Cisco オンラインセミナー

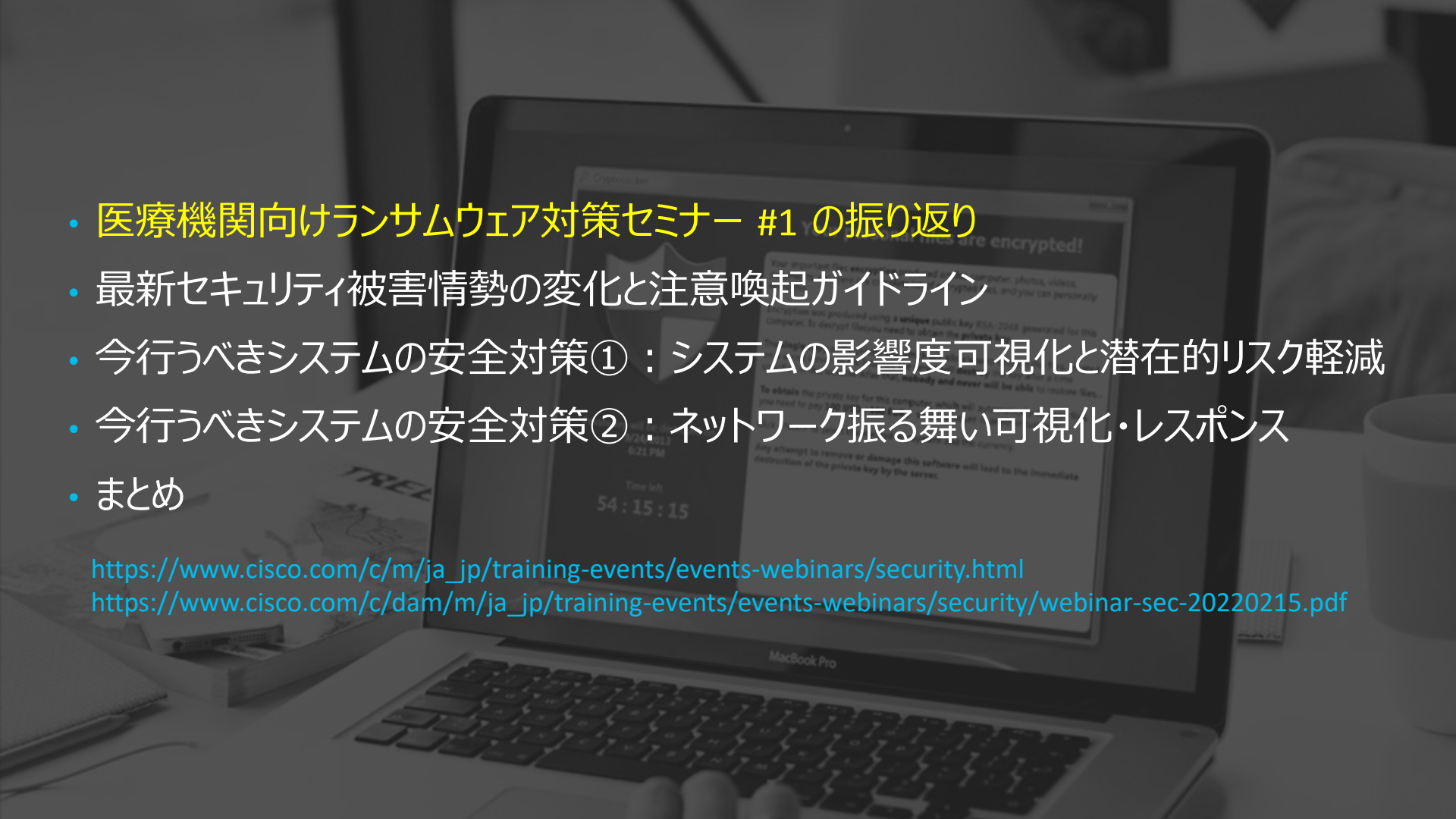
医療機関向け『ランサムウェア対策』セミナー #2

医療機関向けランサムウェア動向と 今行うべき安全対策 総まとめ

シスコシステムズ合同会社　セキュリティ事業
アーキテクト / エバンジェリスト　木村滋

2022/03/15

cisco



- 医療機関向けランサムウェア対策セミナー #1 の振り返り
- 最新セキュリティ被害情勢の変化と注意喚起ガイドライン
- 今行うべきシステムの安全対策①：システムの影響度可視化と潜在的リスク軽減
- 今行うべきシステムの安全対策②：ネットワーク振る舞い可視化・レスポンス
- まとめ

https://www.cisco.com/c/m/ja_jp/training-events/events-webinars/security.html
https://www.cisco.com/c/dam/m/ja_jp/training-events/events-webinars/security/webinar-sec-20220215.pdf

医療機関向け『ランサムウェア対策』セミナー #1

https://www.cisco.com/c/m/ja_jp/training-events/events-webinars/security.html
https://www.cisco.com/c/dam/m/ja_jp/training-events/events-webinars/security/webinar-sec-20220215.pdf

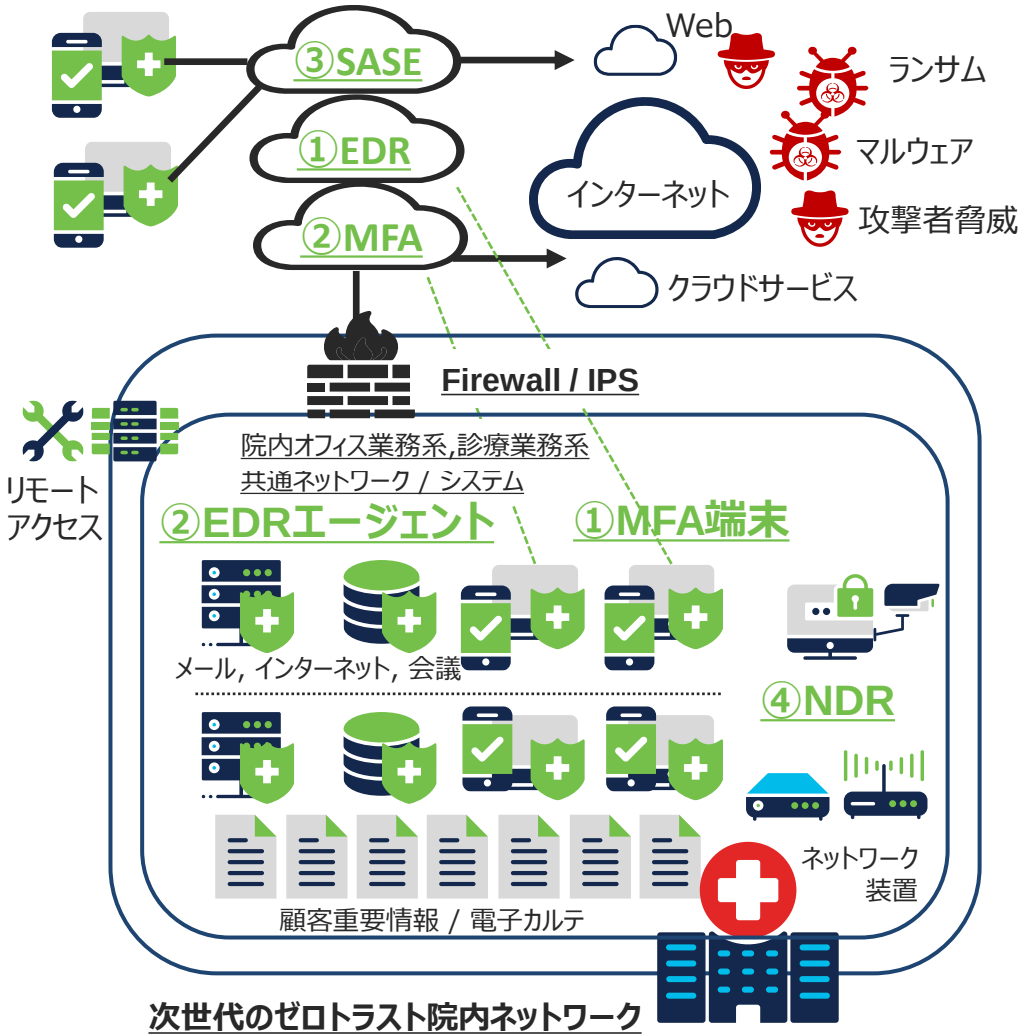
- 医療システムにおけるセキュリティの重要性と事故のポイント
- ランサムウェアの最新動向
- ランサムウェアと医療システムとの関連性と現実
- 厚生労働省の医療機関へのサポート事業（通知，指導，研修，ガイドライン）
- 「医療情報システムの安全管理に関するガイドライン第5.1版」
- 次世代医療情報システム向けゼロトラストアプローチ
- 次世代医療情報システム向けクラウドソリューションの選択
  - 1.MFA, 2.EDR, 3.SASE, 4.NDR

前回のアジェンダ内容の振り返り整理
今回のディスカッションポイント

ガイドラインに準拠：医療機関向け次世代システム

『医療情報安全管理に関するガイドライン』に基づくゼロトラストセキュリティの実現

- **クラウドサービスへの対応**
- **認証・パスワードの対応**
- **サイバー攻撃等による対応**
- **外部メンテナンス業者等の外部からのアクセスの対応**



医療情報システムの安全管理に関するガイドライン第5.1版

https://www.mhlw.go.jp/stf/shingi/0000516275.html

- **6. 医療情報システムの基本的な安全管理**
  - **医療情報システムセキュリティに関するシステム対策**
  - 医療情報システムセキュリティに携わる組織・管理・運用体制の実践

6.1. 方針の制定と公表 (※)
6.2. 医療機関等における情報セキュリティマネジメントシステム（ISMS）の実践
6.3. 組織的安全管理対策 (体制、運用管理規程) (※)
6.4. 物理的安全対策 (※)
6.5. 技術的安全対策 (※)
6.6. 人的安全対策 (※)
6.7. 情報の破棄 (※)
6.8. 医療情報システムの改造と保守 (※)
6.9. 情報及び情報機器の持ち出しについて (※)
6.10. 災害、サイバー攻撃等の非常時の対応 (※)

体制と管理システム，そのマネージメント

6.5 システムアプローチ

(※)「最低限のガイドライン」に従う対策を行う必要がある
制度上の要求事項（法律、厚生労働省通知、他の指導の要求事項）を満たすために必ず実施しなければならない
(2章 :本ガイドラインの読み方)

