囲の明確化（指定基準の策定）

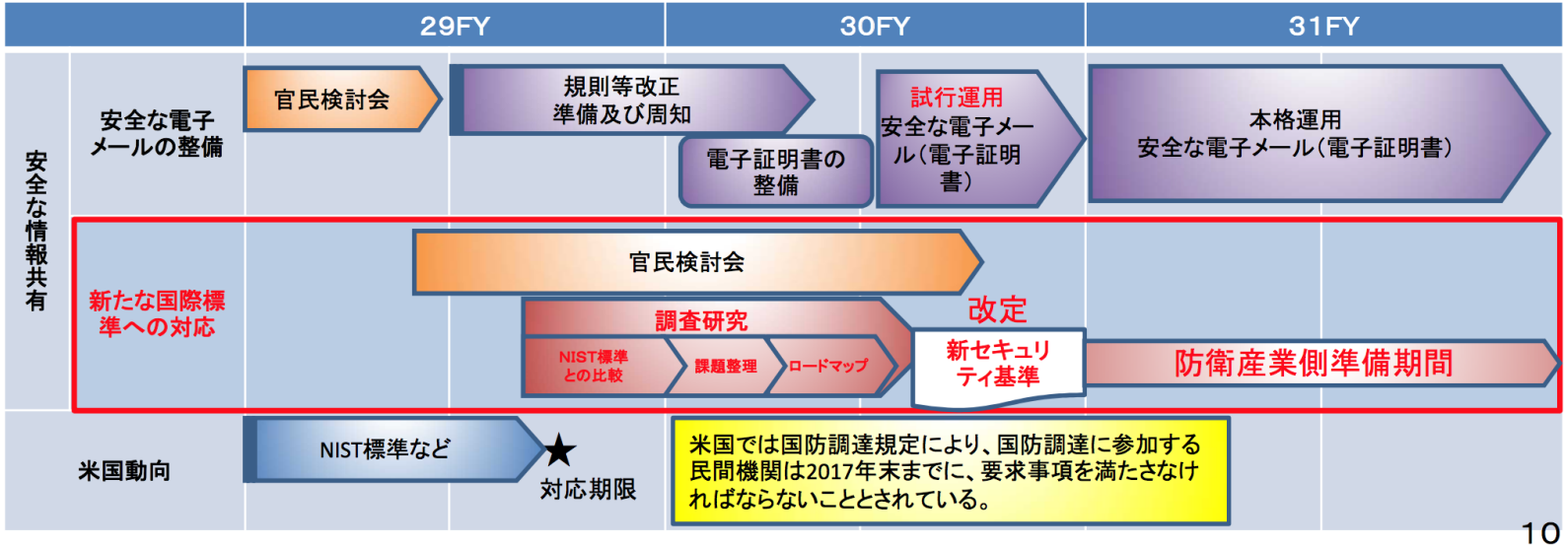
　官側において、対象となる保護情報の範囲を明確にするための「指定基準案」を作成し、今後の官民検討会での協議を踏まえ策定する。

○　サプライチェーンレベルの明確化

　新セキュリティ基準を適合される下請け企業の調査を実施する。

○　調査研究事業

　民間識者等の知見を活用し、NIST標準に適合するための差異分析、課題整理及び適合に向けたロードマップを作成する。



NIST　SP800-171の技術規格と同等の基準で社内の情報システムを構築し、CUIの管理を行うことと求めるとした

２　現在の検討状況

５　情報セキュリティルールの示し方

○　情報セキュリティ特約条項及び情報セキュリティ基準、入札時の公告、「入札及び契約心得」等におけるルールの示し方の検討

・情報セキュリティ特約条項及び情報セキュリティ基準は、NIST SP 800-171の適用の検討による新セキュリティ基準とする方向。
・情報セキュリティルールの示し方について、引き続き入札時の公告、「入札及び契約心得」へ記載する方向。
・契約前に保護すべき情報を取り扱わせる場合、情報セキュリティ特約条項を付した情報保護契約を締結する方向。

