サイバーセキュリティの確保に向けた企業経営層向け意見交換会の開催

資料5－1

- 2024年７月26日(金)、内閣サイバーセキュリティセンターと日本経済団体連合会は、サイバーセキュリティの確保に向けた企業経営層向け意見交換会を実施しました。
- 意見交換会において、河野大臣は、昨今のサイバー情勢を踏まえ、我が国のサイバーセキュリティの強靱化のためには、**官民連携による取組を一層強化**していくことや、**経営トップのリーダーシップによる対策の着実な実施が重要**である旨について述べ、参加者との問題意識の共有を図りました。
- 本意見交換会には、**重要インフラ事業者や日本経済団体連合会会員企業など、様々な分野の企業等の経営層が参加**し、インシデント事例の共有や意見交換を通じて、官民連携の一層の深化を図りました。

開会の挨拶を行う河野大臣

開催概要

開催日時：2024年7月26日（金）8:00～9:00

開催場所：経団連会館

参加者　：重要インフラ事業者等の経営層
約200名

資　　料：NISC Webサイトに掲載

https://www.nisc.go.jp/pdf/policy/infra/ikenkoukan_gaiyou.pdf
https://www.nisc.go.jp/pdf/policy/infra/shiryo1.pdf
https://www.nisc.go.jp/pdf/policy/infra/shiryo2.pdf

資料５－２

サイバーセキュリティの確保に向けた企業経営層向け意見交換会

（当日配布資料）

令和６年７月26日
内閣サイバーセキュリティセンター

基本的なサイバーセキュリティ対策の徹底

- 令和５年における不正アクセス禁止法違反の検挙件数のうち、「利用権者のパスワードの設定・管理の甘さにつけ込んで入手」などID・パスワードの悪用が約９割を占めている。（警察庁「令和５年におけるサイバー空間をめぐる脅威の情勢等について」（令和６年３月）より）

  また、実際に窃取されダークウェブ等に掲載・取引されているID・パスワードについても、単純なパスワードが多いとの指摘がある。
- パスワードは長く複雑にして使い回さないといったことを含め、基本的な対策を徹底することが重要。
- NISC及び（独）情報処理推進機構（IPA）において、基本的なサイバーセキュリティ対策をHP等に掲載し、注意喚起を実施。

よく使われるパスワードの例
The world's most common online passwords

順位	パスワード	順位	パスワード
1	123456	6	12345
2	admin	7	password
3	12345678	8	123
4	123456789	9	Aa123456
5	1234	10	UNKNOWN

(出典)「The world's most common online passwords」に関し、世界経済フォーラム
https://www.weforum.org/agenda/2024/07/popular-passwords-cybercrime-digital-safety/

(出典) NISC　みんなで使おうサイバーセキュリティ・ポータルサイト
https://security-portal.nisc.go.jp/guidance/cybersecurity9principles.html

単純なパスワードを使わないなどの基本的な対策を徹底することが必要

JAXAにおいて発生した不正アクセスによる情報漏えい

- 昨年来、外部からJAXAに対して複数のサイバー攻撃が行われた。
- 昨年10月に判明したインシデントにおいて、JAXAが管理していた情報の一部（外部機関と業務を共同で実施するにあたっての情報および個人情報）が漏洩していたことを確認。