ガイドライン「6.5 技術的安全対策」の解釈のポイント

https://www.mhlw.go.jp/stf/shingi/0000516275.html

技術的安全対策の項目	項目番号	考えられる対策例	該当対策カテゴリ
(5) ネットワーク上からの不正アクセス	6.5B (5)	• 「Firewall」, 「IPS/IDS」はカテゴリとして導入推奨の明記がされている • コンピュータウイルス等が侵入した場合を想定した内部脅威監視　などのモニタリングが必要	Firewall / UTM / NGFW / IPS NDR (Network Detection Response) SASE / SIG (Secure Internet Gateway Medigate (医療機器可視化)

ガイドラインに準拠 : 医療機関向け次世代システム

『医療情報安全管理に関するガイドライン』に基づくゼロトラストセキュリティの実現

優先度の高いセキュリティソリューションカテゴリ : **MFA, EDR, SASE, SIG, NDR**

2要素 +α 他要素認証ソリューション

MFA

MFA (Multi Factor Authentication, Zero Trust)

次世代エンドポイント EDR + EPP

EDR

EDR (Endpoint Detection & Response)

統合クラウド・セキュリティ / DNSセキュリティ

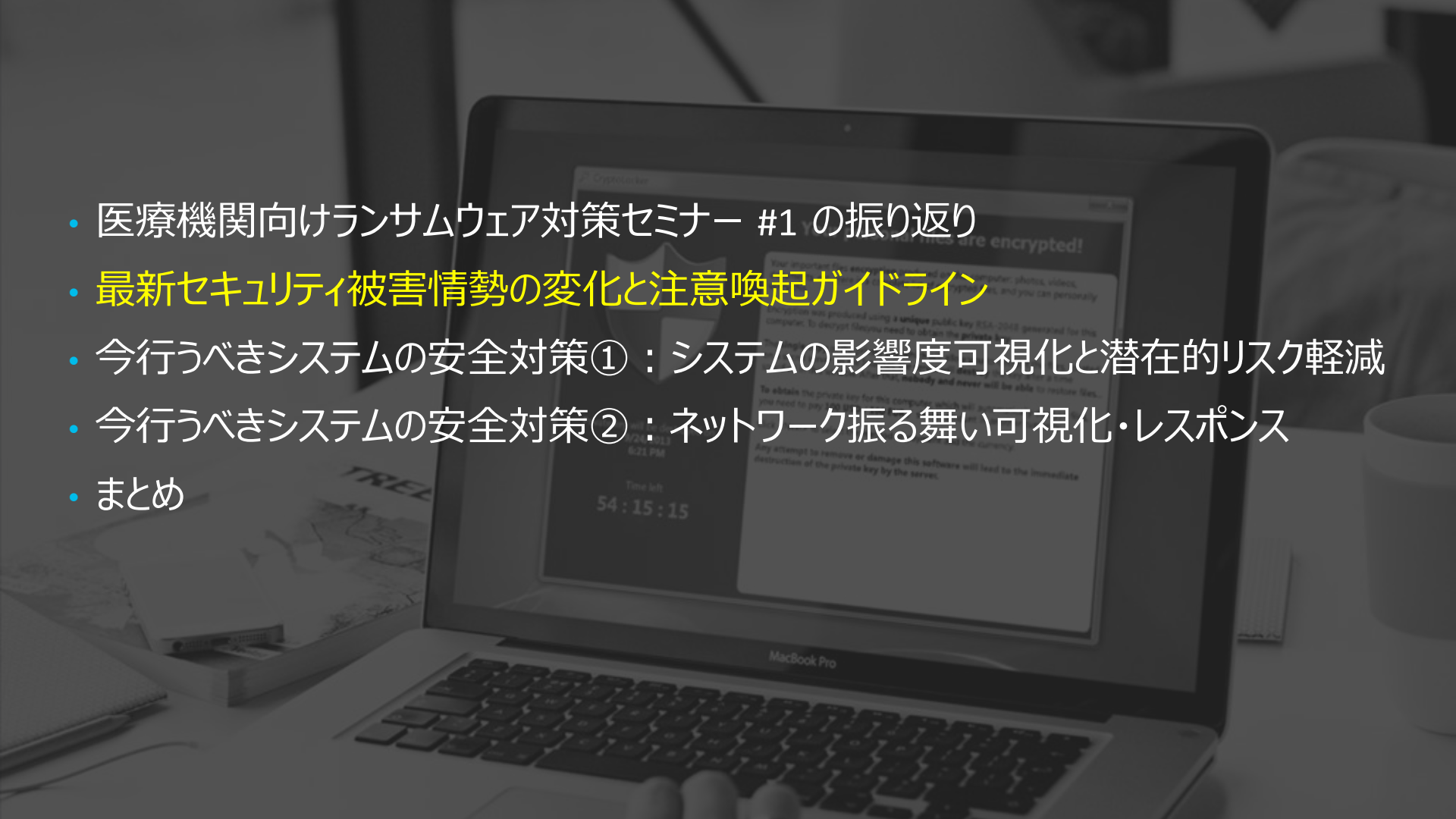
SASE / SIG

SASE (Secure Access Service Edge) / SIG (Secure Gateway)

振る舞いベースネットワーク可視化

NDR

NDR (Network Detection & Response)



- 医療機関向けランサムウェア対策セミナー #1 の振り返り
- 最新セキュリティ被害情勢の変化と注意喚起ガイドライン
- 今行うべきシステムの安全対策①：システムの影響度可視化と潜在的リスク軽減
- 今行うべきシステムの安全対策②：ネットワーク振る舞い可視化・レスポンス
- まとめ

ウクライナ情勢によるサイバー攻撃アクターの変化

『医療情報安全管理に関するガイドライン』に基づくゼロトラストセキュリティの実現

セキュリティ

ウクライナ情勢の進展に関するTalosの見解

木村 滋
2022年3月7日

ウクライナの活動に関するコンテンツ：

- ウクライナで進行中のサイバー攻撃に関する現在のエグゼクティブガイダンス
- 脅威アドバイザリ：HermeticWiper
- 脅威アドバイザリ: Cyclops Blink
- 群衆からの攻撃による新たな危機拡大リスク
- 改ざんとワイパーによるウクライナキャンペーンの継続的な注意喚起
- Cisco stands beside its customers in Ukraine

https://gblogs.cisco.com/jp/2022/03/security-talos-on-the-developing-situation-in-ukraine/

- 政治思想によるモチベーションの高いアクターグループが結集
  - 国家による支援を受けている高度なアクターグループ
  - 従来のサイバー犯罪者アクターグループ
    - 技術と精巧さが多岐にわたっている
- ウクライナ国内への攻撃
  - フェイク情報、改ざん、ワイパーマルウェア、BGPハイジャック（銀行向けハイジャック）
  - ウクライナ外務省、国防省、内務省、国立銀行へのDDoS

- **西側支援国への攻撃**
  - 米国国防省、大手国営銀行、ウクライナ高官へのDDoS
  - 西側支援諸国に対する、対ロシア制裁に対する国民の支持を低下させる目的
  - 国内産業、国内インフラに対し、制裁に伴うペナルティを強調する目的のサイバー作戦増加の可能性

日本政府側の動き

2022年3月1日に 経済産業省 / 金融庁 / 総務省 / 厚生労働省 / 国土交通省 / 警察庁 / NICT 各省庁 7組織連名で現在の情勢におけるサイバーセキュリティ注意喚起を発表
以下、https://www.meti.go.jp/press/2021/03/20220301007/20220301007-1.pdf より抜粋

サイバーセキュリティ対策の強化について（注意喚起）

昨今の情勢を踏まえるとサイバー攻撃事案のリスクは高まっていると考えられます。本日、国内の自動車部品メーカーから被害にあった旨の発表がなされたところです。

政府機関や重要インフラ事業者をはじめとする各企業・団体等においては、組織幹部のリーダーシップの下、サイバー攻撃の脅威に対する認識を深めるとともに、以下に掲げる対策を講じることにより、対策の強化に努めていただきますようお願いいたします。

また、中小企業、取引先等、サプライチェーン全体を俯瞰し、発生するリスクを自身でコントロールできるよう、適切なセキュリティ対策を実施するようお願いいたします。

さらに、国外拠点等についても、国内の重要システム等へのサイバー攻撃の足掛かりになることがありますので、国内のシステム等と同様に具体的な支援・指示等によりセキュリティ対策を実施するようお願いいたします。

実際に情報流出等の被害が発生していなかったとしても、不審な動きを検知した場合は、早期対処のために速やかに所管省庁、セキュリティ関係機関に対して連絡していただくとともに、警察にもご相談ください。

1．リスク低減のための措置
- ○パスワードが単純でないかの確認、アクセス権限の確認・多要素認証の利用・不要なアカウントの削除等により、本人認証を強化する。
- ○IoT 機器を含む情報資産の保有状況を把握する。特に VPN 装置やゲートウェイ等、インターネットとの接続を制御する装置の脆弱性は、攻撃に悪用されることが多いことから、セキュリティパッチ（最新のファームウェアや更新プログラム等）を迅速に適用する。
- ○メールの添付ファイルを不用意に開かない、URL を不用意にクリックしない、連絡・相談を迅速に行うこと等について、組織内に周知する。

2．インシデントの早期検知
- ○サーバ等における各種ログを確認する。
- ○通信の監視・分析やアクセスコントロールを再点検する。

3．インシデント発生時の適切な対処・回復
- ○データ消失等に備えて、データのバックアップの実施及び復旧手順を確認する。
- ○インシデント発生時に備えて、インシデントを認知した際の対処手順を確認し、対外応答や社内連絡体制等を準備する。

経産省注意喚起の解釈

【検討範囲】

- ✓ 政府機関や重要インフラ事業者をはじめとする各企業・団体等においてサイバー攻撃の脅威に対する認識を深めるとともに対策の強化に努める
- ✓ 中小企業 、取引先等、全体を俯瞰し、発生するリスクを自身でコントロールできるよう、適切なセキュリティ対策を実施