６　クラウドサービスの利用

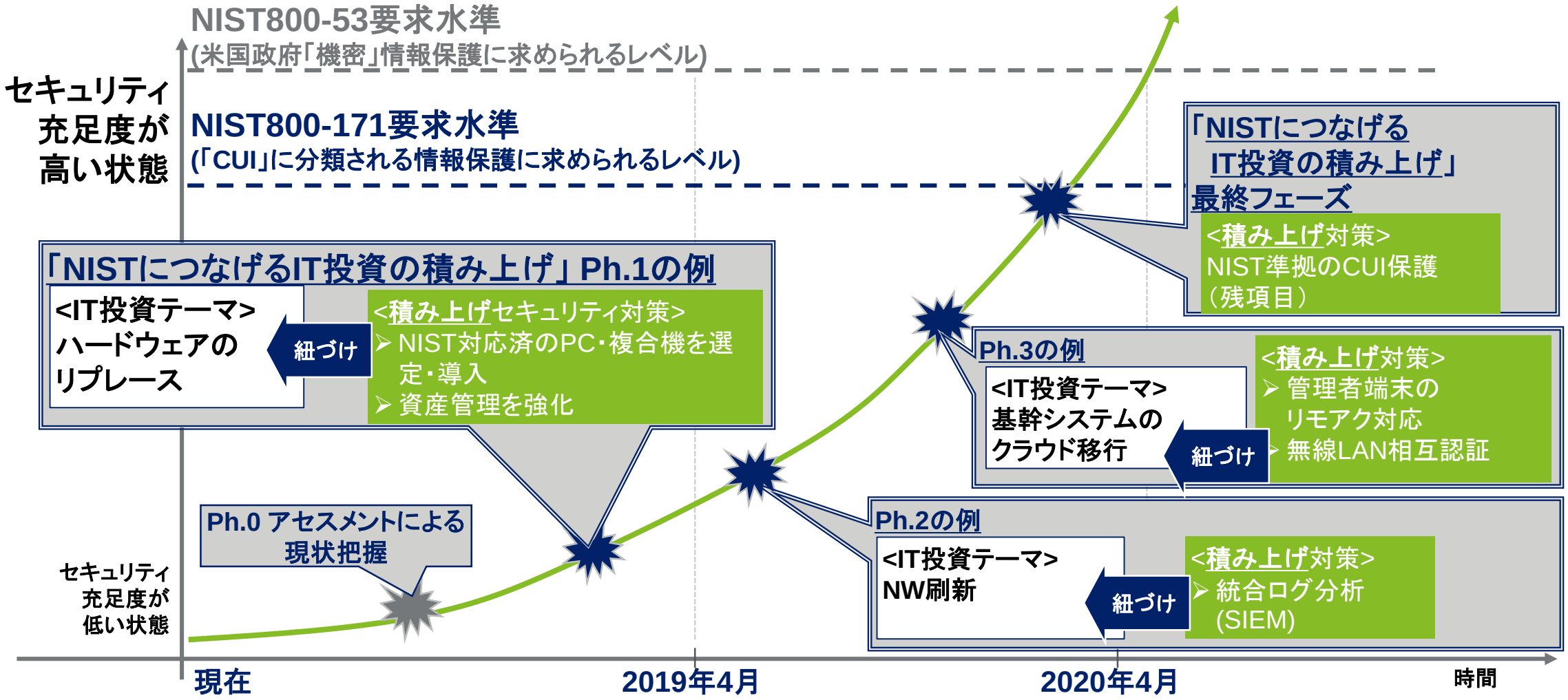
○　社内・社外のクラウドサービスを利用する際のセキュリティ要件のあり方に関する検討

国際標準に準拠したクラウドサービスを認定する枠組みについて、関係省庁等と協議の上検討

7. IT投資計画の見直し

NIST SP800-171要求水準に効率的に近づけるためには、ハード、ソフト、ネットワーク機器の購入計画を見直し、NIST要求水準を満たす商品へ入れ替えることが有効