【侵害範囲】

①第三者がVPN装置の脆弱性を起点にJAXAの一部のサーバ及び端末に侵入。先だって公表された脆弱性が悪用された可能性が高い。

②侵入したサーバからさらに侵害を広げ、アカウント情報等を窃取。

③窃取したアカウント情報等を用いて、MS365に対して正規ユーザを装った不正アクセスを実施。

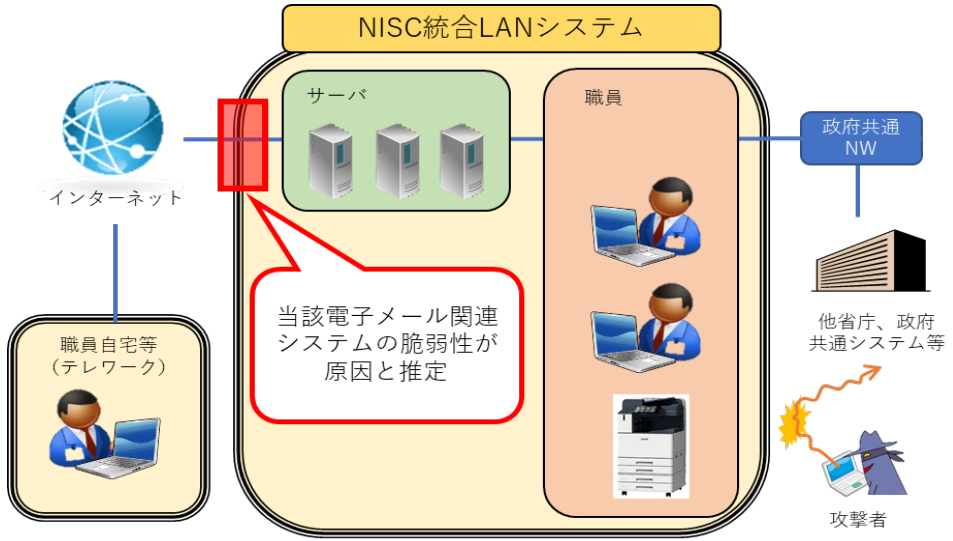
【対策】

- 脆弱性対応を迅速に行うための体制整備や内部通信ログの監視強化等の短期的対策を実施
- セキュリティを強化するための恒久対策を検討し、エンドポイントを含めたネットワーク全体の更なる監視強化、外部からの接続方法の改善、運用管理の効率化・可視化、なりすまし対策の強化等の対策を策定

関係機関等から提供される情報に十分に注意を払い、迅速に脆弱性への対応を行う必要

NISC電子メール関連システムからのメールデータ漏えい可能性

- NISCの電子メール関連システムに対し不正通信があり、インターネット経由で送受信した個人情報を含むメールデータの一部が外部に漏えいした可能性があることが判明、昨年８月に公表。
- 未知の脆弱性を悪用した攻撃（いわゆるゼロデイ攻撃）と推定。
- 機器交換等の対策を講じた上で、**内部監視等のサイバーセキュリティ対策を強化**。
- **対策等を講じた後、昨年秋に、新たな外部への不正通信の試みを検知、いずれも遮断**。
  （更なる被害を未然に防止。その後、新たな未知の脆弱性を悪用した攻撃であったことが判明。）



内部監視の強化など、ゼロトラストの考え方を踏まえた対策を講じることが有効

Living Off The Land 戦術（システム内寄生戦術）等への対応

- 近年、国際的に、Living Off The Land 戦術（システム内寄生戦術）といった、検知が容易でないサイバー攻撃が確認。国内においても、システム内に組み込まれている正規の管理ツールや標準機能を用いた侵害事例が見られている。
- 国外の様々な組織から検知方法や対策に関するレポートが発出されており、これらを参考にした取組を行うことで、サイバー攻撃に起因する被害の拡大や攻撃者による再侵入を防ぐことが可能。
- NISC及び一般社団法人JPCERT/CCからも注意喚起を発出。対策強化を推奨するとともに、各組織の経営層に対し、対応に必要となる人材、予算等の確保を併せて呼びかけ。

ファイブ・アイズ５か国及びマイクロソフト社が、中国背景とされるサイバー攻撃グループVolt Typhoonについて、注意喚起を発出（2023年5月）

- 有事における機能不全を念頭に置いた、**重要インフラへの事前のアクセス確保**（pre-positioning）を目的としたサイバー攻撃が発生
- 長期間の潜伏に必要な**高度な検知回避能力**が特徴
  - ✓ ネットワーク機器の脆弱性を突いて侵入。ゼロデイ脆弱性も悪用
  - ✓ マルウェアを使わず、正規ユーザになりすまし、正規ツールを駆使（Living off the Land）
  - ✓ 侵入痕跡となるログの消去 等
- 米国においては、本土及び島嶼部の米軍基地にサービスを提供する重要インフラ（通信、エネルギー、水道など）への攻撃の脅威が高まっている

(出典) PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure (2024.2) 等

JPCERT/CCが、攻撃活動への対応方法について解説する注意喚起を発出（2024年6月）

I. 概要
II. 攻撃概要と基本的な対処コンセプト
　（1）Volt Typhoonの攻撃活動の特徴
　（2）Volt Typhoonの攻撃への対処の基本コンセプト
III. 攻撃活動の事例
IV. 推奨調査項目（短期的な対応）
　・ドメインコントローラーでのログなどの調査　等
V. 推奨対策（中長期的な対策）
　・攻撃の侵入経路になり得るインターネットに接続されたアプライアンス（SSL-VPN等）の設定や運用の点検　等
VI. 参考情報