➢ 産業、業種、業態共通
➢ 理解を深め自組織で制御
➢ ガイドから実施へ

【対応策】

（リスク低減のための措置）
- ✓ パスワード強化対策
- ✓ IoT機器を含む情報資産の保有状況を把握と脆弱性対応
- ✓ フィッシングメール対策

システム的対応 : MFA

システム的対応 : パッチ、脆弱性管理

システム的対応 : メールセキュリティ

（インシデントの早期検知）
- ✓ サーバ等における各種ログ確認
- ✓ 通信の監視・分析やアクセスコントロールの再点検

運用管理
構成・設定管理

（インシデント発生時の適切な対処・回復）
- ✓ データ損失などに備えたデータバック実施と復旧手順の確認
- ✓ インシデント発生時の対応のための体制やプロセス、対処手順の整備

システム的対応
運用管理

組織・体制

➢ 情報資産の管理強化
➢ インフラにおけるセキュリティ対策強化
➢ セキュリティ運用の強化

CISA – “Shields Up”

https://www.cisa.gov/shields-up

CISA : Cybersecurity and Infrastructure Security Agency : アメリカサイバーセキュリティ庁 (https://www.cisa.gov/)
CISA Shield Up : 昨今の情勢に対する各組織のサイバー攻撃影響に備え対応するためのエグゼクティブガイドライン

サイバー攻撃からの防御
✓ **リモートアクセス、特権アクセス、管理アクセスに多要素認証を実装**
✓ ソフトウェア最新性の確認管理 : CISA 既知脆弱性カタログ参照
✓ 不必要サービス, ポートの制御
✓ クラウドサービスの制御強化 : https://www.cisa.gov/uscert/ncas/analysis-reports/ar21-013a
✓ 脆弱性スキャンによる侵入テストの実施

迅速な侵入検出への対策・運用
✓ ログの有効化
✓ **ネットワーク全体がマルウェア対策で保護されていること**

侵入発生時の組織体制
✓ テクノロジ、法務、事業継続、組織内の役割/責任分担、CSIRT、レスポンスチームの構成
✓ 机上演習の実施

システム的対応 : MFA

システム的対応 :
脆弱性管理, パッチマネージメント

システム的対応 : EDR, SASE, NDR

脅威アクターが利用する可能性のある脆弱性

Talos Blog Cisco / Kenna Top 10 Exploitable Vulnerability

Top 10 Exploitable Vulnerabilities

TALOS

CVE	Kenna Score	Description
CVE-2021-40444	100	Microsoft MSHTML Remote Code Execution Vulnerability
CVE-2021-36942	100	Windows LSA Spoofing Vulnerability
CVE-2021-34527	100	Windows Print Spooler Remote Code Execution Vulnerability
CVE-2022-0609	97	Google Chrome could allow a remote attacker to execute arbitrary code on the system, caused by a use-after-free in Animation. By persuading a victim to visit a specially crafted Web site, a remote attacker could exploit this vulnerability to execute arbitrary code or cause a denial of service condition on the system.
CVE-2021-21220	100	Insufficient validation of untrusted input in V8 in Google Chrome prior to 89.0.4389.128 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-0609	97	Google Chrome could allow a remote attacker to execute arbitrary code on the system, caused by a use-after-free in Animation. By persuading a victim to visit a specially crafted Web site, a remote attacker could exploit this vulnerability to execute arbitrary code or cause a denial of service condition on the system.
CVE-2020-1313	100	An elevation of privilege vulnerability exists when the Windows Update Orchestrator Service improperly handles file operations, aka 'Windows Update Orchestrator Service Elevation of Privilege Vulnerability'.
CVE-2020-0796	100	A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 3.1.1 (SMBv3) protocol handles certain requests, aka 'Windows SMBv3 Client/Server Remote Code Execution Vulnerability'.
CVE-2020-0646	100	A remote code execution vulnerability exists when the Microsoft .NET Framework fails to validate input properly, aka '.NET Framework Remote Code Execution Injection Vulnerability'.
CVE-2021-1675	100	Windows Print Spooler Elevation of Privilege Vulnerability

https://gblogs.cisco.com/jp/2022/03/security-ukraine-update/

CISA KNOWN EXPLOITED VULNERABILITIES CATALOG (95)
(CISA 既知の利用可能な脆弱性カタログ 95種)

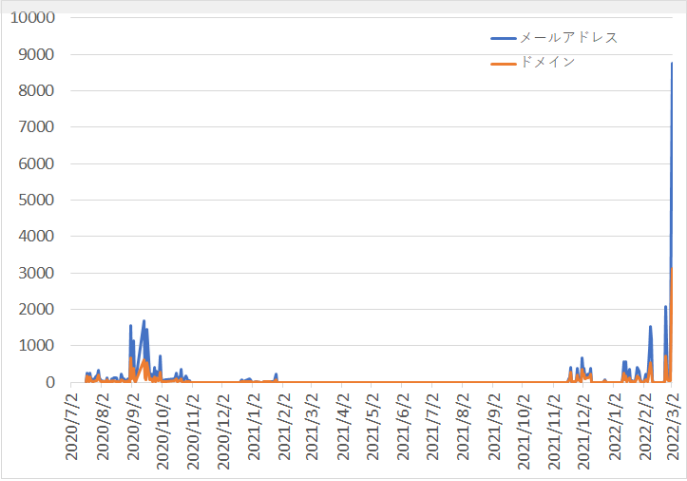
CVE	Vendor/Project	Product	Vulnerability Name	Date Added to Catalog	Short Description	Action	Due Date	Notes
CVE-2021-27104	Accellion	FTA	Accellion FTA OS Command Injection Vulnerability	2021-11-03	Accellion FTA 9_12_370 and earlier is affected by OS command execution via a crafted POST request to various admin endpoints.	Apply updates per vendor instructions.	2021-11-17	
CVE-2021-27102	Accellion	FTA	Accellion FTA OS Command Injection Vulnerability	2021-11-03	Accellion FTA 9_12_411 and earlier is affected by OS command execution via a local web service call.	Apply updates per vendor instructions.	2021-11-17	
CVE-2021-27101	Accellion	FTA	Accellion FTA SQL Injection Vulnerability	2021-11-03	Accellion FTA 9_12_370 and earlier is affected by SQL injection via a crafted Host header in a request to document_root.html.	Apply updates per vendor instructions.	2021-11-17	
CVE-2021-27103	Accellion	FTA	Accellion FTA SSRF Vulnerability	2021-11-03	Accellion FTA 9_12_411 and earlier is affected by SSRF via a crafted POST request to wmProgressstat.html.	Apply updates per vendor instructions.	2021-11-17	
CVE-2021-21017	Adobe	Acrobat and Reader	Adobe Acrobat and Reader Heap-based Buffer Overflow Vulnerability	2021-11-03	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a heap-based buffer overflow vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	Apply updates per vendor instructions.	2021-11-17	
CVE-2021-28550	Adobe	Acrobat and Reader	Adobe Acrobat and Reader Use-After-Free Vulnerability	2021-11-03	Acrobat Reader DC versions versions 2021.001.20150 (and earlier), 2020.001.30020 (and earlier) and 2017.011.30194 (and earlier) are affected by a Use After Free vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	Apply updates per vendor instructions.	2021-11-17	
CVE-2018-4939	Adobe	ColdFusion	Adobe ColdFusion Deserialization of Untrusted Data	2021-11-03	Adobe ColdFusion Update 5 and earlier versions, ColdFusion 11 Update 13 and earlier versions have an exploitable Deserialization of Untrusted Data	Apply updates per vendor	2022-05-03	

https://www.cisa.gov/known-exploited-vulnerabilities-catalog

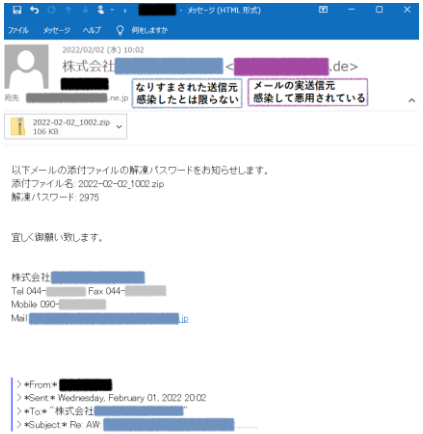
マルウェア Emotet の感染再拡大に関する注意喚起

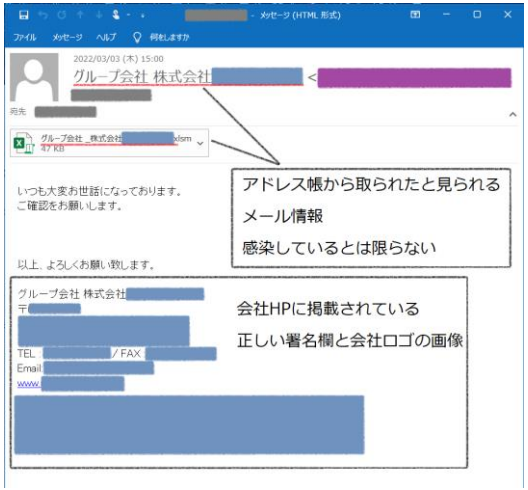
2022年2月10日にJPCERTからマルウェアEmotetの感染再拡大に関する注意喚起
（以下 https://www.jpcert.or.jp/at/2022/at220006.html から引用）