「NISTにつなげるIT投資の積み上げ」のイメージ



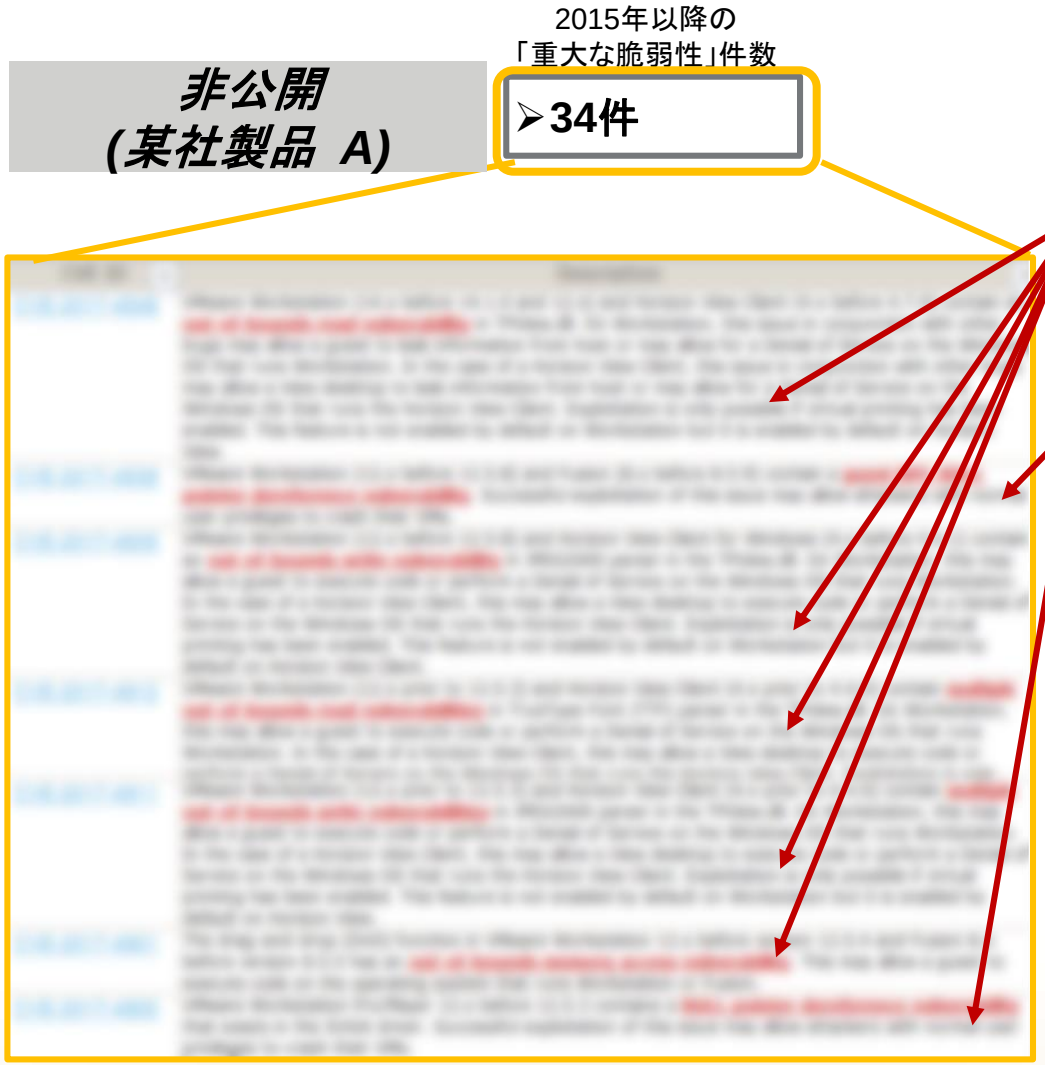
サイバー攻撃への致命的な脆弱性が多数報告されている製品群は、組織運用の足枷になるだけでなく、ゼロデイ攻撃のターゲットになり得るため、採用を回避、またはNIST推奨製品への入替を検討すべき

その他の「ブラックリスト製品」の例、具体リスク、代替推奨製品

	製品カテゴリ	「ブラックリスト製品」(※1)	脆弱性報告件数/主な内容 2015年以降の「重大な脆弱性」件数	脆弱性報告件数/主な内容 主な脆弱性の内容	代替となるNIST推奨製品(※2)
IT機器	スマートフォン	➢ *本日は非公開*	➢23件	NFCリーダ経由の不正コード実行	➢ *本日は非公開*
セキュリティ製品	アンチウィルス/EDR		➢23件	権限昇格攻撃	
	仮想化		➢34件	ヒープ領域破壊(Use-After-Free)	
	リモートアクセス管理		➢27件	リモートでのDoS攻撃	
	バックアップ		➢18件	認証のバイパス	

同一企業の製品群にも推奨／非推奨が存在することは、企業単位でなく製品単位でのセキュリティ設計良否の差異が存在することを示しており、選定時に考慮が必要

例：同一企業の異なる複数製品間の比較に考察



2015年以降の「重大な脆弱性」件数

非公開 (某社製品 A)

➢34件

■脆弱性の発現の傾向

- ➢割り当てを超えたメモリアクセスによる不正コード実行脆弱性
- ➢Nullポインタ例外を用いたVMクラッシュの脆弱性

■同社の別製品にとの比較

非公開 (某社製品 B)

2015年以降の「重大な脆弱性」件数

➢7件

→左記製品と同様の脆弱性種類の傾向は見られない

■考察

- ➢特定の脆弱性種類の頻繁な発現は、下記の要素に依存すると推察される
  - ✓アーキテクチャ
  - ✓コアライブラリ等コンポーネント選択
  - ✓開発チームのスキル等
- ➢こうした要素を多く含むか否かは、（企業ではなく）「製品固有の傾向」であると考えるべき