(出典)https://www.jpcert.or.jp/at/2024/at240013.html

攻撃の巧妙化・高度化を前提とし、関係機関等からの注意喚起も踏まえた対策が必要

サイバー攻撃の変遷

2005年　内閣官房情報セキュリティセンター設置

公開サーバへの攻撃

エストニア・2007年

ウェブサーバ・外向けサービスへの大量送信
SQLインジェクションによる情報漏えい 等

ウェブサイト・
インターネットバンキング等の停止

2015年　サイバーセキュリティ基本法施行（NISCも改組）

IT系システムの侵害

Wannacry・2017年
コロニアルパイプライン・2021年
大阪急性期・総合医療センター・
2022年

情報システム内部への侵入・暗号化
(主に既知の脆弱性を悪用)

暗号化・システム障害
身代金要求

有事に備えた重要インフラ等への侵入

ウクライナ・2015年/2022年等
Volt Typhoon・2023年

最深部・制御系システムに至る高度な侵入能力
（ゼロデイ脆弱性の積極活用など）
高度な潜伏能力
（Living-off-the-Landなど）

インフラ機能停止

機微情報の窃取の危険

Black Tech・2023年

情報システムへの権限外アクセス・利用

機密情報の漏えい・悪用

出典：サイバー安全保障分野での対応能力の向上に向けた有識者会議（第１回）資料

国家安全保障戦略（抄）

サイバー空間の安全かつ安定した利用、特に国や重要インフラ等の安全等を確保するために、**サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させる**。

【略】

武力攻撃に至らないものの、国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃のおそれがある場合、これを未然に排除し、また、このようなサイバー攻撃が発生した場合の被害の拡大を防止するために能動的サイバー防御を導入する。そのために、**サイバー安全保障分野における情報収集・分析能力を強化**するとともに、**能動的サイバー防御の実施のための体制を整備**することとし、以下の(ア)から(ウ)までを含む必要な措置の実現に向け検討を進める。

(ア) 重要インフラ分野を含め、**民間事業者等がサイバー攻撃を受けた場合等の政府への情報共有**や、**政府から民間事業者等への対処調整、支援等の取組を強化**するなどの取組を進める。

(イ) **国内の通信事業者が役務提供する通信に係る情報を活用**し、**攻撃者による悪用が疑われるサーバ等を検知**するために、所要の取組を進める。

(ウ) **国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃**について、**可能な限り未然に攻撃者のサーバ等への侵入・無害化ができるよう、政府に対し必要な権限が付与**されるようにする。

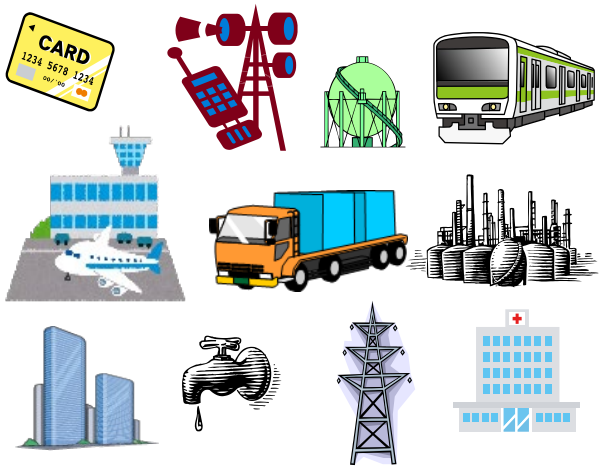
能動的サイバー防御を含むこれらの取組を実現・促進するために、**内閣官房サイバーセキュリティセンター（ＮＩＳＣ）を発展的に改組**し、**サイバー安全保障分野の一元的に総合調整する新たな組織を設置**する。そして、**これらのサイバー安全保障分野における新たな取組の実現のために法制度の整備**、運用の強化**を図る**。

全体イメージ

（サイバー安全保障分野での対応能力の向上に向けた有識者会議（第１回）資料）

「国民生活の基盤をなす経済活動」や「社会の安定性」をサイバー攻撃から守るため、
能動的なサイバー防御を実施する体制を整備する。

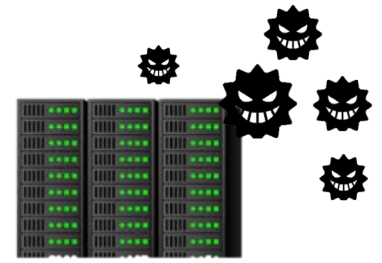
守る対象（例）



全てのステイクホルダーがメリットを実感できる
サイバー攻撃対応のエコシステムを官民を横断して構築

Internet

攻撃者



通信事業者

通信情報の活用
攻撃サーバ等を検知するため、明確な法的根拠を設けた上で、通信情報を活用

官民連携の強化
官民の情報共有により、事案の未然防止、対処支援強化を図る

アクセス・無害化措置
確認された攻撃サーバ等に対し、必要に応じ無害化

政　府