2022年3月に入り、Emotetに感染しメール送信に悪用される可能性のある.jpメールアドレス数が2020年の感染ピーク時の約5倍以上に急増しています。



［図1： Emotetに感染しメール送信に悪用される可能性のある.jpメールアドレス数の新規観測の推移 (外部からの提供観測情報)（2022年3月3日更新）］



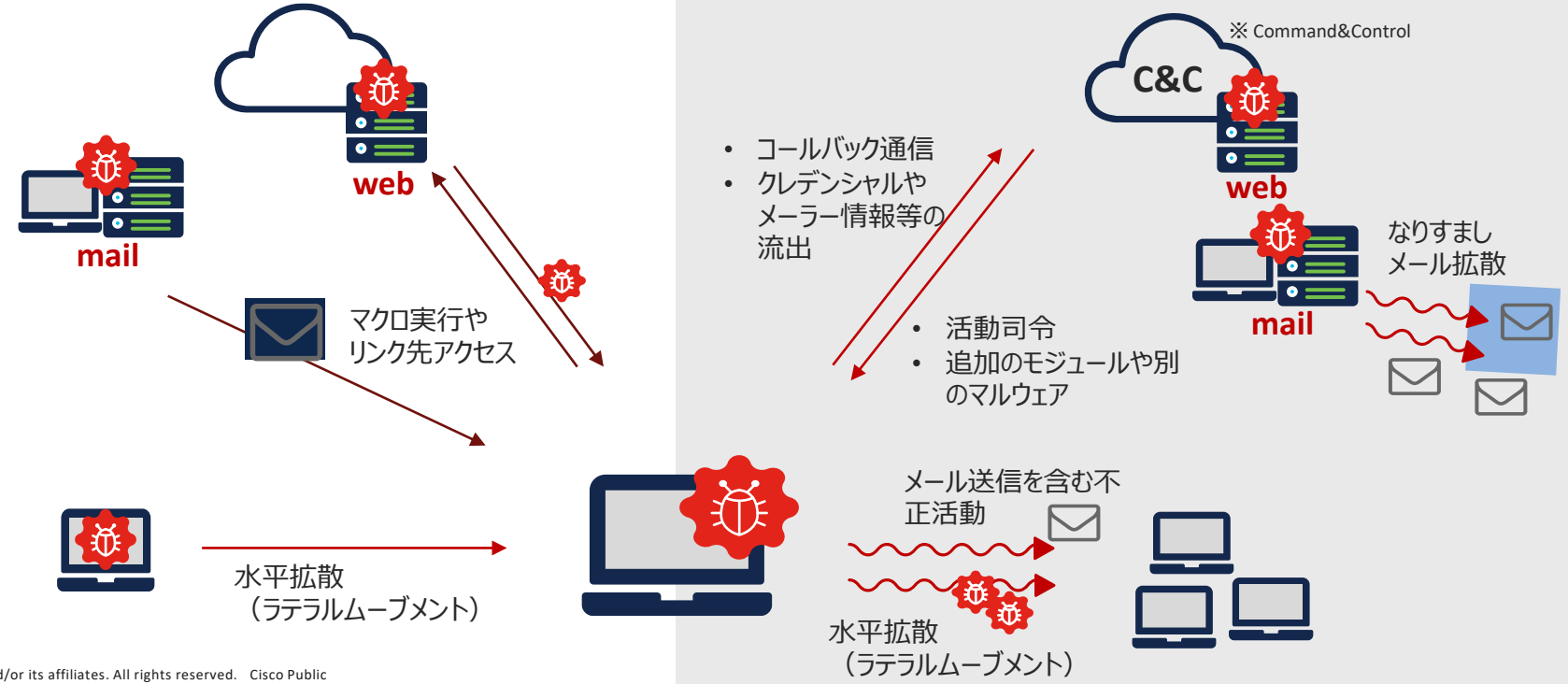


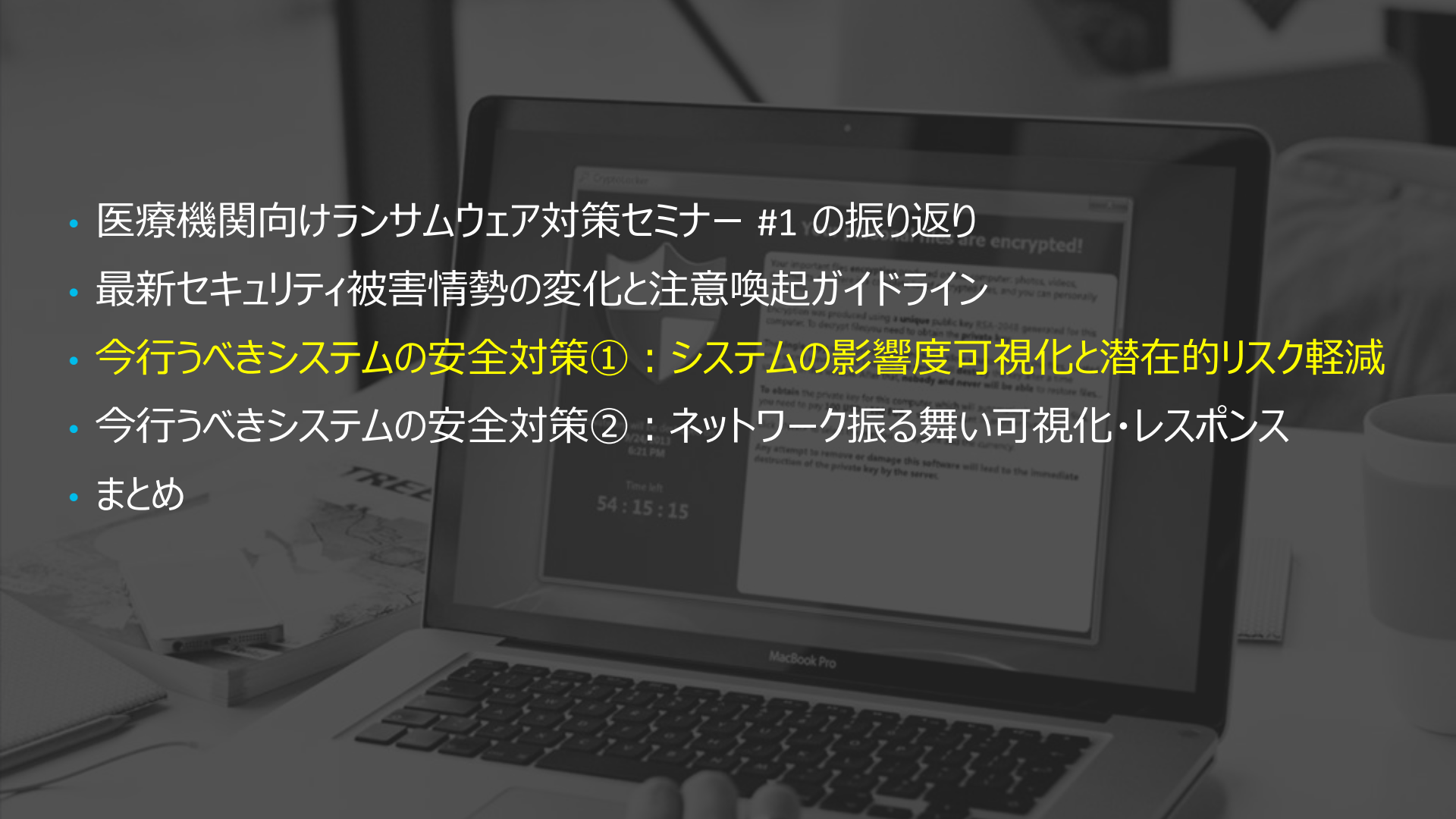
［図2, 図2-1：Emotetメールサンプル］

主にマクロ付きの Excel や Word ファイル、あるいはこれらをパスワード付き Zip ファイルとしてメールに添付する形式で配信されており、ファイルを開封 後にマクロを有効化する操作を実行することで Emotet の感染に繋がります。
（中略）メール本文中のリンクをクリックすることで悪性なExcelや Word ファイルがダウンロードされたり、アプリケーションのインストールを装い Emotet 感染をねらうケースも観測しています。

Emotet の感染拡大活動

活動は検知システムの回避技術を使いながら断続的に継続される





- 医療機関向けランサムウェア対策セミナー #1 の振り返り
- 最新セキュリティ被害情勢の変化と注意喚起ガイドライン
- 今行うべきシステムの安全対策①：システムの影響度可視化と潜在的リスク軽減
- 今行うべきシステムの安全対策②：ネットワーク振る舞い可視化・レスポンス
- まとめ

今行うべきシステムの安全対策①
システムの影響度可視化と潜在的リスク軽減

- ガイドラインに準拠可能な次期システム移行には時間が必要
  - 検討、稟議、承認、ベンダー選定、調整、スケジュール
- 既存診療システムに対して大きな変更ができない
- **最小限なシステム変更で実現**可能
- 事故・感染が起こってしまった、しかし**短時間で対処**可能

統合クラウド・セキュリティ / DNSセキュリティ

SASE / SIG

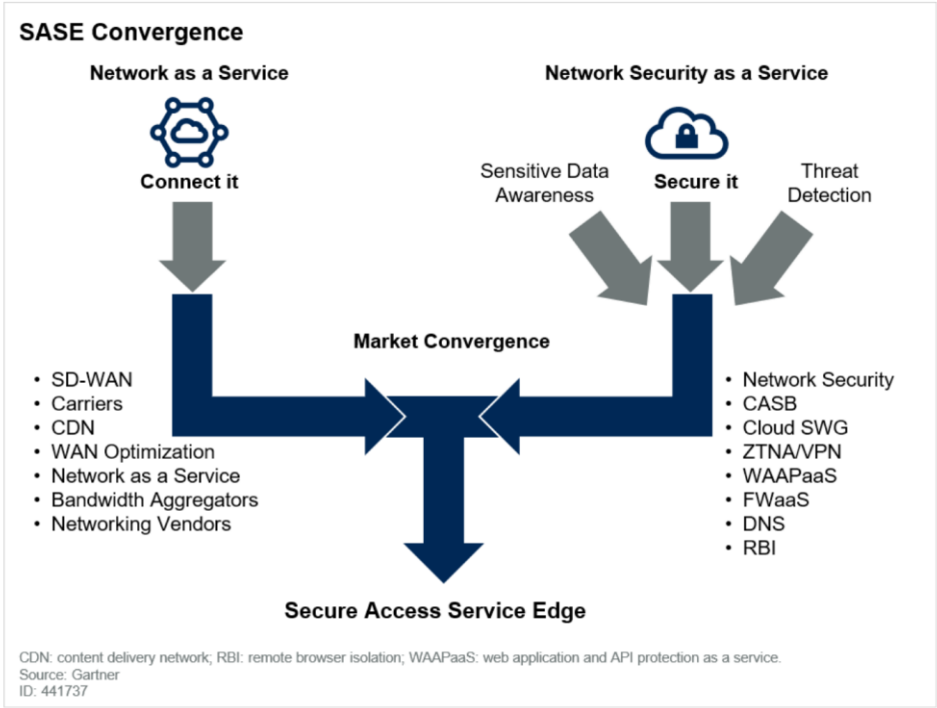
SASE (Secure Access Service Edge) / SIG (Secure Gateway)

今行うべき次期ベストソリューション①
- **クラウドサブスクリプション**
- **最低限なシステム変更で利用可能**
- **端末、ネットワークに変更無し**

Gartner定義 – SASE
Secure Access Service Edge

- SASE (Secure Access Service Edge)
  - 「包括的WAN/ネットワークセキュリティ機能 (**SWG, CASB, FWaaS, DNS Security**等) を組み合わせて、デジタル企業のダイナミックなセキュアアクセスのニーズをサポート」
  - SASE : **新興クラウドサービス**

Figure 1. SASE Convergence



Gartner - The Future of Network Security Is in the Cloud (SASE)
https://www.gartner.com/doc/reprints?id=1-1OG9EZYB&ct=190903&st=sb

SASE / SIG プロダクトの機能実装トレンド

SASE (Secure Access Service Edge) / SIG (Secure Internet Gateway)

サブスクリプション型ライセンス

SASE / クラウドセキュリティ製品の実装トレンド

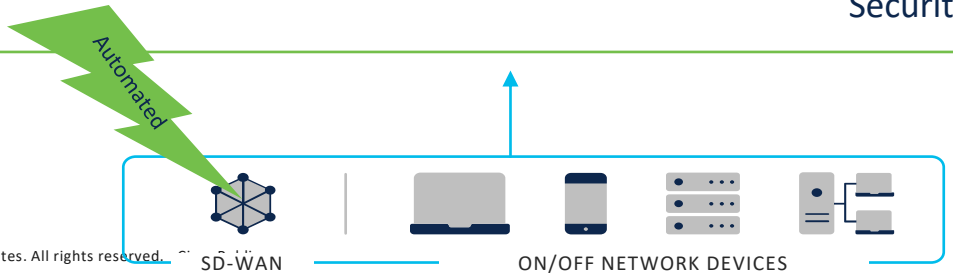
クラウド提供
DNS セキュリティ

・クラウド提供プロキシ
・RBI (ブラウザ隔離)

・クラウド提供 Firewall
・クラウド提供 IDS/IPS (L7アプリ認識)

・CASB (シャドーIT管理)
・DLP (情報漏えい保護)
(Cloud App & Data Security)

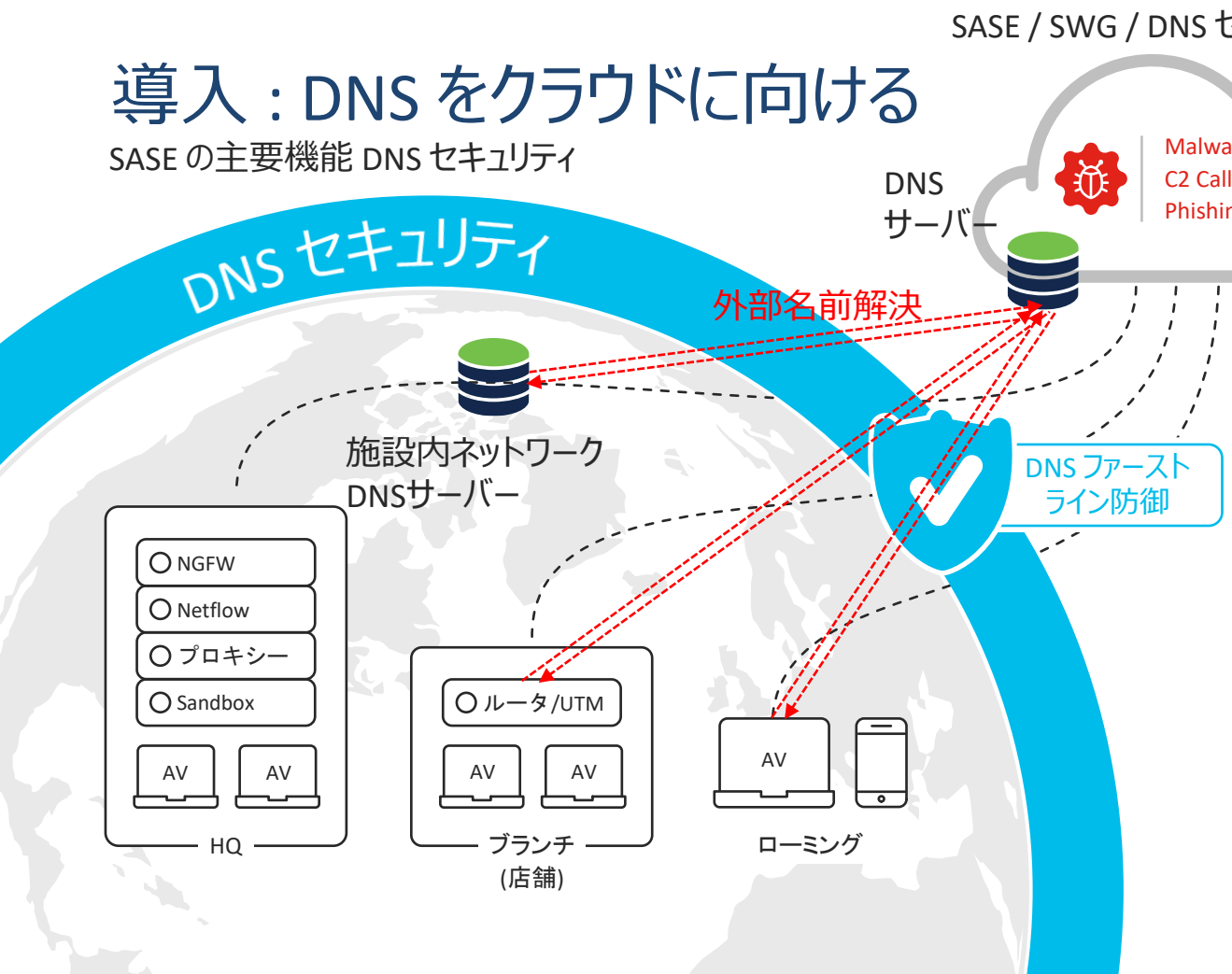
インタラクティブ脅威インテリジェンス



RBI (Remote Browser Isolation)
CASB (Cloud Access Security Broker)
DLP (Data Loss Prevention)

導入：DNS をクラウドに向ける

SASE の主要機能 DNS セキュリティ



導入効果

既存環境への影響度が無い

基礎設備 (DNS) 利用

DNSをクラウドに向けるだけ

数分でのグローバル展開可能

組織の影響度の迅速な現状把握

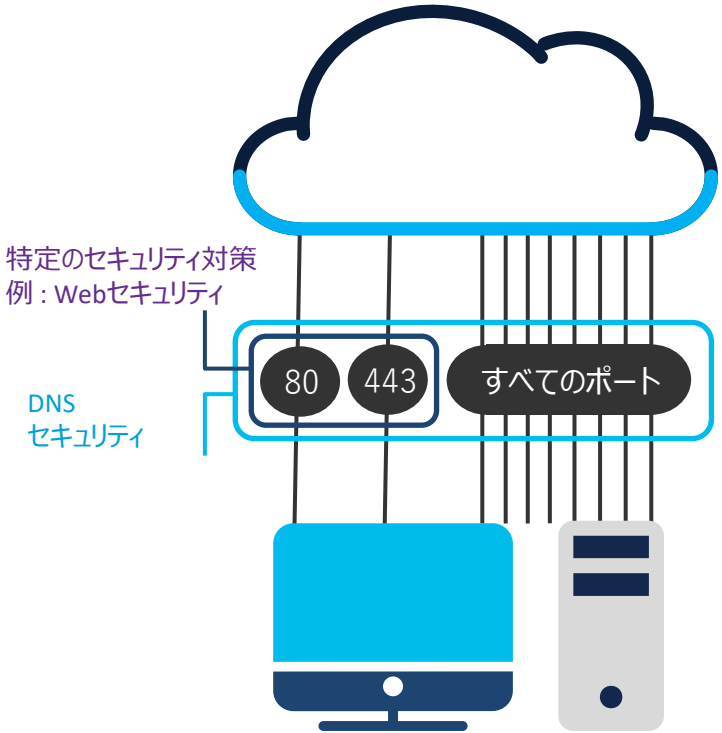
感染拡大の速やかな停止

簡単導入と効果 – DNS セキュリティ

SASE の主要機能 DNS セキュリティ : インターネットの基礎設備 (DNS) に構成可能

DNS セキュリティ により全内部端末の全外向き通信を保護

SASE の主要機能 DNS セキュリティ : インターネット の基礎設備 (DNS) に構成可能

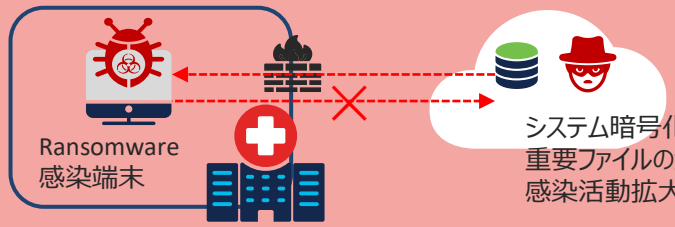


Web セキュリティ / Proxyでは、Port 80/443の通信のみが検査・保護の対象

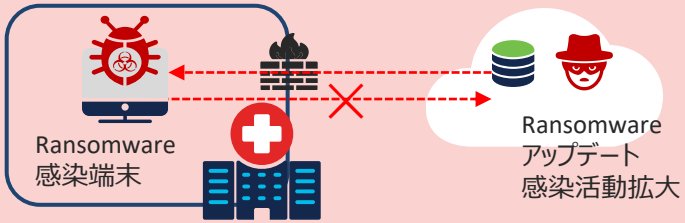
DNSで保護を行うため、全ポート/アプリが保護対象
(ポートやプロトコルに依存せず全てが対象)

ユースケース：DNS セキュリティ による効果

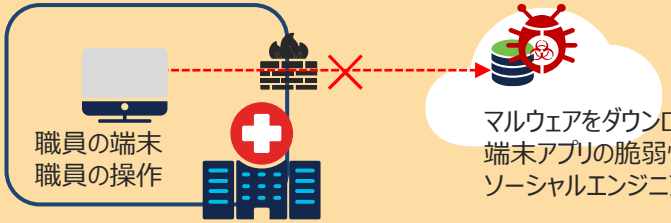
コマンドアンドコントロール (C&C) 通信
感染済み端末の漏洩・破壊活動実行を防止
ファイル暗号化, 漏洩, 内部システムへの展開



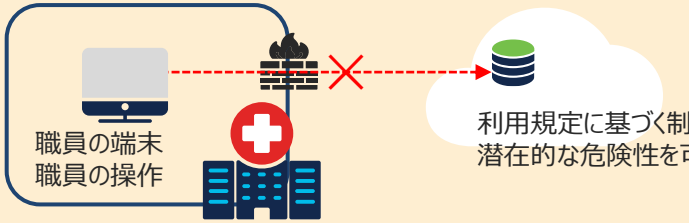
ドロッパーサイト, コマンドアンドコントロール (C&C) 通信
初期感染済み端末の活動多機能化を防止
初期感染からの感染拡大活動の抑止



マルウェア, フィッシング, 暗号化マイニング, 危険ドメイン
新規感染を防止
フィッシングメール, 偽装Webサイト, 詐欺SNS情報, の防止



URL フィルタリング
業務に関連しないサイトを防止 (アダルト, ギャンブル, 他)
利用規程の遵守, 潜在的な危険性を防止



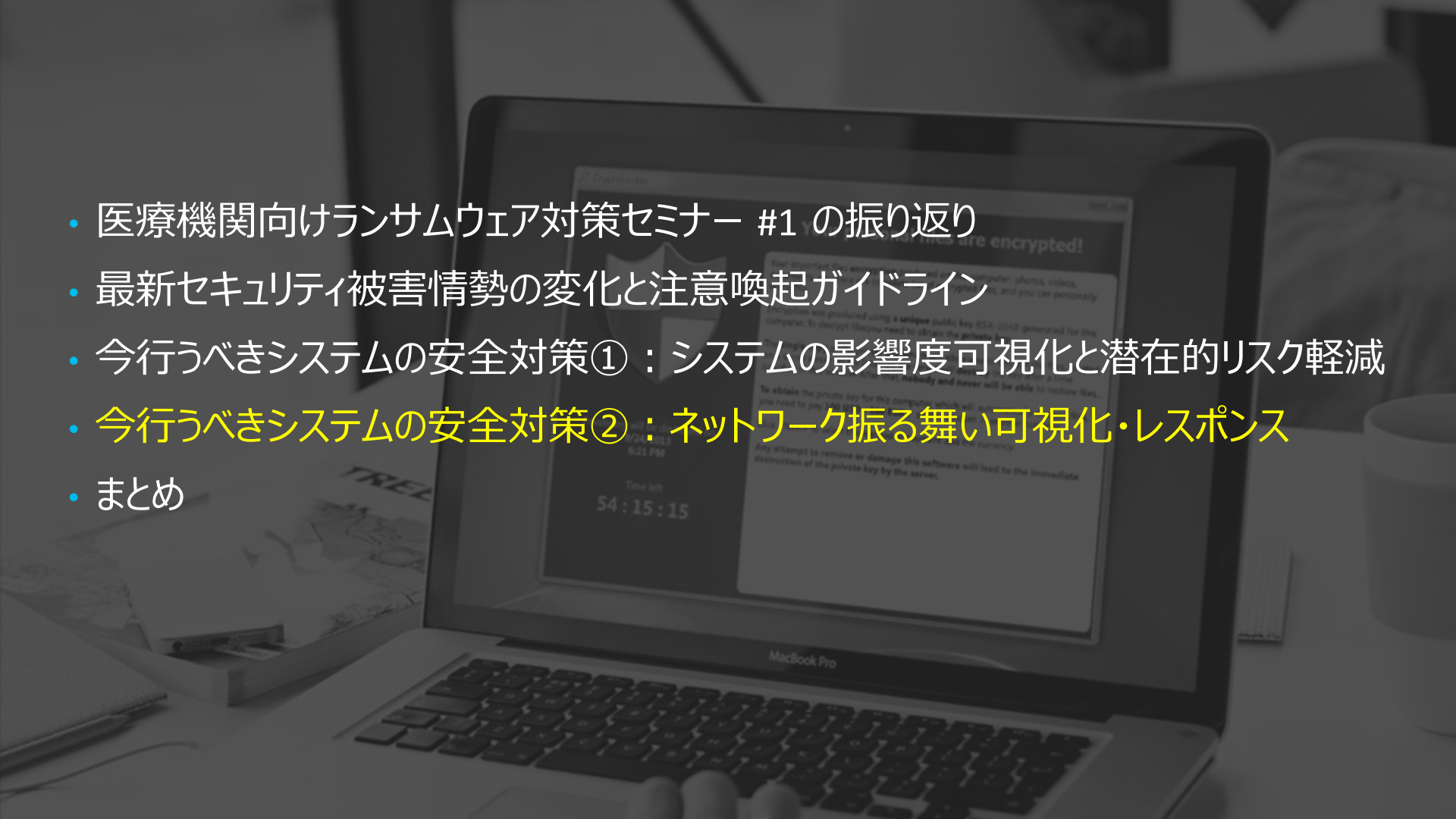
次のステップ : DNS セキュリティ から SASE へ

ベースライン強化から DX / テレワーク化対応へ

1. DNS セキュリティから利用を開始

2. SASE / SIG へマイグレーション

- DNS セキュリティ +α のクラウド・セキュリティ機能を利用
  - **+α クラウドセキュリティで診療ネットワークを強化**
  - **+α クラウドセキュリティでテレワークを本格導入**
    - +α : Firewall, IDS/IPS, クラウドシャドーIT管理, URLフィルタ, 情報漏洩防止, ブラウザ隔離
  - **UTM アップデート (ファームウェア, IPS シグネチャ, マルウェアパターン等) 負荷から脱却**
- **最新ガイドライン対応**
  - 6.5B (2) 情報の区分管理とアクセス権限の管理, 6.5B (4) 不正ソフトウェア対策, 6.5B (5) ネットワーク上からの不正アクセス



- 医療機関向けランサムウェア対策セミナー #1 の振り返り
- 最新セキュリティ被害情勢の変化と注意喚起ガイドライン
- 今行うべきシステムの安全対策①：システムの影響度可視化と潜在的リスク軽減
- 今行うべきシステムの安全対策②：ネットワーク振る舞い可視化・レスポンス
- まとめ

今行うべきシステムの安全対策②
ネットワーク振る舞い可視化・レスポンス

- ガイドラインに準拠可能な次期システム移行には時間が必要
  - 検討、稟議、承認、ベンダー選定、調整、スケジュール
- 既存診療システムネットワークリソースを有効活用
- 新要素である振る舞い検知を追加
  - マシンラーニング, AI, クラウドインテリジェンス を活用

今行うべき次期ベストソリューション②
- **シグネチャでなく振る舞いベース**
- **ポイントセキュリティで無くネットワーク全体の洞察を要素に追加**

振る舞いベースネットワーク可視化

NDR

NDR (Network Detection & Response)

Gartner定義 – NDR Network Detection & Response

- Network Detection & Response (NDR)
  - シグネチャベースでは無い技術（機械学習やその他の分析技術）
  - 実際のトラフィックフロー（NetFlowなど）の記録を分析しモデルを構築する
  - North-South方向の通信に加えて、East-West方向の通信も監視
  - 不審なネットワークとラフィックの検出に対応するための、自動または手動での応答機能を提供

Network Traffic Analysis (NTA) : 2019

↓

Network Detection & Response (NDR) : 2020

- 他のセキュリティツールが見落としている不審な活動を検出
- エージェントレス

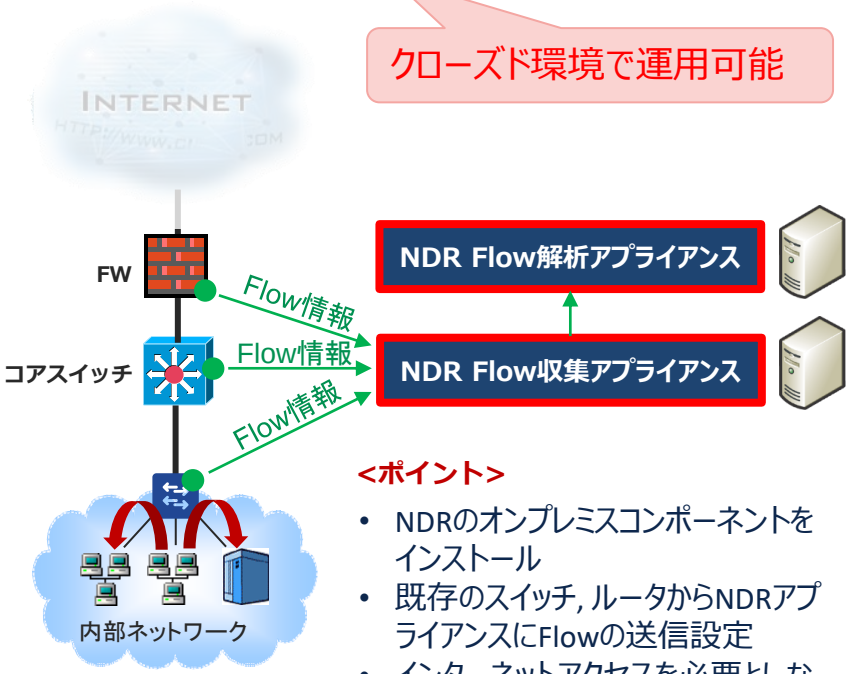
日本の産業市場における NDR の採用状況

NDR:2019-2025 CAGR(年平均成長率) :**28%** (日本)

出典：富士キメラ総研
「2020 ネットワークセキュリティビジネス調査総覧《市場編》」
ネットワークセキュリティビジネス市場の展望

導入：必要最低限なアプライアンス追加とネットワーク機器フロー収集設定

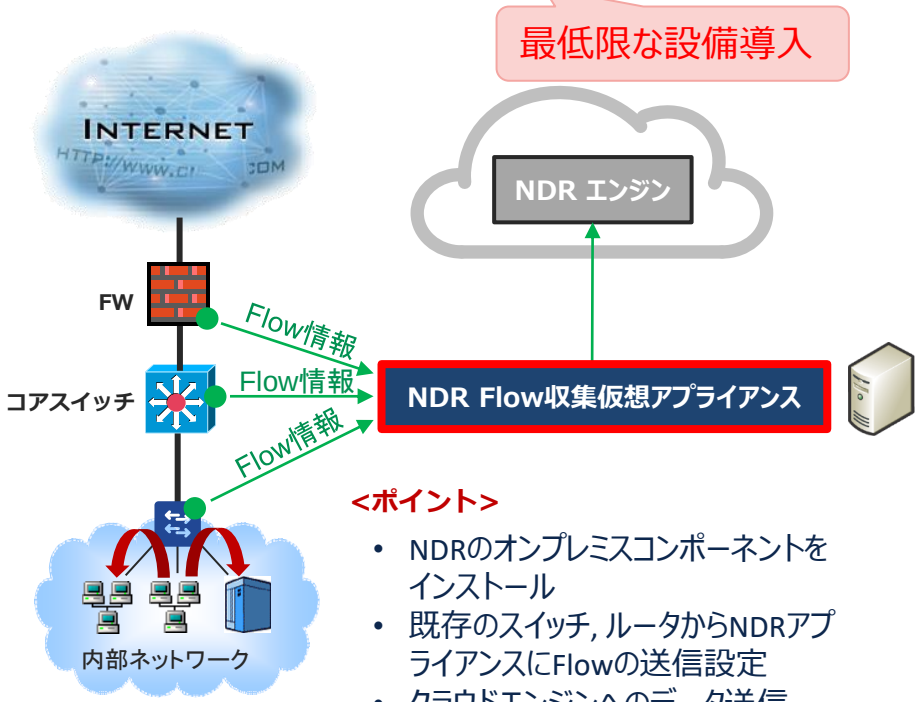
NDR オンプレミス エンジン型



<ポイント>

- NDRのオンプレミスコンポーネントをインストール
- 既存のスイッチ, ルータからNDRアプライアンスにFlowの送信設定
- インターネットアクセスを必要としない（クローズ環境にマッチ）

NDR クラウド エンジン型

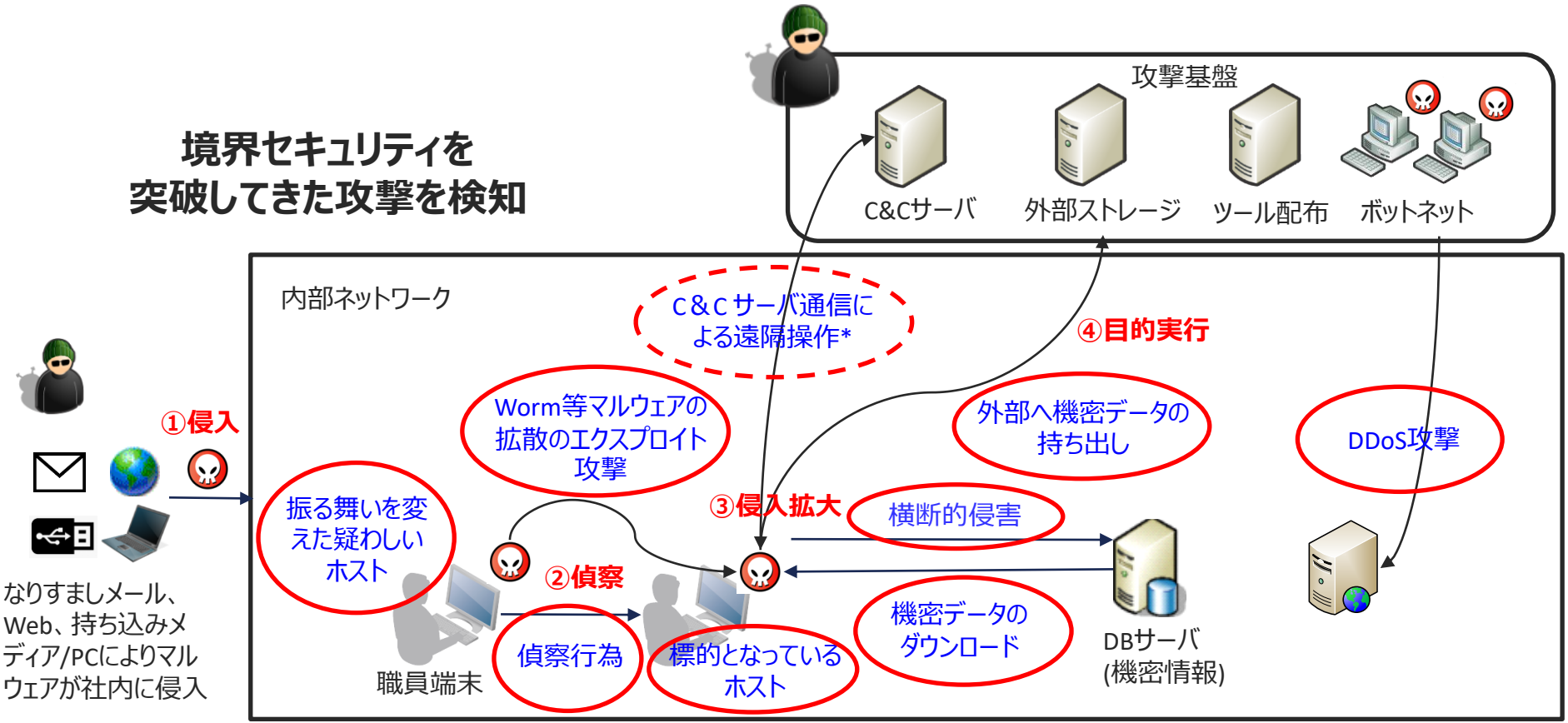


<ポイント>

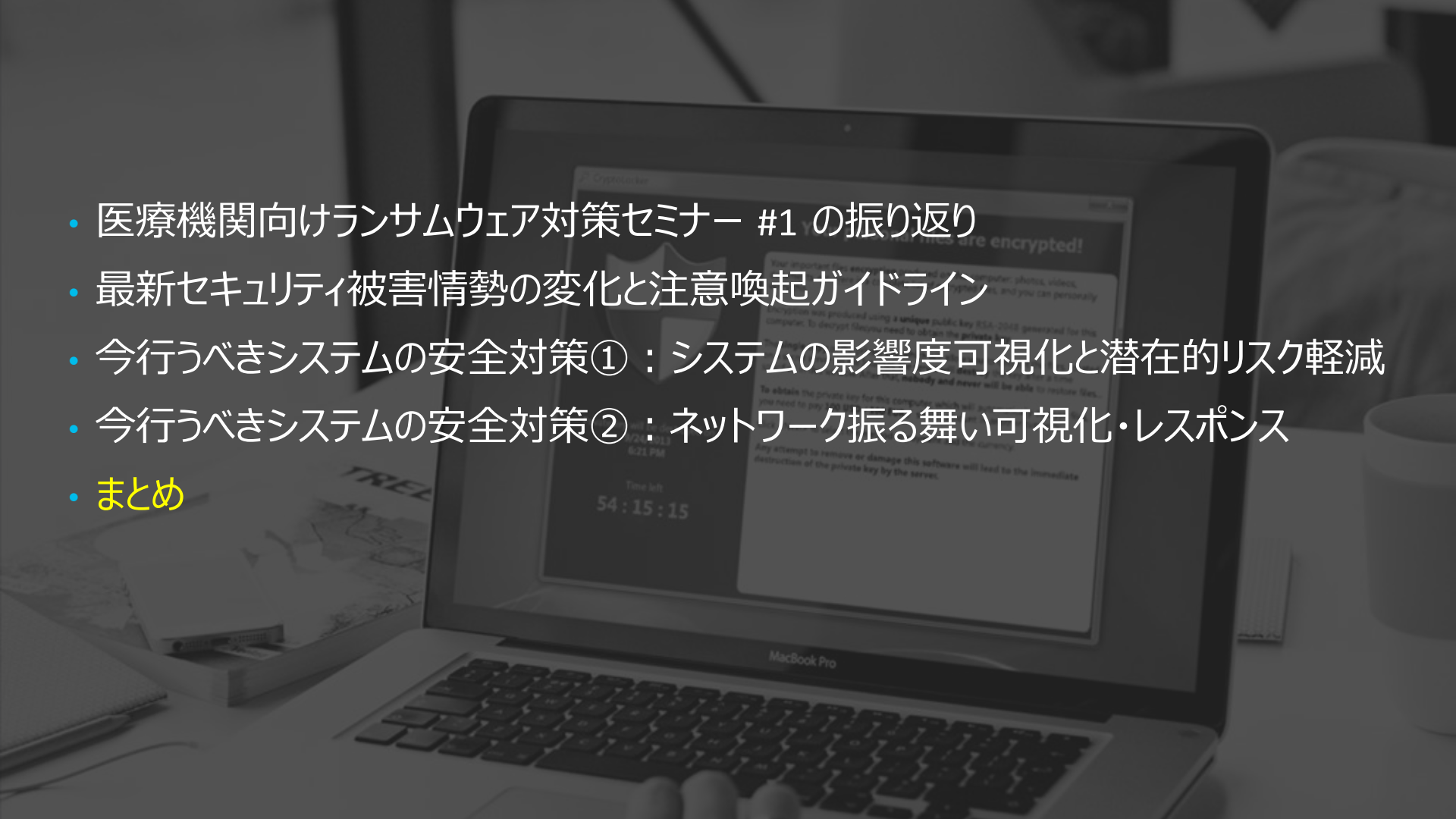
- NDRのオンプレミスコンポーネントをインストール
- 既存のスイッチ, ルータからNDRアプライアンスにFlowの送信設定
- クラウドエンジンへのデータ送信、ダッシュボードアクセスが必要

NDR の効果 : ランサムウェア, 内部犯行可能性の把握

境界セキュリティを
突破してきた攻撃を検知

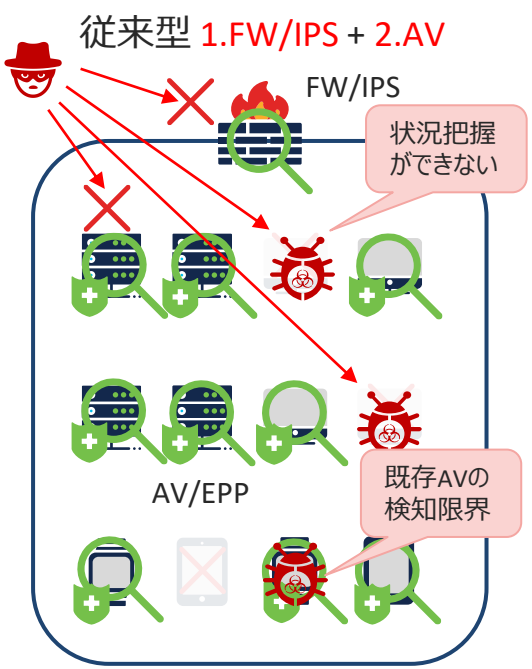


*C&Cサーバ通信を検知するためには別途有償ライセンスが必要のため点線で記載

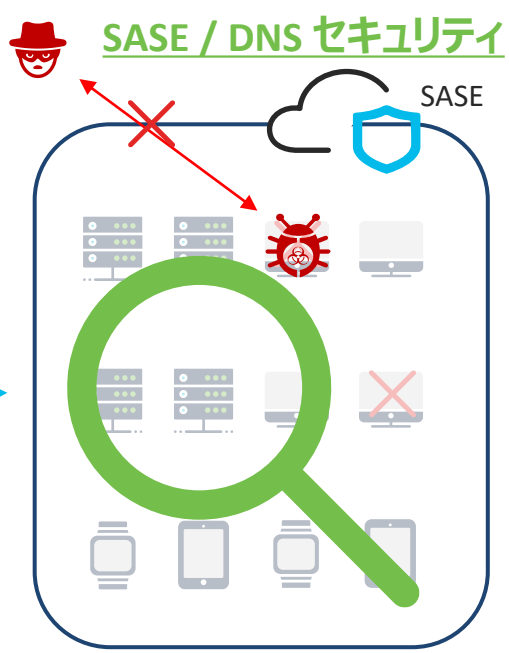


- 医療機関向けランサムウェア対策セミナー #1 の振り返り
- 最新セキュリティ被害情勢の変化と注意喚起ガイドライン
- 今行うべきシステムの安全対策①：システムの影響度可視化と潜在的リスク軽減
- 今行うべきシステムの安全対策②：ネットワーク振る舞い可視化・レスポンス
- まとめ

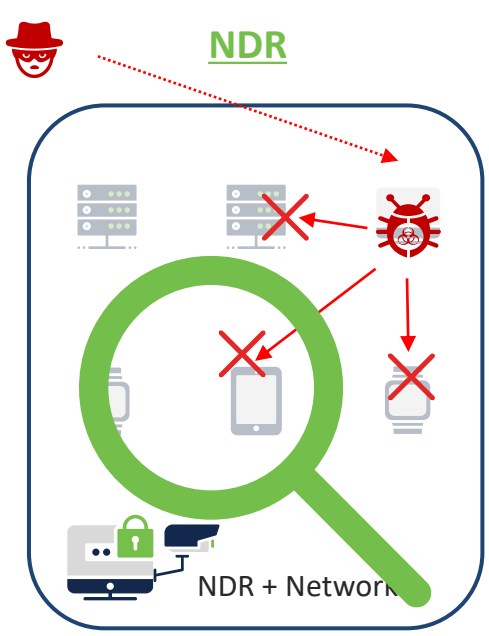
まとめ : SASE / DNS セキュリティと NDR の効果 : 共通



- FW / IPS / UTM による脅威把握一元化
- アップデートがされていないコンポーネント
- 全体影響度の可視化の課題
  - アップデート
  - インストールができない端末
  - 管理者の把握状況



- 全体像の可視化 (DNSベース)
  - 包括的洞察情報の提供
- 感染端末の把握と防御
- 新規感染活動の把握と防御
- 常に最新のインテリジェンスを利用



- 全体像の可視化 (ネットワークベース)
  - ネットワーク内部活動
  - 内部犯行、偵察活動の検知
  - 感染の横展開の検知

まとめ : SASE / DNS セキュリティと NDR の効果 : 共通

- **単一ポイントのみで監視・防御を行うアプローチの危険性**

  - セキュリティ対策は Firewall / IPS / UTM / メールセキュリティ / AV のみで安全（？）
  - ネットワーク境界の UTM / IPS シグネチャ、マルウェアパターンは常に情報がアップデートされている（？）
  - 常にすべての AV ソフトウェアを正しくアップデートしている（？）
  - エージェントがインストールできない端末（医療業務タブレット、IoT等）は無い（？）

- **全体像の把握を洞察と防御に利用するアプローチの重要性**

  - **端末、機器、ソフトウェア、防御のポイントのみに依存しないアプローチ**
  - **外部の客観的知見（インテリジェンス, 振る舞いエンジン）を取り入れるアプローチ**
  - **マシンラーニング / AI 利用**
    - **リアルタイムクラウド脅威インテリジェンスからの危険性のフィードバック**
    - **振る舞いベースのエンジン**

まとめ：医療機関向け『ランサムウェア対策』セミナー#2

- 医療機関向けランサムウェア対策セミナー #1 の振り返り
  - 診療ネットワークのオープン化DX化の重要性, ゼロトラストへの対応, 医療情報システムの安全管理に関するガイドライン第5.1版 6.5 技術的安全対策
  - 重要ソリューション : MFA, EDR, SASE/SIG, NDR

- 最新セキュリティ被害情勢の変化と注意喚起ガイドライン
  - ウクライナ情勢, Emotet, 国内外のガイドラインアップデート

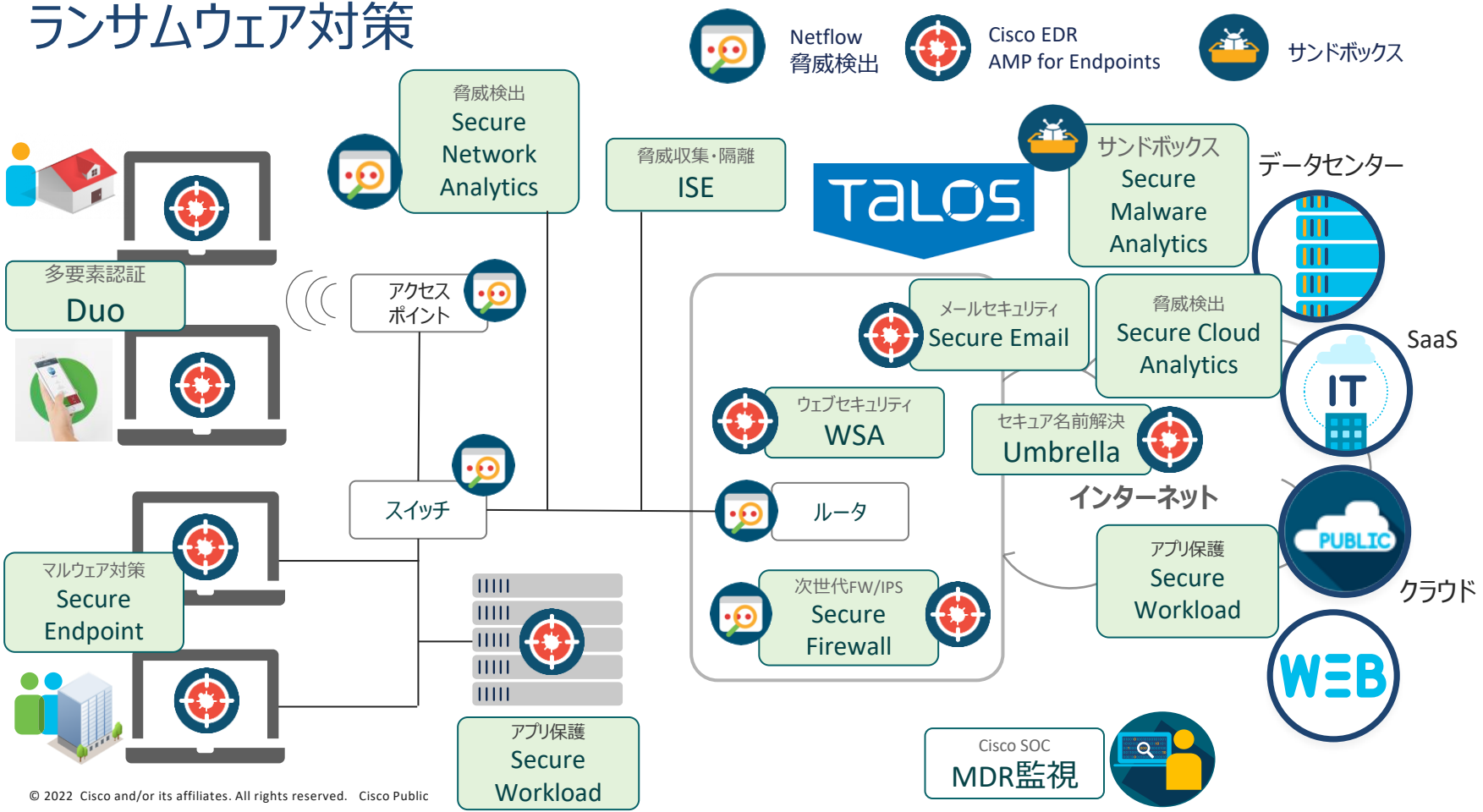
- **今行うべきシステムの安全対策①：システムの影響度可視化と潜在的リスク軽減**
  - DNS セキュリティ （+ SASE 今後の展開のポイント）
- **今行うべきシステムの安全対策②：ネットワーク振る舞い可視化・レスポンス**
  - NDR

Thank you

ランサムウェア対策

	侵入・初期感染	偵察・感染拡大	実行・被害	原因特定・対応
多要素認証 Duo	多要素認証で侵入を防御 端末の健全性を確認			
メールセキュリティ Secure Email	標的型メールを破棄 マルウェアファイルを破棄			
ウェブセキュリティ WSA	不正サイトアクセス防止 マルウェアファイルを破棄		C2通信の検出と遮断	
セキュア名前解決 Umbrella	不正サイトアクセス防止 マルウェアファイルを破棄		C2通信の検出と遮断	不正サイトアクセス継続監視 C2通信収束確認
次世代FW/IPS Secure Firewall	不正アクセスを防止 マルウェアファイルを破棄		C2通信の検出と遮断	
マルウェア対策 Secure EP (AMP)	マルウェア感染の防止・脅威の継続監視 侵入経路・拡散範囲の把握			脅威の継続監視 侵入経路・拡散範囲の把握
脅威検出 Secure N/CA		感染拡大を検出・継続的な監視 ラテラルムーブメント対策	C2通信の検出	脅威の継続監視 C2通信収束確認
脅威収集・隔離 ISE		脅威情報を集約、認証・認可 脅威の隔離・通信制御指示	脅威の隔離	
アプリ保護 Secure WR		感染拡大を検出・継続的な監視 ラテラルムーブメント対策	C2通信の検出と遮断	

ランサムウェア対策



Thank you

Possibilities